弹性负载均衡

最佳实践

文档版本 01

发布日期 2025-11-14

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，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，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目 录

1 ELB 选型和业务规划

1.1 ELB 实例规格选型

应用场景

弹性负载均衡服务提供了**独享型**和**共享型**ELB实例以供您根据实际业务**规模**和业务**类型**进行选择。

独享型实例提供了**固定规格**和**弹性规格**两种规格，您可以请参考**弹性负载均衡价格计算器**根据业务规模进行价格估算。

- **弹性规格**：适用于业务用量波动较大的场景，按实例使用量收取LCU费用。
- **固定规格**：适用于业务用量较为稳定的场景，按固定规格折算收取LCU费用。

本实践主要帮助您选择适用实际业务场景的ELB实例。

了解 ELB 的实例类型

弹性负载均衡服务提供**独享型**和**共享型负载**两种类型的实例供用户选择。

独享型相比共享型，**性能更卓越**，支持多种更为丰富的应用协议，具备更为灵活的七层处理能力。

实例类型的区别详见**独享型负载均衡与共享型弹性负载均衡的区别**。

表 1-1 产品类型对比

产品类型	独享型负载均衡	共享型负载均衡
部署模式	负载均衡实例资源独享，性能不受其它实例的影响，您可根据业务需要选择不同规格的实例。	集群部署，实例资源共享，支持性能保障模式。

产品类型	独享型负载均衡	共享型负载均衡
实例规格	• 弹性规格：按弹性规格的**实际使用量**计费。 • 固定规格：提供多种规格大小供选择，不同固定规格的实例提供差异化的性能指标。	不涉及。
性能上限	**单实例单可用区**最高支持**2千万并发连接**，选择多个可用区后，对应的最高性能规格（新建连接数/并发连接数等）加倍。 性能指标详情请参见**独享型负载均衡实例规格**。	• 未开启性能保障模式的实例，不提供性能保障。 • 开启性能保障模式后，提供**并发连接数5万**、**每秒新建连接数5000**、每秒查询速率5000的保障能力，**超出部分不提供性能保障**。
可用区	支持自定义可用区。	不涉及。
计费项	• 固定规格：实例规格费（按固定规格折算LCU数量收取）。 • 弹性规格：实例费和实际使用的LCU费用。	性能保障模式下收取实例费用。

了解独享型和共享型实例的关键功能对比

独享型相比共享型，支持多种更为丰富的应用协议，具备更为灵活的七层处理能力。

实例类型的更多功能区别详见**独享型负载均衡与共享型弹性负载均衡的功能对比**。

表 1-2 产品类型对比

对比项	独享型负载均衡	共享型负载均衡
产品定位	具备强大的四层和七层处理能力，支持多种应用协议和高级转发策略。	基础的四层与七层能力。
推荐应用场景	大流量高并发的业务场景，如大型网站、云原生应用、车联网、多可用区容灾应用。	流量负载较低的业务场景。
前端协议	TCP、UDP、HTTP、HTTPS、**QUIC**、**TLS**。	TCP、UDP、HTTP、HTTPS。
后端协议	TCP、UDP、HTTP、**HTTPS**、**QUIC**、**TLS**、**GRPC**。	TCP、UDP、HTTP。

对比项	独享型负载均衡	共享型负载均衡
转发能力对比	具备强大的四层和七层处理能力，详情参见**高级转发策略**。 • 支持基于域名、路径、HTTP请求方法、HTTP请求头、查询字符串、网段的转发规则。 • 支持转发至后端服务器组、重定向至监听器、重定向至URL、重写、返回固定响应。	支持基础的四层与七层处理能力，详情参见**转发策略（共享型）**。 • 仅支持基于域名或路径的转发规则。 • 仅支持转发至后端服务器组、重定向至监听器。
后端服务器组关键差异	• 后端服务器组**支持被多个ELB实例/监听器重复使用** • 转发模式：负载均衡均衡、**主备转发**	• 后端服务器组**仅支持被一个监听器使用** • 转发模式：负载均衡均衡
后端服务器	• 支持添加相同VPC下的云服务器和辅助弹性网卡 • 支持通过IP类型后端功能添加不同VPC和线下IDC的服务器	仅支持添加云上相同VPC下的云服务器

了解应用型和网络型的差异

独享型ELB实例支持选择应用型和网络型，支持您根据具体业务类型进一步选择。

- **应用型**（HTTP/HTTPS）：支持HTTP、HTTPS和QUIC协议，适用于七层高性能要求业务，实时音视频、互动直播和游戏等业务。
- **网络型**（TCP/UDP/TLS）：支持TCP、UDP和TLS协议，适用于四层大流量高并发业务，如文件传输、即时通信、在线视频等业务。

表 1-3 监听协议类型说明

类型	协议	说明	适用场景
网络型	TCP	• 基于源地址的会话保持。 • 数据传输快。	• 适用于注重可靠性，对数据准确性要求高的场景，如文件传输、发送或接收邮件、远程登录。 • 对性能和并发规模无特别要求的Web应用。
网络型	UDP	• 可靠性相对低 • 数据传输快	适用于关注实时性而相对不注重可靠性的场景，如视频聊天、游戏、金融实时行情推送。

类型	协议	说明	适用场景
网络型	TLS	• 加密传输数据，可以阻止未经授权的访问。 • 支持单向认证和双向认证	适用于需要超高性能和大规模TLS卸载的场景。
应用型	HTTP	• 基于Cookie的会话保持。 • 使用X-Forward-For获取源地址。	适用于需要对数据内容进行识别的应用，如Web应用、移动游戏等。
应用型	HTTPS	• 加密传输数据，可以阻止未经授权的访问。 • 加解密操作在负载均衡器上完成，可减少后端服务器的处理负载。 • 多种加密协议和加密套件可选。	适用于需要加密传输的应用，如电子商务、金融服务等场景。
应用型	QUIC	• 基于UDP的快速互联网连接。 • 避免队头阻塞的多路复用。 • 改善拥塞控制。	适用于弱网络、网络频繁切换的业务场景。

1.2 独享型 ELB 子网规划的推荐方案

应用场景

本实践文档旨在为使用ELB的用户提供子网规划建议，以确保ELB实例的稳定运行并满足未来业务扩展的需求。

通过合理规划子网，可以避免因ELB实例占用IP地址数量超过预期而影响业务扩展的情况。

ELB 实例对子网 IP 地址的使用场景

ELB实例的前端子网将为ELB实例分配虚拟IP地址**用于与内网中的资源进行通信**。后端子网将为ELB实例分配IP地址**用于与后端服务器进行通信和健康检查**。

ELB使用的子网IP地址详情请见**表1-4**，ELB实例使用的IP地址主要分布在后端子网，因此用户可以通过规划一个ELB实例专属的后端子网，避免ELB实例使用业务子网过多的IP地址而影响业务扩展。

在ELB支持**IPv4/IPv6双栈**场景时，由于需要支持IPv6地址通信，**使用的子网IP地址数量为仅支持IPv4通信时的两倍**。

说明

TLS监听器的业务转发和健康检查场景归属为七层业务转发和七层监听器健康检查。

表 1-4 ELB 实例对 IP 地址的使用情况说明（单可用区）

IP地址使用场景	IP地址归属子网	是否与可用区数量有关	使用IP地址个数
ELB实例的虚拟IP	前端子网	否	1个
四层业务转发	后端子网	随可用区数量线性叠加	• 实例未开启IP类型后端：0个 • 实例开启IP类型后端：4个
四层监听器健康检查	后端子网	随可用区数量线性叠加	1个
七层业务转发	后端子网	否	通常为20个，变化范围为8~128个。 实际使用IP地址个数可能会随区域和业务规模情况有浮动变化。 **说明** 关联同一后端子网的ELB实例可以重复使用这些占用的IP地址。
七层监听器健康检查	后端子网	否	重复使用**七层业务转发**使用的IP地址

ELB 实例使用 IP 地址数量总结

ELB在支持IPv4/IPv6双栈通信时，使用的IP地址数量为仅支持IPv4通信时的两倍。

前端子网仅为ELB实例分配用于对外通信的虚拟IP地址，在IPv4场景下分配一个，IPv4/IPv6双栈场景下分配2个，与可用区数量无关。

以下表格列举ELB实例**仅支持IPv4通信**时使用后端子网的IP地址个数。

说明

七层业务转发使用**后端子网**IP地址数量通常为20个，实际使用IP地址个数可能会随区域和业务规模情况有浮动变化，变化范围为8~128个。如**表1-5**中，以20个作为示例个数列举。

表 1-5 ELB 实例使用**后端子网** IP 地址数量总结（IPv4 场景）

实例部署场景	业务转发场景	使用IP地址个数最小值	使用IP地址个数最大值
单可用区实例	仅四层业务转发	1	5
	仅七层业务转发	20	20
	四层和七层业务转发	21	25

实例部署场景	业务转发场景	使用IP地址个数最小值	使用IP地址个数最大值
双可用区实例	仅四层业务转发	2	10
	仅七层业务转发	20	20
	四层和七层业务转发	22	30
三可用区实例	仅四层业务转发	3	15
	仅七层业务转发	20	20
	四层和七层业务转发	23	35

规划 ELB 实例使用的子网

通常一个ELB实例会占用后端子网10到20个IP地址不等，主要用于ELB实例与后端服务器通信。如果您实例的后端子网使用了业务子网，当业务子网规划的网段较小时，容易导致业务子网的IP地址耗尽，无法完成业务扩展。

建议您规划**专用的ELB后端子网，**使ELB后端子网与业务子网隔离，同时后端子网规划一个较大CIDR地址段，以便分配较多的IP地址数量。 所有ELB实例的后端子网都可以选择该子网，避免业务子网被ELB实例占用。您可以根据业务场景按需分配子网，相应调整专用子网的大小。

如果VPC子网不足，您可以参考**为虚拟私有云添加IPv4扩展网段**扩展子网网段。

表 1-6 子网规划场景建议

子网	使用场景	具体作用
业务子网	业务部署	用于分配业务部署所需ECS、ENI等实例的IP地址 。
前端子网	分配ELB实例对外服务的IP地址	用于分配ELB实例对外服务的虚拟IP地址，可以与业务子网相同。
后端子网	• 健康检查 • 业务请求转发	用于分配ELB实例与后端服务器通信的IP地址，不建议使用业务子网。

如**图1-1**所示，在区域A内，子网Subnet-frontend用作**业务子网**和**ELB的前端子网**，建议您的后端服务器部署在该子网中，子网Subnet-backend仅用作**ELB的后端子网**。

图 1-1 规划 1 个 VPC 和两个子网

关键操作步骤

步骤1 如图1-1所示，创建一个VPC-elb，两个子网Subnet-frontend和Subnet-backend，详情请参考**创建虚拟私有云和子网**。

步骤2 创建一个独享型ELB，详情请参考**购买独享型负载均衡器**。

如图1-2所示，ELB的所属VPC选择**步骤1**中创建的VPC-elb，前端子网选择**步骤1**中创建的Subnet-frontend，后端子网选择**步骤1**中创建的Subnet-backend。

图 1-2 独享型负载均衡器的网络配置

步骤3 根据图1-2的界面提示，在后端服务器的安全组中放通后端子网的网段，详情请参考**配置后端服务器的安全组**。

----结束

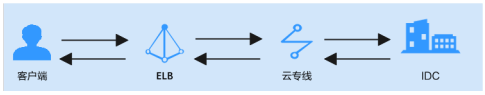
1.3 独享型 ELB 通过 IP 类型后端挂载云下 IDC 的服务器

应用场景

如果您需要使用ELB挂载云下IDC服务器实现负载均衡，您可以通过ELB和专线/VPN等产品的组合配置，将ELB的请求转发至云下IDC（Internet Data Center）服务器。

实践方案架构

图 1-3 独享型 ELB 挂载云下 IDC 的服务器架构图



本实践通过云专线连通云下IDC服务器与云上虚拟私有云，独享型ELB实例通过IP类型后端挂载云下IDC的服务器作为后端服务器处理客户端请求。

- 独享型负载均衡（ELB-Test）在VPC-Test-01（172.16.0.0/12）中。
- 云下服务器（IDC-IP-Test）部署在云下IDC中。
- 通过使用IP类型后端功能将云下IDC中的服务器（IDC-IP-Test）添加至独享型负载均衡（ELB-Test）的后端服务器组中。

资源规划说明

本实践示例中需要创建虚拟私有云VPC、弹性负载均衡ELB、弹性公网IP、云专线、弹性云服务器ECS和与云下IDC服务器，资源规划总体说明请参见表1-7。

本实践以公网访问为例，如果您的客户端与ELB实例为私网连通场景，您可以直接通过私网地址进行访问。

表 1-7 资源规划

资源	数量	说明
虚拟私有云和子网	1个虚拟私有云和其下2个子网	• VPC-Test-01，本示例网段为：172.16.0.0/12。 • subnet-frontend，本示例网段为：172.16.0.0/16。 • subnet-backend，本示例网段为：172.18.0.0/16。
弹性负载均衡	1个	被访问的ELB实例。 • 所属VPC：VPC-Test-01。 • 前端子网：subnet-frontend。 • 后端子网：subnet-backend。
云专线	1条	通过云专线（DC）打通云下IDC与云上虚拟私有云网络。
弹性云服务器	1台	ECS-client，用于访问云下IDC服务器。
弹性公网IP	2个	• 被访问的ELB实例绑定的对公网提供服务的EIP。 • ECS-client绑定EIP实现通过公网访问ELB实例。
云下IDC服务器	1台	IDC-IP-Test，部署在云下数据中心的服务器。

准备工作

- 购买一台ECS用作访问客户端ECS-client并绑定EIP。购买ECS详情请参考**快速购买和使用Linux ECS（一屏购买方式）**。
- 创建虚拟私有云VPC-Test-01和子网subnet-frontend、子网subnet-backend。具体操作，请参考**创建虚拟私有云和子网**。
- 创建独享型ELB实例并开启“IP类型后端”开关，为ELB绑定EIP。具体操作，请参见**购买独享型负载均衡器**和**绑定IPv4公网IP**。

步骤一：通过云专线打通云下 IDC 与 VPC 网络

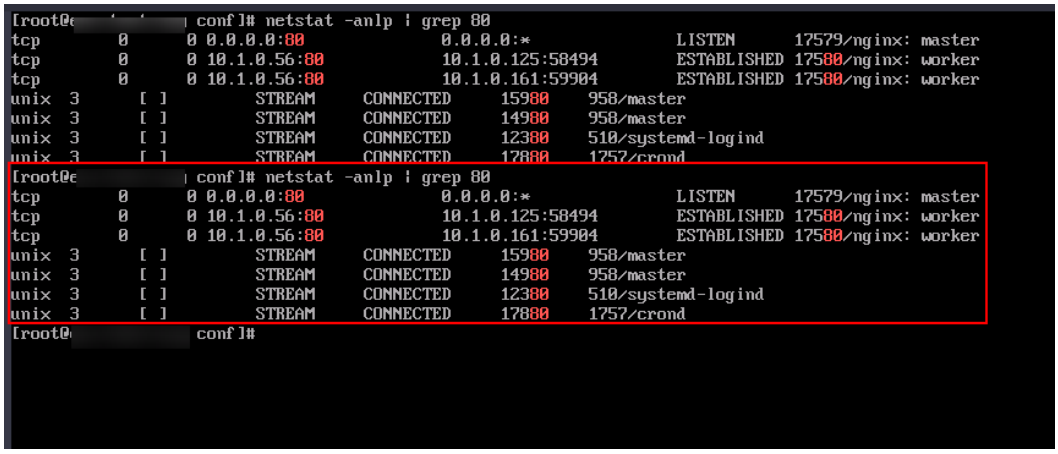
您可以通过自助方式开通云专线服务，实现虚拟私有云中的云服务器和本地的数据中心或私有网络进行通信。

具体操作详情请参考**通过云专线实现云下IDC访问云上VPC（虚拟网关VGW）**。

步骤二：在云下 IDC 的服务器中部署服务

在云下IDC的服务器IDC-IP-Test中部署Nginx，后续用于验证网络连通性。

图 1-4 云下 IDC 的服务器部署 Nginx 成功



步骤三：创建后端服务器组并添加云下 IDC 的 IP 地址作为后端服务器

1. 进入**后端服务器组列表页面**。
2. 在后端服务器列表页面，单击页面右上角“创建后端服务器组”按钮。
3. 配置后端分配策略，关键参数详情请参见**表1-8**，其余配置项保持默认值即可。

表 1-8 配置后端分配策略参数说明

参数	示例	说明
名称	**server_group**	创建的后端服务器组的名称。
负载均衡类型	**独享型**	可使用该后端服务器组的负载均衡实例类型。

参数	示例	说明
所属负载均衡器	**关联已有**	使用该后端服务器组的负载均衡实例。 单击“关联已有”后，选择您已创建完成的负载均衡实例。
后端协议	**HTTP**	后端云服务器自身提供的网络服务的协议。 本实践方案选择HTTP协议。
分配策略类型	**加权轮询算法**	负载均衡采用的算法，本实践方案保持默认的加权轮询算法。 加权轮询算法：根据后端服务器的权重，按顺序依次将请求分发给不同的服务器，权重大的后端服务器被分配的概率高。 更多关于分配策略的信息，请参见**配置流量分配策略分发流量**。

4. 单击“下一步”，添加后端服务器并配置健康检查。
5. 切换到“IP类型后端”页签，单击“添加IP类型后端”。
6. 在添加IP类型后端页面，添加线下IDC服务器作为后端服务器，设置如下：
   - **IP类型后端IP**：10.1.0.56，云下IDC服务器IDC-IP-Test的私网IP。
   - **业务端口**：根据后端业务进行设置，本实践设置为80端口。
   - **权重**：保持默认值1。
7. 单击“确定”，完成IP类型后端的添加。
8. 保持健康检查开启，其余健康检查参数保持默认。
9. 单击“下一步”。
10. 确认配置无误后，单击“立即创建”。

步骤四：添加监听器并选择后端服务器组

1. 进入**弹性负载均衡列表页面**。
2. 在目标弹性负载均衡实例的操作列，单击“添加监听器”。
3. 在添加监听器页面，前端协议选择“HTTP”，监听端口选择“80”端口，其余配置保持默认。
4. 单击“下一步：配置后端分配策略”，后端服务器组参数选择“使用已有”。
   选择中**步骤三**已经创建的后端服务器组，完成后单击“下一步：确认配置”。
5. 确认配置参数后，单击“提交”，完成监听器的创建。

步骤五：验证通过 IP 类型后端可以访问云下 IDC 服务器

1. 通过客户端访问验证网络连通性。
   a. 远程登录客户端ECS_client。
      弹性云服务器有多种登录方法，具体请参见**登录弹性云服务器**。
   b. 通过curl -v http://<IP>:<端口>命令测试网络连通性。
      本实践执行以下命令：

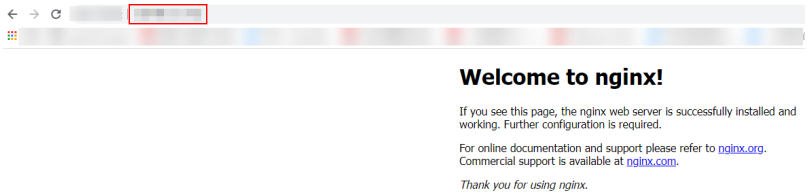
```
curl -v http://<ELB的EIP地址>:<监听端口>
```

如果成功收到Nginx默认欢迎页的内容，表明ELB成功转发请求至云下IDC服务器。

2. 通过浏览器访问验证连通性。

   使用浏览器访问“http://<ELB的EIP地址>”，显示如下页面，说明请求被ELB实例转发到云下IDC服务器。

图 1-5 通过浏览器访问到 Nginx 默认欢迎页



1.4 通过 IP 类型后端功能添加服务器至 ELB

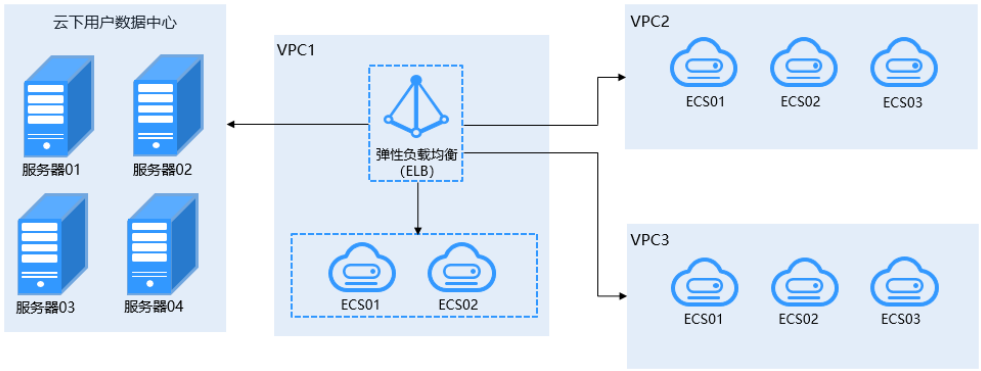
1.4.1 方案概述

应用场景

某公司在云上多个VPC及云下用户数据中心（IDC）拥有多台后端服务器，如图1-6所示。希望使用弹性负载均衡将访问流量分发到这些后端服务器上。

本节操作介绍通过独享型负载均衡实现将云上、云下多台后端服务器添加至ELB的方法。

图 1-6 添加云上、云下多台后端服务器至 ELB



方案架构

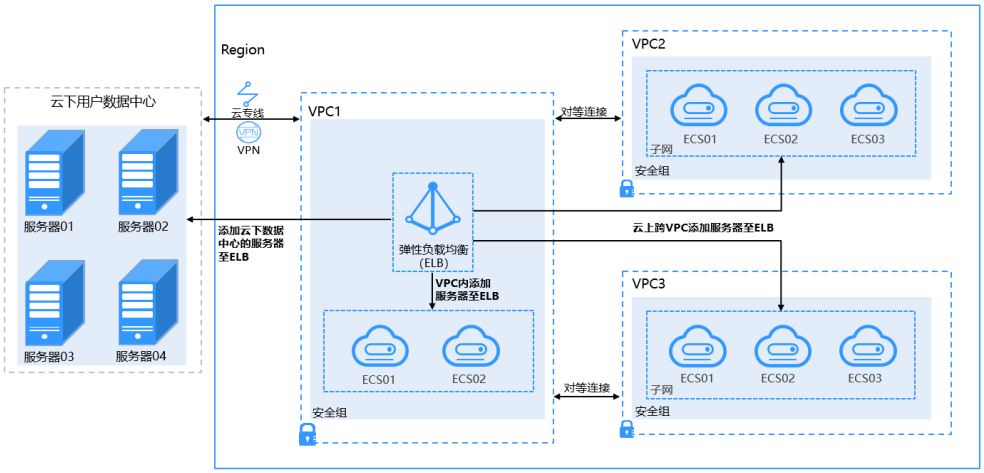
通过分析，可以通过为独享型负载均衡添加IP类型后端来实现将云上、云下多台后端服务器添加至ELB。

如图1-7所示：

- 无论是否开启IP类型后端功能，均可添加弹性负载均衡所在VPC内的后端服务器至ELB后端服务器组。

- 独享型负载均衡器开启IP类型后端（原跨VPC后端）功能后：
  - 通过云专线或VPN，支持将云下用户数据中心的服务器添加至ELB后端服务器组。
  - 通过在云上VPC之间建立对等连接，支持将其他VPC内的服务器添加至ELB后端服务器组。
  - 通过IP类型后端功能添加ELB同VPC中的服务器至ELB后端服务器组。

图 1-7 添加服务器至 ELB



方案优势

独享型负载均衡实例支持混合负载均衡的能力，后端服务器组不仅支持添加云上同VPC内的服务器，还支持跨VPC添加云上其他VPC和云下数据中心的服务器。帮助用户根据业务诉求灵活配置，将流量请求转发到云上、云下的服务器上。

- 独享型负载均衡支持在后端服务器组中添加云上同VPC内的服务器。
- 跨VPC添加云上其他VPC中的服务器，需要先在ELB所在的VPC和云上其他VPC之间建立对等连接，然后通过IP类型功能添加
- 通过IP类型后端功能添加云下数据中心的服务器，需要先通过云专线或VPN连通云上ELB所在的VPC和云下数据中心。

约束限制

使用混合负载均衡功能时，请注意以下事项：

- 请前往负载均衡器基本信息页面开启IP类型后端功能，否则该功能无法正常使用。
- IP类型后端的IP地址只允许为IPv4类型的地址。
- IP类型后端的IP地址不能为公网IP地址，否则请求不可达。
- 请确保负载均衡器的后端子网有足够的IP地址（至少有16个可用IP地址），否则该功能无法正常使用。可以通过负载均衡器的“基本信息 > 后端子网”添加多个后端子网来增加后端子网的IP地址。
- IP类型后端的安全组规则必须放通负载均衡器的后端子网网段，否则会导后端业务流量与健康检查异常。

- IP类型后端功能开启后无法关闭。

1.4.2 通过 IP 类型后端添加云上不同 VPC 的服务器至 ELB

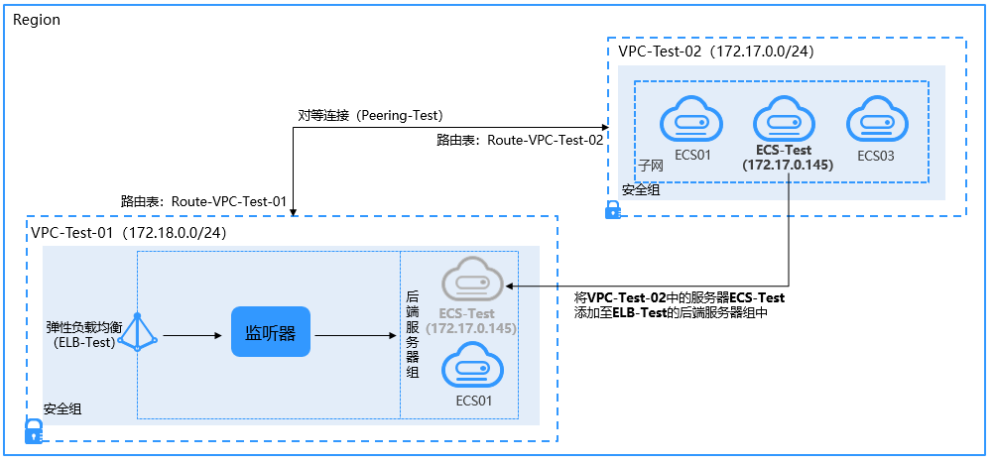
应用场景

本实践以用户常用的云上跨不同VPC添加服务器至ELB后端服务器组为例。

方案架构

- 独享型负载均衡（ELB-Test）在VPC-Test-01（172.18.0.0/24）中。
- 服务器（ECS-Test）在VPC-Test-02（172.17.0.0/24）中。
- 通过使用IP类型后端功能将VPC-Test-02（172.17.0.0/24）中的服务器（ECS-Test）添加至独享型负载均衡（ELB-Test）的后端服务器组中。

图 1-8 最佳实践拓扑图



方案优势

独享型负载均衡实例支持混合负载均衡的能力，支持跨不同VPC添加云上其他VPC的服务器。帮助用户根据业务诉求灵活配置，将流量请求转发到服务器上。

资源和成本规划

资源的实际费用以华为云管理控制台显示为准。

表 1-9 资源规划

资源	资源名称	资源说明	数量
VPC	VPC-Test-01	创建独享型负载均衡（ELB-Test）所在VPC： 172.18.0.0/24	1

资源	资源名称	资源说明	数量
	VPC-Test-02	服务器（ECS-Test）所在的VPC： 172.17.0.0/24	1
对等连接	Peering-Test	在ELB所在的VPC和云上其他VPC之间建立对等连接 本端VPC网段：172.18.0.0/24 对端VPC网段：172.17.0.0/24	1
路由表	Route-VPC-Test-01	创建对等连接路由，所属VPC：VPC-Test-01 目的地址：172.17.0.0/24	1
	Route-VPC-Test-02	创建对等连接路由，所属VPC：VPC-Test-02 目的地址：172.18.0.0/24	1
ELB	ELB-Test	独享型负载均衡	1
EIP	EIP-Test	用于给ELB-Test绑定的弹性公网IP 119.3.233.52	1
ECS	ECS-Test	ECS所属VPC：VPC-Test-02 私网IP：172.17.0.145	1

操作流程

图 1-9 最佳实践操作流程

步骤一：创建 VPC

1. 进入**虚拟私有云控制台**。
2. 根据**表1-9**创建VPC-Test-01，完成后单击“立即创建”。详见**《虚拟私有云用户指南》**。
   - 名称：VPC-Test-01
   - IPv4网段：172.18.0.0/24
   - 其他参数根据需要设置即可。
3. 参考**表1-9**规划，创建VPC-Test-02。
   - 名称：VPC-Test-02
   - IPv4网段：172.17.0.0/24
   - 其他参数根据需要设置即可。

图 1-10 创建所需 VPC

步骤二：创建 VPC 对等连接

1. 在虚拟私有云控制台单击左侧“对等连接”。
2. 单击右上角的“创建对等连接”。
3. 根据**表1-9**创建对等连接Peering-Test，完成后单击“立即创建”。详见**《虚拟私有云用户指南》**。
   - 名称：Peering-Test
   - 本端VPC：VPC-Test-01
   - 对端VPC：VPC-Test-02
   - 其他参数根据需要设置即可。

步骤三：添加对等连接路由

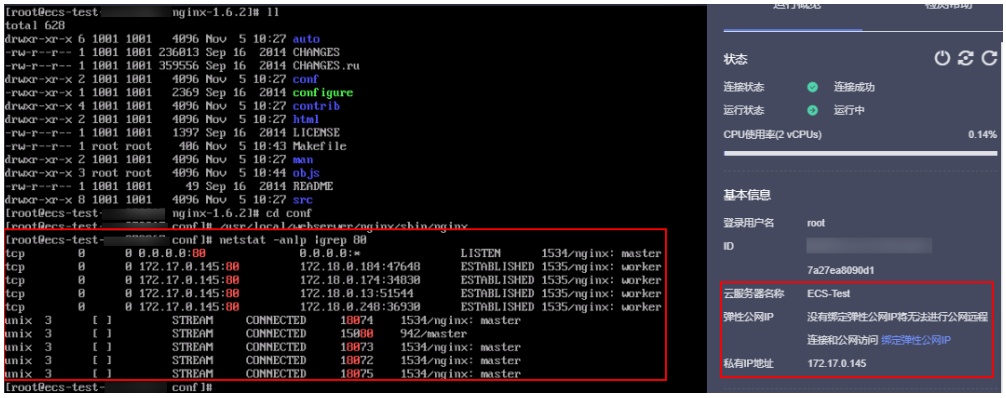
1. 在虚拟私有云控制台单击左侧“路由表”。
2. 单击右上角的“创建路由表”。
3. 根据**表1-9**创建路由表Route-VPC-Test-01，完成后单击“确定”。详见**《虚拟私有云用户指南》**。
   - 路由表名称：Route-VPC-Test-01
   - 所属VPC：VPC-Test-01
   - 目的地址：172.17.0.0/24
   - 下一跳类型：对等连接
   - 下一跳：Peering-Test
4. 重复以上步骤，参考**表1-9**规划，创建Route-VPC-Test-02。
   - 路由表名称：Route-VPC-Test-02
   - 所属VPC：VPC-Test-02
   - 目的地址：172.18.0.0/24
   - 下一跳类型：对等连接
   - 下一跳：Peering-Test

步骤四：创建弹性服务器

1. 选择“计算 > 弹性云服务器”。
2. 单击右上角的“购买弹性云服务器”。
3. 根据**表1-9**创建服务器ECS-Test，根据需要设置相关参数。详见**《购买弹性云服务器》**。

   虚拟私有云选择VPC-Test-02，服务器名称设置为ECS-Test。
4. 后端服务器ECS-Test创建成功后，在其上部署Nginx。

图 1-11 在 ECS-Test 上部署 Nginx



步骤五：创建独享型 ELB 并为其添加 HTTP 监听器和后端服务器组

1. 进入**购买弹性负载均衡页面**。
2. 根据**表1-9**创建独享型负载均衡ELB-Test，根据需要设置相关参数。详见**《弹性负载均衡用户指南》**。
   - 实例规格类型：独享型
   - 所属VPC：VPC-Test-01
   - 名称：ELB-Test
   - IP类型后端：开启
   - 其他参数根据需要设置。
3. 独享型ELB创建成功后，在ELB-Test中添加HTTP监听器和后端服务器组。

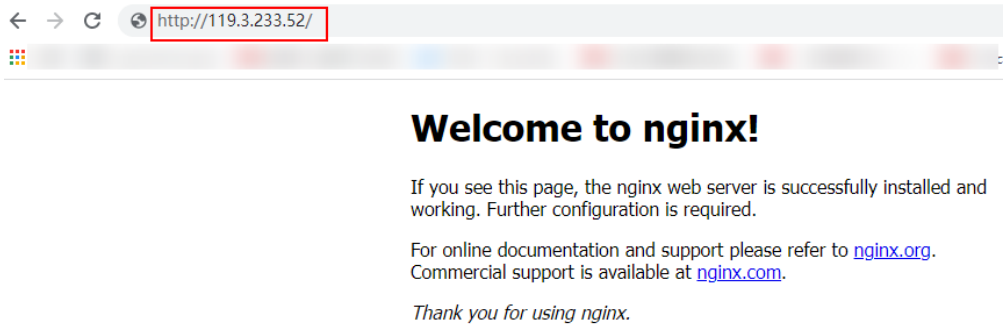
步骤六：将 ECS 添加至 ELB 后端服务器组

1. 单击上述创建的独享型负载均衡ELB-Test名称。
2. 切换到“监听器”页签，单击上述所创建的HTTP监听器。
3. 在监听器“基本信息”页签，在下方后端服务器组界面，单击“查看/添加后端服务器”。
4. 进入右侧“后端服务器组”页面。
5. 在“IP类型后端”右侧，单击“添加”，设置相关参数，完成后单击“确定”。详见《弹性负载均衡用户指南》。
   - IP类型后端IP：172.17.0.145（ECS-Test的私网IP）
   - 业务端口：根据后端业务需要设置
   - 权重：根据需要设置
6. 单击“确定”，完成添加。

步骤七：验证 IP 类型后端添加后端服务器是否成功

1. 单击上述创建的独享型负载均衡ELB-Test操作列的“更多”。
2. 选择“绑定IPv4公网IP”，给ELB-Test绑定一个弹性公网IP（EIP-Test：119.3.233.52）。
3. 使用浏览器访问“http://119.3.233.52/”，显示如下页面，说明本次访问请求被ELB实例转发到后端服务器“ECS-Test”上，“ECS-Test”正常处理请求并返回请求的页面。

图 1-12 验证 IP 类型后端添加后端服务器是否成功



1.4.3 通过 IP 类型后端添加云上相同 VPC 的服务器至 ELB

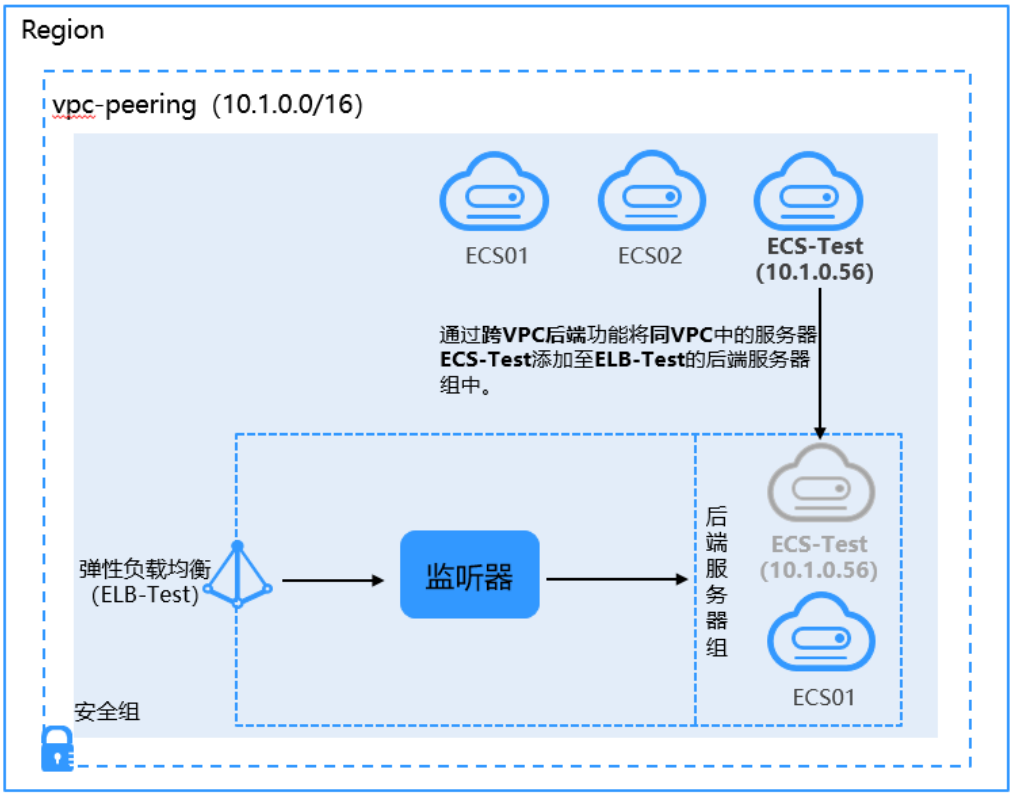
应用场景

您还可以通过IP类型后端功能添加与ELB同VPC内的服务器至ELB后端服务器组。

方案架构

- 独享型负载均衡（ELB-Test）在vpc-peering（10.1.0.0/16）中；
- 服务器（ECS-Test）也在vpc-peering（10.1.0.0/16）中；
- 通过使用IP类型后端功能将后端服务器（ECS-Test）添加至独享型负载均衡（ELB-Test）的后端服务器组中。

