弹性负载均衡

常见问题

文档版本	01
发布日期	2025-10-30

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 高频常见问题

2 异常检查

2.1 ELB 丢包异常自助排查

问题场景

使用弹性负载均衡服务时，如果您的业务出现丢包现象，可以参考本文进行自助排查。

排查思路

表 2-1 客户端丢包排查项

排查项	说明
排查项一：访问控制黑名单限制导致丢包	由于访问控制策略限制导致客户端请求丢包。
排查项二：通过IP类型后端负载存在并发连接限制导致丢包	由于IP类型后端的后端服务器存在并发连接数限制导致客户端请求丢包。
排查项三：能ping通ELB的IP地址，但实际业务丢包	通过ping命令无法确认后端服务器连通性导致客户端请求丢包。

排查项一：访问控制黑名单限制导致丢包

- 问题现象：仅部分特定IP可以正常访问，或仅部分特定IP无法正常访问。
- 问题分析：当您设置了访问控制策略并生效时：
  - 黑名单：黑名单IP地址组内的客户端将被ELB强制丢包。
  - 白名单：仅白名单IP地址组内的客户端可以正常访问，白名单IP地址组外的客户端将被ELB强制丢包。
- 解决方案：您可通过查看监控指标“黑白名单阻断数据包数”和“黑白名单阻断流量”判断是否有数据包因为访问控制策略黑白名单的限制导致丢包，查看监控

指标详情请参考**监控弹性负载均衡**。您可进一步确认您的访问控制策略配置正确，避免目标客户端被访问控制策略强制丢包。

排查项二：通过 IP 类型后端负载存在并发连接限制导致丢包

- 问题现象：通过IP类型后端进行业务转发时，实际业务量并未达到实例规格上限，但出现了访问失败或者丢包现象。
- 问题分析：由于IP类型后端添加的单个后端服务器最多支持100000并发连接数，当添加的IP类型后端服务器数量较小时，通过IP类型后端进行转发的并发连接数限制可能低于实例规格。
- 排查思路：您可以通过公式计算ELB实例通过IP类型后端负载场景的并发连接数限制。

  假如您有一个ELB实例，部署在两个可用区，添加了10个IP类型后端。通过IP类型后端转发时，并发连接数限制计算如下：

  - 单实例公网并发连接计算公式：100000并发连接数 × IP类型后端个数 × 可用区数量。

    本示例并发连接数限制：100000 × 10 × 2 = 2000000。
  - 由于私网场景下，当从创建ELB的AZ发起访问时，流量将被分配至本AZ中的ELB上。

    单实例私网并发连接计算公式：100000并发连接数 × IP类型后端个数。

    本示例并发连接数限制：100000 × 10 = 1000000。

  建议您确认实际业务量是否超过IP类型后端转发场景下的并发连接限制，您可以通过增加IP类型后端的数量来提高该场景下的并发连接数上限。

排查项三：能 ping 通 ELB 的 IP 地址，但实际业务丢包

- 问题现象：使用ping命令测试ELB的IP地址确认网络连通正常，但实际业务出现访问失败或者丢包。
- 问题分析：在ELB实例正常运行时，使用ping命令探测ELB的IP地址，ELB实例会响应 ICMP Echo请求，即能ping通。由于ping数据包不会转发至后端服务器，因此ping命令的结果无法反映后端服务器真实的连通状态。
- 解决方案：建议您不要依赖ping命令来判断ELB的可用性，您可以通过curl命令来测试ELB服务是否可用。

2.2 为什么通过负载均衡无法访问后端业务?

问题描述

当出现以下问题时，可以参考本章节排查解决。

- 可以直接访问后端业务，但是无法通过负载均衡访问后端业务。
- 通过私网IP可以访问负载均衡，但是公网IP无法访问负载均衡。
- 后端服务器健康检查异常。

背景介绍

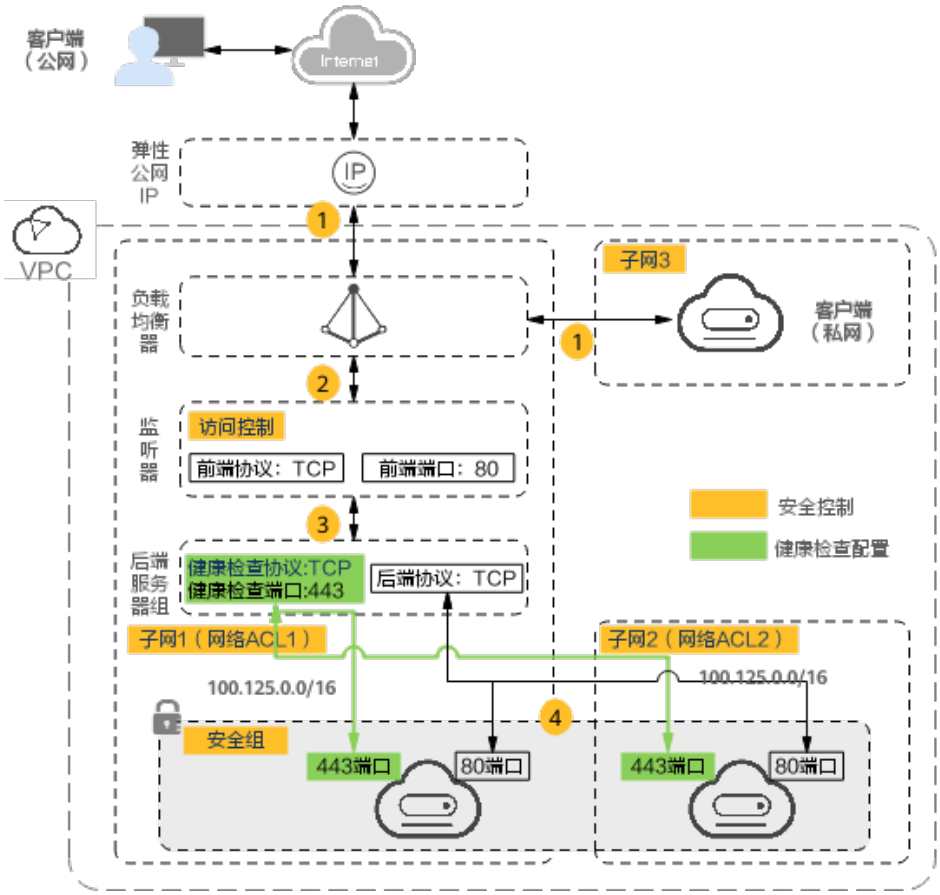
客户端通过负载均衡访问服务器示意图如**图2-1**。

1. 公网客户端的流量经过EIP传送到负载均衡器；私网客户端的流量直接通过私网IP传送到负载均衡器。
2. 负载均衡器根据监听器配置的前端协议/端口，将流量转发给匹配到的监听器。
3. 监听器首先判断后端服务器的健康检查是否正常，只有健康检查为正常时，才会转发流量给后端服务器。
4. 监听器会根据后端服务器的权重和分配策略，转发流量给相应的后端服务器。

通常情况下，客户端通过负载均衡器无法访问后端服务器可能原因包括安全控制（如黄色矩形框）和健康检查配置问题（如绿色矩形框）。

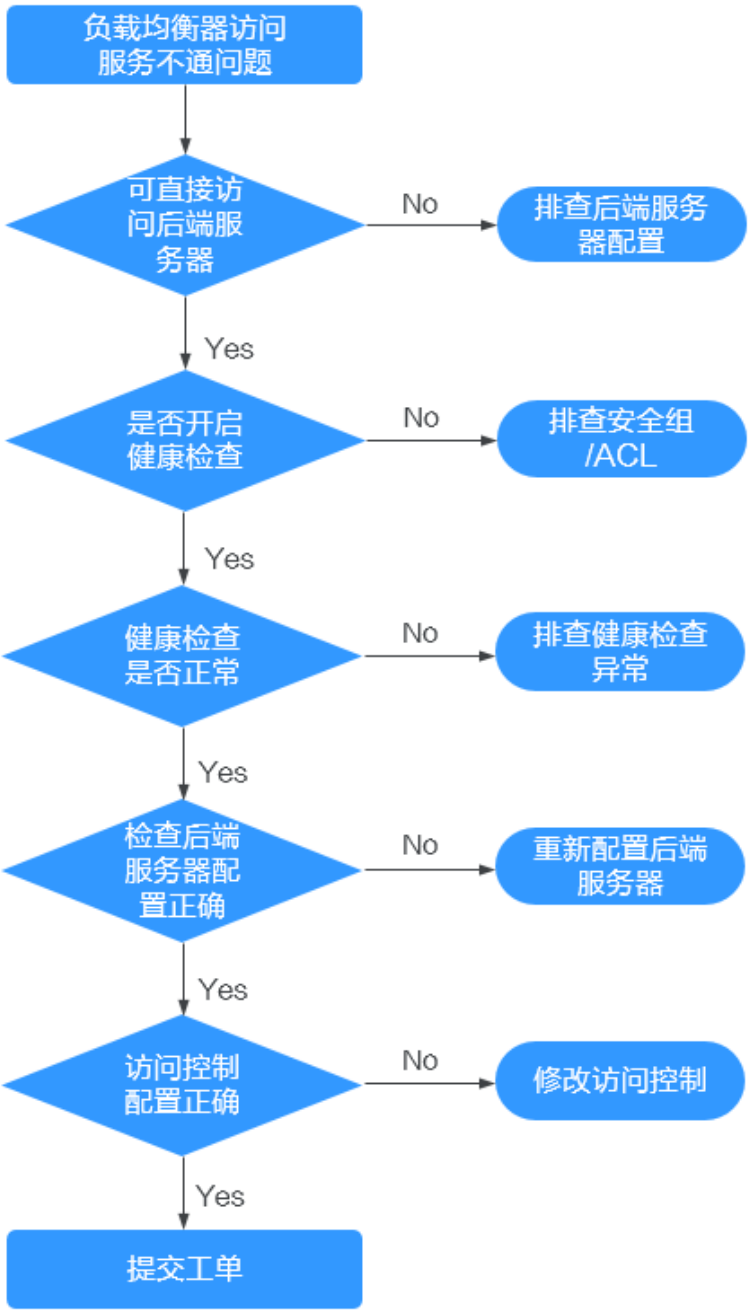
建议您按照从后端到前端的顺序进行排查，从而帮助您快速找到问题的原因。

图 2-1 客户端通过负载均衡访问后端服务器示意图



排查思路

图 2-2 排查思路



1. **步骤一：排查是否可直接访问后端服务器**：使用客户端直接访问后端服务器，确认后端服务器配置和业务配置无问题。
2. **步骤二：排查是否开启健康检查**：通过“监听器 > 后端服务器组”查看是否开启了健康检查选项。
3. **步骤三：排查健康检查是否正常**：通过“监听器 > 后端服务器组”查看服务器的健康检查结果是否为正常。健康检查异常的情况下，负载均衡不会向这台服务器转发流量。

4. **步骤四：排查后端服务器配置是否正确**：通过“监听器 > 后端服务器组”查看后端服务器的权重和业务端口是否配置正确。
5. **步骤五：检查访问控制配置是否正确**：通过“监听器 > 基本信息”查看是否开启了访问控制，以及访问控制是否限制了客户端的访问。

步骤一：排查是否可直接访问后端服务器

可以通过客户端直接访问后端服务器的IP地址来快速定界是ELB配置问题，还是后端服务器本身业务配置问题。使用客户端直接访问后端服务器时，请注意放通客户端到后端服务器之间的网络ACL。

- **公网客户端：**使用公网客户端访问后端服务器时，您需要为后端服务器暂时绑定EIP。待验证完成后，再释放此EIP。
- **私网客户端：**无需绑定EIP。如果是不同VPC的客户端访问，请注意配置VPC对等连接。

执行完成后，如果仍无法访问，请执行**步骤二：排查是否开启健康检查**。

步骤二：排查是否开启健康检查

当客户端直接访问后端服务器业务正常时，请检查负载均衡器是否开启了健康检查。当服务器开启了健康检查，而健康检查失败时，负载均衡器不会向此后端服务器转发流量。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
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，单击需要查看的负载均衡名称。
5. 在“监听器”页签下，查看是否已开启健康检查。
   - **已经开启健康检查：**请执行**步骤三：排查健康检查是否正常**。
   - **未开启健康检查：**
     - 共享型负载均衡：请检查后端服务器的安全组和网络ACL规则已经放通100.125.0.0/16网段。
     - 独享型负载均衡：请检查后端服务器的安全组已经放通ELB后端子网所在的VPC网段。

     此网段是ELB访问后端服务器使用的地址，不会存在安全风险。放通网段后，如果仍无法访问，请执行**步骤四：排查后端服务器配置是否正确**。

注意

- 共享型实例四层监听器开启“获取客户端IP”功能后，后端服务器安全组规则和网络ACL规则均无需放通100.125.0.0/16网段及客户端IP地址。
- 独享型负载均衡四层监听器未开启“IP类型后端”功能时，后端服务器安全组规则和网络ACL规则均无需放通ELB后端子网所在的VPC网段。

步骤三：排查健康检查是否正常

当服务器开启了健康检查，而健康检查失败时，负载均衡器不会向此后端服务器转发流量。

- **存在异常的后端服务器：**请参考**健康检查异常如何排查**进行排查。
- **无异常的后端服务器：**请执行**步骤四：排查后端服务器配置是否正确**。

执行完成后，如果仍无法访问，请执行**步骤四：排查后端服务器配置是否正确**。

步骤四：排查后端服务器配置是否正确

1. 在“后端服务器组 > 后端服务器”页面查看已添加的后端服务器的参数，重点观察以下参数：
   - **权重：**权重如果设置为0，则不会向这个服务器转发流量
   - **业务端口：**需要与实际的业务端口相同。
2. 在“监听器”页面，单击待查看的四层（TCP/UDP）监听器，查看是否打开了“获取客户端IP”选项。
   - 如果打开了此选项，ELB会直接使用客户端的真实IP访问后端服务器。此时需要在安全组和网络ACL中设置放通客户端的真实IP地址。

     此外，如果开启了“获取客户端IP”，不支持后端服务器和客户端使用同一台服务器，原因是后端服务器会根据报文源IP为本地IP判定该报文为本机发出的报文，无法将应答报文返回给ELB，最终导致回程流量不通。
   - 如果未开启“获取客户端IP”，需检查后端服务器安全组是否放通相应网段。
     - 对于独享型负载均衡，需要确保后端服务器放通独享型ELB后端子网所在的VPC网段。
     - 对于共享型负载均衡，需要确保后端服务器放通100.125.0.0/16网段。

执行完成后，如果仍无法访问，请执行**步骤五：检查访问控制配置是否正确**。

步骤五：检查访问控制配置是否正确

在监听器的“基本信息”页签，查看访问控制配置是否正确，是否已经放通了客户端的IP地址。

提交工单

如果上述方法均不能解决您的疑问，请**提交工单**寻求更多帮助。

2.3 为什么同一客户端同时访问不同 ELB 实例、IP 或端口会概率性超时?

