ALIBABA CLOUD

Alibaba Cloud

负载均衡
教程专区

文档版本：20220309

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.ALB教程

1.1. 配置全链路HTTPS访问实现加密通信

本文介绍如何使用

ALB

配置全链路HTTPS加密通信。

应用场景

随着企业的业务大量上云，云上承载业务的安全性变得越来越重要，尤其在金融、政府等行业，为了保障业务的安全性，往往会存在全链路加密的要求。这就要求负载均衡在提供服务的时候，不仅要保障前端（客户端到负载均衡）通信的安全，还要保障后端（负载均衡到业务服务器）通信的安全。

ALB

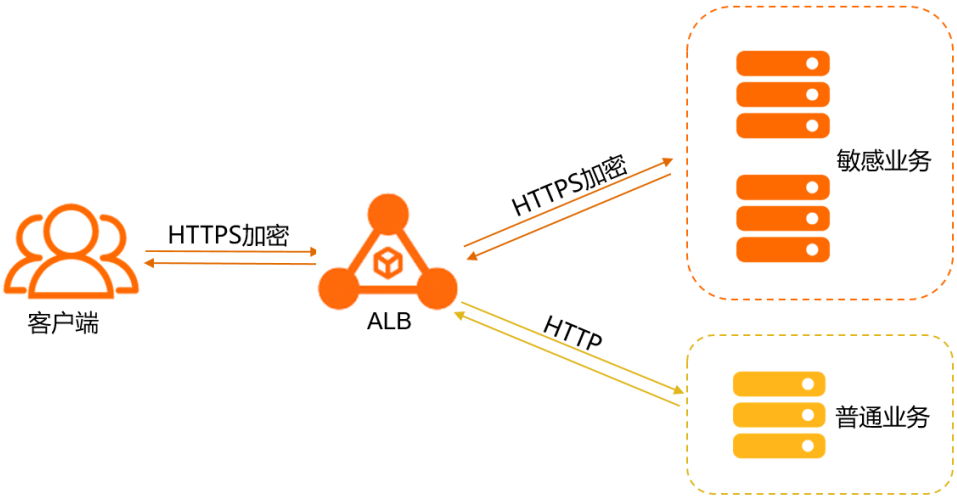
提供全链路HTTPS加密功能，可以实现客户端到

ALB

、

ALB

到后端服务器之间的全链路加密通信，提升敏感业务的安全性。



配置全链路HTTPS访问

1. 登录应用型负载均衡ALB控制台。
2. 在顶部菜单栏，选择

   ALB

   实例的所属地域。
3. 在左侧导航栏，选择**应用型负载均衡ALB > 服务器组**。
4. 完成以下配置，然后单击**创建**。
   - **VPC**：选择

     ALB

实例所在的VPC。

- **选择后端协议**：选择**HTTPS**。
- 更多参数说明，请参见管理服务器组中的创建服务器组。

5. 在**服务器组创建成功**对话框，单击**添加后端服务器**。或者在**服务器组**页面，找到刚创建的服务器组，然后在**操作**列单击**编辑后端服务器**。
6. 在**后端服务器**页签，单击**添加后端服务器**。
7. 在**添加后端服务器**面板，选择后端服务器类型，选中目标服务器，然后单击**下一步**。
8. 设置服务器的端口为**443**及权重，然后单击**确定**。
9. 创建HTTPS监听，具体操作，请参见添加HTTPS监听。

> **说明** 在**选择服务器组**配置向导中，您需要选择刚创建的后端服务器组。

1.2. Nginx服务配置多个HTTPS域名

本文主要介绍如何给

应用型负载均衡ALB

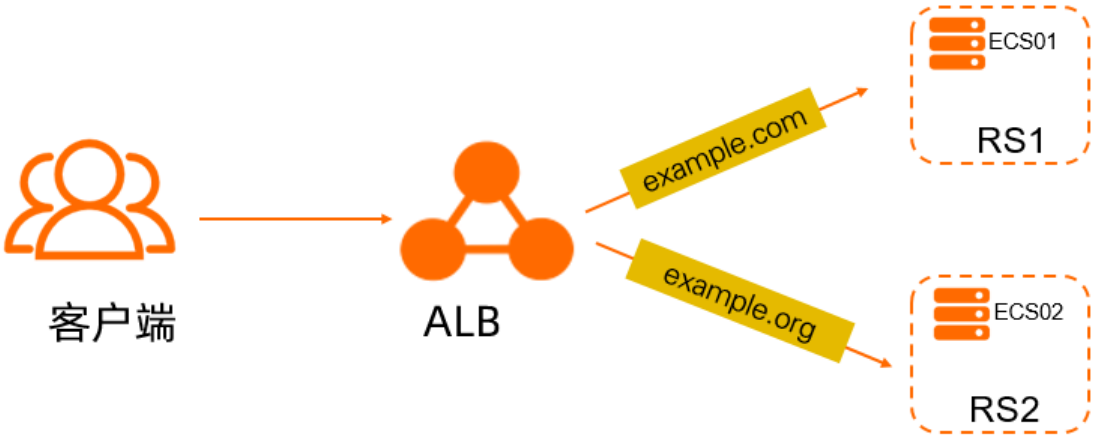
实例的HTTPS监听挂载多个证书，将不同的域名访问请求转发至不同的后端服务器的Nginx服务。

场景示例

ALB

会根据客户端请求的HTTPS域名去查找证书，如果找到域名对应的证书，则返回该证书完成HTTPS认证，并根据转发规则转发到对应后端服务器；如果没有找到域名对应的证书，则返回默认证书完成HTTPS认证，并根据转发规则转发到默认后端服务器。本文配置如下：

- 监听默认证书选择default，监听默认服务器组选择RS1。
- 扩展证书example1绑定域名`example.com`，域名为`example.com`的客户端请求转发至默认后端服务器组RS1。
- 扩展证书example2绑定域名`example.org`，域名为`example.org`的客户端请求转发至后端服务器组RS2。



前提条件

- 已创建

  ALB

  实例。具体操作，请参见创建应用型负载均衡。
- 已创建服务器组RS1和RS2。具体操作，请参见管理服务器组。
- 已在服务器组RS1和RS2中分别添加ECS01和ECS02实例，并在ECS01和ECS02中部署了不同的Nginx服务。
- 已购买证书或者上传第三方证书到SSL证书服务，并绑定域名。关于创建证书，请参见提交证书申请。本文需要以下证书：
  - 默认证书default。
  - 已绑定域名 `example.com` 的扩展证书example1。
  - 已绑定域名 `example.org` 的扩展证书example2。

背景信息

一个

ALB

实例可添加的扩展证书数量（不包含监听默认证书）基础版实例为10个，标准版实例为25个。

步骤一：添加HTTPS监听

1. 登录应用型负载均衡ALB控制台。
2. 在顶部菜单栏，选择

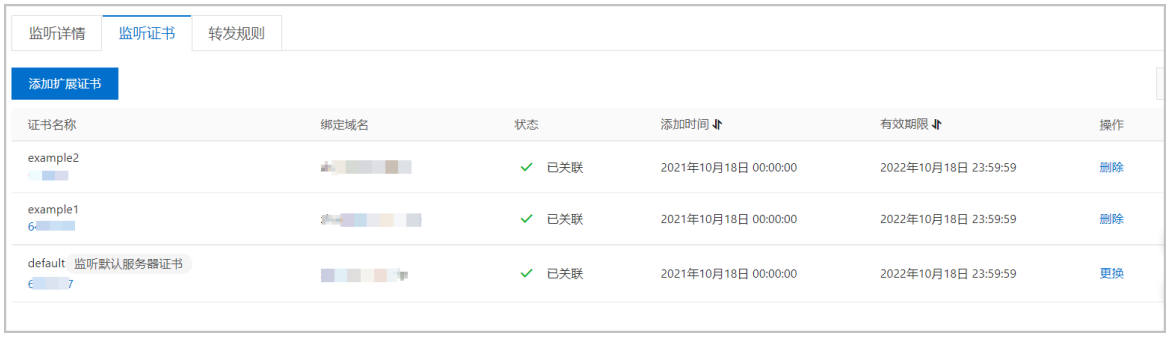
   ALB

   实例所属的地域。
3. 在**实例**页面，找到目标实例，然后在**操作**列单击**创建监听**。
4. 在**配置监听**页面，根据以下信息配置监听，然后单击**下一步**。

   本文主要配置如下，关于其他配置参数及具体操作步骤，请参见添加HTTPS监听。
   - **选择服务器证书**：default。
   - **选择服务器组**：RS1。

步骤二：添加扩展证书

1. 在**实例**页面，找到目标实例，单击实例ID。
2. 在**监听**页签，找到已创建的HTTPS监听，然后在**操作**列单击**管理证书**。
3. 在**监听证书**页签，单击**添加扩展证书**。
4. 在**添加扩展证书**对话框，选择证书example1，然后单击**确定**。继续重复此步骤添加扩展证书example2。



步骤三：配置转发规则

1. 在**实例**页面，找到目标实例，单击实例ID。
2. 在**监听**页签，找到已创建的HTTPS监听，然后在**操作**列单击**查看/编辑转发规则**。
3. 在**转发规则**页签，单击**插入新规则**。
4. 配置转发规则，然后单击**确定**。
   - 如果**域名**是`example.com`，那么**转发至**RS1，**权重**：100。
   - 如果**域名**是`example.org`，那么**转发至**RS2，**权重**：100。

> **说明**
>
> - 权重越大ECS实例将被分配到更多的访问请求，本文配置为默认值100。
> - 权重取值范围为：1~100。

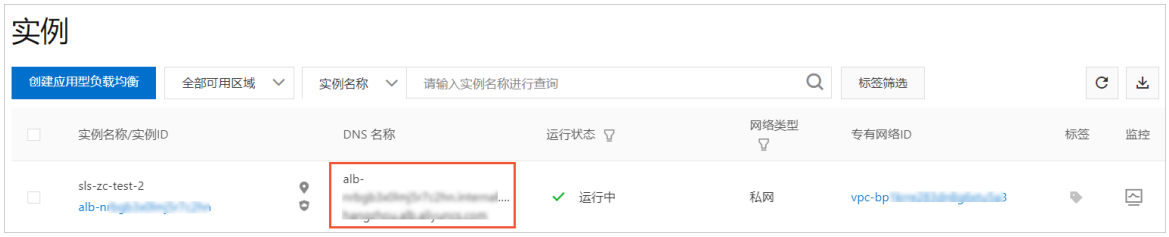
步骤四：配置域名解析

将`example.com`和`example.org`通过CNAME域名解析的方式解析到ALB实例的公网服务域名上。

1. 登录应用型负载均衡ALB控制台。
2. 在顶部菜单栏选择地域。
3. 选择要进行域名解析的

   ALB

   实例，复制其对应的DNS名称。



4. 完成以下步骤来添加CNAME解析记录。
   i. 登录域名解析控制台。
   ii. 在**域名解析**页面单击**添加域名**。
   iii. 在**添加域名**对话框中输入您的主机域名，然后单击**确定**。

> **注意** 您的主机域名需已完成TXT记录验证。

   iv. 在目标域名的**操作**列单击**解析设置**。
   v. 在**解析设置**页面单击**添加记录**。
   vi. 在**添加记录**面板配置以下信息完成CNAME解析配置，然后单击**确认**。

配置	说明
记录类型	在下拉列表中选择**CNAME**。
主机记录	您的域名的前缀。
解析线路	选择默认。
记录值	输入加速域名对应的CNAME地址，即您复制的 ALB 实例的DNS名称。
TTL	全称Time To Live，表示DNS记录在DNS服务器上的缓存时间，本文使用默认值。

> **说明**
>
> - 新增CNAME记录实时生效，修改CNAME记录取决于本地DNS缓存的解析记录的TTL到期时间，一般默认为10分钟。
> - 添加时如遇添加冲突，请换一个解析域名。

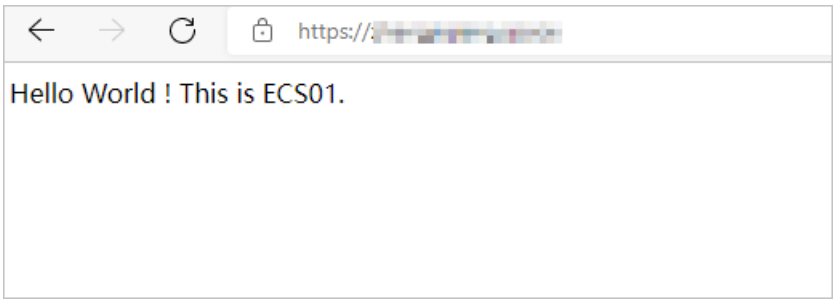
步骤五：结果验证

在浏览器中分别输入 `example.com` 和 `example.org` 均可访问到

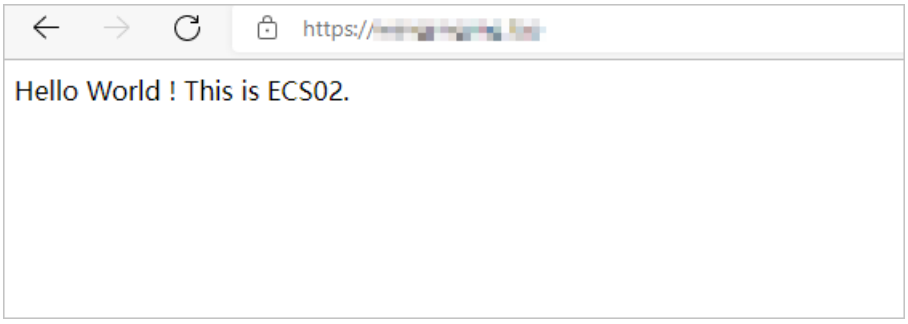
ALB

，本文在服务器组RS1和RS2对应的后端服务器ECS01和ECS02两个实例上使用Nginx服务搭建了两个静态网页。

- 在浏览器中输入扩展证书example1绑定域名 `example.com` ，将根据已配置的转发规则，转发至服务器组RS1对应的后端服务器ECS01。如下图所示：



- 在浏览器中输入扩展证书example2绑定域名 `example.org` ，将根据已配置的转发规则，转发至服务器组RS2对应的后端服务器ECS02。如下图所示：



1.3. 使用ALB将HTTP访问重定向至HTTPS

HTTPS是加密数据传输协议，安全性高。当企业进行HTTPS安全改造后，为了方便用户访问，可以使用

ALB

在用户无感知的情况下将普通HTTP访问重定向至HTTPS。

前提条件

- 已创建了HTTP监听。具体操作，请参见添加HTTP监听。
- 已创建了HTTPS监听。具体操作，请参见添加HTTPS监听。

设置HTTP重定向至HTTPS

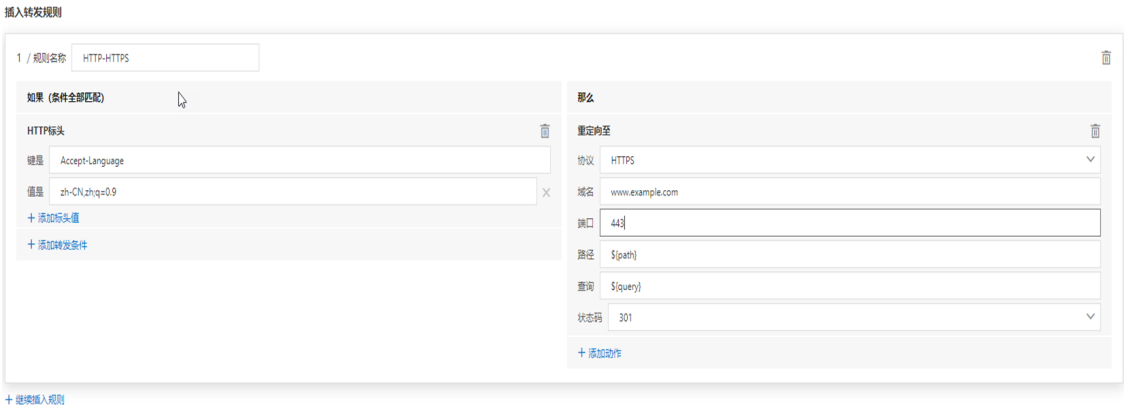
1. 登录应用型负载均衡ALB控制台。
2. 在顶部菜单栏，选择

   ALB

   实例的所属地域。
3. 在**实例**页面，单击目标实例ID。
4. 在**监听**页签，找到已创建的HTTP监听，然后在**操作**列单击**查看/编辑转发规则**。

5. 在**转发规则 > 请求方向转发规则**页签，单击**插入新规则**。
6. 在**插入新规则**区域，根据您的实际情况配置转发规则。

   本教程将Accept-Language为中文的访问重定向至https://www.example.com。



   转发动作：选择**重定向至**。

   - **协议**：选择**HTTPS**。
   - **端口**：输入您已创建的HTTPS协议监听端口。

   更多参数说明，请参见管理监听转发规则。

7. 单击**确定**，后续访问

   ALB

   域名且Accept-Language是中文的请求都会跳转到https://www.example.com。

1.4. 使用ALB流量镜像功能实现仿真压测

本文介绍如何使用

ALB

流量镜像功能仿真在线流量。

应用场景

很多企业的线上业务对安全性和稳定性有着极高的要求，在新功能发布前的测试中，为了不影响线上业务，不能直接在线上环境测试，但同时需要在测试环境中模拟在线流量对新功能进行测试。

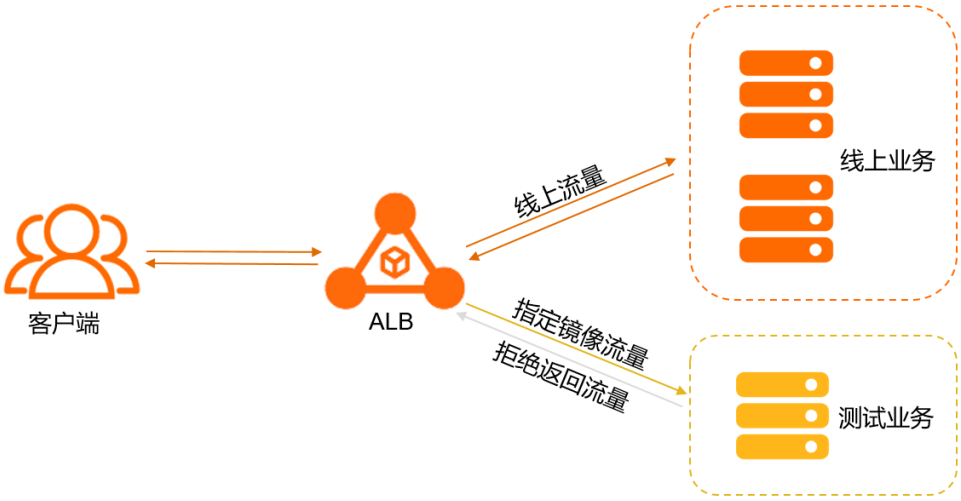
ALB

提供的流量镜像功能可以实现在线流量仿真，将在线流量镜像到测试环境的后端服务器，同时

ALB

自动丢弃镜像后端服务器返回的响应数据，保证镜像后端服务器的测试业务不会影响到线上业务，主要有以下应用场景：

- 测试新功能和服务性能。
- 仿真线上数据，不需要额外制造测试数据。
- 复现线上问题，方便故障定位。



限制说明

- 目前流量镜像功能白名单开放，如需体验请提交工单。
- 公网

  ALB

  和私网

  ALB

  都支持流量镜像功能。
- ALB

  实例包含基础版和标准版，仅标准版

  ALB

  实例支持流量镜像功能。

前提条件

- 已创建线上业务服务器组和测试业务服务器组，且后端协议均设置为HTTP。具体操作，请参见管理服务器组。
- 已创建监听。具体操作，请参见添加HTTP监听、添加HTTPS监听或添加QUIC监听。

通过流量镜像实现在线流量仿真

1. 登录应用型负载均衡ALB控制台。
2. 在顶部菜单栏，选择

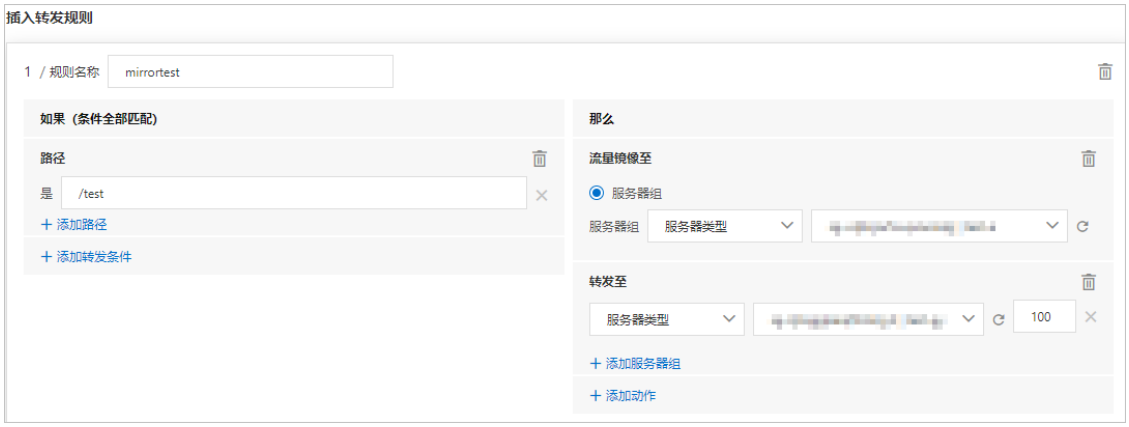
   ALB

   实例的所属地域。
3. 在**实例**页面，单击目标实例ID。
4. 在**监听**页签，找到目标监听，然后在**操作**列单击**查看/编辑转发规则**。
5. 在**转发规则 > 请求方向转发规则**页签，单击**插入新规则**。
6. 在**插入转发规则**区域，根据您的实际情况配置转发规则。

   本文以将**路径**为**/test**的流量镜像至测试业务服务器为例。

转发动作：选择**流量镜像至**测试业务服务器组和**转发至**正常业务服务器组。

> 注意 由于
>
> ALB
>
> 会丢弃测试业务服务器组返回的响应数据，所以本条转发规则内一定要添加**转发至**正常业务服务器组的动作，以免影响线上业务。



7. 单击**确定**，设置的指定流量将镜像至测试业务服务器组。

相关文档

管理监听转发规则

1.5. 使用ALB实现灰度发布

灰度发布（又称为金丝雀发布）是一种平滑过渡的发布方式，将老版本应用与新版本应用同时部署在环境中，让一部分用户继续使用老版本应用，一部分用户开始使用新版本应用，然后根据用户使用情况调整新版本流量占比，逐步把所有用户都迁移到新版本应用。

