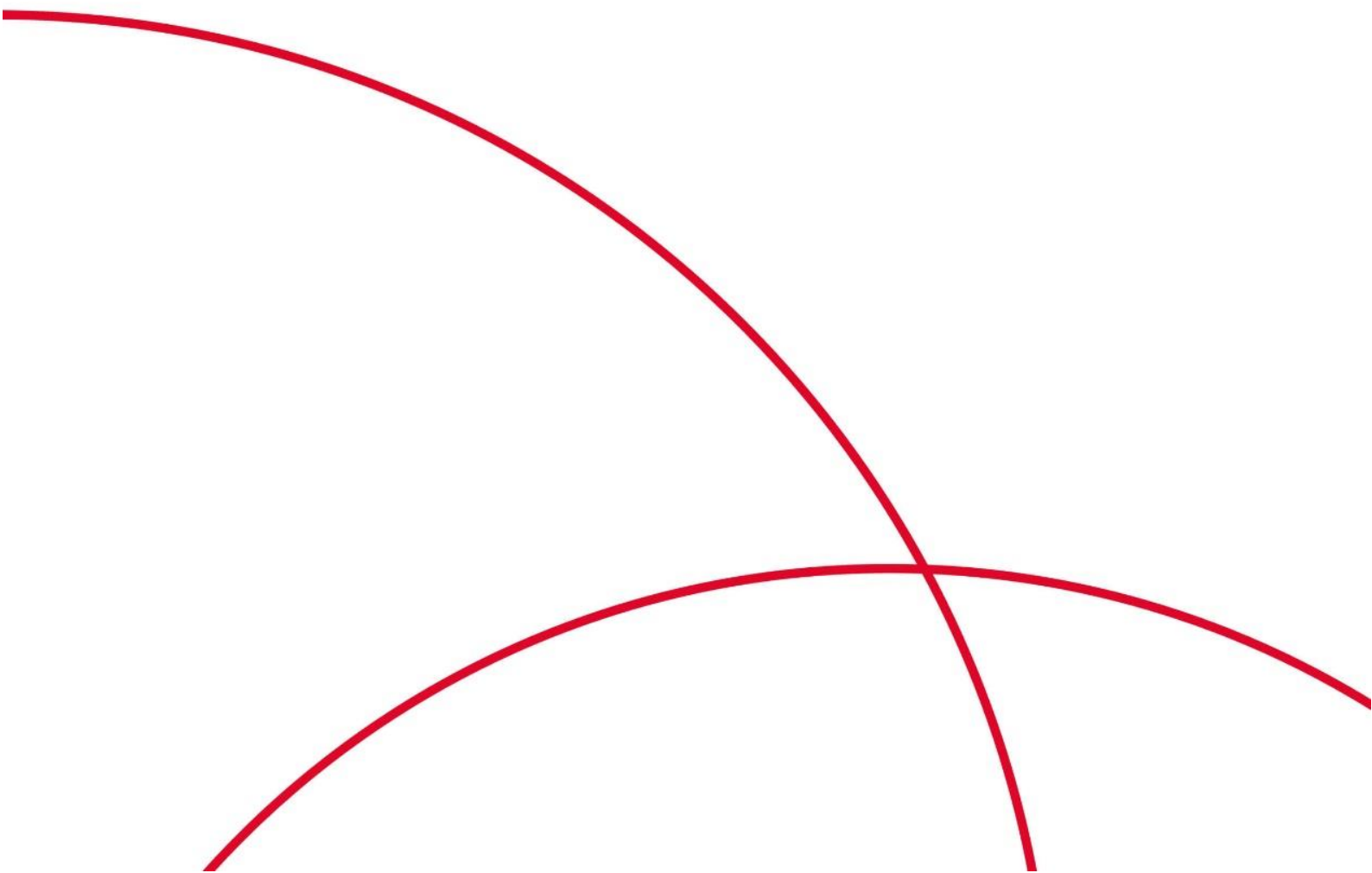




弹性负载均衡

用户使用指南

天翼云科技有限公司



目 录

1 产品介绍	1
1.1 什么是弹性负载均衡	1
1.2 产品优势	3
1.3 弹性负载均衡是如何工作的	4
1.4 应用场景	7
1.5 独享型负载均衡与共享型负载均衡的区别.....	9
1.6 独享型负载均衡实例规格	16
1.7 公网和私网负载均衡器	18
1.8 ELB 网络流量路径说明.....	20
1.9 权限管理	21
1.10 基本概念	24
1.10.1 产品基本概念	24
1.10.2 区域和可用区	26
1.11 与其他服务的关系.....	27
2 快速入门	29
2.1 入门概述	29
2.2 入门流程	30
2.3 共享型增强型负载均衡快速入门.....	30
3 负载均衡器	37
3.1 什么是负载均衡器	37
3.2 规划和准备	39
3.3 创建独享型负载均衡器	42
3.4 创建共享型负载均衡器	47
3.5 变更公网带宽	49
3.6 修改 IP 地址.....	50
3.7 为实例绑定/解绑 EIP	51
3.8 启用和停用负载均衡器	52
3.9 删除负载均衡器	53
3.10 导出负载均衡器列表	54

4 监听器	55
4.1 什么是监听器	55
4.2 协议和端口	56
4.3 流量分配策略	57
4.4 会话保持	59
4.5 访问控制策略	61
4.6 添加 TCP 监听器	63
4.7 添加 UDP 监听器	70
4.8 添加 HTTP 监听器	76
4.9 添加 HTTPS 监听器	85
4.10 添加/修改监听器的超时时间	97
4.11 修改/删除监听器	98
5 HTTP/HTTPS 监听器高级配置	99
5.1 转发策略（共享型）	99
5.2 转发策略（独享型）	103
5.3 高级转发策略（独享型）	106
5.3.1 高级转发策略简介	106
5.3.2 转发规则和动作类型	107
5.3.3 配置高级转发策略	111
5.4 HTTPS 双向认证	117
5.5 HTTP 重定向至 HTTPS	123
5.6 TLS 安全策略	125
6 后端云主机	137
6.1 后端云主机介绍	137
6.2 后端云主机配置安全组（独享型）	138
6.3 后端云主机配置安全组（共享型）	140
6.4 添加或移除后端云主机（独享型）	142
6.5 添加或移除后端云主机（共享型）	148
6.6 配置混合负载均衡-跨 VPC 后端（独享型）	153
6.7 后端云主机配置权重	155
6.8 配置慢启动（独享型）	156
7 健康检查	157
7.1 健康检查介绍	157
7.2 配置健康检查	161
7.3 修改健康检查协议	164
7.4 关闭健康检查	165
8 证书管理	166

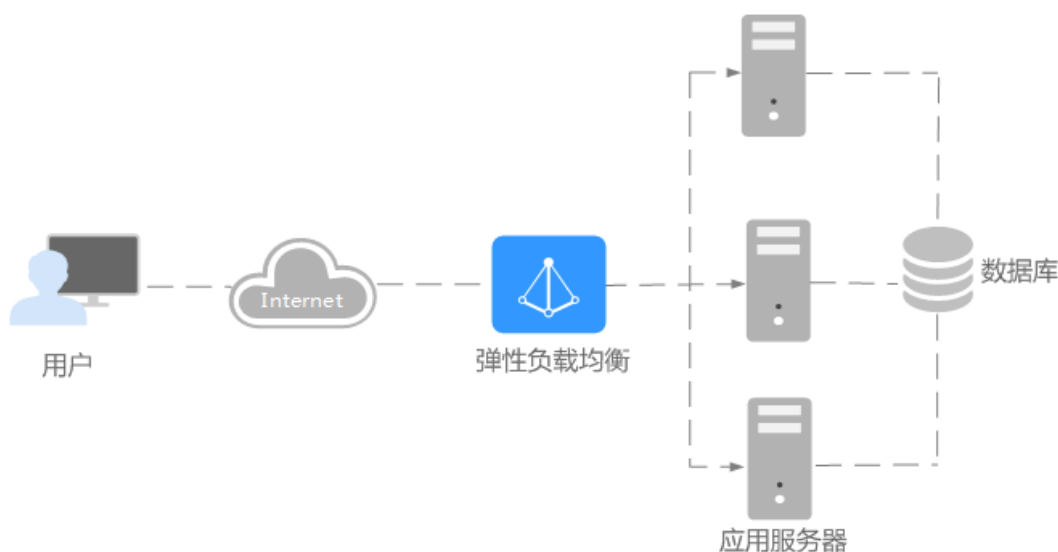
8.1 证书简介	166
8.2 格式转换	166
8.3 创建/修改/删除证书	167
8.4 绑定/更换证书	169
8.5 快速查询证书所关联的监听器	170
9 标签管理	171
9.1 证书格式	173
10 IP 地址组（黑名单/白名单）	175
11 监控	178
11.1 监控指标说明	178
11.2 设置告警规则	189
11.2.1 添加告警规则	189
11.2.2 修改告警规则	189
11.3 查看监控指标	190
12 常见问题	191
12.1 高频常见问题	191
12.2 弹性负载均衡使用	191
12.2.1 异常检查	191
12.2.1.1 如何检查弹性负载均衡服务不通或异常中断？	191
12.2.2 功能支持	192
12.2.2.1 弹性负载均衡器是否可以单独使用？	192
12.2.2.2 弹性负载均衡分配的 EIP 是否为独占？	192
12.2.2.3 单个用户默认可以创建多少个负载均衡器或监听器？	192
12.2.2.4 当负载均衡器正在运行中是否可以调整后端云主机的数量？	192
12.2.2.5 弹性负载均衡是否可以添加不同操作系统的服务器？	193
12.2.2.6 是否支持在业务不中断的前提下，将共享型负载均衡升级为独享型负载均衡？	193
12.2.3 性能负载	193
12.2.3.1 如何检查弹性负载均衡前后端流量不一致？	193
12.2.3.2 如何检查请求不均衡？	193
12.2.3.3 如何检查弹性负载均衡业务访问延时大？	193
12.2.3.4 如何检查压测性能上不去？	194
12.3 负载均衡器	194
12.3.1 ELB 如何根据不同的协议来分发流量？	194
12.3.2 共享型增强型 ELB 有实例规格吗？	195
12.3.3 修改分配策略类型会导致业务中断吗？	195
12.3.4 独享型负载均衡器的带宽和 EIP 的带宽有什么区别？	195
12.4 监听器	195
12.4.1 监听器中分配算法和会话保持算法是什么关系？	195

12.4.2 如何启用 WebSocket 支持?	197
12.4.3 独享型负载均衡器为什么添加不了监听器?	197
12.5 后端云主机	197
12.5.1 为什么后端云主机上收到的健康检查报文间隔和设置的间隔时间不一致?	197
12.5.2 使用 ELB 后, 后端云主机能否访问公网?	198
12.5.3 如何检查后端云主机网络状态?	198
12.5.4 如何检查后端云主机网络配置?	198
12.5.5 如何检查后端云主机服务状态?	198
12.5.6 后端云主机什么时候被认为是健康的?	199
12.6 健康检查	199
12.6.1 健康检查异常如何排查?	199
12.6.2 使用 UDP 协议有什么注意事项?	208
12.6.3 健康检查为什么会导导致 ELB 会频繁向后端云主机发送探测请求?	210
12.7 HTTP/HTTPS 监听器	210
12.7.1 为什么配置证书后仍出现不安全提示?	210
12.7.2 配置转发策略时, 为什么无法选择已有的后端主机组?	210
12.8 会话保持	210
12.8.1 如何检查弹性负载均衡会话保持不生效问题?	210
12.8.2 ELB 支持什么类型的会话保持?	211
12.9 证书管理	211
12.9.1 如何生成服务器证书和 CA 证书?	211
12.9.2 更换证书会导致网络或者 ELB 连接中断吗?	211
13 修订记录.....	212

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云主机。
- **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和转发策略将请求转发到一个后端主机组里的后端云主机。
- **后端云主机：**每个监听器会绑定一个后端主机组，后端主机组中可以添加一个或多个后端云主机。后端主机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云主机。

可以为后端云主机配置流量转发权重，不能为后端主机组配置权重。

您可以开启健康检查功能，对每个后端主机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云主机上；而当该后端云主机恢复正常运行时，弹性负载均衡会将其自动恢复到弹性负载均衡服务中。

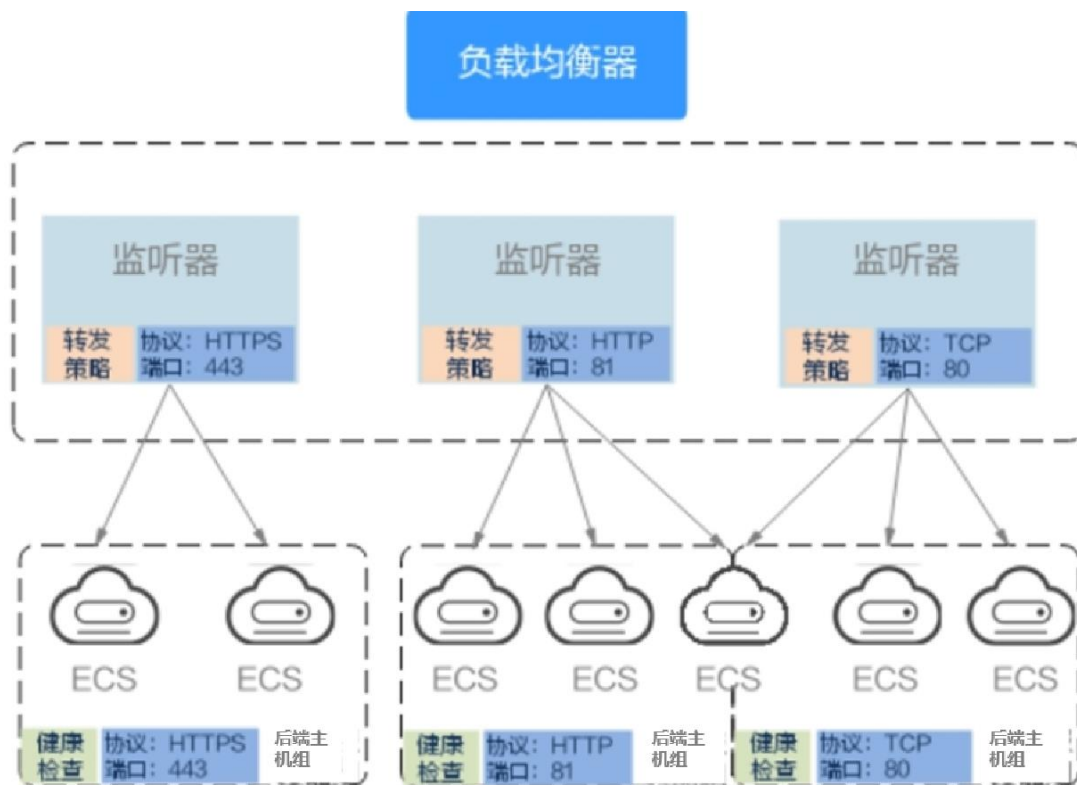


图1-1 弹性负载均衡组件图

弹性负载均衡的类型

弹性负载均衡支持独享型负载均衡、共享型负载均衡。

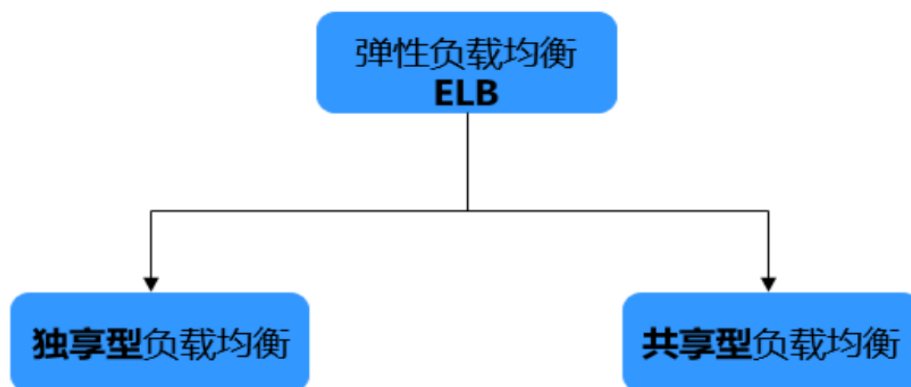


图1-2 弹性负载均衡类型

- 独享型负载均衡：独享型负载均衡实例资源独享，实例的性能不受其它实例的影响，您可根据业务需要选择不同规格的实例。
- 共享型负载均衡：属于集群部署，实例资源共享，实例的性能会受其它实例的影响，不支持选择实例规格。

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
请联系客户经理或天翼云客服了解具体 API 内容。

1.2 产品优势

独享型负载均衡的优势

- 超高性能
可实现性能独享，资源隔离，满足用户的海量业务访问需求。
此外，选择多个可用区之后，对应的性能规格（新建连接数/并发连接数等）会加倍。例如：单实例最大支持 2kw 并发，那么双 AZ 就支持 4kw 并发。

📖 说明

- 对于公网访问，会根据源 IP 的不同将流量分配到创建的多个 AZ 中的 ELB 上。
- 对于内网访问：
 - 当从创建 ELB 的 AZ 访问时，流量将被分配到本 AZ 中的 ELB 上，当本 AZ 的 ELB 不可用时，容灾到创建的其他 AZ 的 ELB 上；
 - 当从未创建 ELB 的 AZ 访问时，会根据源 IP 的不同将流量分配到创建的多个 AZ 中的 ELB 上。
- 高可用
支持多可用区的同城双活容灾，无缝实时切换。完善的健康检查机制，保障业务实时在线。
- 超安全
支持 TLS1.3，提供全链路 HTTPS 数据传输，支持多种安全策略，根据业务不同安全要求灵活选择安全策略。
- 多协议
支持 TCP/UDP/HTTP/HTTPS/QUIC 协议，满足不同协议接入需求。

- **无边界**
提供混合负载均衡能力（跨 VPC 后端），可以将同区域云上多 VPC 内的资源进行统一负载。
- **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。
- **可靠性**
支持跨可用区双活容灾，流量分发更均衡。

共享型负载均衡的优势

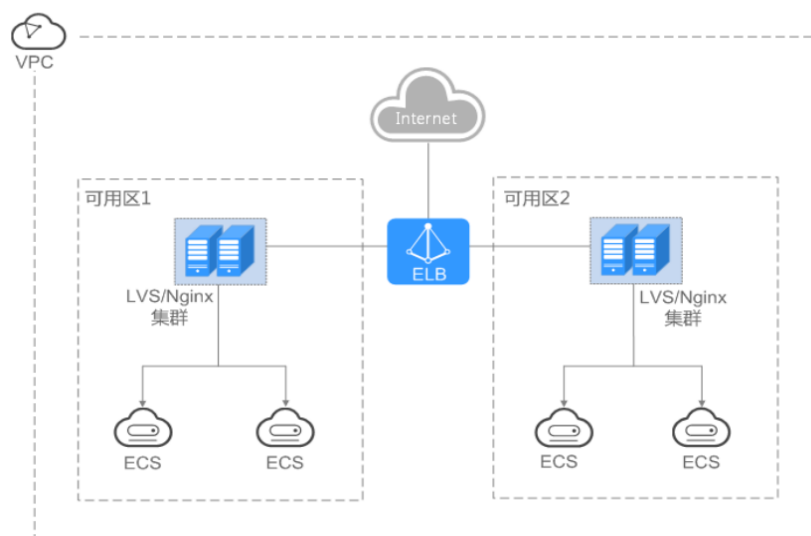


图1-3 高可用

- **多协议**
支持 TCP/UDP/HTTP/HTTPS，不支持 QUIC 协议，满足不同协议接入需求。
- **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 弹性负载均衡是如何工作的

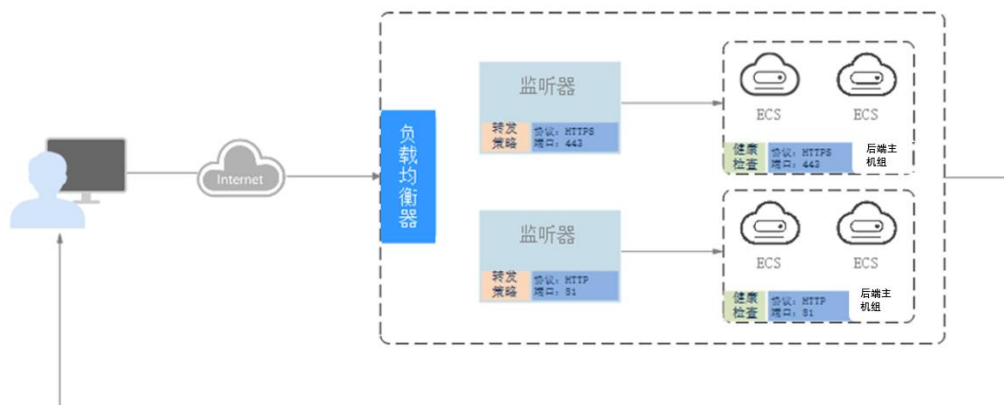


图1-4 ELB 工作原理图

弹性负载均衡的工作原理如下：

1. 客户端向您的应用程序发出请求。
2. 负载均衡器中的监听器接收与您配置的协议和端口匹配的请求。
3. 监听器再根据您的配置将请求转发至相应的后端主机组。如果配置了转发策略，监听器会根据您配置的转发策略评估传入的请求，如果匹配，请求将被转发至相应的后端主机组。
4. 后端主机组中健康检查正常的后端云主机将根据分配策略和您在监听器中配置的转发策略的路由规则接收流量，处理流量并返回客户端。

请求的流量分发与负载均衡器所绑定的监听器配置的转发策略和后端主机组配置的分配策略类型相关。

分配策略类型

独享型负载均衡支持加权轮询算法、加权最少连接、源 IP 算法。共享型负载均衡支持加权轮询算法、加权最少连接、源 IP 算法。

- **加权轮询算法：**根据后端云主机的权重，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，权重大的后端云主机被分配的概率高。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。

图 1-5 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 2 台权重相同的后端云主机，负载均衡器节点会将 50% 的客户端流量分发到其可用区中的每一台后端云主机。

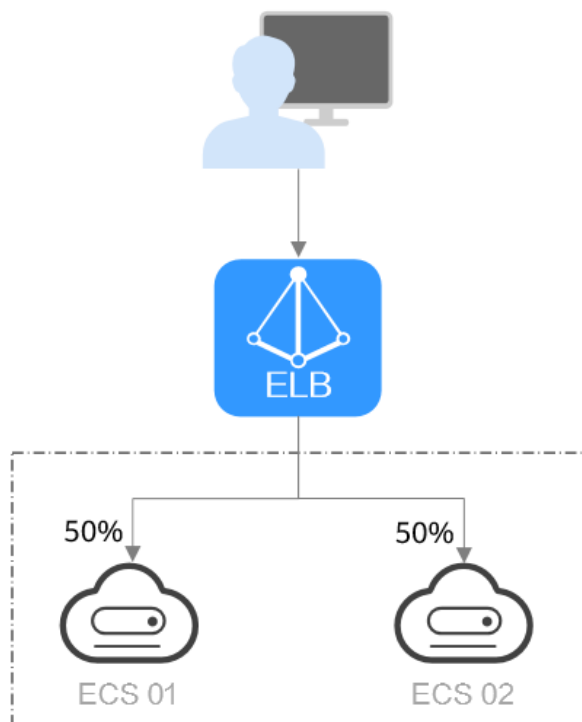


图1-5 加权轮询算法流量分发

- 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。

图 1-6 展示弹性负载均衡器使用加权最少连接算法的流量分发流程。假设可用区内有 2 台权重相同的后端云主机，ECS 01 已有 100 个连接，ECS 02 已有 50 个连接，则新的连接会优先分配到 ECS 02 上。

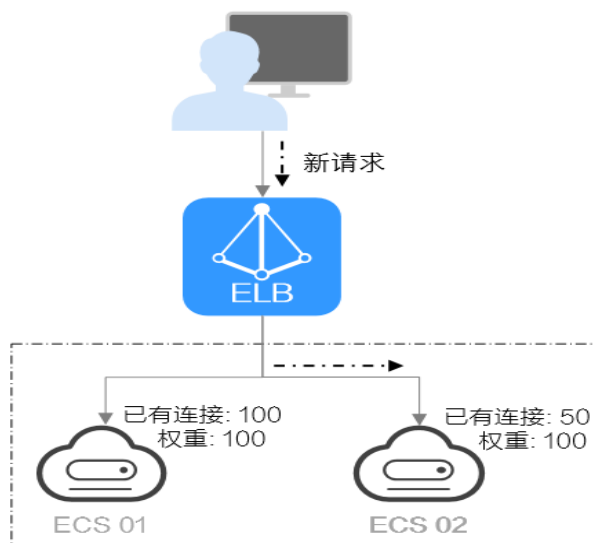


图1-6 加权最少连接算法流量分发

- 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，同时对后端云主机进行编号，按照运算结果将请求分发到对应编号的服务器上。这使得对同源 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。

图 1-7 展示弹性负载均衡器使用源 IP 算法的流量分发流程。假设可用区内有 2 台权重相同的后端云主机，ECS 01 已经处理了一个 IP-A 的请求，则 IP-A 新发起的请求会自动分配到 ECS 01 上。

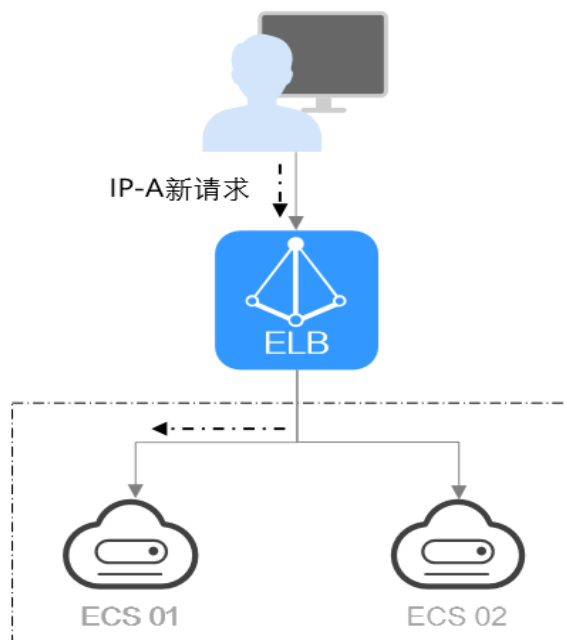


图1-7 源 IP 算法流量分发

影响负载均衡的因素

一般情况下，影响负载均衡的因素包括分配策略、会话保持、长连接、权重等。负载等相关。假设可用区内有 2 台权重相同且不为 0 的后端云主机，流量分配策略选择“加权最少连接”，未开启会话保持，ECS 01 已有 100 个连接，ECS 02 已有 50 个连接。如果有客户端 A 使用长连接访问了 ECS 01，长连接未断开期间，客户端 A 的业务流量将持续转发到 ECS 01，其他客户端的业务流量则根据分配策略优先分配到 ECS 02。

1.4 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云主机处理。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云主机。从

而提升访问效率，如图 1-9 所示。

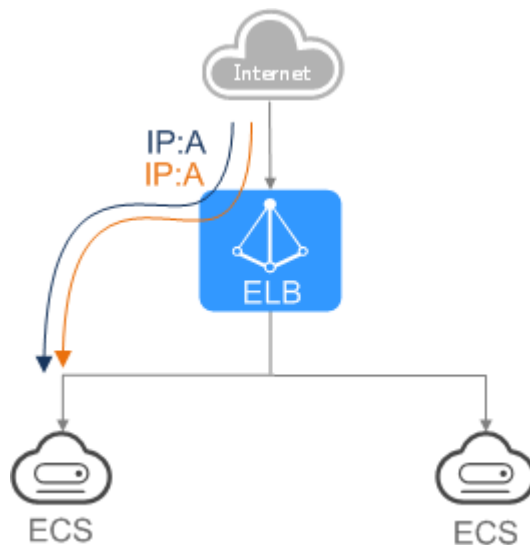


图1-8 会话保持流量分发

使用 ELB 消除单点故障

对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主机。负载均衡器会通过健康检查及时发现并屏蔽有故障的云主机，并将流量转发到其他正常运行的后端云主机，确保业务不中断，如 1-10 所示。

例如官网，计费业务，Web 业务等。

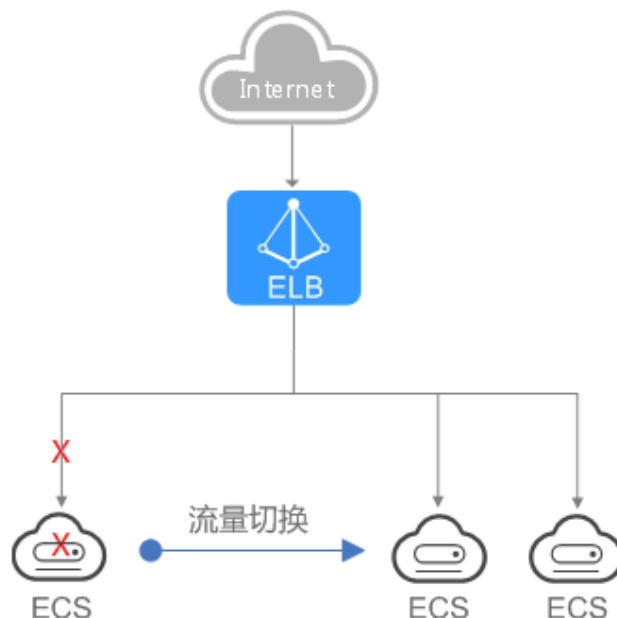


图1-9 消除单点故障

使用 ELB 跨可用区特性实现业务容灾部署

对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主机进行处理，如 1--11 所示。

例如银行业务，警务业务，大型应用系统等。

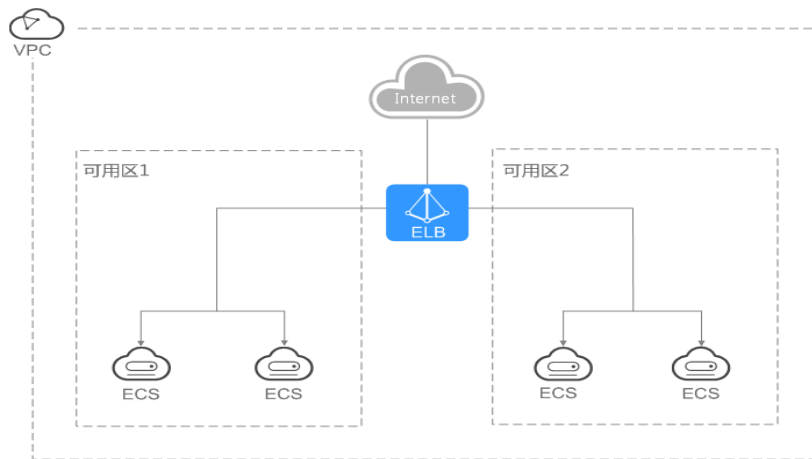


图1-10 多可用区部署

1.5 独享型负载均衡与共享型负载均衡的区别

弹性负载均衡有不同的负载均衡，分别是独享型负载均衡、共享型负载均衡，便于用户根据不同的应用场景和功能需求选择合适的负载均衡器类型。

独享型负载均衡对比共享型负载均衡，不仅支持多可用区和 IPv6 功能，在转发性能和稳定性上也有较大提升。具体的差异如下表所示。（“√”表示支持，“×”表示不支持。）

表1-1 性能对比

类型	独享型负载均衡	共享型负载均衡
部署模式	实例 性能独享 ， 资源隔离 ，实例的性能不受其它实例的影响，您可根据业务需要选择不同规格的实例。	资源节点所有用户共用集群性能。

类型	独享型负载均衡	共享型负载均衡
并发连接数	<p>单实例最高支持 2kw 并发，选择多个可用区后，对应的性能规格（新建连接数/并发连接数等）加倍。</p> <p>例如：单实例最大支持 2kw 并发，那么双 AZ 就支持 4kw 并发。</p> <p>说明</p> <ul style="list-style-type: none"> 对于公网访问，会根据源 IP 的不同将流量分配到创建的多个 AZ 中的 ELB 上。 对于内网访问： <ul style="list-style-type: none"> 当从创建 ELB 的 AZ 访问时，流量将被分配到本 AZ 中的 ELB 上，当本 AZ 的 ELB 不可用时，容灾到创建的其他 AZ 的 ELB 上； 当从未创建 ELB 的 AZ 访问时，会根据源 IP 的不同将流量分配到创建的多个 AZ 中的 ELB 上。 	<p>具体视资源节点的集群规模情况而定，如有连接数相关性能保障需求，建议选择独享型负载均衡。</p>

表1-2 功能对比-支持的协议

协议类型	描述	独享型负载均衡	共享型负载均衡
QUIC	<p>前端为 UDP 协议的监听器，支持 QUIC（Quick UDP Internet Connection）作为后端监听协议。使用 QUIC 协议的监听器具有低延迟、高可靠和无队头阻塞的优点，非常适合移动互联网应用、支持在 WIFI 和运营商网络中无缝切换，而不用重新去建立连接。</p>	√	×
HTTP/2	<p>HTTP/2，即超文本传输协议 2.0，是下一代 HTTP 协议。向下兼容 HTTP1.X 协议版本，同时性能和安全性都得到了提升。此功能目前仅支持协议类型为 HTTPS 的监听器。</p>	√	√
四层（TCP/UDP）协议	<p>四层负载均衡：支持 TCP 和 UDP 协议，监听器收到访问请求后，将请求直接转发给后端云主机。转发效率高，数据传输快。</p>	√	√

协议类型	描述	独享型负载均衡	共享型负载均衡
七层 (HTTP/HTTPS) 协议	七层负载均衡：支持 HTTP 和 HTTPS 协议，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。转发效率不如四层负载均衡，但是支持加密传输、基于 Cookie 的会话保持等高级功能。	√	√
WebSocket 协议	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。	√	√

表1-3 功能对比-支持的后端类型

后端类型	描述	独享型负载均衡	共享型负载均衡
配置混合负载均衡 (跨 VPC 后端)	独享型负载均衡实例支持混合负载均衡的能力，后端主机组不仅支持添加云上 VPC 内的服务器，还支持添加其他 VPC 的服务器。帮助用户根据业务诉求灵活配置。	√	×
SubENI (后端绑定辅助弹性网卡)	支持后端云主机绑定辅助弹性网卡。辅助弹性网卡 (Submission Elastic Network Interfaces, 以下简称 SubENI) 是一种基于弹性网卡的衍生资源，用于解决单个云主机实例挂载的弹性网卡超出上限，不满足用户使用需要的问题。辅助弹性网卡通过 VLAN 接口挂载在弹性网卡上，您可以通过创建辅助弹性网卡，使单个云主机实例挂载更多网卡，实现灵活、高可用的网络方案配置。	√	×
弹性云主机 (ECS)	后端云主机支持弹性云主机。	√	√

表1-4 功能对比-支持高级转发策略 (HTTP/HTTPS 监听器)

组成部分	类型	描述	独享型负载均衡	共享型负载均衡
转发规则	域名	触发转发的域名，仅支持精确域名。	√	√

组成部分	类型	描述	独享型负载均衡	共享型负载均衡
	URL	触发转发的 URL。 URL 的匹配规则有：精确匹配、前缀匹配、正则匹配。	√	√
	HTTP 请求方法	触发转发的 HTTP 请求方法。 主要有：GET、POST、PUT、DELETE、PATCH、HEAD、OPTIONS。	√	×
	HTTP 请求头	触发转发的 HTTP 请求头。 请求头是键值对的形式，需要分别设置值。	√	×
	查询字符串	当请求中的字符串与设置好的转发策略中的字符串相匹配时，触发转发。	√	×
	网段	触发转发的请求网段。	√	×
动作	转发至后端主机组	如果满足转发策略条件，则将请求转发至配置好的后端主机组。	√	√
	重定向至监听器	如果满足转发策略条件，则将请求转发至配置好的监听器上。	√	×
	添加重定向至 URL	如果满足转发策略条件，则将请求重定向至配置好的 URL。 客户端访问 ELB 网址 A 后，ELB 返回 302 或者其他 3xx 返回码和目的网址 B，客户端自动跳转到网址 B，网址 B 可自定义。	√	×
	返回固定响应	如果满足转发策略条件，则返回固定响应。 用户访问 ELB 实例后，ELB 直接返回响应，不向后端云主机继续转发，返回响应的状态码和内容可以自定义。	√	×

表1-5 功能对比-高级特性

特性类型	描述	独享型负载均衡	共享型负载均衡
支持选择实例规格	负载均衡提供多种规格供选择，不同规格的实例提供差异化的性能指标，可以根据具体的业务访问量，选择合适的规格。详见 1.6 独享型负载均衡实例规格。	√	×
支持全链路 HTTPS 数据传输	添加监听器时，前端协议选择“HTTPS”，后端协议也支持选择“HTTPS”。	√	×
支持 IPv6 地址	负载均衡支持转发来自 IPv6 客户端的请求。支持将负载均衡当前使用 IPv6 地址修改为其它子网的 IP 地址。	√	×
支持修改 IPv4 私有 IP	可以将负载均衡当前使用 IPv4 私有 IP 修改为当前子网或者其它子网的目标 IP 地址。	√	×
支持慢启动（后端服务延时接收流量）	弹性负载均衡支持七层（HTTP/HTTPS）后端协议开启慢启动功能，在设置的慢启动时间内线性增加请求分配权重，达到请求数线性增加的目的。慢启动能够实现业务的平滑启动，完美避免业务抖动问题。	√	×
支持 HTTPS 双向认证	开通双向认证，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。 此功能目前仅支持协议类型为 HTTPS 的监听器。	√	√
支持 SNI 多域名证书特性（开启 SNI）	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。开启 SNI 之后，用户需要添加域名对应的证书。	√	√
支持自定义超时时间	弹性负载均衡支持配置和修改监听器的超时时间（空闲超时时间、请求超时时间、响应超时时间），方便用户根据自身业务情况，自定义调整超时时间。例如，HTTP/HTTPS 协议客户端的请求文件比较大，可以增加请求超时时间，以便能够顺利完成文件的传输。 独享型负载均衡支持修改 TCP/UDP/HTTP/HTTPS 协议的超时时间。 共享型负载均衡器支持修改 TCP/HTTP/HTTPS 协议的超时时间，但是不支持修改 UDP 的超时时间。	√	√

