负载均衡

产品文档

版权所有：建行云

文档目录

- 产品简介
  - 负载均衡概述
    - 产品概述
    - 使用CLB
  - 地域和可用性
    - 地域
    - 可用区
    - 如何选择地域和可用区
  - 功能优势
    - 高性能
    - 低成本
    - 弹性扩展
    - 跨运营商高可用
  - 应用场景
  - 实例类型
- 推荐解决方案
  - 推荐解决方案
- 快速入门
  - IPv4负载均衡快速入门
    - 步骤一：创建IPv4负载均衡实例
    - 步骤二：配置IPv4负载均衡监听器、转发组和转发规则
    - 步骤三：绑定云主机
    - 步骤四：配置安全组
    - 步骤五：配置重定向功能
    - 步骤六：解绑云主机
    - 步骤七：删除负载均衡实例
  - IPv6负载均衡快速入门
    - 步骤一：创建IPv6负载均衡实例
    - 步骤二：配置IPv6负载均衡监听器、转发组和转发规则
    - 步骤三：绑定云主机
    - 步骤四：配置安全组
    - 步骤五：配置重定向功能
    - 步骤六：解绑云主机
    - 步骤七：删除负载均衡实例
- 操作指南

版权所有：建行云

- 负载均衡实例
  - 创建IPv4负载均衡实例
  - 创建IPV6负载均衡实例
  - 导出负载均衡实例
  - 删除负载均衡实例
- 负载均衡监听器
  - 负载均衡监听器概述
  - 配置TCP监听器
    - 配置TCP监听器
    - 前提条件
    - 操作步骤
      - 步骤一：配置监听器
      - 步骤二：绑定后端云服务器
      - 步骤三：修改/删除监听器（可选）
  - 配置UDP监听器
    - 配置UDP监听器
    - 前提条件
    - 操作步骤
      - 步骤一：配置监听器
      - 步骤二：绑定后端云服务器
      - 步骤三：修改/删除监听器（可选）
  - 配置HTTP监听器
    - 配置HTTP监听器
    - 前提条件
    - 操作步骤
      - 步骤一：配置监听器
      - 步骤二：绑定后端云服务器
      - 步骤三：修改/删除监听器（可选）
  - 配置HTTPS监听器
    - 配置HTTPS监听器
    - 前提条件
    - 操作步骤
      - 步骤一：配置监听器
      - 步骤二：绑定后端云服务器
      - 步骤三：修改/删除监听器（可选）
  - 均衡方式
  - 会话保持
  - 七层重定向配置

版权所有：建行云

七层重定向配置
重定向概述
自动重定向
手动重定向
七层转发域名和URL规则说明
七层转发配置说明
转发域名匹配说明
转发 URL 路径配置规则
七层健康检查配置说明
后端服务器
后端云服务器概述
管理后端服务器
后端云服务器简述
前提条件
操作步骤
添加负载均衡后端云服务器
修改负载均衡后端服务器权重
修改负载均衡后端服务器端口
解绑负载均衡后端服务器
管理弹性网卡
弹性网卡简介
前提条件
操作步骤
健康检查
健康检查概述
健康检查概述
健康检查状态
TCP 健康检查
UDP 健康检查
HTTP 健康检查
健康检查时间窗
配置健康检查
配置健康检查
前提条件
TCP监听器
TCP 监听器
配置 TCP 健康检查
UDP监听器

版权所有：建行云

UDP 监听器
配置 UDP 健康检查
HTTP监听器
配置 HTTP 健康检查
HTTPS监听器
配置 HTTPS 健康检查
证书管理
管理证书
管理证书
证书要求
配置证书
更新证书
查看证书关联的负载均衡
证书要求及转换证书格式
证书上传流程
常用证书申请流程
证书格式要求
RSA私钥格式要求
证书转换为PEM格式说明
证书转换为PEM格式说明
DER格式证书转换为PEM格式
P7B格式证书转换为PEM格式
PFX格式证书转换为PEM格式
CER/CRT格式证书转换为PEM格式
SSL单向认证和双向认证说明
监控告警
获取监控数据
监控指标说明
配置告警策略
应用场景
基本概念
操作步骤
告警指标说明
外网监听器/内网监听器
最佳实践
最佳实践
常见问题
负载均衡有几种类型

版权所有：建行云

什么是健康检查
负载均衡是否可以直接获取客户端IP
负载均衡的VIP是否支持ping
公网IP和EIP的区别是什么?
健康检查提示 CVM 实例异常该如何处理?
权重置为0与解绑 RS 有什么区别?
为什么健康检查探测频率过高?
关于 Telnet 负载均衡监听端口的说明
CVM 可通过配置内网型负载均衡，将流量从端口A转发回同一台服务器的其他端口吗?
关于内网回环问题的说明
HTTPS 支持的加密套件有哪些?
证书过期后如何处理?
一个监听器可以绑定多少个 HTTPS 证书?
CLB 目前支持哪些类型的证书?
添加 HTTPS 监听器后，负载均衡到后端云服务器间的请求是否依然通过 HTTP 协议传输?
HTTPS 监听使用什么端口?
HTTPS 支持哪些版本的SSL/TLS安全协议?

版权所有：建行云

产品简介
负载均衡概述
产品概述

最近更新时间: 2023-03-16 16:29:14

建行云负载均衡（Cloud Load Balancer，简称CLB）产品能够为用户提供高效、安全的流量分发服务，用户通过使用建行云CLB产品，可以将高并发的应用请求以相应的负载均衡策略和转发规则均衡的转发到后台应用服务器，实现业务的平稳运行。

了解CLB时，通常会涉及到以下概念：

- 负载均衡实例：云上的负载均衡规则。
- 监听器：负载均衡服务监听器，主要包括监听端口、负载均衡策略及健康检查等，用于监听对应的后台应用服务。
- 虚拟服务地址：系统分配的服务地址，可分为内网IP和公网IP。
- 私有网络：自定义的虚拟网络空间，与其他资源逻辑隔离。
- 地域和可用区：实例和其他资源的启动位置。
- 云控制台：基于Web的用户控制台。

版权所有：建行云

使用CLB

最近更新时间: 2023-03-16 16:29:14

CLB提供基于Web的用户控制台，如用户已注册云平台账号，用户可以直接登录用户控制台，对CLB实例进行操作。

版权所有：建行云

地域和可用性

地域

最近更新时间: 2023-03-16 16:29:14

地域是指物理的数据中心的地理区域。云平台不同地域之间完全隔离，保证不同地域间最大程度的稳定性和容错性。为了降低访问时延、提高下载速度，建议用户选择最靠近用户客户的地域。

- 不同地域之间网络完全隔离，不同地域之间的云产品默认不能通过内网通信。
- 不同地域之间云产品可以通过公网IP进行Internet访问；处于私有网络中的云产品也可以通过云平台提供的对等连接经由高速互联网络通信，以获得比Internet访问更稳定高速的互联。
- 负载均衡当前不支持跨地域的流量转发，即负载均衡服务绑定服务器时，只能选择绑定本地域的云服务器。

版权所有：建行云

可用区

最近更新时间: 2023-03-16 16:29:14

可用区（Zone）是指云平台在同一地域内电力和网络互相独立的物理数据中心。目标是能够保证可用区间故障相互隔离（大型灾害或者大型电力故障除外），不出现故障扩散，使得用户的业务持续在线服务。通过启动独立可用区内的实例，用户可以保护应用程序不受单一位置故障的影响。

- 同一地域下不同可用区的基础网络服务器可以通过内网访问。
- 同一地域下不同可用区，同一个VPC下的云产品之间均通过内网互通，可以直接使用内网IP访问。
- 上述内网互通是指同一账户下的资源互通，不同账户的资源内网完全隔离。

版权所有：建行云

如何选择地域和可用区

最近更新时间: 2023-03-16 16:29:14

关于选择地域和可用区时，用户需要考虑几个因素：

- 负载均衡所在的地域、用户以及用户的目标用户所在的地理位置；建议申请负载均衡时选择最靠近用户客户的地域，以降低访问时延、提高访问速度。
- 不同可用区间可能会有网络的通信延迟，需要结合业务的实际需求进行评估，在高可用和低延迟之间找到最佳平衡点。

版权所有：建行云

功能优势

高性能

最近更新时间: 2023-03-16 16:29:14

建行云CLB集群支持超过千万级的最大并发连接数，集群最大流量带宽高达数十Gbps,可满足主流的网络业务场景使用。

版权所有：建行云

低成本

最近更新时间: 2023-03-16 16:29:14

建行云CLB产品可同时提供针对TCP/UDP四层和HTTP/HTTPS七层的应用做转发，满足主要的负载均衡业务场景，用户无需再额外配备其他硬件负载均衡设备。

弹性扩展

最近更新时间: 2023-03-16 16:29:14

建行云CLB产品可以在业务流量突增时进行带宽的动态扩容，实现用户的业务平稳运行。

版权所有：建行云

跨运营商高可用

最近更新时间: 2023-03-16 16:29:14

负载均衡的公网IP目前已经实现多线BGP接入（目前已接入联通、电信以及移动），BGP属性公网IP与运营商互联，实现单IP多线路，降低运营商互访的网络延迟，同时做到运营商的高可用。

版权所有：建行云

应用场景

最近更新时间: 2023-03-16 15:59:27

建行云CLB产品可以提供TCP/UDP四层负载均衡和HTTP/HTTPS七层负载均衡。

1.四层CLB

四层CLB主要实现针对VIP+端口的业务流量转发，当用户申请一个CLB实例后，该实例会被分配一个Virtual IP（VIP），用户使用该VIP，并配置不同的转发端口，即可实现TCP/UDP层面的请求转发。

2.七层CLB

七层CLB主要实现针对VIP+端口+URL的应用层流量转发，用户申请一个CLB实例后，使用该实例的VIP地址，并配置相应的转发端口和URL，即可实现HTTP/HTTPS的应用层流量转发。

版权所有：建行云

实例类型

最近更新时间: 2023-03-16 15:59:27

建行云CLB有两种实例类型，分为内网CLB和公网CLB。

1.内网CLB

用户申请CLB实例时，可以选择内网负载均衡类型，内网负载均衡类型主要用于用户在内网应用流量做转发，内网负载均衡实例的Virtual IP（以下简称VIP）为内网IP地址，该地址只能在VPC内部使用，无法在互联网上进行使用和访问。

2.公网CLB

用户申请CLB实例时，除选择内网负载均衡类型外，还可以选择公网负载均衡类型，公网负载均衡类型的VIP为互联网IP地址，用户使用该VIP地址可以由互联网访问云上部署的应用。目前IP版本可支持IPV4和IPV6。

版权所有：建行云

推荐解决方案

推荐解决方案

最近更新时间: 2023-03-15 15:08:16

1.公网负载均衡+内网负载均衡结合使用

建行云负载均衡可同时提供内网负载均衡和公网负载均衡能力，公网负载均衡实例的IP地址为互联网IP，用户可以通过互联网来访问公网负载均衡VIP，内网负载均衡实例的IP地址为内网IP，该IP仅可以在租户VPC内部使用。用户可以将公网负载均衡实例和内网负载均衡实例结合使用，公网负载均衡实例用于对外提供访问入口，内网负载均衡实例用于内部业务流量转发，这样既可减少互联网IP地址的使用，又能避免将内部应用暴露在互联网，提高了应用的安全。

