

# 负载均衡 操作指南





【版权声明】

©2013-2025 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】

## 🔗 腾讯云

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或95716。





## 文档目录

操作指南

负载均衡实例

域名化负载均衡升级指南

创建负载均衡实例

创建 IPv6 负载均衡实例

创建 IPv6 NAT64 负载均衡实例

配置负载均衡的转发域名

配置负载均衡安全组

内网负载均衡实例绑定 EIP

启停负载均衡实例

克隆负载均衡实例

导出负载均衡实例

升级为性能容量型实例

调整性能容量型实例规格

删除负载均衡实例

释放闲置实例

配置实例修改保护

配置实例删除保护

调整实例公网配置

负载均衡监听器

负载均衡监听器概述

配置 TCP 监听器

配置 UDP 监听器

配置 TCP SSL 监听器

配置 QUIC 监听器 配置 HTTP 监听器

配置 HTTPS 监听器

均衡方式

会话保持

七层重定向配置

七层个性化配置

七层转发域名和 URL 规则说明

CLB 支持 QUIC 协议

CLB 支持 SNI 多域名证书

七层协议支持 gRPC

#### 后端服务器

后端服务器概述 管理后端服务器 绑定弹性网卡 绑定云函数 SCF 跨地域绑定2.0(新版) 跨地域绑定1.0(旧版)



混合云部署 后端云服务器的安全组配置 健康检查 健康检查概述 配置健康检查 健康探测源 IP 支持100.64.0.0/10网段 健康探测源 IP 诊断助手 证书管理 管理证书 申请证书 证书要求及转换证书格式 SSL 单向认证和双向认证说明 日志管理 访问日志概述 查看操作日志 配置访问日志 抽样采集日志 配置健康检查日志 访问日志仪表盘 监控告警 获取监控数据 监控指标说明 配置告警策略 告警指标说明 访问管理 概述 授权定义 策略示例 传统型负载均衡 传统型负载均衡概述 配置传统型负载均衡 传统型负载均衡管理后端云服务器

## 操作指南 负载均衡实例 域名化负载均衡升级指南

最近更新时间: 2025-05-19 11:58:01

您可以对存量的公网负载均衡实例升级为域名化负载均衡实例。升级后负载均衡将以域名的方式提供服务,产品控制台将不再展示 VIP 信息。

## 升级前后负载均衡服务对比

对比项	升级后	升级前
SLA	99.99%	99.95%
是否支持域名	是	否
是否支持自动扩展 VIP	支持	不支持
VIP 是否会变化	随着业务请求的变化,VIP 可能会动态变化,且控制 台不再展示 VIP 地址	VIP 固定不变
健康探测源 IP	默认 100.64.0.0/10 网段,有效避免地址冲突	<b>默认负载均衡实例 VIP,可选</b> 100.64.0.0/10 网段

## 限制说明

- 基础网络中的实例不支持升级,请先完成迁移,详情请参见 迁移指导。
- 传统型负载均衡不支持升级,请先升级为负载均衡实例,详情请参见 传统型实例升级 。
- 容器创建的负载均衡实例暂时不支持控制台直接升级,如有升级需求,请寻求在线支持。
- DDoS高防包暂不支持对域名化负载均衡进行防护,升级为域名化负载均衡后,DDoS高防失效将严重影响业务安全。已绑定 DDoS高防包的公网负载均衡实例用户,或有DDoS防护需求的公网负载均衡实例用户,不建议升级为域名化负载均衡实例。如 有其他问题,请寻求在线支持。

## 前提条件

- 1. 客户对外提供访问使用 CNAME 域名解析的方式,详情请参见 配置负载均衡的转发域名 。
- 2. 健康探测源 IP 修改为 100.64.0.0/10 网段,详情请参见 健康探测源 IP 诊断助手。

## 操作步骤

### 方式一: 指定实例升级

- 1. 登录 负载均衡控制台。
- 2. (可选)通过健康探测源 IP 诊断助手,确认待升级实例的健康探测源 IP 为 100.64.0.0/10 网段,详情请参见 健康探测源 IP 诊断助手。
- 3. 在**实例管理**页面左上角选择地域,在实例列表找到目标实例,单击右侧操作栏下的**更多 > 升级为域名化实例**。

4. 记录升级弹窗中的分配域名,并将自有域名 CNAME 到分配的域名。

#### 5. 在**升级为域名化实例**弹窗中点击确定,完成升级。

<ul> <li>応/名称 网络类型</li> <li>応/名称 网络类型</li> <li>加/名称 风络类型</li> <li>加/名称 公网</li> <li>升级优势</li> <li>域名化公网负载均衡将以域名的方式提供服务请求动态变化,横向灵活扩展。</li> <li>升级前准备</li> <li>健康探测源 IP 修改为 100.64 网段,若在店 100.64.0.0/10 网段。 [2]</li> <li>升级共興</li> </ul>	分配域名 (	<ol> <li>当</li> <li>tencentclb.com</li> <li>1</li> <li>提升至99.99%,自动替换</li> </ol>	前 VIP 14 战障 VIP,降低对客户业务的	升级后 VIP 动态 IP 影响。弹性更佳,VIP 随业
ID/名称 网络类型       ゆ     公网       小級优势     公网       域名化公网负载均衡将以域名的方式提供服务请求动态变化、横向灵活扩展。       升级前准备       健康探测源 IP 修改为 100.64 网段、若在屁 100.64.0.0/10 网段。 ビ       升级共興	分配域名 (	〕 当 tencentclb.com 1	前 VIP 34 34 34 34	升级后 VIP 动态 IP 影响。弹性更佳,VIP 随业
b     方級优势     域名化公网负载均衡将以域名的方式提供服务请求动态变化,横向灵活扩展。 <b>升级前准备</b> 健康探测源 IP 修改为 100.64 网段,若在后 <u>100.64.0.0/10 网段。</u> [2]     升級先期	□ (务:可用性更强, SLA 从99.95%) 端服务器中配置有 iptables 等其他	tencentclb.com 1 提升至99.99%,自动替换	14 故障 VIP,降低对客户业务的	动态 IP 影响。弹性更佳,VIP 随业
<b>升级优势</b> 域名化公网负载均衡将以域名的方式提供服务请求动态变化,横向灵活扩展。 <b>升级前准备</b> 健康探测源 IP 修改为 100.64 网段,若在后 100.64.0.0/10 网段。 记	务:可用性更强,SLA 从99.95%排 就服务器中配置有 iptables 等其他	提升至 <b>99.99%,</b> 自动替换	故障 VIP,降低对客户业务的	影响。弹性更佳,VIP 随业
71 98 02 998		9安全策略时,注意放通该	网段,详细信息可参考 <mark>健康执</mark>	<u>深测源 IP 支持</u>
<ol> <li>通过配置 CNAME 域名解析的方式使用负</li> <li>2 执行升级操作</li> </ol>	0载均衡,详细信息可参考	<u>₹.</u> 12		
升级影响				
• 升级对 CLB 的 <b>转发服务没有影响,资费</b> 7	下变。			
• 升级后,控制台将不再展示 VIP 信息,VI	P 随业务请求而动态变化。			
• 升级后,不支持回滚。				

### 方式二: 批量实例升级

- 1. 登录 负载均衡控制台。
- 2. (可选)通过健康探测源 IP 诊断助手,确认待升级实例的健康探测源 IP 为 100.64.0.0/10 网段,详情请参见 健康探测源 IP 诊断助手。
- 3. 在实例管理页面左上角选择地域,在实例列表中勾选未升级的负载均衡实例。
- 4. 在实例列表上方,选择**更多操作 > 升级为域名化实例**。
- 5. 记录升级弹窗中的分配域名,并将自有域名 CNAME 到分配的域名。
- 6. 在**升级为域名化实例**弹窗中点击确定,完成升级。





```
健康探测源 IP 修改为 100.64 网段,若在后端服务器中配置有 iptables 等其他安全策略时,注意放通该网段,详细信息可参考 健康探测源 IP 支持
100.64.0.0/10 网段。 IZ
```

#### 升级步骤

1. 通过配置 CNAME 域名解析的方式使用负载均衡,详细信息可参考 使用指导。 🖸

#### 2. 执行升级操作。

#### 升级影响

- 升级对 CLB 的转发服务没有影响,资费不变。
- 升级后,控制台将不再展示 VIP 信息, VIP 随业务请求而动态变化。
- 升级后,不支持回滚。

如有其他问题,请提交<mark>工单申请</mark>。

确定	取消



## 创建负载均衡实例

最近更新时间: 2025-06-16 15:48:32

腾讯云提供了两种购买负载均衡的方式: 官网购买和 API 购买。本小节将详细介绍两种购买方式。

## 官网购买

所有用户均可通过 腾讯云官方网站 购买负载均衡。腾讯云账户分为标准账户类型和传统账户类型,2020年6月17日零点后注册的账户 均为标准账户类型,该时间点前注册的账户请在控制台查看您的账户类型,具体操作请参见 判断账户类型。

- 1. 登录腾讯云 负载均衡购买页。
- 2. 按需选择以下负载均衡相关配置。

#### 标准账户类型

参数	说明
计费模式	支持包年包月和按量计费两种计费模式。
地域	选择所属地域。CLB 支持的地域详情请参见 地域列表 。
实例类型	仅支持负载均衡实例类型。自2021年10月20日起停止购买传统型负载均衡,详情请参见 传统型负载均衡 停售公告 。
网络类型	网络类型分为公网和内网两种类型,详情请参见 网络类型 。 • 公网:使用负载均衡分发来自公网的请求。 • 内网:使用负载均衡分发来自腾讯云内网的请求。内网不支持配置以下的弹性公网 IP、IP 版本、运营商 类型、网络计费模式、带宽上限,默认不显示这些配置项。 不同计费模式下,网络类型支持情况不同: • 包年包月模式下,仅支持公网网络类型。 • 按量计费模式下,支持公网和内网两种网络类型。
弹性公网 IP	<ul> <li>不选择弹性公网 IP 时,腾讯云将为您分配一个公网 CLB,公网 IP 不可更改。(包年包月模式下的公网 CLB 默认仅支持不选择弹性公网 IP。)</li> <li>选择弹性公网 IP 时,腾讯云将为您分配一个弹性公网 IP 和一个内网 CLB,功能类似于公网 CLB。 (仅按量计费模式下的公网 CLB 支持选择弹性公网 IP。)</li> </ul>
IP 版本	CLB 的 IP 版本可以选择 IPv4、IPv6 或者 IPv6 NAT64。仅按量计费模式支持 IPv6 版本,其余限制情 况请参见 IP 版本 。IPv6 版本的负载均衡目前处于内测阶段,如需使用,请提交 工单申请 。
所属网络	<ul> <li>负载均衡支持的所属网络分为私有网络和基础网络。</li> <li>私有网络是用户在腾讯云上建立的一块逻辑隔离的网络空间,在私有网络内,用户可以自由定义网段划分、IP 地址和路由策略。</li> <li>基础网络是腾讯云上所有用户的公共网络资源池,所有云服务器的内网 IP 地址都由腾讯云统一分配,无法自定义网段划分、IP 地址。</li> <li>两者相比,私有网络较基础网络更适合有网络自定义配置需求的场景,且基础网络产品整体已于2022年12月31日正式下线,详情请参见基础网络下线通知。建议您选择私有网络。</li> </ul>
运营商类型	运营商类型分为:BGP(多线 )、中国移动、中国电信和中国联通。 • 包年包月模式下,仅支持 BGP(多线 )运营商类型,默认不显示此配置项。



	<ul> <li>按量计费模式下,支持以上4种选择。目前仅广州、上海、南京、济南、杭州、福州、北京、石家庄、武汉、长沙、成都、重庆地域支持静态单线 IP 线路类型,其他地域支持情况请以控制台页面为准。如需体验静态单线 IP 线路,请联系商务经理申请。申请通过后,即可在购买页选择中国移动、中国联通或中国电信的运营商类型。</li> </ul>
主/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备可用区。
实例规格	支持共享型实例和性能容量型实例。 <ul> <li>共享型实例按照规格提供性能保障,单实例最大支持并发连接数5万、每秒新建连接数5000、每秒查询数(QPS)5000。</li> <li>性能容量型实例按照规格提供性能保障,单实例最大可支持并发连接数1000万、每秒新建连接数100万、每秒查询数(QPS)30万。</li> </ul>
网络计费模 式	网络计费模式分为:按带宽计费(包月带宽)、按带宽计费(按小时带宽)、按流量、共享带宽包。 <ul> <li>包年包月的实例计费模式仅支持按带宽计费(包月带宽)的网络计费模式。</li> <li>按量计费的实例计费模式支持按带宽计费(按小时带宽)、按使用流量、共享带宽包三种网络计费模式。</li> </ul>
带宽上限	<ul> <li>共享型公网 CLB 带宽上限为2Gbps,共享型内网 CLB 带宽建议不要超过5Gbps。</li> <li>性能容量型 CLB 带宽上限依据所选规格而定,具体请参见 实例规格对比。</li> </ul>
所属项目	选择所属项目。
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	可输入60个字符,允许英文字母、数字、中文字符、"-"、"_"、"."。不填写时默认自动生成。

#### 传统账户类型

参数	说明
计费模 式	仅支持按量计费模式。
地域	选择所属地域。CLB 支持的地域详情请参见 地域列表 。
实例类 型	仅支持负载均衡实例类型。自2021年10月20日起停止购买传统型负载均衡,详情请参见 传统型负载均衡停 售公告 。
网络类 型	网络类型分为公网和内网两种类型,详情请参见 网络类型 。
IP 版本	CLB 的 IP 版本可以选择 IPv4、IPv6 或者 IPv6 NAT64。使用限制详情请参见 IP 版本 。IPv6 版本的负 载均衡目前处于内测阶段,如需使用,请提交 <mark>工单申请</mark> 。
所属网 络	负载均衡支持的所属网络分为私有网络和基础网络。



	<ul> <li>私有网络是用户在腾讯云上建立的一块逻辑隔离的网络空间,在私有网络内,用户可以自田定义网段划分、IP 地址和路由策略。</li> <li>基础网络是腾讯云上所有用户的公共网络资源池,所有云服务器的内网 IP 地址都由腾讯云统一分配,无法自定义网段划分、IP 地址。</li> <li>两者相比,私有网络较基础网络更适合有网络自定义配置需求的场景,且基础网络产品整体已于2022年12月31日正式下线,详情请参见基础网络下线通知。建议您选择私有网络。</li> </ul>
运营商 类型	运营商类型分为:BGP(多线)、中国移动、中国电信和中国联通。 目前仅广州、上海、南京、济南、杭州、福州、北京、石家庄、武汉、长沙、成都、重庆地域支持静态单线 IP 线路类型。其他地域支持情况请以控制台页面为准,如需体验,请联系商务经理申请。申请通过后,即可在购 买页选择中国移动、中国联通或中国电信的运营商类型。
实例规 格	支持共享型实例和性能容量型实例。 <ul> <li>共享型实例按照规格提供性能保障,单实例最大支持并发连接数5万、每秒新建连接数5000、每秒查询数 (QPS)5000。</li> <li>性能容量型实例按照规格提供性能保障,单实例最大可支持并发连接数1000万、每秒新建连接数100万、 每秒查询数(QPS)30万。</li> </ul>
所属项 目	选择所属项目。
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	可输入60个字符,允许英文字母、数字、中文字符、"_"、"_"、"."。不填写时默认自动生成。

- 3. 完成以上配置后,确认购买时长(仅包年包月模式支持)、购买数量、费用及服务协议,单击**立即购买**。
  - 包年包月模式:跳转至确认信息页面,若有可用的现金券或优惠券(代金券\折扣券),可勾选使用,核对信息无误后单击提交
     订单。在支付页面选择支付方式并完成支付。
  - 按量计费模式: 在弹出的负载均衡订单确认对话框中单击确定订单。
- 4. 购买成功后即开通负载均衡服务,您可进行负载均衡配置使用。

#### 共享型实例购买方式

- 1. 登录腾讯云 负载均衡购买页。
- 2. 参考以上 官网购买 的操作步骤,按需选择共享型负载均衡实例相关配置,在"实例规格"选择共享型。

实例规格 共享型 🗸

3. 继续参考以上 官网购买 的操作步骤完成后续操作。

#### 性能容量型实例购买方式

- 1. 登录腾讯云 负载均衡购买页。
- 2. 参考以上 官网购买 的操作步骤,按需选择性能容量型负载均衡实例相关配置,并且"实例规格"选择性能容量型。

包年包月的性能容量型实例



性能容量型	~				
型号	最大并发连接数(个)	每秒新建连接数(个)	每秒查询数(个)	带宽上限(Mbps)	折算LCU数
● 标准型(clb.c2.me	dium) 100,000	10,000	10,000	2,048	12
◯ 高阶型1(clb.c3.sn	nali) 200,000	20,000	20,000	4,096	24
○ 高阶型2(clb.c3.m	edium) 500,000	50,000	30,000	6,144	36
──超强型1(clb.c4.sn	nal) 1,000,000	100,000	50,000	10,240	60
○ 超强型2(clb.c4.m	edium) 2,000,000	200,000	100,000	20,480	130
◯ 超强型3(clb.c4.la	ge) 5,000,000	500,000	200,000	40,960	260
超强型4(clb.c4.xla	arge) 10,000,000	1,000,000	300,000	61,440	390
性能保障实例可按所选规	格保障性能指标				

#### 按量计费的性能容量型实例

实例规格	<b>性能容量型</b> 提供性能保障,转发性能不受其它到	➤ 实例的影响,单实例最大可支持最.	大并发连接数10,000,000,新建连	接数1,000,000,每秒查询数3	00,000。(计费说明 🖬 )
	型号	最大并发连接数(个)	每秒新建连接数(个)	每秒查询数(个)	带宽上限(Mbps)
	● 标准型(clb.c2.medium)	100,000	10,000	10,000	2,048
	高阶型1(clb.c3.small)	200,000	20,000	20,000	4,096
	高阶型2(clb.c3.medium)	500,000	50,000	30,000	6,144
	○ 超强型1(clb.c4.small)	1,000,000	100,000	50,000	10,240
	◎ 超强型2(clb.c4.medium)	2,000,000	200,000	100,000	20,480
	◎ 超强型3(clb.c4.large)	5,000,000	500,000	200,000	40,960
	◎ 超强型4(clb.c4.xlarge)	10,000,000	1,000,000	300,000	61,440
	按量计费模式下,所选规格为最高降	限速规格,LCU 单价不变,详见 🕻	↑费说明 🖸		

3. 继续参考以上 官网购买 的操作步骤完成后续操作。

## API 购买

🗲 腾讯云

欲通过 API 购买负载均衡的用户,请参见 负载均衡 API – 购买负载均衡实例。

## 后续操作

- 若需为负载均衡创建监听器,请参见 负载均衡监听器。
- 若需为负载均衡的监听器绑定后端服务,请参见 后端服务器。

## 相关文档

#### 产品属性选择



## 创建 IPv6 负载均衡实例

最近更新时间: 2025-05-19 11:58:01

#### () 说明:

- IPv6 负载均衡内测中,如需使用,请提交 工单申请。
- 目前仅支持如下地域开通 IPv6 负载均衡:广州、深圳金融、上海、上海金融、南京、北京、北京金融、成都、重庆、中国 香港、新加坡、弗吉尼亚、圣保罗。其中,针对地域为深圳金融、上海金融的金融行业监管要求定制的合规专区,需提交 工单申请使用专区。
- IPv6 负载均衡不支持传统型负载均衡。
- IPv6 负载均衡支持获取客户端 IPv6 源地址。四层默认透传 IPv6 负载均衡的客户端源地址,七层 IPv6 负载均衡通过
   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 的客户端无法访问该 IPv6 负载均衡。
- 互联网 IPv6 网络大环境还处于建设初期,如出现线路访问不通的情况,请提交工单反馈。

#### 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

腾讯云 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,腾讯云会给 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:



## 步骤1: 创建 IPv6 负载均衡实例

- 1. 登录腾讯云官网,进入 负载均衡购买页。
- 2. 按需选择以下负载均衡相关配置。

标准账户类型	
参数	说明
计费模 式	支持包年包月和按量计费两种计费模式。仅按量计费模式支持 IPv6 版本,其余限制情况请参见 IP 版 本 。
地域	选择所属地域。CLB 支持的地域详情请参见 地域列表 。
实例类 型	仅支持负载均衡实例类型。自2021年10月20日起停止购买传统型负载均衡,详情请参见 传统型负载均 衡停售公告 。
网络类 型	网络类型分为公网和内网两种类型,详情请参见 网络类型 。IPv6 负载均衡需选择公网类型。
弹性公 网 IP	不选择弹性公网 IP。
IP 版 本	选择 IPv6 版本。
所属网 络	选择所属网络,请选择已获取的私有网络和子网。若现有的网络不合适,可 新建私有网络 或 新建子 网 。
运营商 类型	运营商类型为 BGP(多线)。
实例规 格	支持共享型实例和性能容量型实例。 <ul> <li>共享型实例按照规格提供性能保障,单实例最大支持并发连接数5万、每秒新建连接数5000、每秒查 询数(QPS)5000。</li> <li>性能容量型实例按照规格提供性能保障,单实例最大可支持并发连接数1000万、每秒新建连接数100 万、每秒查询数(QPS)30万。</li> </ul>
双栈混 绑	启用后,该负载均衡实例的七层监听器可以同时绑定 IPv4和 IPv6的后端服务器,四层监听器不支持混 绑,只能绑定 IPv6的后端服务器。
网络计 费模式	网络计费模式分为:按流量、共享带宽包。
带宽上 限	<ul> <li>共享型公网 CLB 带宽上限为2Gbps,共享型内网 CLB 带宽建议不要超过5Gbps。</li> <li>性能容量型 CLB 带宽上限依据所选规格而定,具体请参考 实例规格对比。</li> </ul>
所属项 目	选择所属项目。
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	可输入60个字符,允许英文字母、数字、中文字符、"_"、"_"、"."。不填写时默认自动生成。
访问日 志	访问日志可助您快速从访问日志中监控客户端请求(流量、响应时间、状态码等 )、辅助排查问题,及用 户行为统计分析(PV/UV等),为业务运维/运营提供数据支持。
服务协 议	勾选"我已阅读并同意《腾讯云服务协议》和《负载均衡CLB服务等级协议》"。

#### 传统账户类型

参数	说明
计费模式	仅支持共享带宽包模式。
地域	选择所属地域。CLB 支持的地域详情请参见 <mark>地域列表</mark> 。
实例类型	仅支持负载均衡实例类型。自2021年10月20日起停止购买传统型负载均衡,详情请参见 传统型负载 均衡停售公告 。
网络类型	网络类型分为公网和内网两种类型,详情请参见 网络类型 。
IP 版本	选择 IPv6 版本。使用限制详情请参见 IP 版本。
所属网络	<ul> <li>负载均衡支持的所属网络分为基础网络和私有网络。</li> <li>基础网络是腾讯云上所有用户的公共网络资源池,所有云服务器的内网 IP 地址都由腾讯云统一分配,无法自定义网段划分、IP 地址。</li> <li>私有网络是用户在腾讯云上建立的一块逻辑隔离的网络空间,在私有网络内,用户可以自由定义网段划分、IP 地址和路由策略。</li> <li>两者相比,私有网络较基础网络更适合有网络自定义配置需求的场景,且基础网络产品整体已于2022年12月31日正式下线,详情请参见基础网络下线通知。建议您选择私有网络。</li> </ul>
运营商类 型	运营商类型为 BGP(多线)。
实例规格	<ul> <li>支持共享型实例和性能容量型实例。</li> <li>・共享型实例按照规格提供性能保障,单实例最大支持并发连接数5万、每秒新建连接数5000、每秒 查询数(QPS)5000。</li> <li>・性能容量型实例按照规格提供性能保障,单实例最大可支持并发连接数1000万、每秒新建连接数 100万、每秒查询数(QPS)30万。</li> </ul>
网络计费 模式	网络计费模式为共享带宽包。
带宽上限	1-1024Mbps。
所属项目	选择所属项目。
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	可输入60个字符,允许英文字母、数字、中文字符、"-"、"_"、"."。不填写时默认自动生



	成。
服务协议	勾选"我已阅读并同意《腾讯云服务协议》和《负载均衡CLB服务等级协议》"。

 在购买页选择各项配置后,单击**立即购买**。在负载均衡订单确认弹出窗口中,单击确认订单。返回至 负载均衡实例列表页,即可查 看已购的 IPv6负载均衡。

### 步骤2: 创建 IPv6 负载均衡监听器

- 1. 登录 负载均衡控制台,单击 IPv6负载均衡实例 ID,进入详情页。
- 2. 选择监听器管理标签页,单击新建,如创建一个 TCP 监听器。

说明:
 支持创建四层 IPv6负载均衡监听器(TCP/UDP/TCP SSL)和七层 IPv6负载均衡监听器(HTTP/HTTPS),详情请
 参见 负载均衡监听器概述。

- 3. 在**基本配置**中配置名称、监听协议端口和均衡方式,单击下一步。
- 4. 配置健康检查,单击**下一步**。
- 5. 配置会话保持,单击**提交**。
- 6. 监听器创建完成后,选中该监听器,在右侧单击绑定。

 说明: 绑定云服务器前,请确定该云服务器已获取 IPv6地址。

7. 在弹出框中,选择需要通信的 IPv6云服务器,并配置服务端口和权重,单击确定即可。

## 更多操作

### IPv6 CLB 混绑 IPv6 和 IPv4 后端服务

开启双栈混绑后,IPv6 CLB 七层监听器,可以同时绑定 IPv6 和 IPv4 的后端云服务器,并支持从 XFF 中获取源 IP。IPv6 CLB 四 层监听器不支持混绑,只能绑定 IPv6 的后端服务器。

- 1. 开启双栈混绑。
- 在购买页购买 IPv6 CLB 时,启用双栈混绑。

双栈混绑	✓ 启用双栈混绑
	启用后,该负载均衡实例的七层监听器可以同时绑定 IPv4 和 IPv6的后端服务器,四层监听器不支持混绑,只能绑定 IPv6 的后端服务器

#### • 在 IPv6 CLB 实例详情页面,启用双栈混绑。

÷	- Ib-	(lb-	)		
	基本信息	监听器管理	重定向配置	监控	安全组
	基本信息				
	名称	lb- )	<i>p</i> *		
	ID	lb-	6		
	状态	正常			
	VIP			(IPv6) <b>F</b>	1
	双栈混绑	已开启 🖍			
	实例类型	公网			
	地域	上海			
	可用区	上海二区			
	运营商	BGP			
	所属网络	Default-VPC	(172.17.0.0/16	2)	
	所属子网	Default-Subr	net(172.17.64.0/20	)	
	支持获取Client IP 🤅	) 支持			
	所属项目	默认项目			
	标签	P			
	删除保护	未开启开启	删除保护		
	配置修改保护	未开启 开启	配置保护		

#### 2. 创建七层 HTTP 或 HTTPS 监听器。



#### 3. 选择绑定 IPv6 或 IPv4 类型的后端服务。

绑定后端服务							×
IP版本① IPv6 O IPv4							
所属网络 Default-VPC (vpc- ?)							
请选择实例		已选择 (1)					
<b>云服务器 弹性网卡 容器实例</b> 默认端口 默认权重		ID/实例名	端口	权重 (j			
IP地址         ▼         按照IP地址搜索,关键字用"]"或空         Q		ins- (未命名)					
✓ ID/实例名		(公)/172.17.96.6( 内)	80	- 10	+	添加端口	删除
▼ 1054 (KWPE) i(公)/172.17.96.6(内)          10 ▼ 条/页        1 /1页 ▶         支持按住 shift 键进行多选	$\leftrightarrow$						
		确认 取消					

## 相关文档

搭建 IPv6 私有网络



## 创建 IPv6 NAT64 负载均衡实例

最近更新时间: 2025-05-19 11:58:01

#### () 说明:

- IPv6 NAT64 负载均衡仅支持北京、上海、广州三个地域。
- IPv6 NAT64 负载均衡不支持传统型负载均衡。
- IPv6 NAT64 负载均衡绑定的安全组支持 IPv4 地址,暂不支持 IPv6 地址; IPv6 NAT64 CLB 支持 IPv6 客户端和 IPv4 客户端的访问,如有 IPv4 客户端访问的需求请提交工单 获取 IPv4 VIP。
- 互联网 IPv6 网络大环境还处于建设初期,不提供 SLA 保障,如出现线路访问不通的情况,请提交工单反馈。

负载均衡支持创建 IPv6 NAT64 负载均衡实例,腾讯云会给实例分配一个 IPv6 公网地址(即 IPv6 版的 VIP),该 VIP 适配原有的 服务将来自 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 改造即可快速接入来自 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

腾讯云 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 负载均衡的操作流程,零学习成本,低门槛使用。

### 操作指南

#### 创建 IPv6 NAT64 负载均衡

- 1. 登录腾讯云官网,进入 负载均衡购买页。
- 2. 请正确选择如下参数:



- 计费模式: 支持包年包月和按量计费两种计费模式。
- 地域: 仅支持北京、上海、广州三个地域。
- 实例类型: 负载均衡。
- 网络类型: 公网。
- IP 版本: IPv6 NAT64。
- 所属网络:私有网络。
- 其他配置和普通实例配置相同,详情请参见 创建负载均衡实例 。

3. 在购买页选择各项配置后,单击**立即购买**,返回至 负载均衡实例列表页,即可查看已购的 IPv6 NAT64 负载均衡。

### 使用 IPv6 NAT64 负载均衡

登录 负载均衡控制台 ,单击实例 ID,进入详情页,在"监听器管理"页面配置监听器、转发规则、绑定云服务器,详情请参见 负载均 衡快速入门 。

## 相关文档

混合云部署场景下通过 TOA 获取客户端真实 IP



## 配置负载均衡的转发域名

最近更新时间: 2024-11-06 14:54:12

当客户端发起请求时,负载均衡会根据配置的监听器转发规则将请求转发至后端服务器。监听器转发规则中的域名是您的后端服务所使 用的域名,本文介绍如何配置域名。

## 操作步骤

#### 步骤一: 注册域名

域名注册是在互联网上建立服务的基础。

- 如果您已经在其他注册商拥有了自己的域名,您可以将域名转入腾讯云域名服务,详情请参见 域名转入腾讯云。
- 如果您还没有域名,您需要进行域名注册,详情请参见 域名注册。

#### 步骤二: 添加域名解析

域名注册成功后,您可为域名添加域名解析,以便通过域名访问网站。

1. 登录 云解析 DNS 控制台,在域名解析列表页面,单击目标域名右侧操作列的解析,本文档以 example.com 域名为例。

添加解	<mark>所</mark> 购买解	析套餐	批量操作	٣						清输入却要搜索的球名	Q,
	域名			编码	祈状态 ③	解析套板	最后操作时间	<	操作		
	example.com	n		IE S	NEWERT	免费音餐	2019-02-15 19:15:30		解析 升级套餐	更多 ▼	

- 2. 在记录管理页签,单击添加记录。
- 3. 在添加记录区域,填写以下参数:
  - 3.1 按需填写主机记录,主机记录就是域名前缀,详情请参见 子域名说明 和 泛解析说明,常见用法有:
  - www:解析后的域名为 www.example.com 。
  - @: 直接解析主域名 example.com 。
  - \*: 泛解析,匹配其他所有域名 \*.example.com 。
  - 3.2 选择记录类型, 域名化实例推荐选择 CNAME 。

添加记录快速滚	加网站/邮箱解析 暫停	开启 删除 分	行配至项目				请输入您要搜索的记录	Q		
主机记录	记录类型 🔻	线路类型	记录值	MX优先级	TTL (秒)	最后操作时间	操作			
按如下提示选填	CNAME	默认	按如下提示选填	-	600	-	保存取消			
提示 将城名指向云服务器 将城名指向另一个城 建立邮箱请选择「MI	提示 杨斌在描向云服务器,请选择「A」; 将或在描向另一个域名,请选择「CNAME」; 建立邮箱请选择「MX」,根据邮箱服务商提供的MX记录填写。									
А	用来指定域名的IPv4地址(如:	8.8.8.8) , 如果需要将场	名指向一个IP地址,就需要添加	点击自动填充						
CNAME	如果需要将城名指向另一个城名	1,再由另一个城名提供ip	地址,就需要添加CNAME记录。							
МХ	如果需要设置邮箱,让邮箱能收	到邮件,就需要添加MXi	日录。					_		
тхт	在这里可以填写任何东西,长度	限制255。绝大多数的TX	T记录是用来做SPF记录(反垃圾曲	昣(牛) 。						
NS	域名服务器记录,如果需要把子	城名交给其他DNS服务商	解析,就需要添加NS记录。							
AAAA	用来指定主机名 (或城名) 对应	Z的IPv6地址 (例如: ff06:	0:0:0:0:0:0:c3) 记录。							
SRV	记录了哪台计算机提供了哪个服务。格式为:服务的名字、点、协议的类型,例如:_xmpp-server_tcp。									
显性URL	URL 从一个地址301重定向到另一个地址的时候,就需要添加显性URL记录(注:DNSPod目前只支持301重定向)。									
隐性URL	體性URL 类似于显性URL,区别在于隐性URL不会改变地址栏中的域名。									



3.3 线路类型:保持选择"默认"类型,否则会导致部分用户无法解析。例如,您需要将联通用户指向 2.com ,所有非联通用户 都指向 1.com 。您可以通过添加线路类型为默认、记录值为 1.com 和线路类型为联通、记录值为 2.com 的两 条 CNAME 记录来实现。

添加记录	新手快速解析	批量操作 ▼	更多操作 ▼					全部记录,	高级筛选	请输入搜索的内容	Q	φ
	主机记录 \$	记录类型 🕈	线路类型 🕈	记录值 🕈	权重 \$	优先级 \$	TTL ‡	备注	最后操作时间:	操作		
	www	CNAME *	默认 ▼	1.com			600		2024-10-14 0§	确认 取消	收起	切换
	各个记录类型有不同的 CNAME 将域	<b>用途,一般选择</b> 洺指向另一个域名	<b>A 记录</b> 查看详细 地址,与其保持相同	<mark>指引 </mark> ☑ 解析,如 https://www.dnspod.cn								
	www	CNAME *	联通 ▼	2.com			600		2024-10-14 0§	确认取消	帮助	切换
共0条									20 ▼ 条/页	₩ ◀ 1 /	1页 🕨	H

3.4 填写记录值,CNAME 记录值可填写为负载均衡提供给您的域名。

- 3.5 其余值可以保持默认值,操作完成后,单击保存。
- 4. 添加记录完成后,可以在记录管理页签的记录列表查看刚才添加的记录。

	主机记录 ◆	记录类型 🕏	线路类型 🕏	记录值 🗲	权重 🕈	优先级 ◆	TTL ‡	备注	最后操作时间;
•	www	CNAME	默认	lh-ma600w30- cysougyrraonycz.clb.gz- tencentclb.cloud	-		600	-	2024-05-06 1

## 步骤三: 验证解析结果

()	说明:
	解析大概需要十分钟左右生效。

以上操作完成后,您可在浏览器中输入添加域名解析后的 CNAME 域名(如本例中的 www.example.com ),测试域名是否解析正常。

## 配置负载均衡安全组

最近更新时间: 2025-05-19 11:58:01

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,如需提升配额请前往 配额管理,提交配额申请。
- 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。
- 跨地域绑定2.0和混合云部署,不支持安全组默认放通,请在后端服务器上放通 Client IP 和服务端口。
- 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。如存量实例需对来自 EIP 的流量生效,请提交 工单申请。
- 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。
- 传统型内网负载均衡和基础网络的内网负载均衡不支持绑定安全组。
- 传统型内网负载均衡和基础网络的负载均衡不支持安全组默认放通功能,裸金属云服务器 暂不支持安全组默认放通能力。
- 黑石 2.0 服务器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、NAT64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

── CLB的安全组	
<b>〔1〕</b> 负载均衡	
开启默认放通,来自CLB的流量不必再经过CVM的安全组	
⑦ 云服务器 ← ⑦ CVM的安全组 ← ⑦ EIP/公网IP ← ○ 客户	

#### 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

────────────────────────────────────	
(王) 负载均衡	
▼不开启默认放通	
── CVM的安全组	
$\downarrow$	
受 云服务器     ←	∞IP ← ○3 客户

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(原"应用型内网负载均衡"),如果您的 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);如果您的 CLB 属于基础网络,无需在后端 CVM 的安全组上配置,默认放通健康检查 IP。
  - 对于传统型内网负载均衡,如果实例创建于2016年12月5日前且网络类型为 VPC 网络,则需要在后端 CVM 的安全组上放通 CLB 的 VIP(用作健康检查);其他类型的传统型内网 CLB,无需在后端 CVM 的安全组上配置,默认放通健康检查 IP。

## 操作步骤

如下公网 CLB 的安全组配置示例,预实现 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。

#### <u>小 注意:</u>

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。

添加	1入站规则				×
类	型	来源①	协议端口 ③	策略 备注	
	自定义	♥ 0.0.0.0/0	TCP:80	允许 ▼ 放通80端口,允许任息	删除
			+ 新增一行		
			完成取消		

- 2. 将安全组绑定 CLB
  - 2.1 登录 负载均衡控制台。
  - 2.2 在实例管理页面找到目标 CLB 实例,单击实例 ID。
  - 2.3 在实例详情页面单击安全组页签,在"已绑定安全组"模块单击配置。



#### 2.4 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。

部项目 ▼							
			į	已选择(1)			
					id/名称	备注	
l名称或ID		Q,		<u>^</u>	sg- 放通 80 端口		0
名称	备注				ACCE OF SHIELD		
通 80 端口		•					
			$\Leftrightarrow$				
	I 全称或ID 各称 ■ 80 端口	1会称或ID   各称或ID   各称或ID   日本   日本	各称或D Q 各称或D	经称或ID Q           E称	注各称或D Q 各称或D Q 各称 前注	I公子40 <sup>3</sup> IOFA <sup>10</sup> <	100点49     田注       143称或ID     Q       146     音注       160 朔口     ●       160 前口     ●       170 前口     ●

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。

E信息 监听器管	理 重定向配置	监控	安全组						
用默认放通 🗊 👥 🚺									
用后,CLB 和 CVM 之间影	认放通,来自 CLB 的流量只需	需通过 CLB 上安全纠	组的校验;不启	用,来自 CLB 的流量则	则需同时通过 CLE	3 和 CVI	M 上安全组的校验。当 CLB 不能	邦定安全组时,其监	听端口默认对所有 IP 放通,具
×19 12									
(1) 通知: 2019年12月	17日后,将增加实例最多绑定;	安全组数、安全组织	『定最多实例数、	规则引用数等限制,词	洋情请参考 限制计	説明 🖸			
0									
口继宁中全组				排度 銀定	±त त्यां २७ प्र	4			
已绑定安全组				排序 绑定	规则预划	ŧ			
<b>已绑定安全组</b> 优先级 ①	安全组ID/名称	1	操作	排序 绑定	规则预测	ē 1,011	出站规则		
<b>已绑定安全组</b> 优先级 ①	安全组ID/名称 59-	1	操作 解绑	排序 绑定	规则预测入站规	و السا 9-	出站规则 <b>  放通80端口</b>		14 14
<b>已绑定安全组</b> 优先级 ① 1	安全组ID/名称 <del>59-</del> 放通80端口	1	操作 解绑	排序 绑定	规则预】 入站规 	ŧ ۱ <u>۱۱</u> 9-	出站规则 <b> 放通80端口</b>		編
已绑定安全组 优先级 ① 1	安全组ID/名称 <del>59-</del> 放通80端口	3	操作 解绑	排序 绑定	规则预3 入站规 ▼ S 来3	t 191 9-	出站规则  放通80端口 端口协议	策略	幅
<b>已绑定安全组</b> 优先级 ① 1	安全億10/名祭 5 <mark>9-</mark> 放通60端口	3	操作 解 <del>第</del>	排序 棚定	规则预算 入站规 ▼ \$ 	€ !则 g- .0.0/0	出站规则 <b>放通80缩口</b> 信口协议 TCP-80	策略	編 备注 放通801階口, 允
<b>已绑定安全组</b> 优先级 ① 1	安全组10/名称 9 <mark>0-</mark> 放通60端口	1	操作 解绑	<b>排序 凱定</b>	规则预3 入站规 ▼ S 系3 0.0	\$ 100 9- 8 .0.0/0	出結規則 <b>放通eo痛口</b> 端口协议 TCP:80	旗略	編 音注 放通80頃口,允 意IP55向
<b>已頻定安全組</b> 代先級 ① 1	安全坦D/名称 90- 放通600%口	1	操作	相序 凱定	规则预3 入站规 ▼ S	8 19) 9-	出結规则 】 <b>放通60%口</b> 	策略	編 备注 放通80項口,允 憲(P5)向 无规则时,既认

#### 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。

() 说明: 传统型内网负载均衡和基础网络的负载均衡不支持安全组默认放通功能。

• 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**实例管理**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预览规则中的安全组规则,CVM 的安全组对来自本 CLB 的流量默认放通。

监听 2019年12月1 狀认放通 () 定安全组	器管理 7日后,将增加实 つい 、2001 次M 之间默认放语	重定向配置 例最多绑定安全 計:不启用,来自	监控 上组数、安全组绑双 自 CLB 的流量需消	安全组 定最多交例数、规则引用] 通过 CVM 上的安全组的时	<b>故等限制,详情请参考 限制说明 亿</b> 2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.	3LB 的监听缩口默认:	刘所有 甲 放道。
2019年12月1 默认放通 后,CLB和C 定安全组	7日后,将增加实	<b>例最多绑定安全</b> 1):不启用,来自 批序	全组数、安全组绑双 自 CLB 的流量需道	定最多实例数、规则引用) 通过 CVM 上的安全组的转	数等限制,详情请参考 限制说明 区 2016,内网 CLB 暂不支持绑定安全组,C	LB 的监听端口默认:	对所有 IP 放通。
2019年12月1 默认放通 后,CLB和C 定安全组	7日后,将增加实 	<b>例最多绑定安全</b> 1: 不启用,来自 批序	全组数、安全组绑页 自 CLB 的流量需测	定最多实例数、规则引用) 通过 CVM 上的安全组的机	<b>故等限制,详情诸参考 限制说明 包</b> 20验。内网 CLB 暂不支持绑定安全组,C	LB 的监听端口默认	对所有 IP 放道。
默认放通 <b>【</b> 后, CLB 和 C 定安全组	D .vm 之间默认放通	新 不启用,来自 批序	自 CLB 的流量需测	通过 CVM 上的安全组的机	0验。内网 CLB 暂不支持绑定安全组,C	LB 的监听端口默认:	对所有 IP 放通。
默认放通 <u></u> 后, CLB和 C <b>定安全组</b>	<mark>●</mark> ₩M 之间默认放通	<ol> <li>新</li> <li>新</li> <li>市</li> <li>市</li></ol>	自 CLB 的流量需测	通过 CVM 上的安全组的柜	战验。内网 CLB 暂不支持绑定安全组,C	LB 的监听端口默认:	对所有 IP 放通。
定安全组		排席		400135556			
定安全组		排席		相同時時(二			
定安全组		北席		相則竊悔 ①			
		2002	绑定	入站规则	出站规则		
版	安全组ID/名称	操作					
	sg-	<del>0</del> 248		▼ sg-   sg-			编辑规则
	sg-	8+37		来源	端口协议	策略	备注
				::/0	TCP:22,3389,80,443,20,21	允许	一键放通入站规则
				ALL	ALL	拒绝	无规则时,默认拒绝所有流 量(系统添加,无法修改)
	无级③	5级① 安全组D/名称 5g- 5g-	t级① 安全組ID/名称 操作 59- 解绑 59- 解绑	4级① 安全編印/名称 操作 90- 解節 90- 解節	L級① 安全組D/名称 操作 sg- sg- 約所 ::/0 ALL	148① 安全組口/名称 操作 50- 解卵 50- 解卵 50- アン・ 50- アン・ 50- アン・ 50- アン・ 50- アン・ 50- アン・ 50- アン・ 50- アン・ 50- アン・ 第二 日 50- アン・ 来源 道口协议 二/0 TCP:22,3389,80,443,20,21 ALL ALL	t級① 安全組印/名称 操作 90- 91- 第第第 第7 第7 第7 第7 第7 第7 第7 第7 第

#### 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

2.1 在 云服务器控制台上,单击 CLB 绑定的 CVM 的 ID,进入详情页。

2.2 选择**安全组**标签页,在"已绑定安全组"模块单击**配置**。



🔗 腾讯云

i manager and							登录 更多
ia息 弹性网卡	公网IP 监括	安全组	操作日志				
通知: 2019年12月	17日后,将增加实例最多	那定安全组数、安全!	追绑定最多实例数、规则引	用数等限制,详情请参考 國	制说明 🖸		
已爆定安全相			推序 揭定	规则预改			
<b>我先报</b> ①	应今细10/222	1日41:		入站规则	出站规则		
NOTES O	34.3530.076444	10(1)-					
1	放通22,80	解掷		¥ S	放通22,80		編輯规则
				来源	端口协议	策略	备注
				0.0.0.0/0	TCP:8080	允许	放通云服务器调□ 8080
				0.0.0/0	TCP:3389	允许	放通Windows远 程登录
				0.0.0/0	TCP:22	允许	放通Linux SSH远 程登录



