



弹性负载均衡

用户指南

发布日期 2020-07-30

# 目录

<b>1 产品介绍</b>	<b>1</b>
1.1 什么是弹性负载均衡	1
1.2 产品优势	2
1.3 应用场景	3
1.4 弹性负载均衡是如何工作的	5
1.5 公网和私网负载均衡器	6
1.6 与其他服务的关系	8
1.7 基本概念	8
1.7.1 产品基本概念	8
1.7.2 区域和可用区	9
<b>2 负载均衡器</b>	<b>11</b>
2.1 公网和私网负载均衡器	11
2.2 规划和准备	12
2.3 创建负载均衡器	13
2.4 变更配置	16
2.5 为实例绑定/解绑 EIP	16
2.6 删除负载均衡器	17
<b>3 监听器</b>	<b>19</b>
3.1 什么是监听器	19
3.2 协议和端口	20
3.3 创建监听器	21
3.4 流量分配策略	24
3.5 会话保持	25
3.6 访问控制策略	26
3.7 修改监听器	28
3.8 HTTP/HTTPS 高级配置	28
3.8.1 转发策略	28
3.8.2 HTTPS 双向认证	32
3.8.3 HTTP/2	37
3.8.4 HTTP 重定向至 HTTPS	38
3.8.5 配置 SNI	39
<b>4 后端服务器</b>	<b>40</b>

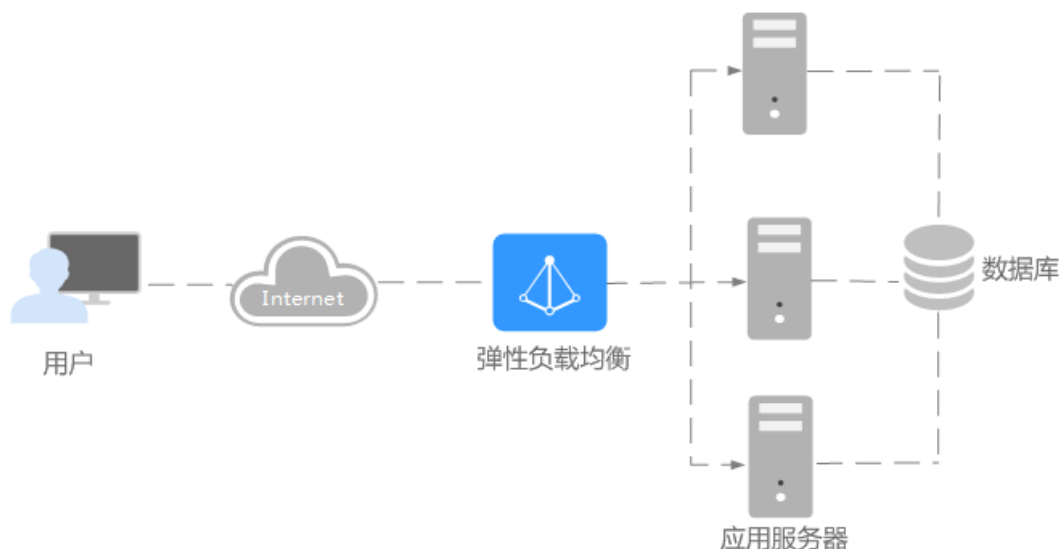
4.1 后端服务器介绍.....	40
4.2 后端服务器配置安全组.....	40
4.3 添加或移除后端服务器.....	42
<b>5 健康检查.....</b>	<b>47</b>
5.1 配置健康检查.....	47
5.2 关闭健康检查.....	48
<b>6 证书管理.....</b>	<b>50</b>
6.1 证书格式.....	50
6.2 格式转换.....	51
6.3 创建证书.....	52
<b>7 访问日志.....</b>	<b>54</b>
<b>8 监控.....</b>	<b>58</b>
8.1 监控指标说明.....	58
8.2 设置告警规则.....	61
8.2.1 添加告警规则.....	62
8.2.2 修改告警规则.....	62
8.3 查看监控指标.....	62
<b>9 审计.....</b>	<b>64</b>
9.1 支持审计的关键操作列表.....	64
9.2 查看审计日志.....	65
<b>10 常见问题.....</b>	<b>67</b>
10.1 高频常见问题.....	67
10.2 弹性负载均衡使用.....	67
10.2.1 异常检查.....	67
10.2.1.1 如何检查弹性负载均衡服务不通或异常中断？ .....	67
10.2.2 功能支持.....	68
10.2.2.1 弹性负载均衡器是否可以单独使用？ .....	68
10.2.2.2 弹性负载均衡分配的 EIP 是否为独占？ .....	68
10.2.2.3 单个用户默认可以创建多少个负载均衡器或监听器？ .....	68
10.2.2.4 当负载均衡器正在运行中是否可以调整后端服务器的数量？ .....	68
10.2.2.5 弹性负载均衡是否可以添加不同操作系统的服务器？ .....	68
10.2.3 性能负载.....	68
10.2.3.1 如何检查弹性负载均衡前后端流量不一致？ .....	68
10.2.3.2 如何检查请求不均衡？ .....	69
10.2.3.3 如何检查弹性负载均衡业务访问延时大？ .....	69
10.2.3.4 如何检测压测性能上不去？ .....	69
10.3 负载均衡器.....	69
10.3.1 ELB 如何根据不同的协议来分发流量？ .....	69
10.3.2 如何配置私网或公网负载均衡？ .....	70
10.4 监听器.....	70

10.4.1 监听器中分配算法和会话保持算法是什么关系？ .....	70
10.4.2 弹性负载均衡如何支持多证书？ .....	71
10.4.3 如何启用 WebSocket 支持？ .....	71
10.5 后端服务器.....	71
10.5.1 为什么后端服务器上收到的健康检查报文间隔和设置的间隔时间不一致？ .....	71
10.5.2 使用 ELB 后，后端服务器能否访问公网？ .....	71
10.5.3 如何检查后端服务器网络状态？ .....	71
10.5.4 如何检查后端服务器网络配置？ .....	72
10.5.5 如何检查后端服务器服务状态？ .....	72
10.5.6 后端服务器什么时候被认为是健康的？ .....	73
10.6 健康检查.....	73
10.6.1 健康检查异常如何排查？ .....	73
10.6.2 使用 UDP 协议有什么注意事项？ .....	78
10.6.3 健康检查为什么会导导致 ELB 会频繁向后端服务器发送探测请求？ .....	80
10.7 获取源 IP.....	80
10.7.1 如何获取来访者的真实 IP？ .....	80
10.8 HTTP/HTTPS 监听器.....	86
10.8.1 为什么配置证书后仍出现不安全提示？ .....	86
10.9 会话保持.....	87
10.9.1 如何检查弹性负载均衡会话保持不生效问题？ .....	87
10.9.2 ELB 支持什么类型的会话保持？ .....	87
<b>11 附录.....</b>	<b>88</b>
11.1 TOA 插件配置.....	88
<b>12 修订记录.....</b>	<b>94</b>

# 1 产品介绍

## 1.1 什么是弹性负载均衡

弹性负载均衡（Elastic Load Balance，简称ELB）是将访问流量根据分配策略分发到后端多台服务器的流量分发控制服务。弹性负载均衡可以通过流量分发扩展应用系统对外的服务能力，同时通过消除单点故障提升应用系统的可用性。



### 弹性负载均衡的组件

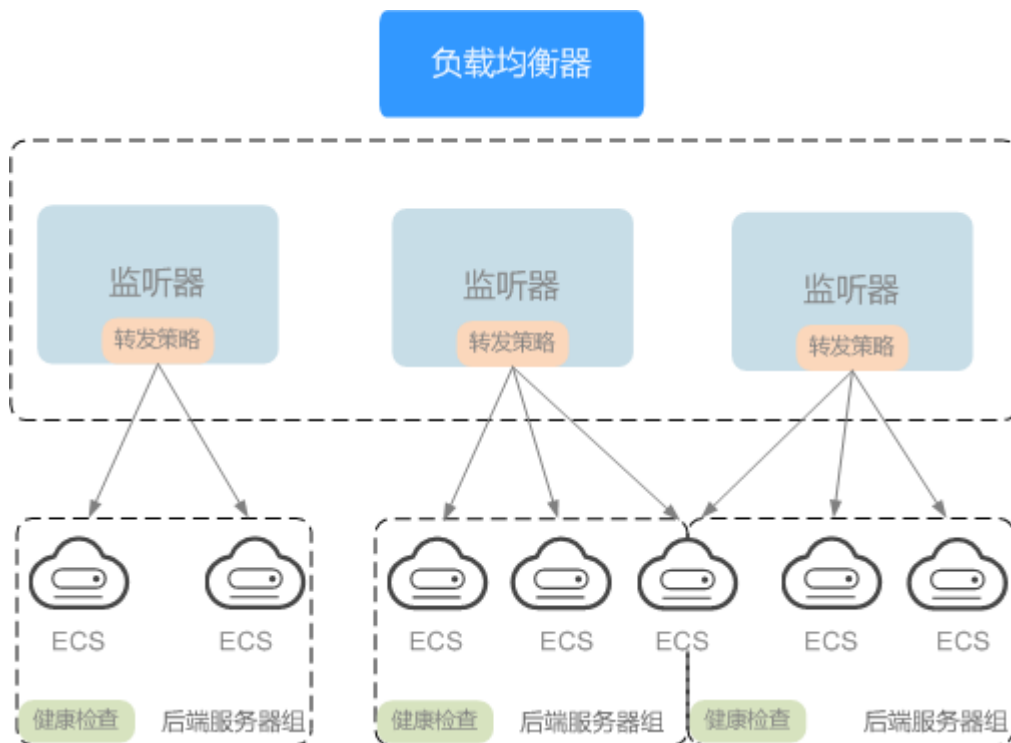
弹性负载均衡由以下3部分组成：

- **负载均衡器**：接受来自客户端的传入流量并将请求转发到一个或多个可用区中的后端服务器。
- **监听器**：您可以向您的弹性负载均衡器添加一个或多个监听器。监听器使用您配置的协议和端口检查来自客户端的连接请求，并根据您定义的分配策略将请求转发到一个后端服务器组里的后端服务器。
- **后端服务器**：每个监听器会绑定一个后端服务器组，后端服务器组中可以添加一个或多个后端服务器。后端服务器组使用您指定的协议和端口号将请求转发到一个或多个后端服务器。

可以为后端服务器配置流量转发权重，不能为后端服务器组配置权重。

您可以开启健康检查功能，对每个后端服务器组配置运行状况检查。当后端某台服务器健康检查出现异常时，弹性负载均衡会自动将新的请求分发到其它健康检查正常的后端服务器上；而当该后端服务器恢复正常运行时，弹性负载均衡会将其自动恢复到弹性负载均衡服务中。

图 1-1 弹性负载均衡组件图



## 如何访问弹性负载均衡

可以使用以下方式访问和管理弹性负载均衡：

- 管理控制台  
请使用管理控制台方式访问弹性负载均衡。可直接登录管理控制台，从主页选择“弹性负载均衡”。
- 查询API  
通过调用API的方式访问弹性负载均衡，具体操作请参见《弹性负载均衡API参考》。

## 1.2 产品优势

弹性负载均衡具有以下优势：

- 高性能  
集群支持最高1亿并发连接，满足用户的海量业务访问需求。
- 高可用  
采用集群化部署，支持多可用区的同城双活容灾，无缝实时切换。

- 灵活扩展  
根据应用流量自动完成分发，与弹性伸缩服务无缝集成，灵活扩展用户应用的对外服务能力。
- 简单易用  
快速部署ELB，实时生效，支持多种协议、多种调度算法可选，用户可以高效地管理和调整分发策略。

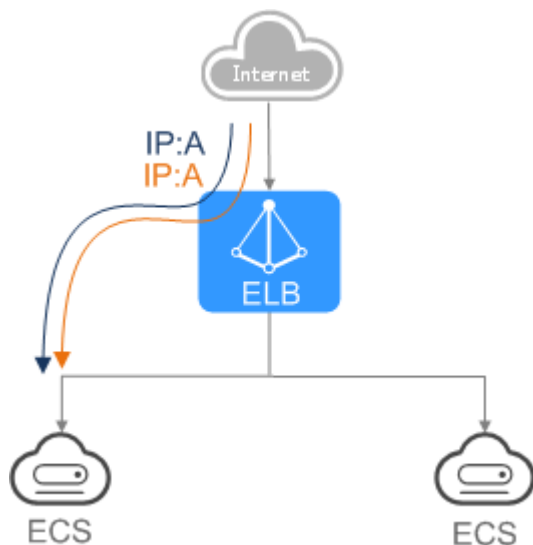
## 1.3 应用场景

### 使用 ELB 为高访问量业务进行流量分发

对于业务量访问较大的业务，可以通过ELB设置相应的分配策略，将访问量均匀的分到多个后端服务器处理。例如大型门户网站，移动应用市场等。

同时您还可以开启会话保持功能，保证同一个客户请求转发到同一个后端服务器。从而提升访问效率，如[图1-2](#)所示。

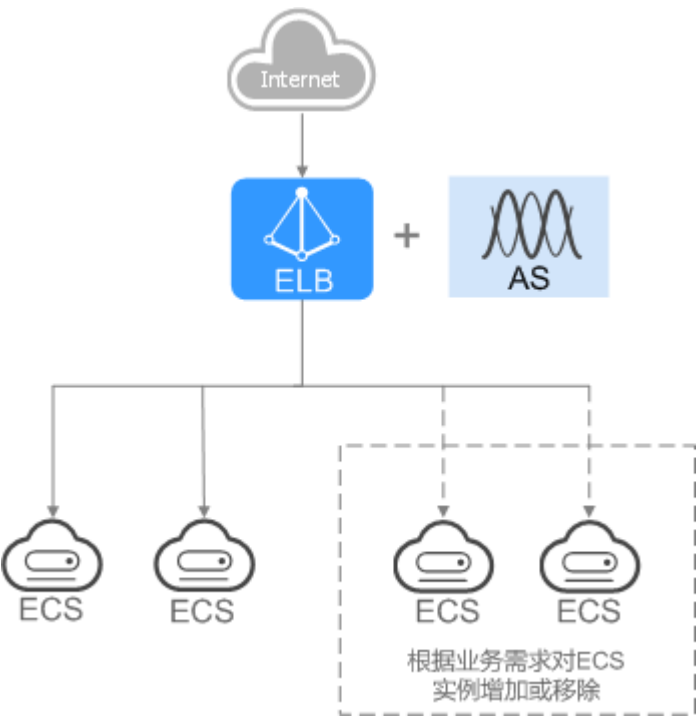
图 1-2 会话保持流量分发



### 使用 ELB 和 AS 为潮汐业务弹性分发流量

对于存在潮汐效应的业务，结合弹性伸缩服务，随着业务量的增长和收缩，弹性伸缩服务自动增加或者减少的ECS实例，可以自动添加到ELB的后端云服务器组或者从ELB的后端云服务器组移除。负载均衡实例会根据流量分发、健康检查等策略灵活使用ECS实例资源，在资源弹性的基础上大大提高资源可用性，如[图1-3](#)所示。例如电商的“双11”、“双12”、“618”等大型促销活动，业务的访问量短时间迅速增长，且只持续短暂的几天甚至几小时。使用负载均衡及弹性伸缩能最大限度的节省IT成本。

图 1-3 灵活扩展

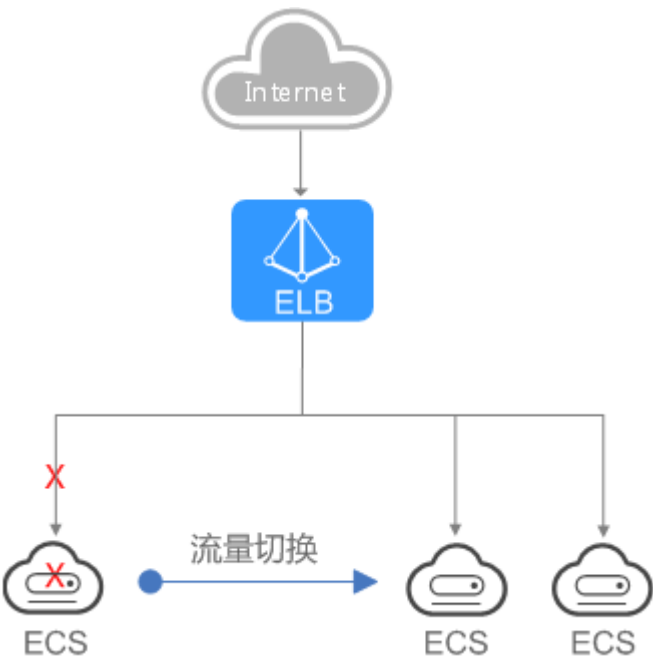


使用 ELB 消除单点故障

对于可靠性有较高要求的业务，可以在负载均衡器上添加多个后端云服务器。负载均衡器会通过健康检查及时发现并屏蔽有故障的云服务器，并将流量转发到其他正常运行的后端云服务器，确保业务不中断，如图1-4所示。

例如官网，Web业务等。

图 1-4 消除单点故障



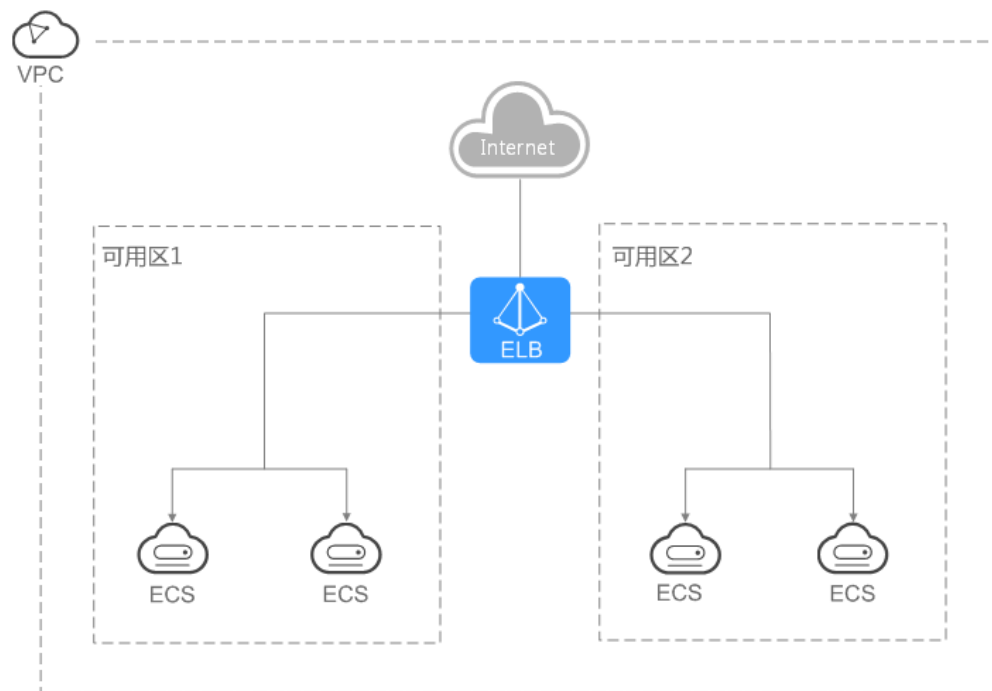


## 使用 ELB 跨可用区特性实现业务容灾部署

对于可靠性和容灾有很高要求的业务，弹性负载均衡可将流量跨可用区进行分发，建立实时的业务容灾部署。即使出现某个可用区网络故障，负载均衡器仍可将流量转发到其他可用区的后端云服务器进行处理，如图1-5所示。

例如银行业务，警务业务，大型应用系统等。

图 1-5 多可用区部署



## 1.4 弹性负载均衡是如何工作的

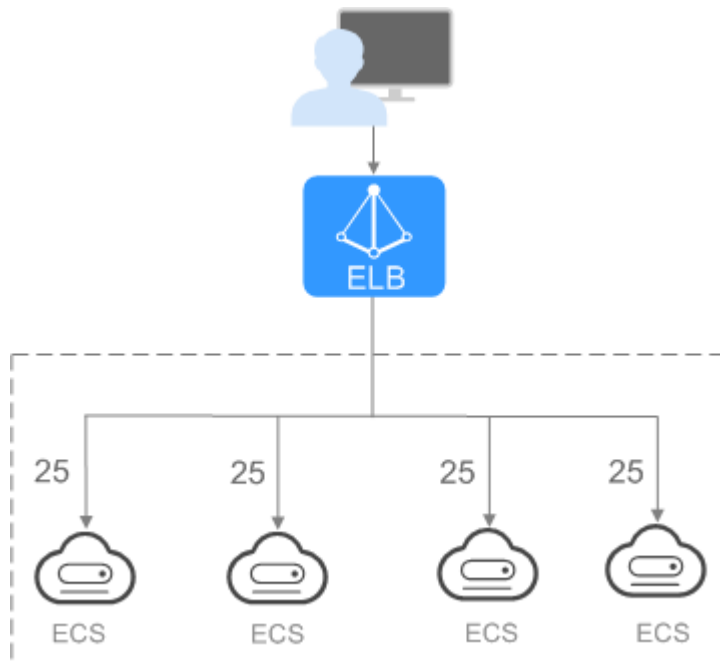
您可以在弹性负载均衡服务中创建一个负载均衡器。该负载均衡器会接收来自客户端的请求，并将请求转发到一个或多个可用区的后端服务器中进行处理。请求的流量分发与负载均衡器配置的分配策略类型相关。

负载均衡算法，支持以下三种调度算法：

- 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。它用相应的权重表示服务器的处理性能，按照权重的高低以及轮询方式将请求分配给各服务器，相同权重的服务器处理相同数目的连接数。常用于短连接服务，例如HTTP等服务。
- 加权最少连接：最少连接是通过当前活跃的连接数来估计服务器负载情况的一种动态调度算法。加权最少连接就是在最少连接数的基础上，根据服务器的不同处理能力，给每个服务器分配不同的权重，使其能够接受相应权值数的服务请求。常用于长连接服务，例如数据库连接等服务。
- 源IP算法：将请求的源IP地址进行一致性Hash运算，得到一个具体的数值，同时对后端服务器进行编号，按照运算结果将请求分发到对应编号的服务器上。这可以使对同一源IP的访问进行负载分发，同时使得同一个客户端IP的请求始终被派发到某特定的服务器。该方式适合负载均衡无cookie功能的TCP协议。