2.开通CLB健康检查功能

建行云CLB健康检查功能可以根据配置来探测CLB后端绑定的端口是否存在异常，如果CLB探测到后端绑定的端口存在异常，则会在页面上将该端口的状态置为“异常”，并可自动切断CLB实例和后端应用的通信，避免正常的业务请求转发到异常的应用上，有效的提高了应用的可用性。

版权所有：建行云

快速入门
IPv4负载均衡快速入门
步骤一：创建IPv4负载均衡实例

最近更新时间: 2023-12-06 15:30:09

1.选择CLB实例的地域

建行云CLB实例仅支持在单个地域内的流量转发，处在不同地域的云产品之间内网无法访问。

2.选择网络类型

建行云CLB提供两种不同网络类型的负载均衡实例，其中，内网负载均衡网络主要用于VPC网络内部的流量分发，公网负载均衡网络主要负责将来自外部互联网请求的流量分发到内部服务应用。

3.选择可用区类型

建行云CLB提供两种可用区类型，单可用区建立的负载均衡实例分布在单一的可用区，多可用区建立的负载均衡实例由主可用区和备可用区组成。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。多可用区只对网络类型为公网的负载均衡实例提供。

4.选择IP版本

建行云CLB提供两种不同IP版本，分别是IPv4和IPv6。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 负载均衡只对网络类型为公网的负载均衡实例提供。

版权所有：建行云

5.选择所属VPC网络

选择负载均衡实例所属的VPC网络，其中公网类型的负载均衡只选择所属VPC网络即可，建行云随机分配负载均衡VIP；内网类型的负载均衡除需要选择所属VPC外，还需要选择VPC内的子网，建行云在选定的子网网段下随机分配负载均衡VIP。

6.公网类型负载均衡带宽上限

公网类型的负载均衡除可以选择所属运营商外，还可对公网IP的带宽做选择，带宽上限选择范围在1Mbps–2000Mbps。建议用户在申请使用公网CLB实例前，预先评估好业务流量，避免由于CLB实例带宽过小而对业务造成影响。

7.选择申请数量

用户可以选择同时创建的CLB实例数量，其中每个账号下最多允许一次性创建20个CLB实例。

如图所示。

负载均衡 LB

地域
武汉
处在不同地域的云产品内网不通
实例类型
应用型LB 推荐
支持HTTP(S)/TCP/UDP协议
支持基于域名+URL的转发
全面覆盖传统型LB功能
网络类型
公网
内网
可用区类型
单可用区
多可用区
IP版本
IPv4
IPv6
网络
如果现有的网络不合适，您可以去控制台 新建私有网络
所属运营商
请选择
公网带宽
按使用流量
带宽上限
1Mbps
10Mbps
40Mbps
2000Mbps
1
Mbps
实例名
创建后命名
立即命名
购买数量
1

步骤二：配置IPv4负载均衡监听器、转发组和转发规则

最近更新时间: 2023-12-06 15:48:27

1. 创建完成后，在【CLB详情】-【监听器管理】页面，可以查看该CLB实例绑定的监听器信息，单击【新建】创建一个HTTP监听器（此处以创建HTTP监听器为例）。

2. 创建七层HTTP监听器时，填写监听器名称、监听的端口，这里我们默认填写了80端口。创建完成后，单击【创建转发规则】可以为监听器配置域名+URL，这里的域名和URL支持通配和正则，但存在一定的限制条件。
3. 均衡方式可以选择按权重轮询、IP Hash或加权最小连接数三种方式。
4. 点击【下一步，健康检查】，可打开健康检查开关，并配置健康检查的检查域名、检查目录、检测间隔间隔、不健康阈值次数、健康阈值次数，以及HTTP请求方式和HTTP状态检测，配置完成后将根据健康检查规则系统自动检测后端端口是否异常，如存在异常将自动隔离。
5. 点击【下一步，会话保持】，可打开会话保持开关，配置会话保持时间。若关闭会话保持功能，选择轮询的方式进行调度，则请求会被依次分配到不同后端服务器上；若开启会话保持功能，或关闭会话保持功能但选择ip_hash 的调度方式，则请求会被持续分配到同一台后端服务器上。

6. 如果不希望连接落到同一台后端云服务器时，可以在配置的第三步关闭会话保持。

7. 创建完成后，可以看到该监听器下已经配置了 www.example.com/image/的转发组和转发规则 。

步骤三：绑定云主机

最近更新时间: 2023-03-16 16:00:17

创建完成监听器后，可通过【绑定云主机】来绑定流量分发的后端云主机，在弹出框中会展示同地域、相同网络环境、未被隔离、未过期、带宽（峰值）不为 0 的可选云服务器列表。选择所有需要关联的云服务器，单击【确定】按钮。绑定云主机时，平台默认监听后端80端口。由于应用型负载均衡配置灵活，可以在同一监听器下绑定不同后端端口的云服务器。

步骤四：配置安全组

最近更新时间: 2023-03-16 16:00:14

创建完负载均衡后，需配置负载均衡的安全组来隔离公网流量，安全组配置完成后，可选择开启或关闭安全组，默认开启，具体配置方法参照VPC产品安全组配置说明。同时，公网负载均衡需配置WAF防火墙。安全组要将负载均衡的VIP和端口放通。

版权所有：建行云

步骤五：配置重定向功能

最近更新时间: 2023-03-16 16:00:14

重定向配置分为手动重定向和自动重定向两种，自动重定向主要针对域名下路径较多的情况，需要系统自动为已经存在的HTTPS:443 监听器创建HTTP监听器进行转发。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。只有公网负载均衡有配置重定向功能。

在CLB详情选取重定向配置，也可新建一个手动重定向配置，

1.选取原访问的协议、端口和域名，并指定目的协议、端口和域名。

2.单击【下一步】后，可以选取原访问路径和重定向后的访问路径，域名下路径较多时，可以添加多条路径进行重定向，需要注意的是，路径的配置不允许回环（也就是A->B B->C的情况），且当前只允许在同一个CLB实例中进

行。

3.重定向策略配置完成后，可以在CLB重定向配置详情页查看策略。其中，原有的监听器树状图中，HTTP监听器的路径下增加了一个重定向标识，用于说明该路径下绑定的后端服务器将不会再收到请求，请求会被重定向到刚才配置的HTTPS监听器中。

当原转发规则进行修改后，重定向策略会默认解除，需重新配置。

步骤六：解绑云主机

最近更新时间: 2023-12-06 15:46:45

1. 选择“LB实例列表”选项，进入LB实例列表页面。
2. 点击相应的负载均衡实例ID进入负载均衡详情页。
3. 点击【监听管理】，找到需要修改的监听器。
4. 在监听器管理页面，点找到需要解绑的云主机，并点击右侧【解绑】按钮，即可解除负载均衡实例和相应后端云服务器的绑定关系。

