弹性负载均衡

用户使用指南

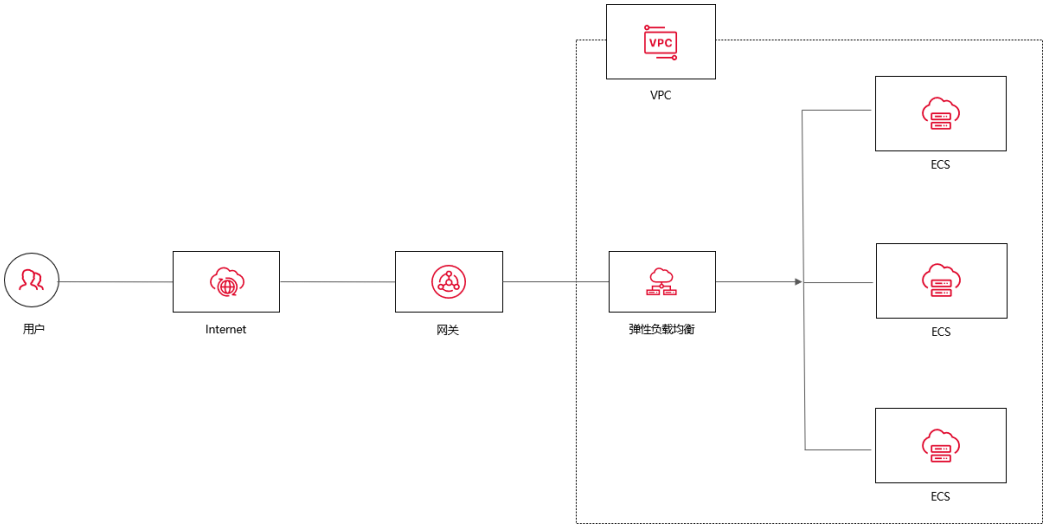
天翼云科技有限公司

目录

1 弹性负载均衡产品简介

1.1 产品定义

弹性负载均衡（CT-ELB ，Elastic Load Balancing）是一种分发控制网络流量的服务，通过预先设定的算法将访问流量自动分发到多台云主机，扩展应用系统对外的服务能力，实现更高水平的应用系统容错性能。



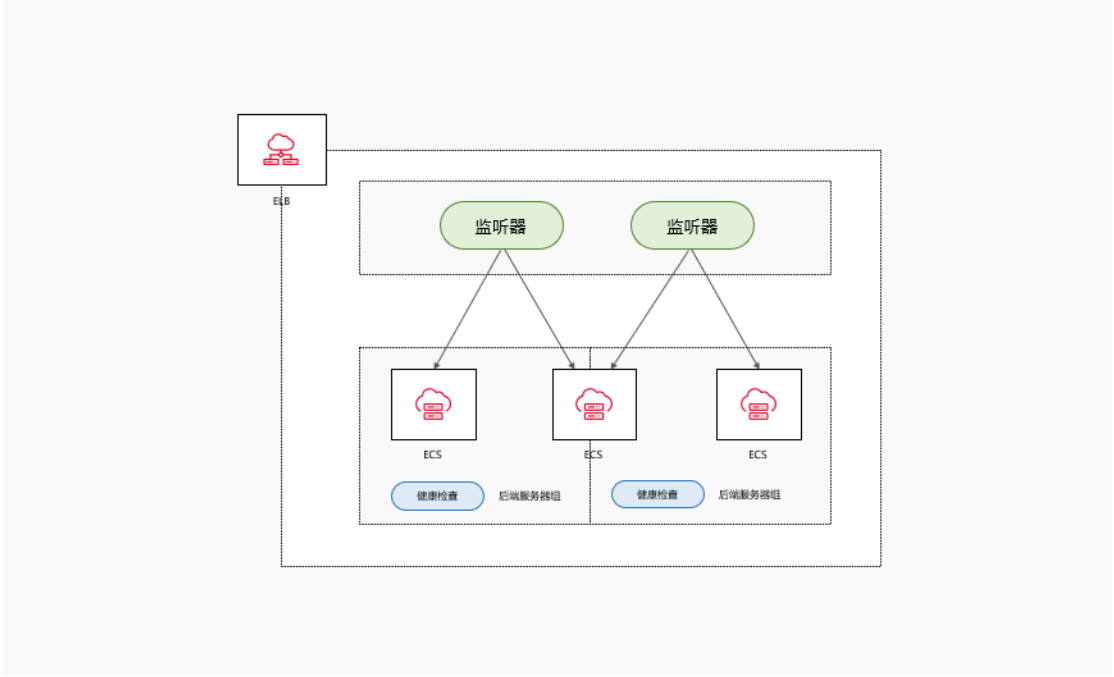
产品架构

弹性负载均衡的产品架构主要包含以下组件：

- 负载均衡器：即负载均衡实例，可以接收来自客户端的请求流量，并经流量分配到一个或多个可用的后端主机。
- 监听器：监听器是弹性负载均衡的核心组件，监听器指定要监听的协议和端口号，并根据配置的负载均衡算法将请求转发到后端主机。监听器也会对后端主机进行健康检查。
- 后端主机组：每个监听器关联一个后端主机组，后端主机组包含多个后端主机。当

监听器接收到客户端请求时，它将请求转发给后端主机组中的一个或多个后端主机。后端主机组负责将请求传递给相应的后端主机，实现负载均衡和高可用性。

- 转发策略：转发策略定义了负载均衡器将流量请求转发给后端主机的方式。
- 访问策略组：访问策略组可帮助您控制访问权限，确保负载均衡器只接收来自指定网络范围的请求，从而提高应用程序的安全性。
- 证书管理：用户将证书上传到负载均衡中，在创建 HTTPS 协议监听的时候需绑定证书，提供 HTTPS 服务。



天翼云弹性负载均衡 AZ 级容灾高可用架构具有如下特点：

- 网元跨 AZ 多活，单 AZ 故障，其它 AZ 承载全部流量
- 集群模式，任意节点故障业务流量自动切换到其它可用节点
- 四七层网元分离，分布式处理，服务可用性更高
- 后端主机支持跨 AZ，业务可跨 AZ 负载

- 支持与弹性伸缩联动，后端主机组根据业务负载自动弹缩主机数量
- 监听器支持转发策略，灵活匹配业务域名、URL 转发流量到特定后端主机

工作原理

弹性负载均衡的工作原理如下：

- 客户端发起请求：客户端向负载均衡器发送请求，请求可以是 HTTP 请求、TCP 连接请求或 UDP 数据包等。
- 负载均衡器接收请求 :负载均衡器中的监听器接收到请求后 ,根据预先配置进行筛选，以确定如何处理该请求。
- 监听器转发请求：监听器会根据配置的负载均衡算法，选择一个或多个后端主机来处理请求。
- 后端主机处理请求：后端主机接收到请求后进行处理，并将响应返回给负载均衡器。

通过以上过程，弹性负载均衡器可以分配客户端请求到多个后端云主机，实现负载均衡和高可用性。

转发策略

监听器可以根据不同的转发策略来决定如何将流量分配给后端主机。以下是天翼云支持的弹性负载均衡转发策略类型：

调度算法	权重	算法策略
轮询	调度算法权重算法策略轮询权重取值范围为[1,256]	根据后端主机的权重，将流量按照顺序逐个分发给后端主机，每台主机依次接收请求，实现流量均衡。相应的权重表示后端主机的处理性能，常用于短连接服务。
最小连接	权重取值范围为[1,256]	将流量分发给当前连接数最少的主机，以确保负载较小的主机能够处理更多的请求。加权最小连接即根据主机的权重和当前连接数来分发流量，常用于长连接服务。
源算法	在非 0 的权重下，由于使用了源算法，各个后端主机的权重属性将不再生效	通过对请求的源 IP 地址进行 Hash 运算，可以将其转化为一个具体的数值。同时，后端主机也会被编号。根据 Hash 运算的结果，将请求分发到对应编号的后端主机上，从而实现了对不同源 IP 地址的访问进行负载均衡，同时确保同一个客户端 IP 的请求始终被派发到相同的主机上。

访问方式

您可以使用以下方式来访问和管理弹性负载均衡：

- 管理控制台：您可以直接登录“控制中心”，选择“网络>弹性负载均衡”来访问和管理弹性负载均衡。在控制台中，您可以查看负载均衡器的状态、性能指标和配置信息等，并进行相关的操作和管理。
- API 接口：您可以通过调用 API 接口的方式来访问和管理弹性负载均衡。通过调用 API 接口可以实现负载均衡器的创建、修改、删除和查询等操作。具体请参考 API 参考。

1.2 网络流量路径

1.2.1 入网流量路径

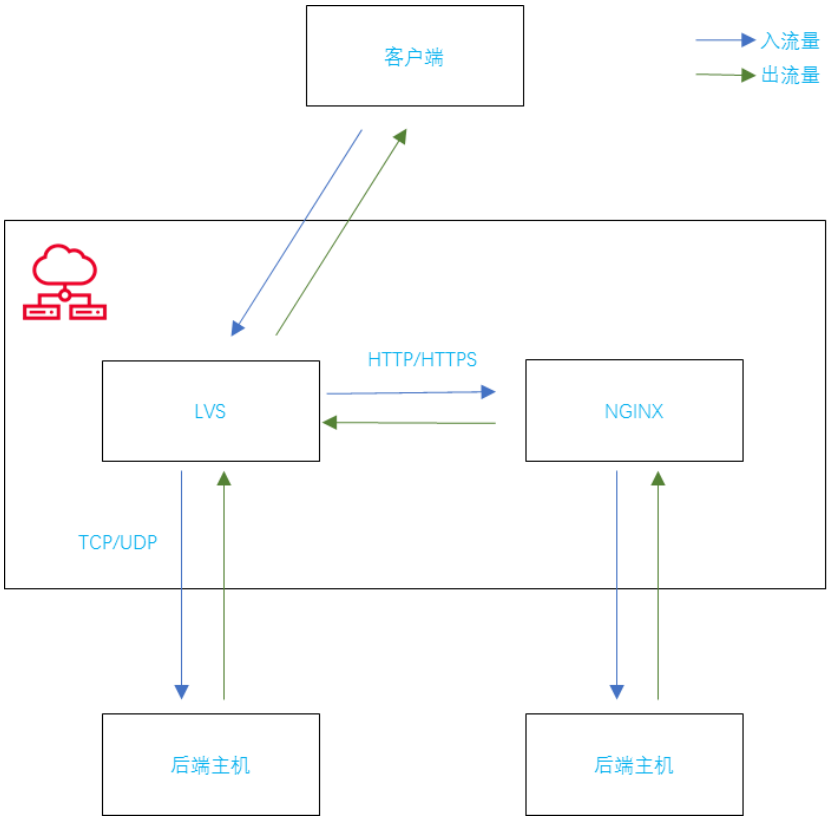
对于入网流量，在负载均衡器使用四层协议 TCP/UDP 时，可以通过 LVS 集群进行转发。LVS 集群的节点会根据负载均衡器的流量分配策略，将接收到的访问请求直接分发到后端主机上，从而实现负载均衡。

而当负载均衡器使用七层协议 HTTP/HTTPS 时，通常涉及到两个层次的负载均衡。首先，请求会经过 LVS 集群，LVS 会将请求平均分发到 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主机。

对于七层协议 HTTPS 的流量，在最终分发到后端服务器之前，通常需要在 Nginx 集群内进行证书验证和数据包解密操作。这是为了确保安全性。然后，通过 HTTP 协议将请求转发到后端服务器进行处理。

1.2.2 出网流量路径

出网流量的路径取决于数据请求进入网络的方式。对于通过负载均衡器进入的访问流量，相应的响应流量也会通过负载均衡器返回。负载均衡器通过绑定的弹性公网 IP 接收来自公网的流量，并在 EIP 上进行计费。从负载均衡器到后端云主机之间的通信通过 VPC 内网进行，不会产生额外费用。



1.3 基本概念

名词	说明

负载均衡服务	天翼云提供的一种网络负载均衡服务，提供四层和七层负载均衡服务。
负载均衡实例	负载均衡实例是一个运行的负载均衡服务。要使用负载均衡服务，必须先创建一个负载均衡实例。
监听器	监听器负责监听负载均衡器上的请求，规定了如何将请求转发给后端云主机处理。
后端服务器组	一组处理负载均衡分发的前端请求的云主机实例。
后端服务器	处理前端请求的云主机实例。
弹性公网带宽	弹性公网带宽是指对外提供服务，可以访问网络，网络其他计算机可以访问主机的流量。
负载均衡器协议/端口	指协议支持四层的 TCP 和七层的 HTTP。端口可根据业务需求在 1-65535 范围内任意设定。如需要使用 80、8080、443、8443 备案端口，请提前进行备案。4 个备案端口默认是关闭状态，备案完成后将开通。
云主机协议/端口	用于指定与负载均衡绑定的云主机的协议及端口，协议支持四层的 TCP 和七层的 HTTP。端口可根据业务需求在 1-65535 范围内任意设定。云主机端口不受备案限制。

会话保持	用户可以选择打开或关闭会话保持功能。如果打开会话保持，针对 7 层（HTTP）服务，提供基于 cookie 的会话保持；针对 4 层（TCP）服务，提供基于 IP 地址的会话保持。
健康检查	健康检查用于检查后端主机的状态。用户可自定义健康检查方式和频率，负载均衡根据预设的健康检查规则定时检查后端云主机是否正常运行，一旦检测到云主机为非健康状态，则不会将访问流量分派到这些非健康云主机实例。
负载方式	负载方式即负载均衡算法，支持轮询、最小连接数和源地址三种算法。
轮询算法	轮询算法是依据后端主机的权重，将请求轮流发送给后端云主机，常用于短连接服务，例如 HTTP 等服务。
最小连接数算法	最小连接数算法是优先将请求发给拥有最小连接数的后端云主机，常用于长连接服务，例如数据库连接等服务。
源算法	源算法是将请求的源地址进行 hash 运算，并结合后端的云主机的权重派发请求至某匹配的云主机，这可以使得同一个客户端 IP 的请求始终被派发至某特定的云主机。该方式适合负载均衡无 cookie 功能的 TCP 协议。
默认配额	默认配额是指每个用户在每个区域节点资源的数量，如默认配额无法满足用户需求，可通过控制台申请调整配额。

1.4 产品优势

高性能

弹性负载均衡基于 DPDK 架构提供高性能的处理能力，能够处理大量的网络流量和连接请求。能够对七层 SSL 卸载，减轻后端主机压力,单实例可支持 1000w 并发。

高可用

弹性负载均衡集群结构可将请求分发到不同的弹性负载均衡实例，提高了应用程序的可用性。采用集群化部署，支持多可用区的同城双活容灾，无缝实时切换。完善的健康检查机制，保障业务实时在线。

多协议

弹性负载均衡确实支持多种协议，包括 TCP、UDP、HTTP 和 HTTPS。这使得您能够根据不同的协议需求进行流量分发和负载均衡。

高可靠

主备和集群模式部署，避免单一负载均衡器成为瓶颈，支持快速的故障切换和双活容灾，从而实现更均衡的流量分发和负载均衡能力。

简单易用

快速部署弹性负载均衡，实时生效，支持多种调度算法（轮询、最少连接、源算法等），用户可以根据应用程序的特性和需求进行灵活的定制，高效地管理和调整分发策略，以获得最佳的性能和负载均衡效果。

低成本

使用天翼云负载均衡服务，用户无需再投入额外的负载均衡硬件，减少了硬件投资成本。用户无需进行繁琐的负载均衡硬件的部署、配置和维护工作，减轻了运维负担。节省了大量的硬件费用和人力支出。

1.5 功能特性

支持四、七层协议的转发

支持 TCP/UDP/HTTP/HTTPS 协议，满足不同协议接入需求，可以根据不同的应用场景选择不同的协议进行接入。四层转发工作在 OSI 模型的传输层，在接收到客户端的流量以后通过修改数据包的地址信息将流量转发到应用主机。七层转发工作在 OSI 模型的应用层，七层转发会与客户端建立一条完整的连接并将应用层的请求流量解析出来，再按照调度算法选择一个应用主机。

支持获取用户真实源 IP

在四层转发（TCP/UDP）服务中，弹性负载均衡支持通过配置 TOA 插件获取用户真实 IP。在七层转发（HTTP/HTTPS）服务中，弹性负载均衡支持通过 HTTP 头中的 X-Forwarded-For 获取来访者真实 IP。

支持灵活的转发策略

用户设置负载均衡监听器的负载方式时，可选择轮询、最小连接数模式的流量分发方式。监听器支持配置转发策略，可支持按域名转发，URL 转发，URL 转发支持精确匹配、前缀匹配、正则表达式匹配，为用户提供灵活易用的流量分发能力。

支持会话保持功能

用户可针对负载均衡服务监听器开启会话保持功能，确保用户的请求在同一台主机上进行处理，以避免会话丢失。针对 7 层 （HTTP 协议）服务，负载均衡系统是基于 cookie 的会话保持；针对 4 层（TCP 协议）服务，负载均衡系统是基于 IP 地址的会话保持。它可以将同一个客户端的请求始终发送到同一台后端主机，以维持会话的连续性。

支持对后端主机进行健康检查

支持用户自定义健康检查方式和频率，负载均衡根据预设的健康检查规则定时检查后端主机组运行情况，一旦检测到云主机为非健康状态，则不会将访问流量分派到这些非健康云主机实例。

支持 IPv4 和 IPv6 双栈方案

兼容 IPv4 和 IPv6 地址，并且能够同时处理 IPv4 和 IPv6 流量。用户可以将 IPv4 和 IPv6 的流量通过负载均衡器进行负载均衡，并将其分发到后端的 IPv4 和 IPv6 云主机上，满足不同网络环境和要求下的负载均衡需求。

支持访问控制功能

通过设置黑、白名单等措施，对负载均衡器的访问进行灵活控制。黑名单是指禁止特定的 IP 访问负载均衡，白名单是指允许特定的 IP 访问负载均衡。通过对黑、白名单的设置，实现对系统的安全保护和访问控制。

支持跨可用区容灾

支持用户将后端服务节点部署在不同的可用区，通过负载均衡服务将流量分发到这些节点上。如果某个可用区出现故障，负载均衡服务可以自动将流量切换到其他正常的可用区，从而实现跨可用区容灾。

1.6 应用场景

1.6.1 分发流量应对高访问量业务

场景说明

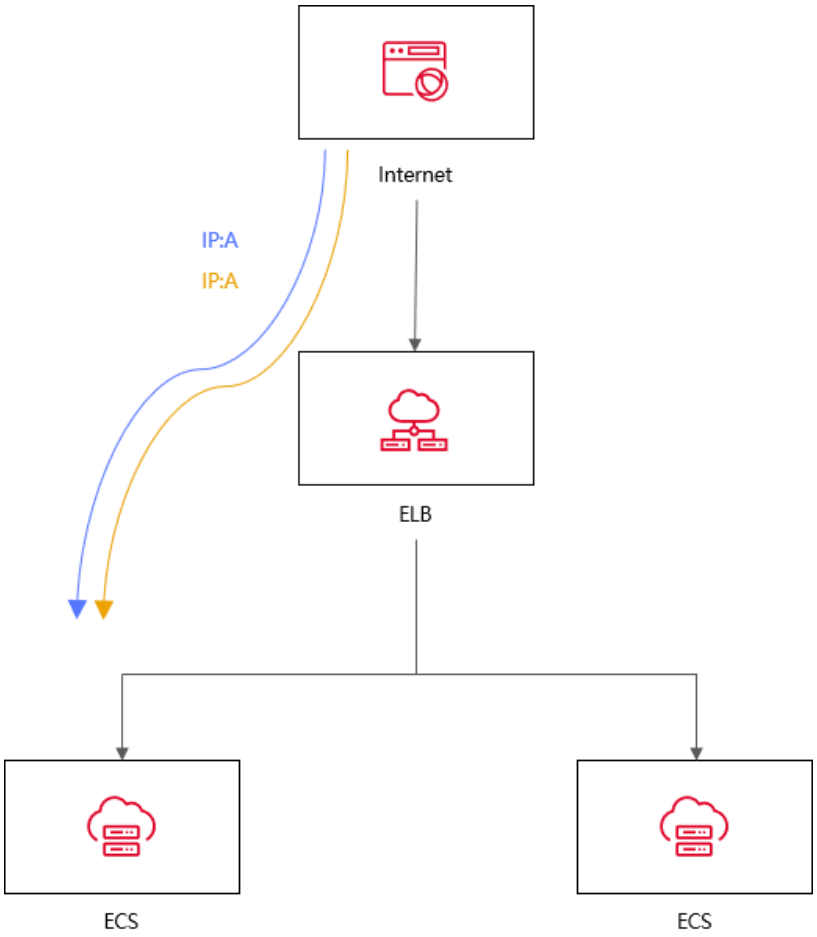
针对高访问量的业务，可以使用负载均衡来实现流量分发，通过设置适当的转发策略，将访问量均衡地分配到多个后端云主机，从而有效提高业务处理的效率和性能。同时，负载均衡还可以实现会话保持、健康检查等功能，保证业务的可用性和稳定性。后端的云主机还可以部署在不同的可用区中，实现后端主机的高可用。

场景特点

业务访问量大，高并发，单机难以支撑，负载均衡通过流量负载分担到多台后端主机承载，提升业务可靠性，有效支撑大流量、大并发业务。

典型应用对象

应用于各种高访问量的业务场景，如大型门户网站、移动应用市场、电商平台等，从而帮助企业应对高访问量的业务挑战，提高业务的可用性和性能，降低运维成本和风险。



1.6.2 集成弹性伸缩自动调整资源

场景说明

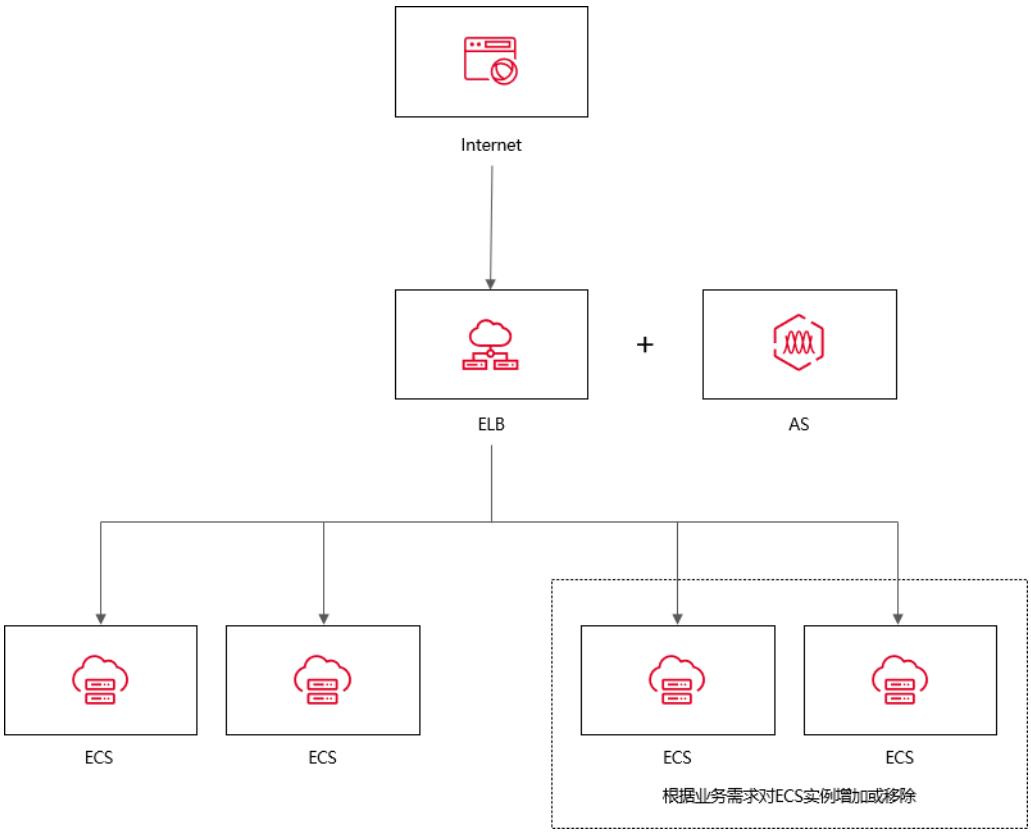
针对在某些特定时间段内，业务流量出现大幅度波动，可以使用负载均衡集成弹性伸缩服务来实现自动化的资源调整。弹性伸缩服务可以根据业务流量的变化自动调整云主机数量，从而保证业务处理能力的充足和稳定，提高业务的可用性和性能。同时，结合负载均衡技术，可以将流量合理地分配到多个云主机上进行处理，进一步提高业务的处理效率和吞吐量。

场景特点

业务流量波动大，不稳定、常出现突发性增加或减少的情况。弹性伸缩服务能够根据实时流量变化自动调整资源数量。结合负载均衡，流量可智能分配到多个云主机上，提高处理效率和吞吐量。

典型应用对象

应用于业务流量通常呈现出大幅波动的场景中，例如电商的“双 11”、“双 12”、“618”等大型促销活动。使用负载均衡及弹性伸缩能根据业务的实际情况及时调整资源数量，以满足业务的处理需求，最大限度的节省 IT 成本。



1.6.3 消除业务单点故障

场景说明

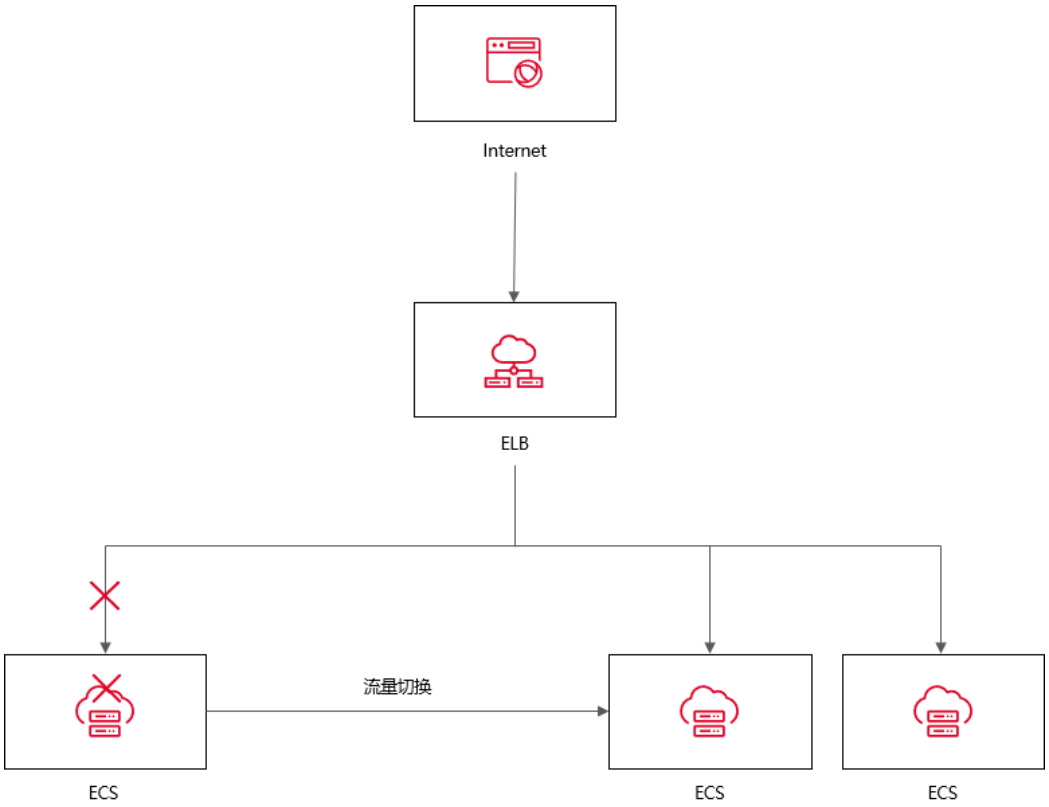
为了提高业务的可靠性，可以使用负载均衡来消除单点故障。在负载均衡器上添加多个后端云主机，并将它们部署在不同的可用区内，从而实现负载均衡的高可用性和容错能力。当某个云主机发生故障时，负载均衡器可以自动将请求转发到其他可用的云主机上进行处理，保证业务的连续性和稳定性。

场景特点

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。

典型应用对象

应用于官网，计费业务，Web 业务等使用场景。通过将请求分发到多台云主机上，即使某个云主机出现故障，也不会对整个系统造成影响，从而保证了系统的高可靠性。同时，弹性负载均衡还支持自动检测和剔除故障云主机，可以有效地提高系统的容错能力。



1.6.4 跨可用区实现业务容灾部署

场景说明

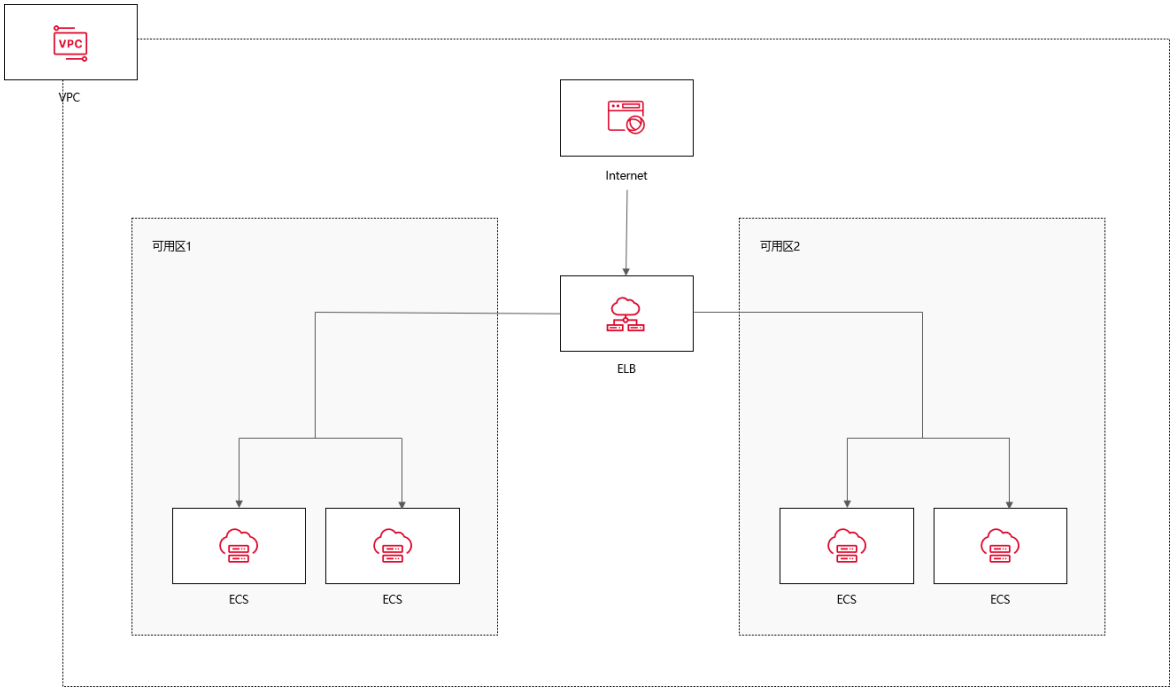
弹性负载均衡可以通过跨可用区的部署来实现业务容灾。可用区是天翼云在不同地理位置提供的独立数据中心，它们通常相互隔离，具有独立的供电、网络和硬件设施，因此在某个可用区发生故障时，其他可用区仍然能够正常运行。通过在不同可用区中部署弹性负载均衡器和后端资源，可以实现业务容灾部署，提高容错性、故障恢复能力和用户体验。

场景特点

弹性负载均衡跨可用区实现业务容灾部署具有高可用性、容错性和故障恢复能力的特点。通过在多个可用区中部署资源，系统可以在某个可用区故障时继续提供稳定可靠的服务，并自动将流量切换到其他可用区。

典型应用对象

可应用于包括 Web 应用程序、银行业务、数据库集群和大型应用系统等。通过将实例部署在多个可用区，并使用负载均衡将流量分发到这些实例，可以实现高可用性和负载均衡。如果一个可用区出现故障，流量将自动路由到其他可用区的实例，确保应用的可用性。



1.7 产品类型和规格

1.7.1 按网络类型区分

根据网络类型的不同，负载均衡服务可分为外网负载均衡和内网负载均衡。

外网负载均衡

外网负载均衡可以将来自公网的流量均衡地分发到多个后端主机组，实现高可用性和性能的提升。

外网负载均衡在使用中具有以下特点：

- 外网负载均衡使用公网弹性 IP 作为负载均衡器的虚拟 IP 地址，作为对外提供服务的入口。
- 外网负载均衡的公网流量费用是按照所使用的弹性 IP 的带宽进行计费。
- 外网负载均衡支持将 IPv4 和 IPv6 类型的弹性 IP 绑定到负载均衡器上，以适应不同网络环境和协议的需求，使负载均衡器能够同时处理 IPv4 和 IPv6 的流量。
- 用户可以根据实际需求，调整负载均衡器所使用的弹性 IP 的带宽大小。
- 外网负载均衡还支持对 IPv4 流量的带宽进行调整。

内网负载均衡

内网负载均衡通过内网 IP 地址对内部主机进行负载均衡，实现内部服务的高可用性和性能优化，同时确保内网环境的安全性。

内网负载均衡具有以下特点：

- 内网负载均衡支持自动分配 IP 地址或手动指定一个内网 IP 地址作为负载均衡器的虚拟 IP 地址（VIP）。
- 支持绑定弹性 IP 以实现公网流量负载。通过将 EIP 与内网负载均衡器绑定，可以将公网流量通过 EIP 转发到内网负载均衡器，再分发到后端主机组。
- 内网负载均衡器同时支持 IPv4 和 IPv6 实例，以满足不同类型的网络需求。

1.7.2 按产品性能区分

天翼云弹性负载均衡产品按性能可划分如下经典型负载均衡和性能保障型负载均衡，您可以根据实际需求选择适合的负载均衡器型号和配置。

经典型负载均衡

经典型负载均衡适用于访问量较小，应用模型简单的 web 业务，可满足大部分应用程序的负载均衡需求，具备基本的流量分发和健康检查功能。

经典型负载均衡为免费规格，同 VPC 内多实例性能共享，为主备模式部署，无性能保障，经典型总体性能情况如下：

规格	最大连接数	新建连接数（CPS）	QPS（HTTP）	QPS（HTTPS）
经典型	30000	5000	5000	1000

性能保障型负载均衡

性能保障型负载均衡适用于对性能有较高要求的应用场景，能够提供更强大的性能和扩展能力。

性能保障型负载均衡为收费产品，为集群模式部署，支持经典型升级为性能保障型，支持规格升级、降级。

- 经典型升级性能保障型

随着业务规模发展，存量经典型实例的性能无法满足业务需求时，可选择升级性能保障型，以获得更高的负载性能和性能保障

注意

经典型升级性能保障型，升级过程涉及底层迁移，有秒级流量中断，建议在业务低谷时段维护窗口操作。

- 规格升级、降级

升配：当用户业务快速增长，当前规格无法满足性能要求时，可使用规格变配功能，平滑升级更高规格；

降配：用户购买规格过大，或业务量出现持续一段时间的低谷时，可选择降配，将大规格降低成小规格，节省使用成本；

性能保障型负载均衡有如下规格：

规格	最大连接数	新建连接数（CPS）	QPS（HTTP）	QPS（HTTPS）
标准型 I	100000	10000	10000	2000
标准型 II	200000	20000	20000	4000
增强型 I	400000	30000	30000	6000
增强型 II	600000	50000	50000	10000
高阶型 I	1000000	50000	50000	10000

1.7.3 按资源池区分

不同资源池的产品架构分为主备模式和集群模式，具体资源池信息如下：

主备模式资源池

华东地区：

上海 7/杭州 2/合肥 2/芜湖 2/南京 2/南京 3/南京 4/南京 5/九江

华南地区：

福州 3/福州 4/福州 25/佛山 3/广州 6/南宁 2/郴州 2/长沙 3/海口 2/武汉 3/武汉 4

西北地区：

西安 3/西安 4/西安 5/中卫 2/西宁 2/兰州 2/乌鲁木齐 27/中卫 5

西南地区：

贵州 3/重庆 2/成都 4/昆明 2/拉萨 3

北方地区：

北京 4/北京 5/晋中/雄安 2/石家庄 20/内蒙 6/辽阳 1

集群模式资源池

华东地区：

上海 36/华东 1/南昌 5

华南地区：

广州 4/南宁 23/武汉 41/长沙 42

西南地区：

西南 1

北方地区：

青岛 20/华北 2

两种模式的性能及其功能具有以下区别：

产品架构及性能区别

对比项	主备模式资源池	集群模式资源池
产品部署模式	主备模式部署	集群模式
产品架构	单 AZ，虚拟网元	多 AZ，多活模式，物理网元
可扩展性	受虚拟网元规格限制，性能提升空间有限	易于扩展，通过扩展集群规模，提升产品性能能力
可用性	只能单 AZ 主备，AZ 级故障无法容灾	跨 AZ 容灾，集群内多主机互备，可用性比主备模式有质的提升
转发能力	受限底层虚拟网元处理能力限制大概 2Gbps	根据集群规模转发能力可达 100Gbps 以上
并发能力	最高 100w 并发	最高规格 1000w，集群最大并发根据集群规模可达亿级

产品功能区别

对比项	主备模式资源池	集群模式资源池
HTTP/HTTPS 协议监听器支持服务端获取监听协议/端口	不支持	支持
证书修改	支持	支持

TCP 协议监听器获取客户端真实源 IP	支持（使用 proxy protocol）	支持（使用 TOA）
HTTP 重定向到 HTTPS	不支持	支持
修改主机服务端口和权重	不支持	支持
websocket 协议	不支持	支持
HTTPS 双向认证	支持	支持
IPv6 功能	不支持	支持
转发策略-域名转发/URL 转发	支持	支持
访问控制-黑白名单	支持	支持
专线访问 LB	不支持	支持
监听器自定义超时时间	不支持	支持
跨 VPC 后端主机	不支持	支持

1.8 产品使用限制

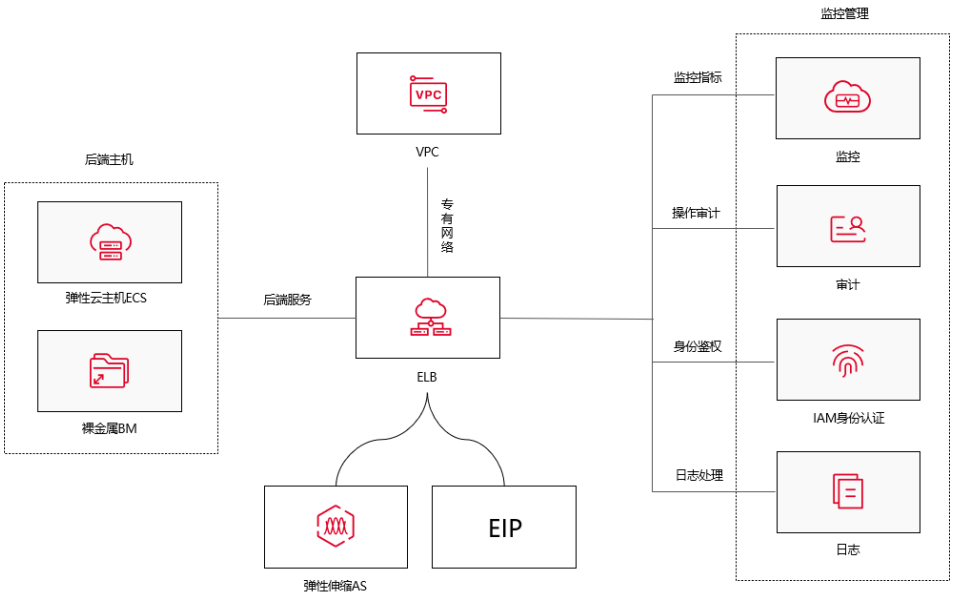
为保证弹性负载均衡产品正常使用，在使用之前，请您务必仔细阅读以下使用限制。

资源	默认限制
一个账号在单地域可创建的免费负载均衡数量	1（可开工单提升配额，注意经典型负载均衡为免费规格，提升配额后同 VPC 内多实例性能共享，无性能保

	障，如用于生产业务，建议选择性能保障型实例，性能保障型未上线的地域，建议联系您的客户经理，由天翼云工程师为您调整）
一个账号在单地域可创建性能保障型负载均衡数量	20
一个负载均衡实例可添加的监听器数量	3（可开工单提升配额）
一个负载均衡实例的监听器可绑定的主机数量	100
一个负载均衡实例中的监听器可选择的端口范围	1-65535
一个账号在单地域可创建的证书数量	10

1.9 与其他服务之间的关系

弹性负载均衡与其他天翼云服务之间的关系非常密切，可以协同工作，为用户提供高性能、高可用、高安全性的应用程序服务。



说明：

服务名称	交互功能	相关内容
虚拟私有云 VPC	创建弹性负载均衡时，需要指定弹性负载均衡关联的 VPC 和子网	创建 VPC
弹性云主机	弹性负载均衡的后端主机组，关联开启后端的主机实例	购买弹性云主机
物理机		购买物理机
弹性 IP	创建公网弹性负载均衡时，需要绑定公网 IP 来做公网服务的流量分发	购买弹性 IP

弹性伸缩	弹性伸缩服务可以与弹性负载均衡集成，根据实际的负载情况自动调整云主机实例的数量。	创建弹性伸缩
云监控服务	云监控服务可以监控弹性伸缩的性能指标，如请求数、连接数、响应时间等。	查看云监控
日志审计	日志审计可以用于收集和分析弹性负载均衡器的日志数据，以监控负载均衡器的性能、检测异常行为等。	购买日志审计

1.10 支持地域信息

为保证弹性负载均衡产品正常使用，在使用之前，请您务必仔细阅读以下支持地域信息。

芜湖 2、合肥 2、北京 5、重庆 2、福州 3、福州 4、福州 25、贵州 3、佛山 3、广州 6、南宁 2、南宁 23、兰州 2、新加坡 3、法兰克福 1、圣保罗 1、迪拜 1、武汉 3、武汉 4、武汉 41、华东 1、石家庄 20、长沙 3、海口 2、华北 2、郴州 2、南京 2、南

京 3、南京 4、南京 5、九江、辽阳 1、中卫 2、内蒙 6、中卫 2、西宁 2、青岛 20、成都 4、西安 3、西安 4、西安 5、晋中、上海 7、上海 36、乌鲁木齐 27、拉萨 3、香港 1、昆明 2、杭州 2 均支持弹性负载均衡。

2 计费说明

2.1 包年包月计费方式

本文对弹性负载均衡产品计费进行说明。

计费说明

经典型负载均衡产品免费提供，但与弹性负载均衡关联的弹性云主机、弹性 IP、带宽等云产品需按照云产品订购页面公示的计费信息支付相应服务费用。

性能保障型负载均衡为收费产品，根据选择的性能规格不同有不同的定价，当前为包周期方式计费。

适用场景

1、长期稳定使用

- 适用于需要长期稳定运行的服务，提供稳定的资源保障。

2、成本可控

- 对于需要长期使用的资源，包年包月可以降低长期成本，相比按需付费更为经济。

收费方式

包年包月是一种预付费模式，即先付费再使用。按月计费，以自然月为计费单位。

价格说明

性能保障型负载均衡包年包月计费方式的不同规格定价如下：

规格	价格（元/月）
标准型 I	360
标准型 II	720
增强型 I	1000
增强型 II	1300
高阶型 I	1800
高阶型 II	2500
超强型 I	4500
超强型 II	10000