问题描述

表 2-2 问题概述

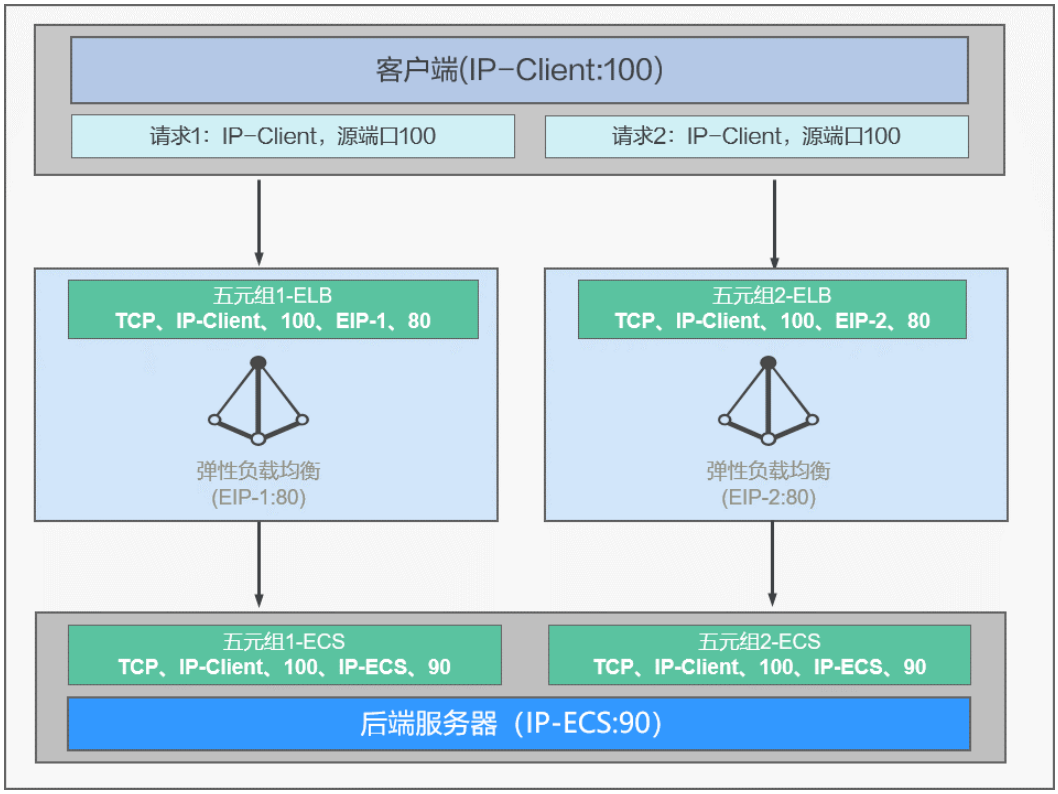
触发场景	• 多个四层ELB实例或同一四层ELB实例的多个监听器挂载相同后端服务器，同一客户端同时访问这些ELB实例。 • 开启全端口监听的监听器，同一客户端同时访问ELB实例不同的监听端口后转发到相同的后端服务器的相同端口。
问题现象	客户端概率性访问超时。
问题原因	在上述触发问题的场景中，同一个客户端通过ELB实例访问到**业务端口相同的后端服务器**时，后端服务器从弹性负载均衡处接收的客户端请求报文的源IP和源端口相同，出现请求报文的五元组冲突，从而导致访问失败或超时。

问题分析

什么场景下后端服务器上不同四层连接会出现五元组冲突?

- 客户端请求源端口硬编码为固定端口：客户端访问不同的弹性负载均衡时，客户端请求的源端口固定，例如固定为80端口。
- 客户端请求源端口由操作系统自动选择：由于客户端访问不同的弹性负载均衡，即访问的目的IP地址不同，从而导致操作系统选择的客户端请求源端口可能相同。

图 2-3 后端服务器接收请求报文五元组冲突示意图



同一客户端通过两个负载均衡器访问同一个后端服务器，客户端请求源端口相同且弹性负载均衡已开启获取客户端IP（DNAT模式）功能时，连接建立过程如图2-3。

1. 客户端发出源IP（IP-client）和源端口(100)相同的TCP请求1和TCP请求2到两个弹性负载均衡的公网IP地址EIP-1（12.xx.xx.xx）和EIP-2（13.xx.xx.xx）。
2. 两个弹性负载均衡的TCP监听端口都是80，收到的请求1和请求2的五元组报文如下：

   表 2-3 负载均衡器接收五元组详情

五元组报文	协议	源IP	源端口	目的IP	目的端口
五元组1-ELB	TCP	IP-Client	100	12.xx.xx.xx	80
五元组2-ELB	TCP	IP-Client	100	13.xx.xx.xx	80

3. 弹性负载均衡将接收到请求转发到同一台后端服务器（IP-ECS），该后端服务器配置的**业务端口**都是90。
4. 由于弹性负载均衡已开启获取客户端IP功能，源IP和源端口不会被修改，后端服务器接收到ELB转发的请求1和请求2，请求报文五元组如下：

表 2-4 后端服务器接收五元组详情

五元组报文	协议	源IP	源端口	目的IP	目的端口
五元组1-ECS	TCP	IP-Client	100	IP-ECS	90
五元组2-ECS	TCP	IP-Client	100	IP-ECS	90

5. 后端服务器接收到五元组报文相同的请求1和请求2，就会导致连接建立失败。

解决方案

为解决后端服务五元组冲突问题，客户端需要避免使用相同的源端口访问不同的实例或监听器，具体而言，您可采用以下措施：

- 客户端请求源端口硬编码为固定端口时：修改固定源端口配置，使客户端通过不同的固定端口访问不同的负载均衡器。
- 客户端请求源端口由操作系统自动选择时：
  - 允许客户端进行重试，客户端操作系统重连后，将通过不同的客户源端口发出请求，从而解决五元组冲突。
  - 若用户业务对重置连接极其敏感，需要更高的连接成功率，则请通过IP类型后端添加后端服务器。在IP类型后端场景下，产品底层基于FullNAT模式实现，获取客户端IP功能将会失效，源IP将会修改为负载均衡器后端子网中的IP地址。此时，若用户有获取客户端真实源IP的诉求，请通过配置TOA插件获取，详情请参见**TOA插件配置**。
- 在多组监听场景下，避免监听器使用相同的后端服务器。

2.4 为什么同一客户端同时访问绑定了多个 EIP 的 ELB 实例会概率性超时?

问题描述

表 2-5 问题概述

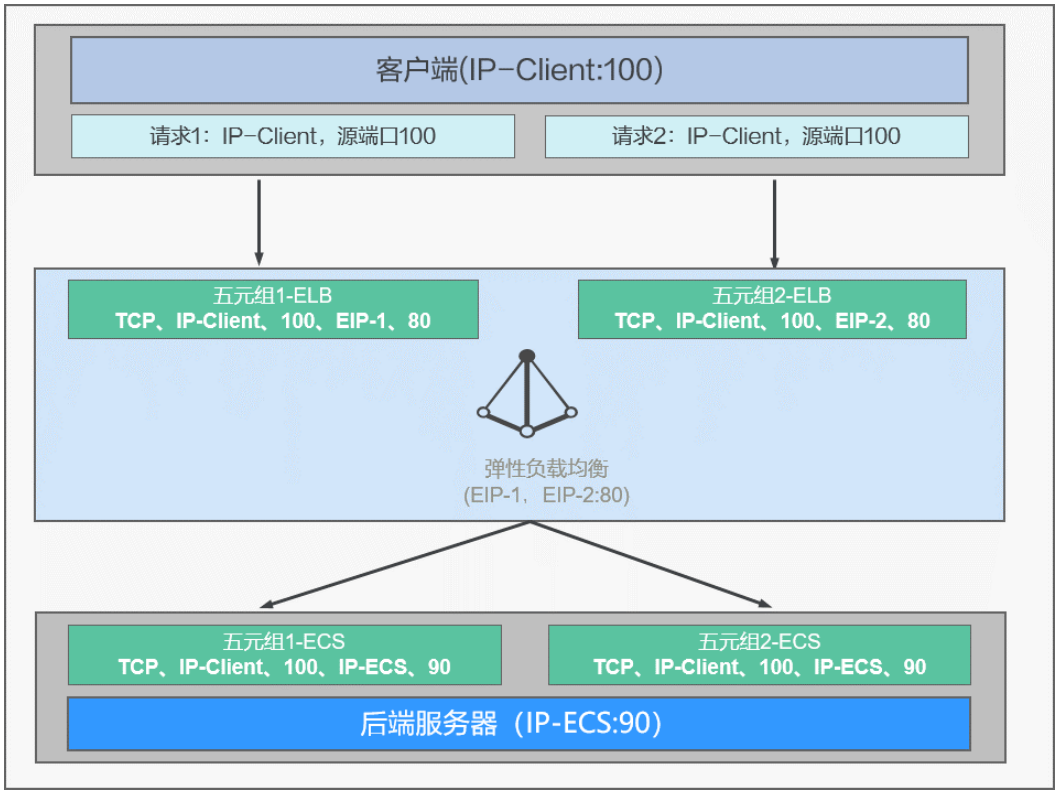
触发场景	同一四层ELB实例具有多个弹性公网IP地址，同一客户端通过不同的公网IP地址同时访问到这个ELB实例相同的监听端口。
问题现象	客户端请求概率性访问超时或连接被重置。
问题原因	同一个客户端通过不同的EIP访问ELB实例时，通过相同的监听端口访问到**相同的后端服务器**时，出现请求报文的五元组冲突，从而导致访问失败或超时。

问题分析

当ELB绑定了多个EIP时，什么场景下后端服务器上不同四层连接会出现五元组冲突?

- 客户端请求源端口硬编码为固定端口：客户端访问同一弹性负载均衡的不同EIP时，客户端请求的源端口固定，例如固定为80端口。
- 客户端请求源端口由操作系统自动选择：由于客户端访问不同的EIP，即访问的目的IP地址不同，从而导致操作系统选择的客户端请求源端口可能相同。

图 2-4 ELB 绑定多个 EIP 时，后端服务器接收请求报文五元组冲突示意图



同一客户端通过**两个不同的EIP**访问到负载均衡器的**同一个后端服务器**，客户端请求源端口相同且弹性负载均衡已开启获取客户端IP（DNAT模式）功能时，连接建立过程如图2-4。

1. 客户端发出源IP（IP-client）和源端口(100)相同的TCP请求1和TCP请求2通过**EIP-1**（12.xx.xx.xx）和**EIP-2**（13.xx.xx.xx）到达弹性负载均衡。
2. 弹性负载均衡的TCP监听端口是80，收到的请求1和请求2的五元组报文如下：

   表 2-6 负载均衡器接收五元组详情

五元组报文	协议	源IP	源端口	目的IP	目的端口
五元组1-ELB	TCP	IP-Client	100	12.xx.xx.xx	80
五元组2-ELB	TCP	IP-Client	100	13.xx.xx.xx	80

3. 弹性负载均衡将接收到请求转发到同一台后端服务器（IP-ECS），该后端服务器配置的**业务端口**都是90。

4. 由于弹性负载均衡已开启获取客户端IP功能，**源IP和源端口不会被修改**，后端服务器接收到ELB转发的请求1和请求2，请求报文五元组如下：

   表 2-7 后端服务器接收五元组详情

五元组报文	协议	源IP	源端口	目的IP	目的端口
五元组1-ECS	TCP	IP-Client	100	IP-ECS	90
五元组2-ECS	TCP	IP-Client	100	IP-ECS	90

5. 后端服务器接收到五元组报文相同的请求1和请求2，就会导致连接建立失败。

解决方案

为解决后端服务五元组冲突问题，客户端需要避免使用相同的源端口访问不同的实例或监听器，具体而言，您可采用以下措施：

- 客户端请求源端口由操作系统自动选择时：
  - 允许客户端进行重试，客户端操作系统重连后，将通过不同的客户源端口发出请求，从而解决五元组冲突。
  - 若用户业务对重置连接极其敏感，需要更高的连接成功率，则请通过**IP类型后端**添加后端服务器。在IP类型后端场景下，产品底层基于FullNAT模式实现，获取客户端IP功能将会失效，源IP将会修改为负载均衡器后端子网中的IP地址。此时，若用户有获取客户端真实源IP的诉求，请通过配置TOA插件获取，详情请参见**TOA插件配置**。
- 在**ELB绑定多个EIP**使用的业务场景下，避免同一客户端发送请求到不同的EIP，多个EIP推荐用于容灾场景的业务部署。

2.5 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。请您排查并解决健康检查异常问题后，再重新访问ELB。
2. 检查安全组规则是否放通了对应的网段：
   - 对于独享型负载均衡，检查后端服务器所在的安全组入方向是否放通ELB后端子网所属网段。
   - 对于共享型负载均衡，检查客户后端服务安全组入方向是否放通了100.125.0.0/16网段。

⚠ 注意

- 共享型实例四层监听器开启“获取客户端IP”功能后，后端服务器安全组规则和网络ACL规则均无需放通100.125.0.0/16网段及客户端IP地址。
- 独享型负载均衡四层监听器未开启“IP类型后端”功能时，后端服务器安全组规则和网络ACL规则均无需放通ELB后端子网所属网段。

3. 检查ELB与客户端之间是否是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，ELB会向客户端和服务端发送RST断开连接。
4. 检查是否开启了会话保持，且会话保持类型选择的是源IP地址。如果是，需要注意请求到达ELB之前，请求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. 检查是否是HTTP/HTTPS监听器，并配置了会话保持。如果是，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. 检查后端服务器组的会话保持是否超时。如果您开启了会话保持且未修改默认的会话保持时间，那么四层监听器和七层监听器的后端服务器组默认会话保持时间是20分钟，超时后会断开连接。
7. 检查您访问ELB的服务器是否为后端服务器。

   四层监听器（TCP/UDP）开启“获取客户端IP”功能之后，不支持同一台服务器既作为后端服务器又作为客户端的场景。
8. 检查您是否通过IP类型后端功能添加了后端服务器。如果是，需要确认在ELB所在的VPC和后端服务器所在的VPC之间是否建立了对等连接。
9. 请检查您的账户是否欠费，欠费会导致EIP等付费资源被冻结，而无法使用。

2.6 如何排查 ELB 返回的异常状态码?

