

弹性负载均衡

# 最佳实践

文档版本 02  
发布日期 2023-09-26



版权所有 © 华为云计算技术有限公司 2023。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

## 商标声明



HUAWEI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。

# 华为云计算技术有限公司

地址：贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址：<https://www.huaweicloud.com/>

---

## 目录

---

<b>1 使用访问日志定位异常后端服务器.....</b>	<b>1</b>
<b>2 查看流量使用情况.....</b>	<b>4</b>
<b>3 跨 VPC 添加服务器至负载均衡器.....</b>	<b>7</b>
3.1 方案概述.....	7
3.2 云上跨 VPC 添加服务器至 ELB.....	9
3.3 通过跨 VPC 后端功能添加同 VPC 内的服务器至 ELB.....	19
<b>4 使用高级转发策略实现新旧版本应用平滑过渡.....</b>	<b>28</b>
<b>5 独享 WAF 接入应用型 ELB，增强 Web 业务安全防护能力.....</b>	<b>37</b>

# 1 使用访问日志定位异常后端服务器


## 应用场景

您可以通过云日志服务，查看访问七层共享型负载均衡请求的详细日志记录，分析负载均衡的响应状态码，快速定位异常的后端服务器。


## 前期准备


1. 您已经创建了七层负载均衡。
2. 您已经开通了云日志服务。

## 创建日志组

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。区域和项目选择“华北-北京四”。
3. 选择“服务列表 > 管理与监管 > 云日志服务”。
4. 单击左侧导航栏“日志管理”。
5. 单击“创建日志组”，在弹出框内，输入日志组名称。

### 创建日志组

日志组名称  

日志存储时间(天) 7 

确定

取消

6. 单击“确定”，创建完成。

## 创建云日志流

1. 选择已创建的日志组名称，进入该日志组页面。
2. 单击“创建日志流”，在弹出框内，输入日志流名称。



3. 单击“确定”，创建完成。

## 配置访问日志

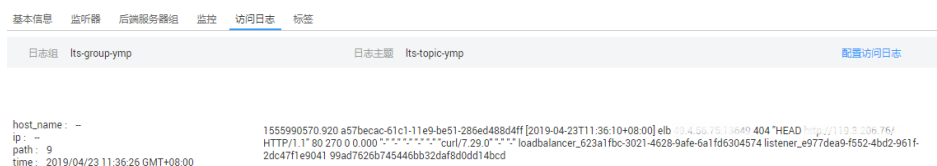
1. 选择“服务列表 > 网络 > 弹性负载均衡”。
2. 在“负载均衡器”界面，单击需要配置访问日志的负载均衡器名称。
3. 在该负载均衡器界面的“访问日志”页签，单击“配置访问日志”。
4. 开启日志记录，选择您在云日志服务中创建的日志组和日志流。
5. 单击“确定”，配置完成。

### 须知

确保创建的云日志组的地域和负载均衡器的地域相同。

## 查看访问日志

- “弹性负载均衡”控制台，进入访问日志界面，即可查看访问日志。



- “云日志服务”控制台，进入日志主题界面，在相应日志流名称所在行，单击“实时查看”或者“搜索日志”，即可查看访问日志。



## 定位异常服务器

筛选异常日志如下：

```
1554944564.344 - [2019-04-11T09:02:44+08:00] elb 10.133.251.171:51527 500 "GET http://10.154.73.58/lrange/guestbook HTTP/1.1" 411 3726 3545 19.028 "500" "0.009" "19.028" "19.028" "172.17.0.82:3000"
```

```
"Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/  
73.0.3683.103 Safari/537.36" "http://10.154.73.58:5971/" "-" loadbalancer_ed0f790b-  
e194-4657-9f97-53426227099e listener_b21dd0a9-690a-4945-950e-b134095c6bd9  
6b6aaf84d72b40fcb2d2b9b28f6a0b83
```

### 分析日志:

在 [2019-04-11T09:02:44+08:00 时，ELB接收到客户端地址和端口（10.133.251.171:51527）发起的“GET / HTTP/1.1”请求，ELB将请求转发给后端服务器（172.17.0.82:3000）处理，后端服务器响应状态码500。ELB最终向客户端响应状态码500。

具体字段分析可参照[访问日志](#)。

### 分析结果:

后端服务器（172.17.0.82:3000）异常，不能正常响应请求。

### 说明

“172.17.0.82:3000”是后端服务器的私网IP。

# 2 查看流量使用情况

## 应用场景

在视频直播中，网络访问流量的突增可能会引起业务的动荡，因此绝大多数的视频直播平台都会使用ELB自动分发流量到多台服务器，如果您担心流量过大，引起业务问题，需要查看弹性负载均衡使用流量，或者针对公网负载均衡，您需要查看某一段时间内弹性负载均衡绑定的EIP流量使用情况，云监控服务可以监控ELB的流量数据。

## 前提条件

已经正常运行了一段时间的负载均衡器。

关联的后端服务器在关机、故障、删除状态，无法在云监控中查看其监控指标。当后端服务器再次启动或恢复后，即可正常查看。

## 查看绑定的 EIP 使用流量


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。  
区域和项目选择“华北-北京四”。
3. 选择“服务列表 > 网络 > 虚拟私有云”。
4. 在左侧导航树，选择“弹性公网IP和带宽 > 弹性公网IP”。
5. 在弹性负载均衡绑定的EIP名称所在行，选择需要查看的EIP点击，切换到“带宽”页签，支持查看“近1小时”、“近3小时”、“近12小时”、“近1天”、“近7天”的数据。


图 2-1 EIP 使用流量监控结果



表 2-1 EIP 和带宽支持的监控指标

指标名称	含义	取值范围	测试对象	监控周期（原始指标）
出网带宽	该指标用于统计测试对象出云平台的网络速度（原指标为上行带宽）。	$\geq 0$ bits/s	带宽或弹性公网IP。	1分钟
入网带宽	该指标用于统计测试对象入云平台的网络速度（原指标为下行带宽）。	$\geq 0$ bits/s	带宽或弹性公网IP。	1分钟
出网带宽使用率	该指标用于统计测量对象出云平台的带宽使用率，以百分比为单位。	0-100%	带宽或弹性公网IP。	1分钟
入网带宽使用率	该指标用于统计测量对象入云平台的带宽使用率，以百分比为单位。	0-100%	带宽或弹性公网IP。	1分钟
出网流量	该指标用于统计测试对象出云平台的网络流量（原指标为上行流量）。	$\geq 0$ bytes	带宽或弹性公网IP。	1分钟
入网流量	该指标用于统计测试对象入云平台的网络流量（原指标为下行流量）。	$\geq 0$ bytes	带宽或弹性公网IP。	1分钟

## 查看弹性负载均衡使用流量

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。区域和项目选择“华北-北京四”。
3. 选择“服务列表 > 网络 > 弹性负载均衡”。



4. 在“负载均衡器”界面，单击需要查看流量的负载均衡器名称。
5. 切换到“监控”页签，单击需要查看的监控粒度，查看网络流入速率和网络流出速率。  
支持查看“近1小时”、“近3小时”、“近12小时”、“近1天”和“近7天”的数据。具体参数解释可参考[支持的监控指标](#)。