应用场景

互联网产品需要快速迭代开发上线，同时又要保证质量。为保证刚上线的系统出现问题后可以很快控制影响，需要设计一套灰度发布系统，按照发布策略选取部分用户流量，先行使用新版本应用，然后通过收集这部分用户对新版本应用的反馈，以及新版本应用的日志、性能、稳定性等指标来评审新版应用。根据评审情况，决定是否继续增加新版本的应用实例和流量，直至全量升级，或者发现问题后及时回滚到老版本。

准备工作

1. 将您的老版本业务和新版本业务分别部署在不同的服务器，为了增加业务处理能力，请分别部署在多台服务器上。
2. 创建ALB实例，基础版

   ALB

   实例不支持条件类型为Cookie的规则，需要创建标准版

   ALB

   实例。具体操作，请参见创建应用型负载均衡。
3. 创建服务器组，将承载老版本应用和新版本应用的服务器组分别加入不同的服务器组。具体操作，请参见管理服务器组。

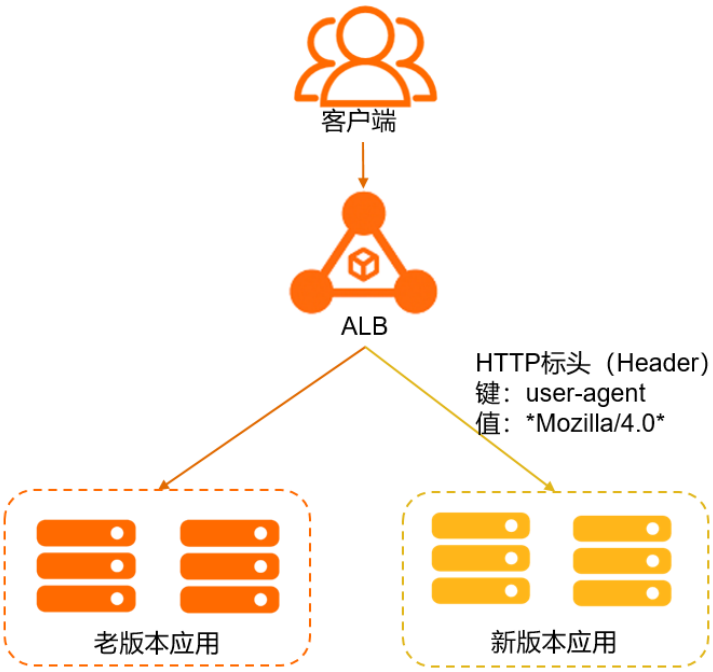
4. 创建监听，并将监听默认服务器组设置为老版本应用服务器组。具体操作，请参见添加HTTP监听、添加HTTPS监听或添加QUIC监听。

   此时用户请求将全部转发至老版本应用。本文提供以下三种不同的灰度方式，您可以根据需要选择一种或多种搭配使用。

   - 基于HTTP标头实现灰度发布
   - 基于Cookie实现灰度发布
   - 基于不同服务器组实现灰度发布

基于HTTP标头实现灰度发布

本示例将用户请求中HTTP标头键是user-agent、值是*Mozilla/4.0*的访问转发至新版本应用。



1. 登录应用型负载均衡ALB控制台。
2. 在顶部菜单栏，选择

   ALB

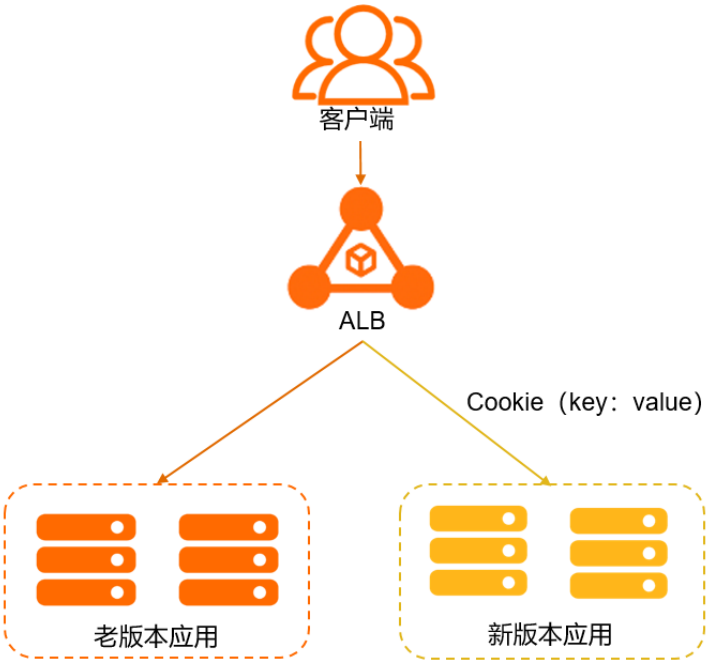
   实例所属的地域。
3. 在**实例**页面，单击目标实例ID。
4. 在**监听**页签，找到目标监听，然后在**操作**列单击**查看/编辑转发规则**。
5. 在**转发规则**页签，单击**插入新规则**。
6. 配置转发规则，然后单击**确定**。
   - 转发条件：在下拉列表中选择**HTTP标头**，然后将键设置为*user-agent*，值设置为**Mozilla/4.0**。
   - 转发动作：在下拉列表中选择**转发至**，然后选择新版本应用对应的服务器。

   更多参数说明，请参见管理监听转发规则。

   > **说明** 您可以根据需要增加转发条件来增加新版本应用的流量，待运行一段时间稳定后，将所有的流量从老版本应用切换到新版本应用中，平滑地将老版本应用下线。

基于Cookie实现灰度发布

本示例将用户请求中Cookie为key:value的访问转发至新版本应用。



1. 登录应用型负载均衡ALB控制台。
2. 在顶部菜单栏，选择

   ALB

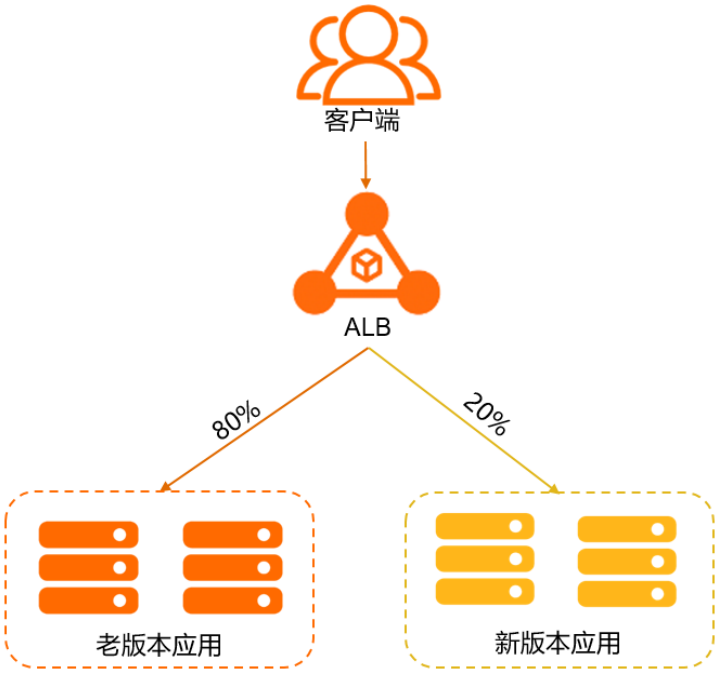
   实例所属的地域。
3. 在**实例**页面，单击目标实例ID。
4. 在**监听**页签，找到目标监听，然后在**操作**列单击**查看/编辑转发规则**。
5. 在**转发规则**页签，单击**插入新规则**。
6. 配置转发规则，然后单击**确定**。
   - 转发条件：在下拉列表中选择**Cookie**，然后设置为*key*:*value*。
   - 转发动作：在下拉列表中选择**转发至**，然后选择新版本应用的服务器。

   更多参数说明，请参见管理监听转发规则。

> **说明** 您可以根据需要增加转发条件来增加新版本应用的流量，待运行一段时间稳定后，将所有的流量从老版本应用切换到新版本应用中，平滑地将老版本应用下线。

基于不同服务器组实现灰度发布

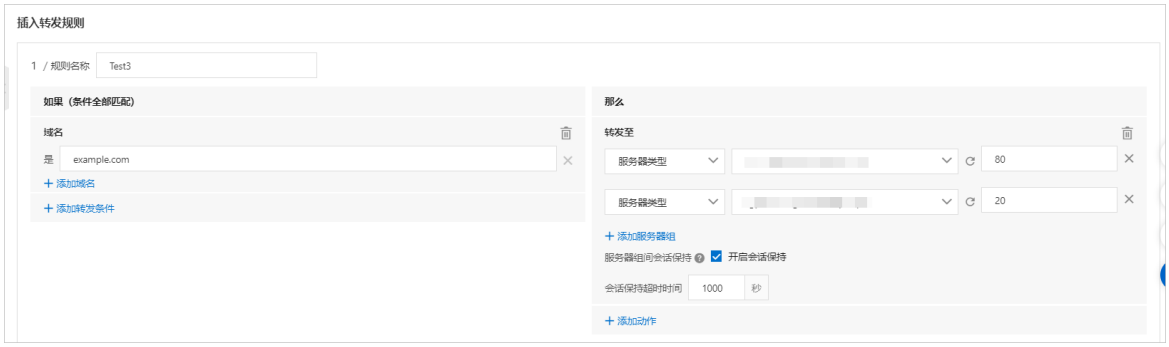
本示例将域名为*example.com*的访问分别转发至老版本应用和新版本应用，且老版本应用和新版本应用接收的请求比重分别为80%和20%。



1. 登录应用型负载均衡ALB控制台。
2. 在顶部菜单栏，选择

   ALB

   实例所属的地域。
3. 在**实例**页面，单击目标实例ID。
4. 在**监听**页签，找到目标监听，然后在**操作**列单击**查看/编辑转发规则**。
5. 在**转发规则**页签，单击**插入新规则**。
6. 配置转发规则，然后单击**确定**。



   - 转发条件：在下拉列表中选择**域名**，然后将域名设置为*example.com*。
   - 转发动作：在下拉列表中选择**转发至**，然后选择老版本应用服务器组（权重80）和新版本应用服务器组（权重20）。

   更多参数说明，请参见管理监听转发规则。

> **说明** 您可以根据需要调整服务器组权重来增加新版本应用的流量占比，待运行一段时间稳定后，将所有的流量从老版本应用切换到新版本应用中，平滑地将老版本应用下线。

1.6. 使用QUIC协议提升音视频业务访问速度

QUIC（Quick UDP Internet Connections）协议能帮助您大幅提升客户端访问速度，尤其是在弱网络、Wi-Fi和移动网络频繁切换等场景下，无需重连即可实现多路复用，提升资源的访问效率，同时保障数据传输的安全性。

背景信息

QUIC协议又被称为快速UDP互联网连接协议，提供与SSL相同的安全性，同时具备多路复用、0-RTT握手等多种优势，具有极佳的弱网性能，在丢包和网络延迟严重的情况下仍可提供可用的服务。QUIC协议在应用程序层面可以实现不同的拥塞控制算法，不需要操作系统和内核支持，相比于传统的TCP协议，拥有了更好的改造灵活性，适合用于在TCP协议优化遇到瓶颈的业务。

随着短视频、直播等新兴业务的飞速发展，流媒体传输对于带宽和延迟提供了双重要求，QUIC协议可以有效解决网络、视频卡顿的问题，提升音视频资源的访问效率，同时保障数据传输的安全性。目前，阿里云

应用型负载均衡ALB

支持的QUIC协议版本有：Q46、Q44、Q43、Q39、Q36和Q35。

场景示例

使用Chrome浏览器访问

ALB

实例时，

ALB

会根据配置的监听所绑定的证书域名`example.com`访问后端服务器。主要有以下两种应用场景：

- 当同时配置了HTTPS监听和QUIC监听时，系统会优先使用QUIC监听，此时在Chrome浏览器中输入证书绑定的域名`example.com`，

  ALB

  实例将会通过配置的QUIC监听将客户端的请求转发至默认后端服务器组RS1。
- 当QUIC监听不可用时，系统会自动切换到关联的HTTPS监听，此时在Chrome浏览器中输入证书绑定的域名`example.com`，

  ALB

  实例将会通过配置的HTTPS监听将客户端的请求转发至默认后端服务器组RS1。

客户端要求

- 如果您使用Chrome浏览器，支持直接对

  ALB

  发起QUIC协议请求。
- 如果您使用其他客户端，则客户端必须集成支持QUIC协议的网络库，例如：lsquic-client或cronet网络库。
- 使用Chrome浏览器访问QUIC，需要使用指定的Chrome浏览器版本：
  - ALB

    支持的QUIC协议最高版本是Q46，对应的Chrome浏览器版本为Chrome 74-81。

- 对于更高版本的Chrome浏览器，已经默认使用Q50及以上版本，如果需要访问

  ALB

  ，则需要降级Chrome版本。

前提条件

- 已创建

  ALB

  实例。具体操作，请参见创建应用型负载均衡。
- 已创建服务器组RS1。具体操作，请参见管理服务器组。
- 已在服务器组RS1中添加ECS01实例，并在ECS01实例中部署了Nginx的视频服务。
- 您已经在

  ALB

  实例上部署了SSL服务器证书，该证书已绑定了域名 `example.com` 。

步骤一：创建QUIC监听

1. 登录应用型负载均衡ALB控制台。
2. 在顶部菜单栏，选择

   ALB

   实例所属的地域。
3. 在**实例**页面，找到目标实例，单击目标实例ID。在**监听**页签，单击**创建监听**。
4. 在**配置监听**配置向导，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。 本示例选择QUIC。
监听端口	输入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** 在同一个负载均衡实例内，监听端口不可重复。
监听名称	输入监听名称，自定义。
高级配置	单击**修改**展开高级配置。
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。

监听配置	说明
Gzip数据压缩	开启该配置对特定文件类型进行压缩。 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 header字段： ○ 通过`SLB-ID`头字段获取负载均衡实例的ID。 ○ 通过`X-Forwarded-Proto`头字段获取负载均衡实例的监听协议。 ○ 通过`X-Forwarded-Port`头字段获取负载均衡实例的监听端口。

5. 在**配置SSL证书**配置向导，选择服务器证书，然后单击**下一步**。
6. 在**选择服务器组**配置向导，选择**服务器类型**，然后选择服务器组。查看后端服务器信息，然后单击**下一步**。
7. 在**配置审核**配置向导，确认配置信息，单击**提交**。

步骤二：创建HTTPS监听

创建HTTPS监听时，请开启QUIC升级，并关联已创建的QUIC监听。

1. 在**实例**页面，找到在步骤一中创建了QUIC监听的实例，单击该实例ID。
2. 在**监听**页签，单击**创建监听**。
3. 在**配置监听**配置向导，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。 本示例选择**HTTPS**。
监听端口	输入用来接收请求并向后端服务器进行请求转发的监听端口，本示例输入**443**。通常HTTP协议使用80端口，HTTPS协议使用443端口。 端口范围为1~65535。 **说明** 在同一个负载均衡实例内，监听端口不可重复。
监听名称	输入监听名称。长度为2~256个字符，必须是无害字符串以及中文。
高级配置	单击**修改**展开高级配置。
启用HTTP 2.0	选择是否开启HTTP 2.0。

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。 **说明** 该功能对使用HTTP 2.0的请求暂不生效。
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。
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，Brotli支持压缩所有类型，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`头字段获取来访者真实IP。 ○ 添加`SLB-ID`头字段获取负载均衡实例的ID。 ○ 添加`X-Forwarded-Proto`头字段获取实例的监听协议。 ○ 添加`X-Forwarded-Clientcert-subjectdn`头字段获取访问负载均衡实例客户端证书的所有者信息。 ○ 添加`X-Forwarded-Clientcert-issuerdn`头字段获取访问负载均衡实例客户端证书的所发行者信息。 ○ 添加`X-Forwarded-Clientcert-fingerprint`头字段获取访问负载均衡实例客户端证书的指纹取值。 ○ 添加`X-Forwarded-Clientcert-clientverify`头字段获取访问负载均衡实例客户端证书的校验结果。 ○ 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-Port`头字段获取访问负载均衡实例客户端的端口。
开启QUIC升级	选择是否开启QUIC升级，如果开启QUIC升级，请选择一个关联的QUIC监听。
WAF安全防护	选择是否为监听开启WAF安全防护。

4. 在**配置SSL证书**配置向导，选择服务器证书，然后单击**下一步**。

> 说明 如果您要设置TLS安全策略，单击**高级配置**后的**修改**。

5. 在**选择服务器组**配置向导，选择**服务器类型**，然后选择服务器组，查看后端服务器信息，然后单击**下一步**。
6. 在**配置审核**页面，确认配置信息，单击**提交**。

步骤三：配置域名解析

将 `example.com` 通过CNAME域名解析的方式解析到

ALB

实例的公网服务域名上。

1. 登录应用型负载均衡控制台。
2. 在顶部菜单栏选择地域。
3. 选择要进行域名解析的

   ALB

   实例，复制其对应的DNS名称。
4. 完成以下步骤来添加CNAME解析记录。
   i. 登录域名解析控制台。
   ii. 在**域名解析**页面单击**添加域名**。
   iii. 在**添加域名**对话框中输入您的主机域名，然后单击**确定**。

   > 注意 您的主机域名需已完成TXT记录验证。

   iv. 在目标域名的**操作**列单击**解析设置**。
   v. 在**解析设置**页面单击**添加记录**。

vi. 在**添加记录**面板配置以下信息完成CNAME解析配置，然后单击**确认**。

配置	说明
记录类型	在下拉列表中选择**CNAME**。
主机记录	您的域名的前缀。
解析线路	选择默认。
记录值	输入加速域名对应的CNAME地址，即您复制的 ALB 实例的DNS名称。
TTL	全称Time To Live，表示DNS记录在DNS服务器上的缓存时间，本文使用默认值。

> **说明**
>
> - 新增CNAME记录实时生效，修改CNAME记录取决于本地DNS缓存的解析记录的TTL到期时间，一般默认为10分钟。
> - 添加时如遇添加冲突，请换一个解析域名。

步骤四：结果验证

在Chrome浏览器中输入`example.com`可访问到

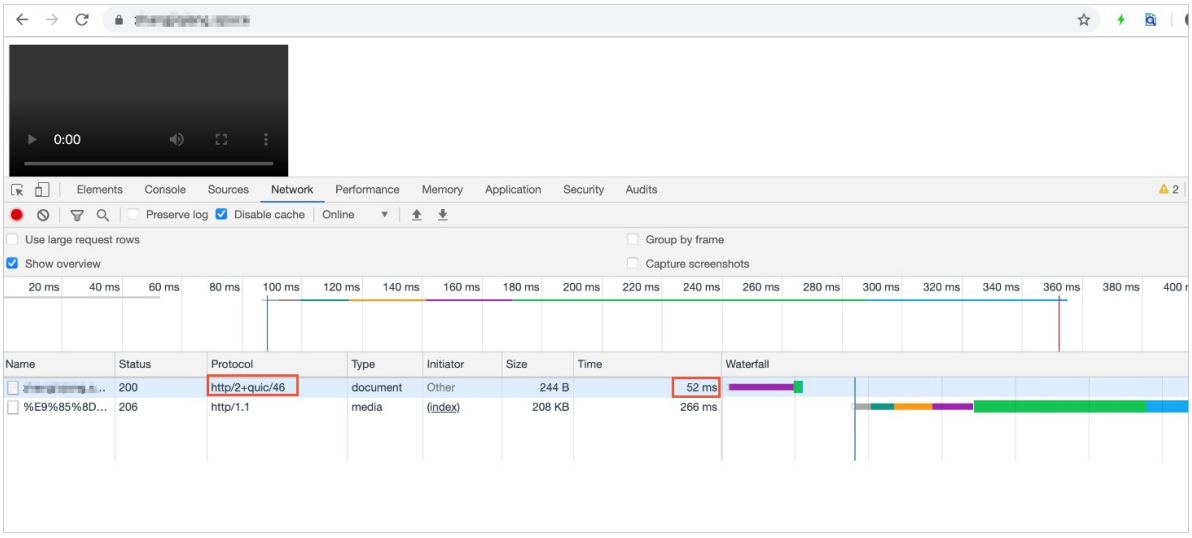
ALB

实例，本文在服务器组RS1对应的后端服务器ECS01上使用Nginx搭建了视频服务。

- 当同时配置了HTTPS监听和QUIC监听时，在Chrome浏览器中输入证书绑定的域名`example.com`，并按`F12`可以查看当前网页的**Protocol**为**http/2+quic/46**，**Time**为52ms。

  > **说明** http/2+quic/46表示使用了QUIC协议，即Q46。

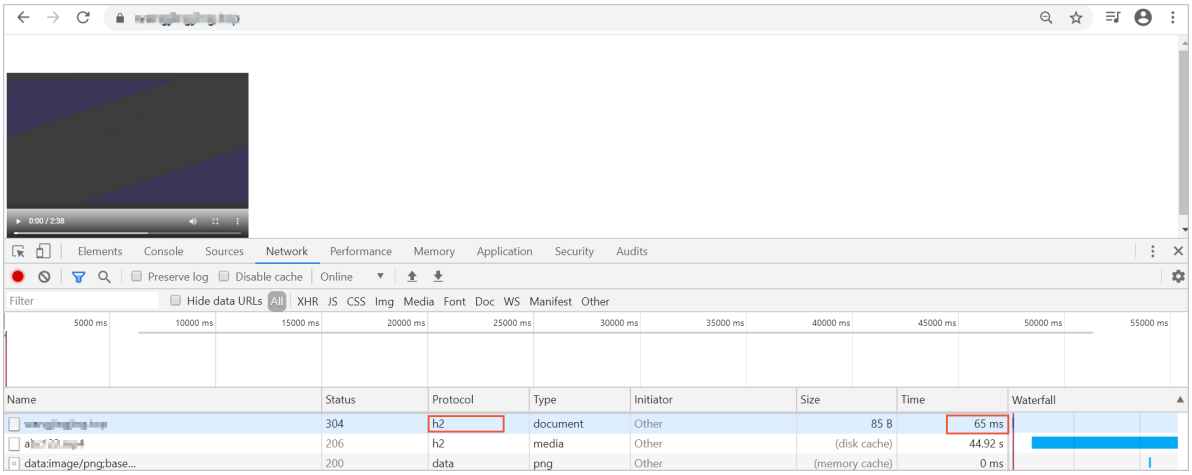
  如下图所示：



- 当QUIC监听不可用时，在Chrome浏览器中输入证书绑定的域名 `example.com` ，并按 `F12` 可以查看当前网页的**Protocol**为**h2**，**Time**为**65ms**。