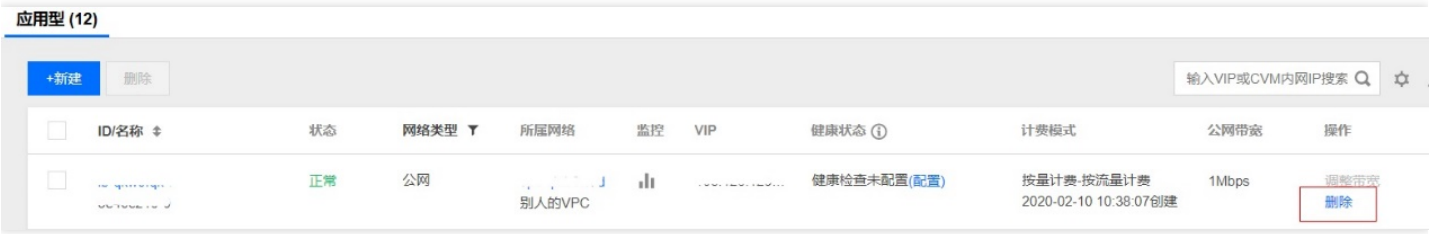
步骤七：删除负载均衡实例

最近更新时间: 2023-12-06 15:46:45

1.登录建行云租户控制台，点击“负载均衡”产品，进入负载均衡产品页面，点击左侧菜单“LB实例列表”选项，进入LB实例列表页面。

2.选择需要删除的LB实例，点击右侧【删除】按钮，在弹出的确认对话框中确认是否是需要删除的LB实例，如确认无误，则点击下方的“确认”按钮删除该LB实例。

【注意】该删除操作无法回退，我们强烈建议用户在删除前确认该LB实例下绑定的云主机数量为0，所创建的监听器均无业务使用。



IPv6负载均衡快速入门

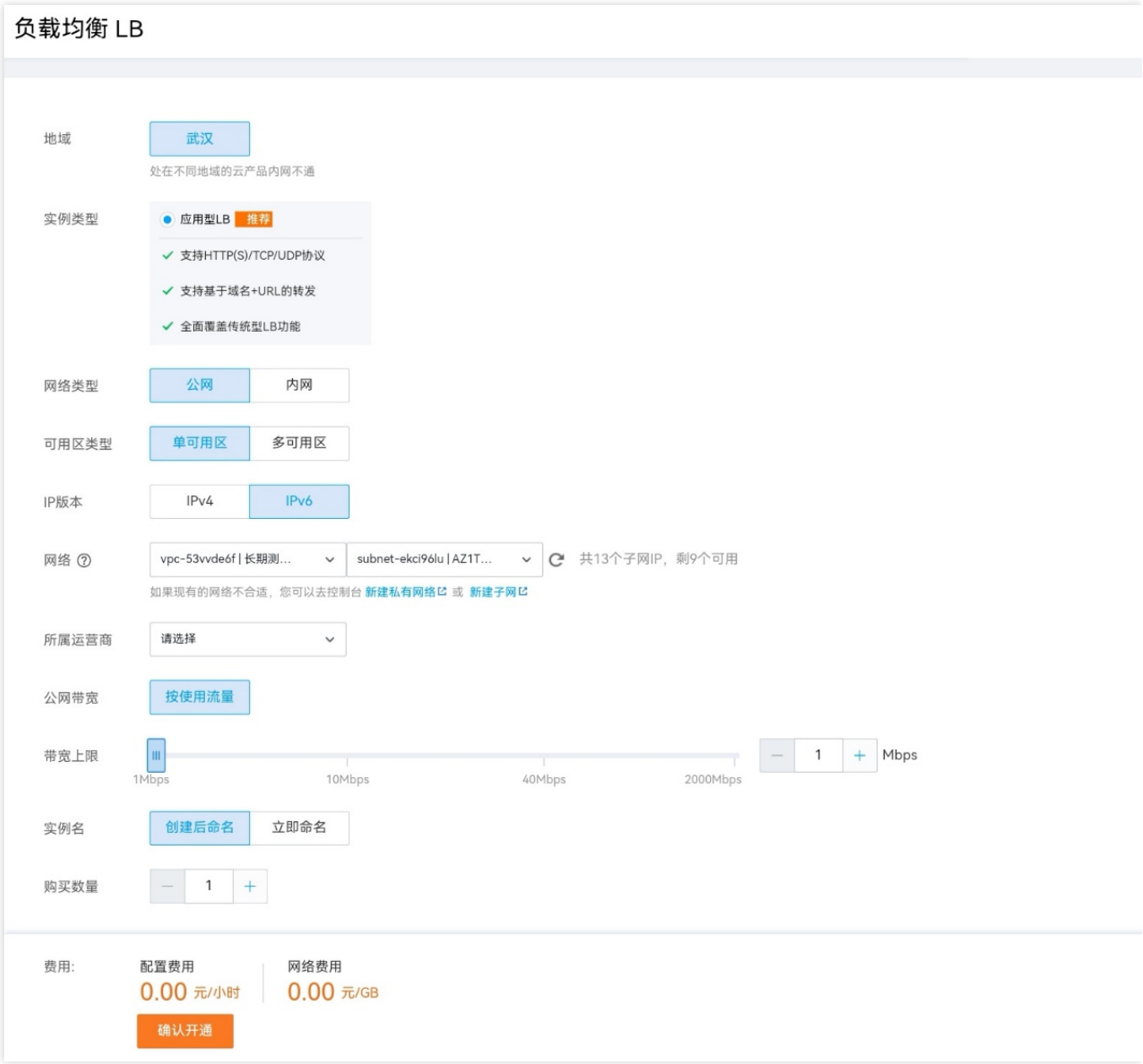
步骤一：创建IPv6负载均衡实例

最近更新时间: 2023-12-06 15:54:07

1. 选择CLB实例的地域
   建行云CLB实例仅支持在单个地域内的流量转发。
2. 选择网络类型
   网络类型需选择公网，IPv6负载均衡仅支持公网负载均衡，不支持内网负载均衡。
3. 选择可用区类型
   可用区类型需选择单可用区，IPv6负载均衡仅支持单可用区，不支持多可用区。
4. 选择IP版本
   IP版本选择IPv6。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 负载均衡只对网络类型为公网的负载均衡实例提供。
5. 选择所属VPC网络
   选择IPv6负载均衡实例所属的VPC网络。用户创建公网IPv6负载均衡时，建行云在选定的子网网段下随机分配负载均衡VIP。
6. 公网类型负载均衡带宽上限
   公网类型的负载均衡除可以选择所属运营商外，还可对公网IP的带宽做选择，带宽上限选择范围在1Mbps-2000Mbps。建议用户在申请使用公网CLB实例前，预先评估好业务流量，避免由于CLB实例带宽过小而对业务造成影响。
7. 选择申请数量
   用户可以选择同时创建的CLB实例数量，其中每个账号下最多允许一次性创建20个CLB实例。

版权所有：建行云

如图所示。


负载均衡 LB
地域
武汉
处在不同地域的云产品内网不通
实例类型
应用型LB 推荐
支持HTTP(S)/TCP/UDP协议
支持基于域名+URL的转发
全面覆盖传统型LB功能
网络类型
公网
内网
可用区类型
单可用区
多可用区
IP版本
IPv4
IPv6
网络
vpc-53vvde6f | 长期测...
subnet-ekci96lu | AZ1T...
共13个子网IP，剩9个可用
如果现有的网络不合适，您可以去控制台 新建私有网络 或 新建子网
所属运营商
请选择
公网带宽
按使用流量
带宽上限
1Mbps
10Mbps
40Mbps
2000Mbps
1
Mbps
实例名
创建后命名
立即命名
购买数量
1
费用:
配置费用
0.00 元/小时
网络费用
0.00 元/GB
确认开通

步骤二：配置IPv6负载均衡监听器、转发组和转发规则

最近更新时间: 2023-03-16 16:00:14

1.创建完成后，在【CLB详情】-【监听器管理】页面，单击【新建】创建一个HTTP监听器。

2.创建七层HTTP监听器时，填写监听器名称、监听的端口。

3.设置均衡方式、健康检查、会话支持等，完成转发规则设置。

步骤三：绑定云主机

最近更新时间: 2023-03-16 16:00:14

1.进入“监听器管理”页面，选择对应的监听器、域名和URL 路径，单击绑定。

2.选择对应的云服务器，设置端口及权重，默认端口为80，单击确定，完成云主机绑定。

步骤四：配置安全组

最近更新时间: 2023-12-06 15:32:20

创建完负载均衡后，需配置负载均衡的安全组来隔离公网流量，安全组配置完成后，可选择开启或关闭安全组，默认开启，具体配置方法详见VPC产品安全组配置说明。同时，公网负载均衡需配置WAF防火墙。

版权所有：建行云

步骤五：配置重定向功能

最近更新时间: 2023-12-06 15:32:20

重定向配置分为手动重定向和自动重定向两种。手工重定向可选择原访问的协议、端口和域名，并指定目的协议、端口和域名，完成手工重定向后，系统将自动将原访问地址的请求重定向至对应路径的目的地址。自动重定向主要针对域名下路径较多的情况，需要系统自动为已经存在的HTTPS:443 监听器创建HTTP监听器进行转发。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。

步骤六：解绑云主机

最近更新时间: 2023-12-06 15:33:52

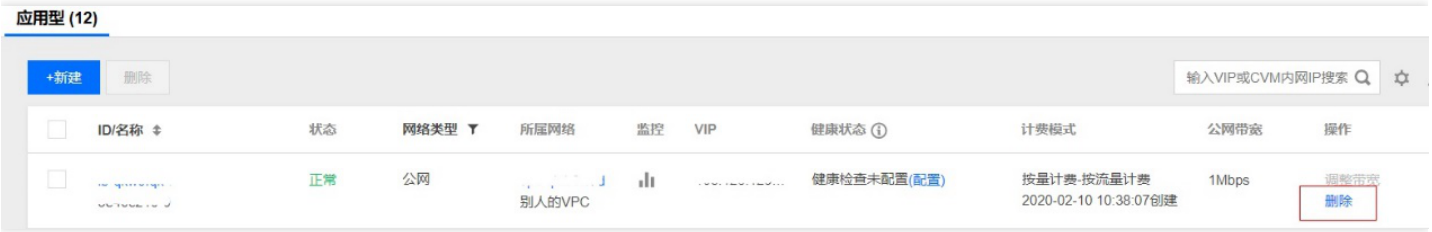
1. 选择“LB实例列表”选项，进入LB实例列表页面。 2.点击相应的负载均衡实例ID进入负载均衡详情页。 3.点击【监听管理】，找到需要修改的监听器。 4.在监听器管理页面，点找到需要解绑的云主机，并点击右侧【解绑】按钮，即可解除负载均衡实例和相应后端云服务器的绑定关系。

步骤七：删除负载均衡实例

最近更新时间: 2023-12-06 15:56:48

1. 登录建行云租户控制台，点击“负载均衡”产品，进入负载均衡产品页面，点击左侧菜单“LB实例列表”选项，进入LB实例列表页面。
2. 选择需要删除的LB实例，点击右侧【删除】按钮，在弹出的确认对话框中确认是否是需要删除的LB实例，如确认无误，则点击下方的“确认”按钮删除该LB实例。

【注意】该删除操作无法回退，我们强烈建议用户在删除前确认该LB实例下绑定的云主机数量为0，所创建的监听器均无业务使用。



操作指南
负载均衡实例
创建IPv4负载均衡实例

最近更新时间: 2023-12-06 15:32:38

1.登录建行云负载均衡申请页，点击新建。

2.选择对应的地域、实例类型等参数，进行负载均衡相关配置。

参数	说明
地域	选择所属地域
实例类型	应用型LB
网络类型	网络类型分为公网和内网两种类型。
	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内网的请求。内网不支持配置IP 版本、运营商类型、带宽上限。
可用区类型	单可用区、多可用区（内网默认为多可用区，不支持用户配置）
IP 版本	IPv4
网络	选择所属VPC和子网。当用户创建内网IPv4负载均衡时，建行云在选定的子网网段下随机分配负载均衡VIP；当用户创建公网IPv4负载均衡时，建行云随机分配负载均衡VIP。
运营商类型	运营商类型分为：中国移动、中国电信和中国联通、BGP-C等
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。目前仅公网 IPv4 版本的 CLB 支持主备可用区。
带宽上限	1-2000Mbps。
实例	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。

版权所有：建行云

名	

3.确认申请实例数量，单击【确认开通】。

4.完成负载均衡服务申请，即可进行负载均衡配置使用。

创建IPV6负载均衡实例

最近更新时间: 2023-12-06 15:55:22

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

建行云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（简称：IPv6 CLB）实例，建行云会给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。

操作流程

步骤一：创建IPv6负载均衡实例

1. 登录建行云负载均衡申请页，点击新建。
2. 选择对应的地域、实例类型等参数，进行负载均衡相关配置。

参数	说明
地域	选择所属地域
实例类型	应用型LB
网络类型	公网
可用区类型	单可用区
IP 版本	IPv6
网络	选择所属VPC和子网。用户创建公网IPv6负载均衡时，建行云在选定的子网网段下随机分配负载均衡VIP。
运营商类型	运营商类型分为：外网IP或外网CAP
带宽上限	1-2000Mbps。

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. 在申请页选择各项配置后，单击确认开通。
4. 确认后即可完成IPv6负载均衡申请。

步骤二：创建 IPv6 负载均衡监听器

5. 登录建行云租户控制台，点击负载均衡模块，选择IPv6负载均衡实例ID，进入详情页。
6. 选择监听器管理标签页，单击【新建】，如创建一个TCP监听器。
7. 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】。
8. 配置健康检查，单击【下一步】。
9. 配置会话保持，单击【提交】。
10. 监听器创建完成后，选中该监听器，单击【绑定】。
11. 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】完成创建。

版权所有：建行云

导出负载均衡实例

最近更新时间: 2023-03-17 09:50:29

用户可导出某地域的负载均衡实例列表，以便分析实例资源配置和使用情况。

具体操作步骤：

1.登录建行云租户控制台，点击负载均衡模块，在“LB实例列表”页面左上角选择所在地域。

2.在实例列表中，并点击下载图标，可将实例列表下载至本地。

删除负载均衡实例

最近更新时间: 2023-03-17 09:50:29

当负载均衡实例已不再使用后，可对该实例进行删除。实例删除后将彻底销毁，无法恢复。因此，在删除实例之前，请务必先解绑所有后端云服务器并观察一段时间后，再进行删除操作，以免影响到正常业务。

通过控制台删除负载均衡实例的具体操作步骤：

1.登录建行云租户控制台，点击负载均衡模块。

2.选择需要删除的负载均衡实例，单击【删除】按钮。

3.确认删除后将完成负载均衡的删除工作。

版权所有：建行云

负载均衡监听器
负载均衡监听器概述

最近更新时间: 2023-03-17 16:30:35

创建负载均衡实例后，用户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，并依据均衡策略将分发流量至后端服务器上。

负载均衡监听器需配置：

1.监听协议和监听端口。负载均衡的监听端口，亦被称为前端端口，用来接收请求并向后端服务器转发请求的端口。

2.监听策略，如均衡策略、会话保持 等。

3.健康检查 策略。

4.绑定后端服务。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。

如果用户使用四层监听器（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。

建行云负载均衡支持以下协议的请求转发：

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

协议分类	协议	说明	应用场景
四层协议	TCP	面向连接的、可靠的传输层协议 • 传输的源端和终端需先三次握手建立连接，再传输数 • 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	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。