查看费用账单

从天翼云的费用中心查看使用弹性负载均衡的费用账单。 查看入口：官网首页—>点击右上角账号头像显示下拉菜单—>选择费用中心，进入费用账单页面。

续费

性能保障型负载均衡有两种续订方式：

- 在弹性负载均衡控制台的弹性负载均衡实例列表页，选择 ELB 实例进行续费。

- 在费用中心管理控制台—>订单管理—>续订管理页面进行续费。

到期与通知

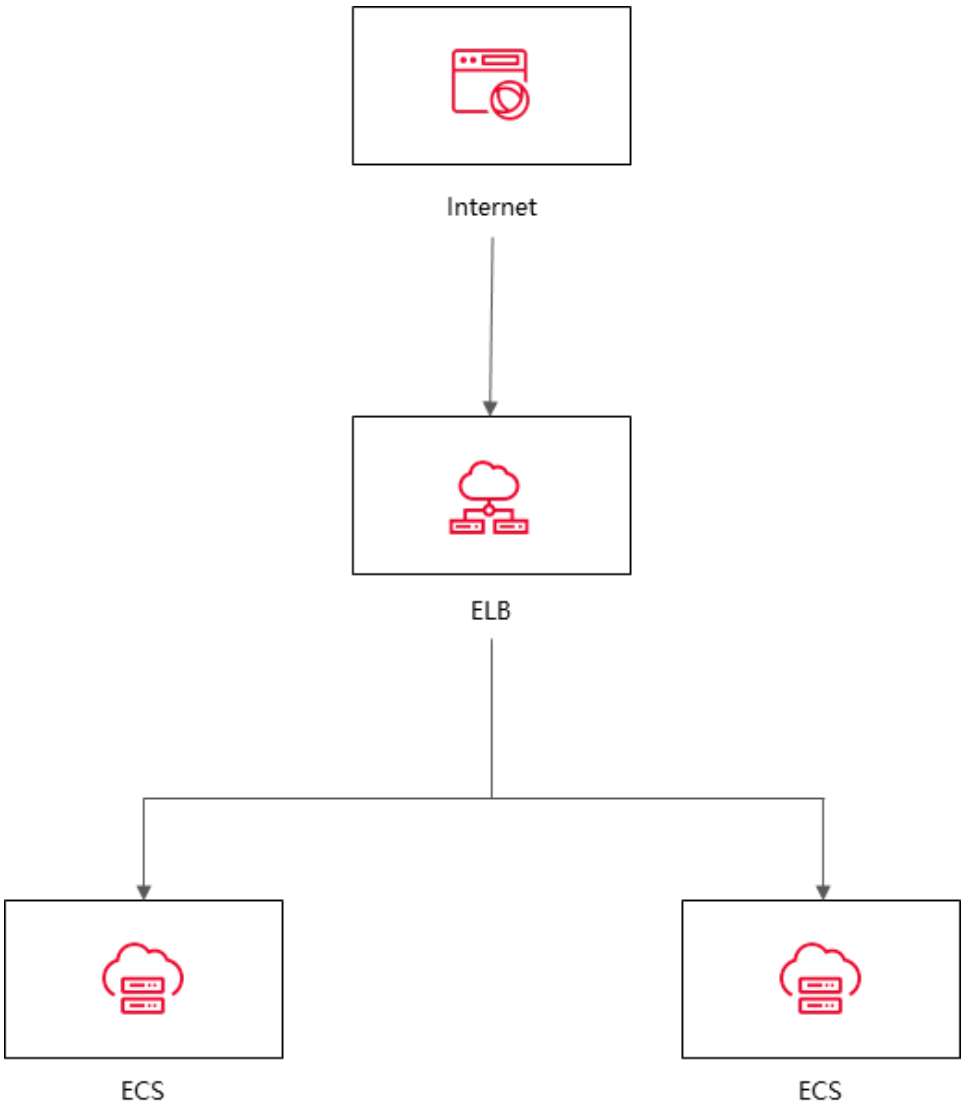
包年包月的弹性负载均衡实例到期时，将会被冻结。冻结期间，弹性负载均衡实例不能正常配置和转发流量。超期满 15 日后仍未续订的实例及配置将会被销毁，且无法恢复。相关通知计划如下：

- 提醒及通知方式：邮件、短信。
- 资源到期通知：弹性负载均衡实例到期前 7 天、3 天、1 天以及到期当天，会分别发送到期提醒。
- 资源释放通知：弹性负载均衡实例到期后 1 天、3 天、7 天，会分别发送释放提醒。
- 资源销毁通知：当用户的弹性负载均衡实例销毁后，会向用户发送 1 次销毁通知。

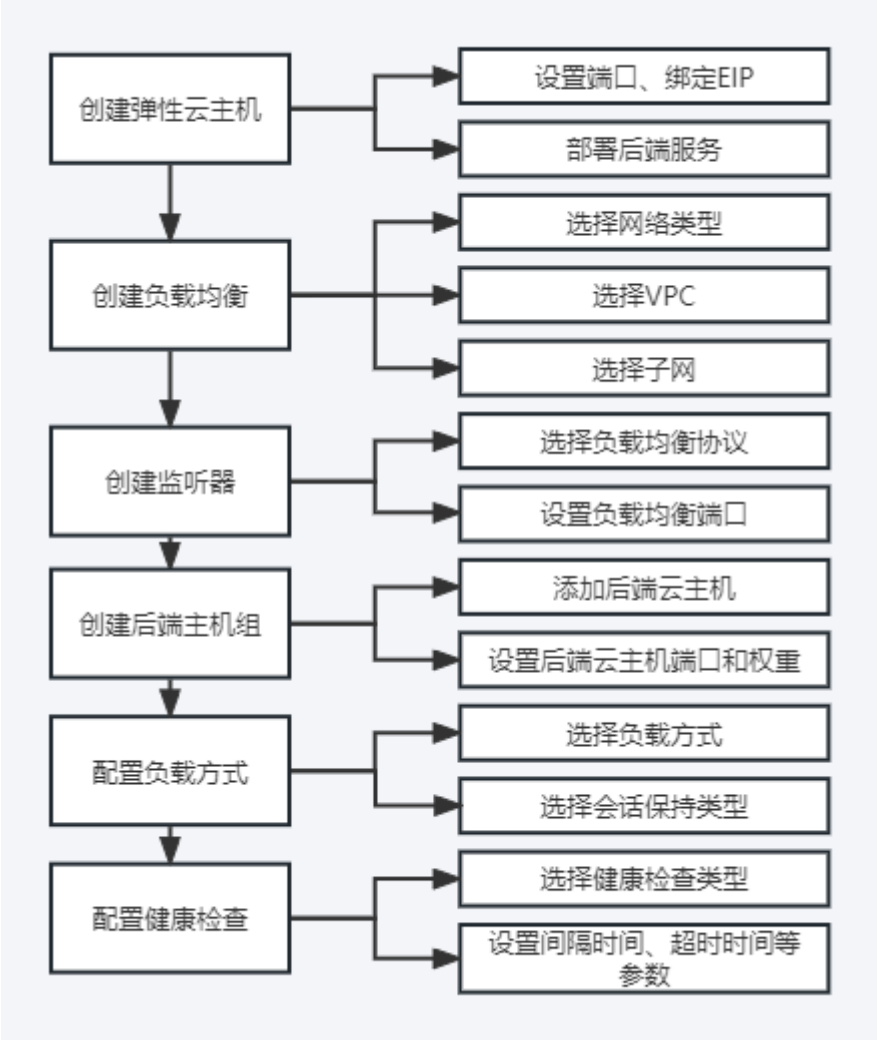
3 快速入门

3.1 入门概述

快速入门以具体场景为例，指引您使用弹性负载均衡快速创建一个负载均衡实例，将访问请求分发到配置的弹性云主机。



弹性负载均衡的配置流程如图所示：



3.2 准备工作

选择实例地域

弹性负载均衡默认不支持跨地域部署，请确保您选择的地域与 ECS 实例在同一个地域。举例来说明一下，ECS 实例所属地域为华东-华东 1，您规划的弹性负载均衡实例地域为华东-华东 1，ECS 实例和弹性负载均衡实例在同一个地域。

选择实例的网络类型

在创建负载均衡实例的时候可以选择不同的网络类型：

- 如果您需要使用负载均衡分发来自公网的请求，网络类型请选择外网，该实例拥有

一个公网 IP，用来接收来自互联网的请求。

- 如果您需要使用负载均衡分发来自私网的请求，网络类型请选择内网，当网络类型选择内网的时候，负载均衡虚拟 IP 可以自动分配也可以手动分配。

选择实例类型

您可以根据业务需求选择不同的负载均衡实例类型：

- 如果您的业务访问量较小，应用模型简单，可以选择经典型负载均衡，经典型负载均衡为免费产品。经典型负载均衡也具备基本的流量分发和健康检查功能。
- 如果您的业务对性能有较高的要求，可以选择性能保障型负载均衡，性能保障型负载均衡为收费产品。性能保障型负载均衡能够提供更强大的性能和扩展能力。

3.3 入门操作

3.3.1 操作场景

通过弹性云主机搭建服务（例如 Web 服务），当业务量大时单台云主机能力有限，需要两台同时进行业务负载。

本场景通过将弹性负载均衡和弹性云主机的组合使用，实现用户请求分均衡发至两台云主机。

3.3.2 创建弹性云主机

天翼云弹性负载均衡只负责将访问流量自动分发到多台弹性云主机上，不具备处理请求的能力。在当前场景中，需要通过弹性云主机实例来处理用户的请求。

弹性 IP（EIP）是可以独立申请的公网 IP 地址，包括公网 IP 地址与公网出口带宽服务。

在当前场景中，创建的弹性云主机需要与 EIP 绑定，后续操作需要使用浏览器进行公网 IP 地址访问，验证最终操作结果。具体操作，请参见创建弹性云主机。

1. 登录控制中心；
2. 在控制中心页面左上角点击  ，选择区域，本文我们选择华东 1；
3. 在控制中心页面，依次选择“计算>弹性云服务器”；
4. 在“弹性云服务器”界面单击“创建云主机”，根据界面提示配置参数，并单击“立即购买”。

示例中使用的两台弹性云服务器的规格如下：

参数项	参数值
实例名称	ecs-01、ecs-02
区域	华东-华东 1
操作系统	CentOS7.6
CPU	2vCPUs
内存	4GB
系统盘	40GB
数据盘	10GB
公网带宽	5 Mbit/s
安全组	默认安全组，开放 22、80 端口，实际业务中根据具体情况而定。
弹性 IP	自动分配
登录方式	密码
创建密码	自定义

3.3.3 搭建 Nginx 后端服务

在弹性云主机实例上部署 Nginx，设置 Nginx 的默认目录下的 index.html 页面内容，使访问 ecs-01 时返回一个标题为“Welcome to ecs-01”的页面，访问 ecs-02 时返回一个标题为“Welcome to ecs-02”的页面。主要是为了区分访问不同云主机实例时，返回的页面呈现效果不一样。具体步骤如下：

1. 登录弹性云服务器，具体操作请参见登录弹性云主机；
2. 安装 Nginx，执行以下命令，下载对应当前系统版本的 nginx 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.el7.ngx.noarch.rpm
```

3. 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.el7.ngx.noarch.rpm
```

4. 安装 Nginx，执行以下命令；

```
yum -y install nginx
```

5. 安装完成之后，启动 Nginx 并设置开机启动，执行以下命令；

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

6. 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；

7. 修改 ecs-01 的 index.html 页面，index.html 的默认目录是“/usr/share/nginx/html”，修改“index.html”页面，使访问 ecs-01 时返回一个标题为“Welcome to ecs-01”的页面；

   a. 进入到 index.html 所在的目录执行以下命令。

      cd /usr/share/nginx/html

   b. 执行以下命令打开文件“index.html”。

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

   c. 按 i 键进入编辑模式。修改 index.html 的文件内容，修改的部分如下所示：

```
...
<body>
 <h1>Welcome to <strong>ELB</strong> ecs-01</h1>

        <div class="content">

            <div class="alert">
                <h2>ELB01</h2>
                <div class="content">
```

```
                    <p><strong>Welcome to ecs-01</strong></p>
                    <p><strong>Welcome to ecs-01</strong></p>
                    <p><strong>Welcome to ecs-01</strong></p>
                </div>
            </div>
        </div>
    </body>
```

d. 按 Esc 退出编辑，输入:wq 保存后退出。

8. 修改 ecs-02 的 index.html 页面，index.html 的默认目录是“/usr/share/nginx/html”，修改“index.html”页面，使访问 ecs-02 时返回一个标题为“Welcome to ecs-02”的页面；

a. 进入到 index.html 所在的目录执行以下命令。

cd /usr/share/nginx/html

b. 执行以下命令打开文件“index.html”。

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

c. 按 i 键进入编辑模式。修改 index.html 的文件内容，修改的部分如下所示：

```
...
<body>
 <h1>Welcome to <strong>ELB</strong> ecs-02</h1>

        <div class="content">
```

```
            <div class="alert">
                <h2>ELB02</h2>
                <div class="content">
                    <p><strong>Welcome to ecs-02</strong></p>
                    <p><strong>Welcome to ecs-02</strong></p>
                    <p><strong>Welcome to ecs-02</strong></p>
                </div>
            </div>
        </div>
    </body>
```

d. 按 Esc 退出编辑，输入:wq 保存后退出。

9. 使用任意浏览器分别访问“http://ECS01 的公网 IP 地址”和“http://ECS02 的公网 IP 地址”，分别出现标题为“Welcome to ecs-01”和“Welcome to ecs-02”页面时，说明部署修改 html 页面成功。

3.3.4 创建负载均衡器

负载均衡实例接收来自客户端的请求，并按照监听规则将请求分发至后端服务器。使用 ELB 服务，您需要创建一个 ELB 实例，在实例中添加监听和后端服务器。

1. 登录天翼云控制中心，选择资源节点；本文我们选择的是华东-华东 1；
2. 在控制中心页面，依次选择“网络 >弹性负载均衡”；
3. 在网络控制台页面，点击“创建负载均衡”；
4. 在“创建负载均衡”页面，根据界面提示配置参数；

5. 点击“立即创建”；

6. 创建完成后，在“负载均衡器”界面，即可看到新建的负载均衡器；

7. 具体配置参数如下：

参数项	参数值
地域	华东-华东 1
类型	经典型
名称	CT-ELB 的名称，名称由数字、字母、中文、-、_组成，不能以数字、_和-开头。
所属 VPC	使用和 ECS 相同的 VPC
网络类型	外网
弹性 IP	使用已有
企业项目	default
描述	选填

3.3.5 添加监听器、后端服务器

配置完负载均衡实例后，需要为实例配置监听器。监听器负责检查连接请求，根据负载均衡算法和转发策略配置将请求流量分发到后端主机。具体步骤如下：

1. 登录天翼云控制中心，选择资源节点；本文我们选择的是华东-华东 1；

2. 在控制中心页面，依次选择“网络 > 弹性负载均衡”；

3. 在负载均衡页面，点击名称为 elb-01 的负载均衡器；

4. 在“监听器”页签，点击“添加监听器”；

5. 在“协议&监听器”页面，根据界面提示配置参数；

参数项	描述	参数值
名称	监听器的名称，名称应为 2-32 位，英文开头，支持大小写英文和数字。	listener01
负载均衡器协议/端口	协议可选择 TCP、UDP、HTTP、HTTPS，端口取值范围 1~65535。	HTTP/80
描述	关于监听器的描述。	选填

6. 点击“下一步”，新建后端主机组。配置参数如下：

参数项	描述	参数值
后端主机组名称	名称应为 2-32 位，英文开头，支持大小写英文和数字。	group01
选择后端主机组	一组处理负载均衡分发的前端请求的云主机实例。	云主机
可添加主机	可在搜索栏根据主机名、IP 地址搜索，勾选搜索结果中的云主机。	ecs-01、ecs-02
端口	后端云主机的服务监听端口，取值范围[1-65535]。	80
权重	后端云主机权重。权重值决定了后端云主机处理的请求的比例。例如，一个权重为 2 的云主机处理的请求数是权重为 1 的两倍。	用户自行配置权重大小。

7. 添加后端云主机后，点击“下一步”，进入“负载均衡方式&健康检查”配置页面。

具体配置参数如下：

参数项	描述	参数值
后端主机组名称	默认	group01
负载方式	可选择轮询算法、最少连接算法、源算法三种。 • 轮询算法：请求以轮询的方式依次分发给各后端主机，加权轮询对权重高的主机会获得更多的轮询次数； • 最小连接算法：动态调度算法，通过服务器当前活跃的连接数来评估服务器的负载情况，负载均衡将请求分发给活跃连接数最小的后端主机。加权最小连接数会结合权重分配后端主机； • 源算法：基于源 IP 地址的一致性哈希，相同的源地址会调度到相同的后端主机。	轮询算法
健康检测	开启健康检查，负载均衡对后端主机的服务状态进行探测。负载均衡将不会分发流量给服务异常的主机。	开启
健康检查类型	可选择 HTTP、TCP	HTTP
间隔时间（秒）	取值范围 1~20940	5
超时时间（秒）	取值范围 2~60	2

检查路径	长度范围 1~80 以 ‘/’ 开头，可包含数字、大小写字母或 ‘/’ ,路径中可包含 ‘-’ ‘_’ ‘.’ ‘=’	/
HTTP 方法	可选择 GET、HEAD 两种	GET

8. 点击“立即创建”，即可完成配置，在监听器页签能查看到创建的监听器。

3.3.6 验证负载均衡服务

配置完成负载均衡后，可以验证负载均衡是否生效。将域名映射到 ELB 实例的 EIP 上，然后可通过访问 ELB 实例对应的域名，验证是否实现访问到不同的后端服务器。

- 使用浏览器访问“http://www.xxx.com”，显示一个标题为“Welcome to ecs-01”的页面，说明本次访问请求被 ELB 实例转发到弹性云服务器"ecs-01"。
- 再次使用浏览器访问“http://www.xxx.com”，显示一个标题为“Welcome to ecs-02”的页面，说明本次访问请求被 ELB 实例转发到弹性云服务器"ecs-02"。

用户在实际使用弹性负载均衡时，应该根据自身业务和应用场景选择合适的配置方式和策略，以实现负载均衡、扩展性和高可用性等目标。

4 用户指南

4.1 负载均衡器

4.1.1 负载均衡器概述

负载均衡器是弹性负载均衡中分配和管理网络流量的关键组件，是承载业务的负载均衡服务实例，其作用是根据预先设定的规则，接收来自客户端的请求流量，并将流量分配到一个或多个可用的后端主机，以确保系统的稳定性和高可用性。创建负载均衡器后，您还需要添加监听器和后端主机，然后才能使用负载均衡服务提供的功能。

经典型和性能保障型负载均衡器

依据不同产品性能，天翼云提供经典型负载均衡器和性能保障型负载均衡器，您可以根据实际需求选择适合的配置。

- 经典型负载均衡

经典型负载均衡适用于访问量较小，应用模型简单的 web 业务，可满足大部分应用程序的负载均衡需求，具备基本的流量分发和健康检查功能。经典型负载均衡为免费规格，同 VPC 内多实例性能共享，为主备模式部署。

- 性能保障型负载均衡

性能保障型负载均衡适用于对性能有较高要求的应用场景，能够提供更强大的性能和扩展能力。性能保障型负载均衡为收费产品，为集群模式部署，支持经典型升级为性能保障型，支持规格升级、降级。

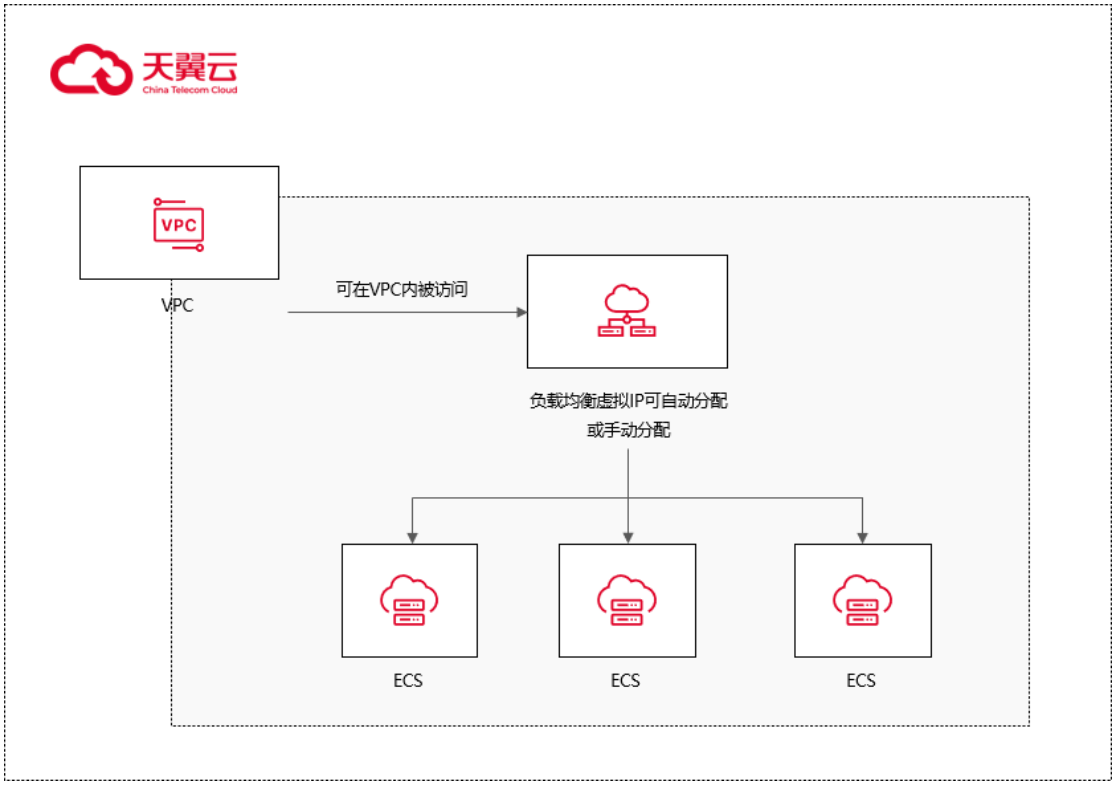
内网和外网负载均衡器

依据不同网络类型，天翼云还支持内网负载均衡器和外网负载均衡器。

- 内网负载均衡

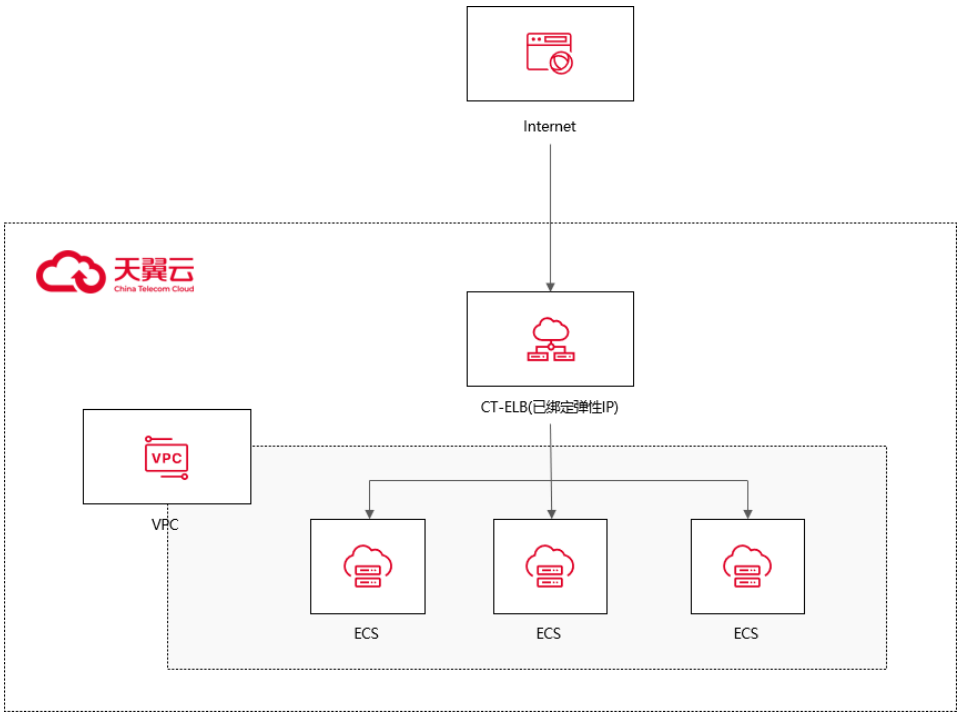
内网负载均衡通过内网 IP 地址对内部主机进行负载均衡，实现内部服务的高可用

性和性能优化，同时确保内网环境的安全性。



- 外网负载均衡

外网负载均衡可以将来自公网的流量均衡地分发到多个后端主机组，实现高可用性和性能的提升。



经典型/性能保障型与外网/内网的对应关系

经典型负载均衡器和性能保障型负载均衡器都可以用于内网和外网负载均衡。经典型负载均衡器适用于场景需求较为简单的应用，可以提供基本的负载均衡功能。性能保障型负载均衡器则专注于对性能要求更高的应用场景，提供更强大的性能和扩展能力。通过使用性能保障型负载均衡，您可以获得更高的负载性能、低延迟和更好的吞吐量。无论是内网还是外网负载均衡，您都可以根据实际需求选择适合的负载均衡器类型。无论是经典型还是性能保障型负载均衡器，您都可以根据实际需求选择将其用于内网或外网负载均衡。具体配置和使用方式请参考天翼云的帮助文档。

4.1.2 规划和准备

区域选择

选择靠近你的目标用户或数据源的云服务区域可以减少数据传输的延迟，提高系统性能和用户体验。

不同地区的定价可能有所不同，你可以根据自己的预算和需求选择最经济实惠的区域。

不同区域资源池的产品架构性能及其功能有所区别，具体可参考弹性负载均衡产品介绍>产品类型和规格>按资源池区分章节内容。

网络选择

天翼云支持内网负载均衡和外网负载均衡。

内网负载均衡通过内网 IP 地址对内部主机进行负载均衡，内网地址是在创建时根据所属 VPC 和子网自动创建的，目前不能修改。如果使用的是内网负载均衡，则不需要配置和购买带宽。如果为内网负载均衡绑定一个公网 EIP，则可作为公网负载均衡使用，同时可支持内网、公网访问。

外网负载均衡可以将来自公网的流量均衡地分发到多个后端主机组，实现高可用性和性能的提升。弹性负载均衡的公网 IP 地址是根据绑定的 EIP 来决定。

如果负载均衡当前已经绑定弹性 IP，则可进行弹性 IP 带宽的修改，带宽修改仅允许扩容不允许缩容。目前仅集群模式资源池支持负载均衡 IPv6 带宽，主备、集群模式资源池列表见产品简介>产品类型和规格>按资源池区分，实际情况以控制台展现为准。

产品类型

天翼云弹性负载均衡产品按性能可划分如下经典型负载均衡和性能增强型负载均衡，您可以根据实际需求选择适合的负载均衡器型号和配置。具体可参考产品介绍>产品类型和规格>按产品性能区分章节内容。

协议类型

负载均衡提供四层 TCP/UDP 协议和七层 HTTP/HTTPS 协议监听，可根据应用场景选择合适的监听协议。

监听协议	说明	使用场景
TCP	面向连接的协议，在发送数据之前需要经过三次握手建立可靠的连接； 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，如邮件服务、文件传输服务； 无特殊要求的 web 应用；
UDP	无连接协议，发送数据前不需要建立连接，直接发送数据，不提供差错恢复和数据重传; 可靠性相对较低，需要上层协议做可靠性措施; 数据传输快;	适用于对实时性要求较高，对可靠性要求相对不高的业务，如语音、视频、证券行情实时推送等。
HTTP	应用层协议，基于 TCP 协议，B/S 架构，浏览器请求数据，服务端响应数据; 基于 cookie 做会话保持 l 使用 X-forwarded-for 头字段获取客户端真实 IP 地址;	需要对数据内容进行识别的应用，如 web 应用、门户网站等
HTTPS	加密的 HTTP 传输协议，可阻止未经授权的访问;	对安全性要求较高的 HTTP 应用 需要加密传输的应用

监听协议	说明	使用场景
	统一的证书管理服务，可将证书传至负载均衡，由负载均衡终结处理客户的 HTTPS 请求	

负载方式

在为业务配置负载均衡时，需要选择合适的流量负载方式，对流量进行负载分发，可避免服务器负载不均，部分服务器负载过高影响服务性能，天翼云弹性负载均衡提供以下负载方式供您选择：

轮询算法：请求以轮询的方式依次分发给各后端主机，加权轮询对权重高的主机会获得更多的轮询次数；

最小连接算法：动态调度算法，通过主机当前活跃的连接数来评估主机的负载情况，负载均衡将请求分发给活跃连接数最小的后端主机。加权最小连接数会结合权重分配后端主机；

源算法：基于源 IP 地址的一致性哈希，相同的源地址会调度到相同的后端主机。

后端云主机

在使用负载均衡器之前，需要先创建弹性云主机实例并在其上部署相关的业务应用。然后，将这些云主机实例添加到负载均衡器的后端主机组，以处理来自客户端的请求转发。在创建后端主机时，需要注意以下几点：

地域一致性：确保后端服务器实例和负载均衡器位于相同的地域，避免潜在的网络延迟和性能问题。

操作系统一致性：建议选择相同操作系统的后端服务器实例，以便统一操作系统配置和软件环境，简化管理任务。

4.1.3 创建负载均衡器

前提条件

在您创建负载均衡器前，确保您已经做好了相关准备，按需选择您需要的网络类型、产品类型并进行相关配置。具体请参考规划和准备。

使用须知

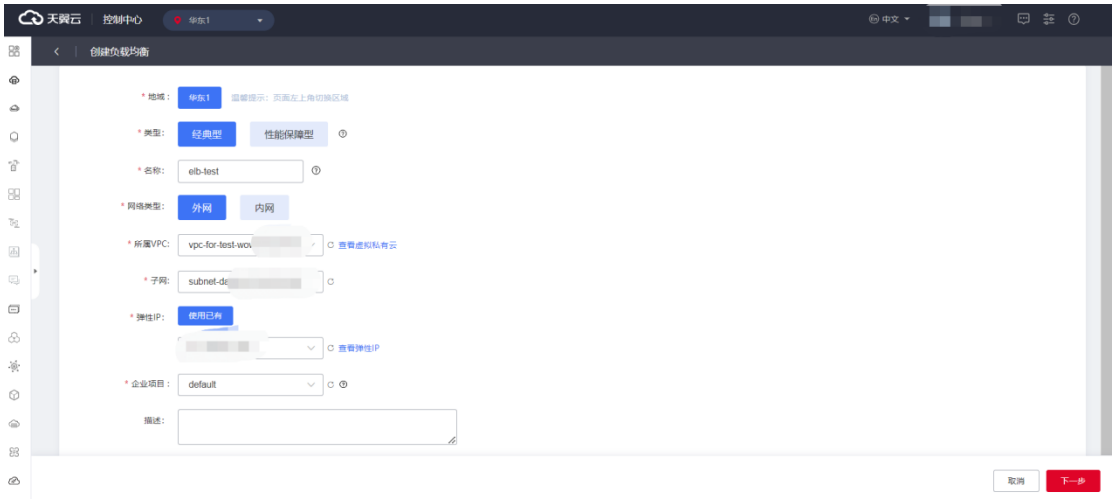
- 负载均衡器创建后，不支持修改 VPC。如果要修改 VPC，请重新创建负载均衡器，并选择对应的 VPC。
- 如果子网未开启 IPv6,则负载均衡不支持 IPv6。如果子网已开启 IPv6,则负载均衡支持 IPv6。
- 如果只需要 IPv6 公网，可以创建内网负载均衡后绑定 IPv6 公网带宽。目前仅集群资源池支持负载均衡 IPv6，主备、集群模式资源池列表见产品简介>产品类型和规格>按资源池区分，实际情况以控制台展现为准。

操作步骤

1. 点击天翼云门户首页的“控制中心”，输入登录的用户名和密码，进入控制中心页面。
2. 在管理控制台上方单击图标，选择区域，本文操作均选择华东-华东 1。
3. 在系统首页，选择“网络>弹性负载均衡>负载均衡器”。

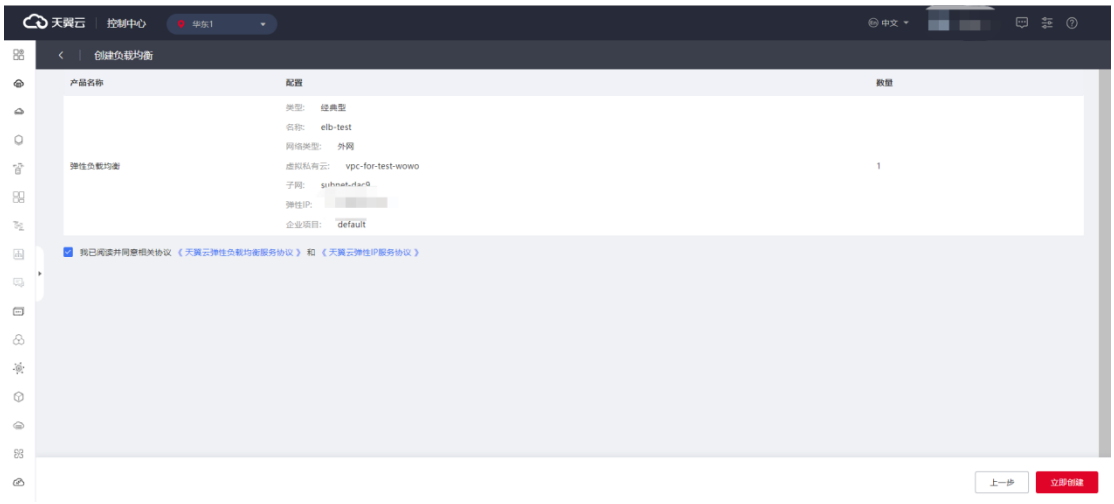
4. 单击“创建负载均衡”，进入负载均衡创建页面。

5. 按需选择产品类型、网络类型等配置。各配置项详细说明，请参考负载均衡器配置说明。



6. 在“确认配置”页面，检查确认负载均衡器的相关配置。

7. 勾选我已阅读并同意相关协议-《天翼云负载均衡服务等级协议》、《天翼云弹性 IP 服务协议》，点击“立即创建”。



8. 创建负载均衡器一般需要几分钟，请耐心等待。用户可前往控制台查看负载均衡器的状态，当其状态变为“运行中”时，表示负载均衡器创建完成。

负载均衡器配置说明

参数	**说明**
地域	选择对应的区域资源池，本文选择华东-华东 1。
类型	可选经典型或性能保障型。
名称	负载均衡器的名称。
网络类型	可选外网或者内网。外网：选择外网，出现“弹性 IP”字段，目前只支持使用已有的弹性 IP。外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行处理。需要绑定一个已有的 EIP。（注意：如果只需要 IPv6 公网，则可以创建内网负载均衡后绑定 IPv6 公网带宽。目前仅集群资源池支持负载均衡 IPv6，主备、集群模式资源池列表见产品简介>产品类型和规格>按资源池区分，实际情况以控制台展现为准。内网：选择内网，出现”负载均衡虚拟 IP”字段，可选择”自动分

参数	说明
	配”或“手动分配”。内网负载均衡器通过内网 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。
所属 VPC	所属虚拟私有云。您可以选择使用已有的虚拟私有云网络，或者创建新的虚拟私有云。更多关于虚拟私有云的信息，请参见《虚拟私有云用户指南》。
子网	所属子网。注意：如果子网未开启 IPv6,则负载均衡不支持 IPv6。如果子网已开启 IPv6,则负载均衡支持 IPv6。
规格	规格参数为典型场景的测试数据，性能保障型有此字段，您可以根据实际需要选择标准型 I、标准型 II、增强型 I、增强型 II 或高阶型 I。
企业项目	选择所述的企业项目名称。
计费方式	经典型为经典型负载均衡产品免费提供，性能保障型负载均衡为收费产品，当前仅支持包年/包月方式计费。
计费周期	性能保障型负载均衡有此字段，通过滑轨选择，可选 1-11 个月，1/2/3 年。
描述	可添加负载均衡器相关描述。

4.1.4 查询负载均衡器

操作场景

您已经创建了负载均衡器，创建的在负载均衡器信息列表可见，且处于“运行中”状态。

在控制中心的“弹性负载均衡”界面的信息列表，可以查看已创建负载均衡器的状态、子网等详细信息。

操作步骤

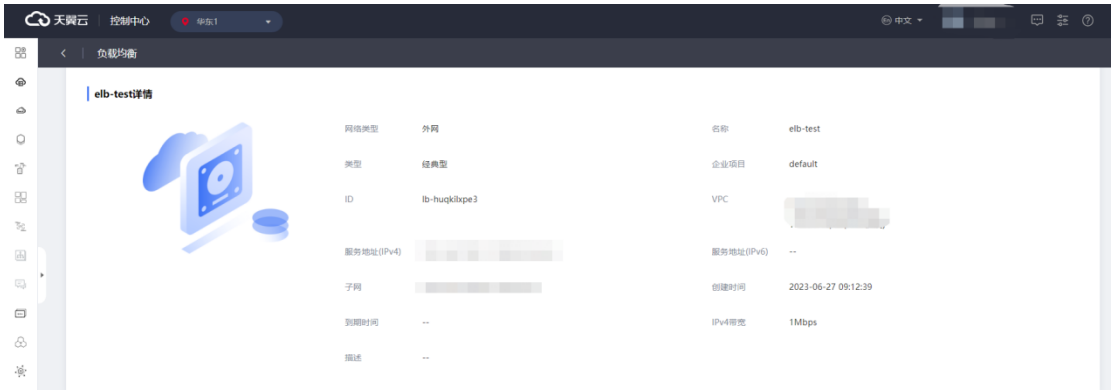
1. 点击天翼云门户首页的“控制中心”,输入登录的用户名和密码,进入控制中心页面。

2. 在管理控制台顶端单击图标，选择区域，本文选择华东-华东 1。

3. 在系统首页，选择“网络>弹性负载均衡>负载均衡器”。

4. 在负载均衡器信息列表右上角的下拉框中，可设置通过名称、服务地址等参数搜索负载均衡器。

5. 单击负载均衡器名称，进入负载均衡器详情页面，查看负载均衡器的详细信息。



4.1.5 续订性能保障型负载均衡

操作场景

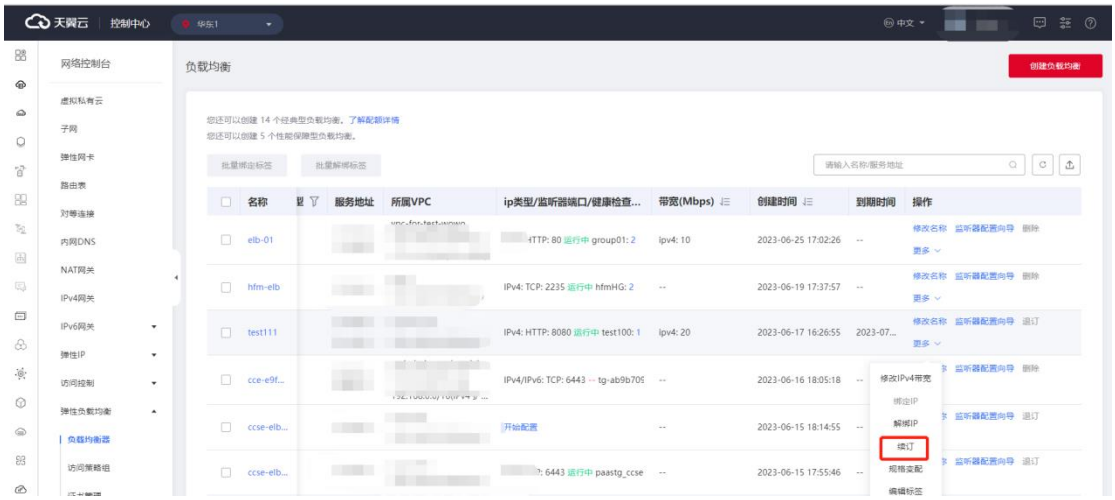
如果您已经创建并购买了性能保障型负载均衡，您需要根据规定的续订期限来续订服务。

如果您的业务增长或发生变化，您可能需要调整负载均衡器的配置。在这种情况下，您可能需要在合适的时机续订负载均衡服务以适应新的需求。

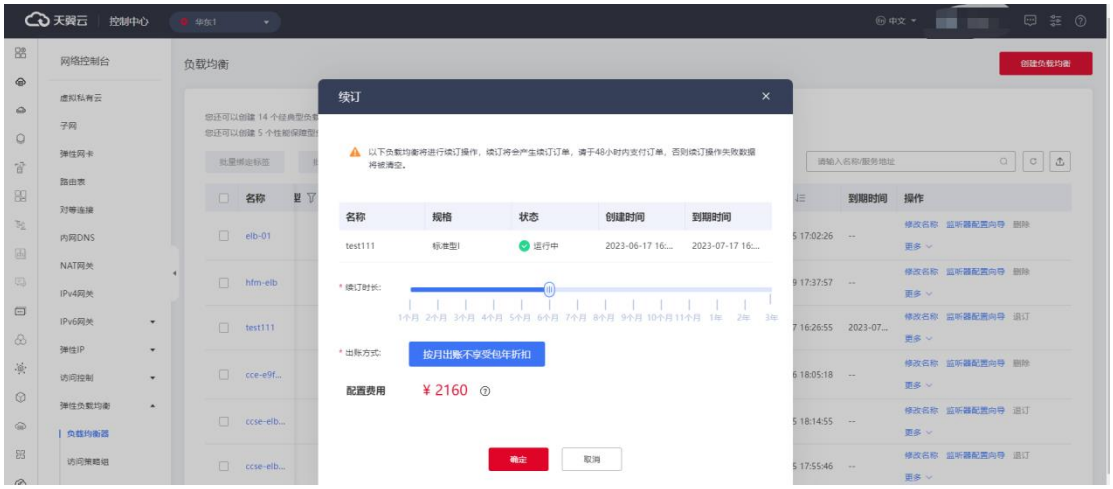
操作步骤

1. 登录天翼云控制中心。

2. 在“负载均衡器”列表页面，单击负载均衡器所在行的“更多>续订“按钮。



3. 在弹出的续订窗口，选择续订时长，完成续订操作。



4.1.6 经典型升级性能保障型

操作场景

随着业务规模发展，存量经典型实例的性能无法满足业务需求时，可选择升级性能保障型，以获得更高的负载性能和性能保障

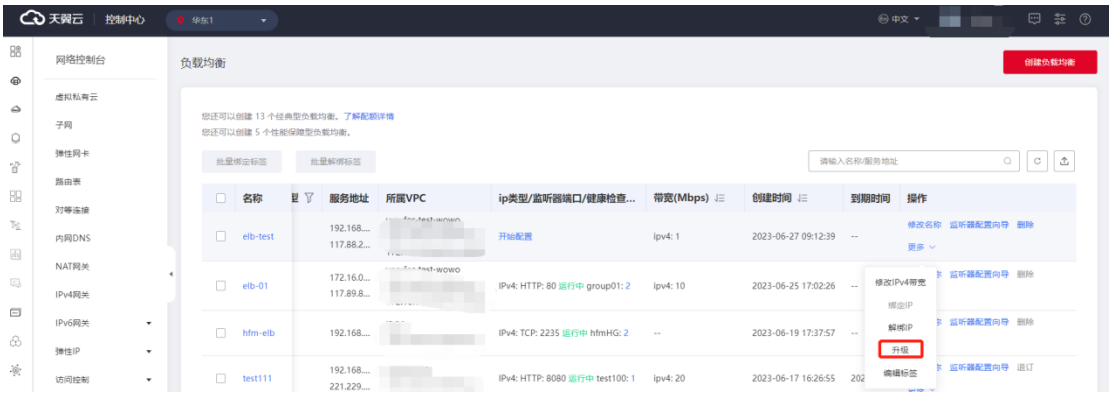
使用须知

经典型升级性能保障型，升级过程涉及底层迁移，有秒级流量中断，建议在业务低谷时段维护窗口操作。

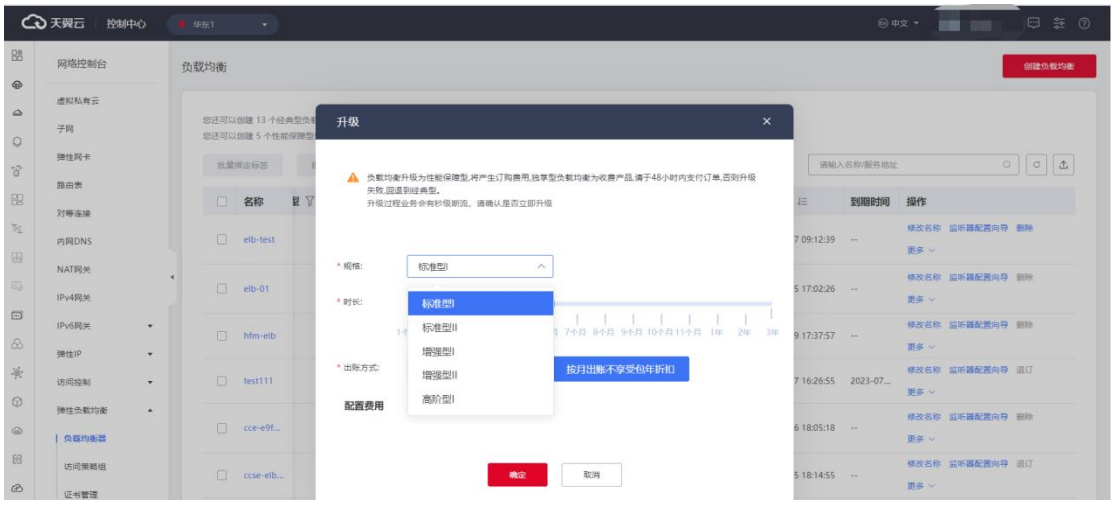
操作步骤

负载均衡支持从免费的经典型升级成性能规格更强的性能保障型。可在控制台执行升级：

1. 登录天翼云控制中心。
2. 选择“网络>弹性负载均衡>负载均衡器”。
3. 在“负载均衡器”列表页面，单击经典型负载均衡器所在行的“升级”按钮。



4. 在弹出的升级窗口，选择要升级的性能保障型规格，选择订购时长，完成升级操作。



注意：经典型升级性能保障型涉及配置迁移，有秒级业务中断，请谨慎操作。

4.1.7 性能保障型规格变配

前提条件

在您需要改变性能保障型负载均衡器规格前，您需要了解具体规格相关参数，具体参见产品简介>产品类型和规格。

操作场景

当用户业务快速增长，当前规格无法满足性能要求时，可使用规格变配功能，平滑升级更高规格；

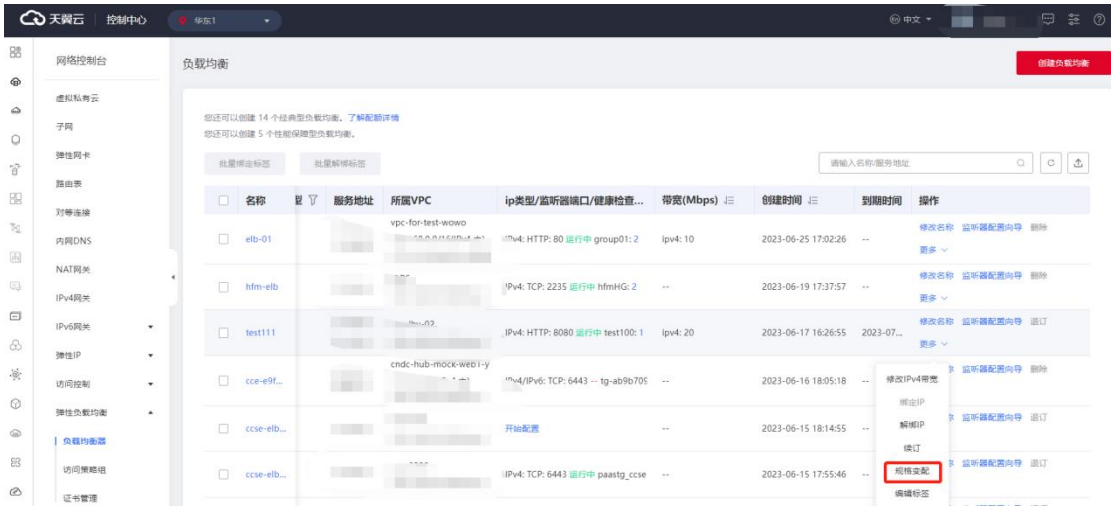
用户购买规格过大，或业务量出现持续一段时间的低谷时，可选择降配，将大规格降低成小规格，节省使用成本；