  > 说明 h2表示使用了HTTPS协议。

  如下图所示：



经测试，QUIC协议大幅提升了客户端访问后端服务器视频的速度。

1.7. 自定义TLS安全策略提升网站安全等级

配置HTTPS监听时，选择高版本的TLS安全策略，可以提高您的业务安全性，网站安全等级也会随之提升，TLS安全策略包含TLS协议版本和配套的加密算法套件。

背景信息

HTTPS加密时代已经来临，国内外大型跨国公司或者个人网站，大多已经启用了全站HTTPS部署，这也是未来互联网发展的趋势。

在全站HTTPS部署网站的安全评级中，有些网站安全等级评分较高，而有些网站评分却较低。网站评分低的大部分原因是服务器启用了低版本的TLS安全策略。低版本的TLS安全策略存在许多安全漏洞，存在被攻击的风险。

应用型负载均衡ALB

支持自定义TLS安全策略，您可以自定义TLS版本以及配套的加密算法，提升您网站的安全等级，提高业务的安全性。

使用限制

基础版

ALB

实例不支持自定义TLS安全策略，需要升级为标准版

ALB

实例。具体操作，请参见实例变配。

新建HTTPS监听并使用自定义TLS安全策略

1. 在

   ALB

   实例所属地域，创建自定义TLS安全策略。具体操作，请参见TLS安全策略。
2. 创建HTTPS监听，选择已创建的自定义TLS安全策略。具体操作，请参见添加HTTPS监听。

自定义已有HTTPS监听的TLS安全策略

1. 在

   ALB

   实例所属地域，创建自定义TLS安全策略。具体操作，请参见TLS安全策略。
2. 在左侧导航栏，选择**应用型负载均衡ALB > 实例**。
3. 找到目标实例，然后单击实例ID。
4. 在**监听**页签，找到目标HTTPS监听，然后单击监听ID。
5. 在**SSL证书**区域，单击**TLS安全策略**后的 图标。
6. 在**编辑TLS安全策略**对话框，选择已创建的自定义TLS安全策略，然后单击**保存**。

1.8. 使用弹性伸缩实现自动添加ALB后端服务器

弹性伸缩的伸缩组支持关联

应用型负载均衡ALB

的服务器组，通过配置触发任务，自动调整伸缩组的ECS实例并添加到

ALB

实例的服务器组。

ALB

实例将访问流量分发到通过伸缩组自动创建的ECS实例中，有效增强了

ALB

的服务能力。

背景信息

应用型负载均衡服务通过设置虚拟服务地址，将添加的同一地域的多个ECS实例虚拟成一个高性能、高可用的应用服务池。简单来说，应用型负载均衡服务通过组合

ALB

实例 、监听和后端服务器，提供流量分发控制服务。更多信息，请参见什么是应用型负载均衡ALB。

伸缩组关联

ALB

实例的服务器组后，无论是伸缩组自动创建ECS实例，还是您向伸缩组手动添加ECS实例，ECS实例都会自动加入到

ALB

实例的服务器组。

ALB

实例会根据流量分发、健康检查等策略灵活使用ECS实例资源，在资源弹性的基础上大大提高资源可用性。

场景示例

某新闻网站播出了热点新闻，访问量突增，新闻的时效性降低后，访问量回落。由于该新闻网站的业务量波动无规律，访问量突增和回落的具体时间难以预测，所以手动调整实例很难做到及时性，而且调整数量也不确定。面对如上的场景，您可以利用弹性伸缩的报警任务，由阿里云根据CPU使用率等衡量指标自动调整其弹性资源的管理服务，同时自动关联

ALB

服务器组。在业务需求高峰期增长时，无缝增加计算资源。在业务量下降时，可以自动减少计算资源，从而节约成本。

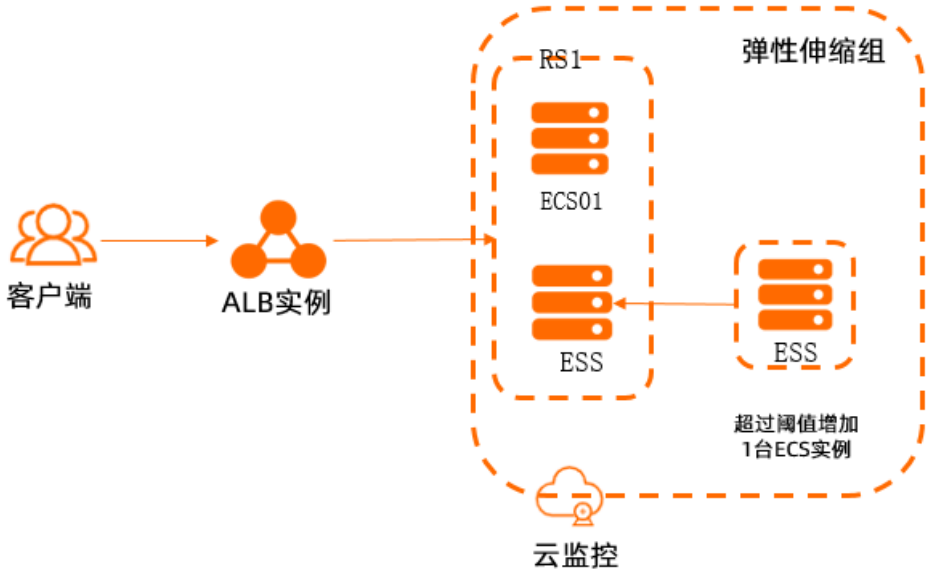
ALB

将客户端的请求通过配置的转发规则分发给后端服务器ECS01，当ECS01的CPU使用率达到100%时，通过创建弹性伸缩服务并配置报警任务，自动新建ECS实例并添加到

ALB

实例的服务器组RS1。

> **说明** 这些ECS实例的权重默认为50，您可以根据需要在对应ALB实例中调整权重。



前提条件

- 您持有一个或多个处于**运行中**状态的

  ALB

  实例。具体操作，请参见创建应用型负载均衡。
- ALB

  实例和伸缩组必须位于同一地域。
- ALB

  实例和伸缩组必须位于同一专有网络。
- ALB

  实例至少配置了一个监听。具体操作，请参见添加HTTP监听。
- ALB

  实例必须开启健康检查。具体操作，请参见健康检查。
- ALB

  实例已创建服务器RS1组并添加了ECS01实例，服务器组处于可用状态。
- 您已创建了ECS01实例的自定义镜像。具体操作，请参见使用实例创建自定义镜像。

步骤一：创建伸缩组

本步骤重点介绍在创建伸缩组时，与

ALB

实例相关的参数配置。关于其他参数的配置，请参见创建伸缩组。

1. 登录弹性伸缩控制台。
2. 在左侧导航栏中，单击**伸缩组管理**。
3. 在顶部菜单栏处，选择地域。
4. 进入**伸缩组管理**页面。

- 创建关联ALB实例的伸缩组时，单击**创建伸缩组**。
- 修改未配置ALB实例的伸缩组时，找到目标伸缩组，在**操作**列单击**修改**。

> 说明 如果您在创建伸缩组，需在**创建伸缩组**对话框，配置**网络类型**为**专有网络**，配置**添加已有实例**为ECS01。

5. 在**创建伸缩组**或者**修改伸缩组**对话框，配置**关联应用型负载均衡ALB服务器组**。
   i. 选择已创建的服务器组RS1。
   ii. 设置服务器组的端口为**80**，权重默认为**50**。

6. 根据需要配置其余选项，单击**确认**。

步骤二：创建伸缩配置

1. 在**伸缩组管理**页面的**操作**列单击**查看详情**，在**实例配置来源**页签单击**伸缩配置**。
2. 在**伸缩配置**页签，单击**创建伸缩配置**完成以下配置，然后单击**下一步系统配置**。

配置项	说明
付费模式	ECS的付费方式，本文选择**按量付费**。

配置项	说明
实例规格	与创建的ECS01实例规格相同，本文选择**ecs.s6-c1m1.small**。
镜像	选择已经创建的ECS01实例的自定义镜像。
安全组	选择已创建的ECS01实例所在安全组。

3. 在**系统配置**配置向导，单击**下一步 确认配置**。
4. 在**确认配置**配置向导，填写**伸缩配置名称**，然后单击**确认创建**。
5. 在**伸缩配置建立成功**对话框，单击**启用配置**。

步骤三：创建伸缩规则

1. 在**伸缩组管理**页面的**操作**列单击**查看详情**，在**伸缩规则与伸缩活动**页签单击**伸缩规则**。
2. 在**伸缩规则**页签，单击**创建伸缩规则**完成以下配置，单击**确认**。

配置项	说明
规则名称	输入自定义规则名称。
伸缩规则类型	本文选择**简单规则**。
执行的操作	本文选择**调整至2台**。

步骤四：创建报警任务并添加伸缩规则

1. 在**自动触发任务管理 > 报警任务**页面，单击**系统监控**页签。
2. 单击**创建报警任务**完成以下配置，单击**确认**。

配置项	说明
名称名称	自定义任务名称。
监控资源	选择步骤一创建的伸缩组。
监控项	本文选择（ECS）**CPU使用率**。
统计周期	本文选择**1分钟**。
统计办法	本文设置**Maximum（最大值）>= 阈值 60%**。

配置项	说明
重复几次后报警	本文选择**1次**。
报警触发规则	选择步骤三创建的伸缩规则。

步骤五：基于CPU使用率自动创建ALB后端服务器

通过stress压测的方式，增加ECS01实例的CPU使用率，使CPU使用率达到100%，从而触发弹性伸缩的报警任务，根据创建的弹性伸缩服务自动新建ECS实例并添加到

ALB

实例的服务器组。

1. 远程登录ECS01实例后，执行以下命令安装stress。

```
yum install -y epel-release
yum install stress -y
```

2. 执行以下命令通过stess工具对ECS01实例进行压测。

```
stress --cpu 1 --io 4 --vm 2 --vm-bytes 128M --timeout 60s &
```

3. 返回弹性伸缩的**报警任务**页面，等待几分钟后，报警**状态**显示**报警** 。

4. 进入**伸缩组管理**页面，在**实例数/容量**列查看**总实例数**变为2个。证明已添加一台新的ECS实例到伸缩组。

5. 登录应用型负载均衡ALB控制台。
6. 在左侧导航栏，选择**应用型负载均衡ALB > 服务器组** 。
7. 单击创建的目标服务器组RS1的ID，单击**后端服务器**页签，可以看到后端服务器有两台实例，其中以ESS命名的实例为通过弹性伸缩服务自动添加的ECS实例。

相关文档

相关文档

- CreateScalingGroup：调用CreateScalingGroup创建一个伸缩组。
- AttachLoadBalancers：调用AttachLoadBalancers添加一个或多个负载均衡实例。
- EnableScalingGroup：调用EnableScalingGroup启用一个伸缩组。
- CreateScalingConfiguration：调用CreateScalingConfiguration创建一个伸缩配置。
- CreateScalingRule：调用CreateScalingRule创建一条伸缩规则。
- ExecuteScalingRule：调用ExecuteScalingRule执行一条伸缩规则。
- CreateAlarm：调用CreateAlarm创建一个报警任务。
- AttachAlbServerGroups：调用AttachAlbServerGroups向伸缩组添加一个或多个ALB服务器组。

1.9. 使用ALB挂载跨地域VPC内的服务器

应用型负载均衡ALB（Application Load Balancer）支持跨地域挂载功能。本文指导您通过

ALB

和CEN（Cloud Enterprise Network）转发路由器的配置，使

ALB

的请求转发到其它地域的服务器。

场景示例

本文以下图场景为例。某企业在阿里云西南1（成都）地域创建了专有网络VPC1，在该VCP1中创建了一个

ALB

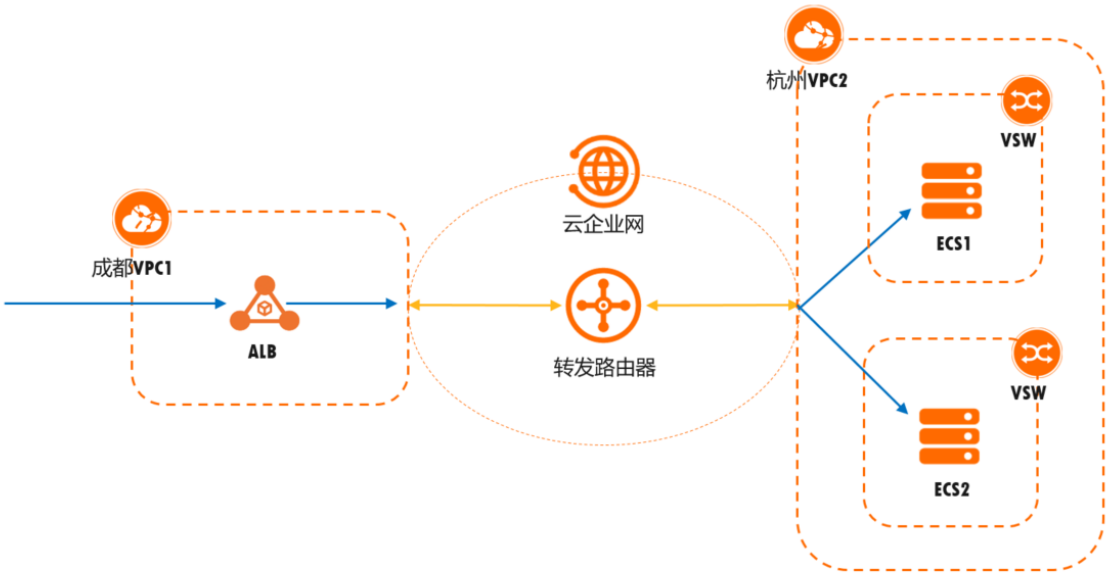
实例。同时在华东1（杭州）创建了专有网络VPC2，并在该专有网络中创建了ECS实例。该企业希望VPC1中的

ALB

实例能够跨地域访问VPC2内的ECS实例，通过云企业网实现VPC1与VP2的互通，即可实现

ALB

跨地域挂载服务器的目的。该场景多用于游戏、金融等行业，可有效保证数据传输质量，降低时延。



本文示例中的网段规划如下表所示。您也可以自行规划网段，请确保您的网段之间没有重叠。

地域	VPC	交换机	交换机可用区	网段规划
西南1（成都）	VPC1 主网段：172.16.0.0/12	VSW1	成都 可用区A	172.16.0.0/24
		VSW2	成都 可用区B	172.16.6.0/24
华东1（杭州）	VPC2 主网段：192.168.0.0/16	VSW3	杭州 可用区H	192.168.8.0/24
		VSW4	杭州 可用区I	192.168.7.0/24

注意事项

- 目前只有西南1（成都）地域的

  ALB

  支持挂载跨地域VPC内的服务器，且该功能目前白名单开放，如需体验请提交工单或联系您的客户经理申请。
- 公网

  ALB

  和私网

  ALB

  都支持跨域挂载VPC内的服务器。
- ALB

  包含基础版和标准版，仅标准版支持跨域挂载VPC内的服务器。
- ALB

  跨地域挂载的后端服务器仅支持IP类型。

- VPC1和VPC2需要加入同一个CEN。
- 企业版转发路由器会在指定的两个可用区的交换机实例上创建弹性网卡ENI（Elastic Network Interface），作为VPC实例向企业版转发路由器发送流量的入口。在您创建VPC实例时，请确保在企业版转发路由器指定的两个可用区中各创建一个交换机实例，以便将VPC实例连接至企业版转发路由器。更多信息，请参见企业版转发路由器支持的地域和可用区。

准备工作

- 您已经在西南1（成都）地域创建了专有网络VPC1，在华东1（杭州）创建了专有网络VPC2。并在VPC1中创建了交换机VSW1和VSW2，VSW1位于可用区A，VSW2位于可用区B。在VPC2中创建了交换机VSW3和VSW4，VSW3位于可用区H，VSW4位于可用区I。具体操作，请参见创建和管理专有网络。
- 您已经在VPC2中创建了ECS1实例并部署了应用服务。具体操作，请参见使用向导创建实例。
- 您已经在VPC1中创建了一个

  ALB

  实例。具体操作，请参见创建应用型负载均衡。
- 您已经创建了云企业网实例并为该云企业网实例购买了带宽包。具体操作，请参见创建云企业网实例和使用带宽包。

配置步骤

步骤一：创建

ALB

服务器组

创建IP类型的服务器组，并为该服务器添加远端IP。

1. 登录应用型负载均衡ALB控制台。
2. 在左侧导航栏，选择**应用型负载均衡ALB > 服务器组**。
3. 在**服务器组**页面，单击**创建服务器组**，完成以下配置，然后单击**创建**。

配置	说明
服务器组类型	选择服务器组类型。本文选择**IP类型**。 **说明** ALB跨域挂载VPC内的服务器，只支持按照IP地址添加后端服务器，且该功能需要白名单开放。
服务器组名称	输入服务器组名称。长度为2~128个字符，必须以大小写字母或中文开头，可包含数字、半角句号（.）、下划线（_）和短划线（-）。
VPC	从VPC下拉列表中选择一个VPC。本文选择**VPC1**。

配置	说明
选择后端协议	选择一种后端协议。本文选择**HTTP**。 **说明** 基础版 ALB 实例的HTTPS监听只能选择后端协议是HTTP的服务器组。
选择调度算法	选择一种调度算法。本文使用默认值**加权轮询**。
选择资源组	选择归属的资源组。
开启会话保持	开启或关闭会话保持。
配置健康检查	开启或关闭健康检查。本文选择默认开启。
高级配置	本文使用默认配置。更多信息，请参见管理服务器组。

4. 在**服务器组**页面，找到目标服务器组，然后在**操作**列单击**编辑后端服务器**。
5. 在**后端服务器**页签，单击**添加IP**。
6. 在**添加后端服务器**面板，输入ECS1的私网IP地址，并打开**远端IP**，然后单击**下一步**。
7. 设置添加的IP地址的端口和权重，然后单击**确定**。本文端口输入80，权重使用默认值。

步骤二：为

ALB

实例配置监听

1. 登录应用型负载均衡ALB控制台。
2. 在顶部菜单栏，选择

   ALB

   的所属地域。本文选择**西南1（成都）**。
3. 在**实例**页面，找到已经在VPC1中创建好的

   ALB

   实例，单击目标实例**操作**列下的**创建监听**，打开监听配置向导。
4. 在**配置监听**配置向导，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**HTTP**。
监听端口	输入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。本文输入**80**。
监听名称	自定义监听的名称。

监听配置	说明
高级配置	本文使用默认配置。

5. 在**选择服务器组**配置向导，在**选择服务器组**的下拉框选择**IP类型**，并选择目标服务器组，然后单击**下一步**。
6. 在**配置审核**配置向导，确认配置信息，单击**提交**。

步骤三：创建VPC连接

1. 登录云企业网管理控制台。
2. 在**云企业网实例**页面，单击已创建的云企业网实例ID。
3. 在云企业网实例详情页面，单击**VPC**下侧的⊕图标。
4. 在**连接网络实例**页面，配置以下参数信息，然后单击**确定创建**。

参数	说明
实例类型	本文选择**专有网络（VPC）**。
地域	选择要连接的网络实例所在的地域。本文选择**西南1（成都）**。
转发路由器	系统自动为您在该地域创建转发路由器。本文创建的为企业版转发路由器。关于转发路由器的更多信息，请参见转发路由器工作原理。
设定转发路由器的主/备可用区	选择转发路由器的主备可用区。本文**主可用区**选择**成都 可用区A**，**备可用区**选择**成都 可用区B**。
资源归属UID	选择要连接的网络实例所归属的账号类型。本文使用默认值**同账号**。
付费方式	本文使用默认值**按量付费**。
连接名称	输入连接名称。 名称长度为2~128个字符，以大小写字母或中文开头，可包含数字、下划线（_）或短划线（-）。
网络实例	选择要连接的VPC网络实例ID。本文选择VPC1。
交换机	分别从主备可用区中选择交换机。本文主可用区选择VSW1，备可用区选择VSW2。
高级配置	系统默认选中高级功能。本文使用默认配置。

5. VPC1连接创建完成后，单击**继续创建连接**，然后重复步骤4，创建VPC2网络实例连接。

   参数配置如下，其余参数选择默认配置。

   - **地域**选择**华东1（杭州）**。
   - **主可用区**选择**杭州 可用区H**，**备可用区**选择**杭州 可用区I**。
   - **网络实例**选择VPC2。

- **交换机**可用区选择VSW3，备可用区选择VSW4。

步骤四：创建跨地域连接

1. 登录云企业网管理控制台。
2. 在**云企业网实例**页面，单击已创建的云企业网实例ID。
3. 在**基本信息 > 转发路由器**页签，找到目标转发路由器实例，在**操作**列单击**创建网络实例连接**。

   目标转发路由器实例可以选择VP1或者VP2关联的转发路由器实例。本文选择VPC1关联的转发路由器实例。
4. 在**连接网络实例**页面，配置跨地域连接信息，然后单击**确定创建**。

配置项	说明
实例类型	选择**跨地域**。
地域	要互通的地域。本文选择**西南1（成都）**。
转发路由器	要互通的地域下的转发路由器实例。 如果当前地域下您暂无转发路由器实例，系统默认为您自动创建。
连接名称	跨地域连接名称。 名称长度为2~128个字符，以大小写字母或中文开头，可包含数字、下划线（_）或短划线（-）。
带宽分配方式	本文选择**从带宽包分配**。
对端地域	要互通的对端地域。本文选择**华东1（杭州）**。
转发路由器	要互通的对端地域下的转发路由器实例。 如果当前地域下您暂无转发路由器实例，系统默认为您自动创建。
带宽包实例	选择已绑定的带宽包实例。
带宽	输入允许使用的带宽值。单位：Mbps。
高级配置	本文使用默认配置。

步骤五：为VPC1的系统路由表添加路由条目

检查VPC1中的系统路由表是否已经有目标网段的路由指向转发路由器VPC1连接，如果没有，则执行以下步骤添加路由条目。

1. 登录专有网络管理控制台。
2. 在**专有网络**，单击VPC1的实例ID。
3. 在VPC详情页面，单击**资源管理**页签，在**路由表**下方单击数字链接。
4. 在**路由表**页面，找到**路由表类型**为**系统**的路由表，单击其ID。
5. 在路由表详情页面，选择**路由条目列表 > 自定义**页签，然后单击**添加自定义路由条目**。
6. 在**添加路由条目**面板，配置以下参数，然后单击**确定**。

参数	说明
名称	输入路由条目的名称。
目标网段	输入要转发到的目标网段。本文输入ECS1服务器的IP地址：*192.168.7.54*。
下一跳类型	选择下一跳的类型。本文选择**转发路由器**。
转发路由器	选择具体的转发路由器实例。本文选择VPC1连接。

