ALIBABA CLOUD

阿里云

负载均衡

监听

文档版本：20210303

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

您已经创建负载均衡实例，具体操作，请参见创建负载均衡实例。

步骤一：配置监听

完成以下操作，完成监听配置。

1. 登录负载均衡管理控制台。
2. 在左侧导航栏，选择**实例 > 实例管理**。
3. 选择实例的地域。
4. 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，单击**监听配置向导**。

   - 在**实例管理**页面，单击目标实例ID。在**监听**页面，单击**添加监听**。

5. 配置协议监听。

监听配置	说明
选择负载均衡协议	选择监听的协议类型。 本操作，选择TCP。

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。 **说明** 现在是公测阶段，您需要在配额管理申请**TCP/UDP协议监听同端口公测权限**，在同一个负载均衡实例内，才能在以下地域支持UDP和TCP监听端口重复。其他情况下，监听端口不可重复。 ○ 阿联酋（迪拜） ○ 澳大利亚（悉尼） ○ 阿联酋（迪拜） ○ 英国（伦敦） ○ 德国（法兰克福） ○ 美国（硅谷） ○ 美国（弗吉尼亚） ○ 印度尼西亚（雅加达） ○ 日本（东京） ○ 印度（孟买） ○ 新加坡 ○ 马来西亚（吉隆坡） ○ 中国香港 ○ 华南1（深圳） ○ 华北5（呼和浩特） ○ 华北1（青岛） ○ 西南1（成都） ○ 华北3（张家口） ○ 华东2（上海） ○ 华北2（北京） ○ 华东1（杭州）
高级配置	

监听配置	说明
调度算法	负载均衡支持轮询、加权轮询（WRR）、加权最小连接数（WLC）和一致性哈希（CH）四种调度算法。 ○ **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。 ○ **加权最小连接数(WLC)**：除了根据每台后端服务器设定的权重值来进行轮询，同时还考虑后端服务器的实际负载（即连接数）。当权重值相同时，当前连接数越小的后端服务器被轮询到的次数（概率）也越高。 ○ **一致性哈希（CH）**： ■ **源IP**：基于源IP地址的一致性hash，相同的源地址会调度到相同的后端服务器。 ■ **四元组**：基于四元组的一致性hash（源IP、目的IP、源端口和目的端口），相同的流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。
开启会话保持	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。
访问控制方式	开启访问控制后，选择一种访问控制方式： ○ **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，白名单适用于应用只允许特定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，则负载均衡监听不会转发请求。 ○ **黑名单：禁止特定IP访问负载均衡SLB**，来自所选访问控制策略组中设置的IP地址或地址段的所有请求都不会转发，黑名单适用于应用只限制某些特定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。
选择访问控制策略组	选择访问控制策略组，作为该监听的白名单或黑名单。 **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。

监听配置	说明
启用连接优雅中断	启用连接优雅中断后，您可以在移除后端服务器或者健康检查失败后，使现有连接在一定时间内正常传输。
连接优雅中断超时时间	启用连接优雅中断，您可以在移除后端服务器前，设定保持连接的最大时间。当移除后端服务器或者健康检查失败超过设置的时间时，负载均衡器会强制关闭连接。 取值范围：10~900。 单位：秒。
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。
监听名称	设置监听的名称，用户自定义。
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，无需采用其它手段获取。
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。

6. 单击**下一步**。

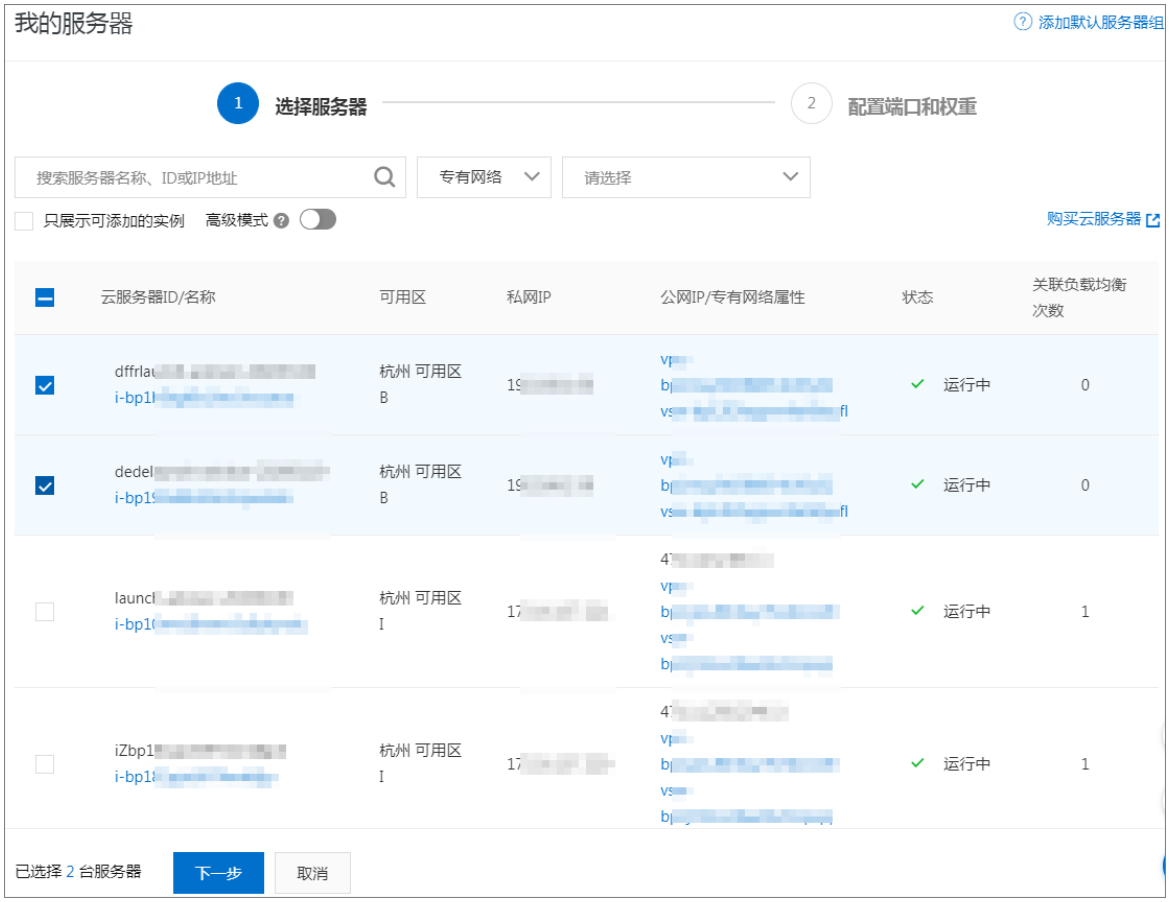
步骤二：添加后端服务器

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. 选择**默认服务器组**，单击**继续添加**。

2. 在**我的服务器**页面，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**页签下，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，该服务器不会再接受新请求。