		• 服务端可直接获取客户端IP	
	UDP	无连接的传输层协议 • 传输的源端和终端不建立连接，不需维护连接状态 • 每一条 UDP 连接都只能是点到点的 • 支持一对一，一对多，多对一和多对多的交互通信 • 支持基于客户端 IP（源IP）的会话保持 • 服务端可直接获取客户端IP	适用于对传输效率要求高、对准确性要求相对较低的场景，如即时通讯、在线视频等。
七层协议	HTTP	应用层协议 • 支持基于请求域名和 URL 的转发 • 支持基于 Cookie 的会话保持	需要对请求的内容进行识别的应用，例如 Web 应用、App 服务等。
	HTTPS	加密的应用层协议 • 支持基于请求域名和 URL 的转发 • 支持基于 Cookie 的会话保持 • 统一的证书管理服务，CLB 完成解密操作 • 支持单向认证和双向认证	需加密传输的 HTTP 应用。

端口配置

端口类型	说明	限制
监听端口（负载均衡端口）	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。 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。	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/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RS服	服务端口是云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	在同一个负载均衡实例内： • 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

务端口）	监听端口可以将流量转发到多个云服务器的多个端口上。	台云服务器的同一个端口。 • 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。

配置TCP监听器

配置TCP监听器

最近更新时间: 2023-03-17 14:17:49

用户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

最近更新时间: 2023-03-17 14:17:49

用户需要 创建负载均衡实例。

版权所有：建行云

操作步骤

步骤一：配置监听器

最近更新时间: 2023-03-17 14:40:09

1. 登录建行云租户控制台，点击负载均衡模块，单击【LB实例列表】。
2. 选择对应的CLB实例，进入详情页。
3. 在 TCP/UDP 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。

1. 基本配置

监听器基本配置	说明	示例
名称	监听器的名称。	clbtest-tcp80

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

2. 健康检查 健康检查详情请参见健康检查中的 TCP健康检查。 3. 会话保持

会话保持配置	说明	示例
会话保持开关	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。 • 按权重轮询调度支持会话保持，加权最小连接数调度不支持开启会话保持功能。 注：要求关闭会话保持功能，非必要不开启	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

步骤二：绑定后端云服务器

最近更新时间: 2023-03-17 14:40:09

1. 在“监听器管理”页面，选择已创建的监听器，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。
   注：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。

步骤三：修改/删除监听器（可选）

最近更新时间: 2023-03-17 14:40:05

如果用户需要修改或删除已创建的监听器，请在“监听器管理”页面，单击已创建完毕的监听器，单击修改或删除图标按钮。

配置UDP监听器

配置UDP监听器

最近更新时间: 2023-03-17 14:40:05

用户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。

前提条件

最近更新时间: 2023-03-17 14:40:05

用户需要 创建负载均衡实例。

版权所有：建行云

操作步骤

步骤一：配置监听器

最近更新时间: 2023-03-17 15:41:44

1.登录建行云租户控制台，点击负载均衡模块，单击【LB实例列表】。

2.选择对应的CLB实例，进入详情页。

3.在 TCP/UDP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。

1. 基本配置

监听器基本配置	说明	示例
名称	监听器的名称。	clbtest-udp8000

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

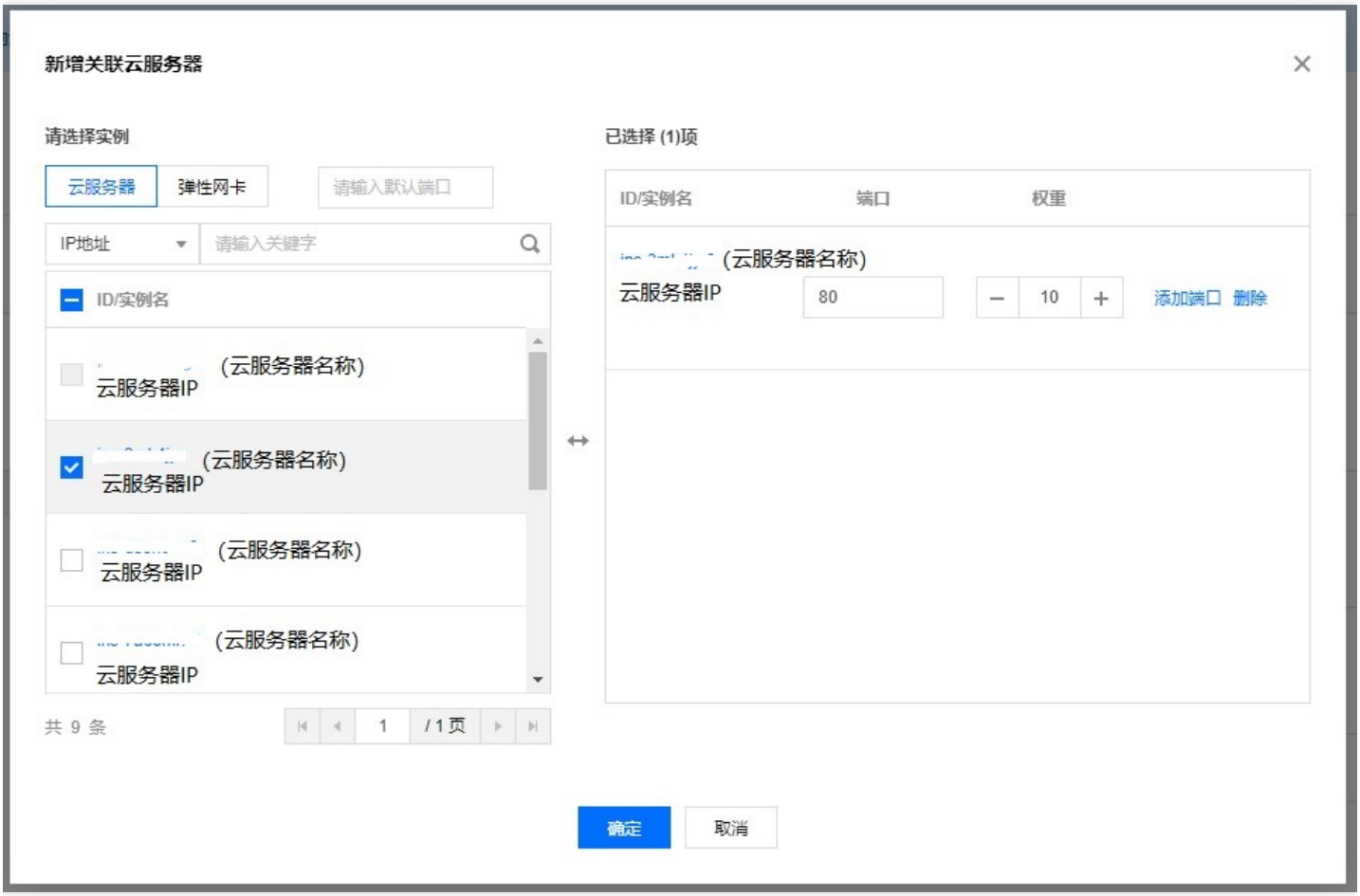
2. 健康检查 健康检查详情请参见健康检查中的 UDP健康检查。 3. 会话保持

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。 • 按权重轮询调度支持会话保持，加权最小连接数调度不支持开启会话保持功能。 注：要求关闭会话保持功能，非必要不开启	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

步骤二：绑定后端云服务器

最近更新时间: 2023-03-17 15:41:43

1. 在“监听器管理”页面，单击已创建的监听器，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
   注：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。



步骤三：修改/删除监听器（可选）

最近更新时间: 2023-03-17 15:41:38

如果用户需要修改或删除已创建的监听器，请在“监听器管理”页面，单击已创建完毕的监听器，单击修改或删除。

配置HTTP监听器

配置HTTP监听器

最近更新时间: 2023-03-17 14:40:05

用户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。

版权所有：建行云

前提条件

最近更新时间: 2023-03-17 14:40:05

用户需要 创建负载均衡实例。

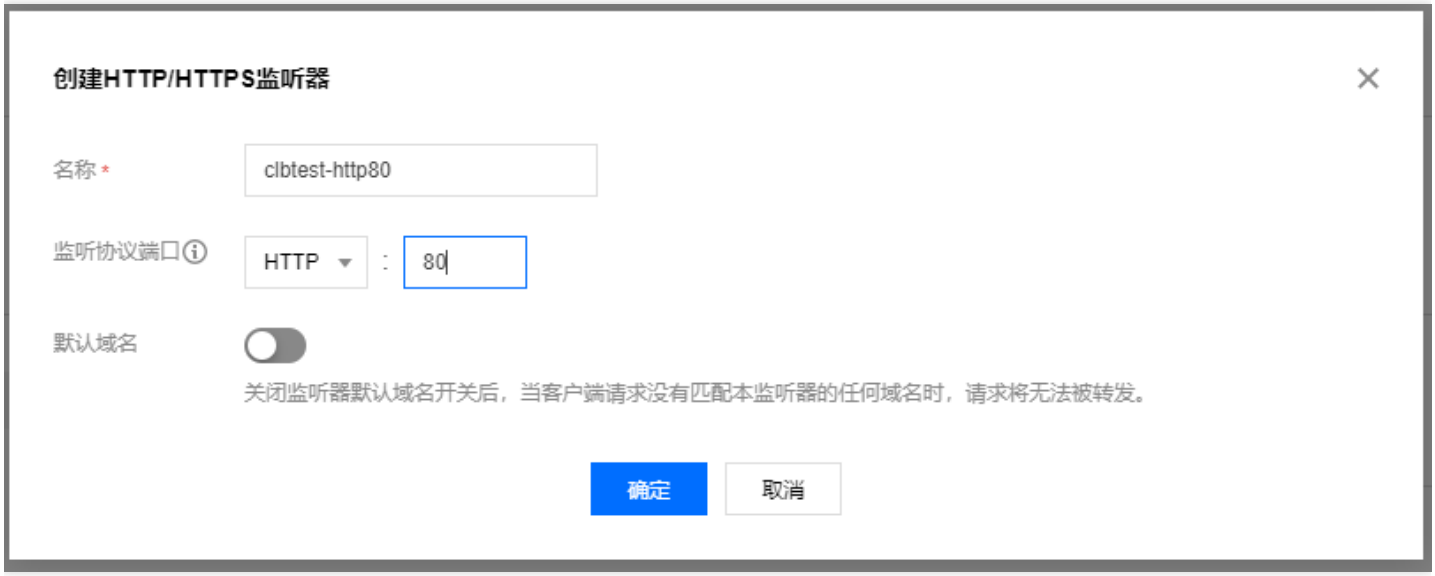
版权所有：建行云

操作步骤

步骤一：配置监听器

最近更新时间: 2023-03-17 15:41:38

1. 登录建行云租户控制台，点击负载均衡模块，左侧导航栏单击【LB实例列表】。
2. 选择对应的CLB实例，进入详情页。
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。



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。	clbtest-http80
监听协议	• 监听协议：本示例选择 HTTP。 • 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，843、1020、1433、1434、3306、3389、6006、20000、36000、42222、48369、56000、65010端口为系统保留端口，暂不对外开放。 • 同一个负载均衡实例内，监听端口不可重复。	HTTP:80