## 内网负载均衡实例绑定 EIP

最近更新时间: 2025-06-16 15:48:32

内网负载均衡用于分发来自腾讯云内网的请求,没有公网 IP 且不能与公网互通。若您需要使用内网负载均衡并与公网互通,则可选择 内网负载均衡绑定弹性公网 IP,通过弹性公网 IP 访问公网。

#### 使用限制

#### • 地域限制

济南、福州、石家庄、武汉、长沙地域没有内网 CLB,因此不支持此功能。

- 产品属性限制
  - 仅标准账户类型支持,传统账户类型不支持。
  - 仅负载均衡实例类型支持,传统型负载均衡不支持。
  - 仅 VPC 的内网 CLB 支持,基础网络的内网 CLB 不支持。
- 功能限制
  - 目前内网 CLB 不支持端口段。
  - 内网 CLB 仅能绑定同地域且未被其他资源绑定的 EIP。
  - 每个内网 CLB 仅能与一个 EIP 互相绑定。
  - 内网 CLB 绑定 EIP 后,功能类似于公网 CLB,但公网 CLB 无法拆分为内网 CLB 和 EIP。
- 安全组限制
  - 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。如存量实例需对来自 EIP 的流量生效,请提交 工单申请。
  - 内网 CLB 绑定 EIP 并开启安全组默认放通后,来自 CLB 的流量只需通过 CLB 上安全组的校验,CVM 的安全组对来自本 CLB 的流量默认放通。

#### 操作步骤

#### 方式一: 购买 CLB 时选择 EIP

- 1. 登录腾讯云 负载均衡购买页。
- 2. 按需选择以下负载均衡相关配置,其余配置详情请参见 购买方式。

参数	说明
计费模式	选择"按量计费"模式。
地域	选择所属地域。CLB 支持的地域详情请参见 地域列表 。
实例类型	仅支持负载均衡实例类型。
网络类型	选择"公网"网络类型。
弹性公网 IP	选择弹性公网 IP,腾讯云将为您分配一个弹性公网 IP 和一个内网 CLB。弹性公网 IP 的类型支持:常规 IP、 加速 IP、静态单线 IP。

#### 方式二: 内网 CLB 绑定 EIP

1. 登录 负载均衡控制台,单击左侧导航栏的实例管理。

2. 在**实例管理**页面左上角选择地域,在实例列表中选择目标内网 CLB 实例,在右侧"操作"列选择更多 > 绑定弹性公网 IP。



3. 在弹出的绑定弹性公网 IP 对话框中,选择需绑定的 EIP,单击提交即可为内网 CLB 绑定 EIP。

① 说明: 加速 IP 和静态单线 IP 目前处于内测阶段,如需使用,请提交 工单申请。

4. (可选)在实例列表中选择目标内网 CLB 实例,在右侧 "操作"列选择更多 > 解绑弹性公网 IP 即可为内网 CLB 解绑。

## 相关文档

- 绑定弹性公网 IP API 文档
- 购买方式
- 产品属性选择



## 启停负载均衡实例

最近更新时间: 2025-05-19 11:58:01

您可以启动或停止实例。停止实例后,不再接收和转发流量,不再进行健康检查,并且禁 Ping。

 说明: 此功能处于内测中,如需使用,请联系 在线支持。

### 应用场景

当您配置了大量 CLB 实例时,某些实例出于业务考虑暂时无需使用,但又不能删除时,可以选择停止实例。

- 停止实例后,所有监听器也会停止,实例不再接收和转发流量。
- 启动实例后,所有监听器也会启动,实例正常接收和转发流量。
- 停止监听器后,监听器不再接收和转发流量。停止全部监听器以后,整个实例会停止。
- 启动监听器后,监听器正常接收和转发流量。启动全部监听器以后,整个实例会启动。
- 停止实例后,若启动任意监听器,实例会转为启动状态,其他监听器仍然保持停止状态,实例和已开启的监听器可正常接收和转发流 量。

## 限制说明

- 传统型负载均衡类型不支持。
- 仅 VPC 网络支持,基础网络不支持。
- TLS 1.3及以下协议版本不支持。

## 前提条件

- 您已 创建负载均衡实例。
- 您已 创建监听器。

## 操作步骤

- 1. 登录 负载均衡控制台。
- 2. 在**实例管理**页面左上角选择地域,在实例列表找到目标实例,单击右侧操作栏下的更多 > 启动或更多 > 停止。





3. (可选)在监听器管理页签,找到目标监听器,单击启动监听器或停止监听器。

新建 + :(HTTPS:80) + / 亩 ⊙ + :(HTTP:8080) + / 亩 ⊙	HTTP/HTTPS监听器(已配置2个)	
+ :(HTTPS:80) + / m ⊙ + :(HTTP:8080) + / m ⊙	新建	
+ (HTTP:8080) + / m 💽	+ :(HTTPS:80)	+ 💉 🖻 💽
	+ :(HTTP:8080)	+ 💉 📺 💿



## 克隆负载均衡实例

最近更新时间: 2025-05-19 11:58:01

负载均衡提供了克隆实例功能,您可以一键快速复制已有实例的配置,包括 CLB 的实例属性、监听器、安全组和日志等配置。

#### 限制说明

- 实例属性维度限制
  - 支持克隆网络计费模式为按量计费与包年包月的实例,包年包月实例克隆后的新实例网络计费模式会转换为按小时带宽计费,其
     带宽、规格与原实例设置保持一致。
  - 不支持克隆未关联实例计费项的 CLB。
  - 不支持克隆传统型负载均衡实例和高防 CLB。
  - 不支持克隆基础网络类型的实例。
  - 不支持克隆 Anycast 类型的实例。
  - 不支持克隆 IPv6 NAT64 版本的实例。
  - 不支持克隆被封禁或冻结的实例。
  - 执行克隆操作前,请确保实例上没有使用已过期证书,否则会导致克隆失败。
- 配额维度限制
  - 当实例的监听器个数超过 50 个时,不支持克隆。
  - 当共享型实例的公网带宽上限超过 2G 时,不支持克隆。

### 通过控制台克隆实例

- 1. 登录 负载均衡控制台,单击左侧导航栏的实例管理。
- 2. 在**实例管理**页面左上角选择地域,在实例列表中找到待克隆的实例,单击右侧操作列的更多 > 克隆。
- 3. 在弹出的克隆负载均衡对话框中,填入克隆实例的名称,单击确定。

克隆负载均衡	×
<ol> <li>将为您创建一个新的实例,该实例的属性、监听器、安全组等配置与原实例保持 一致。</li> </ol>	
使用限制:	
1. 执行克隆操作前,请确保该实例未使用已过期证书,否则会导致克隆失败,前 往查看 <u>证书管理</u> <sup>1</sup> 2;	
2. 不支持克隆实例的删除保护、配置修改保护属性。	
ID/实例名	
VIP 待分配	
新名称 请输入负载均衡名称	
确定取消	

## 通过 API 克隆实例

🔗 腾讯云

详情请参见 API 接口 克隆负载均衡实例。



## 导出负载均衡实例

最近更新时间: 2024-08-19 10:08:51

您可以在控制台中导出某地域的负载均衡实例列表,并且可以自定义导出的字段,以便分析实例资源配置和使用情况。

## 操作步骤

- 1. 登录 负载均衡控制台,在实例管理页面左上角选择所在地域。
- 2. 在实例列表中,勾选目标实例,并在右上角单击 💵 图标。
- 3. 在弹出的**导出实例**对话框中,可选择导出字段和导出范围,单击确认将实例列表下载至本地。

导出实例				×
寻出字段:				
✔ 导出全部				
实例字段:				
V ID	✓ 名称	✓ 状态	✔ 域名	
VIP	✓ 可用区	✔ 网络类型	✔ 所属网络	
✔ 运营商	✔ 实例规格	✓ 计费模式	✔ 带宽上限	
✔ 所属项目	✓ 标签	✔ 绑定个性化配置	1 🔽 创建时间	
规则字段:				
✓ 监听器ID、盟 ID、RS IP、	监听协议、监听端口、结 RS端口、RS权重	转发规则ID、转发域名、	转发URL、云服务器	
后端服务类型:				
○ 非目标组	目标组			
如果一个CLB部	分监听器绑定目标组,	部分监听器绑定非目标线	徂, 则需分别导出	
*出范围:				
全部实例	仅搜索结果 📃 仅送	时实例		
	确认	取消		
参数	说明			
	可导出的字段包	回括:		
	• 实例字段			
寻出字段	● 规则字段			
	其中,规则字段	殳中的 "RS 健康状	代态"仅在导出范围;	为"仅选中实例"、并且勾选了规则字段时才为可!
	态,否则不可见	<b>l</b> .		
∋屮沽国	<b>导</b> 出范围句括:			
тцюв	<ul> <li>◆日池園已出・</li> <li>◆ 全部实例</li> </ul>			
	• 人汉东泊木	1		
	● 1X 匹甲头例			



其中,未勾选任何实例时,"仅选中实例"为置灰状态不可选。
# 升级为性能容量型实例

最近更新时间: 2025-05-19 11:58:01

负载均衡的实例规格支持共享型实例和性能容量型实例。默认情况下所有实例均为共享型实例,共享型实例可升级为性能容量型实例。

# 升级优势

- 共享型 CLB 实例提供并发连接数5万、每秒新建连接数5000、每秒查询数(QPS)5000 的保障能力。
- 升级为性能容量型实例后,单实例最大可支持并发连接数1000万、每秒新建连接数100万、每秒查询数(QPS)30万。

# 升级影响

- 限速相关
  - 升级时,内网性能容量型实例默认为对应规格的带宽上限,升级后可在控制台调整规格;公网性能容量型实例的默认带宽与升级前一致,升级后可在控制台调整带宽。
  - 升级后,将按照实例规格限速,超过实例规格上限后将会出现限速和丢包现象。性能容量型的限速指标可参考以下监控指标,详 情请参见 监控指标说明。
    - ClientConcurConn(客户端到 LB 的并发连接数)
    - ClientNewConn (客户端到 LB 的新建连接数)
    - TotalReq (每秒请求数)
    - ClientOuttraffic (客户端到 LB 的出带宽)
    - ClientIntraffic (客户端到 LB 的入带宽)
  - 升级后,实际消耗性能如未超出实例性能限速值,将不会对存量连接造成影响。
- 计费相关
  - 升级前后的计费模式不变。
  - 升级后,将根据实际消耗性能,按小时收取性能容量单位 LCU 费用,详情请参见 性能容量单位 LCU 计费说明 。
- 网络连接相关

升级过程中网络不会中断,升级时间在1分钟以内。

• 回退相关

升级后,不支持回退为共享型实例。

# 升级限制

- 支持批量升级多个包年包月或按量计费的共享型实例,暂不支持同时升级包年包月和按量计费的共享型实例。
- 传统型负载均衡实例不支持升级为性能容量型实例。

# 升级方式

- 1. 登录 负载均衡控制台,单击左侧导航栏的实例管理。
- 在负载均衡的实例列表中,勾选需升级的目标共享型实例,单击实例列表上方的更多操作 > 升级为性能容量型。或在待升级的目标 共享型实例右侧,单击操作列的更多 > 升级为性能容量型。



ŧ	掘		删除		分配至项目	编	韻标签	更多操	作 👻							
	ID/睿	称 \$		监控	状态	域	名	升级为	的性能容量型	2 E	×					
	lb-i lb-i	22		ılı	正常	1000		升级为 <b>动态</b> (IP)	域各化实例 IP /6)	广州王	ΞIX					
新建	删除	分配到	项目	编辑标签	更多操作 ~								所属项目: 所有项目			d C T F f
ID/名	除 ‡	监控	状态	域名	VIP/EIP	可用区	网络出口 丁	网络类型 了	所属网络	实例规格 🔽	健康状态	计费模式 了	带宽上限	所属项目	标签 了	操作
		۵۵	正常	-		ł.		内网	vpc-qmnqrq27 ryan-广₩vpc2 (10.110.0.0/16)	共享型①	<b>未配置</b> (未绑定后端服务: 1)	按量计费-按网络流 量 2025-05-16 10:56:00 (UTC+08:00)创建	-	默认项目		<b>配置监听器 更多 &gt;</b> 启动
	ť	۵	正常		÷	ļ		内网	vpc-ji2nc6ul TEST-VPC (192.168.0.0/16)	共享型①	正常	按量计费-按网络流 量 2025-05-13 17:03:00 (UTC+08:00)创建		默认项目		<ul> <li>停止</li> <li>克隆</li> <li>升級力性能容量型</li> <li>財定弾性公別P</li> <li>▶</li> <li>4</li> <li>配置安全組</li> <li>→</li> <li>編唱称変</li> <li>分配至项目</li> <li>删除</li> </ul>

3. 在弹出的**实例升级**对话框中,单击确定。

# 相关文档

性能容量单位 LCU 计费说明

# 调整性能容量型实例规格

最近更新时间: 2025-02-27 10:18:43

负载均衡性能容量型实例支持调整规格,具体规格详情请参见 <mark>实例规格对比</mark> 。

#### () 说明:

- 若所选规格低于现有规格,降配调整后的规格存在不能很好地满足业务需求的风险,预估会有限速丢包对业务产生影响, 请评估后谨慎操作。
- 包年包月的性能容量型实例调整规格,费用由所选规格而定,不同规格的费用详情请参见 计费说明 。
- 按量计费的性能容量型实例调整规格,所选规格为最高限速规格,LCU 单价不变。

# 操作步骤

- 1. 登录 负载均衡控制台,单击左侧导航栏的实例管理。
- 2. 在"实例管理"页面左上角选择地域,在实例列表中找到待调整规格的性能容量型实例,单击右侧操作列的更多 > 调整规格。

ID/名称 \$	监控	状态	域名	VIP/EIP	可用区	网络类型 🍸	所属网络	实例规格 ▼	健康状态	计费模式 ▼	标签 ▼	操作
						搜索 "实例规格:标准型"	", 找到 5 条结果 返回原發	列表				
	di	正常		动态	广州三区	公网	a,	标准型①	健康检查未配置(配置)	按量计费-按网络流量 2023-08-23 11:03创 建		<b>配置监听器 更多 ▼</b> 启动
-	dı	正常			广州三区	公网	85	标准型①	健康检查未配置(配置)	包年包月-按网络带宽 2023-09-02 11:35到 期		停止 调整网络配置 调整规格 转为句年句日

#### 或单击目标性能容量型实例进入基本信息页 > 计费信息 > 实例规格 > 调整规格。

计费信息	
实例计费模式	按量计费
网络计费模式	按流量计费
带宽上限	
实例规格	标准型 🕤 调整规格
创建时间	2023-08-23 11:03:42

3. 在弹出的调整规格对话框中,选择规格型号,单击确认。

#### ▲ 注意:

- 1. 若所选目标规格带宽上限低于当前带宽上限,请先调整当前带宽上限,或选择其他规格。
- 2. 若所选目标规格低于现有规格,降配调整后的规格存在不能很好地满足业务需求的风险,预估会有限速丢包对业务产生 影响。需要再次确认调整操作。



 $\times$ 

#### 调整规格

当前规格 高阶型1

型号	最大并发连接数(个)	每秒新建连接数(个)	每秒查询数(个)	带宽上限(Mbps)
○ 高阶型1	200,000	20,000	20,000	4,096
○ 高阶型2	500,000	50,000	30,000	6,144
◯ 超强型1	1,000,000	100,000	50,000	10,240
○ 超强型2	2,000,000	200,000	100,000	20,480
○ 超强型3	5,000,000	500,000	200,000	40,960
○ 超强型4	10,000,000	1,000,000	300,000	61,440

按量计费模式下,所选规格为最高限速规格,LCU单价不变,详见 计费说明 🖸 公网带宽影响网络计费,请在网络计费模式中单独配置。





# 删除负载均衡实例

最近更新时间: 2025-05-19 11:58:01

#### () 说明:

- 计费模式为"包年包月"的实例不支持删除,您可以选择退订或在实例到期后不续费。
- 负载均衡实例支持批量删除,但暂不支持包年包月与按量计费同批删除。

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更多 > 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**确认**即可删除。

最终确认对话框如下图所示,我们建议您确认绑定规则数为 **"O"** 、绑定的后端服务器为 **"无"** 、操作安全提示为 **"绿色"** 后,再 进行删除操作。

ID/名称	绑定规则	则数 绑定的法	云服务器 操作安全损	示
lt h	t O	无	$\oslash$	
揭作坦 <del>云</del> ∶∎	则除后,负裁均衡	·实例 VID 收听哭 娃绸	合和则实配罢修如彻底清险	日不可物
and the second s	则际加, 贝勒均衡	关例  VIP、监听奋、我/	又观则守能且付饭191以有防。	日七日多

# 通过 API 删除负载均衡实例

详细步骤请参见 删除负载均衡。



# 释放闲置实例

最近更新时间: 2023-10-27 14:36:52

闲置实例是指创建时间超过7天,且未创建监听器或未绑定后端服务器的按量计费实例。为了减少不必要扣费,请及时释放闲置实例, 有助于您更好地管理成本。

# 限制说明

负载均衡支持批量释放同一地域下的闲置实例,不支持批量释放多个地域下的闲置实例。

# 操作步骤

△ 注意:

由于闲置实例数据存在一天缓存期,请您确保需要释放的实例处于未使用状态,以防误释放实例。

- 1. 登录 负载均衡控制台,在左侧导航栏单击闲置实例。
- 2. 在闲置实例页面左上角选择地域,在闲置实例列表中找到需释放的闲置实例,在右侧"操作"列单击删除。
- 3. (可选)在闲置实例列表左侧勾选全部实例,单击页面上方的删除。
- 4. 在弹出的对话框中确认实例信息,单击确定。

确认要删除以下负载	均衡?			×
ID/名称	绑定规则数	绑定的云服务器	操作安全提示	
lb- lb-	3	无	0	
	确定	取消		

# 配置实例修改保护

最近更新时间: 2024-12-02 16:45:22

开启配置保护功能后,可以防止误操作导致实例被修改。

# 限制说明

- 开启配置实例修改保护后,通过控制台和 API 均无法修改 CLB 配置,包括安全组、监听器、转发规则、重定向配置、绑定/解绑 RS 服务器等。
- 开启配置实例修改保护后,支持删除或退还实例。

# 操作步骤

- 1. 登录 负载均衡控制台,在**实例管理**页面左上角选择所在地域。
- 2. 在实例列表中,单击目标**实例 ID**。
- 3. 在实例**基本信息**页面,单击**开启配置保护**。

基本信息		
名称	lb-i Y 🎤	
ID	lb-m، ال	
状态	正常	
域名	lb-m	Б
VIP	动态 IP	
实例类型	公网	
地域	广州	
可用区	广州六区	
网络出口	中心出口一	
运营商	BGP(多线)	
所属网络	chalqh)	
支持获取Client IP	支持	
所属项目	默认项目	
标签	jî.	
删除保护	未开启 开启删除保护	
配置修改保护	未开启	
实例防护状态()	<mark>未启用</mark> 对象接入未启用,前往Web应用防火墙(WAF)了解详情	

4. 在弹出的**开启配置修改保护**对话框中,输入**原因备注**,单击**提交**。



开启后,通过控制台和API均无法修改CLB配置,包括安全组、监听器、车 重定向配置 细定/解细RS服条器等 请谨慎操作	专发规则、
原因备注	

5. 配置修改保护成功。

计费信息					
实例计费模式	按量计费				
网络计费模式	按流量计费				
带宽上限	5Mbps 调整网络	配置①			
实例规格①	共享型①升级为	实例已开启配置修改保护功能,保护原因是: 📲			
四层集群	共享型				
七层标签	共享型 🧨				
创建时间	2024-05-06 11:1	14:10			

# 配置实例删除保护

最近更新时间: 2025-05-19 11:58:01

开启删除保护功能后,可以防止误删除导致实例被释放。

# 限制说明

若 CLB 实例欠费停服,则即使开启删除保护功能也会被动释放。

# 操作步骤

- 1. 登录 负载均衡控制台,在**实例管理**页面左上角选择所在地域。
- 2. 在实例列表中,单击目标实例 ID。
- 3. 在实例基本信息页面,单击**开启删除保护**。



← II	
基本信息	i听器管理 重定向配置 监控 安全组
基本信息	
名称	
ID	
状态	正常
域名	
VIP	ā
网络类型	公网
地域	
可用区	广州六区 (主)/广州五区 (备)
网络出口	中心出口一
运营商	BGP(多线)
所属网络	D
支持获取Client IP(j	支持
所属项目	默认项目
标签	aaa:bbb 🥕
绑定后端服务个数	0
删除保护	未开启 开启删除保护
配置修改保护	未开启 开启配置保护
实例防护状态①	<mark>未启用</mark> 对象接入未启用,前往Web应用防火墙(WAF)了解详情
删除实例	

4. 在弹出的**打开删除保护**对话框中,单击**确认**。

```
    ① 说明:
    实例开启删除保护功能后,在控制台或调用 API 都无法删除该实例。若想删除实例,则需在实例基本信息页面单击关闭删
    除保护后才可删除。
```

# 相关文档

#### 删除负载均衡实例

# 调整实例公网配置

最近更新时间: 2024-10-31 10:32:22

公网类型的负载均衡可按需调整公网网络的带宽或计费模式,实时生效。

# 限制说明

- IPv4 版本的负载均衡:仅标准账户类型支持调整网络配置,传统账户类型不支持。
- IPv6 版本的负载均衡:标准账户类型和传统账户类型都支持调整网络配置。
- 若您无法确定账户类型,请参见 判断账户类型。

# 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)
包年包月	按带宽计费(包月带宽)	
	按带宽计费(小时带宽)	0_2049(会2049)
按量计费	按流量计费	0-2048(22048)
	共享带宽包	

() 说明:

如需更高上限请提交 工单申请 或联系您的商务经理。

## 调整带宽

1. 登录 负载均衡控制台。

2. 在"实例管理"页面,选择所在地域,找到目标公网负载均衡实例,并在右侧"操作"栏下选择更多 > 调整网络配置。

3. 在弹出的"调整网络配置"对话框中,设置目标带宽上限值,并单击提交。

# 调整计费模式

1. 登录 负载均衡控制台。

 在"实例管理"页面,选择所在地域,找到目标公网负载均衡实例,并在右侧"操作"栏下单击更多,然后选择调整网络配置或转为 按量计费/包年包月,调整说明如下:

实例计费模 式	网络计费模 式	调整网络计费模式	调整费用
包年包月	按带宽计费 (包月带 宽)	支持转为按量计费:实例计费转为按量计费,网络计费 转为按流量计费。每个 CLB 实例仅允许转换2次。	转换后退还费用 = 已购订 单费用 – 资源已使用费 用。
按量计费	按带宽计费 (小时带 宽)	支持转为包年包月:实例计费转为包年包月,网络计费 转为按带宽计费(包月带宽)。每个 CLB 实例仅允许转 换2次。	调整需要补交费用,即按官 网价格购买包年包月的费 用。

	支持转为按流量计费:实例计费不变,网络计费转为按 流量计费。每个 CLB 实例仅允许转换2次。	不涉及补交和退还费用。
	支持加入共享带宽包:实例计费不变,网络计费转为共 享带宽包计费。每个 CLB 实例仅允许转换2次。	不涉及补交和退还费用。
	支持转为包年包月:实例计费转为包年包月,网络计费 转为按带宽计费(包月带宽)。每个 CLB 实例仅允许转 换2次。	调整需要补交费用,即按官 网价格购买包年包月的费 用。
按流量计费	支持转为按带宽计费(小时带宽): 实例计费不变,网 络计费转为按带宽计费(小时带宽)。每个 CLB 实例仅 允许转换2次。	不涉及补交和退还费用。
	支持加入共享带宽包:实例计费不变,网络计费转为共 享带宽包计费。不限制转换次数。	不涉及补交和退还费用。
共享带宽包	支持退出共享带宽包:实例计费不变,网络计费转为按 流量计费。不限制转换次数。	不涉及补交和退还费用。

#### 调整操作如下:

ID/名称 ◆	监控	状态	VIP	可用区	网络类型 🍸	所属网络	实例规格 ▼	健康状态	计费模式 🍸	标签 🔻	操作
				ł	叟索 " 、 讠	十费模式:包年包",找	到1条结果 返回原列	表			
	di	正常	n.	广州五区	公网	Default-VPC	共享型	健康检查未配置	包年包月-按网络 带宽 2022-08-18 13:53		配置监听器 更多 ▼
			-			(172.16.0.0/16)		(	到期		续费
1条									20 ▼ 条	/页 🕅 🔳	调整网络配置
											转为按量计费
											升级为性能容量型
											配置安全组
											仲胡特尔

# "按量计费 - 按网络带宽"转为"包年包月"

ID/名称 \$	监控	状态	VIP	可用区	网络类型 🍸	所属网络	实例规格 ▼	健康状态	计费模式 🍸	标签 ▼	操作
					搜索"、	计费模式:按量计",找	3到1条结果 返回原列	表			
	dı	正常	5	广州五区	公网	Default-VPC	共享型	健康检查未配置	按量计费-按网络 带宽 2022-03-03 14:23	-	配置监听器 更多 ▼
			-			(172.16.0.0/16)		(	创建		克隆
共 1 条									20 🔻 🗍	2/页 14 4	调整网络配置转为包在包目
										_	升级为性能容量型
											加入带宽包
											和罢中会组

#### "按量计费 - 按网络带宽"转为"按量计费 - 按网络流量"

负载均衡



All 24 0 FAGE AND		rorath 3	- Delinent .		~ M 100 10 .	11111111111111	77-47 E	- 3 + 13 <u>111</u>		- 9- 5. ALLA	100.7.2.	betty: *
A 2 0 742 64 BUNNE 28 BUNNE				友	到1条结果返回原	计费模式:按量计",挂	搜索 " 、					
9       0	置监听器 更多 ▼	- 克隆	按量计费-按网络 带宽 2022-03-03 14:23 创建	健康检查未配置 (配置)	共享型	Default-VPC (172.16.0.0/16)	公网	广州五区	۲ G	正常	dı	
Approximate	网络配置	页 🛛 🖌 🧃 調整	20 🔻 🗍									条
Automation       Automation       Automation         Automation       Automation       Automation       Automation       Automation         Automation       A	5 + 6	升级										
Cartier       Care	·荒包 6~49											
No. 1       200       100       100       100       10000       10000       10000							<b>我包</b> "	'共享带货	宽"加入"	网络带	- 按	安重计费
AT A DATE AND AND AND A DATE AND AND A DATE	F	示签 ▼ 操	计费模式 🍸	健康状态	实例规格 ▼	所属网络	网络类型 🍸	可用区	VIP	状态	监控	D/名称 \$
Ali 28 b (1985) (198					到1条结果 返回原列	十费模式:按量计",找	搜索"、、议					
A A A A A A A A A A A A A A A A A A A	监听器 更多 ▼	配: 克隆 调整原	按量计费-按网络 带宽 2022-03-03 14:23 创建	健康检查未配置 (配置)	共享型	Default-VPC (172.16.0.0/16)	公网	广州五区	6	正常	dı	
Calified - type#intell"         With the state of t	<ul> <li>日</li> <li>年包月</li> <li>性能容量型</li> <li></li> <li></li></ul>		<b>20 ▼</b> 条 /									条
Search 2       Search 2 <th< td=""><td>6-49</td><td>200 C</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></th<>	6-49	200 C										
best best best best best best best best												
NUMB 0       NUM 0       NUM 0       NUM 0							<b>月"</b>	'包年包月	量"转为"	网络流	⋛─按	建计费
ALT       A	F	标签 🏲      探	计费模式 下	健康状态	实例规格 ▼	所属网络	网络类型 🍸	可用区	VIP	状态	监控	D/名称 🕈
1     28     10     1'HEX     28     12     12     13     12     13     12     12     13     12     14     15     13					到 1 条结果 返回原列	十费模式:按量计",找	搜索'、`					
Ali ER ID FARS OR DELANDO IN REE IN TO THE AND TO THE OR OTHER AND TO THE AND												
A       20 = 0/2       1 ≤ 1       1 ≤ 1       100 ± 0/2       100 ±	1监听器 更多 ▼	定陸	按量计费-按网络 流量 2022-06-10 14:58 创建	<mark>异常(</mark> 异常端口 数:1)	共享型	Default-VPC (172.16.0.0/16)	公网	广州四区	<u>ا</u> تا	正常	di	
Abgelities       Abgelities<	年包月	uig 14 ▲ 转为'	20 ▼ 条									条
Code 4 加速 45 VIP VIR MARKE ▼ 所属网络 文明规格 ▼ 健康状态 计最低式 ▼ 作签 ▼ 操作     Code 4 加速 45 VIP VIR MARKE ▼ 所属网络 文明规格 ▼ 健康状态 计最低式 ▼ 作签 ▼ 操作     Code 4 加速 1 计最优式设计计", 找到 4 条结果 《国旗规格 ▼ 健康状态 计最低式 ▼ 作签 ▼ 操作     Code 4 加速 1 计最优式设计计", 找到 4 条结果 《国旗规格 ▼ 健康状态 1 计最低式 ▼ 作签 ▼ 操作     Code 4 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	性能容量型	升级:										
	<i>∞4</i> 9	98 C W										
D/名称 <sup>1</sup> 班位       VIP       可用应       网络类型 <sup>1</sup> 所展网络       文网规称 <sup>2</sup> 就是就公       计费模式 <sup>1</sup> 就用       文网规称 <sup>2</sup> 就是就公       计费模式 <sup>1</sup> 法       ····································						带宽"	<b>费 - 按网络</b>	'按量计费	量"转为"	网络流	一按	安量计费
此 正常       广州四区       公网       Default-VPC       共安型       デ業       (第第第日)       第第二       第日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日		示签 ▼ 操作	计费模式 🍸	健康状态	实例规格 🔻	所属网络	网络类型 🍸	可用区	VIP	状态	监控	D/名称 🕈
▲ 正常 哈 广州四区 公网 Default-VPC 代72.16.0.016 共東型 発常(异常器口 設定 1014.58 20 年 余 / ① 14.58 32 - 余 / ① 14.58 32 - 余 / ① 14.58 20 年 余 / ② 14 20 年 余 / ② 14 20 年 余 / ② 15 20 年 余 / ② 14 20 年 余 / ③ 14 20 年 余 / ④ 14 20 年 余					1 条结果 返回原列	费模式:按量计",找到	搜索"、、计					
▲ 正常 哈 广州四区 公网 Default-VPC 共享型 発常(発電) (172.16.0.016) 第二 第二 (202-06-10 14.58) 前選 202-06-10 14.58 前選 202-06-10 14.58 前型 202-06-10 14.58 100-06-10 100-06-1			位导计弗 你回路									
A     20 * 条/页     K      林均包年包月       月級为性総容量型     加入事意包       加入事意包       日本日本中的	监听器 更多 ▼ 各配置	克隆	按重订算-按网络 流量 2022-06-10 14:58 创建	<mark>异常(</mark> 异常端口 数:1)	共享型	Default-VPC (172.16.0.0/16)	公网	广州四区	G	正常	di	
并级为性能容量型 加入带宽包 起≥±☆44 安量计费 – 按网络流量"加入"共享带宽包"	<b>王包月</b>	■ ■ ■ 転为包	<b>20 ▼</b> 条/									条
安量计费 - 按网络流量"加入"共享带宽包"	IRF音里呈	开级为 加入带										
安量计费 - 按网络流量"加入"共享带宽包"		和華山										
安量计费 - 按网络流量"加入"共享带宽包"												
							<b>8包</b> "	'共享带货	量"加入"	网络流	一按	建计费



ID/名称 \$	监控	状态	VIP	可用区	网络类型 🍸	所属网络	实例规格 ▼	健康状态	计费模式 🍸	标签 🔻	操作
					搜索"、、计	十费模式:按量计",找到	到1条结果 返回原列	し表			
-	dı	正常	Ē	广州四区	公网	Default-VPC (172.16.0.0/16)	共享型	<mark>异常(</mark> 异常端口 数:1)	按量计费-按网络 流量 2022-06-10 14:58 创建		配置监听器 更多 ▼ 克隆 调整网络配置
1 条									20 🔻 😤	2/页 14 4	转为包年包月
											加入带宽包
											ED 48 CD 42-49
按量计费	- 共3	<b>享带宽</b>	包"退出"	'共享带宽	包"						
<b>按量计费</b>	- <b>共</b>	<b>享带宽</b>	<b>包"退出"</b>	<b>"共享带贲</b> <sup>可用区</sup>	<b>[包."</b> 网络类型 下	所属网络	实例规格 <b>下</b>	健康状态	计费模式 ▼	标签 7	操作
<b>按量计费</b>	<b>- 共</b>	<b>享带宽</b>	<b>包"退出"</b>	<b>(共享带贷</b> <sup>可用区</sup>	<b>(包)"</b> 网络类型 T 搜索 "	所属网络 ",找到 1 条结果		健康状态	计费模式 ▼	标签 7	操作
<b>按量计费</b> ID/名称 *	- <b>共</b> <sup>協控</sup>	<b>享带宽</b> <sup>状态</sup>	<b>包"退出"</b> <sup>VIP</sup>	<b><sup>4</sup>共享带资</b> <sup>可用区</sup>	<b>2包."</b> 网络类型 <sup>*</sup> 沒示。	所属网络 *,找到1条结界 Default-VPC (172.16.0.0/16)	实例规格 ▼ <b>果 返回原列表</b> 共享型	健康状态 异常 (异常端口 数: 1)	计费模式 ▼ 按量计费-共享带 宽包 2022-06-10 14:58 创建	标签 🍸	操作 配置监听器 更多 ➤ 克隆 调整网络配置
<b>按量计费</b> ID/名称 ◆	— 共3 篮控	<b>拿带贲</b> ****	<b>包"退出"</b>	ゲ共享帯策	<b>207</b> 网络类型 T 提索"	所属网络 *, 找到 1 条结束 Dofault-VPC (172.18.0.0/16)	实例规格 Y R 返回原列表 共享型	健康状态 异常 (异常端口 数: 1)	计费模式 ▼ 技量计费-共享帯 宽包 2022-06-10 14:58 创建	标签 <b>▼</b> 系/页 K ◀	操作           配置监听器 更多 ▼           克隆           调整网络配置           升级为性能容量型           退出带宽句
<b>按量计费</b> 1D/名称 <b>*</b> 1 余	— 共早 篮控	<b>拿带宽</b> **态	<b>包"退出"</b>	<b><sup>4</sup>共享带资</b> <sup>可用区</sup>	<b>2包"</b> 网络类型 T 提索。	所属网络 **,找到 1 条结界 Default-VPC (172.18.0.0/16)	实例规格 ▼ 集 返回原列表 共享型	健康状态 异常(异常端口 数:1)	计费模式 ▼ 按量计费-共享带 窓包 2022-06-10 14:58 创建 20 ★ 3	标签 ▼ 条/页 II <	操作 配置监听器 更多 ▼ 克隆 调整网络配置 升级为性能容量型 退出带宽包 配置安全组

3. 在弹出的对话框中,单击提交。

# 负载均衡监听器 负载均衡监听器概述

最近更新时间: 2024-12-02 16:45:22

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,并依据均衡策略将流量分发至后端服务器 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。需选择后端服务器的 IP 和端口,服务端口亦被称为后端端口,后端服务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,例如:对 TCP、UDP 等四层协议请求进行四层负载均衡,对 HTTP、HTTPS 等七层协议请求进行七层负载均衡。

- 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。

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。

腾讯云负载均衡支持以下协议的请求转发:

- TCP(传输层)
- UDP(传输层)
- TCP SSL (传输层)
- QUIC(传输层)
- HTTP(应用层)
- HTTPS(应用层)

#### () 说明:

传统型内网负载均衡实例不支持配置 TCP SSL 监听器。

协议分类	协议	说明	应用场景
四层协议	ТСР	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 <mark>配置 TCP 监听器</mark> 。
	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	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 。



		<ul> <li>每一条 UDP 连接都只能是点到点的</li> <li>支持一对一,一对多,多对一和多对多的 交互通信</li> <li>支持基于客户端 IP(源 IP)的会话保持</li> <li>服务端可直接获取客户端 IP</li> </ul>	
	TCP SSL	安全的 TCP • TCP SSL 监听器支持配置证书,阻止未 经授权的访问 • 统一的证书管理服务,CLB 完成解密操作 • 支持单向认证和双向认证 • 服务端可直接获取客户端 IP	适用于 TCP 协议下对安全性要求非常高的场 景,支持基于 TCP 的自定义协议。详情请参见 配置 TCP SSL 监听器 。
	QUIC	基于 UDP 的多路并发传输的协议。 • 在 UDP 上实现了数据的可靠传输、安全 和 HTTP2,等效于 TCP + TLS + HTTP2。 • 在 QIUC 连接中,无论 IP 或端口发生什 么变化,连接不会中断或者重连,可实现 无缝连接迁移。	适用于音视频业务、游戏业务等在网络发生变化 时,例如 4G 网络与 Wi-Fi 网络频繁切换,能 够平滑迁移连接无中断的场景。详情请参见 配置 QUIC 监听器。
	НТТР	应用层协议 <ul> <li>支持基于请求域名和 URL 的转发</li> <li>支持基于 Cookie 的会话保持</li> </ul>	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 。
七层协议	HTTPS	加密的应用层协议 <ul> <li>支持基于请求域名和 URL 的转发</li> <li>支持基于 Cookie 的会话保持</li> <li>统一的证书管理服务,CLB 完成解密操作</li> <li>支持单向认证和双向认证</li> </ul>	需加密传输的 HTTP 应用。详情请参见 配置 HTTPS 监听器 。

# 端口配置

端口类型	说明	限制
监听端口 (前端端 口)	监听端口是负载均衡接收请求并向后端服务器转发请求的 端口。您可以为1 – 65535端口配置负载均衡,包括21 (FTP)、25(SMTP)、80(HTTP)、443 (HTTPS)等。	在同一个负载均衡实例内: • UDP 类协议可以和 TCP 类协议的监听端口重 复。例如,可以同时创建监听器 TCP:80 和监 听器 UDP:80。 • 同一类协议下监听端口不可重复,TCP/TCP SSL/HTTP/HTTPS 同属于 TCP 类。例如, 不可以同时创建监听器 TCP:80 和监听器 HTTP:80。
服务端口 (后端端 口)	服务端口是后端服务器提供服务的端口,接收并处理来自 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后端服务器的多个端口 上。	在同一个负载均衡实例内: <ul> <li>不同监听协议的服务端口可以重复。例如,监听器 HTTP:80 和监听器 HTTPS:443 可以同时绑定同一台后端服务器的同一个端口。</li> <li>四层监听器(TCP/UDP)的同一种监听协议下,同一个后端服务端口只能被一个监听器绑</li> </ul>



定,即四元组(VIP、监听协议、后端服务内 网 IP、后端服务端口)需要唯一。

# 相关文档

使用约束

🕥 腾讯云

# 配置 TCP 监听器

最近更新时间: 2025-05-23 17:06:12

您可以在负载均衡实例上添加一个 TCP 监听器转发来自客户端的 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 监听器绑定的后端服务器可直接获取客户端的真实 IP。

# 前提条件

您需要 创建负载均衡实例。

### 操作步骤

#### 步骤1: 配置监听器

- 1. 登录 负载均衡控制台,在左侧导航栏单击实例管理。
- 2. 在 CLB 实例列表页面左上角选择地域,在实例列表右侧的操作列中单击配置监听器。
- 3. 在 TCP/UDP/TCP SSL/QUIC 监听器下,单击新建,在弹出的"创建监听器"对话框中配置 TCP 监听器。

#### 3.1 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	<ul> <li>监听协议:本示例选择 TCP。</li> <li>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。</li> <li>同一个负载均衡实例内,监听端口不可重复。</li> </ul>	TCP:80
均衡方式	<ul> <li>TCP 监听器中,负载均衡支持加权轮询(WRR)和加权最小连接数(WLC)两种调度算法</li> <li>加权轮询算法: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。加权轮询算法根据新建连接数来调度,权值越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。</li> <li>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。</li> <li>①说明:</li> <li>选取加权最小连接数的均衡方式后,监听器不支持开启会话保持功能。</li> </ul>	加权轮询
ProxyProt ocol 配置	勾选后,可以开启 ProxyProtocol 配置。支持通过 ProxyProtocol 协议携带客户 端源地址到后端服务器。	勾选后使 用
双向 RST	勾选后,对应操作会向两端(客户端和服务器)发送 RST 报文来关闭连接;若不勾 选,则不发送双向 RST,长连接仍然存在直至超时。	勾选后使 用



	当前 TCP 连接超时时间默认为900秒。超过该时间阈值,会话中无数据传输则断开连	
连接空闲超时	接,如需调整可提交  工单申请 。	00074
时间	● 性能容量型实例的取值范围:300−1980,单位:秒。	900秒
	● 其他类型实例的取值范围:300-900,单位:秒。	

#### 3.2 健康检查

#### 健康检查详情请参见 TCP 健康检查。

3.3 会话保持

会话保持 配置	说明	示例
会话保持 开关	<ul> <li>开启会话保持后,负载均衡监听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。</li> <li>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。</li> <li>加权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。</li> </ul>	开启
会话保持 时间	会话保持时间 <ul> <li>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。</li> <li>可配置范围30 - 3600秒。</li> </ul>	30s

### 步骤2: 绑定后端服务器

1. 在监听器管理页面,单击刚才创建的监听器,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。

#### () 说明:

默认端口功能:先填写"默认端口",再选择后端服务器后,每台后端服务器的端口均为默认端口。

#### 步骤3:安全组(可选)

您可以配置负载均衡的安全组来进行公网流量的隔离,详情请参见配置负载均衡安全组。

### 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,图标修改或面图标删除。



# 配置 UDP 监听器

最近更新时间: 2025-05-23 17:06:12

您可以在负载均衡实例上添加一个 UDP 监听器转发来自客户端的 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。

# 限制说明

UDP 监听器的4789端口为系统保留端口,暂不对外开放。

# 前提条件

您需要 创建负载均衡实例 。

# 操作步骤

### 步骤1: 配置监听器

- 1. 登录 负载均衡控制台,在左侧导航栏单击实例管理。
- 2. 在 CLB 实例列表页面左上角选择地域,在实例列表右侧的操作列中单击配置监听器。
- 3. 在 TCP/UDP/TCP SSL/QUIC 监听器下,单击新建,在弹出的创建监听器对话框中配置 UDP 监听器。

#### 3.1 基本配置

监听器基本配 置	说明	示例
名称	监听器的名称。	test-udp- 8000
监听协议端口	<ul> <li>监听协议:本示例选择 UDP。</li> <li>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,其中4789端口为系统保留端口,暂不对外开放。</li> <li>同一个负载均衡实例内,监听端口不可重复。</li> </ul>	UDP:8000
均衡方式	<ul> <li>UDP 监听器中,负载均衡支持加权轮询(WRR)和加权最小连接数(WLC)两种 调度算法。</li> <li>加权轮询算法: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。加权 轮询算法根据新建连接数来调度,权值越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。</li> <li>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。</li> <li>说明:选取加权最小连接数的均衡方式后,监听器不支持开启会话保持功能。</li> </ul>	加权轮询
按 QUIC ID 调 度	启用后,CLB 将按 QUIC ID 来调度,相同的 QUIC Connection ID 会调度到相同的后端服务器。如果客户端请求没有包含 QUIC Connection ID,则降级到普通加权轮询,即按四元组(源 IP+目的 IP+源端口+目的端口)进行调度。 当前功能内测中,如需使用,请提交 工单申请。	开启
ProxyProtoc ol 配置	勾选后,可以开启 ProxyProtocol 配置。支持通过 ProxyProtocol 协议携带客户 端源地址到后端服务器。	勾选后使用

#### 3.2 健康检查

#### 健康检查详情请参见 UDP 健康检查。

3.3 会话保持

会话保持配置	说明	示例
会话保持开关	<ul> <li>开启会话保持后,负载均衡监听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。</li> <li>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。</li> <li>加权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。</li> </ul>	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

### 步骤2: 绑定后端服务器

1. 在监听器管理页面,单击刚才创建的监听器,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。

#### () 说明:

默认端口功能:先填写"默认端口",再选择后端服务器后,每台后端服务器的端口均为默认端口。

## 步骤3:安全组(可选)

您可以配置负载均衡的安全组来进行公网流量的隔离,详情请参见配置负载均衡安全组。

### 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,图标修改或面图标删除。

# 配置 TCP SSL 监听器

最近更新时间: 2025-05-13 09:27:22

您可以在负载均衡实例上添加一个 TCP SSL 监听器转发来自客户端加密的 TCP 协议请求。TCP SSL 协议适用于需要超高性能、大规模 TLS 卸载的场景。TCP SSL 协议的监听器,后端服务器可直接获取客户端的真实 IP。

() 说明:

腾讯云

- TCP SSL 监听器目前仅支持负载均衡实例类型,不支持传统型负载均衡。
- 使用 TCP SSL 监听器,访问 CLB 的请求为 HTTPS 协议,CLB 校验证书后通过 HTTP 协议转发到后端。