图 1-13 使用 IP 类型后端功能添加同 VPC 的 ECS 至 ELB



方案优势

独享型负载均衡实例支持混合负载均衡的能力，后端服务器组支持添加云上同VPC内的服务器。帮助用户根据业务诉求灵活配置，将流量请求转发到服务器上。

资源和成本规划

资源的实际费用以华为云管理控制台显示为准。

表 1-10 资源规划

资源	资源名称	资源说明	数量
VPC	vpc-peering	创建独享型负载均衡（ELB-Test）和ECS-Test所在VPC： 规划网段：10.1.0.0/16	1
对等连接	Peering-Test	在ELB所在的VPC和云上其他VPC之间建立对等连接 本端VPC网段：10.1.0.0/16 对端VPC网段：任选	1
路由表	Route-VPC-Test-01	创建对等连接路由，所属VPC：vpc-peering 目的地址：10.1.0.0/16	1
ELB	ELB-Test	独享型负载均衡（ELB-Test） 私网IP：10.1.0.9	1
EIP	EIP-Test	用于给ELB-Test绑定的弹性公网IP 120.46.131.153	1
ECS	ECS-Test	ECS所属VPC：vpc-peering 私网IP：10.1.0.56	1

操作流程

图 1-14 操作流程

步骤一：创建 VPC

1. 进入**虚拟私有云控制台**。
2. 根据**表1-10**创建vpc-peering，完成后单击“立即创建”。详见**《虚拟私有云用户指南》**。
   - 名称：vpc-peering
   - IPv4网段：10.1.0.0/16
   - 其他参数根据需要设置即可。

步骤二：创建 VPC 对等连接

1. 在虚拟私有云控制台单击左侧“对等连接”。
2. 单击右上角的“创建对等连接”。
3. 根据**表1-10**创建对等连接Peering-Test，完成后单击“立即创建”。详见**《虚拟私有云用户指南》**。
   - 名称：Peering-Test
   - 本端VPC：vpc-peering

- 对端VPC：任选
- 其他参数根据需要设置即可。

步骤三：添加对等连接路由

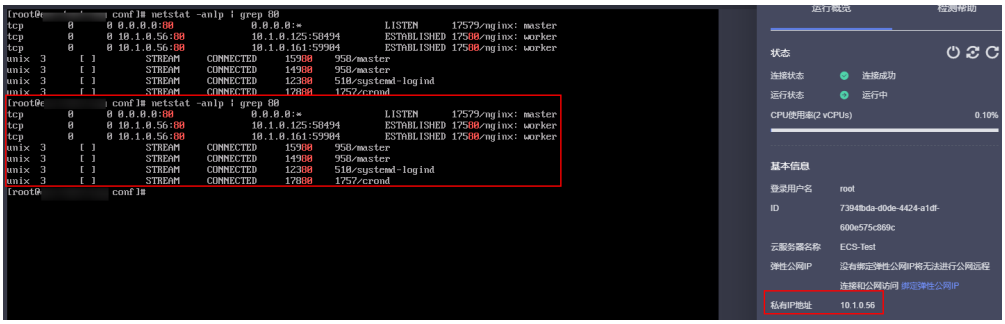
1. 在虚拟私有云控制台单击左侧“路由表”。
2. 单击右上角的“创建路由表”。
3. 根据**表1-10**创建路由表Route-VPC-Test-01，完成后单击“确定”。详见**《虚拟私有云用户指南》**。
   - 路由表名称：Route-VPC-Test-01
   - 所属VPC：vpc-peering
   - 目的地址：10.1.0.0/16
   - 下一跳类型：对等连接
   - 下一跳：Peering-Test

步骤四：创建弹性服务器

1. 进入**购买弹性云服务器**页面。
2. 根据**表1-10**创建服务器ECS-Test，根据需要设置相关参数。详见**《弹性云服务器用户指南》**。

   虚拟私有云选择vpc-peering，服务器名称设置为ECS-Test。
3. 服务器ECS-Test创建成功后，在其上部署Nginx。

图 1-15 在 ECS-Test 上部署 Nginx



步骤五：创建独享型 ELB 并为其添加 HTTP 监听器和后端服务器组

1. 进入**购买弹性负载均衡页面**。
2. 根据**表1-10**创建独享型负载均衡ELB-Test，根据需要设置相关参数。详见**《弹性负载均衡用户指南》**。
   - 实例规格类型：独享型
   - 所属VPC：vpc-peering
   - 名称：ELB-Test
   - IP类型后端：开启
   - 其他参数根据需要设置。
3. 独享型ELB创建成功后，在ELB-Test中添加HTTP监听器和后端服务器组。

步骤六：将 ECS 添加至 ELB 后端服务器组

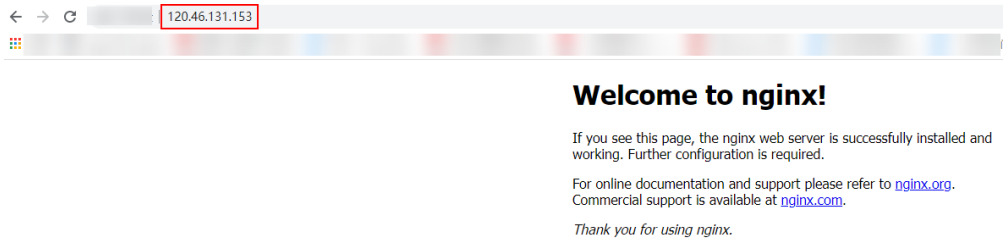
单击上述创建的独享型负载均衡ELB-Test名称。

1. 在监听器“基本信息”页签，在下方后端服务器组界面，单击“查看/添加后端服务器”。
2. 进入右侧“后端服务器组”页面。
3. 在“IP类型后端”右侧，单击“添加”设置相关参数，完成后单击“确定”。详见《弹性负载均衡用户指南》。
   - IP类型后端IP：10.1.0.56（ECS-Test的私网IP）
   - 业务端口：根据后端业务设置
   - 权重：根据需要设置

步骤七：验证通过 IP 类型后端功能添加同 VPC 后端服务器组是否成功

1. 单击上述创建的独享型负载均衡ELB-Test操作列的“更多”。
2. 选择“绑定IPv4公网IP”，给ELB-Test绑定一个弹性公网IP（EIP-Test：120.46.131.153）。
3. 使用浏览器访问“http://120.46.131.153/”，显示如下页面，说明本次访问请求被ELB实例转发到后端服务器“ECS-Test”上，“ECS-Test”正常处理请求并返回请求的页面。

图 1-16 验证通过 IP 类型后端功能添加同 VPC 后端服务器是否成功



1.5 将 ELB 加入弹性伸缩组实现自动添加或移除后端服务器

弹性伸缩能够实现应用系统自动按需调整资源，在业务增长时能够实现自动增加服务器实例的数量，以满足突增的业务需求，在业务下降时能够实现服务器数量自动缩减，以实现保障业务运行的同时节约资源。将ELB加入到弹性伸缩组，弹性伸缩可以根据您设定的策略，自动地增加或减少服务器的数量，在保证您的业务正常运转的同时节约成本。

应用场景

如果您的业务是一个网站，当网站的负载增加时云服务器的CPU使用率会增大，负载降低时CPU使用率会降低。配置两条监控CPU使用率的告警策略，分别在CPU使用率高于70%时增加一台云服务器，在CPU使用率低于30%时减少一台云服务器，保证网站业务始终有合适数量的云服务器，实现自动添加或移除云服务器的功能。

操作步骤

本实践提供搭建Discuz!论坛的配置示例。

表 1-11 搭建 Discuz!论坛步骤

任务	分类	子任务描述	说明
搭建网站	申请服务	申请虚拟私有云	申请为云服务器提供网络服务的虚拟私有云vpc-DISCUZ。
		购买弹性公网IP	需申请使云服务器和互联网互通的弹性公网IP。
		创建安全组并添加规则	为了保证论坛的网络安全，需要设置安全组对网络访问进行控制。创建的安全组sg-DISCUZ。
		购买弹性云服务器	需要购买两台弹性云服务器，云服务器discuz01用于部署论坛数据库，discuz02用于部署论坛业务。购买云服务器discuz01时绑定之前购买的弹性公网IP，discuz02暂不绑定弹性公网IP。
	配置服务器	在discuz01上搭建数据库	在discuz01上安装云数据库 RDS for MySQL，启动RDS for MySQL，设置开机自启动。
		在discuz02上部署网站代码	先将discuz01上的弹性公网IP解绑，再绑定至discuz02，在discuz02上部署Web环境和网站代码。
	配置特性	释放弹性公网IP	为了节省弹性公网IP资源，使用负载均衡服务前请先释放discuz02绑定的弹性公网IP。
		创建弹性负载均衡	为了在伸缩组中均衡访问网站的流量，需要购买独享型负载均衡器elb-DISCUZ。
		制作镜像	为了后续增加的云服务器可以自动搭建Web环境和部署网站代码，需要制作discuz02的镜像discuz_centos6.5(40GB)，该镜像在创建伸缩配置时作为私有镜像使用。
创建弹性伸缩	-	创建伸缩配置	伸缩配置是伸缩组内实例（弹性云服务器）的模板，定义了伸缩组内待添加的实例的规格数据。创建伸缩配置as-config-discuz。
		创建伸缩组	伸缩组是云服务器进行伸缩的基本单位，伸缩活动将会以伸缩组为单位进行。创建弹性伸缩组as-group-discuz。
		创建伸缩策略	伸缩策略能够触发伸缩活动，配置两条监控CPU使用率的告警策略，在业务负载增加时增加云服务器数量，在业务负载减少时减少云服务器数量。
		手动移入实例	为保证discuz02可以和后续移入伸缩组中的服务器共同承载论坛业务，需要将discuz02手动移入伸缩组。

任务	分类	子任务描述	说明
		修改最小实例数	最小实例数定义了伸缩组中云服务的最少数量，修改最小实例数为1后，伸缩组至少会保证有一台云服务器。discuz02是手动移入，在实例移除策略中被移出的优先级最低，故修改最小实例数可以保证discuz02在伸缩组中不被移出。
访问网站	验证配置结果	验证网站是否可以正常访问	获取负载均衡服务的弹性公网IP地址，在浏览器中输入http://*弹性公网IP地址*/forum.php进行验证。若可以访问则说明各项配置已生效。

准备工作

- 您可以参考**《搭建Discuz!论坛网站》**完成后端网站业务的搭建。
- 创建独享型ELB实例elb-DISCUZ，且ELB已绑定EIP，ELB所属VPC与弹性伸缩组的保持一致。具体操作，请参见**购买独享型负载均衡器**和**绑定IPv4公网IP**。
- 创建一个后端服务器组，并关联至独享型ELB实例elb-DISCUZ。

步骤一：创建伸缩配置

伸缩配置定义了移入伸缩组的云服务器的规格，为了移入伸缩组的云服务器能自动承载业务，使用镜像discuz_centos6.5(40GB)，并使伸缩配置中的参数和discuz02保持一致。

1. 登录管理控制台，选择“计算 > 弹性伸缩”。
2. 在“伸缩实例”页面，单击“创建伸缩配置”。

   参考**表1-12**进行关键参数配置，未列出的参数选择默认值即可。

表 1-12 伸缩配置关键参数

参数	解释	取值样例
配置模板	选择“使用新模板”，重新选择云服务器类型、vCPUs、内存、镜像、磁盘等参数信息，创建新的弹性伸缩配置。	使用新模板
规格	可以选择多个规格，避免在伸缩时规格售罄的风险。规格使用优先策略包括“选择优先”和“成本优先”，请根据需要选择。	s3.medium.2 s3.large.2
镜像	为伸缩组中移入的实例提供软件和系统应用配置的模板，选择私有镜像discuz_centos6.5(40GB)。	私有镜像 discuz_centos6.5(40GB)
磁盘	为伸缩组中的移入的实例提供存储和存储管理功能。	系统盘 高IO 40GB 数据盘 高IO 100GB

参数	解释	取值样例
安全组	安全组是一个逻辑上的分组，用来实现安全组内和组间弹性云服务器的访问控制，加强弹性云服务器的安全保护。选择安全组sg-DISCUZ。	sg-DISCUZ
弹性公网IP	伸缩组中已经添加了负载均衡后，伸缩配置可以不配置弹性公网IP。系统会自动将加入伸缩组的实例添加到负载均衡上，伸缩组中的实例统一通过负载均衡绑定的弹性公网IP对外提供服务。	不使用

3. 伸缩配置参数配置完成后，单击“立即创建”。

步骤二：创建伸缩组并关联至 ELB 实例

1. 单击“创建弹性伸缩组”。
   参考**表1-13**进行关键参数配置，未列出的参数选择默认值即可。

表 1-13 伸缩组关键参数

参数	解释	取值样例
最大实例数	伸缩组中弹性云服务器数量的最大值。	50
期望实例数	伸缩组中期望的云服务器数量，本实践中要将搭建Discuz!论坛的云服务器手动移入，为避免移入前发生伸缩活动，将期望实例数设置为0。	0
最小实例数	伸缩组中弹性云服务器数量的最小值。	0
虚拟私有云	为伸缩组中的实例提供所使用的网络。必须和云服务器discuz02属于同一VPC。	VPC-DISCUZ
子网	子网可以方便您管理vpc中的网络。选择中申请虚拟私有云时创建的子网。	vpc-test
负载均衡	为伸缩组中的实例均分流量，选择独享型负载均衡器elb-DISCUZ。后端端口配置为需要监听的业务端口，示例中配置为80，权重为1。	使用独享型

参数	解释	取值样例
健康检查方式	健康检查方式选择“负载均衡健康检查”，负载均衡健康检查是通过系统向后端云服务器发起心跳检查的方式来实现的，推荐使用该方式。	负载均衡健康检查

2. 参数配置完后，单击“立即创建”。
3. 返回弹性伸缩组列表，若伸缩组为“已启用”状态，说明伸缩组创建成功。

步骤三：创建伸缩策略

为了能实现云服务器的自动伸缩，配置两条监控CPU使用率的告警策略，在业务负载上升时增加云服务器数量的策略as-policy-discuz01，在业务负载降低时减少云服务器数量的策略as-policy-discuz02。

1. 在已创建的弹性伸缩组“as-group-discuz”所在行，单击操作列的“查看伸缩策略”。
2. 单击“添加伸缩策略”。

   参考**表1-14**配置伸缩策略as-policy-discuz01的参数，当系统连续3次监控到CPU使用率超过70%时，触发伸缩策略as-policy-discuz01，伸缩组会增加一台弹性云服务器。

表 1-14 伸缩策略 as-policy-discuz01 关键参数

参数	解释	取值样例
策略名称	创建伸缩策略的名称。	as-policy-discuz01
策略类型	选择“告警策略”。	告警策略
告警规则	可选择“现在创建”或“使用已有”。	现在创建
告警规则名称	新建告警规则的名称。	as-alarm-cpu-01
监控类型	定义监控指标的类型，是系统支持的或是自定义的。选择“系统监控”。	系统监控
触发条件	选择弹性伸缩支持的监控指标并对监控指标设定告警条件。	CPU使用率最大值 > 70%
监控周期	告警规则刷新告警状态的周期。	5分钟
连续出现次数	触发告警时的采样点数目。	3

参数	解释	取值样例
执行动作	设置伸缩活动执行动作及实例的个数或实例百分比。 执行动作包括： ● 增加 当执行伸缩活动时，向伸缩组增加实例。 ● 减少 当执行伸缩活动时，从伸缩组中减少实例。 ● 设置为 将伸缩组中的期望实例数设置为固定值。	增加1个实例
冷却时间	为了避免告警策略频繁触发，必须设置冷却时间。	900

3. 单击“确定”。
4. 再次单击“添加伸缩策略”，配置伸缩策略as-policy-discuz02的参数，当系统连续3次监控到CPU使用率低于30%时，触发伸缩策略as-policy-discuz02，伸缩组会减少一台弹性云服务器。
5. 单击“确定”。
6. 返回伸缩策略列表页面，若伸缩策略为“已启用”状态，说明伸缩策略创建成功。

步骤四：将云服务器移入伸缩组

将云服务器discuz02移入伸缩组。

1. 单击伸缩组as-group-discuz名称进入伸缩组详情页面。
2. 切换到“伸缩实例”页签，将discuz02手动移入伸缩组中。

步骤五：修改最小实例数

为保证discuz02不被伸缩活动移出伸缩组，需修改伸缩组的最小实例数。

1. 单击伸缩组as-group-discuz名称，进入伸缩组详情页面。
2. 单击页面右上角的“修改伸缩组”。修改最小实例数为1。
3. 修改完成后，单击“确定”。

步骤六：结果验证

若论坛可以正常使用，当伸缩组中的云服务器CPU使用率持续高于70%（在伸缩组的“监控”页签可对监控指标进行观察），伸缩组会自动增加一台云服务器（在伸缩组的“活动历史”页签可对伸缩活动历史进行查看）。当伸缩组中的云服务器CPU使用率持续低于30%，且伸缩组中至少存在两台云服务器时，伸缩组会自动减少一台云服务器，则本次实践是成功的。若不然，请联系技术支持定位伸缩组不能正常进行伸缩活动的原因。

相关文档

- 当应用场景有变化，需要在云服务器上部署新的软件时，可使用弹性伸缩的生命周期挂钩功能，在实例加入和移出伸缩组时进行自定义操作，灵活地管理加入或移出弹性伸缩组的实例。具体操作可参见**生命周期挂钩**。
- 当所需的弹性云服务器的规格变更时，可创建新的伸缩配置，操作可参考**使用新模板创建伸缩配置**。创建完成后，可参考**为伸缩组更换伸缩配置**，即可改变伸缩组新加入实例的规格。

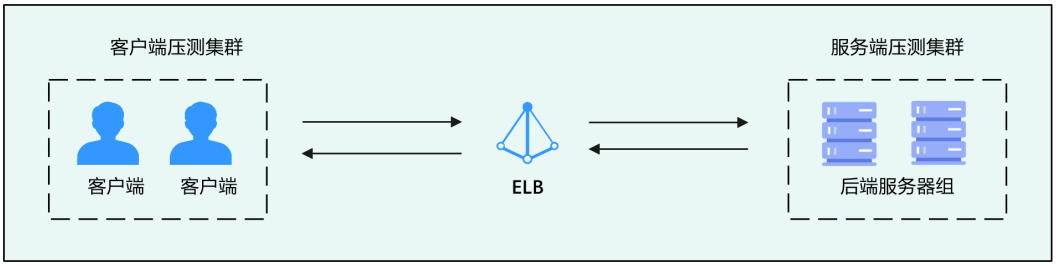
1.6 ELB 压测方案

通过ELB您可以进行大规模的业务流量负载，ELB的性能和稳定性将决定业务是否可以正常运行。在使用ELB承接真实业务流量前，可以通过对ELB进行压测提前模拟极端业务场景，确保ELB在真实业务转发中高可用。

压测方案架构

压测方案参考架构如**图1-17**。

图 1-17 压测方案架构



压测方案

- **TCP/TLS压测指标**

  压测TCP/TLS监听器转发的业务时，通常有如**表1-15**中的3个关键指标可以参考，监控详情请参考**弹性负载均衡监控指标说明**。

  表 1-15 TCP/TLS 监听器压测参考指标说明

指标名称	压测建议
新建连接数	建议使用短连接业务进行压测，测试负载均衡与后端服务器对新建连接的处理能力。
并发连接数	建议使用长连接业务进行压测，测试负载均衡与后端服务器对并发连接的处理能力。
带宽	建议压测业务使用大包，测试负载均衡处理带宽的能力，以确保在实际应用中能够稳定高效地处理大流量。

- **HTTP/HTTPS压测指标**

  压测HTTP/HTTPS监听器转发的业务时，通常有如**表1-16**中的4个关键指标可以参考，监控详情请参考**弹性负载均衡监控指标说明**。

表 1-16 HTTP/HTTPS 监听器压测参考指标说明

指标名称	压测建议
新建连接数	建议使用短连接业务进行压测，测试负载均衡与后端服务器对新建连接的处理能力。
并发连接数	建议使用长连接业务进行压测，测试负载均衡与后端服务器对并发连接的处理能力。
带宽	建议压测业务使用大包，测试负载均衡处理带宽的能力，以确保在实际应用中能够稳定高效地处理大流量。
每秒查询速率（QPS）	建议压测业务配置较大的请求速率，测试负载均衡与后端服务器处理请求的能力。

- **后端服务器组配置**
  - 推荐使用“云服务器”作为压测的后端服务器。使用“IP类型后端”的后端服务器存在部分约束，详情请参考。
  - 不建议流量分配策略使用“源IP算法”和开启会话保持功能，因为该配置下单个客户端的并发连接会集中在1个后端服务器上，造成后端服务器负载压力不均。

压测工具建议

建议您使用华为云性能测试（CodeArts PerfTest）服务进行压测，性能测试服务支持快速模拟大规模并发用户的业务高峰场景，可以支持报文内容和时序自定义、多事务组合的复杂场景测试，测试完成后会为您提供专业的测试报告。

压测示例

本实践以压测HTTP监听器进行举例。

创建后端协议为HTTP的后端服务器组，并将两台ECS添加至后端服务器组中，业务端口均设置为80端口。

创建一个独享型ELB实例（网络型和应用型），添加HTTP监听器并设置转发至的后端服务器组。

两台ECS的基础配置如下**表1-17**。

表 1-17 ECS 基础配置

vCPUs	4vCPUs
内存	8GiB
操作系统	Huawei Cloud EulerOS 2.0 标准版 64位(10GiB)

操作步骤

1. 分别远程登录两台ECS，参考以下步骤安装HTTP服务。

a. 安装Nginx。
```
yum install -y nginx
```
b. 初始化默认页面。
```
echo "performance test" > /usr/share/nginx/html/index.html
```
c. Nginx默认监听TCP 80端口，您可以根据压测需要修改/etc/nginx/nginx.conf来监听更多端口。
d. 启动HTTP服务。
```
systemctl start nginx
```
e. 执行以下任一条命令，确认访问HTTP服务正常（默认为80端口）。
```
curl -X GET http://localhost 或者 curl -X GET http://127.0.0.1:80
```

2. 在CodeArts服务中进行流量压测，具体操作请参考。

压测性能不佳常见问题

- **后端服务器存在CPU性能瓶颈**

  后端服务器的CPU性能存在瓶颈，会导致压测性能较低。

  解决方案：排查压测过程中所有后端服务器的CPU使用率，提高后端服务器的性能规格。

- **部署业务依赖的应用存在性能瓶颈**

  客户端请求经过负载均衡转发到后端服务器后，由于后端服务器的业务应用可能会依赖其他服务（例如，数据库、DNS等），而这些服务存的性能瓶颈也会导致压测性能低。

  解决方案：排查后端服务器部署的整个业务流程并消除每个环节的瓶颈点。

- **端口不足**

  客户端或者服务端端口资源不足可能会导致无法压测到较高的并发连接。

  解决方案：排查以下可能原因并采取对应的建议措施：

  - 主动关闭TCP连接一方的连接会进入TIME_WAIT状态，大量TIME_WAIT状态的连接会导致端口耗尽。

    建议：

    i. 压测业务配置改为长连接，避免频繁新建和关闭连接。
    ii. 设置sysctl -w net.ipv4.tcp_tw_reuse=1，允许TIME_WAIT连接复用。
    iii. 客户端设置sysctl -w net.ipv4.ip_local_port_range="1024 65535"，扩大端口资源，缓解端口耗尽问题。
  - 压测使用的客户端和后端服务器数量有限，导致端口资源不足。

    建议：增加客户端和后端服务器的数量。

2 安全防护

2.1 ELB 安全最佳实践

1. **建议合理地使用身份凭证，提升账号安全。**

   无论用户通过ELB控制台还是API、SDK访问ELB，都会要求访问请求方出示身份凭证，并进行身份合法性校验，同时提供登录保护和登录验证策略加固身份认证安全。ELB服务基于统一身份认证服务（Identity and Access Management，IAM），支持四种身份认证方式：用户名密码、访问密钥、临时访问密钥、AccessCode凭证。同时还提供**登录保护**及**登录验证策略**。

   a. 建议使用临时AK/SK进行业务处理，减小凭证泄露导致数据泄露的风险。

      使用ELB API或SDK查询指标、告警等资源时，都需要进行身份凭证认证，用于确保请求的机密性、完整性和请求者身份的正确性。建议您为应用程序或服务配置IAM委托或临时AK/SK，通过IAM委托可以获取一组临时AK/SK，临时AK/SK到期自动过期失效，可以有效降低凭证泄露造成的数据泄露风险。详情请参见**临时访问密钥**和**通过委托获取临时AK/SK**。

   b. 定期轮转永久AK/SK减小凭证泄漏导致数据泄露的风险。

   c. 定期修改用户名密码，避免使用弱密码。

      定期重置密码是提高系统和应用程序安全性的重要措施之一，不仅可以降低密码泄露的风险，还可以帮助用户满足合规要求，减少安全威胁，提高用户的安全意识。同时建议您提高配置密码的复杂度，避免使用弱密码。详情请参见**密码策略**。

2. **建议针对不同的用户授予不同的API的管理权限。**

   ELB的API的权限管理，参见**ELB权限管理**和**ELB权限授权项说明**。

3. **建议关闭API接口的“证书私钥显示”功能。**

   在业务在使用ELB的HTTPS监听器/TLS监听器时，需要用户首先将证书托管到ELB服务，ELB服务查询证书的API能够返回证书和私钥。如果证书API授权不合理，容易导致私钥泄露，可能引发安全风险。一旦私钥泄露，可能带来攻击者劫持拦截伪造数据的风险。提供如下操作建议：

