弹性负载均衡

最佳实践

文档版本	01
发布日期	2024-07-11

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 通过 IP 类型后端功能添加服务器至 ELB

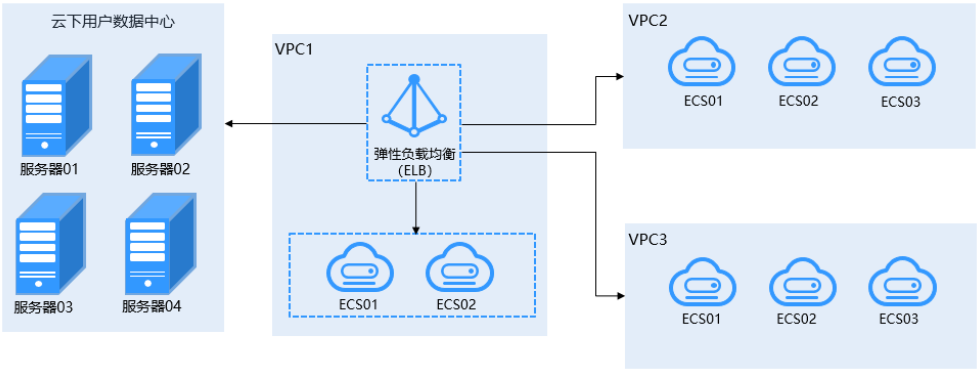
1.1 方案概述

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1-1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 1-1 添加云上、云下多台后端服务器至 ELB



方案架构

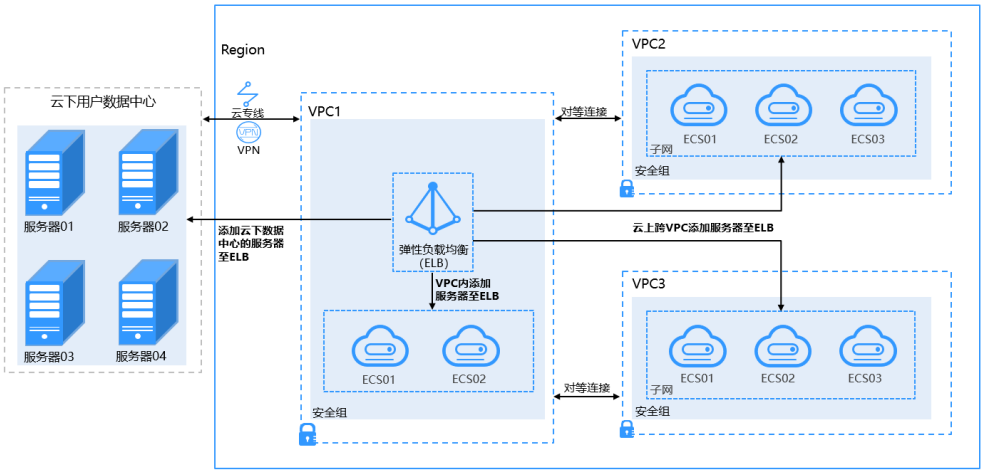
通过分析，可以通过为独享型负载均衡添加IP类型后端来实现将云上、云下多台后端服务器添加至ELB。

如图1-2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 1-2 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。

1.2 通过 IP 类型后端添加云上不同 VPC 的服务器至 ELB

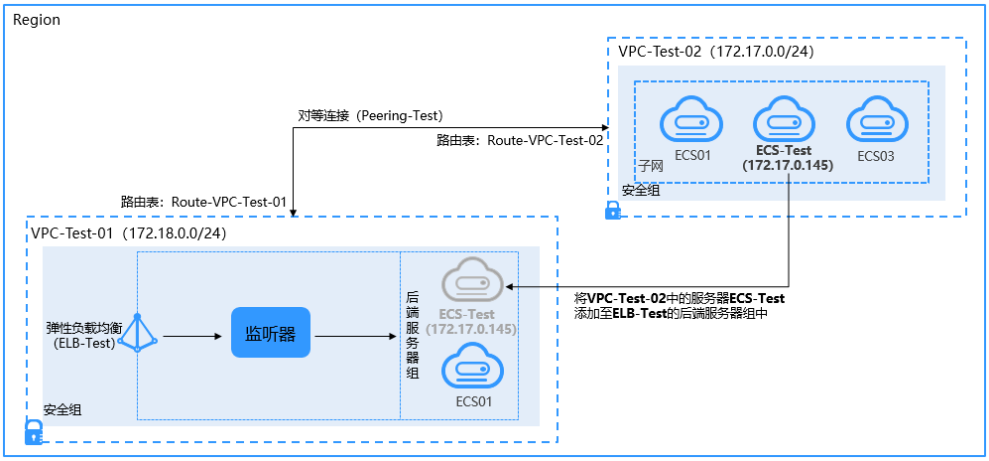
应用场景

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 1-3 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 1-1 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
	VPC-Test-02	服务器（ECS-Test）所在的VPC： 172.17.0.0/24	1

资源	资源名称	资源说明	数量
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 1-4 最佳实践操作流程

步骤一：创建 VPC

1. 登录华为云管理控制台。
2. 选择“网络 > 虚拟私有云”，单击“创建虚拟私有云”。
3. 根据**表1-1**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。
4. 参考**表1-1**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 1-5 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1-1**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

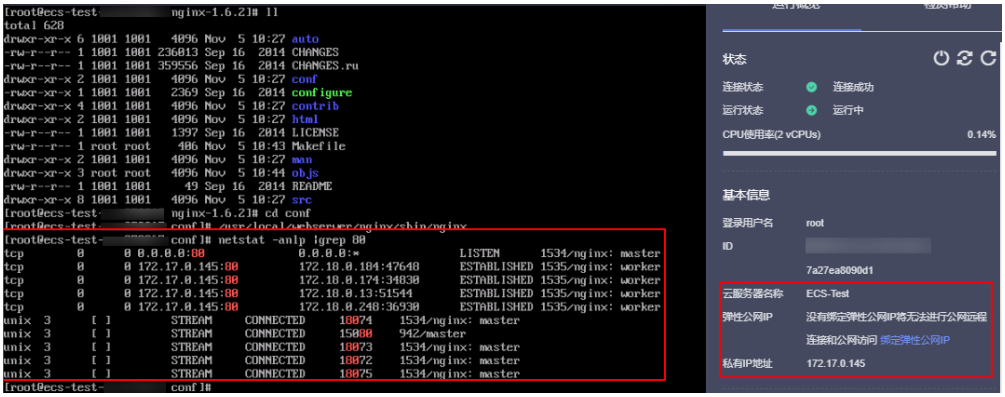
1. 在虚拟私有云控制台单击左侧“路由表”。
2. 单击右上角的“创建路由表”。
3. 根据**表1-1**创建路由表Route-VPC-Test-01，完成后单击“确定”。详见**《虚拟私有云用户指南》**。
   - 路由表名称：Route-VPC-Test-01
   - 所属VPC：VPC-Test-01
   - 目的地址：172.17.0.0/24
   - 下一跳类型：对等连接
   - 下一跳：Peering-Test
4. 重复以上步骤，参考**表1-1**规划，创建Route-VPC-Test-02。
   - 路由表名称：Route-VPC-Test-02
   - 所属VPC：VPC-Test-02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