特性类型	描述	独享型负载均衡	共享型负载均衡
支持安全策略	对于银行，金融类加密传输的应用，在创建和配置 HTTPS 监听器时，您可以选择使用安全策略，可以提高您的业务安全性。安全策略包含 TLS 协议版本和配套的加密算法套件。	√	×
支持获取监听器端口号	通过 X-Forwarded-Port 头字段获取 ELB 实例监听器端口号。	√	√
支持获取客户端请求端口号	通过 X-Forwarded-For-Port 头字段获取客户端请求端口号。	√	√
支持重写 X-Forwarded-Host	开关关闭：ELB 透传客户端的 X-Forwarded-Host。 开关开启：ELB 以客户端请求头的 Host 重写 X-Forwarded-Host 向后端传输。	√	√

表1-6 ELB 支持的其他特性

特性类型	描述	独享型负载均衡	共享型负载均衡
支持多可用区	<p>可以选择在多个可用区创建负载均衡实例，各可用区间根据算法采取最优路径处理访问请求，同时互为备份，提高业务处理效率和可靠性。</p> <p>此外，选择多个可用区之后，对应的性能规格（新建连接数/并发连接数等）会加倍。例如：单实例最大支持 2kw 并发，那么双 AZ 就支持 4kw 并发。</p> <p>说明</p> <ul style="list-style-type: none"> 对于公网访问，会根据源 IP 的不同将流量分配到创建的多个 AZ 中的 ELB 上。 对于内网访问： <ul style="list-style-type: none"> 当从创建 ELB 的 AZ 访问时，流量将被分配到本 AZ 中的 ELB 上，当本 AZ 的 ELB 不可用时，容灾到创建的其他 AZ 的 ELB 上； 当从未创建 ELB 的 AZ 访问时，会根据源 IP 的不同将流量分配到创建的多个 AZ 中的 ELB 上。 	√	×

特性类型	描述	独享型负载均衡	共享型负载均衡
支持加权轮询算法 /加权最少连接/源 IP 算法	弹性负载均衡支持的分配策略类型有：加权轮询算法、加权最小连接、源 IP 算法。	√	√
支持公网和私网负载均衡	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主机进行处理。 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。	√	√
支持修改公网带宽	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 ELB 实例关联的弹性公网 IP 的带宽。	√	√
支持绑定/解绑 EIP	可以根据业务需要为负载均衡实例绑定 IP 地址，或者将负载均衡实例已经绑定的 IP 地址进行解绑。	√	√
支持会话保持	会话保持功能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。	√	√
支持访问控制	可以通过添加白名单和黑名单的方式控制访问负载均衡监听器的 IP。 通过白名单能够设置允许特定 IP 访问，而其它 IP 不许访问。 通过黑名单能够设置允许特定的 IP 不能访问，而其它 IP 允许访问。	√	√
支持健康检查	负载均衡器会定期向后端云主机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云主机是否可用。	√	√
支持管理证书	负载均衡器支持两种类型的证书，服务器证书和 CA 证书。配置 HTTPS 监听器时，需要为监听器绑定服务器证书，如果开启双向认证功能，还需要绑定 CA 证书。您可以创建证书、更换证书等。	√	√

特性类型	描述	独享型负载均衡	共享型负载均衡
支持添加标签	对于拥有大量云资源的用户，可以通过给云资源打标签，快速查找具有某标签的云资源，可对这些资源标签统一进行检视、修改、删除等操作，方便用户对云资源的管理。	√	√
支持访问日志	通过对接云日志服务，可以查看和分析七层负载均衡 HTTP 和 HTTPS 的详细访问记录，包括请求时间、客户端 IP 地址、请求路径和服务器响应等。	√	√
支持查看监控指标	通过配置监控，您可以对弹性负载均衡器的运行状态进行日常监控，可以查看弹性负载均衡器的各项监控指标。	√	√
支持审计日志	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。	√	√

1.6 独享型负载均衡实例规格

独享型负载均衡支持按规格购买，关键指标如下，请根据自身业务规划选择实例规格。实际业务超过规格限定时，会限制新建请求的建立、以及丢包等问题。

- 并发最大连接数-Max Connection**
 并发最大连接数是指在四层监听或者七层监听时，一个负载均衡实例能够承载的最大连接数量。当实例上的连接数超过规格定义的最大连接数时，为了保障已有的连接业务性能，新建连接请求将被丢弃。
- 每秒新建连接数-Connection Per Second (CPS)**
 每秒新建连接数是指在四层监听或者七层监听时，新建连接的速率。当新建连接的速率超过规格定义的每秒新建连接数时，为了保障已有的连接业务性能，新建连接请求将被丢弃。
 对于七层监听器，HTTPS 监听器在建立连接时，使用 SSL 握手会占用更多系统资源，因此 HTTPS 的每秒新建连接数相当于 1/10 倍的 HTTP 每秒新建连接数。如小型 I 的新建连接数为 10000，指的是 HTTP 新建连接数为 10000，HTTPS 每秒新建连接数为 $10000 * 1/10 = 1000$ 。
- 每秒查询数-Query Per Second (QPS)**
 每秒查询数是指仅在七层监听时，每秒可以处理的 HTTP/HTTPS 的查询请求的数量。当请求速率超过规格所定义的每秒查询数时，为了保障已有的连接业务性能，新建连接请求将被丢弃。
- 每秒带宽 (MB/S)**
 每秒带宽可以在四层监听或者七层监听时保障带宽的性能。

独享型负载均衡开放的实例规格，如表 1-7 和表 1-8 所示。（各地域因资源情况不同，开放的规格可能略有差异，请以控制台购买页为准）

⚠ 注意

独享型负载均衡的类型选定后将无法修改，请您合理评估选择。

例如：您初始创建了网络型 ELB 实例，则只能创建 TCP/UDP 监听器，无法添加或修改为应用型 ELB 实例，即无法创建 HTTP/HTTPS 监听器。

表1-7 独享型负载均衡实例规格-网络型(TCP/UDP)

规格类型	最大连接数	新建连接数(CPS)	带宽(Mb/S)	折算 LCU 数(个/AZ)
小型 I	500000	10000	50	10
小型 II	1000000	20000	100	20
中型 I	2000000	40000	200	40
中型 II	4000000	80000	400	80
大型 I	10000000	200000	1000	200
大型 II	20000000	400000	2000	400

表1-8 独享型负载均衡实例规格-应用型(HTTP/HTTPS)

规格类型	最大连接数	新建连接数(CPS)(HTTP)	新建连接数(CPS)(HTTPS)	每秒查询数(QPS)(HTTP)	每秒查询数(QPS)(HTTPS)	带宽(Mb/S)	折算 LCU 数(个/AZ)
小型 I	200000	2000	200	4000	2000	50	10
小型 II	400000	4000	400	8000	4000	100	20
中型 I	800000	8000	800	16000	8000	200	40
中型 II	2000000	20000	2000	40000	20000	400	100
大型 I	4000000	40000	4000	80000	40000	1000	200
大型 II	8000000	80000	8000	160000	80000	2000	400

 说明

- 如果一个负载均衡器下创建了多个监听器，则上述表格中的每秒查询数（QPS）是指该负载均衡器下的所有监听器的 QPS 之和不超过规格所定义的 QPS 值。
- 带宽规格是指入流量加出流量的总和不超过表中的数值。如：对于小型 I 独享型负载均衡，入流量+出流量≤50Mb/S。
- 带宽规格是 ELB 所能提供的带宽保障范围，保障范围内资源可用；超出保障范围的，无法保障带宽性能。

1.7 公网和私网负载均衡器

负载均衡按照支持的**网络类型**的不同分为**公网负载均衡器**和**私网负载均衡器**。

公网负载均衡器

通过给负载均衡器绑定弹性公网 IP，使其支持转发公网流量请求，称为公网负载均衡器。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主机进行处理。

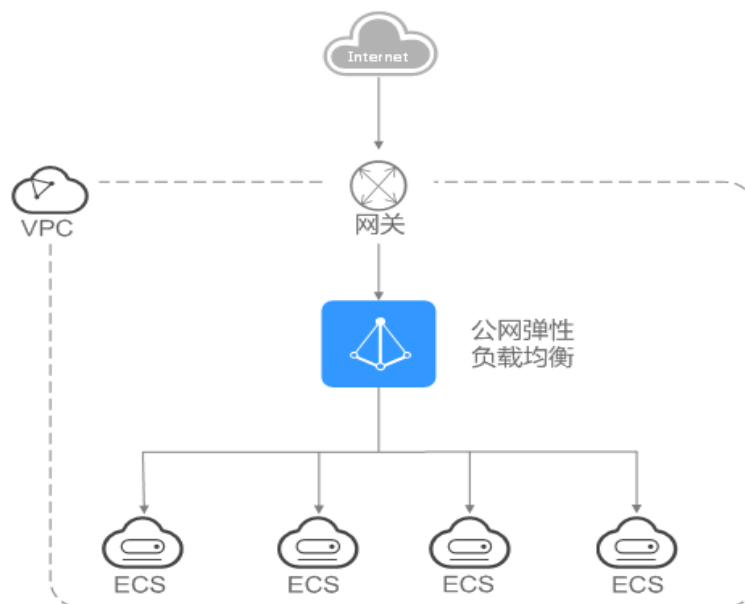


图1-11 公网负载均衡器

私网负载均衡器

通过给负载均衡器绑定弹性私网 IP，使其支持转发私网流量请求，称为私网负载均衡器。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。

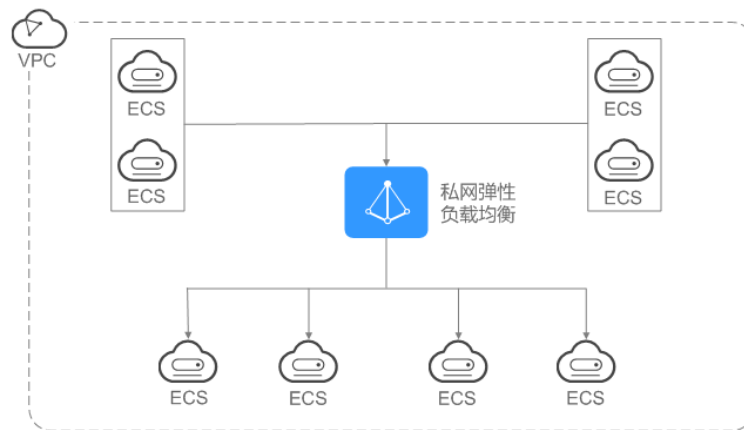


图1-12 私网负载均衡器

实例规格类型与公网/私网负载均衡器的对应关系

表1-9 独享型负载均衡与公网/私网负载均衡器的对应关系

实例规格类型	网络类型	对应关系
独享型负载均衡	IPv4 公网	ELB 绑定弹性公网 IP，支持 IPv4 公网流量请求的，称为公网负载均衡器。
	IPv4 私网	ELB 绑定私网 IP，支持 IPv4 私网流量请求的，称为私网负载均衡器。
	IPv6	既支持 IPv6 公网请求又支持 IPv6 私网请求。 ELB 绑定弹性公网 IP，支持 IPv6 公网流量请求的，称为公网负载均衡器。 ELB 绑定私网 IP，支持 IPv6 私网流量请求的，称为私网负载均衡器。

表1-10 共享型负载均衡与公网/私网负载均衡器的对应关系

实例规格类型	网络类型	对应关系
共享型负载均衡	公网	既支持公网流量请求又支持私网流量请求。 ELB 绑定弹性公网 IP，支持公网流量请求的，称为公网负载均衡器。 ELB 绑定私网 IP，支持私网流量请求的，称为私网负载均衡器。
	私网	ELB 绑定私网 IP，支持私网流量请求的，称为私网负载均衡器。

1.8 ELB 网络流量路径说明

负载均衡将来自客户端的请求通过负载均衡器分发至后端云主机，后端云主机再将响应通过内网返回给负载均衡。负载均衡器和后端云主机之间是通过内网进行通信的。

- 如果负载均衡器后端云主机仅处理来自负载均衡的访问请求，服务器可以不购买 EIP 或者 NAT 网关等服务，仅有私网 IP 即可。
- 如果负载均衡器后端云主机还需要直接对公网提供服务，或者需要访问公网资源，则服务器需要购买 EIP 或者 NAT 网关等服务。

入网流量路径

对于入网流量，负载均衡会根据用户配置的流量分配策略，对来自公网或者私网的访问请求进行转发和处理。如图 1-14 所示。

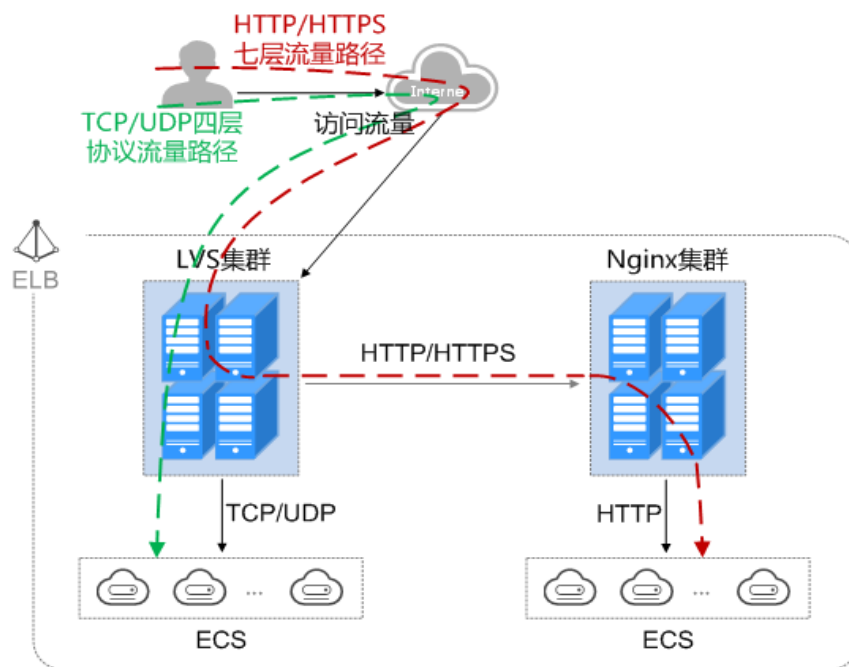


图1-13 入网流量路径

当负载均衡器使用四层协议 TCP/UDP 时：

- 四层协议 TCP/UDP 的流量只经过 LVS 集群进行转发。
- LVS 集群的所有节点会根据负载均衡器的流量分配策略，将接收到的访问请求直接分发到后端云主机。

当负载均衡器使用七层协议 HTTP/HTTPS 时：

- 七层协议 HTTP/HTTPS 的流量，需要经过 LVS 集群先将访问请求平均分发到 Nginx 集群的所有节点，然后 Nginx 集群的节点再根据负载均衡器的转发策略，将接收到的请求最终分发到后端云主机。
- 七层协议 HTTPS 的流量，在最终分发到服务器前，还需要在 Nginx 集群内进行证书验证以及数据包的解密操作。然后通过 HTTP 协议将请求分发到后端云主机。

出网流量路径

出网流量遵循请求从哪进来，响应从哪出去的原则。如出网流量路径所示。

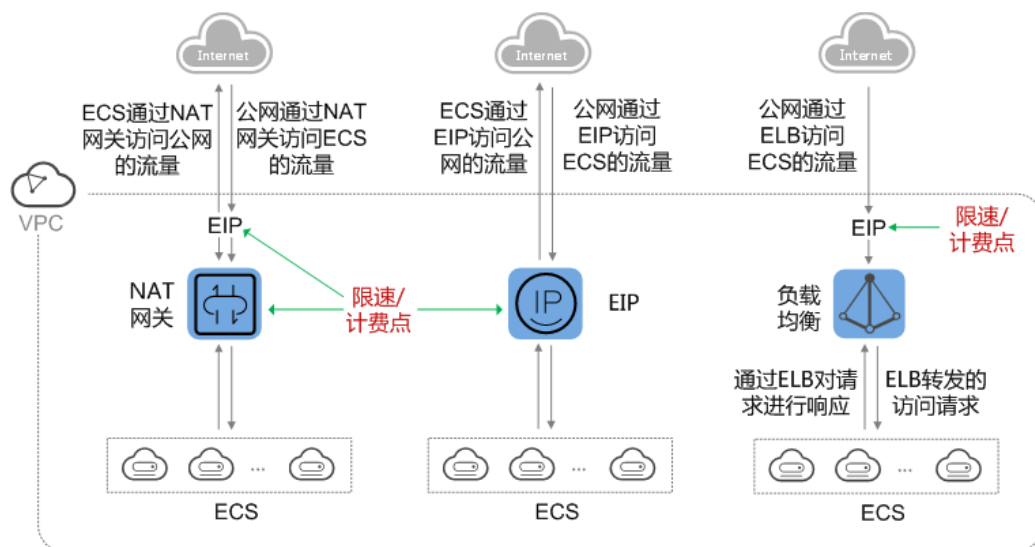


图1-14 出网流量路径

- 通过负载均衡器进入的访问流量，对应的响应流量通过负载均衡器返回。
 由于负载均衡器实际是通过绑定的 EIP 接收来自公网的流量和响应请求，所以负载均衡器的限制实际是在负载均衡器绑定的 EIP 上，并在 EIP 上进行计费。从负载均衡到后端云主机之间通过 VPC 内网进行通信，不收取费用。
- 通过 NAT 网关进入的访问流量，对应的响应流量通过 NAT 网关返回。在 NAT 网关上限速和计费。
 由于 NAT 网关实际是通过绑定的 EIP 接收来自公网的流量和访问公网，所以 NAT 网关上进行的是连接数的限制，带宽或者流量的限制是在 NAT 网关绑定的 EIP 上，并分别在 NAT 网关和弹性公网 IP 上进行计费。
- 通过 EIP 进入的访问流量，对应的响应流量通过 EIP 返回，在 EIP 上限速和计费。

1.9 权限管理

如果您需要对云上购买的弹性负载均衡（Elastic Load Balance，简称 ELB）资源，给企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称 IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制云上资源的访问。

通过 IAM，您可以在云帐号中给员工创建 IAM 用户，并使用策略来控制他们对云上资源的访问范围。例如您的员工中有负责软件开发的人员，您希望他们拥有 ELB 的使用权限，但是不希望他们拥有删除负载均衡器等高危操作的权限，那么您可以使用 IAM 为开发人员创建用户，通过授予仅能使用负载均衡器，但是不允许删除负载均衡器的权限策略，控制他们对 ELB 资源的使用范围。

如果帐号已经能满足您的要求，不需要创建独立的 IAM 用户进行权限管理，您可以跳过本章节，不影响您使用 ELB 服务的其它功能。

IAM 是提供权限管理的基础服务。关于 IAM 的详细介绍，请参见《IAM 产品介绍》。

ELB 权限

默认情况下，帐号管理员创建的 IAM 用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

ELB 部署时通过物理区域划分，为项目级服务。授权时，“作用范围”需要选择“区域级项目”，然后在指定区域对应的项目中设置相关权限，并且该策略仅对此项目生效，如果在“所有项目”中设置权限，则该权限在所有区域项目中都生效。访问 ELB 时，需要先切换至授权区域。

根据授权精细程度分为角色和策略。

- **角色：** IAM 最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于云上各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- **策略：** IAM 最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对 ELB 服务，帐号管理员能够控制 IAM 用户仅能对某一类云主机资源进行指定的管理操作。多数细粒度策略以 API 接口为粒度进行权限拆分，ELB 支持的 API 授权项请参见《弹性负载均衡接口参考》。

如表 1-11 所示，包括了 ELB 的所有系统权限。

表1-11 ELB 系统权限

系统角色/策略名称	描述	类别
ELB FullAccess	操作权限：对弹性负载均衡服务的所有执行权限。 作用范围：项目级服务。	系统策略
ELB ReadOnlyAccess	操作权限：对弹性负载均衡服务的只读权限。 作用范围：项目级服务。	系统策略

系统角色/策略名称	描述	类别
ELB Administrator	<p>操作权限：对弹性负载均衡服务的所有执行权限。拥有该权限的用户必须同时拥有 Tenant Administrator、VPC Administrator、CES Administrator、Server Administrator、Tenant Guest 权限。</p> <p>作用范围：项目级服务。</p> <p>说明</p> <ul style="list-style-type: none"> 此策略名称之前为 ELB Service Administrator，新的策略名称于 2020/3/30 22:00（北京时间）正式生效。 如果帐号已经申请开通细粒度权限，设置 ELB 系统权限时请配置细粒度策略，不要配置 RBAC 策略。 	系统角色

表 1-12 列出了 ELB 常用操作与系统权限的授权关系，您可以参照该表选择合适的系统权限。

表1-12 常用操作与系统策略的关系

操作	ELB FullAccess	ELB ReadOnlyAccess	ELB Administrator
创建负载均衡器	√	×	√
查询负载均衡器	√	√	√
查询负载均衡器状态树	√	√	√
查询负载均衡器列表	√	√	√
更新负载均衡器	√	×	√
删除负载均衡器	√	×	√
创建监听器	√	×	√
查询监听器	√	√	√
修改监听器	√	×	√
删除监听器	√	×	√
创建后端主机组	√	×	√
查询后端主机组	√	√	√
修改后端主机组	√	×	√
删除后端主机组	√	×	√

操作	ELB FullAccess	ELB ReadOnlyAccess	ELB Administrator
创建后端云主机	√	×	√
查询后端云主机	√	√	√
修改后端云主机	√	×	√
删除后端云主机	√	×	√
创建健康检查	√	×	√
查询健康检查	√	√	√
修改健康检查	√	×	√
关闭健康检查	√	×	√
创建弹性公网 IP	×	×	√
绑定弹性公网 IP	×	×	√
查询弹性公网 IP	√	√	√
解绑弹性公网 IP	×	×	√
查看监控指标	×	×	√
查看访问日志	×	×	√

📖 说明

- 解绑弹性公网 IP，还需要配置 VPC 服务的 vpc:bandwidths:update 和 vpc:publicIps:update 细粒度权限，具体可联系客户经理或天翼云客服系统。
- 查看监控指标，还需要配置 CES 服务的 CES ReadOnlyAccess 权限，具体可在云监控服务中查询。
- 查看访问日志，还需要配置 LTS 服务的 LTS ReadOnlyAccess 权限，具体可在云日志服务中查询。

1.10 基本概念

1.10.1 产品基本概念

表1-13 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，分发流量到后端云主机处理。
后端云主机	负载均衡器会将客户端的请求转发给后端云主机处理。例如，您可以添加 ECS 实例作为负载均衡器的后端云主机，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主机组里的后端云主机。
后端主机组	把具有相同特性的后端云主机放在一个组，负载均衡实例进行流量分发时，流量分配策略以后端主机组为单位生效。
健康检查	负载均衡器会定期向后端云主机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云主机是否可用。负载均衡器如果判断后端云主机健康检查异常，就不会将流量分发到异常后端云主机，而是分发到健康检查正常的后端云主机，从而提高了业务的可靠性。当异常的后端云主机恢复正常运行后，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 。
会话保持	会话保持，指负载均衡器可以识别客户与服务器之间交互过程的关联性，在实现负载均衡的同时，保持将其他相关联的访问请求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 的客户端和服务器端通过握手连接，连接成功后才能相互通信。
SNI	您需要在创建 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域名证书的 TLS 扩展，开启 SNI 之后，用户需要添加域名对应的证书。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。
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。

名词	说明
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。

1.10.2 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）从地理位置和网络时延维度划分，同一个 Region 内共享弹性计算、块存储、对象存储、VPC 网络、弹性公网 IP、镜像等公共服务。Region 分为通用 Region 和专属 Region，通用 Region 指面向公共租户提供通用云服务的 Region；专属 Region 指只承载同一类业务或只面向特定租户提供业务服务的专用 Region。
- 可用区（AZ，Availability Zone）一个 AZ 是一个或多个物理数据中心的集合，有独立的风火水电，AZ 内逻辑上再将计算、网络、存储等资源划分成多个集群。一个 Region 中的多个 AZ 间通过高速光纤相连，以满足用户跨 AZ 构建高可用性系统的需求。

0 阐明了区域和可用区之间的关系。

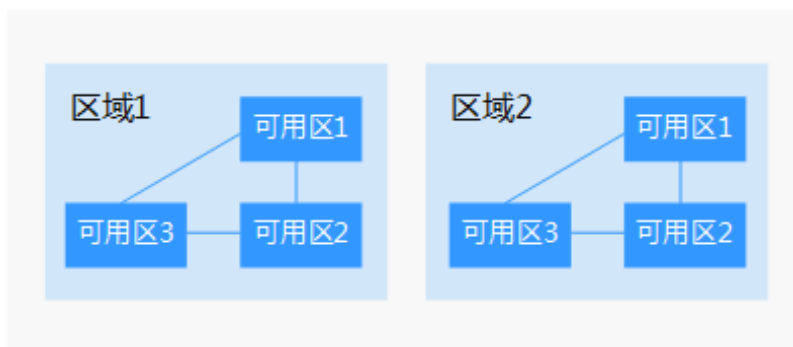


图1-15 区域和可用区

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。请向管理员获取区域和终端节点信息。

1.11 与其他服务的关系

弹性负载均衡与其他服务的依赖关系如图 1-18 所示。

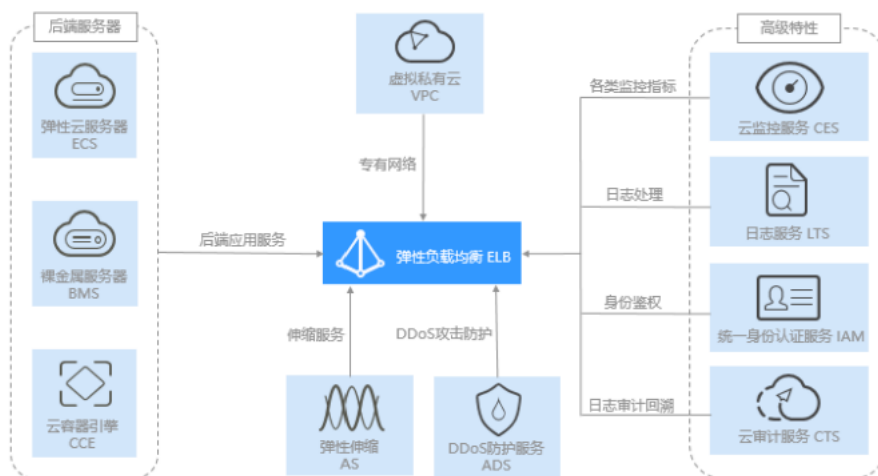


图1-16 弹性负载均衡服务与其他服务的关系示例图。

表1-14 弹性负载均衡与其他服务之间的关系

服务名称	交互功能
弹性云主机	通过相关服务部署用户业务，并接收 ELB 分发的访问流量。
虚拟私有云	创建 ELB 时需要使用虚拟私有云服务创建的弹性公网 IP、带宽。
统一身份认证服务	需要统一身份认证提供鉴权。
云审计服务	使用云审计服务记录弹性负载均衡服务的资源操作。
云监控服务	当用户开通了弹性负载均衡服务后，无需额外安装其他插

服务名称	交互功能
	件，即可在云监控查看对应服务的实例状态。
DDos 防护服务	当用户购买了 DDoS 防护服务后，配置了负载均衡器的公网 IP，确保了弹性负载均衡服务免受外部攻击，提高安全可靠性的。
云日志服务	配置访问日志时需要您对接云日志服务，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。

2 快速入门

2.1 入门概述

您可以使用独享型负载均衡或共享型负载均衡创建一个负载均衡实例，将访问请求分发到多台弹性云主机上。

该快速入门以具体场景为例，指引您使用共享型负载均衡快速创建一个负载均衡实例，将访问请求分发到两台弹性云主机上。

- 用于业务有大量访问请求，需要通过 ELB 实例将访问流量分发到两台弹性云主机进行处理，实现业务流量的负载分担。同时，通过配置健康检查，负载均衡实例可以监控弹性云主机的运行状况，自动将访问流量分发到正常工作的弹性云主机进行处理，消除单点故障，提升业务的可用性。

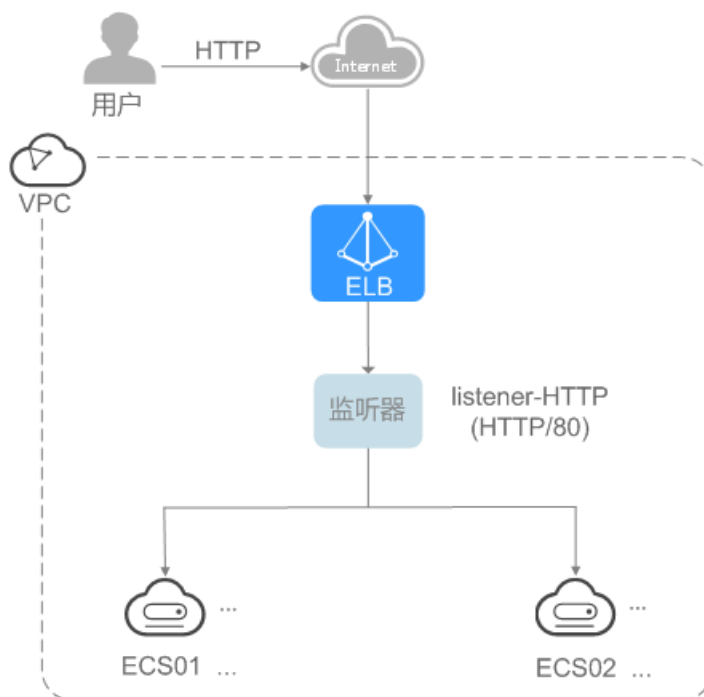


图2-1 简易图

方案延伸：可根据业务的实际访问量，将快速入门场景中的两台弹性云主机扩展到多台。以满足实际业务流量下的负载分担需求。

2.2 入门流程

图 2-2 为入门使用流程。



图2-2 入门流程

2.3 共享型增强型负载均衡快速入门

操作场景

假如您有一个 Web 应用，由于业务量比较大，需要使用两个弹性云主机（简称 ECS）进行业务负载分担。

共享型负载均衡可以将访问流量根据流量分配策略分发到后端多台服务器，实现业务的负载分担。同时消除了单点故障，提升了业务的可用性。

前提条件

- 后端云主机的安全组已经开通了业务需要使用的端口（也可以先开通所有端口，

业务部署完成后再限制不使用的端口)。

- 由于共享型弹性负载均衡通过“100.125.0.0/16”网段的 IP 与后端云主机互访，为了保证健康检查功能正常使用，后端云主机的安全组必须开通“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，后端云主机安全组规则和网络 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“跨 VPC 后端”功能时，后端云主机安全组规则和网络 ACL 规则均无需放通 ELB 所在的 VPC 网段。

创建弹性云主机

负载均衡只负责流量转发，不具备处理请求的能力。因此，需要通过 ECS 实例处理用户的请求。

在当前场景中，弹性云主机需要创建并绑定弹性 IP（简称 EIP）。ECS 绑定 EIP 仅作为本次示例中配置 ECS 后端业务所需，用户实际使用时，需要根据自身业务规划确定 ECS 是否绑定 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 > 计算 > 弹性云主机”。
4. 在“弹性云主机”界面单击“创建弹性云主机”，根据界面提示配置参数，并单击“立即申请”。

示例中使用的两台弹性云主机的规格如下：

表2-1 弹性云主机规格

参数项	参数值
名称	ECS01、ECS02
操作系统	CentOS 7.2 64bit
CPU	2vCPUs
内存	4GB
系统盘	40GB
数据盘	100GB
公网带宽	5 Mbit/s

5. 单击“提交”。

搭建后端服务

在 ECS 实例上部署 Nginx，编辑 HTML 页面，使访问 ECS01 时返回一个标题为

“Welcome to ELB test page one!” 的页面，访问 ECS02 时返回一个标题为 “Welcome to ELB test page two!” 的页面。

1. 登录弹性云主机。
2. 安装 nginx。
 - a. 使用 `wget` 命令，下载对应当前操作系统版本的 Nginx 安装包。此处以 CentOS 7.6 版本的操作系统为例。

```
wget http://nginx.org/packages/centos/7/noarch/RPMS/nginx-release-centos-7-0.el7ngx.noarch.rpm
```

- b. 执行以下命令，建立 Nginx 的 yum 仓库。此处以 CentOS 7.6 版本的操作系统为例。

```
rpm -ivh nginx-release-centos-7-0.el7ngx.noarch.rpm
```

- c. 执行以下命令，安装 Nginx。

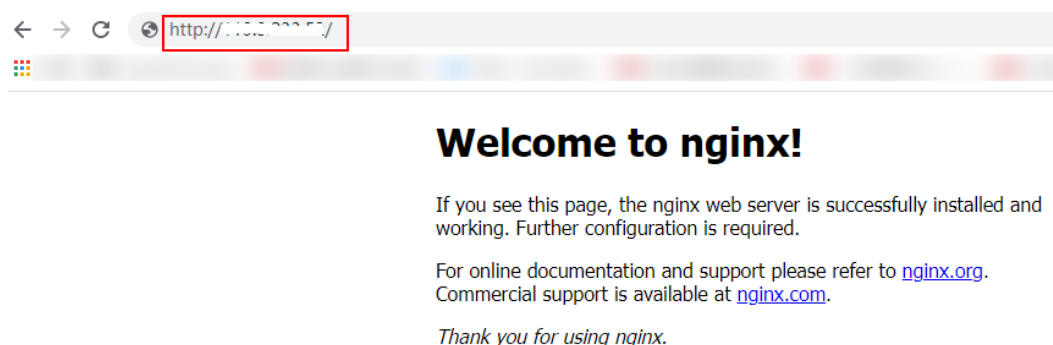
```
yum -y install nginx
```

- d. 执行以下命令，启动 Nginx 并设置开机启动。

```
systemctl start nginx
systemctl enable nginx
```

- e. 在任意终端使用浏览器访问 “`http://ECS 的公网IP 地址`”，显示如下页面，说明 nginx 安装成功。

图2-3 nginx 安装成功



3. 修改 ECS 实例 ECS01 的 html 页面。

Nginx 的默认根目录是 “`/usr/share/nginx/html`”，修改 “`index.html`” 页面，用来标识到 ECS01 的访问。

- a. 执行以下命令打开文件 “`index.html`”。

```
vim /usr/share/nginx/html/index.html
```

- b. 按 `i` 键进入编辑模式。

- c. 修改打开的 “`index.html`” 文件。

修改文件内容，涉及内容修改部分如下所示：

```
...
<body>
    <h1>Welcome to <strong>ELB</strong> test page one!</h1>
```

```

<div class="content">
  <p>This page is used to test the <strong>ELB</strong>!</p>

  <div class="alert">
    <h2>ELB01</h2>
    <div class="content">
      <p><strong>ELB test (page one)!</strong></p>
      <p><strong>ELB test (page one)!</strong></p>
      <p><strong>ELB test (page one)!</strong></p>
    </div>
  </div>
</div>
</body>
    
```

d. 按 **Esc** 键退出编辑模式，并输入:**wq** 保存后退出。

4. 修改 ECS 实例 ECS02 的 html 页面。

Nginx 的默认根目录是 “/usr/share/nginx/html”，修改 “index.html” 页面，用来标识到 ECS02 的访问。

a. 执行以下命令打开文件 “index.html”。

```
vim /usr/share/nginx/html/index.html
```

b. 按 **i** 键进入编辑模式。

c. 修改打开的 “index.html” 文件。

修改文件内容，涉及内容修改部分如下所示：

```

...
<body>
  <h1>Welcome to <strong>ELB</strong> test page two!</h1>

  <div class="content">
    <p>This page is used to test the <strong>ELB</strong>!</p>

    <div class="alert">
      <h2>ELB02</h2>
      <div class="content">
        <p><strong>ELB test (page two)!</strong></p>
        <p><strong>ELB test (page two)!</strong></p>
        <p><strong>ELB test (page two)!</strong></p>
      </div>
    </div>
  </div>
</body>
    
```

d. 按 **Esc** 键退出编辑模式，并输入:**wq** 保存后退出。

5. 使用浏览器分别访问 “[http://ECS01 的公网IP 地址](http://ECS01的公网IP地址)” 和 “[http://ECS02 的公网IP 地址](http://ECS02的公网IP地址)”，验证 nginx 服务。

如果页面显示修改后的 html 页面，说明 nginx 部署成功。

ECS01 的 html 页面：

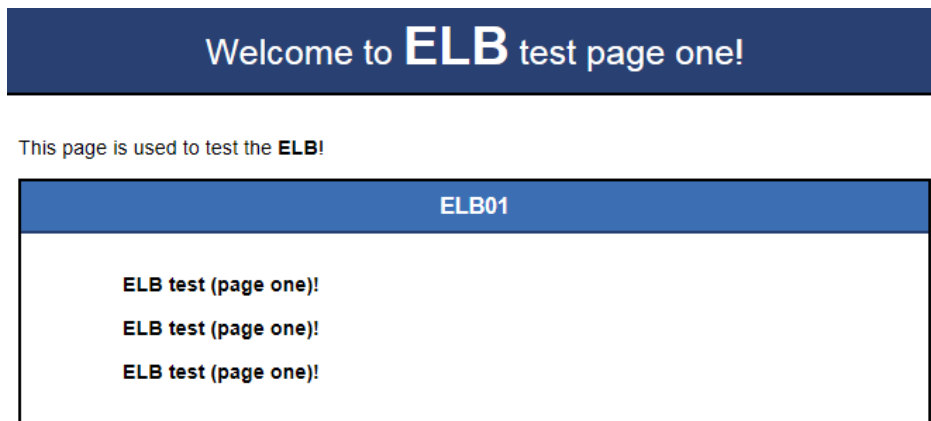


图2-4 ECS01 的 nginx 部署成功页面

ECS02 的 html 页面:

