弹性负载均衡

用户指南

文档版本 01

发布日期 2025-11-19

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 独享型 ELB 使用流程概述

如果您初次使用弹性负载均衡ELB服务，您可以根据本文内容快速了解使用本云服务的流程。

弹性负载均衡是一种对流量进行按需分发的服务，通过将流量分发到不同的后端服务器来扩展应用系统的吞吐能力，并且可以消除系统中的单点故障，提升应用系统的可用性。

ELB 组成架构

图 1-1 ELB 组成架构图

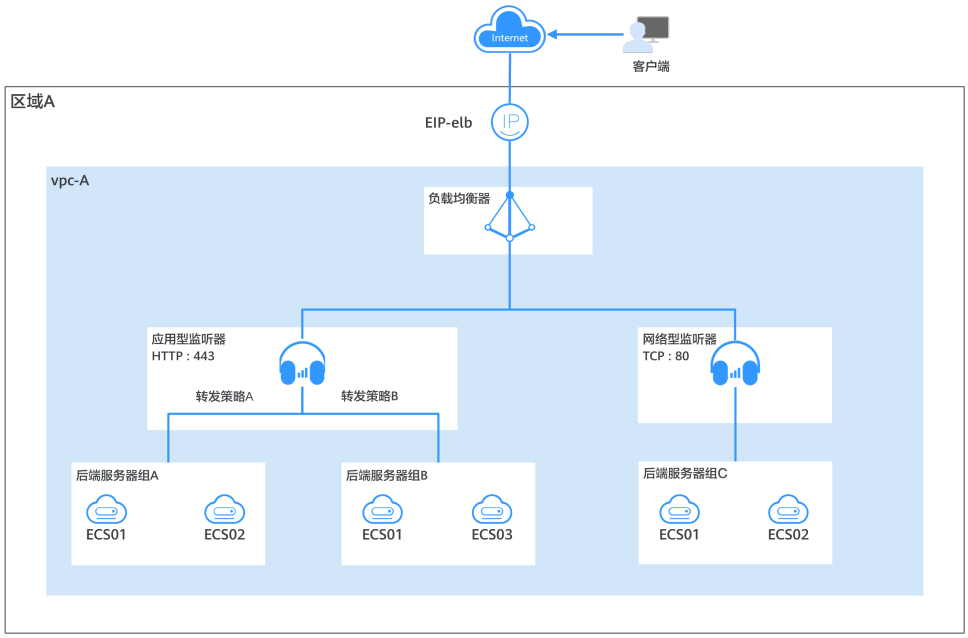


表 1-1 ELB 组成架构说明

概念	说明	相关文档
负载均衡器	您创建的承载业务的弹性负载均衡服务实体。 创建负载均衡器后，您还需要在负载均衡器中配置监听器后才能使用负载均衡服务提供的功能。	独享型负载均衡器概述
监听器	监听器是ELB最小的业务单元，负责监听访问到负载均衡器上的请求。 监听器需要配置监听器协议和端口处理对应的业务请求，例如TCP协议，80端口。每个ELB至少配置一个监听器才能监听并分发业务流量。支持配置多个不同的监听器用于处理不同协议和端口的业务。 网络型监听器将流量转发至默认后端服务器组，应用型监听器按照转发策略转发流量。	监听器概述
转发策略	仅应用型监听器支持配置转发策略。转发策略用于确定应用型负载均衡器如何将请求分发到一个或多个后端服务器组。 应用型ELB具备强大的七层处理能力，支持多种应用协议与转发策略，支持您基于业务实际进行灵活的流量负载。	高级转发策略
后端服务器组	后端服务器组是一个或多个后端服务器的逻辑集合，组内的服务器用于处理负载均衡器分发的业务请求。 后端服务器组可以独立于负载均衡器而存在，同一服务器组可以关联到多个不同负载均衡器下。	后端服务器组概述
后端服务器	后端服务器组内用于处理客户端请求的实际服务器，可以是弹性云服务器实例、裸金属服务器实例、辅助弹性网卡或IP地址。当添加对象是辅助弹性网卡或IP地址时，实际处理请求的是辅助弹性网卡或IP地址所在的服务器。 通常会使用健康检查来探测后端服务器的健康状态，以确保只有健康的服务器才会接收流量。如果某台服务器健康检查异常，服务器组内的流量将不会分发到该台服务器，保证了业务的稳定性。	后端服务器概述

使用流程引导

建议您通过以下几个步骤快速实现弹性负载均衡服务的部署应用，详细操作可参见对应文档。

图 1-2 ELB 使用流程引导

操作步骤	说明
购买独享型负载均衡器	创建一个负载均衡器，并选择合适的配置选项，建议您重点关注以下配置。 • 基础配置：实例类型、计费方式，区域和可用区等。 • 实例规格：弹性规格和固定规格，网络型和应用型。 • 网络配置：网络类型（IPv4和IPv6），VPC和子网规划。
创建后端服务器组	创建后端服务器组并添加后端服务器进行统一管理调度。 由于后端服务器组独立于负载均衡器而存在，建议您先完成后端服务组的创建。后端服务器组的后端协议和监听器的前端协议存在匹配关系，建议您创建时重点关注后端协议类型，便于后续配置监听器时直接选择对应服务器组。
• 网络型监听器 • 应用型监听器	根据实际业务流量转发需求配置监听器，前端协议和端口应匹配业务请求。 • 应用型（HTTP/HTTPS）：支持HTTP、HTTPS和QUIC协议，适用于七层高性能要求业务，实时音视频、互动直播和游戏等业务。 • 网络型（TCP/UDP/TLS）：支持TCP、UDP和TLS协议，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。
高级转发策略	如果您使用应用型监听器进行流量转发，支持您根据请求的域名、路径、HTTP请求方法、HTTP请求头、查询字符串和网段等条件识别特定的业务流量并转发到不同的后端服务器组。

协议类型匹配关系

独享型负载均衡使用场景下，一个后端服务器组可关联至多个负载均衡实例和监听器使用，多个弹性负载均衡实例需归属同一企业项目。

后端服务器组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，前端/后端协议匹配关系详见表1-2。

表 1-2 前端/后端协议匹配关系

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

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

说明

弹性负载均衡支持TLS、GRPC、QUIC协议陆续上线中，请以控制台实际为准。

1.2 通过 IAM 授予使用 ELB 的权限

1.2.1 通过 IAM 角色或策略授予使用 ELB 的权限

如果您需要对您所拥有的ELB进行**角色与策略**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。

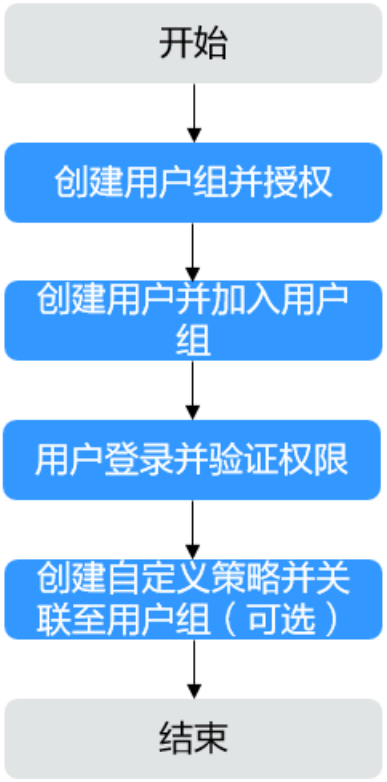
本章节为您介绍角色与策略的授权方法，操作流程如**图1-3**所示。

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**角色与策略权限管理**。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**授权参考**。

示例流程

图 1-3 给用户授予 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**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ELBReadOnlyAccess），表示“ELBReadOnlyAccess”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ELBReadOnlyAccess）的任一服务，若提示权限不足，表示“ELBReadOnlyAccess”已生效。

ELB 自定义策略样例

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**策略授权参考**。

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**。下面为您介绍常用的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ELBFullAccess的系统策略，但不希望用户拥有ELBFullAccess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ELBFullAccess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"
            ]
        }
    ]
}
```

1.2.2 通过 IAM 身份策略授予使用 ELB 的权限

如果您需要对您所拥有的ELB进行**身份策略**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用户或用户组，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，您可以跳过本章节，不影响您使用ELB服务的其它功能。

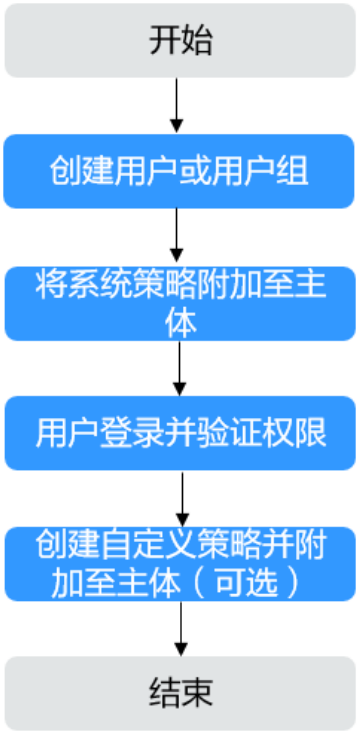
本章节为您介绍身份策略的授权方法，操作流程如图1-4所示。

前提条件

授权操作前，请您了解可以添加的ELB权限，并结合实际需求进行选择。ELB支持的系统策略，请参见**身份策略权限管理**。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**授权参考**。

示例流程

图 1-4 给用户授予 ELB 权限流程



1. **创建用户**或**创建用户组**
   在IAM控制台创建用户或用户组。
2. **将系统身份策略附加至用户或用户组**
   为用户或用户组授予弹性负载均衡只读权限的系统策略“ELBReadOnlyAccessPolicy”，并将策略附加至用户或用户组。
3. **用户登录**并验证权限

使用已授权的用户登录控制台，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ELBReadOnlyAccessPolicy），表示“ELBReadOnlyAccessPolicy”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ELBReadOnlyAccessPolicy）的任一服务，若提示权限不足，表示“ELBReadOnlyAccessPolicy”已生效。

ELB 自定义策略样例

如果系统预置的ELB系统策略，不满足您的授权要求，可以创建自定义身份策略。自定义身份策略中可以添加的授权项（Action）请参考。

目前华为云支持以下两种方式创建自定义身份策略：

- 可视化视图创建自定义身份策略：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视图创建自定义身份策略：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：**创建自定义身份策略并附加至主体**。

您可以在创建自定义身份策略时，可以通过资源类型（Resource）元素来选择特定资源，以及服务级条件键（Condition）元素来控制策略何时生效。支持的资源类型和条件键请参考身份策略授权。下面为您介绍常用的ELB自定义身份策略样例。

- 示例1：授权创建和删除负载均衡器的权限。

```
{
    "Version": "5.0",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "elb:loadbalancers:create",
                "elb:loadbalancers:delete"
            ]
        }
    ]
}
```

- 示例2：多个授权项策略

  一个自定义身份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。多个授权语句策略描述如下：

```
{
    "Version": "5.0",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "elb:loadbalancers:create",
                "elb:loadbalancers:delete"
            ]
        },
        {
            "Effect": "Deny",
            "Action": [
                "elb:loadbalancers:get",
                "elb:loadbalancers:list"
            ]
        },
```

