ALIBABA CLOUD

阿里云

负载均衡

监听

文档版本：20220414

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.监听概述

创建负载均衡实例后，您需要为实例配置监听。负载均衡实例监听负责检查连接请求，然后根据调度算法定义的转发策略将请求流量分发至后端服务器。

负载均衡提供四层（TCP或UDP协议）和七层（HTTP或HTTPS协议）监听，您可根据应用场景选择监听协议：

协议	说明	使用场景
TCP	• 面向连接的协议，在正式收发数据前，必须和对方建立可靠的连接。 • 基于源地址的会话保持。 • 在网络层可直接看到来源地址。 • 数据传输快。	• 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。 • 无特殊要求的Web应用。 更多信息，请参见添加TCP监听。
UDP	• 面向非连接的协议，在数据发送前不与对方进行三次握手，直接进行数据包发送，不提供差错恢复和数据重传。 • 可靠性相对低；数据传输快。	关注实时性而相对不注重可靠性的场景，如视频聊天、金融实时行情推送。 更多信息，请参见添加UDP监听。
HTTP	• 应用层协议，主要解决如何包装数据。 • 基于Cookie的会话保持。 • 使用X-Forward-For获取客户真实IP地址。	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。 更多信息，请参见添加HTTP监听。
HTTPS	• 加密传输数据，可以阻止未经授权的访问。 • 统一的证书管理服务，您可以将证书上传到负载均衡，解密操作直接在负载均衡上完成。	需要加密传输的应用。 更多信息，请参见添加HTTPS监听。

2.添加TCP监听

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

前提条件

您已经创建

CLB

实例，具体操作，请参见创建实例。

步骤一：配置监听

1. 登录传统型负载均衡CLB控制台。
2. 在顶部菜单栏，选择

   CLB

   实例的所属地域。
3. 选择以下一种方法，打开监听配置向导。
   - 在**实例管理**页面，找到目标实例，然后在**操作**列单击**监听配置向导**。
   - 在**实例管理**页面，找到目标实例，单击实例ID。在**监听**页签，单击**添加监听**。
4. 完成以下配置，然后单击**下一步**。

监听配置	说明
选择负载均衡协议	选择TCP。
监听端口	输入接收请求并向后端服务器进行请求转发的监听端口。 端口范围为1~65535。 TCP和UDP协议监听支持开启全端口功能，监听端口段。
监听名称	自定义监听的名称。
高级配置	单击**修改**展开高级配置。

调度算法	选择调度算法。
	- **加权轮询(WRR)**：权重值越高的后端服务器，被轮询到的概率越高。
	- **轮询(RR)**：按照访问顺序依次将外部请求分发到后端服务器。
	- **一致性哈希（CH）**：
	  - **四元组**：基于四元组（源IP、目的IP、源端口和目的端口）的一致性哈希，相同的流会调度到相同的后端服务器。
	  - **源IP**：基于源IP地址的一致性哈希，相同的源地址会调度到相同的后端服务器。
	说明 仅性能保障型实例支持一致性哈希（CH）调度算法。

监听配置	说明
开启会话保持	选择是否开启会话保持。 开启会话保持后，负载均衡监听会把来自同一客户端的访问请求分发到同一台后端服务器上。 TCP协议是基于IP地址的会话保持，即来自同一IP地址的访问请求转发到同一台后端服务器上。
启用访问控制	选择是否启用访问控制。 开启访问控制后，选择一种访问控制方式，并设置访问控制策略组，作为该监听的白名单或黑名单。 ○ **白名单：允许特定IP访问负载均衡SLB**，仅转发来自所选访问控制策略组中设置的IP地址或地址段的请求，白名单适用于只允许特定IP访问的场景。设置白名单存在一定业务风险。一旦设置白名单，就只有白名单中的IP可以访问负载均衡监听。 如果开启了白名单访问，但访问策略组中没有添加任何IP，则负载均衡监听会转发全部请求。 ○ **黑名单：禁止特定IP访问负载均衡SLB**，不会转发来自所选访问控制策略组中设置的IP地址或地址段，黑名单适用于只限制某些特定IP访问的场景。 如果开启了黑名单访问，但访问策略组中没有添加任何IP，则负载均衡监听会转发全部请求。 **说明** IPv4实例只能绑定IPv4访问控制策略组，IPv6实例只能绑定IPv6访问控制策略组。具体操作，请参见创建访问控制策略组。
开启监听带宽限速	选择是否配置监听带宽。 对于按带宽计费的负载均衡实例，您可以针对不同监听设定不同的带宽峰值来限定监听的流量。实例下所有监听的带宽峰值总和不能超过该实例的带宽。默认不开启，各监听共享实例的总带宽。 **说明** 使用流量计费方式的实例默认不限制带宽峰值。
连接超时时间	指定TCP连接的超时时间，范围10~900秒。
ProxyProtocol配置	通过Proxy Protocol协议携带客户端源地址到后端服务器。 **说明** 私网连接（PrivateLink）场景目前暂不支持通过ProxyProtocol获取源地址。
获取客户端真实IP	针对四层监听，后端服务器可直接获得来访者的真实IP地址，默认开启。
创建完毕自动启动监听	是否在监听配置完成后启动负载均衡监听，默认开启。

步骤二：添加后端服务器

添加处理前端请求的后端服务器。您可以使用实例配置的默认服务器组，也可以为监听配置一个虚拟服务器组、主备服务器组或者启动主备服务器组模式。更多信息，请参见后端服务器概述。

1. 在**后端服务器**配置向导页面，选择将监听请求转发至后端服务器的类型，本文以默认后端服务器组为例。

   选择**默认服务器组**，然后单击**继续添加**。

2. 在**选择服务器**配置向导，选择要添加的ECS实例，然后单击**下一步**。
3. 在**配置端口和权重**配置向导，配置添加的后端服务器的权重，权重越高的ECS实例将被分配到更多的访问请求。

   > **说明** 权重设置为0的服务器不会接受新请求。

4. 单击**添加**，配置后端服务器（ECS实例）开放用来接收请求的端口，端口范围为1~65535。

   同一个负载均衡实例内，后端服务器端口可以相同。

5. 单击**下一步**。

步骤三：配置健康检查

负载均衡通过健康检查来判断后端服务器（ECS实例）的业务可用性。健康检查机制提高了前端业务整体可用性，避免了后端ECS异常对总体服务的影响。

在**健康检查**配置向导，单击**修改**更改健康检查配置。具体操作，请参见配置健康检查。

步骤四：提交配置

1. 在**配置审核**配置向导，检查监听配置，您可以单击**修改**更改配置。
2. 确认无误后，单击**提交**。
3. 等待配置成功后，单击**知道了**。

   配置成功后，您可以在监听页面查看已创建的监听。

相关文档

- CreateLoadBalancerTCPListener：创建TCP监听。

3.添加UDP监听

UDP协议多用于关注实时性而相对不注重可靠性的场景，如视频聊天和金融实时行情推送等。您可以添加一个UDP监听转发来自UDP协议的请求。

背景信息

在添加UDP监听前，注意以下限制：

- UDP监听的250、4789和4790三个端口为系统保留端口，暂时不对外开放。
- 暂不支持分片包。
- 经典网络负载均衡实例的UDP监听暂不支持查看源地址。
- 在以下两种情况下，UDP协议监听配置需要五分钟才能生效：
  - 移除后端服务器。
  - 健康检查检测到异常后，将后端服务器的权重设置为0。
- 由于IPv6的IP头部较IPv4更长，当您在

  CLB

  IPv6实例上使用UDP监听时，需要确保后端服务器（通常是ECS云服务器）与

  CLB

  通信的网卡的MTU不大于1200（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。

  如果使用TCP/HTTP/HTTPS监听，TCP协议支持MSS自动协商，因此不需要额外配置。

前提条件

您已经创建

CLB

实例，具体操作，请参见创建实例。

步骤一：配置监听

1. 登录传统型负载均衡CLB控制台。
2. 在顶部菜单栏，选择

   CLB

   实例的所属地域。
3. 选择以下一种方法，打开监听配置向导。
   - 在**实例管理**页面，找到目标实例，然后在**操作**列单击**监听配置向导**。
   - 在**实例管理**页面，找到目标实例，单击实例ID。在**监听**页签，单击**添加监听**。
4. 完成以下配置，然后单击**下一步**。

监听配置	说明
选择负载均衡协议	选择**UDP**。

监听配置	说明
监听端口	用来接收请求并向后端服务器进行请求转发的监听端口。 端口范围为1~65535。
监听名称	自定义监听的名称。
高级配置	单击**修改**展开高级配置。
调度算法	选择调度算法。 ○ **加权轮询(WRR)**：权重值越高的后端服务器，被轮询到的概率越高。 ○ **轮询(RR)**：按照访问顺序依次将外部请求分发到后端服务器。 ○ **一致性哈希（CH）**： ■ **QUIC ID**：基于QUIC Connection ID一致性hash，相同的QUIC Connection ID会调度到相同的后端服务器。 注意 QUIC协议正在快速演进，该算法基于draft-ietf-quic-transport-10实现，无法保证所有QUIC版本的兼容性，建议充分测试后再用于生产环境。 ■ **四元组**：基于四元组（源IP、目的IP、源端口和目的端口）的一致性哈希，相同的流会调度到相同的后端服务器。 ■ **源IP**：基于源IP地址的一致性哈希，相同的源地址会调度到相同的后端服务器。
开启会话保持	选择是否开启会话保持。 开启会话保持后，负载均衡监听会把来自同一客户端的访问请求分发到同一台后端服务器上。
启用访问控制	选择是否启用访问控制。 开启访问控制后，选择一种访问控制方式，并设置访问控制策略组，作为该监听的白名单或黑名单。 ○ **白名单：允许特定IP访问负载均衡SLB**，仅转发来自所选访问控制策略组中设置的IP地址或地址段的请求，白名单适用于只允许特定IP访问的场景。设置白名单存在一定业务风险。一旦设置白名单，就只有白名单中的IP可以访问负载均衡监听。 如果开启了白名单访问，但访问策略组中没有添加任何IP，则负载均衡监听会转发全部请求。 ○ **黑名单：禁止特定IP访问负载均衡SLB**，不会转发来自所选访问控制策略组中设置的IP地址或地址段，黑名单适用于只限制某些特定IP访问的场景。 如果开启了黑名单访问，但访问策略组中没有添加任何IP，则负载均衡监听会转发全部请求。 **说明** IPv4实例只能绑定IPv4访问控制策略组，IPv6实例只能绑定IPv6访问控制策略组。具体操作，请参见创建访问控制策略组。