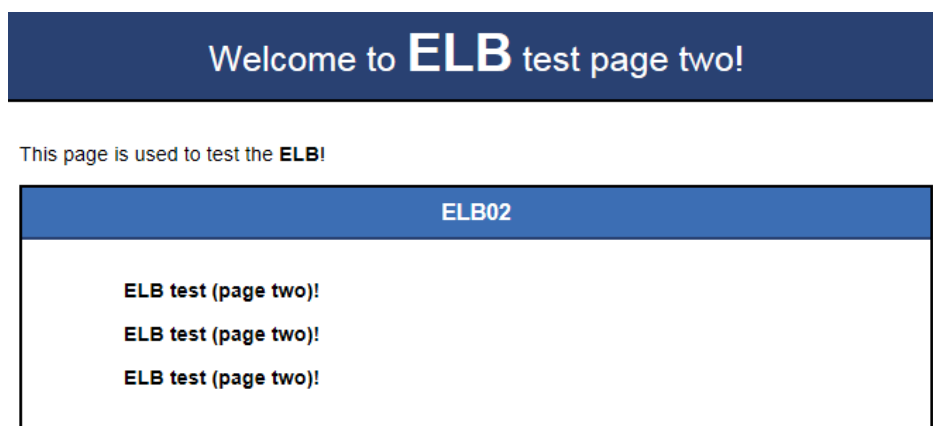




图2-5 ECS02 的 nginx 部署成功页面

新建负载均衡器

在当前场景中，ELB 需要创建并绑定弹性 IP（简称 EIP）。ELB 绑定 EIP 仅作为本次示例中通过 ELB 访问后端业务所需，用户实际使用时，需要根据自身业务规划确定 ELB 是否绑定 EIP。具体原则请参见 1.7 公网和私网负载均衡器。

1. 在管理控制台左上角单击   图标，选择区域和项目。
2. 选择“服务列表 > 网络 > 弹性负载均衡”。
3. 在“负载均衡器”界面单击“创建弹性负载均衡”，根据界面提示配置参数。
4. 单击“立即申请”。
5. 确认配置信息，并单击“提交”。
6. 创建完成后，在“负载均衡器”界面，选择对应的区域即可看到新建的负载均衡器。

添加监听器

负载均衡监听器通过指定的协议和端口进行流量转发。同时监听器将根据健康检查的配置自动检查其后端云主机的运行状况。如果发现某台服务器运行不正常，则会停止向该服务器发送流量，并重新将流量发送至正常运行的服务器。

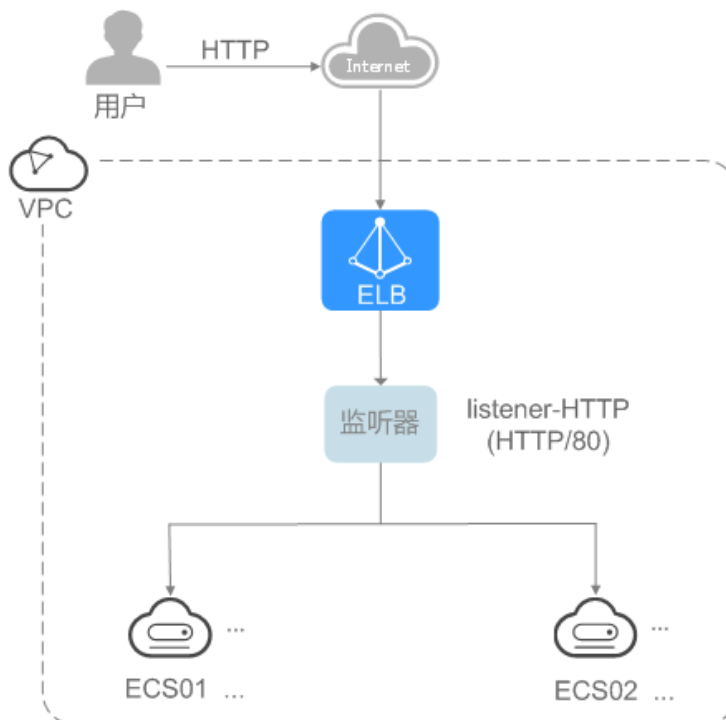


图2-6 数据转发示意图

1. 选择“服务列表 > 网络 > 弹性负载均衡”。
2. 在“负载均衡器”界面，单击需要添加监听器的负载均衡名称“elb-01”。
3. 切换到“监听器”页签，单击“添加监听器”。
4. 配置监听器，单击“下一步”。

名称：监听器名称，示例为“listener-HTTP”。

前端协议/端口：负载分发的协议和端口，示例为“HTTP/80”。

5. 配置后端主机组和开启健康检查，单击“完成”。

后端主机组

- 名称：后端主机组名称，示例为“server_group-ELB”。
- 分配策略类型：负载均衡采用的算法，示例为“加权轮询算法”。

健康检查配置

- 协议：前端协议为 TCP、HTTP 或者 HTTPS 时，健康检查支持 TCP 和 HTTP 协议，设置后不可修改，示例为“HTTP”。
- 域名：健康检查的请求域名。示例为“www.example.com”。
- 端口：健康检查端口号，示例为“80”。

未配置健康检查端口时，默认使用后端云主机端口进行健康检查。配置后，使用配置的健康检查端口进行健康检查。

6. 在新添加的监听器下，单击后端主机组页签的“添加”。

- 勾选需要添加的服务器，设置业务端口，单击“完成”。
服务器勾选“ECS01”和“ECS02”。
业务端口：业务所使用的端口，示例为“80”。

验证负载均衡服务

负载均衡实例配置完成后，可通过访问 ELB 实例对应的域名，验证是否实现访问到不同的后端云主机。

- 修改本地 PC 的“C:\Windows\System32\drivers\etc\hosts”文件，将域名映射到创建的 ELB 实例的 EIP 上。

ELB 实例的 EIP 请在负载均衡器的基本信息界面查看。

```
# localhost name resolution is handled within DNS itself.
# 127.0.0.1      localhost
# ::1           localhost

11.11.11.14 www.example.com
```

图2-7 本地 PC 的 hosts 文件

- 在本地 PC 的命令行窗口，执行以下命令测试域名映射 ELB 实例的 EIP 是否成功。

ping www.example.com

如有回复数据包，则说明域名映射成功。

- 使用浏览器访问“http://www.example.com”，显示如下页面，说明本次访问请求被 ELB 实例转发到弹性云主机"ECS01"，"ECS01"正常处理请求并返回请求的页面。

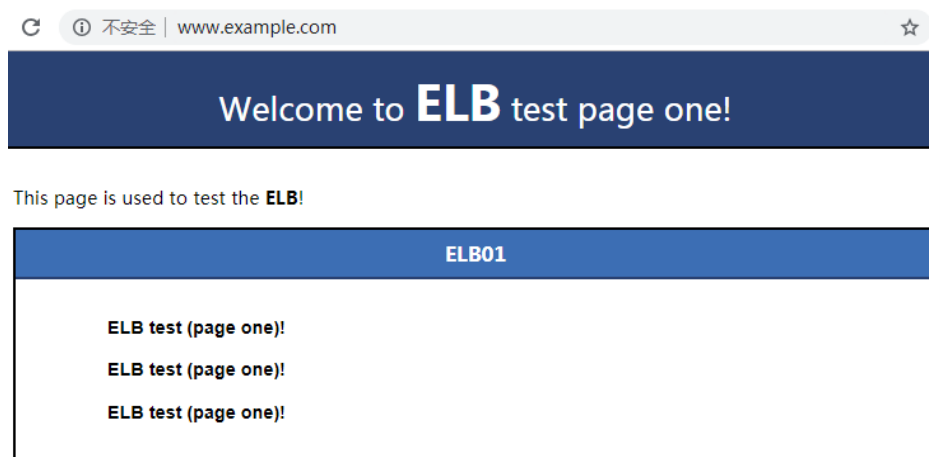


图2-8 访问到 ECS01

- 再次使用浏览器访问“http://www.example.com”，显示如下页面，说明本次访问请求被 ELB 实例转发到弹性云主机"ECS02"，"ECS02"正常处理请求并返回请求的页面。

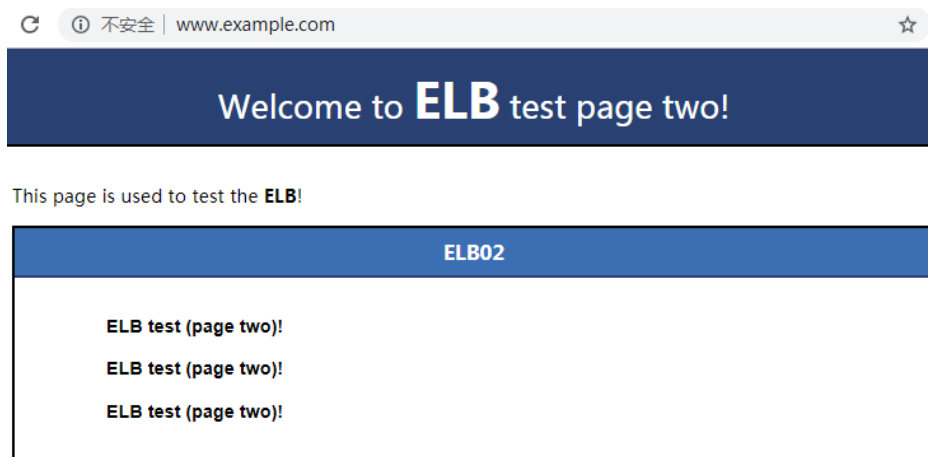


图2-9 访问到 ECS02

3 负载均衡器

3.1 什么是负载均衡器

负载均衡器是指您创建的承载业务的负载均衡服务实体。创建负载均衡器后，您还需要在负载均衡器中添加监听器和后端云主机，然后才能使用负载均衡服务提供的功能。

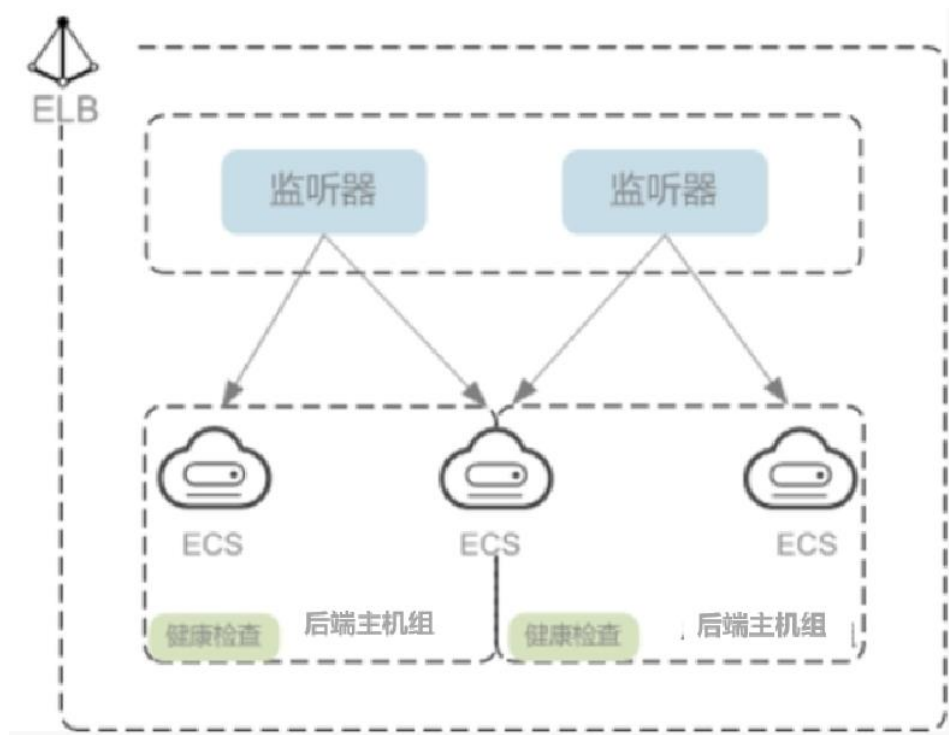


图3-1 负载均衡器结构图

网络类型

按照网络类型分类，负载均衡器分为**公网负载均衡器**和**私网负载均衡器**。

- **公网负载均衡器**：负责处理来自公网访问请求分发的负载均衡实体。

公网负载均衡器接收公网的访问请求，然后向绑定了监听器的后端云主机分发这些请求。创建公网负载均衡器时，需要为负载均衡器创建 EIP 或者绑定已有的 EIP 。

使用场景

需要通过服务器集群对公网提供服务，且需要统一的入口，并将公网用户请求合理地分配到服务器集群时。

需要对服务器集群做故障容错和故障恢复时。

- **私网负载均衡器**：负责处理来自弹性负载均衡同一个 VPC 内访问请求的负载均衡实体。

私网负载均衡器由于没有公网域名和 EIP，所以只能在 VPC 内部被访问，不能被 Internet 的公网用户访问。私网负载均衡通过使用私有 IP 将来自同一个 VPC 内的访问请求分发到后端云主机上，通常用于内部服务集群。

使用场景

私网负载均衡的客户端和服务器端均在云平台内部，通过 VPC 内网访问，主要场景如下：

当内部服务器端有多台，需要将客户端请求合理地分发到各台服务器时；

当需要对内部服务器集群做故障容错和故障恢复时；

当用户想对外屏蔽自己的物理 IP 地址，对客户端提供透明化的服务时：

同时使用公网负载均衡和私网负载均衡：

例如，某业务 Web 服务器和数据库服务器分开部署，Web 服务器需要对公网用户提供访问，后端的数据库服务器只能通过内网进行访问。该场景可以同时使用公网负载均衡器和私网负载均衡器，将 Web 服务器连接至公网负载均衡器，将相应的数据库服务器连接至私网负载均衡器。公网负载均衡器接收来自公网的请求并分发至后端 Web 服务器，处理后将对数据库的请求发送到私网负载均衡，再由私网负载均衡转发请求至数据库服务器。

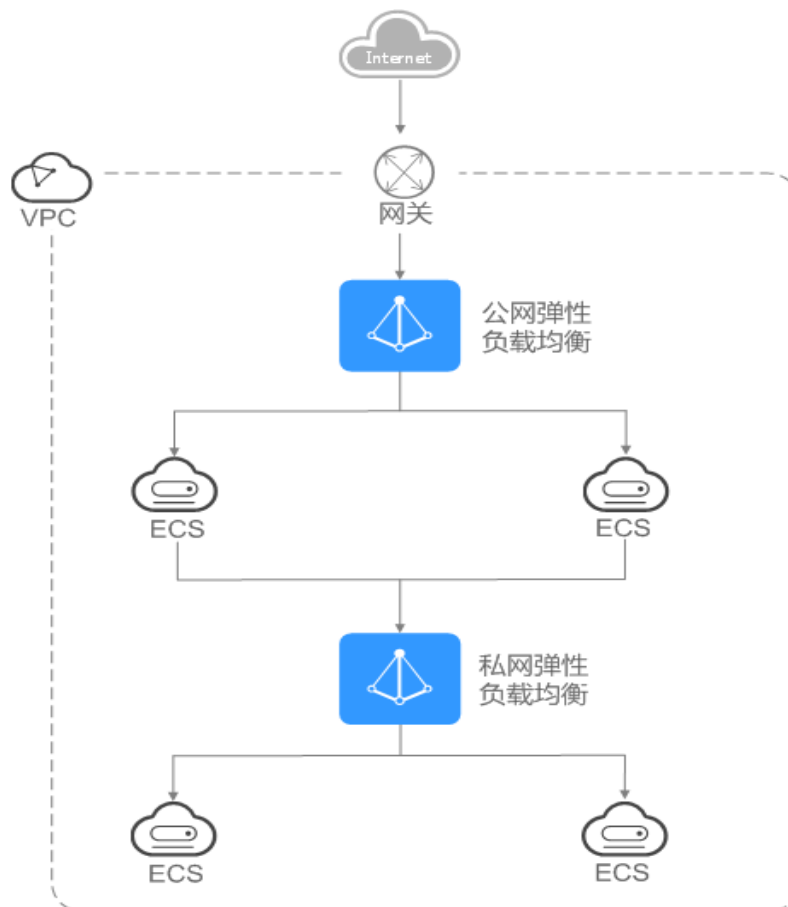


图3-2 同时使用公网负载均衡和私网负载均衡

3.2 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、协议以及后端云主机等。

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。

- 共享型负载均衡不支持跨区域关联后端云主机，因此在创建共享型负载均衡时，需选择与后端云主机相同的区域。
- 独享型负载均衡支持跨区域、跨 VPC 添加后端云主机。

规划实例可用区

独享型负载均衡支持多可用区，选择的每个可用区都会创建相应的负载均衡实例。

这些可用区的负载均衡实例间采用双活或者多活模式，遵循就近原则进行业务流量分摊。例如：分发到可用区 1 后端云主机的流量，是由可用区 1 的负载均衡实例或者靠近可用区 1 的实例进行分发。

选择与后端云主机相同的可用区，可以减少网络时延以及提高访问速度。

如果业务需要考虑容灾能力，建议采取以下两种方式创建负载均衡实例：

- **单实例多可用区（可用区容灾）**
对于业务量没有超过独享型负载均衡最大规格（大型 II）限制的，可以创建一个负载均衡实例，并选择多个可用区，这样单个可用区的负载均衡实例故障不会影响所有业务，多个可用区之间可以实现业务容灾。
- **多实例多可用区（实例容灾+可用区容灾）**
对于超高业务量，超过独享型负载均衡最大规格（大型 II）限制的，可以创建多个负载均衡实例，并且每个负载均衡实例选择多个可用区，这样单个负载均衡实例故障不会影响所有业务，多个负载均衡实例和多个可用区之间均可以实现业务容灾。

📖 说明

- 对于公网访问，会根据源 IP 的不同将流量分配到创建的多个 AZ 中的 ELB 上。
- 对于内网访问：
 - 当从创建 ELB 的 AZ 访问时，流量将被分配到本 AZ 中的 ELB 上，当本 AZ 的 ELB 不可用时，容灾到创建的其他 AZ 的 ELB 上；
 - 当从未创建 ELB 的 AZ 访问时，会根据源 IP 的不同将流量分配到创建的多个 AZ 中的 ELB 上。

选择网络类型

独享型负载均衡网络类型可以选择 IPv4 公网、IPv4 私网和 IPv6。

- 如果选择了 IPv4 公网，负载均衡实例会分配到一个 IPv4 的公网 IP 地址，可以处理来自 Internet 上 IPv4 公网的访问请求。
- 如果选择了 IPv4 私网，负载均衡实例会分配到一个 IPv4 的私网 IP 地址，可以处理来自 VPC 内部 IPv4 私网的访问请求。
- 如果选择了 IPv6，负载均衡实例就会分配到一个 IPv6 的 IP 地址，可以处理来自 VPC 内部 IPv6 私网的访问请求，如果同时购买了公网带宽，则可以同时来自 VPC 内部 IPv6 私网的访问请求和来自 Internet 上 IPv6 公网的访问请求。

共享型实例网络类型可以选择公网或者私网。

- 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。公网负载均衡实例可以同时处理来自 VPC 内网的访问请求。

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。

- 如果只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。

选择实例规格

独享型负载均衡可以独享已购买创建的实例资源，同时分别提供了六种 L4 的实例规格和六种 L7 的实例规格。L4 规格的实例只支持四层协议 TCP/UDP 的转发能力，L7 规格的实例只支持七层协议 HTTP/HTTPS 的转发能力。具体的规格需要评估实际的业务量，根据业务实际需要购买相应规格的实例。业务量的评估可以参考以下几个原则：

- 如果是 L4 规格，建议重点关注长连接的并发连接数，实例规格的“最大连接数”应作为关键参考指标。需要根据实际的业务场景，预估一个负载均衡实例需要承载的最大连接数，并选择相应的规格。
- 如果是 L7 规格，实例规格的“每秒查询数 (QPS)”应作为关键参考指标，该指标决定了一个七层应用系统的业务吞吐量。需要根据实际的业务场景，预估一个负载均衡实例需要承载的 QPS，并选择相应的规格。
- 在使用过程中可以结合负载均衡实例的监控指标，查看实际业务量的峰值、趋势和规律，对实例规格进行更精确的选择。

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云主机。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主机的 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，即三次握手是客户端和后端云主机直接建立的，负载均衡只是进行了数据的转发。

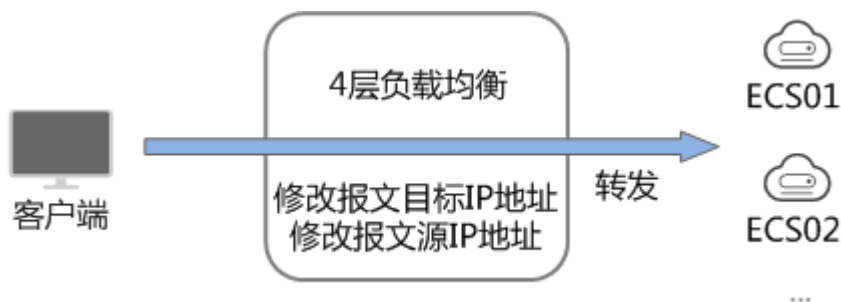


图3-3 四层负载均衡

- 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，先代理后端云主机和客户端建立连接（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云主机。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云主机建立连接。

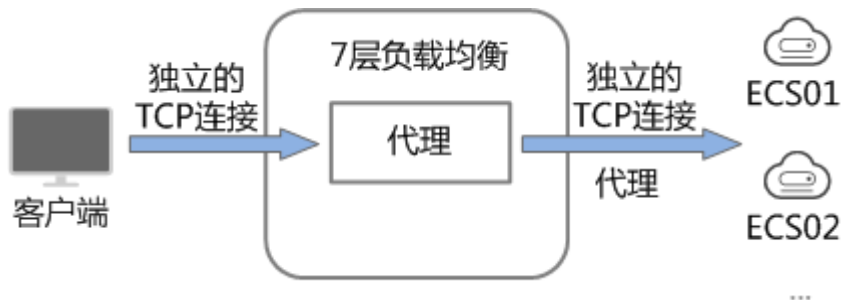


图3-4 七层负载均衡

后端云主机

在使用负载均衡器前，需要先创建 ECS 实例并部署相关业务应用，然后将 ECS 实例添加到负载均衡器的后端主机组来处理转发的客户端访问请求。创建后端云主机时，请注意以下事项：

- 确保后端云主机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云主机实例作为后端云主机，以便后续管理和维护。

3.3 创建独享型负载均衡器

操作场景

在您创建独享型负载均衡器前，确保您已经做好了相关规划，详情参考 3.2 规划和准备。

约束与限制

负载均衡器创建后，不支持修改 VPC。如果要修改 VPC，请重新创建负载均衡器，并选择对应的 VPC。

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“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 3-1 所示。

表3-1 负载均衡器配置参数

参数	说明	取值样例
实例规格类型	选择独享型。	独享型
计费模式	性能独享型负载均衡器的收费类型。 按需计费	按需计费
区域	不同区域的资源之间内网不互通。请选择靠近业务的区域，可以降低网络时延、提高访问速度。	-
可用区	<p>可以选择在多个可用区创建负载均衡实例，提高服务的可用性。如果业务需要考虑容灾能力，建议选择多个可用区。当一个可用区出现故障或不可用时，业务可以快速切换到另一个可用区的负载均衡继续提供服务。</p> <p>此外，选择多个可用区之后，对应的性能规格（新建连接数/并发连接数等）会加倍。例如：单实例最大支持 2kw 并发，那么双 AZ 就支持 4kw 并发。</p> <p>说明</p> <ul style="list-style-type: none"> 对于公网访问，会根据源 IP 的不同将流量分配到创建的多个 AZ 中的 ELB 上。 对于内网访问： <ul style="list-style-type: none"> 当从创建 ELB 的 AZ 访问时，流量将被分配到本 AZ 中的 ELB 上，当本 AZ 的 ELB 不可用时，容灾到创建的其他 AZ 的 ELB 上； 当从未创建 ELB 的 AZ 访问时，会根据源 IP 的不同将流量分配到创建的多个 AZ 中的 ELB 上。 <p>说明</p> <p>针对已有实例，如果修改可用区配置，可能会导致该实例的业务闪断数秒，请在购买时做好规划，确实要修改的话建议选择闲时操作。</p>	-
跨 VPC 后端	<p>开启后，用户可以为负载均衡器添加当前 VPC 以外的后端，跨 VPC 后端通过 IP 地址形式添加。</p> <p>说明</p> <ul style="list-style-type: none"> 若要使用该功能，请先正确配置 VPC 路由，确保后端可达。 开启跨 VPC 后端，需要占用后端子网下的 IP 地址，请确保预留足够的 IP 地址。当您选择子网后可以在子网后面的问号处查看所需 IP 的具体个数。 	-

参数	说明	取值样例
网络类型	<p>可以单独选择一个网络类型，也可以同时选择多个。</p> <p>IPv4 公网：负载均衡器通过 IPv4 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进行处理。</p> <p>IPv4 私网：负载均衡器通过 IPv4 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。</p> <p>IPv6：系统会为实例分配一个 IPv6 地址，转发来自 IPv6 客户端的请求。</p> <p>说明 如果公网或私网 IP 均未选择，则 ELB 实例创建完成后无法与客户端通信。请在使用 ELB 或测试业务连通性时，务必确保该 ELB 绑定了公网或私网 IP。</p>	IPv4 公网
所属 VPC	<p>所属虚拟私有云。无论选择哪种网络类型，均需配置此项。</p> <p>您可以选择使用已有的虚拟私有云网络，或者单击“查看虚拟私有云”创建新的虚拟私有云。</p> <p>更多关于虚拟私有云的信息，请参见《虚拟私有云用户指南》。</p>	vpc-4536
子网	<p>选择创建负载均衡实例的子网。</p> <p>无论选择哪种网络类型，均需配置此项。</p> <p>当网络类型选择“IPv6”，且所选的 VPC 下无支持 IPv6 的子网时，请为已有子网开启 IPv6 或创建支持 IPv6 的子网。详见《虚拟私有云用户指南》。</p>	subnet-4536
IPv4 公网配置		
弹性 IP	<p>当网络类型勾选“IPv4 公网”时，需要指定弹性 IP。弹性 IP 可以使用已有的 IP 地址，也可以新建。弹性 IP 选择使用已有时，需要选择已有的弹性 IP 地址。</p> <p>新建：系统为弹性负载均衡实例新建一个弹性 IP。</p> <p>使用已有：为弹性负载均衡实例选择一个已有的弹性 IP 地址。</p>	-

参数	说明	取值样例
公网带宽	<p>弹性 IP 使用的带宽类型。</p> <p>可选“按带宽计费”或“按流量计费”或“加入共享带宽”。</p> <p>按带宽计费：指定带宽上限，按使用时间计费，与使用的流量无关。</p> <p>按流量计费：指定带宽上限，按实际使用的上行流量计费，与使用时间无关。</p> <p>加入共享带宽</p>	加入共享带宽
带宽	指定具体的带宽上限	100Mbps
IPv4 私网配置		
IPv4 地址	<p>选择 IPv4 地址的分配方式。</p> <p>自动分配 IP 地址：由系统自动分配 IPv4 地址。</p> <p>手动指定 IP 地址：手动指定 IPv4 地址。</p> <p>说明：负载均衡器的 IP 地址不受所在 VPC 子网 ACL 配置的限制，所以能够被客户端直接访问。建议您使用监听器的访问控制功能限制客户端访问负载均衡器。</p>	自动分配 IP 地址
IPv6 网络配置		
IPv6 地址	<p>选择 IPv6 的 IP 地址的分配方式。</p> <p>说明</p> <p>负载均衡器的 IP 地址不受所在 VPC 子网 ACL 配置的限制，所以能够被客户端直接访问。建议您使用监听器的访问控制功能限制客户端访问负载均衡器。</p> <p>详细请参考 4.5 访问控制策略。</p>	自动分配 IP 地址

参数	说明	取值样例
规格	<p>“应用型（HTTP/HTTPS）”和“网络型（TCP/UDP）”请至少勾选一种，勾选后可选择相应能力的规格。</p> <p>应用型（HTTP/HTTPS）的不同规格所需的子网的IP地址不同，您可以在子网后面的问号处查看所需IP的具体个数。</p> <p>不同的实例规格在性能上存在差异。可以从最大连接数，新建连接数（CPS）、每秒查询数（QPS）、带宽等维度对实际业务进行评估，然后选择适合的规格。</p> <p>独享型实例的规格分为四层能力和七层能力，分别支持以下六种规格。</p> <p>小型 I</p> <p>小型 II</p> <p>中型 I</p> <p>中型 II</p> <p>大型 I</p> <p>大型 II</p>	中型 II
名称	负载均衡器的名称。	elb93wd
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
高级配置		
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。命名规格请参照表 3-2。	键：elb_key1 值：elb-01

表3-2 负载均衡器标签命名规则

参数	规则	样例
键	<p>不能为空。</p> <p>对于同一负载均衡器键值唯一。</p> <p>长度不超过 36 个字符。</p> <p>仅允许使用英文字母、数字、下划线、中划线、“@”字符。</p>	elb_key1

参数	规则	样例
值	长度不超过 43 个字符。 仅允许使用英文字母、数字、下划线、中划线、“@” 字符。	elb-01

- 单击“立即申请”。
- 确认配置信息，单击“提交”。

3.4 创建共享型负载均衡器

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 3.2 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云主机，后端云主机再将响应通过内网返回给负载均衡。

约束与限制

负载均衡器创建后，不支持修改 VPC。如果要修改 VPC，请重新创建负载均衡器，并选择对应的 VPC。

创建共享型负载均衡器


- 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“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 3-3 所示。

表3-3 共享型负载均衡器配置参数

参数	说明	取值样例
实例规格类型	负载均衡的实例类型。	共享型
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。	-

参数	说明	取值样例
网络类型	<p>可选公网或者私网。</p> <p>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云主机进行处理。</p> <p>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云主机进行处理。</p>	私网
所属 VPC	<p>所属虚拟私有云。</p> <p>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。</p> <p>更多关于虚拟私有云的信息，请参见《虚拟私有云用户指南》。</p>	-
子网	所属子网。	-
私有 IP 地址	<p>选择 IP 地址的分配方式。</p> <p>自动分配 IP 地址：由系统自动分配 IPv4 地址。</p> <p>手动指定 IP 地址：手动指定 IPv4 地址。</p> <p>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。</p>	192.168.0.2
弹性 IP	<p>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云主机。</p> <p>您可以选择使用已有的 EIP，或者创建新的 EIP。</p> <p>您可以根据实际情况选择以下方式：</p> <p>新创建：新创建一个 EIP。</p> <p>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。</p>	新创建
弹性 IP 类型	<p>使用新创建弹性 IP 时，选择的 EIP 的类型。</p> <p>电信</p>	电信
公网带宽	<p>弹性 IP 使用的带宽类型。</p> <p>可选“按带宽计费”或“按流量计费”。按带宽计费：指定带宽上限，按使用时间计费，与使用的流量无关。按流量计费：指定带宽上限，按实际使用的上行流量计费，与使用时间无关。</p>	按带宽计费
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-yss0

参数	说明	取值样例
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。 命名规格请参照表 3-4。	键： elb_key 1 值：elb-01

表3-4 负载均衡器标签命名规则

参数	规则	样例
键	不能为空。 对于同一负载均衡器键值唯一。 长度不超过 36 个字符。 仅允许使用英文字母、数字、下划线、中划线、@ 字符、中文字符。	elb_key1
值	长度不超过 43 个字符。 英文字母、数字、下划线、中划线、@ 字符、中文字符。。	elb-01


5. 单击“立即申请”。
6. 确认配置信息，并单击“提交”。

3.5 变更公网带宽

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 ELB 实例关联的弹性公网 IP 的带宽。

修改公网带宽

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：
 - 独享型负载均衡：在“弹性负载均衡”页签，待修改带宽的负载均衡器所在行，单击“修改 IPv4 带宽”或“修改 IPv6 带宽”。

共享型负载均衡：在“弹性负载均衡”页签，待修改带宽的负载均衡器所在行，单击“修改带宽”或“修改 IPv4 带宽”。

5. 在“变更规格”区域，设置新的带宽大小，单击“下一步”。可以选择系统定义好的带宽也可以自定义带宽的大小。自定义修改带宽的范围为 1-2000Mbit/s。

说明

您还可以在此处修改带宽名称。

6. 确认修改后的带宽大小，单击“提交”。


3.6 修改 IP 地址

操作场景

弹性负载均衡支持修改 IPv4 私有 IP，可以将负载均衡当前使用 IPv4 私有 IP 修改为当前子网或者其它子网的目标 IP 地址。

当前仅独享型负载均衡支持此功能。

修改 IPv4 私有 IP


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”页面，需修改负载均衡器所在行，单击“更多 > 修改 IPv4 私有 IP”。
5. 在“修改 IPv4 私有 IP”对话框中，选择需要修改的目标 IP 所在子网，并设置目标 IP 地址。

不同子网下修改 IPv4 地址，可以勾选“自动分配 IPv4 地址”，勾选后，系统会自动分配一个所选择子网的 IPv4 地址。

同一子网下修改 IPv4 地址，必须指定 IP，不支持自动分配。

6. 单击“确定”。

修改 IPv6 地址

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”页面，需修改负载均衡器所在行，单击“更多 > 修改 IPv6 地址”。
5. 在“修改 IPv6 地址”对话框中，选择需要修改的目标 IP 所在子网。当前 IPv6 地址只支持自动分配，所以修改 IPv6 地址，必须更换子网。

3.7 为实例绑定/解绑 EIP

操作场景

可以根据业务需要为负载均衡实例绑定 IP 地址，或者将负载均衡实例已经绑定的 IP 地址进行解绑。


经典型负载均衡不支持此功能。

- 独享型：支持绑定和解绑 IPv4 公网 IP、IPv4 私有 IP、IPv6 地址。
- 共享型：支持绑定和解绑 IPv4 公网 IP。

说明


- 解绑 IPv4 公网 IP 后，对应的弹性负载均衡器将无法进行 IPv4 公网流量转发；
- 解绑 IPv4 私有 IP 后，对应的弹性负载均衡器将无法基于 IPv4 私有 IP 进行私网流量转发；
- 解绑 IPv6 地址后，对应的弹性负载均衡器将无法基于 IPv6 地址进行流量转发，请谨慎操作。

绑定 IPv4 公网 IP

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，待修改的负载均衡器所在行，选择“更多 > 绑定 IPv4 公网 IP”。
5. 在“绑定 IPv4 公网 IP”对话框中，选择需要绑定的公网 IP。
6. 单击“确定”。

绑定 IPv4 私有 IP

当前仅独享型负载均衡支持此功能。

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，待修改的负载均衡器所在行，选择“更多 > 绑定 IPv4 私有 IP”。
5. 在“绑定 IPv4 私有 IP”对话框中，选择待绑定的 IPv4 地址所在子网，并设置目标 IP 地址。


系统默认自动分配 IP 地址，如果需要手动指定 IP 地址，请去勾选“自动分配 IPv4 地址”，并在参数“IPv4 地址”行输入目标 IP 地址。

输入的 IP 地址必须属于所选择的子网且未被使用。


6. 单击“确定”。

绑定 IPv6 地址

当前仅独享型负载均衡支持此功能。

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，待修改的负载均衡器所在行，选择“更多 > 绑定 IPv6 地址”。
5. 在“绑定 IPv6 地址”对话框中，选择待绑定的 IPv6 地址所在子网。
6. 单击“确定”。

解绑 IPv4 公网 IP


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，待设置的负载均衡器所在行，选择“更多 > 解绑 IPv4 公网 IP”。
5. 在“解绑 IPv4 公网 IP”对话框中，确认需要释放的 IPv4 公网 IP 地址，单击“是”。

说明

解绑 IPv4 公网 IP 后，对应弹性负载均衡器将无法进行 IPv4 公网流量转发，请谨慎操作。

解绑 IPv4 私有 IP

当前仅独享型负载均衡支持此功能。

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，待设置的负载均衡器所在行，选择“更多 > 解绑 IPv4 私有 IP”。
5. 在“解绑 IPv4 私有 IP”对话框中，确认需要释放的 IPv4 私有 IP 地址，单击“是”。

说明

解绑 IPv4 私有 IP 后，对应的弹性负载均衡器将无法基于 IPv4 私有 IP 进行私网流量转发，请谨慎操作。


3.8 启用和停用负载均衡器

操作场景

您可以随时启用和停用负载均衡器。停用负载均衡后，该负载均衡将无法进行流量转发。

目前只有经典型负载均衡支持此功能。

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，需要启用或者停用的负载均衡器所在行，单击“更多 > 启用”或者“更多 > 停用”。
5. 单击“是”。

3.9 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。

注意

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

请先按以下顺序删除该负载均衡器配置的资源：

1. **转发策略：**如果监听器配置了转发策略，请删除所有转发策略。
2. **重定向：**如果配置了 HTTP 监听器重定向至 HTTPS 监听器，请删除所有重定向。
3. **后端云主机：**如果监听器对应的后端主机组添加了后端云主机，请删除所有后端云主机。
4. **监听器：**请删除 ELB 下的所有监听器。
5. **后端主机组：**请删除监听器对应的所有后端主机组。