```
        {
            "Effect": "Allow",
            "Action": [
                "vpc:vpcs:get",
                "vpc:vpcs:list"
            ]
        }
    ]
}
```

1.3 负载均衡器

1.3.1 独享型负载均衡器概述

弹性负载均衡服务能够根据您配置的分配策略将访问流量请求分发到多台后端服务器，提升您业务系统的可用性和扩展性。负载均衡器是指您创建的承载流量转发任务的ELB服务实例，您可以参考本文规划ELB实例的配置。

实例区域

- 不同区域的资源之间内网不互通。建议选择靠近业务的区域，可以降低网络时延、提高访问速度。
- 支持通过IP类型后端功能实现跨不同VPC添加后端服务器，详见**配置不同VPC的服务器作为后端服务器（IP类型后端）**。
- 实现跨区域间网络互通，详情请参见**连通不同区域的VPC网络**。

实例可用区

独享型负载均衡支持多可用区部署，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，可以减少网络时延并提高访问速度。

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 1-3 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 1-4 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，流量将被分配至本AZ中的ELB上，当本AZ的ELB不可用时，容灾切换到创建的其他AZ的ELB上。 如果本AZ的ELB正常，但是本AZ的流量超过规格，此时业务也会受影响，因此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的不同将流量分配至创建的多个AZ中的ELB上。
云专线访问	流量优先分配至**通过云专线对接的AZ**下部署的ELB，否则分配至其他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，否则分配至其他AZ下的ELB。

实例规格

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

建议参考**表1-5**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 1-5 实例规格选择说明

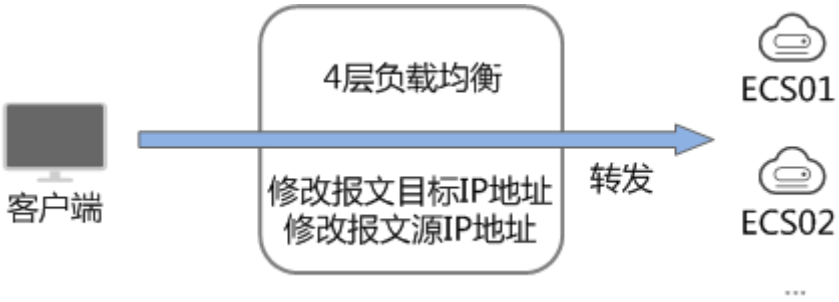
实例规格	规格选择说明
网络型规格	建议重点关注长连接的最大并发连接数，实例规格的“最大并发连接数”应作为关键参考指标。需要根据实际的业务场景，预估一个负载均衡实例需要承载的最大连接数，并选择相应的规格。
应用型规格	实例规格的“每秒查询速率 (QPS)”应作为关键参考指标，该指标决定了一个七层应用系统的业务吞吐量。需要根据实际的业务场景，预估一个负载均衡实例需要承载的QPS，并选择相应的规格。

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 1-5 网络型负载均衡器



- 应用型：聚焦应用层协议，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 1-6 应用型负载均衡器

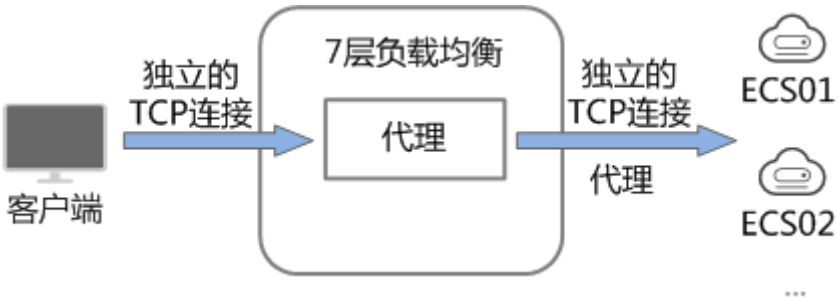


表 1-6 实例规格协议类型说明

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 1-7 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	需要为负载均衡器绑定EIP或者GEIP 。 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，建议先创建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：

- 建议后端服务器实例的所属区域和负载均衡器的所属区域相同。
- 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。

相关文档

- **独享型ELB使用流程概述**
- **购买独享型负载均衡器**
- **变更独享型负载均衡器的基础配置**
- **变更独享型负载均衡器的网络配置**
- **监听器概述**
- **后端服务器组概述**

1.3.2 购买独享型负载均衡器

操作场景

弹性负载均衡为您提供强大的网络层和应用层业务处理能力，可以将您海量的业务请求分发到多个后端服务器，保障了您业务的可用性。弹性负载均衡提供了多种流量分配策略、健康检查等机制，帮助您的业务系统持续稳定运行。

本文为您介绍如何创建一个弹性负载均衡实例。在您创建独享型负载均衡器前，请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**。

前提条件

您已经创建了用于部署弹性负载均衡的VPC和子网。具体操作，请参见**通过VPC快速搭建IPv4网络**和**通过VPC快速搭建IPv4/IPv6双栈网络**。

创建独享型负载均衡器

1. 进入**购买弹性负载均衡页面**。
2. 根据界面提示选择负载均衡器的基础配置，配置参数如**表1-8**所示。

表 1-8 负载均衡器的基础配置

参数	说明
计费模式	• 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。
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。
名称	待创建负载均衡器的名称。 • 长度范围为1~255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	创建负载均衡器时，可以将其加入已启用的企业项目。 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。 关于创建和管理企业项目的详情，请参见《**企业管理用户指南**》。

3. 选定独享型负载均衡实例的基础配置后，您需选择弹性负载均衡的实例规格，实例规格配置参数如**表1-9**所示。

表 1-9 负载均衡器的规格说明

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**。
负载均衡类型	• **应用型**（HTTP/HTTPS）：支持HTTP、HTTPS和QUIC协议，适用于七层高性能要求业务，实时音视频、互动直播和游戏等业务。 • **网络型**（TCP/UDP/TLS）：支持TCP、UDP和TLS协议，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。 • **应用型+网络型**：同时配置网络型（TCP/UDP/TLS）与应用型（HTTP/HTTPS）功能，为客户快速开通两种负载均衡类型的实例，可以实现全方位流量负载均衡管理，满足客户多样化的需求。
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。 弹性负载均衡支持将客户端请求跨可用区分发，建议选择与后端服务器所在可用区相同的可用区，可以减少网络时延以及提高访问速度。 **警告** • 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。

4. 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1-10**所示。

表 1-10 负载均衡器的网络配置

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。 如果网络类型未选择，则无法为ELB实例分配对外服务的IPv4私网地址或IPv6地址，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。 • **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。如果您有IPv4公网业务需求，请为负载均衡实例绑定弹性公网IP。 • **IPv6网络**：系统会为实例分配一个IPv6地址，转发来自IPv6客户端的请求。
所属VPC	负载均衡器所属虚拟私有云，**独享型ELB创建完成后不支持切换**，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	前端子网为独享型负载均衡提供私网IP地址，**用于与内网中的资源进行通信**。 ELB实例创建完成后，如果需要更换前端子网，可以通过解绑并绑定新的IPv4和IPv6地址实现。解绑IP地址可能会影响业务的正常运行，请谨慎操作。 根据您为ELB实例配置的网络类型分配对应的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网络**：前端子网作为IPv6子网为ELB实例下发IPv6地址。 当网络类型选择“IPv6网络”，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》。
IPv4地址	如果网络类型选择了“IPv4私网”，则需要选择IPv4地址的分配方式。 • **自动分配IP地址**：由系统自动为负载均衡器分配IPv4地址。 • **手动指定IP地址**：手动指定负载均衡器的IPv4地址。 **说明** 负载均衡器的IP地址不受所在子网的网络ACL规则限制，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**。

参数	说明
后端子网	后端子网为独享型负载均衡提供私网IP地址，**用于与后端服务器进行通信和健康检查**。 ● 默认选项为“与前端子网保持一致”。 ● 支持您选择负载均衡器所属VPC下的其他子网，也支持您通过单击“添加子网”新建子网。 通过合理规划子网，可以避免因ELB实例占用IP地址数量超过预期而影响业务扩展的情况，详情请参考**独享型ELB子网规划的推荐方案**。 **说明** ● 若创建独享型负载均衡时指定的后端子网未开启IPv6，负载均衡实例创建后将不支持IPv6网络。 ● 负载均衡实例会占用后端子网中的部分IP地址与后端服务器进行通信，负载均衡实例的规格，可用区的数量和IP类型后端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。
IPv6地址	如果网络类型选择了“IPv6网络”，则需要选择IPv6的IP地址的分配方式。 ● **自动分配**：由系统自动分配IPv6地址。 ● **手动指定**：手动指定IPv6地址。 **说明** 负载均衡器的IP地址不受所在子网的网络ACL规则限制，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	如果网络类型选择了“IPv6网络”，支持选择IPv6的共享带宽。 共享带宽可以实现多个弹性公网IP共同使用一条带宽，提供区域级别的带宽共享及复用能力。 可以选择暂不设置共享带宽、选择已有的共享带宽或新建共享带宽。
IP类型后端	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。支持添加与ELB实例不同VPC的服务器IP地址，详情请参见**配置不同VPC的服务器作为后端服务器（IP类型后端）**。 开启IP类型后端，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。

5. 您可以为弹性负载均衡配置弹性公网IP满足IPv4公网业务诉求，配置详情见**表1-11**。

表 1-11 为负载均衡器配置弹性公网 IP

参数	说明
弹性公网IP	支持您为负载均衡器配置对应的弹性公网IP以处理IPv4公网业务流量。 • **现在购买**：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。 • **暂不购买**：您可在弹性负载均衡创建完成后根据实际需求进行弹性公网IP的绑定。 **说明** 如果您希望通过全域弹性公网IP处理公网业务流量，您可以在全域弹性公网IP控制台将全域弹性公网IP绑定至ELB实例，详情请参考**将全域弹性公网IP绑定至实例**。
线路	使用新创建弹性公网IP时，选择的弹性公网IP的线路类型。 • **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。适用于对网络稳定性和连通性有极高要求的关键业务，如金融交易、在线游戏、大型企业应用、视频直播等。 • **静态BGP**：成本低，便于自动调度，但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。适用于网络环境相对稳定，变动较少且自身应用系统具备容灾功能的业务场景。 • **优选BGP**：是特定方向的优质线路。使用BGP协议与多家主流运营商线路互联对接，建立直连中国内地的公网互联路径，提供中国-香港区域与中国内地间的低时延、高质量的网络互通。（该线路资源仅在“中国-香港”区域支持。） • **弹性公网IP池**：弹性公网IP池为EIP分配全动态BGP线路，持续保证网络稳定、高效。 更多静态BGP与全动态BGP区别信息请参见**静态BGP与全动态BGP有何区别?**
公网带宽	弹性公网IP使用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**：共享带宽提供区域级别的带宽复用共享能力，可帮助您节省公网带宽成本。
带宽大小	指定具体的公网带宽上限。

6. 弹性负载均衡的高级配置支持为实例设置描述和标签，配置详见**表1-12**。

表 1-12 负载均衡器的高级配置

参数	说明
高级配置 > 描述	单击 ，展开折叠的高级配置区域，可以设置该参数。 您可以根据需要在文本框中输入对该负载均衡器的描述信息。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。
高级配置 > 标签	单击 ，展开折叠的高级配置区域，可以设置该参数。 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1-13**。 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。
同步编辑关联资源标签	当您为ELB绑定了关联资源使用时，可以使用标签对这些资源统一进行管理。 您勾选的关联资源标签会随着弹性负载均衡标签同步编辑。 支持关联资源：弹性公网IP。 受关联资源服务自身标签的影响，同步效果可能会受影响，请以实际结果为准。

表 1-13 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。

7. 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。

8. 选择弹性负载均衡实例的购买数量。
9. 单击“立即购买”，完成创建。
10. 返回弹性负载均衡列表页面，即可查看新创建的实例。

    弹性负载实例创建完成后，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。

查看弹性负载均衡拓扑图

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要查看拓扑图的ELB名称。

   进入弹性负载均衡详情页。
3. 选择“概览”页签，查看弹性负载均衡的拓扑图。

   拓扑图直观地为您展示当前弹性负载均衡的监听器，以及监听器关联转发的后端服务器组。

   您还可以通过拓扑图提供功能，对监听器和后端服务器组快捷执行部分常见操作，具体说明如下:

   - 查看监听器的基本信息，添加/编辑转发策略。
   - 查看后端服务器组的基本信息，查看组内后端服务器的信息。
   - 查看异常后端服务器。

后续操作

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。

- 添加网络型监听器：**网络型监听器**
- 添加应用型监听器：**应用型监听器**
- 创建后端服务器组并添加后端服务器
  - **创建后端服务器组**
  - **配置相同VPC的服务器作为后端服务器**
  - **配置不同VPC的服务器作为后端服务器（IP类型后端）**

相关文档

- 了解概念：
  - 了解**什么是弹性负载均衡**。
  - 了解弹性负载均衡的功能，详见**弹性负载均衡功能对比**。
  - 了解如何规划弹性负载均衡，详见**独享型负载均衡器概述**。
- API操作：
  - **创建负载均衡器**
  - **计算预占IP**

高频问题

负载均衡器与后端服务器的可用区可以不一致吗?

可以，弹性负载均衡支持将客户端请求跨可用区分发。

创建负载均衡器后可以变更规格吗?

ELB实例创建后可以变更规格，详情请见**变更实例规格**。

创建独享型负载均衡器后为什么会占用子网 IP?

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

通过合理规划子网，可以避免因ELB实例占用IP地址数量超过预期而影响业务扩展的情况，详情请参考**独享型ELB子网规划的推荐方案**。

为什么 ELB 实例创建后，状态会显示“闲置扣费中”？

ELB实例**创建完成后开始计费**，计费详情请参考**计费项（独享型）**。

为了帮助您提升资源利用率，如果ELB实例超过7天未使用且满足以下任一条件时，ELB控制台会主动提示您的ELB实例状态为“闲置扣费中”：

- 实例处于已停止状态
- 实例未添加监听器
- 实例的监听器已全部停用
- 实例未绑定后端服务器

闲置的实例仍在收取费用，确认不再使用的实例建议释放以便节省您的成本。

1.3.3 配置独享型负载均衡器的保护模式

您可以对负载均衡器开启修改保护或删除保护功能，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。

- **删除保护**：开启删除保护，防止因误操作导致负载均衡器被删除。如果您需要删除负载均衡器，请确认关闭**删除保护**开关。
- **修改保护**：开启修改保护，防止因误操作导致负载均衡器的配置被修改。如果您需要修改负载均衡器的配置或删除负载均衡器，请确认关闭**修改保护**开关。

开启或关闭删除保护

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要配置删除保护的负载均衡器名称。
3. 切换到负载均衡实例的“基本信息”页签，开启或关闭“删除保护”开关。

⚠ 注意

如果您的负载均衡实例由云容器引擎服务（CCE）管理，修改负载均衡实例的配置将会影响集群的运行，请您谨慎操作。

4. 删除保护开启后，您将无法删除该负载均衡实例，其余操作不受影响。

开启或关闭修改保护

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要配置修改保护的负载均衡器名称。
3. 切换到负载均衡实例的“基本信息”页签，单击修改保护右侧的“设置”。
4. 在设置修改保护的弹窗中，开启或关闭“修改保护开关”。
   建议您填写“添加修改保护原因”。

   ⚠ 注意

   如果您的负载均衡实例由云容器引擎服务（CCE）管理，修改负载均衡实例的配置将会影响集群的运行，请您谨慎操作。
5. 单击“确定”。
6. 修改保护开启后，您将无法修改负载均衡实例的配置且无法删除该负载均衡实例，其余操作不受影响。

相关文档

- 控制台相关操作：
  - **变更独享型负载均衡器的基础配置**
  - **释放独享型负载均衡器**
- API操作：
  - **创建负载均衡器**
  - **更新负载均衡器**

1.3.4 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，随着业务的发展变化，可能会出现业务流量增长超出预期、业务类型调整、后端服务迁移等使用需求变化。弹性负载均衡支持您根据实际使用需求的变化，灵活调整实例规格和实例可用区等基础配置，帮助您优化业务架构。

变更实例规格

弹性规格的负载均衡实例相对于固定规格实例在扩缩容场景具有明显优势，如果您的业务具有明显的峰谷波动，您可以使用弹性规格实例简化管理，降低运维复杂度。

如果您使用固定规格的实例，当规格大小无法满足业务增长或业务流量低于预期时，您可以变更规格大小来保障业务安全和控制成本。如果您的业务类型发生变化，也支持您变更弹性负载均衡实例的规格类型。

您可通过控制台提供的“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。

  - 应用型实例：支持HTTP/HTTPS/QUIC监听器。
  - 网络型实例：支持TCP/UDP/TLS监听器。
- **负载均衡实例固定规格的规格大小**（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1-14**和**表1-15**。

警告

- 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：
  - （TCP/UDP/TLS）业务的部分新建连接会受影响。
  - （HTTP/HTTPS/QUIC）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 1-14 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 1-15 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，系统会根据新老规格配置差异补收或退还差价。
	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。

1. 进入**弹性负载均衡列表页面**。

2. 在弹性负载均衡列表页面，在目标负载均衡实例所在行“操作”列选择“更多 > 变更规格”。
3. 根据界面提示选择变更后的规格，单击“下一步”。

   如果您的负载均衡实例绑定了EIP，您可以单击“带宽详情”展开查看绑定的EIP。支持您单击目标EIP操作列的“修改带宽”前往修改弹性公网IP控制台修改EIP带宽以适应ELB的规格变化。
4. 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”。
5. 返回弹性负载均衡列表页面，您可在目标实例的“规格”列查看生效的新规格。

变更实例可用区

独享型负载均衡实例创建后，在如下典型的业务场景您可能需要变更ELB实例的可用区，您可以通过控制台提供的“变更可用区”变更负载均衡实例部署的可用区。

- **维护业务高可用性**：原可用区出现资源不足或故障风险时，您可以为ELB实例增加可用区，实现跨可用区容灾。
- **优化业务架构性能**：部署业务的后端服务器资源迁移至新的可用区时，您可以同步调整ELB实例的可用区，实现减少流量的跨可用区转发降低时延。

变更可用区完成后，流量会重新分配到变更后的可用区。

说明

变更可用区功能陆续上线中，请以控制台实际为准。

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表中，在目标负载均衡实例所在行“操作”列选择“更多 > 变更可用区”。
3. 根据界面提示选择变更后的可用区，单击“下一步”。
4. 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。

5. 返回弹性负载均衡列表页面，单击目标负载均衡实例名称，切换到“基本信息”页签可以查看已经生效的新可用区。

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。

相关文档

API操作：**更新负载均衡器**、**变更负载均衡器计费模式**、**新增负载均衡器可用区**、**移除负载均衡器可用区**。

1.3.5 变更独享型负载均衡器的网络配置

弹性负载均衡通过绑定的私网或公网IP地址与外部进行通信，这些IP地址承载了流量的转发。如果您的ELB实例当前绑定的IP地址因为业务架构升级、安全问题或者合规要求等需要变更，您可以参考本文进行操作。

网络类型

弹性负载均衡按照**支持的网络类型的**不同分为**公网负载均衡器**和**私网负载均衡器**。

- **公网负载均衡器**：您需要为ELB实例绑定EIP或者GEIP。负载均衡器接收公网的访问请求，然后向监听器绑定的后端服务器分发这些请求。
- **私网负载均衡器**：通过私有IP将来自私网的访问请求分发到后端服务器上，通常用于内部服务集群。

IP 版本

独享型负载均衡支持IPv4/IPv6双栈网络。

- **TCP和UDP协议通信**：
  - **默认情况**：
    - 客户端访问ELB的IPv4地址时只能与IPv4后端服务器通信。
    - 客户端访问ELB的IPv6地址时只能与IPv6后端服务器通信。
  - **监听器开启IPv4/IPv6地址转换**：无论客户端访问到ELB的IPv4还是IPv6地址，都可以和IPv4或IPv6后端服务器通信。
- **TLS/HTTP/HTTPS和QUIC协议通信**：客户端和ELB之间使用IPv4或IPv6网络通信时，ELB和后端服务器之间都使用IPv4网络通信。

说明

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

图 1-7 TCP 和 UDP 协议未开启 IPv4/IPv6 地址转换业务架构图

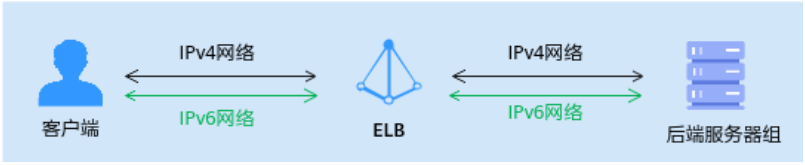


图 1-8 TCP 和 UDP 协议开启 IPv4/IPv6 地址转换业务架构图

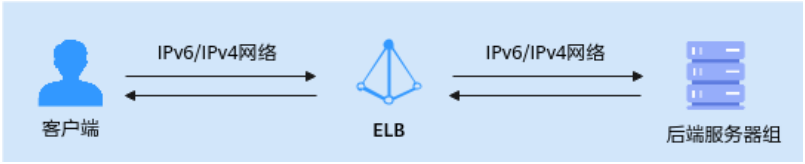
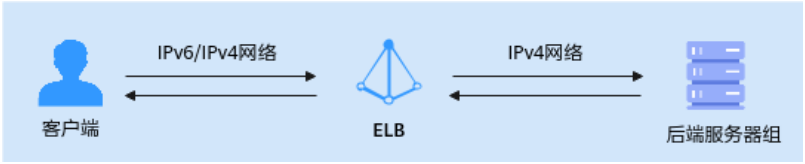


图 1-9 TLS/HTTP/HTTPS/QUIC 协议业务架构图



绑定/解绑定 IP 地址

可以根据业务实际需要为ELB实例绑定IP地址，或者将ELB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**。

如果您希望通过全域弹性公网IP处理公网业务流量，您可以在全域弹性公网IP控制台将弹性公网IP绑定至ELB实例，详情请参考**将全域弹性公网IP绑定至实例**。

注意

解绑IP地址后，弹性负载均衡将会无法使用对应的IP地址进行流量转发，请谨慎操作。

绑定/解绑 IPv4 公网 IP

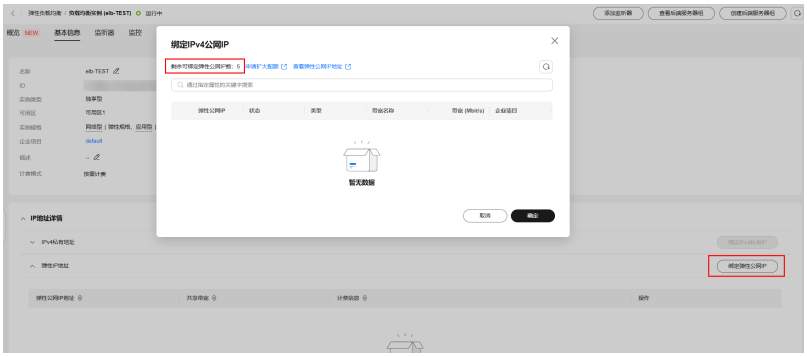
独享型ELB实例支持绑定多个弹性公网IP，单个ELB实例支持绑定EIP的数量详情见**查看您的配额**。

说明

- 独享型ELB实例支持绑定多个弹性公网IP功能陆续上线中。如果您有使用需求，可以提交**工单**进行申请。
- 如果您的实例出现提示“当前实例不支持绑定多弹性公网IP”，说明实例版本较低，可以提交**工单**申请升级该实例的版本。

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，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”。
      如果您需要继续为ELB实例绑定EIP，请进入ELB实例的“基本信息”页签，在弹性公网IP地址所在行单击“绑定弹性公网IP”进行绑定。

图 1-10 ELB 实例支持绑定多个弹性公网 IP



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. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，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. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，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. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，需修改负载均衡器所在行，单击“更多 > 修改IPv4私有IP”。
3. 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。
4. 单击“确定”。

修改 IPv6 地址

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，需修改负载均衡器所在行，单击“更多 > 修改IPv6地址”。
3. 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。
4. 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。

⚠ 注意

- 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. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡器列表页面，待修改带宽的负载均衡器所在行的“操作”列，单击“更多”。
3. 单击“修改IPv4带宽”或“ 修改IPv6带宽”。

4. 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。
5. 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. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，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。
3. 单击“确定”。

相关文档

- **ELB的IPv4/IPv6双栈实例可以切换到仅IPv4模式吗?**
- **API操作：更新负载均衡器**

1.3.6 导出独享型负载均衡器

操作场景

您可以将当前账号下拥有的弹性负载均衡信息，以Excel文件的形式导出至本地。

当前支持导出全部实例的基本信息、导出选中部分实例的基本信息，也支持导出选中实例的详细信息。

基本信息：包括负载均衡器的名称、ID、状态、实例类型、规格等信息。

详细信息：默认支持导出负载均衡器的基本信息和监听器的基本信息，额外支持导出监听器的转发策略、后端服务器组、后端服务器和证书（名称/ID）四项信息。

导出实例的基本信息

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡器列表左上方，单击“导出”。
   a. 选择“导出全部实例基本信息到XLSX”：系统会将当前区域内所有弹性负载均衡实例的基本信息自动导出为Excel文件，并下载至本地。
   b. 选择“导出已选中实例基本信息到XLSX”：系统会将当前区域内您所选中的弹性负载均衡实例的基本信息自动导出为Excel文件，并下载至本地。

导出实例的详细信息

如果您想备份弹性负载均衡实例关联监听器、后端服务器组、转发策略、后端服务器和使用证书等信息，您可以选择导出实例的详细信息。

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡器列表左上方，单击“导出”，选择“导出已选中实例详细信息到XLSX”。
3. 在“导出实例”弹窗页面，勾选导出项目。
   a. 默认支持导出负载均衡器的基本信息和监听器的基本信息。
   b. 支持勾选监听器的转发策略、后端服务器组、后端服务器和证书（名称/ID）四项信息。
      支持您勾选“全选”选项，导出实例的全部信息。
4. 单击“确定”，开始导出实例实例的详细信息。
5. 完成导出实例信息后，单击“确定”，关闭弹窗。

查看导出的实例信息

系统会将弹性负载均衡实例的信息自动导出为Excel文件，并下载至本地。

实例的基本信息：每一行数据对应一个弹性负载均衡实例的基本信息。

实例的详细信息：由于一个弹性负载均衡实例可能关联多个监听器和后端服务器组，一个弹性负载均衡实例的详细信息会对应多行数据。

1.3.7 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。

警告

- 当您主动释放ELB实例时，如果希望ELB可以保留一段时间，您可以使用回收站功能，防止因误删除/退订ELB造成业务损失。
- 如果您未启用回收站功能，请您确认数据完成备份或不再使用该资源，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

删除负载均衡器时，您可根据实际业务需求选择勾选如下：

- 释放负载均衡绑定的弹性公网IP，如不释放可能会被其他资源绑定继续计费。
- 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负载均衡实例关联使用，将无法执行删除）。

说明

支持批量删除负载均衡器的功能陆续上线中，已发布区域请以控制台实际为准。

删除单个按需计费的负载均衡器

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，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。
3. 您可根据实际业务需求选择勾选如下：
   - 释放负载均衡绑定的弹性公网IP，如不释放可能会被其他资源绑定继续计费。
   - 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负载均衡实例关联使用，将无法执行删除）。
4. 在删除确认对话框，输入“DELETE”。
5. 单击“确定”。

批量删除按需计费的负载均衡器

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，选择目标负载均衡器后，单击列表页上方的“更多>删除”。

   弹出删除弹性负载均衡器侧拉窗。
3. 您可根据实际业务需求选择勾选如下：
   - 释放负载均衡绑定的弹性公网IP，如不释放可能会被其他资源绑定继续计费。
   - 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负载均衡实例关联使用，将无法执行删除）。
4. 在删除确认对话框，输入“DELETE”。
5. 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。

退订单个包年/包月计费的负载均衡器

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，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。
3. 在退订确认对话框，输入“UNSUBSCRIBE”，单击“是”。
4. 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”。
5. 在弹窗中，确认退订信息，单击“退订”。

批量退订包年/包月计费的负载均衡器

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. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，选择目标负载均衡器后，单击列表页上方的“退订”。
3. 在退订确认对话框，输入“UNSUBSCRIBE”，单击“是”。
4. 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”。
5. 在弹窗中，确认退订信息，单击“退订”。

1.3.8 复制独享型负载均衡器

复制实例概述

实例复制将为您创建一个新的ELB，新ELB自身的属性、监听器、日志等配置与原ELB一致。

说明

弹性负载均衡支持复制功能陆续上线中，请以控制台实际为准。

约束与限制

- 复制实例的所属VPC与原实例保持一致。
- 原实例的公网配置将不会被复制，您可在复制完成后为新实例绑定弹性公网IP。
- 实例复制功能仅支持按需计费模式，实例复制完成后您可修改新实例的计费模式。

复制实例

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，在目标负载均衡器所在行的“操作”列，单击“复制”。

在“实例复制”弹窗，设置复制实例信息，详情见**表1-16**。

表 1-16 弹性负载均衡配置复制设置

参数	说明
新实例名称	复制后新独享型负载均衡实例的名称，支持修改。 默认格式：原实例名称-副本。
可用区	默认与原实例保持一致，支持修改。 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。 更多可用区规划请参考**规划实例可用区**。
计费模式	通过实例复制功能创建的新实例仅支持按需计费模式。
实例规格	默认与原实例保持一致，且不支持修改。
网络类型	实例私网类型与原实例保持一致，且不支持修改。 公网配置将不会被复制，您可在复制完成后为新实例绑定弹性公网IP。
前端子网	默认与原实例保持一致，支持修改。 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。
IPv4地址	选择ELB对外服务的IPv4地址，支持两种分配方式。 • 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。
IPv6地址	当原实例支持IPv6网络时，复制后的新实例默认支持IPv6网络。 自动分配IP地址：由系统自动分配IPv6地址。
后端子网	默认与原实例保持一致，支持修改。 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。 独享型负载均衡实例会占用后端子网中的部分IP地址，实际占用IP地址的数量以您在控制台复制实例时所占用的IP地址个数为准。 如果您为新实例的更换了后端子网，为确保新实例健康检查结果正常，请确保后端服务器的安全组和网络ACL规则放通ELB后端子网所属网段。
企业项目	创建弹性负载均衡时，需要将弹性负载均衡加入已有的企业项目内。 企业项目管理提供了一种按企业项目管理云资源的方式，帮助您实现以企业项目为基本单元的资源及人员的统一管理，默认项目为default。

参数	说明
后端服务器组	复制独享型负载均衡实例时支持复用或复制后端服务器组。 若您已开启企业项目管理，仅当复制后的新实例与原实例在同一企业项目时，支持复用或复制后端服务器组。 • 复用：新ELB实例将会直接使用原ELB实例的后端服务器组。 • 复制：系统将会根据原有配置创建新的后端服务器组，然后将其关联到新ELB实例使用。

3. 单击“确定”，进行实例复制。
   复制时间会受到负载均衡实际配置复杂度的影响，预计2分钟内完成。
4. 复制完成后，单击“关闭”，结束复制任务。

相关文档

- 变更独享型负载均衡器的基础配置
- 变更独享型负载均衡器的网络配置
- API操作：复制已有负载均衡器

1.3.9 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。

说明

弹性负载均衡支持启停功能陆续上线中，请以控制台实际为准。

启用或停用 ELB 实例

1. 进入弹性负载均衡列表页面。
2. 在弹性负载均衡列表页面，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”。
3. 单击“确定”。
4. 您可以通过弹性负载均衡列表页面的“状态”列，查看目标实例的启停状态。

注意

停用的负载均衡器仍会继续计费。

相关文档

- 更新负载均衡器
- 计费项（独享型）

1.3.10 独享型负载均衡器回收站

当您主动删除按需计费的ELB实例或主动退订未到期的包年/包月的ELB实例时，如果希望ELB可以保留一段时间，您可以使用回收站功能，防止因误删除/退订ELB造成的业务损失。

说明

独享型负载均衡支持回收站功能陆续上线中，请以控制台实际为准。

回收站策略

在使用ELB的回收站功能时，需要配置回收站策略。

回收站策略包括：

- **进入回收站实例的创建时长**：当您的ELB实例创建时间超过您设置的时长后，在实例被删除或退订时会进入回收站。
- **回收站内实例的保存时长**：ELB实例进入回收站的时间超过您设置的保存时长后，将自动销毁。

独享型ELB实例的后端服务器组可以关联到多个ELB实例下进行使用，后端服务器组不会随ELB实例进入回收站。

ELB实例从回收站进行恢复时，ELB实例及其下配置（监听器、转发策略和后端服务器组）将同时恢复。

绑定资源的处理策略

- 如果您的独享型ELB实例绑定了弹性公网IP（EIP），EIP的处理策略详情见**表1-17**。

表 1-17 绑定弹性 IP 的处理策略

ELB实例计费模式	操作	EIP是否删除	恢复ELB实例	销毁ELB实例
按需计费	删除ELB实例时，勾选“释放该负载均衡绑定的弹性公网IP”。	是	• EIP带宽独享 – 如果公网IP地址未被占用，EIP同步恢复并绑定至ELB。 – 如果公网IP地址已被占用，EIP无法恢复。 • EIP使用共享带宽 – 共享带宽存在：EIP同步恢复加入共享带宽并绑定至ELB。 – 共享带宽已删除：EIP无法恢复。	已删除
	删除ELB实例时，不勾选“释放该负载均衡绑定的弹性公网IP”。	否	如果EIP未被占用，将恢复与ELB的绑定关系。	已解绑，不会删除
包年/包月	退订ELB实例时，选择退订弹性公网IP。 **说明** 仅当您的EIP和ELB为同一订单购买时，支持同时退订EIP。	是	• EIP带宽独享 – 如果公网IP地址未被占用，EIP同步恢复并绑定至ELB。 – 如果公网IP地址已被占用，EIP无法恢复。 • EIP使用共享带宽 – 共享带宽存在：EIP同步恢复加入共享带宽并绑定至ELB。 – 共享带宽已删除：EIP无法恢复。	已删除
	退订ELB实例时，不退订弹性公网IP。	否	如果EIP未被占用，将恢复与ELB的绑定关系。	已解绑，不会删除

- 如果您的独享型ELB实例绑定了全域弹性公网IP（GEIP），删除/退订ELB实例时，GEIP会自动解除与ELB实例的绑定关系。ELB从回收站恢复时，无法恢复与GEIP的绑定关系。

回收站计费规则

- 回收站中的ELB实例将停用并停止计费。
- ELB实例绑定的资源（如云服务器、弹性公网IP），遵循对应资源的计费策略。
- 按需计费或包年/包月的ELB实例从回收站恢复后，都会转为按需计费实例。如果您需要包年/包月的实例，请及时变更计费模式。
- 回收站内的ELB实例，当账户欠费时会进入宽限期、保留期，受宽限期和保留期的影响，在未达到自定义保存时长时，ELB也可能会被系统提前删除。了解宽限期保留期的具体时长请参见**宽限保留期**。

约束与限制

- 在以下场景中，删除或退订的ELB不支持放入回收站。
  - 账号处于欠费、受限或冻结的异常状态。
  - ELB距离创建时间的天数小于配置的回收站策略天数。
  - ELB处于保留期或ELB保留期到期后被系统释放。
- ELB进入回收站后，会占用ELB的资源配额。

  当ELB配额不足时，请及时对回收站中的ELB进行清理。

开启回收站

1. 进入**弹性负载均衡列表页面**。
2. 选择ELB列表上方的“回收站”页签。
3. 在“回收站”页签下，单击“开启回收站”。
4. 在“回收站策略配置”弹窗中，确认回收站策略。
   a. 进入回收站实例的创建时长：当您的ELB实例创建时间超过您设置的时长后，在删除或退订时会进入回收站。
   b. 回收站内实例的保存时长：ELB实例进入回收站的时间超过您设置的保存时长后，将自动销毁。
5. 单击“确定”，回收站策略生效。

配置回收站策略

回收站功能开启后，您可以更改回收站策略以满足您最新的业务诉求。支持修改进入回收站实例的创建时长和回收站内实例的保存时长。

1. 进入**弹性负载均衡列表页面**。
2. 选择ELB列表上方的“回收站”页签。
3. 在“回收站”页签下，单击“策略配置”。
4. 在“回收站策略配置”弹窗中，修改回收站策略。
   a. 进入回收站实例的创建时长：当您的ELB实例创建时间超过您设置的时长后，在删除或退订时会进入回收站。
   b. 回收站内实例的保存时长：ELB实例进入回收站的时间超过您设置的保存时长后，将自动销毁。

5. 单击“确定”，新的回收站策略生效。

关闭回收站

如果您需要关闭回收站，请清空回收站内的ELB实例，您可以选择回复或销毁回收站内的ELB实例。

1. 进入**弹性负载均衡列表页面**。
2. 选择ELB列表上方的“回收站”页签。
3. 在“回收站”页签下，单击“关闭回收站”。
4. 在“关闭回收站”弹窗中，单击“确定”。

恢复回收站内的弹性负载均衡实例

如果您希望恢复使用回收站内的ELB实例，您可以对ELB实例执行恢复操作。

1. 进入**弹性负载均衡列表页面**。
2. 选择ELB列表上方的“回收站”页签。
3. 在“回收站”页签下，单击待恢复的ELB所在行的操作列下的“恢复”。
   进入“恢复弹性负载均衡实例”页面。
4. 单击“确定”，恢复回收站内的ELB实例
   - 恢复成功，您可以在弹性负载均衡列表中查看ELB实例，状态为“运行中”。
     ELB恢复的绑定资源可参考**绑定资源的处理策略**进行查看。
   - 若恢复失败，您仍可以在回收站中查看此ELB实例。

销毁回收站内的弹性负载均衡实例

如果在回收站内实例未达到的回收策略设置的保存时长时，您希望彻底删除回收站内的ELB实例，您可以对ELB实例执行销毁操作。

⚠ 注意

销毁ELB实例后不可恢复，请谨慎操作。

1. 进入**弹性负载均衡列表页面**。
2. 选择ELB列表上方的“回收站”页签。
3. 在“回收站”页签下，单击待恢复的ELB所在行的操作列下的“销毁”。
   进入“销毁弹性负载均衡实例”页面。
4. 单击“确定”，销毁回收站内的ELB实例。
   当ELB从“回收站”列表页消失时，表示销毁成功。

相关文档

API操作：**开关回收站**、**更新回收站的配置**、**还原负载均衡器**、**销毁回收站负载均衡器**。

1.3.11 关联服务

1.3.11.1 将 ELB 接入云模式 WAF 防护

如果您的业务服务器部署在云上，您可以使用将ELB接入云模式WAF的方式将网站的域名或IP添加到WAF进行防护。

已经使用了独享型ELB进行流量转发的网站，才支持使用“云模式-ELB接入”将网站接入WAF，该方式WAF是旁路检测，不参与流量转发。

说明

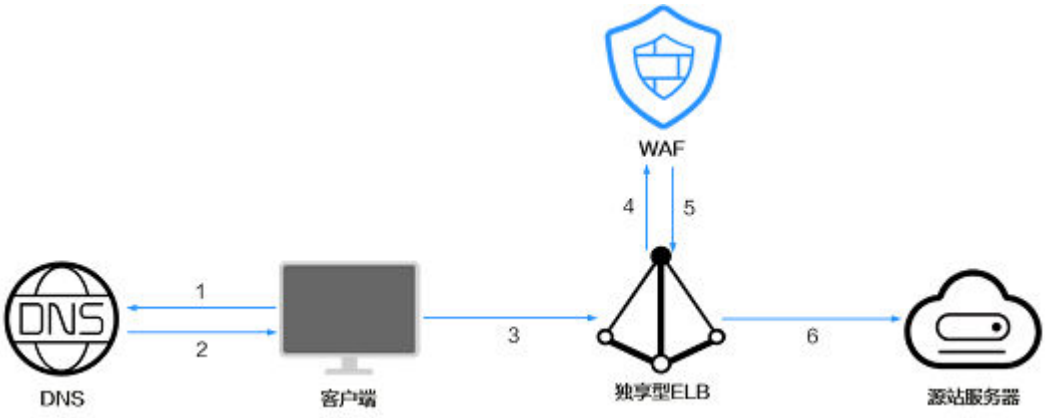
该功能陆续上线中，已发布区域请以控制台实际为准。

方案概述

ELB接入云模式WAF实例后，WAF通过SDK模块化的方式集成在ELB网关中。将网站接入WAF后，网站流量会被ELB镜像给WAF。WAF检测后，将结果同步给ELB，由ELB根据WAF检测结果决定是否将客户端请求转发到源站。该过程中，WAF不参与流量转发，避免因额外引入一层转发而带来各种兼容性和稳定性问题。

接入WAF后，网站访问示意图如**图1-11**所示，更多详情请见**将网站接入WAF防护（云模式-ELB接入）**。

图 1-11 网站访问示意图



前提条件

- 已**购买云模式的WAF实例**，并已了解**网站接入**的相关信息。

  说明

  云模式WAF的ELB接入方式需要**提交工单**申请开通后才能使用。

- 已购买应用型规格的独享型负载均衡并**添加HTTP监听器**或**添加HTTPS监听器**，防护网站对应的服务器已添加到该ELB监听器转发的后端服务组中，并确认ELB转发业务的连通性正常。

在 ELB 控制台接入云模式 WAF 实例

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要接入云模式WAF实例的负载均衡名称。
3. 切换到“关联服务”页签，单击“添加WAF策略配置”，为ELB配置WAF防护策略。

相关参数说明如表1-18所示。

表 1-18 基本信息参数说明

参数	参数说明	取值样例
防护域名	配置为您想防护的域名或IP（公网IP/私网IP），且该域名已解析到当前负载均衡器的弹性公网IP上。 域名：支持单域名和泛域名。 ● 单域名：输入防护的单域名。例如：www.example.com。 ● 泛域名 – 如果各子域名对应的服务器IP地址相同：输入防护的泛域名。例如：子域名a.example.com，b.example.com和c.example.com对应的服务器IP地址相同，可以直接添加泛域名*.example.com。 – 如果各子域名对应的服务器IP地址不相同：请将子域名按“单域名”方式逐条添加。 – WAF支持添加“*”的泛域名。 **说明** WAF支持防护公网IP、私网IP，如果配置为私网IP，必须确保相应的网络路径是可访问的，以便于WAF能够正确地对流量进行监控和过滤。	单域名：www.example.com 泛域名：*.example.com IP： XXX.XXX.1.1
监听器	选择防护的监听器。 ● “所有监听器” ● “指定监听器”	所有监听器
策略配置	默认为“系统自动生成策略”，您也可以选择已创建的防护策略或在域名接入后根据防护需求配置防护规则。 系统自动生成的策略说明如下： ● Web基础防护（“仅记录”模式、常规检测） 仅记录SQL注入、XSS跨站脚本、远程溢出攻击、文件包含、Bash漏洞攻击、远程命令执行、目录遍历、敏感文件访问、命令/代码注入等攻击行为。 ● 网站反爬虫（“仅记录”模式、扫描器） 仅记录漏洞扫描、病毒扫描等Web扫描任务，如OpenVAS、Nmap的爬虫行为。 **说明** ● “仅记录”模式：发现攻击行为后WAF只记录攻击事件不阻断攻击。 ● 只有专业版和铂金版支持选择自定义的防护策略。	系统自动生成策略

a. 单击“确定”，防护网站添加成功。
您可在WAF控制台防护网站列表中查看已添加防护网站。

相关文档

- 购买云模式的WAF实例
- 将网站接入WAF防护（云模式-ELB接入）
- 添加HTTP监听器
- 添加HTTPS监听器
- 添加QUIC监听器

1.4 监听器

1.4.1 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。

支持的监听协议和场景

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1-19。

对于网络型规格的负载均衡器，在创建监听器时，支持选择TCP、TLS或者UDP。

对于应用型规格的负载均衡器，在创建监听器时，支持选择HTTP、QUIC或者HTTPS。

表 1-19 监听协议类型说明

类型	协议	说明	适用场景
网络型	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。 • 对性能和并发规模无特别要求的Web应用。
网络型	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。

类型	协议	说明	适用场景
网络型	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。
应用型	HTTP	• 基于Cookie的会话保持。 • 使用X-Forward-For获取源地址。	适用于需要对数据内容进行识别的应用，如Web应用、移动游戏等。
应用型	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。	适用于需要加密传输的应用，如电子商务、金融服务等场景。
应用型	QUIC	• 基于UDP的快速互联网连接。 • 避免队头阻塞的多路复用。 • 改善拥塞控制。	适用于弱网络、网络频繁切换的业务场景。

说明

网络型号规格实例支持创建TLS监器，应用型规格实例支持创建QUIC监听器陆续上线中，请以控制台实际为准。

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、QUIC）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。

注意

前端协议和端口设置后不允许修改，如果您需要修改，请重新创建监听器。

表 1-20 前端协议和端口说明

前端协议	TCP、UDP、TLS、HTTP、HTTPS、QUIC
前端端口	在同一个负载均衡实例内，仅UDP/QUIC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。UDP协议和QUIC协议的前端端口也不能重复。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 1-21 后端协议和端口说明

后端协议	TCP、UDP、TLS、HTTP、HTTPS、QUIC、GRPC
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，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 1-12 四层监听器超时时间示意图

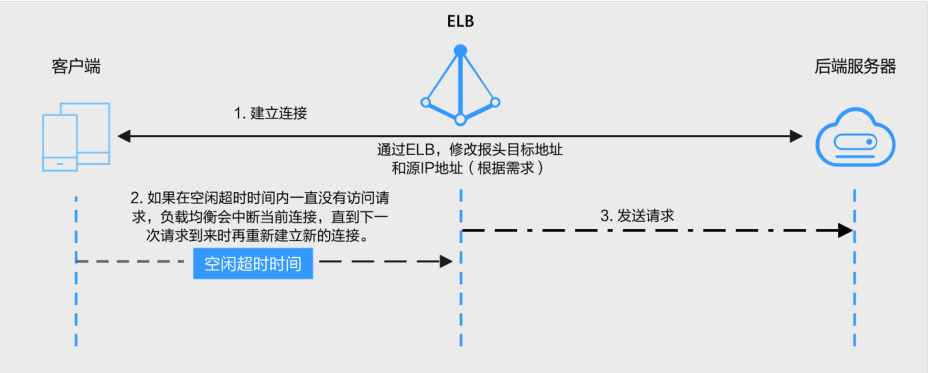


图 1-13 七层监听器超时时间示意图

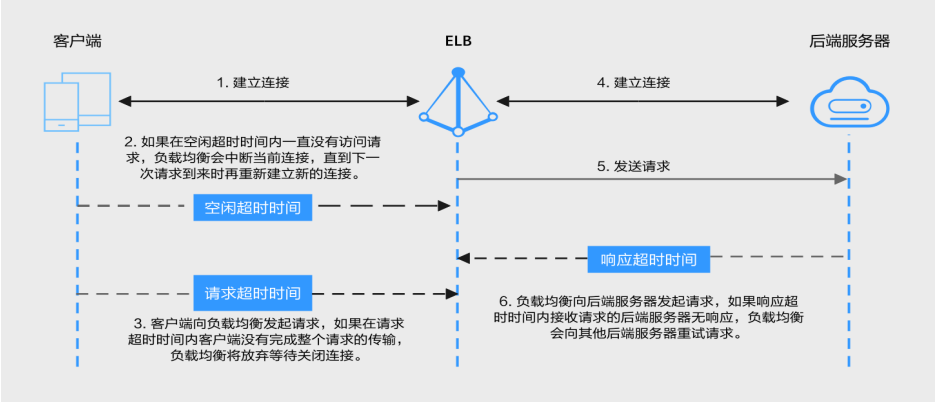


表 1-22 四层监听器超时时间

协议	类别	描述	取值范围	默认超时时间
• TCP • UDP • TLS	空闲超时时间	如果在空闲超时时间内一直没有访问请求，负载均衡会中断当前连接，直到下一次请求到来时再重新建立新的连接。	10~4000秒	300秒

表 1-23 七层监听器超时时间

协议	类别	描述	取值范围	默认超时时间
• HTTP • HTTPS • QUIC	空闲超时时间	如果在空闲超时时间内一直没有访问请求，负载均衡会中断当前连接，直到下一次请求到来时再重新建立新的连接。	0~4000秒	60秒
	请求超时时间	客户端向负载均衡发起请求，如果在请求超时时间内客户端没有完成整个请求的传输，负载均衡将放弃等待关闭连接。	1~300秒	60秒

协议	类别	描述	取值范围	默认超时时间
	响应超时时间	负载均衡向后端服务器发起请求，如果响应超时时间内接收请求的后端服务器无响应，负载均衡会向其他后端服务器重试请求。如果重试期间后端服务器一直没有响应，则负载均衡会给客户端返回HTTP 504错误码。 如果开启了会话保持功能，响应超时时间内对应的后端服务器无响应，负载均衡将不会发起重试请求，直接返回HTTP 504错误码。	1~300秒	60秒

1.4.2 网络型监听器

1.4.2.1 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，则无法创建TCP监听器。

添加 TCP 监听器

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要添加监听器的负载均衡名称。
3. 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1-24**。

表 1-24 独享型负载均衡配置 TCP 监听器参数说明

参数	说明
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。

参数	说明
监听端口	负载均衡器对外提供服务时接收请求的端口。 ● **单端口监听**：仅对设置的一个监听端口进行监听。 ● **全端口监听**：前端协议是TCP、UDP或TLS协议时，支持全端口监听。全端口监听可以对监听端口段内的所有端口进行监听，并将监听端口上接收到的请求转发到后端服务器的后端端口。 **说明** 全端口监听功能陆续上线中，已发布区域请以控制台实际为准。
名称（可选）	监听器名称。
IPv4/IPv6地址转换	当后端子网已开启IPv6时，弹性负载均衡支持IPv4和IPv6的网络地址转换。 仅TCP和UDP监听器支持此功能。 ● 此功能关闭时： – 客户端访问ELB的IPv4地址时只能与IPv4后端服务器通信。 – 客户端访问ELB的IPv6地址时只能与IPv6后端服务器通信。 ● 此功能开启时：无论客户端访问到ELB的IPv4还是IPv6地址，都可以和IPv4或IPv6后端服务器通信。 该功能开启后，不支持开启获取客户端IP功能，TCP监听器场景可以通过TOA插件获取客户源IP。 **警告** 开启或关闭此功能时，会造成已有的长连接断开。客户端连接请求重试后会恢复，建议您谨慎操作。 **说明** 该功能陆续上线中，已发布区域请以控制台实际为准。
获取客户端IP	独享型ELB默认支持“获取客户端IP”。 TCP监听器转发时，ELB实例与后端服务器之间直接使用客户端真实的IP地址通信，通过后端服务器的日志记录便可获取客户端的真实IP。 该功能在IP类型后端场景失效。开启IPv4/IPv6地址转换时，不支持该功能。您也可以通过TOA插件或ProxyProtocol获取客户端真实IP，详情请参考**独享型ELB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。 IP类型后端场景下，**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。 **警告** 请确保后端服务器具有解析ProxyProtocol协议的能力，否则会导致业务中断，请谨慎开启。 **说明** 该功能陆续上线中，已发布区域请以控制台实际为准。

参数	说明
访问控制	您可以使用ELB监听器的**访问控制**功能来**控制访问ELB监听器的IP地址**，更多信息请参见访问控制策略。 监听器的访问控制默认支持“**允许所有IP访问**”。 您可以为访问控制设置**白名单**或**黑名单**，并选择适用的IP地址组。 • **白名单**：只有白名单中的IP可以访问ELB的监听器。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。 • **黑名单**：黑名单中的IP禁止访问ELB的监听器。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。
更多设置（可选）	
空闲超时时间（秒）	如果在空闲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：10~4000。
每秒新建连接限速（每可用区）	默认不限速，支持选择“限速”并输入限速值。 限速值代表当前监听器下，负载均衡实例在每个可用区支持的每秒新建连接数上限。 取值范围：1~1,000,000。当限速值大于弹性负载均衡的实例规格时，以实例规格为上限。 **说明** 该功能陆续上线中，已发布区域请以控制台实际为准。
每秒并发连接限速（每可用区）	默认不限速，支持选择“限速”并输入限速值。 当前监听器下，负载均衡实例在每个可用区支持的每秒并发连接数上限。 取值范围：1~1,000,000。当限速值大于弹性负载均衡的实例规格时，以实例规格为上限。 降低并发连接限速，已建立连接不受影响。 **说明** 该功能陆续上线中，已发布区域请以控制台实际为准。
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（可选）	对于监听器描述。 字数范围：0/255。

4. 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1-51**。

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1-52**。

5. 单击“下一步：确认配置”。
6. 确认配置无误后，单击“提交”。

相关文档

- **通过IPv4/IPv6地址转换实现IPv6客户端访问IPv4业务**
- **通过ELB的全端口监听转发功能实现多端口转发**

1.4.2.2 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，则无法创建UDP监听器。
- 如果监听器关联到UDP协议的后端服务器组，流量路径经过云专线或VPN，并通过IP类型后端进行转发时，健康检查结果可能异常。如果您有此种应用场景，建议提交**工单**进行咨询。

添加 UDP 监听器

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要添加监听器的负载均衡名称。
3. 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1-25**。

表 1-25 独享型负载均衡配置 UDP 监听器参数说明

参数	说明
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。

参数	说明
监听端口	负载均衡器对外提供服务时接收请求的端口。 ● **单端口监听**：仅对设置的一个监听端口进行监听。 ● **全端口监听**：前端协议是TCP、UDP或TLS协议时，支持全端口监听。全端口监听可以对监听端口段内的所有端口进行监听，并将监听端口上接收到的请求转发到后端服务器的后端端口。
名称（可选）	监听器名称。
IPv4/IPv6地址转换	当后端子网已开启IPv6时，弹性负载均衡支持IPv4和IPv6的网络地址转换。 仅TCP和UDP监听器支持此功能。 ● 此功能关闭时： – 客户端访问ELB的IPv4地址时只能与IPv4后端服务器通信。 – 客户端访问ELB的IPv6地址时只能与IPv6后端服务器通信。 ● 此功能开启时：无论客户端访问到ELB的IPv4还是IPv6地址，都可以和IPv4或IPv6后端服务器通信。 该功能开启后，不支持开启获取客户端IP功能，TCP监听器场景可以通过TOA插件获取客户源IP。 **警告** 开启或关闭此功能时，会造成已有的长连接断开。客户端连接请求重试后会恢复，建议您谨慎操作。 **说明** 该功能陆续上线中，已发布区域请以控制台实际为准。
获取客户端IP	独享型ELB默认支持“获取客户端IP”。 UDP监听器转发时，ELB实例与后端服务器之间直接使用客户端真实的IP地址通信，通过后端服务器的日志记录便可获取客户端的真实IP。 该功能在IP类型后端场景失效。开启IPv4/IPv6地址转换时，不支持该功能。
访问控制	您可以使用ELB监听器的**访问控制**功能来**控制访问ELB监听器的IP地址**，更多信息请参见访问控制策略。 监听器的访问控制默认支持“**允许所有IP访问**”。 您可以为访问控制设置**白名单**或**黑名单**，并选择适用的IP地址组。 ● **白名单**：只有白名单中的IP可以访问ELB的监听器。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。 ● **黑名单**：黑名单中的IP禁止访问ELB的监听器。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。
更多设置（可选）	

参数	说明
空闲超时时间	如果在空闲超时时间内一直没有访问请求，负载均衡会中断当前连接，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
每秒新建连接限速（每可用区）	默认不限速，支持选择“限速”并输入限速值。 限速值代表当前监听器下，负载均衡实例在每个可用区支持的每秒新建连接数上限。 取值范围：1~1,000,000。当限速值大于弹性负载均衡的实例规格时，以实例规格为上限。 **说明** 该功能陆续上线中，已发布区域请以控制台实际为准。
每秒并发连接限速（每可用区）	默认不限速，支持选择“限速”并输入限速值。 限速值代表当前监听器下，负载均衡实例在每个可用区支持的每秒并发连接数上限。 取值范围：1~1,000,000。当限速值大于弹性负载均衡的实例规格时，以实例规格为上限。 降低并发连接限速，已建立连接不受影响。 **说明** 该功能陆续上线中，已发布区域请以控制台实际为准。
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（可选）	对于监听器描述。 字数范围：0/255。

4. 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1-51**。
      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1-52**。
5. 单击“下一步：确认配置”。
6. 确认配置无误后，单击“提交”。

相关文档

- **通过IPv4/IPv6地址转换实现IPv6客户端访问IPv4业务**
- **通过ELB的全端口监听转发功能实现多端口转发**

1.4.2.3 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。

约束与限制

- 独享型负载均衡器已经选择四层“网络型”类型的规格。
- QUIC协议的版本有：Q043、Q046、Q050。
- QUIC协议的UDP监听器不支持分片包。

添加后端为 QUIC 协议的 UDP 监听器

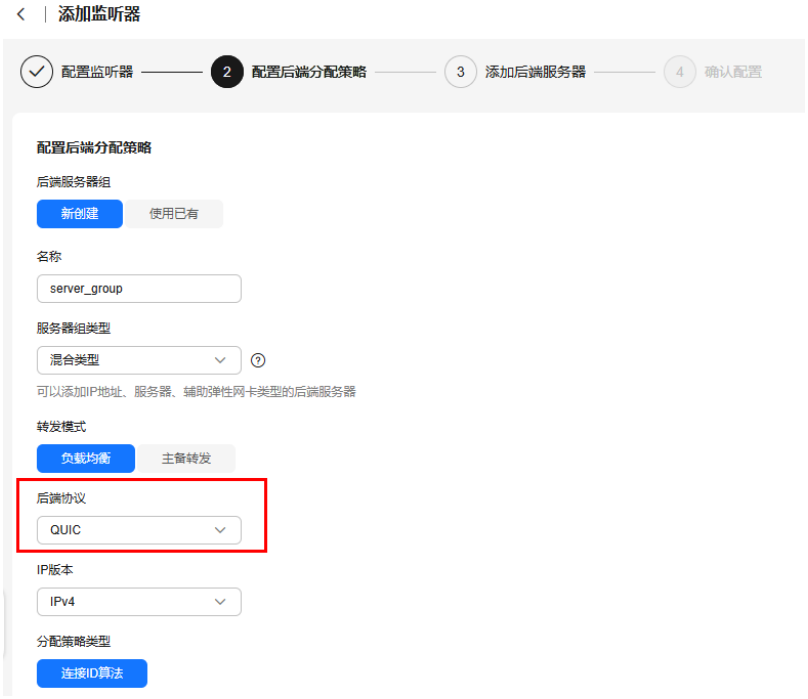
1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要添加监听器的负载均衡名称。

   此负载均衡器需要选择“网络型”规格。
3. 切换到“监听器”页签，单击“添加监听器”。
4. 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 1-14 前端协议选择“UDP”

5. 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 1-15 后端协议选择“QUIC”



6. 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**。

1.4.2.4 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，已发布区域请以控制台实际为准。

约束与限制

- 仅支持TLS新建连接数的网络型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. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要添加监听器的负载均衡名称。
3. 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1-26**。

表 1-26 独享型负载均衡配置 TLS 监听器参数说明

参数	说明
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。
监听端口	负载均衡器对外提供服务时接收请求的端口。 • **单端口监听**：仅对设置的一个监听端口进行监听。 • **全端口监听**：前端协议是TCP、UDP或TLS协议时，支持全端口监听。全端口监听可以对监听端口段内的所有端口进行监听，并将监听端口上接收到的请求转发到后端服务器的后端端口。
名称（可选）	监听器名称。
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。 **警告** 请确保后端服务器具有解析ProxyProtocol协议的能力，否则会导致业务中断，请谨慎开启。
访问控制	您可以使用ELB监听器的**访问控制**功能来**控制访问ELB监听器的IP地址**，更多信息请参见**访问控制策略**。 监听器的访问控制默认支持“**允许所有IP访问**”。 您可以为访问控制设置**白名单**或**黑名单**，并选择适用的IP地址组。 • **白名单**：只有白名单中的IP可以访问ELB的监听器。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。 • **黑名单**：黑名单中的IP禁止访问ELB的监听器。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。
证书配置	
SSL解析方式	请选择客户端到服务器端认证方式。 • **单向认证**：仅客户端对服务器端的身份进行认证。 • **双向认证**：客户端对服务器端的身份进行认证，服务器端也需要对客户端的身份进行认证。
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。在进行双向认证时，只有当客户端能够出具指定CA签发的证书，HTTPS连接才能成功。

参数	说明
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。
SNI	SNI（Server Name Indication 服务器名称指示）是一种TLS协议的扩展，用于解决在一个监听器托管多个域名时，需要根据不同的请求域名匹配证书进行认证的问题。 客户端在发起SSL握手请求时提交请求的域名信息，ELB在收到请求后，会根据请求的域名查找证书。 如果能够找到请求域名对应的SNI证书，则使用该证书进行认证。 如果没有找到请求域名对应的SNI证书，则使用**服务器证书**进行认证。 详情请参见**开启SNI证书实现多域名访问**。
SNI证书	开启SNI之后，您需要为监听器配置至少一个SNI证书。 只能选择指定了**SNI扩展域名**的服务器证书。
更多配置（可选）	
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）	如果在空闲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]。
每秒新建连接限速（每可用区）	默认不限速，支持选择“限速”并输入限速值。 限速值代表当前监听器下，负载均衡实例在每个可用区支持的每秒新建连接数上限。 取值范围：1~1,000,000。当限速值大于弹性负载均衡的实例规格时，以实例规格为上限。 **说明** 该功能陆续上线中，已发布区域请以控制台实际为准。
每秒并发连接限速（每可用区）	默认不限速，支持选择“限速”并输入限速值。 限速值代表当前监听器下，负载均衡实例在每个可用区支持的每秒并发连接数上限。 取值范围：1~1,000,000。当限速值大于弹性负载均衡的实例规格时，以实例规格为上限。 降低并发连接限速，已建立连接不受影响。 **说明** 该功能陆续上线中，已发布区域请以控制台实际为准。
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。

参数	说明
描述	对于监听器描述。 字数范围：0/255。

4. 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1-51**。
      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1-52**。
5. 单击“下一步：确认配置”。
6. 确认配置无误后，单击“提交”。

相关文档

- **通过独享型ELB实现TLS卸载（单向认证）**
- **通过独享型ELB实现TLS卸载（双向认证）**
- **在四层独享型ELB转发下获取客户端真实IP**

高频问题

TLS 监听转发在大并发场景有限制吗?

由于使用TLS监听器进行转发，会涉及FULLNAT转换，可能触发TCP五元组分配不足的问题。建议您使用TLS监听器转发时，您单台后端服务器的并发连接数不超过20万。如果超过该推荐值，可能导致五元组端口号分配不足，影响您业务的正常运行。

1.4.3 应用型监听器

1.4.3.1 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

- HTTP监听器仅支持添加后端协议为HTTP的后端服务器组。
- 如果您的独享型负载均衡实例类型为网络型，则无法创建HTTP监听器。

添加 HTTP 监听器

1. 进入**弹性负载均衡列表页面**。

2. 在弹性负载均衡列表页面，单击需要添加监听器的负载均衡名称。
3. 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1-27**。

表 1-27 独享型负载均衡配置 HTTP 监听器参数说明

参数	说明
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。
监听端口	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]。
名称（可选）	监听器名称。
重定向至监听器	将HTTP监听器接受的请求转发至HTTPS监听器，可以加密通信过程，增强业务的安全性。 例如：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。实际业务转发将以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。 HTTP监听器被重定向后，会返回301返回码。
获取客户端IP	独享型ELB默认支持“获取客户端IP”。 HTTP监听器转发时，支持通过X-Forwarded-For字段传递客户端的真实IP，X-Forwarded-For字段记录的第一个IP地址即为客户端真实IP。 更多详情请参考**独享型ELB获取客户端真实IP**。
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，便于灵活地分流业务，合理地分配资源。 更多信息请参见**高级转发策略概述**。
访问控制	您可以使用ELB监听器的**访问控制**功能来**控制访问ELB监听器的IP地址，**更多信息请参见**访问控制策略**。 监听器的访问控制默认支持“**允许所有IP访问**”。 您可以为监听器的访问控制设置**白名单**或**黑名单**，并选择适用的IP地址组。 • **白名单**：只有白名单中的IP可以访问ELB的监听器。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。 • **黑名单**：黑名单中的IP禁止访问ELB的监听器。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。
更多设置（可选）	

参数	说明
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和Gzip支持压缩的类型如下： text/html 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，已发布区域请以控制台实际为准。
后端建连失败重调度	开启此开关，当ELB与后端服务器因连接错误或请求超时导致建连失败时，ELB会向后端服务器组内的其他后端服务器发起重试。 最多重试4次，若均失败，则返回502或504错误码。 ● 连接错误：ELB在连接后端服务器时发生错误 ，如无法连接、拒绝连接等，返回502错误码。 ● 请求超时：后端服务器没有响应，返回504错误码。 – 连接超时：ELB尝试与后端服务器建立连接，但在超时时间内没有成功。 – 等待响应超时：ELB已发送请求到后端服务器，但在超时时间内没有及时收到响应。 注意：对于非幂等性请求方法的请求，例如POST、PATCH和DELETE，如果ELB已经将请求转发到后端服务器之后发生了错误，则不会重试。 **说明** 该功能陆续上线中，已发布区域请以控制台实际为准。
空闲超时时间（秒）	如果在空闲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，如果在请求超时时间内客户端没有完成整个请求的传输，负载均衡将放弃等待关闭连接。 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，如果响应超时时间内接收请求的后端服务器无响应，负载均衡会向其他后端服务器重试请求。如果重试期间后端服务器一直没有响应，则负载均衡会给客户端返回HTTP 504错误码。 如果开启了会话保持功能，响应超时时间内对应的后端服务器无响应，负载均衡将不会发起重试请求，直接返回HTTP 504错误码。 时间取值范围[1-300]。

参数	说明
每秒新建连接限速（每可用区）	默认不限速，支持选择“限速”并输入限速值。 限速值代表当前监听器下，负载均衡实例在每个可用区支持的每秒新建连接数上限。 取值范围：1~1000000。当限速值大于弹性负载均衡的实例规格时，以实例规格为上限。 **说明** 该功能陆续上线中，已发布区域请以控制台实际为准。
每秒并发连接限速（每可用区）	默认不限速，支持选择“限速”并输入限速值。 限速值代表当前监听器下，负载均衡实例在每个可用区支持的每秒并发连接数上限。 取值范围：1~1000000。当限速值大于弹性负载均衡的实例规格时，以实例规格为上限。 降低并发连接限速，已建立连接不受影响。 **说明** 该功能陆续上线中，已发布区域请以控制台实际为准。
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。 **说明** 该功能陆续上线中，已发布区域请以控制台实际为准。
描述	对于监听器描述。 字数范围：0/255。
附加HTTP头字段	根据您的业务需求，您可以选择添加的HTTP头字段。 • **客户端访问信息**： – 通过重写X-Real-IP字段获取客户端的源IP地址。 – 通过重写X-Forwarded-For-Port字段获取客户端的端口。 – 通过重写X-Forwarded-Host字段获取客户端的域名。 • **负载均衡器信息**： – 通过重写X-Forwarded-Proto字段获取访问负载均衡实例的监听器的协议。 – 通过重写X-Forwarded-ELB-IP字段获取负载均衡实例的公网IP地址。 – 通过重写X-Forwarded-Port字段获取负载均衡实例的监听端口。 – 通过重写X-Forwarded-ELB-ID字段获取访问的负载均衡实例的ID。 更多详情请参考**配置附加HTTP头字段**。 **说明** 支持附加HTTP头字段功能陆续上线中，已发布区域请以控制台实际为准。

4. 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1-51**。
      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1-52**。
5. 单击“下一步：确认配置”。
6. 确认配置无误后，单击“提交”。

高频问题

HTTP 监听转发在大并发场景有限制吗?

由于使用HTTP监听器进行转发，会涉及FULLNAT转换，在Websocket场景可能触发TCP五元组分配不足的问题。建议您使用HTTP监听器转发时，您单台后端服务器的并发连接数不超过20万。如果超过该推荐值，可能导致五元组端口号分配不足，影响您业务的正常运行。

1.4.3.2 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。

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

- HTTPS监听器仅支持添加后端协议为HTTP/HTTPS/GRPC的后端服务器组。
- 如果您的独享型负载均衡实例为网络型，则无法创建HTTPS监听器。
- 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。

添加 HTTPS 监听器

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要添加监听器的负载均衡名称。
3. 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1-28**。

表 1-28 独享型负载均衡配置 HTTPS 监听器参数说明

参数	说明
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。
监听端口	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]。
名称（可选）	监听器名称。
升级至QUIC	当您创建HTTPS监听器时，可以选择“升级至QUIC”，HTTPS可以协商升级到QUIC以降低时延和提升通信性能，尤其在弱网环境和高延迟的业务场景。
获取客户端IP	独享型ELB默认支持“获取客户端IP”。 HTTPS监听器转发时，支持通过X-Forwarded-For字段传递客户端的真实IP，X-Forwarded-For字段记录的第一个IP地址即为客户端真实IP。 更多详情请参考**独享型ELB获取客户端真实IP**。
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，便于灵活地分流业务，合理地分配资源。 更多信息请参见**高级转发策略概述**。
访问控制	您可以使用ELB监听器的**访问控制**功能来**控制访问ELB监听器的IP地址**，更多信息请参见**访问控制策略**。 监听器的访问控制默认支持“**允许所有IP访问**”。 您可以为监听器的访问控制设置**白名单**或**黑名单**，并选择适用的IP地址组。 • **白名单**：只有白名单中的IP可以访问ELB的监听器。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。 • **黑名单**：黑名单中的IP禁止访问ELB的监听器。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。
证书配置	
SSL解析方式	请选择客户端到服务器端认证方式。 • **单向认证**：仅客户端对服务器端的身份进行认证。 • **双向认证**：客户端对服务器端的身份进行认证，服务器端也需要对客户端的身份进行认证。
CA证书	协议类型为HTTPS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。在进行双向认证时，只有当客户端能够出具指定CA签发的证书，HTTPS连接才能成功。

参数	说明
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。
SNI	SNI（Server Name Indication 服务器名称指示）是一种TLS协议的扩展，用于解决在一个监听器托管多个域名时，需要根据不同的请求域名匹配证书进行认证的问题。 客户端在发起SSL握手请求时提交请求的域名信息，ELB在收到请求后，会根据请求的域名查找证书。 如果能够找到请求域名对应的SNI证书，则使用该证书进行认证。 如果没有找到请求域名对应的SNI证书，则使用**服务器证书**进行认证。 详情请参见**开启SNI证书实现多域名访问**。
SNI证书	开启SNI之后，您需要为监听器配置至少一个SNI证书。 只能选择指定了**SNI扩展域名**的服务器证书。 详情请参见**开启SNI证书实现多域名访问**。
更多配置（可选）	
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**。
0-RTT	0-RTT数据传输，有助于减少请求响应时间。 仅当安全策略支持TLS 1.3版本的协议，支持开启0-RTT数据传输。 开启有重放攻击的安全风险，请谨慎开启。 **说明** 该功能陆续上线中，已发布区域请以控制台实际为准。
HTTP/2	协议类型为HTTPS时，可选择是否支持HTTP/2。 更多详情请参见**开启HTTP/2提升通信效率**。
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和Gzip支持压缩的类型：text/html 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，已发布区域请以控制台实际为准。

参数	说明
后端建连失败重调度	开启此开关，当ELB与后端服务器因连接错误或请求超时导致建连失败时，ELB会向后端服务器组内的其他后端服务器发起重试。 最多重试4次，若均失败，则返回502或504错误码。 ● 连接错误：ELB在连接后端服务器时发生错误 ，如无法连接、拒绝连接等，返回502错误码。 ● 请求超时：后端服务器没有响应，返回504错误码。 – 连接超时：ELB尝试与后端服务器建立连接，但在超时时间内没有成功。 – 等待响应超时：ELB已发送请求到后端服务器，但在超时时间内没有及时收到响应。 注意：对于非幂等性请求方法的请求，例如POST、PATCH和DELETE，如果ELB已经将请求转发到后端服务器之后发生了错误，则不会重试。 **说明** 该功能陆续上线中，已发布区域请以控制台实际为准。
空闲超时时间（秒）	如果在空闲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，如果在请求超时时间内客户端没有完成整个请求的传输，负载均衡将放弃等待关闭连接。 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，如果响应超时时间内接收请求的后端服务器无响应，负载均衡会向其他后端服务器重试请求。如果重试期间后端服务器一直没有响应，则负载均衡会给客户端返回HTTP 504错误码。 如果开启了会话保持功能，响应超时时间内对应的后端服务器无响应，负载均衡将不会发起重试请求，直接返回HTTP 504错误码。 时间取值范围[1-300]。
每秒新建连接限速（每可用区）	默认不限速，支持选择“限速”并输入限速值。 限速值代表当前监听器下，负载均衡实例在每个可用区支持的每秒新建连接数上限。 取值范围：1~1,000,000。当限速值大于弹性负载均衡的实例规格时，以实例规格为上限。 **说明** 该功能陆续上线中，已发布区域请以控制台实际为准。

参数	说明
每秒并发连接限速（每可用区）	默认不限速，支持选择“限速”并输入限速值。 限速值代表当前监听器下，负载均衡实例在每个可用区支持的每秒并发连接数上限。 取值范围：1~1,000,000。当限速值大于弹性负载均衡的实例规格时，以实例规格为上限。 降低并发连接限速，已建立连接不受影响。 **说明** 该功能陆续上线中，已发布区域请以控制台实际为准。
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。 **说明** 该功能陆续上线中，已发布区域请以控制台实际为准。
描述	对于监听器描述。 字数范围：0/255。
附加HTTP头字段	根据您的业务需求，您可以选择添加的HTTP头字段。 • **客户端访问信息**： – 通过重写X-Real-IP字段获取客户端的源IP地址。 – 通过重写X-Forwarded-For-Port字段获取客户端的端口。 – 通过重写X-Forwarded-Host字段获取客户端的域名。 • **负载均衡器信息**： – 通过重写X-Forwarded-Proto字段获取访问负载均衡实例的监听器的协议。 – 通过重写X-Forwarded-ELB-IP字段获取负载均衡实例的公网IP地址。 – 通过重写X-Forwarded-Port字段获取负载均衡实例的监听端口。 – 通过重写X-Forwarded-ELB-ID字段获取访问的负载均衡实例的ID。 更多详情请参考**配置附加HTTP头字段**。 **说明** 支持附加HTTP头字段功能陆续上线中，已发布区域请以控制台实际为准。

4. 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1-51**。
      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1-52**。

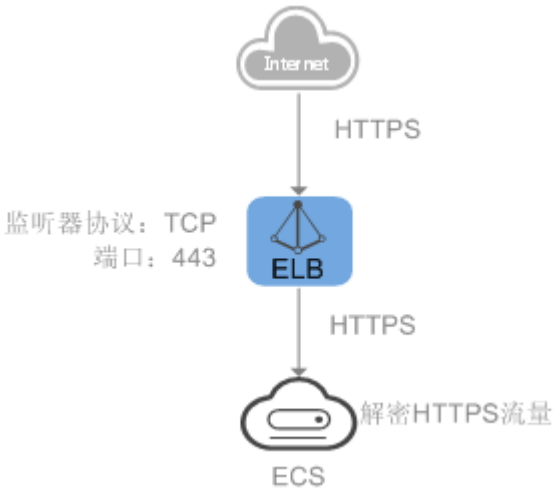
5. 单击“下一步：确认配置”。
6. 确认配置无误后，单击“提交”。

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 1-16 TCP 透传 HTTPS 流量



高频问题

HTTPS 监听转发在大并发场景有限制吗?

由于使用HTTPS监听器进行转发，会涉及FULLNAT转换，在Websocket场景可能触发TCP五元组分配不足的问题。建议您使用HTTPS监听器转发时，您单台后端服务器的并发连接数不超过20万。如果超过该推荐值，可能导致五元组端口号分配不足，影响您业务的正常运行。

1.4.3.3 添加 QUIC 监听器

操作场景

QUIC协议是基于UDP的快速互联网连接协议，改善拥塞控制，不依赖内核协议支持，用户使用具有更高的灵活性。

QUIC协议具备低时延、避免队头阻塞的多路复用优势，极佳的弱网性能可以有效解决网络、视频卡顿的问题，提升网络使用体验，同时保障数据传输的安全性。

约束与限制

- 仅支持应用型负载均衡实例可以创建QUIC监听器。

  说明

  应用型规格实例支持创建QUIC监听器功能陆续上线中，请以控制台实际为准。
- QUIC监听器仅支持添加后端协议为HTTP/HTTPS的后端服务器组。
- QUIC监听器关联的后端服务器组流量分配策略不支持源IP算法。
- 仅支持IQUIC，即HTTP/3，支持的版本为h3。
- QUIC监听器不支持添加以下HTTP头字段：
  - X-Forwarded-For-Port：通过重写X-Forwarded-For-Port字段获取客户端的端口。
  - X-Real-IP：通过重写X-Real-IP字段获取客户端的源IP地址。
- QUIC监听器不支持基于网段的转发策略。

添加 QUIC 监听器

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要添加监听器的负载均衡名称。
3. 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1-29**。

表 1-29 独享型负载均衡配置 QUIC 监听器参数说明

参数	说明
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QUIC。
监听端口	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]。
名称（可选）	监听器名称。
获取客户端IP	独享型ELB默认支持“获取客户端IP”。 QUIC监听器转发时，支持通过X-Forwarded-For字段传递客户端的真实IP，X-Forwarded-For字段记录的第一个IP地址即为客户端真实IP。 更多详情请参考**独享型ELB获取客户端真实IP**。
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，便于灵活地分流业务，合理地分配资源。 更多信息请参见**高级转发策略概述**。

参数	说明
访问控制	您可以使用ELB监听器的**访问控制**功能来**控制访问ELB监听器的IP地址**，更多信息请参见**访问控制策略**。 监听器的访问控制默认支持“**允许所有IP访问**”。 您可以为监听器的访问控制设置**白名单**或**黑名单**，并选择适用的IP地址组。 • **白名单**：只有白名单中的IP可以访问ELB的监听器。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。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。
证书配置	
服务器证书	QUIC监听器默认SSL解析方式为“单向认证”，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**。
SNI	SNI（Server Name Indication 服务器名称指示）是一种TLS协议的扩展，用于解决在一个监听器托管多个域名时，需要根据不同的请求域名匹配证书进行认证的问题。 客户端在发起SSL握手请求时提交请求的域名信息，ELB在收到请求后，会根据请求的域名查找证书。 如果能够找到请求域名对应的SNI证书，则使用该证书进行认证。 如果没有找到请求域名对应的SNI证书，则使用**服务器证书**进行认证。 详情请参见**开启SNI证书实现多域名访问**。
SNI证书	开启SNI之后，您需要为监听器配置至少一个SNI证书。 只能选择指定了**SNI扩展域名**的服务器证书。
更多配置（可选）	

参数	说明
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，已发布区域请以控制台实际为准。
后端建连失败重调度	开启此开关，当ELB与后端服务器因连接错误或请求超时导致建连失败时，ELB会向后端服务器组内的其他后端服务器发起重试。 最多重试4次，若均失败，则返回502或504错误码。 ● 连接错误：ELB在连接后端服务器时发生错误 ，如无法连接、拒绝连接等，返回502错误码。 ● 请求超时：后端服务器没有响应，返回504错误码。 – 连接超时：ELB尝试与后端服务器建立连接，但在超时时间内没有成功。 – 等待响应超时：ELB已发送请求到后端服务器，但在超时时间内没有及时收到响应。 注意：对于非幂等性请求方法的请求，例如POST、PATCH和DELETE，如果ELB已经将请求转发到后端服务器之后发生了错误，则不会重试。 **说明** 该功能陆续上线中，已发布区域请以控制台实际为准。

参数	说明
超时时间	弹性负载均衡支持配置监听器的超时时间，方便用户根据自身业务情况，自定义调整超时时间。 ● 空闲超时时间（秒） 如果在空闲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，如果在请求超时时间内客户端没有完成整个请求的传输，负载均衡将放弃等待关闭连接。 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，如果响应超时时间内接收请求的后端服务器无响应，负载均衡会向其他后端服务器重试请求。如果重试期间后端服务器一直没有响应，则负载均衡会给客户端返回HTTP 504错误码。 如果开启了会话保持功能，响应超时时间内对应的后端服务器无响应，负载均衡将不会发起重试请求，直接返回HTTP 504错误码。 时间取值范围[1-300]。
