

CECSTACK 5.3.0

服务器负载均衡 SLB 用户指南

文档密级：公开

文档版本：01

发布日期：2025-01-23

【版权声明】

版权所有 © 中电云计算技术有限公司 2025。 保留一切权利。

本文档的版权归中电云计算技术有限公司所有。非经中电云计算技术有限公司书面许可，任何人不得以包括通过程序或设备监视、复制、传播、展示、镜像、上载、下载、摘编等方式或以其他方式擅自使用本文档的任何内容。

【商标声明】

 中国电子云 和本文档所示其他中电云计算技术有限公司及/或其他关联公司的商标均为中电云计算技术有限公司及/或其关联公司所有。未经中电云计算技术有限公司及/或其关联公司书面许可，任何人不得以任何形式使用，也不得向他人表明您有权展示、使用或做其他处理。如您有宣传、展示等任何使用需要，您必须取得中电云计算技术有限公司及/或其关联公司事先书面授权。

本文档中出现的其他公司的商标或注册商标，由各自的所有人拥有。

【注意】

您购买的产品、服务或特性等应以中电云计算技术有限公司商业合同中的约定为准，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，中电云计算技术有限公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容可能会不定期进行更新。本文档仅作为使用指导，其中的陈述、信息或建议等均不构成任何明示或暗示的担保。

前言

概述

本文档主要介绍服务器负载均衡 SLB 的产品介绍和操作指南等信息，以便读者全方位的了解服务器负载均衡 SLB。

读者对象

本文档适用于以下读者：

- 维护工程师
- 技术支持工程师
- 系统管理员

本书约定

符号标志约定

本书采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。 “注意”不涉及人身伤害。
 说明	对正文的重点信息进行必要的补充说明。 “说明”不是安全警示信息，不涉及人身、设备及环境伤害信息。
 提示	配置、操作、或使用产品的技巧、窍门。

修订记录

文档版本	发布时间	修订说明
01	2025-01-23	第一次正式发布。

目 录

1 产品介绍	1
1.1 产品简介	1
1.2 基本概念	2
1.3 产品优势	3
1.4 实例规格	3
1.5 实现原理	4
1.6 关键指标	5
1.7 关联服务	5
1.8 应用场景	5
1.9 使用限制	6
1.10 访问方式	6
2 快速入门	7
2.1 进入 SLB 实例页面	7
2.2 通过 SLB 实现业务流量的负载分担	7
2.2.1 背景介绍	7
2.2.2 配置流程	8
3 操作指南	18
3.1 SLB 实例	18
3.1.1 SLB 概述	18
3.1.2 新建 SLB 实例	18
3.1.3 查看 SLB 实例信息	20
3.1.4 修改 SLB 实例规格限速信息	22
3.1.5 IP 地址管理	23
3.1.6 变配 SLB 实例	26
3.1.7 启动/停止 SLB 实例	27
3.1.8 续费 SLB 实例（包年包月计费模式）	27
3.1.9 退订/删除 SLB 实例	27
3.2 监听器	28
3.2.1 监听器概述	28
3.2.2 创建监听器	29
3.2.3 编辑限速信息	36
3.2.4 转发规则	37

3.2.5 启用/停止监听器	42
3.2.6 日志设置	42
3.2.7 删除监听器	46
3.3 服务器组	46
3.3.1 服务器组概述	46
3.3.2 创建服务器组	47
3.3.3 查看服务器组详情	49
3.3.4 后端服务器	49
3.3.5 健康检查	53
3.3.6 删除服务器组	57
3.4 证书管理	57
3.4.1 证书概述	57
3.4.2 创建证书	58
3.4.3 删除证书	59
3.5 访问控制	59
3.5.1 访问控制概述	59
3.5.2 创建访问控制组	60
3.5.3 删除访问控制组	60
3.6 安全策略	61
3.6.1 安全策略概述	61
3.6.2 创建自定义策略	61
3.6.3 删除自定义策略	61
3.7 监控信息	62
3.7.1 监控概述	62
3.7.2 监控项说明	62
4 常见问题	65

1 产品介绍

1.1 产品简介

什么是服务器负载均衡 SLB

服务器负载均衡（Server Load Balancer，简称 SLB），是将业务访问流量根据分发策略分发到后端服务器组的网络服务。支持多种负载均衡分发策略，通过流量分发，可快速提高应用系统对外的服务能力。

为什么选择服务器负载均衡 SLB

服务器负载均衡 SLB 能够为您的业务提供高弹性、高可用性、成本优势等特点。

主要功能

- 提供基于域名和 URL 路径的转发
SLB 对外提供虚拟地址 VIP，将相同或不同 VPC 下的后端实例（云服务器）或 IP 服务虚拟为一个服务资源池，将来自前端的访问流量按照域名和 URL 路径分别分发给不同的后端服务进行处理，提升整体对外服务的能力。
- 多种协议侦听
SLB 支持 TCP/UDP/HTTP/HTTPS 等多种协议的不同端口侦听服务，以支持多样的客户端服务接入和流量分发。
- 健康检查
SLB 会检查后端服务资源池中实例的健康状态，自动隔离、挂载后端提供服务的实例，消除设备单点故障，保障业务的正常运行。
- 自动扩缩容后端实例数
SLB 后端可以绑定指定的高可用组，通过设置弹性伸缩策略，自动调整后端服务实例的数量，合理配置资源，满足业务弹性访问的要求。
- 会话保持
SLB 支持基于 HTTP/HTTPS 协议类型的会话保持功能。
- 空闲连接超时
SLB 支持基于 TCP/HTTP/HTTPS 协议的空闲连接超时。
- 源 IP 透传
TCP 支持基于 ProxyProtocol 携带源 IP，HTTP/HTTPS 支持通过 X-Forwarded-For 的 header 携带源 IP。
- 支持 HTTP/2
SLB 支持处理 HTTP 2.0 请求，提升服务的整体访问性能。

三种类型负载均衡对比

	基础负载均衡 BLB	网络负载均衡 NLB	服务器负载均衡 SLB
用途	主要面向网络层，提供基于IP的转发能力，满足海量数据包的转发需求	主要面向传输层，提供TCP/UDP协议支持，满足大流量的转发需求	主要面向传输层、应用层交付，提供TCP/UDP/HTTP/HTTPS等协议支持，提供高级路由功能
性能	支持弹性扩容，性能无上限	最大支持1000万并发连接、12万新建连接	高阶型最大支持20万并发连接、2万新建连接、2万QPS
典型应用场景	作为四、七层负载均衡的流量入口，对接数据库、容器化等应用类型	四层大流量转发场景，物联网、音视频等业务入口	Web网站、电商平台、管理系统等

1.2 基本概念

概念	说明
SLB实例	<p>服务器负载均衡实例是一个运行的负载均衡服务，用来接收流量并将其分配给后端的实例。</p> <p>根据网络类型不同，SLB实例分为如下类型：</p> <ul style="list-style-type: none"> 私网 IPv4 SLB 实例：提供专有网络子网内的负载均衡服务。 公网 IPv4 SLB 实例：可以提供公网负载均衡服务，IPv4 负载均衡需要绑定弹性公网 IP 使用。 私网 IPv6 SLB 实例：提供专有网络子网内的 IPv6 流量的负载均衡服务。 公网 IPv6 SLB 实例：可以提供公网 IPv6 负载均衡服务，私网 IPv6 SLB 实例需要购买带宽后才可以对外提供服务。
监听器	监听器负责监听SLB实例上的请求，监听器关联服务器组后，根据用户配置的流量分发策略，将流量分发到后端服务器。
域名/URL转发策略	对于HTTP/HTTPS的监听器，支持基于域名/URL的转发策略，可将不同域名或者不同URL的请求转发到不同的后端服务器组进行处理。若可以匹配到监听器的转发策略，则按该转发策略进行转发，否则将请求转发到监听器绑定的后端服务器组。
服务器组	<p>服务器组是多个后端服务器的集合，支持云服务器、IP服务器。服务器组定义了流量分配策略（加权轮询算法、加权最少连接数算法、源IP算法、随机算法和源IP端口算法）及健康检查等配置，监听器需要关联一个服务器组进行使用。</p> <p>用户可以自主管理服务器组，可根据业务系统的规模，按需增加或删除组内的后端服务器实例。</p>
健康检查	SLB实例会定期请求后端服务器的服务运行状态，通过服务的运行状态来判断后端服务器是否可用。若SLB实例发现后端服务器的服务运行状态异常，则不会再将流量分发给该后端服务器。
会话保持	<p>后端服务器组提供会话保持功能，在会话的生命周期内，可将来自相同客户端的访问请求转发到同一台后端服务器上进行处理。</p> <p>按照所使用的协议不同，分为四层会话保持和七层会话保持。四层会话保持基于源IP，七层会话保持类型支持负载均衡器Cookie和应用程序Cookie。</p>
证书管理	对于TCPSSL和HTTPS协议，监听器支持证书管理功能，在配置HTTPS/TCPSSL监听器时，需要为监听器绑定服务器证书。在使用HTTPS/TCPSSL协议时，服务器证书用于SSL握手协商，需提供证书内容和私钥。

概念	说明
	支持双向认证。
访问控制	监听器支持设置黑白名单，对请求来源实现过滤和访问控制。

1.3 产品优势

简单易用

快速部署，实时生效，支持 4 层协议（TCP、UDP、TCPSSL）和 7 层协议（HTTP、HTTPS），支持多种调度算法，可以高效地管理和调整分发策略。

安全合规

基于国产化体系构建，架构更加安全，部署结构符合政企安全规范。支持公网和私网类型负载均衡实例，可隐藏内部网络结构，提升系统的安全性和可用性。

灵活扩展

根据业务负载情况，可自主添加或删除后端服务器数量，实现业务动态调整。或者绑定弹性伸缩，实现业务的无缝扩缩容。

节约成本

无需购买大型硬件设备，无需人力和运维支出，为您节约大量成本。

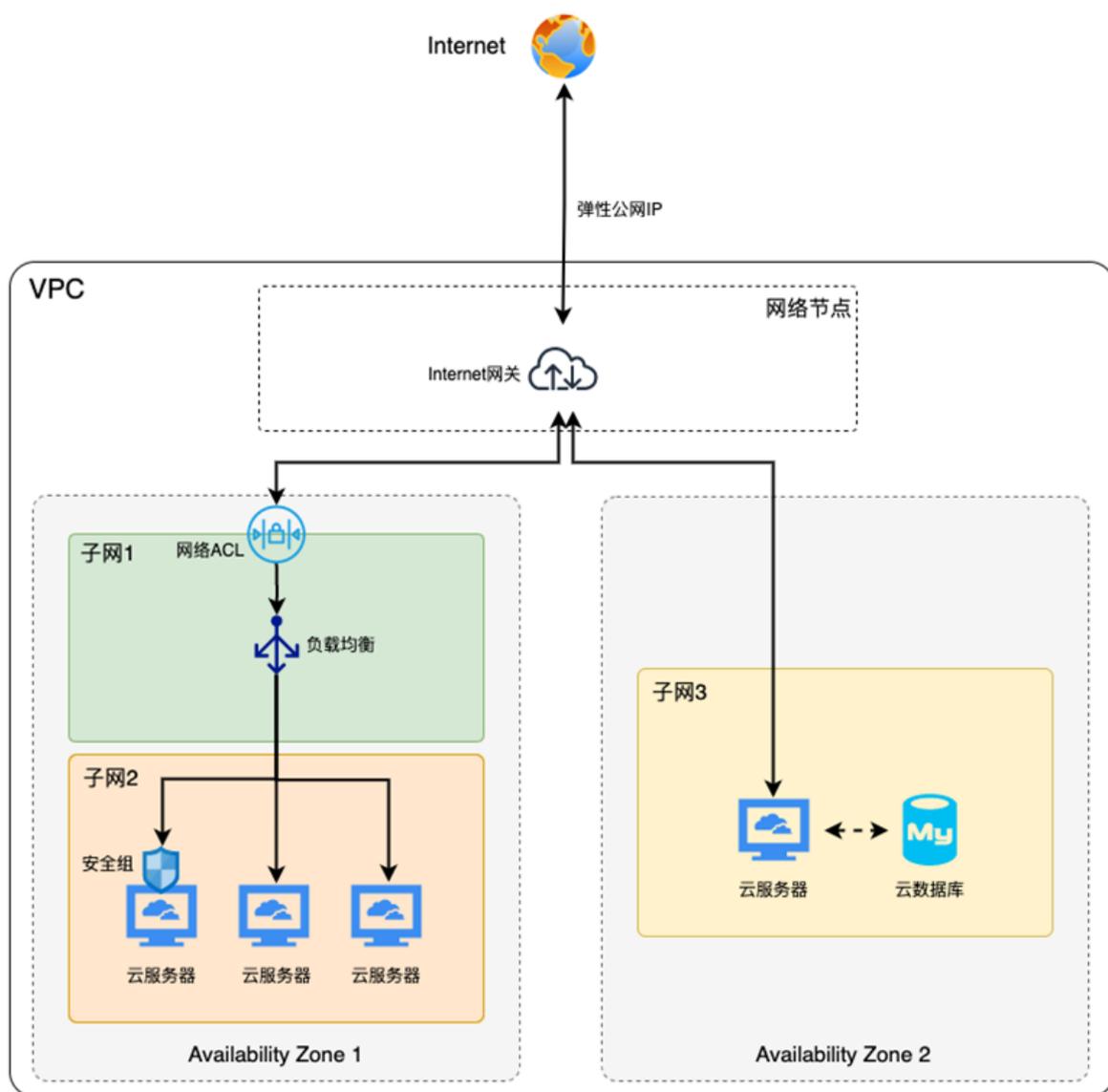
1.4 实例规格

服务器负载均衡 SLB 提供了多种规格套餐，用户可根据实际的业务需要选择使用：

- 基础型：提供最大 5000 并发连接数，最大 3000 每秒新建连接数 CPS，最大 1000 每秒请求数 QPS。
- 标准型：提供最大 50000 并发连接数，最大 5000 每秒新建连接数 CPS，最大 5000 每秒请求数 QPS。
- 高阶型：提供最大 200000 并发连接数，最大 20000 每秒新建连接数 CPS，最大 20000 每秒请求数 QPS。

1.5 实现原理

产品架构



组件	功能描述
SLB实例	为部署在后端的多个云资源提供公网、私网入向访问的能力，实现共享带宽、均衡流量，极大地节省了公网带宽成本。同时隐藏云服务器的真实地址，提升安全性。
弹性公网IP	公网地址，可以绑定至云服务器、NAT网关、负载均衡等云资源上，为以上云资源提供公网访问的能力。

业务流

云服务器通过服务器负载均衡 SLB 对外提供 Internet 访问的业务流如下：

- (1) 用户在控制台创建 VPC、子网、路由表、云服务器、服务器负载均衡 SLB 等资源。
- (2) SLB 实例所在子网的路由表中配置去往 Internet 网关的路由（如目的地址是 0.0.0.0/0，下一跳是 Internet 网关）。
- (3) SLB 实例配置监听器端口（如 HTTP 80）、均衡算法、配置后端服务器组，后端服务器组添加云服务器。
- (4) 确保后端服务器组中云服务器的健康检查状态为“正常”。
- (5) 在 Internet 访问 SLB 实例的弹性公网 IP 地址和 80 端口，实现 Internet 访问。

1.6 关键指标

为没有绑定弹性公网 IP 的云资源提供对外的公网访问能力，默认可申请的带宽上限为 500 Mbps，可以通过配额进行提升。

1.7 关联服务

服务器负载均衡 SLB 支持绑定弹性公网 IP。

服务器负载均衡 SLB 可以为没有绑定弹性公网 IP 的云资源提供对外的公网访问能力，均衡流量，实现业务的高可用性和扩展性。

1.8 应用场景

业务弹性扩容

服务器负载均衡 SLB 绑定后端服务器组时，可以将访问流量均匀地分配到多台后端服务器上，绑定弹性伸缩组后可根据业务的负载情况自动增加或减少后端服务器的数量，以应对大流量、突发流量对系统造成的冲击。

例如大型业务网站促销、秒杀、抢购或其他可能导致存在突发流量的业务系统。

通过 SLB 消除业务的单点故障风险

对可靠性和连续性有较高要求的业务，可以使用负载均衡的架构进行部署，在负载均衡器上添加多个后端云服务器或 IP 服务器。负载均衡器会通过健康检查的状态及时发现并移除有故障的后端服务器，并将流量转发到其他正常运行的后端云服务器，确保业务不中断，保证应用系统正常提供服务。

例如计费业务、官方网站等。

业务跨可用区容灾

服务器负载均衡 SLB 单实例采用集群多活部署，对后端的真实服务器自动执行健康检查，发现服务器异常时会自动地将该服务器从负载均衡后端移除，不会再将流量转发至该服务器，直至该服务器的健康检查状态恢复正常后再继续转发流量至该服务器。

服务器负载均衡 SLB 采用多可用区部署，对外屏蔽可用区级故障，有效保障了业务的连续性。

例如游戏业务、电商网站等。

业务跨区域容灾

可以在不同区域下部署 SLB 实例，同时后端分别挂载与 SLB 实例同区域的后端服务器。解析层使用 DNS 做智能解析，将域名解析到不同区域的 SLB 实例的服务地址上，可实现全局负载均衡。当某个区域出现故障导致该区域的服务不可用时，DNS 系统中自动移除对应区域 SLB 的解析记录，即可实现该区域中的用户访问不受影响，有效地保障了业务的连续性。

例如金融业务、大型电商网站等。

1.9 使用限制

服务器负载均衡 SLB 在使用过程中需要遵循如下限制：

- 使能 SLB 实例的跨 VPC 访问功能后，SLB 实例需要占用子网内的 IP 地址。
- SLB 实例一旦创建，无法修改跨 VPC 访问功能。
- 后端协议为 TCP/UDP 时，不支持配置会话保持功能。
- 后端协议为 HTTP，且后端转发策略为加权轮询算法时，支持配置会话保持。后端转发策略为加权最小连接算法、源 IP 算法或随机算法时，不支持配置会话保持功能。

1.10 访问方式

您可以通过以下方式管理服务器负载均衡 SLB 和相关资源：

- 网络控制台：通过网络控制台可以可视化地管理各种云资源，如 SLB 实例、监听器、服务器组等。
- OpenAPI：通过调用 API 接口来管理相应的云资源，方便以编程的方式使用。

2 快速入门

2.1 进入SLB实例页面

前提条件

已获取系统的 URL 登录地址，以及对应的用户名和密码。

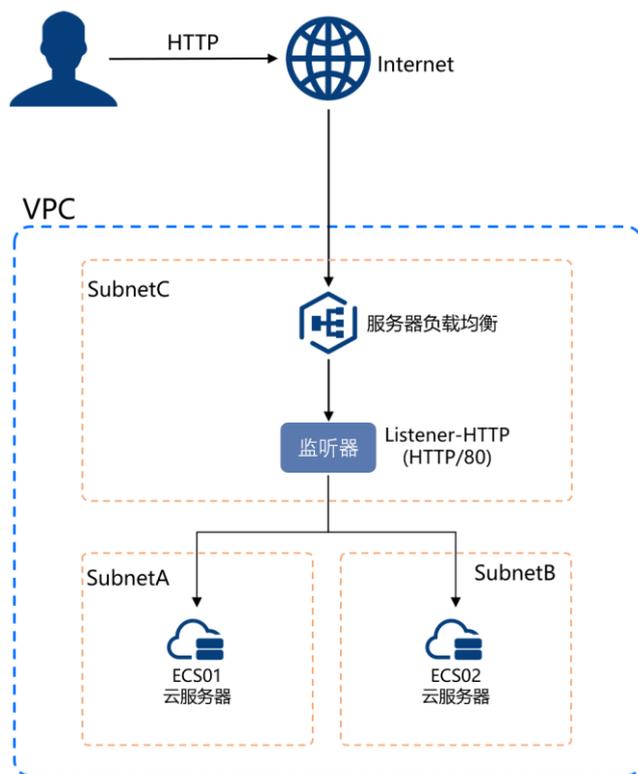
操作步骤

- (1) 登录系统。
- (2) 单击“云服务”页签，在“网络”分类下选择“服务器负载均衡 SLB”，进入 SLB 实例页面。

2.2 通过SLB实现业务流量的负载分担

2.2.1 背景介绍

某个公司的业务有大量访问请求，此时需要通过 SLB 实例将访问流量分发到两台云服务器上进行处理，实现业务流量的负载分担。



系统中已做如下配置：

- 已创建专有网络 VPC “192.168.0.0/16” 及其子网 SubnetA “192.168.1.0/24”、子网 SubnetB “192.168.2.0/24” 和子网 SubnetC “192.168.3.0/24”。
- 已在子网 SubnetA 下创建云服务器 ECS01 “192.168.1.2”，且 ECS01 上已安装 nginx 服务。
- 已在子网 SubnetB 下创建云服务器 ECS02 “192.168.2.2”，且 ECS02 上已安装 nginx 服务。
- 已创建弹性公网 IP 实例 EIP01 “10.252.245.26”，且与云服务器 ECS01 绑定。
- 已创建弹性公网 IP 实例 EIP02 “10.252.226.248”，且与云服务器 ECS02 绑定。

