弹性负载均衡

用户指南

文档版本 01

发布日期 2024-07-15

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目 录

1 独享型用户指南

1.1 权限管理

1.1.1 创建用户并授权使用 ELB

如果您需要对您所拥有的ELB进行精细的权限管理，您可以使用**统一身份认证服务**（Identity and Access Management，简称IAM），通过IAM，您可以：

- 根据企业的业务组织，在您的华为云账号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用ELB资源。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将ELB资源委托给更专业、高效的其他华为云账号或者云服务，这些账号或者云服务可以根据权限进行代运维。

如果华为云账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用ELB服务的其它功能。

本章节为您介绍对用户授权的方法，操作流程如**图1-1**所示。

前提条件

给用户组授权之前，请您了解用户组可以添加的ELB权限，并结合实际需求进行选择。ELB支持的系统权限，请参见：**ELB系统权限**。若您需要对除ELB之外的其它服务授权，IAM支持服务的所有权限请参见**系统权限**。

示例流程

图 1-1 给用户授权 ELB 权限流程

1. **创建用户组并授权**

   在IAM控制台创建用户组，并授予弹性负载均衡服务只读权限“ELB ReadOnlyAccess”。
2. **创建用户并加入用户组**

   在IAM控制台创建用户，并将其加入**1.创建用户组并授权**中创建的用户组。
3. **用户登录**并验证权限

   新创建的用户登录控制台，切换至授权区域，验证权限：
   - 在“服务列表”中选择弹性负载均衡，进入ELB主界面，单击右上角“购买弹性负载均衡”，尝试购买弹性负载均衡器，如果无法购买弹性负载均衡器（假设当前权限仅包含ELB ReadOnlyAccess），表示“ELB ReadOnlyAccess”已生效。
   - 在“服务列表”中选择除弹性负载均衡器外（假设当前策略仅包含ELB ReadOnlyAccess）的任一服务，若提示权限不足，表示“ELB ReadOnlyAccess”已生效。

1.1.2 ELB 自定义策略

如果系统预置的ELB权限，不满足您的授权要求，可以创建自定义策略。自定义策略中可以添加的授权项（Action）请参考**《弹性负载均衡接口参考》**中“ 策略及授权项说明”章节。

目前华为云支持以下两种方式创建自定义策略：

- 可视化视图创建自定义策略：无需了解策略语法，按可视化视图导航栏选择云服务、操作、资源、条件等策略内容，可自动生成策略。
- JSON视图创建自定义策略：可以在选择策略模板后，根据具体需求编辑策略内容；也可以直接在编辑框内编写JSON格式的策略内容。

具体创建步骤请参见：**创建自定义策略**。本章为您介绍常用的ELB自定义策略样例。

ELB 自定义策略样例

- 示例1：授权用户更新负载均衡器

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "elb:loadbalancers:put"
            ]
        }
    ]
}
```

- 示例2：拒绝用户删除负载均衡器

  拒绝策略需要同时配合其他策略使用，否则没有实际作用。用户被授予的策略中，一个授权项的作用如果同时存在Allow和Deny，则遵循Deny优先。

  如果您给用户授予ELB FullAccess的系统策略，但不希望用户拥有ELB FullAccess中定义的删除负载均衡器权限，您可以创建一条拒绝删除负载均衡器的自定义策略，然后同时将ELB FullAccess和拒绝策略授予用户，根据Deny优先原则，则用户可以对ELB执行除了删除负载均衡器外的所有操作。拒绝策略示例如下：

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "elb:loadbalancers:delete"
            ]
        }
    ]
}
```

- 示例3：多个授权项策略

  一个自定义策略中可以包含多个授权项，且除了可以包含本服务的授权项外，还可以包含其他服务的授权项，可以包含的其他服务必须跟本服务同属性，即都是项目级服务或都是全局级服务。多个授权语句策略描述如下：

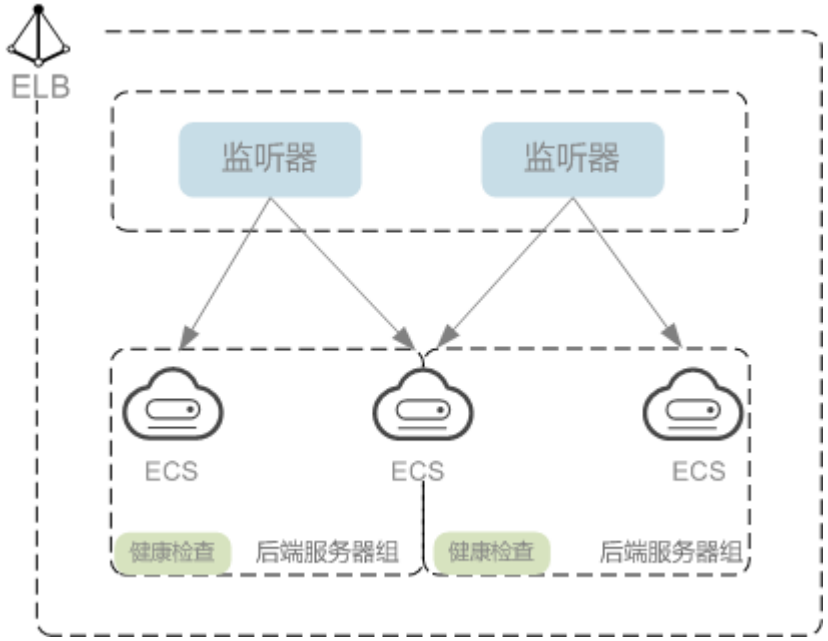
```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "elb:loadbalancers:get",
                "elb:loadbalancers:list",
                "elb:loadbalancers:delete",
                "ecs:cloudServers:delete"
            ]
        }
    ]
}
```

1.2 负载均衡器

1.2.1 独享型负载均衡器概述

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

图 1-2 负载均衡器结构图



实例区域

- 建议选择距离业务目标客户距离最近的区域，可以减少网络时延以及提高下载速度。
- 支持通过跨VPC后端功能实现跨VPC添加后端服务器，详见**IP类型后端（跨VPC后端）**。
- 支持通过云连接服务实现跨区域间通信，详见**《云连接用户指南》**。

实例可用区

独享型负载均衡支持多可用区，选择的每个可用区都会创建相应的负载均衡实例。

弹性负载均衡可将客户端请求跨可用区分发，选择与后端服务器相同的可用区，可以减少网络时延以及提高访问速度。

不同可用区的负载均衡实例间采用双活或者多活模式，客户端访问的请求就近分配到同可用区的实例。

表 1-1 弹性负载均衡可用区容灾规划场景说明

可用区容灾方案	推荐业务场景	场景优势
单实例多可用区	对于业务量没有超过独享型负载均衡最大规格限制的，建议创建一个负载均衡实例，并选择多个可用区。	单个可用区的负载均衡实例故障不会影响所有业务，多个可用区之间可以实现业务容灾。
多实例多可用区	对于超高业务量，超过独享型负载均衡最大规格限制的，建议创建多个负载均衡实例，并且每个负载均衡实例选择多个可用区。	单个负载均衡实例故障不会影响所有业务，多个负载均衡实例和多个可用区之间均可以实现业务容灾。

表 1-2 流量的可用区分配说明

流量来源	可用区分配说明
公网访问	根据源IP的不同将流量分配到创建的多个AZ中的ELB上，多个AZ的ELB性能加倍。
私网访问	• 当从创建ELB的AZ发起访问时，流量将被分配到本AZ中的ELB上，当本AZ的ELB不可用时，容灾到创建的其他AZ的ELB上。如果本AZ的ELB正常，但是本AZ的流量超过规格，业务也会受影响，私网场景要考虑客户端访问的均衡性。 私网流量使用率建议通过AZ粒度监控观察是否超限。 • 当从未创建ELB的AZ访问时，根据源IP的不同将流量分配到创建的多个AZ中的ELB上。
云专线访问	流量优先分配到云专线对接的AZ下部署的ELB，否则分配到其他AZ下的ELB。
客户端跨VPC访问	流量优先分配至客户端源VPC子网所在AZ部署的ELB，否则分配到其他AZ下的ELB。

实例规格

独享型负载均衡可以独享已购买创建的实例资源。

网络型规格的实例只支持四层协议TCP/UDP的转发能力，应用型规格的实例支持七层协议HTTP/HTTPS的转发能力。

具体的规格需要评估实际的业务量，根据业务实际需要购买相应规格的实例。规格详情请参见**负载均衡实例的规格**。

在使用过程中可以结合负载均衡实例的监控指标，查看实际业务量的峰值、趋势和规律，对实例规格进行更精确的选择。

建议参考**表1-3**并结合负载均衡实例的监控指标评估业务量的峰值、趋势和规律，对实例规格进行更精确的选择。

表 1-3 实例规格选择说明

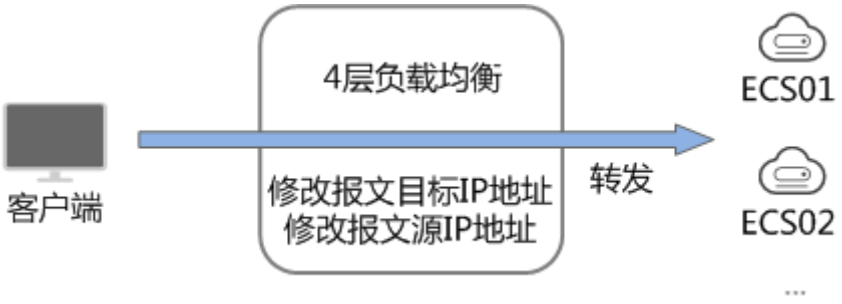
实例规格	规格选择说明
网络型规格	建议重点关注长连接的最大并发连接数，实例规格的“最大并发连接数”应作为关键参考指标。需要根据实际的业务场景，预估一个负载均衡实例需要承载的最大连接数，并选择相应的规格。
应用型规格	实例规格的“每秒查询速率 (QPS)”应作为关键参考指标，该指标决定了一个七层应用系统的业务吞吐量。需要根据实际的业务场景，预估一个负载均衡实例需要承载的QPS，并选择相应的规格。

实例协议类型

弹性负载均衡提供基于四层协议的网络型实例和基于七层协议的应用型实例，在负载均衡器中通过添加监听器选择相应的协议。

- 网络型：适用于四层大流量高并发业务，如文件传输、即时通信、在线视频等业务。

  图 1-3 网络型负载均衡器

- 应用型：聚焦HTTP和HTTPS应用层协议，提供强大的应用层业务处理能力和基于请求内容的高级转发策略。

  图 1-4 应用型负载均衡器

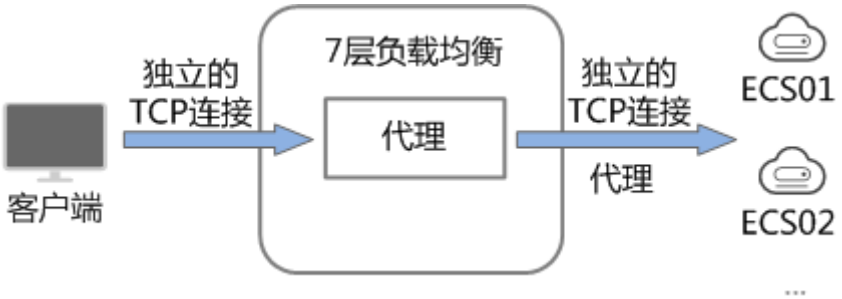
  

表 1-4 实例规格协议类型说明

协议类型	协议类型说明
网络型	监听器收到访问请求后，将请求直接转发给后端服务器。转发过程仅修改报文中目标IP地址和源IP地址，将目标地址改为后端云服务器的IP地址，源地址改为负载均衡器的IP地址。四层协议连接的建立，即三次握手是客户端和后端服务器直接建立的，负载均衡只是进行了数据的转发。
应用型	监听器收到访问请求后，需要识别并通过HTTP/HTTPS协议报文头中的相关字段，进行数据的转发。监听器收到访问请求后，先代理后端服务器和客户端建立连接（三次握手），接收客户端发送的包含应用层内容的报文，然后根据报文中的特定字段和流量分配策略判断需要转发的后端服务器。此场景中，负载均衡类似一个代理服务器，分别和客户端以及后端服务器建立连接。

说明

客户端到ELB之间支持TCP长连接，客户端和ELB之间建立TCP连接之后，可以持续发送业务请求（HTTP/HTTPS请求），提高TCP连接复用率可以降低TCP频繁建连的开销。

实例网络类型

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

表 1-5 弹性负载均衡网络类型说明

负载均衡器网络类型	使用说明	使用场景
公网负载均衡器	创建公网负载均衡器时，需要为负载均衡器创建EIP或者绑定已有的EIP 。 公网负载均衡器接收公网的访问请求，然后向绑定了监听器的后端服务器分发这些请求。	• 需要通过服务器集群对公网提供服务，且需要统一的入口，并将公网用户请求合理地分配到服务器集群时。 • 需要对服务器集群做故障容错和故障恢复时。
私网负载均衡器	私网负载均衡器由于没有公网域名和EIP，所以只能在VPC内部被访问，不能被Internet的公网用户访问。 私网负载均衡通过使用私有IP将来自同一个VPC内的访问请求分发到后端服务器上，通常用于内部服务集群。	• 当内部服务器端有多台，需要将客户端请求合理地分发到各台服务器时。 • 当需要对内部服务器集群做故障容错和故障恢复时。 • 当用户想对外屏蔽自己的物理IP地址，对客户端提供透明化的服务时。

后端服务器

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

- 确保后端服务器实例的所属地域和负载均衡器的所属地域相同。
- 建议您选择相同操作系统的后端服务器实例作为后端服务器，以便后续管理和维护。
- 弹性负载均衡不支持后端FTP服务，但是可以支持SFTP场景。

1.2.2 创建独享型负载均衡器

操作场景

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

约束与限制

- 负载均衡器创建后，不支持修改VPC。如果要修改VPC，请重新创建负载均衡器，并选择对应的VPC。
- 独享型负载均衡实例创建完成后，您还需要创建监听器，才可以对负载均衡实例地址进行**ping**验证。

创建独享型负载均衡器

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面单击“购买弹性负载均衡器”。
   根据界面提示选择负载均衡器的基础配置，配置参数如**表1-6**所示。

表 1-6 负载均衡器的基础配置

参数	说明
实例类型	负载均衡的实例类型，选定后不支持修改。 独享型实例适用于大流量高并发的业务场景，如大型网站、云原生应用、车联网、多可用区容灾应用。 实例类型的区别详见**独享型负载均衡与共享型弹性负载均衡的区别**。
计费模式	独享型负载均衡器的收费类型。 • 包年/包月：预付费模式，即先付费再使用，按照订单的购买周期进行结算。 • 按需计费：后付费模式，即先使用再付费，按照弹性负载均衡实际使用时长计费，秒级计费，按小时结算。

参数	说明
区域	不同区域的资源之间内网不互通。请选择靠近业务的区域，可以降低网络时延、提高访问速度。
可用区	在同一区域下，电力、网络隔离的物理区域，可用区之间内网互通，不同可用区之间物理隔离。 如果业务需要考虑容灾能力，建议选择多个可用区，提高服务的可用性。当一个可用区出现故障或不可用时，业务可以快速切换到另一个可用区的负载均衡继续提供服务。更多可用区规划请参考**实例可用区**。 选择多个可用区之后，对应的最高性能规格（新建连接数/并发连接数等）会加倍。例如：单实例单AZ最高支持2千万并发连接，那么单实例双AZ最高支持4千万并发连接。 **说明** • 实例创建后，修改可用区配置可能会导致该实例的业务闪断数秒，请在购买时做好规划。 • 推荐选择闲时进行修改可用区配置的操作，详情请参见**变更实例可用区**。
规格	按需计费模式下，独享型负载均衡支持按弹性规格和固定规格两种规格进行购买。包年/包月计费模式下，仅支持按固定规格进行购买。 • 弹性规格：适用于业务用量较大的场景，按实例使用量收取LCU费用。 • 固定规格：适用于业务用量较为稳定的场景，按固定规格折算收取LCU费用。 “应用型（HTTP/HTTPS）”和“网络型（TCP/UDP）”请至少勾选一种，勾选后可选择相应能力的规格。请您根据自身业务规划选择实例规格，如何选择规格详见**独享型负载均衡的实例规格**。 **说明** 弹性规格已上线区域请参见**功能总览**中的弹性规格，其余区域持续上线中。
名称	待创建负载均衡器的名称。 • 长度范围为1~64位。 • 名称由中文、英文字母、数组、下划线（_）、中划线（-）和点组成。
企业项目	企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。
描述	您可对负载均衡器添加相关描述。

参数	说明
标签	标签用于标识云资源，可对云资源进行分类和搜索。标签由标签“键”和标签“值”组成，标签键用于标记标签，标签值用于表示具体的标签内容。命名规格请参照表1-7。 您最多可以添加20个标签。 **说明** 如果您的组织已经设定弹性负载均衡的相关标签策略，则需按照标签策略规则为弹性负载均衡添加标签。标签如果不符合标签策略的规则，则可能会导致弹性负载均衡创建失败，请联系组织管理员了解标签策略详情。

表 1-7 负载均衡器标签命名规则

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

5. 选定负载均衡器的规格后，请根据界面提示选择负载均衡器的网络配置，配置参数如表1-8所示。

表 1-8 负载均衡器的网络配置

参数	说明
IP类型后端（跨VPC后端）	开启后，支持用户按照IP地址为负载均衡器添加后端服务器。支持添加跨VPC的服务器IP地址。 **说明** • 若要使用该功能，请先正确配置VPC路由，确保后端可达。 • 开启IP类型后端（跨VPC后端），ELB需要占用后端子网中的IP地址与后端服务器进行通信，请确保预留足够的IP地址。当您选择子网后可以在子网后面的问号处查看所需IP的具体个数。

参数	说明
网络类型	可以单独选择一个网络类型，也可以同时选择多个。 • IPv4公网：负载均衡器通过IPv4公网IP对外提供服务，将来自公网的客户端请求按照指定的负载均衡策略分发到后端服务器进行处理。 • IPv4私网：负载均衡器通过IPv4私网IP对外提供服务，将来自同一个VPC的客户端请求按照指定的负载均衡策略分发到后端服务器进行处理。 • IPv6公网私网：系统会为实例分配一个IPv6地址，转发来自IPv6客户端的请求。 **说明** 如果公网或私网IP均未选择，则ELB实例创建完成后无法与客户端通信。请在使用ELB或测试业务连通性时，务必确保该ELB绑定了公网或私网IP。
所属VPC	负载均衡器所属虚拟私有云，独享型ELB创建完成后不支持修改，请做好相关网络规划。 您可以选择使用已有的虚拟私有云网络，或者单击“查看虚拟私有云”创建新的虚拟私有云。 您可以通过共享VPC功能，使用其他账号共享的VPC和子网，以实现网络资源的共享和统一管理，提升资源管控效率、降低运维成本。 有关VPC子网共享的更多信息，请参见《虚拟私有云用户指南》的“共享VPC”相关内容。
前端子网	独享型负载均衡所在的子网，从该子网中分配ELB实例对外服务的IP地址。 ELB创建完成后，支持解绑IP地址后，绑定新的前端子网下的IP地址。 根据配置的网络类型为ELB实例分配对应的IP地址： • IPv4私网：前端子网作为IPv4子网为ELB实例下发IPv4私有地址。 • IPv6公网私网：前端子网作为IPv6子网为ELB实例下发IPv6地址。 **说明** 当网络类型选择“IPv6公网私网”，且所选的VPC下无支持IPv6的子网时，请为已有子网开启IPv6或创建支持IPv6的子网。详见《虚拟私有云用户指南》。

参数	说明
后端子网	负载均衡实例将使用后端子网中的IP地址与后端服务器建立连接。 ● 默认选择：与前端子网保持一致。 ● 支持选择：负载均衡器所属VPC下的其他子网。 ● 支持新建：添加子网。 **说明** ● 负载均衡实例会占用后端子网中的部分IP地址，负载均衡实例的规格，可用区的数量和跨VPC功能的使用会影响占用IP地址的数量。实际占用IP地址的数量以您在控制台创建的负载均衡实例所占用的IP地址个数为准。 ● 应用型负载均衡器需要额外占用8-30个后端子网中的IP地址进行流量转发，具体占用地址数量与ELB集群规模有关，请以最终结果为准。如果多个ELB实例在同一集群且实例的后端子网相同，会复用占用的IP地址，以节省占用地址数量。
IPv4私网配置	
IPv4地址	选择IPv4地址的分配方式。 ● 自动分配IPv4地址：由系统自动分配IPv4地址。 ● 手动指定IP地址：手动指定IPv4地址。 **说明** 负载均衡器的IP地址不受所在后端子网ACL配置的限制，所以能够被客户端直接访问。建议您使用监听器的访问控制功能限制客户端访问负载均衡器。 详细请参考**访问控制策略**。
IPv6网络配置	
IPv6地址	选择IPv6的IP地址的分配方式。 ● 自动分配IPv6地址：由系统自动分配IPv6地址。 ● 手动指定IP地址：手动指定IPv6地址。 **说明** 负载均衡器的IP地址不受所在后端子网ACL配置的限制，所以能够被客户端直接访问。建议您使用监听器的访问控制功能限制客户端访问负载均衡器。 详细请参考**访问控制策略**。
共享带宽	选择IPv6的共享带宽。 可以选择暂不设置共享带宽或选择已有的共享带宽或新建共享带宽。
IPv4公网配置	
弹性公网IP	当网络类型勾选“IPv4公网”时，需要指定弹性公网IP。 ● 新创建：系统为弹性负载均衡实例新创建一个弹性公网IP。 ● 使用已有：为弹性负载均衡实例选择一个已有的弹性公网IP地址。

参数	说明
弹性公网IP类型	使用新创建弹性公网IP时，选择的弹性公网IP的链路类型。 ● 全动态BGP：可以根据设定的寻路协议实时自动优化网络结构，以保证客户使用的网络持续稳定、高效。 ● 静态BGP：网络结构发生变化时，无法实时自动调整网络设置以保障用户体验。
公网带宽	弹性公网IP使用的公网带宽的计费方式。 可选“按带宽计费”或“按流量计费”或“加入共享带宽”。 ● 按带宽计费：指定带宽上限，按使用时间计费，与使用的流量无关。 ● 按流量计费：指定带宽上限，按实际使用的上行流量计费，与使用时间无关。 ● 加入共享带宽
带宽	指定具体的带宽上限。

6. 当负载均衡的计费模式选定“包年/包月”时，需要指定实例的购买时长。
   “包年/包月”模式的负载均衡支持自动续费：
   - 按月购买：则自动续费周期为一个月，
   - 按年购买：则自动续费周期为一年。
7. 单击“立即购买”。
8. 确认配置信息，根据界面提示完成创建操作。

导出负载均衡器列表

负载均衡器创建完成后，您可以将当前账号下拥有的所有负载均衡器信息，以Excel文件的形式导出至本地，作为本地备份数据查看。

该文件记录了负载均衡器的名称、ID、状态、实例类型、规格等信息。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在负载均衡器列表左上方，单击“导出”，导出弹性负载均衡器列表。
   系统会将您所选的负载均衡信息自动导出为Excel文件，并下载至本地。

1.2.3 通过共享 VPC 创建独享型 ELB

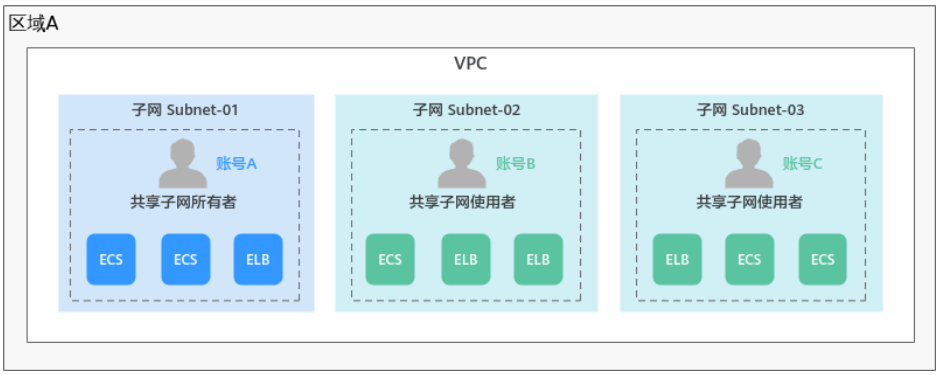
操作场景

创建独享型负载均衡器时，您可以通过共享VPC功能，使用其他账号共享的VPC和子网，以实现网络资源的共享和统一管理，提升资源管控效率、降低运维成本。

例如，为了规范管理网络资源，某企业使用账号A作为IT管理账号，用于管理基础公共资源，包括VPC、子网等。同时，账号A将多个子网共享给其他账号共同使用。

- 账号A：IT管理账号，作为资源所有者，创建VPC及子网，并将多个子网分别共享给其他账号使用。
- 账号B：业务账号，作为资源使用者，使用账号A共享的子网2创建独享型ELB。
- 账号C：业务账号，作为资源使用者，使用账号A共享的子网3创建独享型ELB。

图 1-5 业务规划示意图



本章节介绍通过共享VPC创建独享型负载均衡器的操作指导。有关VPC子网共享的更多信息，请参见《虚拟私有云用户指南》的“**共享VPC**”相关内容。

约束与限制

- 单个资源使用者最多可同时接收100个共享子网，当共享子网数量超过100个时，使用者将无法接收到超出数量的共享子网。
- 共享VPC功能不计费，资源使用者只需要为自己所创建的资源付费。

前提条件

作为资源所有者的账号A已创建共享VPC和子网，并指定资源使用者为账号B。创建共享的详细操作，请参见**创建共享**。

操作步骤

1. 以账号B登录控制台，进入**资源访问管理**页面，接受共享邀请。
   详细内容，请参见**接受/拒绝共享邀请**。
2. 进入**购买弹性负载均衡**页面。
3. 根据业务需要，完成购买独享型负载均衡器的基础配置和网络配置等各项参数的设置。
   设置“网络”相关参数时，选择由账号A共享的VPC和子网。

图 1-6 设置网络参数

其余配置，请参见**创建独享型负载均衡器**。

1.2.4 配置独享型负载均衡器的修改保护

您可以对负载均衡器开启修改保护功能，防止因误操作导致负载均衡器的配置被修改或负载均衡器被删除。

开启或关闭修改保护

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要开启修改保护的负载均衡器名称。
5. 切换到负载均衡器的“基本信息”页签，单击修改保护右侧的“设置”。
6. 在设置修改保护的弹窗中，开启或关闭“修改保护开关”。
   您可填写“添加修改保护原因”。
7. 单击“确定”。

说明

如果您需要修改负载均衡器的配置或删除负载均衡器，请先关闭“修改保护”开关。

1.2.5 变更独享型负载均衡器的基础配置

独享型负载均衡实例创建后，用户可根据实际使用需求变化，变更实例规格和实例可用区等基础配置。

变更实例规格

用户可根据实际使用需求变化，通过控制台提供的“变更规格”变更负载均衡实例规格的以下配置：

- 负载均衡实例的规格弹性：弹性规格或固定规格。
- 负载均衡实例的规格类型：网络型和应用型。
  您需保留至少一种实例规格类型，且移除负载均衡实例的规格类型时，必须先删除该规格类型支持的监听器。

  - 应用型（HTTP/HTTPS）实例，支持HTTP/HTTPS监听器。
  - 网络型（TCP/UDP）实例，支持TCP/UDP监听器。
- 负载均衡实例的规格大小（如小型 I、中型 I、大型 I等）。

不同计费模式下，独享型负载均衡实例支持的规格变更有差异，详见表1-9和表1-10。

说明

- 升级实例规格不会对用户的业务造成影响。
- 降低实例规格时会对业务造成短暂的影响：
  - 网络型（TCP/UDP）业务的部分新建连接会受影响。
  - 应用型（HTTP/HTTPS）业务的部分新建连接会受影响，还可能会造成部分长连接中断。

按需计费模式

表 1-9 按需计费模式下变更规格说明

计费模式	规格弹性	转弹性规格	转固定规格	增加规格类型	移除规格类型	升级规格	降低规格
按需计费	弹性规格	-	√	√	√	-	-
	固定规格	√	-	√	√	√	√

包年/包月计费模式

表 1-10 包年/包月计费模式下变更规格说明

计费模式	变更模式	增加规格类型	移除规格类型	升级规格	降低规格	实例变更规格说明
包年/包月	即时变更	×	×	√	×	新规格在当前计费周期内立即生效，您需要为当前计费周期的剩余时间补交差价。
	续费变更	×	×	√	√	变更规格后，实例在当前计费周期内无任何变动，新规格将在下一周期生效计费。

说明

包年/包月的独享型负载均衡实例默认不支持降低规格，如您有需求，可提交工单进行申请。

1. 登录管理控制台。

2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，在目标负载均衡实例所在行“操作”列选择“更多 > 变更规格”。
5. 根据界面提示选择变更后的规格，单击“下一步”。
6. 确认负载均衡实例变更前后的信息，单击“提交订单”。

说明

包年/包月的独享型负载均衡实例，提交订单后需确认订单信息并选择付款方式，单击“确认付款”。

变更实例可用区

独享型负载均衡实例创建后，用户可根据实际使用需求变化，通过控制台提供的“变更可用区”变更负载均衡实例部署的可用区。

变更可用区完成后，流量会重新分配到变更后的可用区。

变更可用区功能仅支持增加部署负载均衡实例的可用区，不支持移除已有可用区。

说明

变更可用区功能的发布区域请参考**功能总览**。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，在目标负载均衡实例所在行“操作”列选择“更多 > 变更可用区”。
5. 根据界面提示选择变更后的可用区，单击“下一步”。
6. 确认负载均衡实例变更前后的信息，单击“提交”。

注意

变更可用区时会对业务造成短暂的影响，部分业务会出现长连接闪断，连接请求重试后可恢复。建议您在业务低峰期变更可用区。

高频问题

弹性负载均衡可以修改实例的规格类型吗?

可以修改实例的规格类型。通过变更规格操作，用户可以实现网络型规格与应用型规格的切换。

变更实例规格对业务有影响吗?

升级实例规格不会对用户的业务造成影响，降低实例规格时会对业务造成短暂的影响。

1.2.6 变更独享型负载均衡器的网络配置

您可以通过变更负载均衡实例的网络配置来满足您的业务要求。

绑定/解绑定 IP 地址

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

支持绑定和解绑IPv4公网IP、IPv4私有IP、IPv6地址。

说明

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

绑定/解绑 IPv4 公网 IP

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，待修改的负载均衡器所在行，选择“更多 ”。
   a. 绑定IPv4公网IP：
      i. 单击“绑定IPv4公网IP”。
      ii. 在“绑定IPv4公网IP”对话框中，选择需要绑定的公网IP，单击“确定”。
   b. 解绑IPv4公网IP：
      i. 单击“解绑IPv4公网IP”。
      ii. 在“解绑IPv4公网IP”对话框中，确认需要释放的IPv4公网IP地址，单击“确定”。

绑定/解绑 IPv4 私有 IP

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，待修改的负载均衡器所在行，选择“更多”。
   a. 绑定IPv4私有IP：
      i. 单击“绑定IPv4私有IP”。

ii. 在“绑定IPv4私有IP”对话框中，选择待绑定的IPv4地址所在子网，设置目标IP地址后，单击“确定”。

说明

- 系统默认自动分配IP地址，如果需要手动指定IP地址，请去勾选“自动分配IPv4地址”，并在参数“IPv4地址”行输入目标IP地址。
- 输入的IP地址必须属于所选择的子网且未被使用。

b. 解绑IPv4私有IP：

i. 单击“绑定IPv4私有IP”。

ii. 在“解绑IPv4私有IP”对话框中，确认需要释放的IPv4私有IP地址，单击“确定”。

绑定/解绑 IPv6 地址

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，待修改的负载均衡器所在行，选择“更多”。
   a. 绑定IPv6地址：
      i. 单击“绑定IPv6地址”。
      ii. 在“绑定IPv6地址”对话框中，选择待绑定的IPv6地址所在子网，单击“确定”。
   b. 解绑IPv6地址：
      i. 单击“解绑IPv6地址”。
      ii. 在“解绑IPv6地址”对话框中，确认需要释放的IPv6地址，单击“确定”。

修改 IP 地址

独享型弹性负载均衡支持修改IPv4私有IP和修改IPv6地址。

- 修改IPv4私有IP：支持将负载均衡当前使用IPv4私有IP修改为当前子网或者其他子网的目标IP地址。
- 修改IPv6地址：仅支持将负载均衡实例当前使用IPv6地址修改为其他子网的IPv6地址，负载均衡实例所在VPC下需存在其他已开启IPv6功能的子网。

修改 IPv4 私有 IP

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”页面，需修改负载均衡器所在行，单击“更多 > 修改IPv4私有IP”。
5. 在“修改IPv4私有IP”对话框中，选择需要修改的目标IP所在子网，并设置目标IP地址。

- 不同子网下修改IPv4地址，可以勾选“自动分配IPv4地址”，勾选后，系统会自动分配一个所选择子网的IPv4地址。
- 同一子网下修改IPv4地址，必须指定IP，不支持自动分配。

6. 单击“确定”。

修改 IPv6 地址

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”页面，需修改负载均衡器所在行，单击“更多 > 修改IPv6地址”。
5. 在“修改IPv6地址”对话框中，选择需要修改的目标IP所在子网，并设置目标IP地址。

   当前IPv6地址只支持自动分配，所以修改IPv6地址，必须更换子网。
6. 单击“确定”。

修改公网带宽

当负载均衡器支持公网流量请求时（IPv4公网或IPv6），公网与负载均衡器之间的流量通过公网带宽进行访问，用户可以按照实际需求更改负载均衡实例关联的公网带宽。弹性负载均衡在变更公网带宽的时候，访问流量不会中断。

说明

- 变更负载均衡实例的公网带宽时，需考虑变更独享型负载均衡实例的规格，避免因负载均衡实例的带宽不足造成流量通过负载均衡器时被限速。
- 公网带宽为负载均衡实例绑定的弹性公网IP带宽，是客户端访问负载均衡实例时的最高流量限制。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，待修改带宽的负载均衡器所在行的“操作”列，单击“更多”。
5. 单击“修改IPv4带宽”或“ 修改IPv6带宽”。
6. 在“修改带宽”区域，设置新的带宽大小，单击“下一步”。

   可以选择系统定义好的带宽也可以自定义带宽大小。自定义修改带宽的范围为1-2,000 Mbit/s。
7. 确认修改后的带宽大小，单击“提交”。

说明

如果您更改了付费方式和带宽信息，具体扣费会以变更后费用为准。

加入/移出 IPv6 共享带宽

当独享型负载均衡实例绑定IPv6地址且加入IPv6共享带宽后，负载均衡实例可以基于IPv6地址进行公网流量转发。

您可以根据业务需要为负载均衡实例配置IPv6共享带宽。

说明

移出IPv6共享带宽后，对应的弹性负载均衡器将无法基于IPv6地址进行公网流量转发，请谨慎操作。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”页面，待设置的负载均衡器所在行，单击“更多”。
   a. 加入IPv6共享带宽：
      i. 单击“加入IPv6共享带宽”。
      ii. 在“加入IPv6共享带宽”对话框中，选择待加入的共享带宽。
      如果当前没有共享带宽可选择，请根据界面提示创建共享带宽。
   b. 移出IPv6共享带宽：
      i. 单击“移出IPv6共享带宽”。
      ii. 在“移出IPv6共享带宽”对话框中，确认待移出的共享带宽。
5. 单击“确定”。

1.2.7 释放独享型负载均衡器

操作场景

当您确认负载均衡不需要继续使用时，您可以根据需求随时释放您的负载均衡器。

注意

用户须自行确认数据完成备份或不再使用，资源释放后，数据将立即删除且无法恢复，请谨慎操作。

约束与限制

- 如果**负载均衡器配置了修改保护**，则无法执行删除，请先在负载均衡器的基本信息页签中关闭“修改保护”。
- 如果负载均衡器的**监听器配置了修改保护**，则无法执行删除，请先在监听器的基本信息页签中关闭“修改保护”。
- 如果负载均衡器的**后端服务器组配置了修改保护**，则无法执行删除，请先在后端服务器组的基本信息页签中关闭“修改保护”。

删除按需计费的负载均衡器

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

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，选择目标负载均衡器所在行的操作列下的“更多 > 删除”。
   弹出删除确认对话框。
5. 您可根据实际业务需求选择勾选“删除该负载均衡实例的后端服务器组”。
   如果后端服务器组已被其他独享型负载均衡实例使用，将不会执行删除。
6. 在删除确认对话框，输入“DELETE”。
7. 单击“确定”。

退订包年/包月的负载均衡器

退订公网类型负载均衡器时，可以选择是否同时退订EIP，绑定的EIP不会被默认自动删除，不会影响EIP的正常使用。

退订单个负载均衡器

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，在目标负载均衡器所在行“操作”列选择“更多 > 退订”。
   弹出退订确认对话框。
5. 在退订确认对话框，输入“UNSUBSCRIBE”，单击“是”。
6. 根据页面提示选择退订原因，确认退款金额并勾选退订须知信息，单击“退订”。
7. 在弹窗中，确认退订信息，单击“退订”。

批量退订负载均衡器

包年/包月的独享型负载均衡支持批量退订，具体操作如下：

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，勾选需要操作的负载均衡器。
5. 在负载均衡器列表左上方，单击“退订”。

6. 在退订确认对话框，输入“UNSUBSCRIBE”，单击“是”。
7. 根据页面提示选择退订原因，确认退款金额并勾选退订须知信息，单击“退订”。
8. 在弹窗中，确认退订信息，单击“退订”。

1.2.8 启停独享型负载均衡器

您可以随时启用和停用负载均衡器。负载均衡器停用后，将不再接收和转发流量。

当您配置的某些负载均衡器出于业务考虑暂时无需使用，但又不能删除时，可以选择启停操作。

启用或停用 ELB 实例

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，需要启用或者停用的负载均衡器所在行，单击“更多 > 启用”或者“更多 > 停用”。
5. 单击“是”。

注意

停用的负载均衡器仍会继续计费。

1.3 监听器

1.3.1 监听器概述

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

支持的协议类型

负载均衡提供四层协议和七层协议监听，您可根据从客户端到负载均衡器的应用场景选择监听协议，详细说明可参见表1-11。

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

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

表 1-11 监听协议类型说明

协议类型		说明	适用场景
四层协议	TCP	• 基于源地址的会话保持。 • 数据传输快。	• 适用于注重可靠性，对数据准确性要求高的场景，如文件传输、发送或接收邮件、远程登录。 • 对性能和并发规模有要求的Web应用。
四层协议	UDP	• 可靠性相对低 • 数据传输快	适用于关注实时性而相对不注重可靠性的场景，如视频聊天、游戏、金融实时行情推送。
四层协议	TLS	• 加密传输数据，可以阻止未经授权的访问。 • 支持单向认证和双向认证	适用于需要超高性能和大规模TLS卸载的场景。
七层协议	HTTP	• 基于Cookie的会话保持。 • 使用X-Forward-For获取源地址。	需要对数据内容进行识别的应用，如Web应用、移动游戏等。
七层协议	HTTPS	• 加密传输数据，可以阻止未经授权的访问。 • 加解密操作在负载均衡器上完成，可减少后端服务器的处理负载。 • 多种加密协议和加密套件可选。	需要加密传输的应用。

前端协议和端口

前端协议和端口即是负载均衡器提供服务时接收请求的端口。

负载均衡系统支持四层（TCP、UDP、TLS）和七层（HTTP、HTTPS）协议的负载均衡，可通过具体提供的服务能力选择对应的协议以及该协议对外呈现的端口。

说明

前端协议和端口设置后不允许修改，如果要修改，请重新创建监听器。

表 1-12 前端协议和端口说明

前端协议	TCP、UDP、TLS、HTTP、HTTPS

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

后端协议和端口

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

表 1-13 后端协议和端口说明

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

全端口监听

当独享型负载均衡的前端协议是TCP或UDP协议时，支持全端口监听功能。

监听器开启全端口监听功能后，可以对前端端口段内的所有端口进行监听，并将前端端口上接收到的请求转发到后端服务器的后端端口。

监听器超时时间

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

图 1-7 四层监听器超时时间示意图

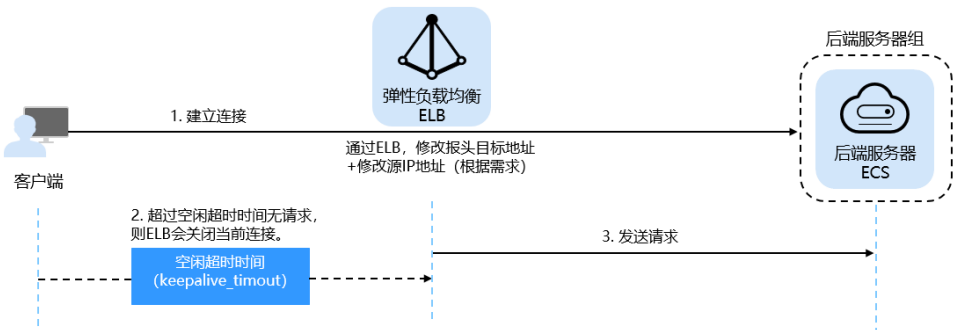


图 1-8 七层监听器超时时间示意图

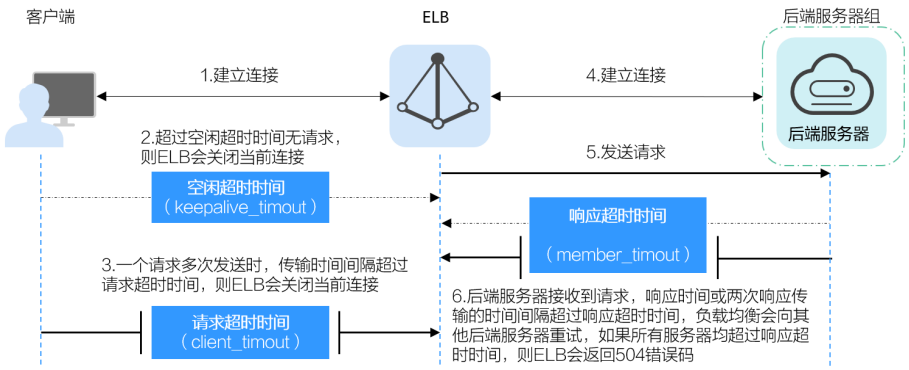


表 1-14 超时时间

协议	类别	描述	取值范围	默认超时时间
TCP	空闲超时时间	如果在超时时间内一直没有访问请求，负载均衡会关闭当前连接，直到下一次请求到来时再重新建立新的连接。	10~4000s	300s
UDP	空闲超时时间		10~4000s	300s
HTTP/HTTPS	空闲超时时间		0~4000s	60s
	请求超时时间	客户端向负载均衡发起请求，一个请求多次发送时，传输时间间隔超过请求超时时间，则负载均衡将放弃等待关闭连接。	1~300s	60s
	响应超时时间	负载均衡向后端服务器发起请求，如果超时时间内接收请求的后端服务器无响应或两次响应传输的时间间隔超过响应超时时间，负载均衡会向其他后端服务器重试请求。如果重试期间后端服务器一直没有响应，则负载均衡会给客户端返回HTTP 504错误码。 **说明** 当开启了会话保持功能时，如果响应超时时间内对应的后端服务器无响应，则直接会返回HTTP 504错误码。	1~300s	60s

1.3.2 网络型监听器

1.3.2.1 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，速度可以相对较慢的场景，如文件传输、发送或接收邮件、远程登录等。您可以添加一个TCP监听器转发来自TCP协议的请求。

约束与限制

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

添加 TCP 监听器

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要添加监听器的负载均衡名称。
5. 切换到“监听器”页签，单击“添加监听器”，配置监听器。配置监听器参数参见**表1-15**。

表 1-15 独享型负载均衡配置 TCP 监听器参数说明

参数	说明
名称	监听器名称。
前端协议	客户端与负载均衡监听器建立流量分发连接的协议。 协议选择TCP。
全端口监听	仅独享型负载均衡的TCP和UDP监听器支持此开关，开启后不支持关闭。 开启此开关，监听器可以对前端端口段内的所有端口进行监听，并将前端端口上接收到的请求转发到后端服务器的后端端口。 **说明** 该功能陆续上线中，已发布区域请参见**四层协议全端口监听和转发**。
前端端口	客户端与负载均衡监听器建立流量分发连接的端口。 取值范围为：[1-65535]。 **说明** 全端口监听开启时，需输入前端端口的起始端口和结束端口。

参数	说明
访问控制	支持通过白名单和黑名单进行访问控制，更多信息请参见**访问控制策略**： • 允许所有IP访问 • 黑名单 • 白名单
IP地址组	设置白名单或者黑名单时，必须选择一个IP地址组。如果还未创建IP地址组，需要先创建IP地址组，更多关于IP地址组的信息请参见**访问控制IP地址组**。
获取客户端IP	开启此开关，后端服务器可以获取到客户端的真实IP地址。 独享型负载均衡默认开启，且不可关闭。
高级配置	
空闲超时时间	如果在超时时间内一直没有访问请求，负载均衡会中断当前连接，直到下一次请求到来时再重新建立新的连接。 取值范围：10~4000s
描述	对于监听器描述。 字数范围：0/255。

6. 单击“下一步：配置后端分配策略”，配置监听器的默认后端服务器组。
   a. 推荐选择“使用已有”后端服务器组，您可参考**创建后端服务器组**进行创建。
   b. 您也可选择“新创建”后端服务器组，添加后端服务器并配置健康检查，
      i. 配置后端服务器组参数请参见**表1-47**。
      ii. 单击“下一步：添加后端服务器”，添加后端服务器并配置健康检查。
      添加后端服务器详见**后端服务器概述**，配置健康检查参数请参见**表1-48**。
7. 单击“下一步：确认配置”。
8. 确认配置无误后，单击“提交”。

1.3.2.2 添加 UDP 监听器

操作场景

UDP协议适用于关注实时性而相对不注重可靠性的场景，如视频聊天、游戏、金融实时行情推送。您可以添加一个UDP监听器转发来自UDP协议的请求。

约束与限制

- UDP监听器不支持分片包。
- UDP监听器的前端端口当前不支持4789。

- UDP监听器支持的最大MTU为1500，请确保与ELB通信的网卡的MTU不大于1500（有些应用程序需要根据此MTU值同步修改其配置文件），否则数据包可能会因过大被丢弃。
- 独享型负载均衡前端协议为“UDP”时，后端协议可以选择“UDP”或“QUIC”。
- 如果您的独享型负载均衡实例类型为应用型（HTTP/HTTPS），则无法创建UDP监听器。

添加 UDP 监听器

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要添加监听器的负载均衡名称。
5. 切换到“监听器”页签，单击“添加监听器”，配置监听器。配置监听器参数参见**表1-16**。

表 1-16 独享型负载均衡配置 UDP 监听器参数说明

参数	说明
名称	监听器名称。
前端协议	客户端与负载均衡监听器建立流量分发连接的协议。 协议选择UDP。
全端口监听	仅独享型负载均衡的TCP和UDP监听器支持此开关，开启后不支持关闭。 开启此开关，监听器可以对前端端口段内的所有端口进行监听，并将前端端口上接收到的请求转发到后端服务器的后端端口。 **说明** 该功能陆续上线中，已发布区域请参见**四层协议全端口监听和转发**。
前端端口	客户端与负载均衡监听器建立流量分发连接的端口。 取值范围为：[1-65535]。 **说明** 全端口监听开启时，需输入前端端口的起始端口和结束端口。
访问控制	支持通过白名单和黑名单进行访问控制，更多信息请参见**访问控制策略**： • 允许所有IP访问 • 黑名单 • 白名单
IP地址组	设置白名单或者黑名单时，必须选择一个IP地址组。如果还未创建IP地址组，需要先创建IP地址组，更多关于IP地址组的信息请参见**访问控制IP地址组**。

参数	说明
获取客户端IP	开启此开关，后端服务器可以获取到客户端的真实IP地址。 独享型负载均衡默认开启，且不可关闭。
高级配置	
空闲超时时间	如果在超时时间内一直没有访问请求，负载均衡会中断当前连接，直到下一次请求到来时再重新建立新的连接。 取值范围：10~4000s
描述	对于监听器描述。 字数范围：0/255。

6. 单击“下一步：配置后端分配策略”，配置监听器的默认后端服务器组。
   a. 推荐选择“使用已有”后端服务器组，您可参考**创建后端服务器组**进行创建。
   b. 您也可选择“新创建”后端服务器组，添加后端服务器并配置健康检查，
      i. 配置后端服务器组参数请参见**表1-47**。
      ii. 单击“下一步：添加后端服务器”，添加后端服务器并配置健康检查。
      添加后端服务器详见**后端服务器概述**，配置健康检查参数请参见**表1-48**。
7. 单击“下一步：确认配置”。
8. 确认配置无误后，单击“提交”。

1.3.2.3 添加后端为 QUIC 协议的 UDP 监听器

操作场景

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

说明

- QUIC协议的版本有：Q043、Q046、Q050。
- QUIC协议的UDP监听器不支持分片包。

约束与限制

- 独享型负载均衡支持使用后端监听器为QUIC协议。
- 独享型负载均衡器已经选择四层“网络型（TCP/UDP）”类型的规格。

添加后端为 QUIC 协议的 UDP 监听器

1. 登录管理控制台。

2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要添加监听器的负载均衡名称。
   此负载均衡器需要选择“网络型（TCP/UDP）”规格，使其能够创建四层（TCP/UDP）监听器。
5. 切换到“监听器”页签，单击“添加监听器”。
6. 在“添加监听器”页签，“前端协议”请选择“UDP”，其他参数根据实际情况设置，完成后单击“下一步：配置后端分配策略”。

图 1-9 前端协议选择“UDP”

7. 在“配置后端分配策略”页面，“后端协议”选择“QUIC”，其他参数根据实际情况设置。

图 1-10 后端协议选择“QUIC”

8. 根据需要配置相关参数，配置完成后，单击“提交”。

相关操作

监听器创建完成后，还需要添加后端服务器，更多后端服务器信息请参考**后端服务器概述**。

1.3.2.4 添加 TLS 监听器

操作场景

TLS协议适用于需要超高性能和大规模TLS卸载的场景。您可以添加一个TLS监听器转发来自客户端加密的TCP协议请求。

说明

该功能陆续上线中，已发布区域请参见**弹性负载均衡支持TLS协议**。

约束与限制

- 仅支持TLS新建连接数的网络型（TCP/UDP/TLS）负载均衡实例可以创建TLS监听器。
- TLS监听器仅支持添加后端协议为TCP或TLS的后端服务器组。

添加 TLS 监听器

1. 登录管理控制台。

2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要添加监听器的负载均衡名称。
5. 切换到“监听器”页签，单击“添加监听器”配置监听器参数参见**表1-17**。

表 1-17 独享型负载均衡配置 TLS 监听器参数说明

参数	说明
名称	监听器名称。
前端协议	客户端与负载均衡监听器建立流量分发连接的协议。 协议选择TLS。
全端口监听	仅独享型负载均衡的TCP/UDP/TLS监听器支持此开关，开启后不支持关闭。 开启此开关，监听器可以对前端端口段内的所有端口进行监听，并将前端端口上接收到的请求转发到后端服务器的后端端口。 **说明** 全端口监听开启时，需输入前端端口的起始端口和结束端口。
前端端口	客户端与负载均衡监听器建立流量分发连接的端口。 取值范围为：[1-65535]。 **说明** 全端口监听开启时，需输入前端端口的起始端口和结束端口。
SSL解析方式	确保服务安全，请选择客户端到服务器端认证方式。 可选择“单向认证”或“双向认证”。 ● 如仅进行服务器端认证，请选择单向认证。 ● 双向认证需要负载均衡实例与访问用户互相提供身份认证，从而允许通过认证的用户访问负载均衡实例，后端服务器无需额外配置双向认证。
服务器证书	协议类型为TLS时，需绑定服务器证书。 服务器证书用于SSL握手协商，需提供证书内容和私钥。
CA证书	协议类型为TLS时，且SSL解析方式为“双向认证”时，需绑定CA证书。 CA证书又称客户端CA公钥证书，用于验证客户端证书的签发者；在开启HTTPS双向认证功能时，只有当客户端能够出具指定CA签发的证书时，HTTPS连接才能成功。

参数	说明
开启SNI	TLS协议的负载均衡可以选择是否开启SNI。 SNI是为了解决一个服务器使用多个域名和证书的TLS扩展。 开启SNI后，允许客户端在发起SSL握手请求时就提交请求的域名信息，ELB收到SSL请求后，会根据域名去查找证书，如果找到域名对应的证书，则返回该证书；如果没有找到域名对应的证书，则返回缺省证书。详见**开启SNI证书实现多域名访问**。
SNI证书	HTTPS协议的负载均衡设置开启SNI后需要选择域名对应的证书。 可选择已创建或者创建新的SNI证书。
访问控制	支持通过白名单和黑名单进行访问控制，更多信息请参见**访问控制策略**。 • 允许所有IP访问 • 黑名单 • 白名单
IP地址组	设置白名单或者黑名单时，必须选择一个IP地址组。如果还未创建IP地址组，需要先创建IP地址组，更多关于IP地址组的信息请参见**访问控制IP地址组**。
获取客户端IP	TLS监听器下，获取客户端IP功能失效，可通过开启ProxyProtocol功能获取客户端真实IP。
ProxyProtocol	支持通过ProxyProtocol协议携带客户端真实IP到后端服务器。 **说明** 请确保后端服务器具有解析ProxyProtocol协议的能力，否则可能导致业务中断，请谨慎开启。
高级配置	
安全策略	支持选择可用的安全策略，更多信息请参见**安全策略**。
空闲超时时间（秒）	如果在超时时间内一直没有访问请求，负载均衡会中断当前连接，直到下一次请求到来时再重新建立新的连接。 时间取值范围[0-4000]。
标签	可通过配置该项使用标签功能。标签的“键”和“值”是一一对应的，其中“键”值是唯一的。
描述	对于监听器描述。 字数范围：0/255。

6. 单击“下一步：配置后端分配策略”，配置监听器的默认后端服务器组。
   a. 推荐选择“使用已有”后端服务器组。

b. 您也可选择“新创建”后端服务器组，添加后端服务器并配置健康检查，

i. 配置后端服务器组参数请参见**表1-47**。

ii. 单击“下一步：添加后端服务器”，添加后端服务器并配置健康检查。

添加后端服务器详见**后端服务器概述**，配置健康检查参数请参见**表1-48**。

7. 单击“下一步：确认配置”。
8. 确认配置无误后，单击“提交”。

1.3.3 应用型监听器

1.3.3.1 添加 HTTP 监听器

操作场景

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

约束与限制

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

添加 HTTP 监听器

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要添加监听器的负载均衡名称。
5. 切换到“监听器”页签，单击“添加监听器”，配置监听器。配置监听器参数参见**表1-18**。

表 1-18 独享型负载均衡配置 HTTP 监听器参数说明

参数	说明
名称	监听器名称。
前端协议	客户端与负载均衡监听器建立流量分发连接的协议。 选择HTTP协议。
前端端口	客户端与负载均衡监听器建立流量分发连接的端口。 取值范围为：[1-65535]。

参数	说明
重定向	重定向开关是否开启。 协议类型为HTTP时，可根据需要设置该项。需要保证业务建立安全连接时，若同时创建了HTTPS监听器和HTTP监听器，可以通过重定向功能，将HTTP监听器访问重定向至HTTPS监听器。 HTTP监听器被重定向后，会返回301返回码。
重定向至	重定向开关开启，需要选择重定向至的HTTPS监听器的名称。
访问控制	支持通过白名单和黑名单进行访问控制，更多信息请参见**访问控制策略**： • 允许所有IP访问 • 黑名单 • 白名单
IP地址组	设置白名单或者黑名单时，必须选择一个IP地址组。如果还未创建IP地址组，需要先创建IP地址组，更多关于IP地址组的信息请参见**访问控制IP地址组**。
获取客户端IP	开启此开关，后端服务器可以获取到客户端的真实IP地址。 独享型负载均衡默认开启，且不可关闭。
高级转发策略	高级转发策略支持多样化的转发规则和转发动作，便于灵活的分流业务，合理的分配资源。 更多信息请参见**高级转发策略概述**。
高级配置	

参数	说明
HTTP/HTTPS头字段	根据您的业务需求，开启您需要添加的HTTP/HTTPS头字段功能开关。 ● 获取类头字段： – 获取弹性公网IP：ELB通过X-Forwarded-ELB-IP头字段获取负载均衡实例的公网IP地址。 – 获取监听器端口号：ELB通过X-Forwarded-Port头字段获取监听器的端口号。 – 获取客户端请求端口号：ELB通过X-Forwarded-For-Port头字段获取客户端请求的端口号。 – 获取负载均衡实例ID：ELB通过X-Forwarded-ELB-ID头字段获取负载均衡实例的ID。 ● 重写类头字段： – 重写X-Forwarded-Host：ELB以客户端请求头的Host重写X-Forwarded-Host传递到后端服务器。 – 重写X-Forwarded-Proto：ELB以监听器的前端协议重写X-Forwarded-Proto头字段传递到后端服务器。 – 重写X-Real-IP：ELB以客户端的源IP地址重写X-Real-IP传递到后端服务器。 更多详情请参考**配置HTTP/HTTPS头字段**。
数据压缩	开启将对特定文件类型进行压缩；关闭则不会对任何文件类型进行压缩。 ● Brotli支持压缩所有类型。 ● Gzip支持压缩的类型如下： text/xml text/plain text/css application/javascript application/x-javascript application/rss+xml application/atom+xml application/xml application/json。 **说明** 该功能陆续上线中，已发布区域请参见**数据压缩**。
空闲超时时间（秒）	如果在超时时间内一直没有访问请求，负载均衡会中断当前连接，直到下一次请求到来时再重新建立新的连接。 时间取值范围[0-4000]。
请求超时时间（秒）	客户端向负载均衡发起请求，如果在超时时间内客户端没有完成整个请求的传输，负载均衡将放弃等待关闭连接。 时间取值范围[1-300]。