每秒新建连接限速（每可用区）	默认不限速，支持选择“限速”并输入限速值。 限速值代表当前监听器下，负载均衡实例在每个可用区支持的每秒新建连接数上限。 取值范围：1~1000000。当限速值大于弹性负载均衡的实例规格时，以实例规格为上限。 **说明** 该功能陆续上线中，已发布区域请以控制台实际为准。
每秒并发连接限速（每可用区）	默认不限速，支持选择“限速”并输入限速值。 限速值代表当前监听器下，负载均衡实例在每个可用区支持的每秒并发连接数上限。 取值范围：1~1000000。当限速值大于弹性负载均衡的实例规格时，以实例规格为上限。 如果降低并发连接限速，已建立连接不受影响。 **说明** 该功能陆续上线中，已发布区域请以控制台实际为准。
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。 **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。

参数	说明
描述	对于监听器描述。 字数范围：0/255。
附加HTTP头字段	根据您的业务需求，您可以选择添加的HTTP头字段。 • **客户端访问信息**： – 通过重写X-Forwarded-Host字段获取客户端的域名。 • **负载均衡器信息**： – 通过重写X-Forwarded-Proto字段获取访问负载均衡实例的监听器的协议。 – 通过重写X-Forwarded-ELB-IP字段获取负载均衡实例的公网IP地址。 – 通过重写X-Forwarded-Port字段获取负载均衡实例的监听端口。 – 通过重写X-Forwarded-ELB-ID字段获取访问的负载均衡实例的ID。 更多详情请参考**配置附加HTTP头字段**。 **说明** 支持附加HTTP头字段功能陆续上线中，已发布区域请以控制台实际为准。

4. 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1-51**。
      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1-52**。
5. 单击“下一步：确认配置”。
6. 确认配置无误后，单击“提交”。

1.4.3.4 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路径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1-30**。

表 1-30 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、路径。	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、路径、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、写入Header、删除Header、限速。

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）。
  - 一条转发策略的转发规则中添加了域名和路径时，请求需同时满足域名和路径的条件，才能匹配到该条转发策略。
- 独享型负载均衡器未开启“高级转发策略”时的匹配优先级如下：
  - 当请求同时满足转发动作分别为域名和路径的两条转发策略时，优先按照域名进行匹配，如**表1-31**。
  - 不同域名间优先级互相独立。
  - 转发规则为路径时，匹配优先级如下：精确匹配 > 前缀匹配 > 正则匹配，匹配类型相同时路径长度越长，优先级越高。

表 1-31 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	路径	/test
	2	域名	www.elb.com

说明

如**表1-31**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：
  - 转发规则支持路径，不支持查询字符串。如果您的路径设置为/path/resource?name=value，该条转发策略将失效。
  - 每个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“路径匹配规则”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. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要添加转发策略的负载均衡器名称。
3. 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。
4. 单击“添加转发策略”按钮。参考**表1-32**配置参数。

表 1-32 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。 域名或者路径至少要指定一个。	www.test.com
	路径	• 匹配说明 触发转发的路径。路径由英文字母、数字和特殊字符_~';@^-%#$.*+?,=!:|\/()[]{}组成。 • 匹配方式 – 精确匹配：请求的路径和设定路径完全一致，只能由/开头。 – 前缀匹配：请求的路径匹配已设定路径的开头，只能由/开头。 – 正则匹配：请求的路径和设定的路径正则表达式匹配。	/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。	-

参数	类型	说明	样例
	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。	-

5. 配置完成，单击“保存”。

1.4.3.5 高级转发策略

1.4.3.5.1 高级转发策略概述

当您使用弹性负载均衡负载七层业务时，基于不同的客户端请求会有不同的流量分发处理需求。弹性负载均衡支持配置高级转发策略，支持您根据客户端请求的特征来更精细地控制流量分发。

高级转发策略简介

高级转发策略支持多样化的转发规则和转发动作，便于灵活地分流业务，合理地分配资源。

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 每个客户端请求根据转发策略进行匹配，匹配到多条转发策略时基于**转发策略的优先级**顺序进行转发。

步骤3 ELB根据匹配上的转发策略的转发动作，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

图 1-17 高级转发策略（独享型）示意图

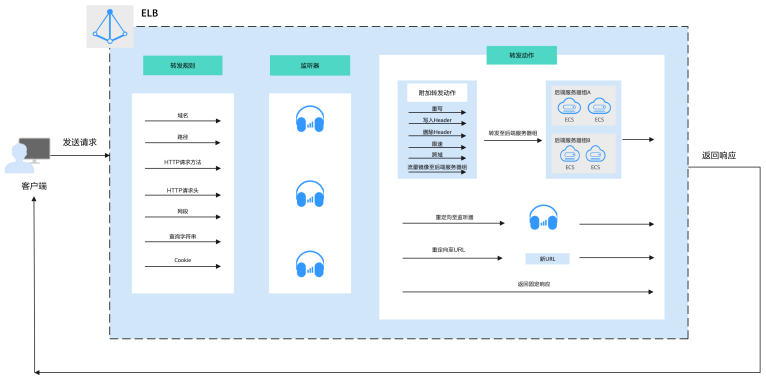


表 1-33 高级转发策略支持的转发规则与动作

转发策略设置	描述
转发规则	域名、路径、HTTP请求方法、HTTP请求头、查询字符串、网段、Cookie。 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、写入Header、删除Header、重写、限速、跨域、流量镜像至后端服务器组。 ● 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/写入Header/删除Header/限速/跨域/流量镜像至后端服务器组。 ● 转发动作设置为“返回固定响应”时，支持额外添加转发动作：限速。 详见**转发动作**。

说明

支持设置Cookie类型的转发条件、支持额外设置转发动作重写/写入Header/删除Header/限速/跨域/流量镜像至后端服务器组功能陆续上线中，已发布区域请以控制台实际开放为准。如果您有使用需求，可以提交**工单**进行处理。

匹配原理

- **匹配策略**：每个客户端请求会按照**转发策略**进行匹配，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。如果匹配到多条转发策略，基于**转发策略优先级顺序**进行转发（**转发策略编号的数值越小，优先级越高，越先匹配**）。
  - 一条转发策略的转发规则中添加了多个条件时，请求需同时满足所有条件，才能匹配到该条转发策略。
  - 如果请求能匹配到监听器中您配置的转发策略，则按该转发策略转发请求。
  - 如果请求不能匹配到监听器中您配置的转发策略，则将请求按照默认转发策略进行转发。

- **转发策略优先级**：**决定**客户端请求匹配转发规则顺序的机制。当一个客户端请求满足多条转发策略的转发规则时，转发策略编号的数值越小、优先级越高、越先匹配。
- **默认转发策略**：每个七层协议的监听器创建后，都会有一条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）。
  - 如果客户端请求没有匹配到您配置的转发策略，将按照默认转发策略进行转发。
  - 默认转发策略的优先级最低且不参与转发策略排序。可以修改默认的后端服务器组，但不可删除默认转发策略。

转发规则

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

表 1-34 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。域名由以点分隔的字符串组成，单个字符串不超过63个字符，域名总长度不能超过100个字符。 • 匹配方式 – 精确匹配及通配符匹配：只能由英文字母、数字和特殊字符.-?=~_+\^*!$&\|()[]组成，支持星号（*）和半角问号（？）作为通配符使用。不支持以.开头和结尾，不支持..的形式。 – 正则匹配：只能由英文字母、数字和特殊字符.-?=~_+\^*!$&|()[]组成。 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**
路径	• 匹配说明 触发转发的路径，可以并列添加多个路径。路径由英文字母、数字和特殊字符_~';@^-%#$.*+?,=!:|\/()[]{}组成，长度范围为1~128个字符。 • 匹配方式 – 精确匹配：请求的路径和设定路径完全一致，只能由/开头。 – 前缀匹配：请求的路径匹配已设定路径的开头，只能由/开头。 – 正则匹配：请求的路径和设定的路径正则表达式匹配。 更多关于路径匹配转发规则的信息，请参见**路径高级转发策略匹配示例**。 路径示例： 请求链接为：https://www.example.com**/login.php**?locale=zh-cn#videos 转发规则选择“路径”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!$'()*+,./:;=?@^-_'。 ● 值（value）：一个键下可以配置多个值。只能包含英文字母、数字和特殊字符!$'()*+,./:;=?@^-_'。支持*和？作为通配符使用。 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。 **说明** HTTP请求头User-agent和Connection仅支持首字母大写的形式。 ● 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!#$%&'()*+,.\/:;<=>?@[]^-_'{|}~。支持*和？作为通配符使用。 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
Cookie	触发转发的Cookie。 Cookie是键值对的形式，需要分别设置值： ● 键（key）：键的长度为1~100个字符，且首尾字符不能为空格。 ● 值（value）：一个键下配置一个值，值的长度为1~100个字符。 支持输入多个Cookie键值对，键值对支持英文字母、数字和特殊字符!%'"()*+,./:=?@^-_`~。 Cookie示例： 键（key）：cookie_name 值（value）：cookie_value

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。

转发动作设置为“转发至后端服务器组”和“返回固定响应”时，支持额外添加转发动作。ELB将首先执行额外的转发动作，然后再将请求转发至对应的后端服务器组或返回固定响应。额外转发动作中，限速的优先级最高。

支持额外添加的转发动作如下：

- 转发至后端服务器组：重写/写入Header/删除Header/限速/跨域/流量镜像至后端服务器组。
- 返回固定响应：限速。

表 1-35 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。
	您可以添加多个后端服务器组，且必须为每个后端服务器组配置权重，请求将根据配置的权重值转发至不同的后端服务器组。支持配置的权重值为0~100的整数。
	支持开启后端服务器组间会话保持并设置会话保持超时时间。
	● 一条转发策略最多支持添加5个后端服务器组。
	● 会话保持超时时间的取值范围为1~1440分钟。
	说明
	● 支持添加多个后端服务器组并配置权重和后端服务器组间会话保持功能陆续上线中，已发布区域请以控制台实际开放为准。
	● 为保证后端服务器组内会话保持生效，请开启后端服务器组间会话保持。
	● 弹性负载均衡严格按照为后端服务器组配置的权重转发请求至后端服务器组，以下情况会造成业务风险。
	  ● 后端服务器组内的后端服务器健康检查结果全部异常。
	  ● 后端服务器组内未添加后端服务器。
	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/写入Header/删除Header/限速。
	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** 设置“重定向至监听器”的转发策略后，优先级低于该策略的转发策略会失效。 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。

转发动作	描述
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，字符串间以点分隔，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** 转发规则选择路径的正则匹配后，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。 **说明** 转发动作设置为“返回固定响应”时，支持额外添加转发动作：限速。 详情见**添加转发动作（可选）**。 **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> **说明** 如果您需要显示中文，建议加入<meta charset="utf-8">指定编码，否则浏览器会将中文解析成乱码。 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 1-36 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，字符串间以点分隔，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。如果您使用特殊字符{}，仅支持**${host}**的格式，表示与源域名相同。 • **路径**：由英文字母、数字和特殊字符_~';@^-%#&$.*+?,=!:|\/()[]{}组成，只能由/开头。如果您使用特殊字符{}，仅支持**${path}**的格式，表示与源路径相同。 **说明** 转发规则选择路径的正则匹配后，转发动作“重定向至URL”和“重写”中的路径支持正则表达式替换。路径替换规则详情见**转发动作的路径支持URL的正则表达式示例**。 • **查询字符串**：只能包含英文字母、数字和特殊字符!$'()*+,./:;=?@&^-_'，&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。
写入Header	如果满足转发规则的条件，则将在请求中写入配置的Header后再访问后端服务器组。 输入头字段名称和头字段内容，将覆盖请求中的头变量。默认支持配置5个Header变量。 Header是键值对的形式，需要分别设置值： • 键（key）：键的长度为1~40个字符，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。值的长度为1~128个字符，只能包含英文字母、数字和特殊字符!#$%&'()*+,.\/:;<=>?@[]^-_'{\|}~。还支持*和？两种通配符。 – 用户指定：用户指定写入的Header键。只能包含英文字母、数字和特殊字符!#$%&'"()*+,.\\/:;<=>?@[]^-_` {|}~。首尾字符不能为空格。 – 系统定义：支持写入以下指定的Header键。客户端端口/客户端IP地址/客户端请求协议/负载均衡实例ID/负载均衡实例监听端口/负载均衡绑定的弹性公网IP/负载均衡绑定的私网IP。 – 引用：引用请求头字段中的某一个Header键值。只能由小写英文字母、数字、下划线和中划线组成。 写入Header示例参见**表1-37**。

转发动作	描述
删除Header	如果满足转发规则的条件，则将在请求中删除配置的Header后再访问后端服务器组。 输入Header头字段名称，将删除请求Header中对应的键值对内容。默认支持配置5个Header变量。 键（ key ）：只能由英文字母、数字、下划线和中划线组成。
限速	转发动作转发至后端服务器组和返回固定响应支持设置限速。 请根据需要配置以下参数 ● QPS(总限速)：每秒查询速率，支持取值范围：1~100000。请求速率超过设置的限速后，新建连接请求将被丢弃，并会返回给客户端503状态码。 ● QPS(基于客户端源IP限速)：基于客户端源IP进行限速，取值范围：1~100000。同时配置QPS(总限速)和QPS(基于客户端源IP限速)时，基于客户端源IP限速值要小于总限速值。请求速率超过设置的限速后，新建连接请求将被丢弃，并会返回给客户端503状态码。 **说明** QUIC协议的监听器不支持设置基于客户端源IP限速。

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，_和-，且不能以下划线（_）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，_和-，且不能以下划线（_）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。
流量镜像至后端服务器组	将转发至后端服务器组的流量请求镜像到选择的后端服务器组，适用于网络流量检查、审计分析以及问题定位等场景。 添加的其他可选转发动作也会对镜像到后端服务器组中的流量请求生效。

表 1-37 写入 Header 示例

原有请求头	写入Header键	写入Header键值		转发至后端服务器组请求头
header1:aaa header2:bbb	header3	自定义	ccc	header1:aaa header2:bbb header3:ccc

原有请求头	写入Header键	写入Header键值		转发至后端服务器组请求头
	header3	系统指定	客户端端口	header1:aaa header2:bbb header3:客户端端口
	header3	引用	header1	header1:aaa header2:bbb header3:aaa

说明

不支持对请求中的以下Header键值进行修改（不区分大小写）：

connection、upgrade、content-length、transfer-encoding、keep-alive、te、host、cookie、remoteip、authority、x-forwarded-host、x-forwarded-for、x-forwarded-for-port、x-forwarded-tls-certificate-id、x-forwarded-tls-protocol、x-forwarded-tls-cipher、x-forwarded-elb-ip、x-forwarded-port、x-forwarded-elb-id、x-forwarded-elb-vip、x-real-ip、x-forwarded-proto、x-nuwa-trace-ne-in、x-nuwa-trace-ne-out。

路径高级转发策略匹配示例

配置了5个基于路径的高级转发策略，如表1-38所示。

表 1-38 路径高级转发策略匹配示例

请求路径	转发策略	设定的路径	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
/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：

- 当请求路径为“**/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**。

- 当请求路径为“**/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**。
- 当请求路径为“**/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。

转发规则选择路径的正则匹配后，转发动作的路径支持正则表达式替换。

路径替换流程

1. 路径匹配：客户端发送请求，并匹配到某一条路径转发规则的正则表达式。路径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 1-39 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：路径	正则匹配	• 路径正则匹配条件：/test/(.*)/(.*)/index • 匹配成功的请求路径：/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

高频问题

为什么请求 URL 中符号“#”后的字段无法匹配转发策略?

HTTP规范中，请求URL中的“#”符号为“片段标识符“（Fragment Identifier）。“#”字符后面的字段为仅用于在客户端定位已获取资源的特定片段，如HTML页面中的锚点，不会被发送到请求的服务器，即不会发送到ELB进行转发规则的匹配。

相关文档

- 控制台操作：**添加高级转发策略**、**转发策略排序**、**修改转发策略**。
- API操作：
  - **创建转发策略**、**更新转发策略**、**批量更新转发策略优先级**。
  - **创建转发规则**、**更新转发规则**。

1.4.3.5.2 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**：域名、路径、HTTP请求方法、HTTP请求头、查询字符串、网段、Cookie。详见**转发规则**。
- **支持的转发动作**：转发至后端服务器组、重定向至监听器、重定向至URL、返回固定响应和附加转发动作重写/写入Header/删除Header/限速/跨域/流量镜像至后端服务器组。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. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要添加转发策略的负载均衡器名称。
3. 在“监听器”页签，单击目标监听器名称。
4. 在监听器“基本信息”页面，单击“开启高级转发策略”。
5. 单击“确认”。

添加高级转发策略

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要添加转发策略的负载均衡器名称。
3. 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。
4. 单击“添加转发策略”按钮，参考**表1-34**和**表1-35**配置参数。
5. 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。

您可以直接编辑选择转发策略的优先级，也可以通过排序来设置优先级。

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要修改转发策略的负载均衡器名称。
3. 切换到监听器页签，单击需要修改转发策略的监听器名称。
4. 切换到“转发策略”页签，单击上方的“排序”。
5. 通过鼠标拖拽转发策略模块来调整转发策略的优先级
6. 单击“保存”。

修改转发策略

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要修改转发策略的负载均衡器名称。
3. 在“监听器”页签，单击需要修改转发策略的监听器名称。
4. 切换到“转发策略”页签，选择需要修改的转发策略，单击“编辑”。
5. 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. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要删除转发策略的负载均衡器名称。
3. 在监听器页签，单击需要删除转发策略的监听器名称。
4. 切换到“转发策略”页签，选择需要删除的转发策略，单击“删除”。
5. 在弹出的“删除转发策略”对话框中，单击“确定”。

1.4.3.6 配置附加 HTTP 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 1-40 客户端访问信息

头字段	功能说明
X-Real-IP	通过重写X-Real-IP字段获取客户端的源IP地址，传输到后端服务器的报文中。
X-Forwarded-For-Port	通过重写X-Forwarded-For-Port字段获取客户端的端口，传输到后端服务器的报文中。

头字段	功能说明
X-Forwarded-Host	通过重写X-Forwarded-Host字段获取客户端的域名，传输到后端服务器的报文中。

表 1-41 负载均衡器信息

头字段	功能说明
X-Forwarded-Proto	通过重写X-Forwarded-Proto字段获取访问负载均衡实例的监听器的协议，传输到后端服务器的报文中。
X-Forwarded-ELB-IP	通过重写X-Forwarded-ELB-IP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。
X-Forwarded-Port	通过重写X-Forwarded-Port字段获取负载均衡实例的监听端口，传输到后端服务器的报文中。
X-Forwarded-ELB-ID	通过重写X-Forwarded-ELB-ID字段获取访问的负载均衡实例的ID，传输到后端服务器的报文中。

表 1-42 客户端证书数据信息

头字段	功能说明
X-Forwarded-Clientcert-subjectdn	通过重写X-Forwarded-Clientcert-subjectdn字段获取客户端证书的所有者信息。
X-Forwarded-Clientcert-issuerdn	通过重写X-Forwarded-Clientcert-issuerdn字段获取客户端证书的发行者信息。
X-Forwarded-Clientcert-fingerprint	通过重写X-Forwarded-Clientcert-fingerprint字段获取客户端证书的指纹取值。
X-Forwarded-Clientcert-clientverify	通过重写X-Forwarded-Clientcert-clientverify字段获取客户端证书的校验结果。
X-Forwarded-Clientcert-serialnumber	通过重写X-Forwarded-Clientcert-serialnumber字段获取客户端证书的序列号。
X-Forwarded-Clientcert-ciphers	通过重写X-Forwarded-Clientcert-ciphers字段获取客户支持的加密算法列表。
X-Forwarded-Clientcert-end	通过重写X-Forwarded-Clientcert-end字段获取客户端证书的截止日期。

头字段	功能说明
X-Forwarded-Clientcert	通过重写X-Forwarded-Clientcert字段获取pem格式的客户端证书。

表 1-43 TLS 负载均衡器元数据信息

头字段	功能说明
X-Forwarded-TLS-Cipher	通过重写X-Forwarded-TLS-Cipher字段获取客户端和负载均衡器通信使用的TLS加密算法名称。
X-Forwarded-Tls-Protocol	通过重写X-Forwarded-Tls-Protocol字段获取TLS连接使用的协议版本加密算法名称。
X-Forwarded-Tls-Alpn-Protocol	通过重写X-Forwarded-Tls-Alpn-Protocol字段获取客户端和负载均衡器在SSL握手期间协商的应用层协议。
X-Forwarded-Tls-Sni	通过重写X-Forwarded-Tls-Sni字段获取客户端TLS请求的服务器名称。
X-Forwarded-Tls-Ja3	通过重写X-Forwarded-Tls-Ja3字段获取客户端TLS请求的JA3指纹。
X-Forwarded-Tls-Ja4	通过重写X-Forwarded-Tls-Ja4字段获取客户端TLS请求的JA4指纹。
X-Forwarded-Tls-Certificate-ID	通过重写X-Forwarded-Tls-Certificate-ID字段获取负载均衡器使用的TLS证书的ID。

说明

支持配置附加HTTP头字段功能逐步上线中，请以控制台实际为准。

添加 HTTP 头字段

1. 进入**弹性负载均衡列表页面**。
2. 您可以通过以下两种操作入口，添加HTTP请求头。
   - 在弹性负载均衡列表页面，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”。
   - 在弹性负载均衡列表页面，在目标负载均衡器所在行的操作列，单击“添加监听器”。
3. 在“添加监听器”界面，展开更多配置（可选），根据您的业务需求，勾选您需要添加HTTP头字段。
4. 根据界面提示，完成监听器后续的配置步骤。
5. 确认配置完成，单击“提交”。

修改 HTTP 头字段

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击目标负载均衡器名称。
3. 在“监听器”页签，在目标监听器所在行的操作列，单击“编辑”。
4. 在“编辑监听器”界面，展开高级配置，根据您的业务需求选择HTTP头字段。
5. 单击“确定”。

相关文档

- **通过独享型ELB获取客户端证书数据信息**
- API操作：**创建监听器**

1.4.3.7 为 HTTP/HTTPS 监听器配置数据压缩

ELB支持为HTTP/HTTPS监听器配置数据压缩功能，通过数据压缩可以减少传输数据，提升传输效率并降低带宽损耗。

数据压缩概述

客户端发送HTTP/HTTPS请求时，在请求头中加入**Accept-Encoding:gzip,deflate,br,***表示客户端支持压缩功能，并将客户端支持的压缩算法写入请求头的值。服务端接收请求，如果发现客户端支持数据压缩功能，则按照服务端的配置，对响应体进行压缩并在响应头中加入**Content-Encoding**通知客户端响应内容已加密和具体的加密算法。

在通过弹性负载均衡业务转发时，客户端、负载均衡器、后端服务器的服务端之间的压缩行为需要协调配置。如果后端服务器先进行了压缩，ELB不会再次进行压缩而是直接透传后端服务器的响应内容到客户端。当前ELB仅支持对后端响应码为200、403和404的响应体进行压缩。

图 1-18 负载均衡器进行压缩示意图

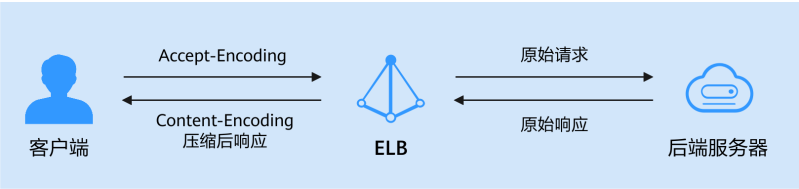
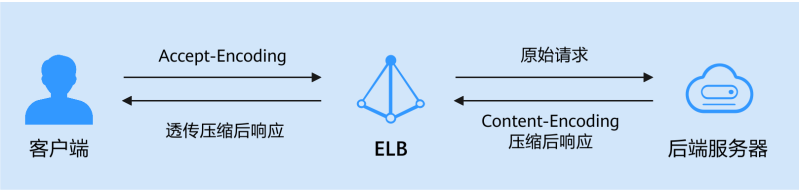


图 1-19 后端服务器进行压缩示意图



约束与限制

Brotli和Gzip支持压缩的类型：text/html text/xml text/plain text/css application/javascript application/x-javascript application/rss+xml application/atom+xml application/xml application/json。

为 HTTP/HTTPS 监听器开启数据压缩

您可以在新添加HTTP/HTTPS时开启数据压缩，也可以在监听器创建完成后进行编辑。

1. 进入**弹性负载均衡列表页面**。
2. 您可以通过以下两种操作入口，添加HTTP/HTTPS监听器。
   - 在弹性负载均衡列表页面，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”。
   - 在弹性负载均衡列表页面，在目标负载均衡器所在行的操作列，单击“添加监听器”。
3. 在“添加监听器”界面，展开**高级配置**，根据您的业务需求，开启数据压缩的功能开关。

   图 1-20 配置数据压缩

4. 根据界面提示，完成监听器后续的配置步骤。
5. 确认配置完成，单击“提交”。

相关文档

- **添加HTTP监听器**
- **添加HTTPS监听器**
- **修改监听器**

1.4.3.8 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. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要开启HTTP/2功能的监听器的负载均衡器名称。
3. 在该负载均衡界面的“监听器”页签，单击“添加监听器”。
4. 在“添加监听器”界面，前端协议选择“HTTPS”。
5. 在“添加监听器”界面，展开高级配置，打开HTTP/2功能。
6. 确认配置，单击“提交”。

图 1-21 开启 HTTP 监听器的 HTTP/2 功能

已有 HTTPS 监听器

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要修改HTTP/2功能的负载均衡器名称。
3. 在“监听器”页签，单击需要修改HTTP/2功能开关的监听器名称。
4. 在监听器的“基本信息”页面，单击“编辑监听器”。
5. 在“编辑监听器”界面，展开高级配置，开启或者关闭HTTP/2功能。
6. 单击“确定”。

图 1-22 修改 HTTPS 监听器的 HTTP/2 功能

1.4.4 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**购买独享型负载均衡器**。
- 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. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要为监听器配置修改保护的负载均衡名称。
3. 在“监听器”页签，单击需要为配置修改保护的监听器名称。
4. 在监听器的“基本信息”页签，单击修改保护右侧的“设置”。
5. 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. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要修改监听器的负载均衡名称。
3. 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”。
4. 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. 进入**弹性负载均衡列表页面**。

2. 在弹性负载均衡列表页面，单击需要修改监听器的负载均衡名称。
3. 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。
4. 在监听器的“基本信息”页面，单击“编辑监听器”。
5. 在“编辑监听器”页面，单击“高级配置”。
6. 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”。
7. 单击“确定”。

启用或停用监听器

如果由于系统维护升级、紧急故障隔离或流量切换等业务原因，您仅要暂时停止某个监听器的业务转发，您可以使用监听器的停用和启用功能来改变监听器的运行状态。

警告

停用监听器会造成转发流量中断并停止监控和健康检查探测，请谨慎操作。

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击目标监听器所在的负载均衡名称。
3. 在监听器页签，选择目标监听器。

   您可以启动或停止监听来改变其运行状态。当监听处于配置中时，无法删除、编辑或更换服务器组。

   a. 停止监听器：单击操作列的“停用”，在“停用监听器”弹窗中，输入“YES”，单击“确定”后完成停用。

      监听器停用后，监听器的健康检查结果会保持停用前的状态，仅作为参考结果显示。

   b. 启用监听器：单击操作列的“启用”，在“启用监听器”弹窗中，输入“YES”，单击“确定”后完成停用。

      监听器启用后，ELB实例会重新发起健康和健康检查探测，请优先确认健康检查结果，避免对业务造成影响。

更换监听器的后端服务器组

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击目标监听器所在的负载均衡名称。
3. 选择“监听器”页签，在监听器列表中，单击目标监听器的名称。
4. 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”。
5. 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。

6. 单击“确定”。

删除监听器

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要删除监听器的负载均衡名称。
   a. 删除单个监听器：
      i. 在“监听器”页签，需要删除监听器所在行的“操作”列，单击“删除 ”。
      ii. 在删除监听器的弹窗页面，输入“DELETE”。
   b. 批量删除监听器：
      i. 在“监听器”页签，勾选多个希望删除的监听器。
      ii. 单击“监听器”列表页面上方的“删除”。
      iii. 在删除监听器的侧拉弹窗页面，输入“DELETE”。
3. 单击“确定”，完成删除。

1.4.5 复制监听器

当您需要为多个应用或服务创建具有相同配置的监听器时，手动配置每一个监听器不仅耗时而且容易出错。如果您需要创建一个**与已有监听器相同配置**的监听器，您可以通过ELB提供的监听器复制功能快速高效地完成相同配置监听器的创建，提升您的操作效率。

说明

监听器支持复制功能陆续上线中，请以控制台实际为准。

约束与限制

- 仅支持本ELB实例内或相同VPC的ELB实例间使用监听器复制功能。
- 仅同类型ELB实例（独享型/共享型、网络型/应用型）之间可以使用监听器复制功能。
- 复制监听器操作仅支持复制出1个新的监听器。
- 进行复制的监听器为应用型监听器时：
  - 监听器设置升级至QUIC配置或HTTP重定向到HTTPS配置时，需要复制监听器完成后再进行操作。
  - 转发策略也会被复制。

复制监听器

1. 进入**弹性负载均衡列表页面**。

1. 在弹性负载均衡列表页面，单击需要复制监听器的负载均衡名称。
2. 在“监听器”页签，在目标监听器的操作列，单击“更多”，单击“复制”。
3. 在“复制监听器”弹窗，配置参数请参见**表1-44**。

表 1-44 复制监听器参数说明

参数	说明
进行复制的监听器	
源前端协议	当前监听器的前端协议，复制出的新监听器与当前监听器的前端协议保持一致。
源端口	当前监听器的端口。
复制出的新监听器	
目的负载均衡器	复制出的新监听器所在的ELB实例。 仅支持选择**本ELB实例**或**相同VPC的其他ELB实例**。 监听器复制到目标负载均衡器下时，需满足正常创建监听器、转发策略、后端服务器组、后端服务器的条件。
监听端口	负载均衡器对外提供服务时接收请求的端口。 ● **目的负载均衡器为本ELB实例**：您为复制出的新监听器配置的监听端口不能与源端口相同。 ● **目的负载均衡器为相同VPC的其他ELB实例**：你可以按需设置新监听器的端口。
名称（可选）	复制出的新监听器名称，长度范围为1~255位。 只能由中文、英文字母、数字、下划线、中划线和点组成。
后端服务器组	复制后的新监听器的后端服务器组，适用于**监听器进行默认转发的后端服务器组**和**通过转发策略转发的后端服务器组**。 ● **复用**：新监听器将会直接使用当前监听器的后端服务器组。 ● **复制**：系统将会根据原有配置创建新的后端服务器组，然后将其关联到新监听器使用。 通过复制创建的新后端服务器组名称默认为原后端服务组名称加上后缀“-copy”。

4. 单击“确定”，进行监听器复制。
5. 复制完成后，单击“关闭”，结束复制任务。

常见问题

复制出的新监听与被复制的监听器配置完全一样吗?

复制监听器时，除了您需要为复制出新监听器选择的目标负载均衡器、监听端口、名称和后端服务器组外，新监听器的其余配置与被复制的监听器配置完全一致。

1.5 后端服务器组

1.5.1 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1-45：

表 1-45 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1-23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1-46。

图 1-23 后端服务器组使用架构图

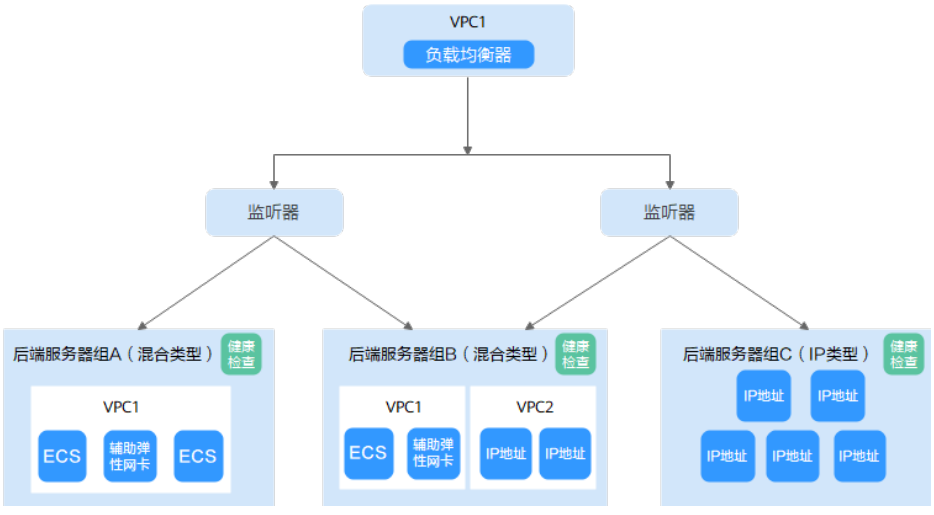


表 1-46 后端服务器组分类及说明

后端服务器组类型	可添加后端服务器分类	举例说明
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IP类型后端功能后，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1-23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。
IP类型	开启IP类型后端功能后，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1-23，后端服务器组C可添加IP地址作为后端服务器。

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。

控制后端服务器组流量分发

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1-47**所示的关键功能可供用户配置。

表 1-47 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。	创建后端服务器组
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。	配置流量分配策略分发流量
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提升了客户端的访问效率。	配置会话保持提升访问效率
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，实现后端服务器组扩容后业务的平滑启动。	配置慢启动平滑扩容后端服务器组
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自动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。	创建后端服务器组

后端服务器组与监听器协议匹配关系

独享型负载均衡使用场景下，一个后端服务器组可关联至多个负载均衡实例和监听器使用，多个弹性负载均衡实例需归属同一企业项目。

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1-48**。

表 1-48 前端/后端协议匹配关系

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

说明

弹性负载均衡支持TLS、GRPC、QUIC协议陆续上线中，请以控制台实际为准。

相关文档

- 创建后端服务器组
- 控制后端服务器组流量分发
- 配置相同VPC的服务器作为后端服务器
- 配置不同VPC的服务器作为后端服务器（IP类型后端）

1.5.2 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1-49。

表 1-49 创建后端服务器组（独享型）指引

创建场景	操作步骤
独立创建后端服务器组后关联至负载均衡实例使用	创建后端服务器组。

创建场景	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**。
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1-50**。

表 1-50 前端/后端协议匹配关系

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

创建后端服务器组

1. 进入**后端服务器组列表页面**。
2. 在后端服务器列表页面，单击页面右上角“创建后端服务器组”按钮。
3. 配置后端分配策略，参数详情请参见**表1-51**。

表 1-51 配置后端分配策略参数说明

参数	说明
名称	待创建的后端服务器组的名称。

参数	说明
实例类型	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：必须同时向服务器组中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。仅TCP、UDP、TLS协议的监听器支持添加主备转发模式的后端服务器组。 **说明** 该功能陆续上线中，已发布区域请以控制台实际为准。
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IP类型后端功能后按照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IP类型后端功能才能添加后端服务器。 **说明** 该功能陆续上线中，已发布区域请以控制台实际为准。
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》**。
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。

参数	说明
IP版本	后端服务器组支持添加后端服务器的IP地址版本，默认支持IPv4的后端服务器。 当后端协议为TCP或UDP协议时，支持设置该参数。 ● IPv4：仅支持IPv4类型的后端服务器地址。 ● 双栈：同时支持IPv4和IPv6类型的后端服务器地址。 **说明** 该功能陆续上线中，已发布区域请以控制台实际为准。
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，已发布区域请以控制台实际为准。 **说明** 仅独享型负载均衡支持TCP、UDP类型的后端服务器组开启全端口转发功能。
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**配置流量分配策略分发流量**。

参数	说明
后端全异常转发模式	仅负载均衡转发模式的后端服务器组支持该功能。 后端全异常转发模式默认关闭，如果后端服务器健康检查结果全部异常，将会无法将请求转发到该后端服务器组。 开启后端全异常转发模式后，如果后端服务器健康检查结果全部异常，将忽略健康检查结果，转发请求到组内的所有后端服务器。 该功能可以避免因健康检查错误配置导致检查结果异常，造成的业务不可使用情况，提高业务的可用性。 如果您为后端服务器组开启可用区亲和转发，后端全异常转发模式将失效。
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**配置会话保持提升访问效率**。 **说明** • TLS协议的后端服务器组不支持设置会话保持。 • QUIC协议的后端服务器组默认开启会话保持，无此开关。
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**配置慢启动平滑扩容后端服务器组**。
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，已发布区域请以控制台实际为准。
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，控制台默认值为300秒。
可用区亲和转发	如果后端协议为TCP或UDP协议，支持开启此功能。 开启可用区亲和转发后，后端全异常转发模式失效。 弹性负载均衡接收流量后，转发流量到服务器组中与ELB实例相同可用区的后端服务器，有效降低ELB转发请求到后端服务器的时延。 更多关于可用区亲和转发的信息，请参见**配置可用区亲和转发降低时延**。 **说明** 该功能陆续上线中，已发布区域请以控制台实际为准。

参数	说明
可用区亲和失效阈值	用于判断可用区的健康状况，当单可用区内健康的后端服务器数量或占比低于设定阈值时，判定该可用区不健康，可用区亲和功能失效，执行亲和失效转发动作。 如果后端服务器组未开启健康检查，默认组内的后端服务器全部为健康状态。 • 百分比：单可用区内健康检查结果正常的服务器个数除以该可用区服务器的总数。 • 绝对值：可用区内健康检查结果正常的服务器个数。 百分比为0%或绝对值为0时，判定可用区健康，可用区亲和转发始终生效。
可用区亲和失效转发动作	当系统通过可用区亲和失效阈值判定可用区不健康时，可用区亲和功能失效，执行可用区亲和失效转发动作。 后端服务器组的请求将根据您设置的动作进行转发，如果您业务要求容灾高可用，推荐您选择“转发到所有可用区的健康后端服务器”。 详情请参见**配置可用区亲和转发降低时延**。
描述（可选）	后端服务器组的描述。

4. 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、IP类型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1-52**。更多关于健康检查的信息，请参见**健康检查介绍**。

   表 1-52 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，已发布区域请以控制台实际为准。

参数	说明
健康检查方法	如果健康检查协议选择HTTP/HTTPS/GRPC协议，则该项是必选参数。 健康检查发送请求的方法。 ● GET：采用GET方法发送健康检查请求，后端服务器返回全部信息。 ● HEAD：采用HEAD方法发送健康检查请求，后端服务器仅返回 HTTP 头部信息，提升请求效率。请确保您的后端服务器支持HEAD请求，否则可能会导致健康检查失败，此时可以使用GET方法来进行健康检查。 ● POST：采用POST方法发送健康检查请求。请确保您的后端服务器支持POST请求，否则可能会导致健康检查失败，此时可以使用GET方法来进行健康检查。 **说明** ● 健康检查协议为HTTP和HTTPS协议时，支持GET方法和HEAD方法。 ● 健康检查协议为GRPC协议时，支持GET方法和POST方法。
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，字符串间以点分隔，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]。

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]。
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。

5. 单击“下一步”。
6. 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1-49**。

1.5.3 控制后端服务器组流量分发

1.5.3.1 配置流量分配策略分发流量

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。

创建后端服务器组时流量分配策略默认为加权轮询算法，您可以根据实际业务需要进行修改。

本文列出弹性负载均衡支持的所有分配策略，不同协议的后端服务器组支持的流量分配策略存在差异。

表 1-53 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。
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1-24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 1-24 加权轮询算法流量分发

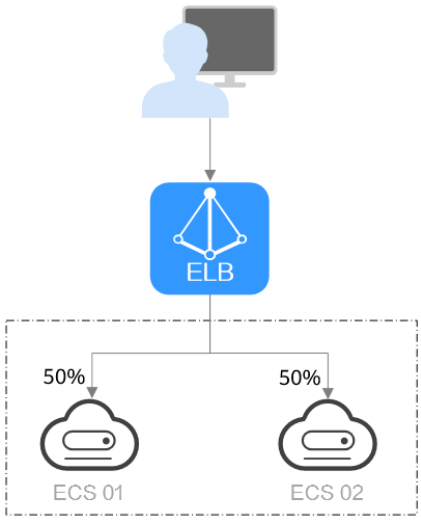


表 1-54 加权轮询算法说明

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1-25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 1-25 加权最少连接算法流量分发

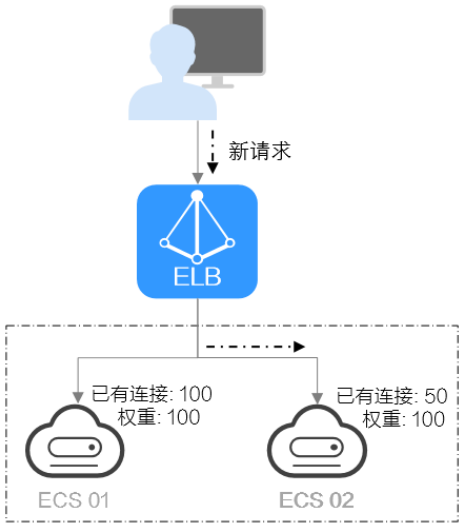


表 1-55 加权最少连接说明

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1-26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 1-26 源 IP 算法流量分发

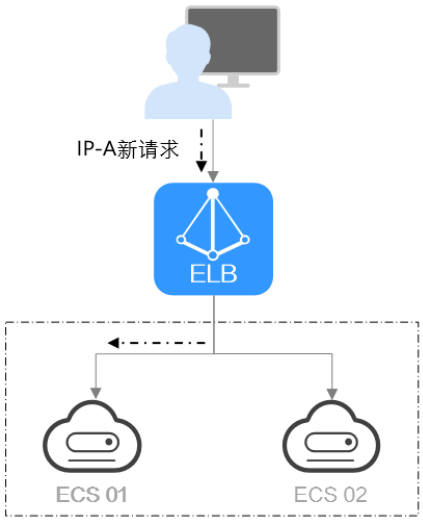


表 1-56 源 IP 算法说明

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相同的请求具有相同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1-27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 1-27 连接 ID 算法流量分发

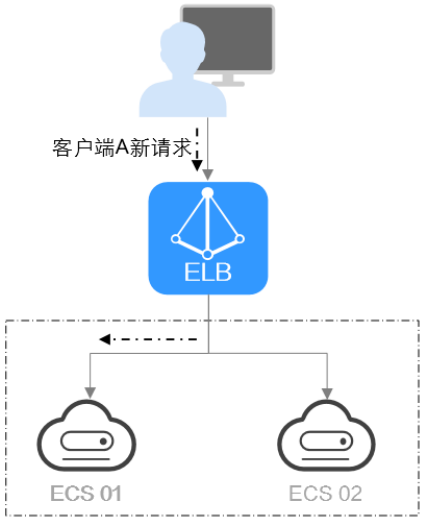


表 1-57 连接 ID 算法说明

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ID算法可以确保源相同QUIC连接上的请求具有相同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。

修改流量分配策略

⚠ 注意

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. 进入**后端服务器组列表页面**。
2. 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”。
3. 在“修改后端服务器组”弹窗中进行修改，选择“分配策略类型”。
4. 单击“确定”。

1.5.3.2 配置会话保持提升访问效率

在电商购物和用户登录的场景中，客户端与服务器的连接需要保持联系性，如果客户端请求经过ELB转发后被分配到不同的后端服务器进行处理，会导致重复登录或丢失操作进度的问题，影响业务体验。后端服务器组支持开启会话保持功能，负载均衡器可以识别客户端请求的特征（如IP/cookie），在实现负载均衡的同时，将相关联的客户端访问请求分配到同一台服务器上进行处理，提升访问效率和用户体验。

会话保持介绍

不同通信协议的后端服务器组，在不同的流量分配策略下，支持的会话保持类型存在差异，支持详情请参考表1-58。

表 1-58 独享型负载均衡会话保持支持情况

后端服务器组协议	分配策略类型	会话保持类型
• TCP • UDP	加权轮询算法	源IP地址
	加权最少连接	源IP地址
	源IP算法	不支持设置会话保持
• HTTP • HTTPS • GRPC	加权轮询算法	• 负载均衡器cookie • 应用程序cookie
	加权最少连接	• 负载均衡器cookie • 应用程序cookie
	源IP算法	不支持设置会话保持
QUIC	连接ID算法	源IP地址

表 1-59 会话保持介绍

会话保持类型	说明	会话保持时间	会话保持失效的场景
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。
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。	• 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。
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**分配策略类型**选择“源IP算法”时，已默认支持基于源IP地址的会话保持。
- 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。
- 当前QUIC协议的后端服务器组默认支持会话保持，无会话保持功能开关。
- 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，请以控制台实际为准。
- 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。

配置会话保持

1. 进入**后端服务器组列表页面**。
2. 在后端服务器组列表页面，在目标后端服务器组所在行的操作列单击“编辑”。
3. 在“修改后端服务器组”弹窗中，开启或关闭会话保持功能开关。
   开启会话保持功能需配置会话保持类型以及会话保持时间。
4. 单击“确定”。

1.5.3.3 配置慢启动平滑扩容后端服务器组

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，避免业务抖动问题。

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

- 仅独享型负载均衡支持HTTP、HTTPS和GRPC类型的后端服务器组开启慢启动功能。
- 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。

配置慢启动

1. 进入**后端服务器组列表页面**。
2. 在后端服务器组列表页面，在目标后端服务器组所在行的操作列单击“编辑”。

图 1-28 后端服务器组编辑入口

3. 在“修改后端服务器组”弹窗中，开关或关闭慢启动功能开关。

   开启慢启动功能需配置慢启动时间，取值范围为30~1200秒。当慢启动时间结束后，负载均衡器向后端服务器发送完整比例的流量请求。
4. 单击“确定”。

1.5.3.4 配置可用区亲和转发降低时延

如果您使用弹性负载均衡将流量转发到TCP或UDP协议的后端服务器组，您可以开启可用区亲和功能，将流量转发到与ELB实例相同可用区的后端服务器以降低业务时延。

说明

后端服务器组支持配置可用区亲和转发功能陆续上线中，请以控制台实际为准。

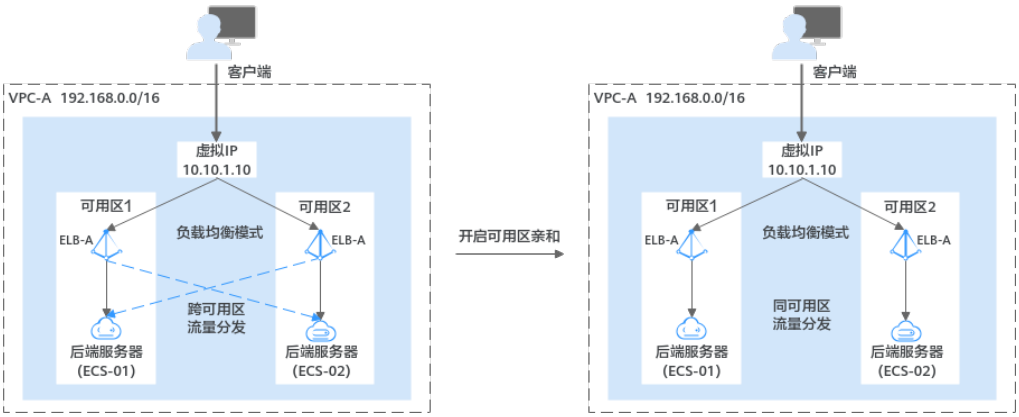
可用区亲和概述

弹性负载均衡ELB支持多可用区部署，默认状态下ELB实例进行流量转发时，会将流量转发至后端服务器组中的所有后端服务器。

当后端服务器组开启了可用区亲和转发模式后，ELB实例会将流量转发至与ELB实例相同可用区的后端服务器，从而减少了流量从ELB实例到后端服务器跨可用区转发的时延。

如果您为后端服务器组开启可用区亲和转发，后端全异常转发模式将失效。

图 1-29 开启可用区亲和转发示意图



可用区属性判定

可用区（AZ，Availability Zone）：一个AZ是一个或多个物理数据中心的集合，有独立的风火水电，AZ内逻辑上再将计算、网络、存储等资源划分成多个集群。

- 弹性负载均衡的可用区：

  独享型负载均衡支持多可用区部署，选择的每个可用区都会创建相应的负载均衡实例。

  独享型负载均衡创建后，也支持通过**变更实例可用区**功能变更实例的可用区属性。
- 后端服务器的可用区：

  表 1-60 后端服务器的可用区

后端服务器类型	可用区属性
云服务器	由云服务器实例的可用区决定。
辅助弹性网卡	由所属主弹性网卡已绑定实例的可用区决定。
IP类型后端	由您添加IP类型后端到后端服务器组时指定对应的逻辑可用区，系统可以识别该指定的可用区信息。

可用区亲和失效阈值

用于判断可用区的健康状况，当单可用区内健康的后端服务器数量或占比低于设定阈值时，判定该可用区不健康，可用区亲和功能失效，执行亲和失效转发动作。

- **百分比**：单可用区内健康检查结果正常的服务器个数除以该可用区服务器的总数。
- **绝对值**：可用区内健康检查结果正常的服务器个数。

ELB实例部署的每个可用区的健康状态判断互不影响，都会根据对应可用区内的健康的后端服务器数量或占比独立判断。

说明

- 如果百分比为0%或绝对值为0时，判定可用区健康，可用区亲和转发功能始终生效。
- 如果后端服务器组未开启健康检查，默认组内的后端服务器全部为健康状态，判定可用区健康。
- 如果亲和可用区内没有添加任何后端服务器时，判定可用区不健康，直接执行可用区亲和失效转发动作。
- 当后端服务器组开启了健康检查，后端服务器权重设置为0时，该后端服务器的健康检查结果也会参与可用区亲和失效阈值的判定。

如果您的后端服务器组开启“关闭权重为0后端的健康检查”的功能，权重设置为0的后端服务器会被剔除后再进行可用区健康判定。示例计算如下：

警告

开启可用区亲和，当亲和条件与亲和失效转发动作配置不合理时可能会造成流量转发中断，请注意在不同可用区合理部署您的后端服务器。

可用区亲和失效转发动作

当系统通过可用区亲和失效阈值判定可用区不健康时，可用区亲和功能失效，执行可用区亲和失效转发动作。

如果您业务要求容灾高可用，推荐您选择“转发到所有可用区的健康后端服务器”。

配置可用区亲和转发功能时，请注意保证无论可用区亲和是否失效，流量转发符合预期结果。

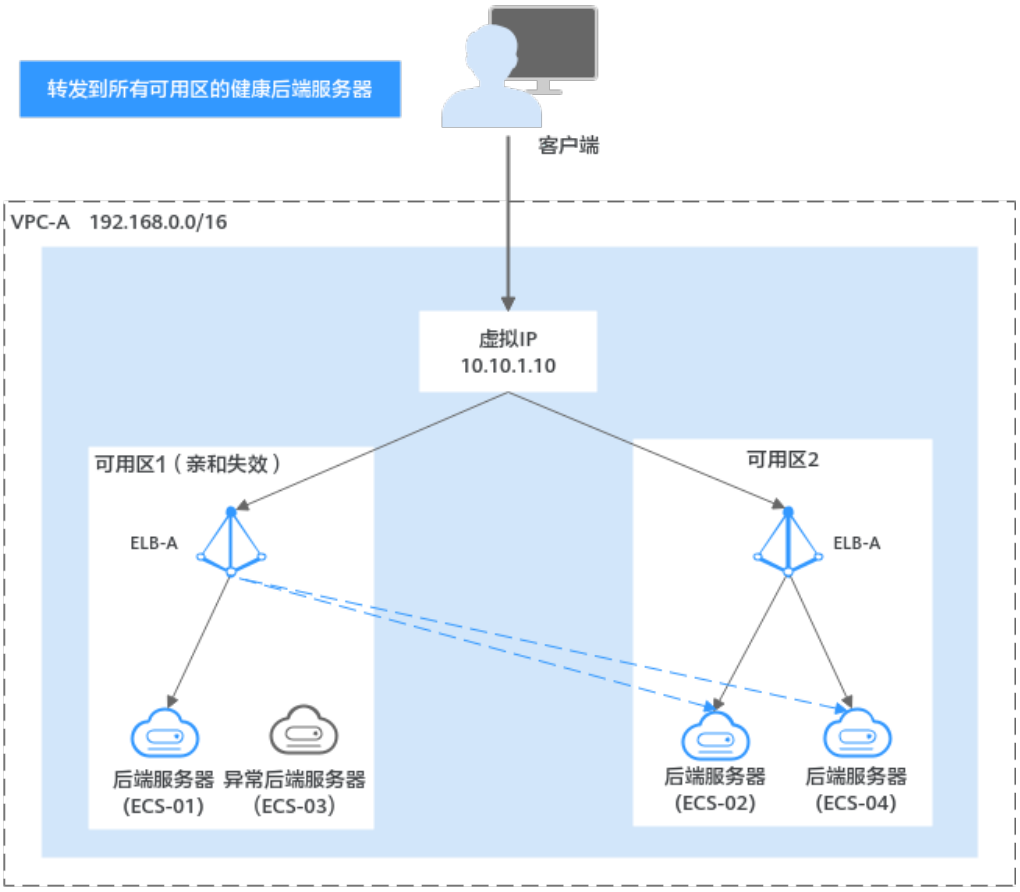
表 1-61 可用区亲和失效转发动作说明

动作	转发说明
转发到所有可用区的健康后端服务器	部署在亲和失效可用区的ELB实例将请求转发到**所有可用区的健康检查结果正常**的后端服务器。
转发到非亲和可用区的健康后端服务器	部署在亲和失效可用区的ELB实例将请求转发到**其他可用区的健康检查结果正常**的后端服务器。
转发到亲和可用区的所有后端服务器	部署在亲和失效可用区的ELB实例将请求转发到**本可用区所有的后端服务器**，包括本可用区的异常后端服务器。
转发到所有用区的所有后端服务器	部署在亲和失效可用区的ELB实例将请求转发到**所有可用区的所有后端服务器**，包括所有异常的后端服务器。

转发到所有可用区的健康后端服务器

部署在亲和失效可用区的ELB实例将请求转发到**所有可用区健康检查结果正常**的后端服务器，推荐您选择该种配置。

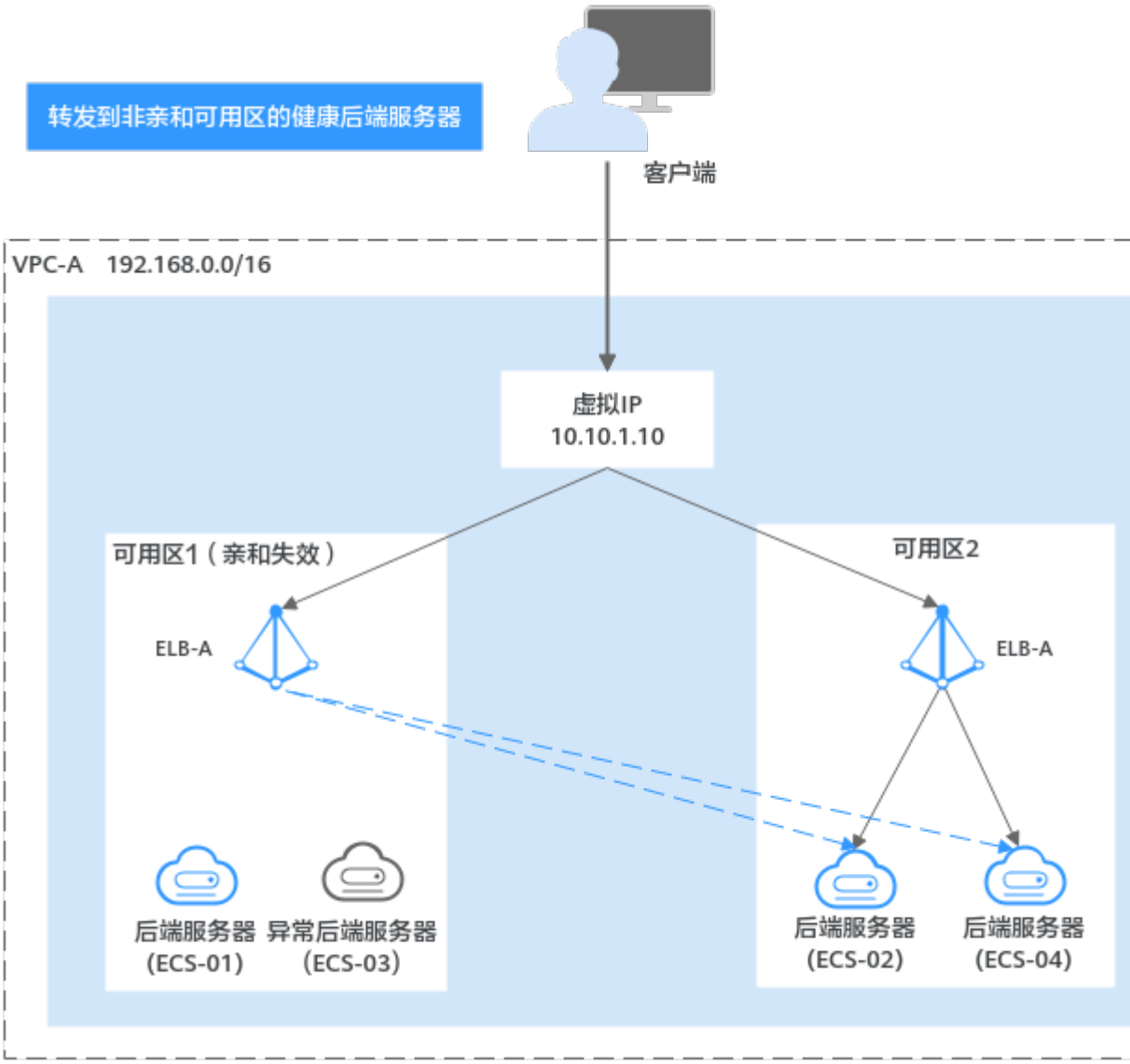
图 1-30 转发到所有可用区的健康后端服务器示意图



转发到非亲和可用区的健康后端服务器

部署在亲和失效可用区的ELB实例将请求转发到**其他可用区的健康检查结果正常**的后端服务器。

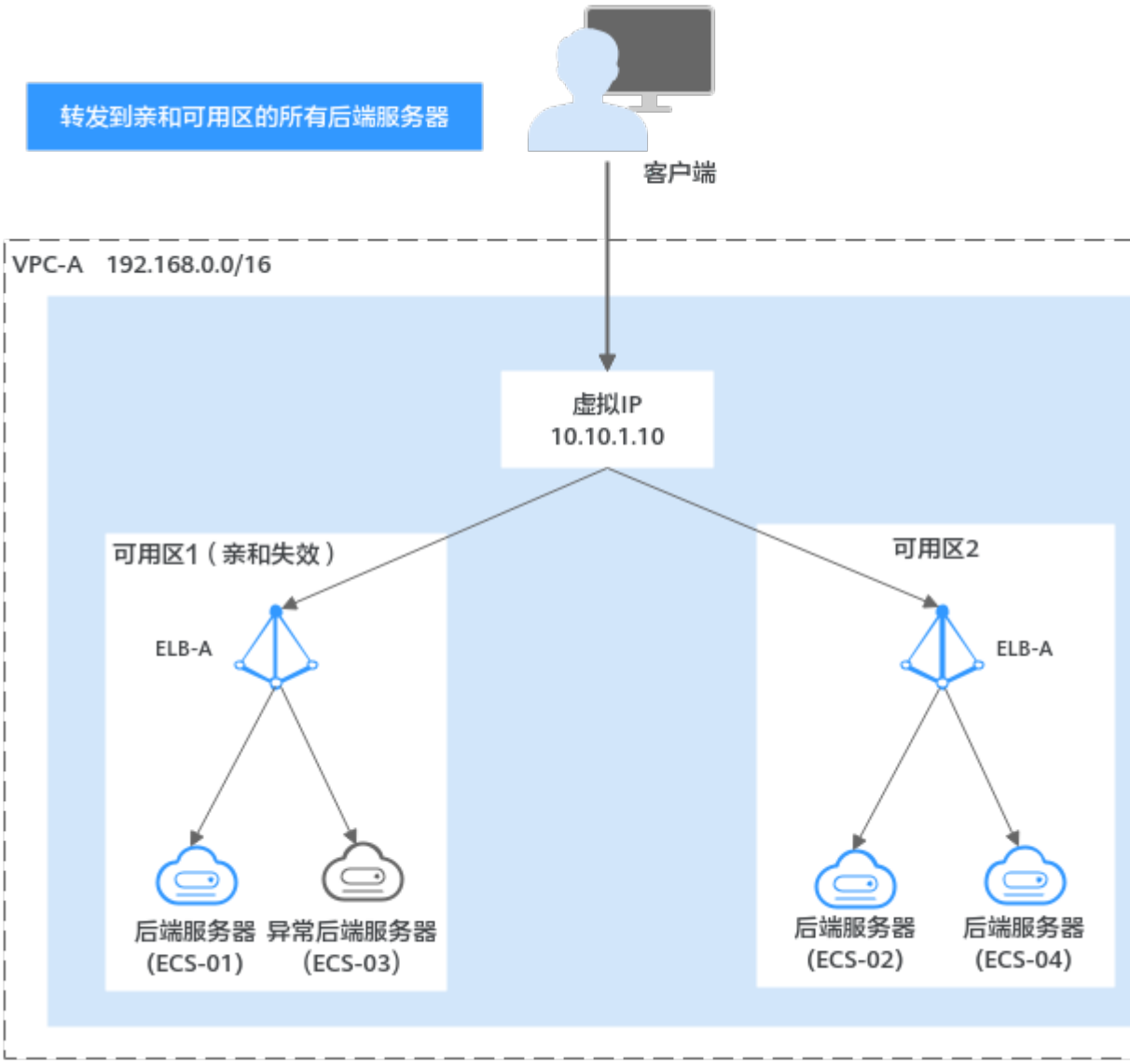
图 1-31 转发非亲和可用区的健康后端服务器示意图



转发到亲和可用区的所有后端服务器

部署在亲和失效可用区的ELB实例将请求转发到**本可用区所有的后端服务器**，包括本可用区的异常后端服务器。

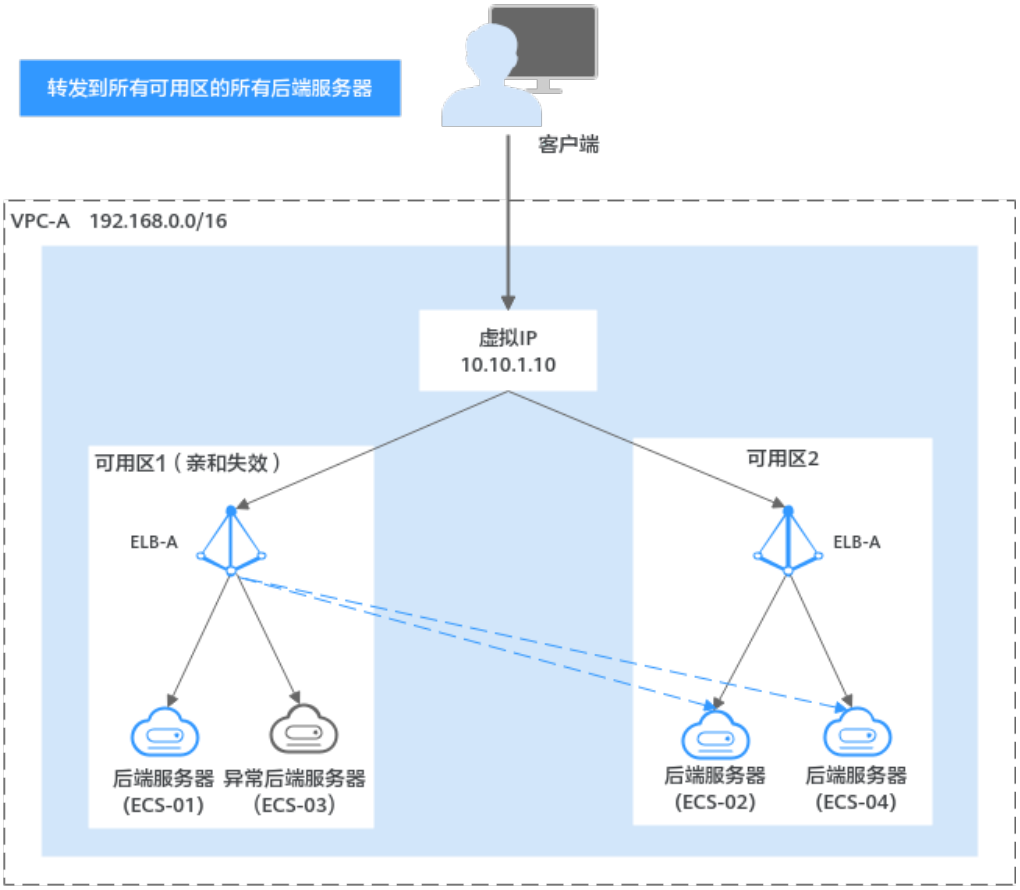
图 1-32 转发亲和可用区的所有后端服务器示意图



转发到所有可用区的所有后端服务器

部署在亲和失效可用区的ELB实例将请求转发到**所有可用区的所有后端服务器**，包括所有异常的后端服务器。

图 1-33 转发所有可用区的所有后端服务器示意图



配置可用区亲和转发

1. 进入**后端服务器组列表页面**。
2. 在后端服务器组列表页面，在目标后端服务器组所在行的操作列单击“编辑”。
3. 在“修改后端服务器组”弹窗中，开启或关闭“可用区亲和转发”功能开关。
   开启可用区亲和转发功能需配置**可用区亲和失效阈值**和**可用区亲和失效转发动作**。
4. 单击“确定”，更新配置生效。

1.5.4 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/TLS）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/QUIC）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1-48**。
- 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。

更换后端服务器组

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击目标监听器所在的负载均衡名称。
3. 选择“监听器”页签，在监听器列表中，单击目标监听器的名称。
4. 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”。
5. 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。
6. 单击“确定”。

1.5.5 管理后端服务器组

当您的后端服务器组创建后，您可以根据实际使用需求对服务器组进行管理。

配置后端服务器组修改保护

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。

后端服务器组开启修改保护后，您将无法对后端服务器组执行编辑和配置健康检查，也无法管理组内的后端服务器。

1. 进入**后端服务器组列表页面**。
2. 在后端服务器组列表页面，单击需要配置修改保护的后端服务器组名称。
3. 在后端服务器组的“基本信息”页签下，单击修改保护右侧的“设置”。
4. 在设置修改保护弹窗中，开启“修改保护”开关。
5. 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。

配置后端服务器组的后端服务器移除保护

您可以对后端服务器组开启移除保护功能，防止因误操作导致后端服务器组内的后端服务器被移除。

后端服务器组开启移除保护后，您将无法移除组内的后端服务器。

⚠ 注意

如果您的负载均衡实例由云容器引擎服务（CCE）管理，开启后端服务器组的移除保护可能影响集群的正常运行，请您谨慎操作。

1. 进入**后端服务器组列表页面**。
2. 在后端服务器组列表页面，单击需要配置移除保护的后端服务器组名称。
3. 在后端服务器组的“基本信息”页签下，单击移除保护右侧的开关进行配置。

说明

如果您需要移除后端服务器组的后端服务器，请先关闭“移除保护”开关。

查看后端服务器组

您可以根据需要查看后端服务器组的的详细信息。

1. 进入**后端服务器组列表页面**。
2. 在后端服务器组列表页面，单击待查看的后端服务器组名称。
3. 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，包括名称、ID、后端协议和健康检查的详细配置信息。
   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资源。
   c. 在“关联资源”页签下，查看服务器组已关联的资源，包括负载均衡器、监听器和转发策略。

删除后端服务器组

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。

如果七层监听器自定义的转发策略转发至该后端服务器组，则无法执行删除，请先更换转发策略的后端服务器组。

- 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。

1. 进入**后端服务器组列表页面**。
2. 在后端服务器组列表页面，在目标后端服务器组所在行的操作列单击“删除”。
3. 在“确认删除后端服务器组”对话框中，单击“确定”。

批量删除后端服务器组

说明

支持批量删除后端服务器组功能陆续上线中，请以控制台实际为准。

1. 进入**后端服务器组列表页面**。
2. 在后端服务器组列表页面，勾选希望删除的多个后端服务器组。
3. 单击后端服务器组列表页上方的“删除”。
4. 在“删除后端服务器组”侧拉对话框中，输入“DELETE”。

5. 单击“确定”，完成删除。

1.6 后端服务器

1.6.1 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1-62**。

表 1-62 添加后端服务器分类

后端服务器类型	使用说明	添加指引
云服务器	直接添加与负载均衡器同VPC的弹性云服务器（ECS）实例作为后端服务器。	**配置相同VPC的服务器作为后端服务器**
辅助弹性网卡	直接添加与负载均衡器同VPC的辅助弹性网卡（SubENI）实例作为后端服务器。	**配置相同VPC的服务器作为后端服务器**
IP类型后端	开启**IP类型后端**功能后，直接添加IP地址作为后端服务器处理请求。 您需确保添加的IP地址与ELB实例之间网络互通。	**配置不同VPC的服务器作为后端服务器（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1-63**，更多流量策略分配策略详情见**配置流量分配策略分发流量**。

表 1-63 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 来计算每台服务器负载。 • 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台后端服务器上。 • 每台后端服务器的权重只做0和非0的区分。

1.6.2 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，若后端服务器所在的子网关联了网络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“IP类型后端”功能，ELB四层监听器转发的流量将不受安全组规则和网络ACL规则限制，安全组规则和网络ACL规则无需额外放通。

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

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. 进入**弹性云服务器列表**页面。
2. 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。
3. 选择“安全组”页签，单击安全组名称，查看安全组规则。
4. 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1-64**配置安全组入方向的访问规则。

   表 1-64 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。
5. 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”。

1.6.3 配置相同 VPC 的服务器作为后端服务器

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。

独享型负载均衡的后端服务器组支持直接添加同VPC内添加ECS实例、BMS实例和辅助弹性网卡作为后端服务器。

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直接添加云服务器和辅助弹性网卡。
- 仅支持添加与后端服务器组同VPC的ECS实例、BMS实例和辅助弹性网卡。
- 独享型弹性负载均衡对裸金属服务器（BMS）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》**。

添加同 VPC 的后端服务器

1. 进入**后端服务器组列表页面**。
2. 在后端服务器组列表页面，单击需要添加后端服务器的后端服务器组名称。
3. 切换到“后端服务器”页签，根据需求选择添加以下同VPC的服务器实例。
   a. 云服务器（ECS或BMS）：选择下方“云服务器”页签，并单击“添加”。支持通过指定关键字搜索后添加，私网IP地址支持选择主网卡和扩展网卡。
   b. 辅助弹性网卡（SubENI）：选择下方“辅助弹性网卡”页签，并单击“添加”。支持通过指定关键字进行搜索后添加。
4. 选中目标添加的后端服务器，单击“下一步”。
5. 设置服务器业务端口和服务器的权重，单击“完成”。
   支持批量设置端口和权重。

批量导入同 VPC 的云服务器

1. 进入**后端服务器组列表页面**。
2. 在后端服务器组列表页面，单击需要添加后端服务器的后端服务器组名称。
3. 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”。
4. 在“添加后端服务器”侧拉窗中，单击“批量导入”。
5. 在“导入”弹窗中，您可单击“下载模板”下载模板文件到本地。
   模板文件需要您填写私网IP地址、业务端口和权重。
6. 单击“添加文件”，上传您本地配置完成的导入文件。
   系统将为您匹配导入文件对应的云服务器信息。
7. 选中目标添加的后端服务器，单击“导入”。

修改后端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**。

1. 进入**后端服务器组列表页面**。
2. 在后端服务器组列表页面，单击需要修改后端服务器端口/权重的后端服务器组名称。
3. 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”或“辅助弹性网卡”区域。
4. 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”。
5. 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。

6. 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. 进入**后端服务器组列表页面**。
2. 在后端服务器组列表页面，单击需要移除后端服务器的后端服务器组名称。
3. 切换到“后端服务器”页签，选择下方“云服务器”或“辅助弹性网卡”页签。
4. 勾选需要移除的服务器，单击服务器列表上方的“移除”。
5. 在移除后端服务器的对话框中单击“是”。

   如果您的ECS开启了回收站功能，同步删除云服务器时，ECS将会先进入回收站。ECS从回收站销毁后才会自动删除ELB侧云服务器的记录。

1.6.4 配置不同 VPC 的服务器作为后端服务器（IP 类型后端）

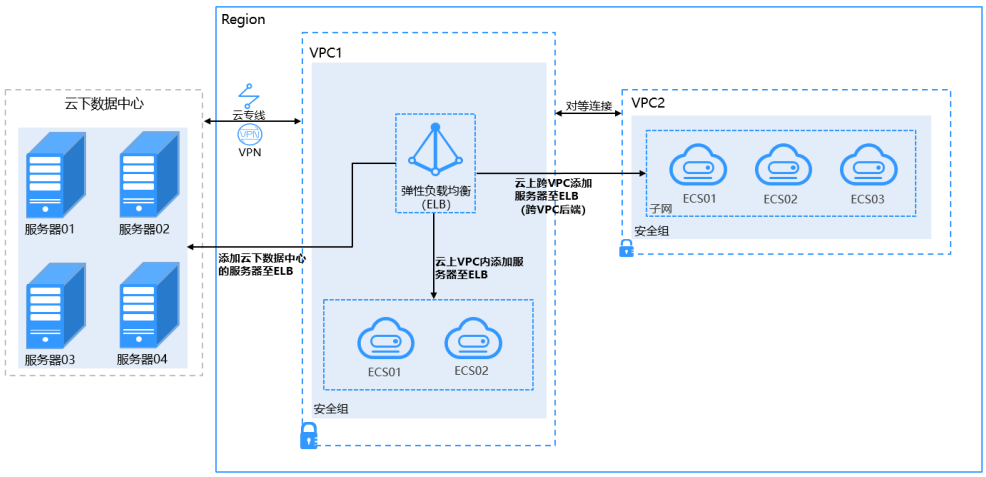
独享型负载均衡实例支持云上云下混合负载均衡的能力，后端服务器组不仅支持直接添加云上同VPC内的实例（比如弹性云服务器和辅助弹性网卡），还支持通过IP类型后端功能添加已实现网络互通的云上其他VPC和云下数据中心（IDC）服务器的IP地址作为后端服务器。

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。

说明

原“跨VPC后端”已更名为“IP类型后端”。

图 1-34 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。
- 在将请求转发至其他VPC的IP地址前，您需确认目标VPC与ELB所在VPC已实现网络连通。
- IP类型后端仅支持添加私网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100,000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。
- 如果监听器关联到UDP协议的后端服务器组，流量路径经过云专线或VPN，并通过IP类型后端进行转发时，健康检查结果可能异常。如果您有此种应用场景，建议提交**工单**进行咨询。

IP 类型后端网络连通指引

通过华为云丰富的网络服务，您可以灵活连通不同VPC之间的网络，包括同区域内VPC的网络，不同区域内VPC的网络，或者不同账号内VPC的网络等。

不同VPC之间网络连通后，通过IP类型后端添加的后端服务器可参与流量负载分发。

网络连通方案详情请参见**VPC网络连接方案概述**。

表 1-65 IP 类型后端网络连通指引

连通场景	网络服务	功能介绍	相关文档
添加云上同一个区域、不同VPC的后端服务器	VPC对等连接	对等连接是建立在两个VPC之间的网络连接，用于连通同一个区域内的VPC，可以实现不同VPC之间的云上内网通信。对等连接可以连通相同账号或者不同账号下的VPC网络。	**连通整个VPC网络的对等连接配置示例**

连通场景	网络服务	功能介绍	相关文档
	企业路由器（ER）	对于同一个区域的VPC，可以在一个企业路由器中接入相同账号或者不同账号下的多个VPC，构建中心辐射型组网。企业路由器可以同时连接多个VPC，相比对等连接，企业路由器更适用于多VPC互联的复杂组网。	通过企业路由器实现同区域VPC互通
添加云上不同区域、不同VPC的后端服务器	云连接（CC） • 云连接实例 • 云连接中心网络	对于不同区域的VPC，不论VPC属于同一个账号还是不同账号，都可以接入云连接中实现内网通信。云连接提供以下两种方案： • 云连接实例：直接将不同区域的VPC接入云连接实例连通网络。 • 中心网络：将同区域的VPC接入企业路由器连通网络，再将不同区域的企业路由器接入中心网络连通跨区域网络。该方案的网络架构扩展性更强，适用于多VPC互联的复杂组网。	• 通过云连接实例实现跨区域VPC互通 • 通过中心网络和企业路由器实现跨区域VPC互通
	虚拟专用网络（VPN）	基于公网，通过VPN的加密通道连通不同区域的VPC。	通过VPN实现跨地域VPC互联
	云专线（DC）	基于物理专线，通过云专线可以连通不同区域的VPC。	通过云专线连通不同区域的VPC网络
添加云下数据中心的后端服务器	虚拟专用网络（VPN）	基于公网，通过VPN的加密通道连通VPC和云下数据中心网络。	通过企业版站点入云VPN实现数据中心和VPC互通
	云专线（DC）	基于物理专线，通过云专线可以连通VPC和云下数据中心网络。	通过云专线实现云下IDC访问云上VPC（虚拟网关VGW）

开启 IP 类型后端

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要开启IP类型后端功能的负载均衡名称。
3. 在“基本信息”页面，单击“开启IP类型后端”。
4. 单击“确定”。

添加 IP 类型后端

1. 进入**后端服务器组列表页面**。

2. 在后端服务器组列表页面，单击需要添加后端服务器的后端服务器组名称。
3. 切换到“后端服务器”页签，选择下方“IP类型后端”页签，并单击“添加”。
4. 填写“IP类型后端IP”、“业务端口”和“权重”。
5. 单击“确定”。

批量导入 IP 类型后端

1. 进入**后端服务器组列表页面**。
2. 在后端服务器组列表页面，单击需要添加后端服务器的后端服务器组名称。
3. 切换到“后端服务器”页签，选择下方“IP类型后端”页签，并单击“添加”。
4. 在“添加IP类型后端”侧拉窗中，单击“导入”。
5. 在“导入”弹窗中，您可单击“下载模板”下载模板文件到本地。
   模板文件需要您填写IP类型后端IP、业务端口和权重。
6. 单击“添加文件”，上传您本地配置完成的导入文件。
   系统将对您导入的文件进行校验。
7. 选中目标添加的IP类型后端，单击“导入”。

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. 进入**后端服务器组列表页面**。
2. 在后端服务器组列表页面，单击需要修改IP类型后端权重的后端服务器组名称。
3. 在该后端服务器组界面，切换到“后端服务器”页签，单击下方“IP类型后端”页签。
4. 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”。
5. 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。
6. 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. 进入**后端服务器组列表页面**。
2. 在后端服务器组列表页面，单击需要移除后端服务器的后端服务器组名称。
3. 切换到“后端服务器”页签，选择下方“IP类型后端”页签。
4. 勾选需要移除的IP类型后端，单击服务器列表上方的“移除”。
5. 在移除后端服务器的对话框中单击“是”。

1.7 健康检查

1.7.1 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**配置健康检查**。

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1-66**。

表 1-66 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、GRPC、TLS
HTTP	TCP、HTTP、HTTPS、GRPC、TLS

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

说明

TLS协议与GRPC协议陆续上线中，已发布区域请以控制台实际为准。

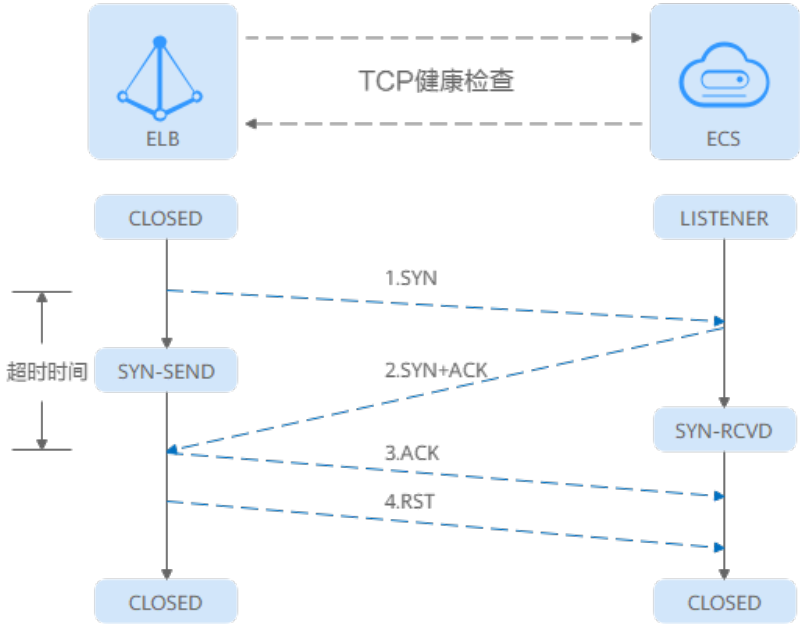
健康检查源 IP

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1-35**所示。

图 1-35 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。

⚠ 注意

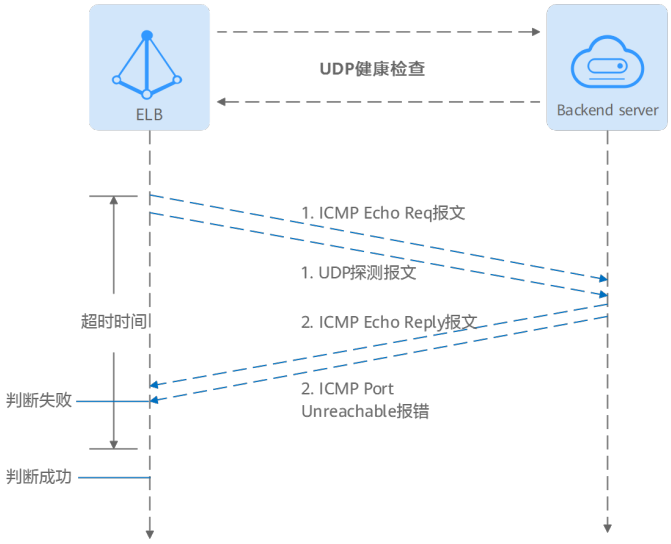
正常的TCP三次握手后，会进行数据传输，但是在健康检查时会发送RST中断建立的TCP连接。该实现方式可能会导致后端服务器中的应用认为TCP连接异常退出，并打印错误信息，如“Connection reset by peer”。解决方案如下：

- 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1-36**所示。

图 1-36 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。

⚠ 注意

- 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。
- UDP探测报文的载荷（ playload ）无实际意义，仅用于填充发送报文时的内容，通常为字符“H”，不建议客户服务端解析该内容。

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1-37所示。

图 1-37 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。

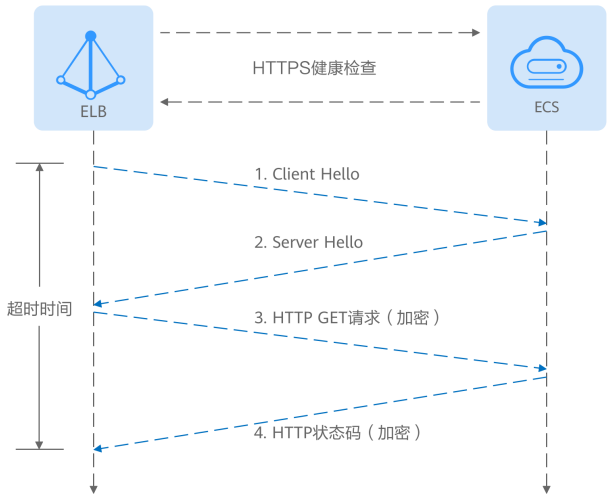
⚠ 注意

- 当独享型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。
- 在HTTP健康检查请求中，User-Agent头字段主要用于标识此类请求为健康检查发出的探测请求。User-Agent的值可能随业务需求而动态调整，建议客户的后端服务请勿根据此header头做检验和判断。
- 当选择“使用后端服务器的内网IP为域名”为健康检查域名时，由于Host请求头可能为空值，建议客户的后端服务请勿根据Host请求头做检验和判断。

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1-38所示。

图 1-38 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。

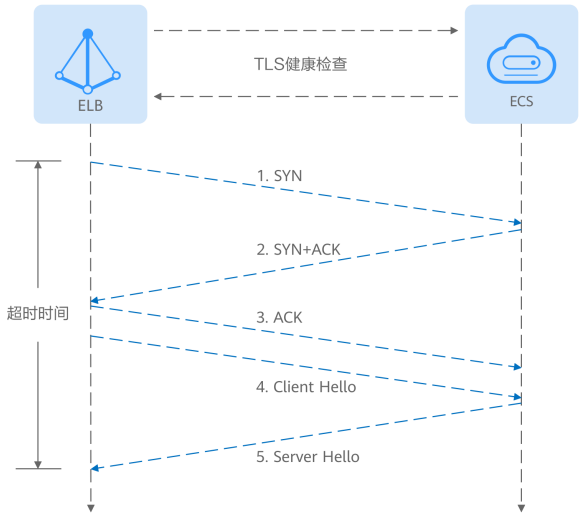
说明

- 在HTTPS健康检查请求中，User-Agent头字段主要用于标识此类请求为健康检查发出的探测请求。 User-Agent的值可能随业务需求而动态调整，建议您的后端服务请勿根据此header头检验和判断。
- 当选择“使用后端服务器的内网IP为域名”为健康检查域名时，建议您的后端服务请勿根据Host请求头做检验和判断。

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 1-39 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 1-40 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1-67中的三个因素决定：

表 1-67 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：

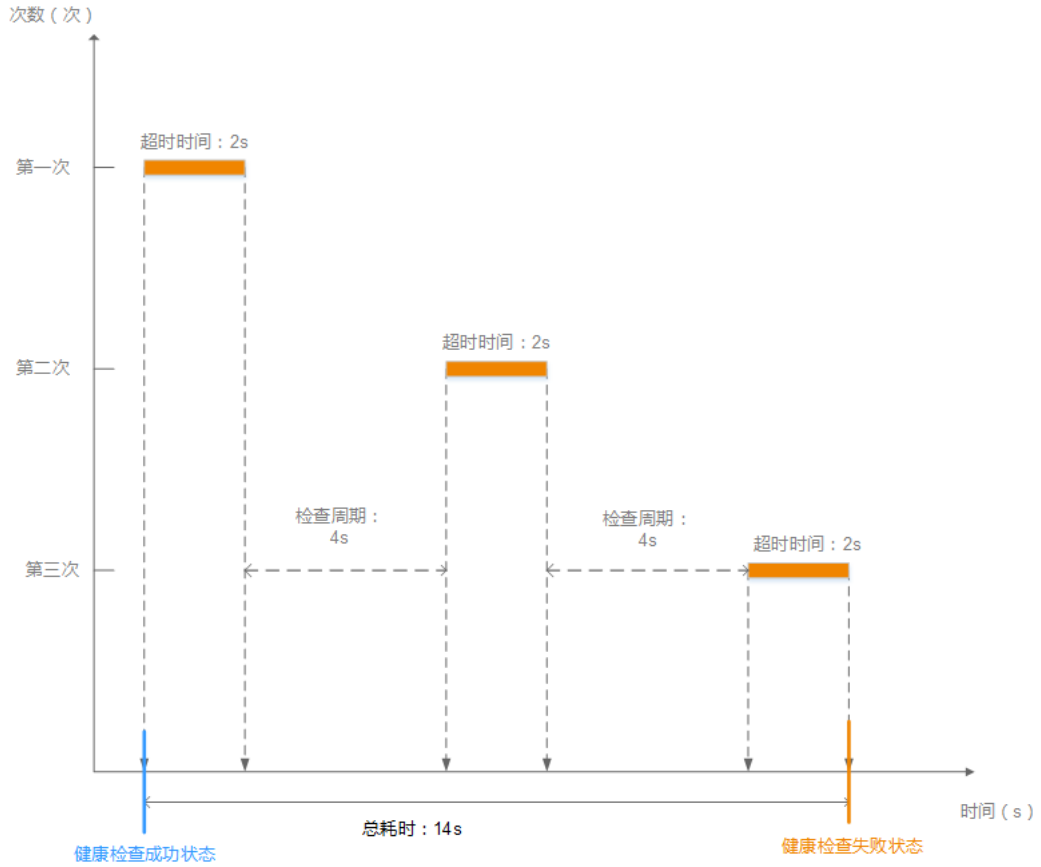
- 健康检查成功时间窗 = 超时时间×健康检查正常阈值 + 检查间隔×(健康检查正常阈值-1)
- 健康检查失败时间窗 = 超时时间×健康检查异常阈值 + 检查间隔×(健康检查异常阈值-1)

如图1-41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 1-41 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**。

1.7.2 配置健康检查

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. 进入**后端服务器组列表页面**。
2. 在后端服务器组列表页面，单击需要修改健康检查的后端服务器组名称。
3. 在后端服务器组的“基本信息”页签下，单击健康检查区域右侧的“配置健康检查”。
4. 在“配置健康检查”弹窗，可根据需要参考**表1-68**进行配置。

表 1-68 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。 **说明** 开启或关闭健康检查期间，监控指标正常主机数/异常主机数会出现短暂波动，一个监控周期后可恢复。	-
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。 独享型支持选择TCP、HTTP、HTTPS、TLS、GRPC协议。	HTTP

参数	说明	示例
健康检查方法	仅关联独享型负载均衡实例使用的后端服务器组支持该参数。 如果健康检查协议选择HTTP/HTTPS/GRPC协议，则该项是必选参数。 健康检查发送请求的方法。 ● GET：采用GET方法发送健康检查请求，后端服务器返回全部信息。 ● HEAD：采用HEAD方法发送健康检查请求，后端服务器仅返回 HTTP 头部信息，提升请求效率。 请确保您的后端服务器支持HEAD请求，否则可能会导致健康检查失败，此时可以使用GET方法来进行健康检查。 ● POST：采用POST方法发送健康检查请求。 请确保您的后端服务器支持POST请求，否则可能会导致健康检查失败，此时可以使用GET方法来进行健康检查。 **说明** ● 健康检查协议为HTTP和HTTPS协议时，支持GET方法和HEAD方法。 ● 健康检查协议为GRPC协议时，支持GET方法和POST方法。 ● 支持设置健康检查方法的功能陆续上线中，请以控制台实际为准。	GET
健康检查协议版本	如果健康检查协议选择HTTP/HTTPS/GRPC/TCP/TLS协议，则该项是必选参数。 选择健康检查HTTP协议版本。 ● 默认支持“根据监听器自动选择”，即： – 使用TCP监听器时，默认使用HTTP1.0版本。 – 使用HTTP/HTTPS/QUIC/TLS监听器时，默认使用HTTP1.1版本。 ● 支持您选择“HTTP1.0”或“HTTP1.1”版本。	根据监听器自动选择

参数	说明	示例
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，字符串间以点分隔，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。 ● 默认**使用后端云服务器的业务端口**进行健康检查。 ● 支持**指定特定端口**进行健康检查。	80
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]。 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

参数	说明	示例
是否开启内容校验	如果健康检查协议选择TCP/UDP协议，则支持开启内容校验，然后在**请求发送内容**中输入定义请求内容（例如**TargetID**），在**响应校验内容**中输入预期返回的校验结果（例如**elbResponse**）。 同时，您需要在后端服务器部署的应用中加入对应的内容校验逻辑，例如收到**TargetID**的请求时，返回**elbResponse**。当elb实例收到后端服务器返回的信息与响应校验内容一致时，判定健康检查成功，否则健康检查失败。 如果开启内容校验，您需进行如下配置： ● 校验内容格式：支持选择**ascii字符**或**十六进制**格式。 – **ascii字符**：长度限制为1-64个字符，包括所有的可显示ascii字符。 – **十六进制**：长度限制为2-64个字符，只能为偶数位，不限大小写。 ● 请求发送内容：健康检查报文将发送的报文。 ● 响应校验内容：预期收到的健康检查响应报文，如果未收到对应响应，健康检查结果将判断为异常。 **说明** 支持设置内容校验的功能陆续上线中，请以控制台实际为准。	-
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

参数	说明	示例
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

5. 单击“确定”。

关闭健康检查

1. 进入**后端服务器组列表页面**。
2. 在后端服务器组列表页面，单击需要关闭健康检查的后端服务器组名称。
3. 在后端服务器组的“基本信息”页签下，单击健康检查区域右侧的“配置健康检查”。
4. 在“配置健康检查”界面，可根据需要关闭健康检查。
5. 单击“确定”。

相关文档

- **健康检查异常诊断**
- **其他自助问题诊断**
- **健康检查异常排查（独享型）**

1.8 安全管理

1.8.1 独享型 ELB 获取客户端真实 IP

获取客户端 IP 功能概述

对于独享型ELB实例，“获取客户端IP”功能在四层监听器和七层监听器的实现方法存在不同。

- 四层协议监听器（TCP/UDP）默认支持“获取客户端IP”功能，ELB实例与后端服务器之间直接使用客户端真实的IP地址通信，通过后端服务器的日志记录便可获取客户端的真实IP。

- 七层协议监听器（HTTP/HTTPS/QUIC）默认支持“获取客户端IP”功能，即支持通过X-Forwarded-For字段传递客户端的真实IP，X-Forwarded-For字段记录的第一个IP地址即为客户端真实IP。
- TLS监听器不支持“获取客户端IP”功能，您可以开启ProxyProtocol功能来获取客户端真实IP。

注意事项

监听器支持“获取客户端IP”功能后：

- 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。
- 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）。后端服务器迁移完成后，需要通过报文重传来恢复流量。

四层监听获取客户端真实 IP

部分特殊场景，四层监听器的“获取客户端IP”功能失效，您可以参考**表1-69**。

更多详情，您可以参考**在四层独享型ELB转发下获取客户端真实IP**。

表 1-69 四层监听获取客户端真实 IP 方法总结

监听器	“获取客户端IP”功能	“获取客户端IP”功能失效场景	其他方法
TCP监听器	支持	• 与IP类型后端通信。 • 开启IPv4/IPv6地址转换开关后，客户端IP地址发生转换。	• 通过**TOA插件**获取客户端真实IP（仅支持IPv4场景） • **通过ProxyProtocol协议获取客户端真实IP**
UDP监听器	支持	• 与IP类型后端通信。 • 开启IPv4/IPv6地址转换开关后，客户端IP地址发生转换。	不涉及
TLS监听器	不支持	不涉及	**通过ProxyProtocol协议获取客户端真实IP**

七层监听获取客户端真实 IP

您需要对后端服务器进行配置，确保服务器可以正确解析X-Forwarded-For字段以获取客户端的真实IP。

X-Forwarded-For字段格式如下：