操作步骤

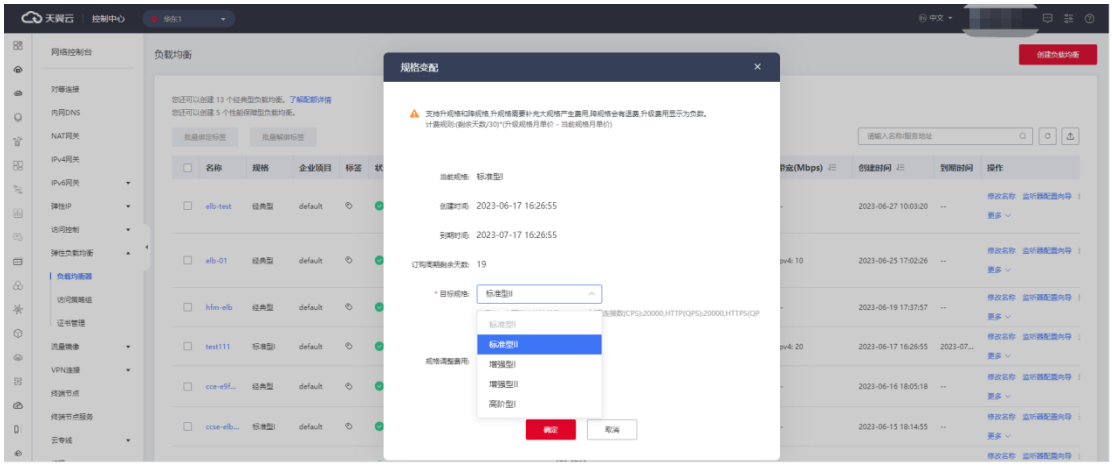
性能保障型负载均衡支持规格调整，可升规格或降规格，可在控制台执行规格变配，具体操作步骤如下：

1. 登录天翼云控制中心。
2. 选择“网络>弹性负载均衡>负载均衡器”。

3. 在“负载均衡器”列表页面，单击性能保障型负载均衡器所在行的“规格变配”按钮。



4. 在弹出的规格变配窗口，选择要调整到的目标规格，点击“确定”，完成变配操作。



4.1.8 删除负载均衡器

操作场景

如果您的业务需求发生变化，不再需要负载均衡器来分配流量和请求，那么您可以考虑删除负载均衡器。

使用须知

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

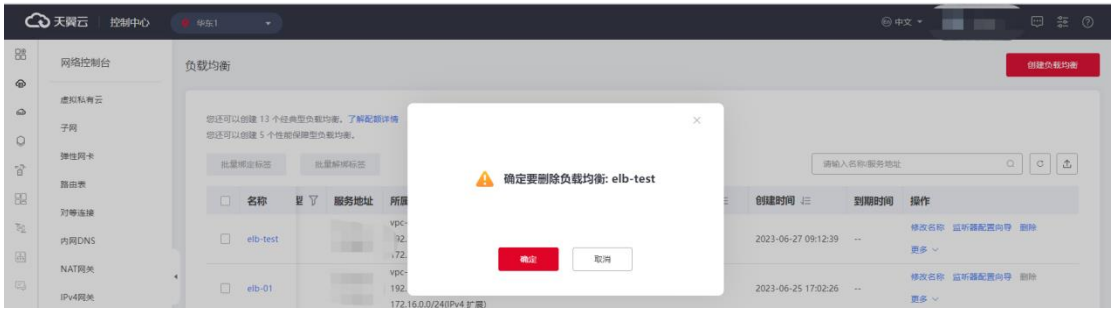
弹性 IP 不会被默认自动删除，不影响弹性 IP 的正常使用。

前提条件

- 如果该负载均衡器下有监听器，不能删除，需先删除监听器后才可删除负载均衡器。
- 如果监听器对应的后端主机组添加了后端主机，请删除所有后端主机。
- 如果监听器配置了转发策略，需要删除所有转发策略。
- 如果配置了 HTTP 监听器重定向至 HTTPS 监听器，需要删除所有重定向。

操作步骤

1. 登录天翼云控制中心。
2. 选择“网络>弹性负载均衡>负载均衡器”。
3. 在“负载均衡器”界面，找到目标实例，单击负载均衡器所在行的“删除”按钮。
4. 在确认对话框单击“确定”，则可删除指定负载均衡器。



4.1.9 负载均衡绑定/解绑弹性 IP

- **绑定弹性 IP**

操作场景：

如果负载均衡器当前未绑定弹性 IP，您可以根据业务需要为负载均衡器绑定弹性 IP。

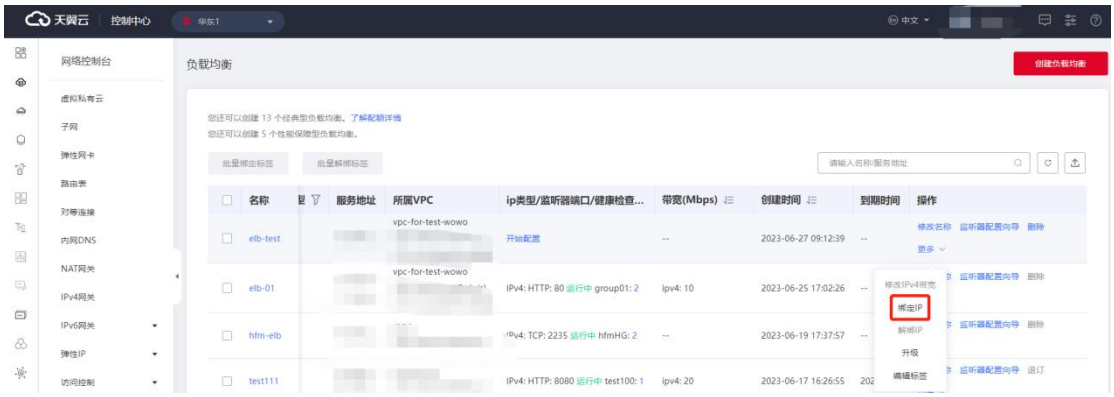
操作步骤：

1.点击天翼云门户首页的“控制中心”，输入登录的用户名和密码，进入控制中心页面。

2.在管理控制台上方单击图标，选择区域，本文操作均选择华东-华东 1。

3.在系统首页，选择“网络>弹性负载均衡>负载均衡器”。

4.在“负载均衡器”列表页面，单击负载均衡器所在行的“更多>绑定 IP”，进行弹性 IP 绑定。



- **解绑弹性 IP**

操作场景：

如果负载均衡当前已经绑定弹性 IP，则可以解除弹性 IP 的绑定。

操作步骤:

1.点击天翼云门户首页的“控制中心”，输入登录的用户名和密码，进入控制中心页面。

2.在管理控制台上方单击图标，选择区域，本文操作均选择华东-华东 1。

3.在系统首页，选择“网络>弹性负载均衡>负载均衡器”。

4.在“负载均衡器”列表页面，单击负载均衡器所在行的“更多>解绑 IP”，进行弹性 IP 绑定。

4.1.10 负载均衡修改 IPv4 带宽

操作场景

如果负载均衡当前已经绑定弹性 IP，则可以在点击“修改 IPv4 带宽”进行弹性 IP 带宽的修改。

使用须知

带宽修改仅允许扩容不允许缩容。

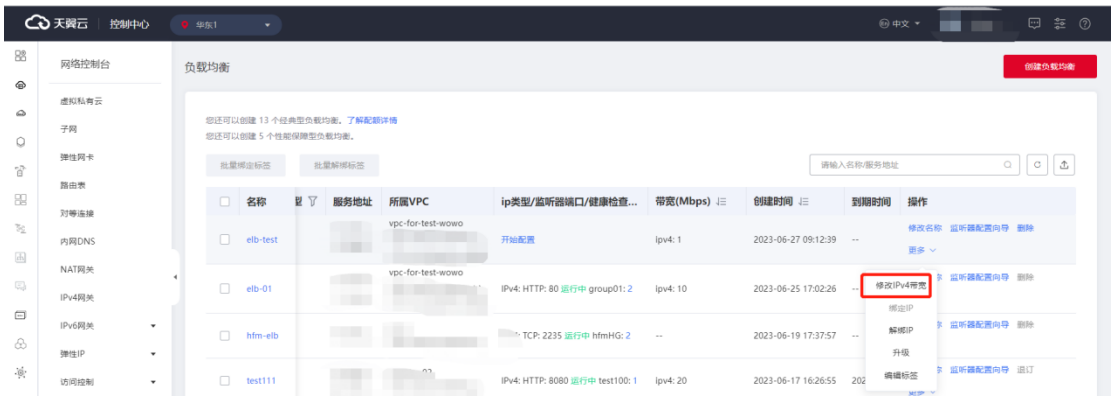
操作步骤

1.点击天翼云门户首页的“控制中心” ,输入登录的用户名和密码,进入控制中心页面。

2.在管理控制台上方单击图标，选择区域，本文操作均选择华东-华东 1。

3.在系统首页，选择“网络>弹性负载均衡>负载均衡器”。

4.在“负载均衡器”列表页面，单击负载均衡器所在行的“更多>修改 IPv4 带宽”。



4.1.11 负载均衡绑定/解绑 IPv6 带宽

弹性负载均衡支持绑定 IPv6 带宽的操作，本文帮助您快速熟悉负载均衡对 IPv6 带宽的绑定。

- **绑定 IPv6 带宽**

前提条件

如果子网已经开启 IPv6，在负载均衡创建时会自动分配 IPv6 地址，实现支持 IPv6 的效果。此时 IPv6 为内网 IPv6 地址，如果需要被公网访问或访问公网，需绑定 IPv6 带宽。

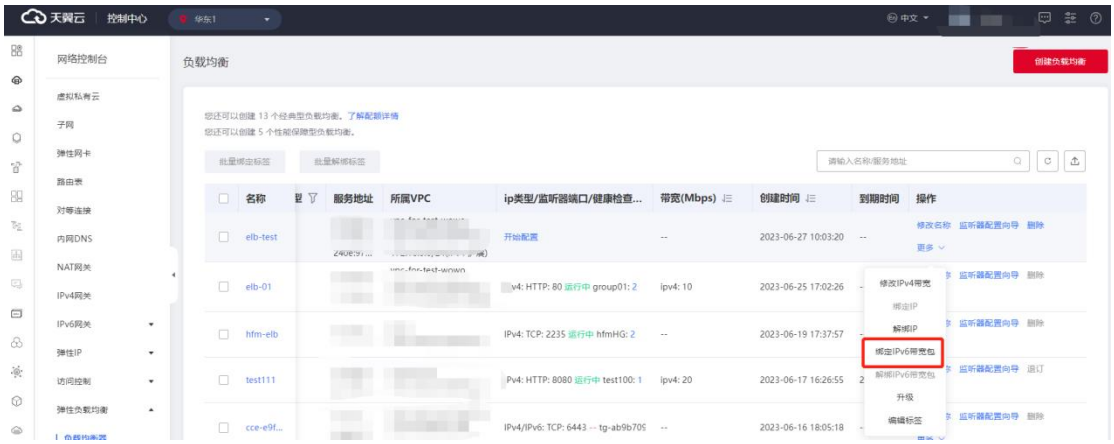
操作步骤

1.点击天翼云门户首页的“控制中心”，输入登录的用户名和密码，进入控制中心页面。

2.在管理控制台上方单击图标，选择区域，本文操作均选择华东-华东 1。

3.在系统首页，选择“网络>弹性负载均衡>负载均衡器”。

4.在“负载均衡器”列表页面，单击负载均衡器所在行的“更多>绑定 IPv6 带宽包”，进行 IPv6 带宽的绑定。



- **解绑绑定 IPv6 带宽**

前提条件

如果已经绑定 IPv6 带宽，根据业务需要，可以进行 IPv6 带宽的解绑。

操作步骤：

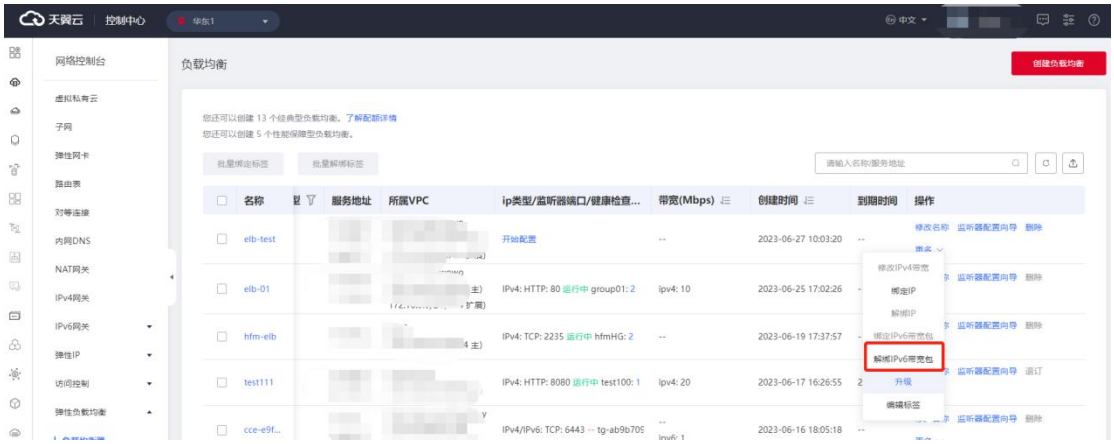
1.点击天翼云门户首页的“控制中心”，输入登录的用户名和密码，进入控制中心页面。

2.在管理控制台上方单击图标，选择区域，本文操作均选择华东-华东 1。

3.在系统首页，选择“网络>弹性负载均衡>负载均衡器”。

4.在“负载均衡器”列表页面，单击负载均衡器所在行的“更多>绑定 IPv6 带宽包”，

进行 IPv6 带宽的解绑。



4.1.12 负载均衡标签管理

操作场景

当您的云环境中存在多个弹性负载均衡器时，编辑使用标签可以帮助您对其进行分类分组管理，对弹性负载均衡器的使用情况进行追踪和优化，提高弹性负载均衡器的管理效率和灵活性。

负载均衡器的编辑标签时，通常需要指定标签键和标签值来标识和分类负载均衡器。标签键用于描述标签的分类或属性，而标签值则用于具体区分不同的负载均衡器。

使用须知

- 您可以最多添加 10 个标签。
- 标签的“键”和“值”是一一对应的，其中“键”值是唯一的。

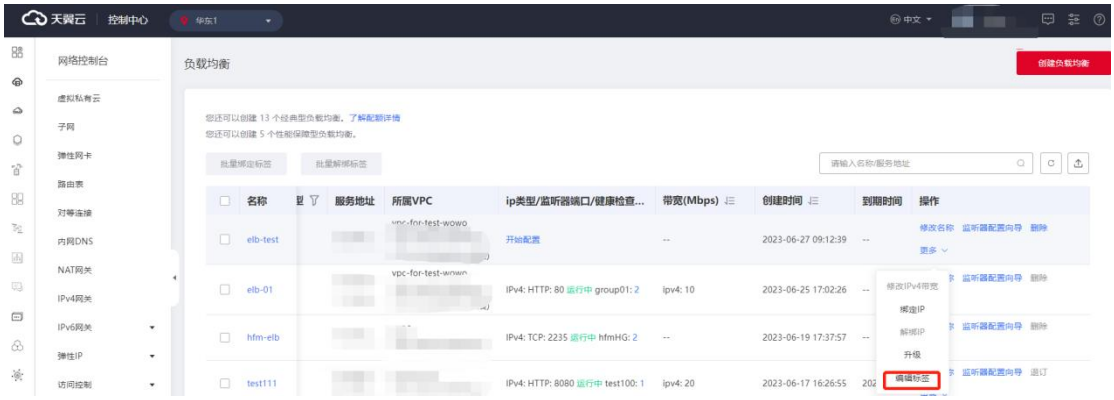
添加标签

1.点击天翼云门户首页的“控制中心”，输入登录的用户名和密码，进入控制中心页面。

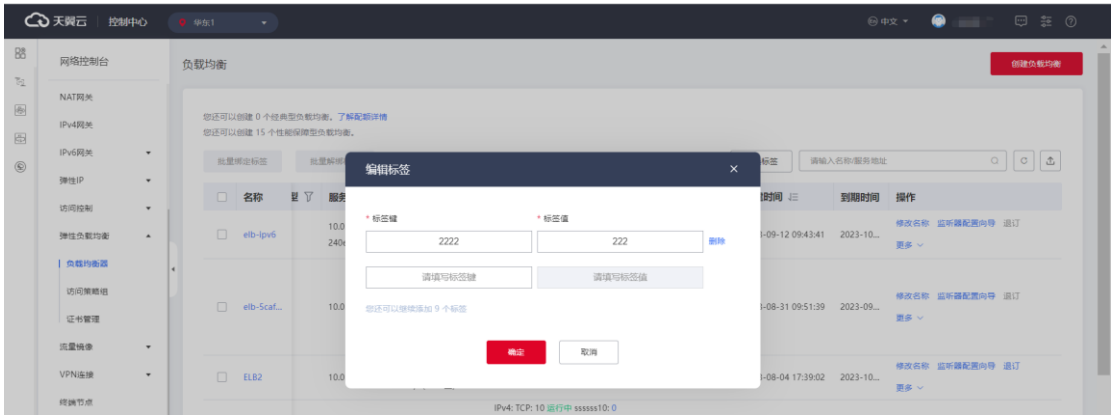
2.在管理控制台上方单击图标，选择区域，本文操作均选择华东-华东 1。

3.在系统首页，选择“网络>弹性负载均衡>负载均衡器”。

4.在“负载均衡器”列表页面，单击负载均衡器所在行的“更多>编辑标签”。



5. 输入标签键和标签值，点击“确定”。



6.在控制中心的“弹性负载均衡”界面的信息列表，还支持对已创建的负载均衡器批量编辑标签/批量解绑标签。

修改标签

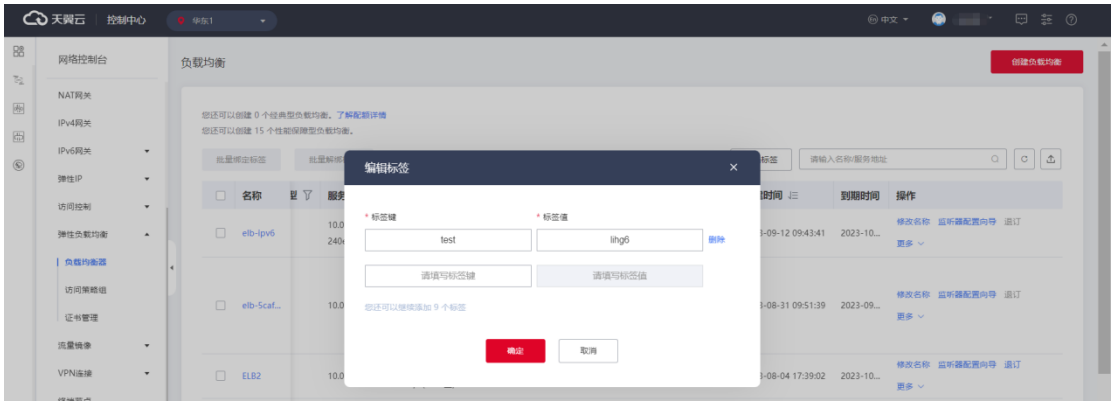
1.点击天翼云门户首页的“控制中心”，输入登录的用户名和密码，进入控制中心页面。

2.在管理控制台上方单击图标，选择区域，本文操作均选择华东-华东 1。

3.在系统首页，选择“网络>弹性负载均衡>负载均衡器”。

4.在“负载均衡器”列表页面，单击负载均衡器所在行的“更多>编辑标签”。

5.在弹出的标签页，输入修改的“键”和“值”。



6.点击“确定”，完成标签修改。

删除标签

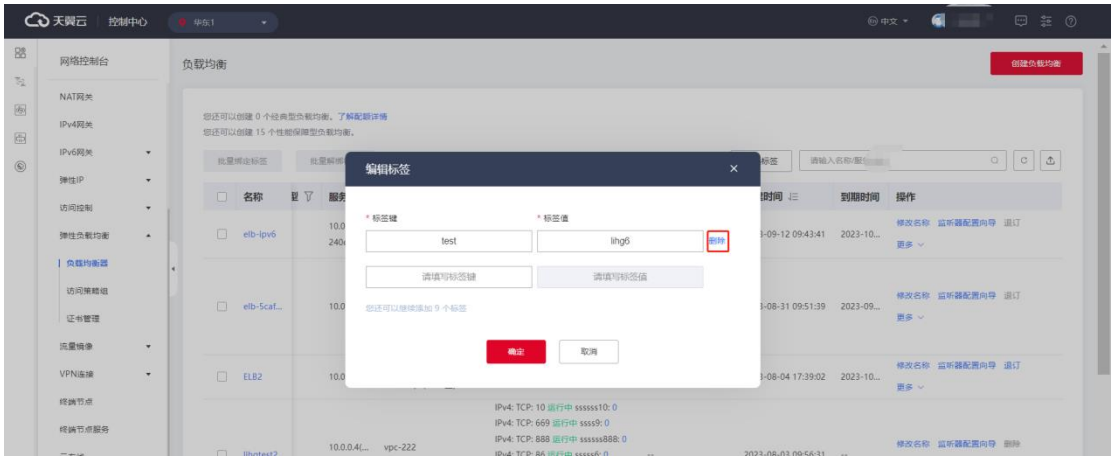
1. 点击天翼云门户首页的“控制中心”,输入登录的用户名和密码 ,进入控制中心页面。

2. 在管理控制台上方单击图标 ，选择区域，本文操作均选择华东-华东 1。

3. 在系统首页，选择“网络>弹性负载均衡>负载均衡器”。

4. 在“负载均衡器”列表页面，单击负载均衡器所在行的“更多>编辑标签”。

5. 在弹出的标签页，选择要删除的标签，点击指定标签所在行的“删除”。



6. 点击“确定”，完成标签删除。

4.1.13 退订负载均衡

操作场景

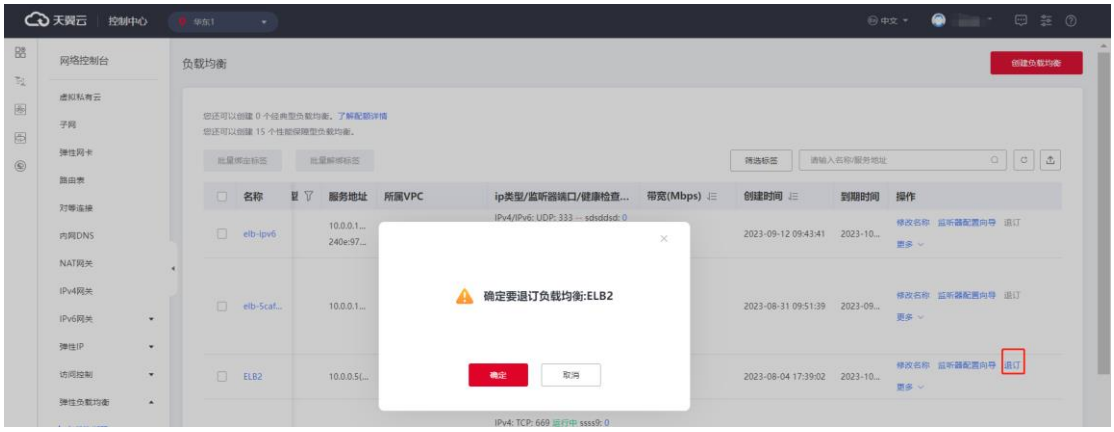
如果您购买了性能保障型负载均衡，因业务调整需要退订或更换其他产品，您可进行性能保障型负载均衡退订操作。

注意事项

如果该负载均衡器下有监听器，不能退订，需先删除监听器，具体操作步骤详见删除监听器。退订事宜具体以合同签订为准，退订规则详见退订规则说明。已续订或超过7天的性能保障型负载均衡不支持退订。

操作步骤

1. 点击天翼云门户首页的“控制中心”,输入登录的用户名和密码 ,进入控制中心页面。
2. 在管理控制台上方单击图标 ，选择区域，本文操作均选择华东-华东 1。
3. 在系统首页，选择“网络>弹性负载均衡>负载均衡器”。
4. 在“负载均衡器”界面，找到目标实例，单击负载均衡器所在行的“退订”按钮。
5. 在确认对话框单击“确定”，进入退订管理/退订申请页面。



6. 在退订申请页面，确认需退订的弹性负载均衡产品信息，选择退订原因，勾选“我已

确认本次退订金额和相关费用”。

7. 点击“退订”，退订申请提交成功。

8. 您可以在订单详情中查看退订进度。完成退订操作。

4.2 监听器

监听器使用前端（客户端到负载均衡器）连接的协议以及端口和后端（负载均衡器到后端弹性云主机）连接的协议以及端口配置负载均衡策略。负载均衡器支持协议 TCP、UDP、HTTP、HTTPS。负载均衡器可以监听的端口范围为 1-65535。

4.2.1 监听器概述

监听器负责检查连接请求，根据负载均衡算法和转发策略配置将请求流量分发到后端主机。

负载均衡提供四层 TCP/UDP 协议和七层 HTTP/HTTPS 协议监听，可根据应用场景选择合适的监听协议：

监听协议	说明	使用场景
TCP	● 面向连接的协议，在发送数据之	● 适用于注重可靠性、对数据准

	前需要经过三次握手建立可靠的连接。 ● 基于源地址的会话保持。 ● 数据传输快。	确性要求高，如邮件服务、文件传输服务。 ● 无特殊要求的 web 应用。
UDP	● 无连接协议，发送数据前不需要建立连接，直接发送数据，不提供差错恢复和数据重传。 ● 可靠性相对较低，需要上层协议做可靠性措施。 ● 数据传输快。	● 适用于对实时性要求较高，对可靠性要求相对不高的业务，如语音、视频、证券行情实时推送等。
HTTP	● 应用层协议，基于 TCP 协议，B/S 架构，浏览器请求数据，服务端响应数据。 ● 基于 cookie 做会话保持。 ● 使用 X-forwarded-for 头字段获取客户端真实 IP 地址。	● 需要对数据内容进行识别的应用，如 web 应用、门户网站等。
HTTPS	● 加密的 HTTP 传输协议，可阻止未经授权的访问。 ● 统一的证书管理服务，可将证书传至负载均衡，由负载均衡终结处理客户的 HTTPS 请求。	● 对安全性要求较高的 HTTP 应用。 ● 需要加密传输的应用。

4.2.2 协议和端口

监听器的协议和端口即是弹性负载均衡提供服务时接收请求的端口。弹性负载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。

协议	支持端口
TCP	• 端口范围：1-65535 • 同一个弹性负载均衡实例下，不同监听器的端口不能相同
UDP	
HTTP	
HTTPS	

4.2.3 添加监听器

4.2.3.1 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的场景，如邮件服务、文件传输服务和远程登陆等。

前提条件

您已经创建了弹性负载均衡器。具体操作详见创建弹性负载均衡器。

操作步骤

步骤一：创建监听器

1.登录弹性负载均衡控制台。

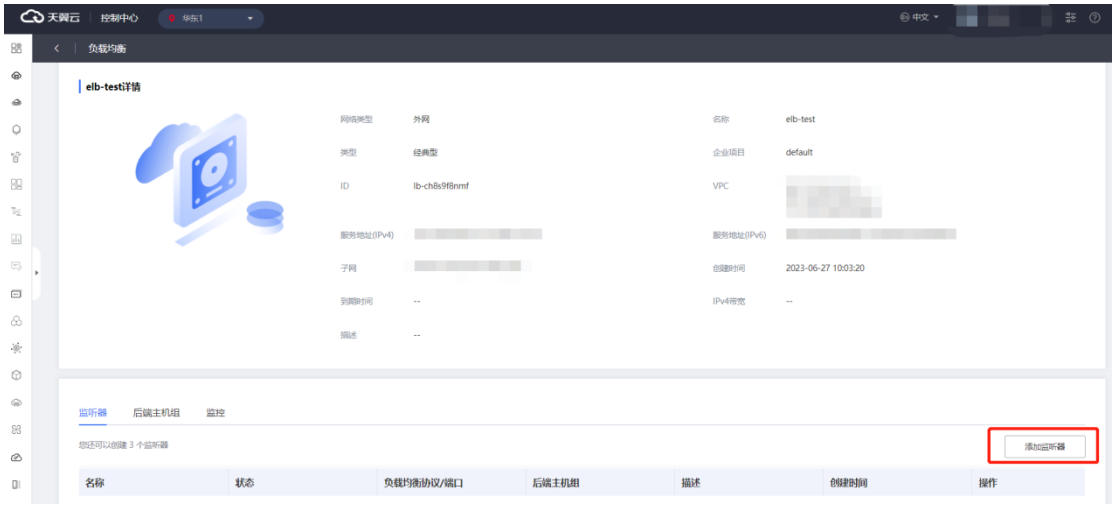
2.在顶部右侧选择弹性负载均衡所属区域，本文选择华东-华东 1。

3.选择以下一种方法打开监听器配置向导。

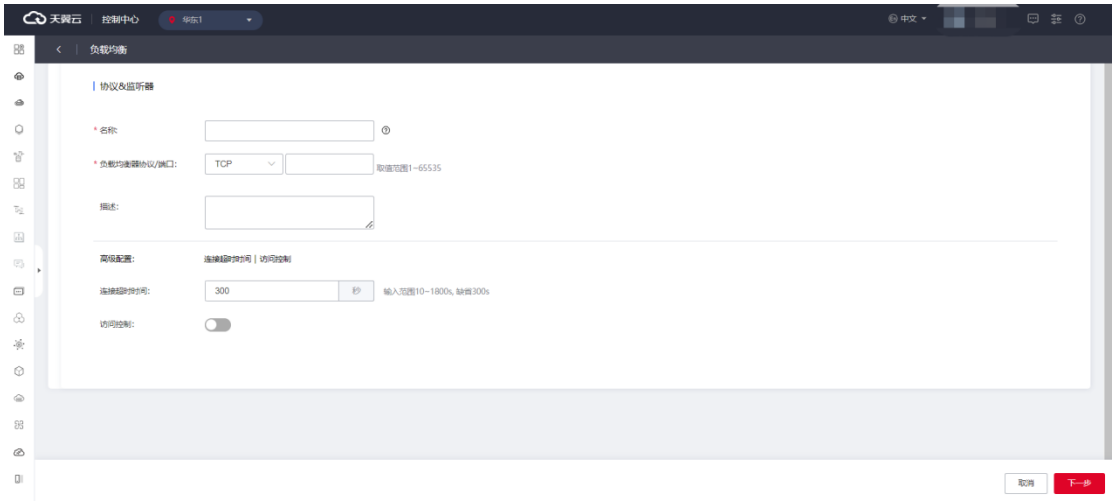
- 在负载均衡器列表页面，找到目标实例，在操作列单击“监听器配置向导”。

- 在 ip 类型/监听器端口/健康检查/服务器组列下方单击“开始配置”。

- 在负载均衡器列表页面，找到目标实例，单击实例名称进入实例详情页，单击“添加监听器”。



4.在协议&监听配置向导完成相关参数配置，具体可参考 TCP 监听器配置说明，然后点击“下一步”。



TCP 监听器配置说明

监听配置	说明
名称	设置监听器的名称，名称应为 2-32 位，英文开头，支持大小写英文和数字。
负载均衡器协议/端口	下拉列表选择 TCP 协议，输入监听端口，取值范围 1~65535
描述	可选，填写监听器描述
高级配置	监听器的特定参数配置：连接超时时间|访问控制

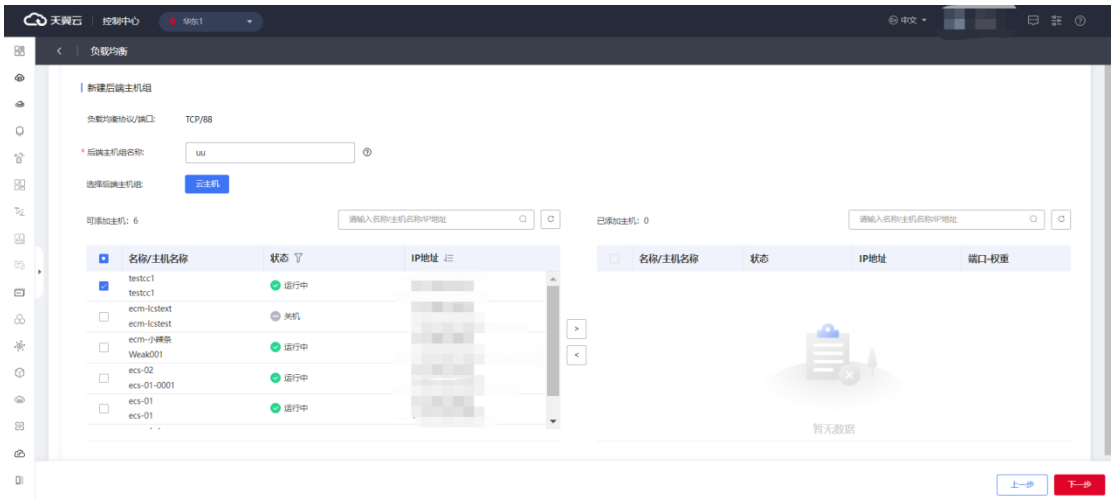
连接超时时间	仅集群资源池支持设置 TCP 连接的超时时间，主备、集群模式资源池列表见产品简介>产品类型和规格>按资源池区分，实际情况以控制台展现为准。
访问控制	选择是否开启访问控制。开启访问控制后，选择一种访问控制方式：黑名单、白名单。并设置访问策略组作为该监听器的白名单或黑名单。 ● 白名单：允许特定 IP 访问负载均衡，仅转发来自所选访问策略组中设置的 IP 地址或地址段的请求，白名单适用于只允许特定 IP 访问的场景。 ● 黑名单：禁止特定 IP 访问负载均衡，不转发来自所选访问策略组中的 IP 或地址段，黑名单适用于只限制禁止特定 IP 访问的场景

步骤二：添加后端主机组

添加处理前端请求的后端云主机组。

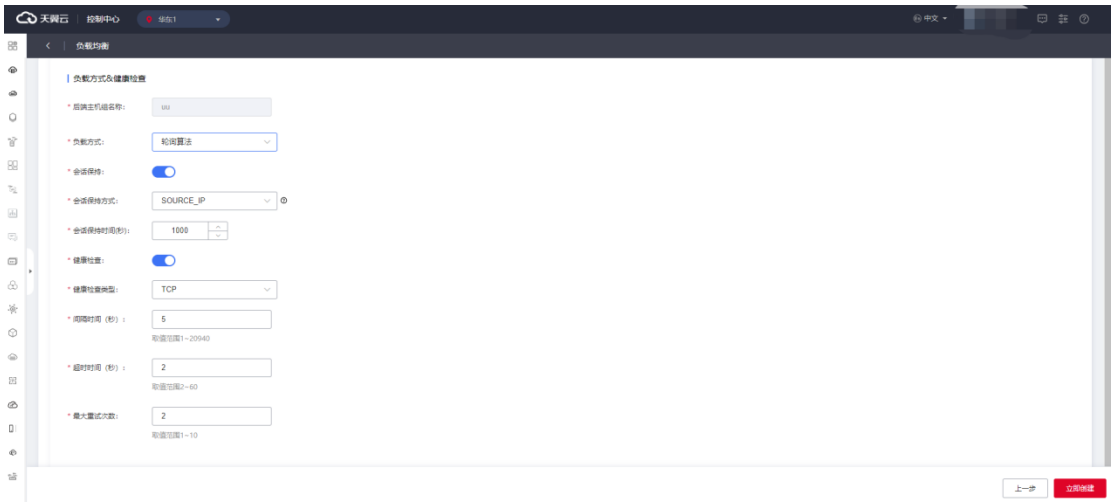
1.设置后端主机组名称。

2.从主机列表中选择可添加的云主机，然后点击“下一步”，即完成后端云主机的添加。



步骤三：进行负载方式和健康检查配置。

参考 TCP 监听器负载方式&健康检查配置说明完成步骤三后，点击“立即创建”，完成 TCP 监听器创建。



TCP 监听器负载方式&健康检查配置说明

负载方式&健康检查配置	说明
负载方式	从下拉列表框选择负载方式 ● 轮询算法：请求以轮询的方式依次分发给各后端主机，加权轮询对权重高的主机会获得更多的轮询次数； ● 最小连接算法：动态调度算法，通过主机当前活跃的连接数来评估主机的负载情况，负载均衡将请求分发给活跃连接数最小的后端主机。加权最小连接数会结合权重分配后端主机； ● 源算法：基于源 IP 地址的一致性哈希，相同的源地址会调度到相同的后端主机。
会话保持	选择是否开启会话保持。

	开启会话保持后，负载均衡监听器会把来自同一客户端的访问请求分发到同一台后端主机上。
会话保持方式	TCP 协议的会话保持方式为 SOURCE_IP 方式。即来自同一 IP 地址的访问请求转发到同一台后端主机上。
会话保持时间	设置会话保持的时间，取值范围为 1- 86400，缺省 1000s
健康检查	开启健康检查，负载均衡对后端主机的服务状态进行探测。负载均衡将不会分发流量给服务异常的主机。
健康检查类型	TCP，TCP 协议监听器只可选 TCP。
间隔时间	健康检查的检查间隔，缺省 5s
超时时间	健康检查超时时间，缺省 2s
最大重试次数	健康检查的重试次数，缺省 2，连续检查失败达到重试次数，则判断健康检查失败。

4.2.3.2 添加 UDP 监听器

操作场景

UDP 协议适用于对实时性要求较高 ,对可靠性要求相对不高的业务 ,如语音、视频、证券行情实时推送等。

前提条件

您已经创建了弹性负载均衡实例。具体操作参考创建弹性负载均衡器。

操作步骤

步骤一：创建监听器

1.登录弹性负载均衡控制台。

2.在顶部右侧选择负载均衡所属区域，本文选择华东-华东 1。

3.选择以下一种方法打开监听器配置向导。

- 在负载均衡器列表页面，找到目标实例，在操作列单击“监听器配置向导”。
- 在 ip 类型/监听器端口/健康检查/服务器组列下方单击“开始配置”。
- 在负载均衡器列表页面 ,找到目标实例 ,单击实例名称进入实例详情页 ,单击“添加监听器”。

9. 在协议&监听配置向导参考 UDP 监听器配置说明， 完成相关配置，然后点击“下一步”。

UDP 监听器配置说明

监听配置	**说明**
名称	设置监听器的名称，名称应为 2-32 位，英文开头，支持大小写英文和数字。
负载均衡器协议/端口	下拉列表选择 UDP 协议，输入监听端口，取值范围 1~65535
描述	可选，填写监听器描述
访问控制	选择是否开启访问控制。开启访问控制后，选择一种访问控制方式：黑名单、白名单。并设置访问策略组作为该监听器的白名单或黑名单。 ● 白名单：允许特定 IP 访问负载均衡，仅转发来自所选访问策略组中设置的 IP 地址或地址段的请求，白名单适用于只允许特定 IP 访问的场景。

	● 黑名单：禁止特定 IP 访问负载均衡，不转发来自所选访问策略组中的 IP 或地址段，黑名单适用于只限制特定 IP 访问的场景

步骤二：添加后端主机组

添加处理前端请求的后端主机组。

1.设置后端主机组名称。

2.选择后端主机类型，仅可选云主机。

3.从主机列表中选择可添加的云主机，然后点击“下一步”，即完成后端云主机的添加。

步骤三：参考 UDP 监听器负载方式&健康检查配置说明，完成负载方式和健康检查配置。完成步骤三后，点击立即创建，完成 UDP 监听器创建。

UDP 监听器负载方式&健康检查配置说明

负载方式&健康检查配置	说明
负载方式	从下拉列表框选择负载方式，UDP 协议只支持选择轮询算法和最小连接算法。 ● 轮询算法：请求以轮询的方式依次分发给各后端主机，加权轮询对权重高的主机会获得更多的轮询次数。 ● 最小连接算法：动态调度算法，通过主机当前活跃的连接数来评估主机的负载情况，负载均衡将请求分发给活跃连接数最小的后端主机。加权最小连接数会结合权重分配后端主机。 ● 源算法：基于源 IP 地址的一致性哈希，相同的源地

	址会调度到相同的后端主机。
会话保持	选择是否开启会话保持。 开启会话保持后，负载均衡监听器会把来自同一客户端的访问请求分发到同一台后端主机上。
会话保持方式	UDP 协议的会话保持方式为 SOURCE_IP 方式。即来自同一 IP 地址的访问请求转发到同一台后端主机上。
会话保持时间	设置会话保持的时间，取值范围为 1- 86400，缺省 1000s。
健康检查	开启健康检查，负载均衡对后端主机的服务状态进行探测。负载均衡将不会分发流量给服务异常的主机。
健康检查类型	UDP，UDP 协议监听器只可选 UDP。
间隔时间	健康检查的检查间隔，缺省 5s。
超时时间	健康检查超时时间，缺省 2s。
最大重试次数	健康检查的重试次数，缺省 2，连续检查失败达到重试次数，则判断健康检查失败。

4.2.3.3 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、门户网站等。

前提条件

您已经创建了弹性负载均衡实例。具体操作详见创建弹性负载均衡器。

步骤一：创建监听器

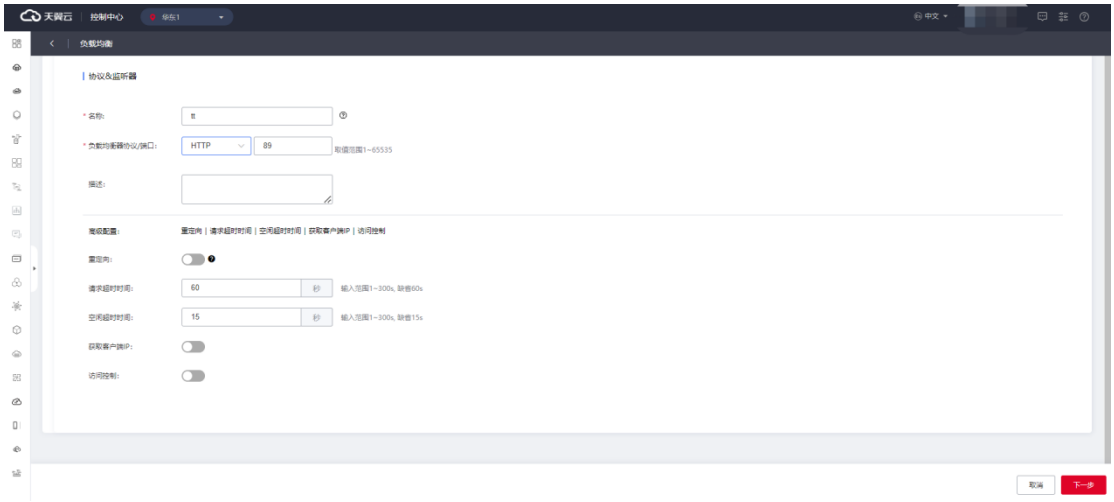
1.登录弹性负载均衡弹性负载均衡控制台；

2.在顶部右侧选择弹性负载均衡所属区域，本文选择华东-华东 1；

3.选择以下一种方法打开监听器配置向导。

- 在负载均衡器列表页面页面，找到目标实例，在操作列单击“监听器配置向导”。
- 在 ip 类型/监听器端口/健康检查/服务器组列下方单击“开始配置”。
- 在负载均衡器列表页面，找到目标实例，单击“实例名称”进入实例详情页，单击添加“监听器”。