监听配置	说明
开启监听带宽限速	选择是否配置监听带宽。 对于按带宽计费的负载均衡实例，您可以针对不同监听设定不同的带宽峰值来限定监听的流量。实例下所有监听的带宽峰值总和不能超过该实例的带宽。默认不开启，各监听共享实例的总带宽。 **说明** 使用流量计费方式的实例默认不限制带宽峰值。
ProxyProtocol配置	通过Proxy Protocol协议携带客户端源地址到后端服务器。 **说明** 私网连接（PrivateLink）场景目前暂不支持通过ProxyProtocol获取源地址。
获取客户端真实IP	针对四层监听，后端服务器保留来访者的真实源IP地址，默认开启。 **说明** 经典网络实例的UDP协议可通过开启**ProxyProtocol**配置获取源地址。
创建完毕自动启动监听	是否在监听配置完成后启动负载均衡监听，默认开启。

步骤二：添加后端服务器

添加处理前端请求的后端服务器。您可以使用实例配置的默认服务器组，也可以为监听配置一个虚拟服务器组、主备服务器组或者启动主备服务器组模式。更多信息，请参见后端服务器概述。

1. 在**后端服务器**配置向导页面，选择将监听请求转发至后端服务器的类型，本文以默认后端服务器组为例。

   选择**默认服务器组**，然后单击**继续添加**。

2. 在**选择服务器**配置向导，选择要添加的ECS实例，然后单击**下一步**。
3. 在**配置端口和权重**配置向导，配置添加的后端服务器的权重，权重越高的ECS实例将被分配到更多的访问请求。

   说明 权重设置为0的服务器不会接受新请求。

4. 单击**添加**，配置后端服务器（ECS实例）开放用来接收请求的端口，端口范围为1~65535。

   同一个负载均衡实例内，后端服务器端口可以相同。

5. 单击**下一步**。

步骤三：配置健康检查

负载均衡通过健康检查来判断后端服务器（ECS实例）的业务可用性。健康检查机制提高了前端业务整体可用性，避免了后端ECS异常对总体服务的影响。

在**健康检查**配置向导，单击**修改**更改健康检查配置。具体操作，请参见配置健康检查。

步骤四：提交配置

1. 在**配置审核**配置向导，检查监听配置，您可以单击**修改**更改配置。
2. 确认无误后，单击**提交**。
3. 等待配置成功后，单击**知道了**。

   配置成功后，您可以在监听页面查看已创建的监听。

相关文档

相关文档

- 配置健康检查
- 添加默认服务器
- 创建虚拟服务器组
- 创建和管理主备服务器组
- 访问控制概述
- CreateLoadBalancerUDPListener

4.添加HTTP监听

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

前提条件

您已经创建

传统型负载均衡CLB

实例。具体操作，请参见创建实例。

步骤一：配置监听

1. 登录传统型负载均衡CLB控制台。
2. 选择实例的地域。
3. 选择以下一种方法，打开监听配置向导。
   - 在**实例管理**页面，找到目标实例，然后在**操作**列单击**监听配置向导**。
   - 在**实例管理**页面，单击目标实例ID，然后在**监听**页签单击**添加监听**。
4. 配置协议监听，然后单击**下一步**。

监听配置	说明
选择负载均衡协议	选择监听的协议类型。 本文选择**HTTP**。
后端协议	当本文选择的是**HTTP**协议时，**后端协议**为**HTTP**。
监听端口	用来接收请求并向后端服务器进行请求转发的监听端口。端口范围为1~65535。HTTP协议使用80端口。
监听名称	设置自定义监听名称。长度限制为1~256个字符，允许包含中文、字母、数字、短划线（-）、正斜线（/）、半角句号（.）和下划线（_）。
高级配置	单击**修改**展开高级配置。
调度算法	选择调度算法。 ○ **加权轮询(WRR)**：权重值越高的后端服务器，被轮询到的次数（概率）也越高。 ○ **轮询(RR)**：按照访问顺序依次将外部请求分发到后端服务器。
监听转发	选择是否将HTTP监听的流量转发到HTTPS监听。 **说明** 如果开启监听转发，确保您已经创建了HTTPS监听。

监听配置	说明
开启会话保持	选择是否开启会话保持。 开启会话保持功能后，负载均衡会把来自同一客户端的访问请求分发到同一台后端服务器上进行处理。 HTTP协议会话保持基于Cookie。负载均衡提供了两种Cookie处理方式： ○ **植入Cookie**：您只需要指定Cookie的过期时间。 客户端第一次访问时，负载均衡会在返回请求中植入Cookie（即在HTTP或HTTPS响应报文中插入ServerId），下次客户端携带此Cookie访问，负载均衡服务会将请求定向转发给之前记录到的后端服务器上。 ○ **重写Cookie**：可以根据需要指定HTTPS或HTTP响应中插入的Cookie。您需要在后端服务器上维护该Cookie的过期时间和生存时间。 负载均衡服务发现用户自定义了Cookie，将会对原来的Cookie进行重写，下次客户端携带新的Cookie访问，负载均衡服务会将请求定向转发给之前记录到的后端服务器。
启用访问控制	选择是否启用访问控制。 开启访问控制后，选择一种访问控制方式，并设置访问控制策略组，作为该监听的白名单或黑名单。 ○ **白名单：允许特定IP访问负载均衡SLB**，仅转发来自所选访问控制策略组中设置的IP地址或地址段的请求，白名单适用于只允许特定IP访问的场景。设置白名单存在一定业务风险。一旦设置白名单，就只有白名单中的IP可以访问负载均衡监听。 如果开启了白名单访问，但访问策略组中没有添加任何IP，则负载均衡监听会转发全部请求。 ○ **黑名单：禁止特定IP访问负载均衡SLB**，不会转发来自所选访问控制策略组中设置的IP地址或地址段，黑名单适用于只限制某些特定IP访问的场景。 如果开启了黑名单访问，但访问策略组中没有添加任何IP，则负载均衡监听会转发全部请求。 **说明** IPv6实例只能绑定IPv6访问控制策略组，IPv4实例只能绑定IPv4访问控制策略组。详情参见创建访问控制策略组。
开启监听带宽限速	选择是否配置监听带宽，取值范围为0~5120 Mbps。 对于按带宽计费的负载均衡实例，您可以针对不同监听设定不同的带宽峰值来限定监听的流量。实例下所有监听的带宽峰值总和不能超过该实例的带宽。默认不开启，各监听共享实例的总带宽。 **说明** 使用流量计费方式的实例默认不限制带宽峰值。

监听配置	说明
连接空闲超时时间	指定连接空闲超时时间，取值范围为1~60秒。 在超时时间内一直没有访问请求，负载均衡会暂时中断当前连接，直到下一次请求来临时重新建立新的连接。
连接请求超时时间	指定请求超时时间，取值范围为1~180秒。 在超时时间内后端服务器一直没有响应，负载均衡将放弃等待，给客户端返回HTTP 504错误码。
Gzip数据压缩	开启该配置对特定文件类型进行压缩，关闭该配置则不会对任何文件类型进行压缩。 目前Gzip支持压缩的类型包括：`text/xml`、`text/plain`、`text/css`、`application/javascript`、`application/x-javascript`、`application/rss+xml`、`application/atom+xml`和`application/xml`。
附加HTTP头字段	选择您要添加的自定义HTTP头字段： ○ 添加`X-Forwarded-For`头字段获取客户端真实IP。 ○ 添加`SLB-ID`头字段获取负载均衡实例的ID。 ○ 添加`SLB-IP`头字段获取负载均衡实例IP地址。 ○ 添加`X-Forwarded-Proto`头字段获取负载均衡的监听协议。 ○ 添加`X-Forwarded-Port`头字段获取负载均衡实例的监听端口。 ○ 添加`X-Forwarded-Client-srcport`头字段获取访问负载均衡实例客户端的端口。
获取客户端真实IP	获取来访者的真实IP地址，默认开启。
创建完毕自动启动监听	是否在监听配置完成后启动负载均衡监听，默认开启。
WAF安全防护	选择是否为监听开启WAF安全防护。

步骤二：添加后端服务器

添加处理前端请求的后端服务器。您可以使用实例配置的默认服务器组，也可以为监听配置一个虚拟服务器组或主备服务器组。更多信息，请参见后端服务器概述。

本操作中，以默认后端服务器组为例。

1. 在**后端服务器**配置页面，选择**默认服务器组**，然后单击**继续添加**。
2. 在**我的服务器**面板，选择要添加的后端服务器，然后单击**下一步**。
3. 在**权重**列下，配置添加的后端服务器的权重。

> 说明
>
> - 权重越大ECS实例将被分配到更多的访问请求，默认为100。可通过单击**重置**修改**权重**为默认值。
> - 权重设置为0，该服务器不会再接受新请求。

4. 单击**添加**，配置后端服务器用来接收请求的端口，端口范围为1~65535。然后单击**下一步**。

   同一个负载均衡实例内，后端服务器端口可以相同。

步骤三：配置健康检查

负载均衡通过健康检查来判断后端服务器（ECS实例）的业务可用性。健康检查机制提高了前端业务整体可用性，避免了后端ECS异常对总体服务的影响。

在**健康检查**配置向导，单击**修改**更改健康检查配置。具体操作，请参见配置健康检查。

步骤四：提交配置

1. 在**配置审核**配置向导，检查监听配置，您可以单击**修改**更改配置。
2. 确认无误后，单击**提交**。
3. 等待配置成功后，单击**知道了**。

   配置成功后，您可以在监听页面查看已创建的监听。

相关文档

相关文档

- 添加默认服务器
- 配置健康检查
- 创建虚拟服务器组
- 创建和管理主备服务器组
- 访问控制概述
- 基于域名或URL路径进行转发
- 概述
- CreateLoadBalancerHTTPSListener：调用CreateLoadBalancerHTTPSListener创建HTTPS监听。