ELB返回的常见异常状态码有400、403、502、504等。若遇到这些状态码建议您先直接访问后端服务器，查看后端服务器是否异常。

若后端服务器响应正常，在遇到ELB返回异常状态码时请参考**表2-8**的可能原因进行排查。如果仍无法解决，请联系客服人员继续排查。

表 2-8 ELB 常见状态码

状态码	含义	可能原因
400	错误请求	• 客户端发送的请求格式不符合HTTP规范。 • 向HTTPS服务发送了HTTP请求。 • 请求头超出64K限制。
401	未授权	一般是后端服务器返回，后端服务器鉴权失败。
403	禁止访问	一般是后端服务器返回，后端服务器拦截了该请求。
404	资源未找到	• 后端服务器返回错误码，需排查后端服务器业务。 • ELB转发策略配置不正确，未指定到正确的后端服务器。
408	请求超时	客户端超过请求超时时间（默认60s）未发送请求。发送TCP keep-alive不会阻止此超时。
413	有效负载过大	客户端发送的请求body体超过10GB。
414	URI过长	客户端发送的请求URL或查询字符串参数过大。

状态码	含义	可能原因
499	客户端主动断开连接	ELB还未将响应信息返回给客户端，客户端主动断开连接。此错误码仅记录在访问日志中。
500	服务器内部错误	后端服务器返回，为服务器内部错误。
501	未实现	ELB服务无法识别此请求。 ELB仅支持Transfer-Encoding标头的chunked和identity，建议您使用 Content-Encoding 标头代替。
502	无效网关	• ELB未正确配置后端服务器的监听通信端口。 • ELB在尝试建立连接或向后端服务发送数据时从后端服务器收到了 TCP RST。 • 后端服务器响应格式错误，或者包含无效的 HTTP 响应头。 • 未正确配置后端服务器，例如未正确配置路由、网络ACL等。
503	服务不可用	一般是后端返回，表示后端服务不可用。
504	网关超时	• 首次连接时，ELB未能在连接超时到期之前 (默认为5s) 建立与后端服务器的连接。 • ELB与后端服务器建立了连接，但在响应超时时间（默认为300s）到期之前未响应。 • 子网的网络ACL未放通ELB到后端服务器的访问规则。

2.7 如何排查 ELB 返回至客户端的异常请求头?

在异常返回码的基础上，ELB会将典型的异常情况通过“x-router-code” header头通知客户端，常见的有40000，40001，50000， 50001，您可以参考下表排查异常header值的可能原因：

表 2-9 ELB 返回至客户端的异常请求头

header值	含义	可能原因
40000	默认后端服务器组没有配置后端后端服务器	• 客户端请求没有命中任何转发策略。 • 后端服务器组没有配置后端服务器。
40001	转发策略对应的后端服务器组没有配置后端服务器	• 客户端请求命中了错误的转发策略。 • 转发策略对应的后端服务器组没有配置后端服务器。

header值	含义	可能原因
50000	ELB的后端服务器全都不可用	• 健康检查配置异常，导致ELB认为后端服务器异常不可用。 • 后端服务器自身异常不可用，需自行排查后端服务器。
50001	配置正在加载中	配置尚未加载完毕，请等待配置加载完成，稍后重试。

2.8 如何检查 ELB 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。因为这些请求可能因为是异常请求被弹性负载均衡拒绝，没有转发至后端服务器。

2.9 如何检查 ELB 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。

说明

一般情况下，影响负载均衡分配的因素包括分配策略、会话保持、长连接、权重等。换言之，最终是否均匀分配不仅与分配策略相关，还与使用的长短连接、后端的性能负载等相关。

2.10 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，超带宽会产生拥塞、丢包等异常情况。

   说明

   带宽超限指的是您的突发的流量超过了带宽基准的速率，并不是带宽被占满导致的。每个带宽都有基准的速率，超过这个速率就称为带宽超速的现象，这种情况下限速策略就会生效，会导致一定程度的丢包，这种情况需要您进一步排查业务情况或提升带宽的上限。
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。

2.11 如何检查 ELB 压测性能受限?

1. 检查后端服务器的负载状态，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。

   说明

   带宽超限指的是您的突发的流量超过了带宽基准的速率，并不是带宽被占满导致的。每个带宽都有基准的速率，超过这个速率就称为带宽超速的现象，这种情况下限速策略就会生效，会导致一定程度的丢包，这种情况需要您进一步排查业务情况或提升带宽的上限。
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。
5. 压测TLS监听器时，流量经过ELB后会进行源地址转换，ELB到单个后端服务器存在端口号数量约束，可能会导致TLS并发连接数达不到压测标准，建议添加多台后端服务器进行压测。

2.12 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，不用观察session是否丢失，而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）。

2.13 如何检查 SSL/TLS 认证异常?

当您使用ELB的HTTPS或TLS监听器时，可能会遇到SSL/TLS认证协商失败导致的错误。由于协商过程涉及多个步骤，因此可能出现多种错误，您可以参考以下内容从客户端收到响应进行排查。

本文以java语言为例，提供常见错误排查建议。

排查项一：服务器未提供证书满足客户端校验要求

- 报错信息：
  ```
  Exception in thread "main" javax.net.ssl.SSLHandshakeException: Received fatal alert: handshake_failure
  ```
- 异常原因：ELB服务器没有提供证书或者提供的证书不符合客户端的校验要求，导致握SSL/TLS手失败。
- 解决方案：

- 请检查监听器上配置的证书是否正确。
- 请确认监听器的TLS安全策略使用的加密套件是否满足客户端要求。

排查项二：证书验证报错

- 报错信息：
  ```
  Exception in thread "main" javax.net.ssl.SSLHandshakeException:
  sun.security.validator.ValidatorException: PKIX path building failed:
  sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to
  requested target
  ```
- 异常原因：服务器证书校验时，证书验证报错，可能是证书链不完整或证书颁发机构不受信任。
- 解决方案：将监听器的证书更换为有效的由证书颁发机构（CA）签发的证书。

排查项三：客户端收到的服务器证书主机名与请求主机名不匹配

- 报错信息：
  ```
  Exception in thread "main" javax.net.ssl.SSLHandshakeException:
  java.security.cert.CertificateException: No name matching localhost found
  ```
- 异常原因：通常发生在双向认证场景，客户端接收到服务器证书主机名与客户端请求连接的主机名不匹配，即验证localhost失败。
- 解决方案：请检查请求客户端是否携带包含localhost的证书。

排查项四：TLS 安全策略的版本不匹配

- 报错信息：
  ```
  Exception in thread "main" javax.net.ssl.SSLHandshakeException: No appropriate protocol (protocol is
  disabled or cipher suites are inappropriate)
  ```
- 异常原因：客户端和服务器之间无法找到共同支持的SSL/TLS协议版本或加密套件。
- 解决方案：请检查客户端和ELB监听器使用的TLS安全策略的TLS协议版本、加密套件的版本是否匹配。

3 健康检查

3.1 健康检查异常排查（独享型）

问题描述

客户端的请求通过负载均衡器的监听器访问后端服务器异常，监听器的健康检查列显示“异常”。

当健康检查探测到您的后端服务器异常时，ELB将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。

背景介绍

负载均衡器通过向后端服务器发起心跳检查的方式来实现健康检查功能，并判断后端服务器是否可用。更多检查原理详见**健康检查介绍**。

- 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。
- 当后端服务器的权重设置为0时：
  - 独享型负载均衡器：新的请求不会转发到该后端服务器，健康检查会继续探测，健康检查状态显示为实际结果。
  - 共享型负载均衡器：新的请求不会再转发到该后端服务器，健康检查状态显示为“异常”。

排查思路

负载均衡已提供自助问题诊断工具帮助用户定位健康检查异常问题，如果通过自助诊断工具排查仍然无法定位问题，请参考**表3-1**进一步排查。

因为健康检查包含检查间隔和阈值判断，相关配置的修改完成后需要等待一定的时间，配置才会生效。

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。

表 3-1 排查思路

排查手段	排查项目
自助诊断工具排查	后端服务器的安全组配置
	后端服务器子网的网络ACL配置
	健康检查参数配置
其他异常排查项	检查后端服务器组是否关联监听器
	检查ELB是否绑定EIP或私网IP
	检查后端服务器是否正常
	检查后端服务器防火墙
	检查后端服务器路由
	检查后端服务器负载
	检查后端服务器hosts.deny文件

后端服务器的安全组配置

独享型负载均衡的后端服务器安全组规则必须放通ELB用于健康检查的协议和端口和健康检查的源地址。

健康检查的协议和端口为用户在健康检查配置页面进行设置，您可在后端服务器组的基本信息页面查看。独享型负载均衡用于健康检查的源地址为ELB后端子网所在的VPC网段。

您可通过自助诊断工具后端服务器的安全组规则进行诊断。后端服务器安全组规则的检查项目如下表3-2所示。

表 3-2 安全组规则排查项目

排查项	处理措施
健康检查入方向源地址检查	请确保后端服务器的安全组入方向规则放通健康检查协议对应的传输层协议、健康检查端口和ELB后端子网所在的VPC网段。 配置指导详情见配置后端服务器的安全组（独享型）。
健康检查入方向端口检查	
健康检查入方向协议检查	
健康检查出方向源地址检查	默认的安全组出方向规则全部放通。如果您设置了出方向规则，请确保后端服务器的安全组出方向规则放通健康检查协议对应的传输层协议、健康检查端口和ELB后端子网所在的VPC网段。 配置指导详情见配置后端服务器的安全组（独享型）。
健康检查出方向端口检查	
健康检查出方向协议检查	

说明

若独享型ELB实例未开启“IP类型后端”功能，ELB四层监听器转发的流量将不受安全组规则和网络ACL规则限制，安全组规则和网络ACL规则无需额外放通。建议您使用监听器的访问控制功能对访问IP进行限制，详情请参考**访问控制策略**。

后端服务器子网的网络 ACL 配置

网络ACL为子网级别的可选安全层，若后端服务器的子网关联了网络ACL规则，网络ACL规则必须放通ELB用于健康检查的协议和端口和健康检查的源地址。

网络ACL默认规则会拒绝所有入站和出站流量，启用网络ACL后，您必须对网络ACL规则进行配置。

您可通过自助诊断工具后端服务器的安全组规则进行诊断。后端服务器的网络ACL规则的检查项目如下**表3-3**所示。

表 3-3 网络 ACL 规则排查项目

排查项	处理措施
健康检查入方向协议检查	请确保后端服务器子网的网络ACL入方向规则放通健康检查协议对应的传输层协议、健康检查端口和ELB后端子网所在的VPC网段。 配置指导详情见**配置网络ACL规则（独享型）**。
健康检查入方向源地址检查	
健康检查入方向源端口检查	
健康检查入方向目的地址检查	
健康检查入方向目的端口检查	
健康检查出方向协议检查	请确保后端服务器子网的网络ACL出方向规则放通健康检查协议对应的传输层协议、健康检查端口和ELB后端子网所在的VPC网段。 配置指导详情见**配置网络ACL规则（独享型）**。
健康检查出方向源地址检查	
健康检查出方向源端口检查	
健康检查出方向目的地址检查	
健康检查出方向目的端口检查	

说明

若独享型ELB实例未开启“IP类型后端”功能，ELB四层监听器转发的流量将不受安全组规则和网络ACL规则限制，安全组规则和网络ACL规则无需额外放通。建议您使用监听器的访问控制功能对访问IP进行限制，详情请参考**访问控制策略**。

健康检查参数配置

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. 在后端服务器组页面，单击需要检查健康检查参数配置的后端服务器组名称。
6. 在后端服务器组的“基本信息”页签下，查看以下健康检查配置参数。

   更多健康检查参数设置信息，请参见**修改健康检查配置**。

表 3-4 健康检查配置参数

健康检查参数	说明
域名	健康检查使用HTTP协议时，如果后端服务器设置了校验HOST头能力，需要将后端服务器配置的域名填写到“健康检查配置”页面中的“域名”处。
协议	后端服务器的安全组和网络ACL规则必须放通健康检查协议对应的传输层协议。
端口	建议指定后端服务器的业务端口为健康检查端口，配置详情请参见**修改健康检查配置**。
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。

说明

- 您的健康检查协议为“HTTP”，健康检查异常时，如果您已确认端口没有问题，请修改检查路径或者将健康检查协议修改为“TCP”，只检查端口。
- 检查路径需填写绝对路径。示例如下：
  - 访问链接为：http://www.example.com或http://192.168.63.187:9096，则检查路径填写“/”。
  - 访问链接为：http://www.example.com/chat/try/，则检查路径填写“/chat/try/”。
  - 访问链接为：http://192.168.63.187:9096/chat/index.html，则检查路径填写“/chat/index.html”。

检查后端服务器组是否关联监听器

在异常的服务器所在的后端服务器组是否关联了监听器。

后端服务器组未关联至负载均衡的监听器下，健康检查状态无法探测。

如果后端服务器组已经关联了监听器，请继续排查问题项。

检查 ELB 是否绑定 EIP 或私网 IP

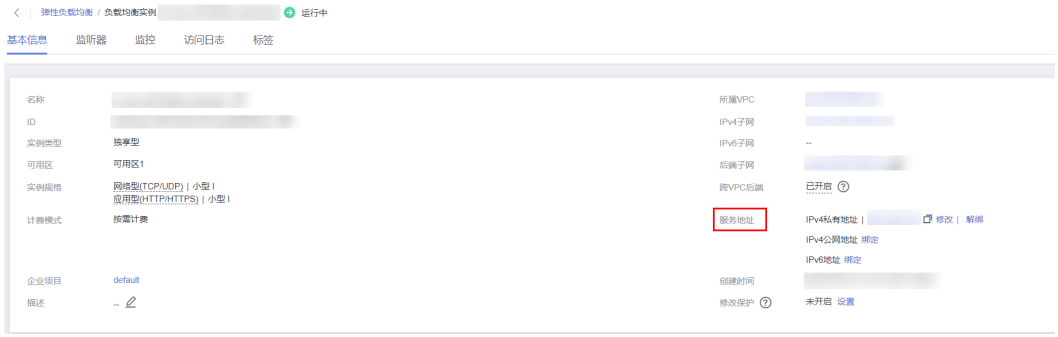
说明

该检查项仅适用于四层监听器（TCP/UDP）。

对于四层监听器（TCP/UDP）下的异常后端服务器，请检查其关联的负载均衡器是否绑定EIP或私网IP。

负载均衡实例初次创建时，如果未绑定EIP或私网IP时，四层监听器（TCP/UDP）所关联的后端服务器会显示健康检查异常。

图 3-1 查看负载均衡器的 EIP 或者私网 IP



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，则表示后端服务器的健康检查端口在监听状态，如图3-2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，默认和后端服务器业务端口一致。

图 3-2 后端服务器正常被监听的回显示例

图 3-3 后端服务器没有被监听的回显示例

如果健康检查端口没有在监听状态（后端服务器没有被监听），您需要先启动后端服务器上的业务，启动业务后再查看健康检查端口是否被正常监听。

- 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。

对于独享型ELB：HTTP/HTTPS健康检查正常返回状态码均为200。

图 3-4 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 3-5 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。

检查后端服务器防火墙

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ELB发起健康检查的源IP网段。

当后端服务器关联至独享型负载均衡使用，请您在防火墙规则中放通ELB后端子网所在的VPC网段。

检查后端服务器路由

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3-6所示。

图 3-6 默认路由指向网关示例

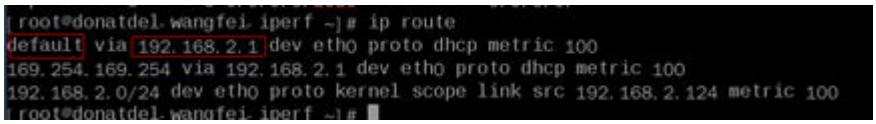
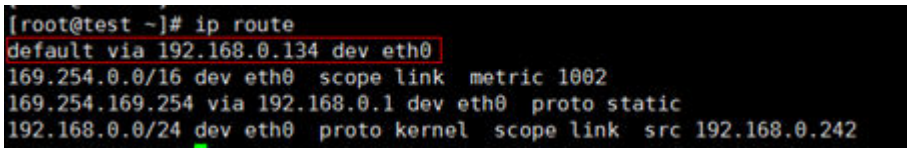