删除负载均衡器

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，在目标负载均衡器所在行的操作列单击“删除”。



5. 单击“是”。

3.10 导出负载均衡器列表

操作场景

您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。

导出弹性负载均衡器列表

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。

4 监听器

4.1 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，分发流量到后端云主机处理。

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 4-1。

对于支持**四层能力**的负载均衡器，在创建监听器时，支持选择 **TCP** 或者 **UDP**。

对于支持**七层能力**的负载均衡器，在创建监听器时，支持选择 **HTTP** 或者 **HTTPS**。

表4-1 监听协议类型说明

协议类型		说明	适用场景
四层协议	TCP	基于源地址的会话保持。 数据传输快。	适用于注重可靠性，对数据准确性要求高的场景，如文件传输、发送或接收邮件、远程登录。 对性能和并发规模有要求的 Web 应用。
四层协议	UDP	可靠性相对较低 数据传输快	适用于关注实时性而相对不注重可靠性的场景，如视频聊天、游戏、金融实时行情推送。
七层协议	HTTP	基于 Cookie 的会话保持。 使用 X-Forward-For 获取源地址。	需要对数据内容进行识别的应用，如 Web 应用、移动游戏等。

协议类型		说明	适用场景
七层协议	HTTPS	加密传输数据，可以阻止未经授权的访问。 加解密操作在负载均衡器上完成，可减少后端的处理负载。 多种加密协议和加密套件可选。	需要加密传输的应用。

4.2 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。

📖 说明

前端协议和端口设置后不允许修改，如果要修改，请重新创建监听器。

表4-2 前端协议和端口说明

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。
UDP	
HTTP	
HTTPS	

常用取值示例：
TCP/80
HTTPS/443

后端协议和端口

后端协议和端口即是后端云主机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4-3 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	
HTTPS	

4.3 流量分配策略

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云主机中进行处理。请求的流量分发与负载均衡器所绑定的后端主机组配置的分配策略类型相关。

分配策略类型

独享型负载均衡支持加权轮询算法、加权最少连接、源 IP 算法，共享型负载均衡支持加权轮询算法、加权最少连接、源 IP 算法。

- 加权轮询算法：**根据后端云主机的权重，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，权重大的后端云主机被分配的概率高。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。

图 4-1 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 2 台权重相同的后端云主机，负载均衡器节点会将 50% 的客户端流量分发到其可用区中的每一台后端云主机。

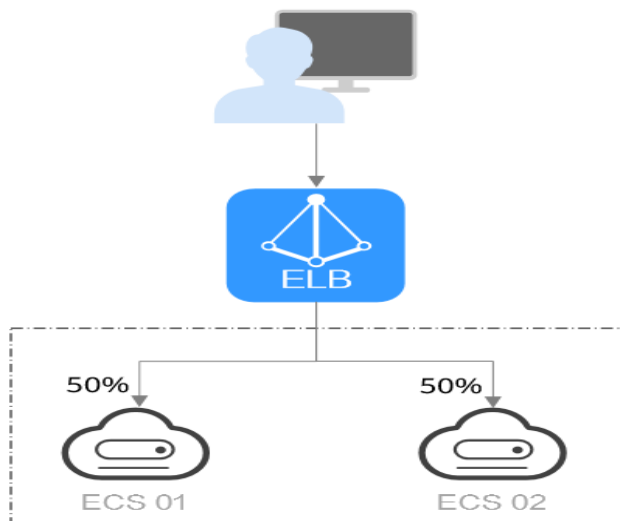


图4-1 加权轮询算法流量分发

- 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。

图 4-2 展示弹性负载均衡器使用加权最少连接算法的流量分发流程。假设可用区内有 2 台权重相同的后端云主机，ECS 01 已有 100 个连接，ECS 02 已有 50 个连接，则新的连接会优先分配到 ECS 02 上。

图4-2 加权最少连接算法流量分发

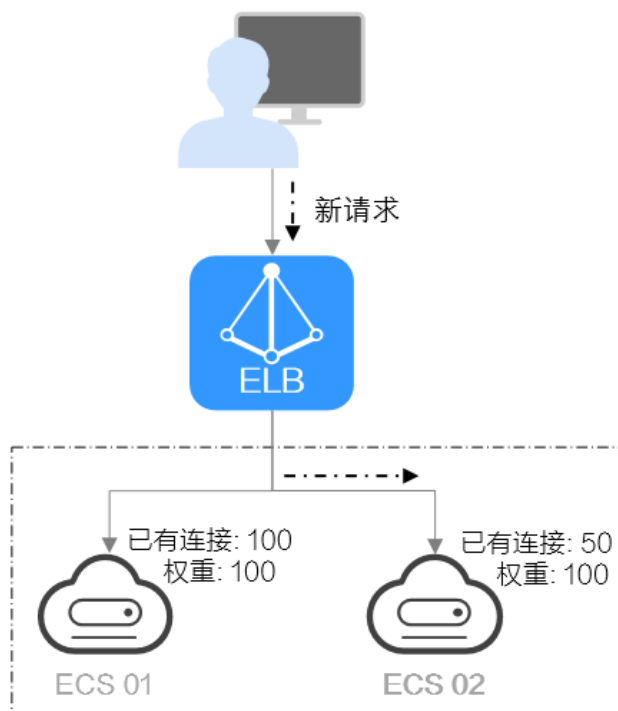


图4-3 加权最少连接算法流量分发

- 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，同时对后端云主机进行编号，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。

图 4-4 展示弹性负载均衡器使用源 IP 算法的流量分发流程。假设可用区内有 2 台权重相同的后端云主机，ECS 01 已经处理了一个 IP-A 的请求，则 IP-A 新发起的请求会自动分配到 ECS 01 上。

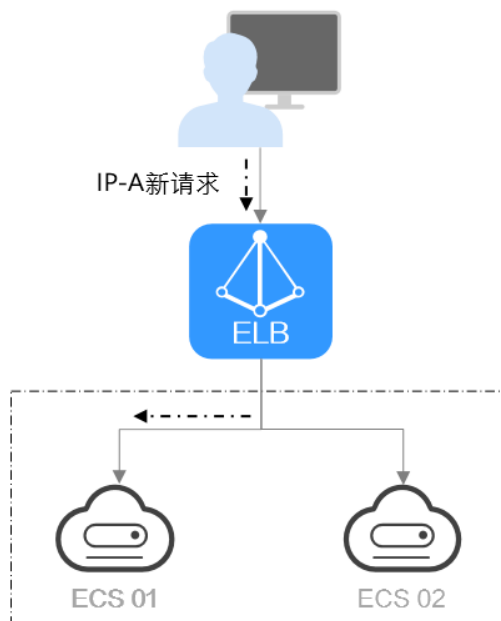




图4-4 源 IP 算法流量分发

修改分配策略

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，单击需要修改分配策略的负载均衡名称。
5. 在该负载均衡器界面，切换到“后端主机组”页签，单击后端主机组所在行的 。
6. 选择“分配策略类型”。

说明

修改分配策略立即生效，不影响已经建立连接的流量转发，只影响新建连接的流量分配。

7. 单击“确定”。

4.4 会话保持

会话保持，指负载均衡器可以识别客户与服务器之间交互过程的关联性，在实现负载均衡的同时，保持将其他相关联的访问请求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，所以需要重新登录。如果配置了会话保持功能，上述一系列的操作

过程将由同一台服务器完成，避免被负载均衡器分配到不同的服务器上，所以也无需重复登录。

按照所使用的协议的不同，会话保持可以分为**四层会话保持**和**七层会话保持**。

前提条件

只有当分配策略类型选择“加权轮询算法”或“加权最少连接”时，才可配置会话保持。

约束与限制

如果您需要从**云专线**、**VPN**、**云连接**访问 ELB，请您使用源 IP 负载均衡算法代替会话保持功能。

四层会话保持和七层会话保持的区别

表4-4 四层会话保持和七层会话保持的区别



类型	说明	支持的会话保持类型	会话保持时间	会话保持失效的场景
四层会话保持	当使用的协议为 TCP 或 UDP 时，即为四层会话保持。	源 IP 地址： 基于源 IP 地址的简单会话保持，将请求的源 IP 地址作为散列键 (HashKey)，从静态分配的散列表中找出对应的服务器。即来自同一 IP 地址的访问请求会被转发到同一台后端云主机上进行处理。	默认时间：20 分钟； 最长时间：1 小时 取值范围：1-60 分钟	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。

类型	说明	支持的会话保持类型	会话保持时间	会话保持失效的场景
七层会话保持	当使用的协议为 HTTP 或 HTTPS 时，即为七层会话保持。	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云主机处理。 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云主机处理。	默认时间：20 分钟； 最长时间：24 小时 取值范围：1-1440 分钟	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。

独享型负载均衡器支持源 IP 地址、负载均衡器 cookie 两种会话保持类型。

共享型负载均衡器支持源 IP 地址、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. 共享型和独享型负载均衡，在该负载均衡界面的“后端主机组”页签，单击需要配置会话保持的后端主机组名称右侧的 。
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”。

说明

您还可以在进行“添加监听器”或“添加后端主机组”操作时，配置会话保持。

4.5 访问控制策略

共享型和独享型负载均衡器用户可以通过添加白名单和黑名单的方式控制访问负载均衡监听器的 IP。通过白名单能够设置允许特定 IP 访问，而其它 IP 不许访问。通过黑名单能够设置允许特定的 IP 不能访问，而其它 IP 允许访问。

须知

- 设置白名单和黑名单是共享型和独享型负载均衡的功能，设置白名单和黑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器；一旦设置黑名单，黑名单中的 IP 不能访问负载均衡监听器。
- 访问流量的 IP 先通过白名单或黑名单访问控制，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或黑名单设置访问控制。
- 访问控制只限制实际业务的流量转发，不限制 ping 命令操作，被限制的 IP 仍可以 ping 通后端云主机。
- 配置了白名单，但是不在白名单的 IP 也能访问后端云主机，可能的原因是该连接为长连接。需要客户端或后端云主机断开该长连接。访问控制策略对新建的连接是实时生效的。

设置访问控制策略


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，单击负载均衡名称，进入监听器管理界面。
5. 在需要添加访问控制策略的监听器基本信息页面，单击访问控制右侧“设置访问控制”按钮，如表 4-5 所示配置访问控制策略。

表4-5 访问控制参数说明

参数	说明	样例
访问策略	<p>可以选择允许所有 IP 访问、白名单和黑名单。</p> <p>允许所有 IP 访问：不进行访问控制，允许所有 IP 访问负载均衡监听器。</p> <p>白名单：仅允许 IP 地址组中的 IP 访问负载均衡监听器。</p> <p>黑名单：不允许 IP 地址组中的 IP 访问负载均衡监听器。</p>	黑名单
IP 地址组	<p>设置白名单或者黑名单时，必须选择一个 IP 地址组。如果还未创建 IP 地址组，需要先创建 IP 地址组，更多关于 IP 地址组的信息请参见 9.1 错误!表格结果无效。。</p>	ipGroup-b2

参数	说明	样例
访问控制开关	<p>当访问策略选择白名单或者黑名单时，可以开启或者关闭访问控制开关。</p> <p>开启：开启访问控制开关，设置的白名单和黑名单才会生效。</p> <p>关闭：关闭访问控制开关，设置的白名单和黑名单不生效。</p>	-

6. 配置完成，点击“确定”。

4.6 添加 TCP 监听器

操作场景

TCP 协议适用于注重可靠性，对数据准确性要求高，速度可以相对较慢的场景，如文件传输、发送或接收邮件、远程登录等。您可以添加一个 TCP 监听器转发来自 TCP 协议请求。

注意

- 前端协议为“TCP”时，后端协议默认为“TCP”，且不支持修改。
- 如果您的独享型负载均衡实例类型为应用型（HTTP/HTTPS），则无法创建 TCP 监听器。

添加独享型负载均衡 TCP 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”，配置监听器。配置监听器参数参见表 4-6。

表4-6 独享型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	<p>客户端与负载均衡监听器建立流量分发连接的协议。</p> <p>协议选择 TCP，端口取值范围[1-65535]。</p>	TCP/80
高级配置		

参数	说明	示例
访问策略	支持通过白名单和黑名单进行访问控制，更多信息请参见 4.5 访问控制策略： 允许所有 IP 访问 黑名单 白名单	黑名单
IP 地址组	设置白名单或者黑名单时，必须选择一个 IP 地址组。如果还未创建 IP 地址组，需要先创建 IP 地址组，更多关于 IP 地址组的信息请参见 9.1 错误!表格结果无效。 。	ipGroup-b2
空闲超时时间	如果在超时时间内一直没有访问请求，负载均衡会中断当前连接，直到下一次请求到来时再重新建立新的连接。 取值范围：10~4000s	300
描述	对于监听器描述。 字数范围：0/255。	-

6. 单击“下一步”，配置后端主机组及配置健康检查。配置后端主机组参数请参见表 4-7。

表4-7 独享型负载均衡配置后端主机组参数说明

参数	说明	示例
后端主机组	把具有相同特性的后端云主机放在一个组。 新创建 使用已有 说明 使用已有后端主机组时，请确保此后端主机组未被使用。并且只能选择前端协议匹配的后端主机组。例如前端协议是 TCP 时，后端协议只能是 TCP。	新创建
名称	后端主机组名称。	server_group-sq4v
后端协议	云主机开通的协议。 前端协议为 TCP 时，后端协议默认为 TCP，不支持修改。	TCP

参数	说明	示例
分配策略类型	<p>负载均衡采用的算法。</p> <p>加权轮询算法：根据后端云主机的权重，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。</p> <p>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。</p> <p>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，同时对后端云主机进行编号，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。</p> <p>说明</p> <ul style="list-style-type: none"> • 用户可以根据自身需求选择相应的算法来分配用户访问量，提升负载均衡能力。 • 对于加权轮询算法和加权最少连接，当服务器的权重为“0”时，将不会被分发访问请求。 	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>说明</p> <p>当分配策略类型为“加权轮询算法”或“加权最少连接”时，可配置会话保持。</p>	-
会话保持类型	<p>TCP 和 UDP 协议仅支持源 IP 地址类型。</p> <p>源 IP 地址：基于源 IP 地址的简单会话保持，将请求的源 IP 地址作为散列键（HashKey），从静态分配的散列表中找出对应的服务器。即来自同一 IP 地址的访问请求会被转发到同一台后端云主机上进行处理。</p>	源 IP 地址
会话保持时间（分钟）	<p>当分配策略类型选择“加权轮询算法”或“加权最少连接”，会话保持开启后，需添加会话保持时间。</p> <p>四层会话保持的会话保持时间取值范围为[1, 60]。</p> <p>七层会话保持的会话保持时间取值范围为[1, 1440]。</p>	20
描述	<p>后端主机组的描述。</p> <p>字数范围：0/255。</p>	-

7. 单击“下一步：添加后端云主机”。添加后端云主机并配置健康检查。添加后端服务器详见添加或移除后端云主机（独享型）。

配置健康检查参数请参见表 4-8。

表4-8 独享型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	健康检查支持 TCP、HTTP、HTTPS 协议，设置后不可修改。	HTTP
端口	健康检查端口号，取值范围[1, 65535]，为可选参数。 说明：未配置健康检查端口时，默认使用后端云主机端口进行健康检查。配置后，使用配置的健康检查端口进行健康检查。	80
健康检查配置		
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]。	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]。 说明 例如： 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”。	/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
HTTP 状态码	自定义健康检查返回的状态码。当“协议”为 HTTP 或 HTTPS 时生效。 可输入 200-599 范围内不重复的单个数字或正序的数字区间。多个 HTTP 状态码使用逗号隔开，最多支持 5 个。 说明 如果您要使用该特性，请进入至 ELB 服务控制台后，单击页面左下角的“体验新版”。目前新版控制台在公测中，待公测结束后即可正常使用。	200

8. 单击“下一步”确认配置。
9. 确认配置无误后，单击“提交”。

添加共享型负载均衡 TCP 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”，配置监听器。配置监听器参数参见表 4-9。

表4-9 共享型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	客户端与负载均衡监听器建立流量分发连接的协议。 协议选择 TCP，端口取值范围[1-65535]。	TCP/80
高级配置		
访问策略	支持通过白名单和黑名单进行访问控制，更多信息请参见 4.5 访问控制策略： 允许所有 IP 访问 黑名单 白名单	白名单
IP 地址组	设置白名单或者黑名单时，必须选择一个 IP 地址组。如果还未创建 IP 地址组，需要先创建 IP 地址组，更多关于 IP 地址组的信息请参见 9.1 错误!表格结果无效。 。	ipGroup-b2
空闲超时时间（秒）	如果在超时时间内一直没有访问请求，负载均衡会中断当前连接，直到下一次请求到来时再重新建立新的连接。 取值范围：10~4000s	300
描述	对于监听器描述。 字数范围：0/255。	-

6. 单击“下一步”，配置后端主机组及配置健康检查。配置后端主机组参数请参见表 4-10。

表4-10 共享型负载均衡配置后端主机组参数说明

参数	说明	示例
后端主机组	<p>把具有相同特性的后端云主机放在一个组。</p> <p>新创建</p> <p>使用已有</p> <p>说明</p> <p>使用已有后端主机组时，请确保此后端主机组未被使用。并且只能选择前端协议匹配的后端主机组。例如前端协议是 TCP 时，后端协议只能是 TCP。</p>	新创建
名称	后端主机组名称。	server_group-sq4v
后端协议	<p>云主机开通的协议。</p> <p>前端协议为 TCP 时，后端协议默认为 TCP，不支持修改。</p>	TCP
分配策略类型	<p>负载均衡采用的算法。</p> <p>加权轮询算法：根据后端云主机的权重，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。</p> <p>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。</p> <p>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，同时对后端云主机进行编号，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。</p> <p>说明</p> <ul style="list-style-type: none"> • 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。 • 对于加权轮询算法和加权最少连接，当服务器的权重为“0”时，将不会被分发访问请求。 	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>说明</p> <p>当分配策略类型为“加权轮询算法”时，可配置会话保持。</p>	-

参数	说明	示例
会话保持类型	TCP 和 UDP 协议仅支持源 IP 地址类型。 源 IP 地址： 基于源 IP 地址的简单会话保持，将请求的源 IP 地址作为散列键（HashKey），从静态分配的散列表中找出对应的服务器。即来自同一 IP 地址的访问请求会被转发到同一台后端云主机上进行处理。	源 IP 地址
会话保持时间（分钟）	当分配策略类型选择“加权轮询算法”或“加权最少连接”，会话保持开启后，需添加会话保持时间。 四层会话保持的会话保持时间取值范围为[1, 60]。 七层会话保持的会话保持时间取值范围为[1, 1440]。	20
描述	后端主机组的描述。 字数范围：0/255。	-

7. 单击“下一步：配置后端分配策略”。配置健康检查参数请参见表 4-11。

表4-11 共享型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	健康检查支持 TCP、HTTP 协议，设置后不可修改。	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。 说明：未配置健康检查端口时，默认使用后端云主机端口进行健康检查。配置后，使用配置的健康检查端口进行健康检查。	80
配置		
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]。	3

参数	说明	示例
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]。 说明 例如： 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”。	/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“完成”。

4.7 添加 UDP 监听器

操作场景

UDP 协议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。您可以添加一个 UDP 监听器转发来自 UDP 协议的请求。

注意

- 独享型负载均衡前端协议为“UDP”时，后端协议可以选择“UDP”或“QUIC”。
- 共享型负载均衡前端协议为“UDP”时，后端协议默认为“UDP”，且不支持修改。
- 如果您的独享型负载均衡实例类型为应用型（HTTP/HTTPS），则无法创建 UDP 监听器。

添加独享型负载均衡 UDP 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”，配置监听器。配置监听器参数参见表 4-12。

表4-12 独享型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。 协议选择 UDP，端口取值范围[1-65535]。	UDP/80
高级配置		
访问策略	支持通过白名单和黑名单进行访问控制，更多信息请参见 4.5 访问控制策略： 允许所有 IP 访问 黑名单 白名单	黑名单
IP 地址组	设置白名单或者黑名单时，必须选择一个 IP 地址组。如果还未创建 IP 地址组，需要先创建 IP 地址组，更多关于 IP 地址组的信息请参见 9.1 错误!表格结果无效。 。	ipGroup-b2
空闲超时时间	如果在超时时间内一直没有访问请求，负载均衡会中断当前连接，直到下一次请求到来时再重新建立新的连接。 取值范围：10~4000s	300
描述	对于监听器描述。 字数范围：0/255。	-

6. 单击“下一步”，配置后端主机组及配置健康检查。配置后端主机组参数请参见表 4-13。

表4-13 独享型负载均衡配置后端主机组参数说明

参数	说明	示例
后端主机组	把具有相同特性的后端云主机放在一个组。 新创建 使用已有 说明 使用已有后端主机组时，请确保此后端主机组未被使用。 并且只能选择前端协议匹配的后端主机组。例如前端协议是 TCP 时，后端协议只能是 TCP。	新创建
名称	后端主机组名称。	server_group-sq4v

参数	说明	示例
后端协议	云主机开通的协议。 前端协议为 UDP 时，后端协议默认为 UDP ，不支持修改。	UDP
分配策略类型	负载均衡采用的算法。 加权轮询算法 ：根据后端云主机的权重，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。 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。 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，同时对后端云主机进行编号，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。 说明 <ul style="list-style-type: none"> • 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。 • 对于加权轮询算法和加权最少连接，当服务器的权重为“0”时，将不会被分发访问请求。 	加权轮询算法
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服务器进行处理。 说明 当分配策略类型为“加权轮询算法”或“加权最少连接”时，可配置会话保持。	-
会话保持类型	TCP 和 UDP 协议仅支持源 IP 地址类型。 源 IP 地址 ：基于源 IP 地址的简单会话保持，将请求的源 IP 地址作为散列键（HashKey），从静态分配的散列表中找出对应的服务器。即来自同一 IP 地址的访问请求会被转发到同一台后端云主机上进行处理。	源 IP 地址

参数	说明	示例
会话保持时间（分钟）	当分配策略类型选择“加权轮询算法”或“加权最少连接”，会话保持开启后，需添加会话保持时间。 四层会话保持的会话保持时间取值范围为[1, 60]。 七层会话保持的会话保持时间取值范围为[1, 1440]。	20
描述	后端主机组的描述。 字数范围：0/255。	-

7. 配置健康检查参数请参见表 4-14。

表4-14 独享型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	健康检查仅支持 UDP 协议，且不支持修改。	UDP
高级配置		
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]。	3
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“完成”。

添加共享型负载均衡 UDP 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”，配置监听器。配置监听器参数参见表 4-15。

表4-15 共享型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

参数	说明	示例
前端协议/端口	负载分发的协议和端口。 协议选择 UDP，端口取值范围[1-65535]。	UDP/80
高级配置		
访问策略	支持通过白名单和黑名单进行访问控制，更多信息请参见 4.5 访问控制策略： 允许所有 IP 访问 黑名单 白名单	白名单
IP 地址组	设置白名单或者黑名单时，必须选择一个 IP 地址组。如果还未创建 IP 地址组，需要先创建 IP 地址组，更多关于 IP 地址组的信息请参见 9.1 错误!表格结果无效。 。	ipGroup-b2
描述	对于监听器描述。 字数范围：0/255。	-
标签	可通过配置该项使用标签功能。标签的“键”和“值”是一一对应的，其中“键”值是唯一的。	-

6. 单击“下一步”，配置后端主机组及配置健康检查。配置后端主机组参数请参见表 4-16。

表4-16 共享型负载均衡配置后端主机组参数说明

参数	说明	示例
后端主机组	把具有相同特性的后端云主机放在一个组。 新创建 使用已有 说明 使用已有后端主机组时，请确保此后端主机组未被使用。并且只能选择前端协议匹配的后端主机组。例如前端协议是 TCP 时，后端协议只能是 TCP。	新创建
名称	后端主机组名称。	server_group-sq4v
后端协议	云主机开通的协议。 前端协议为 UDP 时，后端协议默认为 UDP，不支持修改。	UDP

参数	说明	示例
分配策略类型	<p>负载均衡采用的算法。</p> <p>加权轮询算法：根据后端云主机的权重，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。</p> <p>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。</p> <p>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，同时对后端云主机进行编号，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。</p> <p>说明</p> <ul style="list-style-type: none"> • 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。 • 对于加权轮询算法和加权最少连接，当服务器的权重为“0”时，将不会被分发访问请求。 	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>说明</p> <p>当分配策略类型为“加权轮询算法”时，可配置会话保持。</p>	-
会话保持类型	<p>TCP 和 UDP 协议仅支持源 IP 地址类型。</p> <p>源 IP 地址：基于源 IP 地址的简单会话保持，将请求的源 IP 地址作为散列键（HashKey），从静态分配的散列表中找出对应的服务器。即来自同一 IP 地址的访问请求会被转发到同一台后端云主机上进行处理。</p>	源 IP 地址
会话保持时间（分钟）	<p>当分配策略类型选择“加权轮询算法”或“加权最少连接”，会话保持开启后，需添加会话保持时间。</p> <p>四层会话保持的会话保持时间取值范围为[1, 60]。</p> <p>七层会话保持的会话保持时间取值范围为[1, 1440]。</p>	20

参数	说明	示例
描述	后端主机组的描述。 字数范围：0/255。	-

7. 配置健康检查参数请参见表 4-17。

表4-17 共享型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	健康检查支持 UDP 协议，不支持修改。	UDP
高级配置		
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]。	3
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“完成”。

4.8 添加 HTTP 监听器


操作场景

HTTP 协议适用于需要对数据内容进行识别的应用，如 Web 应用、小的手机游戏等。您可以添加一个 HTTP 监听器转发来自 HTTP 协议的请求。

注意

- 前端协议为“HTTP”时，后端协议默认为“HTTP”，且不支持修改。
- 如果您的独享型负载均衡实例类型为网络型（TCP/UDP），则无法创建 HTTP 监听器。

添加独享型负载均衡 HTTP 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”，配置监听器。配置监听器参数参

见表 4-18。

表4-18 独享型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。 协议选择 HTTP，端口取值范围[1-65535]。	HTTP/80
重定向	重定向开关是否开启。 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 监听器和 HTTP 监听器，可以通过重定向功能，将 HTTP 监听器访问重定向至 HTTPS 监听器。 HTTP 监听器被重定向后，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。	-listener-9ecd (HTTPS/443)
高级配置		
访问策略	支持通过白名单和黑名单进行访问控制，更多信息请参见 4.5 访问控制策略： 允许所有 IP 访问 黑名单 白名单	黑名单
IP 地址组	设置白名单或者黑名单时，必须选择一个 IP 地址组。如果还未创建 IP 地址组，需要先创建 IP 地址组，更多关于 IP 地址组的信息请参见 9.1 错误!表格结果无效。 。	ipGroup-b2
获取弹性公网 IP	通过 X-Forwarded-ELB-IP 头字段获取 ELB 实例公网 IP 地址。若您需要将 ELB 公网 IP 透传到后端，只需在创建 HTTP 监听器时，打开该开关。	-
获取监听器端口号	通过 X-Forwarded-Port 头字段获取 ELB 实例监听器端口号。若您需要将 ELB 实例监听器的端口号透传到后端，只需在创建 HTTP 监听器时，打开该开关。	-
获取客户端请求端口号	通过 X-Forwarded-For-Port 头字段获取客户端请求端口号。若您需要将客户端请求的端口号透传到后端，只需在创建 HTTP 监听器时，打开该开关。	-

参数	说明	示例
重写 X-Forwarded-Host	开关关闭：ELB 透传客户端的 X-Forwarded-Host。 开关开启：ELB 以客户端请求头的 Host 重写 X-Forwarded-Host 向后端传输。	-
空闲超时时间（秒）	如果在超时时间内一直没有访问请求，负载均衡会中断当前连接，直到下一次请求到来时再重新建立新的连接。 时间取值范围[0-4000]。	60
请求超时时间（秒）	客户端向负载均衡发起请求，如果在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。 时间取值范围[1-300]。	60
响应超时时间（秒）	负载均衡向后端云主机发起请求，如果超时时间内接收请求的后端云主机无响应，负载均衡会向其他后端云主机重试请求。如果重试期间后端云主机一直没有响应，则负载均衡会给客户端返回 HTTP 504 错误码。 时间取值范围[1-300]。 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云主机无响应，则直接会返回 HTTP 504 错误码。	60
描述	对于监听器描述。 字数范围：0/255。	-

6. 单击“下一步”，配置后端主机组及配置健康检查。配置后端主机组参数请参见表 4-19。

表4-19 独享型负载均衡配置后端主机组参数说明

参数	说明	示例
后端主机组	把具有相同特性的后端云主机放在一个组。 新创建 使用已有 说明 使用已有后端主机组时，请确保此后端主机组未被使用。并且只能选择前端协议匹配的后端主机组。例如前端协议是 TCP 时，后端协议只能是 TCP。	新创建
名称	后端主机组名称。	server_group-sq4v

参数	说明	示例
后端协议	云主机开通的协议。 前端协议为 HTTP 时，后端协议默认为 HTTP，不支持修改。	HTTP
分配策略类型	负载均衡采用的算法。 加权轮询算法： 根据后端云主机的权重，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。 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。 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，同时对后端云主机进行编号，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。 说明 <ul style="list-style-type: none"> • 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。 • 对于加权轮询算法和加权最少连接，当服务器的权重为“0”时，将不会被分发访问请求。 	加权轮询算法
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服务器进行处理。 说明 当分配策略类型为“加权轮询算法”或“加权最少连接”时，可配置会话保持。	-
会话保持类型	前端协议为 HTTP 或 HTTPS 时，支持负载均衡器 cookie 类型的会话保持。 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云主机处理。	负载均衡器 cookie
会话保持时间（分钟）	当分配策略类型选择“加权轮询算法”或“加权最少连接”，会话保持开启后，需添加会话保持时间。 四层会话保持的会话保持时间取值范围为[1，60]。 七层会话保持的会话保持时间取值范围为[1，1440]。	20

参数	说明	示例
描述	后端主机组的描述。 字数范围：0/255。	-

7. 配置健康检查参数请参见表 4-20。

表4-20 独享型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	健康检查支持 HTTP、TCP、HTTPS 协议，设置后不可修改。	HTTP
端口	健康检查端口号，取值范围[1, 65535]，为可选参数。 说明：未配置健康检查端口时，默认使用后端云主机端口进行健康检查。配置后，使用配置的健康检查端口进行健康检查。	80
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
高级配置		
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]。	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]。 说明 例如： 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”。	/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

参数	说明	示例
HTTP 状态码	<p>自定义健康检查返回的状态码。当“协议”为 HTTP 或 HTTPS 时生效。</p> <p>可输入 200-599 范围内不重复的单个数字或正序的数字区间。多个 HTTP 状态码使用逗号隔开，最多支持 5 个。</p> <p>说明：如果您要使用该特性，请进入至 ELB 服务控制台后，单击页面左下角的“体验新版”。目前新版控制台在公测中，待公测结束后即可正常使用。</p>	200

- 单击“完成”。

添加共享型负载均衡 HTTP 监听器


- 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，单击需要添加监听器的负载均衡名称。
- 切换到“监听器”页签，单击“添加监听器”，配置监听器。配置监听器参数参见表 4-21。

表4-21 共享型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	<p>负载分发的协议和端口。</p> <p>协议选择 HTTP，端口取值范围[1-65535]。</p>	HTTP/80
重定向	<p>重定向开关是否开启。</p> <p>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 监听器和 HTTP 监听器，可以通过重定向功能，将 HTTP 监听器访问重定向至 HTTPS 监听器。</p> <p>HTTP 监听器被重定向后，会返回 301 返回码。</p>	-
重定向至	选择需要重定向 HTTPS 监听器的名称。	-listener-9ecd (HTTPS/443)
高级配置		

参数	说明	示例
访问策略	支持通过白名单和黑名单进行访问控制，更多信息请参见 4.5 访问控制策略： 允许所有 IP 访问 黑名单 白名单	白名单
IP 地址组	设置白名单或者黑名单时，必须选择一个 IP 地址组。如果还未创建 IP 地址组，需要先创建 IP 地址组，更多关于 IP 地址组的信息请参见 9.1 错误!表格结果无效。 。	ipGroup-b2
空闲超时时间（秒）	如果在超时时间内一直没有访问请求，负载均衡会中断当前连接，直到下一次请求到来时再重新建立新的连接。 时间取值范围[0-4000]。	60
请求超时时间（秒）	客户端向负载均衡发起请求，如果在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。 时间取值范围[1-300]。	60
响应超时时间（秒）	负载均衡向后端云主机发起请求，如果超时时间内接收请求的后端云主机无响应，负载均衡会向其他后端云主机重试请求。如果重试期间后端云主机一直没有响应，则负载均衡会给客户端返回 HTTP 504 错误码。 时间取值范围[1-300]。 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云主机无响应，则直接会返回 HTTP 504 错误码。	60
描述	对于监听器描述。 字数范围：0/255。	-
标签	可通过配置该项使用标签功能。标签的“键”和“值”是一一对应的，其中“键”值是唯一的。	-

6. 单击“下一步”，配置后端主机组及配置健康检查。配置后端主机组参数请参见表 4-22。

表4-22 共享型负载均衡配置后端主机组参数说明

参数	说明	示例
后端主机组	<p>把具有相同特性的后端云主机放在一个组。</p> <p>新创建</p> <p>使用已有</p> <p>说明</p> <p>使用已有后端主机组时，请确保此后端主机组未被使用。并且只能选择前端协议匹配的后端主机组。例如前端协议是 TCP 时，后端协议只能是 TCP。</p>	新创建
名称	后端主机组名称。	server_group-sq4v
后端协议	<p>云主机开通的协议。</p> <p>前端协议为 HTTP 时，后端协议默认为 HTTP，不支持修改。</p>	HTTP
分配策略类型	<p>负载均衡采用的算法。</p> <p>加权轮询算法：根据后端云主机的权重，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。</p> <p>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。</p> <p>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，同时对后端云主机进行编号，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。</p> <p>说明</p> <ul style="list-style-type: none"> • 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。 • 对于加权轮询算法和加权最少连接，当服务器的权重为“0”时，将不会被分发访问请求。 	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>说明</p> <p>当分配策略类型为“加权轮询算法”时，可配置会话保持。</p>	-

参数	说明	示例
会话保持类型	共享型负载均衡，HTTP 和 HTTPS 协议支持负载均衡器 cookie、应用程序 cookie 类型。 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云主机处理。 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云主机处理。	负载均衡 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）	当分配策略类型选择“加权轮询算法”或“加权最少连接”，会话保持开启后，需添加会话保持时间。 四层会话保持的会话保持时间取值范围为[1, 60]。 七层会话保持的会话保持时间取值范围为[1, 1440]。	20
描述	后端主机组的描述。 字数范围：0/255。	-

7. 配置健康检查参数请参见表 4-23。

表4-23 共享型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	健康检查支持 TCP、HTTP 协议，设置后不可修改。	HTTP
端口	健康检查端口号，取值范围[1, 65535]，为可选参数。 说明：未配置健康检查端口时，默认使用后端云主机端口进行健康检查。配置后，使用配置的健康检查端口进行健康检查。	80
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
高级配置		
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]。	3

参数	说明	示例
检查路径	<p>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]。</p> <p>说明</p> <p>例如：</p> <p>访问链接为：http://www.example.com/chat/try/，则检查路径填写“/chat/try/”。</p> <p>访问链接为：http://192.168.63.187:9096/chat/index.html，则检查路径填写“/chat/index.html”。</p>	/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“完成”。

4.9 添加 HTTPS 监听器

操作场景

HTTPS 协议适用于需要加密传输的应用。您可以添加一个 HTTPS 监听转发来自 HTTPS 协议的请求。ELB 对于用户的 HTTPS 的请求进行解密，然后发送至后端云主机；后端云主机处理完请求后的返回包首先发送至 ELB，由 ELB 进行加密后，再传回用户侧。

添加 HTTPS 监听器时，要求后端子网预留足够的 IP 地址，可以通过负载均衡器的“基本信息 > 后端子网”添加多个后端子网来增加后端子网的 IP 地址。添加子网后，请取消对应子网的 ACL 配置，否则可能导致负载均衡访问异常。

注意

- 独享型负载均衡前端协议为“HTTPS”时，后端协议可以选择“HTTP”或“HTTPS”。
- 共享型负载均衡前端协议为“HTTPS”时，后端协议默认为“HTTP”，且不支持修改。
- 如果您的独享型负载均衡实例类型为网络型（TCP/UDP），则无法创建 HTTPS 监听器。

添加独享型负载均衡 HTTPS 监听器

1. 登录管理控制台。
2. 在管理控制台左上角单击  图标，选择区域和项目。
3. 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”，配置监听器。配置监听器参数参见表 4-24。

表4-24 独享型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。 协议选择 HTTPS，端口取值范围[1-65535]。	HTTPS/443
SSL 解析方式	确保服务安全，请选择客户端到服务器端认证方式。可选择“单向认证”或“双向认证”。 <ul style="list-style-type: none"> ● 如仅进行服务器端认证，请选择单向认证。 ● 双向认证需要负载均衡实例与访问用户互相提供身份认证，从而允许通过认证的用户访问负载均衡实例，后端云主机无需额外配置双向认证。 	单项认证
服务器证书	协议类型为 HTTPS 时，需绑定服务器证书。 服务器证书用于 SSL 握手协商，需提供证书内容和私钥。详见 8.3 创建/修改/删除证书。	-
CA 证书	协议类型为 HTTPS 时，需绑定 CA 证书。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。详见创建/修改/删除证书。	-
开启 SNI	HTTPS 协议的负载均衡可以选择是否开启 SNI。 SNI 是为了解决一个服务器使用多个域名和证书的 TLS 扩展。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，ELB 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。详见 SNI 证书-HTTPS 监听器绑定多个证书（多域名访问）	-
SNI 证书	HTTPS 协议的负载均衡设置开启 SNI 后需要选择域名对应的证书。可选择已创建或者创建新的 SNI 证书。详见创建/修改/删除证书。	-
高级配置		