参数	说明
响应超时时间（秒）	负载均衡向后端服务器发起请求，如果超时时间内接收请求的后端服务器无响应，负载均衡会向其他后端服务器重试请求。如果重试期间后端服务器一直没有响应，则负载均衡会给客户端返回HTTP 504错误码。 时间取值范围[1-300]。 **说明** 当开启了会话保持功能时，响应超时时间内如果对应的后端服务器无响应，则直接会返回HTTP 504错误码。
描述	对于监听器描述。 字数范围：0/255。

6. 单击“下一步：配置后端分配策略”，配置监听器的默认后端服务器组。
   a. 推荐选择“使用已有”后端服务器组，您可参考**创建后端服务器组**进行创建。
   b. 您也可选择“新创建”后端服务器组，添加后端服务器并配置健康检查，
      i. 配置后端服务器组参数请参见**表1-47**。
      ii. 单击“下一步：添加后端服务器”，添加后端服务器并配置健康检查。
      添加后端服务器详见**后端服务器概述**，配置健康检查参数请参见**表1-48**。
7. 单击“下一步：确认配置”。
8. 确认配置无误后，单击“提交”。

1.3.3.2 添加 HTTPS 监听器

操作场景

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

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

如果您不希望负载均衡器对HTTPS流量进行解密，可以通过配置相同端口的TCP监听器将HTTPS流量透传到后端服务器。具体原理参见**TCP监听器将HTTPS流量透传到后端服务器**。

约束与限制

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

添加 HTTPS 监听器

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要添加监听器的负载均衡名称。
5. 切换到“监听器”页签，单击“添加监听器”，配置监听器。配置监听器参数参见**表1-19**。

表 1-19 独享型负载均衡配置 HTTPS 监听器参数说明

参数	说明
名称	监听器名称。
前端协议	客户端与负载均衡监听器建立流量分发连接的协议。 协议选择HTTPS。
前端端口	客户端与负载均衡监听器建立流量分发连接的端口。 取值范围为：[1-65535]。
SSL解析方式	确保服务安全，请选择客户端到服务器端认证方式。 可选择“单向认证”或“双向认证”。 • 如仅进行服务器端认证，请选择单向认证。 • 双向认证需要负载均衡实例与访问用户互相提供身份认证，从而允许通过认证的用户访问负载均衡实例，后端服务器无需额外配置双向认证。
CA证书	协议类型为HTTPS且SSL解析方式为“双向认证”时，需绑定CA证书。 CA证书又称客户端CA公钥证书，用于验证客户端证书的签发者；在开启HTTPS双向认证功能时，只有当客户端能够出具指定CA签发的证书时，HTTPS连接才能成功。 详见**创建证书**。
服务器证书	协议类型为HTTPS时，监听器需绑定服务器证书。 服务器证书用于SSL握手协商，具有服务器身份验证和加密传输双重功能。 详见**创建证书**。
开启SNI	HTTPS协议的负载均衡可以选择开启SNI，以满足您的多域名访问或关联多个服务器证书的需求。 开启SNI后，允许客户端在发起SSL握手请求时就提交请求的域名信息，ELB收到SSL请求后，会根据域名去查找证书，如果找到域名对应的证书，则返回该证书；如果没有找到域名对应的证书，则返回缺省证书。详见**开启SNI证书实现多域名访问**。

参数	说明
SNI证书	HTTPS协议的负载均衡设置开启SNI后需要选择域名对应的证书。 可选择已创建或者创建新的SNI证书。 详见**创建证书**。
访问控制	支持通过白名单和黑名单进行访问控制，更多信息请参见**访问控制策略**： • 允许所有IP访问 • 黑名单 • 白名单
IP地址组	设置白名单或者黑名单时，必须选择一个IP地址组。如果还未创建IP地址组，需要先创建IP地址组，更多关于IP地址组的信息请参见**访问控制IP地址组**。
获取客户端IP	开启此开关，后端服务器可以获取到客户端的真实IP地址。 独享型负载均衡默认开启，且不可关闭。
高级转发策略	高级转发策略支持多样化的转发规则和转发动作，便于灵活的分流业务，合理的分配资源。 更多信息请参见**高级转发策略概述**。
高级设置	
安全策略	支持选择可用的安全策略，更多信息请参见**安全策略**。
HTTP/2	协议类型为HTTPS时，可选择是否支持该协议类型。详见**开启HTTP/2提升通信效率**。

参数	说明
HTTP/HTTPS头字段	根据您的业务需求，开启您需要添加的HTTP/HTTPS头字段功能开关。 ● 获取类头字段： – 获取弹性公网IP：ELB通过X-Forwarded-ELB-IP头字段获取负载均衡实例的公网IP地址。 – 获取监听器端口号：ELB通过X-Forwarded-Port头字段获取监听器的端口号。 – 获取客户端请求端口号：ELB通过X-Forwarded-For-Port头字段获取客户端请求的端口号。 – 获取负载均衡实例ID：ELB通过X-Forwarded-ELB-ID头字段获取负载均衡实例的ID。 ● 重写类头字段： – 重写X-Forwarded-Host：ELB以客户端请求头的Host重写X-Forwarded-Host传递到后端服务器。 – 重写X-Forwarded-Proto：ELB以监听器的前端协议重写X-Forwarded-Proto头字段传递到后端服务器。 – 重写X-Real-IP：ELB以客户端的源IP地址重写X-Real-IP传递到后端服务器。 更多详情请参考**配置HTTP/HTTPS头字段**。
数据压缩	开启将对特定文件类型进行压缩；关闭则不会对任何文件类型进行压缩。 ● Brotli支持压缩所有类型。 ● Gzip支持压缩的类型如下： text/xml text/plain text/css application/javascript application/x-javascript application/rss+xml application/atom+xml application/xml application/json。 **说明** 该特性陆续上线中，已发布区域请参见**数据压缩**。
空闲超时时间（秒）	如果在超时时间内一直没有访问请求，负载均衡会中断当前连接，直到下一次请求到来时再重新建立新的连接。 时间取值范围[0-4000]。
请求超时时间（秒）	客户端向负载均衡发起请求，如果在超时时间内客户端没有完成整个请求的传输，负载均衡将放弃等待关闭连接。 时间取值范围[1-300]。

参数	说明
响应超时时间（秒）	负载均衡向后端服务器发起请求，如果超时时间内接收请求的后端服务器无响应，负载均衡会向其他后端服务器重试请求。如果重试期间后端服务器一直没有响应，则负载均衡会给客户端返回HTTP 504错误码。 时间取值范围[1-300]。 **说明** 当开启了会话保持功能时，响应超时时间内如果对应的后端服务器无响应，则直接会返回HTTP 504错误码。
描述	对于监听器描述。 字数范围：0/255。

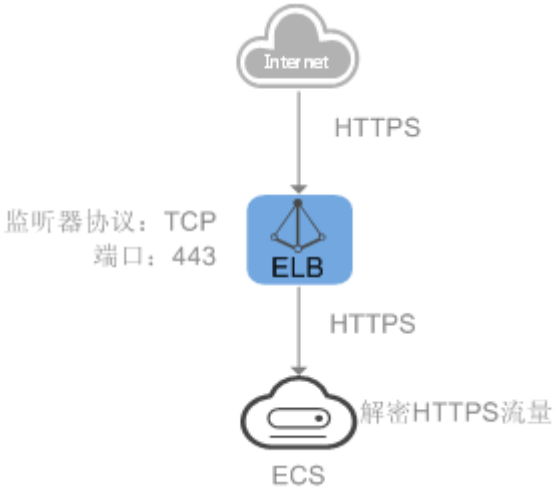
6. 单击“下一步：配置后端分配策略”，配置监听器的默认后端服务器组。
   a. 推荐选择“使用已有”后端服务器组，您可参考**创建后端服务器组**进行创建。
   b. 您也可选择“新创建”后端服务器组，添加后端服务器并配置健康检查，
      i. 配置后端服务器组参数请参见**表1-47**。
      ii. 单击“下一步：添加后端服务器”，添加后端服务器并配置健康检查。
      添加后端服务器详见**后端服务器概述**，配置健康检查参数请参见**表1-48**。
7. 单击“下一步：确认配置”。
8. 确认配置无误后，单击“提交”。

TCP 监听器将 HTTPS 流量透传到后端服务器

如果您不希望负载均衡器对HTTPS流量进行解密，可以通过配置相同端口的TCP监听器将HTTPS流量透传到后端服务器。并且在实例的安全组配置相同端口的TCP入方向规则，以允许相同端口上来自负载均衡器的入站流量。

如下图所示，TCP监听器如何将端口为443的HTTPS流量进行无解密透传到后端服务器。

图 1-11 TCP 透传 HTTPS 流量



1.3.3.3 转发策略

转发策略概述

您可以通过给独享型负载均衡添加转发策略，将来自不同域名或者不同URL的请求转发到不同的后端服务器组处理，便于灵活的分流业务，合理的分配资源。

转发策略由**转发规则**和**转发动作**两部分组成，参见**表1-20**。

表 1-20 转发策略支持的规则与动作

策略分类	转发规则	动作
转发策略	域名、URL。	转发至后端服务器组、重定向至监听器（仅HTTP监听器支持）。
高级转发策略	域名、URL、HTTP请求方法、HTTP请求头、查询字符串、网段。	转发至后端服务器组、重定向至监听器、重定向至URL、返回固定响应、重写。

说明

独享型负载均衡开启“高级转发策略”功能后，请参考**管理高级转发策略**配置高级转发策略。

匹配原理

- 在添加了转发策略后，负载均衡器将按以下规则转发前端请求：
  - 如果能匹配到监听器的转发策略，则按该转发策略将请求转发到对应的后端服务器组。
  - 如果不能匹配到监听器的转发策略，则按照默认转发策略将请求转发到监听器默认的后端服务器组（创建监听器时配置的后端服务器组）。
- 匹配优先级：
  - 不同域名间优先级互相独立，转发规则域名与URL同时存在时，优先按照域名进行匹配。
  - 转发规则为URL时，匹配优先级如下：精确匹配 > 前缀匹配 > 正则匹配，匹配类型相同时URL长度越长，优先级越高。

表 1-21 转发策略示例

访问请求	转发策略	转发规则	设定值
www.elb.com/test	1	URL	/test
	2	域名	www.elb.com

说明

如表1-21中，访问请求www.elb.com/test同时满足转发策略1和转发策略2，优先按照域名进行匹配，则请求将按照转发策略2进行转发。

约束与限制

- 此功能目前仅支持协议类型为HTTP、HTTPS的监听器。
- 负载均衡控制台不支持创建相同的转发策略。
- 一个监听器最多支持配置100条转发策略，超过配额的转发策略不生效。
- 配置转发策略时，请注意以下事项：
  - 转发规则URL仅支持路径，不支持查询字符串。如果您的URL设置为/path/resource?name=value，该条转发策略将失效。
  - 每个URL路径需要存于后端服务器（即必须是后端服务器上真实存在的路径），否则访问后端服务器时，后端服务器会返回404。
  - 因为正则匹配采用顺序匹配的方式，只要任意规则匹配成功就结束匹配。所以配置“URL匹配规则”为“正则匹配”的多个匹配规则时，规则之间不能重叠。
  - 不能配置URL路径完全相同的转发策略。
  - 输入的域名总长度不能超过100个字符。

添加转发策略

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要添加转发策略的负载均衡器名称。
5. 在“监听器”页签，您可以通过以下两种操作入口，进入监听器的“转发策略”页签。
   - 在目标监听器所在行的“转发策略”列，单击“添加/编辑转发策略”。
   - 单击目标监听器的名称，并切换到“转发策略”页签。
6. 单击“添加转发策略”按钮。参考表1-22配置参数。

表 1-22 添加转发策略的参数

参数	类型	说明	样例
如果**转发规则**	域名	触发转发的域名，仅支持精确域名。 域名或者URL至少要指定一个。	www.test.com

参数	类型	说明	样例
	URL	• 匹配说明 触发转发的URL。URL由英文字母、数字和特殊字符_~';@^-%#$.*+?,=!:|\/()[]{}组成。 • 匹配方式 – 精确匹配：请求的URL和设定URL完全一致，只能由/开头。 – 前缀匹配：请求的URL匹配已设定URL开头的URL，只能由/开头。 – 正则匹配：请求的URL和设定的URL正则表达式匹配。	/login.php
然后**转发动作**	转发至后端服务器组	如果请求与配置的转发规则匹配，则将请求转发至配置的后端服务器组。	-
	重定向至监听器	如果请求与配置的转发规则匹配，则将请求重定向至配置的监听器。 仅HTTP监听器支持配置该动作类型。 **说明** 选择“重定向至监听器”后，除访问控制以外原HTTP监听器的配置会失效，将以重定向至的HTTPS监听器的配置进行转发。	-

7. 配置完成，单击“保存”。

1.3.3.4 高级转发策略

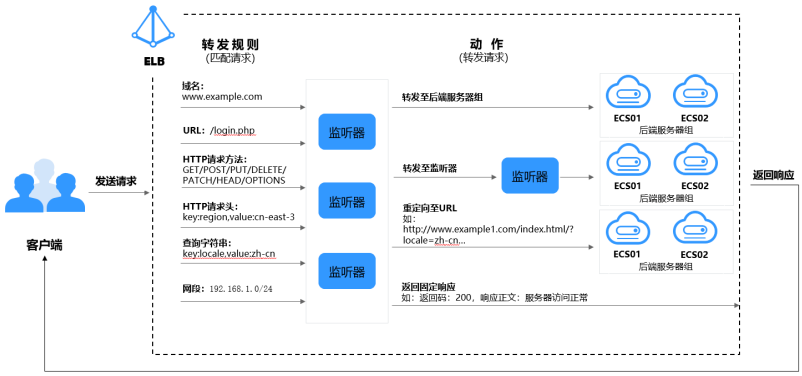
1.3.3.4.1 高级转发策略概述

高级转发策略简介

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

高级转发策略支持多样化的转发规则和转发动作，便于灵活的分流业务，合理的分配资源。详情见**表1-23**。

图 1-12 高级转发策略（独享型）示意图



高级转发策略的实现分为以下四个步骤：

步骤1 客户端发送请求至ELB。

步骤2 ELB首先根据事先设置好的高级转发策略中的转发规则匹配请求。

步骤3 ELB再根据转发规则对应的动作将客户端请求转发至对应的后端服务器进行处理。

步骤4 最后返回响应至客户端。

----结束

表 1-23 高级转发策略支持的转发规则与动作

转发策略设置	描述
转发规则	域名、URL、HTTP请求方法、HTTP请求头、查询字符串、网段。 详见**转发规则**。
转发动作	转发至后端服务器组、重定向至监听器、重定向至URL、返回固定响应、重写。 详见**转发动作**。 **说明** 转发动作设置为“转发至后端服务器组”时，支持额外添加转发动作：重写。 详情见**添加转发动作（可选）**。

说明

转发动作支持重写功能陆续上线中，已发布区域请参见**转发动作支持重写**。

匹配原理

每个HTTP/HTTPS监听器创建后，都会有一个默认的转发策略将请求转发到监听器默认的后端服务器组（即创建监听器时配置的后端服务器组）。

默认转发策略的优先级最低，不参与转发策略排序；可以编辑，但不可删除。

每个请求会按照转发策略的优先级顺序（转发策略编号的数值越小，优先级越高）逐条匹配，一旦能够匹配到一条转发策略，立即按照当前转发策略进行转发。

- 如果能匹配到监听器的转发策略，则按该转发策略转发请求。
- 如果不能匹配到监听器的转发策略，则将请求按照默认转发策略进行转发。

转发规则

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

表 1-24 高级转发策略的转发规则

转发规则	描述
域名	• 匹配说明 触发转发的域名。 – 可以并列添加多个域名。至少包含两个字符串，字符串间以点分割，单个字符串不超过63个字符，域名的长度不能超过100个字符。 – 字符串只能由英文字母、数字、中划线、小数点和特殊字符*组成。字符串中须以英文字母、数字或*开头，不能以中划线结尾。*只能出现在开头且必须以*.开始。 • 匹配方式 支持精确域名和泛域名匹配。 域名示例： 请求链接为：https://**www.example.com**/login.php?locale=zh-cn#videos 转发规则选择“域名”时，填写：**www.example.com**
URL	• 匹配说明 触发转发的URL，可以并列添加多个URL。URL由英文字母、数字和特殊字符_~';@^-%#$.*+?,=!:|\/()[]{}组成，长度范围为1~128个字符。 如果URL中包含特殊字符（如：?或#）本身，则需要先将特殊字符进行转义后再配置URL转发策略。 • 匹配方式 – 精确匹配：请求的URL和设定URL完全一致。只能由/开头，支持星号（*）和半角问号（?）作为通配符使用。 – 前缀匹配：请求的URL匹配已设定URL开头的URL。只能由/开头，支持星号（*）和半角问号（?）作为通配符使用。 – 正则匹配：请求的URL和设定的URL正则表达式匹配。 更多关于URL匹配转发规则的信息，请参见**URL高级转发策略匹配示例**。 URL示例： 请求链接为：https://www.example.com**/login.php**?locale=zh-cn#videos 转发规则选择“URL”时，填写：**/login.php**

转发规则	描述
查询字符串	当请求中的字符串与设置好的转发策略中的字符串相匹配时，触发转发。 查询字符串是键值对的形式，需要分别设置值： ● 键（key）：只能包含英文字母、数字和特殊字符!$'()*+,./:;=?@^-_'。 ● 值（value）：一个键下可以配置多个值。只能包含英文字母、数字和特殊字符!$'()*+,./:;=?@^-_'。还支持*和？两种通配符。 查询字符串示例： 请求链接为：https://www.example.com/login.php?**locale=zh-cn**#videos 转发规则需配置“查询字符串”： 键（key）：**locale** 值（value）：**zh-cn**
HTTP请求方法	触发转发的HTTP请求方法。 ● 可以并列设置多个请求方法。 ● 主要分为以下几种：GET、POST、PUT、DELETE、PATCH、HEAD、OPTIONS HTTP请求方法示例： GET
HTTP请求头	触发转发的HTTP请求头。 请求头是键值对的形式，需要分别设置值： ● 键（key）：只能由英文字母、数字、下划线和中划线组成。 ● 值（value）：一个键下可以配置多个值。只能包含英文字母、数字和特殊字符!#$%&'()*+,.\/:;<=>?@[]^-_'{|}~。还支持*和？两种通配符。 HTTP请求头示例： 键（key）：Accept-Language 值（value）：zh-CN
网段	触发转发的请求网段。 网段示例： 192.168.1.0/24或2020:50::44/127

转发动作

高级转发策略支持的转发动作类型有：转发至后端服务器组、重定向至监听器、重定向至URL、返回固定响应、重写。

表 1-25 高级转发策略的转发动作

转发动作	描述
转发至后端服务器组	如果满足转发规则的条件，则将请求转发至配置好的后端服务器组。 **说明** 转发动作设置为“转发至后端服务器组”时，支持额外添加转发动作：重写。 详情见**添加转发动作（可选）**。
重定向至监听器	如果满足转发规则的条件，则将请求转发至配置好的监听器上。 **说明** 选择“重定向至监听器”并配置监听器后，除访问控制以外原有监听器配置会失效。 例如：配置了重定向至监听器后，当客户端通过HTTP请求访问的时候，后端服务器会返回HTTPS的响应，即强制以HTTPS请求访问网页。因此实际以HTTPS监听器的配置为准向后端服务器进行转发，原有HTTP监听器的配置失效。
重定向至URL	如果满足转发规则的条件，则将请求重定向至配置好的URL。 客户端访问ELB网址A后，ELB返回302或者其他3xx返回码和目的网址B，客户端自动跳转到网址B，网址B可自定义。 需要设置如下参数，其中协议、域名、端口和路径至少设置一条。 • **协议**：可以选择“${protocol}”或“HTTP”或“HTTPS”。${protocol}表示与源协议相同。 • **域名**：至少包含两个字符串，字符串间以点分割，字符串只能由英文字母、数字、中划线和小数点组成。字符串必须以英文字母或数字开头，不能以中划线结尾。${host}表示与源域名相同。 • **端口**：取值范围是1~65535。${port}表示与源端口相同。 • **路径**：由英文字母、数字和特殊字符_~';@^-%#&$.*+?,=!:\|\/()[]{}组成，只能由/开头。${path}表示与源路径相同。 **说明** 转发规则选择URL的正则匹配后，转发动作“重定向至URL”中的路径支持正则表达式替换。路径替换规则详情见**转发动作的路径支持URL的正则表达式示例**。 • **查询字符串**：只能包含英文字母、数字和特殊字符!$'()*+,./:;=?@&^-_'，&仅支持作为分隔符使用。 • **返回码**：可以选择“301”、“302”、“303”、“307”、“308”。 **重定向至URL示例** 重定向的链接为：http://www.example1.com/index.html?locale=zh-cn#videos 协议：HTTP 域名：www.example1.com 端口：8081 路径：/index.html 查询字符串：locale=zh-cn 返回码：301

转发动作	描述
返回固定响应	如果满足转发规则的条件，则返回固定响应。 用户访问ELB实例后，ELB直接返回响应，不向后端服务器继续转发，返回响应的状态码和内容可以自定义。 需要设置如下参数： ● **返回码**：默认支持2XX、4XX、5XX系列状态码。 ● **Content-Type**：可以选择“text/plain”、“text/css”、“text/html”、“application/javascript”、“application/json”。 ● **响应正文**：非必填项，取值范围是0~1024个字符。 **响应正文示例** text/plain 很抱歉,暂不支持该语言. text/css <head><style type="text/css">div {background-color:red}#div {font-size:15px;color:red}</style></head> text/html <form action="/" method="post" enctype="multipart/form-data"><input type="text" name="description" value="some text"><input type="file" name="myFile"><button type="submit">Submit</button></form> application/javascript String.prototype.trim = function() {var reExtraSpace = /^\s*(.*?)\s+$/;return this.replace(reExtraSpace, "$1")} application/json { "publicip": { "type": "5_bgp","ip_version": 4},"bandwidth": {"name": "bandwidth123","size": 10,"share_type": "PER"}} **说明** 填写响应正文时，请不要有回车格式，否则无法保存。

表 1-26 添加转发动作（可选）

转发动作	描述
重写	如果满足转发规则的条件，则将请求重写为配置好的URL后再访问后端服务器组。 需要设置如下参数： ● **域名**：至少包含两个字符串，字符串间以点分割，字符串只能由英文字母、数字、中划线和小数点组成。字符串必须以英文字母或数字开头，不能以中划线结尾。${host}表示与源域名相同。 ● **路径**：由英文字母、数字和特殊字符_~';@^-%#&$.*+?,=!:|\/()[]{}组成，只能由/开头。${path}表示与源路径相同。 **说明** 转发规则选择URL的正则匹配后，转发动作“重定向至URL”和“重写”中的路径支持正则表达式替换。路径替换规则详情见**转发动作的路径支持URL的正则表达式示例**。 ● **查询字符串**：只能包含英文字母、数字额特殊字符!$'()*+,./:;=?@&^-_'，&仅支持作为分隔符使用。 **说明** 重写类型的转发动作中域名、路径和查询字符串不能全部为空或者默认值。

转发动作	描述
跨域	如果满足转发规则的条件，则ELB支持跨域请求，可以添加跨域资源共享CORS（Cross-Origin Resource Sharing）标头以允许浏览器跨域访问 Web应用程序。 跨域：在Web开发中，出于安全原因，浏览器实施的同源策略限制了从一个源加载的网页脚本访问来自不同源的资源。如果客户端发送的请求URL的协议、域名或者端口三者之间任意一个与当前返回的页面URL不同即为跨域。 ● 允许的访问来源：设置允许通过浏览器访问服务器资源的路径。 单个值必须以http://或者https://开头，后边加一个正确的域名或一级泛域名，单个值可以不加端口，也可以指定端口，端口范围：1~65535。最多设置32个值，请以英文逗号分隔，也支持设置通配符“*”。 ● 允许的方法：选择跨域访问时允许的HTTP方法。 支持的方法包括：GET，POST、PUT、DELETE、HEAD、OPTIONS、PATCH。 ● 允许的请求头部：设置允许的跨域资源共享请求标头。 单个值只允许包含大小写字母、数字，不能以下划线（_）和短划线（-）开头或结尾，最长32个字符。最多设置32个值，请以英文逗号分隔。 ● 允许的响应头部：设置允许浏览器、JavaScript脚本访问的响应标头。 单个值只允许包含大小写字母、数字，不能以下划线（_）和短划线（-）开头或结尾，最长32个字符。最多设置32个值，请以英文逗号分隔。 ● 携带凭证：跨域访问时是否允许携带凭证信息。 取值：允许或不允许，默认允许。 ● 浏览器缓存时间：对于预检请求，设置OPTIONS预检请求在浏览器的最大缓存时间。 取值范围：-1~172800，单位：秒。

URL 高级转发策略匹配示例

配置了5个URL高级转发策略，如**表1-27**所示。

表 1-27 URL 高级转发策略匹配示例

请求URL	转发策略	设定的URL	匹配模式	转发策略优先级	转发至后端服务器组
/elb/abc.html	转发策略01	/elb/abc.html	前缀匹配	优先级 1	后端服务器组01
	转发策略02	/elb	前缀匹配	优先级 2	后端服务器组02

请求URL	转发策略	设定的URL	匹配模式	转发策略优先级	转发至后端服务器组
/exa/index.html	转发策略03	/exa[^\s]*	正则匹配	优先级 3	后端服务器组03
	转发策略04	/exa/index.html	正则匹配	优先级 4	后端服务器组04
/mpl/index.html	转发策略05	/mpl/index.html	精确匹配	优先级 5	后端服务器组05

转发情况如下：

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

转发动作的路径支持 URL 的正则表达式示例

转发动作“重定向至URL”和“重写”中的路径由英文字母、数字和特殊字符_~';@^-%#&$.*+?,=!:|\/()[]{}组成，只能由/开头。${path}表示与源路径相同。

转发规则选择URL的正则匹配后，转发动作的路径支持正则表达式替换。

路径替换流程

1. URL匹配：客户端发送请求，并匹配到某一条URL转发规则的正则表达式。URL中支持写入一个或多个正则表达式，支持写入多个()。
2. 路径按照正则表达式的规范提取替换变量：转发动作中的路径通过$1来获取( )中的变量，最多可以获取九个变量至$9。
3. 自由组合出目标路径：获取的变量对路径设置中的$1进行替换，最终拼接成重写或重定向的实际路径。

路径替换示例

当客户端发送请求的路径为/test/ELB/elb/index时，匹配转发规则的转发条件/test/(.*)/(.*)/index，经转发路径/$1/$2提取变量后，最终后端服务器接收到的请求路径为/ELB/elb。

表 1-28 路径支持 URL 的正则表达式替换示例

匹配动作		说明
转发规则：URL	正则匹配	• URL正则匹配条件：/test/(.*)/(.*)/index • 匹配成功的请求URL：/test/ELB/elb/index
转发动作：重写或重定向至URL	路径	• 路径替换条件：/$1/$2 • 提取替换变量 $1：提取出ELB $2：提取出elb • 目标路径：/ELB/elb

1.3.3.4.2 管理高级转发策略

操作场景

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

每条高级转发策略必须包含转发规则和动作。

- 支持的转发规则有：域名、URL、HTTP请求方法、HTTP请求头、查询字符串、网段。详见**转发规则**。
- 支持的转发动作有：转发至后端服务器组、重定向至监听器、重定向至URL、重写、返回固定响应。详见**转发动作**。
- 支持单条转发策略中添加多个转发规则。
- 支持转发策略排序。

约束与限制

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

开启高级转发策略

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要添加转发策略的负载均衡器名称。
5. 在“监听器”页签，单击目标监听器名称。
6. 在监听器“基本信息”页面，单击“开启高级转发策略”。
7. 单击“确认”。

添加高级转发策略

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要添加转发策略的负载均衡器名称。
5. 在“监听器”页签，您可以通过以下两种操作入口，进入监听器的“转发策略”页签。
   - 在目标监听器所在行的“操作”列，单击“添加/编辑转发策略”。
   - 单击目标监听器的名称，并切换到“转发策略”页签。
6. 单击“添加转发策略”按钮，参考**表1-24**和**表1-25**配置参数。
7. 配置完成，单击“保存”。

转发策略排序

一个监听器可以添加多个转发策略，转发策略按照优先级从高到低开始匹配，数值越小优先级越高。

您可以通过排序更改非默认转发策略的优先级，您不能更改默认转发策略的优先级。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要修改转发策略的负载均衡器名称。
5. 切换到监听器页签，单击需要修改转发策略的监听器名称。
6. 切换到“转发策略”页签，单击上方的“排序”。
7. 通过鼠标拖拽转发策略模块来调整转发策略的优先级
8. 单击“保存”。

修改转发策略

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要修改转发策略的负载均衡器名称。
5. 在“监听器”页签，单击需要修改转发策略的监听器名称。
6. 切换到“转发策略”页签，选择需要修改的转发策略，单击“编辑”。
7. 根据界面提示修改参数，单击“保存”。

删除转发策略

用户可以根据实际需要删除已经创建的转发策略。

转发策略删除后无法恢复，请谨慎操作。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要删除转发策略的负载均衡器名称。
5. 在监听器页签，单击需要删除转发策略的监听器名称。
6. 切换到“转发策略”页签，选择需要删除的转发策略，单击“删除”。
7. 在弹出的“删除转发策略”对话框中，单击“确定”。

1.3.3.5 配置 HTTP/HTTPS 头字段

HTTP头字段是指在超文本传输协议（HTTP）的请求和响应消息中的消息头部分。HTTP头部字段可以根据需要自定义，本文介绍可通过HTTP和HTTPS监听器支持的非标准头字段实现的功能特性。

表 1-29 获取类头字段开关

头字段	功能开关	功能说明	独享型负载均衡
X-Forwarded-ELB-IP	获取弹性公网IP	开启**获取弹性公网IP**开关，ELB可通过X-Forwarded-ELB-IP头字段获取负载均衡实例的公网IP地址，传输到后端服务器的报文中。 格式如下(XX.XXX.XX.XXX代表ELB的弹性公网IP)： `X-Forwarded-ELB-IP：XX.XXX.XX.XXX`	√
X-Forwarded-ELB-ID	获取负载均衡实例ID	开启**获取负载均衡实例ID**开关，ELB可通过X-Forwarded-ELB-ID头字段获取负载均衡实例的ID，传输到后端服务器的报文中。	√
X-Forwarded-Port	获取监听器端口号	开启**获取监听器端口号**开关，ELB可通过X-Forwarded-Port头字段获取监听器的端口号，传输到后端服务器的报文中。	√
X-Forwarded-For-Port	获取客户端请求端口号	开启**获取客户端请求端口号**开关，ELB可通过X-Forwarded-For-Port头字段获取客户端请求的端口号，传输到后端服务器的报文中。	√

表 1-30 重写类头字段开关

头字段	功能开关	功能说明	独享型负载均衡
X-Forwarded-Host	重写X-Forwarded-Host	• 开启**重写X-Forwarded-Host**开关：ELB以客户端请求头的Host重写X-Forwarded-Host传递到后端服务器。 • 关闭**重写X-Forwarded-Host**开关：ELB透传客户端的X-Forwarded-Host到后端服务器。	√
X-Forwarded-Proto	重写X-Forwarded-Proto	• 开启**重写X-Forwarded-Proto**开关：ELB以监听器的前端协议重写X-Forwarded-Proto头字段传递到后端服务器。 • 关闭**重写X-Forwarded-Proto**开关：ELB透传客户端的X-Forwarded-Proto到后端服务器。	√
X-Real-IP	重写X-Real-IP	• 开启**重写X-Real-IP**开关：ELB以客户端的源IP地址重写X-Real-IP传递到后端服务器。 • 关闭**重写X-Real-IP**开关：ELB透传客户端的X-Real-IP到后端服务器。	√

说明

- 不同HTTP/HTTPS头字段的发布区域请参考**功能总览**。
- “√”表示负载均衡支持该行对应的请求头；“×”表示负载均衡不支持该行对应的请求头。

添加 HTTP/HTTPS 头字段

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 您可以通过以下两种操作入口，添加HTTP/HTPS监听器请求头。
   - 在“负载均衡器”界面，单击目标负载均衡器名称。在“负载均衡器”界面的“监听器”页签，单击“添加监听器”。
   - 在“负载均衡器”界面，在目标负载均衡器所在行的操作列，单击“添加监听器”。
5. 在“添加监听器”界面，展开高级配置，根据您的业务需求，开启您需要添加HTTP/HTTPS头字段的功能开关。
6. 根据界面提示，完成监听器后续的配置步骤。
7. 确认配置完成，单击“提交”。

修改 HTTP/HTTPS 头字段

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击目标负载均衡器名称。
5. 在“监听器”页签，在目标监听器所在行的操作列，单击“编辑”。
6. 在“编辑监听器”界面，展开高级配置，根据您的业务需求，开启或关闭HTTP/HTTPS头字段的功能开关。
7. 单击“确定”。

1.3.4 管理监听器

操作场景

当您创建完监听器后，您可以根据实际业务需求为监听器配置修改保护、对监听器的配置进行修改、更换监听器的后端服务器组以及删除监听器等操作。

前提条件

- 您已经创建ELB实例，详情请参见**创建独享型负载均衡器**。
- 您已经创建可用的后端服务器组，详情请参见**创建后端服务器组**。
- 您已经创建监听器，详情请参见**监听器概述**。

监听器配置修改保护

您可以对监听器开启修改保护功能，防止因误操作导致监听器的配置被修改或监听器被删除。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要为监听器配置修改保护的负载均衡名称。
5. 在“监听器”页签，单击需要为配置修改保护的监听器名称。
6. 在监听器的“基本信息”页签，单击修改保护右侧的“设置”。
7. 在设置修改保护的弹窗中，开启“修改保护开关”。

说明

如果您需要修改监听器的配置或删除监听器，请先关闭“修改保护”开关。

修改监听器

说明

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

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要修改监听器的负载均衡名称。
5. 您可以通过以下两种操作入口，修改监听器。
   - 在目标监听器所在行的“操作”列，单击“编辑”。
   - 单击目前监听器的名称，进入监听器的“基本信息”页面，单击“编辑监听器”。
6. 在“编辑监听器”页面修改参数，单击“确定”。

修改监听器的超时时间

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

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要修改监听器的负载均衡名称。
5. 切换到“监听器”页签，单击需要配置超时时间的目标监听器名称。
6. 在监听器的“基本信息”页面，单击“编辑监听器”。
7. 在“编辑监听器”页面，单击“高级配置”。
8. 根据需要配置“空闲超时时间”或“请求超时时间”或“响应超时时间”。
9. 单击“确定”。

更换监听器的后端服务器组

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”列表，单击目标监听器所在的负载均衡名称。
5. 选择“监听器”页签，在监听器列表中，单击目标监听器的名称。
6. 在监听器的“基本信息”页签，单击“后端服务器组”区域右侧“更换后端服务器组”。
7. 在弹出的对话框中，单击服务器组名称方框。

   将显示搜索框、所有可选服务器组和“创建后端服务器组”。

   a. 选择已有服务器组，可直接单击目标服务器组名称，也可在搜索框中按名称搜索。
   b. 您也可单击“创建后端服务器组”创建新的后端服务器组。创建完成后单击刷新按钮，在已有服务器组中进行选择。

说明

若创建新的服务器组，后端协议应与监听器的前端协议匹配才可被当前监听器使用。

8. 单击“确定”。

删除监听器

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要删除监听器的负载均衡名称。
5. 在“监听器”页签，需要删除监听器所在行的“操作”列，单击“删除 ”。
6. 在删除监听器的弹窗页面，输入“DELETE”。
7. 单击“确定”。

1.4 后端服务器组

1.4.1 后端服务器组概述

后端服务器组简介

后端服务器组是一个或多个后端服务器的逻辑集合，用于将客户端的流量转发到一个或多个后端服务器，满足用户同时处理海量并发业务的需求。后端服务器可以是云服务器实例、辅助弹性网卡或IP地址。

后端服务器组参与流量转发过程如表1-31：

表 1-31 后端服务器组参与流量转发过程

步骤一	来自客户端的请求先传入负载均衡器，再经由负载均衡器上的监听器转发到后端服务器组。
步骤二	后端服务器组中健康检查正常的后端服务器处理转发的业务请求。
步骤三	实现同时对用户的海量并发业务进行处理，从而提升用户应用系统的可用性。

独享型负载均衡器使用的后端服务器组分为混合类型和IP类型，混合类型支持添加云服务器实例、辅助弹性网卡和IP地址作为后端服务器，IP类型仅支持添加IP地址作为后端服务器。

图1-13展示了不同类型后端服务器组的使用架构，详细的对比说明见表1-32。

图 1-13 后端服务器组使用架构图

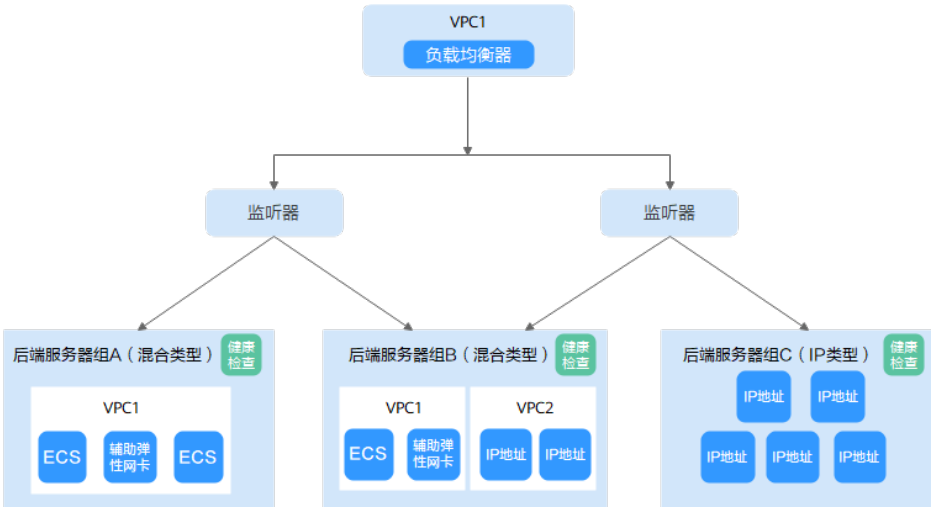


表 1-32 后端服务器组分类及说明

后端服务器组类型	可添加后端服务器分类	举例说明	操作指导
混合类型	• 支持直接添加与负载均衡器同VPC的云服务器实例（ECS和BMS）和辅助弹性网卡作为后端服务器。 • 开启跨VPC后端功能后，也支持添加云上其他VPC和云下数据中心的IP地址作为后端服务器。	如图1-13所示： • 后端服务器组A可添加与负载均衡器在同一虚拟私有云VPC1中的弹性云服务器（ECS）和辅助弹性网卡（Supplementary Network Interface）作为后端云服务器。 • 后端服务器组B中可跨VPC添加VPC2中的IP地址作为后端服务器。	• 添加后端云服务器 • 添加辅助弹性网卡 • 添加跨VPC后端
IP类型	开启跨VPC后端功能后，支持添加云上或云下数据中心的IP地址作为后端服务器。	如图1-13，后端服务器组C可添加IP地址作为后端服务器。	添加跨VPC后端

后端服务器组优势

在负载均衡器的使用中引入后端服务器组有如下优势：

- 通过后端服务器组可以对后端服务器进行统一管理，灵活地添加或者移除后端服务器，降低用户的管理和使用成本。

- 后端服务器组支持**健康检查功能**，可保证流量转发到正常的后端服务器，提升用户业务的可靠性。

后端服务器组关键功能

为保证用户业务的稳定和多样化的流量转发需求，后端服务器组提供了如**表1-33**所示的关键功能可供用户配置。

表 1-33 后端服务器组关键功能

关键功能	功能说明	功能详情
转发模式	根据后端服务器组配置的转发模式，负载均衡将切换后端服务器处理请求流量。 支持“负载均衡”和“主备转发”两种类型。 • 负载均衡：负载均衡器配置的流量分配策略将请求的流量分发至不同的后端服务器。 • 主备转发：当主机健康检查结果正常时，负载均衡将流量转发至主机；当主机健康检查结果异常时，流量将被切换至备机。 **说明** • 仅独享型负载均衡的后端服务器组支持选择转发模式。 • 后端服务器组支持选择转发模式的发布区域请参考**功能总览**中的主备转发模式。	**转发模式介绍（独享型）**。
健康检查	负载均衡器通过健康检查来判断后端服务器是否可用。 如果某个后端服务器健康检查异常，负载均衡器将不会把流量转发给异常后端服务器，从而提升了业务的可靠性。	**健康检查介绍**。
流量分配策略	负载均衡器按照后端服务器组配置的流量分配策略对请求的流量进行分发。	**流量分配策略介绍**。
会话保持	开启会话保持后，负载均衡器将属于同一个会话的请求都转发到固定的后端服务器进行处理，避免了客户端重复登录后端服务器。	**会话保持介绍**。

关键功能	功能说明	功能详情
慢启动	慢启动指负载均衡器向组内新增的后端服务器线性增加请求分配权重的启动模式。 当配置慢启动时间结束，负载均衡向后端服务器发送完整比例的流量请求，实现业务的平滑启动。 **说明** 仅独享型负载均衡支持HTTP和HTTPS类型的后端服务器组开启慢启动功能。	慢启动介绍（独享型）。
全端口转发	开启全端口转发后，后端服务器组添加后端服务器时无需指定后端端口，监听器将按照前端请求端口转发流量至后端服务器对应的端口。 **说明** 仅独享型负载均衡支持TCP、UDP和QUIC类型的后端服务器组开启全端口转发功能。	-

后端服务器组创建指引

后端服务器组独立创建后仅可关联至前端协议与后端协议匹配的监听器使用，监听器与后端服务器组的前端/后端协议匹配关系详见表1-34。

您有多种方式创建后端服务器组，详见表1-35。

表 1-34 前端/后端协议匹配关系

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

表 1-35 后端服务器组创建指引

弹性负载均衡类型	约束与限制	后端服务器组创建方法
独享型负载均衡	支持将一个后端服务器组关联至多个负载均衡实例和监听器使用。 弹性负载均衡实例需归属同一企业项目。	创建后端服务器组。

1.4.2 后端服务器组关键功能

1.4.2.1 健康检查介绍

负载均衡器会定期向后端服务器发送请求以测试其运行状态，这些测试称为健康检查。通过健康检查来判断后端服务器是否可用。

负载均衡器如果判断后端服务器健康检查异常，就不会将流量分发到异常后端服务器，而是分发到健康检查正常的后端服务器，从而提高了业务的可靠性。当异常的后端服务器恢复正常运行后，负载均衡器会将其自动恢复到负载均衡服务中，承载业务流量。

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

健康检查协议

您可以在创建后端服务器组和创建监听器时为后端服务器组配置健康检查，通常，使用默认的健康检查配置即可，也根据业务需要选择不同的健康检查协议。

您也可以在后端服务器组创建后修改健康检查，详情可见**修改健康检查配置**。

后端服务器组的后端协议与支持的健康检查协议存在匹配关系，详情请参见**表1-36**。

表 1-36 后端服务器组支持的健康检查协议（独享型）

后端服务器组的后端协议	健康检查协议
TCP	TCP、HTTP、HTTPS
UDP	UDP
QUIC	UDP
TLS	TCP、HTTP、HTTPS、TLS、GRPC
HTTP	TCP、HTTP、HTTPS、TLS、GRPC
HTTPS	TCP、HTTP、HTTPS、TLS、GRPC

后端服务器组的后端协议	健康检查协议
GRPC	TCP、HTTP、HTTPS、TLS、GRPC

说明

TLS协议与GRPC协议陆续上线中，已发布区域请参见**弹性负载均衡支持TLS协议**和**弹性负载均衡支持GRPC协议**。

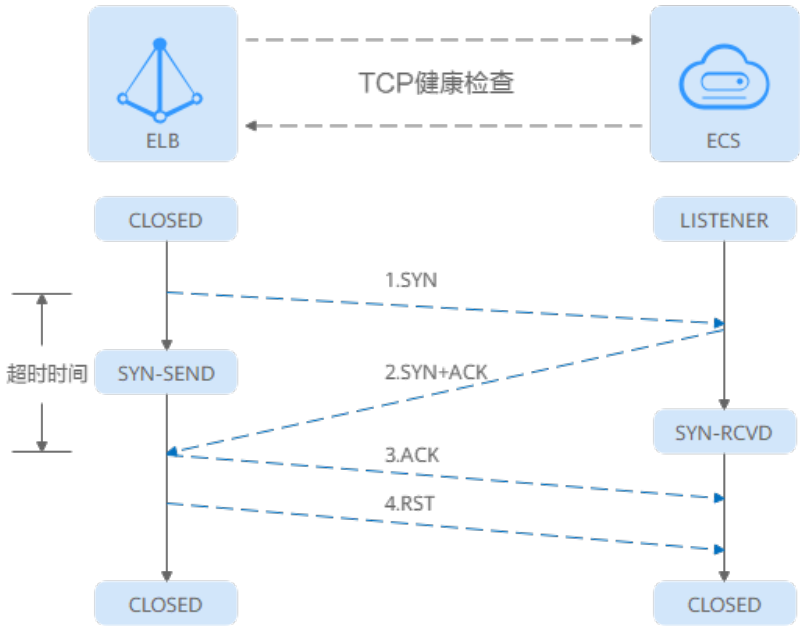
健康检查源 IP

独享型负载均衡器以ELB后端子网内的IP为健康检查源地址，向后端服务器发起健康检查探测请求。为确保健康检查结果正常，请确保后端服务器的安全组规则配置放行ELB后端子网所属网段，详情见**配置后端服务器的安全组**。

TCP 健康检查

对于四层（TCP）和七层（HTTP/HTTPS）后端协议，您可以配置TCP健康检查，通过发起TCP三次握手来获取后端服务器的状态信息，如**图1-14**所示。

图 1-14 TCP 健康检查



TCP健康检查的机制如下：

1. ELB节点根据健康检查配置，向后端服务器（IP+健康检查端口）发送TCP SYN报文。
2. 后端服务器收到请求报文后，如果相应的端口已经被正常监听，则会返回SYN+ACK报文。
   - 如果在超时时间内没有收到后端服务器的SYN+ACK报文，则判定健康检查失败。随后发送RST报文给后端服务器中断TCP连接。

- 如果在超时时间内收到了SYN+ACK报文，则判定健康检查成功，并进一步发送ACK报文给后端服务器。随后发送RST报文给后端服务器中断TCP连接。

须知

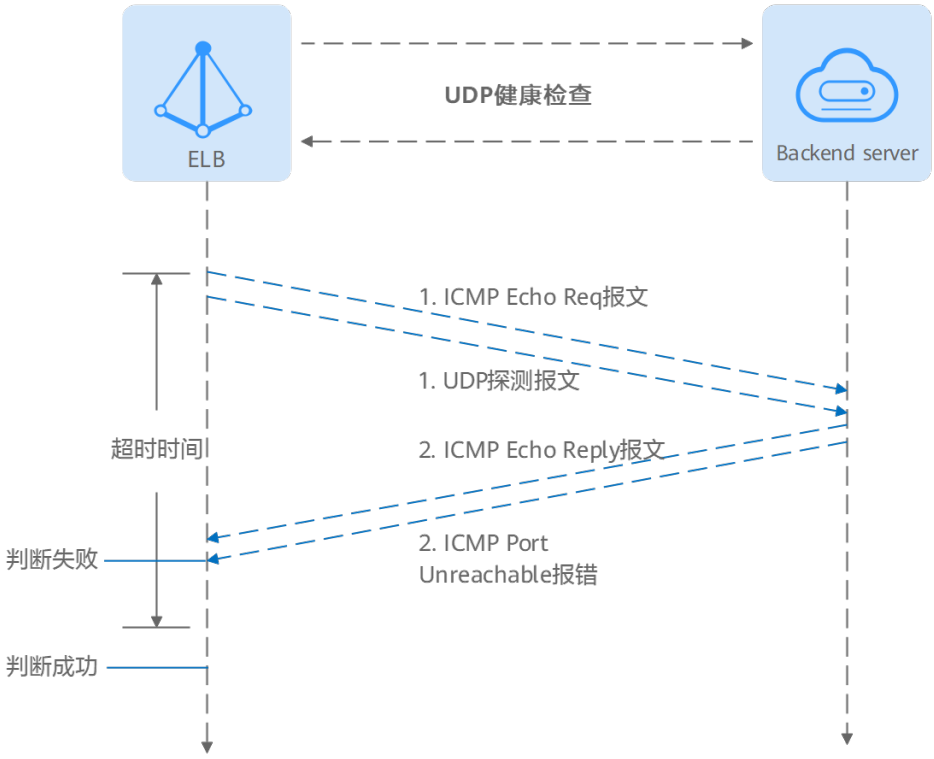
正常的TCP三次握手后，会进行数据传输，但是在健康检查时会发送RST中断建立的TCP连接。该实现方式可能会导致后端服务器中的应用认为TCP连接异常退出，并打印错误信息，如“Connection reset by peer”。解决方案如下：

- 采用**HTTP健康检查**。
- 后端服务器忽略健康检查的连接错误。

UDP 健康检查

对于四层（UDP）后端协议，默认配置UDP健康检查，通过发送UDP探测报文获取后端服务器的状态信息，如**图1-15**所示。

图 1-15 UDP 健康检查



UDP健康检查机制如下：

1. 四层ELB节点根据健康检查配置，向后端服务器发送ICMP Echo Request报文和UDP探测报文。
2. 如果在超时时间内收到ICMP Echo Reply报文，且没有收到后端服务器返回的ICMP Port Unreachable报文，则判定健康检查成功。否则，判定健康检查失败。

说明

在大并发场景下，UDP协议的健康检查结果可能存在服务真实状态不一致的问题：

如果后端服务器是Linux服务器，由于Linux的防ICMP攻击保护机制，会限制后端服务器发送ICMP的速度。此时如果后端服务已经出现异常，但由于无法返回Port Unreachable报文，会导致负载均衡实例收不到ICMP应答进行判定健康检查成功，最终导致后端服务的真实状态与健康检查结果不一致。

HTTP 健康检查

对于四层（TCP）和七层（HTTP/HTTPS）后端协议，您可以配置HTTP健康检查，通过HTTP GET请求来获取状态信息。检查原理如图1-16所示。

图 1-16 HTTP 健康检查

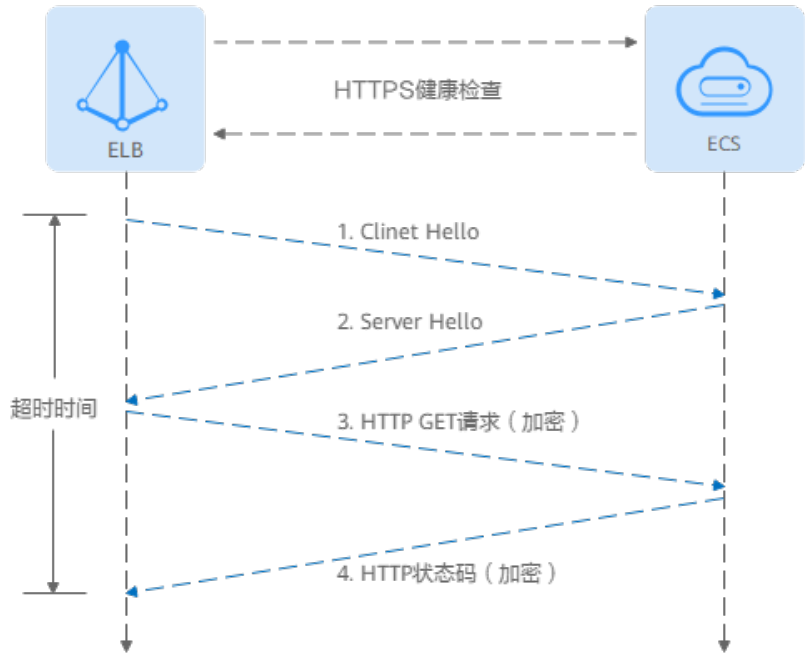
HTTP健康检查机制如下：

1. ELB节点根据健康检查配置，向后端服务器（IP+端口+检查路径）发出HTTP GET请求（可以选择设置域名）。
2. 后端服务器收到请求后，根据服务的情况返回相应的HTTP状态码。
   - 如果七层ELB节点在响应超时时间内收到了后端服务器的响应，将HTTP状态码与预置的状态码进行对比，如果匹配则认为健康检查成功，后端服务器运行正常。
   - 如果七层ELB节点在响应超时时间内没有收到后端服务器的响应，则判定健康检查失败。

HTTPS 健康检查

对于四层（TCP）和七层（HTTP/HTTPS）后端协议，您也可以配置HTTPS健康检查。HTTPS健康检查首先通过TLS握手建立SSL连接，再通过发送加密的HTTP GET请求来获取后端服务器的状态信息。检查原理如图1-17所示。

图 1-17 HTTPS 健康检查



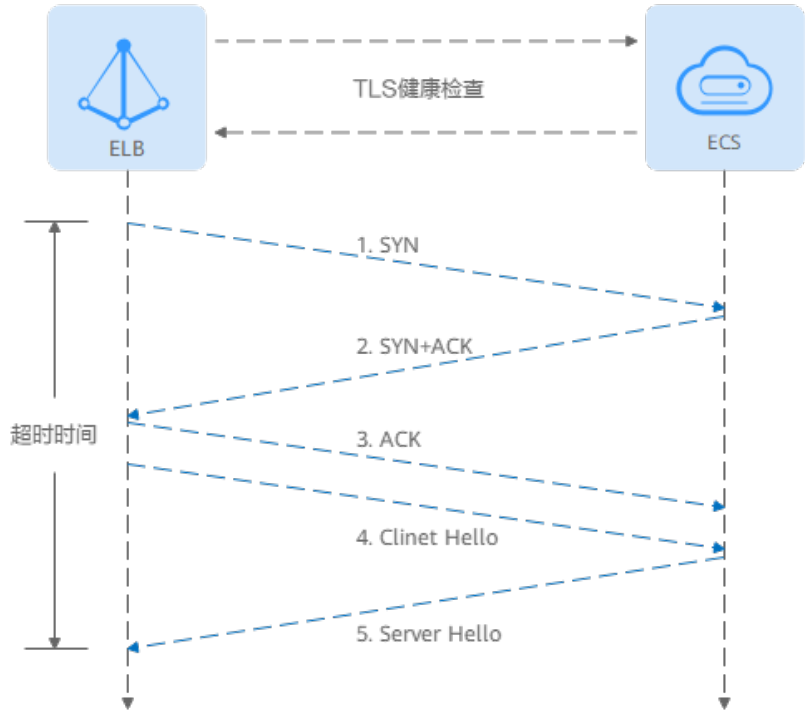
HTTPS健康检查机制如下：

1. ELB节点向后端服务器发送Client Hello请求，与后端服务器建立SSL连接。
2. ELB节点收到后端服务器返回Server Hello报文后，根据健康检查配置，向后端服务器（IP+端口+检查路径）发出加密的HTTP GET请求（可以选择设置域名）。
3. 后端服务器收到请求后，根据服务的情况返回相应的HTTP状态码。
   - 如果七层ELB节点在响应超时时间内收到了后端服务器的响应，将HTTP状态码与预置的状态码进行对比，如果匹配则认为健康检查成功，后端服务器运行正常。
   - 如果七层ELB节点在响应超时时间内没有收到后端服务器的响应，则判定健康检查失败。

TLS 健康检查

对于HTTP、HTTPS和TLS后端协议，您可以配置TLS健康检查，通过TLS 握手，发送Client Hello，解析服务端发送的Server Hello来获取后端服务器的状态。

图 1-18 TLS 健康检查



TLS健康检查的机制如下：

1. ELB节点根据健康检查配置，向后端服务器（IP+健康检查端口）发送TCP SYN报文。
   - 如果在超时时间内没有收到SYN+ACK报文，则判定健康检查失败。
   - 如果在超时时间内收到了SYN+ACK报文，则向后端服务器发送会发送Client Hello（SSL协商），协商的版本号包括了TLSv1.0、TLSv1.1、TLSv1.2、TLSv1.3。
2. 如果在超时时间内收到后端服务器返回的Server Hello报文，则判定健康检查成功。否则，判定健康检查失败。

GRPC 健康检查

图 1-19 GRPC 健康检查

GRPC健康检查机制如下：

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

3. ELB通过读取HTTP/2头中的grpc-status的值作为返回的GRPC状态码。
   - 如果七层ELB节点在响应超时时间内收到了后端服务器的响应，将返回的GRPC状态码与自定义的健康检查返回码进行对比，如果匹配则认为健康检查成功，后端服务器运行正常。
   - 如果七层ELB节点在响应超时时间内没有收到后端服务器的响应，则判定健康检查失败。

健康检查时间窗

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

健康检查时间窗由**表1-37**中的三个因素决定：

表 1-37 健康检查时间窗的影响因素

影响因素	说明
检查间隔	每隔多久进行一次健康检查。
超时时间	等待服务器返回健康检查的时间。
健康检查阈值	判定健康检查结果正常或异常时，所需的健康检查连续成功或失败的次数。