```
X-Forwarded-For: <请求客户端真实IP, 代理服务器1-IP, 代理服务器2-IP, ...>
```

使用此方式获取客户端真实IP时，获取的第一个IP地址就是客户端真实IP。

更多详情，您可以参考**在七层独享型ELB转发下获取客户端真实IP**。

相关文档

- 在控制台添加以下监听器时：“获取客户端IP”功能开关默认打开，且不支持关闭。
  - 网络型：**添加TCP监听器**、**添加UDP监听器**、**添加后端为QUIC协议的UDP监听器**。
  - 应用型：**添加HTTP监听器**、**添加HTTPS监听器**、**添加QUIC监听器**。
- **创建监听器**接口：transparent_client_ip_enable只支持设置为true，默认支持获取客户端IP功能。

1.8.2 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和TLS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 1-70 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 1-71 安全策略差异说明（TLS 协议）

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
Protocol-TLS 1.3	×	×	×	×	×	√	√	√	×	×
Protocol-TLS 1.2	√	√	√	√	√	√	√	√	√	√
Protocol-TLS 1.1	√	√	×	√	×	√	×	×	√	×
Protocol-TLS 1.0	√	×	×	√	×	√	×	×	×	×

表 1-72 安全策略差异说明（加密套件）

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

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-ECDSA-AES256-SHA	√	√	√	√	×	√	×	×	√	×
ECDHE-RSA-AES128-GCM-SHA256	×	×	×	√	×	√	√	√	√	×
TLS_AES_256_GCM_SHA384	×	×	×	×	×	√	√	√	×	×
TLS_CHACHA20_POLY1305_SHA256	×	×	×	×	×	√	√	√	×	×
TLS_AES_128_GCM_SHA256	×	×	×	×	×	√	√	√	×	×
TLS_AES_128_CCM_8_SHA256	×	×	×	×	×	√	√	√	×	×
TLS_AES_128_CCM_SHA256	×	×	×	×	×	√	√	√	×	×
DHE-RSA-AES128-SHA	×	×	×	√	×	×	×	×	×	×
DHE-DSS-AES128-SHA	×	×	×	√	×	×	×	×	×	×
CAMELLIA128-SHA	×	×	×	√	×	×	×	×	×	×
EDH-RSA-DES-CBC3-SHA	×	×	×	√	×	×	×	×	×	×
DES-CBC3-SHA	×	×	×	√	×	×	×	×	×	×
ECDHE-RSA-RC4-SHA	×	×	×	√	×	×	×	×	×	×

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

表 1-73 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	√	√	√	√	×	√	×	×	×	×

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
IE 8-10 / Win 7	√	√	√	√	×	√	×	×	×	×
IE 11 / Win 7	√	√	√	√	√	√	√	√	√	√
IE 11 / Win 10	√	√	√	√	√	√	√	√	√	√
Edge 15 / Win 10	√	√	√	√	√	√	√	√	√	√
Edge 16 / Win 10	√	√	√	√	√	√	√	√	√	√
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. 进入**弹性负载均衡列表页面**。
2. 单击页面左边的“TLS安全策略”。
3. 在TLS安全策略页面，单击页面右上角的“创建自定义策略”。
4. 配置自定义策略参数，参数说明参见**表1-74**。

表 1-74 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
企业项目	创建自定义策略时，可以将其加入已启用的企业项目。 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。
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（可选）	自定义策略相关信息的描述说明。

5. 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. 进入**弹性负载均衡列表页面**。
2. 单击页面左边的“TLS安全策略”。
3. 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“。
4. 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1-74**。
5. 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. 进入**弹性负载均衡列表页面**。
2. 单击左侧导航栏的“TLS安全策略”。
3. 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“。
4. 在确认删除弹窗，单击“确定“。

为 HTTPS 监听器添加安全策略

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要创建安全策略的监听器的负载均衡器名称。
3. 在该负载均衡界面的“监听器”区域，单击“添加监听器”。
4. 在“添加监听器”界面，前端协议选择“HTTPS”。
5. 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**。
6. 配置完成，单击“确定”。

为 HTTPS 监听器修改安全策略

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要修改安全策略的监听器的负载均衡器名称。
3. 切换至“监听器”页签，单击需要修改安全策略的监听器名称。
4. 在监听器的基本信息页面，单击“编辑监听器”。
5. 在“编辑监听器”界面，展开高级配置，选择安全策略参数。
6. 单击“确定”。

1.8.3 开启 SNI 证书实现多域名访问

SNI（Server Name Indication 服务器名称指示）是一种TLS协议的扩展，用于解决在一个监听器托管多个域名时，需要根据不同的请求域名匹配证书进行认证的问题。

SNI 概述

当您需要在同一个监听器上部署多个HTTPS后端服务时，每个服务可能使用不同的域名和证书，并需要将请求分发至不同的后端服务器组。

如果HTTPS监听器只绑定一个服务器证书，监听器将无法根据客户端请求的域名动态选择对应的证书进行认证，导致多域名场景认证异常。

开启SNI功能支持您扩展监听器上配置的证书，实现监听器根据请求域名的不同自动选择匹配的证书传递到客户端进行认证。客户端在发起SSL握手请求时提交请求的域名信息，ELB在收到请求后根据请求的域名查找对应的证书，如果监听器没有匹配到域名对应的证书，ELB将使用默认的服务器证书进行认证。

SNI 证书

- SNI证书是用于多域名认证场景的**服务器证书**，即指定了**SNI扩展域名**的服务器证书。在ELB控制台指定的**SNI扩展域名**必须与证书实际支持认证的域名保持一致。

- 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。在选择认证证书时，如果同域名绑定了两个证书，ELB会优先选择ECC类型的证书。

约束与限制

- 仅HTTPS和TLS 监听器，支持开启SNI功能。开启SNI后，您需要为监听器配置至少一个SNI证书，如果您需要新建证书可参照**创建证书**。
- 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，详情请见**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调整为50个SNI证书，如您有需求，可提交**工单**进行处理。

证书匹配规则

- 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。

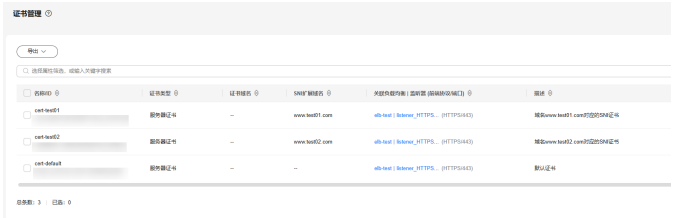
  且依据最长尾缀匹配：当证书中的域名同时存在*.b.test.com和*.test.com时，那么a.b.test.com会优先匹配到*.b.test.com。

- cert-default为创建HTTPS监听器时绑定的默认服务器证书，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，则会使用SNI证书认证鉴权。如果匹配失败，则会使用默认的服务器证书认证鉴权。

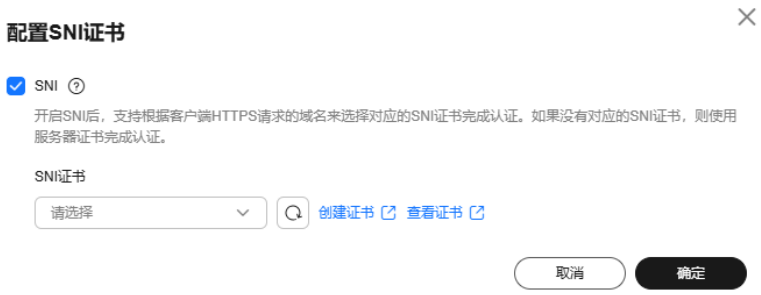
图 1-42 配置证书说明



监听器开启 SNI

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击负载均衡名称。
3. 在“监听器”页签，单击需要开启SNI的监听器名称。
4. 在监听器基本信息页面，单击SNI右侧“配置”。
5. 开启SNI的开关，选择需要配置的SNI证书。

图 1-43 配置 SNI 证书



6. 单击“确定”。

相关文档

- 创建证书
- 添加TLS监听器
- 添加HTTPS监听器

1.8.4 证书管理

1.8.4.1 证书概述

在弹性负载均衡服务配置单向认证或双向认证时，您需要为HTTPS或TLS监听器配置证书。弹性负载均衡证书管理控制台支持获取您在华为云云证书与管理服务中统一管理的SSL服务器证书，也支持您上传您本地拥有的证书。

证书使用场景

当您为弹性负载均衡添加HTTPS或TLS监听器来转发业务请求时，您需要选择SSL解析认证方式。单向认证需要为监听器配置服务器证书，双向认证需要同时配置服务器证书和CA证书。

表 1-75 SSL 解析方式

单向认证	仅客户端对服务器端进行认证，您需要为监听器绑定服务器证书，用于验证服务器身份。
双向认证	弹性负载均衡实例与客户端互相提供身份认证，从而允许通过认证的用户访问实例。您需要为监听器绑定服务器证书和CA证书，分别用于验证服务器和客户端的身份，后端服务器无需额外配置双向认证。

弹性负载均衡支持创建三种类型的证书，服务器证书、CA证书、服务器SM双证书。

表 1-76 证书类型

服务器证书	在使用HTTPS或TLS协议时，服务器证书用于SSL握手协商过程验证服务器的身份，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签发机构的身份。在配置双向认证功能时，只有当客户端能够出具指定CA签发的证书时，才能成功建立连接。
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。 ● **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

服务器SM双证书持续上线中，请以控制台实际为准。

视频介绍

本视频介绍在ELB服务中如何管理证书。

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-----
```