5.添加HTTPS监听

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。

前提条件

您已经创建

CLB

实例，具体操作，请参见创建实例。

步骤一：配置监听

1. 登录传统型负载均衡CLB控制台。
2. 在顶部菜单栏处，选择实例所属地域。
3. 选择以下一种方法，打开监听配置向导。
   - 在**实例管理**页面，找到目标实例，然后在**操作**列单击**监听配置向导**。
   - 在**实例管理**页面，单击目标实例ID，然后在**监听**页签单击**添加监听**。
4. 完成以下配置，然后单击**下一步**。

监听配置	说明
选择负载均衡协议	选择监听的协议类型。 本文选择**HTTPS**。
后端协议	当本文选择的是**HTTPS**协议时，**后端协议**为**HTTP**协议。
监听端口	用来接收请求并向后端服务器进行请求转发的监听端口。端口范围为1~65535。 HTTPS协议使用443端口。
监听名称	设置自定义监听名称。长度限制为1~256个字符，允许包含中文、字母、数字、短划线（-）、正斜线（/）、半角句号（.）和下划线（_）。
高级配置	单击**修改**展开高级配置。
调度算法	选择调度算法。 ○ **加权轮询(WRR)**：权重值越高的后端服务器，被轮询到的次数（概率）也越高。 ○ **轮询(RR)**：按照访问顺序依次将外部请求分发到后端服务器。

监听配置	说明
开启会话保持	选择是否开启会话保持。 开启会话保持功能后，负载均衡会把来自同一客户端的访问请求分发到同一台后端服务器上进行处理。 HTTPS协议会话保持基于Cookie。负载均衡提供了两种Cookie处理方式： ○ **植入Cookie**：您只需要指定Cookie的过期时间。 客户端第一次访问时，负载均衡会在返回请求中植入Cookie（即在HTTP或HTTPS响应报文中插入ServerId），下次客户端携带此Cookie访问，负载均衡服务会将请求定向转发给之前记录到的后端服务器上。 ○ **重写Cookie**：可以根据需要指定HTTPS或HTTP响应中插入的Cookie。您需要在后端服务器上维护该Cookie的过期时间和生存时间。 负载均衡服务发现用户自定义了Cookie，将会对原来的Cookie进行重写，下次客户端携带新的Cookie访问，负载均衡服务会将请求定向转发给之前记录到的后端服务器。
启用HTTP2.0	选择是否开启CLB前端协议版本为HTTP 2.0。
启用访问控制	选择是否启用访问控制。 开启访问控制后，选择一种访问控制方式，并设置访问控制策略组，作为该监听的白名单或黑名单。 ○ **白名单：允许特定IP访问负载均衡SLB**，仅转发来自所选访问控制策略组中设置的IP地址或地址段的请求，白名单适用于只允许特定IP访问的场景。设置白名单存在一定业务风险。一旦设置白名单，就只有白名单中的IP可以访问负载均衡监听。 如果开启了白名单访问，但访问策略组中没有添加任何IP，则负载均衡监听会转发全部请求。 ○ **黑名单：禁止特定IP访问负载均衡SLB**，不会转发来自所选访问控制策略组中设置的IP地址或地址段，黑名单适用于只限制某些特定IP访问的场景。 如果开启了黑名单访问，但访问策略组中没有添加任何IP，则负载均衡监听会转发全部请求。 **说明** IPv6实例只能绑定IPv6访问控制策略组，IPv4实例只能绑定IPv4访问控制策略组。详情参见创建访问控制策略组。
开启监听带宽限速	选择是否配置监听带宽。 对于按带宽计费的负载均衡实例，您可以针对不同监听设定不同的带宽峰值来限定监听的流量。实例下所有监听的带宽峰值总和不能超过该实例的带宽。默认不开启，各监听共享实例的总带宽。 **说明** 使用流量计费方式的实例默认不限制带宽峰值。

监听配置	说明
连接空闲超时时间	指定连接空闲超时时间，取值范围为1~60秒。 在超时时间内一直没有访问请求，负载均衡会暂时中断当前连接，直到下一次请求来临时重新建立新的连接。
连接请求超时时间	指定请求超时时间，取值范围为1~180秒。 在超时时间内后端服务器一直没有响应，负载均衡将放弃等待，给客户端返回HTTP 504错误码。
Gzip数据压缩	开启该配置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。 目前Gzip支持压缩的类型包括：`text/xml` 、`text/plain` 、`text/css` 、`application/javascript` 、`application/x-javascript` 、`application/rss+xml` 、`application/atom+xml` 、`application/xml` 、和 `application/json` 。
附加HTTP头字段	选择您要添加的自定义HTTP头字段： ○ 添加 `X-Forwarded-For` 头字段获取客户端真实IP。 ○ 添加 `SLB-ID` 头字段获取负载均衡实例的ID。 ○ 添加 `SLB-IP` 头字段获取负载均衡实例IP地址。 ○ 添加 `X-Forwarded-Proto` 头字段获取负载均衡的监听协议。 ○ 添加 `X-Forwarded-Port` 头字段获取负载均衡实例的监听端口。 ○ 添加 `X-Forwarded-Client-srcport` 头字段获取访问负载均衡实例客户端的端口。
获取客户端真实IP	获取来访者的真实IP地址，默认开启。
创建完毕自动启动监听	是否在监听配置完成后启动负载均衡监听，默认开启。
WAF安全防护	选择是否为监听开启WAF安全防护。

步骤二：配置SSL证书

添加HTTPS监听，您需要上传服务器证书或CA证书并选择TLS安全策略，如下表所示。

证书	说明	单向认证是否需要	双向认证是否需要
服务器证书	用来证明服务器的身份。 用户浏览器用来检查服务器发送的证书是否是由自己信赖的中心签发的。	是 服务器证书需要上传到负载均衡的证书管理系统。	是 服务器证书需要上传到负载均衡的证书管理系统。

证书	说明	单向认证是否需要	双向认证是否需要
客户端证书	用来证明客户端的身份。 用于证明客户端用户的身份，使得客户端用户在与服务器端通信时可以证明其真实身份。您可以用自签名的CA证书为客户端证书签名。	否	是 需要客户端进行安装。
CA 证书	服务器用CA证书验证客户端证书的签名。如果没有通过验证，拒绝连接。	否	是 CA证书需要上传到负载均衡的证书管理系统。
TLS安全策略	仅性能保障型实例支持选择使用的TLS安全策略。 TLS安全策略包含HTTPS可选的TLS协议版本和配套的加密算法套件，具体说明请参见TLS安全策略说明。	是	是

在上传证书前，请注意：

- 目前阿里云负载均衡支持的公钥算法：RSA 1024、RSA 2048、RSA 4096、ECDSA P-256、ECDSA P-384和ECDSA P-521。
- 上传的证书格式必须是PEM。
- 证书上传到负载均衡后，负载均衡即可管理证书，不需要在后端ECS上绑定证书。
- 因为证书的上传、加载和验证都需要一些时间，所以使用HTTPS协议的实例生效也需要一些时间。一般一分钟后就会生效，最长不会超过三分钟。
- HTTPS监听使用的ECDHE算法簇支持前向保密技术，不支持将DHE算法簇所需要的安全增强参数文件上传，即PEM证书文件中含 `BEGIN DH PARAMETERS` 字段的字串上传。更多信息，请参见证书要求。
- HTTPS监听的会话ticket保持时间默认为300秒。
- HTTPS监听实际产生的流量会比账单流量更多一些，因为会使用一些流量用于协议握手。
- 在新建连接数很高的情况下，会占用较大的流量。

1. 在**SSL证书**配置页面，选择已上传的服务器证书，或单击**新建服务器证书**上传一个服务器证书。
2. 如果您要开启HTTPS双向认证或者设置TLS安全策略，单击**高级配置**后面的**修改**。
3. 打开双向认证，并选择一个已上传的CA证书，或新建一个CA证书。
4. 选择TLS安全策略，更多信息，参见TLS安全策略说明。

步骤三：添加后端服务器

添加处理前端请求的后端服务器。您可以使用实例配置的默认服务器组，也可以为监听配置一个虚拟服务器组或主备服务器组。更多信息，请参见后端服务器概述。

本文以默认后端服务器组为例。

1. 在**后端服务器**配置页面，选择**默认服务器组**，然后单击**继续添加**。
2. 在**我的服务器**面板，选择要添加的后端服务器，然后单击**下一步**。
3. 在**权重**列下，配置添加的后端服务器的权重。

> 说明
>
> - 权重越大ECS实例将被分配到更多的访问请求，默认为100。可通过单击**重置**修改**权重**为默认值。
> - 权重设置为0，该服务器不会再接受新请求。

4. 单击**添加**，配置后端服务器用来接收请求的端口，端口范围为1~65535。然后单击**下一步**。

   同一个负载均衡实例内，后端服务器端口可以相同。

步骤四：配置健康检查

负载均衡通过健康检查来判断后端服务器（ECS实例）的业务可用性。健康检查机制提高了前端业务整体可用性，避免了后端ECS异常对总体服务的影响。

步骤五：提交配置

1. 在**配置审核**配置向导，检查监听配置，您可以单击**修改**更改配置。
2. 确认无误后，单击**提交**。
3. 等待配置成功后，单击**知道了**。

   配置成功后，您可以在监听页面查看已创建的监听。

相关文档

相关文档

- 添加默认服务器
- 创建虚拟服务器组
- 创建和管理主备服务器组
- 访问控制概述
- 基于域名或URL路径进行转发
- 添加扩展域名
- CreateLoadBalancerHTTPSListener：调用CreateLoadBalancerHTTPSListener创建HTTPS监听。

6.扩展域名

6.1. 概述

性能保障型负载均衡HTTPS监听支持挂载多个证书，将来自不同访问域名的请求转发至不同的后端服务器组。

服务器名称指示（Server Name Indication，SNI）是对SSL / TLS协议的扩展，允许在单个IP地址上承载多个SSL证书。当客户端访问负载均衡时，默认使用访问域名配置的证书解密。如果找不到匹配的证书，则使用监听配置的证书。