健康检查时间窗的计算方法如下：

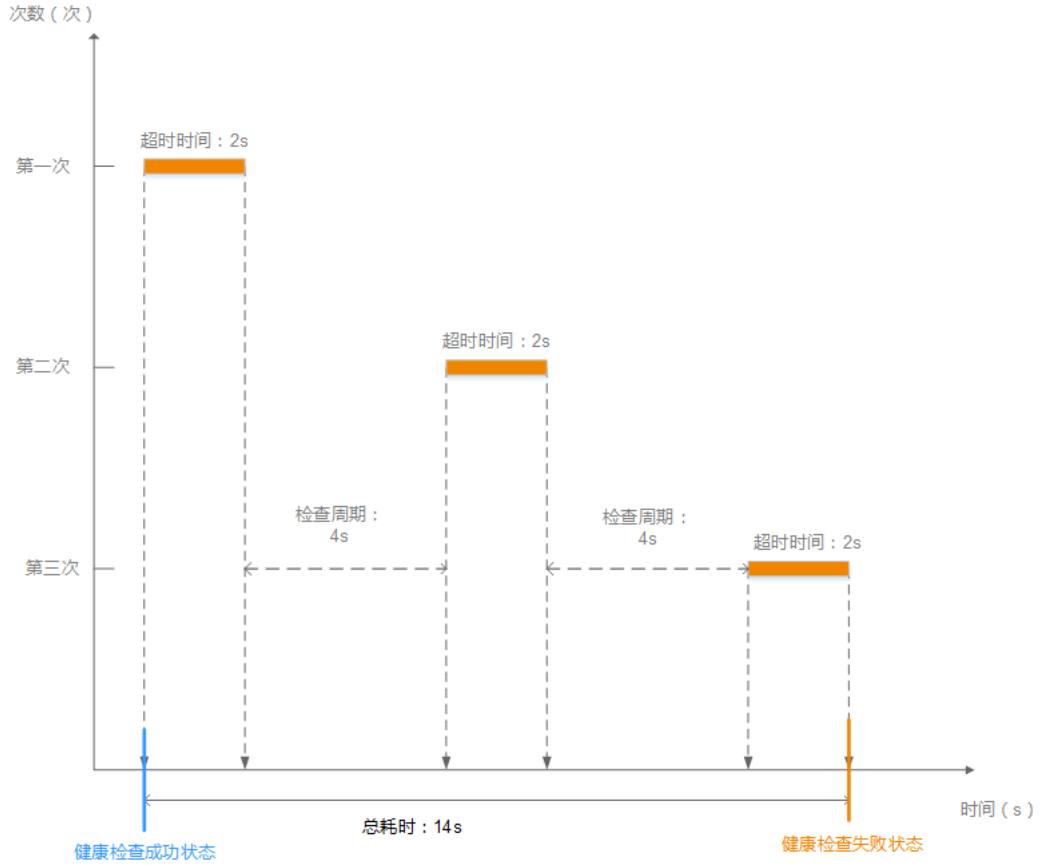
- 健康检查成功时间窗 = 超时时间×健康检查正常阈值 + 检查间隔×(健康检查正常阈值-1)
- 健康检查失败时间窗 = 超时时间×健康检查异常阈值 + 检查间隔×(健康检查异常阈值-1)

如**图1-20**所示：

- 检查间隔：4s
- 超时时间：2s
- 健康检查异常阈值：3次

健康检查检测到后端服务器从正常到失败状态，健康检查失败时间窗 = 超时时间×健康检查异常阈值+检查间隔×(健康检查异常阈值-1) = 2 x 3+4 x (3-1) = 14s。

图 1-20 健康检查失败时间窗



健康检查异常排查

如果您的健康检查异常，排查方法请参考**健康检查异常如何排查**。

1.4.2.2 流量分配策略介绍

分配策略类型总览

负载均衡会根据配置的流量分配策略，将来自客户端的请求按照对应的流量分配策略转发至相应的后端服务器。

弹性负载均衡支持加权轮询算法、加权最小连接、源IP算法、连接ID算法等多种分配策略，用于支持不同的业务场景。

本文列出弹性负载均衡支持的所有分配策略，不同类型的负载均衡器和后端服务器组支持的流量分配策略不同。

表 1-38 流量分配策略对比

分配策略类型	描述
加权轮询算法	根据组内后端服务器设置的权重，依次将请求分发给不同的服务器。

分配策略类型	描述
加权最少连接	将请求分发给（当前连接/权重）比值最小的后端服务器进行处理。
一致性哈希算法 • 源IP算法 • 连接ID算法	对请求的特定字段进行一致性哈希计算，并根据计算的哈希值将请求均匀地分配到后端服务器中。相同哈希值的请求，将会被分配到相同的后端服务器，即使后端服务器组中的后端服务器个数在发生变化。 • 源IP算法：根据请求的源IP地址进行哈希计算，源IP相同的请求会被分配到同一台后端服务器。 • 连接ID算法：根据QUIC协议请求的ID进行哈希计算，相同QUIC ID连接上的请求会被分配到同一台后端服务器。

分配策略详情

独享型负载均衡支持加权轮询算法、加权最少连接、源IP算法、连接ID算法。

加权轮询算法

图1-21展示弹性负载均衡器使用加权轮询算法的流量分发流程。假设可用区内有2台权重相同的后端服务器，负载均衡器节点会将50%的客户端流量分发到其可用区中的每一台后端服务器。

图 1-21 加权轮询算法流量分发

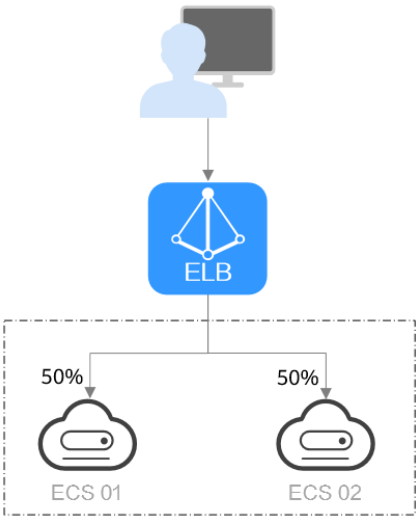


表 1-39 加权轮询算法说明

概述	加权轮询算法根据组内后端服务器设置的权重，依次将请求分发给不同的服务器。权重大的后端服务器被分配的概率高，相同权重的服务器处理相同数目的连接数。

推荐场景	加权轮询算法常用于短连接服务，例如HTTP等服务。 • 灵活负载：当对后端服务器的负载分配有更精细的要求时，可以通过设置不同的权重来实现对服务器的灵活调度，使得性能较好的服务器能够处理更多的请求。 • 动态负载：当后端服务器的性能和负载情况经常发生变化时，可以通过动态调整权重来适应不同的场景，实现负载均衡。
缺点	• 加权轮询算法需要配置每个后端服务器的权重，对于有大量后端服务器或频繁变动的场景，运维工作量较大。 • 权重设置不准确可能会导致负载不均衡的情况，需要根据后端服务器的实际性能进行调整。

加权最少连接

图1-22展示弹性负载均衡器使用加权最少连接算法的流量分发流程。假设可用区内有2台权重相同的后端服务器，ECS 01已有100个连接，ECS 02已有50个连接，则新的连接会优先分配到ECS 02上。

图 1-22 加权最少连接算法流量分发

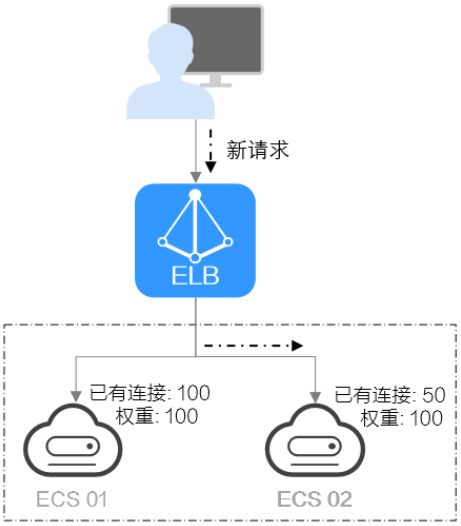


表 1-40 加权最少连接说明

概述	最少连接是通过当前活跃的连接数来评估服务器负载情况的一种动态负载均衡算法。加权最少连接就是在最少连接数的基础上，根据服务器的不同处理能力，给每个服务器分配不同的权重，使其能够接受相应权值数的服务请求。

推荐场景	加权最少连接常用于长连接服务，例如数据库连接等服务。 • 灵活负载：当后端服务器的性能差异较大时，同时考虑后端服务器的连接数和权重来进行负载，可以更精确地将请求分配到后端服务器上，避免出现过载或空闲的情况。 • 动态负载：当后端服务器的连接数和负载情况经常发生变化时，可以通过实时监控连接数变化进行动态的负载调整。 • 更高稳定负载：对于需要高稳定性的业务场景，加权最小连接算法可以降低后端服务器的峰值负载，提高业务的稳定性和可靠性。
缺点	• 加权最小连接算法的实现更复杂：需要实时监控负载均衡器与后端服务器之间的连接数变化。 • 对后端服务器的连接数存在依赖：算法依赖于准确获取负载均衡服务和后端服务器的连接数，如果获取不准确或监控不及时，可能导致负载分配不均衡。同时由于算法只能统计到负载均衡器与后端服务器之间的连接，后端服务器整体连接数无法获取，因此对于后端服务器挂载到多个弹性负载均衡的场景，也可能导致负载分配不均衡。 • 新增后端服务器时可能导致过载：如果已有的连接数过大，大量的新建连接会被分配到新加入的后端服务器上，可能会导致新加入的后端服务器瞬间过载影响系统稳定性。

源 IP 算法

图1-23展示弹性负载均衡器使用源IP算法的流量分发流程。假设可用区内有2台权重相同的后端服务器，ECS 01已经处理了一个IP-A的请求，则IP-A新发起的请求会自动分配到ECS 01上。

图 1-23 源 IP 算法流量分发

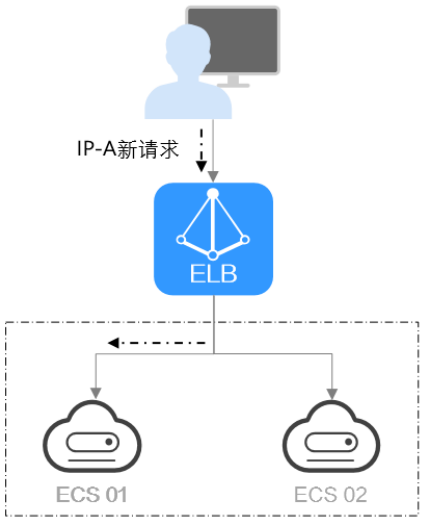


表 1-41 源 IP 算法说明

概述	根据请求的源IP地址进行一致性哈希计算，源IP地址相同的请求会被分配到同一台后端服务器。
推荐场景	源IP算法常用于需要保持用户状态或会话的应用。 • 基于源IP的会话保持：源IP算法可以确保源IP相同的请求具有相当的哈希值并被分配到同一台后端服务器上，从而实现会话保持。 • 保持数据一致：一致性哈希算法将相同哈希值的请求调度到相同后端服务器上，保证多次请求数据的一致性。 • 均衡性要求较高：一致性哈希算法能够提供相对均衡的负载分配效果，减少后端服务器的负载差异。
缺点	• 后端服务器数量变动可能导致不均衡：一致性哈希算法在后端服务器数量变动时会尽力保障请求的一致性，部分请求会重新分配。当后端服务器数量较少时，重新分配过程中有可能导致负载不均衡的情况发生。 • 扩展复杂性增加：由于一致性哈希算法将请求根据哈希因子进行哈希计算，当后端服务器数量变化时，会导致一部分请求需要重新分配，这会引入一定的复杂性。

连接 ID 算法

图1-24展示弹性负载均衡器使用连接ID算法的流量分发流程。假设可用区内有2台权重相同的后端服务器，ECS 01已经处理了一个客户端A的请求，则客户端A上新发起的请求会自动分配到ECS 01。

图 1-24 连接 ID 算法流量分发

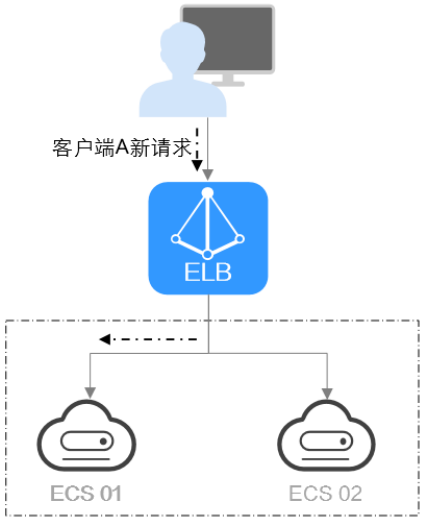


表 1-42 连接 ID 算法说明

概述	根据QUIC 协议请求的QUIC ID进行哈希计算，相同QUIC连接上的请求会被分配到同一台后端服务器。QUIC ID是QUIC连接的唯一标识符，连接ID算法可以实现基于连接级别的负载均衡。 仅QUIC协议的后端服务器组支持连接ID算法。
推荐场景	连接ID算法常用于实现连接级别负载均衡的应用。 ● 基于QUIC连接的会话保持：连接IP算法可以确保源相同QUIC连接上的请求具有相当的哈希值并被分配到同一台后端服务器上，从而实现会话保持。 ● 保持数据一致：一致性哈希算法将相同哈希值的请求调度到相同后端服务器上，保证多次请求数据的一致性。 ● 均衡性要求较高：一致性哈希算法能够提供相对均衡的负载分配效果，减少后端服务器的负载差异。
缺点	● 后端服务器数量变动可能导致不均衡：一致性哈希算法在后端服务器数量变动时会尽力保障请求的一致性，部分请求会重新分配。当后端服务器数量较少时，重新分配过程中有可能导致负载不均衡的情况发生。 ● 扩展复杂性增加：由于一致性哈希算法将请求根据哈希因子进行哈希计算，当后端服务器数量变化时，会导致一部分请求需要重新分配，这会引入一定的复杂性。

1.4.2.3 会话保持介绍

会话保持，指负载均衡器可以识别客户与服务器之间交互过程的关联性，在实现负载均衡的同时，保持将其他相关联的访问请求分配到同一台服务器上。

会话保持有什么作用呢，举例说明如下：如果有一个用户在服务器甲登录了，访问请求被分配到服务器甲，在很短的时间，这个用户又发出了一个请求，如果没有会话保持功能的话，这个用户的请求很有可能会被分配到服务器乙去，这个时候在服务器乙上是没有登录的，所以需要重新登录。如果配置了会话保持功能，上述一系列的操作过程将由同一台服务器完成，避免被负载均衡器分配到不同的服务器上，提高访问效率。

四层会话保持和七层会话保持的区别

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

表 1-43 四层会话保持和七层会话保持的区别

类型	说明	支持的会话保持类型	会话保持时间	会话保持失效的场景
四层会话保持	当使用的协议为TCP或UDP时，即为四层会话保持。	**源IP地址**：基于源IP地址的简单会话保持，将请求的源IP地址作为散列键（HashKey），从静态分配的散列表中找出对应的服务器。即来自同一IP地址的访问请求会被转发到同一台后端服务器上进行处理。	• 默认时间：20分钟 • 最长时间：60分钟 • 取值范围：1-60分钟	• 客户端的源IP地址发生变化。 • 客户端访问请求超过会话保持时间。
七层会话保持	当使用的协议为HTTP或HTTPS时，即为七层会话保持。	• **负载均衡器cookie**：负载均衡器会根据客户端第一个请求生成一个cookie，后续所有包含这个cookie值的请求都会由同一个后端服务器处理。 • **应用程序cookie**：该选项依赖于后端应用。后端应用生成一个cookie值，后续所有包含这个cookie值的请求都会由同一个后端服务器处理。	• 默认时间：20分钟 • 最长时间：1440分钟 • 取值范围：1-1440分钟	• 如果客户端发送请求未附带cookie，则会话保持无法生效。 • 客户端访问请求超过会话保持时间。

说明

- 当**分配策略类型**选择“源IP算法”时，四层和七层会话已支持基于源IP地址的会话保持。
- 当**分配策略类型**选择“加权轮询算法”或“加权最少连接”时，才可配置会话保持。

约束与限制

- 如果您需要从**云专线**、**VPN**、**云连接**访问ELB，请您使用源IP负载均衡算法代替会话保持功能。
- 独享型负载均衡器支持源IP地址、负载均衡器cookie、应用程序cookie的会话保持类型。

说明

- 独享型负载均衡器支持应用程序cookie的会话保持陆续上线中，已发布区域请参见**独享型负载均衡支持应用程序cookie**。
- 对于HTTP、HTTPS类型的后端服务器，变更会话保持的状态可能会导致监听器与后端服务器组的访问出现秒级中断。
- 如果您开启了会话保持功能，那么有可能会造成后端服务器的访问量不均衡。如果出现了访问不均衡的情况，建议您暂时关闭会话保持功能，再观察是否依然存在访问不均衡的情况。

1.4.2.4 转发模式介绍（独享型）

负载均衡流量在后端服务器组的转发模式，支持“负载均衡”和“主备转发”两种类型。

说明

- 仅独享型负载均衡的后端服务器组支持选择转发模式。
- 后端服务器组支持选择转发模式的发布区域请参考**功能总览**中的主备转发模式。

表 1-44 后端服务器组的转发模式说明

转发模式	功能说明	推荐场景
负载均衡	后端服务器组内可以添加多个后端服务器。 负载均衡器按照后端服务器组配置的流量分配策略将请求的流量分发至不同的后端服务器。	按照监听器配置的转发策略将不同的请求转发到不同的后端服务器。
主备转发	必须向其中添加两个后端服务器，一个为主服务器，一个为备服务器。 主备转发的实现依赖健康检查的结果。当主机健康检查结果正常时，负载均衡将流量转发至主机；当主机健康检查结果异常时，流量将被切换至备机。	使用主备转发的后端服务器组功能实现业务的容灾。

1.4.2.5 慢启动介绍（独享型）

慢启动指负载均衡器向组内新增的后端服务器线性增加请求分配权重，直到配置的慢启动时间结束，负载均衡器向后端服务器正常发送完请求的启动模式。更多后端服务器分配权重设置，请见**后端服务器的权重**。

慢启动能够实现业务的平滑启动，完美避免业务抖动问题。

说明

仅独享型负载均衡支持HTTP和HTTPS类型的后端服务器组开启慢启动功能。

后端服务器在以下两种状态会退出慢启动状态。

- 到达已设定的慢启动时间。
- 慢启动时间内后端服务器变为异常。

约束与限制

- 仅在流量分配策略使用加权轮询算法时生效。
- 慢启动仅对新增后端服务器生效，后端服务器组首次添加后端服务器时慢启动不生效。
- 后端服务器的慢启动结束之后，不会再次进入慢启动模式。
- 在健康检查开启时，后端服务器健康检查结果正常后慢启动生效。
- 在健康检查关闭时，慢启动立即生效。

1.4.3 创建后端服务器组

操作场景

负载均衡实例的监听器绑定后端服务器组后，才能正常转发访问请求。

独享型负载均衡支持同一个后端服务器组绑定在多个负载均衡实例的监听器上。

您可通过三种方式为负载均衡实例创建后端服务器组，详见**表1-45**。

表 1-45 创建后端服务器组（独享型）指引

创建场景	创建步骤
独立创建后端服务器组后关联至负载均衡实例使用	**操作步骤**。
添加监听器时，选择“新创建”后端服务器组。	您可根据使用需求添加不同协议的监听器，详情见**监听器概述**。 具体添加步骤如下： • **添加TCP监听器**。 • **添加UDP监听器**。 • **添加HTTP监听器**。 • **添加HTTPS监听器**。 • **添加TLS监听器**
更换监听器的后端服务器组时，选择“创建后端服务器组”。	**更换后端服务器组**。

约束与限制

后端服务器组独立创建后仅可关联至前端协议与后端协议匹配的监听器使用，协议匹配关系详见**表1-46**。

表 1-46 前端/后端协议匹配关系

监听器的前端协议	后端服务器组的后端协议
TCP	TCP

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

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 弹性负载均衡 > 后端服务器组”。
5. 在“后端服务器组”界面，单击页面右上角“创建后端服务器组”按钮。
6. 配置后端分配策略，参数详情请参见**表1-47**。

表 1-47 配置后端分配策略参数说明

参数	说明
负载均衡类型	可使用该后端服务器组的负载均衡实例类型，请选择独享型。
所属负载均衡器	使用该后端服务器组的负载均衡实例。 您可在创建后端服务器时将后端服务器组关联至已有独享型负载均衡实例，也可创建后再进行关联。 • 暂不关联 • 关联已有
转发模式	负载均衡流量转发模式，支持“负载均衡”类型和“主备转发”两种类型。 • 负载均衡：属于普通后端服务器组，里面可以添加多个后端服务器，扩展业务的服务能力。 • 主备转发：必须同时向其中添加后端服务器，且只能添加两个后端服务器，一个为主服务器，一个为备服务器。当主服务器故障时，流量将转发至备服务器，提升业务的可靠性。 **说明** 该特性陆续上线中，已发布区域请参见**主备转发模式**。

参数	说明
服务器组类型	指定后端服务器组的类型。 • 混合类型：既支持按照弹性云服务器和辅助弹性网卡实例添加后端服务器，也支持开启跨VPC后端功能后按照IP地址添加后端服务器。 混合类型一定需要指定虚拟私有云，且后端服务器组绑定的是该虚拟私有云下的负载均衡。 • IP类型：按照IP地址添加后端服务器。 IP类型必须开启跨VPC后端功能才能添加后端服务器。 **说明** 该特性陆续上线中，已发布区域请参见**后端服务器组支持选型**。
名称	待创建的后端服务器组的名称。
虚拟私有云	如果“服务器组类型”选择了“混合类型”，则该项是必选参数。 后端服务器组所属的VPC，后端服务器组可被该虚拟私有云下的负载均衡器关联使用。 您可以选择使用已有的虚拟私有云，也可以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》**。 **说明** 该特性陆续上线中，已发布区域请参见**后端服务器组支持选型**。
后端协议	后端云服务器自身提供的网络服务的协议。 • 负载均衡模式下，支持选择的协议有：HTTP、HTTPS、GRPC、TCP、UDP、TLS、QUIC。 • 主备转发模式下，支持选择的协议有：TCP、UDP、TLS、QUIC。
全端口转发	开启全端口转发后，后端服务器组添加后端服务器时无需指定后端端口，监听器将按照前端请求端口转发流量至后端服务器对应的端口。 全端口转发功能开启后不支持关闭。 **说明** 该功能陆续上线中，已发布区域请参见**四层协议全端口监听和转发**。 **说明** 仅独享型负载均衡支持TCP、UDP和QUIC类型的后端服务器组开启全端口转发功能。

参数	说明
分配策略类型	负载均衡采用的算法。 • 加权轮询算法：根据后端服务器的权重，按顺序依次将请求分发给不同的服务器，权重大的后端服务器被分配的概率高。 • 加权最少连接：加权最少连接是在最少连接数的基础上，根据服务器的不同处理能力，给每个服务器分配不同的权重，使其能够接受相应权值数的服务请求。 • 源IP算法：对不同源IP的访问进行负载分发，同时使得同一个客户端IP的请求始终被派发至某特定的服务器。 • 连接ID算法：当后端协议选择QUIC时，支持连接ID算法。对不同连接ID的访问进行负载分发，同时使得同一个连接ID的请求始终被派发至某特定的服务器。 更多关于分配策略的信息，请参见**流量分配策略介绍**。
会话保持	仅分配策略类型选择加权轮询算法、加权最少连接或连接ID算法时支持开启会话保持。 开启会话保持后，弹性负载均衡将属于同一个会话的请求都转发到同一个后端服务器进行处理。 更多关于会话保持的信息，请参见**会话保持介绍**。 **说明** TLS协议的后端服务器组不支持设置会话保持。
会话保持类型	如果“会话保持”功能开启，则该项是必选参数。 选择会话保持的类型： • **源IP地址：**基于源IP地址的简单会话保持，将请求的源IP地址作为散列键（HashKey），从静态分配的散列表中找出对应的服务器。即来自同一IP地址的访问请求会转发到同一台后端服务器上进行处理。 • **负载均衡器cookie：**负载均衡器会根据客户端第一个请求生成一个cookie，后续所有包含这个cookie值的请求都会由同一个后端服务器处理。 • **应用程序cookie：**该选项依赖于后端应用。后端应用生成一个cookie值，后续所有包含这个cookie值的请求都会由同一个后端服务器处理。 **说明** • 当后端协议选择TCP/UDP/QUIC时，支持源IP地址类型。 • 当后端协议选择HTTP/HTTPS/GRPC时，支持负载均衡器cookie和应用程序cookie。
会话保持时间（分钟）	如果“会话保持”功能开启，则该项是必填参数。 • 四层会话保持的时间取值范围为1~60分钟。 • 七层会话保持的时间取值范围为1~1440分钟。

参数	说明
慢启动	如果“分配策略类型”选择“加权轮询算法”，则该项是可选参数。 慢启动指负载均衡器向组内新增的后端服务器线性增加请求分配权重的启动模式。 当配置慢启动时间结束，负载均衡向后端服务器发送完整比例的流量请求，实现业务的平滑启动。 **说明** 仅独享型负载均衡支持HTTP/HTTPS/GRPC类型的后端服务器组开启慢启动功能。 更多关于慢启动的信息，请参见**慢启动介绍（独享型）**。
慢启动时间（秒）	如果“慢启动”功能开启，则该项是必填参数。 慢启动开启后需添加的慢启动时间。
延迟注销	如果后端协议为TCP/UDP/QUIC协议时，默认开启延迟注销功能。 开启延迟注销功能后，负载均衡器停止向移除的后端云服务器或者健康检查失败的后端云服务器发送新的请求，保持现有连接在延迟注销时间内正常传输。 **说明** 该功能陆续上线中，已发布区域请参见**延迟注销**。
延迟注销时间（秒）	如果“延迟注销”功能开启，则该项是必填参数。 负载均衡器与后端服务器的现有连接在延迟注销时间内正常传输，超过延迟注销时间后全部断开。 支持设置的范围为10~4000秒，默认值为300秒。
描述	后端服务器组的描述

7. 单击“下一步”，添加后端服务器并配置健康检查。

   独享型后端服务器组支持添加云服务器、跨VPC后端和辅助弹性网卡作为后端服务器，详情可参见**后端服务器概述**。

   配置健康检查参数请参见**表1-48**。更多关于健康检查的信息，请参见**健康检查介绍**。

   表 1-48 配置健康检查参数说明

参数	说明
是否开启	开启或者关闭健康检查。 如果开启健康检查，您可单击“参数设置”设置健康检查的参数。

参数	说明
健康检查协议	健康检查请求的协议类型。 ● 支持选择TCP、HTTP、HTTPS、TLS、GRPC协议。 ● 当后端协议选择UDP和QUIC协议，健康检查协议默认为UDP且不可修改。 **说明** TLS协议和GRPC协议陆续上线中，已发布区域请参见**功能总览**。
健康检查域名	如果健康检查协议选择HTTP/HTTPS/GRPC协议，则该项是必选参数。 健康检查的请求域名。 ● 默认使用后端服务器的内网IP为域名。 ● 您也可选择指定特定域名，特定域名只能由字母，数字，中划线组成，中划线不能在开头或末尾，至少包含两个字符串，单个字符串不能超过63个字符，字符串间以点分割，且总长度不超过100个字符。
健康检查端口	健康检查端口号，取值范围[1，65535]，为可选参数。 **说明** 默认使用后端云服务器的业务端口进行健康检查。指定特定端口后，使用指定的端口进行健康检查。
健康检查路径	如果健康检查协议选择HTTP/HTTPS/GRPC协议，则该项是必填参数。 指定健康检查的URL地址。检查路径只能以/开头，长度范围[1-80]。 支持使用英文字母、数字和‘-’、‘/’、‘.’、‘?’、‘#’、‘%’、‘&’以及扩展字符集_;~!（）*[]@$^:',+。
检查间隔（秒）	每次健康检查响应的最大间隔时间。 取值范围[1-50]。
超时时间（秒）	每次健康检查响应的最大超时时间。取值范围[1-50]。
健康检查正常阈值	表示判定后端服务器为正常状态时，所需的连续健康检查成功次数，取值范围[1-10]。
健康检查异常阈值	表示判定后端服务器为异常状态时，所需的连续健康检查失败次数，取值范围[1-10]。

参数	说明
健康检查返回码	如果健康检查协议选择HTTP/HTTPS/GRPC协议，则该项是必填参数。 自定义健康检查返回的状态码，仅当健康检查请求成功且返回指定状态码时判定后端服务器状态正常。 可输入支持状态码范围内不重复的单个数字或正序的数字区间，如0-10，200-300。多个HTTP状态码请输入回车键隔开，最多支持输入5个。 ● 检查协议为HTTP/HTTPS时，状态码范围：200-599。 ● 检查协议为GRPC时，状态码范围：0-99。 **说明** 支持设置健康检查返回码的功能陆续上线中，请以控制台实际为准。

8. 单击“下一步”。
9. 确认配置无误后，单击“立即创建”。

后续操作

创建后端服务器组后，您可通过两种方式将后端服务器组关联到独享型负载均衡实例的监听器上使用，详见**表1-45**。

1.4.4 修改后端服务器组配置

1.4.4.1 配置后端服务器组修改保护

操作场景

您可以对后端服务器组开启修改保护功能，防止因误操作导致后端服务器组的配置被修改或后端服务器组被删除。

约束与限制

后端服务器组开始修改保护后，用户将不能执行以下操作：

- 修改后端服务器组配置的基本信息。
- 为后端服务器组配置健康检查。
- 为后端服务器组添加后端服务器。
- 删除后端服务器组及其所关联资源。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。

3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 弹性负载均衡 > 后端服务器组”。
5. 在后端服务器组界面，单击需要配置修改保护的后端服务器组名称。
6. 在后端服务器组的“基本信息”页签下，单击修改保护右侧的“设置”。
7. 在设置修改保护弹窗中，开启“修改保护”开关。
8. 单击“确定”。

说明

如果您需要修改后端服务器组的配置或删除后端服务器组，请先关闭“修改保护”开关。

1.4.4.2 修改后端服务器组配置场景说明

后端服务器组创建后，用户可根据使用需求修改后端服务器组的健康检查配置和基本信息。

健康检查

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

健康检查功能详情参见**健康检查介绍**。

修改健康检查步骤详情见**修改健康检查配置**。

后端服务器组的基本信息

选定目标后端服务器后，可对以下基本信息进行修改，详情见**表1-49**。

表 1-49 支持修改的后端服务器组信息

参数	修改场景说明
名称	用户可自定义后端服务器组的名称。 修改名称步骤详情见**修改流量分配策略配置**。
分配策略类型	用户可根据使用需求修改后端服务器组的流量分配策略。 后端服务器组根据配置的流量分配策略转发流量到不同的后端服务器。 流量分配策略详情参见**流量分配策略介绍**。 修改流量分配策略步骤详情见**修改流量分配策略配置**。

参数	修改场景说明
会话保持	用户可根据使用需求开启或关闭会话保持。 当用户开启了会话保持功能后，会话保持可以使来自同一客户端的请求被转发到同一台后端服务器上，客户端的请求将无需重复登录后端服务器。 开启了会话保持功能，也可能会造成后端服务器的访问量不均衡，此时建议您暂时关闭会话保持功能，再观察是否依然存在访问不均衡的情况。 会话保持功能详情参见**会话保持介绍**。 修改会话保持步骤详情见**修改会话保持配置**。
慢启动	用户可根据使用需求开启或关闭慢启动。 慢启动能够实现业务的平滑启动，完美避免业务抖动问题。建议用户在添加后端服务器前开启慢启动。 慢启动功能详情参见**慢启动介绍（独享型）**。 修改慢启动步骤详情见**修改慢启动配置**。
描述	用户可自定义对目标后端服务器组的描述。 修改描述步骤详情见**修改流量分配策略配置**。

1.4.4.3 修改健康检查配置

操作场景

本章节指导用户在后端服务器组创建后修改健康检查配置。

若切换健康检查协议，负载均衡会根据新的健康检查协议重新检查后端服务器。健康检查通过后，负载均衡向后端服务器继续转发流量。

健康检查切换周期内，客户端可能收到503错误码。

约束与限制

- 健康检查协议与服务器组的后端协议是两个相互独立的能力，所以健康检查协议可以与后端协议不同。
- 为了减少后端服务器的CPU占用，建议您使用TCP协议做健康检查。如果您希望使用HTTP健康检查协议，建议使用HTTP+静态文件的方式。
- 为保证健康检查功能正常，配置健康检查后必须放通对应的安全组规则，详情请参考**配置后端服务器的安全组**。

说明

开启健康检查后不会影响已建立连接的流量转发，负载均衡会立即对后端服务器执行健康检查。

- 如果健康检查正常，则新建连接的流量会根据分配策略和权重向该服务器转发流量。
- 如果健康异常，则系统会设置该服务器状态为异常，不转发新的流量到该服务器。

开启健康检查

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 弹性负载均衡 > 后端服务器组”。
5. 在后端服务器组界面，单击需要修改健康检查的后端服务器组名称。
6. 在后端服务器组的“基本信息”页签下，单击健康检查区域右侧的“配置健康检查”。
7. 在“配置健康检查”弹窗，可根据需要参考**表1-50**进行配置。

表 1-50 配置健康检查参数说明

参数	说明	示例
是否开启	开启或者关闭健康检查。	-
健康检查协议	• 健康检查支持选择TCP、HTTP、HTTPS方式。 • 当后端协议选择UDP，健康检查协议默认为UDP且不可修改。	HTTP
健康检查域名	如果健康检查协议选择HTTP/HTTPS协议，则该项是必选参数。 健康检查的请求域名。 • 默认使用后端服务器的内网IP为域名。 • 您也可选择指定特定域名，特定域名只能由字母，数字，中划线组成，中划线不能在开头或末尾，至少包含两个字符串，单个字符串不能超过63个字符，字符串间以点分割，且总长度不超过100个字符。	www.elb.com
健康检查端口	健康检查端口号，取值范围[1，65535]，为可选参数。 **说明** 默认使用后端云服务器的业务端口进行健康检查。指定特定端口后，使用指定的端口进行健康检查。	80

参数	说明	示例
健康检查路径	如果健康检查协议选择HTTP/HTTPS协议，则该项是必填参数。 指定健康检查的URL地址。检查路径只能以/开头，长度范围[1-80]。 后端服务器组关联独享型负载均衡器：检查路径支持使用英文字母、数字和‘-’、‘/’、‘.’、‘?’、‘#’、‘%’、‘&’以及扩展字符集_;~!（）*[]@$^:',+。	/index.html
检查间隔（秒）	每次健康检查响应的最大间隔时间。 取值范围[1-50]。	5
超时时间（秒）	每次健康检查响应的最大超时时间。取值范围[1-50]。	3
健康检查正常阈值	表示判定后端服务器为正常状态时，所需的连续健康检查成功次数，取值范围[1-10]。	3
健康检查异常阈值	表示判定后端服务器为异常状态时，所需的连续健康检查失败次数，取值范围[1-10]。	3
健康检查返回码	如果健康检查协议选择HTTP/HTTPS/GRPC协议，则该项是必填参数。 自定义健康检查返回的状态码，仅当健康检查请求成功且返回指定状态码时判定后端服务器状态正常。 可输入支持状态码范围内不重复的单个数字或正序的数字区间，如0-10，200-300。多个状态码请输入回车键隔开，最多支持输入5个。 ● 检查协议为HTTP/HTTPS时，状态码范围：200-599。 ● 检查协议为GRPC时，状态码范围：0-99。 **说明** 支持设置健康检查返回码的功能陆续上线中，请以控制台实际为准。	200

8. 单击“确定”。

关闭健康检查

1. 登录管理控制台。

2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 弹性负载均衡 > 后端服务器组”。
5. 在后端服务器组界面，单击需要关闭健康检查的后端服务器组名称。
6. 在后端服务器组的“基本信息”页签下，单击健康检查区域右侧的“配置健康检查”。
7. 在“配置健康检查”界面，可根据需要关闭健康检查。
8. 单击“确定”。

1.4.4.4 修改流量分配策略配置

操作场景

本章节指导用户在后端服务器组中的修改流量分配策略。

流量分配策略详情参见**流量分配策略介绍**。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 弹性负载均衡 > 后端服务器组”。
5. 在后端服务器组列表，在目标后端服务器组所在行的操作列单击“编辑”。
6. 在“修改后端服务器组”弹窗中进行修改，选择“分配策略类型”。
7. 单击“确定”。

说明

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

1.4.4.5 修改会话保持配置

操作场景

本章节指导用户在后端服务器组中修改会话保持功能。

说明

您还可以在进行“添加监听器”或“创建后端服务器组”操作时，配置会话保持功能。

开启会话保持

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。

3. 单击页面左上角的，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 弹性负载均衡 > 后端服务器组”。
5. 在后端服务器组界面，在目标后端服务器组所在行的操作列单击“编辑”。
6. 在“修改后端服务器组”弹窗中，开启会话保持功能，配置会话保持类型以及会话保持时间参数。
7. 单击“确定”。

关闭会话保持

1. 登录管理控制台。
2. 在管理控制台左上角单击图标，选择区域和项目。
3. 单击页面左上角的，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 弹性负载均衡 > 后端服务器组”。
5. 在后端服务器组界面，在目标后端服务器组所在行的操作列单击“编辑”。
6. 在“修改后端服务器组”弹窗中，关闭会话保持功能。
7. 单击“确定”。

1.4.4.6 修改慢启动配置

操作场景

本章节指导用户在后端服务器组中修改慢启动功能。

慢启动详情参见**慢启动介绍（独享型）**。

说明

您还可以在进行“添加监听器”或“创建后端服务器组”操作时，配置慢启动。

开启慢启动

1. 登录管理控制台。
2. 在管理控制台左上角单击图标，选择区域和项目。
3. 单击页面左上角的，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 弹性负载均衡 > 后端服务器组”。
5. 在后端服务器组界面，在目标后端服务器组所在行的操作列单击“编辑”。

图 1-25 后端服务器组编辑入口

6. 在“修改后端服务器组”弹窗中，开启慢启动功能并配置慢启动时间。

慢启动时间（秒）：取值范围为30~1200，当慢启动时间结束，负载均衡向后端服务器发送完整比例的流量请求。

7. 单击“确定”。

关闭慢启动

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 弹性负载均衡 > 后端服务器组”。
5. 在后端服务器组界面，在目标后端服务器组所在行的操作列单击“编辑”。
6. 在“修改后端服务器组”弹窗中，关闭慢启动功能。
7. 单击“确定”。

1.4.5 更换后端服务器组

操作场景

本章节指导用户更换在监听器下配置的默认转发后端服务器组。

ELB四层监听器（TCP/UDP）将客户端请求转发到默认后端服务器组。

ELB七层监听器（HTTP/HTTPS）将客户端的请求按转发策略的优先级进行转发。若用户未自定义转发策略，客户端请求将被转发至默认后端服务器组。

约束与限制

- 监听器开启重定向，不支持更换后端服务器组。
- 后端服务器组的后端协议应与监听器的前端协议匹配，匹配关系详见**表1-34**。
- 独享型负载均衡实例的后端服务器组支持被监听器重复关联。
- 共享型负载均衡实例的后端服务器组仅支持更换已关联在本实例下且未被监听器使用的后端服务器组。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”列表，单击目标监听器所在的负载均衡名称。
5. 选择“监听器”页签，在监听器列表中，单击目标监听器的名称。
6. 在监听器的“基本信息”页签，单击“后端服务器组”区域右侧“更换后端服务器组”。
7. 在弹出的对话框中，单击服务器组名称方框。

   将显示搜索框、所有可选服务器组和“创建后端服务器组”。

   a. 选择已有服务器组，可直接单击目标服务器组名称，也可在搜索框中按名称搜索。

b. 您也可单击“创建后端服务器组”创建新的后端服务器组。创建完成后单击刷新按钮，在已有服务器组中进行选择。

说明

若创建新的服务器组，后端协议应与监听器的前端协议匹配才可被当前监听器使用。

8. 单击“确定”。

1.4.6 查看后端服务器组

操作场景

本章节指导用户查看后端服务器组的的详细信息，主要信息如下：

- 基本信息：后端服务器组的基本信息，包括名称、ID和后端协议等信息。
- 健康检查：后端服务器组是否开启健康检查以及健康检查的详细配置信息。
- 后端服务器：后端服务器组中已添加的后端服务器资源。
- 关联资源：后端服务器组与关联资源间的关系，关联资源包括负载均衡器、监听器和转发策略。

说明

- 仅关联独享型负载均衡器使用的后端服务器组支持查看关联资源。
- 查看后端服务器组关联资源功能发布区域请参考**功能总览**。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 弹性负载均衡 > 后端服务器组”。
5. 在后端服务器组列表，单击待查看的后端服务器组名称。
6. 选择不同的页签，查看需要的信息。
   a. 在“基本信息”页签下，查看服务器组基本信息和健康检查配置。
   b. 在“后端服务器”页签下，查看服务器组中已添加的后端服务器。
   c. 在“关联资源”页签下，查看服务器组已关联的资源。

1.4.7 删除后端服务器组

操作场景

本章节指导用户删除已创建的后端服务器组。

约束与限制

- 如果后端服务器组已被监听器使用，无法执行删除，需先将目标后端服务器组从监听器下释放。
  - 在监听器下释放默认转发后端服务器组，详情请参见**更换后端服务器组**。

  - 七层监听器还需保证自定义的转发策略不使用该后端服务器组。
- 如果后端服务器组中包含后端服务器，不能执行删除操作，需先移除已添加的后端服务器。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 弹性负载均衡 > 后端服务器组”。
5. 在后端服务器组列表，在目标后端服务器组所在行的操作列单击“删除”。
6. 在“确认删除后端服务器组”对话框中，单击“确定”。

1.5 后端服务器

1.5.1 后端服务器概述

负载均衡器会将客户端的请求转发给后端服务器处理。

负载均衡器支持随时增加或减少后端服务器数量，保证应用业务的稳定和可靠，屏蔽单点故障。

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

不同类型的后端服务器组，支持添加不同类型的后端服务器，详情见**表1-51**。

表 1-51 添加后端服务器分类

后端服务器组类型	支持的后端服务器类型	添加指引
混合类型	• 支持直接添加与负载均衡器同VPC的弹性云服务器（ECS）实例和辅助弹性网卡（SubENI）实例作为后端服务器。 • 开启跨VPC后端功能后，支持添加云上其他VPC和云下数据中心的IP地址作为后端服务器。 **说明** 混合类型一定需要指定虚拟私有云，且后端服务器组绑定该虚拟私有云下的负载均衡。	• **添加后端云服务器** • **添加辅助弹性网卡** • **添加IP类型后端**

后端服务器组类型	支持的后端服务器类型	添加指引
IP类型	支持添加云上或云下数据中心的IP地址作为后端服务器。 **说明** 负载均衡实例需开启跨VPC后端功能才能添加IP类型的后端服务器组。	**添加IP类型后端**

注意事项

- 建议您选择相同操作系统的后端服务器，以便日后管理和维护。
- 新添加后端服务器后，若健康检查开启，负载均衡器会向后端服务器发送请求以检测其运行状态，响应正常则直接上线，响应异常则开始健康检查机制定期检查，检查正常后上线。
- 关机或重启已有业务的后端服务器，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服务器的访问量不均衡。如果出现了访问不均衡的情况，建议您暂时关闭会话保持功能，观察一下是否依然存在这种情况。
- 支持在任意时刻增加或减少后端服务器的数量，且可以支持不同的后端服务器切换操作。但是，为了保证您对外业务的稳定，建议在执行上述操作时能够开启健康检查功能，并同时保证至少有1台正常运行的后端服务器。

约束与限制

- 一个后端服务器组最多支持添加500个后端服务器。
- 确保后端服务器的安全组已针对后端服务器端口和健康检查端口配置了相应的入方向规则，详情请参见**配置后端服务器的安全组**。
- 独享型负载均衡的网络型(TCP/UDP)实例不支持同一台服务器既作为后端服务器又作为客户端的场景。

后端服务器的权重

在后端服务器组内添加后端服务器后，需设置后端服务服务器的转发权重。权重越高的后端服务器将被分配到越多的访问请求。

每台后端服务器的权重取值范围为[0, 100]，新的请求不会转发到权重为0的后端服务器上。

以下三种流量分配策略支持权重设置，详情见**表1-52**，更多流量策略分配策略详情见**流量分配策略介绍**。

表 1-52 流量分配策略的权重设置说明

流量分配策略类型	权重设置说明
加权轮询算法	• 在非0的权重下，负载均衡器会将请求按权重值的大小分配给所有的后端服务器，且在轮询时，权重大的后端服务器被分配的概率高。 • 当后端服务器的权重都设置为相等时，负载均衡器将按照简单的轮询策略分发请求。
加权最少连接	• 在非0的权重下，负载均衡器会通过 overhead=当前连接数/权重 来计算每个服务器负载。 • 每次调度会选择overhead最小的后端服务器。
源IP算法	• 在非0的权重下，在一段时间内，同一个客户端的IP地址的请求会被调度至同一个后端服务器上。 • 每台后端服务器的权重取只做0和非0的区分。

1.5.2 配置后端服务器的安全组

操作场景

为了确保负载均衡器与后端服务器进行正常通信和健康检查正常，添加后端服务器后必须检查后端服务器所在的安全组规则和网络ACL规则。

- 后端服务器的安全组规则必须放通源地址为ELB后端子网所属网段。默认情况下，ELB后端子网与ELB所在子网一致。查看如何**配置安全组规则**。
- 网络ACL为子网级别的可选安全层，若ELB的后端子网关联了网络ACL规则，网络ACL规则必须配置允许源地址为ELB后端子网所属网段。查看如何**配置网络ACL规则**。

说明

若独享型ELB实例未开启“跨VPC后端”功能，ELB四层监听器转发的流量将不受安全组规则和网络ACL规则限制，安全组规则和网络ACL规则无需额外放通。

建议您使用监听器的访问控制功能对访问IP进行限制，详情请参考**访问控制策略**。

约束与限制

- 后端服务器组开启健康检查，后端服务器的安全组规则必须配置放通ELB用于健康检查的协议和端口。
- 如果健康检查使用UDP协议，则还必须配置安全组规则放行ICMP协议，否则无法对已添加的后端服务器执行健康检查。

配置安全组规则

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

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 选择“计算 > 弹性云服务器”。
4. 在弹性云服务器列表，单击待变更安全组规则的弹性云服务器名称。
   系统跳转至该弹性云服务器详情页面。
5. 选择“安全组”页签，单击安全组名称，查看安全组规则。
6. 单击“ID”或者“更改安全组规则”，系统自动跳转至安全组界面。
7. 在入方向规则页签，单击“添加规则”，根据所在后端服务器组的后端协议类型按**表1-53**配置安全组入方向的访问规则。

   表 1-53 放通安全组规则（独享型）

后端协议	策略	协议端口	源地址
HTTP或者HTTPS	允许	协议：TCP 端口：后端服务器端口和健康检查端口	**ELB后端子网所属网段**
TCP	允许	协议：TCP 端口：健康检查端口	
UDP	允许	协议：UDP、ICMP 端口：健康检查端口	

   说明

   - 创建负载均衡实例后，不建议变更后端子网。若更换后端子网，负载均衡器已占用的后端子网IP地址不会释放，原后端子网所属网段仍需保持放通状态。
   - 为负载均衡实例新增后端子网，新增后端子网所属网段也需全部放通。
8. 单击“确定”，完成安全组规则配置。

配置网络 ACL 规则

网络ACL是一个子网级别的可选安全层，通过与子网关联的出方向/入方向规则控制出入子网的数据流。网络ACL与安全组类似，都是安全防护策略，当您想增加额外的安全防护层时，就可以启用网络ACL。

网络ACL默认规则会拒绝所有入站和出站流量，启用网络ACL后，您可以通过配置网络ACL入方向规则，放行源网段为ELB后端子网所在网段，目的端口为后端服务器端口。

- 当独享型负载均衡实例与后端服务器在同一个子网时，网络ACL规则不起作用，此时健康检查是通的，且客户端也能访问到后端服务器。
- 当独享型负载均衡实例与后端服务器不在同一个子网时，网络ACL规则是生效的，此时健康检查不通，且客户端访问不到后端服务器。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。

3. 在系统首页，选择“网络 > 虚拟私有云”。
4. 在左侧导航栏选择“访问控制 > 网络ACL”。
5. 在“网络ACL”列表区域，选择网络ACL的名称列，单击您需要修改的“网络ACL名称”进入网络ACL详情页面。
6. 在入方向规则或出方向规则页签，单击“添加规则”，添加入方向或出方向规则。
   - 策略：选择允许。
   - 类型：与后端服务器的IP类型保持一致。
   - 协议：和后端协议一致。
   - 源地址：此方向允许的源地址，填写ELB后端子网网段。
   - 源端口范围：选择业务所在端口范围。
   - 目的地址：此方向允许的目的地址。选择默认值为0.0.0.0/0，代表支持所有的IP地址。
   - 目的端口范围：选择业务所在端口范围。
   - 描述：网络ACL规则的描述信息，非必填项。
7. 单击“确定”。

1.5.3 后端云服务器

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

负载均衡器支持随时增加或减少后端云服务器数量，保证应用业务的稳定和可靠。

约束与限制

- 服务器组类型需为混合类型，IP类型服务器组不支持添加后端云服务器。
- 仅支持添加与后端服务器组同VPC的云服务器。
- 后端云服务器支持添加弹性云服务器和裸金属服务器两种服务器实例。独享型弹性负载均衡对裸金属服务器的规格有兼容性要求，部分存量规格实例无法添加，支持添加的实例规格详见**《裸金属服务器实例家族》**。

添加后端服务器

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 弹性负载均衡 > 后端服务器组”。
5. 在“后端服务器组”界面，单击需要添加后端服务器的后端服务器组名称。
6. 切换到“后端服务器”页签，选择下方“云服务器”页签，并单击“添加”。
7. 支持通过指定关键字搜索后端服务器。私网IP地址支持选择主网卡和扩展网卡。
   勾选添加的后端服务器，单击“下一步”。
8. 设置后端端口和服务器的权重，单击“完成”。
   支持批量设置后端端口。

修改后端云服务器的端口和权重

每台后端服务器的权重取值范围为[0, 100]，新的请求不会转发到权重为0的后端服务器上。

仅当流量分配策略为加权轮询算法、加权最少连接算法和源IP算法时支持权重设置，更多详情见**后端服务器的权重**。

说明

后端服务器的业务端口支持修改功能陆续上线中，已发布区域请参见**修改后端服务器的业务端口**。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 弹性负载均衡 > 后端服务器组”。
5. 在“后端服务器组”界面，单击需要修改后端服务器端口/权重的后端服务器组名称。
6. 在该后端服务器组界面，选择“后端服务器”页签，单击下方“云服务器”区域。
7. 勾选需要设置端口/权重的后端服务器，单击服务器列表上方的“修改端口/权重”。
8. 在“修改端口/权重”弹窗页面，根据需要修改权重/端口的后端数量进行相应操作。
   - 修改端口：
     - 修改单个后端服务器端口：在目标服务器所在行，设置“业务端口”。
     - 批量修改后端服务器端口：在“批量修改端口”后的输入框中设置端口值，单击输入框右侧的“确定”。
   - 修改权重：
     - 修改单个后端服务器权重：在目标服务器所在行，设置“修改后权重”。
     - 批量修改后端服务器权重：在“批量修改权重”后的输入框中设置权重值，单击输入框右侧的“确定”。

     说明

     将后端服务器的权重值批量设置为“0”，可以实现批量屏蔽后端服务器。
9. 单击弹窗下方的“确定”，完成设置。

移除后端服务器

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

说明

移除后端服务器后，长连接在超时时间内会复用TCP连接，请求会继续转发，仍然会有流量进入后端服务器。已有连接在请求超时时间后没有数据传输，ELB会将连接断开。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 弹性负载均衡 > 后端服务器组”。
5. 在“后端服务器组”界面，单击需要移除后端服务器的后端服务器组名称。
6. 切换到“后端服务器”页签，选择下方“云服务器”页签。
7. 勾选需要移除的云服务器，单击服务器列表上方的“移除”。
8. 在移除后端服务器的对话框中单击“是”。

1.5.4 IP 类型后端（跨 VPC 后端）

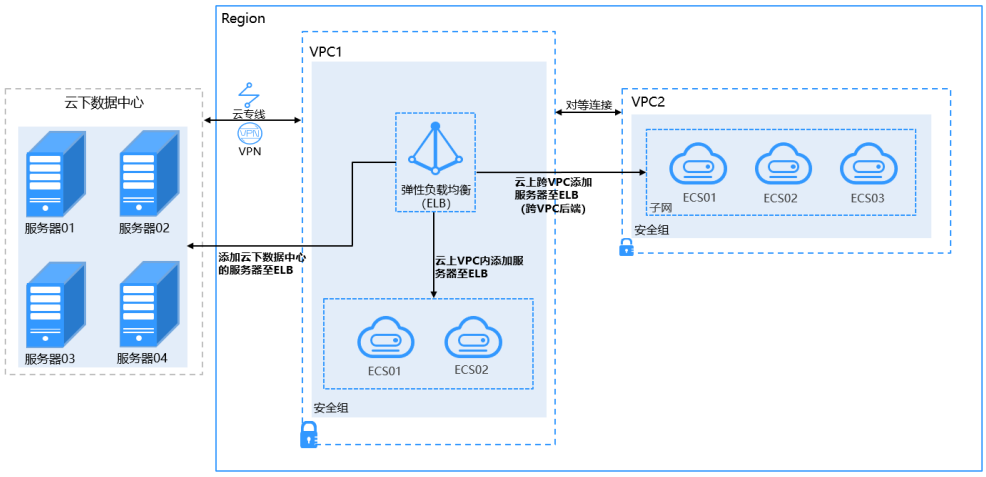
独享型负载均衡实例支持混合负载均衡的能力，后端服务器组不仅支持添加云上同VPC内的云服务器和辅助弹性网卡，还支持通过IP类型后端功能添加云上其他VPC和云下数据中心的IP地址作为后端服务器。

添加IP类型后端帮助用户根据业务诉求灵活配置后端服务，将流量请求转发到云上、云下的服务器上。

说明

原“跨VPC后端”已更名为“IP类型后端”。

图 1-26 ELB 支持添加云上、云下的服务器



约束与限制

- IP类型后端功能开启后无法关闭。
- 只支持添加私网IPv4地址作为后端服务器。
- 通过IP类型后端添加的单个后端服务器最多支持5W并发连接数。

- 通过IP类型后端功能添加的后端服务器，默认开启的获取客户端IP功能会失效。请使用**TOA模块**获取客户端IP地址。

说明

后端协议为UDP的服务器组支持IP类型后端功能陆续上线中，已发布区域请参见**UDP协议支持跨VPC**。

添加 IP 类型后端场景

开启IP类型后端功能后，独享型负载均衡可添加IP类型的后端服务器。根据添加的IP地址来源不同需做不同的准备，如**表1-54**。

表 1-54 添加 IP 地址

ELB实例添加跨VPC后端	必做准备
添加云上其他VPC中的IP	需要先在ELB所在的VPC和云上其他VPC之间建立对等连接，然后通过跨VPC功能添加。 建立对等连接详见**《虚拟私有云用户指南》**。
添加云上同VPC中的IP	需要对ELB所在的VPC创建对等连接并添加对等连接路由，再通过跨VPC功能添加。 详情见**《通过IP类型后端功能添加同VPC内的服务器至ELB》**。
添加云下数据中心的IP	需要先通过云专线或VPN连通云上ELB所在的VPC和云下数据中心，详见**《云专线用户指南》**或**《虚拟专用网络用户指南》**。

开启 IP 类型后端

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要开启IP类型后端功能的负载均衡名称。
5. 在“基本信息”页面，单击“开启IP类型后端”。
6. 单击“确定”。

添加 IP 类型后端

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 弹性负载均衡 > 后端服务器组”。

5. 在“后端服务器组”界面，单击需要添加后端服务器的后端服务器组名称。
6. 切换到“后端服务器”页签，选择下方“IP类型后端（跨VPC后端）”页签，并单击“添加”。
7. 填写“IP类型后端IP”、“业务端口”和“权重”。
8. 单击“确定”。

修改 IP 类型后端的权重和端口

每台后端服务器的权重取值范围为[0, 100]，新的请求不会转发到权重为0的后端服务器上。

仅当流量分配策略为加权轮询算法、加权最少连接算法和源IP算法时支持权重设置，更多详情见**后端服务器的权重**。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 弹性负载均衡 > 后端服务器组”。
5. 在“后端服务器组”界面，单击需要修改IP类型后端权重的后端服务器组名称。
6. 在该后端服务器组界面，切换到“后端服务器”页签，单击下方“跨VPC后端”页签。
7. 勾选需要设置权重的后端服务器，单击服务器列表上方的“修改端口/权重”。
8. 在“修改端口/权重”弹窗页面，根据需要修改权重的后端数量进行相应操作。
   - 修改端口：
     - 修改单个后端服务器端口：在目标服务器所在行，设置“业务端口”。
     - 批量修改后端服务器端口：在“批量修改端口”后的输入框中设置端口值，单击输入框右侧的“确定”。
   - 修改权重：
     - 修改单个后端服务器权重：在目标服务器所在行，设置“修改后权重”。
     - 批量修改后端服务器权重：在“批量修改权重”后的输入框中设置权重值，单击输入框右侧的“确定”。

     说明

     将后端服务器的权重值批量设置为“0”，可以实现批量屏蔽后端服务器。
9. 单击弹窗下方的“确定”，完成批量设置。

移除 IP 类型后端

说明

移除后端服务器后，长连接在超时时间内会复用TCP连接，请求会继续转发，仍然会有流量进入后端服务器。已有连接在请求超时时间后没有数据传输，ELB会将连接断开。

1. 登录管理控制台。

2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 弹性负载均衡 > 后端服务器组”。
5. 在“后端服务器组”界面，单击需要移除后端服务器的后端服务器组名称。
6. 切换到“后端服务器”页签，选择下方“IP类型后端”页签。
7. 勾选需要移除的IP类型后端，单击服务器列表上方的“移除”。
8. 在移除后端服务器的对话框中单击“是”。

1.5.5 辅助弹性网卡

独享型负载均衡实例的后端服务器组的后端服务器不仅支持同VPC内添加ECS实例、跨VPC添加IP地址，还支持**添加辅助弹性网卡**。

辅助弹性网卡是一种基于弹性网卡的衍生资源，用于解决单个云服务器实例挂载的弹性网卡超出上限，不满足用户使用需要的问题。辅助弹性网卡通过VLAN子接口挂载在弹性网卡上，您可以通过创建辅助弹性网卡，使单个云服务器实例挂载更多网卡，实现灵活、高可用的网络方案配置。

更多关于辅助弹性网卡信息，请详见**《虚拟私有云用户指南》**。

说明

辅助弹性网卡功能支持区域请参见**功能总览**。

约束与限制

后端服务器组类型需为混合类型，IP类型服务器组不支持该功能。

添加辅助弹性网卡

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 弹性负载均衡 > 后端服务器组”。
5. 在“后端服务器组”界面，单击需要添加辅助弹性网卡的后端服务器组名称。
6. 切换到“后端服务器”页签，选择下方“辅助弹性网卡”页签，并单击“添加”。