参数	说明	示例
访问策略	支持通过白名单和黑名单进行访问控制，更多信息请参见 4.5 访问控制策略： 允许所有 IP 访问 黑名单 白名单	白名单
IP 地址组	设置白名单或者黑名单时，必须选择一个 IP 地址组。如果还未创建 IP 地址组，需要先创建 IP 地址组，更多关于 IP 地址组的信息请参见 9.1 错误!表格结果无效。。	ipGroup-b2
HTTP/2	协议类型为 HTTPS 时，可选择是否支持该协议类型。详见 HTTP/2。	-
安全策略	支持选择可用的安全策略，更多信息请参见 5.6 TLS 安全策略。	安全策略 TLS-1-0
获取弹性公网 IP	通过 X-Forwarded-ELB-IP 头字段获取 ELB 实例公网 IP 地址。若您需要将 ELB 公网 IP 透传到后端，只需在创建 HTTP 监听器时，打开该开关。	-
获取监听器端口号	通过 X-Forwarded-Port 头字段获取 ELB 实例监听器端口号。若您需要将 ELB 实例监听器的端口号透传到后端，只需在创建 HTTP 监听器时，打开该开关。	-
获取客户端请求端口号	通过 X-Forwarded-For-Port 头字段获取客户端请求端口号。若您需要将客户端请求的端口号透传到后端，只需在创建 HTTP 监听器时，打开该开关。	-
重写 X-Forwarded-Host	开关关闭：ELB 透传客户端的 X-Forwarded-Host。 开关开启：ELB 以客户端请求头的 Host 重写 X-Forwarded-Host 向后端传输。	-
空闲超时时间（秒）	如果在超时时间内一直没有访问请求，负载均衡会中断当前连接，直到下一次请求到来时再重新建立新的连接。 时间取值范围[0-4000]。	60
请求超时时间（秒）	客户端向负载均衡发起请求，如果在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。 时间取值范围[1-300]。	60

参数	说明	示例
响应超时时间（秒）	负载均衡向后端云主机发起请求，如果超时时间内接收请求的后端云主机无响应，负载均衡会向其他后端云主机重试请求。如果重试期间后端云主机一直没有响应，则负载均衡会给客户端返回 HTTP 504 错误码。 时间取值范围[1-300]。 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云主机无响应，则直接会返回 HTTP 504 错误码。	60
描述	对于监听器描述。 字数范围：0/255。	-

6. 单击“下一步”，配置后端主机组及配置健康检查。配置后端主机组参数请参见表 4-25。

表4-25 独享型负载均衡配置后端主机组参数说明

参数	说明	示例
后端主机组	把具有相同特性的后端云主机放在一个组。 新创建 使用已有 说明 使用已有后端主机组时，请确保此后端主机组未被使用。并且只能选择前端协议匹配的后端主机组。例如前端协议是 TCP 时，后端协议只能是 TCP。	新创建
名称	后端主机组名称。	server_group-sq4v
后端协议	云主机开通的协议。 前端协议为 HTTPS 时，后端协议支持修改，可修改为 HTTP 或 HTTPS。	HTTP

参数	说明	示例
分配策略类型	<p>负载均衡采用的算法。</p> <p>加权轮询算法：根据后端云主机的权重，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。</p> <p>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。</p> <p>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，同时对后端云主机进行编号，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。</p> <p>说明</p> <ul style="list-style-type: none"> • 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。 • 对于加权轮询算法和加权最少连接，当服务器的权重为“0”时，将不会被分发访问请求。 	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>说明</p> <p>当分配策略类型为“加权轮询算法”时，可配置会话保持。</p>	-
会话保持类型	<p>前端协议为 HTTP 或 HTTPS 时，支持负载均衡器 cookie 类型的会话保持。</p> <p>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云主机处理。</p>	负载均衡器 cookie
会话保持时间（分钟）	<p>当分配策略类型选择“加权轮询算法”或“加权最少连接”，会话保持开启后，需添加会话保持时间。</p> <p>四层会话保持的会话保持时间取值范围为[1, 60]。</p> <p>七层会话保持的会话保持时间取值范围为[1, 1440]。</p>	20
描述	<p>后端主机组的描述。</p> <p>字数范围：0/255。</p>	-

7. 配置健康检查参数请参见表 4-26。

表4-26 独享型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	健康检查支持 HTTP、TCP、HTTPS 协议，设置后不可修改。	HTTP
前端端口	取值范围[1, 65535]。	80
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
高级配置		
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]。	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]。 说明 例如： 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”。	/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
HTTP 状态码	自定义健康检查返回的状态码。当“协议”为 HTTP 或 HTTPS 时生效。 可输入 200-599 范围内不重复的单个数字或正序的数字区间。多个 HTTP 状态码使用逗号隔开，最多支持 5 个。 说明： 如果您要使用该特性，请进入至 ELB 服务控制台后，单击页面左下角的“体验新版”。目前新版控制台在公测中，待公测结束后即可正常使用。	200

8. 单击“提交”。

添加共享型负载均衡 HTTPS 监听器

1. 登录管理控制台。


2. 在管理控制台左上角单击  图标，选择区域和项目。
3. 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”，配置监听器。配置监听器参数参见表 4-27。

表4-27 共享型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。 协议选择 HTTPS ，端口取值范围[1-65535]。	HTTPS/443
SSL 解析方式	确保服务安全，请选择客户端到服务器端认证方式。可选择“单向认证”或“双向认证”。 ● 如仅进行服务器端认证，请选择单向认证。 双向认证需要负载均衡实例与访问用户互相提供身份认证，从而允许通过认证的用户访问负载均衡实例，后端云主机无需额外配置双向认证。	单向认证
服务器证书	协议类型为 HTTPS 时，需绑定服务器证书。 服务器证书用于 SSL 握手协商，需提供证书内容和私钥。详见 8.3 创建/修改/删除证书。	-
开启 SNI	HTTPS 协议的负载均衡可以选择是否开启 SNI 。 SNI 是为了解决一个服务器使用多个域名和证书的 TLS 扩展。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， ELB 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。详见 SNI 证书-HTTPS 监听器绑定多个证书（多域名访问）	-
SNI 证书	HTTPS 协议的负载均衡设置开启 SNI 后需要选择域名对应的证书。可选择已创建或者创建新的 SNI 证书。详见创建/修改/删除证书。	-
高级配置		

参数	说明	示例
访问策略	支持通过白名单和黑名单进行访问控制，更多信息请参见 4.5 访问控制策略： 允许所有 IP 访问 黑名单 白名单	白名单
IP 地址组	设置白名单或者黑名单时，必须选择一个 IP 地址组。如果还未创建 IP 地址组，需要先创建 IP 地址组，更多关于 IP 地址组的信息请参见 9.1 错误!表格结果无效。 。	ipGroup-b2
HTTP/2	协议类型为 HTTPS 时，可选择是否支持该协议类型。详见 HTTP/2。	-
安全策略	支持选择可用的安全策略，更多信息请参见 5.6 TLS 安全策略。	安全策略 TLS-1-2
获取弹性公网 IP	通过 X-Forwarded-ELB-IP 头字段获取 ELB 实例公网 IP 地址。若您需要将 ELB 公网 IP 透传到后端，只需在创建 HTTP 监听器时，打开该开关。	-
获取监听器端口号	通过 X-Forwarded-Port 头字段获取 ELB 实例监听器端口号。若您需要将 ELB 实例监听器的端口号透传到后端，只需在创建 HTTP 监听器时，打开该开关。	-
获取客户端请求端口号	通过 X-Forwarded-For-Port 头字段获取客户端请求端口号。若您需要将客户端请求的端口号透传到后端，只需在创建 HTTP 监听器时，打开该开关。	-
重写 X-Forwarded-Host	开关关闭：ELB 透传客户端的 X-Forwarded-Host。 开关开启：ELB 以客户端请求头的 Host 重写 X-Forwarded-Host 向后端传输。	-
空闲超时时间（秒）	如果在超时时间内一直没有访问请求，负载均衡会中断当前连接，直到下一次请求到来时再重新建立新的连接。 时间取值范围[0-4000]。	60
请求超时时间（秒）	客户端向负载均衡发起请求，如果在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。 时间取值范围[1-300]。	60

参数	说明	示例
响应超时时间（秒）	负载均衡向后端云主机发起请求，如果超时时间内接收请求的后端云主机无响应，负载均衡会向其他后端云主机重试请求。如果重试期间后端云主机一直没有响应，则负载均衡会给客户端返回 HTTP 504 错误码。 时间取值范围[1-300]。 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云主机无响应，则直接会返回 HTTP 504 错误码。	60
描述	对于监听器描述。 字数范围：0/255。	-

6. 单击“下一步”，配置后端主机组及配置健康检查。配置后端主机组参数请参见表 4-28。

表4-28 共享型负载均衡配置后端主机组参数说明

参数	说明	示例
后端主机组	把具有相同特性的后端云主机放在一个组。 新创建 使用已有 说明 使用已有后端主机组时，请确保此后端主机组未被使用。并且只能选择前端协议匹配的后端主机组。例如前端协议是 TCP 时，后端协议只能是 TCP。	新创建
名称	后端主机组名称。	server_group-sq4v
后端协议	云主机开通的协议。 前端协议为 HTTPS 时，后端协议默认为 HTTP，不支持修改。	HTTP

参数	说明	示例
分配策略类型	<p>负载均衡采用的算法。</p> <p>加权轮询算法：根据后端云主机的权重，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。</p> <p>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。</p> <p>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，同时对后端云主机进行编号，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 的请求始终被派发到某特定的服务器。</p> <p>说明</p> <ul style="list-style-type: none"> • 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。 • 对于加权轮询算法和加权最少连接，当服务器的权重为“0”时，将不会被分发访问请求。 	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>说明</p> <p>当分配策略类型为“加权轮询算法”时，可配置会话保持。</p>	-
会话保持类型	<p>共享型负载均衡，HTTP 和 HTTPS 协议支持负载均衡器 cookie、应用程序 cookie 类型。</p> <p>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云主机处理。</p> <p>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云主机处理。</p>	负载均衡 cookie
cookie 名称	<p>当会话保持选择应用程序 cookie 时，需要填写 cookie 名称。</p>	cookieName-qsp
会话保持时间（分钟）	<p>当分配策略类型选择“加权轮询算法”或“加权最少连接”，会话保持开启后，需添加会话保持时间。</p> <p>四层会话保持的会话保持时间取值范围为[1, 60]。</p> <p>七层会话保持的会话保持时间取值范围为[1, 1440]。</p>	20

参数	说明	示例
描述	后端主机组的描述。 字数范围：0/255。	-

7. 配置健康检查参数请参见表 4-29。

表4-29 共享型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	健康检查支持 TCP、HTTP 协议，设置后不可修改。	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。 说明：未配置健康检查端口时，默认使用后端云主机端口进行健康检查。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		
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]。	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]。 说明 例如： 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”。	/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“完成”。

添加共享型负载均衡 HTTPS 监听器

如果您不希望负载均衡器对 HTTPS 流量进行解密，可以通过配置相同端口的 TCP

监听器 将 HTTPS 流量透传到后端云主机。并且在实例的安全组配置相同端口的 TCP 入方向规则，以允许相同端口上来自负载均衡器的入站流量。如下图所示，TCP 监听器如何将端口为 443 的 HTTPS 流量进行无解密透传到后端云主机。

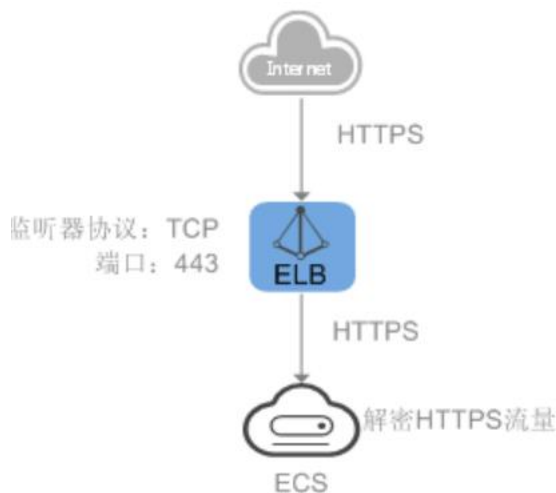


图4-5 连接 ID 算法流量分发

配置 QUIC 协议的 UDP 监听器（独享型）

操作场景

前端为 UDP 协议的监听器，支持 QUIC（Quick UDP Internet Connection）作为后端监听协议。配合连接 ID 算法，将同一个连接 ID 的请求转发到后端云主机。使用 QUIC 协议的监听器具有低延迟、高可靠和无队头阻塞的优点，非常适合移动互联网易用、支持在 WIFI 和运营商网络中无缝切换，而不用重新去建立连接。


QUIC 协议的版本有：Q043、Q046、Q050。

QUIC 协议的 UDP 监听器不支持分片包。

约束与限制

独享型负载均衡支持使用后端监听器为 QUIC 协议。

独享型负载均衡器已经选择四层“网络型（TCP/UDP）”类型的规格。

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。此负载均衡器需要选择网络型（TCP/UDP）规格，使其能够创建四层(TCP/UDP)监听器
5. 切换到“监听器”页签，单击“添加监听器”。
6. 在“添加监听器”页签，“前端协议”请选择“UDP”，其他参数根据实际情况

设置，完成后单击“下一步”。

7. 在“配置后端分配策略”页面，“后端协议”选择“QUIC”，其他参数根据实际情况设置。
8. 根据需要配置相关参数，配置完成后，单击“提交”。

4.10 添加/修改监听器的超时时间


操作场景

弹性负载均衡支持配置和修改监听器的超时时间（空闲超时时间、请求超时时间、响应超时时间），方便用户根据自身业务情况，自定义调整超时时间。例如，HTTP/HTTPS 协议客户端的请求文件比较大，可以增加请求超时时间，以便能够顺利完成文件的传输。




共享型负载均衡器支持修改 TCP/HTTP/HTTPS 协议的超时时间，但不支持修改 UDP 的超时时间。

独享型负载均衡支持修改 TCP/UDP/HTTP/HTTPS 协议的超时时间。

添加超时时间

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”。
6. 在“添加监听器”页签，可以根据实际业务诉求修改超时时间。修改后单击“下一步”。
7. 根据需要配置相关参数，配置完成后，单击“提交”。

修改超时时间

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“添加监听器”。
共享型负载均衡器，单击需要修改超时时间的目标监听器名称右侧  按钮。
独享型负载均衡器，单击需要修改超时时间的目标监听器名称右侧  按钮，选择修改监听器。
6. 在“修改监听器”页签，点击高级配置。
7. 修改“空闲超时时间”或“请求超时时间”或“响应超时时间”后，单击“下一

步”。

8. 单击“完成”。

4.11 修改/删除监听器

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。

监听器被删除后无法恢复，请谨慎操作。

说明

目前暂不支持修改“前端协议/端口”和“后端协议”，如果要修改监听器的协议或端口，请重新创建监听器。

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：
独享型负载均衡器，单击需要修改的监听器名称右侧的  按钮，选择“修改监听器”。
共享型负载均衡器，单击需要修改的监听器名称右侧的  。
6. 修改参数，单击“完成”。

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云主机，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。
- 如果监听器包含了转发策略，删除监听器之前需先删除转发策略。
- 删除监听器后会同时删除所绑定的后端主机组。

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”。

5 HTTP/HTTPS 监听器高级配置

5.1 转发策略（共享型）

操作场景

您可以通过给共享型负载均衡添加转发策略，将来自不同域名或者不同 URL 的请求转发到不同的后端主机组处理。

例如：您可以通过添加转发策略，将视频、图片、音频、文本等请求分别转发到不同的后端主机组上去处理，便于灵活的分流业务，合理的分配资源。

转发策略由**转发规则**和**动作**两部分组成：

- 支持的转发规则有：**域名、URL**。
- 支持的动作类型有：**转发至后端主机组**。

约束与限制

- 此功能目前仅支持协议类型为 HTTP、HTTPS 的监听器。
- 配置转发策略时，请注意以下事项：
每个 URL 路径需要存于后端云主机（即必须是后端云主机上真实存在的路径），

否则访问后端云主机时，后端云主机会返回 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主机组。
 - 如果不能匹配到监听器的转发策略，则按照默认转发策略将请求转发到监听器默认的后端主机组（创建监听器时配置的后端主机组）。

注意

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。将出现冲突的转发策略都删除后重新添加，即可恢复正常。

添加转发策略

- 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，单击需要添加转发策略的负载均衡器名称。
- 切换到监听器页签，单击目标监听器名称。
- 单击“转发策略”右侧的“添加”按钮。
- 在“添加转发策略”弹框中参考表 5-1 配置参数。
- 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5-1 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

配置类型	参数	说明	样例
	URL 匹配规则	<p>精确匹配</p> <p>请求的 URL 和设定 URL 完全一致。</p> <p>前缀匹配</p> <p>请求的 URL 匹配以设定 URL 开头的 URL。</p> <p>正则匹配</p> <p>请求的 URL 和设定的 URL 正则表达式匹配。</p> <p>说明</p> <ul style="list-style-type: none"> 匹配的优先级为：精确匹配 > 前缀匹配 > 正则匹配 前缀匹配遵循“最长字符串匹配”原则，例如存在 /elb 和 /elbvip 两个规则，访问的 URL 为 /elbvipplus，则会优先匹配 /elbvip 这个规则。 	精确匹配
	URL	触发转发的 URL。	/login.php
	描述	转发策略的描述。	-
添加后端主机组	后端主机组	<p>可选择“新创建”或“使用已有”。</p> <p>选择“新创建”，可参考表 6-3 和表 6-4 进行参数配置。</p> <p>选择“使用已有”，为转发策略选择已有的后端主机组即可。</p>	新创建

URL 匹配示例

如表 5-2 所示，是一个 URL 匹配示例，转发情况如 0 所示。

表5-2 URL 匹配示例

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

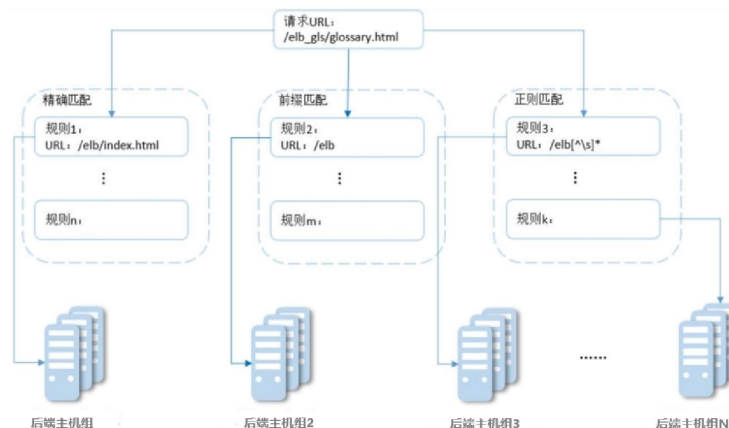




图5-1 转发示例



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 对应的后端主机组 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主机组 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。

5.2 转发策略（独享型）

未开启“高级转发策略”功能时，请参考此章节为独享型负载均衡添加转发策略。

操作场景

您可以通过给独享型负载均衡添加转发策略，将来自不同域名或者不同 URL 的请求转发到不同的后端主机组处理。

例如：您可以通过添加转发策略，将视频、图片、音频、文本等请求分别转发到不同的后端主机组上去处理，便于灵活的分流业务，合理的分配资源。



转发策略由**转发规则**和**动作**两部分组成：

- 支持的转发规则有：域名、URL。
- 支持的动作类型有：转发至后端主机组、重定向至监听器（仅 HTTP 监听器支持）。

约束与限制

- 此功能目前仅支持协议类型为 HTTP、HTTPS 的监听器。
- HTTPS 监听器不支持“重定向至监听器”动作类型。
- 配置转发策略时，请注意以下事项：
 - 每个 URL 路径需要存于后端云主机（即必须是后端云主机上真实存在的路径），否则访问后端云主机时，后端云主机会返回 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。
 - 输入的域名总长度不能超过 46 个字符。
- 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主机组。
 - 如果不能匹配到监听器的转发策略，则按照默认转发策略将请求转发到监听器默认的后端主机组（创建监听器时配置的后端主机组）。

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. 单击目标监听器右侧的  按钮，选择“设置转发策略”。
- 或者直接单击页面右侧的“转发策略”，切换到转发策略页签，单击“添加转发

策略”

7. 在右侧“转发策略”子页签中，单击“添加转发策略”。参考表 5-3 配置参数。

表5-3 添加转发策略的参数

参数		说明	样例
转发规则	域名	触发转发的域名，仅支持精确域名。 域名或者 URL 至少要指定一个。 说明 高级转发策略支持泛域名转发，详细请参考 5.3 高级转发策略（独享型）。	www.test.com
	URL	触发转发的 URL。URL 的匹配规则有如下三种： 精确匹配 请求的 URL 和设定 URL 完全一致。 前缀匹配 请求的 URL 匹配已设定 URL 开头的 URL。 正则匹配 请求的 URL 和设定的 URL 正则表达式匹配。	/login.php
动作	转发至后端主机组	如果请求与配置的转发规则（条件）匹配，则将请求转发至配置的后端主机组。	转发至后端主机组
	重定向至监听器	如果请求与配置的转发规则（条件）匹配，则将请求重定向至配置的监听器。 仅 HTTP 监听器支持配置该动作类型。 说明 选择“重定向至监听器”并配置监听器后，除访问控制以外原有监听器配置会失效。 例如：配置了重定向至监听器后，当客户端通过 HTTP 请求访问的时候，后端云主机返回 HTTPS 的响应，即强制以 HTTPS 请求访问网页。因此实际以 HTTPS 监听器的配置为准向后端云主机进行转发，原有 HTTP 监听器的配置就无效了。	-
后端主机组		为转发策略选择已有的后端主机组。 “动作”选择“转发至后端主机组”时需要设置。	-
监听器		为转发策略选择已有的监听器。 “动作”选择“重定向至监听器”时需要设置。	-

8. 配置完成，单击“保存”。

URL 匹配示例

如表 5-4 所示，是一个 URL 匹配示例，转发情况如 0 所示。

表5-4 URL 匹配示例

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

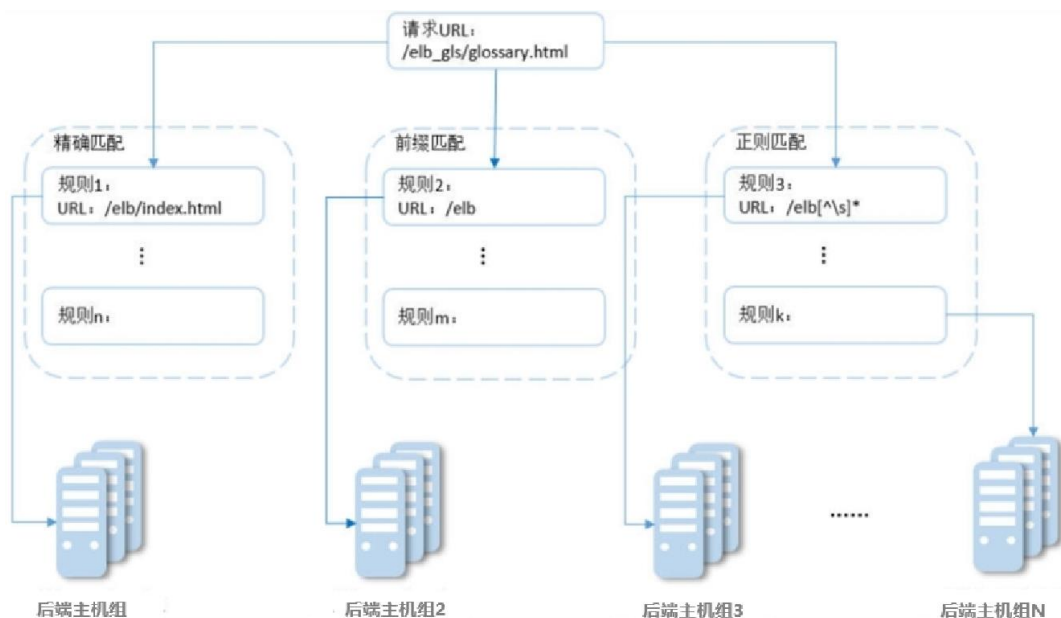



图5-2 转发示例

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 对应的后端主机组 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主机组 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. 单击转发策略右侧的  按钮，选择“设置转发策略”。
或者直接打开页面右侧的“转发策略”。
7. 在右侧“转发策略”子页签中，选择需要修改的转发策略，单击“编辑”。
8. 根据界面提示修改参数，单击“保存”。

删除转发策略

用户可以根据实际需要删除已经创建的转发策略。

转发策略删除后无法恢复，请谨慎操作。

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. 单击转发策略右侧的  按钮，选择“设置转发策略”。
或者直接打开页面右侧的“转发策略”。
7. 在右侧“转发策略”子页签中，选择需要删除的转发策略，单击“删除”。
8. 单击“是”。

5.3 高级转发策略（独享型）

5.3.1 高级转发策略简介

独享型负载均衡支持开启高级转发策略功能。开启了“高级转发策略”功能后，请参考以下内容独享型负载均衡添加转发策略。



图5-3 已开启高级转发策略

高级转发策略开启后，ELB 实例会根据您配置的高级转发策略将不同的请求按照不同的方式处理。

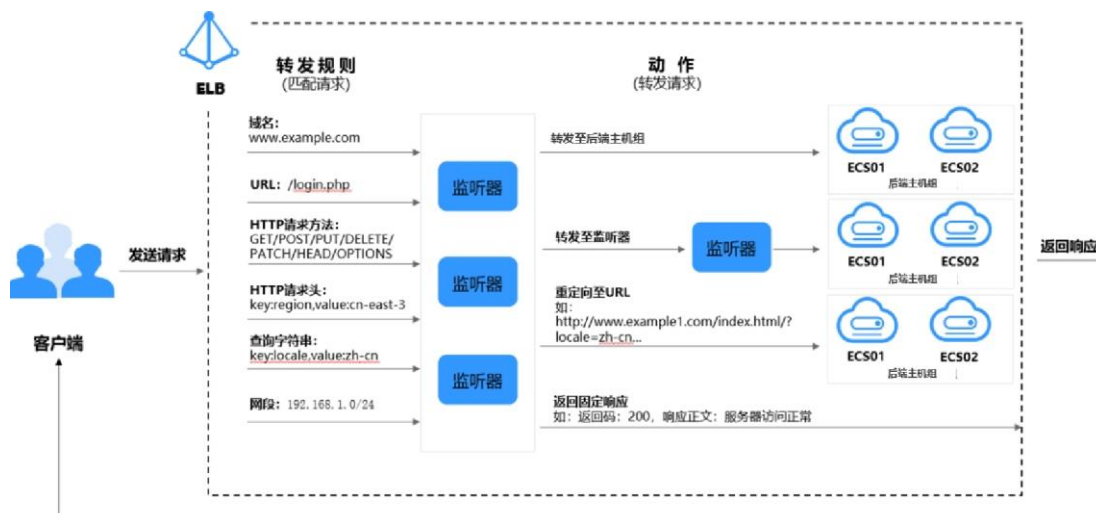


图5-4 高级转发策略（独享型）示意图

1. 客户端发送请求至 ELB；
2. ELB 首先根据事先设置好的高级转发策略中的转发规则匹配请求；
3. ELB 再根据转发规则对应的动作将客户端请求转发至对应的后端云主机进行处理；
4. 最后由后端云主机返回响应至客户端。

每条高级转发策略必须包含**转发规则**和**动作**。

- 支持的转发规则有：域名、URL、HTTP 请求方法、HTTP 请求头、查询字符串、网段。
- 支持的动作类型有：转发至后端主机组、重定向至监听器、添加重定向至 URL、返回固定响应。

5.3.2 转发规则和动作类型

每个监听器都具有默认转发策略，您也可以选择定义其他转发策略。每条转发策略由优先级、一个或多个转发规则以及转发动作组成。您可以随时添加或编辑转发策略。

默认转发策略

每个 HTTP/HTTPS 监听器创建后，都会有一个默认的转发策略，该转发策略的转发规则是监听器的协议和端口，动作为“转发至后端主机组”，后端主机组为创建监听器时配置的后端主机组。

默认转发策略的优先级最低，不参与转发策略排序；可以编辑，但不可删除。

当开启高级转发策略时，支持设置默认转发策略是否使用后端主机组。

转发规则类型

高级转发策略支持的转发规则类型有：域名、URL、HTTP 请求方法、HTTP 请求头、查询字符串、网段。

- **域名**

触发转发的域名，支持精确域名、泛域名。

可以并列添加多个域名。每个域名的长度不能超过 46 个字符。

至少包含两个字符串，字符串间以点分割，字符串只能由英文字母、数字、中划线、小数点和特殊字符*组成。字符串中须以英文字母、数字或*开头，不能以中划线结尾。*只能出现在开头且必须以*.开始。

域名示例：

```
请求链接为：https://www.example.com/login.php?locale=zh-cn&region=cn-north-4#videos
```

转发规则选择“域名”时，填写：www.example.com

- **URL**

触发转发的 URL。

可以并列添加多个 URL。

由英文字母、数字和特殊字符_~!;@^-%#\$.*+?;=!:|V0[]{}组成，并在精确匹配和前缀匹配时，只能由/开头。

URL 的匹配模式有如下三种：

- **精确匹配**

请求的 URL 和设定 URL 完全一致。

- **前缀匹配**

请求的 URL 匹配已设定 URL 开头的 URL。

- **正则匹配**

请求的 URL 和设定的 URL 正则表达式匹配。

URL 示例：

```
请求链接为：https://www.example.com/login.php?locale=zh-cn&region=cn-north-4#videos
```

转发规则选择“URL”时，填写：/login.php

注意

如果 URL 中包含特殊字符（如：?或#），则需要先将特殊字符进行转义后再配置 URL 转发策略。

- **查询字符串**

当请求中的字符串与设置好的转发策略中的字符串相匹配时，触发转发。

查询字符串是键值对的形式，需要分别设置值：

- **键（key）**：只能包含英文字母、数字和特殊字符!\$()*+,-/:;=?@^_-'。

- 值 (value)：一个键下可以配置多个值。只能包含英文字母、数字和特殊字符!\$()'*,./:;=?@^-'。还支持*和? 两种通配符。

查询字符串示例：

```
请求链接为：https://www.example.com/login.php?locale=zh-cn&region=cn-north-4#videos
转发规则需配置两个“查询字符串”：
查询字符串 A：
键 (key)：locale
值 (value)：zh-cn
查询字符串 B：
键 (key)：region
值 (value)：cn-north-4
```

- **HTTP 请求方法**

触发转发的 HTTP 请求方法。

可以并列设置多个请求方法。

主要分为以下几种：

GET、POST、PUT、DELETE、PATCH、HEAD、OPTIONS

HTTP 请求方法示例：

```
GET
```

- **HTTP 请求头**

触发转发的 HTTP 请求头。

请求头是键值对的形式，需要分别设置值：

- 键 (key)：只能由英文字母、数字、下划线和中划线组成。
- 值 (value)：一个键下可以配置多个值。只能包含英文字母、数字和特殊字符!#\$%&'()*+.,\/:;<=>?@[^-'{}~。还支持*和? 两种通配符。

HTTP 请求头示例：

```
键 (key)：Accept-Language
值 (value)：zh-CN
```

- **网段**

触发转发的请求网段。

网段示例：

```
192.168.1.0/24 或 2020:50::44/127
```

动作类型

高级转发策略支持的动作类型有：转发至后端主机组、重定向至监听器、重定向至 URL、返回固定响应。

- **转发至后端主机组**

如果满足转发策略条件，则将请求转发至配置好的后端主机组。需要配置后端主机组。

- **重定向至监听器**

如果满足转发策略条件，则将请求转发至配置好的监听器上。需要配置监听器。

📖 说明

选择“重定向至监听器”并配置监听器后，除访问控制以外原有监听器配置会失效。

例如：配置了重定向至监听器后，当客户端通过 HTTP 请求访问的时候，后端云主机返回 HTTPS 的响应，即强制以 HTTPS 请求访问网页。因此实际以 HTTPS 监听器的配置为准向后端云主机进行转发，原有 HTTP 监听器的配置就无效了。

● 重定向至 URL

如果满足转发策略条件，则将请求重定向至配置好的 URL。

客户端访问 ELB 网址 A 后，ELB 返回 302 或者其他 3xx 返回码和目的网址 B，客户端自动跳转到网址 B，网址 B 可自定义。

需要设置如下参数：

- **协议：**可以选择“`${protocol}`”或“HTTP”或“HTTPS”。`${protocol}`表示与源协议相同。
- **域名：**至少包含两个字符串，字符串间以点分割，字符串只能由英文字母、数字、中划线和小数点组成。字符串必须以英文字母或数字开头，不能以中划线结尾。`${host}`表示与源域名相同。
- **端口：**取值范围是 1~65535。`${port}`表示与源端口相同。
- **路径：**由英文字母、数字和特殊字符`_~';@^-%#&$.*+?=:|\/\[\]{}`组成，只能由/开头。`${path}`表示与源路径相同。
- **查询字符串：**只能包含英文字母、数字和特殊字符`!$()*+,-./:;=?@&^_-'`，&仅支持作为分隔符使用。
- **返回码：**可以选择“301”、“302”、“303”、“307”、“308”。

📖 说明

协议、域名、端口和路径至少设置一条。

重定向至 URL 示例

```
重定向的链接为: http://www.example1.com/index.html?locale=zh-cn#videos
协议: HTTP
域名: www.example1.com
端口: 8081
路径: /index.html
查询字符串: locale=zh-cn
返回码: 301
```

● 返回固定响应

如果满足转发策略条件，则返回固定响应。

用户访问 ELB 实例后，ELB 直接返回响应，不向后端云主机继续转发，返回响应的状态码和内容可以自定义。

需要设置如下参数：

- **返回码：**默认支持 2XX、4XX、5XX 系列状态码。
- **Content-Type：**可以选择“text/plain”、“text/css”、“text/html”、“application/javascript”、“application/json”。
- **响应正文：**非必填项。

响应正文示例：

```
text/plain
```

很抱歉, 暂不支持该语言.

text/css

```
<head><style type="text/css">div {background-color:red}#div {font-size:15px;color:red}</style></head>
```

text/html

```
<form action="/" method="post" enctype="multipart/form-data"><input type="text" name="description" value="some text"><input type="file" name="myFile"><button type="submit">Submit</button></form>
```

application/javascript

```
String.prototype.trim = function() {var reExtraSpace = /\s*(.*?)\s+$/;return this.replace(reExtraSpace, "$1")}
```

application/json

```
{ "publicip": { "type": "5 bgp", "ip version": 4 }, "bandwidth": { "name": "bandwidth123", "size": 10, "share_type": "PER" }}
```

📖 说明

填写响应正文时, 请不要有回车格式, 否则无法保存。

5.3.3 配置高级转发策略

操作场景

独享型负载均衡开启高级转发策略功能后, ELB 实例会根据您配置的高级转发策略将不同的请求按照不同的方式处理。

每条高级转发策略必须包含转发规则和动作。

- 支持的转发规则有: 域名、URL、HTTP 请求方法、HTTP 请求头、查询字符串、网段。
- 支持的动作类型有: 转发至后端主机组、重定向至监听器、添加重定向至 URL、返回固定响应。
- 支持域名类型转发规则以*.开头。
- 支持单条转发策略中添加多个转发规则。
- 支持转发策略排序。

约束与限制

- 高级转发策略开启后不允许关闭。
- 一个高级转发策略支持添加 10 个条件 (所有转发规则的条件之和)。

开启高级转发策略

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. 在页面右侧“基本信息”中，单击“开启高级转发策略”
7. 单击“确定”。

添加高级转发策略



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. 单击目标监听器右侧的  按钮，选择“设置转发策略”。
或者直接单击页面右侧的“转发策略”，进入到转发策略页签。
7. 在右侧“转发策略”子页签中，单击“添加转发策略”。
参考表 5-5 配置参数。
8. 配置完成，单击“保存”。

表5-5 添加转发策略的参数

参数		说明	样例
转发规则	域名	触发转发的域名，支持精确域名、泛域名。 可以并列添加多个域名。 至少包含两个字符串，字符串间以点分割，字符串只能由英文字母、数字、中划线、小数点和特殊字符*组成。字符串中须以英文字母、数字或*开头，不能以中划线结尾。*只能出现在开头且必须以*.开始。	www.example.com

