ALIBABA CLOUD

阿里云

全球加速

用户指南

文档版本：20220526

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

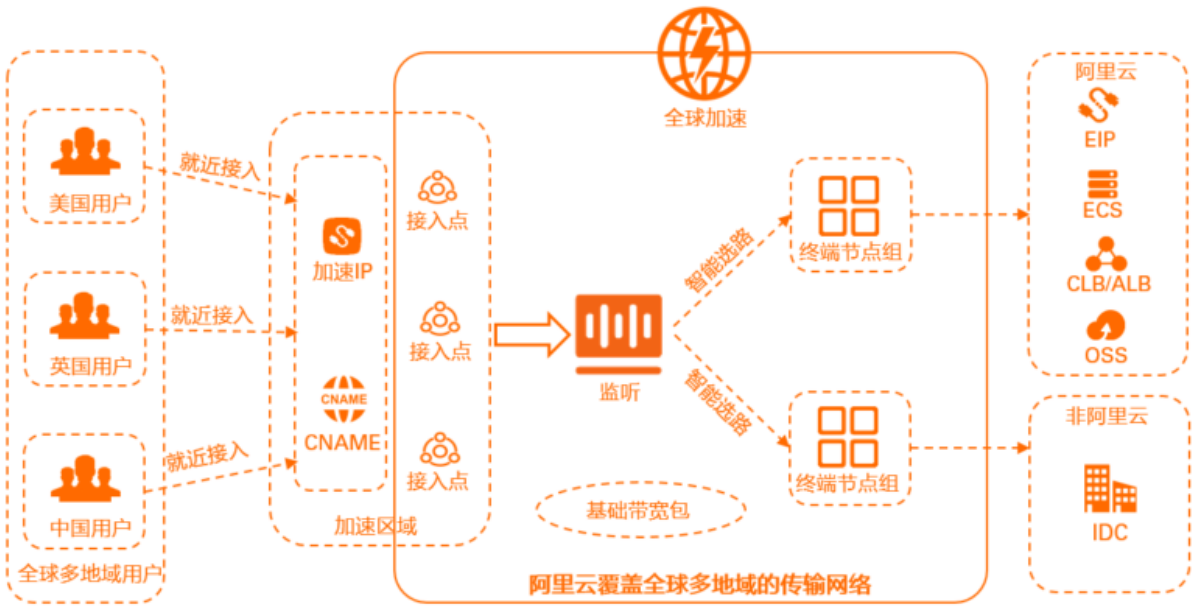
格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**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.全球加速实例

1.1. 全球加速实例概述

全球加速实例是一个运行的全球加速服务。全球加速提供多种实例规格，每种实例规格的加速能力都不同，可满足不同场景的加速服务。



在创建全球加速实例后，您首先需要配置一个带宽包，然后设置加速区域。全球加速会为每个接入加速区域的地域分配一个加速IP。客户端流量根据监听的配置通过加速IP就近从接入点进入阿里云加速网络，全球加速可以智能选择路由并自动完成网络调度，然后把客户端的网络访问请求送达至最佳终端节点，避开公网的拥堵，达到减少时延的效果。全球加速的终端节点可以是云服务器ECS（Elastic Compute Service）、传统型负载均衡CLB（Classic Load Balancer）、应用型负载均衡ALB（Application Load Balancer）、对象存储OSS（Object Storage Service）、阿里云公网IP、自定义源站IP或自定义源站域名。

实例规格

全球加速支持多种规格，每种规格提供的加速能力不同，具体如下表所示。

规格	加速地域个数	最大带宽处理能力	最大并发连接数	实例价格（元/月）
小型 I	1	20 Mbps	5千	1099
小型 II	2	40 Mbps	1万	2099
小型III	3	60 Mbps	1.5万	3099
中型 I	5	100 Mbps	2.5万	5099
中型 II	8	160 Mbps	4万	8099
中型III	10	200 Mbps	5万	10099
大型 I	全部地域	400 Mbps	10万	20099
大型 II	全部地域	600 Mbps	15万	30099