版权所有：建行云

端口		
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。 要求：默认域名关闭	默认关闭

2.创建转发规则

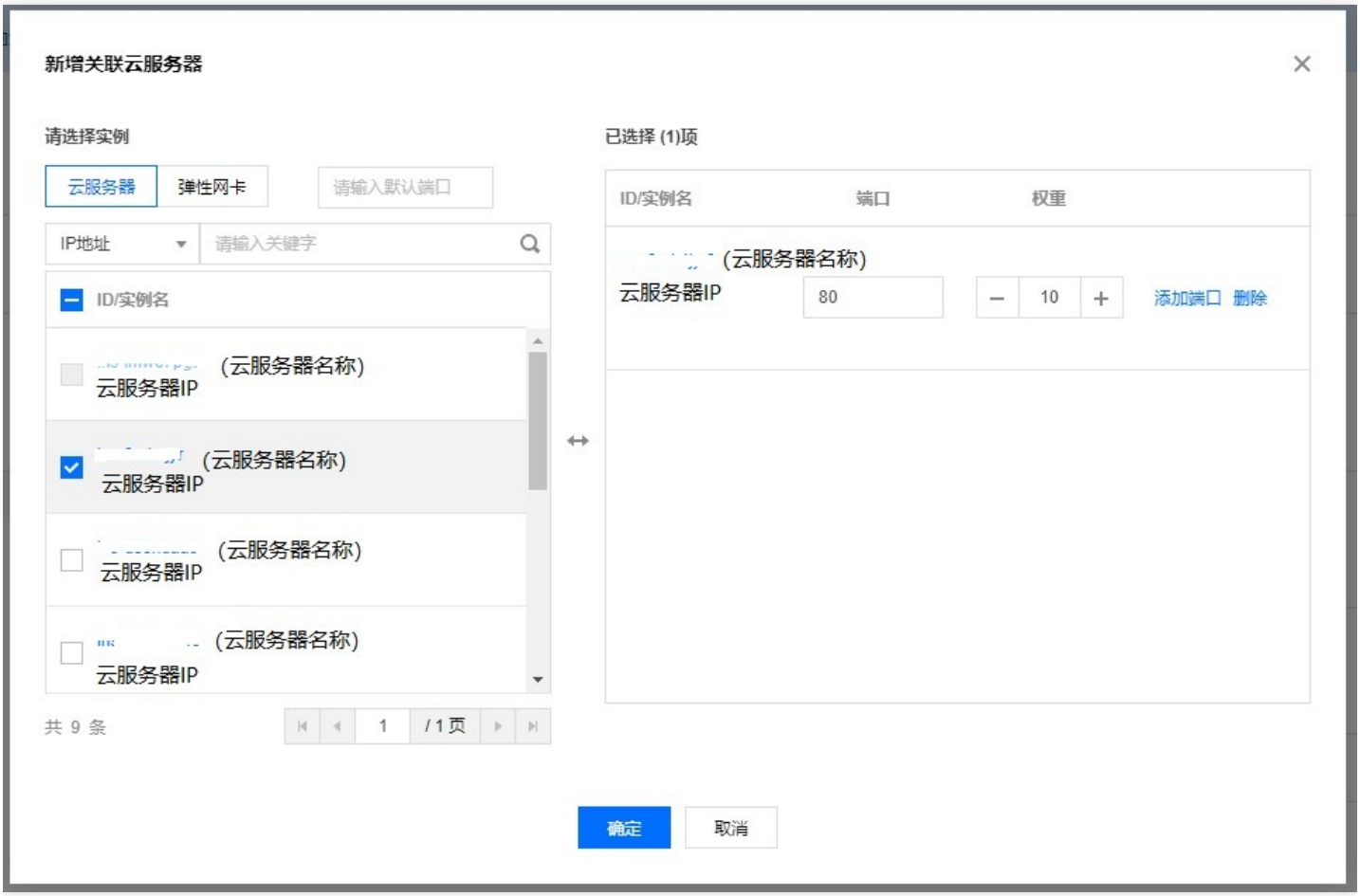
转发规则基本配置	说明	示例
域名	转发域名： • 长度限制：1 – 80个字符。 不能以 _ 开头。 • 支持精准域名和通配域名。 • 支持正则表达式。 • 具体配置规则，详情请参见 转发域名配置规则。	www.clbtest.com
URL路径	转发 URL 路径： • 长度限制：1 – 200个字符。 • 支持正则表达式。 • 具体配置规则，详情请参见 转发 URL 路径配置规则。	/index1
均衡方式	HTTP 监听器中，负载均衡支持按权重轮询（WRR）、加权最小连接数（WLC）和 IP Hash 三种调度算法： • 按权重轮询：根据后端服务器的权重，按依次将请求分发给不同的服务器。按权重轮询根据**新建连接数**来调度，权值高的服务器被轮询到的次数（概率）越高，相同权值的服务器处理相同数目的连接数。 • 加权最小连接数：根据服务器当前活跃的连接数来估计服务器的负载情况，加权最小连接数根据服务器负载和权重来综合调度，当权重值相同时，当前连接数越小的后端服务器被轮询到的次数（概率）也越高。 • IP Hash：根据请求的源 IP 地址，使用散列键（Hash Key）从静态分配的散列表找出对应的服务器，若该服务器为可用且未超载状态，则请求发送到该服务器，反之则返回空。	按权重轮询

3. 健康检查 健康检查详情请参见健康检查中的 HTTP健康检查。 4. 会话保持

步骤二：绑定后端云服务器

最近更新时间: 2023-03-17 15:41:38

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。
   注：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。



步骤三：修改/删除监听器（可选）

最近更新时间: 2023-03-17 15:41:38

如果用户需要修改或删除已创建的监听器，请在“监听器管理”页面，单击已创建完毕的监听器，单击修改或删除。

配置HTTPS监听器

配置HTTPS监听器

最近更新时间: 2023-03-17 14:40:05

用户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。

版权所有：建行云

前提条件

最近更新时间: 2023-03-17 14:40:04

用户需要 创建负载均衡实例。

版权所有：建行云

操作步骤

步骤一：配置监听器

最近更新时间: 2023-03-17 15:41:38

1. 登录建行云租户控制台，点击负载均衡模块，左侧导航栏单击【LB实例列表】。
2. 选择对应的CLB实例，进入详情页。
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。

1. 创建监听器

监听器基本配置	说明	示例
名	监听器的名称。	clbtest-

称		https443
监听协议端口	• 监听协议：本示例选择 HTTPS。 • 监听端口：用来接收请求并向后端服务器转发请求的端口，端口范围为1 – 65535。其中，843、1020、1433、1434、3306、3389、6006、20000、36000、42222、48369、56000、65010端口为系统保留端口，暂不对外开放。 • 同一个负载均衡实例内，监听端口不可重复。	HTTPS:443
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。 要求：默认域名关闭	默认关闭
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 证书管理中已有的证书，或上传证书。	单向认证

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.clbtest.com
URL路径	转发 URL 路径： • 长度限制：1 – 200个字符。 • 支持正则表达式。 • 具体配置规则，详情请参见 转发 URL 路径配置规则。	/index1
均衡	HTTPS 监听器中，负载均衡支持加权轮询（WRR）、加权最小连接数	按权重轮询

方式	（WLC）和 IP Hash 三种调度算法： • 按权重轮询：根据后端服务器的权重，按依次将请求分发给不同的服务器。按权重轮询根据**新建连接数**来调度，权值高的服务器被轮询到的次数（概率）越高，相同权值的服务器处理相同数目的连接数。 • 加权最小连接数：根据服务器当前活跃的连接数来估计服务器的负载情况，加权最小连接数根据服务器负载和权重来综合调度，当权重值相同时，当前连接数越小的后端服务器被轮询到的次数（概率）也越高。 • IP Hash：根据请求的源 IP 地址，使用散列键（Hash Key）从静态分配的散列表找出对应的服务器，若该服务器为可用且未超载状态，则请求发送到该服务器，反之则返回空。	

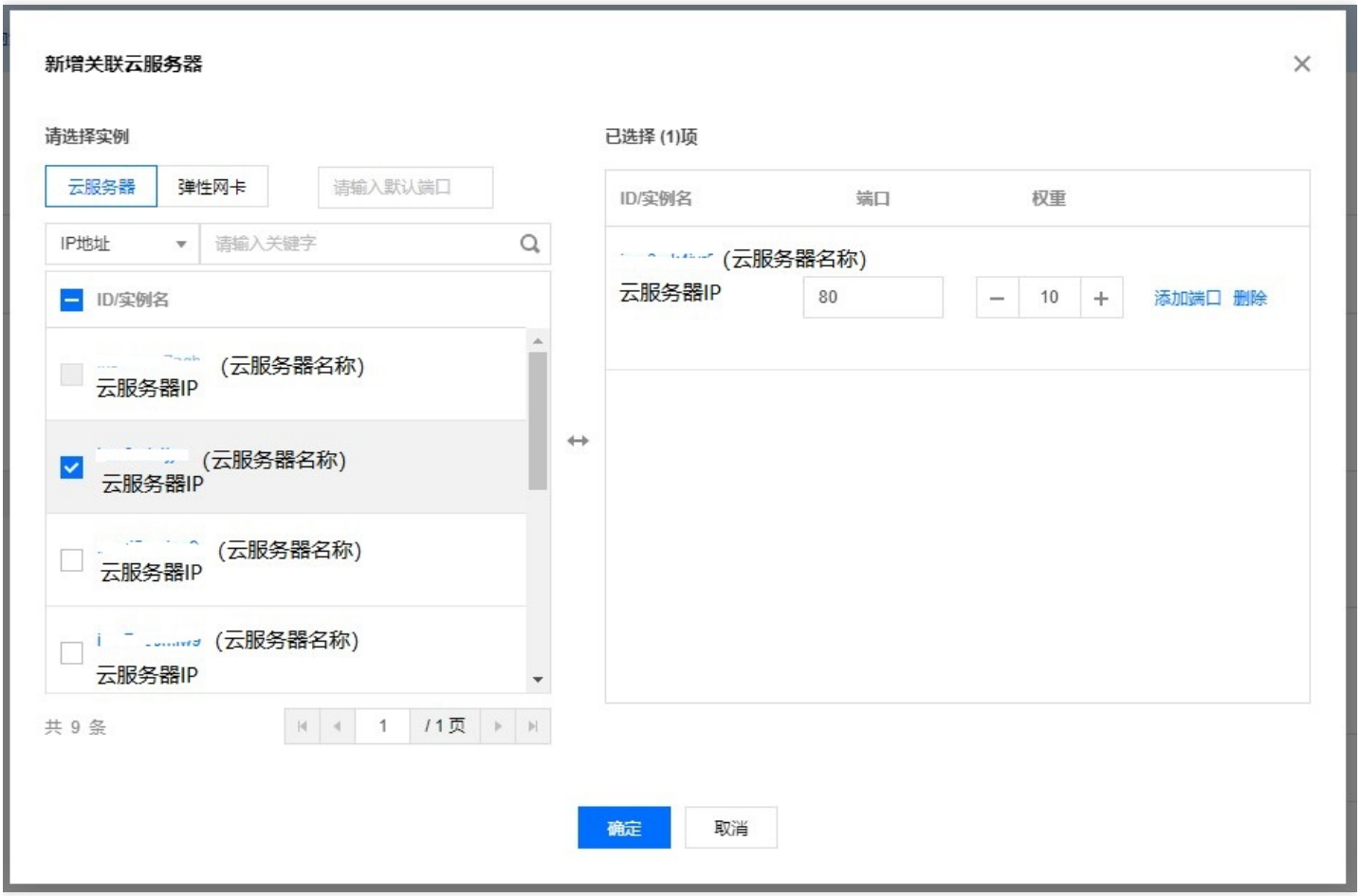
3. 健康检查 健康检查详情请参见 HTTPS健康检查。 4. 会话保持

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。 • 按权重轮询调度支持会话保持，加权最小连接数调度不支持开启会话保持功能。 注：要求关闭会话保持功能，非必要不开启	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