   支持根据ID、私有IP地址、所属弹性网卡私有IP地址、子网名称、子网ID进行搜索添加，然后单击“下一步”。
7. 设置后端端口和服务器的权重，单击“完成”，完成添加。

修改辅助弹性网卡的端口和权重

每台后端服务器的权重取值范围为[0, 100]，新的请求不会转发到权重为0的后端服务器上。

仅当流量分配策略为加权轮询算法、加权最少连接算法和源IP算法时支持权重设置，更多详情见**后端服务器的权重**。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 弹性负载均衡 > 后端服务器组”。
5. 在“后端服务器组”界面，单击需要修改后端服务器权重的后端服务器组名称。
6. 在该后端服务器组界面，切换到“后端服务器”页签，单击下方“辅助弹性网卡”页签。
7. 勾选需要设置端口/权重的后端服务器，单击服务器列表上方的“修改端口/权重”。
8. 在“修改端口/权重”弹窗页面，根据需要修改端口/权重的后端数量进行相应操作。
   - 修改端口：
     - 修改单个后端服务器端口：在目标服务器所在行，设置“业务端口”。
     - 批量修改后端服务器端口：在“批量修改端口”后的输入框中设置端口值，单击输入框右侧的“确定”。
   - 修改权重：
     - 修改单个后端服务器权重：在目标服务器所在行，设置“权重”。
     - 批量修改后端服务器权重：在“批量修改权重”后的输入框中设置权重值，单击输入框右侧的“确定”。

     说明

     将后端服务器的权重值批量设置为“0”，可以实现批量屏蔽后端服务器。
9. 单击弹窗下方的“确定”，完成批量设置。

移除辅助弹性网卡

说明

移除后端服务器后，长连接在超时时间内会复用TCP连接，请求会继续转发，仍然会有流量进入后端服务器。已有连接在请求超时时间后没有数据传输，ELB会将连接断开。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 弹性负载均衡 > 后端服务器组”。
5. 在“后端服务器组”界面，单击需要移除辅助弹性网卡的后端服务器组名称。
6. 切换到“后端服务器”页签，选择下方“辅助弹性网卡”页签。
7. 勾选需要移除的弹性辅助网卡，单击服务器列表上方的“移除”。
8. 在“移除后端服务器”对话框中单击“是”。

1.6 安全管理

1.6.1 独享型 ELB 获取客户端真实 IP

获取客户端 IP 功能概述

监听器开启“获取客户端IP”功能后，负载均衡器和后端服务器之间直接使用真实的IP进行通信。

目前，独享型负载均衡对“获取客户端IP”功能的支持情况如表1-55。

表 1-55 独享型负载均衡“获取客户端 IP”功能说明

监听器类型	开启“获取客户端IP”	关闭“获取客户端IP”
四层（TCP/UDP）监听器	默认开启	×
七层（HTTP/HTTPS）监听器	默认开启	×

约束与限制

- 开启“获取客户端IP”之后，不支持同一台服务器既作为后端服务器又作为客户端的场景。

  如果后端服务器和客户端使用同一台服务器，且开启“获取客户端IP”，则后端服务器会根据报文源IP为本地IP判定该报文为本机发出的报文，无法将应答报文返回给ELB，最终导致回程流量不通。
- 开启此功能后，后端服务器发生迁移时，可能出现流量中断（例如单向数据传输和推送信息类的业务场景）。所以后端服务器迁移完成后，需要通过报文重传来恢复流量。
- 通过跨VPC后端功能添加的后端服务器，默认开启的获取客户端IP功能会失效。请使用TOA模块获取客户端IP地址。

其他获取客户端真实 IP 方法

负载均衡的监听器还可通过如下补充方法获取客户端的真实IP，详情见表1-56。

表 1-56 独享型负载均衡获取客户端真实 IP 补充方法

监听器类型	其他获取客户端真实IP方法
四层（TCP）监听器	配置TOA插件获取。
七层（HTTP/HTTPS）监听器	七层服务获取客户端IP。

1.6.2 开启 HTTP/2 提升通信效率

HTTP/2 概述

HTTP/2即超文本传输协议 2.0，能通过二进制分帧提升网络通信效率，实现多路复用减少延迟。如果您需要保证HTTPS业务更加安全高效，可以在配置HTTPS监听器时，开启HTTP/2功能。

约束与限制

仅HTTPS监听器支持HTTP/2功能。

管理 HTTPS 监听器的 HTTP/2 功能

在添加HTTPS监听时，您可以开启HTTP/2功能。在HTTPS监听器添加完成后，您也可以开启或关闭HTTP/2功能。

新添加 HTTPS 监听器

在添加HTTPS监听时，您可以开启HTTP/2功能。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要开启HTTP/2功能的监听器的负载均衡器名称。
5. 在该负载均衡界面的“监听器”页签，单击“添加监听器”。
6. 在“添加监听器”界面，前端协议选择“HTTPS”。
7. 在“添加监听器”界面，展开高级配置，打开HTTP/2功能。
8. 确认配置，单击“提交”。

图 1-27 开启 HTTP 监听器的 HTTP/2 功能

已有 HTTPS 监听器

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要修改HTTP/2功能的负载均衡器名称。
5. 在“监听器”页签，单击需要修改HTTP/2功能开关的监听器名称。
6. 在监听器的“基本信息”页面，单击“编辑监听器”。
7. 在“编辑监听器”界面，展开高级配置，开启或者关闭HTTP/2功能。
8. 单击“确定”。

图 1-28 修改 HTTPS 监听器的 HTTP/2 功能

1.6.3 配置 TLS 安全策略实现加密通信

对于银行和金融类等需要加密传输的应用，通常会配置HTTPS加密以确保数据的安全传输。弹性负载均衡默认支持部分常用的TLS安全策略来满足您的安全加密需求。

在创建和配置HTTPS监听器时，您可以选择使用合适的默认安全策略，或者**创建自定义策略**，来提高您的业务安全性。

TLS安全策略包含TLS协议版本和配套的加密算法套件。

默认安全策略

TLS协议版本越高，加密通信的安全性越高，但是相较于低版本TLS协议，高版本TLS协议对浏览器的兼容性较差。

对于高安全性要求的业务，推荐采用高版本的TLS协议版本以强化安全防护；而对于安全性要求较低的业务，则可考虑使用兼容性更广的低版本TLS协议以确保业务的广泛适用。

表 1-57 默认安全策略参数说明

名称	支持的TLS版本类型	使用的加密套件列表
TLS-1-0	TLS 1.2 TLS 1.1 TLS 1.0	• ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • AES128-GCM-SHA256 • AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • AES128-SHA256 • AES256-SHA256 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-RSA-AES256-SHA • ECDHE-ECDSA-AES256-SHA • AES128-SHA • AES256-SHA
TLS-1-1	TLS 1.2 TLS 1.1	
TLS-1-2	TLS 1.2	

名称	支持的TLS版本类型	使用的加密套件列表
tls-1-0-inherit	TLS 1.2 TLS 1.1 TLS 1.0	• ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • AES128-GCM-SHA256 • AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • AES128-SHA256 • AES256-SHA256 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • DHE-RSA-AES128-SHA • ECDHE-RSA-AES256-SHA • ECDHE-ECDSA-AES256-SHA • AES128-SHA • AES256-SHA • DHE-DSS-AES128-SHA • CAMELLIA128-SHA • EDH-RSA-DES-CBC3-SHA • DES-CBC3-SHA • ECDHE-RSA-RC4-SHA • RC4-SHA • DHE-RSA-AES256-SHA • DHE-DSS-AES256-SHA • DHE-RSA-CAMELLIA256-SHA

名称	支持的TLS版本类型	使用的加密套件列表
TLS-1-2-Strict	TLS 1.2	• ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • AES128-GCM-SHA256 • AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • AES128-SHA256 • AES256-SHA256 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384
TLS-1-0-WITH-1-3	TLS 1.3 TLS 1.2 TLS 1.1 TLS 1.0	• ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • AES128-GCM-SHA256 • AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • AES128-SHA256 • AES256-SHA256 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-RSA-AES256-SHA • ECDHE-ECDSA-AES256-SHA • AES128-SHA • AES256-SHA • TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256 • TLS_AES_128_CCM_SHA256 • TLS_AES_128_CCM_8_SHA256

名称	支持的TLS版本类型	使用的加密套件列表
TLS-1-2-FS-WITH-1-3	TLS 1.3 TLS 1.2	• ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256 • TLS_AES_128_CCM_SHA256 • TLS_AES_128_CCM_8_SHA256
TLS-1-2-FS	TLS 1.2	• ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384

名称	支持的TLS版本类型	使用的加密套件列表
hybrid-policy-1-0	TLS 1.2 TLS 1.1	• ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • AES128-GCM-SHA256 • AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • AES128-SHA256 • AES256-SHA256 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-RSA-AES256-SHA • ECDHE-ECDSA-AES256-SHA • AES128-SHA • AES256-SHA • ECC-SM4-SM3 • ECDHE-SM4-SM3
tls-1-2-strict-no-cbc	TLS 1.2	• ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES128-GCM-SHA256

说明

上述列表为ELB支持的加密套件，同时客户端也支持多个加密套件。在实际使用时，加密套件的选择范围为：ELB和客户端支持的加密套件的交集，加密套件的选择顺序为：ELB支持的加密套件顺序。

默认安全策略差异对比

下表中，“√”表示支持，“×”表示不支持。

表 1-58 安全策略差异说明

安全策略	tls-1-0	tls-1-1	tls-1-2	tls-1-0-inherit	tls-1-2-strict	tls-1-0-with-1-3	tls-1-2-fs-with-1-3	tls-1-2-fs	hybrid-policy-1-0	tls-1-2-strict-no-cbc
TLS 协议										
Protocol-TLS 1.3	×	×	×	×	×	√	√	√	×	×
Protocol-TLS 1.2	√	√	√	√	√	√	√	√	√	√
Protocol-TLS 1.1	√	√	×	√	×	√	×	×	√	×
Protocol-TLS 1.0	√	×	×	√	×	√	×	×	×	×
加密套件										
ECDHE-RSA-AES128-GCM-SHA256	√	√	√	×	√	×	×	×	×	√
ECDHE-RSA-AES256-GCM-SHA384	√	√	√	√	√	√	√	√	√	√
ECDHE-RSA-AES128-SHA256	√	√	√	√	√	√	√	√	√	×
ECDHE-RSA-AES256-SHA384	√	√	√	√	√	√	√	√	√	×
AES128-GCM-SHA256	√	√	√	√	√	√	×	×	√	×
AES256-GCM-SHA384	√	√	√	√	√	√	×	×	√	×
AES128-SHA256	√	√	√	√	√	√	×	×	√	×
AES256-SHA256	√	√	√	√	√	√	×	×	√	×

安全策略	tls-1-0	tls-1-1	tls-1-2	tls-1-0-inherit	tls-1-2-strict	tls-1-0-with-1-3	tls-1-2-fs-with-1-3	tls-1-2-fs	hybrid-policy-1-0	tls-1-2-strict-no-cbc
ECDHE-RSA-AES128-SHA	√	√	√	√	×	√	×	×	√	×
ECDHE-RSA-AES256-SHA	√	√	√	√	×	√	×	×	√	×
AES128-SHA	√	√	√	√	×	√	×	×	√	×
AES256-SHA	√	√	√	√	×	√	×	×	√	×
ECDHE-ECDSA-AES128-GCM-SHA256	√	√	√	√	√	√	√	√	√	√
ECDHE-ECDSA-AES128-SHA256	√	√	√	√	√	√	√	√	√	×
ECDHE-ECDSA-AES128-SHA	√	√	√	√	×	√	×	×	√	×
ECDHE-ECDSA-AES256-GCM-SHA384	√	√	√	√	√	√	√	√	√	√
ECDHE-ECDSA-AES256-SHA384	√	√	√	√	√	√	√	√	√	×
ECDHE-ECDSA-AES256-SHA	√	√	√	√	×	√	×	×	√	×
ECDHE-RSA-AES128-GCM-SHA256	×	×	×	√	×	√	√	√	√	×
TLS_AES_256_GCM_SHA384	×	×	×	×	×	√	√	√	×	×

安全策略	tls-1-0	tls-1-1	tls-1-2	tls-1-0-inherit	tls-1-2-strict	tls-1-0-with-1-3	tls-1-2-fs-with-1-3	tls-1-2-fs	hybrid-policy-1-0	tls-1-2-strict-no-cbc
TLS_CHACHA20_POLY1305_SHA256	×	×	×	×	×	√	√	√	×	×
TLS_AES_128_GCM_SHA256	×	×	×	×	×	√	√	√	×	×
TLS_AES_128_CCM_8_SHA256	×	×	×	×	×	√	√	√	×	×
TLS_AES_128_CCM_SHA256	×	×	×	×	×	√	√	√	×	×
DHE-RSA-AES128-SHA	×	×	×	√	×	×	×	×	×	×
DHE-DSS-AES128-SHA	×	×	×	√	×	×	×	×	×	×
CAMELLIA128-SHA	×	×	×	√	×	×	×	×	×	×
EDH-RSA-DES-CBC3-SHA	×	×	×	√	×	×	×	×	×	×
DES-CBC3-SHA	×	×	×	√	×	×	×	×	×	×
ECDHE-RSA-RC4-SHA	×	×	×	√	×	×	×	×	×	×
RC4-SHA	×	×	×	√	×	×	×	×	×	×
DHE-RSA-AES256-SHA	×	×	×	√	×	×	×	×	×	×
DHE-DSS-AES256-SHA	×	×	×	√	×	×	×	×	×	×
DHE-RSA-CAMELLIA256-SHA	×	×	×	√	×	×	×	×	×	×
ECC-SM4-SM3	×	×	×	×	×	×	×	×	√	×

安全策略	tls-1-0	tls-1-1	tls-1-2	tls-1-0-inherit	tls-1-2-strict	tls-1-0-with-1-3	tls-1-2-fs-with-1-3	tls-1-2-fs	hybrid-policy-1-0	tls-1-2-strict-no-cbc
ECDHE-SM4-SM3	×	×	×	×	×	×	×	×	√	×

表 1-59 安全策略兼容的浏览器/客户端参考说明

安全策略	tls-1-0	tls-1-1	tls-1-2	tls-1-0-inherit	tls-1-2-strict	tls-1-0-with-1-3	tls-1-2-fs-with-1-3	tls-1-2-fs	hybrid-policy-1-0	tls-1-2-strict-no-cbc
Android 8.0	√	√	√	√	√	√	√	√	√	√
Android 9.0	√	√	√	√	√	√	√	√	√	√
Chrome 70 / Win 10	√	√	√	√	√	√	√	√	√	√
Chrome 80 / Win 10	√	√	√	√	√	√	√	√	√	√
Firefox 62 / Win 7	√	√	√	√	√	√	√	√	√	√
Firefox 73 / Win 10	√	√	√	√	√	√	√	√	√	√
IE 8 / XP	√	√	√	√	×	√	×	×	×	×
IE 8-10 / Win 7	√	√	√	√	×	√	×	×	×	×
IE 11 / Win 7	√	√	√	√	√	√	√	√	√	√
IE 11 / Win 10	√	√	√	√	√	√	√	√	√	√
Edge 15 / Win 10	√	√	√	√	√	√	√	√	√	√
Edge 16 / Win 10	√	√	√	√	√	√	√	√	√	√

安全策略	tls-1-0	tls-1-1	tls-1-2	tls-1-0-inherit	tls-1-2-strict	tls-1-0-with-1-3	tls-1-2-fs-with-1-3	tls-1-2-fs	hybrid-policy-1-0	tls-1-2-strict-no-cbc
Edge 18 / Win 10	√	√	√	√	√	√	√	√	√	√
Java 8u161	√	√	√	√	√	√	√	√	√	√
Java 11.0.3	√	√	√	√	√	√	√	√	√	√
Java 12.0.1	√	√	√	√	√	√	√	√	√	√
OpenSSL 1.0.2s	√	√	√	√	√	√	√	√	√	√
OpenSSL 1.1.0k	√	√	√	√	√	√	√	√	√	√
OpenSSL 1.1.1c	√	√	√	√	√	√	√	√	√	√
Safari 10 / iOS 10	√	√	√	√	√	√	√	√	√	√
Safari 10 / OS X 10.12	√	√	√	√	√	√	√	√	√	√
Safari 12.1.1 / iOS 12.3.1	√	√	√	√	√	√	√	√	√	√

创建自定义策略

弹性负载均衡默认支持部分常用的TLS安全策略以满足通用需求，但当您有特定的安全需求时，例如需要仅支持特定版本的TLS协议、禁用某些加密算法套件等，您可以创建自定义TLS安全策略并配置到监听器中，从而进一步提升业务的安全性。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 单击页面左边的“TLS安全策略”。
5. 在TLS安全策略页面，单击页面右上角的“创建自定义策略”。
6. 配置自定义策略参数，参数说明参见**表1-60**。

表 1-60 自定义策略参数说明

参数	说明
名称	自定义策略的名称。
选择协议版本	自定义策略支持的TLS协议版本类型。支持选择多个协议版本。 包含： ● TLS 1.0 ● TLS 1.1 ● TLS 1.2 ● TLS 1.3
选择加密算法套件	选择与协议版本配套的加密算法套件。支持选择多个加密算法套件。
描述	自定义策略相关信息的描述说明。

7. 确认参数配置，单击“确定”。

管理自定义安全策略

自定义安全策略创建完成后，支持您对其进行修改和删除操作。

修改自定义安全策略

您可以根据使用需求对创建完成的自定义安全策略进行修改，支持修改名称、协议版本、加密算法套件和描述。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 单击页面左边的“TLS安全策略”。
5. 在TLS安全策略页面，待修改的自定义安全策略所在行的操作列，单击“修改“。
6. 在“修改自定义安全策略“弹窗，修改自定义安全策略，参数说明参见**表1-60**。
7. 确认参数配置，单击“确定”。

删除自定义安全策略

您可对创建完成的自定义安全策略进行删除。

说明

如果自定义安全策略已被关联监听器使用，则无法执行删除，请先修改关联监听器的安全策略。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。

3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 单击左侧导航栏的“TLS安全策略”。
5. 在TLS安全策略页面，待删除的自定义安全策略所在行的操作列，单击“删除“。
6. 在确认删除弹窗，单击“确定“。

为 HTTPS 监听器添加安全策略

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要创建安全策略的监听器的负载均衡器名称。
5. 在该负载均衡界面的“监听器”区域，单击“添加监听器”。
6. 在“添加监听器”界面，前端协议选择“HTTPS”。
7. 在“添加监听器”界面，选择“高级配置 > 安全策略”。
   支持选择**默认安全策略**或自定义策略。
   如果列表中无自定义策略，您可以选择**创建自定义策略**。
8. 配置完成，单击“确定”。

为 HTTPS 监听器修改安全策略

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要修改安全策略的监听器的负载均衡器名称。
5. 切换至“监听器”页签，单击需要修改安全策略的监听器名称。
6. 在监听器的基本信息页面，单击“编辑监听器”。
7. 在“编辑监听器”界面，展开高级配置，选择安全策略参数。
8. 单击“确定”。

1.6.4 访问控制管理

1.6.4.1 访问控制策略

当您需要对客户端访问弹性负载均衡实施精细的访问控制时，您可以开启ELB监听器的访问控制功能，并设置对应的访问控制策略来控制访问ELB监听器的IP地址。

访问控制策略

您可以为监听的访问控制策略设置白名单或黑名单：

- 白名单：只有白名单中的IP可以访问ELB的监听器。仅转发来自所选访问控制IP地址组中设置的IP地址或网段的请求。

配置了白名单，但是不在白名单的IP也能访问后端服务器，可能的原因是该连接为长连接，需要客户端或后端服务器断开该长连接。

- 黑名单：黑名单中的IP禁止访问ELB的监听器。不会转发来自所选访问控制策略组中设置的IP地址或网段的请求。

说明

- 访问控制只限制实际业务的流量转发，不限制ping命令操作，被限制的IP仍可以ping通后端服务器。
- 访问流量的IP先通过监听器访问控制策略的限制，然后转发至后端服务器，所以后端服务器安全组的规则设置不会影响负载均衡的访问控制策略。

设置访问控制策略

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击负载均衡名称，进入监听器管理界面。
5. 您可以通过以下两种操作入口，为监听器设置访问控制策略。
   - 在目标监听器所在行的“访问控制”列，单击“设置”。
   - 单击目标监听器名称，进入监听器的基本信息页面，单击访问控制右侧的“设置”。
6. 在“设置访问控制”的弹窗中，如表1-61所示配置访问控制。

表 1-61 访问控制参数说明

参数	说明
访问控制	可以选择允许所有IP访问、白名单和黑名单。 • 允许所有IP访问：不进行访问控制，允许所有IP访问负载均衡监听器。 • 白名单：仅允许IP地址组中的IP访问负载均衡监听器。 • 黑名单：不允许IP地址组中的IP访问负载均衡监听器。
IP地址组	设置白名单或者黑名单时，必须选择一个IP地址组。如果还未创建IP地址组，需要先创建IP地址组，更多关于IP地址组的信息请参见IP地址组。
访问控制开关	当访问控制选择白名单或者黑名单时，可以开启或者关闭访问控制开关。 • 开启：开启访问控制开关，设置的白名单和黑名单才会生效。 • 关闭：关闭访问控制开关，设置的白名单和黑名单不生效。

7. 配置完成，单击“确定”。

1.6.4.2 访问控制 IP 地址组

访问控制 IP 地址组简介

IP地址组是多个IP地址的集合，用来统一管理具有相同安全要求或需要频繁修改的IP地址。

弹性负载均衡支持对监听器设置访问控制策略。对于需要使用**黑名单**和**白名单**，在监听器上设置**访问控制**的用户，开启白名单或黑名单时必须选择一个IP地址组。

- 白名单：允许IP地址组中的IP访问负载均衡的监听器。如果IP地址组未包含任何IP地址，则对应的负载均衡监听器禁止任何IP地址访问。
- 黑名单：限制IP地址组中的IP访问负载均衡的监听器。如果IP地址组未包含任何IP地址，则对应的负载均衡监听器允许所有IP地址访问。

约束与限制

- 默认情况下，一个用户可以创建50个IP地址组。
- 同一个IP地址组，最多可以关联50个监听器。

创建 IP 地址组

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 弹性负载均衡 > IP地址组”。
5. 在“IP地址组”界面，单击“创建IP地址组”。
6. 配置IP地址组参数，参数说明参见**表1-62**。

表 1-62 IP 地址组参数说明

参数	说明	样例
名称	IP地址组的名称。	ipGroup-01
企业项目	企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。详见**《企业管理用户指南》**。	-

参数	说明	样例
IP地址	需要通过白名单或黑名单进行访问控制的IP地址，支持IPv4地址和IPv6地址。 • 每行一个IP地址或一个网段，以回车结束。 • 每个IP地址或者网段都可以用“|”分隔添加备注，备注长度范围是0到255字符，不能包含<>。 • 每个IP地址组最多可添加300个IP地址或网段。	• 不带IP地址描述：10.168.2.24 • 带IP地址描述：10.168.16.0/24 | ECS01
描述	IP地址组相关信息的描述说明。	-

7. 确认参数配置，单击“确定”。

管理 IP 地址组内的 IP 地址

IP地址组创建后，您可根据使用需求对组内的IP地址进行修改，支持的修改操作如下：

- **添加IP地址**
- **批量修改IP地址**
- **删除IP地址**

IP地址组内输入IP地址，支持的格式如下详见**表1-62**。

添加 IP 地址

IP地址组创建后您可向其中添加IP地址，不影响IP地址组中已有的IP地址。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 弹性负载均衡 > IP地址组”。
5. 在“IP地址组”界面，单击需要添加IP地址的地址组名称，进入IP地址组的详情页面。
6. 在IP地址页签下方，单击“添加IP地址”。在“添加IP地址”页面，添加IP地址。
7. 单击“确定”，完成添加。

批量修改 IP 地址

如果您希望对IP地址组内的所有IP地址进行批量修改，请参考以下操作。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。

3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 弹性负载均衡 > IP地址组”。
5. 在“IP地址组”界面，您可以通过以下两种操作入口，批量修改IP地址。
   a. 批量修改IP地址及其基本信息：
      i. 在需要修改IP地址的地址组所在行的操作列，单击“修改”。支持修改IP地址组的名称，组内所有IP地址和描述。
      ii. 单击“确定”，完成修改。
   b. 仅批量修改IP地址：
      i. 单击需要修改IP地址的地址组名称，进入IP地址组的详情页面。
      ii. 在IP地址页签下方，单击“修改IP地址”。支持修改IP地址组的内所有IP地址。
      iii. 单击“确定”，完成修改。

删除 IP 地址

如果你希望批量删除IP地址组内的多个IP地址，请参考**批量修改IP地址**。

如果您希望对IP地址组内的单IP地址进行删除，请参考以下操作。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 弹性负载均衡 > IP地址组”。
5. 在“IP地址组”界面，单击需要修改IP地址的地址组名称，进入IP地址组的详情页面。
6. 在IP地址列表中，单击目标IP地址所在行的“删除”，弹出删除确认对话框。
7. 确认无误后，单击“是”，删除IP地址。

查看 IP 地址组详情

您可查看IP地址组的详情，快速了解IP地址组的使用情况，包括如下信息：

- IP地址组的基本信息，包括IP地址组的名称、ID、创建时间和描述。
- IP地址组内添加的IP地址。
- IP地址组关联的监听器资源。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 弹性负载均衡 > IP地址组”。
5. 在“IP地址组”界面，单击需要查看详情的地址组名称，进入IP地址组的详情页面。
6. 支持查看IP地址组基本信息。

a. 在“IP地址”页签下，查看IP地址组内的IP地址条目。
b. 在“关联监听器”页签下，查看IP地址组已关联的监听器。

删除 IP 地址组

如果IP地址组已经关联监听器的访问控制策略使用，无法完成删除。

您可在IP地址组列表页或通过**查看IP地址组详情**查看IP地址组已关联的监听器资源，解除IP地址组与监听器的关联请参考**设置访问控制策略**。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 弹性负载均衡 > IP地址组”。
5. 在“IP地址组”界面，需要删除的IP地址组所在行，单击“删除”。
6. 确认需要删除的IP地址组，单击“确定”。

1.6.5 开启 SNI 证书实现多域名访问

操作场景

当您需要在同一个监听器中，根据HTTPS请求域名的不同来选择不同的证书进行认证并将请求分发至不同的后端服务器组时，您可通过开启SNI功能来实现配置多域名HTTPS网站。

SNI（Server Name Indication）是为了解决一个服务器使用域名证书的TLS扩展。开启SNI之后，用户需要添加域名对应的证书，允许客户端在发起SSL握手请求时就提交请求的域名信息，负载均衡收到SSL请求后，会根据域名去查找证书。如果找到域名对应的证书，则返回该证书；如果没有找到域名对应的证书，则返回缺省证书。

约束与限制

- 仅HTTPS和TLS 监听器，支持开启SNI功能，支持绑定多个证书。
- ELB不会自动更新证书，如果您有证书过期了，需要手动更换或者删除证书，详见**绑定/更换证书**。
- 一个HTTPS监听器默认支持配置30个SNI证书，监听器关联的所有SNI证书默认支持的域名总数为30个。

  说明

  独享型负载均衡的监听器最多支持50个SNI证书，如您有需求，可提交**工单**进行处理。

前提条件

- 已创建负载均衡器，具体步骤可参照**创建独享型负载均衡器**。
- 已经创建用于SNI证书，具体步骤可参照**创建证书**。
- 已经创建HTTPS监听器，具体步骤可参照**添加HTTPS监听器**。

SNI 证书约束

- 用于SNI的证书，需要指定域名，指定的域名必须与证书中的域名保持一致。
- 目前支持一个域名可以同时绑定ECC类型的证书和RSA类型的证书。在选择SNI证书时，支持选择同域名绑定的两个证书，使用时ELB会优先选择ECC类型的证书。
- SNI证书匹配规则：

  当证书的域名为*.test.com，那么可支持a.test.com、b.test.com等，不支持a.b.test.com、c.d.test.com等。

  且依据最长尾缀匹配：当证书中的域名同时存在*.b.test.com和*.test.com时，那么a.b.test.com会优先匹配到*.b.test.com。
- 证书示例如图1-29所示，图中的cer-default为创建HTTPS监听器时绑定的默认证书，cert-test01和cert-test02为新创建的用于SNI的证书。

  其中，证书cert-test01填写的域名为www.test01.com、cert-test02填写的域名为www.test02.com。

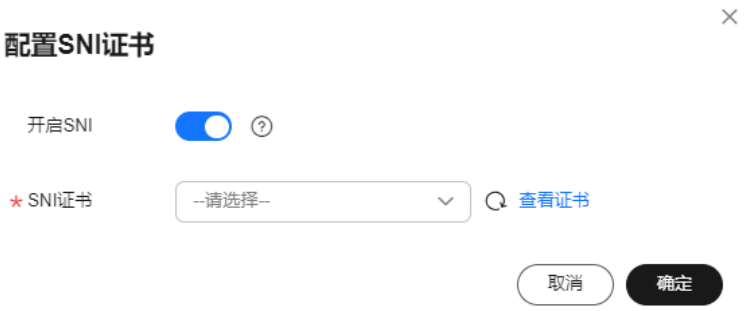
  如果访问负载均衡的域名与SNI证书匹配成功，则会返回SNI的证书认证鉴权。如果匹配失败，则会返回默认证书认证鉴权。

图 1-29 配置证书说明

监听器开启 SNI

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击负载均衡名称。
5. 在“监听器”页签，单击需要开启SNI的监听器名称。
6. 在监听器基本信息页面，单击SNI右侧“配置”。
7. 开启SNI的开关，选择需要配置的SNI证书。

图 1-30 配置 SNI 证书



8. 单击“确定”。

1.6.6 证书管理

1.6.6.1 证书概述

负载均衡器支持三种类型的证书，服务器证书、CA证书、服务器SM双证书。配置HTTPS监听器时，需要为监听器绑定服务器证书，如果开启双向认证功能，还需要绑定CA证书。

- 服务器证书：在使用HTTPS协议时，服务器证书用于SSL握手协商，需提供证书内容和私钥。
- CA证书： 又称客户端CA公钥证书，用于验证客户端证书的签发者；在开启HTTPS双向认证功能时，只有当客户端能够出具指定CA签发的证书时，HTTPS连接才能成功。
- 服务器SM双证书：在使用HTTPS协议时，若采用商密SSL协议，需提供双证书。双证书包括**签名证书**和**加密证书**，需成套使用。

  说明

  服务器SM双证书已上线华北-乌兰察布一，其余区域持续上线中。

  - **签名证书：**在签名时使用，仅用于验证身份使用，其公钥和私钥均由服务器自己产生，并由服务器自己保管，证书颁发机构（Certificate Authority，简称“CA”）不负责其保管任务。
  - **加密证书：**在密钥协商时使用，其私钥和公钥均由CA产生，并由CA保管（存根）。

说明

证书管理既支持在华为云购买的证书，也支持您自己生成的证书。

使用证书的注意事项

- 同一个证书在负载均衡器上只需上传一次，可以使用在多个负载均衡器实例中。
- 如果创建的服务器证书用于SNI，则需要指定域名，且指定的域名必须与证书中的域名保持一致。一个证书可以指定多个域名。
- 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。如果监听器开启了SNI功能，则支持绑定多个服务器证书。
- 负载均衡器只支持原始证书，不支持对证书进行加密。

- 可以使用自签名的证书，使用自签名证书和第三方机构颁发的证书对负载均衡器无区别，但是使用自签名证书会存在安全隐患，建议客户使用权威机构颁发的证书。
- 负载均衡器只支持PEM格式的证书，其它格式的证书需要转换成PEM格式后，才能上传到负载均衡。
- ELB不会自动更新证书，如果您有证书过期了，需要手动更换或者删除证书。

证书格式要求

在创建证书时，您可以直接输入证书内容或上传证书文件。

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

服务器证书、CA证书的“证书内容”格式均需按以下要求。

服务器SM双证书中的“SM签名证书内容”和“SM加密证书内容”格式均需按以下要求。

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

示例如下：

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

私钥格式要求

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

服务器SM双证书中的“SM签名证书私钥”和“SM加密证书私钥”格式均需按以下要求。

需注意必须是无密码的私钥，私钥内容格式为：

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

示例如下：

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


1.6.6.2 格式转换

操作场景

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

DER 转换为 PEM

DER格式通常使用在Java平台。

运行以下命令进行证书转化：

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

运行以下命令进行私钥转化：

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

P7B 转换为 PEM

P7B格式通常使用在Windows Server和Tomcat中。

运行以下命令进行证书转化：

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

PFX 转换为 PEM

PFX格式通常使用在Windows Server中。

运行以下命令进行证书转化：

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

运行以下命令进行私钥转化：

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

1.6.6.3 创建证书

操作场景

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

- 服务器证书：同时支持云证书管理服务提供的服务器数字证书和您的自有证书。
- CA证书：仅支持上传您的自有CA证书
- 服务器SM双证书：同时支持云证书管理服务提供的服务器数字证书和您的自有证书。

说明

- 如果您不希望将证书上传到负载均衡器上进行管理，您可以将证书存放到后端服务器上，然后配置相同端口的TCP监听器将HTTPS流量透传到后端服务器。具体原理参见**TCP监听器将HTTPS流量透传到后端服务器**。
- 如果在两个区域想要使用同一个证书，需要在两个区域分别使用的证书信息创建两个证书。

创建服务器证书

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏单击“证书管理”。
5. 单击“创建证书”，配置参数请参见**表1-63**。

表 1-63 服务器证书参数说明

参数	说明
证书类型	创建证书的类型，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。 ● 服务器SM双证书：在使用HTTPS协议时，若采用商密SSL协议，需提供双证书。双证书包括签名证书和加密证书，需成套使用。
证书来源	服务器证书同时支持SSL证书管理服务提供的数字证书和您的自有证书。 ● SCM证书：SSL证书管理服务管理的服务器数字证书，您需要到云证书管理服务控制台签发证书或上传自有证书。 ● 自有证书：您需要在负载均衡控制台上传自有证书的证书内容和私钥。 **说明** 推荐使用云证书管理服务对您的证书进行统一管理。
证书	仅SCM证书支持该参数。 支持选择您在云证书管理服务统一管理的证书。
证书名称	仅自有证书支持该参数。 您的自有证书名称。
企业项目	企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。

参数	说明
证书内容	仅自有证书支持该参数。 证书内容必须为PEM格式。 单击“上传”，选择上传证书文件，请确保您的浏览器是最新版本。 证书内容格式如下： -----BEGIN CERTIFICATE----- Base64-encoded certificate -----END CERTIFICATE-----
私钥	仅自有证书支持该参数。 单击“上传”，选择上传私钥文件，请确保您的浏览器是最新版本。 需注意必须是无密码的私钥。符合PEM格式，私钥格式如下： -----BEGIN PRIVATE KEY----- [key] -----END PRIVATE KEY-----
域名	如果创建的证书用于SNI，则需要指定域名。 域名只能由字母、数字、中划线组成，中划线不能在开头或末尾，单个字符串不超过63个字符，字符串间以点分隔。 最多可支持100个域名，域名间以逗号分隔；单个域名长度不超过100个字符，且总长度不超过10000个字符。
描述	添加对该证书的描述信息，非必填项。

创建 CA 证书

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏单击“证书管理”。
5. 单击“创建证书”，配置参数请参见**表1-64**。

表 1-64 CA 证书参数说明

参数	说明
证书类型	创建证书的类型，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；在开启HTTPS双向认证功能时，只有当客户端能够出具指定CA签发的证书时，HTTPS连接才能成功。
证书名称	您的CA证书名称。
企业项目	企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。
证书内容	证书内容必须为PEM格式。 单击“上传”，选择上传证书文件，请确保您的浏览器是最新版本。 证书内容格式如下： -----BEGIN CERTIFICATE----- Base64-encoded certificate -----END CERTIFICATE-----
描述	添加对该证书的描述信息，非必填项。

6. 单击“确定”，完全创建。

创建服务器 SM 双证书

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏单击“证书管理”。
5. 单击“创建证书”，配置参数请参见**表1-65**。

表 1-65 服务器 SM 双证书参数说明

参数	说明
证书类型	创建证书的类型，选择服务器SM双证书。 ● 服务器证书：在使用HTTPS协议时，服务器证书用于SSL握手协商，需提供证书内容和私钥。 ● CA证书：又称客户端CA公钥证书，用于验证客户端证书的签发者；在开启HTTPS双向认证功能时，只有当客户端能够出具指定CA签发的证书时，HTTPS连接才能成功。 ● 服务器SM双证书：在使用HTTPS协议时，若采用商密SSL协议，需提供双证书。双证书包括签名证书和加密证书，需成套使用。
证书来源	服务器证书同时支持SSL证书管理服务提供的数字证书和您的自有证书。 ● SCM证书：SSL证书管理服务管理的服务器数字证书，您需要到云证书管理服务控制台签发证书或上传自有证书。 ● 自有证书：您需要在负载均衡控制台上传自有证书的证书内容和私钥。 **说明** 推荐使用云证书管理服务对您的证书进行统一管理。
证书	仅SCM证书支持该参数。 支持选择您在云证书管理服务统一管理的证书。
证书名称	仅自有证书支持该参数。 您的自有证书名称。
企业项目	企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。
SM签名证书内容	仅自有证书支持该参数。 SM签名证书内容必须为PEM格式。 单击“上传”，选择上传证书文件，请确保您的浏览器是最新版本。 证书内容格式如下： -----BEGIN CERTIFICATE----- Base64-encoded certificate -----END CERTIFICATE-----
SM签名证书私钥	仅自有证书支持该参数。 单击“上传”，选择上传私钥文件，请确保您的浏览器是最新版本。 需注意必须是无密码的私钥。符合PEM格式，私钥格式如下： -----BEGIN PRIVATE KEY----- [key] -----END PRIVATE KEY-----

参数	说明
SM加密证书内容	仅自有证书支持该参数。 SM加密证书内容必须为PEM格式。 单击“上传”，选择上传证书文件，请确保您的浏览器是最新版本。 证书内容格式如下： -----BEGIN CERTIFICATE----- Base64-encoded certificate -----END CERTIFICATE-----
SM加密证书私钥	仅自有证书支持该参数。 单击“上传”，选择上传私钥文件，请确保您的浏览器是最新版本。 需注意必须是无密码的私钥。符合PEM格式，私钥格式如下： -----BEGIN PRIVATE KEY----- [key] -----END PRIVATE KEY-----
域名	如果创建的证书用于SNI，则需要指定域名。 域名只能由字母、数字、中划线组成，中划线不能在开头或末尾，单个字符串不超过63个字符，字符串间以点分隔。 最多可支持100个域名，域名间以逗号分隔；单个域名长度不超过100个字符，且总长度不超过10000个字符。
描述	添加对该证书的描述信息，非必填项。

1.6.6.4 管理证书

操作场景

当您确认证书不需要继续使用时，您可以根据需求在弹性负载均衡控制台管理您的证书。

约束与限制

已被HTTPS监听器绑定使用的证书，无法执行删除操作，请先为关联监听器执行**更换证书**操作。

快速查询证书关联的监听器

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏单击“证书管理”。

5. 在证书列表中，在“监听器 (前端协议/端口)”所在列，单击监听器名称，即可查看监听器详细信息。

   当关联监听器数量大于5个，在“监听器 (前端协议/端口)”所在列，单击“查看所有”，单击监听器名称，即可查看监听器详细信息。

修改证书

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏单击“证书管理”。
5. 在证书列表中，在需要修改的证书所在行，单击“修改”。
6. 在“修改证书”对话框中，修改证书的相关信息。
7. 确认修改信息，单击“确定”，完成修改。

删除证书

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏单击“证书管理”。
5. 在证书列表中，在需要修改的证书所在行，单击“删除”。
6. 在确认对话框中单击“确定”，完成删除。

1.6.6.5 绑定/更换证书

操作场景

为了支持HTTPS数据传输加密认证，在创建HTTPS协议监听的时候需绑定证书，您可以参考本章节绑定证书。如果弹性负载均衡实例使用的证书过期或者其它原因需要更换，您可以参考本章节更换证书。

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

说明

弹性负载均衡的证书和私钥的更换对业务没有影响。

约束与限制

- 仅HTTPS协议的监听器才支持绑定/更换证书。
- 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。
- 切换证书后立即生效，已经建立的连接会继续使用老证书，新建立的连接将会使用新的证书。

前提条件

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

绑定证书

通过添加HTTPS监听器来绑定证书。详见**添加HTTPS监听器**。

更换证书

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要修改HTTPS监听器的负载均衡名称。
5. 在“监听器”页签下，单击目标监听器所在行操作列的“编辑”。
6. 在“服务器证书”或“CA证书”下选择需要更换的证书。
7. 在“编辑监听器”对话框中，单击“确定”。

1.6.6.6 批量更换证书

操作场景

如果使用的证书过期或者其它原因需要更换，您可以通过修改证书功能批量更换监听器所绑定的证书。

说明

弹性负载均衡的证书和私钥的更换对业务没有影响。

约束与限制

- 只有HTTPS协议的监听器才支持绑定/更换证书，TCP/UDP/HTTP协议的监听器不支持绑定/更换证书。
- 切换证书后立即生效。已经建立的连接会继续使用老证书，新建立的连接将会使用新的证书。
- 证书管理既支持在华为云购买的证书，也支持您自己生成的证书。

修改证书

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏单击“证书管理”。
5. 在证书列表中，在需要修改的证书所在行，单击“修改”。
6. 在“修改证书”对话框中，修改证书的相关信息。

7. 确认修改信息，单击“确定”，完成修改。

1.6.7 敏感操作保护

操作场景

弹性负载均衡支持敏感操作保护，在控制台进行敏感操作时，需要输入一种能证明身份的凭证，身份验证通过后方可进行相关操作。为了账号安全，建议开启操作保护功能。

该功能只有管理员可配置，对账号以及账号下的用户的资源都生效。普通用户只有查看权限，不能对其进行设置，如需修改，请联系管理员为您操作或添加权限。

开启操作保护

操作保护默认关闭，您可以参考以下步骤开启操作保护。

1. 登录管理控制台。
2. 在“控制台”页面，鼠标移动至右上方的用户名，在下拉列表中选择“安全设置”。

图 1-31 安全设置

3. 在“安全设置”页面中，选择“敏感操作 > 操作保护 > 立即启用”。

图 1-32 敏感操作

4. 在“操作保护设置”页面中，选择“开启”，单击“确定”后，开启操作保护。

   开启后，您以及账号中的IAM用户进行敏感操作时，例如删除弹性云服务器资源，需要输入验证码进行验证，避免误操作带来的风险和损失。

说明

- 用户如果进行敏感操作，将进入“操作保护”页面，选择认证方式，包括邮箱、手机和虚拟MFA三种认证方式。
  - 如果用户只绑定了手机，则认证方式只能选择手机。
  - 如果用户只绑定了邮箱，则认证方式只能选择邮件。
  - 如果用户未绑定邮箱、手机和虚拟MFA，进行敏感操作时，华为云将提示用户绑定邮箱、手机或虚拟MFA。
- 如需修改验证手机、邮箱、虚拟MFA设备，请在账号中修改。

验证操作保护

当您已经开启操作保护，在进行敏感操作时，系统会先进行操作保护验证：

- 若您绑定了邮箱，需输入邮箱验证码。
- 若您绑定了手机，需输入手机验证码。
- 若您绑定了虚拟MFA，需输入MFA设备上的6位动态验证码。

如图 操作保护身份验证所示，尝试删除负载均衡器时，弹出以下验证框，选择一种验证方式：

图 1-33 操作保护身份验证

关闭操作保护

如需关闭操作保护，请参考以下步骤操作。

1. 登录管理控制台。
2. 在“控制台”页面，鼠标移动至右上方的用户名，在下拉列表中选择“安全设置”。

图 1-34 安全设置

3. 在“安全设置”页面中，选择“敏感操作 > 操作保护 > 立即修改”。

图 1-35 修改敏感操作

4. 在“操作保护设置”页面中，选择“关闭”，单击“确定”后，关闭操作保护。

相关链接

- 如何绑定虚拟MFA设备?
- 如何获取MFA验证码?

1.7 访问日志

操作场景

在您使用七层（应用型）ELB期间，ELB的访问日志功能支持查看和分析对七层负载均衡进行请求的详细访问日志记录，包括请求时间、客户端IP地址、请求路径和服务器响应等。

如果您遇到后端服务器导致的业务故障或异常，您可以查看访问弹性负载均衡的详细日志记录，分析负载均衡的响应状态码，快速定位异常的后端服务器。

说明

由于弹性负载均衡会将访问日志等运维数据内容展示到云日志服务控制台，请您在使用过程中，注意您的隐私及敏感信息数据保护，不建议将隐私或敏感数据通过访问日志涉及的的字段传输，必要时请加密保护。

约束与限制

- 仅七层（应用型）负载均衡器支持配置访问日志。
- 客户订阅的访问日志中不包含返回码为400的请求，因为该类请求不符合HTTP规范，无法被正常处理。

前提条件

- 您已经创建了七层（应用型）负载均衡器。具体操作，请参见**创建独享型负载均衡器**。
- 您已经开通了云日志服务。具体操作，请参见**开始使用云日志服务**。
- 您已经创建了后端服务器组并且已添加后端服务器，在后端服务器中已部署了业务。具体操作，请参见**创建后端服务器组**。
- 您已经在ELB中创建了HTTP或HTTPS监听器。具体操作，请参见**添加HTTP监听器**或**添加HTTPS监听器**。

操作流程

图 1-36 定位异常后端服务器操作流程

创建日志组

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
   区域和项目选择“华北-北京四”。
3. 单击页面左上角的 ，选择“管理与监管 > 云日志服务”。
4. 单击左侧导航栏“日志管理”。
5. 单击 “创建日志组”，在弹出框内，输入日志组名称。

图 1-37 创建日志组

6. 单击“确定”，创建完成。

创建日志流

1. 在云日志服务管理控制台，单击日志组名称对应的 按钮。
2. 单击“创建日志流”，在弹出框内，输入日志流名称。

图 1-38 创建日志流

3. 单击“确定”，创建完成。

配置访问日志

1. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
2. 在“负载均衡器”界面，单击需要配置访问日志的负载均衡器名称。
3. 在该负载均衡器界面的“访问日志”页签，单击“配置访问日志”。
4. 开启日志记录，选择您在云日志服务中创建的日志组和日志流。

图 1-39 配置 ELB 访问日志

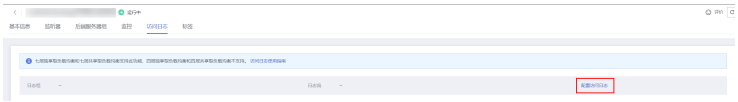


图 1-40 配置 ELB 访问日志

5. 单击“确定”，配置完成。

须知

确保创建的云日志组的地域和负载均衡器的地域相同。

查看访问日志

您可以通过以下两种方式查看访问日志的详细信息：

- “弹性负载均衡”控制台，进入访问日志界面，即可查看访问日志。
- （推荐）“云日志服务”控制台，在日志组列表，单击查看目标日志组。进入日志组详情页，在相应日志流名称所在行，单击看目标日志流的日志详情。

日志显示格式如下所示，不支持修改日志格式。

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

日志示例如下：

```
1644819836.370 eb11c5a9-93a7-4c48-80fc-03f61f638595 [2022-02-14T14:23:56+08:00] elb_01
192.168.1.1:888 200 "POST https://www.test.com/example/ HTTP/1.1" 1411 251 3 0.011 "200" "0.000"
```

```
"0.011" "0.011" "192.168.1.2:8080" "okhttp/3.13.1" "-" "-"
loadbalancer_295a7eee-9999-46ed-9fad-32a62ff0a687 listener_20679192-8888-4e62-a814-a2f870f62148
3333fd44fe3b42cbaa1dc2c641994d90 pool_89547549-6666-446e-9dbc-e3a551034c46 "-"
f2bc165ad9b4483a9b17762da851bbbb 121.64.212.1:443 "10.1.1.2:8080" - TLSv1.2 ECDHE-RSA-AES256-
GCM-SHA384 www.test.com 56704 -
```

日志字段说明如表1-66。

表 1-66 字段说明

参数	描述	取值说明	示例取值
msec	以秒为单位的时间，日志写入时的分辨率为毫秒。	浮点型数据	1644819836.370
access_log_topic_id	访问日志流ID。	uuid	eb11c5a9-93a7-4c48-80fc-03f61f638595
time_iso8601	日志写入时的时间，采用ISO 8601标准格式本地时间。	-	[2022-02-14T14:23:56+08:00]
log_ver	ELB服务日志版本号。	固定值：elb_01	elb_01
remote_addr: remote_port	客户端IP地址：客户端端口。	记录客户端IP地址和客户端端口号。	192.168.1.1:888
status	ELB响应的状态码。	记录请求状态码。	200
request_method scheme://host request_uri server_protocol	请求方法。请求方式：//主机名：请求URI 请求协议。	• request_method：请求方法。 • scheme: http或https。 • host: 主机名，可能为域名或者IP。 • request_uri：浏览器发起的不做任何修改的原生URI。不包括协议及主机名。	"POST https://www.test.com/example/ HTTP/1.1"
request_length	从客户端收到的请求长度（包括请求header和请求body）。	整型数据	1411
bytes_sent	发送到客户端的字节数 。	整型数据	251
body_bytes_sent	发送到客户端的字节数（不包括响应头）。	整型数据	3

参数	描述	取值说明	示例取值
request_time	请求处理时间，即ELB收到第一个客户端请求报文到ELB发送完响应报文的时间间隔（单位：秒）。	浮点型数据	0.011
upstream_status	从上游服务器获得的响应状态码，当ELB代理进行请求重试时会包含多个响应的状态码，当请求未被正确转发到后端服务器时此字段为 -。	后端返回给ELB的状态码	"200"
upstream_connect_time	与上游服务器建立连接所花费的时间，时间以秒为单位，分辨率为毫秒。当ELB代理进行请求重试时会包含多个连接的时间，当请求未被正确转发到后端服务器时此字段为 -。	浮点型数据	"0.000"
upstream_header_time	从上游服务器接收响应头所花费的时间，时间以秒为单位，分辨率为毫秒。当ELB代理进行请求重试时会包含多个响应时间，当请求未被正确转发到后端服务器时此字段为 -。	浮点型数据	"0.011"
upstream_response_time	从上游服务器接收响应所花费的时间，时间以秒为单位，分辨率为毫秒。当ELB代理进行请求重试时会包含多个响应时间，当请求未被正确转发到后端服务器时此字段为 -。	浮点型数据	"0.011"
upstream_addr	后端主机的IP地址和端口号。可能有多个值，每个值都是ip:port或者-，用逗号空格隔开。	IP地址+端口号	"192.168.1.2:8080" （实际日志可能有多个值，每个值都是ip:port或者-,用逗号空格隔开）

参数	描述	取值说明	示例取值
http_user_agent	ELB收到请求头中的http_user_agent内容，表示客户端的系统型号、浏览器信息等。	记录浏览器的相关信息	"okhttp/3.13.1"
http_referer	ELB收到请求头中的http_referer内容，表示该请求所在的页面链接。	页面链接请求	"-"
http_x_forwarded_for	ELB收到请求头中的http_x_forwarded_for内容，表示请求经过的代理服务器IP地址。	IP地址	"-"
lb_name	负载均衡器的名称（格式为“loadbalancer_”+“负载均衡器ID”）。	字符串	loadbalancer_295a7eee-9999-46ed-9fad-32a62ff0a687
listener_name	监听器的名称（格式为“listener_”+“监听器ID”）。	字符串	listener_2067919 2-8888-4e62-a814-a2f870f62148
listener_id	监听器在ELB服务内部的ID（客户可忽略）。	字符串	3333fd44fe3b42cbaa1dc2c641994d90
pool_name	后端服务器组名称（格式为“pool_”+“后端服务器组ID”）。	字符串	pool_89547549-6666-446e-9dbc-e3a551034c46
member_name	后端服务器的名称（格式为“member_”+“服务器ID”，尚未支持）。可能有多个值，每个值都是member_id或者-，用逗号空格隔开。	字符串	"-" (实际日志可能有多个值，每个值都是member_id或者-，用逗号空格隔开)
tenant_id	租户ID。	字符串	f2bc165ad9b4483a9b17762da851bbbb
eip_address:eip_port	弹性IP地址和监听器监听的端口号。	弹性IP地址和监听器监听的端口号。	121.64.212.1:443

参数	描述	取值说明	示例取值
upstream_addr_priv	后端主机的IP地址和端口号。可能有多个值，每个值都是ip:port或者-，用逗号空格隔开。	IP地址+端口号	"-" （独享型负载均衡为"-"）
certificate_id	[HTTPS监听器]SSL连接建立时使用的证书ID（尚未支持）。	字符串	-
ssl_protocol	[HTTPS监听器]SSL连接建立使用的协议，非HTTPS监听器，此字段为 -。	字符串	TLSv1.2
ssl_cipher	[HTTPS监听器]SSL连接建立使用的加密套件，非HTTPS监听器，此字段为 -。	字符串	ECDHE-RSA-AES256-GCM-SHA384
sni_domain_name	[HTTPS监听器]SSL握手时客户端提供的SNI域名，非HTTPS监听器，此字段为 -。	字符串	www.test.com
tcpinfo_rtt	ELB与客户端之间的tcp rtt时间，单位：微秒。	整型数据	56704
self_defined_header	该字段为保留字段，默认为“-”。	字符串	-

日志分析示例：

在[2022-02-14T14:23:56+08:00]时，ELB接收到客户端地址和端口（192.168.1.1:888）发起的“POST /HTTP/1.1”请求，ELB将请求转发给后端服务器（100.64.0.129:8080），后端服务器响应状态码200，ELB最终向客户端响应状态码200。

分析结果：

后端服务器正常响应请求。

定位异常后端服务器

筛选异常日志如下：

```
1554944564.344 - [2019-04-11T09:02:44+08:00] elb 10.133.251.171:51527 500 "GET http://10.154.73.58/lrange/guestbook HTTP/1.1" 411 3726 3545 19.028 "500" "0.009" "19.028" "19.028" "172.17.0.82:3000" "Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36" "http://10.154.73.58:5971/" "-" loadbalancer_ed0f790b-e194-4657-9f97-53426227099e listener_b21dd0a9-690a-4945-950e-b134095c6bd9 6b6aaf84d72b40fcb2d2b9b28f6a0b83
```

分析日志：

在 [2019-04-11T09:02:44+08:00 时，ELB接收到客户端地址和端口（10.133.251.171:51527）发起的 “GET / HTTP/1.1” 请求，ELB将请求转发给后端服务器（172.17.0.82:3000）处理，后端服务器响应状态码500。ELB最终向客户端响应状态码500。

分析结果：

后端服务器（172.17.0.82:3000）异常，不能正常响应请求。

说明

“172.17.0.82:3000”是后端服务器的私网IP。

配置日志转储

如果您希望将日志转储进行二次分析，您可以参考本章设置日志转储。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“管理与监管 > 云日志服务”。
4. 在左侧导航栏，单击“日志转储”。
5. 在日志转储页面，单击“配置转储”。

图 1-41 配置日志转储

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

1.8 资源和标签

1.8.1 标签管理

操作场景

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

如果您的组织已经设定弹性负载均衡的相关标签策略，则需按照标签策略规则为弹性负载均衡添加标签。标签如果不符合标签策略的规则，则可能会导致弹性负载均衡创建失败，请联系组织管理员了解标签策略详情。

为负载均衡器添加标签

给负载均衡器添加标签有以下两种方法。

- 在创建负载均衡器的时候，输入标签的“键”和“值”。
  操作步骤和配置参数，请参见**创建独享型负载均衡器**。
- 给已创建的负载均衡器添加标签。
  a. 登录管理控制台。
  b. 在管理控制台左上角单击 图标，选择区域和项目。
  c. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
  d. 在“负载均衡器”界面，单击已创建的负载均衡器名称。
  e. 在“标签”页签下，单击“添加标签”，输入“键”和“值”。
  f. 确认正确，单击“确认”。

  说明

  - 一个负载均衡器最多可以增加20个标签。
  - 标签的“键”和“值”是一一对应的，其中“键”值是唯一的。

为监听器添加标签

给已创建的监听器添加标签的方法如下：

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击已创建的负载均衡器名称。
5. 切换到监听器页签，单击需要添加标签的监听器名称。
6. 切换到监听器子页面的标签页签，单击“添加标签”，输入“键”和“值”。
7. 确认正确，单击“确认”。

说明

- 一个监听器最多可以增加20个标签。
- 标签的“键”和“值”是一一对应的，其中“键”值是唯一的。

修改标签

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要修改标签的负载均衡器名称。
5. 在“标签”页签下，在需要修改的标签所在行，单击“编辑”，输入修改的“值”。

说明

“键”值不支持修改。

6. 确认正确，单击“确认”。

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

删除标签

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要删除标签的负载均衡器名称。
5. 在“标签”页签下，在需要删除的标签所在行，单击 "删除"。
6. 确认正确，单击“确认”。

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

1.8.2 关于配额

什么是配额?

为防止资源滥用，平台限定了各服务资源的配额，对用户的资源数量和容量做了限制。如您最多可以创建多少台弹性云服务器、多少块云硬盘。

如果当前资源配额限制无法满足使用需要，您可以申请扩大配额。

怎样查看我的配额?

1. 登录管理控制台。
2. 单击管理控制台左上角的 ，选择区域和项目。
3. 在页面右上角，选择“资源 > 我的配额”。
   系统进入“服务配额”页面。

   图 1-42 我的配额

4. 您可以在“服务配额”页面，查看各项资源的总配额及使用情况。
   如果当前配额不能满足业务要求，请参考后续操作，申请扩大配额。

如何申请扩大配额?