   a. 关闭“证书私钥显示”功能

      您可以通过API关闭该功能，关闭方法请参见**修改证书私钥字段回显开关**。

   b. 限制用户权限

      所有者将ELB的证书私钥显示开关的API修改禁用。

在IAM权限管理控制台中设置自定义权限策略，示例如下：

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "elb:certificates:setPrivateKeyEcho"
            ]
        }
    ]
}
```

4. **建议设置监听器访问控制，提升访问安全。**

   用户可以通过设置白名单和黑名单的方式控制访问负载均衡监听器的IP。

   通过白名单能够设置允许特定IP访问，而其它IP不许访问。

   通过黑名单能够设置允许特定的IP不能访问，而其它IP允许访问。

   详情参见**访问控制策略**。

5. **建议HTTP监听器重定向到HTTPS监听器，提升业务安全性。**

   将HTTP监听器重定向HTTPS监听器，可以提升业务的安全性，详情请参见**HTTP请求重定向到HTTPS** 。

6. **建议针对高安全的业务，使用HTTPS的双向认证以及自定义TLS安全策略。**

   a. HTTPS双向认证

      一般的HTTPS业务场景只对服务器做认证，因此只需要配置服务器的证书即可。某些关键业务，需要对通信双方的身份都要做认证，以确保业务的安全性。

      此时，除了配置服务器的证书之外，还需要配置客户端的证书，以实现通信双方的双向认证功能。 具体操作，参见**通过ELB部署HTTPS双向认证**。

   b. 自定义TLS安全策略

      对于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。弹性负载均衡默认支持部分常用的TLS安全策略来满足您的安全加密需求。

      在创建和配置HTTPS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。 具体操作，参见**配置TLS安全策略**。

7. **建议开通审计日志功能，记录ELB的操作事件用于审计。**

   云审计服务（Cloud Trace Service，CTS），是华为云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。

   用户开通云审计服务后，ELB可记录ELB的操作事件用于审计。

   a. CTS的详细介绍和开通配置方法，请参见**CTS快速入门**。

   b. ELB支持审计的操作事件请参见**支持审计的关键操作**。

   c. 查看审计日志请参见**查看审计日志**。

8. **建议订阅ELB业务监控的关键告警指标，以防业务过载。**

   云监控（Cloud Eye）服务是面向华为云资源的监控平台，提供了实时监控、及时告警、资源分组、站点监控等能力，使您全面了解云上资源的使用情况和业务的运行状况。

   通过云监控，可以按时间轴查看ELB的网络流量，错误日志相关情况，动态告警分析潜在风险。

关于弹性负载均衡服务支持的监控指标，以及如何创建监控告警规则等内容，请参见**监控弹性负载均衡**。

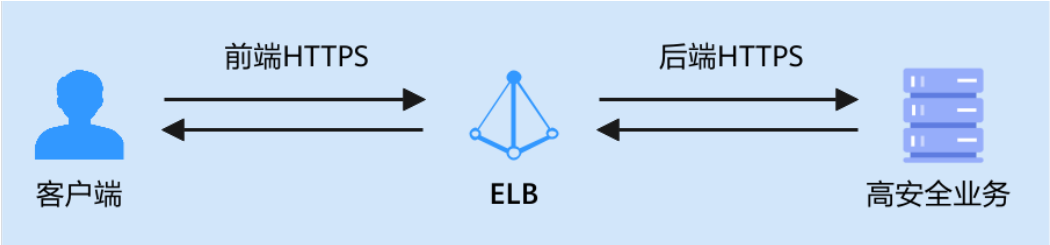
主要业务监控项的告警配置操作，请参见**通过CES监控ELB业务状况并设置告警**。

2.2 通过 ELB 全链路 HTTPS 实现访问加密

应用场景

企业大型核心业务的敏感业务数据（如金融、政务等）对云上传输的安全性要求越来越高，因此在业务通过弹性负载均衡进行负载时，不仅要求客户端请求与负载均衡器之间的通信安全，也要求负载均衡器与后端业务服务器之间的通信安全。通过ELB提供的全链路HTTPS安全加密功能，可以实现业务流量从客户端到后端业务服务器之间的全链路HTTPS加密，同时兼顾性能和运维效率。

图 2-1 全链路 HTTPS



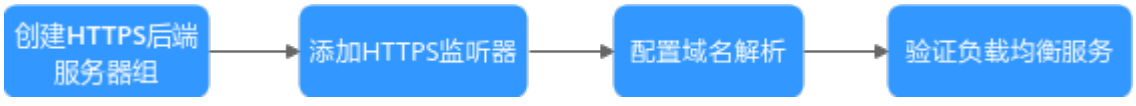
前提条件

- 已创建独享型ELB实例，且ELB已绑定EIP。具体操作，请参见**购买独享型负载均衡器**和**绑定IPv4公网IP**。
- 已购买证书或者上传第三方证书到SSL证书服务并绑定域名。推荐您在华为云云证书与管理服务购买服务器证书，详情请参见**购买SSL证书**。

  将您购买的证书同步到弹性负载均衡控制台，详情请参见**创建证书**。
- 已购买ECS01实例，并且在ECS01中部署了应用服务。部署测试业务详情请参见**搭建后端服务**。

操作流程

图 2-2 配置全链路 HTTPS 业务操作流程



步骤一：创建 HTTPS 后端服务器组

1. 进入**后端服务器组列表页面**。
2. 在后端服务器列表页面，单击页面右上角“创建后端服务器组”按钮。
3. 配置后端分配策略，关键参数详情请参见**表2-1**，其余配置项保持默认值即可。

表 2-1 配置后端分配策略参数说明

参数	示例	说明
名称	**server_group**	创建的后端服务器组的名称。
负载均衡类型	**独享型**	可使用该后端服务器组的负载均衡实例类型。
所属负载均衡器	**关联已有**	使用该后端服务器组的负载均衡实例。 单击“关联已有”后，选择您已创建完成的负载均衡实例。
后端协议	**HTTPS**	后端云服务器自身提供的网络服务的协议。 本实践方案选择HTTPS协议。
分配策略类型	**加权轮询算法**	负载均衡采用的算法，本实践方案保持默认的加权轮询算法。 加权轮询算法：根据后端服务器的权重，按顺序依次将请求分发给不同的服务器，权重大的后端服务器被分配的概率高。 更多关于分配策略的信息，请参见**配置流量分配策略分发流量**。

4. 单击“下一步”，添加后端服务器并配置健康检查。
5. 单击“添加云服务器”，选择您已创建好的ECS01实例，设置业务端口为443端口，其余选项保持默认，完成云服务器的添加。
6. 开启健康检查，其余健康检查参数保持默认。
7. 单击“下一步”。
8. 确认配置无误后，单击“立即创建”。

步骤二：添加 HTTPS 监听器

1. 进入**弹性负载均衡列表页面**。
2. 在目标弹性负载均衡实例的操作列，单击“添加监听器”。
3. 在添加监听器页面，前端协议选择“HTTPS”。

图 2-3 添加 HTTPS 监听器并配置单向认证

4. 单击“下一步：配置后端分配策略”，后端服务器组参数选择“使用已有”。选择已经创建完成的服务器组，完成后单击“下一步：确认配置”。
5. 确认配置参数后，单击“提交”，完成HTTPS监听器的创建。

步骤三：配置域名解析

通过为域名添加A类型记录集解析，将域名解析到ELB的公网地址，使得客户端可以通过公网域名访问ELB。

以下提供将网站域名解析至IPv4地址的配置示例，更多关于A类型记录集的配置指导，请参考**配置网站解析**。

1. 进入**云解析服务控制台**。
2. 在左侧树状导航栏，选择“公网域名”。
   进入域名列表页面。
3. 在待添加记录集的公网域名所在行，单击操作列的“管理解析”。
4. 单击“添加记录集”，进入“添加记录集”页面。
5. 设置记录集参数，如**表2-2**所示。

表 2-2 A 类型记录集参数说明

参数	示例	说明
记录类型	**A – 将域名指向IPv4地址**	记录集的类型，本实践为**A – 将域名指向IPv4地址**。
主机记录	**www**	您域名的前缀。
线路类型	**全网默认**	解析的线路类型用于DNS服务器在解析域名时，根据访问者的来源，返回对应的服务器IP地址。 默认值为“全网默认”。 全网默认：默认线路类型，当未根据访问者来源设置解析线路时，系统会返回默认解析结果。
TTL(秒)	**300**	解析记录在本地DNS服务器的缓存时间，以秒为单位。 本实践使用默认值300秒。
记录值	**192.168.12.2**	域名对应的IPv4地址，本实践为ELB绑定的弹性公网IP地址。
高级配置（可选）	-	您可以单击 ，展开折叠的高级配置区域，设置记录集的别名和权重并添加标签和描述，本文保持默认设置。

6. 单击“确定”。
7. 返回“解析记录”页面。

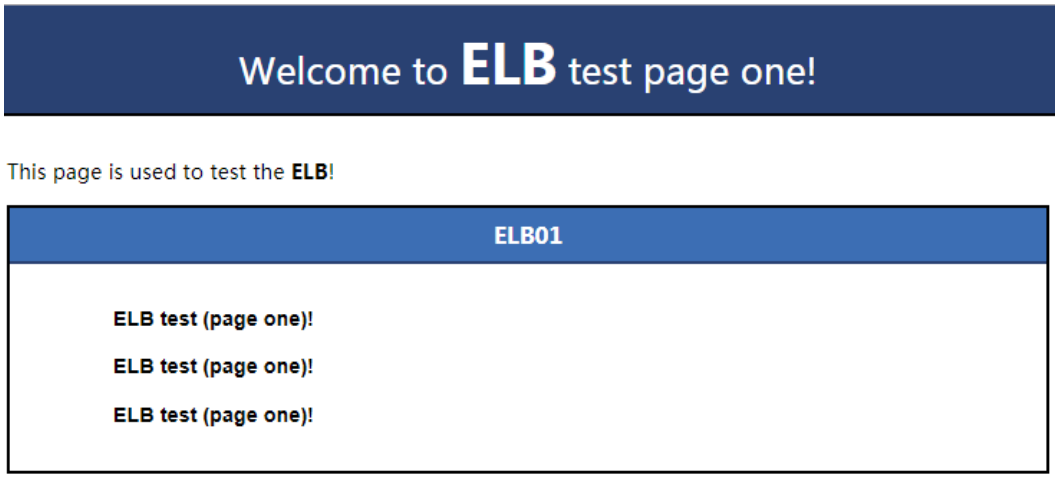
   添加完成后，您可以在域名对应的记录集列表中查看已添加的记录集。当记录集的状态显示为“正常”时，表示记录集添加成功。

步骤四：验证负载均衡服务

ECS实例上分别部署应用，使访问ECS01时返回标题为“Welcome to ELB test page one!”的页面。详细操作，您可参考**搭建后端服务**。

通过浏览器访问**ELB绑定的域名**“https://ELB的域名”，显示如下页面，说明本次访问请求被ELB实例转发到弹性云服务器"ECS01"，全链路HTTPS应用部署成功。

图 2-4 访问到 ECS01



2.3 将独享 WAF 接入 ELB 以增强 Web 业务安全防护能力

应用场景

如果您的业务服务器部署在华为云，您可以将WAF独享引擎实例接入应用型ELB，对重要的域名或仅有IP的Web服务进行防护。

HTTP(S)请求经由ELB转发后会先经过WAF，恶意攻击流量在WAF上被检测过滤，而正常流量转发给后端服务器，从而确保Web业务的安全、稳定、可用。

本文档将介绍通过将独享WAF实例添加到应用型ELB，增强Web业务的防护能力。

约束与限制

- 后端服务器所在安全组需放行独享型ELB实例所在的后端子网地址和业务端口，详情请参见**配置后端服务器的安全组（独享型）**。
- 独享WAF实例所在的安全组已放通相关端口，详细操作请参见**添加安全组规则**。

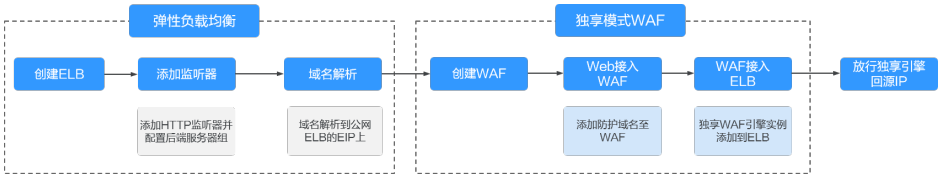
流量路径说明

应用型ELB接入独享WAF对Web业务进行防护后，流量路径如**图2-5**所示。

图 2-5 流量路径图

操作流程

图 2-6 独享 WAF 接入应用型 ELB 的操作流程

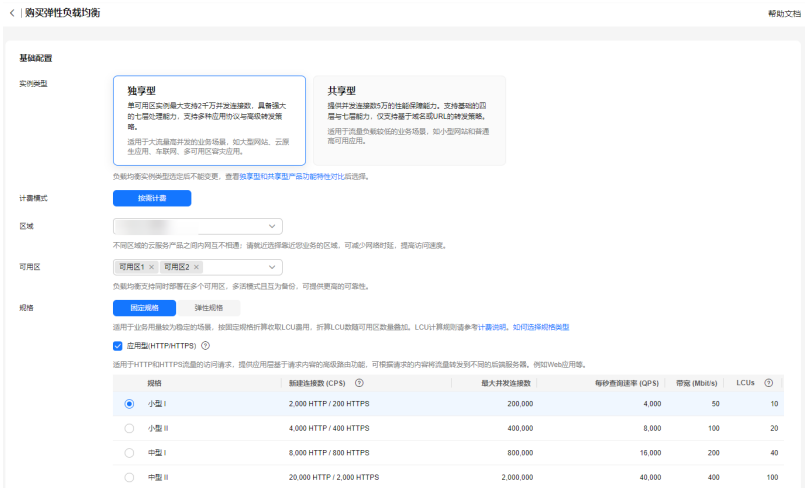


步骤一：创建应用型负载均衡器

1. 进入**弹性负载均衡列表页面**。
2. 在“负载均衡器”界面单击“购买弹性负载均衡器”，购买详情请参考**创建独享型负载均衡器**。

   根据界面提示选择负载均衡器的基础配置，如图所示选择“应用型”规格实例。

   图 2-7 创建应用型负载均衡器（独享型）



3. 选定负载均衡器的规格后，请根据界面提示选择负载均衡器的网络配置。

   网络类型需选择“IPv4公网”，并为负载均衡器选定弹性公网IP，以便接收公网请求。

   图 2-8 为负载均衡器配置弹性公网 IP

4. 确认配置信息，单击“立即购买”，完成创建。

步骤二：添加 HTTP 监听器并配置后端服务器组

1. 进入**弹性负载均衡列表页面**。
2. 在“负载均衡器”界面，单击**步骤一**中创建的负载均衡名称。
3. 切换到“监听器”页签，单击“添加监听器”，配置HTTP监听器并指定前端端口。
   更多添加详情请参见**添加HTTP监听器**。

图 2-9 添加 HTTP 监听器

4. 单击“下一步：配置后端分配策略”，选择“新创建”后端服务器组。

图 2-10 配置后端服务器组

5. 单击“下一步：添加后端服务器”，添加后端服务器并配置健康检查。
6. 单击“下一步：确认配置”，确认配置无误后，单击“提交”。

步骤三：域名解析到 ELB 的弹性公网 IP

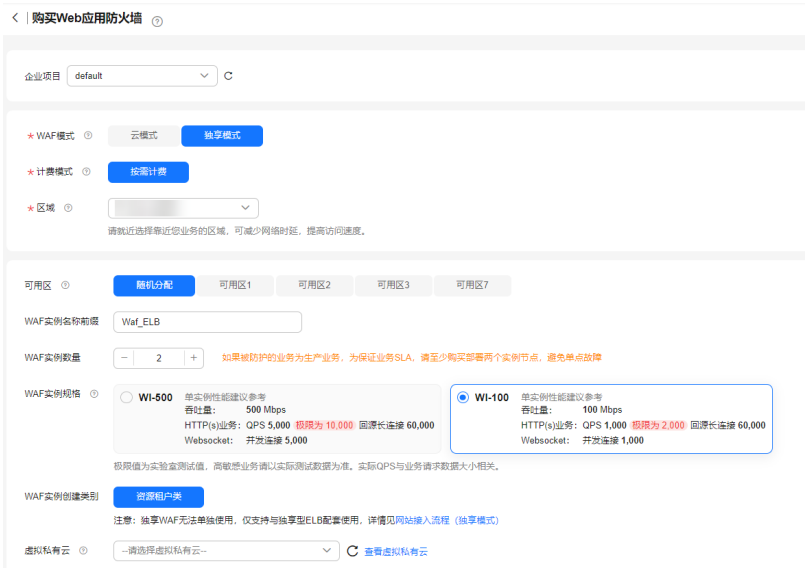
负载均衡器配置完成后，将目标域名如：www.example.com解析到创建的ELB实例的弹性公网IP上，实现对访问域名请求的均衡转发。

在您的实际业务中建议使用华为云云解析服务DNS完成域名解析，具体操作参见**配置网站解析**。

步骤四：创建独享模式 WAF 实例

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“安全与合规 > Web应用防火墙 WAF”。
4. 在页面的右上角，单击“购买WAF实例”。根据界面提示选择WAF实例的配置，如图所示选择“独享模式”。

图 2-11 创建独享模式 WAF 实例



说明

当前独享模式的WAF实例已不支持购买，仅支持已购买的独享模式WAF实例继续使用。

5. 确认配置信息，完成创建。

步骤五：Web 业务接入 WAF

将网站“www.example.com”接入WAF，更多配置详情参见**添加防护网站（独享模式）**。

1. 登录管理控制台。

2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“安全与合规 > Web应用防火墙 WAF”。
4. 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。
5. 在网站列表左上角，单击“添加防护网站”。
   在弹窗中选择“独享模式”并单击“确定”。

图 2-12 添加防护域名

6. 确认高级配置，“是否已使用代理”请选择“七层代理”。

图 2-13 确认高级配置

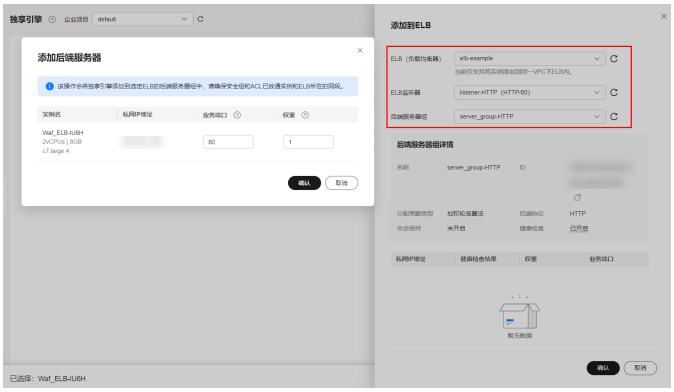
步骤六：WAF 实例接入 ELB

将独享WAF实例添加到ELB的后端服务器组中，请确保安全组和ACL已放通实例和ELB所在的网段。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“安全与合规 > Web应用防火墙 WAF”。

4. 在左侧导航树中，选择“系统管理 > 独享引擎”，进入“独享引擎”页面。
5. 在**步骤四**中创建的实例所在行的“操作”列，单击“更多 > 添加到ELB”。
6. 在“添加到ELB”页面，选择**步骤一：创建应用型负载均衡器**和**步骤二：添加HTTP监听器并配置后端服务器组**步骤中创建的“ELB（负载均衡器）”、“ELB监听器”和“后端服务器组”。

图 2-14 WAF 实例添加到 ELB



7. 单击“确认”，为WAF实例配置业务端口，“业务端口”需要配置为WAF独享引擎实例实际监听的业务端口，即**步骤五：Web业务接入WAF**源站配置中的“防护对象端口”。
8. 单击“确认”，完成配置。

步骤七：放行独享引擎回源 IP

网站以“独享模式”成功接入WAF后，所有网站访问请求将先经过负载均衡器然后流转到独享引擎实例进行监控，经独享引擎实例过滤后再返回到源站服务器，流量经独享引擎实例返回源站的过程称为回源。

在服务器看来，接入WAF后所有源IP都会变成独享引擎实例的回源IP（即独享引擎实例对应的子网IP），以防止源站IP暴露后被黑客直接攻击。

源站服务器上的安全软件很容易认为独享引擎的回源IP是恶意IP，有可能触发屏蔽WAF回源IP的操作。一旦WAF的回源IP被屏蔽，WAF的请求将无法得到源站的正常响应，因此，网站以“独享模式”接入WAF防护后，您需要在源站服务器上设置放行创建的独享引擎实例对应的子网IP，不然可能会出现网站打不开或打开极其缓慢等情况。

详细操作步骤请参考**回源到ELB**。

2.4 使用 DDoS 原生高级防护提升 ELB 防御 DDoS 攻击能力

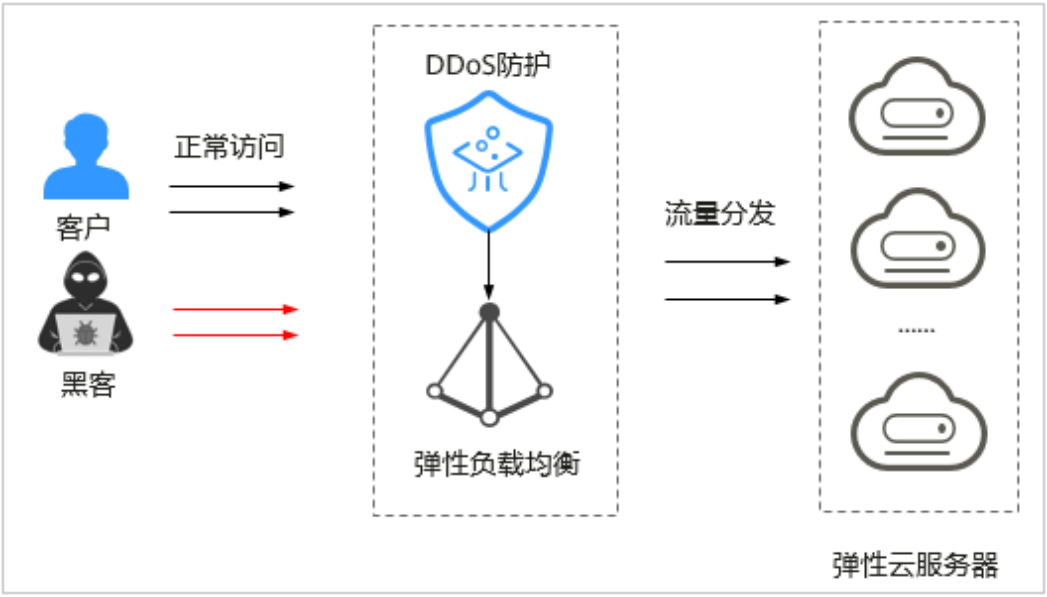
应用场景

DDoS原生高级防护可以提升云服务的DDoS防御能力，确保云服务上的业务安全。通过部署负载均衡ELB，并将ELB的公网IP地址接入DDoS原生高级防护，可以大幅度提高对不同类型DDoS攻击的防御能力。

方案架构

当您的网站类业务部署在华为云ECS上时，您可以为网站业务配置“DDoS原生高级防护+ELB”联动防护，即ECS源站服务器部署ELB后将ELB的公网IP添加到DDoS原生高级防护实例进行防护，进一步提升ECS防御DDoS攻击能力。

图 2-15 华为云“DDoS 原生高级防护+ELB”联动防护



方案优势

相比直接为ECS开启DDoS原生高级防护，“DDoS原生高级防护+ELB”联动防护通过ELB丢弃未监听协议和端口的流量，对不同类型的DDoS攻击（例如，SSDP、NTP、Memcached等反射型攻击、UDP Flood攻击、SYN Flood大包攻击）有更好的防御效果，可以大幅度提升ECS防御DDoS攻击能力，确保用户业务安全、可靠。

资源和成本规划

资源	资源说明	数量	成本说明
弹性负载均衡ELB	用于将访问流量分发到后端ECS服务器，缓解DDoS攻击造成的单点故障。	1	ELB的计费方式及标准请参考**ELB计费说明**。
DDoS原生高级防护	用于接入ELB的公网IP，防护DDoS攻击。	1	DDoS原生高级防护的计费方式及标准请参考**DDoS防护AAD计费说明**。

操作步骤

步骤1 创建一个负载均衡实例，具体操作请参考**购买负载均衡器**。

表 2-3 关键参数说明

参数	说明
“区域”	选择与ECS实例相同的区域。
“弹性公网IP”	选择“现在购买”。
“线路”	选择“全动态BGP”。

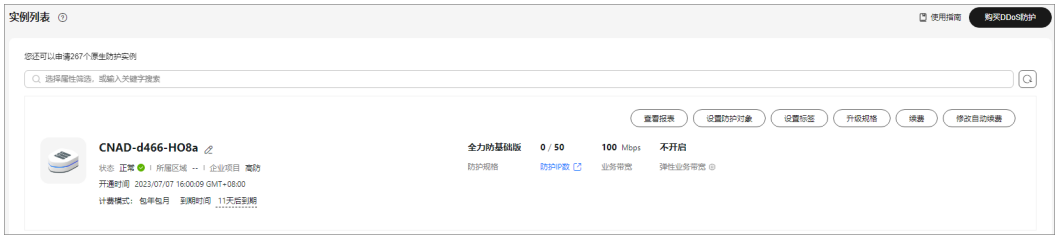
步骤2 获取创建的负载均衡实例的公网IP地址，如图2-16所示。

图 2-16 ELB 实例公网 IP

步骤3 在与ECS实例相同的区域购买DDoS原生高级防护实例。

步骤4 在左侧导航栏选择“DDoS原生高级防护 > 实例列表”，进入DDoS原生高级防护“实例列表”页面。

图 2-17 实例列表



步骤5 在目标实例所在框的右上方，单击“设置防护对象”。

步骤6 在弹出的“设置防护对象”对话框中，勾选步骤2中ELB的EIP后，单击“确定”。

成功添加防护对象后，您可以为防护对象配置防护策略。DDoS原生高级防护将为ECS源站服务器提供DDoS攻击全力防护能力，在业务遭受DDoS攻击时，自动触发流量清洗。

有关配置防护策略的详细操作，请参见添加防护策略。

----结束

2.5 通过 CES 监控 ELB 业务状况并设置告警

应用场景

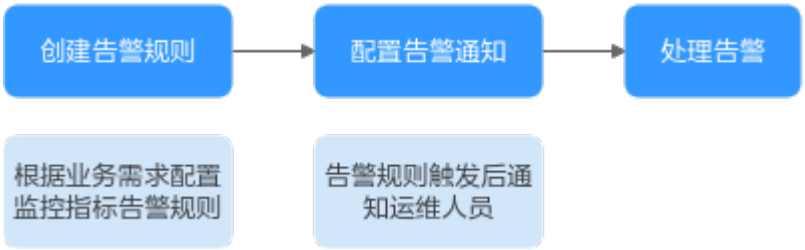
用户在使用ELB的过程中有了解业务负载详情的需求，为使用户更好地掌握ELB的流量负载情况，华为云提供了立体化监控平台云监控服务（CES）。通过云监控服务用户可以执行自动实时监控、告警和通知操作，帮助用户实时掌握通过ELB负载的运行情况。

在自动实时监控的基础上，您可以在云监控服务中设置告警规则，规定在某些特殊情况出现时向您发送告警通知。

您可以参考本实践设置基础业务场景的监控指标，监控阈值可以动态调整，但是不建议高于推荐指标的阈值。

操作流程

图 2-18 通过 CES 监控 ELB 业务设置告警规则流程



创建监控告警规则和通知

当监控指标触发设定的阈值或者事件发生时，云监控服务会在第一时间通过消息通知服务实时告知您云上资源异常，以免因此造成业务损失。

1. 登录**云监控服务管理控制台**。
2. 选择“告警 > 告警规则”。
3. 单击“创建告警规则”。
4. 在“创建告警规则”界面，根据界面提示配置参数。
   a. 根据界面提示，配置告警规则的基本信息

表 2-4 配置规则信息

参数	参数说明	取值样例
名称	系统会随机产生一个名称，用户也可以进行修改。	alarm-elb
描述	告警规则描述（此参数非必填项）。	-

   b. 选择监控对象，配置告警内容参数。

表 2-5 配置告警内容

参数	参数说明	取值样例
告警类型	告警规则适用的告警类型。	指标
云产品	当告警类型选择指标时，需配置告警规则监控的服务名称。 弹性负载均衡支持的监控指标，请参见**云产品监控指标**。	弹性负载均衡-弹性负载均衡

参数	参数说明	取值样例
资源层级	当告警类型选择指标时，需选择告警规则的资源层级，可选择云产品或子维度，推荐选择云产品。 在弹性负载均衡服务中，指标划分了多个子维度（包含弹性负载均衡、监听器、后端主机组、可用区等）。	云产品
监控范围	当告警类型选择指标时，需选择告警规则适用的资源范围，可选择全部资源、资源分组或指定资源。 **说明** • 选择“全部资源”时，则当前云产品下任何资源满足告警策略时，都会触发告警。可单击“选择排除资源”排除不需要监控的资源。 • 选择“资源分组”时，该分组下任何资源满足告警策略时，都会触发告警。可单击“选择排除资源”排除不需要监控的资源。 • 选择“指定资源”时，在“监控对象”单击“选择指定资源”进行指定资源的选择。	全部资源
触发规则	• 自定义创建：自定义创建告警策略，当监控指标满足告警策略则发送告警。 • 关联模板：选择关联模板后，所关联模板内容修改后，该告警规则中所包含策略也会跟随修改。	自定义创建
告警策略	当监控指标在一定周期内多次触发告警策略的阈值时，系统将向用户发送告警通知。 监控指标详情配置请参见**基础场景推荐监控指标（独享型）**或**基础场景推荐监控指标（共享型）**。 **说明** 告警规则内最多可添加50条告警策略，若其中一条告警策略达到条件都会触发告警。	-
告警级别	根据告警的严重程度不同等级，可选择紧急、重要、次要、提示。	-

c. 根据界面提示，配置**告警通知**参数。

图 2-19 配置告警通知

表 2-6 配置告警通知

参数	参数说明
发送通知	配置是否发送短信、邮件、语音通知、HTTP、HTTPS、FunctionGraph（函数）、FunctionGraph（工作流）、企业微信、钉钉、飞书或Welink通知用户。
通知方式	根据需要可选择通知组或主题订阅的方式。 ● 通知组的通知内容模板在云监控服务配置。 ● 主题订阅的通知内容模板需要在消息通知服务配置。
通知策略	当通知方式选择通知策略时，需要选择告警通知的策略。通知策略是包含通知组选择、生效时间、通知内容模板等参数的组合编排。
通知组	当通知方式选择通知组时，需要选择发送告警通知的通知组。
通知对象	当通知方式选择主题订阅时，需要发送告警通知的对象，可选择云账号联系人或主题名称。 ● 云账号联系人为注册时的手机和邮箱。 ● 主题是消息发布或客户端订阅通知的特定事件类型，若此处没有需要的主题则需先创建主题并添加订阅，创建主题并添加订阅请参见**创建主题**、**添加订阅**。
通知内容模板	当通知方式选择通知组或主题订阅时，可选择已有模板或创建通知内容模板。
生效时间	当通知方式选择通知组或主题订阅时，需要设置生效时间。 该告警仅在生效时间段发送通知消息，非生效时段则在隔日生效时段发送通知消息。 如生效时间为08:00-20:00，则该告警规则仅在08:00-20:00发送通知消息。
触发条件	当通知方式选择通知组或主题订阅时，需要设置触发条件。 可以选择“出现告警”、“恢复正常”两种状态，作为触发告警通知的条件。

d. 根据界面提示，配置归属企业项目和标签。

表 2-7 配置规则信息

参数	参数说明
归属企业项目	告警规则所属的企业项目。只有拥有该企业项目权限的用户才可以查看和管理该告警规则。
标签	标签由键值对组成，用于标识云资源，可对云资源进行分类和搜索。 ● 键的长度最大128字符，值的长度最大225字符。 ● 最多可创建20个标签。

e. 配置完成后，单击“立即创建”，完成告警规则的创建。

告警规则添加完成后，当监控指标触发设定的阈值时，云监控服务会在第一时间通过消息通知服务实时告知您云上资源异常，以免因此造成业务损失。

基础场景推荐监控指标（独享型）

推荐您将以下监控指标作为独享型负载均衡使用的基础业务场景告警监控。

独享型负载均衡支持的监控指标详情请参考**监控指标详情**。

性能监控场景

您可通过配置关键使用率指标告警快速识别业务流量是否超限。

告警处理建议：及时通过**变更ELB实例规格和增加实例可用区**进行扩容。

表 2-8 性能监控指标推荐

监控指标			**告警策略**				
指标ID	指标名称	监控对象	指标值类型	连续触发次数	比较关系	阈值	告警周期
l4_ncps_usage	4层新建连接数使用率	• 弹性负载均衡 • 弹性负载均衡-可用区	原始值	3	>	紧急：80%	1小时
l4_con_usage	4层并发连接数使用率	• 弹性负载均衡 • 弹性负载均衡-可用区	原始值	3	>	紧急：80%	1小时
l4_in_bps_usage	4层入带宽使用率	• 弹性负载均衡 • 弹性负载均衡-可用区	原始值	3	>	重要：80%	1小时
l4_out_bps_usage	4层出带宽使用率	• 弹性负载均衡 • 弹性负载均衡-可用区	原始值	3	>	重要：80%	1小时

监控指标			告警策略				
l7_ncps_usage	7层新建连接数使用率	• 弹性负载均衡 • 弹性负载均衡-可用区	原始值	3	>	紧急：80%	1小时
l7_con_usage	7层并发连接数使用率	• 弹性负载均衡 • 弹性负载均衡-可用区	原始值	3	>	紧急：80%	1小时
l7_qps_usage	7层查询速率使用率	• 弹性负载均衡 • 弹性负载均衡-可用区	原始值	3	>	紧急：80%	1小时
l7_in_bps_usage	7层入带宽使用率	• 弹性负载均衡 • 弹性负载均衡-可用区	原始值	3	>	重要：80%	1小时
l7_out_bps_usage	7层出带宽使用率	• 弹性负载均衡 • 弹性负载均衡-可用区	原始值	3	>	重要：80%	1小时
dropped_connections	丢弃连接数	弹性负载均衡	原始值	1	>	紧急：0	1小时
dropped_packets	丢弃数据包	弹性负载均衡	原始值	1	>	紧急：0	1小时
dropped_traffic	丢弃网络带宽	弹性负载均衡	原始值	1	>	紧急：0	1小时

七层业务监控

您可通过配置指标**7层协议返回码**等告警快速识别7层业务请求是否被正确处理。

告警处理建议：通过**访问日志**排查业务情况。

表 2-9 七层业务监控指标推荐

监控指标			告警策略				
指标ID	指标名称	测量对象	指标值类型	连续触发次数	比较关系	阈值	告警周期
mb_l7_qps	7层查询速率	弹性负载均衡-监听器	原始值	1	环比波动	重要：20%	1小时
mc_l7_http_2xx	7层协议响应状态码（2XX）	弹性负载均衡-监听器	原始值	1	环比波动	重要：20%	1小时
me_l7_http_4xx	7层协议响应状态码（4XX）	弹性负载均衡-监听器	原始值	1	环比波动	重要：20%	1小时
mf_l7_http_5xx	7层协议响应状态码（5XX）	弹性负载均衡-监听器	原始值	1	环比波动	重要：20%	1小时
m14_l7_rt	7层协议RT平均值	弹性负载均衡-监听器	原始值	1	环比波动	重要：20%	1小时
m15_l7_upstream_4xx	7层后端响应状态码（4XX）	弹性负载均衡-监听器	原始值	1	环比波动	重要：20%	1小时
m16_l7_upstream_5xx	7层后端响应状态码（5XX）	弹性负载均衡-监听器	原始值	1	环比波动	重要：20%	1小时

后端服务器健康状况

您可通过配置指标**异常主机数**告警及时获取后端服务器的健康状况。

告警处理建议：请及时排查**后端服务器异常原因**。

表 2-10 服务器健康状况监控指标推荐

监控指标			告警策略				
指标ID	指标名称	测量对象	指标值类型	连续触发次数	比较关系	阈值	告警周期

监控指标			告警策略				
m9_abnormal_servers	异常主机数	• 弹性负载均衡 • 弹性负载均衡-监听器 • 弹性负载均衡-后端主机组	原始值	1	>	紧急：0	1小时

基础场景推荐监控指标（共享型）

推荐您将以下监控指标作为共享型负载均衡使用的基础业务场景告警监控。

共享型负载均衡支持的监控指标详情请参考**监控指标详情**。

性能监控场景

您可通过配置关键使用率指标告警快速识别业务流量是否超限。

表 2-11 性能监控指标推荐

监控指标			告警策略				
指标ID	指标名称	测量对象	指标值类型	连续触发次数	比较关系	阈值	告警周期
m1_cps	并发连接数	弹性负载均衡	原始值	3	>	紧急：40000	1小时
m4_ncps	新建连接数	弹性负载均衡	原始值	3	>	紧急：4000	1小时

七层业务监控

您可通过配置指标**7层协议返回码**告警快速识别7层业务请求是否被正确处理。

告警处理建议：通过**访问日志**排查业务情况。

表 2-12 七层业务监控指标推荐

监控指标			告警策略				
指标ID	指标名称	测量对象	指标值类型	连续触发次数	比较关系	阈值	告警周期

监控指标			告警策略				
mb_l7_qps	7层查询速率	弹性负载均衡-监听器	原始值	1	环比波动	重要：20%	1小时
m14_l7_rt	7层协议RT平均值	弹性负载均衡-监听器	原始值	1	环比波动	重要：20%	1小时
mc_l7_http_2xx	7层协议响应状态码（2XX）	弹性负载均衡-监听器	原始值	1	环比波动	重要：20%	1小时
me_l7_http_4xx	7层协议响应状态码（4XX）	弹性负载均衡-监听器	原始值	1	环比波动	重要：20%	1小时
mf_l7_http_5xx	7层协议响应状态码（5XX）	弹性负载均衡-监听器	原始值	1	环比波动	重要：20%	1小时
m15_l7_upstream_4xx	7层后端响应状态码（4XX）	弹性负载均衡-监听器	原始值	1	环比波动	重要：20%	1小时
m16_l7_upstream_5xx	7层后端响应状态码（5XX）	弹性负载均衡-监听器	原始值	1	环比波动	重要：20%	1小时

后端服务器健康状况

您可通过配置指标**异常主机数**告警及时获取后端服务器的健康状况。

告警处理建议：请及时排查**后端服务器异常原因**。

表 2-13 服务器健康状况监控指标推荐

监控指标			告警策略				
指标ID	指标名称	测量对象	指标值类型	连续触发次数	比较关系	阈值	告警周期
m9_abnormal_servers	异常主机数	弹性负载均衡	原始值	1	>	紧急：0	1小时

相关文档

- 查看监控指标看板。
- 弹性负载均衡事件监控说明。

2.6 通过 CTS 查询 ELB 的操作记录

应用场景

云审计服务能够为您提供云服务资源的操作记录，记录的信息包括发起操作的用户身份、IP地址、具体的操作内容的信息，以及操作返回的响应信息。根据这些操作记录，您可以很方便地实现安全审计、问题跟踪、资源定位，帮助您更好地规划和利用已有资源、甄别违规或高危操作。

用户开通云审计服务后，可记录ELB的操作事件用于审计。本实践将介绍云审计服务（CTS）记录中相关字段释义。

什么是事件

事件即云审计服务追踪并保存的云服务资源的操作日志，操作包括用户对云服务资源新增、修改、删除等操作。您可以通过“事件”了解到谁在什么时间对系统哪些资源做了什么操作。

什么是管理类追踪器和数据类追踪器

管理追踪器会自动识别并关联当前用户所使用的所有云服务，并将当前用户的所有操作记录在该追踪器中。管理追踪器记录的是管理类事件，即用户对云服务资源新建、修改、删除等操作事件。

数据追踪器会记录用户对OBS桶中的数据操作的详细信息。数据类追踪器记录的是数据类事件，即OBS服务上报的用户对OBS桶中数据的操作事件，例如上传数据、下载数据等。

在 CTS 新版事件列表查看创建 ELB 的审计事件

1. 根据业务需要创建独享型ELB实例，具体操作请参见购买独享型负载均衡器。
2. 登录CTS控制台。
3. 单击左侧导航栏的“事件列表”，进入事件列表信息页面。
4. 在列表上方，可以通过筛选时间范围，查询最近1小时、最近1天、最近1周的操作事件，也可以自定义最近7天内任意时间段的操作事件。
5. 事件列表支持通过高级搜索来查询对应的操作事件，您可以在筛选器组合一个或多个筛选条件，本实践选择“**云服务：ELB**”。

表 2-14 事件筛选参数说明

参数名称	说明
云服务	云服务的名称缩写，**本实践选择云服务：ELB**。 输入的值区分大小写，需全字符匹配，不支持模糊匹配模式。

图 2-20 筛选 ELB 服务的事件

6. 在事件列表页，可以看到存在1的事件记录。
7. 单击事件名称，查看事件记录详情。

图 2-21 创建 ELB 事件详情

8. 在事件列表页面，您还可以导出操作记录文件、刷新列表、设置列表展示信息等。
   a. 在搜索框中输入任意关键字，按下Enter键，可以在事件列表搜索符合条件的数据。
   b. 单击“导出”按钮，云审计服务会将查询结果以.xlsx格式的表格文件导出，该.xlsx文件包含了本次查询结果的所有事件，且最多导出5000条信息。
   c. 单击按钮，可以获取到事件操作记录的最新信息。

d. 单击按钮，可以自定义事件列表的展示信息。启用表格内容折行开关，可让表格内容自动折行，禁用此功能将会截断文本，默认停用此开关。

9. （可选）在新版事件列表页面，单击右上方的“返回旧版”按钮，可切换至旧版事件列表页面。

CTS 记录的字段释义

表 2-15 CTS 记录的字段释义

字段	含义
request	请求体内容，以创建ELB请求为例，即调用创建ELB API传递的完整请求体信息。
trace_id	CTS记录的id。
code	记录用户请求的响应，标识事件对应接口返回的HTTP状态码。
trace_name	查询事件列表对应的事件名称。
resource_type	操作的资源类型，以创建ELB为例，资源类型即为loadbalancer。
trace_rating	标识事件等级，目前有三种。创建ELB成功时，trace_rating即为normal。 • normal：代表本次操作成功。 • warning：代表本次操作失败。 • incident：代表本次操作引起了比失败更严重的后果，比如会造成节点故障或用户业务故障等情况。
message	标识ELB为此条事件添加的备注信息。
source_ip	发起请求的源IP。
domain_id	账号ID。
trace_type	标识事件发生源头类型，主要包括API调用（ApiCall），Console页面调用（ConsoleAction）和系统间调用（SystemAction）。
service_type	查询事件列表对应的云服务类型，ELB服务的service_type即为ELB。
event_type	事件对应的事件类型。
project_id	事件所属的项目ID。
read_only	标记是否为只读请求。增删改请求的read_only均为false，只有读请求是true
resource_id	事件对应的资源id

字段	含义
tracker_name	记录事件对应的追踪器名称。 • 当“trace_type”字段值为“system”时，该字段值默认为“system”。 • 当“trace_type”字段值为“data”时，该字段值为对应数据类追踪器名称。
operation_id	事件对应的操作ID。
resource_account_id	资源所在的账号ID。
time	事件产生的时间戳。
resource_name	资源名称。
user	记录了操作用户的信息。
record_time	云审计服务记录本次事件的时间戳。
user_agent	请求客户端代理标识。
api_version	API版本。
response	请求响应体。
request_id	本次请求的request id, 可用于ELB服务追踪定位问题。

相关文档

- **ELB支持审计的关键操作**
- **通过CTS查询ELB的操作记录**

2.7 配置客户端重试机制提高业务可用性

ELB 的高可用机制

为了实现提高ELB服务的高可用性，推荐用户购买多可用区的实例，同时开启对后端服务器的健康检查功能。

- **系统高可用部署机制**：ELB实例采用多AZ多活的集群化部署，消除了单AZ机房故障的影响，同时实现了AZ内的会话同步，消除了ELB集群单AZ内的服务器单点故障的影响，保证了服务的系统稳定性。
- **健康检查机制**： ELB实例基于用户配置的健康检查探测策略，对后端服务器进行健康检查，能够保证**新连接**能够转发到健康的后端服务器。

客户端重试应用场景

通常情况下，ELB的高可用机制能够应对核心业务的容灾场景。然而，在极端场景下，可能会出现连接reset或超时等问题，影响业务的连续性和用户体验。建议您配置客户

端重试机制，通过重试发起新的连接，特别是支持连接超时、连接reset等异常的重试能力，以提高系统的容错性和稳定性。

在如下的业务场景中，建议配置客户端支持重试的能力：

1. **后端服务器健康检查失败**：ELB实例的后端服务器健康失败，对于异常后端服务器上存量的四层连接，在会话保持/延迟注销时间内，有报文到达ELB后，仍会转发到异常后端服务器。
2. **ELB实例跨可用区流量的高可用切换**：极端场景下如果ELB实例所在的集群发生单可用区整体故障，多可用区部署的ELB实例会将故障可用区内的流量切换到其他正常的可用区。此时，故障可用区内正在传输数据的长连接无法恢复，需要客户端重新发起连接。

重试的重要性

无论是客户端还是服务端，都有可能受到基础设施或者运行环境的影响，遇到暂时性的故障（例如瞬时的网络抖动/磁盘抖动，服务暂时不可用或者调用超时等），从而导致业务访问的超时。

通过设计完备的客户端自动重试机制可以大幅降低此类故障对业务的影响，保障操作最终能成功执行。

后端服务不可用的场景

表 2-16 推荐重试场景

场景	说明
后端服务器异常	后端服务器（ECS/容器），因业务进程夯住、业务进程故障、硬件故障、虚拟化迁移失败、网络不可达等多种故障场景，导致后端服务器健康检查失败。
复杂的网络环境	由于客户端与ELB以及后端服务器之间复杂网络环境引起，可能出现偶发的网络抖动、数据重传等问题，此时，客户端发起的请求可能会出现暂时性失败。
复杂的硬件问题	由于客户端所在的硬件偶发性故障引起，例如虚拟机HA，磁盘时延抖动等场景，此时，客户端发起的请求可能会出现暂时性失败。

推荐的客户端重试准则

表 2-17 客户端重试准则

重试准则	说明
重试触发条件	连接超时、连接reset等异常场景。
仅重试幂等的操作	推荐仅重试支持幂等性的业务。 执行重试可能导致某个操作被重复执行，因此不是所有操作均适合设计重试机制。

重试准则	说明
适当的重试次数与间隔	根据业务需求和实际场景调整适当的重试次数与间隔，否则可能引发下述问题： ● 如果重试次数不足或间隔太长，应用程序可能无法完成操作而导致失败。 ● 如果重试次数过大或间隔过短，应用程序可能会占用过多的系统资源，且可能因请求过多而堵塞在服务器上无法恢复。 常见的重试间隔方式包括立即重试、固定时间重试、指数退避时间重试、随机时间重试等。
避免重试嵌套	重试嵌套可能导致重试时间被指数级放大。
记录重试异常并打印失败报告	在重试过程中，建议在WARN级别上打印重试错误日志，同时，仅在重试失败时打印异常信息。
复用成熟开源生态库重试机制	如成熟的开源中间件软件，有丰富的Client端库，基于其连接池的保活机制和探测机制，设置合理的重试间隔和重试次数、以及退避策略等。 自定义重试机制，可以参考开源生态连接池的保活机制和探测机制。

相关文档

- 配置Redis客户端重试机制
- phpredis重试最佳实践

3 基础功能

3.1 通过 ELB 将 HTTP 请求重定向至 HTTPS

应用场景

HTTPS是加密数据传输协议，安全性高，如果您需要保证业务建立安全连接，可以通过负载均衡的HTTP重定向功能，将客户端的HTTP访问重定向至HTTPS访问ELB。

⚠ 注意

- 因为HTTP标准协议只支持GET和HEAD方法的重定向，所以设置了HTTP重定向至HTTPS后，POST和其他方法会被改为GET方法，这是客户端浏览器的行为，而非ELB修改的。如果您需要实现除GET和HEAD方法以外的访问方式，建议直接使用HTTPS方式进行访问。
- HTTP重定向至HTTPS是指所有的HTTP请求都将转给HTTPS监听器处理为HTTPS请求，但HTTPS请求是通过HTTP被发送给后端服务器的。
- HTTP监听器重定向至HTTPS监听器，HTTPS监听器所关联的后端服务器上不能再安装证书，否则会引起HTTPS请求不生效。

前提条件

- 您已创建ELB实例，本实践将以独享型ELB为例。具体操作，请参见**创建独享型负载均衡器**。
- 您已创建两台ECS实例，ECS与已创建的ELB实例属于同一个VPC。第一台ECS_client用作客户端发送HTTPS请求，第二台ECS_server用作服务器端来处理请求。具体操作，请参见**购买云服务器**。
- 您已在ELB的证书管理控制台创建服务器证书用于创建HTTPS监听器。具体操作，请参见**创建证书**。

操作流程

图 3-1 配置重定向至 HTTPS 监听器操作流程

步骤一：创建 HTTPS 监听器

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要设置重定向的负载均衡名称。
3. 在该负载均衡界面的“监听器”页签，单击“添加监听器”，配置监听器。配置监听器参数参见**表3-1**。

图 3-2 添加 HTTPS 监听器

表 3-1 独享型负载均衡配置 HTTPS 监听器参数说明

参数	示例	说明
前端协议	HTTPS	客户端与负载均衡监听器建立流量分发连接的协议。
监听端口	443	客户端与负载均衡监听器建立流量分发连接的端口。
名称	listener-HTTPS	监听器名称。
获取客户端IP	默认开启	后端服务器可以获取到客户端的真实IP地址。
高级转发策略	开启	高级转发策略支持多样化的转发规则和转发动作，便于灵活地分流业务，合理地分配资源。

参数	示例	说明
访问控制	允许所有IP访问	支持通过白名单和黑名单对特性IP的访问请求进行控制。
SSL解析方式	单向认证	客户端到服务器端认证方式，本实践仅进行服务器端认证。
服务器证书	选择已创建的服务器证书	服务器证书用于SSL握手协商，具有服务器身份验证和加密传输双重功能。
SNI	暂不开启	HTTPS协议的负载均衡可以选择开启SNI，以满足您的多域名访问或关联多个服务器证书的需求。

4. 保持“更多配置（可选）”参数设置默认不变，单击“下一步：配置后端分配策略”。
5. 选择“新创建”后端服务器组，其余参数保持默认不变，单击“下一步：添加后端服务器”。
6. 选择将ECS_server添加到新创建的后端服务器组，开启健康检查并保持默认参数设置不变。
7. 单击“下一步：确认配置”后，单击“提交”，完成HTTPS监听器的创建。

步骤二：创建 HTTP 监听器并同步开启重定向

ELB支持在创建HTTP监听器时开启重定向并选择重定向至的HTTPS监听器，也支持在HTTP监听器创建完成后通过设置转发策略实现重定向的设置。

1. 进入**弹性负载均衡列表页面**。
2. 在“负载均衡器”界面，单击需要设置重定向的负载均衡名称。
3. 在该负载均衡界面的“监听器”页签，单击“添加监听器”，配置监听器。配置监听器参数参见**表3-2**。

图 3-3 添加 HTTP 监听器

表 3-2 独享型负载均衡配置 HTTP 监听器参数说明

参数	示例	说明
前端协议	HTTP	客户端与负载均衡监听器建立流量分发连接的协议。
监听端口	80	客户端与负载均衡监听器建立流量分发连接的端口。
名称（可选）	listener-HTTP	监听器名称。
重定向至监听器	勾选开启并选择**步骤一：创建HTTPS监听器**创建的HTTPS监听器	重定向用于将HTTP监听的流量转发到HTTPS监听，以实现HTTP协议强制跳转HTTPS。
获取客户端IP	默认开启	后端服务器可以获取到客户端的真实IP地址。
高级转发策略	开启	高级转发策略支持多样化的转发规则和转发动作，便于灵活地分流业务，合理的分配资源。
访问控制	允许所有IP访问	支持通过白名单和黑名单对特性IP的访问请求进行控制。

4. 保持“更多配置（可选）”参数设置默认不变，单击“下一步：确认配置”。
5. 单击“提交”，完成HTTP监听器的创建和重定向设置。

说明

- HTTP监听器被重定向，除访问控制以外原有监听器配置会失效。
- HTTP监听器被重定向后，会返回301返回码。

步骤三：验证重定向至 HTTPS

远程登录ECS_client实例，执行curl -H "Accept-Language: zh-CN,zh" "http://ELB的私网IP地址：80" 命令测试ECS_client实例访问ELB的HTTP请求是否能够重定向成功。

如下图所示，如果收到状态码301，表示访问ELB的HTTP请求被重定向至HTTPS监听器。

图 3-4 验证重定向至 HTTPS 监听器