格式转换

弹性负载均衡仅支持PEM格式的证书，其它格式的证书需要转换成PEM格式后，才能上传到弹性负载均衡服务。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
```

1.8.4.2 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：在使用HTTPS协议时，服务器证书用于SSL握手协商。同时支持云证书与管理服务提供的服务器数字证书和您的自有证书。
- 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。仅支持上传您的自有CA证书。
- 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，当前不支持SM双证书的证书链。同时支持云证书与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. 进入**弹性负载均衡列表页面**。
2. 在左侧导航栏单击“证书管理”。
3. 单击“创建证书”，配置参数请参见**表1-77**。

表 1-77 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。

参数	说明
证书来源	服务器证书同时支持云证书与管理服务中SSL证书管理提供的数字证书和您的自有证书。 ● SSL证书管理：云证书与管理服务中统一管理的SSL服务器数字证书，您需要到云证书与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** 推荐使用云证书与管理服务对您的证书进行统一管理。
证书	仅云证书与管理服务中SSL证书管理提供的证书支持该参数。 选择您在云证书与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，只能由中文、英文字母、数字、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。
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-----
SNI扩展域名（可选）	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。

4. 单击“确定”，完全创建。

创建 CA 证书

1. 进入**弹性负载均衡列表页面**。
2. 在左侧导航栏单击“证书管理”。
3. 单击“创建证书”，配置参数请参见**表1-78**。

表 1-78 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。 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。

4. 单击“确定”，完全创建。

创建服务器 SM 双证书

1. 进入**弹性负载均衡列表页面**。
2. 在左侧导航栏单击“证书管理”。
3. 单击“创建证书”，配置参数请参见**表1-79**。

表 1-79 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，当前不支持SM双证书的证书链。

参数	说明
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。 ● SSL证书管理服务：云证书与管理服务中统一管理的SSL服务器数字证书，您需要到云证书与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** 推荐使用云证书与管理服务对您的证书进行统一管理。
证书	仅SSL证书管理的证书支持该参数。 支持选择您在云证书与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-----
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-----

参数	说明
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。

1.8.4.3 管理证书

在日常的业务运维中，您可以根据实际需求在ELB控制台对您的证书进行更新或删除，确保业务的安全性和连续性。

快速查询证书关联的监听器

1. 进入**证书管理列表页面**。
2. 在证书列表中，在“关联负载均衡丨监听器 (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“关联负载均衡丨监听器 (前端协议/端口)”所在列，单击“查看所有”，即可查看证书关联的所有监听器。

为证书配置修改保护

您可以对证书开启修改保护功能，防止因误操作导致证书的配置被修改或证书被删除。开启证书修改保护后，您无法对证书执行修改或删除操作。将证书绑定至监听器和从监听器解绑等操作仍可正常进行，不受影响。

说明

证书支持修改保护功能陆续上线中，已发布区域请以控制台实际开放为准。

1. 进入**证书管理列表页面**。
2. 在证书列表中，在需要修改的证书所在行的修改保护列，单击“设置”。
3. 在“设置修改保护”对话框中，开启修改保护的开关并填写“添加修改保护原因”。
4. 单击“确定”，完成配置。

修改证书信息

1. 进入**证书管理列表页面**。
2. 在证书列表中，在需要修改的证书所在行，单击“修改”。
3. 在“修改证书”对话框中，修改证书的相关信息。
4. 确认修改信息，单击“确定”，完成修改。

删除证书

您可以删除不再使用的证书，ELB服务已支持进行批量删除证书操作，便于提高您对证书的管理效率。

已被监听绑定使用的证书，无法执行删除操作，请先为关联监听器执行**通过编辑监听器更换证书**操作。

1. 进入**弹性负载均衡列表页面**。
2. 在左侧导航栏单击“证书管理”。
3. 您可以删除单个证书，也可以同时删除多个证书：
   a. **删除单个证书**：
      i. 在证书列表中，在需要修改的证书所在行，单击“删除”。
      ii. 在确认对话框中单击“确定”，完成删除。
   b. **删除多个证书**：
      i. 在证书列表中，勾选多个需要删除的证书。
      ii. 单击证书列表上方的“删除”按钮。
      iii. 在“删除证书”的侧拉窗中，输入“DELETE”。
      iv. 单击“确定”，完成删除。

1.8.4.4 绑定/更换证书

操作场景

通过证书对通信双方进行身份认证广泛用于对数据安全高要求的业务场景，当证书过期或有其他原因需要更换时，如果配置不当，可能会影响实际业务运行。

您可以参考本章节对监听器进行绑定证书和更换证书的操作。如果其他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/TLS/QUIC协议的监听器才支持配置证书。
- 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

添加HTTPS/TLS/QUIC监听器时可以绑定证书。详情见：

- **添加HTTPS监听器**。
- **添加TLS监听器**
- **添加QUIC监听器**

通过编辑监听器更换证书

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要更换监听器证书的负载均衡名称。
3. 在“监听器”页签下，单击目标监听器所在行操作列的“编辑”。
4. 在“服务器证书”或“CA证书”下选择需要更换的证书。
5. 在“编辑监听器”对话框中，单击“确定”。

1.8.4.5 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，从而简化证书管理操作流程，提高运维效率。

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/QUIC协议的监听器才支持绑定/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。

通过修改证书批量更换监听器的证书

1. 进入**弹性负载均衡列表页面**。
2. 在左侧导航栏单击“证书管理”。
3. 在证书列表中，在需要修改的证书所在行，单击“修改”。
4. 在“修改证书”对话框中，修改证书的相关信息。
5. 确认修改信息，单击“确定”，完成修改。

1.8.5 访问控制管理

1.8.5.1 访问控制策略

当您需要对客户端访问ELB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。

说明

负载均衡器的IP地址不受所在子网的网络ACL规则限制，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。

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ELB绑定的IP地址。
- 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

警告

当您修改访问控制策略前，请您务必了解该操作可能带来的影响，避免误操作造成网络中断或者引入不必要的网络安全问题。

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击负载均衡名称，进入监听器管理界面。
3. 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”。
4. 在“设置访问控制”的弹窗中，如**表1-80**所示配置访问控制。

表 1-80 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**。 最多支持选择5个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。

5. 配置完成，单击“确定”。

相关文档

- **访问控制IP地址组**
- API操作：
  - **创建IP地址组**
  - **更新IP地址组的IP列表项**

1.8.5.2 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。
- 单监听器的访问控制策略，最多支持选择5个IP地址组。IP地址组内合计最多可添加300个IP地址或网段。

说明

如果您希望扩大IP地址组支持添加的地址或网段数量，可以提交**工单**进行处理。

创建 IP 地址组

1. 进入**弹性负载均衡列表页面**。
2. 在左侧导航栏，选择“ 弹性负载均衡 > IP地址组”。
3. 在“IP地址组”界面，单击“创建IP地址组”。
4. 配置IP地址组参数，参数说明参见**表1-81**。

表 1-81 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》**。	-
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、一个网段或连续地址段，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。	-

5. 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1-81**。

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. 进入**弹性负载均衡列表页面**。
2. 在左侧导航栏，选择“ 弹性负载均衡 > IP地址组”。
3. 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。
4. 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。
5. 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. 进入**弹性负载均衡列表页面**。
2. 在左侧导航栏，选择“ 弹性负载均衡 > IP地址组”。
3. 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

如果您希望批量删除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. 进入**弹性负载均衡列表页面**。
2. 在左侧导航栏，选择“ 弹性负载均衡 > IP地址组”。
3. 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。
4. 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。
5. 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. 进入**弹性负载均衡列表页面**。
2. 在左侧导航栏，选择“ 弹性负载均衡 > IP地址组”。
3. 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。
4. 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. 进入**弹性负载均衡列表页面**。
2. 在左侧导航栏，选择“ 弹性负载均衡 > IP地址组”。
3. 在“IP地址组”界面，需要删除的IP地址组所在行，单击“删除”。
4. 确认需要删除的IP地址组，单击“确定”。

1.8.6 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 1-44 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 1-45 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 1-46 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 1-47 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 1-48 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?

1.9 ELB 接入访问日志

当您通过ELB的HTTP/HTTPS/QUIC/TLS监听器对外提供业务负载时，如果后端服务器出现突发异常，通过逐一排查后端服务器的日志进行分析，难以快速定位问题根因。

弹性负载均衡ELB支持将七层监听器转发的业务接入云日志服务进行分析，云日志将记录包括请求时间、客户端IP地址、请求路径和服务器响应等信息。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，快速定位出异常的后端服务器。

警告

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。

什么是 ELB 访问日志

弹性负载均衡是接收和分发客户端访问请求的入口，ELB的七层访问日志记录了传输请求的详细信息，通过接入云日志服务，结合云日志服务提供的分析能力，您可以快速地对ELB分发的业务请求进行分析和问题定位。

ELB的访问日志记录了以下几类信息：

- 时间信息：如msec和time_iso8601等字段记录了请求的时间，用于对请求进行时序分析、故障时间定位。
- 客户端请求基础信息：如remote_addr:remote_port、request_method scheme://host request_uri server_protocol和http_user_agent等字段记录了请求的基础信息，用于对请求进行用户分析和安全审计。

- 请求响应与性能指标：如status、bytes_sent和request_time等字段记录了响应状态和处理时间等信息，用于请求状态定位和性能监控。
- 负载均衡器信息：如lb_name、listener_id、pool_name和eip_address:eip_port等字段记录了处理请求的ELB实例配置，用于识别处理请求的资源配置，提升运维效率。
- 后端服务器信息：如upstream_status、upstream_connect_time和upstream_addr_priv等字段记录了后端服务器返回请求的信息和后端服务器配置，用于识别后端服务器的健康状态和性能分析。
- HTTPS相关信息：如ssl_protocol、sni_domain_name和certificate_id等字段记录了HTTPS协议相关信息，用于排查HTTPS请求。
- 其他辅助信息：access_log_topic_id、log_ver和tenant_id等字段记录了系统和日志标识等信息，用于日志管理。

费用说明

ELB接入云日志后，云日志服务根据日志读写流量、日志存储量、日志转测的流量等计费，云日志服务的详细计费信息请参考**云日志服务的计费项**。

约束与限制

- 仅采用HTTP/HTTPS/QUIC/TLS监听器的负载均衡实例支持配置访问日志。
- 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。

准备工作

- 创建支持HTTP/HTTPS/QUIC/TLS协议的负载均衡器。具体操作，请参见**购买独享型负载均衡器**。
- 开通云日志服务。具体操作，请参见**开始使用云日志服务**。
- 创建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**。
- 在ELB中创建HTTP/HTTPS/QUIC/TLS监听器。

配置访问日志

1. 进入**弹性负载均衡列表页面**。
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”。

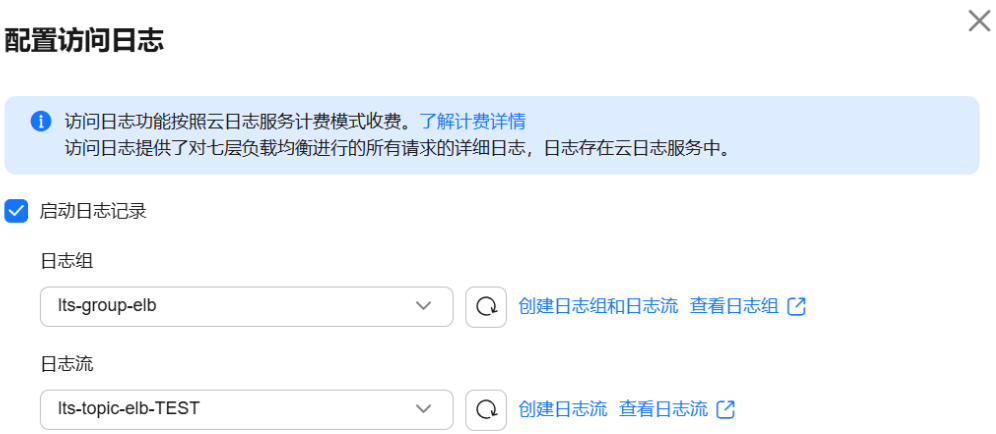
图 1-49 配置访问日志入口

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。
   如果您尚未在云日志服务创建日志组和日志流，可以在ELB服务控制台进行创建。
   单击查看创建日志组和日志流详情
   a. 单击“创建日志组和日志流”。
   b. 在“创建日志组&日志组”侧拉窗中，设置日志组名称、日志流名称和日志存储时间。

   图 1-50 在 ELB 服务控制台创建日志组和日志流

   c. 单击“确定”，完成日志组和日志流的创建。

   图 1-51 启动日志记录



5. 单击“确定”，配置完成。

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：进入目标ELB实例详情页的**访问日志**页签，即可查看访问日志。
- “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 $request_header_length
$actions_executed $error_reason "$pool_usr_name"
```

日志示例如下：

```
1644819836.370 eb11c5a9-93a7-4c48-80fc-03f61f638595 [2024-02-14T14:23:56+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 "-" 129 waf - "我的后端服务器组"
```

日志示例分析：

在[2024-02-14T14:23:56+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。

日志示例分析结果：

后端服务器正常响应请求。

详细的日志字段说明如**表1-82**。

表 1-82 ELB 日志字段说明

参数	描述	取值说明	示例
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。	-	[2024-02-14T14:23:56+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

参数	描述	取值说明	示例
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
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"

参数	描述	取值说明	示例
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）
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_20679192-8888-4e62-a814-a2f870f62148

参数	描述	取值说明	示例
listener_id	监听器在ELB服务内部的ID。	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”或“pool_”+“后端服务器组ID*负载均衡器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
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

参数	描述	取值说明	示例
self_defined_header	该字段为保留字段，默认为“-”。	字符串	"-"
request_header_length	客户端请求的header头大小。	整型数据	129
actions_executed	waf的执行结果。	字符串 ● waf：请求waf成功。 ● waf-failed ：请求waf失败。 ● waf-block：请求被waf拦截。	waf

参数	描述	取值说明	示例
error_reason	请求waf失败的原因。	字符串 • WAFUnhandledException：异常内部错误，需要联系业务定位。 • WAFRequestHeaderLengthExceeded：客户端请求头超过限制。 • WAFRequestBodyLengthExceeded：客户端body体过大。 • WAFRequestHeaderContentLengthEmpty：客户端body体长度为0 • WAFResponseBodyReadError：读取waf返回的body error。 • WAFResponseReadTimeout：读取waf返回的结果超时 • WAFConnectionTimeout：连接waf超时。 • WAFConnectionError： 连接waf失败。 • WAFNoBackendAvailable：waf没有可用后端。 • WAFNoBackendOnline：waf没有后端在线。	-
pool_usr_name	后端服务器组的名称	字符串	"我的后端服务器组"