2.2.2 配置流程

2.2.2.1 配置步骤

配置步骤如下：

- (1) [搭建后端服务](#)
- (2) [新建 SLB 实例](#)
- (3) [配置 SLB 服务器组](#)
- (4) [配置 SLB 实例监听器](#)
- (5) [验证负载均衡服务](#)

2.2.2.2 搭建后端服务

1. 配置云服务器 ECS01 的 Nginx 服务

简介

在 ECS01 和 ECS02 上启用 Nginx 服务，并编辑 index.html 页面，使访问 ECS01 时返回一个标题为 “Welcome to ECS01 test page” 的页面，访问 ECS02 时返回一个标题为 “Welcome to ECS02 test page” 的页面。

前提条件

ECS01 和 ECS02 上已安装 Nginx 服务。

操作步骤

- (1) 远程登录云服务器 ECS01 实例。
- (2) 执行以下命令，启用 Nginx 服务并查看服务状态。

```
#启用 Nginx 服务
systemctl start nginx
#查看 Nginx 服务的状态
systemctl status nginx
```

```
[root@ecs-wintclu9prjvma ~]#
[root@ecs-wintclu9prjvma ~]# systemctl start nginx
[root@ecs-wintclu9prjvma ~]# systemctl status nginx
● nginx.service - The nginx HTTP and reverse proxy server
   Loaded: loaded (/usr/lib/systemd/system/nginx.service; disabled; vendor preset: disabled)
   Active: active (running) since Fri 2024-03-29 01:59:22 UTC; 6h ago
     Process: 2024 ExecStart=/usr/sbin/nginx (code=exited, status=0/SUCCESS)
    Process: 2023 ExecStartPre=/usr/sbin/nginx -t (code=exited, status=0/SUCCESS)
    Process: 2021 ExecStartPre=/usr/bin/rm -f /run/nginx.pid (code=exited, status=0/SUCCESS)
   Main PID: 2026 (nginx)
     Tasks: 3 (limit: 22757)
    Memory: 14.0M
   CGroup: /system.slice/nginx.service
           └─2026 nginx: master process /usr/sbin/nginx
             └─2027 nginx: worker process
               └─2028 nginx: worker process

Mar 29 01:59:21 ecs-wintclu9prjvma systemd[1]: Starting The nginx HTTP and reverse proxy server...
Mar 29 01:59:22 ecs-wintclu9prjvma nginx[2023]: nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
Mar 29 01:59:22 ecs-wintclu9prjvma nginx[2023]: nginx: configuration file /etc/nginx/nginx.conf test is successful
Mar 29 01:59:22 ecs-wintclu9prjvma systemd[1]: Started The nginx HTTP and reverse proxy server.
[root@ecs-wintclu9prjvma ~]#
```

- (3) 在任意终端使用浏览器访问“http://ECS01 的公网 IP 地址”，显示如下页面，说明 Nginx 服务启用成功。



- (4) 修改 ECS 实例 ECS01 的 `index.html` 页面。
Nginx 的默认根目录 `root` 是 `/usr/share/nginx/html`，直接修改 `html` 下的 `index.html` 静态页面，用来标识到 ECS01 的访问。

- a. 执行如下命令打开文件“`index.html`”：

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

- b. 按 `i` 键进入编辑模式。

- c. 请在 `<body></body>` 标签内输入如下信息：

```
<h1>Welcome to <strong>ECS01</strong> test page</h1>
  <div class="content">
    <p>Hello nginx , This is ECS01 </p>
  </div>
```

```
<body>
  <h1>Welcome to <strong>ECS01</strong> test page </h1>

  <div class="content">

    <p>Hello nginx , This is ECS01</p>

  </div>
</body>
```

d. 按“Esc”，输入:wq保存编辑并退出。

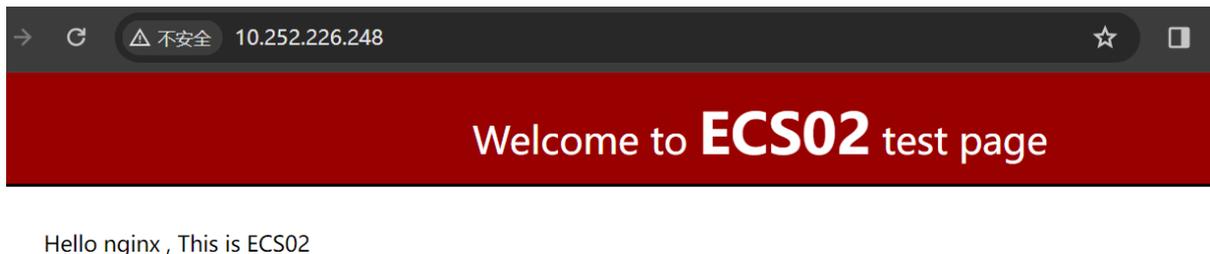
- (5) 在任意终端使用浏览器访问“http://ECS01的公网IP地址”，显示如下页面，说明index.html文件修改成功。



至此，云服务器 ECS01 上的配置完成。

2. 配置云服务器 ECS02 的 Nginx 服务

请参照[配置云服务器 ECS01 的 Nginx 服务](#)章节的操作步骤，配置云服务器 ECS02 的 Nginx 服务。配置完成后，在任意终端使用浏览器访问“http://ECS02 的公网 IP 地址”，显示如下页面，说明 index.html 文件修改成功。



2.2.2.3 新建 SLB 实例

- (1) 在 SLB 实例页面，单击页面右上角的“新建负载均衡”，进入新建负载均衡页面。
- (2) 根据下表中的参数说明进行配置，未列出的参数保持默认配置即可。

参数	配置说明	参数取值
区域	选择SLB实例所属的区域。	和云服务器ECS01和ECS02的区域保持一致

参数	配置说明	参数取值
	请确保SLB实例的区域和服务器组中添加的服务器区域相同。	
可用区	选择SLB实例所属的可用区。	默认配置
规格	<p>根据需要选择实例规格：</p> <ul style="list-style-type: none"> 基础型：最大可以支持连接数 5000，新建连接数（CPS）：3000，每秒查询数（QPS）：1000。 标准型：最大可以支持连接数 50000，新建连接数（CPS）：5000，每秒查询数（QPS）：5000。 高阶型：最大可以支持连接数 200000，新建连接数（CPS）：20000，每秒查询数（QPS）：20000。 <p>默认支持以上规格，系统具体支持的实例规格信息，请以界面上显示的为准。</p>	基础型
计费模式	<p>选择SLB实例的计费模式。</p> <ul style="list-style-type: none"> 按需计费：是一种先使用后付费的计费模式。 包年包月：是一种需要先付费才能使用资源的计费模式，适用于流量峰值比较稳定且需要长期使用的业务场景。 	按需计费
专有网络	<p>选择SLB实例所属的专有网络。</p> <p>您可以选择使用已有的专有网络，或者单击“新建VPC”创建新的专有网络。</p>	VPC
子网类型	<p>选择SLB实例所属子网的类型。</p> <ul style="list-style-type: none"> 标准型：默认仅能与VPC内的其它子网进行通信，或者通过Internet网关、NAT网关、VPC对等连接等网关组件与VPC外的网络进行通信。 直通型：默认可以和云下物理环境中的网段进行三层互通。 	标准型
子网	<p>选择SLB实例所属的子网。</p> <p>您可以选择使用已有的子网网段，或者单击“新建子网”创建新的子网网段。</p>	subnet03
实例IP地址	<p>配置SLB实例的私有IP地址。</p> <ul style="list-style-type: none"> 自动分配：由系统自动分配SLB实例的私有IP地址。 手动分配：需要您手动指定SLB实例的私有IP地址。 	自动分配
公网IPv4	选择SLB实例是否支持分发来自公网的请求。	开启
弹性公网IP	<p>启用“公网IPv4”时需配置该项。绑定弹性公网IP的SLB实例可以接收来自公网的访问请求并将请求分发到服务器组内的后端服务器。</p> <p>您可以选择已有或新购弹性公网IP与SLB实例进行绑定。</p> <ul style="list-style-type: none"> 选择已有：在弹性公网IP实例下拉框中选择系统中已创建的EIP实例。 新购弹性公网IP： <ul style="list-style-type: none"> 线路：选择弹性公网IP的线路，目前仅支持“单线”，即通过单个网络运营商访问公网，成本低且便于自主调度。当进行跨运营商访问时，单线公网IP 	<p>新购弹性公网IP</p> <ul style="list-style-type: none"> 线路：单线 带宽：10 Mbps 弹性公网名称：EIP03

参数	配置说明	参数取值
	<p>地址会存在延迟过长、丢包增加、抖动增大等问题。</p> <ul style="list-style-type: none"> 带宽：弹性公网 IP 的带宽大小，默认为 10 Mbps，带宽范围为 1-500 Mbps。 弹性公网名称：弹性公网 IP 的名称，可根据需要自定义名称或使用系统缺省名称。 	
名称	SLB实例的名称，自定义名称或使用系统缺省名称。	SLB01

新建负载均衡

* 部门:

资源集:

* 区域:

* 可用区: 华东1-杭州可用区1-zone 华东1-杭州可用区2-zone

* 规格:
最大可以支持连接数6000, 新建连接数 (CPS): 3000, 每秒查询数 (QPS): 1000

* 计费模式:

* 专有网络:

外网出口: Internet

子网类型:

* 子网:
可用私网IP数量253个

国密: 开启

跨VPC访问: 开启

* 资源子网: 需要占用2个IP; 当前可用IP数253个

* 实例IP地址:

公网IPv4: 开启

* 弹性公网IP:

* 线路:

* 带宽:

* 弹性公网名称:

启用IPv6: 开启

* 名称:

描述:

0/255

新建实例数量: 个 费用配置: 基础型负载均衡SLB按需计费 ¥0.18/小时 + 弹性公网带宽 ¥1/小时 + 弹性公网IP ¥0.2/小时

- (3) 单击“下一步”，进入确认配置页面。
- (4) 确认要创建的 SLB 实例信息无误后，单击“确定新建”，完成创建 SLB 实例操作。

2.2.2.4 配置 SLB 服务器组

1. 新建 SLB 服务器组

- (1) 在 SLB 实例页面，单击左侧导航栏的“SLB 服务器组”，进入 SLB 服务器组页面。
- (2) 单击“新建服务器组”，进入新建服务器组页面。
- (3) 根据下表中的参数说明进行配置，未列出的参数保持默认配置即可。

参数	配置说明	参数取值
名称	服务器组的名称，可根据需要自定义名称或使用系统缺省名称。	ServerGroup1
专有网络	选择服务器组所属的专有网络。 您可以选择使用已有的专有网络，或者单击“新建VPC”创建新的专有网络。	VPC
后端协议	选择后端服务器自身提供的网络服务的协议。 支持选择的协议有：TCP、UDP、HTTP、HTTPS。 后端服务器组的后端协议必须与监听器的前端协议保持一致，但 HTTP 和 HTTPS 监听器除外，HTTP 和 HTTPS 监听器对应的后端协议为 HTTP 或 HTTPS 均可。	HTTP
服务器组类型	选择服务器组的类型，支持如下： <ul style="list-style-type: none"> • ECS 服务器组：支持添加与 SLB 实例同 VPC 的云服务器实例（云服务器和裸金属服务器）作为后端服务器。 • IP 服务器组：开启“跨VPC访问”功能后，支持添加与 SLB 实例所属 VPC 以外的 IP 地址作为后端服务器。 	ECS服务器组
IP地址类型	选择服务器支持的IP版本，包含IPv4和IPv6。 服务器组创建后，将不支持修改IP地址类型。	IPv4
分配策略类型	选择负载均衡采用的算法。 <ul style="list-style-type: none"> • 加权轮询算法：SLB 实例按照后端服务器的权重，从高到低以轮询的方式将请求分发给各服务器，相同权重的服务器处理相同数目的连接数。当后端服务器的权重都设置为同一个值时，权重属性不生效，将按照简单的轮询策略。 • 加权最少连接数算法：最少连接是通过当前活跃的连接数来估计服务器负载情况的一种动态调度算法。加权最少连接数是在最少连接数的基础上，根据服务器的处理能力差异，给每个服务器分配不同的权重，使其能够接受相应权重值的服务请求。 • 源 IP 算法：将请求的源 IP 地址进行一致性 Hash 运算，得到一个具体的数值，同时对后端服务器进行编号，按照运算结果将请求分发到对应编号的服务器上。本算法可以实现对不同源 IP 的访问进行负载分发，同时保证同一个客户端 IP 的请求始终被派发至某特定的服务器。 • 随机算法：将请求随机分配给后端服务器，权重越高的后端服务器会被分配更多的访问请求。 	加权轮询算法

参数	配置说明	参数取值
	<ul style="list-style-type: none"> 源 IP 端口算法：仅后端协议选择“TCP”或“UDP”时支持该算法。将请求的源 IP 地址和端口进行一致性 Hash 算法，得到一个具体的数值，同时对后端服务器进行标号，按照运算结果将请求分发到对应标号的服务器上。本算法可以实现对不同源 IP 端口的访问进行负载分发，同时保证源 IP 和端口相同的请求会分配给相同的服务器。与源 IP 算法相比，本算法可能将相同源 IP 地址不同端口的请求分发到不同的后端服务器中。 	

新建服务器组

* 部门:

资源集:

* 名称:

* 专有网络:

* 后端协议:

* 服务器组类型:

* IP地址类型: IPv4 IPv6

* 分配策略类型:

* 会话保持: 是 否

* 健康检查配置: 开启 不开启

描述:

0/255

(4) 单击“新建”，完成创建服务器组操作。

2. 添加后端服务器

(1) 在 SLB 实例页面，单击左侧导航栏的“SLB 服务器组”，进入 SLB 服务器组页面。

- (2) 单击 **ServerGroup1** 的 ID，进入服务器组详情页面。
- (3) 在服务器列表页签，单击“添加服务器”，弹出添加服务器窗口。
- (4) 在选择服务器页面，选择云服务器 **ECS01** 和 **ECS02** 后，单击“下一步”。



- (5) 在修改参数页面，批量配置后端服务器的参数：
 - o 业务端口：后端服务器处理访问请求的端口，输入“80”。
 - o 权重：后端服务器的权重值，输入“100”。
 - o 角色：选择后端服务器为“主服务器”。



- (6) 单击“确定”，页面显示添加结果。
- (7) 单击“关闭”，关闭添加服务器窗口。

2.2.2.5 配置 SLB 实例监听器

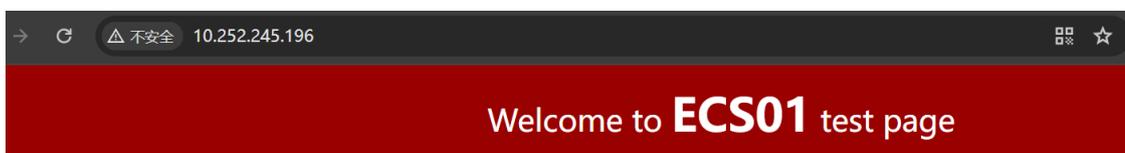
- (1) 在 SLB 实例页面，单击 SLB01 实例的 ID 链接，进入该 SLB 实例的基本信息页面。
- (2) 单击左侧导航栏中的“监听器”，进入监听器页面。
- (3) 单击“新建监听器”，弹出新建监听器窗口。
- (4) 根据下表中的参数说明进行配置，未列出的参数保持默认配置即可。

参数	配置说明	参数取值
名称	监听器的名称，可根据需要自定义名称或使用系统缺省名称。	listener01
前端协议/端口	选择监听协议并设置监听端口。 <ul style="list-style-type: none">监听协议：客户端与 SLB 实例监听器建立流量分发连接的协议。监听端口：接收请求并向后端服务器进行请求转发的监听端口，范围为 1~65535。	访问Nginx服务通常使用HTTP协议，默认的端口号是80。 <ul style="list-style-type: none">监听协议：HTTP监听端口：80
访问策略	选择访问策略： <ul style="list-style-type: none">允许所有 IP 访问：不进行访问控制，允许所有 IP 访问 SLB 实例。白名单：仅转发来自所选访问控制组中设置的 IP 地址或地址段的请求，适用于应用只允许特定 IP 访问的场景。黑名单：来自所选访问控制组中设置的 IP 地址或地址段的所有请求都不会转发，适用于应用只限制某些特定 IP 访问的场景。	允许所有IP访问
服务器组	选择要将监听请求转发到的服务器组。	ServerGroup1

- (5) 单击“确定”，完成创建 HTTP 监听器。

2.2.2.6 验证负载均衡服务

- (1) 在任意终端的浏览器中访问“http://SLB 的公网 IP 地址”，测试负载均衡服务。若如下图所示，则表示本次请求被 SLB 转发到了云服务器 ECS01 上，ECS01 正常处理请求并返回页面。



- (2) 由于服务器组的负载均衡采用加权轮询算法，且两台云服务器的权重都是“100”。所以刷新浏览器，再次发送请求，若如下图所示，则表示本次请求 SLB 转发到了云服务器 ECS02 上。

🔄 ⚠️ 不安全 10.252.245.196 ☆

Welcome to **ECS02** test page

Hello nginx , This is ECS02

3 操作指南

3.1 SLB实例

3.1.1 SLB 概述

SLB 实例类型

支持公网和私网两种类型的服务器负载均衡 SLB 实例。

实例类型	说明
公网IPv4 SLB实例	<ul style="list-style-type: none">只有 IPv4 地址，私网访问 IPv4 私网地址，公网访问 IPv4 EIP。支持“解绑 IPv4 公网 IP”。
私网IPv4 SLB实例	<ul style="list-style-type: none">只有 IPv4 地址，只能私网 IPv4 访问。支持“绑定 IPv4 公网 IP”。

3.1.2 新建 SLB 实例

简介

SLB 实例接收来自客户端的请求，并将请求分发给后端服务器。本文为您介绍如何创建 SLB 实例。

操作步骤

- (1) 在 SLB 实例页面，单击页面右上角的“新建负载均衡”，进入新建负载均衡页面。
- (2) 根据下表中的参数说明进行配置。

参数	说明
租户	仅租户管理员需配置该项。 选择SLB实例所属的租户。
部门	选择SLB实例所属的部门。
资源集	选择SLB实例所属的资源集。
区域	选择SLB实例所属的区域。 请确保SLB实例的区域和服务器组中添加的服务器的区域相同。
可用区	选择SLB实例所属的可用区。
规格	根据需要选择实例规格： <ul style="list-style-type: none">基础型：最大可以支持连接数 5000，新建连接数（CPS）：3000，每秒查询数（QPS）：1000。标准型：最大可以支持连接数 50000，新建连接数（CPS）：5000，每秒查询数（QPS）：5000。