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。单击**修改**更改健康检查配置，更多信息，请参见健康检查概述。

步骤四：提交配置

完成以下操作，确认监听配置。

1. 在**配置审核**页面，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. 在**配置成功**页面，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
- 访问控制概述
- CreateLoadBalancerTCPListener

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。

前提条件

您已经创建负载均衡实例，具体操作，请参见创建负载均衡实例。

背景信息

在添加UDP监听前，注意如下限制：

- 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SLB 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SLB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。

步骤一：配置监听

完成以下操作，完成监听配置。

1. 登录负载均衡管理控制台。
2. 在左侧导航栏，选择**实例 > 实例管理**。
3. 选择实例的地域。
4. 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，单击**监听配置向导**。

   - 在**实例管理**页面，单击目标实例ID。在**监听**页面，单击**添加监听**。

5. 配置协议监听。

监听配置	说明
选择负载均衡协议	选择监听的协议类型。 本操作，选择**TCP**。
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。 **说明** 现在是公测阶段，您需要在配额管理申请**TCP/UDP协议监听同端口公测权限**，在同一个负载均衡实例内，才能在以下地域支持UDP和TCP监听端口重复。其他情况下，监听端口不可重复。 ○ 阿联酋（迪拜） ○ 澳大利亚（悉尼） ○ 阿联酋（迪拜） ○ 英国（伦敦） ○ 德国（法兰克福） ○ 美国（硅谷） ○ 美国（弗吉尼亚） ○ 印度尼西亚（雅加达） ○ 日本（东京） ○ 印度（孟买） ○ 新加坡 ○ 马来西亚（吉隆坡） ○ 中国香港 ○ 华南1（深圳） ○ 华北5（呼和浩特） ○ 华北1（青岛） ○ 西南1（成都） ○ 华北3（张家口） ○ 华东2（上海） ○ 华北2（北京） ○ 华东1（杭州）

监听配置	说明
高级配置	
调度算法	负载均衡支持轮询、加权轮询（WRR）、加权最小连接数（WLC）和一致性哈希（CH）四种调度算法。 ○ **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。 ○ **加权最小连接数(WLC)**：除了根据每台后端服务器设定的权重值来进行轮询，同时还考虑后端服务器的实际负载（即连接数）。当权重值相同时，当前连接数越小的后端服务器被轮询到的次数（概率）也越高。 ○ **一致性哈希（CH）**： ■ **源IP**：基于源IP地址的一致性hash，相同的源地址会调度到相同的后端服务器。 ■ **四元组**：基于四元组的一致性hash（源IP、目的IP、源端口和目的端口），相同的流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。
开启会话保持	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。

监听配置	说明
访问控制方式	开启访问控制后，选择一种访问控制方式： ○ **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，白名单适用于应用只允许特定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，则负载均衡监听不会转发请求。 ○ **黑名单：禁止特定IP访问负载均衡SLB**，来自所选访问控制策略组中设置的IP地址或地址段的所有请求都不会转发，黑名单适用于应用只限制某些特定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。
选择访问控制策略组	选择访问控制策略组，作为该监听的白名单或黑名单。 **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。
启用连接优雅中断	启用连接优雅中断后，您可以在移除后端服务器或者健康检查失败后，使现有连接在一定时间内正常传输。
连接优雅中断超时时间	启用连接优雅中断，您可以在移除后端服务器前，设定保持连接的最大时间。当移除后端服务器或者健康检查失败超过设置的时间时，负载均衡器会强制关闭连接。 取值范围：10~900。 单位：秒。
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。
监听名称	设置监听的名称，用户自定义。
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，无需采用其它手段获取。
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。

6. 单击**下一步**。

步骤二：配置协议监听

完成以下操作， 配置协议监听：

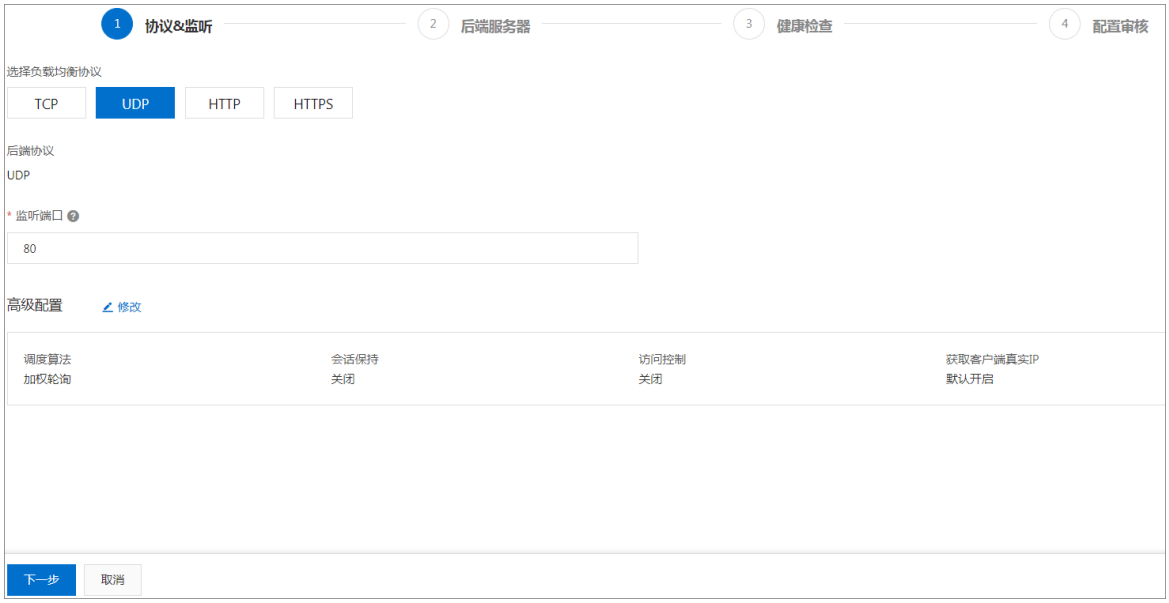
1. 在**协议&监听**页面，根据以下信息配置UDP监听。

监听配置	说明
选择负载均衡协议	选择监听的协议类型。 本操作选择**UDP**。
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。 **说明** 现在是公测阶段，您需要在配额管理申请**TCP/UDP协议监听同端口公测权限**，在同一个负载均衡实例内，才能在以下地域支持UDP和TCP监听端口重复。其他情况下，监听端口不可重复。 ○ 阿联酋（迪拜） ○ 澳大利亚（悉尼） ○ 阿联酋（迪拜） ○ 英国（伦敦） ○ 德国（法兰克福） ○ 美国（硅谷） ○ 美国（弗吉尼亚） ○ 印度尼西亚（雅加达） ○ 日本（东京） ○ 印度（孟买） ○ 新加坡 ○ 马来西亚（吉隆坡） ○ 中国香港 ○ 华南1（深圳） ○ 华北5（呼和浩特） ○ 华北1（青岛） ○ 西南1（成都） ○ 华北3（张家口） ○ 华东2（上海）