# 3 跨 VPC 添加服务器至负载均衡器

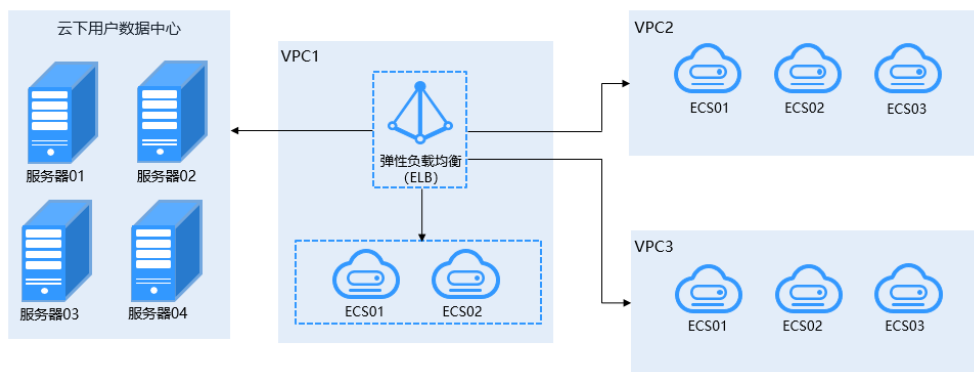
## 3.1 方案概述

### 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3-1所示。希望使用弹性负载均衡（Elastic Load Balance，简称ELB）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 3-1 添加云上、云下多台后端服务器至 ELB



### 方案架构

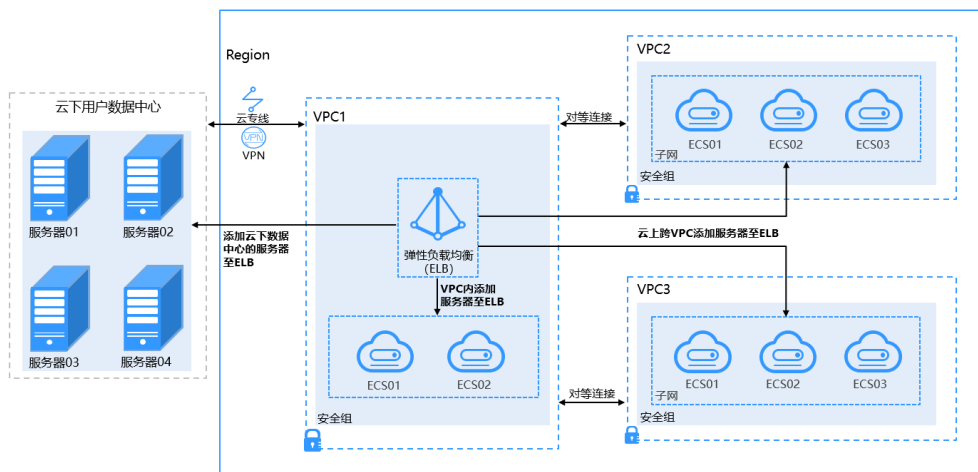
通过分析，可以使用**独享型负载均衡的跨VPC后端功能（配置混合负载均衡）**来实现将云上、云下多台后端服务器添加至ELB。

如图3-2所示：

- 无论是否开启跨VPC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。
- 通过跨VPC后端功能添加ELB同VPC中的服务器至ELB后端服务器组。

图 3-2 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，然后通过跨VPC功能添加
- 通过跨VPC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跨VPC后端功能，否则该功能无法正常使用。
- 添加的跨VPC后端的IP地址只允许为IPv4类型的地址。
- 添加的跨VPC后端的IP地址不能为本VPC内的IP地址以及公网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。
- 跨VPC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。
- 跨VPC后端功能开启后无法关闭。

## 3.2 云上跨 VPC 添加服务器至 ELB

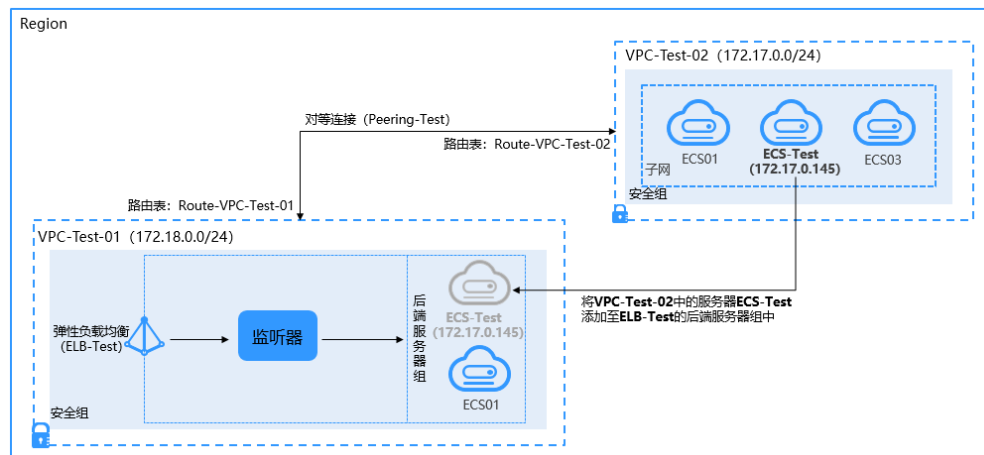
### 应用场景

本实践以用户常用的云上跨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；
- 通过使用跨VPC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 3-3 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 3-1 资源规划

资源	资源名称	资源说明	数量	每月费用（元）
VPC	VPC-Test-01	创建独享型负载均衡（ELB-Test）所在VPC： 172.18.0.0/24	1	00.00

资源	资源名称	资源说明	数量	每月费用（元）
	VPC-Test-02	服务器（ECS-Test）所在的VPC： 172.17.0.0/24	1	00.00
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	00.00
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	00.00
	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	00.00
ELB	ELB-Test	独享型负载均衡	1	400 本例使用的是华东-上海一， 应用型(HTTP/HTTPS)   小型   网络型(TCP/UDP)   小型
EIP	EIP-Test	用于给ELB-Test绑定的弹性公网IP 119.3.233.52	1	115 本例使用的是华东-上海一，带宽5M。
ECS	ECS-Test	ECS所属VPC：VPC-Test-02 私网IP：172.17.0.145	1	267.78 本例使用的是华东-上海一，c7.large.2，CentOS7.6操作系统的云服务器。包含系统盘价格。

## 操作流程

图 3-4 最佳实践操作流程



### 步骤一：创建 VPC

**步骤1** 登录华为云管理控制台。

**步骤2** 选择“网络 > 虚拟私有云”，单击“创建虚拟私有云”。

**步骤3** 根据表3-1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。

图 3-5 创建 VPC-Test-01



**步骤4** 重复**步骤2~步骤3**，参考**表3-1**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 3-6 创建所需 VPC

名称	IPv4网段	状态	子网个数	路由表	服务器个数	企业项目	操作
VPC-Test-01	172.18.0.0/24 (主网段)	可用	1	1	0	longterm-EPSTest-...	编辑网段 删除
VPC-Test-02	172.17.0.0/24 (主网段)	可用	1	1	1	longterm-EPSTest-...	编辑网段 删除

----结束

## 步骤二：创建 VPC 对等连接

**步骤1** 在虚拟私有云控制台单击左侧“对等连接”。

**步骤2** 单击右上角的“创建对等连接”。

**步骤3** 根据表3-1创建对等连接Peering-Test，完成后单击“确定”。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。



图 3-7 创建对等连接 Peering-Test

### 创建对等连接

选择本端VPC

\* 名称

\* 本端VPC  

本端VPC网段 172.18.0.0/24

选择对端VPC

\* 帐户  当前帐户  

\* 对端项目  

\* 对端VPC

对端VPC网段 172.17.0.0/24

描述   
0/255

---结束

### 步骤三：添加对等连接路由

步骤1 在虚拟私有云控制台单击左侧“路由表”。

步骤2 单击右上角的“创建路由表”。

步骤3 根据表3-1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

图 3-8 创建路由表 Route-VPC-Test-01

创建路由表

添加路由

目的地址 ?	下一跳类型 ?	下一跳 ?	描述
Local	Local	Local	系统默认，表示VPC内实例互通
172.17.0.0/24	对等连接	Peering-Test(9d408232-8739-4c36-a...)	