> 注意
>
> - 仅性能保障型负载均衡支持SNI。
> - 目前阿里云负载均衡支持如下公钥算法：
>   - RSA 1024
>   - RSA 2048
>   - RSA 4096
>   - ECDSA P-256
>   - ECDSA P-384
>   - ECDSA P-521

当您有将多个域名绑定到同一个负载均衡服务地址上， 然后通过不同的域名区分不同的访问来源并且使用HTTPS加密访问的需求时，可以通过配置扩展域名实现。

扩展域名功能已在各地域发布。

6.2. 添加扩展域名

本文介绍添加扩展域名的操作步骤。

操作步骤

1. 登录传统型负载均衡CLB控制台。
2. 在**实例管理**页面，单击目标实例ID。
3. 在**监听**页签，找到已创建的HTTPS监听，在**操作**列选择 **> 扩展域名管理**。
4. 在**扩展域名管理**面板，单击**添加扩展域名**。

i. 输入域名。域名只能由字母、数字、短划线（-）和半角句号（.）组成，首位必须是字母或数字。

合法域名检测，请参见阿里云域名检测工具。

域名转发策略支持精确匹配和通配符匹配两种模式：

- 精确域名：www.aliyun.com
- 通配符域名（泛域名）：*.aliyun.com, *.market.aliyun.com

当前端请求同时匹配多条域名策略时，策略的匹配优先级为：精确匹配高于小范围通配符匹配，小范围通配符匹配高于大范围通配符匹配，如下表所示。

模式	请求测试URL	配置的域名转发策略		
		www.aliyundoc.com	*.aliyundoc.com	*.market.aliyundoc.com
精确匹配	www.aliyun.com	✓	×	×
泛域名匹配	market.aliyun.com	×	✓	×
泛域名匹配	info.market.aliyun.com	×	×	✓

ii. 选择该域名关联的证书。

> 说明
> - 证书中的域名和您添加的扩展域名必须一致。
> - 如果您配置了泛域名证书，则只有第一个泛域名证书可以被自动匹配。

iii. 单击**确定**。

扩展域名需要和转发策略配合使用才能生效，还需要配置相同域名转发策略才能生效 。

5. （可选）执行以下步骤，配置转发策略。

i. 在**提示**页面，单击**去配置**，或者在**实例管理**页面，单击目标实例ID进入**监听**页签。

ii. 找到已创建的HTTPS监听，单击操作列下的**配置转发策略**。

iii. 在**配置转发策略**面板，单击**添加转发策略**。

iv. 配置转发策略。

更多信息，请参见基于域名或URL路径进行转发。

> 说明 确保转发策略中配置的域名和您添加的扩展域名一致。

相关文档

- CreateDomainExtension

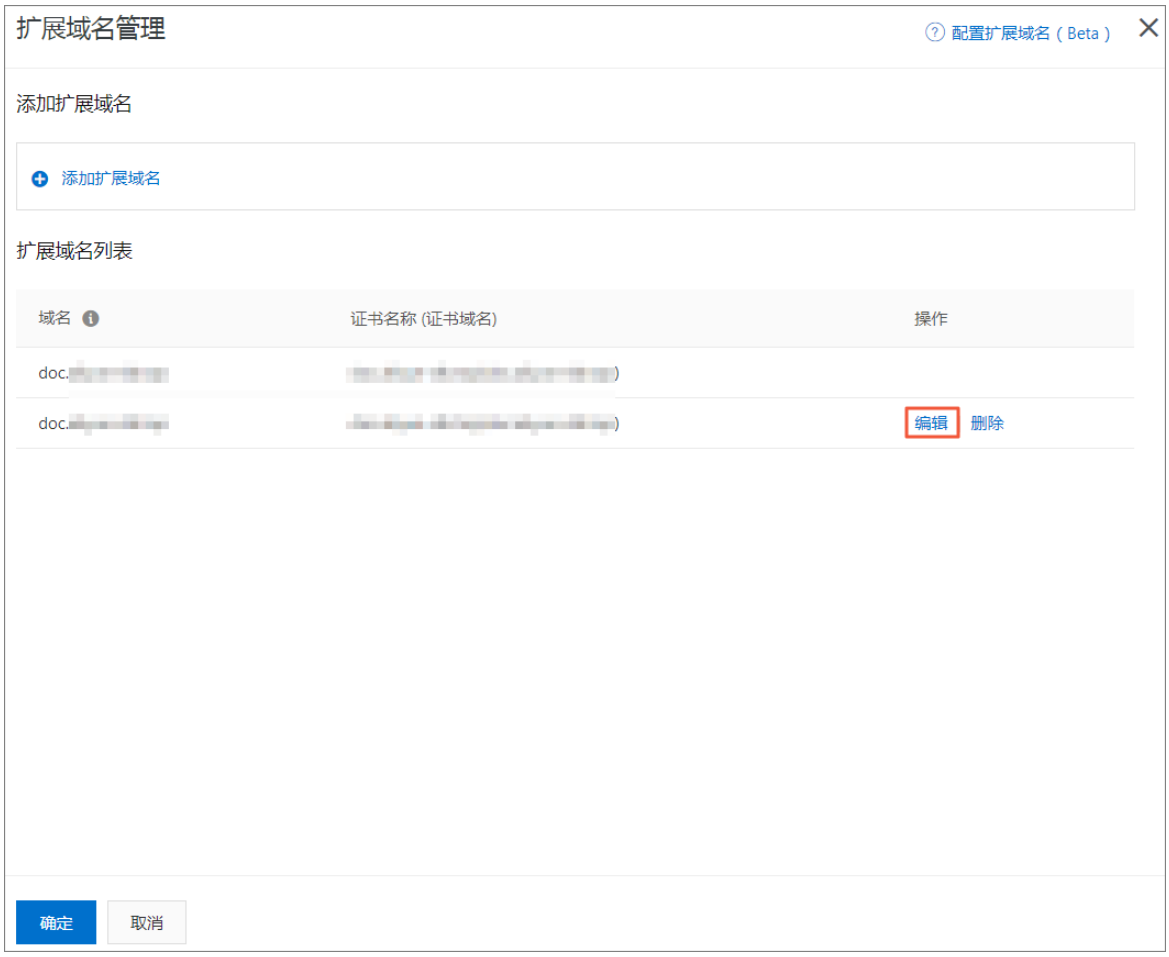
6.3. 编辑扩展域名

您可以替换已添加的扩展域名使用的证书。

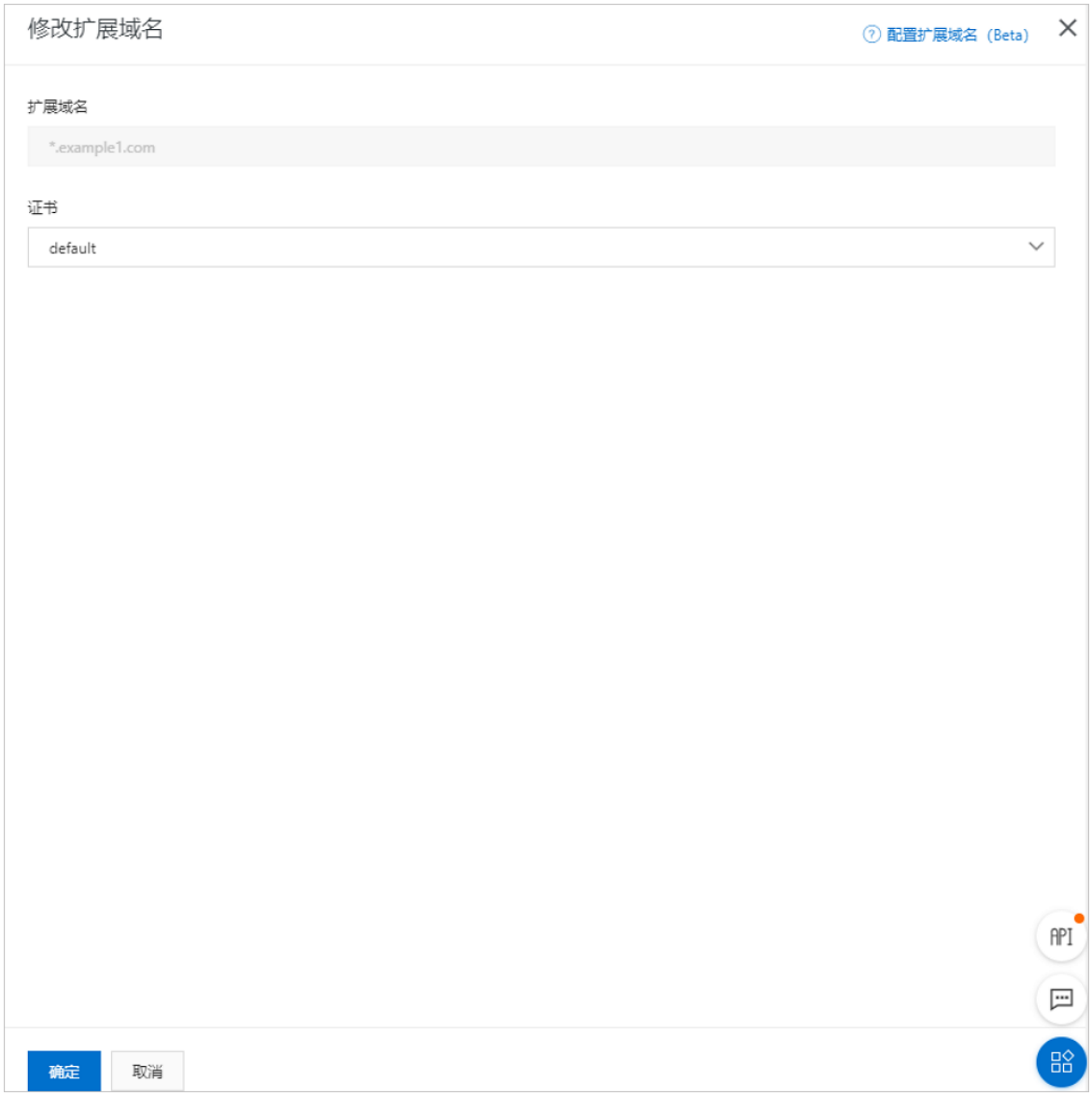
操作步骤

1. 登录传统型负载均衡CLB控制台。
2. 在左侧导航栏，选择**实例 > 实例管理**。
3. 在**实例管理**页面，单击负载均衡实例的ID。
4. 单击**监听**页签，找到已创建的HTTPS监听，在**操作**列选择 > **扩展域名管理**。