记录自定义 header

除了常用的header字段外，ELB支持您通过all_headers字段记录请求中其他header的值，可以更完整地记录日志，增强ELB日志与实际业务的关联性。

- **推荐使用场景**
  - 问题快速定位与追踪：在复杂业务系统中，仅通过ELB提供的默认日志信息（如 IP、URL、状态码）难以关联具体业务上下文时，添加额外参数辅助分析。
  - 安全合规性与审计追溯：部分行业（如医疗、金融）有严格的合规要求，需日志记录特定业务信息以满足监管审计。
- **约束与限制**
  - 针对同一个header参数，拦截操作的优先级更高，拦截操作仅针对需要打印的header信息生效。
  - 自定义header不会记录以下字段信息：host、user-agent、referer、x-forwarded-for、x-clienttraceid、traceparent。
  - 访问日志自定义header的长度默认支持1KB，支持提升至4KB，如果您有使用需求可以提工单申请。
- **操作步骤**

  a. 在负载均衡实例的“访问日志”页签下，单击记录自定义header下方的“查看/编辑”。

  b. 在记录自定义header侧拉窗中，选择要添加记录自定义header的监听器。

  如果您需要为多个监听器记录自定义header，您可以单击侧拉窗左上方的“添加”。

  c. 在“打印的header信息”列，单击“全部”或“自定义”。

  i. **全部**：ELB的日志将会记录所有的header信息。

  ii. **自定义**：ELB的日志仅记录您写入的header信息。选择“自定义”后，您需要在下方的输入框中，输入您希望记录的header字段。

  d. 如果您不希望日志中记录某些header信息，您也可以通过输入“拦截的header信息”，对header信息进行拦截。

  在“拦截的header信息”下方的输入header信息后，ELB日志将不会记录对应的字段。

  e. 单击“确定”。

定位异常后端服务器

筛选异常日志如下：

```
1554944564.344 - [2024-04-11T09:02:44+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 [2024-04-11T09:02:44+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（私网IP地址为172.17.0.82:3000）异常，不能正常响应请求。

相关文档

- 最佳实践：**通过ELB的访问日志查询客户端请求源IP**。
- 如果您希望将日志转储进行二次分析，您可以配置日志转储，详情请参考**日志转储**。
- 如果您希望对ELB的日志数据进行统一管理，请参考如下文档：
  - 在云日志控制台接入LTS：**弹性负载均衡 ELB接入LTS**。
  - AOM支持创建日志指标规则，将ELB上报到LTS的日志数据提取为指标来统一管理，便于后续在指标浏览、仪表盘界面实时监控。通过接入AOM，您可以对日志进行统计，支持以下统计类型：count、countKeyword、sum、avg、max、min、P50、P75、P90、P95和P99，详情请参见**配置日志指标接入AOM**。
- API操作：**创建云日志**、**查询云日志详情**。

高频问题

如何对 ELB 的日志进行 P99 指标监控?

您可以通过将ELB的访问日志接入应用运维管理 AOM服务实现对日志进行指标监控，详情请参见**配置日志指标接入AOM**。

1.10 资源和标签

1.10.1 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。

当您为独享型ELB绑定了关联资源使用时，支持同步编辑关联资源标签，这些资源统一进行管理。为ELB编辑标签时，勾选的关联资源标签会随着弹性负载均衡标签同步编辑。受关联资源服务自身标签的影响，同步效果可能会受影响，请以实际结果为准。

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**购买独享型负载均衡器**。
- 给已创建的负载均衡器添加标签。
  a. 进入**弹性负载均衡列表页面**。
  b. 在“负载均衡器”界面，单击已创建的负载均衡器名称。

c. 在“标签”页签下，单击“添加标签”，输入“键”和“值”。
标签的“键”和“值”是一一对应的，其中“键”值是唯一的。
d. 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。

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. 进入**弹性负载均衡列表页面**。
2. 在“负载均衡器”界面，单击已创建的负载均衡器名称。
3. 切换到监听器页签，单击需要添加标签的监听器名称。
4. 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”。
标签的“键”和“值”是一一对应的，其中“键”值是唯一的。
5. 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。

修改标签

1. 进入**弹性负载均衡列表页面**。
2. 在“负载均衡器”界面，单击需要修改标签的负载均衡器名称。
3. 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。

4. 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. 进入**弹性负载均衡列表页面**。
2. 在“负载均衡器”界面，单击需要删除标签的负载均衡器名称。
3. 在“标签”页签下，在需要删除的标签所在行，单击 "删除"。
4. 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。

1.10.2 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 1-52 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 1-53 我的配额

3. 在页面右上角，单击“申请扩大配额”。

图 1-54 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”。

设置配额预警

弹性负载均衡的配额项支持设置配额预警，当配额达到预警阈值时，您会收到告警通知，方便您提前申请提升配额。

创建了配额预警后，系统会根据预先设置的预警阈值每小时审计一次，若超过预警阈值则会发送预警消息。预警消息的发送需间隔24小时，若发送预警消息后24小时内，再次超过预警阈值，则不会再次发送预警消息。

1. 登录华为云首页。
1. 单击页面右上角的“管理控制台”。
2. 系统进入“管理控制台”页面。
3. 单击管理控制台左上角的 ，选择区域和项目。
4. 在页面右上角，选择“资源 > 我的配额”。

5. 单击左侧“配额预警”，系统进入“配额预警”页面。
6. 您可以在“配额预警”页面，单击“设置预警”。
7. 对各项资源配置预警阈值、预警区域参数。
8. 打开“发送通知”，设置“通知对象”。
9. 设置完成后，单击“保存”。

1.11 使用 CES 监控 ELB

1.11.1 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. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页，单击需要查看监控指标的负载均衡器名称。
3. 支持查看“负载均衡器”、“监听器”和“后端服务器组”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。
   c. 后端服务器组粒度：切换到“监控”页签，监控粒度选择“后端服务器组”进行查看。

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 ”，在右侧页面选择“弹性负载均衡 ELB”。
5. 在“云服务监控详情页”单击需要查看监控指标的负载均衡器名称。
   或者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**。

1.11.2 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

负载均衡器的监控指标

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。

说明

与七层业务相关的监控指标仅支持协议：HTTP/HTTPS/QUIC/GRPC。

表 1-83 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	单位	进制	测量对象（维度）	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连接的个数。 在七层负载均衡器中，指从客户端到ELB建立的所有TCP连接的个数。	≥ 0	Count	不涉及	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活跃TCP和UDP连接的个数。 Windows和Linux服务器都可以使用如下命令查看。 `netstat -an`	≥ 0	Count	不涉及	独享型负载均衡器	1分钟
m3_inact_conn	非活跃连接数	从测量对象到后端服务器建立的非活跃TCP和UDP连接的个数。 Windows和Linux服务器都可以使用如下命令查看。 `netstat -an`	≥ 0	Count	不涉及	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。	≥ 0	Count/s	不涉及	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数据包的个数。	≥ 0	Count/s	不涉及	独享型负载均衡器	1分钟
m6_out_pps	流出数据包数	测量对象每秒发出数据包的个数。	≥ 0	Count/s	不涉及	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	单位	进制	测量对象（维度）	监控周期（原始指标）
m7_in_Bps	网络流入速率	从外部访问测量对象的网络速率。	≥ 0	**Byte/s**	1000(SI)	独享型负载均衡器	1分钟
m8_out_Bps	网络流出速率	测量对象访问外部的网络速率。	≥ 0	**Byte/s**	1000(SI)	独享型负载均衡器	1分钟
m9_abnormal_servers	异常主机数	测量对象中健康检查异常的后端服务器个数。	≥ 0	Count	不涉及	独享型负载均衡器	1分钟
ma_normal_servers	正常主机数	测量对象中健康检查正常的后端服务器个数。	≥ 0	Count	不涉及	独享型负载均衡器	1分钟
m22_in_bandwidth	入网带宽	测量对象入网带宽。	≥ 0	bit/s	1000(SI)	独享型负载均衡器	1分钟
m23_out_bandwidth	出网带宽	测量对象出网带宽。	≥ 0	bit/s	1000(SI)	独享型负载均衡器	1分钟
m26_in_bandwidth_ipv6	IPv6入网带宽	流入测量对象的IPv6网络带宽。	≥ 0	bit/s	1000(SI)	独享型负载均衡器	1分钟
m27_out_bandwidth_ipv6	IPv6出网带宽	流出测量对象的IPv6网络带宽。	≥ 0	bit/s	1000(SI)	独享型负载均衡器	1分钟
m1e_server_rps	后端服务器每秒重置报文个数	测量后端服务器每秒发送至客户端的重置（RST）报文个数。重置报文由后端服务器生成，然后由负载均衡器转发。 支持协议：TCP	≥ 0	Count/s	不涉及	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	单位	进制	测量对象（维度）	监控周期（原始指标）
m21_client_rps	客户端每秒重置报文个数	测量客户端每秒发送至后端服务器的重置（RST）报文个数。重置报文由客户端生成，然后由负载均衡器转发。 支持协议：TCP	≥ 0	Count/s	不涉及	独享型负载均衡器	1分钟
m1f_lvs_rps	负载均衡器每秒重置报文个数	测量负载均衡器每秒生成的重置（RST）报文个数。 支持协议：TCP	≥ 0	Count/s	不涉及	独享型负载均衡器	1分钟
mb_l7_qps	7层查询速率	测量对象7层查询速率。	≥ 0	Count/s	不涉及	独享型负载均衡器	1分钟
mc_l7_http_2xx	7层协议响应状态码（2XX）	测量对象每秒返回7层2XX系列响应状态码的个数。	≥ 0	Count/s	不涉及	独享型负载均衡器	1分钟
md_l7_http_3xx	7层协议响应状态码（3XX）	测量对象每秒返回7层3XX系列响应状态码的个数。	≥ 0	Count/s	不涉及	独享型负载均衡器	1分钟
me_l7_http_4xx	7层协议响应状态码（4XX）	测量对象每秒返回7层4XX系列响应状态码的个数。	≥ 0	Count/s	不涉及	独享型负载均衡器	1分钟
mf_l7_http_5xx	7层协议响应状态码（5XX）	测量对象每秒返回7层5XX系列响应状态码的个数。	≥ 0	Count/s	不涉及	独享型负载均衡器	1分钟
m10_l7_http_other_status	7层协议响应状态码(Others)	测量对象每秒返回7层其他响应状态码的个数。 不包含：2XX、3XX、404、499、502。	≥ 0	Count/s	不涉及	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	单位	进制	测量对象（维度）	监控周期（原始指标）
m11_l7_http_404	7层协议响应状态码404	测量对象每秒返回7层404响应状态码的个数。	≥ 0	Count/s	不涉及	独享型负载均衡器	1分钟
m12_l7_http_499	7层协议响应状态码499	测量对象每秒返回7层499响应状态码的个数。	≥ 0	Count/s	不涉及	独享型负载均衡器	1分钟
m13_l7_http_502	7层协议响应状态码502	测量对象每秒返回7层502响应状态码的个数。	≥ 0	Count/s	不涉及	独享型负载均衡器	1分钟
m14_l7_rt	7层协议RT平均值	测量对象7层平均响应时间。 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。 **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	ms	1000(SI)	独享型负载均衡器	1分钟
m15_l7_upstream_4xx	7层后端响应状态码(4XX)	测量对象的后端服务器每秒返回7层4XX系列响应状态码的个数。	≥ 0	Count/s	不涉及	独享型负载均衡器	1分钟
m16_l7_upstream_5xx	7层后端响应状态码(5XX)	测量对象的后端服务器每秒返回7层5XX系列响应状态码的个数。	≥ 0	Count/s	不涉及	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	单位	进制	测量对象（维度）	监控周期（原始指标）
m17_l7_upstream_rt	7层后端的RT平均值	测量对象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。 **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。	≥ 0	ms	1000(SI)	独享型负载均衡器	1分钟
m1a_l7_upstream_rt_max	7层后端的RT最大值	测量对象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。	≥ 0	ms	1000(SI)	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	测量对象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。	≥ 0	ms	1000(SI)	独享型负载均衡器	1分钟
m1c_l7_rt_max	7层协议的RT最大值	测量对象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。	≥ 0	ms	1000(SI)	独享型负载均衡器	1分钟
m1d_l7_rt_min	7层协议的RT最小值	测量对象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。	≥ 0	ms	1000(SI)	独享型负载均衡器	1分钟
l7_con_usage	7层并发连接使用率	7层的ELB实例并发连接数使用率。	≥ 0	%	不涉及	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	单位	进制	测量对象（维度）	监控周期（原始指标）
l7_in_bps_usage	7层入带宽使用率	7层的ELB实例入带宽使用率。 **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	%	不涉及	独享型负载均衡器	1分钟
l7_out_bps_usage	7层出带宽使用率	7层的ELB实例出带宽使用率。 **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	%	不涉及	独享型负载均衡器	1分钟
l7_ncps_usage	7层新建连接数使用率	7层的ELB实例新建连接数使用率。	≥ 0	%	不涉及	独享型负载均衡器	1分钟
l7_qps_usage	7层查询速率使用率	7层的ELB实例查询速率使用率。	≥ 0	%	不涉及	独享型负载均衡器	1分钟
l4_con_usage	4层并发连接使用率	4层的ELB实例并发连接数使用率。	≥ 0	%	不涉及	独享型负载均衡器	1分钟
l4_in_bps_usage	4层入带宽使用率	4层的ELB实例入带宽使用率。 **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	%	不涉及	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	单位	进制	测量对象（维度）	监控周期（原始指标）
l4_out_bps_usage	4层出带宽使用率	4层的ELB实例出带宽使用率。 **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	%	不涉及	独享型负载均衡器	1分钟
l4_ncps_usage	4层新建连接数使用率	4层的ELB实例新建连接数使用率。	≥ 0	%	不涉及	独享型负载均衡器	1分钟
ipgroup_blocked_packets	黑白名单每秒阻断数据报文的个数	每秒黑白名单阻断流入测量对象数据报文的个数。	≥ 0	Count/s	不涉及	独享型负载均衡器	1分钟
ipgroup_blocked_traffic	黑白名单阻断的网络带宽	黑白名单阻断流入测量对象的网络带宽。	≥ 0	bit/s	1000(SI)	独享型负载均衡器	1分钟
dropped_connections	丢弃连接数	测量对象每秒丢弃连接的个数。	≥ 0	Count/s	不涉及	独享型负载均衡器	1分钟
dropped_packets	丢弃数据包	测量对象每秒丢弃数据报文的个数。	≥ 0	Count/s	不涉及	独享型负载均衡器	1分钟
dropped_traffic	丢弃网络带宽	测量对象丢弃网络带宽。	≥ 0	bit/s	1000(SI)	独享型负载均衡器	1分钟
m18_l7_upstream_2xx	7层后端响应状态码(2XX)	测量对象的后端服务器每秒返回7层2XX系列响应状态码的个数。	≥ 0	Count/s	不涉及	独享型负载均衡器	1分钟
m19_l7_upstream_3xx	7层后端响应状态码(3XX)	测量对象的后端服务器每秒返回7层3XX系列响应状态码的个数。	≥ 0	Count/s	不涉及	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	单位	进制	测量对象（维度）	监控周期（原始指标）
l7_upstream_101	7层后端响应状态码101	测量对象的后端服务器每秒返回7层101响应状态码的个数。	≥ 0	Count/s	不涉及	独享型负载均衡器	1分钟
l7_upstream_400	7层后端响应状态码400	测量对象的后端服务器每秒返回7层400响应状态码的个数。	≥ 0	Count/s	不涉及	独享型负载均衡器	1分钟
l7_upstream_403	7层后端响应状态码403	测量对象的后端服务器每秒返回7层403响应状态码的个数。	≥ 0	Count/s	不涉及	独享型负载均衡器	1分钟
l7_upstream_404	7层后端响应状态码404	测量对象的后端服务器每秒返回7层404响应状态码的个数。	≥ 0	Count/s	不涉及	独享型负载均衡器	1分钟
l7_upstream_500	7层后端响应状态码500	测量对象的后端服务器每秒返回7层500响应状态码的个数。	≥ 0	Count/s	不涉及	独享型负载均衡器	1分钟
l7_upstream_501	7层后端响应状态码501	测量对象的后端服务器每秒返回7层501响应状态码的个数。	≥ 0	Count/s	不涉及	独享型负载均衡器	1分钟
l7_upstream_502	7层后端响应状态码502	测量对象的后端服务器每秒返回7层502响应状态码的个数。	≥ 0	Count/s	不涉及	独享型负载均衡器	1分钟
l7_upstream_503	7层后端响应状态码503	测量对象的后端服务器每秒返回7层503响应状态码的个数。	≥ 0	Count/s	不涉及	独享型负载均衡器	1分钟
l7_upstream_504	7层后端响应状态码504	测量对象的后端服务器每秒返回7层504响应状态码的个数。	≥ 0	Count/s	不涉及	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	单位	进制	测量对象（维度）	监控周期（原始指标）
l7_upstream_other_status	7层后端响应状态码（Others）	测量对象的后端服务器每秒返回7层后端其他响应状态码的个数。 不包含：101、2XX、3XX、400、403、404、500、501、502、503、504。	≥ 0	Count/s	不涉及	独享型负载均衡器	1分钟
elb_http_2xx	负载均衡响应状态码(2XX)	负载均衡每秒返回2XX响应状态码的个数。	≥ 0	Count/s	不涉及	独享型负载均衡器	1分钟
elb_http_3xx	负载均衡响应状态码(3XX)	负载均衡每秒返回3XX响应状态码的个数。	≥ 0	Count/s	不涉及	独享型负载均衡器	1分钟
elb_http_4xx	负载均衡响应状态码(4XX)	负载均衡每秒返回4XX响应状态码的个数。	≥ 0	Count/s	不涉及	独享型负载均衡器	1分钟
elb_http_5xx	负载均衡响应状态码(5XX)	负载均衡每秒返回5XX响应状态码的个数。	≥ 0	Count/s	不涉及	独享型负载均衡器	1分钟
elb_http_400	负载均衡响应状态码400	负载均衡每秒返回400响应状态码的个数。	≥ 0	Count/s	不涉及	独享型负载均衡器	1分钟
elb_http_404	负载均衡响应状态码404	负载均衡每秒返回404响应状态码的个数。	≥ 0	Count/s	不涉及	独享型负载均衡器	1分钟
elb_http_408	负载均衡响应状态码408	负载均衡每秒返回408响应状态码的个数。	≥ 0	Count/s	不涉及	独享型负载均衡器	1分钟
elb_http_499	负载均衡响应状态码499	负载均衡每秒返回499响应状态码的个数。	≥ 0	Count/s	不涉及	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	单位	进制	测量对象（维度）	监控周期（原始指标）
elb_http_502	负载均衡响应状态码502	负载均衡每秒返回502响应状态码的个数。	≥ 0	Count/s	不涉及	独享型负载均衡器	1分钟
elb_http_503	负载均衡响应状态码503	负载均衡每秒返回503响应状态码的个数。	≥ 0	Count/s	不涉及	独享型负载均衡器	1分钟
elb_http_504	负载均衡响应状态码504	负载均衡每秒返回504响应状态码的个数。	≥ 0	Count/s	不涉及	独享型负载均衡器	1分钟
l7_2xx_ratio	七层2XX请求占比	七层2XX响应状态码的个数占比。	≥ 0	%	不涉及	独享型负载均衡器	1分钟
l7_4xx_ratio	七层4XX请求占比	七层4XX响应状态码的个数占比。	≥ 0	%	不涉及	独享型负载均衡器	1分钟
l7_5xx_ratio	七层5XX请求占比	七层5XX响应状态码的个数占比。	≥ 0	%	不涉及	独享型负载均衡器	1分钟
mirror_in_traffic	入方向流量镜像的带宽	测量对象入方向流量镜像的带宽。	≥ 0	bit/s	1000(SI)	独享型负载均衡器	1分钟
mirror_out_traffic	出方向流量镜像的带宽	测量对象出方向流量镜像的带宽。	≥ 0	bit/s	1000(SI)	独享型负载均衡器	1分钟
mirror_in_packets	入方向流量镜像的报文速率	测量对象入方向流量镜像的报文速率。	≥ 0	Count/s	不涉及	独享型负载均衡器	1分钟
mirror_out_packets	出方向流量镜像的报文速率	测量对象出方向流量镜像的报文速率。	≥ 0	Count/s	不涉及	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	单位	进制	测量对象（维度）	监控周期（原始指标）
client_tls_negotiation_error	客户端发起TLS握手失败次数	客户端每秒发起TLS会话失败的次数。 支持的协议：HTTPS/TLS/QUIC	≥ 0	Count/s	不涉及	独享型负载均衡器	1分钟
upstream_tls_negotiation_error	负载均衡器向后端服务器TLS握手失败	负载均衡器向后端服务器每秒发起TLS会话失败的次数。 支持的协议：HTTPS/TLS/QUIC	≥ 0	Count/s	不涉及	独享型负载均衡器	1分钟

监听器的监控指标

说明

与七层业务相关的监控指标仅支持监听协议：HTTP/HTTPS/QUIC。

表 1-84 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	单位	进制	测量对象（维度）	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连接的个数。 在七层负载均衡器中，指从客户端到ELB建立的所有TCP连接的个数。	≥ 0	Count	不涉及	监听器（独享型）	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活跃TCP和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`	≥ 0	Count	不涉及	监听器（独享型）	1分钟

指标ID	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
m3_inact_conn	非活跃连接数	从测量对象到后端服务器建立的所有非活跃TCP和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`	≥ 0	Count	不涉及	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。	≥ 0	Count/s	不涉及	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数据包的个数。	≥ 0	Count/s	不涉及	监听器（独享型）	1分钟
m6_out_pps	流出数据包数	测量对象每秒发出数据包的个数。	≥ 0	Count/s	不涉及	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的网络速率。	≥ 0	Byte/s	1000(SI)	监听器（独享型）	1分钟
m8_out_Bps	网络流出速率	测量对象访问外部的网络速率。	≥ 0	Byte/s	1000(SI)	监听器（独享型）	1分钟
m9_abnormal_servers	异常主机数	测量对象中健康检查异常的后端服务器个数。	≥ 0	Count	不涉及	监听器（独享型）	1分钟
ma_normal_servers	正常主机数	测量对象中健康检查正常的后端服务器个数。	≥ 0	Count	不涉及	监听器（独享型）	1分钟
m22_in_bandwidth	入网带宽	测量对象入网带宽。	≥ 0	bit/s	1000(SI)	监听器（独享型）	1分钟
m23_out_bandwidth	出网带宽	测量对象出网带宽。	≥ 0	bit/s	1000(SI)	监听器（独享型）	1分钟

指标ID	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
m1e_server_rps	后端服务器每秒重置报文个数	测量后端服务器每秒发送至客户端的重置（RST）报文个数。重置报文由后端服务器生成，然后由负载均衡器转发。 支持的协议：TCP	≥ 0	Count/s	不涉及	监听器（独享型）	1分钟
m21_client_rps	客户端每秒重置报文个数	测量客户端每秒发送至后端服务器的重置（RST）报文个数。重置数据包由客户端生成，然后由负载均衡器转发。 支持的协议：TCP	≥ 0	Count/s	不涉及	监听器（独享型）	1分钟
m1f_lvs_rps	负载均衡器每秒重置报文个数	测量负载均衡器每秒生成的重置（RST）报文个数。 支持的协议：TCP	≥ 0	Count/s	不涉及	监听器（独享型）	1分钟
mb_l7_qps	7层查询速率	测量对象7层查询速率。	≥ 0	Count/s	不涉及	监听器（独享型）	1分钟
mc_l7_http_2xx	7层协议响应状态码(2XX)	测量对象每秒返回7层2XX系列响应状态码的个数。	≥ 0	Count/s	不涉及	监听器（独享型）	1分钟
md_l7_http_3xx	7层协议响应状态码(3XX)	测量对象每秒返回7层3XX系列响应状态码的个数。	≥ 0	Count/s	不涉及	监听器（独享型）	1分钟
me_l7_http_4xx	7层协议响应状态码(4XX)	测量对象每秒返回7层4XX系列响应状态码的个数。	≥ 0	Count/s	不涉及	监听器（独享型）	1分钟
mf_l7_http_5xx	7层协议响应状态码(5XX)	测量对象每秒返回7层5XX系列响应状态码的个数。	≥ 0	Count/s	不涉及	监听器（独享型）	1分钟

指标ID	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
m10_l7_http_other_status	7层协议响应状态码(Others)	测量对象每秒返回7层其他响应状态码的个数。 不包含：2XX、3XX、404、499、502。	≥ 0	Count/s	不涉及	监听器（独享型）	1分钟
m11_l7_http_404	7层协议响应状态码(404)	测量对象每秒返回7层404响应状态码的个数。	≥ 0	Count/s	不涉及	监听器（独享型）	1分钟
m12_l7_http_499	7层协议响应状态码(499)	测量对象每秒返回7层499响应状态码的个数。	≥ 0	Count/s	不涉及	监听器（独享型）	1分钟
m13_l7_http_502	7层协议响应状态码(502)	测量对象每秒返回7层502响应状态码的个数。	≥ 0	Count/s	不涉及	监听器（独享型）	1分钟
m14_l7_rt	7层协议RT平均值	测量对象7层平均响应时间。 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。 **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。	≥ 0	ms	1000(SI)	监听器（独享型）	1分钟
m15_l7_upstream_4xx	7层后端响应状态码(4XX)	测量对象的后端服务器每秒返回7层4XX系列响应状态码的个数。	≥ 0	Count/s	不涉及	监听器（独享型）	1分钟
m16_l7_upstream_5xx	7层后端响应状态码(5XX)	测量对象的后端服务器每秒返回7层5XX系列响应状态码的个数。	≥ 0	Count/s	不涉及	监听器（独享型）	1分钟

指标ID	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
m17_l7_upstream_rt	7层后端的RT平均值	测量对象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。 **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。	≥ 0	ms	1000(SI)	监听器（独享型）	1分钟
m1a_l7_upstream_rt_max	7层后端的RT最大值	测量对象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。	≥ 0	ms	1000(SI)	监听器（独享型）	1分钟
m1b_l7_upstream_rt_min	7层后端的RT最小值	测量对象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。	≥ 0	ms	1000(SI)	监听器（独享型）	1分钟
m1c_l7_rt_max	7层协议的RT最大值	测量对象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。	≥ 0	ms	1000(SI)	监听器（独享型）	1分钟
m1d_l7_rt_min	7层协议的RT最小值	测量对象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。	≥ 0	ms	1000(SI)	监听器（独享型）	1分钟
ipgroup_blocked_packets	黑白名单每秒阻断数据报文的个数	每秒黑白名单阻断流入测量对象数据报文的个数。	≥ 0	Count/s	不涉及	监听器（独享型）	1分钟

指标ID	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
ipgroup_blocked_traffic	黑白名单阻断的网络带宽	黑白名单阻断流入测量对象的网络带宽。	≥ 0	bit/s	1000(SI)	监听器（独享型）	1分钟
m18_l7_upstream_2xx	7层后端响应状态码(2XX)	测量对象的后端服务器每秒返回2XX系列响应状态码的个数。	≥ 0	Count/s	不涉及	监听器（独享型）	1分钟
m19_l7_upstream_3xx	7层后端响应状态码(3XX)	测量对象的后端服务器每秒返回3XX系列响应状态码的个数。	≥ 0	Count/s	不涉及	监听器（独享型）	1分钟
l7_upstream_101	7层后端响应状态码101	测量对象的后端服务器每秒返回101响应状态码的个数。	≥ 0	Count/s	不涉及	监听器（独享型）	1分钟
l7_upstream_400	7层后端响应状态码400	测量对象的后端服务器每秒返回400响应状态码的个数。	≥ 0	Count/s	不涉及	监听器（独享型）	1分钟
l7_upstream_403	7层后端响应状态码403	测量对象的后端服务器每秒返回403响应状态码的个数。	≥ 0	Count/s	不涉及	监听器（独享型）	1分钟
l7_upstream_404	7层后端响应状态码404	测量对象的后端服务器每秒返回404响应状态码的个数。	≥ 0	Count/s	不涉及	监听器（独享型）	1分钟
l7_upstream_500	7层后端响应状态码500	测量对象的后端服务器每秒返回500响应状态码的个数。	≥ 0	Count/s	不涉及	监听器（独享型）	1分钟
l7_upstream_501	7层后端响应状态码501	测量对象的后端服务器每秒返回501响应状态码的个数。	≥ 0	Count/s	不涉及	监听器（独享型）	1分钟
l7_upstream_502	7层后端响应状态码502	测量对象的后端服务器每秒返回502响应状态码的个数。	≥ 0	Count/s	不涉及	监听器（独享型）	1分钟

指标ID	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
l7_upstream_503	7层后端响应状态码503	测量对象的后端服务器每秒返回503响应状态码的个数。	≥ 0	Count/s	不涉及	监听器（独享型）	1分钟
l7_upstream_504	7层后端响应状态码504	测量对象的后端服务器每秒返回504响应状态码的个数。	≥ 0	Count/s	不涉及	监听器（独享型）	1分钟
l7_upstream_other_status	7层后端响应状态码（Others）	测量对象的后端服务器每秒返回7层后端其他响应状态码的个数。 不包含：101、2XX、3XX、400、403、404、500、501、502、503、504。	≥ 0	Count/s	不涉及	监听器（独享型）	1分钟
elb_http_2xx	负载均衡响应状态码(2XX)	负载均衡每秒返回2XX响应状态码的个数。	≥ 0	Count/s	不涉及	监听器（独享型）	1分钟
elb_http_3xx	负载均衡响应状态码(3XX)	负载均衡每秒返回3XX响应状态码的个数。	≥ 0	Count/s	不涉及	监听器（独享型）	1分钟
elb_http_4xx	负载均衡响应状态码(4XX)	负载均衡每秒返回4XX响应状态码的个数。	≥ 0	Count/s	不涉及	监听器（独享型）	1分钟
elb_http_5xx	负载均衡响应状态码(5XX)	负载均衡每秒返回5XX响应状态码的个数。	≥ 0	Count/s	不涉及	监听器（独享型）	1分钟
elb_http_400	负载均衡响应状态码400	负载均衡每秒返回400响应状态码的个数。	≥ 0	Count/s	不涉及	监听器（独享型）	1分钟
elb_http_404	负载均衡响应状态码404	负载均衡每秒返回404响应状态码的个数。	≥ 0	Count/s	不涉及	监听器（独享型）	1分钟

指标ID	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
elb_http_408	负载均衡响应状态码408	负载均衡每秒返回408响应状态码的个数。	≥ 0	Count/s	不涉及	监听器（独享型）	1分钟
elb_http_499	负载均衡响应状态码499	负载均衡每秒返回499响应状态码的个数。	≥ 0	Count/s	不涉及	监听器（独享型）	1分钟
elb_http_502	负载均衡响应状态码502	负载均衡每秒返回502响应状态码的个数。	≥ 0	Count/s	不涉及	监听器（独享型）	1分钟
elb_http_503	负载均衡响应状态码503	负载均衡每秒返回503响应状态码的个数。	≥ 0	Count/s	不涉及	监听器（独享型）	1分钟
elb_http_504	负载均衡响应状态码504	负载均衡每秒返回504响应状态码的个数。	≥ 0	Count/s	不涉及	监听器（独享型）	1分钟
l7_2xx_ratio	七层2XX请求占比	七层2XX响应状态码的个数占比。	≥ 0	%	不涉及	监听器（独享型）	1分钟
l7_4xx_ratio	七层4XX请求占比	七层4XX响应状态码的个数占比。	≥ 0	%	不涉及	监听器（独享型）	1分钟
l7_5xx_ratio	七层5XX请求占比	七层5XX响应状态码的个数占比。	≥ 0	%	不涉及	监听器（独享型）	1分钟
mirror_in_traffic	入方向流量镜像的带宽	测量对象入方向流量镜像的带宽。	≥ 0	bit/s	1000(SI)	监听器（独享型）	1分钟
mirror_out_traffic	出方向流量镜像的带宽	测量对象出方向流量镜像的带宽。	≥ 0	bit/s	1000(SI)	监听器（独享型）	1分钟

指标ID	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
mirror_in_packets	入方向流量镜像的报文速率	测量对象入方向流量镜像的报文速率。	≥ 0	Count/s	不涉及	监听器（独享型）	1分钟
mirror_out_packets	出方向流量镜像的报文速率	测量对象出方向流量镜像的报文速率。	≥ 0	Count/s	不涉及	监听器（独享型）	1分钟
client_tls_negotiation_error	客户端发起TLS握手失败次数	客户端每秒发起TLS会话失败的次数。 支持的协议：HTTPS/TLS/QUIC	≥ 0	Count/s	不涉及	监听器（独享型）	1分钟
upstream_tls_negotiation_error	负载均衡器向后端服务器TLS握手失败次数	负载均衡器向后端服务器每秒发起TLS会话失败的次数。 支持的协议：HTTPS/TLS/QUIC	≥ 0	Count/s	不涉及	监听器（独享型）	1分钟

后端服务器组的监控指标

说明

与七层业务相关的监控指标仅支持协议：HTTP/HTTPS/QUIC/GRPC。

表 1-85 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	单位	进制	测量对象（维度）	监控周期（原始指标）
m9_abnormal_servers	异常主机数	测量对象中健康检查异常的后端服务器个数。	≥ 0	Count	不涉及	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	单位	进制	测量对象（维度）	监控周期（原始指标）
ma_normal_servers	正常主机数	测量对象中健康检查正常的后端服务器个数。	≥ 0	Count	不涉及	后端服务器组（独享型）	1分钟
mb_l7_qps	7层查询速率	测量对象7层查询速率。	≥ 0	Count/s	不涉及	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	测量对象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。 **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。	≥ 0	ms	1000(SI)	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	测量对象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。	≥ 0	ms	1000(SI)	后端服务器组（独享型）	1分钟
m1b_l7_upstream_rt_min	7层后端的RT最小值	测量对象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。	≥ 0	ms	1000(SI)	后端服务器组（独享型）	1分钟
m15_l7_upstream_4xx	7层后端响应状态码(4XX)	测量对象的后端服务器每秒返回7层4XX系列响应状态码的个数。	≥ 0	Count/s	不涉及	后端服务器组（独享型）	1分钟
m16_l7_upstream_5xx	7层后端响应状态码(5XX)	测量对象的后端服务器每秒返回7层5XX系列响应状态码的个数。	≥ 0	Count/s	不涉及	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	单位	进制	测量对象（维度）	监控周期（原始指标）
m18_l7_upstream_2xx	7层后端响应状态码(2XX)	测量对象的后端服务器每秒返回2XX系列响应状态码的个数。	≥ 0	Count/s	不涉及	后端服务器组（独享型）	1分钟
m19_l7_upstream_3xx	7层后端响应状态码(3XX)	测量对象的后端服务器每秒返回3XX系列响应状态码的个数。	≥ 0	Count/s	不涉及	后端服务器组（独享型）	1分钟
m25_l7_resp_Bps	7层响应带宽	测量对象后端服务器的七层响应发送带宽。 **说明** 当监听器开启HTTP/2时，该指标无法作为参考。	≥ 0	bit/s	1000(SI)	后端服务器组（独享型）	1分钟
m24_l7_req_Bps	7层请求带宽	测量对象后端服务器的七层请求接收带宽。 **说明** 当监听器开启HTTP/2时，该指标无法作为参考。	≥ 0	bit/s	1000(SI)	后端服务器组（独享型）	1分钟
l7_upstream_101	7层后端响应状态码101	测量对象的后端服务器每秒返回101响应状态码的个数。	≥ 0	Count/s	不涉及	后端服务器组（独享型）	1分钟
l7_upstream_400	7层后端响应状态码400	测量对象的后端服务器每秒返回400响应状态码的个数。	≥ 0	Count/s	不涉及	后端服务器组（独享型）	1分钟
l7_upstream_403	7层后端响应状态码403	测量对象的后端服务器每秒返回403响应状态码的个数。	≥ 0	Count/s	不涉及	后端服务器组（独享型）	1分钟
l7_upstream_404	7层后端响应状态码404	测量对象的后端服务器每秒返回404响应状态码的个数。	≥ 0	Count/s	不涉及	后端服务器组（独享型）	1分钟
l7_upstream_500	7层后端响应状态码500	测量对象的后端服务器每秒返回500响应状态码的个数。	≥ 0	Count/s	不涉及	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	单位	进制	测量对象（维度）	监控周期（原始指标）
l7_upstream_501	7层后端响应状态码501	测量对象的后端服务器每秒返回501状态响应码的个数。	≥ 0	Count/s	不涉及	后端服务器组（独享型）	1分钟
l7_upstream_502	7层后端响应状态码502	测量对象的后端服务器每秒返回502状态响应码的个数。	≥ 0	Count/s	不涉及	后端服务器组（独享型）	1分钟
l7_upstream_503	7层后端响应状态码503	测量对象的后端服务器每秒返回503响应状态码的个数。	≥ 0	Count/s	不涉及	后端服务器组（独享型）	1分钟
l7_upstream_504	7层后端响应状态码504	测量对象的后端服务器每秒返回504状态响应码的个数。	≥ 0	Count/s	不涉及	后端服务器组（独享型）	1分钟
l7_upstream_other_status	7层后端响应状态码（Others）	测量对象的后端服务器每秒返回7层后端其他响应状态码的个数。 不包含：101、2XX、3XX、400、403、404、500、501、502、503、504。	≥ 0	Count/s	不涉及	后端服务器组（独享型）	1分钟

可用区的监控指标

表 1-86 可用区的监控指标

指标ID	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	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。	≥ 0	Count	不涉及	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活跃TCP和UDP连接的个数。 Windows和Linux服务器都可以使用如下命令查看。 `netstat -an`	≥ 0	Count	不涉及	可用区	1分钟
m3_inact_conn	非活跃连接数	从测量对象到后端服务器建立的非活跃TCP和UDP连接的个数。 Windows和Linux服务器都可以使用如下命令查看。 `netstat -an`	≥ 0	Count	不涉及	可用区	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。	≥ 0	Count/s	不涉及	可用区	1分钟
m5_in_pps	流入数据包数	测量对象每秒接收到数据包的个数。	≥ 0	Count/s	不涉及	可用区	1分钟
m6_out_pps	流出数据包数	测量对象每秒发出数据包的个数。	≥ 0	Count/s	不涉及	可用区	1分钟
m7_in_Bps	网络流入速率	从外部访问测量对象的网络速率。	≥ 0	Byte/s	1000(SI)	可用区	1分钟
m8_out_Bps	网络流出速率	测量对象访问外部的网络速率。	≥ 0	Byte/s	1000(SI)	可用区	1分钟

指标ID	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
m26_in_bandwidth_ipv6	IPv6入网带宽	流入测量对象的IPv6网络带宽。	≥ 0	bit/s	1000(SI)	可用区	1分钟
m27_out_bandwidth_ipv6	IPv6出网带宽	流出测量对象的IPv6网络带宽。	≥ 0	bit/s	1000(SI)	可用区	1分钟
m1e_server_rps	后端服务器每秒重置报文个数	测量后端服务器每秒发送至客户端的重置（RST）报文个数。重置报文由后端服务器生成，然后由负载均衡器转发。 支持协议：TCP	≥ 0	Count/s	不涉及	可用区	1分钟
m21_client_rps	客户端每秒重置报文个数	测量客户端每秒发送至后端服务器的重置（RST）报文个数。重置报文由客户端生成，然后由负载均衡器转发。 支持协议：TCP	≥ 0	Count/s	不涉及	可用区	1分钟
m1f_lvs_rps	负载均衡器每秒重置报文个数	测量负载均衡器每秒生成的重置（RST）报文的个数。 支持协议：TCP	≥ 0	Count/s	不涉及	可用区	1分钟
l4_con_usage	4层并发连接使用率	4层的ELB实例并发连接数使用率。	≥ 0	%	不涉及	可用区	1分钟
l4_in_bps_usage	4层入带宽使用率	4层的ELB实例入带宽使用率。 **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	%	不涉及	可用区	1分钟

指标ID	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
l4_out_bps_usage	4层出带宽使用率	4层的ELB实例出带宽使用率。 **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	%	不涉及	可用区	1分钟
l4_ncps_usage	4层新建连接数使用率	4层的ELB实例新建连接数使用率。	≥ 0	%	不涉及	可用区	1分钟
l7_in_bps_usage	7层入带宽使用率	7层的ELB实例入带宽使用率。 **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	%	不涉及	可用区	1分钟
l7_out_bps_usage	7层出带宽使用率	7层的ELB实例出带宽使用率。 **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	%	不涉及	可用区	1分钟
l7_con_usage	7层并发连接使用率	7层的ELB实例并发连接数使用率。	≥ 0	%	不涉及	可用区	1分钟
l7_ncps_usage	7层新建连接数使用率	7层的ELB实例新建连接数使用率。	≥ 0	%	不涉及	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。

1.11.3 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1-87**

表 1-87 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。

1.11.4 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. 进入**EIP列表页面**。
2. 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 1-55 EIP 使用流量监控结果

表 1-88 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

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. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页，单击需要查看流量的负载均衡器名称。
3. 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。

1.12 使用 CTS 审计 ELB 关键操作

1.12.1 ELB 支持审计的关键操作

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1-89**所示。

表 1-89 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

操作名称	资源类型	事件名称
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

1.12.2 查看 ELB 的审计日志

操作场景

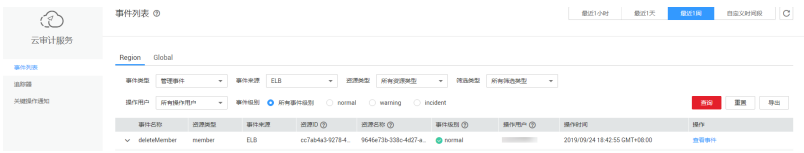
在您开启了云审计服务后，系统开始记录云服务资源的操作。云审计服务管理控制台保存最近7天的操作记录。

本节介绍如何在云审计服务管理控制台查看或导出最近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 1-56 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 1-57 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 升级至独享型负载均衡器

升级概述

独享型ELB相比共享型ELB，性能更卓越，支持多种更为丰富的应用协议，具备更为灵活的七层处理能力。

升级至独享型实例后，ELB实例使用的IP地址和实例ID均保持不变，四层监听器将开启获取客户端IP功能，七层监听器将开启高级转发策略。

升级过程支持回退，保障您放心升级。

说明

支持升级至独享型ELB的功能陆续上线中，已发布区域请以控制台实际开放为准。如果您有使用需求，可以提交工单进行处理。

升级限制

- 仅按需计费模式的共享型实例支持升级。
- 仅建议通过弹性负载均衡控制台和API创建的实例升级，其他方式创建的ELB实例有升级需求请提工单咨询。
- 如果当前共享型ELB实例已被CCE使用，暂时无法进行升级操作，您可提工单进一步咨询。

升级影响

- 升级过程中业务可能会出现长连接闪断，闪断时间为1~2秒，客户端重新建立连接后可恢复。
- 升级过程中，ELB实例及其相关资源和配置都无法操作。
- 升级过程中，ELB的监控数据可能出现波动导致数据暂时不准确，建议您关注自身业务的实际运行情况。升级完成后监控数据将恢复正常。
- 独享型ELB将以后端子网内的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。

开始升级前，请确保后端服务器的安全组规则和网络ACL规则配置放行**ELB后端子网所属网段**，否则会导致健康检查异常，业务异常。

详情见**配置后端服务器的安全组和网络ACL（独享型）**。

- 升级至独享型实例后，会话保持将在独享型实例重新生效。

升级计费说明

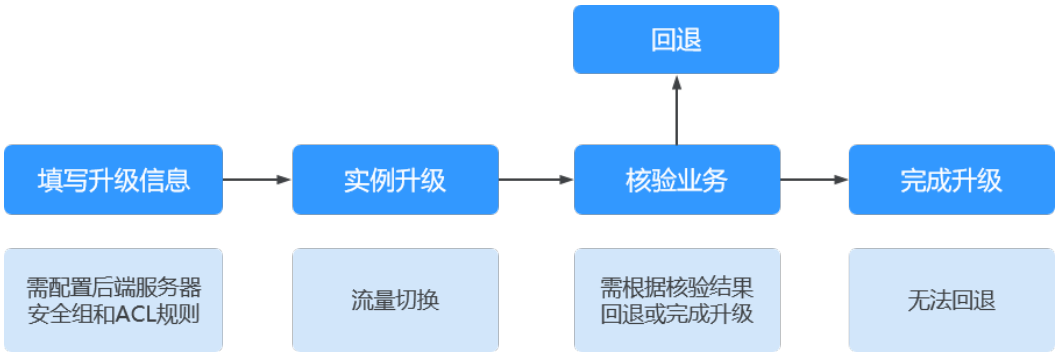
- 升级成功后，将按照独享型实例计费规则收费，请自行评估您的商务折扣是否会受到影响。
- 升级为独享型ELB，计费规则详见**计费项（独享型）**。

升级注意事项

- 若您的业务采用UDP协议且存在报文分片传输，则建议不要升级实例，否则业务会受损。
- 实例升级过程不改变已有转发策略优先级，升级完成后您可**通过排序来设置优先级**。
- 升级过程中，请勿修改关联云服务资源。

操作流程

图 2-1 升级流程示意图



步骤一：填写升级信息

1. 通过控制台进入实例升级页面。
   a. 进入**弹性负载均衡列表页面**。
   b. 在弹性负载均衡列表页面，在目标共享型负载均衡器所在行的“操作”列，单击“升级至独享型”。
2. 在“升级须知”弹窗，了解**升级影响和限制**，勾选“我已知晓以上升级须知”。
3. 单击“去升级”，进入填写升级信息流程。您需确认升级后的独享型实例配置，详情见**表2-1**。

表 2-1 弹性负载均衡配置升级设置

参数	说明
可用区	升级后新增参数。 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。 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。 更多可用区规划请参考**规划实例可用区**。 **注意** 实例升级后，修改可用区配置可能会导致该实例的业务闪断数秒，请在升级时做好规划。
规格	升级后新增参数。 “应用型（HTTP/HTTPS）”和“网络型（TCP/UDP）”请至少勾选一种： ● 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。 ● 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。 共享型ELB实例下若已创建监听器，则默认支持监听器对应的ELB实例规格类型。 请您根据自身业务规划选择规格，如何选择规格详见**独享型负载均衡的实例规格**。
网络类型	支持多选，根据选择的网络类型，为弹性负载均衡分配网络服务地址。 ● 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 网络：系统会为实例分配IPv6地址，转发来自IPv6客户端的请求。 – 默认支持处理来自同一个VPC的IPv6客户端的请求。 – 升级完成后，加入IPv6共享带宽支持处理来自公网IPv6客户端的请求。 **注意** 若您业务有IPv6通信需求，建议您在升级时勾选IPv6 网络。升级完成后，不支持添加IPv6功能。

参数	说明
前端子网	独享型负载均衡所在的子网，不支持变更。从该子网中分配ELB实例对外服务的IP地址。 若网络类型选择支持IPv6网络，则该子网需开启IPv6功能。 您可单击“跳转到子网详情页”跳转到该子网的基本信息页签，开启IPv6功能。
后端子网	升级后新增参数。 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。 独享型负载均衡实例会占用后端子网中的部分IP地址，实际占用IP地址的数量以您在控制台升级实例所占用的IP地址个数为准。 ● 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。

4. 根据页面提示，在ELB实例关联的后端服务器的安全组规则和网络ACL规则中，放通独享型ELB后端子网所属网段。

   操作详情见**配置后端服务器的安全组规则和网络ACL规则（独享型）**。

   a. 单击“配置安全组规则”，便捷跳转至安全组列表页。

      您可通过筛选**服务器私有地址**，快速定位ELB关联后端服务器的安全组。

   b. 如果您的ELB实例所属后端子网启用了网络ACL。

      单击“配置ACL规则”，便捷跳转至网络ACL列表页。

      您可通过筛选**子网名称**或**子网ID**，快速定位ELB关联后端服务器的网络ACL规则。

5. 确认安全组规则和ACL规则配置放通后，勾选确认复选框。

   单击“下一步：实例升级”，进入实例升级任务。

步骤二：实例升级

实例升级分初始化配置和流量切换两个步骤进行，升级时间会受到负载均衡实际配置复杂度的影响，预计5分钟内完成升级。

实例升级过程中，您可随时通过弹性负载均衡列表页的状态列单击**查看任务**，查看升级进展。

- 实例升级成功，自动进入**步骤三：核验业务**。
- 实例升级失败：

  a. 请查看**升级原因**提示，如不能解决您的问题，请联系客服提交工单处理。

  b. 单击“回退”，回退完成。

     i. 单击“重新升级”，重新进入**步骤一：填写升级信息**。

     ii. 单击“关闭”，结束升级任务。

步骤三：核验业务

您可在当前页面查看实例的详细配置，也可单击“查看实例详情”进入实例详情页进行查看。

请确认升级至独享型实例后的配置信息，并核验您的业务是否正常，推荐参见**核验业务示例**。

1. 核验业务正常，单击“下一步：完成升级”，进入**步骤四：完成升级**。

   ⚠ 注意

   单击“完成升级”后，升级任务无法回退，请谨慎选择。

2. 核验业务异常，单击“回退”，回退完成。
   a. 单击“重新升级”，重新进入**步骤一：填写升级信息**。
   b. 单击“关闭”，结束升级任务。

步骤四：完成升级

您的负载均衡实例已完成**升级至独享型**的升级流程，单击“关闭”，结束升级任务。

原共享型负载均衡器的业务已全部升级至独享型负载均衡器。

核验业务示例

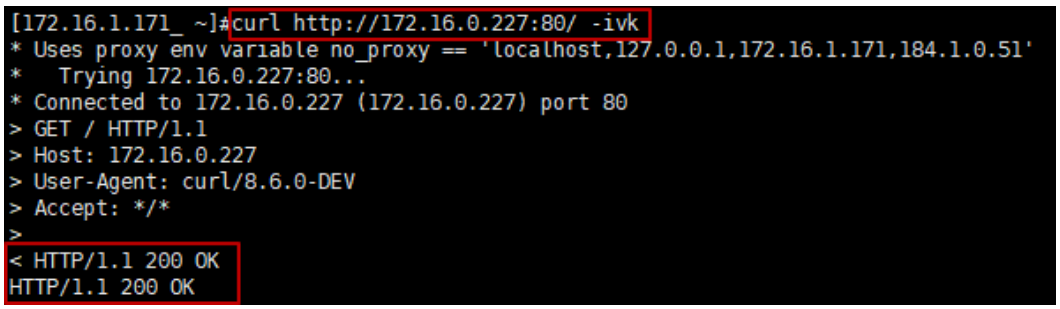
- 如果您的业务采用HTTP/HTTPS监听器进行转发，推荐您执行以下命令查看回显中返回的状态码是否正常。