监听配置	说明
高级配置	
调度算法	负载均衡支持轮询、加权轮询（WRR）、加权最小连接数（WLC）和一致性哈希（CH）四种调度算法。 ○ **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。 ○ **加权最小连接数(WLC)**：除了根据每台后端服务器设定的权重值来进行轮询，同时还考虑后端服务器的实际负载（即连接数）。将访问请求分发给当前连接数最小的后端服务器，权重越大的被分发的几率越大。 ○ **一致性哈希（CH）**： ■ **源IP**：基于源IP地址的一致性hash，相同的源地址会调度到相同的后端服务器。 ■ **四元组**：基于四元组的一致性hash（源IP+目的IP+源端口+目的端口），相同的流会调度到相同的后端服务器。 ■ **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。
启用访问控制	选择是否启用访问控制。

监听配置	说明
访问控制方式	开启访问控制后，选择一种访问控制方式： ○ **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，白名单适用于应用只允许特定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**，来自所选访问控制策略组中设置的IP地址或地址段的所有请求都不会转发，黑名单适用于应用只限制某些特定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。
选择访问控制策略组	选择访问控制策略组，作为该监听的白名单或黑名单。 **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。
获取客户端真实IP	UDP协议监听的后端服务器可直接获取客户端的真实IP。 **说明** 经典网络实例的UDP协议暂不支持查看源地址。
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。

2. 单击**下一步**。



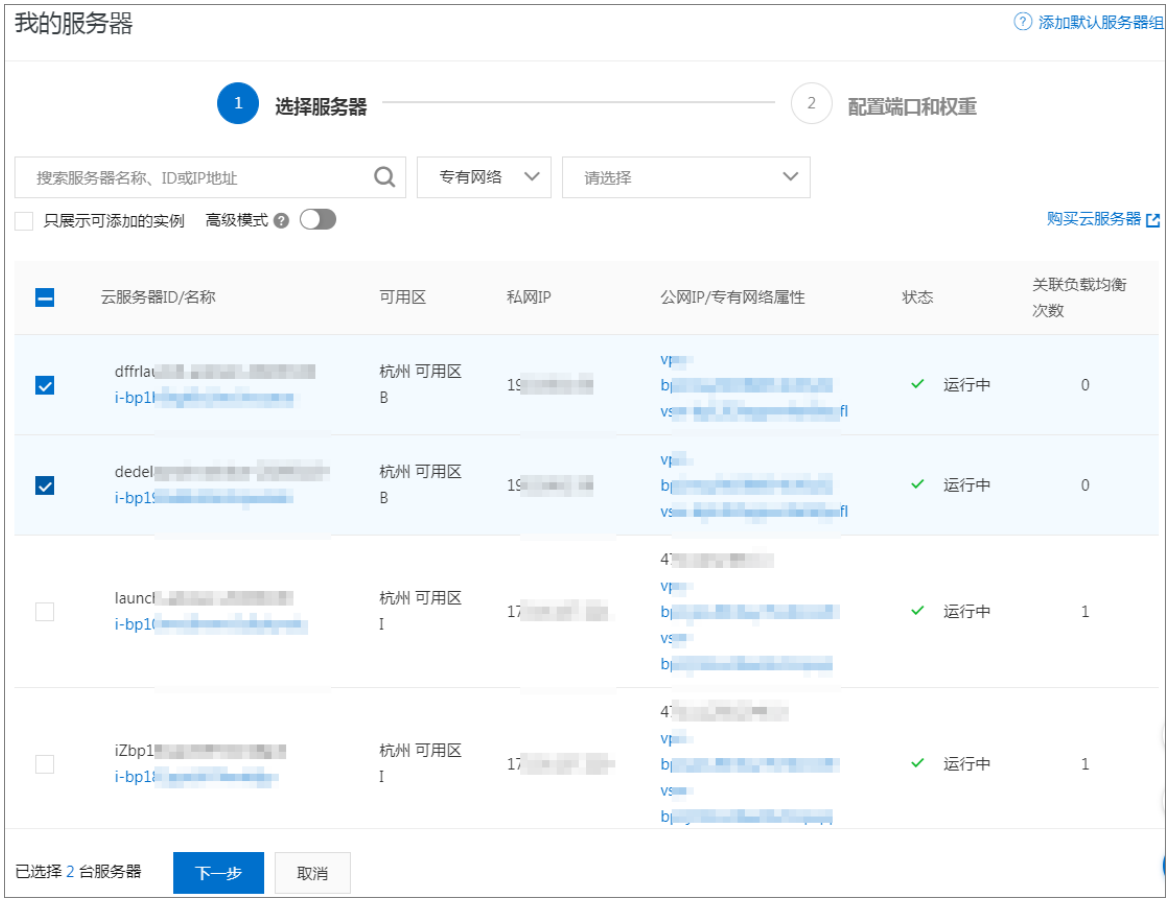
步骤三：添加后端服务器

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。详情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. 选择**默认服务器组**，单击**继续添加**。

2. 选择要添加的ECS实例，然后单击**下一步**。



3. 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，该服务器不会再接受新请求。

4. 单击**添加**，在**默认服务器组**页签下，配置默认服务器端口。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。单击**修改**更改健康检查配置，更多信息，请参见健康检查概述。

步骤四：提交配置

完成以下操作，确认监听配置。

1. 在**配置审核**页面，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. 在**配置成功**页面，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应用和小的手机游戏等。您可以添加一个HTTP监听转发来自HTTP协议的请求。