步骤二：绑定后端云服务器

最近更新时间: 2023-03-17 15:41:38

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。
   注：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。



步骤三：修改/删除监听器（可选）

最近更新时间: 2023-03-17 15:41:38

如果用户需要修改或删除已创建的监听器，请在“监听器管理”页面，单击已创建完毕的监听器，单击修改或删除图标按钮。

均衡方式

最近更新时间: 2023-03-17 11:35:46

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。推荐使用按权重轮询。

1.按权重轮询

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

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

2.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。

- 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。

3.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。

版权所有：建行云

• 用户推荐：将请求的源地址进行哈希运算，并结合用户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。

会话保持

最近更新时间: 2023-03-17 11:35:46

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。

注：建议用户按需配置会话保持功能。

1.四层会话保持

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：

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

2.七层会话保持

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

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

3.连接超时时间

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

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

4.配置会话保持

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

版权所有：建行云

七层重定向配置

七层重定向配置

最近更新时间: 2023-03-17 15:41:38

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。 注：

- 会话保持：如果客户端访问了 clbtest.com/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 clbtest.com/test/456.html 时，原会话保持机制将失效。

重定向概述

最近更新时间: 2023-03-17 15:41:38

• 自动重定向

o 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。

o 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。

o 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

o 简介

用户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。

注：若域名已经配置过自动重定向，则无法再配置手动重定向。

版权所有：建行云

自动重定向

最近更新时间: 2023-03-17 15:41:38

建行云 CLB 支持一键式的 HTTP 强转 HTTPS。
假定开发者需要配置网站 https://www.clbtest.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.clbtest.com） 还是 HTTPS 请求（https://www.clbtest.com）， 都可通过 HTTPS 协议进行安全访问。

前提条件

已配置HTTP:443 监听器。

操作步骤

1. 请在建行云负载均衡控制台完成 CLB的HTTPS监听器的配置，搭建https://clbtest.com 的Web环境。详情请参见 配置HTTPS监听器 。
2. 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】。
3. 选择自动重定向配置，并选择已配置的HTTPS监听器和域名，单击【下一步：配置路径】。
4. 单击【提交】即可完成配置。
5. 完成重定向配置后，可以看到已为HTTPS:443 监听器自动配置了HTTP:80 监听器，且 HTTP 的流量均会被自动重定向到 HTTPS。

版权所有：建行云

手动重定向

最近更新时间: 2023-03-17 15:41:33

建行云 CLB 支持配置一对一的重定向跳转。例如，可将页面https://www.clbtest.com/index1 重定向至新主页 https://www.newclbtest.com/index2。

前提条件

- 已配置 HTTPS 监听器。
- 已配置转发域名https://www.clbtest.com/index1。
- 已配置转发域名和路径https://www.newclbtest.com/index2。

操作步骤

1. 请在建行云负载均衡控制台完成CLB的HTTPS监听器的配置，搭建https://clbtest.com的 Web 环境。详情请参见 配置HTTPS监听器。
2. 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】。
3. 选择手动重定向配置，选择原访问的前端协议端口HTTPS:443和域名https://www.clbtest.com/index1，选择重定向后的前端协议端口HTTPS:443 和域名https://www.newclbtest.com/index2， 单击【下一步：配置路径】。
4. 原访问路径选择/index1，重定向后的访问路径选择/index2，单击【提交】即可完成配置。
5. 完成重定向配置后，可以看到HTTP:443 监听器中，https://www.clbtest.com/index1 已重定向至 https://www.newclbtest.com/index2。

版权所有：建行云

七层转发域名和URL规则说明
七层转发配置说明

最近更新时间: 2024-11-06 16:38:09

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 配置负载均衡的转发域名。

- 转发域名长度限制：1 - 80个字符。
- 不能以 _ 开头。
- 支持精准域名，如 www.clbtest.com。
- 支持通配域名，目前仅支持 *.clbtest.com 或者 www.clbtest.* 的形式，即 * 在开头或结尾，且单个域名中仅支持 * 出现一次。
- 非正则表达式的转发域名，支持的字符集为：a-z 0-9 . - 。
- 转发域名支持正则表达式，正则表达式的域名：
  - 支持的字符集为： a-z 0-9 . - ? = ~ _ - + \ ^ * ! $ & | ( ) [ ]。
  - 需以 ~ 开头，且 ~ 仅能出现一次。
  - 负载均衡支持的正则域名举例如下：~^www\d+.clbtest.com$。

转发域名匹配说明

最近更新时间: 2023-03-17 15:55:08

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clbtest.qcould.com 为例，格式如下所示：
   - 精准域名 clbtest.qcloud.com，精确匹配 clbtest.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 clbtest.qcloud.* 匹配所有以 clbtest.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：精准域名 > 前缀通配符域名 > 后缀通配符域名 > 正则表达式域名，同一级域名如果有多个域名同时命中，匹配顺序无法保证先后，建议使用更加精准的域名以避免多个规则同时命中的情况。
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：www.clbtest1.com ，www.clbtest2.com，其中 www.clbtest1.com 是默认域名。当用户访问 www.clbtest.com 时，由于没有匹配到任何一个域名，CLB会将该请求转发给默认域名 www.clbtest1.com。
注：根据安全要求，用户须保持监听器默认域名按钮关闭。

版权所有：建行云

转发 URL 路径配置规则

最近更新时间: 2023-03-17 15:55:08

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。

- 转发 URL 长度限制：1 – 200个字符。
- 非正则表达式的转发 URL ，必须以 / 开头，支持的字符集为：a–z A–Z 0–9 . – _ / = ? :。
- 转发 URL 支持正则表达式：
  - 正则表达式的 URL，需以 ~ 开头，且 ~ 仅能出现一次。
  - 正则表达式的 URL 支持的字符集为： a–z A–Z 0–9 . – _ / = ? ~ ^ * $: ( ) [ ] + |。
  - 正则表达式的 URL 举例如下：~*.png$。
- 转发 URL 匹配规则如下：
  - = 开头表示精确匹配。
  - ^~ 开头表示 URL 以某个常规字符串开头，不是正则匹配。
  - ~开头表示区分大小写的正则匹配。
  - ~* 开头表示不区分大小写的正则匹配。
  - / 通用匹配，如果没有其它匹配，任何请求都会匹配到。

转发 URL 路径匹配说明

1、 匹配规则：按最长前缀匹配，优先精确匹配，而后模糊匹配。

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、 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）

版权所有：建行云

七层健康检查配置说明

最近更新时间: 2023-03-17 15:55:08

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，当用户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 . - _。

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 . - _ / = ? :。

版权所有：建行云

后端服务器
后端云服务器概述

最近更新时间: 2024-04-08 11:05:29

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支持实例类型，包括云服务器 CVM与弹性网卡 ENI。

版权所有：建行云

管理后端服务器
后端云服务器简述

最近更新时间: 2024-04-08 11:05:29

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。

版权所有：建行云

前提条件

最近更新时间: 2023-03-17 11:21:10

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。

版权所有：建行云

操作步骤

添加负载均衡后端云服务器

最近更新时间: 2023-03-17 11:30:41

1. 登录建行云租户控制台，点击负载均衡模块。
2. 在“LB实例列表”页，单击目标负载均衡实例进行详情页。
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
   a. 在 HTTP/HTTPS 监听器区域，单击目标监听器左侧的+。
   b. 在展开的域名左侧单击+
   c. 选中展开的 URL 路径，单击【绑定】。
   • 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。
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，单击【确定】。
   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、再勾选相关服务器并设定权重值，单击【确定】。

版权所有：建行云

修改负载均衡后端服务器权重

最近更新时间: 2023-03-17 11:30:41

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），为用户介绍如何修改负载均衡后端服务器权重。

1. 登录建行云租户控制台，点击负载均衡模块。
2. 在“LB实例列表”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。
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。

注：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。

方式1：单独修改某台服务器权重。

a. 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】。

b. 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。

a. 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. 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

最近更新时间: 2023-03-17 11:30:41

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），为用户介绍如何修改负载均衡后端服务器端口。

1. 登录建行云租户控制台，点击负载均衡模块。
2. 在“LB实例列表”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。
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。

方式1：单独修改某台服务器端口。

a.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.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。

a.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】。

b.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

最近更新时间: 2023-03-17 11:30:41

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），为用户介绍如何解绑已绑定的负载均衡后端服务器。

1. 登录建行云租户控制台，点击负载均衡模块。
2. 在“LB实例列表”页面，点击进去目标负载均衡实例详情页。
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 。
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。

a.找到需要解绑的服务器，在右侧操作栏，单击【解绑】。

b.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。

a.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】。

b.在“解绑”弹窗中，确认解绑的服务，单击【提交】。

管理弹性网卡
弹性网卡简介

最近更新时间: 2024-04-08 11:08:41

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。

版权所有：建行云

前提条件

最近更新时间: 2023-03-17 11:21:10

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

最近更新时间: 2024-04-08 11:10:34

绑定弹性网卡

1. 首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。
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。

解绑弹性网卡

- 手动解绑 负载均衡控制台支持解绑已绑定的弹性网卡，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），为用户介绍如何解绑已绑定的ENI。

1. 登录建行云租户控制台，点击负载均衡模块。
2. 在“LB实例列表”页面，点击进去目标负载均衡实例详情页。
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 。
4. 在 HTTP/HTTPS 监听器模块右侧服务器列表中，找到需要解绑的服务器，在右侧操作栏，单击【解绑】。
5. 在“解绑”弹窗中，确认解绑的服务，单击【提交】。

- 自动解绑

当用户进行云服务器与弹性网卡的解绑操作后，为保证流量转发的有效性以及减少资源浪费，负载均衡会自动解绑此弹性网卡。

版权所有：建行云

健康检查

健康检查概述

健康检查概述

最近更新时间: 2023-03-17 10:49:57

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CVM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。用户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CVM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 CVM，而不会转发到异常的CVM。
- 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CVM。
- 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），因此强烈建议用户打开健康检查，允许负载均衡帮用户自动检查并移除异常的后端服务器。

版权所有：建行云

健康检查状态

最近更新时间: 2023-03-17 10:49:57

根据健康检查探测情况，后端 CVM 的健康检查状态如下所示：

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

版权所有：建行云

TCP 健康检查

最近更新时间: 2023-03-17 10:49:51

针对四层 TCP 监听器，用户可以配置 TCP 健康检查，通过 SYN 包即发起 TCP 三次握手来获取后端 CVM 的状态信息。用户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 CVM 的状态信息。

TCP 健康检查机制如下：

1. 负载均衡向后端 CVM（内网IP 地址+健康检查端口）发送 SYN 连接请求报文。
2. 后端 CVM 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。
3. 若在响应超时时间内，负载均衡收到后端 CVM 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 CVM 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 CVM 返回的 SYN+ACK 应报文，则表示服务运行异常，判定健康检查失败，并向后端 CVM 发送 RST 复位报文中断 TCP 连接。

版权所有：建行云

UDP 健康检查

最近更新时间: 2023-03-17 10:49:51

针对四层 UDP 监听器，用户可以配置 UDP 健康检查，通过Ping命令和向健康检查端口发送 UDP 探测报文来获取健康状态。用户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 CVM 的状态信息。