确定 取消

步骤4 重复3~4，参考表3-1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

----结束

## 步骤四：创建弹性服务器

步骤1 选择“计算 > 弹性云服务器”。

步骤2 单击右上角的“购买弹性云服务器”。

步骤3 根据表3-1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》。

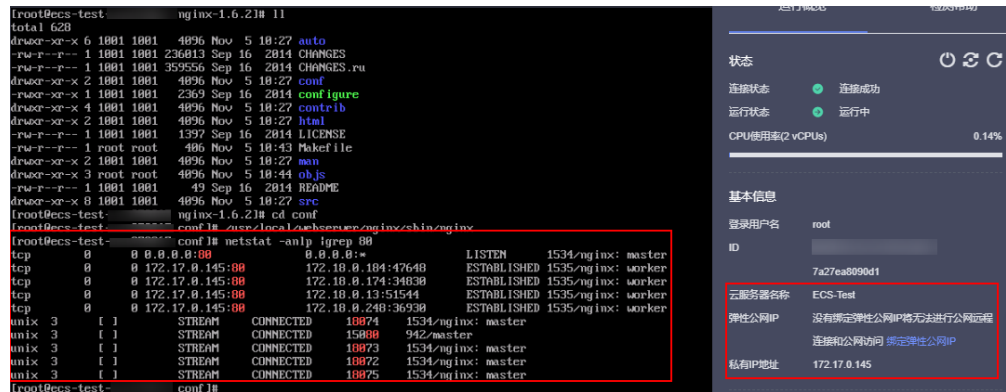
虚拟私有云选择VPC-Test-02，服务器名称设置为ECS-Test。

图 3-9 创建弹性服务器 ECS-Test



步骤4 后端服务器ECS-Test创建成功后，在其上部署Nginx。

图 3-10 在 ECS-Test 上部署 Nginx



----结束

## 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

步骤1 选择“网络 > 弹性负载均衡”。

步骤2 单击右上角的“购买弹性负载均衡”。

步骤3 根据表3-1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》。

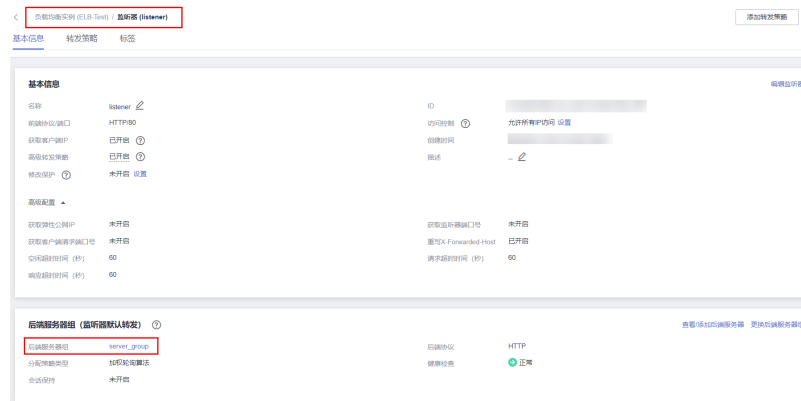
- 实例规格类型：独享型
- 跨VPC后端：开启
- 所属VPC：VPC-Test-01
- 名称：ELB-Test
- 其他参数根据需要设置。

图 3-11 创建独享型负载均衡 ELB-Test



步骤4 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。详见《弹性负载均衡用户指南》

图 3-12 HTTP 监听器&后端服务器组

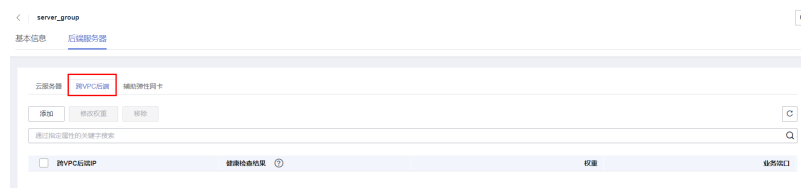


----结束

### 步骤六：将 ECS 添加至 ELB 后端服务器组

- 步骤1 单击上述创建的独享型负载均衡ELB-Test名称。
- 步骤2 切换到“监听器”页签，单击上述所创建的HTTP监听器。
- 步骤3 切换至右边的“后端服务器组”页签，单击“跨VPC后端”。

图 3-13 跨 VPC 后端



- 步骤4 单击“添加跨VPC后端”，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》。
  - 跨VPC后端IP: 172.17.0.145 (ECS-Test的私网IP)
  - 后端端口: 填写业务端口
  - 权重: 根据需要设置

图 3-14 添加跨 VPC 后端

## 添加跨VPC后端

**i** 如果添加的是跨VPC后端，请启用TOA模块获取客户端IP地址。  
跨VPC后端的安全组规则必须放通负载均衡器的后端子网网段，否则负载均衡器无法向后端服务器发送请求，健康检查也会出现异常。

批量添加端口

**i** 您最多可以添加494个后端服务器，如需申请更多配额请点击[申请扩大配额](#)。

跨VPC后端IP	后端端口 ?	权重 ?	操作
<input type="text" value="172 . 17 . 0 . 145"/>	<input type="text" value="80"/>	<input type="text" value="10"/>	移除

----结束

## 步骤七：验证跨 VPC 添加后端服务器是否成功

**步骤1** 单击上述创建的独享型负载均衡ELB-Test操作列的“更多”。

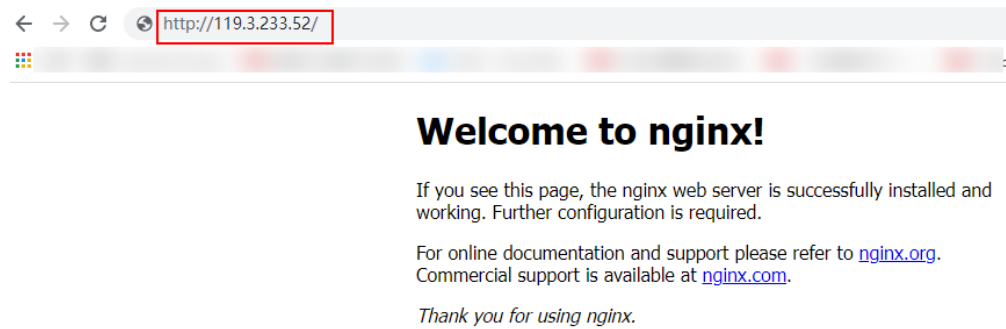
**步骤2** 选择“绑定IPv4公网IP”，给ELB-Test绑定一个弹性公网IP（EIP-Test：119.3.233.52）。