步骤六：配置回源路由

查看

ALB

实例的回源路由，并分别为VPC2的系统路由表和VPC1关联的转发路由器添加ALB的回源路由。

1. 执行以下步骤，查看

   ALB

   实例的回源路由。

   i. 登录应用型负载均衡ALB控制台。

   ii. 在顶部菜单栏，选择实例的所属地域。本文选择**西南1（成都）**。

   iii. 在**实例**页面，单击在VPC1中已经创建好的

   ALB

   实例ID。

   iv. 单击**实例详情**页签，然后在**回源路由**右侧单击**查看**。

2. 执行以下步骤，为VPC2内的系统路由表添加

   ALB

   的回源路由。

   i. 登录专有网络管理控制台。

   ii. 在**专有网络**页面，单击VPC2的实例ID。

   iii. 在VPC详情页面，单击**资源管理**页签，在**路由表**下方单击数字链接。

   iv. 在**路由表**页面，找到**路由表类型**为**系统**的路由表，单击其ID。

v. 在路由表详情页面，选择**路由条目列表 > 自定义**页签，然后单击**添加自定义路由条目**。

vi. 在**添加路由条目**面板，配置以下参数，然后单击**确定**。

参数	说明
名称	输入路由条目的名称。
目标网段	输入要转发到的目标网段。本文输入步骤1中ALB实例的回源路由。如果回源路由有多条，请重复配置操作， 直到所有回源路由全部配置完。
下一跳类型	选择下一跳的类型。本文选择**转发路由器**。
转发路由器	选择具体的转发路由器实例。本文选择VPC2关联的转发路由器。

为VPC2配置的路由条目：

目标网段	下一跳
100.XX.XX.0/25	VPC2关联的转发路由器
100.XX.XX.128/25	VPC2关联的转发路由器
100.XX.XX.64/26	VPC2关联的转发路由器
100.XX.XX.128/26	VPC2关联的转发路由器
100.XX.XX.192/26	VPC2关联的转发路由器
100.XX.XX.0/26	VPC2关联的转发路由器

3. 执行以下步骤，为VPC1关联的转发路由器添加

ALB

的回源路由。

i. 登录云企业网管理控制台。

ii. 在**云企业网实例**页面，单击已创建的云企业网实例ID。

iii. 在**基本信息 > 转发路由器**页签，找到连接VPC1的转发路由器实例，并单击该目标转发路由器实例ID。

iv. 单击**转发路由器路由表**页签，在页签左侧区域，单击目标路由表ID，在路由表详情页面的**路由条目**页签下，单击**创建路由条目**。

v. 在**添加路由条目**对话框，配置路由条目信息，然后单击**确定**。

配置项	说明
路由表	系统默认选择当前路由表。
所属转发路由器	系统默认选择当前转发路由器实例。
路由条目名称	路由条目名称。 长度为0~128个字符，可包含大小写字母、数字、中文、半角逗号（,）、半角句号（.）、半角分号（;）、正斜线（/）、at（@）、下划线（_）和短划线（-）。
目的地址CIDR	路由条目的目标网段。本文输入步骤1中ALB实例的回源路由。如果回源路由有多条，请重复配置操作， 直到所有回源路由全部配置完。
是否为黑洞路由	系统默认选择否。
下一跳连接	选择路由的下一跳连接。本文选择VPC1连接。
路由条目描述	路由条目的描述信息。 长度为2~256个字符，可包含大小写字母、数字、中文、半角逗号（,）、半角句号（.）、半角分号（;）、正斜线（/）、at（@）、下划线（_）和短划线（-）。

为VPC1关联的转发路由器配置的路由条目：

目标网段	下一跳
100.XX.XX.0/25	VPC1连接
100.XX.XX.128/25	VPC1连接
100.XX.XX.64/26	VPC1连接
100.XX.XX.128/26	VPC1连接
100.XX.XX.192/26	VPC1连接
100.XX.XX.0/26	VPC1连接

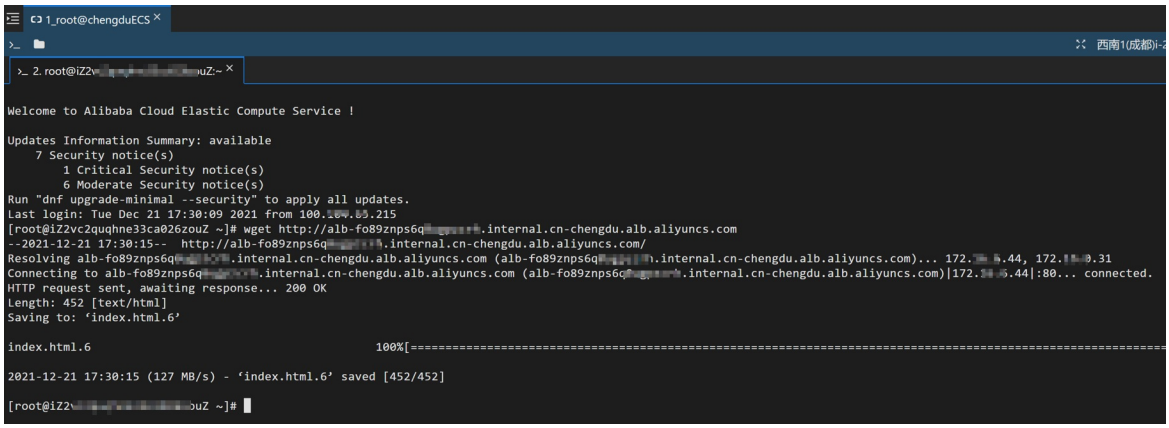
步骤七：测试连通性

1. 登录VPC1的ECS实例。具体操作，请参见ECS远程连接操作指南。
2. 执行 `wget http://DNS名称` 命令，测试VPC1中的ECS是否能通过ALB访问跨域跨VPC2内的ECS1。

   本文执行以下命令。

```
wget http://alb-fo89znps6q********.internal.cn-chengdu.alb.aliyuncs.com
```

如果能接收到回复报文，表示连接成功。



1.10. 使用ALB挂载IDC服务器

应用型负载均衡ALB（Application Load Balancer）支持挂载本地IDC（Internet Data Center）服务器。本文指导您通过

ALB

和CEN（Cloud Enterprise Network）转发路由器等产品的组合配置，使

ALB

的请求转发到本地IDC服务器。

场景示例

本文以下图场景为例。某企业在阿里云西南1（成都）地域创建了专有网络VPC1，在该VPC1中创建了一个

ALB

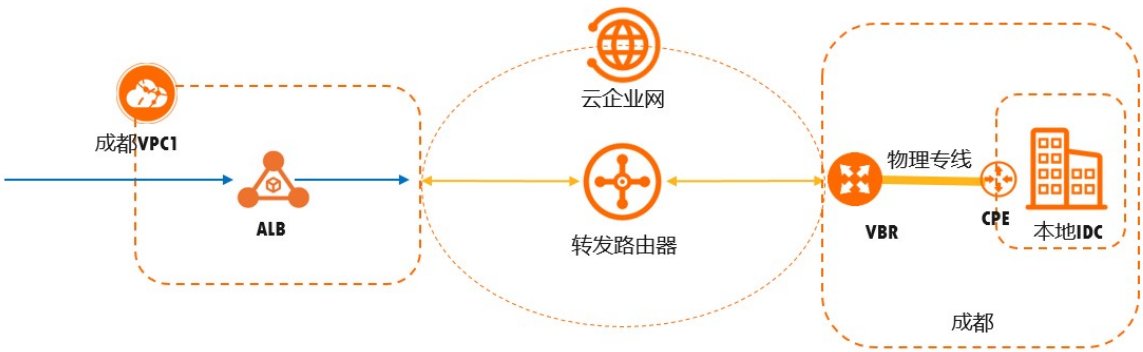
实例。该企业希望VPC1中的

ALB

实例可以将请求转发至同地域的IDC服务器，本地IDC通过VBR接入阿里云，ALB通过CEN与VPC互通，即可实现

ALB

挂载同地域IDC服务器的目的。



本文示例中的网段规划如下表所示。您也可以自行规划网段，请确保您的网段之间没有重叠。

V西南（成都）地域	交换机	交换机可用区	网段规划
VPC1 主网段：172.16.0.0/12	VSW1	成都 可用区A	172.16.0.0/24
	VSW2	成都 可用区B	172.16.6.0/24
VBR	不涉及	不涉及	客户侧IPv4互联IP：10.0.0.2/30 阿里云侧IPv4互联IP：10.0.0.1/30
本地IDC	VSW3	不涉及	192.168.20.0/24

注意事项

- ALB

  支持挂载本地IDC服务器，该功能目前白名单开放，如需体验请提交工单或联系您的客户经理申请。
- 公网

  ALB

  和私网

  ALB

  都支持挂载本地IDC服务器。
- ALB

  挂载本地IDC服务器时，后端服务器仅支持IP类型。
- 企业版转发路由器会在指定的两个可用区的交换机实例上创建弹性网卡ENI（Elastic Network Interface），作为VPC实例向企业版转发路由器发送流量的入口。在您创建VPC实例时，请确保在企业版转发路由器指定的两个可用区中各创建一个交换机实例，以便将VPC实例连接至企业版转发路由器。更多信息，请参见企业版转发路由器支持的地域和可用区。

准备工作

- 您已经在西南1（成都）地域创建了专有网络VPC1，并在VPC1创建了交换机VSW1和VSW2，VSW1位于可用区A，VSW2位于可用区B。具体操作，请参见创建和管理专有网络。
- 您已经在VPC1中创建了一个

  ALB

  实例。具体操作，请参见创建应用型负载均衡。
- 您已经在VPC1中创建了ECS1实例并部署了应用服务。具体操作，请参见使用向导创建实例。
- 您已经创建了云企业网实例。具体操作，请参见创建云企业网实例。
- 您已经创建了物理专线和边界路由器VBR。具体操作，请参见创建独享专线连接和创建边界路由器。

配置步骤

步骤一：创建

ALB

服务器组

创建IP类型的服务器组，并为该服务器添加远端IP。

1. 登录应用型负载均衡ALB控制台。
2. 在左侧导航栏，选择**应用型负载均衡ALB > 服务器组**。
3. 在**服务器组**页面，单击**创建服务器组**，完成以下配置，然后单击**创建**。

配置	说明
服务器组类型	选择服务器组类型。本文选择**IP类型**。 **说明** ALB挂载本地IDC服务器，只支持按照IP地址添加后端服务器，且该功能需要白名单开放。
服务器组名称	输入服务器组名称。长度为2~128个字符，必须以大小写字母或中文开头，可包含数字、半角句号（.）、下划线（_）和短划线（-）。
VPC	从VPC下拉列表中选择一个VPC。本文选择**VPC1**。
选择后端协议	选择一种后端协议。本文选择**HTTP**。 **说明** 基础版 ALB 实例的HTTPS监听只能选择后端协议是HTTP的服务器组。
选择调度算法	选择一种调度算法。本文使用默认值**加权轮询**。
选择资源组	选择归属的资源组。
开启会话保持	开启或关闭会话保持。
配置健康检查	开启或关闭健康检查。本文选择默认开启。
高级配置	本文使用默认配置。更多信息，请参见管理服务器组。

4. 在**服务器组**页面，找到目标服务器组，然后在**操作**列单击**编辑后端服务器**。
5. 在**后端服务器**页签，单击**添加IP**。
6. 在**添加后端服务器**面板，输入本地IDC服务器IP地址，并打开**远端IP**，然后单击**下一步**。
7. 设置添加的IP地址的端口和权重，然后单击**确定**。本文端口输入80，权重使用默认值。

步骤二：为

ALB

实例配置监听

1. 登录应用型负载均衡ALB控制台。
2. 在顶部菜单栏，选择

   ALB

   的所属地域。本文选择**西南1（成都）**。
3. 在**实例**页面，找到已经在VPC1中创建好的

   ALB

   实例，单击目标实例**操作**列下的**创建监听**，打开监听配置向导。
4. 在**配置监听**配置向导，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**HTTP**。
监听端口	输入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。本文输入**80**。
监听名称	自定义监听的名称。
高级配置	本文使用默认配置。

5. 在**选择服务器组**配置向导，在**选择服务器组**的下拉框选择**IP类型**，并选择目标服务器组，然后单击**下一步**。
6. 在**配置审核**配置向导，确认配置信息，单击**提交**。

步骤三：创建VPC连接

1. 登录云企业网管理控制台。
2. 在**云企业网实例**页面，单击已创建的云企业网实例ID。
3. 在云企业网实例详情页面，单击**VPC**下侧的⊕图标。
4. 在**连接网络实例**页面，配置以下参数信息，然后单击**确定创建**。

参数	说明
实例类型	本文选择**专有网络（VPC）**。
地域	选择要连接的网络实例所在的地域。本文选择**西南1（成都）**。
转发路由器	系统自动为您在该地域创建转发路由器。本文创建的为企业版转发路由器。关于转发路由器的更多信息，请参见转发路由器工作原理。
设定转发路由器的主/备可用区	选择转发路由器的主备可用区。本文**主可用区**选择**成都 可用区A**，**备可用区**选择**成都 可用区B**。
资源归属UID	选择要连接的网络实例所归属的账号类型。本文使用默认值**同账号**。
付费方式	本文使用默认值**按量付费**。

参数	说明
连接名称	输入连接名称。 名称长度为2~128个字符，以大小写字母或中文开头，可包含数字、下划线（_）或短划线（-）。
网络实例	选择要连接的VPC网络实例ID。本文选择VPC1。
交换机	分别从主备可用区中选择交换机。本文主可用区选择VSW1，备可用区选择VSW2。
高级配置	系统默认选中高级功能。本文使用默认配置。

步骤四：创建VBR连接

1. 创建VPC连接后，单击**继续创建连接**。
2. 在**连接网络实例**页面，配置以下参数信息，然后单击**确定创建**。

参数	说明
实例类型	本文选择**边界路由器（VBR）**。
地域	选择要连接的网络实例所在的地域。本文选择**西南1（成都）**。
转发路由器	系统自动选择当前地域已创建的转发路由器。此处选择成都的转发路由器。
资源归属UID	选择要连接的网络实例所归属的账号类型。本文使用默认值**同账号**。
连接名称	输入连接名称。 名称长度为2~128个字符，以大小写字母或中文开头，可包含数字、下划线（_）或短划线（-）。
网络实例	选择要连接的VBR网络实例ID。本文选择已创建的VBR实例。
高级配置	系统默认选中高级功能。本文使用默认配置。更多操作，请参见创建VBR连接。

步骤五：为VPC1的系统路由表添加路由条目

检查VPC1中的系统路由表是否已经有目标网段的路由指向转发路由器VPC1连接，如果没有，则执行如下步骤添加路由条目。

1. 登录专有网络管理控制台。
2. 在**专有网络**，单击VPC1的实例ID。
3. 在VPC详情页面，单击**资源管理**页签，在**路由表**下方单击数字链接。
4. 在**路由表**页面，找到**路由表类型**为**系统**的路由表，单击其ID。
5. 在路由表详情页面，选择**路由条目列表 > 自定义**页签，然后单击**添加自定义路由条目**。
6. 在**添加路由条目**面板，配置以下参数，然后单击**确定**。

参数	说明
名称	输入路由条目的名称。
目标网段	输入要转发到的目标网段。本文输入本地IDC服务器网段：*192.168.20.0/24*。
下一跳类型	选择下一跳的类型。本文选择**转发路由器**。
转发路由器	选择具体的转发路由器实例。本文选择VPC1连接。

步骤六：配置VBR路由

在VBR上配置指向本地IDC的路由。

1. 登录高速通道管理控制台。
2. 在顶部菜单栏，选择目标地域，然后在左侧导航栏，单击**边界路由器（VBR）**。
3. 在**边界路由器（VBR）**页面，单击目标VBR实例ID。
4. 在边界路由器详情页面，单击**路由条目**页签，然后单击**添加路由条目**。
5. 在**添加路由条目**面板，配置以下参数信息，然后单击**确定**。

参数	说明
下一跳类型	选择路由条目的下一跳类型。本文选择**物理专线接口**。
目标网段	本文输入本地IDC中服务器网段：*192.168.20.0/24*。
下一跳	选择物理专线接口。

步骤七：配置回源路由

查看

ALB

实例的回源路由，并分别为VPC1关联的转发路由器和本地IDC添加ALB的回源路由。

1. 执行以下步骤，查看

   ALB

   实例的回源路由。

   i. 登录应用型负载均衡ALB控制台。

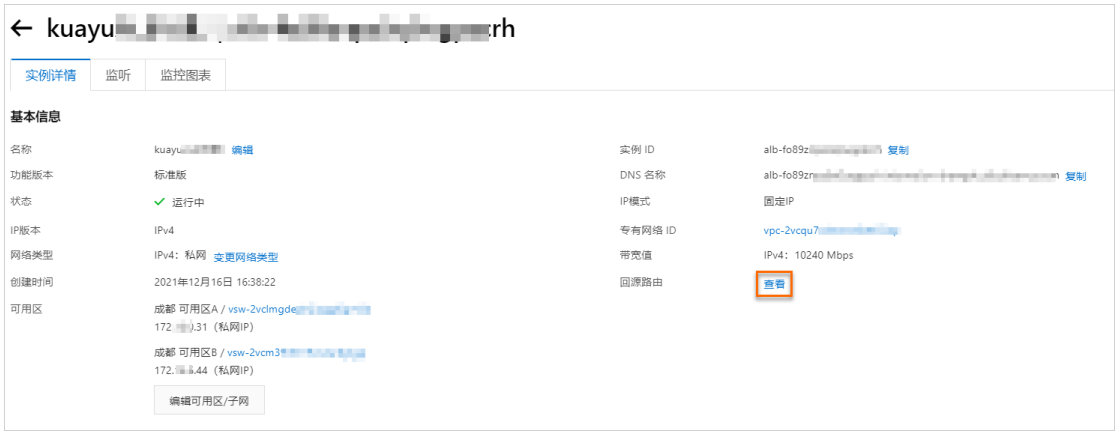
   ii. 在顶部菜单栏，选择实例的所属地域。本文选择**西南1（成都）**。

   iii. 在**实例**页面，单击在VPC1中已经创建好的

   ALB

   实例ID。

iv. 单击**实例详情**页签，然后在**回源路由**右侧单击**查看**。



2. 执行以下步骤，为VPC1关联的转发路由器添加

   ALB

   的回源路由。

   i. 登录云企业网管理控制台。

   ii. 在**云企业网实例**页面，单击已创建的云企业网实例ID。

   iii. 在**基本信息 > 转发路由器**页签，找到连接VPC1的转发路由器实例，并单击该目标转发路由器实例ID。

   iv. 单击**转发路由器路由表**页签，在页签左侧区域，单击目标路由表ID，在路由表详情页面的**路由条目**页签下，单击**创建路由条目**。

v. 在**添加路由条目**对话框，配置路由条目信息，然后单击**确定**。

配置项	说明
路由表	系统默认选择当前路由表。
所属转发路由器	系统默认选择当前转发路由器实例。
路由条目名称	路由条目名称。 长度为0~128个字符，可包含大小写字母、数字、中文、半角逗号（,）、半角句号（.）、半角分号（;）、正斜线（/）、at（@）、下划线（_）和短划线（-）。
目的地址CIDR	路由条目的目标网段。本文输入步骤1中ALB实例的回源路由。如果回源路由有多条，请重复配置操作， 直到所有回源路由全部配置完。
是否为黑洞路由	系统默认选择否。
下一跳连接	选择路由的下一跳连接。本文选择VPC1连接。
路由条目描述	路由条目的描述信息。 长度为2~256个字符，可包含大小写字母、数字、中文、半角逗号（,）、半角句号（.）、半角分号（;）、正斜线（/）、at（@）、下划线（_）和短划线（-）。

为VPC1关联的转发路由器配置的路由条目：

目标网段	下一跳
100.XX.XX.0/25	VPC1连接
100.XX.XX.128/25	VPC1连接
100.XX.XX.64/26	VPC1连接
100.XX.XX.128/26	VPC1连接
100.XX.XX.192/26	VPC1连接
100.XX.XX.0/26	VPC1连接

3. 执行以下步骤，为本地IDC添加

   ALB

   的回源路由。

   在本地网关设备上添加

   ALB

   的回源路由，配置的路由示例如下。如果回源路由有多条，请重复配置操作， 直到所有回源路由全部配置完。

> **说明** 路由示例仅供参考，不同厂商的不同设备可能会有所不同。

```
ip route 100.XX.XX.0/25 255.255.255.128 VBR实例阿里云侧IP地址
```

步骤八：测试连通性

1. 登录VPC1的ECS实例。具体操作，请参见ECS远程连接操作指南。
2. 执行 `wget http://DNS名称` 命令，测试VPC1中的ECS是否能通过ALB访问本地IDC服务器。

   本文执行以下命令。

   ```
   wget http://alb-fo89znps6q********.internal.cn-chengdu.alb.aliyuncs.com
   ```

   如果能接收到回复报文，表示连接成功。

2.CLB教程

2.1. 使用CLB部署HTTPS业务（单向认证）

要配置HTTPS单向认证的监听，您仅需要在配置监听时上传服务器证书。

步骤一：上传服务器证书

在配置HTTPS监听（单向认证）前，您需要购买服务器证书，并将服务器证书上传到负载均衡的证书管理系统。上传后，无需在后端ECS上进行其它证书配置。

1. 登录传统型负载均衡CLB控制台。
2. 在左侧导航栏，选择**证书管理**，单击**创建证书**。
3. 单击**上传非阿里云签发证书**。
4. 按照以下信息，配置证书：
   - 证书名称：长度限制为1~80个字符，只允许包含字母、数字、短划线（-）、正斜线（/）、半角句号（.）、下划线（_）和星号（*）。
   - 证书部署地域：选择**华东1（杭州）**。

     > **说明** 证书的地域和负载均衡实例的地域要相同。

   - 证书类型：选择**服务器证书**。
   - 证书内容和私钥：复制服务器证书的内容和私钥。单击**查看样例**查看合法的证书格式。上传的证书必须是PEM格式，详情请参见证书要求。
5. 单击**确定**，完成上传。