# 应用场景

TCP SSL适用于 TCP 协议下对安全性要求非常高的场景:

- TCP SSL 监听器支持配置证书,阻止未经授权的访问。
- 支持统一的证书管理服务,由 CLB 完成解密操作。
- 支持单向认证和双向认证。
- 服务端可直接获取客户端 IP。

# 前提条件

您需要 创建负载均衡实例。

## 操作步骤

#### 步骤1: 配置监听器

- 1. 登录 负载均衡控制台,在左侧导航栏单击实例管理。
- 2. 在 CLB 实例列表页面左上角选择地域,在实例列表右侧的操作列中单击配置监听器。
- 3. 在 TCP/UDP/TCP SSL/QUIC 监听器下,单击新建,在弹出的创建监听器对话框中配置 TCP SSL 监听器。

#### 3.1 基本配置

监听器基本 配置	说明	示例
名称	监听器的名称。	test-tcpssl- 9000
监听协议端 口	<ul> <li>监听协议:本示例选择 TCP SSL。</li> <li>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。</li> <li>同一个负载均衡实例内,监听端口不可重复。</li> </ul>	TCP SSL:9000
SSL 解析方 式	支持单向认证和双向认证,详情请参见 单向认证和双向认证说明 。	单向认证
服务器证书	可以选择 SSL 证书平台 中已有的证书,或新建证书。	选择已有证书
均衡方式	TCP SSL 监听器中,负载均衡支持加权轮询(WRR)和加权最小连接数 (WLC)两种调度算法	加权轮询

	<ul> <li>加权轮询算法: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。加 权轮询算法根据新建连接数来调度,权值越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。</li> <li>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。</li> </ul>	
ProxyProt ocol 配置	勾选后,可以开启 ProxyProtocol 配置。支持通过 ProxyProtocol 协议携带客 户端源地址到后端服务器。	勾选后使用

#### 3.2 健康检查

健康检查详情请参见 TCP SSL 健康检查。

3.3 会话保持(暂不支持)

TCP SSL 监听器暂不支持会话保持。

#### 步骤2: 绑定后端服务器

1. 在监听器管理页面,单击刚才创建的监听器,如上述 TCP SSL: 9000 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。

## () 说明:

默认端口功能:先填写"默认端口",再选择后端服务器后,每台后端服务器的端口均为默认端口。

### 步骤3:安全组(可选)

您可以配置负载均衡的安全组来进行公网流量的隔离,详情请参见配置负载均衡安全组。

### 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 ✔ 图标修改或 面图标删除。



# 配置 QUIC 监听器

最近更新时间: 2025-06-26 16:02:22

您可以在负载均衡实例上添加一个 QUIC 监听器,转发来自客户端加密的 QUIC 协议请求。QUIC 协议的监听器,后端服务器可直接 获取客户端的真实 IP。

QUIC(Quick UDP Internet Connection),又称为快速 UDP 互联网连接,是由 Google 提出的使用 UDP 进行多路并发传输 的协议,QUIC 相比现在广泛应用的 TCP+TLS+HTTP2 协议有如下优势:

- 减少连接建立时间。
- 改善拥塞控制。
- 避免队头阻塞的多路复用。
- 连接迁移。

# 使用场景

当 QUIC 版本为 Q043 时,QUIC 监听器支持连接迁移,当您的网络发生变化时,例如 4G 网络与 Wi−Fi 网络频繁切换,能够平滑 迁移连接无中断,适用于音视频业务、游戏业务等。

## 限制说明

- 仅负载均衡实例支持 QUIC 监听器,传统型负载均衡不支持。
- 仅 VPC 网络类型的负载均衡实例支持 QUIC 监听器,基础网络类型不支持。
- 仅 IPv4、IPv6 NAT64 版本的负载均衡实例支持 QUIC 监听器,IPv6 版本不支持。

## 前提条件

您需要 创建负载均衡实例 。

### 操作步骤

#### 步骤1: 配置监听器

- 1. 登录 负载均衡控制台,在左侧导航栏单击实例管理。
- 2. 在 CLB 实例列表页面左上角选择地域,在实例列表右侧的操作列中单击配置监听器。
- 3. 在 TCP/UDP/TCP SSL/QUIC 监听器下,单击新建,在弹出的创建监听器对话框中配置 QUIC 监听器。

#### 3.1 基本配置

监听器基本配置	说明	示例
名称	监听器的名称。	test- quic-443
监听协议端口	<ul> <li>监听协议:本示例选择 QUIC。选择 QUIC 后,CLB 可接收客户端发起的 QUIC 请求,CLB 和后端服务器之间仍然使用 TCP 协议。</li> <li>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。</li> <li>同一个负载均衡实例内,监听端口不可重复。</li> </ul>	QUIC:44 3
SSL 解析方式	支持单向认证和双向认证,详情请参见 单向认证和双向认证说明 。	单向认证



服务器证书	可以选择 SSL 证书平台 中已有的证书,或新建证书。	选择已有证 书
均衡方式	<ul> <li>QUIC 监听器中,负载均衡支持加权轮询(WRR)和加权最小连接数(WLC)两种 调度算法</li> <li>加权轮询算法:根据后端服务器的权重,依次将请求分发给不同的服务器。加权轮 询算法根据新建连接数来调度,权值越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。</li> <li>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。</li> </ul>	加权轮询
Proxy Protocol 配置	勾选后,可以开启 Proxy Protocol 配置。支持通过 Proxy Protocol 协议携带客户 端源地址到后端服务器。	勾选后使用

#### 3.2 健康检查

健康检查详情请参见 TCP SSL 健康检查。

3.3 会话保持

QUIC 监听器暂不支持会话保持。

#### 步骤2: 绑定后端服务器

- 1. 在监听器管理页面,单击刚才创建的监听器,如上述 QUIC:443 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。

#### () 说明:

默认端口功能:先填写**默认端口**,再选择后端服务器后,每台后端服务器的端口均为默认端口。

#### 步骤3:配置安全组

您需配置负载均衡的安全组来进行公网流量的隔离,详情请参见 配置负载均衡安全组。

### 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 ✔ 图标修改或 面图标删除。

# 相关文档

CLB 支持 QUIC 协议

# 配置 HTTP 监听器

最近更新时间: 2025-05-23 17:06:12

您可以在负载均衡实例上添加一个 HTTP 监听器转发来自客户端的 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。

# 前提条件

您需要 创建负载均衡实例。

## 操作步骤

#### 步骤1: 配置监听器

- 1. 登录 负载均衡控制台,在左侧导航栏单击实例管理。
- 2. 在 CLB 实例列表页面左上角选择地域,在实例列表右侧的操作列中单击配置监听器。
- 3. 在 HTTP/HTTPS 监听器下,单击新建,在弹出的"创建监听器"对话框中配置 HTTP 监听器。
  - 3.1 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-http- 80
监听协议端口	<ul> <li>监听协议:本示例选择 HTTP。</li> <li>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。</li> <li>同一个负载均衡实例内,监听端口不可重复。</li> </ul>	HTTP:80
	开启后,CLB 与后端服务之间使用长连接,CLB 不再透传源 IP,请从 XFF 中获 取源 IP。为保证正常转发,请在 CLB 上打开安全组默认放通或者在 CVM 的安全 组上放通 100.127.0.0/16。	
启用长连接	<ul> <li>① 说明:</li> <li>开启后,CLB与后端服务的连接数范围在请求[QPS,QPS*60]区间 波动,具体数值取决于连接复用率。后端 RS 热迁移时可能会有存量连 接池无法复用的情况。若后端服务对连接数上限有限制,则建议谨慎开 启。此功能目前处于内测中,如需使用,请提交 内测申请。</li> <li>健康检查中的健康探测源 IP 100.64.0.0/10 网段已默认放通,此网段 下的 IP 无需再次放通。</li> </ul>	不启用
Gzip 压缩	<ul> <li>透传模式: CLB 可以透传压缩包,此时需要后端 CVM 开启压缩功能,详情请参见 负载均衡开启 Gzip 配置。</li> <li>兼容模式: CLB 对指定文件进行压缩,无需后端 CVM 同步开启压缩功能。</li> </ul>	透传模式

#### 3.2 创建转发规则

# 🔗 腾讯云

() 说明:
--------

CLB 访问后端服务器的 HTTP 版本是 HTTP 1.1。

转发规则基本配 置	说明	示例
域名	<ul> <li>转发域名:</li> <li>• 长度限制:1-80个字符。</li> <li>• 不能以`_`开头。</li> <li>• 支持精准域名和通配域名。</li> <li>• 支持正则表达式。</li> <li>• 具体配置规则,详情请参见 转发域名配置规则。</li> </ul> ⑦ 说明: 新增域名功能使用限制: 1. 不支持传统账户类型(原"带宽非上移账户")。若您无法确定账户 类型,请参见判断账户类型。当前传统型负载均衡购买入口已关闭,如存量实例需要升级,请参考传统型负载均衡为级。 2. 不支持传统型负载均衡和基础网络的负载均衡。	www.exa mple.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。	默认启用
URL 路径	转发 URL 路径: <ul> <li>长度限制: 1 – 200个字符。</li> <li>支持正则表达式。</li> <li>具体配置规则,详情请参见 转发 URL 路径配置规则。</li> </ul>	/index
均衡方式	<ul> <li>HTTP 监听器中,负载均衡支持加权轮询(WRR)、加权最小连接数(WLC)</li> <li>和 IP Hash 三种调度算法:</li> <li>加权轮询算法: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。 加权轮询算法根据新建连接数来调度,权值越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。</li> <li>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。</li> <li>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。</li> </ul>	加权轮询
获取客户端 IP	默认启用,详情请参见 获取客户端IP 。	已开启

3.3 健康检查

#### 健康检查详情请参见 HTTP 健康检查。

3.4 会话保持



会话保持 配置	说明	示例
会话保持 开关	开启会话保持后,负载均衡监听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。 加权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。	开启
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 – 86400秒。	30s

### 步骤2: 绑定后端服务器

- 1. 在监听器管理页面,单击刚才创建的监听器,如上述 HTTP:80 监听器,单击左侧的 + 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。

HTTP/HTTPS监听器(已配置1个)							
新建							
— 80(HTTP:80)	+ 🖌 🖮 💿	转发规则详情 展开 ▼					
- www.example.com	默认访问 🧪 🕂	已绑定后端服务					
/index	✓ <sup>™</sup>	<b>绑定</b> 修改端口 修改权重 解绑			按照内网IP搜索,	用" "分割关键字	Q Ø
		ID/名称	端口健康状态①	IP地址	端口	权重	操作
			监听器创建完成	成,请 <b>绑定后端服务</b>			
		已选 0 项, 共 0 项					

说明:
 默认端口功能:先填写"默认端口",再选择后端服务器后,每台后端服务器的端口均为默认端口。

#### 步骤3:安全组(可选)

您可以配置负载均衡的安全组来进行公网流量的隔离,详情请参见配置负载均衡安全组。

### 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,图标修改或面图标删除。

# 配置 HTTPS 监听器

最近更新时间: 2025-05-13 09:27:22

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。

# 前提条件

您需要 创建负载均衡实例。

# 操作步骤

#### 步骤1: 配置监听器

- 1. 登录 负载均衡控制台,在左侧导航栏单击实例管理。
- 2. 在 CLB 实例列表页面左上角选择地域,在实例列表右侧的操作列中单击配置监听器。
- 3. 在 HTTP/HTTPS 监听器下,单击新建,在弹出的"创建监听器"对话框中配置 HTTPS 监听器。

#### 3.1 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	<ul> <li>监听协议:本示例选择 HTTPS。</li> <li>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。</li> <li>同一个负载均衡实例内,监听端口不可重复。</li> </ul>	HTTPS:443	
启用长连接	开启后,CLB 与后端服务之间使用长连接,CLB 不再透传源 IP,请从 XFF 中获 取源 IP。为保证正常转发,请在 CLB 上打开安全组默认放通或者在 CVM 的安全 组上放通 100.127.0.0/16 。		
	<ul> <li>① 说明:</li> <li>开启后,CLB与后端服务的连接数范围在请求[QPS,QPS*60]区间 波动,具体数值取决于连接复用率。后端 RS 热迁移时可能会有存量连 接池无法复用的情况。若后端服务对连接数上限有限制,则建议谨慎开 启。此功能目前处于内测中,如需使用,请提交 内测申请。</li> <li>健康检查中的健康探测源 IP 100.64.0.0/10 网段已默认放通,此 网段下的 IP 无需再次放通。</li> </ul>	不启用	
Gzip 压缩	<ul> <li>透传模式: CLB 可以透传压缩包,此时需要后端 CVM 开启压缩功能,详情请参见 负载均衡开启 Gzip 配置。</li> <li>兼容模式: CLB 对指定文件进行压缩,无需后端 CVM 同步开启压缩功能。</li> </ul>	_	
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。	不启用	



SSL 解析方式	支持单向认证和双向认证。负载均衡器代理了 SSL 加解密的开销,保证访问安全, 详情请参见 <mark>单向认证和双向认证说明</mark> 。	单向认证
服务器证书	可以选择 SSL 证书平台 中已有的证书,或新建上传证书。服务器证书支持配置双 证书,即两种不同类型的加密算法的证书。 说明:配置双证书,仅负载均衡支持,传统型负载均衡不支持,并且配置双证后, 不支持开启 QUIC 功能。	选择已有

#### 3.2 创建转发规则

转发规则基本配 置	说明	示例	
域名	转发域名: • 长度限制: 1-80个字符。 • 不能以`_`开头。 • 支持精准域名和通配域名。 • 支持正则表达式。 • 具体配置规则,详情请参见 转发域名配置规则。		
	<ol> <li>说明: 新增域名功能使用限制:</li> <li>1.不支持传统账户类型(原"带宽非上移账户")。若您无法确定账户类型,请参见判断账户类型。当前传统型负载均衡购买入口已关闭,如存量实例需要升级,请参考传统型负载均衡升级。</li> <li>2.不支持传统型负载均衡和基础网络的负载均衡。</li> </ol>	www.examp le.com	
默认域名	<ul> <li>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。</li> <li>一个监听器下仅能配置一个默认域名。</li> </ul>	开启	
HTTP 2.0	启用 HTTP2.0 后,CLB 可以接收 HTTP 2.0 的请求,无论客户端请求 CLB 时 使用哪种 HTTP 版本,CLB 访问后端服务器的 HTTP 版本都是 HTTP 1.1。	开启	
URL 路径	转发 URL 路径: <ul> <li>长度限制: 1 - 200个字符。</li> <li>支持正则表达式。</li> <li>具体配置规则,详情请参见转发 URL 路径配置规则。</li> </ul>	/index	
均衡方式	<ul> <li>HTTPS 监听器中,负载均衡支持加权轮询(WRR)、加权最小连接数(WLC)和 IP Hash 三种调度算法:</li> <li>加权轮询算法: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。加权轮询算法根据新建连接数来调度,权值越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。</li> <li>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。</li> <li>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</li> </ul>	加权轮询	



	器,反之则返回空。	
后端协议	后端协议是指 CLB 与后端服务之间的协议: <ul> <li>后端协议选择 HTTP 时,后端服务需部署 HTTP 服务。</li> <li>后端协议选中 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。</li> <li>后端协议选中 gRPC 时,后端服务需部署 gRPC 服务。仅 HTTP2.0 开启且 QUIC 关闭的情况下,后端转发协议支持选择 gRPC。</li> </ul>	НТТР
获取客户端 IP	默认启用,详情请参见 获取客户端IP 。	已开启

#### 3.3 健康检查

#### 健康检查详情请参见 HTTPS 健康检查。

3.4 会话保持

会话保持配置	说明	示例
会话保持开关	<ul> <li>开启会话保持后,负载均衡监听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。</li> <li>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。</li> <li>加权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。</li> </ul>	开启
会话保持时间	<ul> <li>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。</li> <li>可配置范围30 - 86400秒。</li> </ul>	30s

# 步骤2: 绑定后端服务器

- 1. 在监听器管理页面,单击刚才创建的监听器,如上述 HTTPS:443 监听器,单击左侧的 + 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。



HTTP/HTTPS监听器(已配置1个) 新建					
— 80(HTTPS:80)	+ 🖍 🖻 💿	转发规则详情 展开 ▼			
- www.example.com	默认访问 🧪 +	已绑定后端服务			
/index 🖍 🛅		<mark>绑定</mark> 修改塔口 修改权重 解绑		用" "分割关键字	Q Ø
		ID/名称 端口健康状态① IP地址	端口	权重	操作
		监听器创建完成,请 <b>绑定后端服务</b>			
		已选 0 项,共 0 项			
① 说明:					

默认端口功能:先填写"默认端口",再选择后端服务器后,每台后端服务器的端口均为默认端口。

### 步骤3:安全组(可选)

您可以配置负载均衡的安全组来进行公网流量的隔离,详情请参见配置负载均衡安全组。

### 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 ✔图标修改或 面图标删除。

# 均衡方式

最近更新时间: 2025-05-13 09:27:22

均衡方式是负载均衡向 后端服务器 分配流量的算法,根据不同的均衡方式可以达到不同的均衡效果。

### 加权轮询算法

加权轮询算法(Weighted Round–Robin Scheduling)是以轮叫的方式、依次请求调度不同的服务器。加权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。加权轮询算法根 据新建连接数来调度,权重高值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,并结合您所设置的后端服务器权重,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:

- 1.1 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。
- 1.2 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。
- 1.3 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)。



# 会话保持

最近更新时间: 2025-04-11 16:23:52

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 中无新请求则断开会话保持状态,会话保持与均衡方式相关:

均衡方式	特点	支持会话保持
加权轮询	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
加权最小连接数	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 – 86400秒,会话保持与均衡方式相关:

均衡方式	特点	支持会话保持
加权轮询	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
加权最小连接数	根据服务器负载和权重来综合调度	不支持会话保持
IP Hash	根据客户端 IP 和权重来综合调度	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,如需调整请开通 个性化配置。超过该时间阈值,会话中无数据传 输则断开连接。

当前 TCP 连接超时时间默认为900秒,支持通过编辑监听器的连接空闲超时时间属性进行调整。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**开启**,输入保持时间,单击提交。

# 长连接和会话保持的关系

长连接的开启方式请参见 配置 HTTP 监听器 和 配置 HTTPS 监听器。

## 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,再访问到后端服务器,此时不开会 话保持,下一次访问,能否访问到同一台服务器?

**答:**不一定。

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 机挑选一台后端服务器,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,找到同一台后端服务器,Client 访问的服务器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。
# 七层重定向配置

最近更新时间: 2025-05-13 09:27:22

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 www.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 www.example.com/bbs/test/456.html 时,原会话保持机制将失效。

• TCP / UDP 重定向: 暂不支持 IP + Port 级别的重定向,后续版本将提供。

## 重定向概述

- 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。
- 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。

#### () 说明:

- 若域名已经配置过自动重定向,则无法再配置手动重定向。
- 泛域名负载均衡只支持配置自动重定向,不支持配置手动重定向。

#### ○ 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。

### 使用限制

重定向配置包含协议/端口、域名和路径的配置,为避免回环请注意以下限制信息:

- 原访问的路径和重定向的访问路径一致,则不允许配置。
- 原访问的路径若已经配置了重定向策略(包含原访问路径和重定向访问路径),则不允许再次配置。
- 如果重定向访问路径配置的是其他重定向策略的原访问路径,则不允许配置。

# 自动重定向

腾讯云 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 腾讯云负载均衡控制台 完成 CLB 的 HTTPS 监听器的配置并搭建 https://www.example.com 的 Web 环境。详情请 参见 配置 HTTPS 监听器。
- 2. 完成 HTTPS 监听器配置后的结果如下图所示。

- test(HTTPS:80)	+ 🖍 🖻 💿	转发规则详情 展开 マ					
- www.com	默认访问 🥒 +	已绑定后端服务					
	/ 首	<b>耕定</b> 修改幾口 修改权重	解绑		按照内网IP搜索	,用" "分割关键	字 <b>Q</b> Ø
		ID/名称	端口健康状态()	IP地址	端口	权重	操作
		□ ins 未命名	探测中	)(公) (内)	88	10	解绑

- 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,单击提交即可完成配置。

亲	新建重定向配置	
	白动舌空向配带	
	HTTP 强制强转为 H	ITTPS,系统自动为已存在的 HTTPS:443 监听器创建 HTTP:80 监听器,创建成功后 HTTP 访问将被重定向至 HTTPS。
	前端协议和端口	HTTPS:443 vwwcom v
	配置路径	
	原访问路径	重定向至路径
	/index	/index
	域名配置	
	重定向状态码 🛈	301 0 302 307
	手动重定向配置	
	用户手动配置原访问	弛地和重定向地址,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
	<i>百</i> 6年友。	
	提交 取消	

🕛 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. 完成重定向配置后的结果如下图所示,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。



甘木信白	收成器管理	雷会内系	<b>*</b>	的技		9	
整个1百思	盈听發官注	里定问即	a	mfr	安主地	3	
泪 <b>动</b> 根云,	当你配罢了白完♡重会	2向策略 原誌	安切副時期	网络改善 计	東完向策略会	新江設施 泰莱泰新研	
		EIMJARAH ( MAKAK	2474694322		EVELIAI AKAB ZU	W/W/99980: / WESCHED/INDE	
HTTP/HTTPS	听器						
新建							
新建							
新建 — test-rew	rrite(HTTPS:443)				转发	规则详情 展开 🔻	
新建 — test-rew	rrite(HTTPS:443)				转发	规则详情 展开 ▼	
新建 — test-rew	rrite(HTTPS:443)				转发已绑	规则详情 展开 ▼ 定后端服务	
新建 — test-rew — w	rrite(HTTPS:443) www.example.com /bbs/test1/image/URI				转发已绑	规则详情 展开 ▼ 定后端服务	Mr.3/r#
新建 — test-rew	rrite(HTTPS:443) www.example.com /bbs/test1/image/URI	_			转发已绑	规则详情 展开 <del>▼</del> 定后端服务 院 修改端口	修改者
新建 — test-rew — w — w — 未命名(I	rrite(HTTPS:443) ww.example.com /bbs/test1/image/URt HTTP:80)	_	] +	× ū	转发已绑	规则详情 展开 ▼ 定后端服务 院定 修改端口	修改社
新建 — test-rew — w — w — ************************************	rrite(HTTPS:443) www.example.com /bbs/test1/image/URL HTTP:80)	_	+	Î.	转发 已绑	<b>规则详情 展开 ▼</b> 定后端服务 疑定 修改端口 CVM ID/名称	修改初
新建 - test-rew - w - 未命名(1	rrite(HTTPS:443) www.example.com /bbs/test1/image/URI HTTP:80) www.example.com	-	+	/ ū / +	转发 已绑	<b>规则详情 展开 ▼</b> 定后端服务 旋 修改端口 CVM ID/名称	修改初
新建 - test-rew - w - 未命名()	rrite(HTTPS:443) www.example.com /bbs/test1/image/URI HTTP:80) www.example.com /bbs/test1/image/URI	-	+	/ 回 / +	转发 已绑	規则详情 展开 ▼ 定后端服务 院定 修改端口 CVM ID/名称	修改? <b>端口状</b> 监证

# 手动重定向

腾讯云 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

- 请在 腾讯云负载均衡控制台 完成 CLB 的 HTTPS 监听器的配置,搭建 https://www.example.com 的 Web 环境。详情请参见 配置 HTTPS 监听器。
- 2. 完成 HTTPS 配置后的结果如下图所示。

HTTP/HTTPS监听器(已配置2个)			
- 55(HTTPS:555)	+ 🖌 🖻 💿	转发规则详情 展开 🗸	
	默认访问 🖌 🕂	已期定后端服务	
	i ii	<b>第</b> 定 修改鎮口 修改权重 解绑	按照内网IP搜索,用1"分青 Q. 🗘
<ul> <li>succession is</li> </ul>	+ 🖍 🔟 💿	ID/名称 端口健康状态③ IP地址	端口 权重 操作
		监听器创建完成,请 <b>绑定后端服务</b>	

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。



选择**手动重定向配置**,选择原访问的前端协议端口、域名和路径,选择重定向后的前端协议端口、域名和路径,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**提交**即可完成配置。

建重定向配置						
自动重定向配置 HTTP 强制强转为 HT	TPS,系统自动为已存在的 HT	TTPS:443 监听器创建 HTTP:80 监听器,	创建成功后 HTTP 访问	]将被重定向至 HTTPS。		
<b>手动重定向配置</b> 用户手动配置原访问 <sup>1</sup>	也址和重定向地址,系统自动将	务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算	§略,实现 HTTP/HTTPS 之间请求的自动跳	转。
原访问		重定向至				
监听协议和端口	HTTPS:12	▼ HTTPS:443	Ŧ			
域名		t tr	Ŧ			
路径	/index 新建重定向路径	▼ /index	•	۵		
域名配置						
重定向状态码 ()	301 🔾 302 🔵 307					
保留 URL 🛈	✓ 开启 开启后,匹配重定向规则后仍 则会被重定向到 www.exampl	保留原路径剩余的 URL,如将 www.exa e.com/c	ample.com/a/b 重定向到	则www.example.com/c,访问,	www.example.com/a/b/test 会被重定向到 v	vww.example.com/c/te
なる						

## () 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. 完成重定向配置后的结果如下图所示,可以看到 HTTPS:443 监听器中, https://www.example.com/forsale 已重定向至 https://www.new.com/index 。

HTTP/HTTPS监听器	
arren	
- test-sni(HTTPS:443)	+ ノ 直 转发规则详情 展开 -
- www.example.com	② / + 已绑定后端服务
/forsale	🕘 🖍 📋 🗰 🗰 Markan (Marka)
- www.new.com	已经设置重定向,该路径下绑定的后端服务器将不再接收流 量。
/index	4

# 七层个性化配置

> 腾讯云

最近更新时间: 2025-06-25 09:57:22

CLB 支持实例维度个性化配置功能,允许用户设置单 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为每个地域200条。
- 个性化配置的长度限制为4k。
- 当前一个实例仅允许绑定一个个性化配置,一个个性化配置可以绑定多个实例。
- 个性化配置仅针对负载均衡(原"应用型负载均衡")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	<ul> <li>默认值:</li> <li>TLSv1、 TLSv1.1、 TLSv1.2</li> <li>建议值: TLSv1.2、 TLSv1.3</li> </ul>	TLSv1 TLSv1.1 TLSv1.2 TLSv1.3	使用的 TLS 协议版本。
ssl_ciphers	ssl_ciphers 默 认值	ssl_ciphers 参数 范围	加密套件。
client_header_timeo ut	60s	[30-120]s	获取到 Client 请求头部的超时时间, 超时返回 408。
client_header_buffe r_size	4k	[1-256]k	存放 Client 请求头部的默认 Buffer 大小。
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,而是指空闲一段时间没 有传输数据的超时时间,超时返回408。
client_max_body_si ze	60M	[1-10240]M	<ul> <li>客户端请求 body 最大的大小。</li> <li>默认配置范围为1M-256M,直接配置即可。</li> <li>最大支持10240M,即10G。当 client_max_body_size 的配置范围大于 256M 时,必须设置 proxy_request_buffering 的值为 off。</li> </ul>
keepalive_timeout	75s	[0-900]s	Client-Server 长连接保持时间,设置为0则禁 用长连接。如需设置超过900s,请提交 工单申 请,最大可设置到3600s。



add_header	用户自定义添加		向客户端返回特定的头部字段,格式为 add_header xxx yyy。例如针对让浏览器强制 使用 HTTPS 协议,从而避免了通过 HTTP 访 问网站时的安全风险。 add_header Strict-Transport- Security "max-age=86400; includeSubdomains"; 也可以利用 add_header 达成 CORS 的能力: add_header Access-Control-Allow- Origin *: 允许所有域访问资源。如果你只想允许 特定域访问,可以将 * 替换为具体的域名,例如 https://example.com。 add_header 'Access-Control-Allow- Methods' 'GET, POST, OPTIONS, DELETE, PUT': 指定允许的 HTTP 方法。 add_header 'Access-Control-Allow- Methods' 'GET, POST, OPTIONS, DELETE, PUT': 指定允许的 HTTP 方法。 add_header 'Access-Control-Allow- Headers' 'Origin, X-Requested-With, Content-Type, Accept, Authorization': 指定允许的请求头。
more_set_headers	用户自定义添加	_	向客户端返回特定的头部字段,格式为 more_set_headers "A:B"。
proxy_connect_time out	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。
server_tokens	off	on, off	<ul><li>on 表示显示版本信息。</li><li>off 表示隐藏版本信息。</li></ul>
keepalive_requests	100	[1-10000]	Client-Server 长连接上最多能发送的请求数 量。
proxy_buffer_size	4k	[1-32]k	Server 响应头的大小,默认为 proxy_buffer 中设置的单个缓冲区大小,使用 proxy_buffer_size 时,必须同时设置 proxy_buffers。
proxy_buffers	84k	[3-8] [4-16]k	缓冲区数量和缓冲区大小。
proxy_request_buff ering	off	on, off	<ul> <li>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。</li> <li>off 表示不缓存客户端请求体: CLB 收到请求后,立即转发给后端CVM,此时会导致后端CVM有一定性能压力。</li> </ul>
proxy_set_header	X-Real-Port \$remote_port	<ul> <li>X-Real-Port \$remote_por t</li> </ul>	转发给后端服务器添加的请求 header 头 ● X-Real-Port \$remote_port 表示客户端 端口。



		<ul> <li>X-clb-lbid \$lbid</li> <li>Stgw- request-id \$stgw_reque st_id</li> <li>X- Forwarded- Port \$vport</li> <li>X-Method \$request_me thod</li> <li>X-Uri \$uri</li> <li>X-Args \$args</li> </ul>	<ul> <li>X-clb-lbid \$lbid 表示 CLB 的 LBID, 是 CLB 实例的标识。</li> <li>Stgw-request-id \$stgw_request_id 表示请求 ID (CLB 内部使用)。</li> <li>X-Forwarded-Port 表示 CLB 监听器的 端口。</li> <li>X-Method 表示客户端请求方法。</li> <li>X-Uri 表示客户端请求路径 URI。</li> <li>X-Args \$args 表示客户端请求中的参数。</li> </ul>
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,非整个请求传输时间。
ssl_verify_depth	5	[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 响应码是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。
ssl_early_data	off	on, off	启用或禁止 TLS 1.3 0-RTT。仅当 ssl_protocols 字段取值包含 TLSv1.3 时,开 启 ssl_early_data 才会生效。 <b>开启</b> ssl_early_data 后,有重放攻击的风险,请谨 慎开启。
http2_max_field_siz e	4k	[1-256]k	限制 HPACK 压缩的请求头字段的最大大小( Size )。
proxy_intercept_err ors	off	on, off	是否开启代理 error_page。 配置 error_page 必须提前设置 proxy_intercept_errors 为 on。
error_page	_	error_page code [ = [ response]] uri	当发生特定错误码(Code)的时候,能够显示一 个预定义的 URI,默认状态码(Response)为 302。URI 必须是以 / 开头的路径。配置 error_page 必须提前设置 proxy_intercept_errors 为 on。
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。
I7_toa	off	on, off	TOA 功能开关。开启 toa 功能后,默认将 TOA 中的客户端源 IP 和客户端源端口,分别添加在 \$remote_addr 和 \$remote_port 中。即 X- Forwarded-For 和 X-Real-IP 中已经透传了 TOA 中的 IP 信息。



			注意:此参数仅支持 IPv4 CLB 实例配置。
l7_toa_proxy_trans parent	off	on, off	<ul> <li>该配置关闭时,CLB 跟后端 RS 新建连接时,默认将收到的四元组的源 IP 地址作为客户端源 IP 封包传给后端。</li> <li>该配置打开时,代表将 TOA 中的客户端源 IP 封包传给后端 RS。如果开启了长连接,则统一使用100.127.0.0/16网段内的 IP。</li> </ul>
			汪意:此参致仪支持 IPv4 CLB 实例配置。

#### () 说明:

```
其中, proxy_buffer_size 和 proxy_buffers 配置的值需要满足约束条件: 2 * max (proxy_buffer_size,
proxy_buffers.size) ≤ (proxy_buffers.num - 1) * proxy_buffers.size。例如, 配置 proxy_buffer_size 为
24k, proxy_buffers 为 8 8k, 则2 * 24k = 48k, (8 - 1) * 8k = 56k, 此时 48k ≤ 56k, 因此配置不会报错, 否则
报错。
以下参数已由负载均衡器默认下发,故不允许将头字段名称设置为以下字段(不区分大小写): X-Stgw-Time、Host、
```

X-Client-Proto、X-Forwarded-Proto、X-Client-Proto-Ver、X-Client-Spdy、X-Real-IP、X-Forwarded-For、Upgrade、Connection。

## 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, "!" 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: <code>!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!PSK:!DHE</code> 。 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:

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: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-AES128-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-SHA256:SRP-RSA-AES128-SHA256:DH-RSA-AES128-SHA:DH-RSA-AES128-GCM-SHA256:DH-DSS-AES128-SHA256:SRP-RSA-AES128-SHA256:DH-RSA-AES128-SHA:DH-RSA-AES128-GCM-SHA256:DH-DSS-AES128-SHA256:SRP-RSA-AES128-SHA256:DH-RSA-AES128-SHA:DH-RSA-AES128-GCM-SHA256:DH-DSS-AES128-SHA256:SRP-RSA-AES-256-CBC-SHA:ECDH-ECDSA-AES256-GCM-SHA384:ECDH-RSA-AES256-GCM-SHA384:DH-DSS-AES128-SHA256:SRP-RSA-AES-256-CBC-SHA:ECDH-ECDSA-AES256-GCM-SHA384:AES128-SHA:DH-DSS-AES128-SHA256:AES128-SHA256:DH-RSA-SEED-SHA:ECDH-ECDSA-AES128-SHA:DA-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. 在个性化配置页面顶部选择地域,单击新建。
- 3. 在新建个性化配置页面,填写配置名和代码配置项,代码配置项以 ; 结尾。配置完成后,单击确认。

許述 「一州 1 ssl_protocols TLSv1 TLSv1.1 TLSv1.2; 2 client_header_timeout 60s; 3 client_header_buffer_size 4k; 4 client_body_timeout 60s; 5 client_max_body_size 60M; 6 keepalive_timeout 75s; 7 add_header xxx yyy; 8 more_set_headers "A:B"; 9 proxy_connect_timeout 4s; 10 proxy_read_timeout 60s;	I 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"; Construction of the terms of the terms of the terms of the terms of terms	铭	tinatest		
<pre>1 ssl_protocols TLSv1 TLSv1.1 TLSv1.2; 2 client_header_timeout 60s; 3 client_header_buffer_size 4k; 4 client_body_timeout 60s; 5 client_max_body_size 60M; 6 keepalive_timeout 75s; 7 add_header xxx yyy; 8 more_set_headers "A:B"; 9 proxy_connect_timeout 4s; 10 proxy_read_timeout 60s;</pre>	<pre>1 ssl_protocols TLSv1 TLSv1.1 TLSv1.2; 2 client_header_timeout 60s; 3 client_header_buffer_size 4k; 4 client_body_timeout 60s; 5 client_max_body_size 60M; 6 keepalive_timeout 75s; 7 add_header xxx yyy; 8 more_set_headers "A:B"; 9 more_set_headers "A:B";</pre>	载地域	广州		
<pre>2 client_header_timeout 60s; 3 client_header_buffer_size 4k; 4 client_body_timeout 60s; 5 client_max_body_size 60M; 6 keepalive_timeout 75s; 7 add_header xxx yyy; 8 more_set_headers "A:B"; 9 proxy_connect_timeout 4s; 10 proxy_read_timeout 60s;</pre>	<pre>2 client_header_timeout 60s; 3 client_header_buffer_size 4k; 4 client_body_timeout 60s; 5 client_max_body_size 60M; 6 keepalive_timeout 75s; 7 add_header xxx yyy; 8 more_set_headers "A:B"; 9</pre>	FRE	1	<pre>ssl_protocols TLSv1 TLSv1.1 TLSv1.2;</pre>	145
<pre>3 client_header_buffer_size 4k; 4 client_body_timeout 60s; 5 client_max_body_size 60M; 6 keepalive_timeout 75s; 7 add_header xxx yyy; 8 more_set_headers "A:B"; 9 proxy_connect_timeout 4s; 10 proxy_read_timeout 60s;</pre>	<pre>3 client_header_buffer_size 4k; 4 client_body_timeout 60s; 5 client_max_body_size 60M; 6 keepalive_timeout 75s; 7 add_header xxx yyy; 8 more_set_headers "A:B"; 9 more_set_headers to for the formula for the formula formula for the formula formula for the formula for</pre>		2	<pre>client_header_timeout 60s;</pre>	
<pre>4 client_body_timeout 60s; 5 client_max_body_size 60M; 6 keepalive_timeout 75s; 7 add_header xxx yyy; 8 more_set_headers "A:B"; 9 proxy_connect_timeout 4s; 10 proxy_read_timeout 60s;</pre>	<pre>4 client_body_timeout 60s; 5 client_max_body_size 60M; 6 keepalive_timeout 75s; 7 add_header xxx yyy; 8 more_set_headers "A:B"; 9 more_set_headers "A:B";</pre>		3	<pre>client_header_buffer_size 4k;</pre>	
<pre>5 client_max_body_size 60M; 6 keepalive_timeout 75s; 7 add_header xxx yyy; 8 more_set_headers "A:B"; 9 proxy_connect_timeout 4s; 10 proxy_read_timeout 60s;</pre>	<pre>5 client_max_body_size 60M; 6 keepalive_timeout 75s; 7 add_header xxx yyy; 8 more_set_headers "A:B"; 9</pre>		4	<pre>client_body_timeout 60s;</pre>	
<pre>6 keepalive_timeout 75s; 7 add_header xxx yyy; 8 more_set_headers "A:B"; 9 proxy_connect_timeout 4s; 10 proxy_read_timeout 60s;</pre>	<pre>6 keepalive_timeout 75s; 7 add_header xxx yyy; 8 more_set_headers "A:B"; </pre>		5	client_max_body_size 60M;	-
<pre>7 add_header xxx yyy; 8 more_set_headers "A:B"; 9 proxy_connect_timeout 4s; 10 proxy_read_timeout 60s;</pre>	7 add_header xxx yyy; 8 more_set_headers "A:B";		6	keepalive_timeout 75s;	
8 more_set_headers "A:B"; 9 proxy_connect_timeout 4s; 10 proxy_read_timeout 60s;	8 more_set_headers "A:B";		7	add_header xxx yyy;	
9 proxy_connect_timeout 4s; 10 proxy_read_timeout 60s;			8	more_set_headers "A:B";	
<pre>10 proxy_read_timeout 60s;</pre>	9 proxy_connect_timeout 4s;		9	proxy_connect_timeout 4s;	
	10 proxy_read_timeout 60s;		10	proxy_read_timeout 60s;	
11 prove cond timoout for.	11 prove cond timoout 60c.		11	prove cond timeout 60c.	