1. 登录管理控制台。
2. 在页面右上角，选择“资源 > 我的配额”。
   系统进入“服务配额”页面。

   图 1-43 我的配额

3. 在页面右上角，单击“申请扩大配额”。

   图 1-44 申请扩大配额

4. 在“新建工单”页面，根据您的需求，填写相关参数。
   其中，“问题描述”项请填写需要调整的内容和申请原因。
5. 填写完毕后，勾选协议并单击“提交”。

1.9 使用 CES 监控 ELB

1.9.1 监控弹性负载均衡

使用场景

用户在使用ELB的过程中有了解业务负载详情的需求，为使用户更好地掌握ELB的流量负载情况，华为云提供了立体化监控平台云监控服务（CES）。通过云监控服务用户可以执行自动实时监控、告警和通知操作，帮助用户实时掌握通过ELB负载的运行情况。

云监控服务不需要开通，会在用户创建云服务资源后自动启动。关于云监控服务的更多介绍，请参见**云监控服务产品介绍**。

设置告警规则

在自动实时监控的基础上，您可以在云监控服务中设置告警规则，规定在某些特殊情况出现时向您发送告警通知。

设置ELB监控信息告警规则的方法，请参见**创建告警规则和通知**。

云监控服务还支持事件类型数据上报、查询和告警的功能。方便您将业务中的各类重要事件或对云资源的操作事件收集到云监控服务，并在事件发生时进行告警。创建ELB事件监控的告警通知的方法，请参见**创建事件监控的告警通知**。

查看监控指标

云监控服务对**弹性负载均衡监控指标说明**进行实时监控，您可以在弹性负载均衡控制台或云监控服务控制台查看各项指标的详细监控数据。

在 ELB 服务控制台查看监控指标

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要查看监控指标的负载均衡器名称。
5. 支持查看“负载均衡器”和“监听器”粒度的监控指标。
   a. 负载均衡器粒度：切换到“监控”页签，监控粒度选择“负载均衡器”进行查看。
   b. 您可以通过以下两种操作入口查看监听器粒度的监控指标：
      i. 切换到“监控”页签，监控粒度选择“监听器”并选定目标监听器后进行查看。
      ii. 单击目标监听器名称，切换到“监控”页签，查看监听器的监控指标。

在 CES 服务控制台查看监控指标

在CES控制台查看ELB监控指标详情的方法，请参见**查看云服务监控指标**。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“管理与监管 > 云监控服务”。
4. 在左侧导航树选择“云服务监控 > 弹性负载均衡”。
5. 在“云服务监控”页面，单击需要查看监控指标的负载均衡器名称。或单击目标负载均衡器右侧操作列的“查看监控指标”。
6. 选择需要查看监控指标的时间段。支持选择系统定义的时间段（如“近1小时”），或自定义时间段。
7. 单击右上角的“设置监控指标”，设置需要查看的监控指标。

查看事件监控数据

云监控服务对**ELB支持的监控事件**进行实时监控，您可以在云监控服务控制台查看事件的详细数据。

查看ELB监控事件的方法，请参见**查看事件监控数据**。

1.9.2 弹性负载均衡监控指标说明

功能说明

本节定义了弹性负载均衡服务上报云监控的监控指标的命名空间，监控指标列表和维度定义。您可以在云监控服务控制台**查看弹性负载均衡服务上报的监控指标**以及产生告警信息。

命名空间

SYS.ELB

监控指标

独享型负载均衡全面支持负载均衡器、监听器、后端服务器组和可用区等多维度的监控。当前后端服务器组维度的监控仅支持7层协议。

表 1-67 独享型负载均衡器的监控指标

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
m1_cps	并发连接数	在四层负载均衡器中，指从测量对象到后端服务器建立的所有TCP和UDP连接的数量。 在七层负载均衡器中，指从客户端到ELB建立的所有TCP连接的数量。 单位：个	≥ 0个	独享型负载均衡器	1分钟
m2_act_conn	活跃连接数	从测量对象到后端服务器建立的所有**ESTABLISHED**状态的TCP或UDP连接的数量。 Windows和Linux服务器都可以使用如下命令查看。 `netstat -an` 单位：个	≥ 0个	独享型负载均衡器	1分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
m3_inact_conn	非活跃连接数	从测量对象到所有后端服务器建立的所有除**ESTABLISHED**状态之外的TCP连接的数量。 Windows和Linux服务器都可以使用如下命令查看。 `netstat -an` 单位：个	≥ 0个	独享型负载均衡器	1分钟
m4_ncps	新建连接数	从客户端到测量对象每秒新建立的连接数。 单位：个/秒	≥ 0个/秒	独享型负载均衡器	1分钟
m5_in_pps	流入数据包数	测量对象每秒接收到的数据包的个数。 单位：个/秒	≥ 0个/秒	独享型负载均衡器	1分钟
m6_out_pps	流出数据包数	测量对象每秒发出的数据包的个数。 单位：个/秒	≥ 0个/秒	独享型负载均衡器	1分钟
m7_in_Bps	网络流入速率	从外部访问测量对象所消耗的流量。 单位：字节/秒	≥ 0bytes/s	独享型负载均衡器	1分钟
m8_out_Bps	网络流出速率	测量对象访问外部所消耗的流量。 单位：字节/秒	≥ 0bytes/s	独享型负载均衡器	1分钟
m9_abnormal_servers	异常主机数	健康检查统计监控对象后端异常的主机个数。 单位：个	≥ 0个	独享型负载均衡器	1分钟
ma_normal_servers	正常主机数	健康检查统计监控对象后端正常的主机个数。 单位：个	≥ 0个	独享型负载均衡器	1分钟
m22_in_bandwidth	入网带宽	统计测量对象当前入网带宽。 单位：比特/秒	≥ 0bit/s	独享型负载均衡器	1分钟
m23_out_bandwidth	出网带宽	统计测量对象当前出网带宽。 单位：比特/秒	≥ 0bit/s	独享型负载均衡器	1分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
m26_in_bandwidth_ipv6	ipv6入网带宽	统计流入测量对象消耗的IPv6网络带宽 单位：比特/秒	≥ 0bit/s	独享型负载均衡器	1分钟
m27_out_bandwidth_ipv6	ipv6出网带宽	统计流出测量对象消耗的IPv6网络带宽 单位：比特/秒	≥ 0bit/s	独享型负载均衡器	1分钟
m1e_server_rps	后端服务器重置数量	统计后端服务器发送至客户端的重置（RST）数据包的计数。这些重置数据包由后端服务器生成，然后由负载均衡器转发。 （仅TCP监听器支持此指标） 单位：个/秒	≥ 0个/秒	独享型负载均衡器	1分钟
m21_client_rps	客户端重置数量	统计客户端发送至后端服务器的重置（RST）数据包的计数。这些重置数据包由客户端生成，然后由负载均衡器转发。 （仅TCP监听器支持此指标） 单位：个/秒	≥ 0个/秒	独享型负载均衡器	1分钟
m1f_lvs_rps	负载均衡器重置数量	统计负载均衡器生成的重置（RST）数据包的计数。 （仅TCP监听器支持此指标） 单位：个/秒	≥ 0个/秒	独享型负载均衡器	1分钟
mb_l7_qps	7层查询速率	统计测量对象当前7层查询速率。 （仅HTTP和HTTPS监听器支持此指标） 单位：个/秒	≥ 0个/秒	独享型负载均衡器	1分钟
mc_l7_http_2xx	7层协议返回码(2XX)	统计测量对象当前7层2XX系列状态响应码的数量。 （仅HTTP和HTTPS监听器支持此指标） 单位：个/秒	≥ 0个/秒	独享型负载均衡器	1分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
md_l7_http_3xx	7层协议返回码(3XX)	统计测量对象当前7层3XX系列状态响应码的数量。 （仅HTTP和HTTPS监听器支持此指标） 单位：个/秒	≥ 0个/秒	独享型负载均衡器	1分钟
me_l7_http_4xx	7层协议返回码(4XX)	统计测量对象当前7层4XX系列状态响应码的数量。 （仅HTTP和HTTPS监听器支持此指标） 单位：个/秒	≥ 0个/秒	独享型负载均衡器	1分钟
mf_l7_http_5xx	7层协议返回码(5XX)	统计测量对象当前7层5XX系列状态响应码的数量。 （仅HTTP和HTTPS监听器支持此指标） 单位：个/秒	≥ 0个/秒	独享型负载均衡器	1分钟
m10_l7_http_other_status	7层协议返回码(Others)	统计测量对象当前7层非2XX,3XX,4XX,5XX系列状态响应码的数量。 （仅HTTP和HTTPS监听器支持此指标） 单位：个/秒	≥ 0个/秒	独享型负载均衡器	1分钟
m11_l7_http_404	7层协议返回码(404)	统计测量对象当前7层404状态响应码的数量。 （仅HTTP和HTTPS监听器支持此指标） 单位：个/秒	≥ 0个/秒	独享型负载均衡器	1分钟
m12_l7_http_499	7层协议返回码(499)	统计测量对象当前7层499状态响应码的数量。 （仅HTTP和HTTPS监听器支持此指标） 单位：个/秒	≥ 0个/秒	独享型负载均衡器	1分钟
m13_l7_http_502	7层协议返回码(502)	统计测量对象当前7层502状态响应码的数量。 （仅HTTP和HTTPS监听器支持此指标） 单位：个/秒	≥ 0个/秒	独享型负载均衡器	1分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
m14_l7_rt	7层协议RT平均值	统计测量对象当前7层平均响应时间。 （仅HTTP和HTTPS监听器支持此指标） 从测量对象收到客户端请求开始，到测量对象将所有响应返回给客户端为止。 单位：毫秒 **说明** websocket场景下RT平均值可能会非常大，此时该指标无法作为时延指标参考。	≥ 0ms	独享型负载均衡器	1分钟
m15_l7_upstream_4xx	7层后端返回码(4XX)	统计测量对象当前7层后端4XX系列状态响应码的数量。 （仅HTTP和HTTPS监听器支持此指标） 单位：个/秒	≥ 0个/秒	独享型负载均衡器	1分钟
m16_l7_upstream_5xx	7层后端返回码(5XX)	统计测量对象当前7层后端5XX系列状态响应码的数量。 （仅HTTP和HTTPS监听器支持此指标） 单位：个/秒	≥ 0个/秒	独享型负载均衡器	1分钟
m17_l7_upstream_rt	7层后端的RT平均值	统计测量对象当前7层后端平均响应时间。 从测量对象将请求转发给后端服务器开始，到测量对象收到后端服务器返回响应为止。 （仅HTTP和HTTPS监听器支持此指标） 单位：毫秒 **说明** websocket场景下RT平均值可能会非常大，此时该指标无法作为时延指标参考。	≥ 0ms	独享型负载均衡器	1分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
m1a_l7_upstream_rt_max	7层后端的RT最大值	统计测量对象当前7层后端最大响应时间。 从测量对象将请求转发给后端服务器开始，到测量对象收到后端服务器返回响应为止。 （仅HTTP和HTTPS监听器支持此指标） 单位：毫秒	≥ 0ms	独享型负载均衡器	1分钟
m1b_l7_upstream_rt_min	7层后端的RT最小值	统计测量对象当前7层后端最小响应时间。 从测量对象将请求转发给后端服务器开始，到测量对象收到后端服务器返回响应为止。 （仅HTTP和HTTPS监听器支持此指标） 单位：毫秒	≥ 0ms	独享型负载均衡器	1分钟
m1c_l7_rt_max	7层协议的RT最大值	统计测量对象当前7层最大响应时间。 从测量对象收到客户端请求开始，到测量对象将所有响应返回给客户端为止。 （仅HTTP和HTTPS监听器支持此指标） 单位：毫秒	≥ 0ms	独享型负载均衡器	1分钟
m1d_l7_rt_min	7层协议的RT最小值	统计测量对象当前7层最小响应时间。 从测量对象收到客户端请求开始，到测量对象将所有响应返回给客户端为止。 （仅HTTP和HTTPS监听器支持此指标） 单位：毫秒	≥ 0ms	独享型负载均衡器	1分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
m25_l7_resp_Bps	7层响应带宽	统计周期时间内主机组的响应发送带宽。 单位：比特/秒 **说明** 当监听器开启HTTP/2时，该指标无法作为参考。	≥ 0bit/s	独享型负载均衡器	1分钟
m24_l7_req_Bps	7层请求带宽	统计周期时间内主机组的请求接收带宽。 单位：比特/秒 **说明** 当监听器开启HTTP/2时，该指标无法作为参考。	≥ 0bit/s	独享型负载均衡器	1分钟
l7_con_usage	7层并发连接使用率	统计7层的ELB实例并发连接数使用率。 单位：百分比	≥ 0%	独享型负载均衡器	1分钟
l7_in_bps_usage	7层入带宽使用率	统计7层的ELB实例入带宽使用率。 单位：百分比 **注意** 若入带宽使用率达到100%，说明已经超出ELB规格所提供的性能保障，您的业务可以继续使用更高带宽，但对于带宽超出的部分，ELB无法承诺服务可用性指标。	≥ 0%	独享型负载均衡器	1分钟
l7_out_bps_usage	7层出带宽使用率	统计7层的ELB实例出带宽使用率。 单位：百分比 **注意** 若出带宽使用率达到100%，说明已经超出ELB规格所提供的性能保障，您的业务可以继续使用更高带宽，但对于带宽超出的部分，ELB无法承诺服务可用性指标。	≥ 0%	独享型负载均衡器	1分钟
l7_ncps_usage	7层新建连接数使用率	统计7层的ELB实例新建连接数使用率。 单位：百分比	≥ 0%	独享型负载均衡器	1分钟
l7_qps_usage	7层查询速率使用率	统计7层的ELB实例查询速率使用率。 单位：百分比	≥ 0%	独享型负载均衡器	1分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
l4_con_usage	4层并发连接使用率	统计4层的ELB实例并发连接数使用率。 单位：百分比	≥ 0%	独享型负载均衡器	1分钟
l4_in_bps_usage	4层入带宽使用率	统计4层的ELB实例入带宽使用率。 单位：百分比 **注意** 若入带宽使用率达到100%，说明已经超出ELB规格所提供的性能保障，您的业务可以继续使用更高带宽，但对于带宽超出的部分，ELB无法承诺服务可用性指标。	≥ 0%	独享型负载均衡器	1分钟
l4_out_bps_usage	4层出带宽使用率	统计4层的ELB实例出带宽使用率。 单位：百分比 **注意** 若出带宽使用率达到100%，说明已经超出ELB规格所提供的性能保障，您的业务可以继续使用更高带宽，但对于带宽超出的部分，ELB无法承诺服务可用性指标。	≥ 0%	独享型负载均衡器	1分钟
l4_ncps_usage	4层新建连接数使用率	统计4层的ELB实例新建连接数使用率。 单位：百分比	≥ 0%	独享型负载均衡器	1分钟
elb_http_2xx	负载均衡2xx状态响应码	统计负载均衡平均每秒返回2xx状态响应码的数量	≥ 0个/秒	独享型负载均衡器	1分钟
elb_http_3xx	负载均衡3xx状态响应码	统计负载均衡平均每秒返回3xx状态响应码的数量	≥ 0个/秒	独享型负载均衡器	1分钟
elb_http_4xx	负载均衡4xx状态响应码	统计负载均衡平均每秒返回4xx状态响应码的数量	≥ 0个/秒	独享型负载均衡器	1分钟
elb_http_400	负载均衡400状态响应码	统计负载均衡平均每秒返回400状态响应码的数量	≥ 0个/秒	独享型负载均衡器	1分钟
elb_http_404	负载均衡404状态响应码	统计负载均衡平均每秒返回404状态响应码的数量	≥ 0个/秒	独享型负载均衡器	1分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
elb_http_408	负载均衡408状态响应码	统计负载均衡平均每秒返回408状态响应码的数量	≥ 0个/秒	独享型负载均衡器	1分钟
elb_http_499	负载均衡499状态响应码	统计负载均衡平均每秒返回499状态响应码的数量	≥ 0个/秒	独享型负载均衡器	1分钟
elb_http_5xx	负载均衡5xx状态响应码	统计负载均衡平均每秒返回5xx状态响应码的数量	≥ 0个/秒	独享型负载均衡器	1分钟
elb_http_502	负载均衡502状态响应码	统计负载均衡平均每秒返回502状态响应码的数量	≥ 0个/秒	独享型负载均衡器	1分钟
elb_http_503	负载均衡503状态响应码	统计负载均衡平均每秒返回503状态响应码的数量	≥ 0个/秒	独享型负载均衡器	1分钟
elb_http_504	负载均衡504状态响应码	统计负载均衡平均每秒返回504状态响应码的数量	≥ 0个/秒	独享型负载均衡器	1分钟

表 1-68 监听器支持的监控指标（独享型）

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
m1_cps	并发连接数	在四层负载均衡器中，指从测量对象到后端服务器建立的所有TCP和UDP连接的数量。 在七层负载均衡器中，指从客户端到ELB建立的所有TCP连接的数量。 单位：个	≥ 0个	监听器（独享型）	1分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
m2_act_conn	活跃连接数	从测量对象到后端服务器建立的所有**ESTABLISHED**状态的TCP或UDP连接的数量。 Windows和Linux服务器都可以使用如下命令查看。 `netstat -an` 单位：个	≥ 0个	监听器（独享型）	1分钟
m3_inact_conn	非活跃连接数	从测量对象到所有后端服务器建立的所有除**ESTABLISHED**状态之外的TCP连接的数量。 Windows和Linux服务器都可以使用如下命令查看。 `netstat -an` 单位：个	≥ 0个	监听器（独享型）	1分钟
m4_ncps	新建连接数	从客户端到测量对象每秒新建立的连接数。 单位：个/秒	≥ 0个/秒	监听器（独享型）	1分钟
m5_in_pps	流入数据包数	测量对象每秒接收到的数据包的个数。 单位：个/秒	≥ 0个/秒	监听器（独享型）	1分钟
m6_out_pps	流出数据包数	测量对象每秒发出的数据包的个数。 单位：个/秒	≥ 0个/秒	监听器（独享型）	1分钟
m7_in_Bps	网络流入速率	从外部访问测量对象所消耗的流量。 单位：字节/秒	≥ 0bytes/s	监听器（独享型）	1分钟
m8_out_Bps	网络流出速率	测量对象访问外部所消耗的流量。 单位：字节/秒	≥ 0bytes/s	监听器（独享型）	1分钟
m9_abnormal_servers	异常主机数	健康检查统计监控对象后端异常的主机个数。 单位：个	≥ 0个	监听器（独享型）	1分钟
ma_normal_servers	正常主机数	健康检查统计监控对象后端正常的主机个数。 单位：个	≥ 0个	监听器（独享型）	1分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
m22_in_bandwidth	入网带宽	统计测量对象当前入网带宽。 单位：比特/秒	≥ 0bit/s	监听器（独享型）	1分钟
m23_out_bandwidth	出网带宽	统计测量对象当前出网带宽。 单位：比特/秒	≥ 0bit/s	监听器（独享型）	1分钟
m1e_server_rps	后端服务器重置数量	统计后端服务器发送至客户端的重置（RST）数据包的计数。这些重置数据包由后端服务器生成，然后由负载均衡器转发。 （仅TCP监听器有此指标） 单位：个/秒	≥ 0个/秒	监听器（独享型）	1分钟
m21_client_rps	客户端重置数量	统计客户端发送至后端服务器的重置（RST）数据包的计数。这些重置数据包由客户端生成，然后由负载均衡器转发。 （仅TCP监听器有此指标） 单位：个/秒	≥ 0个/秒	监听器（独享型）	1分钟
m1f_lvs_rps	负载均衡器重置数量	统计负载均衡器生成的重置（RST）数据包的计数。 （仅TCP监听器有此指标） 单位：个/秒	≥ 0个/秒	监听器（独享型）	1分钟
mb_l7_qps	7层查询速率	统计测量对象当前7层查询速率。 （HTTP和HTTPS监听器才有此指标） 单位：个/秒。	≥ 0个/秒	监听器（独享型）	1分钟
mc_l7_http_2xx	7层协议返回码(2XX)	统计测量对象当前7层2XX系列状态响应码的数量。 （HTTP和HTTPS监听器才有此指标） 单位：个/秒。	≥ 0个/秒	监听器（独享型）	1分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
md_l7_http_3xx	7层协议返回码(3XX)	统计测量对象当前7层3XX系列状态响应码的数量。 （HTTP和HTTPS监听器才有此指标） 单位：个/秒。	≥ 0个/秒	监听器（独享型）	1分钟
me_l7_http_4xx	7层协议返回码(4XX)	统计测量对象当前7层4XX系列状态响应码的数量。 （HTTP和HTTPS监听器才有此指标） 单位：个/秒。	≥ 0个/秒	监听器（独享型）	1分钟
mf_l7_http_5xx	7层协议返回码(5XX)	统计测量对象当前7层5XX系列状态响应码的数量。 （HTTP和HTTPS监听器才有此指标） 单位：个/秒。	≥ 0个/秒	监听器（独享型）	1分钟
m10_l7_http_other_status	7层协议返回码(Others)	统计测量对象当前7层非2XX,3XX,4XX,5XX系列状态响应码的数量。（HTTP和HTTPS监听器才有此指标） 单位：个/秒。	≥ 0个/秒	监听器（独享型）	1分钟
m11_l7_http_404	7层协议返回码(404)	统计测量对象当前7层404状态响应码的数量。 （HTTP和HTTPS监听器才有此指标） 单位：个/秒。	≥ 0个/秒	监听器（独享型）	1分钟
m12_l7_http_499	7层协议返回码(499)	统计测量对象当前7层499状态响应码的数量。 （HTTP和HTTPS监听器才有此指标） 单位：个/秒。	≥ 0个/秒	监听器（独享型）	1分钟
m13_l7_http_502	7层协议返回码(502)	统计测量对象当前7层502状态响应码的数量。 （HTTP和HTTPS监听器才有此指标） 单位：个/秒。	≥ 0个/秒	监听器（独享型）	1分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
m14_l7_rt	7层协议RT平均值	统计测量对象当前7层平均响应时间。 （HTTP和HTTPS监听器才有此指标） 从测量对象收到客户端请求开始，到测量对象将所有响应返回给客户端为止。 单位：毫秒。 **说明** websocket场景下RT平均值可能会非常大，此时该指标无法作为时延指标参考。	≥ 0ms	监听器（独享型）	1分钟
m15_l7_upstream_4xx	7层后端返回码(4XX)	统计测量对象当前7层后端4XX系列状态响应码的数量。 （HTTP和HTTPS监听器才有此指标） 单位：个/秒。	≥ 0个/秒	监听器（独享型）	1分钟
m16_l7_upstream_5xx	7层后端返回码(5XX)	统计测量对象当前7层后端5XX系列状态响应码的数量。 （HTTP和HTTPS监听器才有此指标） 单位：个/秒。	≥ 0个/秒	监听器（独享型）	1分钟
m17_l7_upstream_rt	7层后端的RT平均值	统计测量对象当前7层后端平均响应时间。 （HTTP和HTTPS监听器才有此指标） 从测量对象将请求转发给后端服务器开始，到测量对象收到后端服务器返回响应为止。 单位：毫秒。 **说明** websocket场景下RT平均值可能会非常大，此时该指标无法作为时延指标参考。	≥ 0ms	监听器（独享型）	1分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
m1a_l7_upstream_rt_max	7层后端的RT最大值	统计测量对象当前7层后端最大响应时间。 （HTTP和HTTPS监听器才有此指标） 从测量对象将请求转发给后端服务器开始，到测量对象收到后端服务器返回响应为止。 单位：毫秒。	≥ 0ms	监听器（独享型）	1分钟
m1b_l7_upstream_rt_min	7层后端的RT最小值	统计测量对象当前7层后端最小响应时间。 （HTTP和HTTPS监听器才有此指标） 从测量对象将请求转发给后端服务器开始，到测量对象收到后端服务器返回响应为止。 单位：毫秒。	≥ 0ms	监听器（独享型）	1分钟
m1c_l7_rt_max	7层协议的RT最大值	统计测量对象当前7层最大响应时间。 （HTTP和HTTPS监听器才有此指标） 从测量对象收到客户端请求开始，到测量对象将所有响应返回给客户端为止。 单位：毫秒。	≥ 0ms	监听器（独享型）	1分钟
m1d_l7_rt_min	7层协议的RT最小值	统计测量对象当前7层最小响应时间。 （HTTP和HTTPS监听器才有此指标） 从测量对象收到客户端请求开始，到测量对象将所有响应返回给客户端为止。 单位：毫秒。	≥ 0ms	监听器（独享型）	1分钟

表 1-69 后端服务器组的监控指标（独享型）

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
m9_abnormal_servers	异常主机数	健康检查统计监控对象后端异常的主机个数。 单位：个	≥ 0个	后端服务器组（独享型）	1分钟
ma_normal_servers	正常主机数	健康检查统计监控对象后端正常的主机个数。 单位：个	≥ 0个	后端服务器组（独享型）	1分钟
mb_l7_qps	7层查询速率	统计测量对象当前7层查询速率。 单位：个/秒	≥ 0个/秒	后端服务器组（独享型）	1分钟
m17_l7_upstream_rt	7层后端的RT平均值	统计测量对象当前7层后端平均响应时间。 （HTTP和HTTPS监听器才有此指标） 从测量对象将请求转发给后端服务器开始，到测量对象收到后端服务器返回响应为止。 单位：毫秒 **说明** websocket场景下RT平均值可能会非常大，此时该指标无法作为时延指标参考。	≥ 0ms	后端服务器组（独享型）	1分钟
m1a_l7_upstream_rt_max	7层后端的RT最大值	统计测量对象当前7层后端最大响应时间。 （HTTP和HTTPS监听器才有此指标） 从测量对象将请求转发给后端服务器开始，到测量对象收到后端服务器返回响应为止。 单位：毫秒	≥ 0ms	后端服务器组（独享型）	1分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
m1b_l7_upstream_rt_min	7层后端的RT最小值	统计测量对象当前7层后端最小响应时间。 （HTTP和HTTPS监听器才有此指标） 从测量对象将请求转发给后端服务器开始，到测量对象收到后端服务器返回响应为止。 单位：毫秒	≥ 0ms	后端服务器组（独享型）	1分钟
m18_l7_upstream_2xx	7层后端返回码(2XX)	统计测量对象当前7层后端2XX系列状态响应码的数量。（HTTP和HTTPS监听器才有此指标） 单位：个/秒	≥ 0个/秒	后端服务器组（独享型）	1分钟
m19_l7_upstream_3xx	7层后端返回码(3XX)	统计测量对象当前7层后端3XX系列状态响应码的数量。（HTTP和HTTPS监听器才有此指标） 单位：个/秒	≥ 0个/秒	后端服务器组（独享型）	1分钟
m15_l7_upstream_4xx	7层后端返回码(4XX)	统计测量对象当前7层后端4XX系列状态响应码的数量。（HTTP和HTTPS监听器才有此指标） 单位：个/秒	≥ 0个/秒	后端服务器组（独享型）	1分钟
m16_l7_upstream_5xx	7层后端返回码(5XX)	统计测量对象当前7层后端5XX系列状态响应码的数量。 （HTTP和HTTPS监听器才有此指标） 单位：个/秒	≥ 0个/秒	后端服务器组（独享型）	1分钟
m25_l7_resp_Bps	7层响应带宽	统计周期时间内主机组的响应发送带宽。 单位：比特/秒 **说明** 当监听器开启HTTP/2时，该指标无法作为参考。	≥ 0bit/s	后端服务器组（独享型）	1分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
m24_l7_req_Bps	7层请求带宽	统计周期时间内主机组的请求接收带宽。 单位：比特/秒 **说明** 当监听器开启HTTP/2时，该指标无法作为参考。	≥ 0bit/s	后端服务器组（独享型）	1分钟

表 1-70 可用区的监控指标

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
m1_cps	并发连接数	在四层负载均衡器中，指从测量对象到后端服务器建立的所有TCP和UDP连接的数量。 在七层负载均衡器中，指从客户端到ELB建立的所有TCP连接的数量。 单位：个	≥ 0个	可用区	1分钟
m2_act_conn	活跃连接数	从测量对象到后端服务器建立的所有**ESTABLISHED**状态的TCP或UDP连接的数量。 Windows和Linux服务器都可以使用如下命令查看。 `netstat -an` 单位：个	≥ 0个	可用区	1分钟
m3_inact_conn	非活跃连接数	从测量对象到所有后端服务器建立的所有除**ESTABLISHED**状态之外的TCP连接的数量。 Windows和Linux服务器都可以使用如下命令查看。 `netstat -an` 单位：个	≥ 0个	可用区	1分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
m4_ncps	新建连接数	从客户端到测量对象每秒新建立的连接数。 单位：个/秒	≥ 0个/秒	可用区	1分钟
m5_in_pps	流入数据包数	测量对象每秒接收到的数据包的个数。 单位：个/秒	≥ 0个/秒	可用区	1分钟
m6_out_pps	流出数据包数	测量对象每秒发出的数据包的个数。 单位：个/秒	≥ 0个/秒	可用区	1分钟
m7_in_Bps	网络流入速率	从外部访问测量对象所消耗的流量。 单位：字节/秒	≥ 0bytes/s	可用区	1分钟
m8_out_Bps	网络流出速率	测量对象访问外部所消耗的流量。 单位：字节/秒	≥ 0bytes/s	可用区	1分钟
m26_in_bandwidth_ipv6	ipv6入网带宽	统计流入测量对象消耗的IPv6网络带宽 单位：比特/秒	≥ 0bit/s	可用区	1分钟
m27_out_bandwidth_ipv6	ipv6出网带宽	统计流出测量对象消耗的IPv6网络带宽 单位：比特/秒	≥ 0bit/s	可用区	1分钟
m1e_server_rps	后端服务器重置数量	统计后端服务器发送至客户端的重置（RST）数据包的计数。这些重置数据包由后端服务器生成，然后由负载均衡器转发。 （仅TCP监听器支持此指标） 单位：个/秒	≥ 0个/秒	可用区	1分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
m21_client_rps	客户端重置数量	统计客户端发送至后端服务器的重置（RST）数据包的计数。这些重置数据包由客户端生成，然后由负载均衡器转发。 （仅TCP监听器支持此指标） 单位：个/秒	≥ 0个/秒	可用区	1分钟
m1f_lvs_rps	负载均衡器重置数量	统计负载均衡器生成的重置（RST）数据包的计数。 （仅TCP监听器支持此指标） 单位：个/秒	≥ 0个/秒	可用区	1分钟
mb_l7_qps	7层查询速率	统计测量对象当前7层查询速率。 （仅HTTP和HTTPS监听器支持此指标） 单位：个/秒	≥ 0个/秒	可用区	1分钟
mc_l7_http_2xx	7层协议返回码(2XX)	统计测量对象当前7层2XX系列状态响应码的数量。 （仅HTTP和HTTPS监听器支持才有此指标） 单位：个/秒	≥ 0个/秒	可用区	1分钟
md_l7_http_3xx	7层协议返回码(3XX)	统计测量对象当前7层3XX系列状态响应码的数量。 （仅HTTP和HTTPS监听器支持此指标） 单位：个/秒	≥ 0个/秒	可用区	1分钟
me_l7_http_4xx	7层协议返回码(4XX)	统计测量对象当前7层4XX系列状态响应码的数量。 （仅HTTP和HTTPS监听器支持此指标） 单位：个/秒	≥ 0个/秒	可用区	1分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
mf_l7_http_5xx	7层协议返回码(5XX)	统计测量对象当前7层5XX系列状态响应码的数量。 （仅HTTP和HTTPS监听器支持此指标） 单位：个/秒	≥ 0个/秒	可用区	1分钟
m10_l7_http_other_status	7层协议返回码(Others)	统计测量对象当前7层非2XX,3XX,4XX,5XX系列状态响应码的数量。 （HTTP和HTTPS监听器才有此指标） 单位：个/秒	≥ 0个/秒	可用区	1分钟
m11_l7_http_404	7层协议返回码(404)	统计测量对象当前7层404状态响应码的数量。 （仅HTTP和HTTPS监听器支持此指标） 单位：个/秒	≥ 0个/秒	可用区	1分钟
m12_l7_http_499	7层协议返回码(499)	统计测量对象当前7层499状态响应码的数量。 （仅HTTP和HTTPS监听器支持此指标） 单位：个/秒	≥ 0个/秒	可用区	1分钟
m13_l7_http_502	7层协议返回码(502)	统计测量对象当前7层502状态响应码的数量。 （仅HTTP和HTTPS监听器支持此指标） 单位：个/秒	≥ 0个/秒	可用区	1分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
m14_l7_rt	7层协议RT平均值	统计测量对象当前7层平均响应时间。 （仅HTTP和HTTPS监听器支持此指标） 从测量对象收到客户端请求开始，到测量对象将所有响应返回给客户端为止。 单位：毫秒 **说明** websocket场景下RT平均值可能会非常大，此时该指标无法作为时延指标参考。	≥ 0ms	可用区	1分钟
m15_l7_upstream_4xx	7层后端返回码(4XX)	统计测量对象当前7层后端4XX系列状态响应码的数量。 （仅HTTP和HTTPS监听器支持此指标） 单位：个/秒	≥ 0个/秒	可用区	1分钟
m16_l7_upstream_5xx	7层后端返回码(5XX)	统计测量对象当前7层后端5XX系列状态响应码的数量。 （仅HTTP和HTTPS监听器支持此指标） 单位：个/秒	≥ 0个/秒	可用区	1分钟
m17_l7_upstream_rt	7层后端的RT平均值	统计测量对象当前7层后端平均响应时间。 从测量对象将请求转发给后端服务器开始，到测量对象收到后端服务器返回响应为止。 （仅HTTP和HTTPS监听器支持此指标） 单位：毫秒 **说明** websocket场景下RT平均值可能会非常大，此时该指标无法作为时延指标参考。	≥ 0ms	可用区	1分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
m1a_l7_upstream_rt_max	7层后端的RT最大值	统计测量对象当前7层后端最大响应时间。 从测量对象将请求转发给后端服务器开始，到测量对象收到后端服务器返回响应为止。 （仅HTTP和HTTPS监听器支持此指标） 单位：毫秒	≥ 0ms	可用区	1分钟
m1b_l7_upstream_rt_min	7层后端的RT最小值	统计测量对象当前7层后端最小响应时间。 从测量对象将请求转发给后端服务器开始，到测量对象收到后端服务器返回响应为止。 （仅HTTP和HTTPS监听器支持此指标） 单位：毫秒	≥ 0ms	可用区	1分钟
m1c_l7_rt_max	7层协议的RT最大值	统计测量对象当前7层最大响应时间。 从测量对象收到客户端请求开始，到测量对象将所有响应返回给客户端为止。 （仅HTTP和HTTPS监听器支持此指标） 单位：毫秒	≥ 0ms	可用区	1分钟
m1d_l7_rt_min	7层协议的RT最小值	统计测量对象当前7层最小响应时间。 从测量对象收到客户端请求开始，到测量对象将所有响应返回给客户端为止。 （仅HTTP和HTTPS监听器支持此指标） 单位：毫秒	≥ 0ms	可用区	1分钟
l4_con_usage	4层并发连接使用率	统计4层的ELB实例并发连接数使用率。 单位：百分比	≥ 0%	可用区	1分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
l4_in_bps_usage	4层入带宽使用率	统计4层的ELB实例入带宽使用率。 单位：百分比 **注意** 若入带宽使用率达到100%，说明已经超出ELB规格所提供的性能保障，您的业务可以继续使用更高带宽，但对于带宽超出的部分，ELB无法承诺服务可用性指标。	≥ 0%	可用区	1分钟
l4_out_bps_usage	4层出带宽使用率	统计4层的ELB实例出带宽使用率。 单位：百分比 **注意** 若出带宽使用率达到100%，说明已经超出ELB规格所提供的性能保障，您的业务可以继续使用更高带宽，但对于带宽超出的部分，ELB无法承诺服务可用性指标。	≥ 0%	可用区	1分钟
l4_ncps_usage	4层新建连接数使用率	统计4层的ELB实例新建连接数使用率。 单位：百分比	≥ 0%	可用区	1分钟
l7_in_bps_usage	7层入带宽使用率	统计7层的ELB实例入带宽使用率。 单位：百分比 **注意** 若入带宽使用率达到100%，说明已经超出ELB规格所提供的性能保障，您的业务可以继续使用更高带宽，但对于带宽超出的部分，ELB无法承诺服务可用性指标。	≥ 0%	可用区	1分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
l7_out_bps_usage	7层出带宽使用率	统计7层的ELB实例出带宽使用率。 单位：百分比 **注意** 若出带宽使用率达到100%，说明已经超出ELB规格所提供的性能保障，您的业务可以继续使用更高带宽，但对于带宽超出的部分，ELB无法承诺服务可用性指标。	≥ 0%	可用区	1分钟
l7_con_usage	7层并发连接使用率	统计7层的ELB实例并发连接数使用率。 单位：百分比	≥ 0%	可用区	1分钟
l7_ncps_usage	7层新建连接数使用率	统计7层的ELB实例新建连接数使用率。 单位：百分比	≥ 0%	可用区	1分钟
l7_qps_usage	7层查询速率使用率	统计7层的ELB实例查询速率使用率。 单位：百分比	≥ 0%	可用区	1分钟

维度

Key	Value
lbaas_instance_id	独享型负载均衡器的ID。
lbaas_listener_id	独享型负载均衡监听器的ID。
lbaas_pool_id	后端服务器组的ID
available_zone	独享型负载均衡器的可用区。

1.9.3 弹性负载均衡事件监控说明

事件监控概述

事件监控提供了事件类型数据上报、查询和告警的功能。方便您将业务中的各类重要事件或对云资源的操作事件收集到云监控服务，并在事件发生时进行告警。

事件即云监控服务保存并监控的弹性负载均衡资源的关键操作。您可以通过“事件”了解到谁在什么时间对系统哪些资源做了什么操作。

事件监控为您提供上报自定义事件的接口，方便您将业务产生的异常事件或重要变更事件采集上报到云监控服务。

事件监控默认开通，您可以在事件监控中查看系统事件和自定义事件的监控详情，目前支持的弹性负载均衡系统事件请参见**ELB支持的监控事件说明**。

ELB 支持的监控事件说明

目前，独享型弹性负载均衡已支持监控的事件详见**表1-71**

表 1-71 弹性负载均衡支持的事件说明

事件来源	事件名称	事件ID	事件级别	事件说明	处理建议	事件影响
ELB	健康检查异常	healthCheckUnhealthy	重要	一般是由于后端服务器服务离线导致。事件上报一定次数后，不再上报。	检查后端服务器的服务运行状态。	ELB不会往异常的后端转发流量，如果云服务器组下只有一个后端，则业务会中断。
	健康检查恢复正常	healthCheckRecovery	次要	后端服务器健康检查恢复正常。	无需处理。	负载均衡器到后端服务器流量恢复正常。

1.9.4 查看流量使用情况

应用场景

在视频直播中，网络访问流量的突增可能会引起业务的动荡，因此视频直播平台通常都会使用ELB自动分发流量到多台服务器。如果您担心流量过大引起业务问题，需要查看弹性负载均衡的使用流量，或者针对公网负载均衡，您需要查看某一时间段内弹性负载均衡绑定的EIP流量使用情况，云监控服务可以监控ELB的流量数据。

前提条件

已经正常运行了一段时间的负载均衡器。

关联的后端服务器在关机、故障、删除状态，无法在云监控中查看其监控指标。当后端服务器再次启动或恢复后，即可正常查看。

查看绑定的 EIP 使用流量

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。

3. 单击页面左上角的 ，选择“网络 > 虚拟私有云”。
4. 在左侧导航树，选择“弹性公网IP和带宽 > 弹性公网IP”。
5. 在弹性负载均衡绑定的EIP名称所在行，选择需要查看的EIP单击，切换到“带宽”页签，支持查看“近1小时”、“近3小时”、“近12小时”、“近1天”、“近7天”的数据。

图 1-45 EIP 使用流量监控结果

表 1-72 EIP 和带宽支持的监控指标

指标名称	含义	取值范围	测试对象	监控周期（原始指标）
出网带宽	该指标用于统计测试对象出云平台的网络速度（原指标为上行带宽）。	≥ 0 bits/s	带宽或弹性公网IP。	1分钟
入网带宽	该指标用于统计测试对象入云平台的网络速度（原指标为下行带宽）。	≥ 0 bits/s	带宽或弹性公网IP。	1分钟
出网带宽使用率	该指标用于统计测量对象出云平台的带宽使用率，以百分比为单位。	0-100%	带宽或弹性公网IP。	1分钟
入网带宽使用率	该指标用于统计测量对象入云平台的带宽使用率，以百分比为单位。	0-100%	带宽或弹性公网IP。	1分钟
出网流量	该指标用于统计测试对象出云平台的网络流量（原指标为上行流量）。	≥ 0 bytes	带宽或弹性公网IP。	1分钟
入网流量	该指标用于统计测试对象入云平台的网络流量（原指标为下行流量）。	≥ 0 bytes	带宽或弹性公网IP。	1分钟

查看弹性负载均衡使用流量

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要查看流量的负载均衡器名称。
5. 切换到“监控”页签，单击需要查看的监控粒度，查看网络流入速率和网络流出速率。

   支持查看“近1小时”、“近3小时”、“近12小时”、“近1天”和“近7天”的数据。

1.10 审计

1.10.1 支持审计的关键操作列表

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

云审计支持的弹性负载均衡操作事件列表如表1-73所示。

表 1-73 云审计服务支持的弹性负载均衡操作列表

操作名称	资源类型	事件名称
配置访问日志	logtank	createLogtank
删除访问日志	logtank	deleteLogtank
创建证书	certificate	createCertificate
更新证书	certificate	updateCertificate
删除证书	certificate	deleteCertificate
创建健康检查	healthmonitor	createHealthMonitor
更新健康检查	healthmonitor	updateHealthMonitor
删除健康检查	healthmonitor	deleteHealthMonitor
创建转发策略	l7policy	createL7policy
更新转发策略	l7policy	updateL7policy
删除转发策略	l7policy	deleteL7policy
创建转发规则	l7rule	createl7rule
更新转发规则	l7rule	updateL7rule
删除转发规则	l7rule	deleteL7rule
创建监听器	listener	createListener

操作名称	资源类型	事件名称
更新监听器	listener	updateListener
删除监听器	listener	deleteListener
创建负载均衡器	loadbalancer	createLoadbalancer
更新负载均衡器	loadbalancer	updateLoadbalancer
删除负载均衡器	loadbalancer	deleteLoadbalancer
添加后端云服务器	member	createMember
更新后端云服务器	member	updateMember
移除后端云服务器	member	batchUpdateMember
创建后端服务器组	pool	createPool
更新后端服务器组	pool	updatPool
删除后端服务器组	pool	deletePool

1.10.2 查看审计日志

操作场景

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

本节介绍如何在云审计服务管理控制台查看最近7天的操作记录。

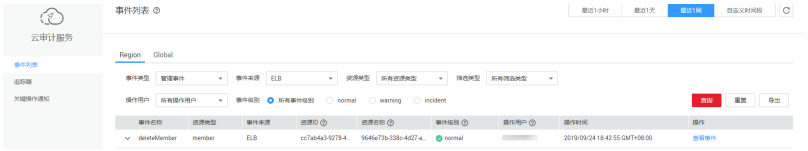
操作步骤

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

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

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

图 1-46 展开记录



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

图 1-47 查看事件

```
"context": {
    "code": "204",
    "source_ip": "10.45.152.59",
    "trace_type": "ApiCall",
    "event_type": "system",
    "project_id": "0503dda897000fed2f78c00909158a4d",
    "trace_id": "116a2aff-deb8-11e9-95f5-d5c0b02a9b97",
    "trace_name": "deleteMember",
    "resource_type": "member",
    "trace_rating": "normal",
    "api_version": "v2.0",
    "service_type": "ELB",
    "response": "{\"member\": {\"project_id\": \"0503dda897000fed2f78c00909158a4d\", \"name\": \"9646e73b-338c-
    "resource_id": "                                    ",
    "tracker_name": "system",
    "time": "1569321775225",
    "resource_name": "9646e73b-338c-4d27-a17c-219be532812c",
    "record_time": "1569321775903",
    "user": {
        "domain": {
            "name": "
            "id": "0503dda878000fed0f75c0096d70a960"
        },
```

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

审计日志示例

- 创建负载均衡器

```
request {"loadbalancer":{"name":"elb-test-zcy","description":"","tenant_id":"05041fffa40025702f6dc009cc6f8f33","vip_subnet_id":"ed04fd93-e74b-4794-b63e-e72baa02a2da","admin_state_up":true}}
code 201
source_ip 124.71.93.36
trace_type ConsoleAction
event_type system
project_id 05041fffa40025702f6dc009cc6f8f33
trace_id b39b21a1-8d49-11ec-b548-2be046112888
trace_name createLoadbalancer
resource_type loadbalancer
trace_rating normal
api_version v2.0
service_type ELB
response {"loadbalancer": {"description": "", "provisioning_status": "ACTIVE", "provider": "vlb", "project_id": "05041fffa40025702f6dc009cc6f8f33", "vip_address": "172.18.0.205", "pools": [], "operating_status": "ONLINE", "name": "elb-test-zcy", "created_at": "2022-02-14T03:53:39", "listeners": [], "id": "7ebe23cd-1d46-4a49-b707-1441c7f0d0d1", "vip_port_id": "5b36ff96-3773-4736-83cf-38c54abedeea", "updated_at": "2022-02-14T03:53:41", "tags": [], "admin_state_up": true, "vip_subnet_id": "ed04fd93-e74b-4794-b63e-e72baa02a2da", "tenant_id": "05041fffa40025702f6dc009cc6f8f33"}}
```


resource_id 7ebe23cd-1d46-4a49-b707-1441c7f0d0d1
tracker_name system
time 2022/02/14 11:53:42 GMT+08:00
resource_name elb-test-zcy
record_time 2022/02/14 11:53:42 GMT+08:00
request_id
user {"domain": {"name": "CBUInfo", "id": "0503dda87802345ddafed096d70a960"}, "name": "zcy", "id": "09f106afd2345cdeff5c009c58f5b4a"}

- 删除负载均衡器

request
code 204
source_ip 124.71.93.36
trace_type ConsoleAction
event_type system
project_id 05041fffa40025702f6dc009cc6f8f33
trace_id 4f838bbf-8d4a-11ec-a1fe-1f93fdaf3bec
trace_name deleteLoadbalancer
resource_type loadbalancer
trace_rating normal
api_version v2.0
service_type ELB
response {"loadbalancer": {"listeners": [], "vip_port_id": "5b36ff96-3773-4736-83cf-38c54abedeea", "tags": [], "tenant_id": "05041fffa40025702f6dc009cc6f8f33", "admin_state_up": true, "id": "7ebe23cd-1d46-4a49-b707-1441c7f0d0d1", "operating_status": "ONLINE", "description": "", "pools": [], "vip_subnet_id": "ed04fd93-e74b-4794-b63e-e72baa02a2da", "project_id": "05041fffa40025702f6dc009cc6f8f33", "provisioning_status": "ACTIVE", "name": "elb-test-zcy", "created_at": "2022-02-14T03:53:39", "vip_address": "172.18.0.205", "updated_at": "2022-02-14T03:53:41", "provider": "vlb"}}
resource_id 7ebe23cd-1d46-4a49-b707-1441c7f0d0d1
tracker_name system
time 2022/02/14 11:58:03 GMT+08:00
resource_name elb-test-zcy
record_time 2022/02/14 11:58:03 GMT+08:00
request_id
user {"domain": {"name": CBUInfo", "id": "0503dda87802345ddafed096d70a960"}, "name": "zcy", "id": "09f106afd2345cdeff5c009c58f5b4a"}

2 共享型用户指南

2.1 权限管理

2.1.1 创建用户并授权使用 ELB

如果您需要对您所拥有的ELB进行精细的权限管理，您可以使用**统一身份认证服务**（Identity and Access Management，简称IAM），通过IAM，您可以：

- 根据企业的业务组织，在您的华为云账号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用ELB资源。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将ELB资源委托给更专业、高效的其他华为云账号或者云服务，这些账号或者云服务可以根据权限进行代运维。

如果华为云账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用ELB服务的其它功能。

本章节为您介绍对用户授权的方法，操作流程如**图2-1**所示。

前提条件

给用户组授权之前，请您了解用户组可以添加的ELB权限，并结合实际需求进行选择。ELB支持的系统权限，请参见：**ELB系统权限**。若您需要对除ELB之外的其它服务授权，IAM支持服务的所有权限请参见**系统权限**。

示例流程

图 2-1 给用户授权 ELB 权限流程

1. **创建用户组并授权**

   在IAM控制台创建用户组，并授予弹性负载均衡服务只读权限“ELB ReadOnlyAccess”。
2. **创建用户并加入用户组**

   在IAM控制台创建用户，并将其加入**1.创建用户组并授权**中创建的用户组。
3. **用户登录**并验证权限

   新创建的用户登录控制台，切换至授权区域，验证权限：
   - 在“服务列表”中选择弹性负载均衡，进入ELB主界面，单击右上角“购买弹性负载均衡”，尝试购买弹性负载均衡器，如果无法购买弹性负载均衡器（假设当前权限仅包含ELB ReadOnlyAccess），表示“ELB ReadOnlyAccess”已生效。
   - 在“服务列表”中选择除弹性负载均衡器外（假设当前策略仅包含ELB ReadOnlyAccess）的任一服务，若提示权限不足，表示“ELB ReadOnlyAccess”已生效。

2.1.2 ELB 自定义策略

如果系统预置的ELB权限，不满足您的授权要求，可以创建自定义策略。自定义策略中可以添加的授权项（Action）请参考**《弹性负载均衡接口参考》**中“ 策略及授权项说明”章节。

目前华为云支持以下两种方式创建自定义策略：

- 可视化视图创建自定义策略：无需了解策略语法，按可视化视图导航栏选择云服务、操作、资源、条件等策略内容，可自动生成策略。
- JSON视图创建自定义策略：可以在选择策略模板后，根据具体需求编辑策略内容；也可以直接在编辑框内编写JSON格式的策略内容。

具体创建步骤请参见：**创建自定义策略**。本章为您介绍常用的ELB自定义策略样例。

ELB 自定义策略样例

- 示例1：授权用户更新负载均衡器

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "elb:loadbalancers:put"
            ]
        }
    ]
}
```

- 示例2：拒绝用户删除负载均衡器

  拒绝策略需要同时配合其他策略使用，否则没有实际作用。用户被授予的策略中，一个授权项的作用如果同时存在Allow和Deny，则遵循Deny优先。

  如果您给用户授予ELB FullAccess的系统策略，但不希望用户拥有ELB FullAccess中定义的删除负载均衡器权限，您可以创建一条拒绝删除负载均衡器的自定义策略，然后同时将ELB FullAccess和拒绝策略授予用户，根据Deny优先原则，则用户可以对ELB执行除了删除负载均衡器外的所有操作。拒绝策略示例如下：

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "elb:loadbalancers:delete"
            ]
        }
    ]
}
```

- 示例3：多个授权项策略

  一个自定义策略中可以包含多个授权项，且除了可以包含本服务的授权项外，还可以包含其他服务的授权项，可以包含的其他服务必须跟本服务同属性，即都是项目级服务或都是全局级服务。多个授权语句策略描述如下：

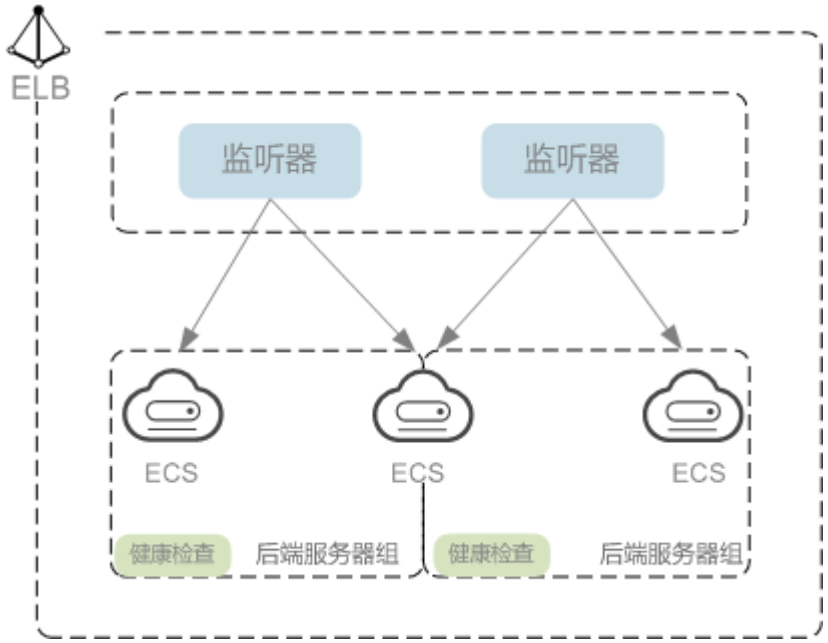
```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "elb:loadbalancers:get",
                "elb:loadbalancers:list",
                "elb:loadbalancers:delete",
                "ecs:cloudServers:delete"
            ]
        }
    ]
}
```

2.2 负载均衡器

2.2.1 共享型负载均衡器概述

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

图 2-2 负载均衡器结构图



规划实例区域

负载均衡器选择区域时需要注意以下事项：

- 选择距离业务目标客户距离最近的区域，可以减少网络时延以及提高下载速度。
- 共享型负载均衡不支持跨区域关联后端服务器，因此在创建共享型负载均衡时，需选择与后端服务器相同的区域。

选择网络类型

共享型实例网络类型可以选择公网或者私网。

- 如果需要使用负载均衡分发来自Internet公网的访问请求，需要创建公网负载均衡器。公网负载均衡实例可以同时处理来自VPC内网的访问请求。

  创建公网负载均衡器会绑定一个EIP，用来接收来自Internet公网的访问请求。
- 如果只需要使用负载均衡分发来自VPC内网的访问请求，选择创建私网负载均衡器。

  私网负载均衡器仅分配一个私网IP，仅能用来接收来自同个VPC内的访问请求。

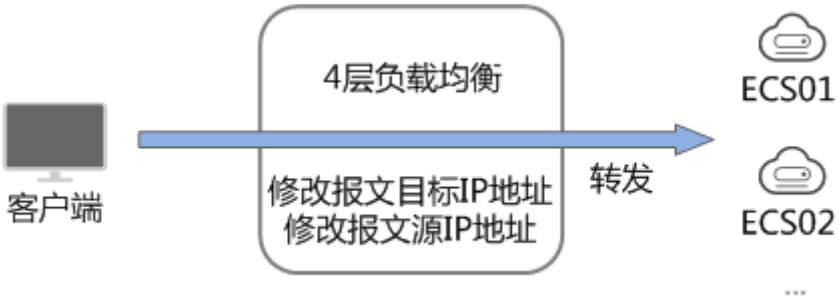
选择协议类型

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

- 使用四层协议的负载均衡，监听器收到访问请求后，将请求直接转发给后端服务器。转发过程仅修改报文中目标IP地址和源IP地址，将目标地址改为后端云服务器

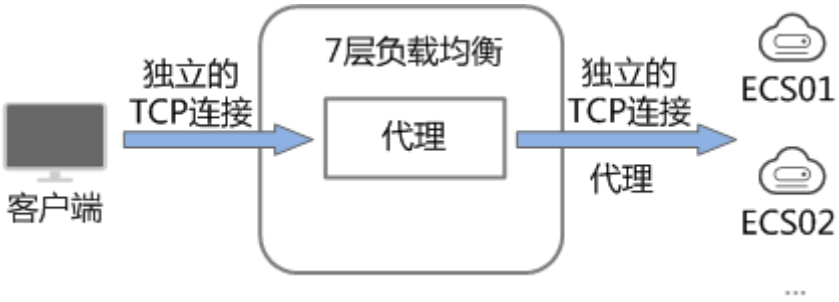
的IP地址，源地址改为负载均衡器的IP地址。四层协议连接的建立，即三次握手是客户端和后端服务器直接建立的，负载均衡只是进行了数据的转发。

图 2-3 四层负载均衡



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

图 2-4 七层负载均衡



说明

客户端到ELB之间支持TCP长连接，客户端和ELB之间建立TCP连接之后，可以持续发送业务请求（HTTP/HTTPS请求），提高TCP连接复用率可以降低TCP频繁建连的开销。

后端服务器

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

- 确保后端服务器实例的所属地域和负载均衡器的所属地域相同。
- 建议您选择相同操作系统的后端服务器实例作为后端服务器，以便后续管理和维护。
- 弹性负载均衡不支持后端FTP服务，但是可以支持SFTP场景。

2.2.2 创建共享型负载均衡器

操作场景

在您创建共享型负载均衡器前，确保您已经做好了相关规划，详情参考**共享型负载均衡器概述**。

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

约束与限制

- 负载均衡器创建后，不支持修改VPC。如果要修改VPC，请重新创建负载均衡器，并选择对应的VPC。
- 共享型负载均衡实例创建完成后，您还需要创建监听器并添加后端云服务器，才可以对负载均衡实例地址进行**ping**验证。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面单击“购买弹性负载均衡器”。根据界面提示选择负载均衡器的基础配置，配置参数如**表2-1**所示。

表 2-1 负载均衡器的基础配置

参数	说明
实例类型	负载均衡的实例类型，选定后不支持修改。 实例类型的区别详见**独享型负载均衡与共享型弹性负载均衡的区别**。
计费模式	共享型负载均衡器的收费类型。 • 包年/包月 • 按需计费
区域	不同区域的资源之间内网不互通。请选择靠近您客户的区域，可以降低网络时延、提高访问速度。
名称	负载均衡器的名称。
企业项目	企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。
描述	可添加负载均衡器相关描述。

参数	说明
标签	标签用于标识云资源，可对云资源进行分类和搜索。标签由标签“键”和标签“值”组成，标签键用于标记标签，标签值用于表示具体的标签内容。命名规格请参照**表2-2**。 您最多可以添加20个标签。 **说明** 如果您的组织已经设定弹性负载均衡的相关标签策略，则需按照标签策略规则为弹性负载均衡添加标签。标签如果不符合标签策略的规则，则可能会导致弹性负载均衡创建失败，请联系组织管理员了解标签策略详情。

表 2-2 负载均衡器标签命名规则

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

5. 选定负载均衡器的基础配置后，请根据界面提示选择负载均衡器的网络配置，配置参数如**表2-3**所示。

表 2-3 负载均衡器的网络配置

参数	说明
网络类型	可选公网或者私网。 • IPv4公网：公网负载均衡器通过公网IP对外提供服务，将来自公网的客户端请求按照指定的负载均衡策略分发到后端服务器进行处理。 • IPv4私网：私网负载均衡器通过私网IP对外提供服务，将来自同一个VPC的客户端请求按照指定的负载均衡策略分发到后端服务器进行处理。
所属VPC	负载均衡器所属虚拟私有云，共享型ELB创建完成后不支持修改，请做好相关网络规划。 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》**。