5. 找到目标扩展域名，然后在**操作**列单击**编辑**。



6. 在**修改扩展域名**页面，选择新的证书，然后单击**确定**。

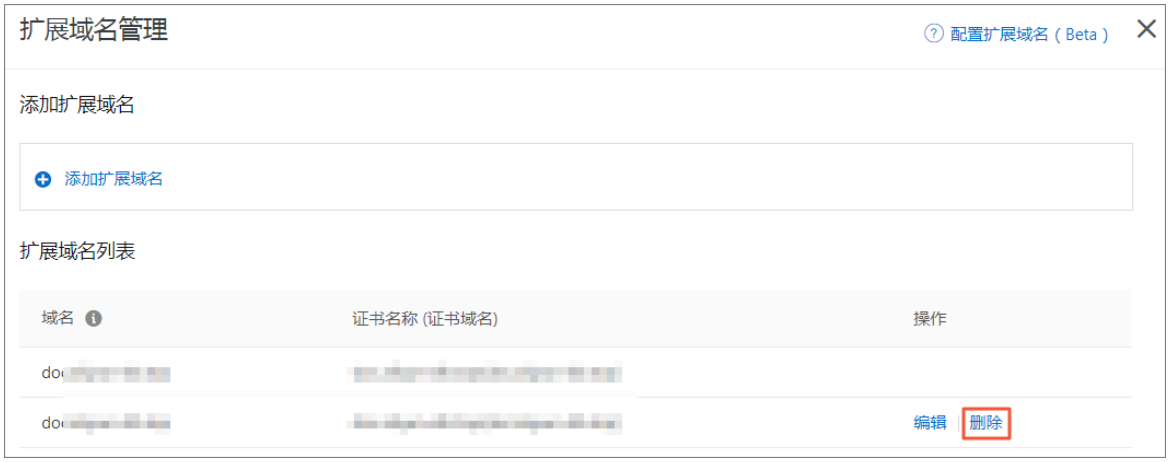


6.4. 删除扩展域名

当扩展域名不需要使用时，可以删除扩展域名。

操作步骤

1. 登录传统型负载均衡CLB控制台。
2. 在左侧导航栏，选择**实例 > 实例管理**。
3. 在**实例管理**页面，单击负载均衡实例的ID。
4. 单击**监听**页签，然后单击HTTPS监听操作列下的 **> 扩展域名管理**。
5. 在**扩展域名管理**页面，单击扩展域名操作列下的**删除**。



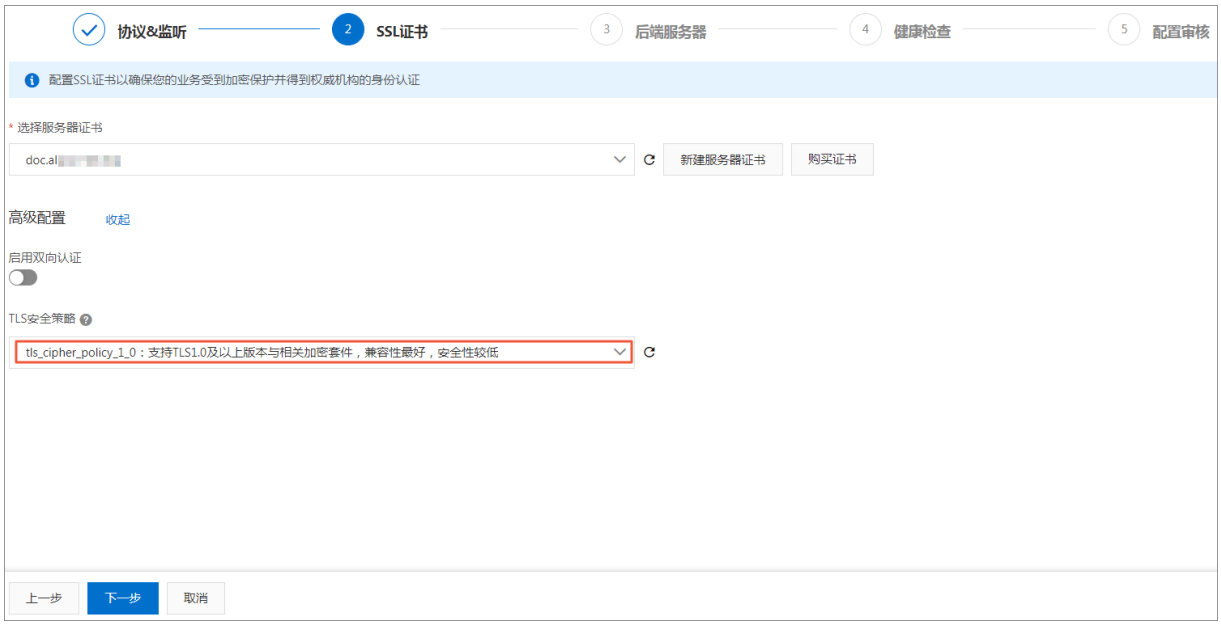
6. 在弹出的删除对话框中，单击**确定**。

7.TLS安全策略说明

性能保障型负载均衡实例在创建和配置HTTPS监听时，支持选择TLS安全策略。

选择TLS安全策略

您可以在添加或者配置HTTPS监听时，在**SSL证书**页签，单击**高级配置**后面的修改，在展开项中选择TLS安全策略。具体操作，请参见添加HTTPS监听。



TLS安全策略

TLS安全策略包含HTTPS可选的TLS协议版本和配套的加密算法套件。TLS协议版本越高，HTTPS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。

安全策略	支持TLS版本	支持加密算法套件
tls_cipher_policy_1_0	TLSv1.0、TLSv1.1和TLSv1.2	ECDHE-ECDSA-AES128-GCM-SHA256、ECDHE-ECDSA-AES256-GCM-SHA384、ECDHE-ECDSA-AES128-SHA256、ECDHE-ECDSA-AES256-SHA384、ECDHE-RSA-AES128-GCM-SHA256、ECDHE-RSA-AES256-GCM-SHA384、ECDHE-RSA-AES128-SHA256、ECDHE-RSA-AES256-SHA384、AES128-GCM-SHA256、AES256-GCM-SHA384、AES128-SHA256、AES256-SHA256、ECDHE-ECDSA-AES128-SHA、ECDHE-ECDSA-AES256-SHA、ECDHE-RSA-AES128-SHA、ECDHE-RSA-AES256-SHA、AES128-SHA、AES256-SHA、DES-CBC3-SHA

安全策略	支持TLS版本	支持加密算法套件
tls_cipher_policy_1_1	TLSv1.1和TLSv1.2	ECDHE-ECDSA-AES128-GCM-SHA256、ECDHE-ECDSA-AES256-GCM-SHA384、ECDHE-ECDSA-AES128-SHA256、ECDHE-ECDSA-AES256-SHA384、ECDHE-RSA-AES128-GCM-SHA256、ECDHE-RSA-AES256-GCM-SHA384、ECDHE-RSA-AES128-SHA256、ECDHE-RSA-AES256-SHA384、AES128-GCM-SHA256、AES256-GCM-SHA384、AES128-SHA256、AES256-SHA256、ECDHE-ECDSA-AES128-SHA、ECDHE-ECDSA-AES256-SHA、ECDHE-RSA-AES128-SHA、ECDHE-RSA-AES256-SHA、AES128-SHA、AES256-SHA、DES-CBC3-SHA
tls_cipher_policy_1_2	TLSv1.2	ECDHE-ECDSA-AES128-GCM-SHA256、ECDHE-ECDSA-AES256-GCM-SHA384、ECDHE-ECDSA-AES128-SHA256、ECDHE-ECDSA-AES256-SHA384、ECDHE-RSA-AES128-GCM-SHA256、ECDHE-RSA-AES256-GCM-SHA384、ECDHE-RSA-AES128-SHA256、ECDHE-RSA-AES256-SHA384、AES128-GCM-SHA256、AES256-GCM-SHA384、AES128-SHA256,AES256-SHA256、ECDHE-ECDSA-AES128-SHA、ECDHE-ECDSA-AES256-SHA、ECDHE-RSA-AES128-SHA、ECDHE-RSA-AES256-SHA、AES128-SHA、AES256-SHA、DES-CBC3-SHA
tls_cipher_policy_1_2_strict	TLSv1.2	ECDHE-ECDSA-AES128-GCM-SHA256、ECDHE-ECDSA-AES256-GCM-SHA384、ECDHE-ECDSA-AES128-SHA256、ECDHE-ECDSA-AES256-SHA384、ECDHE-RSA-AES128-GCM-SHA256、ECDHE-RSA-AES256-GCM-SHA384、ECDHE-RSA-AES128-SHA256、ECDHE-RSA-AES256-SHA384、ECDHE-ECDSA-AES128-SHA、ECDHE-ECDSA-AES256-SHA、ECDHE-RSA-AES128-SHA、ECDHE-RSA-AES256-SHA
tls_cipher_policy_1_2_strict_with_1_3	TLSv1.2及TLSv1.3	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、ECDHE-ECDSA-AES128-GCM-SHA256、ECDHE-ECDSA-AES256-GCM-SHA384、ECDHE-ECDSA-AES128-SHA256、ECDHE-ECDSA-AES256-SHA384、ECDHE-RSA-AES128-GCM-SHA256、ECDHE-RSA-AES256-GCM-SHA384、ECDHE-RSA-AES128-SHA256、ECDHE-RSA-AES256-SHA384、ECDHE-ECDSA-AES128-SHA、ECDHE-ECDSA-AES256-SHA、ECDHE-RSA-AES128-SHA、ECDHE-RSA-AES256-SHA

TLS安全策略支持的加密算法套件

安全策略	tls_cipher_policy_1_0	tls_cipher_policy_1_1	tls_cipher_policy_1_2	tls_cipher_policy_1_2_strict	tls_cipher_policy_1_2_strict_with_1_3