```
]#curl -H "Accepte-Language: zh-CN,zh" 'http://          :80'
<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
</body>
</html>
```

3.2 通过 ELB 部署 HTTPS 单向认证

应用场景

如果您的业务需要向客户端证明服务器端的合法性，而无需对客户端的身份进行额外验证以简化通信流程时，您可以参考本文在ELB中配置HTTPS单向认证。

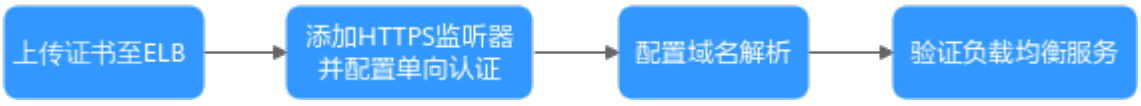
本文使用通过**云证书与管理**服务购买的证书提供身份认证。

前提条件

- 已创建独享型ELB实例，且ELB已绑定EIP。具体操作，请参见**购买独享型负载均衡器**和**绑定IPv4公网IP**。
- 已创建协议类型为HTTPS协议的后端服务器组。服务器组中添加了ECS01实例，并且在ECS01中部署了应用服务。
- 已购买证书或者上传第三方证书到SSL证书服务并绑定公网域名。推荐您在华为云云证书与管理服务购买服务器证书，详情请参见**购买SSL证书**。

操作流程

图 3-5 配置 HTTPS 业务单向认证操作流程



步骤一：上传服务器证书到 ELB 控制台

在ELB添加HTTPS监听器前，您需要将您的证书上传到将ELB控制台。

1. 进入**弹性负载均衡列表页面**。
2. 在左侧导航栏单击“证书管理”。
3. 单击“创建证书”，配置参数请参见**表3-3**。

表 3-3 服务器证书参数说明

参数	说明
证书类型	创建证书的类型，本文选择服务器证书。
证书来源	服务器证书同时支持SSL证书管理服务提供的数字证书和您的自有证书。 本文选择“SSL证书管理”以同步您在华为云云证书与管理服务已经购买的SSL证书。
证书	选择您需要上传到ELB控制台的证书。
企业项目	企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。
SNI扩展域名（可选）	将自动同步SSL证书已绑定的所有域名。 当您的证书用于配置SNI证书时，将支持根据客户端HTTPS请求的域名来选择对应的SNI证书完成认证。
描述	添加对该证书的描述信息，非必填项。

4. 单击“确定”，完成创建。

步骤二：添加 HTTPS 监听器并配置单向认证

1. 进入**弹性负载均衡列表页面**。
2. 在目标弹性负载均衡实例的操作列，单击“添加监听器”。
3. 在添加监听器页面，协议类型选择“HTTPS”，“SSL解析方式”选择“单向认证”，
   在服务器证书的配置项中选择**步骤一**中上传到ELB控制台的服务器证书。

图 3-6 添加 HTTPS 监听器并配置单向认证

4. 单击“下一步：配置后端分配策略”，后端服务器组参数选择“使用已有”。选择已经创建完成的服务器组，完成后单击“下一步：确认配置”。
5. 确认配置参数后，单击“提交”，完成HTTPS监听器的创建。

步骤三：配置域名解析

通过为域名添加A类型记录集解析，将域名解析到ELB的公网地址，使得客户端可以通过公网域名访问ELB。

以下提供将网站域名解析至IPv4地址的配置示例，更多关于A类型记录集的配置指导，请参考**配置网站解析**。

1. 进入**云解析服务控制台**。
2. 在左侧树状导航栏，选择“公网域名”。
   进入域名列表页面。
3. 在待添加记录集的公网域名所在行，单击操作列的“管理解析”。
4. 单击“添加记录集”，进入“添加记录集”页面。
5. 设置记录集参数，如**表3-4**所示。

表 3-4 A 类型记录集参数说明

参数	示例	说明
记录类型	**A – 将域名指向IPv4地址**	记录集的类型，本实践为**A – 将域名指向IPv4地址**。
主机记录	**www**	您域名的前缀。
线路类型	**全网默认**	解析的线路类型用于DNS服务器在解析域名时，根据访问者的来源，返回对应的服务器IP地址。 默认值为“全网默认”。 全网默认：默认线路类型，当未根据访问者来源设置解析线路时，系统会返回默认解析结果。
TTL(秒)	**300**	解析记录在本地DNS服务器的缓存时间，以秒为单位。 本实践使用默认值300秒。
记录值	**192.168.12.2**	域名对应的IPv4地址，本实践为ELB绑定的弹性公网IP地址。
高级配置（可选）	-	您可以单击 ，展开折叠的高级配置区域，设置记录集的别名和权重并添加标签和描述，本文保持默认设置。

6. 单击“确定”。
7. 返回“解析记录”页面。

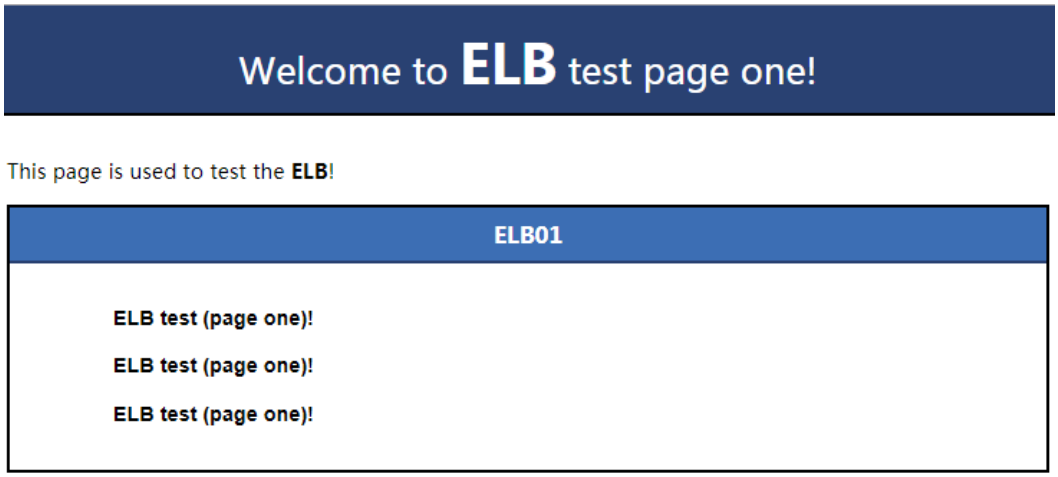
   添加完成后，您可以在域名对应的记录集列表中查看已添加的记录集。当记录集的状态显示为“正常”时，表示记录集添加成功。

步骤四：验证负载均衡服务

ECS实例上分别部署应用，使访问ECS01时返回标题为“Welcome to ELB test page one!”的页面。详细操作，您可参考**搭建后端服务**。

通过浏览器访问**ELB绑定的域名**“https://ELB的域名”，显示如下页面，说明本次访问请求被ELB实例转发到弹性云服务器"ECS01"，HTTPS单向认证应用部署成功。

图 3-7 访问到 ECS01



3.3 通过 ELB 部署 HTTPS 双向认证

应用场景

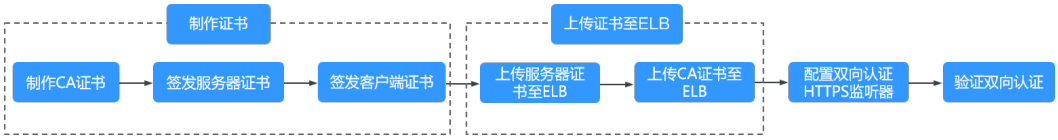
一般的HTTPS业务场景只对服务器做认证，因此只需要配置服务器的证书即可。某些关键业务，需要对通信双方的身份都要做认证，以确保业务的安全性。

此时，除了配置服务器的证书之外，还需要配置客户端的证书，以实现通信双方的双向认证功能。

本章节以自签名证书为例，介绍如何配置HTTPS双向认证。但是自签名证书存在安全隐患，建议客户使用**云证书与管理**服务购买证书、或购买其他权威机构颁发的证书。

操作流程

图 3-8 配置 HTTPS 业务双向认证操作流程



步骤一：使用 OpenSSL 制作 CA 证书

1. 登录到任意一台安装有openssl工具的Linux机器。
2. 创建工作目录并进入该目录。

   mkdir ca

   cd ca
3. 创建CA证书的openssl配置文件ca_cert.conf，内容如下：

```
[ req ]
distinguished_name     = req_distinguished_name
prompt                 = no

[ req_distinguished_name ]
 O                     = ELB
```


4. 创建CA证书私钥文件ca.key。

   openssl genrsa -out ca.key 2048

   图 3-9 生成 CA 证书私钥文件

   ```
   [root@elbv30003 ca]# openssl genrsa -out ca.key 2048
   Generating RSA private key, 2048 bit long modulus (2 primes)
   ............+++++
   ........................+++++
   e is 65537 (0x010001)
   [root@elbv30003 ca]#
   ```

5. 创建CA证书的csr请求文件ca.csr。

   openssl req -out ca.csr -key ca.key -new -config ./ca_cert.conf

6. 创建自签名的CA证书ca.crt。

   openssl x509 -req -in ca.csr -out ca.crt -sha1 -days 5000 -signkey ca.key

   图 3-10 创建自签名 CA 证书

   ```
   [root@elbv30003 ca]# openssl x509 -req -in ca.csr -out ca.crt -sha1 -days 5000 -signkey ca.key
   Signature ok
   subject=O = ELB
   Getting Private key
   [root@elbv30003 ca]#
   ```

步骤二：使用 CA 证书签发服务器证书

用户可以用权威CA签发的证书或者自签名的证书，这里以自签名证书为例说明如何创建服务器证书。

1. 登录到生成CA证书的服务器。
2. 创建与CA平级的目录，并进入该目录。

   mkdir server

   cd server

3. 创建服务器证书的openssl配置文件server_cert.conf，内容如下：

   ```
   [ req ]
   distinguished_name     = req_distinguished_name
   prompt                 = no

   [ req_distinguished_name ]
    O                     = ELB
    CN                    = www.test.com
   ```

   说明

   CN字段可以根据需求改为服务器对应的域名、IP地址。

4. 创建服务器证书私钥文件server.key。

   openssl genrsa -out server.key 2048

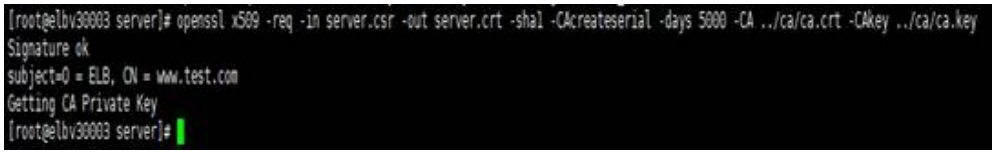
5. 创建服务器证书的csr请求文件server.csr。

   openssl req -out server.csr -key server.key -new -config ./server_cert.conf

6. 使用CA证书签发服务器证书server.crt。

   openssl x509 -req -in server.csr -out server.crt -sha1 -CAcreateserial -days 5000 -CA ../ca/ca.crt -CAkey ../ca/ca.key

图 3-11 签发服务器证书



步骤三：使用 CA 证书签发客户端证书

1. 登录到生成CA证书的服务器。
2. 创建与CA平级的目录，并进入该目录。

   mkdir client

   cd client
3. 创建客户端证书的openssl配置文件client_cert.conf，内容如下：

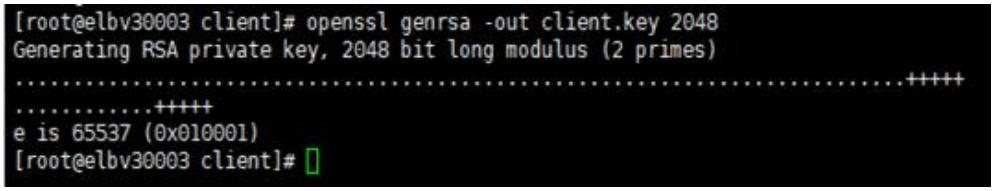
```
[ req ]
distinguished_name     = req_distinguished_name
prompt                 = no

[ req_distinguished_name ]
 O                     = ELB
 CN                    = www.test.com
```

   说明

   CN字段可以根据需求改为对应的域名、IP地址。
4. 创建客户端证书私钥文件client.key。

   openssl genrsa -out client.key 2048

   图 3-12 创建客户端证书私钥文件



5. 创建客户端证书的csr请求文件client.csr。

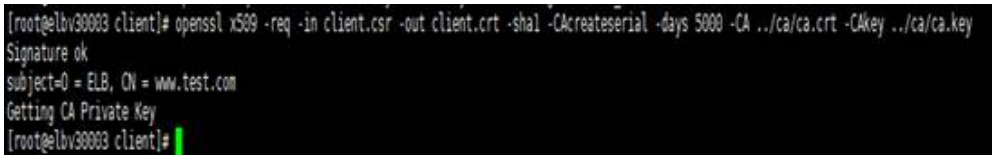
   openssl req -out client.csr -key client.key -new -config ./client_cert.conf

   图 3-13 创建客户端证书 csr 文件

6. 使用CA证书签发客户端证书client.crt。

   openssl x509 -req -in client.csr -out client.crt -sha1 -CAcreateserial -days 5000 -CA ../ca/ca.crt -CAkey ../ca/ca.key

   图 3-14 签发客户端证书



7. 把客户端证书格式转为浏览器可识别的p12格式。

   openssl pkcs12 -export -clcerts -in client.crt -inkey client.key -out client.p12

   说明

   该命令执行时需要输入导出密码，请输入并记住该密码，在证书导入浏览器时需要使用。

步骤四：上传服务器证书到 ELB 控制台

1. 登录负载均衡控制台页面。
2. 单击“证书管理 > 创建证书”。
3. 在创建证书页面，证书类型选择“服务器证书”，同时把前面生成的服务器证书server.crt以及私钥server.key的内容复制到对应的区域，单击“确定”按钮。

   说明

   复制内容时请将最后的换行符删除，避免保存时报错。

   说明

   服务器证书和私钥内容只支持上传pem格式。

步骤五：上传 CA 证书到 ELB 控制台

步骤1 登录负载均衡控制台页面。

步骤2 单击“证书管理 > 创建证书”。

步骤3 在创建证书页面，证书类型选择“CA证书”，同时把**步骤一：使用OpenSSL制作CA证书**创建的客户端CA证书ca.crt的内容复制到证书内容区域，单击“确定”按钮。

说明

复制内容时请将最后的换行符删除，避免保存时报错。

图 3-15 创建 CA 证书

说明

CA证书内容只支持上传pem格式。

----结束

步骤六：配置 HTTPS 双向认证监听器

1. 登录负载均衡控制台页面。
2. 在添加监听器页面，协议类型选择“HTTPS”，“SSL解析方式”选择“双向认证”，并且在服务器证书和CA证书两个配置项中选择所添加的服务器证书和CA证书对应的名称。

图 3-16 添加 HTTPS 监听器并配置双向认证

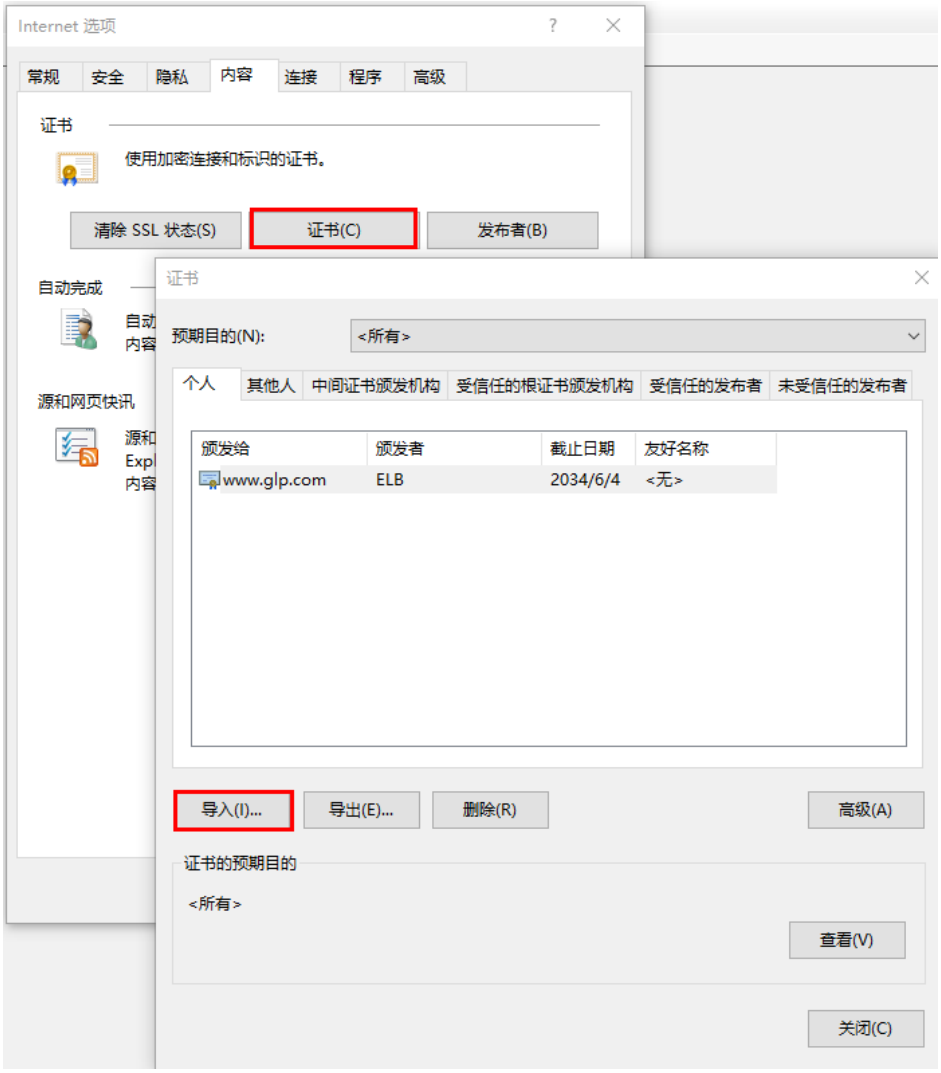
3. 单击“下一步：配置后端分配策略”，后端服务器组参数选择“使用已有”。选择已经创建完成的服务器组，完成后单击“下一步：确认配置”。
4. 确认配置参数后，单击“提交”，完成HTTPS监听器的创建。

步骤七：导入客户端证书并验证

浏览器方式功能测试

1. 浏览器导入客户端证书（以Internet Explorer 11为例说明）
   a. 把客户端证书从Linux机器导出来，即前面签发的client.p12证书文件。
   b. 单击“设置 > Internet选项”，切换到“内容”页签。
   c. 单击“证书”，然后单击“导入”，导入client.p12证书文件。

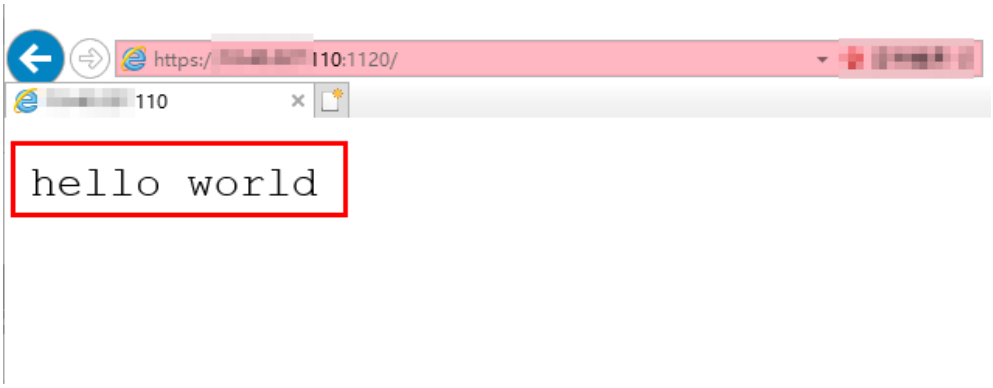
图 3-17 安装 client.p12 证书



2. 测试验证

   在浏览器中输入地址，浏览器会弹出证书选择窗口，如下，选择客户端证书，然后点确定按钮，可以正常访问网站，如图12 正常访问网站。

图 3-18 正常访问网站



Curl工具方式功能测试验证

1. 导入客户端证书

   把客户端证书client.crt和客户端私钥文件client.key拷贝到新目录，如目录/home/client_cert。

2. 测试验证

   在shell界面，输入以下命令，请输入正确的证书地址和密钥文件地址，以及负载均衡器的IP地址和监听器端口(以下用https://XXX.XXX.XXX.XXX:XXX 表示，以实际IP地址和端口为准)。

   ```
   curl -k --cert /home/client_cert/client.crt --key /home/client_cert/client.key https://XXX.XXX.XXX.XXX:XXX/ -I
   ```

   如果可以正确获得响应码，如图3-19说明验证成功。

   图 3-19 正确响应码示例

   ```
   [192.168.10.216  test]#curl -k --cert client.crt --key client.key https://192.168.10.16:4500 -I
   HTTP/1.1 200 OK
   Date: Fri, 25 Sep 2020 10:11:17 GMT
   Content-Type: application/octet-stream
   Connection: keep-alive
   Set-Cookie: name=d92f80b6-55e9-4b61-9c37-932ccd7b02f2; path=/; Expires=Sat, 26-Sep-20 10:11:19 GMT
   Server: elb
   ```

3.4 通过独享型 ELB 实现 TLS 卸载（单向认证）

应用场景

如果您的四层业务对安全性要求较高，可以使用SSL加密来提高业务安全性。然而，在后端服务器上直接配置SSL加密认证会降低您业务的处理效率。您可以通过独享型ELB的TLS监听器进行转发，将证书部署在监听器上，独享型ELB接收加密的流量后会将请求解析为明文再传输至后端服务器，后端服务器无需配置证书。

TLS卸载在提升安全性的同时，也提高了后端服务器的处理效率，简化了后端服务器的配置和运维复杂度，帮助您的四层业务流量实现高效安全的转发。

前提条件

- 已创建独享型ELB实例，且ELB已绑定EIP。具体操作，请参见**购买独享型负载均衡器**和**绑定IPv4公网IP**。
- 已购买证书或者上传第三方证书到SSL证书服务并绑定公网域名。推荐您在华为云云证书与管理服务购买服务器证书，详情请参见**购买SSL证书**。
- 已创建协议类型为TLS协议的后端服务器组，服务器组中添加了ECS01和ECS02实例，并且在其中部署了应用服务。

  单击查看本示例ECS01的部署命令

  - yum install -y nginx
  - systemctl start nginx.service
  - cd /usr/share/nginx/html/
  - echo "Hello World! This is ECS01 for the ELB test." > index.html

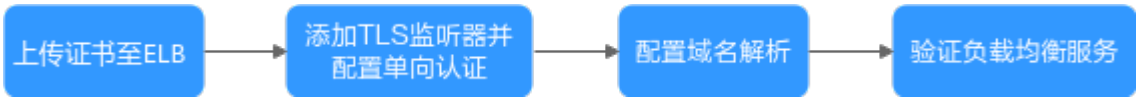
  单击查看本示例ECS02的部署命令

  - yum install -y nginx
  - systemctl start nginx.service
  - cd /usr/share/nginx/html/

- echo "Hello World! This is ECS02 for the ELB test." > index.html

操作步骤

图 3-20 配置 TLS 卸载单向认证操作流程



步骤一：上传服务器证书到 ELB 控制台

在ELB添加TLS监听器前，您需要将您的证书上传到将ELB控制台。

1. 进入**弹性负载均衡列表页面**。
2. 在左侧导航栏单击“证书管理”。
3. 单击“创建证书”，配置参数请参见**表3-5**。

表 3-5 服务器证书参数说明

参数	说明
证书类型	创建证书的类型，本文选择服务器证书。
证书来源	服务器证书同时支持SSL证书管理服务提供的数字证书和您的自有证书。 本文选择“SSL证书管理”以同步您在华为云云证书与管理服务已经购买的SSL证书。
证书	选择您需要上传到ELB控制台的证书。
企业项目	企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。
SNI扩展域名（可选）	将自动同步SSL证书已绑定的所有域名。 当您的证书用于配置SNI证书时，将支持根据客户端HTTPS请求的域名来选择对应的SNI证书完成认证。
描述	添加对该证书的描述信息，非必填项。

4. 单击“确定”，完成创建。

步骤二：添加 TLS 监听器并配置单向认证

1. 进入**弹性负载均衡列表页面**。
2. 在目标弹性负载均衡实例的操作列，单击“添加监听器”。
3. 在添加监听器页面，前端协议选择“TLS”，“SSL解析方式”选择“单向认证”，

   在服务器证书的配置项中选择**步骤一**中上传到ELB控制台的服务器证，其他参数可保持默认值或者根据实际情况修改。

图 3-21 添加 TLS 监听器并配置单向认证

4. 单击“下一步：配置后端分配策略”，后端服务器组参数选择“使用已有”。选择已经创建完成的服务器组，完成后单击“下一步：确认配置”。
5. 确认配置参数后，单击“提交”，完成TLS监听器的创建。

步骤三：配置域名解析

通过为域名添加A类型记录集解析，将域名解析到ELB的公网地址，使得客户端可以通过公网域名访问ELB。

以下提供将网站域名解析至IPv4地址的配置示例，更多关于A类型记录集的配置指导，请参考**配置网站解析**。

1. 进入**云解析服务控制台**。
2. 在左侧树状导航栏，选择“公网域名”。
   进入域名列表页面。
3. 在待添加记录集的公网域名所在行，单击操作列的“管理解析”。

4. 单击“添加记录集”，进入“添加记录集”页面。
5. 设置记录集参数，如表3-6所示。

表 3-6 A 类型记录集参数说明

参数	示例	说明
记录类型	**A – 将域名指向IPv4地址**	记录集的类型，本实践为**A – 将域名指向IPv4地址**。
主机记录	**www**	您域名的前缀。
线路类型	**全网默认**	解析的线路类型用于DNS服务器在解析域名时，根据访问者的来源，返回对应的服务器IP地址。 默认值为“全网默认”。 全网默认：默认线路类型，当未根据访问者来源设置解析线路时，系统会返回默认解析结果。
TTL(秒)	**300**	解析记录在本地DNS服务器的缓存时间，以秒为单位。 本实践使用默认值300秒。
记录值	**192.168.12.2**	域名对应的IPv4地址，本实践为ELB绑定的弹性公网IP地址。
高级配置（可选）	-	您可以单击 ，展开折叠的高级配置区域，设置记录集的别名和权重并添加标签和描述，本文保持默认设置。

6. 单击“确定”。
7. 返回“解析记录”页面。

   添加完成后，您可以在域名对应的记录集列表中查看已添加的记录集。当记录集的状态显示为“正常”时，表示记录集添加成功。

步骤四：验证负载均衡服务

在浏览器中输入ELB实例绑定的域名，例如**https://www.elbtest.com**。由于浏览器缓存的影响，客户端请求可能复用TLS会话，建议您采用无痕模式的浏览器访问域名进行验证。多次刷新页面，可以观察到请求分发至了两台ECS。如果实践过程中使用的证书为自签名证书，浏览器将会有不安全提示，但这不影响负载均衡功能的测试验证，仅影响浏览器对连接的信任标识。

图 3-22 请求转发到 ECS01

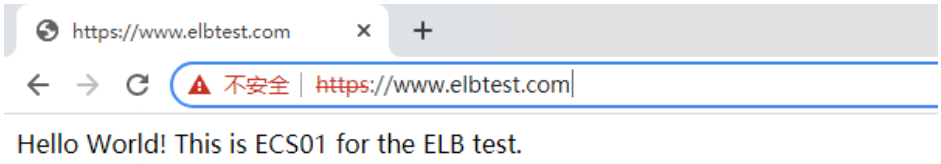
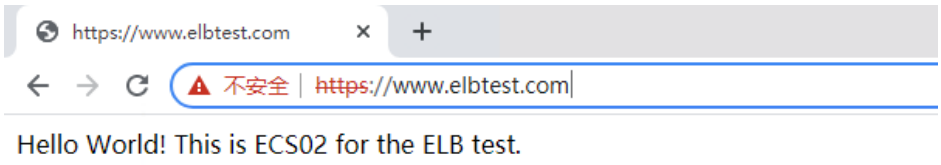


图 3-23 请求转发到 ECS02



相关文档

- 添加TLS监听器详细操作，请参见**添加TLS监听器**。
- API相关操作：
  - **添加监听器**
  - **创建证书**

3.5 通过独享型 ELB 实现 TLS 卸载（双向认证）

应用场景

如果您的四层业务对安全性要求极高，您可以通过TLS双向认证对通信双方进行认证进一步提高业务的安全性。

前提条件

- 已创建独享型ELB实例，且ELB已绑定EIP。具体操作，请参见**购买独享型负载均衡器**和**绑定IPv4公网IP**。
- 已购买SSL证书或者上传第三方证书到SSL证书服务并绑定公网域名。推荐您在华为云云证书与管理服务购买服务器证书，详情请参见**购买SSL证书**。
- 已购买CA证书并导出CA证书文件至本地或者直接使用自签名的CA证书。推荐您在华为云云证书与管理服务购买CA证书并导出私有CA证书到您的本地环境，详情请参见**购买私有CA**和**导出私有CA证书**。

- 通过私有CA签发私有证书并安装至客户端。具体操作请参见**申请私有证书**和**在客户端安装私有证书**。
- 已创建协议类型为TLS协议的后端服务器组，服务器组中添加了ECS01和ECS02实例，并且在其中部署了应用服务。

  单击查看本示例ECS01的部署命令
  - yum install -y nginx
  - systemctl start nginx.service
  - cd /usr/share/nginx/html/
  - echo "Hello World! This is ECS01 for the ELB test." > index.html

  单击查看本示例ECS02的部署命令
  - yum install -y nginx
  - systemctl start nginx.service
  - cd /usr/share/nginx/html/
  - echo "Hello World! This is ECS02 for the ELB test." > index.html

操作步骤

图 3-24 配置 TLS 卸载双向认证操作流程

步骤一：上传服务器证书到 ELB 控制台

在ELB添加TLS监听器前，您需要将您的证书上传到将ELB控制台。

1. 进入**弹性负载均衡列表页面**。
2. 在左侧导航栏单击“证书管理”。
3. 单击“创建证书”，配置参数请参见**表3-7**。

表 3-7 服务器证书参数说明

参数	说明
证书类型	创建证书的类型，本文选择服务器证书。
证书来源	服务器证书同时支持SSL证书管理服务提供的数字证书和您的自有证书。 本文选择“SSL证书管理”以同步您在华为云云证书与管理服务已经购买的SSL证书。
证书	选择您需要上传到ELB控制台的证书。
企业项目	企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。

参数	说明
SNI扩展域名（可选）	将自动同步SSL证书已绑定的所有域名。 当您的证书用于配置SNI证书时，将支持根据客户端HTTPS请求的域名来选择对应的SNI证书完成认证。
描述	添加对该证书的描述信息，非必填项。

4. 单击“确定”，完成创建。

步骤二：上传 CA 证书到 ELB 控制台

在ELB添加TLS监听器前，您需要将您的CA证书上传到将ELB控制台。

1. 进入**弹性负载均衡列表页面**。
2. 在左侧导航栏单击“证书管理”。
3. 单击“创建证书”，配置参数请参见**表3-8**。

表 3-8 CA 证书参数说明

参数	说明
证书类型	创建证书的类型，本文选择CA证书。
证书名称	您的CA证书名称。
企业项目	企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。
证书内容	证书内容必须为PEM格式。 单击“上传”，上传您本地的CA证书文件，请确保您的浏览器是最新版本。 证书内容格式如下： -----BEGIN CERTIFICATE----- Base64-encoded certificate -----END CERTIFICATE-----
描述	添加对该证书的描述信息，非必填项。

4. 单击“确定”，完成创建。

步骤三：添加 TLS 监听器并配置双向认证

1. 进入**弹性负载均衡列表页面**。
2. 在目标弹性负载均衡实例的操作列，单击“添加监听器”。
3. 在添加监听器页面，协议类型选择“TLS”，“SSL解析方式”选择“双向认证”，

   在服务器证书的配置项中选择**步骤一**中上传到ELB控制台的服务器证书。

   在CA证书的配置项中选择**步骤二**中上传到ELB控制台的服务器证书。

图 3-25 添加 TLS 监听器并配置双向认证

4. 单击“下一步：配置后端分配策略”，后端服务器组参数选择“使用已经”。选择已经创建完成的服务器组，完成后单击“下一步：确认配置”。
5. 确认配置参数后，单击“提交”，完成TLS监听器的创建。

步骤四：配置域名解析

通过为域名添加A类型记录集解析，将域名解析到ELB的公网地址，使得客户端可以通过公网域名访问ELB。

更多关于A类型记录集的配置指导，请参考**配置网站解析**。

1. 进入**云解析服务控制台**。
2. 在左侧树状导航栏，选择“公网域名”。
   进入域名列表页面。
3. 在待添加记录集的公网域名所在行，单击操作列的“管理解析”。
4. 单击“添加记录集”，进入“添加记录集”页面。
5. 设置记录集参数，如**表3-9**所示。

表 3-9 A 类型记录集参数说明

参数	示例	说明
记录类型	**A – 将域名指向IPv4地址**	记录集的类型，本实践为**A – 将域名指向IPv4地址**。

参数	示例	说明
主机记录	**www**	您域名的前缀。
线路类型	**全网默认**	解析的线路类型用于DNS服务器在解析域名时，根据访问者的来源，返回对应的服务器IP地址。 默认值为“全网默认”。 全网默认：默认线路类型，当未根据访问者来源设置解析线路时，系统会返回默认解析结果。
TTL(秒)	**300**	解析记录在本地DNS服务器的缓存时间，以秒为单位。 本实践使用默认值300秒。
记录值	**192.168.12.2** **192.168.12.3**	域名对应的IPv4地址，本实践为ELB绑定的弹性公网IP地址。
高级配置（可选）	-	您可以单击 ，展开折叠的高级配置区域，设置记录集的别名和权重并添加标签和描述，本文保持默认设置。

6. 单击“确定”。
7. 返回“解析记录”页面。

   添加完成后，您可以在域名对应的记录集列表中查看已添加的记录集。当记录集的状态显示为“正常”时，表示记录集添加成功。

步骤五：验证 TLS 双向认证

您可以参考以下方案对TLS双向认证进行验证。

Windows 客户端验证

1. 在浏览器中输入ELB实例绑定的域名，例如**https://www.elbtest.com**，在弹出的对话框中选择用于客户端验证您本人身份的证书并单击“确定”。

图 3-26 选择用户客户端验证您身份的证书

2. 由于浏览器缓存的影响，客户端请求可能复用TLS会话，建议您采用无痕模式的浏览器访问域名进行验证。多次刷新页面，可以观察到请求分发至了两台ECS。

图 3-27 请求转发到 ECS01

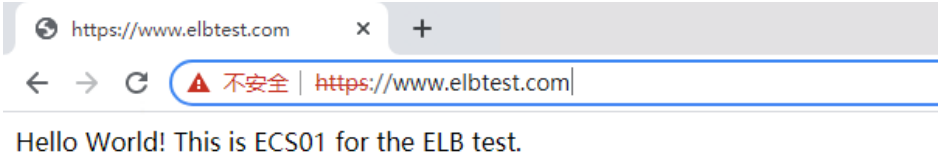
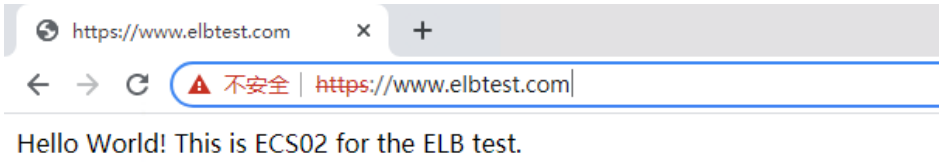


图 3-28 请求转发到 ECS02



Linux 客户端验证

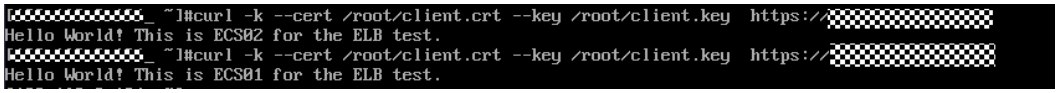
登录您的Linux客户端，执行以下命令验证TLS双向认证过程。