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1-1**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。
4. 后端服务器ECS-Test创建成功后，在其上部署Nginx。

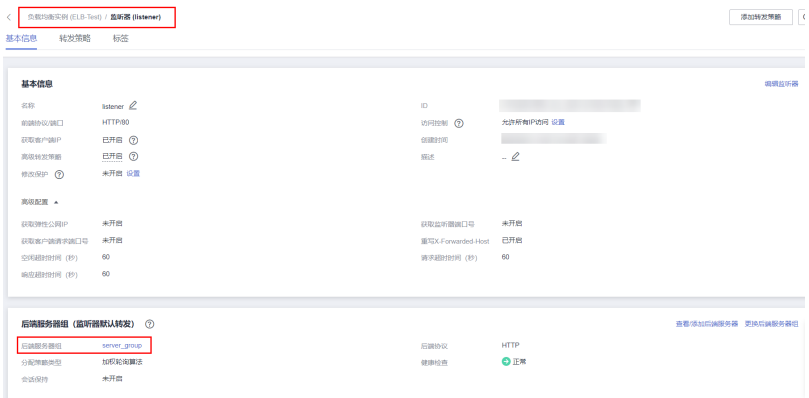
图 1-6 在 ECS-Test 上部署 Nginx



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. 选择“网络 > 弹性负载均衡”。
2. 单击右上角的“购买弹性负载均衡”。
3. 根据**表1-1**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
   - 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。
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。

图 1-7 HTTP 监听器&后端服务器组



步骤六：将 ECS 添加至 ELB 后端服务器组

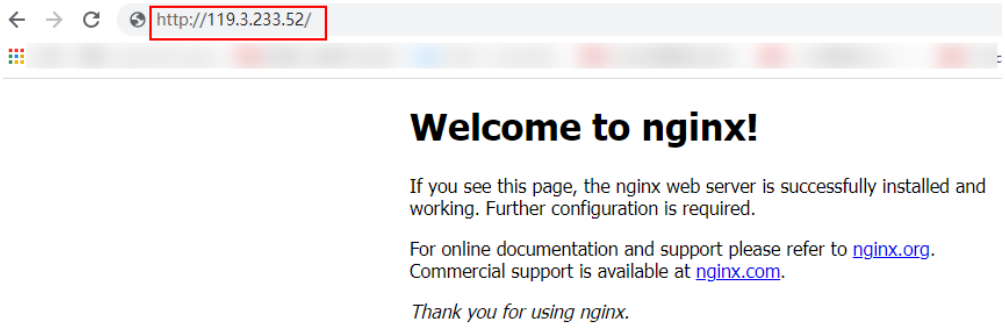
1. 单击上述创建的独享型负载均衡ELB-Test名称。
2. 切换到“监听器”页签，单击上述所创建的HTTP监听器。
3. 在监听器“基本信息”页签，在下方后端服务器组界面，单击“查看/添加后端服务器”。
4. 进入右侧“后端服务器组”页面。

5. 在“IP类型后端（跨VPC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：验证跨 VPC 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 1-8 验证跨 VPC 添加后端服务器是否成功



1.3 通过 IP 类型后端添加云上相同 VPC 的服务器至 ELB

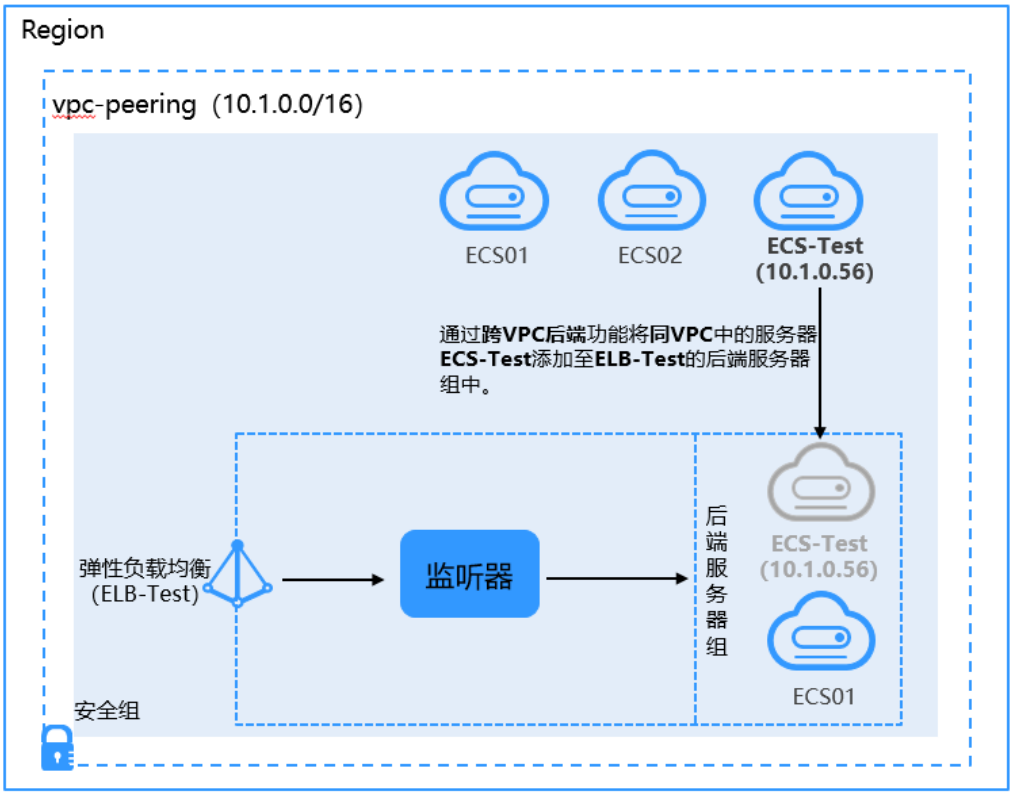
应用场景

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 1-9 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 1-2 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-Test-01 目的地址：10.1.0.0/16	1