  ```
  curl http://ELB的IP:监听端口 -ivk
  curl https://ELB的IP:监听端口 -ivk
  ```

  此处EIP的IP可分别采用ELB的私网IP地址或ELB绑定的EIP地址。

  HTTP 状态码 200 表示请求已经成功。

  图 2-2 ELB 的 HTTP/HTTPS 业务正常的回显示例

- 如果您的业务采用TCP监听器进行转发，推荐您执行以下命令与ELB建立TCP连接。

  ```
  socat tcp:ELB的IP:监听端口,connect-timeout=3 /dev/null
  ```

  此处EIP的IP可分别采用ELB的私网IP地址或ELB绑定的EIP地址。

  如果没有回显信息没有报错，那么TCP连接建立成功。

  图 2-3 与 ELB 建立 TCP 连接成功的回显示例

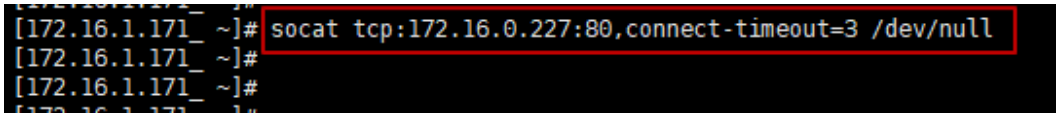
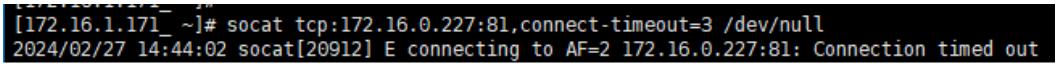
  

图 2-4 与 ELB 建立 TCP 连接失败的回显示例



- 如果您的业务采用UDP监听器进行转发，建议您自行确认业务转发正常后再单击“完成升级”。

相关文档

- 高级转发策略（独享型）
- 配置后端服务器的安全组
- 配置不同VPC的服务器作为后端服务器（IP类型后端）

2.2 通过 IAM 授予使用 ELB 的权限

2.2.1 通过 IAM 角色或策略授予使用 ELB 的权限

如果您需要对您所拥有的ELB进行角色与策略的权限管理，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。

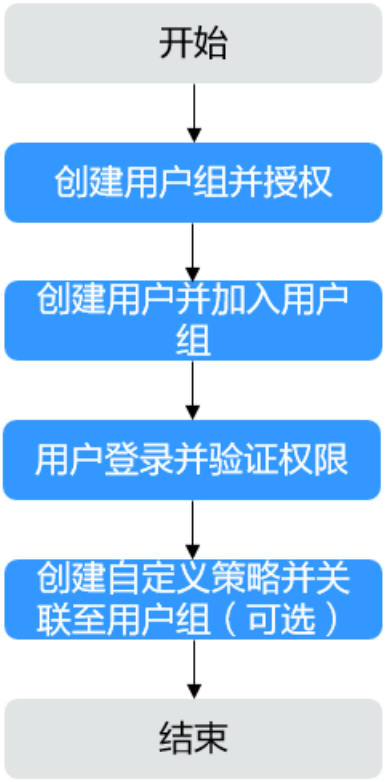
本章节为您介绍角色与策略的授权方法，操作流程如图2-5所示。

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，请参见角色与策略权限管理。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授权参考。

示例流程

图 2-5 给用户授予 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**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ELBReadOnlyAccess），表示“ELBReadOnlyAccess”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ELBReadOnlyAccess）的任一服务，若提示权限不足，表示“ELBReadOnlyAccess”已生效。

ELB 自定义策略样例

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**策略授权参考**。

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**。下面为您介绍常用的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ELBFullAccess的系统策略，但不希望用户拥有ELBFullAccess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ELBFullAccess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"
            ]
        }
    ]
}
```

2.2.2 通过 IAM 身份策略授予使用 ELB 的权限

如果您需要对您所拥有的ELB进行**身份策略**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用户或用户组，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，您可以跳过本章节，不影响您使用ELB服务的其它功能。

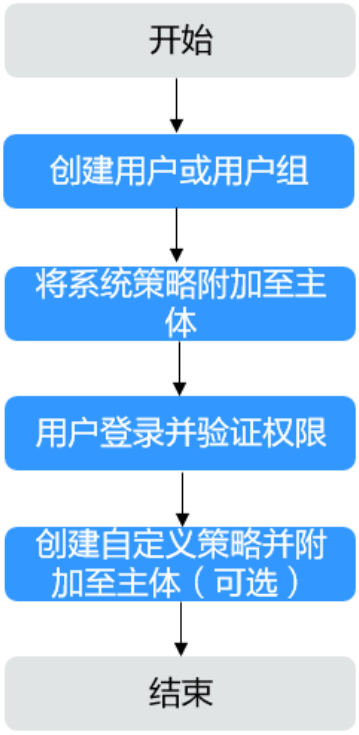
本章节为您介绍身份策略的授权方法，操作流程如**图2-6**所示。

前提条件

授权操作前，请您了解可以添加的ELB权限，并结合实际需求进行选择。ELB支持的系统策略，请参见**身份策略权限管理**。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**授权参考**。

示例流程

图 2-6 给用户授予 ELB 权限流程



1. **创建用户**或**创建用户组**

   在IAM控制台创建用户或用户组。
2. **将系统身份策略附加至用户或用户组**

   为用户或用户组授予弹性负载均衡只读权限的系统策略“ELBReadOnlyAccessPolicy”，并将策略附加至用户或用户组。
3. **用户登录**并验证权限

使用已授权的用户登录控制台，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ELBReadOnlyAccessPolicy），表示“ELBReadOnlyAccessPolicy”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ELBReadOnlyAccessPolicy）的任一服务，若提示权限不足，表示“ELBReadOnlyAccessPolicy”已生效。

ELB 自定义策略样例

如果系统预置的ELB系统策略，不满足您的授权要求，可以创建自定义身份策略。自定义身份策略中可以添加的授权项（Action）请参考。

目前华为云支持以下两种方式创建自定义身份策略：

- 可视化视图创建自定义身份策略：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视图创建自定义身份策略：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：**创建自定义身份策略并附加至主体**。

您可以在创建自定义身份策略时，可以通过资源类型（Resource）元素来选择特定资源，以及服务级条件键（Condition）元素来控制策略何时生效。支持的资源类型和条件键请参考身份策略授权。下面为您介绍常用的ELB自定义身份策略样例。

- 示例1：授权创建和删除负载均衡器的权限。

```
{
    "Version": "5.0",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "elb:loadbalancers:create",
                "elb:loadbalancers:delete"
            ]
        }
    ]
}
```

- 示例2：多个授权项策略

  一个自定义身份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。多个授权语句策略描述如下：

```
{
    "Version": "5.0",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "elb:loadbalancers:create",
                "elb:loadbalancers:delete"
            ]
        },
        {
            "Effect": "Deny",
            "Action": [
                "elb:loadbalancers:get",
                "elb:loadbalancers:list"
            ]
        },
```

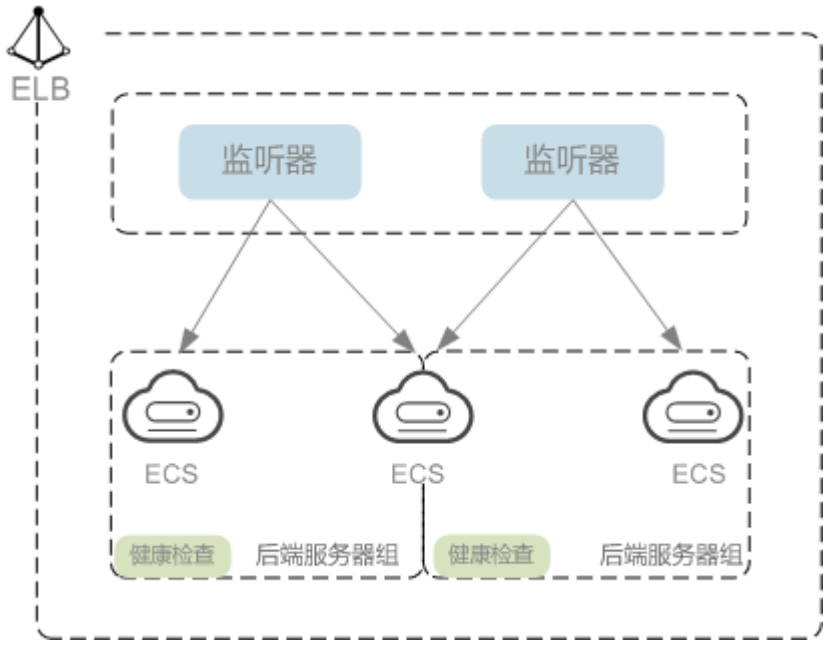
```
        {
            "Effect": "Allow",
            "Action": [
                "vpc:vpcs:get",
                "vpc:vpcs:list"
            ]
        }
    ]
}
```

2.3 负载均衡器

2.3.1 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 2-7 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。

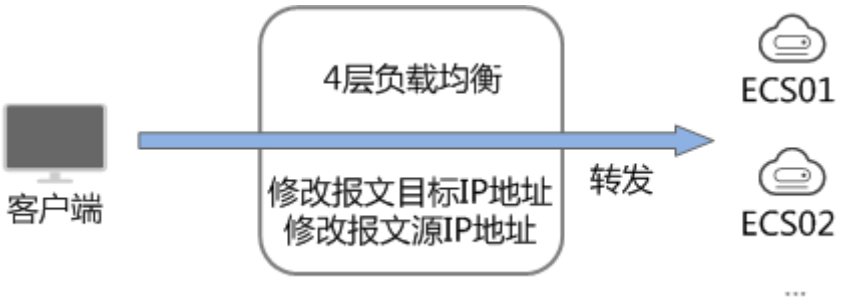
  私网负载均衡器仅分配一个私网IP，仅能用来接收来自同个VPC内的访问请求。

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。

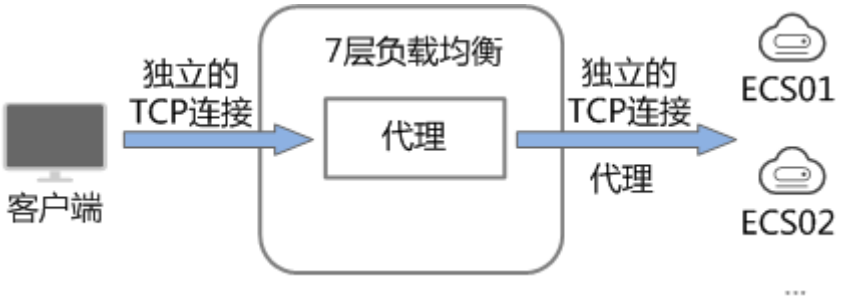
- 使用四层协议的负载均衡，监听器收到访问请求后，将请求直接转发给后端服务器。转发过程仅修改报文中目标IP地址和源IP地址，将目标地址改为后端云服务器的IP地址，源地址改为负载均衡器的IP地址。四层协议连接的建立，即三次握手是客户端和后端服务器直接建立的，负载均衡只是进行了数据的转发。

  图 2-8 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 2-9 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，建议先创建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：

- 建议后端服务器实例的所属区域和负载均衡器的所属区域相同。
- 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。

2.3.2 购买共享型负载均衡器

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**。

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，才可以对负载均衡实例地址进行ping验证。

创建共享型负载均衡器

1. 进入**购买弹性负载均衡页面**。
2. 在弹性负载均衡列表页面，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2-2**所示。

表 2-2 负载均衡器的基础配置

参数	说明
计费模式	共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。
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。
名称	待创建负载均衡器的名称。 • 长度范围为1~255位。 • 名称由中文、英文字母、数组、下划线（_）、中划线（-）和点组成。

参数	说明
企业项目	创建负载均衡器时，可以将其加入已启用的企业项目。 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。 关于创建和管理企业项目的详情，请参见《企业管理用户指南》。

3. 选定共享型负载均衡实例的基础配置后，您需选择弹性负载均衡的实例规格。

表 2-3 负载均衡器的规格说明

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。 共享型实例适用于流量负载较低的业务场景，如小型网站和普通高可用应用。 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。

4. 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2-4所示。

表 2-4 负载均衡器的网络配置

参数	说明
网络类型	网络类型默认支持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。 如果您有IPv4公网业务需求，请为负载均衡实例绑定弹性公网IP。
所属VPC	负载均衡器所属虚拟私有云，共享型ELB创建完成后不支持切换，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。 更多关于虚拟私有云的信息，请参见《虚拟私有云用户指南》。
前端子网	共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。 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。

参数	说明
IPv4地址	选择IPv4地址的分配方式。 • 自动分配IPv4地址：由系统自动为负载均衡器分配IPv4地址。 • 手动指定IP地址：手动指定负载均衡器的IPv4地址。 **说明** 负载均衡器的IP地址不受所在子网的网络ACL配置的限制，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。

5. 您可以为弹性负载均衡配置弹性公网IP满足IPv4公网业务诉求，配置详情见**表2-5**。

表 2-5 为负载均衡器配置弹性公网 IP

参数	说明
弹性公网IP	支持您为负载均衡器配置对应的弹性公网IP以处理IPv4公网业务流量。 • 现在购买：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。 • 暂不购买：您可在弹性负载均衡创建完成后根据实际需求进行弹性公网IP的绑定。。
线路	使用新创建弹性公网IP时，选择的弹性公网IP的线路类型。 • 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。 适用于对网络稳定性和连通性有极高要求的关键业务，如金融交易、在线游戏、大型企业应用、视频直播等。 • 静态BGP：成本低便于自动调度，但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。 适用于网络环境相对稳定，变动较少且自身应用系统具备容灾功能的业务场景。 • 弹性公网IP池：弹性公网IP池为EIP分配全动态BGP线路，持续保证网络稳定、高效。 更多静态BGP与全动态BGP区别信息请参见**静态BGP与全动态BGP有何区别?**

参数	说明
公网带宽	弹性公网IP使用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：共享带宽提供区域级别的带宽复用共享能力，可帮助您节省公网带宽成本。
带宽大小	指定具体的带宽上限。

6. 弹性负载均衡的高级配置支持为实例设置描述和标签，配置详见**表2-6**。

表 2-6 负载均衡器的高级配置

参数	说明
高级配置 > 描述	单击 ，展开折叠的高级配置区域，可以设置该参数。 您可以根据需要在文本框中输入对该负载均衡器的描述信息。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。
高级配置 > 标签	单击 ，展开折叠的高级配置区域，可以设置该参数。 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2-7**。 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 2-7 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。

参数	规则
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。

7. 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。
8. 单击“立即购买”，完成创建。

高频问题

共享型 ELB 实例业务超出性能保障模式上限怎么办?

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

2.3.3 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或删除保护功能，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。

开启或关闭删除保护

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要配置删除保护的负载均衡器名称。
3. 切换到负载均衡实例的“基本信息”页签，开启或关闭“删除保护”开关。

⚠ 注意

如果您的负载均衡实例由云容器引擎服务（CCE）管理，修改负载均衡实例的配置将会影响集群的运行，请您谨慎操作。

4. 删除保护开启后，您将无法删除该负载均衡实例，其余操作不受影响。

开启或关闭修改保护

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要开启修改保护的负载均衡器名称。
3. 切换到负载均衡实例的“基本信息”页签，单击修改保护右侧的“设置”。
4. 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”。

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。

2.3.4 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. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡器列表页面，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. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，待修改带宽的负载均衡器所在行的“操作”列，单击“更多”。
3. 单击“修改IPv4带宽”。
4. 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。
5. 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。

2.3.5 导出共享型负载均衡器

操作场景

您可以将当前账号下拥有的弹性负载均衡信息，以Excel文件的形式导出至本地。

当前支持导出全部实例的基本信息、导出选中部分实例的基本信息，也支持导出选中实例的详细信息。

基本信息：包括负载均衡器的名称、ID、状态、实例类型、规格等信息。

详细信息：默认支持导出负载均衡器的基本信息和监听器的基本信息，额外支持导出监听器的转发策略、后端服务器组、后端服务器和证书（名称/ID）四项信息。

导出实例的基本信息

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡器列表左上方，单击“导出”。
   a. 选择“导出全部实例基本信息到XLSX”：系统会将当前区域内所有弹性负载均衡实例的基本信息自动导出为Excel文件，并下载至本地。
   b. 选择“导出已选中实例基本信息到XLSX”：系统会将当前区域内您所选中的弹性负载均衡实例的基本信息自动导出为Excel文件，并下载至本地。

导出实例的详细信息

如果您想备份弹性负载均衡实例关联监听器、后端服务器组、转发策略、后端服务器和使用证书等信息，您可以选择导出实例的详细信息。

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡器列表左上方，单击“导出”，选择“导出已选中实例详细信息到XLSX”。
3. 在“导出实例”弹窗页面，勾选导出项目。
   a. 默认支持导出负载均衡器的基本信息和监听器的基本信息。
   b. 支持勾选监听器的转发策略、后端服务器组、后端服务器和证书（名称/ID）四项信息。
      支持您勾选“全选”选项，导出实例的全部信息。
4. 单击“确定”，开始导出实例实例的详细信息。
5. 完成导出实例信息后，单击“确定”，关闭弹窗。

查看导出的实例信息

系统会将弹性负载均衡实例的信息自动导出为Excel文件，并下载至本地。

实例的基本信息：每一行数据对应一个弹性负载均衡实例的基本信息。

实例的详细信息：由于一个弹性负载均衡实例可能关联多个监听器和后端服务器组，一个弹性负载均衡实例的详细信息会对应多行数据。

2.3.6 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. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，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。
3. 在删除确认对话框，输入“DELETE”。
4. 单击“确定”。

批量删除按需计费的负载均衡器

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，选择目标负载均衡器后，单击列表页上方的“更多>删除”。

   弹出删除弹性负载均衡器侧拉窗。
3. 您可根据实际业务需求选择勾选如下：
   - 释放负载均衡绑定的弹性公网IP，如不释放可能会被其他资源绑定继续计费。
   - 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负载均衡实例关联使用，将无法执行删除）。
4. 在删除确认对话框，输入“DELETE”。
5. 单击“确定”。

2.3.7 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. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，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”。
3. 单击“是”。
4. 您可以通过弹性负载均衡列表页面的“状态”列，查看目标实例的启停状态。

⚠ 注意

停用的负载均衡器仍会继续计费。

2.3.8 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. 进入**弹性负载均衡列表页面**。
2. 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。
3. 单击性能保障模式的“开启”。
4. 选择“立即开启”即可开启性能保障模式。

图 2-10 开启性能保障模式

2.4 监听器

2.4.1 监听器概述

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2-8**。

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 2-8 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。

⚠ 注意

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 2-9 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 2-10 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

2.4.2 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. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要添加监听器的负载均衡名称。
3. 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2-11**。

表 2-11 共享型负载均衡配置监听器参数说明

参数	说明
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。
监听端口	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]。
获取客户端IP	共享型ELB支持开启此开关，ELB实例与后端服务器之间直接使用客户端真实的IP地址通信。 更多详情请参见**共享型ELB获取客户端真实IP**。

参数	说明
访问控制	当您需要对客户端访问弹性负载均衡实施精细的**IP**控制时，您可以使用ELB监听器的**访问控制**功能来**控制访问ELB监听器的IP地址，**更多信息请参见**访问控制策略**。 监听器的访问控制默认支持“**允许所有IP访问**”。 您可以为监听器的访问控制设置**白名单**或**黑名单**，并选择适用的IP地址组。 • **白名单**：只有白名单中的IP可以访问ELB的监听器。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。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。
更多设置（可选）	
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
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。

4. 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2-23**。
      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2-24**。
5. 单击“下一步：确认配置”。
6. 确认配置无误后，单击“提交”。

2.4.3 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。
- 共享型的UDP监听器的端口当前不支持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. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要添加监听器的负载均衡名称。
3. 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2-12**。

表 2-12 共享型负载均衡配置监听器参数说明

参数	说明
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。
监听端口	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]。
名称（可选）	监听器名称。
获取客户端IP	共享型ELB支持开启此开关，ELB实例与后端服务器之间直接使用客户端真实的IP地址通信。 更多详情请参见**共享型ELB获取客户端真实IP**。
访问控制	当您需要对客户端访问弹性负载均衡实施精细的**IP**控制时，您可以使用ELB监听器的**访问控制**功能来**控制访问ELB监听器的IP地址，**更多信息请参见**访问控制策略**。 监听器的访问控制默认支持“**允许所有IP访问**”。 您可以为监听器的访问控制设置**白名单**或**黑名单**，并选择适用的IP地址组。 • **白名单**：只有白名单中的IP可以访问ELB的监听器。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。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。
更多设置（可选）	

参数	说明
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。

4. 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2-23**。
      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2-24**。
5. 单击“下一步：确认配置”。
6. 确认配置无误后，单击“提交”。

2.4.4 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. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要添加监听器的负载均衡名称。
3. 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2-13**。

表 2-13 共享型负载均衡配置监听器参数说明

参数	说明
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。
监听端口	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
重定向至监听器	将HTTP监听器接受的请求转发至HTTPS监听器，可以加密通信过程，增强业务的安全性。 例如：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。实际业务转发将以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。
获取客户端IP	共享型ELB的HTTP监听器默认支持“获取客户端IP”。 HTTP监听器转发时，支持通过X-Forwarded-For字段传递客户端的真实IP，X-Forwarded-For字段记录的第一个IP地址即为客户端真实IP。 更多详情请参考**共享型ELB获取客户端真实IP**。
访问控制	当您需要对客户端访问弹性负载均衡实施精细的**IP**控制时，您可以使用ELB监听器的**访问控制**功能来**控制访问ELB监听器的IP地址，**更多信息请参见**访问控制策略**。 监听器的访问控制默认支持“**允许所有IP访问**”。 您可以为监听器的访问控制设置**白名单**或**黑名单**，并选择适用的IP地址组。 • **白名单**：只有白名单中的IP可以访问ELB的监听器。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。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。
更多设置（可选）	
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。

参数	说明
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。
附加HTTP头字段	通过重写X-Forwarded-ELB-IP字段获取负载均衡实例的公网IP地址。

4. 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2-23**。
      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2-24**。
5. 单击“下一步：确认配置”。
6. 确认配置无误后，单击“提交”。

2.4.5 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. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要添加监听器的负载均衡名称。
3. 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2-14**。

表 2-14 共享型负载均衡配置监听器参数说明

参数	说明
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。
监听端口	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]。
获取客户端IP	共享型ELB的HTTPS监听器默认支持“获取客户端IP”。 HTTPS监听器转发时，支持通过X-Forwarded-For字段传递客户端的真实IP，X-Forwarded-For字段记录的第一个IP地址即为客户端真实IP。 更多详情请参考**共享型ELB获取客户端真实IP**。
访问控制	当您需要对客户端访问弹性负载均衡实施精细的**IP**控制时，您可以使用ELB监听器的**访问控制**功能来**控制访问ELB监听器的IP地址**，更多信息请参见**访问控制策略**。 监听器的访问控制默认支持“**允许所有IP访问**”。 您可以为监听器的访问控制设置**白名单**或**黑名单**，并选择适用的IP地址组。 • **白名单**：只有白名单中的IP可以访问ELB的监听器。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。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。
证书配置	
SSL解析方式	请选择客户端到服务器端认证方式。 • **单向认证**：仅客户端对服务器端的身份进行认证。 • **双向认证**：客户端对服务器端的身份进行认证，服务器端也需要对客户端的身份进行认证。
服务器证书	协议类型为HTTPS时，需绑定服务器证书。 服务器证书用于SSL握手协商，需提供证书内容和私钥。
CA证书	协议类型为HTTPS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。在进行双向认证时，只有当客户端能够出具指定CA签发的证书，HTTPS连接才能成功。

参数	说明
SNI	SNI（Server Name Indication 服务器名称指示）是一种TLS协议的扩展，用于解决在一个监听器托管多个域名时，需要根据不同的请求域名匹配证书进行认证的问题。 客户端在发起SSL握手请求时提交请求的域名信息，ELB在收到请求后，会根据请求的域名查找证书。 如果能够找到请求域名对应的SNI证书，则使用该证书进行认证。 如果没有找到请求域名对应的SNI证书，则使用**服务器证书**进行认证。 详情请参见**开启SNI证书实现多域名访问**。
SNI证书	开启SNI之后，您需要为监听器配置至少一个SNI证书。 只能选择指定了**SNI扩展域名**的服务器证书。
更多配置（可选）	
安全策略	支持选择可用的安全策略，更多信息请参见**配置TLS安全策略实现加密通信**。
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**。
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。
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。
附加HTTP头字段	通过重写X-Forwarded-ELB-IP字段获取负载均衡实例的公网IP地址。

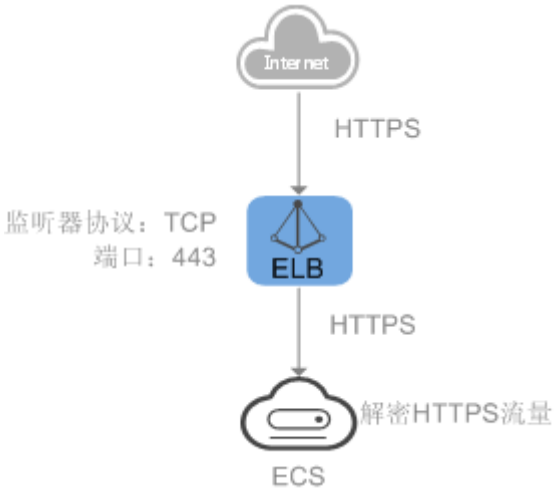
4. 单击“下一步：配置后端分配策略”，配置监听器的默认后端服务器组。
   a. 推荐选择“使用已有”后端服务器组，您可参考**创建后端服务器组**进行创建。
   b. 您也可选择“新创建”后端服务器组，添加后端服务器并配置健康检查，
      i. 配置后端服务器组参数请参见**表2-23**。
      ii. 单击“下一步：添加后端服务器”，添加后端服务器并配置健康检查。
      添加后端服务器详见**后端服务器概述**，配置健康检查参数请参见**表2-24**。
5. 单击“下一步：确认配置”。
6. 确认配置无误后，单击“提交”。

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 2-11 TCP 透传 HTTPS 流量



2.4.6 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路径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**、**路径**。
- 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）。
  - 一条转发策略的转发规则中添加了域名和路径时，请求需同时满足域名和路径的条件，才能匹配到该条转发策略。
- 匹配优先级：
  - 当请求同时满足转发动作分别为域名和路径的两条转发策略时，优先按照域名进行匹配，如表2-15。
  - 不同域名间优先级互相独立。
  - 转发规则为路径时，匹配优先级如下：精确匹配 > 前缀匹配 > 正则匹配，匹配类型相同时路径长度越长，优先级越高。

表 2-15 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	路径	/test
	2	域名	www.elb.com

说明

如表2-15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：
  - 转发规则路径不支持查询字符串。如果您的路径设置为/path/resource?name=value，该条转发策略将失效。
  - 每个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“路径匹配规则”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. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要添加转发策略的负载均衡器名称。
3. 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。
4. 单击“添加转发策略”按钮。参考**表2-16**配置参数。
5. 配置完成，单击“保存”。

表 2-16 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。 域名或者路径至少要指定一个。	www.test.com
	路径	• 匹配说明 触发转发的路径，由英文字母、数字和特殊字符_~';@^-%#$.*+?,=!:|\/()[]{}组成。 • 匹配方式 – 精确匹配：请求的路径和设定的路径完全一致，只能由/开头。 – 前缀匹配：请求的路径匹配已设定路径开头的，只能由/开头。 – 正则匹配：请求的路径和设定的路径正则表达式匹配。	/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

参数		说明	样例
	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。	-
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。	-

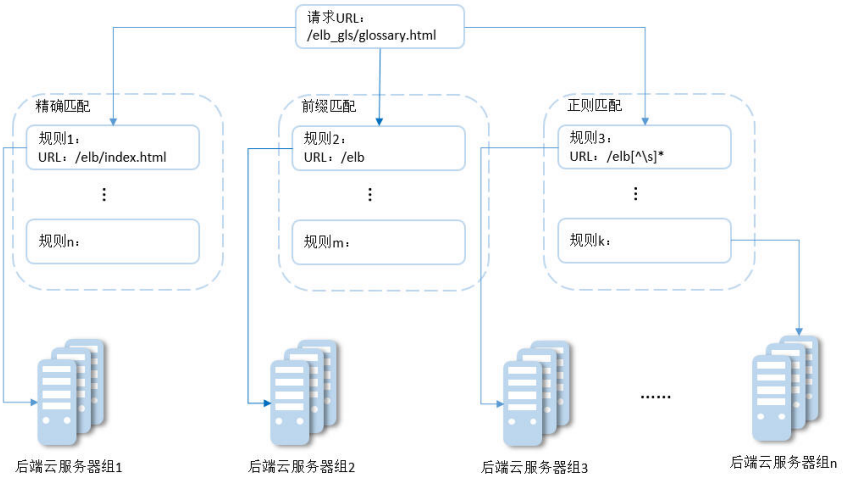
路径匹配示例

如表2-17所示，是一个路径匹配示例，转发情况如图2-12所示。

表 2-17 路径匹配示例

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

图 2-12 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. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要修改转发策略的负载均衡器名称。
3. 切换到监听器页签，单击需要修改转发策略的监听器名称。
4. 切换到“转发策略”页签，选择需要修改的转发策略，单击“编辑”。
5. 根据界面提示修改参数，单击“保存”。

删除转发策略

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要删除转发策略的负载均衡器名称。
3. 切换到监听器页签，单击需要删除转发策略的监听器名称。
4. 切换到“转发策略”页签，选择需要删除的转发策略，单击“删除”。
5. 在弹出的“删除转发策略”对话框中，单击“确定”。

2.4.7 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. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要开启HTTP/2功能的监听器的负载均衡器名称。
3. 在该负载均衡界面的“监听器”页签，单击“添加监听器”。
4. 在“添加监听器”界面，前端协议选择“HTTPS”。
5. 在“添加监听器”界面，展开高级配置，打开HTTP/2功能。
6. 确认配置，单击“提交”。

图 2-13 开启 HTTP 监听器的 HTTP/2 功能

已有 HTTPS 监听器

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要修改HTTP/2功能的负载均衡器名称。
3. 在“监听器”页签，单击需要修改HTTP/2功能开关的监听器名称。
4. 在监听器的“基本信息”页面，单击“编辑监听器”。
5. 在“编辑监听器”界面，展开高级配置，开启或者关闭HTTP/2功能。
6. 单击“确定”。

图 2-14 修改 HTTPS 监听器的 HTTP/2 功能

2.4.8 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**购买共享型负载均衡器**。
- 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**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. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要为监听器配置修改保护的负载均衡名称。
3. 在“监听器”页签，单击需要为配置修改保护的监听器名称。
4. 在监听器的“基本信息”页签，单击修改保护右侧的“设置”。
5. 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. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要修改监听器的负载均衡名称。
3. 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”。
4. 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. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要修改监听器的负载均衡名称。
3. 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。
4. 在监听器的“基本信息”页面，单击“编辑监听器”。
5. 在“编辑监听器”页面，单击“高级配置”。
6. 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”。
7. 单击“确定”。

更换监听器的后端服务器组

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击目标监听器所在的负载均衡名称。
3. 选择“监听器”页签，在监听器列表中，单击目标监听器的名称。
4. 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”。
5. 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。
6. 单击“确定”。

2.4.9 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. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要删除监听器的负载均衡名称。
   a. 删除单个监听器：
      i. 在“监听器”页签，需要删除监听器所在行的“操作”列，单击“删除 ”。
      ii. 在删除监听器的弹窗页面，输入“DELETE”。
   b. 批量删除监听器：
      i. 在“监听器”页签，勾选多个希望删除的监听器。
      ii. 单击“监听器”列表页面上方的“删除”。
      iii. 在删除监听器的侧拉弹窗页面，输入“DELETE”。
3. 单击“确定”，完成删除。

2.5 后端服务器组

2.5.1 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 2-18 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 2-19 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	仅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。

控制后端服务器组流量分发

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2-20**所示的关键功能可供用户配置。

表 2-20 后端服务器组关键功能

关键功能	功能说明	功能详情
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。	**配置流量分配策略分配流量**
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。	**配置会话保持提升访问效率**

后端服务器组与监听器协议匹配关系

共享型负载均衡使用场景下，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。

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2-21**。

表 2-21 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

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

2.5.2 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。

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 2-22 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**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**。
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. 进入**后端服务器组列表页面**。
2. 在后端服务器组列表页面，单击页面右上角“创建后端服务器组”按钮。
3. 配置后端分配策略，参数详情请参见**表2-23**。

表 2-23 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**配置流量分配策略分配流量**。
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**配置会话保持提升访问效率**。
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。

4. 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2-24**。更多关于健康检查的信息，请参见**健康检查介绍**。

表 2-24 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，字符串间以点分隔，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]。

5. 单击“下一步”。
6. 确认配置无误后，单击“立即创建”。

2.5.3 控制后端服务器组流量分发

2.5.3.1 配置流量分配策略分配流量

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 2-25 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。
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2-15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 2-15 加权轮询算法流量分发

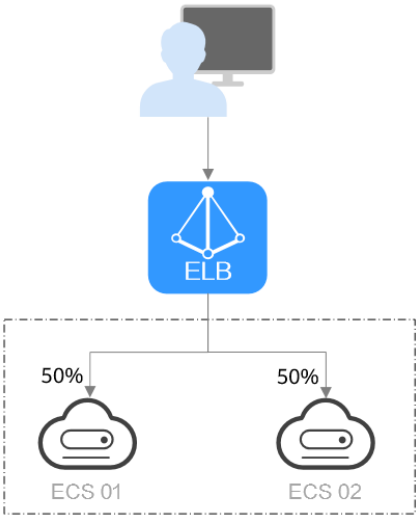


表 2-26 加权轮询算法说明

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2-16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 2-16 加权最少连接算法流量分发

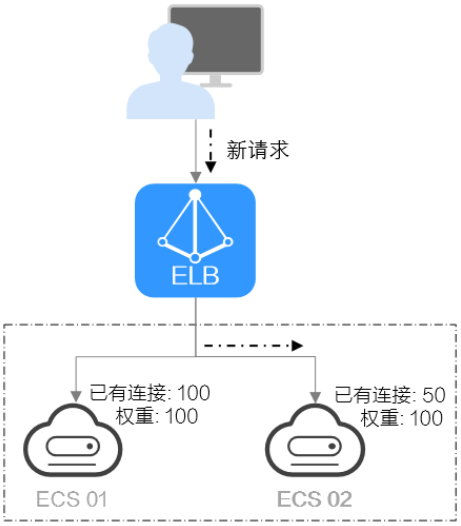


表 2-27 加权最少连接说明

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2-17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 2-17 源 IP 算法流量分发

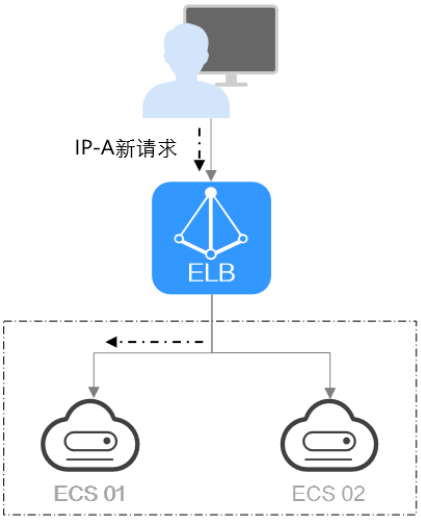


表 2-28 源 IP 算法说明

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。

修改流量分配策略

1. 进入后端服务器组列表页面。

2. 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”。
3. 在“修改后端服务器组”弹窗中进行修改，选择“分配策略类型”。
4. 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。

2.5.3.2 配置会话保持提升访问效率

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 2-29 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。

类型	说明	支持的会话保持类型	会话保持时间	会话保持失效的场景
七层会话保持	当使用的协议为HTTP或HTTPS时，即为七层会话保持。	• **负载均衡器cookie**：负载均衡器会根据客户端第一个请求生成一个cookie，后续所有包含这个cookie值的请求都会由同一个后端服务器处理。 • **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。

配置会话保持

1. 进入**后端服务器组列表页面**。
2. 在后端服务器组列表页面，在目标后端服务器组所在行的操作列单击“编辑”。
3. 在“修改后端服务器组”弹窗中，开启或关闭会话保持功能。
   开启会话保持功能需配置会话保持类型以及会话保持时间参数。

4. 单击“确定”。

2.5.4 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2-21**。
- 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. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击目标监听器所在的负载均衡名称。
3. 选择“监听器”页签，在监听器列表中，单击目标监听器的名称。
4. 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”。
5. 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。
6. 单击“确定”。

2.5.5 管理后端服务器组

当您的后端服务器组创建后，您可以根据实际使用需求对服务器组进行管理。

配置后端服务器组修改保护

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。

后端服务器组开启修改保护后，您将无法对后端服务器组执行编辑和配置健康检查，也无法管理组内的后端服务器。

1. 进入**后端服务器组列表页面**。
2. 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。
3. 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”。
4. 在设置修改保护弹窗中，开启“修改保护”开关。
5. 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。

配置后端服务器组的后端服务器移除保护

您可以对后端服务器组开启移除保护功能，防止因误操作导致后端服务器组内的后端服务器被移除。

后端服务器组开启移除保护后，您将无法移除组内的后端服务器。

注意

如果您的负载均衡实例由云容器引擎服务（CCE）管理，开启后端服务器组的移除保护可能影响集群的正常运行，请您谨慎操作。

1. 进入**后端服务器组列表页面**。
2. 在后端服务器组列表页面，单击需要配置修改保护的后端服务器组名称。
3. 在后端服务器组的“基本信息”页签下，单击移除保护开关进行配置。

说明

如果您需要移除后端服务器组的后端服务器，请先关闭“移除保护”开关。

查看后端服务器组

您可以根据需要查看后端服务器组的的详细信息。

1. 进入**后端服务器组列表页面**。
2. 在后端服务器组列表页面，单击待查看的后端服务器组名称。
3. 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，包括名称、ID、后端协议和健康检查的详细配置信息。
   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资源。

删除后端服务器组

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。

1. 进入**后端服务器组列表页面**。

2. 在后端服务器组列表页面，在目标后端服务器组所在行的操作列单击“删除”。
3. 在“确认删除后端服务器组”对话框中，单击“确定”。

批量删除后端服务器组

说明

支持批量删除后端服务器组功能陆续上线中，请以控制台实际为准。

1. 进入**后端服务器组列表页面**。
2. 在后端服务器组列表页面，勾选希望删除的多个后端服务器组。
3. 单击后端服务器组列表页上方的“删除”。
4. 在“删除后端服务器组”侧拉对话框中，输入“DELETE”。
5. 单击“确定”，完成删除。

2.6 后端服务器

2.6.1 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2-30**，更多流量策略分配策略详情见**配置流量分配策略分配流量**。

表 2-30 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。

2.6.2 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，若后端服务器的子网关联了网络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. 进入**弹性云服务器列表**页面。
2. 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。
3. 选择“安全组”页签，单击安全组名称，查看安全组规则。
4. 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2-31**配置安全组入方向的访问规则。

   表 2-31 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

5. 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”。

2.6.3 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. 进入**后端服务器组列表页面**。
2. 在后端服务器组列表页面，单击需要添加后端服务器的后端服务器组名称。
3. 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”。
4. 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。
5. 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。

批量导入云服务器

1. 进入**后端服务器组列表页面**。
2. 在后端服务器组列表页面，单击需要添加后端服务器的后端服务器组名称。
3. 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”。
4. 在“添加后端服务器”侧拉窗中，单击“批量导入”。
5. 在“导入”弹窗中，您可单击“下载模板”下载模板文件到本地。
   模板文件需要您填写私网IP地址、业务端口和权重。
6. 单击“添加文件”，上传您本地配置完成的导入文件。
   系统将为您匹配导入文件对应的云服务器信息。
7. 选中目标添加的后端服务器，单击“导入”。

修改后端云服务器的权重和端口

1. 进入**后端服务器组列表页面**。
2. 在后端服务器组列表页面，单击需要修改后端服务器端口/权重的后端服务器组名称。
3. 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。
4. 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”。
5. 在“修改权重”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。
6. 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. 进入**后端服务器组列表页面**。
2. 在后端服务器组列表页面，单击需要移除后端服务器的后端服务器组名称。
3. 切换到“后端服务器”页签，选择下方“云服务器”页签。
4. 勾选需要移除的云服务器，单击服务器列表上方的“移除”。
5. 在移除后端服务器的对话框中单击“确定”。