**图1-6**展示弹性负载均衡器使用加权轮询算法的流量分发流程。假设可用区内有4台权重相同的后端服务器，负载均衡器节点会将25%的客户端流量分发到其可用区中的每一台后端服务器。

**图 1-6** 加权轮询算法流量分发

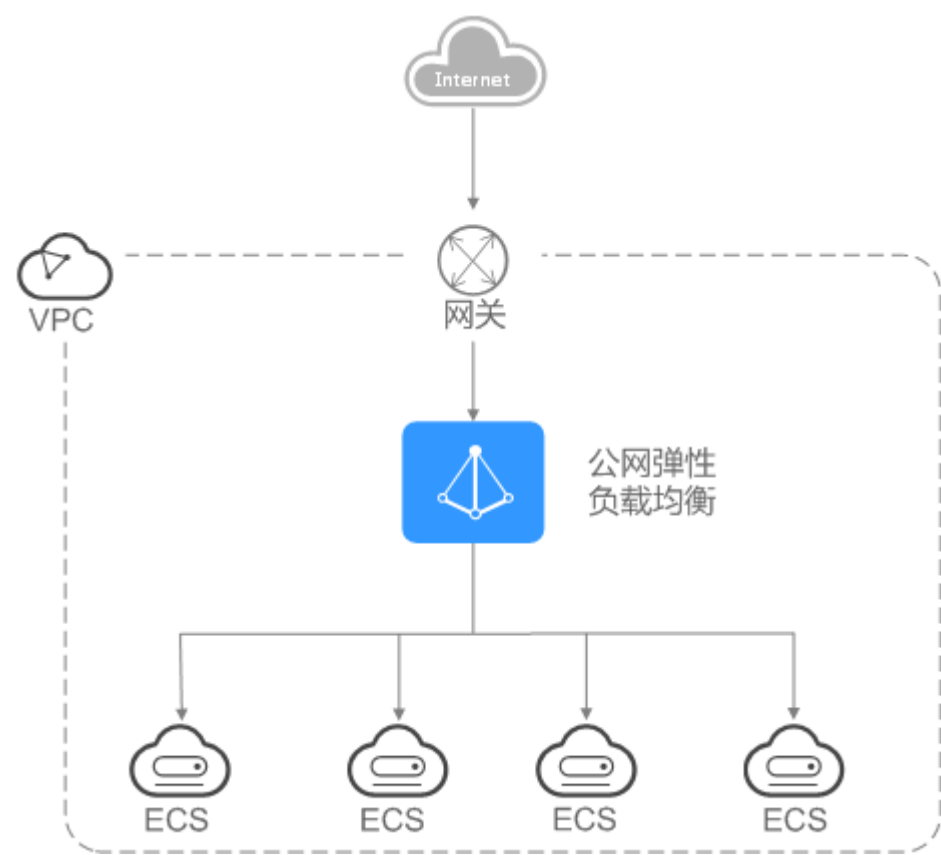


## 1.5 公网和私网负载均衡器

### 公网负载均衡器

公网负载均衡器通过公网IP对外提供服务，将来自公网的客户端请求按照指定的负载均衡策略分发到后端云服务器进行处理。

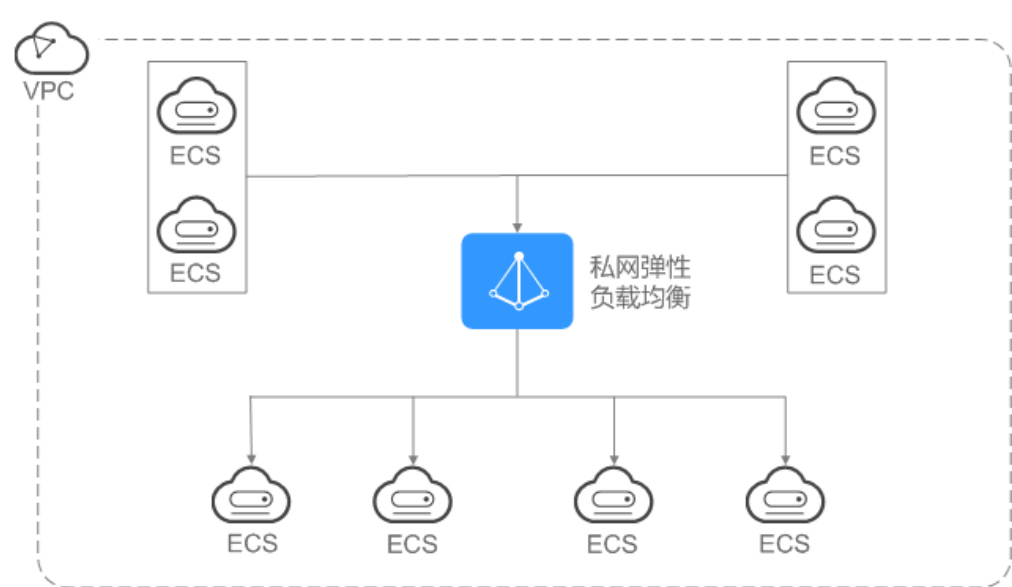
图 1-7 公网负载均衡器



私网负载均衡器

私网负载均衡器通过私网IP对外提供服务，将来自同一个VPC的客户端请求按照指定的负载均衡策略分发到后端进行处理。

图 1-8 私网负载均衡器



## 1.6 与其他服务的关系

- 虚拟私有云（VPC）  
创建ELB时需要使用虚拟私有云服务创建的弹性IP、带宽。
- 弹性伸缩（AS）  
当配置了负载均衡服务后，弹性伸缩在添加和移除云服务器时，自动在负载均衡服务中添加和移除云服务器。
- 统一身份认证服务（IAM）  
需要统一身份认证提供鉴权。
- 云审计（CTS）  
使用云审计服务记录弹性负载均衡服务的资源操作。
- 云监控（Cloud Eye）  
当用户开通了弹性负载均衡服务后，无需额外安装其他插件，即可在云监控查看对应服务的实例状态。

## 1.7 基本概念

### 1.7.1 产品基本概念

表 1-1 弹性负载均衡基本概念

名词	说明
负载均衡器	负载均衡器是指您创建的承载业务的负载均衡服务实体。
监听器	监听器负责监听负载均衡器上的请求，根据配置的流量分配策略，分发流量到后端云服务器处理。
后端服务器	负载均衡器会将客户端的请求转发给后端服务器处理。例如，您可以添加ECS实例作为负载均衡器的后端服务器，监听器使用您配置的协议和端口检查来自客户端的连接请求，并根据您定义的分配策略将请求转发到后端服务器组里的后端云服务器。
后端服务器组	把具有相同特性的后端服务器放在一个组，负载均衡实例进行流量分发时，流量分配策略以后端服务器组为单位生效。
健康检查	负载均衡器会定期向后端服务器发送请求以测试其运行状态，这些测试称为健康检查。通过健康检查来判断后端服务器是否可用。负载均衡器如果判断后端服务器健康检查异常，就不会将流量分发到异常后端服务器，而是分发到健康检查正常的后端服务器，从而提高了业务的可靠性。当异常的后端服务器恢复正常运行后，负载均衡器会将其自动恢复到负载均衡服务中，承载业务流量。
重定向	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HTTP访问重定向至HTTPS。

名词	说明
会话保持	会话保持就是指在负载均衡器上有这么一种机制，可以识别客户与服务器之间交互过程的关联性，在作负载均衡的同时，还保证一系列相关联的访问请求会保持分配到同一台服务器上。
WebSocket	WebSocket (WS)是HTML5一种新的协议。它实现了浏览器与服务器全双工通信，能更好地节省服务器资源和带宽并达到实时通讯。WebSocket建立在TCP之上，同HTTP一样通过TCP来传输数据，但是它和HTTP最大不同在于，WebSocket是一种双向通信协议，在建立连接后，WebSocket服务器和Browser/Client Agent都能主动的向对方发送或接收数据，就像Socket一样；WebSocket需要类似TCP的客户端和服务端通过握手连接，连接成功后才能相互通信。
SNI	如果用户的后台应用对外提供多个域名的访问，并且每个域名都使用独立的证书，则需要创建HTTPS监听器时开启SNI功能。SNI（Server Name Indication）是为了解决一个服务器使用多个域名和证书的TLS扩展，主要解决一台服务器只能使用一个证书的缺点。开启SNI后，允许客户端在发起SSL握手请求时就提交请求的域名信息，负载均衡收到SSL请求后，会根据域名去查找证书，如果找到域名对应的证书，则返回该证书；如果没有找到域名对应的证书，则返回缺省证书。负载均衡在配置HTTPS 监听器支持此功能，即支持绑定多个证书。
长连接	长连接是指在一个连接上可以连续发送多个数据包，在连接保持期间，如果没有数据包发送，需要双方发链路检测包。
短连接	短连接是指通讯双方有数据交互时，就建立一个连接，数据发送完成后，则断开此连接，即每次连接只完成一项业务的发送。
并发连接	并发连接指客户端向服务器发起请求并建立了TCP连接的总和，负载均衡的并发连接是指每秒钟所能接收并处理的TCP连接总和。

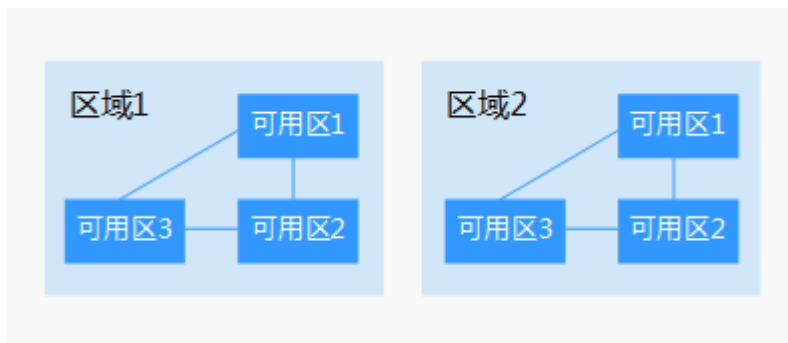
### 1.7.2 区域和可用区

#### 什么是区域、可用区？

- 我们用区域和可用区来描述数据中心的位置，您可以在特定的区域、可用区创建资源。
- 区域（Region）指物理的数据中心。每个区域完全独立，这样可以实现最大程度的容错能力和稳定性。资源创建成功后不能更换区域。
  - 可用区（AZ，Availability Zone）是同一区域内，电力和网络互相隔离的物理区域，一个可用区不受其他可用区故障的影响。一个区域内可以有多个可用区，不同可用区之间物理隔离，但内网互通，既保障了可用区的独立性，又提供了低价、低时延的网络连接。

图1-9阐明了区域和可用区之间的关系。

图 1-9 区域和可用区



## 如何选择区域？

建议就近选择靠近您或者您的目标用户的区域，这样可以减少网络时延，提高访问速度。

## 如何选择可用区？

是否将资源放在同一可用区内，主要取决于您对容灾能力和网络时延的要求。

- 如果您的应用需要较高的容灾能力，建议您将资源部署在同一区域的不同可用区内。
- 如果您的应用要求实例之间的网络延时较低，则建议您将资源创建在同一可用区内。

## 区域和终端节点

当您通过API使用资源时，您必须指定其区域终端节点。有关公有云的区域和终端节点的更多信息，请参阅[地区和终端节点](#)。

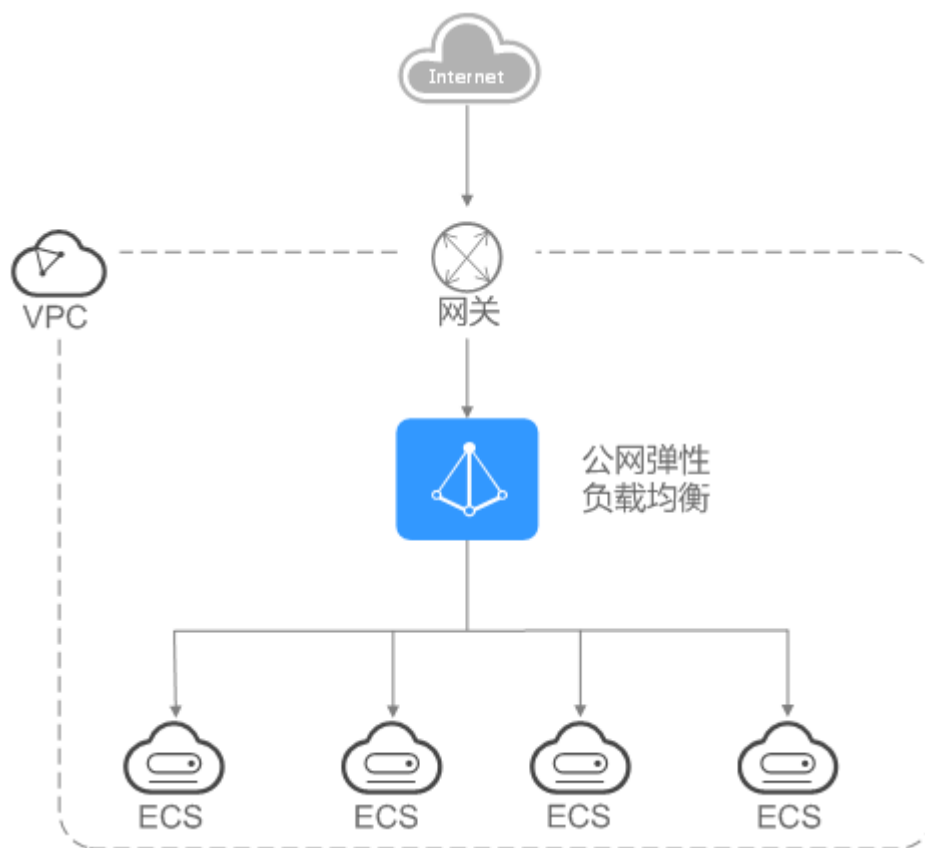
# 2 负载均衡器

## 2.1 公网和私网负载均衡器

### 公网负载均衡器

公网负载均衡器通过公网IP对外提供服务，将来自公网的客户端请求按照指定的负载均衡策略分发到后端云服务器进行处理。

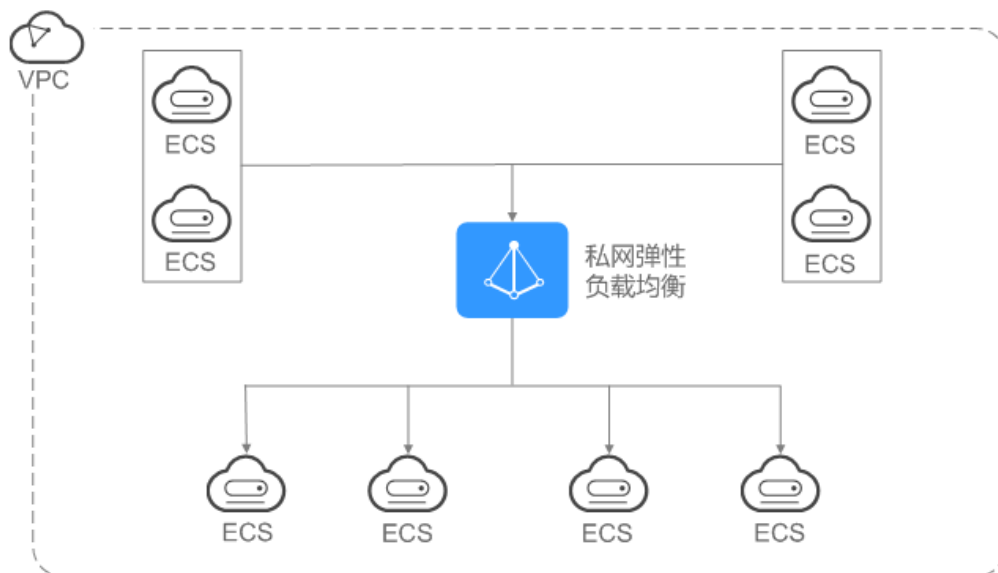
图 2-1 公网负载均衡器



## 私网负载均衡器

私网负载均衡器通过私网IP对外提供服务，将来自同一个VPC的客户端请求按照指定的负载均衡策略分发到后端进行处理。

图 2-2 私网负载均衡器



## 2.2 规划和准备

在使用负载均衡前，需要根据业务规划待创建负载均衡器的区域、类型、协议以及后端服务器等。

### 规划实例区域

负载均衡器选择区域时需要注意以下事项：

- 选择距离业务目标客户距离最近的区域，可以减少网络时延以及提高下载速度。
- 选择与后端服务器相同的区域，负载均衡不支持跨区域部署。

### 网络类型（公网或私网）

负载均衡器分为公网负载均衡器和私网负载均衡器。

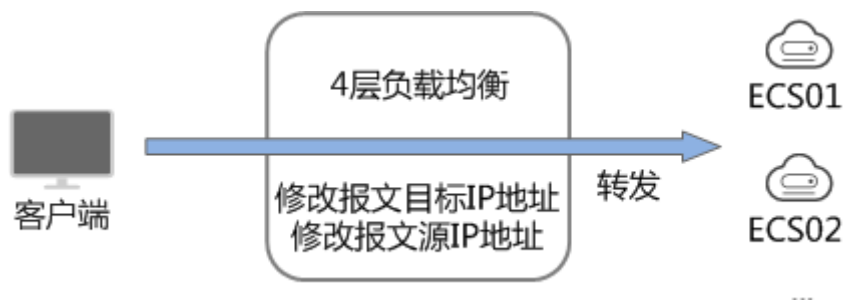
- 如果需要使用负载均衡分发来自Internet公网的访问请求，需要创建公网负载均衡器。  
创建公网负载均衡器会绑定一个EIP，用来接收来自Internet公网的访问请求。
- 如果需要使用负载均衡分发来自VPC内网的访问请求，选择创建私网负载均衡器。  
私网负载均衡器仅分配一个私网IP，仅能用来接收来自同个VPC内的访问请求。

### 选择协议类型

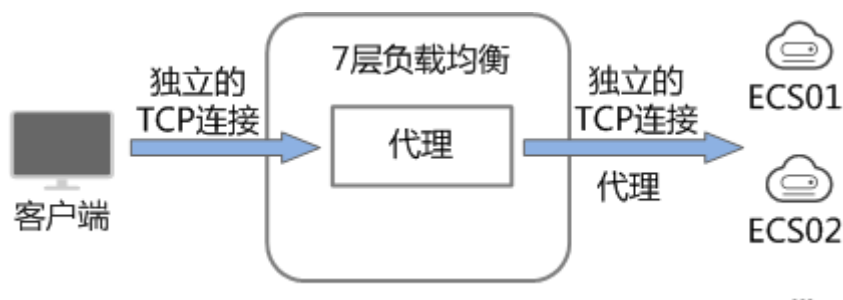
提供基于四层协议和七层协议的负载均衡，在负载均衡器中通过加监听器选择相应的协议。



- 使用四层协议的负载均衡，监听器收到访问请求后，将请求直接转发给后端服务器。转发过程仅修改报文中目标IP地址和源IP地址，将目标地址改为后端云服务器的IP地址，源地址改为负载均衡器的IP地址。四层协议连接的建立，既三次握手是客户端和后端服务器直接建立的，负载均衡只是进行了数据的转发。



- 使用七层协议的负载均衡，也称为“内容交换”。监听器收到访问请求后，需要识别并通过HTTP/HTTPS协议报文头中的相关字段，进行数据的转发。监听器收到访问请求后，先代理后端服务器和客户端建立连接（三次握手），接收客户端发送的包含应用层内容的报文，然后根据报文中的特定字段和流量分配策略判断需要转发的后端服务器。此场景中，负载均衡类似一个代理服务器，分别和客户端以及后端服务器建立连接。



## 后端服务器

在使用负载均衡器前，需要先创建ECS实例或者BMS实例并部署相关业务应用，然后将ECS实例或者BMS实例添加到负载均衡器的后端服务器组来处理转发的客户端访问请求。创建后端服务器时，请注意以下事项：

- 确保后端服务器实例的所属地域和负载均衡器的所属地域相同。
- 建议您选择相同操作系统的后端服务器实例作为后端服务器，以便后续管理和维护。

## 2.3 创建负载均衡器

### 前提条件

在您创建负载均衡器前，确保您已经做好了相关规划，详情参考[规划和准备](#)。

负载均衡作为流量转发服务，将来自客户端的请求通过负载均衡器转发至后端服务器，后端服务器再将响应通过内网返回给负载均衡。

创建负载均衡器


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. 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“创建弹性负载均衡”。根据界面提示进行配置参数，配置参数如表2-1所示。

表 2-1 负载均衡器配置参数

参数	说明	取值样例
区域	不同区域的资源之间内网不互通。 请选择靠近您客户的区域，可以降低网络时延、提高访问速度。	-
网络类型	可选公网或者私网。 <ul style="list-style-type: none"><li>公网：公网负载均衡器通过公网IP对外提供服务，将来自公网的客户端请求按照指定的负载均衡策略分发到后端服务器进行处理。</li><li>私网：私网负载均衡器通过私网IP对外提供服务，将来自同一个VPC的客户端请求按照指定的负载均衡策略分发到后端服务器进行处理。</li></ul>	私网
所属VPC	所属虚拟私有云。 您可以选择使用已有的虚拟私有云网络，或者创建新的虚拟私有云。 更多关于虚拟私有云的信息，请参见《虚拟私有云用户指南》。	-
子网	所属子网。	-
私有IP地址	选择所属子网时，不勾选“自动分配IPv4地址”，需要输入相应的IP。	192.168.0.2

参数	说明	取值样例
弹性公网IP	负载均衡器绑定EIP后可以接收来自公网的访问请求并自动分发到多台后端服务器。 您可以选择使用已有的EIP，或者创建新的EIP。 您可以根据实际情况选择以下方式： <ul style="list-style-type: none"><li>● 新创建：新创建一个EIP。</li><li>● 使用已有：使用已有EIP创建负载均衡器，需在页面选择已有EIP。</li></ul>	新创建
弹性公网IP类型	使用新创建弹性公网IP时，选择的EIP的类型。 全动态BGP：可以根据设定的寻路协议实时自动优化网络结构，以保证客户使用的网络持续稳定、高效。	全动态BGP
带宽	设置新创建的EIP带宽大小。	10 Mbit/s
名称	负载均衡器的名称。	elb-ys0
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。	default
描述	可添加负载均衡器相关描述。	-
标签	标签用于标识云资源，可对云资源进行分类和搜索。标签由标签“键”和标签“值”组成，标签键用于标记标签，标签值用于表示具体的标签内容。 命名规格请参照 <a href="#">表2-2</a> 。	<ul style="list-style-type: none"><li>● 键：elb_key1</li><li>● 值：elb-01</li></ul>

表 2-2 负载均衡器标签命名规则

参数	规则	样例
键	<ul style="list-style-type: none"><li>不能为空。</li><li>对于同一负载均衡器键值唯一。</li><li>长度不超过36个字符。</li><li>不能包含非打印字符：“=”，“*”，“&lt;”，“&gt;”，“\”，“，”，“ ”，“/”。</li><li>由英文字母、数字、下划线、中划线、中文字符组成。</li></ul>	elb_key1
值	<ul style="list-style-type: none"><li>长度不超过43个字符。</li><li>不能包含非打印字符：“=”，“*”，“&lt;”，“&gt;”，“\”，“，”，“ ”，“/”。</li><li>由英文字母、数字、下划线、点、中划线、中文字符组成。</li></ul>	elb-01


5. 单击“立即申请”。
6. 确认配置信息，并单击“提交”或“去支付”。

2.4 变更配置

操作场景

当负载均衡器是公网类型时，通过带宽提供负载均衡器和公网之间的访问流量，您可以按照实际需求更改实例的带宽。

操作步骤


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. 选择“服务列表 > 网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，所需修改负载均衡器所在行，单击“修改带宽”。
5. 在“变更规格”区域，选择新的带宽大小，单击“下一步”。
6. 单击“提交”。

2.5 为实例绑定/解绑 EIP

操作场景


您可以为私网类型负载均衡器绑定一个EIP。绑定后，负载均衡器便可以转发来自公网的请求。

## 绑定 EIP

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. 选择“服务列表 > 网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，所需修改负载均衡器所在行，选择“绑定弹性公网IP”。
5. 在“绑定弹性公网IP”弹框中，选择需要绑定EIP，单击“确定”。

也可以进入负载均衡器基本信息页面，在EIP信息处，单击“绑定”，进行EIP设置。

## 解绑 EIP

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. 选择“服务列表 > 网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，所需修改负载均衡器所在行，选择“解绑弹性公网IP”。
5. 单击“是”。

也可以进入负载均衡器基本信息界面，在EIP信息处，单击“解绑”。

## 2.6 删除负载均衡器

### 操作场景

当您确认负载均衡不需要继续使用时，您可以根据需求随时删除负载均衡器。删除弹性负载均衡后无法恢复，请谨慎操作。


删除公网类型负载均衡器时，绑定的EIP不会被默认自动删除，不会影响EIP的正常使用。

### 前提条件

已经删除该负载均衡器配置的以下资源。



- 监听器
- 后端服务器组
- 后端服务器

### 操作步骤

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. 选择“服务列表 > 网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，所需修改负载均衡器所在行，单击“删除”。
5. 单击“是”。

## 导出弹性负载均衡器列表

您也可以选择导出弹性负载均衡器列表，作为本地备份数据查看。

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. 选择“服务列表 > 网络 > 弹性负载均衡”。
4. 在管理控制台的“负载均衡器”界面，单击  导出弹性负载均衡器列表。