图 3-7 默认路由未指向网关示例



如果回显中没有像图3-6中的第一条路由信息，或者路由指向的IP的不是后端服务器所在VPC子网的网关，请您配置默认路由指向网关。

检查后端服务器负载

通过云监控服务，查看后端服务器的CPU/内存/网络连接数等，来判断后端服务器的负载是否过高。

如果负载很高，可能会导致健康检查的连接或请求超时。

检查后端服务器 hosts.deny 文件

建议您排查后端服务器的/etc/hosts.deny文件，对于独享型负载均衡，该文件中不能写入ELB后端子网所在的VPC网段。

提交工单

如果上述方法均不能解决您的疑问，请**提交工单**寻求更多帮助。

3.2 健康检查异常排查（共享型）

问题描述

客户端的请求通过负载均衡器的监听器访问后端服务器异常，监听器的健康检查列显示“异常”。

当健康检查探测到您的后端服务器异常时，ELB将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。

背景介绍

负载均衡器通过向后端服务器发起心跳检查的方式来实现健康检查功能，并判断后端服务器是否可用。更多检查原理详见**健康检查介绍**。

- 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。

- 当后端服务器的权重设置为0时：
  - 独享型负载均衡器：新的请求不会转发到该后端服务器，健康检查会继续探测，健康检查状态显示为实际结果。
  - 共享型负载均衡器：新的请求不会再转发到该后端服务器，健康检查状态显示为“异常”。

排查思路

负载均衡已提供自助问题诊断工具帮助用户定位健康检查异常问题，如果通过自助诊断工具排查仍然无法定位问题，请参考**表3-5**进一步排查。

因为健康检查包含检查间隔和阈值判断，相关配置的修改完成后需要等待一定的时间，配置才会生效。

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。

表 3-5 排查思路

排查手段	排查项目
自助诊断工具排查	**后端服务器的安全组配置**
	后端服务器子网的网络ACL配置
	健康检查参数配置
其他异常排查项	**检查后端服务器组是否关联监听器**
	检查ELB是否绑定EIP或私网IP
	检查后端服务器是否正常
	检查后端服务器防火墙
	检查后端服务器路由
	检查后端服务器负载
	检查后端服务器hosts.deny文件

后端服务器的安全组配置

共享型负载均衡的后端服务器安全组规则必须放通ELB用于健康检查的协议和端口和健康检查的源地址。

健康检查的协议和端口为用户在健康检查配置页面进行设置，您可在后端服务器组的基本信息页面查看。共享型负载均衡用于健康检查的源地址为100.125.0.0/16网段的IP。

您可通过自助诊断工具后端服务器的安全组规则进行诊断。后端服务器安全组规则的检查项目如下**表3-6**所示。

表 3-6 安全组规则排查项目

排查项	处理措施
健康检查入方向源地址检查	请确保后端服务器的安全组入方向规则放通健康检查协议对应的传输层协议、健康检查端口和100.125.0.0/16网段的IP。 配置指导详情见**配置后端服务器的安全组（共享型）**。
健康检查入方向端口检查	
健康检查入方向协议检查	
健康检查出方向源地址检查	默认的安全组出方向规则全部放通。如果您设置了出方向规则，请确保后端服务器的安全组出方向规则放通健康检查协议对应的传输层协议、健康检查端口和100.125.0.0/16网段的IP。 配置指导详情见**配置后端服务器的安全组（共享型）**。
健康检查出方向端口检查	
健康检查出方向协议检查	

说明

若共享型ELB实例开启“获取客户端IP”功能，共享型ELB四层监听器转发的流量将不受安全组规则和网络ACL限制，安全组规则和网络ACL规则均无需额外放通。建议您使用监听器的访问控制功能对访问IP进行限制，详情请参考**访问控制策略**。

后端服务器子网的网络 ACL 配置

网络ACL为子网级别的可选安全层，若后端服务器的子网关联了网络ACL规则，网络ACL规则必须放通ELB用于健康检查的协议和端口和健康检查的源地址。

网络ACL默认规则会拒绝所有入站和出站流量，启用网络ACL后，您必须对网络ACL规则进行配置。

您可通过自助诊断工具后端服务器的安全组规则进行诊断。后端服务器的网络ACL规则的检查项目如下**表3-7**所示。

表 3-7 网络 ACL 规则排查项目

排查项	处理措施
健康检查入方向协议检查	请确保后端服务器子网的网络ACL入方向规则放通健康检查协议对应的传输层协议、健康检查端口和100.125.0.0/16网段的IP。 配置指导详情见**配置网络ACL规则（共享型）**。
健康检查入方向源地址检查	
健康检查入方向源端口检查	
健康检查入方向目的地址检查	
健康检查入方向目的端口检查	

排查项	处理措施
健康检查出方向协议检查	请确保后端服务器子网的网络ACL出方向规则放通健康检查协议对应的传输层协议、健康检查端口和100.125.0.0/16网段的IP。 配置指导详情见**配置网络ACL规则（共享型）**。
健康检查出方向源地址检查	
健康检查出方向源端口检查	
健康检查出方向目的地址检查	
健康检查出方向目的端口检查	

说明

若共享型ELB实例开启“获取客户端IP”功能，共享型ELB四层监听器转发的流量将不受安全组规则和网络ACL限制，安全组规则和网络ACL规则均无需额外放通。建议您使用监听器的访问控制功能对访问IP进行限制，详情请参考**访问控制策略**。

健康检查参数配置

1. 在左侧导航栏，选择“ 弹性负载均衡 > 后端服务器组”。
2. 在后端服务器组页面，单击需要检查健康检查参数配置的后端服务器组名称。
3. 在后端服务器组的“基本信息”页签下，查看以下健康检查配置参数。
   更多健康检查参数设置信息，请参见**修改健康检查配置**。

表 3-8 健康检查配置参数

健康检查参数	说明
域名	健康检查使用HTTP协议时，如果后端服务器设置了校验HOST头能力，需要将后端服务器配置的域名填写到“健康检查配置”页面中的“域名”处。
协议	后端服务器的安全组和网络ACL规则必须放通健康检查协议对应的传输层协议。
端口	建议指定后端服务器的业务端口为健康检查端口。
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。

说明

- 您的健康检查协议为“HTTP”，健康检查异常时，如果您已确认端口没有问题，请修改检查路径或者将健康检查协议修改为“TCP”，只检查端口。
- 检查路径需填写绝对路径。示例如下：
  - 访问链接为：http://www.example.com或http://192.168.63.187:9096，则检查路径填写“/”。
  - 访问链接为：http://www.example.com/chat/try/，则检查路径填写“/chat/try/”。
  - 访问链接为：http://192.168.63.187:9096/chat/index.html，则检查路径填写“/chat/index.html”。

检查后端服务器组是否关联监听器

在异常的服务器所在的后端服务器组是否关联了监听器。

后端服务器组未关联至负载均衡的监听器下，健康检查状态无法探测。

如果后端服务器组已经关联了监听器，请继续排查问题项。

检查 ELB 是否绑定 EIP 或私网 IP

说明

- 该检查项仅适用于四层监听器（TCP/UDP）。

对于四层监听器（TCP/UDP）下的异常后端服务器，请检查其关联的负载均衡器是否绑定EIP或私网IP。

负载均衡实例初次创建时，如果未绑定EIP或私网IP时，四层监听器（TCP/UDP）所关联的后端服务器会显示健康检查异常。

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，则表示后端服务器的健康检查端口在监听状态，如图3-8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，默认和后端服务器业务端口一致。

图 3-8 后端服务器正常被监听的回显示例

图 3-9 后端服务器没有被监听的回显示例

如果健康检查端口没有在监听状态（后端服务器没有被监听），您需要先启动后端服务器上的业务，启动业务后再查看健康检查端口是否被正常监听。

- 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。

  对于共享型ELB：HTTP健康检查正常返回状态码是200、202或者401。

  图 3-10 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 3-11 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。

检查后端服务器防火墙

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ELB发起健康检查的源IP网段。

当后端服务器关联至共享型负载均衡使用，请您在防火墙规则中放通100.125.0.0/16网段的IP。

检查后端服务器路由

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3-12所示。

图 3-12 默认路由指向网关示例

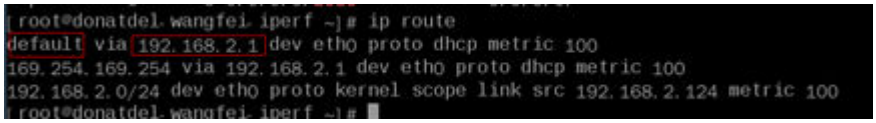
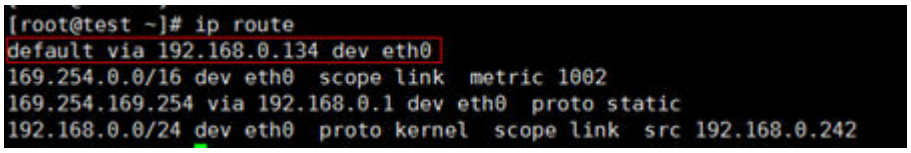


图 3-13 默认路由未指向网关示例



如果回显中没有像图3-12中的第一条路由信息，或者路由指向的IP的不是后端服务器所在VPC子网的网关，请您配置默认路由指向网关。

检查后端服务器负载

通过云监控服务，查看后端服务器的CPU/内存/网络连接数等，来判断后端服务器的负载是否过高。

如果负载很高，可能会导致健康检查的连接或请求超时。

检查后端服务器 hosts.deny 文件

建议您排查后端服务器的/etc/hosts.deny文件，对于共享型负载均衡，该文件中不能写入100.125.0.0/16网段的IP。

提交工单

如果上述方法均不能解决您的疑问，请提交工单寻求更多帮助。

3.3 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。

3.4 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：

- 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。
- 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。

- 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。
- 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服务器在端口扫描时，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服务器的状态信息。针对此种情况，用户需要确保后端服务器开启ICMP协议，确认方法如下：

  用户登录后端服务器，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。

3.5 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，检查间隔用户可配，健康检查会根据检查间隔一直探测，所以每隔几秒会有访问。您可以通过**修改健康检查配置**的周期来控制访问后端服务器的频率。

3.6 健康检查什么时候启动?

后端服务器新加入后，在第一个周期内随机一个时间开始检测，后续按照“检查间隔”启动。

3.7 如何处理健康检查导致的大量日志?

1. 可以增加健康检查间隔时间，配置方法详见**修改健康检查配置**。

   存在的风险：延长健康检查的间隔时间后，后端ECS实例出现故障时，负载均衡发现故障ECS实例的时间也会增长。

2. 可以关闭健康检查，配置方法详见**修改健康检查配置**。

   存在的风险：关闭健康检查后，负载均衡不再检查后端服务器，一旦某台后端服务器发生故障，则无法实现访问流量自动切换至其它正常的后端服务器。

3. 切换健康检查协议，配置方法：进入控制台，选择产生检查日志的后端服务器组，单击配置健康检查配，切换健康检查协议。

   存在的风险：负载均衡将只检查监听端口状态，不检查HTTP状态，会导致负载均衡无法实时获知HTTP应用是否出现问题。

3.8 健康检查正常默认返回的状态码有哪些?

表 3-9 健康检查正常返回的状态码

ELB类型	健康检查协议	健康检查正常返回的状态码
独享型	HTTP	200
	HTTPS	200
共享型	HTTP	• 200 • 202 • 401

4 功能支持

4.1 ELB 是否可以单独使用?

弹性负载均衡服务不可以单独使用。

弹性负载均衡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，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。因此弹性负载均衡要基于后端实例（如：弹性云服务器）来使用，不可以单独使用。

4.2 ELB 是否自带防 DDoS 攻击和 Web 代码层次安全的功能?

- ELB服务不提供DDoS等安全防护功能，防护功能一般配合高防系统来使用；
- DDoS防护是华为云默认开启的防护，所有公网的入口流量都会被DDos防护。

说明

DDoS高防（Advanced Anti-DDoS，AAD）是基于Anti-DDoS清洗设备和大数据运营平台构建的DDoS防护服务，通过流量转发方式对用户源站进行隐藏保护，是企业重要业务连续性的有力保障，用户可以通过修改DNS解析或对外服务地址为高防IP，将恶意攻击流量引流到高防IP清洗，保护对外IP地址不被黑洞（无法访问），确保重要业务不被攻击中断。可服务于华为云、非华为云及IDC的互联网主机。

4.3 ELB 是否可以添加不同操作系统的服务器?

ELB可以添加不同操作系统的服务器。ELB本身不会对后端服务器使用的操作系统进行限制，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。

通常情况，建议您选择2台相同操作系统的后端服务器进行配置，以便您日后的管理维护。

4.4 ELB 支持跨用户、跨不同 VPC 使用么?

- 共享型ELB不支持跨用户使用，也不支持添加不同VPC的后端服务器。
- 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VPC内的服务器，还支持添加其他VPC、其他Region、云下数据中心的服务器。

4.5 后端服务器可以反过来访问 ELB 吗?

通常情况，不建议同一台服务器既作为后端服务器又作为客户端的业务场景。

如果您有特殊业务需求，请谨慎选择方案。

- 公网通信：如果后端服务器绑定了公网IP地址，可以访问ELB的公网IP地址。
- 私网通信：
  - 七层监听器支持后端服务器作为客户端访问ELB。
  - 如果四层监听器开启“获取客户端IP”功能，不支持后端服务器作为客户端访问ELB。
  - 如果四层监听器未开启“获取客户端IP”，支持后端服务器作为客户端访问ELB。

    说明

    如果ELB开启“IP类型后端”功能，“获取客户端IP”功能将失效，支持后端服务器作为客户端访问ELB。

4.6 ELB 能否实现全链路 HTTPS 协议?

独享型ELB支持，共享型ELB不支持。

独享型负载均衡支持全链路HTTPS数据传输，即在添加监听器时，前端协议选择“HTTPS”，后端协议也支持选择“HTTPS”。

如果是非全链路HTTPS，负载均衡支持后端协议选择HTTP协议。

说明

全链路HTTPS仅支持在负载均衡器上做双向验证。

4.7 ELB 支持 IPv6 网络吗?

目前，共享型负载均衡仅支持IPv4网络，不支持IPv6网络。独享型负载均衡支持IPv4网络和IPv6网络。

当独享型负载均衡使用TCP/UDP监听器时，如果客户端和ELB之间使用IPv6网络通信，ELB和后端服务器之间必须使用IPv6网络通信；当独享型负载均衡使用TLS/HTTP/HTTPS/QUIC监听器时，如果客户端和ELB之间使用IPv6网络通信，ELB和后端服务器之间必须使用IPv4网络通信。

说明

- 创建独享型负载均衡时，若指定的后端子网未开启IPv6，负载均衡实例创建后将不支持IPv6网络。
- 如果您的业务需要支持IPv6网络，您需要在创建独享型负载均衡时指定已开启IPv6的子网作为后端子网。

4.8 如何通过监控数据和日志快速判断 ELB 的响应时间?