- 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。

绑定至实例						×
() 个性化配置仅针对负载均衡	fī(原"应用型负载均衡")的七层	HTTP/H	TTPS	监听器生效。		
请选择 CLB 实例 (共3个)				已选择 (共1/100个)		
支持搜索实例 ID、实例名称、V	P	Q		实例 ID	实例名称	
🚽 实例 ID	实例名称			lb-	lb-	8
V lb-	lb-					
lb-	lb-					
lb-	lb-		↔			
共3条 10 ❤条/页	<li>&lt; 1 /1页 ▶</li>	M				
		确定		取消		
		WORL		-90/13		



- 4. 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。
- 7. (可选)绑定实例后,也可以在实例的列表页中找到对应的个性化配置信息。

#### () 说明:

若列表页中未显示"绑定个性化配置"列,则在列表页右上角单击**众**图标,在弹出的**自定义列表字段**对话框中勾选"绑定个 性化配置"选项,单击**确定**,列表页即可显示"绑定个性化配置"列。

默认配置代码示例如下,代码复制时请您确认尾行无空行,以确保配置成功:

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;

# 七层转发域名和 URL 规则说明

最近更新时间: 2025-06-25 11:42:42

## 业务流程图

负载均衡(原"应用型负载均衡")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。

# 七层转发配置说明

## 转发域名配置规则

七层负载均衡可以将来自不同域名和 URL 的请求转发到不同的服务器上处理,一个七层监听器可以配置多个域名,一个域名可以配置 多条转发路径。转发域名的配置方式请参考 <mark>配置负载均衡的转发域名</mark> 。

配置限制:转发域名长度限制1 – 80个字符,不能以 📃 开头,暂不支持后缀为中文的域名。

域名配置规则	说明	举例
精准匹配	<b>支持的字符集为:</b> a-z 0-9 。	www.example.com



通配匹配	<ul> <li>支持的字符集为: a-z 0-9 。</li> <li>需以星号(*)作为通配符使用。</li> <li>支持 * 在开头或结尾,且单个域名中仅支持 * 出现一次。</li> </ul>	*.example.com <b>或</b> www.example.*
正则匹配	<ul> <li>• 支持的字符集为: a-z 0-9 ? = ~ +</li> <li>\ ^ * ! \$ &amp; Ⅰ ( ) [ ] 。</li> <li>● 需以 ~ 开头,且 ~ 仅能出现一次。</li> </ul>	~^www\d+\.example\.com\$

#### 转发域名匹配说明

#### 转发域名通用匹配策略

- 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.qcloud.com 为例,格式如下所示:
  - 精准域名 example.qcloud.com ,精确匹配 example.qcloud.com 域名。
  - 前缀通配符域名 \*.qcloud.com 匹配所有以 qcloud.com 结尾的域名。
  - 后缀通配符域名 example.qcloud.\* 匹配所有以 example.qcloud 开头的域名。
  - 正则匹配域名 ~^www\d+\.example\.com\$ 根据正则表达式进行匹配。
  - 匹配优先级:精确路径>前缀路径(非正则)>正则路径(~)。正则表达式之间无优先级差异,一个域名如果命中多个正则规则时,具体的生效顺序和底层的配置顺序有关,如果客户有精确的转发需求,建议通过精确路径匹配和前缀匹配方式进行区分。
- **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

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 ),让默认规则可控,每个监听器下 只能配置一个默认域名。

例如,在 CLB1 的HTTP:80监听器下配置了2个域名:<br/>www.test1.comwww.test1.comwww.test2.com其中<br/>www.test1.comwww.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<br/>www.test1.comwww.test1.com

HTTP/HTTPS监听器				
新建				
- http-80(HTTP:80)				
- www.test1.com	默认访问			
/				
- www.test2.com				

() 说明:

• 2020年05月18日之前,七层监听器是否配置默认域名为可选项,您可以选择配置默认域名或者不配置。



- 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。
- 自2020年05月18日起:
  - 所有新建的七层监听器都必须配置默认域名:七层监听器的第一个规则一定会启用默认域名,调用 API 创建七层规则 时,CLB会 将 DefaultServer 字段自动设置为 true。
  - 所有已配置默认域名的监听器,修改或删除默认域名时需指定新的默认域名:控制台操作时需您指定新的默认域名;调用 API 操作时,若不设置新的默认域名 CLB 会随机选取一个剩余域名设置为新的默认域名。
  - 存量未配置默认域名的规则:您可以按业务需求直接配置默认域名,操作步骤如下"操作四";若您不配置,腾讯云 会将 CLB 加载的第一个域名设置为默认域名,存量监听器会在2020年06月19日内处理完毕。

上述策略自2020年05月18日起逐步实施,各个实例生效日可能略有差异。自2020年06月20日起,所有转发域名不为空的七 层监听器都会有默认域名。

默认域名的有如下四项相关操作:

•操作一:当为七层监听器配置第一条转发规则时,默认域名必须是开启状态。

创建转发规则		×
1 基本配置	2 健康检查 > 3 会话保持	
域名①	www.test.com	
默认域名	启用 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,详 <b>情</b>	
URL路径()		
均衡方式	加权轮询 🔻	
	当后端CVM的权重都设置为同一个值时,权重属性将不生效,将按照简单的轮询 分发请求	策略

- •操作二:关闭当前默认域名。
  - 某监听器下有多个域名,关闭当前默认域名时,需指定新的默认域名。



编辑域名	×
域名(j)	www.test.com
默认域名	新信載者 ● ◆ ◆ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●
新的默认域名	Server),母小监师器只能配合自必须配合一个新从观者, <b>评审</b> www.test2.com
	关闭 提交

○ 当某监听器只有一个域名,且该域名是默认域名时,不允许关闭默认域名。

编辑域名		×
域名(	www.test.com	
默认域名	<mark>新増域名</mark> 启用 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,详情	
	关闭 提交	

- •操作三:删除默认域名。
  - 某监听器下有多个域名,删除默认域名下的规则:
    - 若该规则不是默认域名的最后一条规则,可以直接删除。
    - 若该规则是默认域名的最后一条规则,需设置新的默认域名。

HTTP/HTTPS监听器				_
新建		确认要删除该转发	<b>史规则</b>	×
http-80(HTTP:80)	转发规则详情展开,	监听器	http-80 (HTTP: 80)	
www.test1.com	已绑定后端服务	域名	www.test2.com (版认城名)	
/index		規则	1	
— www.test2.com 默认访问	CVM ID/名科	绑定后端服务①	0个	IF
		新的默认域名 ①	www.test1.com +	5
			请配置新的默认域名	
			确定关闭	

○ 当某监听器只有一个域名时,可以直接删除所有规则且不必设置新的默认域名。



•操作四:修改默认域名,您可以在监听器列表快捷修改默认域名。

HTTP/HTTPS监听器	
- http-80(HTTP:80)	+ 🖍 🖻
- www.test1.com	默认访问
- www.test2.com	<ul> <li>✓ +</li> <li>设置为默认域名</li> </ul>

## 转发 URL 路径配置规则

七层负载均衡可以将来自不同 URL 的请求转发到不同的服务器上处理,一个域名可以配置多条转发 URL 路径。 配置限制:转发 URL 长度限制1 – 200个字符。

路径匹配规则	说明	举例
通用匹配	<ul> <li>支持的字符集为: a-z A-Z 0-9 / = ? : 。</li> <li>必须以 / 开头,区分大小写。</li> <li>按最长前缀匹配,优先精确匹配,而后模糊匹配。</li> </ul>	/index
正则匹配	<ul> <li>支持的字符集为: a-z A-Z 0-9 / = ? ~ ^ * \$</li> <li>: () [] + 1。</li> <li>需以 ~ 开头,且 ~ 仅能出现一次。</li> <li>不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。</li> <li>~ 开头表示否定正则匹配。</li> </ul>	~* .png\$
精确匹配	<ul> <li>支持的字符集为: a-z A-Z 0-9 / = ? : 。</li> <li>需以 = 开头精确匹配。</li> <li>优先级最高,匹配后不再匹配其他路径。</li> </ul>	=/index.html

## 转发 URL 路径匹配说明





- 匹配规则:按最长前缀匹配,优先精确匹配,而后模糊匹配。
   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规则中:
  - 1.1 example.qcloud.com/test1/image/index1.html
     精确匹配转发规则1设置的 URL 规则,则该请求将被转发到转发规则1所关联的后端云服务器中,即图中 CVM1 和 CVM2 的80端口。
  - **1.2** example.qcloud.com/test1/image/hello.html 无精确匹配,按最长前缀将匹配到转发规则2,因此该请求将被转发 到转发规则2所关联的后端云服务器中,即图中 CVM2 和 CVM3 的81端口。
  - 1.3 example.qcloud.com/test2/video/mp4/ 无精确匹配,按最长前缀将匹配到转发规则3,因此该请求将被转发到转发规则3所关联的后端云服务器中,即图中 CVM4 的90端口。
  - 1.4 example.qcloud.com/test3/hello/index.html 无精确匹配,按最长前缀将匹配到根目录 Default URL: example.qcloud.com/,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。
  - **1.5** example.gcloud.com/test2/无精确匹配,按最长前缀将匹配到根目录 Default URL: example.gcloud.com/。
- 2. 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。
- 3. 例如,客户端请求 example.qcloud.com/test1/image/index1.html 匹配了转发规则1,但此时转发规则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,不会重定向到其他页面。
- 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。
- 5. 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。
- 6. 七层 URL 路径末尾斜杠的说明:当用户设置的 URL 是以 / 结尾,但客户端访问时并没有带 / ,那么该请求会被重定向到以 / 结尾的规则(301重定向)。
  - 例如, HTTP:80 监听器下, 配置的域名是 www.test.com 。
  - 6.1 该域名下设置的 URL 为 /abc/ :
  - 客户端访问 www.test.com/abc 时,会被重定向到 www.test.com/abc/。
  - 客户端访问 www.test.com/abc/ 时,会匹配到 www.test.com/abc/。
  - 6.2 该域名下设置的 URL 为 / abc :
    - 客户端访问 www.test.com/abc 时,会匹配到 www.test.com/abc 。
    - 客户端访问 www.test.com/abc/ 时,也会匹配到 www.test.com/abc 。

### () 说明:

当业务未配置"/" location,并尝试访问 https://xxx/ 时,若 index.html 内容为空,则返回 200;若 index.html 不存 在,则返回 404。

## 七层健康检查配置说明

### 健康检查域名配置规则

健康检查域名是七层负载均衡探测后端服务健康状态的域名。

- 健康检查域名长度限制: 1-80个字符。
- 健康检查域名默认为转发域名。
- 健康检查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。
- 健康检查域名支持的字符集为: a-z 0-9 . \_ , 例如 www.example.qcloud.com 。

## 健康检查路径配置规则

健康检查路径是七层负载均衡探测后端服务健康状态的 URL 路径。

- 健康检查路径长度限制: 1-200个字符。
- 健康检查路径默认为 / ,且必须以 / 开头。
- 健康检查路径不支持正则表达式,建议指定某个固定 URL 路径(静态页面)进行健康检查。
- 健康检查路径支持的字符集为: a-z A-Z 0-9 . \_ / = ? :,例如 /index 。



# CLB 支持 QUIC 协议

最近更新时间: 2025-05-15 17:46:21

QUIC 协议能帮您大幅提升 App 访问速度,在弱网络、Wi−Fi 和4G 频繁切换等场景下,无需重连即可实现多路复用。本文档将为您 介绍,如何在负载均衡控制台中,配置 QUIC 协议。

# QUIC 概述

QUIC(Quick UDP Internet Connection),又称为快速 UDP 互联网连接,是由 Google 提出的使用 UDP 进行多路并发传输 的协议,QUIC 相比现在广泛应用的 TCP+TLS+HTTP2 协议有如下优势:

- 减少连接建立时间。
- 改善拥塞控制。
- 避免队头阻塞的多路复用。
- 连接迁移。

CLB 开启 QUIC 后,客户端可以和 CLB 之间建立 QUIC 连接,当二者协商无法建立 QUIC 连接时自动降级到 HTTPS 或 HTTP/2。若开启 QUIC 后端协议只能使用 HTTP1.x 协议。

## 使用限制

- 仅负载均衡实例类型支持,传统型负载均衡实例类型不支持。
- 仅七层 HTTPS 监听器支持 QUIC 协议。
- 当前 CLB 支持的 QUIC 版本有:Q050、Q046、Q043、h3-29 和 h3-27。

## 操作步骤

根据需求创建负载均衡实例,详情请参见 创建负载均衡实例 。

- 1. 登录 负载均衡控制台,在左侧导航栏,单击实例管理。
- 2. 在**实例管理**页面中,单击**负载均衡**。
- 3. 创建负载均衡实例,在右侧操作栏,单击配置监听器。

新建 删除	भ्रा	配至项目	编辑标签	更多操作 ▼				Pfr.M	I项目:所有项目			Q \$\phi \$\p\$
ID/名称 \$	监控	状态	域名	VIP	网络类型 下	所属网络	实例规格	健康状态	计费模式 ▼	带宽上限	标签 ▼	操作
lt s	.lı	正常		$\frac{1}{2} = 1 \geq 0$	公网	аñ,	ž		按量计费-按网络 流量 00:10创建	10Mbps	能	配置监听器 更多 🔻

4. 在监听器管理页面的 "HTTP/HTTPS 监听器" 下,单击新建。



< <b>*****</b>	derm.				
基本信息	监听器管理	重定向配置	监控	安全组	
温馨提示:	当您配置了自定义重	定向策略,原转发规则进	进行修改后, 重	定向策略会默认解除,需要重新酯	置。查看也
HTTP/HTTPS业 新建	盔听器				
	您还未创建监	乐器, 点击开始创建		点击左侧节点查看详情	Ling to the second s

5. 在**创建监听器**页面,切换监听协议端口为 HTTPS,根据需要填写完后,单击**提交**。



创建监听器	×
名称	
	不能超过60个字符
监听协议	•
监听器端口	
	端口范围:1-65535
启用长连接	
	开启后,CLB 与 RS 连接数范围在请求[QPS, QPS*60]区间波动,具体数值取决于连接
	复用率。如 RS 对连接数上限有限制,请谨慎操作。
Gzip 压缩	○ 透传模式 ○ 兼容模式
	CLB 可以透传压缩包,此时需要后端 CVM 开启压缩功能
启用SNI	
SSL解析方式	单向认证(推荐) ▼ 详细对比 🔽
	注意:当您需要客户端也提供证书时,请选择SSL双向认证。
服务器证书	○ 选择已有 ○ 新建
	■ ■ ■ ▼ 添加证书 删除
1、当选用HTT 器之间转发协 <sup>。</sup>	「PS监听协议时,客户端到负载均衡的访问使用HTTPS;而负载均衡到后端云服务 🗙 议,可在创建转发规则时选择 HTTP 或 HTTPS。
2、HTTPS 监 管理证书	听器的服务器证书支持配置双证书,即两种不同加密算法类型的证书,详情请参见
3、负载均衡器 SSL证书。	\$代理了SSL加解密的开销,保证访问安全。您可以到SSL证书管理平台,申请免费
4、当您希望启	吕用SNI时,无需在当前页面配置证书,在域名配置页面单独配置证书即可。

6. 在**监听器管理**标签页,单击该新建监听器的+符号。



← It-tain	iye .				
基本信息	监听器管理	重定向配置	监控	安全组	
温馨提示:	当您配置了自定义重定	全向策略, 原转发规则进	行修改后,	重定向策略会默认解除,	需要重新配置。查看已
HTTP/HTTPS; 新建	监听器				
+ Iniai	10770346	+	/ Ū	点击左侧节点	ē 看详情

7. 在**创建转发规则**页面,打开 QUIC 协议,创建七层规则,并填写相关字段后,单击**下一步**,即可完成基本配置。

## () 说明:

- 创建完成后 ,若需修改 QUIC 协议的开关状态,请在对应规则的域名处编辑。
- QUIC 使用 UDP 协议,会占用 CLB 的 UDP 端口,即 HTTPS 监听器开启 QUIC 协议后,自动占用对应的 UDP 端口和 TCP 端口。例如,当 HTTPS:443 监听器开启 QUIC 协议后,该规则会同时占用 TCP:443 和 UDP:443 端口,因此您不能再创建 TCP:443 和 UDP:443 监听器。

∕⊘膨	衛田云
-----	-----

创建转发规则		×
1 基本配置	2 健康检查 > 3 会话保持	
域名	新增域名	
默认域名	启用	
	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	
HTTP2.0	Server),每十监听器只能能直且必须能直一十款以现者,详有	
QUIC		
URL路径()	1	
均衡方式	加权轮询	
	WRR 根据新建连接数来调度,权重越高的后端服务器被轮询到的概率越高	
后端协议①	HTTP •	
获取客户端 IP	已启用	
后端目标组		
	关闭下一步	

# 后续操作

填写完基本配置后,可继续完成 健康检查 和 会话保持 的相关操作。

# CLB 支持 SNI 多域名证书

最近更新时间: 2025-05-15 17:46:21

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

腾讯云 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 购买负载均衡实例。

() 说明:

传统型负载均衡不支持基于域名和 URL 的转发,因此传统型负载均衡不支持 SNI。

## 操作步骤

- 1. 登录 负载均衡控制台。
- 2. 参考 配置监听器 的操作步骤配置监听器,并且在配置 HTTPS 监听器时,开启 SNI。



创建监听器			×
名称			
	不能超过60个字符		
监听协议	HTTPS 🔻		
监听器端口			
	端口范围:1 - 65535		
启用长连接			
	开启后, CLB 与 RS 连	接数范围在请求[QPS, QPS*60]区间波动,具体数值取决于连接	
Gzip 压缩	<ul> <li>夏田率。如 KS 对连接:</li> <li>● 透传模式 ●</li> </ul>	蚁工略有略制,項僅俱無FF。 兼容模式	
	CLB 可以透传压缩包,	此时需要后端 CVM 开启压缩功能	
启用SNI()			
1、当选用HTT 之间转发协议, 2、HTTPS 监F 理证书	PS监听协议时,客户端 可在创建转发规则时选 所器的服务器证书支持配	到负载均衡的访问使用HTTPS;而负载均衡到后端云服务器 🗙 择 HTTP 或 HTTPS。 )置双证书,即两种不同加密算法类型的证书,详情请参见管	
3、负载均衡器 SSL证书。	代理了SSL加解密的开锁	肖,保证访问安全。您可以到SSL证书管理平台,申请免费	
4、当您希望启	用SNI时,无需在当前页	面配置证书,在域名配置页面单独配置证书即可。	
		关闭 提交	

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。



域名(	
默认域名	新增或名 启用 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
HTTP2.0	Server),设个监听益只能能直且必须能直一个新环境名,详有
QUIC	
URL路径()	
均衡方式	加权轮询
后端协议	WRR 根据新建连接数来调度,权重越高的后端服务器被轮询到的概率越高 HTTP  ▼
SSL解析方式	<ul> <li>单向认证(推荐) ▼</li> <li>详细对比</li> <li>详细对比</li> <li>注意:当您需要客户端也提供证书时,请选择SSL双向认证。</li> </ul>
服务器证书	● 选择已有     新建       ■■     ■■       ▼     添加证书
获取客户端 IP	已启用
后端目标组()	
	关闭 下一步

# 七层协议支持 gRPC

最近更新时间: 2025-05-13 09:27:22

gRPC 是 Google 发布的基于 HTTP 2.0 传输层协议的高性能开源软件框架,提供了支持多种编程语言、对网络设备进行配置和纳 管的方法。本文指导您通过配置 HTTPS 监听器的 gRPC 协议的健康检查,将客户端的 gRPC 请求通过 CLB 实例转发到后端协议 为 gRPC 的后端服务。

# 使用场景

当客户端通过 HTTPS 请求访问协议类型为 gRPC 的后端服务时,您可以通过 CLB 实例的 HTTPS 监听器支持 gRPC 协议来实 现。



## 前提条件

- 您已创建 VPC,详情请参见 创建私有网络。
- 您已在 VPC 中创建了 CVM 实例,并在实例上部署了 gRPC 服务,详情请参见 通过镜像创建实例。
- 您已购买了 CLB 实例,详情请参见 创建负载均衡实例 。

## 使用限制

- 仅负载均衡类型支持,传统型负载均衡不支持。
- IPv6 版本 CLB 与开启了七层混绑的 IPv6 版本 CLB 不支持。
- 仅 VPC 网络支持,基础网络不支持。
- 后端服务不支持 SCF (需要 SCF target 内部支持 gRPC 协议)。

# 操作步骤

## 步骤1: 配置监听器

- 1. 登录 负载均衡控制台,在左侧导航栏单击实例管理。
- 2. 在 CLB 实例列表页面左上角选择地域,在实例列表右侧的操作列中单击配置监听器。
- 3. 在 HTTP/HTTPS 监听器下,单击新建,在弹出的创建监听器对话框中配置 HTTPS 监听器。

#### 3.1 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	<ul> <li>监听协议:本示例选择 HTTPS。</li> <li>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。</li> <li>同一个负载均衡实例内,监听端口不可重复。</li> </ul>	HTTPS:443
	开启后,CLB 与后端服务之间使用长连接,CLB 不再透传源 IP,请从 XFF 中获取 源 IP。为保证正常转发,请在 CLB 上打开安全组默认放通或者在 CVM 的安全组上 放通100.127.0.0/16。	
启用长连接	<ul> <li>① 说明:</li> <li>开启后,CLB与后端服务的连接数范围在请求[QPS,QPS*60]区间波动,具体数值取决于连接复用率。若后端服务对连接数上限有限制,则建议谨慎开启。此功能目前处于内测中,如需使用,请提交内测申请。</li> <li>健康检查中的健康探测源 IP 100.64.0.0/10 网段已默认放通,此网段下的 IP 无需再次放通。</li> </ul>	不启用
Gzip 压缩	<ul> <li>透传模式: CLB 可以透传压缩包,此时需要后端 CVM 开启压缩功能,详情请参见 负载均衡开启 Gzip 配置。</li> <li>兼容模式: CLB 对指定文件进行压缩,无需后端 CVM 同步开启压缩功能。</li> </ul>	_
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。	不启用
SSL 解析方 式	支持单向认证和双向认证。负载均衡器代理了 SSL 加解密的开销,保证访问安全。	单向认证
服务器证书	可以选择 SSL 证书平台 中已有的证书,或新建证书。	选择已有

### 3.2 创建转发规则

转发规则基本配 置	说明	示例
域名	转发域名: • 长度限制: 1 - 80个字符。 • 不能以`_`开头。 • 支持精准域名和通配域名。 • 支持正则表达式。 具体配置规则,详情请参见 转发域名配置规则。	www.example .com
默认域名	<ul> <li>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。</li> <li>一个监听器下仅能配置一个默认域名。</li> </ul>	开启
HTTP 2.0	启用 HTTP2.0 后,CLB 可以接收 HTTP 2.0 的请求,无论客户端请求 CLB 时使用哪种 HTTP 版本,CLB 访问后端服务器的 HTTP 版本都是 HTTP 1.1。	开启

QUIC	启用 QUIC 后,客户端可以和 CLB 之间建立 QUIC 连接,当二者协商无法建 立 QUIC 连接时自动降级到 HTTPS 或 HTTP/2,但 CLB 和后端服务器之间 仍然使用 HTTP1.x 协议。详情请参见 CLB 支持 QUIC 协议 。	开启
URL 路径	转发 URL 路径: <ul> <li>长度限制: 1 – 200个字符。</li> <li>支持正则表达式。</li> <li>具体配置规则,详情请参见 转发 URL 路径配置规则 。</li> </ul>	/index
均衡方式	<ul> <li>HTTPS 监听器中,负载均衡支持加权轮询(WRR)、加权最小连接数(WLC)和 IP Hash 三种调度算法:</li> <li>加权轮询算法: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。加权轮询算法根据新建连接数来调度,权值越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。</li> <li>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。</li> <li>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。</li> </ul>	加权轮询
后端协议	后端协议是指 CLB 与后端服务之间的协议: <ul> <li>后端协议选择 HTTP 时,后端服务需部署 HTTP 服务。</li> <li>后端协议选中 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。</li> <li>后端协议选中 gRPC 时,后端服务需部署 gRPC 服务。仅 HTTP2.0 开启且 QUIC 关闭的情况下,后端转发协议支持选择 gRPC。</li> </ul>	gRPC
获取客户端 IP	默认启用,详情请参见 获取客户端IP 。	已开启

#### 3.3 HTTPS 健康检查。

#### 3.4 会话保持

腾讯云

会话保持配 置	说明	示例
会话保持开 关	<ul> <li>开启会话保持后,负载均衡监听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。</li> <li>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。</li> <li>加权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。</li> </ul>	开启
会话保持时 间	<ul> <li>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。</li> <li>可配置范围30s - 86400s。</li> </ul>	30s

## 步骤2: 绑定后端云服务器

- 1. 在监听器管理页面,单击刚才创建的监听器,如上述 HTTPS:443 监听器,单击左侧的 + 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。

#### () 说明:

腾讯云

默认端口功能:先填写"默认端口",再选择云服务器后,每台云服务器的端口均为默认端口。

## 步骤3:安全组(可选)

您可以配置负载均衡的安全组来进行公网流量的隔离,详情请参见配置负载均衡安全组。

## 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,图标修改或面图标删除。

# 后端服务器 后端服务器概述

最近更新时间: 2024-10-12 16:44:41

后端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服务器。在配置 负载均衡监听器 时,需绑定后端服务器,负 载均衡通过不同的 轮询方式,将请求转发到后端服务器上,并由后端服务器来做处理,保证应用平稳可靠的运行。

## 支持的后端服务器类型

负载均衡支持的后端服务类型包括实例类型、IP 类型和 云函数 SCF 类型,其中:

- 实例类型又包括 云服务器 CVM、弹性网卡 ENI 和 容器实例 EKS。
- IP 类型主要用于绑定云上多 VPC 的内网 IP, 以及云下 IDC 的内网 IP。

## 注意事项

在添加后端服务器时,我们建议您:

- 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 连接并使多个请求使用它,可减少 Web 服务器上的负载并提高 负载均衡的吞吐量。
- 确保后端服务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,详情请参见后端云服务器的安全组配置。

# 相关文档

- 管理后端服务器
- 绑定弹性网卡
- 混合云部署
- 绑定云函数 SCF

# 管理后端服务器

最近更新时间: 2025-05-23 17:06:12

负载均衡将请求路由至运行正常的后端服务器实例,首次使用负载均衡或根据业务需求,需要增加或删除后端服务器数量时,可按照本 文指引进行操作。

## 前提条件

需已创建负载均衡实例并配置监听器,详情请参见 负载均衡快速入门。

## 操作步骤

## 添加负载均衡后端云服务器

🕛 说明:

- 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。若从弹性伸缩组移除 某云服务器实例,则该云服务器实例会自动从负载均衡后端云服务器中删除。
- 如需使用 API 添加负载均衡后端服务器,请参见 绑定后端服务器到负载均衡 接口说明。
- 若您的账户类型为传统账户类型,且实例的运营商类型为中国移动、中国电信或中国联通,则仅能绑定网络计费模式为按流 量计费和共享带宽包的云服务器。账户类型详情请参见 判断账户类型,运营商类型详情请参见 运营商类型。
- 1. 登录 负载均衡控制台。
- 2. 在**实例管理**页面的"负载均衡"页签中,单击目标负载均衡实例右侧操作列的配置监听器。
- 3. 在配置监听器模块中,选择需要绑定后端云服务器的监听器。

#### • HTTP/HTTPS 监听器

3.1 在 HTTP/HTTPS 监听器区域,单击目标监听器左侧的 +。

+ test-http-80(HTTP:80)

3.2 在展开的域名左侧单击+。



## 3.3 选中展开的 URL 路径,单击**绑定**。

HTTP/HTTPS监听器(已配置1个) 新建	
— test-http-80(HTTP:80)	转发规则详情 展开 ▼
www.example.com 默认访问	已绑定后端服务
/	第定 修改端口 修改权重 解绑 按照内网IP搜索,用" "分割 Q ↓
	ID/名称 端口健康状态 () IP地址 端口 权重 操作
	监听器创建完成,请 <b>绑定后端服务</b>

#### • TCP/UDP/TCP SSL 监听器

在 TCP/UDP/TCP SSL 监听器模块的左侧列表中,选中需要绑定后端云服务器的监听器,单击绑定。

TCP/UDP/TCP SSL/QUIC监听器(已配置1个) 新建	
test-tcp(TCP:443)	<b>监听器详情</b> 展开 ▼
	已绑定后端服务
	第定 修改端口 修改权重 解绑 按照内网ⅠP搜索,用" "分書 Q ♀
	ID/名称 端口健康状态 ③ IP地址 端口 权重 操作
	监听器创建完成,请 <b>绑定后端服务</b>

#### 4. 为负载均衡实例绑定后端服务。

• 方式1: 在绑定后端服务弹出框中,单击**云服务器**,选择需要关联的云服务器(可多选),并填写相关云服务器需要被转发的端口与 权重,详情请参见 服务器常用端口,单击确定。

#### () 说明:

- 在绑定后端服务弹出框中仅展示同地域、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。
- 绑定多个后端服务器时,CLB 将按 Hash 算法转发流量,起到均衡负载的作用。
- 权重越大转发的请求越多,默认为10,可配置范围为0 100。当权重设置为0,该服务器不会再接受新请求。如开启
   会话保持,可能会造成后端服务器的请求不均匀,详情请参见均衡算法选择与权重配置实例。



绑定后端服务						×
目标类型() <b>O</b> 实例 OIP类型						
所属网络 lb_						
请选择实例		已选择 (2)				
<b>云服务器 弹性网卡</b> 容器突例 默认满口 默认权重		ID/实例名	端口	权重 ()		
IP地址 ▼ 按照P地址搜索,关键字用1"或空 Q		ins-	80	- 10 +	添加端口 删除	
- ID/实例名		ine			1	
ins.		115-	80	- 10 +	添加端口删除	
ins-	↔					
ins-						
10 ▼ 条/页   < 1   /1页 →						
支持按住 shift 键进行多选						
		确认 取消				
	-					

方式2:如需批量绑定服务器且预设端口值一致时,可在绑定后端服务弹出框中,单击云服务器,并输入默认端口值(端口选择请参见服务器常用端口)、再勾选相关服务器并设定权重值,单击确定。



绑定后端服 <b>务</b>						×
目标类型 🛈 🔹 文例 🔿 IP 类型						
所属网络 Ib_auto 请选择实例		己选择 (2)				
云服务器 弹性网卡 容器实例 80 默认权重		ID/实例名	端口	权重 🛈		
IP地址 ▼ 按照IP地址撞索,关键字用""或空 Q		ins-f	80	- 10	+	添加端口删除
■ ID/实例名 ID/实例名 Ins-	ŧ	ins-(	80	- 10	+	添加端口 删除
10 ▼ 条/页 < 1 /1页 →						
支持按住 shift 键进行多选		确 <mark>认</mark> 取消				

#### 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,接下来将以 "HTTP/HTTPS 监听器"为例(TCP/UDP/TCP SSL 监听器的修改方式相同),为您介绍如何修改负载均衡后端服务器权重。

() 说明:

- 如需使用 API 修改负载均衡后端服务器权重,请参见 修改负载均衡器后端服务器权重 接口说明。
- 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。
- 2. 在**实例管理**页面的"负载均衡"页签中,单击目标负载均衡实例右侧操作列的配置监听器。
- 3. 在 HTTP/HTTPS 监听器模块左侧列表中,展开实例与监听器规则,选中 URL 路径。

<ul> <li>test-http(HTTP:80)</li> </ul>	
- 1.1.1.1	默认访问
/1.1.21.3	



4. 在 HTTP/HTTPS 监听器模块右侧服务器列表中,修改相关服务器权重。

#### () 说明:

权重越大转发的请求越多,默认为10,可配置范围为0 – 100。 当权重设置为0,该服务器不会再接受新请求。 如开启会 话保持,可能会造成后端服务器的请求不均匀,详情请见 均衡算法选择与权重配置实例 。

- 方式1: 单独修改某台服务器权重。
  - 4.1 找到需要修改权重的服务器,并将鼠标悬浮于对应权重上方,单击》编辑按钮。

<b>绑定</b> 修改端口 修改权重	解绑		按照内网IP搜索,	用" "分割关键字	Q Ø
ID/名称	端口健康状态()	IP地址	端口	权重	操作
	健康		80 🎤	10 <mark>/</mark> 编辑	解绑

4.2 在修改权重弹窗中,输入修改后的权重值,单击提交。

#### • 方式2: 批量修改某些服务器权重。

① 说明:		
批量修改权重后的服务器权重相同。		

4.1 单击服务器前方复选框,选中多台服务器,在列表上方,单击修改权重。

<b>绑定</b> 修改端口 修改权重	解绑		按照内网IP搜索,	用" "分割关键号	₽ <b>Q</b> Ø
✓ ID/名称	端口健康状态(;)	IP地址	端口	权重	操作
	健康		80	10	解绑

4.2 在修改权重弹窗中,输入修改后的权重值,单击提交。

### 修改负载均衡后端服务器端口

负载均衡控制台支持修改后端服务器端口,接下来将以 "HTTP/HTTPS 监听器"为例(TCP/UDP/TCP SSL 监听器的修改方式相同),为您介绍如何修改负载均衡后端服务器端口。

()	说明:			
	如需使用 API 修改负载均衡后端服务器端口,	请参见	修改监听器绑定的后端机器的端口 接口说	兑明。

#### 1. 登录 负载均衡控制台。

2. 在**实例管理**页面的负载均衡页签中,单击目标负载均衡实例右侧操作列的配置监听器。

- ∽ 腾讯云
- 3. 在 HTTP/HTTPS 监听器模块左侧列表中,展开实例与监听器规则,选中 URL 路径。

— test-h	http(HTTP:80)		
	1.1.1.1	默认访问	
	—/1.1.21.3		

- 4. 在 HTTP/HTTPS 监听器模块右侧服务器列表中,修改相关服务器端口,端口选择请参见 服务器常用端口 。
- 方式1: 单独修改某台服务器端口。
  - 4.1 找到需要修改端口的服务器,并将鼠标悬浮于对应端口上方,单击》编辑按钮。

<b>绑定</b> 修改端口 修改权重	解绑		按照内网IP搜索,	用" "分割关键字	Q Ø
ID/名称	端口健康状态()	IP地址	端口	权重	操作
	健康		80 🎤	10 <mark>/</mark> 编辑	解绑

4.2 在修改端口弹窗中,输入修改后的端口值,单击提交。

• 方式2: 批量修改某些服务器端口。

()	) 说明:
	批量修改端口后的服务器端口相同。

4.1 单击服务器前方复选框,选中多台服务器,在列表上方,单击修改端口。

绑定         修改城口         修改权重         解绑	按照内网IP搜索,	用" "分割关键字	α ¢
✓ ID/名称 端口健康状态() IP地址	端口	权重	操作
✓ 健康	80	10	解绑

4.2 在修改端口弹窗中,输入修改后的端口值,单击提交。

#### 解绑负载均衡后端服务器

负载均衡控制台支持解绑已绑定的后端服务器,接下来将以 "HTTP/HTTPS 监听器"为例(TCP/UDP/TCP SSL 监听器的解绑方 式相同),为您介绍如何解绑已绑定的负载均衡后端服务器。

() 说明:

- 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。
- 如需使用 API 解绑负载均衡后端服务器,请参见 从负载均衡监听器上解绑后端服务 接口说明。


- 1. 登录 负载均衡控制台。
- 2. 在实例管理页面的"负载均衡"页签中,单击目标负载均衡实例右侧操作列的配置监听器。
- 3. 在 HTTP/HTTPS 监听器模块左侧列表中,展开实例与监听器规则,选中 URL 路径 。

— test-http(HTTP:80)		
- 1.1.1.1	默认访问	
——/1.1.21.3		

- 4. 在 HTTP/HTTPS 监听器模块右侧服务器列表中,解绑已绑定的后端服务器。
- 方式1: 单独解绑某台服务器。
  - 4.1 找到需要解绑的服务器,在右侧操作栏,单击**解绑**。

绑定	修改端口修改权重解	绑		按照内网IP搜索,用	]" "分割关键字	Q, Q	¢
	ID/名称	端口健康状态()	IP地址	端口	权重	操作	
		健康		80	10	解绑	

4.2 在解绑弹窗中,确认解绑的服务,单击提交。

• 方式2: 批量解绑某些服务器。

4.1 单击服务器前方复选框,选中多台服务器,在列表上方,单击解绑。

銵	<mark>吃 修改端口 修改权重</mark>	¥绑		按照内网IP搜索,用	" "分割关键字	Q	φ
<b>~</b>	ID/名称	端口健康状态①	IP地址	端口	权重	操作	
~		健康		80	10	解绯	3

4.2 在解绑弹窗中,确认解绑的服务,单击提交。

# 绑定弹性网卡

最近更新时间: 2025-05-23 17:06:12

# 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 弹性网卡控制台,将所需的弹性网卡与云服务器做绑定。

# 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左侧的 + 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。

HTTF #	/HTTPS监听器(已配置1个) 建								
-	test(HTTP:80)	+ 💉 🗓 💿	转发规则详情 展开 マ						
	- www.example.com	默认访问 🧪 🕂	已绑定后端服务						
	/index	ŕ	<b>绑定</b> 修改端口 修	改权重 解绑		按照内网IP搜索,	用" "分割关键字	Q	φ
			ID/名称	端口健康状态()	IP地址	端口	权重	操作	
				监听器创建学	完成,请 <b>绑定后端服务</b>				

- 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"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,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。
- 4. 绑定完毕的配置详情如下。

HTTP/ 新	/HTTPS监听器(已配置1个) 建							
-	test(HTTP:80)	+ 🖍 🗓 💿	转发规则详情 展开 ᢦ					
	- www.example.com	默认访问 🧪 🕂	已绑定后端服务					
	/index	r ū	<b>绑定</b> 修改端口 修改权重	解绑		按照内网IP搜索,	用" "分割关键字	Qφ
			D/名称	端口健康状态①	IP地址	端口	权重	操作
				异常 🟵		66	10	解绑



# 绑定云函数 SCF

最近更新时间: 2025-05-15 17:46:21

您可以通过编写云函数 SCF 来实现 Web 后端服务,然后使用负载均衡 CLB 绑定云函数 SCF 并对外提供服务。

# 背景信息

云函数(Serverless Cloud Function,SCF)是腾讯云为企业和开发者们提供的无服务器执行环境,帮助您在无需购买和管理服 务器的情况下运行代码。在您创建完云函数后,可以通过创建 CLB 触发器将云函数与事件进行关联。CLB 触发器会将请求内容以参数 形式传递给云函数,并将云函数返回作为响应返回给请求方。

# 使用场景

### 通用的 HTTP/HTTPS 接入

适用于电商、社交、工具等 App 应用程序,以及个人博客、活动页面等 Web 应用程序等场景。方案流程如下所示: 1. App、浏览器、H5、小程序等发起 HTTP/HTTPS 请求,通过 CLB 访问 SCF。

- 2. 由 CLB 做证书卸载, SCF 仅需提供 HTTP 服务。
- 3. 请求转给 SCF 后,继续后续处理,例如写入云数据库或调用其他 API。



#### CVM/SCF 平滑切换

适用于 HTTP/HTTPS 服务从 CVM 迁移至 SCF 的场景,以及当 CVM(SCF)服务有问题时,快速迁移至 SCF (CVM)的故障切换场景。方案流程如下所示:

- 1. App、浏览器、H5、小程序等发起 HTTP/HTTPS 请求。
- 2. 通过 DNS 解析将请求解析到 CLB 的 VIP 上。
- 3. 一个 CLB 转发请求给 CVM,另一个 CLB 转发请求给 SCF。
- 4. 客户端无感知,即可完成后端服务在 CVM 和 SCF 之间的平滑切换。

### CVM/SCF 业务分流

适用于秒杀、抢购等场景,使用 SCF 处理高弹性服务、使用 CVM 处理日常业务。

- 1. 通过 DNS 解析将域名 A 解析到其中一个 CLB 的 VIP 上,将域名 B 解析到另外一个 CLB 的VIP 上。
- 2. 其中一个 CLB 转发请求给 CVM,另外一个 CLB 转发请求给 SCF。

### 限制说明

- 仅广州、深圳金融、上海、上海金融、北京、南京、成都、中国香港、新加坡、东京、硅谷、圣保罗、雅加达地域支持绑定 SCF。
- 仅标准账户类型支持绑定 SCF,传统账户类型不支持。建议升级为标准账户类型,详情可参见 账户类型升级说明。
- 传统型负载均衡不支持绑定 SCF。



- 基础网络类型不支持绑定 SCF。
- CLB 默认支持绑定同地域下的所有 SCF,可支持跨 VPC 绑定 SCF,不支持跨地域绑定。
- 目前仅 IPv4、IPv6 NAT64 版本的负载均衡支持绑定 SCF,IPv6 版本的暂不支持。
- 仅七层(HTTP、HTTPS)监听器支持绑定 SCF,四层(TCP、UDP、TCP SSL)监听器和七层 QUIC 监听器不支持。
- CLB 绑定 SCF 仅支持绑定"Event 函数"类型的云函数。
- 同一个 CLB 规则下,只能绑定一个云函数,且不支持与其他类型的后端服务器混绑。
- 当前 CLB 绑定函数的响应 body 最大不能超过 128 kb。

### 前提条件

- 1. 创建负载均衡实例
- 2. 配置 HTTP 监听器 或 配置 HTTPS 监听器

## 操作步骤



### 步骤1: 创建云函数

- 1. 登录 Serverless 控制台,单击左侧导航栏的函数服务。
- 2. 在函数服务页面上方选择期望创建函数的地域和命名空间,并单击新建,进入函数创建流程。如下图所示:

函数服务	🔇 成都	(2) > 命名空间	default		× \$	:	升级套餐	① 购买资	源包		I	函数服务	丐帮助文档 E
<ol> <li>由于AF 如果您</li> </ol>	PI 网关产品 使用的是:	品计划于 2025年6 API 网关基础功能	月30日停止服∮ ,建议改用 <mark>函数</mark>	5,2024年7月1日; ; <mark>URL</mark> ピ,如果您修	起,新老用户不再 使用的是更高阶的能	支持新 皆力,i	ī建API网关触发 请使用 <u>TSE云房</u>	、器,存量触发器 ( <b>生网关</b> ピ,查	客不受影响。2025年 看 <u>迁移指引</u> Ľ	6月30日起, API 网关触发器下线,存量触发器	将不可用	•	< 2 / 2 >
新建	删除	已选中0个函数,	批量删除单次.	上限为10个函数			请选择您要进	进行过滤的标签,	使用并发配额过滤	时可使用">0"、"=128"等方法进行搜索		Q	C @ *
_ 函数名 ↓		函数状态	♡ 监控	函数类型 🕜	运行环境	T	描述		日志配置	最大独占配额① 可配余额:115,200MB	操作		
		⊘ 正常	۵۵	Web函数	Python 3.6				未配置	未配置	复制	<b>牛发管</b> 理	L 删除
		⊘ 正常	۵۵	Event函数	Python 3.6				未配置	未配置	复制	<b>牛发管</b> 理	▮ 删除

- 3. 在新建函数页面,您可以根据实际需求选择创建函数的方式。更多创建细节,请参见创建函数。
  - 模板创建: 通过填写必选的函数名称,使用函数模板中的配置来完成函数的创建。
  - 从头开始:通过填写必填的函数名称、运行环境来完成函数的创建。
  - 使用容器镜像:基于容器镜像来创建函数。详情见 使用镜像部署函数。
- 4. 本文以从头开始为例,配置函数基础信息。
  - 函数类型:接收云 API、多种触发器的 JSON 格式事件触发函数执行。详情见事件函数概述。
  - 函数名称: 函数名称默认填充,可根据需要自行修改。

- 地域: 地域选择与 CLB 实例相同的地域。
- 运行环境:运行环境选择 "Python3.6",可根据需要自行修改。
- **时区:** 云函数内默认使用 UTC 时间,您可以通过配置环境变量 TZ 修改。在您选择时区后,将自动添加对应时区的 TZ 环境变量。
- 5. 在函数代码输入框中输入如下代码。

### ▲ 注意:

腾讯云

CLB 绑定 SCF 时,需按照特定响应集成格式返回,详情请参见 集成响应。



6. 在日志配置中,选择是否开启日志投递。如下图所示:

日志配置	① 开启日志投递后,函数调用日志会默认投递到日志服务 SCF 专用日志主题。腾讯云日志服务CLS为独立计费产品,可能会产生日志服务费用,具体清查看CLS计	费详情 🛛
日志投递	启用 ①	
日志格式	○ 默认格式 ○ 精简格式 ①	

日志投递默认不开启。启用时,可将函数运行日志实时投递到指定位置。详情见日志投递配置。



7. 在高级配置中,您可以根据实际需求对函数进行环境配置、权限配置、层配置、网络配置等,详情见 函数相关配置。

8. 在触发器配置中,选择是否创建触发器。如果您选择"自定义创建",详情见 触发器概述。

9. 单击完成。您可以在 函数服务 中查看已创建的函数。

### 步骤2: 部署云函数

1. 在函数服务页面的列表中,单击刚才创建的函数名。

2. 在函数管理页面,单击函数代码页签,在页签底部单击部署。



← Ib-test 正常					函数服务帮助文
函数管理 函数管理					版本: \$LATEST ▼ 操作 ▼
版本管理 國物研究	函数化和 🖻	管理 吃饭信白	日士本海		
			口心旦问		
触发管理 提交方法②*	在线编辑	执行方法 🕐 🔹 inde	ex.main_handler	运行环境 Python 3.6	Python 3.6 开发数程 🖸 下載 🔻
监控信息 Cloud St	tudio 编辑选择	<sup>奚</sup> 查看 转到 终端	帮助	II 测试模板:Hello Work	d事件模板 🌄 测试 🙃 部署 🔻
	随管理器		🔹 index.py 🛛 🗙	≡ Python - Get Started	□ …
100000 > 打	I开的编辑器		src > 💠 index.py	>	
开方面(初) 部署日志 80 → 10 → 10 → 10 → 10 → 10 → 10 → 10 →	B-TEST	•	1 2 3 4 5 6 7 8 9 10 11	<pre># -*- coding: utf8 -*- import json def main_handler(event, context): return { "isBase64Encoded": False, "statusCode": 200, "headers": {"Content-Type": "body": "<html><body><h1>He } }</h1></body></html></pre>	"text/html"}, llo CLB
<u></u> 二 > 大	纲			i 函数 lb-test 加载完成。	
> Bi Python 3.6.1	1间线 164-bit <u>⊗1∆</u> 0	自动部署:关闭		行1.2	列1 空格:4 LF Python Layout: US _ 🕻
- year sort				10.03	
部署	测试				切换到日版编辑器 使用遇到问题 ⑦

### 步骤3: 绑定云函数

- 1. 登录 负载均衡控制台,在左侧导航栏单击实例管理。
- 2. 在**实例管理**页面的负载均衡页签中,单击目标实例右侧操作列的配置监听器。
- 3. 在 HTTP/HTTPS 监听器列表中,选择需要绑定云函数 SCF 的监听器,分别单击目标监听器左侧的 + 和展开的域名左侧的 +, 然 后选中展开的 URL 路径,单击**绑定**。

HTTP/HTTPS监听器(已配置1个)					
- tes (HTTP:443)	+ 🖌 🖮 💿	转发规则详情 展开 -			
- ww	默认访问,/ +	已绑定后端服务			
-/	× ū	<b>绑定</b> 修改第日	修改权量解绑		按照内网P/撞索,用"分清 Q 🗘
		ID/各称	端口健康状态()	IP地址	端口 权重 操作
			监听器创建完	成,请绑定后端服	务

4. 在弹出的绑定后端服务对话框中,目标类型选择云函数 SCF,选择命名空间、函数名和版本/别名,设置权重后,单击确认。



绑定后端服务	5						×
目标类型①	○ 实例 ○	IP类型 🔵 云函数SCF					
命名空间		函数名		版本/别名		权重 🕄	
de	Ŧ	lb-	Ŧ	版本 🔻 \$LATEST	Ŧ	- 10 +	删除
				<b>确认</b> 取消			

5. 返回监听器管理页签,在转发规则详情区域显示负载均衡已绑定的云函数,即已创建 CLB 触发器。

专发规则详情 展开 ▼					
却定后端服务					
绑定修改函数	修改权重	解绑		按照内网IF	>捜索,用" "分割 Q 🗘
命名空间	函数名	端口健康状态()	版本/别名	权重	操作
default	hello-clb	健康	版本:\$LATEST	10	修改 解绑

器。

2、在绑定 SCF 时,响应 body 大小有 128k 限制。如果超过了这个限制,CLB 会响应客户端 403 错误码。

# 结果验证

1. 若使用公网 CLB 绑定云函数,且 IP 模式为固定 IP,可以通过 CLB 实例的 VIP 和端口访问云函数。若显示 Hello CLB,则说明 云函数已成功部署。



2. 若使用公网 CLB 绑定云函数,且 IP 模式为动态 IP,可以通过 CLB 实例的域名和端口访问云函数。若显示 Hello CLB,则说明 云函数已成功部署。



← → C S lb-, ..., er fw.clb.ap-, ..., centclb.com/

# Hello CLB

3. 若使用内网 CLB 绑定云函数,可以通过与 CLB 实例同一 VPC 的云服务器访问云函数。若显示 Hello CLB,则说明云函数已成 功部署。



# 相关文档

创建 SCF 函数

# 🔗 腾讯云

# 跨地域绑定2.0(新版)

最近更新时间: 2025-04-0110:09:32

负载均衡(CLB)支持通过云联网,跨地域绑定后端服务器,允许客户选取多个后端服务器的地域,跨 VPC、跨地域绑定后端服务 器。

目前该功能处于内测阶段,如果您需要体验该功能,请提交 内测申请。

## 应用场景

- 满足 P2P 等游戏业务中,多地同服的场景。客户后端服务集群在广州,客户希望在上海、北京等多地创建 CLB,绑定相同的广州 后端服务集群。起到游戏加速、流量收敛的作用,有效保证数据传输质量,降低时延。
- 2. 满足金融业务支付、订单付款等场景,有效保证关键业务的数据传输质量,保证数据一致性。



## 与旧版跨地域绑定的区别

对比项	跨地域绑定2.0(新版)	跨地域绑定1.0(旧版)
是否支持同时绑定多地域内 服务	支持: ● 新版跨地域绑定 CLB 支持同时绑定多个地域的 CVM。 ● 例如北京的 CLB 可以同时绑定北京和上海的 CVM。	不支持: • 旧版跨地域绑定 CLB 仅能绑定一 个地域的 CVM。 • 例如北京的 CLB 可以绑定上海的 CVM,但北京的 CLB 不能同时 绑定北京和上海的 CVM。
是否支持跨域后改回不跨域	支持:新版跨地域绑定支持修改回原来的同地域绑 定。	不支持:旧版跨地域绑定修改后端实 例地域属性后,如该地域和 CLB 地 域不同,将无法修改回原来的同地域 绑定。