4.在协议&监听配置向导依据 HTTP 监听器配置说明完成以下配置，然后点击下一步。



HTTP 监听器配置说明

监听配置	说明
名称	设置监听器的名称，名称应为 2-32 位，英文开头，支持大小写英文和数字。
负载均衡器协议/端口	下拉列表选择 HTTP 协议，输入监听端口，取值范围 1~65535。
描述	可选，填写监听器描述。
高级配置	监听器的特定参数配置：重定向|请求超时时间|空闲超

	时时间|获取客户端 IP|访问控制。
重定向	仅集群模式资源池支持开启重定向，将把此 HTTP 监听器的访问请求重定向至选定的 HTTPS 监听器。主备、集群模式资源池列表见产品简介>产品类型和规格>按资源池区分，实际情况以控制台展现为准。 此功能方便业务从 HTTP 迁移至 HTTPS 的场景，可将习惯性访问 HTTP 的客户端平滑迁移到 HTTPS。 前置条件：需要预先配置好 HTTPS 监听器。 开启重定向后，下方出现重定向至选项，从下拉列表框选择目标 HTTPS 监听器。 注意：只能重定向至 HTTPS 监听器，并且每个监听器只能重定向一次。开启重定向功能后，如需获取源 IP 能力，请在重定向后监听器开启。
请求超时时间	输入范围 1~300s，缺省 60s。 集群模式资源池支持设置 HTTP 请求超时时间，在请求超时时间内接收请求的后端主机无响应，负载均衡会向所有其它后端主机重试请求。主备、集群模式资源池列表见产品简介>产品类型和规格>按资源池区分，实际情况以控制台展现为准。 如果重试所有后端主机一直没有响应，则负载均衡会给客户端返回 HTTP 504 错误码。
空闲超时时间	输入范围 1~300s，缺省 15s。

	集群模式资源池支持设置 HTTP 连接的空闲超时时间。在空闲超时时间后仍没有访问请求，负载均衡会中断当前连接。主备、集群模式资源池列表见产品简介>产品类型和规格>按资源池区分，实际情况以控制台展现为准。
获取客户端 IP	开启获取客户端 IP，将通过 X-Forwarded-for 头字段携带客户端源真实 IP。集群模式资源池支持 X-Forwarded-Proto 来获取客户端与负载均衡监听连接时所用的协议（HTTP/HTTPS），支持 X-Forwarded-Port 获取客户端与负载均衡监听连接时所用的端口。主备、集群模式资源池列表见产品简介>产品类型和规格>按资源池区分，实际情况以控制台展现为准。
访问控制	选择是否开启访问控制。开启访问控制后，选择一种访问控制方式：黑名单、白名单。并设置访问策略组作为该监听器的白名单或黑名单。 ● 白名单：允许特定 IP 访问负载均衡，仅转发来自所选访问策略组中设置的 IP 地址或地址段的请求，白名单适用于只允许特定 IP 访问的场景。 ● 黑名单：禁止特定 IP 访问负载均衡，不转发来自所选访问策略组中的 IP 或地址段，黑名单适用于只限制特定 IP 访问的场景。

步骤二：添加后端主机组

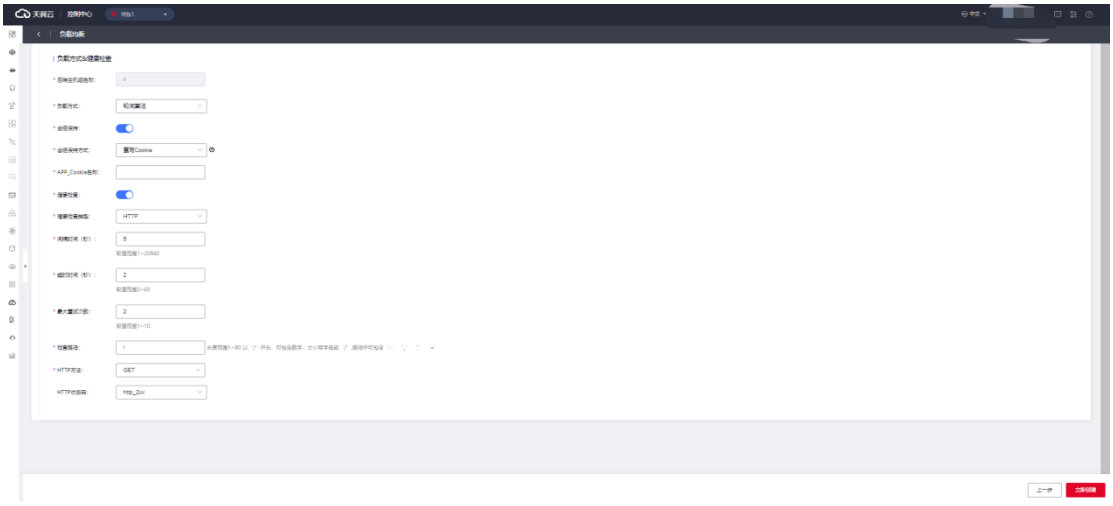
添加处理前端请求的后端主机组。

1. 设置后端主机组名称。

2. 选择后端主机类型，仅可选云主机。

3.从主机列表中选择可添加的云主机，然后点击“下一步”，即完成后端云主机的添加。

步骤三：参考 HTTP 监听器负载方式&健康检查配置说明，完成负载方式和健康检查配置。



完成步骤三后，点击“立即创建”，完成 HTTP 监听器创建。

HTTP 监听器负载方式&健康检查配置说明

负载方式&健康检查配置	说明
负载方式	从下拉列表框选择负载方式 ● 轮询算法：请求以轮询的方式依次分发给各后端主机，加权轮询对权重高的主机会获得更多的轮询次数； ● 最小连接算法：动态调度算法，通过主机当前活跃的连接数来评估主机的负载情况，负载均衡将请求分发给活跃连接数最小的后端主机。加权最小连接数会结

	合权重分配后端主机；
会话保持	选择是否开启会话保持。 开启会话保持后，负载均衡监听器会把来自同一客户端的访问请求分发到同一台后端主机上。
会话保持方式	集群模式资源池 HTTP 协议的会话保持方式支持如下 • 重写 cookie/植入 cookie。 • 植入 cookie：客户端首次访问时，负载均衡在返回请求中植入 cookie（即在 HTTP 或 HTTPS 响应报文中插入 ServerID），下次客户端携带此 cookie 访问，负载均衡会将请求转发给之前记录到的后端云主机上。植入 cookie 需要指定会话保持时间。 • 重写 cookie：负载均衡对用户自定义的 cookie 进行重写，下次客户端携带新的 cookie 访问，负载均衡会将请求转发给之前记录到的后端云主机； • 选择植入 cookie 时，可设置会话保持超时时间。缺省 3600s。 • 选择重写 cookie，负载均衡发现用户自定义的 cookie，对原来的 cookie 进行重写，下次客户端携带新的 cookie 访问，负载均衡服务将请求定向转发给之前记录到的后端主机。重写

	cookie 方式该 cookie 的会话保持时间由后端主机维护。
健康检查	开启健康检查，负载均衡对后端主机的服务状态进行探测。负载均衡将不会分发流量给服务异常的主机。
健康检查类型	可选 HTTP 或 TCP。
间隔时间	健康检查的检查间隔，缺省 5s
超时时间	健康检查超时时间，缺省 2s
最大重试次数	健康检查的重试次数，缺省 2，连续检查失败达到重试次数，则判断健康检查失败。
检查路径	可设置 HTTP 健康检查的路径，长度范围 1~80 以‘/’开头，可包含数字、大小写字母或‘/’,路径中可包含‘-’ ‘_’ ‘.’ ‘=’。
HTTP 方法	可选 GET 或 HEAD。
WebSocket 支持	选用 HTTP 监听时，默认支持无加密版本 WebSocket 协议（WS 协议）。仅集群资源池支持，主备、集群模式资源池列表见产品简介>产品类型和规格>按资源池区分，实际情况以控制台展现为准。
HTTP 状态码	选择 HTTP 健康检查范围的状态码，可选 http_2xx，http_3xx，http_4xx，http_5xx。

4.2.3.4 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。

前提条件

您已经创建了弹性负载均衡实例。具体操作详见创建负载均衡器。

操作步骤

步骤一：创建监听器

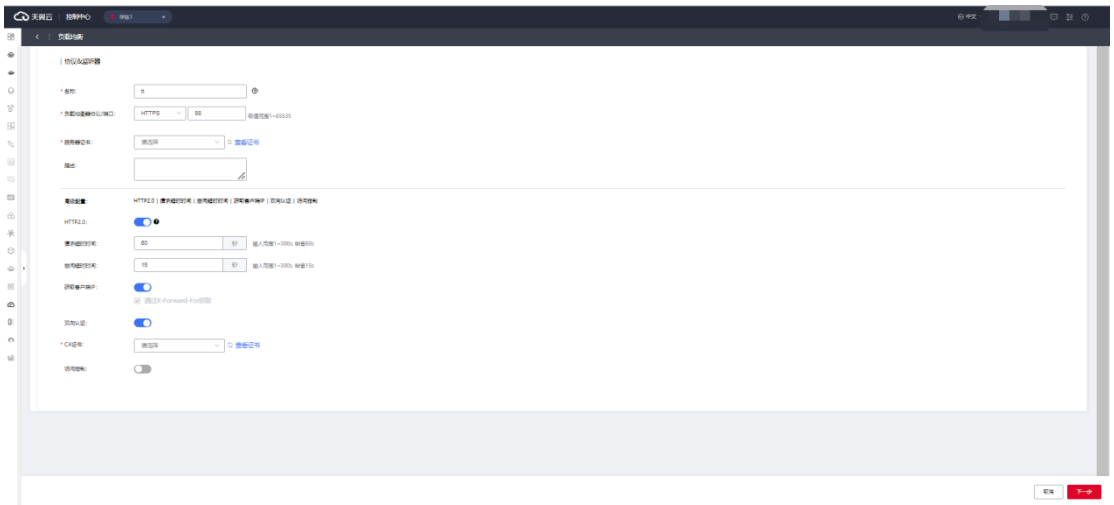
1.登录弹性负载均衡控制台；

2.在顶部右侧选择弹性负载均衡所属区域，本文选择华东-华东 1。

3.选择以下一种方法打开监听器配置向导。

- 在实例列表页面，找到目标实例，在操作列单击“监听器配置向导】”。
- 在 ip 类型/监听器端口/健康检查/服务器组列下方单击“开始配置”。
- 在实例列表页面，找到目标实例，单击“实例名称”进入实例详情页，单击“添加监听器”。

4.在协议&监听配置向导依据 HTTPS 监听器配置说明完成以下配置，然后点击“下一步”。



HTTPS 监听器配置说明

监听配置	说明

名称	设置监听器的名称，名称应为 2-32 位，英文开头，支持大小写英文和数字。
负载均衡器协议/端口	下拉列表选择 HTTPS 协议，输入监听端口，取值范围 1~65535。
描述	可选，填写监听器描述。
高级配置	监听器的特定参数配置：HTTP2.0|请求超时时间|空闲超时时间|获取客户端 IP|双向认证|访问控制。
HTTP2.0	选择是否开启 HTTP2.0 功能，开启后，可提升客户端与负载均衡间的访问性能，负载均衡与后端云主机仍采用 HTTP1.X 协议。
请求超时时间	输入范围 1~300s，缺省 60s。 集群资源池支持设置 HTTP 请求超时时间，在请求超时时间内接收请求的后端主机无响应，负载均衡会向所有其它后端主机重试请求。如果重试所有后端主机一直没有响应，则负载均衡会给客户端返回 HTTP 504 错误码。主备、集群模式资源池列表见产品简介>产品类型和规格>按资源池区分，实际情况以控制台展现为准。
空闲超时时间	输入范围 1~300s，缺省 15s； 集群模式资源池支持设置 HTTP 连接的空闲超时时间。在空闲超时时间后仍没有访问请求，负载均衡会中断当前连接。主备、集群模式资源池列表见产品简介>产品类型和规格>按资源池区分，实际情况以控制台展现为准。

获取客户端源信息	开启获取客户端源信息，将通过 X-Forwarded-for 头字段携带客户端源真实 IP。集群资源池可以支持 X-Forwarded-Proto 来获取客户端与负载均衡监听连接时所用的协议（HTTP/HTTPS），支持 X-Forwarded-Port 获取客户端与负载均衡监听连接时所用的端口。主备、集群模式资源池列表见产品简介>产品类型和规格>按资源池区分，实际情况以控制台展现为准。
访问控制	选择是否开启访问控制。开启访问控制后，选择一种访问控制方式：黑名单、白名单。并设置访问策略组作为该监听器的白名单或黑名单。 ● 白名单：允许特定 IP 访问负载均衡，仅转发来自所选访问策略组中设置的 IP 地址或地址段的请求，白名单适用于只允许特定 IP 访问的场景。 ● 黑名单：禁止特定 IP 访问负载均衡，不转发来自所选访问策略组中的 IP 或地址段，黑名单适用于只限制特定 IP 访问的场景。
双向认证	选择是否开启双向认证，支持 CA 证书。 双向认证指的是客户端需要认证主机端真实性，同时主机端也需要认证客户端的真实性，具体可参考证书管理。
WebSocket 支持	当选择 HTTPS 监听时，默认支持加密版本的 WebSocket 协议（WSS 协议）。仅集群模式资源池支持，主备、集群模式资源池列表见产品简介>产品类型和规格>按资源池区

	分，实际情况以控制台展现为准。

步骤二：添加后端主机组

添加处理前端请求的后端主机组。

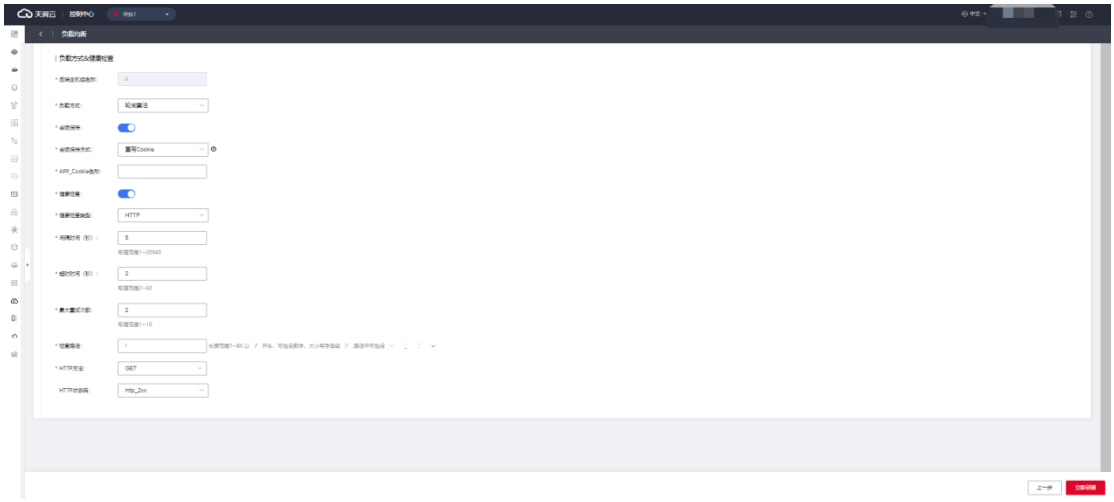
前提条件：您已经创建了弹性云主机，具体操作可参考创建弹性云主机。

1. 设置后端主机组名称。

2. 选择后端主机类型，可选云主机。

3.从主机列表中选择可添加的云主机，然后点击“下一步”，即完成后端云主机的添加。

步骤三：参考 HTTPS 监听器负载方式&健康检查配置说明，完成负载方式和健康检查配置。完成步骤三后，点击【立即创建】，完成 HTTP 监听器创建。



HTTPS 监听器负载方式&健康检查配置说明

负载方式&健康检查配置	说明
负载方式	从下拉列表框选择负载方式 ● 轮询算法：请求以轮询的方式依次分发给各后端主机，加权轮询对权重高的主机会获得更多的轮询次数。 ● 最小连接算法：动态调度算法，通过主机当前活跃的

	连接数来评估主机的负载情况，负载均衡将请求分发给活跃连接数最小的后端主机。加权最小连接数会结合权重分配后端主机。
会话保持	选择是否开启会话保持。 开启会话保持后，负载均衡监听器会把来自同一客户端的访问请求分发到同一台后端主机上。
会话保持方式	集群模式资源池 HTTPS 协议的会话保持方式如下： • 重写 cookie/植入 cookie。 • 植入 cookie：客户端首次访问时，负载均衡在返回请求中植入 cookie（即在 HTTP 或 HTTPS 响应报文中插入 ServerID），下次客户端携带此 cookie 访问，负载均衡会将请求转发给之前记录到的后端云主机上。植入 cookie 需要指定会话保持时间。 • 重写 cookie：负载均衡对用户自定义的 cookie 进行重写，下次客户端携带新的 cookie 访问，负载均衡会将请求转发给之前记录到的后端云主机； • 选择植入 cookie 时，可设置会话保持超时时间。缺省 3600s。 • 选择重写 cookie，负载均衡发现用户自定义的 cookie，对原来的 cookie 进行重写，下次客户

	端携带新的 cookie 访问，负载均衡服务将请求定向转发给之前记录到的后端主机。重写 cookie 方式该 cookie 的会话保持时间由后端主机维护。
健康检查	开启健康检查，负载均衡对后端主机的服务状态进行探测。负载均衡将不会分发流量给服务异常的主机。
健康检查类型	可选 HTTP 或 TCP。
间隔时间	健康检查的检查间隔，缺省 5s。
超时时间	健康检查超时时间，缺省 2s。
最大重试次数	健康检查的重试次数，缺省 2，连续检查失败达到重试次数，则判断健康检查失败。
检查路径	可设置 HTTP 健康检查的路径，长度范围 1~80 以‘/’开头，可包含数字、大小写字母或‘/’,路径中可包含‘-’ ‘_’ ‘.’ ‘=’
HTTP 方法	可选 GET 或 HEAD。
HTTP 状态码	选择 HTTP 健康检查范围的状态码，可选 http_2xx，http_3xx，http_4xx，http_5xx。

4.2.4 修改监听器

操作场景：

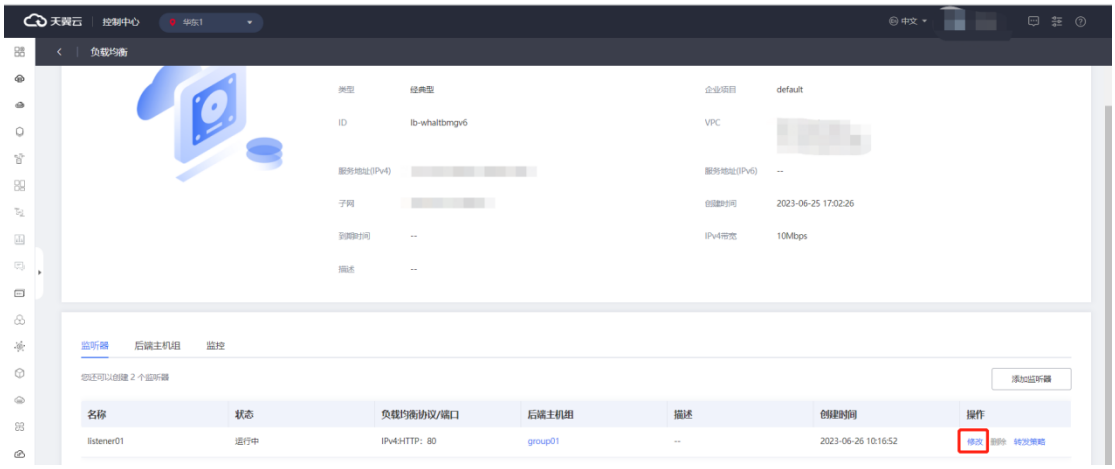
如果您已创建监听器，您可以根据实际业务需求，修改监听器相关配置。

使用限制：

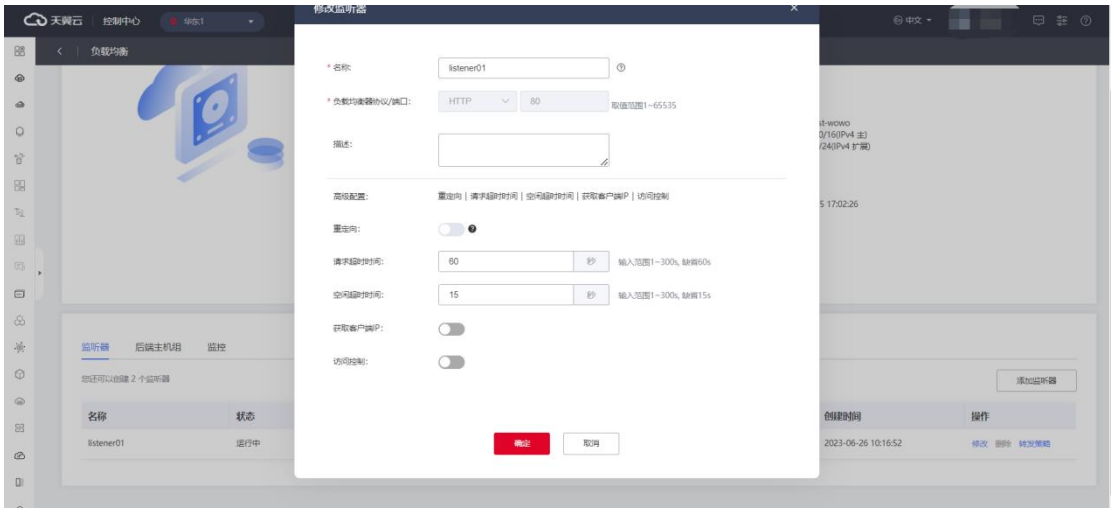
- 已创建的负载均衡器协议/端口不支持修改。
- 名称修改应为 2-32 位，英文开头，支持大小写英文和数字。

操作步骤：

1. 登录天翼云控制中心。
2. 选择“网络>弹性负载均衡>负载均衡器”。
3. 单击已创建的负载均衡器实例名称；
4. 在该负载均衡界面的“监听器”区域，单击监听器所在行的“修改”选项。



5. 在“修改监听器”界面，根据页面提示配置参数，进行修改。
6. 单击“确定”按钮。



4.2.5 访问策略组管理

创建访问策略组

使用场景:

如果您需要对访问策略进行分类分组优化管理，你可以通过创建访问策略组来实施。

使用须知：

您可创建 20 个访问策略组。

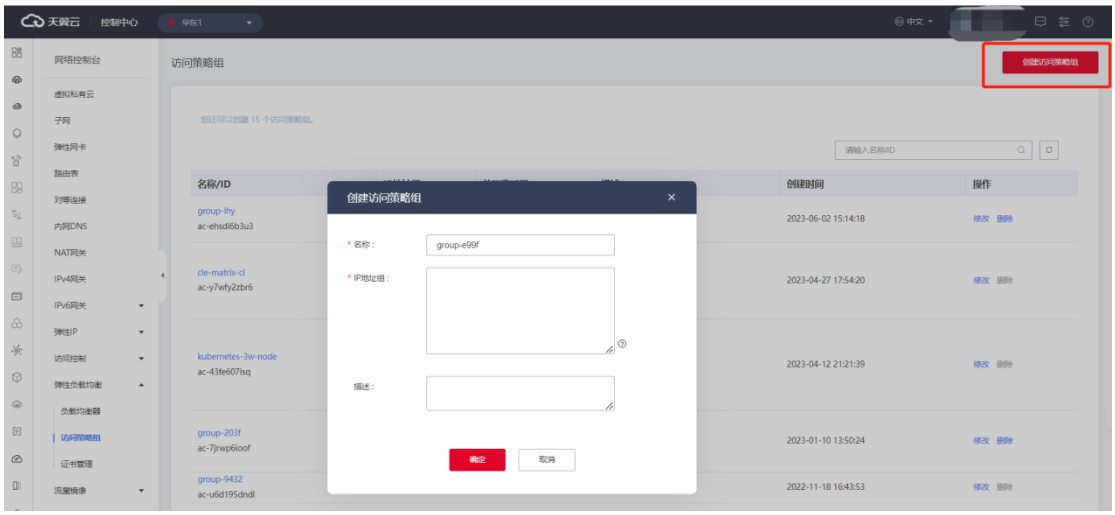
操作步骤:

1.点击天翼云门户首页的“控制中心”，输入登录的用户名和密码，进入控制中心页面。

2.在管理控制台上方单击图标，选择区域，本文操作均选择华东-华东 1。

2.在系统首页，选择“网络>弹性负载均衡>访问策略组”。

3.在访问策略组页面，单击“创建访问策略组”，进入访问策略组创建页面。



4.根据业务需要，配置相关参数，具体可参考访问策略组配置说明。

访问策略组配置说明

访问策略组配置	说明

名称	访问策略租的名称，
IP 地址组	1.每行一个 IP 地址段，以"IP/掩码长度"格式填写，主机 IP 用 32 位掩码，如 192.168.1.100/32, 192.168.2.0/24，添加网段主机位要全 0； 2.每个 IP 地址或网段都可以用“|”分隔添加备注，如“192.168.10.10/32|ECS01”，备注长度范围是 0 到 255 字符，不能包含<>； 3.每个 IP 地址组最多可添加 50 个 IP 地址或网段。
描述	访问策略组相关描述信息。

5.点击对应的访问策略组名称，可查看改访问策略组详情。

修改访问策略组

使用场景:

如果您已经创建了访问策略组，根据业务需要，您可以对访问策略组进行修改。

操作步骤:

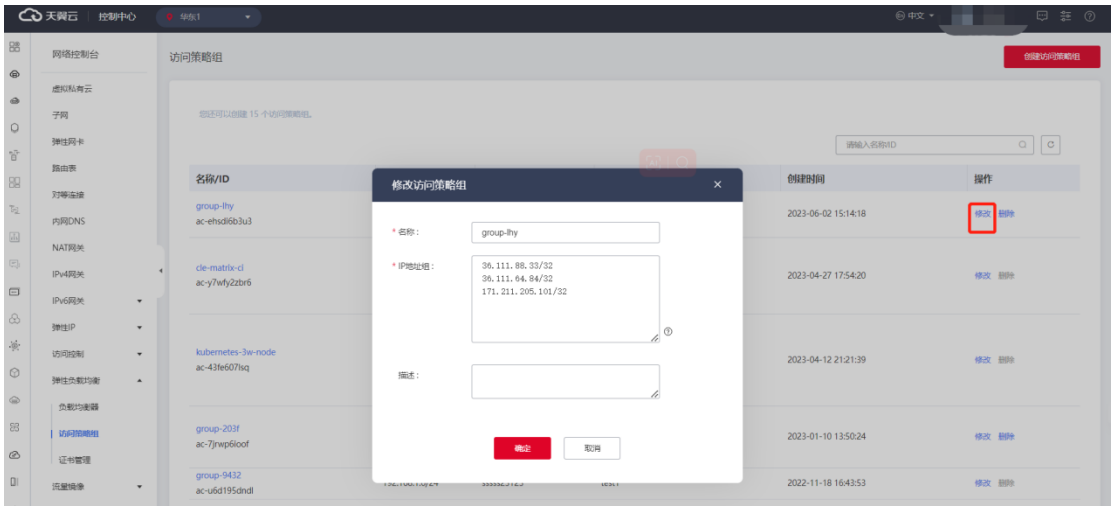
1.点击天翼云门户首页的“控制中心”，输入登录的用户名和密码，进入控制中心页面。

2.在管理控制台上方单击图标，选择区域，本文操作均选择华东-华东 1。

3.在系统首页，选择“网络>弹性负载均衡>访问策略组”。

4.在访问策略组列表页面，选择需要修改的访问策略组进行修改操作。

5.具体修改参数可参考访问策略组配置说明。



删除访问策略组

使用场景

如果您已经创建了访问策略组，根据业务需要，您可在访问策略组列表信息页面，选择指定的访问策略组，进行删除访问策略组的操作。

使用限制

IP 地址组存在关联的联监听器，无法删除。访问策略删除后，无法恢复。

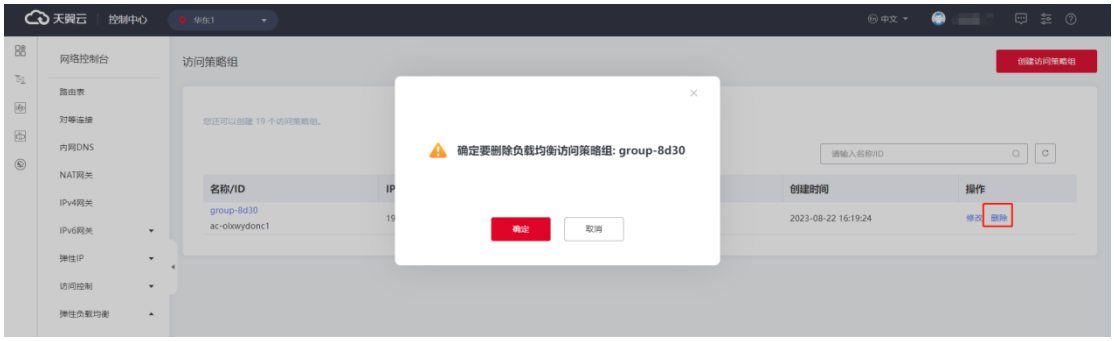
操作步骤

1.点击天翼云门户首页的“控制中心”，输入登录的用户名和密码，进入控制中心页面。

2.在管理控制台上方单击图标，选择区域，本文操作均选择华东-华东 1。

3.在系统首页，选择“网络>弹性负载均衡>访问策略组”。

4.在访问策略组列表页面，选择需要修改的访问策略组进行删除操作。



4.2.6 配置访问控制

操作场景

弹性负载均衡支持访问控制的操作，您可以通过黑名单或白名单限制对负载均衡的访问。

前提条件

配置访问控制您需创建先访问策略组，并明确需要的访问控制方式。如没有创建访问策略组，可在配置访问过程中跳转至访问策略组创建。

使用须知

天翼云访问策略支持以下两种访问控制方式：

- 白名单：允许特定 IP 访问负载均衡，仅转发来自所选访问策略组中设置的 IP 地址或地址段的请求，白名单适用于只允许特定 IP 访问的场景。
- 黑名单 禁止特定 IP 访问负载均衡 ,不转发来自所选访问策略组中的 IP 或地址段，黑名单适用于只限制特定 IP 访问的场景。

从添加监听器页面来开启访问控制

操作步骤

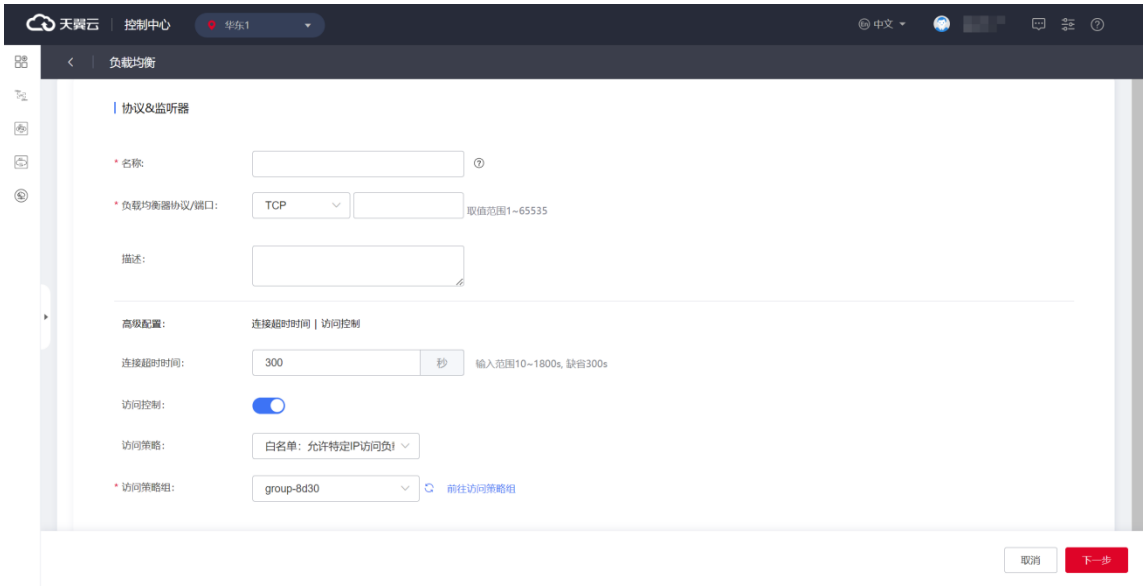
1.登录天翼云控制中心。

2.选择“网络>弹性负载均衡>负载均衡器”。

3.单击已创建的负载均衡器实例名称。

4.在监听器添加页面，打开“访问控制”开关。

5.打开开关后下方出现“访问策略“和“访问策略组”配置选项，访问策略根据访问控制需求，可选择“黑名单：禁止特定 IP 访问负载均衡”或“白名单：允许特定 IP 访问负载均衡”。



6.配置好后，点击“下一步”完成配置。

访问控制还可从监听器修改页面来开启

操作步骤

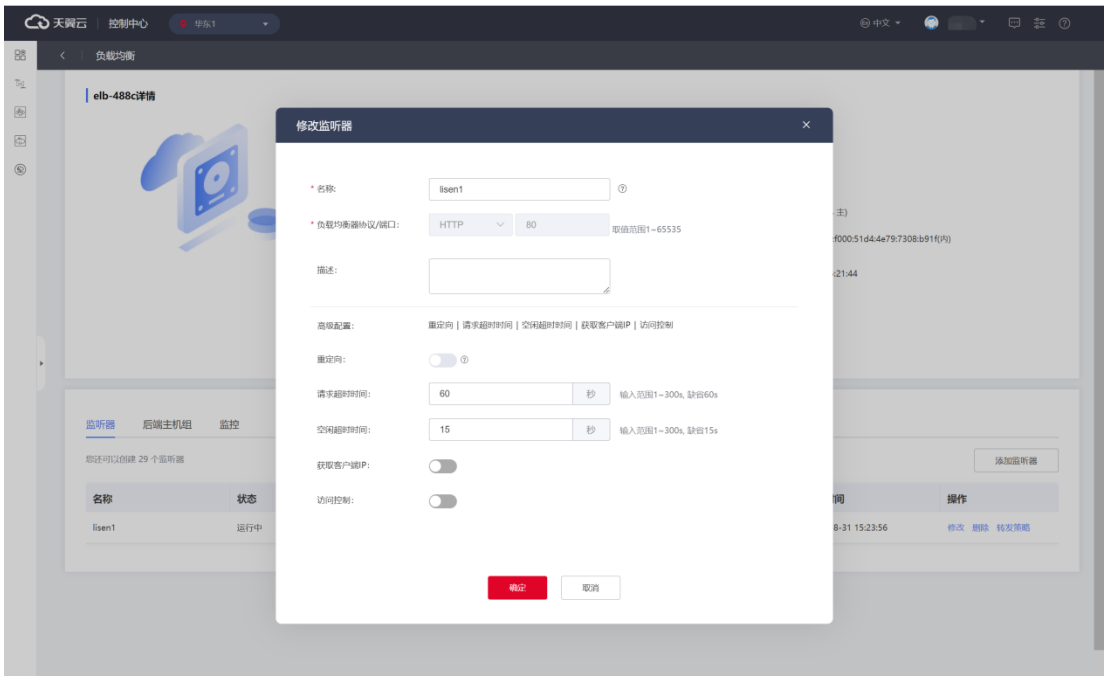
1.登录天翼云控制中心。

2.选择“网络>弹性负载均衡>负载均衡器”。

3.单击已创建的负载均衡器实例名称。

4.在负载均衡详情页，监听器列表对应监听器的操作字段，点击“修改”。

5.在修改监听器窗口打开“访问控制”开关。



6.选择“访问策略”，选择“访问策略组”，点击“确定”完成访问控制配置。

4.2.7 配置 HTTPS 监听器引用证书

操作场景

HTTPS 协议监听器关联证书，做 SSL 握手，加密认证，配置安全的通信通道，保护数据的机密性和完整性。

操作步骤

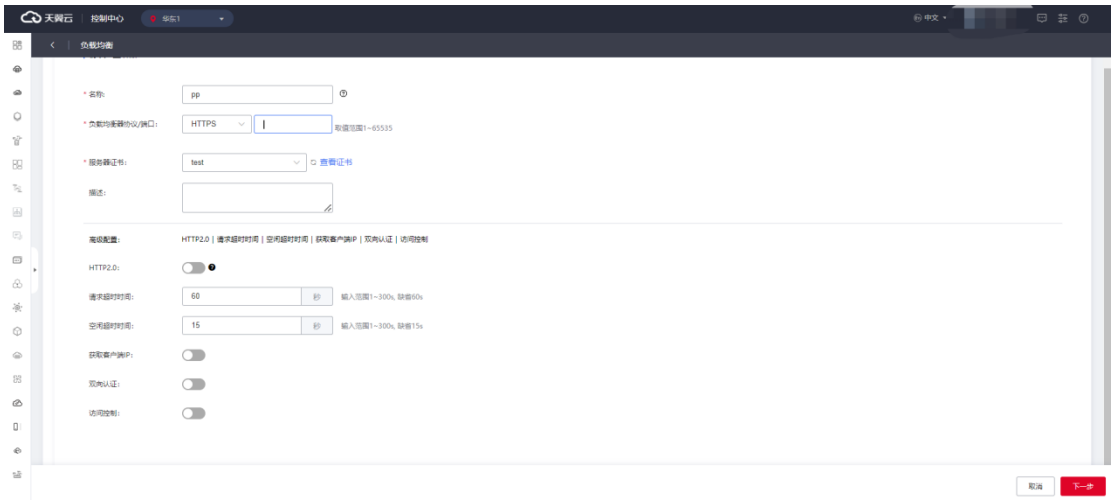
1.点击负载均衡实例名称进入“负载均衡详情页”。

2.点击“添加监听器”按钮，添加监听器，并配置 HTTPS 证书。

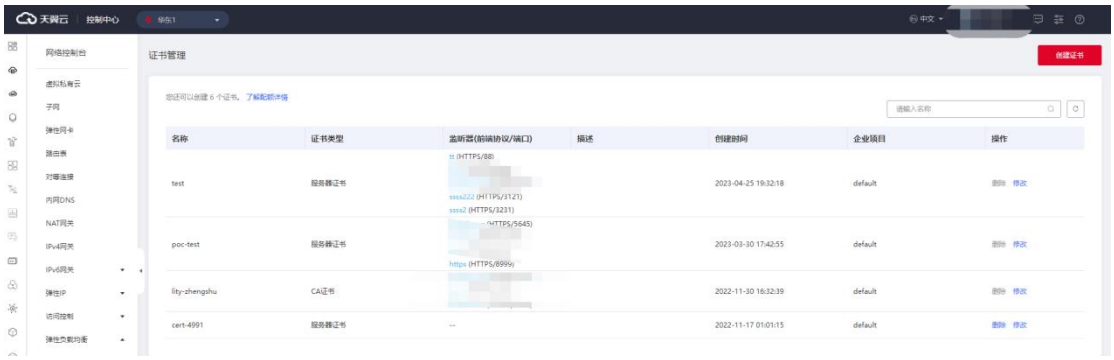
a) 设置监听器的名称，支持中英文字符，数字，长度 2~63 个字符。

b) 负载均衡器协议选择 HTTPS，在右侧输入服务端口，选择 HTTPS 协议后，下方出

现服务器证书字段。



c) 选择服务器证书,从下拉列表框选择已创建的服务器证书，支持刷新，如当前没有证书，点击“查看证书”跳转到证书管理页面，可在此页面创建证书。



d)配置监听器描述，可选配置，可以不输入描述。

3. 单击“下一步”，配置后端主机组；配置主机组名称，选择后端主机类型，可选云主机。

4. 继续点击“下一步”配置负载方式和健康检查，完成相关操作。

4.2.8 配置 HTTP 重定向

操作场景

HTTPS 在 HTTP 的基础上通过传输加密和身份认证保证了传输过程中的安全性。如果企业为了保障业务建立安全连接，想要从 HTTP 升级使用 HTTPS，可以使用 HTTP

重定向功能帮助用户业务从 HTTP 平滑无感知的迁移到 HTTPS。当客户端通过 HTTP 请求访问云上的 web 服务时，配置了 HTTP 到 HTTPS 的重定向后，弹性负载均衡会返回 HTTPS 的响应，从而强制客户端以 HTTPS 的方式访问 web 服务。

前提条件

已创建 HTTPS 监听器，并运行正常。

注意事项

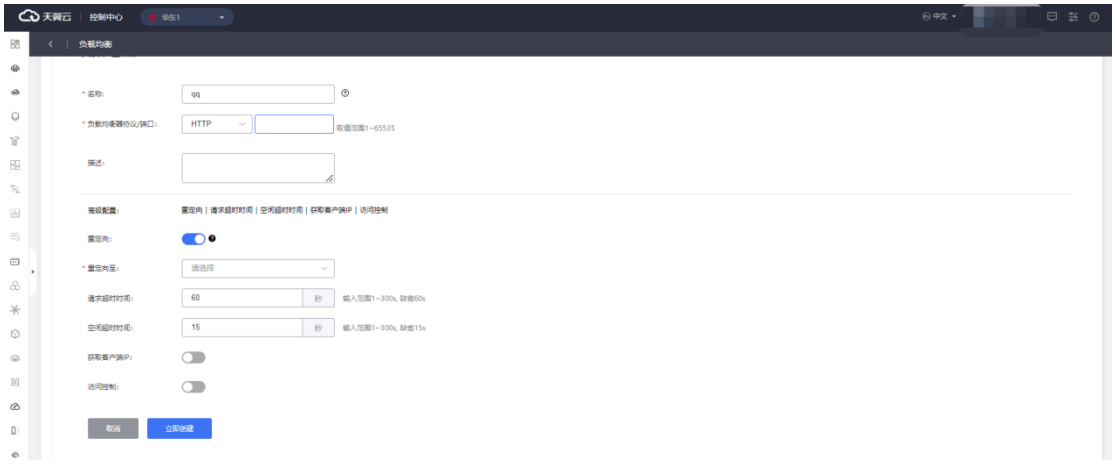
只能重定向至 HTTPS 监听器，并且每个监听器只能重定向一次。开启重定向功能后，如需获取源 IP 能力，请在重定向后监听器开启。

重定向的监听器不可创建转发策略。

- **添加 HTTP 监听器时配置重定向**

操作步骤

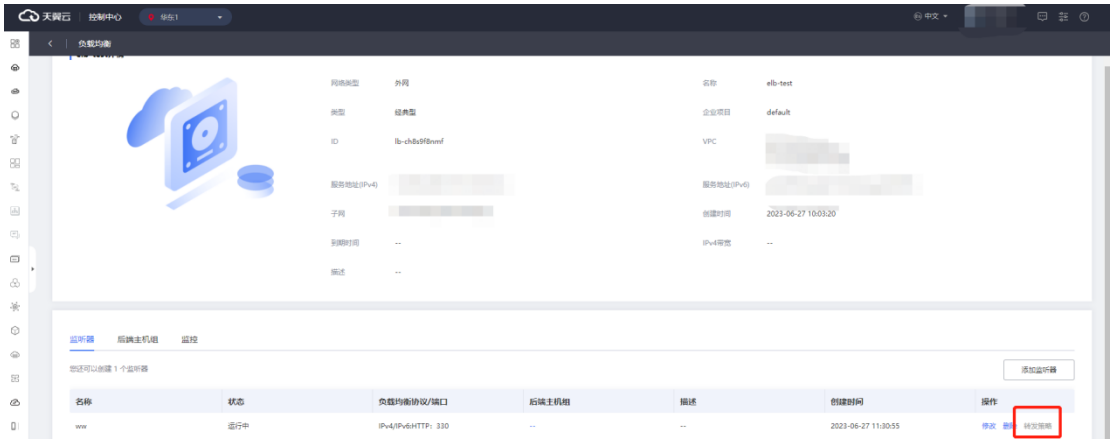
1.添加 HTTP 协议监听器，在高级配置中可见 HTTP 重定向参数，通过开关控制。