资源	资源名称	资源说明	数量
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 1-10 操作流程

步骤一：创建 VPC

1. 登录华为云管理控制台。
2. 选择“网络 > 虚拟私有云”，单击“创建虚拟私有云”。
3. 根据**表1-2**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。

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1-2**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

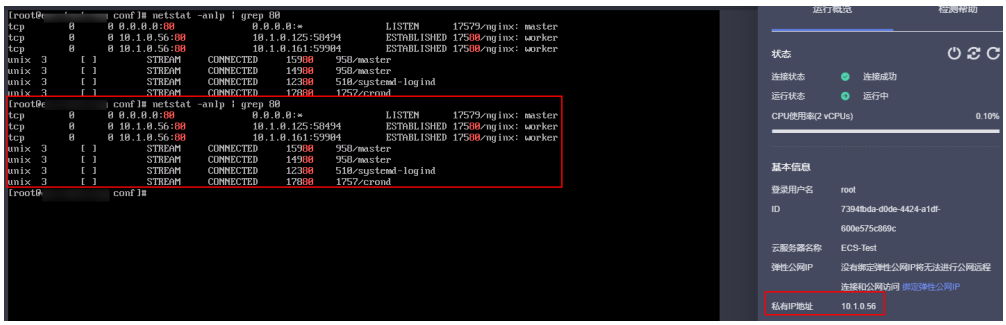
1. 在虚拟私有云控制台单击左侧“路由表”。
2. 单击右上角的“创建路由表”。
3. 根据**表1-2**创建路由表Route-VPC-Test-01，完成后单击“确定”。详见**《虚拟私有云用户指南》**。
   - 路由表名称：Route-VPC-Test-01
   - 所属VPC：vpc-peering
   - 目的地址：10.1.0.0/16
   - 下一跳类型：对等连接
   - 下一跳：Peering-Test

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1-2**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。
4. 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. 选择“网络 > 弹性负载均衡”。
2. 单击右上角的“购买弹性负载均衡”。
3. 根据**表1-2**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
   - 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。
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。

步骤六：将 ECS 添加至 ELB 后端服务器组

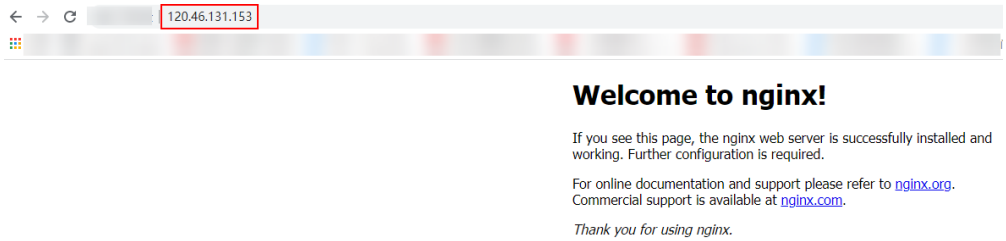
单击上述创建的独享型负载均衡ELB-Test名称。

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（跨VPC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：验证通过跨 VPC 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 1-12 验证通过跨 VPC 后端功能添加同 VPC 后端服务器是否成功



2 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 2-1 操作流程图

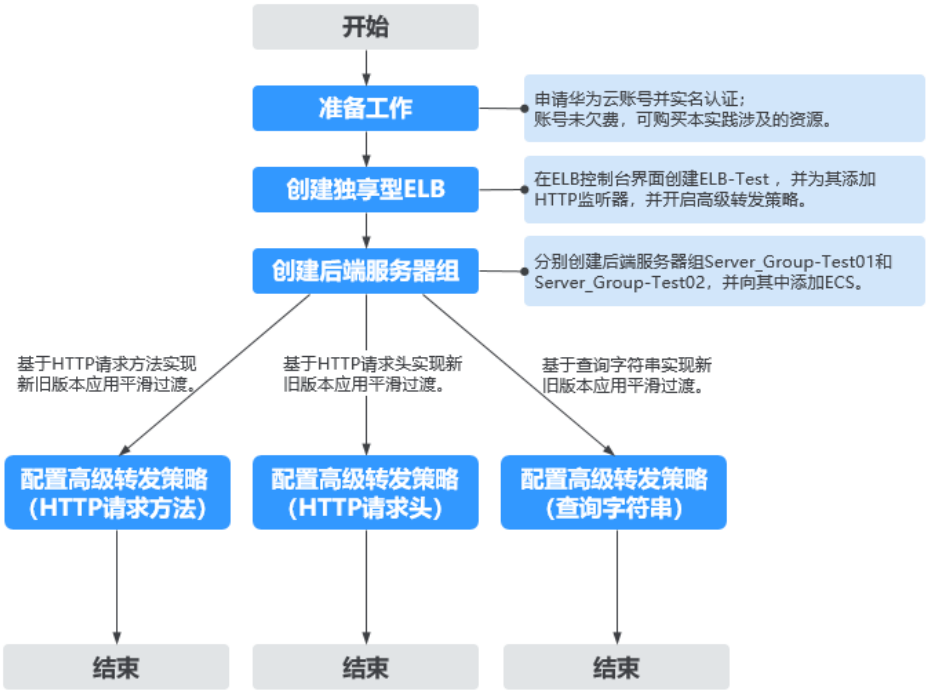


表 2-1 资源规划

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**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. 登录华为云管理控制台。
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. 单击右上角的“购买弹性负载均衡”。
5. 根据**表2-1**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**。
6. 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**。
7. 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**。

图 2-2 开启高级转发策略

步骤二：创建后端服务器组并添加后端服务器

1. 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. 在左侧导航栏，选择“ 弹性负载均衡 > 后端服务器组”。
5. 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