安全策略		tls_cipher_policy_1_0	tls_cipher_policy_1_1	tls_cipher_policy_1_2	tls_cipher_policy_1_2_strict	tls_cipher_policy_1_2_strict_with_1_3
TLS		1.2、1.1及1.0	1.1及1.2	1.2	1.2	1.2及1.3
CIPHER	ECDHE-RSA-AES128-GCM-SHA256	✔	✔	✔	✔	✔
	ECDHE-RSA-AES256-GCM-SHA384	✔	✔	✔	✔	✔
	ECDHE-RSA-AES128-SHA256	✔	✔	✔	✔	✔
	ECDHE-RSA-AES256-SHA384	✔	✔	✔	✔	✔
	AES128-GCM-SHA256	✔	✔	✔	-	-
	AES256-GCM-SHA384	✔	✔	✔	-	-
	AES128-SHA256	✔	✔	✔	-	-
	AES256-SHA256	✔	✔	✔	-	-
	ECDHE-RSA-AES128-SHA	✔	✔	✔	✔	✔
	ECDHE-RSA-AES256-SHA	✔	✔	✔	✔	✔
	AES128-SHA	✔	✔	✔	-	-
	AES256-SHA	✔	✔	✔	-	-
	DES-CBC3-SHA	✔	✔	✔	-	-
	TLS_AES_128_GCM_SHA256	-	-	-	-	✔
	TLS_AES_256_GCM_SHA384	-	-	-	-	✔
	TLS_CHACHA20_POLY1305_SHA256	-	-	-	-	✔
	TLS_AES_128_CCM_SHA256	-	-	-	-	✔

安全策略		tls_cipher_policy_1_0	tls_cipher_policy_1_1	tls_cipher_policy_1_2	tls_cipher_policy_1_2_strict	tls_cipher_policy_1_2_strict_with_1_3
	TLS_AES_128_CCM_8_SHA256	-	-	-	-	✔
	ECDHE-ECDSA-AES128-GCM-SHA256	-	-	-	-	✔
	ECDHE-ECDSA-AES256-GCM-SHA384	-	-	-	-	✔
	ECDHE-ECDSA-AES128-SHA256	-	-	-	-	✔
	ECDHE-ECDSA-AES256-SHA384	-	-	-	-	✔
	ECDHE-ECDSA-AES128-SHA	-	-	-	-	✔
	ECDHE-ECDSA-AES256-SHA	-	-	-	-	✔

说明 上表中的✔表示支持，-表示不支持。

8.共享实例带宽

负载均衡支持按带宽计费的负载均衡实例下的所有监听共享实例的总带宽。

开启监听带宽限速

在创建监听时，您可以选择开启或者关闭监听带宽限速。

- 开启监听带宽限速：您可以对监听的带宽进行限制，但所有监听带宽峰值的总和不能超过实例的带宽峰值。
- 关闭监听带宽限速：不限制监听带宽的情况下，实例下的所有监听共享实例带宽。

如何共享带宽？

例如您购买了一个带宽峰值为10 Mbps的负载均衡实例，并在该实例下创建了三个监听（监听A、监听B和监听C）。监听A的带宽峰值设置为4 Mbps，另外两个监听没有设置带宽峰值。三个监听的带宽使用可能出现如下几种情况：

- 如果监听A和监听C一直没有流量，那么监听B最多也只能消耗剩余的6 Mbps带宽（10 Mbps-4 Mbps=6 Mbps）。
- 如果监听C一直没有流量，而监听B的出流量很大，超过了剩余的6 Mbps带宽。此时，监听B会产生丢包；监听A因为有设置的4 Mbps的带宽，并且经过的流量没有超过设置的带宽峰值，所以不会产生丢包。
- 如果监听A、监听B和监听C经过的流量都很大的情况下，那么监听B和监听C就会共享（竞争）剩余的6 Mbps带宽。此时，监听A的流量不会受监听B和监听C的影响，始终能达到预留的4 Mbps峰值；如果监听B和监听C的流量一样，两个监听占用的带宽去会趋近于均分。

因此，对监听带宽的限制值是资源预留，这是为了保证核心的业务始终有足够的带宽。非核心的业务可以不设置监听带宽值，它们竞争实例剩余的带宽资源。

9.配置监听转发（redirect）

HTTPS是加密数据传输协议，安全性高。

传统型负载均衡CLB

支持将HTTP访问重定向至HTTPS，方便您进行全站HTTPS部署。

CLB

已经在全部地域开放了HTTP重定向功能，且在英国（伦敦）地域支持配置重定向状态码。

前提条件

您已经创建了一个

CLB

实例，并为该实例添加了HTTPS监听。具体操作，请参见添加HTTPS监听。

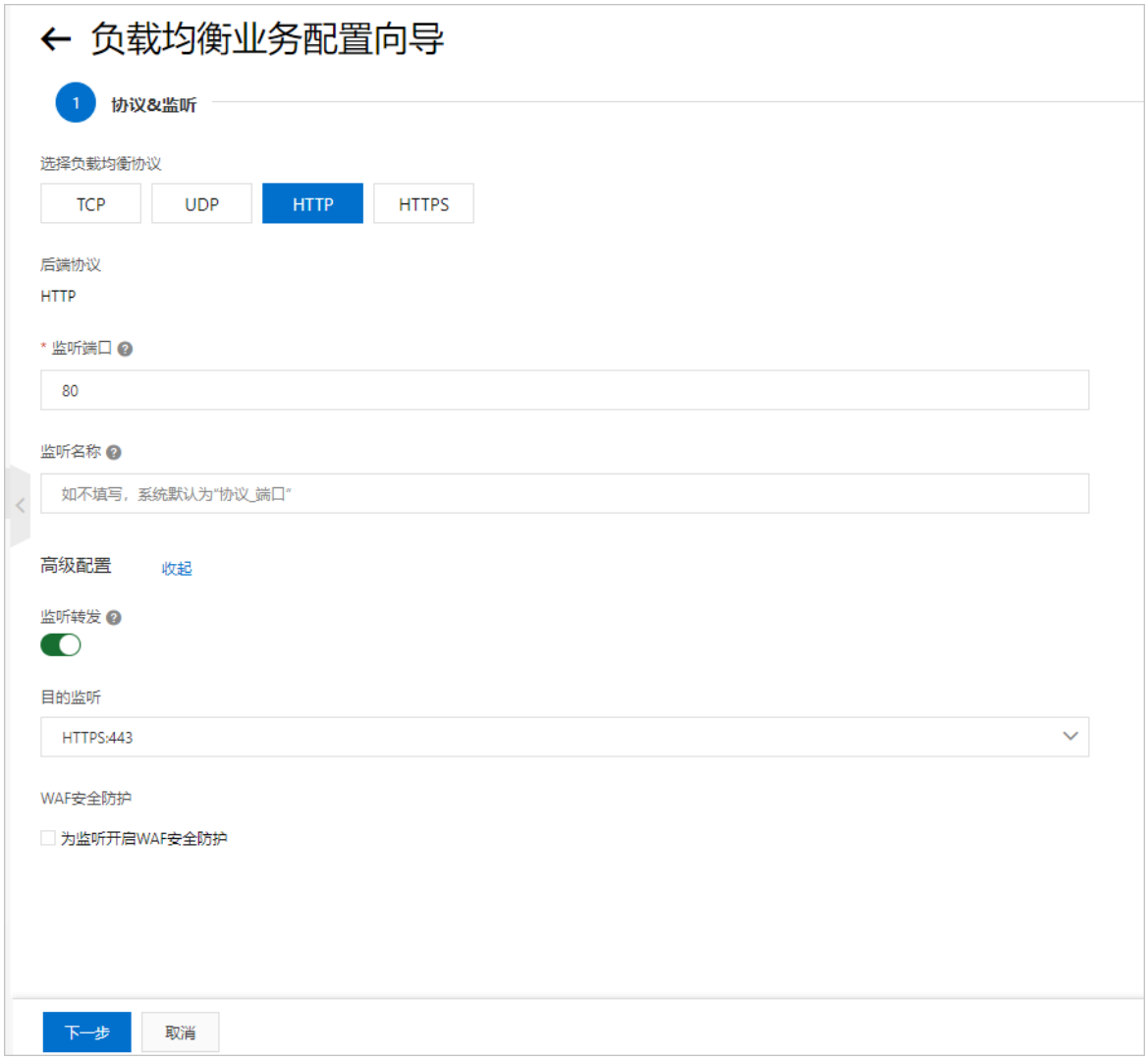
操作步骤

1. 登录传统型负载均衡CLB控制台。
2. 在顶部菜单栏处，选择

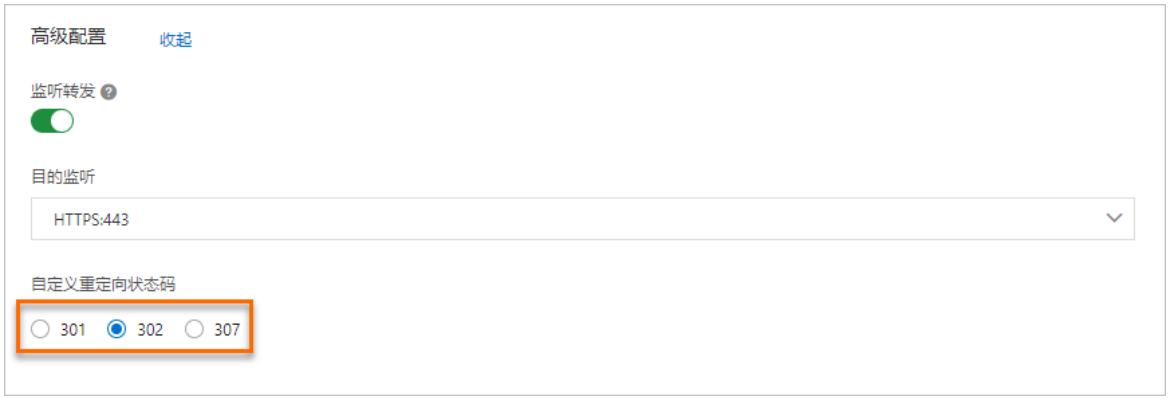
   CLB

   实例所属地域。
3. 选择以下一种方法，打开监听配置向导。
   - 在**实例管理**页面，找到目标实例，然后在**操作**列单击**监听配置向导**。
   - 在**实例管理**页面，单击目标实例ID链接，然后在**监听**页签单击**添加监听**。
4. 在打开的**协议&监听**对话框，选择负载均衡协议为**HTTP**，并配置监听端口。
5. 在**高级配置**右侧单击**修改**，在展开项中打开**监听转发**开关，选择目标监听，然后单击**下一步**。