规格	加速地域个数	最大带宽处理能力	最大并发连接数	实例价格（元/月）
大型III	全部地域	800 Mbps	20万	40099
大型IV	全部地域	1 Gbps	25万	50099
大型V	全部地域	1.2 Gbps	30万	60099
大型VI	全部地域	1.4 Gbps	35万	70099
大型VII	全部地域	1.6 Gbps	40万	80099
大型VIII	全部地域	1.8 Gbps	45万	90099
超大型 I	全部地域	2 Gbps	50万	100099
超大型 II	全部地域	4 Gbps	100万	200099

> **说明** 目前，大型III及以上规格仅白名单开放。如需使用，请提交工单。

1.2. 创建和管理全球加速实例

全球加速是一款覆盖全球的网络加速服务，为全球用户提供高可用和高性能的网络加速服务。本文为您介绍如何创建和管理全球加速实例。

创建全球加速实例

使用全球加速前，您必须先创建全球加速实例。

1.
2. 在**实例列表**页面，单击**创建加速实例**。
3. 在购买页面，根据以下信息配置全球加速实例，然后单击**立即购买**并完成支付。

配置	说明
类型	选择购买全球加速实例的类型： ○ **基础型**：基础型全球加速可用于三层（IP协议）加速场景，您只需要配置加速区域和终端节点组即可实现业务加速。更多信息，请参见使用基础型全球加速实现访问加速。 > **说明** 目前基础型全球加速功能白名单开放。如需使用，请提交工单。 ○ **标准型**：标准型全球加速主要用于四层（TCP和UDP协议）和七层（HTTP和HTTPS协议）加速。
规格	选择购买全球加速实例的规格。仅**类型**为**标准型**时支持选择。 全球加速支持的实例规格，请参见实例规格。

配置	说明
加速IP类型	选择全球加速实例提供的加速IP类型。 ○ **弹性公网IP**（默认值）：采用自定义就近接入模式，您可以根据业务需要定向选择就近接入点，每个接入点为您提供独立的EIP。 ○ **任播弹性公网IP**：采用自动就近接入模式，无需配置加速区域，全球加速在全球多地域提供一个Anycast EIP。 说明 ■ 目前加速IP类型支持选择任播弹性公网的功能白名单开放。如需使用，请提交工单。 ■ 仅实例类型为**标准型**，**规格**为**大型 I** 及以上时支持选择**任播弹性公网IP**。 ■ 加速IP类型为**任播弹性公网IP**的全球加速实例，只支持绑定按量付费的带宽包。 加速IP类型更多信息，请参见加速区域概述。
实例	默认选择**实例**。
购买时长	选择购买全球加速实例的时长。

为全球加速实例变配

标准型全球加速实例支持变配功能，您可以通过变配功能修改标准型全球加速实例的规格。目前仅支持对全球加速实例规格进行升配操作，降配操作白名单开放。如需开通降配功能，请。

1.
2. 在**实例列表**页面，找到目标全球加速实例，在**操作**列单击**变配**。
3. 在**变配提示**对话框，确认变配操作提示信息后，单击**确定**。

> **说明** 变配操作可能会新增终端节点出公网IP（新增数量与全球加速实例规格有关，具体以控制台显示为准），需要您手工确认新增的出公网IP为可用状态。

4. 在**变配**页面，选择要修改的规格并选中服务协议，然后单击**立即购买**并完成支付。

   全球加速各种规格提供的加速能力，请参见实例规格。

更多操作

操作	步骤
更新全球加速实例的基本信息	1. 在**实例列表**页面，找到目标全球加速实例，单击全球加速实例ID。 2. 单击**实例信息**页签，单击**实例名称**右侧的**编辑**。 3. 在弹出的对话框中输入实例名称，然后单击**确定**。
为全球加速实例续费	1. 在**实例列表**页面，找到目标全球加速实例，在**操作**列单击**续费**。 2. 在**续费**页面，选择续费时长，并选中服务协议，然后单击**立即购买**并完成支付。