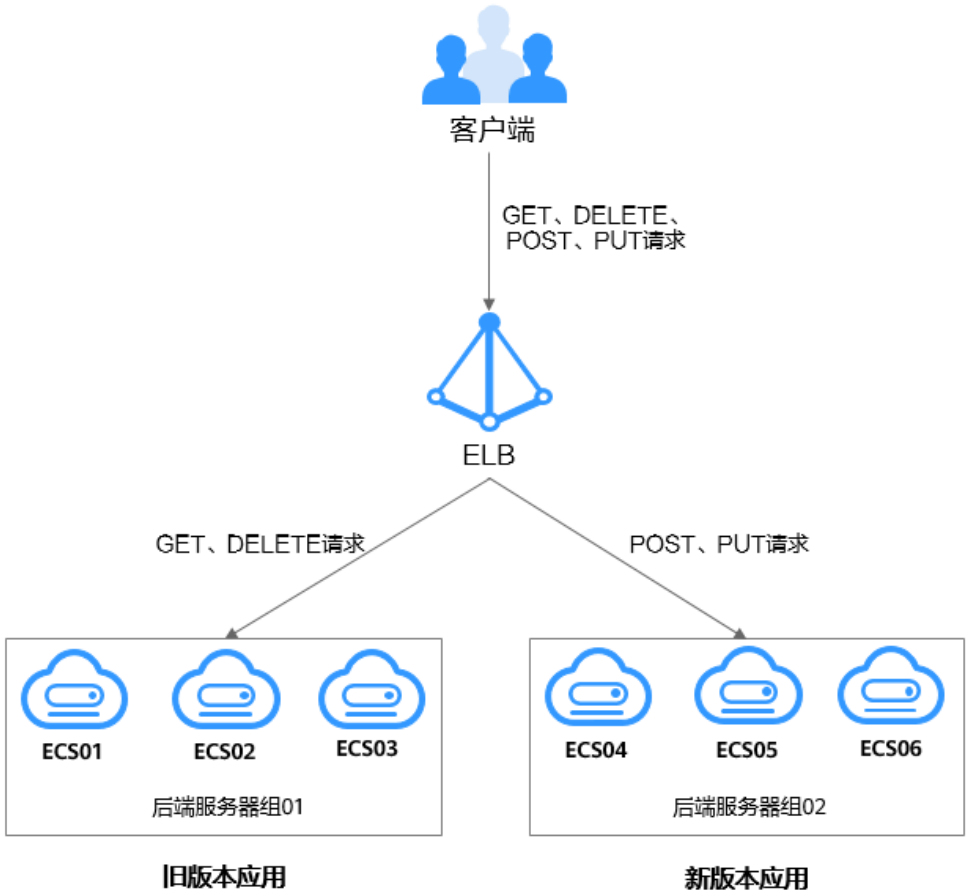
- 所属负载均衡器：选择关联已有ELB-Test
- 后端协议：HTTP
- 其他参数根据需要设置。

6. 参考步骤5再添加后端服务器组Server_Group-Test02。
7. 单击后端服务器组Server_Group-Test01名称，添加ECS01、ECS02、ECS03至Server_Group-Test01。
8. 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。