前提条件

您已经创建了负载均衡实例。具体操作，请参见创建负载均衡实例。

步骤一：配置协议与监听

1. 登录负载均衡管理控制台。
2. 在左侧导航栏，选择**实例 > 实例管理**。
3. 选择实例的地域。
4. 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，单击**监听配置向导**。
   - 在**实例管理**页面，单击目标实例ID，然后单击**监听**页签下的**添加监听**。
5. 配置协议与监听，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。 本操作，选择**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。
监听名称	设置监听的名称，用户自定义。
高级配置	
调度算法	负载均衡支持轮询、加权轮询（WRR）、加权最小连接数（WLC）和一致性哈希（CH）四种调度算法。 - **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。 - **加权最小连接数(WLC)**：除了根据每台后端服务器设定的权重值来进行轮询，同时还考虑后端服务器的实际负载（即连接数）。当权重值相同时，当前连接数越小的后端服务器被轮询到的次数（概率）也越高。
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。启用访问控制后，您可以通过配置访问控制策略来实现允许某些特定IP访问负载均衡，或禁止某些特定IP访问负载均衡的功能。
访问控制方式	开启访问控制后，选择一种访问控制方式： ○ **白名单**，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。 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，则负载均衡监听不会转发请求。 ○ **黑名单**，来自所选访问控制策略组中设置的IP地址或地址段的所有请求都不会转发。 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。
选择访问控制策略组	选择访问控制策略组，作为该监听的白名单或黑名单。 **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。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，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。
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或主备服务组。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 > 继续添加**。
2. 在**我的服务器**页面，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**页签下，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，该服务器不会再接受新请求。

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。单击**修改**更改健康检查配置。更多信息，请参见健康检查概述。

步骤四：提交配置

完成以下操作，确认监听配置。

1. 在**配置审核**页面，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. 在**配置成功**页面，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
- CreateLoadBalancerHTTPListener

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

您已经创建负载均衡实例，具体操作，请参见创建负载均衡实例。

步骤一：配置协议与监听

1. 登录负载均衡管理控制台。
2. 在左侧导航栏，选择**实例 > 实例管理**。
3. 选择实例的地域。
4. 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，单击**监听配置向导**。
   - 在**实例管理**页面，单击目标实例ID，然后单击**监听**页签下的**添加监听**。
5. 配置协议与监听，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。 本操作，选择**HTTPS**。
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	设置监听的名称，用户自定义。
高级配置	
调度算法	负载均衡支持轮询、加权轮询（WRR）、加权最小连接数（WLC）和一致性哈希（CH）四种调度算法。 ○ **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。 ○ **加权最小连接数(WLC)**：除了根据每台后端服务器设定的权重值来进行轮询，同时还考虑后端服务器的实际负载（即连接数）。当权重值相同时，当前连接数越小的后端服务器被轮询到的次数（概率）也越高。 ○ **一致性哈希（CH）**： ■ **源IP**：基于源IP地址的一致性hash，相同的源地址会调度到相同的后端服务器。 ■ **四元组**：基于四元组的一致性hash（源IP、目的IP、源端口和目的端口），相同的流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。启用访问控制后，您可以通过配置访问控制策略来实现允许某些特定IP访问负载均衡，或禁止某些特定IP访问负载均衡的功能。
访问控制方式	开启访问控制后，选择一种访问控制方式： ○ **白名单**，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。 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，则负载均衡监听不会转发请求。 ○ **黑名单**，来自所选访问控制策略组中设置的IP地址或地址段的所有请求都不会转发。 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。
选择访问控制策略组	选择访问控制策略组，作为该监听的白名单或黑名单。 **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。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，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。
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：配置SSL证书

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

> **注意** 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

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。
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

证书	说明	单向认证是否需要	双向认证是否需要

在上传证书前，请注意：

- 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。
- 目前负载均衡HTTPS监听不支持SNI（Server Name Indication），您可以改用TCP监听在后端ECS上实现SNI功能。
- HTTPS监听的会话ticket保持时间设置为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. 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. 选择TLS安全策略，详情参见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 > 继续添加**。
2. 在**我的服务器**页面，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**页签下，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，该服务器不会再接受新请求。

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。单击**修改**更改健康检查配置，更多信息，请参见健康检查概述。

步骤五：提交配置

1. 在**配置审核**页面，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. 在**配置成功**页面，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