图 3-15 ELB 绑定 EIP



**步骤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 3-16 验证跨 VPC 添加后端服务器是否成功



----结束

## 3.3 通过跨 VPC 后端功能添加同 VPC 内的服务器至 ELB

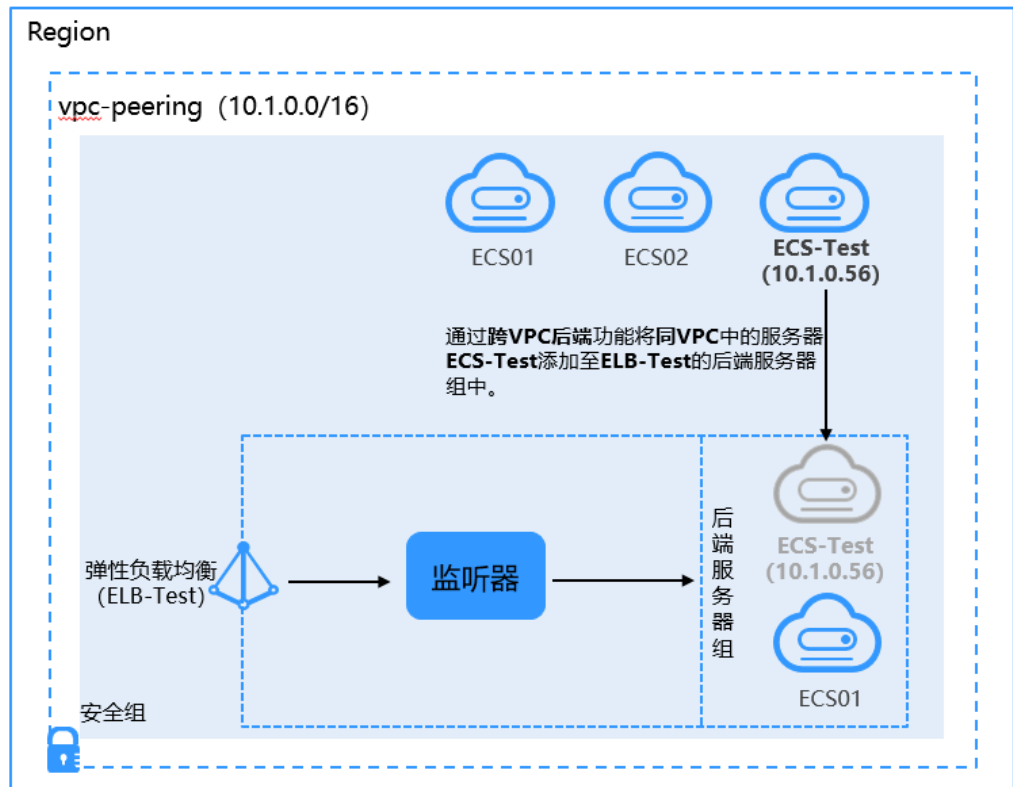
### 应用场景

您还可以通过跨VPC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；
- 通过使用跨VPC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 3-17 使用跨 VPC 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 3-2 资源规划

资源	资源名称	资源说明	数量	每月费用（元）
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	00.00
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	00.00

资源	资源名称	资源说明	数量	每月费用（元）
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: 10.1.0.0/16	1	00.00
ELB	ELB-Test	独享型负载均衡 (ELB-Test) 私网IP: 10.1.0.9	1	400 本例使用的是华东-上海一， 应用型(HTTP/HTTPS)   小型 I 网络型(TCP/UDP)   小型 I
EIP	EIP-Test	用于给ELB-Test绑定的弹性公网IP 120.46.131.153	1	115 本例使用的是华东-上海一，带宽5M。
ECS	ECS-Test	ECS所属VPC: vpc-peering 私网IP: 10.1.0.56	1	267.78 本例使用的是华东-上海一，c7.large.2，CentOS7.6操作系统的云服务器。包含系统盘价格。



## 操作流程

图 3-18 操作流程



### 步骤一：创建 VPC

**步骤1** 登录华为云管理控制台。

**步骤2** 选择“网络 > 虚拟私有云”，单击“创建虚拟私有云”。

**步骤3** 根据表3-2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。

图 3-19 创建 vpc-peering

**基本信息**

区域

名称

IPv4网段  ·  ·  ·  /

企业项目  [创建企业项目](#)

---

高级配置 ▾ 标签 | 描述

---

**默认子网**

可用区

名称

子网IPv4网段  ·  ·  ·  /

可用IP数: 251  
子网创建完成后, 子网网段无法修改

子网IPv6网段  开启IPv6

----结束

## 步骤二：创建 VPC 对等连接

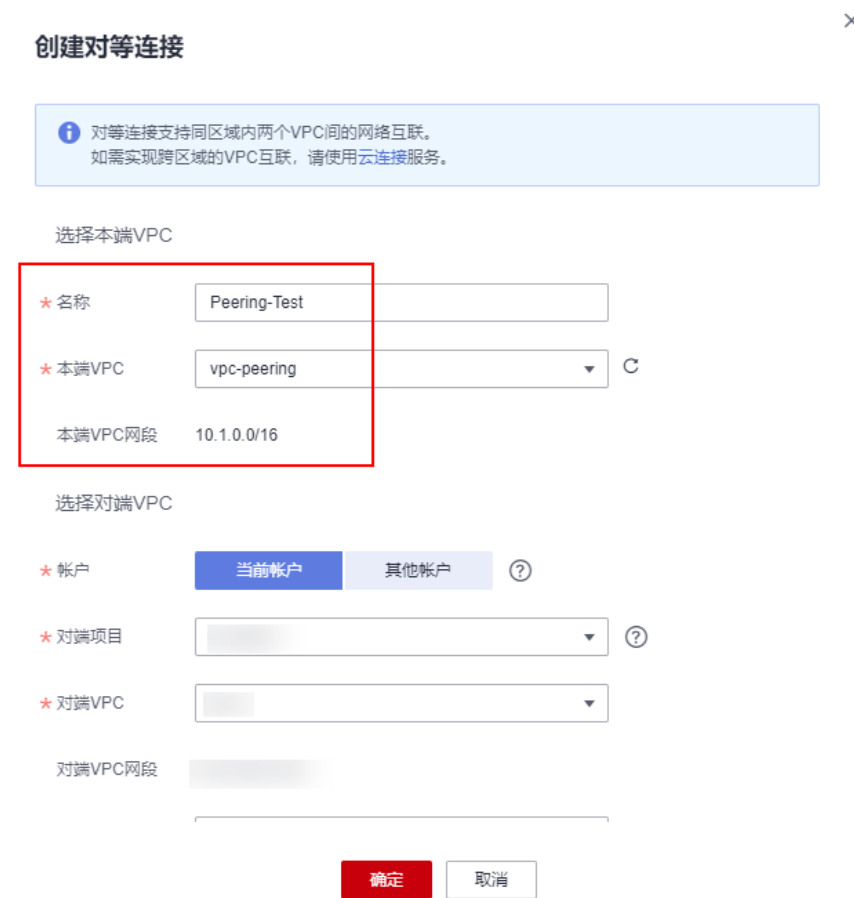
**步骤1** 在虚拟私有云控制台单击左侧“对等连接”。

**步骤2** 单击右上角的“创建对等连接”。

**步骤3** 根据表3-2创建对等连接Peering-Test，完成后单击“确定”。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。

图 3-20 创建对等连接 Peering-Test



----结束

### 步骤三：添加对等连接路由

**步骤1** 在虚拟私有云控制台单击左侧“路由表”。

**步骤2** 单击右上角的“创建路由表”。

**步骤3** 根据表3-2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

图 3-21 创建路由表 Route-VPC-Test-01

创建路由表

\* 路由表名称: Route-VPC-Test-01

\* 所属VPC: vpc-peering

IPv4网段: 10.1.0.0/16

您还可创建1个路由表。

描述: [Text Area]

添加路由

目的地址	下一跳类型	下一跳	描述
Local	Local	Local	系统默认, 表示VPC内实例互通
10.0.0.0/16	对等连接	Peering-Test(dc0e99f2-4419-4ed9-9...	

继续添加

确定 取消

----结束

## 步骤四：创建弹性服务器

步骤1 选择“计算 > 弹性云服务器”。

步骤2 单击右上角的“购买弹性云服务器”。

步骤3 根据表3-2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》。

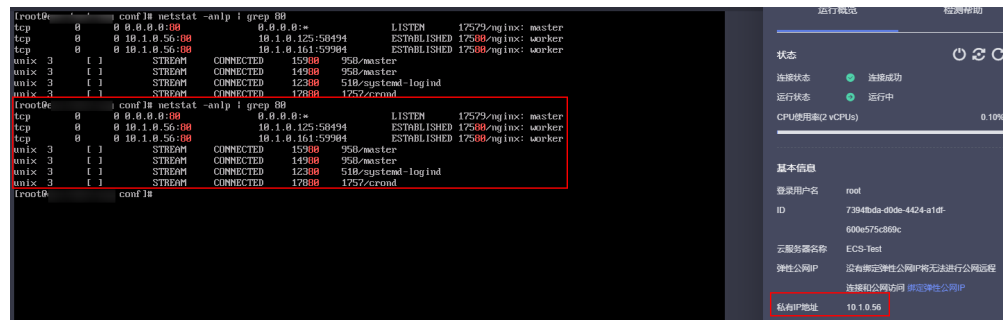
虚拟私有云选择vpc-peering，服务器名称设置为ECS-Test。

图 3-22 创建弹性服务器 ECS-Test



步骤4 服务器ECS-Test创建成功后，在其上部署Nginx。

图 3-23 在 ECS-Test 上部署 Nginx



----结束

## 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

**步骤1** 选择“网络 > 弹性负载均衡”。

**步骤2** 单击右上角的“购买弹性负载均衡”。

**步骤3** 根据表3-2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
- 跨VPC后端：开启
- 所属VPC：vpc-peering
- 名称：ELB-Test
- 其他参数根据需要设置。