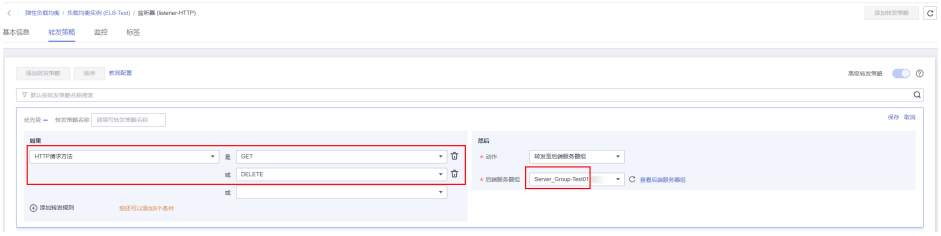
图 2-3 基于 **HTTP 请求方法**实现新旧版本应用平滑过渡



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”。

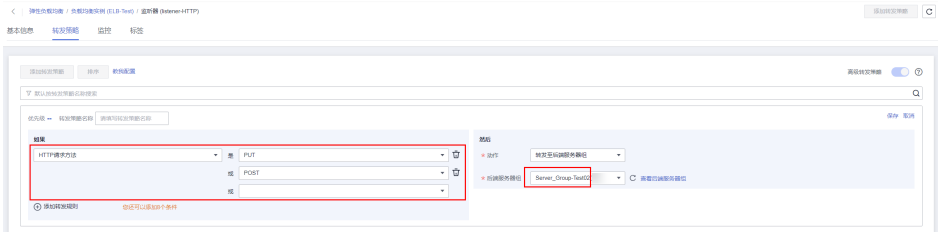
图 2-4 基于 HTTP 请求方法将部分请求转发至旧版本应用上



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”。

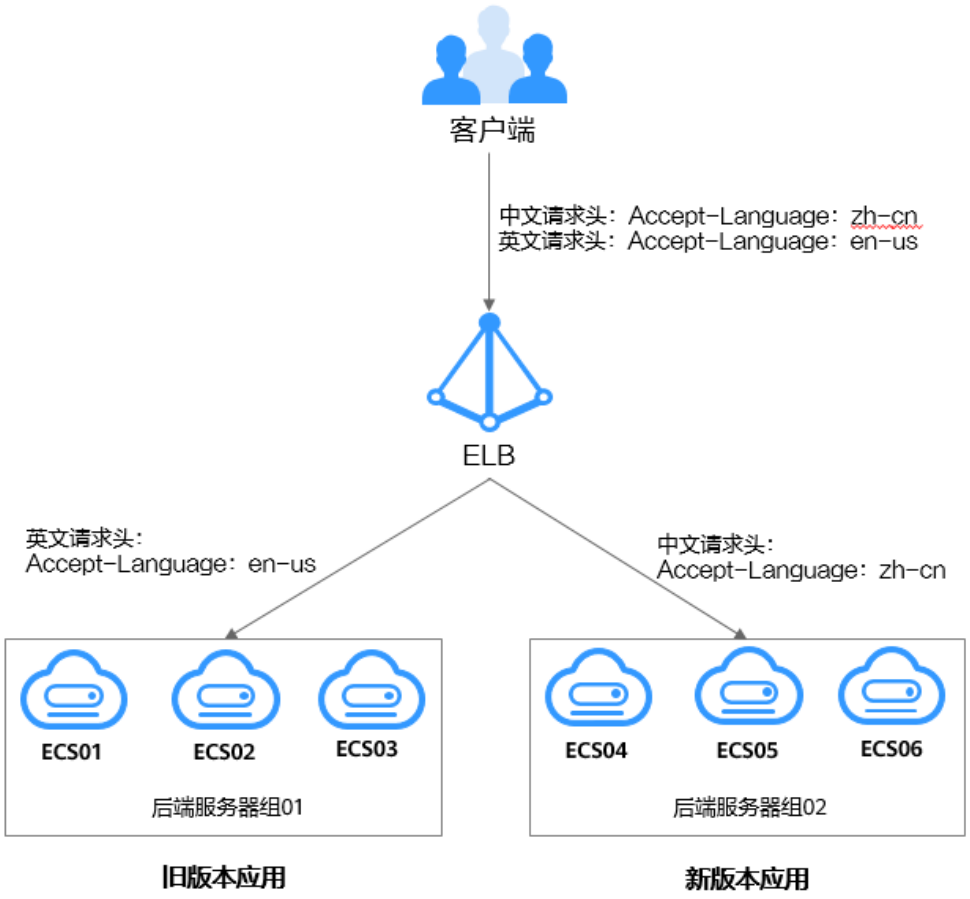
图 2-5 基于 HTTP 请求方法将部分请求转发至新版本应用上



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。

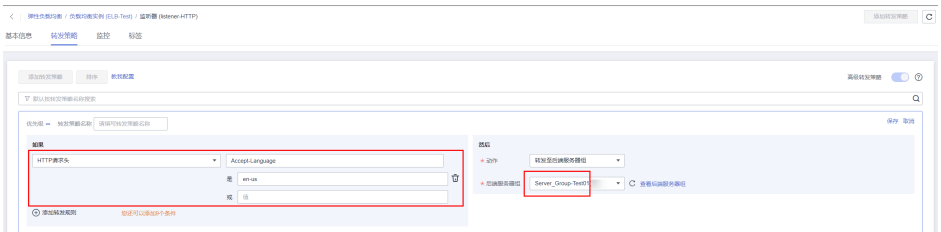
图 2-6 基于 **HTTP 请求头**实现新旧版本应用平滑过渡



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”。

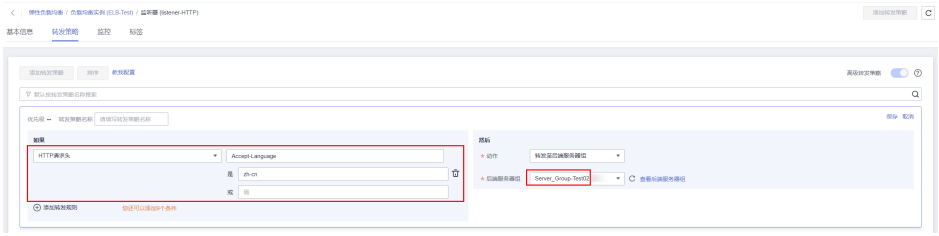
图 2-7 基于 HTTP 请求头将部分请求转发至旧版本应用上



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”。

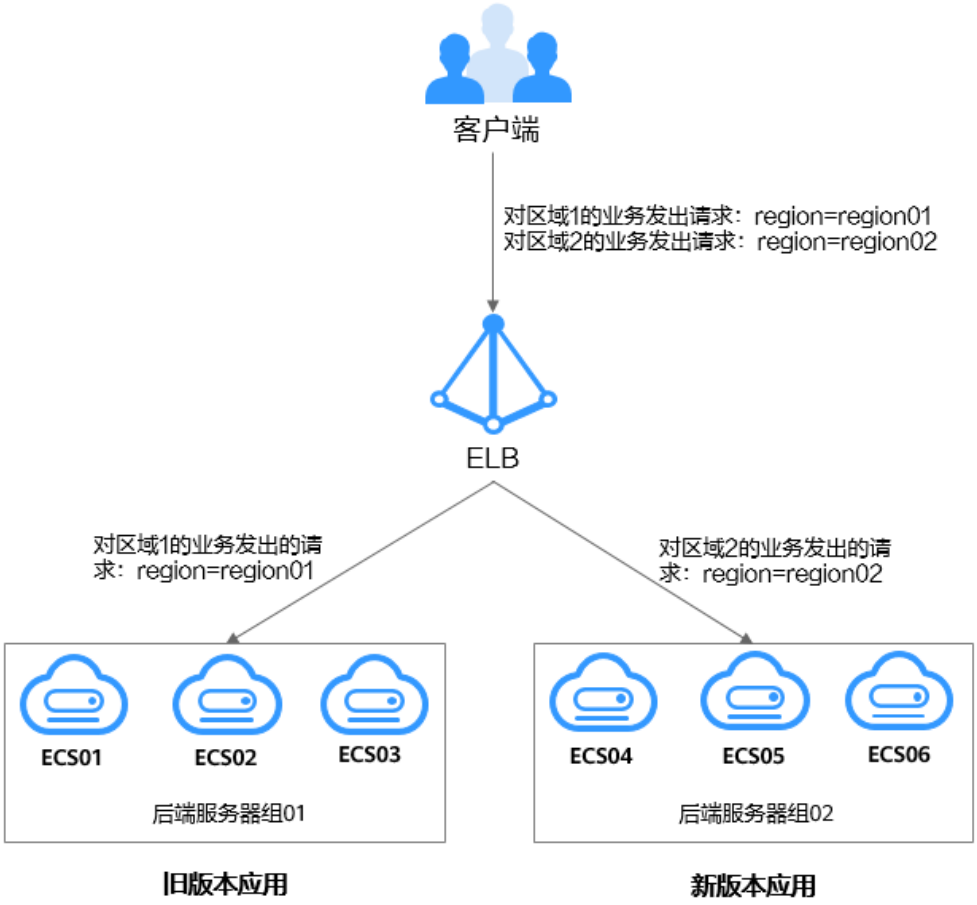
图 2-8 基于 HTTP 请求头将部分请求转发至新版本应用上



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 2-9 基于**查询字符串**实现新旧版本应用平滑过渡