```
curl -k --cert /root/client.crt --key /root/client.key https://www.elbtest.com
```

其中，**--cert /root/client.crt**指定了客户端证书文件的位置，**--key /root/client.key**指定与客户端证书关联的私钥位置。

如果可以收到以下的报文，表示客户端与服务器端之间完成了TLS双向认证并将请求分发到了两台ECS。

图 3-29 验证 TLS 双向认证（Linux）



相关文档

- 添加TLS监听器详细操作，请参见**添加TLS监听器**。
- API相关操作：
  - **添加监听器**
  - **创建证书**

4 高级功能

4.1 通过 ELB 部署 QUIC 协议以提升应用加载速度

QUIC协议是基于UDP的快速互联网连接协议，改善拥塞控制，不依赖内核协议支持，用户使用具有更高的灵活性。

QUIC协议具备低时延、避免队头阻塞的多路复用优势，极佳的弱网性能可以有效解决网络、视频卡顿的问题，提升网络使用体验，同时保障数据传输的安全性。

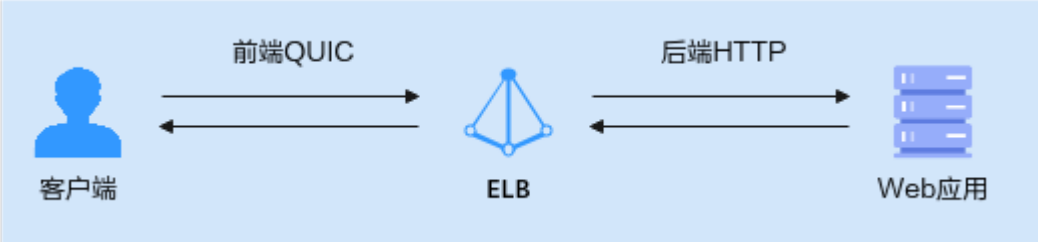
QUIC 协议概述

QUIC协议基于UDP协议实现，不需要完成TCP协议的三次握手且可以绕过TCP协议的队头阻塞，在应用层实现流（Stream）级别的多路复用，单个流丢包不用阻塞其他流。相对于传统的TCP协议，QUIC协议拥有更高的灵活性。

QUIC与HTTP/3的协商

- HTTP/3是QUIC的标准应用层协议，第一次请求时，服务器通过HTTP/1.1或HTTP/2与浏览器建立连接，并通知浏览器支持QUIC。第二次请求通过竞速机制，QUIC建立连接更快即可升级到QUIC协议，浏览器和服务器默认通过HTTP/3协商QUIC连接。
- 客户端仅支持通过HTTP/3使用QUIC，如果无法建立HTTP/3连接，将会使用HTTP/1.1或HTTP/2。

图 4-1 客户端通过 ELB 访问 Web 应用



准备工作

- 已创建独享型ELB实例，且ELB已绑定EIP。具体操作，请参见**购买独享型负载均衡器**和**绑定IPv4公网IP**。

- 已创建两台ECS，ECS与已创建的ELB实例属于同一个VPC，更多详细设置请参考**快速购买ECS**，本实践方案以ECS安装CentOS系统为例。第一台ECS_client用作客户端发送HTTP请求，第二台ECS_server用作部署Web应用的后端服务器。
- 已购买证书或者上传第三方证书到SSL证书服务，推荐您在云证书与管理服务购买服务器证书，详情请参见**购买SSL证书**。
- 已创建协议类型为**HTTP**协议的后端服务器组，服务器组中添加了ECS_server实例，本实践后端服务器的业务端口为442端口。

步骤一：配置客户端支持 HTTP/3

对于Web应用，支持QUIC连接的客户端环境需要支持HTTP/3，更多详情您可参考**curl官网文档中HTTP/3和QUIC支持**。

1. 远程登录客户端ECS_client。

   弹性云服务器有多种登录方法，具体请参见**登录弹性云服务器**。

2. 执行以下命令安装基础的依赖环境。

   a. 安装启用epel源的软件包并更新缓存。

   ```
   sudo yum install -y epel-release
   sudo yum makecache
   ```

   b. 安装所需软件包。

   ```
   sudo yum install -y git perl-IPC-cmd autoconf automake libtool libpsl-devel
   ```

3. 构建支持QUIC和HTTP/3的curl工具。

   单击查看安装参考

   - 安装OpenSSL提供TLS支持，用于QUIC加密通信，必须为3.5或者更新的版本。

     ```
     % git clone --quiet --depth=1 -b openssl-$OPENSSL_VERSION https://github.com/openssl/openssl
     % cd openssl
     % ./config --prefix=<somewhere1> --libdir=lib
     % make
     % make install
     ```

   - 安装nghttp3，用于实现HTTP/3和QPACK协议层。

     ```
     % cd ..
     % git clone -b $NGHTTP3_VERSION https://github.com/ngtcp2/nghttp3
     % cd nghttp3
     % git submodule update --init
     % autoreconf -fi
     % ./configure --prefix=<somewhere2> --enable-lib-only
     % make
     % make install
     ```

   - 安装实现QUIC协议的核心库ngtcp2。

     ```
     % cd ..
     % git clone -b $NGTCP2_VERSION https://github.com/ngtcp2/ngtcp2
     % cd ngtcp2
     % autoreconf -fi
     % ./configure PKG_CONFIG_PATH=<somewhere1>/lib/pkgconfig:<somewhere2>/lib/pkgconfig LDFLAGS="-Wl,-rpath,<somewhere1>/lib" --prefix=<somewhere3> --enable-lib-only --with-openssl
     % make
     % make install
     ```

   - 安装curl，用于发起支持HTTP/3的请求。

     ```
     % cd ..
     % git clone https://github.com/curl/curl
     % cd curl
     % autoreconf -fi
     % LDFLAGS="-Wl,-rpath,<somewhere1>/lib" ./configure --with-openssl=<somewhere1> --with-nghttp3=<somewhere2> --with-ngtcp2=<somewhere3>
     ```

```
% make
% make install
```

步骤二：在后端服务器中部署 Web 应用

1. 远程登录后端服务器ECS_server。
2. 在后端服务器中，新建目录quic_testweb。
   ```
   mkdir quic_testweb
   ```
3. 在quic_testweb目录下，新建一个index.html文件。
   a. 新建index.html文件。
      ```
      vi index.html
      ```
   b. 按**i**键进入编辑模式，index.html的脚本如下。
      ```
      hello, this is quic!
      ```
4. 按**Esc**键退出编辑模式，输入**:wq**保存index.html文件。

步骤三：添加 QUIC 监听器

1. 进入**弹性负载均衡列表页面**。
2. 在目标弹性负载均衡实例的操作列，单击“添加监听器”。
3. 在添加监听器页面，前端协议选择“QUIC”，本实践方案设置442端口。

图 4-2 添加 QUIC 监听器

4. 单击“下一步：配置后端分配策略”，后端服务器组参数选择“使用已有”。选择已经创建完成的**HTTP**服务器组，完成后单击“下一步：确认配置”。
5. 确认配置参数后，单击“提交”，完成QUIC监听器的创建。

步骤四：验证 QUIC 生效

1. 通过以下curl命令访问ELB绑定的EIP和监听端口：
   ```
   curl --http3-only -k -i https://<EIP>:<PORT>
   ```
2. 收到如**图4-3**所示页面，则表示客户端通过ELB与后端服务之间通过QUIC协商实现了HTTP/3通信。

图 4-3 验证通过 QUIC 协商实现了 HTTP/3 通信

```
[root@[redacted] curl]# curl --http3-only -k -i https://[redacted]:442
HTTP/3 200
date: Wed, 25 Jun 2025 07:20:29 GMT
content-type: text/html
content-length: 21
last-modified: Wed, 25 Jun 2025 07:06:58 GMT
server: elb

hello, this is quic!
```

4.2 通过 ELB 部署 gRPC 协议转发以提高并发效率

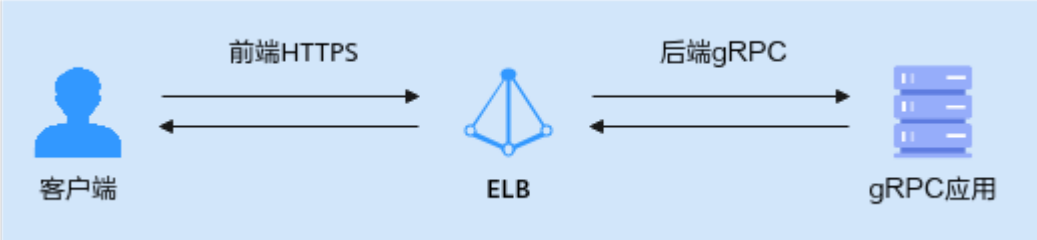
应用场景

gRPC是一种高性能且开源的远程过程调用（RPC Remote Procedure Calls）框架，广泛应用于微服务通信和移动端API等需要高性能、低延迟和跨语言支持的分布式应用场景。当前弹性负载均衡服务已支持使用HTTPS协议的监听器进行gRPC请求接收，后端服务器组使用gRPC协议进行转发的功能，基于gRPC协议支持HTTP/2多路复用的优势，显著提高流量的吞吐效率。

实践方案架构

某公司在区域A的弹性云服务器ECS中部署了gRPC应用服务，在ECS所在的虚拟私有云内创建了弹性负载均衡实例。弹性负载均衡实例通过HTTPS监听器接收业务请求再转发到gRPC协议的后端服务器组中，部署了gRPC应用服务的ECS作为后端服务器接收处理客户端请求并返回响应。

图 4-4 客户端通过 ELB 访问 gRPC 应用服务



准备工作

- 已创建独享型ELB实例，且ELB已绑定EIP。具体操作，请参见**购买独享型负载均衡器**和**绑定IPv4公网IP**。
- 已购买证书或者上传第三方证书到SSL证书服务并绑定公网域名。推荐您在华为云云证书与管理服务购买服务器证书，详情请参见**购买SSL证书**。
- 已购买ECS01实例，并且在ECS01中部署了gRPC应用服务。更多关于gRPC服务的详情，请参见**gRPC官网文档**。

操作步骤

图 4-5 配置 gRPC 协议转发操作流程

步骤一：创建 GRPC 协议的后端服务器组

1. 进入**后端服务器组列表页面**。
2. 在后端服务器列表页面，单击页面右上角“创建后端服务器组”按钮。
3. 配置后端分配策略，关键参数详情请参见**表4-1**，其余配置项保持默认值即可。

表 4-1 配置后端分配策略参数说明

参数	示例	说明
名称	**server_group_gRPC**	创建的后端服务器组的名称。
负载均衡类型	**独享型**	可使用该后端服务器组的负载均衡实例类型。
所属负载均衡器	**关联已有**	使用该后端服务器组的负载均衡实例。 单击“关联已有”后，选择您已创建完成的负载均衡实例。
后端协议	**GRPC**	后端云服务器自身提供的网络服务的协议。 本实践方案选择GRPC协议。
分配策略类型	**加权轮询算法**	负载均衡采用的算法，本实践方案保持默认的加权轮询算法。 加权轮询算法：根据后端服务器的权重，按顺序依次将请求分发给不同的服务器，权重大的后端服务器被分配的概率高。 更多关于分配策略的信息，请参见**配置流量分配策略分发流量**。

4. 单击“下一步”，添加后端服务器并配置健康检查。
5. 单击“添加云服务器”，选择您已创建好的ECS01实例，设置业务端口，其余选项保持默认，完成云服务器的添加。

⚠ 注意

此处设置的业务端口必须与实际部署gRPC业务的端口保持一致，且后端服务器的安全组需放行该业务端口

6. 开启健康检查，其余健康检查参数保持默认。
7. 单击“下一步”。
8. 确认配置无误后，单击“立即创建”。

步骤二：添加 HTTPS 监听器

1. 进入**弹性负载均衡列表页面**。
2. 在目标弹性负载均衡实例的操作列，单击“添加监听器”。
3. 在添加监听器页面，前端协议选择“HTTPS”，并且在“更多配置（可选）”中，开启“**HTTP/2**”开关。

图 4-6 添加 HTTPS 监听器并配置单向认证

图 4-7 开启 HTTP/2

4. 单击“下一步：配置后端分配策略”，后端服务器组参数选择“使用已有”。选择**步骤一**中已经创建完成的GRPC协议后端服务器组，完成后单击“下一步：确认配置”。
5. 确认配置参数后，单击“提交”，完成HTTPS监听器的创建。

步骤三：配置域名解析

通过为域名添加A类型记录集解析，将域名解析到ELB的公网地址，使得客户端可以通过公网域名访问ELB。

以下提供将网站域名解析至IPv4地址的配置示例，更多关于A类型记录集的配置指导，请参考**配置网站解析**。

1. 进入**云解析服务控制台**。
2. 在左侧树状导航栏，选择“公网域名”。
   进入域名列表页面。
3. 在待添加记录集的公网域名所在行，单击操作列的“管理解析”。
4. 单击“添加记录集”，进入“添加记录集”页面。
5. 设置记录集参数，如**表4-2**所示。

表 4-2 A 类型记录集参数说明

参数	示例	说明
记录类型	**A – 将域名指向IPv4地址**	记录集的类型，本实践为**A – 将域名指向IPv4地址**。
主机记录	**www**	您域名的前缀。
线路类型	**全网默认**	解析的线路类型用于DNS服务器在解析域名时，根据访问者的来源，返回对应的服务器IP地址。 默认值为“全网默认”。 全网默认：默认线路类型，当未根据访问者来源设置解析线路时，系统会返回默认解析结果。
TTL(秒)	**300**	解析记录在本地DNS服务器的缓存时间，以秒为单位。 本实践使用默认值300秒。
记录值	**192.168.12.2**	域名对应的IPv4地址，本实践为ELB绑定的弹性公网IP地址。
高级配置（可选）	-	您可以单击 ，展开折叠的高级配置区域，设置记录集的别名和权重并添加标签和描述，本文保持默认设置。

6. 单击“确定”。
7. 返回“解析记录”页面。
   添加完成后，您可以在域名对应的记录集列表中查看已添加的记录集。当记录集的状态显示为“正常”时，表示记录集添加成功。

步骤四：验证 gRPC 业务连通性

完成以上操作后，客户端可以通过ELB访问部署在后端服务器上的gRPC服务。由于浏览器不支持直接处理gRPC协议特定的数据帧格式，您可参考以下步骤测试客户端与gRPC服务之间的连通性。

1. 本文以ECS作为客户端进行验证，远程登录ECS。
   弹性云服务器有多种登录方法，具体请参见**登录弹性云服务器**。
2. grpcurl是用于与gRPC服务进行交互的命令行工具。在客户端中安装grpcurl用于验证gRPC服务，以下提供安装示例。
   a. 安装grpcurl软件包，本实践提供两种安装示例。

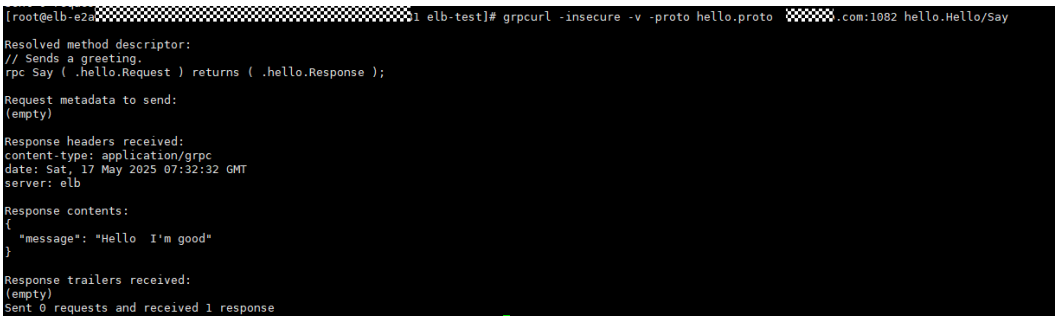
- 通过yum自动安装grpcurl软件包。
  ```
  yum install grpcurl
  ```
- 手动安装指定版本的grpcurl软件包。
  ```
  rpm -ivh grpcurl_1.9.3_linux_386.rpm
  ```

b. 验证grpcurl安装成功。
```
grpcurl --version
```

图 4-8 验证安装 grpcurl 成功

3. 在客户端中执行以下命令，尝试访问后端服务器中的gRPC服务。
   ```
   grpcurl -insecure -proto <.proto文件> <域名>:<监听端口> <gRPC服务名称>/<方法>
   ```
   如果收到类似下图所示的回复报文，则表示客户端可以通过ELB访问部署了gRPC服务的后端服务器。

图 4-9 验证访问 gRPC 服务



4.3 ELB 使用 WebSocket 协议实现聊天信息实时交互

WebSocket协议是一种在单个TCP连接上进行全双工通信的网络协议。WebSocket协议通信下，服务器可以主动向客户端发送数据，使得客户端和服务器之间的连接更持久，数据交换更简单，通信过程更高效。应用型ELB默认支持WebSocket协议，可以帮助您对需要实时通信的业务进行负载。

Websocket 协议概述

- **什么是Websocket协议**

  当前Web应用场景日渐丰富多样，对通信技术的要求也更高。例如实时社交、协同办公、在线客服通知等功能要求服务器能够实时推送数据。采用轮询技术的传统方案，即客户端在固定时间间隔内向服务器发送请求以获取最新数据，在以上场景存在明显缺陷。如果客户端需要频繁发送请求，而HTTP头字段信息冗长，会导致有效数据信息占比低、带宽资源浪费并增加服务器的压力。

  为了适应以上业务场景需求，HTML5引入支持了WebSocket协议。在全双工通信下，服务器和客户端能同时收发数据，服务器可以主动推送新数据，减少客户端的询问请求。这种双向通信机制有效减少通信冗余，提升了实时业务体验，还可以帮助您节省服务器资源和带宽资源。

  更多关于WebSocket协议的详细信息，您参考官方文档**The WebSocket Protocol**。

  ELB的HTTP/HTTPS监听默认支持WebSocket协议。

- **Websocket协议适用场景**

  Websocket协议的核心优势为**全双工实时通信**，广泛应用于需要**高频交互**和**低延迟**的业务场景。

  - **实时社交与互动**：在线聊天室、直播弹幕、多人在线棋牌类游戏等需要不同玩家的状态同步。
  - **协同办公与在线教育**：多人文档在线编辑、在线课堂互动等需要结果共享。
  - **地图导航**：交通导航中乘客位置变化和主动推送拥堵情况。
  - **客服与通知**：用户与客服之间即时信息互通。

实践方案架构

图 4-10 客户端通过 ELB 访问 Websocket 应用程序

本实践方案提供一个简易的聊天信息实时交互示例如下：客户端向服务器端发送请求，服务器端进行响应，客户端接收响应后发送新的请求，服务器端再次响应的实时交互。

准备工作

- 创建独享型ELB实例，并选择了应用型规格实例，且ELB已绑定EIP。具体操作，请参见**购买独享型负载均衡器**和**绑定IPv4公网IP**。
- 创建两台ECS，ECS与已创建的ELB实例属于同一个VPC，更多详细设置请参考**快速购买ECS**，本实践方案以ECS安装CentOS系统为例。第一台ECS_client用作客户端发送HTTP请求，第二台ECS_server用作部署WebSocket应用的后端服务器。

步骤一：在后端服务器中部署 WebSocket 应用

1. 远程登录后端服务器ECS_server。

   弹性云服务器有多种登录方法，具体请参见**登录弹性云服务器**。
2. 执行以下命令确保服务器端的python版本不低于python 3.7。
   ```
   yum install python39
   ```
3. websockets 库提供了简洁的 API，使得在 Python 中建立 WebSocket 连接变得容易，执行以下命令安装最新版websockets库。

   a. 安装Python包管理工具pip。
   ```
   sudo yum install python3-pip
   ```
   b. 安装WebSocket
   ```
   pip install websockets
   ```
4. 在后端服务器中，新建目录websocket。
   ```
   mkdir websocket
   ```
5. 在websocket目录下，新建一个websocket_server.py文件，并且在其中部署测试websocket应用服务。

a. 新建websocket_server.py文件。
```
vi websocket_server.py
```
b. 按**i**键进入编辑模式。

单击查看本示例代码参考

- websocket_server.py文件脚本，默认端口配置为8081。
```
import asyncio
import websockets

async def echo(websocket):
    print(websocket.request.path)
    try:
        async for message in websocket:
            print(f"Received: {message}")
            await websocket.send("Hello client,this is server!")
            print(f"Sent: Hello client,this is server!")
    except websockets.exceptions.ConnectionClosed as e:
        print(f"Connection closed with error: {e}")
    except Exception as e:
        print(f"Unexpected error: {e}")

async def main():
    print("Starting server...")
    start_server = await websockets.serve(echo, "0.0.0.0", 8081)
    print("Server started")
    while True:
        await asyncio.sleep(1)

asyncio.run(main())
```

6. 按**Esc**键，输入**:wq**保存websocket_server.py文件。
7. 运行websocket_server.py文件。
```
python3 websocket_server.py
```
8. 收到如图4-11的回显，表示WebSocket应用部署成功。

图 4-11 WebSocket 应用部署成功

步骤二：在客户端中部署 WebSocket 应用

1. 远程登录客户端ECS_client。

   弹性云服务器有多种登录方法，具体请参见登录弹性云服务器。
2. 执行以下命令确保客户端的python版本不低于python 3.7。
```
yum install python39
```
3. 执行以下命令在客户端中安装最新版websockets库。

   a. 安装Python包管理工具pip。
```
sudo yum install python3-pip
```
   b. 安装WebSocket
```
pip install websockets
```
4. 在客户端服务器中，新建目录websocket_client。
```
mkdir websocket_client
```
5. 在websocket目录下，新建一个websocket_client.py文件，并且在其中部署websocket应用服务。

   a. 新建websocket_client.py文件。
```
vi websocket_client.py
```


b. 按**i**键进入编辑模式。

单击查看本示例代码参考

- websocket_client.py文件脚本，使客户端可以访问ELB对外服务的EIP地址和端口，本实践示例端口为8081端口。

```
import asyncio
import websockets

async def hello():
    uri = "ws://EIP_ELB:8081"
    try:
        async with websockets.connect(uri) as websocket:
            while True:
                await websocket.send("Hello server,this is client!")
                print("Sent: Hello server,this is client!")
                response = await websocket.recv()
                print(f"Received: {response}")
                await asyncio.sleep(1)
    except websockets.exceptions.ConnectionClosedError as e:
        print(f"Connection closed with error: {e}")

asyncio.get_event_loop().run_until_complete(hello())
```

6. 按**Esc**键，输入**:wq**保存websocket_client.py文件。

步骤三：创建 HTTP 后端服务器组并添加后端服务器

1. 进入**后端服务器组列表页面**。
2. 在后端服务器列表页面，单击页面右上角“创建后端服务器组”按钮。
3. 在配置后端分配策略页面，选择将后端服务器组Server_Group关联至已经创建完成的ELB实例，后端协议选择“HTTP”。
4. 其余设置保持默认，单击“下一步”。
5. 在添加后端服务器页面，云服务器页签下，单击“添加云服务器”。
6. 在添加后端服务器侧拉窗中，选择ECS_server，并设置业务端口为8081。
7. 单击“下一步”后确认配置信息。
8. 单击“立即创建”。

步骤四：创建 HTTP 监听器并选择后端服务器组

1. 进入**弹性负载均衡列表页面**。
2. 在目标弹性负载均衡实例的操作列，单击“添加监听器”。
3. 在添加监听器页面，协议类型选择“HTTP”，端口设置为“8081”。

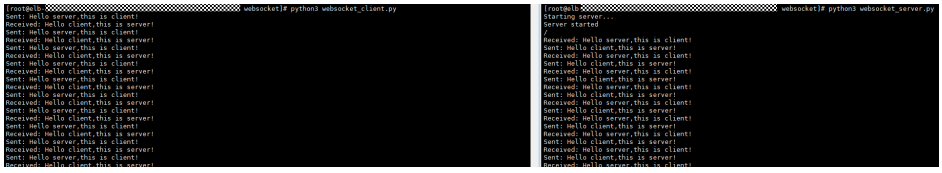
图 4-12 添加 HTTP 监听器

4. 单击“下一步：配置后端分配策略”，后端服务器组参数选择“使用已有”。选择步骤三创建完成的服务器组Server_Group，完成后单击“下一步：确认配置”。
5. 确认配置参数后，单击“提交”，完成HTTP监听器的创建。

步骤五：验证结果

1. 远程登录客户端ECS_client。
2. 运行代码python websocket_client.py文件。
```
python3 websocket_client.py
```
3. 看到客户端和后端服务器相继打印“Sent: Hello server, this is client!”和“Received: Hello client, this is server!”，验证了ELB通过WebSocket协议实现了实时聊天。

图 4-13 ELB 通过 WebSocket 协议实现了实时聊天。



4.4 通过 ELB 的全端口监听转发功能实现多端口转发

应用场景

如果您的业务存在动态端口或同时监听多个端口的场景，配置固定端口的监听器将会使您的负载均衡配置更加繁琐。如果您希望可以更灵活地对大量端口进行监听，推荐您使用独享型ELB的全端口监听功能。全端口监听可以实现在一个监听器中对多个监听端口或端口段进行监听转发，简化了监听器配置，使您的运维更加便捷。

前提条件

- 已创建独享型ELB实例，实例类型包含网络型，且ELB已绑定EIP。具体操作，请参见**购买独享型负载均衡器**和**绑定IPv4公网IP**。
- 已创建ECS01和ECS02实例，并且在其中部署了应用服务。服务器ECS01和ECS02加入的安全组已经放行30000~30005端口。

  单击查看本示例ECS01的部署命令

  - 登录ECS01，执行如下命令，新建脚本文件。
    ```
    vi ECS01_install.sh
    ```
  - 进入编辑模式，复制并粘贴以下命令。
    ```
    #!/bin/bash

    # 安装Nginx并自动配置多端口
    yum install -y nginx

    for PORT in {30000..30005}; do
      # 生成HTML文件
      echo "Hello World! This is ECS01, server port is $PORT." > /usr/share/nginx/html/index_$PORT.html
      # 生成Nginx配置
      printf "server { listen $PORT; location / { root /usr/share/nginx/html; index index_$PORT.html; } }\n" > /etc/nginx/conf.d/app_$PORT.conf
    done

    # 启动Nginx并测试
    nginx -t && systemctl restart nginx
    curl --parallel-max 11 $(for PORT in {30000..30005}; do echo "http://localhost:$PORT "; done)
    ```
  - 输入**:wq**，保存文件修改。
  - 执行以下命令 ，运行脚本文件。
    ```
    sudo sh ECS01_install.sh
    ```
  - 如果显示如下执行结果，表示30000到30005端口都可以正常访问
    ```
    Hello World! This is ECS01, server port is 30000.
    Hello World! This is ECS01, server port is 30001.
    Hello World! This is ECS01, server port is 30002.
    Hello World! This is ECS01, server port is 30003.
    Hello World! This is ECS01, server port is 30004.
    Hello World! This is ECS01, server port is 30005.
    ```

步骤一：创建后端服务器组并开启全端口转发

本实践方案使用支持全端口转发功能的后端服务器组，后端服务器组开启全端口转发后，组内添加后端服务器时无需指定后端端口，监听器将按照前端请求端口转发流量至后端服务器对应的端口。

1. 进入**后端服务器组列表页面**。
2. 在后端服务器列表页面，单击页面右上角“创建后端服务器组”按钮。
3. 配置后端分配策略，关键参数详情请参见**表4-3**，其余配置项保持默认值即可。

表 4-3 配置后端分配策略参数说明

参数	示例	说明
名称	**server_group**	创建的后端服务器组的名称。
负载均衡类型	**独享型**	可使用该后端服务器组的负载均衡实例类型。

参数	示例	说明
所属负载均衡器	**关联已有**	使用该后端服务器组的负载均衡实例。 单击“关联已有”后，选择您已创建完成的负载均衡实例。
后端协议	**TCP**	后端云服务器自身提供的网络服务的协议。 本实践方案选择TCP协议。
全端口转发	**开启**	开启全端口转发后，后端服务器组添加后端服务器时无需指定后端端口，监听器将按照前端请求端口转发流量至后端服务器对应的端口。 全端口转发功能开启后不支持关闭。
分配策略类型	**加权轮询算法**	负载均衡采用的算法，本实践方案保持默认的加权轮询算法。 加权轮询算法：根据后端服务器的权重，按顺序依次将请求分发给不同的服务器，权重大的后端服务器被分配的概率高。 更多关于分配策略的信息，请参见**配置流量分配策略分发流量**。

4. 单击“下一步”，添加后端服务器并配置健康检查。
5. 单击“添加云服务器”，选择您已创建好的ECS01和ECS02实例，其余选项保持默认，完成云服务器的添加。
6. 开启健康检查，后端服务器组开启全端口转发，后端服务器无默认业务端口，需要配置健康检查端口。

   本实践的配置实例端口为80，其余健康检查参数保持默认。
7. 单击“下一步”。
8. 确认配置无误后，单击“立即创建”。

步骤二：创建 TCP 监听器并开启全端口监听

本实践方案以TCP监听器为例进行全端口监听转发。

1. 进入**弹性负载均衡列表页面**。
2. 在目标弹性负载均衡实例的操作列，单击“添加监听器”。
3. 在添加监听器页面，协议类型选择“TCP”，并开启全端口监听，前端端口设置为30000~30005端口。

图 4-14 添加 TCP 监听并开启全端口监听

4. 单击“下一步：配置后端分配策略”，配置后端服务器组。

   单击“使用已有”，并选择**步骤一：创建后端服务器组并开启全端口转发**中创建的后端服务器组。

5. 单击“下一步：确认配置”，确认完成后，完成TCP监听器的创建。

步骤三：配置域名解析

通过为域名添加A类型记录集解析，将域名解析到ELB的公网地址，使得客户端可以通过公网域名访问ELB。

更多关于A类型记录集的配置指导，请参考**配置网站解析**。

1. 进入**云解析服务控制台**。
2. 在左侧树状导航栏，选择“公网域名”。

   进入域名列表页面。
3. 在待添加记录集的域名所在行，单击操作列的“管理解析”。
4. 单击“添加记录集”，进入“添加记录集”页面。
5. 设置记录集参数，如**表4-4**所示。

表 4-4 A 类型记录集参数说明

参数	示例	说明
记录类型	**A – 将域名指向IPv4地址**	记录集的类型，本实践为**A – 将域名指向IPv4地址**。
主机记录	**www**	您域名的前缀。
线路类型	**全网默认**	解析的线路类型用于DNS服务器在解析域名时，根据访问者的来源，返回对应的服务器IP地址。 默认值为“全网默认”。 全网默认：默认线路类型，当未根据访问者来源设置解析线路时，系统会返回默认解析结果。

参数	示例	说明
TTL(秒)	**300**	解析记录在本地DNS服务器的缓存时间，以秒为单位。 本实践使用默认值300秒。
记录值	**192.168.12.2**	域名对应的IPv4地址，本实践为ELB绑定的弹性公网IP地址。
高级配置（可选）	-	您可以单击 ，展开折叠的高级配置区域，设置记录集的别名和权重并添加标签和描述，本文保持默认设置。

6. 单击“确定”。
7. 返回“解析记录”页面。

   添加完成后，您可以在域名对应的记录集列表中查看已添加的记录集。当记录集的状态显示为“正常”时，表示记录集添加成功。

步骤四：验证全端口监听

- 测试ELB可用性

  a. 以任意一台可以访问公网的Linux客户端为例。多次执行curl 域名 端口命令（端口为30000-30005之间任意端口），收到类似回复报文为**Hello World! This is ECS01, server port is 具体端口号.**，则表示ELB可以将请求转发至后端服务器。

  图 4-15 Linux 客户端请求访问到 ECS01

  ```
  Hello World! This is ECS01, server port is 30000.
  ```

  b. 通过浏览器访问域名加30000-30005之间的任意端口，例如http://域名:30000，可以看到类似下图的页面，表示客户端能够正常访问应用。

  图 4-16 浏览器请求访问到 ECS01

  Hello World! This is ECS01, server port is 30000.

- 模拟业务故障

  a. 停用ECS01服务。在ECS01中执行systemctl stop nginx.service停用应用。

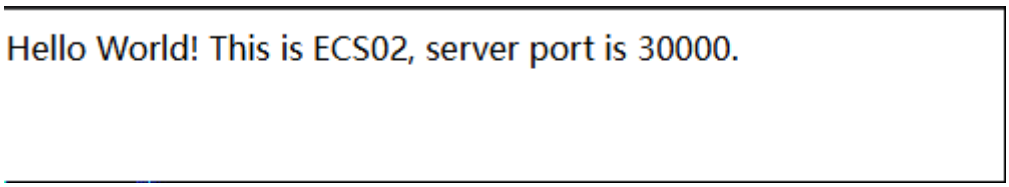
  等待几分钟后，客户端再次执行curl 域名 端口命令（端口为30000-30005之间任意端口），仍然收到下图回复报文Hello World! This is …

  图 4-17 客户端请求访问到 ECS02