图 3-24 创建独享型负载均衡 ELB-Test



**步骤4** 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。详见《弹性负载均衡用户指南》。

----结束

## 步骤六：将 ECS 添加至 ELB 后端服务器组

**步骤1** 单击上述创建的独享型负载均衡ELB-Test名称。

**步骤2** 切换到“监听器”页签，单击上述所创建的HTTP监听器。

**步骤3** 切换至右边的“后端服务器组”页签，单击“跨VPC后端”。

**步骤4** 单击“添加跨VPC后端”，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》。

- 跨VPC后端IP：10.1.0.56（ECS-Test的私网IP）
- 后端端口：填写业务端口

- 权重：根据需要设置

图 3-25 添加跨 VPC 后端



----结束

## 步骤七：验证通过跨 VPC 后端功能添加同 VPC 后端服务器组是否成功

**步骤1** 单击上述创建的独享型负载均衡ELB-Test操作列的“更多”。

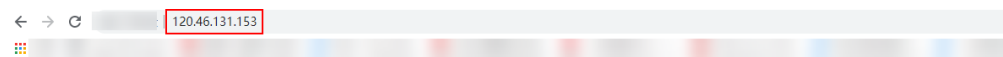
**步骤2** 选择“绑定IPv4公网IP”，给ELB-Test绑定一个弹性公网IP（EIP-Test：120.46.131.153）。

图 3-26 ELB 绑定 EIP



**步骤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 3-27 验证通过跨 VPC 后端功能添加同 VPC 后端服务器是否成功



### Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to [nginx.org](http://nginx.org). Commercial support is available at [nginx.com](http://nginx.com).

Thank you for using nginx.

----结束

# 4 使用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

- 已拥有华为云帐号，并且华为云帐号已实名认证。
- 华为云帐号未欠费，并且有足够的金额可以购买本最佳实践所涉及的资源。
- 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 4-1 操作流程图

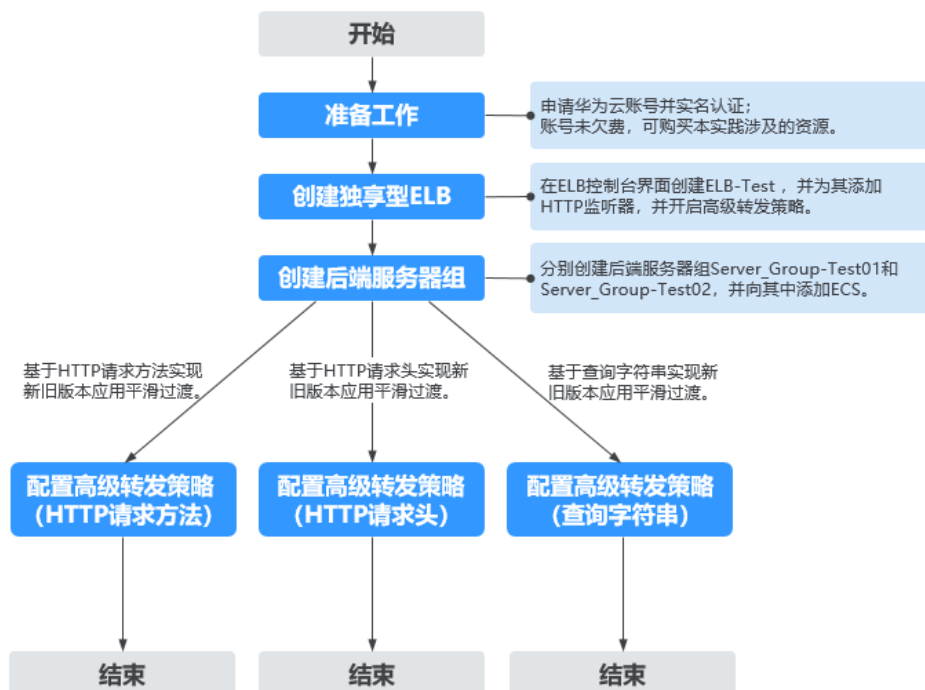


表 4-1 资源规划

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VPC添加ECS至ELB的后端服务器组中，详细请参考[跨VPC添加服务器至负载均衡器](#)。

## 创建独享型 ELB 实例&添加 HTTP 监听器&开启高级转发策略

**步骤1** 登录华为云管理控制台。

**步骤2** 选择“网络 > 弹性负载均衡”。

**步骤3** 单击右上角的“购买弹性负载均衡”。

**步骤4** 根据[表4-1](#)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
- 名称：ELB-Test
- 其他参数根据需要设置。

**步骤5** 独享型ELB创建成功后，在ELB-Test中添加HTTP监听器。详见《[弹性负载均衡用户指南](#)》。

图 4-2 HTTP 监听器



**步骤6** HTTP监听器创建成功后，开启高级转发策略。详见《[弹性负载均衡用户指南](#)》

图 4-3 开启高级转发策略

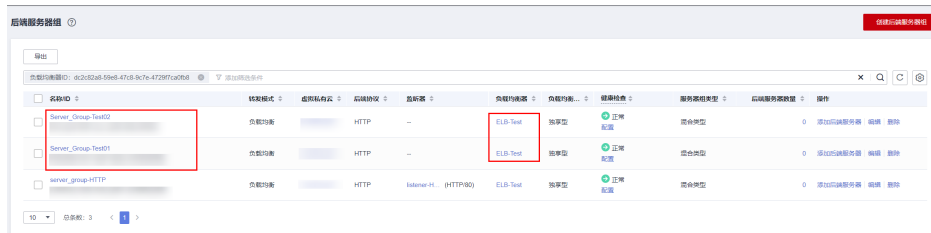


----结束

## 创建后端服务器组并添加后端服务器

- 步骤1** 单击上述创建的独享型负载均衡ELB-Test名称。
- 步骤2** 在监听器页签，单击右上角的“创建后端服务器组”。
- 名称：Server\_Group-Test01
  - 后端协议：HTTP
  - 其他参数根据需要设置。
- 步骤3** 参考**步骤2**再添加后端服务器组Server\_Group-Test02。