步骤二：配置负载均衡实例

1. 登录传统型负载均衡CLB控制台。
2. 在**实例管理**页面，单击**创建负载均衡**。
3. 配置负载均衡实例，单击**立即购买**完成支付。

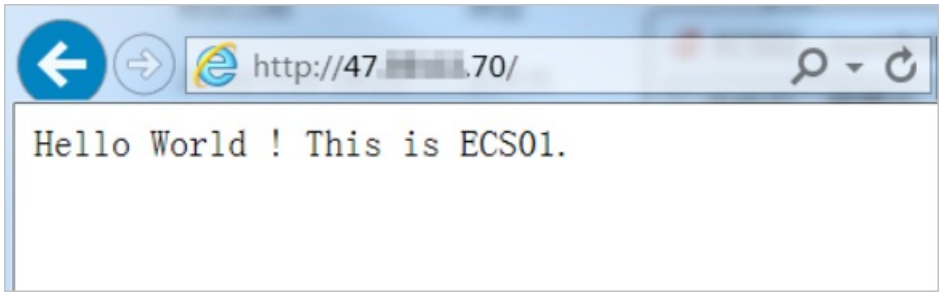
   实例类型选择**公网**，地域选择**华东1（杭州）**。详细配置信息请参见创建实例。
4. 创建成功后，返回**实例管理**页面，选择**华东1（杭州）**地域。
5. 单击已创建的负载均衡实例ID链接，或者直接单击**监听配置向导**。
6. 在**监听**页签下，单击**添加监听**。
7. 在**协议&监听**页签下，完成如下配置。
   - **选择负载均衡协议**：HTTPS。
   - **监听端口**：443。
   - **调度算法**：轮询（RR）。
8. 单击**下一步**，在**SSL证书**页签下，选择已经上传的服务器证书和TLS安全策略。
9. 单击**下一步**，选择**默认服务器组**，单击**继续添加**，添加ECS服务器，后端协议监听端口设置为80。
10. 其他参数保持默认值，单击**下一步**至**提交**，完成负载均衡实例配置。

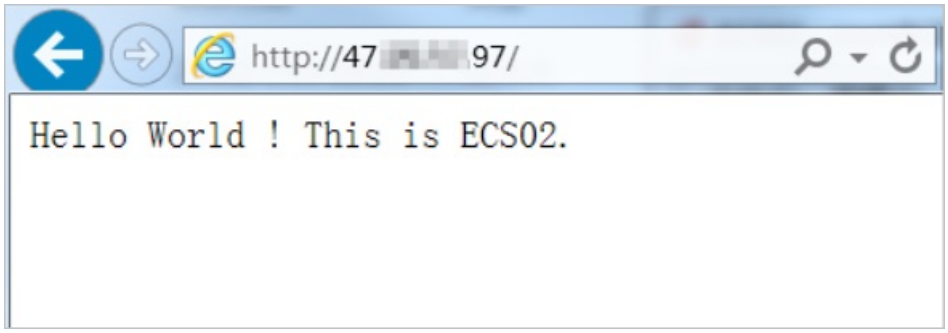
步骤三：测试负载均衡服务

1. 负载均衡实例配置完成后，在**实例管理**页面，查看健康检查状态。

   当状态为**正常**时，表示后端服务器可以正常接收处理负载均衡监听转发的请求。

2. 在浏览器中输入负载均衡的公网服务地址。





2.2. 使用CLB部署HTTPS业务（双向认证）

HTTPS单向认证只对服务器做认证，HTTPS双向认证对服务器和客户端做双向认证。当您在处理一些关键业务时，HTTPS双向认证通过对通信双方做双向认证，为您的业务提供更高的安全性。本文为您介绍如何使用CLB部署HTTPS双向认证。

配置步骤

本指南中使用自签名的CA证书为客户端证书签名，完成以下操作配置HTTPS监听（双向认证）：

前提条件

- 您已通过OpenSSL官网下载并安装 OpenSSL 工具（1.1.1 或以上版本）。
- 您已经创建了实例ECS01和ECS02，并部署了2个不同的应用服务。具体操作，请参见使用向导创建实例。

步骤一：准备服务器证书

您可以通过浏览器检查服务器发送的证书是否是由自己信赖的中心签发的。您可以向阿里云云盾SSL证书购买服务器证书，或者向其他服务商处购买。更多信息，请参见上传证书。

步骤二：使用OpenSSL生成CA证书

1. 打开命令窗口，执行以下命令在*/root*目录下新建一个*ca*文件夹，并在*ca*文件夹下创建四个子文件夹。

```
sudo mkdir ca
 cd ca
 sudo mkdir newcerts private conf server
```

其中：

- *newcerts*文件夹：用于存放CA签署过的数字证书（证书备份目录）。
- *private*文件夹：用于存放CA的私钥。
- *conf*文件夹：用于存放一些简化参数用的配置文件。
- *server*文件夹：用于存放服务器证书文件。

2. 执行以下命令，在*conf*目录下新建一个包含以下信息的*openssl.conf*文件。

```
[ ca ]
 default_ca = foo
 [ foo ]
 dir = /root/ca
 database = /root/ca/index.txt
 new_certs_dir = /root/ca/newcerts
 certificate = /root/ca/private/ca.crt
 serial = /root/ca/serial
 private_key = /root/ca/private/ca.key
 RANDFILE = /root/ca/private/.rand
 default_days = 365
 default_crl_days= 30按照提示输入客户端c
 default_md = md5
 unique_subject = no
 policy = policy_any
 [ policy_any ]
 countryName = match
 stateOrProvinceName = match
 organizationName = match
 organizationalUnitName = match
 localityName = optional
 commonName = supplied
 emailAddress = optional
```

3. 依次执行以下命令，生成私钥key文件。

```
cd /root/ca
    sudo openssl genrsa -out private/ca.key
```

运行结果如下图所示：

```
root@iZ[redacted]1iZ:~/ca/conf# cd /root/ca
root@iZ[redacted]iZ:~/ca# sudo openssl genrsa -out private/ca.key
Generating RSA private key, 2048 bit long modulus
.....+++
..+++
e is 65537 (0x10001)
```

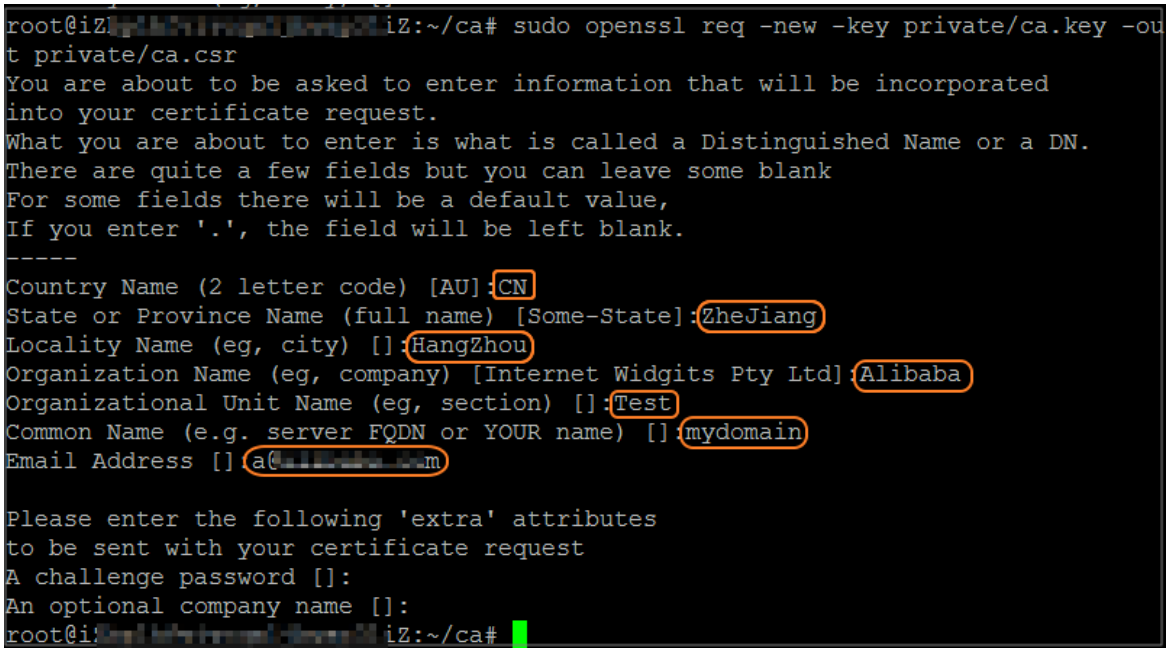
4. 执行以下命令并按照界面提示输入对应信息，生成证书请求*csr*文件。

```
  sudo openssl req -new -key private/ca.key -out private/ca.csr
```

运行结果如下图所示，供您参考。*Common Name*需要输入您的

传统型负载均衡CLB

的域名。



5. 运行以下命令生成凭证*crt*文件。

```
sudo openssl x509 -req -days 365 -in private/ca.csr -signkey private/ca.key -out priv
ate/ca.crt
```

6. 运行以下命令为CA的key设置起始序列号。

   起始序列号可以是任意四个字符。本示例中您可以自定义*FACE*。

```
sudo echo FACE > serial
```

7. 运行以下命令创建CA键库。

```
sudo touch index.txt
```

步骤三：生成客户端证书

1. 打开命令窗口，执行以下命令，在*ca*目录内创建一个存放客户端key的目录*users*。

```
sudo mkdir users
```

2. 完成以下操作为客户端创建一个key。

   i. 执行以下命令。

```
sudo openssl genrsa -des3 -out /root/ca/users/client.key 1024
```

   ii. 根据提示，输入pass phrase。

   pass phrase是当前key的口令，以防止本密钥泄漏后被人盗用。两次输入同一个密码。

3. 执行以下命令为客户端key创建一个证书签名请求*csr*文件。

```
sudo openssl req -new -key /root/ca/users/client.key -out /root/ca/users/client.csr
```

输入该命令后，根据提示输入步骤2输入的pass phrase，然后根据提示，提供对应的信息。

> **说明** `A challenge password` 是客户端证书口令（请注意将它和 `client.key` 的口令区分开，`client.key` 为客户端密钥，本教程设置密码为test），可以与服务器端证书或者根证书口令一致。

运行结果如下图所示：

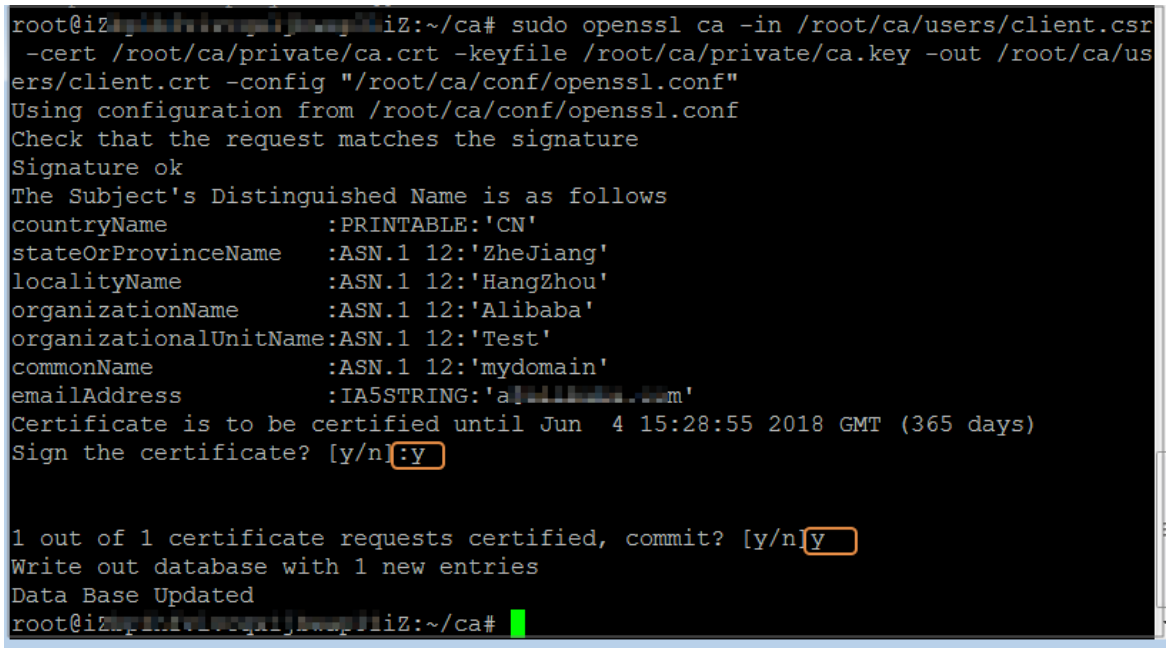
```
root@iZ[redacted]1iZ:~/ca# sudo openssl req -new -key private/ca.key -ou
t private/ca.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CN
State or Province Name (full name) [Some-State]:ZheJiang
Locality Name (eg, city) []:HangZhou
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Alibaba
Organizational Unit Name (eg, section) []:Test
Common Name (e.g. server FQDN or YOUR name) []:mydomain
Email Address []:a@[redacted]m

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
root@iZ[redacted]1iZ:~/ca#
```

4. 执行以下命令，使用步骤二：使用OpenSSL生成CA证书中的CA Key为刚才的客户端key签名。

```
sudo openssl ca -in /root/ca/users/client.csr -cert /root/ca/private/ca.crt -keyfile
/root/ca/private/ca.key -out /root/ca/users/client.crt -config "/root/ca/conf/openssl.c
onf"
```

当出现确认是否签名的提示时，两次都输入*y*。

运行结果如下图所示：

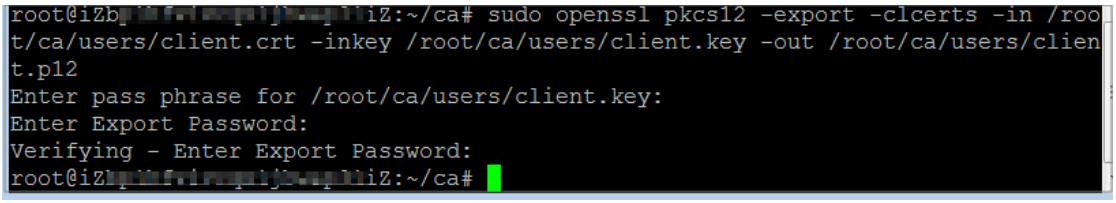


5. 完成以下操作将证书转换为浏览器可以识别的*PKCS12*文件。
   i. 执行以下命令。

   ```
   sudo openssl pkcs12 -export -clcerts -in /root/ca/users/client.crt -inkey /root/ca/users/client.key -out /root/ca/users/client.p12
   ```

   ii. 按照提示输入客户端client.key的pass phrase。
   iii. 输入用于导出证书的密码。此密码为客户端证书的保护密码，在安装客户端证书时需要输入该密码。

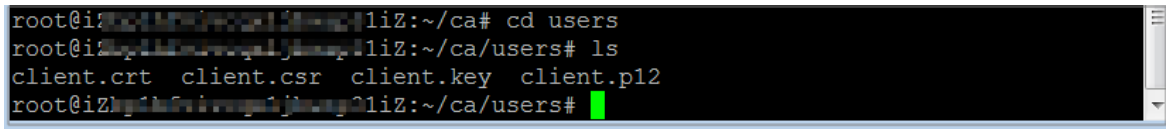
   运行结果如下图所示：



6. 执行以下命令查看生成的客户端证书。

   ```
   cd users
    ls
   ```

   运行结果如下图所示：



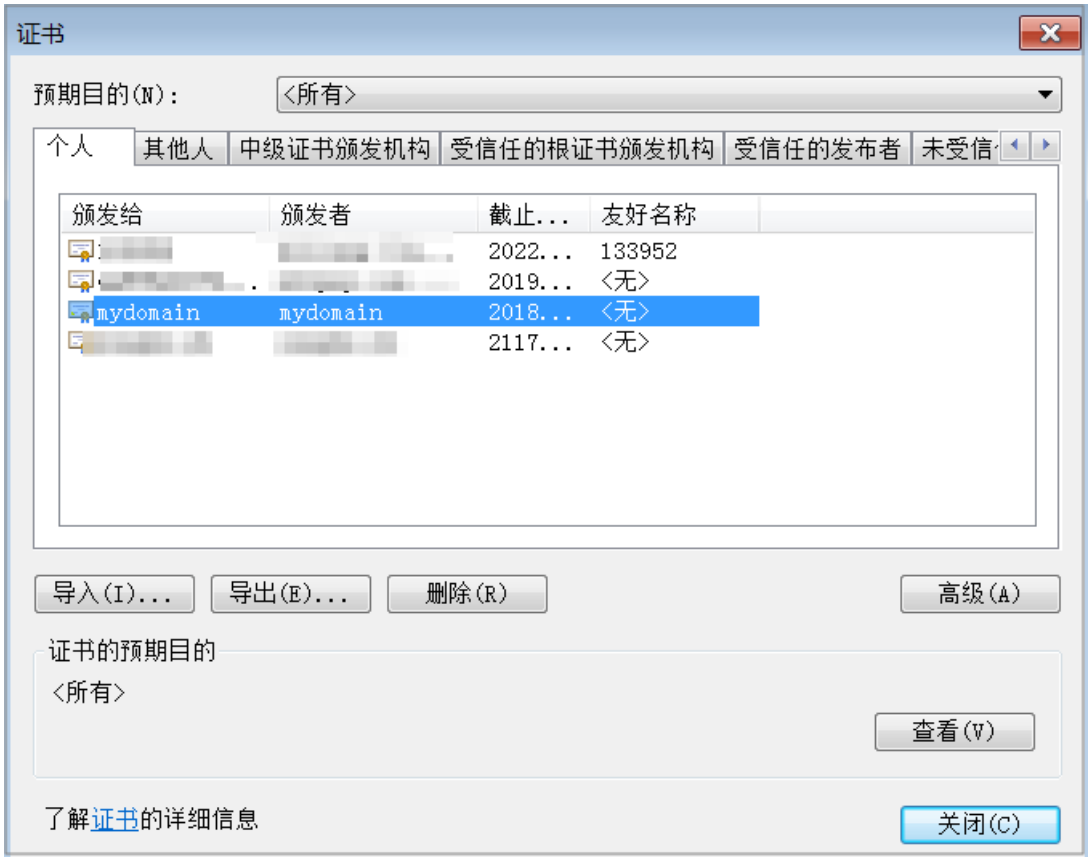
步骤四：安装客户端证书

将生成的客户端证书安装到客户端。本教程以Windows客户端，IE浏览器为例。

1. 打开命令行窗口，执行以下命令导出步骤三：生成客户端证书中生成的客户端证书。

```
scp root@IPaddress:/root/ca/users/client.p12 ./          //IPaddress是生成客户端证书的服务器的IP地址
```

2. 在IE浏览器中导入下载的客户端证书。
   i. 打开IE浏览器，选择**设置** > **Internet选项**。
   ii. 单击**内容**页签，然后单击**证书**，导入下载的客户端证书。在导入证书时需要输入步骤三：生成客户端证书生成*PKCS12*文件的密码。



步骤五：上传服务器证书和CA证书

1. 登录传统型负载均衡CLB控制台。
2. 在左侧导航栏，选择**传统型负载均衡 CLB(原SLB)** > **证书管理**，然后单击**创建证书**，上传服务器证书。
3. 在**创建证书**面板，单击**上传非阿里云签发证书**，完成以下配置，然后单击**创建**。

配置	说明
证书名称	输入证书名称。 名称长度限制为1~80个字符，只能包含字母、数字、连接号（-）、正斜线（/）、英文句点（.）、下划线（_）和星号（*）。
组织	选择证书所属的组织。
资源集	选择证书所属的资源集。

配置	说明
证书类型	本文选择**服务器证书**。
公钥证书	复制服务器证书内容。 单击**查看样例**查看正确的证书样式。详情参见证书要求。
私钥	复制服务器证书的私钥内容。 单击**查看样例**查看正确的证书样式。详情参见证书要求。 **注意** 只有上传服务器证书时，才需要上传私钥。
证书部署地域	本文选择**华东1（杭州）**。

4. 在左侧导航栏，选择**传统型负载均衡 CLB(原SLB) > 证书管理**，然后单击**创建证书**，上传CA证书。
5. 在**创建证书**面板，单击**上传非阿里云签发证书**，完成以下配置，然后单击**创建**。

配置	说明
证书名称	输入证书名称。 名称长度限制为1~80个字符，只能包含字母、数字、连接号（-）、正斜线（/）、英文句点（.）、下划线（_）和星号（*）。
组织	选择证书所属的组织。
资源集	选择证书所属的资源集。
证书类型	本文选择**CA证书**。
客户端CA公钥证书	上传客户端CA公钥证书。 单击**查看样例**查看正确的证书样式。详情参见证书要求。
证书部署地域	本文选择**华东1（杭州）**。

步骤六：配置HTTPS双向认证监听

1. 登录传统型负载均衡CLB控制台。
2. 在**实例管理**页面，单击**创建传统型负载均衡**。
3. 配置负载均衡实例，单击**立即购买**完成支付。

   实例类型选择**公网**，地域选择**华东1（杭州）**。详细配置信息请参见创建实例。
4. 创建成功后，返回**实例管理**页面，选择**华东1（杭州）**地域。
5. 单击已创建的负载均衡实例ID链接，或者在操作列单击**监听配置向导**。
6. 在**监听**页签下，单击**添加监听**。
7. 在**协议&监听**页签下，完成以下配置，然后单击**下一步**。

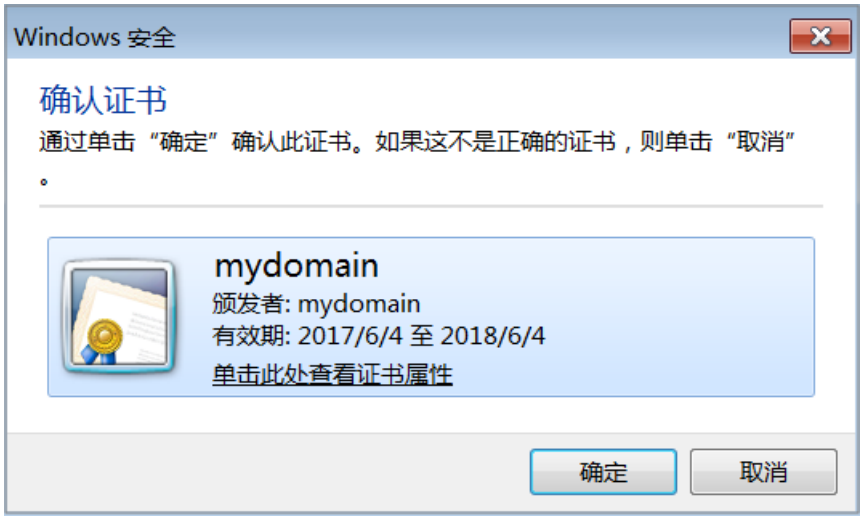
- **选择负载均衡协议**：HTTPS
- **监听端口**：*443*
- **调度算法**：轮询（RR）

8. 在**SSL证书**页签下，选择已上传的服务器证书。
9. 单击**高级设置**后面的**修改**，打开双向认证，选择已上传的CA证书，然后单击**下一步**。
10. 选择**默认服务器组**，单击**继续添加**，添加ECS服务器，后端协议监听端口设置为*443*。
11. 其他参数保持默认值，单击**下一步**至**提交**，完成负载均衡实例配置。