1. 开启“HTTP 重定向”开关，选择重定向目标 HTTPS 监听器，点击“立即创建”，监听器直接进入创建步骤。

2. 当 HTTP 监听器状态跳转至“运行中”，则创建成功。

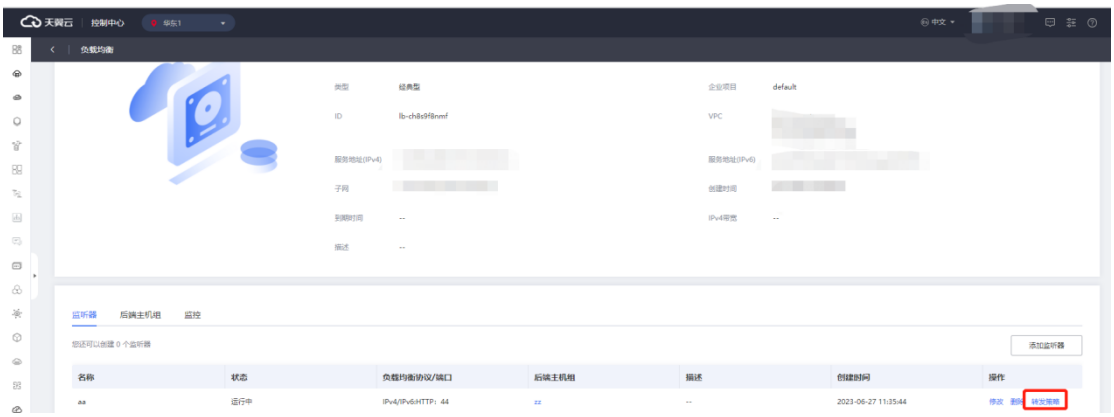
3. 重定向的监听器不可创建转发策略，到此监听器的访问都将被重定向至已配置的 HTTPS 监听器。



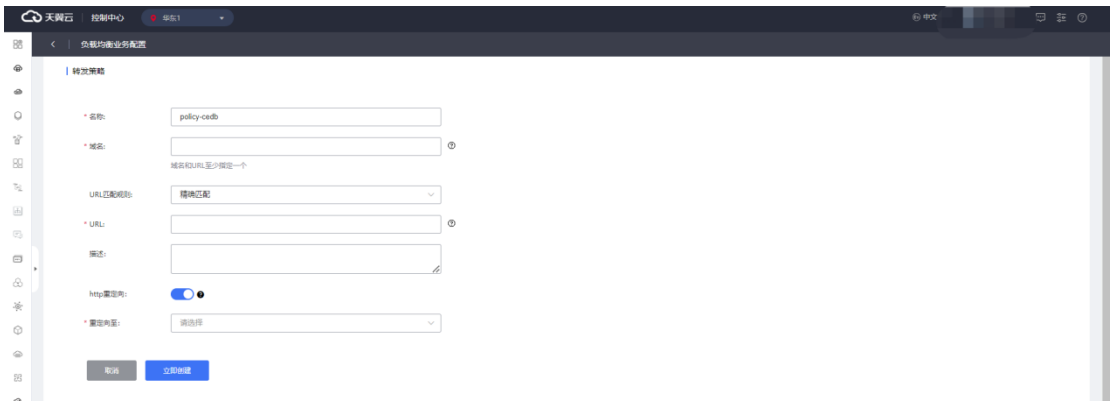
- **在监听器的转发策略配置中开启重定向**

操作步骤

1.在 HTTP 监听器详情页面，点击“转发策略”，匹配特定域名或 URL 做重定向。



2.在弹出的转发策略页面开启“HTTP 重定向”后，直接点击“立即创建”，略过后端主机和健康检查配置步骤。



4.2.9 配置 HTTPS 双向认证

操作场景：

HTTPS 协议监听器可配置 CA 证书，对客户端证书的签名进行验证，实现安全审计、数据分析、安全测试和访问控制等功能。

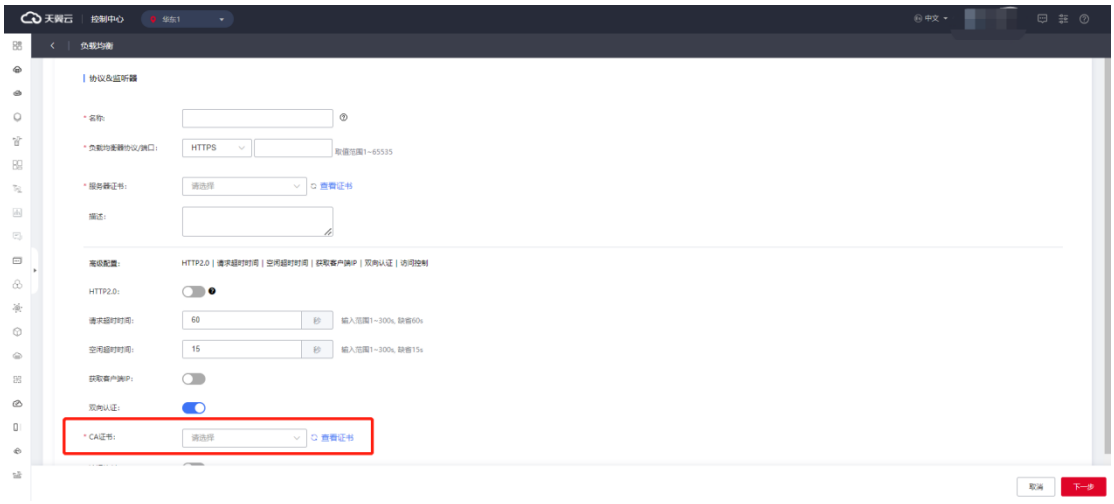
操作步骤：

1.登录弹性负载均衡弹性负载均衡控制台；

2.在顶部右侧选择弹性负载均衡所属区域，本文选择华东-华东 1；

3.打开监听器配置向导，在协议&监听器页面，选择 HTTPS 协议并输入端口。

4.在 HTTPS 监听器添加步骤中，选择开启“双向认证”，下方出现 CA 证书选择下拉列表框。

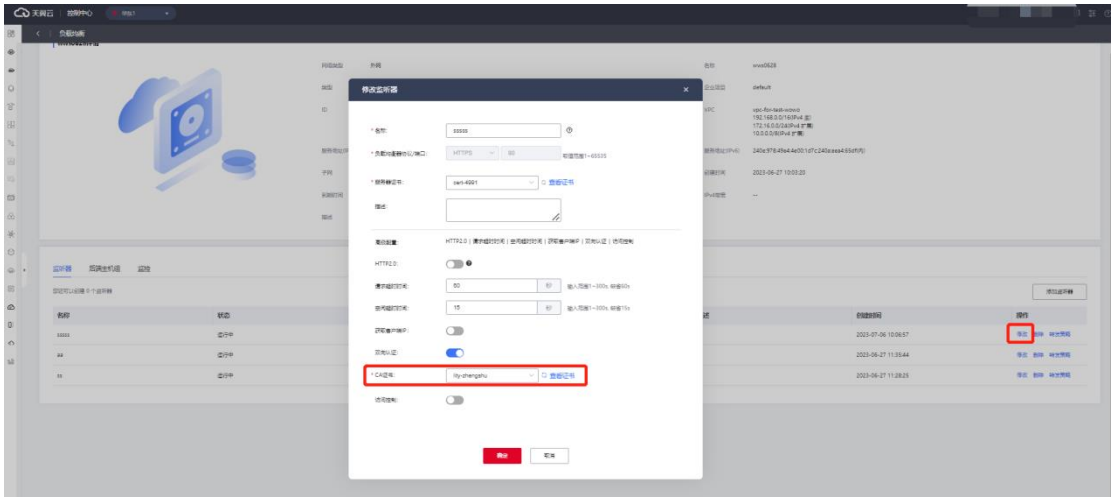


4. 点击刷新图标，可刷新证书列表，选择所需证书。

5. 如未创建证书，可点击“查看证书”跳转到证书管理页面创建证书。

7.配置好相关参数后，点击“下一步”配置负载方式和健康检查，完成相关操作。

8.如需替换证书，可在修改监听器页面选择要替换的证书，并点击“确定”，完成操作。



4.2.10 开启 HTTP2.0

操作场景

HTTPS 监听器支持开启 HTTP2.0 功能。HTTP2.0 即位超文本传输协议 2.0，它可以支持多路复用并且相对于 HTTP1.1 更安全。

使用限制

仅 HTTPS 监听器支持 HTTP/2 功能。

HTTP2.0 功能目前仅在集群模式资源池上线。主备、集群模式资源池列表见产品简介>产品类型和规格>按资源池区分，实际情况以控制台展现为准。

目前不支持 HTTP2.0 修改功能。

注意事项

HTTP2.0 是客户端至 ELB 段开启，ELB 至后端主机仍为 HTTP 1.x。

- **在添加添加监听器时，选择 HTTPS 协议，通过开关控制开启或关闭 HTTP2.0 功能**

操作步骤

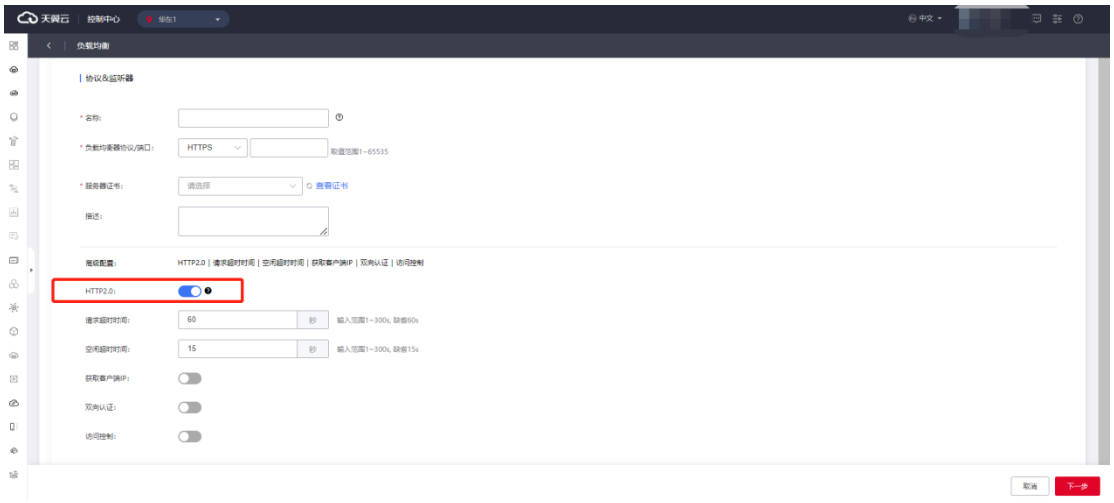
1.登录弹性负载均衡弹性负载均衡控制台；

2.在顶部右侧选择弹性负载均衡所属区域，本文选择华东-华东 1；

3.打开监听器配置向导，在协议&监听器页面，选择 HTTPS 协议并输入端口；

4.在 HTTPS 监听器添加步骤中，选择开启“HTTP2.0”控制开关；

5.配置好相关参数后，点击“下一步”配置负载方式和健康检查，完成相关操作。



- **修改监听器时，可通过开关控制开启或关闭 HTTP2.0 功能**

1. 登录天翼云控制中心。

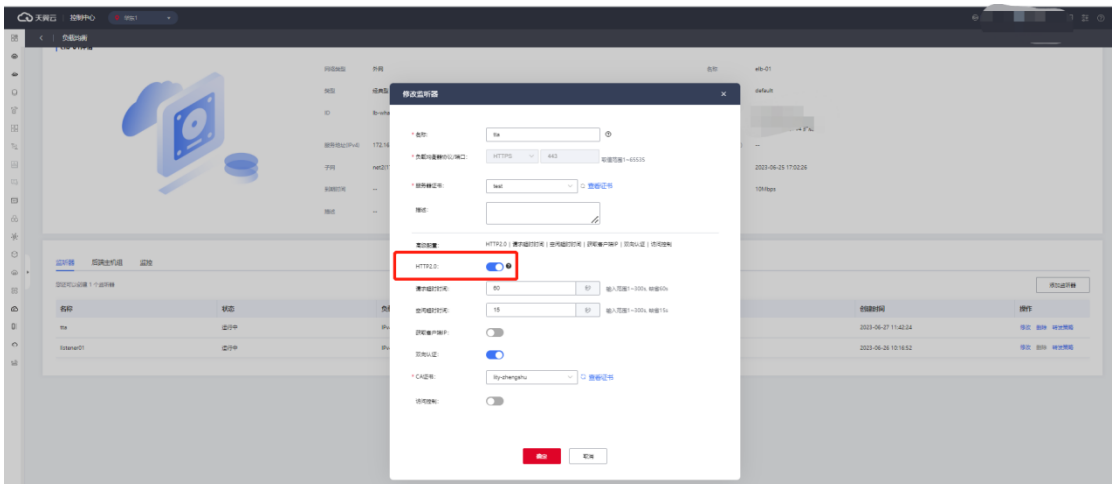
2. 选择“网络>弹性负载均衡>负载均衡器”。

3. 单击已创建的负载均衡器实例名称；

4. 在该负载均衡界面的“监听器”区域，单击监听器所在行的“修改”选项。

5. 在监听器修改页面可开启或关闭开启或关闭 HTTP2.0 功能；

6. 点击“确定”，完成相关操作。



4.2.11 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，删除监听器。

注意事项

- 监听器被删除后无法恢复，请谨慎操作。
- 如果该监听器下有后端主机组，不能删除，需先删除后端主机组后才可删除监听器。
- 如果该监听器中包含重定向、转发策略或被重定向调用，不能删除，需先删除转发策略或取消重定向。

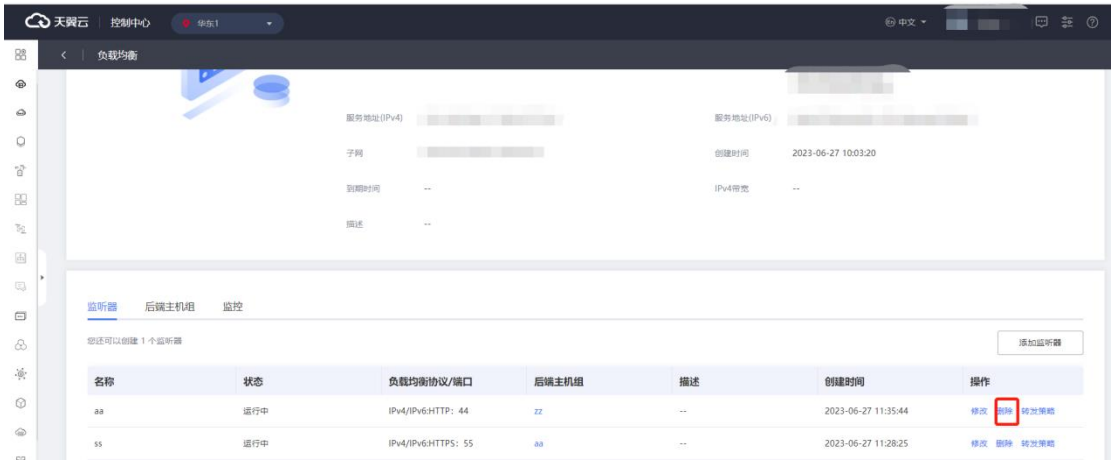
操作步骤

1.登录天翼云控制中心。

2.选择“网络>弹性负载均衡>负载均衡器”。

3.单击已创建的负载均衡器实例名称。

4.在该负载均衡界面的“监听器”区域，单击监听器所在行的“删除”选项，并点击“确定”，删除指定的监听器。



4.2.12 开启获取客户端 IP

操作场景

HTTP 请求和应答会在头字段携带一些信息 ,除了 RFC 2616 中定义的标准的 HTTP 头字段，还有一些非标准的 HTTP 标头可供应用程序自动添加和使用。

所有资源池均支持非标准的头字段 X-Forwarded-For，创建监听时，X-Forwarded-For 头字段可以获取来访者客户端 IP 地址。

如果您想要获取客户端的真实 IP，您可以开启“获取客户端 IP”功能。

注意事项

在四层转发 TCP 服务中，集群模式资源池支持通过配置 TOA 插件获取客户端真实源 IP，具体可参考弹性负载均衡最佳实践>TCP 请求获取客户端真实源 IP 地址。目前不支持通过此方式获取 UDP 的客户端真实 IP 地址。在四层转发 TCP/UDP 服务中,主备模式资源池支持通过 Proxy protocol 获取用户真实 IP。主备、集群模式资源池列表见产品简介>产品类型和规格>按资源池区分，实际情况以控制台展现为准。

在七层转发（HTTP/HTTPS）服务中，弹性负载均衡支持通过 HTTP 头中的 X-Forwarded-For 获取来访者真实 IP。本文以下主要说明在七层转发（HTTP/HTTPS）

服务中获取客户端 IP 的方式。

- **在创建监听器时开启获取客户端 IP**

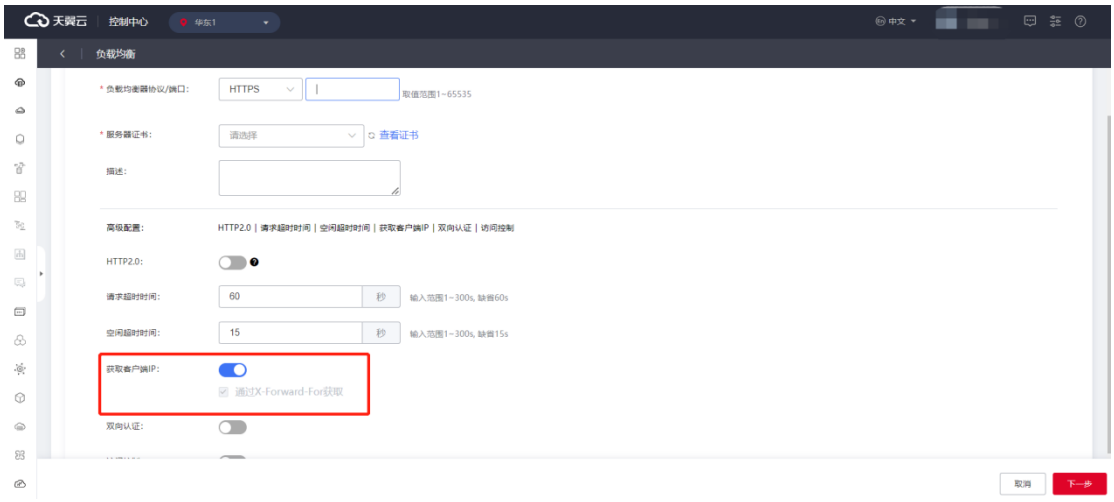
操作步骤

1.登陆弹性负载均衡控制台。

2.打开监听器配置向导，在负载均衡器实例页面添加监听器。

3.在协议&监听器页面，负载均衡器协议/端口选择 HTTP/HTTPS 协议。

4. 开启获取客户端 IP 选项；开启后默认通过 X-Forward-For 获取。



5.点击“下一步”，按照监听器创建后端主机组的配置添加云主机，然后点击“下一步”进行负载方式&健康检查配置，并点击“立即创建‘则完成相关配置。

- **为已创建的监听器开启获取客户端 IP**

前提条件

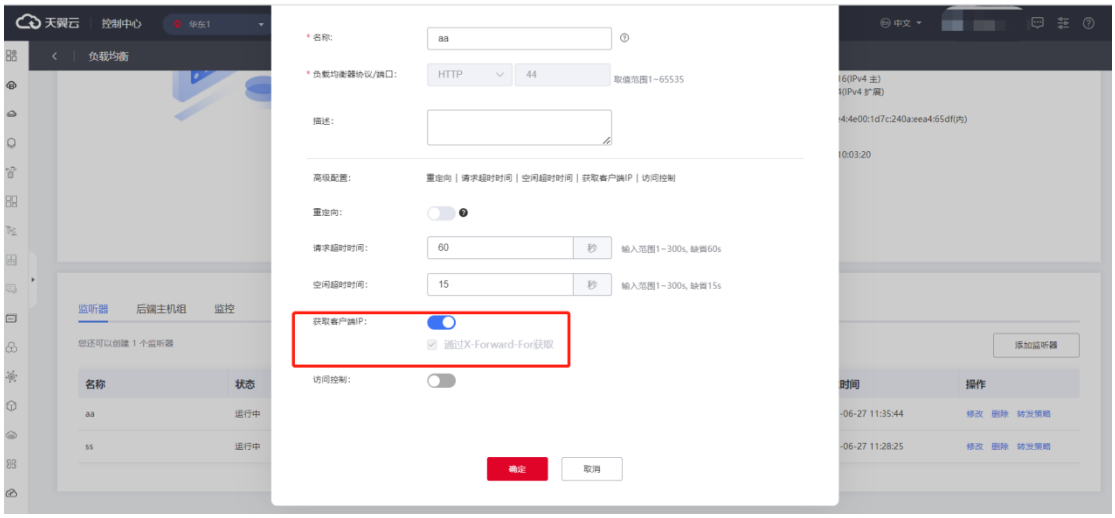
已创建 HTTP/HTTPS 监听器。

操作步骤

1.登陆弹性负载均衡控制台。

2.在该负载均衡界面的“监听器“区域，单击监听器所在行的“修改”选项。

3.在弹出的修改监听器页面开启获取客户端 IP 选项；默认通过 X-Forward-For 获取。



4.点击确定，完成开启获取客户端 IP 配置。

4.2.13 转发策略

4.2.13.1 添加转发策略

操作场景

HTTP/HTTPS 支持配置基于域名和路径的转发策略，可以将来自不同域名或者不同 URL 路径的请求转发到不同的后端主机组来处理。

可以通过转发策略，将同一个网站的视频，图片，文本的请求分发到不同的后端主机组来处理，便于合理的分配资源。

注意事项

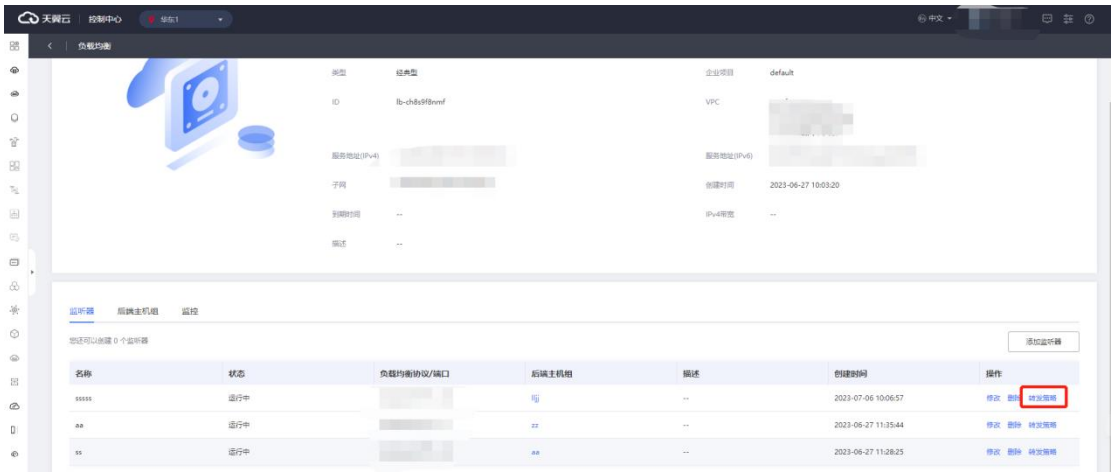
- 目前仅 HTTP、HTTPS 的监听器添加转发策略。
- 重定向的监听器不可创建转发策略。
- 目前支持的转发规则为：域名，URL。
- 如果创建了相同的转发策略（出现转发策略冲突），则会出现转发策略故障，此时

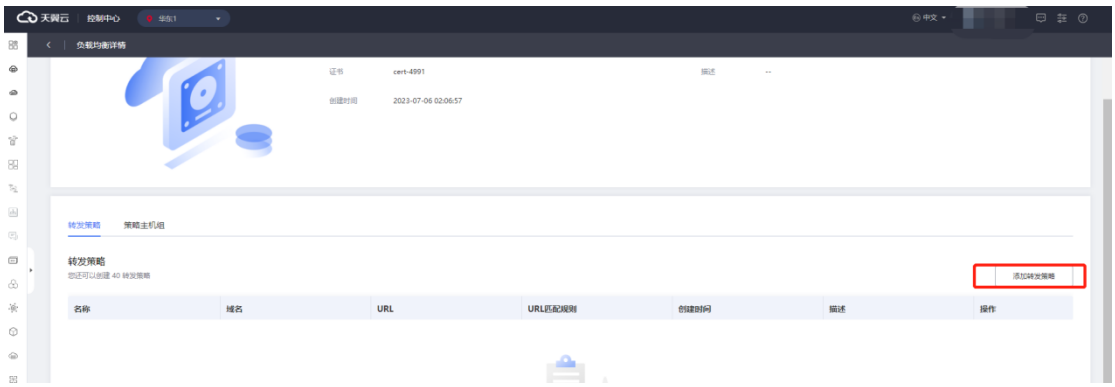
即使把前面创建的转发策略删除，后面的转发策略依然会显示故障。将出现冲突的转发策略都删除后重新添加，即可恢复正常。

操作步骤

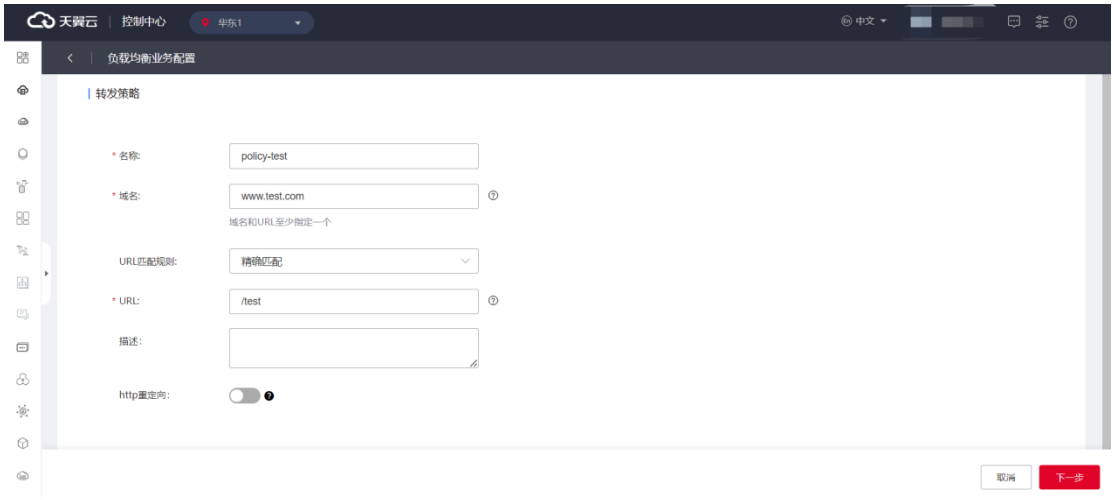
1. 进入“负载均衡详情页”，点击“监听器”详情的操作列，单击转发策略。

2. 单击“添加转发策略”，进入转发策略配置页。





3. 按照转发策略配置说明进行转发策略配置后，点击“下一步”：



转发策略配置说明

参数	说明	取值样例
名称	转发策略的名称。	policy-test
域名	域名转发所需配置的域名。 域名和 URL 至少指定一个。	www.test.com
URL 匹配规则	支持的 URL 匹配规则有：精确匹配、前缀匹配和正则匹配。 精确匹配： 请求的 URL 和设定 URL 完全一致。 例：URL 为/test，用户 URL 必须为/test 才匹配。 前缀匹配： 请求的 URL 匹配以设定 URL 开头的 URL。 例：URL 为/test，用户 URL 为 /test123、/test7fds 等各种以/test 开头	精确匹配

	的字符串时匹配。 正则匹配：请求的 URL 和设定的 URL 正则表达式匹配。	
URL	URL 匹配的请求路径。域名和 URL 至少指定一个。	/test
描述	自定义描述内容	Xx

4. 按照监听器创建后端主机组的配置添加云主机，然后点击“下一步”进行负载方式&健康检查配置，并点击“立即创建”则完成相关配置。

4.2.13.2 修改转发策略

操作场景

您可根据业务需要修改 HTTP/HTTPS 监听器的转发策略。

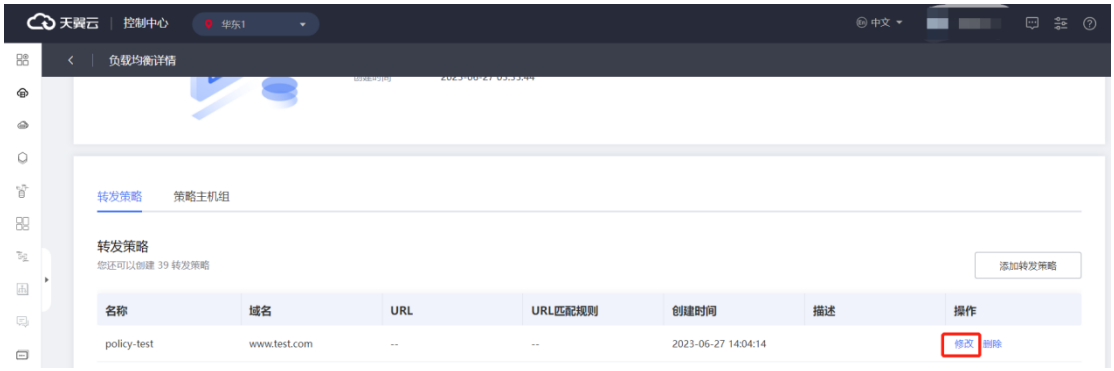
注意事项

目前仅支持修改转发策略名称及描述。

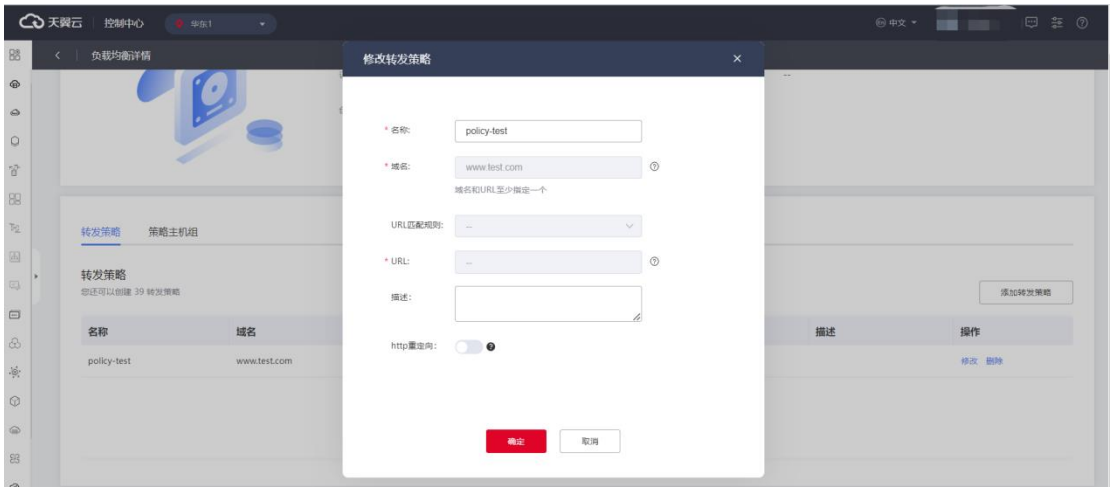
操作步骤

1.进入“负载均衡详情页”，在“监听器”详情的操作列，单击转发策略。

2.在转发策略页面，单击转发策略所在行的“修改”选项。



3.在“修改转发策略”界面，根据页面提示配置参数。



4. 单击“确定”按钮；完成转发策略修改。

4.2.13.3 删除转发策略

操作场景

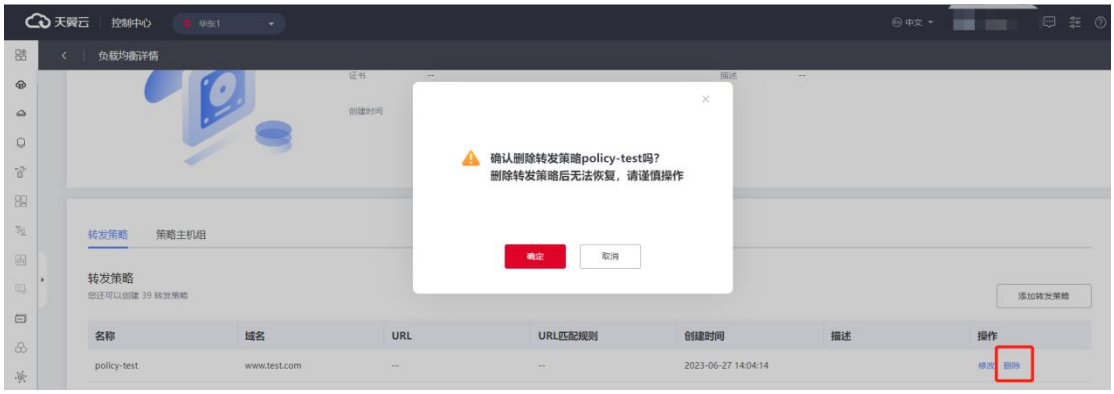
您可根据业务需要删除 HTTP/HTTPS 监听器的转发策略。

操作步骤

1.进入“负载均衡详情页”，在“监听器”详情的操作列，单击转发策略；

2.在转发策略页面，单击转发策略所在行的“删除”选项；

3.在弹出页面点击“确定”，即可删除所选的的转发策略。



4.3 后端主机组

4.3.1 后端主机组概述

后端主机组简介

每个监听器都会关联一个后端主机组，后端主机组是一组相同或类似的云主机实例，可以包含一个或多个后端主机。添加后端主机组的具体操作可参考本文监听器>添加监听器>添加后端主机组章节内容。

后端主机组功能

后端主机组的主要功能是将负载均衡器接收到的流量分发给组内的主机，以确保流量在各个主机之间进行均衡分配，从而实现高可用性和高性能。负载均衡器可以根据不同的算法（如轮询、最小连接等）来决定将流量转发到哪个后端主机。

通过后端主机可以对后端主机进行统一管理，灵活地添加或者移除后端主机，降低用户的管理和使用成本。

使用负载均衡集成弹性伸缩服务可实现后端主机组自动扩展的能力。当负载增加时，可以动态添加更多的主机实例来处理流量，以满足应用程序的需求。同样地，当负载减少时，多余的主机实例可以被自动移除，以节省资源和成本。

此外，后端主机组还支持健康检查功能，可监测主机实例的状态和可用性。如果某个主

机实例发生故障或不可用，负载均衡器将自动将流量转发到其他健康的主机，以确保应用程序的连续性和可靠性。

网络流量路径

不论用户配置的是外网负载均衡还是内网负载均衡，弹性负载均衡和后端主机之间都使用的是内网地址通信的。如果后端云主机只需要处理来自弹性负载均衡的请求，那么此云主机不需要购买弹性 IP。后端云主机使用内网 IP 对弹性负载均衡做应答，弹性负载均衡再将此应答做 NAT 地址转换后转发给用户端。

4.3.2 查看后端主机组

操作场景

天翼云弹性负载均衡支持查看已添加的后端主机组。

前提条件

在添加监听器时，您设置了后端主机组名称，并进行了相关配置。具体可参考添加监听器。

操作步骤

1.点击天翼云门户首页的“控制中心”，输入登录的用户名和密码，进入控制中心页面；

2. 在管理控制台顶端单击图标，选择区域，本文选择华东-华东 1；

3. 在系统首页，选择“网络>弹性负载均衡>负载均衡器”；

4. 在弹出页面点击要查看的“后端主机组”名称，即可查看后端主机组下的云主机等信息。

4.3.3 修改后端主机组配置

场景说明

在添加后端主机组后，用户可根据使用需求修改后端组的相关配置。

使用须知

支持后端主机组名称、会话保持、健康检查、间隔时间、超时时间、最大重试次数等相关参数的修改。

- **基于 TCP/UDP 协议的后端主机组**

操作步骤

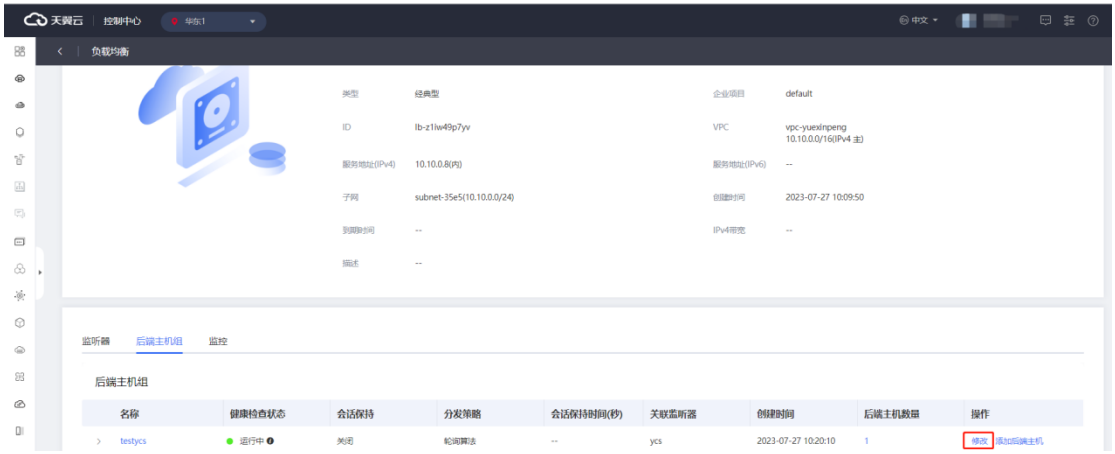
1.点击天翼云门户首页的“控制中心”，输入登录的用户名和密码，进入控制中心页面；

2. 在管理控制台顶端单击图标，选择区域，本文选择华东-华东 1；

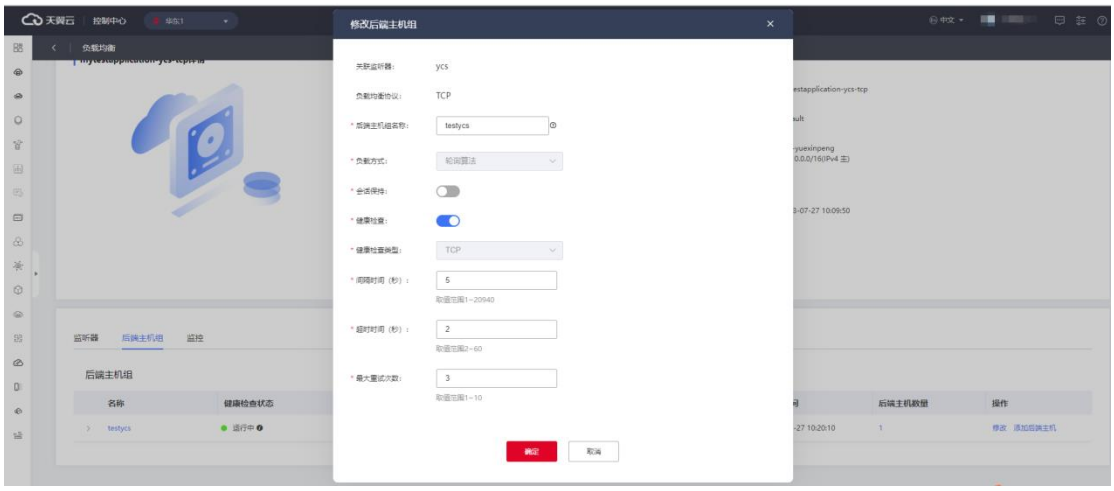
3. 在系统首页，选择“网络>弹性负载均衡>负载均衡器”；

4. 在负载均衡器列表中，选择要修改的 TCP/UDP 协议的负载均衡器；

5. 在弹出页面点击指定的“后端主机组”所在列的“修改”按钮；



6.根据参数说明完成后端主机组参数修改；



7.点击“确定”完成修改。

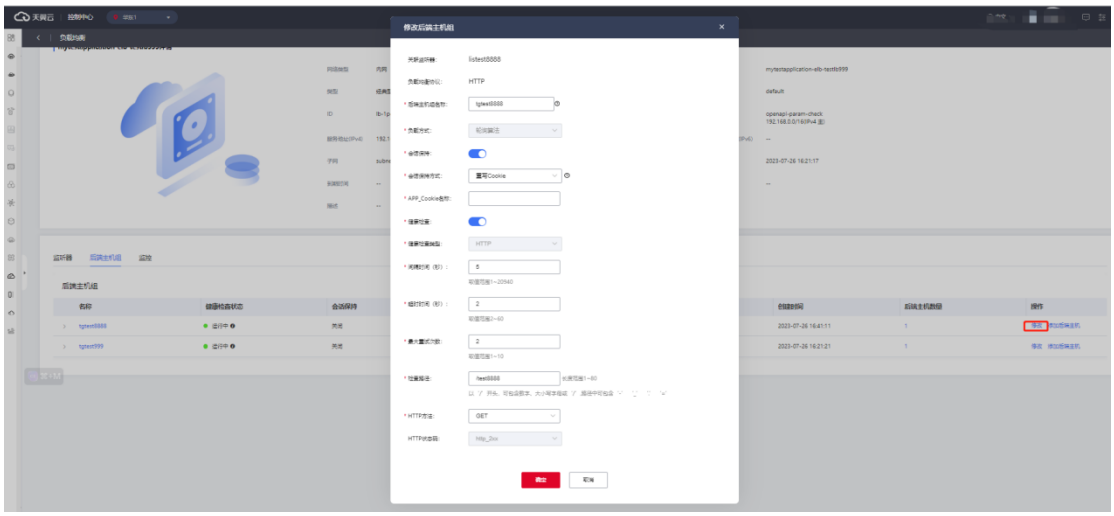
参数	说明
后端主机组名称	可修改后端主机组名称。 名称应为 2-32 位，英文开头，支持大小写英文和数字
负载均衡协议	不支持修改。
负载方式	不支持修改。
会话保持	选择是否开启会话保持。可选“开启”或“关闭”。 ● 开启会话保持后，负载均衡监听器会把来自同一客户端的访

	问请求分发到同一台后端主机上。 ● 会话保持方式：TCP/UDP 协议的会话保持方式为 SOURCE_IP 方式。 ● 会话保持时间修改的取值范围为 1- 86400。
健康检查	选择是否开启健康检查。可选“开启”或“关闭”。 ● 开启健康检查，负载均衡对后端主机的服务状态进行探测。负载均衡将不会分发流量给服务异常的主机。 ● 健康检查类型：TCP 协议监听器只可选 TCP；UDP 协议监听器只可选 UDP。 ● 间隔时间（秒）： 取值范围 1~20940。 ● 超时时间（秒）：取值范围 2~60。 ● 最大重试次数：取值范围 1~10。

- **基于 HTTP/HTTPS 协议的后端主机组**

操作步骤

1. 点击天翼云门户首页的“控制中心”,输入登录的用户名和密码,进入控制中心页面；
2. 在管理控制台顶端单击图标，选择区域，本文选择华东-华东 1；
3. 在系统首页，选择“网络>弹性负载均衡>负载均衡器”；
4. 在负载均衡器列表中，选择要修改的 HTTP/HTTPS 协议的负载均衡器；
5. 在弹出页面点击指定的“后端主机组”所在列的“修改”按钮；



6.根据参数说明完成后端主机组参数修改；

参数	说明
后端主机组名称	可修改后端主机组名称。 名称应为 2-32 位，英文开头，支持大小写英文和数字
负载均衡协议	不支持修改。
负载方式	不支持修改。
会话保持	选择是否开启会话保持。可选“开启”或“关闭”。 ● 开启会话保持后，负载均衡监听器会把来自同一客户端的访问请求分发到同一台后端主机上。 ● 会话保持方式：集群模式资源池 HTTP 协议的会话保持方式支持重写 cookie/植入 cookie。 植入 cookie：客户端首次访问时，负载均衡在返回请求中植入 cookie（即在 HTTP 或 HTTPS 响应报文中插入 ServerID），下次客户端携带此 cookie 访问，负载均衡会将请求转发给之前