参数	说明
	<ul style="list-style-type: none"> 高阶型：最大可以支持连接数 200000，新建连接数（CPS）：20000，每秒查询数（QPS）：20000。 <p>默认支持以上规格，系统具体支持的实例规格信息，请以界面上显示的为准。</p>
计费模式	<p>选择SLB实例的计费模式。</p> <ul style="list-style-type: none"> 按需计费：是一种先使用后付费的计费模式。 包年包月：是一种需要先付费才能使用资源的计费模式，适用于流量峰值比较稳定且需要长期使用的业务场景。
专有网络	<p>选择SLB实例所属的专有网络。</p> <p>您可以选择使用已有的专有网络，或者单击“新建VPC”创建新的专有网络。</p>
外网出口	<p>显示所选专有网络使用的外网出口信息。</p>
子网类型	<p>选择SLB实例所属子网的类型。</p> <ul style="list-style-type: none"> 标准型：默认仅能与 VPC 内的其它子网进行通信，或者通过 Internet 网关、NAT 网关、VPC 对等连接等网关组件与 VPC 外的网络进行通信。 直通型：默认可以和云下物理环境中的网段进行三层互通。
子网	<p>选择SLB实例所属的子网。</p> <p>您可以选择使用已有的子网网段，或者单击“新建子网”创建新的子网网段。</p>
国密	<p>选择SLB实例是否开启国密。</p> <p>开启国密将不支持TLS 1.3以及相关特性。</p>
跨VPC访问	<ul style="list-style-type: none"> 若子网类型为“标准型”，则可选择 SLB 实例是否启用跨 VPC 访问功能。开启跨 VPC 访问功能后，系统将使用资源子网（默认为 SLB 实例的 VIP 所属子网）中的 IP 地址创建负载均衡资源，请确保该子网拥有 9 个额外的可用 IP 地址。 若子网类型为“直通型”，则默认勾选“跨 VPC 访问”，资源子网为 SLB 实例的 VIP 所属子网，且不可修改。
资源子网	<p>配置SLB实例的资源子网：</p> <ul style="list-style-type: none"> 若不启用跨 VPC 访问，则 SLB 实例资源将会使用保留子网，由于所有 VPC 使用相同的保留子网网段，跨 VPC 访问会存在网段路由冲突。 启用跨 VPC 访问后，SLB 实例资源将会占用此处所选择的子网的 IP，如果需要跨 VPC 访问 SLB 或者 SLB 跨 VPC 访问后端服务，请确保 SLB 实例的 VIP 所在的子网和资源子网都配置了相应的路由。
实例IP地址	<p>配置SLB实例的私有IP地址。</p> <ul style="list-style-type: none"> 自动分配：由系统自动分配 SLB 实例的私有 IP 地址。 手动分配：需要您手动指定 SLB 实例的私有 IP 地址。
公网IPv4	<p>选择SLB实例是否支持分发来自公网的请求。</p>
弹性公网IP	<p>启用“公网IPv4”时需配置该项。绑定弹性公网IP的SLB实例可以接收来自公网的访问请求并将请求分发到服务器组内的后端服务器。</p> <p>您可以选择已有或新购弹性公网IP与SLB实例进行绑定。</p> <ul style="list-style-type: none"> 选择已有：在弹性公网 IP 实例下拉框中选择系统中已创建的 EIP 实例。 新购弹性公网 IP： <ul style="list-style-type: none"> 线路：选择弹性公网 IP 的线路，目前仅支持“单线”，即通过单个网络运营商访问公网，成本低且便于自主调度。当进行跨运营商访问时，单线公网 IP 地址会存在延迟过长、丢包增加、抖动增大等问题。

参数	说明
	<ul style="list-style-type: none"> 带宽：弹性公网 IP 的带宽大小，默认为 10 Mbps，带宽范围为 1-500 Mbps。 弹性公网名称：弹性公网 IP 的名称，可根据需要自定义名称或使用系统缺省名称。
启用IPv6	仅当选择开启了IPv6的子网时，该项才可配置。 选择SLB实例是否启用IPv6。
IPv6地址	启用IPv6后，可选择IPv6地址的分配方式： <ul style="list-style-type: none"> 自动分配：由系统自动分配 SLB 实例的内网 IPv6 地址。 手动分配：由用户指定 IPv6 地址，需配置地址后缀展示方式，指定 SLB 实例的 IPv6 地址。
名称	SLB实例的名称，自定义名称或使用系统缺省名称。
描述	输入描述信息，最多255个字符。
新建实例数量	单次要创建SLB实例的数量，目前仅支持1个。
开通时长	若计费模式选择“包年包月”，则需选择SLB实例的开通时长，可选时长为1-9个月、1-3年。

(3) 单击“下一步”，进入确认配置页面。

(4) 确认要创建的 SLB 实例信息无误后，单击“确定新建”，完成创建 SLB 实例操作。

3.1.3 查看 SLB 实例信息

1. 简介

本文介绍如何查看 SLB 实例资源概况及单个 SLB 实例的详情信息。

若 SLB 实例列表由于列项过多而无法显示在同一页面时，可通过定制列操作，自定义 SLB 实例列表要显示的列项信息，方便查看。

2. 在 SLB 实例列表查看实例信息

在 SLB 实例页面，您可以查看所选区域下已有的 SLB 实例信息，具体参数说明如下表所示。

参数	说明
负载均衡名称/ID	SLB实例的名称和ID信息。 <ul style="list-style-type: none"> 单击名称后的, 可修改 SLB 实例的名称。 单击 ID 后的, 可复制 SLB 实例的 ID 信息。 单击 ID, 可进入 SLB 实例详情页面。
状态	SLB实例的状态，包括运行中、新建中、配置中、删除中、异常、已停止和升级中。 单击状态右侧的  , 可筛选查看指定状态的SLB实例信息。
实例规格	SLB实例的规格。
国密	SLB实例是否支持国密。 单击国密右侧的  , 可筛选查看支持/不支持国密特性的SLB实例信息。

参数	说明
跨VPC	SLB实例是否支持跨VPC访问。 单击跨VPC右侧的  , 可筛选查看支持/不支持跨VPC访问特性的SLB实例信息。
专有网络ID	SLB实例所属的专有网络的ID信息。 <ul style="list-style-type: none"> 单击 ID, 可跳转至该专有网络的详情页面。 单击 ID 后的, 可复制专有网络的 ID 信息。
IP地址/带宽	SLB实例的IP地址和带宽信息: <ul style="list-style-type: none"> 私网 IP: SLB 实例的私网 IP 地址。 公网 IP: SLB 实例绑定的弹性公网 IP 的地址及带宽大小。 <ul style="list-style-type: none"> 单击 IP 地址, 可跳转至该弹性公网 IP 的详情页面。 IPv6: SLB 实例的私网 IPv6 地址及带宽大小。 <ul style="list-style-type: none"> 单击 IPv6 地址, 可跳转至 IPv6 网关详情页面查看该 IPv6 地址的详细信息。
计费模式	SLB实例的计费模式, 包括包年包月和按需计费。
监听器 (前端协议/端口)	<ul style="list-style-type: none"> 若 SLB 实例未关联监听器, 则显示--。 若 SLB 实例已关联监听器, 则显示所关联监听器的 ID, 及监听器中配置的前端协议和端口信息。 <ul style="list-style-type: none"> 单击监听器 ID, 可进入该监听器的详情页面。
租户	仅租户管理员可查看到该项。 SLB实例所属租户的名称。
部门	SLB实例所属部门的名称。
资源集	SLB实例所属资源集的名称和ID。
后端健康状况	SLB实例后端服务器处于健康或不健康状态的个数。
创建时间	SLB实例的创建时间。
操作	<p>可对SLB实例进行的操作:</p> <ul style="list-style-type: none"> IP 地址管理 变配 SLB 实例 启动/停止 SLB 实例 修改 SLB 实例规格限速信息 续费 SLB 实例 (包年包月计费模式) 退订 SLB 实例 (包年包月计费模式) 删除 SLB 实例 (按需计费模式)

3. 查看 SLB 系统资源

SLB 实例分为系统资源和租户资源。

- SLB 系统资源由云服务创建, 用于部署云服务依赖的相关资源。
- SLB 租户资源由租户创建, 用于实现将业务访问流量根据分发策略分发到后端服务器组。

SLB 实例列表默认不展示系统资源，只有当前用户为“系统级平台用户”时，才有权限配置是否要“显示系统资源”。

在 SLB 实例页面，单击“显示系统资源”后的 ，可以在 SLB 实例列表中显示当前用户权限下的所有 SLB 系统资源，SLB 系统资源会在 SLB 实例名称前标识“系统”标签。

4. 定制 SLB 实例列表

- (1) 在 SLB 实例页面，单击页面右上角的 ，在弹出的下拉窗口中选择一个或多个要显示/隐藏的列名。
- (2) 单击“确定”，完成定制 SLB 实例列表操作。

5. 查看 SLB 实例详情

在 SLB 实例页面，单击 SLB 实例的 ID，进入该 SLB 实例的详情页面，可查看如下信息：

- 基本信息：SLB 实例的基本信息、规格限速信息和计费信息。
- IP 地址管理：SLB 实例的 IP 地址信息。
- 监听器：SLB 实例的监听器列表信息。
- 监控：支持从 SLB 实例、监听器和转发策略维度查看监控信息。

3.1.4 修改 SLB 实例规格限速信息

简介

SLB 实例规格限速默认仅展示最大连接数和每秒查询数（Queries Per Second, QPS），且不支持修改。

通过该功能，可配置 SLB 实例规格的限速，包括新建连接数、每秒包数和带宽。

前提条件

已在运维中心的“运维 > 网络 > 服务器负载均衡 SLB > SLB 全局参数”页面，将对应参数的配置信息置为“true”，若某一参数为“false”，则将不支持在此页面修改此规格参数的限速。

- slb_enable_config_qos_cps_limit: 新建连接数
- slb_enable_config_qos_pps_limit: 每秒包数
- slb_enable_config_qos_bandwidth_limit: 带宽

若以上参数的配置信息均为“false”，则“编辑限速信息”将不会在页面上显示。

限制与指导

新建连接数、每秒包数和带宽的限速，下发配置生效大约需要 10 秒左右。

操作步骤

- (1) 在 SLB 实例页面，单击 SLB 实例的 ID，进入该 SLB 实例的基本信息页面。
- (2) 在规格限速信息区域，单击“编辑限速信息”，弹出限速调整窗口。
- (3) 根据下表中的参数说明进行配置。

参数	说明
新建连接数(CPS)	<p>CPS（Connection Per Second，新建连接数）表示SLB实例每秒可以新建的连接数。</p> <p>配置SLB实例新建连接数的限速信息：</p> <ul style="list-style-type: none"> • 无限速：不限制 SLB 实例每秒可以新建连接数的数量。 • 限速：输入 SLB 实例每秒可以新建连接数的最大值。
每秒包数(PPS)	<p>PPS（Packets Per Second，每秒包数）表示SLB实例每秒能够处理数据包的数量。</p> <p>配置SLB实例每秒包数的限速信息：</p> <ul style="list-style-type: none"> • 无限速：不限制 SLB 实例每秒可以处理数据包的数量。 • 限速：输入 SLB 实例每秒可以处理数据包数量的最大值。
带宽(Kbps)	<p>表示SLB每秒能够传输的数据量，单位为Kbps。</p> <p>配置SLB实例带宽的限速信息：</p> <ul style="list-style-type: none"> • 无限速：不限制 SLB 实例每秒能够传输的数据量。 • 限速：输入 SLB 实例每秒能够传输数据量的最大值。

(4) 单击“确定”，完成修改 SLB 实例规格限速信息。

3.1.5 IP 地址管理

3.1.5.1 服务 IP 地址

1. 添加 IPv4 地址

简介

SLB 实例最多支持拥有 8 个私网 IPv4，每一个私网 IPv4 绑定一个 EIP，EIP 可以来自于不同的运营商。并支持为指定的私网 IPv4 启用 IPv6。

操作步骤

- (1) 在 SLB 实例页面，单击 SLB 实例对应操作列的“IP 地址管理”，进入 IP 地址管理页面。
- (2) 单击“添加 IPv4 地址”，弹出添加 IPv4 地址窗口。
- (3) 根据下表中的参数说明进行配置。

参数	说明
IPv4地址	<p>选择SLB实例私有IPv4地址的分配方式。</p> <ul style="list-style-type: none"> • 自动分配：由系统自动分配 SLB 实例的私有 IPv4 地址。 • 手动分配：需要您手动指定 SLB 实例的私有 IPv4 地址。
公网IPv4	选择SLB实例是否支持分发来自公网的请求。
弹性公网IP	<p>启用“公网IPv4”时需配置该项。绑定弹性公网IP的SLB实例可以接收来自公网的访问请求并将请求分发到服务器组内的后端服务器。</p> <p>在下拉列表中选择已有的EIP实例进行绑定。</p>

(4) 单击“确定”，完成添加 IPv4 地址操作。

2. 绑定 IPv4 公网 IP

简介

私网 IPv4 SLB 实例绑定弹性公网 IP 后，便可以转发来自公网的请求。

限制与指导

- 仅私网 IPv4 SLB 实例支持绑定 IPv4 公网 IP。
- SLB 实例所在的区域必须和弹性公网 IP 的区域相同。
- 一个私网 IPv4 只能绑定一个弹性公网 IP。

前提条件

已创建一个弹性公网 IP。

操作步骤

- (1) 在 SLB 实例页面，单击 SLB 实例对应操作列的“绑定 IPv4 公网 IP”，弹出绑定 IPv4 公网 IP 窗口。
- (2) 选择一个要绑定的弹性公网 IP。
- (3) 单击“确定”，完成绑定操作。

3. 解绑 IPv4 公网 IP

简介

公网 IPv4 SLB 实例解绑弹性公网 IP 后，将无法进行 IPv4 公网流量转发。

限制与指导

仅公网 IPv4 SLB 实例支持解绑 IPv4 公网 IP。

操作步骤

- (1) 在 SLB 实例页面，单击 SLB 实例对应操作列的“IP 地址管理”，进入 IP 地址管理页面。
- (2) 单击私网 IP 地址对应操作列的“解绑 IPv4 公网 IP”，弹出确认窗口。
- (3) 确定要解绑的弹性公网 IP 信息无误后，单击“确定”，完成解绑操作。

4. 启用 IPv6

简介

SLB 实例启用 IPv6 后，会在拥有一个私网 IPv4 地址的基础上，再拥有一个私网 IPv6 地址，从而具备 IPv4 和 IPv6 双栈接入能力。SLB 实例可使用该 IPv6 地址对外提供服务。

限制与指导

若 SLB 所在子网未开启 IPv6，则 SLB 实例对应操作列的“启用 IPv6”灰显。

操作步骤

- (1) 在 SLB 实例页面，单击 SLB 实例对应操作列的“IP 地址管理”，进入 IP 地址管理页面。
- (2) 单击私网 IP 地址对应操作列的“启用 IPv6”，弹出启用 IPv6 窗口。
- (3) 根据下表中的参数说明进行配置。

参数	说明
IPv6地址	启用IPv6后，可选择IPv6地址的分配方式： <ul style="list-style-type: none">• 自动分配：由系统为 SLB 实例分配其所在子网的 IPv6 网段中的 IPv6 地址。• 手动分配：由用户指定 IPv6 地址，需配置地址后缀展示方式，指定 SLB 实例的 IPv6 地址。

- (4) 单击“确定”，完成启用 IPv6 操作。

5. 停用 IPv6

简介

SLB 实例停用 IPv6 后，将仅拥有一个私网 IPv4 地址，无法再使用该 IPv6 地址对外提供服务。

限制与指导

- SLB 实例停用 IPv6 后，拥有的 IPv6 地址将被立即释放，下次启用 IPv6 时将会为 SLB 实例重新分配新的 IPv6 地址。
- 若 SLB 实例的监听器关联了 IPv6 服务器组，则需要先解除监听器和 IPv6 服务器组的关联后，再进行停用 IPv6 操作。

前提条件

SLB 实例已启用 IPv6。

操作步骤

- (1) 在 SLB 实例页面，单击 SLB 实例对应操作列的“IP 地址管理”，进入 IP 地址管理页面。
- (2) 单击私网 IP 地址对应操作列的“停用 IPv6”，弹出停用 IPv6 窗口。
- (3) 单击“确定”，完成停用 IPv6 操作。

6. 删除私网 IP 地址

简介

当您确认 SLB 实例不需要继续使用某一个私网 IP 时，您可以随时删除私网 IP 地址。

限制与指导

- 仅有一条私网 IPv4 地址时，不支持删除操作。
- 若 IPv6 地址已购买带宽包，则需要先删除 IPv6 地址的带宽后，才支持删除操作。

操作步骤

- (1) 在 SLB 实例页面，单击 SLB 实例对应操作列的“IP 地址管理”，进入 IP 地址管理页面。

- (2) 单击私网 IP 地址对应操作列的“删除”，弹出删除窗口。
- (3) 确认要删除的私网 IP 地址信息无误后，单击“确定”，完成删除私网 IP 操作。

3.1.5.2 资源子网 IP 地址

1. 查看资源子网 IP 地址列表

简介

可查看 SLB 实例所占用的 IPv4 和 IPv6 的信息。

操作步骤

- (1) 在 SLB 实例页面，单击 SLB 实例对应操作列的“IP 地址管理”，进入 IP 地址管理页面。
- (2) 在资源子网 IP 地址页签，可查看资源子网 IP 地址的信息，参数说明如下表所示。

参数	说明
IPv4地址	SLB实例占用的IPv4地址，即Nginx Pod IPv4地址。
IPv6地址	SLB实例占用的IPv6地址，即和Nginx Pod IPv4地址相同Port的IPv6地址。
IPv4网段	IPv4地址所属的网段。
IPv6网段	IPv6地址所属的网段。
可用区	SLB实例所在的可用区。

3.1.6 变配 SLB 实例

简介

支持对 SLB 实例的规格进行变配操作，包括升配或降配，实例的费用会根据变配后的规格进行调整。

限制与指导

- SLB 实例升配后，实例规格和默认限速值均会调整，但是自定义的限速不会调整。请在升配后，调整自定义实例限速为合适的值。
- SLB 实例默认不支持降配操作，若在特殊场景需要进行 SLB 实例降配操作，可以联系运维管理员临时启用降配功能。降配后，实例的规格和默认限速均会调整。



注意

降配操作会删除自定义的限速，以防止降配前自定义的限速值超过降配后实例资源的承载能力。

操作步骤

- (1) 在 SLB 实例页面，单击 SLB 实例对应操作列的“变配”，进入变配页面。
- (2) 确认 SLB 实例当前的配置信息，并选择要变配到的规格后，单击“下一步”，进入变配确认页面。
- (3) 确认 SLB 实例信息和费用后，单击“确认变更”，返回 SLB 实例列表页面，该 SLB 实例状态显示为“升级中”。
- (4) 待 SLB 实例状态由“升级中”变为“运行中”，则表示该 SLB 实例的规格已完成变配。

3.1.7 启动/停止 SLB 实例

1. 简介

您可以随时启动和停止 SLB 实例。

出于业务考虑，某些 SLB 实例暂时无需使用，但又不能删除时，可以选择停止实例。SLB 实例停止后，将不再接收和转发流量。

2. 启动实例

- (1) 在 SLB 实例页面，单击 SLB 实例对应操作列的“更多 > 启动实例”，弹出确认窗口。
- (2) 确认要启动的 SLB 实例信息无误后，单击“确定”，可启动 SLB 实例。

3. 停止实例

- (1) 在 SLB 实例页面，单击 SLB 实例对应操作列的“更多 > 停止实例”，弹出确认窗口。
- (2) 确认要停止的 SLB 实例信息无误后，单击“确定”，可停止 SLB 实例。

3.1.8 续费 SLB 实例（包年包月计费模式）

简介

包年包月计费模式的 SLB 实例支持续费操作。

限制与指导

- 未过期的 SLB 实例，续费操作成功后会在当前周期结束后生效。
- 已过期的 SLB 实例，新续费周期从过期时间开始计算。

操作步骤

- (1) 在 SLB 实例页面，单击 SLB 实例对应操作列的“更多 > 续费”，进入续费页面。
- (2) 选择续费时长及费用后，单击“去开启”，完成续费 SLB 实例操作。

3.1.9 退订/删除 SLB 实例

1. 简介

当您确认 SLB 实例不需要继续使用时，您可以随时退订或释放 SLB 实例。

- 包年包月计费模式的 SLB 实例支持退订操作。
- 按需计费模式的 SLB 实例支持删除操作。

2. 限制与指导

- 若 SLB 实例下存在关联的监听器，则无法进行删除操作。
- 若 SLB 已绑定弹性公网 IP，则无法进行删除操作。

3. 退订 SLB 实例（包年包月计费模式）

- (1) 在 SLB 实例页面，单击 SLB 实例对应操作列的“更多 > 退订”，进入退订页面。
- (2) 选择并确认要退订的 SLB 实例信息及退款金额无误后，单击“退订”，完成退订 SLB 实例操作。

4. 删除 SLB 实例（按需计费模式）

- (1) 在 SLB 实例页面，单击 SLB 实例对应操作列的“更多 > 删除”，弹出确认窗口。
- (2) 确认要删除的 SLB 实例信息无误后，单击“确定”，即可删除该 SLB 实例。

3.2 监听器

3.2.1 监听器概述

创建 SLB 实例后，您需要为 SLB 实例配置监听器。监听器负责监听 SLB 实例上的请求，并根据调度算法定义的转发策略将流量分发至后端服务器上。

支持的协议类型

负载均衡支持四层协议和七层协议监听，您可根据应用场景选择监听协议。

- 四层协议：传输层协议（TCP、UDP 或 TCPSSL），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（HTTP 或 HTTPS），基于 URL、HTTP 头部等应用层信息进行流量分发。