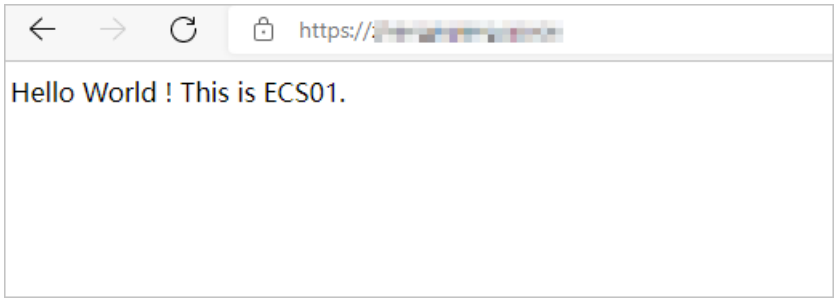
步骤七：测试HTTPS双向认证

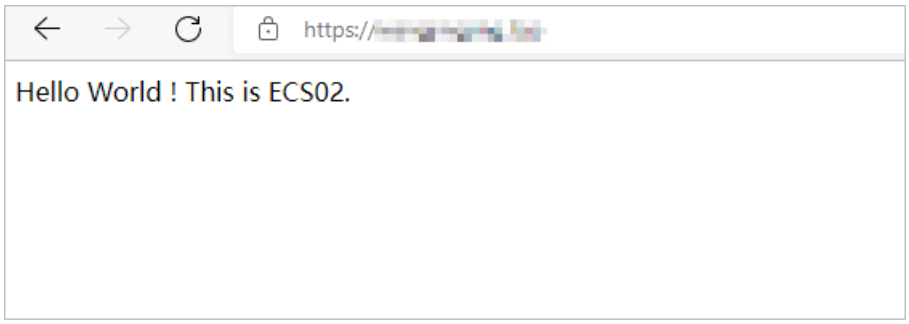
1. 在**实例管理**页面，查看健康检查状态。

   当状态为**正常**时，表示后端服务器可以正常接收处理负载均衡监听转发的请求。
2. 在浏览器中，输入负载均衡的公网服务地址，在弹出的对话框中根据提示确认证书。



3. 刷新浏览器，您可以观察到请求在两台ECS服务器之间转换。





2.3. 将HTTP访问重定向至HTTPS

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。

前提条件

您已经创建CLB实例，具体操作，请参见**创建实例**。

背景信息

本教程以将HTTP:80访问重定向转发至HTTPS:443为例。

步骤一：创建HTTPS监听

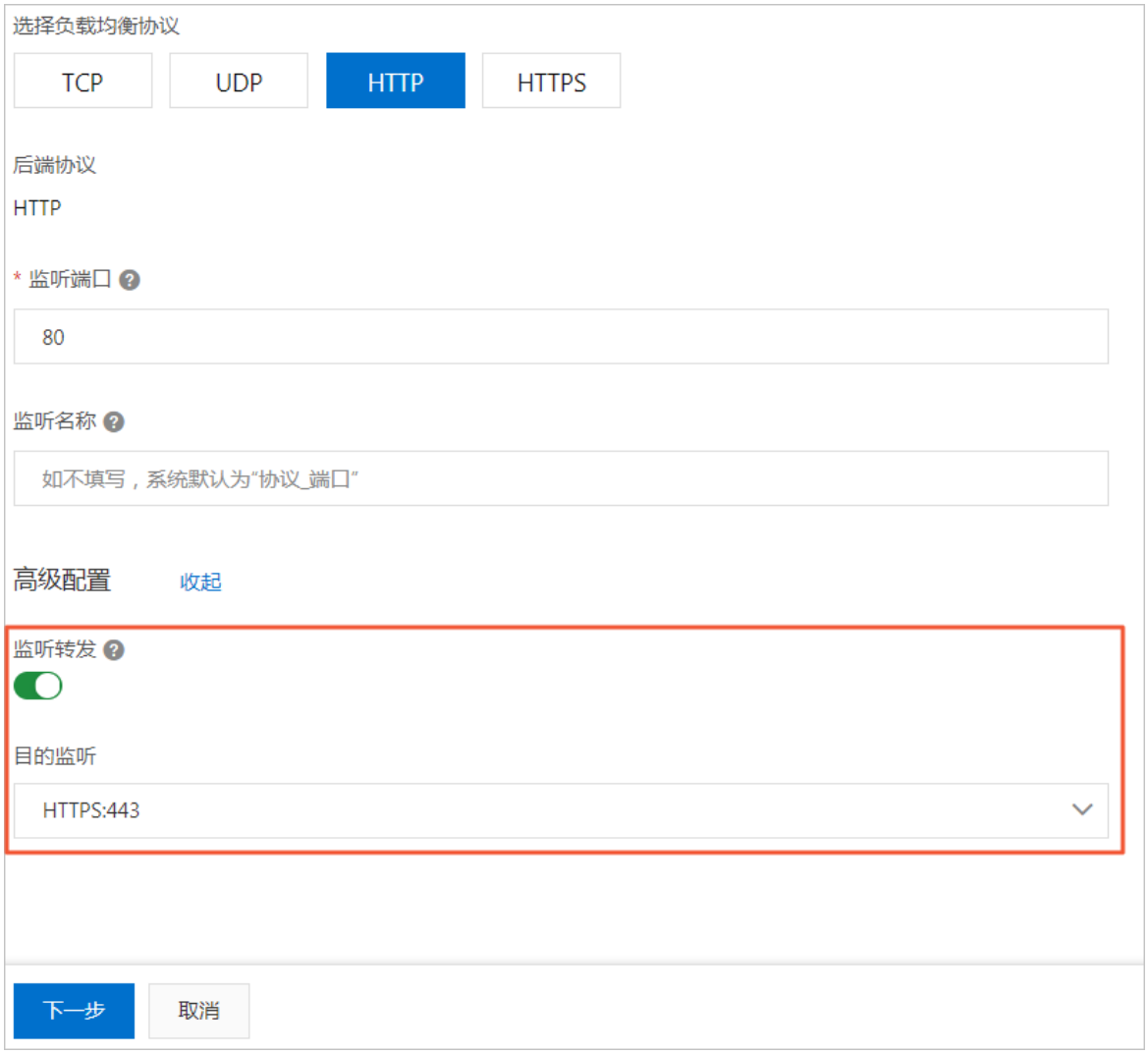
- 登录传统型负载均衡CLB控制台。
- 在顶部菜单栏选择负载均衡实例所属的地域。
- 选择以下一种方法，打开监听配置向导。
  - 在**实例管理**页面，找到目标实例，然后在**操作**列单击**监听配置向导**。
  - 在**实例管理**页面，单击目标实例ID，然后在**监听**页签单击**添加监听**。
- 在**协议&监听**配置向导，根据以下信息配置监听，然后单击**下一步**。本文主要配置如下，关于其他配置参数及具体操作步骤，请参见**添加HTTPS监听**。
  - **选择负载均衡协议**：HTTPS。
  - **监听端口**：443。

步骤二：创建HTTP监听配置重定向

1. 登录传统型负载均衡CLB控制台。
2. 在顶部菜单栏选择负载均衡实例所属的地域。
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. 在**协议&监听**配置向导，负载均衡协议选择**HTTP**， 监听端口输入**80**。
5. 单击**高级配置**后的**修改**。
6. 开启**监听转发**，选择目的监听为**HTTPS:443**，单击**下一步**。



7. 确认后，单击**提交**，等待配置成功后，单击**知道了**。

2.4. 单CLB实例配置多域名HTTPS网站（HTTPS多域名）

本教程指导您如何给

传统型负载均衡CLB

实例HTTPS监听挂载多个证书，将来自不同域名的访问请求转发至不同的后端虚拟服务器组。

场景描述

本教程以华东1（杭州）地域的

CLB

实例CLB1为例。本教程指导您创建一个HTTPS监听，认证方式为单向认证，然后将来自域名为 `*.example.com` 的客户端请求转发至虚拟服务器组test1上，将来自域名为 `www.aliyundoc.com` 的客户端请求转发至虚拟服务器组test2上。

前提条件

- 在华东1（杭州）地域创建

  CLB

  实例CLB1。具体操作，请参见创建实例。
- 上传本教程中需要使用的证书。具体操作，请参见概述。
  - 监听使用的默认证书为default。
  - 域名 `*.example.com` 使用的证书为example1。
  - 域名 `www.aliyundoc.com` 使用的证书为example2。

步骤一：添加HTTPS监听

完成以下操作，添加HTTPS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. 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**。
4. 配置监听。

   本操作的主要配置如下，其他配置请参见添加HTTPS监听。
   - **双向认证**：关闭。
   - **SSL证书**：选择服务器证书default。
   - **后端服务器**：需要创建test1和test2两个虚拟服务器组。

步骤二：配置转发规则

完成以下操作，配置转发规则：

1. 在**实例管理**页面，单击CLB1实例ID。
2. 在**监听**页签，找到已创建的HTTPS监听，然后在**操作**列单击**配置转发策略**。
3. 在**转发策略**面板，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。

本教程中配置域名转发规则，URL不进行设置。

- 设置规则名称，在**域名**列输入 `*.example.com` ，选择test1虚拟服务器组，单击**添加转发策略**。
- 设置规则名称，在**域名**列输入 `www.aliyundoc.com` ，选择test2虚拟服务器组，单击**添加转发策略**。

> **说明** 转发规则中设置的域名，必须与证书中和步骤三：添加扩展域名中添加的扩展域名保持一致。

步骤三：添加扩展域名

完成以下操作，添加扩展域名：

1. 在**实例管理**页面，单击CLB1实例ID。
2. 在**监听**页签，找到已创建的HTTPS监听，然后在**操作**列选择 > **扩展域名管理**。
3. 在**扩展域名管理**面板，单击**添加扩展域名**，配置扩展域名，然后单击**确定**。
   - 输入域名。域名只能使用字母、数字、短划线（-）和半角句号（.）。

     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和*.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。

       > **说明** 在下表中，✓表示支持，×表示不支持。

模式	请求测试URL	配置的转发域名策略		
		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	×	×	✓

   - 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。

> **注意** 配置完成后，如果出现问题，请尝试重启浏览器后再测试，避免缓存对结果的影响。

2.5. 基于域名或URL路径进行转发

传统型负载均衡CLB

的七层监听（HTTPS与HTTP协议）支持配置基于域名或URL路径的转发策略。您可以将来自不同域名或URL路径的请求转发至不同的后端服务器组，合理分配服务器资源。

域名和URL路径转发原理介绍

URL路径转发支持字符串匹配，按照前缀最长匹配原则。例如您配置了*/abc*和*/abcd*两个规则，当您访问*/abcde*时，系统优先匹配*/abcd*规则。

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`。

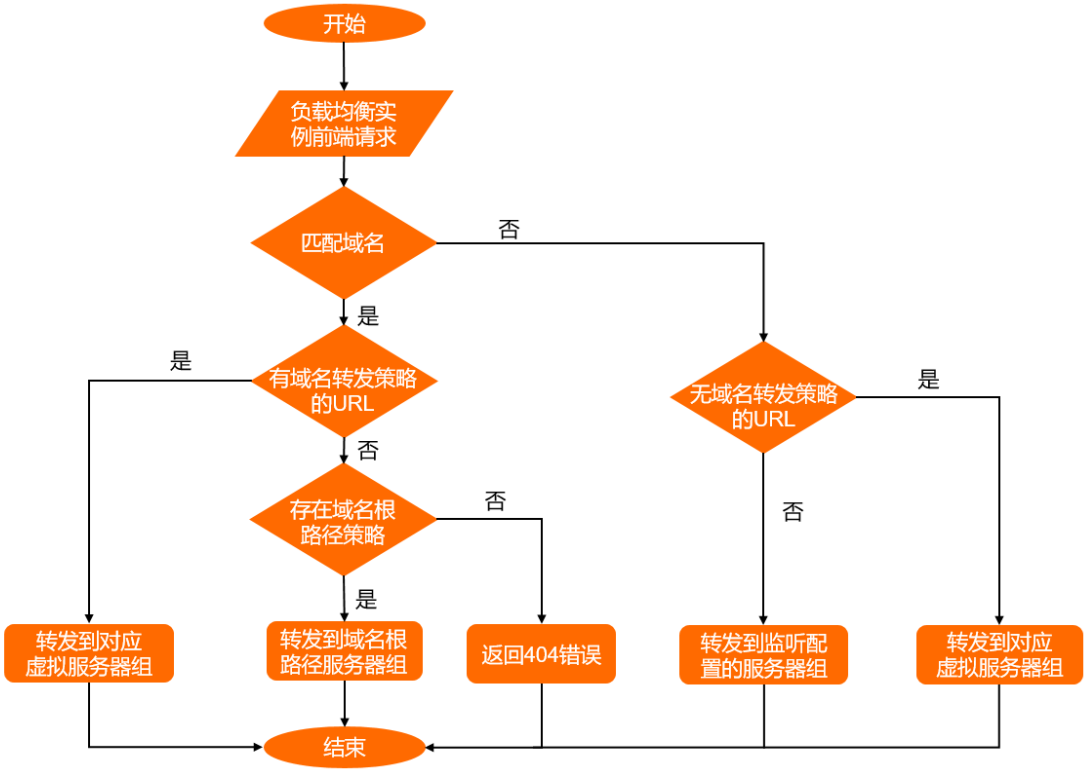
  当前端请求同时匹配多条域名策略时，策略的匹配优先级为：精确匹配>小范围通配符匹配>大范围通配符匹配。

  > **说明** 下表中”✓“代表匹配，“×”代表不匹配。

模式	请求测试URL	配置的转发域名策略		
		www.aliyun.com	*.aliyun.com	*.market.aliyun.com
精确匹配	www.aliyun.com	✓	×	×
泛域名匹配	market.aliyun.com	×	✓	×
	info.market.aliyun.com	×	×	✓

您可以在一个监听下添加多条转发策略，每条转发策略关联不同的虚拟服务器组（一个虚拟服务器组由一组ECS实例组成）。例如您可以将所有读请求转发至一组后端服务器上，而将写请求转发至另一组后端服务器上，这样可以更灵活地适配业务需求，合理分配资源。

如下图所示，在配置了转发策略后，负载均衡系统将按照以下两种方式匹配策略，转发前端请求：



- 方式一：前端请求中存在域名，则根据域名匹配转发策略。
  - 存在匹配该域名的转发策略，则继续匹配URL路径部分。

    若URL路径部分也能匹配，则将请求转发至对应的虚拟服务器组；若URL路径部分未能命中该域名下的任何规则，则将请求转发给域名根路径转发策略（转发策略中只配置了域名，没有配置URL路径）。

    当用户没有为该域名配置根路径转发策略时，将向客户端返回404错误。
  - 不存在匹配该域名的转发策略，则按照方式二匹配转发策略。
- 方式二：前端请求中不存在域名或者转发策略中不存在与之相匹配的域名，则直接匹配无域名转发策略（转发策略中只配置了URL，没有配置域名）。

  成功匹配到转发策略时，将请求转发至对应的虚拟服务器组；未能匹配到任何转发策略时，将请求转发至此监听配置的服务器组。

前提条件

- 您已创建

  CLB

  实例，并为该实例配置了HTTP监听或者HTTPS监听。具体操作，请参见添加HTTP监听或添加HTTPS监听。
- 您已创建虚拟服务器组。具体操作，请参见创建虚拟服务器组。

添加域名或URL路径转发策略

1. 登录传统型负载均衡CLB控制台。
2. 选择目标

CLB

实例所属地域。

3. 在**实例管理**页面，单击目标实例ID链接。
4. 在**监听**页签，在目标七层监听**操作**列单击**配置转发策略**。
5. 在**转发策略**面板，根据以下信息配置转发策略，配置完成后单击**添加转发策略**。

- **域名**：输入要转发的请求域名。域名只能使用字母、数字、短划线（-）和半角句号（.）。
- **URL**：输入请求路径。路径必须以正斜线（/）开头，只能包含字母、数字、短划线（-）、半角句号（.）、正斜线（/）、百分号（%）、半角问号（?）、井号（#）和and（&）。

  > **说明** 如果请求的URL路径中包含特殊字符，您需要使用URL特殊字符转义编码。例如，如果配置的转发策略使用包含特殊字符“/#/”的URL路径，那么在访问对应的服务时，需要使用特殊字符井号（#）的转义编码“%23”，即请求的URL路径中必须是“/%23/”，这样才能按设定的转发规则转发请求。

- **虚拟服务器组**：选择关联的虚拟服务器组。
- **备注**：输入备注信息。
- **添加转发策略**：选择是否需要再添加一个转发策略。

6. （可选）单击**添加域名**或**添加规则**新增一个域名或URL策略。

   一个HTTP或HTTPS监听最多可添加的转发策略个数，请参见使用限制。

编辑转发策略

您可以修改转发策略关联的后端服务器。

1. 登录传统型负载均衡CLB控制台。
2. 选择目标

   CLB

   实例所属地域。
3. 在**实例管理**页面，单击目标实例ID链接。
4. 在**监听**页签，在目标七层监听**操作**列单击**配置转发策略**。
5. 在**转发策略**面板的**转发策略列表**区域，在目标转发策略的**操作**列单击**编辑**选项。
6. 在**编辑转发策略**面板，修改目标转发策略的备注和虚拟服务器组。
7. 您可以根据需要打开**转发规则高级配置**，根据以下信息完成配置，然后单击**确定**。

高级配置	说明
调度算法	选择调度算法。 ○ **加权轮询**：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**：按照访问顺序依次将外部请求依序分发到后端服务器。
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/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/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。更多信息，请参见会话保持规则配置。

高级配置	说明
开启健康检查	○ **健康检查方法**：本文默认为**HEAD**。 ○ **健康检查端口**：健康检查服务访问后端时的探测端口。 默认值为配置监听时指定的后端端口。 ○ **健康检查路径**：用于健康检查页面文件的URI，建议对静态页面进行检查。 ○ **健康检查域名（可选）**：默认使用各后端服务器的内网IP为域名。 ○ **正常状态码**：选择健康检查正常的HTTP状态码。 默认值为http_2xx和http_3xx。 ○ **健康检查响应超时时间**：接收来自运行状况检查的响应需要等待的时间。如果后端ECS在指定的时间内没有正确响应，则判定为健康检查失败。 ○ **健康检查间隔时间**：进行健康检查的时间间隔。 默认为2秒。 ○ **健康不检查健康阈值**：同一LVS节点服务器针对同一ECS服务器，从成功到失败的连续健康检查失败次数。 可选值2~10，默认为3次。 ○ **健康检查健康阈值**：同一LVS节点服务器针对同一ECS服务器，从失败到成功的连续健康检查成功次数。 可选值2~10，默认为3次。

删除转发策略

1. 登录传统型负载均衡CLB控制台。
2. 选择目标

   CLB

   实例所属地域。
3. 在**实例管理**页面，单击目标实例的ID链接。
4. 在**监听**页签，在目标七层监听**操作**列单击**配置转发策略**。
5. 在**转发策略**面板的**转发策略列表**区域，在目标转发策略的**操作**列单击**删除**。

相关文档

- CreateDomainExtension：调用CreateDomainExtension创建扩展域名。
- DescribeDomainExtensionAttribute：调用DescribeDomainExtensionAttribute查询已添加的扩展域名属性。
- SetDomainExtensionAttribute：调用SetDomainExtensionAttribute修改扩展域名的证书。
- DescribeDomainExtensions：调用DescribeDomainExtensions查询已添加的扩展域名。
- DeleteDomainExtension：调用DeleteDomainExtension删除扩展域名。

2.6. 相同域名不同路径的流量转发

传统型负载均衡CLB

支持配置基于域名和路径的转发策略。您可以将来自相同域名不同路径的请求转发给不同的后端服务器组，合理分配服务器资源。

背景信息

> **说明** 只有7层监听（HTTPS或HTTP协议）支持配置转发策略。

本教程以四个部署了Nginx服务器的ECS为例，演示如何通过配置域名加URL转发规则，完成如下表所示的流量转发。

前端请求	流量转发至
www.example.com/tom	后端服务器SLB_tom1和SLB_tom2，属于虚拟服务器组TOM。
www.example.com/jerry	后端服务器SLB_jerry1和SLB_jerry2，属于虚拟服务器组JERRY。

前提条件

1. 已创建一个公网

   CLB

   实例。具体操作，请参见创建实例。
2. 已创建一个七层监听，调度算法选择**轮询（RR）**。具体操作，请参见添加HTTP监听或添加HTTPS监听。
3. 已创建两个虚拟服务器组TOM和JERRY。具体操作，请参见创建虚拟服务器组。
   - 虚拟服务器组TOM中添加服务器SLB_tom1和SLB_tom2，将端口设置为80，权重使用默认值100。
   - 虚拟服务器组JERRY中添加服务器SLB_jerry1和SLB_jerry2，将端口设置为80，权重使用默认值100。

配置转发策略

执行下面的操作步骤配置路径转发策略：

1. 在顶部菜单栏，选择

   CLB

   实例的所属地域。
2. 在**实例管理**页面，单击目标实例ID。
3. 在**监听**页签，在目标七层监听的**操作**列单击**配置转发策略**。
4. 配置两条转发规则：将来自*www.example.com/tom*的请求转发至虚拟服务器组TOM，以及将来自*www.example.com/jerry*的请求转发至虚拟服务器组JERRY。

参数说明如下：

- **域名**：输入要转发的请求域名。域名只能使用字母、数字、短划线（-）和半角句号（.）。
- **URL**：输入请求路径。路径必须以正斜线（/）开头，只能包含字母、数字和特殊字符 `-./%?#&` 。

> **说明** 如果您只想配置域名转发策略，则不需要配置URL。

- **虚拟服务器组**：选择关联的虚拟服务器组。
- **备注**：输入描述。

> **说明** 一个HTTP或HTTPS监听最多可添加转发策略个数请参见使用限制。

5. 单击**添加转发策略**，然后单击**确定**。
6. 验证转发策略是否配置成功。
   - 在浏览器中输入*www.example.com/jerry*，将返回如下结果：`This is Jerry2!` 。
   - 在浏览器中输入*www.example.com/tom*，将返回如下结果：`This is Tom1.` 。
   - 在浏览器中输入*www.example.com*，将返回如下结果：`Welcome to nginx!` 。

相关文档

- 域名和URL路径转发原理介绍

2.7. 保留客户端真实源地址（七层监听）

您可以通过设置负载均衡的七层监听服务保留客户端的真实源IP地址。

背景信息

七层负载均衡（HTTP或HTTPS协议）服务需要对应用服务器进行配置，然后使用 `X-Forwarded-For` 的方式获取客户端的真实源IP地址。真实的客户端源IP存放在HTTP头部的X-Forwarded-For字段，格式如下：