# 3 监听器

## 3.1 什么是监听器

创建负载均衡器后，需要为负载均衡器配置监听器。监听器负责监听负载均衡器上的请求，根据配置流量分配策略，分发流量到后端服务器处理。

### 支持的协议类型

负载均衡提供四层协议和七层协议监听，您可根据从客户端到负载均衡器的应用场景选择监听协议，详细说明可参见[表3-1](#)。

表 3-1 监听协议类型说明

协议类型		说明	适用场景
四层协议	TCP	<ul style="list-style-type: none"><li>基于源地址的会话保持。</li><li>数据传输快。</li></ul>	<ul style="list-style-type: none"><li>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。</li><li>对性能和并发规模有要求的Web应用。</li></ul>
四层协议	UDP	<ul style="list-style-type: none"><li>可靠性相对低</li><li>数据传输快</li></ul>	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。
七层协议	HTTP	<ul style="list-style-type: none"><li>基于Cookie的会话保持。</li><li>使用X-Forward-For获取源地址。</li></ul>	需要对数据进行识别的应用，如Web应用、移动游戏等。

协议类型		说明	适用场景
七层协议	HTTPS	<ul style="list-style-type: none"><li>加密传输数据，可以阻止未经授权的访问。</li><li>加解密操作在负载均衡器上完成，可减少后端的处理负载。</li></ul>	需要加密传输的应用。

## 3.2 协议和端口

### 前端协议和端口

前端协议和端口即是负载均衡器提供服务时接收请求的端口。负载均衡系统支持四层（TCP、UDP）和七层（HTTP、HTTPS）协议的负载均衡，可通过具体提供的服务能力选择对应的协议以及该协议对外呈现的端口。

前端协议	前端端口
TCP	在同一个负载均衡实例内，相同协议的前端端口不可以重复，UDP协议可以和其他协议的前端端口可以重复。但是其他的协议间的端口不能重复。取值范围：1-65535。 常用取值示例： TCP/80 HTTPS/443
UDP	
HTTP	
HTTPS	

### 后端协议和端口

后端协议和端口即是后端云服务器自身提供的网络服务的协议以及协议的端口，如使用Windows操作系统上安装的IIS（webservice），该服务默认的协议为HTTP，端口为80。

表 3-2 后端协议和端口说明

后端协议	后端端口
TCP	在同一个负载均衡实例内，后端端口可以重复，取值范围：1-65535。 常用取值示例： TCP/80 HTTP/443
UDP	
HTTP	



### 3.3 创建监听器

#### 操作场景

创建负载均衡器后，需要为负载均衡器配置监听。监听器是使用前端（从客户端到负载均衡器）连接的协议和端口配置监听器，用于检查连接请求的进程。

监听器将根据健康检查的配置自动检查其后端云服务器的运行状况。如果发现某台云服务器运行不正常，则会停止向该云服务器发送流量，并重新将流量发送至正常运行的云服务器。

#### 添加监听器


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. 选择“服务列表 > 网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要添加监听器的负载均衡名称。
5. 切换到“监听器”页签，单击“添加监听器”。配置参数参见[表3-3](#)，[表3-4](#)和[表3-5](#)。

表 3-3 负载均衡配置监听器参数说明

参数	说明	示例
名称	监听器名称。	listener-pnqy
前端协议/端口	负载分发的协议和端口。 支持以下协议，端口取值范围[1-65535]。 <ul style="list-style-type: none"><li>• HTTP</li><li>• TCP</li><li>• HTTPS</li><li>• UDP</li></ul>	HTTP/80
重定向	协议类型为HTTP时，可根据需要设置该项。需要保证业务建立安全连接时，若同时创建了HTTPS和HTTP监听器，可以通过重定向功能，将HTTP访问重定向至HTTPS。 HTTP监听器被重定向后，后端服务器会返回301返回码。	-
重定向至	选择需要重定向HTTPS监听器的名称。	-
服务器证书	协议类型为HTTPS时，需使用证书。	-
高级配置		

参数	说明	示例
HTTP/2	协议类型为HTTPS时,可选择是否支持该协议类型。	-
双向认证	用户需要在HTTPS监听上同时绑定服务器证书与CA证书,才能进行服务端与客户端的双向认证。	-
CA证书	协议类型为HTTPS时,需使用证书。且双向认证开关打开时为必选参数。	-
描述	对于监听器描述。	-

表 3-4 负载均衡配置后端服务器组参数说明

参数	说明	示例
后端服务器组	把具有相同特性的后端服务器放在一个组。 <ul style="list-style-type: none"><li>• 新创建</li><li>• 使用已有</li></ul>	新创建
名称	后端服务器组名称。	server_group-sq4v
后端协议	云服务器开通的协议。	HTTP
分配策略类型	负载均衡采用的算法。 <ul style="list-style-type: none"><li>• 加权轮询算法：按顺序依次将请求分发给不同的服务器。它用相应的权重表示服务器的处理性能，按照权重的高低以及轮询方式将请求分配给各服务器，相同权重的服务器处理相同数目的连接数。</li><li>• 加权最少连接：通过当前活跃的连接数来估计服务器负载情况的一种动态调度算法。</li><li>• 源IP算法：将请求的源IP地址作为散列键（HashKey），从静态分配的散列表找出对应的服务器。</li></ul> <b>说明</b> 用户可以根据自身需求选择相应的算法来分配用户访问流量，提升负载均衡能力。	加权轮询算法

参数	说明	示例
会话保持	开启会话保持后，弹性负载均衡将属于同一个会话的请求都转发到同一个进行处理。 <b>说明</b> 对于HTTP、HTTPS类型的监听器，变更会话保持的状态可能会导致本监听器访问出现秒级中断。	-
会话保持类型	会话保持的方式包括： <ul style="list-style-type: none"><li>源IP地址：将请求的源IP地址作为散列键（HashKey），从静态分配的散列表找出对应的服务器。</li><li>负载均衡器cookie：负载均衡器会根据客户端第一个请求生成一个cookie，后续所有包含这个cookie值的请求都会由同一个后端服务器处理。</li><li>应用程序cookie：该选项依赖于后端应用。后端应用生成一个cookie值，后续所有包含这个cookie值的请求都会由同一个后端服务器处理。</li></ul> <b>说明</b> <ul style="list-style-type: none"><li>TCP协议仅支持源IP地址类型。HTTP协议和https协议支持HTTP cookie和应用程序 cookie类型。用户可根据自身需求选择相应的会话保持方式来分配用户访问流量，提升负载均衡能力。</li><li>四层会话保持时间限制1分钟，七层会话保持时间限制24小时。</li></ul>	源IP地址
cookie名称	当会话保持选择应用程序cookie时，需要填写cookie名称。	cookieName-qsps
会话保持时间（分钟）	当会话保持开启时，需添加会话保持时间。取值范围[1，60]。	20
描述	后端服务器组的描述	-

表 3-5 负载均衡配置健康检查参数说明

参数	说明	示例
是否开启	开启或者关闭健康检查。	-

参数	说明	示例
协议	<ul style="list-style-type: none"><li>健康检查支持TCP和HTTP方式，设置后不可修改。</li><li>当前端协议选择UDP，健康检查协议默认为UDP。</li></ul>	HTTP
域名	健康检查的请求域名。默认值为空，由数字、字母、‘-’、‘.’组成的字符串，只能以数字或字符开头。只有健康检查协议为HTTP时，需要设置。	www.elb.com
端口	健康检查端口号，取值范围[1, 65535]，为可选参数。 <b>说明</b> 未配置健康检查端口时，默认使用后端云服务器端口进行健康检查。配置后，使用配置的健康检查端口进行健康检查。	80
高级配置	分为默认设置和自定义设置。	默认设置
检查周期（秒）	每次健康检查响应的最大间隔时间。 取值范围[1-50]。	5
超时时间（秒）	每次健康检查响应的最大超时时间。取值范围[1-50]。	10
检查路径	指定健康检查的URL地址的路径。当“协议”为HTTP时生效。检查路径只能以/开头，长度范围[1-80]。	/index.html
最大重试次数	健康检查最大的重试次数，取值范围[1-10]。	3

- 单击“完成”。
- 配置完成，单击“确定”。

## 3.4 流量分配策略

负载均衡算法，支持以下三种调度算法：

- 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。它用相应的权重表示服务器的处理性能，按照权重的高低以及轮询方式将请求分配给各服务器，相同权重的服务器处理相同数目的连接数。常用于短连接服务，例如HTTP等服务。
- 加权最少连接：最少连接是通过当前活跃的连接数来估计服务器负载情况的一种动态调度算法。加权最少连接就是在最少连接数的基础上，根据服务器的不同处理能力，给每个服务器分配不同的权重，使其能够接受相应权值数的服务请求。常用于长连接服务，例如数据库连接等服务。


- 源IP算法：将请求的源IP地址进行Hash运算，得到一个具体的数值，同时对后端服务器进行编号，按照运算结果将请求分发到对应编号的服务器上。这可以使得对不同源IP的访问进行负载分发，同时使得同一个客户端IP的请求始终被派发至某特定的服务器。该方式适合负载均衡无cookie功能的TCP协议。

## 权重设置

每台后端服务器的权重取值范围为[0, 100]。新的请求不会转发到权重为0的后端服务器上，此时健康检查状态没有参考意义。以下三种算法支持权重设置。

- 在加权轮询算法中，每台后端服务器的权重取值范围为[0, 100]。新的请求不会转发到权重为0的后端。在非0的权重下，负载均衡器会将请求按权重值的大小分配给所有的后端服务器。当后端服务器的权重都设置为相等时，权重属性将不再生效，负载均衡器将按照简单的轮询策略分发请求。
- 在加权最少连接算法中，每台后端服务器的权重取值范围为[0, 100]。新的请求不会转发到权重为0的后端。在非0的权重下，负载均衡器会通过  $\text{overhead} = \text{当前连接数} / \text{权重}$  来计算每个服务器负载。每次调度会选择overhead最小的后端服务器。
- 在源IP算法中，每台后端服务器的权重取值范围为[0, 100]，但是只做0和非0的区分。新的请求不会转发到权重为0的后端。在非0的权重下，由于使用了源IP算法，各个后端服务器的权重属性将不再生效，在一段时间内，同一个客户端的IP地址的请求会被调度至同一个后端服务器上。

权重设置步骤如下：

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. 选择“服务列表 > 网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要修改后端服务器权重的负载均衡名称。
5. 在该负载均衡界面，切换到“后端服务器组”页签，在目标服务器所在行的操作列中，编辑“权重”列，设置需要权重值。
6. 单击“确定”。

## 3.5 会话保持

会话保持就是指在负载均衡器上有这么一种机制，可以识别客户与服务器之间交互过程的关联性，在作负载均衡的同时，还保证一系列相关联的访问请求会保持分配到同一台服务器上。

会话保持有什么作用呢，举例说明一下：如果有一个用户在服务器甲登录了，访问请求被分配到服务器甲，在很短的时间，这个用户又发出了一个请求，如果没有会话保持功能的话，这个用户的请求很有可能会被分配到服务器乙去，这个时候在服务器乙上是没有登录的，所以你要重新登录，但是用户并不知道自己的请求被分配到了哪里，用户的感受就是登录了，怎么又要登录，用户体验很不好。如果配置了会话保持功能，所有这一系列的操作过程都由同一台服务器完成，而不能被负载均衡器分配到不同的服务器上。

### 四层会话保持

四层协议的会话保持支持基于源IP地址的简单会话保持，即来自同一IP地址的访问请求会转发到同一台后端服务器上进行处理。

四层会话保持失效的场景如下：

- 客户端的源IP地址发生变化。
- 客户端访问请求超过会话保持时间。

#### 说明

- 当创建四层协议监听器，分配策略类型选择“加权轮询算法”，可配置会话保持时间。
- 四层会话保持时间默认为20分钟，最长为1小时。

## 七层会话保持

七层协议的会话保持支持HTTP cookie和应用程序cookie的会话保持。用户可根据自身需求选择相应的会话保持方式来分配用户访问流量，提升负载均衡能力。

- HTTP cookie：负载均衡器会根据客户端第一个请求生成一个cookie，后续所有包含这个cookie值的请求都会由同一个后端服务器处理。
- 应用程序cookie：该选项依赖于后端应用。后端应用生成一个cookie值，后续所有包含这个cookie值的请求都会由同一个后端服务器处理。

七层会话保持失效的场景如下：



- 如果客户端发送请求未附带cookie，则会话保持无法生效。
- 客户端访问请求超过会话保持时间。

#### 说明

- 当创建七层协议监听器，分配策略类型选择“加权轮询算法”，可配置会话保持时间。
- 七层会话保持时间默认为20分钟，最长为24小时。

负载均衡器支持源IP、负载均衡器cookie、应用程序cookie三种会话保持类型。

## 配置会话保持

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. 选择“服务列表 > 网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要配置会话保持的负载均衡名称。
5. 在该负载均衡界面的“后端服务器组”页签，单击需要配置会话保持的后端服务器组名称右侧的。
6. 开启会话保持功能，配置会话保持类型以及会话保持时间参数。
7. 单击“确定”。

## 3.6 访问控制策略

负载均衡器用户可以通过添加白名单的方式控制访问负载均衡监听器的IP，能够设置允许特定IP访问，而其他IP不许访问。

须知

- 设置白名单是负载均衡的功能，设置白名单存在一定业务风险。一旦设置白名单，就只有白名单中的IP可以访问负载均衡监听。
- 如开启访问控制而不设置白名单列表，则这个负载均衡监听就无人可以访问。
- 访问流量的IP先通过白名单访问控制，然后负载均衡转发流量，通过安全组安全规则限制，所以安全组的规则设置是不会影响负载均衡的白名单设置访问控制。

添加白名单


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. 选择“服务列表 > 网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击负载均衡名称，进入监听器管理界面。
5. 在需要添加白名单的监听器的基本信息页面，单击访问控制右侧“设置”按钮，如表3-6所示配置白名单。

表 3-6 参数配置

参数	说明	样例
访问控制开关	开启 <ul style="list-style-type: none"><li>● 开启访问控制开关而不设置白名单列表，表示不允许任何IP访问负载均衡监听器。</li><li>● 开启访问控制开关且在白名单列表中设置了IP，表示允许该IP访问负载均衡监听器。</li></ul> 关闭 <ul style="list-style-type: none"><li>● 关闭访问控制开关，表示允许任何IP访问负载均衡监听器。</li></ul>	-
白名单	允许能够访问负载均衡的监听器的IP或网段。 说明 <ul style="list-style-type: none"><li>● 多个IP或网段间用逗号隔开，最多可以输入300个IP或网段。</li><li>● 白名单列表中不支持IPv6类型的IP地址。</li></ul>	10.168.2.24, 10.168.16.0/24



6. 配置完成，点击“确定”。

## 3.7 修改监听器


### 操作场景

如果您已创建监听器，您可以根据实际业务需求，可以修改或者删除监听器。


### 修改监听器

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. 选择“服务列表 > 网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要修改监听器的负载均衡名称。
5. 切换到“监听器”页签，单击需要修改的监听器名称右侧的.
6. 修改参数，单击“确定”。

### 删除监听器

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. 选择“服务列表 > 网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要删除监听器的负载均衡名称。

#### 说明

- 如果该监听器下有后端服务器，删除监听器之前需移除服务器。
  - 如果HTTP设置了重定向至HTTPS，删除HTTPS监听器之前需删除HTTPS重定向规则。
  - 删除监听器后会同时删除所绑定的后端服务器组。
5. 切换到“监听器”页签，单击需要删除的监听器名称右侧的.
  6. 单击“是”。

## 3.8 HTTP/HTTPS 高级配置

### 3.8.1 转发策略

### 操作场景

负载均衡用户可以通过添加转发策略支持自行设定的域名和URL，将来自不同域名或者不同URL的请求转发到不同的后端服务器组处理。此功能目前仅支持协议类型为HTTP、HTTPS的监听器。

一个监听器最多可添加500条转发策略，您可以将视频、图片、音频、文本等请求分别转发到不同的后端服务器组上去处理，便于灵活的分流业务，合理的分配资源。

配置转发策略时，请注意以下事项：



- 每个URL路径需要存于后端服务器，否则后端服务器会返回404。
- 不能配置转发策略完全一样的两条路径。
- 因为正则匹配采用顺序匹配的方式，只要任意规则匹配成功就结束匹配。所以配置“URL匹配规则”为“正则匹配”的多个匹配规则时，规则之间不能重叠。

在添加了转发策略后，负载均衡器将按以下规则转发前端请求：

- 如果能匹配到监听器的转发策略，则按该转发策略将请求转发到对应的后端服务器组。
- 如果不能匹配到监听器的转发策略，则将请求转发到监听器对应的后端服务器组。

添加转发策略


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. 选择“服务列表 > 网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要添加转发策略的负载均衡器名称。
5. 切换到监听器页签，单击目标监听器名称。
6. 单击“转发策略”右侧的“添加”按钮。
7. 在“添加转发策略”弹框中参考表3-7配置参数。
8. 配置完成，单击“确定”。  
也可在负载均衡器页面单击目标监听器名称，跳转至监听器页面，添加转发策略。

表 3-7 添加转发策略的参数

配置类型	参数	说明	样例
配置转发策略	名称	转发策略的名称。	forwarding_policy-q582
	域名	触发转发的域名，仅支持精确域名。注意，域名或者URL至少要指定一个。	www.test.com
	URL	触发转发的URL。	/login.php

配置类型	参数	说明	样例
	URL匹配规则	<ul style="list-style-type: none"><li>精确匹配 请求的URL和设定URL完全一致。</li><li>前缀匹配 请求的URL匹配以设定URL开头的URL。</li><li>正则匹配 请求的URL和设定的URL正则表达式匹配。</li></ul> <b>说明</b> 匹配的优先级为： 精确匹配>前缀匹配>正则匹配	精确匹配
	描述	转发策略的描述。	-
添加后端服务器组	后端服务器组	可选择“新创建”或“使用已有”。选择“新创建”，可参考表4-1和表4-2进行参数配置。选择“使用已有”，为转发策略选择已有的后端服务器组即可。 <b>说明</b> 后端协议只能选择HTTP。	新创建

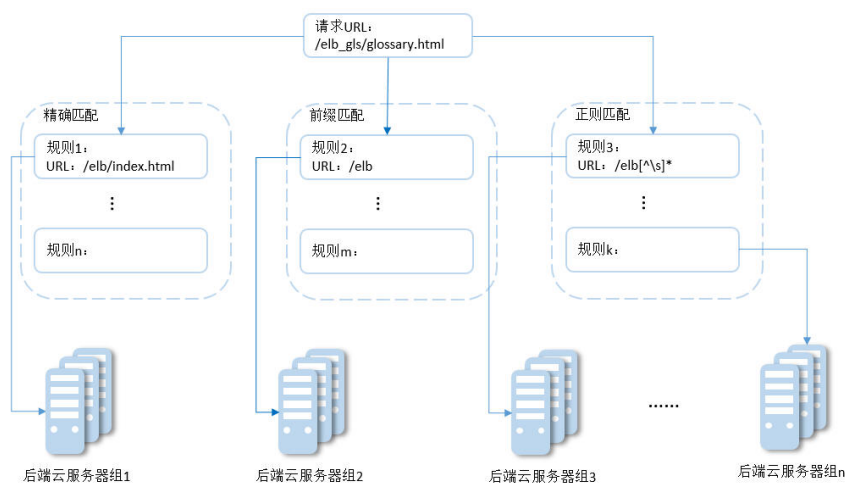
URL 匹配示例

如表3-8所示，是一个URL匹配示例，转发情况如图3-1所示。

表 3-8 URL 匹配示例

模式	请求URL	设定URL			
-	-	/elb/ index.html	/elb	/elb[^\s]*	/ index.html
精确匹配	/elb/ index.html	√	-	-	-
前缀匹配		√	√	-	-
正则匹配		√	-	√	-



图 3-1 转发示例





以上图为例

请求的URL: /elb\_gls/glossary.html先在精确匹配规则中查找，如果没有找到精确匹配的规则，则继续在前缀匹配规则中查找，找到匹配的规则2，将该请求转发到规则2对应的后端服务器组2。此时虽然请求URL和正则匹配规则中的规则3相匹配，但由于前缀匹配的优先级比较高，所以最终将请求转发至后端服务器组2。

## 修改转发策略

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. 选择“服务列表 > 网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要修改转发策略的负载均衡器名称。
5. 切换到监听器页签，单击需要修改转发策略的监听器名称。
6. 单击“转发策略”。
7. 单击目标转发策略名称右侧的.
8. 在弹出的“修改转发策略”对话框中，修改参数，单击“确认”。

## 删除转发策略

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. 选择“服务列表 > 网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要删除转发策略的负载均衡器名称。
5. 切换到监听器页签，单击需要删除转发策略的监听器名称。
6. 单击“转发策略”。
7. 单击目标转发策略名称右侧的.
8. 在弹出的“删除转发策略”对话框中，单击“是”，删除转发策略。

## 3.8.2 HTTPS 双向认证

### 使用场景

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（如银行支付），需要对通信双方的身份都要做认证，即双向认证，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，建议购买权威机构颁发的证书。

### 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 3-2 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 3-3 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]#
```

## 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
```

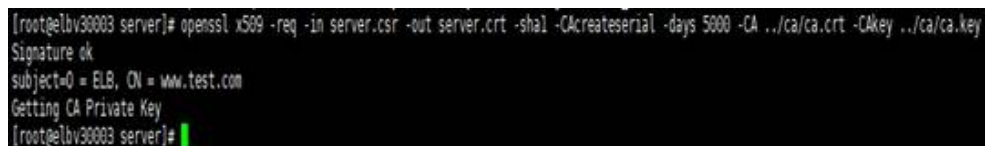
5. 创建服务器证书的csr请求文件server.csr。

```
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 3-4 签发服务器证书



```
[root@elbv30003 server]# openssl x509 -req -in server.csr -out server.crt -sha1 -CAcreateserial -days 5000 -CA ../ca/ca.crt -CAkey ../ca/ca.key
Signature ok
subject=O = ELB, CN = www.test.com
Getting CA Private Key
[root@elbv30003 server]#
```

## 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 3-5 创建客户端证书私钥文件

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

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 3-6 创建客户端证书 csr 文件

```
[root@elbv30003 client]# openssl req -out client.csr -key client.key -new -config ./client_cert.conf
```

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 3-7 签发客户端证书