参数	说明
前端子网	共享型负载均衡默认支持IPv4私网，支持通过私网IP对外提供服务。 前端子网作为共享型负载均衡所在的IPv4子网，将为ELB实例下发IPv4私有地址。
IPv4地址	选择IPv4地址的分配方式。 ● 自动分配IP地址：由系统自动分配IPv4地址。 ● 手动指定IP地址：手动指定IPv4地址。 **说明** 负载均衡器的IP地址不受所在后端子网ACL配置的限制，所以能够被客户端直接访问。建议您使用监听器的访问控制功能限制客户端访问负载均衡器。 详细请参考**访问控制策略**。
性能保障模式	性能保障模式提供最大并发连接数5万、每秒新建连接数5000、每秒查询速率5000 的保障能力。 默认开启，不支持关闭。
弹性公网IP	负载均衡器绑定EIP后可以接收来自公网的访问请求并自动分发到多台后端服务器。 您可以选择使用已有的EIP，或者创建新的EIP。 您可以根据实际情况选择以下方式： ● 新创建：新创建一个EIP。 ● 使用已有：使用已有EIP创建负载均衡器，需在页面选择已有EIP。
弹性公网IP类型	使用新创建弹性公网IP时，选择的EIP的类型。 ● 静态BGP：网络结构发生变化时，无法实时自动调整网络设置以保障用户体验。 ● 全动态BGP：可以根据设定的寻路协议实时自动优化网络结构，以保证客户使用的网络持续稳定、高效。
公网带宽	弹性公网IP使用的带宽类型。 ● 按带宽计费：指定带宽上限，按使用时间计费，与使用的流量无关。 ● 按流量计费：指定带宽上限，按实际使用的上行流量计费，与使用时间无关。 ● 加入共享带宽：加入共享带宽的EIP，不单独收取带宽和流量费，以共享带宽费用为准。
带宽	设置新创建的EIP带宽大小。

6. 当负载均衡的计费模式选定“包年/包月”时，需要指定实例的购买时长。
   “包年/包月”模式的负载均衡支持自动续费：
   - 按月购买：则自动续费周期为一个月，
   - 按年购买：则自动续费周期为一年。

7. 单击“立即购买”。
8. 确认配置信息，根据界面提示完成创建操作。

导出负载均衡器列表

负载均衡器创建完成后，您可以将当前账号下拥有的所有负载均衡器信息，以Excel文件的形式导出至本地，作为本地备份数据查看。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在负载均衡器列表左上方，单击“导出”，导出弹性负载均衡器列表。

2.2.3 配置共享型负载均衡器的修改保护

您可以对负载均衡器开启修改保护功能，防止因误操作导致负载均衡器的配置被修改或负载均衡器被删除。

开启或关闭修改保护

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要开启修改保护的负载均衡器名称。
5. 切换到负载均衡器的“基本信息”页签，单击修改保护右侧的“设置”。
6. 在设置修改保护的弹窗中，开启或关闭“修改保护开关”。
   您可填写“添加修改保护原因”。
7. 单击“确定”。

说明

如果您需要修改负载均衡器的配置或删除负载均衡器，请先关闭“修改保护”开关。

2.2.4 变更共享型负载均衡器的网络配置

您可以通过变更负载均衡实例的网络配置来满足您的业务要求。

绑定/解绑 IPv4 公网 IP

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

共享型负载均衡器支持绑定和解绑IPv4公网IP。

说明

解绑IPv4公网IP后，对应的弹性负载均衡器将无法进行IPv4公网流量转发。

1. 登录管理控制台。

2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，待修改的负载均衡器所在行，选择“更多 ”。
   a. 绑定IPv4公网IP：
      i. 单击“绑定IPv4公网IP”。
      ii. 在“绑定IPv4公网IP”对话框中，选择需要绑定的公网IP，单击“确定”。
   b. 解绑IPv4公网IP：
      i. 单击“解绑IPv4公网IP”。
      ii. 在“解绑IPv4公网IP”对话框中，确认需要释放的IPv4公网IP地址，单击“确定”。

修改公网带宽

当负载均衡器支持公网流量请求时，公网与负载均衡器之间的流量通过公网带宽进行访问，用户可以按照实际需求更改负载均衡实例关联的公网带宽。弹性负载均衡在变更公网带宽的时候，访问流量不会中断。

说明

公网带宽为负载均衡实例绑定的弹性公网IP带宽，是客户端访问负载均衡实例时的最高流量限制。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，待修改带宽的负载均衡器所在行的“操作”列，单击“更多”。
5. 单击“修改IPv4带宽”。
6. 在“修改带宽”区域，设置新的带宽大小，单击“下一步”。

   可以选择系统定义好的带宽也可以自定义带宽大小。自定义修改带宽的范围为1-2,000 Mbit/s。
7. 确认修改后的带宽大小，单击“提交”。

   说明

   如果您更改了付费方式和带宽信息，具体扣费会以变更后费用为准。

2.2.5 删除共享型负载均衡器

操作场景

当您确认负载均衡不需要继续使用时，您可以根据需求随时删除负载均衡器。

> **⚠ 注意**
>
> 删除弹性负载均衡后无法恢复，请谨慎操作。

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

约束与限制

- 如果**负载均衡器配置了修改保护**，则无法执行删除，请先在负载均衡器的基本信息页签中关闭“修改保护”。
- 如果负载均衡器的**监听器配置了修改保护**，则无法执行删除，请先在监听器的基本信息页签中关闭“修改保护”。
- 如果负载均衡器的**后端服务器组配置了修改保护**，则无法执行删除，请先在后端服务器组的基本信息页签中关闭“修改保护”。

删除负载均衡器

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，选择目标负载均衡器所在行的操作列下的“更多 > 删除”。

   弹出删除确认对话框。
5. 在删除确认对话框，输入“DELETE”。
6. 单击“确定”。

2.2.6 启停共享型负载均衡器

您可以随时启用和停用负载均衡器。负载均衡器停用后，将不再接收和转发流量。

当您配置的某些负载均衡器出于业务考虑暂时无需使用，但又不能删除时，可以选择启停操作。

启用或停用 ELB 实例

您可以随时启用和停用负载均衡器。负载均衡器停用后，将不再接收和转发流量。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，需要启用或者停用的负载均衡器所在行，单击“更多 > 启用”或者“更多 > 停用”。
5. 单击“是”。

⚠ 注意

停用的负载均衡器仍会继续计费。

2.2.7 共享型负载均衡开启性能保障模式

性能保障模式

共享型实例性能保障模式提供并发连接数5万、每秒新建连接数5000、每秒查询数5000 的保障能力，可以为您提供更加稳定、更高质量的负载均衡服务，解决非性能保障模式下资源易抢占的问题。

2022年7月10号起，新创建的共享型实例默认开启性能保障模式。

2022年7月10号前创建的共享型实例均未开启性能保障模式，您可以参考本节操作开启性能保障模式。

使用须知

- 性能保障模式开启后，无法关闭。
- 性能保障模式开启后，将按需收取弹性负载均衡实例费用。具体价格请参考**价格详情**。

开启性能保障模式

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 单击需要开启性能保障模式的共享型实例，进入“基本信息”页面。
5. 单击性能保障模式的“开启”。
6. 选择“立即开启”即可开启性能保障模式。

图 2-5 开启性能保障模式

2.3 监听器

2.3.1 什么是监听器

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

支持的协议类型

负载均衡提供四层协议和七层协议监听，您可根据从客户端到负载均衡器的应用场景选择监听协议，详细说明可参见表2-4。

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

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

表 2-4 监听协议类型说明

协议类型		说明	适用场景
四层协议	TCP	• 基于源地址的会话保持。 • 数据传输快。	• 适用于注重可靠性，对数据准确性要求高的场景，如文件传输、发送或接收邮件、远程登录。 • 对性能和并发规模有要求的Web应用。

协议类型		说明	适用场景
四层协议	UDP	• 可靠性相对低 • 数据传输快	适用于关注实时性而相对不注重可靠性的场景，如视频聊天、游戏、金融实时行情推送。
七层协议	HTTP	• 基于Cookie的会话保持。 • 使用X-Forward-For获取源地址。	需要对数据内容进行识别的应用，如Web应用、移动游戏等。
七层协议	HTTPS	• 加密传输数据，可以阻止未经授权的访问。 • 加解密操作在负载均衡器上完成，可减少后端服务器的处理负载。 • 多种加密协议和加密套件可选。	需要加密传输的应用。

前端协议和端口

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

说明

前端协议和端口设置后不允许修改，如果要修改，请重新创建监听器。

表 2-5 前端协议和端口说明

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

后端协议和端口

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

表 2-6 后端协议和端口说明

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

2.3.2 添加 TCP 监听器

操作场景

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

约束与限制

前端协议为“TCP”时，后端协议默认为“TCP”，且不支持修改。

共享型负载均衡添加 TCP 监听器

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要添加监听器的负载均衡名称。
5. 切换到“监听器”页签，单击“添加监听器”，配置监听器。配置监听器参数参见**表2-7**。

表 2-7 共享型负载均衡配置监听器参数说明

参数	说明
名称	监听器名称。
前端协议	客户端与负载均衡监听器建立流量分发连接的协议。 协议选择TCP。
前端端口	客户端与负载均衡监听器建立流量分发连接的端口。 取值范围为：[1-65535]。

参数	说明
访问控制	支持通过白名单和黑名单进行访问控制，更多信息请参见**访问控制策略**： • 允许所有IP访问 • 黑名单 • 白名单
IP地址组	设置白名单或者黑名单时，必须选择一个IP地址组。如果还未创建IP地址组，需要先创建IP地址组，更多关于IP地址组的信息请参见**访问控制IP地址组**。
获取客户端IP	开启此开关，后端服务器可以获取到客户端的真实IP地址。
高级配置	
空闲超时时间（秒）	如果在超时时间内一直没有访问请求，负载均衡会中断当前连接，直到下一次请求到来时再重新建立新的连接。 取值范围：10~4000s
描述	对于监听器描述。 字数范围：0/255。

6. 单击“下一步：配置后端分配策略”，配置监听器的默认后端服务器组。
   a. 推荐选择“使用已有”后端服务器组，您可参考**创建后端服务器组**进行创建。
   b. 您也可选择“新创建”后端服务器组，添加后端服务器并配置健康检查，
      i. 配置后端服务器组参数请参见**表2-27**。
      ii. 单击“下一步：添加后端服务器”，添加后端服务器并配置健康检查。
      添加后端服务器详见**后端服务器概述**，配置健康检查参数请参见**表2-28**。
7. 单击“下一步：确认配置”。
8. 确认配置无误后，单击“提交”。

2.3.3 添加 UDP 监听器

操作场景

UDP协议适用于关注实时性而相对不注重可靠性的场景，如视频聊天、游戏、金融实时行情推送。您可以添加一个UDP监听器转发来自UDP协议的请求。

约束与限制

- UDP监听器不支持分片包。
- UDP监听器的前端端口当前不支持4789。

- UDP监听器支持的最大MTU为1500，请确保与ELB通信的网卡的MTU不大于1500（有些应用程序需要根据此MTU值同步修改其配置文件），否则数据包可能会因过大被丢弃。
- 共享型负载均衡前端协议为“UDP”时，后端协议默认为“UDP”，且不支持修改。

共享型负载均衡添加 UDP 监听器

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要添加监听器的负载均衡名称。
5. 切换到“监听器”页签，单击“添加监听器”，配置监听器。配置监听器参数参见**表2-8**。

表 2-8 共享型负载均衡配置监听器参数说明

参数	说明
名称	监听器名称。
前端协议	客户端与负载均衡监听器建立流量分发连接的协议。 协议选择UDP。
前端端口	客户端与负载均衡监听器建立流量分发连接的端口。 取值范围为：[1-65535]。
访问控制	支持通过白名单和黑名单进行访问控制，更多信息请参见**访问控制策略**： • 允许所有IP访问 • 黑名单 • 白名单
IP地址组	设置白名单或者黑名单时，必须选择一个IP地址组。如果还未创建IP地址组，需要先创建IP地址组，更多关于IP地址组的信息请参见**访问控制IP地址组**。
获取客户端IP	开启此开关，后端服务器可以获取到客户端的真实IP地址。
高级配置	
描述	对于监听器描述。 字数范围：0/255。

6. 单击“下一步：配置后端分配策略”，配置监听器的默认后端服务器组。
   a. 推荐选择“使用已有”后端服务器组，您可参考**创建后端服务器组**进行创建。

b. 您也可选择“新创建”后端服务器组，添加后端服务器并配置健康检查，
   i. 配置后端服务器组参数请参见**表2-27**。
   ii. 单击“下一步：添加后端服务器”，添加后端服务器并配置健康检查。
   添加后端服务器详见**后端服务器概述**，配置健康检查参数请参见**表2-28**。

7. 单击“下一步：确认配置”。
8. 确认配置无误后，单击“提交”。

2.3.4 添加 HTTP 监听器

操作场景

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

约束与限制

前端协议为“HTTP”时，后端协议默认为“HTTP”，且不支持修改。

添加共享型负载均衡 HTTP 监听器

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要添加监听器的负载均衡名称。
5. 切换到“监听器”页签，单击“添加监听器”，配置监听器。配置监听器参数参见**表2-9**。

表 2-9 共享型负载均衡配置监听器参数说明

参数	说明
名称	监听器名称。
前端协议	客户端与负载均衡监听器建立流量分发连接的协议。 协议选择HTTP。
前端端口	客户端与负载均衡监听器建立流量分发连接的端口。 取值范围为：[1-65535]。
重定向	重定向开关是否开启。 协议类型为HTTP时，可根据需要设置该项。需要保证业务建立安全连接时，若同时创建了HTTPS监听器和HTTP监听器，可以通过重定向功能，将HTTP监听器访问重定向至HTTPS监听器。 HTTP监听器被重定向后，会返回301返回码。
重定向至	选择需要重定向HTTPS监听器的名称。

参数	说明
访问控制	支持通过白名单和黑名单进行访问控制，更多信息请参见**访问控制策略**： • 允许所有IP访问 • 黑名单 • 白名单
IP地址组	设置白名单或者黑名单时，必须选择一个IP地址组。如果还未创建IP地址组，需要先创建IP地址组，更多关于IP地址组的信息请参见**访问控制IP地址组**。
获取客户端IP	HTTP监听器默认开启此开关且不支持关闭，后端服务器可以获取到客户端的真实IP地址。
高级配置	
获取弹性公网IP	通过X-Forwarded-ELB-IP头字段获取ELB实例公网IP地址。 若您需要将ELB公网IP透传到后端，只需在创建HTTP监听器时，打开该开关。
空闲超时时间（秒）	如果在超时时间内一直没有访问请求，负载均衡会中断当前连接，直到下一次请求到来时再重新建立新的连接。 时间取值范围[0-4000]。
请求超时时间（秒）	客户端向负载均衡发起请求，如果在超时时间内客户端没有完成整个请求的传输，负载均衡将放弃等待关闭连接。 时间取值范围[1-300]。
响应超时时间（秒）	负载均衡向后端服务器发起请求，如果超时时间内接收请求的后端服务器无响应，负载均衡会向其他后端服务器重试请求。如果重试期间后端服务器一直没有响应，则负载均衡会给客户端返回HTTP 504错误码。 时间取值范围[1-300]。 **说明** 当开启了会话保持功能时，响应超时时间内如果对应的后端服务器无响应，则直接会返回HTTP 504错误码。
描述	对于监听器描述。 字数范围：0/255。

6. 单击“下一步：配置后端分配策略”，配置监听器的默认后端服务器组。
   a. 推荐选择“使用已有”后端服务器组，您可参考**创建后端服务器组**进行创建。
   b. 您也可选择“新创建”后端服务器组，添加后端服务器并配置健康检查，
      i. 配置后端服务器组参数请参见**表2-27**。
      ii. 单击“下一步：添加后端服务器”，添加后端服务器并配置健康检查。

添加后端服务器详见**后端服务器概述**，配置健康检查参数请参见**表2-28**。

7. 单击“下一步：确认配置”。
8. 确认配置无误后，单击“提交”。

2.3.5 添加 HTTPS 监听器

操作场景

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

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

如果您不希望负载均衡器对HTTPS流量进行解密，可以通过配置相同端口的TCP监听器将HTTPS流量透传到后端服务器。具体原理参见**TCP监听器将HTTPS流量透传到后端服务器**。

约束与限制

共享型负载均衡前端协议为“HTTPS”时，后端协议默认为“HTTP”，且不支持修改。

添加共享型负载均衡 HTTPS 监听器

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要添加监听器的负载均衡名称。
5. 切换到“监听器”页签，单击“添加监听器”，配置监听器。配置监听器参数参见**表2-10**。

表 2-10 共享型负载均衡配置监听器参数说明

参数	说明
名称	监听器名称。
前端协议	客户端与负载均衡监听器建立流量分发连接的协议。 协议选择HTTPS。
前端端口	客户端与负载均衡监听器建立流量分发连接的端口。 取值范围为：[1-65535]。

参数	说明
SSL解析方式	确保服务安全，请选择客户端到服务器端认证方式。 可选择“单向认证”或“双向认证”。 • 如仅进行服务器端认证，请选择单向认证。 • 双向认证需要负载均衡实例与访问用户互相提供身份认证，从而允许通过认证的用户访问负载均衡实例，后端服务器无需额外配置双向认证。
CA证书	双向认证开启后需要配置CA证书。 详见**创建证书**。
服务器证书	协议类型为HTTPS时，需绑定服务器证书。 服务器证书用于SSL握手协商，需提供证书内容和私钥。 详见**创建证书**。
开启SNI	HTTPS协议的负载均衡可以选择是否开启SNI。 SNI是为了解决一个服务器使用多个域名和证书的TLS扩展。 开启SNI后，允许客户端在发起SSL握手请求时就提交请求的域名信息，ELB收到SSL请求后，会根据域名去查找证书，如果找到域名对应的证书，则返回该证书；如果没有找到域名对应的证书，则返回缺省证书。详见**开启SNI证书实现多域名访问**。
SNI证书	HTTPS协议的负载均衡设置开启SNI后需要选择域名对应的证书。 可选择已创建或者创建新的SNI证书。 详见**创建证书**。
访问控制	支持通过白名单和黑名单进行访问控制，更多信息请参见**访问控制策略**： • 允许所有IP访问 • 黑名单 • 白名单
IP地址组	设置白名单或者黑名单时，必须选择一个IP地址组。如果还未创建IP地址组，需要先创建IP地址组，更多关于IP地址组的信息请参见**访问控制IP地址组**。
获取客户端IP	HTTPS监听器默认开启此开关且不支持关闭，后端服务器可以获取到客户端的真实IP地址。
高级配置	
安全策略	支持选择可用的安全策略，更多信息请参见**TLS安全策略**。
HTTP/2	协议类型为HTTPS时，可选择是否支持该协议类型。详见**开启HTTP/2提升通信效率**。

参数	说明
获取弹性公网IP	通过X-Forwarded-ELB-IP头字段获取ELB实例公网IP地址。 若您需要将ELB公网IP透传到后端，只需在创建HTTP监听器时，打开该开关。
空闲超时时间（秒）	如果在超时时间内一直没有访问请求，负载均衡会中断当前连接，直到下一次请求到来时再重新建立新的连接。 时间取值范围[0-4000]。
请求超时时间（秒）	客户端向负载均衡发起请求，如果在超时时间内客户端没有完成整个请求的传输，负载均衡将放弃等待关闭连接。 时间取值范围[1-300]。
响应超时时间（秒）	负载均衡向后端服务器发起请求，如果超时时间内接收请求的后端服务器无响应，负载均衡会向其他后端服务器重试请求。如果重试期间后端服务器一直没有响应，则负载均衡会给客户端返回HTTP 504错误码。 时间取值范围[1-300]。 **说明** 当开启了会话保持功能时，响应超时时间内如果对应的后端服务器无响应，则直接会返回HTTP 504错误码。
描述	对于监听器描述。 字数范围：0/255。

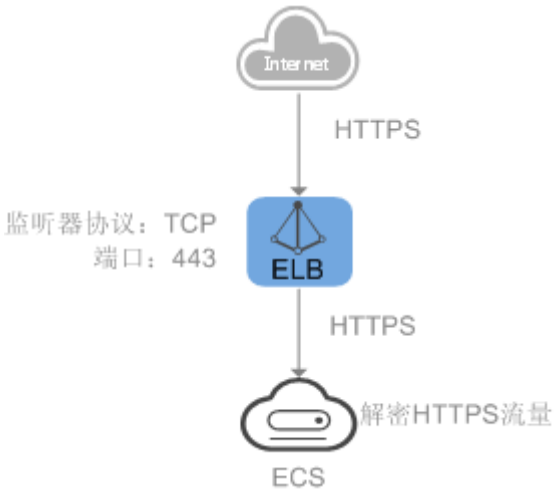
6. 单击“下一步：配置后端分配策略”，配置监听器的默认后端服务器组。
   a. 推荐选择“使用已有”后端服务器组，您可参考**创建后端服务器组**进行创建。
   b. 您也可选择“新创建”后端服务器组，添加后端服务器并配置健康检查，
      i. 配置后端服务器组参数请参见**表2-27**。
      ii. 单击“下一步：添加后端服务器”，添加后端服务器并配置健康检查。
      添加后端服务器详见**后端服务器概述**，配置健康检查参数请参见**表2-28**。
7. 单击“下一步：确认配置”。
8. 确认配置无误后，单击“提交”。

TCP 监听器将 HTTPS 流量透传到后端服务器

如果您不希望负载均衡器对HTTPS流量进行解密，可以通过配置相同端口的TCP监听器将HTTPS流量透传到后端服务器。并且在实例的安全组配置相同端口的TCP入方向规则，以允许相同端口上来自负载均衡器的入站流量。

如下图所示，TCP监听器如何将端口为443的HTTPS流量进行无解密透传到后端服务器。

图 2-6 TCP 透传 HTTPS 流量



2.3.6 转发策略

操作场景

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

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

转发策略由**转发规则**和**转发动作**两部分组成：

- 支持的转发规则有：**域名**、**URL**。
- HTTP监听器支持的动作类型有：**转发至后端服务器组**、**重定向至监听器**。
- HTTPS监听器支持的动作类型有：**转发至后端服务器组**。

匹配原理

- 在添加了转发策略后，负载均衡器将按以下规则转发前端请求：
  - 如果能匹配到监听器的转发策略，则按该转发策略将请求转发到对应的后端服务器组。
  - 如果不能匹配到监听器的转发策略，则按照默认转发策略将请求转发到监听器默认的后端服务器组（创建监听器时配置的后端服务器组）。
- 匹配优先级：
  - 不同域名间优先级互相独立，转发规则域名与URL同时存在时，优先按照域名进行匹配。
  - 转发规则为URL时，匹配优先级如下：精确匹配 > 前缀匹配 > 正则匹配，匹配类型相同时URL长度越长，优先级越高。

表 2-11 转发策略示例

访问请求	转发策略	转发规则	设定值
www.elb.com/test	1	URL	/test
	2	域名	www.elb.com

说明

如表2-11中，访问请求www.elb.com/test同时满足转发策略1和转发策略2，优先按照域名进行匹配，则请求将按照转发策略2进行转发。

约束与限制

- 此功能目前仅支持协议类型为HTTP、HTTPS的监听器。
- 负载均衡控制台不支持创建相同的转发策略。
- 一个监听器最多支持配置100条转发策略，超过配额的转发策略不生效。
- 配置共享型ELB的转发策略时，请注意以下事项：
  - 转发规则URL仅支持路径，不支持查询字符串。如果您的URL设置为/path/resource?name=value，该条转发策略将失效。
  - 每个URL路径需要存于后端服务器（即必须是后端服务器上真实存在的路径），否则访问后端服务器时，后端服务器会返回404。
  - 因为正则匹配采用顺序匹配的方式，只要任意规则匹配成功就结束匹配。所以配置“URL匹配规则”为“正则匹配”的多个匹配规则时，规则之间不能重叠。
  - 不能配置URL路径完全相同的转发策略。
  - 输入的域名总长度不能超过100个字符。

注意

如果通过调用API接口创建了相同的转发策略，则会出现转发策略故障，此时即使把前面创建的转发策略删除，后面的转发策略依然会显示故障。将出现冲突的转发策略都删除后重新添加，即可恢复正常。

添加转发策略

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要添加转发策略的负载均衡器名称。
5. 在“监听器”页签，您可以通过以下两种操作入口，进入监听器的“转发策略”页签。
   - 在目标监听器所在行的“操作”列，单击“添加/编辑转发策略”。

- 单击目标监听器的名称，并切换到“转发策略”页签。

6. 单击“添加转发策略”按钮。参考**表2-12**配置参数。
7. 配置完成，单击“保存”。

表 2-12 添加转发策略的参数

参数		说明	样例
转发规则	域名	触发转发的域名，仅支持精确域名。 域名或者URL至少要指定一个。	www.test.com
	URL	● 匹配说明 触发转发的URL路径。URL由英文字母、数字和特殊字符 _~';@^-%#$.*+?,=!:|\/()[]{}组成。 ● 匹配方式 – 精确匹配：请求的URL和设定URL完全一致，只能由/开头。 – 前缀匹配：请求的URL匹配已设定URL开头的URL，只能由/开头。 – 正则匹配：请求的URL和设定的URL正则表达式匹配。	/login.php
动作	转发至后端服务器组	如果请求与配置的转发规则（条件）匹配，则将请求转发至配置的后端服务器组。	转发至后端服务器组
	重定向至监听器	如果请求与配置的转发规则（条件）匹配，则将请求重定向至配置的监听器。 仅HTTP监听器支持配置该动作类型。 **说明** 选择“重定向至监听器”并配置监听器后，除访问控制以外原有监听器配置会失效。 例如：配置了重定向至监听器后，当客户端通过HTTP请求访问的时候，后端服务器会返回HTTPS的响应，即强制以HTTPS请求访问网页。因此实际以HTTPS监听器的配置为准向后端服务器进行转发，原有HTTP监听器的配置就无效了。	-

参数	说明	样例
后端服务器组	为转发策略选择已有的后端服务器组。 “动作”选择“转发至后端服务器组”时需要设置。	-
监听器	为转发策略选择已有的监听器。 “动作”选择“重定向至监听器”时需要设置。	-

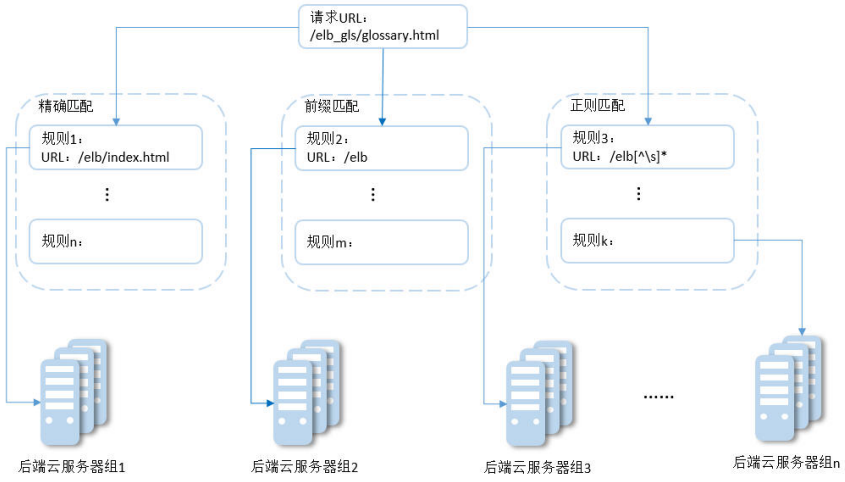
URL 匹配示例

如表2-13所示，是一个URL匹配示例，转发情况如图2-7所示。

表 2-13 URL 匹配示例

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

图 2-7 转发示例



以上图为例

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

修改转发策略

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要修改转发策略的负载均衡器名称。
5. 切换到监听器页签，单击需要修改转发策略的监听器名称。
6. 切换到“转发策略”页签，选择需要修改的转发策略，单击“编辑”。
7. 根据界面提示修改参数，单击“保存”。

删除转发策略

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要删除转发策略的负载均衡器名称。
5. 切换到监听器页签，单击需要删除转发策略的监听器名称。
6. 切换到“转发策略”页签，选择需要删除的转发策略，单击“删除”。
7. 在弹出的“删除转发策略”对话框中，单击“确定”。

2.3.7 管理监听器

操作场景

当您创建完监听器后，您可以根据实际业务需求为监听器配置修改保护、对监听器的配置进行修改以及更换监听器的后端服务器组等操作。

前提条件

- 您已经创建ELB实例，详情请参见**创建共享型负载均衡器**。
- 您已经创建可用的后端服务器组，详情请参见**创建后端服务器组**。
- 您已经创建监听器，详情请参见**什么是监听器**。

监听器配置修改保护

您可以对监听器开启修改保护功能，防止因误操作导致监听器的配置被修改或监听器被删除。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要为监听器配置修改保护的负载均衡名称。
5. 在“监听器”页签，单击需要为配置修改保护的监听器名称。

6. 在监听器的“基本信息”页签，单击修改保护右侧的“设置”。
7. 在设置修改保护的弹窗中，开启“修改保护开关”。

说明

如果您需要修改监听器的配置或删除监听器，请先关闭“修改保护”开关。

修改监听器

说明

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

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要修改监听器的负载均衡名称。
5. 您可以通过以下两种操作入口，修改监听器。
   - 在目标监听器所在行的“操作”列，单击“编辑”。
   - 单击目前监听器的名称，进入监听器的“基本信息”页面，单击“编辑监听器”。
6. 在“编辑监听器”页面修改参数，单击“确定”。

修改监听器的超时时间

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

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要修改监听器的负载均衡名称。
5. 切换到“监听器”页签，单击需要配置超时时间的目标监听器名称。
6. 在监听器的“基本信息”页面，单击“编辑监听器”。
7. 在“编辑监听器”页面，单击“高级配置”。
8. 根据需要配置“空闲超时时间”或“请求超时时间”或“响应超时时间”。
9. 单击“确定”。

更换监听器的后端服务器组

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。

3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”列表，单击目标监听器所在的负载均衡名称。
5. 选择“监听器”页签，在监听器列表中，单击目标监听器的名称。
6. 在监听器的“基本信息”页签，单击“后端服务器组”区域右侧“更换后端服务器组”。
7. 在弹出的对话框中，单击服务器组名称方框。

   将显示搜索框、所有可选服务器组和“创建后端服务器组”。

   a. 选择已有服务器组，可直接单击目标服务器组名称，也可在搜索框中按名称搜索。
   b. 您也可单击“创建后端服务器组”创建新的后端服务器组。创建完成后单击刷新按钮，在已有服务器组中进行选择。

      说明

      若创建新的服务器组，后端协议应与监听器的前端协议匹配才可被当前监听器使用。
8. 单击“确定”。

2.3.8 删除监听器

操作场景

如果您已创建监听器，您可以根据实际业务需求，可以修改或者删除监听器。

监听器被删除后无法恢复，请谨慎操作。

约束与限制

如果监听器已开启修改保护，则不能修改或删除监听器，您可到监听器的基本信息页面关闭修改保护开关。

删除监听器

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要删除监听器的负载均衡名称。
5. 在“监听器”页签，需要删除监听器所在行的“操作”列，单击“删除 ”。
6. 在删除监听器的弹窗页面，输入“DELETE”。
7. 单击“确定”。

2.4 后端服务器组

2.4.1 后端服务器组概述

后端服务器组简介

后端服务器组是一个或多个后端服务器的逻辑集合，用于将客户端的流量转发到一个或多个后端服务器，满足用户同时处理海量并发业务的需求。共享型负载均衡器仅支持添加云服务器作为后端服务器。

后端服务器组参与流量转发过程如下：

表 2-14 后端服务器组参与流量转发过程

步骤一	来自客户端的请求先传入负载均衡器，再经由负载均衡器上的监听器转发到后端服务器组。
步骤二	后端服务器组中健康检查正常的后端服务器处理转发的业务请求。
步骤三	实现同时对用户的海量并发业务进行处理，从而提升用户应用系统的可用性。

共享型负载均衡器使用的后端服务器组不区分类型。

表 2-15 服务器组添加后端服务器说明（共享型）

添加后端服务器分类	添加说明	操作指导
云服务器	支持添加与负载均衡器同VPC的云服务器实例（弹性云服务器和裸金属服务器）作为后端服务器。	**添加后端云服务器。**

后端服务器组优势

在负载均衡器的使用中引入后端服务器组有如下优势：

- 通过后端服务器组可以对后端服务器进行统一管理，灵活地添加或者移除后端服务器，降低用户的管理和使用成本。
- 后端服务器组支持**健康检查功能**，可保证流量转发到正常的后端服务器，提升用户业务的可靠性。

后端服务器组关键功能

为保证用户业务的稳定和多样化的流量转发需求，后端服务器组提供了如**表2-16**所示的关键功能可供用户配置。

表 2-16 后端服务器组关键功能

关键功能	功能说明	功能详情
健康检查	负载均衡器通过健康检查来判断后端服务器是否可用。 如果某个后端服务器健康检查异常，负载均衡器将不会把流量转发给异常后端服务器，从而提升了业务的可靠性。	**健康检查介绍**。
流量分配策略	负载均衡器按照后端服务器组配置的流量分配策略对请求的流量进行分发。	**流量分配策略介绍**。
会话保持	开启会话保持后，负载均衡器将属于同一个会话的请求都转发到固定的后端服务器进行处理，避免了客户端重复登录后端服务器。	**会话保持介绍**。

后端服务器组创建指引

后端服务器组独立创建后仅可关联至前端协议与后端协议匹配的监听器使用，监听器与后端服务器组的前端/后端协议匹配关系详见**表2-17**。

您有多种方式创建后端服务器组，详见**表2-18**。

表 2-17 前端/后端协议匹配关系

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

表 2-18 后端服务器组创建指引

弹性负载均衡类型	约束与限制	后端服务器组创建方法
共享型负载均衡	一个后端服务器组仅能关联在一个共享型负载均衡实例下，且仅能被一个监听器使用。	**创建后端服务器组**。

2.4.2 后端服务器组关键功能

2.4.2.1 健康检查介绍

负载均衡器会定期向后端服务器发送请求以测试其运行状态，这些测试称为健康检查。通过健康检查来判断后端服务器是否可用。

负载均衡器如果判断后端服务器健康检查异常，就不会将流量分发到异常后端服务器，而是分发到健康检查正常的后端服务器，从而提高了业务的可靠性。当异常的后端服务器恢复正常运行后，负载均衡器会将其自动恢复到负载均衡服务中，承载业务流量。

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

健康检查协议

您可以在创建后端服务器组和创建监听器时为后端服务器组配置健康检查，通常，使用默认的健康检查配置即可，也根据业务需要选择不同的健康检查协议。

您也可以在后端服务器组创建后修改健康检查，详情可见**修改健康检查配置**。

后端服务器组的后端协议与支持的健康检查协议存在匹配关系，详情请参见**表2-19**。

表 2-19 后端服务器组支持的健康检查协议（共享型）

后端服务器组的后端协议	健康检查协议
TCP	TCP、HTTP
UDP	UDP
HTTP	TCP、HTTP
HTTPS	TCP、HTTP

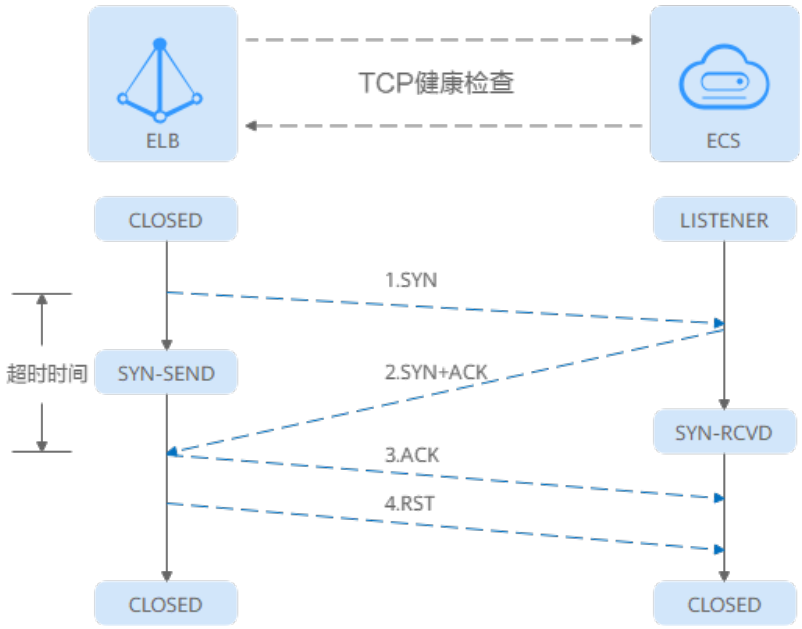
健康检查源 IP

共享型负载均衡器以网段100.125.0.0/16网段内的IP为健康检查源地址，向后端服务器发起健康检查探测请求。为确保健康检查结果正常，请确保后端服务器的安全组规则配置放行100.125.0.0/16网段，详情见**配置后端服务器的安全组**。

TCP 健康检查

对于四层（TCP）和七层（HTTP/HTTPS）后端协议，您可以配置TCP健康检查，通过发起TCP三次握手来获取后端服务器的状态信息，如**图2-8**所示。

图 2-8 TCP 健康检查



TCP健康检查的机制如下：

1. ELB节点根据健康检查配置，向后端服务器（IP+健康检查端口）发送TCP SYN报文。
2. 后端服务器收到请求报文后，如果相应的端口已经被正常监听，则会返回SYN+ACK报文。
   - 如果在超时时间内没有收到后端服务器的SYN+ACK报文，则判定健康检查失败。随后发送RST报文给后端服务器中断TCP连接。
   - 如果在超时时间内收到了SYN+ACK报文，则判定健康检查成功，并进一步发送ACK报文给后端服务器。随后发送RST报文给后端服务器中断TCP连接。

须知

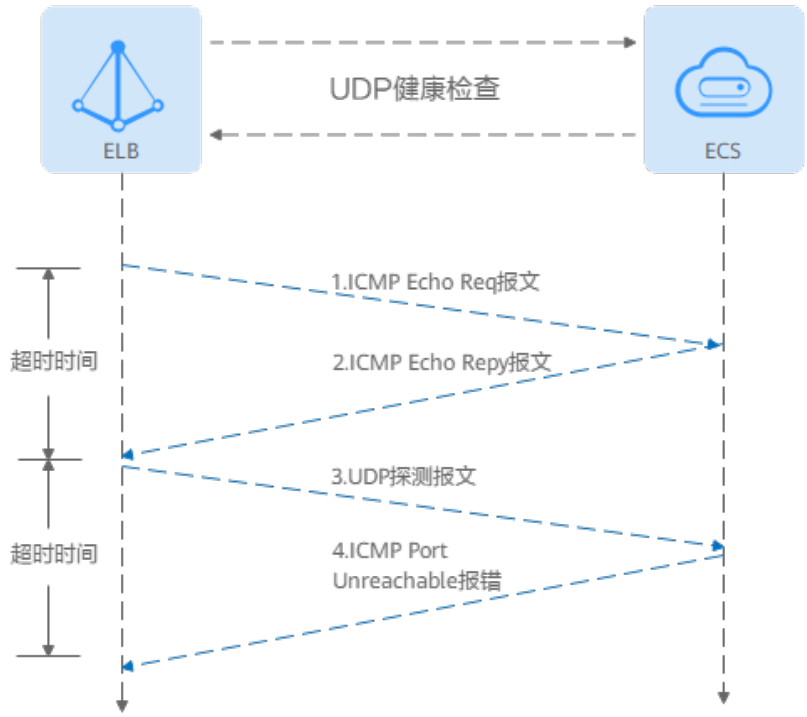
正常的TCP三次握手后，会进行数据传输，但是在健康检查时会发送RST中断建立的TCP连接。该实现方式可能会导致后端服务器中的应用认为TCP连接异常退出，并打印错误信息，如“Connection reset by peer”。解决方案如下：

- 采用**HTTP健康检查**。
- 后端服务器忽略健康检查的连接错误。

UDP 健康检查

对于四层（UDP）后端协议，默认配置UDP健康检查，通过发送UDP探测报文获取后端服务器的状态信息，如**图2-9**所示。

图 2-9 UDP 健康检查



UDP健康检查机制如下：

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

HTTP 健康检查

对于四层（TCP）和七层（HTTP/HTTPS）后端协议，您可以配置HTTP健康检查，通过HTTP GET请求来获取状态信息。检查原理如图2-10所示。

图 2-10 HTTP 健康检查

HTTP健康检查机制如下：

1. ELB节点根据健康检查配置，向后端服务器（IP+端口+检查路径）发出HTTP GET请求（可以选择设置域名）。

2. 后端服务器收到请求后，根据服务的情况返回相应的HTTP状态码。
   - 如果七层ELB节点在响应超时时间内收到了后端服务器的响应，将HTTP状态码与预置的状态码进行对比，如果匹配则认为健康检查成功，后端服务器运行正常。
   - 如果七层ELB节点在响应超时时间内没有收到后端服务器的响应，则判定健康检查失败。

说明

当共享型ELB实例的TCP监听器选择HTTP健康检查时，ELB会使用HTTP1.0发起探测。HTTP1.0采用短连接通信模式，即ELB发送完请求之后收到服务端拆链报文才会解析HTTP响应内容，所以请确保服务端发送完响应内容后立即主动断开TCP连接，否则会导致健康检查探测异常。

健康检查时间窗

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

健康检查时间窗由表2-20中的三个因素决定：

表 2-20 健康检查时间窗的影响因素

影响因素	说明
检查间隔	每隔多久进行一次健康检查。
超时时间	等待服务器返回健康检查的时间。
健康检查阈值	判定健康检查结果正常或异常时，所需的健康检查连续成功或失败的次数。

健康检查时间窗的计算方法如下：

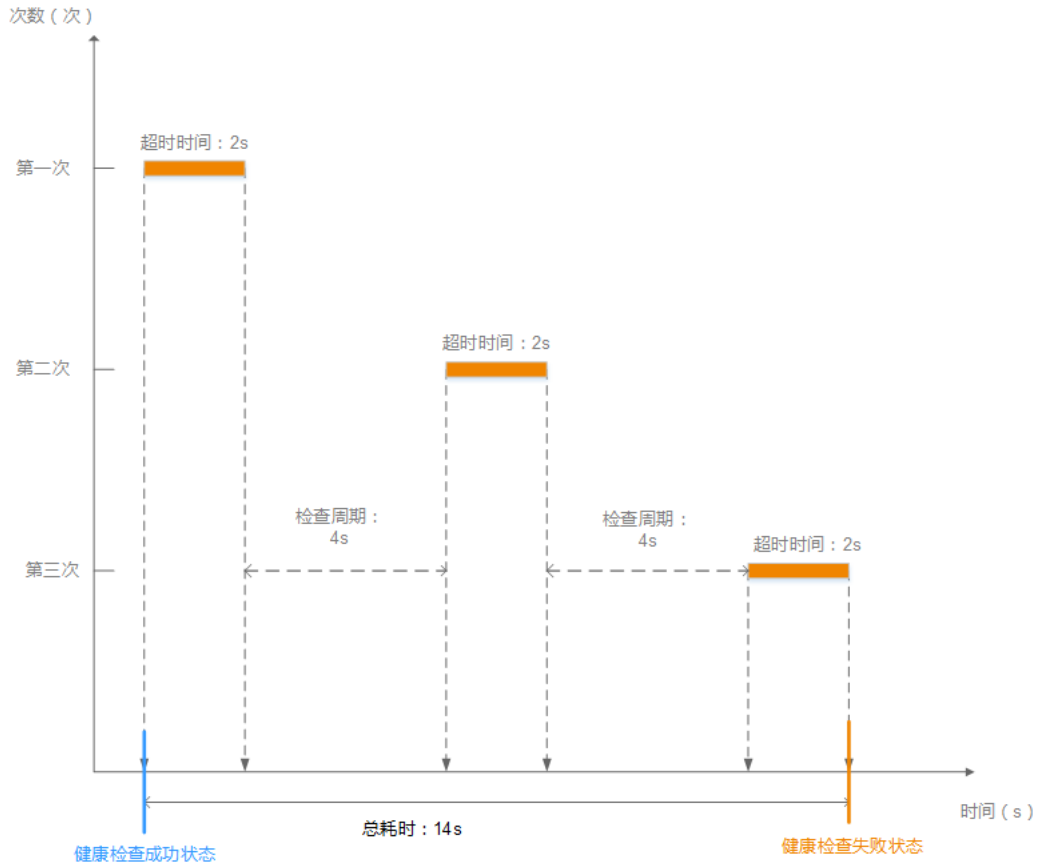
- 健康检查成功时间窗 = 超时时间×健康检查正常阈值 + 检查间隔×(健康检查正常阈值-1)
- 健康检查失败时间窗 = 超时时间×健康检查异常阈值 + 检查间隔×(健康检查异常阈值-1)

如图2-11所示：

- 检查间隔：4s
- 超时时间：2s
- 健康检查异常阈值：3次

健康检查检测到后端服务器从正常到失败状态，健康检查失败时间窗 = 超时时间×健康检查异常阈值+检查间隔×(健康检查异常阈值-1) = 2 x 3+4 x (3-1) = 14s。

图 2-11 健康检查失败时间窗



健康检查异常排查

如果您的健康检查异常，排查方法请参考**健康检查异常如何排查**。

2.4.2.2 流量分配策略介绍

分配策略类型总览

负载均衡会根据配置的流量分配策略，将来自客户端的请求按照对应的流量分配策略转发至相应的后端服务器。

共享型弹性负载均衡支持加权轮询算法、加权最小连接、源IP算法等多种分配策略，用于支持不同的业务场景。

本文列出共性型弹性负载均衡支持的所有分配策略。

表 2-21 流量分配策略对比

分配策略类型	描述
加权轮询算法	根据组内后端服务器设置的权重，依次将请求分发给不同的服务器。
加权最少连接	将请求分发给（当前连接/权重）比值最小的后端服务器进行处理。

分配策略类型	描述
一致性哈希算法：源IP算法	对请求的特定字段进行一致性哈希计算，并根据计算的哈希值将请求均匀地分配到后端服务器中。相同哈希值的请求，将会被分配到相同的后端服务器，即使后端服务器组中的后端服务器个数在发生变化。 源IP算法：根据请求的源IP地址进行哈希计算，源IP相同的请求会被分配到同一台后端服务器。

分配策略详情

共享型负载均衡支持加权轮询算法、加权最少连接、源IP算法。

加权轮询算法

图2-12展示弹性负载均衡器使用加权轮询算法的流量分发流程。假设可用区内有2台权重相同的后端服务器，负载均衡器节点会将50%的客户端流量分发到其可用区中的每一台后端服务器。

图 2-12 加权轮询算法流量分发

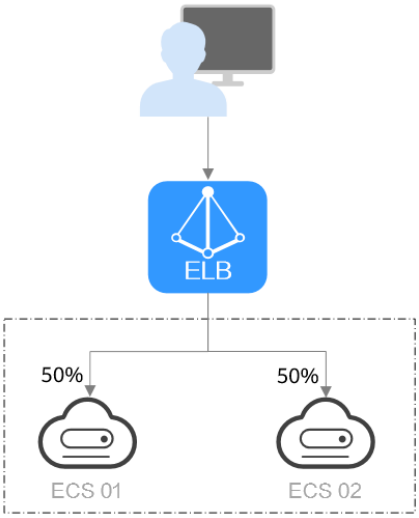


表 2-22 加权轮询算法说明

概述	加权轮询算法根据组内后端服务器设置的权重，依次将请求分发给不同的服务器。权重大的后端服务器被分配的概率高，相同权重的服务器处理相同数目的连接数。

推荐场景	加权轮询算法常用于短连接服务，例如HTTP等服务。 • 灵活负载：当对后端服务器的负载分配有更精细的要求时，可以通过设置不同的权重来实现对服务器的灵活调度，使得性能较好的服务器能够处理更多的请求。 • 动态负载：当后端服务器的性能和负载情况经常发生变化时，可以通过动态调整权重来适应不同的场景，实现负载均衡。
缺点	• 加权轮询算法需要配置每个后端服务器的权重，对于有大量后端服务器或频繁变动的场景，运维工作量较大。 • 权重设置不准确可能会导致负载不均衡的情况，需要根据后端服务器的实际性能进行调整。

加权最少连接

图2-13展示弹性负载均衡器使用加权最少连接算法的流量分发流程。假设可用区内有2台权重相同的后端服务器，ECS 01已有100个连接，ECS 02已有50个连接，则新的连接会优先分配到ECS 02上。

图 2-13 加权最少连接算法流量分发

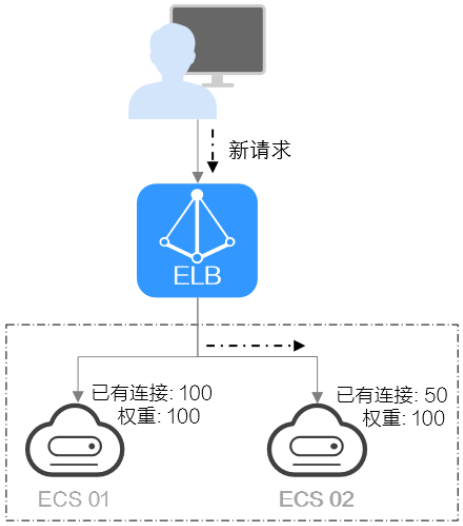


表 2-23 加权最少连接说明

概述	最少连接是通过当前活跃的连接数来评估服务器负载情况的一种动态负载均衡算法。加权最少连接就是在最少连接数的基础上，根据服务器的不同处理能力，给每个服务器分配不同的权重，使其能够接受相应权值数的服务请求。

推荐场景	加权最少连接常用于长连接服务，例如数据库连接等服务。 • 灵活负载：当后端服务器的性能差异较大时，同时考虑后端服务器的连接数和权重来进行负载，可以更精确地将请求分配到后端服务器上，避免出现过载或空闲的情况。 • 动态负载：当后端服务器的连接数和负载情况经常发生变化时，可以通过实时监控连接数变化进行动态的负载调整。 • 更高稳定负载：对于需要高稳定性的业务场景，加权最小连接算法可以降低后端服务器的峰值负载，提高业务的稳定性和可靠性。
缺点	• 加权最小连接算法的实现更复杂：需要实时监控负载均衡器与后端服务器之间的连接数变化。 • 对后端服务器的连接数存在依赖：算法依赖于准确获取负载均衡服务和后端服务器的连接数，如果获取不准确或监控不及时，可能导致负载分配不均衡。同时由于算法只能统计到负载均衡器与后端服务器之间的连接，后端服务器整体连接数无法获取，因此对于后端服务器挂载到多个弹性负载均衡的场景，也可能导致负载分配不均衡。 • 新增后端服务器时可能导致过载：如果已有的连接数过大，大量的新建连接会被分配到新加入的后端服务器上，可能会导致新加入的后端服务器瞬间过载影响系统稳定性。

源 IP 算法

图2-14展示弹性负载均衡器使用源IP算法的流量分发流程。假设可用区内有2台权重相同的后端服务器，ECS 01已经处理了一个IP-A的请求，则IP-A新发起的请求会自动分配到ECS 01上。

图 2-14 源 IP 算法流量分发

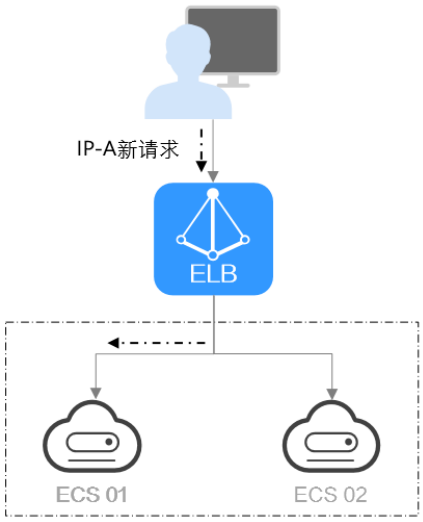


表 2-24 源 IP 算法说明

概述	根据请求的源IP地址进行一致性哈希计算，源IP地址相同的请求会被分配到同一台后端服务器。
推荐场景	源IP算法常用于需要保持用户状态或会话的应用。 ● 基于源IP的会话保持：源IP算法可以确保源IP相同的请求具有相当的哈希值并被分配到同一台后端服务器上，从而实现会话保持。 ● 保持数据一致：一致性哈希算法将相同哈希值的请求调度到相同后端服务器上，保证多次请求数据的一致性。 ● 均衡性要求较高：一致性哈希算法能够提供相对均衡的负载分配效果，减少后端服务器的负载差异。
缺点	● 后端服务器数量变动可能导致不均衡：一致性哈希算法在后端服务器数量变动时会尽力保障请求的一致性，部分请求会重新分配。当后端服务器数量较少时，重新分配过程中有可能导致负载不均衡的情况发生。 ● 扩展复杂性增加：由于一致性哈希算法将请求根据哈希因子进行哈希计算，当后端服务器数量变化时，会导致一部分请求需要重新分配，这会引入一定的复杂性。

2.4.2.3 会话保持介绍

会话保持，指负载均衡器可以识别客户与服务器之间交互过程的关联性，在实现负载均衡的同时，保持将其他相关联的访问请求分配到同一台服务器上。

会话保持有什么作用呢，举例说明如下：如果有一个用户在服务器甲登录了，访问请求被分配到服务器甲，在很短的时间，这个用户又发出了一个请求，如果没有会话保持功能的话，这个用户的请求很有可能会被分配到服务器乙去，这个时候在服务器乙上是没有登录的，所以需要重新登录。如果配置了会话保持功能，上述一系列的操作过程将由同一台服务器完成，避免被负载均衡器分配到不同的服务器上，提高访问效率。

四层会话保持和七层会话保持的区别

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

表 2-25 四层会话保持和七层会话保持的区别

类型	说明	支持的会话保持类型	会话保持时间	会话保持失效的场景
四层会话保持	当使用的协议为TCP或UDP时，即为四层会话保持。	**源IP地址**：基于源IP地址的简单会话保持，将请求的源IP地址作为散列键（HashKey），从静态分配的散列表中找出对应的服务器。即来自同一IP地址的访问请求会被转发到同一台后端服务器上进行处理。	• 默认时间：20分钟 • 最长时间：60分钟 • 取值范围：1-60分钟	• 客户端的源IP地址发生变化。 • 客户端访问请求超过会话保持时间。
七层会话保持	当使用的协议为HTTP或HTTPS时，即为七层会话保持。	• **负载均衡器cookie**：负载均衡器会根据客户端第一个请求生成一个cookie，后续所有包含这个cookie值的请求都会由同一个后端服务器处理。 • **应用程序cookie**：该选项依赖于后端应用。后端应用生成一个cookie值，后续所有包含这个cookie值的请求都会由同一个后端服务器处理。	• 默认时间：20分钟 • 最长时间：1440分钟 • 取值范围：1-1440分钟	• 如果客户端发送请求未附带cookie，则会话保持无法生效。 • 客户端访问请求超过会话保持时间。

说明

- 当**分配策略类型**选择“源IP算法”时，四层和七层会话已支持基于源IP地址的会话保持。
- 当**分配策略类型**选择“加权轮询算法”或“加权最少连接”时，才可配置会话保持。

约束与限制

- 如果您需要从**云专线**、**VPN**、**云连接**访问ELB，请您使用源IP负载均衡算法代替会话保持功能。
- 共享型负载均衡支持源IP地址、负载均衡器cookie、应用程序cookie的会话保持类型。

说明

- 对于HTTP、HTTPS类型的后端服务器，变更会话保持的状态可能会导致监听器与后端服务器组的访问出现秒级中断。
- 如果您开启了会话保持功能，那么有可能会造成后端服务器的访问量不均衡。如果出现了访问不均衡的情况，建议您暂时关闭会话保持功能，再观察是否依然存在访问不均衡的情况。

2.4.3 创建后端服务器组

操作场景

负载均衡实例的监听器绑定后端服务器组后，才能正常转发访问请求。

说明

本章节指导用户创建可关联至共享型负载均衡使用的后端服务器组。

您可通过三种方式为负载均衡实例创建后端服务器组，详见**表1 创建后端服务器组指引**。

表 2-26 创建后端服务器组指引

创建场景	创建步骤
独立创建后端服务器组并关联至负载均衡实例使用	**操作步骤**。
添加监听器时，选择“新创建”后端服务器组。	用户可根据使用需求添加不同协议的监听器，详情见**什么是监听器**。 具体添加步骤如下： • **添加TCP监听器**。 • **添加UDP监听器**。 • **添加HTTP监听器**。 • **添加HTTPS监听器**。
更换监听器的后端服务器组时，选择“创建后端服务器组”。	**更换后端服务器组**。

约束与限制

共享型负载均衡器下的后端服务器组仅能被一个监听器使用。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 弹性负载均衡 > 后端服务器组”。

5. 在“后端服务器组”界面，单击页面右上角“创建后端服务器组”按钮。
6. 配置后端分配策略，参数详情请参见**表2-27**。

表 2-27 配置后端分配策略参数说明

参数	说明
负载均衡类型	可使用该后端服务器组的负载均衡实例类型，选择“共享型”。
所属负载均衡器	使用该后端服务器组的负载均衡实例。
名称	待创建的后端服务器组的名称。
后端协议	后端云服务器自身提供的网络服务的协议。 支持选择的协议有：HTTP、TCP、UDP。
分配策略类型	负载均衡采用的算法。 • 加权轮询算法：根据后端服务器的权重，按顺序依次将请求分发给不同的服务器，权重大的后端服务器被分配的概率高。 • 加权最少连接：加权最少连接是在最少连接数的基础上，根据服务器的不同处理能力，给每个服务器分配不同的权重，使其能够接受相应权值数的服务请求。 • 源IP算法：对不同源IP的访问进行负载分发，同时使得同一个客户端IP的请求始终被派发至某特定的服务器。 更多关于分配策略的信息，请参见**流量分配策略介绍**。
会话保持	开启会话保持后，弹性负载均衡将属于同一个会话的请求都转发到同一个服务器进行处理。 更多关于会话保持的信息，请参见**会话保持介绍**。
会话保持类型	当会话保持开启后，需选择会话保持类型： • **源IP地址：**基于源IP地址的简单会话保持，将请求的源IP地址作为散列键（HashKey），从静态分配的散列表中找出对应的服务器云主机。即来自同一IP地址的访问请求会转发到同一台后端服务器云主机上进行处理。 • **负载均衡器cookie：**负载均衡器会根据客户端第一个请求生成一个cookie，后续所有包含这个cookie值的请求都会由同一个后端服务器处理。 • **应用程序cookie：**该选项依赖于后端应用。后端应用生成一个cookie值，后续所有包含这个cookie值的请求都会由同一个后端服务器处理。 **说明** • 当后端协议选择TCP/UDP时，支持源IP地址类型。 • 当后端协议选择HTTP时，支持负载均衡器cookie和应用程序cookie。