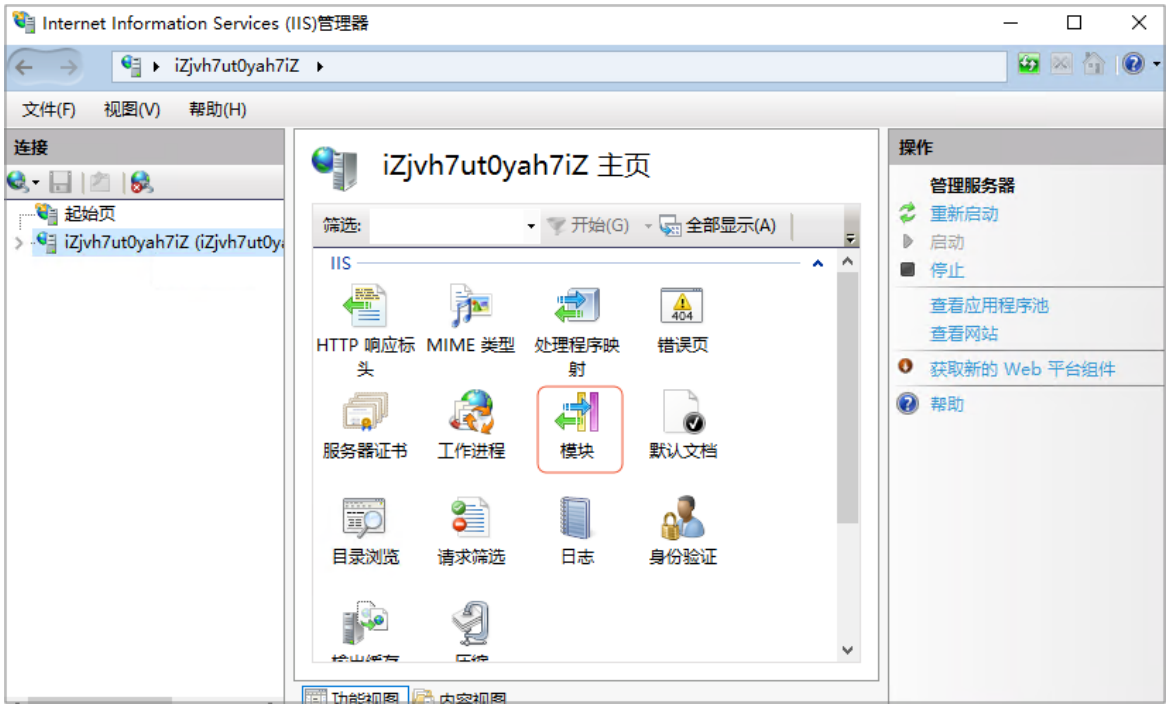
```
X-Forwarded-For：用户真实IP，代理服务器1-IP， 代理服务器2-IP，...
```

当使用此方式获取客户端真实IP时，获取的第一个地址就是客户端真实IP。

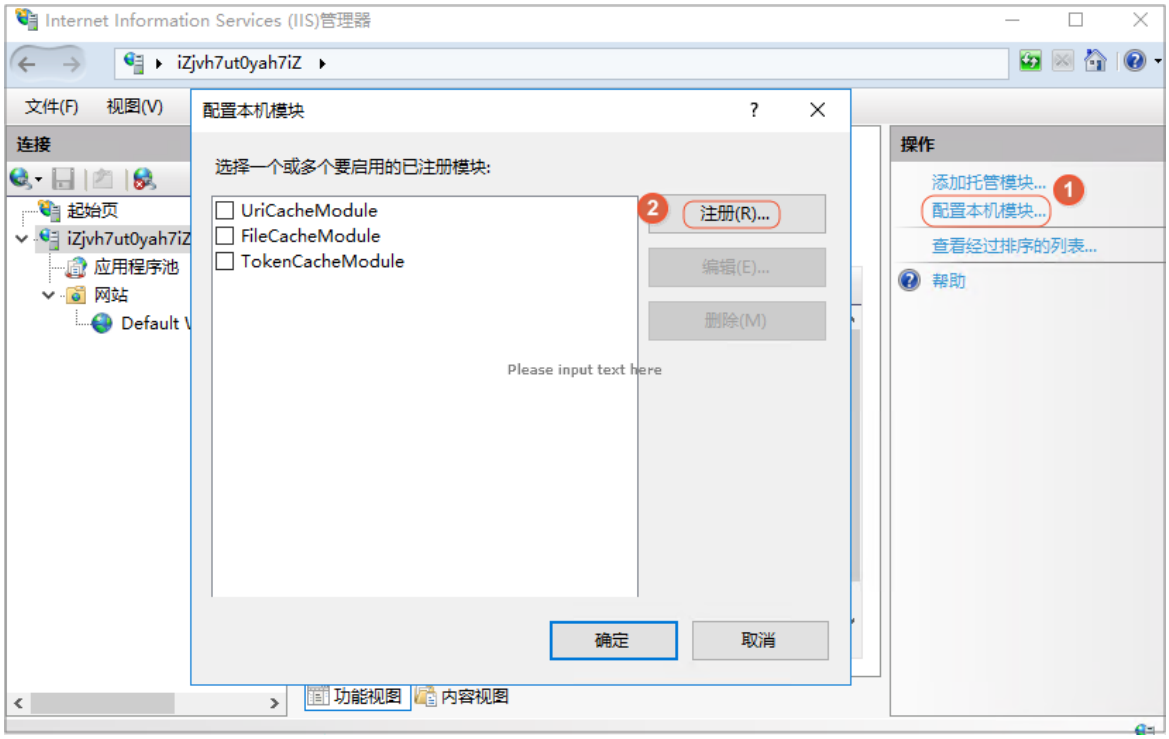
> **说明** 负载均衡的HTTPS监听是在负载均衡服务上的加密控制，后端仍旧使用HTTP协议，因此，在Web应用服务器上配置HTTPS和HTTP监听没有区别。

配置IIS7或IIS8服务器

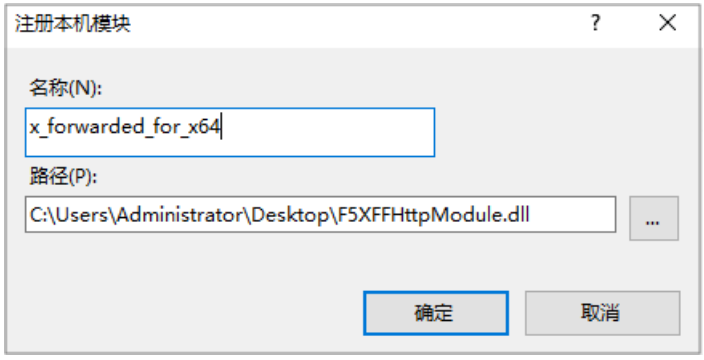
1. 下载并解压F5XForwardedFor文件。
2. 根据自己的服务器操作系统版本将*x86*\或*x64*\目录下的*F5XFFHttpModule.dll*和*F5XFFHttpModule.ini*拷贝到某个目录，例如*C:\F5XForwardedFor*\。确保IIS进程对该目录有读取权限。
3. 打开**IIS管理器**，双击**模块**功能。



4. 单击**配置本机模块**，然后在弹出的对话框中，单击**注册**。

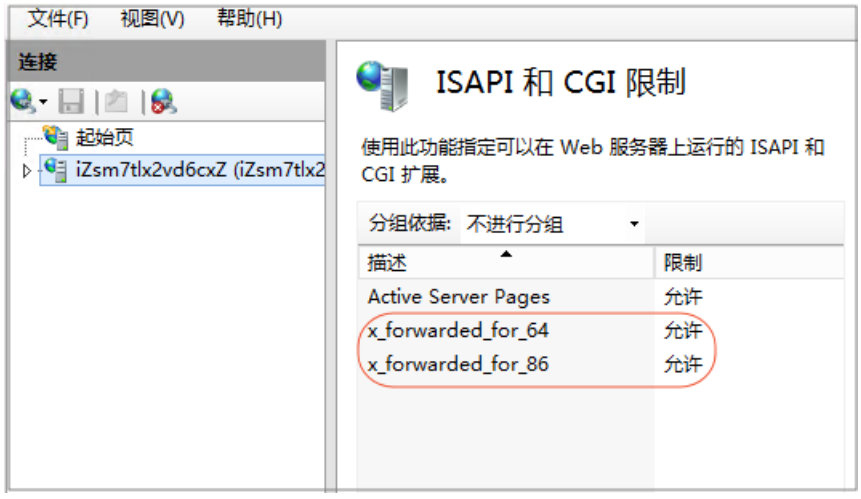


5. 添加下载的*.dll*文件。



6. 为添加的两个文件授权允许运行ISAPI和CGI扩展。

> 说明 确保您已经安装了ISAPI和CGI应用程序。



7. 重启IIS服务器，等待配置生效。

配置Apache服务器

本文以安装目录*alidata/*为例，执行命令的时候，请以实际路径为准。

1. 执行以下命令，安装Apache的一个第三方模块mod_rpaf。

```
wget https://github.com/gnif/mod_rpaf/archive/v0.6.0.tar.gz
tar zxvf v0.6.0.tar.gz
sudo apt-get install apache2-dev
whereis apxs2
cd mod_rpaf-0.6.0/alidata/server/httpd/bin/apxs -i -c -n mod_rpaf-2.0.so mod_rpaf-2.0.
c
```

2. 修改Apache的配置文件*/alidata/server/httpd/conf/httpd.conf*，在最末尾添加以下配置信息。

```
LoadModule rpaf_module modules/mod_rpaf-2.0.so
RPAFenable On
RPAFsethostname On
RPAFproxy_ips  <IP_address>
RPAFheader X-Forwarded-For
```

> **说明** 如果您要获取代理服务器的地址，可以将代理服务器的网段添加到 `RPAFproxy_ips <IP_address>` ，如负载均衡的IP地址段100.64.0.0/10（100.64.0.0/10是阿里云保留地址，其他用户无法分配到该网段内，不会存在安全风险）和高防IP地址段。多个IP地址段用半角逗号（,）分隔。

3. 添加完成后重启Apache。

```
/alidata/server/httpd/bin/apachectl restart
```

配置Nginx服务器

本文以安装目录*alidata/*为例，执行命令的时候，请以实际路径为准。

1. 执行以下命令，安装http_realip_module。

```
wget http://nginx.org/download/nginx-1.0.12.tar.gz
tar zxvf nginx-1.0.12.tar.gz
cd nginx-1.0.12
./configure --user=www --group=www --prefix=/alidata/server/nginx --with-http_stub_sta
tus_module --without-http-cache --with-http_ssl_module --with-http_realip_module
make
make install
kill -USR2 `cat /alidata/server/nginx/logs/nginx.pid`
kill -QUIT `cat /alidata/server/nginx/logs/ nginx.pid.oldbin`
```

2. 执行以下命令，打开*nginx.conf*文件。

```
vi /alidata/server/nginx/conf/nginx.conf
```

3. 在以下配置信息后添加新的配置字段和信息。

```
fastcgi connect_timeout 300;
fastcgi send_timeout 300;
fastcgi read_timeout 300;
fastcgi buffer_size 64k;
fastcgi buffers 4 64k;
fastcgi busy_buffers_size 128k;
fastcgi temp_file_write_size 128k;
```

需要添加的配置字段和信息为：

```
set_real_ip_from IP_address;
real_ip_header X-Forwarded-For;
```

> **说明** 如果您要获取代理服务器的地址，可以将代理服务器的网段添加到 `set_real_ip_from <IP_address>` ，如负载均衡的IP地址段100.64.0.0/10（100.64.0.0/10是阿里云保留地址，其他用户无法分配到该网段内，不会存在安全风险）和高防IP地址段。多个IP地址段用逗号分隔。

4. 执行以下命令，重启Nginx。

```
/alidata/server/nginx/sbin/nginx -s reload
```

2.8. 在弹性伸缩中使用传统型负载均衡

伸缩组支持关联传统型负载均衡CLB（原SLB）实例，通过CLB实例将访问流量分发到伸缩组内的多个ECS实例，有效增强伸缩组的服务能力。

前提条件

- 您持有一个或多个处于**运行中**状态的CLB实例。具体操作，请参见创建实例。
- CLB实例和伸缩组必须位于同一地域。
- 如果CLB实例和伸缩组的网络类型均为专有网络，则必须位于同一专有网络。
- 当CLB实例的网络类型为经典网络，伸缩组的网络类型为专有网络时，如果CLB实例的后端服务器组中包含专有网络ECS实例，该ECS实例必须与伸缩组位于同一专有网络。
- CLB实例配置至少一个监听。具体操作，请参见监听概述。
- CLB实例必须开启健康检查。具体操作，请参见配置健康检查。

背景信息

传统型负载均衡服务通过设置虚拟服务地址，将添加的同一地域的多个ECS实例虚拟成一个高性能、高可用的应用服务池。简单来说，传统型负载均衡服务通过组合CLB实例 、监听和后端服务器，提供流量分发控制服务。更多信息，请参见什么是传统型负载均衡CLB。

伸缩组关联CLB实例后，无论是伸缩组自动创建ECS实例，还是您向伸缩组手动添加ECS实例，ECS实例都会自动加入到CLB实例的后端服务器组。CLB实例会根据流量分发、健康检查等策略灵活使用ECS实例资源，在资源弹性的基础上大大提高资源可用性。

> **说明** 这些ECS实例的权重默认为50，您可以根据需要在对应CLB实例中调整权重，具体操作请参见编辑后端服务器的权重。

操作步骤

本步骤重点介绍CLB实例相关的控制台操作，如需了解其它配置，请参见创建伸缩组。

1. 登录弹性伸缩控制台。
2. 在左侧导航栏中，单击**伸缩组管理**。
3. 在顶部菜单栏处，选择地域。
4. 进入伸缩组关联CLB实例的页面。
   - 创建关联CLB实例的伸缩组时，单击**创建伸缩组**。
   - 修改未配置CLB实例的伸缩组时，找到待操作的伸缩组，在**操作**列中，单击**修改**。
5. 如果您在创建伸缩组，配置**网络类型**。
6. 配置**关联传统型负载均衡CLB（原SLB）**。
   i. 选择CLB实例。

      一个伸缩组默认最多可以关联30个CLB实例和5个虚拟服务器组。如需手动申请提升配额值，请前往配额中心申请。如果没有出现可选的CLB实例，请检查您的CLB实例是否满足前提条件。

   ii. 选择CLB实例的后端服务器组。

      伸缩组支持选择默认服务器组和虚拟服务器组。更多信息，请参见后端服务器概述。

      - 默认服务器组用于接收前端请求的ECS实例。如果监听没有设置虚拟服务器组或主备服务器组，默认将请求转发至默认服务器组中的ECS。
      - 虚拟服务器组用于将不同的请求转发到不同的后端服务器上，或通过域名和URL进行请求转发。
7. 根据需要配置其余选项。

相关文档

相关文档

- CreateScalingGroup
- AttachLoadBalancers
- DetachLoadBalancers
- AttachVServerGroups
- DetachVServerGroups

2.9. 通过Proxy Protocol获取客户端真实IP（四层监听）

您可以通过

传统型负载均衡CLB

的四层监听获取客户端真实IP地址。

背景信息

正常情况下，对于四层负载均衡，在后端服务器上获取的源IP即为客户端真实IP。但如果对客户端IP地址做了NAT转换，则后端服务器无法直接获取客户端的真实IP。

CLB

四层监听支持通过Proxy Protocol携带原始连接信息（源IP、目的IP、源端口、目的端口等）添加到TCP数据头中且不会丢弃或覆盖任何原有数据，

CLB

仅支持Proxy Protocol v2版本。更多信息，请参见The PROXY protocol。

适用场景

通过Proxy Protocol获取客户端真实IP适用于场景：

CLB

实例IP类型为IPv6，后端服务器的IP类型为IPv4。

前提条件

- 启用Proxy Protocol之前，请确保您的后端服务器支持Proxy Protocol v2版本，否则会导致新建连接失败。

  Nginx Plus R16及以后版本或者开源Nginx 1.13.11及以后版本支持Proxy Protocol v2版本。

- 如果实例的多个

  CLB

  监听挂载同一组后端服务器，必须将所有实例的监听都开启Proxy Protocol功能。

步骤一：创建TCP或UDP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. 在**实例管理**页面，找到目标实例，在**操作**列单击**监听配置向导**。
4. 根据配置向导，完成监听配置。
   - **选择负载均衡协议**：选择**TCP**或者**UDP**。
   - **ProxyProtocol配置**：在**高级配置**右侧单击**修改**，选中**通过ProxyProtocol协议携带客户端源地址到后端服务器**。

   更多参数说明，请参见添加TCP监听或添加UDP监听。

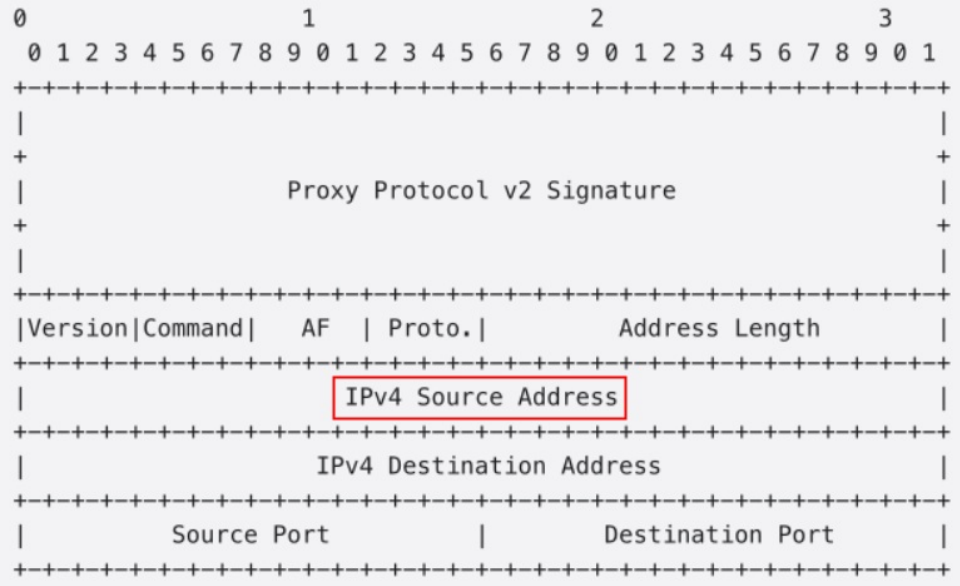
步骤二：配置Nginx服务器

执行以下命令，配置Proxy Protocol获取源地址功能。

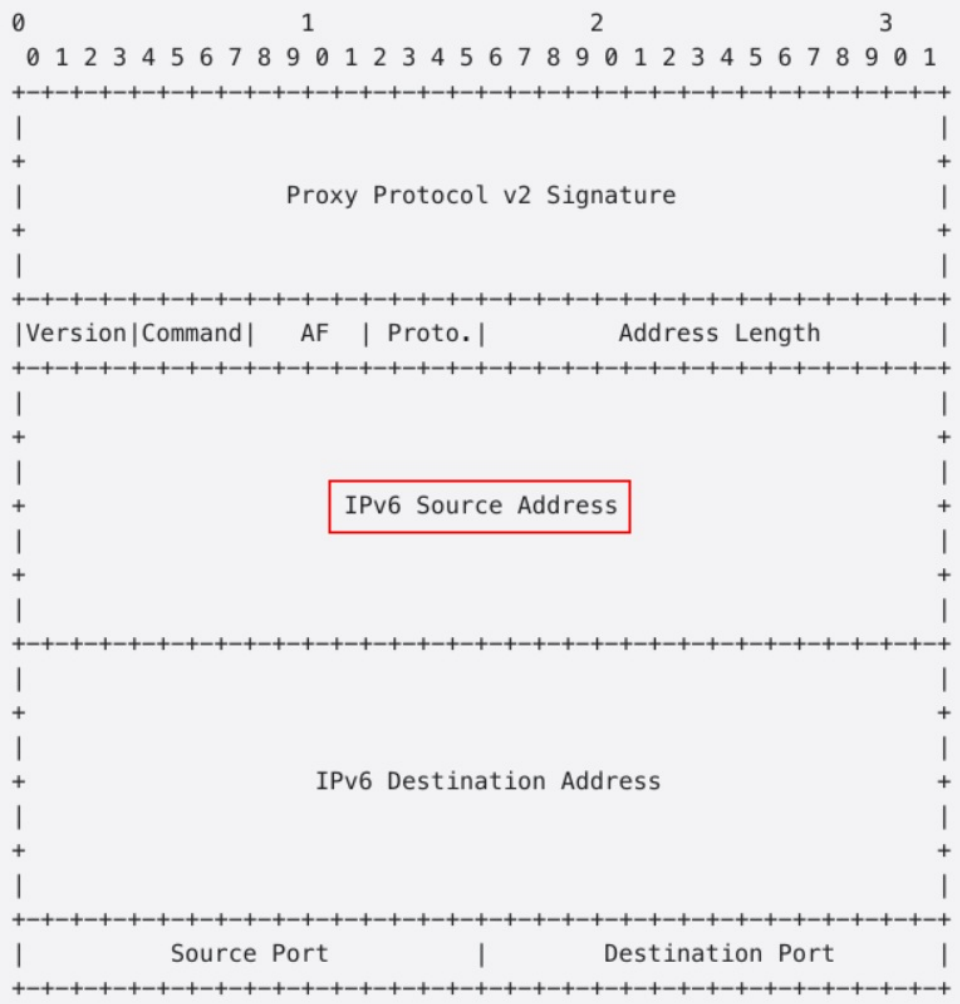
```
http {
    #...
    server {
        listen 80   proxy_protocol;
        listen 443  ssl proxy_protocol;
        #...
    }
}
stream {
    #...
    server {
        listen 12345 proxy_protocol;
        #...
    }
}
```

步骤三：获取客户端真实源IP地址

- 携带客户端IPv4地址的Proxy Protocol v2二进制头格式如下所示：



- 携带客户端IPv6地址的Proxy Protocol v2二进制头格式如下所示：



2.10. 压力测试的方法

四层负载均衡采用开源软件LVS（Linux Virtual Server）结合Keepalived的方式实现负载均衡，七层负载均衡由Tengine实现负载均衡。

压力测试建议

在进行压力测试时，配置建议如下：

- 压测负载均衡转发能力建议使用短连接。

  一般来说压测除了验证会话保持和均衡性等功能外，主要想验证负载均衡的转发能力，因此使用短连接比较合适，用于测试负载均衡和后端服务器的处理能力。使用短连接测试时，需要注意客户端端口不足的问题。