   此处目的监听可以是该实例下任意端口的HTTPS监听。



在英国（伦敦）地域支持配置**自定义重定向状态码**。



6. 在**配置审核**页签，单击**提交**，然后在弹出的提示框中，单击**知道了**。

   监听转发开启后，该

   CLB

   实例所有来自HTTP的访问都会转发至HTTPS，并根据HTTPS的监听配置进行转发。


实例详情
监听
虚拟服务器组
默认服务器组
主备服务器组
监控
添加监听
监听名称
前端协议/端口
后端协议/端口
运行状态
健康检查状态
访问控制
监控
服务器组
操作
http_80
HTTP:80
重定向至 HTTPS: 443
运行中
修改监听配置
启动
停止

10.FAQ

10.1. 负载均衡服务FAQ

包含以下问题：

传统型负载均衡CLB是否支持端口跳转？

支持。

具体操作，请参见配置监听转发（redirect）。

禁用公网网卡是否影响负载均衡服务？

如果ECS有公网IP，禁用公网网卡会影响负载均衡服务。

因为在有公网网卡的情况下，默认路由会走公网，禁用后无法回包从而影响负载均衡服务。建议不要禁止公网网卡，如一定要禁止，需要修改默认路由为私网才会不影响服务，但需要考虑业务是否对公网有依赖，如通过公网访问RDS等。

为什么每个连接达不到带宽峰值？

因为负载均衡系统通过集群部署的方式为负载均衡实例提供服务，所有外部的访问请求都将平均分散到这些负载均衡系统服务器上进行转发。所以，设定的带宽峰值将被平均设定在多台系统服务器上。

单个连接下载的流量上限计算方法为：`单个连接下载峰值=设置的负载均衡总带宽/(N-1)`。N为流量转发分组个数，当前值固定为4。例如您在控制台上设置的是10 Mbps带宽上限，那么单个客户端可下载的最大流量为`10/(4-1)=3.33 Mbps`。

基于负载均衡的实现原理，建议在配置单个监听的带宽峰值时根据您实际的业务情况并结合其实现方式来设定一个较为合理的值，从而确保您业务的正常对外服务不会受到影响和限制。

负载均衡各监听支持的连接超时时间范围是多少？

- TCP监听连接超时时间：10~900秒
- HTTP监听：
  - 连接空闲超时时间：1~60秒。
  - 连接请求超时时间：1~180秒。
- HTTPS监听：

- 连接空闲超时时间：1~60秒。
- 连接请求超时时间：1~180秒。

为什么负载均衡服务地址会连接访问超时？

从服务端分析，以下情况会导致服务地址连接访问超时：

- 服务地址被安全防护

  如流量黑洞和清洗，WAF防护（WAF的特点是建连后向客户端和服务器集群双向发送RST报文）。

- 客户端端口不足

  尤其容易发生在压测的时候，客户端端口不足会导致建立连接失败，负载均衡默认会抹除TCP连接的timestamp属性，Linux协议栈的tw_reuse（time_wait状态连接复用）无法生效，time_wait状态连接堆积导致客户端端口不足。

  解决方法：客户端使用长连接代替短连接。使用RST报文断开连接（socket设置SO_LINGER属性），而不是发FIN包这种方式断开。

- 后端服务器accept队列满

  后端服务器accept队列满，导致后端服务器不回复syn_ack报文，客户端超时。

  解决方法：默认的net.core.somaxconn的值为128，执行 `sysctl -w net.core.somaxconn=1024` 更改它的值，并重启后端服务器上的应用。

- 从四层负载均衡后端服务器访问该四层负载均衡的服务地址

  四层负载均衡，在该负载均衡的后端服务器上去访问该负载均衡的服务地址会导致连接失败，常见的场景是后端应用使用URL拼接的方式跳转访问。

- 对连接超时的RST处理不当

  负载均衡上建立TCP连接后，如果900秒未活动，则会向客户端和服务器双向发送RST断开连接，有的应用对RST异常处理不当，可能会对已关闭的连接再次发送数据导致应用超时。

为什么有时候会话保持会失败？

- 查看是否在监听配置中已经开启了会话保持功能。
- HTTP或HTTPS监听在后端服务器返回4xx响应码的报文中无法插入会话保持所需Cookie。

  解决方案：改用TCP监听，因为TCP监听是以源客户端的IP来做会话保持的，另外后端ECS上也可以插入Cookie，并增加Cookie的判断来多重保障。

- 302重定向会改变会话保持中的SERVERID字串。

  负载均衡植入Cookie时，如果后端ECS中有回复302重定向的报文，将改变会话保持中的SERVERID字串，导致会话保持失效。

  排查方法：在浏览器端捕抓请求与响应的回复，或用抓包软件抓包后分析是否存在302的响应报文，对比前后报文的Cookie中的SERVERID字串是否不同了。

  解决方案：改用TCP监听，因为TCP监听是以源客户端的IP来做会话保持的，另外后端ECS上也可以插入Cookie，并增加Cookie的判断来多重保障。

- 会话保持时间设置过小，会话保持时间过小也会导致会话保持失败。

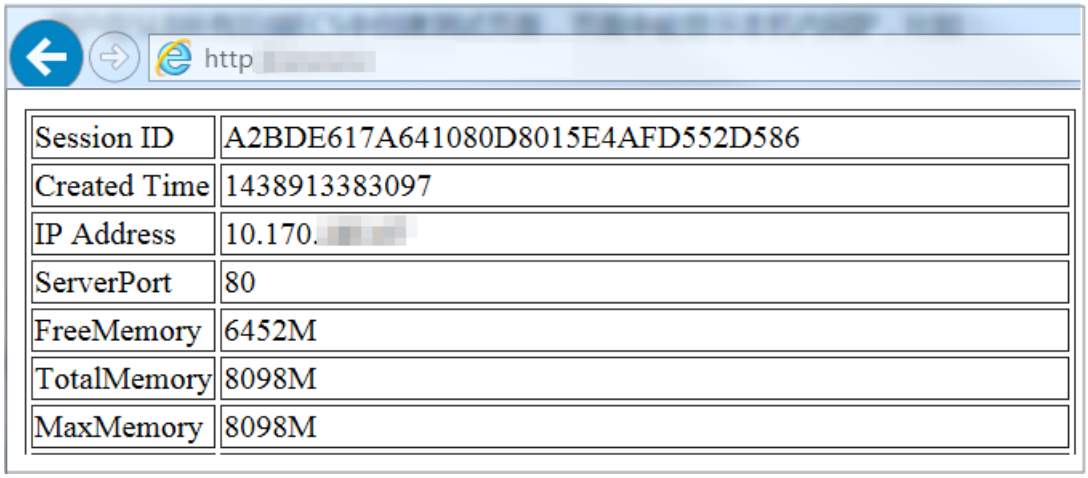
如何查看会话保持字符串？

可以在浏览器中用F12查看回应报文中是否含有SERVERID字符串或用户指定的关键字，或者运行 `curl www.example.com -c /tmp/cookie123` 保存一下Cookie，再用 `curl www.example.com -b /tmp/cookie123` 访问。

如何使用Linux curl测试负载均衡会话保持？

1. 创建测试页面。

   在负载均衡所有后端ECS中创建测试页面，如下图所示页面中能显示本机内网IP。内网IP用于判断相应请求被指派到的物理服务器。通过观察该IP的一致性，来判断负载均衡会话保持的有效性。

2. Linux系统内执行curl命令。

   假设负载均衡服务IP地址是 10.170.XX.XX，创建的测试页面URL为： `http://10.170.XX.XX/check.jsp` 。

   i. 登录用来测试的Linux服务器。

   ii. 执行以下命令查询负载均衡服务器Cookie值。

   ```
   curl -c test.cookie http://10.170.XX.XX/check.jsp
   ```

   > **说明** 阿里云负载均衡会话保持默认模式是植入Cookie，而curl测试默认不会保存和发送Cookie，所以必须先保存相应的Cookie，用于Cookie测试。否则，curl测试结果是随机的，会误认为负载均衡会话保持无效。

   iii. 执行以下命令持续测试。

   ```
   for ((a=1;a<=30;a++));
       do curl  -b test.cookie http://10.170.XX.XX/check.jsp  | grep '10.170.XX.XX';
       sleep 1;
   done
   ```

   > **说明** a≤30是重复测试次数，可以按需修改。 `grep '10.170.XX.XX'` 是筛选显示的IP信息，根据后端ECS内网IP情况进行相应修改。

   iv. 观察上述测试返回的IP，如果是同一台ECS内网IP，则证明负载均衡会话保持有效；反之则证明负载均衡会话保持有问题。

一个请求通过负载均衡到达后端服务器，如果客户端在未收到后端服务器的回复前主动断开和负载均衡的连接，负载均衡会同时断开和后端服务器的连接么？

负载均衡在读写过程中不会断开与后端服务器的连接。

负载均衡是否支持客户端请求自带TOA字段？

默认不支持。客户端请求自带的TOA（TCP Option Address）字段会与负载均衡内部交互使用的TOA字段冲突，导致无法获取客户端的真实IP地址。

但您可以通过以下方法来获取客户端的真实IP：

- 通过Proxy Protocol获取客户端真实IP（四层监听）
- 保留客户端真实源地址（七层监听）

10.2. 七层监听（HTTPS或HTTP）FAQ

本文包含以下常见问题：

- 为什么请求经过七层负载均衡转发后，后端服务器的响应头中的某些参数会被删除？
- 为什么在HTTP请求的头部增加了Transfer-Encoding: chunked字段？
- 为什么HTTP监听访问正常但HTTPS监听打开网址不加载样式？
- HTTPS监听使用什么端口？
- 负载均衡支持哪些类型的证书？
- 负载均衡是否支持keytool创建的证书？
- 可以使用PKCS#12（PFX）格式的证书么？
- 添加证书时，为什么会出现KeyEncryption的错误？
- 负载均衡HTTPS支持哪些SSL协议版本？
- HTTPS session ticket的保持时间是多久？
- 可以上传包含DH PARAMETERS字段的证书吗？
- HTTPS监听是否支持SNI?
- HTTP或HTTPS监听访问后端服务器的HTTP协议版本是什么？
- 后端服务器能否获取客户端访问HTTP或HTTPS监听的协议版本？
- HTTP或HTTPS连接的超时时间是如何规定的？