```
[root@elbv30003 client]# openssl x509 -req -in client.csr -out client.crt -sha1 -CAcreateserial -days 5000 -CA ../ca/ca.crt -CAkey ../ca/ca.key
Signature ok
subject=O = ELB, CN = www.test.com
Getting CA Private Key
[root@elbv30003 client]#
```

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。

## 配置服务器证书和私钥

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，点击“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。

## 配置 CA 证书

**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[使用CA证书签发服务器证书](#)创建的客户端CA证书ca.crt的内容复制到证书内容区域，点击“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

CA证书内容只支持上传pem格式。

----结束

## 配置 HTTPS 双向认证

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”，打开双向认证开关，并且在证书和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。

### 添加后端服务器

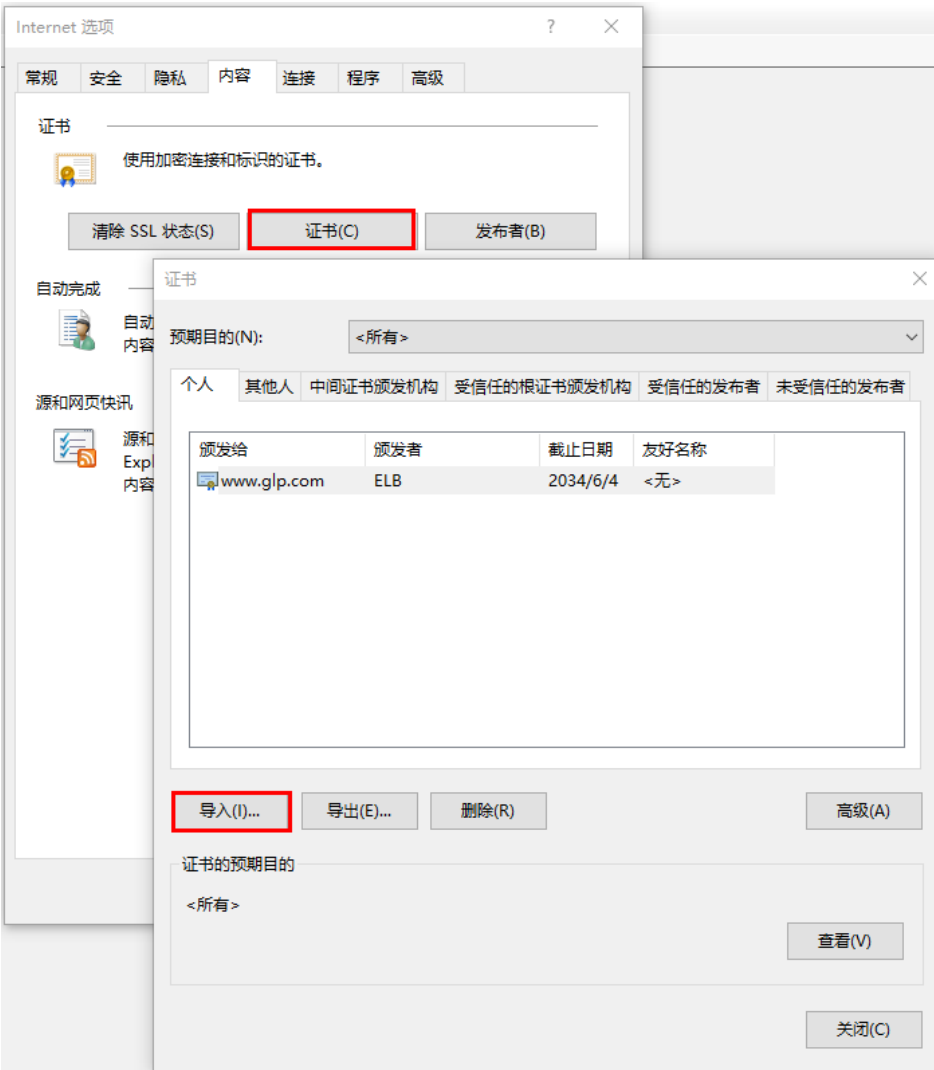
请参考[添加后端服务器](#)相关操作指导，此处不展开描述。

## 导入客户端证书并测试

### 浏览器方式功能测试

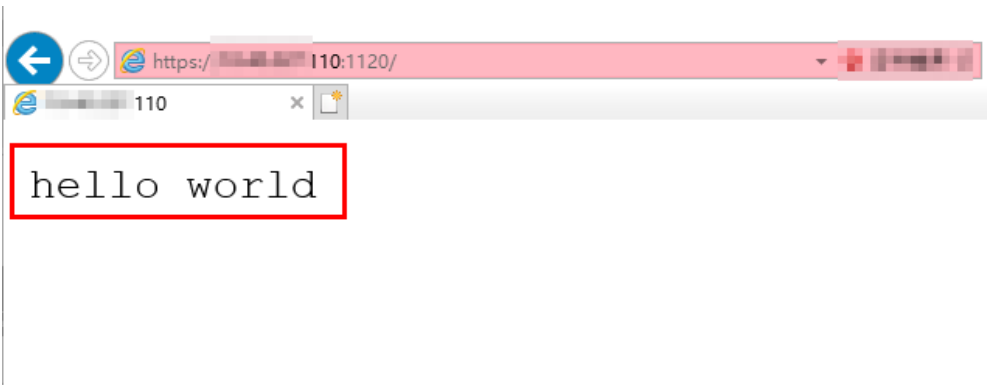
1. 浏览器导入客户端证书（以Internet Explorer 11为例说明）
  - a. 把客户端证书从Linux机器导出来，即前面签发的client.p12证书文件。
  - b. 单击“设置 > Internet选项”，切换到“内容”页签。
  - c. 单击“证书”，然后单击“导入”，导入client.p12证书文件。

图 3-8 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 3-9 正常访问网站



Curl工具方式功能测试



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3-10**说明验证成功。

图 3-10 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
```

## 3.8.3 HTTP/2

### 操作场景

HTTP/2，即超文本传输协议 2.0，是下一代HTTP协议。如果您需要保证HTTPS业务更加安全，可以在配置HTTPS监听器时，开启HTTP/2功能。如果您已创建了HTTPS监听器，可以在已创建的HTTPS监听器中开启或者关闭支持HTTP/2功能。


### 开启 HTTPS 监听器的 HTTP/2 功能

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. 选择“服务列表 > 网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要开启HTTP/2功能的监听器的负载均衡器名称。
5. 在该负载均衡器界面的“监听器”页签，单击“添加监听器”。
6. 在“添加监听器”界面，展开高级配置，打开HTTP/2功能。
7. 配置完成，单击“确定”。

#### 说明

只有HTTPS监听器可以开启或关闭HTTP/2功能。

### 修改 HTTPS 监听器的 HTTP/2 功能

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. 选择“服务列表 > 网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要修改HTTP/2功能的负载均衡器名称。
5. 切换“监听器”页签，在需要修改HTTP/2功能开关的监听器名称所在行，单击修改操作键。

6. 在“修改监听器”界面，展开高级配置，开启或者关闭HTTP/2功能。
7. 确认正确，单击“确认”。

### 3.8.4 HTTP 重定向至 HTTPS

#### 操作场景

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HTTP访问重定向至HTTPS。

该功能可以满足您如下需求，PC、手机浏览器等以HTTP请求访问Web服务，配置了HTTP访问重定向至HTTPS后，后端服务器返回HTTPS的响应。默认强制以HTTPS访问网页。

#### 前提条件

- 已经创建HTTPS监听器
- 已经创建HTTP监听器

#### 添加重定向


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. 选择“服务列表 > 网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要重定向的HTTP监听器的负载均衡名称。
5. 在该负载均衡界面的“监听器”页签，单击需要重定向的HTTP监听器名称。
6. 选择“重定向 > 添加”，选择需要重定向至HTTPS监听器的名称。

表 3-9 重定向参配置参数

参数	说明	样例
名称	重定向的名称。	redirect-g8h9
重定向至	选择需要重定向HTTPS监听器的名称。	-
描述	重定向的描述。	-

7. 在确认对话框单击“确定”。

#### 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，后端服务器会返回301返回码。

#### 修改重定向

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. 选择“服务列表 > 网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要重定向的HTTP监听器的负载均衡名称。
5. 在该负载均衡界面的“监听器”页签，单击需要重定向的HTTP监听器名称。
6. 选择“重定向 > 修改”，选择需要重定向至HTTPS监听器的名称。
7. 在确认对话框单击“确定”。

## 删除重定向

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. 选择“服务列表 > 网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击已经重定向的HTTP监听器的负载均衡名称。
5. 在该负载均衡界面的“监听器”页签，单击已经重定向的HTTP监听器名称。
6. 选择“重定向 > 删除”。
7. 在确认对话框单击“是”。

## 3.8.5 配置 SNI

### 操作场景

如果用户的后台应用对外提供多个域名的访问，并且每个域名都使用独立的证书，则需要创建HTTPS监听器时开启SNI功能。SNI（Server Name Indication）是为了解决一个服务器使用多个域名和证书的TLS扩展，主要解决一台服务器只能使用一个证书的缺点。开启SNI后，允许客户端在发起SSL握手请求时就提交请求的域名信息，负载均衡收到SSL请求后，会根据域名去查找证书，如果找到域名对应的证书，则返回该证书；如果没有找到域名对应的证书，则返回缺省证书。负载均衡在配置HTTPS 监听器支持此功能，即支持绑定多个证书。


### 前提条件

已经创建证书，具体步骤可参照[创建证书](#)。

#### 说明

用于SNI的证书，需要指定域名，每个证书只能指定一个域名。

### 操作步骤

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. 选择“服务列表 > 网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击负载均衡名称。
5. 切换到“监听器”页签，在需要添加SNI的监听器的基本信息页面，单击SNI右侧“配置”。
6. 开启SNI的开关，选择需要配置的SNI证书。
7. 单击“确定”。

# 4 后端服务器

## 4.1 后端服务器介绍

负载均衡器会将客户端的请求转发给后端服务器处理。例如，您可以添加ECS实例作为负载均衡器的后端服务器，监听器使用您配置的协议和端口检查来自客户端的连接请求，并根据您定义的分配策略将请求转发到后端服务器组里的后端云服务器。

新添加后端服务器后，若健康检查开启，负载均衡器会向后端服务器发送请求以检测其运行状态，响应正常则直接上线，响应异常则开始健康检查机制定期检查，检查正常后上线。

您可以随时增加或减少负载均衡器的后端服务器数量，保证应用业务稳定和可靠，屏蔽单点故障，您可以在负载均衡器所在地域内的可用区中，绑定后端服务器实例，并且确保至少有一台后端服务器在正常运行。

### 注意事项

绑定后端服务器时，请注意以下事项：

- 确保后端服务器和负载均衡器属于同一个VPC。
- 建议您选择相同操作系统的后端服务器，以便日后管理和维护。
- 您可以设置后端服务器组内各后端服务器的转发权重。权重越高的后端服务器将被分配到更多的访问请求。
- 如果您开启了会话保持功能，那么有可能会造成后端服务器的访问量不均衡。如果出现了访问不均衡的情况，建议您暂时关闭会话保持功能，观察一下是否依然存在这种情况。


## 4.2 后端服务器配置安全组

### 操作场景

由于ELB流量转到后端服务器以后，源IP会被转换为100.125的IP，所以添加后端服务器之前首先要检查后端服务器所在安全组规则是否配置放行100.125.0.0/16网段，并配置ELB用于健康检查的协议和端口，如果健康检查使用UDP协议，则还需要配置安全组规则放行ICMP协议，否则无法对已添加的后端服务器执行健康检查。

首次创建后端服务器时，如果用户未配置过VPC，系统将会创建默认VPC。由于默认VPC的安全组策略为组内互通、禁止外部访问，即外部网络无法访问后端服务器，为了确保负载均衡器可同时在监听器端口和健康检查端口上与已创建后端服务器的进行通信，就需要配置安全组入方向的访问规则。

## 配置安全组规则


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. 选择“计算 > 弹性云服务器”。
4. 在弹性云服务器列表，单击待变更安全组规则的名称。  
系统跳转至该详情页面。
5. 选择“安全组”页签，单击安全组名称，查看安全组规则。
6. 单击“ID”或者“更改安全组规则”，系统自动跳转至安全组界面。
7. 在入方向规则页签，单击“添加规则”，配置安全组入方向的访问规则。  
如果是TCP，HTTP或者HTTPS监听器：
  - 若配置了不同于后端服务器端口的健康检查端口，放通TCP协议，端口和ELB健康检查端口一致。
  - 若采用默认的健康检查方式，放通TCP协议，端口和后端服务器端口一致。
  - 安全组规则必须放通100.125.0.0/16网段，否则会导致健康检查异常。如果UDP监听器：
  - 若配置了不同于后端服务器端口的健康检查端口，放通UDP协议，端口和ELB健康检查端口一致。
  - 若采用默认的健康检查方式，放通UDP协议，端口和后端服务器端口一致。
  - 安全组规则必须放通100.125.0.0/16网段，否则会导致健康检查异常。
  - 放通ICMP协议。
8. 单击“确定”，完成安全组规则配置。

## 配置网络 ACL 规则

网络ACL是一个子网级别的可选安全层，通过与子网关联的出方向/入方向规则控制出入子网的数据流。网络ACL与安全组类似，都是安全防护策略，当您想增加额外的安全防护层时，就可以启用网络ACL。但是网络ACL默认规则会拒绝所有入站和出站流量，如果此网络ACL和负载均衡所属同一个子网，或者此网络ACL和负载均衡相关联的后端服务器所属同一个子网那么负载均衡的业务也会受到影响，收不到来自于公网或者私网的任何请求流量，或者会导致后端服务器异常。

您可以通过配置网络ACL入方向规则，放行100.125.0.0/16网段。

由于ELB会将访问后端服务器的公网IP转换为内部的100.125.0.0/16网段的IP地址，所以无法通过配置网络ACL规则来限制公网IP访问后端服务器。

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. 在系统首页，选择“网络 > 虚拟私有云”。
4. 在左侧导航栏选择“访问控制 > 网络ACL”。

5. 在“网络ACL”列表区域，选择网络ACL的名称列，单击您需要修改的“网络ACL名称”进入网络ACL详情页面。
6. 在入方向规则或出方向规则页签，单击“添加规则”，添加入方向或出方向规则。
  - 策略：选择允许。
  - 协议：和监听器协议一致。
  - 源地址：此方向允许的源地址，填写100.125.0.0/16。
  - 源端口范围：选择业务所在端口范围。
  - 目的地址：此方向允许的目的地址。选择默认值为0.0.0.0/0，代表支持所有的IP地址。
  - 目的端口范围：选择业务所在端口范围。
  - 描述：网络ACL规则的描述信息，非必填项。
7. 单击“确定”。

## 4.3 添加或移除后端服务器


### 操作场景

在使用负载均衡服务时，确保至少有一台后端服务器在正常运行，可以接收负载均衡转发的客户端请求。如果请求的需求流量上升，用户需要向负载均衡器添加更多后端服务器处理需求。

移除负载均衡器绑定的后端服务器，后端服务器将不再收到负载均衡器转发的需求，但不会对服务器本身产生任何影响，只是解除了后端服务器和负载均衡器的关联关系。您可以在业务增长或者需要增强可靠性时再次将它添加至后端服务器组中。

如果负载均衡器与某个弹性伸缩组关联，则该弹性伸缩组中的实例会自动添加至负载均衡后端实例，从弹性伸缩组移除的服务器实例会自动从负载均衡后端服务器中删除。

### 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. 选择“服务列表 > 网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要添加后端服务器的负载均衡名称。
5. 切换到“后端服务器组”页签，单击目标后端服务器组名称。
6. 在目标后端服务器组的基本信息页面，单击“添加”。选择后端云服务器所在的子网，勾选需要添加的后端服务器，单击“下一步”。

#### 说明

如果服务器有多张网卡时，只能选择主网卡所在的子网，通过主网卡添加后端服务器。


7. 设置业务端口和服务器的权重，单击“确定”。

#### 说明

在“添加端口”处依次填写每台后端服务器的业务端口。如果多台后端服务器的业务端口相同，可以在“批量添加端口”处批量填写业务端口并单击“确定”。

8. 单击“确定”，完成添加。

移除后端服务器

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. 选择“服务列表 > 网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要移除后端服务器的负载均衡名称。
5. 切换到“后端服务器组”页签，单击需移除的服务器所在后端服务器组的名称。
6. 在该后端服务器组的基本信息页面，需移除单个后端服务器，可单击目标后端服务器操作列的“移除”；如需移除多个后端服务器，可勾选所有需要移除的服务器，单击服务器列表上方的“移除”。
7. 在“移除后端服务器”对话框中单击“是”。

添加后端服务器组


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. 选择“服务列表 > 网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要添加后端服务器组的负载均衡名称。
5. 切换到“后端服务器组”页签，单击“添加后端服务器组”。
6. 在弹出的“添加后端服务器组”对话框中配置相关参数。  
参数配置请参见[表4-1](#)和[表4-2](#)。

表 4-1 负载均衡配置后端服务器组参数说明

参数	说明	示例
名称	后端服务器组名称。	server_group-sq4v
后端协议	云服务开通的协议。	HTTP

参数	说明	示例
分配策略类型	<p>负载均衡采用的算法。</p> <ul style="list-style-type: none"><li>• 加权轮询算法：根据服务器的权重，按顺序依次将请求分发给不同的服务器。它用相应的权重表示服务器的处理性能，按照权重的高低以及轮询方式将请求分配给各服务器，相同权重的服务器处理相同数目的连接数。</li><li>• 加权最少连接：最少连接是通过当前活跃的连接数来估计服务器负载情况的一种动态调度算法。加权最少连接就是在最少连接数的基础上，根据服务器的不同处理能力，给每个服务器分配不同的权重，使其能够接受相应权值数的服务请求。</li><li>• 源IP算法：相同的源IP地址的请求始终被分发到相同的服务器处理。</li></ul> <p><b>说明</b> 用户可以根据自身需求选择相应的算法来分配用户访问流量，提升负载均衡能力。</p>	加权轮询算法
会话保持	<p>开启会话保持后，弹性负载均衡将属于同一个会话的请求都转发到同一个服务器进行处理。</p> <p><b>说明</b> 对于HTTP、HTTPS类型的监听器，变更会话保持的状态可能会导致本监听器访问出现秒级中断。</p>	-



参数	说明	示例
会话保持类型	<p>会话保持的方式包括：</p> <ul style="list-style-type: none"><li>源IP地址：相同的源IP地址的请求始终被分发到相同的后端服务器处理。</li><li>负载均衡器cookie：负载均衡器会根据客户端第一个请求生成一个cookie，后续所有包含这个cookie值的请求都会由同一个后端服务器处理。</li><li>应用程序cookie：该选项依赖于后端应用。后端应用生成一个cookie值，后续所有包含这个cookie值的请求都会由同一个后端服务器处理。</li></ul> <p><b>说明</b></p> <ul style="list-style-type: none"><li>TCP协议仅支持源IP地址类型。HTTP协议和https协议支持负载均衡器cookie和应用程序 cookie类型。用户可根据自身需求选择相应的会话保持方式来分配用户访问流量，提升负载均衡能力。</li><li>四层会话保持时间限制1分钟，七层会话保持时间限制24小时。</li></ul>	应用程序cookie
cookie名称	当会话保持选择应用程序cookie时，需要填写cookie名称。	cookieName-qsp
会话保持时间（分钟）	当会话保持开启时，需添加会话保持时间。取值范围[1，60]。	20
描述	后端服务器组的描述	-



表 4-2 负载均衡配置健康检查参数说明

参数	说明	示例
是否开启	开启或者关闭健康检查。	-
协议	<ul style="list-style-type: none"><li>当前端协议选择TCP, HTTP或者HTTPS，健康检查支持TCP和HTTP方式，设置后不可修改。</li><li>当前端协议选择UDP，健康检查协议默认为UDP。</li></ul>	HTTP
域名	健康检查的请求域名。默认值为空，由数字、字母、‘-’、‘.’组成的字符串，只能以数字或字母开头。只有健康检查协议为HTTP时，需要设置。	www.elb.com



参数	说明	示例
端口	健康检查服务访问后端时的探测端口。取值范围[1, 65535]，为可选参数。 <b>说明</b> 未配置健康检查端口时，默认使用后端服务器端口进行健康检查。配置后，使用配置的健康检查端口进行健康检查。	80
高级配置	分为默认设置和自定义设置。	默认设置
检查周期 (秒)	每次健康检查响应的最大间隔时间。取值范围[1-50]。	5
超时时间 (秒)	每次健康检查响应的最大超时时间。取值范围[1-50]。	10
检查路径	指定健康检查的URL地址的路径。当“协议”为HTTP时生效。检查路径只能以/开头，长度范围[1-80]。	/index.html
最大重试次数	健康检查最大的重试次数，取值范围[1-10]。	3

7. 单击“确定”。

## 修改后端服务器组

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. 选择“服务列表 > 网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要修改的后端服务器组的负载均衡名称。
5. 切换到“后端服务器组”页签，单击需要修改的后端服务器组名称右侧的。
6. 修改参数，单击“确定”。

## 删除后端服务器组

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. 选择“服务列表 > 网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要删除的后端服务器组的负载均衡名称。
5. 切换到“后端服务器组”页签，单击需要删除的后端服务器组名称右侧的。
6. 单击“是”。

# 5 健康检查

## 5.1 配置健康检查

### 操作场景

您可以在添加监听器时配置健康检查。通常，使用默认的健康检查配置即可。

### 背景信息

- 健康检查与ELB的后端协议是两个相互独立的能力，所以健康检查协议可以与ELB的后端协议相同，也可以不同。
- 为了减少后端服务器的CPU占用，建议您使用TCP协议做健康检查。如果您希望使用HTTP健康检查协议，建议使用HTTP+静态文件的方式。
- 通过增加“检查间隔”，可以降低健康检查的检测频率。

### 操作步骤


- 登录管理控制台。
- 在管理控制台左上角单击图标，选择区域和项目。
- 选择“服务列表 > 网络 > 弹性负载均衡”。
- 在“负载均衡器”界面，单击需要开启健康检查的负载均衡名称。
- 在“后端服务器组”页签下，选择需要开启健康检查的后端服务器组名称。
- 在基本信息页面，单击“健康检查”右侧的“配置”。
- 在“配置健康检查”界面，可根据需要开启健康检查。参考[表5-1](#)进行配置。

表 5-1 健康检查配置参数说明

参数	说明	示例
是否开启	开启或者关闭健康检查。	-

参数	说明	示例
协议	<ul style="list-style-type: none"><li>健康检查支持TCP和HTTP方式，设置后不可修改。</li><li>当前端协议选择UDP，健康检查协议默认为UDP。</li></ul>	HTTP
域名	健康检查的请求域名。默认值为空，由数字、字母、‘-’、‘.’组成的字符串，只能以数字或字符开头。只有健康检查协议为HTTP时，需要设置。	www.elb.com
端口	健康检查端口号，取值范围[1, 65535]，为可选参数。 <b>说明</b> 未配置健康检查端口时，默认使用后端云服务器端口进行健康检查。配置后，使用配置的健康检查端口进行健康检查。	80
检查间隔（秒）	每次健康检查响应的最大间隔时间。 取值范围[1-50]。	5
超时时间（秒）	每次健康检查响应的最大超时时间。取值范围[1-50]。 <b>说明</b> 超时时间配置应小于等于检查周期，若配置大于检查周期则取检查周期值为超时时间	3
检查路径	指定健康检查的URL地址的路径。当“协议”为HTTP时生效。检查路径只能以/开头，长度范围[1-80]。	/index.html
最大重试次数	健康检查最大的重试次数，取值范围[1-10]。	3

8. 单击“确定”。


## 5.2 关闭健康检查

### 操作场景

如果您不需要四层或七层的健康检查功能，可以在创建监听器或后端服务器组时，不开启健康检查开关。对于已经创建健康检查的后端服务器组，可以在修改健康检查时，选择关闭健康检查开关。

您可以关闭健康检查功能，但关闭健康检查后，后端服务器将不再收到健康检查报文，此时监听器认为后端服务器处理健康状态。当后端某个服务器健康检查出现异常时，负载均衡还是会把请求转发到该异常的后端服务器上，造成部分业务不可访问。在此场景下，需要用户保证主机业务端口正常。所以建议您不要关闭健康检查。

## 操作步骤

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. 选择“服务列表 > 网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要关闭健康检查的负载均衡名称。
5. 在“后端服务器组”页签下，选择需要关闭健康检查的后端服务器组名称。
6. 在基本信息页面，单击“健康检查”右侧的“配置”。
7. 在“配置健康检查”界面，可根据需要关闭健康检查。
8. 单击“确定”。

# 6 证书管理

## 6.1 证书格式

### 证书格式要求

在创建证书时，您可以直接输入证书内容或上传证书文件。

如果是通过根证书机构颁发的证书，您拿到的证书是唯一的一份，不需要额外的证书，配置的站点即可被浏览器等访问设备认为可信。

证书内容格式为：

- 以“-----BEGIN CERTIFICATE-----”作为开头，“-----END CERTIFICATE-----”作为结尾。
- 每行64字符，最后一行不超过64字符。
- 证书之间不能有空行。