- 压测负载均衡吞吐量建议使用长连接，用于测试带宽上限或特殊业务。

  压测工具的超时时间建议设置为一个较小值，如5秒。超时时间太大的话，测试结果会体现在平均响应时间加长，不利于判断压测水位是否已到达。超时时间调小，测试结果会体现在成功率上，便于快速判断压测水位。

- 后端服务器提供一个静态网页用于压测，以避免应用逻辑带来的损耗。
- 压测时，监听配置建议如下：
  - 不开启会话保持功能，否则压力会集中在个别后端服务器。

- 关闭健康检查功能，减少健康检查对后端服务器的访问请求。
- 性能测试服务的5000并发规格能够提供5个及5个以上的公网IP。

压力测试工具建议

不建议您使用Apache ab作为压力测试工具：Apache ab在大量并发场景下存在3s、6s、9s阶梯式停顿的现象。Apache ab会通过判断content length来确定请求是否成功，而负载均衡挂载多台后端服务器时，返回的content length会不一致，导致测试结果有误。

可能导致压测性能低的原因

四层监听经过LVS后直接到达后端服务器；七层监听经过LVS后，还需要经过Tengine才到达后端服务器。

如果您使用七层监听进行压力测试，发现压测性能比较低。可能是以下原因造成的：

- 客户端端口不足。

  在进行压力测试时，客户端端口不足会导致建立连接失败。负载均衡会默认抹除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，即socket设置SO_LINGER属性。

- 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net.core.somaxconn的值为128，执行 `sysctl -w net.core.somaxconn=1024` 命令更改net.core.somaxconn的值，并重启后端服务器上的应用。

- 后端服务器连接过多。

  由于架构设计的原因，使用七层负载均衡时，用户长连接经过Tengine后变成短连接，可能导致后端服务器连接过多，从而表现为压测性能低。

- 后端服务器依赖的应用成为瓶颈。

  请求经过负载均衡到达后端服务器后，后端服务器本身负载正常，但由于所有的后端服务器上的应用又依赖其它应用，例如数据库，当数据库成为瓶颈时，也会引起性能降低。

- 后端服务器的健康检查状态异常。

  在压测时，容易忽略后端服务器的健康检查状态，如果有后端服务器健康检查失败或者健康检查状态经常跳跃（好到坏，又从坏到好，反复变化），也会导致压测性能低。

2.11. 使用访问日志快速定位异常后端服务器

某段时间客户端访问延迟时，您可以结合阿里云日志服务，通过仪表盘巡检，分析负载均衡的响应时间，快速定位异常后端服务器。

本教程介绍如何使用访问日志快速定位异常后端服务器，更多访问日志详情请参见配置访问日志。

步骤一：配置负载均衡访问日志

在配置访问日志前，请确保：

1. 您已经创建了七层负载均衡。
2. 您已经开通了日志服务。

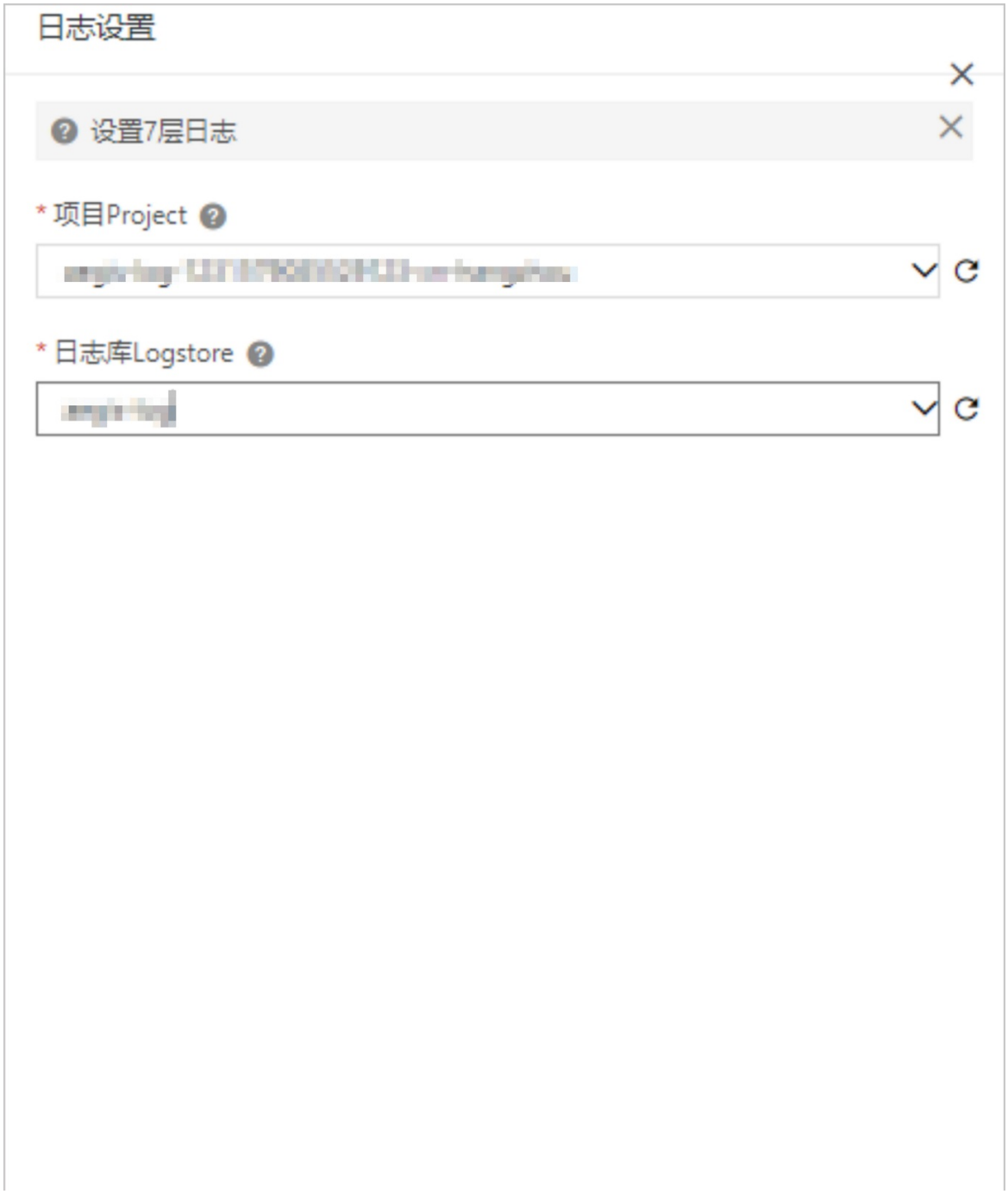
完成以下操作，配置访问日志：

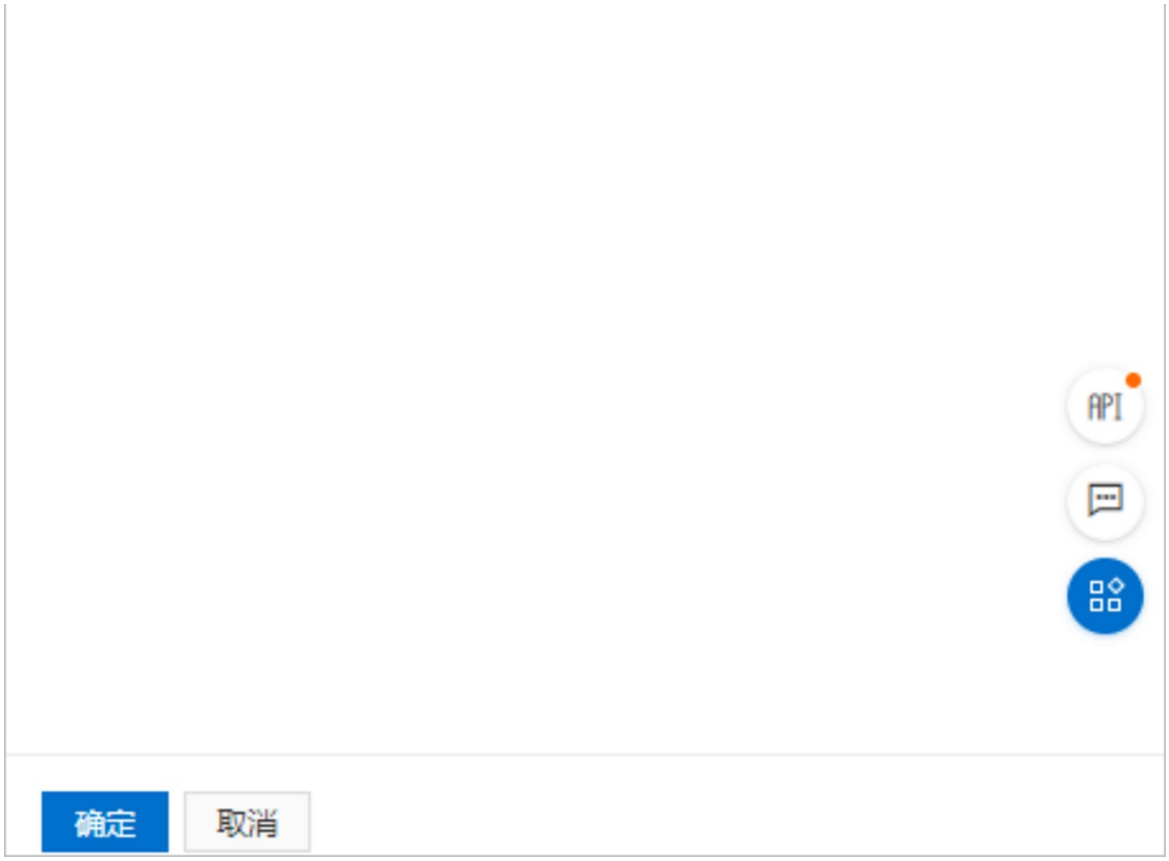
1. 登录负载均衡管理控制台。
2. 在左侧导航栏，选择 **日志管理 > 访问日志** 。
3. 选择实例的所属地域。
4. 单击**立即授权**，然后在弹出的对话框，单击**同意授权**授权SLB访问日志服务。

   如果您使用的是子账号，需要主账号进行授权。详情参见授权RAM用户（子账号）使用访问日志。

   > **说明** 该操作只有首次配置时需要。

5. 在**访问日志**页面，找到目标SLB实例，然后单击**设置**。
6. 选择日志服务（LogProject）和日志库（LogStore），然后单击**确定**





> **说明** 确保Project的名称全局唯一，且Project的地域和负载均衡实例的地域相同。

步骤二：查看访问日志

完成以下操作，查询访问日志：

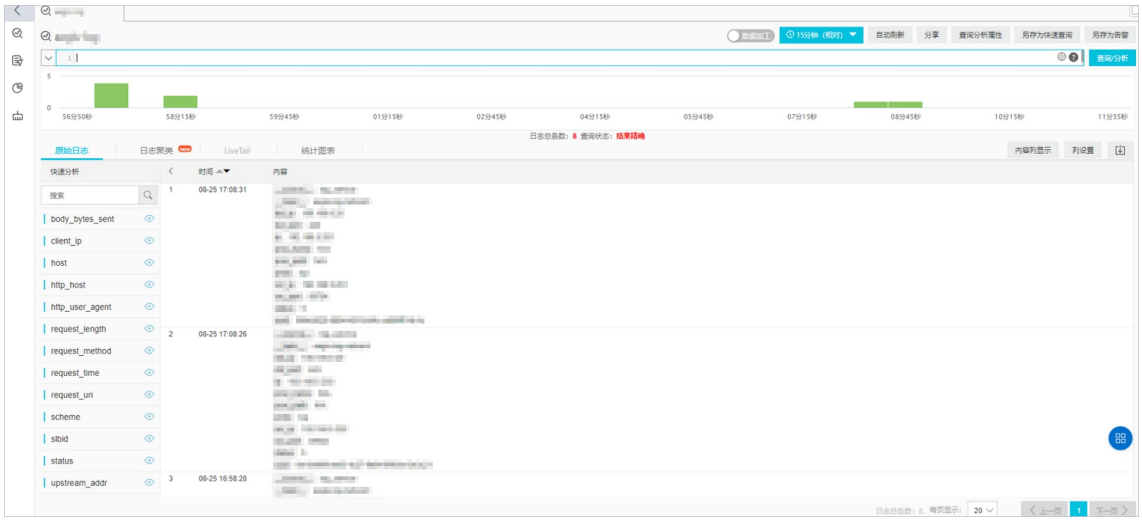
1. 进入日志查询页面。您可以通过负载均衡控制台和日志服务控制台进入日志查询页面。
   - 负载均衡控制台

     在**访问日志**页面，单击**查看日志**。

   - 日志服务控制台

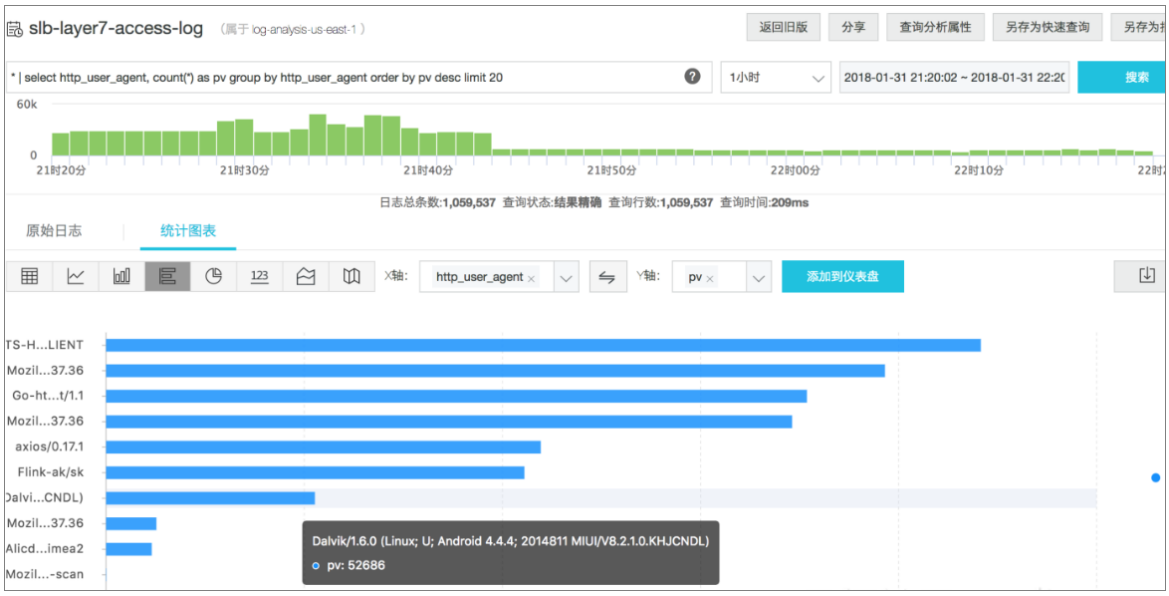
在**日志库**页面，单击日志库的**查询/分析**选项。



2. 单击目标日志字段，查看对应的日志信息。
3. 输入SQL语句查询特定的访问日志。

   例如输入如下SQL语句查询Top20的客户端，用于分析请求访问来源，辅助商业决策。

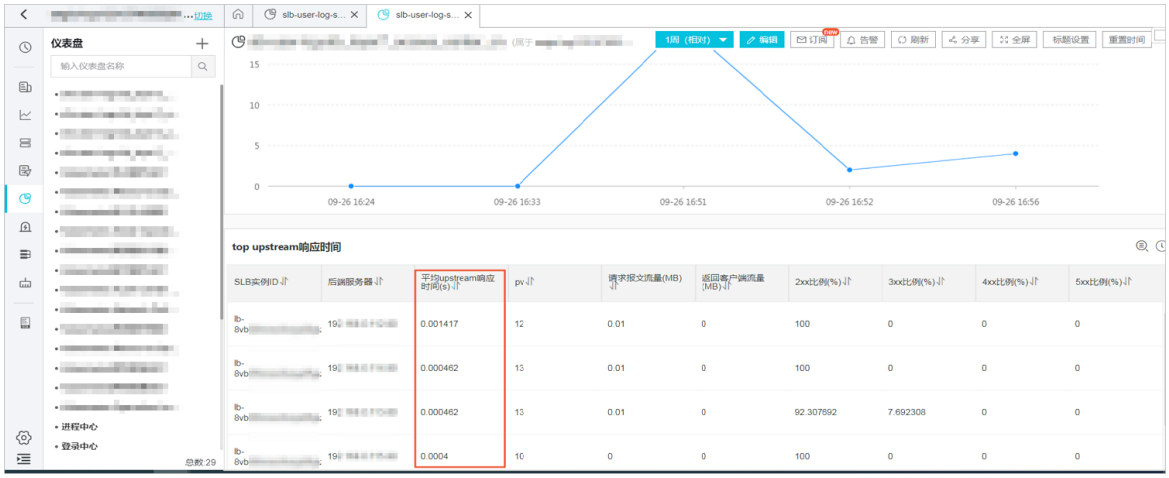
```
* | select ip_to_province(client_ip) as client_ip_province, count(*) as pv group by
    client_ip_province order by pv desc limit 50
```



步骤三：定位异常后端服务器

您可以通过日志服务的仪表盘定位异常后端服务器。

1. 登录日志服务控制台，单击负载均衡的Project链接。
2. 在左侧导航栏，单击  。
3. 单击负载均衡访问日志的名称链接。



4. 在仪表盘中，查看**top upstream响应时间**页签下负载均衡SLB的响应时间，可以将参数**平均upstream响应时间(s)**设置降序排列，查看是否有后端服务器的响应时间超过1s。

   如果有响应时间超过1s的后端服务器，执行**ssh**命令，登录该后端服务器，查看CPU是否持续高位运行，进行高负载处理。

2.12. 通过OpenAPI开发者门户创建VPC类型实例时指定IP

使用OpenAPI开发者门户创建VPC类型负载均衡实例时，支持在负载均衡实例所属交换机支持的网段中，指定其中一个地址作为负载均衡实例的私网IP地址。

操作步骤

1. 登录OpenAPI开发者门户。
2. 搜索负载均衡产品的CreateLoadBalancer接口，并单击操作列的**去调试**。
3. 设置创建负载均衡实例的参数。

   此处设置部分参数作为示例，详细参数说明请参见创建实例：

   - RegionId：表示负载均衡实例的地域，此处设置为*cn-hangzhou*。
   - VpcId：表示负载均衡实例所属VPC的ID。

     此处可登录专有网络VPC控制台，选择华东1（杭州）区域，查看VPC的ID。
   - VSwitchId：表示负载均衡所属交换机的ID，如果需要指定负载均衡IP地址，该参数必须要设置。

     此处可在专有网络VPC控制台，单击负载均衡实例所属VPC的ID，在**网络资源**页面下，单击交换机的个数，查看交换机的ID。

     单击交换机ID，查看交换机的目标网段，如192.168.0.0/24。
   - Address：指定负载均衡实例的私网IP地址，该地址必须包含在交换机的目标网段下，例如192.168.0.3。
4. 单击**发起调用**。

   返回结果如下：

   - XML格式

```
<?xml version="1.0" encoding="UTF-8" ?>
    <NetworkType>vpc</NetworkType>
    <LoadBalancerName>auto_named_slb</LoadBalancerName>
    <Address>192.168.0.3</Address>
    <ResourceGroupId>rg-acfmxazb4ph*****</ResourceGroupId>
    <RequestId>09197EEB-7013-4F56-A5CE-A756FFE5B75D</RequestId>
    <AddressIPVersion>ipv4</AddressIPVersion>
    <LoadBalancerId>lb-bp1h66tp5uat84kh******</LoadBalancerId>
    <VSwitchId>vsw-bp14cagpfysr29fe*****</VSwitchId>
    <VpcId>vpc-bp18sth14qii3pn*****</VpcId>
```

- JSON格式

```
{
    "NetworkType": "vpc",
    "LoadBalancerName": "auto_named_slb",
    "Address": "192.168.0.3",
    "ResourceGroupId": "rg-acfmxazb4******",
    "RequestId": "09197EEB-7013-4F56-A5CE-A756FFE5B75D",
    "AddressIPVersion": "ipv4",
    "LoadBalancerId": "lb-bp1h66tp5uat84******",
    "VSwitchId": "vsw-bp14cagpfysr29*******",
    "VpcId": "vpc-bp18sth14qii3*********"
}
```

5. 登录负载均衡管理控制台，选择华东1（杭州）区域，查看IP为192.168.0.3的负载均衡实例是否创建成功。

2.13. 查看用量明细

当您想获取负载均衡的用量明细时，可以在阿里云费用中心导出查看。

操作步骤

1. 登录传统型负载均衡CLB控制台。
2. 在菜单栏右上角选择**费用 > 用户中心**。
3. 在左侧导航栏，选择**用量明细**。
4. 在**用量明细**页面，**产品**选择**负载均衡**，配置需要查看的负载均衡用量的**计量规格**、**使用时间**和**计量粒度**。

5. 单击**导出CSV**。
6. 在**导出记录**页面观察，当**状态**从**等待下载**变为**导出成功**，在**操作**列单击**下载**，即可将用量明细文件导出至本地。

该文件打开后包含以下信息，可根据实例ID、地域或者服务地址等查看具体用量明细使用情况。

A	B	C	D	E	F	G	H	I
实例ID	地域	服务地址	服务地址类型	带宽(bit/s)	上行流量	下行流量	开始时间	结束时间
lb- rikve	us-east-1	47	internet	0	0	0	######	######
lb- rikve	us-east-1	47	internet	0	0	0	######	######
lb- rikve	us-east-1	47	internet	0	0	0	######	######
lb- rikve	us-east-1	47	internet	0	0	0	######	######
lb- ea2x	cn-chengdu	47	internet	0	3516	3516	######	######
lb- ea2x	cn-chengdu	47	internet	0	3362	3362	######	######
lb- ea2x	cn-chengdu	47	internet	0	3308	3308	######	######
lb- ea2x	cn-chengdu	47	internet	0	3376	3376	######	######
lb- a00xg	cn-beijing-btc-a01	59	internet	1048576	0	0	######	######
lb- a00xg	cn-beijing-btc-a01	59	internet	1048576	0	0	######	######
lb- a00xg	cn-beijing-btc-a01	59	internet	1048576	0	0	######	######
lb- a00xg	cn-beijing-btc-a01	59	internet	1048576	0	0	######	######
lb- 0uwd68	cn-beijing-btc-a01	10 4	internet	31457280	0	0	######	######
lb- 0uwd68	cn-beijing-btc-a01	10 4	internet	31457280	0	0	######	######
lb- 0uwd68	cn-beijing-btc-a01	10 4	internet	31457280	0	0	######	######
lb- 0uwd68	cn-beijing-btc-a01	10 4	internet	31457280	0	0	######	######