2.7 健康检查

2.7.1 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**配置健康检查**。

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2-32**。

表 2-32 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

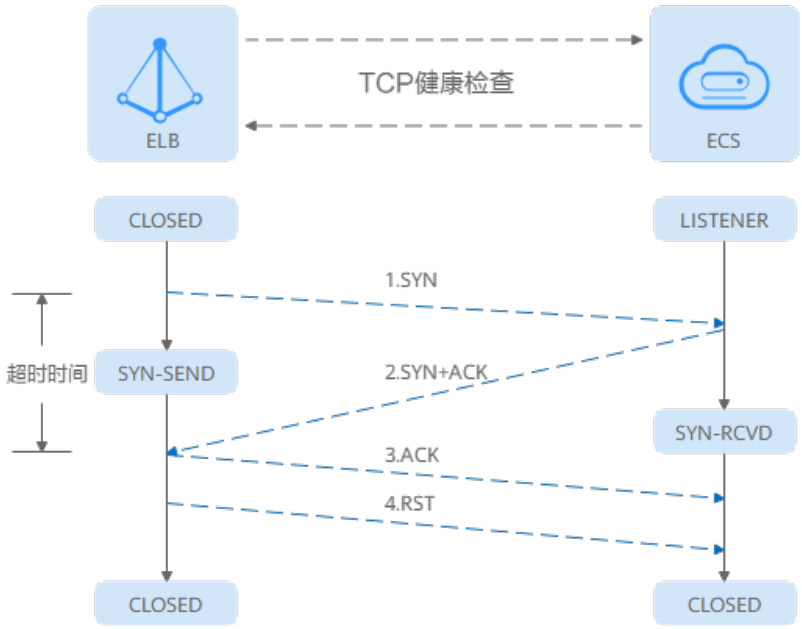
健康检查源 IP

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2-18**所示。

图 2-18 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。

⚠ 注意

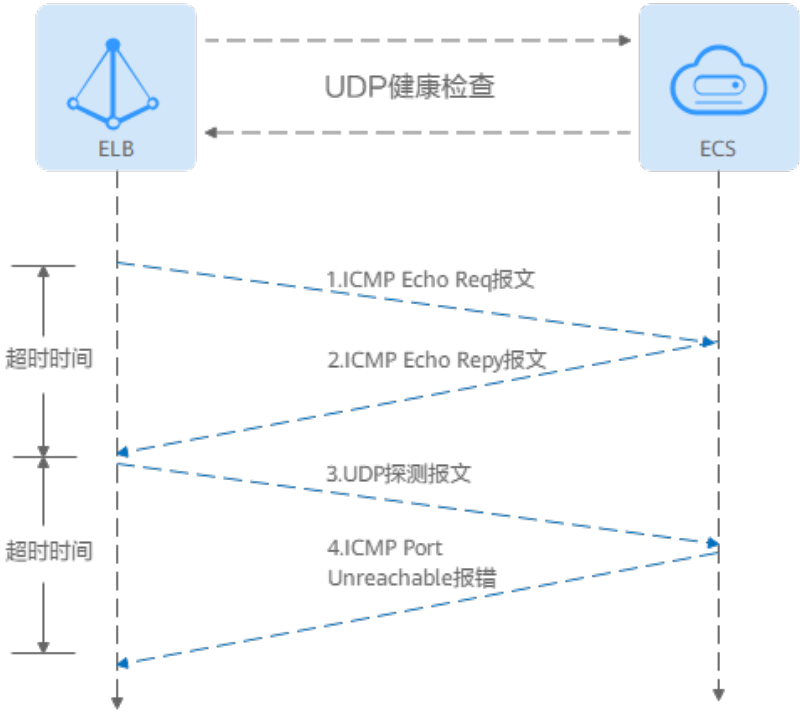
正常的TCP三次握手后，会进行数据传输，但是在健康检查时会发送RST中断建立的TCP连接。该实现方式可能会导致后端服务器中的应用认为TCP连接异常退出，并打印错误信息，如“Connection reset by peer”。解决方案如下：

- 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2-19**所示。

图 2-19 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。

⚠ 注意

- 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。
- UDP探测报文的载荷（playload）无实际意义，仅用于填充发送报文时的内容，通常为字符“H”，不建议客户服务端解析该内容。

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2-20所示。

图 2-20 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。

⚠ 注意

在HTTP健康检查请求中，User-Agent头字段主要用于标识此类请求为健康检查发出的探测请求。User-Agent的值可能随业务需求而动态调整，建议您的后端服务请勿根据此header头做检验和判断。

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2-33中的三个因素决定：

表 2-33 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)

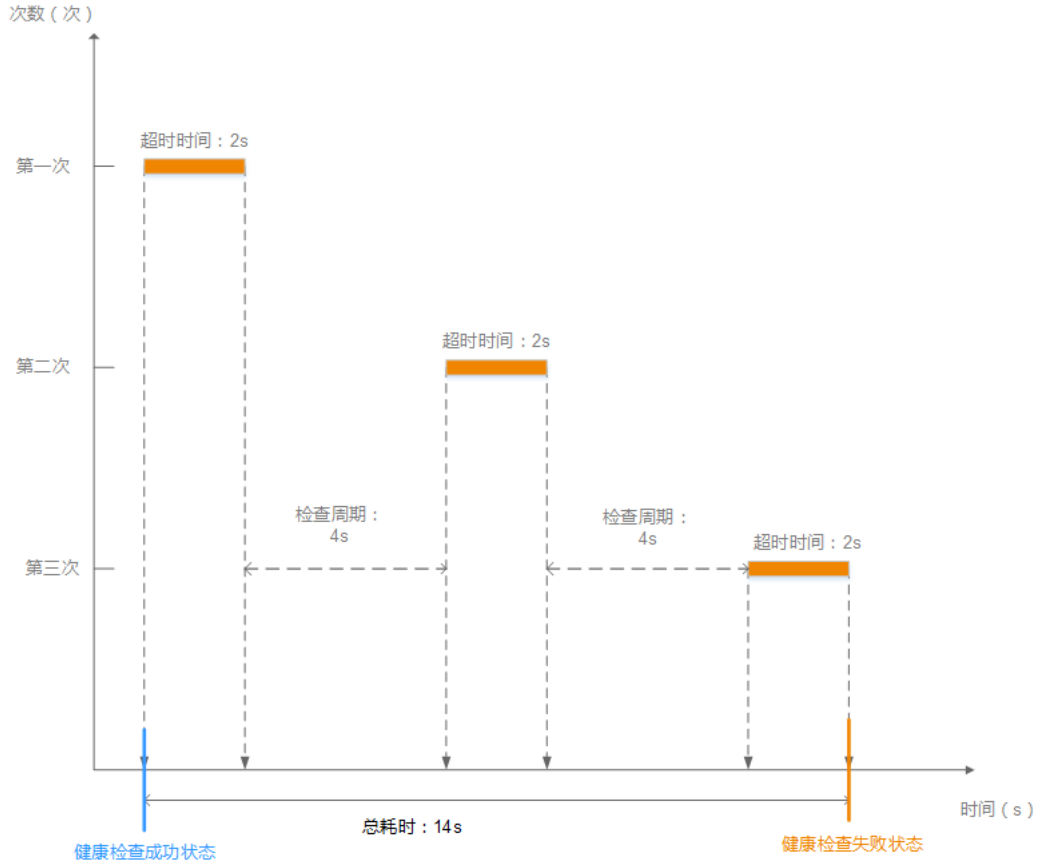
- 健康检查失败时间窗 = 超时时间×健康检查异常阈值 + 检查间隔×(健康检查异常阈值-1)

如图2-21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 2-21 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**。

2.7.2 配置健康检查

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. 进入**后端服务器组列表页面**。
2. 在后端服务器组列表页面，单击需要修改健康检查的后端服务器组名称。
3. 在后端服务器组的“基本信息”页签下，单击健康检查区域右侧的“配置健康检查”。
4. 在“配置健康检查”弹窗，可根据需要参考**表2-34**进行配置。

表 2-34 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。 **说明** 开启或关闭健康检查期间，监控指标正常主机数/异常主机数会出现短暂波动，一个监控周期后可恢复。
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。 ● TCP和UDP健康检查协议使用HTTP1.0版本。 ● HTTP健康检查协议使用HTTP1.1版本。
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，字符串间以点分隔，且总长度不超过100个字符。

参数	说明
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]。

5. 单击“确定”。

关闭健康检查

1. 进入**后端服务器组列表页面**。
2. 在后端服务器组列表页面，单击需要关闭健康检查的后端服务器组名称。
3. 在后端服务器组的“基本信息”页签下，单击健康检查区域右侧的“配置健康检查”。
4. 在“配置健康检查”界面，可根据需要关闭健康检查。
5. 单击“确定”。

2.8 安全管理

2.8.1 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2-35**。

表 2-35 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”

⚠ 注意

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。

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要修改监听器的负载均衡名称，进入监听器列表页。
3. 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”。
4. 在“编辑监听器”弹窗页面，开启“获取客户端IP”开关。
5. 确认相关信息，单击“确定”。

关闭“获取客户端 IP”

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要修改监听器的负载均衡名称，进入监听器列表页。

3. 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”。
4. 在“编辑监听器”弹窗页面，关闭“获取客户端IP”开关。
5. 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2-36**。

表 2-36 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**。

2.8.2 开启 SNI 证书实现多域名访问

SNI（Server Name Indication 服务器名称指示）是一种TLS协议的扩展，用于解决在一个监听器托管多个域名时，需要根据不同的请求域名匹配证书进行认证的问题。

SNI 概述

当您需要在同一个监听器上部署多个HTTPS后端服务时，每个服务可能使用不同的域名和证书，并需要将请求分发至不同的后端服务器组。

如果HTTPS监听器只绑定一个服务器证书，监听器将无法根据客户端请求的域名动态选择对应的证书进行认证，导致多域名场景认证异常。

开启SNI功能支持您扩展监听器上配置的证书，实现监听器根据请求域名的不同自动选择匹配的证书传递到客户端进行认证。客户端在发起SSL握手请求时提交请求的域名信息，ELB在收到请求后根据请求的域名查找对应的证书，如果监听器没有匹配到域名对应的证书，ELB将使用默认的服务器证书进行认证。

SNI 证书

- SNI证书是用于多域名认证场景的**服务器证书**，即指定了**SNI扩展域名**的服务器证书。在ELB控制台指定的**SNI扩展域名**必须与证书实际支持认证的域名保持一致。
- 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。在选择认证证书时，如果同域名绑定了两个证书，ELB会优先选择ECC类型的证书。

约束与限制

- 开启SNI后，需选择SNI证书，具体步骤可参照**创建证书**。
- 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。

证书匹配规则

- 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。

- cert-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证书认证鉴权。如果匹配失败，则会返回默认的服务器证书认证鉴权。

监听器开启 SNI

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击目标负载均衡器的名称。
3. 在“监听器”页签，单击需要开启SNI的监听器名称。
4. 在监听器基本信息页面，单击SNI右侧“配置”。
5. 开启SNI的开关，选择需要配置的SNI证书。
6. 单击“确定”。

2.8.3 配置 TLS 安全策略实现加密通信

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. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要创建安全策略的监听器的负载均衡器名称。
3. 在该负载均衡界面的“监听器”区域，单击“添加监听器”。
4. 在“添加监听器”界面，前端协议选择“HTTPS”。
5. 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2-37**所示。

表 2-37 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	
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。

6. 配置完成，单击“确定”。

共享型默认安全策略差异说明

表 2-38 安全策略差异说明

安全策略	tls-1-0	tls-1-1	tls-1-2	tls-1-2-strict
TLS 协议				
Protocol-TLS 1.3	-	-	-	-
Protocol-TLS 1.2	√	√	√	√
Protocol-TLS 1.1	√	√	-	-
Protocol-TLS 1.0	√	-	-	-
加密套件				
EDHE-RSA-AES128-GCM-SHA256	√	√	√	√
ECDHE-RSA-AES256-GCM-SHA384	√	√	√	√
ECDHE-RSA-AES128-SHA256	√	√	√	√
ECDHE-RSA-AES256-SHA384	√	√	√	√
AES128-GCM-SHA256	√	√	√	√
AES256-GCM-SHA384	√	√	√	√
AES128-SHA256	√	√	√	√
AES256-SHA256	√	√	√	√
ECDHE-RSA-AES128-SHA	√	√	√	-
ECDHE-RSA-AES256-SHA	√	√	√	-
AES128-SHA	√	√	√	-
AES256-SHA	√	√	√	-
ECDHE-ECDSA-AES128-GCM-SHA256	√	√	√	√
ECDHE-ECDSA-AES128-SHA256	√	√	√	√
ECDHE-ECDSA-AES128-SHA	√	√	√	-
ECDHE-ECDSA-AES256-GCM-SHA384	√	√	√	√

安全策略	tls-1-0	tls-1-1	tls-1-2	tls-1-2-strict
ECDHE-ECDSA-AES256-SHA384	√	√	√	√
ECDHE-ECDSA-AES256-SHA	√	√	√	-
ECDHE-RSA-AES128-GCM-SHA256	-	-	-	-
TLS_AES_256_GCM_SHA384	-	-	-	-
TLS_CHACHA20_POLY1305_SHA256	-	-	-	-
TLS_AES_128_GCM_SHA256	-	-	-	-
TLS_AES_128_CCM_8_SHA256	-	-	-	-
TLS_AES_128_CCM_SHA256	-	-	-	-
DHE-RSA-AES128-SHA	-	-	-	-
DHE-DSS-AES128-SHA	-	-	-	-
CAMELLIA128-SHA	-	-	-	-
EDH-RSA-DES-CBC3-SHA	-	-	-	-
DES-CBC3-SHA	-	-	-	-
ECDHE-RSA-RC4-SHA	-	-	-	-
RC4-SHA	-	-	-	-
DHE-RSA-AES256-SHA	-	-	-	-
DHE-DSS-AES256-SHA	-	-	-	-
DHE-RSA-CAMELLIA256-SHA	-	-	-	-
ECC-SM4-SM3	-	-	-	-
ECDHE-SM4-SM3	-	-	-	-

修改安全策略

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. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要修改安全策略的监听器的负载均衡器名称。
3. 切换至“监听器”页签，单击需要修改安全策略的监听器名称。

4. 在监听器的基本信息页面，单击“编辑监听器”。
5. 在“编辑监听器”界面，展开高级配置，选择安全策略参数。
6. 单击“确定”。

2.8.4 访问控制

2.8.4.1 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ELB绑定的IP地址。
- 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ELB绑定的IP地址。
- 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. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击负载均衡名称，进入监听器管理界面。
3. 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”。
4. 在“设置访问控制”的弹窗中，如**表2-39**所示配置访问控制。

表 2-39 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。

参数	说明
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。

5. 配置完成，单击“确定”。

2.8.4.2 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。
- 单监听器的访问控制策略，最多支持选择5个IP地址组。IP地址组内合计最多可添加300个IP地址或网段。

说明

如果您希望扩大IP地址组支持添加的地址或网段数量，可以提交**工单**进行处理。

创建 IP 地址组

1. 进入**弹性负载均衡列表页面**。
2. 在左侧导航栏，选择“ 弹性负载均衡 > IP地址组”。
3. 在“IP地址组”界面，单击“创建IP地址组”。
4. 配置IP地址组参数，参数说明参见**表2-40**。

表 2-40 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》**。	-
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。	-

5. 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. 进入**弹性负载均衡列表页面**。
2. 在左侧导航栏，选择“ 弹性负载均衡 > IP地址组”。
3. 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。
4. 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。

5. 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. 进入**弹性负载均衡列表页面**。
2. 在左侧导航栏，选择“ 弹性负载均衡 > IP地址组”。
3. 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

如果您希望批量删除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. 进入**弹性负载均衡列表页面**。
2. 在左侧导航栏，选择“ 弹性负载均衡 > IP地址组”。
3. 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。
4. 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。
5. 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. 进入**弹性负载均衡列表页面**。
2. 在左侧导航栏，选择“ 弹性负载均衡 > IP地址组”。
3. 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。
4. 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. 进入**弹性负载均衡列表页面**。
2. 在左侧导航栏，选择“ 弹性负载均衡 > IP地址组”。
3. 在“IP地址组”界面，需要删除的IP地址组所在行，单击“删除”。
4. 确认需要删除的IP地址组，单击“是”。

2.8.5 证书管理

2.8.5.1 证书概述

在弹性负载均衡服务配置单向认证或双向认证时，您需要为HTTPS或TLS监听器配置证书。弹性负载均衡证书管理控制台支持获取您在华为云云证书与管理服务中统一管理的SSL服务器证书，也支持您上传您本地拥有的证书。

证书使用场景

当您为弹性负载均衡添加HTTPS或TLS监听器来转发业务请求时，您需要选择SSL解析认证方式。单向认证需要为监听器配置服务器证书，双向认证需要同时配置服务器证书和CA证书。

表 2-41 SSL 解析方式

单向认证	仅客户端对服务器端进行认证，您需要为监听器绑定服务器证书，用于验证服务器身份。
双向认证	弹性负载均衡实例与客户端互相提供身份认证，从而允许通过认证的用户访问实例。您需要为监听器绑定服务器证书和CA证书，分别用于验证服务器和客户端的身份，后端服务器无需额外配置双向认证。

弹性负载均衡支持创建三种类型的证书，服务器证书、CA证书、服务器SM双证书。

表 2-42 证书类型

服务器证书	在使用HTTPS或TLS协议时，服务器证书用于SSL握手协商过程验证服务器的身份，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签发机构的身份。在配置双向认证功能时，只有当客户端能够出具指定CA签发的证书时，才能成功建立连接。

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。 ● **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

服务器SM双证书持续上线中，请以控制台实际为准。

视频介绍

本视频介绍在ELB服务中如何管理证书。

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-----
```

格式转换

弹性负载均衡仅支持PEM格式的证书，其它格式的证书需要转换成PEM格式后，才能上传到弹性负载均衡服务。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
```

2.8.5.2 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：在使用HTTPS协议时，服务器证书用于SSL握手协商。同时支持云证书与管理服务提供的服务器数字证书和您的自有证书。
- 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。仅支持上传您的自有CA证书。
- 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，当前不支持SM双证书的证书链。同时支持云证书与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2-43**。

表 2-43 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。

参数	说明
证书来源	服务器证书同时支持云证书与管理服务中SSL证书管理提供的数字证书和您的自有证书。 ● SSL证书管理：云证书与管理服务中统一管理的SSL服务器数字证书，您需要到云证书与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** 推荐使用云证书与管理服务对您的证书进行统一管理。
证书	仅云证书与管理服务中SSL证书管理提供的证书支持该参数。 选择您在云证书与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，只能由中文、英文字母、数字、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。
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-----
SNI扩展域名（可选）	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2-44。

表 2-44 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。 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2-45。

表 2-45 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，当前不支持SM双证书的证书链。
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。 ● SSL证书管理服务：云证书与管理服务中统一管理的SSL服务器数字证书，您需要到云证书与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** 推荐使用云证书与管理服务对您的证书进行统一管理。
证书	仅SSL证书管理的证书支持该参数。 支持选择您在云证书与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。

2.8.5.3 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**通过编辑监听器更换证书**操作。

快速查询证书关联的监听器

1. 进入**证书管理列表页面**。
2. 在证书列表中，在“关联负载均衡丨监听器 (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“关联负载均衡丨监听器 (前端协议/端口)”所在列，单击“查看所有”，即可查看证书关联的所有监听器。

修改证书信息

1. 进入**证书管理列表页面**。
2. 在证书列表中，在需要修改的证书所在行，单击“修改”。
3. 在“修改证书”对话框中，修改证书的相关信息。
4. 确认修改信息，单击“确定”，完成修改。

2.8.5.4 绑定/更换证书

操作场景

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

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

说明

弹性负载均衡的证书和私钥的更换对业务没有影响。

约束与限制

- 仅HTTPS/TLS/QUIC协议的监听器才支持配置证书。
- 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**。

通过编辑监听器更换证书

1. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页面，单击需要更换监听器证书的负载均衡名称。
3. 在“监听器”页签下，单击目标监听器所在行操作列的“编辑”。
4. 在“服务器证书”或“CA证书”下选择需要更换的证书。
5. 在“编辑监听器”对话框中，单击“确定”。

2.8.5.5 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，从而简化证书管理操作流程，提高运维效率。

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/QUIC协议的监听器才支持绑定/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。

通过修改证书批量更换监听器的证书

1. 进入**弹性负载均衡列表页面**。
2. 在左侧导航栏单击“证书管理”。
3. 在证书列表中，在需要修改的证书所在行，单击“修改”。
4. 在“修改证书”对话框中，修改证书的相关信息。
5. 确认修改信息，单击“确定”，完成修改。

2.8.6 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 2-22 安全设置

3. 在“安全设置”页面中，选择“敏感操作 > 操作保护 > 立即启用”。

图 2-23 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 2-24 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 2-25 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 2-26 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?

2.9 访问日志

操作场景

在您使用共享型ELB期间，支持对采用HTTP/HTTPS监听器的负载均衡实例的访问日志进行记录，包括请求时间、客户端IP地址、请求路径和服务器响应等。

弹性负载均衡ELB支持将七层监听器转发的业务接入云日志服务进行分析，云日志将记录包括请求时间、客户端IP地址、请求路径和服务器响应等信息。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，快速定位出异常的后端服务器。

警告

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。

费用说明

ELB接入云日志后，云日志服务根据日志读写流量、日志存储量、日志转测的流量等计费，云日志服务的详细计费信息请参考**云日志服务的计费项**。

约束与限制

- 仅采用HTTP/HTTPS监听器的共享型负载均衡实例支持配置访问日志。
- 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**购买共享型负载均衡器**。
- 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**。

配置访问日志

1. 进入**弹性负载均衡列表页面**。
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”。

图 2-27 配置访问日志入口

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。

   如果您尚未在云日志服务创建日志组和日志流，可以在ELB服务控制台进行创建。

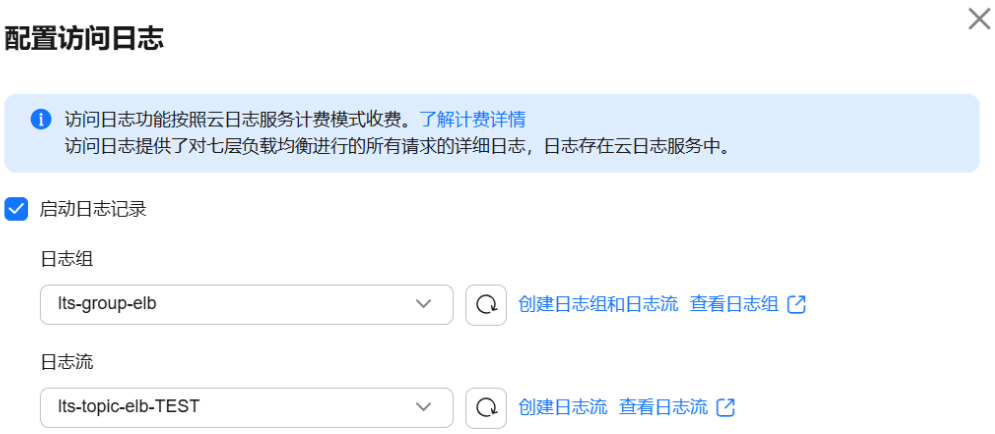
   单击查看创建日志组和日志流详情

   a. 单击“创建日志组和日志流”。
   b. 在“创建日志组&日志组”侧拉窗中，设置日志组名称、日志流名称和日志存储时间。

   图 2-28 在 ELB 服务控制台创建日志组和日志流

   c. 单击“确定”，完成日志组和日志流的创建。

图 2-29 启动日志记录



5. 单击“确定”，配置完成。

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2-46。

表 2-46 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

参数	描述	取值说明	示例取值
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
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

参数	描述	取值说明	示例取值
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）
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"

参数	描述	取值说明	示例取值
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_20679192-8888-4e62-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
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)

参数	描述	取值说明	示例取值
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。

相关文档

- 最佳实践：**通过ELB的访问日志查询客户端请求源IP**。
- 如果您希望将日志转储进行二次分析，您可以配置日志转储，详情请参考**日志转储**。
- 如果您希望对ELB的日志数据进行统一管理，请参考如下文档：
  - 在云日志控制台接入LTS：**弹性负载均衡 ELB接入LTS**。
  - AOM支持创建日志指标规则，将ELB上报到LTS的日志数据提取为指标来统一管理，便于后续在指标浏览、仪表盘界面实时监控。通过接入AOM，您可以对日志进行统计，支持以下统计类型：count、countKeyword、sum、avg、max、min、P50、P75、P90、P95和P99，详情请参见**配置日志指标接入AOM**。

- API操作：**创建云日志**、**查询云日志详情**。

2.10 资源和标签

2.10.1 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**购买共享型负载均衡器**。
- 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。

2.10.2 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”。

设置配额预警

弹性负载均衡的配额项支持设置配额预警，当配额达到预警阈值时，您会收到告警通知，方便您提前申请提升配额。

创建了配额预警后，系统会根据预先设置的预警阈值每小时审计一次，若超过预警阈值则会发送预警消息。预警消息的发送需间隔24小时，若发送预警消息后24小时内，再次超过预警阈值，则不会再次发送预警消息。

1. 登录华为云首页。
1. 单击页面右上角的“管理控制台”。
2. 系统进入“管理控制台”页面。
3. 单击管理控制台左上角的 ，选择区域和项目。
4. 在页面右上角，选择“资源 > 我的配额”。

5. 单击左侧“配额预警”，系统进入“配额预警”页面。
6. 您可以在“配额预警”页面，单击“设置预警”。
7. 对各项资源配置预警阈值、预警区域参数。
8. 打开“发送通知”，设置“通知对象”。
9. 设置完成后，单击“保存”。

2.11 使用 CES 监控 ELB

2.11.1 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 ”，在右侧页面选择“弹性负载均衡 ELB”。
5. 在“云服务监控详情页”单击需要查看监控指标的负载均衡器名称。

或者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。

2.11.2 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

负载均衡器的监控指标

共享型负载均衡支持负载均衡器和监听器维度的监控。

表 2-47 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	单位	进制	测量对象（维度）	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。	≥ 0	Count	不涉及	共享型负载均衡器	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活跃TCP和UDP连接的个数。 Windows和Linux服务器都可以使用如下命令查看。 `netstat -an`	≥ 0	Count	不涉及	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	单位	进制	测量对象（维度）	监控周期（原始指标）
m3_inact_conn	非活跃连接数	从测量对象到后端服务器建立的非活跃TCP和UDP连接的个数。 Windows和Linux服务器都可以使用如下命令查看。 `netstat -an`	≥ 0	Count	不涉及	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。	≥ 0	Count/s	不涉及	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数据包的个数。	≥ 0	Count/s	不涉及	共享型负载均衡器	1分钟
m6_out_pps	流出数据包数	测量对象每秒发出数据包的个数。	≥ 0	Count/s	不涉及	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的网络速率。	≥ 0	Byte/s	1000(SI)	共享型负载均衡器	1分钟
m8_out_Bps	网络流出速率	测量对象访问外部的网络速率。	≥ 0	Byte/s	1000(SI)	共享型负载均衡器	1分钟
m9_abnormal_servers	异常主机数	测量对象中健康检查异常的后端服务器个数。	≥ 0	Count	不涉及	共享型负载均衡器	1分钟
ma_normal_servers	正常主机数	测量对象中健康检查正常的后端服务器个数。	≥ 0	Count	不涉及	共享型负载均衡器	1分钟
m22_in_bandwidth	入网带宽	测量对象入网带宽。	≥ 0	bit/s	1000(SI)	共享型负载均衡器	1分钟
m23_out_bandwidth	出网带宽	测量对象出网带宽。	≥ 0	bit/s	1000(SI)	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	单位	进制	测量对象（维度）	监控周期（原始指标）
m1e_server_rps	后端服务器每秒重置报文个数	测量后端服务器每秒发送至客户端的重置（RST）报文个数。重置数据包由后端服务器生成，然后由负载均衡器转发。 支持协议：TCP	≥ 0	Count/s	不涉及	共享型负载均衡器	1分钟
m21_client_rps	客户端每秒重置报文个数	测量客户端每秒发送至后端服务器的重置（RST）报文个数。重置数据包由客户端生成，然后由负载均衡器转发。 支持协议：TCP	≥ 0	Count/s	不涉及	共享型负载均衡器	1分钟
m1f_lvs_rps	负载均衡器每秒重置报文个数	测量负载均衡器每秒生成的重置（RST）报文个数。 支持协议：TCP	≥ 0	Count/s	不涉及	共享型负载均衡器	1分钟
mb_l7_qps	7层查询速率	测量对象7层查询速率。 支持协议：HTTP/HTTPS	≥ 0	Count/s	不涉及	共享型负载均衡器	1分钟
mc_l7_http_2xx	7层协议响应状态码(2XX)	测量对象每秒返回7层2XX系列响应状态码的个数。 支持协议：HTTP/HTTPS	≥ 0	Count/s	不涉及	共享型负载均衡器	1分钟
md_l7_http_3xx	7层协议响应状态码(3XX)	测量对象每秒返回7层3XX系列响应状态码的个数。 支持协议：HTTP/HTTPS	≥ 0	Count/s	不涉及	共享型负载均衡器	1分钟
me_l7_http_4xx	7层协议响应状态码(4XX)	测量对象每秒返回7层4XX系列响应状态码的个数。 支持协议：HTTP/HTTPS	≥ 0	Count/s	不涉及	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	单位	进制	测量对象（维度）	监控周期（原始指标）
mf_l7_http_5xx	7层协议响应状态码(5XX)	测量对象每秒返回7层5XX系列响应状态码的个数。 支持协议：HTTP/HTTPS	≥ 0	Count/s	不涉及	共享型负载均衡器	1分钟
m10_l7_http_other_status	7层协议响应状态码(Others)	测量对象每秒返回7层其他响应状态码的个数。 不包含：2XX、3XX、404、499、502。 支持协议：HTTP/HTTPS	≥ 0	Count/s	不涉及	共享型负载均衡器	1分钟
m11_l7_http_404	7层协议响应状态码404	测量对象每秒返回7层404响应状态码的个数。 支持协议：HTTP/HTTPS	≥ 0	Count/s	不涉及	共享型负载均衡器	1分钟
m12_l7_http_499	7层协议响应状态码499	测量对象每秒返回7层499响应状态码的个数。 支持协议：HTTP/HTTPS	≥ 0	Count/s	不涉及	共享型负载均衡器	1分钟
m13_l7_http_502	7层协议响应状态码502	测量对象每秒返回7层502响应状态码的个数。 支持协议：HTTP/HTTPS	≥ 0	Count/s	不涉及	共享型负载均衡器	1分钟
m14_l7_rt	7层协议RT平均值	测量对象7层平均响应时间。 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。 支持协议：HTTP/HTTPS **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。	≥ 0	ms	1000(SI)	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	单位	进制	测量对象（维度）	监控周期（原始指标）
m15_l7_upstream_4xx	7层后端响应状态码(4XX)	测量对象的后端服务器每秒返回7层4XX系列响应状态码的个数。 支持协议：HTTP/HTTPS	≥ 0	Count/s	不涉及	共享型负载均衡器	1分钟
m16_l7_upstream_5xx	7层后端响应状态码(5XX)	测量对象的后端服务器每秒返回7层5XX系列响应状态码的个数。 支持协议：HTTP/HTTPS	≥ 0	Count/s	不涉及	共享型负载均衡器	1分钟
m18_l7_upstream_2xx	7层后端响应状态码(2XX)	测量对象的后端服务器每秒返回7层2XX系列响应状态码的个数。 支持协议：HTTP/HTTPS	≥ 0	Count/s	不涉及	共享型负载均衡器	1分钟
m19_l7_upstream_3xx	7层后端响应状态码(3XX)	测量对象的后端服务器每秒返回7层3XX系列响应状态码的个数。 支持协议：HTTP/HTTPS	≥ 0	Count/s	不涉及	共享型负载均衡器	1分钟
m17_l7_upstream_rt	7层后端RT平均值	测量对象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。 支持协议：HTTP/HTTPS **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。	≥ 0	ms	1000(SI)	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	单位	进制	测量对象（维度）	监控周期（原始指标）
m1a_l7_upstream_rt_max	7层后端RT最大值	测量对象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。 支持协议：HTTP/HTTPS	≥ 0	ms	1000(SI)	共享型负载均衡器	1分钟
m1b_l7_upstream_rt_min	7层后端RT最小值	测量对象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。 支持协议：HTTP/HTTPS	≥ 0	ms	1000(SI)	共享型负载均衡器	1分钟
m1c_l7_rt_max	7层协议RT最大值	测量对象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。 支持协议：HTTP/HTTPS	≥ 0	ms	1000(SI)	共享型负载均衡器	1分钟
m1d_l7_rt_min	7层协议RT最小值	测量对象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。 支持协议：HTTP/HTTPS	≥ 0	ms	1000(SI)	共享型负载均衡器	1分钟
m25_l7_resp_Bps	7层响应带宽	测量对象后端服务器的七层响应发送带宽。 **说明** 当监听器开启HTTP/2时，该指标无法作为参考。	≥ 0	bit/s	1000(SI)	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	单位	进制	测量对象（维度）	监控周期（原始指标）
m24_l7_req_Bps	7层请求带宽	测量对象后端服务器的七层请求接收带宽。 **说明** 当监听器开启HTTP/2时，该指标无法作为参考。	≥ 0	bit/s	1000(SI)	共享型负载均衡器	1分钟

监听器的监控指标

表 2-48 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	单位	进制	测量对象（维度）	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	Count	不涉及	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活跃TCP和UDP连接的个数。 Windows和Linux服务器都可以使用如下命令查看。 `netstat -an` 单位：个	≥ 0	Count	不涉及	监听器（共享型）	1分钟

指标ID	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
m3_inact_conn	非活跃连接数	从测量对象到后端服务器建立的非活跃TCP和UDP连接的个数。 Windows和Linux服务器都可以使用如下命令查看。 `netstat -an` 单位：个	≥ 0	Count	不涉及	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。	≥ 0	Count/s	不涉及	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数据包的个数。	≥ 0	Count/s	不涉及	监听器（共享型）	1分钟
m6_out_pps	流出数据包数	测量对象每秒发出数据包的个数。	≥ 0	Count/s	不涉及	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的网络速率。	≥ 0	Byte/s	1000(SI)	监听器（共享型）	1分钟
m8_out_Bps	网络流出速率	测量对象访问外部的网络速率。	≥ 0	Byte/s	1000(SI)	监听器（共享型）	1分钟
m22_in_bandwidth	入网带宽	测量对象入网带宽。	≥ 0	bit/s	1000(SI)	监听器（共享型）	1分钟

指标ID	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
m23_out_bandwidth	出网带宽	测量对象出网带宽。	≥ 0	bit/s	1000(SI)	监听器（共享型）	1分钟
m1e_server_rps	后端服务器每秒重置报文个数	测量后端服务器每秒发送至客户端的重置（RST）报文个数。重置报文由后端服务器生成，然后由负载均衡器转发。 支持协议：TCP	≥ 0	Count/s	不涉及	监听器（共享型）	1分钟
m21_client_rps	客户端每秒重置报文个数	测量客户端每秒发送至后端服务器的重置（RST）报文个数。重置报文由客户端生成，然后由负载均衡器转发。 支持协议：TCP	≥ 0	Count/s	不涉及	监听器（共享型）	1分钟
m1f_lvs_rps	负载均衡器每秒重置报文个数	测量负载均衡器每秒生成的重置（RST）报文个数。 支持协议：TCP	≥ 0	Count/s	不涉及	监听器（共享型）	1分钟
mb_l7_qps	7层查询速率	测量对象7层查询速率。 支持协议：HTTP/HTTPS	≥ 0	Count/s	不涉及	监听器（共享型）	1分钟
mc_l7_http_2xx	7层协议响应状态码(2XX)	测量对象每秒返回7层2XX系列响应状态码的个数。 支持协议：HTTP/HTTPS	≥ 0	Count/s	不涉及	监听器（共享型）	1分钟
md_l7_http_3xx	7层协议响应状态码(3XX)	测量对象每秒返回7层3XX系列响应状态码的个数。 支持协议：HTTP/HTTPS	≥ 0	Count/s	不涉及	监听器（共享型）	1分钟

指标ID	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
me_l7_http_4xx	7层协议响应状态码(4XX)	测量对象每秒返回7层4XX系列响应状态码的个数。 支持协议：HTTP/HTTPS	≥ 0	Count/s	不涉及	监听器（共享型）	1分钟
mf_l7_http_5xx	7层协议响应状态码(5XX)	测量对象每秒返回7层5XX系列响应状态码的个数。 支持协议：HTTP/HTTPS	≥ 0	Count/s	不涉及	监听器（共享型）	1分钟
m10_l7_http_other_status	7层协议响应状态码(Others)	测量对象每秒返回7层其他响应状态码的个数。 不包含：2XX、3XX、404、499、502。 支持协议：HTTP/HTTPS	≥ 0	Count/s	不涉及	监听器（共享型）	1分钟
m11_l7_http_404	7层协议响应状态码404	测量对象每秒返回7层404响应状态码的个数。 支持协议：HTTP/HTTPS	≥ 0	Count/s	不涉及	监听器（共享型）	1分钟
m12_l7_http_499	7层协议响应状态码499	测量对象每秒返回7层499响应状态码的个数。 支持协议：HTTP/HTTPS	≥ 0	Count/s	不涉及	监听器（共享型）	1分钟
m13_l7_http_502	7层协议响应状态码502	测量对象每秒返回7层502响应状态码的个数。 支持协议：HTTP/HTTPS	≥ 0	Count/s	不涉及	监听器（共享型）	1分钟

指标ID	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
m14_l7_rt	7层协议RT平均值	测量对象7层平均响应时间。 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。 支持协议：HTTP/HTTPS **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。	≥ 0	ms	1000(SI)	监听器（共享型）	1分钟
m15_l7_upstream_4xx	7层后端响应状态码(4XX)	测量对象的后端服务器每秒返回7层4XX系列响应状态码的个数。 支持协议：HTTP/HTTPS	≥ 0	Count/s	不涉及	监听器（共享型）	1分钟
m16_l7_upstream_5xx	7层后端响应状态码(5XX)	测量对象的后端服务器每秒返回7层5XX系列响应状态码的个数。 支持协议：HTTP/HTTPS	≥ 0	Count/s	不涉及	监听器（共享型）	1分钟
m18_l7_upstream_2xx	7层后端响应状态码(2XX)	测量对象的后端服务器每秒返回7层2XX系列响应状态码的个数。 支持协议：HTTP/HTTPS	≥ 0	Count/s	不涉及	监听器（共享型）	1分钟
m19_l7_upstream_3xx	7层后端响应状态码(3XX)	测量对象的后端服务器每秒返回7层3XX系列响应状态码的个数。 支持协议：HTTP/HTTPS	≥ 0	Count/s	不涉及	监听器（共享型）	1分钟

指标ID	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
m17_l7_upstream_rt	7层后端RT平均值	测量对象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。 支持协议：HTTP/HTTPS **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。	≥ 0	ms	1000(SI)	监听器（共享型）	1分钟
m1a_l7_upstream_rt_max	7层后端RT最大值	测量对象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。 支持协议：HTTP/HTTPS	≥ 0	ms	1000(SI)	监听器（共享型）	1分钟
m1b_l7_upstream_rt_min	7层后端RT最小值	测量对象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。 支持协议：HTTP/HTTPS	≥ 0	ms	1000(SI)	监听器（共享型）	1分钟
m1c_l7_rt_max	7层协议RT最大值	测量对象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。 支持协议：HTTP/HTTPS	≥ 0	ms	1000(SI)	监听器（共享型）	1分钟

指标ID	指标名称	指标含义	取值范围	单位	进制	测量对象（维度）	监控周期（原始指标）
m1d_l7_rt_min	7层协议的RT最小值	测量对象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。 支持协议：HTTP/HTTPS	≥ 0	ms	1000(SI)	监听器（共享型）	1分钟
m25_l7_resp_Bps	7层响应带宽	测量对象后端服务器的七层响应发送带宽。 **说明** 当监听器开启HTTP/2时，该指标无法作为参考。	≥ 0	bit/s	1000(SI)	监听器（共享型）	1分钟
m24_l7_req_Bps	7层请求带宽	测量对象后端服务器的七层请求接收带宽。 **说明** 当监听器开启HTTP/2时，该指标无法作为参考。	≥ 0	bit/s	1000(SI)	监听器（共享型）	1分钟

维度

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

2.11.3 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. 进入**EIP列表页面**。
2. 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 2-49 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

指标名称	含义	取值范围	测试对象	监控周期（原始指标）
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. 进入**弹性负载均衡列表页面**。
2. 在弹性负载均衡列表页，单击需要查看流量的负载均衡器名称。
3. 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。

2.12 使用 CTS 审计 ELB 关键操作

2.12.1 ELB 支持审计的关键操作

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2-50**所示。

表 2-50 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

操作名称	资源类型	事件名称
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

2.12.2 查看 ELB 的审计日志

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或导出最近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

```
"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"}

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，已发布区域请以控制台实际为准。

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，已发布区域请以控制台实际为准。

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IP类型后端发起健康检查异常诊断。

操作步骤

1. 进入**弹性负载均衡列表页面**。
2. 在左侧导航栏，选择“ 自助问题诊断”。
3. 在弹性负载均衡自助诊断界面，单击“ELB健康检查异常”页签。
4. 选择异常后端服务器关联的负载均衡实例。
5. 选择需要诊断的异常后端服务器。
6. 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。

高频问题

- 为什么后端服务器健康检查结果显示为“未知”？

  当后端服务器组开启健康检查但未关联至监听器时，健康检查结果显示为“未知”。

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	• **计费项（独享型）**。 • **计费项（共享型）**。

计费常见场景	参考文档
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转发过的访问者真实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。

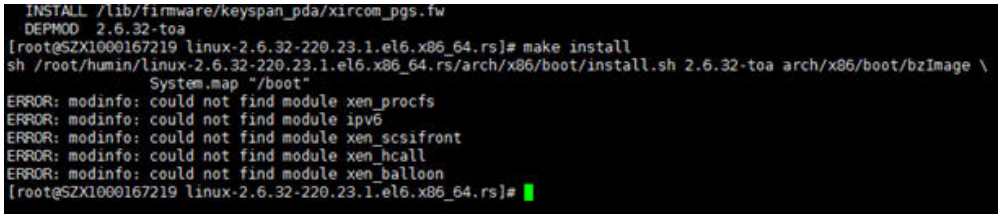
图 4-1 安装内核模块

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

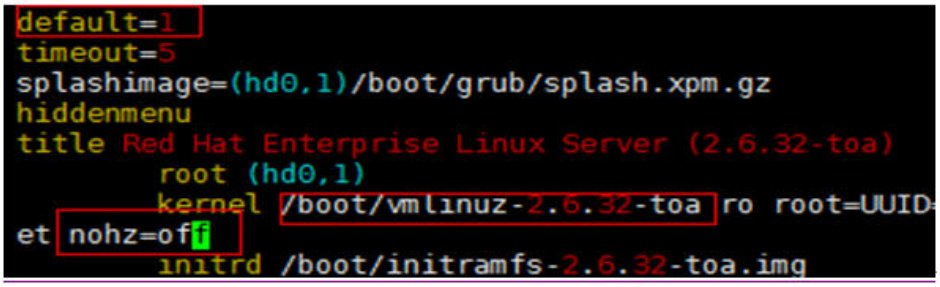


7. 打开“/boot/grub/grub.conf”文件，配置开机默认启动，如图4-3所示。

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。

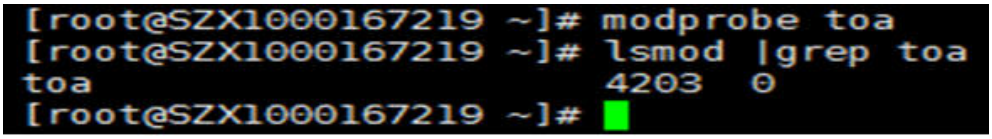
重启系统时，系统将加载vmlinuz-2.6.32-toa内核。

8. 待系统重启完成之后，执行以下命令加载TOA模块。

modprobe toa

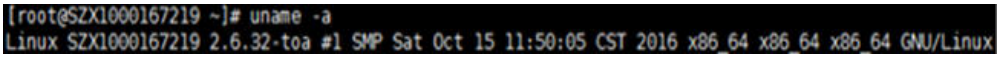
建议将modprobe toa命令加入开机启动脚本，以及系统定时监控脚本中，如图4-4所示。

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。