示例如下：

```
-----BEGIN CERTIFICATE-----
MIIDljCCAougAwIBAgIJALV96mEtVF4EMA0GCSqGSIb3DQEBBQUAMGoxCzAJBgNV
BAYTAnh4MQswCQYDVQQIEwJ4eDELMAkGA1UEBxMCeHgxGzAJBgNVBAoTAnh4MQsw
CQYDVQQLEwJ4eDELMAkGA1UEAxMCeHgxGjAYBgkqhkiG9w0BCQEWCh4eEAXNjMu
Y29tMB4XDTE3MTExMjYxM1oXDTEwMTExMjYxM1owajELMAkGA1UEBhMC
eHgxGzAJBgNVBAGTAnh4MQswCQYDVQQHEwJ4eDELMAkGA1UEChMCeHgxGzAJBgNV
BAsTAnh4MQswCQYDVQQDEwJ4eDEaMBGCSqGSIb3DQEJARYLeHh4QDE2My5jb20w
gZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMU832iM+d3FILgTWmpZBUoYcIWV
cAAyE7FsZ9LNerOyjlpyi256oydpdV6qPPC7igJjpu4QOI362BrWzJCYQbg4
WpUDqr84V1f9vdQc75v9WoujcnlKszzpV6qePPC7igJjpu4QOI362BrWzJCYQbg4
Uzo1KYBhLFxl0TovAgMBAAGjc8wgcwwHQYDVR0OBBYEFMbTvDyvE2KsRy9zPq/J
WOjovG+WMIGcBgNVHSMegZQwgZGAFMbTvDyvE2KsRy9zPq/JWOjovG+WoW6kbDBq
MQswCQYDVQQGEwJ4eDELMAkGA1UECBMCeHgxGzAJBgNVBACeHh4QDE2My5jb20w
EwJ4eDELMAkGA1UECXMceHgxGzAJBgNVBAMTAnh4MR0wGAYIKoZIhvcNAQkBFgt4
eHhAMTYzLmNvbYIJALV96mEtVF4EMA0GCSqGSIb3DQEJARYLeHh4QDE2My5jb20w
BQADgYEAAsKc/1iwiAla2RU3YCxqZFEsZZvQxikrDkDbFeoa6Tk49Fnb1f7FCW6
PTtY3HPWL5ygsMsSy0Fi3xp3jmulwzJhcQ3tcK5gC99HWp6Kw37RL8WoB8GWFUOQ
4tHLOjBixkZROPRhH+zMlrqUexv6fsb3NWKhnlfh1Mj5wQE4Ldo=
-----END CERTIFICATE-----
```

## 私钥格式要求

在创建服务器证书时，您也需要上传证书的私钥。您可直接输入私钥文件内容或上传符合格式的私钥文件。

需注意必须是无密码的私钥，私钥内容格式为：

- 以“-----BEGIN RSA PRIVATE KEY-----”作为开头，“-----END RSA PRIVATE KEY-----”作为结尾。
- 私钥之间不能有空行，并且每行64字符，最后一行不超过64字符。

示例如下：

```
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQDFPN9ojPndxSC4E1pqWQVKGHCFLXAAGBOxbGfSzXqzsoyacotu
eqMqXQbxrPSQFATeVmhZPNVEMdvcAMjYsV/mymtAwVqVA6q/OfdX/b3UHO+b/VqL
o3J5SrM86Veqnjzwu4oCSabuEDiN+tga1syQmEG4OFM6NSmAYSxcZdE6LwIDAQAB
AoGBAJvLzJCylsCjCKHWL6onbSUTDtyFwPViD1QrVatQYabF14g8CGUZG/9fgheu
TXPtTDcvu7cZdUArvgYW3I9F9IBb2ImF3a44xfiAKdDhzr4DK/vQhvhPuuTeZA41
r2zp8Cu+Bp40pSxmoAOK3B0/peZAka01Ju7c7ZChDWrxleHZAKEA/6dcaWHotfGS
eW5YLbSms3f0m0GH38nRI7oxyCW6yMIDkFHURVMBKW1OhrcuGo8u0nTmi5IH9gRg
5bH8XcujlQJBAMWBQgzCHyoSeryD3TFieXIFzgDBw6Ve5hyMjUjtvgdVKoxRPvpO
kclc39QHP6Dm2wrXXHEej+9RILxBZCVQNbMCQQC42i+Ut0nHvPuXN/UkXzomDHde
h1ySsOAO4H+8Y6OSI87l3HUrByCQ7stX1z3L0HofjHqV9Koy9emGTFLEzSdAkB7
Ei6cUKKmztKyE3rr+RcATEmwAw3tEJOHmrW5ErApVZKr2TzLMQZ7WZplPzQRCYnY
2ZZLDuZWFFG3vW+wKKktAkAaQ5GNzbwkRLpXF1FZFuNF7erxypzstbUmU/31b7tS
i5LmxTGKL/xRYtZEHjya4lkkkg40q1MrUsgIYbFYMF2
-----END RSA PRIVATE KEY-----
```

## 6.2 格式转换

### 操作场景

负载均衡只支持PEM格式的证书，其它格式的证书需要转换成PEM格式后，才能上传到负载均衡。以下是转换成PEM格式的几种常用办法。

### DER 转换为 PEM

DER格式通常使用在Java平台中。

运行以下命令进行证书转化：

```
openssl x509 -inform der -in certificate.cer -out certificate.pem
```

运行以下命令进行私钥转化：

```
openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem
```

### P7B 转换为 PEM

P7B格式通常使用在Windows Server和Tomcat中。

运行以下命令进行证书转化：

```
openssl pkcs7 -print_certs -in incertificate.p7b -out outcertificate.cer
```

### PFX 转换为 PEM

PFX格式通常使用在Windows Server中。

运行以下命令进行证书转化：

```
openssl pkcs12 -in certname.pfx -nokeys -out cert.pem
```

运行以下命令进行私钥转化：

```
openssl pkcs12 -in certname.pfx -nocerts -out key.pem -nodes
```

## 6.3 创建证书


### 操作场景

为了支持HTTPS数据传输加密认证，在创建HTTPS协议监听的时候需绑定证书，负载均衡提供证书管理功能。

#### 说明

- 新建证书只能绑定于所选类型的负载均衡器，请确保负载均衡器类型选择正确。

### 创建证书

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. 选择“服务列表 > 网络 > 弹性负载均衡”。
4. 在左侧导航栏单击“证书管理”。
5. 单击“创建证书”，配置证书内容。
  - 证书名称
  - 证书类型：
    - 服务器证书：在使用HTTPS协议时，服务器证书用于SSL握手协商，需提供证书内容和私钥。
    - CA证书：又称客户端CA公钥证书，用于验证客户端证书的签发者；在开启HTTPS双向认证功能时，只有当客户端能够出具指定CA签发的证书时，HTTPS连接才能成功。
  - 证书内容：证书内容必须为PEM格式。  
单击“上传”，选择上传证书文件，请确保您的浏览器是最新版本。
  - 私钥  
单击“上传”，选择上传私钥文件，请确保您的浏览器是最新版本。  
需注意必须是无密码的私钥。私钥格式如下：

```
-----BEGIN PRIVATE KEY-----  
[key]  
-----END PRIVATE KEY-----
```

#### 说明

若是证书链，需要配置从子证书到根证书的所有证书内容和私钥，且证书内容和私钥的配置顺序必须保持一致。

例如：某用户有三个证书，它们的关系是子证书 > 中级证书 > 根证书，则正确的配置顺序是子证书 > 中级证书 > 根证书。

- 域名




如果创建的证书用于SNI，则需要指定域名，每个证书只能指定一个域名。且域名必须与证书中的域名一致。


- 描述
6. 填写完成后，单击“确定”。

## 删除证书


删除证书时，只能删除未使用的证书，在使用中的证书无法删除。

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. 选择“服务列表 > 网络 > 弹性负载均衡”。
4. 在左侧导航栏单击“证书管理”。
5. 在证书列表中，在需要修改的证书所在行，单击“删除”。
6. 在确认对话框中单击“确定”，完成删除。

## 修改证书

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. 选择“服务列表 > 网络 > 弹性负载均衡”。
4. 在左侧导航栏单击“证书管理”。
5. 在证书列表中，在需要修改的证书所在行，单击“修改”。
6. 在“修改证书”对话框中，修改证书的相关信息。
7. 在确认对话框中单击“确定”，完成修改。

## 绑定证书


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. 选择“服务列表 > 网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要添加HTTPS协议的负载均衡器名称。
5. 切换到“监听器”页签，单击“添加监听器”。
6. 在弹出的“添加监听器”对话框中，完成参数配置。当“前端协议/端口”选择HTTPS协议时，监听器需绑定证书，即设置“服务器证书”参数。
7. 填写完成后，单击“确定”。

# 7 访问日志

## 操作场景

负载均衡的访问日志功能支持查看和分析对七层负载均衡HTTP和HTTPS进行请求的详细访问日志记录，包括请求时间、客户端IP地址、请求路径和服务器响应等。配置访问日志时需要您对接云日志服务，已创建需要关联的云日志组和日志流。配置了访问日志后，新连接上的请求日志才会上传到AOM日志桶。

## 配置访问日志

1. 在“云日志服务”界面创建日志组。
  - a. 登录管理控制台。
  - b. 在管理控制台左上角单击图标，选择区域和项目。
  - c. 选择“服务列表 > 云日志服务”。
  - d. 单击左侧导航栏“日志管理”。
  - e. 单击“创建日志组”，在弹出框内，输入日志组名称。
  - f. 单击“确定”，创建完成。
2. 在“云日志服务”界面创建日志流。
  - a. 选择已创建的日志组名称，进入该日志组页面。
  - b. 单击“创建日志流”，在弹出框内，输入日志流名称。
  - c. 单击“确定”，创建完成。
3. ELB对接云日志服务时，为了支持实时显示日志记录，需要在相应日志流下，手动搜索。
  - a. 在新创建日志流名称所在行，单击“搜索日志”。
  - b. 在搜索输入框按照提示输入搜索内容。
  - c. 点击“搜索”图标，完成搜索。
4. 在“弹性负载均衡”界面配置访问日志。
  - a. 选择“服务列表 > 网络 > 弹性负载均衡”。
  - b. 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。
  - c. 在该负载均衡器界面的“访问日志”页签，单击“配置访问日志”。

- d. 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。
- e. 单击“确定”，配置完成。

查看访问日志

当您配置了访问日志，可以查看访问日志的详细信息。

查看方式以下两种：

1. 通过“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。
2. （推荐）通过“云日志服务”控制台，进入日志主题界面，选择相应日志主题名称，单击“实时日志”，即可查看访问日志。

日志显示格式如下，日志字段说明如表7-1所示。

```
$msec $access_log_topic_id [$time_iso8601] $log_ver $remote_addr:$remote_port $status
"$request_method $scheme://$host$router_request_uri $server_protocol" $request_length $bytes_sent
$body_bytes_sent $request_time "$upstream_status" "$upstream_connect_time" "$upstream_header_time"
"$upstream_response_time" "$upstream_addr" "$http_user_agent" "$http_referer" "$http_x_forwarded_for"
$lb_name $listener_name $listener_id
$pool_name "$member_name" $tenant_id $eip_address:$eip_port "$upstream_addr_priv" $certificate_id
$ssl_protocol $ssl_cipher $sni_domain_name $tcpinfo_rtt
```

表 7-1 字段说明

参数	描述
msec	以秒为单位的时间，日志写入时的分辨率为毫秒。
access_log_topic_id	访问日志流ID。
time_iso8601	日志写入时的时间，采用ISO 8601标准格式本地时间。
log_ver	ELB服务日志版本号。
remote_addr: remote_port	客户端IP地址：客户端端口。
status	ELB响应的状态码。
request_method scheme://host router_request_uri server_protocol	请求方法 请求方式：//主机名：请求URI 请求协议。
request_length	从客户端收到的请求长度（包括请求head和请求body）。
bytes_sent	发送到客户端的字节数。
body_bytes_sent	发送到客户端的字节数（不包括响应头）。
request_time	请求处理时间，即ELB收到第一个客户端请求报文到ELB发送完响应报文的时间间隔（单位：秒）。
upstream_status	从上游服务器获得的响应状态码，当ELB代理进行请求重试时会包含多个响应的状态码，当请求未被正确转发到后端服务器时此字段为-。

参数	描述
upstream_connect_time	与上游服务器建立连接所花费的时间，时间以秒为单位，分辨率为毫秒。当ELB代理进行请求重试时会包含多个连接的时间，当请求未被正确转发到后端服务器时此字段为 -。
upstream_header_time	从上游服务器接收响应头所花费的时间，时间以秒为单位，分辨率为毫秒。当ELB代理进行请求重试时会包含多个响应时间，当请求未被正确转发到后端服务器时此字段为 -。
upstream_response_time	从上游服务器接收响应所花费的时间，时间以秒为单位，分辨率为毫秒。当ELB代理进行请求重试时会包含多个响应时间，当请求未被正确转发到后端服务器时此字段为 -。
upstream_addr	后端服务器在ELB服务内部IP地址和端口（客户可忽略）。
http_user_agent	ELB收到请求头中的http_user_agent内容，表示客户端的系统型号、浏览器信息等。
http_referer	ELB收到请求头中的http_referer内容，表示该请求所在的页面链接。
http_x_forwarded_for	ELB收到请求头中的http_x_forwarded_for内容，表示请求经过的代理服务器IP地址。
lb_name	负载均衡器的名称（格式为“loadbalancer_” + “负载均衡器ID”）。
listener_name	监听器的名称（格式为“listener_” + “监听器ID”）。
listener_id	监听器在ELB服务内部的ID（客户可忽略）。
pool_name	后端服务器组名称（格式为“pool_” + “后端服务器组ID”）。
member_name	后端服务器的名称（格式为“member_” + “服务器ID”，尚未支持）。
tenant_id	租户ID。
eip_address:eip_port	弹性IP地址和监听器监听的端口号。
upstream_addr_priv	后端主机的IP地址和端口号。
certificate_id	[HTTPS监听器]SSL连接建立时使用的证书ID（尚未支持）。
ssl_protocol	[HTTPS监听器]SSL连接建立使用的协议，非HTTPS监听器，此字段为 -。
ssl_cipher	[HTTPS监听器]SSL连接建立使用的加密套件，非HTTPS监听器，此字段为 -。

参数	描述
sni_domain_name	[HTTPS监听器]SSL握手时客户端提供的SNI域名，非HTTPS监听器，此字段为 -。
tcpinfo_rtt	ELB与客户端之间的tcp rtt时间，单位：微秒。

配置日志转储

如果您希望将日志转储进行二次分析，您可以参考本章设置日志转储。

1. 选择“服务列表 > 云日志服务”。
2. 单击“日志转储”。

配置转储

\* 日志组名称

--请选择--

C

\* 企业项目

C 查看企业项目

\* 日志流名称

--请选择--

\* 转储方式

 OBS

 DIS

\* OBS桶

--请选择--

C 查看OBS

选中的桶会将读写策略授权给云日志服务，请谨慎修改桶策略，防止转储失败。

自定义转储路径

☐

日志文件前缀

请输入日志文件前缀

?

\* 转储格式

原始日志格式

\* 是否开启转储

☒

\* 转储周期

3 小时

?

3. 根据实际情况设置转储方式和其他配置项，具体操作请参见《云日志服务用户指南》。

# 8 监控

## 8.1 监控指标说明

### 功能说明

本节定义了弹性负载均衡服务上报云监控的监控指标的命名空间，监控指标列表和维度定义。用户可以通过云监控提供的API接口来检索弹性负载均衡服务上报的监控指标以及产生告警信息。

### 命名空间

SYS.ELB

### 监控指标

指标ID	指标名称	含义	取值范围	测量对象	监控周期 (原始指标)
m1_cps	并发连接数	从测量对象到后端服务器建立的所有TCP和UDP连接的数量。 单位：个	≥ 1 个	负载均衡器、负载均衡监听器。	1分钟
m2_act_conn	活跃连接数	从测量对象到后端服务器建立的所有 <b>ESTABLISHED</b> 状态的TCP或UDP连接的数量。 Windows和Linux服务器都可以使用如下命令查看。 <code>netstat -an</code> 单位：个	≥ 1 个		

指标ID	指标名称	含义	取值范围	测量对象	监控周期 (原始指标)
m3_inact_conn	非活跃连接数	从测量对象到所有后端服务器建立的所有除 <b>ESTABLISHED</b> 状态之外的 TCP 连接的数量。  Windows 和 Linux 服务器都可以使用如下命令查看。 <code>netstat -an</code> 单位：个	≥ 1 个		
m4_ncps	新建连接数	从客户端到测量对象每秒新建立的 TCP 和 UDP 连接数。 单位：个/秒	≥ 1 个/秒		
m5_in_pps	流入数据包数	测量对象每秒接收到的数据包的个数。 单位：个/秒	≥ 1 个/秒		
m6_out_pps	流出数据包数	测量对象每秒发出的数据包的个数。 单位：个/秒	≥ 1 个/秒		
m7_in_Bps	网络流入速率	从外部访问测量对象所消耗的流量。 单位：字节/秒	≥ 1 bytes/s		
m8_out_Bps	网络流出速率	测量对象访问外部所消耗的流量。 单位：字节/秒	≥ 1 bytes/s		
m9_abnormal_servers	异常主机数	健康检查统计监控对象后端异常的主机个数。 单位：个	≥ 1 个	负载均衡器	1分钟
ma_normal_servers	正常主机数	健康检查统计监控对象后端正常的主机个数。 单位：个	≥ 1 个		
7层（HTTP/HTTPS）支持的监控指标					
mb_l7_qps	7层查询速率	统计测量对象当前7层查询速率。（HTTP和HTTPS监听器才有此指标） 单位：次/秒。	≥ 1 个/秒	负载均衡器和负载均衡监听器。	1分钟

指标ID	指标名称	含义	取值范围	测量对象	监控周期 (原始指标)
mc_l7_http_2xx	7层协议返回码 (2XX)	统计测量对象当前7层2XX系列状态响应码的数量。 ( HTTP和HTTPS监听器才有此指标 ) 单位：个/秒。	$\geq 1$ 个/秒		
md_l7_http_3xx	7层协议返回码 (3XX)	统计测量对象当前7层3XX系列状态响应码的数量。 ( HTTP和HTTPS监听器才有此指标 ) 单位：个/秒。	$\geq 1$ 个/秒		
me_l7_http_4xx	7层协议返回码 (4XX)	统计测量对象当前7层4XX系列状态响应码的数量。 ( HTTP和HTTPS监听器才有此指标 ) 单位：个/秒。	$\geq 1$ 个/秒		
mf_l7_http_5xx	7层协议返回码 (5XX)	统计测量对象当前7层5XX系列状态响应码的数量。 ( HTTP和HTTPS监听器才有此指标 ) 单位：个/秒。	$\geq 1$ 个/秒		
m10_l7_http_other_status	7层协议返回码 (Others)	统计测量对象当前7层非2XX,3XX,4XX,5XX系列状态响应码的数量。( HTTP和HTTPS监听器才有此指标 ) 单位：个/秒。	$\geq 1$ 个/秒		
m11_l7_http_404	7层协议返回码 (404)	统计测量对象当前7层404状态响应码的数量。 ( HTTP和HTTPS监听器才有此指标 ) 单位：个/秒。	$\geq 1$ 个/秒		
m12_l7_http_499	7层协议返回码 (499)	统计测量对象当前7层499状态响应码的数量。 ( HTTP和HTTPS监听器才有此指标 ) 单位：个/秒。	$\geq 1$ 个/秒		



指标ID	指标名称	含义	取值范围	测量对象	监控周期 (原始指标)
m13_l7_http_502	7层协议返回码 (502)	统计测量对象当前7层502状态响应码的数量。 ( HTTP和HTTPS监听器才有此指标 ) 单位：个/秒。	≥ 1 个/秒		
m14_l7_rt	7层协议RT平均值	统计测量对象当前7层平均响应时间。( HTTP和HTTPS监听器才有此指标 ) 从测量对象收到客户端请求开始，到测量对象将所有响应返回给客户端为止。 单位：毫秒。	≥ 1ms		

a: 对于有多个测量维度的测量对象，使用接口查询监控指标时，所有测量维度均为必选。

- 查询单个监控指标时，多维度dim使用样例：dim.0=lbaas\_instance\_id, 223e9eed-2b02-4ed2-a126-7e806a6fee1f&dim.1=lbaas\_listener\_id, 3baa7335-8886-4867-8481-7cbba967a917。
- 批量查询监控指标时，多维度dim使用样例：

```
"dimensions": [  
  {  
    "name": "lbaas_instance_id",  
    "value": "223e9eed-2b02-4ed2-a126-7e806a6fee1f"  
  },  
  {  
    "name": "lbaas_listener_id",  
    "value": "3baa7335-8886-4867-8481-7cbba967a917"  
  }  
],
```

维度

Key	Value
lbaas_instance_id	负载均衡器的ID。
lbaas_listener_id	负载均衡监听器的ID。

8.2 设置告警规则

## 8.2.1 添加告警规则

1. 登录管理控制台。
2. 选择“管理与部署 > 云监控服务”。
3. 在左侧导航树栏，选择“告警 > 告警规则”。
4. 在“告警规则”界面，单击“创建告警规则”进行添加，设置弹性负载均衡器的告警规则。

以创建弹性负载均衡器的告警规则为例：

- a. 单击“资源类型”，选择“弹性负载均衡”。
- b. 单击“维度”，可以选择“增强型负载均衡器”或“监听器”，这里以选择“负载均衡器”为例。
- c. 按照需要设置其他参数，修改完成后单击“立即创建”。

弹性负载均衡器告警规则设置完成后，如果通知功能已开启，当符合规则的告警产生时，系统会自动进行通知。

### 说明

更多关于弹性负载均衡器监控规则的信息，请参见《云监控服务用户指南》。

## 8.2.2 修改告警规则

1. 登录管理控制台。
2. 选择“管理与部署 > 云监控服务”。
3. 在左侧导航树栏，选择“告警 > 告警规则”。
4. 在“告警规则”界面，选择已有的告警规则进行修改，设置弹性负载均衡器的告警规则。

- a. 单击待修改的告警规则名称，进入详情页。
- b. 单击右上角的“修改”。
- c. 根据界面提示修改配置参数。
- d. 按照需要设置其他参数，修改完成后单击“立即修改”。

弹性负载均衡器告警规则设置完成后，如果通知功能已开启，当符合规则的告警产生时，系统会自动进行通知。

### 说明

## 8.3 查看监控指标

### 操作场景

公有云平台提供的云监控服务，可以对弹性负载均衡器的运行状态进行日常监控。您可以通过管理控制台，直观地查看弹性负载均衡器的各项监控指标。

由于监控数据的获取与传输会花费一定时间，因此，云监控显示的是当前时间5~10分钟前的弹性负载均衡状态。如果您的弹性负载均衡器刚刚创建完成，请等待5~10分钟后查看监控数据。

## 前提条件

- 已经正常运行了一段时间的弹性负载均衡器。  
关机、故障、删除状态的后端服务器，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。

### 说明

- 关机、故障24小时以上的后端服务器，云监控将默认该负载均衡器不存在，并在监控列表中删除，不再对其进行监控，但告警规则需要用户手动清理。
- 负载均衡器已对接云监控服务，即已在云监控服务页面设置告警规则。  
对接云监控服务之前，用户无法查看到未对接资源的监控数据。具体操作，请参见[设置告警规则](#)。

## 操作步骤

1. 登录管理控制台。
2. 选择“管理与部署 > 云监控服务”。
3. 在左侧导航树选择“云服务监控 > 弹性负载均衡”。
4. 单击待查看的负载均衡器所在行的“查看监控指标”，查看负载均衡器监控指标。