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。

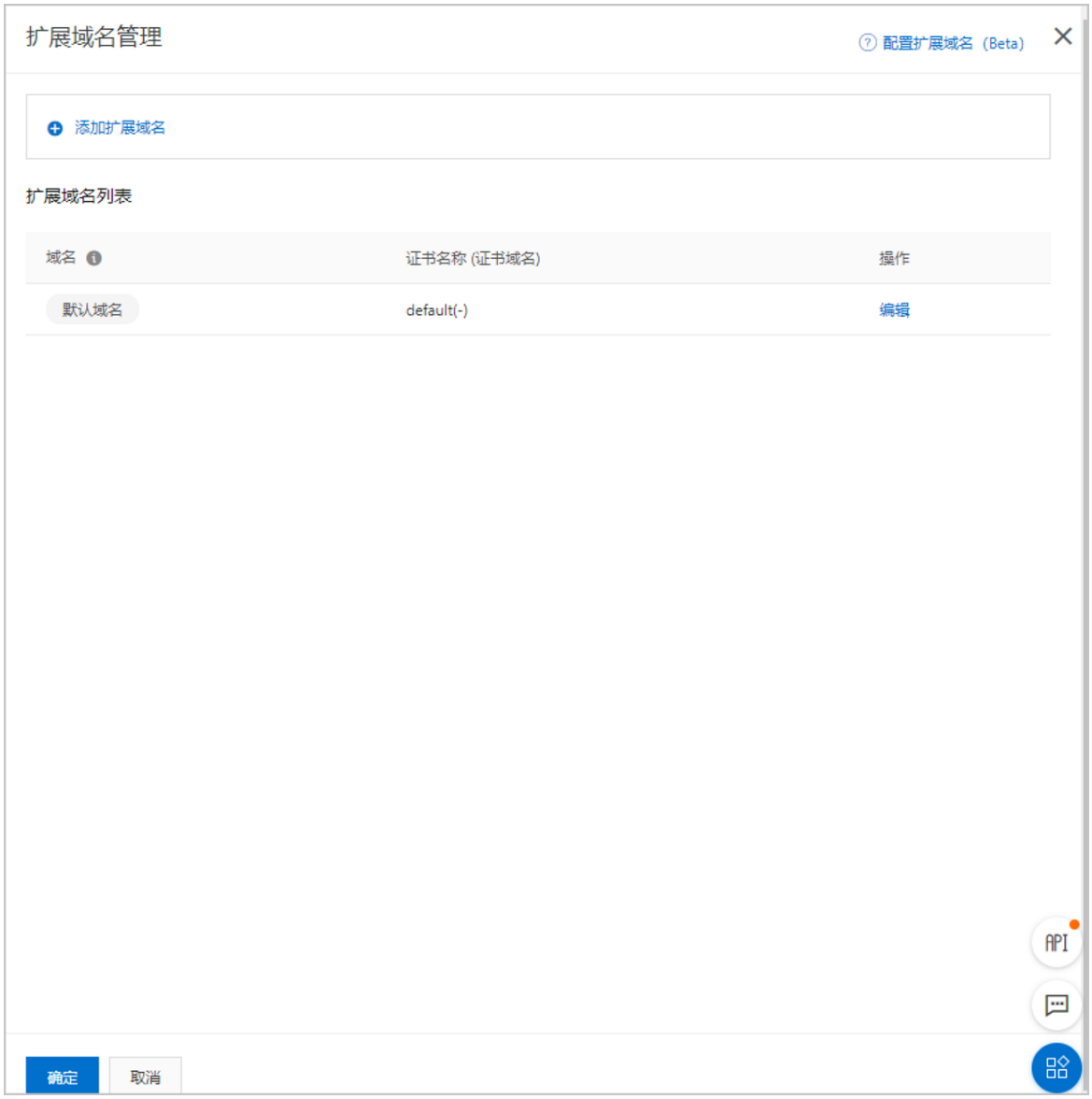
6.2. 添加扩展域名

本文介绍添加扩展域名的操作步骤。

操作步骤

1. 登录负载均衡管理控制台。
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，选择操作列下的 **> 扩展域名管理**。

5. 在**扩展域名管理**页面，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.aliyun.com	*.aliyun.com	*.market.aliyun.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。

6. （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**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**页面，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