支持 CLB 类型	支持公网 CLB 和内网 CLB。	支持公网 CLB。
CVM 释放时 CLB 是否自 动解绑	同地域绑定时自动解绑: • CLB 绑定同地域的 CVM,若该 CVM 被释 放,则 CLB 会自动与该 CVM 解绑。 跨地域绑定时自动解绑: • CLB 跨地域绑定 CVM,若该 CVM 被释放, 则 CLB 不会自动解除与该 CVM 的绑定关系, 需手动解绑	同地域绑定时自动解绑: • CLB 绑定同地域的 CVM,若该 CVM 被释放,则 CLB 会自动与 该 CVM 解绑。 跨地域绑定时自动解绑: • CLB 跨地域绑定 CVM,若该 CVM 被释放,则 CLB 会自动与 该 CVM 解绑。
价格是否优惠	通过 <del>云联网计费</del> ,会进行精细化成本核算,价格更 低。	日95计费。

## 限制条件

- 跨网互联绑定后端服务器暂不支持传统型负载均衡。
- 该功能仅标准账户类型支持。若您无法确定账户类型,请参见 判断账户类型。
- 仅 VPC 支持,基础网络不支持。
- 不支持负载均衡实例的 VPC 网段和后端服务的 VPC 网段重叠,否则会绑定失败。
- IPv4 和 IPv6 NAT64 版本的负载均衡实例支持该功能。IPv6 版本的实例需开启双栈混绑功能,开启后七层监听器可以同时绑定
   IPv4 和 IPv6 的后端服务器,当七层监听器混绑 IPv4 IP 时,支持跨地域绑定2.0和混合云部署。IPv6 版本的实例绑定 IPv6 的 后端服务器时,不支持跨地域绑定2.0和混合云部署。
- 跨地域绑定2.0和混合云部署,不支持 安全组默认放通,请在后端服务器上放通 Client IP 和服务端口。
- 跨地域绑定2.0和混合云部署不支持绑定其它负载均衡实例(即不支持 CLB 绑定 CLB )。
- 四七层监听器均支持获取客户端 IP,四层负载均衡在后端 CVM 上获取的源 IP 即为客户端 IP,七层负载均衡需通过 X-Forwarded-For 或 remote\_addr 字段获取客户端 IP。详情请参见 绑定云上 IP 场景下获取客户端真实 IP。

# 前提条件

- 1. 已提交内测申请,跨地域绑定请通过 内测申请,跨境绑定请进行 商务申请。
- 2. 已创建负载均衡实例,详情请参见 创建负载均衡实例。
- 3. 已创建云联网实例,详情请参见 新建云联网实例。
- 4. 将需要绑定的目标 VPC 关联至已创建的云联网实例,详情请参见 关联网络实例。

# 操作步骤

- 1. 登录 负载均衡控制台。
- 2. 在**实例管理**页面左上角选择地域,在实例列表找到目标实例,单击实例 ID。
- 3. 在"基本信息"页面的"后端服务"区域,单击点击配置绑定非本 VPC 的内网 IP。



		人類的時代
基本信息监	听器管理 重定向配置 监控 安全组	
基本信息		访问日志 (七层)
名称	LB, mar /	仅七层监听器(HTTP/HTTPS)支持配置访问日志(Access Log),四层监听器(TCP/UDP/TCP SSL)不支持
ID	ibiliti - dīj	日志服务CLS① 未开启 🖌
状态	正常	10万二日士福久(n) 04-16方は書士日 24-18-16-16-16-1-16-1-18-16-16-1
域名		第二十二十二十二十二十二十二十二十二十二十二十二十二十二十二十二十二十二十二十
VIP	12	
实例类型	公网	后诸服务
地域	ГĦ	提供跨网互联股务,如下2种策略只能二选一
可用区	́тм=в	- 静地域概定1.0, CLB 可以跨地域规定某一 VPC 内的云服务器, 点击配置 特地域概定3.0, CLB 可以跨地域规定某一 VPC 内的云服务器, 点击配置
运营商	BGP (多线)	- FRAMEWEZ V, OLD PIKAWEZ IS YFO, Z PIUC VIP, MUSCH
所属网络	b man and an	
支持获取Client IP①	支持	
所属项目	默认项目	
标签	1	
删除保护	未开启 开启删除保护	
域名防护状态()	未信用 前往Web应用防火墙(WAF)了躺洋情	

4. 在弹出的"打开启用非本 VPC 内 IP"对话框中,单击提交。

打开启用非本VPC内IP	×
启用后,CLB 支持绑定非本 VPC 的内网 IP。	
提交关闭	

5. 在"基本信息"页面的"后端服务"区域查看到"启用非本 VPC 内 IP"开关已开启,表示可以绑定云上 IP。

后端服务	
提供跨网互联服务,如下2种策略只能二选一	
- 跨地域绑定1.0,CLB 可以跨地域绑定某一 VPC 内的云服务器 ,点击配置	
- 跨地域绑定2.0,CLB 可以绑定云上多 VPC、云下 IDC 内 IP,(已经配置)	
- 跨地域绑定2.0和混合云部署,不支持安全组默认放通,请在后端服务器上放通 Client IP 和服务端口。	
启用非本VPC内IP	
新增SNAT IP	

- 6. 在实例详情页面,单击"监听器管理"页签,在配置监听器模块中,为负载均衡实例绑定后端服务,详情请参见 添加负载均衡后端 云服务器 。
- 7. 在弹出的"绑定后端服务"对话框中,选择"其他 VPC",单击**云服务器**,选择需要关联的云服务器(可多选),并填写相关云服 务器需要被转发的端口与权重,详情请参见 服务器常用端口,单击**确认**。



8. 返回"已绑定后端服务"区域可以查看已绑定的其他地域的 CVM。

已绑定 绑定	后端服务 修改院正 修改院董 解绑			按照内网	IP搜索, 用" "	分害 Q 🗘
	ID/各称	端口健康状态①	IP地址	端口	权重	操作
	ins	健康	43. <b>Junior</b> 1997	31631	10	解绑
	ins	健康	111 (公)	31631	10	解绑

# 相关文档

跨地域绑定计费说明

# 跨地域绑定1.0(旧版)

最近更新时间: 2024-12-02 16:45:22

当前,公网负载均衡已支持跨地域绑定云服务器,允许客户选取其他某个地域的云服务器,跨 VPC、跨地域绑定后端云服务器。如果 您需要体验该功能,境内跨地域绑定请通过 工单申请,境外跨地域绑定请进行 商务申请 。

### () 说明:

腾讯云

- 跨地域绑定云服务器暂不支持内网负载均衡和传统型负载均衡。
- 传统账户类型仅网络计费模式为共享带宽包的负载均衡实例支持跨地域绑定1.0功能。

### 应用场景

- 满足 P2P 等游戏业务中,多地同服的场景。客户后端服务集群在广州,客户希望在上海、北京等多地创建 CLB,绑定相同的广州 后端服务集群。起到游戏加速、流量收敛的作用,有效保证数据传输质量,降低时延。
- 2. 满足金融业务支付、订单付款等场景,有效保证关键业务的数据传输质量,保证数据一致性。



### 操作步骤

- 1. 登录 负载均衡控制台。
- 2. 在实例详情页面找到目标负载均衡实例,单击实例 ID。
- 3. 在基本信息页面的后端服务模块,单击跨地域绑定1.0后的点击配置,修改后端云服务器的地域及网络属性。

()	说明:			
	如果公网负载均衡已经绑定了同地域的云服务器,	切换地域时需要先解绑您的云服务器,	详情请参考	解绑负载均衡后端服
	务器。			



#### to sugget a prior to be a set of the set of

← Ib-	here and the second second second	负载均衡帮助文档区
基本信息	听器管理 重定向配置 监控 安全组	
甘土作白		
基本信息		<b>汾</b> 问日志(て辰)
名称	cis-	仅七层监听器(HTTP/HTTPS)支持配置访问日志(Access Log),四层监听器(TCP/UDP/TCP SSL)不
ID	1b-1	支持
状态	正常	日志服务CLS① 未开启 ✔
域名	-	腾讯云日志服务CLS为独立计费产品,计费标准请参见CLS计费并情℃
VIP	151	
实例类型	公网	
地域	ГM	后端服务
可用区	广州五区	提供跨网互联服务,如下2种策略只能二选一
运营商	BGP (多线)	- 跨球磁時走1.0, CLB 可以跨地域時定录一 VPC 内的云影号器 (点击部度) - 跨地域規定2.0, CLB 可以規定云上多 VPC、云下 IDC 内 IP, 点击配置
所属网络	yu ana ana ana ana ana ana ana ana ana an	
支持获取Client IP()	支持	
所属项目	默认项目	
标签	A shared of the second second of	
删除保护	未开启 开启删除保护	
域名防护状态①	未启用 前往Web应用防火墙(WAF)了解详情	

4. 在弹出的修改后端服务配置对话框的后端服务地域列表和后端服务网络列表中选择所需地域和网络,并单击提交。

### () 说明:

- 当前负载均衡仅能绑定一个地域的云服务器,例如,北京的 CLB 可以绑定上海的 CVM,但是北京的 CLB 不能同时绑 定北京和上海的 CVM。
- 当您修改后端实例服务属性后,如该地域和 CLB 地域不同,将无法修改回原来的同地域绑定。
- 当前暂不允许同地域跨 VPC 绑定负载均衡和云服务器。
- 支持跨基础网络和 VPC 的场景。
- 跨域绑定产生的带宽费用将按天结算,使用带宽峰值阶梯计费,详情请参见 跨地域绑定计费说明 。



修改后端服务配置	×
温馨提示:当您修改后端实例地域属性时,如该地域和CLB地域不同,将无法修改回同地域绑定。 需求请提工单申请。了解更多	,后续
LB地域 广州	
LB所属网络 Defa	
后端服务地域 上海 ▼	
后端服务网络 基础网络 🔻	
费用 申请方按当日实际使用带宽峰值阶梯计费,按天结算计费详情	
提交关闭	

# 计费说明

跨地域绑定的功能通过跨域对等连接的原理实现,计费详情请参见 计费说明。



# 混合云部署

最近更新时间: 2025-05-23 17:06:12

在混合云部署的场景中,可以使用负载均衡直接绑定云下本地数据中心(IDC)内 IP,实现跨 VPC 与 IDC 之间的后端服务器的绑 定。

目前该功能处于内测阶段,如果您需要体验该功能,境内跨地域绑定请提交 内测申请,境外跨地域绑定请提交 商务申请。

## 方案优势

- 快速搭建混合云,无缝连接云上云下,负载均衡可将请求同时转发至云上 VPC 内服务器和云下 IDC 机房内云服务器。
- 复用腾讯云的高质量公网接入能力。
- 复用腾讯云负载均衡的丰富功能特性,例如四/七层接入、健康检查、会话保持等。
- 内网通过 云联网 互通,支持精细化选路保障质量。



# 限制说明

- 跨地域绑定2.0暂不支持传统型负载均衡。
- 该功能仅标准账户类型支持。若您无法确定账户类型,请参见 判断账户类型。
- 仅 VPC 支持,基础网络不支持。



- IPv4 和 IPv6 NAT64 版本的负载均衡实例支持该功能。IPv6 版本的实例需开启双栈混绑功能,开启后七层监听器可以同时绑定
   IPv4 和 IPv6 的后端服务器,当七层监听器混绑 IPv4 IP 时,支持跨地域绑定2.0和混合云部署。IPv6 版本的实例绑定 IPv6 的 后端服务器时,不支持跨地域绑定2.0和混合云部署。
- 跨地域绑定2.0和混合云部署,不支持安全组默认放通,请在后端服务器上放通 Client IP 和服务端口。
- 跨地域绑定2.0和混合云部署不支持绑定其它负载均衡实例(即不支持 CLB 绑定 CLB )。
- 目前仅广州、上海、济南、杭州、合肥、北京、天津、成都、重庆、南京、武汉、北京金融、上海金融、中国香港、新加坡、硅谷、 法兰克福、圣保罗地域支持该功能。
- TCP SSL 监听器需在 RS 上通过通用 TOA 获取源 IP,详情请参见 混合云部署场景下通过 TOA 获取客户端真实 IP 。
- HTTP 和 HTTPS 监听器需通过 X−Forwarded−For (XFF) 获取源 IP。
- TCP 和 UDP 监听器支持通过 ProxyProtocol 协议携带客户端源地址到后端服务器。

### 前提条件

- 1. 已提交内测申请,境内跨地域绑定请通过 内测申请,境外跨地域绑定请进行 商务申请。
- 2. 已创建负载均衡实例,详情请参见 创建负载均衡实例。
- 3. 已创建云联网实例,详情请参见新建云联网实例。
- 4. 将与 IDC 关联的专线网关和需要绑定的目标 VPC 关联至已创建的云联网实例,详情请参见 关联网络实例。

## 操作步骤

- 1. 登录 负载均衡控制台。
- 2. 在负载均衡实例管理页面找到目标负载均衡实例,单击实例 ID。
- 3. 在基本信息页面的"后端服务"区域,单击点击配置绑定非本 VPC 的内网 IP。

← lb-nsm6u	084 (lijianhong)	负载均衡帮助文档已
基本信息	监听器管理 重定向配置 监控 安全组	
<b>基本信息</b> 名称 ID 状态 域名	9 ≠ 14 ℃ 正常	访问日志(七层) 仅七层监听器(HTTP/HTTPS)支持配置访问日志(Access Log),四层监听器(TCP/UDP/TCP SSL)不支持 日志服务CLS① 未开启 ♪ 腾讯云日志服务CLS为独立计贯产品,计贯标准请参见CLS计费详情区
VIP		
网络类型	公网 广州	后端服务
可用区网络出口	广州 中心出口-	提供跨网互联服务,如下2种策略只能二选一 - 跨地域域定1.0,CLB可以跨地域频定某一VPC内的云服务器,点击配置 - 跨地域域定2.0,CLB可以绑定五上多 VPC、云下 IDC内 IP, <u>点击配置</u> - 跨地域域定2.01和CLB可以绑定五上多 VPC、云下 IDC内 IP, <u>点击配置</u>
运营商	BGP (多线)	- 『ジルሚがみと2.040) 応言立即者,个文が文主共和NADX通,時位/6項服务容上/DX通 Ullent IP 和服务施口。

4. 在弹出的打开启用非本 VPC 内 IP 对话框中,单击提交。

打开启用非本VPC内IP	×	
启用后, CLB 支持绑定非本 VPC 的内网 IP。		
提交关闭		

5. 在基本信息页面的"后端服务"区域,单击新增 SNAT IP。

### 后端服务

提供跨网互联服务,如下2种策略只能二选一

- 跨地域绑定1.0,CLB 可以跨地域绑定某一 VPC 内的云服务器 , 点击配置
- 跨地域绑定2.0, CLB 可以绑定云上多 VPC、云下 IDC 内 IP, (已经配置)
- 跨地域绑定2.0和混合云部署,不支持安全组默认放通,请在后端服务器上放通 Client IP 和服务端口。



### 新增SNAT IP

6. 在弹出的新增 SNAT IP 对话框中,选择"子网",单击新增分配 IP,最后单击保存。

### () 说明:

- SNAT IP 主要用于混合云部署中将请求转发至 IDC 内服务器的场景,使用负载均衡绑定云联网打通的 IDC 内 IP 时, 必须分配 SNAT IP。SNAT IP 是您的 VPC 的内网 IP。
- 单个 CLB 实例最多支持配置10个 SNAT IP。
- 单个 CLB 实例的单个规则配置单个 SNAT IP,绑定单个后端服务后的连接数最大是5.5万个,若增加 SNAT IP 或增加后端服务时,连接数等比例增加。例如1个 CLB 实例配置了2个 SNAT IP,后端绑定了10个端口,此时该 CLB 实例总的连接数是: 2 x 10 x 5.5万 = 110万个。您可以根据连接数来评估 SNAT IP 的分配个数。
- 删除 SNAT IP 时,该 SNAT IP 上的连接会全部断开,请谨慎操作。



 7. 在实例详情页面,单击监听器管理页签,在配置监听器模块中,为负载均衡实例绑定后端服务,详情请参见添加负载均衡后端云服 务器。

8. 在弹出的**绑定后端服务**对话框中,选择"IP类型",单击**添加内网 IP**,输入需绑定的 IDC 内网 IP 地址,并填写端口与权重,详 情请参见 服务器常用端口,最后单击确认。



绑定后端服务			×
目标类型 ①			
i)注意:绑定内网IP支持绑定云联网关联的跨VPC、跨地域绑定后端云服	务器,但不支持将CLB实例作为	后端IP绑定。	
IP	端口	权重()	
仅支持ipv4地址	1-65535	- 10 +	添加端口删除
仅支持ipv4地址	1-65535	- 10 +	添加端口 删除
添加内网IP	确认取消		
返回 <b>已绑定后端服务</b> 区域可以查看已绑定的 IDC 的内网 IF	<b>D</b> °		
已绑定后端服务			
<b>郑定</b> 修改端口 修改权重 解绑		按照内网IP	搜索,用" "分割关键字 🛛 🗘

ID/名称	网络	端口健康状态(;)	IP地址	端口	权重	操作
	其他网络	探测中	(内)	88	10	解绑

# 相关文档

9.

跨地域绑定2.0(新版)

# 后端云服务器的安全组配置

最近更新时间: 2023-10-30 16:23:31

# 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。有关更多信息,请参阅 安全组操作指南。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:
  - 对于内网负载均衡(原"应用型内网负载均衡"),如果您的 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);如果您的 CLB 属于基础网络,无需在后端 CVM 的安全组上配置,默认放通健康检查 IP。
  - 对于传统型内网负载均衡,如果实例创建于2016年12月5日前且网络类型为 VPC 网络,则需要在后端 CVM 的安全组上放通 CLB 的 VIP(用作健康检查);其他类型的传统型内网 CLB 无需在后端 CVM 的安全组上配置,默认放通健康检查 IP。

# 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。若您在 CLB 上也配置了安全组,请参见 配置负载均衡安全组 来配 置 CLB 上的安全组规则。

• 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
0.0.0.0/0 + 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:

### 0.0.0.0/0 + 8080 allow

### • 应用场景 3:

内网负载均衡(原"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。

a. 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
0.0.0.0/0 + 8080 drop
```

b. 用作 Client 的服务器安全组出站规则配置如下:

CLB VIP + 8080 allow 0.0.0.0/0 + 8080 drop

### • 应用场景 4:

在2016年12月5日之后,新购的 VPC 网络类型的传统型内网负载均衡,CVM 安全组仅需放通 Client IP(无需放通 CLB 的 VIP,默认放通健康检查 IP)。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。 a. 后端服务器安全组入站规则配置如下:

```
ClientA IP + 8080 allow
ClientB IP + 8080 allow
0.0.0.0/0 + 8080 drop
```

b. 用作 Client 的服务器安全组出站规则配置如下:

CLB VIP + 8080 allow 0.0.0.0/0 + 8080 drop

### • 应用场景 5: 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:

- 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。
- 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。

## 使用云 API 管理后端服务器安全组

请参考 绑定安全组接口 和 解绑安全组接口。



最近更新时间: 2025-05-23 17:06:12

负载均衡通过健康检查来判断后端服务的可用性,避免后端服务异常影响前端业务,从而提高业务整体可用性。

- 开启健康检查后,无论后端服务器权重是多少(包括权重为0),负载均衡实例都会进行健康检查。您可在实例列表页面的"健康状态"列查看健康检查状态,或者在监听器的绑定后端服务详情页面查看健康检查状态。
  - 当后端服务器实例被判定为异常后,负载均衡实例自动将新的请求转发给其他正常的后端服务器,而不会转发到异常的后端服务器。
  - 当异常实例恢复正常后,负载均衡将其恢复至负载均衡服务中,重新转发请求给此实例。
  - 若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器。
- 关闭健康检查,负载均衡将向所有后端服务器转发流量(包括异常的后端服务器),因此强烈建议您打开健康检查,允许负载均衡帮您自动检查并移除异常的后端服务器。
- 默认被动健康检查,针对四层 TCP SSL 监听器、七层 HTTP/HTTPS 监听器,将默认配置被动健康检查能力(默认开启,不支持关闭)。CLB 向后端服务转发流量的同时并记录后端服务的健康状态。若转发失败则重试将流量转发至其他后端服务上,同时累计此后端服务失败次数1次,累计失败达到3次,则屏蔽该后端服务10秒,屏蔽时间结束后,恢复流量转发并继续记录后端服务的健康状态。

# 健康检查状态

## 单监听器健康检查状态说明

根据健康检查探测情况,后端服务器的健康检查状态如下所示:

状态	说明	是否转发流量
探测 中	新绑定的后端服务器在检查间隔 × 健康阈值时间内的状态,例如,检查 间隔2s,健康阈值3次,则是6s 内 的状态。	CLB 不向处于"探测中"的后端服务转发流量。
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。	<ul> <li>CLB不向"异常"的后端服务转发流量。</li> <li>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权重非 0 的后端服务。</li> </ul>
已关 闭	关闭健康检查。	CLB 向所有后端服务转发流量。

## 列表页健康检查状态说明

根据实例下所有监听器的健康探测情况综合展示。

状态	说明
正常	● 该实例下所有监听器的后端服务正常。



	• 该实例下所有监听器的健康检查均未开启。
异常	该实例下任意一个监听器异常,则展示为异常。
未配置	<ul> <li>该实例未配置任何监听器/规则。</li> <li>该实例下任意一个监听器未绑定后端服务,且不存在异常的监听器。</li> </ul>

# TCP 健康检查

针对四层 TCP 监听器,您可以配置 TCP 健康检查,通过 SYN 包即发起 TCP 三次握手来获取后端服务器的状态信息。您还可以通 过自定义协议的请求内容和返回结果来获取后端服务器的状态信息。



TCP 健康检查机制如下:

- 1. 负载均衡向后端服务器 (内网 IP 地址+健康检查端口)发送 SYN 连接请求报文。
- 2. 后端服务器收到 SYN 请求报文后,若相应端口处于正常监听状态,则会返回 SYN+ACK 响应报文。
- 若在响应超时时间内,负载均衡收到后端服务器返回的 SYN+ACK 响应报文,则表示服务运行正常,判定健康检查成功,并向后 端服务器发送 RST 复位报文中断 TCP 连接。
- 4. 若在响应超时时间内,负载均衡未收到后端服务器返回的 SYN+ACK 响应报文,则表示服务运行异常,判定健康检查失败,并向 后端服务器发送 RST 复位报文中断 TCP 连接。

# UDP 健康检查

针对四层 UDP 监听器,您可以配置 Ping 探测和自定义探测。若您选择了 Ping 探测方式,则只是用 ICMP ECHO 报文进行探测。





### 健康检查机制如下:

- 1. 负载均衡向后端服务器的内网 IP 地址发起 Ping 命令;
- 2. 若 Ping 成功,则表示服务正常,判定健康检查成功;
- 3. 若 Ping 失败,则表示服务异常,判定健康检查失败;

#### ▲ 注意:

- 健康检查依赖 ICMP 协议,需要后端服务器开放回复 ICMP 包 (支持 Ping );
- 如果后端服务器是 Linux 服务器,在大并发场景下,由于 Linux 有防 ICMP 攻击保护机制,会限制服务器发送
   ICMP 的速度,这种情况下可能导致最终后端服务的真实状态与健康检查不一致。
- 解决方案:在配置 UDP 健康检查时,配置自定义输入和输出,向后端服务器发送您指定的字符串,且 CLB 收到您指定的应答后才判断健康检查成功。此方案依赖后端服务器,后端服务器需处理健康检查输入并返回指定输出。

#### 若您选择了自定义探测方式,则可以细分为以下两种情况:

• 第一种,如果仅配置"检查请求"的内容,没有配置"检查返回结果",则使用 ICMP ECHO 报文+ UDP 探测报文。



### 健康检查机制如下:



- 3.1 负载均衡向后端服务器的内网 IP 地址发起 Ping 命令;
- 3.2 负载均衡向后端服务器(内网 IP 地址+健康检查端口)发送 UDP 探测报文;
- 3.3 若 Ping 成功,且在响应超时时间内,后端服务器未返回 port XX unreachable 的报错信息,则表示服务正常,判定健康 检查成功;
- 3.4 若 Ping 失败,或者在响应超时时间内,系统收到后端服务器返回的 port XX unreachable 报错信息,则表示服务异常, 判定健康检查失败;

▲ 注意:

- 健康检查依赖 ICMP 协议,需要后端服务器开放回复 ICMP 包(支持 Ping )、开放回复 ICMP 端口不可达包 (支持探测端口)。
- 如果后端服务器是 Linux 服务器,在大并发场景下,由于 Linux 有防 ICMP 攻击保护机制,会限制服务器发送 ICMP 的速度。此时,即使后端服务已经出现异常,但由于无法向 CLB 返回 port XX unreachable, CLB 由于没收到 ICMP 应答进而判定健康检查成功,最终导致后端服务的真实状态与健康检查不一致。
   解决方案:在配置 UDP 健康检查时,配置自定义输入和输出,向后端服务器发送您指定的字符串,且 CLB 收到 您指定的应答后才判断健康检查成功。此方案依赖后端服务器,后端服务器需处理健康检查输入并返回指定输出。
- 第二种,如果同时配置了"检查请求"和"检查返回结果"的内容,则仅使用 UDP 探测报文,判断 RS 健康状态的条件为:收到 UDP 返回的报文,且与"检查返回结果"的内容匹配。



健康检查机制如下:

3.1 负载均衡向后端服务器(内网 IP 地址 + 健康检查端口)发送 UDP 探测报文;

3.2 若收到 UDP 返回的报文,且与"检查返回结果"的内容匹配,则表示服务正常,判定健康检查成功;

3.3 若在响应超时时间内,未收到 UDP 返回的报文或与"检查返回结果"的内容未匹配,则表示服务异常,判定健康检查失败;

## HTTP 健康检查

针对四层 TCP 监听器和七层 HTTP/HTTPS 监听器,您可以配置 HTTP 健康检查,通过发送 HTTP 请求来获取后端服务器的状态 信息。





HTTP 健康检查机制如下:

- 1. 负载均衡根据健康检查配置,向后端服务器(内网 IP 地址+健康检查端口+检查路径)发送 HTTP 请求(可选择设置检查域名)。
- 2. 后端服务器收到请求后返回相应的 HTTP 状态码。
- 若在响应超时时间内,负载均衡收到了后端服务器返回的 HTTP 状态码,若与设置的 HTTP 状态码匹配成功,则判定健康检查成功,反之则判定健康检查失败。
- 4. 若在响应超时时间内,负载均衡未收到后端服务器的响应,则判定健康检查失败。

### () 说明:

- 针对七层 HTTPS 监听器,当 HTTPS 监听器的转发规则中的后端协议选择 HTTP 时,健康检查使用 HTTP 健康检查;当选择 HTTPS 时,健康检查使用 HTTPS 健康检查。
- HTTPS 健康检查与HTTP 基本类似,不同的是 HTTPS 健康检查是通过发送 HTTPS 请求,根据返回的 HTTPS 状态码判断后端服务器的状态信息。

## 健康检查时间窗

负载均衡的健康检查机制有效提高了业务的可用性。为了避免频繁的健康检查失败引起的切换对系统可用性的冲击,健康检查只有在健 康检查时间窗内连续多次检查成功或失败后,才会进行健康或异常的状态切换。健康检查时间窗由以下因素决定:

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: 2 – 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,控制台显示为失 败。 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,控制台显示为成 功。 可配置范围:2 – 10次。	3次

四层健康检查时间窗的计算方法如下:

### () 说明:

- 响应超时时间要小于检查间隔时间。
- 四层健康检查,即TCP健康检查或UDP健康检查,无论检查成功还是响应超时,前后两次之间发包的检查间隔都是已设置的检查间隔。

- 🔗 腾讯云
  - 健康检查失败时间窗 = 检查间隔 × (不健康阈值 − 1)

下图以健康检查响应超时时间为2s,检查间隔为5s,不健康阈值为3次为例,健康检查失败时间窗 = 5 x (3-1) = 10s。



健康检查成功时间窗 = 检查间隔 × (健康阈值 - 1)
 下图以健康检查成功响应时间为1s,检查间隔为5s,健康阈值为3次为例,健康检查成功时间窗 = 5 x (3-1) = 10s。



### 七层健康检查时间窗的计算方法如下:

健康检查失败时间窗 = 响应超时时间 × 不健康阈值 + 检查间隔 × (不健康阈值 - 1)
 下图以健康检查响应超时时间为2s,检查间隔为5s,不健康阈值为3次为例,健康检查失败时间窗 = 2 x 3 + 5 x (3-1) = 16s。



健康检查成功时间窗 = 健康检查成功响应时间 × 健康阈值 + 检查间隔 × (健康阈值 - 1)
 下图以健康检查成功响应时间为1s,检查间隔为5s,健康阈值为3次为例,健康检查成功时间窗 = 1 x 3 + 5 x (3-1) = 13s。



## 健康检查探测标识

在 CLB 开启健康检查后,后端服务器除接收正常的业务请求外,还会接收到健康检查探测请求。健康检查探测请求有如下标识:

- 健康检查探测请求的源 IP 是 CLB 的 VIP 或 100.64.0.0/10 网段。
- 四层(TCP、UDP、TCP SSL)监听器的健康检查方式若为自定义,且检查请求为空,则默认请求中会带"HEALTH CHECK"标识。
- 七层(HTTP、HTTPS)监听器的健康检查请求 Header 中的 user-agent 为 "clb-healthcheck"。

### 🕛 说明:

- 传统型内网负载均衡,健康检查源 IP 为 169.254.128.0/17 网段。
- 基础网络内网负载均衡,健康检查源 IP 为服务器物理 IP。

# 相关文档

- 配置健康检查
- 配置健康检查日志



- 配置告警策略
- 健康检查异常排查

# 配置健康检查

最近更新时间: 2025-05-23 17:06:12

您可以在配置监听器时开启健康检查功能来判断后端服务的可用性。健康检查详情请参见 健康检查概述 。

### 限制说明

- IPv6 版本的负载均衡的 TCP 监听器不支持 HTTP 健康检查和自定义方式健康检查。
- IPv6 版本的负载均衡的 UDP 监听器不支持自定义方式的健康检查。

## 前提条件

- 1. 您已创建负载均衡实例,详情请参见 创建负载均衡实例 。
- 2. 您已创建负载均衡监听器。
- 创建 TCP 监听器,详情请参见 配置 TCP 监听器 。
- 创建 UDP 监听器,详情请参见 配置 UDP 监听器。
- 创建 TCP SSL 监听器,详情请参见 配置 TCP SSL 监听器。
- 创建 HTTP 监听器,详情请参见 配置 HTTP 监听器。
- 创建 HTTPS 监听器,详情请参见 配置 HTTPS 监听器。

# TCP 监听器

四层 TCP 监听器支持四层 TCP、七层 HTTP 和自定义方式三种类型的健康检查。

- TCP 健康检查通过 SYN 包即发起 TCP 三次握手来获取后端服务器的状态信息。
- HTTP 健康检查通过发送 HTTP 请求来获取后端服务器的状态信息。
- 自定义健康检查通过自定义应用层协议的输入和输出内容来获取后端服务器的状态信息。

### 配置 TCP 健康检查

- 1. 参考前提条件,操作至健康检查页签。
- 2. 在健康检查页签,选择"TCP"检查方式。



创建监听器	×
✓ 基本配置	2 健康检查 3 会话保持
健康检查	帮助您自动检查并移除异常的后端服务器。
健康探测源IP()	100.64.0.0/10网段(推荐) 负载均衡VIP 无需在后端服务器的安全组中配置针对该网段的放通策略,但若在后端服务器上配置有 iptables等其他安全策略时,务必放通健康探测源 IP,否则将导致健康探测异常。
检查方式	O TCP ○ HTTP ○ 自定义
检查端口	默认为后端服务器端口,除非您希望指定特定端口,否则建议留空

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服务器端口。
健康探测源 IP	健康检查探测包的源 IP,默认为 100.64.0.0/10 网段,使用该网段可以有效避免地址冲突。存量用户可 选负载均衡的 VIP 作为健康探测的源 IP,也可通过自助工具一键切换为 100.64.0.0/10 网段,详情请 参见 健康探测源 IP 诊断助手。
检查方式	选择"TCP"表示配置 TCP 健康检查。
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。
显示高级选 项	详情请参见 <u>高级选项</u> 。

# 配置 HTTP 健康检查

- 1. 参考 前提条件,操作至**健康检查**页签。
- 2. 在健康检查页签,选择"HTTP"检查方式。



创建监听器	×
✓ 基本配置	> <b>2 健康检查</b> > 3 会话保持
健康检查	帮助您自动检查并移除异常的后端服务器。
健康探测源IP()	100.64.0.0/10网段(推荐) 负载均衡VIP 无需在后端服务器的安全组中配置针对该网段的放通策略,但若在后端服务器上配置有 iptables等其他安全策略时,务必放通健康探测源 IP,否则将导致健康探测异常。
检查方式	○ TCP ○ HTTP ○ 自定义
检查端口	默认为后端服务器端口,除非您希望指定特定端口,否则建议留空
检查域名	选填,建议配置
检查路径	只支持字母、数字、'-'、'.',默认无Host字段 /
HTTP请求方式()	GET *
HTTP版本①	HTTP/1.1 T
正常状态码①	✓ http_1xx ✓ http_2xx ✓ http_3xx ✓ http_4xx 🗌 http_5xx
	当状态码为http_1xx、http_2xx、http_3xx、http_4xx时,认为后端服务器存活 显示高级选项 ▼
	上一步下一步

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服务器端口。
健康探测源 IP	健康检查探测包的源 IP,默认为 100.64.0.0/10 网段,使用该网段可以有效避免地址冲突。存量用户 可选负载均衡的 VIP 作为健康探测的源 IP,也可通过自助工具一键切换为 100.64.0.0/10 网段,详情 请参见 健康探测源 IP 诊断助手。
检查方式	选择"HTTP"表示配置 HTTP 健康检查。
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。
检查域名	健康检查域名: ● 长度限制: 1 - 80个字符。

▶ 腾讯云			负载均
		<ul> <li>默认为转发域名。</li> <li>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: 名。</li> <li>支持的字符集为: a-z 0-9。</li> </ul>	域
	检查路径	健康检查路径: • 长度限制: 1 – 80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/=?。	
	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,对应的后服务需支持 HEAD。 • 若使用 GET 方法,则后端服务支持 GET 即可。	言端
	HTTP 版本	后端服务的 HTTP 版本。 • 若后端服务器支持的 HTTP 版本为1.0,则无需校验请求的 Host 字段,即无需配置检查域名。 • 若后端服务器支持的 HTTP 版本为1.1,则需要校验请求的 Host 字段,即需要配置检查域名。 说明:当选择 HTTP /1.1 版本时,此时若未配置检查域名,按照 HTTP 标准协议,后端服务器会返 400错误码,提示健康检查异常,建议勾选正常状态码http_4xx。	回
	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。	
	显示高级选项	详情请参见 高级选项 。	

# 配置自定义健康检查

1. 参考 前提条件,操作至**健康检查**页签。

2. 在健康检查页签,选择"自定义"检查方式。



创建监听器	×
✓ 基本配置	> <b>2 健康检查</b> > 3 会话保持
建康检查	
	帮助您自动检查并移除异常的后端服务器。
建康探测源IP()	○ 100.64.0.0/10网段(推荐) ○ 负载均衡VIP
	无需在后端服务器的安全组中配置针对该网段的放通策略,但若在后端服务器上配置有 iptables等其他安全策略时,务必放通健康探测源 IP, <mark>否则将导致健康探测异常。</mark>
检查方式	○ TCP ○ HTTP ○ 自定义
检查端口	默认为后端服务器端口,除非您希望指定特定端口,否则建议留空
输入格式	文本 💌
	只允许ASCII可见字符
检查请求 🔁 *	最大长度限制为500个字符
№亘巡凹站未(j)*	最大长度限制为500个字符
	显示高级选项 🗸
	上一步下一步

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服务器端口。
健康探测源 IP	健康检查探测包的源 IP,默认为 100.64.0.0/10 网段,使用该网段可以有效避免地址冲突。存量用户可选 负载均衡的 VIP 作为健康探测的源 IP,也可通过自助工具一键切换为 100.64.0.0/10 网段,详情请参见 健康探测源 IP 诊断助手。
检查方式	选择"自定义"表示配置自定义协议健康检查。
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。 <ul> <li>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。</li> <li>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。</li> </ul>
检查请求	自定义健康检查请求内容,必填。例如探测 DNS 服务的检查请求示例为: F13E0100000100000000000000377777047465737403636F6D0774656E63656E740363 6F6D0000010001。
检查返回结	自定义健康检查请求时,必须填写健康检查返回结果。例如探测 DNS 服务的检查返回结果示例为:F13E。


果	
显示高级选 项	详情请参见 <mark>高级选项</mark> 。

## UDP 监听器

UDP 支持的健康检查类型为自定义和 PING 两种检查类型。

### 配置自定义健康检查

- 1. 参考 前提条件,操作至**健康检查**页签。
- 2. 在健康检查页签,选择"自定义"检查方式。

创建监听器	$\times$
✓ 基本配置	2 健康检查 > 3 会话保持
健康检查	帮助您自动检查并移除异常的后端服务器。
健康探测源IP()	100.64.0.0/10网段(推荐) 负载均衡VIP 无需在后端服务器的安全组中配置针对该网段的放通策略,但若在后端服务器上配置有 iptables等其他安全策略时,务必放通健康探测源 IP,否则将导致健康探测异常。
检查方式	● 自定义 ○ PING
检查端口	默认为后端服务器端口,除非您希望指定特定端口,否则建议留空
输入格式	文本 🔻
检查请求()	只允许ASCII可见字符 最大长度限制为500个字符
检查返回结果()	最大长度限制为500个字符
	显示高级选项 🚽
	上一步下一步

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服务器端口。
健康探测源 IP	健康检查探测包的源 IP,默认为 100.64.0.0/10 网段,使用该网段可以有效避免地址冲突。存量用户可选 负载均衡的 VIP 作为健康探测的源 IP,也可通过自助工具一键切换为 100.64.0.0/10 网段,详情请参见 健康探测源 IP 诊断助手。



检查方式	选择"自定义"表示健康探测源 IP 向后端服务器发送 UDP 探测报文来获取后端服务器的状态信息。
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。 <ul> <li>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。</li> <li>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。</li> </ul>
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: F13E01000001000000000000377777047465737403636F6D0774656E63656E740363 6F6D0000010001。
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。
显示高级选 项	<mark>详情请参见 高级选项</mark> 。

## 配置 PING 健康检查

- 1. 参考 前提条件,操作至**健康检查**页签。
- 2. 在健康检查页签,选择"PING"检查方式。

创建监听器		×
✓ 基本配置	> <b>2 健康检查</b> > <b>3</b> 会话保持	
健康检查	帮助您自动检查并移除异常的后端服务器。	
健康探测源IP()	100.64.0.0/10网段(推荐) 负载均衡VIP 无需在后端服务器的安全组中配置针对该网段的放通策略,但若在后端服务器上配置有 iptables等其他安全策略时,务必放通健康探测源 IP,否则将导致健康探测异常。	
检查方式	○ 自定义 ○ PING	
	显示高级选项 🗸	
	上一步下一步	

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服务器端口。
健康探测源 IP	健康检查探测包的源 IP,默认为 100.64.0.0/10 网段,使用该网段可以有效避免地址冲突。存量用户可 选负载均衡的 VIP 作为健康探测的源 IP,也可通过自助工具一键切换为 100.64.0.0/10 网段,详情请 参见 健康探测源 IP 诊断助手。
检查方式	选择"PING"表示通过 Ping 后端服务器的 IP 地址来获取后端服务器的状态信息。









检查方式	选择"TCP"表示配置 TCP 健康检查。
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。
显示高级选 项	详情请参见 高级选项 。

## 配置 HTTP 健康检查

- 1. 参考 前提条件,操作至**健康检查**页签。
- 2. 在健康检查页签,选择"HTTP"检查方式。



腾讯云

エーダ トー ツ

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服务器端口。
健康探测源 IP	健康检查探测包的源 IP,默认为 100.64.0.0/10 网段,使用该网段可以有效避免地址冲突。存量用户 可选负载均衡的 VIP 作为健康探测的源 IP,也可通过自助工具一键切换为 100.64.0.0/10 网段,详情 请参见 健康探测源 IP 诊断助手。
检查方式	选择"HTTP"表示配置 HTTP 健康检查。
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。
检查域名	健康检查域名: <ul> <li>长度限制: 1 - 80个字符。</li> <li>默认为转发域名。</li> <li>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。</li> <li>支持的字符集为: a-z 0-9。</li> </ul>
检查路径	健康检查路径: • 长度限制: 1 – 80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/=?。
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。
HTTP 版本	后端服务的 HTTP 版本,仅支持 HTTP1.1 版本。后端服务需要校验请求的 Host 字段,即需要配置检查 域名。 <b>说明</b> :若未配置检查域名,按照 HTTP 标准协议,后端服务器会返回400错误码,提示健康检查异常,建 议勾选正常状态码http_4xx。
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。
显示高级选项	详情请参见 <mark>高级选项</mark> 。

## HTTP 监听器

🕥 腾讯云

#### 配置 HTTP 健康检查

- 1. 参考 前提条件,操作至**健康检查**页签。
- 2. 在健康检查页签,选择"HTTP"检查方式。



腾讯云

$\mathcal{O}$	腾讯云	负载均
	HTTP状态码	B检测 ✓ http_1xx ✓ http_2xx ✓ http_3xx ✓ http_4xx □ http_5xx 当状态码为http_1xx、http_2xx、http_3xx、http_4xx时,认为后端服务器存活 上一步 下一步
	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服务器端口。
	健康探测 源 IP	健康检查探测包的源 IP,默认为 100.64.0.0/10 网段,使用该网段可以有效避免地址冲突。存量用户可选 负载均衡的 VIP 作为健康探测的源 IP,也可通过自助工具一键切换为 100.64.0.0/10 网段,详情请参见 健康探测源 IP 诊断助手。
	检查方式	选择"HTTP"表示配置 HTTP 健康检查。
	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。
	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。
	检查路径	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/=?。
	响应超时	<ul> <li>健康检查响应的最大超时时间。</li> <li>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。</li> <li>可配置范围: 2 - 60秒。</li> </ul>
	检测间隔	<ul> <li> 负载均衡进行健康检查的时间间隔。</li> <li> 可配置范围: 2 - 300秒。</li> </ul>
	不健康阈 值	<ul> <li>• 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。</li> <li>● 可配置范围: 2 - 10次。</li> </ul>
	健康阈值	<ul> <li>• 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。</li> <li>● 可配置范围: 2 - 10次。</li> </ul>
	HTTP 请 求方式	健康检查的 HTTP 请求方式,可选:GET 或 HEAD,默认为 GET。 <ul> <li>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。</li> </ul>

负载均衡



	● 若使用 GET 方法,则后端服务支持 GET 即可。
正常状态	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、
码	http_3xx、http_4xx 和 http_5xx。

### 配置 TCP 健康检查

- 1. 参考前提条件,操作至健康检查页签。
- 2. 在健康检查页签,选择"TCP"检查方式。



腾讯云



	器端口。
健康源探测 IP	健康检查探测包的源 IP,默认为 100.64.0.0/10 网段,使用该网段可以有效避免地址冲 突。存量用户可选负载均衡的 VIP 作为健康探测的源 IP,也可通过自助工具一键切换为 100.64.0.0/10 网段,详情请参见 健康探测源 IP 诊断助手。
检查方式	选择"TCP"表示配置 TCP 健康检查。
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。
显示高级选项	详情请参见 <mark>高级选项</mark> 。

## HTTPS 监听器

#### () 说明:

当 HTTPS 监听器转发规则中的后端协议选择 HTTP 协议时,健康检查使用 HTTP 健康检查;当选择 HTTPS 协议时,健 康检查使用 HTTPS 健康检查。

HTTPS 监听器的健康检查配置参考以上的 HTTP 监听器 的健康检查即可。

#### 高级选项

健康检查配置	说明	默认 值
响应超时	<ul> <li>健康检查响应的最大超时时间。</li> <li>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。</li> <li>可配置范围: 2 - 60秒。</li> </ul>	2秒
检测间隔	<ul> <li>负载均衡进行健康检查的时间间隔。</li> <li>可配置范围: 2 - 300秒。</li> </ul>	5秒
不健康阈值	<ul> <li>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。</li> <li>可配置范围: 2 - 10次。</li> </ul>	3次
健康阈值	<ul> <li>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。</li> <li>可配置范围: 2 - 10次。</li> </ul>	3次

## 相关文档

- 健康检查概述
- 配置告警策略

# 健康探测源 IP 支持100.64.0.0/10网段

最近更新时间: 2025-05-23 17:06:12

本文介绍如何将 CLB 健康探测的源 IP 由 CLB 的虚拟服务地址(VIP)设置为 100.64.0.0/10 网段( 100.64.0.0/10 是腾讯 云的保留地址,其他用户无法分配到该网段内,不存在安全风险),本文以 TCP 监听器为例。

### 使用场景

- 1. 收敛后端服务器安全组
- 1. 健康探测源 IP 收敛为 100.64.0.0/10 网段。
- 2. 解决自建 Kubernetes 集群内网回环问题
- 3. K8s 服务需要同时对集群内和集群外暴露。其中集群内通过集群内部负载均衡(IPVS)实现,集群外通过内网负载均衡 CLB 实现。IPVS 会把内网 CLB 的 IP 地址绑定在本地的一个接口上,这样集群内访问内网 CLB 的地址实际上用的是集群内的 IPVS 负载均衡。
- 4. 而在容器服务 TKE 中,内网 CLB 使用了 CLB 的 VIP 地址作为健康探测源 IP,这与原生的 K8s 实现方式 IPVS 绑定的地址冲 突,导致内网 CLB 健康检查失败。
- 5. 设置健康探测源 IP 为 100.64.0.0/10 网段,可以避免地址冲突,解决健康检查失败问题。

#### 处理步骤

1. 登录 负载均衡控制台。

- 2. 在**实例管理**页面左上角选择地域,在实例列表中找到目标实例,在操作列单击配置监听器。
- 3. 在**监听器管理**页签,找到目标监听器,单击监听器右侧的 **♪**图标编辑监听器。
- 4. 在弹出的编辑监听器对话框中,单击下一步至健康检查页签。
- 5. 在健康检查页签中,健康检查源 IP 选择 100.64.0.0/10 网段,单击下一步后再单击提交。

编辑监听器	
✓ 基本配置	2 健康检查 3 会话保持
健康检查	不可能不可能不可能不可能不可能不可能不可能不可能不可能不可能不可能不可能不可能不
健康探测源IP()	100.64.0.0/10网段(推荐) 负载均衡VIP 无需在后端服务器的安全组中配置针对该网段的放通策略,但若在后端服务器上配置有 iptables等其他安全策略时,务必放通健康探测源 IP, 否则将导致健康探测异常。
检查方式	<b>○</b> ТСР ○ НТТР ○ 自定义
检查端口	默认为后端服务器端口,除非您希望指定特定端口,否则建议留空
	显示高级选项 🗸
	上一步下一步

## 热点问题

#### 将健康探测源 IP 切换为100.64.0.0/10网段有什么优势?

- 健康探测源 IP 使用 100.64.0.0/10 网段时,您无需在后端服务器的安全组中额外针对该网段配置放行策略。若在后端服务器中 配置 iptables 等其他安全策略,请务必放通该网段,否则将会导致健康探测失败。
- 收敛后端服务器的安全策略统一为 100.64.0.0/10 网段。
- 100.64.0.0/10 网段是腾讯云内部地址,用户无法分配到该网段,不会存在地址冲突问题。

#### 使用100.64.0.0/10网段作为健康探测源 IP 时,是固定的一个 IP 吗?

是 100.64.0.0/10 网段中的某个指定 IP 作为探测 IP,并不是一个固定的 IP。

#### 相关文档

- 配置健康检查
- 健康检查探测标识

## 健康探测源 IP 诊断助手

最近更新时间: 2025-05-23 17:06:12

本文介绍如何快速诊断账号下 CLB 实例的健康探测源 IP 是否使用了100.64.0.0/10网段。通过该自助工具,还可以一键完成健康探测的源 IP 由 CLB 的虚拟服务地址(VIP)切换为100.64.0.0/10网段操作。

### 使用场景

对健康探测源 IP 进行诊断,快速诊断账号下 CLB 实例的健康探测源 IP 是否使用了100.64.0.0/10网段并支持一键切换。

()	说明:		
	建议先选择1-2个实例,	进行诊断和切换用于功能验证,	然后再批量操作。

#### 处理步骤

- 1. 登录 负载均衡控制台。
- 2. 在左侧导航栏选择自助助手 > 健康探测源 IP 诊断。
- 3. 在页面顶部选择地域,并单击开始诊断。
- 4. 在健康探测源 IP 诊断页面,选择目标实例后,并单击开始诊断。
- 5. 诊断完成后,展示诊断结果。
- 若目标实例中,没有使用 CLB 的虚拟服务地址( VIP )作为健康探测源 IP,则如下图所示。

健康探测源 IP 诊断	×
诊断已完成,无异常	
没有健康探测源 IP 为负载均衡 VIP 的监听器/规则。	
我知道了	

若目标实例中,有使用 CLB 的虚拟服务地址(VIP)作为健康探测源 IP,则如下图所示。此时单击一键切换可快速完成健康探测的源 IP 由 CLB 的虚拟服务地址(VIP)切换为100.64.0.0/10网段操作。

健康探测源 IP 诊断 X		
() 诊断已完成,存在异常		
健康探测源 IP 为负载均衡 VIP 的监听器/规则		
实例 ID	监听SS	7层监听器规则
lb	tcp:80	1
共 1 条		10 ▼ 条/页 🛛 🖌 1 /1页 🕨 网
使用 100.64.0.0/10 网段作为健康探测源 IP,可以有效避免地址冲突,解决健康检查失败问题。 注意:需要在后端服务器上配置的安全策略中放通 100.64 网段,否则会导致健康探测异常。 一般现换 取消		



## 其他操作

#### 诊断报告状态说明

状态信息	状态说明
正常 – 无需切换	该次诊断的 CLB 实例中,没有实例的健康探测源 IP 是该实例的虚拟服务地址(VIP)。
正常 – 切换已完成	该次诊断的 CLB 实例中,有实例的健康探测源 IP 是该实例的虚拟服务地址(VIP),且已完成将健 康探测源 IP 切换为100.64.0.0/10网段的操作。
警告 - 未切换	该次诊断的 CLB 实例中,有实例的健康探测源 IP 是该实例的虚拟服务地址(VIP ),且未完成切 换,建议及时操作。

#### 查看诊断报告

- 1. 登录 负载均衡控制台。
- 2. 在左侧导航栏选择自助助手 > 健康探测源 IP 诊断。
- 3. 在页面顶部选择地域后可查看对应地域的诊断报告信息。
- 4. 单击操作列中的查看报告,可查看历史诊断报告中的详细信息。

报告ID	诊断状态	诊断时间	操作
jes galances	正常-无需切换	2023-04-20 11:09:00	宣看报告 删除
jc	警告-未切换	2023-04-20 11:09:32	宣看报告 删除

#### 删除诊断报告

- 1. 登录 负载均衡控制台。
- 2. 在左侧导航栏选择自助助手 > 健康探测源 IP 诊断。
- 3. 在页面顶部选择地域后可查看对应地域的诊断报告信息。
- 4. 单击操作列中的删除,在弹出的确定删除对话框中,单击确定,即可删除历史诊断报告。

## 相关文档

- 配置健康检查
- 健康检查探测标识
- 健康探测源 IP 支持100.64.0.0/10网段

## 证书管理

## 管理证书

最近更新时间: 2025-05-15 17:46:21

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 。

#### 证书类型

负载均衡支持的证书类型包括:国际标准证书(RSA/ECC)、国密标准证书(SM2)。证书加密算法具体内容可查看 RSA 加密算法 与 ECC 加密算法的区别、国密标准证书(SM2)介绍 。

#### () 说明:

HTTPS 监听器的 SSL 解析中的服务器证书支持配置双证书,即两种不同加密算法类型的证书,详情请参见 配置 HTTPS 监听器 。

收听出来到	证书类型	证书认证方式	
监听器尖空		单向认证	双向认证
	RSA、ECC、SM2 单证书配置	支持	支持
LITTDO	RSA 和 ECC 双证书配置	支持	支持
ппго	RSA 和 SM2 双证书配置	支持	不支持
	ECC 和 SM2 双证书配置	支持	不支持
TCP_SSL、 QUIC	RSA、ECC 单证书配置	支持	支持
TCP、UDP、 HTTP		不支持配置证书	

#### 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。

#### 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:

证书更新后立即生效,系统不会删除旧证书,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。

腾讯云

- 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. 在弹出的更新证书对话框中,填写新证书的证书内容和密钥内容,并单击确定。

更新证书		×
更新方式	推荐 更新证书 上传新证书	
当前证书		
新证书		
	所有使用该证书的负载均衡实例将会自动更新为新证书,请谨慎核对。	
	确定取消	

## 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 ID	test
证书类型	服务器证书
加密算法	ECC 256
证书内容 已关联负载均衡	BEGIN CERTIFICATE 复制 验 1b- 1b- 1b- 1b- 1b- 1b- 1b- 1b-
主域名	the second se
备用域名	
上传时间	2022-11-09 21:57:09
启用时间	2022-09-15 22:35:23
\+++0n+)51	



## 申请证书

最近更新时间: 2025-05-15 17:46:21

### 注册账号

腾讯云平台申请证书首先需要注册腾讯云账号并且完成实名认证。

- 1. 新用户请单击 腾讯云官网 右上角的免费注册,进入注册页面。
- 2. 请您 注册腾讯云账号,即可登录 腾讯云控制台。
- 3. 完成 实名认证,方可继续申请证书。

#### 申请免费证书

#### () 说明:

- 免费证书仅提供二级域名及其子域名证书申请,不支持 IP 与泛域名申请。例如 dnspod.cn 、 docs.dnspod.cn 。
- 亚洲诚信范围内(不一定在腾讯云申请)的同一主域最多只能申请20张免费证书,申请时请注意该域名是否在其他服务商
   平台存在亚洲诚信下的证书,避免申请达到上限无法申请。更多详情请参见免费证书名额相关问题。
- 免费证书到期后如需继续使用证书,请重新申请并安装。
- 1. 登录腾讯云控制台,进入我的证书管理页面,并在免费证书页签单击申请免费证书。
- 2. 在证书对比界面单击**申请免费证书,**填写证书申请表单,如下图所示:



证书部题       □田33 / J J SOK         □ 世书明或正常过期24/时后、全帮放占用免费证书的强度免费证书超度说明 2         □ 计研究定笔 •       □ 項写中「望名,例如tencent.com         □ 出市でに、Comの円臨送www.tencent.com,不包含sstiencent.com,需要管理语: 」如果你定定望名 (例如 'tencent.com) 或者绑定户,请购定付置证书,前往购空         ■ 本物住連名操析平台添加 ● 会和DNS验证 ● 白DDNS验证 ● 文件验证         □ 子动DNS验证 ● 白DDNS验证 ● 文件验证         □ 日本市住連名操析平台添加 ● 会解析记录 (不影响速名使用),证书意发成功后即可删除记录         □ 日本市住連名操作平台添加 ● 会解析记录 (不影响速名使用),证书意发成功后即可删除记录         □ 日のて         □ 計算「可應想」 2024年4月25日起。 勝讯云新室发的免疫证予有效期调整为900天,第略生效 前申请的证书有效期仍为12个月、关于免费证书策略通道         □ DigCert Global Root G2         □ 2025年1月14日15時認念费证书的供证书由 USERTrust RSA Certification Authority调整为 DigCert Global Root G2 查 算计情 2         ■ Analy 通道整件的供证书由 USERTrust RSA Certification Authority调整为 DigCert Global Root G2 查 算计情 2         ■ Analy 通道整件的研究 (1) 「如果」 DigCert Global Root G2 查 算计情 2         ■ Analy 通道報告:       ● SATUR (1) ● Comment (1) ●	1 提交证书申	3 <b>请 〉 2</b> 验证域名
	证书额度	已用3张 / 共50张
田井朝定城名・     可慎写单个域名、例如tencent.com     Unipercent.com     Unipercent.com     Unipercent.com     Unipercent.com     Unipercent.com     Set		证书吊销或正常过期24小时后,会释放占用免费证书的额度免费证书额度说明 <sup>12</sup>
Interest com只屬送www.tencent.com,不包含sil.tencent.com,屬单独申請: 如齋那定这場名(例如*tencent.com)或者绑定P。请购买付费证书,前往购买         基名德证方式。       ● 予动DNS验证 ● 自动DNS验证 ● 文件验证         王动韵往域名解析平台添加一条解析记录(不影响域名使用),证书室发成功后即可删除记录         正书有效期       90天         提起「商通知,2024年4月26日起,顯讯云新签发的免费证书有效期调整为90天,策略生效前申请的证书有效期仍为12个月。关于免费证书前处需要通知[2]         配证书信息       DiglCert Global Root G2         2025年1月14日15时起免费证书的根证书由 USERTrust RSA Certification Authority调整为 DiglCert Global Root G2         2025年1月14日15时起免费证书前根证书由 USERTrust RSA Certification Authority调整为 DiglCert Global Root G2         路透着信息         解放送着和客户编的漆客管性略词、了解更多         正容者注意(选纲)         「「」」」         如用"静心证书音注名,不能超过200字         正书者注名(选纲)         」「」」         为了保障私期安全,目前 不支持密码规定,请勿填写私的密码, 如需需要预讯云负载均衡、CDN等云服,请勿如写私的密码, 如需要要预讯云负载均衡、CDN等云服,请勿填写私的密码, 如需要要预讯云负载均衡、CDN等云服, 请勿填写私的密码, 如需需要预讯云负载均衡、CDN等云服务,请勿填写私的密码, 可加量预制示云负载均衡、CDN等云服务, 请勿填写私的密码, 確如       」         建文申请, 进行域名。例如, tencent.com 、ssl.tencent.com 。         或全       上方域名。例如, tencent.com 、ssl.tencent.com 。         或金融正方式:       ● 自动阶为如 DNS。	正书绑定域名 *	请填写单个域名,例如tencent.com
ARABUTASION OF FUDDNS验证 ● BUDNS验证 ○ 文件验证 FUDDNS验证 ● BUDNS验证 ○ 文件验证 FUDDNS验证 ● BUDNS验证 ○ 文件验证 FUDDNS验证 ● SUDDNS验证 ● SUDDNS验证 ○ 文件验证 FUDDNS验证 ● SUDDNS验证 ● SUDDNS验证 ○ 文件验证 FUDDNS验证 ● SUDDNS验证 ● SUDDNS ● S		tencent.com只赠送www.tencent.com,不包含ssl.tencent.com,需单独申请; 如需绑定泛域名(例如 *.tencent.com)或者绑定IP,请购买付费证书。 <mark>前往购买</mark>
F动前往域名解析平台添加一条解析记录(不影响域名使用),证书签发成功后即可删除记录             E书有效期        90天             提到「商通知、2024年4月25日起、餐讯无新答发的免费证书有效期调整为90天、策略生效         前申请的证书有效期仍为12个月。关于免费证书策略调整通知                和歌音》             跟证书信息        DigiCert Global Root G2           2025年1月14日15时起免费证书的根证书由 USERTrust RSA Certification Authority调整为         DigiCert Global Root G2 <b>宣看详情 G</b> 器           Piscaff           Conschaff             BK达择           Conschaff           Conschaff             BK达择           Conschaff           Conschaff             BK达择           Conschaff           Bosary          DigiCert Global Root G2         Conschaff             BK达择           Conschaff           Conschaff             BK达择           Conschaff           Bosary             BSA           Tert            Tert             Agen           Sen为it           Midel和 Bogita             Conschaff           Sen           Sen             Agen           Sen           Sen              Sen	或名验证方式 *	● 手动DNS验证    自动DNS验证①    文件验证
中市湖山、2024年4月25日起、勝讯云新签发的免费证书有效期调整为90天、策略生效前申请的证书有效期仍为12个月、关于免费证书策略调整通知口         短江书信息       DigiCert Global Root G2         2025年1月14日15时起免费或证书的根证书由 USERTrust RSA Certification Authority调整为DigiCert Global Root G2畫看详情已         密等信息          電話描       ● RSA貫法 ④●         RE法选择       ● RSA貫法 ④●         REAd对浏览器和電子端的兼容性更好,但对网站服务器的性能开销更大:ECC加密效率更高,服务器性能开销小但兼容性略弱。了解更多         日本語社名(法規)		手动前往域名解析平台添加一条解析记录(不影响域名使用),证书签发成功后即可删除记录
<ul> <li>提到厂商通知, 2024年4月25日起, 腾讯云新釜发的免费证书效期调整为90天, 策略生效前申请的证书有效期仍为12个月。关于免费证书算路调整通知 C</li> <li>R证书信息 DigiCet Global Root G2 2025年1月14日15时起免费证书的根证书由 USERTrust RSA Certification Authority调整为 DigiCet Global Root G2 查看详情 C</li> <li>RSA劳动览器和客广端的兼容性更好,但对网站服务器的性能开销更大; ECC加密效率更高,服务器性能开销/U电器管性感弱。了解更多</li> <li>I书备注名(选辑) 请输入证书备注名,不能超过200字</li> <li>公纳密码(选填)</li></ul>	E书有效期	90天
Burt #fall       DigiCert Global Root G2         2025年1月14日15时起免费证书的根证书由 USERTrust RSA Certification Authority调整为 DigiCert Global Root G2查看详情 C         WE ##       ● RSA算法 (任命)         RSA对浏览器和客户端的兼容性更好,但对网站服务器的性能开销更大; ECC加密效率更高,服务器 性能开销小但兼容性略弱。了解更多         E书备注名(选填)       请输入证书备注名,不能超过200字         此书备注名(选填)       请输入证书备注名,不能超过200字         此都密碍(选填)		接到厂商通知,2024年4月25日起,腾讯云新签发的免费证书有效期调整为90天,策略生效 前申请的证书有效期仍为12个月。 <b>关于免费证书策略调整通知 [2</b>
2025年1月14日15时起免费证书的根证书由 USERTrust RSA Certification Authority调整为 DigiCert Global Root G2查看详情 G AS等信息 < FK选择 ORA算法 (197) RSA对波宽器和客户端的兼容性更好,但对网站服务器的性能开销更大; ECC加密效率更高,服务器 性能开销小但兼容性路弱。了解更多 FK等 注意 (法编) · · · · · · · · · · · · · · · · · · ·	<b>录证书信息</b>	DigiCert Global Root G2
AGG PER A C A SA PER (PE) Rokady (PE) Ro		2025年1月14日15时起免费证书的根证书由 USERTrust RSA Certification Authority调整为 DigiCert Global Root G2 <b>查看详情                                    </b>
諸法择       ● RSA算法 ④●         SASATJ浏览器和客户端的兼容性更好,但对网站服务器的性能开销更大;ECC加密效率更高,服务器 性能开销小但兼容性略弱。了解更多         正书备注名(选填)       · · · · · · · · · · · · · · · · · · ·	示签等信息 へ	
RSA对浏览器和客户端的兼容性更好,但对网站服务器的性能开销更大;ECC加密效率更高,服务器性能开销小但兼容性路弱。了解更多         E书备注名(选填)       请输入证书备注名,不能超过200字         (3)       请输入证书备注名,不能超过200字         (3)       方保障私钥安全,目前不支持密码找回功能,请您牢记私钥密码。         力了保障私钥安全,目前不支持密码找回功能,请您牢记私钥密码。       力了保障私钥安全,目前不支持密码找回功能,请您牢记私钥密码。         如需都署勝讯云负载均衡、CDN等云服务,请勿填写私钥密码。       什么是私钥密码[2]         (法)       「标签键」」       「你签值」         小常都會選び       「「你签值」」       ③         (法)       「「」       「「」         (3)       健值粘贴板       「         (面)       「」」       「」」         (3)       健值粘贴板       「         (3)       健值粘贴板       「         (4)       「」」       「」         (法)       「」」」       」         (3)       健值粘贴板       「         (3)       疑個利表       「         (4)       「       」         (3)       近回列表       」         (4)       「       」         (5)       说明:       」         (1)       小       」         (2)       法       」       」         (3)       近 (1)       」       」         (4)       「       」         (5)       」 <td>「法选择</td> <td>○ RSA算法 推荐</td>	「法选择	○ RSA算法 推荐
田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田		RSA对浏览器和客户端的兼容性更好,但对网站服务器的性能开销更大;ECC加密效率更高,服务器 性能开销小但兼容性略弱。 <b>了解更多</b>
Adffræme (选填) 为了保障私钥安全,目前不支持密码找回功能,请您牢记私钥密码。 加需部署腾讯云负载均衡、CDN等云服务,请勿填写私钥密码。什么是私钥密码 ID 标签键	亚书备注名(选填)	请输入证书备注名,不能超过200字
为了保障私钥安全,目前不支持密码找回功能,请您牢记私钥密码。 如需部署腾讯云负载均衡、CDN等云服务,请勿填写私钥密码。什么是私钥密码 2         孫密       标签键         小签键       标签值         • 添加       ③ 键值粘贴板         『旗项目       >         建文申请,进行域名验证       返回列表         近书绑定域名:       请填写单个域名。例如       tencent.com、sl.tencent.com。         • 说明:       • 自动DNS验证: 验证方法请参见 自动添加 DNS。	仏钥密码(选填)	
☆ 标签键		为了保障私钥安全,目前 不支持密码找回 功能,请您牢记私钥密码。 如需部署腾讯云负载均衡、CDN等云服务,请勿填写私钥密码 。 <b>什么是私钥密码                                    </b>
+ 添加 ③ 键值粘贴板          」	云签	标签键
▲ 展项目 账认项目 ~   提交申请,进行域名验证 返回列表 <b>证书绑定域名:</b> 请填写单个域名。例如 tencent.com、ssl.tencent.com。 <b>域名验证方式:</b> ① 说明:   ● 自动DNS验证: 验证方法请参见 自动添加 DNS。		+ 添加 ③ 键值粘贴板
提交申请,进行域名验证 逐回列表 <b>证书绑定域名:</b> 请填写单个域名。例如 tencent.com、ssl.tencent.com。 域名验证方式: ① 说明: • 自动DNS验证: 验证方法请参见 自动添加 DNS。	斤属项目	默认项目 ~
握交申请,进行域名验证 <b>证书绑定域名:</b> 请填写单个域名。例如 tencent.com 、 ssl.tencent.com 。 域名验证方式: ① 说明: • 自动DNS验证:验证方法请参见 自动添加 DNS 。		
<ul> <li>证书绑定域名:请填写单个域名。例如 tencent.com 、 ssl.tencent.com 。</li> <li>域名验证方式:</li> <li>① 说明: <ul> <li>自动DNS验证:验证方法请参见 自动添加 DNS 。</li> </ul> </li> </ul>	提交申请,进行	· 域名验证
<b>域名验证方式:</b>	证书绑定域名	:请填写单个域名。例如 tencent.com 、 ssl.tencent.com 。
① <b>说明:</b> ● 自动DNS验证:验证方法请参见 自动添加 DNS 。	域名验证方式	:
● 目动DNS验证:验证方法请参见 目动添加 DNS 。	() 说明:	
	• 自云	DNS验证:验证方法请参见 自动添加 DNS 。

- 手动DNS验证:验证方法请参见 DNS 验证。
- 文件验证:验证方法请参见 文件验证。



- 算法选择: 默认加密算法为RSA算法。加密算法具体内容请参见 RSA 加密算法与 ECC 加密算法的区别?
- 证书备注名: 可选,请输入证书的备注名称,不可超过200字。
- 私钥密码:可选,为了保障私钥安全,目前不支持密码找回功能,请您牢记私钥密码。