# 9 审计

## 9.1 支持审计的关键操作列表

通过云审计服务，您可以记录与弹性负载均衡相关的操作事件，便于日后的查询、审计和回溯。

云审计支持的弹性负载均衡列表操作事件如表9-1所示。

表 9-1 云审计服务支持的弹性负载均衡操作列表

操作名称	资源类型	事件名称
配置访问日志	accesslog	create access log
删除访问日志	accesslog	delete access log
创建证书	certificate	create certificate
更新证书	certificate	update certificate
删除证书	certificate	delete certificate
创建健康检查	healthmonitor	create healthmonitor
更新健康检查	healthmonitor	update healthmonitor
删除健康检查	healthmonitor	delete healthmonitor
创建转发策略	l7policy	create forwarding policy
更新转发策略	l7policy	update forwarding policy
删除转发策略	l7policy	delete forwarding policy
创建转发规则	l7rule	create forwarding rule
更新转发规则	l7rule	update forwarding rule
删除转发规则	l7rule	delete forwarding rule
创建监听器	listener	create listener

操作名称	资源类型	事件名称
更新监听器	listener	update listener
删除监听器	listener	delete listener
创建负载均衡器	loadbalancer	create loadbalancer
更新负载均衡器	loadbalancer	update loadbalancer
删除负载均衡器	loadbalancer	delete loadbalancer
添加后端云服务器	member	add backend ecs
更新后端云服务器	member	update backend ecs
移除后端云服务器	member	remove backend ecs
创建后端服务器组	pool	create backend member group
更新后端服务器组	pool	update backend member group
删除后端服务器组	pool	delete backend member group


## 9.2 查看审计日志

### 操作场景

在您开启了云审计服务后，系统开始记录云服务资源的操作。云审计服务管理控制台保存最近7天的操作记录。

本节介绍如何在云审计服务管理控制台查看最近7天的操作记录。

### 操作步骤

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“服务列表”，选择“管理与部署 > 云审计服务”，进入云审计服务信息页面。
4. 单击左侧导航树的“事件列表”，进入事件列表信息页面。
5. 事件列表支持通过筛选来查询对应的操作事件。当前事件列表支持四个维度的组合查询，详细信息如下：
  - 事件类型、事件来源、资源类型和筛选类型。  
在下拉框中选择查询条件。  
其中筛选类型选择事件名称时，还需选择某个具体的事件名称。  
选择资源ID时，还需选择或者手动输入某个具体的资源ID。  
选择资源名称时，还需选择或手动输入某个具体的资源名称。
  - 操作用户：在下拉框中选择某一具体的操作用户，此操作用户指用户级别，而非租户级别。

- 事件级别：可选项为“所有事件级别”、“normal”、“warning”、“incident”，只可选择其中一项。
- 时间范围：可选择查询最近七天内任意时间段的操作事件。


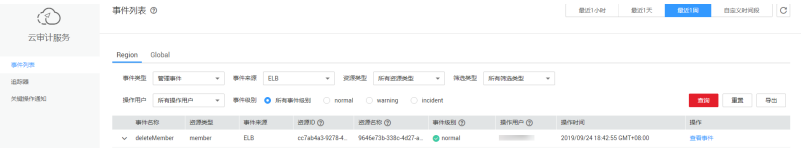
6. 在需要查看的记录左侧，单击  展开该记录的详细信息。如图 [展开记录](#) 所示。

图 9-1 展开记录



7. 在需要查看的记录右侧，单击“查看事件”，弹出一个窗口，如图 [查看事件](#) 所示，显示了该操作事件结构的详细信息。

图 9-2 查看事件



关于云审计服务事件结构的关键字段详解，请参见《云审计服务用户指南》的事件结构。

# 10 常见问题

## 10.1 高频常见问题

- [如何获取来访者的真实IP?](#)
- [健康检查异常如何排查?](#)
- [使用UDP协议有什么注意事项?](#)
- [ELB支持什么类型的会话保持?](#)
- [如何启用WebSocket支持?](#)
- [如何检查弹性负载均衡会话保持不生效?](#)
- [监听器中分配算法和会话保持算法是什么关系?](#)
- [ELB如何根据不同的协议来分发流量?](#)

## 10.2 弹性负载均衡使用

### 10.2.1 异常检查

#### 10.2.1.1 如何检查弹性负载均衡服务不通或异常中断?

1. 检查后端云服务器的健康检查状态是否正常，如果异常，流量会切换到其他后端云服务器。
2. 客户后端服务安全策略中是否放通了100.125.0.0/16网段。
3. 弹性负载均衡与客户端的TCP连接，创建TCP连接的超时时间是300s，超时时间用户不能设置。如果超过300s，弹性负载均衡会向客户端和服务端发送RST断开连接。
4. 如果选择的是源IP算法，需要注意请求到达弹性负载均衡之前IP是否发生变化。  
例如：ELB配合CDN、WAF服务使用，请求经过CDN、WAF后，IP会被代理，到达ELB的IP无法保持一致，导致会话保持失效。若您要使用CDN、WAF服务，建议使用七层监听器，使用基于cookie的会话保持。

5. 如果是HTTP或HTTPS监听器，配置了会话保持，需要注意发送的请求是否带有cookie，如果带有cookie，则观察该cookie值是否发生了变化（因为7层会话保持基于cookie）。
6. 查看后端服务器组的会话保持是否超时。若您未做配置四层监听器的后端服务器组默认会话保持时间是1分钟，七层监听器的后端服务器组默认会话保持时间是1天。

## 10.2.2 功能支持

### 10.2.2.1 弹性负载均衡器是否可以单独使用？

不可以。

弹性负载均衡器是为客户提供的服务产品，要基于弹性云服务器来使用，不可以单独使用。

### 10.2.2.2 弹性负载均衡分配的 EIP 是否为独占？

在您创建使用ELB服务的整个生命周期内：

负载均衡的弹性公网IP支持解绑，解绑后的负载均衡变成私网型负载均衡，解绑后的弹性公网IP可被其他资源绑定。

### 10.2.2.3 单个用户默认可以创建多少个负载均衡器或监听器？

单个用户默认可创建50个负载均衡器，默认可创建100个监听器。如果需要创建更多弹性负载均衡器或监听器，请申请更高配额。

单个弹性负载均衡器下可创建的监听器个数，与当前用户下的监听器剩余配额相等。

### 10.2.2.4 当负载均衡器正在运行中是否可以调整后端服务器的数量？

我们支持在任意时刻增加或减少负载均衡器的后端服务器的数量，且可以支持不同的后端服务器切换操作。但是，为了保证您对外业务的稳定，请确保在执行上述操作时能够开启负载均衡器的健康检查功能，并同时保证负载均衡后端至少有1台正常运行的服务器。

### 10.2.2.5 弹性负载均衡是否可以添加不同操作系统的服务器？

可以。

ELB本身不会限制后端的服务器使用哪种操作系统，只要您的2台服务器中的应用服务部署是相同且保证数据的一致性即可。但是，我们建议您选择2台相同操作系统的服务器进行配置，以便您日后的管理维护。

## 10.2.3 性能负载

### 10.2.3.1 如何检查弹性负载均衡前后端流量不一致？

检查客户端请求是否有失败的请求，特别是返回码是4xx的请求。因为这些请求可能是因为异常请求被弹性负载均衡拒绝，没有转发至后端服务器。



### 10.2.3.2 如何检查请求不均衡？

1. 检查是否开启了会话保持。如果配置了会话保持，而客户端的个数又比较少时，很容易导致不均衡。
2. 检查后端云服务器的健康检查状态是否正常，特别要关注下是否有健康检查状态一会正常一会异常的情况。健康检查异常或者状态切换都会导致流量不均衡。
3. 检查负载均衡算法是否是源IP算法。此时同一个IP发过来的请求都会分发到同一个后端，导致流量不均衡。
4. 后端服务是否开启了TCP keepalive保持长连接。如果开启，则有可能因为长连接上的请求数不同导致流量不均衡。
5. 将云服务器添加到ELB后端时是否设置了权重，权重不同，分发的流量也不同。

### 10.2.3.3 如何检查弹性负载均衡业务访问延时大？

1. 将EIP绑定到后端云服务器，不经过弹性负载均衡直接访问后端服务，查看访问延时。用来判断是弹性负载均衡的问题，还是前端网络问题或者后端服务问题。
2. 查看业务流量是否超过了EIP的带宽限制。
3. 如果直接访问后端存在业务访问延时大，需要排查后端服务是否压力过大，是否配置了安全策略等。
4. 查看异常主机数的监控来判断后端云服务器的健康检查状态是否有跳变。在后端服务状况不稳定时，因为弹性负载均衡的重试机制，如果连接一台后端超时，请求会重新发往下一台后端，请求成功，这样业务就表现为访问成功，但是延时很大。
5. 如果问题依然存在，请联系客服。

### 10.2.3.4 如何检测压测性能上不去？

1. 检查后端云服务器的负载状态，如果CPU达到100%，可能是后端应用达到性能瓶颈。
2. 查看流量是否超过绑定到弹性负载均衡的EIP的带宽，带宽超限后，会有大量丢包和请求失败，影响压测性能。
3. 如果是短连接测试，可能是客户端端口不足导致建立连接失败，可以通过客户端处于time\_wait状态的连接数量来判断。
4. 后端服务器的监听队列backlog满了，导致后端服务器不回复syn\_ack报文，使得客户端连接超时。可以通过调整net.core.somaxconn参数来调大backlog的上限值。

## 10.3 负载均衡器

### 10.3.1 ELB 如何根据不同的协议来分发流量？

ELB采用FullNAT模式转发。如下图所示，四层协议转发经过LVS，七层转发协议，经过LVS后再到NGINX。

图 10-1 四层转发协议

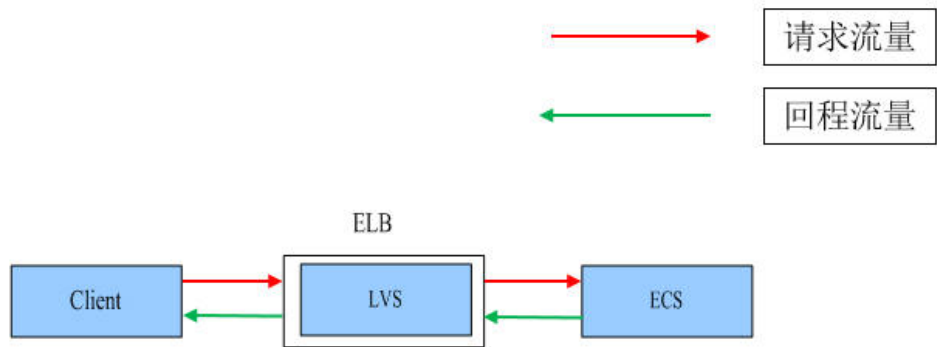
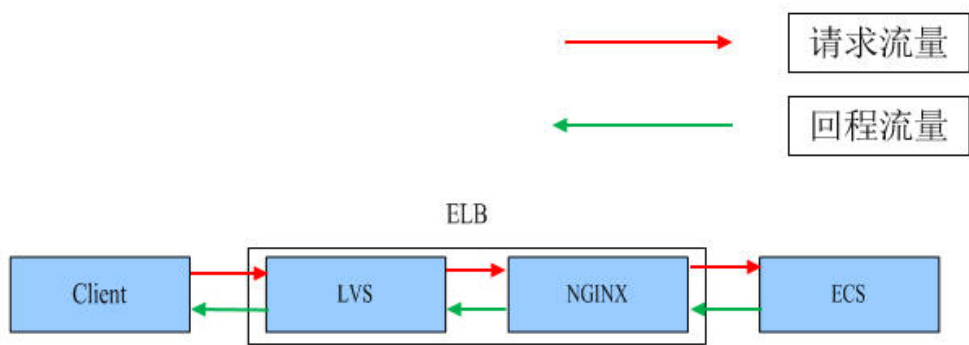


图 10-2 七层转发协议



10.3.2 如何配置私网或公网负载均衡？

创建一个负载均衡，系统分配一个私有IP，默认是私网负载均衡，如果为这个私有IP绑定一个公网的IP，则可作为公网负载均衡。负载均衡同时可支持私网、公网访问。

10.4 监听器

10.4.1 监听器中分配算法和会话保持算法是什么关系？

表 10-1 负载均衡会话保持支持情况

分配策略	会话保持	L4 ( TCP、UDP )	L7 ( HTTP/HTTPS )
加权轮询算法	源IP地址	支持	不支持
	负载均衡器cookie	不涉及	支持
	应用程序cookie	不涉及	支持
加权最少连接	源IP地址	不支持	不支持
	负载均衡器cookie	不涉及	不支持

分配策略	会话保持	L4 ( TCP、UDP )	L7 ( HTTP/HTTPS )
	应用程序cookie	不涉及	不支持
源IP地址	源IP地址	支持	支持
	负载均衡器cookie	不涉及	不支持
	应用程序cookie	不涉及	不支持

一般建议：算法可以使用轮询算法，四层会话保持使用源IP地址，7层使用负载均衡器cookie方式。

## 10.4.2 弹性负载均衡如何支持多证书？

每个监听器只支持一个证书/证书链，如果要支持多证书/证书链，需创建多个监听器。

## 10.4.3 如何启用 WebSocket 支持？

无需配置，当选用HTTP监听时，默认支持无加密版本WebSocket协议（WS协议）；当选择HTTPS监听时，默认支持加密版本的WebSocket协议（WSS协议）。

# 10.5 后端服务器

## 10.5.1 为什么后端服务器上收到的健康检查报文间隔和设置的间隔时间不一致？

ELB的每个lvs、nginx节点都会探测后端服务器，每个节点的间隔时间与设置的间隔时间保持一致。

后端服务器收到的是多个节点的探测报文，故在间隔时间内会收到多个检查报文。

## 10.5.2 使用 ELB 后，后端服务器能否访问公网？

后端服务器能否访问公网和ELB没有关系，如果后端服务器本身可以访问公网，使用了ELB以后仍可以访问，如果服务器本身不可以访问公网，使用ELB之后仍不可以。

## 10.5.3 如何检查后端服务器网络状态？

1. 确认虚拟机主网卡已经正确分配到IP地址。
  - a. 登录虚拟机内部。
  - b. 执行ifconfig命令或ip address查看网卡的IP信息。

### 说明

Windows虚拟机可以在命令行中执行ipconfig查看。

2. 从虚拟机内部ping所在子网的网关，确认基本通信功能是否正常。

- a. 通常网关地址结尾为.1，可以在VPC详情页面中确认，切换“子网”页签，查看“网关”列，显示网关地址。
- b. 执行ping命令，观察能否ping通即可。若无法ping通网关则需首先排查二三层网络问题。

### 10.5.4 如何检查后端服务器网络配置？

1. 确认虚拟机使用的网卡安全组配置是否正确。
  - a. 在弹性云服务器详情页面查看网卡使用的安全组。
  - b. 查看安全组是否已放行100.125.0.0/16网段的地址，如果没有放行，请添加100.125.0.0/16网段的入方向规则，用户可根据自己的实际业务场景添加入方向规则。
2. 确认虚拟机使用网卡子网的网络ACL不会对流量进行拦截。

在虚拟私有云页面左侧导航栏，单击“网络ACL”，确认涉及的子网已放通。

### 10.5.5 如何检查后端服务器服务状态？

1. 确认服务器服务是否开启。
  - a. 登录虚拟机内部。
  - b. 执行如下命令，查看系统的端口监听状态，如图10-3所示。

**netstat -ntpl**

#### 说明

Windows虚拟机可以在命令行中执行**netstat -ano**查看系统的端口监听状态，或者查看服务端软件状态。

图 10-3 系统的端口监听状态

```
[root@ecs-67a0 ~]# netstat -ntpl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:80               0.0.0.0:*               LISTEN      25847/./httpterm-s
tcp        0      0 0.0.0.0:22               0.0.0.0:*               LISTEN      1437/sshd
tcp6       0      0 :::22                   :::*                   LISTEN      1437/sshd
[root@ecs-67a0 ~]#
```

2. 从虚拟机测试服务通信功能是否正常。

例如：该虚拟机的端口为http 80，使用curl命令，校验服务通信功能是否正常。

```
[root@ecs-67a0 ~]# curl 127.0.0.1:80 -v
* About to connect() to 127.0.0.1 port 80 (#0)
* Trying 127.0.0.1...
* Connected to 127.0.0.1 (127.0.0.1) port 80 (#0)
> GET / HTTP/1.1
> User-Agent: curl/7.29.0
> Host: 127.0.0.1
> Accept: */*
< HTTP/1.1 200
< Connection: close
< Content-length: 14
< Cache-Control: no-cache
< X-req: size=14, time=500 ms
< X-rsp: id=test1, code=200, cache=0, size=14, time=500 ms
helloworld!!
* Closing connection 0
[root@ecs-67a0 ~]#
```

## 10.5.6 后端服务器什么时候被认为是健康的？

首次添加的服务器健康检查成功一次就上线，后续按照配置的“最大重试次数”上线。

## 10.6 健康检查

### 10.6.1 健康检查异常如何排查？

#### 问题描述

客户端通过负载均衡器访问后端服务器异常，负载均衡器的“后端服务器组”页签显示后端服务器的健康检查结果为“异常。”

#### 背景介绍

ELB的健康检查通过向后端服务器发起心跳检查的方式来实现，检查过程中使用内网地址100.125.0.0/16通信。为了确保健康检查的正常进行，您需要确保服务器已经放通100.125.0.0/16网段的地址，使得ELB能够正常访问到后端服务器。

当健康检查探测到您的后端服务器异常时，ELB会将异常的服务器暂时移出后端服务器组，不再向异常的后端服务器转发流量。直到健康检查检测到后端服务器恢复正常时，ELB才会向此服务器继续转发流量。

说明

- 当ELB后端服务器的健康检查状态处于异常状态时，ELB不会向该后端服务器转发请求。
- 当健康检查关闭时，ELB默认后端服务器正常在线，会将请求转发至后端服务器。
- ELB会使用100.125.0.0/16网段IP向后端服务器发送健康检查请求和正常的客户端请求。
- 当后端服务器的权重为0时，流量不会再转发到该后端服务器上，此时健康检查的状态无参考意义。

排查思路

以下排查思路根据原因的出现概率进行排序，建议您从高频原因往低频原因排查，从而帮助您快速找到问题的原因。

如果解决完某个可能原因仍未解决问题，请继续排查其他可能原因。

说明

相关修改配置的操作，修改完配置后需要等待一定的时间，配置才会生效，因为健康检查包含检查周期和阈值（根据默认配置为几十秒生效，如果健康检查恢复正常，在ELB关联的后端服务器基本信息界面可以看到健康检查状态是否正常）。

图 10-4 排查思路

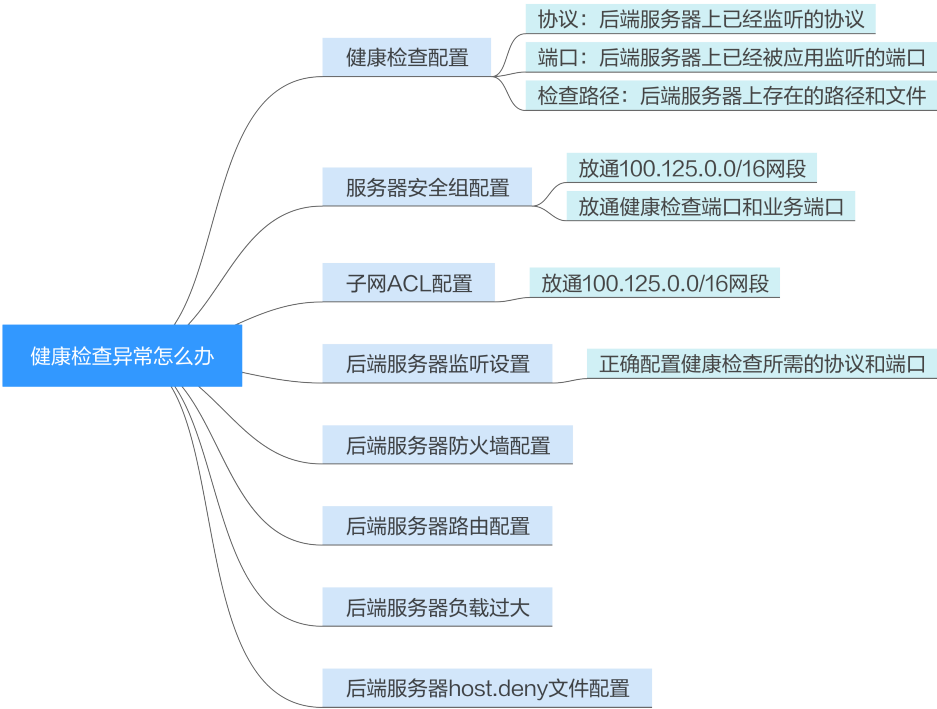


表 10-2 排查思路

可能原因	处理措施
健康检查配置	解决方法请参考 <a href="#">检查健康检查配置</a> 。
服务器安全组配置	解决方法请参考 <a href="#">检查服务器所在安全组</a> 。

可能原因	处理措施
子网ACL配置	解决方法请参考 <a href="#">检查网络ACL规则</a> 。
后端服务器监听配置	解决方法请参考 <a href="#">检查后端服务器是否正常</a> 。
后端服务器防火墙配置	解决方法请参考 <a href="#">检查服务器防火墙</a> 。
后端服务器路由配置	解决方法请参考 <a href="#">检查服务器路由</a> 。
后端服务器负载过大	解决方法请参考 <a href="#">检查服务器负载</a> 。
后端服务器host.deny文件配置	解决方法请参考 <a href="#">检查服务器host.deny文件</a> 。

检查健康检查配置

单击对应的负载均衡名称，进入负载均衡基本信息页面。切换到“后端服务器组”页签，单击对应的后端服务器组名称，在其基本信息页面，单击“健康检查”右侧的配置按钮。查看以下参数：

- 协议。
- 端口。
- 检查路径。如果是使用HTTP健康检查需要查看此参数，建议配置简单的静态HTML文件。

检查服务器所在安全组

- **TCP、HTTP或HTTPS协议监听器：**后端服务器所在的安全组入方向规则需要放通100.125.0.0/16网段，并在TCP协议中放通健康检查的端口。
  - **健康检查端口与后端服务器业务端口相同：**需要放通后端服务器的业务端口，例如80。
  - **健康检查端口与后端服务器业务端口不同：**需要放通后端服务器的业务端口和健康检查端口，例如80和443。

说明

健康检查的协议和端口在配置的健康检查配置项提示框中获取。

图 10-5 安全组入方向规则配置示例

入方向          IPv4          TCP          80          100.125.0.0/16

- **UDP协议监听器：**不仅需要保证安全组入方向规则放通健康检查的协议、端口和100.125.0.0/16网段。还需要放通后端服务器所在安全组入方向的ICMP协议。

图 10-6 安全组入方向规则放通 ICMP 协议示例

入方向          IPv4          ICMP          Any          100.125.0.0/16




### 说明

- ELB与后端服务器进行通信的网段为100.125.0.0/16网段，ELB流量转到后端服务器后，源IP会被转换为100.125的IP，发起健康检查的节点的IP就属于这个网段，所以后端服务器配置的安全组必须放通这个网段。
- 如果不确认是否是安全组问题，可以把安全组入方向规则的“协议”和“端口范围/ICMP类型”均放通Any测试下。
- UDP协议监听器，也可以参考[使用UDP协议有什么注意事项？](#)。

## 检查网络 ACL 规则

网络ACL是一个子网级别的可选安全层，通过与子网关联的出方向/入方向规则控制出入子网的数据流。网络ACL与安全组类似，都是安全防护策略，当您想增加额外的安全防护层时，就可以启用网络ACL。但是网络ACL默认规则会拒绝所有入站和出站流量，如果此网络ACL和负载均衡所属同一个子网，或者此网络ACL和负载均衡相关联的后端服务器所属同一个子网那么负载均衡的业务也会受到影响，收不到来自于公网或者私网的任何请求流量，或者会导致后端服务器异常。