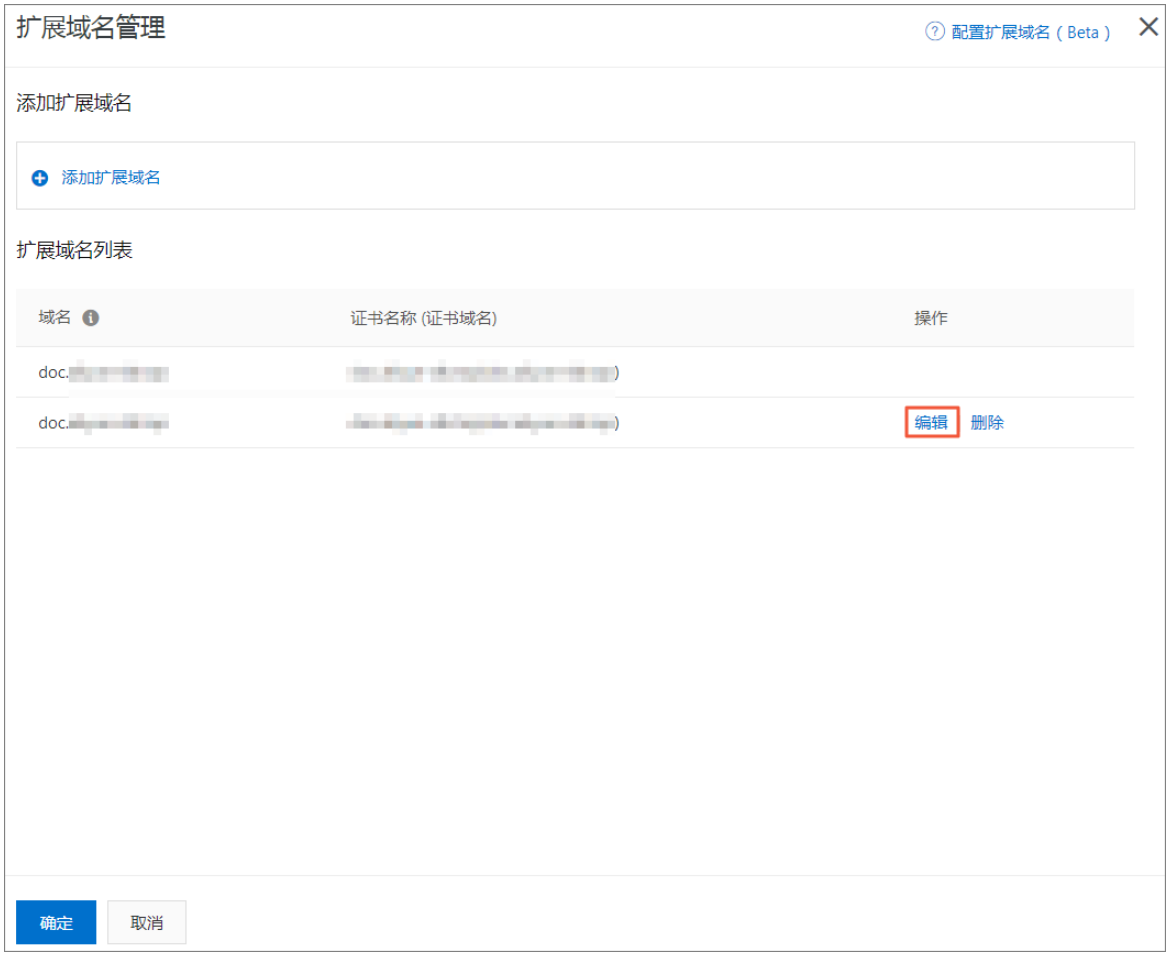
您可以替换已添加的扩展域名使用的证书。

操作步骤

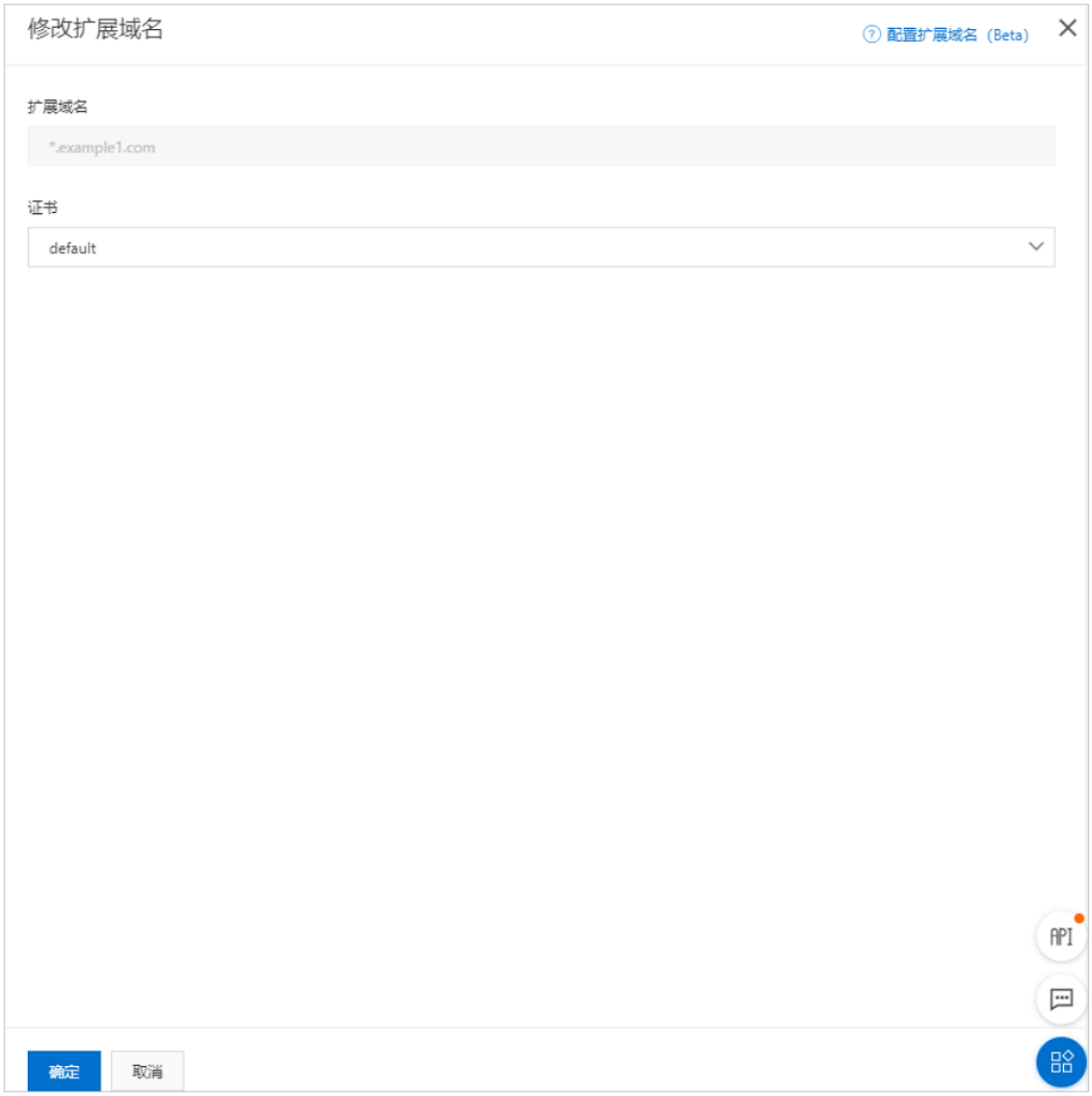
1. 登录负载均衡管理控制台。
2. 在左侧导航栏，选择**实例 > 实例管理**。