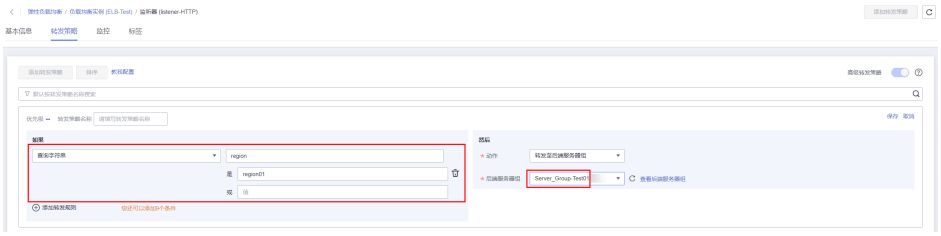
说明

- 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”。

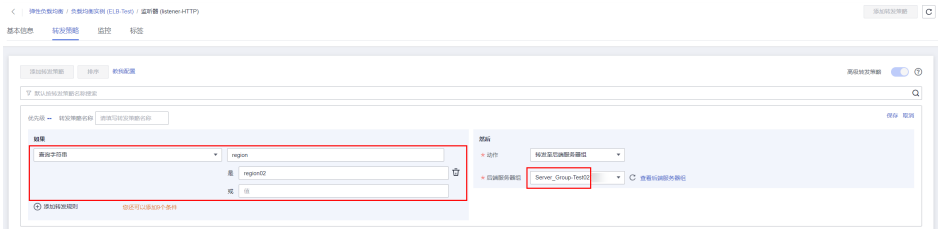
   图 2-10 基于查询字符串将部分请求转发至旧版本应用上

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 2-11 基于查询字符串将部分请求转发至新版本应用上

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**。

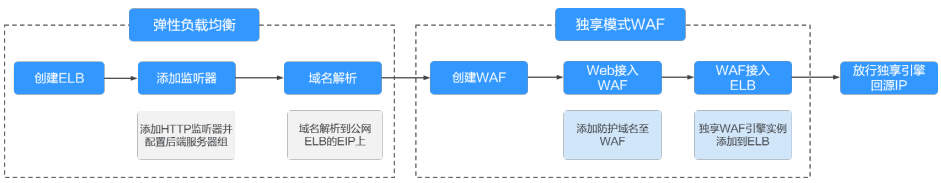
流量路径说明

应用型ELB接入独享WAF对Web业务进行防护后，流量路径如**图3-1**所示。

图 3-1 流量路径图

操作流程

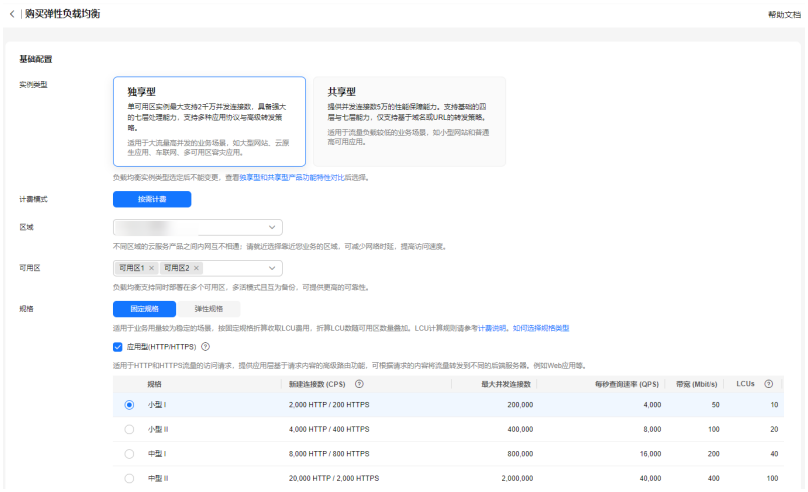
图 3-2 独享 WAF 接入应用型 ELB 的操作流程



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 3-3 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 3-4 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。

图 3-5 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 3-6 配置后端服务器组

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

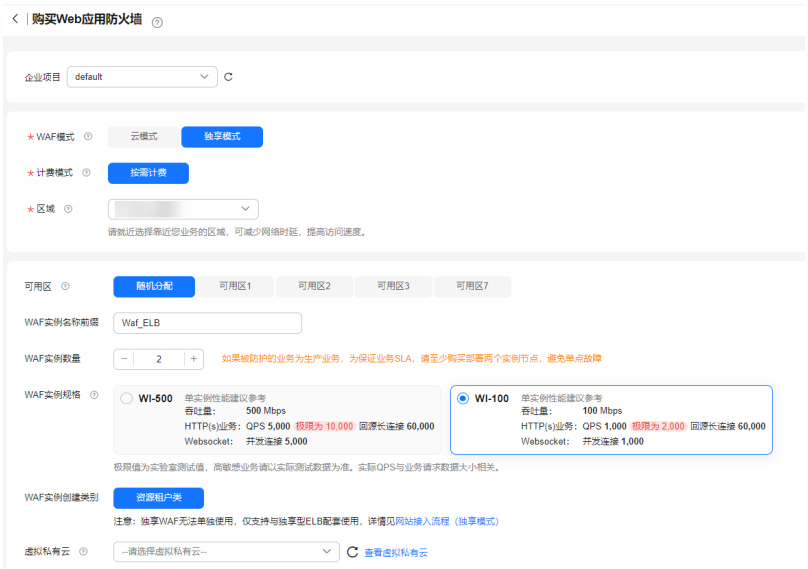
负载均衡器配置完成后，将目标域名如：www.example.com解析到创建的ELB实例的弹性公网IP上，实现对访问域名请求的均衡转发。

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”。
   更多创建WAF实例详情，请参考**购买WAF独享模式**。

   图 3-7 创建独享模式 WAF 实例



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 3-8 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”。

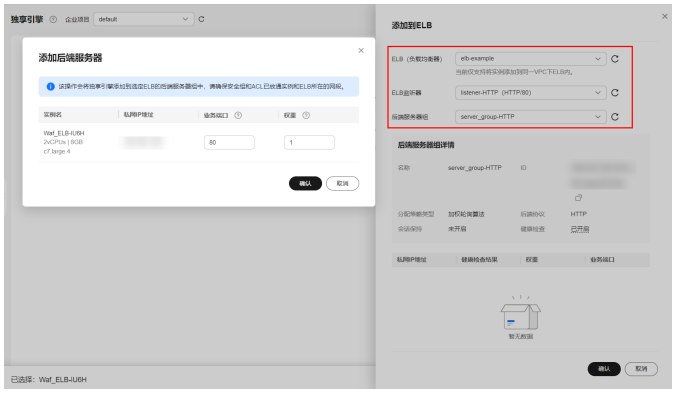
图 3-9 确认高级配置

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 3-10 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**。

4 在 ELB 中配置 HTTPS 双向认证以提升业务安全性

应用场景

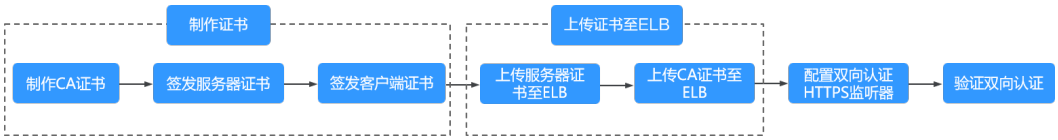
一般的HTTPS业务场景只对服务器做认证，因此只需要配置服务器的证书即可。某些关键业务，需要对通信双方的身份都要做认证，以确保业务的安全性。

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 4-1 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