  ```
  Hello World! This is ECS02, server port is 30000.
  ```

  b. 通过浏览器访问域名加30000-30005之间的任意端口，例如http://域名:30000，可以看到类似下图，表示客户端能够正常访问应用。

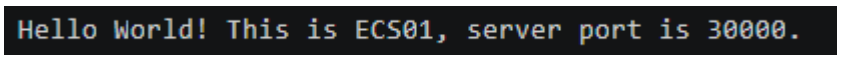
图 4-18 浏览器请求访问到 ECS02



c. 启用ECS01服务，停用ECS02服务。在ECS01中执行systemctl start nginx.service重新启动应用，在ECS02中执行systemctl stop nginx.service停用应用。

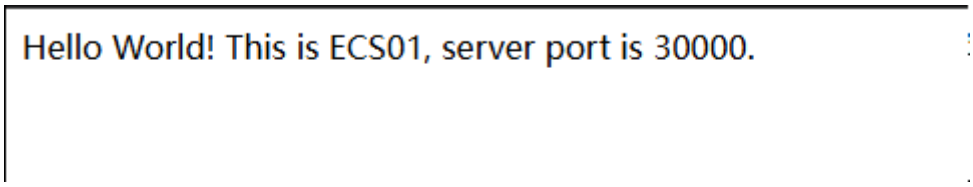
等待几分钟后，在客户端中再次执行telnet 域名 端口命令（端口为30000-30005之间任意端口），仍然收到下图回复报文Hello World! This is …

图 4-19 Linux 客户端请求访问到 ECS01



d. 通过浏览器访问域名加30000-30005之间的任意端口，例如http://域名:30000，可以看到类似下图，表示客户端能够正常访问应用。

图 4-20 浏览器请求访问到 ECS01



e. 如上测试结果表明，后端单台服务器故障不影响ELB可用性，并且30000-30005之间的端口均可以访问服务。

4.5 通过 IPv4/IPv6 地址转换实现 IPv6 客户端访问 IPv4 业务

应用场景

如果访问您四层业务的请求来自IPv6客户端，而您的后端业务仍部署在IPv4环境，您可以通过IPv4/IPv6地址转换功能解决IPv6客户端和IPv4业务后端之间的兼容性问题。此时，您的后端服务服务器无需做IPv6改造即可处理来自IPv6客户端的请求。

说明

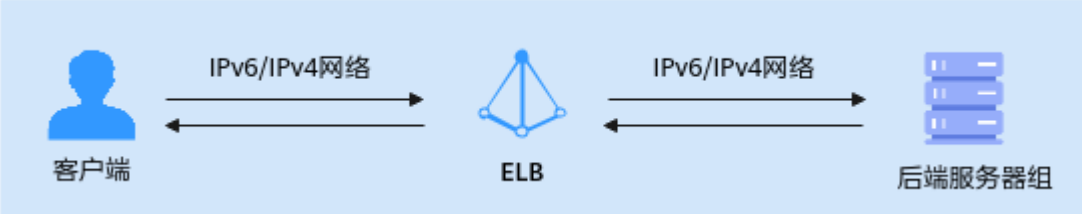
该功能陆续上线中，已发布区域请以控制台实际为准。如果您有使用需求，可以提交**工单**进行申请。

什么是 IPv4/IPv6 地址转换

弹性负载均衡支持开启**IPv4/IPv6地址转换功能**，该功能同时支持**NAT64和NAT46网络地址转换**技术，无论客户端访问ELB的IPv4还是IPv6地址，都可以和IPv4或IPv6后端服务器通信。

- **NAT64**：将IPv6流量转换为IPv4流量。开启该功能后，IPv6客户端经过ELB转发可以访问IPv4服务端。
- **NAT46**：将IPv4流量转换为IPv6流量。开启该功能后，IPv4客户端经过ELB转发可以访问IPv6服务端。

图 4-21 四层（TCP 和 UDP 协议）ELB 开启 IPv4/IPv6 地址转换业务架构图



前提条件

- 已购买ECS01实例，ECS的主网卡为IPv4地址。在ECS01中部署了应用服务，部署测试业务详情请参见**搭建后端服务**。
- 已创建协议类型为TCP或UDP协议的后端服务器组，本实践以TCP协议的后端服务器组为例，服务器组中添加了ECS01。

操作流程

图 4-22 配置 IPv6 客户端访问 IPv4 后端服务

步骤一：创建支持 IPv6 网络的 ELB

1. 进入**购买弹性负载均衡页面**。
2. 根据界面提示选择负载均衡器的基础配置，如图所示选择“网络型”规格实例。

图 4-23 创建网络型负载均衡器（独享型）

3. 选定负载均衡器的规格后，请根据界面提示选择负载均衡器的网络配置。
   网络类型需选择“IPv6网络”，所属VPC和子网需支持IPv6。

图 4-24 网络类型选择“IPV6 网络”

4. 确认配置信息，单击“立即购买”，完成创建。

步骤二：添加监听器并开启 IPv4/IPv6 地址转换功能

1. 进入**弹性负载均衡列表页面**。
2. 在目标弹性负载均衡实例的操作列，单击“添加监听器”。
3. 在添加监听器页面，协议类型选择“TCP”，开启“IPv4/IPv6地址转换”功能。

图 4-25 添加 TCP 监听器并开启“IPv4/IPv6 地址转换”

4. 单击“下一步：配置后端分配策略”，后端服务器组参数选择“使用已有”。选择已经创建完成的服务器组，完成后单击“下一步：确认配置”。
5. 确认配置参数后，单击“提交”，完成TCP监听器的创建。

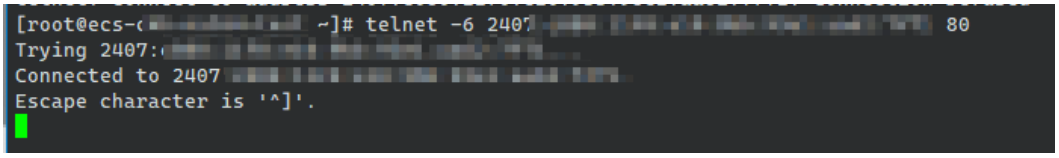
步骤三：后端服务器的安全组放通 ELB 所属子网

来自IPv6客户端的请求经过ELB后会使用ELB后端子网中的IP地址与后端服务器ECS01通信，ECS01的安全组需要放通ELB后端子网所属网段，详情请参见**配置后端服务器的安全组**。

步骤四：验证 IPv6 客户端访问到 IPv4 后端服务

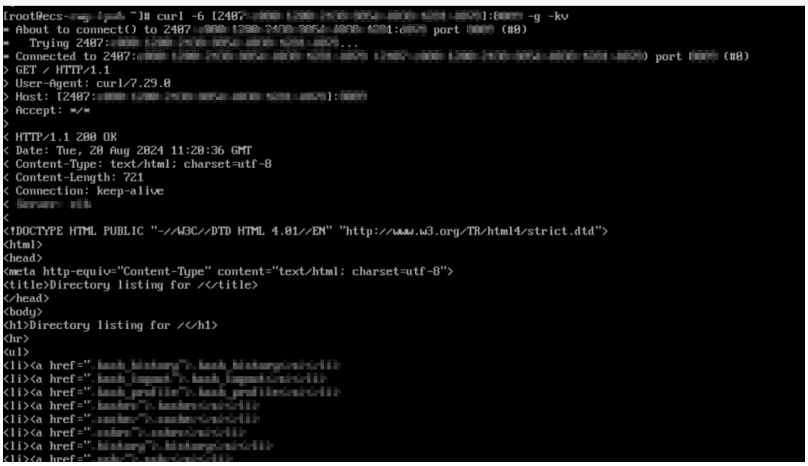
- 在IPv6客户端中执行以下命令，访问ELB的IPv6地址。
  ```
  telnet -6 ${IPv6地址} ${端口号}
  ```
  收到类似下图所示的信息，表示客户端成功访问IPv6地址。

  图 4-26 IPv6 客户端成功访问 ELB 的 IPv6 地址

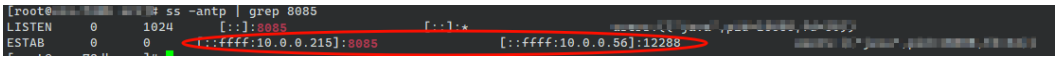
- 使用curl命令验证Web类服务应用的连通性。
  ```
  curl -6 [${ELB IPv6地址}]:${ELB 监听器端口} -g -v
  ```
  收到类似下图所示的信息，表示Web类服务应用网络连通。

  图 4-27 验证 Web 类服务应用的连通性

- 通过执行以下命令确定与后端服务器建立连接
  ```
  ss -antp |grep ${后端云服务器端口}
  ```
  收到下图所示的信息，表示IPv6客户端的源IPv6地址信息经过ELB后转换为ELB后端子网的IPv4地址，并与后端服务器ECS01成功通信。

  图 4-28 IPv6 客户端与 IPv4 后端服务器通信成功

相关文档

IPv4/IPv6地址转换功能开启后，不支持开启**获取客户端IP**功能，TCP监听器场景可以通过**通过ProxyProtocol协议获取客户端真实IP**。

4.6 在四层独享型 ELB 转发下获取客户端真实 IP

应用场景

在使用弹性负载均衡进行业务转发时，您可能需要获取客户端请求的真实IP地址进行进一步分析，特别是在安全防护、数据分析、用户行为分析和故障排查等典型业务场景。

使用ELB进行四层业务转发时，默认情况下ELB实例与后端服务器之间直接使用客户端的IP地址通信，后端服务器可以直接获取客户端真实IP地址。但是在ELB实例与IP类型后端通信、TCP或UDP监听器开启IPv4/IPv6地址转换、使用TLS监听器进行转发等场景，客户端真实IP经过独享型ELB实例时会发生转换，您可以参考本文获取四层业务转发场景的客户端真实IP地址。

约束与限制

- 如果请求经过NAT网关，则只能获取到NAT转换后的IP地址，无法获取NAT转化前的IP地址。
- 如果请求客户端为容器，则只能获取到容器所在主机的IP地址，无法获取容器的IP地址。
- 四层监听器（TCP/UDP）默认开启“获取客户端IP”功能，不支持同一台服务器既作为后端服务器又作为客户端的场景。

  如果后端服务器和客户端使用同一台服务器，则后端服务器会根据报文源IP为本地IP判定该报文为本机发出的报文，无法将应答报文返回给ELB，最终导致回程流量不通。

四层服务获取客户端真实 IP 方法介绍

独享型ELB的四层协议监听器（TCP/UDP）默认支持“获取客户端IP”功能，ELB实例与后端服务器之间直接使用客户端真实的IP地址通信。

部分特殊场景，监听器的“获取客户端IP”功能失效，您可以参考**表4-5**在四层业务转发场景获取客户端真实IP。

表 4-5 四层监听获取客户端真实 IP 方法总结

监听器	监听器的“获取客户端IP”功能	特殊场景获取客户端真实IP
TCP监听器	**TCP/UDP监听器默认支持“获取客户端IP”**	以下场景监听器的“获取客户端IP”功能失效，您可以通过**配置TOA插件**或**通过ProxyProtocol协议**获取客户端真实IP： ● TCP监听器与IP类型后端通信。 ● TCP监听器开启IPv4/IPv6地址转换开关后，客户端IP地址发生转换。
UDP监听器	**TCP/UDP监听器默认支持“获取客户端IP”**	以下场景无法获取客户端真实IP： ● ELB实例与IP类型后端通信。 ● UDP监听器开启IPv4/IPv6地址转换。

监听器	监听器的“获取客户端IP”功能	特殊场景获取客户端真实IP
TLS监听器	不支持	通过ProxyProtocol协议获取客户端真实IP。

TCP/UDP 监听器默认支持“获取客户端 IP”

TCP和UDP监听器的业务转发场景，ELB实例与后端服务器之间直接使用客户端的真实IP地址通信。您无需进行额外设置，通过查看后端服务器的日志记录即可判断是否获取到客户端真实IP。

当Nginx作为后端服务器，您可以参考以下步骤进行验证。

1. 修改http配置块，为Nginx配置访问日志，您可以参考执行以下命令。

```
http {
    log_format main '$remote_addr- $remote_user [$time_local] "$request" '
                '$status $body_bytes_sent "http_referer" '
                '"$http_user_agent" "$http_x_forwarded_for"';
    }
```

图 4-29 配置访问日志

2. 查看Nginx的访问日志，您可以直接获取客户端请求的真实IP。

```
cat /path/server/nginx/logs/access.log
```

日志记录中，第一个IP地址即为客户端的真实IP地址。

图 4-30 查看 Nginx 的日志

TCP 监听器转发下配置 TOA 插件获取客户端真实 IP

TOA内核模块主要用来获取ELB实例转发过的客户端真实IP地址（**仅支持IPv4**），该插件安装在ELB后端服务器，详细过程请参考TOA插件配置。

通过 ProxyProtocol 协议获取客户端真实 IP

您可以通过在监听器上**开启ProxyProtocol功能**开关，并确保**后端服务器具有解析ProxyProtocol协议的能力**来获取客户端真实IP。

- **TCP监听器**在以下场景“获取客户端IP”功能失效：
  - TCP监听器与IP类型后端通信。
  - TCP监听器开启IPv4/IPv6地址转换开关后进行转发。
- **TLS监听器**：仅支持通过ProxyProtocol协议获取客户端真实IP。

警告

请确保后端服务器具有解析ProxyProtocol协议的能力，否则会导致业务中断，请谨慎开启。

详细过程请参考以下操作步骤。

步骤一：为监听器开启 ProxyProtocol

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击目标负载均衡器名称。
3. 在监听器列表页面，单击目标监听器的名称。
4. 在监听器的基本信息页签，单击“编辑监听器”。
5. 在“编辑监听器”页面，开启“ProxyProtocol”开关。
6. 单击“确定”。

步骤二：配置后端服务器支持解析 ProxyProtocol 协议

本文以后端服务器在CentOS 7.5环境下，安装Nginx为例进行介绍，您可以参考执行如下命令进行安装。

1. 运行以下命令安装http_realip_module。

```
yum -y install gcc pcre pcre-devel zlib zlib-devel openssl openssl-devel
wget http://nginx.org/download/nginx-1.17.0.tar.gz
tar zxvf nginx-1.17.0.tar.gz
cd nginx-1.17.0
./configure --prefix=/path/server/nginx --with-http_stub_status_module --without-http-cache --with-http_ssl_module --with-http_realip_module
make
make install
```

2. 打开Nginx的主配置文件nginx.conf。

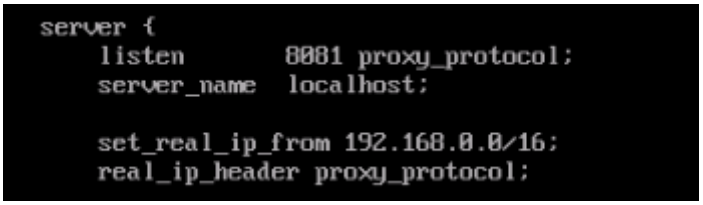
```
vi /path/server/nginx/conf/nginx.conf
```

3. 修改server配置块，修改参考如下。
   a. 启用Proxy Protocol监听。
   b. 配置真实IP提取。

```
server {
  listen 8081 proxy_protocol;
  server_name localhost;

  set_real_ip_from 192.168.0.0/16;
  real_ip_header proxy_protocol;
}
```

将代理服务器的网段添加到 set_real_ip_from <IP_address>，独享型ELB实例需要ELB后端子网网段。

图 4-31 修改 Nginx 配置文件的 server 配置块



4. 修改http配置块，配置访问日志。

```
http {
    log_format main '$remote_addr- $remote_user [$time_local] "$request"'
                '$status $body_bytes_sent "$http_referer" '
                '"$http_user_agent" "$proxy_protocol_addr" ';

}
```

图 4-32 修改 Nginx 配置文件的 http 配置块

```
http {
    log_format  main  '$remote_addr - $remote_user [$time_local] "$request" '
                      '$status $body_bytes_sent "$http_referer" '
                      '"$http_user_agent" "$proxy_protocol_addr"';
```

5. 启动Nginx

```
/path/server/nginx/sbin/nginx
```

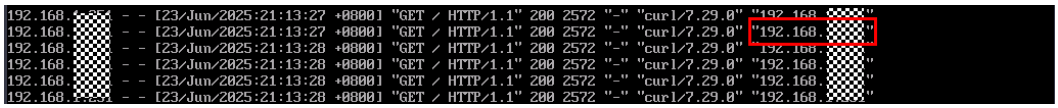
步骤三：验证后端服务器获得了客户端真实 IP

以Nginx作为后端服务器时，客户端访问开启了ProxyProtocol的ELB实例，Nginx日志中的源IP即为真实的客户端IP。

```
cat /path/server/nginx/logs/access.log
```

日志记录中，$proxy_protocol_addr变量对应的IP地址即为客户端的真实IP地址。

图 4-33 通过 ProxyProtocol 协议获取客户端真实 IP



```
192.168.[redacted] - - [23/Jun/2025:21:13:27 +0800] "GET / HTTP/1.1" 200 2572 "-" "curl/7.29.0" "192.168.[redacted]"
192.168.[redacted] - - [23/Jun/2025:21:13:27 +0800] "GET / HTTP/1.1" 200 2572 "-" "curl/7.29.0" "192.168.[redacted]"
192.168.[redacted] - - [23/Jun/2025:21:13:28 +0800] "GET / HTTP/1.1" 200 2572 "-" "curl/7.29.0" "192.168.[redacted]"
192.168.[redacted] - - [23/Jun/2025:21:13:28 +0800] "GET / HTTP/1.1" 200 2572 "-" "curl/7.29.0" "192.168.[redacted]"
192.168.[redacted] - - [23/Jun/2025:21:13:28 +0800] "GET / HTTP/1.1" 200 2572 "-" "curl/7.29.0" "192.168.[redacted]"
192.168.[redacted] - - [23/Jun/2025:21:13:28 +0800] "GET / HTTP/1.1" 200 2572 "-" "curl/7.29.0" "192.168.[redacted]"
```

4.7 在七层独享型 ELB 转发下获取客户端真实 IP

应用场景

在使用弹性负载均衡进行业务转发时，您可能需要获取客户端请求的真实IP地址进行进一步分析，特别是在安全防护、数据分析、用户行为分析和故障排查等典型业务场景。由于通过HTTP/HTTPS/QUIC监听器进行七层业务转发时，客户端真实IP经过独享型ELB实例时会发生转换，您可以参考本文获取客户端真实的IP地址。

约束与限制

- 如果请求经过NAT网关，则只能获取到NAT转换后的IP地址，无法获取NAT转化前的IP地址。
- 如果请求客户端为容器，则只能获取到容器所在主机的IP地址，无法获取容器的IP地址。

七层服务获取客户端真实 IP 方法介绍

- 独享型ELB的七层协议监听器（HTTP/HTTPS/QUIC）默认开启“获取客户端IP”功能，支持通过X-Forwarded-For字段传递客户端的真实IP。
- 对后端服务器进行配置，确保服务器可以正确解析X-Forwarded-For字段以获取客户端的真实IP。

  X-Forwarded-For字段格式如下：

```
X-Forwarded-For: <请求客户端真实IP, 代理服务器1-IP, 代理服务器2-IP, ...>
```

使用此方式获取客户端真实IP时，获取的第一个IP地址就是客户端真实IP。

准备工作

- 已创建独享型ELB实例，且ELB已绑定EIP。具体操作，请参见**购买独享型负载均衡器**和**绑定IPv4公网IP**。
- 已创建协议类型为HTTP协议的后端服务器组。服务器组中添加了ECS01实例，并且在ECS01中部署了应用服务。

步骤一：七层监听器开启“获取客户端 IP”功能

独享型ELB实例的HTTP/HTTPS/QUIC监听器默认开启“获取客户端IP”功能，即默认支持通过X-Forwarded-For走字段记录客户端请求的真实IP。

步骤二：配置后端服务器

根据部署的后端服务器类型，进行相应的配置，确保服务器可以正确解析X-Forwarded-For字段。

配置 Nginx 服务器

例如在CentOS 7.5环境下，可以执行如下命令执行安装：

1. 运行以下命令下载**Nginx源码包**，安装http_realip_module。

```
yum -y install gcc pcre pcre-devel zlib zlib-devel openssl openssl-devel
wget http://nginx.org/download/nginx-1.17.0.tar.gz
tar zxvf nginx-1.17.0.tar.gz
cd nginx-1.17.0
./configure --prefix=/path/server/nginx --with-http_stub_status_module --without-http-cache --with-http_ssl_module --with-http_realip_module
make
make install
```

2. 执行以下命令，打开nginx.conf文件。

```
vi /path/server/nginx/conf/nginx.conf
```

3. 按i进入编辑模式。
4. 修改server配置块，修改参考如下。

```
set_real_ip_from 192.168.0.0/16;
real_ip_header X-Forwarded-For;
```

图 4-34 添加配置字段和信息示例图

```
server {
    listen       80;
    server_name  localhost;

    set_real_ip_from 192.168.0.0/16;
    real_ip_header X-Forwarded-For;
```

说明

将代理服务器的网段添加到 set_real_ip_from <IP_address>，独享型负载均衡需要添加ELB实例的后端子网网段。

5. 修改http配置块，为Nginx配置访问日志，将X-Forwarded-For头字段的客户端请求信息通过http_x_forwarded_for传入日志，您可以参考执行以下命令。

```
http {
    log_format main '$remote_addr- $remote_user [$time_local] "$request" '
                '$status $body_bytes_sent "http_referer" '
                '"$http_user_agent" "$http_x_forwarded_for"';
    }
```

图 4-35 配置访问日志

```
http {
    log_format  main  '$remote_addr - $remote_user [$time_local] "$request" '
                      '$status $body_bytes_sent "$http_referer" '
                      '"$http_user_agent" "$http_x_forwarded_for"';
```

6. 启动Nginx。
   ```
   /path/server/nginx/sbin/nginx
   ```

配置 Tomcat 服务器

本教程中的Tomcat的安装路径为“/usr/tomcat/tomcat8/”。

1. 登录已安装Tomcat的服务器。
2. 执行如下命令，确定Tomcat已经正常运行。
   ```
   ps -ef|grep tomcat
   netstat -anpt|grep java
   ```

图 4-36 正常运行结果示例

```
[root@lilian apache-tomcat-9.0.10]# ps -ef |grep tomcat
root      1009   995  0 15:01 pts/0    00:00:00 grep --color=auto tomcat
root     32223     1  0 14:37 pts/0    00:00:12 /usr/java/jdk-10.0.1/bin/java -Djava.util.logging.config.file=/usr/local/tomc
t-9.0.10/conf/logging.properties -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager -Djdk.tls.ephemeralDHKeySi
tocol.handler.pkgs=org.apache.catalina.webresources -Dorg.apache.catalina.security.SecurityListener.UMASK=0027 -Dignore.endors
th /usr/local/tomcat-01/apache-tomcat-9.0.10/bin/bootstrap.jar:/usr/local/tomcat-01/apache-tomcat-9.0.10/bin/tomcat-juli.jar
sr/local/tomcat-01/apache-tomcat-9.0.10 -Dcatalina.home=/usr/local/tomcat-01/apache-tomcat-9.0.10 -Djava.io.tmpdir=/usr/local/
tomcat-9.0.10/temp org.apache.catalina.startup.Bootstrap start
[root@lilian apache-tomcat-9.0.10]# netstat -anpt|grep java
tcp        0      0 127.0.0.1:32001         0.0.0.0:*               LISTEN      882/java
tcp6       0      0 :::8020                 :::*                    LISTEN      32223/java
tcp6       0      0 :::8888                 :::*                    LISTEN      32223/java
tcp6       0      0 127.0.0.1:8006          :::*                    LISTEN      32223/java
tcp6       0      0 10.0.0.20:8888          100.125.134.52:38390    ESTABLISHED 32223/java
tcp6       0      0 127.0.0.1:31001         127.0.0.1:32001         ESTABLISHED 882/java
tcp6       0      0 10.0.0.20:8888          100.125.134.53:57771    ESTABLISHED 32223/java
tcp6       0      0 10.0.0.20:8888          100.125.134.46:62833    ESTABLISHED 32223/java
tcp6       0      0 10.0.0.20:8888          100.125.19.50:58124     ESTABLISHED 32223/java
tcp6       0      0 10.0.0.20:8888          100.125.19.47:49597     ESTABLISHED 32223/java
tcp6       1      0 10.0.0.20:50648         100.125.15.62:80        CLOSE_WAIT  882/java
tcp6       0      0 10.0.0.20:8888          100.125.19.53:27108     ESTABLISHED 32223/java
```

3. 将server.xml文件中的className="org.apache.catalina.valves.AccessLogValve"模块修改为如下内容。
   a. 打开server.xml文件。
      ```
      vim /usr/tomcat/tomcat8/conf/server.xml
      ```
   b. 修改文件内容参考如下。
      ```
      <Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
      prefix="localhost_access_log." suffix=".txt"
      pattern="%{X-FORWARDED-FOR}i %l %u %t %r %s %b %D %q %{User-Agent}i %T"
      resolveHosts="false" />
      ```

图 4-37 配置示例

```
        <!-- Access log processes all example.
             Documentation at: /docs/config/valve.html
             Note: The pattern used is equivalent to using pattern="common" -->
        <Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
               prefix="localhost_access_log." suffix=".txt"
               pattern="%{X-FORWARDED-FOR}i %l %u %t %r %s %b %D %q %{User-Agent}i %T" resolveHosts="false" />

      </Host>
    </Engine>
```

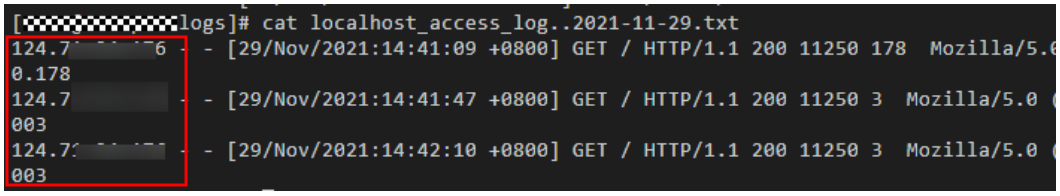
4. 执行如下命令，重启Tomcat服务。
```
cd /usr/tomcat/tomcat8/bin && sh shutdown.sh && sh startup.sh
```
其中“/usr/tomcat/tomcat8/”为Tomcat安装路径，请根据实际情况替换。

图 4-38 重启 Tomcat 服务

5. 执行如下命令，查看最新的日志。

如图中红框所示获取到IP地址，即为获取到的源IP地址。
```
cd /usr/tomcat/tomcat8/logs/
cat localhost_access_log.2021-11-29.txt
```
其中“localhost_access_log.2021-11-29.txt”为当天日志路径，请根据实际情况替换。

图 4-39 查询源 IP 地址



配置 Windows IIS 服务器

本教程以Windows Server 2012配置IIS7为例介绍，其他版本操作可能略有不同。

1. 下载并安装IIS。
2. 从第三方网站下载F5XForwardedFor.dll插件，并获取x86和x64目录下的F5XForwardedFor.dll插件拷贝到IIS服务具有访问权限的目录下，例如C:\F5XForwardedFor2008。
3. 打开IIS管理器，选择“模块 > 配置本机模块”注册拷贝的2个插件。

图 4-40 选择模块选项

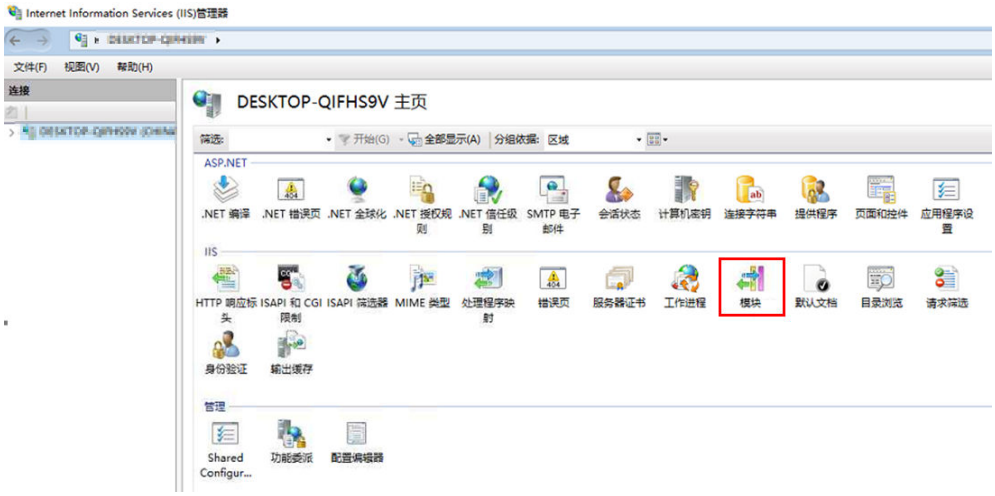
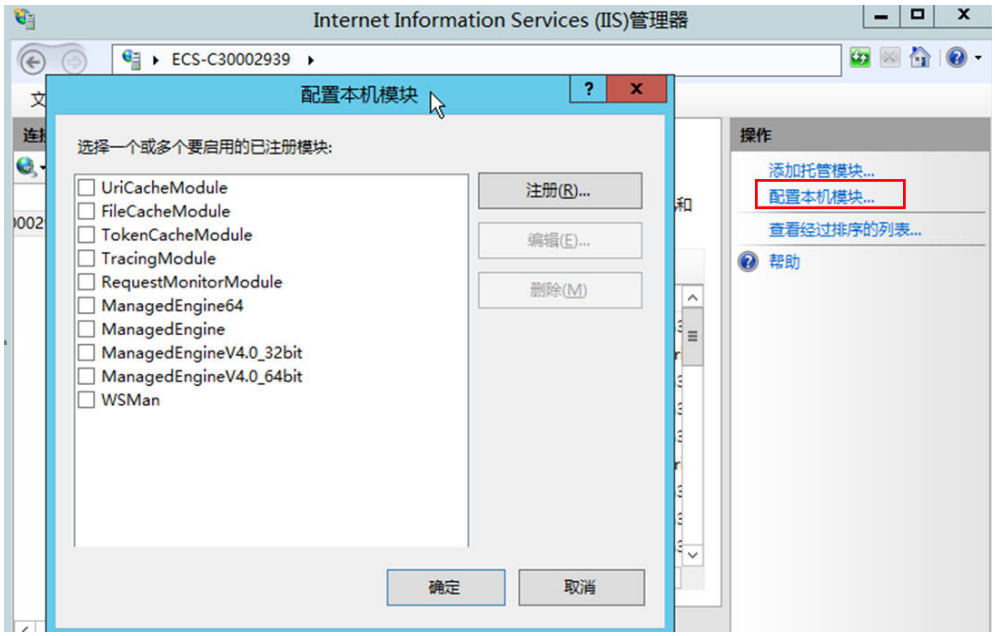
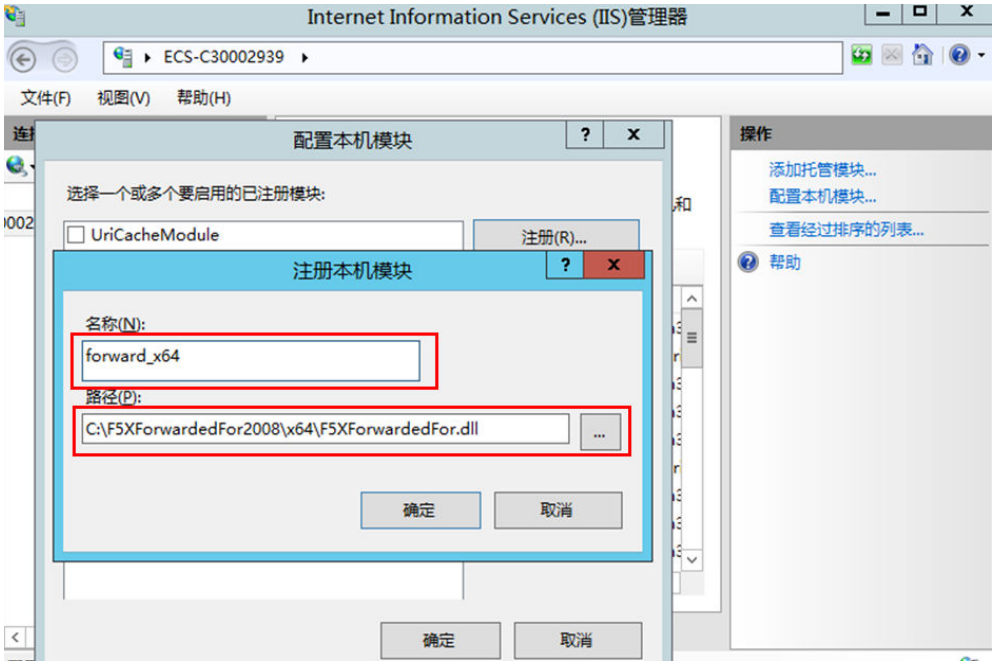


图 4-41 配置本机模块



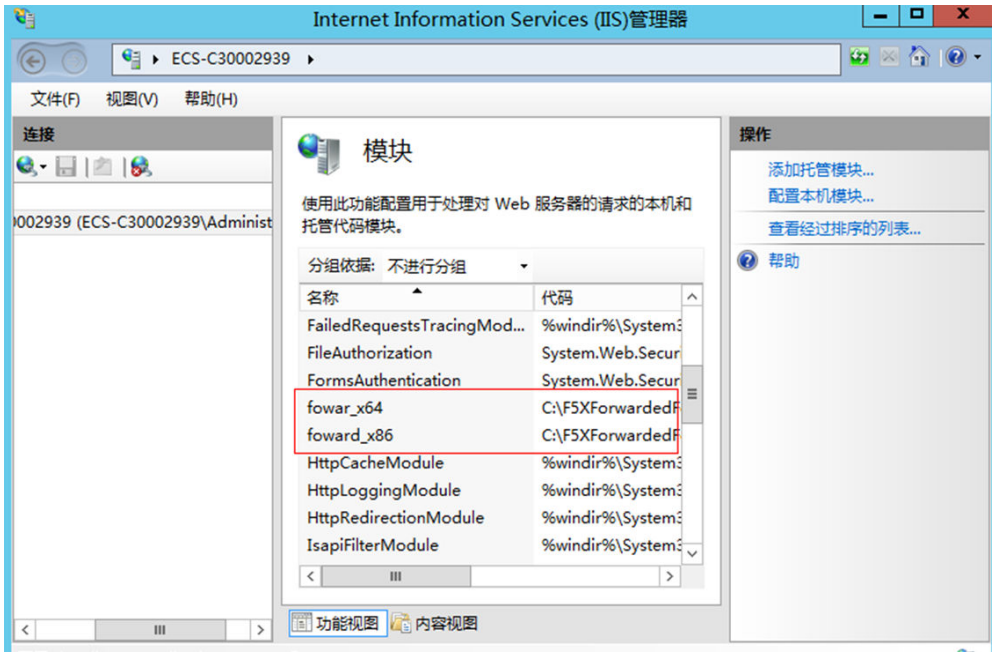
4. 单击“注册”，分别注册x86和x64插件。

图 4-42 注册插件



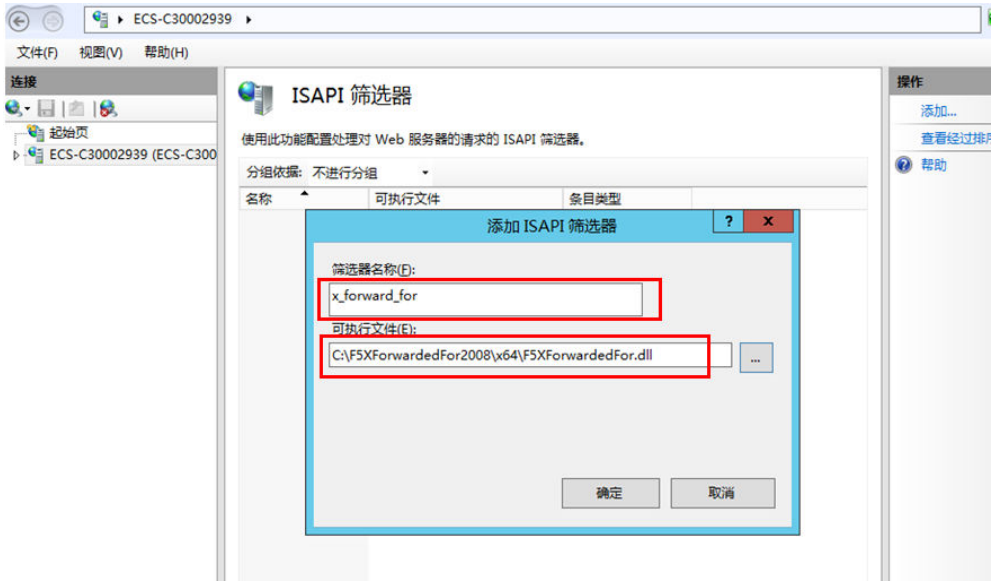
5. 在“模块”页面，确认注册的模块名称出现在列表中。

图 4-43 确认注册成功



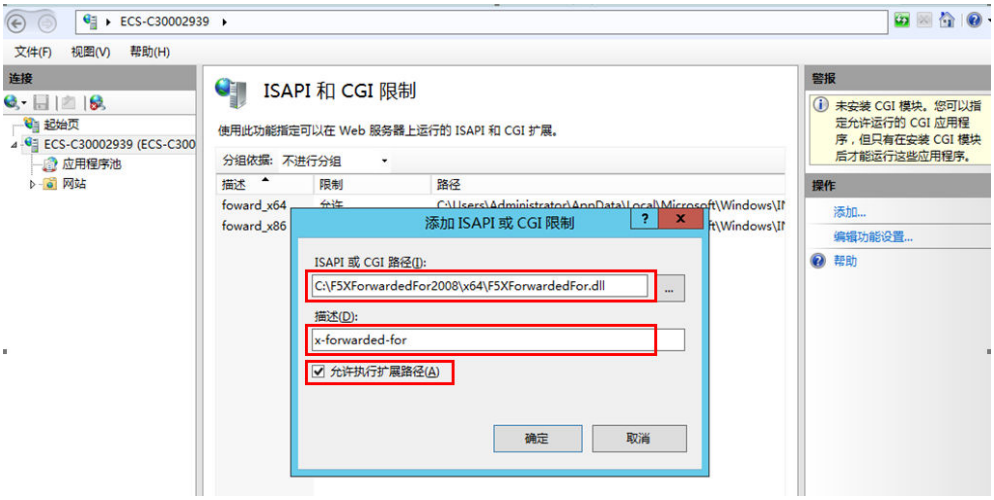
6. 选择IIS管理器主页的“ISAPI筛选器”，为2个插件授权运行ISAPI和CGI扩展。

图 4-44 添加授权



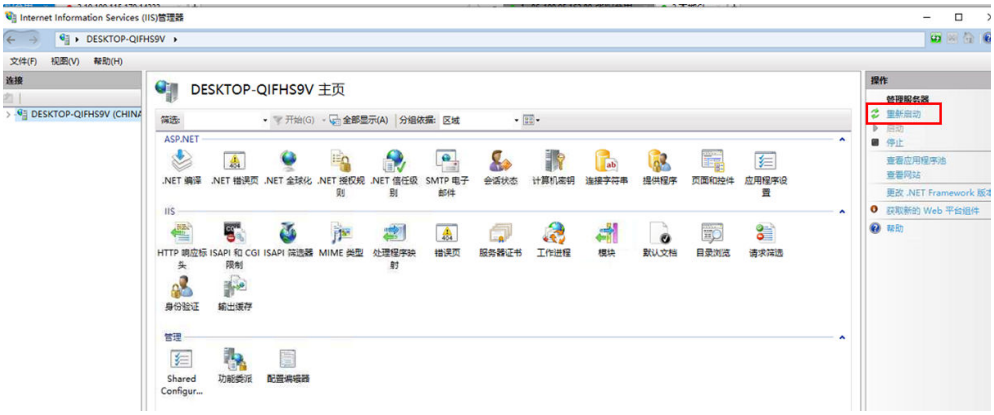
7. 选择“ISAPI和CGI限制”，为2个插件设置执行权限。

图 4-45 允许执行



8. 单击主页的“重新启动”，重启IIS服务，重启后配置生效。

图 4-46 重启 IIS 服务



步骤三：验证后端服务器已获取客户端真实 IP

以Nginx作为后端服务器时，查看Nginx的访问日志，您可以获取客户端请求的真实IP。