```
⚠ 注意:
如需部署腾讯云负载均衡、CDN 等云服务,请勿填写私钥密码。
```

○ 标签:请选择您的标签键和标签值,方便您管理腾讯云已有的资源分类。

```
    说明:
如需添加标签,请参见 管理标签。
```

- **所属项目**:请选择您证书所属项目,方便您通过项目管理您的证书。
- 3. 根据验证操作提示,完成域名身份验证,并单击完成。如下图所示:

<b>~</b>	提交证书申请 〉 2 验证域名		
1	<b>您需要手动为域名添加一条解析记录</b> 请前往域名 ■ 对应的DNS服务商为域名添加如下解析记录。查看操作指	6]	
	主机记录 记录类型 记录值		
	D TXT		
	<b>验证</b> 请在 <b>3天内</b> 完成DNS解析记录的添加,否则审核将会失败 证书签发后才可以删除或者更改该解析记录		
2	验证DNS解析信息是否填写正确 如果您已经为域名	检查解析信息是否正确被添加。	
	验证域名 重新选择验证方式 借审		
3	证书签发后,您还需要将证书部署到云资源上,方可开启HTTPS}	服务。	
	部署证书至云资源 • 一键部署云资源 <sup>[2]</sup> 在腾讯云的云资源上,如CDN、CLB、轻量服务器 • 手动部署 <sup>[2]</sup> 在非腾讯云的云资源上	升级为正式证书,可享受以下权益 <ul> <li>自动续费 亿 无需每年手动购买</li> <li>证书托管 亿 不再因为证书更换/续费而重新部署</li> </ul>	选购证书

4. 域名验证通过后,CA 机构将在24小时内完成签发证书操作,请您耐心等待。

注意:
 提交域名未通过 CA 机构安全审核,具体原因请参见 安全审核失败原因。

### 下载和部署

完成域名审核后,颁发的证书即可单击**下载**到本地进行安装部署或部署到腾讯云相关云服务上。相关操作请参见如何选择 SSL 证书安 装部署类型?

## 相关问题

- 免费 SSL 证书名额相关问题
- SSL 证书配置的 TXT 解析是否可以删除?



- 忘记私钥密码怎么办?
- 免费 SSL 证书一直在待验证怎么办?

# 证书要求及转换证书格式

最近更新时间: 2025-05-15 17:46:21

本文为您介绍 SSL 证书要求及证书格式转换说明。

## 常用证书申请流程

**1. 使用 OpenSSL 工具 在本地生成私钥文件, 其中** privateKey.pem 为您的私钥文件, 请妥善保管。

openssl genrsa -out privateKey.pem 2048

2. 使用 OpenSSL 工具 生成证书请求文件,其中 server.csr 是您的证书请求文件,可用于申请证书。

ppenssl req -new -key privateKey.pem -out server.csr

3. 获取证书请求文件中的内容前往 CA 等机构站点申请证书。

## 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:



#### ----BEGIN CERTIFICATE----

MIIE+TCCA+GgAwIBAgIQU306HIX4KsioTW1s2A2krTANBgkqhkiG9w0BAQUFADCB tTELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDl2lcmlTaWduLCBJbmMuMR8wHQYDVQL ExZWZXJpU2lnbiBUcnVzdCB0ZXR3b3JrMTsw0QYDVQQLEzJUZXJtcyBvZiB1c2Ug YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL3JwYSoAYykw0TEvMC06A1UEAxMm VmVyaVNpZ24gQ2xhc3MgMyBTZWN1cmUgU2VydmVyIENBIC0gRzIwHhcNMTAxMDA4 MDAwMDAwWhcNMTMxMDA3MjM10TUSWjBqMQswCQYDVQQGEwJVUzETMBEGA1UECBMK V2FzaGluZ3RvbjEQMA4GA1UEBxQHU2VhdHRsZTEYMBYGA1UEChQPQW1hem9uLmNv bSBJbMMuMRowGAYDVQQDFBFpYW0uYW1hem9uYXdzLmNvbTCBnzANBgkqhkiG9w0B AQEFAA0BjQAwgYkCgYEA3Xb0EGea2dB8QGEUwLcEpwvGawEkUdLZmGL1rQJZdeeN 3vaF+ZTm8QwSAdk2Gr/RwYXtpx04xvQXmNm+9YmksHmCZdruCrW1eN/P9wBfqMMZ X964CjVov3NrF5AuxU8jgtw0yu//C3hWn0uIVGdg76626gg0oJSaj48R2n0MnVcC AwEAAa0CAdEwggHNMAkGA1UdEwQCMAAwCwYDVR0PBAQDAgWgMEUGA1UdHwQ+MDww 0qA4oDaGNGh0dHA6Ly9TV1JTZWN1cmUtRzItY3JsLnZlcmlzaMduLmNvbS9TV1JT ZWN1cmVHMi5jcmwRAYDVR0gBD0w0zA5BgtghkgBhvhFAQcXAzAqMCgGCCsGAQUF BwIBFhxodHRwczovL3d3dy52ZXJpc21nbi5jb20vcnBhMB0GA1UdJQQWMBQGCCsG AQUFBwMBBggrBgEFBQcDAjAfBgNVHSMEGDAWgBS17wsRzsBBA6NKZZB1shzgVy19 RzB2BggrBgEFBQcDAjAfBgNVHSMEGDAWgBS17wsRzsBBA6NKZZB1shzgVy19 RzB2BggrBgEFBQcDAjAfBgNVHSMEGDAWgBS17wsRzsBBA6NKZZB1shzgVy19 RzB2BggrBgEFBQcDAjAfBgNVHSMEGDAWgBS17wsRzsBBA6NKZZB1shzgVy19 RzB2BggrBgEFBQcDAjAfBgNVHSMEGDAWgBS17wsRzsBBA6NKZZB1shzgVy19 RzB2BggrBgEFBQcDAjAfBgNVHSMEGDAWgBS17wsRzsBBA6NKZZB1shzgVy19 RZB2BggrBgEFBQcDAjAFBgNVHSMEGDAVL1NWUNINY3VZ51HMi1haWEudmVy aXNpZ24uY29tL1NWUNNY3VZUcyLmN1cjBuBggrBgEFBQcBDARiMGChXqBcMFow WDBWFg1pbWFnZS9naWYwITAfMAcGBSS0AwIaBBRLa7ko1gYMu9BS0JsprEsHiyEF GDAmFiRodHRw0i &vbG9nby52ZXJpc21nbi5jb20vdnNsb2dvMS5naWYwDQYJKoZI hvcNAQEFBQADggBBALpFBXeG782QsTt6wEE92BcVCuKjrs13dMK1dFiq30P4y/Bi ZBYEywBt8zNUFHUE25Ub/zmmpe7p0676tmQ8bRp/4qkJoisesHJvFgJ1mksr3IQ 3gaE1aN2BSUHKGLn9N4F09hYwbeEZaCxfgBiLdEIodNwzcvGJ+2L1DWGJ0GrNI NM856xjqhJCPxYzk9buuC11B4Kzu0CTbexz/iEgYV+DiuTxcfA4uhwMDSe0nynbn 1qiwRk450mC0nqH41y4P41Xo02t4A/D1118ZNct/Qf169a2Lf6vc9rF7BELT0e5Y R7CKX7fcSxRaeQdyGj/Jevm9BF/mSdnc1S5vas= ----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的证书格式要求。

### 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。

```
如果您的私钥加密,但不是按上述方案生成的指定格式私钥,例如私钥的开头和结尾是[-----BEGIN PRIVATE KEY-----, ---
--END PRIVATE KEY-----]或[-----BEGIN ENCRYPTED PRIVATE KEY-----, ----END ENCRYPTED
PRIVATE KEY-----],或者私钥中包含 Proc-Type: 4,ENCRYPTED,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 转换为 PEM
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 转换为 PEM

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

私钥转换:私钥一般在 IIS 服务器里可导出。

PFX 转换为 PEM

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 转换为 PEM

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。



## SSL 单向认证和双向认证说明

最近更新时间: 2024-08-19 10:08:51

SSL(Secure Sockets Layer,安全套接字协议)是为网络通信提供安全及数据完整性的一种安全协议。本文主要介绍 SSL 单向 认证和双向认证。

#### 🕛 说明:

负载均衡 CLB 可在创建 TCP SSL 监听器或 HTTPS 监听器时,选择 SSL 解析方式为单向认证或双向认证,详情请参见 配置 TCP SSL 监听器 、配置 HTTPS 监听器 。

#### SSL 单向认证和双向认证的区别

- SSL 单向认证 无需客户端拥有证书,只需服务端拥有证书。SSL 双向认证 需要客户端和服务端双方都拥有证书。
- SSL 单向认证相对于 SSL 双向认证的认证过程,无需在服务端验证客户端证书、以及协商加密方案,服务端发送给客户端也是未加密的密码方案(并不影响 SSL 认证过程的安全性)。
- 一般 Web 应用的用户数量众多,无需在通讯层做用户身份验证,因此配置 SSL 单向认证即可。但部分金融行业用户的应用对接, 可能会要求对客户端做身份验证,此时就需要做 SSL 双向认证。

#### SSL 单向认证

SSL 单向认证只需要验证服务端的身份,无需验证客户端的身份。SSL 单向认证的流程如下图所示。



1. 客户端发起 HTTPS 建立连接请求,将客户端支持的 SSL 协议版本号、加密算法种类、生成的随机数等信息发送给服务端。

2. 服务端向客户端返回 SSL 协议版本号、加密算法种类、生成的随机数等信息,以及服务端的证书(server.crt)。

3. 客户端验证证书(server.crt)是否合法,并从此证书中获取服务端的公钥:



- 检查证书是否过期。
- 检查证书是否已经被吊销。
- 检查证书是否可信。
- 检查收到的证书中的域名与请求的域名是否一致。
- 证书验证通过后,客户端生成一个随机数(密钥 K),作为通信过程中对称加密的密钥,并用服务端证书的公钥进行加密,然后发送给服务端。
- 5. 服务端收到客户端发送的加密信息后,使用私钥(server.key)进行解密,获取对称加密密钥(密钥 K)。
   在接下来的会话中,客户端和服务端将会使用该对称加密密钥(密钥 K)进行通信,保证通信过程中信息的安全。

#### SSL 双向认证

SSL 双向认证需要验证客户端和服务端的身份。SSL 双向认证的流程如下图所示。



- 1. 客户端发起 HTTPS 建立连接请求,将客户端支持的 SSL 协议版本号、加密算法种类、生成的随机数等信息发送给服务端。
- 2. 服务端向客户端返回 SSL 协议版本号、加密算法种类、生成的随机数等信息,以及服务端的证书(server.crt)。
- 3. 客户端验证证书(server.crt)是否合法,并从此证书中获取服务端的公钥:
  - 检查证书是否过期。



- 检查证书是否已经被吊销。
- 检查证书是否可信。
- 检查收到的证书中的域名与请求的域名是否一致。
- 4. 服务端要求客户端发送客户端的证书(client.crt),客户端将自己的证书发送至服务端。
- 5. 服务端验证客户端的证书(client.crt),验证通过后,服务端使用根证书(root.crt)解密客户端证书,然后获取客户端的公钥。
- 6. 客户端向服务端发送自己所支持的对称加密方案。
- 7. 服务端从客户端发送过来的对称加密方案中,选择加密程度最高的加密方式,并使用客户端公钥加密后,返回给客户端。
- 客户端使用客户端的私钥(client.key)解密加密方案,并生成一个随机数(密钥 K),作为通信过程中对称加密的密钥,然后使 用服务端证书的公钥进行加密后再发送给服务端。
- 服务端收到客户端发送的加密信息后,使用服务端的私钥(server.key)进行解密,获取对称加密密钥(密钥 K)。
   在接下来的会话中,客户端和服务端将会使用该对称加密密钥(密钥 K)进行通信,保证通信过程中信息的安全。

## 相关文档

证书要求及转换证书格式

# 日志管理 访问日志概述

最近更新时间: 2024-08-19 10:08:51

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。

#### () 说明:

- 仅七层负载均衡支持配置访问日志,四层负载均衡不支持配置访问日志。
- 当前仅部分地域支持配置访问日志,详情请参见 CLS 的 可用地域 。

## 存储方式

负载均衡的访问日志支持 日志服务(CLS):日志服务是一站式日志服务平台,提供从日志采集、日志存储到日志检索分析、实时消 费、日志投递等多项服务,协助用户通过日志来解决业务运营、安全监控、日志审计、日志分析等问题。

功能特性	配置访问日志到 CLS
获取日志的时间粒度	分钟级
在线检索	支持
检索语法	全文检索、键值检索、模糊关键字检索等,详情请参见检索规则
支持地域	地域支持详情请参见 CLS 的 可用地域
支持类型	支持公网/内网负载均衡
上下游链路	CLS 日志支持投递到 COS,支持使用 CKafka 消费日志
日志存储	腾讯云默认情况下不承诺存储访问日志,如有业务需要请自行配置访问日志到 CLS

## 相关操作

配置访问日志到 CLS

# 查看操作日志

最近更新时间:2025-05-15 17:46:21

您可以在 操作审计控制台 查询、下载负载均衡的操作记录。

操作审计(CloudAudit )是一项支持对您的腾讯云账号进行监管、合规性检查、操作审核和风险审核的服务。CloudAudit 提供腾讯 云账号活动的事件历史记录,这些活动包括通过腾讯云管理控制台、API 服务、命令行工具和其他腾讯云服务执行的操作。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

#### 查看操作记录

- 1. 登录 操作审计控制台。
- 2. 在左侧导航中,单击操作记录,进入操作记录页面。
- 在操作记录页面中,您可以根据操作类型、事件名称、操作者、敏感操作筛选、资源标签等查询操作记录,默认情况下仅展示部分数据,可在页面右边单击设置来获取更多列表字段。

操作记录				产品体验,你说了算	用户之声 🖸 操作审计使用说明 🖸
<ol> <li>以下列表包括了近:</li> </ol>	三个月 API活动的支持服务,如果需	要查看更长时间的操作记录,请使用跟踪	宗集功能,日志数据将持久化存储到指定	存储桶或CLS中。	
() 根据等保合规2.0及	网安法条例要求,企业云上业务日	志必须保存180天以上,建议您可以创建	跟踪集,投递到存储桶,方便长期保存您	的操作日志。	×
近30分钟 近1小时	近1天 近7天	自选时间 ~			C
操作类型	只写	▼ 事件名称 ①	请选择资源类型/事件名称 ✓		
操作者	请输入操作者/ID	Q 敏感操作筛选	全部		
资源标签	请选择标签	~			
查询 重置	展开更多搜索				
事件时间	事件名	高称	资源类型	操作者	资源信息
2025-05-13 18:47:09	9		clb(负载均衡)		⊒
2025-05-13 18:46:2	2		clb(负载均衡)		

筛选条件说明如下:

- **时间范围**:您可以筛选查看30天范围内的日志。
- 操作类型: 支持按全部、读、写过滤。
- 事件名称: 您可以通过各产品的接口文档中的接口名称,搜索过滤您希望查询到的日志。例如 CVM RunInstances (创建 实例)。最多支持同时查询10个事件。

() 说明:

若您未在列表中查找到所需查询产品的事件名称,则请通过 在线客服 提交工单进行反馈,我们将尽快排查处理。

○ 操作者: 操作者可分为以下集中类型:

- **主账号操作**: 用户名显示为 root。
- **子用户操作**: 用户名显示子用户名称,如果子用户已被删除,则显示子用户 ID。
- 角色操作:用户名显示角色名称,如果角色已被删除,则显示角色 ID。
   您可单击操作者,前往"用户列表"页面查看该用户更多信息。
- 敏感操作筛选:支持筛选全部敏感及非敏感操作。敏感操作是可能涉及云资源重要操作的事件,由平台定义。若您需将某些操作 也纳入敏感操作,则请通过 在线客服 提交工单进行反馈,我们将尽快处理。
- 资源标签:支持按照标签筛选。如需了解标签更多信息,请参见标签。
- 资源 ID: 支持输入资源 ID 搜索。例如 ins-fi8oxxxx 。
- 密钥 ID: 支持输入密钥 ID 搜索。例如 xxxxZ0GSXSG2nT5c6Xxxxxxxxxxxxxxxxx 。
- **请求 ID: 支持输入请求 ID 搜索。例如** a7da0568-7580-4798-88c8-xxxxxxxx 。
- API 错误码: 支持输入 API 错误码搜索。请参考各产品 API 文档中的错误码,进行对比后按需搜索。
- 4. 单击查询,即可获取对应操作记录信息。

#### 查看事件详情

1. 若您需查看某一事件的详细信息,可单击列表中的事件名称,并在展开的模块中,可查看事件基本信息、相关资源及事件记录。

事件详情				×
基本信息	事件说明 🖸			
密钥 ID 事件名称 事件时间 源 IP 地址 资源地域 CAM 错误码	AKID6K k Mod 2023-06-27 10:17:18	事件区域 事件源 请求 ID 操作者	ap-guangzhou Ib.api.qcloud.com/v2/index.php	

🕛 说明:

您可通过 "CAM 错误码"字段判断事件是否执行成功。若 CAM 错误码为空,则事件执行成功。若 CAM 错误码不为 空,则事件执行失败,具体错误原因请查看事件详情中的 errorCode 及 errorMessage 字段。

2. 可在事件记录模块中查看事件详细信息,字段说明请参考 附录。



# 配置访问日志

最近更新时间: 2025-05-15 17:46:21

负载均衡支持配置七层(HTTP/HTTPS)访问日志(Access Log),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:

- 日志上报,提供尽力而为服务(Best-Effort Service),优先保障业务转发,再保障日志上报。
- 日志存储和查询,按当前使用的存储服务来提供服务保障 SLA。

() 说明:

- 当前负载均衡仅七层协议(HTTP/HTTPS)支持配置访问日志到CLS,四层协议(TCP/UDP/TCPSL)不支持配置 访问日志到CLS。
- 负载均衡配置访问日志到 CLS 的功能免费,用户仅需支付日志服务 CLS 的费用。
- 当前仅部分地域支持此功能,实际以控制台支持的地域为准。

## 方式一:为单实例配置访问日志

#### 步骤1:开启访问日志存入 CLS

- 1. 登录 负载均衡控制台,单击左侧导航栏的实例管理。
- 2. 在**实例管理**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。

访问日志 (七层)
仅七层监听器(HTTP/HTTPS)支持配置访问日志(Access Log),四层监听器(TCP/UDP/TCP SSL)不支 持
日志服务CLS① 未开启
腾讯云日志服务CLS为独立计费产品,计费标准请参见CLS计费详情记

 在弹出的修改 CLS 日志存放位置对话框中,开启启用日志,并选择存储访问日志的日志集和日志主题,单击确定。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。

修改 CLS 日詞	志存放位置 1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.	
<ol> <li>1. 仅- 请 2. 建ì 在<u>ì</u></li> </ol>	七层负载均衡支持配置访问日志,四层负载均衡不支持配置访问日志。 <sup></sup> 参见 <b>访问日志概述</b> : 义您选择有"推荐"标识日志集和有"CLB"标识的日志主题,该类日志主题 <u>访问日志</u> 页面集中管理 CLB 实例的日志配置情况。	详情 迹可
日用日志		情区
	腾讯云日芯服务 CLS 为强立计资厂而,计资标准请参见CLS 计资件	
日志存储地域	腾讯云口志服务 CLS 为独立计预广品, 计预标准请参见CLS 计数件 成都	
]志存储地域 ]志集	勝讯云日志服务 CLS 为强立计预广品,计预标准请参见CLS 计预详 成都	¢
日志存储地域 日志集 日志主题		ф ф
日志存储地域 日志集 日志主题	▶ ▶ ▶ ▶ ▶ ▶ ▶ ▶ ▶ ▶ ▶ ▶ ▶ ▶ ▶ ▶ ▶ ▶ ▶	ф ф

#### () 说明:

腾讯云

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。

5. 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。

6. (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单击确定即可。

#### 步骤2: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	-

🔗 腾讯云

具体操作如下:

- 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。
- 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,添加完成后,单击页面底部确定。索引字段配置说明请参见开启索引。

索引配置	
<b>导入配置规则</b> 索引状态	▼ 开启后可对日志进行检索分析,将产生索引流量、索引存储及相应费用。费用详情 □
全文索引	T启后支持使用关键词检索日志全文,例如输入 error 检索包含 error 关键词的日志。
	全文分词符     I=D       将日志全文按照分词符拆分成若干个分词用于检索。
	大小写敏感
	包含中文 日志中包含中文且需对中文进行检索时可开启该功能,将每一个汉字拆分为独立的分词用于检索。
键值索引	▼●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●
	大小写敏感
	自动配置①
	批量添加字段 显示内置保留字段 按字段名称搜索 Q
	字段名称         字段别名①         字段类型①         分词符①         包含中文①         开启统计①
	请输入字段别名     text ~     请输入分词符     ●
	请输入学段别名     text ~     请输入分词符     ③     ③

4. 索引配置完成后结果如下图所示。

索引配置							编辑
<b>导入配置规则</b> 日志主题名称	CLB						
日志主题ID		ť					
索引状态	已开启						
全文索引 🛈	已开启						
	大小写敏感 否						
	全文分词符 () I=[]						
	是否包含中文() 不包含						
键值索引 🛈	已开启						
	大小写敏感 否						
	自动配置 () 否					按字段名称搜	嗦 Q
	字段名称		别名	字段类型()	分词符 ①	包含中文()	开启统计 🛈
				text	无	无	开启
				text	无	无	开启

## 步骤3: 查看访问日志



- 1. 登录 日志服务控制台。
- 2. 在左侧导航栏中,单击**检索分析**。
- 3. 在顶部选择需要查询的日志主题。
- 4. 选择检索分析语句输入模式,日志服务提供两种模式来输入检索分析语句。详情可参见 语法规则 。

() 说明:	
SOURCE_	字段记录的是 CLB 集群的转发节点机器 IP。

4.1 交互模式:通过鼠标点击指定检索条件及统计分析规则,自动生成检索分析语句,易用性高。

⑦交互模式 ~	· ①历史记录	<b>一</b> 语句模板		
监听器转发域名 <b>全部</b>	客户端状态码 <b>全部</b>	后端服务地址 <b>全部</b>	+	≡
🗠 添加统计语句 🛛				

4.2 语句模式:直接输入检索分析语句,需符合语法规则,灵活度高。

[/]语	吾句模式 >	口收藏夹	①历史记录	🔁 语句模板	
1	e.g	_SOURCE:	127.0.0.1	AND "http/1.0"	或者使用AI智能编写

- 5. 输入检索分析语句后,在右侧选择时间范围,然后单击搜索按钮,执行检索分析。
  - 5.1 当检索分析语句仅包含检索条件时:可在**原始日志**中查看匹配检索条件的日志,默认按日志时间倒排。
  - 5.2 当检索分析语句包含 SQL 语句时:可在**统计图表**中查看分析结果,同时还可在**原始日志**中查看符合检索条件的日志,以便于对 比分析统计结果及原始日志。