	记录到的后端云主机上。植入 cookie 需要指定会话保持时间，取值范围为 1- 86400。 重写 cookie：负载均衡对用户自定义的 cookie 进行重写，下次客户端携带新的 cookie 访问，负载均衡会将请求转发给之前记录到的后端云主机；选择植入 cookie 时，可设置会话保持超时时间。缺省 3600s。选择重写 cookie，负载均衡发现用户自定义的 cookie，对原来的 cookie 进行重写，下次客户端携带新的 cookie 访问，负载均衡服务将请求定向转发给之前记录到的后端主机。重写 cookie 方式该 cookie 的会话保持时间由后端主机维护。
健康检查	选择是否开启健康检查。可选“开启”或“关闭”。 ● 开启健康检查，负载均衡对后端主机的服务状态进行探测。负载均衡将不会分发流量给服务异常的主机。 ● 健康检查类型：不支持修改。 ● 间隔时间（秒）： 取值范围 1~20940。 ● 超时时间（秒）：取值范围 2~60。 ● 最大重试次数：取值范围 1~10。 ● 检查路径： 以‘/’开头，可包含数字、大小写字母或‘/’，路径中可包含 ‘-’ ‘，长度范围 1~80。 ● HTTP 方法：可选 GET 或 HEAD。 ● HTTP 状态码：不支持修改。

4.3.4 配置会话保持

应用场景

在大多数电子商务的应用系统或者需要进行用户身份认证的在线系统中，一个客户与服务器经常经过好几次的交互过程才能完成一笔交易。由于这几次交互过程是密切相关的，服务器在进行这些交互过程的某一个交互步骤时，往往需要了解上一次交互过程的处理结果，或者上几步的交互过程结果，所以这就要求这些相关的交互过程都由一台服务器完成，而不能被负载均衡器分散到不同的服务器上,此时就需要相应的会话保持策略来保证相关的请求始终被负载到后端的一台服务器。

通过会话保持，Web 应用程序可以跟踪用户的状态和数据，并提供个性化的体验，而不必在每个请求中重新验证用户或重建状态。

会话保持原理分析

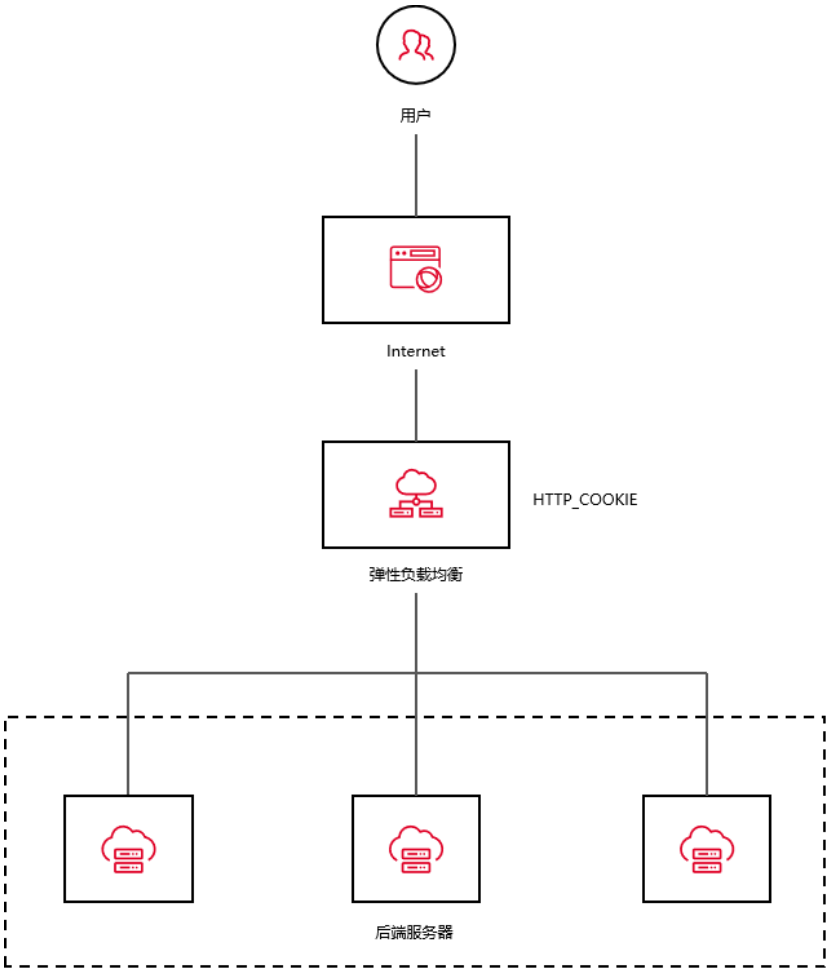
针对于不同资源池负载均衡会话保持方式的名称和行为略有差异，例如主备模式资源池，会话保持的名称和行为如下：

主备、集群模式资源池列表见产品简介-产品类型和规格，实际情况以控制台展现为准。

HTTP_COOKIE

在 HTTP_COOKIE 方式下，ELB 负责在 HTTP 响应头插入会话保持 cookie，后端服务器无需做任何修改。当客户首次请求时，ELB 选择后端一台服务器转发，在后端服务器回复 HTTP 响应头时，ELB 插入会话保持 cookie，该 cookie 的值为后端服务

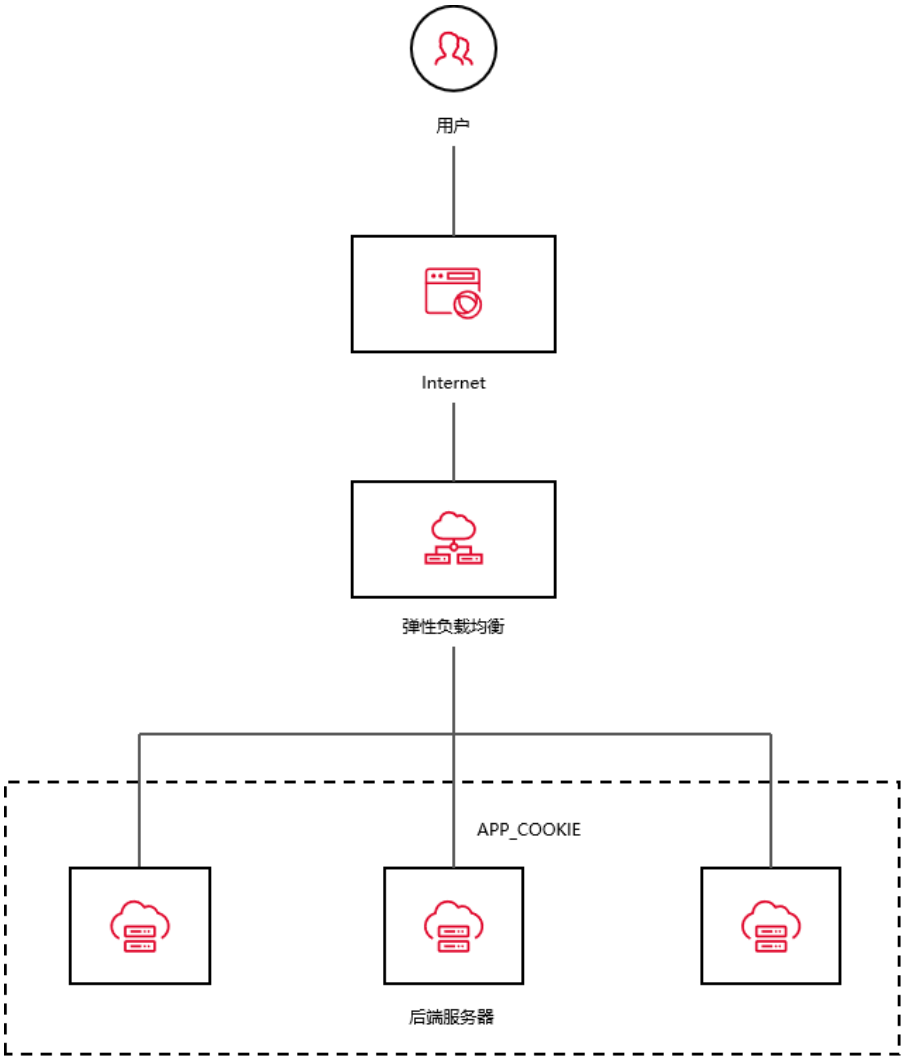
器 SERVERID。在 cookie 有效期内，后续客户端请求都携带会话保持 cookie，ELB 根据该 cookie 的值将请求转发给同一后端服务器处理。



APP_COOKIE

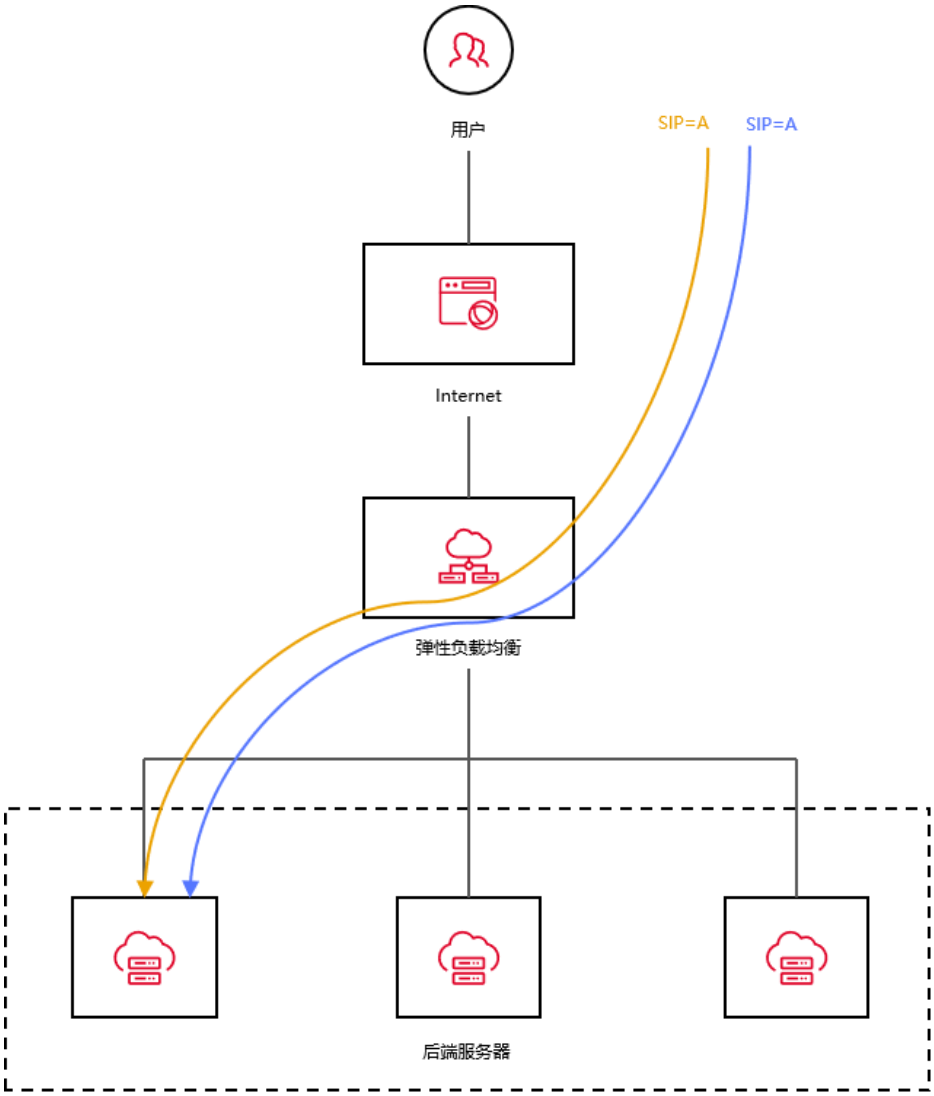
在 APP_COOKIE 方式下，后端服务器负责在 HTTP 响应头插入会话保持 cookie，ELB 只对 cookie 做记录和透传。当客户首次请求时，ELB 选择后端一台服务器转发，在后端服务器回复 HTTP 响应头时，ELB 记录下会话保持 cookie 的值与后端服务器的关联关系，将该 cookie 透传给客户端。在 cookie 有效期内，后续客户端请求都携带会话保持 cookie，ELB 根据该 cookie 的值与后端服务器的关联关系，将请

求转发给同一后端服务器处理。相比于 HTTP_COOKIE， APP_COOKIE 由后端服务器决定是否会话保持，适用于需要后端控制的复杂业务场景。



SOURCE_IP

根据收到请求的客户端源 IP 地址信息，ELB 将相同源 IP 地址的流量分发到相同的后端服务器上。



天翼云集群模式资源池适用于以下规则：

主备、集群模式资源池列表见产品简介-产品类型和规格，实际情况以控制台展现为准。

植入 COOKIE

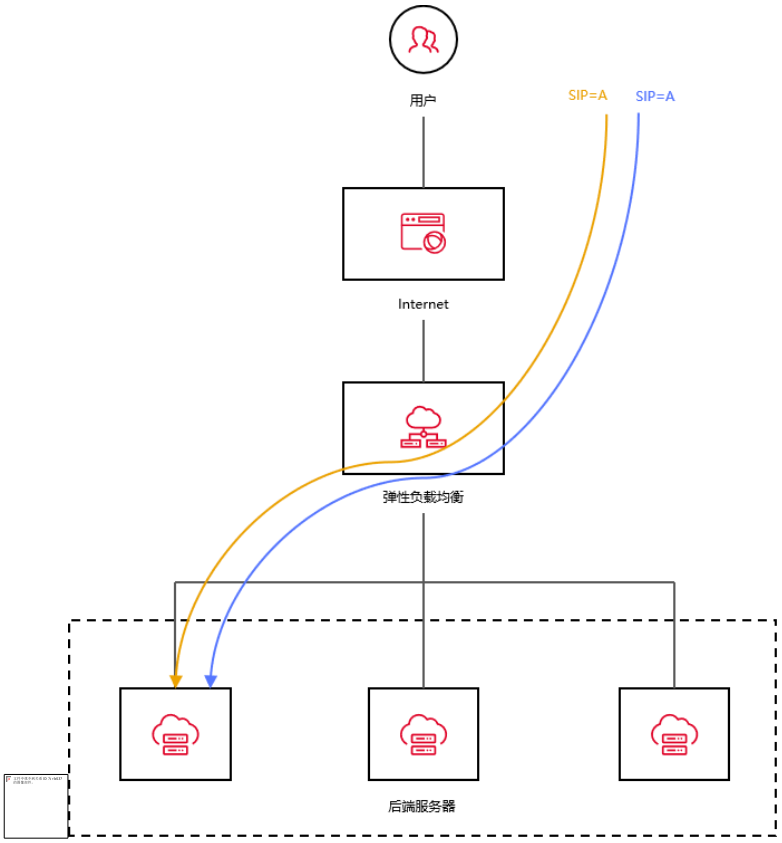
原理与以上的 HTTP_COOKIE 相同。

重写 COOKIE

在重写 Cookie 方式下，后端服务器负责在 HTTP 响应头插入会话保持 cookie，ELB 对 cookie 做改写。当客户首次请求时，ELB 选择后端一台服务器转发，在后端服务器回复 HTTP 响应头时，ELB 将会话保持 cookie 的值改写为后端服务器的 SERVERID。在 cookie 有效期内，后续客户端请求都携带会话保持 cookie，ELB 根据该 cookie 的值将请求转发给同一后端服务器处理。相比于植入 Cookie， 重写 Cookie 由后端服务器决定是否会话保持，适用于需要后端控制的复杂业务场景。

SOURCE_IP

根据收到请求的客户端源 IP 地址信息，ELB 将相同源 IP 地址的流量分发到相同的后端服务器上。



前提条件

- 您已在所在可用区创建 VPC，并创建业务主机，完成服务配置。
- 您已创建负载均衡实例。

操作步骤

1.登录天翼云控制中心，选择资源节点；本文我们选择的是华东-华东 1。

2.在控制中心页面，依次选择“网络 > 弹性负载均衡”。

3.在负载均衡页面，点击“ELB 实例名称”，进入详情页面。

4.在监听器页签，点击“添加监听器”按钮，创建监听器。

5.在监听器创建页面填写监听器名称，设置负载均衡器协议/端口等参数信息，完成后点击“下一步”。

1.创建后端主机组，选择后端云主机，添加到后端主机组，添加完成点击“下一步”。

2.在“负载均衡&健康检查”配置页面，找到“会话保持方式”，点击下拉框便可以选择不同的会话保持类型。在实际业务中，您可以根据具体情况进行会话方式的选择，最后完成负载方式、健康检查等其它配置。

3.点击“立即创建”完成配置并创建监听器。

4.3.5 健康检查

健康检查概述

健康检查是弹性负载均衡中的一项关键功能，用于确定后端资源的可用性和健康状况。

弹性负载均衡的健康检查工作原理是通过定期向后端主机发送健康检查请求，并根据主机的响应判断其健康状态。如果响应符合预期，则将主机标记为健康状态，否则标

记为不健康状态。根据主机的健康状态，负载均衡器决定将新的请求转发给哪些主机，以实现工作负载的均衡分配，并定期重新进行健康检查以更新主机的状态。这种方式能够提高系统的可靠性和性能，确保请求被正确处理并防止向不健康的主机转发。

弹性负载均衡器通常提供了多种健康检查的设置选项，包括检查的频率、超时时间、健康状态判断规则等。这些设置可以根据具体的应用需求进行调整。通过定期的健康检查，弹性负载均衡可以及时发现故障或不可用的后端资源，并自动从负载均衡中排除，确保流量只被发送到可用的资源上，提高了系统的可用性和可靠性。

功能特点

健康检查配置针对特定的后端实例或目标组。可以指定具体的端口和协议（如 HTTP、HTTPS、TCP 等）进行检查。

ELB 根据健康检查的结果，将后端实例标记为“健康”或“不健康”。如果主机实例被标记为不健康，ELB 将不会将流量发送到该实例。

健康检查可以定义成功的响应代码范围，还可以配置超时时间，即在多长时间内等待响应。

用户可以指定健康检查的频率。较短的间隔可以更快地检测到故障，但可能增加后端实例的负载。

用户可以设置连续多少次健康检查失败后将实例标记为不健康。

当一个不健康的实例重新变为健康状态时，ELB 会自动将流量重新引导到该实例，实现自动恢复。

开启健康检查

操作场景

用户可以配置运行状况检查，这些检查可用来监控后端云主机的运行状况，以便负

载均衡器只将请求发送到正常运行的后端云主机。而当该故障云主机恢复正常运行时，负载均衡会将其自动恢复到对外或对内的服务中。

注意

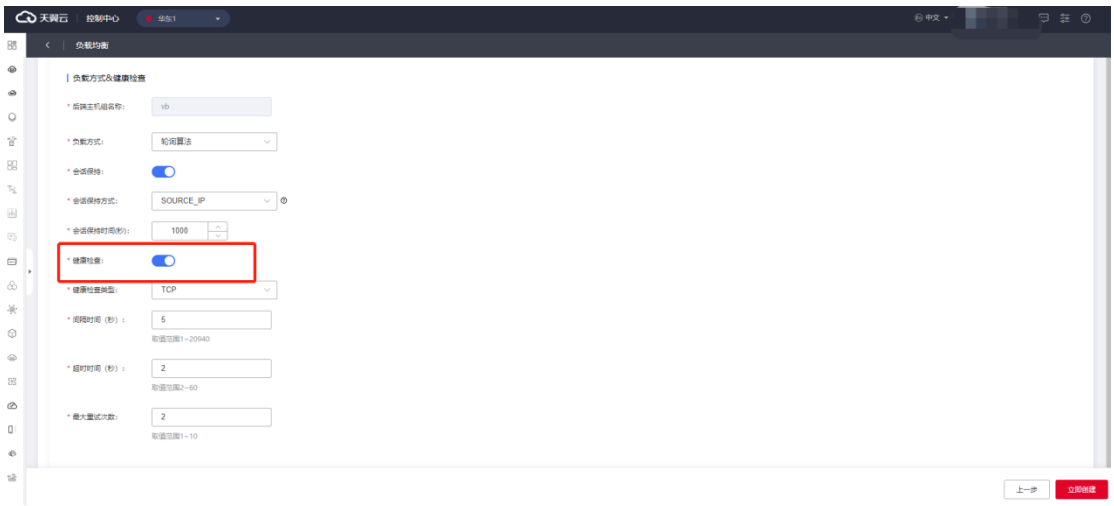
- 健康检查支持协议 TCP、UDP、HTTP。TCP 协议监听器只可选 TCP，UDP 协议监听器只可选 UDP。 HTTP 协议/HTTPS 协议监听器可选 HTTP 或 TCP。
- 只支持在添加监听器操作过程中开启健康检查。
- 弹性负载均衡使用 100.89.0.0/16 来对后端云主机做健康检查，如果开启健康检查功能需要在安全组时需要放通此网段。

操作步骤

1.登录弹性负载均衡控制台。

2.在顶部右侧选择弹性负载均衡所属区域，本文选择华东-华东 1。

3.打开监听器配置向导创建监听器 ,在监听器负载方式&健康检查页面开启“健康检查”选项，并点击“立即创建”，则完成监听器健康检查功能开启。



健康检查的配置参数说明

健康检查配置	说明
健康检查	默认开启，可关闭或打开

健康检查类型	可选的方式：HTTP、TCP、UDP。TCP 协议监听器只可选 TCP，UDP 协议监听器只可选 UDP。 HTTP 协议/Https 协议监听器可选 HTTP 或 TCP。
间隔时间	每隔多久进行一次健康检查。缺省 5s，取值范围：1~20940
超时时间	等待主机返回健康检查的时间。缺省 2s，取值范围 2~60s
最大重试次数	缺省 2 次，取值范围 1~10，健康检查失败达到最大重试次数后，进入健康检查失败状态。
检查路径	HTTP 检查类型选项，长度 1~80，检查 URL。以‘/’开头，可包含数字、大小写字母或‘/’,路径中可包含‘-’ ‘_’ ‘.’ ‘=’
HTTP 方法	HTTP 检查类型选项，可选：GET、HEAD。 GET 检查类型：使用 GET 方法发送 HTTP 请求到后端主机，负载均衡器期望从主机获取完整的响应内容。这种检查类型通常用于检查后端主机的完整性和性能，并确保主机能够正确地处理和响应 GET 请求。 HEAD 检查类型：使用 HEAD 方法发送 HTTP 请求到后端主机，负载均衡器仅期望从主机获取 HTTP 响应头部，而不需要获取完整的响应内容。这种检查类型通常用于检查主机的可用性和响应时间，而无需传输大量数据。
HTTP 状态码	选择 HTTP 健康检查范围的状态码，可选 http_2xx，

	http_3xx，http_4xx，http_5xx

健康检查默返回状态码说明

HTTP 状态码	说明
HTTP 状态码 200	表示正常响应。当健康检查请求成功被云主机处理并返回有效的响应时，通常会返回 200 状态码。
HTTP 状态码 3xx	重定向。在健康检查中，重定向状态码可能会出现在特定情况下。
HTTP 状态码 4xx	客户端错误。这些状态码表示请求存在问题，可能是由于无效的 URL、参数错误等。健康检查中，如果主机返回了 4xx 状态码，通常表示主机无法正常处理该请求。
HTTP 状态码 5xx	主机错误。这些状态码表示主机在处理请求时遇到了错误。在天翼云健康检查中，如果主机返回了 5xx 状态码，通常表示主机出现了故障或内部错误。

健康检查异常排查

当健康检查探测到您的后端主机异常时，弹性负载均衡将不再向异常的后端主机转发流量。直到健康检查检测到后端主机恢复正常时，弹性负载均衡才会向此主机继续转发流量。那么当您遇到健康检测异常可以按如下思路进行排查：

- 检查后端主机组是否关联监听器
- 检查健康检查配置：检查健康检查配置参数信息，例如域名、协议是否正确，检查您配置的健康检查端口和监听的端口是否一致，检查路径是否正确等。
- 检查主机所在安全组、网络 ACL 是否放行 ELB 健康检查源地址网段 100.89.0.0/16。
- 检查后端主机是否正常：后端主机当前宕机或不可访问，会导致检查异常。

- 检查主机防火墙、路由。

4.3.6 负载方式

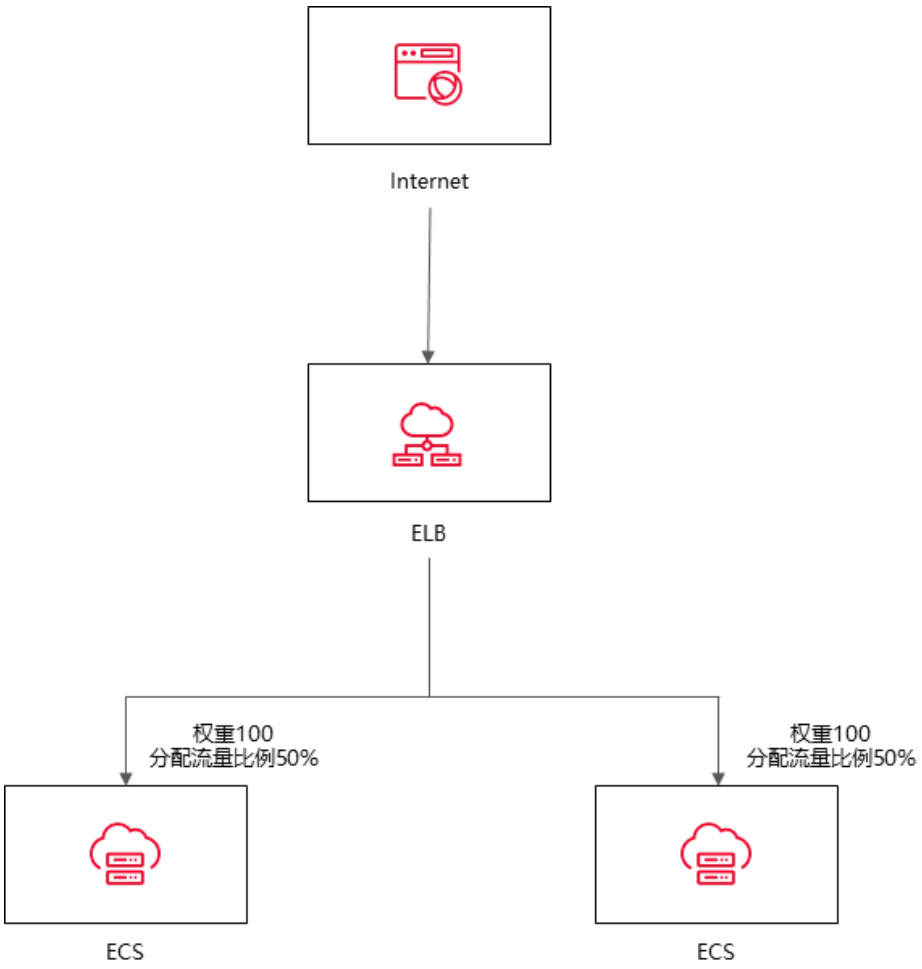
负载方式

弹性负载均衡可以根据不同的负载方式，匹配不同的算法策略来决定如何将流量分配给后端主机。以下是天翼云弹性负载均衡支持的负载方式及对应的算法策略：

负载算法	权重	算法策略
轮询算法	权重取值范围为[1,256]	根据后端主机的权重，将流量按照顺序逐个分发给后端主机，每台主机依次接收请求，实现流量均衡。相应的权重表示后端主机的处理性能，常用于短连接服务。
最小连接算法	权重取值范围为[1,256]	将流量分发给当前连接数最少的主机，以确保负载较小的主机能够处理更多的请求。加权最小连接即根据主机的权重和当前连接数来分发流量，常用于长连接服务。
源IP算法	在非 0 的权重下，由于使用了源 IP 算法，各个后端主机的权重属性将不再生效	将请求的源 IP 地址进行 Hash 运算，得到一个具体的数值，同时对后端主机进行编号，按照运算结果将请求分发到对应编号的主机上。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主机。

轮询算法

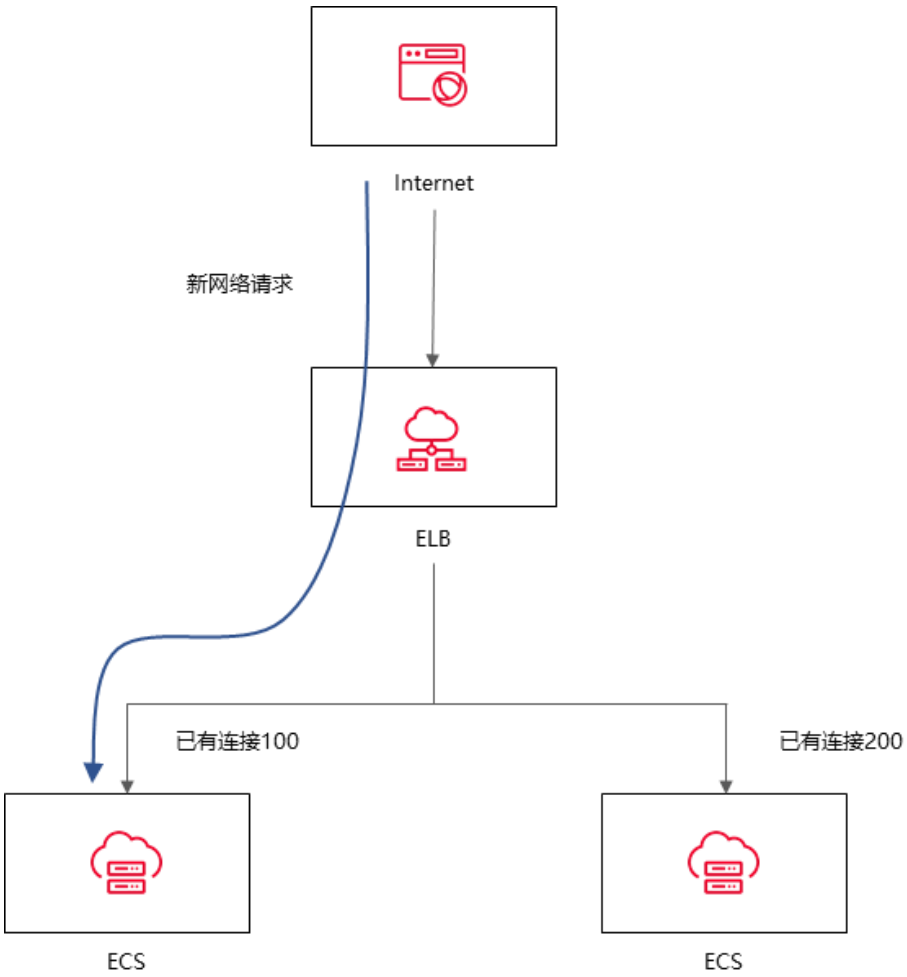
- 轮询算法根据后端主机的权重，将流量按照顺序逐个分发给后端主机，每台主机依次接收请求，实现流量均衡。相应的权重表示后端主机的处理性能，常用于短连接服务。
- 权重取值范围为[1,256]。



最小连接算法

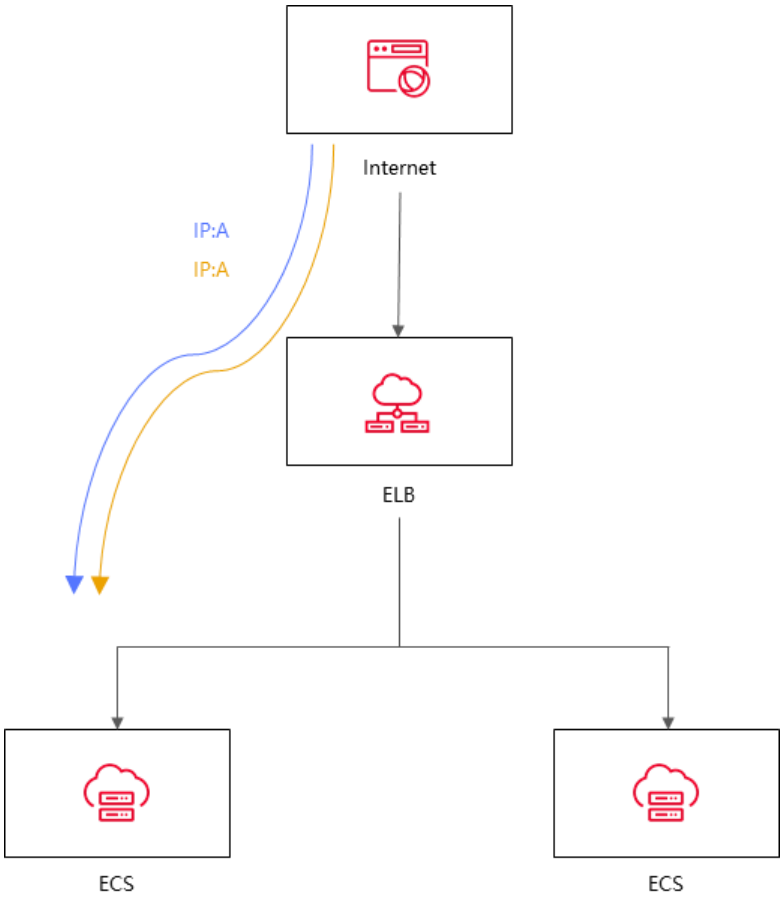
- 最小连接算法将流量分发给当前连接数最少的主机，以确保负载较小的主机能够处理更多的请求。加权最小连接即根据主机的权重和当前连接数来分发流量，常用于长连接服务。

- 权重取值范围为[1,256]。



源 IP 算法

- 源 IP 算法将请求的源 IP 地址进行 Hash 运算，得到一个具体的数值，同时对后端主机进行编号，按照运算结果将请求分发到对应编号的主机上。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主机。
- 在非 0 的权重下，由于使用了源 IP 算法，各个后端主机的权重属性将不再生效。



4.4 后端云主机

4.4.1 后端主机概述

后端主机是指可接收和处理来自负载均衡器转发的流量的云主机实例。弹性负载均衡将传入的网络流量分发到多个后端主机进行处理，以实现负载均衡和提高应用程序的可用性、可扩展性和性能并屏蔽单点故障。

针对在某些特定时间段内，业务流量出现大幅度波动，可以使用负载均衡集成弹性伸缩服务来实现自动化的资源调整。弹性伸缩服务可以根据业务流量的变化自动调整云主机数量，从而保证业务处理能力的充足和稳定，提高业务的可用性和性能。同时，结合负载均衡技术，可以将流量合理地分配到多个云主机上进行处理，进一步提高业务的处理效率和吞吐量。

后端主机通常是通过后端主机组进行管理的，您可以配置每个主机的和端口，并将后端主机与主机组进行关联。

约束与限制；

- 目前仅支持添加与负载均衡器同 VPC 的云主机实例作为后端主机。
- 一个负载均衡实例的监听器可绑定的主机数量为 100 台。

后端主机的权重

后端主机的权重用于指定负载均衡器在将请求分发给后端主机时所采用的权重比例。通过为每个后端主机设置不同的权重，可以实现对主机资源的分配控制和负载均衡策略的调整。

天翼云负载均衡支持的算法会根据后端主机的权重比例，决定将多少流量分发给每个后端主机，具体如下：

调度算法	权重	算法策略
轮询	调度算法权重算法策略轮询权重取值范围为[1,256]	根据后端主机的权重，将流量按照顺序逐个分发给后端主机，每台主机依次接收请求，实现流量均衡。相应的权重表示后端主机的处理性能，常用于短连接服务。
最小连接	权重取值范围为[1, 256]	将流量分发给当前连接数最少的主机，以确保负载较小的主机能够处理更多的请求。加权最小连接即根据主机的权重和当前连接数来分发流量，常用于长连接服务。

源算法	在非 0 的权重下，由于使用了源算法，各个后端主机的权重属性将不再生效	将请求的源 IP 地址进行 Hash 运算，得到一个具体的数值，同时对后端主机进行编号，按照运算结果将请求分发到对应编号的主机上。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主机。

通过调整后端服务器的权重，您可以根据服务器的性能、处理能力或其他因素，合理分配请求流量。较高权重的主机将处理更多的请求，而较低权重的主机将处理较少的请求，从而实现负载均衡和资源优化。

4.4.2 添加后端云主机

操作场景：

在使用负载均衡服务时，确保至少有一台后端主机在正常运行，可以接收负载均衡转发的客户端请求。

负载均衡器支持随时增加或减少后端主机数量，保证应用业务的稳定和可靠。

前提条件：

您已经创建了弹性云主机，具体操作可参考创建弹性云主机。

使用须知：

- 目前仅支持添加与负载均衡器同 VPC 的云主机实例作为后端主机。
- 一个负载均衡实例的监听器可绑定的主机数量为 100 台。

负载均衡器运行时增加或减少负载均衡器的后端主机的数量，且可以支持不同的后

端主机切换操作。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一台正常运行的云主机。

操作建议

建议您选择相同操作系统的后端主机，以便日后管理和维护。

新添加后端主机后，若健康检查开启，负载均衡器会向后端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。

关机或重启已有业务的后端主机，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。

如果您开启了会话保持功能，那么有可能会造成后端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。

操作步骤

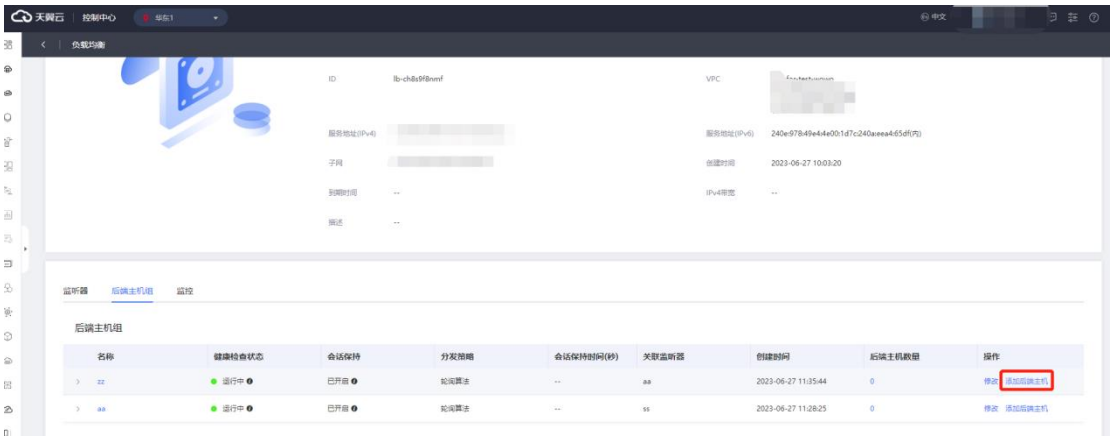
1.登录天翼云控制中心。

2.选择“网络>弹性负载均衡>负载均衡器”。

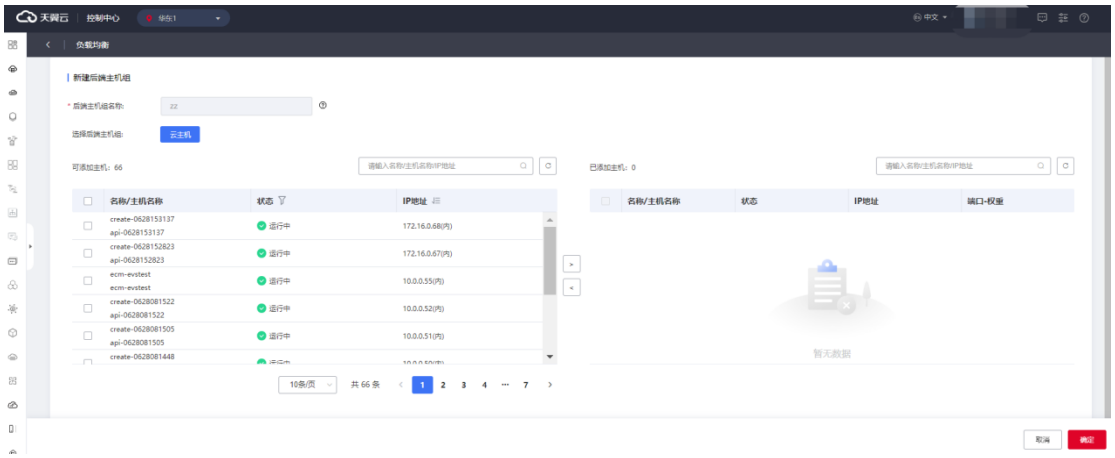
3.单击已创建的负载均衡器实例名称。

4.在该负载均衡详情界面，选择“后端主机组”标签。

5.选定特定的后端主机组，点击“添加后端主机”。



6.在主机列表中选择要添加的云主机，点击“确定”即完成后端云主机的添加。



您也可以在添加监听器的过程中添加后端主机，具体操作可参考用户指南添加监听器。

4.4.3 查看后端云主机

操作场景

天翼云弹性负载均衡支持已添加的后端云主机详情及其状态。还支持查看特定云主机相关的弹性网卡、云硬盘、安全组、弹性 IP 等信息。

前提条件

您已经创建了云主机，并添加云主机到特定的负载均衡监听器上，且后端云主机处于“运行中”状态。

操作步骤

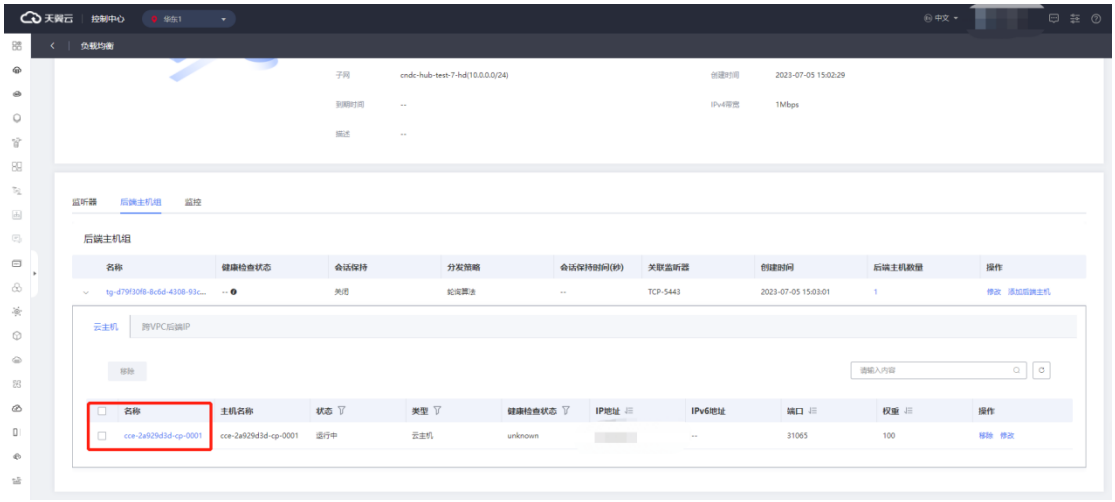
1.登录天翼云控制中心。

2.选择“网络>弹性负载均衡>负载均衡器”。

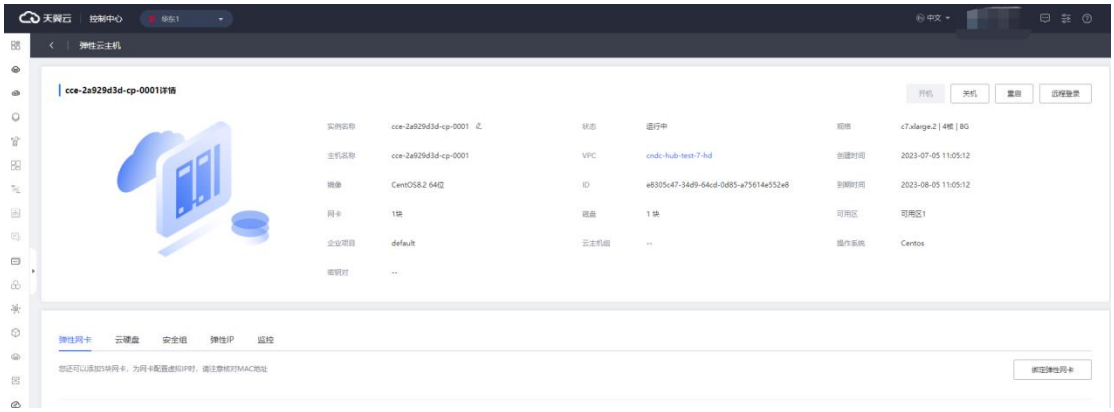
3.单击已创建的负载均衡器实例名称。

4.在该负载均衡详情界面，选择“后端主机组”标签。

5.选定特定的后端主机组，在云主机列表中可查看添加的后端云主机。



5. 点击特定的云主机的名称，即可查看改云主机详情。



4.4.4 移除后端云主机

操作场景

解绑后端主机与负载均衡器的关联后，后端主机将不再接收到负载均衡器转发的请

求，但这不会对云主机本身造成任何影响。您可以在业务增长或需要增强可靠性时重新将其添加到后端主机组中。

操作步骤

1.登录天翼云控制中心。

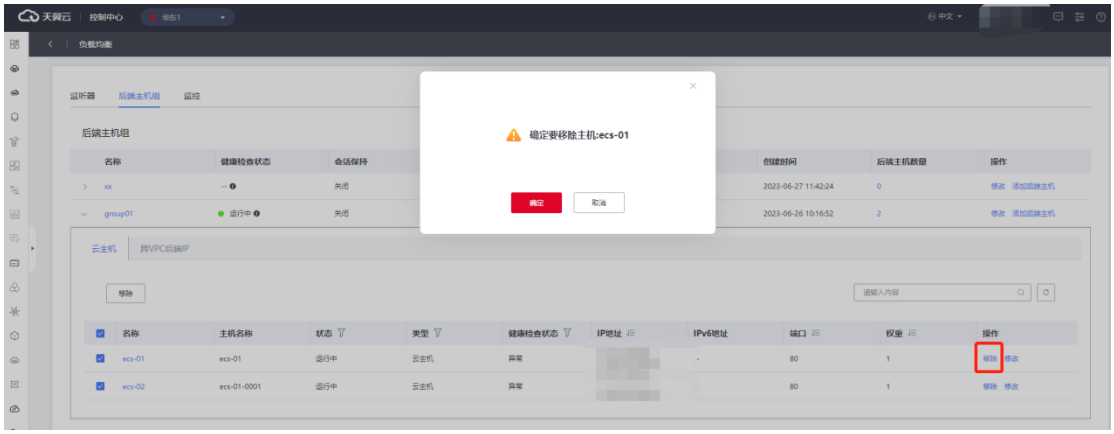
2.选择“网络>弹性负载均衡>负载均衡器”。

3.单击已创建的负载均衡器实例名称。

4.在该负载均衡详情界面，选择“后端主机组”标签。

5.选定特定的后端主机组，从云主机列表中选择要移除的主机，点击“移除”。

6.点击“确定”即完成移除云主机操作。



4.4.5 修改后端主机端口和权重

操作场景

负载均衡后端主机组支持对后端主机的端口和权重进行修改，权重越高的后端主机将被分配到越多的访问请求。

修改后端主机端口和权重功能目前仅在集群模式资源池上线。主备、集群模式资源池列表见产品简介>产品类型和规格>按资源池区分，实际情况以控制台展现为准。

使用须知

在将后端云主机添加到弹性负载均衡器后，您可以为每个后端云主机指定不同的端口号。每台后端主机的权重取值范围为[1, 256]。

操作步骤

1.登录天翼云控制中心。

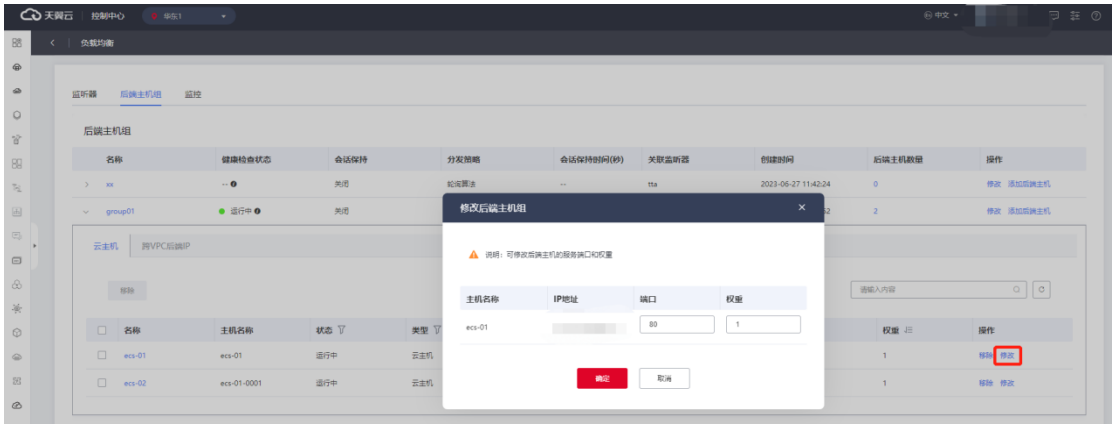
2.选择网络>弹性负载均衡>负载均衡器”。

3.单击已创建的负载均衡器实例名称。

4.在该负载均衡详情界面，选择“后端主机组”标签。

5.选定特定的后端主机组，点击左侧箭头展开主机组，显示“云主机”和“跨 VPC 后端 IP”两个选项卡，选择“云主机”选项卡。

6.从云主机列表中选择要修改的云主机，点击“修改”。



6.依据后端主机端口和权重配置说明，在弹出的修改后端主机窗口内修改后端主机的端口和权重配置。

7.点击“确定”，即可完成修改后端主机端口和权重的操作。

后端主机端口和权重配置说明

参数	说明
端口	后端云主机的服务监听端口，取值范围[1-65535]。

权重	后端虚拟机权重。权重值决定了后端云主机处理的请求的比例。例如，一个权重为 2 的云主机处理的请求数是权重为 1 的两倍。默认情况下，权重为 1。

4.4.6 后端主机安全组配置

操作场景

为了确保负载均衡器与后端服务器之间的正常通信和健康检查，添加后端服务器后需要检查后端服务器所属的安全组规则和网络 ACL 规则。当流量从弹性负载均衡器转发到后端服务器时，源 IP 将被替换为 100.89.0.0/16 网段的 IP 地址。