相关文档

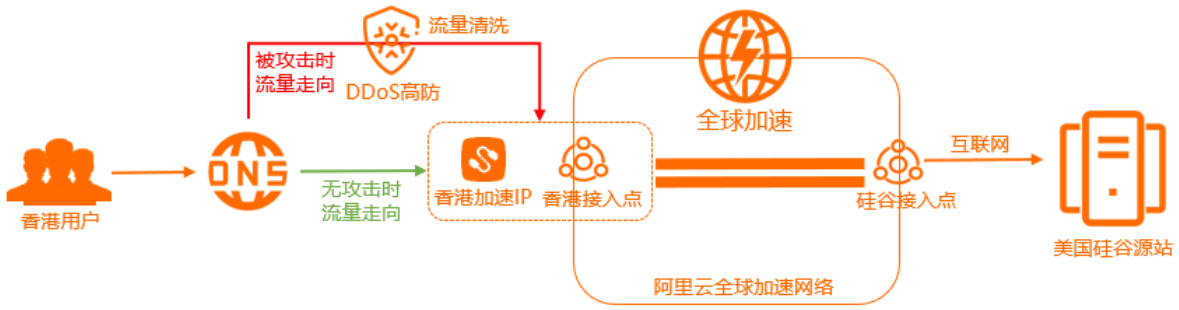
- CreateAccelerator：调用CreateAccelerator接口创建一个全球加速实例。
- ListAccelerators：调用ListAccelerators接口查询全球加速实例列表。
- DescribeAccelerator：调用DescribeAccelerator接口查询指定的全球加速实例信息。
- UpdateAccelerator：调用UpdateAccelerator修改全球加速实例。
- UpdateAcceleratorConfirm：调用UpdateAcceleratorConfirm确认修改的全球加速实例规格信息。
- DeleteAccelerator：调用DeleteAccelerator删除指定的全球加速实例。
- DescribeAcceleratorAutoRenewAttribute：调用DescribeAcceleratorAutoRenewAttribute查询全球加速实例的自动续费状态。
- UpdateAcceleratorAutoRenewAttribute：调用UpdateAcceleratorAutoRenewAttribute接口修改全球加速实例的自动续费属性。

1.3. 提升DDoS阈值

您可以为全球加速提升DDoS阈值，提升DDoS阈值后，全球加速与DDoS高防实例并联部署，仅在特定场景下触发并切换启用DDoS高防实例，保证无DDoS攻击时日常业务的流畅体验以及发生DDoS攻击时达到更好的防护效果。

配置场景

本文以下图场景为例。



某公司的Web服务部署在美国（硅谷），终端用户主要集中在中国（香港）。因跨国公网不稳定，中国（香港）终端用户访问美国（硅谷）的Web服务经常出现延迟、抖动、丢包等网络问题。针对以上问题，该公司使用阿里云全球加速减少了延迟、抖动、丢包等网络问题的出现。但Web服务经常受到DDoS攻击，严重影响Web服务的安全性和可用性。

您可以为全球加速提升DDoS阈值，提升DDoS阈值后，全球加速将与DDoS高防实例并联部署，部署完成后：

- Web服务在无攻击时，中国（香港）地域终端用户的访问请求通过加速IP就近从接入点进入阿里云加速网络，然后通过智能选择路由和自动网络调度，把终端用户的网络访问请求送达至终端节点。
- Web服务在受到攻击时，触发并切换启用DDoS高防实例，清洗过滤流量后再通过就近的接入点进入阿里云加速网络，然后通过智能选择路由和自动网络调度，把终端用户的网络访问请求送达至终端节点。

前提条件

- 您已经注册了阿里云账号。如未注册，请先完成账号注册。
- 您已经提交了提升DDoS阈值功能的使用申请。如未提交，请提交工单。
- 您已经购买了DDoS高防实例，并添加了转发规则。详细信息，请参见购买DDoS高防实例和添加转发规则。

配置步骤

步骤一：提升DDoS阈值

提升DDoS阈值后，全球加速和DDoS高防实例并联部署，保证无DDoS攻击时日常业务的流畅体验以及发生DDoS攻击时达到更好的防护效果。

> **说明** 为全球加速提升DDoS阈值时，系统会判断全球加速是否拥有服务关联角色AliyunServiceRoleForGaAntiDdos：
>
> - 如果全球加速不存在服务关联角色AliyunServiceRoleForGaAntiDdos，系统会自动创建该服务关联角色，并为该服务关联角色添加名称为AliyunServiceRolePolicyForGaAntiDdos的权限策略，授予全球加速拥有访问DDoS高防实例的权限。
> - 如果全球加速已经拥有服务关联角色AliyunServiceRoleForGaAntiDdos，则不会重复创建该服务关联角色。
>
> 详细信息，请参见AliyunServiceRoleForGaAntiDdos。