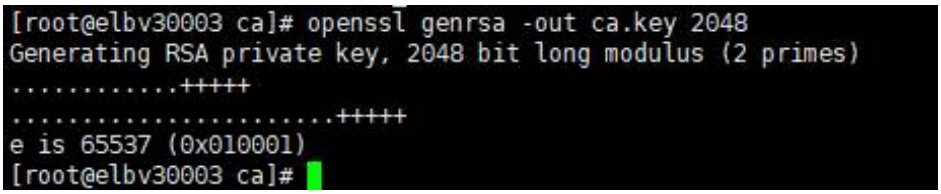
   cd ca
3. 创建CA证书的openssl配置文件ca_cert.conf，内容如下：

```
[ 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 4-2 生成 CA 证书私钥文件



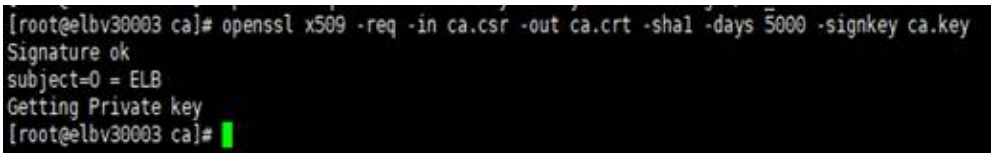
5. 创建CA证书的csr请求文件ca.csr。

   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 4-3 创建自签名 CA 证书



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

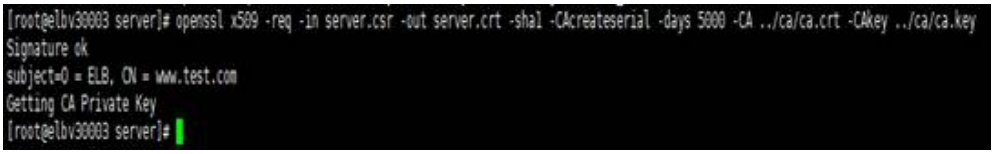
5. 创建服务器证书的csr请求文件server.csr。

   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 4-4 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：

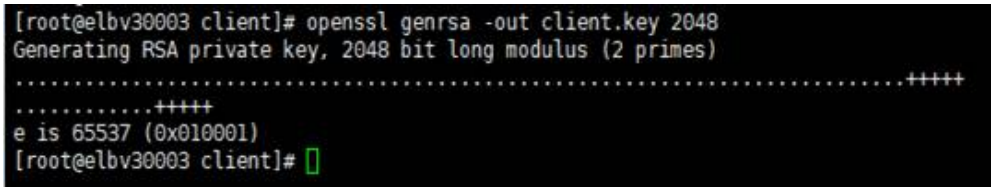
```
[ req ]
distinguished_name     = req_distinguished_name
prompt                 = no

[ 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 4-5 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。

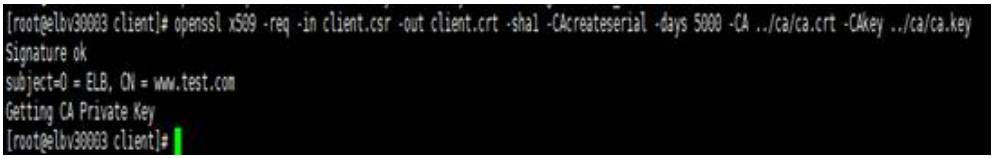
   openssl req -out client.csr -key client.key -new -config ./client_cert.conf

   图 4-6 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 4-7 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 4-8 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。

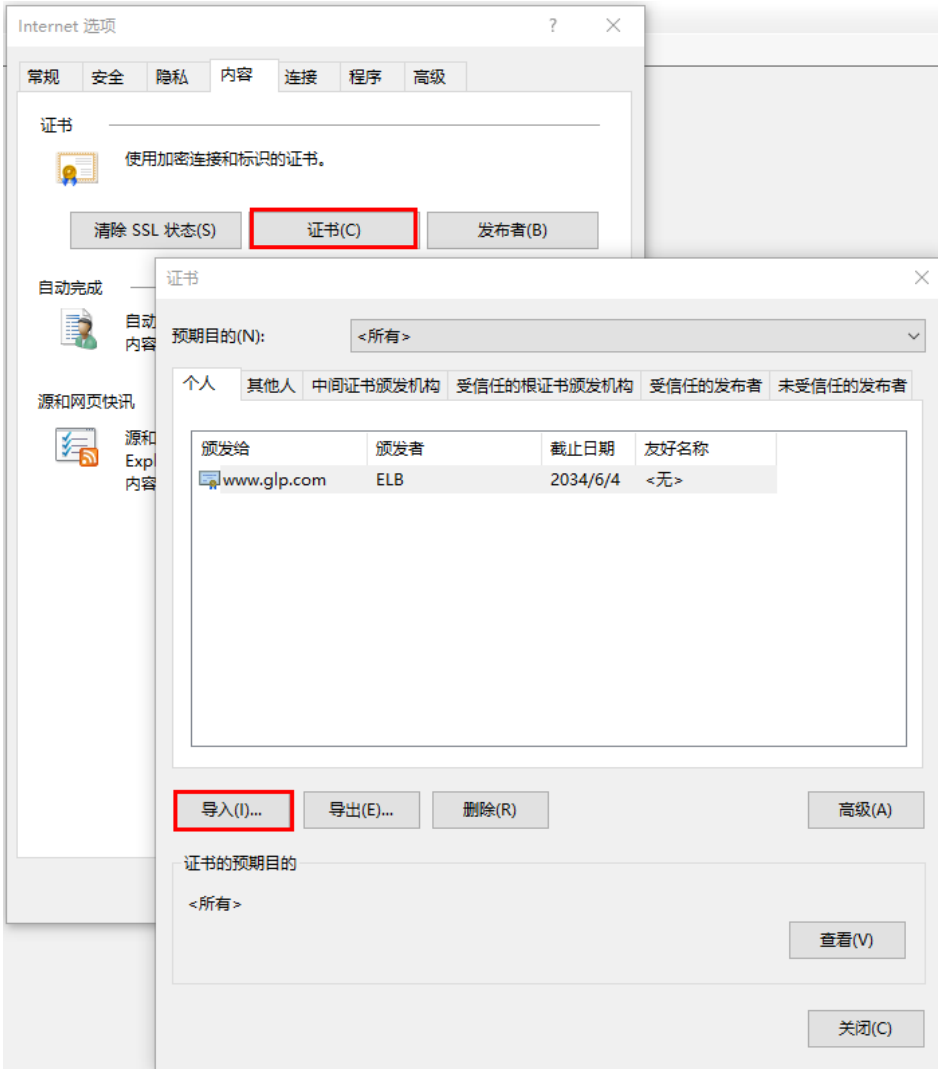
图 4-9 添加 HTTPS 监听器并配置双向认证

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。

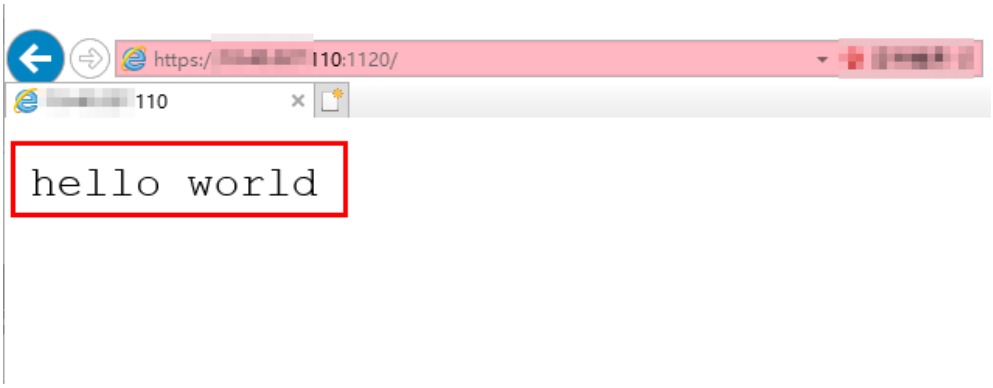
图 4-10 安装 client.p12 证书



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 4-11 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。