七层负载均衡HTTP和HTTPS可以通过监控指标项可以查看ELB的平均响应时间，同时可以通过日志查看每一次请求的响应时间。

1. 登录控制台，并单击需要查询的负载均衡名称。
2. 切换到“监控”页签，并选择正确的七层监听器。
3. 查看“7层后端RT平均值”参数，可以得到负载均衡器到后端服务器的平均响应时间。

表 4-1 平均响应时间

参数名	解释
7层后端的RT平均值	统计监听器当前7层后端平均响应时间。（HTTP和HTTPS监听器才有此指标） 从监听器将请求转发给后端服务器开始，到监听器收到后端服务器返回响应为止。 单位：毫秒。

4. 如果您想查询七层协议每个请求的具体响应时间，您可以通过**访问日志**查看。

访问日志的“request_time”、“upstream_connect_time”、“upstream_header_time”或“upstream_response_time”字段计算可以查看ELB转发请求的耗时情况。访问日志获取方法，请参考**访问日志**。

表 4-2 参数解释

参数名	解释
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_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 -。

4.9 如何获取来访者的真实 IP?

当客户端通过ELB访问后端服务器时，客户端真实的IP地址会被ELB转换，后端服务器获取到的往往是ELB转换后的客户端IP地址。如果需要获取到客户端的真实IP，可以按如下方法操作。

- 七层服务（HTTP/HTTPS协议）：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。

  配置详情见**七层服务**。
- 四层服务（TCP/UDP协议），有两种方式可以获取客户端的真实IP：
  - 方法一：开启监听器的“获取客户端IP”功能。
  - 方法二：配置TOA插件获取。

  配置详情见**四层服务**。

约束与限制

- 如果IP经过NAT，则只能获取到NAT转化后的IP地址，无法获取到NAT转化前的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，不支持同一台服务器既作为后端服务器又作为客户端的场景。
- 独享型负载均衡的四层监听器（TCP/UDP）默认开启源地址透传功能，无需手动开启，且不支持关闭。

说明

如果客户端经过WAF+ELB访问服务器，则还可以通过WAF直接获取客户端真实IP。详见**《Web应用防火墙用户指南》**

七层服务

针对七层服务（HTTP/HTTPS协议），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

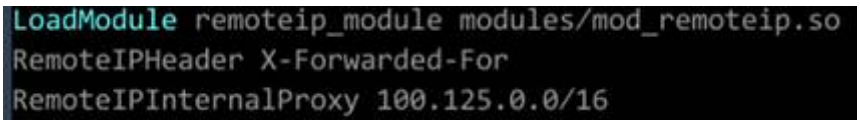
1. 安装Apache 2.4。

   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 4-1 修改 Apache 的配置文件示例图



说明

将代理服务器的网段添加到 RemoteIPInternalProxy <IP_address>。

- 共享型负载均衡需要添加的IP地址段为 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。
- 独享型负载均衡需要添加ELB实例关联的VPC子网网段。

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。

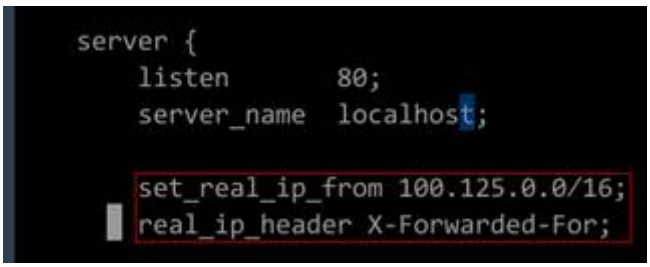
```
vi /path/server/nginx/conf/nginx.conf
```

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 4-2 添加配置字段和信息示例图



说明

将代理服务器的网段添加到 RemoteIPInternalProxy <IP_address>。

- 共享型负载均衡需要添加的IP地址段为 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。
- 独享型负载均衡需要添加ELB实例关联的VPC子网网段。

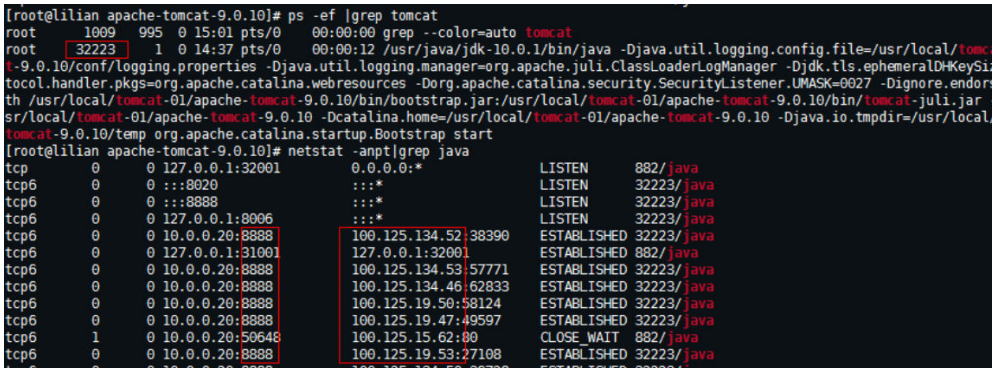
4. 启动Nginx。
```
/path/server/nginx/sbin/nginx
```
5. 查看Nginx的访问日志，您可以获取真实的来访者IP。
```
cat /path/server/nginx/logs/access.log
```

配置Tomcat服务器

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

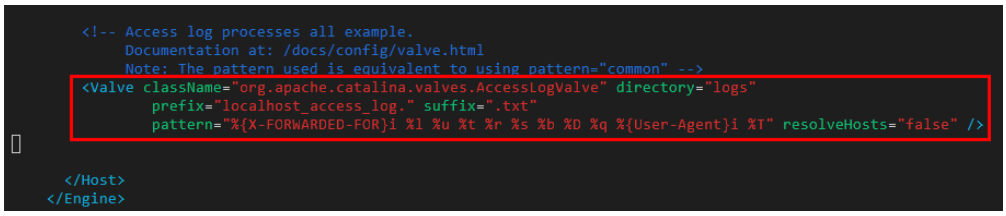
1. 登录已安装Tomcat的服务器。
2. 执行如下命令，确定Tomcat已经正常运行。
```
ps -ef|grep tomcat
netstat -anpt|grep java
```