图 4-4 添加后端服务器组



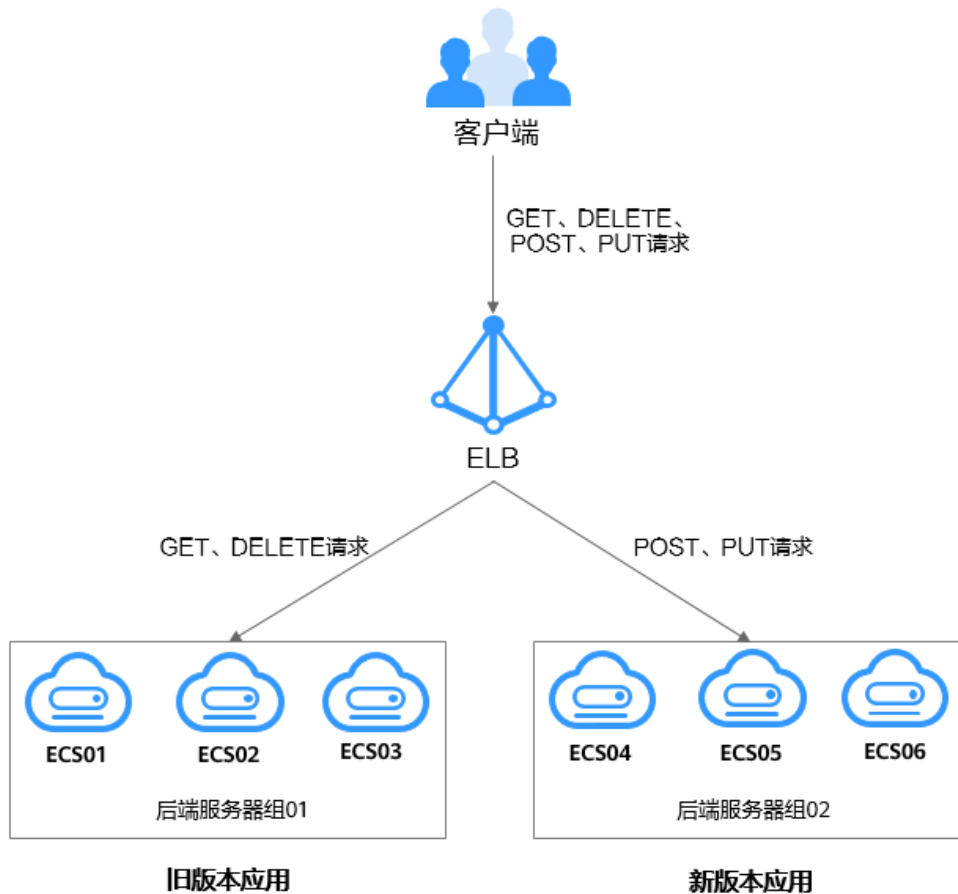
- 步骤4** 单击后端服务器组Server\_Group-Test01名称，添加ECS01、ECS02、ECS03至Server\_Group-Test01。
- 步骤5** 单击后端服务器组Server\_Group-Test02名称，添加ECS04、ECS05、ECS06至Server\_Group-Test02。

----结束

## 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。

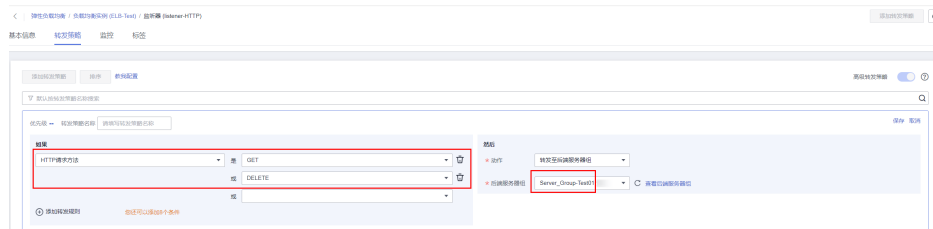
图 4-5 基于 HTTP 请求方法实现新旧版本应用平滑过渡



- 步骤1 单击上述创建的独享型负载均衡ELB-Test名称。
- 步骤2 在“监听器”页签，单击上述创建的HTTP监听器名称。
- 步骤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”。

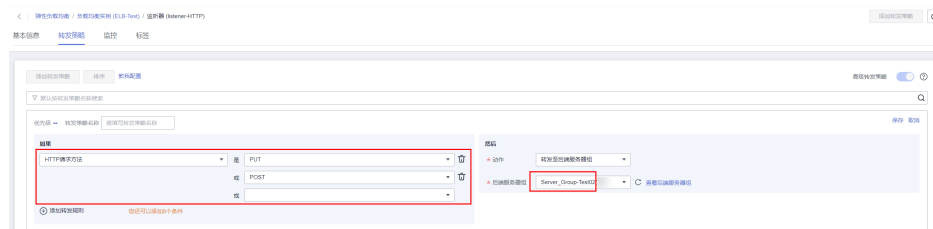
图 4-6 基于 HTTP 请求方法将部分请求转发至旧版本应用上



- 步骤4 单击“保存”。
- 步骤5 参考步骤3和步骤4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 4-7 基于 HTTP 请求方法将部分请求转发至新版本应用上

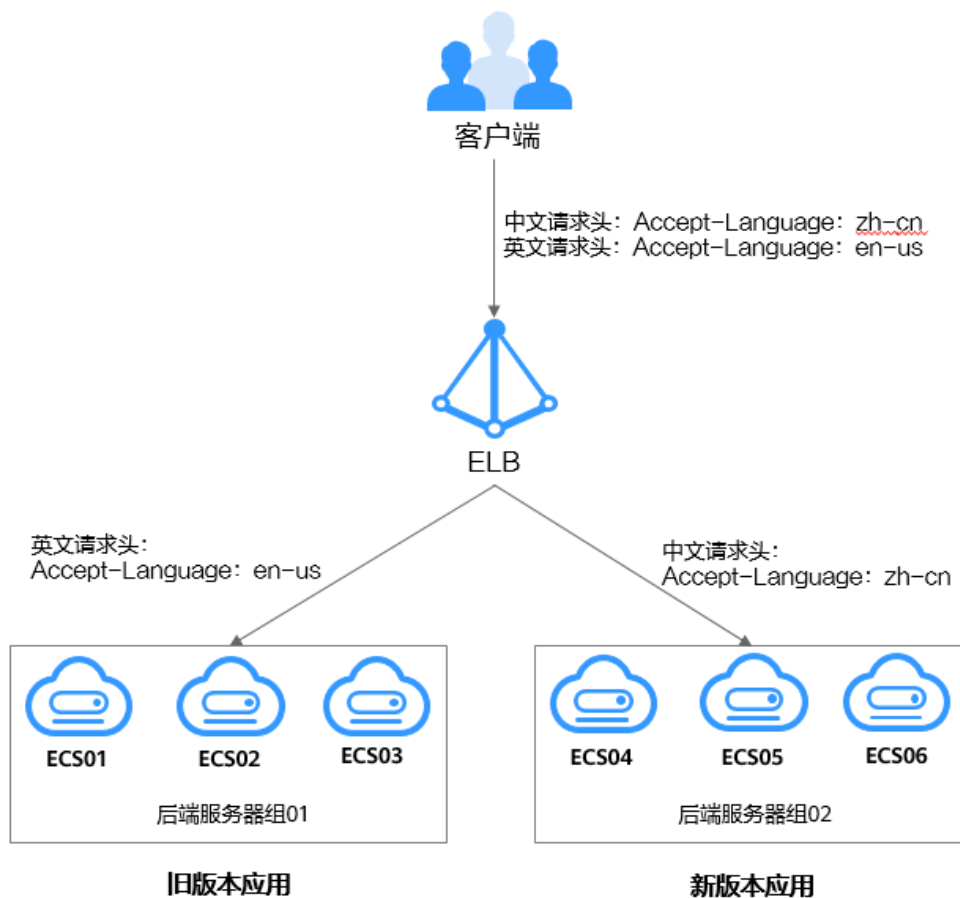


----结束

## 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上。

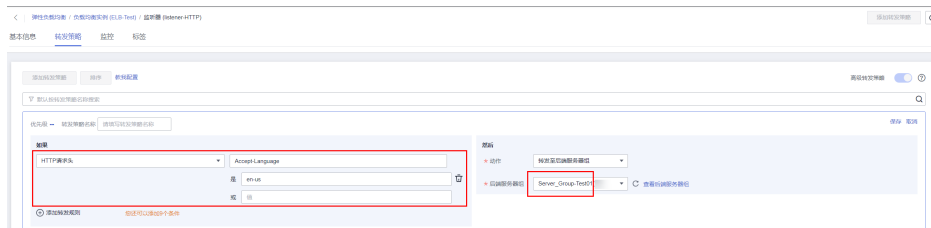
图 4-8 基于 HTTP 请求头实现新旧版本应用平滑过渡



- 步骤1** 单击上述创建的独享型负载均衡ELB-Test名称。
- 步骤2** 切换至“监听器”页签，单击上述创建的HTTP监听器名称。
- 步骤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”。