1.
2. 在**实例列表**页面，找到目标全球加速实例，在**操作**列单击 > **提升DDoS阈值**。
3. 在**提升DDoS阈值**对话框，根据以下信息选择要联动的DDoS高防实例。
   - **DDoS联动产品**：选择要联动的DDoS高防实例类型。本文选择**DDoS高防（国际）**。
   - **DDoS高防实例**：选择要联动的DDoS高防实例。
4. 单击**确定**。

提升DDoS阈值后，系统会分配一个全球加速联动DDoS高防的CNAME，用于全球加速和DDoS高防的联动。

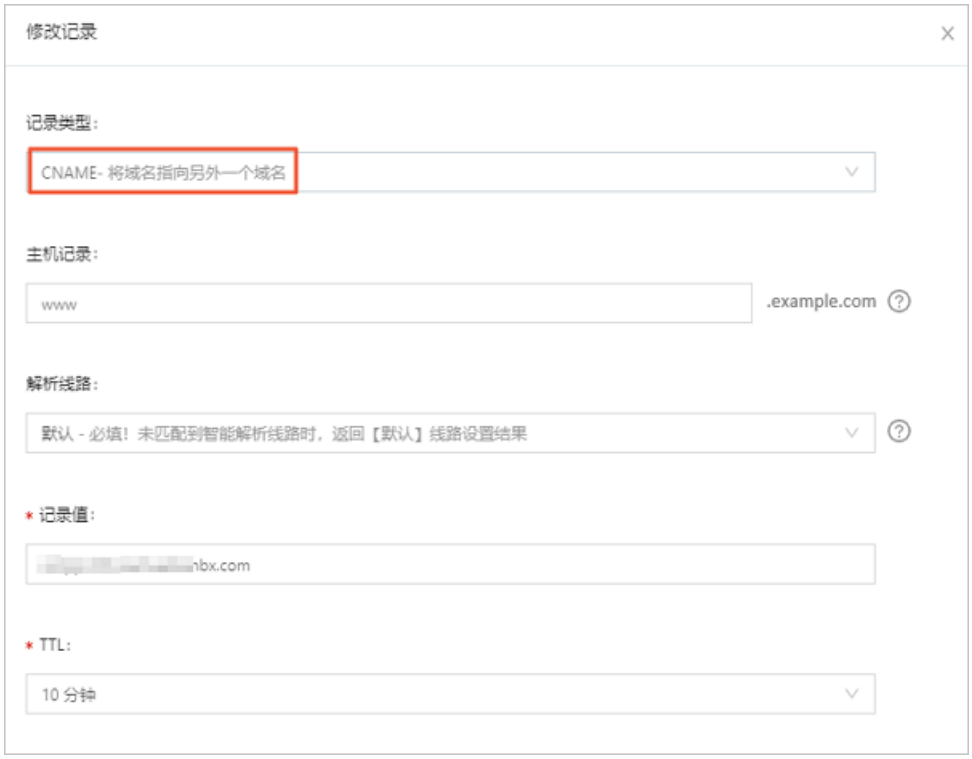
> **说明** CNAME名称中含有-1即为全球加速联动DDoS高防的CNAME，例如ga-bp1f609c76zg6****zuna-1.aliyungaxxxx.com。

步骤二：修改DNS解析

您需要将DNS解析到全球加速联动DDoS高防CNAME，才能实现按需防护，即Web服务在无攻击时，终端用户访问Web服务通过全球加速服务进行加速；Web服务在受到攻击时，访问Web服务的流量切换到DDoS高防节点，流量清洗后再送到全球加速的加速节点。

> **说明** 如果您使用的DNS解析服务为非阿里云云解析DNS，请登录您的DNS服务商系统修改网站域名的解析记录。

1. 登录阿里云云解析DNS控制台。
2. 在**域名解析**页面，找到目标域名，在**操作**列单击**解析设置**。
3. 在**解析设置**页面，找到要修改的解析记录，在**操作**列单击**修改**。
4. 在**修改记录**对话框，选择**记录类型**为**CNAME**，并将**记录值**修改为步骤一：提升DDoS阈值完成后系统分配的全球加速联动DDoS高防CNAME地址。更多关于CNAME记录配置说明，请参见CNAME记录。