参数	说明	样例
URL	<p>触发转发的 URL。</p> <p>可以并列添加多个 URL。</p> <p>由英文字母、数字和特殊字符 <code>_~';@^-%#\$. *+? ,=!: \/()[]{}组成</code>，并在精确匹配和前缀匹配时，只能由/开头。</p> <p>URL 的匹配模式有如下三种：</p> <p>精确匹配 请求的 URL 和设定 URL 完全一致。</p> <p>前缀匹配 请求的 URL 匹配已设定 URL 开头的 URL。</p> <p>正则匹配 请求的 URL 和设定的 URL 正则表达式匹配。</p>	/login.php
HTTP 请求方法	<p>触发转发的 HTTP 请求方法。主要分为以下几种：</p> <p>GET、POST、PUT、DELETE、PATCH、HEAD、OPTIONS</p> <p>可以并列设置多个请求方法。</p>	GET
HTTP 请求头	<p>触发转发的 HTTP 请求头。</p> <p>请求头是键值对的形式，需要分别设置值：</p> <p>键（key）：只能由英文字母、数字、下划线和中划线组成。</p> <p>值（value）：一个键下可以配置多个值。只能包含英文字母、数字和特殊字符 <code>!#\$%&'()*+,-./:;<=>?@[^_`{ }~</code>。</p>	键（key）： Accept-Language 值（value）： zh-CN
查询字符串	<p>触发转发的请求中的字符串。当请求中的字符串与设置好的转发策略中的字符串相匹配时，触发转发。</p> <p>查询字符串是键值对的形式，需要分别设置值：</p> <p>键（key）：只能包含英文字母、数字和特殊字符 <code>!\$()' *+,-./:;=?@^_`</code>。</p> <p>值（value）：一个键下可以配置多个值。只能包含英文字母、数字和特殊字符 <code>!\$()' *+,-./:;=?@^_`</code>。</p>	键（key）： locale 值（value）： zh-cn
网段	触发转发的请求网段。	192.168.1.0/24

参数		说明	样例
动作	转发至后端主机组	如果满足转发策略条件，则将请求转发至配置好的后端主机组。 需要配置后端主机组。	转发至后端主机组
	重定向至监听器	将 HTTP 监听器上的请求转发至配置好的 HTTPS 监听器上。 需要配置监听器。 说明 选择“重定向至监听器”并配置监听器后，除访问控制以外原有监听器配置会失效。 例如：配置了重定向至监听器后，当客户端通过 HTTP 请求访问的时候，后端云主机返回 HTTPS 的响应，即强制以 HTTPS 请求访问网页。因此实际以 HTTPS 监听器的配置为准向后端云主机进行转发，原有 HTTP 监听器的配置就无效了。	-
	重定向至 URL	如果满足转发策略条件，则将请求重定向至配置好的 URL。 客户端访问 ELB 网址 A 后，ELB 返回 302 或者其他 3xx 返回码和目的网址 B，客户端自动跳转到网址 B，网址 B 可自定义。 需要设置如下参数： 协议 ：可以选择 “\${protocol}” 或 “HTTP” 或 “HTTPS”。\${protocol} 表示与源协议相同。 域名 ：至少包含两个字符串，字符串间以点分割，字符串只能由英文字母、数字、中划线和小数点组成。字符串必须以英文字母或数字开头，不能以中划线结尾。 \${host} 表示与源域名相同。 端口 ：取值范围是 1~65535。\${port} 表示与源端口相同。 路径 ：由英文字母、数字和特殊字符 _~;@^-%#&\$.*+?,=!: \/(){} 组成，只能由 / 开头。\${path} 表示与源路径相同。 查询字符串 ：只能包含英文字母、数字、特殊字符 !\$() * + , / : ; = ? @ & ^ _ '，& 仅支持作为分隔符使用。 返回码 ：可以选择 “301”、“302”、“303”、“307”、“308”。 说明 协议、域名、端口和路径至少设置一条。	协议：HTTP 域名： www.example1.com 端口：8081 路径： /index.html 查询字符串： locale=zh-cn 返回码：301

参数	说明	样例
返回固定响应	<p>如果满足转发策略条件，则返回固定响应。用户访问 ELB 实例后，ELB 直接返回响应，不向后端云主机继续转发，返回响应的状态码和内容可以自定义。</p> <p>需要设置如下参数：</p> <p>返回码：只能由数字组成，默认以 2、4、5 开头，且总长度为 3 个字符。</p> <p>Content-Type：可以选择“text/plain”、“text/css”、“text/html”、“application/javascript”、“application/json”。</p> <p>响应正文：非必填项。</p>	<p>返回码：200</p> <p>Content-Type: text/plain</p> <p>响应正文：服务器访问正常</p>

转发策略排序

一个监听器可以添加多个转发策略，多个转发策略之间可以通过排序来设置优先级。



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. 单击转发策略右侧的  按钮，选择“设置转发策略”。或者直接打开页面右侧的“转发策略”。
7. 在右侧“转发策略”子页签中，单击上方的“排序”。
8. 单击转发策略右上角的“上移”或“下移”。
9. 单击“保存”。



图5-5 转发策略排序

URL 高级转发策略匹配示例

配置了 5 个 URL 高级转发策略，如表 5-6 所示。


表5-6 URL 高级转发策略匹配示例

请求 URL	转发策略	设定的 URL	匹配模式	转发策略优先级	转发至后端主机组
/elb/abc.html	转发策略 01	/elb/php.html	前缀匹配	优先级 1	后端主机组 01
	转发策略 02	/elb	前缀匹配	优先级 2	后端主机组 02
/exa/index.html	转发策略 03	/exa[^\s]*	正则匹配	优先级 3	后端主机组 03
	转发策略 04	/exa/index.html	正则匹配	优先级 4	后端主机组 04
/mpl/index.html	转发策略 05	/mpl/index.html	精确匹配	优先级 5	后端主机组 05

转发情况如下：

- 当请求 URL 为“/elb/abc.html”时，初步可以匹配到两个前缀匹配：转发策略 01、转发策略 02，但由于转发策略 01 的优先级高于转发策略 02 的优先级（优先级 2 < 优先级 1），因此最终匹配到转发策略 01，将请求转发至后端主机组 01。
- 当请求 URL 为“/exa/index.html”时，初步可以匹配到两个正则匹配：转发策略 03、转发策略 04，但由于转发策略 03 的优先级高于转发策略 04 的优先级（优先级 4 < 优先级 3），因此最终匹配到转发策略 03，将请求转发至后端主机组 03。
- 当请求 URL 为“/mpl/index.html”时，可以通过精确匹配，匹配到转发策略 05，将请求转发至后端主机组 05。

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. 单击转发策略右侧的  按钮，选择“设置转发策略”。
或者直接打开页面右侧的“转发策略”。

7. 在右侧“转发策略”子页签中，选择需要修改的转发策略，单击“编辑”。
8. 根据界面提示修改参数，单击“保存”。

删除转发策略

用户可以根据实际需要删除已经创建的转发策略。

转发策略删除后无法恢复，请谨慎操作。

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. 单击转发策略右侧的  按钮，选择“设置转发策略”。
或者直接打开页面右侧的“转发策略”。
7. 在右侧“转发策略”子页签中，选择需要删除的转发策略，单击“删除”。
8. 单击“是”。

5.4 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5-6 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5-7 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5-8 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5-9 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5-10 创建客户端证书 csr 文件

```
[root@lbv30003 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5-11 签发客户端证书

```
[root@lbv30003 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@lbv30003 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”，“SSL 解析方式”选择“双向认证”，并且在服务器证书和 CA 证书两个配置项中选择所添加的服务器证书和 CA 证书对应的名称。