图 4-3 正常运行结果示例



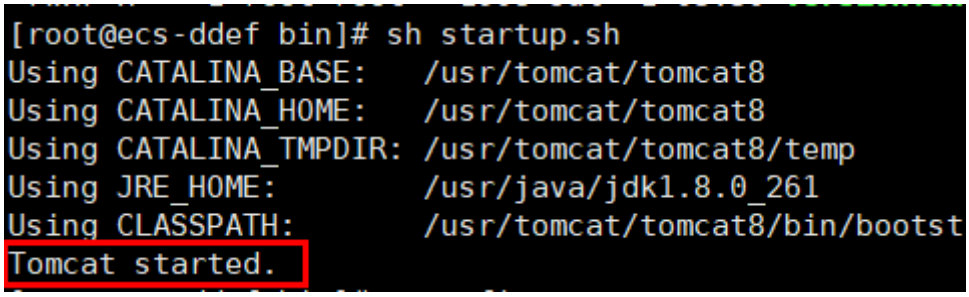
3. 将server.xml文件中的className="org.apache.catalina.valves.AccessLogValve" 模块修改为如下内容。
```
vim /usr/tomcat/tomcat8/conf/server.xml
<Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
prefix="localhost_access_log." suffix=".txt"
pattern="%{X-FORWARDED-FOR}i %l %u %t %r %s %b %D %q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

图 4-4 配置示例



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

图 4-5 重启 Tomcat 服务



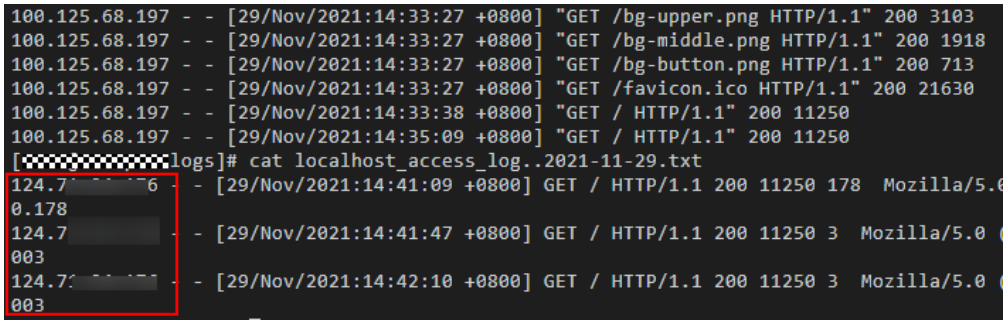
5. 执行如下命令，查看最新的日志。

   如图中红框所示获取到的非100.125网段的IP地址，即为获取到的源IP地址。

   ```
   cd /usr/tomcat/tomcat8/logs/
   cat localhost_access_log..2021-11-29.txt
   ```

   其中“localhost_access_log..2021-11-29.txt”为当天日志路径，请根据实际情况替换。

图 4-6 查询源 IP 地址



配置Windows IIS服务器

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

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

图 4-7 选择模块选项

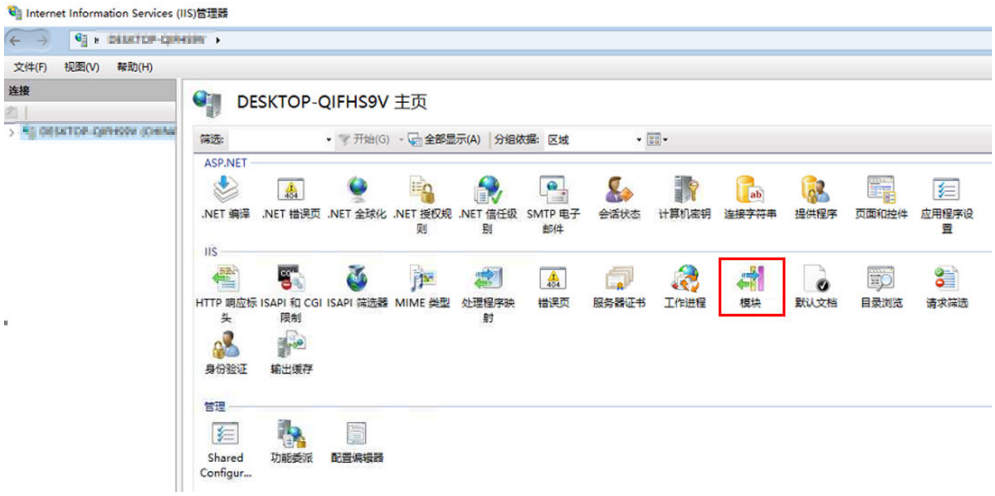
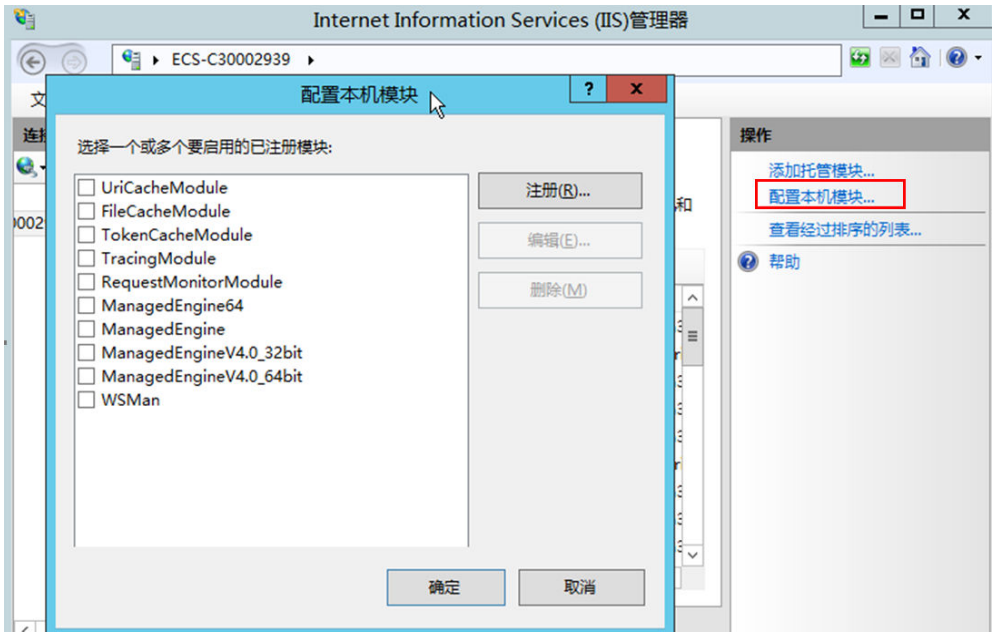
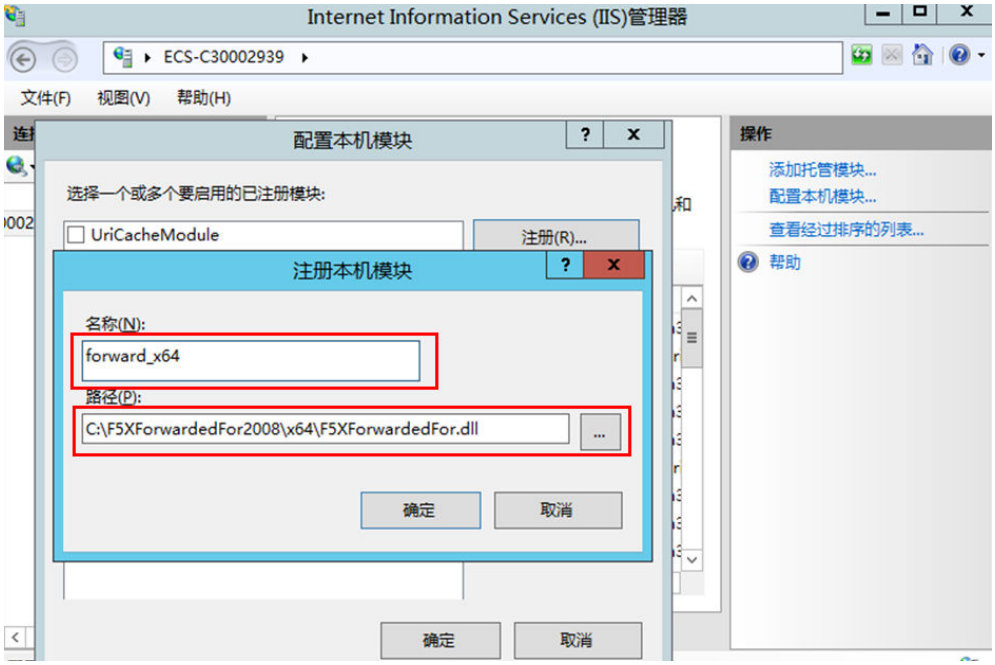


图 4-8 配置本机模块



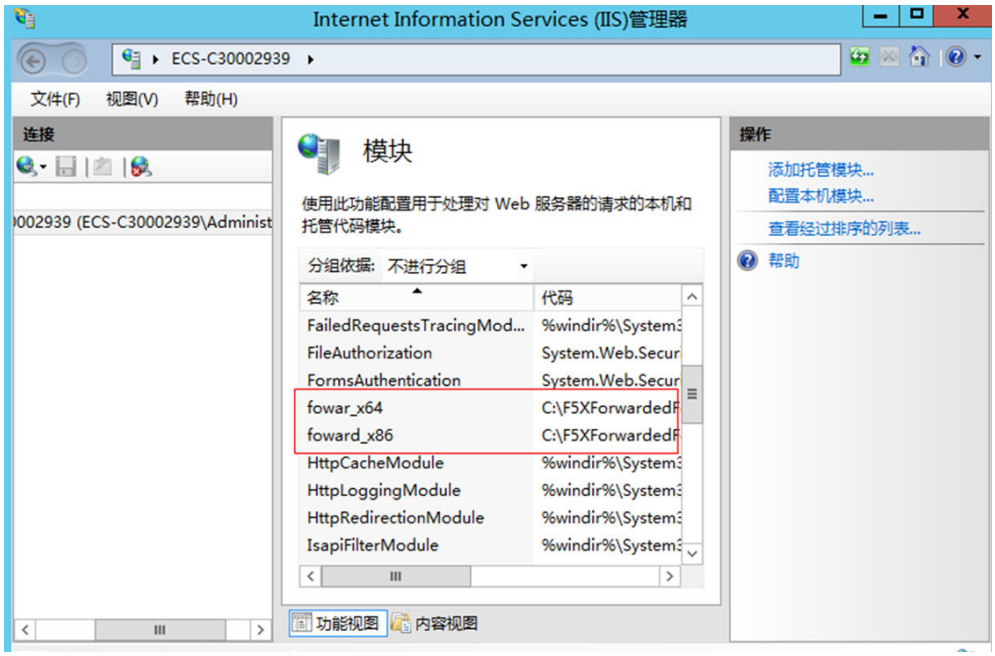
4. 单击“注册”，分别注册x86和x64插件。

图 4-9 注册插件



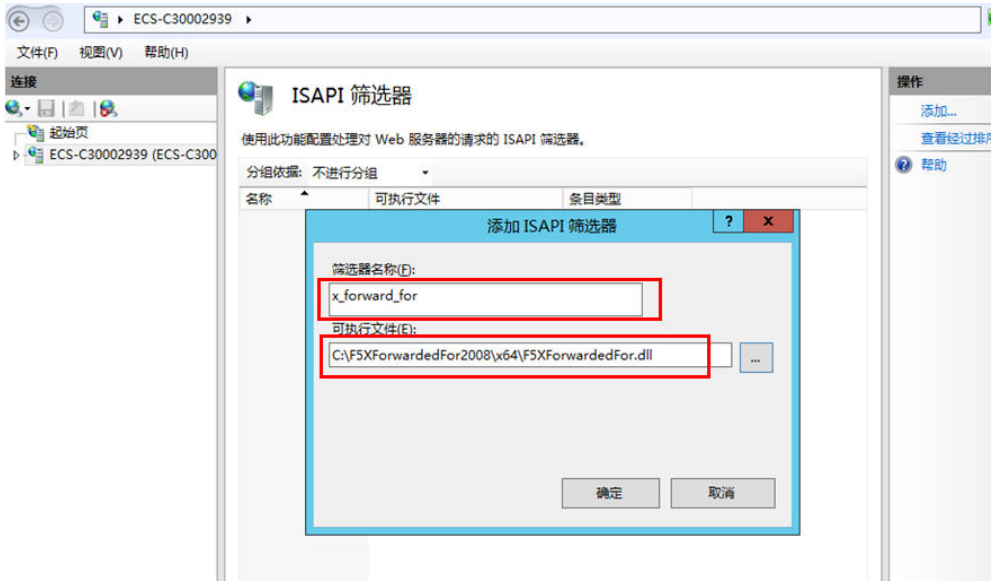
5. 在“模块”页面，确认注册的模块名称出现在列表中。

图 4-10 确认注册成功



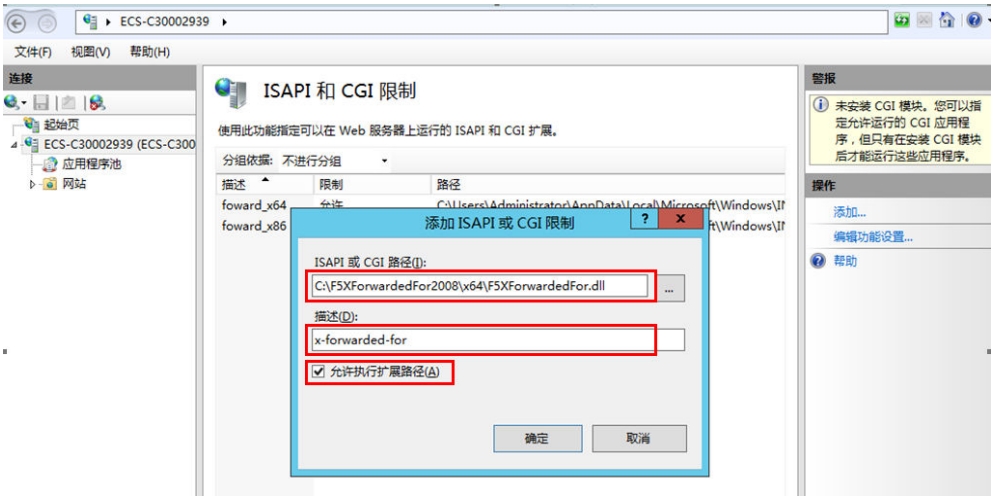
6. 选择IIS管理器主页的“ISAPI筛选器”，为2个插件授权运行ISAPI和CGI扩展。

图 4-11 添加授权



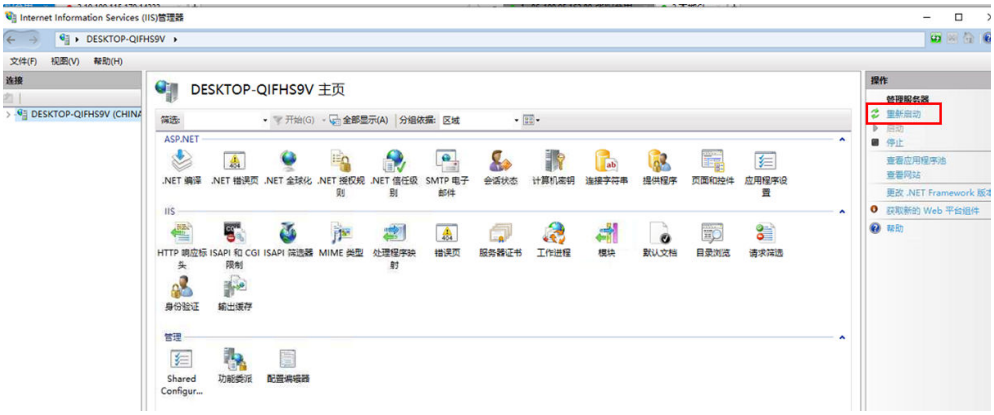
7. 选择“ISAPI和CGI限制”，为2个插件设置执行权限。

图 4-12 允许执行



8. 单击主页的“重新启动”，重启IIS服务，重启后配置生效。

图 4-13 重启 IIS 服务



四层服务

针对四层服务（TCP/UDP协议），有两种方式可以获取客户端的真实IP。

- **方式一（TCP/UDP协议）**：开启监听器的“获取客户端IP”功能。

  ⚠ 注意

  - 开启此功能后，执行后端服务器迁移任务时，可能出现流量中断（例如单向下载、推送类型的流量）。所以后端服务器迁移完成后，需要通过报文重传来恢复流量。
  - 监听器开启此功能后，后端服务器不能作为客户端访问此监听器。
  - 如果监听器之前已经添加了后端服务器、并且开启了健康检查功能，开启“获取客户端IP”功能会重新上线后端服务器，新建流量会有1-2个健康检查间隔的中断。

  a. 开启监听器的“获取客户端IP”功能。
     i. 登录管理控制台。
     ii. 在管理控制台左上角单击 图标，选择区域和项目。
     iii. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
     iv. 在“负载均衡器”界面，单击需要操作的负载均衡名称。
     v. 切换到“监听器”页签。
        - 新增场景：单击“添加监听器”。
        - 修改场景：在需要修改的监听器名称右侧所在行的操作列，单击“编辑”。
     vi. 开启“获取客户端IP”开关。
  b. 设置后端服务器的安全组、网络ACL、操作系统和软件的安全规则，使客户端的IP地址能够访问后端服务器。

     说明

     开启“获取客户端IP”之后，不支持同一台服务器既作为后端服务器又作为客户端的场景。如果后端服务器和客户端使用同一台服务器，且开启“获取客户端IP”，则后端服务器会根据报文源IP为本地IP判定该报文为本机发出的报文，无法将应答报文返回给ELB，最终导致回程流量不通。

- **方式二（TCP协议）**：配置TOA插件获取。

  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**。

4.10 长连接和会话保持区别是什么？

长连接和会话保持没有必然联系。

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。会话保持是指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。

4.11 如何使用 Linux curl 测试负载均衡会话保持?

1. 申请ELB与ECS资源。
   a. 创建3个ECS实例，1个做客户端，2个做服务端。
   b. 创建1个ELB实例与HTTP监听器实例，注意务必开启“会话保持”功能。
2. 启动服务端ECS的HTTP服务。

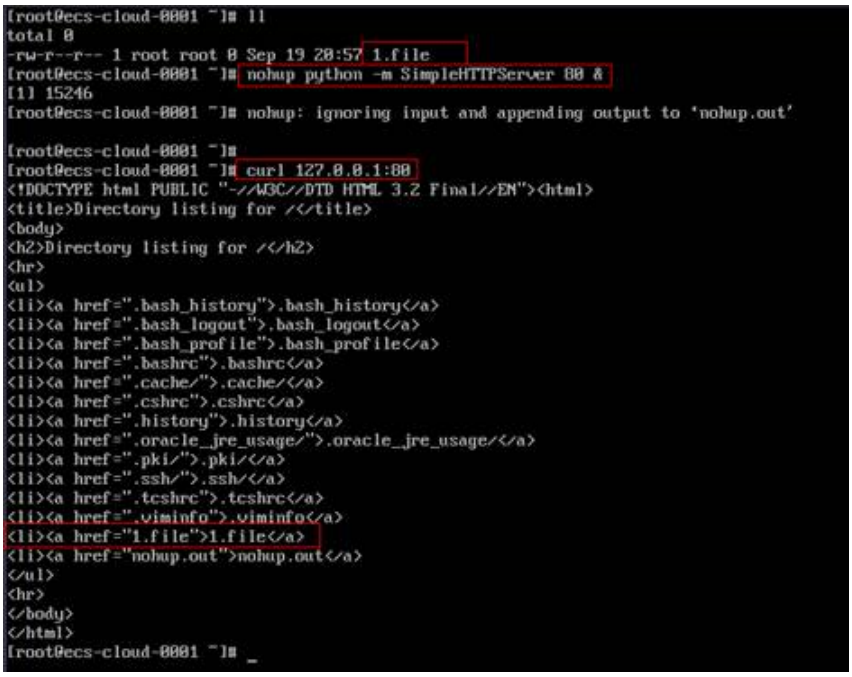
   登录第一个服务端ECS，在当前路径下创建名为“1.file”的文件，以标示第一个节点。

   并在当前路径执行以下命令启动HTTP服务。

   nohup python –m SimpleHTTPServer 80 &

   在第一个部署后端服务的虚拟机执行以下命令，确认HTTP服务正常。

   curl http://127.0.0.1:80



   登录第二个服务端ECS，在当前路径下创建名为“2.file”的文件，以标示第二个节点。

   并在当前路径执行以下命令启动HTTP服务。

   nohup python –m SimpleHTTPServer 80 &

   在本机执行以下命令，确认HTTP服务正常。

   curl http://127.0.0.1:80


```
[root@ecs-cloud-0002 ~]# touch 2.file
[root@ecs-cloud-0002 ~]# nohup python -m SimpleHTTPServer 80 &
[1] 15244
[root@ecs-cloud-0002 ~]# nohup: ignoring input and appending output to 'nohup.out'

[root@ecs-cloud-0002 ~]# curl 127.0.0.1:80
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 3.2 Final//EN"><html>
<title>Directory listing for /</title>
<body>
<h2>Directory listing for /</h2>
<hr>
<ul>
<li><a href=".bash_history">.bash_history</a>
<li><a href=".bash_logout">.bash_logout</a>
<li><a href=".bash_profile">.bash_profile</a>
<li><a href=".bashrc">.bashrc</a>
<li><a href=".cache/">.cache/</a>
<li><a href=".cshrc">.cshrc</a>
<li><a href=".history">.history</a>
<li><a href=".oracle_jre_usage/">.oracle_jre_usage/</a>
<li><a href=".pki/">.pki/</a>
<li><a href=".ssh/">.ssh/</a>
<li><a href=".tcshrc">.tcshrc</a>
<li><a href=".viminfo">.viminfo</a>
<li><a href="2.file">2.file</a>
<li><a href="nohup.out">nohup.out</a>
</ul>
<hr>
</body>
</html>
[root@ecs-cloud-0002 ~]#
```

3. 从客户端ECS指定cookie值对ELB实例发起访问。

   调整以下命令，从客户端ECS对ELB实例发起访问，确认每次请求返回的file名称一致。

   curl --cookie "name=abcd" http://ELB_IP:Port