协议类型		说明
四层协议	TCP	面向连接的、可靠的、基于字节流的传输层通信协议。 <ul style="list-style-type: none"> • 传输的源端和终端需先进行三次握手建立连接，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。
	UDP	无连接的传输层通信协议。 <ul style="list-style-type: none"> • 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。

协议类型		说明
	TCPSSL	可以转发来自客户端加密的TCP协议请求，适用于TCP协议下对安全性要求非常高的场景，例如大规模TLS卸载场景。
七层协议	HTTP	应用层协议。 <ul style="list-style-type: none"> 支持基于请求域名和 URL 的转发。 支持基于 Cookie 的会话保持。
	HTTPS	加密的应用层协议。 <ul style="list-style-type: none"> 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，SLB 完成解密操作。 支持单向认证和双向认证。

3.2.2 创建监听器

限制与指导

- 创建监听器时，若要配置访问策略的黑名单或白名单，您需要先创建访问控制组，具体操作请参见[创建访问控制组](#)。
- 每个访问控制组最多关联 50 个监听器。
- 若监听器要关联 IPv6 地址类型的后端服务器组，则 SLB 实例必须开启 IPv6。

3.2.2.1 创建 TCP 监听器

简介

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。您可以在 SLB 实例上创建一个 TCP 监听器转发来自客户端的 TCP 协议请求。

操作步骤

- 在 SLB 实例页面，单击 SLB 实例的 ID 链接，进入该 SLB 实例的基本信息页面。
- 单击左侧导航栏中的“监听器”，进入监听器页面。
- 单击“新建监听器”，弹出新建监听器窗口。
- 根据下表中的参数说明进行配置。

参数	说明
名称	监听器的名称，可根据需要自定义名称或使用系统缺省名称。
前端协议/端口	选择监听协议并设置监听端口。 <ul style="list-style-type: none"> 监听协议：客户端与 SLB 实例监听器建立流量分发连接的协议，选择“TCP”。 监听端口：接收请求并向后端服务器进行请求转发的监听端口，范围为 1~65535。

参数	说明
访问策略	选择访问策略： <ul style="list-style-type: none"> 允许所有 IP 访问：不进行访问控制，允许所有 IP 访问 SLB 实例。 白名单：仅转发来自所选访问控制组中设置的 IP 地址或地址段的请求，适用于应用只允许特定 IP 访问的场景。 黑名单：来自所选访问控制组中设置的 IP 地址或地址段的所有请求都不会转发，适用于应用只限制某些特定 IP 访问的场景。
访问控制组	当访问策略选择“白名单”或“黑名单”时需配置访问控制组。 选择访问控制组的IP类型后，在下拉列表选择一个访问控制组。
空闲超时时间	根据需要设置空闲超时时长，取值范围为1~3600秒，监听默认为60秒。 若在超时时间内一直没有访问请求，则负载均衡会中断当前连接，直到下一次请求到来时再重新建立新的连接。
服务器组	选择要将监听请求转发到的服务器组。 您可以选择使用已有的服务器组，或者单击“新建服务器组”创建新的服务器组，具体说明请参见 创建服务器组 。
描述	可根据需要输入描述信息，最多255个字符。

(5) 单击“确定”，完成创建 TCP 监听器。

3.2.2.2 创建 UDP 监听器

简介

UDP 协议多用于关注实时性而相对不注重可靠性的场景，如视频聊天和金融实时行情推送等。您可以在 SLB 实例上创建一个 UDP 监听器转发来自客户端的 UDP 协议请求。

操作步骤

- (1) 在 SLB 实例页面，单击 SLB 实例的 ID 链接，进入该 SLB 实例的基本信息页面。
- (2) 单击左侧导航栏中的“监听器”，进入监听器页面。
- (3) 单击“新建监听器”，弹出新建监听器窗口。
- (4) 根据下表中的参数说明进行配置。

参数	说明
名称	监听器的名称，可根据需要自定义名称或使用系统缺省名称。
前端协议/端口	选择监听协议并设置监听端口。 <ul style="list-style-type: none"> 监听协议：客户端与 SLB 实例监听器建立流量分发连接的协议，选择“UDP”。 监听端口：接收请求并向后端服务器进行请求转发的监听端口，范围为 1~65535。
访问策略	选择访问策略： <ul style="list-style-type: none"> 允许所有 IP 访问：不进行访问控制，允许所有 IP 访问 SLB 实例。

参数	说明
	<ul style="list-style-type: none"> 白名单：仅转发来自所选访问控制组中设置的 IP 地址或地址段的请求，适用于应用只允许特定 IP 访问的场景。 黑名单：来自所选访问控制组中设置的 IP 地址或地址段的所有请求都不会转发，适用于应用只限制某些特定 IP 访问的场景。
访问控制组	当访问策略选择“白名单”或“黑名单”时需配置访问控制组。 选择访问控制组的IP类型后，在下拉列表中选择一个访问控制组。
空闲超时时间	根据需要设置空闲超时时长，取值范围为1~3600秒，默认为10秒。 若在超时时间内一直没有访问请求，则负载均衡会中断当前连接，直到下一次请求到来时再重新建立新的连接。
服务器组	选择要将监听请求转发到的服务器组。 您可以选择使用已有的服务器组，或者单击“新建服务器组”创建新的服务器组，具体说明请参见 创建服务器组 。
描述	可根据需要输入描述信息，最多255个字符。

(5) 单击“确定”，完成创建 UDP 监听器。

3.2.2.3 创建 HTTP 监听器

简介

HTTP 协议适用于需要对数据内容进行识别的应用，如 Web 应用和小型手机游戏等。您可以在 SLB 实例上创建一个 HTTP 监听器转发来自客户端的 HTTP 协议请求。

操作步骤

- (1) 在 SLB 实例页面，单击 SLB 实例的 ID 链接，进入该 SLB 实例的基本信息页面。
- (2) 单击左侧导航栏中的“监听器”，进入监听器页面。
- (3) 单击“新建监听器”，弹出新建监听器窗口。
- (4) 根据下表中的参数说明进行配置。

参数	说明
名称	监听器的名称，可根据需要自定义名称或使用系统缺省名称。
前端协议/端口	选择监听协议并设置监听端口。 <ul style="list-style-type: none"> 监听协议：客户端与 SLB 实例监听器建立流量分发连接的协议，选择“HTTP”。 监听端口：接收请求并向后端服务器进行请求转发的监听端口，范围为 1~65535。
访问策略	选择访问策略： <ul style="list-style-type: none"> 允许所有 IP 访问：不进行访问控制，允许所有 IP 访问 SLB 实例。 白名单：仅转发来自所选访问控制组中设置的 IP 地址或地址段的请求，适用于应用只允许特定 IP 访问的场景。

参数	说明
	<ul style="list-style-type: none"> 黑名单：来自所选访问控制组中设置的 IP 地址或地址段的所有请求都不会转发，适用于应用只限制某些特定 IP 访问的场景。
访问控制组	<p>当访问策略选择“白名单”或“黑名单”时需配置访问控制组。</p> <p>选择访问控制组的IP类型后，在下拉列表中选择一个访问控制组。</p>
重定向	<p>若某个SLB实例下同时创建了多个HTTP或HTTPS监听器，则可以通过重定向功能，将该HTTP监听器的监听请求重定向至当前SLB实例下的其它HTTP或HTTPS监听器。</p> <ul style="list-style-type: none"> 重定向：启用该项。 协议：选择要重定向到的协议类型，包括 HTTP 和 HTTPS。 端口：选择要重定向到的端口。 状态码：请根据需要选择 HTTP 监听器重定向的状态，支持如下： <ul style="list-style-type: none"> 301：永久重定向，表示被请求的资源已经永久移动到新位置。 302：临时重定向，表示被请求的资源临时从不同位置响应。 307：临时重定向，307 和 302 类似，区别在于 307 不允许在重定向时改变请求的方法。 308：永久重定向，表示被请求的资源已经永久移动到新位置，308 与 301 类似，区别在于 308 保留了原始请求的方法，即 HTTP 请求中的请求方法和请求主体不会更改。
服务器组	<p>不启用重定向功能时，需选择要将监听请求转发到的服务器组。</p> <p>您可以选择使用已有的服务器组，或者单击“新建服务器组”创建新的服务器组，具体说明请参见创建服务器组。</p>
高级特性	单击“开启”，展开高级特性区域。
Gzip压缩	<p>选择是否启用Gzip压缩功能。</p> <ul style="list-style-type: none"> 开启：可对特定文件类型进行压缩，目前 Gzip 支持压缩的类型包括：<code>text/plain</code>、<code>text/css</code>、<code>application/json</code>、<code>application/x-javascript</code>、<code>text/xml</code>、<code>application/xml</code>、<code>application/xml+rss</code>、<code>text/javascript</code>。 关闭：不会对任何文件类型进行压缩。
空闲超时时间	<p>设置空闲超时时长，范围为1~3600秒。</p> <p>若在超时时间内一直没有访问请求，则负载均衡会中断当前连接，直到下一次请求到来时再重新建立新的连接。</p>
请求超时时间	<p>设置请求超时时间，范围为1~600秒。</p> <p>客户端向负载均衡发起请求，若在超时时间内后端服务器一直没有响应，则负载均衡将放弃等待，并给客户端返回HTTP 504错误码。</p>
附加头	<p>根据需要选择要添加的自定义HTTP头字段：</p> <ul style="list-style-type: none"> 通过 X-Forwarded-For 获取客户端 IP 通过 X-Forwarded-LBID 获取实例 LBID 通过 X-Forwarded-Proto 获取实例监听协议 通过 X-Forwarded-Port 获取实例监听端口 通过 X-Forwarded-Client-Port 获取客户端端口
描述	可根据需要输入描述信息，最多255个字符。

- (5) 单击“确定”，完成创建 HTTP 监听器。

3.2.2.4 创建 HTTPS 监听器

简介

HTTPS 协议适用于需要加密传输的应用。您可以在 SLB 实例上创建一个 HTTPS 监听器转发来自客户端的 HTTPS 协议请求。

操作步骤

- (1) 在 SLB 实例页面，单击 SLB 实例的 ID 链接，进入该 SLB 实例的基本信息页面。
- (2) 单击左侧导航栏中的“监听器”，进入监听器页面。
- (3) 单击“新建监听器”，弹出新建监听器窗口。
- (4) 根据下表中的参数说明进行配置。

参数	说明
名称	监听器的名称，可根据需要自定义名称或使用系统缺省名称。
前端协议/端口	选择监听协议并设置监听端口。 <ul style="list-style-type: none"> • 监听协议：客户端与 SLB 实例监听器建立流量分发连接的协议，选择“HTTPS”。 • 监听端口：接收请求并向后端服务器进行请求转发的监听端口，范围为 1~65535。
访问策略	选择访问策略： <ul style="list-style-type: none"> • 允许所有 IP 访问：不进行访问控制，允许所有 IP 访问 SLB 实例。 • 白名单：仅转发来自所选访问控制组中设置的 IP 地址或地址段的请求，适用于应用只允许特定 IP 访问的场景。 • 黑名单：来自所选访问控制组中设置的 IP 地址或地址段的所有请求都不会转发，适用于应用只限制某些特定 IP 访问的场景。
访问控制组	当访问策略选择“白名单”或“黑名单”时需配置访问控制组。 选择访问控制组的 IP 类型后，在下拉列表中选择一个访问控制组。
国密签名	仅开启了国密的 SLB 实例支持配置该项。 在下拉列表中选择国密签名证书。
国密加密	仅开启了国密的 SLB 实例支持配置该项。 在下拉列表中选择国密加密证书。
服务器证书	选择服务器证书。 服务器证书可用于证明服务器的身份，用户浏览器可用于检查服务器发送的证书是否是由自己信赖的中心签发的。 单击“添加双证书”，可选择第二个服务器证书。
服务器组	选择要将监听请求转发到的服务器组。 您可以选择使用已有的服务器组，或者单击“新建服务器组”创建新的服务器组，具体说明请参见 创建服务器组 。

参数	说明
高级特性	单击“开启”，展开高级特性区域。
Gzip压缩	选择是否启用Gzip压缩功能。 <ul style="list-style-type: none"> 开启：可对特定文件类型进行压缩，目前 Gzip 支持压缩的类型包括：<code>text/plain</code>、<code>text/css</code>、<code>application/json</code>、<code>application/x-javascript</code>、<code>text/xml</code>、<code>application/xml</code>、<code>application/xml+rss</code>、<code>text/javascript</code>。 关闭：不会对任何文件类型进行压缩。
空闲超时时间	设置空闲超时时长，范围为1~3600秒。 若在超时时间内一直没有访问请求，则负载均衡会中断当前连接，直到下一次请求到来时再重新建立新的连接。
请求超时时间	设置请求超时时长，范围为1~600秒。 客户端向负载均衡发起请求，若在超时时间内后端服务器一直没有响应，则负载均衡将放弃等待，并给客户端返回HTTP 504错误码。
附加头	根据需要选择要添加的自定义HTTP头字段： <ul style="list-style-type: none"> 通过 X-Forwarded-For 获取客户端 IP 通过 X-Forwarded-LBID 获取实例 LBID 通过 X-Forwarded-Proto 获取实例监听协议 通过 X-Forwarded-Port 获取实例监听端口 通过 X-Forwarded-Client-Port 获取客户端端口
启用HTTP/2	超文本传输协议2.0，是下一代HTTP协议。如果您需要保证HTTPS业务更加安全，可以启用HTTP/2功能。
双向认证	若SLB实例开启了国密，则不支持配置该项。 选择是否启用双向认证功能。 <ul style="list-style-type: none"> 开启：启用双向认证功能后，只有当客户端能够出具指定 CA 签发的证书时，连接才能成功。 关闭：不启用双向认证。
CA证书	启用双向认证功能后，需在下拉列表中选择CA证书。
安全策略	选择监听器的安全策略。 有关安全策略的说明，请参见 安全策略 。
描述	可根据需要输入描述信息，最多255个字符。

(5) 单击“确定”，完成创建 HTTPS 监听器。

3.2.2.5 创建 TCPSSL 监听器

简介

TCPSSL 协议多用于需要超高性能和大规模 TLS 卸载的场景。您可以在 SLB 实例上创建一个 TCPSSL 监听器转发来自客户端加密的 TCP 协议请求。

操作步骤

- (1) 在 SLB 实例页面，单击 SLB 的 ID 链接，进入该 SLB 实例的基本信息页面。
- (2) 单击左侧导航栏中的“监听器”，进入监听器页面。
- (3) 单击“新建监听器”，弹出新建监听器窗口。
- (4) 根据下表中的参数说明进行配置。

参数	说明
名称	监听器的名称，可根据需要自定义名称或使用系统缺省名称。
前端协议/端口	选择监听协议并设置监听端口。 <ul style="list-style-type: none">监听协议：客户端与 SLB 实例监听器建立流量分发连接的协议，选择“TCPSSL”。监听端口：接收请求并向后端服务器进行请求转发的监听端口，范围为 1~65535。
访问策略	选择访问策略： <ul style="list-style-type: none">允许所有 IP 访问：不进行访问控制，允许所有 IP 访问 SLB 实例。白名单：仅转发来自所选访问控制组中设置的 IP 地址或地址段的请求，适用于应用只允许特定 IP 访问的场景。黑名单：来自所选访问控制组中设置的 IP 地址或地址段的所有请求都不会转发，适用于应用只限制某些特定 IP 访问的场景。
访问控制组	当访问策略选择“白名单”或“黑名单”时需配置访问控制组。 选择访问控制组的IP类型后，在下拉列表选择一个访问控制组。
国密签名	仅开启了国密的SLB实例支持配置该项。 在下拉列表中选择国密签名证书。
国密加密	仅开启了国密的SLB实例支持配置该项。 在下拉列表中选择国密加密证书。
空闲超时时间	设置空闲超时时长，范围为1~3600秒。 若在超时时间内一直没有访问请求，则负载均衡会中断当前连接，直到下一次请求到来时再重新建立新的连接。
服务器证书	选择服务器证书。 服务器证书可用来证明服务器的身份，用户浏览器可用来检查服务器发送的证书是否是由自己信赖的中心签发的。 单击“添加双证书”，可选择第二个服务器证书。
服务器组	选择要将监听请求转发到的服务器组。 您可以选择使用已有的服务器组，或者单击“新建服务器组”创建新的服务器组，具体说明请参见 创建服务器组 。
双向认证	若SLB实例开启了国密，则不支持配置该项。 选择是否启用双向认证功能。 <ul style="list-style-type: none">开启：启用双向认证功能后，只有当客户端能够出具指定 CA 签发的证书时，连接才能成功。关闭：不启用双向认证。
CA证书	启用双向认证功能后，需在下拉列表中选择CA证书。

参数	说明
安全策略	选择监听器的安全策略。 有关安全策略的说明，请参见 安全策略 。
描述	可根据需要输入描述信息，最多255个字符。

(5) 单击“确定”，完成创建 TCPSSL 监听器。

3.2.3 编辑限速信息

简介

支持从监听维度对 TCP、UDP、TCPSSL、HTTP、HTTPS 协议的端口进行限速。

限制与指导

- 若要配置新建连接数、每秒包数和带宽的限速，则需要先在运维中心的“运维 > 网络 > 服务器负载均衡 SLB > SLB 全局参数”页面，将对应参数的配置信息置为“true”，若某一参数为“false”，则将不支持在此页面修改此规格参数的限速。
 - slb_enable_config_qos_cps_limit: 新建连接数
 - slb_enable_config_qos_pps_limit: 每秒包数
 - slb_enable_config_qos_bandwidth_limit: 带宽
- 新建连接数、每秒包数和带宽的限速，下发配置生效大约需要 10 秒左右。

操作步骤

- 在 SLB 实例页面，单击 SLB 实例的 ID，进入该 SLB 实例的基本信息页面。
- 单击左侧导航栏中的“监听器”，进入监听器页面。
- 单击监听器的 ID，进入监听器详情页面。
- 在限速信息区域，单击“编辑限速信息”，弹出限速调整窗口。
- 根据下表中的参数说明进行配置。

参数	说明
最大连接数(个)	表示监听协议的端口能够支持的最大并发连接数。 配置监听器最大连接数的限速信息： <ul style="list-style-type: none"> 无限速：不限制监听器可以支持最大并发连接数的数量。 限速：输入监听器可以支持最大并发连接数的最大值。
每秒查询数(QPS)	仅监听协议为HTTP/HTTPS时，支持配置该项。 QPS（Queries Per Second，每秒查询数）表示监听协议的端口每秒可以处理的查询数量。 配置监听器每秒查询数的限速信息： <ul style="list-style-type: none"> 无限速：不限制监听器每秒可以处理的查询数量。 限速：输入监听器每秒可以处理的查询数量的最大值。

参数	说明
新建连接数(CPS)	<p>CPS（Connection Per Second，新建连接数）表示监听协议的端口每秒可以新建的连接数。</p> <p>配置监听器新建连接数的限速信息：</p> <ul style="list-style-type: none"> • 无限速：不限制监听器每秒可以新建连接数的数量。 • 限速：输入监听器每秒可以新建连接数的最大值。
每秒包数(PPS)	<p>PPS（Packets Per Second，每秒包数）表示监听协议的端口每秒能够处理数据包的数量。</p> <p>配置监听器每秒包数的限速信息：</p> <ul style="list-style-type: none"> • 无限速：不限制监听器每秒可以处理数据包的数量。 • 限速：输入监听器每秒可以处理数据包数量的最大值。
带宽(Kbps)	<p>表示监听协议的端口每秒能够传输的数据量，单位为Kbps。</p> <p>配置SLB实例带宽的限速信息：</p> <ul style="list-style-type: none"> • 无限速：不限制监听器每秒能够传输的数据量。 • 限速：输入监听器每秒能够传输数据量的最大值。

(6) 单击“确定”，完成修改监听器的限速信息。

3.2.4 转发规则

3.2.4.1 添加转发规则

简介

通过配置 SLB 实例的监听转发规则，将客户端请求按照指定规则转发到指定服务器组中的一个或多个后端服务器。

限制与指导

- 仅 HTTPS 和 HTTP 监听器支持配置域名/URL 转发规则。
- 添加转发规则后，负载均衡将按以下规则转发请求：
 - 如果能匹配到监听器的转发规则，则按该转发规则将请求转发到对应的后端服务器组。
 - 如果没有匹配到任何监听器的转发规则，则按照默认监听（域名为空，URL 为“/”）的默认转发规则（转发至监听默认后端服务器组）进行转发。监听默认转发规则只能配置转发到服务器组，不能设置重定向。
 - 重定向支持同一 SLB 的 HTTP 和 HTTPS 监听间互转。
- 若要在中间动作中配置“请求报文：Header 自定义脚本”和“应答报文：Header 自定义脚本”，则需要在运维中心的“运维 > 服务器负载均衡 > SLB 全局参数 > 规格参数”页面，将“slb-action-header-scripts”参数置为 true，具体方法请咨询运维管理员。
- 若要在中间动作中配置“请求报文：Body 自定义脚本”和“应答报文：Body 自定义脚本”，则需要在运维中心的“运维 > 服务器负载均衡 > SLB 全局参数 > 规格参数”页面，将“slb-action-body-scripts”参数置为 true，具体方法请咨询运维管理员。