为什么请求经过七层负载均衡转发后，后端服务器的响应头中的某些参数会被删除？

为了实现会话保持，负载均衡会修改后端服务器响应头中的Date、Server、X-Pad和X-Accel-Redirect等参数值。

解决方案：

- 在自定义的报文头部中加入一个前缀，如xl-server或xl-date，以避开负载均衡的处理。
- 将七层HTTP监听改为四层TCP监听。

为什么在HTTP请求的头部增加了Transfer-Encoding: chunked字段？

现象：

将域名解析到七层负载均衡的服务地址后，从本地主机访问域名时发现在HTTP请求的头部增加了一个Transfer-Encoding: chunked字段，但是从本地主机直接访问后端服务器时是没有这个字段的。

原因：

这是由于七层负载均衡基于Tengine反向代理实现。Transfer-Encoding字段表示Web服务器如何对响应消息体编码，例如Transfer-Encoding: chunked表示Web服务器对响应消息体做了分块传输。

> **说明** 在四层负载均衡服务中，负载均衡仅转发流量，不存在该字段。

为什么HTTP监听访问正常但HTTPS监听打开网址不加载样式？

现象：

分别创建HTTP和HTTPS监听，两个监听使用同样的后端服务器。以HTTP方式访问监听端口对应的网站时，网站正常显示，但使用HTTPS监听访问时，网站排版显示错乱。

原因：

负载均衡默认是不会屏蔽JS文件加载传输的，可能原因：

- 证书和浏览器安全级别不兼容导致。
- 证书是非正规第三方证书，需要联系证书发布者检查证书问题。

解决方案：

1. 打开网站时，按照浏览器提示加载脚本。
2. 在客户端中添加对应证书。

HTTPS监听使用什么端口？

HTTPS监听对端口无特殊要求，建议您使用443端口。

负载均衡支持哪些类型的证书？

支持上传PEM格式的服务器证书和CA证书。

服务器证书需要上传证书内容和私钥，CA证书只需要上传证书内容。

负载均衡是否支持keytool创建的证书？

支持。

但在上传证书前，您需要将证书转换为PEM格式，更多信息，请参见转换证书格式。

可以使用PKCS#12（PFX）格式的证书么？

可以。

但在上传证书前，您需要将证书转换为PEM格式，更多信息，请参见转换证书格式。

添加证书时，为什么会出现KeyEncryption的错误？

该错误由于私钥内容有误导致。更多信息，请参见证书要求。

负载均衡HTTPS支持哪些SSL协议版本？

TLSv1、TLSv1.1以及TLSv1.2版本。

HTTPS session ticket的保持时间是多久？

HTTPS session ticket保持时间为300秒。

可以上传包含DH PARAMETERS字段的证书吗？

HTTPS监听使用的ECDHE算法簇支持前向保密技术，不支持将DHE算法簇所需要的安全增强参数文件上传，即不支持将PEM证书文件中含BEGIN DH PARAMETERS字段的证书上传。

HTTPS监听是否支持SNI？

SNI（Server Name Indication）是为了解决一个服务器使用多个域名和证书的SSL/TLS扩展，负载均衡HTTPS监听支持SNI功能，更多信息，请参见添加扩展域名。

HTTP或HTTPS监听访问后端服务器的HTTP协议版本是什么？

- 客户端请求的协议为HTTP 1.1或者HTTP 2.0版本时，七层监听访问后端服务器的HTTP协议版本是HTTP 1.1。
- 客户端请求的协议为除HTTP 1.1和HTTP 2.0以外其他版本时，七层监听访问后端服务器的HTTP协议版本是HTTP 1.0。

后端服务器能否获取客户端访问HTTP或HTTPS监听的协议版本？

可以。

HTTP或HTTPS连接的超时时间是如何规定的？

- HTTP长连接的请求数量限定是最多连续发送100个请求，超过限定将关闭这条连接。
- HTTP长连接两个HTTP或HTTPS请求之间的超时时间是可配置的，配置范围为1~60秒（存在误差1~2秒），超过后会关闭TCP连接，如果用户有长连接使用需求请尽量保持在13秒之内发送一个心跳请求。
- 负载均衡与后端一台ECS实例TCP三次握手完成过程的超时时间为5秒，超时后选择下一台ECS实例，查询访问日志的upstream响应时间可以定位。
- 负载均衡等待一台ECS实例回复请求的响应时间是可配置的，配置范围为1~180秒，超过后一般会返回504响应码或408响应码给客户端，查询访问日志的upstream响应时间可以定位。
- HTTPS session重用超时间为300秒，超过后同一客户端需要重新进行完整的SSL握手过程。

10.3. WebSocket和WebSocket Secure协议概述

WebSocket（WS）和WebSocket Secure（WSS）协议概述

本文介绍WebSocket和WebSocket Secure协议相关的简介。

什么是WebSocket？

WebSocket是HTML5一种新的协议，它实现了浏览器与服务器全双工（full-duplex）通信，能更好地节省服务器资源和带宽并达到实时通讯。WebSocket建立在TCP之上，同HTTP一样通过TCP来传输数据，但是它和HTTP最大不同是：WebSocket是一种双向通信协议，在建立连接后，WebSocket服务器和Browser/Client Agent都能主动地向对方发送或接收数据，就像Socket一样；WebSocket需要类似TCP的客户端和服务器端通过握手连接，连接成功后才能相互通信。

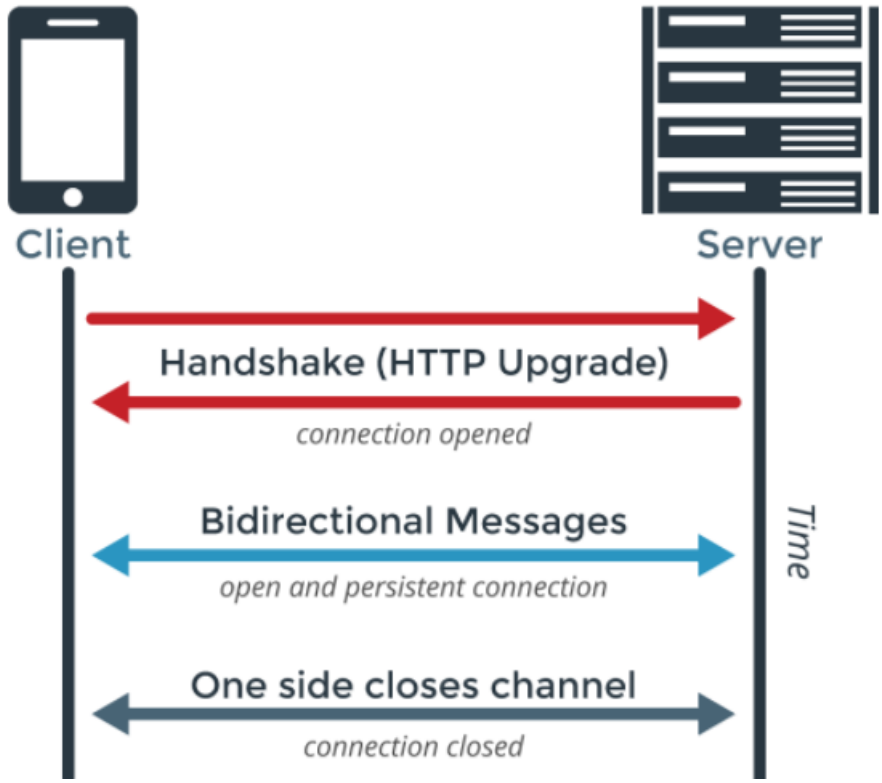
WebSocket Secure是WebSocket的加密版本。

为何使用WebSocket？

随着互联网的蓬勃发展，各种类型的Web应用层出不穷，很多应用要求服务端有能力进行实时推送（例如直播间聊天室），以往很多网站为了实现推送技术，所用的技术都是轮询。轮询是在特定的时间间隔（如每1秒），由浏览器对服务器发出HTTP请求，然后由服务器返回最新的数据给客户端的浏览器。这种传统的模式带来很明显的缺点，即浏览器需要不断地向服务器发出请求，然而HTTP请求可能包含较长的头部，其中真正有效的数据可能只是很小的一部分，显然这样会浪费很多的带宽资源。

在这种情况下，HTML5定义了WebSocket协议，能更好地节省服务器资源和带宽，并且能够更实时地进行通讯。WebSocket实现了浏览器与服务器全双工通信，允许服务器主动发送信息给客户端。

WebSocket协议的交互过程如下图所示。



如何在阿里云负载均衡上启用WebSocket和WebSocket Secure支持？

性能保障型实例无需配置。

- HTTP监听默认支持WebSocket协议。
- HTTPS监听默认支持WebSocket Secure协议。

> **说明** 性能共享型实例需要升级为性能保障型实例才能支持WebSocket和WebSocket Secure。更多信息，请参见性能保障型实例FAQ。

支持的地域

全部地域都已开放WebSocket和WebSocket Secure支持。

相关计费

WebSocket和WebSocket Secure协议不额外收取费用。

使用限制

WebSocket和WebSocket Secure协议的使用限制如下：

- 若负载均衡与ECS后端服务的连接采用HTTP/1.1，建议后端服务器采用支持HTTP/1.1的Web Server。
- 若负载均衡与后端服务超过60秒无消息交互，会主动断开连接，如需要维持连接一直不中断，需要主动实现保活机制，每60秒内进行一次报文交互。