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，选择操作列下的 > **扩展域名管理**。

5. 找到目标扩展域名，然后单击操作列下的**编辑**。



6. 在**修改扩展域名**页面，选择新的证书，然后单击**确定**。

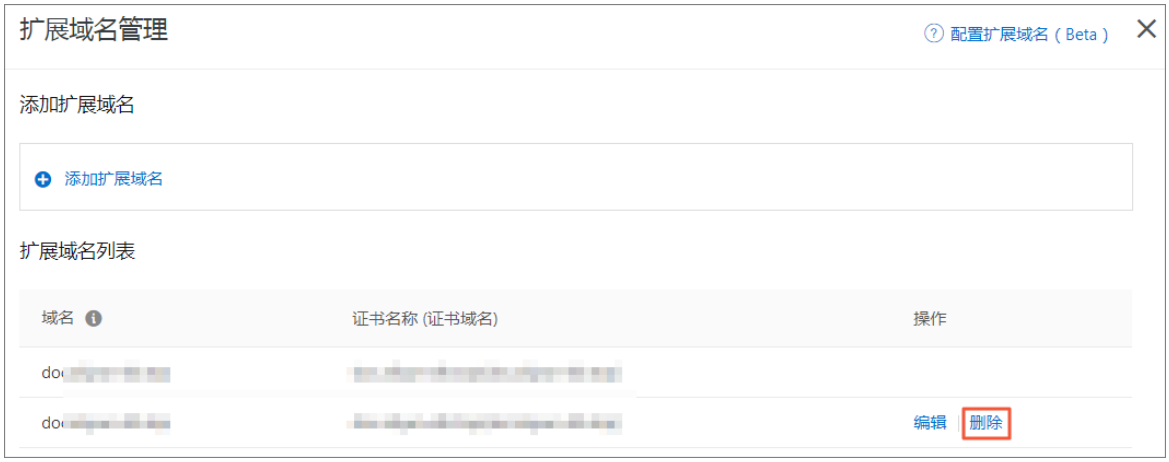


6.4. 删除扩展域名

当扩展域名不需要使用时，可以删除扩展域名。

操作步骤

1. 登录负载均衡管理控制台。
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**。

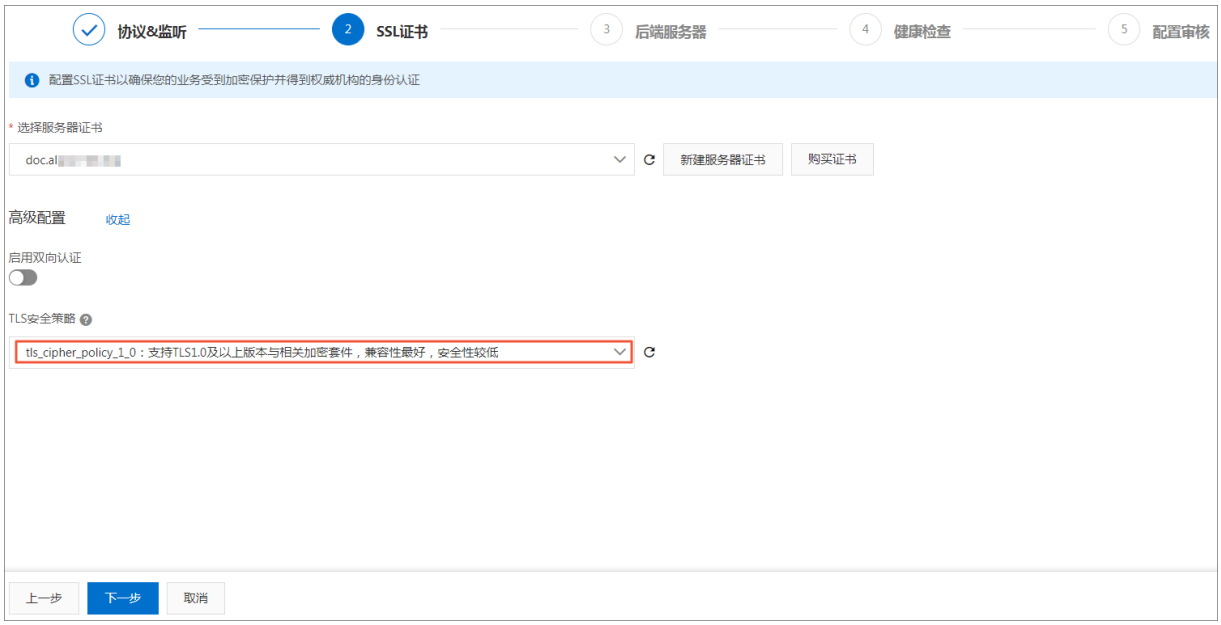


6. 在弹出的删除对话框中，单击**确定**。

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，支持选择使用的TLS安全策略。

您可以在添加或者配置HTTPS监听时，修改**SSL证书**高级配置，选择TLS安全策略，详细操作参见添加HTTPS监听。



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安全策略

安全策略	特点	支持TLS版本	支持加密算法套件
tls_cipher_policy_1_0	兼容性最好，安全性较低	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	特点	支持TLS版本	支持加密算法套件
tls_cipher_policy_1_1	兼容性较好，安全性较好	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	兼容性较好，安全性很高	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	仅支持前向安全的加密套件，安全性极高	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			

安全策略	特点	支持TLS版本	支持加密算法套件
说明 目前支持TLS1.3的地域如下： • 英国（伦敦） • 华北1（青岛） • 华北5（呼和浩特） • 西南1（成都） • 日本（东京） • 印度（孟买） • 澳大利亚（悉尼） • 马来西亚（吉隆坡） • 美国（硅谷） • 美国（弗吉利亚） • 德国（法兰克福） • 阿联酋（迪拜）	仅支持前向安全的加密套件，安全性极高	TLS1.2及TLS1.3	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安全策略差异说明

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	-	1.2/1.1/1.0	1.2/1.1	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	-	-	-	-	✔

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。

在创建监听时，您可以设置带宽峰值也可以选择不设置。

- 配置：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。
- 不限制：不限制带宽的情况下，实例下的监听共享实例带宽。

如何共享带宽？

假如您购买了一个带宽峰值为10 MB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 MB，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一直没有出流量，那么监听B最多也只能跑满剩余的6 MB带宽（10 MB-4 MB)。
- 如果监听C一直没有出流量，而监听B的出流量很大，超过了剩余的6 MB带宽。此时，监听B已经产生丢包，而监听A只有4 MB的出流量，没有超过设置的带宽峰值，所以不会产生丢包。
- 如果监听A一直是满速在跑（监听峰值4 MB），而后监听B和监听C也有出流量并且两个监听的流量很大，那么监听B和监听C就会共享（竞争）剩余的6 MB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 MB峰值；如果监听B和监听C出流量同等大小，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。负载均衡支持将HTTP访问重定向至HTTPS，方便您进行全站HTTPS部署。负载均衡已经在全部地域开放了HTTP重定向功能，并在英国（伦敦）地域支持自定义重定向使用的状态码。