```
<body>
<h2>Directory listing for /</h2>
<hr>
<ul>
<li><a href=".bash_history">.bash_history</a>
<li><a href=".bash_logout">.bash_logout</a>
<li><a href=".bash_profile">.bash_profile</a>
<li><a href=".bashrc">.bashrc</a>
<li><a href=".cache/">.cache/</a>
<li><a href=".cshrc">.cshrc</a>
<li><a href=".history">.history</a>
<li><a href=".oracle_jre_usage/">.oracle_jre_usage/</a>
<li><a href=".pki/">.pki/</a>
<li><a href=".ssh/">.ssh/</a>
<li><a href=".tcshrc">.tcshrc</a>
<li><a href=".viminfo">.viminfo</a>
<li><a href="2.file">2.file</a>
<li><a href="nohup.out">nohup.out</a>
</ul>
<hr>
</body>
</html>
[root@ecs-client ~]# curl --cookie "name=abcd"  http://192.168.172.242:80
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 3.2 Final//EN"><html>
<title>Directory listing for /</title>
<body>
<h2>Directory listing for /</h2>
<hr>
<ul>
<li><a href=".bash_history">.bash_history</a>
<li><a href=".bash_logout">.bash_logout</a>
<li><a href=".bash_profile">.bash_profile</a>
<li><a href=".bashrc">.bashrc</a>
<li><a href=".cache/">.cache/</a>
<li><a href=".cshrc">.cshrc</a>
<li><a href=".history">.history</a>
<li><a href=".oracle_jre_usage/">.oracle_jre_usage/</a>
<li><a href=".pki/">.pki/</a>
<li><a href=".ssh/">.ssh/</a>
<li><a href=".tcshrc">.tcshrc</a>
<li><a href=".viminfo">.viminfo</a>
<li><a href="2.file">2.file</a>
<li><a href="nohup.out">nohup.out</a>
</ul>
<hr>
</body>
</html>
[root@ecs-client ~]# curl --cookie "name=abcd" http://192.168.172.242:80
```


5 负载均衡器

5.1 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。

说明

“FullNAT”是转发模式，是指LVS会转换客户端的源IP和目的IP。

图 5-1 四层转发协议

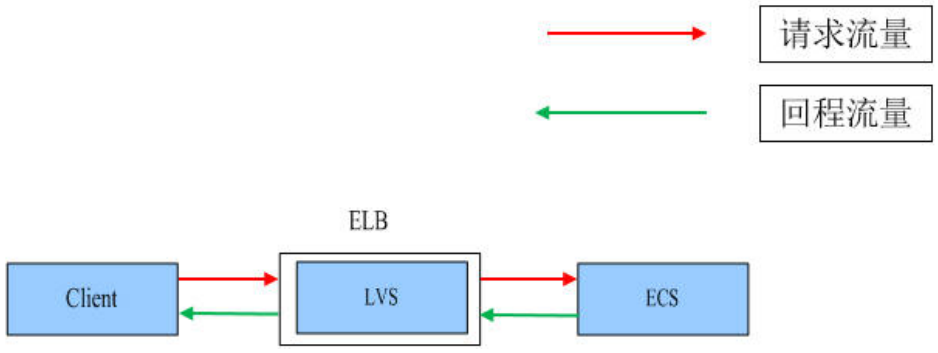
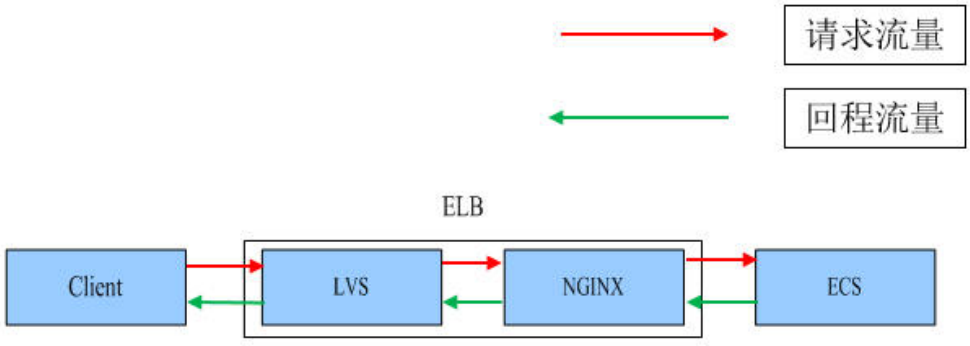


图 5-2 七层转发协议



5.2 容器应用如何配置负载均衡?

容器支持配置负载均衡，有两种配置方式。

- 通过控制台操作。
- 通过kubectl命令行创建。

具体配置方法请参见**容器配置负载均衡**。

5.3 创建独享型 ELB 后为什么会占用多个子网 IP?

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

ELB使用的子网IP地址详情请见**表5-1**，ELB实例使用的IP地址主要分布在后端子网，因此用户可以通过规划一个ELB实例专属的后端子网，避免ELB实例使用业务子网过多的IP地址而影响业务扩展。

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

表 5-1 ELB 实例对 IP 地址的使用情况说明（单可用区）

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

如果是多可用区，占用的IP数会根据算法增加，实际使用IP的数量以您创建出来的独享型负载均衡占用的IP个数为准。

独享型ELB的子网规划推荐您参考**独享型ELB子网规划的推荐方案**。

5.4 ELB 绑定了 EIP，后端的服务器可以通过 ELB 访问公网吗?

不可以。

弹性负载均衡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。ELB绑定EIP只能做负载，即外部访问后端服务。

ELB绑定EIP后，后端服务器可以绑定EIP，也可以不绑定EIP。如果后端服务器想要访问公网，要么直接绑定EIP，要么做NAT网关。

5.5 共享型 ELB 有实例规格吗?

和独享型相比，共享型没有实例规格。

共享型ELB是性能共享，多个ELB共用一个集群，无法确定单个ELB的实例规格，ELB之间的使用性能相互影响；独享型ELB是性能独享，可以确定单个ELB的实例规格，每个ELB之间的使用性能互不影响。

5.6 共享型 ELB 实例业务超出性能保障模式上限怎么办?

共享型ELB实例无法保障超出性能保障模式上限的业务请求，如果您的业务规模较大，建议您尽快升级至独享型负载均衡器。

5.7 独享型负载均衡器的带宽和 EIP 的带宽有什么区别?

如果您通过固定规格的ELB来转发公网流量，需同时注意ELB实例规格的带宽和EIP的公网带宽大小是否匹配您的业务规模。

- 独享型负载均衡器的带宽，又称为“每秒带宽（Mbit/s）”，是指负载均衡实例能够处理的入流量或出流量不超过该带宽规格的数值，即负载均衡器能够处理的流量上限。
- ELB绑定的EIP的公网带宽是华为云到Internet之间的网络带宽流量上限，对应客户端访问ELB时的最高公网流量限制。

5.8 ELB 与 WAF 如何配合使用?

如果您的网站已接入Web应用防火墙（Web Application Firewall，简称WAF）进行安全防护，您可以通过ELB来设置源站服务器的访问控制策略，只放行WAF回源IP段，防止黑客获取您的源站IP后绕过WAF直接攻击源站。详见**《Web应用防火墙用户指南》**。

5.9 ELB 的 IPv4/IPv6 双栈实例可以切换到仅 IPv4 模式吗?

为实现ELB实例IPv4/IPv6双栈的能力，需要为ELB实例指定一个IPv6子网，用于分配访问ELB实例的IPv6地址，IPv6地址会从指定的子网中随机分配。

当您的实例需要关闭IPv6的功能，可以将ELB实例与IPv6地址解绑，IPv6地址将回收至子网中，无法再使用此IPv6地址访问ELB实例。

若要重新使用IPv4/IPv6双栈的能力，目前您可通过调用API的方式为ELB实例重新绑定IPv6子网，重新绑定后，为实例分配的IPv6地址无法保证与之前的IPv6地址一致。

5.10 ELB 是否存在并发连接限制?

- 独享型ELB实例支持的并发连接数请参考**独享型负载均衡实例规格**。
- ELB实例在以下场景涉及FULLNAT转换，在高并发业务场景下可能触发TCP五元组分配不足的异常。建议单台后端服务器的并发连接数不超过20万，如果超过该推荐值，可能导致五元组端口号资源分配不足，影响您业务的正常运行。
  - TLS监听器转发业务流量。
  - HTTP/HTTPS监听器转发WebSocket业务流量。

  如果您的业务涉及以上两种转发场景，您可以根据业务规模计算后端服务器的保底数量。

  计算示例：业务规模需要100万长连接保持，单台后端服务器支持20万并发连接，那么100万÷ 20万=5，因此您至少需要配置五台后端服务器。
- 通过IP类型后端添加的单台后端服务器最多支持10万并发连接数。

6 监听器

6.1 七层监听器支持添加哪些 HTTP 请求头?

当前七层监听器默认添加如表6-1字段。

表 6-1 默认添加字段

字段	含义
X-Forwarded-ELB-IP	将ELB实例的公网IP地址通过报文的HTTP头传递到后端服务器。
X-Forwarded-Host	将客户端请求头的Host设置为X-Forwarded-Host传递到后端服务器。
X-Forwarded-Port	将ELB实例的监听端口通过报文的HTTP头传递到后端服务器。
X-Forwarded-Proto	将客户端请求的协议类型（HTTP/HTTPS）通过报文的HTTP头传递到后端服务器。
X-Forwarded-For	将客户端的源IP地址和代理IP地址通过报文的HTTP头传递到后端服务器。
X-Real-IP	将客户端的源IP地址通过报文的HTTP头传递到后端服务器。

6.2 监听器删除之后，ELB 是否会立即停止转发业务流量?

- 当删除四层监听器时，由于客户端和ELB之间都是短连接，ELB会立即停止转发业务流量；
- 当删除七层监听器时，由于客户端和ELB之间保持长连接，客户端和ELB之间仍然会有部分TCP长连接存在，这些TCP长连接已经建立，不受监听器是否删除的影响，直到客户端在这些TCP连接上停止发送请求时间间隔达到keepalive_timeout超时时间（300s）之后，ELB才会断开这些长连接并停止转发业务流量。

说明

keepalive_timeout为空闲超时时间，只有客户端和ELB之间长连接时才会存在keepalive_timeout。

6.3 ELB 对上传文件的速度和大小是否有限制?

- ELB 七层监听器与四层监听器对客户端上传文件的速度都没有限制，可能EIP带宽限制会影响上传速度。
- 七层监听器的上传文件大小有限制，最大为10G；四层监听器的上传文件大小没有限制。

6.4 支持多个 ELB 转发到同一台后端服务器吗?

支持多个ELB转发到同一台后端服务器。

- ELB实例可以通过直接添加云服务器或辅助弹性网卡的方式添加后端服务器，此时仅要求ELB实例和后端服务器在同一VPC内。
- ELB实例通过IP类型后端添加后端服务器时，只需确保ELB实例与后端服务器的网络连通，此时ELB实例与后端服务器可以在不同VPC内。

6.5 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）。

6.6 监听器的 3 个超时时间分别是什么?

ELB与后端服务器建立连接后，四层和七层监听器的超时时间如表6-2所示。

说明

- 共享型负载均衡支持配置和修改TCP/HTTP/HTTPS的超时时间，不支持UDP超时时间的修改。
- 独享型负载均衡支持配置和修改TCP/UDP/HTTP/HTTPS的超时时间。

图 6-1 七层监听器超时时间示意图

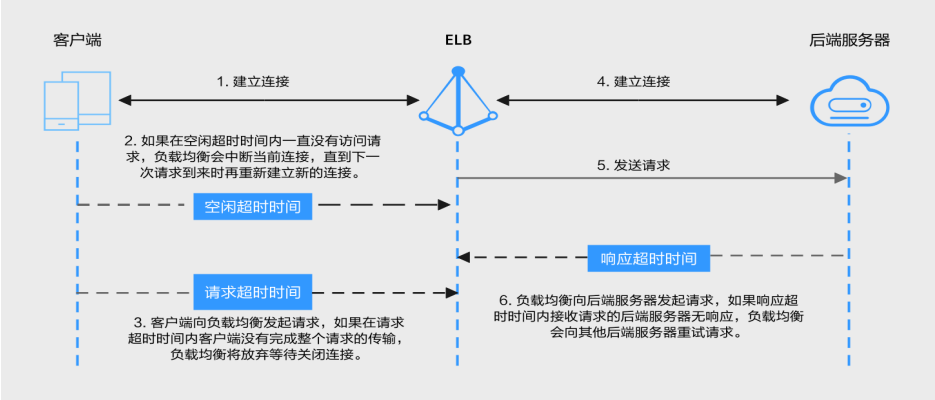


图 6-2 四层监听器超时时间示意图

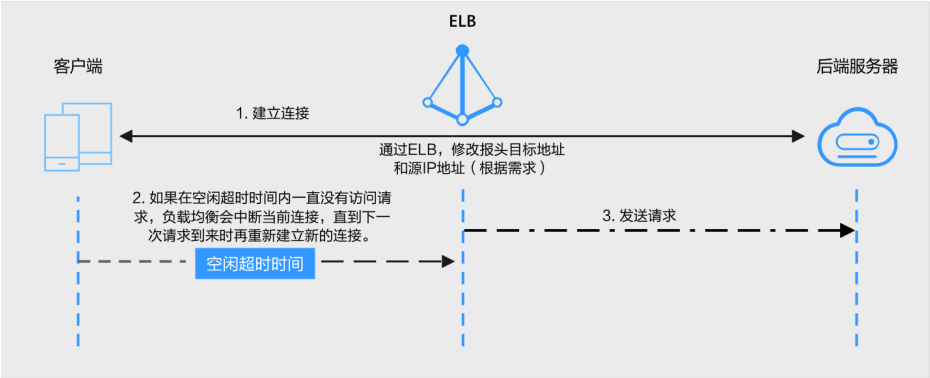


表 6-2 超时时间

协议	类别	描述	取值范围
TCP/UDP/TLS	空闲超时时间	如果在空闲超时时间内一直没有访问请求，负载均衡会关闭当前连接，直到下一次请求到来时再重新建立新的连接。	10~4000s
HTTP/HTTPS/QUIC	空闲超时时间	如果在空闲超时时间内一直没有访问请求，负载均衡会关闭当前连接，直到下一次请求到来时再重新建立新的连接。	0~4000s
	请求超时时间	客户端向负载均衡发起请求，如果在请求超时时间内客户端没有完成整个请求的传输，负载均衡将放弃等待关闭连接。	1~300s
	响应超时时间	负载均衡向后端服务器发起请求，如果响应超时时间内接收请求的后端服务器无响应，负载均衡会向其他后端服务器重试请求。如果重试期间后端服务器一直没有响应，则负载均衡会给客户端返回HTTP 504错误码。 如果开启了会话保持功能，响应超时时间内对应的后端服务器无响应，负载均衡将不会发起重试请求，直接返回HTTP 504错误码。 **说明** 当开启了会话保持功能时，响应超时时间内如果对应的后端服务器无响应，则直接会返回HTTP 504错误码。	1~300s

6.7 添加/修改监听器时，选择不到想选择的后端服务器组是什么原因?

这是因为后端服务器组的协议（后端协议）与监听器的协议（前端协议）存在对应关系，在给监听器添加后端服务器组时，只能添加与其协议对应的后端服务器组。如下所示：

独享型负载均衡

表 6-3 前端/后端协议匹配关系

ELB的规格类型	监听器的前端协议	后端服务器组的后端协议
网络型	TCP	TCP
网络型	UDP	• UDP • QUIC
网络型	TLS	• TLS • TCP
应用型	HTTP	HTTP
应用型	HTTPS	• HTTP • HTTPS • GRPC
应用型	QUIC	• HTTP • HTTPS

共享型负载均衡

表 6-4 前端/后端协议匹配关系

监听器的前端协议	后端服务器组的后端协议
TCP	TCP
UDP	UDP
HTTP	HTTP
HTTPS	HTTP

6.8 为什么 HTTPS 监听器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。
- 域名未备案。

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。

6.9 转发策略的状态显示为“故障”的原因是什么?

可能的原因是：如果创建了相同的转发策略（出现转发策略冲突），则会出现转发策略故障，此时即使把前面创建的转发策略删除，后面的转发策略依然会显示故障。

解决办法：将出现冲突的转发策略全部都删除后再重新添加，即可恢复正常。

7 后端服务器

7.1 后端服务器组中分配策略类型和会话保持类型有什么关系?

后端服务器组的会话保持类型与分配策略类型的支持情况可以参见表7-1和表7-2。

表 7-1 独享型负载均衡会话保持支持情况

后端服务器组协议	分配策略类型	会话保持类型
• TCP • UDP	加权轮询算法	源IP地址
	加权最少连接	源IP地址
	源IP算法	不支持设置会话保持
• HTTP • HTTPS • GRPC	加权轮询算法	• 负载均衡器cookie • 应用程序cookie
	加权最少连接	• 负载均衡器cookie • 应用程序cookie
	源IP算法	不支持设置会话保持 **说明** 当分配策略类型选择“源IP算法”时，已默认支持基于源IP地址的会话保持。
QUIC	连接ID算法	源IP地址

表 7-2 共享型负载均衡会话保持支持情况

后端服务器组协议	分配策略类型	会话保持类型
• TCP • UDP	加权轮询算法	源IP地址
	加权最少连接	源IP地址
	源IP算法	不支持会话保持 **说明** 当分配策略类型选择“源IP算法”时，已默认支持基于源IP地址的会话保持。
HTTP	加权轮询算法	• 负载均衡器cookie • 应用程序cookie
	加权最少连接	• 负载均衡器cookie • 应用程序cookie
	源IP算法	不支持设置会话保持 **说明** 当分配策略类型选择“源IP算法”时，已默认支持基于源IP地址的会话保持。

7.2 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。

7.3 ELB 是否支持非华为云的后端服务器?

- 共享型负载均衡不支持，必须是华为云后端服务器。单击了解更多**后端服务器概述（共享型）**相关内容。
- 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VPC内的服务器，还支持添加其他VPC、其他Region、云下数据中心的服务器。单击了解更多**后端服务器概述（独享型）**。
- ELB不支持数据库实例作为后端服务器。

7.4 为什么 100 或 214 开头的 IP 在频繁访问后端服务器?

共享型负载均衡实例以100.125.0.0/16网段中的IP作为源地址，向后端服务器转发前端业务流量及发起健康检查探测（如果您已开启健康检查）。

所以这些100.125开头的IP为弹性负载均衡服务与后端服务器通信所使用的内部IP，为了保证您的共享型负载均衡实例可正常提供服务，请确保后端服务器的安全策略已放通100.125.0.0/16网段。

说明

如果共享型负载均衡实例所在区域已无100.125.0.0/16网段可供使用，将启用214.0.0.0/8网段中的IP作为源IP转发业务流量及发起健康检查探测。

7.5 ELB 可以跨区域关联后端服务器么?

- 共享型负载均衡不支持跨区域关联后端服务器。
- 独享型负载均衡器支持跨区域、跨不同VPC添加后端服务器。
  - 通过使用云连接服务实现跨区域间通信，详见**《云连接用户指南》**。
  - 通过ELB的IP类型后端功能实现跨不同VPC添加后端服务器，详见**配置不同VPC的服务器作为后端服务器**。

7.6 公网负载均衡的后端服务器要不要绑定 EIP?

负载均衡实例都是通过私网转发访问请求，不需要后端服务器绑定EIP。

7.7 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。

7.8 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. 检查安全组规则是否放通了对应的网段：
      - 对于独享型负载均衡，检查后端服务器所在的安全组入方向是否放通ELB所在VPC的网段。如果没有放通，请在安全组入方向规则中添加ELB所在VPC网段。
      - 对于共享型负载均衡，检查客户后端服务安全组入方向是否放通了100.125.0.0/16网段。如果没有放行，请添加100.125.0.0/16网段的入方向规则。

注意

- 共享型实例四层监听器开启“获取客户端IP”功能后，后端服务器的安全组规则和网络ACL规则均无需放通100.125.0.0/16网段及客户端IP地址。
- 独享型实例四层监听器未开启“IP类型后端”功能时，后端服务器安全组规则和网络ACL规则均无需放通ELB后端子网所在的VPC网段。

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。

7.9 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7-1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 7-1 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 ~]#
```