操作步骤

- (1) 在 SLB 实例页面，单击 SLB 实例的 ID，进入该 SLB 实例的基本信息页面。
- (2) 在左侧导航栏选择“监听器”，进入监听器页面。
- (3) 单击 HTTP/HTTPS 监听器对应操作列的“更多 > 编辑转发规则”，进入转发规则页签页面。
- (4) 单击“添加转发规则”，显示转发规则配置区域。
- (5) 根据下表中的参数说明进行配置。

参数	说明
域名	<ul style="list-style-type: none"> • 域名支持精确匹配和通配符匹配： <ul style="list-style-type: none"> ◦ 精确匹配：例如 <code>www.domain.com</code>。 ◦ 通配符匹配：输入格式必须以“.”开头或“*”结尾，例如 <code>*.domain.com</code> 或 <code>www.domain.*</code>。 • 域名长度限制为 3~64 个字符，只允许包含字母、数字和特殊字符“.”、“-”、“?”、“=”、“~”、“_”、“+”、“/”、“^”、“*”、“!”、“\$”、“&”、“ ”、“(”、“)”、“[”、“]”。 • “*”只能开头或结尾，且“*”只能出现一次。 • 若以“*”开头，则第二个字符必须为“.”。 • 不能连续出现两个“.”。
域名扩展策略	<p>该项默认关闭，配置域名后，可以选择开启域名扩展策略，并配置服务器证书或选择从监听器继承。</p> <p>当前可以通过给域名配置不同的双证书，支持 SNI（Server Name Indication）功能。</p> <p>注意：</p> <ul style="list-style-type: none"> • 如果需要域名扩展策略的证书生效，需要在 TLS 握手阶段指定 SNI 域名，否则使用的是仍然是监听器的默认证书。 • 如果需要使用不同的双证书，需要明确配置两个证书，而不能一个配置证书，另一个继承监听配置。 • 若关闭域名扩展策略，则当前域名的扩展策略配置全部丢失，不会保留，将会使用监听器的配置。
规则名称	<p>可根据需要自定义转发策略的名称。</p> <p>输入规则如下：</p> <ul style="list-style-type: none"> • 必须使用中/英文开头。 • 支持中文、英文字母、数字、下划线、中划线或点。 • 支持 1-127 位字符（1 个汉字等于 2 个字符）。
规则条件（如果条件全部匹配）	
URL	<ul style="list-style-type: none"> • URL 支持如下类型： <ul style="list-style-type: none"> ◦ 精确匹配：请求的 URL 和设定 URL 完全一致。例如，输入格式为 <code>/path1</code>，只能匹配 <code>/path1</code>。 ◦ 前缀匹配：请求的 URL 匹配已设定 URL 开头的 URL。例如，输入格式为 <code>/path1*</code>，可以匹配 <code>/path1/abc</code>。 • URL 输入规则如下： <ul style="list-style-type: none"> ◦ 必须以/开头。 ◦ 支持英文字母、数字和特殊字符。 ◦ 支持输入 1 ~ 64 个字符。

参数	说明
HTTP标头	<p>单击“添加条件”，在下拉菜单中选择“HTTP标头”，即可配置该项。</p> <ul style="list-style-type: none"> 键：输入 HTTP 标头的名称， 值：输入 HTTP 标头的内容。 <p>HTTP标头的键和值均为精确匹配，且区分大小写。</p>
COOKIE	<p>单击“添加条件”，在下拉菜单中选择“COOKIE”，即可配置该项。</p> <p>Cookie的键和值均为精确匹配，且区分大小写。输入要求如下：</p> <ul style="list-style-type: none"> 长度范围为 1~64 个字符， 不支持空格和*?。
HTTP请求方法	<p>单击“添加条件”，在下拉菜单中选择“COOKIE”，即可配置该项，可根据需要配置多个HTTP请求方法的条件。</p> <p>HTTP请求方法支持：HEAD、GET、POST、OPTIONS、PUT、PATCH、DELETE。</p>
中间动作：单击“添加中间动作”，配置中间动作信息。	
动作类型	<p>支持如下动作类型：</p> <ul style="list-style-type: none"> 请求报文：设置 Header 请求报文：删除 Header 请求报文：Header 自定义脚本 请求报文：Body 自定义脚本 应答报文：设置 Header 应答报文：删除 Header 应答报文：Header 自定义脚本 应答报文：Body 自定义脚本 请求报文：重写。具体说明请参见重写动作说明。
键/值/脚本	<p>选择动作类型后，根据页面显示，可配置对应的键、值或脚本内容。</p> <p>部分典型配置信息，请参考HTTP和HTTPS协议的监听器转发规则中间动作典型配置举例。</p>
终结动作：如果满足转发策略的条件，配置将会执行的动作。	
动作类型	<p>转发至：将请求转发至指定的后端服务器组。</p> <p>需配置如下参数：</p> <ul style="list-style-type: none"> 服务器组：在下拉列表中选择要转发到的目标服务器组。
	<p>重定向：将请求重定向至当前SLB实例下的其它HTTP或HTTPS监听器。</p> <p>需配置如下参数：</p> <ul style="list-style-type: none"> 协议：选择要重定向到的协议类型，包括 HTTP 和 HTTPS。 端口：选择要重定向到的端口。 状态码：请根据需要选择 HTTP 监听器重定向的状态，支持如下： <ul style="list-style-type: none"> 301：永久重定向，表示被请求的资源已经永久移动到新位置。 302：临时重定向，表示被请求的资源临时从不同位置响应。 307：临时重定向，307 和 302 类似，区别在于 307 不允许在重定向时改变请求的方法。

参数	说明
	<ul style="list-style-type: none"> ○ 308: 永久重定向, 表示被请求的资源已经永久移动到新位置, 308 与 301 类似, 区别在于 308 保留了原始请求的方法, 即 HTTP 请求中的请求方法和请求主体不会更改。 ● 重写: 具体说明请参见重写动作说明。 <hr/> 固定返回: 直接返回如下配置的响应内容。 需配置如下参数: <ul style="list-style-type: none"> ● 状态码: 返回的 HTTP 状态码, 可输入 100 - 599 间任意值, 允许 1XX、2XX、3XX、4XX、5XX, 其中 X 为任意数字, 比如 200、302、404、500 等。 ● 返回码: 返回的 HTTP 的 reason phrase, 是与数字状态码相关联的简短文本描述, 支持字母、数字、空格和“-”, 最大长度 32。HTTP2.0 规范应答不支持携带。 ● 返回类型: 返回固定内容的格式, 取值: text/plain、text/css、text/html、application/javascript 或 application/json。范围: 字母、数字、空格、“=”、“/”和“-”。 ● 返回内容: 返回的固定内容, 10240 个可见字符。
添加策略	单击“添加策略”, 可添加多条转发策略。
添加域名	单击“添加域名”, 可添加多个域名。

(6) 单击“确定”, 完成添加转发策略操作。

3.2.4.2 重写动作说明

简介

转发规则的中间动作“请求报文: 重写”和终结动作“重定向”均支持重写操作, 能够在负载均衡器收到报文后, 将客户端发送的域名、路径或查询进行修改:

- 中间动作“请求报文: 重写”将请求报文重写后, 转给后端服务。
- 终结动作“重定向”的重写, 直接修改请求报文后, 返还给客户端。

限制与指导

- 只有在终结动作为转发到后端服务器组的情况下, 才能配置中间动作“请求报文: 重写”。
- 每一个转发规则只支持配置一次中间动作“请求报文: 重写”。

参数说明

参数	说明
域名	默认值\${host}, 表示请求的原始域名, 可以修改为其它域名。
路径	默认值\${path}, 表示使用原值。 注意: 若删除默认值, 使用空值, 则表示删除原始请求的路径字段。
路径变量模板	可以在请求报文的路径中, 使用正则的方式提取出变量, 在重写的路径中复用这些变量。变量的提取和使用, 请参考下面的“重写正则使用说明”。 举例:

	<p>若需要将路径 “/aaa/bbb/ccd/ddd/eee/fff” 重写为 “/bbb/ccd”，则建议配置方式如下：</p> <ul style="list-style-type: none"> • 路径：/\${1}/\${2} • 路径变量模板：/aaa/(.*)/(.*)/ 或者 ^/aaa/(.*)/(.*)/ <p>若以上路径中，aaa字段是变化的，则可以使用如下配置方式：</p> <ul style="list-style-type: none"> • 路径：/\${1}/\${2} • 路径变量模板：^/.*/(.*)/(.*)/
查询	<p>默认值\${query}，表示使用原值。</p> <p>注意：若删除默认值，使用空值，则表示删除原始请求的查询字段。</p>
查询变量模板	<p>可以在请求报文的查询字段，使用正则的方式提取出变量，在重写的查询字段中复用这些变量。变量的提取和使用，请参考下面的“重写正则使用说明”。</p> <p>举例：</p> <ul style="list-style-type: none"> • 删除 <p>若需要将查询 “a=aaa&b=bbb&c=ccc&...” 重写为 “a=aaa&c=ccc&...” ，则建议配置方式如下：</p> <ul style="list-style-type: none"> ○ 查询：\${1}&\${2} ○ 查询变量模板：^(.*)&.*&(.*) <ul style="list-style-type: none"> • 修改 <p>若需要将查询 “a=aaa&b=bbb&c=ccc&...” 重写为 “a=aaa&c=ddd” ，则建议配置方式如下：</p> <ul style="list-style-type: none"> ○ 查询：\${1}&c=ddd ○ 查询变量模板：^(.*)&.*

重写正则使用说明

常用的正则	说明
^	匹配输入字符串的开始位置
\$	匹配输入字符串的结尾位置
()	标记一个子表达式的开始和结束位置
*	匹配前面的子表达式零次或多次
.	匹配除换行符 \n 之外的任何单字符
(.*)	贪婪匹配，并且提取为变量
.*	贪婪匹配，不提取为变量
(.*?)	非贪婪匹配，并且提取为变量
.?*	非贪婪匹配，不提取为变量

3.2.5 启用/停止监听器

简介

启用/停止监听器有如下方式：

- 可通过对负载均衡实例进行启动/停止操作，实现批量启动/停止该实例下的所有监听器功能，具体操作请参见[启动/停止 SLB 实例](#)。
- 可直接对指定监听器进行启动/停止操作。

本节介绍如何启用/停止指定监听器。

限制与指导

停止监听器后，流量将无法正常运转，请谨慎操作。

操作步骤

- (1) 在 SLB 实例页面，单击 SLB 实例的 ID，进入该 SLB 实例的基本信息页面。
- (2) 在左侧导航栏选择“监听器”，进入监听器页面。
- (3) 单击监听器对应操作列的“启用”或“停止”，弹出确认窗口。
- (4) 单击“确定”，可启用/停止指定监听器。

3.2.6 日志设置

简介

支持开启或关闭日志投递。

开启后，会将日志投递到日志服务 CLS，您可以在日志服务中查询、检索以下字段的日志信息。

表3-1 七层访问日志项说明

日志项	示例值	说明
upstream_header_time	0.001	SLB向其上游服务器发送请求开始，到接收到上游服务器的第一个响应头为止所花费的时间，单位：秒
body_bytes_sent	950	SLB发送到客户端的响应主体的字节数。这包括了实际的响应内容，但不包括响应头的大小。单位：字节
connection_requests	1	SLB与客户端的TCP当前连接的请求报文编号，从1开始；连接的编号，参考connection说明
ssl_cipher	TLS_AES_256_GCM_SHA384	建立SSL连接使用的套件
pid	85992	处理当前HTTP(S)报文的进程ID
http_x_forwarded_proto	HTTP	请求头中的x_forwarded_protot字段的值
time_iso8601	2024-03-28T17:15:58+08:00	记录请求发生时的准确时间，以ISO 8601格式（YYYY-MM-DDTHH:mm:ssZ）呈现
tcpinfo_rttvar	447	SLB与客户端的TCP连接中rttvar值

日志项	示例值	说明
host	172.16.0.2或者 example.com:8080	客户端在HTTP请求的Host头部字段中指定的主机名和端口号
connection	11004	TCP连接的ID
lb_id	lb-n76to1ed2g5l	SLB实例ID
content_length	22	请求头中的Content-Length字段的值
ssl_protocol	TLSv1.3	SSL协议名称
http_x_forwarded_port	-	请求头中的X-Forwarded-Port字段的值
upstream_response_length	950	SLB从上游服务器接收到的响应体的长度（以字节为单位）
upstream_bytes_sent	126	SLB发送给上游服务器的字节数
ssl_session_id	a97336a0d28c312d 752ea322b110a393 a4285501cdaae4b5 ce0f5af09c1e6079	SLB与客户端SSL握手的会话的ID
http_user_agent_256	curl/7.77.0	客户端在HTTP请求的user-agent header值，限长256字节
server_addr	172.16.0.2	SLB服务接收客户端请求的IP地址
upstream_connect_time	0.000	SLB与上游服务器建立连接消耗的时间；如果连接复用，时间可能为0；包括SSL的握手时间，单位秒
uri_256	/	客户端发送的请求的uri值，限长256字节
request_length	74	客户端请求行的长度（包括请求方法和URL，但不包括HTTP协议版本和后续的请求头部），以字节为单位。
ssl_session_reused	-	当前的SSL/TLS会话是否被重用，变量的值为1，则表示当前的SSL/TLS会话是从缓存中重用的。这意味着SSL/TLS握手过程被跳过了，从而减少了计算开销和延迟。如果值为0，则表示当前会话不是重用的，即进行了一个完整的SSL/TLS握手。
server_port	80	SLB接收客户端请求的端口号
limit_conn_status	PASSED	标识当前连接是否被限速 取值：PASSED、REJECTED或 REJECTED_DRY_RUN
status	200	SLB返回客户端的HTTP应答报文的状态码
server_protocol	HTTP/1.1	客户端请求SLB的协议，通常为：HTTP/1.0、 HTTP/1.1或HTTP/2.0
scheme	http	客户端请求SLB的协议的Scheme，通常为：“http” or “https”
upstream_addr	172.16.0.8:80	SLB转发后端的服务地址
request_method	GET	客户端请求SLB的HTTP的方法
upstream_status	200	后端服务返回SLB的HTTP的状态码

日志项	示例值	说明
upstream_bytes_received	1156	SLB从上游服务器获取的字节数
request_time	0.001	SLB处理请求所花费的总时间，从收到第一个请求报文开始，到发送完响应数据的时间，包括接收请求、处理请求和发送响应的所有阶段，不包括断开连接时间；以秒为单位。一般跟upstream_response_time 配合使用评估前后端时长
tcpinfo_rcv_space	14600	SLB与客户端的TCP连接中rcv_space值
http_x_forwarded_client_port	-	客户端在HTTP请求的x-forwarded-client-port值
tcpinfo_rtt	895	SLB与客户端的TCP连接中RTT值
limit_req_status	PASSED	标识当前连接是否被限速 取值：PASSED、DELAYED、REJECTED、DELAYED_DRY_RUN或REJECTED_DRY_RUN
slb_rule_id	rule-v15961gyomw2	当前请求命中的SLB转发规则ID
remote_addr	172.16.0.7	客户端IP
ssl_client_verify	-	客户端验证结果，取值：SUCCESS、FAILED:reason或NONE
remote_port	23060	客户端端口
pool_id	rsp-jbwnx711hl44	后端服务组ID
bytes_sent	1145	SLB发送到客户端的字节数
ls_id	ls-regllix4t5pd	SLB监听器ID
http_x_forwarded_for	-	请求头中的X-Forwarded-For字段的值
slb_log_type	http_access	当前不同的监听器产生的访问日志类型： <ul style="list-style-type: none"> http_access：七层访问日志包括 HTTP、HTTPS 监听 stream_access：四层访问日志包括 TCP、UDP、TCPSSL 监听
upstream_response_time	0.001	从SLB向后端建立连接开始到接受完数据然后关闭连接为止的时间。
tcpinfo_snd_cwnd	10	SLB与客户端的TCP连接中snd_cwnd值
request_id	dd7d7f2025b33e1040b523e1895f4329	HTTP请求的唯一随机编号
ssl_server_name	www.example.com	SNI请求中包含的Server Name
upstream_header_time	0.010	SLB接收上游服务器的Header时间，包括upstream_connect_time，单位秒

表3-2 四层访问日志项说明

日志项	示例值	说明
upstream_addr	172.16.0.8:80	SLB转发后端的服务地址

日志项	示例值	说明
bytes_received	79	SLB从客户端收取的字节数
ssl_cipher	TLS_AES_256_GCM_SHA384	建立SSL连接使用的套件
upstream_first_byte_time	0.002	从后端获取第一个字节使用的时间，单位秒
pid	84497	处理当前流的进程ID
session_time	0.003	当前流持续时间，单位秒
time_iso8601	2024-03-28T16:21:26+08:00	记录访问发生时的准确时间，以ISO 8601格式（YYYY-MM-DDTHH:mm:ssZ）呈现
upstream_bytes_received	1104	SLB从上游服务器读取的字节数
protocol	TCP	SLB与客户端的流类型，取值：TCP或者UDP
connection	10552	连接的ID
lb_id	lb-n76to1ed2g5l	SLB实例ID
ssl_protocol	TLSv1.3	SSL协议名称
remote_addr	172.16.0.7	客户端IP
ssl_client_verify	-	客户端验证结果，取值：SUCCESS、FAILED:reason或NONE
upstream_bytes_sent	79	SLB发送给上游服务器的字节数
remote_port	17362	客户端端口
ssl_session_id	a97336a0d28c312d752ea322b110a393a4285501cdaae4b5ce0f5af09c1e6079	SLB与客户端SSL握手的会话的ID
pool_id	rsp-o10lv8xnx5z	后端服务组ID
server_addr	172.16.0.2	SLB服务接收客户端请求的IP地址
bytes_sent	1104	SLB发送到客户端的字节数
upstream_session_time	0.003	SLB与上游服务器建立的连接的时间
upstream_connect_time	0.001	SLB与上游服务器建立连接的时间，包括SSL的握手时间，单位秒
ls_id	ls-0yxlc14h5gtv	监听器ID
ssl_session_reused	0	当前的SSL/TLS会话是否被重用，变量的值为1，则表示当前的SSL/TLS会话是从缓存中重用的。这意味着SSL/TLS握手过程被跳过了，从而减少了计算开销和延迟。如果值为0，则表示当前会话不是重用的，即进行了一个完整的SSL/TLS握手。
slb_log_type	stream_access	当前不同的监听器产生的访问日志类型： <ul style="list-style-type: none"> http_access: 七层访问日志包括 HTTP、HTTPS 监听 stream_access: 四层访问日志包括 TCP、UDP、TCPSSL 监听

日志项	示例值	说明
server_port	8080	SLB接收客户端请求的端口号
limit_conn_status	PASSED	标识当前连接是否被限速 取值：PASSED、REJECTED或REJECTED_DRY_RUN
ssl_server_name	www.example.com	SNI请求中包含的Server Name

前提条件

- 在运维中心的“运维 > 网络 > 服务器负载均衡 SLB > SLB 设备”页面，已完成一键部署日志操作，具体操作方法可联系运维管理员。
- 若要开启日志投递，则请先开通日志服务 CLS，并创建日志集和日志主题。

操作步骤

- 在 SLB 实例页面，单击 SLB 实例的 ID，进入该 SLB 实例的基本信息页面。
- 在左侧导航栏选择“监听器”，进入监听器页面。
- 单击监听器对应操作列的“更多 > 日志设置”，弹出日志设置窗口。
- 根据下表中的参数说明进行配置。

参数	说明
开启日志投递	选择是否开启日志投递。
日志集	开启日志投递时，需配置该项。 选择要投递到的日志集。
日志主题	开启日志投递时，需配置该项。 选择要投递到的日志主题。