📖 说明

1. 目前出香港外，其他区域均已上线双向认证功能。

添加后端云主机

请参考添加后端云主机相关操作指导，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。

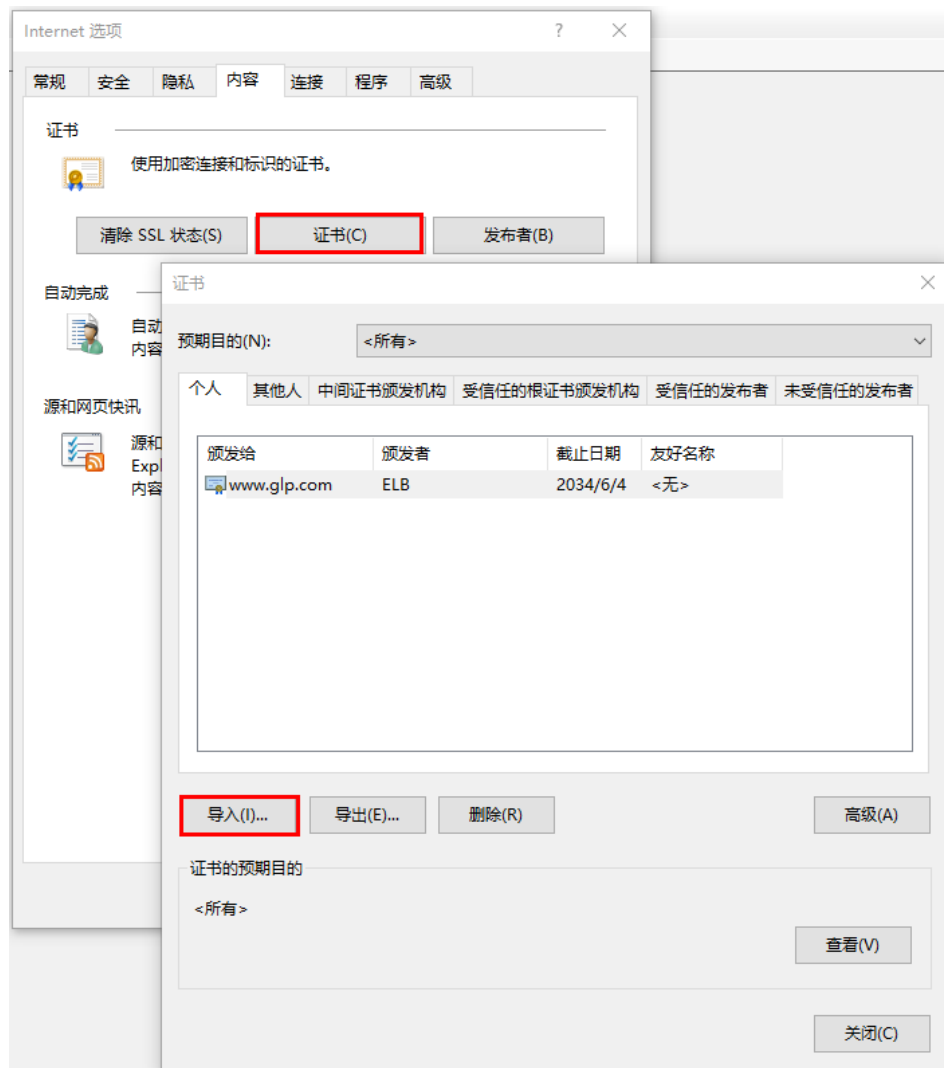


图5-12 安装 client.p12 证书

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 0。

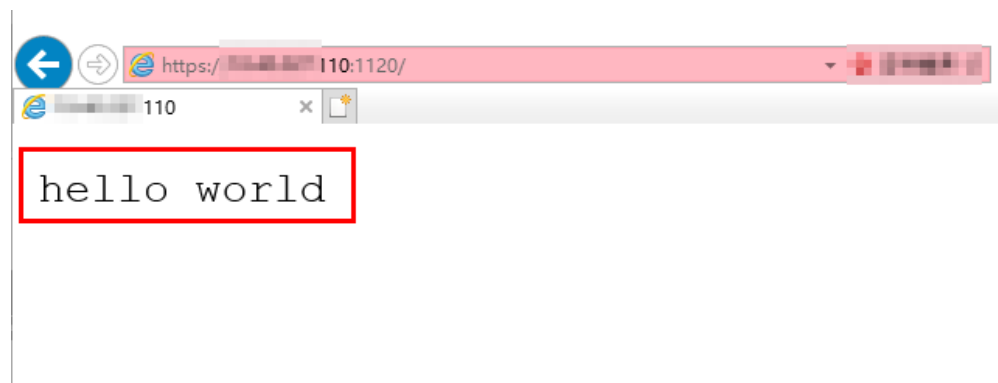


图5-13 正常访问网站

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 5-14 说明验证成功。

图5-14 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
```

5.5 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，后端云主机返回 HTTPS 的响应。默认强制以 HTTPS 访问网页。

⚠ 注意

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

目前，经典型负载均衡不支持此功能。

前提条件

- 已经创建 HTTPS 监听器
- 已经创建 HTTP 监听器

约束与限制

- 独享型负载均衡支持在添加 HTTP 监听器时添加重定向，且添加重定向后不支持修改或删除重定向，如果需要删除重定向，则需删除对应的 HTTP 监听器。
- 独享型负载均衡在 HTTP 监听器创建后不支持添加重定向。

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5-7 重定向参数配置


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，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”。

5.6 TLS 安全策略

操作场景

对于银行，金融类加密传输的应用，在创建和配置 HTTPS 监听器时，您可以选择使用安全策略，可以提高您的业务安全性。安全策略包含 TLS 协议版本和配套的加密算法套件。

目前经典型负载均衡不支持此功能，共享型负载均衡计划支持此功能。

添加安全策略


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，单击需要创建安全策略的监听器的负载均衡器名称。
5. 在该负载均衡界面的“监听器”区域，单击“添加监听器”。
6. 在“添加监听器”界面，前端协议选择“HTTPS”。
7. 在“添加监听器”界面，选择“高级配置 > 安全策略”。支持选择默认策略或自定义策略。，如果列表中无自定义策略，您可以选择创建自定义策略。配置参数如表 5-8 所示。

表5-8 默认安全策略参数说明

名称	说明	支持的 TLS 版本类型	使用的加密套件列表
TLS-1-0	支持 TLS 1.0、TLS 1.1、TLS 1.2 版本与相关加密套件，兼容性好，安全性低。	TLS 1.2 TLS 1.1 TLS 1.0	ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES128-GCM-SHA256
TLS-1-1	支持 TLS 1.1、TLS 1.2 版本与相关加密套件，兼容性较好，安全性中。	TLS 1.2 TLS 1.1	ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES128-GCM-SHA256

名称	说明	支持的 TLS 版本类型	使用的加密套件列表
TLS-1-2	支持 TLS 1.2 版本与相关加密套件，兼容性较好，安全性高。	TLS 1.2	AES128-GCM-SHA256 AES256-GCM-SHA384 ECDHE-ECDSA-AES128-SHA256 ECDHE-RSA-AES128-SHA256 AES128-SHA256 AES256-SHA256 ECDHE-ECDSA-AES256-SHA384 ECDHE-RSA-AES256-SHA384 ECDHE-ECDSA-AES128-SHA ECDHE-RSA-AES128-SHA ECDHE-RSA-AES256-SHA ECDHE-ECDSA-AES256-SHA AES128-SHA AES256-SHA

tls-1-0-inherit	支持 TLS1.0、TLS1.1、TLS1.2 版本与相关加密套件，兼容性好，安全性低。	TLS 1.2 TLS 1.1 TLS 1.0	ECDHE-RSA-AES256-GCM SHA384 <ul style="list-style-type: none"> ● ECDHE-RSA-AES128-GCM SHA256 ● ECDHE-ECDSA-AES256-GCM SHA384 ● ECDHE-ECDSA-AES128-GCM SHA256 ● AES128-GCM-SHA256 ● AES256-GCM-SHA384 ● ECDHE-ECDSA-AES128-SHA256 ● ECDHE-RSA-AES128-SHA256 ● AES128-SHA256 ● AES256-SHA256 ● ECDHE-ECDSA-AES256-SHA384 ● ECDHE-RSA-AES256-SHA384 ● ECDHE-ECDSA-AES128-SHA ● ECDHE-RSA-AES128-SHA ● DHE-RSA-AES128-SHA ● ECDHE-RSA-AES256-SHA ● ECDHE-ECDSA-AES256-SHA ● AES128-SHA ● AES256-SHA ● DHE-DSS-AES128-SHA ● CAMELLIA128-SHA ● EDH-RSA-DES-CBC3-SHA ● DES-CBC3-SHA ● ECDHE-RSA-RC4-SHA ● RC4-SHA ● DHE-RSA-AES256-SHA ● DHE-DSS-AES256-SHA ● DHE-RSA-CAMELLIA256-SHA
TLS-1-2-	支持 TLS 1.2 版本与相	TLS 1.2	ECDHE-RSA-AES256-GCM-

名称	说明	支持的 TLS 版本类型	使用的加密套件列表
Strict	关加密套件，兼容性一般，安全性高。		SHA384 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES128-GCM-SHA256 AES128-GCM-SHA256 AES256-GCM-SHA384 ECDHE-ECDSA-AES128-SHA256 ECDHE-RSA-AES128-SHA256 AES128-SHA256 AES256-SHA256 ECDHE-ECDSA-AES256-SHA384 ECDHE-RSA-AES256-SHA384

名称	说明	支持的 TLS 版本类型	使用的加密套件列表
TLS-1-0-WITH-1-3（独享型实例）	支持 TLS 1.0 及以上版本与相关加密套件，兼容性最好，安全性低。	TLS 1.3 TLS 1.2 TLS 1.1 TLS 1.0	ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES128-GCM-SHA256 AES128-GCM-SHA256 AES256-GCM-SHA384 ECDHE-ECDSA-AES128-SHA256 ECDHE-RSA-AES128-SHA256 AES128-SHA256 AES256-SHA256 ECDHE-ECDSA-AES256-SHA384 ECDHE-RSA-AES256-SHA384 ECDHE-ECDSA-AES128-SHA ECDHE-RSA-AES128-SHA ECDHE-RSA-AES256-SHA ECDHE-ECDSA-AES256-SHA AES128-SHA AES256-SHA TLS_AES_128_GCM_SHA256 TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256 TLS_AES_128_CCM_SHA256 TLS_AES_128_CCM_8_SHA256

名称	说明	支持的 TLS 版本类型	使用的加密套件列表
TLS-1-2-FS-WITH-1-3（独享型实例）	支持 TLS 1.2 及以上版本与前向安全相关的加密套件，兼容性较好，安全性最高。	TLS 1.3 TLS 1.2	ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES128-SHA256 ECDHE-RSA-AES128-SHA256 ECDHE-ECDSA-AES256-SHA384 ECDHE-RSA-AES256-SHA384 TLS_AES_128_GCM_SHA256 TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256 TLS_AES_128_CCM_SHA256 TLS_AES_128_CCM_8_SHA256
TLS-1-2-FS（独享型实例）	支持 TLS 1.2 版本与前向安全相关的加密套件，兼容性一般，安全性最高。	TLS 1.2	ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES128-SHA256 ECDHE-RSA-AES128-SHA256 ECDHE-ECDSA-AES256-SHA384 ECDHE-RSA-AES256-SHA384

名称	说明	支持的 TLS 版本类型	使用的加密套件列表
hybrid-policy-1-0	支持 TLS 1.1、TLS 1.2 版本 与相关 加密套件，兼容性较好，安全性中。	TLS 1.2 TLS 1.1	<ul style="list-style-type: none"> ● ECDHE-RSA-AES256-GCM SHA384 ● ECDHE-RSA-AES128-GCM SHA256 ● ECDHE-ECDSA-AES256-GCM SHA384 ● ECDHE-ECDSA-AES128-GCM SHA256 ● AES128-GCM-SHA256 ● AES256-GCM-SHA384 ● ECDHE-ECDSA-AES128-SHA256 ● ECDHE-RSA-AES128-SHA256 ● AES128-SHA256 ● AES256-SHA256 ● ECDHE-ECDSA-AES256-SHA384 ● ECDHE-RSA-AES256-SHA384 ● ECDHE-ECDSA-AES128-SHA ● ECDHE-RSA-AES128-SHA ● ECDHE-RSA-AES256-SHA ● ECDHE-ECDSA-AES256-SHA ● AES128-SHA ● AES256-SHA ● ECC-SM4-SM3 ● ECDHE-SM4-SM3

📖 说明

- 安全策略“tls-1-0-with-1-3”、“tls-1-2-fs-with-1-3”、“tls-1-2-fs”目前仅支持独享型实例。
- 目前，独享型负载均衡安全策略最高支持 TLS 1.3 协议，共享型负载均衡安全策略计划最高支持 TLS 1.2 协议。
- 上述列表为 ELB 支持的加密套件，同时客户端也支持多个加密套件，这样在实际使用时，加

密套件的选择范围为：ELB 和客户端支持的加密套件的交集，加密套件的选择顺序为：ELB 支持的加密套件顺序。

8. 配置完成，单击“确定”。

安全策略差异说明

表5-9 安全策略差异说明

安全策略	TLS-1-0	TLS-1-1	TLS-1-2	TLS-1-0-inherit	TLS-1-2-Strict	TLS-1-0-WITH-1-3	TLS-1-2-FS-WITH-1-3	TLS-1-2-FS	Hybrid-policy-1-0
TLS 协议									
Protocol-TLS 1.3	-	-	-	-	-	√	√	√	-
Protocol-TLS 1.2	√	√	√	√	√	√	√	√	√
Protocol-TLS 1.1	√	√	-	√	-	√	-	-	√
Protocol-TLS 1.0	√	-	-	√	-	√	-	-	-
加密套件									
EDHE-RSA-AES128-GCM-SHA256	√	√	√	-	√	-	-	-	-
ECDHE-RSA-AES256-GCM-SHA384	√	√	√	√	√	√	√	√	√
ECDHE-RSA-AES128-SHA256	√	√	√	√	√	√	√	√	√
ECDHE-RSA-AES256-SHA384	√	√	√	√	√	√	√	√	√
AES128-GCM-SHA256	√	√	√	√	√	√	-	-	√

AES256-GCM-SHA384	√	√	√	√	√	√	-	-	√
AES128-SHA256	√	√	√	√	√	√	-	-	√
AES256-SHA256	√	√	√	√	√	√	-	-	√
ECDHE-RSA-AES128-SHA	√	√	√	√	-	√	-	-	√
ECDHE-RSA-AES256-SHA	√	√	√	√	-	√	-	-	√
AES128-SHA	√	√	√	√	-	√	-	-	√
AES256-SHA	√	√	√	√	-	√	-	-	√
ECDHE-ECDSA-AES128-GCM-SHA256	√	√	√	√	√	√	√	√	√
ECDHE-ECDSA-AES128-SHA256	√	√	√	√	√	√	√	√	√
ECDHE-ECDSA-AES128-SHA	√	√	√	√	-	√	-	-	√
ECDHE-ECDSA-AES256-GCM-SHA384	√	√	√	√	√	√	√	√	√
ECDHE-ECDSA-AES256-SHA384	√	√	√	√	√	√	√	√	√
ECDHE-ECDSA-AES256-SHA	√	√	√	√	-	√	-	-	√

ECDHE-RSA-AES128-GCM-SHA256	-	-	-	√	-	√	√	√	√
TLS_AES_256_GCM_SHA384	-	-	-	-	-	√	√	√	-
TLS_CHACHA20_POLY1305_SHA256	-	-	-	-	-	√	√	√	-
TLS_AES_128_GCM_SHA256	-	-	-	-	-	√	√	√	-
TLS_AES_128_CCM_8_SHA256	-	-	-	-	-	√	√	√	-
TLS_AES_128_CCM_SHA256	-	-	-	-	-	√	√	√	-
DHE-RSA-AES128-SHA	-	-	-	√	-	-	-	-	-
DHE-DSS-AES128-SHA	-	-	-	√	-	-	-	-	-
CAMELLIA128-SHA	-	-	-	√	-	-	-	-	-
EDH-RSA-DES-CBC3-SHA	-	-	-	√	-	-	-	-	-
DES-CBC3-SHA	-	-	-	√	-	-	-	-	-
ECDHE-	-	-	-	√	-	-	-	-	-

RSA-RC4-SHA									
RC4-SHA	-	-	-	√	-	-	-	-	-
DHE-RSA-AES256-SHA	-	-	-	√	-	-	-	-	-
DHE-DSS-AES256-SHA	-	-	-	√	-	-	-	-	-
DHE-RSA-CAMELLIA256-SHA	-	-	-	√	-	-	-	-	-
ECC-SM4-SM3	-	-	-	-	-	-	-	-	√
ECDHE-SM4-SM3	-	-	-	-	-	-	-	-	√

修改安全策略



1. 登录管理控制台。
2. 在管理控制台左上角单击  图标，选择区域和项目。
3. 单击页面左上角的  ，选择“网络 > 弹性负载均衡”。
4. 单击页面左边的“TLS 安全策略”。
5. 在 TLS 安全策略页面，单击页面右上角的“创建自定义策略”。
6. 配置自定义策略参数，参数说明参见表 3-10。




表5-10 自定义策略参数说明

参数	说明	样例
名称	自定义策略名称	tls-test

参数	说明	样例
选择协议版本	自定义策略支持的 TLS 协议版本类型。支持选择多个协议版本。 包含： <ul style="list-style-type: none"> ● TLS 1.0 ● TLS 1.1 ● TLS 1.2 ● TLS 1.3 	-
选择加密算法套件	选择与协议版本配套的加密算法套件。支持选择多个加密算法套件。	-
描述	自定义策略相关信息的描述说明。	-

修改安全策略

修改安全策略时，后端云主机需要放通安全组，放开对 ELB 健康检查的限制（100.125IP 的限制，UDP 健康检查 icmp 报文的限制等），否则后端健康检查没上线，会影响业务。

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，单击需要修改安全策略的监听器的负载均衡器名称。
5. 切换至“监听器”界面：
 - 独享型负载均衡器，单击需要修改安全策略的监听器名称右侧  的按钮，选择“修改监听器”。
 - 共享型负载均衡器，单击需要修改安全策略的监听器名称右侧的  。
6. 在“修改监听器”界面，展开高级配置，选择安全策略参数。
7. 单击“确认”。

6 后端云主机

6.1 后端云主机介绍

负载均衡器会将客户端的请求转发给后端云主机处理。例如，您可以添加 ECS 实例作为负载均衡器的后端云主机，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主机组里的后端云主机。

新添加后端云主机后，若健康检查开启，负载均衡器会向后端云主机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云主机数量，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，绑定后端云主机实例，并且确保至少有一台后端云主机在正常运行。

在弹性负载均衡控制台，通过后端云主机 IP，或后端云主机 ID 可以查看这个服务器被哪些负载均衡器绑定。

关机或重启已有业务的后端云主机，会断开已经建立的连接，正在传输的流量会丢失。建议在客户端上面配置重试功能，避免业务数据丢失。

注意事项

绑定后端云主机时，请注意以下事项：

- 如果未开启跨 VPC 后端，请确保后端云主机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云主机，以便日后管理和维护。
- 您可以设置后端主机组内各后端云主机的转发权重。权重越高的后端云主机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云主机的访问量不均衡。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。

慢启动

开启慢启动后，负载均衡器向该模式下的后端云主机线性增加请求分配权重，当配置的慢启动持续时间期限结束后，负载均衡器向后端云主机正常发送完请求，并退出慢

启动模式。

使用慢启动功能时，请注意以下事项：

- 目前仅 HTTP 和 HTTPS 类型的后端主机组支持慢启动功能。
- 只对加权轮询算法生效。
- 只对于新增后端云主机开启慢启动，如果原来的主机组没有后端云主机，则新增的首个后端云主机慢启动也不生效。
- 在健康检查开启时，后端云主机在线后慢启动生效；如果慢启动过程中健康检查抖动，慢启动计时不会停止。
- 在健康检查关闭时，慢启动立即生效。
- 后端云主机的慢启动结束之后，不会再次进入慢启动模式。

跨 VPC 后端

跨 VPC 后端支持添加通过以 VPC 对等连接、云连接、VPN 连接与专线连接互通的后端云主机。

使用跨 VPC 后端功能时，请注意以下事项：

- 请前往负载均衡器基本信息页面开启跨 VPC 后端功能，否则该功能无法正常使用。
- 添加的跨 VPC 后端的 IP 地址只允许为 IPv4 类型的地址。
- 添加的跨 VPC 后端的 IP 地址不能为本 VPC 内的 IP 地址以及公网 IP 地址，否则请求不可达。若您要添加跨 VPC 后端，请正确配置路由，详情请参见 6.4 添加或删除后端云主机（独享型）。
- 若要使用跨 VPC 后端功能，请先正确配置 VPC 路由，确保后端可达。
- 只有 TCP，HTTP，HTTPS 类型监听器支持跨 VPC 后端功能。
- 请确保负载均衡器的后端子网有足够的 IP 地址（至少有 16 个可用 IP 地址），否则该功能无法正常使用。可以通过负载均衡器的“基本信息 > 后端子网”添加多个后端子网来增加后端子网的 IP 地址。
- 跨 VPC 后端的安全组规则必须放通负载均衡器的后端子网网段，否则会导后端业务流量与健康检查异常。
- 跨 VPC 后端功能开启后无法关闭。

6.2 后端云主机配置安全组（独享型）

操作场景

添加后端云主机之前首先要检查后端云主机所在安全组规则是否配置放行源网段为 VPC 网段，目的端口为后端云主机端口，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云主机执行健康检查。


首次创建后端云主机时，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云主机，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云主机进行通信，就需要配置安全组入方向的访问规则。

⚠ 注意

- 独享型负载均衡四层监听器未开启“跨 VPC 后端”功能时，后端云主机安全组规则和网络 ACL 规则均无需放通 ELB 所在的 VPC 网段。

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 > 弹性云主机”。
4. 在弹性云主机列表，单击待变更安全组规则的弹性云主机名称。
系统跳转至该弹性云主机详情页面。
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云主机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，端口和后端云主机端口一致。
为保证健康检查正常，安全组规则必须放通源网段为 ELB 关联的 VPC 子网网段，目的端口为后端云主机的健康检查端口，七层 ELB 还需放通目的端口为后端云主机的业务端口。
如果 UDP 监听器：
若配置了不同于后端云主机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，端口和后端云主机端口一致。
为保证健康检查正常，安全组规则必须放通源网段为 ELB 关联的 VPC 子网网段，目的端口为后端云主机的健康检查端口，七层 ELB 还需放通目的端口为后端云主机的业务端口。
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云主机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，或者会导致后端云主机异常。

您可以通过配置网络 ACL 入方向规则，放行源网段为 ELB 所在的 VPC 网段，目的端口为后端云主机端口。


⚠ 注意

- 独享型负载均衡四层监听器未开启“跨 VPC 后端”功能时，后端云主机安全组规则和网络 ACL 规则均无需放通 ELB 所在的 VPC 网段。
- 当独享型负载均衡实例与后端云主机在同一个子网时，网络 ACL 规则不起作用，此时健康检查是通的，且客户端也能访问到后端云主机。
- 当独享型负载均衡实例与后端云主机不在同一个子网时，网络 ACL 规则是生效的，此时健康检查不通，且客户端访问不到后端云主机。

📖 说明

负载均衡器的 IP 地址不受所在 VPC 子网 ACL 配置的限制，所以能够被客户端直接访问。建议您使用监听器的访问控制功能限制客户端访问负载均衡器。

详细请参考 4.5 访问控制策略。

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. 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，填写为 VPC 网段。
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”。

6.3 后端云主机配置安全组（共享型）

操作场景

由于 ELB 流量转到后端云主机以后，源 IP 会被转换为 100.125.0.0/16 的 IP，所以添加后端云主机之前首先要检查后端云主机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云主机执行健康检查。

首次创建后端云主机时，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云主机，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云主机进行通信，就需要配置安全组入方向的访问规则。

注意

- 独享型负载均衡四层监听器未开启“跨 VPC 后端”功能时，后端云主机安全组规则和网络 ACL 规则均无需放通 ELB 所在的 VPC 网段。

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 > 弹性云主机”。
4. 在弹性云主机列表，单击待变更安全组规则的弹性云主机名称。
系统跳转至该弹性云主机详情页面。
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云主机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，端口和后端云主机端口一致。
- 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云主机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，端口和后端云主机端口一致。
- 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

联的后端云主机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，或者会导致后端云主机异常。


您可以通过配置网络 ACL 入方向规则，放行 100.125.0.0/16 网段。

注意

- 独享型负载均衡四层监听器未开启“跨 VPC 后端”功能时，后端云主机安全组规则和网络 ACL 规则均无需放通 ELB 所在的 VPC 网段。

由于 ELB 会将访问后端云主机的公网 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 访问后端云主机。

说明：负载均衡器的 IP 地址不受所在 VPC 子网 ACL 配置的限制，所以能够被客户端直接访问。建议您使用监听器的访问控制功能限制客户端访问负载均衡器。详细请参考访问控制策略

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. 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”。

6.4 添加或移除后端云主机（独享型）

操作场景

在使用负载均衡服务时，确保至少有一台后端云主机在正常运行，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云主机处理需求。

移除负载均衡器绑定的后端云主机，后端云主机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，只是解除了后端云主机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主机组中。

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云主机中删除。

前提条件


若要使用跨 VPC 后端功能，请先正确配置 VPC 路由，确保后端可达。跨 VPC 后端支持添加通过以 VPC 对等连接、云连接、VPN 连接与专线连接互通的后端云主机。

约束与限制

使用跨 VPC 后端功能时，请注意以下事项：

- 请前往负载均衡器基本信息页面开启跨 VPC 后端功能，否则该功能无法正常使用。
- 添加的跨 VPC 后端的 IP 地址只允许为 IPv4 类型的地址。
- 添加的跨 VPC 后端的 IP 地址不能为本 VPC 内的 IP 地址以及公网 IP 地址，否则请求不可达。若您要添加跨 VPC 后端，请正确配置路由，详情请参见 6.4 添加或移除后端云主机（独享型）。
- 只有 TCP，HTTP，HTTPS 类型监听器支持跨 VPC 后端功能。
- 请确保负载均衡器的后端子网有足够的 IP 地址（至少有 16 个可用 IP 地址），否则该功能无法正常使用。可以通过负载均衡器的“基本信息 > 后端子网”添加多个后端子网来增加后端子网的 IP 地址。
- 跨 VPC 后端的安全组规则必须放通负载均衡器的后端子网网段，否则会导致后端业务流量与健康检查异常。
- 跨 VPC 后端功能开启后无法关闭。
- 跨 VPC 后端功能最多可以支持添加 492 个后端云主机。


添加后端云主机

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，单击需要添加后端云主机的负载均衡名称。
5. 切换到“后端主机组”页签，单击目标后端主机组名称。
6. 单击右侧页面中的“添加云主机”、“添加跨 VPC 后端”。
7. 根据需要添加的后端类型选择相应的操作。

添加普通后端：在“添加云主机”界面选择后端云主机所在的子网，勾选需要添加的后端云主机，并选择“私网 IP 地址”，然后单击下一步，设置后端端口和服务器的权重，单击“完成”，完成添加。

添加跨 VPC 后端：在“添加跨 VPC 后端”界面设置业务端口和服务器的权重等配置，单击“确定”，完成添加。

移除后端云主机

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，单击需要移除后端云主机的负载均衡名称。
5. 切换到“后端主机组”页签，单击需移除的服务器所在后端主机组的名称。
6. 在该后端主机组的基本信息页面，需移除单个后端云主机，可单击目标后端云主机操作列的“移除”；如需移除多个后端云主机，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“移除后端云主机”对话框中单击“是”。

添加后端主机组


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，单击需要添加后端主机组的负载均衡名称。
5. 切换到“后端主机组”页签，单击“添加后端主机组”。
6. 在弹出的“添加后端主机组”对话框中配置相关参数。
参数配置请参见表 6-1 和表 6-2。

表6-1 独享型负载均衡配置后端主机组参数说明

参数	说明	示例
名称	后端主机组名称。	server_group-sq4v
后端协议	云主机开通的协议。 支持选择 TCP、UDP、HTTP、HTTPS、QUIC 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> <p>加权轮询算法：根据后端云主机的权重，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。</p> <p>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重数的服务请求。</p> <p>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，同时对后端云主机进行编号，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。</p> <p>说明</p> <ul style="list-style-type: none"> • 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。 • 对于加权轮询算法和加权最少连接，当服务器的权重为“0”时，将不会被分发访问请求。 	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>说明</p> <p>当分配策略类型为“加权轮询算法”时，可配置会话保持。</p>	-
会话保持类型	<p>当会话保持开启后，需选择会话保持类型：</p> <p>源 IP 地址：基于源 IP 地址的简单会话保持，将请求的源 IP 地址作为散列键（HashKey），从静态分配的散列表中找出对应的服务器。即来自同一 IP 地址的访问请求会转发到同一台后端云主机上进行处理。</p> <p>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云主机处理。</p>	负载均衡器 cookie

参数	说明	示例
会话保持时间（分钟）	<p>当会话保持开启时，需添加会话保持时间。</p> <ul style="list-style-type: none"> ● 四层会话保持： <ul style="list-style-type: none"> - 默认时间：20 分钟； - 最长时间：1 小时 - 取值范围：1-60 分钟 ● 七层会话保持： <ul style="list-style-type: none"> - 默认时间：20 分钟； - 最长时间：24 小时 - 取值范围：1-1440 分钟 	20
慢启动	<p>慢启动默认关闭。</p> <p>当开启慢启动时，负载均衡器向该模式下的后端云主机线性增加请求分配权重，当配置的慢启动持续时间期限结束后，负载均衡器向后端云主机发送完整的请求比例，此后本次添加的后端云主机退出慢启动模式。详见 6.8 配置慢启动（独享型）。</p>	-
慢启动时间（秒）	<p>配置慢启动的时间。</p> <p>取值范围为 30~1200，默认为 30 秒。</p>	30
描述	<p>后端主机组的描述。</p> <p>字数范围：0/255。</p>	-



表6-2 独享型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	健康检查支持 HTTP、TCP、HTTPS 协议，设置后不可修改。	HTTP
域名	<p>健康检查的请求域名。</p> <p>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。</p> <p>只有健康检查协议为 HTTP 时，需要设置。</p>	www.elb.com



参数	说明	示例
端口	健康检端口号，取值范围[1, 65535]，为可选参数。 说明：未配置健康检查端口时，默认使用后端云主机端口进行健康检查。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		
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]。	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

- 单击“确定”。

修改后端主机组

- 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，单击需要修改的后端主机组的负载均衡名称。
- 切换到“后端主机组”页签，单击需要修改的后端主机组名称右侧的 。
- 修改参数，单击“确定”。

删除后端主机组

- 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，单击需要删除的后端主机组的负载均衡名称。
- 切换到“后端主机组”页签，单击需要删除的后端主机组名称右侧的 。
- 单击“是”。

6.5 添加或移除后端云主机（共享型）

操作场景

在使用负载均衡服务时，确保至少有一台后端云主机在正常运行，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云主机处理需求。


移除负载均衡器绑定的后端云主机，后端云主机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，只是解除了后端云主机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主机组中。

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云主机中删除。

说明

支持同 VPC 跨子网添加后端云主机。

添加后端云主机

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，单击需要添加后端云主机的负载均衡名称。
5. 切换到“后端主机组”页签，单击目标后端主机组名称。
6. 在目标后端主机组的基本信息页面，单击“添加”。选择后端云主机所在的子网，勾选需要添加的后端云主机，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云主机。
- 不支持通过虚拟 IP 添加后端云主机。

7. 设置业务端口和服务器的权重，单击“完成”。

说明

在“添加端口”处依次填写每台后端云主机的业务端口。

如果多台后端云主机的业务端口相同，可以在“批量添加端口”处批量填写业务端口并单击“完成”。

如果多台后端云主机的权重相同，可以批量设置服务器权重。

移除后端云主机

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，单击需要移除后端云主机的负载均衡名称。

5. 切换到“后端主机组”页签，单击需移除的服务器所在后端主机组的名称。
6. 在该后端主机组的基本信息页面，需移除单个后端云主机，可单击目标后端云主机操作列的“移除”；如需移除多个后端云主机，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“移除后端云主机”对话框中单击“是”。

添加后端主机组


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，单击需要添加后端主机组的负载均衡名称。
5. 切换到“后端主机组”页签，单击“添加后端主机组”。
6. 在弹出的“添加后端主机组”对话框中配置相关参数。
参数配置请参见表 6-3 和表 6-4。

表6-3 共享型负载均衡配置后端主机组参数说明

参数	说明	示例
名称	后端主机组名称。	server_group-sq4v
后端协议	云主机开通的协议。 支持选择 TCP、UDP、HTTP 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> <p>加权轮询算法：根据后端云主机的权重，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。</p> <p>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重数的服务请求。</p> <p>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，同时对后端云主机进行编号，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。</p> <p>说明</p> <ul style="list-style-type: none"> • 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。 • 对于加权轮询算法和加权最少连接，当服务器的权重为“0”时，将不会被分发访问请求。 	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>说明</p> <p>当分配策略类型为“加权轮询算法”时，可配置会话保持。</p>	-



参数	说明	示例
会话保持类型	<p>当会话保持开启后，需选择会话保持类型：</p> <p>源 IP 地址：基于源 IP 地址的简单会话保持，将请求的源 IP 地址作为散列键（HashKey），从静态分配的散列表中找出对应的服务器。即来自同一 IP 地址的访问请求会转发到同一台后端云主机上进行处理。</p> <p>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云主机处理。</p> <p>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云主机处理。</p> <p>说明</p> <ul style="list-style-type: none"> 四层会话保持（使用的是 TCP/UDP 协议）仅支持源 IP 地址类型。 七层会话保持（使用的是 HTTP/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类型来分配用户访问量，提升负载均衡能力。 	负载均衡器 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）	<p>当会话保持开启时，需添加会话保持时间。</p> <p>四层会话保持：</p> <p>默认时间：20 分钟；</p> <p>最长时间：1 小时</p> <p>取值范围：1-60 分钟</p> <p>七层会话保持：</p> <p>默认时间：20 分钟；</p> <p>最长时间：24 小时</p> <p>取值范围：1-1440 分钟</p> <p>说明</p> <p>当会话保持类型为“应用程序 cookie”时，不支持设置会话保持时间。</p>	20
描述	<p>后端主机组的描述。</p> <p>字数范围：0/255。</p>	-

表6-4 共享型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	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。 当前端协议选择 UDP, 健康检查协议默认为 UDP。	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。 说明: 未配置健康检查端口时, 默认使用后端云主机端口进行健康检查。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		
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]。	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

7. 单击“确定”。

修改后端主机组

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主机组的负载均衡名称。
5. 切换到“后端主机组”页签, 单击需要修改的后端主机组名称右侧的  。
6. 修改参数, 单击“确定”。

删除后端主机组

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主机组的负载均衡名称。
5. 切换到“后端主机组”页签，单击需要删除的后端主机组名称右侧的  。
6. 单击“是”。

6.6 配置混合负载均衡-跨 VPC 后端（独享型）

操作场景

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

- 在后端主机组中添加云上同 VPC 内的服务器，请参考 6.4 添加或移除后端云主机（独享型）。
- 跨 VPC 添加云上其他 VPC 中的服务器，需要先在 ELB 所在的 VPC 和云上其他 VPC 之间建立对等连接，然后通过跨 VPC 功能添加。建立对等连接详见《虚拟私有云用户指南》。
- 通过跨 VPC 功能添加云下数据中心的服务器，需要先通过云专线或 VPN 连通云上 ELB 所在的 VPC 和云下数据中心，详见《云专线用户指南》或《虚拟专用网络用户指南》。

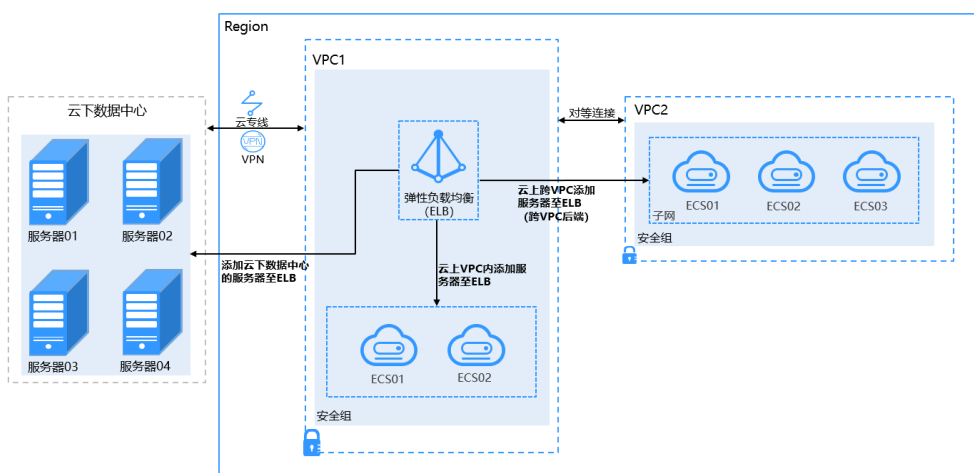


图6-1 ELB 支持添加云上、云下的服务器

前提条件

- 已创建独享型负载均衡。
- 已创建监听器。


- 已正确配置 VPC 路由，确保后端可达。跨 VPC 后端支持添加通过以 VPC 对等连接、云连接、VPN 连接与专线连接互通的后端云主机。

约束与限制


使用混合负载均衡功能时，请注意以下事项：

- 请前往负载均衡器基本信息页面开启跨 VPC 后端功能，否则该功能无法正常使用。
- 添加的跨 VPC 后端的 IP 地址只允许为 IPv4 类型的地址。只有 TCP，HTTP，HTTPS 类型监听器支持跨 VPC 后端功能。
- 请确保负载均衡器的后端子网有足够的 IP 地址（至少有 16 个可用 IP 地址），否则该功能无法正常使用。可以通过负载均衡器的“基本信息 > 后端子网”添加多个 后端子网来增加后端子网的 IP 地址。
- 跨 VPC 后端的安全组规则必须放通负载均衡器的后端子网网段，否则会导后端业务流量与健康检查异常。
- 跨 VPC 后端功能开启后无法关闭。
- 一个监听器最多支持添加 492 个后端云主机（包含普通后端云主机和跨 VPC 后端服务器）。

开启跨 VPC 后端

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，单击需要开启跨 VPC 后端功能的负载均衡名称。
5. 在“基本信息”页面，单击“开启跨 VPC 后端”。
6. 单击“确定”。

添加跨 VPC 后端

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，单击需要添加后端云主机的负载均衡名称。
5. 切换到“后端主机组”页签，单击目标后端主机组。
6. 单击右侧基本信息页的“跨 VPC 后端”。
7. 单击“添加跨 VPC 后端”，填写“跨 VPC 后端 IP”、“后端端口”和“权重”。

说明

请确保“跨 VPC 后端 IP”可达、“后端端口”为实际的后端业务端口，否则将会导致添加的后端云主机异常。


8. 单击“确定”。

6.7 后端云主机配置权重

每台后端云主机的权重取值范围为[0, 100]。新的请求不会转发到权重为 0 的后端云主机上，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，每台后端云主机的权重取值范围为[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云主机，且在轮询时，权重大的后端云主机被分配的概率高。
当后端云主机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，每台后端云主机的权重取值范围为[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 最小的后端云主机。
- 在源 IP 算法中，每台后端云主机的权重取值范围为[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，各个后端云主机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云主机上。

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，单击需要修改后端云主机权重的负载均衡名称。
5. 在该负载均衡界面，切换到“后端主机组”页签，在目标服务器所在行的操作列中，编辑“权重”列，设置权重值。
6. 单击“确定”。

用户可以根据需要批量设置后端云主机权重。具体操作如下

1. 重复步骤 1 至步骤 7 的操作。
2. 在该负载均衡界面，切换到“后端主机组”页签，勾选需要设置权重的后端云主机，单击“修改权重”。
3. 在“修改权重”弹窗中，在输入框中输入权重值，单击输入框右侧的“确定”。或者根据需要在后端云主机列表中分别设置权重值。
4. 单击弹窗下方的“确定”，完成批量设置。

说明将后端云主机的权重值批量设置为“0”，可以实现批量屏蔽后端云主机。

6.8 配置慢启动（独享型）

操作场景

弹性负载均衡支持七层（HTTP/HTTPS）后端协议开启慢启动功能，在设置的慢启动时间内线性增加请求分配权重，达到请求数线性增加的目的。当慢启动时间结束后，负载均衡向后端云主机发送完整比例的流量请求。慢启动能够实现业务的平滑启动，完美避免业务抖动问题。当弹性负载均衡器检测到开启慢启动的后端主机组内的某台后端云主机状态为正常时，这台后端云主机会进入慢启动状态。

后端云主机在以下两种状态会退出慢启动状态。


- 到达已设定的慢启动时间。
- 慢启动时间内后端云主机变为异常。

变为异常而退出慢启动的后端云主机再次加入时，如果检测正常会重新进入到慢启动状态。


前提条件

- 已创建独享型负载均衡。
- 已创建七层（HTTP/HTTPS）监听器。

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，单击需要添加后端云主机的负载均衡名称。
5. 切换到“后端主机组”页签，单击“添加后端主机组”。
6. 在“添加后端主机组”页面，打开“慢启动”开关、并配置慢启动时间，其他参数请根据实际业务诉求填写。
7. 单击“确定”。

相关操作

- 已经创建的后端主机组可以在“后端主机组”页签，单击已创建“后端主机组”右侧的  ，开启慢启动功能。
- 新添加的后端主机组，还需要添加后端云主机，具体操作请参考 6.4 添加或移除后端云主机（独享型）。

7 健康检查

7.1 健康检查介绍

负载均衡器会定期向后端云主机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云主机是否可用。负载均衡器如果判断后端云主机健康检查异常，就不会将流量分发到异常后端云主机，而是分发到健康检查正常的后端云主机，从而提高了业务的可靠性。当异常的后端云主机恢复正常运行后，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。

如果您的业务对负载比较敏感，过于频繁的健康检查报文可能会对您的正常业务产生影响。您可以根据实际的业务情况，通过增大健康检查间隔，或者将七层健康检查改为四层健康检查等方式来降低对业务的影响。如果您的业务系统自身有健康检查机制，也可以关闭负载均衡器的健康检查，但是为了保障业务的持续可用，不建议这样做。

前提条件

对于四层监听器，健康检查适用的版本是 HTTP 1.1；对于七层监听器，共享型负载均衡健康检查适用的版本是 HTTP 1.1，独享型适用 HTTP 1.0。

TCP 健康检查

对于四层（TCP）和七层（HTTP/HTTPS）监听器，您可以配置 TCP 健康检查，通过发起 TCP 三次握手来获取后端云主机的状态信息，如 0 所示。

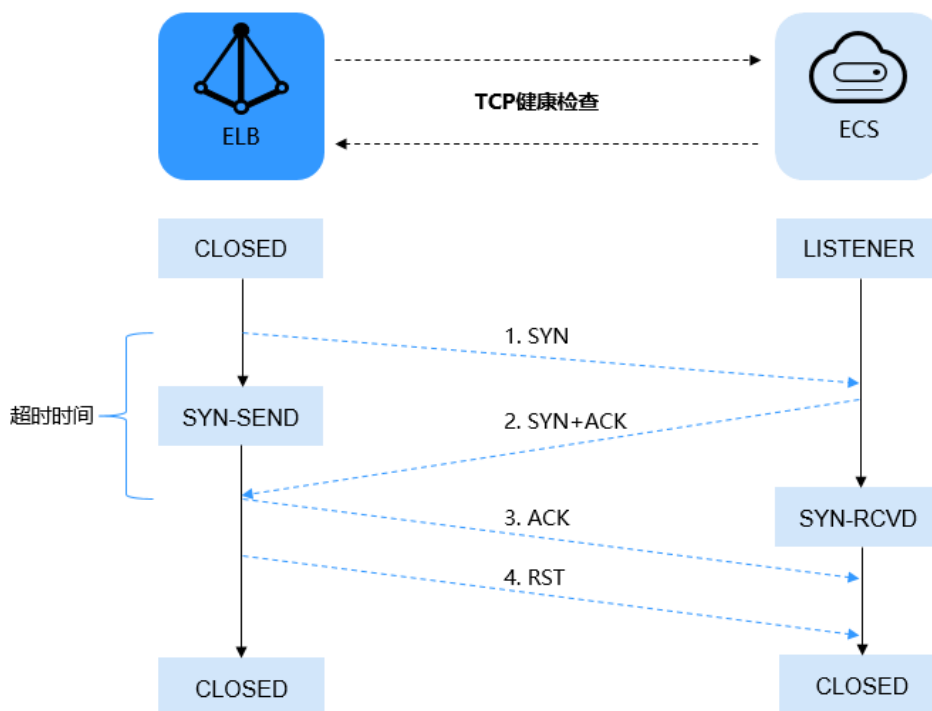


图7-1 TCP 健康检查

TCP 健康检查的机制如下：

1. ELB 节点根据健康检查配置，向后端云主机（IP+健康检查端口）发送 TCP SYN 报文。
2. 后端云主机收到请求报文后，如果相应的端口已经被正常监听，则会返回 SYN+ACK 报文。

如果在超时时间内没有收到后端云主机的 SYN+ACK 报文，则判定健康检查失败。然后发送 RST 报文给后端云主机中断 TCP 连接。

如果在超时时间内收到了 SYN+ACK 报文，则发送 ACK 给后端云主机，判定健康检查成功，并发送 RST 报文给后端云主机中断 TCP 连接。

须知

正常的 TCP 三次握手后，会进行数据传输，但是在健康检查时会发送 RST 中断建立的 TCP 连接。该实现方式可能会导致后端云主机中的应用认为 TCP 连接异常退出，并打印错误信息，如“Connection reset by peer”。解决方案如下：

- 采用 HTTP 方式进行健康检查。
- 后端云主机忽略健康检查的连接错误。

UDP 健康检查

对于四层（UDP）监听器，默认配置 UDP 健康检查，通过发送 UDP 探测报文获取后端云主机的状态信息，如 0 所示。

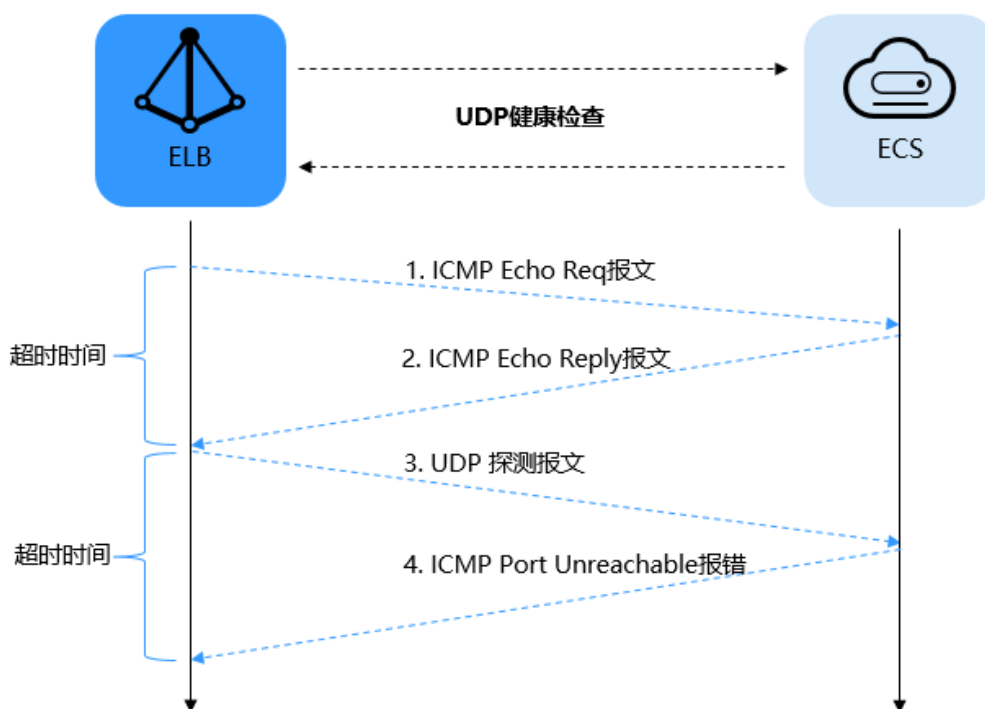


图7-2 UDP 健康检查

UDP 健康检查机制如下：

1. 四层 ELB 节点根据健康检查配置，向后端云主机发送 ICMP Echo Request 报文。如果在超时时间内没有收到 ICMP Echo Reply 报文，则判定健康检查失败。如果在超时时间内收到了 ICMP Echo Reply 报文，则向后端云主机发送 UDP 探测报文。
2. 如果在超时时间内没有收到后端云主机返回的 ICMP Port Unreachable 报文，则判定健康检查成功。否则，判定健康检查失败。

HTTP 健康检查

对于四层（TCP）和七层（HTTP/HTTPS）监听器，您可以配置 HTTP 健康检查，通过 HTTP GET 请求来获取状态信息。对于 HTTPS 监听器，由于负载均衡器对 TLS 协议进行了卸载，负载均衡器与后端云主机之间使用 HTTP 传输，健康检查也采用 HTTP 方式，以提高系统的性能。健康原理如 0 所示。

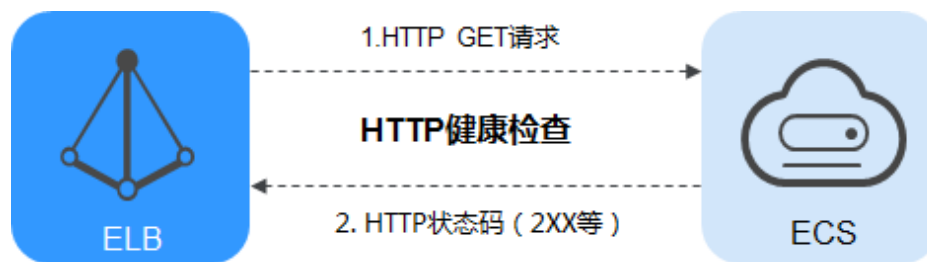


图7-3 HTTP 健康检查

具体机制如下：

1. 七层 ELB 节点根据健康检查配置，向后端云主机（IP+端口+检查路径）发出 HTTP GET 请求（可以选择设置域名）。
2. 后端云主机收到请求后，根据服务的情况返回相应的 HTTP 状态码。

如果七层 ELB 节点在响应超时时间内收到了后端云主机的响应，将 HTTP 状态码与预置的状态码进行对比，如果匹配则认为健康检查成功，后端云主机运行正常。

如果七层 ELB 节点在响应超时时间内没有收到后端云主机的响应，则判定健康检查失败。

健康检查时间窗

健康检查机制的引入，有效提高了业务服务的可用性。但是，为了避免频繁的健康检查失败引起的切换对系统可用性的冲击，健康检查只有连续多次检查成功或失败后，才会进行状态切换。

以共享型负载均衡的健康检查为例，健康检查时间窗由以下三个因素决定：

健康检查时间窗由以下三个因素决定：

- 检查间隔：每隔多久进行一次健康检查。
- 超时时间：等待服务器返回健康检查的时间。
- 最大重试次数：健康检查连续成功的次数。

系统必须连续 3 次检查失败，才会判定后端云主机健康检查失败，与“最大重试次数”设置的数值无关。

健康检查时间窗的计算方法如下：

- 健康检查成功时间窗 = 超时时间 × 最大重试次数 + 检查间隔 × (最大重试次数 - 1)
- 健康检查失败时间窗 = 超时时间 × 3 + 检查间隔 × (3 - 1)

如 0 所示：

- 检查间隔：4s
- 超时时间：2s

健康检查检测到后端云主机从正常到失败状态，健康检查失败时间窗 = 超时时间 × 3 + 检查间隔 × (3 - 1) = 2 × 3 + 4 × (3 - 1) = 14s。

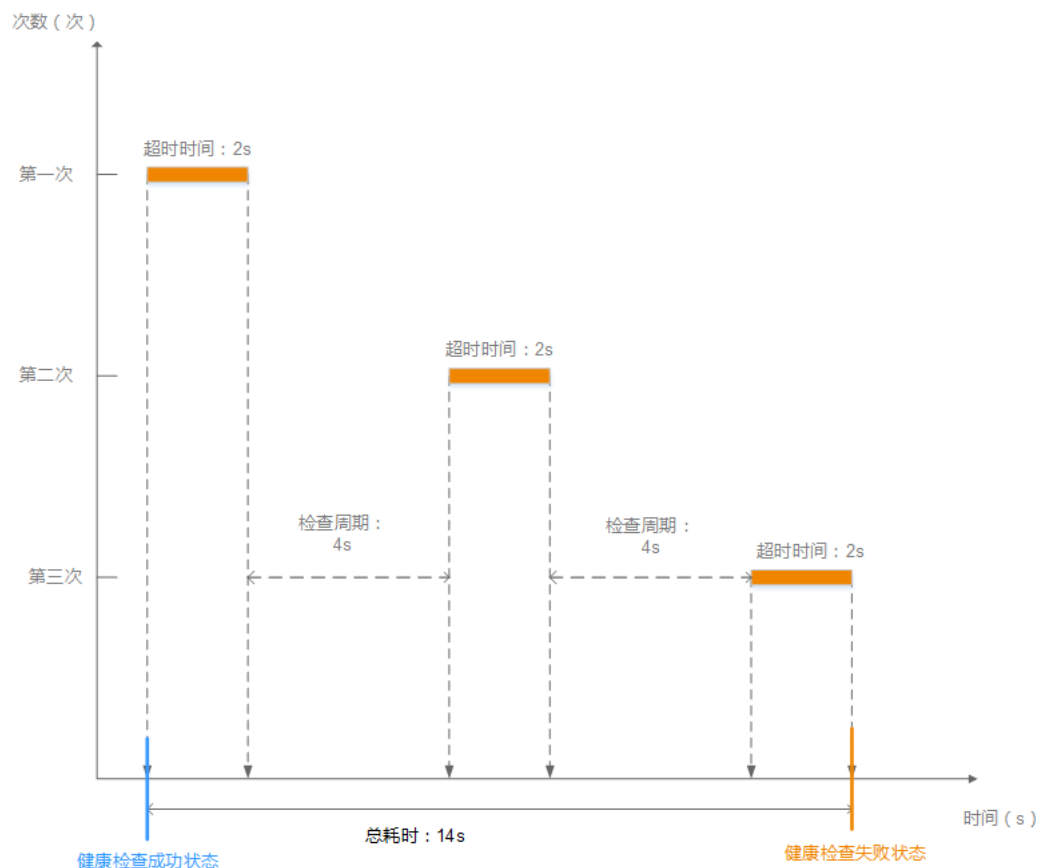


图7-4 健康检查失败时间窗

健康检查异常排查

如果您的健康检查异常，排查方法请参考 12.6.1 健康检查异常如何排查？。

7.2 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。

如果需要变更经典型的健康检查配置，可以在需要修改的监听器所在行，单击“修改”，修改相应参数。

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。
- 为了减少后端云主机的 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。

- 开启健康检查后不会影响已建立连接的流量转发，负载均衡会立即对后端云主机执行健康检查。如果健康检查正常，则新建连接的流量会根据分配策略和权重向该服务器转发流量；如果健康异常，则系统会设置该服务器状态为异常，不转发新的流量到该服务器。建议挑选无业务时间段执行此操作。

配置独享型负载均衡健康检查


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，单击需要开启健康检查的负载均衡名称。
5. 在“后端主机组”页签下，选择需要开启健康检查的后端主机组名称。
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，可根据需要开启健康检查。参考表 7-1 进行配置。

表7-1 独享型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	健康检查支持 TCP、HTTP、HTTPS 方式，设置后不可修改。 当前端协议选择 UDP，健康检查协议默认为 UDP。	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。 说明：未配置健康检查端口时，默认使用后端云主机端口进行健康检查。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		
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]。	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

参数	说明	示例
最大重试次数	健康检查最大的重试次数，取值范围[1-10]。	3
HTTP 状态码	自定义健康检查返回的状态码。当“协议”为 HTTP 或 HTTPS 时生效。 可输入 200-599 范围内不重复的单个数字或正序的数字区间。多个 HTTP 状态码使用逗号隔开，最多支持 5 个。 说明：如果您要使用该特性，请进入至 ELB 服务控制台后，单击页面左下角的“体验新版”。目前新版控制台在公测中，待公测结束后即可正常使用。	200

- 单击“完成”。

配置共享型负载均衡健康检查


- 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“后端主机组”页签下，选择需要开启健康检查的后端主机组名称。
- 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 7-2 进行配置。

表7-2 共享型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	健康检查支持 TCP 和 HTTP 方式，设置后不可修改。 当前端协议选择 UDP，健康检查协议默认为 UDP。	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

参数	说明	示例
端口	健康检查端口号，取值范围[1, 65535]，为可选参数。 说明：未配置健康检查端口时，默认使用后端云主机端口进行健康检查。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		
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]。	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

- 单击“完成”。


7.3 修改健康检查协议

操作场景

当您需要更换健康检查协议时，请参考本章完成操作。切换协议之后，负载均衡会根据新的健康检查协议重新检查后端云主机。

健康检查通过后，负载均衡向后端继续转发流量。健康检查切换周期内，客户端可能收到 503 错误码。

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，单击需要修改健康检查的负载均衡名称。
- 在“后端主机组”页签下，选择需要修改健康检查的后端主机组名称。
- 在基本信息页面，单击“健康检查”右侧的“配置”。
- 修改健康检查的“协议”。
- 单击“确定”。

7.4 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主机组时，不开启健康检查开关。对于已经创建健康检查的后端主机组，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，后端云主机将不再收到健康检查报文，此时监听器认为后端云主机处于健康状态。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云主机上，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。

经典型负载均衡不支持关闭健康检查，以下操作步骤以共享型负载均衡为例。

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“后端主机组”页签下，选择需要关闭健康检查的后端主机组名称。
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”。

8 证书管理

8.1 证书简介

负载均衡器支持两种类型的证书，服务器证书、CA 证书。配置 HTTPS 监听器时，需要为监听器绑定服务器证书，如果开启双向认证功能，还需要绑定 CA 证书。

- 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。

使用证书的注意事项

- 同一个证书在负载均衡器上只需上传一次，可以使用在多个负载均衡器实例中。
- 默认情况下，一个监听器每种类型的证书只能绑定一个，但是一个证书可以被多个监听器绑定。
- 负载均衡器只支持原始证书，不支持对证书进行加密。
- 共享型负载均衡器和后端云主机不能同时使用证书，如果后端云主机使用了证书，那么对应的监听器就不能使用 HTTPS 协议，可以使用 TCP 监听器将 HTTPS 流量透传到后端云主机。独享型负载均衡不存在此限制。
- 可以使用自签名的证书，使用自签名证书和第三方机构颁发的证书对负载均衡器无区别，但是使用自签名证书会存在安全隐患，建议客户使用权威机构颁发的证书。
- 负载均衡器只支持 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。
- 目前 ELB 不支持对证书有效期等进行检查。
- ELB 不会自动选择未过期的证书，如果您有证书过期了，需要手动更换或者删除证书。

8.2 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
```

8.3 创建/修改/删除证书

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，您可以创建证书、修改证书、删除证书。

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

- 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。

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。

企业项目

证书内容：证书内容必须为 PEM 格式。当证书类型为“服务器证书”和“CA 证书”时，需要填写。

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。

证书内容格式如下：

```
-----BEGIN CERTIFICATE-----
Base64-encoded certificate
-----END CERTIFICATE-----
```

私钥：当证书类型为“服务器证书”时，需要填写。

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，则需要配置从子证书到根证书的所有证书内容，且证书内容的配置顺序需要为：子证书（服务器证书） > 中间证书 > 根证书。从权威机构颁发的证书，有可能根证书已经预置到服务器内，所以签发证书不包含根证书。此时直接按照“子证书（服务器证书） > 中间证书”完成配置。

例如，某机构拿到的证书包含 2 个证书文件：子证书（服务器证书）文件 **server.cer**、中间证书文件 **mid.crt** 和 1 个私钥文件 **private.key**。那么需要在“证书内容”输入框中粘贴 **server.cer** 内容、然后回车继续粘贴 **mid.crt** 的内容，并且在“私钥”输入框中粘贴 **private.key** 的内容，才能使整个证书链生效。证书链内容格式如下：

证书内容：

```
-----BEGIN CERTIFICATE-----
子证书（服务器证书）文件 server.cer 内容
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
中间证书文件 mid.crt 内容
-----END CERTIFICATE-----
```

私钥：

```
-----BEGIN PRIVATE KEY-----
私钥文件 private.key 内容
```

```
-----END PRIVATE KEY-----
```


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”。

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。

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“是”，完成删除。

8.4 绑定/更换证书

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，您可以参考本章节绑定证书。如果弹性负载均衡实例使用的证书过期或者其它原因需要更换，您可以参考本章节更换证书。

如果还有其他的服务也使用了待更换的证书，例如 Web 应用防火墙服务。请在所有服务上完成更换证书的操作，以免证书更换不全面而导致业务不可用。

说明

弹性负载均衡的证书和私钥的更换对业务没有影响。




前提条件

已经在弹性负载均衡的“证书管理”页面创建待更换的新证书，如果还未创建，请先[创建证书](#)。

绑定证书

通过添加 HTTPS 监听器来绑定证书。详见 4.9 添加 HTTPS 监听器。

更换证书


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，单击需要修改 HTTPS 监听器的负载均衡名称。
5. 切换到“监听器”页签：
经典型负载均衡器，在需要修改的 HTTPS 监听器所在行，单击“修改”。
共享型负载均衡器，单击需要修改的 HTTPS 监听器名称右侧的 。
独享型负载均衡器，单击需要修改的 HTTPS 监听器名称右侧的  按钮，选择“修改监听器”。
6. “服务器证书”选择需要更换的证书，单击“下一步”。
7. 在“配置后端主机组”对话框中，单击右下角的“完成”。

8.5 快速查询证书所关联的监听器

操作场景

您需要快速查询证书所关联的监听器，方便定位相关配置信息。

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. 在左侧导航栏单击“证书管理”。
5. 在证书列表中，在“监听器（前端协议/端口）”所在列，单击监听器名称，即可查看监听器详细信息。
当关联监听器数量大于 5 个，在“监听器（前端协议/端口）”所在列，单击“查看所有”，单击监听器名称，即可查看监听器详细信息。

9 标签管理


操作场景

对于拥有大量云资源的用户，可以通过给云资源打标签，快速查找具有某标签的云资源，可对这些资源标签统一进行检视、修改、删除等操作，方便用户对云资源的管理。

目前经典型负载均衡不支持此功能。

为负载均衡器添加标签

给负载均衡器添加标签有以下两种方法。

- 在创建负载均衡器的时候，输入标签的“键”和“值”。
操作步骤和配置参数，请参见创建独享型负载均衡器和创建共享型负载均衡器。
- 给已创建的负载均衡器添加标签。
 - 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 > 网络 > 弹性负载均衡”。
 - d. 在“负载均衡器”界面，单击已创建的负载均衡器名称。
 - e. 在“标签”页签下，单击“添加标签”，输入“键”和“值”。
 - f. 确认正确，单击“确认”。

说明

- 一个负载均衡器最多可以增加 10 个标签。
- 标签的“键”和“值”是一一对应的，其中“键”值是唯一的。

为监听器添加标签

给已创建的监听器添加标签的方法如下：


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，单击已创建的负载均衡器名称。
5. 切换到监听器页签，单击需要添加标签的监听器名称。
6. 切换到监听器子页面的标签页签，单击“添加标签”，输入“键”和“值”。
7. 确认正确，单击“确认”。

说明

- 一个监听器最多可以增加 10 个标签。
- 标签的“键”和“值”是一一对应的，其中“键”值是唯一的。

修改标签

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，单击需要修改标签的负载均衡器名称。
5. 在“标签”页签下，在需要修改的标签所在行，单击“编辑”，输入修改的“值”。


说明

“键”值不支持修改。

6. 确认正确，单击“确认”。

以上步骤描述的是修改负载均衡器的标签，修改监听器的标签可参考上面步骤进行，仅操作入口不同。

删除标签

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，单击需要删除标签的负载均衡器名称。
5. 在“标签”页签下，在需要删除的标签所在行，单击“删除”。
6. 确认正确，单击“确认”。