```
cat /path/server/nginx/logs/access.log
```

日志记录中，$http_x_forwarded_for变量对应的字段中，第一个IP地址即为客户端的真实IP地址。

图 4-47 查看 Nginx 的日志

4.8 通过 ELB 的访问日志查询客户端请求源 IP

应用场景

使用弹性负载均衡ELB进行业务转发时，获取客户端请求的真实源IP对于数据分析和业务安全防护至关重要。

ELB支持将七层监听器转发的业务接入云日志服务进行分析，通过ELB的访问日志记录即可快速查询访问客户端请求的源IP。

约束与限制

仅采用HTTP/HTTPS/QUIC/TLS监听器的负载均衡实例支持配置访问日志。

准备工作

- 已创建独享型ELB实例，且ELB已绑定EIP。具体操作，请参见**购买独享型负载均衡器**和**绑定IPv4公网IP**。
- 已创建协议类型为HTTPS协议的后端服务器组，服务器组中添加ECS01实例。ECS实例与ELB位于同一VPC内，并且在ECS01中部署了应用服务，部署测试业务详情请参见**搭建后端服务**。
- 您已经开通了云日志服务，并且已经创建了日志组和日志流。具体操作，请参见**弹性负载均衡 ELB接入LTS**。
- 为日志流设置云端结构化解析模板，系统模板选择ELB。具体操作，请参见**设置日志云端结构化解析**。

步骤一：上传服务器证书到 ELB 控制台

在ELB添加HTTPS监听器前，您需要将您的证书上传到将ELB控制台。

1. 进入**弹性负载均衡列表页面**。
2. 在左侧导航栏单击“证书管理”。
3. 单击“创建证书”，配置参数请参见**表4-6**。

表 4-6 服务器证书参数说明

参数	说明
证书类型	创建证书的类型，本文选择服务器证书。
证书来源	服务器证书同时支持SSL证书管理服务提供的数字证书和您的自有证书。 本文选择“SSL证书管理”以同步您在华为云云证书与管理服务已经购买的SSL证书。
证书	选择您需要上传到ELB控制台的证书。
企业项目	企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。
SNI扩展域名（可选）	将自动同步SSL证书已绑定的所有域名。 当您的证书用于配置SNI证书时，将支持根据客户端HTTPS请求的域名来选择对应的SNI证书完成认证。
描述	添加对该证书的描述信息，非必填项。

4. 单击“确定”，完成创建。

步骤二：添加 HTTPS 监听器并配置单向认证

1. 进入**弹性负载均衡列表页面**。
2. 在目标弹性负载均衡实例的操作列，单击“添加监听器”。
3. 在添加监听器页面，协议类型选择“HTTPS”，“SSL解析方式”选择“单向认证”，

   在服务器证书的配置项中选择**步骤一**中上传到ELB控制台的服务器证书。

   独享型ELB的HTTPS协议监听器默认开启“获取客户端IP”功能，支持通过X-Forwarded-For字段传递客户端的真实IP。

图 4-48 添加 HTTPS 监听器并配置单向认证

4. 单击“下一步：配置后端分配策略”，后端服务器组参数选择“使用已有”。选择已经创建完成的服务器组，完成后单击“下一步：确认配置”。
5. 确认配置参数后，单击“提交”，完成HTTPS监听器的创建。

步骤三：配置 ELB 访问日志

1. 进入**弹性负载均衡列表页面**。
2. 在“负载均衡器”界面，单击需要配置访问日志的负载均衡器名称。
3. 在该负载均衡器界面的“访问日志”页签，单击“配置访问日志”。
4. 开启日志记录，选择您在云日志服务中创建的日志组和日志流。

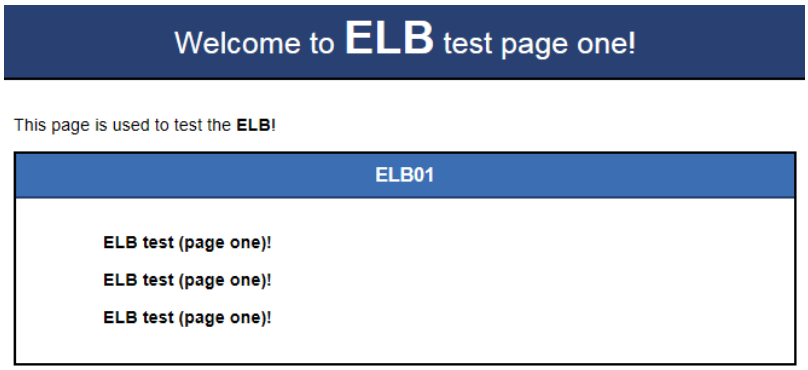
图 4-49 配置 ELB 访问日志

5. 单击“确定”，配置完成。

步骤四：通过弹性公网 IP 访问 ELB

通过在您的浏览器中输入ELB实例绑定的EIP访问ELB实例，页面显示如下图4-50所示，说明访问请求被ELB实例转发至ECS01，应用部署成功。

图 4-50 ECS01 的 nginx 部署成功页面



步骤五：通过访问日志查询客户端 IP

1. 在弹性负载均衡实例的“访问日志”页签，单击“查看详细日志”，访问云日志服务的日志管理列表页。

图 4-51 查看访问日志的日志组

2. 在日志组的列表页，单击日志流名称，进入日志流详情页查看日志。

图 4-52 查看日志流

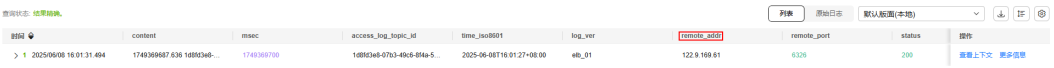
3. 在日志流详情页面，直接查看日志列表的相关字段，即可查看客户端请求的源IP。
   a. 客户端直接访问ELB实例时：日志字段“remote_addr”即为客户端源IP。
   b. 客户端通过代理服务器访问ELB实例时：日志字段“http_x_forwarded_for”中的第一个IP地址即为客户端源IP。

在日志数据中查找包含特定关键词的日志记录，或者根据时间范围来检索日志数据，搜索详情请参考**搜索日志**。

表 4-7 访问日志字段说明

参数	描述	取值说明
remote_addr: remote_port	客户端IP地址：客户端端口。	记录客户端IP地址和客户端端口号。
http_x_forwarded_for	ELB收到请求头中的http_x_forwarded_for，表示请求经过代理服务器。	记录请求经过链路的IP地址，第一个IP地址为客户端源IP。

图 4-53 查看客户端源 IP 地址



相关文档

- **ELB接入访问日志**
- **在七层独享型ELB转发下获取客户端真实IP**
- **在四层独享型ELB转发下获取客户端真实IP**

4.9 通过独享型 ELB 获取客户端证书数据信息

应用场景

当您的业务系统部署在云上并通过ELB对外提供服务时，在ELB上进行双向认证确保了访问客户端的身份安全并降低了在后端服务器进行认证的开发和维护成本。

然而在部分应用层业务授权、个性化定制业务和有较高安全要求的审计场景，后端服务器仍然需要获取请求客户端的身份信息。通过在ELB的监听器上配置请求头获取客户端证书数据信息并传递到转发给后端服务器的报文中，可以在不增加后端服务器业务负担的情况下，使得后端服务可以获取请求客户端的证书信息并进行更精细的安全控制。

说明

该功能陆续上线中，已发布区域请以控制台实际为准。如果您有使用需求，可以提交**工单**进行申请。

准备工作

- 已创建独享型ELB实例，且ELB已绑定EIP。具体操作，请参见**购买独享型负载均衡器**和**绑定IPv4公网IP**。
- 已创建协议类型为HTTPS协议的后端服务器组。服务器组中添加了ECS01实例，并且在ECS01中部署了应用服务。

- 创建两台ECS，ECS与已创建的ELB实例属于同一个VPC，更多详细设置请参考**快速创建ECS**，本实践方案以ECS安装CentOS系统为例。第一台ECS_client用作客户端发送请求，第二台ECS_server用作部署后端应用的后端服务器。
- 为ELB准备证书：
  - 已购买证书或者上传第三方证书到SSL证书服务并绑定公网域名。推荐您在华为云云证书与管理服务购买服务器证书，详情请参见**购买SSL证书**。
  - 已购买CA证书并导出CA证书文件至本地或者直接使用自签名的CA证书。推荐您在华为云云证书与管理服务购买CA证书并导出私有CA证书到您的本地环境，详情请参见**购买私有CA**和**导出私有CA证书**。
- 为客户端准备证书：通过华为云云证书与管理服务创建并激活私有CA后，您就可以通过私有CA申请私有证书并配置到客户端。
  - 私有证书文件名称设置为client.crt，私钥文件文件名称设置为client.key。
  - **申请私有证书**
  - **下载私有证书**
  - **在客户端安装私有证书**

步骤一：上传服务器证书到 ELB 控制台

在ELB添加HTTPS监听器前，您需要将您的证书上传到将ELB控制台。

1. 进入**弹性负载均衡列表页面**。
2. 在左侧导航栏单击“证书管理”。
3. 单击“创建证书”，配置参数请参见**表4-8**。

表 4-8 服务器证书参数说明

参数	说明
证书类型	创建证书的类型，本文选择服务器证书。
证书来源	服务器证书同时支持SSL证书管理服务提供的数字证书和您的自有证书。 本文选择“SSL证书管理”以同步您在华为云云证书与管理服务已经购买的SSL证书。
证书	选择您需要上传到ELB控制台的证书。
企业项目	企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。
SNI扩展域名（可选）	将自动同步SSL证书已绑定的所有域名。 当您的证书用于配置SNI证书时，将支持根据客户端HTTPS请求的域名来选择对应的SNI证书完成认证。
描述	添加对该证书的描述信息，非必填项。

4. 单击“确定”，完成创建。

步骤二：上传 CA 证书到 ELB 控制台

在ELB添加HTTPS监听器前，您需要将您的CA证书上传到ELB控制台。

1. 进入**弹性负载均衡列表页面**。
2. 在左侧导航栏单击“证书管理”。
3. 单击“创建证书”，配置参数请参见**表4-9**。

表 4-9 CA 证书参数说明

参数	说明
证书类型	创建证书的类型，本文选择CA证书。
证书名称	您的CA证书名称。
企业项目	企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。
证书内容	证书内容必须为PEM格式。 单击“上传”，上传您本地的CA证书文件，请确保您的浏览器是最新版本。 证书内容格式如下： -----BEGIN CERTIFICATE----- Base64-encoded certificate -----END CERTIFICATE-----
描述	添加对该证书的描述信息，非必填项。

4. 单击“确定”，完成创建。

步骤三：创建 HTTPS 监听器并配置获取客户端证书数据信息

1. 进入**弹性负载均衡列表页面**。
2. 在目标弹性负载均衡实例的操作列，单击“添加监听器”。
3. 在添加监听器页面，进行如下配置。
   a. **协议类型**：选择“HTTPS”。
   b. **证书配置**：
      i. “SSL解析方式”选择“双向认证”。
      ii. 在服务器证书的配置项中选择**步骤一**中上传到ELB控制台的服务器证书。
      iii. 在CA证书的配置项中选择**步骤二**中上传到ELB控制台的CA证书。

图 4-54 添加 HTTPS 证书配置双向认证

c. **附加HTTP头字段**：

i. 单击展开“更多配置（可选）”。

ii. 单击展开“附加HTTP头字段”下的“客户端证书数据信息”。

iii. 勾选需要添加到转发至后端服务器报文中的证书信息，并输入重写后对应的header头字段名称。

输入字符仅支持小写英文字母、数字、下划线和中划线。

图 4-55 获取客户端证书数据信息

4. 单击“下一步：配置后端分配策略”，后端服务器组参数选择“使用已有”。选择已经创建完成的服务器组，完成后单击“下一步：确认配置”。
5. 确认配置参数后，单击“提交”，完成HTTPS监听器的创建。

步骤四：在后端服务器中部署应用程序

1. 远程登录后端服务器ECS_server。

   弹性云服务器有多种登录方法，具体请参见**登录弹性云服务器**。
2. 请确保服务器端的python版本不低于python 3。
3. 在后端服务器中，新建目录Test。

   ```
   mkdir Test
   ```
4. 在Test目录下，新建一个server.py文件，并且在其中部署应用服务打印出后端服务器收到的请求头。

   a. 新建server.py文件。

   ```
   vi server.py
   ```

   b. 按**i**键进入编辑模式。

   单击查看本示例代码参考

- server.py文件脚本。

```
import http.server
import socketserver
import logging
from datetime import datetime

logging.basicConfig(
    level=logging.INFO,
    format='%(asctime)s - %(message)s',
    handlers=[
        logging.FileHandler('app.log', mode='a'),
        logging.StreamHandler()
    ]
)

class HeaderLoggerHTTPHandler(http.server.BaseHTTPRequestHandler):
    def do_GET(self):
        self.log_headers()
        self.send_response(200)
        self.send_header('Content-type', 'text/plain')
        self.end_headers()
        self.wfile.write(b"Headers logged to app.log")

    def log_headers(self):
        headers = {k: v for k, v in self.headers.items()}
        logging.info(f"{self.command} Request from {self.client_address[0]}")
        for key, value in headers.items():
            logging.info(f"Header: {key} = {value}")


if __name__ == '__main__':
    PORT = 443
    with socketserver.TCPServer(("", PORT), HeaderLoggerHTTPHandler) as httpd:
        print(f"Server started at http://localhost:{PORT}")
        print(f"Headers will be logged to app.log")
        try:
            httpd.serve_forever()
        except KeyboardInterrupt:
            print("\nServer stopped")
```

5. 按**Esc**键，输入**:wq**保存server.py文件。
6. 运行server.py文件。

```
python3 server.py
```

7. 收到如图4-56的回显，表示后端服务部署成功。

图 4-56 后端服务启动成功

步骤五：从客户端访问后端服务

1. 远程登录客户端ECS_client。
2. 将准备工作中已下载至本地的私有证书client.crt和私钥文件client.key上传至客户端。

   上传详情您可以参考**上传文件至云服务器**。
3. 在客户端通过curl命令指定客户端证书文件和与客户端证书配对的私钥文件访问后端服务。

   单击查看本示例curl命令详解

- 用于进行双向认证通信的curl命令语句。
  ```
  curl -k --cert <certificate> --key <private.key> https://<公网IP地址或域名>
  ```
  --cert <certificate>：指定客户端的证书文件，用于完成客户端的身份认证。

  --key <private.key>：指定与客户端证书相对应的私钥文件，用于与客户端证书配合使用完成认证。

  https://<公网IP地址或域名>：指定客户端将要访问的目标地址。

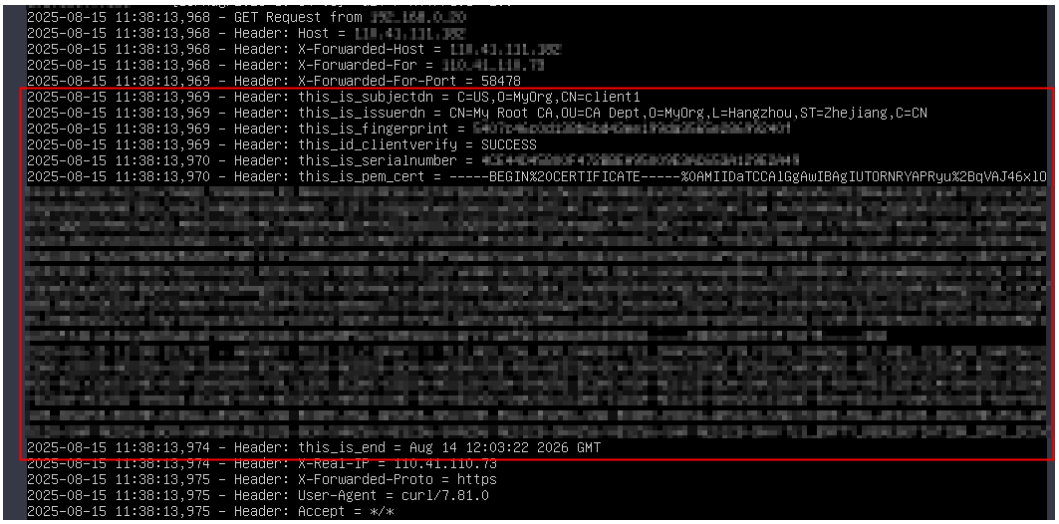
本实践方案使用如下语句访问后端服务：
```
curl -k --cert ./client.crt --key ./client.key https://ELB的EIP地址
```

图 4-57 通过 curl 命令访问后端服务

步骤六：验证服务端获取到客户端证书数据信息

1. 远程登录客户端ECS_server。
2. 在后端服务打印的header头中可以看到客户端证书相关的信息。

图 4-58 验证服务端获取到客户端证书信息



4.10 通过独享型 ELB 的延迟注销实现业务平稳下线

应用场景

如果您发现后端服务器健康检查异常或出于其他业务需求需要移除后端服务器时，该后端服务器已建立的连接通常不会立即中断，导致客户端请求仍然转发至这些后端服务器。这可能会引发业务长期无法下线或出现请求错误的问题。

您可以使用独享型ELB的延迟注销功能。当移除后端服务器或健康检查异常时，该后端服务器的现有连接将在一定时间内正常传输，到达注销时间后主动断开连接，从而保障业务平稳下线。

准备工作

- 已创建独享型ELB实例，具体操作请参考**购买独享型负载均衡器**。
- 创建两台ECS，ECS与已创建的ELB实例属于同一个VPC，更多详细设置请参考**自定义购买ECS**。

  本实践方案以ECS安装CentOS系统为例，一台ECS_client用作客户端发送请求，客户端需支持长连接访问，一台ECS_server用作部署后端应用的后端服务器。

步骤一：创建后端服务器组并开启延迟注销

本实践方案创建开启延迟注销功能的后端服务器组并设置延迟注销时间为30秒。

1. 进入**后端服务器组列表页面**。
2. 在后端服务器列表页面，单击页面右上角“创建后端服务器组”按钮。
3. 配置后端分配策略，关键参数详情请参见**表4-3**，其余配置项保持默认值即可。

表 4-10 配置后端分配策略参数说明

参数	示例	说明
名称	**server_group**	创建的后端服务器组的名称。
负载均衡类型	**独享型**	可使用该后端服务器组的负载均衡实例类型。
所属负载均衡器	**关联已有**	使用该后端服务器组的负载均衡实例。 单击“关联已有”后，选择您已创建完成的负载均衡实例。
后端协议	**TCP**	后端云服务器自身提供的网络服务的协议。 本实践方案选择TCP协议。
分配策略类型	**加权轮询算法**	本实践方案选择加权轮询算法。
延迟注销	**开启**	如果后端协议为TCP/UDP/QUIC协议时，默认开启延迟注销功能。 开启延迟注销功能后，负载均衡器停止向移除的后端云服务器或者健康检查失败的后端云服务器发送新的请求，保持现有连接在延迟注销时间内正常传输。
延迟注销时间（秒）	**30**	负载均衡器与后端服务器的现有连接在延迟注销时间内正常传输，超过延迟注销时间后全部断开。 本实践方案设置为30秒。

4. 单击“下一步”，添加后端服务器并配置健康检查。
5. 单击“添加云服务器”，选择您已创建好的ECS_server实例，其余选项保持默认，完成云服务器的添加。
6. 开启健康检查，其余健康检查参数保持默认。

7. 单击“下一步”。
8. 确认配置无误后，单击“立即创建”。

步骤二：创建 TCP 监听器并配置后端服务器组

本实践方案以TCP监听器为例进行转发。

1. 进入**弹性负载均衡列表页面**。
2. 在目标弹性负载均衡实例的操作列，单击“添加监听器”。
3. 在添加监听器页面，协议类型选择“TCP”，监听端口选择“80”，其余配置保持默认。
4. 单击“下一步：配置后端分配策略”，配置后端服务器组。

   单击“使用已有”，并选择**步骤一：创建后端服务器组并开启延迟注销**中创建的后端服务器组。
5. 单击“下一步：确认配置”，确认完成后，完成TCP监听器的创建。

步骤三：在后端服务器中部署应用

1. 远程登录后端服务器ECS_server。

   弹性云服务器有多种登录方法，具体请参见**登录弹性云服务器**。
2. 在后端服务器中，新建目录Test。

   ```
   mkdir Test
   ```
3. 在Test目录下，新建一个server.py文件，并且在其中部署测试延迟注销的服务，**每秒打印服务端与客户端的连接状态**。

   a. 新建server.py文件。

   ```
   python server.py
   ```

   b. 按**i**键进入编辑模式。

   单击查看本示例代码参考

   - server.py文件脚本，默认端口配置为80。

   ```
   import socket
   import threading
   def handle_client(client_socket, addr):
       print(f"[+] Connection request from {addr}")
       try:
           while True:
               data = client_socket.recv(1024).decode()
               if not data:
                   break
               print(f"[{addr}] Received: {data}")
               client_socket.send(f"ACK: {data}".encode())
       except ConnectionResetError:
           print(f"[-] {addr} Connection interrupted")
       finally:
           client_socket.close()
           print(f"[-] {addr} Connection closed")
   def start_server():
       server = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
       server.bind(('0.0.0.0', 80))
       server.listen(5)
       print("[*] Server started, waiting to be connected...")
       while True:
           client_sock, addr = server.accept()
           client_thread = threading.Thread(target=handle_client, args=(client_sock, addr))
           client_thread.start()
   if __name__ == "__main__":
       start_server()
   ```

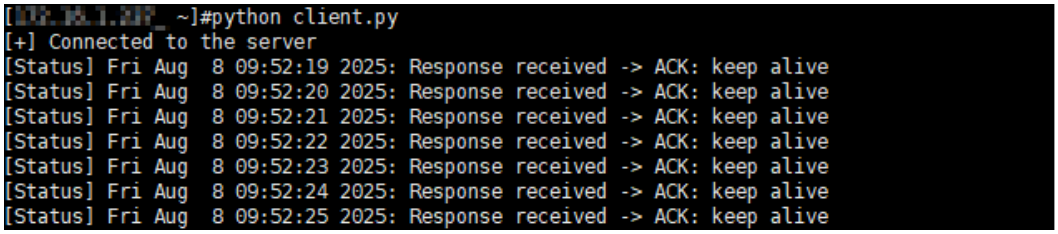

4. 按**Esc**键，输入**:wq**保存server.py文件。
5. 运行server.py文件。
   ```
   python server.py
   ```
6. 收到如图4-59的回显，表示后端服务部署成功。

图 4-59 后端服务启动成功

步骤四：在客户端中部署应用

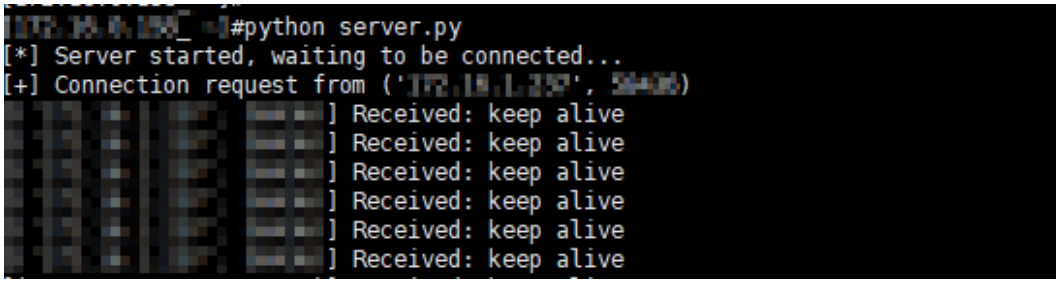
1. 远程登录客户端ECS_client。
2. 在客户端服务器中，新建目录Test_client。
   ```
   mkdir Test_client
   ```
3. 在Test_client目录下，新建一个python_client.py文件，并且在其中部署应用服务，**每秒打印客户端与服务端的连接状态**。
   a. 新建python_client.py文件。
      ```
      vi python_client.py
      ```
   b. 按**i**键进入编辑模式。
      单击查看本示例代码参考
      - python_client.py文件脚本，默认端口配置为80。
        ```
        import socket
        import time
        import threading
        def client_loop():
            try:
                s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
                s.connect(('<your_elb_ip>', 80))   # <your_elb_ip>，替换为您elb实际的私网IP地址
                print("[+] Connected to the server")
                while True:
                    try:
                        s.send("keep alive".encode())
                        response = s.recv(1024).decode()
                        print(f"[Status] {time.ctime()}: Response received -> {response}")
                        time.sleep(1)
                    except (ConnectionResetError, ConnectionAbortedError):
                        print("[-] Connection to server interrupted")
                        break
            except Exception as e:
                print(f"[Error] Connection failed: {e}")
            finally:
                s.close()
        if __name__ == "__main__":
            client_thread = threading.Thread(target=client_loop)
            client_thread.start()
            client_thread.join()
        ```
4. 按**Esc**键，输入**:wq**保存client.py文件。
5. 运行client.py文件。
   ```
   python client.py
   ```
6. 收到如图4-60的回显，客户端打印出时间和连接状态，表示后端服务部署成功。

图 4-60 客户端启动成功



7. 查看后端服务器ECS_server，后端服务服务收到如图4-61的回显，打印出与客户端的连接状态。

图 4-61 后端服务器收到客户端请求



步骤五：移除后端服务器并记录移除时间

本实践以移除后端服务器的场景为例验证延迟注销生效。

1. 进入**后端服务器组列表页面**。
2. 在后端服务器组列表页面，单击需要移除后端服务器的后端服务器组名称。
3. 切换到“后端服务器”页签，选择下方“云服务器”页签。
4. 勾选需要移除的服务器，单击服务器列表上方的“移除”。
5. 在移除后端服务器的对话框中单击“是”。
6. 记录下后端服务服器被移除的时间，此时客户端打印时刻为**09:52:33**。

步骤六：验证延迟注销功能

1. 观察在延迟注销时间内，观察客户端和服务端的打印结果。

   客户端和服务端分别打印出连接状态如图4-62和图4-63，表示两者间保持长连接。

图 4-62 客户端打印连接状态

```
[[redacted]_ ~]#python client.py
[+] Connected to the server
[Status] Fri Aug  8 09:52:19 2025: Response received -> ACK: keep alive
[Status] Fri Aug  8 09:52:20 2025: Response received -> ACK: keep alive
[Status] Fri Aug  8 09:52:21 2025: Response received -> ACK: keep alive
[Status] Fri Aug  8 09:52:22 2025: Response received -> ACK: keep alive
[Status] Fri Aug  8 09:52:23 2025: Response received -> ACK: keep alive
[Status] Fri Aug  8 09:52:24 2025: Response received -> ACK: keep alive
[Status] Fri Aug  8 09:52:25 2025: Response received -> ACK: keep alive
[Status] Fri Aug  8 09:52:26 2025: Response received -> ACK: keep alive
[Status] Fri Aug  8 09:52:27 2025: Response received -> ACK: keep alive
[Status] Fri Aug  8 09:52:28 2025: Response received -> ACK: keep alive
[Status] Fri Aug  8 09:52:29 2025: Response received -> ACK: keep alive
[Status] Fri Aug  8 09:52:30 2025: Response received -> ACK: keep alive
[Status] Fri Aug  8 09:52:31 2025: Response received -> ACK: keep alive
[Status] Fri Aug  8 09:52:32 2025: Response received -> ACK: keep alive
[Status] Fri Aug  8 09:52:33 2025: Response received -> ACK: keep alive
[Status] Fri Aug  8 09:52:34 2025: Response received -> ACK: keep alive
[Status] Fri Aug  8 09:52:35 2025: Response received -> ACK: keep alive
[Status] Fri Aug  8 09:52:36 2025: Response received -> ACK: keep alive
[Status] Fri Aug  8 09:52:37 2025: Response received -> ACK: keep alive
[Status] Fri Aug  8 09:52:38 2025: Response received -> ACK: keep alive
[Status] Fri Aug  8 09:52:39 2025: Response received -> ACK: keep alive
[Status] Fri Aug  8 09:52:40 2025: Response received -> ACK: keep alive
[Status] Fri Aug  8 09:52:41 2025: Response received -> ACK: keep alive
[Status] Fri Aug  8 09:52:42 2025: Response received -> ACK: keep alive
```

图 4-63 服务器打印连接状态