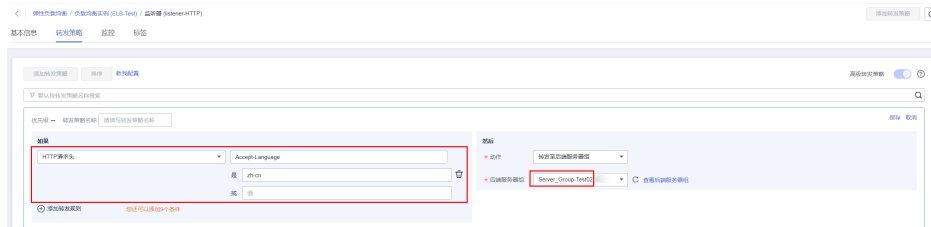
图 4-9 基于 HTTP 请求头将部分请求转发至旧版本应用上



- 步骤4** 单击“保存”。
- 步骤5** 参考**步骤3**和**步骤4**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 4-10 基于 HTTP 请求头将部分请求转发至新版本应用上

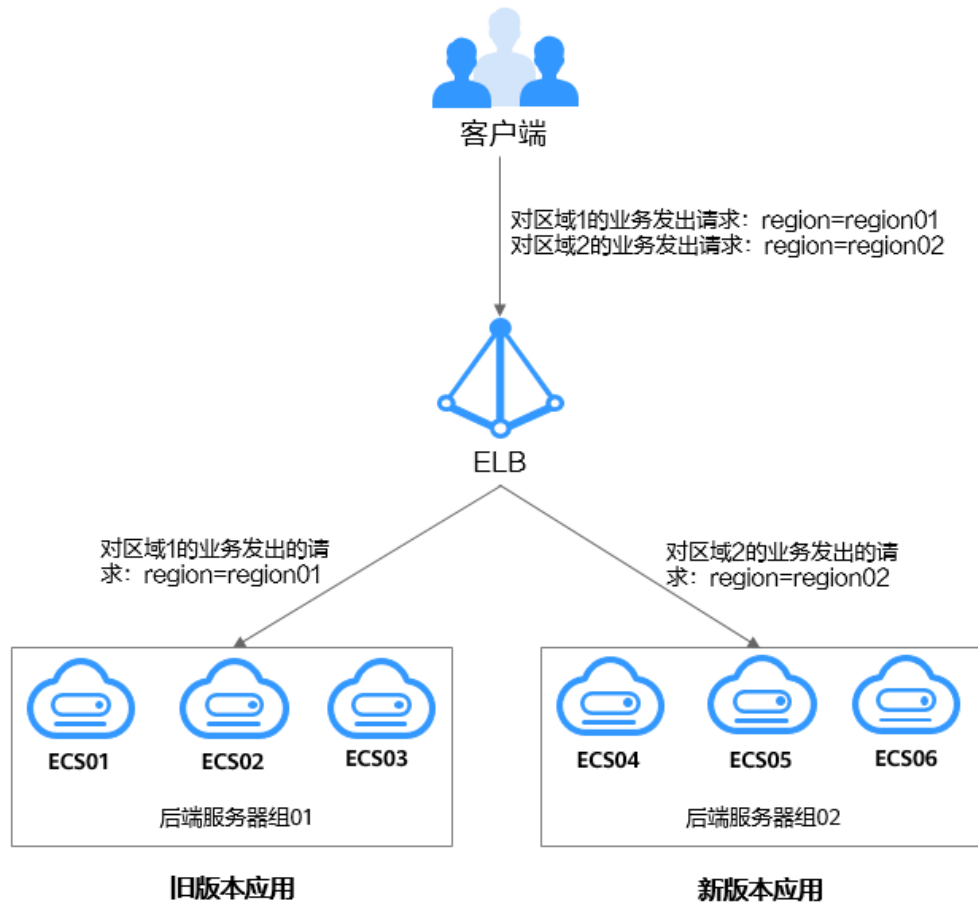


----结束

## 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 4-11 基于查询字符串实现新旧版本应用平滑过渡



### 说明

- 独享型负载均衡支持跨区域、跨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和后端服务器组02中。

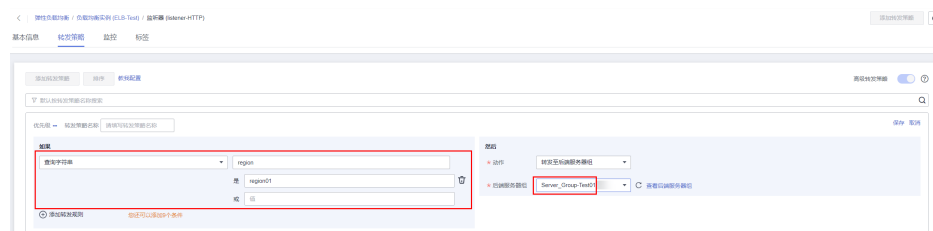
**步骤1** 单击上述创建的独享型负载均衡ELB-Test名称。

**步骤2** 在“监听器”页签，单击上述创建的HTTP监听器名称。

**步骤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 4-12 基于查询字符串将部分请求转发至旧版本应用上

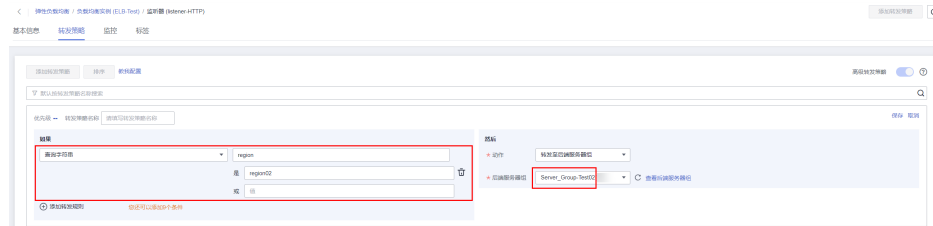


**步骤4** 单击“保存”。

**步骤5** 参考**步骤3**和**步骤4**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 4-13** 基于查询字符串将部分请求转发至新版本应用上



---结束

# 5 独享 WAF 接入应用型 ELB，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。

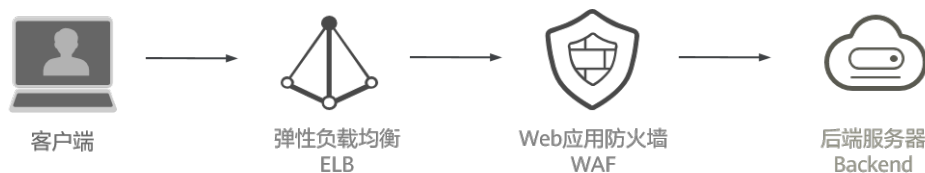
## 约束与限制

- 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

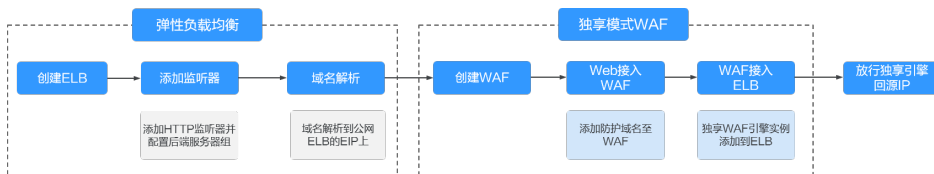
应用型ELB接入独享WAF对Web业务进行防护后，流量路径如[图5-1](#)所示。