您可以通过配置网络ACL入方向规则，放行100.125.0.0/16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. 在系统首页，选择“网络 > 虚拟私有云”。
4. 在左侧导航栏选择“访问控制 > 网络ACL”。
5. 在“网络ACL”列表区域，选择网络ACL的名称列，单击您需要修改的“网络ACL名称”进入网络ACL详情页面。
6. 在入方向规则或出方向规则页签，单击“添加规则”，添加入方向或出方向规则。
  - 策略：选择允许。
  - 协议：和监听器协议一致。
  - 源地址：此方向允许的源地址，填写100.125.0.0/16。
  - 源端口范围：选择业务所在端口范围。
  - 目的地址：此方向允许的目的地址。选择默认值为0.0.0.0/0，代表支持所有的IP地址。
  - 目的端口范围：选择业务所在端口范围。
  - 描述：网络ACL规则的描述信息，非必填项。
7. 单击“确定”。

## 检查后端服务器是否正常

### 说明

如果后端服务器的操作系统为Windows，请通过浏览器直接访问<https://后端服务器的IP:健康检查配置的端口>。如果返回码为2xx或3xx，则表示以后端服务器正常。

- 您可以在后端服务器上通过以下命令查看后端服务器的健康检查端口是否被健康检查协议正常监听。

```
netstat -anlp | grep port
```

回显中包含健康检查端口信息并且显示LISTEN，则表示后端服务器端口在监听状态，如[图10-7](#)中表示880端口被TCP进程所监控。



如果您没有配置健康检查端口信息，默认和后端服务器端口一致。

图 10-7 后端服务器正常被监听的回显示例

```
[root@ecs-elb-srv portable-nginx]# netstat -anlp | grep 8080 | head
tcp        0      0 0.0.0.0:8080 0.0.0.0:* LISTEN
```

图 10-8 后端服务器没有被监听的回显示例

```
[root@donatdel.wangfei.iperf ~]# netstat -anlp | grep 8080
[root@donatdel.wangfei.iperf ~]#
```

- 如果是HTTP健康检查，请您在后端服务器上执行以下命令查看回显中返回的状态码。

curl 后端服务器的私有IP:健康检查端口/健康检查路径 -iv

HTTP健康检查是ELB向后端服务器发起GET请求，当获取到以下所列的响应状态码，认为服务器是正常状态。

对于TCP的监听器，HTTP健康检查正常返回状态码是200。

对于ELB，HTTP健康检查正常返回状态码是200、202或者401。

图 10-9 后端服务器异常的回显示例

```
[root@host-xxx~]# curl 192.168.0.58:8080/index.html -iv
* About to connect() to 192.168.0.58 port 8080 (#0)
* Trying 192.168.0.58...
* Connected to 192.168.0.58 (192.168.0.58) port 8080 (#0)
> GET /index.html HTTP/1.1
> User-Agent: curl/7.29.0
> Host: 192.168.0.58:8080
> Accept: */*
>
* HTTP 1.0, assume close after body
< HTTP/1.0 404 File not found
HTTP/1.0 404 File not found
< Server: SimpleHTTP/0.6 Python/2.7.5
```

图 10-10 后端服务器正常的回显示例

```
[root@host-xxx~]# curl 192.168.0.58:8080/index.html -iv
* About to connect() to 192.168.0.58 port 8080 (#0)
* Trying 192.168.0.58...
* Connected to 192.168.0.58 (192.168.0.58) port 8080 (#0)
> GET /index.html HTTP/1.1
> User-Agent: curl/7.29.0
> Host: 192.168.0.58:8080
> Accept: */*
>
192.168.0.58 . . [08/Apr/2019 17:37:34] "GET /index.html HTTP/1.1" 200
* HTTP 1.0, assume close after body
< HTTP/1.0 200 OK
HTTP/1.0 200 OK
< Server: SimpleHTTP/0.6 Python/2.7.5
```

- 如果HTTP健康检查异常，除了检查健康检查路径外，建议您将配置的HTTP健康检查修改为TCP健康检查。操作如下：

在监听器界面，修改目标监听器，在配置参数里选择已有TCP健康检查的后端服务器组，或者选择新创建TCP健康检查的后端服务器组。配置完成之后，几十秒后去查看健康检查状态是否恢复正常。

## 检查服务器防火墙

如果后端服务器内部开启了防火墙或其他安全类防护软件，这些软件可能会屏蔽 100.125.0.0/16网段的IP，请您在防火墙入方向规则中放通100.125.0.0/16网段。

## 检查服务器路由

请检查是否手动修改了后端服务器内部的路由，查看主网卡（比如eth0）上是否配置默认路由，默认路由是否修改。如果默认路由更改，可能导致健康检查报文无法到达后端服务器。

您可以在后端服务器上通过以下命令查看您的默认路由是否指向网关（经过ELB转发属于跨网段访问，三层通信需要配置默认路由指向网关）。

```
ip route
```

或

```
route -n
```

正常的回显如图10-11所示（如果回显中没有图中第一条路由信息，或者路由指向的IP的不是后端服务器所在VPC子网的网关，请您修改成默认路由）。

图 10-11 默认路由指向网关示例

```
[root@donatdel.wangfei.iperf ~]# ip route
default via 192.168.2.1 dev eth0 proto dhcp metric 100
169.254.169.254 via 192.168.2.1 dev eth0 proto dhcp metric 100
192.168.2.0/24 dev eth0 proto kernel scope link src 192.168.2.124 metric 100
[root@donatdel.wangfei.iperf ~]#
```

图 10-12 默认路由未指向网关示例

```
[root@test ~]# ip route
default via 192.168.0.134 dev eth0
169.254.0.0/16 dev eth0 scope link metric 1002
169.254.169.254 via 192.168.0.1 dev eth0 proto static
192.168.0.0/24 dev eth0 proto kernel scope link src 192.168.0.242
```

## 检查服务器负载

查看后端服务器的负载。如果负载很高，可能会导致健康检查的连接或请求超时。

## 检查服务器 host.deny 文件

建议您排查后端服务器的/etc/hosts.deny文件，文件中不能写入ELB的健康检查 100.125.0.0/16网段。

## 10.6.2 使用 UDP 协议有什么注意事项？

### 什么是 UDP 健康检查

UDP是面向非连接的一种协议，在发送数据前不会通过进行三次握手建立连接，UDP健康检查的实现过程如下：

1. 健康检查的节点根据健康检查配置，向后端发送ICMP request 消息。
  - 如果健康检查节点收到了后端服务器返回的ICMP reply消息，则认为服务正常，继续进行健康检查。

- 如果健康检查节点没有收到后端服务器返回的ICMP reply消息，则认为服务异常，判定健康检查失败。
- 2. 健康检查的节点收到ICMP reply消息后，会给后端服务器发送UDP探测报文。
  - 如果在【超时时间】之内，健康检查的节点服务器收到了后端服务器返回的port unreachable的ICMP消息，则认为服务异常，判定健康检查失败。
  - 如果在【超时时间】之内，健康检查的节点服务器没有收到后端服务器返回的ICMP错误信息，则认为服务正常，判定健康检查成功。

当您配置UDP健康检查时，推荐使用配置页面默认的各项数值。

## 异常排查方法

请您按照以下两种方法排查。

1. 检查健康检查超时时间是否过小。

可能的原因：后端服务器回复的reply或port unreachable类型的ICMP消息未能在超时时间内到达健康检查的节点，导致健康检查结果不准确。

建议采取的措施：将超时时间调整为更大的值。

由于UDP健康检查的原理不同于其他健康检查，建议健康检查超时时间不要过小，否则后端服务器可能会反复上线或下线。

2. 后端服务器是否限制了ICMP消息产生的速率。

Linux系统下，请用以下命令检查ICMP消息速率的限制。

```
sysctl -q net.ipv4.icmp_ratelimit
```

默认值为：1000

```
sysctl -q net.ipv4.icmp_ratemask
```

默认值为：6168

请确认第一条命令返回值为默认值或0，并用以下命令放开port unreachable消息产生的速率限制。

```
sysctl -w net.ipv4.icmp_ratemask=6160
```

更详细的信息请参考Linux Programmer's Manual相关页面：

```
man 7 icmp
```

或者访问地址：<http://man7.org/linux/man-pages/man7/icmp.7.html>

### 说明

放开port unreachable类型ICMP消息的速率限制，会让暴露在公网上的在端口扫描时，不受限制次数地产生port unreachable消息。

## 注意事项

使用UDP协议注意以下事项：

- 负载均衡健康检查是通过UDP报文和Ping报文探测来获取后端云服务器的状态信息。针对此种情况，用户需要确保后端云服务器开启ICMP协议，确认方法如下：  
用户登录后端云服务器，以root权限执行以下命令：  
**cat /proc/sys/net/ipv4/icmp\_echo\_ignore\_all**

若返回值为1，表示ICMP协议关闭；若为0，则表示开启。

- 当前UDP协议服务健康检查可能存在服务真实状态与健康检查不一致的问题：  
如果后端服务器是Linux服务器，在大并发场景下，由于Linux的防ICMP攻击保护机制，会限制服务器发送ICMP的速度。此时，即便服务器已经出现异常，但由于无法向前端返回“port XX unreachable”报错信息，会导致负载均衡由于没收到ICMP 应答进而判定健康检查成功，最终导致服务真实状态与健康检查不一致。

### 10.6.3 健康检查为什么会导致 ELB 会频繁向后端服务器发送探测请求？

ELB是高可用集群部署的，集群内的所有的转发节点会同时向后端服务器发送探测请求，检查周期用户可配，健康检查会根据检查周期一直探测，所以每隔几秒会有访问。您可以通过[配置健康检查](#)的周期来控制访问后端服务器的频率。

## 10.7 获取源 IP

### 10.7.1 如何获取来访者的真实 IP？

#### 背景信息

- 如果IP经过NAT/WAF，则只能获取到NAT/WAF转化后的IP地址，无法获取到NAT/WAF前的IP地址。
- 如果客户端为容器，只能获取到容器所在主机的IP地址，无法获取容器的IP。
- 四层监听器（TCP/UDP）开启“获取客户端IP”功能之后，不支持同一台既作为后端又作为客户端的场景。

#### 七层服务

针对七层（HTTP协议）服务，需要对应用服务器进行配置，然后使用X-Forwarded-For的方式获取来访者的真实IP地址。

真实的来访者IP会被负载均衡放在HTTP头部的X-Forwarded-For字段，格式如下：

X-Forwarded-For: 来访者真实IP, 代理服务器1-IP, 代理服务器2-IP, ...

当使用此方式获取来访者真实IP时，获取的第一个地址就是来访者真实IP。

#### 配置Apache服务器

1. 安装Apache 2.4。  
例如在CentOS 7.5环境下，可以执行如下命令执行安装：  

```
yum install httpd
```
2. 修改Apache的配置文件/etc/httpd/conf/httpd.conf，在最末尾添加以下配置信息。  

```
LoadModule remoteip_module modules/mod_remoteip.so
RemoteIPHeader X-Forwarded-For
RemoteIPInternalProxy 100.125.0.0/16
```

图 10-13 修改 Apache 的配置文件示例图

```
LoadModule remoteip_module modules/mod_remoteip.so
RemoteIPHeader X-Forwarded-For
RemoteIPInternalProxy 100.125.0.0/16
```

### 说明

将代理服务器的网段添加到 RemoteInternalProxy <IP\_address>，如负载均衡的IP地址段 100.125.0.0/16（100.125.0.0/16 是负载均衡服务保留地址，其他用户无法分配到该网段内，不会存在安全风险）和高防IP地址段。多个IP地址段用逗号分隔。

3. 修改Apache的配置文件/etc/httpd/conf/httpd.conf，将日志输出格式修改为如下所示（%a代表源IP地址）：  

```
LogFormat "%a %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" combined"
```
4. 重启Apache。  

```
systemctl restart httpd
```
5. 查看httpd的访问日志，您可以获取真实的来访者IP。

### 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：

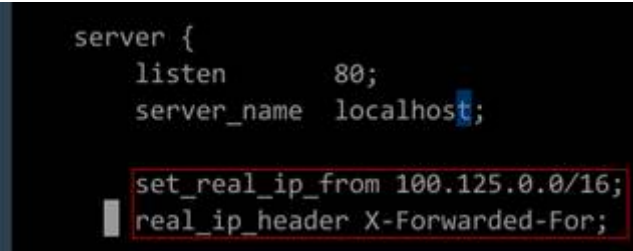
1. 运行以下命令安装http\_realip\_module。  

```
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.conf文件。  

```
vi /path/server/nginx/conf/nginx.conf
```
3. 在以下配置信息后添加新的配置字段和信息。  
在http或者server处，需要添加的配置字段和信息：  

```
set_real_ip_from 100.125.0.0/16;  
real_ip_header X-Forwarded-For;
```

图 10-14 添加配置字段和信息示例图



```
server {  
    listen      80;  
    server_name localhost;  
  
    set_real_ip_from 100.125.0.0/16;  
    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>，如负载均衡的IP地址段 100.125.0.0/16（100.125.0.0/16是负载均衡服务保留地址，其他用户无法分配到该网段内，不会存在安全风险）和高防IP地址段。多个IP地址段用逗号分隔。

4. 启动Nginx。  

```
/path/server/nginx/sbin/nginx
```
5. 查看Nginx的访问日志，您可以获取真实的来访者IP。  

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

### 配置Tomcat服务器

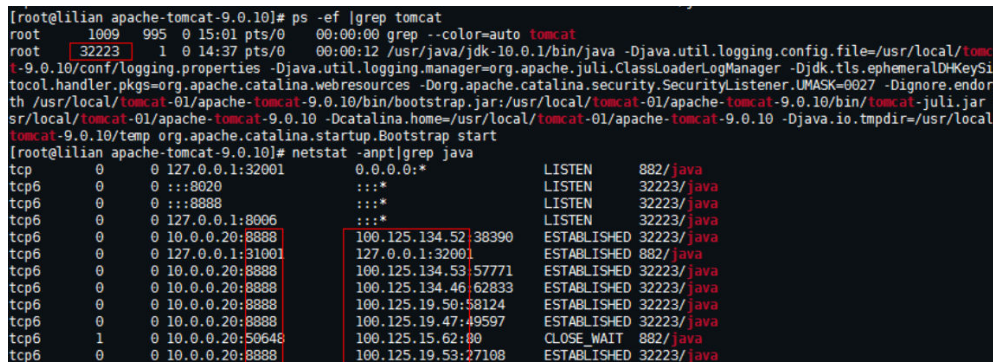
本教程中的Tomcat的安装路径为“/usr/tomcat/tomcat8/”。



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 10-15 正常运行结果示例

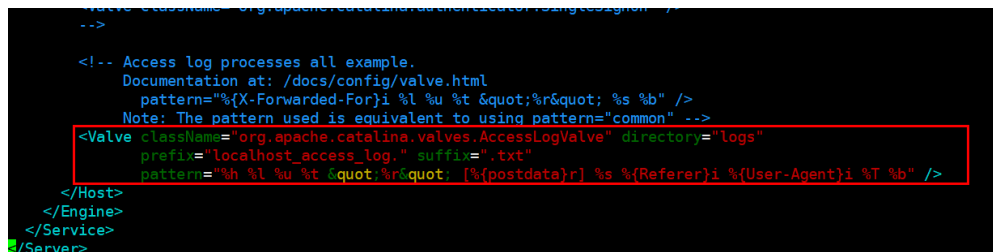


```
[root@lilian apache-tomcat-9.0.10]# ps -ef |grep tomcat
root      1009   995   0 15:01 pts/0    00:00:00 grep --color=auto tomcat
root      32223   1   0 14:37 pts/0    00:00:12 /usr/java/jdk-10.0.1/bin/java -Djava.util.logging.config.file=/usr/local/tomcat-9.0.10/conf/logging.properties -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager -Djdk.tls.ephemeralDHKeySize=1024 -Djava.protocol.handler.pkgs=org.apache.catalina.webresources -Dorg.apache.catalina.security.SecurityListener.Umask=0027 -Dignore.endorsed.dirs=/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:/usr/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 0.0.0.0:8822->0.0.0.0: LISTEN    882/java
tcp6       0      0 :::8822->::: LISTEN    32223/java
tcp6       0      0 :::8888->::: LISTEN    32223/java
tcp6       0      0 127.0.0.1:8806->::: 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. 选择修改server.xml文件，添加如下配置项。  

```
<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 10-16 配置示例



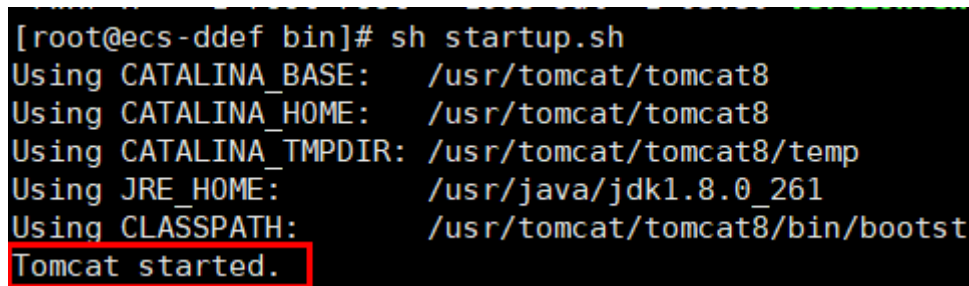
```
<!-- Access log processes all example.
Documentation at: /docs/config/valve.html
pattern="%{X-Forwarded-For}i %l %u %t %r %s %b" />
Note: The pattern used is equivalent to using pattern="common" -->
<Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
prefix="localhost_access_log." suffix=".txt"
pattern="%h %l %u %t %r %s %b %D %q [%{postdata}r] %s %{Referer}i %T %b" />
</Host>
</Engine>
</Service>
</Server>
```

4. 执行如下命令，重启Tomcat服务。  

```
cd /usr/tomcat/tomcat8/bin && sh startup.sh
```

其中“/usr/tomcat/tomcat8/”为Tomcat安装路径，请根据实际情况替换。

图 10-17 重启 Tomcat 服务



```
[root@ecs-ddef bin]# sh startup.sh
Using CATALINA_BASE:   /usr/tomcat/tomcat8
Using CATALINA_HOME:   /usr/tomcat/tomcat8
Using CATALINA_TMPDIR: /usr/tomcat/tomcat8/temp
Using JRE_HOME:        /usr/java/jdk1.8.0_261
Using CLASSPATH:       /usr/tomcat/tomcat8/bin/bootstrap.jar
Tomcat started.
```

5. 执行如下命令，查看最新的日志。  
如图中红框所示获取到的非100.125网段的IP地址，即为获取到的源IP地址。  

```
cat localhost_access_log..2020-09-10.txt
```

其中“localhost\_access\_log..2020-09-10.txt”为当天日志路径，请根据实际情况替换。

图 10-18 查询源 IP 地址

```
[root@ecs-ddef logs]# cat localhost_access_log..2020-09-10.txt
100.125.24.44 - - [10/Sep/2020:20:35:18 +0800] "GET / HTTP/1.1" [-]
100.125.24.43 - - [10/Sep/2020:20:35:18 +0800] "GET / HTTP/1.1" [-]
100.125.24.42 - - [10/Sep/2020:20:35:23 +0800] "GET / HTTP/1.1" [-]
100.125.24.44 - - [10/Sep/2020:20:35:23 +0800] "GET / HTTP/1.1" [-]
100.125.24.43 - - [10/Sep/2020:20:35:23 +0800] "GET / HTTP/1.1" [-]
10. . . .94 - - [10/Sep/2020:20:50:54 +0800] "GET / HTTP/1.1" [-]
10. . . .94 - - [10/Sep/2020:20:54:46 +0800] "GET / HTTP/1.1" [-]
10. . . .94 - - [10/Sep/2020:21:10:43 +0800] "GET / HTTP/1.1" [-]
10. . . .94 - - [10/Sep/2020:21:12:17 +0800] "GET / HTTP/1.1" [-]
```

## 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。  
<https://www.microsoft.com/zh-cn/download/confirmation.aspx?id=1038>
2. 自行下载F5XForwardedFor.dll插件，并根将获取到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 10-19 选择模块选项

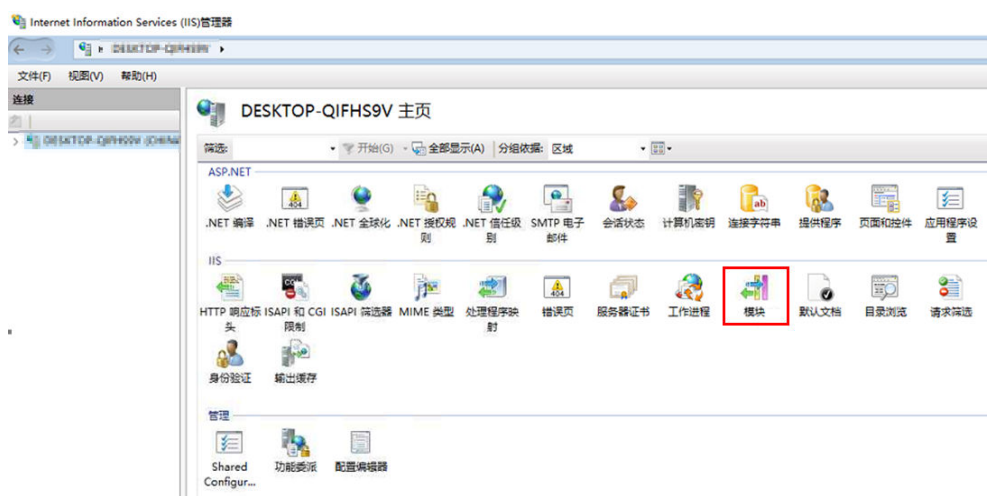
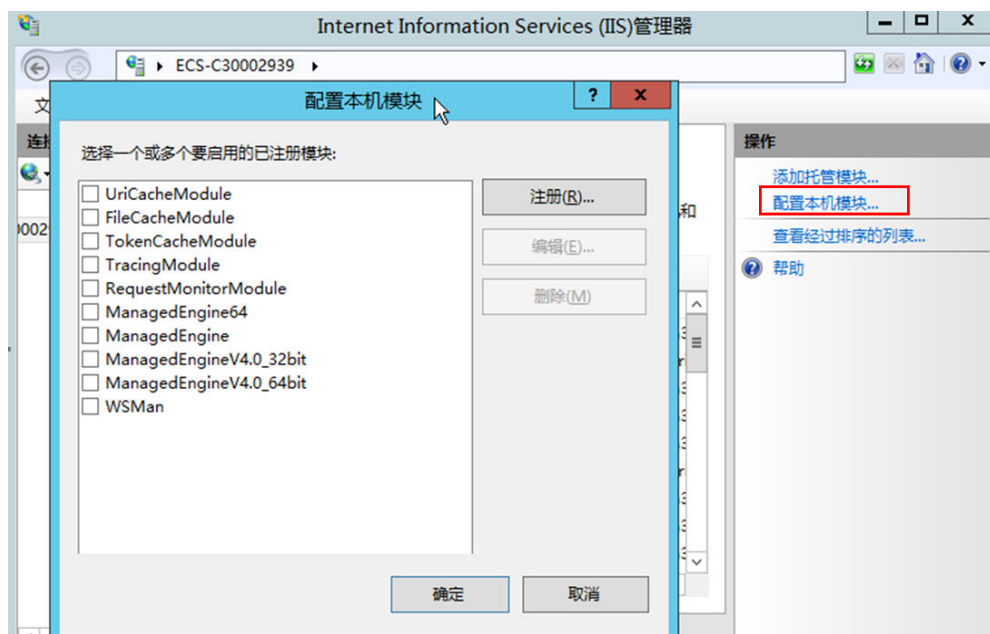
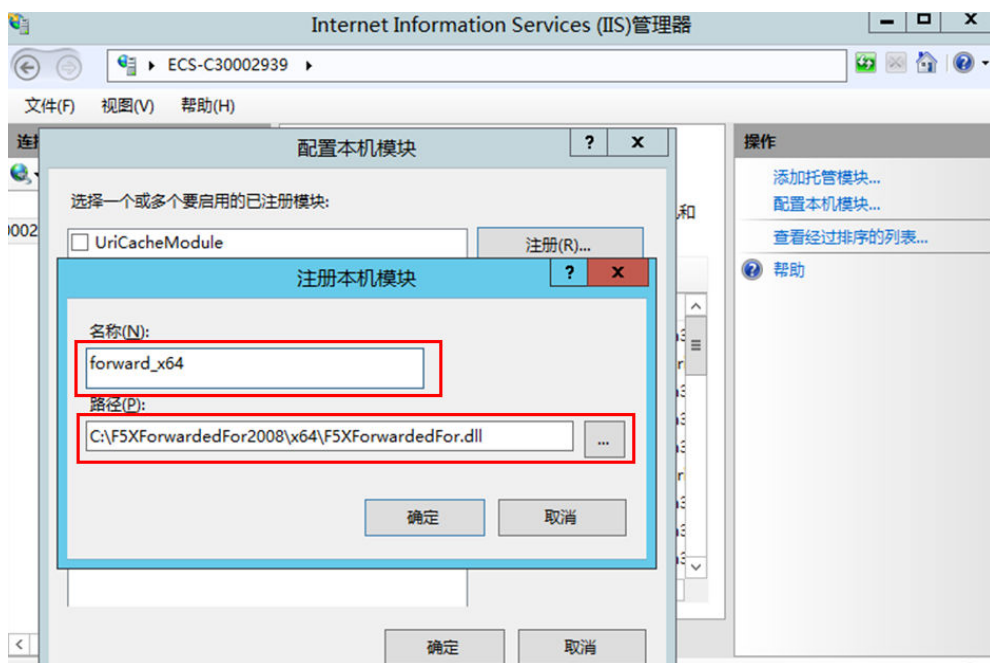