```
[[redacted] ~]#python server.py
[*] Server started, waiting to be connected...
[+] Connection request from ('[redacted]', [redacted])
[('[redacted]', [redacted])] Received: keep alive
[('[redacted]', [redacted])] Received: keep alive
[('[redacted]', [redacted])] Received: keep alive
[('[redacted]', [redacted])] Received: keep alive
[('[redacted]', [redacted])] Received: keep alive
[('[redacted]', [redacted])] Received: keep alive
[('[redacted]', [redacted])] Received: keep alive
[('[redacted]', [redacted])] Received: keep alive
[('[redacted]', [redacted])] Received: keep alive
[('[redacted]', [redacted])] Received: keep alive
[('[redacted]', [redacted])] Received: keep alive
[('[redacted]', [redacted])] Received: keep alive
[('[redacted]', [redacted])] Received: keep alive
[('[redacted]', [redacted])] Received: keep alive
[('[redacted]', [redacted])] Received: keep alive
[('[redacted]', [redacted])] Received: keep alive
[('[redacted]', [redacted])] Received: keep alive
[('[redacted]', [redacted])] Received: keep alive
[('[redacted]', [redacted])] Received: keep alive
[('[redacted]', [redacted])] Received: keep alive
[('[redacted]', [redacted])] Received: keep alive
[('[redacted]', [redacted])] Received: keep alive
[('[redacted]', [redacted])] Received: keep alive
```

2. 等待延迟注销时间30秒后，观察客户端和服务端的打印结果。

   客户端和服务端分别打印出如图4-64和图4-65的回显，表明延迟注销时间结束后，客户端与后端服务器之间的连接断开。根据图4-64显示连接断开时间为**09:53:03**，与移除后端服务器时间**09:52:33**间隔为设置的延迟注销时间30秒。

图 4-64 客户端打印连接断开

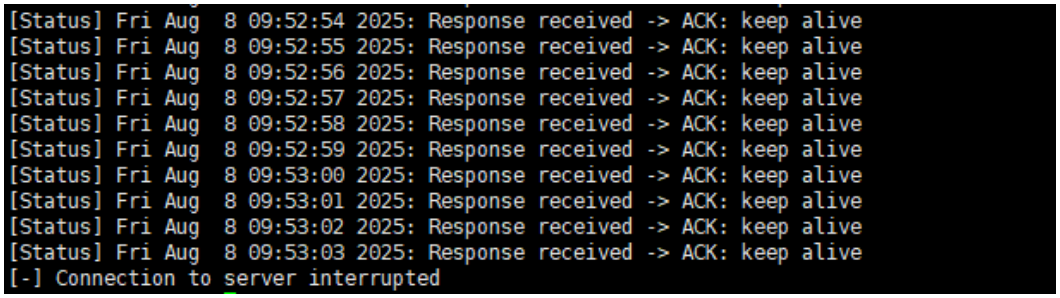
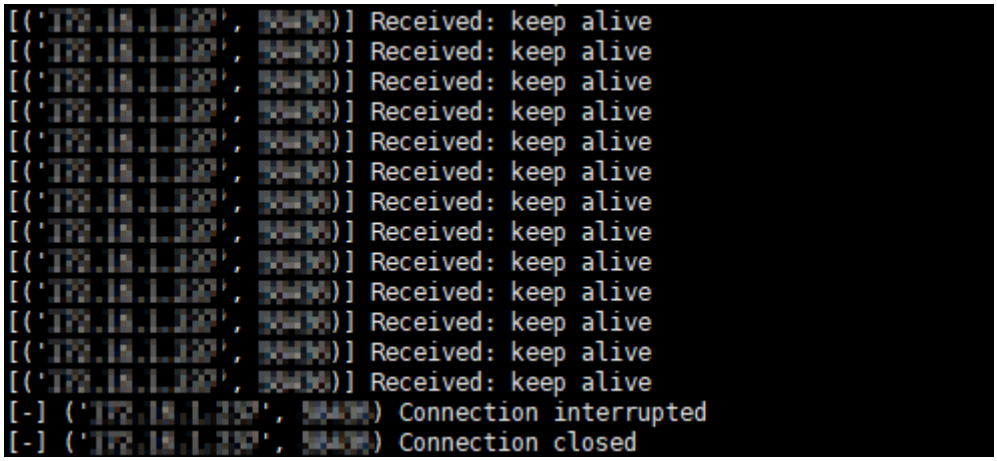


图 4-65 服务器端打印连接断开



5 转发策略

5.1 通过 ELB 的高级转发策略实现新旧版本应用平滑过渡

应用场景

随着公司业务发展，需要用新版本应用替换旧版本应用，使用高级转发策略可以实现旧版本应用向新版本应用平滑过渡。将旧版本应用和新版本应用同时部署在环境中，让一部分用户使用旧版本应用，一部分用户使用新版本应用，然后根据用户使用情况，调整优化新版本应用，逐步将所有用户均迁移至新版本应用。

前提条件

已申请了6台ECS，将您的旧版本业务和新版本业务各自部署在3台服务器上。

操作流程

图 5-1 操作流程图

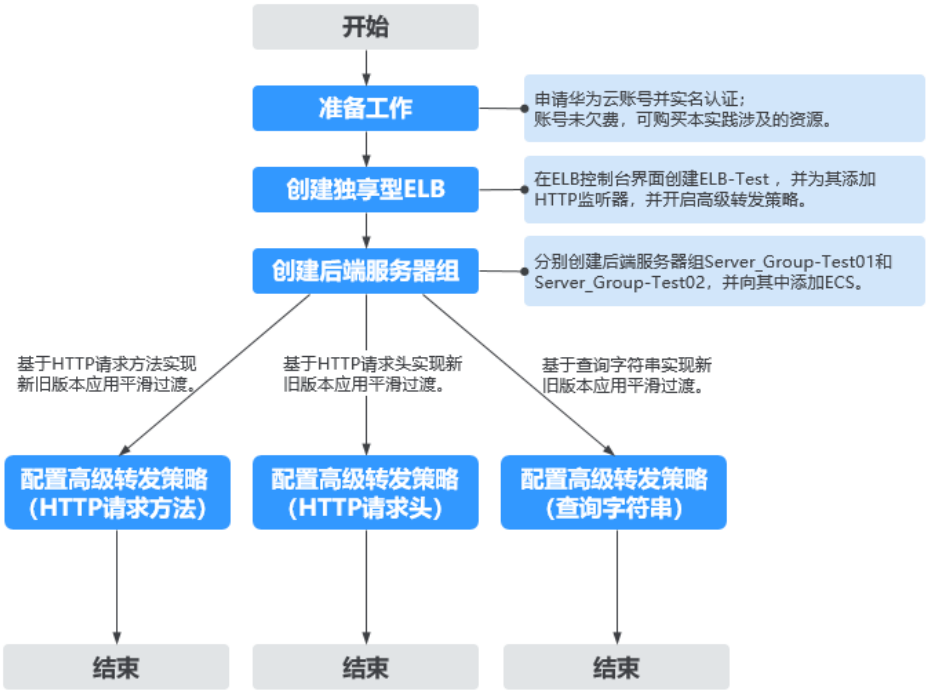


表 5-1 资源规划

资源名称	资源类型	说明
ELB-Test	独享型ELB	独享型ELB支持高级转发策略，因此需创建独享型ELB实例。
Server_Group-Test01	后端服务器组	用于管理部署了旧版本业务的ECS。
Server_Group-Test02	后端服务器组	用于管理部署了新版本业务的ECS。
ECS01	弹性云服务器	上面部署了旧版本业务，添加至Server_Group-Test01。
ECS02	弹性云服务器	上面部署了旧版本业务，添加至Server_Group-Test01。
ECS03	弹性云服务器	上面部署了旧版本业务，添加至Server_Group-Test01。
ECS04	弹性云服务器	上面部署了新版本业务，添加至Server_Group-Test02。
ECS05	弹性云服务器	上面部署了新版本业务，添加至Server_Group-Test02。

资源名称	资源类型	说明
ECS06	弹性云服务器	上面部署了新版本业务，添加至Server_Group-Test02。

说明

本最佳实践中，独享型ELB和ECS均在同一VPC中。在实际应用中，如果您的ECS和ELB不在同一VPC中，可以跨不同VPC添加ECS至ELB的后端服务器组中，详细请参考**通过IP类型后端功能添加服务器至ELB**。

步骤一：创建 HTTP 监听器并开启高级转发策略

1. 进入**弹性负载均衡列表页面**。
2. 单击右上角的“购买弹性负载均衡”。
3. 根据**表5-1**创建独享型负载均衡ELB-Test，根据需要设置相关参数。
   - 实例规格类型：独享型
   - 名称：ELB-Test
   - 其他参数根据需要设置，详见**创建独享型负载均衡器**。
4. 独享型ELB创建成功后，在ELB-Test中添加HTTP监听器。详见**添加监听器**。
5. HTTP监听器创建成功后，开启高级转发策略。详见**高级转发策略**。

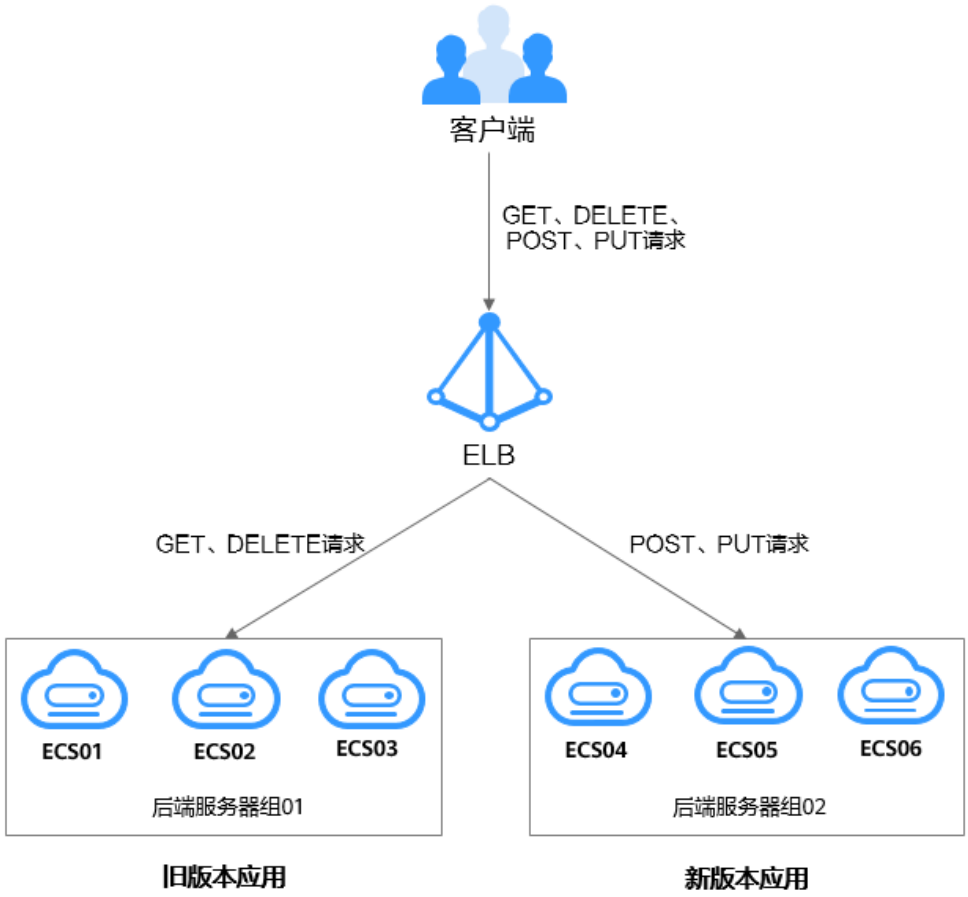
步骤二：创建后端服务器组并添加后端服务器

1. 进入**弹性负载均衡列表页面**。
2. 在左侧导航栏，选择“ 弹性负载均衡 > 后端服务器组”。
3. 在“后端服务器组”界面，单击页面右上角“创建后端服务器组”按钮
   - 名称：Server_Group-Test01
   - 所属负载均衡器：选择关联已有ELB-Test
   - 后端协议：HTTP
   - 其他参数根据需要设置。
4. 参考**步骤5**再添加后端服务器组Server_Group-Test02。
5. 单击后端服务器组Server_Group-Test01名称，添加ECS01、ECS02、ECS03至Server_Group-Test01。
6. 单击后端服务器组Server_Group-Test02名称，添加ECS04、ECS05、ECS06至Server_Group-Test02。

基于 HTTP 请求方法实现新旧版本应用平滑过渡

通过配置转发规则为“HTTP请求方法”的高级转发策略，实现将来自客户端的**GET和DELETE**请求转发至**旧版本应用**上，将来自客户端的**POST和PUT**请求转发至**新版本应用**上。以此种方式运行一段时间后，确认新版本应用无问题后，再将所有请求全部切换至新版本应用。

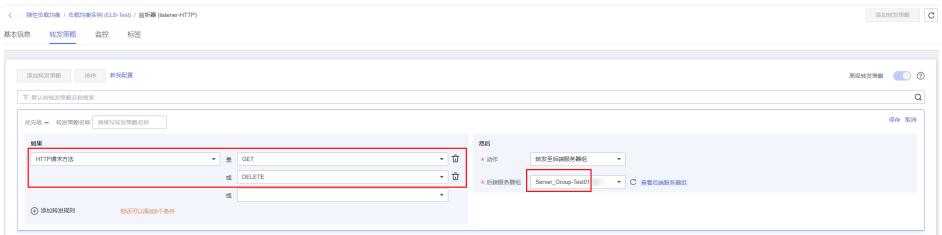
图 5-2 基于 **HTTP 请求方法**实现新旧版本应用平滑过渡



1. 单击上述创建的独享型负载均衡ELB-Test名称。
2. 在“监听器”页签，单击上述创建的HTTP监听器名称。
3. 切换至右边的“转发策略”页面，单击“添加转发策略”。

   转发至旧版本应用：在下拉列表中选择“HTTP请求方法”，选择“GET”和“DELETE”，动作选择“转发至后端服务器组”，后端服务器组选择“Server_Group-Test01”。

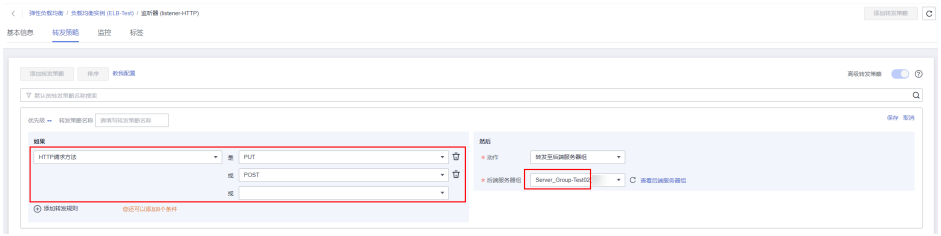
   图 5-3 基于 HTTP 请求方法将部分请求转发至旧版本应用上

4. 单击“保存”。
5. 参考以上步骤再添加一个转发策略，实现将请求转发至新版本应用上。

   转发至新版本应用：在下拉列表中选择“HTTP请求方法”，选择“PUT”和“POST”，动作选择“转发至后端服务器组”，后端服务器组选择“Server_Group-Test02”。

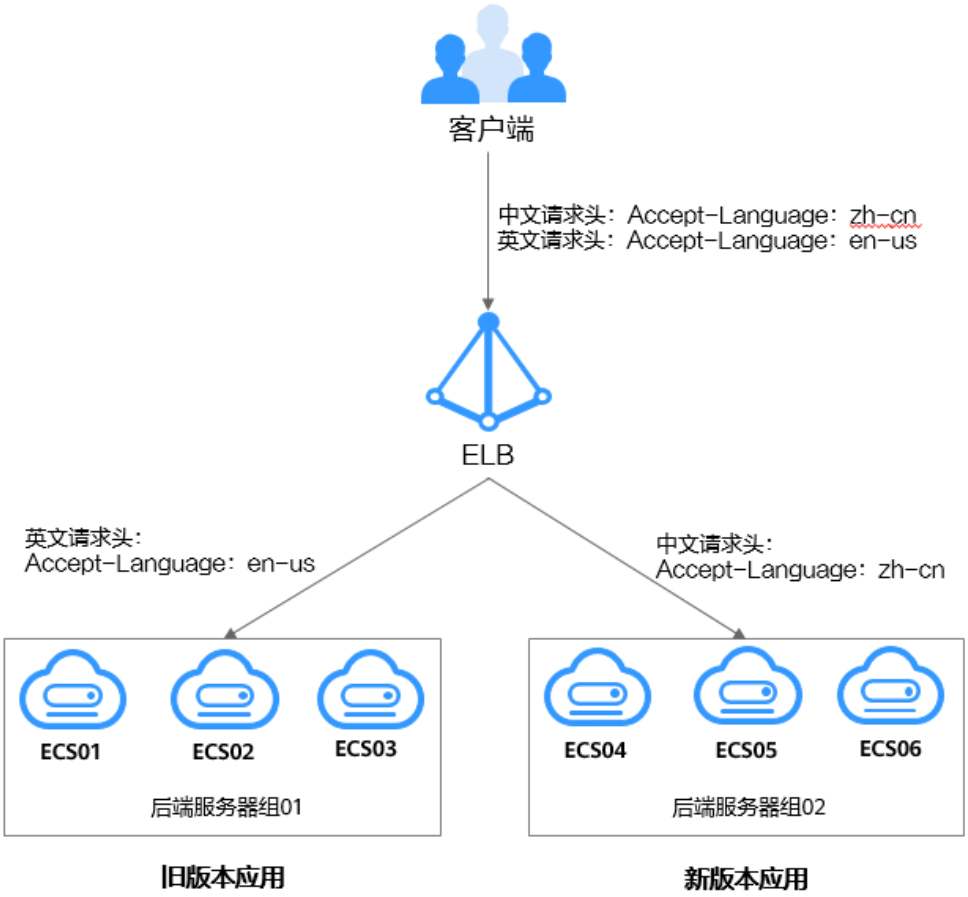
图 5-4 基于 HTTP 请求方法将部分请求转发至新版本应用上



基于 HTTP 请求头实现新旧版本应用平滑过渡

公司的应用分为中文和英文两个语言，通过配置转发规则为“HTTP请求头”的高级转发策略，实现将来自客户端的**英文请求**转发至**旧版本应用**上，将来自客户端的**中文请求**转发至**新版本应用**上。以此种方式运行一段时间后，确认新版本应用无问题后，再将所有请求全部切换至新版本应用。

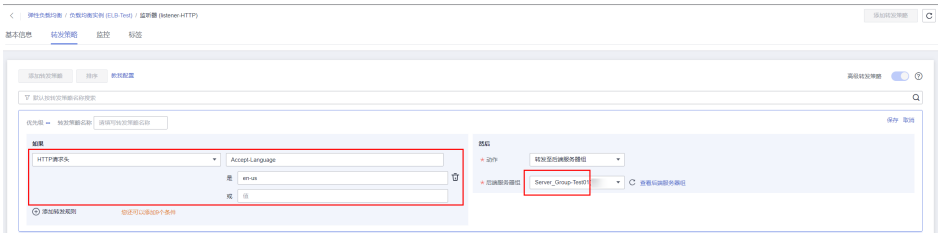
图 5-5 基于 **HTTP 请求头**实现新旧版本应用平滑过渡



1. 单击上述创建的独享型负载均衡ELB-Test名称。
2. 切换至“监听器”页签，单击上述创建的HTTP监听器名称。
3. 切换至右边的“转发策略”页面，单击“添加转发策略”。

   转发至旧版本应用：在下拉列表中选择“HTTP请求头”，键是“Accept-Language”，值是“en-us”，动作选择“转发至后端服务器组”，后端服务器组选择“Server_Group-Test01”。

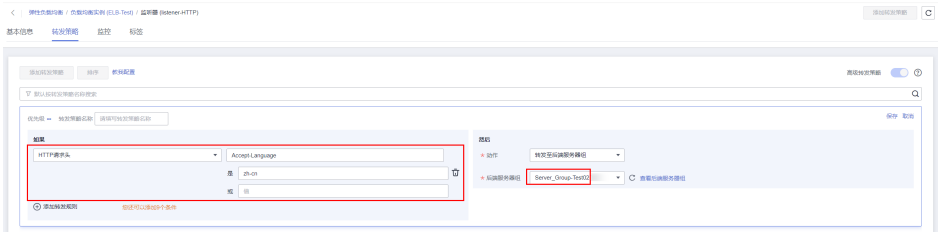
图 5-6 基于 HTTP 请求头将部分请求转发至旧版本应用上



4. 单击“保存”。
5. 参考以上步骤再添加一个转发策略，实现将请求转发至新版本应用上。

   转发至新版本应用：在下拉列表中选择“HTTP请求头”，键是“Accept-Language”，值是“zh-cn”，动作选择“转发至后端服务器组”，后端服务器组选择“Server_Group-Test02”。

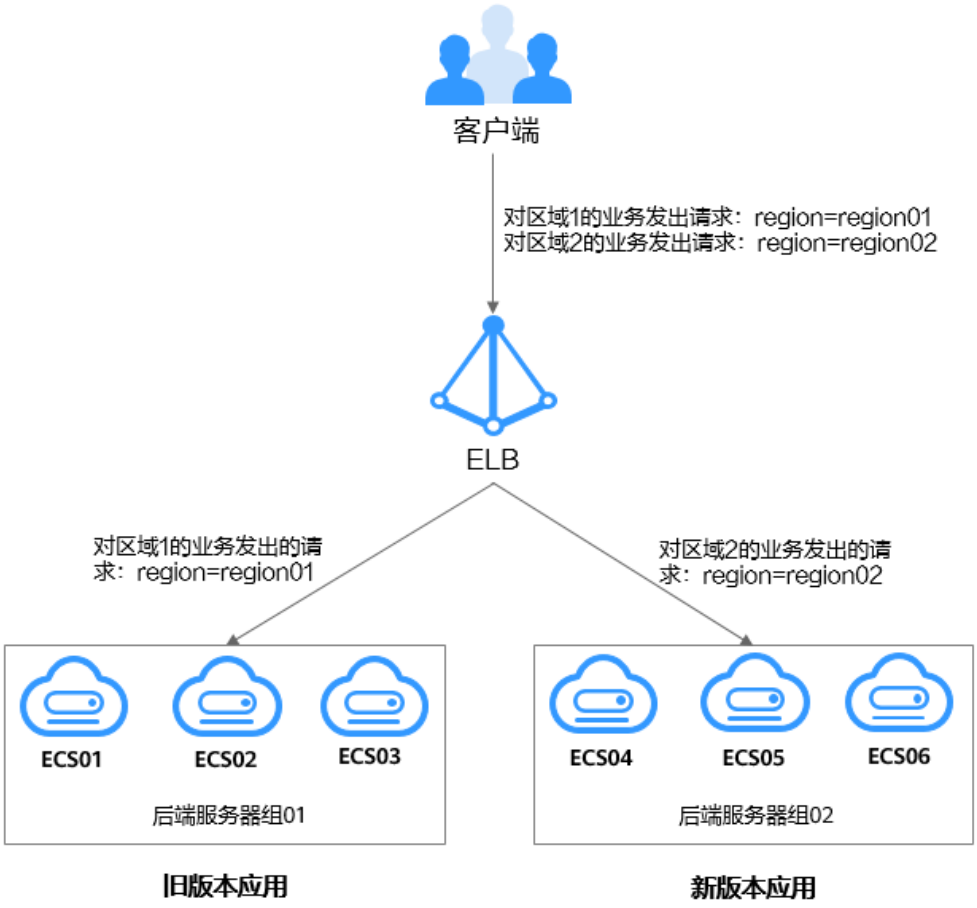
图 5-7 基于 HTTP 请求头将部分请求转发至新版本应用上



基于查询字符串实现新旧版本应用平滑过渡

公司的应用部署在区域1和区域2，通过配置转发规则为“查询字符串”的高级转发策略，实现将客户端对**区域1业务**的请求转发至**旧版本应用**上，将客户端对**区域2业务**的请求转发至**新版本应用**上。以此种方式运行一段时间后，确认新版本应用无问题后，再将所有请求全部切换至新版本应用。

图 5-8 基于**查询字符串**实现新旧版本应用平滑过渡



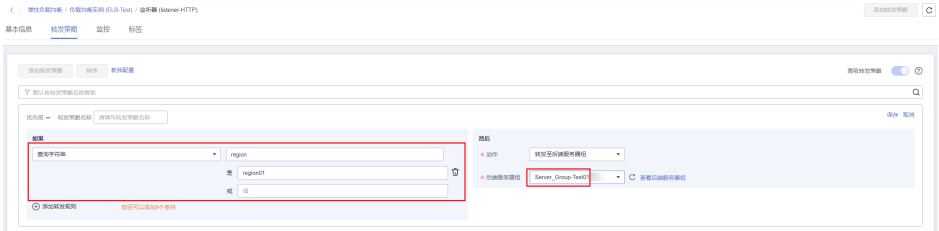
说明

- 独享型负载均衡器支持跨区域、跨不同VPC添加后端服务器。
- 该方案需要先使用云连接服务连通区域1和区域2，然后再使用独享型ELB的跨VPC后端功能将区域1和区域2中的服务器分别添加至ELB的后端服务器组01和后端服务器02中。

1. 单击上述创建的独享型负载均衡ELB-Test名称。
2. 在“监听器”页签，单击上述创建的HTTP监听器名称。
3. 切换至右边的“转发策略”页面，单击“添加转发策略”。

   转发至旧版本应用：在下拉列表中选择“查询字符串”，键是“region”，值是“region01”，动作选择“转发至后端服务器组”，后端服务器组选择“Server_Group-Test01”。

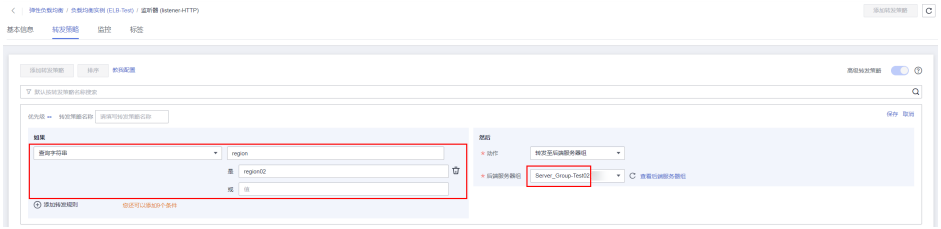
图 5-9 基于查询字符串将部分请求转发至旧版本应用上



4. 单击“保存”。
5. 参考以上步骤再添加一个转发策略，实现将请求转发至新版本应用上。

   转发至新版本应用：在下拉列表中选择“查询字符串”，键是“region”，值是“region02”，动作选择“转发至后端服务器组”，后端服务器组选择“Server_Group-Test02”。

图 5-10 基于查询字符串将部分请求转发至新版本应用上



5.2 配置相同域名不同路径的转发策略实现精准转发

应用场景

独享型负载均衡支持您基于域名和路径将接收到的客户端请求精确地分配到不同的后端服务器组上，以实现高效、合理、精细化管理的流量分发功能。

- **微服务架构**：在微服务架构中，后端服务由多个独立的子服务组成，每个子服务部署在不同的后端服务器上，对外使用同一个域名进行服务。通过基于路径的转发策略，客户端请求被精确分配到处理对应业务逻辑的后端服务器上。
- **灰度发布/AB测试**：在多环境部署中，开发、测试和生产环境可能部署在同一域名下但使用不同路径。通过配置相同域名不同路径转发策略，请求被精确转发到目标环境的后端服务器上。
- **读写分离**：在高并发和数据一致性要求严格的场景下，如订单处理服务，采用读写分离策略优化性能与数据安全。读操作定向转发到读数据库，写操作定向转发到写数据库。

基于域名和路径的转发策略概述

独享型ELB支持高级转发策略，支持基于客户端请求的不同特征设置转发规则和转发动作，便于更灵活分流业务，更合理分配资源。

基于域名和路径的转发规则详见**表5-2**，更多转发规则详情请参考**高级转发策略概述**。

表 5-2 域名和路径的转发规则说明

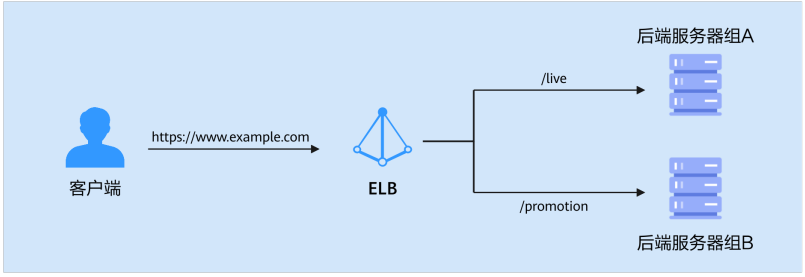
转发规则	描述
域名	• 匹配说明 触发转发的域名，可以并列添加多个域名。域名由以点分隔的字符串组成，单个字符串不超过63个字符，域名总长度不能超过100个字符。 • 匹配方式 – 精确匹配及通配符匹配：只能由英文字母、数字和特殊字符.-?=~_+\^*!$&\|()[]组成，支持星号（*）和半角问号（？）作为通配符使用。不支持以.开头和结尾，不支持..的形式。 – 正则匹配：只能由英文字母、数字和特殊字符.-?=~_+\^*!$&|()[]组成。
路径	• 匹配说明 触发转发的路径，可以并列添加多个路径。路径由英文字母、数字和特殊字符_~';@^-%#$.*+?,=!:|\/()[]{}组成，长度范围为1~128个字符。 • 匹配方式 – 精确匹配：请求的路径和设定路径完全一致，只能由/开头。 – 前缀匹配：请求的路径匹配已设定路径的开头，只能由/开头。 – 正则匹配：请求的路径和设定的路径正则表达式匹配。

实践方案架构

某电商平台希望通过一个域名对外提供多样化的微服务，包括直播和促销活动的能力。直播功能需要高带宽和低延迟的处理能力，而促销活动的能力可能会在短时间内涌入大量客户，导致流量徒增，并产生大量数据读取的动作。如果所有服务在一个后端服务器组上部署，可能导致资源分配不均，在促销活动高峰期影响直播用户的浏览体验。尤其是在用户访问量激增时，服务器负载过高，无法保证服务稳定运行。

该电商平台可以利用华为云独享型ELB实例配置相同域名下不同路径的转发策略实现更加精准的业务流量分发，确保每个微服务都能高效独立运行。如下图5-11，路径**/live**的请求转发至直播服务器组后端服务器组A，确保直播服务获得足够的带宽和处理能力。路径**/promotion**的请求转发至后端服务器组B，优化计算资源以快速响应查询和提交操作。

图 5-11 ELB 实例配置相同域名不同路径的业务转发示意图



约束与限制

- 仅独享型ELB的HTTP/HTTPS/QUIC监听器支持配置高级转发策略。
- 单个监听器最多支持配置100条转发策略，超过配额的转发策略不生效。
- 高级转发策略：一种转发规则支持多个转发条件，一条转发策略最多支持10个转发条件。

准备工作

- 创建独享型ELB实例，且ELB已绑定EIP。具体操作，请参见**购买独享型负载均衡器**和**绑定IPv4公网IP**。
- 创建两个协议类型为**HTTP**协议的后端服务器组，后端服务器组A和后端服务器组B中分别添加了ECS01和ECS02实例，并且在其中部署了应用服务。

  单击查看本示例ECS01的部署命令
  - yum install -y nginx
  - systemctl start nginx.service
  - cd /usr/share/nginx/html/
  - echo "Hello World ! This is live." > index.html

  单击查看本示例ECS02的部署命令
  - yum install -y nginx
  - systemctl start nginx.service
  - cd /usr/share/nginx/html/
  - echo "Hello World ! This is promotion." > index.html
- 注册域名并完成备案。本实践推荐使用域名www.example.com。

步骤一：开启高级转发策略

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要添加转发策略的负载均衡器名称。
3. 在“监听器”页签，单击目标监听器名称。
4. 在监听器“基本信息”页面，单击“开启高级转发策略”。
5. 单击“确认”。

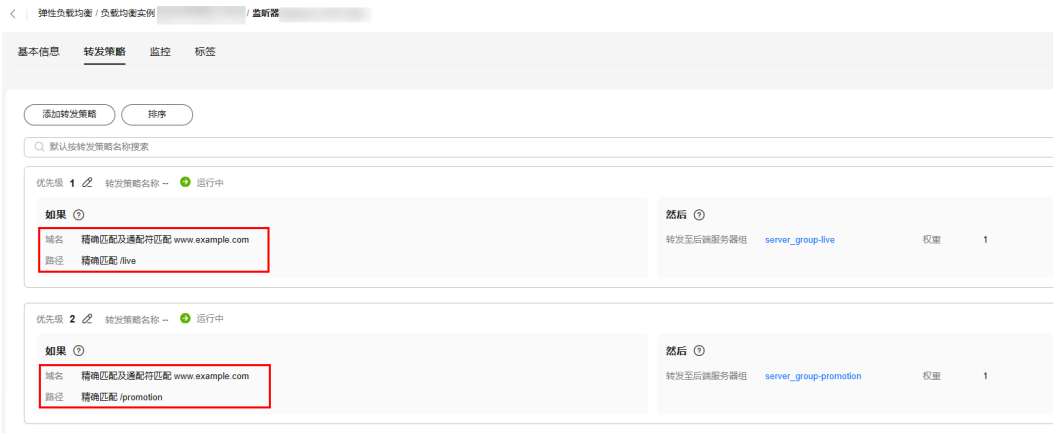
步骤二：配置高级转发策略

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要添加转发策略的负载均衡器名称。
3. 在“监听器”页签，您可以通过以下两种操作入口，进入监听器的“转发策略”页签。
   - 在目标监听器所在行的“操作”列，单击“添加/编辑转发策略”。
   - 单击目标监听器的名称，并切换到“转发策略”页签。
4. 单击“添加转发策略”按钮，配置转发策略。

   域名：输入您用于本实践方案的域名。

   路径：当路径为live时，转发到后端服务器组A；路径为promotion时，转发到后端服务器组B。

5. 配置完成，单击“保存”。



步骤三：配置域名解析

通过为域名添加A类型记录集解析，将域名解析到ELB的公网地址，使得客户端可以通过公网域名访问ELB。

以下提供将网站域名解析至IPv4地址的配置示例，更多关于A类型记录集的配置指导，请参考**配置网站解析**。

1. 进入**云解析服务控制台**。
2. 在左侧树状导航栏，选择“公网域名”。
   进入域名列表页面。
3. 在待添加记录集的公网域名所在行，单击操作列的“管理解析”。
4. 单击“添加记录集”，进入“添加记录集”页面。
5. 设置记录集参数，如**表5-3**所示。

表 5-3 A 类型记录集参数说明

参数	示例	说明
记录类型	**A – 将域名指向IPv4地址**	记录集的类型，本实践为**A – 将域名指向IPv4地址**。
主机记录	**www**	您域名的前缀。
线路类型	**全网默认**	解析的线路类型用于DNS服务器在解析域名时，根据访问者的来源，返回对应的服务器IP地址。 默认值为“全网默认”。 全网默认：默认线路类型，当未根据访问者来源设置解析线路时，系统会返回默认解析结果。
TTL(秒)	**300**	解析记录在本地DNS服务器的缓存时间，以秒为单位。 本实践使用默认值300秒。
记录值	**192.168.12.2**	域名对应的IPv4地址，本实践为ELB绑定的弹性公网IP地址。

参数	示例	说明
高级配置（可选）	-	您可以单击 ，展开折叠的高级配置区域，设置记录集的别名和权重并添加标签和描述，本文保持默认设置。

6. 单击“确定”。
7. 返回“解析记录”页面。

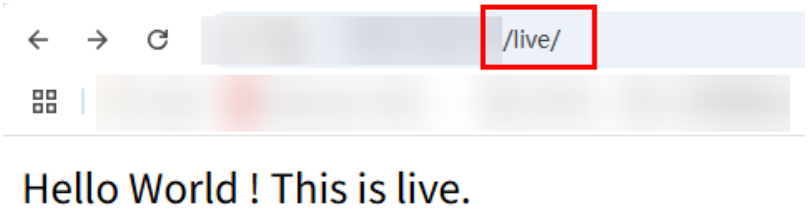
   添加完成后，您可以在域名对应的记录集列表中查看已添加的记录集。当记录集的状态显示为“正常”时，表示记录集添加成功。

步骤四：结果验证

使用浏览器访问http://<域名>/<路径>/，验证ELB将相同域名不同路径的请求转发到对应的后端服务器。

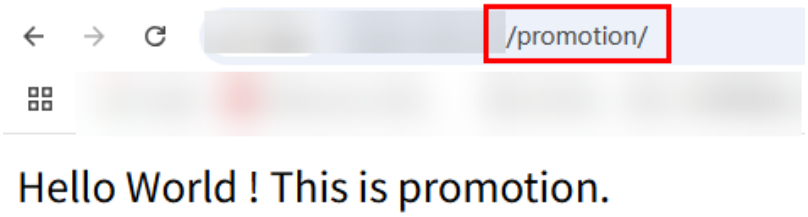
1. 访问地址 **http://www.example.com/live/**，收到如图5-12所示响应。

   图 5-12 客户端请求访问路径 live

2. 访问地址 **http://www.example.com/promotion/**，收到如图5-13所示响应。

   图 5-13 客户端请求访问路径 promotion

相关文档

- **通过ELB的高级转发策略实现新旧版本应用平滑过渡**
- **通过ELB将HTTP请求重定向至HTTPS**

6 ELB 与云原生应用

ELB可以作为云容器引擎CCE流量入口的负载均衡器，通过ELB接入客户的服务请求并转发到CCE的POD/容器中。

CCE中使用ELB的场景如下：

1. CCE的service 主要使用ELB的4层（TCP/UDP监听器）作为负载均衡， 也支持使用7层(HTTP/HTTPS监听器）作为负载均衡，使用一些7层功能，如证书卸载、7层访问日志、7层丰富的CES监控指标等。
2. CCE的ELB ingress 使用ELB的7层（HTTP/HTTPS监听器)，支持更多应用层高级功能，如7层路由，证书卸载、7层访问日志，7层丰富的监控指标。

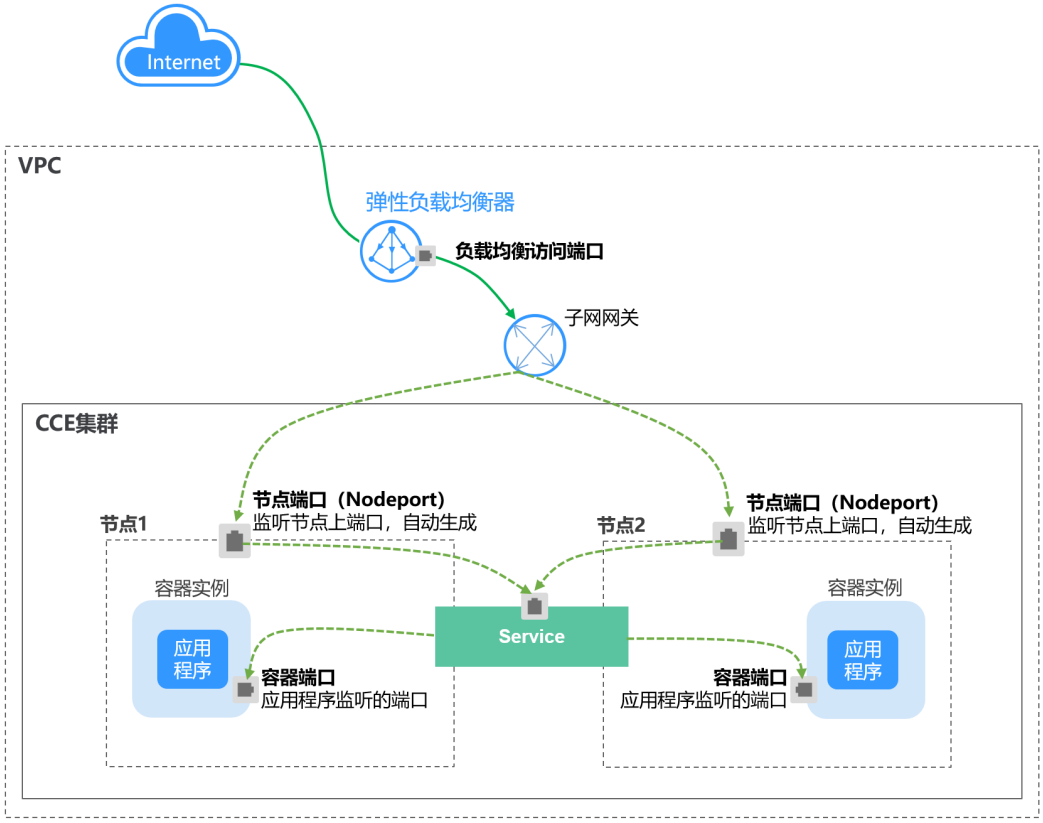
CCE具有强大的弹性能力和自动化能力，能快速拉起后端负载，结合ELB可以实现的服务的高可用、灰度发布等多种弹性和高可用场景。

CCE 集群通过负载均衡类的服务对外提供访问

负载均衡（LoadBalancer）类型的服务在NodePort的基础上添加了外部负载均衡器，可以通过弹性负载均衡（ELB）将外部流量向集群内的多个Pod进行分发，与NodePort类型相比提供了高可靠的保障。Service会自动分配一个外部IP地址，允许客户端通过该IP访问服务。该类型服务不仅支持在OSI模型的第四层（传输层）处理TCP和UDP流量，还能扩展至第七层（应用层），支持HTTP和HTTPS流量的管理。

在云上提供应用访问时，若您需要提供一个稳定且易于管理的对外访问入口，可以使用负载均衡类型的服务。例如生产环境中需从互联网访问的公共服务，这些服务需承受大量外部流量并确保高可用性，如Web应用和API服务等。负载均衡类型服务的访问方式由公网弹性负载均衡服务地址以及设置的访问端口组成，例如“10.117.117.117:80”。

图 6-1 负载均衡（LoadBalancer）



如果您需要配置负载均衡类型的服务，请参考。

通过注解（Annotations）配置负载均衡的高级功能

创建LoadBalancer类型的服务通常为您提供四层的网络访问。通过在YAML中添加注解Annotation（注解），您可以实现CCE提供的一些高级功能。

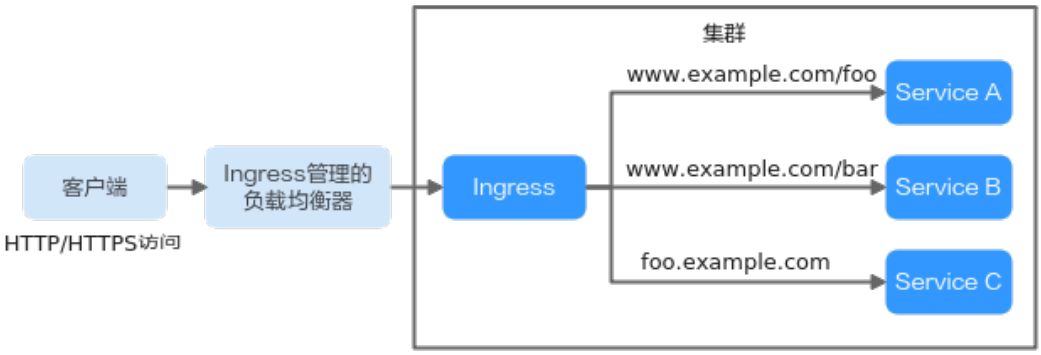
如果您需要在创建LoadBalancer类型的Service时配置更多高级功能，请参考。

云容器引擎 CCE 使用 ELB Ingress

Service基于TCP和UDP协议进行访问转发，为集群提供了四层负载均衡的能力。但是在实际场景中，Service无法满足应用层中存在着大量的HTTP/HTTPS访问需求。因此，Kubernetes集群提供了另一种基于HTTP协议的访问方式——Ingress。

Ingress是Kubernetes集群中一种独立的资源，制定了集群外部访问流量的转发规则。如图6-2所示，用户可根据域名和路径对转发规则进行自定义，完成对访问流量的细粒度划分。

图 6-2 Ingress 示意图



当您希望在CCE集群中配置ELB Ingress实现Ingress流量管理时，请参考。

通过注解（Annotations）配置 ELB Ingress 高级功能

通过在YAML中添加注解（Annotations），您可以实现更多的Ingress高级功能，如果您有使用Ingress高级功能的需求请参考。

自建 Nginx Ingress 迁移到 ELB Ingress

ELB Ingress是基于华为云弹性负载均衡（Elastic Load Balance）实现的Ingress服务。相比于自建Nginx Ingress，ELB Ingress提供更为强大的Ingress流量管理功能，具有以下优势：

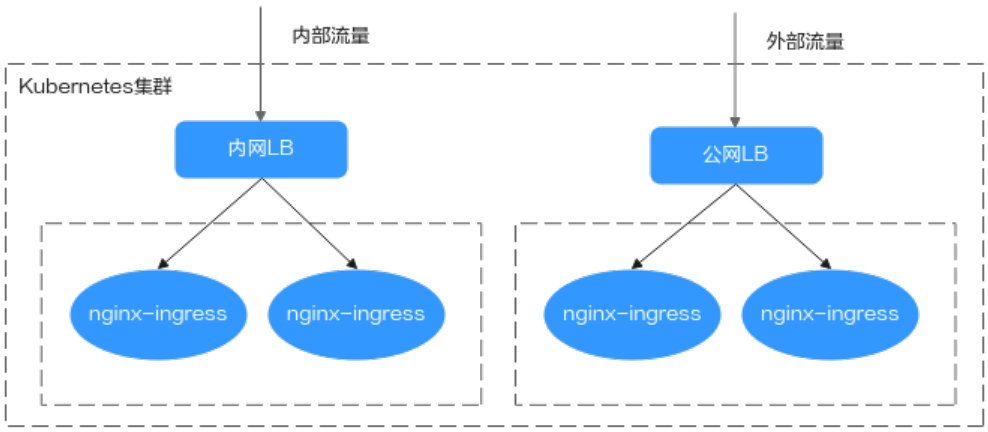
- 全托管免运维：ELB属于全托管免运维的云服务，不占用工作节点。
- 高可用性：ELB支持多可用区的同城双活容灾，无缝实时切换。完善的健康检查机制，保障业务实时在线。
- 自动弹性：ELB支持自动弹性规格，处理能力随业务峰值自动伸缩。
- 超强性能：单个ELB实例最大支持100万QPS、千万级并发连接。
- 云产品生态集成：ELB支持与WAF等多种云产品结合使用。
- 配置变更热更新：配置变更完全热更新，不需要Reload进程，对长连接无损。

您可以参考完成迁移。

自定义部署 Nginx Ingress Controller

Nginx Ingress Controller是一款业界流行的开源Ingress控制器，有着广泛的应用。在大规模集群场景下，用户有在集群中部署多套Nginx Ingress Controller的诉求，不同流量使用不同的控制器，将流量区分开。例如，集群中部分服务需要通过公网Ingress方式对外提供访问，但是又有部分对内开放的服务不允许使用公网访问，只支持对同VPC内的其他服务访问，您可以通过部署两套独立的Nginx Ingress Controller，绑定两个不同的ELB实例来满足这类需求场景。

图 6-3 多个 Nginx Ingress 应用场景



您可以参考，实现在同一个集群中部署多个Nginx Ingress Controller。