参数	说明
会话保持时间（分钟）	当会话保持开启时，需添加会话保持时间。 ● 四层会话保持的时间取值范围为1~60分钟。 ● 七层会话保持的时间取值范围为1~1440分钟。
描述	后端服务器组的描述

7. 单击“下一步”，添加后端服务器并配置健康检查，配置健康检查参数请参见**表2-28**。更多关于健康检查的信息，请参见**健康检查介绍**。

表 2-28 配置健康检查参数说明

参数	说明
是否开启	开启或者关闭健康检查。 如果开启健康检查，您可单击“参数设置”设置健康检查的参数。
健康检查协议	● 健康检查支持选择TCP、HTTP方式。 ● 当后端协议选择UDP，健康检查协议默认为UDP且不可修改。
健康检查域名	如果健康检查协议选择HTTP协议，则该项是必选参数。 健康检查的请求域名，默认使用各后端服务器的内网IP。 若指定特定域名，只能由字母，数字，中划线组成，中划线不能在开头或末尾，至少包含两个字符串，单个字符串不能超过63个字符，字符串间以点分割，且总长度不超过100个字符。
健康检查端口	健康检查端口号，取值范围[1，65535]，为可选参数。 **说明** 默认使用后端云服务器的业务端口进行健康检查。指定特定端口后，使用指定的端口进行健康检查。
健康检查路径	如果健康检查协议选择HTTP协议，则该项是必选参数。 指定健康检查的URL地址。检查路径只能以/开头，长度范围[1-80]。 支持使用英文字母、数字和‘-’、‘/’、‘.’、‘?’、‘#’、‘%’、‘&’。
检查间隔（秒）	每次健康检查响应的最大间隔时间。 取值范围[1-50]。
超时时间（秒）	每次健康检查响应的最大超时时间。取值范围[1-50]。

参数	说明
健康检查正常阈值	表示判定后端服务器为正常状态时，所需的连续健康检查成功次数，取值范围[1-10]。
健康检查异常阈值	表示判定后端服务器为异常状态时，所需的连续健康检查失败次数，取值范围[1-10]。

8. 单击“下一步”。
9. 确认配置无误后，单击“立即创建”。

2.4.4 修改后端服务器组配置

2.4.4.1 配置后端服务器组修改保护

操作场景

您可以对后端服务器组开启修改保护功能，防止因误操作导致后端服务器组的配置被修改或后端服务器组被删除。

约束与限制

后端服务器组开始修改保护后，用户将不能执行以下操作：

- 修改后端服务器组配置的基本信息。
- 为后端服务器组配置健康检查。
- 为后端服务器组添加后端服务器。
- 删除后端服务器组及其所关联资源。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 弹性负载均衡 > 后端服务器组”。
5. 在后端服务器组界面，单击需要配置修改保护的后端服务器组名称。
6. 在后端服务器组的“基本信息”页签下，单击修改保护右侧的“设置”。
7. 在设置修改保护弹窗中，开启“修改保护”开关。
8. 单击“确定”。

说明

如果您需要修改后端服务器组的配置或删除后端服务器组，请先关闭“修改保护”开关。

2.4.4.2 修改后端服务器组配置场景说明

后端服务器组创建后，用户可根据使用需求修改后端服务器组的健康检查配置和基本信息。

健康检查

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

健康检查功能详情参见**健康检查介绍**。

修改健康检查步骤详情见**修改健康检查配置**。

后端服务器组的基本信息

选定目标后端服务器后，可对以下基本信息进行修改，详情见**表2-29**。

表 2-29 支持修改的后端服务器组信息

参数	修改场景说明
名称	用户可自定义后端服务器组的名称。 修改名称步骤详情见**修改流量分配策略配置**。
分配策略类型	用户可根据使用需求修改后端服务器组的流量分配策略。 后端服务器组根据配置的流量分配策略转发流量到不同的后端服务器。 流量分配策略详情参见**流量分配策略介绍**。 修改流量分配策略步骤详情见**修改流量分配策略配置**。
会话保持	用户可根据使用需求开启或关闭会话保持。 当用户开启了会话保持功能后，会话保持可以使来自同一客户端的请求被转发到同一台后端服务器上，客户端的请求将无需重复登录后端服务器。 开启了会话保持功能，也可能会造成后端服务器的访问量不均衡，此时建议您暂时关闭会话保持功能，再观察是否依然存在访问不均衡的情况。 会话保持功能详情参见**会话保持介绍**。 修改会话保持步骤详情见**修改会话保持配置**。
描述	用户可自定义对目标后端服务器组的描述。 修改描述步骤详情见**修改流量分配策略配置**。

2.4.4.3 修改健康检查配置

操作场景

本章节指导用户在后端服务器组创建后修改健康检查配置。

若切换健康检查协议，负载均衡会根据新的健康检查协议重新检查后端服务器。健康检查通过后，负载均衡向后端服务器继续转发流量。

健康检查切换周期内，客户端可能收到503错误码。

约束与限制

- 健康检查协议与服务器组的后端协议是两个相互独立的能力，所以健康检查协议可以与后端协议不同。
- 为了减少后端服务器的CPU占用，建议您使用TCP协议做健康检查。如果您希望使用HTTP健康检查协议，建议使用HTTP+静态文件的方式。
- 为保证健康检查功能正常，配置健康检查后必须放通对应的安全组规则，详情请参考**配置后端服务器的安全组（共享型）**。

说明

开启健康检查后不会影响已建立连接的流量转发，负载均衡会立即对后端服务器执行健康检查。

- 如果健康检查正常，则新建连接的流量会根据分配策略和权重向该服务器转发流量。
- 如果健康异常，则系统会设置该服务器状态为异常，不转发新的流量到该服务器。

开启健康检查

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 弹性负载均衡 > 后端服务器组”。
5. 在后端服务器组界面，单击需要修改健康检查的后端服务器组名称。
6. 在后端服务器组的“基本信息”页签下，单击健康检查区域右侧的“配置健康检查”。
7. 在“配置健康检查”弹窗，可根据需要参考**表2-30**进行配置。

表 2-30 配置健康检查参数说明

参数	说明
是否开启	开启或者关闭健康检查。
健康检查协议	健康检查请求的协议类型。 当后端协议选择UDP，健康检查协议默认为UDP且不可修改。 共享型支持选择TCP、HTTP协议

参数	说明
健康检查域名	如果健康检查协议选择HTTP协议，则该项是必选参数。 健康检查的请求域名。 ● 默认使用后端服务器的内网IP为域名。 ● 您也可选择指定特定域名，特定域名只能由字母，数字，中划线组成，中划线不能在开头或末尾，至少包含两个字符串，单个字符串不能超过63个字符，字符串间以点分割，且总长度不超过100个字符。
健康检查端口	健康检查端口号，取值范围[1，65535]，为可选参数。 **说明** 默认使用后端云服务器的业务端口进行健康检查。指定特定端口后，使用指定的端口进行健康检查。
健康检查路径	如果健康检查协议选择HTTP协议，则该项是必填参数。 指定健康检查的URL地址。检查路径只能以/开头，长度范围[1-80]。 后端服务器组关联共享型负载均衡器：检查路径支持使用英文字母、数字和‘-’、‘/’、‘.’、‘?’、‘%’、‘&’以及‘_’。
检查间隔（秒）	每次健康检查响应的最大间隔时间。 取值范围[1-50]。
超时时间（秒）	每次健康检查响应的最大超时时间。取值范围[1-50]。
健康检查正常阈值	表示判定后端服务器为正常状态时，所需的连续健康检查成功次数，取值范围[1-10]。
健康检查异常阈值	表示判定后端服务器为异常状态时，所需的连续健康检查失败次数，取值范围[1-10]。

8. 单击“确定”。

关闭健康检查

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 弹性负载均衡 > 后端服务器组”。
5. 在后端服务器组界面，单击需要关闭健康检查的后端服务器组名称。
6. 在后端服务器组的“基本信息”页签下，单击健康检查区域右侧的“配置健康检查”。

7. 在“配置健康检查”界面，可根据需要关闭健康检查。
8. 单击“确定”。

2.4.4.4 修改流量分配策略配置

操作场景

本章节指导用户在后端服务器组中的修改流量分配策略。

流量分配策略详情参见**流量分配策略介绍**。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 弹性负载均衡 > 后端服务器组”。
5. 在后端服务器组列表，在目标后端服务器组所在行的操作列单击“编辑”。
6. 在“修改后端服务器组”弹窗中进行修改，选择“分配策略类型”。
7. 单击“确定”。

说明

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

2.4.4.5 修改会话保持配置

操作场景

本章节指导用户在后端服务器组中修改会话保持功能。

说明

您还可以在进行“添加监听器”或“创建后端服务器组”操作时，配置会话保持功能。

开启会话保持

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 弹性负载均衡 > 后端服务器组”。
5. 在后端服务器组界面，在目标后端服务器组所在行的操作列单击“编辑”。
6. 在“修改后端服务器组”弹窗中，开启会话保持功能，配置会话保持类型以及会话保持时间参数。
7. 单击“确定”。

关闭会话保持

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 弹性负载均衡 > 后端服务器组”。
5. 在后端服务器组界面，在目标后端服务器组所在行的操作列单击“编辑”。
6. 在“修改后端服务器组”弹窗中，关闭会话保持功能。
7. 单击“确定”。

2.4.5 更换后端服务器组

操作场景

本章节指导用户更换在监听器下配置的默认转发后端服务器组。

ELB四层监听器（TCP/UDP）将客户端请求转发到默认后端服务器组。

ELB七层监听器（HTTP/HTTPS）将客户端的请求按转发策略的优先级进行转发。若用户未自定义转发策略，客户端请求将被转发至默认后端服务器组。

约束与限制

- 监听器开启重定向，不支持更换后端服务器组。
- 后端服务器组的后端协议应与监听器的前端协议匹配，匹配关系详见**表2-17**。
- 共享型负载均衡实例的后端服务器组仅支持更换已关联在本实例下且未被监听器使用的后端服务器组。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”列表，单击目标监听器所在的负载均衡名称。
5. 选择“监听器”页签，在监听器列表中，单击目标监听器的名称。
6. 在监听器的“基本信息”页签，单击“后端服务器组”区域右侧“更换后端服务器组”。
7. 在弹出的对话框中，单击服务器组名称方框。

   将显示搜索框、所有可选服务器组和“创建后端服务器组”。

   a. 选择已有服务器组，可直接单击目标服务器组名称，也可在搜索框中按名称搜索。
   b. 您也可单击“创建后端服务器组”创建新的后端服务器组。创建完成后单击刷新按钮，在已有服务器组中进行选择。

   说明

   若创建新的服务器组，后端协议应与监听器的前端协议匹配才可被当前监听器使用。

8. 单击“确定”。

2.4.6 查看后端服务器组

操作场景

本章节指导用户查看后端服务器组的的详细信息，主要信息如下：

- 基本信息：后端服务器组的基本信息，包括名称、ID和后端协议等信息。
- 健康检查：后端服务器组是否开启健康检查以及健康检查的详细配置信息。
- 后端服务器：后端服务器组中已添加的后端服务器资源。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 弹性负载均衡 > 后端服务器组”。
5. 在后端服务器组列表，单击待查看的后端服务器组名称。
6. 选择不同的页签，查看需要的信息。
   a. 在“基本信息”页签下，查看服务器组基本信息和健康检查配置。
   b. 在“后端服务器”页签下，查看服务器组中已添加的后端服务器。

2.4.7 删除后端服务器组

操作场景

本章节指导用户删除已创建的后端服务器组。

约束与限制

- 如果后端服务器组已被监听器使用，无法执行删除，需先将目标后端服务器组从监听器下释放。
  - 在监听器下释放默认转发后端服务器组，详情请参见**更换后端服务器组**。
  - 七层监听器还需保证自定义的转发策略不使用该后端服务器组。
- 如果后端服务器组中包含后端服务器，不能执行删除操作，需先移除已添加的后端服务器。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 弹性负载均衡 > 后端服务器组”。

5. 在后端服务器组列表，在目标后端服务器组所在行的操作列单击“删除”。
6. 在“确认删除后端服务器组”对话框中，单击“确定”。

2.5 后端服务器

2.5.1 后端服务器概述

负载均衡器会将客户端的请求转发给后端服务器处理。

负载均衡器支持随时增加或减少后端服务器数量，保证应用业务的稳定和可靠，屏蔽单点故障。

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

共享型负载均衡实例仅支持添加同VPC的弹性云服务器（ECS）实例作为后端服务器，操作详情见**后端云服务器**。

注意事项

- 建议您选择相同操作系统的后端服务器，以便日后管理和维护。
- 新添加后端服务器后，若健康检查开启，负载均衡器会向后端服务器发送请求以检测其运行状态，响应正常则直接上线，响应异常则开始健康检查机制定期检查，检查正常后上线。
- 关机或重启已有业务的后端服务器，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服务器的访问量不均衡。如果出现了访问不均衡的情况，建议您暂时关闭会话保持功能，观察一下是否依然存在这种情况。

约束与限制

- 一个后端服务器组最多支持添加500个后端服务器。
- 确保后端服务器的安全组已针对后端服务器端口和健康检查端口配置了相应的入方向规则，详情请参见**配置后端服务器的安全组**。

后端服务器的权重

在后端服务器组内添加后端服务器后，需设置后端服务服务器的转发权重。权重越高的后端服务器将被分配到越多的访问请求。

每台后端服务器的权重取值范围为[0, 100]，新的请求不会转发到权重为0的后端服务器上。

以下三种流量分配策略支持权重设置，详情见**表2-31**，更多流量策略分配策略详情见**流量分配策略介绍**。

表 2-31 流量分配策略的权重设置说明

流量分配策略类型	权重设置说明
加权轮询算法	• 在非0的权重下，负载均衡器会将请求按权重值的大小分配给所有的后端服务器，且在轮询时，权重大的后端服务器被分配的概率高。 • 当后端服务器的权重都设置为相等时，负载均衡器将按照简单的轮询策略分发请求。
加权最少连接	• 在非0的权重下，负载均衡器会通过 overhead=当前连接数/权重 来计算每个服务器负载。 • 每次调度会选择overhead最小的后端服务器。
源IP算法	• 在非0的权重下，在一段时间内，同一个客户端的IP地址的请求会被调度至同一个后端服务器上。 • 每台后端服务器的权重取只做0和非0的区分。

2.5.2 配置后端服务器的安全组

为了确保负载均衡器与后端服务器进行正常通信和健康检查正常，添加后端服务器后必须检查后端服务器所在的安全组规则和网络ACL规则。

流量经共享型ELB转到后端服务器以后，源IP会被转换为100.125.0.0/16的IP。

- 后端服务器的安全组规则必须配置放行100.125.0.0/16网段。查看如何**配置安全组规则**。
- 网络ACL规则为子网级别的可选安全层，若ELB的后端子网关联了网络ACL，网络ACL规则必须配置允许源地址为ELB后端子网所属网段。查看如何**配置网络ACL规则**。

说明

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

约束与限制

- 后端服务器组开启了健康检查，后端服务器的安全组规则必须配置放通ELB用于健康检查的协议和端口。
- 如果健康检查使用UDP协议，安全组规则还需放行ICMP协议，否则无法对已添加的后端服务器执行健康检查。

配置安全组规则

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

1. 登录管理控制台。

2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 选择“计算 > 弹性云服务器”。
4. 在弹性云服务器列表，单击待变更安全组规则的弹性云服务器名称。
   系统跳转至该弹性云服务器详情页面。
5. 选择“安全组”页签，单击安全组名称，查看安全组规则。
6. 单击“ID”或者“更改安全组规则”，系统自动跳转至安全组界面。
7. 在入方向规则页签，单击“添加规则”，根据所在后端服务器组的后端协议类型按**表2-32**配置安全组入方向的访问规则。

   表 2-32 放通安全组规则（共享型）

后端协议	策略	协议端口	源地址
HTTP	允许	协议：TCP 端口：后端服务器端口和健康检查端口	100.125.0.0/16
TCP	允许	协议：TCP 端口：健康检查端口	100.125.0.0/16
UDP	允许	协议：UDP、ICMP 端口：健康检查端口	100.125.0.0/16

8. 单击“确定”，完成安全组规则配置。

配置网络 ACL 规则

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

您可以通过配置网络ACL入方向规则，放行100.125.0.0/16网段。

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

说明

负载均衡器的IP地址不受后端子网网络ACL规则的限制，所以能够被客户端直接访问。建议您使用监听器的访问控制功能限制客户端访问负载均衡器。详情请参考**访问控制策略**。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。

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

2.5.3 后端云服务器

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

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

约束与限制

- 仅支持添加与共享型负载均衡实例同VPC的云服务器。
- 后端云服务器支持添加弹性云服务器和裸金属服务器两种服务器实例。如果共享型弹性负载均衡的监听器开启“获取客户端IP”功能，将对裸金属服务器的规格有兼容性要求，部分存量规格实例无法添加，支持添加的实例规格详见**《裸金属服务器实例家族》**。

添加后端云服务器

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 弹性负载均衡 > 后端服务器组”。
1. 在“后端服务器组”界面，单击需要添加后端服务器的后端服务器组名称。
2. 切换到“后端服务器”页签，选择下方“云服务器”页签，并单击“添加”。
3. 支持通过指定的关键字搜索后端服务器。私网IP地址支持选择主网卡和扩展网卡。
4. 设置后端端口和服务器的权重，单击“完成”。

   支持批量设置后端端口。

修改后端云服务器的权重和端口

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 弹性负载均衡 > 后端服务器组”。
5. 在“后端服务器组”界面，单击需要修改后端服务器端口/权重的后端服务器组名称。
6. 在该后端服务器组界面，选择“后端服务器”页签，单击下方“云服务器”区域。
7. 勾选需要设置权重的后端服务器，单击服务器列表上方的“修改权重”。
8. 在“修改权重”弹窗页面，根据需要修改权重/端口的后端数量进行相应操作。
   - 修改单个后端服务器权重：在目标服务器所在行，设置“权重”。
   - 批量修改后端服务器权重：在“批量修改权重”后的输入框中设置权重值，单击输入框右侧的“确定”。

   说明

   将后端服务器的权重值批量设置为“0”，可以实现批量屏蔽后端服务器。
9. 单击弹窗下方的“确定”，完成设置。

移除后端云服务器

说明

移除后端服务器后，长连接在超时时间内会复用TCP连接，请求会继续转发，仍然会有流量进入后端服务器。已有连接在请求超时时间后没有数据传输，ELB会将连接断开。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 弹性负载均衡 > 后端服务器组”。
5. 在“后端服务器组”界面，单击需要移除后端服务器的后端服务器组名称。
6. 切换到“后端服务器”页签，选择下方“云服务器”页签。
7. 勾选需要移除的云服务器，单击服务器列表上方的“移除”。
8. 在移除后端服务器的对话框中单击“确定”。

2.6 安全管理

2.6.1 共享型 ELB 获取客户端真实 IP

操作场景

一般情况下，共享型ELB会使用100.125网段的IP和后端服务器进行通信。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，此时，ELB和后端服务器之间直接使用真实的IP进行通信。

目前，共享型负载均衡对“获取客户端IP”功能的支持情况如表2-33。

表 2-33 共享型负载均衡“获取客户端 IP”功能说明

监听器类型	开启“获取客户端IP”	关闭“获取客户端IP”
四层（TCP/UDP）监听器	√	√
七层（HTTP/HTTPS）监听器	默认开启	×

约束与限制

- 开启/关闭“获取客户端IP”的过程中，如果监听器已经添加了后端服务器，则访问监听器的流量会中断，中断时间为10秒（后端服务器组配置的健康检查间隔*2）。
- 开启“获取客户端IP”之后，不支持同一台服务器既作为后端服务器又作为客户端的场景。如果后端服务器和客户端使用同一台服务器，且开启“获取客户端IP”，则后端服务器会根据报文源IP为本地IP判定该报文为本机发出的报文，无法将应答报文返回给ELB，最终导致回程流量不通。
- 如果监听器之前已经添加了后端服务器、并且开启了健康检查功能，开启“获取客户端IP”功能会重新上线后端服务器，新建流量会有1-2个健康检查间隔的中断。
- 开启此功能后，执行后端服务器迁移任务时，可能出现流量中断（例如单向下载、推送类型的流量）。所以后端服务器迁移完成后，需要通过报文重传来恢复流量。

开启“获取客户端 IP”

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要修改监听器的负载均衡名称，进入监听器列表页。
5. 您可以通过以下两种操作入口，开启监听器的“获取客户端IP”功能。
   - 在目标监听器所在行的“操作”列，单击“编辑”。
   - 单击目标监听器名称，进入监听器的基本信息页面，单击“编辑监听器”。
6. 在“编辑监听器”弹窗页面，开启“获取客户端IP”开关。

7. 确认相关信息，单击“确定”。

说明

开启“获取客户端IP”功能后，您还需设置后端服务器的安全组、网络ACL、操作系统和软件的安全规则，使客户端的IP地址能够访问后端服务器。

关闭“获取客户端 IP”

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要修改监听器的负载均衡名称，进入监听器列表页。
5. 您可以通过以下两种操作入口，关闭监听器的“获取客户端IP”功能。
   - 在目标监听器所在行的“操作”列，单击“编辑”。
   - 单击目标监听器名称，进入监听器的基本信息页面，单击“编辑监听器”。
6. 在“编辑监听器”弹窗页面，关闭“获取客户端IP”开关。
7. 确认相关信息，单击“确定”。

其他获取客户端真实 IP 方法

负载均衡的监听器还可通过如下补充方法获取客户端的真实IP，详情见**表2-34**。

表 2-34 共享型负载均衡获取客户端真实 IP 补充方法

监听器类型	获取客户端真实IP补充方法
四层（TCP）监听器	配置**TOA插件**获取。
七层（HTTP/HTTPS）监听器	**七层服务获取客户端IP**。

2.6.2 开启 HTTP/2 提升通信效率

HTTP/2 概述

HTTP/2即超文本传输协议 2.0，能通过二进制分帧提升网络通信效率，实现多路复用减少延迟。如果您需要保证HTTPS业务更加安全高效，可以在配置HTTPS监听器时，开启HTTP/2功能。

约束与限制

仅HTTPS监听器支持HTTP/2功能。

管理 HTTPS 监听器的 HTTP/2 功能

在添加HTTPS监听时，您可以开启HTTP/2功能。在HTTPS监听器添加完成后，您也可以开启或关闭HTTP/2功能。

新添加 HTTPS 监听器

在添加HTTPS监听时，您可以开启HTTP/2功能。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要开启HTTP/2功能的监听器的负载均衡器名称。
5. 在该负载均衡界面的“监听器”页签，单击“添加监听器”。
6. 在“添加监听器”界面，前端协议选择“HTTPS”。
7. 在“添加监听器”界面，展开高级配置，打开HTTP/2功能。
8. 确认配置，单击“提交”。

图 2-15 开启 HTTP 监听器的 HTTP/2 功能

已有 HTTPS 监听器

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要修改HTTP/2功能的负载均衡器名称。
5. 在“监听器”页签，单击需要修改HTTP/2功能开关的监听器名称。

6. 在监听器的“基本信息”页面，单击“编辑监听器”。
7. 在“编辑监听器”界面，展开高级配置，开启或者关闭HTTP/2功能。
8. 单击“确定”。

图 2-16 修改 HTTPS 监听器的 HTTP/2 功能

2.6.3 开启 SNI 证书实现多域名访问

操作场景

当您需要在同一个监听器中，根据HTTPS请求域名的不同来选择不同的证书进行认证并将请求分发至不同的后端服务器组时，您可通过开启SNI功能来实现配置多域名HTTPS网站。

SNI（Server Name Indication）是为了解决一个服务器使用域名证书的TLS扩展。开启SNI之后，用户需要添加域名对应的证书，允许客户端在发起SSL握手请求时就提交请求的域名信息，负载均衡收到SSL请求后，会根据域名去查找证书。如果找到域名对应的证书，则返回该证书；如果没有找到域名对应的证书，则返回缺省证书。

约束与限制

- 仅HTTPS 监听器，支持开启SNI功能，支持绑定多个证书。
- 一个HTTPS监听器默认支持配置30个SNI证书，监听器关联的所有SNI证书默认支持的域名总数为30个。

前提条件

- 已创建负载均衡器，具体步骤可参照**创建共享型负载均衡器**。
- 已经创建用于SNI证书，具体步骤可参照**创建证书**。
- 已经创建HTTPS监听器，具体步骤可参照**添加HTTPS监听器**。

SNI 证书约束

- ELB不会自动更新证书，如果您有证书过期了，需要手动更换或者删除证书，详见**绑定/更换证书**。
- 用于SNI的证书，需要指定域名，指定的域名必须与证书中的域名保持一致。
- 目前支持一个域名可以同时绑定ECC类型的证书和RSA类型的证书，在选择SNI证书时，支持选择同域名绑定的两个证书，在使用时，会优先选择ECC类型的证书。

- SNI证书匹配规则：

  当证书的域名为*.test.com，那么可支持a.test.com、b.test.com等，不支持a.b.test.com、c.d.test.com等。

  且依据最长尾缀匹配：当证书中的域名同时存在*.b.test.com和*.test.com时，那么a.b.test.com会优先匹配到*.b.test.com。

- 证书示例如图2-17所示，图中的cer-default为创建HTTPS监听器时绑定的默认证书，cert-test01和cert-test02为新创建的用于SNI的证书。

  其中，证书cert-test01填写的域名为www.test01.com、cert-test02填写的域名为www.test02.com。

  如果访问负载均衡的域名与SNI证书匹配成功，则会返回SNI的证书认证鉴权。如果匹配失败，则会返回默认证书认证鉴权。

图 2-17 配置证书说明

监听器开启 SNI

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击负载均衡名称。
5. 在“监听器”页签，单击需要开启SNI的监听器名称。
6. 在监听器基本信息页面，单击SNI右侧“配置”。
7. 开启SNI的开关，选择需要配置的SNI证书。

图 2-18 配置 SNI 证书

8. 单击“确定”。

2.6.4 TLS 安全策略

操作场景

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

共享型负载均衡仅支持选择默认安全策略。

添加安全策略

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要创建安全策略的监听器的负载均衡器名称。
5. 在该负载均衡界面的“监听器”区域，单击“添加监听器”。
6. 在“添加监听器”界面，前端协议选择“HTTPS”。
7. 在“添加监听器”界面，选择“高级配置 > 安全策略”。

   共享型负载均衡器支持的默认策略如**表2-35**所示。

表 2-35 默认安全策略参数说明

名称	支持的TLS版本类型	使用的加密套件列表
TLS-1-0	TLS 1.2 TLS 1.1 TLS 1.0	• ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • AES128-GCM-SHA256 • AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • AES128-SHA256 • AES256-SHA256 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-RSA-AES256-SHA • ECDHE-ECDSA-AES256-SHA • AES128-SHA • AES256-SHA
TLS-1-1	TLS 1.2 TLS 1.1	
TLS-1-2	TLS 1.2	

名称	支持的TLS版本类型	使用的加密套件列表
tls-1-0-inherit	TLS 1.2 TLS 1.1 TLS 1.0	• ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • AES128-GCM-SHA256 • AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • AES128-SHA256 • AES256-SHA256 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • DHE-RSA-AES128-SHA • ECDHE-RSA-AES256-SHA • ECDHE-ECDSA-AES256-SHA • AES128-SHA • AES256-SHA • DHE-DSS-AES128-SHA • CAMELLIA128-SHA • EDH-RSA-DES-CBC3-SHA • DES-CBC3-SHA • ECDHE-RSA-RC4-SHA • RC4-SHA • DHE-RSA-AES256-SHA • DHE-DSS-AES256-SHA • DHE-RSA-CAMELLIA256-SHA

名称	支持的TLS版本类型	使用的加密套件列表
TLS-1-2-Strict	TLS 1.2	• ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • AES128-GCM-SHA256 • AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • AES128-SHA256 • AES256-SHA256 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384

说明

- 共享型负载均衡安全策略最高支持TLS 1.2协议。
- 上述列表为ELB支持的加密套件，同时客户端也支持多个加密套件，这样在实际使用时，加密套件的选择范围为：ELB和客户端支持的加密套件的交集，加密套件的选择顺序为：ELB支持的加密套件顺序。

8. 配置完成，单击“确定”。

安全策略差异说明

表 2-36 安全策略差异说明

安全策略	tls-1-0	tls-1-1	tls-1-2	tls-1-0-inherit	tls-1-2-strict	tls-1-0-with-1-3	tls-1-2-fs-with-1-3	tls-1-2-fs	hybrid-policy-1-0
TLS 协议									
Protocol-TLS 1.3	-	-	-	-	-	√	√	√	-
Protocol-TLS 1.2	√	√	√	√	√	√	√	√	√
Protocol-TLS 1.1	√	√	-	√	-	√	-	-	√
Protocol-TLS 1.0	√	-	-	√	-	√	-	-	-

安全策略	tls-1-0	tls-1-1	tls-1-2	tls-1-0-inherit	tls-1-2-strict	tls-1-0-with-1-3	tls-1-2-fs-with-1-3	tls-1-2-fs	hybrid-policy-1-0
加密套件									
EDHE-RSA-AES128-GCM-SHA256	√	√	√	-	√	-	-	-	-
ECDHE-RSA-AES256-GCM-SHA384	√	√	√	√	√	√	√	√	√
ECDHE-RSA-AES128-SHA256	√	√	√	√	√	√	√	√	√
ECDHE-RSA-AES256-SHA384	√	√	√	√	√	√	√	√	√
AES128-GCM-SHA256	√	√	√	√	√	√	-	-	√
AES256-GCM-SHA384	√	√	√	√	√	√	-	-	√
AES128-SHA256	√	√	√	√	√	√	-	-	√
AES256-SHA256	√	√	√	√	√	√	-	-	√
ECDHE-RSA-AES128-SHA	√	√	√	√	-	√	-	-	√
ECDHE-RSA-AES256-SHA	√	√	√	√	-	√	-	-	√
AES128-SHA	√	√	√	√	-	√	-	-	√
AES256-SHA	√	√	√	√	-	√	-	-	√
ECDHE-ECDSA-AES128-GCM-SHA256	√	√	√	√	√	√	√	√	√
ECDHE-ECDSA-AES128-SHA256	√	√	√	√	√	√	√	√	√

安全策略	tls-1-0	tls-1-1	tls-1-2	tls-1-0-inherit	tls-1-2-strict	tls-1-0-with-1-3	tls-1-2-fs-with-1-3	tls-1-2-fs	hybrid-policy-1-0
ECDHE-ECDSA-AES128-SHA	√	√	√	√	-	√	-	-	√
ECDHE-ECDSA-AES256-GCM-SHA384	√	√	√	√	√	√	√	√	√
ECDHE-ECDSA-AES256-SHA384	√	√	√	√	√	√	√	√	√
ECDHE-ECDSA-AES256-SHA	√	√	√	√	-	√	-	-	√
ECDHE-RSA-AES128-GCM-SHA256	-	-	-	√	-	√	√	√	√
TLS_AES_256_GCM_SHA384	-	-	-	-	-	√	√	√	-
TLS_CHACHA20_POLY1305_SHA256	-	-	-	-	-	√	√	√	-
TLS_AES_128_GCM_SHA256	-	-	-	-	-	√	√	√	-
TLS_AES_128_CCM_8_SHA256	-	-	-	-	-	√	√	√	-
TLS_AES_128_CCM_SHA256	-	-	-	-	-	√	√	√	-
DHE-RSA-AES128-SHA	-	-	-	√	-	-	-	-	-
DHE-DSS-AES128-SHA	-	-	-	√	-	-	-	-	-
CAMELLIA128-SHA	-	-	-	√	-	-	-	-	-
EDH-RSA-DES-CBC3-SHA	-	-	-	√	-	-	-	-	-

安全策略	tls-1-0	tls-1-1	tls-1-2	tls-1-0-inherit	tls-1-2-strict	tls-1-0-with-1-3	tls-1-2-fs-with-1-3	tls-1-2-fs	hybrid-policy-1-0
DES-CBC3-SHA	-	-	-	√	-	-	-	-	-
ECDHE-RSA-RC4-SHA	-	-	-	√	-	-	-	-	-
RC4-SHA	-	-	-	√	-	-	-	-	-
DHE-RSA-AES256-SHA	-	-	-	√	-	-	-	-	-
DHE-DSS-AES256-SHA	-	-	-	√	-	-	-	-	-
DHE-RSA-CAMELLIA256-SHA	-	-	-	√	-	-	-	-	-
ECC-SM4-SM3	-	-	-	-	-	-	-	-	√
ECDHE-SM4-SM3	-	-	-	-	-	-	-	-	√

修改安全策略

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

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要修改安全策略的监听器的负载均衡器名称。
5. 切换至“监听器”页签，单击需要修改安全策略的监听器名称。
6. 在监听器的基本信息页面，单击“编辑监听器”。
7. 在“编辑监听器”界面，展开高级配置，选择安全策略参数。
8. 单击“确定”。

2.6.5 访问控制

2.6.5.1 访问控制策略

当您需要对客户端访问弹性负载均衡实施精细的访问控制时，您可以开启ELB监听器的访问控制功能，并设置对应的访问控制策略来控制访问ELB监听器的IP地址。

访问控制策略

您可以为监听的访问控制策略设置白名单或黑名单：

- 白名单：只有白名单中的IP可以访问ELB的监听器。仅转发来自所选访问控制IP地址组中设置的IP地址或网段的请求。

  配置了白名单，但是不在白名单的IP也能访问后端服务器，可能的原因是该连接为长连接，需要客户端或后端服务器断开该长连接。
- 黑名单：黑名单中的IP禁止访问ELB的监听器。不会转发来自所选访问控制策略组中设置的IP地址或网段的请求。

说明

- 访问控制只限制实际业务的流量转发，不限制ping命令操作，被限制的IP仍可以ping通后端服务器。
- 对于共享型负载均衡实例来说，需要创建监听器并添加后端云服务器，才可以ping通。
- 访问流量的IP先通过监听器访问控制策略的限制，然后转发至后端服务器，所以后端服务器安全组的规则设置不会影响负载均衡的访问控制策略。

设置访问控制策略

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击负载均衡名称，进入监听器管理界面。
5. 您可以通过以下两种操作入口，为监听器设置访问控制策略。
   - 在目标监听器所在行的“访问控制”列，单击“设置”。
   - 单击目标监听器名称，进入监听器的基本信息页面，单击访问控制右侧的“设置”。
6. 在“设置访问控制”的弹窗中，如表2-37所示配置访问控制。

表 2-37 访问控制参数说明

参数	说明
访问控制	可以选择允许所有IP访问、白名单和黑名单。 ● 允许所有IP访问：允许所有IP访问负载均衡监听器。 ● 白名单：仅允许IP地址组中的IP访问负载均衡监听器。 ● 黑名单：不允许IP地址组中的IP访问负载均衡监听器。
IP地址组	设置白名单或者黑名单时，必须选择一个IP地址组。如果还未创建IP地址组，需要先创建IP地址组，更多关于IP地址组的信息请参见IP地址组。

参数	说明
访问控制开关	当访问控制选择白名单或者黑名单时，可以开启或者关闭访问控制开关。 • 开启：开启访问控制开关，设置的白名单和黑名单才会生效。 • 关闭：关闭访问控制开关，设置的白名单和黑名单不生效。

7. 配置完成，单击“确定”。

2.6.5.2 访问控制 IP 地址组

IP 地址组简介

IP地址组是多个IP地址的集合，用来统一管理具有相同安全要求或需要频繁修改的IP地址。

弹性负载均衡支持对监听器设置访问控制策略。对于需要使用**黑名单**和**白名单**，在监听器上设置**访问控制策略**的用户，开启白名单或黑名单时必须选择一个IP地址组。

- 白名单：允许IP地址组中的IP访问负载均衡的监听器。如果IP地址组未包含任何IP地址，则对应的负载均衡监听器禁止任何IP地址访问。
- 黑名单：限制IP地址组中的IP访问负载均衡的监听器。如果IP地址组未包含任何IP地址，则对应的负载均衡监听器允许所有IP地址访问。

约束与限制

- 默认情况下，一个用户可以创建50个IP地址组。
- 同一个IP地址组，最多可以关联50个监听器。

创建 IP 地址组

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 弹性负载均衡 > IP地址组”。
5. 在“IP地址组”界面，单击“创建IP地址组”。
6. 配置IP地址组参数，参数说明参见**表2-38**。

表 2-38 IP 地址组参数说明

参数	说明	样例
名称	IP地址组的名称。	ipGroup-01

参数	说明	样例
企业项目	企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。详见《企业管理用户指南》。	-
IP地址	需要通过白名单或黑名单进行访问控制的IP地址，支持IPv4地址和IPv6地址。 • 每行一个IP地址或一个网段，以回车结束； • 每个IP地址或者网段都可以用“|”分隔添加备注，备注长度范围是0到255字符，不能包含<>； • 每个IP地址组最多可添加300个IP地址或网段。	• 不带IP地址描述：10.168.2.24 • 带IP地址描述：10.168.16.0/24 | ECS01
描述	IP地址组相关信息的描述说明。	-

7. 确认参数配置，单击“确定”。

管理 IP 地址组内的 IP 地址

IP地址组创建后，您可根据使用需求对组内的IP地址进行修改，支持的修改操作如下：

- **添加IP地址**
- **批量修改IP地址**
- **删除IP地址**

IP地址组内输入IP地址，支持的格式如下：

- 每行一个IP地址或一个网段，以回车结束。
- 每个IP地址或者网段都可以用“|”分隔添加备注，如“192.168.10.10 | ECS01”，备注长度范围是0到255字符，不能包含<>。
- 每个IP地址组最多可添加300个IP地址或网段。

添加 IP 地址

IP地址组创建后您可向其中添加IP地址，不影响IP地址组中已有的IP地址。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 弹性负载均衡 > IP地址组”。
5. 在“IP地址组”界面，单击需要添加IP地址的地址组名称，进入IP地址组的详情页面。

6. 在IP地址页签下方，单击“添加IP地址”。在“添加IP地址”页面，添加IP地址。
7. 单击“确定”，完成添加。

批量修改 IP 地址

如果您希望对IP地址组内的所有IP地址进行批量修改，请参考以下操作。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 弹性负载均衡 > IP地址组”。
5. 在“IP地址组”界面，您可以通过以下两种操作入口，批量修改IP地址。
   a. 批量修改IP地址及其基本信息：
      i. 在需要修改IP地址的地址组所在行的操作列，单击“修改”。支持修改IP地址组的名称，组内所有IP地址和描述。
      ii. 单击“确定”，完成修改。
   b. 仅批量修改IP地址：
      i. 单击需要修改IP地址的地址组名称，进入IP地址组的详情页面。
      ii. 在IP地址页签下方，单击“修改IP地址”。支持修改IP地址组的内所有IP地址。
      iii. 单击“确定”，完成修改。

删除 IP 地址

如果你希望批量删除IP地址组内的多个IP地址，请参考**批量修改IP地址**。

如果您希望对IP地址组内的单IP地址进行删除，请参考以下操作。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 弹性负载均衡 > IP地址组”。
5. 在“IP地址组”界面，单击需要修改IP地址的地址组名称，进入IP地址组的详情页面。
6. 在IP地址列表中，单击目标IP地址所在行的“删除”，弹出删除确认对话框。
7. 确认无误后，单击“是”，删除IP地址。

查看 IP 地址组详情

您可查看IP地址组的详情，快速了解IP地址组的使用情况，包括如下信息：

- IP地址组的基本信息，包括IP地址组的名称、ID、创建时间和描述。
- IP地址组内添加的IP地址。
- IP地址组关联的监听器资源。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 弹性负载均衡 > IP地址组”。
5. 在“IP地址组”界面，单击需要查看详情的地址组名称，进入IP地址组的详情页面。
6. 支持查看IP地址组基本信息。
   a. 在“IP地址”页签下，查看IP地址组内的IP地址条目。
   b. 在“关联监听器”页签下，查看IP地址组已关联的监听器。

删除 IP 地址组

如果IP地址组已经关联监听器的访问控制策略使用，无法完成删除。

您可在IP地址组列表页或通过**查看IP地址组详情**查看IP地址组已关联的监听器资源，解除IP地址组与监听器的关联请参考**设置访问控制策略**。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 弹性负载均衡 > IP地址组”。
5. 在“IP地址组”界面，需要删除的IP地址组所在行，单击“删除”。
6. 确认需要删除的IP地址组，单击“是”。

2.6.6 证书管理

2.6.6.1 证书概述

负载均衡器支持三种类型的证书，服务器证书、CA证书、服务器SM双证书。配置HTTPS监听器时，需要为监听器绑定服务器证书，如果开启双向认证功能，还需要绑定CA证书。

- 服务器证书：在使用HTTPS协议时，服务器证书用于SSL握手协商，需提供证书内容和私钥。
- CA证书： 又称客户端CA公钥证书，用于验证客户端证书的签发者；在开启HTTPS双向认证功能时，只有当客户端能够出具指定CA签发的证书时，HTTPS连接才能成功。
- 服务器SM双证书：在使用HTTPS协议时，若采用商密SSL协议，需提供双证书。双证书包括**签名证书**和**加密证书**，需成套使用。

  说明

  服务器SM双证书已上线华北-乌兰察布一，其余区域持续上线中。

  - **签名证书：**在签名时使用，仅用于验证身份使用，其公钥和私钥均由服务器自己产生，并由服务器自己保管，证书颁发机构（Certificate Authority，简称“CA”）不负责其保管任务。

- **加密证书：**在密钥协商时使用，其私钥和公钥均由CA产生，并由CA保管（存根）。

说明

证书管理既支持在华为云购买的证书，也支持您自己生成的证书。

使用证书的注意事项

- 同一个证书在负载均衡器上只需上传一次，可以使用在多个负载均衡器实例中。
- 如果创建的服务器证书用于SNI，则需要指定域名，且指定的域名必须与证书中的域名保持一致。一个证书可以指定多个域名。
- 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。如果监听器开启了SNI功能，则支持绑定多个服务器证书。
- 负载均衡器只支持原始证书，不支持对证书进行加密。
- 可以使用自签名的证书，使用自签名证书和第三方机构颁发的证书对负载均衡器无区别，但是使用自签名证书会存在安全隐患，建议客户使用权威机构颁发的证书。
- 负载均衡器只支持PEM格式的证书，其它格式的证书需要转换成PEM格式后，才能上传到负载均衡。
- ELB不会自动更新证书，如果您有证书过期了，需要手动更换或者删除证书。

证书格式要求

在创建证书时，您可以直接输入证书内容或上传证书文件。

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

服务器证书、CA证书的“证书内容”格式均需按以下要求。

服务器SM双证书中的“SM签名证书内容”和“SM加密证书内容”格式均需按以下要求。

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

示例如下：

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

私钥格式要求

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

服务器SM双证书中的“SM签名证书私钥”和“SM加密证书私钥”格式均需按以下要求。

需注意必须是无密码的私钥，私钥内容格式为：

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

示例如下：

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

2.6.6.2 格式转换

操作场景

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

DER 转换为 PEM

DER格式通常使用在Java平台。

运行以下命令进行证书转化：

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

运行以下命令进行私钥转化：

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

P7B 转换为 PEM

P7B格式通常使用在Windows Server和Tomcat中。

运行以下命令进行证书转化：

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

PFX 转换为 PEM

PFX格式通常使用在Windows Server中。

运行以下命令进行证书转化：

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

运行以下命令进行私钥转化：

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

2.6.6.3 创建证书

操作场景

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

- 服务器证书：同时支持云证书管理服务提供的服务器数字证书和您的自有证书。
- CA证书：仅支持上传您的自有CA证书
- 服务器SM双证书：同时支持云证书管理服务提供的服务器数字证书和您的自有证书。

说明

- 如果您不希望将证书上传到负载均衡器上进行管理，您可以将证书存放到后端服务器上，然后配置相同端口的TCP监听器将HTTPS流量透传到后端服务器。具体原理参见**TCP监听器将HTTPS流量透传到后端服务器**。
- 如果在两个区域想要使用同一个证书，需要在两个区域分别使用的证书信息创建两个证书。

创建服务器证书

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏单击“证书管理”。
5. 单击“创建证书”，配置参数请参见**表2-39**。

表 2-39 服务器证书参数说明

参数	说明
证书类型	创建证书的类型，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。 • 服务器SM双证书：在使用HTTPS协议时，若采用商密SSL协议，需提供双证书。双证书包括签名证书和加密证书，需成套使用。
证书来源	服务器证书同时支持SSL证书管理服务提供的数字证书和您的自有证书。 • SCM证书：SSL证书管理服务管理的服务器数字证书，您需要到云证书管理服务控制台签发证书或上传自有证书。 • 自有证书：您需要在负载均衡控制台上传自有证书的证书内容和私钥。 **说明** 推荐使用云证书管理服务对您的证书进行统一管理。
证书	仅SCM证书支持该参数。 支持选择您在云证书管理服务统一管理的证书。

参数	说明
证书名称	仅自有证书支持该参数。 您的自有证书名称。
企业项目	企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。
证书内容	仅自有证书支持该参数。 证书内容必须为PEM格式。 单击“上传”，选择上传证书文件，请确保您的浏览器是最新版本。 证书内容格式如下： -----BEGIN CERTIFICATE----- Base64-encoded certificate -----END CERTIFICATE-----
私钥	仅自有证书支持该参数。 单击“上传”，选择上传私钥文件，请确保您的浏览器是最新版本。 需注意必须是无密码的私钥。符合PEM格式，私钥格式如下： -----BEGIN PRIVATE KEY----- [key] -----END PRIVATE KEY-----
域名	如果创建的证书用于SNI，则需要指定域名。 域名只能由字母、数字、中划线组成，中划线不能在开头或末尾，单个字符串不超过63个字符，字符串间以点分隔。 最多可支持100个域名，域名间以逗号分隔；单个域名长度不超过100个字符，且总长度不超过10000个字符。
描述	添加对该证书的描述信息，非必填项。

创建 CA 证书

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏单击“证书管理”。
5. 单击“创建证书”，配置参数请参见**表2-40**。

表 2-40 CA 证书参数说明

参数	说明
证书类型	创建证书的类型，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；在开启HTTPS双向认证功能时，只有当客户端能够出具指定CA签发的证书时，HTTPS连接才能成功。
证书名称	您的CA证书名称。
企业项目	企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。
证书内容	证书内容必须为PEM格式。 单击“上传”，选择上传证书文件，请确保您的浏览器是最新版本。 证书内容格式如下： -----BEGIN CERTIFICATE----- Base64-encoded certificate -----END CERTIFICATE-----
描述	添加对该证书的描述信息，非必填项。

6. 单击“确定”，完全创建。

创建服务器 SM 双证书

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏单击“证书管理”。
5. 单击“创建证书”，配置参数请参见**表2-41**。

表 2-41 服务器 SM 双证书参数说明

参数	说明
证书类型	创建证书的类型，选择服务器SM双证书。 ● 服务器证书：在使用HTTPS协议时，服务器证书用于SSL握手协商，需提供证书内容和私钥。 ● CA证书：又称客户端CA公钥证书，用于验证客户端证书的签发者；在开启HTTPS双向认证功能时，只有当客户端能够出具指定CA签发的证书时，HTTPS连接才能成功。 ● 服务器SM双证书：在使用HTTPS协议时，若采用商密SSL协议，需提供双证书。双证书包括签名证书和加密证书，需成套使用。
证书来源	服务器证书同时支持SSL证书管理服务提供的数字证书和您的自有证书。 ● SCM证书：SSL证书管理服务管理的服务器数字证书，您需要到云证书管理服务控制台签发证书或上传自有证书。 ● 自有证书：您需要在负载均衡控制台上传自有证书的证书内容和私钥。 **说明** 推荐使用云证书管理服务对您的证书进行统一管理。
证书	仅SCM证书支持该参数。 支持选择您在云证书管理服务统一管理的证书。
证书名称	仅自有证书支持该参数。 您的自有证书名称。
企业项目	企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。
SM签名证书内容	仅自有证书支持该参数。 SM签名证书内容必须为PEM格式。 单击“上传”，选择上传证书文件，请确保您的浏览器是最新版本。 证书内容格式如下： -----BEGIN CERTIFICATE----- Base64-encoded certificate -----END CERTIFICATE-----
SM签名证书私钥	仅自有证书支持该参数。 单击“上传”，选择上传私钥文件，请确保您的浏览器是最新版本。 需注意必须是无密码的私钥。符合PEM格式，私钥格式如下： -----BEGIN PRIVATE KEY----- [key] -----END PRIVATE KEY-----

参数	说明
SM加密证书内容	仅自有证书支持该参数。 SM加密证书内容必须为PEM格式。 单击“上传”，选择上传证书文件，请确保您的浏览器是最新版本。 证书内容格式如下： -----BEGIN CERTIFICATE----- Base64-encoded certificate -----END CERTIFICATE-----
SM加密证书私钥	仅自有证书支持该参数。 单击“上传”，选择上传私钥文件，请确保您的浏览器是最新版本。 需注意必须是无密码的私钥。符合PEM格式，私钥格式如下： -----BEGIN PRIVATE KEY----- [key] -----END PRIVATE KEY-----
域名	如果创建的证书用于SNI，则需要指定域名。 域名只能由字母、数字、中划线组成，中划线不能在开头或末尾，单个字符串不超过63个字符，字符串间以点分隔。 最多可支持100个域名，域名间以逗号分隔；单个域名长度不超过100个字符，且总长度不超过10000个字符。
描述	添加对该证书的描述信息，非必填项。

2.6.6.4 管理证书

操作场景

当您确认证书不需要继续使用时，您可以根据需求删除您在弹性负载均衡控制台创建的证书。

约束与限制

已被HTTPS监听器绑定使用的证书，无法执行删除操作，请先为关联监听器执行**更换证书**操作。

快速查询证书关联的监听器

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏单击“证书管理”。

5. 在证书列表中，在“监听器 (前端协议/端口)”所在列，单击监听器名称，即可查看监听器详细信息。

   当关联监听器数量大于5个，在“监听器 (前端协议/端口)”所在列，单击“查看所有”，单击监听器名称，即可查看监听器详细信息。

修改证书

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏单击“证书管理”。
5. 在证书列表中，在需要修改的证书所在行，单击“修改”。
6. 在“修改证书”对话框中，修改证书的相关信息。
7. 确认修改信息，单击“确定”，完成修改。

删除证书

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏单击“证书管理”。
5. 在证书列表中，在需要修改的证书所在行，单击“删除”。
6. 在确认对话框中单击“确定”，完成删除。

2.6.6.5 绑定/更换证书

操作场景

为了支持HTTPS数据传输加密认证，在创建HTTPS协议监听的时候需绑定证书，您可以参考本章节绑定证书。如果弹性负载均衡实例使用的证书过期或者其它原因需要更换，您可以参考本章节更换证书。

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

说明

弹性负载均衡的证书和私钥的更换对业务没有影响。

约束与限制

- 仅HTTPS协议的监听器才支持绑定/更换证书。
- 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。
- 切换证书后立即生效，已经建立的连接会继续使用老证书，新建立的连接将会使用新的证书。

前提条件

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

绑定证书

通过添加HTTPS监听器来绑定证书。详见**添加HTTPS监听器**。

更换证书

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要修改HTTPS监听器的负载均衡名称。
5. 在“监听器”页签下，单击目标监听器所在行操作列的“编辑”。
6. 在“服务器证书”或“CA证书”下选择需要更换的证书。
7. 在“编辑监听器”对话框中，单击“确定”。

2.6.6.6 批量更换证书

操作场景

如果使用的证书过期或者其它原因需要更换，您可以通过修改证书功能批量更换监听器所绑定的证书。

说明

弹性负载均衡的证书和私钥的更换对业务没有影响。

约束与限制

- 只有HTTPS协议的监听器才支持绑定/更换证书，TCP/UDP/HTTP协议的监听器不支持绑定/更换证书。
- 切换证书后立即生效。已经建立的连接会继续使用老证书，新建立的连接将会使用新的证书。
- 证书管理既支持在华为云购买的证书，也支持您自己生成的证书。

修改证书

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏单击“证书管理”。
5. 在证书列表中，在需要修改的证书所在行，单击“修改”。
6. 在“修改证书”对话框中，修改证书的相关信息。

7. 确认修改信息，单击“确定”，完成修改。

2.6.7 敏感操作保护

操作场景

弹性负载均衡支持敏感操作保护，在控制台进行敏感操作时，需要输入一种能证明身份的凭证，身份验证通过后方可进行相关操作。为了账号安全，建议开启操作保护功能。

该功能只有管理员可配置，对账号以及账号下的用户的资源都生效。普通用户只有查看权限，不能对其进行设置，如需修改，请联系管理员为您操作或添加权限。

开启操作保护

操作保护默认关闭，您可以参考以下步骤开启操作保护。

1. 登录管理控制台。
2. 在“控制台”页面，鼠标移动至右上方的用户名，在下拉列表中选择“安全设置”。

图 2-19 安全设置

3. 在“安全设置”页面中，选择“敏感操作 > 操作保护 > 立即启用”。

图 2-20 敏感操作

4. 在“操作保护设置”页面中，选择“开启”，单击“确定”后，开启操作保护。

   开启后，您以及账号中的IAM用户进行敏感操作时，例如删除弹性云服务器资源，需要输入验证码进行验证，避免误操作带来的风险和损失。

说明

- 用户如果进行敏感操作，将进入“操作保护”页面，选择认证方式，包括邮箱、手机和虚拟MFA三种认证方式。
  - 如果用户只绑定了手机，则认证方式只能选择手机。
  - 如果用户只绑定了邮箱，则认证方式只能选择邮件。
  - 如果用户未绑定邮箱、手机和虚拟MFA，进行敏感操作时，华为云将提示用户绑定邮箱、手机或虚拟MFA。
- 如需修改验证手机、邮箱、虚拟MFA设备，请在**账号**中修改。

验证操作保护

当您已经开启操作保护，在进行敏感操作时，系统会先进行操作保护验证：

- 若您绑定了邮箱，需输入邮箱验证码。
- 若您绑定了手机，需输入手机验证码。
- 若您绑定了虚拟MFA，需输入MFA设备上的6位动态验证码。

如图 操作保护身份验证所示，尝试删除负载均衡器时，弹出以下验证框，选择一种验证方式：

图 2-21 操作保护身份验证

关闭操作保护

如需关闭操作保护，请参考以下步骤操作。

1. 登录管理控制台。
2. 在“控制台”页面，鼠标移动至右上方的用户名，在下拉列表中选择“安全设置”。

图 2-22 安全设置

3. 在“安全设置”页面中，选择“敏感操作 > 操作保护 > 立即修改”。

图 2-23 修改敏感操作

4. 在“操作保护设置”页面中，选择“关闭”，单击“确定”后，关闭操作保护。

相关链接

- 如何绑定虚拟MFA设备?
- 如何获取MFA验证码?