#### 方式二: 批量配置访问日志

#### 步骤1: 创建日志集和日志主题

- 1. 登录 负载均衡控制台,单击左侧导航栏的日志管理 > 访问日志列表。
- 2. 在访问日志页面左上角选择所属地域,在日志集信息区域,单击创建日志集。
- 3. 在弹出的创建日志集对话框中,单击保存。

#### 🕛 说明:

每个地域仅支持创建一个日志集,日志集名称为"clb\_logset"。

- 4. 在**访问日志**页面的日志主题区域,单击新建日志主题。
- 5. 在弹出的新增日志主题对话框,选择存储类型和日志保存时间后,选择左侧的负载均衡实例添加至右侧列表中,单击保存。

🕛 说明:

- 存储类型分为标准存储和低频存储,详情请参见 存储类型概述 。
- 日志保存支持永久保存和按固定时长保存。
- ∽ 腾讯云
  - 新建日志主题时,可选择添加、或不添加负载均衡实例。在日志主题列表的右侧操作列中,单击更多>管理可重新添加负载均衡实例。每个负载均衡实例仅限添加至一个日志主题中。
  - 一个日志集中可创建多个日志主题(Topic),您可将不同的CLB日志放在不同的日志主题中,这些日志主题默认会带CLB标识。

新增日志主题	题							×
名称	test-topic							
	主题名称创建后不	可修改,字符长度为1至	255个字符,允许的字符为a	a-z. A-	Z、0-9、_、-			
存储类型	● 标准存储 CLS发布全新存储	) <b>低频存储</b> 类型-低频存储,详情请	查看存储类型介绍 🖸					
日志永久保存								
日志保存时间	<ul> <li>30</li> <li>该日志主题只保存</li> </ul>	+ 天 [1-3600]天内的日志记录	t					
选择负载均衡	实例				已选择(1)			
负载均衡ID/	名称		Q,		负载均衡ID/名称			Q,
_ 负载均	的衡ID/名称	所属网络	VIP/网络类型		负载均衡ID/名称	所属网络	VIP/网络类型	
Market Ib-		vpc-	123. 公网		ID-	vpc-	123. 公网	٢
		vpc-	106. 公网	$\Leftrightarrow$				
Ib-		vpc-	<b>123.</b> 公网					
共 15 条	10 ▼ 최	€/页 № ◀	1 /2页 ▶ ▶					
支持按住 shift	键进行多选							
			保存		取消			

6. (可选)若需关闭访问日志,在日志主题列表的右侧操作列中,单击停止,停止投递日志即可。

#### 步骤2: 查看访问日志

- 1. 登录 日志服务控制台。
- 2. 在左侧导航栏中,单击**检索分析**。
- 3. 在顶部选择需要查询的日志主题。
- 4. 选择检索分析语句输入模式,日志服务提供两种模式来输入检索分析语句。详情可参见 <mark>语法规则</mark> 。
  - 4.1 交互模式:通过鼠标点击指定检索条件及统计分析规则,自动生成检索分析语句,易用性高。

♥交互模式 ~ □ □ 收藏邦	そ ①历史记录	<b>云</b> 语句模板			
监听器转发域名 <b>全部</b>	客户端状态码 <b>全部</b>	后端服务地址 <b>全部</b>	+	≡	
▶ 添加统计语句					

4.2 语句模式:直接输入检索分析语句,需符合语法规则,灵活度高。





5. 输入检索分析语句后,在右侧选择**时间范围**,然后单击**搜索**按钮,执行检索分析。

- 5.1 当检索分析语句仅包含检索条件时:可在**原始日志**中查看匹配检索条件的日志,默认按日志时间倒排。
- 5.2 当检索分析语句包含 SQL 语句时:可在统计图表中查看分析结果,同时还可在原始日志中查看符合检索条件的日志,以便于对 比分析统计结果及原始日志。

### 日志格式及变量说明

#### 字段类型

目前日志服务支持如下三种字段类型:

名称	类型描述
text	文本类型
long	整型数值类型(Int 64)
double	浮点数数值类型(64 bit)

#### 日志变量说明

变量名	说明	字段类型
stgw_request_id	请求 ID。	text
time_local	访问的时间与时区,例如, "01/Jul/2019:11:11:00 +0800" ,最后 的 "+0800" 表示所处时区为 UTC 之后的8小时,即为北京时间。	text
protocol_type	协议类型(HTTP/HTTPS/SPDY/HTTP2/WS/WSS)。	text
lb_id	CLB 的实例 ID,CLB 实例的唯一标识。	text
server_addr	CLB 的 VIP,仅非域名化实例支持,域名化实例该取值为空。	text
server_port	CLB 的 VPort,即监听端口。	long
server_name	规则的 server_name,CLB 的监听器中配置的域名。	text
remote_addr	客户端 IP。	text
remote_port	客户端端口。	long
status	CLB 返回给客户端的状态码。	long
upstream_addr	RS 地址。	text
upstream_status	RS 返回给 CLB 的状态码。	text
proxy_host	stream ID。	text



request	请求行。	text
request_length	从客户端收到的请求字节数。	long
bytes_sent	发送到客户端的字节数。	long
http_host	请求域名,即 HTTP 头部中的 Host。	text
http_user_agent	HTTP 协议头的 user_agent 字段。	text
http_referer	HTTP 请求来源。	text
http_x_forwarded _for	HTTP 请求中 x-forwarded-for header 的内容。	text
request_time	请求处理时间:从收到客户端的第一个字节开始,直到给客户端发送的最后一个字节 为止,包括客户端请求到 CLB、CLB 转发请求到 RS、RS 响应数据到 CLB、 CLB 转发数据到客户端的总时间。单位:秒。	double
upstream_respons e_time	整个后端请求所花费时间:从开始 CONNECT RS 到从 RS 接收完应答的时间。单位:秒。	double
upstream_connect _time	和 RS 建立 TCP 连接所花费时间:从开始 CONNECT RS 到开始发送 HTTP 请 求的时间。单位:秒。	double
upstream_header _time	从 RS 接收完 HTTP 头部所花费时间:从开始 CONNECT RS 到从 RS 接收完 HTTP 应答头部的时间。单位:秒。	double
tcpinfo_rtt	TCP 连接的 RTT。单位:微秒。	long
tcpinfo_rtt connection	TCP 连接的 RTT。单位:微秒。 连接 ID。	long long
tcpinfo_rtt connection connection_reque sts	TCP 连接的 RTT。单位:微秒。         连接 ID。         连接上的请求个数。	long long long
tcpinfo_rtt connection connection_reque sts ssl_handshake_ti me	TCP 连接的 RTT。单位:微秒。连接 ID。连接上的请求个数。记录 SSL 握手各阶段耗时,格式: x:x:x:x:x:x:x:x: 。其中,冒号分隔的字符串, 单位是 ms,每个阶段耗时若小于1ms 则显示为0。 。第1个字段表示是否 SSL 会话复用。 。第2个字段表示完整的握手时间。 3~7表示 SSL 各阶段耗时。 。第3个字段表示 CLB 从收到 client hello 到发送 server hell done 的时间。 。第3个字段表示 CLB 从收到 client hello 到发送 server 证书完成的时间。 。第5个字段表示 CLB 从以到 client key exchange 完成的时间。 。第6个字段表示 CLB 从收到 client key exchange 开始到收完 client key exchange 的时间。 。 第7个字段表示 CLB 从收到 client key exchange 到发送 server finished 的时间。	long long text
<pre>tcpinfo_rtt connection connection_reque sts  ssl_handshake_ti me ssl_cipher</pre>	TCP 连接的 RTT。单位:微秒。连接 ID。连接上的请求个数。记录 SSL 握手各阶段耗时,格式: x:x:x:x:x:x 。其中,冒号分隔的字符串,单位是 ms,每个阶段耗时若小于1ms则显示为0。第1个字段表示是否 SSL 会话复用。第2个字段表示完整的握手时间。3~7表示 SSL 各阶段耗时。第3个字段表示 CLB 从收到 client hello 到发送 server hell done 的时间。第4个字段表示 CLB 从收到 client hello 到发送 server 证书完成的时间。第6个字段表示 CLB 从收到 client key exchange 完成的时间。第6个字段表示 CLB 从收到 client key exchange 开始到收完 client key exchange 前时间。第7个字段表示 CLB 从收到 client key exchange 到发送 server finished 的时间。SSL 加密套件。	long long text
<pre>tcpinfo_rtt connection connection_reque sts  ssl_handshake_ti me ssl_cipher ssl_protocol</pre>	TCP 连接的 RTT。单位:微秒。连接 ID。连接 L的请求个数。记录 SSL 握手各阶段耗时,格式: x:x:x:x:x:x:x: 。其中,冒号分隔的字符串, 单位是 ms,每个阶段耗时若小于1ms 则显示为0。第1个字段表示是否 SSL 会话复用。第2个字段表示完整的握手时间。3~7表示 SSL 各阶段耗时。第3个字段表示 CLB 从收到 client hello 到发送 server hell done 的时间。第4个字段表示 CLB 从发送 server 证书开始到发送 server 证书完成的时间。第6个字段表示 CLB 从收到 client key exchange 完成的时间。第6个字段表示 CLB 从收到 client key exchange 开始到收完 client key exchange 前时间。第7个字段表示 CLB 从收到 client key exchange 开始到收完 client key exchange 新时间。第5L 加密套件。SSL 加密套件。	long long text text



request_method	请求方式,支持 POST 和 GET 请求。	text
uri	资源标识符。	text
server_protocol	CLB 的协议。	text

## 默认支持检索的日志变量

#### 带 "CLB"标识的日志集默认支持检索的字段如下所示:

索引字段	说明	字段类型
time_local	访问的时间与时区,例如,"01/Jul/2019:11:11:00 +0800",最后 的"+0800"表示所处时区为 UTC 之后的8小时,即为北京时间。	text
protocol_type	协议类型(HTTP/HTTPS/SPDY/HTTP2/WS/WSS)。	text
server_addr	CLB的VIP。	text
server_name	规则的 server_name,CLB 的监听器中配置的域名。	text
remote_addr	客户端 IP。	text
status	CLB 返回给客户端的状态码。	long
upstream_addr	RS 地址。	text
upstream_status	RS 返回给 CLB 的状态码。	text
request_length	从客户端收到的请求字节数。	long
bytes_sent	发送到客户端的字节数。	long
http_host	请求域名,即 HTTP 头部中的 Host。	text
request_time	请求处理时间:从收到客户端的第一个字节开始,直到给客户端发送的最后一个字节 为止,包括客户端请求到 CLB、CLB 转发请求到 RS、RS 响应数据到 CLB、 CLB 转发数据到客户端的总时间。单位:秒。	double
upstream_respons e_time	整个后端请求所花费时间:从开始 CONNECT RS 到从 RS 接收完应答的时间。单 位:秒。	double
vip_vpcid	负载均衡实例所属的私有网络 ID,公网 CLB 的取值为−1。	long
lb_id	CLB 的实例 ID,CLB 实例的唯一标识。	text



# 抽样采集日志

最近更新时间: 2025-05-15 17:46:22

在您开启七层访问日志或者健康检查日志后,针对一些日志量较大的场景,全量日志上报可能会导致日志成本较高。负载均衡支持抽样 采集部分日志,减少数据上报量,从而降低日志成本。

#### () 说明:

负载均衡支持配置访问日志和健康检查日志至日志服务 CLS,实现对日志数据的检索分析、可视化和告警等服务。腾讯云日志 服务 CLS 为独立计费产品,计费标准请参见 CLS 计费详情。

#### 前提条件

- 您已创建访问日志的日志集和日志主题,详情请参见 配置访问日志。
- 您已创建健康检查日志的日志集和日志主题,详情请参见 配置健康检查日志。

### 抽样采集七层访问日志

- 1. 登录 负载均衡控制台,选择左侧导航栏的日志管理 > 访问日志列表。
- 2. 在访问日志详情页左上角选择所在地域,在日志主题列表找到目标日志主题,选择操作列的更多 > 抽样采集。
- 3. 在弹出的 CLB 日志抽样采集管理对话框,开启抽样采集开关,并按需进行参数配置。

参数	说明
抽样采集开关	<ul> <li>开启后,支持抽样采集日志。</li> <li>关闭后,会全量采集日志,不再进行抽样采集。</li> </ul>
默认抽样比例	当您配置了抽样采集日志的抽样规则后,对于未匹配到该抽样规则的日志会按照默认抽样比例进行日志采 集。支持输入1–100的整数。
抽样字段	抽样采集日志的抽样字段默认支持 status 和 server_name。
抽样规则	抽样规则支持正则表达式。例如若您希望抽样采集 status 状态码为400或500的日志,则可设置抽样规 则为:400 500。
抽样比例	用于定义抽样采集的比例,支持输入1-100的整数。
操作	您可以选择删除抽样采集规则。
添加	当目前的抽样规则不能满足您的需求时,您可以选择继续添加抽样规则。每个日志主题最多支持配置5条 抽样规则。



CLB日志抽样采集	管理		×
抽样采集			
默认抽样比例①	10 %		
抽样采集支持按比例	采集符合抽样规则的日志,抽样规则	支持正则表达式,抽样比例支持	1~100的整数,具体说明 🖸
抽样字段	抽样规则	抽样比例	操作
status 💌	400 500	20 %	删除
添加			
		提交取消	

4. 配置完成以后,单击提交,返回到日志主题列表页面,已开启抽样采集的日志主题会添加抽样标识。

test_cold 抽样	投递中	30 🎤	广州	低频存储	2022-07-26 18:02:13	停止 检索 更多 ▼

# 抽样采集健康检查日志

- 1. 登录 负载均衡控制台,选择左侧导航栏的日志管理 > 健康检查日志列表。
- 2. 其余步骤可参考以上的 抽样采集七层访问日志。

### 相关文档

- 配置访问日志
- 配置健康检查日志

腾田元

# 配置健康检查日志

#### 最近更新时间: 2025-05-30 14:25:12

若您想要查看健康检查日志,则需先将日志存储到日志服务 CLS 中,然后在 CLS 中进行查看。负载均衡支持配置健康检查日志到日 志服务 CLS 中,能够进行分钟粒度的日志上报和在线多规则检索,帮助您排查健康检查异常的原因,快速定位问题。

#### 🕛 说明:

健康检查日志功能目前处于内测阶段,如需使用,请提交内测申请。

健康检查日志功能包括日志上报、日志存储和查询:

- 日志上报:优先保障业务转发,再保障日志上报。
- 日志存储和查询:按当前使用的存储服务来提供服务保障 SLA。

#### 限制说明

- 健康检查是跳变日志,仅后端服务器的健康状态发生变化才会产生健康检查日志。
- 负载均衡四层、七层协议均支持配置健康检查日志到日志服务 CLS。
- 负载均衡配置健康检查日志到 CLS 的功能免费,用户仅需支付日志服务 CLS 的费用。
- 仅负载均衡(原"应用型负载均衡")实例类型支持此功能,传统型负载均衡实例类型不支持。
- 当前仅部分地域支持此功能,实际以控制台支持的地域为准。

#### 步骤1: 添加角色授权

若您未开通日志服务,则需先开通日志服务并添加角色授权。

- 1. 登录 负载均衡控制台,单击左侧导航栏的日志管理 > 健康检查日志列表。
- 2. 在健康检查日志页面,单击**立即开通**,并在弹出的对话框中单击前往授权。

#### 您还未开通 CLB 访问日志服务 CLS 的权限

若需使用 日志服务 功能,需要您允许 负载均衡 访问您的部分资源,他们将通过服务角色访问您已授权给予划们的资源以实现当前功能,请您点击前往授权,为 负载均衡 进行相关服务接口的授权。



3. 跳转至访问管理控制台,在角色管理页面,单击同意授权。

#### 步骤2: 创建日志集和日志主题

若您需要配置健康检查日志到日志服务 CLS 中,则需先创建日志集和日志主题。 若已有日志集和日志主题,则可直接跳转至 <mark>步骤3</mark> 开始操作。

- 1. 登录 负载均衡控制台,单击左侧导航栏的日志管理 > 健康检查日志列表。
- 2. 在健康检查日志页面左上角选择所属地域,在日志集信息区域,单击创建日志集。
- 3. 在弹出的创建日志集对话框中,单击保存。
- 4. 在健康检查日志页面的日志主题区域,单击新建日志主题。
- 5. 在弹出的新增日志主题对话框,选择存储类型和日志保存时间后,选择左侧的负载均衡实例添加至右侧列表中,单击保存。



#### () 说明:

- 存储类型分为标准存储和低频存储,详情请参见 存储类型概述。
- 日志保存支持永久保存和按固定时长保存。
- 新建日志主题时,可选择添加、或不添加负载均衡实例。在日志主题列表的右侧操作列中,单击更多 > 管理可重新添加 负载均衡实例。每个负载均衡实例仅限添加至一个日志主题中。
- 每个地域支持创建一个日志集,日志集中可创建多个日志主题(Topic),您可将不同的CLB日志放在不同的日志主题中,这些日志主题默认会带"CLB"标识。

新增日志主	题							×
名称	test-topic							
	主题名称创建质	5不可修改,字符长度为13	至255个字符,允许的字符为	a-z、A-	Z、0-9、_、-			
存储类型	● 标准存储 CLS发布全新有	○ 低频存储 ○ 低频存储,详情请	查看存储类型介绍 🖸					
日志永久保存								
日志保存时间	<ul> <li>30</li> <li>该日志主题只保</li> </ul>	+ 天 保存[1-3600]天内的日志记;	R.					
选择负载均衡	实例				已选择(1)			
负载均衡ID	/名称		Q		负载均衡ID/名称			Q,
_ 负载	均衡ID/名称	所属网络	VIP/网络类型		负载均衡ID/名称	所属网络	VIP/网络类型	
☑ <sup>Ib-</sup>		vpc-	123. 公网		lb-	vpc-	123. 公网	8
lb-		vpc-	1 <b>06.</b> 公网	$\Leftrightarrow$				
lb-		vpc-	123. 公网					
共 15 条	10 -	条/页 🛛 🔺	1 /2页 ▶ №					
支持按住 shif	t 键进行多选							
			保存		取消			

6. (可选)若需关闭健康检查日志,在日志主题列表的右侧操作列中,单击停止,停止投递日志即可。

#### 步骤3: 查看健康检查日志

负载均衡已自动配置以健康检查日志的变量为关键值的索引,您无需手动配置索引,可直接通过检索分析来查询健康检查日志。 1. 登录 负载均衡控制台,单击左侧导航栏的**日志管理 > 健康检查日志列表**。

- 2. 在健康检查日志页面左上角选择所属地域,在日志主题区域,单击右侧"操作"列的检索,跳转至日志服务控制台。
- 3. 在日志服务控制台,单击左侧导航栏的检索分析。
- 4. 在检索分析页面的输入框中输入检索分析语句,选择时间范围,单击检索按钮即可检索 CLB 上报到 CLS 的健康检查日志。

[/]语句模式 ~ □ 収藏夹 ③历史记录 🔁 语句模板	(10) 推荐仪表盘 告警 健康监控 采集配置 索引配置 更多 >
1 e.gSOURCE: 127.0.0.1 AND "http/1.0" 或者使用AI智能编写	※ 2015分钟 × Q
<ul> <li>说明:</li> <li>检索语法详情请参见 语法与规则 。</li> </ul>	



# 健康检查日志格式及说明

### 日志格式

[\$protocol][\$rsport][\$rs\_vpcid][\$vport][\$vpcid][\$time][\$vip][\$rsip][\$status][\$domain] [\$url]

#### 日志变量说明

变量名	说明	字段类型
protocol	协议类型(HTTP/HTTPS/SPDY/HTTP2/WS/WSS)。	text
rsport	后端 RS 端口。	long
rs_vpcid	后端 RS 的所属私有网络 ID。	long
vport	CLB 的 VPort,即监听端口。	long
vpcid	负载均衡 VIP 的所属私有网络 ID,公网 CLB 的 vpcid 为−1。	long
time	访问的时间与时区,例如, "01/Jul/2019:11:11:00 +0800" ,最后的 "+0800" 表示所处时 区为 UTC 之后的8小时,即为北京时间。	text
vip	CLB的VIP。	text
rsip	后端 RS 的 IP 地址。	text
status	当前健康检查状态: <ul> <li>true:表示健康</li> <li>false:表示异常</li> </ul>	text
domain	健康检查域名。若监听器为四层监听器,则无健康检查域名,此参数为空。	text
url	健康检查 URL。若监听器为四层监听器,则无健康检查 URL,此参数为空。	text

# 相关文档

日志服务 CLS 快速入门



# 访问日志仪表盘

最近更新时间: 2025-05-15 17:46:22

负载均衡提供了开箱即用的访问日志仪表盘。您将访问日志配置到日志服务 CLS 后,负载均衡将自动为访问日志配置仪表盘,以图表 形式分析访问日志,实现在负载均衡控制台全面观测、分析、定位问题的能力。

### 仪表盘介绍

每个日志主题对应一个仪表盘,每个仪表盘包含以下数据指标图表:

- PV
- UV
- 请求报文流量
- 返回客户端流量
- 平均请求时间
- 平均响应时间
- 后端服务返回的状态码分布
- 总状态码分布
- PV/UV 趋势
- 请求/返回流量趋势
- 每分钟平均请求/返回时间
- P99、P95、P90、P50访问时间
- 请求数 TOP 实例统计
- 请求数 TOP 域名统计

#### 前提条件

您已成功创建日志主题,操作步骤请参见 创建日志集和日志主题 。

#### 操作步骤

- 1. 登录 负载均衡控制台,选择左侧导航栏的日志管理 > 访问日志仪表盘。
- 2. 在访问日志仪表盘页面,选择所在地域和日志主题,自动显示出该日志主题对应的仪表盘。



访问日志仪表盘 地域 🔇 深圳 ▼ 日志集	clb + 日志主题 test		- \$	访问日初	版义表盘帮助文档
CLB 访问日志仪表盘			在日志級务中查看更多 [2]	近15分钟 🔻	() 关闭 ▼
负载均衡VIP 全部▼ 负载均衡实例名称 全部▼	客户满P 全部 ¥ 后磺服务器IP 全部 ¥	返回码	全部▼		
PV		•••	UV		•••
р	V		U	V	
	1			1	
较1天前	↓80.00 %		较 1 天前	↓80.00 %	
请求报文流量 …	返回客户端流量		平均请求时间 …	平均响应时间	
请求报文流量 <b>164.00</b> B	返回客户端流量 <b>293.00</b> 日	3	平均请求时间 <b>0.00</b> ms	平均响应时间	
较1天前↓80.00%	较1天前↓80.00 %		1 天前暂无数据	1 天前暂无数据	
后端服务返回的状态码分布		•••	请求状态码分布		•••

3. (可选)在访问日志仪表盘页面的仪表盘左上角,可设置负载均衡 VIP、客户端 IP、后端服务器 IP 和返回码过滤项过滤访问日志 并显示。

### 相关文档

- 配置访问日志
- IP 函数

# 监控告警 获取监控数据

最近更新时间: 2025-05-19 11:58:01

腾讯云可观测平台为负载均衡和后端实例提供数据收集和数据展示功能。使用腾讯云可观测平台,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。有关腾讯云可观测平台的更多信息,请参见 腾讯云可观测平台 产品文档。 腾讯云默认为所有用户提供腾讯云可观测平台功能,您无需手动开通,只要您使用了负载均衡,腾讯云可观测平台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,查看实例的性能数据。

ID/名称 \$	监控	状态	VIP
	di	正常	11

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。

÷				1										
基本位	言息	监听器管理		重定向函	置	Γ	监控	安全	组					
		1小时			白	0	时间粒度:	1分钟	~	C	关闭 🗸	•••	✔ 显示图例	
监听器	全部		~	后端服务	全部	5		~	机器端口	1 1	言部		~	

## 腾讯云可观测平台控制台

登录 腾讯云可观测平台控制台,单击左侧导航栏中**云产品监控**模块下的 <mark>负载均衡</mark>--CLB,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。

# API 方式

您可以使用 GetMonitorData 接口获取所有产品的监控数据,具体内容请参见 拉取指标监控数据 ,负载均衡的命名空间请参见 公网 负载均衡监控指标 和 内网负载均衡监控指标 。

# 监控指标说明

最近更新时间: 2025-05-23 17:06:12

腾讯云可观测平台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 腾讯云可观测平台控制台 查看负载均衡的监控,选择**云产品监控 > 负载均衡--CLB**,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。

#### () 说明:

目前仅性能容量型负载均衡实例的并发连接数利用率、新建连接数利用率指标开通以后会上报数据,共享型负载均衡实例暂时 不会上报数据。

## 负载均衡实例维度

指标英文名	指标中文名	指标说明	单 位	统计粒度(秒)
ClientConnu m	客户端到 LB 的活跃连 接数	在统计粒度内的某一时刻,从客户端到负载均 衡或监听器上的活跃连接数。	个	10、60、300
ClientInactiv eConn	客户端到 LB 的非活跃 连接数	在统计粒度内的某一时刻,从客户端到负载均 衡或监听器上的非活跃连接数。	个	10、60、300
ClientConcur Conn	客户端到 LB 的并发连 接数	在统计粒度内的某一时刻,从客户端到负载均 衡或监听器上的并发连接数。	个	10、60、300
ConcurConn VipRatio	并发连接数利用率	在统计粒度内的某一时刻,从客户端到负载均 衡的并发连接数相比实例当前规格的并发连接 数性能上限的利用率。 此指标仅性能容量型实例与已限速的共享型实 例支持。	%	10、60、300
ClientNewCo nn	客户端到 LB 的新建连 接数	在统计粒度内,从客户端到负载均衡或监听器 上的新建连接数。	个/ 秒	10、60、300
NewConnVip Ratio	新建连接数利用率	在统计粒度内的某一时刻,从客户端到负载均 衡的新建连接数相比实例当前规格的新建连接 数性能上限的利用率。 此指标仅性能容量型实例与已限速的共享型实 例支持。	%	10、60、300
ClientInpkg	客户端到 LB 的入包量	在统计粒度内,客户端向负载均衡每秒发送的 数据包数量。	个/ 秒	10、60、300
ClientOutpkg	客户端到 LB 的出包量	在统计粒度内,负载均衡向客户端每秒发送的 数据包数量。	个/ 秒	10、60、300
ClientAccIntr affic	客户端到 LB 的入流量	在统计粒度内,客户端流入到负载均衡所用的 流量。	M B	10、60、300
ClientAccOu	客户端到 LB 的出流量	在统计粒度内,负载均衡流出到客户端所用的	Μ	10、60、300

ttraffic		流量。	В	
ClientOuttraf fic	客户端到 LB 的出带宽	在统计粒度内,负载均衡流出到客户端所用的 带宽。	Mb ps	10、60、300
ClientIntraffi c	客户端到 LB 的入带宽	在统计粒度内,客户端流入到负载均衡所用的 带宽。	Mb ps	10、60、300
OutTraffic	LB 到后端的出带宽	在统计粒度内,后端服务器流出到负载均衡所 用的带宽。	Mb ps	60、300
InTraffic	LB 到后端的入带宽	在统计粒度内,负载均衡流入到后端服务器所 用的带宽。	Mb ps	60、300
AccOuttraffi c	LB 到后端的出流量	在统计粒度内,后端服务器流出到负载均衡的 流量。 此指标仅公网负载均衡实例支持,内网负载均 衡不支持。	M B	10、60、300、 3600
DropTotalCo nns	丢弃连接数	在统计粒度内,负载均衡或监听器上丢弃的连 接数。 此指标仅标准账户类型支持,传统账户类型不 支持,账户类型判断方式请参见 判断账户类 型。	个/ 秒	10、60、300
InDropBits	丟弃入带宽	在统计粒度内,客户端通过外网访问负载均衡 时丢弃的带宽。 此指标仅标准账户类型支持,传统账户类型不 支持,账户类型判断方式请参见 判断账户类 型。	Bit/ s	10、60、300
OutDropBits	丟弃出带宽	在统计粒度内,负载均衡访问外网时丢弃的带 宽。 此指标仅标准账户类型支持,传统账户类型不 支持,账户类型判断方式请参见 判断账户类 型。	Bit/ s	10、60、300
InDropPkts	丟弃流入数据包	在统计粒度内,客户端通过外网访问负载均衡 时丢弃的数据包。 此指标仅标准账户类型支持,传统账户类型不 支持,账户类型判断方式请参见 判断账户类 型。	个/ 秒	10、60、300
OutDropPkts	丟弃流出数据包	在统计粒度内,负载均衡返回给客户端时被丢 弃的数据包。 此指标仅标准账户类型支持,传统账户类型不 支持,账户类型判断方式请参见 判断账户类 型。	个/ 秒	10、60、300
DropQps	丢弃请求数	在统计粒度内,负载均衡或监听器上丢弃的请 求数。 丢弃请求数是因客户后端服务器导致丢弃的请 求数。 此指标为七层监听器独有指标,仅标准账户类 型支持,传统账户类型不支持,账户类型判断	<b>^</b>	60、300

🕗 腾讯云



		方式请参见 判断账户类型 。		
IntrafficVipR atio	入带宽利用率	在统计粒度内,客户端通过外网访问负载均衡 所用的带宽利用率。 此指标仅标准账户类型支持,传统账户类型不 支持,账户类型判断方式请参见 判断账户类 型。 分子为当前入带宽,分母为实例当前设定的带 宽上限。	%	10、60、300
OuttrafficVip Ratio	出带宽利用率	在统计粒度内,负载均衡访问外网所用的带宽 使用率。 此指标仅标准账户类型支持,传统账户类型不 支持,账户类型判断方式请参见 判断账户类 型。 分子为当前出带宽,分母为实例当前设定的带 宽上限。	%	10、60、300
ReqAvg	平均请求时间	在统计粒度内,负载均衡的平均请求时间。 此指标为七层监听器独有指标。	毫 秒	60、300
ReqMax	最大请求时间	在统计粒度内,负载均衡的最大请求时间。 此指标为七层监听器独有指标。	毫 秒	60、300
RspAvg	平均响应时间	在统计粒度内,负载均衡的平均响应时间。 此指标为七层监听器独有指标。	毫 秒	60、300
RspMax	最大响应时间	在统计粒度内,负载均衡的最大响应时间。 此指标为七层监听器独有指标。	毫 秒	60、300
RspTimeout	响应超时个数	在统计粒度内,负载均衡响应超时的个数。 此指标为七层监听器独有指标。	个/ 分 钟	60、300
SuccReq	每分钟成功请求数	在统计粒度内,负载均衡每分钟的成功请求 数。 此指标为七层监听器独有指标。	个/ 分 钟	60、300
TotalReq	每秒请求数	在统计粒度内,负载均衡每秒钟的请求数。 每秒请求数是总请求数剔除超限导致丢弃请求 数之外的接收请求数,包含因客户后端服务器 导致丢弃的请求数。 此指标为七层监听器独有指标。	<b>^</b>	60、300
QpsVipRatio	QPS 利用率	在统计粒度内的某一时刻,负载均衡的 QPS 相比实例当前规格的 QPS 性能上限的利用 率。 此指标仅性能容量型实例与已限速的共享型实 例支持,该指标仅支持实例维度。	%	60、300
ClbHttp2xx	CLB 返回的 2xx 状态 码	在统计粒度内,负载均衡返回 2xx 状态码的 个数(负载均衡和后端服务器返回码之和 )。 此指标为七层监听器独有指标。	个/ 分 钟	60、300

ClbHttp3xx	CLB 返回的 3xx 状态 码	在统计粒度内,负载均衡返回 3xx 状态码的 个数(负载均衡和后端服务器返回码之和)。 此指标为七层监听器独有指标。	个/ 分 钟	60、300
ClbHttp4xx	CLB 返回的 4xx 状态 码	在统计粒度内,负载均衡返回 4xx 状态码的 个数(负载均衡和后端服务器返回码之和)。 此指标为七层监听器独有指标。	个/ 分 钟	60、300
ClbHttp5xx	CLB 返回的 5xx 状态 码	在统计粒度内,负载均衡返回 5xx 状态码的 个数(负载均衡和后端服务器返回码之和)。 此指标为七层监听器独有指标。	个/ 分 钟	60、300
ClbHttp404	CLB 返回的 404 状 态码	在统计粒度内,负载均衡返回 404 状态码的 个数(负载均衡和后端服务器返回码之和)。 此指标为七层监听器独有指标。	个/ 分 钟	60、300
ClbHttp499	CLB 返回的 499 状 态码	在统计粒度内,负载均衡返回 499 状态码的 个数(负载均衡和后端服务器返回码之和)。 此指标为七层监听器独有指标。	个/ 分 钟	60、300
ClbHttp502	CLB 返回的 502 状 态码	在统计粒度内,负载均衡返回 502 状态码的 个数(负载均衡和后端服务器返回码之和)。 此指标为七层监听器独有指标。	个/ 分 钟	60、300
ClbHttp503	CLB 返回的 503 状 态码	在统计粒度内,负载均衡返回 503 状态码的 个数(负载均衡和后端服务器返回码之和)。 此指标为七层监听器独有指标。	个/ 分 钟	60、300
ClbHttp504	CLB 返回的 504 状 态码	在统计粒度内,负载均衡返回 504 状态码的 个数(负载均衡和后端服务器返回码之和)。 此指标为七层监听器独有指标。	个/ 分 钟	60、300
ClbOther	CLB 返回的其他状态 码	在统计粒度内,负载均衡返回其他状态码的个 数(负载均衡和后端服务器返回码之和)。其 他状态码等于 CLB 返回的 1xx 状态码与 CLB 返回的 2xx 状态码之和。 此指标为七层监听器独有指标。	个/ 分 钟	60、300
Http2xx	2xx 状态码	在统计粒度内,后端服务器返回 2xx 状态码 的个数。 此指标为七层监听器独有指标。	个/ 分 钟	60、300
Http3xx	3xx 状态码	在统计粒度内,后端服务器返回 3xx 状态码 的个数。 此指标为七层监听器独有指标。	个/ 分 钟	60、300
Http4xx	4xx 状态码	在统计粒度内,后端服务器返回 4xx 状态码 的个数。 此指标为七层监听器独有指标。	个/ 分 钟	60、300
Http5xx	5xx 状态码	在统计粒度内,后端服务器返回 5xx 状态码 的个数。 此指标为七层监听器独有指标。	个/ 分 钟	60、300

🕗 腾讯云

负载均衡



Http404	404 状态码	在统计粒度内,后端服务器返回 404 状态码 的个数。 此指标为七层监听器独有指标。	个/ 分 钟	60、300
Http499	499 状态码	在统计粒度内,后端服务器返回 499 状态码 的个数。 此指标为七层监听器独有指标。	个/ 分 钟	60、300
Http502	502 状态码	在统计粒度内,后端服务器返回 502 状态码 的个数。 此指标为七层监听器独有指标。	个/ 分 钟	60、300
Http503	503 状态码	在统计粒度内,后端服务器返回 503 状态码 的个数。 此指标为七层监听器独有指标。	个/ 分 钟	60、300
Http504	504 状态码	在统计粒度内,后端服务器返回 504 状态码 的个数。 此指标为七层监听器独有指标。	个/ 分 钟	60、300
OverloadCur Conn	SNAT 并发连接数	在统计周期内,负载均衡的 SNAT IP 每分钟 的并发连接数。 此指标处于内测阶段,如需使用,请提交 内 <mark>测申请</mark> 。	个/ 分 钟	60
ConnRatio	SNAT 端口使用率	在统计周期内,负载均衡的 SNAT IP 的端口 使用率。 端口使用率 = SNAT 并发连接数 / (SNAT IP 数 × 55000 × 服务器个数)。 此指标处于内测阶段,如需使用,请提交内 测申请。	%	60
SnatFail	SNAT 失败数	在统计周期内,负载均衡的 SNAT IP 与后端 服务器每分钟建立连接的失败次数。 此指标处于内测阶段,如需使用,请提交 内 <mark>测申请</mark> 。	个/ 分 钟	60
HealthRsCo unt	健康检查正常数	在统计周期内,负载均衡的健康检查正常个 数。	个	60、300
UnhealthRs Count	健康检查异常数	在统计周期内,负载均衡的健康检查异常个 数。	个	60、300

# 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。
- 后端服务器维度。
- 后端服务的端口维度。

```
🕛 说明:
```

UPD 连接数是将 UDP 包按照源 IP - 源 Port - 目标 IP - 目标 Port 四元算作连接。



指标英文名	指标中文名	指标说明	单位	统计粒度(秒)
ClientConnu m	客户端到 LB 的活跃连 接数	在统计粒度内的某一时刻,从客户端到负载均 衡或监听器上的活跃连接数。	个	10、60、300
ClientNewCo nn	客户端到 LB 的新建连 接数	在统计粒度内,从客户端到负载均衡或监听器 上的新建连接数。	个/秒	10、60、300
ClientInpkg	客户端到 LB 的入包量	在统计粒度内,客户端向负载均衡每秒发送的 数据包数量。	个/秒	10、60、300
ClientOutpkg	客户端到 LB 的出包量	在统计粒度内,负载均衡向客户端每秒发送的 数据包数量。	个/秒	10、60、300
ClientAccIntr affic	客户端到 LB 的入流量	在统计粒度内,客户端流入到负载均衡的流 量。	MB	10、60、300
ClientAccOu ttraffic	客户端到 LB 的出流量	在统计粒度内,负载均衡流出到客户端的流 量。	MB	10、60、300
ClientOuttraf fic	客户端到 LB 的出带宽	在统计粒度内,负载均衡流出到客户端所用的 带宽。	Mbp s	10、60、300
ClientIntraffi c	客户端到 LB 的入带宽	在统计粒度内,客户端流入到负载均衡所用的 带宽。	Mbp s	10、60、300
OutTraffic	LB 到后端的出带宽	在统计粒度内,后端服务器流出到负载均衡所 用的带宽。	Mbp s	60、300
InTraffic	LB 到后端的入带宽	在统计粒度内,负载均衡流入到后端服务器所 用的带宽。	Mbp s	60、300
OutPkg	LB 到后端的出包量	在统计粒度内,后端服务器向负载均衡每秒发 送的数据包数量。	个/秒	60、300
InPkg	LB 到后端的入包量	在统计粒度内,负载均衡向后端服务器每秒发 送的数据包数量。	个/秒	60、300
AccOuttraffi c	LB 到后端的出流量	在统计粒度内,后端服务器流出到负载均衡的 流量。 此指标仅公网负载均衡实例支持,内网负载均 衡不支持。	MB	10、60、300、 3600
ConNum	LB 到后端的连接数	在统计粒度内,从负载均衡到后端服务器的连 接数。	个	60、300
NewConn	LB 到后端的新建连接 数	在统计粒度内,从负载均衡到后端服务器的新 建连接数。	个/分 钟	60、300
HealthRsCo unt	健康检查正常数	在统计周期内,负载均衡的健康检查正常个 数。	个	60、300
UnhealthRs Count	健康检查异常数	在统计周期内,负载均衡的健康检查异常个 数。	个	60、300



# 七层监听器(HTTP/HTTPS)维度

七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。
- 后端服务器维度。
- 后端服务的端口维度。

指标英文名	指标中文名	指标说明	单 位	统计粒度(秒)
ClientConnu m	客户端到 LB 的活跃连 接数	在统计粒度内的某一时刻,从客户端到负载均 衡或监听器上的活跃连接数。	个	10、60、300
ClientNewCo nn	客户端到 LB 的新建连 接数	在统计粒度内,从客户端到负载均衡或监听器 上的新建连接数。	个/ 秒	10、60、300
ClientInpkg	客户端到 LB 的入包量	在统计粒度内,客户端向负载均衡每秒发送的 数据包数量。	个/ 秒	10、60、300
ClientOutpkg	客户端到 LB 的出包量	在统计粒度内,负载均衡向客户端每秒发送的 数据包数量。	个/ 秒	10、60、300
ClientAccIntr affic	客户端到 LB 的入流量	在统计粒度内,客户端流入到负载均衡的流 量。	M B	10、60、300
ClientAccOu ttraffic	客户端到 LB 的出流量	在统计粒度内,负载均衡流出到客户端的流 量。	M B	10、60、300
ClientOuttraf fic	客户端到 LB 的出带宽	在统计粒度内,负载均衡流出到客户端所用的 带宽。	Mb ps	10、60、300
ClientIntraffi c	客户端到 LB 的入带宽	在统计粒度内,客户端流入到负载均衡所用的 带宽。	Mb ps	10、60、300
OutTraffic	LB 到后端的出带宽	在统计粒度内,后端服务器流出到负载均衡所 用的带宽。	Mb ps	60、300
InTraffic	LB 到后端的入带宽	在统计粒度内,负载均衡流入到后端服务器所 用的带宽。	Mb ps	60、300
OutPkg	LB 到后端的出包量	在统计粒度内,后端服务器向负载均衡每秒发 送的数据包数量。	个/ 秒	60、300
InPkg	LB 到后端的入包量	在统计粒度内,负载均衡向后端服务器每秒发 送的数据包数量。	个/ 秒	60、300
AccOuttraffi c	LB 到后端的出流量	在统计粒度内,后端服务器流出到负载均衡的 流量。 此指标仅公网负载均衡实例支持,内网负载均 衡不支持。	M B	10、60、300、 3600
ConNum	LB 到后端的连接数	在统计粒度内,从负载均衡到后端服务器的连 接数。	个	60、300



NewConn

ReqAvg

ReqMax

RspAvg

LB 到后端的新建连接

平均请求时间

最大请求时间

平均响应时间

数

		负载均征
在统计粒度内,从负载均衡到后端服务器的新 建连接数。	个/ 分 钟	60、300
在统计粒度内,负载均衡的平均请求时间。 此指标为七层监听器独有指标。	毫 秒	60、300
在统计粒度内,负载均衡的最大请求时间。 此指标为七层监听器独有指标。	毫 秒	60、300
在统计粒度内,负载均衡的平均响应时间。 此指标为七层监听器独有指标。	毫 秒	60、300
在统计粒度内,负载均衡的最大响应时间。 此指标为七层监听器独有指标。	毫 秒	60、300
在统计粒度内,负载均衡响应超时的个数。 此指标为七层监听器独有指标。	个/ 分 钟	60、300
在统计粒度内,负载均衡每分钟的成功请求 数。 此指标为七层监听器独有指标。	个/ 分 钟	60、300
在统计粒度内,负载均衡每秒钟的请求数。 每秒请求数是总请求数剔除超限导致丢弃请求 数之外的接收请求数,包含因客户后端服务器	个	60、300

RspMax	最大响应时间	在统计粒度内,负载均衡的最大响应时间。 此指标为七层监听器独有指标。	毫 秒	60、300
RspTimeout	响应超时个数	在统计粒度内,负载均衡响应超时的个数。 此指标为七层监听器独有指标。	个/ 分 钟	60、300
SuccReq	每分钟成功请求数	在统计粒度内,负载均衡每分钟的成功请求 数。 此指标为七层监听器独有指标。	个/ 分 钟	60、300
TotalReq	每秒请求数	在统计粒度内,负载均衡每秒钟的请求数。 每秒请求数是总请求数剔除超限导致丢弃请求 数之外的接收请求数,包含因客户后端服务器 导致丢弃的请求数。 此指标为七层监听器独有指标。	<b>^</b>	60、300
QpsVipRatio	QPS 利用率	在统计粒度内的某一时刻,负载均衡的 QPS 相比实例当前规格的 QPS 性能上限的利用 率。 此指标仅性能容量型实例与已限速的共享型实 例支持,该指标仅支持实例维度。	%	60、300
DropQps	丟弃请求数	在统计粒度内,负载均衡或监听器上丢弃的请 求数。 丢弃请求数是因客户后端服务器导致丢弃的请 求数。 此指标为七层监听器独有指标,仅标准账户类 型支持,传统账户类型不支持,账户类型判断 方式请参见 判断账户类型。	Ŷ	60、300
ClbHttp2xx	CLB 返回的 2xx 状态 码	在统计粒度内,负载均衡返回 2xx 状态码的 个数(负载均衡和后端服务器返回码之和 )。 此指标为七层监听器独有指标。	个/ 分 钟	60、300
ClbHttp3xx	CLB 返回的 3xx 状态 码	在统计粒度内,负载均衡返回 3xx 状态码的 个数(负载均衡和后端服务器返回码之和 )。 此指标为七层监听器独有指标。	个/ 分 钟	60、300
ClbHttp4xx	CLB 返回的 4xx 状态 码	在统计粒度内,负载均衡返回 4xx 状态码的 个数(负载均衡和后端服务器返回码之和 )。 此指标为七层监听器独有指标。	个/ 分 钟	60、300