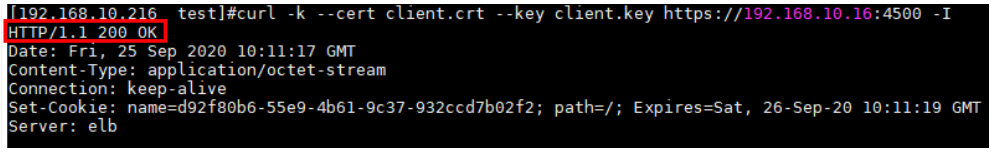
2. 测试验证

   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4-12说明验证成功。

图 4-12 正确响应码示例



5 通过 ELB 将 HTTP 请求重定向至 HTTPS 以提升业务安全性

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HTTP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 5-1 配置 HTTPS 重定向至 HTTPS 监听器操作流程

步骤一：创建 HTTPS 监听器

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，单击需要设置重定向的负载均衡名称。
5. 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5-1。

图 5-2 添加 HTTPS 监听器

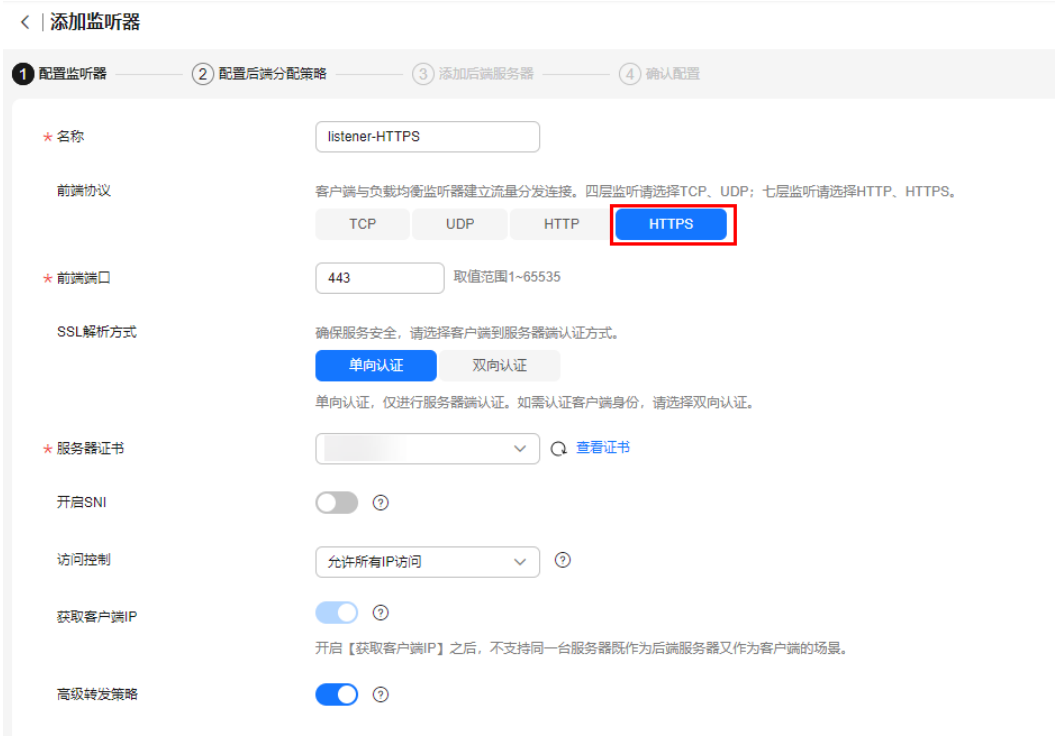


表 5-1 独享型负载均衡配置 HTTPS 监听器参数说明

参数	示例	说明
名称	listener-HTTPS	监听器名称。
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。
前端端口	443	客户端与负载均衡监听器建立流量分发连接的端口。
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。

参数	示例	说明
开启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。
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。
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。

6. 保持“高级配置”参数设置默认不变，单击“下一步：配置后端分配策略”。
7. 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”。
8. 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。
9. 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：添加重定向至 HTTPS 监听器

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。

创建 HTTP 监听器并同步开启重定向

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，单击需要设置重定向的负载均衡名称。
5. 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5-2**。

图 5-3 添加 HTTP 监听器

表 5-2 独享型负载均衡配置 HTTP 监听器参数说明

参数	示例	说明
名称	listener-HTTP	监听器名称。
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。
前端端口	80	客户端与负载均衡监听器建立流量分发连接的端口。
重定向	开启	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。
重定向至	选择**步骤一：创建HTTPS监听器**创建的HTTPS监听器	选择重定向至的HTTPS监听器。
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。
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，便于灵活的分流业务，合理的分配资源。

6. 保持“高级配置”参数设置默认不变，单击“下一步：确认配置”。
7. 单击“提交”，完成HTTP监听器的创建和重定向设置。

创建 HTTP 监听器后配置重定向转发策略

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，单击需要设置重定向的负载均衡名称。
5. 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5-3。

图 5-4 添加 HTTP 监听器

表 5-3 独享型负载均衡配置 HTTP 监听器参数说明

参数	示例	说明
名称	listener-HTTP	监听器名称。
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。
前端端口	80	客户端与负载均衡监听器建立流量分发连接的端口。
重定向	暂不开启	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。
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。
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，便于灵活的分流业务，合理的分配资源。

6. 保持“高级配置”参数设置默认不变，单击“下一步：配置后端分配策略”。
7. 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”。
8. 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。
9. 单击“下一步：确认配置”后，单击“提交”，完成HTTP监听器的创建。
10. 在配置结果页面，单击页面右侧的“去添加”，进入当前HTTP监听器的转发策略”页签。
11. 单击“添加转发策略”添加重定向策略。

表 5-4 重定向至 HTTPS 配置

参数	配置说明
动作	选择“重定向至监听器”。
监听器	选择需要重定向至的HTTPS监听器的名称。

12. 转发策略添加完成后，单击“保存”。

图 5-5 添加重定向至 HTTPS 监听器

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 5-6 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>
```