- 单击“确定”，完成日志设置操作。

3.2.7 删除监听器

- 在 SLB 实例页面，单击 SLB 实例的 ID，进入该 SLB 实例的基本信息页面。
- 在左侧导航栏选择“监听器”，进入监听器页面。
- 单击监听器对应操作列的“删除”，弹出确认窗口。
- 确认要删除的监听器信息无误后，单击“确定”，完成删除监听器操作。

3.3 服务器组

3.3.1 服务器组概述

服务器组是一个或多个后端服务器的逻辑集合，用于将客户端的请求转发到一个或多个后端服务器，满足用户同时处理海量并发业务的需求。后端服务器可以是云服务器 ECS 实例或 IP 地址。

来自客户端的请求先传入 SLB 实例，再经由 SLB 实例上的监听器转发到服务器组。服务器组中健康检查正常的后端服务器会处理转发的业务请求，最终实现对用户的海量并发业务进行处理，从而提升用户应用系统的可用性。

3.3.2 创建服务器组

简介

在使用负载均衡 SLB 服务前，您必须创建服务器组并至少添加一台后端服务器来接收 SLB 转发的客户端请求。

限制与指导

- 若要创建后端协议为“HTTPS”类型的服务器组或要配置服务器组进行 HTTPS 协议的健康检查，则需要先在运维中心的“运维 > 网络 > 服务器负载均衡 SLB > SLB 全局参数”页面，将参数 `slb_pool_type_https` 的配置信息置为“true”，具体操作方法可联系运维管理员。
- 若 SLB 实例启用了国密，则无法选择 HTTPS 协议。

操作步骤

- 在 SLB 实例页面，单击左侧导航栏的“SLB 服务器组”，进入 SLB 服务器组页面。
- 单击“新建服务器组”，进入新建服务器组页面。
- 根据下表中的参数说明进行配置。

参数	说明
租户	仅租户管理员需配置该项。 选择服务器组所属的租户。
部门	选择服务器组所属的部门。
资源集	选择服务器组所属的资源集。
名称	服务器组的名称，可根据需要自定义名称或使用系统缺省名称。
专有网络	选择服务器组所属的专有网络。 您可以选择使用已有的专有网络，或者单击“新建VPC”创建新的专有网络。
后端协议	选择后端服务器自身提供的网络服务的协议。 支持选择的协议有：TCP、UDP、HTTP、HTTPS。 后端服务器组的后端协议必须与监听器的前端协议保持一致，但HTTP和HTTPS监听器除外，HTTP和HTTPS监听器对应的后端协议为HTTP或HTTPS均可。
ProxyProtocol	后端协议选择“TCP”或“UDP”时，支持配置该项。 选择是否通过ProxyProtocol协议携带客户端源地址到后端服务器，支持V1和V2两种ProxyProtocol版本。
服务器组类型	选择服务器组的类型，支持 <ul style="list-style-type: none"> ECS 服务器组：支持添加与 SLB 实例同 VPC 的云服务器实例（云服务器和裸金属服务器）作为后端服务器。 IP 服务器组：开启“跨 VPC 访问”功能后，支持添加与 SLB 实例所属 VPC 以外的 IP 地址作为后端服务器。

参数	说明
IP地址类型	选择服务器支持的IP版本，包含IPv4和IPv6。 服务器组创建后，将不支持修改IP地址类型。
分配策略类型	选择负载均衡采用的算法。 <ul style="list-style-type: none"> • 加权轮询算法：SLB 实例按照后端服务器的权重，从高到低以轮询的方式将请求分发给各服务器，相同权重的服务器处理相同数目的连接数。当后端服务器的权重都设置为同一个值时，权重属性不生效，将按照简单的轮询策略。 • 加权最少连接数算法：最少连接是通过当前活跃的连接数来估计服务器负载情况的一种动态调度算法。加权最少连接数是在最少连接数的基础上，根据服务器的处理能力差异，给每个服务器分配不同的权重，使其能够接受相应权值数的服务请求。 • 源 IP 算法：将请求的源 IP 地址进行一致性 Hash 运算，得到一个具体的数值，同时对后端服务器进行编号，按照运算结果将请求分发到对应编号的服务器上。本算法可以实现对不同源 IP 的访问进行负载分发，同时保证同一个客户端 IP 的请求始终被派发至某特定的服务器。 • 随机算法：将请求随机分配给后端服务器，权重越高的后端服务器会被分配更多的访问请求。 • 源 IP 端口算法：仅后端协议选择“TCP”或“UDP”时支持该算法。将请求的源 IP 地址和端口进行一致性 Hash 算法，得到一个具体的数值，同时对后端服务器进行标号，按照运算结果将请求分发到对应标号的服务器上。本算法可以实现对不同源 IP 端口的访问进行负载分发，同时保证源 IP 和端口相同的请求会分配给相同的服务器。与源 IP 算法相比，本算法可能将相同源 IP 地址不同端口的请求分发到不同的后端服务器中。
会话保持	仅后端协议选择“HTTP”或“HTTPS”时，可配置会话保持功能。 <ul style="list-style-type: none"> • 是：开启会话保持功能，SLB 实例可以识别客户端与服务器之间交互过程的关联性，将属于同一个会话的请求都转发到同一个服务器进行处理。 • 否：不开启会话保持功能。 当后端协议选择“TCP”或“UDP”且分配策略选择“源IP算法”时，会话保持显示为“是”，表示支持会话保持功能，但无法在此配置。
会话保持类型	若会话保持选择“是”，则需要选择会话保持类型。 <ul style="list-style-type: none"> • 应用 cookie：该选项依赖于后端应用。后端应用生成一个 cookie 值，后续所有包含这个 cookie 值的请求都会由同一个后端服务器处理。 • 负载均衡 cookie：SLB 实例会根据客户端第一个请求生成一个 cookie，后续所有包含这个 cookie 值的请求都会由同一个后端服务器处理。
cookie名称	若会话保持类型选择“应用cookie”，则需要配置cookie名称。 cookie名称必须以字母或中文开头，可以包含字母、数字、下划线（_）、中划线（-）、点(.)，最多输入127个字符（1个汉字等于2个字符）。
会话保持时间（分钟）	若会话保持类型选择“负载均衡cookie”，则需要配置会话保持时间。 当超过会话保持时间，连接内无新的请求时，将会自动断开会话保持。可配置范围为1-50分钟。
健康检查配置	选择是否开启健康检查配置，SLB实例通过健康检查来判断后端服务器是否可用。 <ul style="list-style-type: none"> • 开启：开启健康检查，SLB 实例如果判断后端服务器健康检查异常，就不会将流量分发到异常后端服务器，而是分发到健康检查正常的后端服务器，从而提高业务的可靠性。当异常的后端服务器恢复正常运行后，SLB 实例会将其自动恢复到负载均衡服务中，承载业务流量。具体参数说明，请参见开启 TCP/HTTP/HTTPS 健康检查。

参数	说明
	<ul style="list-style-type: none"> 不开启：关闭健康检查，SLB 实例将向所有后端服务器转发流量，可能会导致业务请求转发至异常的后端服务器。
描述	可根据需要输入描述信息，最多255个字符。

(4) 单击“新建”，完成创建服务器组操作。

3.3.3 查看服务器组详情

简介

创建服务器组完成后，您可以查看服务器组详情信息，包含基本信息、服务器列表、关联监听器和健康检查信息。

操作步骤

- (1) 在 SLB 实例页面，单击左侧导航栏的“SLB 服务器组”，进入 SLB 服务器组页面。
- (2) 单击服务器组 ID，进入服务器组详情页面，可查看服务器组的信息如下表：

区域名称	说明
基本信息	服务器组的基本信息，包括服务器组的名称、ID、类型等。
服务器列表	服务器组中已添加的后端服务器信息，相关信息可参考 后端服务器 。
关联监听器	服务器组关联的监听器信息，相关信息可参考 监听器 。
健康检查	服务器组的健康检查信息。若未开启，则可通过单击“立即开启”，配置健康检查信息，具体说明请参见 开启TCP/HTTP/HTTPS健康检查 。

3.3.4 后端服务器

3.3.4.1 后端服务器概述

来自客户端的请求首先传入 SLB 实例，再经由 SLB 实例上的监听器转发给服务器组中的后端服务器进行处理，满足用户同时处理海量并发业务的需求。

后端服务器类型

支持添加的后端服务器类型及说明请见下表。

后端服务器类型	说明	操作指导
ECS服务器	支持添加与SLB实例同VPC的ECS云服务器实例作为后端服务器。	添加ECS服务器类型的后端服务器
IP服务器	SLB实例开启“跨VPC访问”功能后，支持添加其他VPC中的IP地址作为后端服务器。	添加IP服务器类型的后端服务器

主备服务器

后端服务器支持主服务器和备服务器角色，主备服务器使用原则如下：

- 只有在分配策略是“加权轮询算法”或者“最小连接数算法”时，才支持配置主备服务器。
- 相同的服务（IP+业务端口）不能同时作为主或备服务器。
- 当主服务器全部健康检查失败时，才会切换到备服务器；当有一个主服务器健康检查成功，新建连接流量会全部切换到主服务器，存量连接流量仍然运行在备服务器。
- 当主备服务器切换时，Cookie 的会话保持不会失效，仍然会保持到原有的服务器。
- 当服务器组的服务器全部为备服务器时，效果等同于主服务器全部失效，SLB 系统会将流量引入备服务器。

3.3.4.2 添加后端服务器

1. 添加 ECS 服务器类型的后端服务器

简介

创建 ECS 服务器类型的服务器组之后，您需要为其添加云服务器 ECS 实例作为后端服务器来处理转发请求。

前提条件

- 已创建 ECS 服务器类型的服务器组。
- 已创建云服务器 ECS 实例，且其状态为“运行中”。

限制与指导

仅当服务器组的分配策略类型为“加权轮询算法”或“加权最少连接数”时，才支持配置主备服务器。

操作步骤

- (1) 在 SLB 实例页面，单击左侧导航栏的“SLB 服务器组”，进入 SLB 服务器组页面。
- (2) 单击类型为“ECS”的服务器组 ID，进入服务器组详情页面。
- (3) 在服务器列表页签，单击“添加服务器”，弹出添加服务器窗口。
- (4) 在选择服务器页面，选择一个或多个云服务器后，单击“下一步”。
- (5) 在修改参数页面，批量或单个配置后端服务器的参数：
 - 业务端口：后端服务器处理访问请求的端口，范围为 1~65535。
 - 权重：后端服务器的权重值，范围为 0~100。权重越高的云服务器将被分配到更多的访问请求，新的请求不会转发到权重为 0 的后端服务器上。
 - 角色：选择后端服务器为主服务器或备服务器。
- (6) 单击“确定”，页面显示添加结果。
- (7) 单击“关闭”，关闭添加服务器窗口。

2. 添加 IP 服务器类型的后端服务器

简介

创建 IP 类型的服务器组之后，您需要为其添加 IP 地址作为后端服务器来处理转发请求。

前提条件

- 已创建 IP 服务器组类型的服务器组。
- 创建 SLB 实例时，启用“跨 VPC 访问”功能。

限制与指导

不支持添加 SLB 或 BLB 的私网 IP 作为后端服务器。

操作步骤

- (1) 在 SLB 实例页面，单击左侧导航栏的“SLB 服务器组”，进入 SLB 服务器组页面。
- (2) 单击类型为“IP”的服务器组 ID，进入服务器组详情页面。
- (3) 在服务器列表页签，单击“添加 IP 服务器”，弹出添加 IP 服务器窗口。
- (4) 根据下表中的参数说明进行配置。

参数	说明
IP地址	输入要添加服务器的IP地址。
业务端口	输入后端服务器处理访问请求的端口，范围为1~65535。
权重	输入后端服务器的权重值，范围为0~100，权重越高的云服务器将被分配到更多的访问请求，新的请求不会转发到权重为0的后端服务器上。
角色	选择后端服务器为主服务器或备服务器。
描述	可根据需要输入描述信息，最多255个字符。
操作	<ul style="list-style-type: none">• 复制：基于当前行信息，新建一行 IP 服务器信息。• 删除：移除当前行的 IP 服务器信息。
继续添加	添加一个空白行，手动输入IP服务器信息。

- (5) 单击“确定”，完成添加 IP 服务器操作。

3.3.4.3 修改后端服务器

1. 简介

您可根据需要修改后端 ECS 或 IP 服务器的权重和端口号，IP 服务器还支持修改描述信息。支持单个或批量修改后端服务器两种方式。

2. 修改指定后端服务器

- (1) 在 SLB 实例页面，单击左侧导航栏的“SLB 服务器组”，进入 SLB 服务器组页面。
- (2) 单击服务器组 ID，进入服务器组详情页面。

- (3) 在服务器列表页签，单击服务器对应操作列的“编辑”，弹出编辑服务器窗口。
- (4) 根据下表中的参数说明进行修改。

参数	说明
权重	修改后端服务器的权重值，范围为0~100，权重越高的云服务器将被分配到更多的访问请求，新的请求不会转发到权重为0的后端服务器上。
业务端口	修改后端服务器处理访问请求的端口，范围为1~65535。
角色	修改后端服务器的角色，包括主服务器、备服务器。
描述	仅IP服务器可修改该项。 可根据需要修改描述信息，最多255个字符。

- (5) 单击“确定”，完成修改后端服务器操作。

3. 批量修改后端服务器

- (1) 在 SLB 实例页面，单击左侧导航栏的“SLB 服务器组”，进入 SLB 服务器组页面。
- (2) 单击服务器组 ID，进入服务器组详情页面。
- (3) 在服务器列表页签，选择一个或多个服务器后，单击“批量修改”，弹出批量修改服务器窗口。
- (4) 根据下表中的参数说明进行修改。

参数	说明
业务端口	修改后端服务器处理访问请求的端口，范围为1~65535。 可通过“向上复制”或“向下复制”功能进行快速修改。
权重	修改后端服务器的权重值，范围为0~100，权重越高的云服务器将被分配到更多的访问请求，新的请求不会转发到权重为0的后端服务器上。 可通过“向上复制”或“向下复制”功能进行快速修改。
角色	修改后端服务器的角色，包括主服务器、备服务器。
描述	仅IP服务器可修改该项。 可根据需要修改描述信息，最多255个字符。

- (5) 单击“确定”，完成修改后端服务器操作。

3.3.4.4 移除后端服务器

简介

您可以根据需要移除服务器组中的后端服务器，移除后该后端服务器将不再处理来自客户端的请求。

限制与指导

直接在服务器组中移除后端服务器，可能会造成业务中断，建议您先修改后端服务器的权重为 0，然后再从服务器组中移除该后端服务器。

操作步骤

- (1) 在 SLB 实例页面，单击左侧导航栏的“SLB 服务器组”，进入 SLB 服务器组页面。
- (2) 单击服务器组 ID，进入服务器组详情页面。
- (3) 在服务器列表页签，单击后端服务器对应操作列的“删除”，弹出删除服务器窗口。
- (4) 确认要删除的后端服务器信息无误后，单击“确定”，完成移除后端服务器操作。

3.3.5 健康检查

3.3.5.1 健康检查概述

负载均衡通过健康检查来判断后端服务器（ECS 服务器和 IP 服务器）的业务可用性，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，SLB 实例会对所有后端服务器进行健康检查。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。

- 当某台后端服务器被判定为异常后，SLB 实例会自动将新的请求转发给其他正常的后端服务器。
- 当异常后端服务器恢复正常后，SLB 实例会将其恢复至负载均衡服务中，重新转发请求给此服务器。

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。

如果您的业务对负载敏感性高，高频率的健康检查探测可能会对正常业务访问造成影响。您可以结合业务情况，通过降低健康检查频率、增大健康检查间隔、七层检查修改为四层检查等方式，来降低对业务的影响。但为了保障业务的持续可用，不建议关闭健康检查。

3.3.5.2 配置健康检查

1. 开启 TCP/HTTP/HTTPS 健康检查

简介

健康检查可以在创建服务器组的配置中进行，也可以在服务器组详情页面进行配置。

开启健康检查后，当后端服务器状态异常时，不会将流量分发到该服务器；当其恢复正常状态时，会重新将流量分发到该服务器。

本节介绍如何在服务器组详情页配置 TCP/HTTP/HTTPS 健康检查。

前提条件

服务器组未开启健康检查，且服务器的后端协议为 TCP 或 HTTP 或 HTTPS。

限制与指导

若要配置 HTTPS 协议的健康检查，则需要先在运维中心的“运维 > 网络 > 服务器负载均衡 SLB > SLB 全局参数”页面，将参数 `slb_pool_type_https` 的配置信息置为“true”，具体操作方法可联系运维管理员。

操作步骤

- (1) 在 SLB 实例页面，单击左侧导航栏的“SLB 服务器组”，进入 SLB 服务器组页面。
- (2) 单击服务器组 ID，进入服务器组详情页面。
- (3) 在健康检查页签，单击“立即开启”，弹出开启健康检查窗口。
- (4) 根据下表中的参数说明进行配置：

参数	说明
协议：健康检查协议类型，选择“TCP”时，需配置以下参数。	
健康检查端口	健康检查服务访问后端服务器时的探测端口。若未配置健康检查端口，则默认使用业务端口作为健康检查端口。
检查间隔(秒)	每隔该间隔时间进行一次健康检查。
超时时间(秒)	每次健康检查响应的最大超时时间。若超时时间大于检查间隔，则实际生效的超时时间与检查间隔的时间相同。
健康阈值(次)	如果连续N次（N即为健康阈值）健康检查结果均为健康，则识别状态为健康。
不健康阈值(次)	如果连续N次（N即为不健康阈值）健康检查结果均为健康，则识别状态为不健康。
TCP结束方式	选择负载均衡器健康检查使用的短连接的结束方式，支持如下： <ul style="list-style-type: none">● RST 快速结束：通过发送 RST 结束 TCP 连接，能够快速回收 TCP 资源，有利于减少后端服务的连接压力。● FIN 结束：为正常 TCP 结束方式，有利于复杂场景 TCP 结束。
健康检查请求/健康检查应答	健康检查请求和健康检查应答必须同时配置，或者都不配置。 长度为1-64字符，支持：字母、数字、空格、“^”、“\$”、“.”、“{”、“}”。 支持以下4种场景的检查类型： <ul style="list-style-type: none">● 以 xxx 开头：“^abc def”● 以 xxx 结尾：“abc def\$”● 完全匹配：“^abc def\$”● 从第 10 个字符开始匹配：“^.{9}abc” 在健康检查请求中输入请求的内容（例如AccountID），在健康检查应答（可根据需要选择是否区分大小写）中输入预期的返回结果（例如SLB123）。同时在后端服务器的应用逻辑中加入相应的健康检查应答逻辑，如收到AccountID的请求时，回应SLB123。 此时，当负载均衡收到后端服务器发来的正确响应时，则认为健康检查成功，否则认为健康检查失败。此方式能最大程度确保健康检查的可靠性。
协议：健康检查协议类型，选择“HTTP”时，需配置以下参数。	
健康检查端口	健康检查服务访问后端服务器时的探测端口。若未配置健康检查端口，则默认使用业务端口作为健康检查端口。
检查间隔(秒)	每隔该间隔时间进行一次健康检查。

参数	说明
超时时间(秒)	每次健康检查响应的最大超时时间。若超时时间大于检查间隔，则实际生效的超时时间与检查间隔的时间相同。
健康阈值(次)	如果连续N次（N即为健康阈值）健康检查结果均为健康，则识别状态为健康。
不健康阈值(次)	如果连续N次（N即为不健康阈值）健康检查结果均为健康，则识别状态为不健康。
健康检查方法	健康检查的HTTP请求方式，支持HEAD、GET、POST、PUT方法，默认采用HEAD方法。 如果您的后端服务器不支持HEAD方法或HEAD方法被禁用，则可能会出现健康检查失败的情况，此时可以使用GET方法来进行健康检查。
健康检查版本	选择健康检查的版本，支持HTTP 1.0和HTTP 1.1。 <ul style="list-style-type: none"> HTTP 1.0: 无需校验请求的 Host 字段，即无需配置检查域名。 HTTP 1.1: 需要校验请求的 Host 字段，即需要配置检查域名。
健康检查路径	指定健康检查的URL地址的路径，必须以/开头，且只能使用字母、数字、'_'、'-'、'/'、'!'、'%','?','#','&','='这些字符，长度范围为1~80个字符。
健康检查域名	可根据需要配置健康检查的请求域名。 若未配置健康检查域名，则健康检查HTTP版本为1.0时不发送Host Header，健康检查HTTP版本为1.1时，Host Header为健康检查的服务器IP。
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_2xx、http_3xx、http_4xx和http_5xx。
TCP结束方式	选择负载均衡器健康检查使用的短连接的结束方式，支持如下： <ul style="list-style-type: none"> RST 快速结束：通过发送 RST 结束 TCP 连接，能够快速回收 TCP 资源，有利于减少后端服务的连接压力。 FIN 结束：为正常 TCP 结束方式，有利于复杂场景 TCP 结束。
HTTP Body请求/HTTP Body检查	健康检查方法选择GET、POST或PUT时，可配置该项。长度为1-64字符，支持：字母、数字、空格、“^”、“\$”、“.”、“{”、“}”。“ 支持以下4种场景的检查类型，例如： <ul style="list-style-type: none"> 以 xxx 开头：“^abc def” 以 xxx 结尾：“abc def\$” 完全匹配：“^abc def\$” 从第 10 个字符开始匹配：“^{9}abc” 在HTTP Body请求中输入请求的内容（例如“Hello”），在HTTP Body检查中输入预期的返回结果（例如abc）。同时在后端服务器的应用逻辑中加入相应的健康检查应答逻辑，如收到Hello的请求时，回应“abc”。 此时，当负载均衡收到后端服务器发来的正确响应时，则认为健康检查成功，否则认为健康检查失败。此方式能最大程度确保健康检查的可靠性。