以上步骤描述的是删除负载均衡器的标签，删除监听器的标签可参考上面步骤进行，仅操作入口不同。

9.1 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。

服务器证书、CA 证书的“证书内容”格式均需按以下要求。

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-----
MIIDIJCCAougAwIBAgIJALV96mEtVF4EMA0GCSqGSIb3DQEgBBQUAMGoxCzAJBgNV
BAYTAnh4MQswCQYDVQQIEwJ4eDELMAkGA1UEBxMCeHgxGzAJBgNVBAAoTAnh4MQsw
CQYDVQQLEwJ4eDELMAkGA1UEAxMCEHgxGzAJBgNVBAGTAh4MQswCQYDVQQHEwJ4e
DELMAkGA1UEChMCeHgxGzAJBgNVBAsTAh4MQswCQYDVQDEwJ4eDEAMBGGCSqGSIb3
DQEFJARYLeHh4QDE2My5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMU832i
m+d3FILgTWmpZBUoYcIWVcAAAYE7FsZ9LNerOyjJpyi256oypdBvGs9JAUBN5WaFk81U
Qx29wAyNixX+bKa0DBWpUDqr84V1f9vdQc75v9WoujcnlKszzpV6qePPC7igJJpu4Q
OI362BrWzJCYQbg4Uzo1KYBhLFx10TovAgMBAAGjgc8wgcwHQYDVR0OBBYEFMbTvDy
vE2KsRy9zPq/JWOjovg+WMIGcBGNVHSMegZQwgZGAFMbTvDyvE2KsRy9zPq/JWO
jovg+WoW6kbDBQMqswCQYDVQQGEwJ4eDELMAkGA1UECBMCeHgxGzAJBgNVBACTAh
4MQswCQYDVQQKAwJ4eDELMAkGA1UECWMCAh4MQswCQYDVQQDQwEwJ4eDELMAkGA1
UEBxMCeHgxGzAJBgNVBAMTAh4MRowGAYJKoZIhvcNAQkBFgt4eHhAMTYzLmNvbYI
JALV96mEtVF4EMAwGA1UdEwQFMAMBaf8wDQYJKoZIhvcNAQEFBQADgYEAAASk/1i
wiALa2RU3YCxqZFEESZvQxiKrDkDbFeoa6Tk49Fnb1f7FCW6PTtY3HPWl5ygsMs
Sy0Fi3xp3jmuIwzJhcQ3tcK5gC99HWP6Kw37RL8WoB8GWFU04tHLOjBIxkZROP
Rh+zMIrquUxv6fsb3NWKhnlfh1Mj5wQE4Ldo=
-----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
AoGBAJvLzJCyIsCJcKHWL6onbSUTdtyFwPViD1QrVAtQYabF14g8CGUZG/9fgheu
TXPtTDcvu7cZdUArvgYW3I9F9IBb2lmF3a44xfiAKdDhzr4DK/vQhvHPuuTeZA41
r2zp8Cu+Bp40pSxmoAOK3B0/peZAka01Ju7c7ZChDWrXleHZAkEA/6dcaWHotfGS
eW5YLbSms3f0m0GH38nRl7oxyCW6yMIDkFHURVMBKW1OhrCuGo8u0nTmi5IH9gRg
5bH8XcuJlQJBAMWBQgzCHyoSeryD3TF1eXIFzgDBw6Ve5hyMjUtjvgdVKoxRPvpO
kc1c39QHP6Dm2wrXXHEej+9RILxBZCVQNbMCQQC42i+Ut0nHvPuXN/UkXzomDHde
h1ySsOAO4H+8Y6OSI8713HUrByCQ7stX1z3L0HofjHqV9Koy9emGTFLZEzSdAkB7
Ei6cUKKmtkYe3rr+RcATEmwAw3tEJOHmrW5ErApVZKr2TzLMQZ7WZpIPzQRCYnY
2ZZLDuZWFFG3vW+wKKktAkAaQ5GNzbwRlpXF1FZFuNF7erxypzstbUmU/31b7tS
i5LmxTGKL/xRYtZEHjya4Ikkkg40q1MrUsgIYbFYmf2
-----END RSA PRIVATE KEY-----
```

10 IP 地址组（黑名单/白名单）

操作场景

对于需要使用**黑名单**和**白名单**，进行 4.5 访问控制策略的用户，开启白名单或黑名单时必须选择一个 IP 地址组，从而实现允许或者限制 IP 地址组中的 IP 访问负载均衡的监听器。

同一个 IP 地址组，最多可以关联 50 个监听器。目前 IP 地址组既支持 IPv4 地址又支持 IPv6 地址。

创建 IP 地址组


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“IP 地址组”界面，单击“创建 IP 地址组”。
5. 配置 IP 地址组参数，参数说明参见表 10-1。

表10-1 IP 地址组参数说明

参数	说明	样例
名称	IP 地址组的名称。	ipGroup-01
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。详见《企业管理用户指南》。	-

参数	说明	样例
IP 地址	<p>需要通过白名单或黑名单进行访问控制的 IP 地址。</p> <p>每行一个 IP 地址或一个网段，以回车结束；</p> <p>每个 IP 地址或者网段都可以用“ ”分隔添加备注，如“192.168.10.10 ECS01”，备注长度范围是 0 到 255 字符，不能包含<>；</p> <p>每个 IP 地址组最多可添加 300 个 IP 地址和网段。</p> <p>说明</p> <p>如果 IP 地址组未包含任何 IP 地址，当访问控制选择白名单时，则对应的负载均衡监听器禁止任何 IP 地址访问。</p>	10.168.2.24 10.168.16.0/24
描述	IP 地址组相关信息的描述说明。	-

6. 确认参数配置，单击“确定”。

修改 IP 地址组


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“IP 地址组”界面，需要修改的 IP 地址组所在行，单击“修改”。
5. 修改 IP 地址组参数，参数说明参见表 10-2。

表10-2 IP 地址组参数说明


参数	说明	样例
名称	IP 地址组的名称。	ipGroup-01
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。详见《企业管理用户指南》。	-

参数	说明	样例
IP 地址	<p>需要通过白名单或黑名单进行访问控制的 IP 地址。</p> <p>每行一个 IP 地址或一个网段，以回车结束；</p> <p>每个 IP 地址或者网段都可以用“ ”分隔添加备注，如“192.168.10.10 ECS01”，备注长度范围是 0 到 255 字符，不能包含<>；</p> <p>每个 IP 地址组最多可添加 300 个 IP 地址和网段。</p> <p>说明</p> <p>如果 IP 地址组未包含任何 IP 地址，当访问控制选择白名单时，则对应的负载均衡监听器禁止任何 IP 地址访问。</p>	10.168.2.24 10.168.16.0/24
描述	IP 地址组相关信息的描述说明。	-

6. 确认参数配置，单击“确定”。

删除 IP 地址组

如果 IP 地址组已经关联了监听器，则不允许删除。

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“IP 地址组”界面，需要删除的 IP 地址组所在行，单击“删除”。
5. 确认需要删除的 IP 地址组，单击“是”。

11 监控

11.1 监控指标说明

功能说明

本节定义了弹性负载均衡服务计划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。您目前或将来可以在云监控服务控制台查看弹性负载均衡服务上报的监控指标以及产生告警信息，详见 11.3 查看监控指标。

命名空间

SYS.ELB

监控指标

表11-1 ELB 支持的监控指标

指标 ID	指标名称	指标含义	取值范围	测量对象	监控周期 (原始指标)
m1_cps	并发连接数	<p>在四层负载均衡器中，指从测量对象到后端云主机建立的所有 TCP 和 UDP 连接的数量。</p> <p>在七层负载均衡器中，指从客户端到 ELB 建立的所有 TCP</p>	≥ 0 个	<p>独享型负载均衡器</p> <p>共享型负载均衡器</p> <p>独享型负载均衡监听器</p> <p>共享型负载均衡监听器</p>	1 分钟

		连接的数量。 单位：个			
m2_act_conn	活跃连接数	从测量对象到后端云主机建立的所有 ESTABLISHED 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	≥ 0 个		
m3_inact_conn	非活跃连接数	从测量对象到所有后端云主机建立的所有除 ESTABLISHED 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	≥ 0 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	≥ 0 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。	≥ 0 个/秒		

		单位：个/秒			
m6_out_pps	流出数据包数	测量对象每秒发出的数据包个数。 单位：个/秒	≥ 0 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	≥ 0 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	≥ 0 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	≥ 0 个	独享型负载均衡器 共享型负载均衡器	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	≥ 0 个	独享型负载均衡器后端服务组 共享型负载均衡器后端服务组	
m1e_server_rps	后端云主机重置数量	TCP 监听器专属指标。后端云主机每秒通过测量对象发给客户端的重置 (RST) 数据包数。 单位：个/秒	≥ 0 个/秒	共享型负载均衡器 共享型负载均衡器监听器	1 分钟
m21_client_rps	客户端重置数量	TCP 监听器专属指标。客户端每秒通过测量对象发送给后端云主机的	≥ 0 个/秒		

		重置 (RST) 数据包数。 单位: 个/秒			
m1f_lvs_rps	负载均衡器重置数量	TCP 监听器专属指标。测量对象每秒生成的重置 (RST) 数据包数。 单位: 个/秒	≥ 0 个/秒		
m22_in_bandwidth	入网带宽	从外部访问测量对象所消耗的宽。 单位: 比特/秒	≥ 0 bit/s		
m23_out_bandwidth	出网带宽	测量对象访问外部所消耗的带宽。 单位: 比特/秒	≥ 0 bit/s		
mb_17_queries	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。	≥ 0 个/秒	独享型负载均衡器 共享型负载均衡器 独享型负载均衡器监听器 共享型负载均衡器监听器 独享型负载均衡器后端服务组 共享型负载均衡器后端服务组	1 分钟
md_17_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	≥ 0 个/秒	独享型负载均衡器 共享型负载均衡器 独享型负载均衡器监听器	1 分钟

		听器才有此指标) 单位: 个/秒。		共享型负载均衡监听器	
mc_17_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。	≥ 0 个/秒	独享型负载均衡器 共享型负载均衡器 独享型负载均衡监听器 共享型负载均衡监听器	1分钟
me_17_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。	≥ 0 个/秒		
mf_17_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。	≥ 0 个/秒		
m10_17_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	≥ 0 个/秒		

		HTTPS 监听器 才有此指标) 单位: 个/秒。			
m11_17_h ttp_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。	≥0 个/秒		
m12_17_h ttp_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。	≥0 个/秒		
m13_17_h ttp_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。	≥0 个/秒		
m14_17_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	≥0 个/秒		

		<p>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。</p> <p>单位：毫秒。</p>			
m15_17_upstream_4xx	7层后端返回码(4XX)	<p>统计测量对象当前7层后端4XX系列状态响应码的数量。</p> <p>(HTTP和HTTPS监听器才有此指标)</p> <p>单位：个/秒。</p>	≥0个/秒	<p>独享型负载均衡器</p> <p>共享型负载均衡器</p> <p>独享型负载均衡监听器</p> <p>共享型负载均衡监听器</p>	1分钟
m16_17_upstream_5xx	7层后端返回码(5XX)	<p>统计测量对象当前7层后端5XX系列状态响应码的数量。</p> <p>(HTTP和HTTPS监听器才有此指标)</p> <p>单位：个/秒。</p>	≥0个/秒	<p>独享型负载均衡后端主机组</p> <p>共享型负载均衡后端主机组</p>	1分钟
m17_17_upstream_rt	7层后端的RT平均值	<p>统计测量对象当前7层后端平均响应时间。</p> <p>(HTTP和HTTPS监听器才有此指标)</p> <p>从测量对象将请求转发给后端云主机开始，到测量对象收到后端服务</p>	≥0ms		

		器返回响应为止。 单位：毫秒。			
m1a_17_upstream_rt_max	7层后端的RT最大值	统计测量对象当前7层后端最大响应时间。 (HTTP和HTTPS监听器才有此指标) 从测量对象将请求转发给后端云主机开始,到测量对象收到后端服务器返回响应为止。 单位：毫秒。	≥0ms	独享型负载均衡器 共享型负载均衡器 独享型负载均衡后端主机组 共享型负载均衡后端主机组	1分钟
m1b_17_upstream_rt_min	7层后端的RT最小值	统计测量对象当前7层后端最小响应时间。 (HTTP和HTTPS监听器才有此指标) 从测量对象将请求转发给后端云主机开始,到测量对象收到后端服务器返回响应为止。 单位：毫秒。	≥0ms		
m1c_17_rt_max	7层协议的RT最大值	统计测量对象当前7层最大响应时	≥0ms	独享型负载均衡器	1分钟

		间。(HTTP和HTTPS监听器才有此指标)从测量对象将请求转发给后端云主机开始,到测量对象收到后端云主机返回响应止。 单位:毫秒。		共享型负载均衡器 独享型负载均衡监听器 共享型负载均衡监听器	
m1d_l7_rt_min	7层协议的RT最小值	统计测量对象当前7层最小响应时间。(HTTP和HTTPS监听器才有此指标)从测量对象将请求转发给后端云主机开始,到测量对象收到后端云主机返回响应止。 单位:毫秒。	≥0ms		
l7_con_usage	7层并发连接使用率	统计7层的ELB实例并发连接数使用率。 单位:百分比。	≥0%	独享型负载均衡	1分钟
l7_in_bps_usage	7层入带宽使用率	统计7层的ELB实例入带宽使用率。单位:百分比入带宽使用率<100% 注意 若入带宽使用率达到	≥0%		

		100%，说明已经超出 ELB 规格所提供的性能保障，您的业务可以继续使用更高带宽，但对于带宽超出的部分 ELB 无法承诺服务可用性指标。			
l7_out_bps_usage	7 层出带宽使用率	统计 7 层的 ELB 实例出带宽使用率。单位：百分比出带宽使用率 <100%	≥0%		
l7_ncps_usage	7 层新建连接数使用率	统计 7 层的 ELB 实例新建连接数使用率。单位：百分比	≥0%		
l7_qps_usage	7 层查询速率使用率	统计 7 层的 ELB 实例查询速率使用率。单位：百分比	≥0%		
m18_l7_upstream_2xx	7 层后端返回码 (2XX)	统计测量对象当前 7 层后端 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。	≥0 个/s	独享型负载均衡后端服务组 共享型负载均衡后端服务组	1 分钟
m19_l7_u	7 层后端返回	统计测量对	≥0 个/s		

pstream_3xx	码 (3XX)	象当前 7 层后端 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。			
m25_17_resp_Bps	7 层响应带宽	单位: 比特/秒	≥ 0 bit/s		
m24_17_req_Bps	7 层请求带宽	单位: 比特/秒	≥ 0 bit/s		
l4_con_usage	4 层并发连接使用率	统计 4 层的 ELB 实例并发连接数使用率。 单位: 百分比。	$\geq 0\%$	独享型负载均衡	1 分钟
l4_in_bps_usage	4 层入带宽使用率	统计 4 层的 ELB 实例入带宽使用率。单位: 百分比入带宽使用率 <100%	$\geq 0\%$		
l4_out_bps_usage	4 层出带宽使用率	统计 7 层的 ELB 实例出带宽使用率。单位: 百分比出带宽使用率 <100%	$\geq 0\%$		
l4_ncps_usage	4 层新建连接数使用率	统计 7 层的 ELB 实例新建连接数使用率。 单位: 百分比	$\geq 0\%$		

维度

Key	Value
lbaas_instance_id	独享型负载均衡器的 ID。 共享型负载均衡器的 ID。
lbaas_listener_id	独享型负载均衡监听器的 ID。 共享型负载均衡监听器的 ID。
lbaas_pool_id	后端主机组的 ID

11.2 设置告警规则

本章节主要介绍添加、修改告警规则，删除告警规则详见《云监控服务用户指南》。

11.2.1 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. “资源类型”，选择“弹性负载均衡”。
- b. 单击“维度”，可以选择“弹性负载均衡（外网）”或“弹性负载均衡（内网）”或“监听器”或“后端主机组”，这里以选择“弹性负载均衡（内网）”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》。

11.2.2 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，单击需修改的告警规则操作列的“修改”。
 - a. 在“修改告警规则”界面，根据界面提示修改配置参数。
 - b. 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

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》。

11.3 查看监控指标

操作场景

云服务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。您可以通过云监控管理控制台，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、删除状态的后端云主机，无法在云监控中查看其监控指标。当后端云主机再次启动或恢复后，即可正常查看。

📖 说明

关机、故障 24 小时以上的后端云主机，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 11.2 设置告警规则。
- 子帐号用户如果需要在云监控页面中查看 ELB 监控数据，需要为子帐号添加“ELB Administrator”权限，否则无法查询到完整的 ELB 监控数据。

在云监控服务控制台查看监控指标

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. 在“云服务监控”页面，单击需要查看监控指标的负载均衡器名称。或单击目标负载均衡器右侧操作列的“查看监控指标”。
5. 选择需要查看监控指标的时间段。支持选择系统定义的时间段（如“近 1 小时”），或自定义时间段。
6. 单击右上角的“设置监控指标”，设置需要查看的监控指标。

📖 说明

查看云服务监控指标详见《云监控服务用户指南》。

12 常见问题

12.1 高频常见问题

- 错误!未找到引用源。错误!未找到引用源。
- 12.6.1 健康检查异常如何排查?
- 12.6.2 使用 UDP 协议有什么注意事项?
- 12.8.2 ELB 支持什么类型的会话保持?
- 12.4.2 如何启用 WebSocket 支持?
- 12.8.1 如何检查弹性负载均衡会话保持不生效问题?
- 12.4.1 监听器中分配算法和会话保持算法是什么关系?
- 12.3.1 ELB 如何根据不同的协议来分发流量?

12.2 弹性负载均衡使用

12.2.1 异常检查

12.2.1.1 如何检查弹性负载均衡服务不通或异常中断?

1. 检查后端云主机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主机。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，检查后端云主机所在的安全组入方向是否放通 ELB 所在 VPC 的网段。
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

- 独享型负载均衡四层监听器未开启“跨 VPC 后端”功能时，后端云主机安全组规则和网络 ACL 规则均无需放通 ELB 所在的 VPC 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. 检查后端主机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主机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云主机。
8. 检查您是否通过跨 VPC 后端功能添加了后端云主机。如果是，需要确认在 ELB 所在的 VPC 和后端云主机所在的 VPC 之间是否建立了对等连接。

12.2.2 功能支持

12.2.2.1 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，要基于弹性云主机来使用，不可以单独使用。

12.2.2.2 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：

- 独享型负载均衡：分配的弹性 IP 支持解绑，解绑后的独享型负载均衡变成私网型负载均衡，解绑后的弹性 IP 可被其他资源绑定。
- 共享型负载均衡：分配的弹性 IP 支持解绑，解绑后的共享型负载均衡变成私网型负载均衡，解绑后的弹性 IP 可被其他资源绑定。
- 经典型负载均衡：分配的弹性 IP 都是由您所购买的服务独占。

12.2.2.3 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 个共享型和独享型负载均衡器，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。

12.2.2.4 当负载均衡器正在运行中是否可以调整后端云主机的数量？

我们支持在任意时刻增加或减少负载均衡器的后端云主机的数量，且可以支持不同的后端云主机切换操作。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。

12.2.2.5 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。

12.2.2.6 是否支持在业务不中断的前提下，将共享型负载均衡升级为独享型负载均衡？

不支持将共享型负载均衡升级为独享型负载均衡。

12.2.3 性能负载

12.2.3.1 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，没有转发至后端云主机。

12.2.3.2 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. 检查后端云主机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. 将云主机添加到 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。

12.2.3.3 如何检查弹性负载均衡业务访问延时大？

1. 将 EIP 绑定到后端云主机，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主机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。

12.2.3.4 如何检查压测性能上不去？

1. 检查后端云主机的负载状态，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. 后端云主机的监听队列 `backlog` 满了，导致后端云主机不回复 `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。

12.3 负载均衡器

12.3.1 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。

📖 说明

“FullNAT”是转发模式，是指 LVS 会转换客户端的源 IP 和目的 IP。

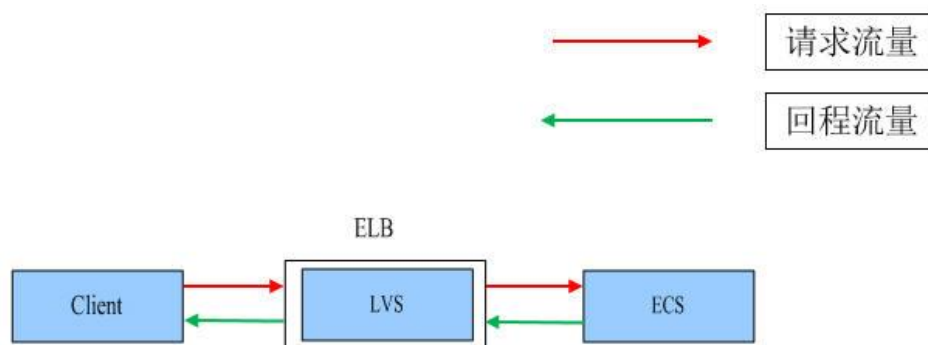


图12-1 四层转发协议

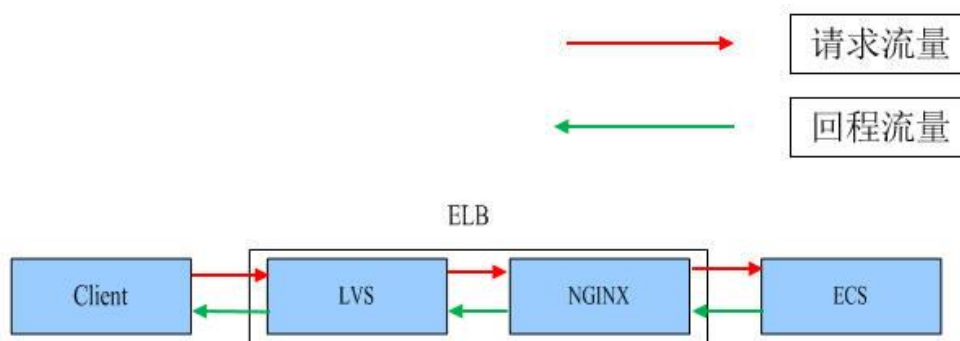


图12-2 七层转发协议

12.3.2 共享型增强型 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。

12.3.3 修改分配策略类型会导致业务中断吗？

修改分配策略类型不会影响现有连接，因此业务不会中断。

12.3.4 独享型负载均衡器的带宽和 EIP 的带宽有什么区别？

独享型负载均衡器的带宽，又称为“每秒带宽（Mb/s）”，是指 ELB 的入流量加出流量总和的最大值。ELB 绑定的 EIP 的带宽是指客户端访问 ELB 时的最高流量限制。

12.4 监听器

12.4.1 监听器中分配算法和会话保持算法是什么关系？

会话保持功能，目的是将同一个用户的会话分发到相同的后端节点，共享型负载均衡支持情况如表 12-2 所示，独享型负载均衡支持情况如表 12-1 所示，经典型支持的情况如表 12-3 所示。

表12-1 独享型负载均衡会话保持支持情况

分配策略	会话保持类型	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

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

表12-2 共享型负载均衡会话保持支持情况

分配策略	会话保持类型	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
	应用程序 cookie	不涉及	不支持
源 IP 地址	源 IP 地址	不涉及	不支持
	负载均衡器 cookie	不涉及	不支持
	应用程序 cookie	不涉及	不支持

表12-3 经典型会话保持支持情况

分配策略	会话保持	L4 (TCP、UDP)	L7 (HTTP/HTTPS)
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	不支持

分配策略	会话保持	L4 (TCP、UDP)	L7 (HTTP/HTTPS)
最少连接	源 IP 地址	支持	不支持
	负载均衡器 cookie	不涉及	不支持
	应用程序 cookie	不涉及	不支持
源 IP 地址	源 IP 地址	不涉及	不支持
	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，七层使用负载均衡器 cookie 方式。

12.4.2 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）。

12.4.3 独享型负载均衡器为什么添加不了监听器？

这是因为您在创建独享型负载均衡时，只选择了网络型（TCP/UDP）实例规格或只选择了应用型（HTTP/HTTPS）实例规格，只能添加对应协议的监听器。

独享型 ELB 实例的类型选定后无法修改，请您合理评估选择。例如：您初始创建了网络型 ELB 实例，则只能创建 TCP/UDP 监听器，无法添加或修改为应用型 ELB 实例，也就无法添加 HTTP/HTTPS 监听器。

表12-4 独享型负载均衡类型与监听器的关系

独享型负载均衡的类型	对应协议	可添加的监听器类型
网络型	TCP/UDP	TCP 监听器、UDP 监听器
应用型	HTTP/HTTPS	HTTP 监听器、HTTPS 监听器

12.5 后端云主机

12.5.1 为什么后端云主机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 节点都会探测后端云主机，每个节点的间隔时间与设置的间隔时间保持一致。

后端云主机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。

12.5.2 使用 ELB 后，后端云主机能否访问公网？

后端云主机能否访问公网和 ELB 没有关系，如果后端云主机本身可以访问公网，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。

12.5.3 如何检查后端云主机网络状态？

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。

12.5.4 如何检查后端云主机网络配置？

1. 确认虚拟机使用的网卡安全组配置是否正确。
 - a. 在弹性云主机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，检查后端云主机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

- 独享型负载均衡四层监听器未开启“跨 VPC 后端”功能时，后端云主机安全组规则和网络 ACL 规则均无需放通 ELB 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。

12.5.5 如何检查后端云主机服务状态？

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 0 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。

```
[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 ~]#
```

图12-3 系统的端口监听状态

- 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 ~]#
```

12.5.6 后端云主机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。

12.6 健康检查

12.6.1 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云主机异常，负载均衡器的“后端主机组”页签显示后端云主机的健康检查结果为“异常”。

- 独享型负载均衡

在“负载均衡器”界面，单击后端云主机所在的负载均衡器名称，切换到“后端主机组”页签，在基本信息页面，查看“健康检查结果”列是否显示“异常”。

- 共享型负载均衡

在“负载均衡器”界面，单击后端云主机所在的负载均衡器名称，切换到“后端主机组”页签，在基本信息页面，查看“健康检查结果”列是否显示“异常”。

- 经典型负载均衡

在“负载均衡器”界面，切换到“经典型”页签，单击后端云主机所在的负载均衡器名称，切换到“监听器”页签，查看“健康检查结果”列是否显示“异常”。

背景介绍

ELB 的健康检查通过向后端云主机发起心跳检查的方式来实现。独享型负载均衡在检查过程中使用 ELB 所在的 VPC 地址通信；共享型负载均衡在检查过程中使用内网地址 100.125.0.0/16 通信。

对于独享型负载均衡，为确保健康检查正常进行，您需要确保服务器已经放通 ELB 所在的 VPC 网段，使得 ELB 能够正常访问到后端云主机。

对于共享型负载均衡，为确保健康检查正常进行，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云主机。

注意

- 独享型负载均衡共享型负载均衡的安全组规则不同，请您在实际排查时务必注意，后文不再赘述。
- 独享型负载均衡，添加后端云主机之前首先要检查其所在安全组规则是否放行源网段为 VPC 网段的地址。独享型负载均衡后端云主机安全组配置请参考 6.2 后端云主机配置安全组（独享型）。
- 共享型负载均衡，需要确保服务器已经放通 100.125.0.0/16 网段的地址。共享型负载均衡后端云主机安全组配置请参考 6.3 后端云主机配置安全组（共享型）。
- 独享型负载均衡四层监听器未开启“跨 VPC 后端”功能时，后端云主机安全组规则和网络 ACL 规则均无需放通 ELB 所在的 VPC 网段。

当健康检查探测到您的后端云主机异常时，ELB 将不再向异常的后端云主机转发流量。直到健康检查检测到后端云主机恢复正常时，ELB 才会向此服务器继续转发流量。

对于共享型负载均衡，如果将健康检查正常的后端云主机的权重调整为 0，则健康检查状态会显示为“异常”。

说明

- 当 ELB 后端云主机的健康检查状态处于异常状态时，ELB 不会向该后端云主机转发请求。
- 当健康检查关闭时，ELB 默认后端云主机正常在线，会将请求转发至后端云主机。
- 共享型 ELB（HTTP/HTTPS 监听器）会使用 100.125.0.0/16 网段 IP 向后端云主机发送健康检查请求和正常的客户端请求。
- 当后端云主机的权重为 0 时，流量不会再转发到该后端云主机上，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间隔和阈值（根据默认配置为几十秒生效，如果健康检查恢复正常，在 ELB 关联的后端云主机基本信息界面可以看到健康检查状态是否正常）。

表12-5 排查思路

可能原因	处理措施
检查后端主机组是否关联监听器	解决方法请参考检查后端主机组是否关联监听器。
检查 ELB 是否绑定 EIP 或私网 IP	解决方法请参考检查 ELB 是否绑定 EIP 或私网 IP。
健康检查配置	解决方法请参考检查健康检查配置。
服务器安全组配置	解决方法请参考检查服务器所在安全组。
子网 ACL 配置	解决方法请参考检查网络 ACL 规则。
后端云主机监听配置	解决方法请参考检查后端云主机是否正常。
后端云主机防火墙配置	解决方法请参考检查服务器防火墙。
后端云主机路由配置	解决方法请参考检查服务器路由。
后端云主机负载过大	解决方法请参考检查服务器负载。
后端云主机 host.deny 文件配置	解决方法请参考检查服务器 hosts.deny 文件。

检查后端主机组是否关联监听器

检查健康检查异常的服务器所在的后端主机组是否关联了监听器。

- 如果后端主机组未关联监听器，请检查是否已创建了监听器。
已经创建了监听器，请将后端主机组关联至监听器。
未创建监听器，请先添加监听器，然后为监听器绑定后端主机组。
- 如果后端主机组已经关联了监听器，请再按照以下原因排查。

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）。
- 对于七层监听器（HTTP/HTTPS），无论 ELB 是否绑定弹性 IP 或私网 IP，均不会影响后端云主机健康检查。

对于四层监听器（TCP/UDP），请检查其关联的负载均衡器是否绑定弹性 IP 或私网 IP。

如果 ELB 未绑定弹性 IP 和私网 IP，请绑定弹性 IP 或私网 IP。

📖 说明

ELB 初次创建时，如果未绑定 EIP 或私网 IP 时，四层监听器（TCP/UDP）所关联的后端云主机会显示健康检查异常。当给 ELB 绑定 EIP 或私网 IP 后，健康检查结果显示正常，再解绑 EIP 或私网 IP 后，健康检查结果依然会显示正常。

检查健康检查配置

独享型和共享型负载均衡，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“后端主机组”页签，单击对应的后端主机组名称，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：

- 域名。健康检查使用 HTTP 协议时，如果后端云主机设置了校验 HOST 头能力，需要将后端云主机配置的域名填写到“健康检查配置”页面中的“域名”处。
- 协议。
- 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

- 检查路径需填写绝对路径。

例如：

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”。

经典型负载均衡，在监听器页面，在健康检查异常的监听器所在行，单击“健康检查”列下的“查看”。弹出健康检查配置项提示框。查看以下参数：

- 健康检查协议/端口
端口必须是后端云主机上真实业务所监听的端口，不是自定义端口。
检查您配置的健康检查端口和监听的端口是否一致。不一致则会导致健康检查异常。
- 健康检查方式。
- 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

检查路径需填写绝对路径。

例如：

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”。

检查服务器所在安全组

- **独享型 ELB**

TCP、HTTP 或 HTTPS 协议监听器：后端云主机所在的安全组入方向规则无需放通 100.125.0.0/16 网段，但需放通独享型 ELB 所在 VPC 的网段，并在 TCP 协议中放通健康检查的端口。

⚠ 注意

- 独享型负载均衡四层监听器未开启“跨 VPC 后端”功能时，后端云主机安全组规则和网络 ACL 规则均无需放通 ELB 所在的 VPC 网段。

- **健康检查端口与后端云主机业务端口相同：**需要放通后端云主机的业务端口，例如 80。
- **健康检查端口与后端云主机业务端口不同：**需要放通后端云主机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12-4展示了安全组入方向规则配置示例。配置项包括：协议选择为 TCP，端口为 80，IP 地址选择为 IPv4，网段为 100.125.0.0/16。

图12-4 安全组入方向规则配置示例

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、端口和独享型 ELB 所在 VPC 的网段。还需要放通后端云主机所在安全组入方向的 ICMP 协议。

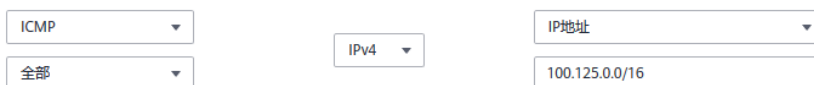


图12-5展示了安全组入方向规则放通 ICMP 协议的配置示例。配置项包括：协议选择为 ICMP，端口为全部，IP 地址选择为 IPv4，网段为 100.125.0.0/16。

图12-5 安全组入方向规则放通 ICMP 协议示例

- **共享型 ELB**

TCP、HTTP 或 HTTPS 协议监听器：后端云主机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。

⚠ 注意

- 独享型负载均衡四层监听器未开启“跨 VPC 后端”功能时，后端云主机安全组规则和网络 ACL 规则均无需放通 ELB 所在的 VPC 网段。

- **健康检查端口与后端云主机业务端口相同：**需要放通后端云主机的业务端口，例如 80。
- **健康检查端口与后端云主机业务端口不同：**需要放通后端云主机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。

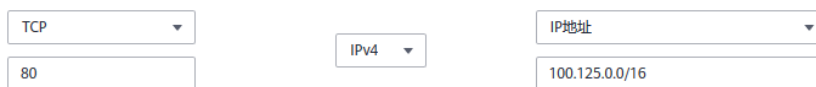


图12-6展示了安全组入方向规则配置示例。配置项包括：协议选择为TCP，端口为80，IP地址选择为IPv4，IP地址范围为100.125.0.0/16。

图12-6 安全组入方向规则配置示例

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。还需要放通后端云主机所在安全组入方向的 ICMP 协议。

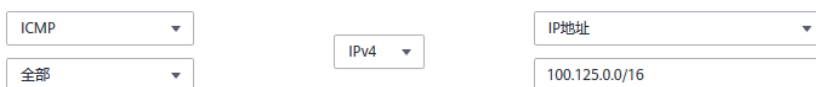


图12-7展示了安全组入方向规则放通 ICMP 协议的配置示例。配置项包括：协议选择为ICMP，端口选择为全部，IP地址选择为IPv4，IP地址范围为100.125.0.0/16。

图12-7 安全组入方向规则放通 ICMP 协议示例

- **经典型内网 ELB：**后端云主机所在的安全组入方向规则无需放通 100.125.0.0/16 网段，但需要保证入方向规则配置了 TCP 协议和 ELB 用于健康检查的端口，并且放通本 VPC 网段。

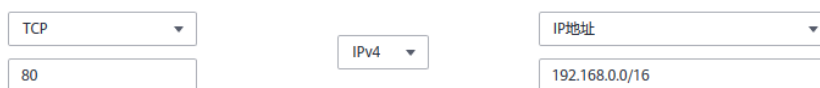


图12-8展示了安全组入方向规则放通 VPC 网段的配置示例。配置项包括：协议选择为TCP，端口为80，IP地址选择为IPv4，IP地址范围为192.168.0.0/16。

图12-8 安全组入方向规则放通 VPC 网段示例

📖 说明

- 共享型 ELB 与后端云主机进行通信的网段为 100.125.0.0/16 网段，ELB 流量转到后端云主机后，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，所以后端云主机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 12.6.2 使用 UDP 协议有什么注意事项？。

检查网络 ACL 规则


⚠️ 注意

- 独享型负载均衡四层监听器未开启“跨 VPC 后端”功能时，后端云主机安全组规则和网络 ACL 规则均无需放通 ELB 所在的 VPC 网段。

● 独享型负载均衡

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云主机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，或者会导致后端云主机异常。


您可以通过配置网络 ACL 入方向规则，放行源网段为 ELB 所在的 VPC 网段，目的端口为后端云主机端口。

- 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. 在系统首页，选择“网络 > 虚拟私有云”。
- d. 在左侧导航栏选择“访问控制 > 网络 ACL”。
- e. 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。
- f. 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，填写为 VPC 网段。
 - 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。
- g. 单击“确定”。

- **共享型负载均衡**

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云主机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，或者会导致后端云主机异常。

您可以通过配置网络 ACL 入方向规则，放行 100.125.0.0/16 网段。

- 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. 在系统首页，选择“网络 > 虚拟私有云”。
- d. 在左侧导航栏选择“访问控制 > 网络 ACL”。
- e. 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。
- f. 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。
- g. 单击“确定”。

检查后端云主机是否正常

📖 说明

如果后端云主机的操作系统为 Windows，请通过浏览器直接访问 `https://后端云主机的IP:健康检查配置的端口`。如果返回码为 2xx 或 3xx，则表示后端云主机正常。

- 您可以在后端云主机上通过以下命令查看后端云主机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，则表示后端云主机的健康检查端口在监听状态，如 0 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，默认和后端云主机业务端口一致。



```
[root@ecs-elb-srv portable-nginx]# netstat -anlp | grep 880 | head
tcp        0      0 0.0.0.0:880 0.0.0.0:* LISTEN
```

图12-9 后端云主机正常被监听的回显示例



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

图12-10 后端云主机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（后端云主机没有被监听），您需要先启动后端云主机上的业务，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，请您在后端云主机上执行以下命令查看回显中返回的状态码。

```
curl 后端云主机的私有IP:健康检查端口/健康检查路径 -iv
```

HTTP 健康检查是 ELB 向后端云主机发起 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：TCP/UDP/HTTP/HTTPS 健康检查正常返回状态码均为 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；TCP 健康检查正常返回状态码是 200。

对于经典公网 ELB，HTTP 健康检查正常返回状态码是 2xx 或者 3xx。

```
[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12-11 后端云主机异常的回显示例

```
[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: */*
>
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
```

图12-12 后端云主机正常的回显示例

- 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 健康检查的后端主机组，或者选择新创建 TCP 健康检查的后端主机组。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

如果后端云主机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 所在的 VPC 网段或 100.125.0.0/16 网段的 IP。

对于独享型负载均衡，请您在防火墙入方向规则中放通 ELB 所在的 VPC 网段。

对于共享型负载均衡，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云主机内部的路由，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云主机。

您可以在后端云主机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 0 所示。

```
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12-13 默认路由指向网关示例

```
[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
```

图12-14 默认路由未指向网关示例

如果回显中没有像 0 中的第一条路由信息，或者路由指向的 IP 的不是后端云主机所在 VPC 子网的网关，请您配置默认路由指向网关。

检查服务器负载

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

如果负载很高，可能会导致健康检查的连接或请求超时。

检查服务器 hosts.deny 文件

建议您排查后端云主机的/etc/hosts.deny 文件，文件中不能写入 ELB 所在的 VPC 网段或健康检查 100.125.0.0/16 网段。

对于独享型负载均衡，该文件中不能写入 ELB 所在的 VPC 网段。

对于共享型负载均衡，该文件中不能写入健康检查 100.125.0.0/16 网段。

12.6.2 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：

- 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云主机返回的 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云主机返回的 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，会给后端云主机发送 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云主机返回的 `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云主机返回的 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：后端云主机回复的 `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，否则后端云主机可能会反复上线或下线。
- 后端云主机是否限制了 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云主机的状态信息。针对此种情况，用户需要确保后端云主机开启 ICMP 协议，确认方法如下：
用户登录后端云主机，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：
如果后端云主机是 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。
- 当负载均衡的类型为经典型私网负载均衡时，不允许创建 UDP 协议的监听器。

12.6.3 健康检查为什么会导致 ELB 会频繁向后端云主机发送探测请求？

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云主机发送探测请求，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 7.2 配置健康检查的周期来控制访问后端云主机的频率。

12.7 HTTP/HTTPS 监听器

12.7.1 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。
- 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。

12.7.2 配置转发策略时，为什么无法选择已有的后端主机组？

后端主机组只能被一个转发策略所引用，因为该后端主机组已经被另一个转发策略所引用，所以选不到想选择的后端主机组。

12.8 会话保持

12.8.1 如何检查弹性负载均衡会话保持不生效问题？

1. 查看后端主机组上是否开启了会话保持。
2. 查看后端云主机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主机，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）。

12.8.2 ELB 支持什么类型的会话保持？

独享型负载均衡器支持源 IP 地址、负载均衡器 cookie 两种会话保持类型。

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

经典型负载均衡器支持源 IP、负载均衡器 cookie 两种会话类型。

12.9 证书管理

12.9.1 如何生成服务器证书和 CA 证书？

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，关于服务器证书和 CA 证书的生成，请参考 5.4 HTTPS 双向认证。

12.9.2 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。

13 修订记录

版本日期	变更说明
2022-12-30	第六次正式发布。 本次变更说明如下： 新增独享型实例（全文适配修改）：创建负载均衡时，支持选择实例规格类型（独享型/共享型）。
2019-06-30	第五次正式发布。 本次变更说明如下： 新增“8.5 快速查询证书所关联的监听器”。 健康检查参数中增加“HTTP 健康检查”：更新 7 健康检查。
2019-03-30	第四次正式发布。 本次变更说明如下： 监听器章节新增安全策略参数，新增安全策略章节： 更新：4 监听器。 新增：5.6 TLS 安全策略。
2018-12-30	第三次正式发布。 根据最新的管理控制台界面修改对应的资料描述和截图。
2018-05-30	第二次正式发布。 新增常见问题“12.6.2 使用 UDP 协议有什么注意事项？”。
2018-02-28	第一次正式发布。
2022-08-25	第一次更新