ClbHttp5xx	CLB 返回的 5xx 状态 码	在统计粒度内,负载均衡返回 5xx 状态码的 个数(负载均衡和后端服务器返回码之和 )。 此指标为七层监听器独有指标。	个/ 分 钟	60、300
ClbHttp404	CLB 返回的 404 状 态码	在统计粒度内,负载均衡返回 404 状态码的 个数(负载均衡和后端服务器返回码之和)。 此指标为七层监听器独有指标。	个/ 分 钟	60、300
ClbHttp499	CLB 返回的 499 状 态码	在统计粒度内,负载均衡返回 499 状态码的 个数(负载均衡和后端服务器返回码之和 )。 此指标为七层监听器独有指标。	个/ 分 钟	60、300
ClbHttp502	CLB 返回的 502 状 态码	在统计粒度内,负载均衡返回 502 状态码的 个数(负载均衡和后端服务器返回码之和)。 此指标为七层监听器独有指标。	个/ 分 钟	60、300
ClbHttp503	CLB 返回的 503 状 态码	在统计粒度内,负载均衡返回 503 状态码的 个数(负载均衡和后端服务器返回码之和 )。 此指标为七层监听器独有指标。	个/ 分 钟	60、300
ClbHttp504	CLB 返回的 504 状 态码	在统计粒度内,负载均衡返回 504 状态码的 个数(负载均衡和后端服务器返回码之和 )。 此指标为七层监听器独有指标。	个/ 分 钟	60、300
ClbOther	CLB 返回的其他状态 码	在统计粒度内,负载均衡返回其他状态码的个 数(负载均衡和后端服务器返回码之和)。其 他状态码等于 CLB 返回的 1xx 状态码与 CLB 返回的 2xx 状态码之和。 此指标为七层监听器独有指标。	个/ 分 钟	60、300
Http2xx	2xx 状态码	在统计粒度内,后端服务器返回 2xx 状态码 的个数。 此指标为七层监听器独有指标。	个/ 分 钟	60、300
Http3xx	3xx 状态码	在统计粒度内,后端服务器返回 3xx 状态码 的个数。 此指标为七层监听器独有指标。	个/ 分 钟	60、300
Http4xx	4xx 状态码	在统计粒度内,后端服务器返回 4xx 状态码 的个数。 此指标为七层监听器独有指标。	个/ 分 钟	60、300
Http5xx	5xx 状态码	在统计粒度内,后端服务器返回 5xx 状态码 的个数。 此指标为七层监听器独有指标。	个/ 分 钟	60、300
Http404	404 状态码	在统计粒度内,后端服务器返回 404 状态码 的个数。 此指标为七层监听器独有指标。	个/ 分 钟	60、300
Http499	499 状态码	在统计粒度内,后端服务器返回 499 状态码 的个数。 此指标为七层监听器独有指标。	个/ 分 钟	60、300



Http502	502 状态码	在统计粒度内,后端服务器返回 502 状态码 的个数。 此指标为七层监听器独有指标。	个/ 分 钟	60、300
Http503	503 状态码	在统计粒度内,后端服务器返回 503 状态码 的个数。 此指标为七层监听器独有指标。	个/ 分 钟	60、300
Http504	504 状态码	在统计粒度内,后端服务器返回 504 状态码 的个数。 此指标为七层监听器独有指标。	个/ 分 钟	60、300
HealthRsCo unt	健康检查正常数	在统计周期内,负载均衡的健康检查正常个 数。	个	60、300
UnhealthRs Count	健康检查异常数	在统计周期内,负载均衡的健康检查异常个 数。	个	60、300

#### () 说明:

如果您需要查看某监听器下某台后端服务器的监控数据,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。

# 相关文档

公网负载均衡监控指标



# 配置告警策略

最近更新时间: 2025-05-23 19:48:02

本文介绍如何创建告警策略。

# 应用场景

您可以针对腾讯云可观测平台支持的监控类型设置性能消耗类指标的阈值告警,在发生异常时及时通知您采取措施。告警策略包括名称、策略类型和告警触发条件、告警对象、告警通知模板五个必要组成部分。您可以根据以下指引进行告警策略的创建。

#### 基本概念

术语	定义
告警策略	由告警名称、告警策略类型、告警触发条件、告警对象和告警通知模板组成。
告警策略类型	告警策略类型用于标识策略分类,类型与云产品对应。例如:当您选择云服务器策略,即可自定义 CPU 使用率、磁盘使用率等指标告警。
告警触发条件	是指标、比较关系、阈值、统计粒度和持续 N 个监控数据点组成的一个有语义的条件。
监控类型	包含云产品监控、应用性能监控、前端性能监控、云拨测和终端性能监控。
通知模板	多个策略一键复用模板,适用于多种场景接收告警通知,详情请参见 新建告警通知模板 。

## 操作步骤

#### 1. 登录 腾讯云可观测平台。

#### 2. 单击告警管理 > 告警配置,进入告警策略配置页面。

3. 单击新建策略, 配置告警策略, 配置说明如下:

配置类 型	配置项	说明
基本信	策略名称	自定义策略名称。
息	备注	自定义策略备注。
配置告 监控类型		支持云产品监控、应用性能监控、前端性能监控、云拨测和终端性能监控。
警规则	策略类型	选择您需要监控的云产品策略类型。
	策略所属项 目	选择策略所属项目后,该策略权限将和项目权限保持一致,如需创建项目,请参见 项目管理 。 同时方便您根据项目对策略进行管理。
	所属标签	选择策略所属标签后,方便您根据标签对策略进行管理。支持为策略关联多个标签。如需创建标 签,请参见 <mark>标签管理</mark> 。
	告警对象	不同云产品策略支持的告警对象维度不同,部分云产品策略仅支持通过单一维度对告警对象进行 筛选,部分云产品策略支持通过多种字段对告警对象进行筛选,可以更精准地匹配和触发告警规 则。 单一告警对象:您可根据实例 ID、实例分组、标签筛选告警对象,也可以直接选择全部实例对 象作为告警对象。标签功能方便您快速筛选绑定标签下的云资源,实现标签下实例增减时,告警

		策略同时更新,减少告警策略二次修改成本 。 多维告警对象:您可根据地域、集群、节点等多种字段来对告警对象进行筛选,并且可以对筛选 字段进行组合,多种字段的组合可以帮助您定义更复杂的告警条件。
	触发条件	告警触发条件是指标、比较关系、阈值、统计粒度和持续 N 个监控数据点组成的一个有语义的 条件。您可以自定义设置指标告警和事件告警触发条件,根据业务需求配置告警指标、统计粒 度、告警阈值、告警分级和告警频率,也可以直接使用触发条件模板和预置触发条件,请参见 配置告警触发条件。
配置告 警通知	告警通知模 板	支持选择系统预设通知模板和用户自定义通知模板,每个告警策略最多只能绑定三个通知模板, 详情请参见 <mark>告警通知</mark> 。
高级配 置	弹性伸缩	部分云产品支持启用弹性伸缩,授权并配置成功后,达到告警条件可触发弹性伸缩策略。

4. 配置完以上信息后单击完成,即成功创建告警策略。



# 告警指标说明

最近更新时间: 2025-05-23 19:48:02

#### 基本说明

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。更多内容请参见 告警概述,配置告警最佳实践可参见 负载均衡 <mark>配置监控告警最佳实践</mark> 。

负载均衡的告警策略包括如下类型:

- 公网负载均衡实例
- 内网负载均衡实例
- 七层监听器
- 四层监听器
- 后端服务器端口

### 实例维度告警策略说明

告警策略类型	告警策略	告警指标	单位
公网负载均衡实例	客户端到 LB 的监控	客户端到 LB 的出带宽	Mbps
		客户端到 LB 的入带宽	Mbps
		客户端到 LB 的连接数	Count
		客户端到 LB 的非活跃连接 数	Count
		客户端到 LB 的并发连接数	Count
		客户端到 LB 的新建连接数	Count/s
		客户端到 LB 的入包量	Count/s
		客户端到 LB 的出包量	Count/s
	LB 到后端的监控	公网出流量	MB
		公网新建连接数	Count/s
		公网连接数	Count
		公网出带宽	Mbps
		公网入带宽	Mbps
		公网出包量	Count/s
		公网入包量	Count/s
	QPS 相关监控	每秒请求数	Count/s



		QPS 利用率	%
		丟弃 QPS	Count/s
		新建连接数利用率	%
		并发连接数利用率	%
		出带宽利用率	%
		入带宽利用率	%
	丢弃/利用率监控	丟弃出带宽	Bit/s
		丢弃入带宽	Bit/s
		丢弃连接数	Count/s
		丟弃流出数据包	Count/s
		丟弃流入数据包	Count/s
内网负载均衡实例		客户端到 LB 的出带宽	Mbps
		客户端到 LB 的入带宽	Mbps
	客户端到 LB 的监控	客户端到 LB 的连接数	Count
		客户端到 LB 的非活跃连接 数	Count
		客户端到 LB 的并发连接数	Count
		客户端到 LB 的新建连接数	Count/s
		客户端到 LB 的入包量	Count/s
		客户端到 LB 的出包量	Count/s
	LB 到后端的监控	入带宽	Mbps
		出带宽	Mbps
	QPS 相关监控	每秒请求数	Count/s
		QPS 利用率	%
		丢弃 QPS	Count
	丢弃/利用率监控	新建连接数利用率	%
		并发连接数利用率	%
		出带宽利用率	%
		入带宽利用率	%
		丢弃出带宽	Bit/s



丢弃入带宽	Bit/s
丢弃连接数	Count/s
丢弃流出数据包	Count/s
丟弃流入数据包	Count/s

# 监听器维度告警策略说明

告警策略类型	告警策略	告警指标	单位
四层监听器	客户端到内网 LB 的监控	客户端到 LB 的出带宽	Mbps
		客户端到 LB 的入带宽	Mbps
		客户端到 LB 的连接数	Count
		客户端到 LB 的非活跃连接 数	Count
		客户端到 LB 的并发连接数	Count
		客户端到 LB 的新建连接数	Count/s
		客户端到 LB 的入包量	Count/s
		客户端到 LB 的出包量	Count/s
	内网 LB 到后端的监控	入包量	Count/s
		出包量	Count/s
		入带宽	Mbps
		出带宽	Mbps
		新建连接数	Count/min
		并发连接数	Count
	客户端到公网 LB 的监控	客户端到 LB 的出带宽	Mbps
		客户端到 LB 的入带宽	Mbps
		客户端到 LB 的连接数	Count
		客户端到 LB 的非活跃连接 数	Count
		客户端到 LB 的并发连接数	Count
		客户端到 LB 的新建连接数	Count/s
		客户端到 LB 的入包量	Count/s
		客户端到 LB 的出包量	Count/s



		入包量	Count/s
		出包量	Count/s
		入带宽	Mbps
	公网 LB 到后端的监控	出带宽	Mbps
		公网连接数	Count
		新建连接数	Count/s
		非活跃连接数	Count
七层监听器		客户端到 LB 的出带宽	Mbps
		客户端到 LB 的入带宽	Mbps
		客户端到 LB 的连接数	Count
	客户端到内网 LB 的监控	客户端到 LB 的非活跃连接 数	Count
		客户端到 LB 的并发连接数	Count
		客户端到 LB 的新建连接数	Count/s
		客户端到 LB 的入包量	Count/s
		客户端到 LB 的出包量	Count/s
	内网 LB 到后端的监控	clb 返回的 2xx 状态码	Count/min
		clb 返回的 3xx 状态码	Count/min
		clb 返回的 4xx 状态码	Count/min
		clb 返回的 5xx 状态码	Count/min
		clb 返回的 404 状态码	Count/min
		clb 返回的 499 状态码	Count/min
		clb 返回的 502 状态码	Count/min
		clb 返回的 503 状态码	Count/min
		clb 返回的 504 状态码	Count/min
		其他状态码	Count/min
		2xx 状态码	Count/min
		3xx 状态码	Count/min
		4xx 状态码	Count/min
		5xx 状态码	Count/min



	404 状态码	Count/min
	499 状态码	Count/min
	502 状态码	Count/min
	503 状态码	Count/min
	504 状态码	Count/min
	平均响应时间	ms
	最大响应时间	ms
	平均请求时间	ms
	响应超时个数	Count/min
	请求最大时延	ms
	每秒请求数	Count/s
	每分钟成功请求数	Count/min
	丟弃 QPS	Count/s
	客户端到 LB 的出带宽	Mbps
	客户端到 LB 的入带宽	Mbps
	客户端到 LB 的连接数	Count
客户端到公网 LB 的监控	客户端到 LB 的非活跃连接 数	Count
	客户端到 LB 的并发连接数	Count
	客户端到 LB 的新建连接数	Count/s
	客户端到 LB 的入包量	Count/s
	客户端到 LB 的出包量	Count/s
公网 LB 到后端的监控	clb 返回的 2xx 状态码	Count/min
	clb 返回的 3xx 状态码	Count/min
	clb 返回的 4xx 状态码	Count/min
	clb 返回的 5xx 状态码	Count/min
	clb 返回的 404 状态码	Count/min
	clb 返回的 499 状态码	Count/min
	clb 返回的 502 状态码	Count/min
	clb 返回的 503 状态码	Count/min



clb 返回的 504 状态码	Count/min
其他状态码	Count/min
2xx 状态码	Count/min
3xx 状态码	Count/min
4xx 状态码	Count/min
5xx 状态码	Count/min
404 状态码	Count/min
499 状态码	Count/min
502 状态码	Count/min
503 状态码	Count/min
504 状态码	Count/min
平均响应时间	ms
最大响应时间	ms
平均请求时间	ms
响应超时个数	Count/min
最大请求时间	ms
每秒请求数	Count/s
活跃连接数	Count
新建连接数	Count/min
入包量	Count/s
出包量	Count/s
出带宽	bps
入带宽	bps

# 后端服务器端口维度告警策略说明

告警策略类型	告警策略	告警指标	单位
后端服务器端口	监听器维度	服务器端口异常数	Count
		健康检查正常 RS 数	Count
	后端服务器端口维度	服务器端口状态异常数	Count

# 🔗 腾讯云

#### ▲ 注意:

- 1. 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。
- 监听器维度的统计包含该监听器下所有后端服务的端口状态,从单一告警收敛到阈值告警,为降低网络抖动的影响,建议您 使用监听器维度的告警。

# 访问管理 概述

最近更新时间:2024-08-14 16:46:51

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。

• 您无法限制其他人的访问权限,易产生误操作造成安全风险。

访问管理(CAM )用于管理腾讯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

腾讯云资源归属、资源使用计量计费的基本主体,可登录腾讯云服务。

○ 子账号

由根账号创建账号,有确定的身份 ID 和身份凭证,且能登录到腾讯云控制台。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,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
了解还有哪些产品支持 CAM	支持 CAM 的云服务列表



# 授权定义

最近更新时间: 2023-10-09 11:06:54

# 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	<pre>qcs::clb:\$region::clb/\$loadbalancerid</pre>
负载均衡后端服务器	<pre>qcs::cvm:\$region:\$account:instance/\$cvminstanceid</pre>

#### 其中:

- 所有 \$region 应为某个 region 的 ID, 可以为空。
- 所有 <code>\$account</code> 应为资源拥有者的 Accountld, 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	<pre>qcs:\$projectid:clb:\$region:\$account:clb/*</pre>
DeleteLoadBalancers	删除负载均衡	<pre>qcs::clb:\$region:\$account:clb/\$loadbalanceri d</pre>
ModifyLoadBalancerAttrib utes	修改负载均衡属性信息	<pre>qcs::clb:\$region:\$account:clb/\$loadbalanceri d</pre>
ModifyForwardLBName	修改负载均衡的名字	<pre>qcs::clb:\$region:\$account:clb/\$loadbalanceri d</pre>
SetLoadBalancerSecurity Groups	设置负载均衡实例的安 全组	<pre>qcs::clb:\$region:\$account:clb/\$loadbalanceri d</pre>

#### 监听器相关

API 操作	资源描述	接口说明
DeleteLoadBalancerListene rs	删除负载均衡监听器	<pre>qcs::clb:\$region:\$account:clb/\$loadba lancerid</pre>



DescribeLoadBalancerListe ners	获取负载均衡监听器列表	<pre>qcs::clb:\$region:\$account:clb/\$loadba lancerid</pre>
ModifyLoadBalancerListene r	修改负载均衡监听器属性	<pre>qcs::clb:\$region:\$account:clb/\$loadba lancerid</pre>
CreateLoadBalancerListene rs	创建负载均衡监听器	<pre>qcs::clb:\$region:\$account:clb/\$loadba lancerid</pre>
DeleteForwardLBListener	删除负载均衡监听器(四层和 七层)	<pre>qcs::clb:\$region:\$account:clb/\$loadba lancerid</pre>
ModifyForwardLBSeventhLi stener	修改负载均衡七层监听的属性	<pre>qcs::clb:\$region:\$account:clb/\$loadba lancerid</pre>
ModifyForwardLBFourthList ener	修改负载均衡四层监听器属性	<pre>qcs::clb:\$region:\$account:clb/\$loadba lancerid</pre>
DescribeForwardLBListener s	查询负载均衡监听器列表	<pre>qcs::clb:\$region:\$account:clb/\$loadba lancerid</pre>
CreateForwardLBSeventhL ayerListeners	创建七层负载均衡监听器	<pre>qcs::clb:\$region:\$account:clb/\$loadba lancerid</pre>
CreateForwardLBFourthLay erListeners	创建四层负载均衡监听器	<pre>qcs::clb:\$region:\$account:clb/\$loadba lancerid</pre>

## 负载均衡域名 + URL 相关

API 操作	资源描述	接口说明
ModifyForwardLBRule sDomain	修改负载均衡监听器转发规则的域名	<pre>qcs::clb:\$region:\$account:clb/\$loadbal ancerid</pre>
CreateForwardLBListe nerRules	创建负载均衡监听器转发规则	<pre>qcs::clb:\$region:\$account:clb/\$loadbal ancerid</pre>
DeleteForwardLBListe nerRules	删除七层负载均衡监听器规则	<pre>qcs::clb:\$region:\$account:clb/\$loadbal ancerid</pre>
DeleteRewrite	删除负载均衡转发规则之间的重定向 关系	<pre>qcs::clb:\$region:\$account:clb/\$loadbal ancerid</pre>
ManualRewrite	手动添加负载均衡转发规则的重定向 关系	<pre>qcs::clb:\$region:\$account:clb/\$loadbal ancerid</pre>
AutoRewrite	自动生成负载均衡转发规则的重定向 关系	<pre>qcs::clb:\$region:\$account:clb/\$loadbal ancerid</pre>

## 后端服务器相关



API操作	资源描述	接口说明
ModifyLoadBalancerBacken ds	修改负载均衡器后端服务器权 重	<pre>qcs::clb:\$region:\$account:clb/\$loadbal ancerid</pre>
DescribeLoadBalancerBack ends	获取负载均衡绑定的后端服务 器列表	<pre>qcs::clb:\$region:\$account:clb/\$loadbal ancerid</pre>
DeregisterInstancesFromLo adBalancer	解绑后端服务器	<pre>qcs::clb:\$region:\$account:clb/\$loadbal ancerid qcs::cvm:\$region:\$account:instance/\$cv minstanceid</pre>
RegisterInstancesWithLoad Balancer	绑定后端服务器到负载均衡	<pre>qcs::clb:\$region:\$account:clb/\$loadbal ancerid qcs::cvm:\$region:\$account:instance/\$cv minstanceid</pre>
DescribeLBHealthStatus	查询负载均衡健康状态	<pre>qcs::clb:\$region:\$account:clb/\$loadbal ancerid</pre>
ModifyForwardFourthBacke ndsPort	修改四层监听器转发规则上云 服务器的端口	<pre>qcs::clb:\$region:\$account:clb/\$loadbal ancerid qcs::cvm:\$region:\$account:instance/\$cv minstanceid</pre>
ModifyForwardFourthBacke ndsWeight	修改四层监听器转发规则上云 服务器的权重	<pre>qcs::clb:\$region:\$account:clb/\$loadbal ancerid qcs::cvm:\$region:\$account:instance/\$cv minstanceid</pre>
RegisterInstancesWithForw ardLBSeventhListener	绑定云服务器到负载均衡七层 监听器的转发规则上	<pre>qcs::clb:\$region:\$account:clb/\$loadbal ancerid qcs::cvm:\$region:\$account:instance/\$cv minstanceid</pre>
RegisterInstancesWithForw ardLBFourthListener	绑定云服务器到负载均衡四层 监听器的转发规则上	<pre>qcs::clb:\$region:\$account:clb/\$loadbal ancerid qcs::cvm:\$region:\$account:instance/\$cv minstanceid</pre>
DeregisterInstancesFromFo rwardLBFourthListener	解绑负载均衡四层监听器转发 规则上的云服务器	<pre>qcs::clb:\$region:\$account:clb/\$loadbal ancerid qcs::cvm:\$region:\$account:instance/\$cv minstanceid</pre>



DeregisterInstancesFromFo rwardLB	解绑负载均衡七层监听器转发 规则上的云服务器	<pre>qcs::clb:\$region:\$account:clb/\$loadbal ancerid qcs::cvm:\$region:\$account:instance/\$cv minstanceid</pre>
ModifyForwardSeventhBac kends	修改七层监听器转发规则上云 服务器的权重	<pre>qcs::clb:\$region:\$account:clb/\$loadbal ancerid qcs::cvm:\$region:\$account:instance/\$cv minstanceid</pre>
ModifyForwardSeventhBac kendsPort	修改七层监听器转发规则上云 服务器的端口	<pre>qcs::clb:\$region:\$account:clb/\$loadbal ancerid qcs::cvm:\$region:\$account:instance/\$cv minstanceid</pre>
DescribeForwardLBBacken ds	查询负载均衡云服务器列表	<pre>qcs::clb:\$region:\$account:clb/\$loadbal ancerid qcs::cvm:\$region:\$account:instance/*</pre>
DescribeForwardLBHealthS tatus	查询负载均衡健康检查状态	<pre>qcs::clb:\$region:\$account:clb/*</pre>
ModifyLoadBalancerRulesP robe	修改负载均衡监听器转发规则 的健康检查及转发路径	<pre>qcs::clb:\$region:\$account:clb/\$loadbal ancerid</pre>


# 策略示例

最近更新时间: 2025-06-03 10:54:02

# 所有 CLB 的全读写策略

## 操作场景

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

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

## 操作步骤

- 1. 登录访问管理控制台,选择左侧导航栏中的策略。
- 2. 在策略管理页面,选择 QcloudCLBFullAccess 策略行的关联用户/组/角色。

访问管理	策略	CAM策略使用说明 ピ
計 概覧 用户 → 、 用户组	<ul> <li>① 用户或者用户组与策略关联后,即可获得策略所描述约操作权限。</li> <li>新建自定义策略 删除 批量授权</li> </ul>	全部策略 自定义策略 QcloudCLBFullAccess Q ③ と
○ 東朝 注 角色 ⊡ 身份提供商 ∨	策略名         服务类型 丁         描述           Octant/O Epullacease         免費快速 (/(18) 全津空防御府職	上次修改时间 操作
□。联合账号 ∨ (p) 访问密钥 ∨	已造 0 项, 共 1 项	10 ¥ 条/页 K ◀ 1 /1页 ▶ H

 在关联用户/用户组/角色弹窗中,勾选需对 CLB 服务拥有全读写权限的账号,单击确定,即可完成子账号对 CLB 服务全读写权限 的配置。

# 所有 CLB 的只读策略

### 操作场景

- 授权子账户只读访问 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: QcloudCLBReadOnlyAccess

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

## 操作步骤

- 1. 登录 访问管理控制台,选择左侧导航栏中的策略。
- 2. 在策略管理页面,选择 QcloudCLBReadOnlyAccess 策略行的关联用户/用户组/角色。

新建自定义策略 影除 批量授权			全部温暖 预设策略 自定义策略	QcloudCLBReadOnlyAccess O Q
策略名	服务类型 丁	描述	上次傳改时间	攝作
QcloudCLBReadOnlyAccess		负载均衡(CLB)只读访问权限	2020-09-29 11:37:49	关联用户/组/角色
已选 0 项, 共 1 项				10 ∨ 奈/页 ⊨ ◀ 1 /1页 ▶ ⊨

 在关联用户/用户组/角色弹窗中,勾选需对 CLB 服务拥有只读权限的账号,并单击确定,即可完成子账号对 CLB 服务只读权限的 配置。

# 某个标签下 CLB 的全读写策略

- 授权一个子账户对某个标签(标签键为 tagkey,标签值为 tagvalue)下的 CLB 的完全管理权限(管理实例、管理监听器等全部 操作),关于标签请参见 基于标签管理项目资源。
- CLB 实例支持配置标签和使用标签鉴权。



# 私有网络的相关策略

如果您希望用户可以查看 CLB 控制台中的私有网络信息,可先将以下操作添加到您策略中,再将该策略关联到该用户。

# 🔗 腾讯云

- DescribeVpcPrivateIPResources: 查看 VPC IP 资源详情
- DescribeOverseaAccelerator: 查询海外加速域名
- DescribeCustomerGateways: 查询对端网关
- DescribeAddresses: 查询弹性公网IP列表
- DescribeNetworkInterfaces: 查询弹性网卡列表
- DescribeCcnAttachedInstances: 查询云联网关联实例列表
- DescribeSecurityGroupLimits: 查询用户安全组配额
- DescribeBandwidthPackages: 查询带宽包资源
- DescribeServiceTemplates: 查询协议端口模板
- DescribeAddressTemplateGroups: 查询 IP 地址模板集合
- DescribeAddressTemplates: 查询 IP 地址模板
- DescribeServiceTemplateGroups: 查询协议端口模板集合

```
具体操作步骤如下:
```

1. 根据 策略,创建一个可以查看 CLB 控制台中的私有网络 VPC IP 资源和弹性公网 IP 列表信息的自定义策略。 策略内容可参考以下策略语法进行设置:

```
{
    "version": "2.0",
    "statement": [{
        "action": [
            "vpc:DescribeVpcPrivateIPResources",
            "vpc:DescribeAddresses"
        ],
        "resource": "*",
        "effect": "allow"
    }]
}
```

- 2. 找到创建的策略,在该策略行的操作列中,单击关联用户/组/角色。
- 3. 在弹出的关联用户/用户组/角色窗口中,选择您需要授权的用户/组,单击确定。

# 标签的相关策略

如果您希望用户可以查看 CLB 控制台中的标签信息,可先将以下操作添加到您的策略中,再将该策略关联到该用户。

- GetTags:获取标签列表
- GetTagKeys: 查询标签键列表
- GetTagValues: 查询标签值列表
- AddResourceTag: 标签关联资源
- DescribeEffectivePolicy: 查询目标节点的有效策略
- UnTagResources: 资源解除关联标签

```
具体操作步骤如下:
```

根据 策略,创建一个自定义策略。
 该策略允许用户在 CLB 控制台中具有查看标签键和标签值信息的权限。策略内容可参考以下策略语法进行设置:



"tag:GetTagKeys",	
"tag:GetTagValues"	

- 2. 找到创建的策略,在该策略行的操作列中,单击关联用户/组/角色。
- 3. 在弹出的关联用户/用户组/角色窗口中,选择您需要授权的用户/组,单击确定。

# SSL 证书的相关策略

如果您希望用户可以查看并使用 CLB 控制台中的 SSL 证书信息,可先将以下操作添加到您的策略中,再将该策略关联到该用户。

- UploadCertificate: 上传证书
- DescribeCertificates: 获取证书列表
- DescribeCertificateDetail: 获取证书详情
- ModifyCertificateAlias: 修改证书备注

具体操作步骤如下:

1. 根据 策略,创建一个自定义策略。

该策略允许用户在 CLB 控制台中具有查看 SSL 证书列表和证书详情的权限。策略内容可参考以下策略语法进行设置:



2. 找到创建的策略,在该策略行的操作列中,单击关联用户/组/角色。

3. 在弹出的关联用户/用户组/角色窗口中,选择您需要授权的用户/组,单击确定。

# CLS 日志的相关策略

如果您希望用户可以查看并使用 CLB 控制台中的 CLS 日志信息,可先将以下操作添加到您的策略中,再将该策略关联到该用户。



- DescribeLogsets: 获取日志集列表
- DescribeTopics: 获取日志主题列表
- CreateTopic: 创建日志主题
- CreateLogset: 创建日志集
- SearchLog: 查询日志
- DescribeDashboards: 获取仪表盘订阅列表

具体操作步骤如下:

1. 根据 <mark>策略</mark>,创建一个自定义策略。

该策略允许用户在 CLB 控制台中具有创建日志主题和查看日志主题列表的权限。策略内容可参考以下策略语法进行设置:



2. 找到创建的策略,在该策略行的操作列中,单击关联用户/组/角色。

3. 在弹出的关联用户/用户组/角色窗口中,选择您需要授权的用户/组,单击确定。

# 腾讯云可观测平台的相关策略

如果您希望用户可以查看并使用 CLB 控制台中的腾讯云可观测平台信息,可先将以下操作添加到您的策略中,再将该策略关联到该用 户。

- GetMonitorData: 拉取监控数据
- DescribeCurrentTimestamp: 返回服务器当前时间戳
- DescribeStorageDuration: 拉取存储时长V3
- DescribeBaseMetricsForConsoleFontEnd: 控制台前端调用获取基础指标

具体操作步骤如下:

1. 根据 <mark>策略</mark>,创建一个自定义策略。

该策略允许用户在 CLB 控制台中具有查看监控数据与返回服务器当前时间戳的权限。策略内容可参考以下策略语法进行设置:





	"resource": "*",

2. 找到创建的策略,在该策略行的操作列中,单击关联用户/组/角色。

3. 在弹出的关联用户/用户组/角色窗口中,选择您需要授权的用户/组,单击确定。

## 云函数的相关策略

如果您希望用户可以查看并使用 CLB 控制台中的云函数信息,可先将以下操作添加到您的策略中,再将该策略关联到该用户。

- GetAccount: 查询账户配额
- GetFunction: 获取函数详情
- UnbindTrigger: 云函数解绑触发器
- BindTrigger: 云函数绑定触发器

具体操作步骤如下:

1. 根据 策略,创建一个自定义策略。

该策略允许用户在 CLB 控制台中具有查看账户配额与获取函数详情的权限。策略内容可参考以下策略语法进行设置:



- 2. 找到创建的策略,在该策略行的操作列中,单击关联用户/组/角色。
- 3. 在弹出的关联用户/用户组/角色窗口中,选择您需要授权的用户/组,单击确定。

## 云服务器的相关策略

如果您希望用户可以查看 CLB 控制台中的云服务器信息,可先将以下操作添加到您的策略中,再将该策略关联到该用户。 DescribeInstances:查看实例列表

具体操作步骤如下:

1. 根据 策略,创建一个自定义策略。

该策略允许用户在 CLB 控制台中具有查看实例列表的权限。策略内容可参考以下策略语法进行设置:

```
"version": "2.0",
"statement": [
```





- 2. 找到创建的策略,在该策略行的操作列中,单击关联用户/组/角色。
- 3. 在弹出的关联用户/用户组/角色窗口中,选择您需要授权的用户/组,单击确定。

# Web 应用防火墙的相关策略

如果您希望用户可以查看 CLB 控制台中的 Web 应用防火墙信息,可先将以下操作添加到您的策略中,再将该策略关联到该用户。 DescribeHost:获取防护域名详情

具体操作步骤如下:

1. 根据 策略,创建一个自定义策略。

该策略允许用户在 CLB 控制台中具有查看防护域名详情的权限。策略内容可参考以下策略语法进行设置:



2. 找到创建的策略,在该策略行的操作列中,单击关联用户/组/角色。

3. 在弹出的关联用户/用户组/角色窗口中,选择您需要授权的用户/组,单击确定。

腾讯云

# 传统型负载均衡 传统型负载均衡概述

最近更新时间: 2024-08-19 10:08:51

#### 概述

传统型负载均衡配置简单,支持简单的负载均衡场景:

- 传统型公网负载均衡: 支持 TCP/UDP/HTTP/HTTPS 协议。
- 传统型内网负载均衡: 支持 TCP/UDP 协议。

负载均衡有两种实例类型:负载均衡(此前亦被称为"应用型负载均衡")和传统型负载均衡。 负载均衡可覆盖传统型负载均衡的所有功能。从产品功能、产品性能等多方面考虑,建议您使用的实例类型是负载均衡,二者的详细对 比参见 <mark>实例类型</mark> 。

#### △ 注意:

目前腾讯云账户分为标准账户类型和传统账户类型,2020年6月17日零点后注册的账户均为标准账户类型,该时间点前注册的 账户请在控制台查看您的账户类型,具体操作请参见 判断账户类型。标准账户类型不再支持传统型负载均衡,所购买的实例均 为负载均衡。

本文介绍传统型负载均衡实例,创建实例后,您须为实例配置监听器。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。

### 监听器配置说明

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. 后端端口,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。
- 3. 监听策略,如均衡策略、会话保持等。
- 4. 健康检查策略。
- 5. 绑定后端服务,选择后端服务器的 IP。

#### 🕛 说明:

在传统型负载均衡中,如果您配置了多个监听器,绑定了多个后端云服务器,那么每个监听器都会按其配置转发给所有后端 服务器。

#### 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,包括 TCP 和 UDP。
- 七层协议:应用层协议,包括 HTTP 和 HTTPS。

### 🕛 说明:

1. 传统型负载均衡主要通过 VIP + Port 接受请求并分配流量到后端服务器,七层协议不支持基于域名和 URL 路径的转发。

2. 传统型内网负载均衡仅支持四层协议,不支持七层协议。



3. 如您需支持上述高级能力,请直接使用负载均衡,而非传统型负载均衡,详情请参见实例类型。

# 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 <ul> <li>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。</li> <li>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。</li> </ul> <li>服务端口可以在同一个负载均衡实例内重复。</li> <li>例如,监听器 HTTP:80 和监听器 HTTPS:443</li> <li>可以同时绑定同一台云服务器的同一个端口。</li>

# 配置传统型负载均衡

最近更新时间: 2024-07-19 15:46:11

创建传统型负载均衡实例后,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。

## 前提条件

您需要 创建负载均衡实例,其中实例类型选择"传统型负载均衡"。

#### △ 注意:

目前腾讯云账户分为标准账户类型和传统账户类型,2020年6月17日零点后注册的账户均为标准账户类型,该时间点前注册的 账户请在控制台查看您的账户类型,具体操作请参见 判断账户类型。标准账户类型不再支持传统型负载均衡,所购买的实例均 为负载均衡。

## 配置监听器

## 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**实例管理**。
- 3. 在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,您也可以在列表页的操作栏中单击配置监听器。

负载均衡(28)	传统型负载均衡	6( <b>7</b> )								
新建 删除	分配至项目	前日	标签			所属项目: 所	有项目 多个关键字用	]竖线" "分隔,多个过滤	転送用 Q (	¢ ±
□ ID/名称 #	盾控	状态	域名	VIP	网络类型 🍸	所國网络	健康状态	创建时间 \$	操作	
10 xc 2605	.lı	正常	158- 12 56 hydd Iaud.com	13	公网	vp vr De 6.(	异常 (异常端口 数:4)	2019-07-30 18:30:0 6	配置监听器	更多 ▼

5. 监听器管理页面如下图所示。

← Ⅱ 基本信息 监听器	<b>着理</b>	安全组							
监听器									
监听器名称					操作				
			列表为空						
绑定后端服务									
<b>绑定</b> 修改权[	<u>前</u> 一 解 第					搜索IP或主机名	Q,	¢	+
D	名称	状态	内同IP	公网IP	权重①	操作			
			监听器创建完成,请 <mark>绑定原</mark>	后端服务					



# 步骤2:配置监听器

在监听器模块下,单击新建,在弹出框中配置 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: CLB 支持的协议包括 TCP、UDP、HTTP、HTTPS,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
后端端口	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	80

#### 创建 TCP 监听器具体基本配置如下图所示:

创建监听器	
1 基本配置	> 2 高级配置 > 3 健康检查
名称	test-tcp-80
监听协议端口①	TCP 💌 : 80
后端端口	80
	关闭下一步

## 2.高级配置

高级配置	说明	示例
均衡方式	<ul> <li>TCP 监听器中,负载均衡支持加权轮询(WRR)和加权最小连接数(WLC)两种调度算法</li> <li>加权轮询算法: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。加权轮询算法 根据<b>新建连接数</b>来调度,权值越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。</li> <li>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。</li> </ul>	加权轮 询
会话保持状 态	开启或关闭会话保持 <ul> <li>开启会话保持后,负载均衡监听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。</li> </ul>	开启



	<ul> <li>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。</li> <li>加权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。</li> </ul>	
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

## 具体配置如下图所示:

创建监听器	
✓ 基本配調	■
均衡方式	加权轮询
会话保持 🚯	当后端CVM的权重都设置为同一个值时,权重属性将不生效,将按照简单的轮询策略分发请求
保持时间	30秒 3600秒 + 秒
	基于源IP地址的会话保持
	上一步下一步

## 3.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 SYN 包进行健康 检查。	开启
检查协议	支持选择配置"TCP"、"HTTP"或"自定义"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 。	默认
响应超时	<ul> <li>健康检查响应的最大超时时间。</li> <li>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。</li> <li>可配置范围: 2 - 60秒,默认值2秒。</li> </ul>	2s
检测间隔	<ul> <li>负载均衡进行健康检查的时间间隔。</li> <li>可配置范围:5-300秒,默认值5秒。</li> </ul>	5s
不健康阈值	<ul> <li>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。</li> <li>可配置范围: 2 – 10次,默认值3次。</li> </ul>	3次
健康阈值	<ul> <li>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。</li> <li>可配置范围: 2 – 10次,默认值3次。</li> </ul>	3次



#### 健康检查具体配置如下图所示:

创建监听器		×
✓ 基本配置	> → 高級配置 > 3 健康检查	
健康检查(j)		
检查协议	● TCP ● HTTP ● 自定义协议	
检查端口	默认为后端服务器端口,除非您希望指定特定端口,否则建议留空	
	隐藏高级选项 🔺	
响应超时	1     -     2     +     秒       2秒     60秒	
检测间隔	5秒 300秒	
不健康阈值()		
健康阈值(		
	上一步提交	

## 步骤3: 绑定后端云服务器

在"监听器管理"页面,单击**绑定**,在弹出框中选择需绑定的后端云服务器,绑定详情如下:



 $\times$ 

#### 绑定云服务器

溫	薯提示:CLB 与 CVM 之间采用内网通信,不收取网络流量费用。							
选择z	云服务器				已选择 (3)			
披露	印或主机名	Θ	Q,		云服务器		权重③	
~	<del>才</del> 129.2(		Î		<del>才</del> 129.	0.42	10 ^	×
	服务器异常 10€ 0.49				<del>才</del> 106.	.29	10 ^	×
	未命名 106.			$\leftrightarrow$	未 108.	.0.18	10 ^	×
	未 1(							
~	未」 106.51 0.0.0.18							
	tke_ ;fd 106							
	8 1 1.0.8		+					
支持	安住Shift进行多选							
			确定		取消			

#### 配置完毕的截图如下所示:

基本信息	监听器管理	监控	安全组				
监听器							
新建							
监听器名称						操作	
> test-to	p-80 (TCP:80)					修改 删除	
绑定后端服务							
绑定	修改权重	解绑					搜索IP或主机名
		名称	状态	内网IP	公网IP	权重①	操作
	За	÷	运行中	1(	10	10	解绑
	9	7	运行中	1(	10	10	解却
	k	7	运行中	10	12	10	解绑

- () 说明:
  - 在传统型负载均衡中,如果您配置了多个监听器,绑定了多个后端云服务器,那么每个监听器都会按其配置转发给所有后端 服务器。
  - 6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。



# 步骤4:安全组(可选)

您可以配置负载均衡的安全组来进行公网流量的隔离,详情请参见配置负载均衡安全组。

### 步骤5: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,选择已创建完毕的监听器,选择修改或删除来完成操作。

基本信息	监听器管理	监控	安全组		
监听器					
新建					
监听器名	称				操作
> 1	est-tcp-80 (TCP:80)				修改 删除

# 传统型负载均衡管理后端云服务器

最近更新时间: 2024-11-04 11:06:42

传统型负载均衡将请求路由至运行正常的后端云服务器实例,首次使用传统型负载均衡或根据业务需求,需要增加或删除后端服务器数 量时,可按照本文指引进行操作。

## 前提条件

需已创建传统型负载均衡实例并配置监听器,详情请参见 传统型负载均衡快速入门。

#### 操作步骤

## 添加传统型负载均衡后端服务器

() 说明:

- 如果传统型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传统型负载均衡后端云服务器。若从弹 性伸缩组移除的云服务器实例会自动从传统型负载均衡后端云服务器中删除。
- 如需使用 API 添加后端服务器,请参见 绑定后端服务到传统型负载均衡 接口说明。
- 1. 登录 负载均衡控制台。

() 说明:

- 2. 在"实例管理"页面,单击传统型负载均衡。
- 3. 在目标传统型负载均衡实例右侧操作列,单击配置监听器。
- 4. 在配置监听器模块,单击创建。
- 5. 在"创建监听器"弹窗中,填写"后端端口"(端口选择请参见 服务器常用端口)及其他相关字段,单击**下一步**,继续完成配置, 详情请参见 配置传统型负载均衡 。

传统型负载	均衡需要在 <b>创建监听器阶段</b> 指定后端服务器的端口。	
创建监听器		×
1 基本配置	〉 2 高级配置 〉 3 健康检查	
名称	test	
监听协议端口①	TCP • : 22	
后端端口	8080	
	关闭下一步	

- 6. 监听器创建完成后,在绑定后端服务模块,单击绑定。
- 7. 在"绑定云服务器"弹窗中,勾选需要绑定的云服务器,在"权重"处填写权重信息,单击确定。

#### () 说明:

• 弹出框中仅展示同地域、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。



- 绑定多个后端服务器时,CLB 将按 Hash 算法转发流量,起到均衡负载的作用。
- 权重越大转发的请求越多,默认为10,可配置范围为0-100。当权重设置为0,该服务器不会再接受新请求。如开启 会话保持,可能会造成后端服务器的请求不均匀,详情请见均衡算法选择与权重配置实例。

绑定云服务器				×				
温馨提示:公网 CLB 绑定的 CVM 需分配大于 0MB 的公网带宽,否则会导致转发不通。								
选择云服务器		已选择 (2)						
搜索IP或主机名	0 Q	云服务器	权重①					
	<u>^</u>		10 🔷	×				
			10	×				
支持按住Shift进行多选								
	确定。	取消						

## 修改传统型负载均衡后端服务器权重

() 说明:

传统型负载均衡暂不支持使用 API 修改后端服务器权重。

- 1. 登录 负载均衡控制台。
- 2. 在"实例管理"页面,单击传统型负载均衡。
- 3. 在目标传统型负载均衡实例右侧操作列,单击配置监听器。
- 4. 在绑定后端服务模块,修改相关服务器权重。

#### () 说明:

权重越大转发的请求越多,默认为10,可配置范围为0-100。 当权重设置为0,该服务器不会再接受新请求。 如开启会话 保持,可能会造成后端服务器的请求不均匀,详情请见 均衡算法选择与权重配置实例 。

○ 方式1: 单独修改某台服务器权重。

4.1.1 找到需要修改权重的服务器,并将鼠标悬浮于对应权重上方,单击》编辑按钮。



绑	<del>定</del> 修改权重	解绑				搜索IP或主机名	φ ±
<b>~</b>	ID	名称	状态	内网IP	公网旧	权重()	操作
			运行中			10	解绑
~		1000	运行中			编辑 10	解绑

4.1.2 在"修改权重"弹窗中,输入修改后的权重值,单击提交。

○ 方式2: 批量修改某些服务器权重。

批量修改权重后的服务器权重相同。
------------------

4.1.1 单击服务器前方复选框,选中多台服务器,在列表上方,单击修改权重。

绑定	修改权重	解绑				搜索IP或主机名	ς φ <u>+</u>
~	ID	名称	状态	内网旧	公网IP	权重③	操作
			运行中			10	解绑
		1010	运行中			10	解绑

4.1.2 在"修改权重"弹窗中,输入修改后的权重值,单击提交。

#### 解绑传统型负载均衡后端服务器

🕛 说明:

解绑后端服务器会解除传统型负载均衡实例与云服务器实例的关联关系,且传统型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。 如需使用 API 解绑后端服务器,请参见 解绑传统型负载均衡的后端服务器 接口说明。

- 1. 登录 负载均衡控制台。
- 2. 在"实例管理"页面,单击**传统型负载均衡**。
- 3. 在目标传统型负载均衡实例右侧操作列,单击配置监听器。
- 4. 在绑定后端服务模块,解绑已绑定的服务器。
  - 方式1: 单独解绑某台服务器。
    - 4.1.1 找到需要解绑的服务器,在右侧操作栏,单击解绑。



绑定修改权国	重 解绑				搜索IP或主机名	Q Ø	Ŧ
ID	名称	状态	内网旧	公网IP	权重()	操作	
		运行中			10	解绑	
	1010	运行中		-	10	解绑	

4.1.2 在 "解绑后端服务" 弹窗中,确认解绑的服务,单击提交。

○ **方式2**: 批量解绑某些服务器。

4.1.1 单击服务器前方复选框,选中多台服务器,在列表上方,单击解绑。

ģ	院修改权重	解绑				搜索IP或主机名	φ ±
	ID	名称	状态	内网IP	公网IP	权重①	操作
<b>~</b>			运行中			10	解绑
~		1010	运行中			10	解绑

4.1.2 在 "解绑后端服务" 弹窗中,确认解绑的服务,单击提交。