(5) 单击“确定”，完成配置健康检查。

2. 开启 UDP 健康检查

简介

健康检查可以在创建服务器组的配置中进行，也可以在服务器组详情页面进行配置。

开启健康检查后，当后端服务器状态异常时，不会将流量分发到该服务器；当其恢复正常状态时，会重新将流量分发到该服务器。

本节介绍如何在服务器组详情页配置 UDP 健康检查。

前提条件

服务器组未开启健康检查，且服务器的后端协议为 UDP。

操作步骤

- (1) 在 SLB 实例页面，单击左侧导航栏的“SLB 服务器组”，进入 SLB 服务器组页面。
- (2) 单击服务器组 ID，进入服务器组详情页面。
- (3) 在健康检查页签，单击“立即开启”，弹出开启健康检查窗口。
- (4) 根据下表中的参数说明进行配置：

参数	说明
协议	健康检查协议类型，此处选择“UDP”。
健康检查端口	健康检查服务访问后端服务器时的探测端口。若未配置健康检查端口，则默认使用业务端口作为健康检查端口。
检查间隔(秒)	每隔该间隔时间进行一次健康检查。
超时时间(秒)	每次健康检查响应的最大超时时间。若超时时间大于检查间隔，则实际生效的超时时间与检查间隔的时间相同。
健康阈值(次)	如果连续N次（N即为健康阈值）健康检查结果均为健康，则识别状态为健康。
不健康阈值(次)	如果连续N次（N即为不健康阈值）健康检查结果均为健康，则识别状态为不健康。
健康检查请求/健康检查应答	<p>长度为1-64字符，支持：字母、数字、空格、“^”、“\$”、“.”、“{”、“}”。</p> <p>支持以下4种场景的检查类型：</p> <ul style="list-style-type: none"> • 以 xxx 开头：“^abc def” • 以 xxx 结尾：“abc def\$” • 完全匹配：“^abc def\$” • 从第 10 个字符开始匹配：“^{9}abc” <p>在健康检查请求中输入请求的内容（例如AccountID），在健康检查应答（可根据需要选择是否区分大小写）中输入预期的返回结果（例如SLB123）。同时在后端服务器的应用逻辑中加入相应的健康检查应答逻辑，如收到AccountID的请求时，回应SLB123。</p> <p>此时，当负载均衡收到后端服务器发来的正确响应时，则认为健康检查成功，否则认为健康检查失败。此方式能最大程度确保健康检查的可靠性。</p> <ul style="list-style-type: none"> • 如果没有配置健康检查请求，将会使用默认值进行健康检查。 • 如果要配置健康检查应答，则必须同时配置健康检查请求，健康检查会进行UDP报文的健康检查。 • 如果不配置健康检查应答，则健康检查将会发送ICMP报文探测，探测成功后，再使用UDP发送默认报文进行健康检查，ICMP和UDP两种探测方式，任何一种失败都会认为健康检查失败。

- (5) 单击“确定”，完成配置健康检查。

3. 关闭健康检查

简介

关闭健康检查后，当后端服务器出现异常时，SLB 还是会把请求转发到异常的服务器上，造成部分业务不可访问，所以建议一般情况下不要关闭健康检查。

前提条件

服务器组已开启健康检查。

操作步骤

- (1) 在 SLB 实例页面，单击左侧导航栏的“SLB 服务器组”，进入 SLB 服务器组页面。
- (2) 单击服务器组对应操作列的“编辑”，进入编辑服务器组页面。
- (3) 在健康检查配置区域，选择“不开启”。
- (4) 单击“确定”，完成关闭健康检查操作。

3.3.6 删除服务器组

简介

您可以根据需要移除服务器组。

限制与指导

- 删除后端服务器组前，请先移除已添加的后端服务器。
- 删除后端服务器组前，请先解除服务器组和监听器的关联。

操作步骤

- (1) 在 SLB 实例页面，单击左侧导航栏的“SLB 服务器组”，进入 SLB 服务器组页面。
- (2) 单击服务器组对应操作列的“删除”，弹出删除服务器组窗口。
- (3) 确认要删除的服务器组信息无误后，单击“确定”，完成删除服务器组操作。

3.4 证书管理

3.4.1 证书概述

负载均衡支持如下类型的证书：

- 服务器证书：在使用 HTTPS 协议时，服务器证书用于 SSL 握手协商，需提供证书内容和私钥。
- CA 证书：又称客户端 CA 公钥证书，用于验证客户端证书的签发者。在开启 HTTPS 双向认证功能时，只有当客户端能够出具指定 CA 签发的证书时，HTTPS 连接才能成功。
- 国密加密：在密钥协商时使用，证书的公钥用于加密，私钥用于解密。
- 国密签名：在签名时使用，证书的私钥用于签名，公钥用于验签。

配置 HTTPS 协议或 TCPSSL 协议监听器时，需要为监听器绑定服务器证书，如果开启双向认证功能，还需要绑定 CA 证书。

如果 SLB 实例开启了国密，则在为该 SLB 实例创建 HTTPS 协议或 TCPSSL 协议监听器时，还需要绑定国密签名和国密加密证书。

3.4.2 创建证书

简介

为了支持 HTTPS 数据传输加密认证，在创建 HTTPS 协议或 TCPSSL 协议监听器时，需要为监听器绑定服务器证书，如果开启双向认证功能，还需要绑定 CA 证书。

如果 SLB 实例开启了国密，则在为该 SLB 实例创建 HTTPS 协议或 TCPSSL 协议监听器时，需要绑定国密签名和国密加密证书。

本节介绍如何创建证书。

操作步骤

- (1) 在 SLB 实例页面，单击左侧导航栏的“SLB 证书管理”，进入 SLB 证书管理页面。
- (2) 单击“新建证书”，弹出新建证书窗口。
- (3) 根据下表中的参数说明进行配置。

参数	说明
租户	仅租户管理员需配置该项。 选择证书所属的租户。
部门	选择证书所属的部门。
资源集	选择证书所属的资源集。
证书名称	证书的名称，可根据需要自定义名称或使用系统缺省名称。
证书类型	选择要创建证书的类型，支持如下： <ul style="list-style-type: none">服务器证书：使用 HTTPS 协议时，服务器证书用于 SSL 握手协商，需提供证书内容和私钥。CA 证书：又称客户端 CA 公钥证书，用于验证客户端证书的签发者。在 HTTPS 双向认证中，只有当客户端能够出具指定 CA 签发的证书时，HTTPS 连接才能成功。国密加密证书：在密钥协商时使用，证书的公钥用于加密，私钥用于解密。国密签名证书：在签名时使用，证书的私钥用于签名，公钥用于验签。
证书内容	<ul style="list-style-type: none">证书包含证书的公钥和签名等信息，证书扩展名为“.pem”或“.crt”，支持直接输入证书内容或上传证书文件。证书内容的格式：以“-----BEGIN CERTIFICATE-----”作为开头，“-----END CERTIFICATE-----”作为结尾，每行 64 个字符，且最后一行不能超过 64 字符，不能有空行。
私钥	证书类型选择“服务器证书”、“国密加密”或“国密签名”时，需要配置私钥。 <ul style="list-style-type: none">证书私钥的扩展名为“.key”，支持直接输入私钥文件内容或上传符合格式的私钥文件。服务器证书的私钥内容的格式：以“-----BEGIN RSA PRIVATE KEY-----”作为开头，“-----END RSA PRIVATE KEY-----”作为结尾。

参数	说明
	<ul style="list-style-type: none"> 国密加密证书/国密签名证书的私钥内容的格式：以“----- BEGIN PRIVATE KEY-----”作为开头，“----- END PRIVATE KEY-----”作为结尾。
域名	证书类型选择“服务器证书”时，可选择配置域名。 如果该证书用于SNI（Server Name Indication，服务器名称指示），则需要指定域名，每个证书只能指定一个域名。 域名的输入要求如下： <ul style="list-style-type: none"> 域名只能由字母、数字、中划线组成，且中划线不能在开头或末尾，单个字符串不超过 63 个字符，字符串间以点分隔。 最多支持 30 个域名，域名间用逗号分隔。 单个域名长度不能超过 100 个字符，且域名总长度不能超过 1024 个字符。
描述	可根据需要输入描述信息，最多255个字符。

(4) 单击“确定”，完成创建证书操作。

3.4.3 删除证书

简介

当您不再需要使用某个证书时，可以删除该证书。

限制与指导

仅当证书未关联监听器时，才可以执行删除操作。

操作步骤

- (1) 在 SLB 实例页面，单击左侧导航栏的“SLB 证书管理”，进入 SLB 证书管理页面。
- (2) 单击证书对应操作列的“删除”，弹出删除证书窗口。
- (3) 确认要删除的证书信息无误后，单击“确定”，完成删除证书操作。

3.5 访问控制

3.5.1 访问控制概述

负载均衡提供监听级别的访问控制，您可以针对不同的监听设置访问白名单或黑名单：

- 白名单：**仅转发来自所选访问控制组中设置的 IP 地址或地址段的请求，适用于应用只允许特定 IP 访问的场景。
 设置白名单存在一定业务风险，设置白名单后，就只有白名单中的 IP 可以访问负载均衡监听。如果设置了白名单访问，但访问控制组中没有添加任何 IP，则负载均衡监听不会转发请求。
- 黑名单：**来自所选访问控制策略组中设置的 IP 地址或地址段的所有请求都不会转发，适用于应用只限制某些特定 IP 访问的场景。
 如果设置了黑名单访问，但访问控制组中没有添加任何 IP，则负载均衡监听会转发全部请求。

3.5.2 创建访问控制组

简介

在配置访问控制前，您需要先配置访问控制组，访问控制组是 IPv4 的 CIDR 地址集合。

操作步骤

- (1) 在 SLB 实例页面，单击左侧导航栏的“SLB 访问控制”，进入 SLB 访问控制页面。
- (2) 单击“新建访问控制组”，弹出新建访问控制组窗口。
- (3) 根据下表中的参数说明进行配置。

参数	说明
租户	仅租户管理员需配置该项。 选择访问控制组所属的租户。
部门	选择访问控制组所属的部门。
资源集	选择访问控制组所属的资源集。
名称	访问控制组的名称，可根据需要自定义名称或使用系统缺省名称。
IP类型	选择访问控制组支持的IP类型，支持IPv4和IPv6。
IP地址	输入IP地址或IP地址段，输入规则如下： <ul style="list-style-type: none">• 每一行一个 IP 地址或网段，以回车结束。• 每个 IP 地址或网段都可以用“ ”分割添加备注，如“192.168.0.1 ECS01”，备注长度范围是 1~255 个字符，不能包含<>。• 每个 IP 地址组最多可添加 300 个 IP 地址或网段。
描述	可根据需要输入描述信息，最多255个字符。

- (4) 单击“确定”，完成创建访问控制组操作。

3.5.3 删除访问控制组

简介

当您不再需要使用某个访问控制组时，可以删除该访问控制组。

限制与指导

仅当访问控制组未关联监听器时，才可以执行删除操作。

操作步骤

- (1) 在 SLB 实例页面，单击左侧导航栏的“SLB 访问控制”，进入 SLB 访问控制页面。
- (2) 单击访问控制组对应操作列的“删除”，弹出删除访问控制组窗口。
- (3) 确认要删除的访问控制组信息无误后，单击“确定”，完成删除访问控制组操作。

3.6 安全策略

3.6.1 安全策略概述

对于金融类等需要加密传输的应用，通常会配置 HTTPS 加密以确保数据的安全传输。SLB 预置了部分常用的 TLS 安全策略（系统策略）以满足加密需求，在创建和配置 HTTPS/TCPSSL 监听器时，您可以选择使用合适的默认安全策略，或者创建自定义安全策略，来提高您的业务安全性。

TLS 安全策略包含 TLS 协议版本和配套的加密算法套件。

3.6.2 创建自定义策略

- (1) 在 SLB 实例页面，单击左侧导航栏的“SLB 安全策略”，进入 SLB 安全策略页面。
- (2) 单击“新建自定义策略”，弹出新建自定义策略窗口。
- (3) 根据下表中的参数说明进行配置。

参数	说明
租户	仅租户管理员需配置该项。 选择安全策略所属的租户。
部门	选择安全策略所属的部门。
资源集	选择安全策略所属的资源集。
安全策略名称	安全策略的名称。
国密	选择安全策略是否支持国密。
协议版本	选择安全协议的版本，支持 TLS 1.0、TLS 1.1、TLS 1.2 和 GMSSL。 若勾选“国密”，则 GMSSL 默认勾选且无法修改。
TLS 1.3 版本	选择是否支持 TLS 1.3 的安全协议版本。 若勾选“国密”，则不支持 TLS 1.3 以及相关特性。
加密算法套件	在左侧可选套件区域，选择一个或多个加密算法套件后，单击  移入右侧已选择套件区域。 可通过上下拖动，设置加密算法套件的顺序。
描述	可根据需要输入描述信息，最多 255 个字符。

- (4) 单击“确定”，完成创建自定义策略操作。

3.6.3 删除自定义策略

简介

当您不再需要使用自定义安全策略时，可以删除该安全策略。

限制与指导

仅当自定义安全策略未关联监听器时，才可以执行删除操作。

操作步骤

- (1) 在 SLB 实例页面，单击左侧导航栏的“SLB 安全策略”，进入 SLB 安全策略页面。
- (2) 单击安全策略对应操作列的“删除”，弹出删除自定义策略窗口。
- (3) 确认要删除的安全策略信息无误后，单击“确定”，完成删除自定义策略操作。

3.7 监控信息

3.7.1 监控概述

SLB 支持流量监控，包括实例、监听器和转发规则三个维度的监控指标。

三个维度说明如下：

- 实例维度：所有经过 SLB 实例的流量的相关指标。
- 监听器维度：所有经过 SLB 实例并且按照监听端口区分的相关指标，理想情况下所有监听监控项的数据的总和跟实例维度数据是相等的。
- 转发规则维度：所有命中转发规则的数据的监控数据，理想情况下同一监听器所有转发规则监控项的数据的总和跟监听器数据是相等的。

注意

一些数据因为限速或防护策略等原因，不会被后续的监听器或转发规则处理统计，会造成实例维度数据、监听器维度数据和转发规则维度数据无法对齐。

3.7.2 监控项说明

3.7.2.1 流量监控

图表	支持的监听器	维度	单位	说明
出入带宽	四层、七层	实例、监听器、转发规则	bps	客户端到SLB的总带宽： <ul style="list-style-type: none">• 出方向带宽：发送给客户端的数据带宽。• 入方向带宽：从客户端接收的数据带宽。
并发连接数	四层、七层	实例、监听器	个	当前存在的连接的总数。
活跃连接数	四层、七层	实例、监听器	个	当前活跃的连接总数。
非活跃连接数	四层、七层	实例、监听器	个	当前处于非活跃状态的连接总数，例如TCP回收状态的连接。
每秒新建连接数	七层	实例	个/秒	每秒新建的连接总数。
每秒丢弃连接数	七层	实例	个/秒	负载均衡器每秒丢弃的连接数。

图表	支持的监听器	维度	单位	说明
正常后端服务器数	四层、七层	实例、监听器、转发规则	个	健康检查正常的后端服务器总数。
异常后端服务器数	四层、七层	实例、监听器、转发规则	个	健康检查不健康的后端服务器总数。
每秒请求数	七层	实例、监听器、转发规则	次/秒	负载均衡器平均每秒处理的请求数，为两次采集的总数跟间隔时间的平均值。
每秒请求数使用率	七层	实例、监听器、转发规则	%	每秒请求数占规格的比值。 注意：由于每秒请求数是两次采集时间间隔的平均数，对于流量不均衡场景，例如红包秒杀场景等，有可能使用率没有达到规格限速，也有可能触发限速。
每秒HTTP状态码个数	七层	实例、监听器、转发规则	个/秒	每秒负载均衡返回HTTP状态码应答报文给客户端的个数。 <ul style="list-style-type: none"> 每秒 1xx 状态码个数：返回 100-199 状态码的应答报文个数。 每秒 2xx 状态码个数：返回 200-299 状态码的应答报文个数。 每秒 3xx 状态码个数：返回 300-399 状态码的应答报文个数。 每秒 4xx 状态码个数：返回 400-499 状态码的应答报文个数。 每秒 5xx 状态码个数：返回 500-599 状态码的应答报文个数。
后端服务每秒HTTP状态码个数	七层	实例、监听器、转发规则	个/秒	每秒后端服务返回HTTP状态码应答报文给负载均衡的个数。 <ul style="list-style-type: none"> 每秒 1xx 状态码个数：返回 100-199 状态码的应答报文个数。 每秒 2xx 状态码个数：返回 200-299 状态码的应答报文个数。 每秒 3xx 状态码个数：返回 300-399 状态码的应答报文个数。 每秒 4xx 状态码个数：返回 400-499 状态码的应答报文个数。 每秒 5xx 状态码个数：返回 500-599 状态码的应答报文个数。
处理请求时间	七层	实例、监听器、转发规则	毫秒	从接受用户请求的第一个字节到发送完响应数据的时间。此时间为采样间隔时间内所有请求的平均时间。
后端服务应答时间	七层	实例、监听器、转发规则	毫秒	向后端建立连接开始到接受完数据然后关闭连接为止的时间。此时间为采样间隔时间内所有请求的平均时间。

3.7.2.2 后端健康状况监控

根据监听类型不同，分为如下情况：

- 若为四层监听，则该监控信息在监听器维度页面显示。
- 若为七层监听，则该监控信息在转发规则维度页面显示。

监控项	说明
IP地址：端口	后端服务的IP地址和端口。
服务器类型	分为ECS或在IP服务器两种。
当前健康状态	当前后端服务的健康状态。
健康走势	提供当前后端服务健康状况的历史曲线，双击可以查看大图。

4 常见问题

1. HTTP 和 HTTPS 协议的监听器转发规则中间动作典型配置举例

HTTP 和 HTTPS 协议的监听器在添加转发规则时，支持配置中间动作，如下是部分动作类型的典型配置，可供参考。

请求报文：Header 自定义脚本

修改 header

```
ngx.req.set_header('Host', 'modify')
```

增加 header

```
ngx.req.set_header('Test', 'add')
```

删除 header

```
ngx.req.clear_header("Test_Ngx_Ver")
```

请求报文：Body 自定义脚本

重写 Body

```
ngx.req.read_body()
local data = '{"data':'modified request body'}'
ngx.req.set_body_data(data)
```

追加 Body

```
ngx.req.read_body()
local data = ngx.req.get_body_data()
if data then
    data = data .. 'append'
    ngx.req.set_body_data(data)
else
    ngx.req.set_body_data('append')
end
```

替换 Body

```
ngx.req.read_body()
local data = ngx.req.get_body_data()
if data then
    local find_str = "req_body"
    local replace_str = "req_body_modified"
    local new_data = string.gsub(data, find_str, replace_str)
    ngx.req.set_body_data(new_data)
```

```
end
```

应答报文：Header 自定义脚本

删除 Header

```
ngx.header['Vary'] = nil
ngx.header['Server'] = nil
```

增加或修改 Header

```
ngx.header['Server'] = 'modify'
ngx.header['Nginx'] = 'add'
```

应答报文：Body 自定义脚本

重写 Body

```
local data, eof = ngx.arg[1], ngx.arg[2]
-- ngx.arg[1] indicates response body data
-- ngx.arg[2] indicates whether it is the end
local rewrite_str = '{"data":"rewrite response body"}\n'
ngx.arg[1] = nil
-- if data is last block, set value
if eof then
    ngx.arg[1] = rewrite_str
end
end
```