2.7 访问日志

操作场景

在您使用七层（应用型）ELB期间，ELB的访问日志功能支持查看和分析对七层负载均衡进行请求的详细访问日志记录，包括请求时间、客户端IP地址、请求路径和服务器响应等。

如果您遇到后端服务器导致的业务故障或异常，您可以查看访问弹性负载均衡的详细日志记录，分析负载均衡的响应状态码，快速定位异常的后端服务器。

说明

由于弹性负载均衡会将访问日志等运维数据内容展示到云日志服务控制台，请您在使用过程中，注意您的隐私及敏感信息数据保护，不建议将隐私或敏感数据通过访问日志涉及的的字段传输，必要时请加密保护。

约束与限制

- 仅七层（应用型）负载均衡器支持配置访问日志。
- 客户订阅的访问日志中不包含返回码为400的请求，因为该类请求不符合HTTP规范，无法被正常处理。

前提条件

- 您已经创建了七层（应用型）负载均衡器。具体操作，请参见**创建共享型负载均衡器**。
- 您已经开通了云日志服务。具体操作，请参见**开始使用云日志服务**。
- 您已经创建了后端服务器组并且已添加后端服务器，在后端服务器中已部署了业务。具体操作，请参见**创建后端服务器组**。
- 您已经在ELB中创建了HTTP或HTTPS监听器。具体操作，请参见**添加HTTP监听器**或**添加HTTPS监听器**。

操作流程

图 2-24 定位异常后端服务器操作流程

创建日志组

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
   区域和项目选择“华北-北京四”。
3. 单击页面左上角的 ，选择“管理与监管 > 云日志服务”。
4. 单击左侧导航栏“日志管理”。
5. 单击 “创建日志组”，在弹出框内，输入日志组名称。

图 2-25 创建日志组

6. 单击“确定”，创建完成。

创建日志流

1. 在云日志服务管理控制台，单击日志组名称对应的 按钮。
2. 单击“创建日志流”，在弹出框内，输入日志流名称。

图 2-26 创建日志流

3. 单击“确定”，创建完成。

配置访问日志

1. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
2. 在“负载均衡器”界面，单击需要配置访问日志的负载均衡器名称。
3. 在该负载均衡器界面的“访问日志”页签，单击“配置访问日志”。
4. 开启日志记录，选择您在云日志服务中创建的日志组和日志流。

图 2-27 配置 ELB 访问日志

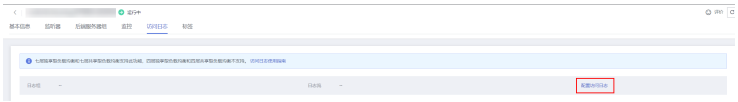


图 2-28 配置 ELB 访问日志

5. 单击“确定”，配置完成。

须知

确保创建的云日志组的地域和负载均衡器的地域相同。

查看访问日志

您可以通过以下两种方式查看访问日志的详细信息：

- “弹性负载均衡”控制台，进入访问日志界面，即可查看访问日志。
- （推荐）“云日志服务”控制台，在日志组列表，单击查看目标日志组。进入日志组详情页，在相应日志流名称所在行，单击看目标日志流的日志详情。

日志显示格式如下所示，不支持修改日志格式。

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

日志示例如下：

```
1644819836.370 eb11c5a9-93a7-4c48-80fc-03f61f638595 [2022-02-14T14:23:56+08:00] elb_01
192.168.1.1:888 200 "POST https://www.test.com/example/ HTTP/1.1" 1411 251 3 0.011 "200" "0.000"
```

```
"0.011" "0.011" "100.64.0.129:8080" "okhttp/3.13.1" "-" "-"
loadbalancer_295a7eee-9999-46ed-9fad-32a62ff0a687 listener_20679192-8888-4e62-a814-a2f870f62148
3333fd44fe3b42cbaa1dc2c641994d90 pool_89547549-6666-446e-9dbc-e3a551034c46 "-"
f2bc165ad9b4483a9b17762da851bbbb 121.64.212.1:443 "10.1.1.2:8080" - TLSv1.2 ECDHE-RSA-AES256-
GCM-SHA384 www.test.com 56704 -
```

日志字段说明如表2-42。

表 2-42 字段说明

参数	描述	取值说明	示例取值
msec	以秒为单位的时间，日志写入时的分辨率为毫秒。	浮点型数据	1644819836.370
access_log_topic_id	访问日志流ID。	uuid	eb11c5a9-93a7-4c48-80fc-03f61f638595
time_iso8601	日志写入时的时间，采用ISO 8601标准格式本地时间。	-	[2022-02-14T14:23:56+08:00]
log_ver	ELB服务日志版本号。	固定值：elb_01	elb_01
remote_addr: remote_port	客户端IP地址：客户端端口。	记录客户端IP地址和客户端端口号。	192.168.1.1:888
status	ELB响应的状态码。	记录请求状态码。	200
request_method scheme://host request_uri server_protocol	请求方法。请求方式：//主机名：请求URI 请求协议。	• request_method：请求方法。 • scheme: http或https。 • host: 主机名，可能为域名或者IP。 • request_uri：浏览器发起的不做任何修改的原生URI。不包括协议及主机名。	"POST https://www.test.com/example/ HTTP/1.1"
request_length	从客户端收到的请求长度（包括请求header和请求body）。	整型数据	1411
bytes_sent	发送到客户端的字节数 。	整型数据	251
body_bytes_sent	发送到客户端的字节数（不包括响应头）。	整型数据	3

参数	描述	取值说明	示例取值
request_time	请求处理时间，即ELB收到第一个客户端请求报文到ELB发送完响应报文的时间间隔（单位：秒）。	浮点型数据	0.011
upstream_status	从上游服务器获得的响应状态码，当ELB代理进行请求重试时会包含多个响应的状态码，当请求未被正确转发到后端服务器时此字段为 -。	后端返回给ELB的状态码	"200"
upstream_connect_time	与上游服务器建立连接所花费的时间，时间以秒为单位，分辨率为毫秒。当ELB代理进行请求重试时会包含多个连接的时间，当请求未被正确转发到后端服务器时此字段为 -。	浮点型数据	"0.000"
upstream_header_time	从上游服务器接收响应头所花费的时间，时间以秒为单位，分辨率为毫秒。当ELB代理进行请求重试时会包含多个响应时间，当请求未被正确转发到后端服务器时此字段为 -。	浮点型数据	"0.011"
upstream_response_time	从上游服务器接收响应所花费的时间，时间以秒为单位，分辨率为毫秒。当ELB代理进行请求重试时会包含多个响应时间，当请求未被正确转发到后端服务器时此字段为 -。	浮点型数据	"0.011"
upstream_addr	后端主机的IP地址和端口号。可能有多个值，每个值都是ip:port或者-，用逗号空格隔开。	IP地址+端口号	"100.64.0.129:8080" （共享型负载均衡场景该IP地址为ELB内部通信使用）

参数	描述	取值说明	示例取值
http_user_agent	ELB收到请求头中的http_user_agent内容，表示客户端的系统型号、浏览器信息等。	记录浏览器的相关信息	"okhttp/3.13.1"
http_referer	ELB收到请求头中的http_referer内容，表示该请求所在的页面链接。	页面链接请求	"-"
http_x_forwarded_for	ELB收到请求头中的http_x_forwarded_for内容，表示请求经过的代理服务器IP地址。	IP地址	"-"
lb_name	负载均衡器的名称（格式为“loadbalancer_”+“负载均衡器ID”）。	字符串	loadbalancer_295a7eee-9999-46ed-9fad-32a62ff0a687
listener_name	监听器的名称（格式为“listener_”+“监听器ID”）。	字符串	listener_2067919 2-8888-4e62-a814-a2f870f62148
listener_id	监听器在ELB服务内部的ID（客户可忽略）。	字符串	3333fd44fe3b42cbaa1dc2c641994d90
pool_name	后端服务器组名称（格式为“pool_”+“后端服务器组ID”）。	字符串	pool_89547549-6666-446e-9dbc-e3a551034c46
member_name	后端服务器的名称（格式为“member_”+“服务器ID”，尚未支持）。可能有多个值，每个值都是member_id或者-，用逗号空格隔开。	字符串	"-" (实际日志可能有多个值，每个值都是member_id或者-，用逗号空格隔开)
tenant_id	租户ID。	字符串	f2bc165ad9b4483a9b17762da851bbbb
eip_address:eip_port	弹性IP地址和监听器监听的端口号。	弹性IP地址和监听器监听的端口号。	121.64.212.1:443

参数	描述	取值说明	示例取值
upstream_addr_priv	后端主机的IP地址和端口号。可能有多个值，每个值都是ip:port或者-，用逗号空格隔开。	IP地址+端口号	"10.1.1.2:8080" (实际日志可能有多个值，每个值都是member_id或者-，用逗号空格隔开)
certificate_id	[HTTPS监听器]SSL连接建立时使用的证书ID（尚未支持）。	字符串	-
ssl_protocol	[HTTPS监听器]SSL连接建立使用的协议，非HTTPS监听器，此字段为 -。	字符串	TLSv1.2
ssl_cipher	[HTTPS监听器]SSL连接建立使用的加密套件，非HTTPS监听器，此字段为 -。	字符串	ECDHE-RSA-AES256-GCM-SHA384
sni_domain_name	[HTTPS监听器]SSL握手时客户端提供的SNI域名，非HTTPS监听器，此字段为 -。	字符串	www.test.com
tcpinfo_rtt	ELB与客户端之间的tcp rtt时间，单位：微秒。	整型数据	56704
self_defined_header	该字段为保留字段，默认为“-”。	字符串	-

日志分析示例：

在[2022-02-14T14:23:56+08:00]时，ELB接收到客户端地址和端口（192.168.1.1:888）发起的“POST /HTTP/1.1”请求，ELB将请求转发给后端服务器（100.64.0.129:8080），后端服务器响应状态码200，ELB最终向客户端响应状态码200。

分析结果：

后端服务器正常响应请求。

配置日志转储

如果您希望将日志转储进行二次分析，您可以参考本章设置日志转储。

1. 登录管理控制台。

2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“管理与监管 > 云日志服务”。
4. 在左侧导航栏，单击“日志转储”。
5. 在日志转储页面，单击“配置转储”。

图 2-29 配置日志转储

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

2.8 资源和标签

2.8.1 标签管理

操作场景

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

如果您的组织已经设定弹性负载均衡的相关标签策略，则需按照标签策略规则为弹性负载均衡添加标签。标签如果不符合标签策略的规则，则可能会导致弹性负载均衡创建失败，请联系组织管理员了解标签策略详情。

为负载均衡器添加标签

给负载均衡器添加标签有以下两种方法。

- 在创建负载均衡器的时候，输入标签的“键”和“值”。
  操作步骤和配置参数，请参见**创建共享型负载均衡器**。
- 给已创建的负载均衡器添加标签。
  a. 登录管理控制台。
  b. 在管理控制台左上角单击 图标，选择区域和项目。
  c. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
  d. 在“负载均衡器”界面，单击已创建的负载均衡器名称。
  e. 在“标签”页签下，单击“添加标签”，输入“键”和“值”。
  f. 确认正确，单击“确认”。

  说明

  - 一个负载均衡器最多可以增加20个标签。
  - 标签的“键”和“值”是一一对应的，其中“键”值是唯一的。

为监听器添加标签

给已创建的监听器添加标签的方法如下：

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击已创建的负载均衡器名称。
5. 切换到监听器页签，单击需要添加标签的监听器名称。
6. 切换到监听器子页面的标签页签，单击“添加标签”，输入“键”和“值”。
7. 确认正确，单击“确认”。

   说明

   - 一个监听器最多可以增加20个标签。
   - 标签的“键”和“值”是一一对应的，其中“键”值是唯一的。

修改标签

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。

3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要修改标签的负载均衡器名称。
5. 在“标签”页签下，在需要修改的标签所在行，单击“编辑”，输入修改的“值”。

   说明

   “键”值不支持修改。
6. 确认正确，单击“确认”。

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

删除标签

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要删除标签的负载均衡器名称。
5. 在“标签”页签下，在需要删除的标签所在行，单击 "删除"。
6. 确认正确，单击“确认”。

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

2.8.2 关于配额

什么是配额?

为防止资源滥用，平台限定了各服务资源的配额，对用户的资源数量和容量做了限制。如您最多可以创建多少台弹性云服务器、多少块云硬盘。

如果当前资源配额限制无法满足使用需要，您可以申请扩大配额。

怎样查看我的配额?

1. 登录管理控制台。
2. 单击管理控制台左上角的 ，选择区域和项目。
3. 在页面右上角，选择“资源 > 我的配额”。

   系统进入“服务配额”页面。

图 2-30 我的配额

4. 您可以在“服务配额”页面，查看各项资源的总配额及使用情况。
   如果当前配额不能满足业务要求，请参考后续操作，申请扩大配额。

如何申请扩大配额?

1. 登录管理控制台。
2. 在页面右上角，选择“资源 > 我的配额”。
   系统进入“服务配额”页面。

图 2-31 我的配额

3. 在页面右上角，单击“申请扩大配额”。

图 2-32 申请扩大配额

4. 在“新建工单”页面，根据您的需求，填写相关参数。
   其中，“问题描述”项请填写需要调整的内容和申请原因。

5. 填写完毕后，勾选协议并单击“提交”。

2.9 使用 CES 监控 ELB

2.9.1 监控弹性负载均衡

使用场景

用户在使用ELB的过程中有了解业务负载详情的需求，为使用户更好地掌握ELB的流量负载情况，华为云提供了立体化监控平台云监控服务（CES）。通过云监控服务用户可以执行自动实时监控、告警和通知操作，帮助用户实时掌握通过ELB负载的运行情况。

云监控服务不需要开通，会在用户创建云服务资源后自动启动。关于云监控服务的更多介绍，请参见**云监控服务产品介绍**。

设置告警规则

在自动实时监控的基础上，您可以在云监控服务中设置告警规则，规定在某些特殊情况出现时向您发送告警通知。

设置ELB监控信息告警规则的方法，请参见**创建告警规则和通知**。

查看监控指标

云监控服务对**监控指标说明**进行实时监控，您可以在弹性负载均衡控制台或云监控服务控制台查看各项指标的详细监控数据。

在 ELB 服务控制台查看监控指标

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要查看监控指标的负载均衡器名称。
5. 支持查看“负载均衡器”和“监听器”粒度的监控指标。
   a. 负载均衡器粒度：切换到“监控”页签，监控粒度选择“负载均衡器”进行查看。
   b. 您可以通过以下两种操作入口查看监听器粒度的监控指标：
      i. 切换到“监控”页签，监控粒度选择“监听器”并选定目标监听器后进行查看。
      ii. 单击目标监听器名称，切换到“监控”页签，查看监听器的监控指标。

在 CES 服务控制台查看监控指标

在CES控制台查看ELB监控指标详情的方法，请参见**查看云服务监控指标**。

1. 登录管理控制台。

2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“管理与监管 > 云监控服务”。
4. 在左侧导航树选择“云服务监控 > 弹性负载均衡”。
5. 在“云服务监控”页面，单击需要查看监控指标的负载均衡器名称。或单击目标负载均衡器右侧操作列的“查看监控指标”。
6. 选择需要查看监控指标的时间段。支持选择系统定义的时间段（如“近1小时”），或自定义时间段。
7. 单击右上角的“设置监控指标”，设置需要查看的监控指标。

2.9.2 监控指标说明

功能说明

本节定义了弹性负载均衡服务上报云监控的监控指标的命名空间，监控指标列表和维度定义。您可以在云监控服务控制台**查看弹性负载均衡服务上报的监控指标**以及产生告警信息。

命名空间

SYS.ELB

监控指标

共享型负载均衡支持负载均衡器、监听器和后端服务器组等多维度的监控。当前后端服务器组维度的监控仅支持7层协议。

表 2-43 共享型 ELB 实例的监控指标

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
m1_cps	并发连接数	在四层负载均衡器中，指从测量对象到后端服务器建立的所有TCP和UDP连接的数量。 在七层负载均衡器中，指从客户端到ELB建立的所有TCP连接的数量。 单位：个	≥ 0个	共享型负载均衡器	1分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
m2_act_conn	活跃连接数	从测量对象到后端服务器建立的所有**ESTABLISHED**状态的TCP或UDP连接的数量。 Windows和Linux服务器都可以使用如下命令查看。 `netstat -an` 单位：个	≥ 0个	共享型负载均衡器	1分钟
m3_inact_conn	非活跃连接数	从测量对象到所有后端服务器建立的所有除**ESTABLISHED**状态之外的TCP连接的数量。 Windows和Linux服务器都可以使用如下命令查看。 `netstat -an` 单位：个	≥ 0个	共享型负载均衡器	1分钟
m4_ncps	新建连接数	从客户端到测量对象每秒新建立的连接数。 单位：个/秒	≥ 0个/秒	共享型负载均衡器	1分钟
m5_in_pps	流入数据包数	测量对象每秒接收到的数据包的个数。 单位：个/秒	≥ 0个/秒	共享型负载均衡器	1分钟
m6_out_pps	流出数据包数	测量对象每秒发出的数据包的个数。 单位：个/秒	≥ 0个/秒	共享型负载均衡器	1分钟
m7_in_Bps	网络流入速率	从外部访问测量对象所消耗的流量。 单位：字节/秒	≥ 0bytes/s	共享型负载均衡器	1分钟
m8_out_Bps	网络流出速率	测量对象访问外部所消耗的流量。 单位：字节/秒	≥ 0bytes/s	共享型负载均衡器	1分钟
m9_abnormal_servers	异常主机数	健康检查统计监控对象后端异常的主机个数。 单位：个	≥ 0个	共享型负载均衡器	1分钟
ma_normal_servers	正常主机数	健康检查统计监控对象后端正常的主机个数。 单位：个	≥ 0个	共享型负载均衡器	1分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
m22_in_bandwidth	入网带宽	统计测量对象当前入网带宽。 单位：比特/秒	≥ 0bit/s	共享型负载均衡器	1分钟
m23_out_bandwidth	出网带宽	统计测量对象当前出网带宽。 单位：比特/秒	≥ 0bit/s	共享型负载均衡器	1分钟
m1e_server_rps	后端服务器重置数量	统计后端服务器发送至客户端的重置（RST）数据包的计数。这些重置数据包由后端服务器生成，然后由负载均衡器转发。 （仅TCP监听器支持此指标） 单位：个/秒	≥ 0个/秒	共享型负载均衡器	1分钟
m21_client_rps	客户端重置数量	统计客户端发送至后端服务器的重置（RST）数据包的计数。这些重置数据包由客户端生成，然后由负载均衡器转发。 （仅TCP监听器支持此指标） 单位：个/秒	≥ 0个/秒	共享型负载均衡器	1分钟
m1f_lvs_rps	负载均衡器重置数量	统计负载均衡器生成的重置（RST）数据包的计数。 （仅TCP监听器支持此指标） 单位：个/秒	≥ 0个/秒	共享型负载均衡器	1分钟
mb_l7_qps	7层查询速率	统计测量对象当前7层查询速率。 （仅HTTP和HTTPS监听器支持此指标） 单位：个/秒	≥ 0个/秒	共享型负载均衡器	1分钟
mc_l7_http_2xx	7层协议返回码(2XX)	统计测量对象当前7层2XX系列状态响应码的数量。 （仅HTTP和HTTPS监听器支持此指标） 单位：个/秒	≥ 0个/秒	共享型负载均衡器	1分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
md_l7_http_3xx	7层协议返回码(3XX)	统计测量对象当前7层3XX系列状态响应码的数量。 （仅HTTP和HTTPS监听器支持此指标） 单位：个/秒	≥ 0个/秒	共享型负载均衡器	1分钟
me_l7_http_4xx	7层协议返回码(4XX)	统计测量对象当前7层4XX系列状态响应码的数量。 （仅HTTP和HTTPS监听器支持此指标） 单位：个/秒	≥ 0个/秒	共享型负载均衡器	1分钟
mf_l7_http_5xx	7层协议返回码(5XX)	统计测量对象当前7层5XX系列状态响应码的数量。 （仅HTTP和HTTPS监听器支持此指标） 单位：个/秒	≥ 0个/秒	共享型负载均衡器	1分钟
m10_l7_http_other_status	7层协议返回码(Others)	统计测量对象当前7层非2XX,3XX,4XX,5XX系列状态响应码的数量。 （仅HTTP和HTTPS监听器支持此指标） 单位：个/秒	≥ 0个/秒	共享型负载均衡器	1分钟
m11_l7_http_404	7层协议返回码(404)	统计测量对象当前7层404状态响应码的数量。 （仅HTTP和HTTPS监听器支持此指标） 单位：个/秒	≥ 0个/秒	共享型负载均衡器	1分钟
m12_l7_http_499	7层协议返回码(499)	统计测量对象当前7层499状态响应码的数量。 （仅HTTP和HTTPS监听器支持此指标） 单位：个/秒	≥ 0个/秒	共享型负载均衡器	1分钟
m13_l7_http_502	7层协议返回码(502)	统计测量对象当前7层502状态响应码的数量。 （仅HTTP和HTTPS监听器支持此指标） 单位：个/秒	≥ 0个/秒	共享型负载均衡器	1分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
m14_l7_rt	7层协议RT平均值	统计测量对象当前7层平均响应时间。 （仅HTTP和HTTPS监听器支持此指标） 从测量对象收到客户端请求开始，到测量对象将所有响应返回给客户端为止。 单位：毫秒 **说明** websocket场景下RT平均值可能会非常大，此时该指标无法作为时延指标参考。	≥ 0ms	共享型负载均衡器	1分钟
m15_l7_upstream_4xx	7层后端返回码(4XX)	统计测量对象当前7层后端4XX系列状态响应码的数量。 （仅HTTP和HTTPS监听器支持此指标） 单位：个/秒	≥ 0个/秒	共享型负载均衡器	1分钟
m16_l7_upstream_5xx	7层后端返回码(5XX)	统计测量对象当前7层后端5XX系列状态响应码的数量。 （仅HTTP和HTTPS监听器支持此指标） 单位：个/秒	≥ 0个/秒	共享型负载均衡器	1分钟
m17_l7_upstream_rt	7层后端的RT平均值	统计测量对象当前7层后端平均响应时间。 从测量对象将请求转发给后端服务器开始，到测量对象收到后端服务器返回响应为止。 （仅HTTP和HTTPS监听器支持此指标） 单位：毫秒 **说明** websocket场景下RT平均值可能会非常大，此时该指标无法作为时延指标参考。	≥ 0ms	共享型负载均衡器	1分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
m1a_l7_upstream_rt_max	7层后端的RT最大值	统计测量对象当前7层后端最大响应时间。 从测量对象将请求转发给后端服务器开始，到测量对象收到后端服务器返回响应为止。 （仅HTTP和HTTPS监听器支持此指标） 单位：毫秒	≥ 0ms	共享型负载均衡器	1分钟
m1b_l7_upstream_rt_min	7层后端的RT最小值	统计测量对象当前7层后端最小响应时间。 从测量对象将请求转发给后端服务器开始，到测量对象收到后端服务器返回响应为止。 （仅HTTP和HTTPS监听器支持此指标） 单位：毫秒	≥ 0ms	共享型负载均衡器	1分钟
m1c_l7_rt_max	7层协议的RT最大值	统计测量对象当前7层最大响应时间。 从测量对象收到客户端请求开始，到测量对象将所有响应返回给客户端为止。 （仅HTTP和HTTPS监听器支持此指标） 单位：毫秒	≥ 0ms	共享型负载均衡器	1分钟
m1d_l7_rt_min	7层协议的RT最小值	统计测量对象当前7层最小响应时间。 从测量对象收到客户端请求开始，到测量对象将所有响应返回给客户端为止。 （仅HTTP和HTTPS监听器支持此指标） 单位：毫秒	≥ 0ms	共享型负载均衡器	1分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
m25_l7_resp_Bps	7层响应带宽	统计周期时间内主机组的响应发送带宽。 单位：比特/秒 **说明** 当监听器开启HTTP/2时，该指标无法作为参考。	≥ 0bit/s	共享型负载均衡器	1分钟
m24_l7_req_Bps	7层请求带宽	统计周期时间内主机组的请求接收带宽。 单位：比特/秒 **说明** 当监听器开启HTTP/2时，该指标无法作为参考。	≥ 0bit/s	共享型负载均衡器	1分钟

表 2-44 监听器支持的监控指标（共享型）

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
m1_cps	并发连接数	在四层负载均衡器中，指从测量对象到后端服务器建立的所有TCP和UDP连接的数量。 在七层负载均衡器中，指从客户端到ELB建立的所有TCP连接的数量。 单位：个	≥ 0个	监听器（共享型）	1分钟
m2_act_conn	活跃连接数	从测量对象到后端服务器建立的所有**ESTABLISHED**状态的TCP或UDP连接的数量。 Windows和Linux服务器都可以使用如下命令查看。 `netstat -an` 单位：个	≥ 0个	监听器（共享型）	1分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
m3_inact_conn	非活跃连接数	从测量对象到所有后端服务器建立的所有除**ESTABLISHED**状态之外的TCP连接的数量。 Windows和Linux服务器都可以使用如下命令查看。 `netstat -an` 单位：个	≥ 0个	监听器（共享型）	1分钟
m4_ncps	新建连接数	从客户端到测量对象每秒新建立的连接数。 单位：个/秒	≥ 0个/秒	监听器（共享型）	1分钟
m5_in_pps	流入数据包数	测量对象每秒接收到的数据包的个数。 单位：个/秒	≥ 0个/秒	监听器（共享型）	1分钟
m6_out_pps	流出数据包数	测量对象每秒发出的数据包的个数。 单位：个/秒	≥ 0个/秒	监听器（共享型）	1分钟
m7_in_Bps	网络流入速率	从外部访问测量对象所消耗的流量。 单位：字节/秒	≥ 0bytes/s	监听器（共享型）	1分钟
m8_out_Bps	网络流出速率	测量对象访问外部所消耗的流量。 单位：字节/秒	≥ 0bytes/s	监听器（共享型）	1分钟
m9_abnormal_servers	异常主机数	健康检查统计监控对象后端异常的主机个数。 单位：个	≥ 0个	监听器（共享型）	1分钟
ma_normal_servers	正常主机数	健康检查统计监控对象后端正常的主机个数。 单位：个	≥ 0个	监听器（共享型）	1分钟
m22_in_bandwidth	入网带宽	统计测量对象当前入网带宽。 单位：比特/秒	≥ 0bit/s	监听器（共享型）	1分钟
m23_out_bandwidth	出网带宽	统计测量对象当前出网带宽。 单位：比特/秒	≥ 0bit/s	监听器（共享型）	1分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
m1e_server_rps	后端服务器重置数量	统计后端服务器发送至客户端的重置（RST）数据包的计数。这些重置数据包由后端服务器生成，然后由负载均衡器转发。 （仅TCP监听器有此指标） 单位：个/秒	≥ 0个/秒	监听器（共享型）	1分钟
m21_client_rps	客户端重置数量	统计客户端发送至后端服务器的重置（RST）数据包的计数。这些重置数据包由客户端生成，然后由负载均衡器转发。 （仅TCP监听器有此指标） 单位：个/秒	≥ 0个/秒	监听器（共享型）	1分钟
m1f_lvs_rps	负载均衡器重置数量	统计负载均衡器生成的重置（RST）数据包的计数。 （仅TCP监听器有此指标） 单位：个/秒	≥ 0个/秒	监听器（共享型）	1分钟
mb_l7_qps	7层查询速率	统计测量对象当前7层查询速率。 （HTTP和HTTPS监听器才有此指标） 单位：个/秒。	≥ 0个/秒	监听器（共享型）	1分钟
mc_l7_http_2xx	7层协议返回码(2XX)	统计测量对象当前7层2XX系列状态响应码的数量。 （HTTP和HTTPS监听器才有此指标） 单位：个/秒。	≥ 0个/秒	监听器（共享型）	1分钟
md_l7_http_3xx	7层协议返回码(3XX)	统计测量对象当前7层3XX系列状态响应码的数量。 （HTTP和HTTPS监听器才有此指标） 单位：个/秒。	≥ 0个/秒	监听器（共享型）	1分钟
me_l7_http_4xx	7层协议返回码(4XX)	统计测量对象当前7层4XX系列状态响应码的数量。 （HTTP和HTTPS监听器才有此指标） 单位：个/秒。	≥ 0个/秒	监听器（共享型）	1分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
mf_l7_http_5xx	7层协议返回码(5XX)	统计测量对象当前7层5XX系列状态响应码的数量。 （HTTP和HTTPS监听器才有此指标） 单位：个/秒。	≥ 0个/秒	监听器（共享型）	1分钟
m10_l7_http_other_status	7层协议返回码(Others)	统计测量对象当前7层非2XX,3XX,4XX,5XX系列状态响应码的数量。（HTTP和HTTPS监听器才有此指标） 单位：个/秒。	≥ 0个/秒	监听器（共享型）	1分钟
m11_l7_http_404	7层协议返回码(404)	统计测量对象当前7层404状态响应码的数量。 （HTTP和HTTPS监听器才有此指标） 单位：个/秒。	≥ 0个/秒	监听器（共享型）	1分钟
m12_l7_http_499	7层协议返回码(499)	统计测量对象当前7层499状态响应码的数量。 （HTTP和HTTPS监听器才有此指标） 单位：个/秒。	≥ 0个/秒	监听器（共享型）	1分钟
m13_l7_http_502	7层协议返回码(502)	统计测量对象当前7层502状态响应码的数量。 （HTTP和HTTPS监听器才有此指标） 单位：个/秒。	≥ 0个/秒	监听器（共享型）	1分钟
m14_l7_rt	7层协议RT平均值	统计测量对象当前7层平均响应时间。 （HTTP和HTTPS监听器才有此指标） 从测量对象收到客户端请求开始，到测量对象将所有响应返回给客户端为止。 单位：毫秒。 **说明** websocket场景下RT平均值可能会非常大，此时该指标无法作为时延指标参考。	≥ 0ms	监听器（共享型）	1分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
m15_l7_upstream_4xx	7层后端返回码(4XX)	统计测量对象当前7层后端4XX系列状态响应码的数量。 （HTTP和HTTPS监听器才有此指标） 单位：个/秒。	≥ 0个/秒	监听器（共享型）	1分钟
m16_l7_upstream_5xx	7层后端返回码(5XX)	统计测量对象当前7层后端5XX系列状态响应码的数量。 （HTTP和HTTPS监听器才有此指标） 单位：个/秒。	≥ 0个/秒	监听器（共享型）	1分钟
m17_l7_upstream_rt	7层后端的RT平均值	统计测量对象当前7层后端平均响应时间。 （HTTP和HTTPS监听器才有此指标） 从测量对象将请求转发给后端服务器开始，到测量对象收到后端服务器返回响应为止。 单位：毫秒。 **说明** websocket场景下RT平均值可能会非常大，此时该指标无法作为时延指标参考。	≥ 0ms	监听器（共享型）	1分钟
m1a_l7_upstream_rt_max	7层后端的RT最大值	统计测量对象当前7层后端最大响应时间。 （HTTP和HTTPS监听器才有此指标） 从测量对象将请求转发给后端服务器开始，到测量对象收到后端服务器返回响应为止。 单位：毫秒。	≥ 0ms	监听器（共享型）	1分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
m1b_l7_upstream_rt_min	7层后端的RT最小值	统计测量对象当前7层后端最小响应时间。 （HTTP和HTTPS监听器才有此指标） 从测量对象将请求转发给后端服务器开始，到测量对象收到后端服务器返回响应为止。 单位：毫秒。	≥ 0ms	监听器（共享型）	1分钟
m1c_l7_rt_max	7层协议的RT最大值	统计测量对象当前7层最大响应时间。 （HTTP和HTTPS监听器才有此指标） 从测量对象收到客户端请求开始，到测量对象将所有响应返回给客户端为止。 单位：毫秒。	≥ 0ms	监听器（共享型）	1分钟
m1d_l7_rt_min	7层协议的RT最小值	统计测量对象当前7层最小响应时间。 （HTTP和HTTPS监听器才有此指标） 从测量对象收到客户端请求开始，到测量对象将所有响应返回给客户端为止。 单位：毫秒。	≥ 0ms	监听器（共享型）	1分钟

表 2-45 后端服务器组的监控指标（共享型）

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
m9_abnormal_servers	异常主机数	健康检查统计监控对象后端异常的主机个数。 单位：个	≥ 0个	后端服务器组（共享型）	1分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
ma_normal_servers	正常主机数	健康检查统计监控对象后端正常的主机个数。 单位：个	≥ 0个	后端服务器组（共享型）	1分钟
m17_l7_upstream_rt	7层后端的RT平均值	统计测量对象当前7层后端平均响应时间。 （HTTP和HTTPS监听器才有此指标） 从测量对象将请求转发给后端服务器开始，到测量对象收到后端服务器返回响应为止。 单位：毫秒 **说明** websocket场景下RT平均值可能会非常大，此时该指标无法作为时延指标参考。	≥ 0ms	后端服务器组（共享型）	1分钟
m1a_l7_upstream_rt_max	7层后端的RT最大值	统计测量对象当前7层后端最大响应时间。 （HTTP和HTTPS监听器才有此指标） 从测量对象将请求转发给后端服务器开始，到测量对象收到后端服务器返回响应为止。 单位：毫秒	≥ 0ms	后端服务器组（共享型）	1分钟
m1b_l7_upstream_rt_min	7层后端的RT最小值	统计测量对象当前7层后端最小响应时间。 （HTTP和HTTPS监听器才有此指标） 从测量对象将请求转发给后端服务器开始，到测量对象收到后端服务器返回响应为止。 单位：毫秒	≥ 0ms	后端服务器组（共享型）	1分钟
mb_l7_qps	7层查询速率	统计测量对象当前7层查询速率。 （HTTP和HTTPS监听器才有此指标） 单位：个/秒	≥ 0个/秒	后端服务器组（共享型）	1分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
m18_l7_upstream_2xx	7层后端返回码(2XX)	统计测量对象当前7层后端2XX系列状态响应码的数量。（HTTP和HTTPS监听器才有此指标） 单位：个/秒	≥ 0个/秒	后端服务器组（共享型）	1分钟
m19_l7_upstream_3xx	7层后端返回码(3XX)	统计测量对象当前7层后端3XX系列状态响应码的数量。（HTTP和HTTPS监听器才有此指标） 单位：个/秒	≥ 0个/秒	后端服务器组（共享型）	1分钟
m15_l7_upstream_4xx	7层后端返回码(4XX)	统计测量对象当前7层后端4XX系列状态响应码的数量。（HTTP和HTTPS监听器才有此指标） 单位：个/秒	≥ 0个/秒	后端服务器组（共享型）	1分钟
m16_l7_upstream_5xx	7层后端返回码(5XX)	统计测量对象当前7层后端5XX系列状态响应码的数量。 （HTTP和HTTPS监听器才有此指标） 单位：个/秒	≥ 0个/秒	后端服务器组（共享型）	1分钟
m25_l7_resp_Bps	7层响应带宽	统计周期时间内主机组的响应发送带宽。 单位：比特/秒 **说明** 当监听器开启HTTP/2时，该指标无法作为参考。	≥ 0bit/s	后端服务器组（共享型）	1分钟
m24_l7_req_Bps	7层请求带宽	统计周期时间内主机组的请求接收带宽。 单位：比特/秒 **说明** 当监听器开启HTTP/2时，该指标无法作为参考。	≥ 0bit/s	后端服务器组（共享型）	1分钟

维度

Key	Value
lbaas_instance_id	共享型负载均衡器的ID。

Key	Value
lbaas_listener_id	共享型负载均衡监听器的ID。
lbaas_pool_id	后端服务器组的ID

2.9.3 查看流量使用情况

应用场景

在视频直播中，网络访问流量的突增可能会引起业务的动荡，因此视频直播平台通常都会使用ELB自动分发流量到多台服务器。如果您担心流量过大引起业务问题，需要查看弹性负载均衡的使用流量，或者针对公网负载均衡，您需要查看某一时间段内弹性负载均衡绑定的EIP流量使用情况，云监控服务可以监控ELB的流量数据。

前提条件

已经正常运行了一段时间的负载均衡器。

关联的后端服务器在关机、故障、删除状态，无法在云监控中查看其监控指标。当后端服务器再次启动或恢复后，即可正常查看。

查看绑定的 EIP 使用流量

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 虚拟私有云”。
4. 在左侧导航树，选择“弹性公网IP和带宽 > 弹性公网IP”。
5. 在弹性负载均衡绑定的EIP名称所在行，选择需要查看的EIP单击，切换到“带宽”页签，支持查看“近1小时”、“近3小时”、“近12小时”、“近1天”、“近7天”的数据。

图 2-33 EIP 使用流量监控结果

表 2-46 EIP 和带宽支持的监控指标

指标名称	含义	取值范围	测试对象	监控周期（原始指标）
出网带宽	该指标用于统计测试对象出云平台的网络速度（原指标为上行带宽）。	≥ 0 bits/s	带宽或弹性公网IP。	1分钟
入网带宽	该指标用于统计测试对象入云平台的网络速度（原指标为下行带宽）。	≥ 0 bits/s	带宽或弹性公网IP。	1分钟
出网带宽使用率	该指标用于统计测量对象出云平台的带宽使用率，以百分比为单位。	0-100%	带宽或弹性公网IP。	1分钟
入网带宽使用率	该指标用于统计测量对象入云平台的带宽使用率，以百分比为单位。	0-100%	带宽或弹性公网IP。	1分钟
出网流量	该指标用于统计测试对象出云平台的网络流量（原指标为上行流量）。	≥ 0 bytes	带宽或弹性公网IP。	1分钟
入网流量	该指标用于统计测试对象入云平台的网络流量（原指标为下行流量）。	≥ 0 bytes	带宽或弹性公网IP。	1分钟

查看弹性负载均衡使用流量

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在“负载均衡器”界面，单击需要查看流量的负载均衡器名称。
5. 切换到“监控”页签，单击需要查看的监控粒度，查看网络流入速率和网络流出速率。

   支持查看“近1小时”、“近3小时”、“近12小时”、“近1天”和“近7天”的数据。

2.10 审计

2.10.1 支持审计的关键操作列表

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

云审计支持的弹性负载均衡操作事件列表如**表2-47**所示。

表 2-47 云审计服务支持的弹性负载均衡操作列表

操作名称	资源类型	事件名称
配置访问日志	logtank	createLogtank
删除访问日志	logtank	deleteLogtank
创建证书	certificate	createCertificate
更新证书	certificate	updateCertificate
删除证书	certificate	deleteCertificate
创建健康检查	healthmonitor	createHealthMonitor
更新健康检查	healthmonitor	updateHealthMonitor
删除健康检查	healthmonitor	deleteHealthMonitor
创建转发策略	l7policy	createL7policy
更新转发策略	l7policy	updateL7policy
删除转发策略	l7policy	deleteL7policy
创建转发规则	l7rule	createl7rule
更新转发规则	l7rule	updateL7rule
删除转发规则	l7rule	deleteL7rule
创建监听器	listener	createListener
更新监听器	listener	updateListener
删除监听器	listener	deleteListener
创建负载均衡器	loadbalancer	createLoadbalancer
更新负载均衡器	loadbalancer	updateLoadbalancer
删除负载均衡器	loadbalancer	deleteLoadbalancer
添加后端云服务器	member	createMember
更新后端云服务器	member	updateMember
移除后端云服务器	member	batchUpdateMember
创建后端服务器组	pool	createPool
更新后端服务器组	pool	updatPool
删除后端服务器组	pool	deletePool

2.10.2 查看审计日志

操作场景

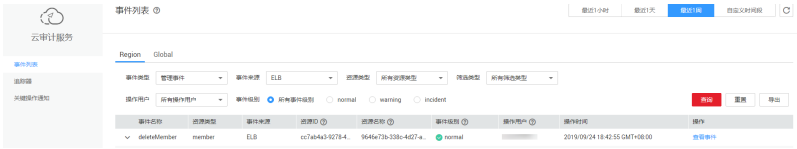
在您开启了云审计服务后，系统开始记录云服务资源的操作。云审计服务管理控制台保存最近7天的操作记录。

本节介绍如何在云审计服务管理控制台查看最近7天的操作记录。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“管理与监管 > 云审计服务”，进入云审计服务信息页面。
4. 单击左侧导航树的“事件列表”，进入事件列表信息页面。
5. 事件列表支持通过筛选来查询对应的操作事件。当前事件列表支持四个维度的组合查询，详细信息如下：
   - 事件类型、事件来源、资源类型和筛选类型。
     在下拉框中选择查询条件。
     其中筛选类型选择事件名称时，还需选择某个具体的事件名称。
     选择资源ID时，还需选择或者手动输入某个具体的资源ID。
     选择资源名称时，还需选择或手动输入某个具体的资源名称。
   - 操作用户：在下拉框中选择某一具体的操作用户，此操作用户指用户级别，而非租户级别。
   - 事件级别：可选项为“所有事件级别”、“normal”、“warning”、“incident”，只可选择其中一项。
   - 时间范围：在页面右上角，可选择查询最近七天内任意时间段的操作事件。
6. 在需要查看的记录左侧，单击 展开该记录的详细信息。如**图 展开记录**所示。

图 2-34 展开记录



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

图 2-35 查看事件

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

审计日志示例

- 创建负载均衡器

request {"loadbalancer":{"name":"elb-test-zcy","description":"","tenant_id":"05041fffa40025702f6dc009cc6f8f33","vip_subnet_id":"ed04fd93-e74b-4794-b63e-e72baa02a2da","admin_state_up":true}}
code 201
source_ip 124.71.93.36
trace_type ConsoleAction
event_type system
project_id 05041fffa40025702f6dc009cc6f8f33
trace_id b39b21a1-8d49-11ec-b548-2be046112888
trace_name createLoadbalancer
resource_type loadbalancer
trace_rating normal
api_version v2.0
service_type ELB
response {"loadbalancer": {"description": "", "provisioning_status": "ACTIVE", "provider": "vlb", "project_id": "05041fffa40025702f6dc009cc6f8f33", "vip_address": "172.18.0.205", "pools": [], "operating_status": "ONLINE", "name": "elb-test-zcy", "created_at": "2022-02-14T03:53:39", "listeners": [], "id": "7ebe23cd-1d46-4a49-b707-1441c7f0d0d1", "vip_port_id": "5b36ff96-3773-4736-83cf-38c54abedeea", "updated_at": "2022-02-14T03:53:41", "tags": [], "admin_state_up": true, "vip_subnet_id": "ed04fd93-e74b-4794-b63e-e72baa02a2da", "tenant_id": "05041fffa40025702f6dc009cc6f8f33"}}
resource_id 7ebe23cd-1d46-4a49-b707-1441c7f0d0d1
tracker_name system
time 2022/02/14 11:53:42 GMT+08:00
resource_name elb-test-zcy
record_time 2022/02/14 11:53:42 GMT+08:00
request_id
user {"domain": {"name": "CBUInfo", "id": "0503dda87802345ddafed096d70a960"}, "name": "zcy", "id": "09f106afd2345cdeff5c009c58f5b4a"}

- 删除负载均衡器

request
code 204
source_ip 124.71.93.36
trace_type ConsoleAction
event_type system
project_id 05041fffa40025702f6dc009cc6f8f33
trace_id 4f838bbf-8d4a-11ec-a1fe-1f93fdaf3bec
trace_name deleteLoadbalancer
resource_type loadbalancer
trace_rating normal
api_version v2.0

service_type ELB
response {"loadbalancer": {"listeners": [], "vip_port_id": "5b36ff96-3773-4736-83cf-38c54abedeea", "tags": [], "tenant_id": "05041fffa40025702f6dc009cc6f8f33", "admin_state_up": true, "id": "7ebe23cd-1d46-4a49-b707-1441c7f0d0d1", "operating_status": "ONLINE", "description": "", "pools": [], "vip_subnet_id": "ed04fd93-e74b-4794-b63e-e72baa02a2da", "project_id": "05041fffa40025702f6dc009cc6f8f33", "provisioning_status": "ACTIVE", "name": "elb-test-zcy", "created_at": "2022-02-14T03:53:39", "vip_address": "172.18.0.205", "updated_at": "2022-02-14T03:53:41", "provider": "vlb"}}
resource_id 7ebe23cd-1d46-4a49-b707-1441c7f0d0d1
tracker_name system
time 2022/02/14 11:58:03 GMT+08:00
resource_name elb-test-zcy
record_time 2022/02/14 11:58:03 GMT+08:00
request_id
user {"domain": {"name": CBUInfo", "id": "0503dda87802345ddafed096d70a960"}, "name": "zcy", "id": "09f106afd2345cdeff5c009c58f5b4a"}

3 自助诊断工具

3.1 自助诊断工具概述

弹性负载均衡自助问题诊断可以帮助您诊断健康检查异常问题，帮助您发现并解决常见问题，提升使用负载均衡的效率。实例诊断期间可能会对您指定的实例进行探测和诊断分析，不会对实例的正常配置和业务造成影响。

目前已支持对如**表3-1**所示的问题进行诊断。

说明

自助问题诊断陆续上线中，已发布区域请参见**自助问题诊断**。

表 3-1 负载均衡实例诊断说明

诊断问题	诊断说明
健康检查异常诊断	• 安全组规则配置：诊断后端服务器的安全组规则配置。 • 网络ACL规则配置：诊断后端服务器的网络ACL规则配置。 • 健康检查配置：诊断健康检查端口配置。
ELB计费问题	了解ELB的计费规则、变更ELB的规格和计费模式。
ELB的使用区别	了解ELB的功能特性差异。

3.2 健康检查异常诊断

操作场景

ELB健康检查异常诊断能帮助您发现健康检查结果异常后端服务器的问题并提供修复建议。

本文介绍如何使用自助ELB健康检查异常诊断功能以及具体的诊断项目。

说明

自助健康检查异常诊断陆续上线中，已发布区域请参见**自助问题诊断**。

前提条件

发起健康检查异常诊断前，请确保您已创建了ELB实例并后端服务器关联至负载均衡的监听器下。

具体操作要求，请参见：

- **创建负载均衡实例**。
- **创建后端服务器组并添加后端服务器**。
- **为负载均衡器添加监听器，并将后端服务器组关联至监听器下**。
- **后端服务器组已开启健康检查**。

约束与限制

- 仅支持对健康检查结果异常的后端服务器发起诊断。
- 仅支持对已关联至监听器使用的后端服务器发起诊断。
- 不支持对跨VPC后端发起健康检查异常诊断。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 单击页面左上角的 ，选择“网络 > 弹性负载均衡”。
4. 在左侧导航栏，选择“ 自助问题诊断”。
5. 在弹性负载均衡自助诊断界面，单击“ELB健康检查异常”页签。
6. 选择异常后端服务器关联的负载均衡实例。
7. 选择需要诊断的异常后端服务器。
8. 单击“开始诊断”，在问题诊断页面，查看诊断进度以及具体的诊断详情。
   显示的诊断结果为该后端服务器诊断异常项目，请及时修复。支持的诊断项目请参见**表3-2**。

图 3-1 自助问题诊断—健康检查异常

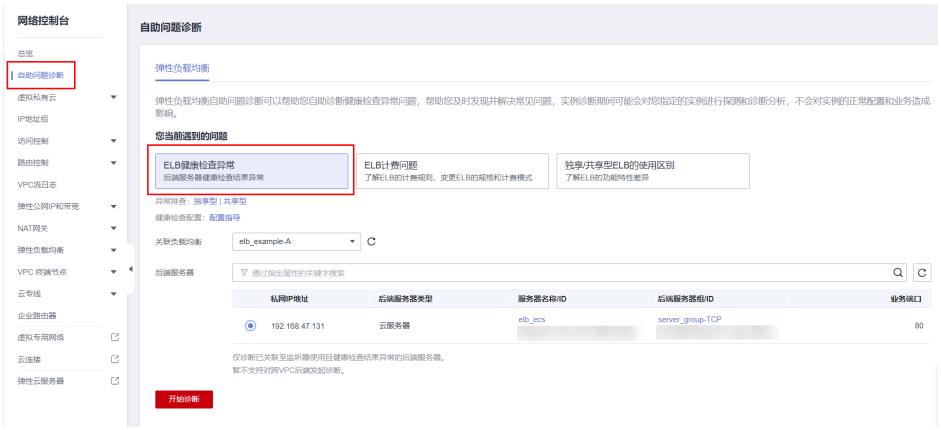


表 3-2 健康检查异常诊断项

诊断项分类	健康检查项目	诊断异常原因	建议
安全组规则配置	健康检查入方向协议检查	后端服务器的安全组入方向规则未放通健康检查对应的传输层协议。	请确保后端服务器配置放通安全组规则，配置详情请参见： • **后端服务器配置安全组（独享型）**。 • **后端服务器配置安全组（共享型）**。
	健康检查入方向源地址检查	后端服务器的安全组入方向规则未放通健康检查源IP。	
	健康检查入方向端口检查	后端服务器的安全组入方向规则未放通健康检查端口。	
	健康检查出方向协议检查	后端服务器的安全组出方向规则未放通健康检查对应的传输层协议。	
	健康检查出方向源地址检查	后端服务器的安全组出方向规则未放通健康检查源IP。	
	健康检查出方向端口检查	后端服务器的安全组出方向规则未放通健康检查端口。	
网络ACL规则配置	健康检查入方向协议检查	后端服务器的网络ACL入方向规则未放通对应的传输层协议。	请确保后端服务器配置放通网络ACL规则，配置详情请参见： • **后端服务器配置网络ACL（独享型）**。 • **后端服务器配置网络ACL（共享型）**。
	健康检查入方向源地址检查	后端服务器的网络ACL入方向规则未放通健康检查源地址。	
	健康检查方向源端口检查	后端服务器的网络ACL入方向规则未放通**全部源端口**。	
	健康检查入方向目的地址检查	后端服务器的网络ACL入方向规则未放通健康检查目的地址。	
	健康检查入方向目的端口检查	后端服务器的网络ACL入方向规则未放通健康检查目的端口。	
	健康检查出方向协议检查	后端服务器的网络ACL出方向规则未放通健康检查对应的传输层协议。	
	健康检查出方向源地址检查	后端服务器的网络ACL出方向规则未放通健康检查源地址。	

诊断项分类	健康检查项目	诊断异常原因	建议
	健康检查出方向源端口检查	后端服务器的网络ACL出方向规则未放通健康检查源端口。	
	健康检查出方向目的地址检查	后端服务器的网络ACL出方向规则未放通健康检查目的地址。	
	健康检查出方向目的端口检查	后端服务器的网络ACL出方向规则未放通**全部目的端口**。	
健康检查配置	健康检查端口配置检查	指定的健康检查端口和后端服务器的业务端口不一致。	建议指定后端服务器的业务端口为健康检查端口，配置详情请参见**修改健康检查配置**。

说明

- 自助诊断项无异常，请参考**健康检查异常如何排查？**进一步诊断。
- 诊断失败，您可单击“重新诊断”或者参考**健康检查异常如何排查？**进一步诊断。

3.3 其他自助问题诊断

如果您在使用ELB的过程中遇到以下问题，也可通过弹性负载均衡自助诊断工具进行诊断。

- **ELB计费问题**。
- **独享型和共享型ELB的使用区别**。

ELB 计费问题

了解ELB的计费规则、变更ELB的规格和计费模式，详情请参见**表3-3**。

表 3-3 负载均衡计费概览

计费常见场景	参考文档
计费规则	• **计费说明（独享型）**。 • **计费说明（共享型）**。
计费模式	**变更计费模式**。
计费规格	**变更实例规格**。

独享型和共享型 ELB 的使用区别

了解ELB的功能特性差异，详情请参见表3-4。

表 3-4 负载均衡区别概览

负载均衡区别场景	参考文档
负载均衡功能对比	独享型负载均衡与共享型弹性负载均衡的区别。
负载均衡配置后端服务器组	• 创建后端服务器组。 • 创建后端服务器组。
负载均衡配置后端服务器	• 后端服务器概述。 • 后端服务器概述。

4 附录

4.1 TOA 插件配置

操作场景

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

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

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

说明

- TOA不支持UDP协议的监听器。
- TOA模块在以下操作系统中验证可以正常工作，其他内核版本安装方法类似。
  - CentOS 6.8（Kernel version 2.6.32）
  - Suse 11 sp3 (Kernel version 3.0.76)
  - CentOS 7/7.2 (Kernel version 3.10.0)
  - Ubuntu 16.04.3 (Kernel version 4.4.0)
  - Ubuntu 18.04 (Kernel version 4.15.0)
  - Ubuntu 20.04 (Kernel version 5.4.0)
  - OpenSUSE 42.2 (Kernel version 4.4.36)
  - Debian 8.2.0 (Kernel version 3.16.0)

前提条件

- 编译内核模块开发环境需与当前内核版本开发环境一致，例如内核版本为kernel-3.10.0-693.11.1.el7，则需要安装对应版本的内核开发包kernel-devel-3.10.0-693.11.1.el7。
- 确保虚拟机可以访问开放源。

- 如果是非root用户，需拥有sudo权限。

操作步骤

- **以下操作步骤是针对Linux内核版本为3.0以上的操作系统。**

1. 准备编译环境。

   说明

   - 安装内核模块开发包的过程中，如果源里面找不到对应内核版本的安装包，需要自行去网上下载需要的安装包。
   - 对于无法获取到内核开发包（kernel-devel）的情况，需要联系镜像提供者获取内核开发包。

   以下是不同Linux发行版本的操作说明，请根据环境选择对应的方案。

   - CentOS环境下的操作步骤。
     i. 执行如下命令，安装gcc编译器。

        sudo yum install gcc

     ii. 执行如下命令，安装make工具。

        sudo yum install make

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

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

        说明

        - 如果自带源里没有对应的内核开发包，可以到如下地址中去下载对应的rpm包。

          地址：https://mirror.netcologne.de/oracle-linux-repos/ol7_latest/getPackage/

          以3.10.0-693.11.1.el7.x86_64为例，下载后执行以下命令安装：

          rpm -ivh kernel-devel-3.10.0-693.11.1.el7.x86_64.rpm。
        - 对于无法获取到内核开发包（kernel-devel）的情况，需要联系镜像提供者获取内核开发包。

   - Ubuntu、Debian环境下的操作步骤。
     i. 执行如下命令，安装gcc编译器。

        sudo apt-get install gcc

     ii. 执行如下命令，安装make工具。

        sudo apt-get install make

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

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

   - SUSE环境下的操作步骤。
     i. 执行如下命令，安装gcc编译器。

        sudo zypper install gcc

     ii. 执行如下命令，安装make工具。

        sudo zypper install make

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

sudo zypper install kernel-default-devel

2. 编译内核模块

a. 使用git工具，执行如下命令，下载TOA内核模块源代码。

git clone https://github.com/Huawei/TCP_option_address.git

说明

如果未安装git工具，请进入以下链接下载TOA模块源代码。

https://github.com/Huawei/TCP_option_address

b. 执行如下命令，进入源码目录，编译模块。

cd src

make

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

说明

- 如果报错提示“config_retpoline=y but not supported by the compiler, Compiler update recommended”，表明gcc版本过老，建议将gcc升级为较新版本。
- 如果在标准Linux发行版本中手动升级过内核版本，且编译TOA模块失败，建议将gcc升级为较新版本。

3. 加载内核模块

a. 执行如下命令，加载内核模块。

sudo insmod toa.ko

b. 执行如下命令，验证模块加载情况，查看内核输出信息。

dmesg | grep TOA

若提示信息包含“TOA: toa loaded”，说明内核模块加载成功。

说明

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

4. 自动加载内核模块

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

自动加载内核模块的方法有以下两种方法：

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

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

toa.modules文件内容，请参考如下示例：

#!/bin/sh

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

if [$? -eq 0]; then

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

fi

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

ii. 执行以下命令，为toa.modules启动脚本添加可执行权限。

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

说明

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

5. 安装多节点

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

内核模块加载成功以后，应用程序可以正常获取访问者的真实源IP地址。

说明

节点的操作系统发行版与内核版本必须相同。

6. 验证TOA内核模块

TOA内核模块安装成功后即可直接获取到源地址，此处提供一个验证的例子。

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

python -m SimpleHTTPServer *port*

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

启动之后，通过客户端访问ELB的IP时，服务端的访问日志如下：

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

说明

上述访问日志中**192.168.0.90**，是后端服务器可以获取到的客户端源IP地址，即客户访问后端服务器的真实IP地址。

- **以下操作步骤是针对Linux内核版本为2.6.32的操作系统。**

说明

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

1. 从以下网站中获取含有TOA模块的内核源代码包（Linux-2.6.32-220.23.1.el6.x86_64.rs.src.tar.gz）。

http://kb.linuxvirtualserver.org/images/3/34/Linux-2.6.32-220.23.1.el6.x86_64.rs.src.tar.gz

2. 解压TOA模块的内核源码包。
3. 修改编译相关参数。
   a. 进入“linux-2.6.32-220.23.1.el6.x86_64.rs”文件夹。
   b. 编辑“net/toa/toa.h”文件。
      将#define TCPOPT_TOA200配置项修改为#define TCPOPT_TOA254
   c. 在shell页面，执行以下命令。

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

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

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

d. 编辑Makefile。

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

4. 执行以下命令，编译软件包。

make -j *n*

说明

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

5. 执行以下命令，安装内核模块。

make modules_install

命令执行结果如图4-1所示。

图 4-1 安装内核模块

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

6. 执行如下命令，安装内核。

make install

命令执行结果如图4-2所示。

图 4-2 安装内核

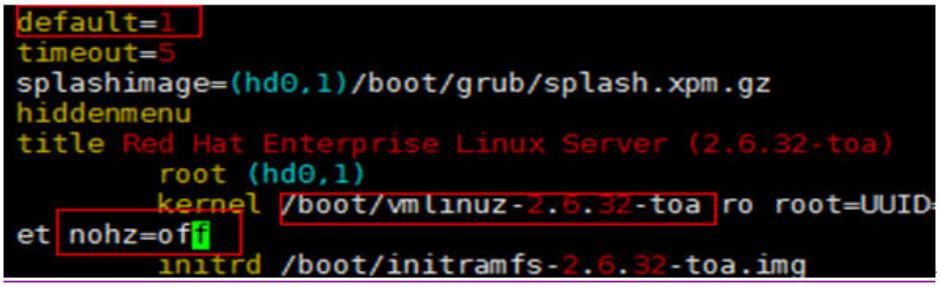
```
  INSTALL /lib/firmware/keyspan_pda/xircom_pgs.fw
  DEPMOD  2.6.32-toa
[root@SZX1000167219 linux-2.6.32-220.23.1.el6.x86_64.rs]# make install
sh /root/humin/linux-2.6.32-220.23.1.el6.x86_64.rs/arch/x86/boot/install.sh 2.6.32-toa arch/x86/boot/bzImage \
        System.map "/boot"
ERROR: modinfo: could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

7. 打开“/boot/grub/grub.conf”文件，配置开机默认启动，如图4-3所示。

a. 将开机默认启动内核由第一个内核修改为第零个内核，即“default=1”修改为“default=0”。

b. 在新增的含有toa模块的vmlinuz-2.6.32-toa内核行末尾添加“nohz=off”参数。如果不关闭nohz，大压力下CPU0可能会消耗过高，导致压力不均匀

图 4-3 配置文件



c. 修改完成后保存退出，重启操作系统。

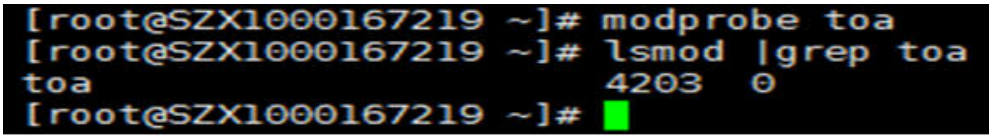
重启系统时，系统将加载vmlinuz-2.6.32-toa内核。

8. 待系统重启完成之后，执行以下命令加载TOA模块。

modprobe toa

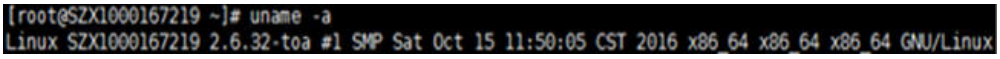
建议将modprobe toa命令加入开机启动脚本，以及系统定时监控脚本中，如图4-4所示。

图 4-4 modprobe toa 命令



TOA模块加载完成后，查询内核信息如图4-5所示。

图 4-5 查询内核



9. 验证TOA内核模块

TOA内核模块安装成功后即可直接获取到源地址，此处提供一个验证的例子。

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

python -m SimpleHTTPServer *port*

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

启动之后，通过客户端访问ELB的IP时，服务端的访问日志如下：

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

说明

上述访问日志中**192.168.0.90**，是后端服务器可以获取到的客户端源IP地址，即客户访问后端服务器的真实IP地址。