图 10-20 配置本机模块



4. 单击“注册”，分别注册x86和x64插件。

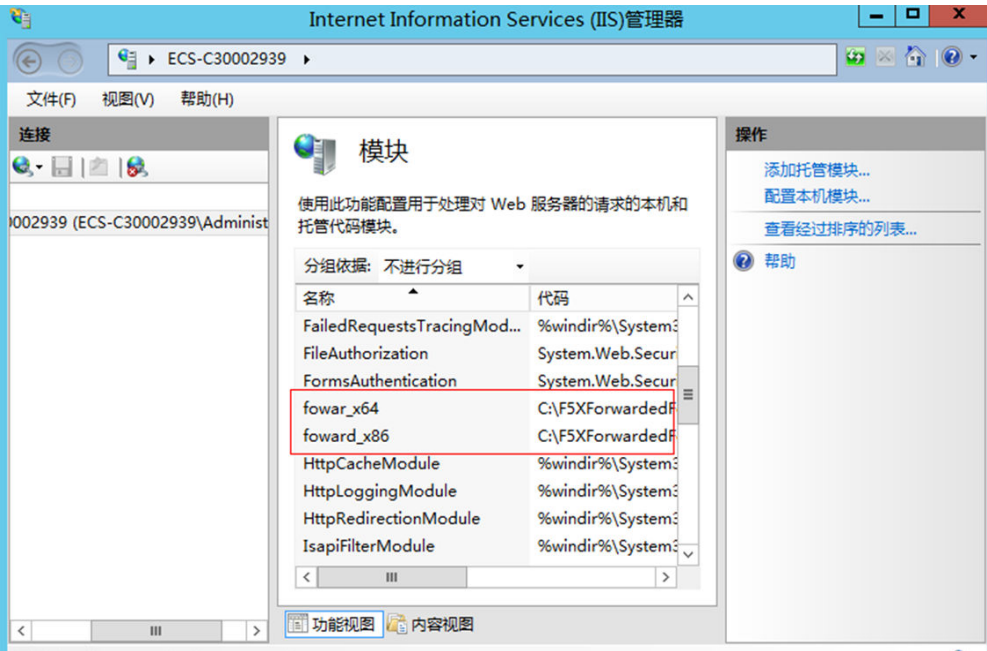
图 10-21 注册插件



5. 在“模块”页面，确认注册的模块名称出现在列表中。

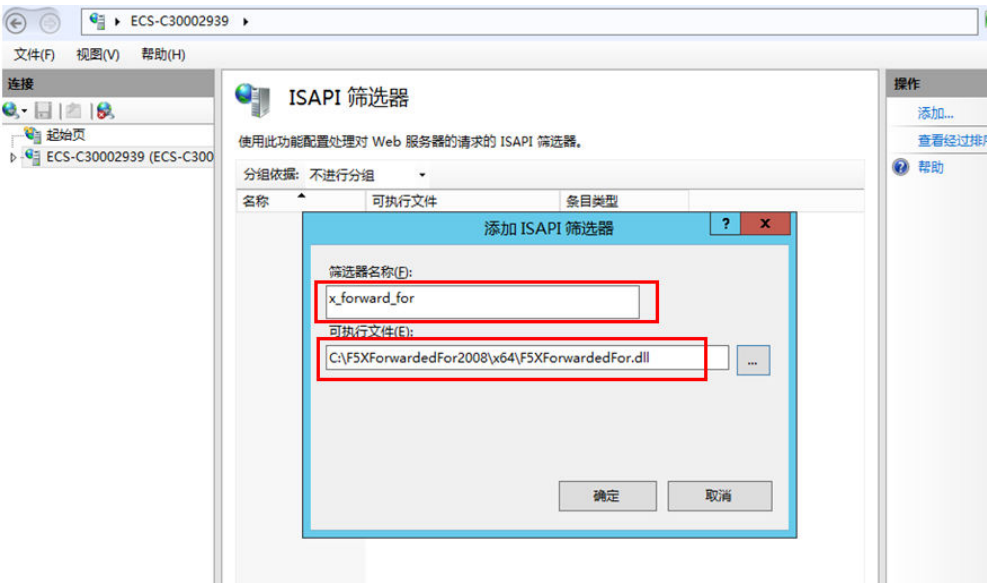


图 10-22 确认注册成功



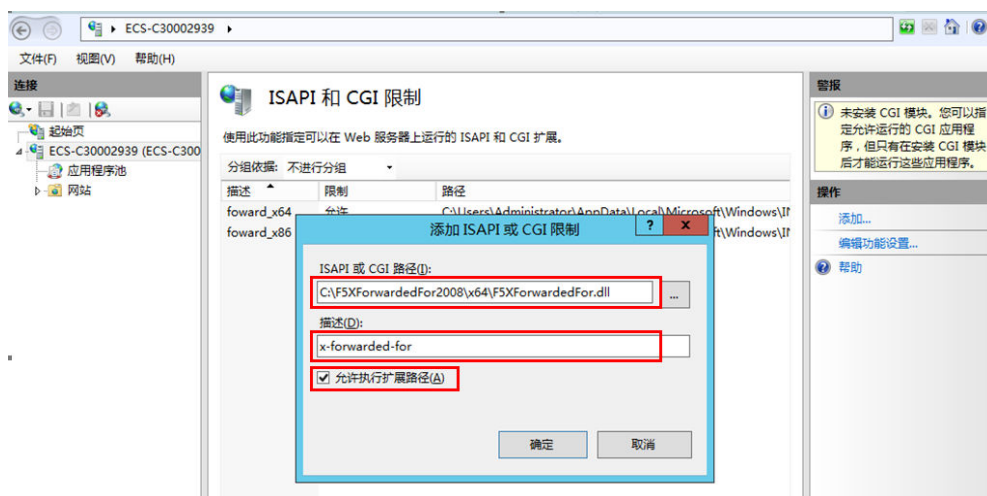
6. 选择IIS管理器主页的“ISAPI筛选器”，为2个插件授权运行ISAPI和CGI扩展。

图 10-23 添加授权



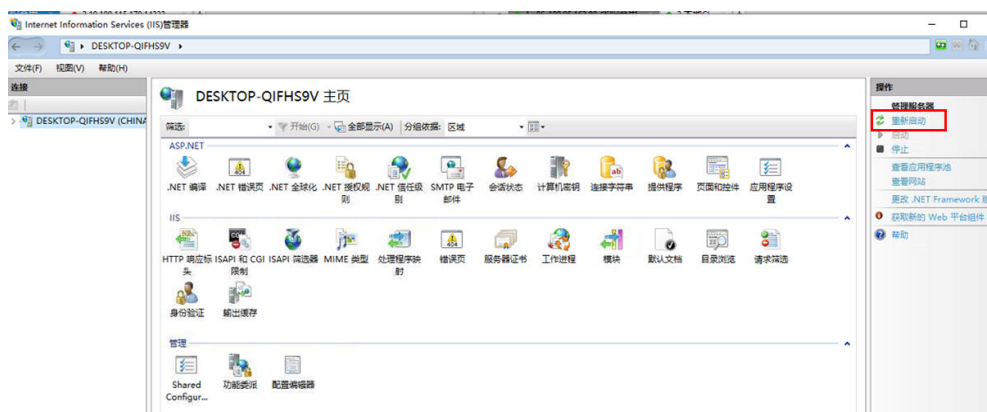
7. 选择“ISAPI和CGI限制”，为2个插件设置执行权限。

图 10-24 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 10-25 重启 IIS 服务



## 四层服务

针对四层（TCP协议）服务，需要配置TOA插件获取。配置TOA插件请参考[TOA插件配置](#)。

## 10.8 HTTP/HTTPS 监听器

### 10.8.1 为什么配置证书后仍出现不安全提示？

可能由于以下原因导致配置证书后仍出现不安全提示。

- 证书所记录的域名与用户访问的域名不一致，建议排查证书所记录的域名，或创建自签名证书。
- 配置了SNI，输入的域名与证书所记录的域名不一致。
- 域名级别与证书级别不一致，例如域名为5级而证书为4级。

其他情况您也可以使用 `curl` 访问的域名命令，根据系统返回的错误信息进行排查。

## 10.9 会话保持

### 10.9.1 如何检查弹性负载均衡会话保持不生效问题？

1. 查看后端服务器组上是否开启了会话保持。
2. 查看后端云服务器的健康检查状态是否正常，如果异常，流量会切换到其他后端云服务器，导致会话保持失效。
3. 如果选择的是源IP算法，需要注意请求到达弹性负载均衡之前IP是否发生变化。
4. 如果是HTTP或HTTPS监听器，配置了会话保持，需要注意发送的请求是否带有cookie，如果带有cookie，则观察该cookie值是否发生了变化（因为7层会话保持基于cookie）。

### 10.9.2 ELB 支持什么类型的会话保持？

负载均衡器支持源IP、负载均衡器cookie、应用程序cookie三种会话保持类型。

# 11 附录

## 11.1 TOA 插件配置

### 操作场景

ELB可以针对客户访问的业务为访问者提供个性化的管理策略，制定策略之前需要获取来访者的真实IP。TOA内核模块主要用来获取ELB转化过的访问者真实IP地址（仅支持IPv4），该插件安装在ELB后端服务器。

本文档仅适用于四层（TCP协议）服务，当客户需要在操作系统中编译TOA内核模块时，可参考本文档进行配置。

Linux内核版本为2.6.32和Linux内核版本为3.0以上的操作系统，在配置TOA内核模块的操作步骤上有所区别，具体操作请参照相应的操作步骤进行配置。

#### 说明

- TOA不支持UDP协议的监听器。
- TOA模块在以下操作系统中验证可以正常工作，其他内核版本安装方法类似。
  - CentOS 6.8 (Kernel version 2.6.32)
  - Suse 11 sp3 (Kernel version 3.0.76)
  - CentOS 7/7.2 (Kernel version 3.10.0)
  - Ubuntu 16.04.3 (Kernel version 4.4.0)
  - Ubuntu 18.04 (Kernel version 4.15.0)
  - OpenSUSE 42.2 (Kernel version 4.4.36)
  - CoreOS 10.10.5 (Kernel version 4.9.16)
  - Debian 8.2.0 (Kernel version 3.16.0)

### 前提条件

- 编译内核模块开发环境需与当前内核版本开发环境一致。
- 确保虚拟机可以访问开放源。
- 如果是非root用户，需拥有sudo权限。

## 操作步骤

- 以下操作步骤是针对Linux内核版本为3.0以上的操作系统。

### 1. 准备编译环境。

#### 说明

安装内核模块开发包的过程中，如果源里面找不到对应内核版本的安装包，需要自行去网上下载需要的安装包。

以下是不同Linux发行版本的操作说明，请根据环境选择对应的方案。

#### - CentOS环境下的操作步骤。

- i. 执行如下命令，安装gcc编译器。

```
sudo yum install gcc
```

- ii. 执行如下命令，安装make工具。

```
sudo yum install make
```

- iii. 执行如下命令，安装内核模块开发包，开发包头文件与库的版本需要与内核版本一致。

```
sudo yum install kernel-devel-`uname -r`
```

#### 说明

如果自带源里没有对应的内核开发包，可以到如下地址中去下载对应的rpm包。

地址：[https://mirror.netcologne.de/oracle-linux-repos/ol7\\_latest/getPackage/](https://mirror.netcologne.de/oracle-linux-repos/ol7_latest/getPackage/)

以3.10.0-693.11.1.el7.x86\_64为例，下载后执行以下命令安装：

```
rpm -ivh kernel-devel-3.10.0-693.11.1.el7.x86_64.rpm
```

#### - Ubuntu、Debian环境下的操作步骤。

- i. 执行如下命令，安装gcc编译器。

```
sudo apt-get install gcc
```

- ii. 执行如下命令，安装make工具。

```
sudo apt-get install make
```

- iii. 执行如下命令，安装内核模块开发包，开发包头文件与库的版本需要与内核版本一致。

```
sudo apt-get install linux-headers-`uname -r`
```

#### - SUSE环境下的操作步骤。

- i. 执行如下命令，安装gcc编译器。

```
sudo zypper install gcc
```

- ii. 执行如下命令，安装make工具。

```
sudo zypper install make
```

- iii. 执行如下命令，安装内核模块开发包，开发包头文件与库的版本需要与内核版本一致。

```
sudo zypper install kernel-default-devel
```

#### - CoreOS环境下的操作步骤。

CoreOS环境下在容器内进行内核模块的编译时，需要先启动一个用于内核模块开发的容器，然后再进行编译。

详细过程参见CoreOS官方文档，获取方式如下链接所示。

<https://coreos.com/os/docs/latest/kernel-modules.html>

## 2. 编译内核模块

- a. 使用git工具，执行如下命令，下载TOA内核模块源代码。

**git clone [https://github.com/Huawei/TCP\\_option\\_address.git](https://github.com/Huawei/TCP_option_address.git)**

### 说明

如果未安装git工具，请进入以下链接下载TOA模块源代码。

[https://github.com/Huawei/TCP\\_option\\_address](https://github.com/Huawei/TCP_option_address)

- b. 执行如下命令，进入源码目录，编译模块。

**cd src**

**make**

编译过程未提示warning或者error，说明编译成功，检查当前目录下是否已经生成toa.ko文件。

### 说明

如果报错提示“config\_retpoline=y but not supported by the compiler, Compiler update recommended”，表明gcc版本过老，建议将gcc升级为较新版本

## 3. 加载内核模块

- a. 执行如下命令，加载内核模块。

**sudo insmod toa.ko**

- b. 执行如下命令，验证模块加载情况，查看内核输出信息。

**dmesg | grep TOA**

若提示信息包含“TOA: toa loaded”，说明内核模块加载成功。

### 说明

CoreOS在容器中编译完内核模块后，需要将内核模块复制到宿主系统，然后在宿主系统中加载内核模块。由于编译内核模块的容器和宿主系统共享/lib/modules目录，可以在容器中将内核模块复制到该目录下，以供宿主系统使用。

## 4. 自动加载内核模块

为了使TOA内核模块在系统启动时生效，可以将加载TOA内核模块的命令加到客户的启动脚本中。

自动加载内核模块的方法有以下两种方法：

- 客户可以根据自身需求，在自定义的启动脚本中添加加载TOA内核模块的命令。
- 参考以下操作步骤配置启动脚本。

- i. 在“/etc/sysconfig/modules/”目录下新建toa.modules文件。该文件包含了TOA内核模块的加载脚本。

toa.modules文件内容，请参考如下示例：

**#!/bin/sh**

**/sbin/modinfo -F filename /root/toa/toa.ko > /dev/null 2>&1**

**if [ \$? -eq 0 ]; then**

**/sbin/insmod /root/toa/toa.ko**

**fi**

其中“/root/toa/toa.ko”为TOA内核模块文件的路径，客户需要将其替换为自己编译的TOA内核模块路径。

- ii. 执行以下命令，为toa.modules启动脚本添加可执行权限。

```
sudo chmod +x /etc/sysconfig/modules/toa.modules
```

#### 说明

客户升级内核后，会导致现有TOA内核模块不匹配，因此需要重新编译TOA内核模块。

### 5. 安装多节点

如果要在相同的客户操作系统中加载此内核模块，可以将toa.ko文件拷贝到需要加载此模块的虚拟机中，然后参照3步骤加载内核模块。

内核模块加载成功以后，应用程序可以正常获取访问者的真实源IP地址。

#### 说明

节点的操作系统发行版与内核版本必须相同。

### 6. 验证TOA内核模块

TOA内核模块安装成功后即可直接获取到源地址，此处提供一个验证的例子。

执行如下命令，在安装有python的后端服务器中启动一个简易的HTTP服务。

```
python -m SimpleHTTPServer port
```

其中，*port*需要与ELB添加该后端服务器时配置的端口一致，默认为80。

启动之后，通过客户端访问ELB的IP时，服务端的访问日志如下：

```
192.168.0.90 - - [06/Aug/2020 14:24:21] "GET / HTTP/1.1" 200 -
```

#### 说明

上述访问日志中192.168.0.90，即后端服务器可以获取到的客户端源IP地址。

- 以下操作步骤是针对Linux内核版本为2.6.32的操作系统。

#### 说明

TOA插件支持2.6.32-xx内核版本的操作系统（CentOS 6.8镜像）。参考如下步骤，进行配置。

1. 从以下网站中获取含有TOA模块的内核源代码包（Linux-2.6.32-220.23.1.el6.x86\_64.rs.src.tar.gz）。

[http://kb.linuxvirtualserver.org/images/3/34/Linux-2.6.32-220.23.1.el6.x86\\_64.rs.src.tar.gz](http://kb.linuxvirtualserver.org/images/3/34/Linux-2.6.32-220.23.1.el6.x86_64.rs.src.tar.gz)

2. 解压TOA模块的内核源代码包。

3. 修改编译相关参数。

- a. 进入“linux-2.6.32-220.23.1.el6.x86\_64.rs”文件夹。

- b. 编辑“net/toa/toa.h”文件。

将#define TCPOPT\_TOA200配置项修改为#define TCPOPT\_TOA254

- c. 在shell页面，执行以下命令。

```
sed -i 's/CONFIG_IPV6=m/CONFIG_IPV6=y/g' .config
```

```
echo -e '\n# toa\nCONFIG_TOA=m' >> .config
```

配置之后IPV6模块将会被编译进内核中，TOA会被编译成单独内核模块，可以单独启动和停止。

- d. 编辑Makefile。

可在“EXTRAVERSION =”等号后加上自定义的一些说明，将会在“uname -r”中显示，例如-toa。



4. 执行以下命令，编译软件包。

```
make -j n
```

#### 📖 说明

*n*可以依据系统CPU核数配置相应的参数，例如：4核CPU，可配置为4，从而加快编译速度。

5. 执行以下命令，安装内核模块。

```
make modules_install
```

命令执行结果如图11-1所示。

图 11-1 安装内核模块

```
INSTALL /lib/firmware/kaweth/trigger_code_fix.bin
INSTALL /lib/firmware/ti_3410.fw
INSTALL /lib/firmware/ti_5052.fw
INSTALL /lib/firmware/mts_cdma.fw
INSTALL /lib/firmware/mts_gsm.fw
INSTALL /lib/firmware/mts_edge.fw
INSTALL /lib/firmware/edgeport/boot.fw
INSTALL /lib/firmware/edgeport/boot2.fw
INSTALL /lib/firmware/edgeport/down.fw
INSTALL /lib/firmware/edgeport/down2.fw
INSTALL /lib/firmware/edgeport/down3.bin
INSTALL /lib/firmware/whiteheat_loader.fw
INSTALL /lib/firmware/whiteheat.fw
INSTALL /lib/firmware/keyspan_pda/keyspan_pda.fw
INSTALL /lib/firmware/keyspan_pda/xircom_pgs.fw
DEPMOD 2.6.32-toa
```

6. 执行如下命令，安装内核。

```
make install
```

命令执行结果如图11-2所示。

图 11-2 安装内核

```
INSTALL /lib/firmware/keyspan_pda/xircom_pgs.fw
DEPMOD 2.6.32-toa
[root@SZX1000167219 linux-2.6.32-220.23.1.el6.x86_64.rs]# make install
sh /root/humin/linux-2.6.32-220.23.1.el6.x86_64.rs/arch/x86/boot/install.sh 2.6.32-toa arch/x86/boot/bzImage \
    System.map "/boot"
ERROR: modinfo: could not find module xen_procfs
ERROR: modinfo: could not find module ipv6
ERROR: modinfo: could not find module xen_scfront
ERROR: modinfo: could not find module xen_hcall
ERROR: modinfo: could not find module xen_balloon
[root@SZX1000167219 linux-2.6.32-220.23.1.el6.x86_64.rs]#
```

7. 打开“/boot/grub/grub.conf”文件，配置开机默认启动，如图11-3所示。
  - a. 将开机默认启动内核由第一个内核修改为第零个内核，即“default=1”修改为“default=0”。
  - b. 在新增的含有toa模块的vmlinuz-2.6.32-toa内核行末尾添加“nohz=off”参数。如果不关闭nohz，大压力下CPU0可能会消耗过高，导致压力不均匀



图 11-3 配置文件

```
default=1
timeout=5
splashimage=(hd0,1)/boot/grub/splash.xpm.gz
hiddenmenu
title Red Hat Enterprise Linux Server (2.6.32-toa)
    root (hd0,1)
    kernel /boot/vmlinuz-2.6.32-toa ro root=UUID=
et nohz=off
initrd /boot/initramfs-2.6.32-toa.img
```

c. 修改完成后保存退出，重启操作系统。

重启系统时，系统将加载vmlinuz-2.6.32-toa内核。

8. 待系统重启完成之后，执行以下命令加载TOA模块。

#### modprobe toa

建议将modprobe toa命令加入开机启动脚本，以及系统定时监控脚本中，如图11-4所示。

图 11-4 modprobe toa 命令

```
[root@SZX1000167219 ~]# modprobe toa
[root@SZX1000167219 ~]# lsmod |grep toa
toa                4203  0
[root@SZX1000167219 ~]#
```

TOA模块加载完成后，查询内核信息如图11-5所示。

图 11-5 查询内核

```
[root@SZX1000167219 ~]# uname -a
Linux SZX1000167219 2.6.32-toa #1 SMP Sat Oct 15 11:50:05 CST 2016 x86_64 x86_64 x86_64 GNU/Linux
```

9. 验证TOA内核模块

TOA内核模块安装成功后即可直接获取到源地址，此处提供一个验证的例子。执行如下命令，在安装有python的后端服务器中启动一个简易的HTTP服务。

**python -m SimpleHTTPServer port**

其中，*port*需要与ELB添加该后端服务器时配置的端口一致，默认为80。

启动之后，通过客户端访问ELB的IP时，服务端的访问日志如下：

```
192.168.0.90 -- [06/Aug/2020 14:24:21] "GET / HTTP/1.1" 200 -
```

#### 说明

上述访问日志中192.168.0.90，即后端服务器可以获取到的客户端源IP地址。

# 12 修订记录

版本日期	变更说明
2020-07-30	第一次正式发布。