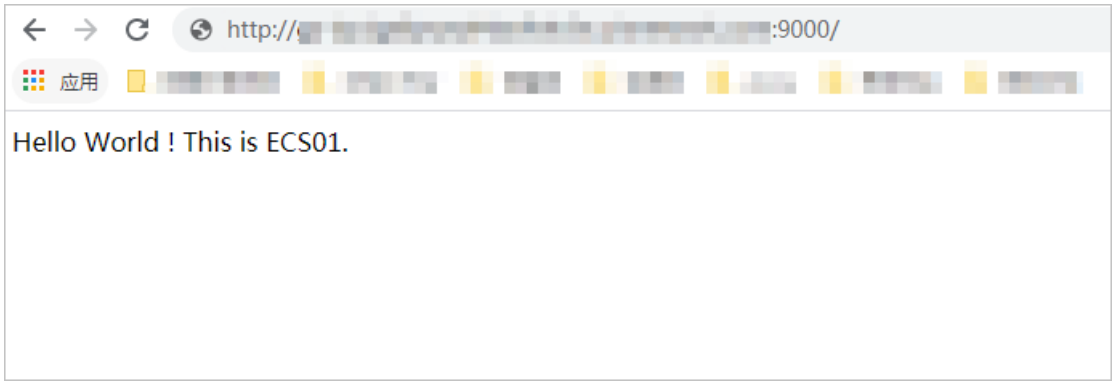


5. 单击**确认**。

步骤三：访问测试

1. 在接入地域（本文为中国香港）的电脑中打开浏览器。
2. 使用网站域名访问美国（硅谷）地域部署的Web服务。

   经测试，可以通过网站域名访问美国（硅谷）地域部署的Web服务。



3. 执行 `dig <网站域名>` 查看解析结果。
   - 源站未被攻击时：解析结果为配置的全球加速的IP。
   - 源站被攻击时：解析结果为DDoS高防实例的IP。

相关文档

- AttachDdosToAccelerator

1.4. 重置DDoS阈值

您可以重置DDoS阈值，重置后，全球加速与DDoS高防实例解绑，您的加速服务将取消DDoS高防的安全防护。

操作步骤

1.
2. 在**实例列表**页面，找到目标全球加速实例，单击其**操作**列下的 > **重置DDoS阈值**。
3. 在**重置DDoS阈值**对话框中，单击**确定**。

相关文档

- DetachDdosFromAccelerator

2.基础带宽包

2.1. 基础带宽包概述

基础带宽包提供了覆盖全球的公网接入带宽和阿里云内网传输带宽，但不包含中国内地与海外互通专线带宽。要实现网络加速服务，您必须购买基础带宽包。

带宽类型

基础带宽包支持标准加速带宽、增强加速带宽和精品加速带宽三种带宽类型。带宽类型不同，加速类型、加速后端服务和加速范围也不同，如下表所示。

带宽类型	加速类型	加速后端服务	加速范围
标准加速带宽	阿里云上应用加速	• 阿里云公网IP • 云服务器ECS • 传统型负载均衡CLB（原SLB） • 应用型负载均衡ALB • 对象存储服务OSS	默认的加速区域和后端服务区域都位于中国内地
增强加速带宽	• 阿里云上应用加速 • 阿里云下应用加速	• 阿里云公网IP • 云服务器ECS • 传统型负载均衡CLB（原SLB） • 应用型负载均衡ALB • 对象存储服务OSS • 自定义IP • 自定义域名	默认的加速区域和后端服务区域都位于中国内地
精品加速带宽	• 阿里云上应用加速 • 阿里云下应用加速	• 阿里云公网IP • 云服务器ECS • 传统型负载均衡CLB（原SLB） • 应用型负载均衡ALB • 对象存储服务OSS • 自定义IP • 自定义域名	默认的加速区域和后端服务区域都位于海外（如果要加速中国内地到海外的访问，需选择中国香港作为接入地域）

说明

- 目前，将ECS、CLB和ALB类型的后端服务作为实例级白名单开放。如果您的全球加速实例需添加ECS、CLB或ALB类型的后端服务，请先提交工单进行实例升级。
- 只有专有网络类型的ECS和CLB才可以作为终端节点的后端服务类型。
- 每个全球加速实例的终端节点出公网IP唯一，不与其他全球加速实例用户共享。