7.10 如何检查通过 EIP 访问后端云服务器?

1. 后端虚拟机绑定EIP。
   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. 单击“ ”，选择“计算 > 弹性云服务器”。
   d. 选择需要绑定EIP的弹性云服务器名称。
   e. 切换到“弹性公网IP”页签后，单击“绑定弹性公网IP”。
   f. 选择需要绑定的EIP，单击“确定”。
2. 查看直接通过EIP访问后端服务器功能是否正常。

Linux可用curl命令做校验，Windows用浏览器访问测试。

7.11 为什么云监控服务统计的 ELB 活跃连接数与后端服务器上的连接数不一致?

云监控服务统计的活跃连接数是指客户端到ELB实例之间的活跃连接数。

对于四层监听器（TCP/UDP），ELB实例会直接透传客户端请求，ELB活跃连接数等于后端服务器上的连接数。

对于七层监听器（HTTP/HTTPS），是客户端和ELB实例建立连接，ELB实例再和后端服务器建立连接。因此，ELB活跃连接数与后端服务器的连接数没有对应关系。

7.12 为什么配置了白名单后还能访问后端服务器?

白名单只对经过ELB实例的访问进行控制，通过控制访问负载均衡的监听器的IP地址，能够设置允许特定IP进行访问，而其它IP不许访问。如果需要对后端服务器进行访问控制，可以通过配置网络ACL或者安全组规则实现。

7.13 ELB 修改后端服务器权重后多久生效?

ELB修改后端服务器权重后，新的权重5秒内会生效。

- 对于TCP、UDP监听器，新的连接会根据修改后的权重转发，已经建立的连接不受影响。
- 对于HTTP、HTTPS监听器，新的请求会根据修改后的权重转发，已有请求不受影响。

说明

后端服务器的权重修改为0后，不会立即生效，仍然会有流量进入服务器，这是因为长连接在超时时间内会复用TCP连接，请求会继续转发。

- TCP和UDP监听器：长连接在空闲超时时间后断开。
- HTTP和HTTPS监听器：长连接在响应超时时间后断开。

8 安全管理

8.1 ELB 是否支持泛域名证书?

支持，客户上传泛域名证书即可。

共享型负载均衡默认支持最长尾缀匹配。

独享型负载均衡使用的SNI证书泛域名匹配方式默认为标准域名分级匹配，即只能匹配同级别的子域名。如您希望修改为最长尾缀匹配，请参考《API参考》修改参数sni_match_algo。

表 8-1 泛域名匹配规则示例

域名	标准域名分级匹配	最长尾缀匹配
*.example.com	abc.example.com、sport.example.com、good.example.com等域名	abc.example.com、mycalc.good.example.com等域名

8.2 配置了证书，访问异常是什么原因?

可能的原因有：

- 您在证书管理界面创建了证书，但因为您未使用HTTPS监听器，所以无法给监听器绑定证书。

  可以使用以下方法解决：

  - 继续使用现有非HTTPS监听器，并在后端服务器上安装证书。
  - 删除现有非HTTPS监听器，重新创建HTTPS监听器，并绑定证书。
- 您在证书管理界面创建了证书，且使用的是HTTPS监听器，但未将证书绑定至该监听器。
- 您的证书已过期。
- 创建证书时指定了域名，但访问的域名和创建证书时配置的域名不一致。
- 创建的证书为证书链时，没有按照证书链的格式拼接证书。

- 您在ELB侧配置了HTTPS监听器+证书，同时在后端服务器上也配置了证书。您在ELB上配置了证书，ELB会对来自客户端的HTTPS请求进行解密，然后发送至后端服务器，而后端服务器上也配置了证书，会导致已经被解密的信息再次被解密。共享型负载均衡存在此限制，独享型负载均衡不存在此限制。

  可以使用以下方法解决：

  - 在后端服务器上配置证书，然后使用TCP监听器将HTTPS流量透传到后端服务器。
  - 在ELB上使用HTTPS监听器并配置证书，在后端服务器上不配置证书。

8.3 更换证书会导致网络或者 ELB 连接中断吗?

不会。

更换证书后，新的证书会立即生效，已经建立的连接会继续使用老证书，新建立的连接将会使用新的证书。

说明

证书过期后，用户访问时会提示“不安全的链接”，一般情况下忽略掉安全告警后，还是可以访问的。

8.4 华为云负载均衡上传证书报错怎么办?

您可通过华为云负载均衡控制台直接上传证书，也可通过在云证书与管理服务控制台上传证书后在负载均衡服务使用。如您通过负载均衡控制台上传证书报错，请检查以下内容：

- 检查证书是否完整。
- 检查上传证书链是否完整。
- 检查上传证书内容前后是否有空格。

8.5 配置访问日志后为什么界面没有显示?

- 确认已创建云日志服务是否已经开启，且云日志组与云日志流已创建，请参见**访问日志**。
- 确认所创建的ELB服务是否可以被正常访问。
- 确认负载均衡是否支持访问日志：

  目前只有七层负载均衡（HTTP/HTTPS）支持访问日志功能，四层负载均衡（TCP/UDP）不支持此功能。

8.6 用户需要做运维协助操作吗?

需要。

如果按照**如何检查后端服务器网络状态?** 到**如何检查通过EIP访问后端云服务器?** 章节，自查指导的操作进行确认后，弹性负载均衡器依然无法通信，则需联系客服解决。

用户需向技术支持人员提供如下表格中的信息：

项目信息	您的值
负载均衡器的ID	-
虚拟私有云的ID	-
负载均衡的服务地址	-
监听器的ID	-
负载均衡器协议/端口	-
健康检查方式(协议/端口)	-
健康检查状态	-
云服务器1的ID	-
云服务器2的ID	-

8.7 华为云负载均衡的访问日志会保留多久?

在ELB控制台配置访问日志后，日志数据默认保存7天。您也可在1~365天之间按需设置日志数据保存天数。

8.8 云监控 EIP 带宽使用统计与 ELB 监控的网络流出速率数据为何不一致?

以下两种情况监控EIP带宽使用统计与ELB监控的网络流出速率数据不一致：

- 如果流量没有超过EIP带宽，EIP未被限流，云监控EIP带宽使用统计外网访问数据，而ELB不仅采集外网访问数据，而且采集内网访问的数据。
- 如果流量超过EIP带宽，EIP会被限流，ELB内访问的数据流量跟EIP访问数据流量不是一个路径，ELB内访问数据流量不会被限流。

8.9 ELB 监控指标中七层协议返回码和七层后端返回码的区别?

ELB七层监听器会终结TCP连接。即客户端和ELB之间会建立TCP连接，ELB和后端主机之间会建立另外一条TCP连接。客户端把HTTP请求发送给ELB之后，ELB会解析并转发HTTP请求到后端主机，然后后端主机再返回HTTP响应给ELB，ELB再解析和转发HTTP响应到客户端，所以通信过程被分成前后两个阶段。协议返回码是指ELB返回给客户端的状态码，后端返回码是指后端主机返回给ELB的状态码。

协议返回码和后端返回码有如下三种情况：

- 后端主机有返回码，这种情况ELB会透传后端主机返回码到客户端，即协议返回码和后端返回码一致；

- ELB和后端主机连接异常或者超时等，ELB会填充后端返回码为502或者504，然后转发给客户端；
- 监听器配置异常或者客户端请求格式和内容异常时，ELB会直接返回4xx或者502返回码，不继续向后端主机转发请求，即有协议返回码，无后端返回码。

8.10 为什么七层监听器的监控中有大量 499 返回码?

HTTP返回码499对应的说明为：client has closed connection，即说明客户端主动断开了连接。

可能的原因：

- 客户端设置的请求超时时间太短，导致客户端未发送完HTTP请求就因为请求超时关闭了连接，建议排查访问日志中的request_time字段，该字段代表客户端请求的总时间，参考该字段的值设置合理的客户端请求超时时间。
- 访问ELB实例的流量太大，触发带宽限速丢包，建议通过云监控排查实例的出带宽使用率指标。更多信息，请参见**《监控指标说明》**。
- 客户端到ELB的网络链路有问题，存在往返延时比较大或丢包等问题，建议排查访问日志的request_time和tcpinfo_rtt字段或抓包排查客户端网络是否有异常。
- 后端服务器处理请求时间太长，超过了客户端的请求超时时间，建议排查后端服务器的CPU、内存、网络是否存在性能瓶颈。
- 客户端遇到未知问题，在未完成HTTP请求的情况下，提前关闭连接。建议排查客户端是否有提前关闭连接的行为。

9 计费

9.1 ELB 什么情况下需要使用公网带宽?

通过公网访问ELB实例时，需要通过ELB的弹性公网IP进行访问，同时使用公网带宽。如果直接通过后端服务器ECS实例的弹性公网IP直接访问后端ECS实例，则使用的是ECS实例本身弹性公网IP绑定的公网带宽，不使用ELB实例的公网带宽。如果通过内网访问ELB实例，只需访问ELB实例的内网地址，不需要使用公网带宽。

9.2 弹性负载均衡器的带宽和弹性云服务器的带宽是否会重复计费?

主要取决于客户的业务是否需要弹性云服务器的带宽。一般来说，弹性云服务器接入弹性负载均衡器后，由弹性负载均衡器对外提供访问业务，弹性云服务器不需要再申请EIP和带宽。但是不排除客户的业务比较特殊，一个弹性云服务器有多个对外业务，此时需要弹性云服务器申请EIP和带宽并独立计费。

9.3 共享型负载均衡器的宽带大小需要根据后端服务器带宽的大小来调整?

- 对于公网共享型ELB后端服务器是用于对外提供服务，ELB将访问流量分担到不同的服务器上，负载均衡器的带宽大小是根据外部访问流量访问ELB后端云服务器的带宽需求进行设置的。
- 对于私网ELB在企业内部进行负载分担，不涉及带宽调整。

9.4 弹性负载均衡的公网带宽是否可调整?

公网弹性负载均衡（ELB绑定EIP）的带宽可以调整。请参见**修改公网带宽**。

9.5 负载均衡冻结后，哪些功能会受影响?

以下几种场景可能会导致您的负载均衡被冻结，冻结后负载均衡器将不再提供服务。

- 账户余额不足而导致扣费失败。
- 公安冻结场景。

冻结期间，负载均衡器会受以下影响：

1. ELB不再进行流量转发，解冻后流量会逐渐恢复。
2. 健康检查停止，健康检查显示的状态为冻结前一刻的状态，解冻后健康检查会恢复。
3. 监控数据会停止上报，解冻后恢复。
4. 负载均衡器冻结后，以下API行为将会被禁止。
   a. 不允许修改负载均衡器除了名称、标签以外的字段。
   b. 如果是公安冻结场景，负载均衡器不允许删除；负载均衡器下的子资源，如监听器、后端服务器组、健康检查、转发策略、转发规则、后端服务器等均不允许增删改。