UDP 健康检查机制如下：

1. 负载均衡向后端 CVM 的内网 IP 地址发起Ping命令；
2. 负载均衡向后端 CVM（内网 IP 地址+健康检查端口）发送 UDP 探测报文；
3. 若Ping成功，且在响应超时时间内，后端 CVM 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；
4. 若Ping失败，或者在响应超时时间内，系统收到后端 CVM 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；

版权所有：建行云

HTTP 健康检查

最近更新时间: 2023-03-17 10:49:51

针对四层 TCP 监听器和七层 HTTP/HTTPS监听器，可以配置 HTTP 健康检查，通过发送 HTTP 请求来获取后端 CVM 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CVM（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 CVM 收到请求后返回相应的 HTTP 状态码。
3. 若在响应超时时间内，负载均衡收到了后端CVM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CVM的响应，则判定健康检查失败。

版权所有：建行云

健康检查时间窗

最近更新时间: 2023-03-17 10:49:51

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

四层健康检查时间窗的计算方法如下： 健康检查失败时间窗=检查间隔×（不健康阈值–1） 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 =5x（3–1）=10s。 健康检查成功时间窗=检查间隔×（健康阈值–1） 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= 5x（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） 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 =2x3+5x（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）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=1x3+5x（3–1）=13s。

版权所有：建行云

配置健康检查

配置健康检查

最近更新时间: 2023-03-17 10:49:51

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。

版权所有：建行云

前提条件

最近更新时间: 2023-03-17 10:49:51

1. 用户已创建负载均衡实例，详情请参见创建负载均衡实例。
2. 用户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 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。

版权所有：建行云

TCP监听器

TCP 监听器

最近更新时间: 2023-03-17 11:09:40

四层 TCP 监听器支持四层 TCP、七层 HTTP 和自定义协议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 CVM 的状态信息。
- HTTP 健康检查通过发送 HTTP 请求来获取后端 CVM 的状态信息。
- 自定义协议通过自定义应用层协议的输入和输出内容来获取后端 CVM 的状态信息。

版权所有：建行云

配置 TCP 健康检查

最近更新时间: 2023-03-17 11:09:40

针对四层TCP监听器转发规则可配置TCP健康检查，

1. 创建TCP监听器并完成基本配置；
2. 配置健康检查，可打开健康检查开关，并按需配置响应超时时间、检测间隔时间、不健康阈值次数、健康阈值次数等信息。
3. 即可完成四层TCP健康检查配置。

UDP监听器

UDP 监听器

最近更新时间: 2023-03-17 11:09:39

UDP监听器支持UDP健康检查，主要为PING检查。

配置 UDP 健康检查

最近更新时间: 2023-03-17 11:09:39

针对四层UDP监听器转发规则可配置UDP健康检查，

1. 创建UDP监听器并完成基本配置；

2. 配置健康检查，可打开健康检查开关，并按需配置响应超时时间、检测间隔时间、不健康阈值次数、健康阈值次数等信息。

3. 即可完成四层UDP健康检查配置。

HTTP监听器
配置 HTTP 健康检查

最近更新时间: 2023-03-17 11:09:39

针对七层HTTP监听器转发规则配置HTTP健康检查，

1. 选择指定的HTTP监听器，创建HTTP监听器转发规则并完成基本配置；
2. 配置健康检查，可打开健康检查开关，并按需配置检查域名、检查目录、检测间隔时间、不健康阀值次数、健康阀值次数，以及HTTP请求方式和需要检测的HTTP状态码等信息。
3. 即可完成七层HTTP健康检查配置。

版权所有：建行云

创建HTTP/HTTPS转发规则
基本配置
2
健康检查
3
会话保持
健康检查
检查域名
不填则默认转发域名
检查目录
后端服务器根目录
/
检测间隔
5秒
300秒
5
秒
不健康阈值
2次
10次
3
次
健康阈值
2次
10次
3
次
HTTP请求方式
HEAD
HTTP状态码检测
http_1xx
http_2xx
http_3xx
http_4xx
http_5xx
当状态码为http_1xx、http_2xx、http_4xx、http_5xx时，认为后端服务器存活
上一步：基本配置
下一步：会话保持
取消

HTTPS监听器
配置 HTTPS 健康检查

最近更新时间: 2023-03-17 11:09:39

针对七层HTTPS监听器转发规则配置HTTPS健康检查，

1. 选择指定的HTTPS监听器，创建HTTPS监听器转发规则并完成基本配置；
2. 配置健康检查，可打开健康检查开关，并按需配置检查域名、检查目录、检测间隔时间、不健康阀值次数、健康阀值次数，以及HTTP请求方式和需要检测的HTTP状态码等信息。
3. 即可完成七层HTTPS健康检查配置。

版权所有：建行云

创建HTTP/HTTPS转发规则
基本配置
2
健康检查
3
会话保持
健康检查
检查域名
不填则默认转发域名
检查目录
后端服务器根目录
/
检测间隔
5秒
300秒
5
秒
不健康阈值
2次
10次
3
次
健康阈值
2次
10次
3
次
HTTP请求方式
HEAD
HTTP状态码检测
http_1xx
http_2xx
http_3xx
http_4xx
http_5xx
当状态码为http_1xx、http_2xx、http_4xx、http_5xx时，认为后端服务器存活
上一步：基本配置
下一步：会话保持
取消

证书管理
管理证书
管理证书

最近更新时间: 2023-03-17 10:10:32

在配置负载均衡的 HTTPS 监听器时，用户可以将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

最近更新时间: 2023-03-17 10:10:32

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

配置证书

最近更新时间: 2023-03-17 10:10:32

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。

版权所有：建行云

更新证书

最近更新时间: 2023-03-17 10:10:32

为避免证书过期对用户的服务产生影响，请在证书过期前更新证书。

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

版权所有：建行云

查看证书关联的负载均衡

最近更新时间: 2023-03-17 09:59:56

1. 登录建行云租户控制台，点击负载均衡模块。
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。

版权所有：建行云

证书要求及转换证书格式
证书上传流程

最近更新时间: 2023-03-17 10:10:32

（1）登录建行云控制台，选择“负载均衡”-“证书管理”，进入证书管理页面。

（2）点击“新建”按钮，在“新建证书”弹出页中，填入“证书名称”、选择“证书类型”（目前有服务器证书和客户端CA证书）

（3）如果选择“服务器证书”，则将生成的证书和秘钥分别粘贴到“证书内容”和“秘钥内容”的文本框，点击【创建】。

注：证书和私钥必须为pem格式

版权所有：建行云

（4）如果选择“客户端CA证书”，则将生成的证书粘贴到“证书内容”的文本框，点击【创建】。

新建证书
证书名称
请输入名称
长度限制为1-80个字符，只能使用中文、英文、数字、下划线、分隔符"-"、小数点
证书类型
服务器证书
客户端CA证书
证书内容
PEM编码
查看样例
创建
取消

常用证书申请流程

最近更新时间: 2023-03-17 10:10:32

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

版权所有：建行云

证书格式要求

最近更新时间: 2023-03-17 10:10:32

• 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，如是其它格式的证书请参考本文“负载均衡支持的证书格式及转换方式”部分内容。
• 如果是通过root CA机构颁发的证书， 用户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，用户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。
• 当用户的证书有证书链时，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。注：一般情况下，机构在颁发证书的时候会有对应说明， 请注意规则说明。
以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：

版权所有：建行云

```
-----BEGIN CERTIFICATE-----
MIIE+TCCA+GgAwIBAgIQU306HIX4KsioTW1s2A2krTANBgkqhkiG9w0BAQUFADCB
tTELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
ExZWZXJpU2lnbiBUcnVzdCBOZXR3b3JrMTswOQYDVQQLEzJUZXJtcyBvZiB1c2Ug
YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL3JwYSoAYykwOTEvMC0GA1UEAxMm
VmVyaVNpZ24gQ2xhc3MgMyBTZWN1cmUgU2VydmVyIENBIC0gRzIwHhcNMTAxMDA4
MDAwMDAwWhcNMTMxMDA3MjM1OTU5WjBqMQswCQYDVQQGEwJVUzETMBEGA1UECBMK
V2FzaGluZ3RvbjEQMA4GA1UEBxQHU2VhdHRsZTEYMBYGA1UEChQPQW1hem9uLmNv
bSBJbmMuMRowGAYDVQQDFBFpYW0uYW1hem9uYXdzLmNvbTCBnzANBgkqhkiG9w0B
AQEFAAOBjQAwgYkCgYEA3Xb0EGea2dB8QGEUwLcEpwvGawEkUdLZmGL1rQJZdeeN
3vaF+ZTm8Qw5Adk2Gr/RwYXtpx04xvQXmNm+9YmksHmCZdruCrW1eN/P9wBfqMMZ
X964CjVov3NrF5AuxU8jgtw0yu//C3hWn0uIVGdg76626gg0oJSaj48R2n0MnVcC
AwEAAaOCAdEwggHNMAkGA1UdEwQCMAAwCwYDVR0PBAQDAgWgMEUGA1UdHwQ+MDww
OqA4oDaGNGh0dHA6Ly9TVlJTZWN1cmUtRzItY3JsLnZlcmlzaWduLmNvbS9TVlJT
ZWN1cmVHMi5jcmwwRAYDVR0gBD0wOzA5BgtghkgBhvhFAQcXAzAqMCgGCCsGAQUF
BwIBFhxodHRwczovL3d3dy52ZXJpc2lnbi5jb20vcnBhMB0GA1UdJQQWMBQGCCsG
AQUFBwMBBggrBgEFBQcDAjAfBgNVHSMEGDAWgBSl7wsRzsBBA6NKZZBIshzgVy19
RzB2BggrBgEFBQcBAQRqMGgwJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLnZlcmlz
aWduLmNvbTBABggrBgEFBQcwAoY0aHR0cDovL1NWUlNlY3VyZS1HMi1haWEudmVy
aXNpZ24uY29tL1NWUlNlY3VyZUcyLmNlcjBuBggrBgEFBQcBDARiMGChXqBcMFow
WDBWFglpbWFnZS9naWYwITAfMAcGBSsOAwIaBBRLa7kolgYMu9BSOJsprEsHiyEF
GDAmFiRodHRwOi8vbG9nby52ZXJpc2lnbi5jb20vdnNsb2dvMS5naWYwDQYJKoZI
hvcNAQEFBQADggEBALpFBXeG782QsTtGwEE9zBcVCuKjrsl3dWK1dFiq30P4y/Bi
ZBYEywBt8zNuYFUE25Ub/zmvmpe7p0G76tmQ8bRp/4qkJoiSesHJvFgJ1mksr3IQ
3gaE1aN2BSUIHxGLn9N4F09hYwwbeEZaCxfgBiLdEIodNwzcvGJ+2LlDWGJOGrNI
NM856xjqhJCPxYzk9buuCl1B4Kzu0CTbexz/iEgYV+DiuTxcfA4uhwMDSe0nynbn
1qiwRk450mCOnqH4ly4P4lXo02t4A/DI1I8ZNct/Qfl69a2Lf6vc9rF7BELT0e5Y
R7CKx7fc5xRaeQdyGj/dJevm9BF/mSdnclS5vas=
-----END CERTIFICATE-----
```