前提条件

确保您已创建了HTTPS监听。详情请参见添加HTTPS监听。

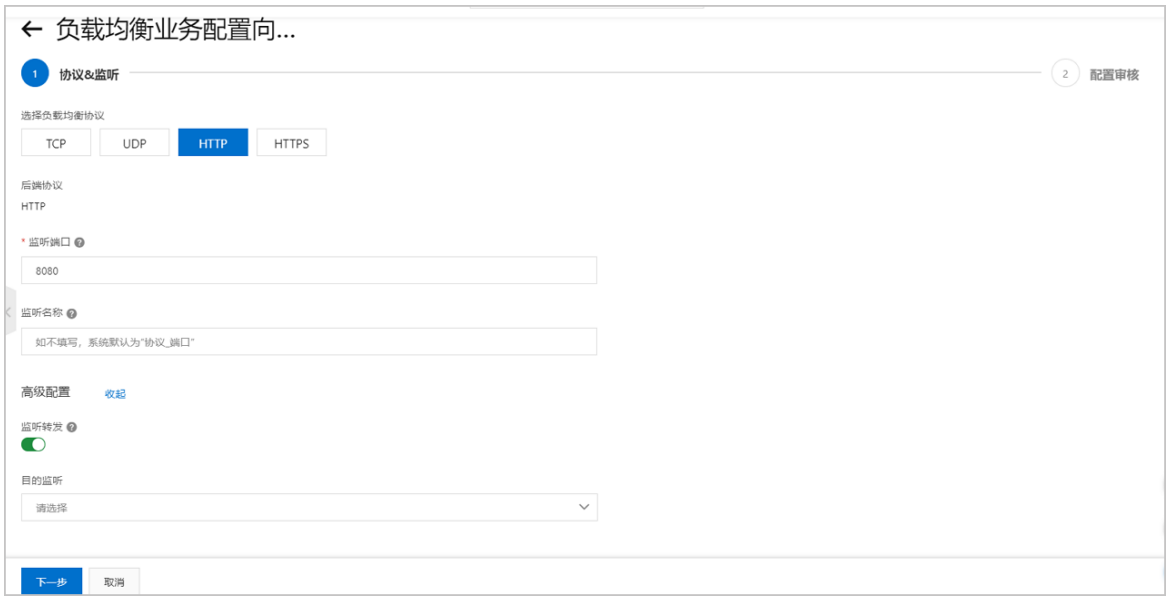
背景信息

仅负载均衡新版控制台在创建HTTP监听时支持配置监听转发。

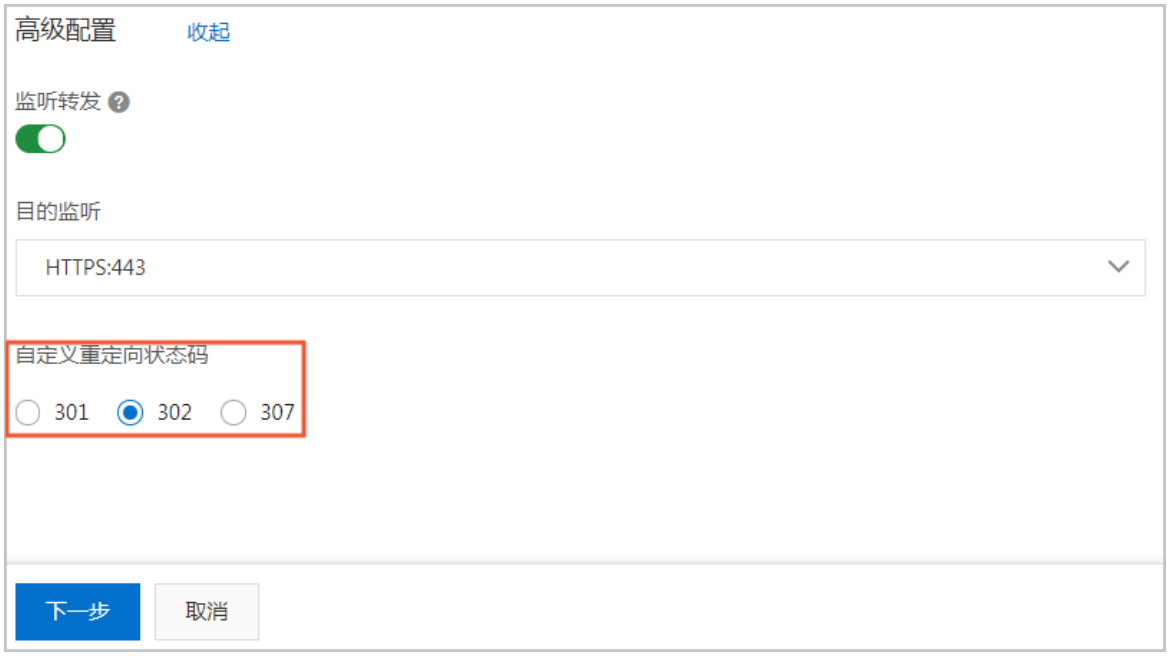
操作步骤

1. 登录负载均衡管理控制台。
2. 在左侧导航栏，选择**实例 > 实例管理**。
3. 在**实例管理**页面，单击目标实例的ID链接。
4. 在**监听**页签下，单击**添加监听**。
5. 在**协议&监听**对话框，负载均衡协议选择**HTTP**，配置监听端口。
6. 在**高级配置**区域下，打开**监听转发**开关，选择目的监听。

   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）地域支持配置重定向跳转使用的状态码。



7. 单击**下一步**。
8. 确认后，单击**提交**。
9. 单击**知道了**。

转发开启后，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。

10.FAQ

10.1. 负载均衡服务FAQ

包含以下问题：

1. 负载均衡是否支持端口跳转？

支持。

详情参见配置监听转发（redirect）。

2. 禁用公网网卡是否影响负载均衡服务？

如果ECS有公网IP，禁用公网网卡就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，如禁用就无法回包从而影响负载均衡服务。建议不要禁止，如一定要这么做，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。

3. 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10Mb带宽上限，那么单个客户端可下载的最大流量为10/(4-1)=3.33Mb。

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。

4. 负载均衡各监听连接超时时间是多少？

- TCP监听： 900秒
- UDP监听： 90秒
- HTTP监听： 60秒
- HTTPS监听： 60秒

5. 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链接访问超时：

- 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900s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。

6. 为什么有时候会话保持失败？

- 查看是否在监听配置中已经开启了会话保持功能。
- HTTP/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。

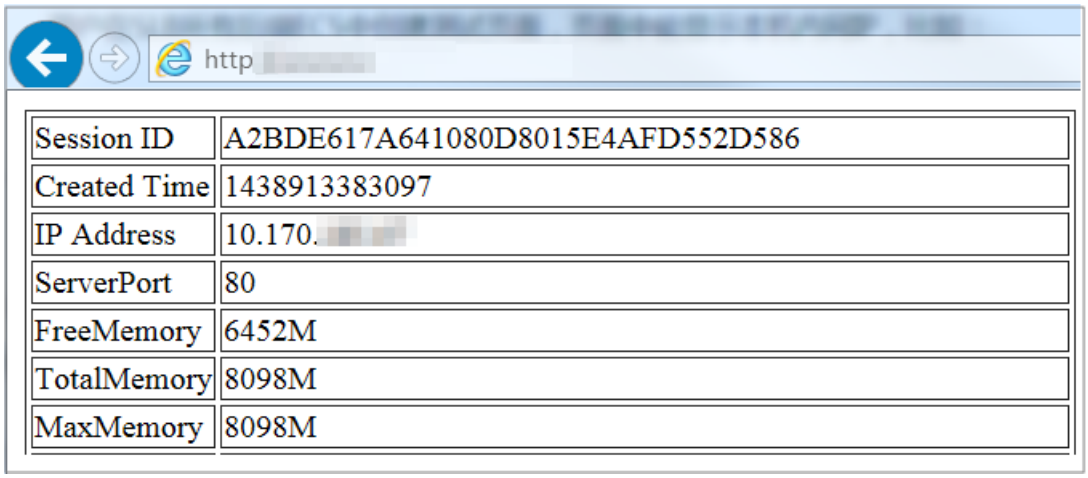
7. 如何查看会话保持字串？

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

8. 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下curl测试。

   假设负载均衡服务IP地址是 1.1.1.1，创建的测试页面URL为： http://1.1.1.1/check.jsp

   i. 登录用来测试的Linux服务器。

   ii. 执行以下命令负载均衡服务器cookie值。

   ```
   curl -c test.cookie http://1.1.1.1/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测试默认是不会保存和发送cookie的。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++)); 2="" do="" curl="" -b="" 1.cookie=""
         check.jsp="">/dev/null | grep '10.170.*';sleep 1; done`
   ```

   > **说明** a<=30是重复测试次数，可以按需修改；grep '10.170.*' 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。

9. 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。

10.2. 七层监听（HTTPS/HTTP）FAQ

本文包含以下常见问题：

1. 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。

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

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。

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。

3. 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。

4. 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。

5. 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。

6. 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。

7. 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。

8. 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。

9. 负载均衡HTTPS支持哪些SSL协议版本？

TLSv1、TLSv1.1以及TLSv1.2版本。

10. HTTPS session ticket的保持时间是多久？

HTTPS session ticket保持时间为300秒。

11. 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。

12. 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。

13. HTTP/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HTTP2/0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HTTP2/0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。

14 后端服务器能否获取客户端访问HTTP/HTTPS监听的协议版本？

可以。

15. HTTP/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/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。