图 5-1 流量路径图





## 操作流程

图 5-2 独享 WAF 接入应用型 ELB 的操作流程



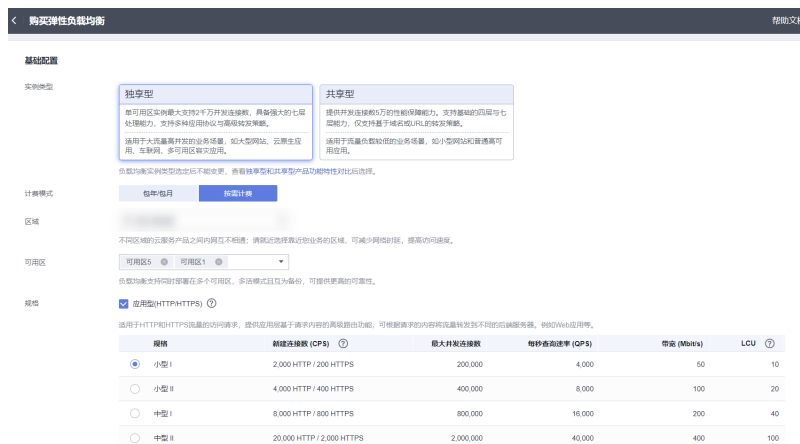


## 步骤一：创建应用型负载均衡器

1. 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“网络 > 弹性负载均衡”。
4. 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 5-3 创建应用型负载均衡器（独享型）



5. 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 5-4 为负载均衡器配置弹性公网 IP



6. 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. 登录管理控制台。



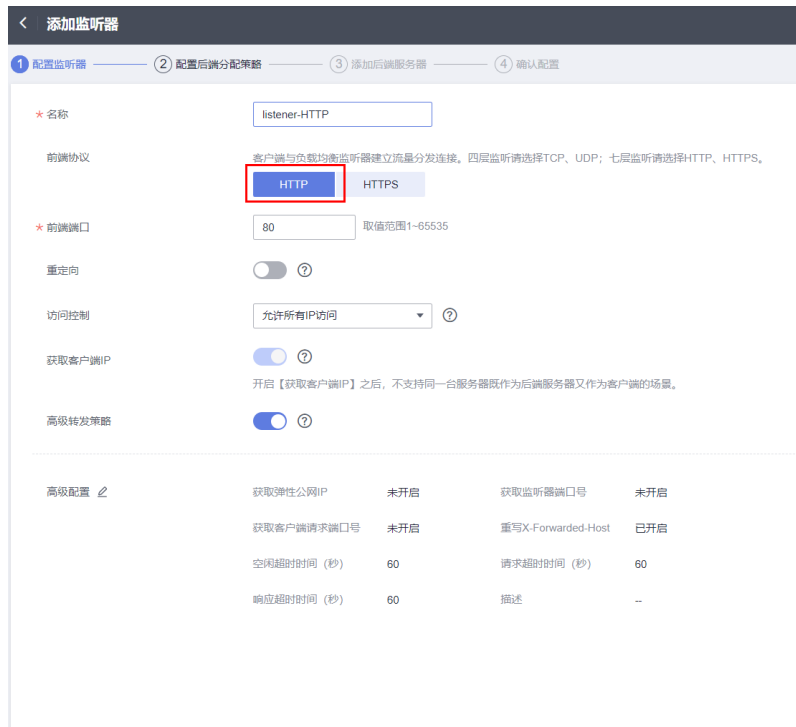
2. 在管理控制台左上角单击  图标，选择区域和项目。
3. 单击页面左上角的  ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击 [步骤一](#)中创建的负载均衡名称。
5. 切换到“监听器”页签，单击“添加监听器”，配置HTTP监听器并指定前端端口。  
更多添加详情请参见[添加HTTP监听器](#)。

图 5-5 添加 HTTP 监听器



6. 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 5-6 配置后端服务器组

添加监听器

配置监听器 2 配置后端分配策略 3 添加后端服务器 4 确认配置

后端服务器组  新创建  使用已有

服务器组类型 混合类型  
可以添加IP地址、服务器、辅助弹性网卡类型的后端服务器

\* 名称 server\_group-HTTP

\* 后端协议 HTTP

\* 分配策略类型  加权轮询算法  加权最少连接  源IP算法

会话保持  ?

慢启动  ?

描述

0/255



7. 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。
8. 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”。

更多创建WAF实例详情，请参考[购买WAF独享模式](#)。

图 5-7 创建独享模式 WAF 实例

The screenshot shows the 'Purchase Web Application Firewall' (购买Web应用防火墙) page in the AWS console. The 'WAF Mode' (WAF模式) is set to 'Dedicated Mode' (独享模式), which is highlighted with a red box. Other settings include 'Billing Mode' (计费模式) set to 'Pay-as-you-go' (按需计费), 'Region' (区域) set to 'cn-hongkong', 'Availability Zone' (可用区) set to 'Randomly Distributed' (随机分配), 'WAF Instance Name Prefix' (WAF实例名称前缀) set to 'Waf\_Elb', 'WAF Instance Count' (WAF实例数量) set to 2, and 'WAF Instance Size' (WAF实例规格) set to 'W1-100'. The page also includes performance metrics and a 'View Virtual Private Cloud' (查看虚拟私有云) link.

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 5-8 添加防护域名

添加防护网站

域名接入示意图

域名信息

网站名称

\* 防护对象

网站备注

源站配置

\* 防护对象端口

需要防护的域名对应的业务端口，如需要防护http://www.example.com: 8080，则防护域名端口选择8080

对外协议	源站协议	VPC	源站地址	源站端口
<input type="radio"/> HTTP	<input type="text" value="HTTP"/>	<input type="text"/>	<input type="text" value="IPv4 内网IP地址"/>	<input type="text" value="80"/>
检测到当前vpc下，仅存在单WAF实例，为避免单点故障，请至少再购买一个实例实现多活架构。 <a href="#">购买实例</a>				
<input type="radio"/> HTTP	<input type="text" value="HTTP"/>	<input type="text"/>	<input type="text" value="IPv4 内网IP地址"/>	<input type="text" value="80"/>
检测到当前vpc下，仅存在单WAF实例，为避免单点故障，请至少再购买一个实例实现多活架构。 <a href="#">购买实例</a>				

添加 您还可以添加78个源站地址

6. 确认高级配置，“是否已使用代理”请选择“是”。

图 5-9 确认高级配置

高级配置

\* 是否已使用代理  是  否

WAF仅支持Web流量，非Web流量接入WAF后无法转发（包括但不限于UDP、SMTP、FTP等非Web类协议）  
若已使用如公网ELB七层负载均衡（或接入CDN、云加速或使用七层代理的产品），为了保证WAF的安全策略能针对真实源IP生效，请务必选择“是”。若已使用DDoS高防，选择“否”

\* 策略配置

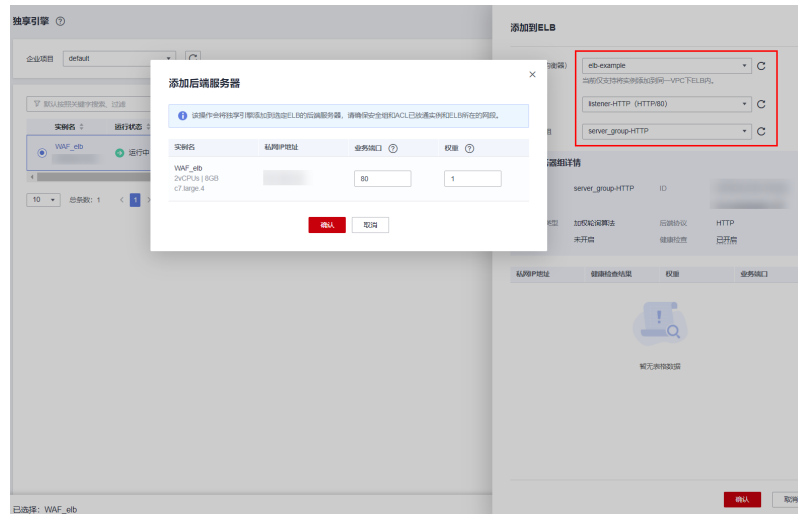
选择系统自动生成策略时，仅支持“仅记录”模式下的Web基础防护的常规检测和网站爬虫中的扫描器防护，且仅专业版以上的版本才支持网站爬虫中的扫描器防护。 [自定义策略](#)

## 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 5-10 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](#)。