证书规则为：

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

（2）中级机构颁发的证书链：

——–BEGIN CERTIFICATE——–

——–END CERTIFICATE——–

——–BEGIN CERTIFICATE——–

——–END CERTIFICATE——–

——–BEGIN CERTIFICATE——–

——–END CERTIFICATE——–

证书链规则：

- 证书之间不能有空行；

- 每一份证书遵守第一点关于证书的格式说明；

RSA私钥格式要求

最近更新时间: 2023-03-17 10:10:32

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。

如果用户不是按照上述方案生成私钥，得到[——–BEGIN PRIVATE KEY——–, ——–END PRIVATE KEY——–] 这种样式的私钥，用户可以按照如下方式转换：

•[](javascript: void 0;)

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

证书转换为PEM格式说明

最近更新时间: 2023-03-17 10:18:31

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。

版权所有：建行云

DER格式证书转换为PEM格式

最近更新时间: 2023-03-17 10:18:31

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

版权所有：建行云

P7B格式证书转换为PEM格式

最近更新时间: 2023-03-17 10:18:31

P7B格式一般出现在windows server和tomcat中。

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

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

私钥转换：私钥一般在IIS服务器里可导出

版权所有：建行云

PFX格式证书转换为PEM格式

最近更新时间: 2023-03-17 10:18:31

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

版权所有：建行云

CER/CRT格式证书转换为PEM格式

最近更新时间: 2023-03-17 10:18:31

对于 CER/CRT 格式的证书，用户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: 2023-03-17 09:59:56

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。

1.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。

2.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：

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：

o 检查证书是否过期。

o 检查证书是否已经被吊销。

o 检查证书是否可信。

o 检查收到的证书中的域名与请求的域名是否一致。

4. 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）。

6. 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。

3.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：

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：

o 检查证书是否过期。
o 检查证书是否已经被吊销。
o 检查证书是否可信。
o 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。
8. 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。
9. 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）。之后的会话中，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。

版权所有：建行云

监控告警

获取监控数据

最近更新时间: 2023-03-17 09:50:29

建行云云监控为负载均衡和后端实例提供数据收集和数据展示功能。使用建行云云监控，用户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。

建行云默认为所有用户提供云监控功能，用户无需手动开通，只要用户使用了负载均衡，云监控即可帮助用户收集相关监控数据。用户可以通过以下几种方式查看负载均衡的监控数据：

方式一：负载均衡控制台

1. 登录建行云租户控制台，点击负载均衡模块，单击负载均衡实例 ID 旁的监控图标，即可通过监控浮窗，快速浏览各个实例的性能数据。 2. 单击负载均衡实例 ID，进入负载均衡详情页，单击【监控】，即可查看当前负载均衡实例的监控数据。

方式二：云监控控制台

登录建行云租户控制台，选择“云产品监控”模块下的负载均衡，单击负载均衡实例 ID 进入监控详情页，即可查看该负载均衡实例的监控数据，展开实例即可查看监听器、后端服务器等监控信息。

版权所有：建行云

监控指标说明

最近更新时间: 2023-03-17 09:50:29

监控从运行状态下的负载均衡实例中收集原始数据，并将数据展示为易读的图标形式。统计数据默认保存一个月，用户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。
建议用户通过 云监控控制台 查看负载均衡的监控，选择云产品监控 > 负载均衡，单击负载均衡实例 ID，进入监控详情页，查看该负载均衡实例的监控数据，展开实例即可查看监听器、后端服务器等的监控信息。

版权所有：建行云

配置告警策略

应用场景

最近更新时间: 2023-03-17 09:59:56

用户可以针对云监控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用户采取措施。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。用户可以根据以下指引进行告警策略的创建。

版权所有：建行云

基本概念

最近更新时间: 2023-03-17 09:59:56

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、告警对象和告警渠道组成
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：当用户选择云服务器策略，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、应用性能观测、前端性能监控和云拨测

版权所有：建行云

操作步骤

最近更新时间: 2023-03-17 09:59:56

1. 登录云监控控制台。

2. 单击告警配置 > 告警策略，进入告警策略配置页面。

3. 单击新建，配置告警策略，配置说明如下：

4. 配置完以上信息后单击保存，即成功创建告警策略。

告警指标说明

最近更新时间: 2023-03-17 09:50:29

用户可以为用户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。这样能确保用户及时发现异常状况从而采取相应措施，保持系统的稳定性和可靠性。更多内容请参考告警概述。

负载均衡的告警策略包括如下类型：

- 外网监听器
- 内网监听器

外网监听器/内网监听器

最近更新时间: 2023-03-17 09:50:29

目前公网负载均衡和内网负载均衡均支持监听器维度的告警，具体指标如下：

最佳实践

最佳实践

最近更新时间: 2023-03-15 15:08:16

HTTP/HTTPS等七层负载均衡当前不支持租户自行定义个性化参数配置；租户使用 HTTPS 双向认证时，负载均衡不会向后端云服务器发送证书内容信息。公网负载均衡实例须配置HTTP/HTTPS监听器，且监听域名须配置WAF防护。

1.负载均衡实例须至少绑定两个后端节点。

2.出于高可用考虑，不应将裸金属作为负载均衡后端服务进行绑定。

3.对于单地域多可用区或多地域多可用区部署的应用，如果需要使用负载均衡，应在每个可用区内申请一个负载均衡实例，负载均衡前由DNS或应用路由等实现交易接入、分发及故障剔除等。

4.用户可以通过选择运营商标签决定将负载均衡实例建在武汉可用名解析到两个可用区的不同负载均衡实例，提高应用可用性。

5.外网和内网负载均衡单可用区实例创建后不可更换可用区；不支持跨 可用区故障迁移。建议租户申请使用多可用区实例。

6.同一个负载均衡实例中，HTTP/HTTPS 监听器和 TCP/UDP 监听器的监听端口不能重复。

7.四层负载均衡的以下组合必须唯一：实例 IP+监听协议+后服务器 IP+ 后端服务端口。

8.同一个负载均衡实例中，多域名如需复用端口，目前支持 http业务；对于https业务，若多域名绑定同一张泛域名证书，则可支持多域名复用端口；若多域名绑定单域名证书，则不支持多域名复用端口。

9.负载均衡提供后端实例的故障探测及剔除机制，即健康检查，健康检查功能必须开启，应用可根据具体业务须求配置健康检查时间。

10.创建HTTP/HTTPS监听器时应保持默认域名开关不开启。

11.配置HTTPS转发协议需要证书，用户在使用过程中应关注证书有效期，在证书到期前及时完成证书更新。

12.可按需配置会话保持功能。

13.可按需选择负载均衡算法，应使用“最小连接数”或“轮询”。

14.根据安全管理相关要求，外网负载均衡应使用HTTP/HTTPS监听器，禁止配置TCP/UDP监听器；

15.应对带宽等关键指标按需配置相应的监控告警策略。

版权所有：建行云

常见问题

负载均衡有几种类型

最近更新时间: 2023-03-15 15:08:16

负载均衡分为四层负载均衡和七层负载均衡两种。四层负载均衡支持TCP和UDP两种协议，基于ip+port进行转发；七层负载均衡支持HTTP和HTTPS两种协议，基于域名+URL进行转发。

版权所有：建行云

什么是健康检查

最近更新时间: 2023-03-15 15:08:16

负载均衡对后端RS服务端口存活状态进行探测，及时剔除异常服务端口，实现业务高可用。

版权所有：建行云

负载均衡是否可以直接获取客户端IP

最近更新时间: 2023-03-16 14:50:54

四层负载均衡（TCP协议）服务可以直接在后端CVM上获取来访者真实IP地址，无需进行额外配置。
七层负载均衡提供X-Forwarded-For的方式获取访问者真实IP，负载均衡侧默认开启，需要后端做响应配置来获取客户端IP。

负载均衡的VIP是否支持ping

最近更新时间: 2023-03-16 14:51:03

Ping负载均衡的vip：由负载均衡集群响应，不会转发到后端的服务器。

公网负载均衡的VIP支持ping。

内网负载均衡否VIP不支持ping。

公网IP和EIP的区别是什么?

最近更新时间: 2023-03-16 14:51:03

公网IP地址为用户申请CVM实例时选择创建的互联网IP地址，该IP地址与申请的CVM实例绑定，绑定后仅能用于该CVM实例的互联网入访与出访服务。不建议租户使用该方式实现互联网的互访。
EIP地址为租户单独申请的互联网IP地址，该EIP地址功能上可以与CVM实例绑定使用，可以与NAT实例绑定使用。公网IP地址可以转换成EIP地址，转换后该公网IP地址即为EIP地址，可以实现与CVM实例解绑、与其他实例绑定等重复使用。EIP地址无法转换成公网IP地址。

版权所有：建行云

健康检查提示 CVM 实例异常该如何处理?

最近更新时间: 2023-03-16 14:51:03

请按如下步骤进行排查:

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

版权所有：建行云

权重置为0与解绑 RS 有什么区别?

最近更新时间: 2023-03-16 14:51:03

- 权重置为0：TCP 监听器存量连接继续转发，UDP 监听器相同五元组的继续转发，HTTP/HTTPS 监听器存量连接继续转发。
- 解绑 RS：TCP/UDP 监听器存量连接停止转发，HTTP/HTTPS 监听器存量连接继续转发。

版权所有：建行云

为什么健康检查探测频率过高?

最近更新时间: 2023-03-16 14:51:03

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

当前，健康检查频率过高的问题，主要跟负载均衡后端健康探测实现机制有关。假设100万的 client 端请求，会分散在4台 CLB 后端物理机上，再转给云服务器。 健康检查探测是在 CLB 的后端物理机上各自探测的。因此，CLB 实例设置5秒1次的探测请求，实际上 CLB 后端的每台物理机都会每5s发送一次探测。因此在后端云服务器上，会收到多次探测请求。假设 CLB 实例所在集群有8台物理机，那么每台机器5s发送一次请求，后端主机可能会在5s中收到8次探测。

该实现方案的优势是：效率高，探测精准，避免误剔除。例如，CLB 实例集群的8台物理机中，其中1台判断失败，仅那1台机器不再转发流量，另外7台的流量是正常的。

版权所有：建行云

关于 Telnet 负载均衡监听端口的说明

最近更新时间: 2023-03-16 14:50:54

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

版权所有：建行云

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

最近更新时间: 2023-03-16 14:51:03

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

版权所有：建行云

关于内网回环问题的说明

最近更新时间: 2023-03-16 14:50:54

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

HTTPS 支持的加密套件有哪些?

最近更新时间: 2023-03-16 14:50:54

可支持的加密套件包括:
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。

版权所有：建行云

证书过期后如何处理?

最近更新时间: 2023-03-16 14:50:54

当前证书过期后，需要用户手动更新证书。证书到期后，相关服务无法正常使用，为避免对业务产生影响，用户须在证书到期前及时更新证书。

版权所有：建行云

一个监听器可以绑定多少个 HTTPS 证书?

最近更新时间: 2023-03-16 14:50:54

当前一个监听只能绑定一个服务器证书；若存在多个域名使用同一个监听器的情况，建议申请多域名证书或者泛域名证书。

版权所有：建行云

CLB 目前支持哪些类型的证书?

最近更新时间: 2023-03-16 14:50:54

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

版权所有：建行云

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

最近更新时间: 2023-03-16 14:50:54

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

HTTPS 监听使用什么端口?

最近更新时间: 2023-03-16 14:50:54

不强制，建议使用443端口。

HTTPS 支持哪些版本的SSL/TLS安全协议?

最近更新时间: 2023-03-16 14:50:54

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

版权所有：建行云