追加 Body

```
local data, eof = ngx.arg[1], ngx.arg[2]
local append_str = '{"data":"append response body"}\n'
if eof then
    if ngx.arg[1] then
        ngx.arg[1] = ngx.arg[1] .. append_str
    else
        ngx.arg[1] = append_str
    end
end
end
```

替换 Body

```
local data, eof = ngx.arg[1], ngx.arg[2]
if data then
    local find_str = "scheme"
    local replace_str = 'modify response body'
    local modified_body = string.gsub(data, find_str, replace_str)
    ngx.arg[1] = modified_body
end
```

end

⚠ 注意

如果服务器返回的应答报文携带了 **Content-Length**、**Content-Type** 的 Header，同时添加了“应答报文：Body 自定义脚本”的中间动作，导致应答的长度和类型发生了变化，则需要添加“应答报文：Header 自定义脚本”，修改 **Content-Length**、**Content-Type** 的 Header 为对应值。如果 **Content-Length** 未知，则可删除 **Content-Length**，设为 nil。

“应答报文：Header 自定义脚本”的配置示例如下：

```
ngx.header['Content-Length'] = ngx.header['Content-Length'] + 13
```

```
ngx.header['Content-Length'] = nil
```

```
ngx.header['Content-Type'] = "text/plain"
```

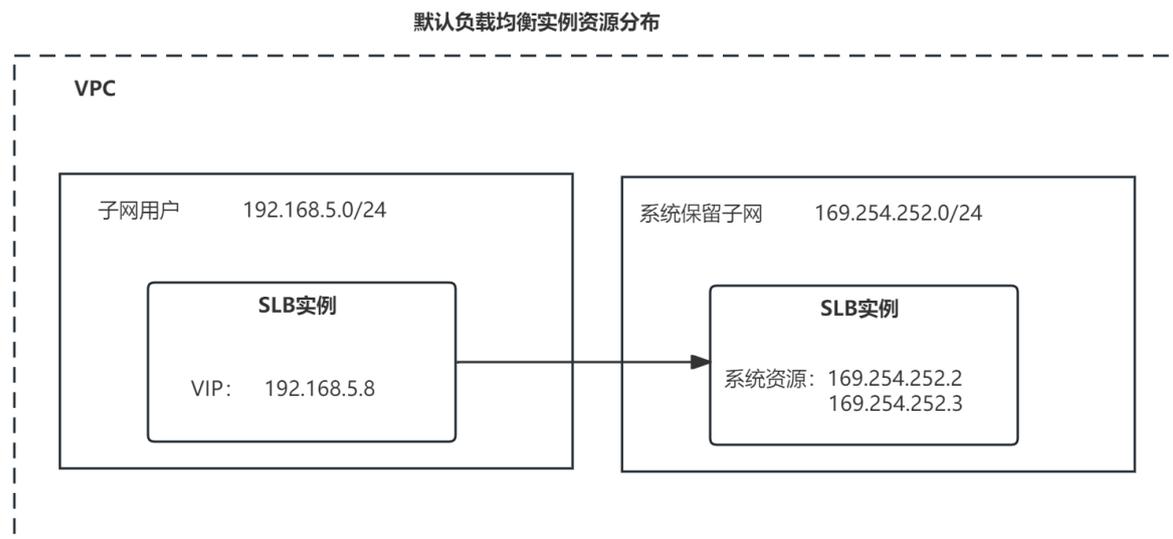
2. 负载均衡实例的“跨 VPC 访问”功能开启和关闭有什么区别？

开启“跨 VPC 访问”功能，负载均衡器的系统计算资源将不再占用保留网段的 IP，保留网段默认为 169.254.252.0/23。负载均衡器会从 VIP 所在子网，额外自动占用 2-8 个 IP 作为负载均衡器计算的系统资源 IP。开启此功能，需要保障最多 9 个 IP 可用。

由于使用用户子网的资源，用户可以配置负载均衡器的系统资源的路由，实现跨 VPC 访问。

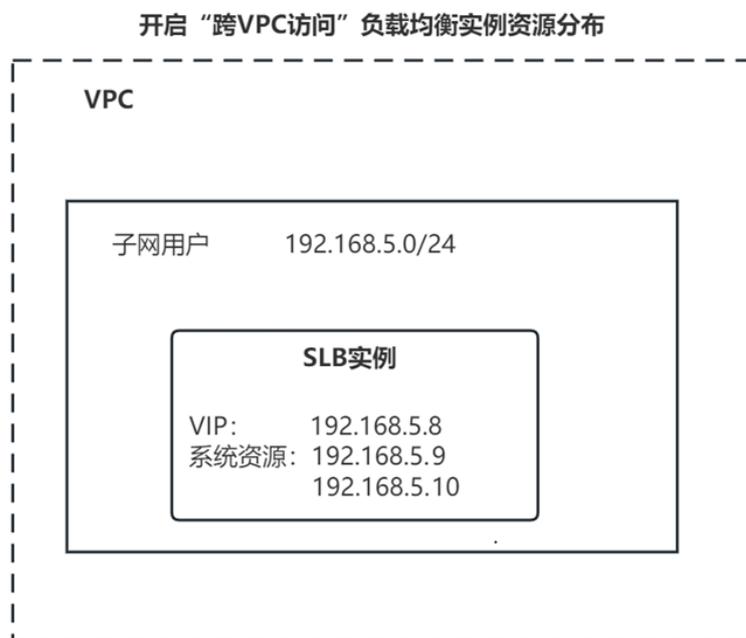
默认不开启“跨 VPC 访问”的场景如[图 4-1](#)所示，为了减少用户子网 IP 占用，使用了保留子网。所有 VPC 负载均衡器占用相同的保留子网，当前客户无法自定义配置路由策略。

图4-1 不开启“跨 VPC 访问”场景



开启“跨 VPC 访问”的场景如[图 4-2](#)所示，负载均衡器系统资源全部分布在用户子网，可以灵活的配置路由。

图4-2 开启“跨 VPC 访问”场景



3. 什么时候使用负载均衡器的“跨 VPC 访问”功能？

目前开启“跨 VPC 访问”功能，将会使用户能够自由的配置负载均衡器的系统资源的路由表，实现跨 VPC 访问能力，包括负载均衡器跨 VPC 访问后端和跨 VPC 的客户端访问负载均衡器。

另外，跨 VPC 访问会消耗额外的计算资源，当有大量应用需要跨 VPC 访问时，仍然建议将这些服务放到同一个 VPC 内部。

4. 新增跨 VPC 访问需求时，如何配置负载均衡器做到平滑演进？

对于已经创建的负载均衡器，由于系统资源已经创建，无法平滑开启“跨 VPC 访问”功能，所以需要另外创建新的支持“跨 VPC 访问”的负载均衡实例。

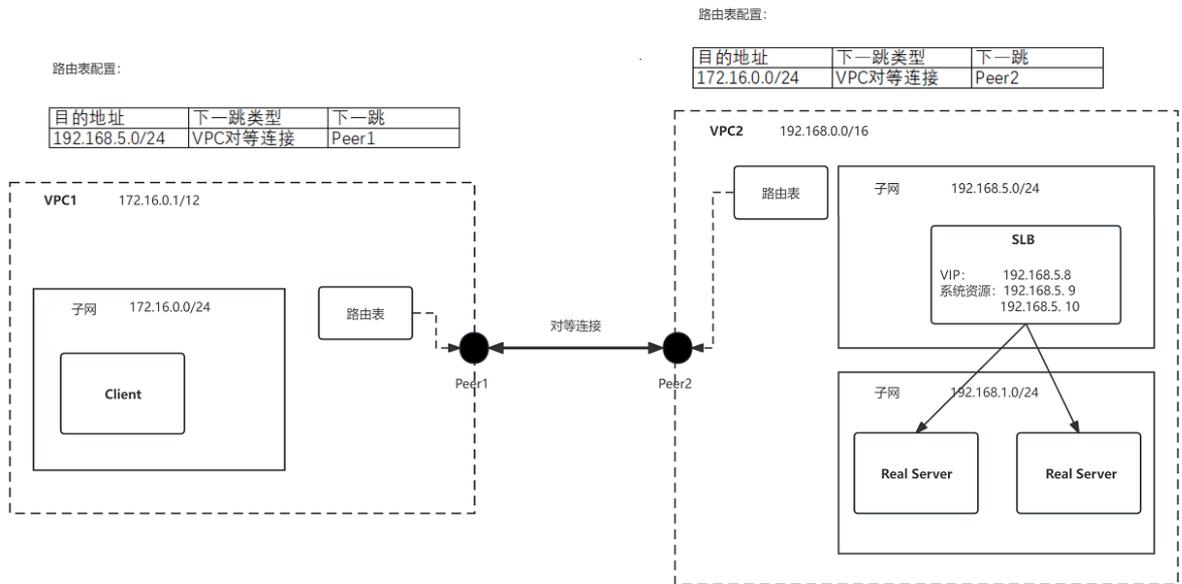
如果新的负载均衡器需要使用以前的负载均衡器的 VIP，有如下两种方法：

- 删除原有的负载均衡器，新建支持“跨 VPC 访问”功能的负载均衡器，并且创建时指定原有 VIP 地址。
- 新建支持“跨 VPC 访问”功能的负载均衡器，利用负载均衡器支持 VIP 地址池功能，解绑原有负载均衡器的 VIP 并绑定到新的负载均衡器。

5. 如何实现跨 VPC 访问 SLB 或者 SLB 跨 VPC 访问后端服务 IP？

目前，可以通过开启“跨 VPC 访问”将负载均衡器的系统资源配置到用户子网，通过配置子网路由打通跨 VPC 的访问能力。

以典型的对等连接为例，说明如下：



操作步骤如下:

- (1) 创建两个 VPC 的 Peer 对 Peer 的对等连接, 对等连接的创建需要确保两个 VPC 的子网不冲突。

VPC对等连接

VPC对等连接名称 ▾ 请输入VPC对等连接名称进行模糊查询 🔍

VPC对等连接名称/ID	状态	本端VPC	本端VPC网段	对端VPC	对端VPC网段
pc-2938 peer-bie81651ea39bta...	已连接	vpc-toi4laly3ve...	172.16.0.0/12	vpc-uffs8s7r654...	192.168.0.0/16
pc-5772 peer-zkhaxamclc6z63...	已连接	vpc-uffs8s7r65...	192.168.0.0/16	vpc-toi4laly3ve...	172.16.0.0/12

- (2) 配置两个 VPC 路由策略, 将两个 VPC 子网指向对端。

图4-3 客户端子网

rtb-p6piiswnfut8k79twzp7

基本信息

名称: rtb-vpc-uffs87r65425ruwjme	ID: rtb-p6piiswnfut8k79twzp7	类型: 默认路由表
专有网络 VPC: vpc-uffs87r65425ruwjme	部门: xtt	资源集: --
新建时间: 2023-10-18 19:07:09	描述: 默认路由表	

目的地址 请输入目的地址进行精确查询

目的地址	下一跳类型	下一跳	状态	类型	描述	操作
169.254.0.128/26	Local	--	active	系统路由	系统默认, 用于VPC内实例互通	系统路由不允许操作
192.168.0.0/24	Local	--	active	系统路由	系统默认, 用于VPC内实例互通	系统路由不允许操作
fc00:0:4:5a49:0:9::96	Local	--	active	系统路由	系统默认, 用于VPC内实例互通	系统路由不允许操作
114.5.168/29	--	--	active	系统路由	系统默认, 用于VPC访问云下...	系统路由不允许操作
169.254.0.192/27	Local	--	active	系统路由	系统默认, 用于VPC内实例互通	系统路由不允许操作
192.168.5.0/24	Local	--	active	系统路由	系统默认, 用于VPC内实例互通	系统路由不允许操作
fc00:0:4:5a49:0:3::96	Local	--	active	系统路由	系统默认, 用于VPC内实例互通	系统路由不允许操作
0.0.0.0/0	Internet网关	--	active	自定义路由	系统默认, 用于Internet访问	编辑 删除
::0	IPv6网关	--	active	自定义路由	系统默认, 用于Internet访问	编辑 删除
172.16.0.0/16	VPC对等连接	peer-zkhamcl6z637k95cm	active	自定义路由	--	编辑 删除

共 10 条 < 1 > 10 条/页 前往

图4-4 负载均衡器子网

rtb-17idksu03nxdjtpq5br

基本信息

名称: rtb-vpc-toi4laly3veuqsymm4dl	ID: rtb-17idksu03nxdjtpq5br	类型: 默认路由表
专有网络 VPC: vpc-toi4laly3veuqsymm4dl	部门: xtt	资源集: --
新建时间: 2023-10-17 19:47:18	描述: 默认路由表	

目的地址 请输入目的地址进行精确查询

目的地址	下一跳类型	下一跳	状态	类型	描述	操作
169.254.0.128/26	Local	--	active	系统路由	系统默认, 用于VPC内实例互通	系统路由不允许操作
172.16.0.0/24	Local	--	active	系统路由	系统默认, 用于VPC内实例互通	系统路由不允许操作
fc00:0:4:5a49:0:b::96	Local	--	active	系统路由	系统默认, 用于VPC内实例互通	系统路由不允许操作
114.5.168/29	--	--	active	系统路由	系统默认, 用于VPC访问云下...	系统路由不允许操作
169.254.0.192/27	Local	--	active	系统路由	系统默认, 用于VPC内实例互通	系统路由不允许操作
172.16.5.0/24	Local	--	active	系统路由	系统默认, 用于VPC内实例互通	系统路由不允许操作
fc00:0:4:5a49:0:c::96	Local	--	active	系统路由	系统默认, 用于VPC内实例互通	系统路由不允许操作
0.0.0.0/0	Internet网关	--	active	自定义路由	系统默认, 用于Internet访问	编辑 删除
::0	IPv6网关	--	active	自定义路由	系统默认, 用于Internet访问	编辑 删除
192.168.0.0/16	VPC对等连接	peer-bie01651ea39btawdva	active	自定义路由	--	编辑 删除

共 10 条 < 1 > 10 条/页 前往

- (3) 创建负载均衡器时, 启用“跨 VPC 访问”功能, 需要确保选择的“子网”在路由策略生效的范围内。

新建负载均衡

* 部门: xtt

资源集:

* 区域: region0

* 可用区: AZ0 AZ1

* 规格: 基础型 标准型 高阶型
基础型: 最大可以支持连接数5000, 新建连接数 (CPS): 3000, 每秒查询数 (QPS): 1000

* 计费模式: 包年包月 按需

* 专有网络: vpc-l2(vpc-8m1srfk92cl5khvhcmjs)

子网类型: 标准型 直通型

* 子网:
可用私网IP数量0个

国密: 开启

跨VPC后端: 开启

创建后可以查看负载均衡器系统资源占用情况:

SLB列表 / lb-76d1jisd2s7

lb-76d1jisd2s7

基本信息

名称: slb-4cjoc	ID: lb-76d1jisd2s7	可用区: AZ0
租户: xtt	部门: xtt	资源集: --
实例规格: 基础型	实例状态: 运行中	网络类型: 私网
专有网络ID: vpc-uffs8s7r65425ruwjmeb	子网ID: snet-81ke7e95l30jb8v74duq	跨VPC后端: 已开启
创建时间: 2023-11-14 14:41:36	占用IP: 192.168.5.10; 192.168.5.9;	国密: 未开启
描述: --		

计费信息

计费模式: 按需	所属订单: 134098898867322880	订单新建时间: 2023-11-14 14:41:36
到期时间: --		

6. 特殊场景性能无法达到规格上限

在特殊情况下, 例如使用少量客户端 IP 或者长链接流量不均存在大流量的情况, 可能会出现 SLB 达不到规格值。

主要原因是由于 SLB 是针对多用户的大量请求场景，对于少量用户或者少量连接的超大流量问题，会有负载不均的问题。负载均衡通过分布式的方式为负载均衡实例提供服务，所有外部的访问请求都会按照源 IP 的 Hash 策略，将流量平均分散到这些负载均衡内部服务器上转发。当单一客户 IP 或 TCP 连接流量过大，容易造成负载不均。

单个负载均衡器内部服务的规格上限为：规格值 × 150% / N，其中，N 为负载均衡器内部服务器的个数，默认基础型为 2 个，标准型为 4 个，高阶型为 8 个。

如果遇到上面问题，建议：

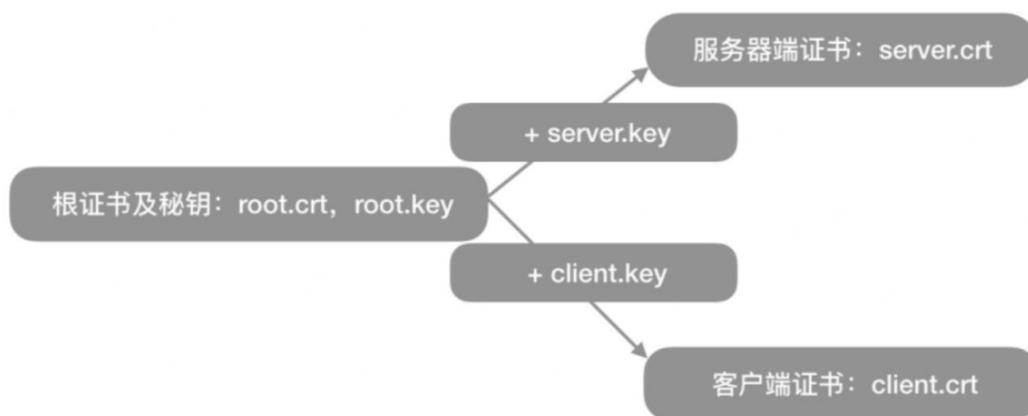
- 尽量使用多个客户端 IP。
- 尽量减少单 TCP 链接的请求数或流量，例如限制 HTTP 的单链接最大请求数。
- 使用较大规格的 SLB 实例。
- 联系管理员，将负载均衡器内部分担策略由源 IP 改为源 IP 和源端口。此方法有一定限制，一些 HTTP 高级特性会失效，例如：TLS 会话复用会失效，或者在集群设备时钟同步出现较大偏差时，HTTP Cookie 时间会不一致造成会话粘性失效。

7. 双向认证、双证书和 SNI（Server Name Indication，服务器名称指示）都是使用两个或多个证书，各自的使用场景如何选择

双向认证

双向认证要求当客户端向服务器发送请求或服务器接收客户端的请求时，服务器需要认证客户端；反之，当服务器向客户端发送请求或客户端接收服务器的请求时，客户端也需要认证服务器。只有双方都通过对方的认证请求时，通信才会被允许，以防止中间人攻击，冒充通信的一方。通过双向认证，通信双方都可以验证对方的身份，确保没有第三方介入。由于双向认证提供了更高的安全性，因此通常用于需要高安全性的场景，如金融服务、医疗信息传输等。

双向认证需要客户端和服务器端各自持有一套证书，但这两套证书来源于同一套根证书。例如，银行的 U 盾就是双向认证的典型应用。



双证书

在一些特殊场景，会有配置两个或多个证书的需求，一般情况下不常用。双证书的典型应用场景为：一个应用同时支持 ECC（椭圆曲线加密）和 RSA 两套证书。ECC 和 RSA 是两种不同的加密算法，各有优劣。ECC 通常具有更高的安全性和更小的密钥大小，而 RSA 则更为普及和兼容性好。

在某些情况下，为了同时满足安全性和兼容性的需求，可能会选择为 SLB 的监听器配置 ECC 和 RSA 双证书。

例如，某些用户早期使用 RSA 证书为电脑上不同规格的浏览器提供服务，后期定制开发了手机 APP，为了更高的安全性使用了 ECC 类型的证书。

SNI

SNI (Server Name Indication, 服务器名称指示), 允许客户端在 TLS 握手期间指定所请求的主机名, 从而使服务器能够根据主机名选择正确的证书。这解决了在单个 IP 地址上部署多个 HTTPS 站点时, 服务器如何根据客户端的请求提供相应域名证书的问题。

例如: `www.domain1.com` 使用证书 1, `www.domain2.com` 使用证书 2。可以在 SLB 监听器转发规则的扩展策略中, 为不同的域名配置不同的证书。

注意

请不要混淆 SNI 的域名和 HTTP 的域名:

- SNI 的域名在 TLS 握手阶段由客户端在 TLS 中指定, 用于选择 TLS 握手证书。
 - HTTP 的域名在 HTTP 报文的 Host Header 携带, 用于转发规则的条件匹配。
-