后端服务器的安全组规则应配置为允许 100.89.0.0/16 网段的流量通过。

网络 ACL 规则是子网级别的可选安全层，如果弹性负载均衡器的后端子网关联了网络 ACL，则网络 ACL 规则应配置为允许源地址为弹性负载均衡器的后端子网所属网段的流量通过。

约束与限制

在启用健康检查的情况下，后端云主机组的安全组规则需要配置允许弹性负载均衡器进行健康检查所需的协议和端口。如果健康检查使用 UDP 协议，还需要配置安全组规则以允许 ICMP 协议通过，否则将无法对已添加的后端云主机执行健康检查。

- **配置安全组规则**

对于首次创建后端服务器时未配置过 VPC 的情况，系统会自动创建默认 VPC。然而，默认 VPC 的安全组策略是禁止外部访问的，即外部网络无法直接访问后端服务器。为了确保负载均衡器能够在监听器端口和健康检查端口上与已创建的后端服务器进行通信，您需要配置安全组入方向的访问规则。

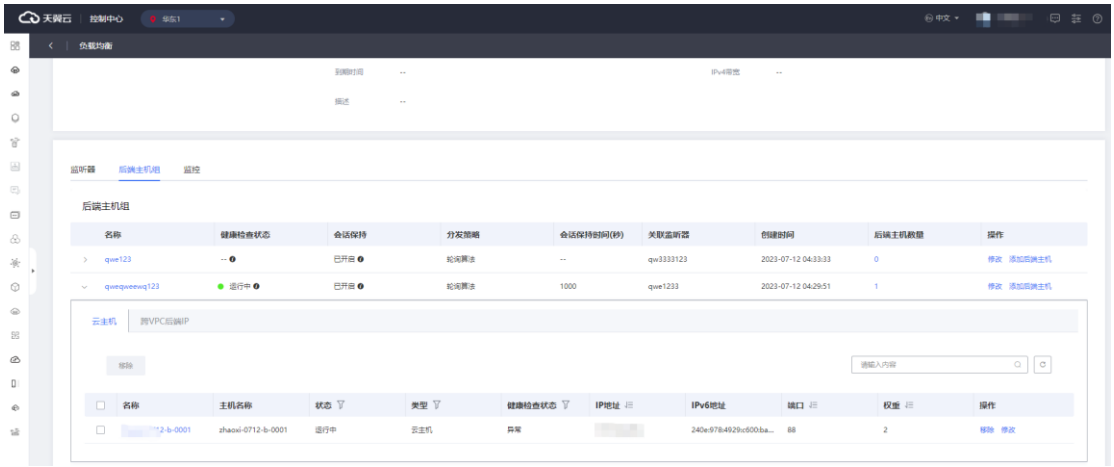
操作步骤

1.点击天翼云门户首页的“控制中心”，输入登录的用户名和密码，进入控制中心页面；

2.在管理控制台顶端单击图标，选择区域，本文选择华东-华东 1；

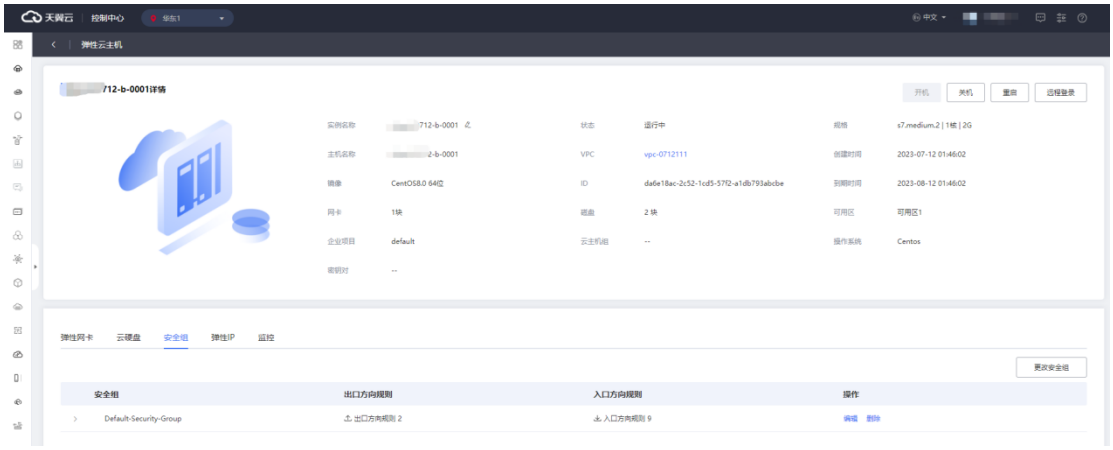
3.在系统首页，选择 “ “网络>弹性负载均衡>负载均衡器” ；

4.点击指定的弹性负载均衡器名称，进入负载均衡器详情页面，点击后端主机组页签查看已添加的弹性云主机；

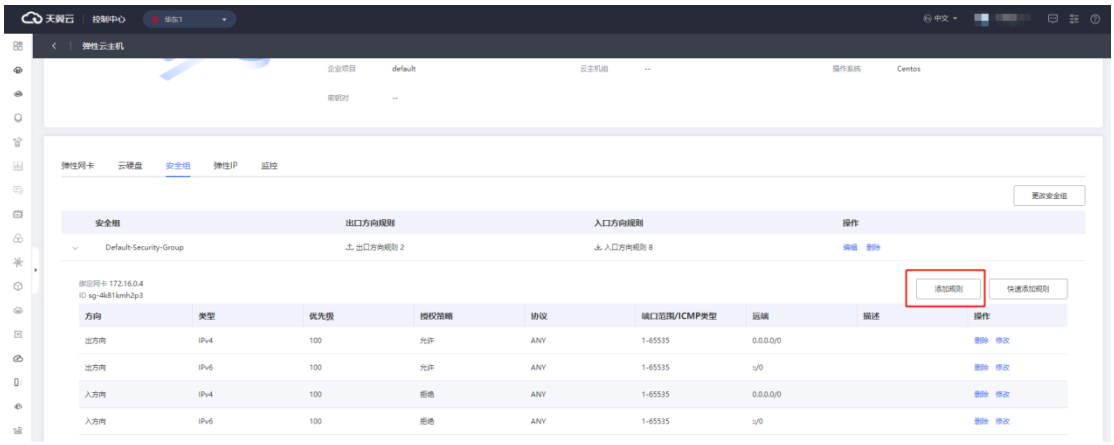


5.点击待变更安全组规则的弹性云主机名称；

6.在跳转的弹性云主机详情页面，点击“安全组”页签；



7.点击安全组名称，在下拉页面点击“添加规则” ；



8.添加规则具体可参考帮助中心>虚拟私有云>安全组>添加安全组规则；

9.根据所在后端主机组的后端协议类型在弹出的页面配置入方向规则；

协议	授权策略	协议端口	源地址
HTTP	允许	协议：TCP 端口：后端主机端口和健康检查端口	100.89.0.0/16
TCP	允许	协议：TCP 端口：健康检查端口	100.89.0.0/16
UDP	允许	协议：UDP、ICMP 端口：健康检查端口	100.89.0.0/16

10.点击“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，用于控制进出子网的数据流，通过与子网关联的入方向/出方向规则进行管理。与安全组类似，网络 ACL 可以增加额外的安全防

护层。

然而，需要注意的是，网络 ACL 的默认规则会拒绝所有的入站和出站流量。如果网络 ACL 与负载均衡所在的子网或与负载均衡关联的后端服务器所在的子网相同，那么负载均衡的业务可能会受到影响，无法接收来自公网或私网的请求流量，导致后端服务器异常。

如果您想要允许来自特定 IP 网段（例如 100.89.0.0/16）的流量通过网络 ACL，您可以配置入方向规则，放行该网段的流量。

需要特别注意的是，由于负载均衡会将公网 IP 转换为内部的 100.89.0.0/16 网段的 IP 地址，因此无法通过配置网络 ACL 规则来限制公网 IP 访问后端服务器。所以，即使您修改了网络 ACL，也不会影响负载均衡将公网 IP 转换为内部 IP 的行为。

使用须知

网络 ACL 无法直接限制客户端对负载均衡器的访问。负载均衡器的 IP 地址不受后端子网所配置的网络 ACL 规则的限制，因此客户端仍然可以直接访问负载均衡器。

如果您需要限制客户端对负载均衡器的访问，建议使用监听器的访问控制功能，具体可参考配置访问控制。

操作步骤

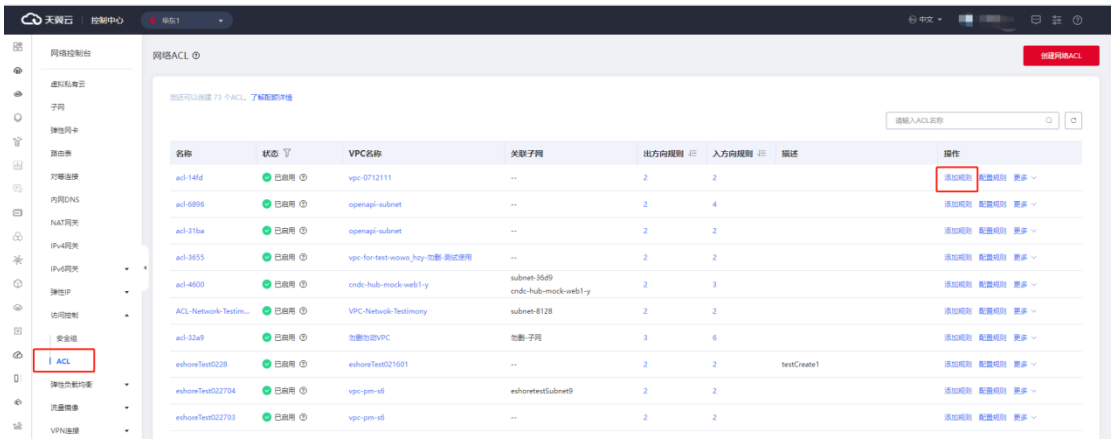
1.点击天翼云门户首页的“控制中心”，输入登录的用户名和密码，进入控制中心页面；

2.在管理控制台顶端单击图标，选择区域，本文选择华东-华东 1；

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，选择需要修改的“网络 ACL 名称”点击“添加规则” ；



6.配置具体操作参数可参考帮助中心>虚拟私有云>网络 ACL> 添加 ACL 规则;

参数	配置
策略	选择允许。
协议	和后端协议一致。
源地址	此方向允许的源地址，填写 100.89.0.0/16。
源端口范围	选择业务所在端口范围，选择 TCP 或 UDP 协议时必须填写。
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，选择 TCP 或 UDP 协议时必须填写。
描述	网络 ACL 规则的描述信息，非必填项。

7.单击“确定”，完成相关配置。

4.4.7 跨 VPC 后端 IP

4.4.7.1 添加跨 VPC 后端 IP

操作场景

天翼云后端主机组不仅可以添加同一 VPC 内的云主机作为后端主机，还支持通过跨 VPC 后端功能将其他 VPC 的 IP 地址添加为后端主机。

使用须知

- 添加跨 VPC 后端 IP 功能目前仅在集群模式资源池上线。主备、集群模式资源池列表见产品简介>产品类型和规格>按资源池区分，实际情况以控制台展现为准。
- 当前仅支持添加其它 VPC 的后端主机，暂不支持添加通过专线打通的线下 IDC 的主机。
- 跨 VPC 后端 IP 添加仅支持对等连接的对端 VPC 后端主机以 IP 形式添加。
- 您最多可添加 200 个跨 VPC 后端 IP，如需要申请更多，则需申请增加配额。

操作步骤

1.登录天翼云控制中心。

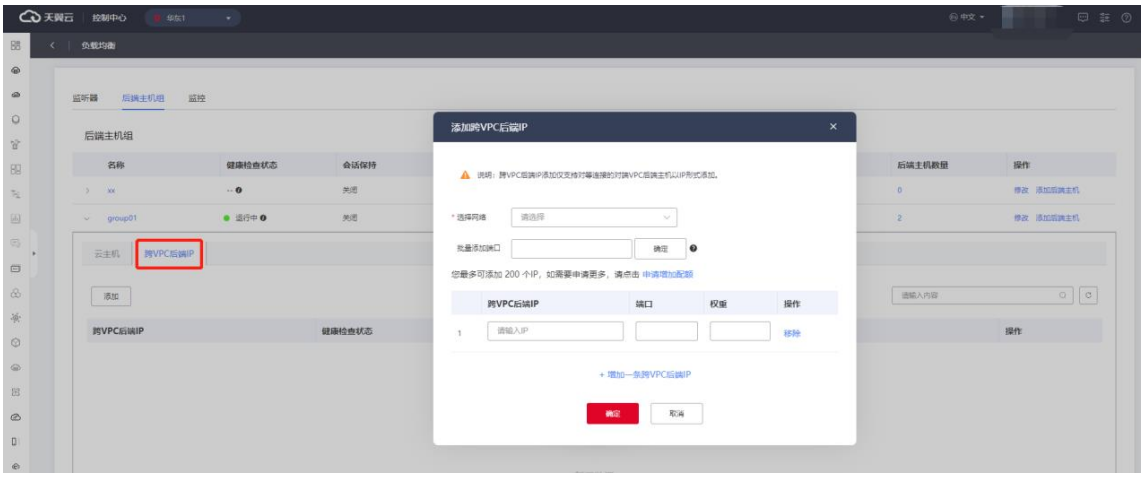
2.选择网络>弹性负载均衡>负载均衡器”。

3.单击已创建的负载均衡器实例名称。

4.在该负载均衡详情界面，选择“后端主机组”标签。

5.选定特定的后端主机组，点击左侧箭头展开主机组，显示“云主机”和“跨 VPC 后端 IP”两个选项卡，选择“跨 VPC 后端 IP”选项卡。

6.点击“添加”按钮。



1.在弹出添加跨 VPC 后端 IP 窗口，依据跨 VPC 后端 IP 参数配置完成添加跨 VPC 后端 IP 参数配置。

2.点击“增加一条跨 VPC 后端 IP”新增一行，可连续添加多行。

3.点击“确定”按钮，完成添加跨 VPC 后端 IP 设置。

跨 VPC 后端 IP 参数配置

跨 VPC 后端 IP 配置	**说明**
选择网络	选择 ELB 实例所在 VPC 之外的其它 VPC，从下拉列表框选择。
批量添加端口	跨 VPC 后端 IP 的服务端口一致时，可在此输入框输入端口，点击确定自动填充所有跨 VPC 后端 IP 的端口设置。
后端 IP 添加	填写跨 VPC 后端 IP、端口、权重，权重不填写缺省为 1，支持移除操作；端口范围为 1-65535；权重取值范围为 1- 256。

4.4.7.2 查看跨 VPC 后端 IP

操作场景

天翼云弹性负载均衡支持查看已经添加在主机组中的跨 VPC 后端 IP 信息。

该功能目前仅在集群模式资源池上线。主备、集群模式资源池列表见产品简介>产品类型和规格>按资源池区分，实际情况以控制台展现为准。

前提条件

您已经在监听器的后端主机组中添加了跨 VPC 后端 IP。

操作步骤

1.登录天翼云控制中心。

2.选择“网络>弹性负载均衡>负载均衡器”。

3.单击已创建的负载均衡器实例名称。

4.在该负载均衡详情界面，选择“后端主机组”标签。

5.选定特定的后端主机组，点击左侧箭头展开主机组，选择“跨 VPC 后端 IP”选项卡，在列表中可查看添加的跨 VPC 后端 IP。

4.4.7.1 修改跨 VPC 后端 IP 端口和权重

操作场景

负载均衡后端主机组支持对跨 VPC 后端 IP 的端口和权重进行修改，权重越高的后端主机将被分配到越多的访问请求。

修改后端主机端口和权重功能目前仅在集群模式资源池上线。主备、集群模式资源池列表见产品简介>产品类型和规格>按资源池区分，实际情况以控制台展现为准。

使用须知

在将跨 VPC 后端 IP 作为后端云主机添加到弹性负载均衡器后，您可以为每个跨 VPC 后端 IP 指定不同的端口号和权重。端口号的取值范围为[1,65535]，权重取值范围为[1, 256]。

操作步骤

1.登录天翼云控制中心。

2.选择网络>弹性负载均衡>负载均衡器”。

3.单击已创建的负载均衡器实例名称。

4.在该负载均衡详情界面，选择“后端主机组”标签。

5.选定特定的后端主机组，点击左侧箭头展开主机组，选择“跨 VPC 后端 IP”选项卡。

6.从云主机列表中选择要修改的后端 IP，点击“修改”。

7.依据后端主机端口和权重配置说明，在弹出的修改后端主机窗口内修改后端主机的端口和权重配置。

8.点击“确定”，即可完成修改后端主机端口和权重的操作。

后端主机端口和权重配置说明

参数	说明
端口	后端云主机的服务监听端口，取值范围[1-65535]。
权重	后端虚拟机权重。权重值决定了后端云主机处理的请求的比例。例如，一个权重为 2 的云主机处理的请求数是权重为 1 的两倍。默认情况下，权重为 1。

4.4.7.2 移除跨 VPC 后端 IP

操作场景

天翼云弹性负载均衡支持对已经添加在主机组中的跨 VPC 后端 IP 进行移除。

该功能目前仅在集群模式资源池上线。主备、集群模式资源池列表见产品简介>产品类型和规格>按资源池区分，实际情况以控制台展现为准。

前提条件

您已经在监听器的后端主机组中添加了跨 VPC 后端 IP。

操作步骤

1.登录天翼云控制中心。

2.选择“网络>弹性负载均衡>负载均衡器”。

3.单击已创建的负载均衡器实例名称。

4.在该负载均衡详情界面，选择“后端主机组”标签。

5.选定特定的后端主机组，点击左侧箭头展开主机组，选择“跨 VPC 后端 IP”选项卡，在列表中选择要移除的跨 VPC 后端 IP，点击“移除”。

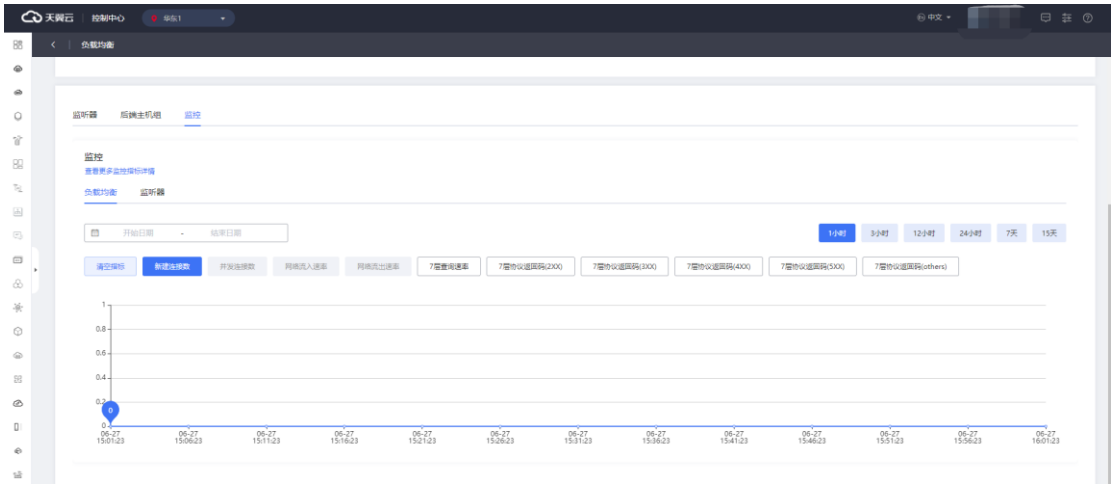
6.在弹框中点击“确认”完成移除。

4.5 监控

操作步骤

1. 在系统首页，选择网络>弹性负载均衡>负载均衡器”。

2. 在负载均衡器列表页面，找到目标实例，单击实例名称进入实例详情页，可查看监控页面。



3. 目前支持对负载均衡器和监听器进行 2 个维度的监控。

4. 为保证弹性负载均衡产品正常使用，在使用之前，请您务必仔细阅读以下监控指标和告警规则。

弹性负载均衡监控指标

序号	指标名称	指标描述
1	活跃连接数	统计测量对象当前处理的活跃连接数量

2	新建连接数	统计测量对象每秒新建连接数量
3	并发连接数	统计测量对象当前处理的并发连接数量
4	网络流入速率	统计每秒流入测量对象的网络流量
5	网络流出速率	统计每秒流出测量对象的网络流量
6	7 层查询速率	该指标用于统计测量对象当前 7 层查询速率
7	7 层协议返回码（2XX）	该指标用于统计测量对象当前 7 层协议 2XX 系列状态响应码的数量
8	7 层协议返回码（3XX）	该指标用于统计测量对象当前 7 层协议 3XX 系列状态响应码的数量
9	7 层协议返回码（4XX）	该指标用于统计测量对象当前 7 层协议 4XX 系列状态响应码的数量
10	7 层协议返回码（5XX）	该指标用于统计测量对象当前 7 层协议 5XX 系列状态响应码的数量
11	7 层协议返回码（Others）	该指标用于统计测量对象当前 7 层协议非 2XX，3XX，4XX，5XX 系列状态响应码的数量

弹性负载均衡告警规则

序号	指标名称	指标描述	单位
1	活跃连接数	统计测量对象当前处理的活跃连接数量	个
2	新建连接数	统计测量对象当前处理的新建连接数量	个
3	并发连接数	统计测量对象当前处理的并发连接数量	个

4	网络流入速率	统计每秒流入测量对象的网络流量	字节/秒
5	网络流出速率	统计每秒流出测量对象的网络流量	字节/秒
6	7 层查询速率	该指标用于统计测量对象当前 7 层查询速率	次/秒
7	7 层协议返回码（2XX）	该指标用于统计测量对象当前 7 层协议 2XX 系列状态响应码的数量	个/秒
8	7 层协议返回码（3XX）	该指标用于统计测量对象当前 7 层协议 3XX 系列状态响应码的数量	个/秒
9	7 层协议返回码（4XX）	该指标用于统计测量对象当前 7 层协议 4XX 系列状态响应码的数量	个/秒
10	7 层协议返回码（5XX）	该指标用于统计测量对象当前 7 层协议 5XX 系列状态响应码的数量	个/秒
11	7 层协议返回码（Others）	该指标用于统计测量对象当前 7 层协议非 2XX，3XX，4XX，5XX 系列状态响应码的数量	个/秒

4.6 证书管理

4.6.1 证书概述

如果 ELB 的监听器和客户端之间使用 HTTPS，需要在 ELB 上部署 SSL 证书。ELB 先使用此证书来终结客户端的 HTTPS 连接，解密来自客户端的请求，再将客户端请求通过 HTTP 方式发送到后端主机组。

天翼云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。

单向认证

客户端需要认证主机端的真实性，而主机端不需要认证客户端的真实性。当配置 ELB HTTPS 类型的监听器时，需要绑定服务器证书。

双向认证

客户端需要认证主机端真实性，同时主机端也需要认证客户端的真实性，需要双方都通过认证，才能正常建立连接响应请求。当配置 ELB HTTPS 类型的监听器，并开启双向认证时，在为监听器绑定服务器证书的同时，还需要绑定 CA 证书来验证客户端的真实性。这样只有当客户端能够出具指定 CA 签发的证书时，HTTPS 才能连接成功。

使用须知

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。

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。

4.6.2 证书格式

证书格式要求

在创建证书时，支持粘贴证书到内容框，或点击上传证书内容。证书包含证书的公钥和签名等信息，证书扩展名为".pem"或".crt"，您可直接输入证书内容或上传证书文件。-（1）通过 Root CA 机构颁发的证书，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。Root CA 证书格式必须符合如下要求：以-----BEGIN CERTIFICATE-----，-----END CERTIFICATE-----开头和结尾。每行 64 个字符，最后一行长度可以不足 64 个字符。证书内容不能包含空格。（2）通过中级 CA 机构颁发的证书，证书文件包含多份证书，需要将服务器证书与中级证书合并在一起上传。证书链格式必须符合如下要求：-----BEGIN CERTIFICATE----------END CERTIFICATE----------BEGIN CERTIFICATE----------END CERTIFICATE----------BEGIN CERTIFICATE----------END CERTIFICATE-----服务器证书放第一位，中级证书放第二位，中间不能有空行。证书内容不能包含空格。证书之间不能有空行，并且每行 64 字节。符合证书的格式要求。

私钥格式要求

私钥是证书的关键部分，用于加密和解密通信数据。建议在生成和使用私钥时，遵循最佳实践并确保其安全性，以保护您的通信安全。

证书的私钥，私钥扩展名为"key",您可直接输入私钥文件内容或上传符合格式的私钥文件。私钥内容格式为:以“-- BEGIN RSA PRIVATE KEY --”作为开头，“--- END RSA PRIVATE KEY--- ”作为结尾。

4.6.3 创建服务器证书

操作场景

当前支持服务器证书，用于 SSL 握手协商，需提供证书内容和私钥，在证书管理页面可创建和管理证书。

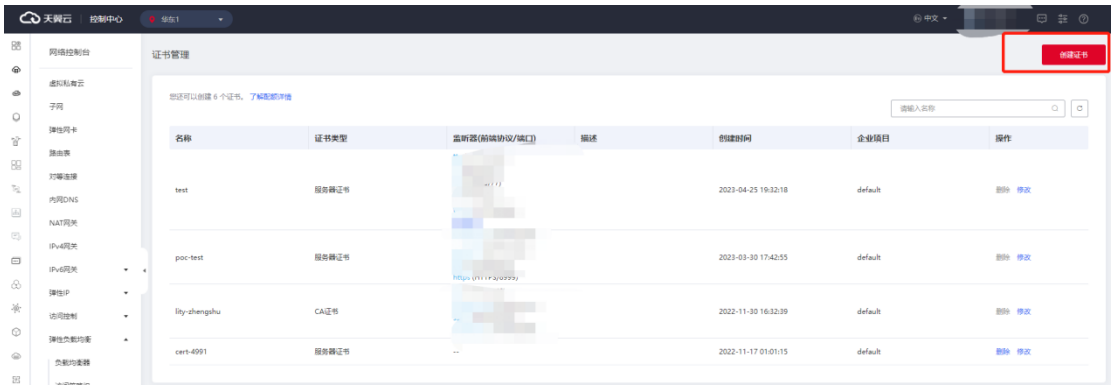
操作步骤

1.点击天翼云门户首页的“控制中心”，输入登录的用户名和密码，进入控制中心页面。

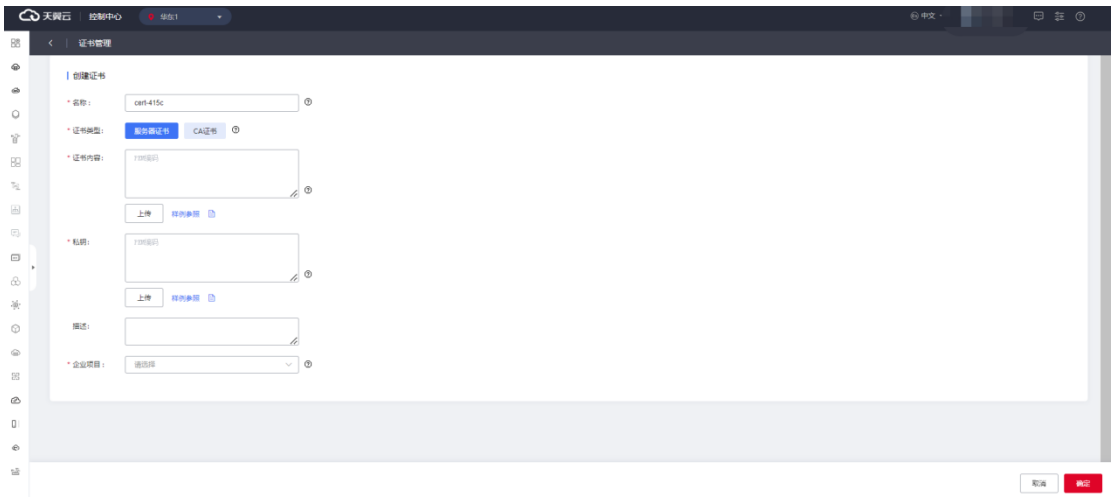
2.在管理控制台上方单击图标，选择区域，本文操作均选择华东-华东 1。

3.在系统首页，选择“网络>弹性负载均衡>证书管理”。

4.在负载均衡页面，单击“创建负载均衡”，进入负载均衡创建页面。



5.参考服务器证书管理配置说明，点击“确定”，完成证书创建。



服务器证书管理配置说明

参数	说明
名称	证书名称，只能由数字、字母、-组成,不能以数字和-开头、以-结尾,且长度为 2-63 字符。
证书类型	可选服务器或者 CA 证书，本操作选择服务器证书。 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 HTTPS 双向认证功能时，只有当客户端能够出具指定 CA 签发的证书时，HTTPS 连接才能成功。
证书内容	支持粘贴证书到内容框，或点击上传证书内容。证书包含证书的公钥和签名等信息，证书扩展名为".pem"或".crt"，您可直接输入证书内容或上传证书文件。- （1）通过 Root CA 机构颁发的证书，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。 Root CA 证书格式必须符合如下要求： 以-----BEGIN CERTIFICATE-----, -----END CERTIFICATE-----开头和结尾。 每行 64 个字符，最后一行长度可以不足 64 个字符。证书内容不能包含空格。 （2）通过中级 CA 机构颁发的证书，证书文件包含多份证书，需要将服务器证书与中级证书合并在一起上传。 证书链格式必须符合如下要求：

	-----BEGIN CERTIFICATE----- -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- -----END CERTIFICATE----- 服务器证书放第一位，中级证书放第二位，中间不能有空行。 证书内容不能包含空格。 证书之间不能有空行，并且每行 64 字节。 符合证书的格式要求。一般情况下，证书机构在颁发证书时会有对应说明，证书要符合证书机构的格式要求。
私钥	证书的私钥，私钥扩展名为"key",您可直接输入私钥文件内容或上传符合格式的私钥文件。私钥内容格式为:以“-- BEGIN RSA PRIVATE KEY --”作为开头，“--- END RSA PRIVATE KEY--- ”作为结尾。
描述	填写证书相关描述，可选。
企业项目	选择所述的企业项目名称，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。

4.6.4 创建 CA 证书

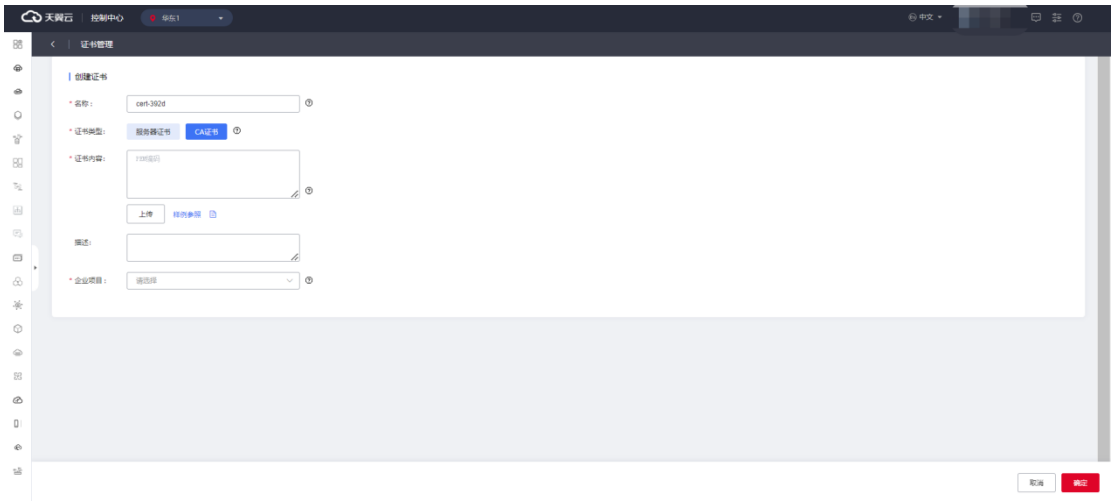
操作场景

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。

操作步骤

1. 在弹性负载均衡证书管理页面点击“创建证书”，进入证书创建页面。



2. 参考 CA 证书管理配置说明，点击“确定”，完成证书创建。

CA 证书管理配置说明

参数	说明
名称	证书名称，只能由数字、字母、-组成,不能以数字和-开头、以-结尾,且长度为 2-63 字符。
证书类型	可选服务器或者 CA 证书，本操作选择 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 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。CA 证书只有单证书，无私钥。
证书内容	支持粘贴证书到内容框，或点击上传证书内容。证书包含证书的公钥

	和签名等信息，证书扩展名为".pem"或".crt"，您可直接输入证书内容或上传证书文件。- （1）通过 Root CA 机构颁发的证书，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。 Root CA 证书格式必须符合如下要求： 以-----BEGIN CERTIFICATE-----, -----END CERTIFICATE-----开头和结尾。 每行 64 个字符，最后一行长度可以不足 64 个字符。证书内容不能包含空格。 （2）通过中级 CA 机构颁发的证书，证书文件包含多份证书，需要将服务器证书与中级证书合并在一起上传。 证书链格式必须符合如下要求： -----BEGIN CERTIFICATE----- -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- -----END CERTIFICATE----- 服务器证书放第一位，中级证书放第二位，中间不能有空行。 证书内容不能包含空格。 证书之间不能有空行，并且每行 64 字节。 符合证书的格式要求。一般情况下，证书机构在颁发证书时会有对应

	说明，证书要符合证书机构的格式要求。
描述	填写证书相关描述，可选。
企业项目	选择所述的企业项目名称，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。

4.6.5 修改证书

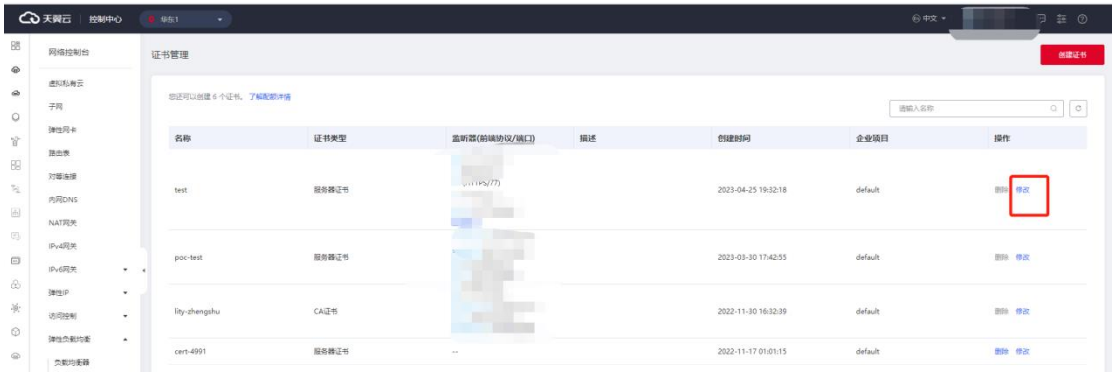
使用须知

服务器证书的证书内容和私钥必须同时替换修改，可复制粘贴到输入框替换现有证书，或通过上传证书内容替换，不可编辑修改当前证书内容，否则将引起证书认证失败故障。

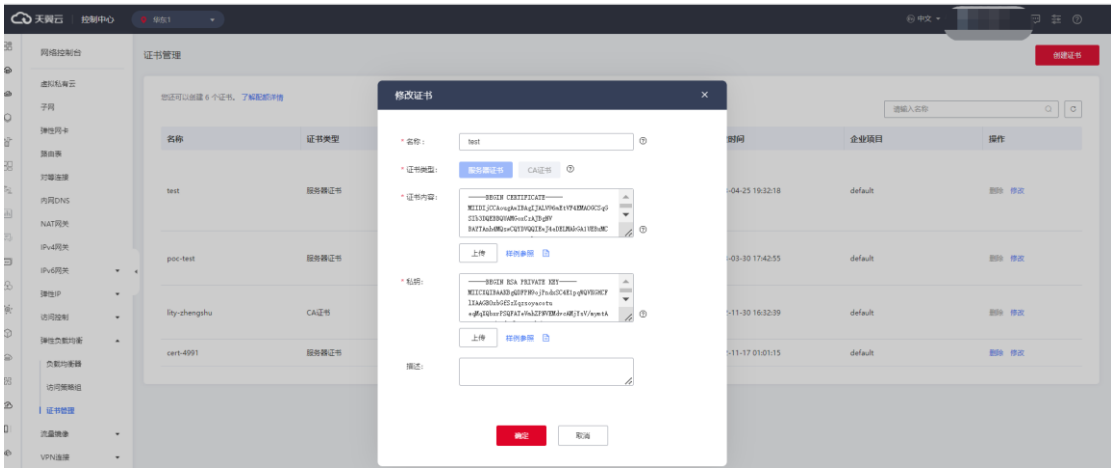
操作步骤

1. 在系统首页，选择“网络>弹性负载均衡>证书管理”。

2. 在证书列表页面，操作字段点击“修改”可修改证书。



3. 在弹出的证书修改页面，依据负载均衡证书修改说明，填写相关参数并点击“确定”，完成证书修改。



负载均衡证书修改说明

参数	说明
名称	自定义修改证书名称，只能由数字、字母、-组成,不能以数字和-开头、以-结尾,且长度为 2-63 字符。
证书类型	不可修改。
证书内容	支持粘贴证书到内容框，或点击上传证书内容。证书包含证书的公钥和签名等信息，证书扩展名为".pem"或".crt"，您可直接输入证书内容或上传证书文件。- （1）通过 Root CA 机构颁发的证书，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。 Root CA 证书格式必须符合如下要求： 以-----BEGIN CERTIFICATE-----, -----END CERTIFICATE-----开头和结尾。 每行 64 个字符，最后一行长度可以不足 64 个字符。证书内容不能包含空格。 （2）通过中级 CA 机构颁发的证书，证书文件包含多份证书，需要将

	服务器证书与中级证书合并在一起上传。 证书链格式必须符合如下要求： -----BEGIN CERTIFICATE----- -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- -----END CERTIFICATE----- 服务器证书放第一位，中级证书放第二位，中间不能有空行。 证书内容不能包含空格。 证书之间不能有空行，并且每行 64 字节。 符合证书的格式要求。一般情况下，证书机构在颁发证书时会有对应说明，证书要符合证书机构的格式要求。
描述	填写负载均衡器相关描述，自定义修改。

4.6.6 绑定/更换证书

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。

更换证书仅部分资源池支持，实际情况以控制台展现为准。

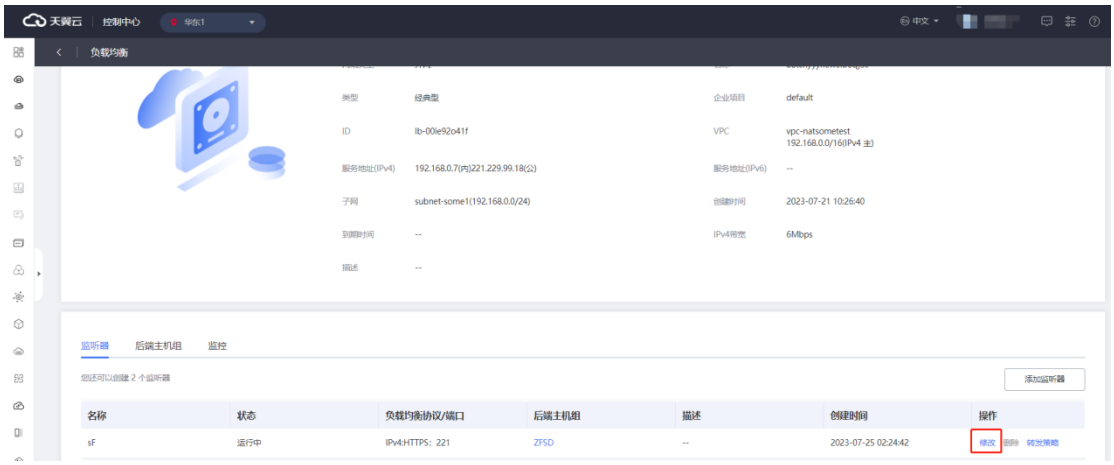
操作场景

为了确保数据传输的安全性和加密认证，创建 HTTPS 协议监听时需要绑定有效的

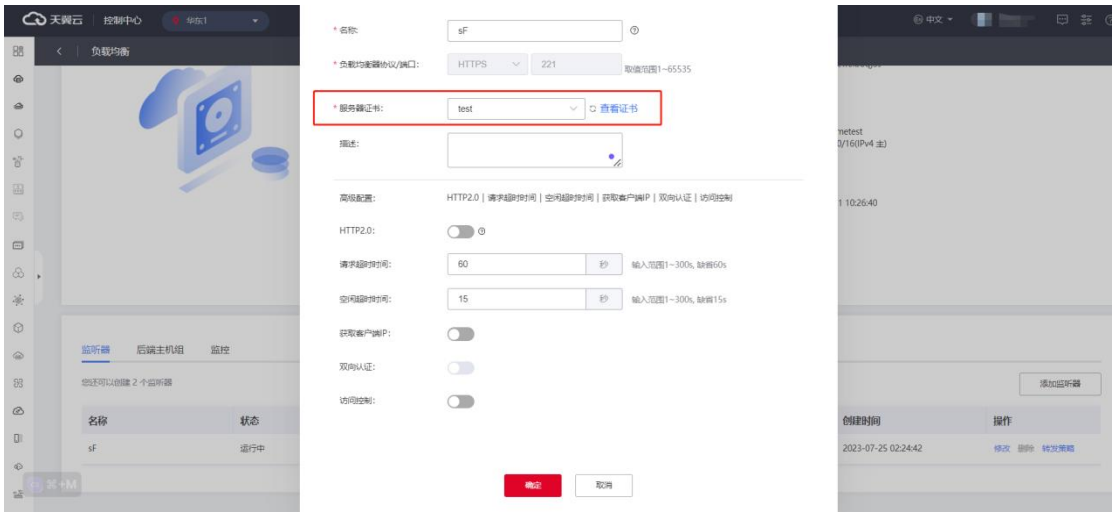
证书，具体可参考添加 HTTPS 监听器。同时，当证书过期或需要更换时，可以参考本文内容进行更换证书相关操作。

操作步骤

1. 点击天翼云门户首页的“控制中心”,输入登录的用户名和密码,进入控制中心页面；
2. 在管理控制台顶端单击图标，选择区域，本文选择华东-华东 1；
3. 在系统首页，选择“网络>弹性负载均衡>负载均衡器”；
4. 在负载均衡器列表页面，点击需要修改 HTTPS 监听器的负载均衡名称；
5. 在弹出页面的“监听器”区域，单击监听器所在行的“修改”选项；



6. 在弹出的页面的“服务器证书”选项中选择要更换的证书；



7.点击“确定”，完成证书更换。

4.6.7 删除证书

使用限制

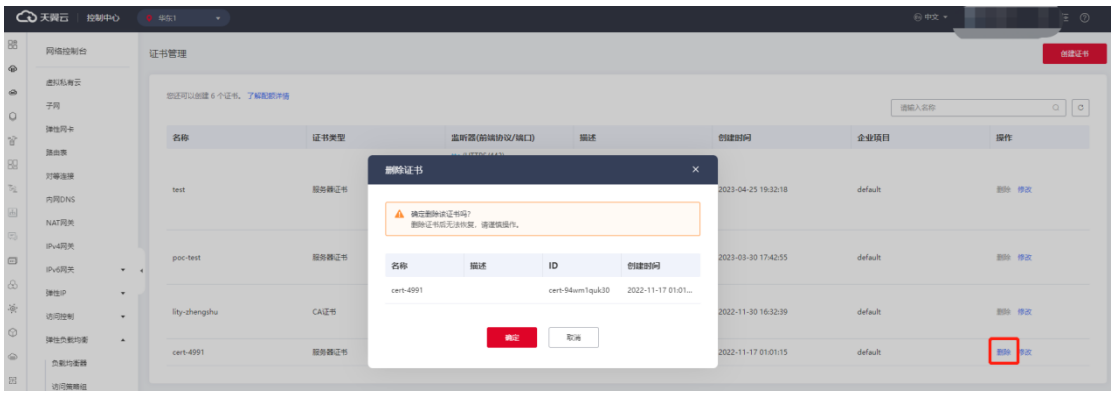
证书删除限制：如果证书关联 HTTPS 监听，则无法删除，需先解除 HTTPS 关联证书，再删除证书。

证书配额限制：每用户可创建 10 个证书。

操作步骤

1.在系统首页，选择“网络>弹性负载均衡>证书管理”。

2.在证书列表页面，操作字段点击“删除”可删除证书。



5 常见问题

5.1 负载均衡器

弹性负载均衡本身是否有高可用性？

负载均衡本身具备高可用性，至少双机部署，在多 AZ 场景下采用高可用集群模式部署，一台 ELB 主机故障或者一个 AZ 的 ELB 主机故障，不影响 ELB 对外提供服务。

如何配置内网或公网负载均衡？

创建负载均衡时，在网络类型字段可选择内网或公网，选择内网时系统分配一个内网 IP，

选择公网时，在下一字段选择已有弹性 IP。如果为内网负载均衡绑定一个公网 EIP，则可作为公网负载均衡使用，同时可支持内网、公网访问。

如何查看弹性负载均衡的地址？

弹性负载均衡的内网地址是在创建时根据所属 VPC 和子网自动创建的 ,目前不能修改。

弹性负载均衡的公网 IP 地址是根据绑定的 EIP 来决定。

可以在“网络>负载均衡>ELB 实例详情”服务地址查看 ELB 的内网地址和公网地址。

弹性负载均衡所属的 VPC 和子网是否支持修改？

不支持。已创建的负载均衡无法更改 VPC 和子网。

使用弹性负载均衡后，后端主机能否访问公网？

后端主机能否访问公网和使用 ELB 没有必然联系 ,ELB 主要是负责访问流量自动分发到多台后端主机上，不会影响后端主机能否访问公网，ELB 本身不为后端主机提供公网访问能力。假如后端主机本身具有访问公网的能力，即使使用了 ELB，后端主机仍然可以进行公网访问。然而，如果后端主机本身不能访问公网，在使用 ELB 后，它仍然无法进行公网访问。

弹性负载均衡是否一定要配置带宽？

如果使用的是内网负载均衡，则不需要配置和购买带宽。

弹性负载均衡的带宽是否可以调整？

公网弹性负载均衡的带宽可以调整，仅支持扩容不允许缩容。目前仅集群模式资源池支持负载均衡 IPv6 带宽，主备、集群模式资源池列表见产品简介>产品类型和规格>按资源池区分，实际情况以控制台展现为准。带宽调整具体可参考用户指南负载均衡修改 IPv4 带宽和负载均衡绑定/解绑 IPv6 带宽。

内网负载均衡支持绑定弹性 IP？

支持，内网 ELB 绑定了弹性 IP 后就变为公网 ELB。具体可以参考用户指南负载均衡绑定/解绑弹性 IP。

弹性负载均衡分配的弹性 IP 是否为独占？

弹性负载均衡绑定的弹性 IP 为独占的，只有 ELB 绑定了 EIP 才能被 Internet 访问。

客户端与服务端的弹性负载均衡建立连接后，为什么会出现 5min 自动断开现象 ？

弹性负载均衡对于 TCP 端口 300 秒不发数据，链接会自动断开，仅集群模式资源池支持时间参数修改，主备、集群模式资源池列表见产品简介>产品类型和规格>按资源池区分，实际情况以控制台展现为准。

弹性负载均衡支持哪些协议？

负载均衡提供四层 TCP/UDP 协议和七层 HTTP/HTTPS 协议监听，可根据应用场景选择合适的监听协议。

监听协议	说明	使用场景
TCP	面向连接的协议，在发送数据之前需要经过三次握手建立可靠的连接，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，如邮件服务、文件传输服务 ;无特殊要求的 web 应用。
UDP	无连接协议 ,发送数据前不需要建立连接 ,直接发送数据 ,不提供差错恢复和数据重传 ;可靠性相对较低 ,需要上层协议做可靠性措施 l 数据传输快。	适用于对实时性要求较高，对可靠性要求相对不高的业务，如语音、视频、证券行情实时推送等。
HTTP	应用层协议，基于 TCP 协议，B/S 架构，浏览器请求数据，服务端响应数据；基于 cookie 做会话保持 ;使用 X-forwarded-for 头字段获取客户端真实 IP 地址。	需要对数据内容进行识别的应用 ,如 web 应用、门户网站等。
HTTPS	加密的 HTTP 传输协议，可阻止未经授权的访问 ;统一的证书管理服务 ,可将证书传至负载均衡，由负载均衡终结处理客户的 HTTPS 请求。	对安全性要求较高的 HTTP 应用 需要加密传输的应用。

使用 UDP 协议有哪些注意事项？

在使用 UDP 协议的弹性负载均衡时，以下是一些需要注意的事项：

UDP 是无连接的协议，您需要确保后端主机能够独立地处理每个 *UDP* 请求。

您需要选择适合您应用程序的负载均衡算法，并确保流量能够均匀分发到后端主机。

UDP 本身不提供可靠性和完整性保证。因此，在设计 *UDP* 健康检查时，需要注意其适用范围和局限性。对于某些应用场景，可能需要结合其他手段来验证 *UDP* 服务的可用性，如在应用层级别实现自定义的心跳机制或应用层级别的错误检测和处理。

弹性负载均衡是否支持跨资源池分流？

不支持跨资源池分流，只能同一个资源池下的云主机进行分流。

如何检查客户端请求是否失败？

您可以监控前端和后端的流量，查看弹性负载均衡监控指标，并对后端实例进行健康检查 ,通过检查客户端请求中是否存在返回码为 4xx 的请求 ,可以确定是否有失败的请求。这些请求可能会因为被弹性负载均衡视为异常请求而被拒绝，从而无法被转发至后端主机。

弹性负载均衡 https 证书是否支持双向认证？

仅集群模式资源池支持，主备、集群模式资源池列表见产品简介>产品类型和规格>按资源池区分，实际情况以控制台展现为准。

弹性负载均衡是否支持获取客户端真实源 IP?

在四层转发（TCP/UDP）服务中，集群模式资源池支持通过配置 TOA 插件获取客户端真实源 IP； 主备模式资源池支持通过 Proxy protocol 获取用户真实 IP， 主备、集群模式资源池列表见产品简介>产品类型和规格>按资源池区分，实际情况以控制台展现为准。在七层转发（HTTP/HTTPS）服务中，弹性负载均衡支持通过 HTTP 头中的 X-Forwarded-For 获取来访者真实 IP。

弹性负载均衡是否支持 HTTP 到 HTTPS 的重定向？

集群模式资源池支持，主备、集群模式资源池列表见产品简介>产品类型和规格>按资源池区分，实际情况以控制台展现为准。HTTP 重定向功能帮助用户业务平滑无感知的从 HTTP 迁移到 HTTPS。

弹性负载均衡是否支持 websocket？

集群模式资源池支持，主备、集群模式资源池列表见产品简介>产品类型和规格>按资源池区分，实际情况以控制台展现为准。如果您选择使用 HTTP 监听器，则默认支持非加密的 WebSocket 协议（WS 协议）。而如果您选择使用 HTTPS 监听器，则默认支持加密的 WebSocket 协议（WSS 协议）。

弹性负载均衡是否支持记录和查询访问日志？

不支持。

弹性负载均衡是否支持访问控制？

弹性负载均衡支持访问控制的操作，您可以通过黑名单禁止特定 IP 访问负载均衡，也可以选择白名单允许特定 IP 访问负载均衡。

基于源地址算法，是否可实现同一源 IP 访问固定后端云主机情况？

选择“源地址算法”，ELB 会将请求的源 IP 地址进行一致性 Hash 运算，得到一个具体的数值，同时对后端主机进行编号，按照运算结果将请求分发到对应编号的主机上。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台特定的主机上。

但是如果后端主机存在下线后重新上线的情况，ELB 会将请求的源 IP 地址重新进行一致性 Hash 运算并对后端主机重新进行编号，因此会出现同一个 IP 地址同时出现在了两台后端主机上。

弹性负载均衡是否可以单独使用？

不可以。弹性负载均衡（CT-ELB ，Elastic Load Balancing）是一种分发控制网络流量的服务，通过预先设定的算法将访问流量自动分发到多台云主机，扩展应用系统对外的服务能力，实现更高水平的应用系统容错性能。弹性负载均衡服务需要和后端主机资源组合使用，才能实现对外服务能力的负载均衡。

弹性负载均衡是否支持 TCP 长连接？

客户端到弹性负载均衡之间支持 TCP 长连接。

弹性负载均衡是否支持后端 FTP 服务？

弹性负载均衡不支持后端 FTP 服务。

弹性负载均衡是否有防 DDoS 攻击和 Web 代码层次安全的功能？

弹性负载均衡没有防 DDoS 攻击和 Web 代码层次安全的功能。

弹性负载均衡对于 IPv6 网络的支持情况是怎样的？

弹性负载均衡支持通过 IPv6 地址对私网和公网提供服务。

对私网提供服务：创建负载均衡器时，如果选择已开启 IPv6 的 VPC 和子网，可以为选择负载均衡器分配 IPv6 地址。负载均衡可通过该 IPv6 地址对 VPC 提供私网服务。

对公网提供服务：创建负载均衡器时，如果选择已开启 IPv6 的 VPC 和子网，可以为选择弹性负载均衡实例分配 IPv6 地址。为分配了 IPv6 地址的弹性负载均衡绑定 IPv6 带宽后，可对通过 IPv6 地址对公网提供服务。

弹性负载均衡如何根据不同的协议来分发流量？

对于入网流量，在负载均衡器使用四层协议 TCP/UDP 时，可以通过 LVS 集群进行转发。LVS 集群的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主机上，从而实现负载均衡。而当负载均衡器使用七层协议 HTTP/HTTPS 时，通常涉及到两个层次的负载均衡。首先，请求会经过 LVS 集群，LVS 会将请求平均分发

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主机。对于七层协议 HTTPS 的流量，在最终分发到后端服务器之前，通常需要在 Nginx 集群内进行证书验证和数据包解密操作。这是为了确保安全性。然后，通过 HTTP 协议将请求转发到后端服务器进行处理。

出网流量的路径取决于数据请求进入网络的方式。对于通过负载均衡器进入的访问流量，相应的响应流量也会通过负载均衡器返回。负载均衡器通过绑定的弹性公网 IP 接收来自公网的流量，并在 EIP 上进行计费。从负载均衡器到后端云主机之间的通信通过 VPC 内网进行，不会产生额外费用。

如何跨 VPC 访问弹性负载均衡？

当需要访问服务的客户端和提供服务的弹性负载均衡在两个同地域的不同 VPC 时，由于 VPC 的网络隔离特性，客户端不能直接访问弹性负载均衡的内网 IP。可以通过创建对等连接并配置相应路由的方式，将两个 VPC 私网打通，实现客户端跨 VPC 访问弹性负载均衡。

经典型弹性负载均衡有实例规格吗？

没有。仅性能保障型负载均衡区分实例规格。

分配有 IPv4 和 IPv6 地址弹性负载均衡实例可以调整为仅有 IPv4 地址的情况吗？

不支持。创建负载均衡器时，如果选择已开启 IPv6 的 VPC 和子网，可以为选择负载均衡器分配 IPv6 地址，创建后不支持取消负载均衡器的 IPv6 地址分配。

弹性负载均衡对上传文件的速度和大小是否有限制？

没有限制。请关注服务链路上其他节点（如弹性 IP、后端主机）的限制。

为什么会有 100 开头的 IP 在频繁访问后端主机？

弹性负载均衡服务将流量转发至后端主机时的源 IP 以及健康检查请求的源 IP 均为

100.89.0.0/16 网段的地址，如果您遇到的 100 开头的 IP 为此段地址，应为正常的业务流量转发或健康检查请求。后端主机的安全组、网络 ACL 或其他访问控制规则应配置为允许 100.89.0.0/16 网段的流量通过。

包年包月的弹性负载均衡实例超期后，哪些功能会受影响？

包年包月的弹性负载均衡实例超期后，可以进行续订，不再进行流量转发，也不能对超期实例进行配置。

5.2 监听器

监听器中分配算法和会话保持算法是什么关系？

分配算法用于决定负载均衡器如何将请求分配给后端实例。它是负载均衡器的核心算法，其目标是平衡负载并确保请求能够有效地分发到可用的后端实例。常见的分配算法包括轮询算法、最小连接算法、源 IP 算法等。

会话保持算法是一种特殊的分配算法。它的目标是确保来自同一客户端的请求始终被分发到同一个后端实例，以维持会话的连续性。会话保持算法基于客户端的某些标识符来决定请求的目标后端实例。这样，即使客户端发出多个请求，它们也会被分发到相同的后端实例，以保持会话状态。天翼云弹性负载均衡支持的分配算法和会话保持算法如下：

分配算法	会话保持类型	TCP/UDP	HTTP/HTTPS	
轮询	SOURCE_IP	支持	不支持	区域资源池为集群模式资源池 ,主备、集群模式资源池列表 见 产 品 简介>产品类型和规格>按资源池区分，实际情况以控制台展现为准。
	植入 cookie	不支持	支持	
	重写 cookie	不支持	支持	
最小连接算法	SOURCE_IP	支持	不支持	
	植入 cookie	不支持	不支持	
	重写 cookie	不支持	不支持	
源 IP 算法	SOURCE_IP	不支持	不支持	
	植入 cookie	不支持	不支持	
	重写 cookie	不支持	不支持	

分配算法	会话保持类型	TCP/UDP	HTTP/HTTPS	
轮询	SOURCE_IP	支持	支持	区域资源池为主备模式资源池，主备、集群模式资源池列表见产品简介>产品类型和规格>按资源池区分，实际情况以控制台展现为准。
	HTTP_COOKIE	不支持	支持	
	APP_COOKIE	不支持	支持	

负载均衡器监听的端口和后端主机的端口关系是什么？是否可以不一致？

负载均衡器监听的端口是客户端到负载均衡器之间的请求的目标端口号，是服务对外暴露的端口号。而后端主机的端口号是实际业务的端口号，可以和 ELB 监听的前端端口号不一样。

弹性负载均衡正在运行中，此时增加监听器，添加新的负载方式是否会导致业务中断？

增加监听器，添加新的负载方式不影响已经创建的现有连接，不会引发业务中断。

监听器是否支持创建转发策略？

TCP、UDP 协议的监听器不支持。HTTP/HTTPS 协议的监听器支持配置基于域名和路径的转发策略。但重定向的监听器不可创建转发策略，到此监听器的访问都将被重定向至已配置的 HTTPS 监听器。

监听器的转发策略的状态显示为“异常”的原因是什么？

监听器的转发策略状态显示为“异常”可能有以下几个原因：

1. 如果监听器的转发策略配置的后端主机出现异常或者不可用，负载均衡器无法将请求转发给后端主机，导致转发策略状态显示为“异常”。
2. 负载均衡器会定期进行健康检查来判断后端主机的可用性。如果健康检查失败次数超过了设定的阈值，负载均衡器会将转发策略状态标记为“异常”。
3. 如果监听器的转发策略配置存在错误，比如创建了相同的转发策略（出现转发策略冲突），则会出现转发策略异常，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异常。
4. 如果后端安装了一些主机安全工具，比如 windows 的 edr，linux 的翼盾，或者是添加云墙，也可能会导致显示异常。

监听器删除之后，弹性负载均衡是否会立即停止转发业务流量？

四层监听器仅负责基于传输层协议（如 TCP）的负载均衡，如果删除了监听器，则弹性负载均衡会关闭与客户端的连接，停止转发流量。七层监听器略有不同，如果客户端和 ELB 之间建立的连接是长连接，在删除七层监听器后，一部分已建立的 TCP 长连接仍然存在，不受监听器删除的影响。

弹性负载均衡 HTTPS 监听器是否支持开启 HTTP2.0 功能？

HTTP2.0 功能目前仅在集群模式资源池上线，主备、集群模式资源池列表见产品简介>产品类型和规格>按资源池区分，实际情况以控制台展现为准。

5.3 后端主机

是否支持修改后端主机端口和权重？

天翼云弹性负载均衡后端主机组支持对后端主机的端口和权重进行修改，修改后端主机端口和权重功能目前仅在集群资源池上线，主备、集群模式资源池列表见产品简介>产品类型和规格>按资源池区分，实际情况以控制台展现为准。

修改后端主机权重后多久生效？

修改后端主机权重后，会立即生效。新的流量将会根据修改后的权重转发，已经建立的连接不受影响。

负载均衡器运行时，是否支持增加或减少后端主机？

支持。负载均衡器运行时增加或减少负载均衡器的后端主机的数量，且可以支持不同的后端主机切换操作。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 台正常运行的云主机。

能否支持客户端到负载均衡是 HTTPS 协议 ,负载均衡到后端主机也是 HTTPS 协议么？

客户端到负载均衡 HTTPS 协议支持，而负载均衡到后转主机 HTTPS 不支持，负载均衡到后端主机会转换为 HTTP 协议。

是否支持多个负载均衡器转发流量到相同的后端主机？

支持。

是否支持添加端口号不一致的后端主机？

支持。在将后端云主机添加到弹性负载均衡器时，您可以为每个后端云主机指定不同的端口号。

弹性负载均衡是否支持添加不同操作系统的云主机？

支持，弹性负载均衡本身不会限制后端云主机的操作系统，只需确保两台云主机上的应用服务部署相同且数据一致即可。然而，我们建议您选择两台操作系统相同的云主机进行配置，以方便以后的管理和维护。

弹性负载均衡是否支持跨 AZ 的后端云主机？

支持。

弹性负载均衡可以只绑定一台云主机上使用吗？

可以，但是仅一台云主机无法做到负载均衡，建议使用两台以上云主机。

使用弹性负载均衡服务后，后端主机能否访问公网？

如果后端主机没有绑定弹性 IP 或使用 NAT 网关，那么后端主机并不能通过弹性负载均衡来主动访问公网。如果想实现后端主机能主动访问公网的需求，需要给后端主机绑定弹性 IP 或使用 NAT 网关。

配置转发策略时， 能否选择已有的后端主机组？

不能，每个转发策略都要新建自己的后端主机组，不能共享后端主机组。

弹性负载均衡的后端主机可以访问弹性负载均衡监听的端口吗？

可以访问。

外网负载均衡的后端主机要不要绑定 EIP？

弹性负载均衡与后端主机之间的流量是通过内网转发的，不需要因为使用负载均衡为后端主绑定 EIP。

如何检查后端主机网络配置？

1. 确认安全组配置是否放通 100.89.0.0/16 地址。在弹性云主机详情页，查看安全组规则，检查是允许 100.89.0.0/16 地址段的流量。如果没有，则需要根据具体情况添加或调整安全组规则，对 100.89.0.0/16 地址段的流量放行。
2. 确认网络 ACL 是否放通 100.89.0.0/16 地址。在弹性云主机所在子网的详情页，查看 ACL 规则，检查是允许 100.89.0.0/16 地址段的流量。如果没有，则需要根据具体情况添加或调整 ACL 规则，对 100.89.0.0/16 地址段的流量放行。

如何检查通过 EIP 访问后端主机？

1. 首先搭建后端主机上的服务，完成弹性负载均衡和后端主机配置。
2. 如果是内网负载均衡，需要先未弹性负载均衡绑定 EIP。
3. 通过访问 EIP 的 IP 地址检查服务是否正常。Linux 系统下可通过 curl 命令进行测试，Windows 系统下可用浏览器访问进行测试。

5.4 会话保持

长连接和会话保持区别是什么？

长连接和会话保持没有必然联系，它们是两个不同的概念。

长连接是指在一个连接上可以连续发送多个数据包，而不是每次请求都建立新的连接，确保客户端和后端主机之间的连接在一段时间内保持打开状态，以便可以在连接保持期间发送多个请求和响应。

会话保持确保同一个客户端的多次请求被发送到同一个后端主机，保持会话状态的一致性。

弹性负载均衡支持何种会话保持方式？

TCP/UDP 协议的会话保持方式为 SOURCE_IP 方式。集群模式资源池 HTTP/HTTPS 协议的会话保持支持重写 cookie 和植入 cookie 方式，主备、集群模式资源池列表见产品简介>产品类型和规格>按资源池区分，实际情况以控制台展现为准。

如何检查弹性负载均衡会话保持不生效问题？

可以按照以下步骤进行排查：

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. 选择源 IP 算法时，需要留意在请求到达弹性负载均衡之前是否会有 IP 变化。
4. 对于 HTTP 或 HTTPS 监听器并启用了会话保持功能，需要关注请求是否携带了 cookie。如果请求中带有 cookie，需要观察该 cookie 值是否有变化（因为基于 7 层的会话保持依赖于 cookie），以确保会话保持的有效性。

会话保持与不保持的区别？

会话保持和不保持是用于描述负载均衡器在请求分发时处理连接的两种不同方式。

- 会话保持：当负载均衡器配置为会话保持时，它将尝试将特定客户端的所有请求都发送到同一台后端主机。当客户端与后端主机建立连接后，负载均衡器将会话信息保存，并在后续的请求中使用该信息来识别并将请求发送到正确的后端云主机。这样可以确保在整个会话期间，由同一客户端发起的请求都被发送到相同的主机，从而保持会话状态的连续性。
- 不保持：当负载均衡器配置为不保持时，它会将每个请求独立地分发到后端主机，而不考虑之前的会话状态。负载均衡器每次都会根据负载均衡算法选择一台合适的后端主机来处理请求。这种方式适用于无状态应用，其中每个请求都是独立的，主机可以根据每个请求的内容来响应，而不依赖于之前的会话信息。

会话保持时间（分钟）默认时间是多少？能改大吗？

会话保持的时间，取值范围为 1- 86400，默认 1000 秒，并且可以修改。

如何使用 Linux curl 测试弹性负载均衡会话保持？

在使用 Linux curl 测试弹性负载均衡（ELB）会话保持时，你可以按照以下步骤进行操作：

1. 安装 curl：如果你的 Linux 系统上没有安装 curl，可以使用适合你的包管理器进行安装。例如，在 Ubuntu 上可以使用以下命令安装 curl：

```
sudo apt update
sudo apt install curl
```

2. 准备测试网址：获取弹性负载均衡器（ELB）的 URL 或域名，确保 ELB 后面有多个可用的后端实例，确保 ELB 开启“会话保持”功能。
3. 使用 curl 发送请求：使用 curl 命令发送多个请求，并观察结果。你可以使用以下命令进行测试：

```
curl -c cookies.txt [弹性负载均衡器的 URL]
```

4. 其中，-c cookies.txt 参数用于保存从主机接收到的 cookie 信息到 cookies.txt 文件中。
5. 多次运行 curl 命令：多次运行上述 curl 命令，以便发送多个请求。你可以使用循环来简化测试过程。以下是一个示例：

```
for i in {1..5}; do curl -b cookies.txt -c cookies.txt [弹性负载均衡器的 URL]; done
```

6. 在上述示例中，-b cookies.txt 参数用于在每次请求中携带之前收到的 cookie 信息来维持会话。
7. 检查请求的响应：检查每个请求的响应，并观察结果。如果会话保持正常，所有的请求应该被发送到相同的后端实例，从而保持会话状态的连续性。

5.5 健康检查

健康检查支持哪些协议？

健康检查支持 TCP、UDP、HTTP 协议。TCP 协议监听器只可选 TCP，UDP 协议监听器只可选 UDP。 HTTP 协议/HTTPS 协议监听器可选 HTTP 或 TCP。

后端主机什么时候被认为是健康的？

只要首次添加的主机经过一次成功的健康检查，就会变为健康状态。之后，根据配置的健康检查“间隔时间”和“最大重试次数”进行周期性健康检查探测，如果健康检查探测失败次数超过“最大重试次数”，将会变为不健康状态。

健康检查为什么会导致 ELB 频繁向后端云主机发送探测请求？

弹性负载均衡采用高可用集群模式部署，集群内的所有转发节点都会独立向后端云主机发送探测请求，检查周期由用户可配置。健康检查会持续进行，根据配置的检查周

期间隔定期进行探测。因此，每隔几秒就会有一次访问请求发送到后端云主机。您可以通过调整健康检查的周期来控制访问后端云主机的频率。

健康检查什么时候启动？

健康检查在后端主机加入负载均衡器后会启动。在第一个周期内，会随机选择一个时间点开始进行健康检测。随后，根据配置的检查间隔，健康检查会按照设定的时间间隔启动。这样可以确保后端主机在加入负载均衡器后的一段时间内有足够的准备时间，避免同时进行健康检查对主机造成过大的负载压力。通过随机启动和设定的检查间隔，可以实现分散负载和平滑过渡，保证后端主机的稳定性和可用性。

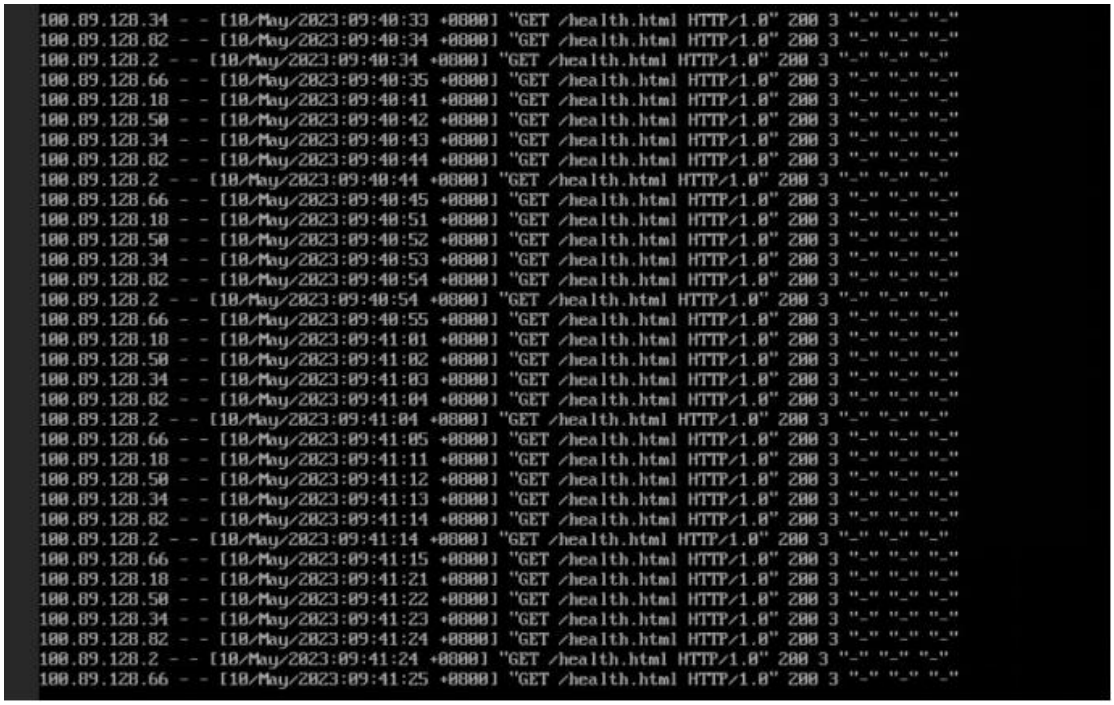
健康检查异常如何排查？

当健康检查探测到您的后端主机异常时，弹性负载均衡将不再向异常的后端主机转发流量。直到健康检查检测到后端主机恢复正常时，弹性负载均衡才会向此主机继续转发流量。那么当您遇到健康检测异常该如何排查呢，排查思路如下：

- 检查后端主机组是否关联监听器
- 检查健康检查配置：检查健康检查配置参数信息，例如域名、协议是否正确，检查您配置的健康检查端口和监听的端口是否一致，检查路径是否正确等。
- 检查主机所在安全组、网络 ACL 是否放行 ELB 健康检查源地址网段 100.89.0.0/16。
- 检查后端主机是否正常：后端主机当前宕机或不可访问，会导致检查异常。
- 检查主机防火墙、路由。

弹性负载均衡对后端主机的健康检测时间间隔需要注意什么？

例如客户的健康检查间隔时间设置的 10s，客户在其后端主机组发现探测时间如下图所示，看起来不是 10s 一个健康检查报文。集群模式资源池弹性负载均衡是跨 AZ 的集群部署方式，所以一个集群里有多个 LB 的成员共同提供 LB 的服务，所有这些成员都会去探测后端主机的健康状态，例如客户的环境里有六个 LB 的成员，.66,.18, .50, .34, .82 和.2,观察下每一个成员就会看到探测间隔是 10s。



健康检查失败状态是什么？

健康检查失败达到最大重试次数后，后端主机进入健康检查失败状态。

负载均衡器中配置了健康检查的最大重试次数，当后端主机连续失败的健康检查次数达到该阈值时，负载均衡器会认定该后端主机不可用，并将其标记为健康检查失败状态。此时，负载均衡器将不再将请求转发给该主机，并将流量转发到其他健康的后端主机上，以确保服务的可用性和稳定性。一旦后端主机恢复正常，经过一定时间的正常健康检查后，负载均衡器会将其重新标记为可用状态。

健康检查正常默认返回的状态码有哪些？

健康检查默认反馈状态码有：

HTTP 状态码	说明
HTTP 状态码 200	表示正常响应。当健康检查请求成功被云主机处理并返回有效的响应时，通常会返回 200 状态码。
HTTP 状态码 3xx	重定向。在健康检查中，重定向状态码可能会出现在特定情况下。
HTTP 状态码 4xx	客户端错误。这些状态码表示请求存在问题，可能是由于无效的 URL、参数错误等。健康检查中，如果主机返回了 4xx 状态码，通常表示主机无法正常处理该请求。
HTTP 状态码 5xx	主机错误。这些状态码表示主机在处理请求时遇到了错误。在天翼云健康检查中，如果主机返回了 5xx 状态码，通常表示主机出现了故障或内部错误。

5.6 证书管理

如何生成服务器证书和 CA 证书？

弹性负载均衡支持服务器证书和 CA 证书创建，具体可参考用户指南证书管理。

控制台证书管理侧，可以创建几个证书？

每个客户可以创建 10 个服务器证书。

弹性负载均衡 HTTPS 监听器是否支持多证书？

集群资源池弹性负载均衡的 HTTPS 监听器支持多个 SSL 证书，主备、集群模式资源池列表见产品简介>产品类型和规格>按资源池区分，实际情况以控制台展现为准。这意味着您可以在同一个负载均衡器上配置多个 SSL 证书来支持不同的域名或子域名的加密连接。通过使用 HTTPS 监听器，您可以将加密的 HTTPS 流量有效地分发到后端实例，这对于在同一个负载均衡器上托管多个网站或应用程序非常实用。使用不同的 SSL 证书可以确保每个网站或应用程序都有其独立的安全性保证。

为什么配置了证书，却访问异常？

如果负载均衡配置了证书，但访问异常，可能有以下几个原因：

1. 证书配置错误 :请确保证书的配置正确无误。检查证书是否正确上传到负载均衡器，并且与域名或主机名匹配。
2. 证书过期或无效：如果证书已过期或者无效，浏览器会拒绝连接或显示安全警告。请确保证书有效期内，并且由受信任的证书颁发机构签发。
3. 安全组或防火墙限制：检查负载均衡器、后端主机以及相关网络设备的安全组或防火墙规则，确保允许来自负载均衡器的 HTTPS 流量通过。
4. 其他网络问题：检查网络连接是否正常，确保网络链路畅通，防止网络延迟、丢包等问题影响访问。

更换证书会导致网络或者弹性负载均衡连接中断吗？

不会。在更换证书时，已经建立的连接将继续使用旧证书，而新建立的连接将使用新证书。

弹性负载均衡是否支持泛域名证书？

支持，用户可以在创建证书时使用泛域名证书。

5.7 操作管理

经典型和性能保障型负载均衡有什么区别？

经典型负载均衡适用于访问量较小，应用模型简单的 web 业务，可满足大部分应用程序的负载均衡需求，具备基本的流量分发和健康检查功能。经典型负载均衡同 VPC 内多实例性能共享。

性能保障型负载均衡适用于对性能有较高要求的应用场景，能够提供更强大的性能和扩展能力。性能保障型负载均衡为收费产品，为集群模式部署，支持经典型升级为性能保障型，支持规格升级、降级。

经典型负载均衡是否支持升级为性能保障型？

支持。你可以登录天翼云控制中心参考经典型升级性能保障型指南进行相关操作。

弹性负载均衡器是否可以单独使用？

不支持。没有后端主机，弹性负载均衡器无法实现流量分配和负载均衡的功能。

一个负载均衡器是否支持绑定多个弹性 IP？

不支持。一个负载均衡实例仅支持绑定一个 EIP，接受来自公网的请求。

一个账号在单地域可创建的负载均衡数量是多少？

一个账号在单地域可创建的免费经典型负载均衡数量是 1 个；一个账号在单地域可创建性能保障型负载均衡数量 20 个。一个负载均衡实例可添加的监听器数量是 3 个。一个负载均衡实例的监听器可绑定的主机数量是 100 个。如有需要，您可通过提工单提升配额。

是否支持绑定其他云平台的 EIP 使用？

不支持。

弹性负载均衡后端主机是否只能选择本天翼云的虚拟主机吗？是否支持其他厂家的主机？

不支持其他厂商主机。

是否支持添加跨租户、跨 VPC 后端主机？有什么限制？

不支持跨租户添加后端云主机。添加跨 VPC 后端主机功能目前仅在集群模式资源池上线，主备、集群模式资源池列表见产品简介>产品类型和规格>按资源池区分，实际情况以控制台展现为准。当前仅支持添加其它 VPC 的后端主机，暂不支持添加通过专线打通的线下 IDC 的主机。 跨 VPC 后端 IP 添加仅支持对等连接的对端 VPC 后端主机以 IP 形式添加。您最多可添加 200 个跨 VPC 后端 IP，如需要申请更多，则需申请增加配额。

5.8 异常排查

为什么通过负载均衡无法访问后端业务？

造成负载均衡无法访问后端业务的原因有很多，遇到这种问题的时候，我们要学会如何去排查。

- 排查是否可直接访问后端主机：负载均衡器无法将请求发送到后端主机，可能是因为后端主机当前宕机或不可访问。可以直接访问后端主机的 IP 地址来进行排查，确保后端主机正常运行。
- 排查健康检查是否正常：如果后端主机未通过健康检查，则负载均衡器将不会将请求发送到该主机。请确保后端主机在健康检查中通过，并检查健康检查的设置是否正确。
- 排查后端主机配置是否正确：在“后端云主机组”页面查看已添加的后端主机的参数，云主机权重如果设置为 0，则不会向这个主机转发流量；业务的端口需要与实际的业务端口相同。
- 检查访问控制配置是否正确：在监听器基本信息页面，查看访问控制配置是否正确，是否已经放通了客户端的 IP 地址。
- 网络配置问题：可能存在网络配置问题，导致负载均衡器无法与后端主机建立连接。确保网络配置正确，并检查网络访问权限、路由表、子网等设置。
- 会话保持配置错误：如果应用程序需要会话保持，但会话保持配置有误，负载均衡器可能会将请求发送到不同的后端主机，导致会话状态丢失。确保会话保持配置正确，并检查会话保持策略和负载均衡器的支持。

如何检查请求的不均衡？

可以通过以下方式检查请求的均衡：

1. 基于轮询算法：如果某个主机处理的请求数量明显少于其他云主机，那么可以认为

存在请求不均衡的情况。

2. 基于权重算法：如果某个主机的权重值过高或过低，可能会导致请求不均衡。
3. 基于源 IP 算法：同一个 IP 发出的请求都会分发到同一个后端，导致流量不均衡。
4. 基于响应时间：如果某个后端的响应时间较长，可能意味着该主机的负载较高或存在性能问题，需要进行调整。
5. 基于健康检查：负载均衡器定期对后端主机进行健康检查，如果某个主机无法正常响应或处于宕机状态，负载均衡器将不再将请求分发给该主机，从而避免请求不均衡。
6. 基于会话保持：如果开启会话保持，负载均衡器会将同一个客户端的请求始终分发到同一个后端主机上，以确保会话的连续性。如果客户端的数量相对较少，并且会话保持的配置不合理，可能会导致请求不均衡的问题。

如何检查弹性负载均衡服务不通或异常中断？

要检查弹性负载均衡（ELB）服务是否不通或异常中断，可以采取以下步骤：

1. 检查负载均衡器的状态：登录到管理控制台，检查负载均衡器的状态。确保负载均衡器处于运行状态，没有错误或警告信息。
2. 检查负载均衡器的健康检查状态：负载均衡器通常会执行健康检查来确定后端服务的可用性。检查负载均衡器的健康检查状态，确保后端实例通过了健康检查，没有标记为不可用或异常。
3. 检查安全组规则和网络访问控制列表（ACL）：确保负载均衡器的安全组规则和网络 ACL 允许来自客户端和后端实例的流量通过。如果有必要，可以针对特定的端口和协议进行更详细的配置。

4. 检查后端实例的状态：确保后端实例正在运行，并且没有故障或异常。检查后端实例的状态和日志，确保应用程序或服务正常工作。
5. 检查 DNS 解析：负载均衡器通常使用域名解析将来自客户端的流量转发到后端实例。检查域名解析是否正确配置，并确保有向负载均衡器发出的请求能够正常解析到正确的 IP 地址。
6. 监控分析：使用云监控服务来监视负载均衡器的性能和资源使用情况。

如何排查 ELB 的异常返回码？

常见异常返回码有 400、401、403、500 等，这里可以参考下表进行排查处理。

状态码	状态码含义	可能原因
400	错误请求	客户端发送的请求格式不符合 HTTP 规范。 请求的语法可能存在错误。 无效的参数或参数不完整
401	未授权	HTTP40 错误代表用户没有访问权限,需要进行身份认证。
403	禁止访问	一般是后端主机返回，后端主机拦截了该请求。
404	资源未找到	后端主机返回错误码，需排查后端主机业务。 ELB 转发策略配置不正确，未指定到正确的后端主机。
408	请求超时	当客户端向主机发送请求后，主机在规定的时间内没有响应
413	请求实体过大	当因请求的实体过大,超出主机的处理能力,导致主机无法处理请求时就会返回此错误代码。
414	URI 太长	客户端发送的请求 URL 或查询字符串参数过大。
499	客户端主动断开连接	ELB 还未将响应信息返回给客户端，客户端主动断开连接。此错误码仅记录在访问日志中。
500	主机内部错误	后端主机返回，为主机内部错误。

501	未实现	ELB 服务无法识别此请求。
502	错误的网关	ELB 未正确配置后端主机的监听通信端口。 ELB 在尝试建立连接或向后端服务发送数据时从后端主机收到了 TCP RST。 后端主机响应格式错误，或者包含无效的 HTTP 响应头。Ÿ 未正确配置后端主机，例如未正确配置路由、网络 ACL 等。
503	服务不可用	一般是后端主机返回，表示后端服务不可用。
504	网关超时	负载均衡设备或代理服务器无法在设定的超时时间内将请求转发到可用的上游服务器而引起的。

负载均衡请求不均衡，怎样排查？

- 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。
- 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。
- 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。

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。

为什么云监控 EIP 带宽使用统计与弹性负载均衡监控的网络流出速率数据不一致？

以下一些因素可能导致云监控 EIP 带宽使用统计与 ELB 监控的网络流出速率数据不一致：

1. 内网外网访问：云监控 EIP 带宽使用统计通常只包括外网访问的数据，而弹性负载均衡监控可能同时包括外网和内网访问的数据。这意味着，如果有内网访问，弹性负载均衡监控的网络流出速率数据会比云监控 EIP 带宽使用统计更高。
2. 限流情况：当流量超过 EIP 的带宽限制时，EIP 会被限流，而弹性负载均衡内部的访问不会受到限制。这可能导致弹性负载均衡监控的网络流出速率数据在超过 EIP 带宽时仍然较高，而云监控 EIP 带宽使用统计可能受到限流影响而较低。

压测性能上不去，如何检测？

- 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。
- 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。
- 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。可通过增加客户端 IP 来解决。
- 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。

如何检查弹性负载均衡业务访问延时大？

通过弹性 IP 直接访问云主机，绕过弹性负载均衡进行访问，以确定访问延时大的问题是由弹性负载均衡引起的，还是前端网络问题或后端云主机问题。

检查后端主机的性能和健康状态。如果后端主机存在性能问题或负载过高，可能会导致访问延迟增加。

检查网络的带宽、延迟和丢包率等指标，确保网络状况良好。网络问题可能会导致业务的访问延迟增加。

如果以上步骤无法解决问题，您可以联系客服寻求技术支持解决。

负载方式选择了“源 IP 算法”，但是同一个 IP 地址同时出现在了两台后端主机上是什么原因？

如果后端主机下线后重新上线，弹性负载均衡会重新进行一致性 Hash 运算并对后端主机进行编号。这可能导致之前分配给某个主机的 IP 地址被分配给另一台云主机，从而出现同一个 IP 地址同时出现在了两台后端主机上的情况。

为什么配置了白名单后还能访问后端主机？

白名单允许特定 IP 访问负载均衡。如果需要对后端主机进行访问控制，可以通过配置网络 ACL 或者安全组规则实现。