购买基础带宽包

如果您需要购买基础带宽包，请至购买页。

2.2. 购买和管理基础带宽包

基础带宽包提供了覆盖全球的公网接入带宽和阿里云内网传输带宽。本文为您介绍如何购买和管理基础带宽包。

购买基础带宽包

1.
2. 在**实例列表**页面的**购买基础带宽包**下拉列表中，按需选择购买不同付费模式的基础带宽包。
   - 单击**购买预付费基础带宽包**，在**全球加速_基础带宽包（包年包月）**购买页面，根据以下信息配置基础带宽包，然后单击**立即购买**并完成支付。

配置	说明
带宽类型	选择购买基础带宽包的带宽类型。 支持**标准加速带宽**、**增强加速带宽**和**精品加速带宽**三种带宽类型。
带宽峰值	选择购买基础带宽包的带宽峰值。单位为Mbps。
购买时长	选择购买基础带宽包的时长。

   - 单击**购买后付费基础带宽包**，在**全球加速_基础带宽包（按量付费）**购买页面，根据以下信息配置基础带宽包，然后单击**立即购买**并完成支付。

配置	说明
带宽类型	选择购买基础带宽包的带宽类型。 目前，仅支持选择**精品加速带宽**类型。
计费方式	选择基础带宽包的计费方式。 目前，仅支持选择**按使用流量计费**。
带宽规格	选择购买基础带宽包的带宽规格。 带宽规格支持选择20Mbps、50Mbps、100Mbps、200Mbps、500Mbps、1000Mbps。

绑定基础带宽包

购买基础带宽包后，您需要将基础带宽包与全球加速实例绑定。绑定后，您才能为加速区域分配加速带宽。

每个全球加速实例可以绑定一个基础带宽包。

绑定绑定基础带宽包之前，您需要了解以下信息：

- 请确保您已经创建了全球加速实例和基础带宽包。具体操作，请参见创建和管理全球加速实例和购买基础带宽包。
- 当全球加速实例加速IP类型为**任播弹性公网IP**时，仅支持绑定精品加速带宽类型且按使用流量计费的基础带宽包。

1.
2. 在**实例列表**页面，找到目标全球加速实例，单击实例ID。
3. 单击**带宽包管理**页签。
4. 在**基础带宽包**区域，找到目标基础带宽包，在**操作**列单击**绑定**。

绑定成功后，基础带宽包的状态变成**可用**。

替换基础带宽包

您可以替换已经绑定到全球加速实例的基础带宽包，实现业务对基础带宽包的弹性需求。替换基础带宽包不会中断全球加速的转发流量。

基础带宽包替换成功后，原基础带宽包会与全球加速实例解绑，新替换的基础带宽包会与全球加速实例绑定。

替换基础带宽包之前，请确保您已经购买了要替换的基础带宽包，且要替换的基础带宽包的带宽必须大于或等于加速区域中已分配的带宽总额。具体操作，请参见购买基础带宽包。

1.
2. 在**实例列表**页面，找到目标全球加速实例，单击实例ID。
3. 单击**带宽包管理**页签。
4. 在**基础带宽包**区域，找到目标基础带宽包，在**操作**列单击**替换**。
5. 在**替换基础带宽包**对话框，选择要替换的基础带宽包，然后单击**确定**。

   仅支持选择状态为**待绑定实例**的基础带宽包。

解绑基础带宽包

您可以将基础带宽包从全球加速实例解绑，解绑后，全球加速实例可以绑定新的基础带宽包。

请确保要解绑基础带宽包的全球加速实例未配置加速区域和监听。如有配置，请删除。详细信息，请参见删除加速区域和删除监听。

1.
2. 在**实例列表**页面，找到目标全球加速实例，单击实例ID。
3. 单击**带宽包管理**页签。
4. 在**基础带宽包**区域，找到目标基础带宽包，在**操作**列单击**解绑**。
5. 在**解绑带宽包**对话框，单击**确定**。

变配

您可以通过变配功能修改预付费基础带宽包的带宽峰值或者后付费基础带宽包的带宽规格，修改后立即生效。

1.
2. 在**实例列表**页面，找到目标全球加速实例，单击实例ID。
3. 单击**带宽包管理**页签。
4. 在**基础带宽包**区域，找到目标基础带宽包，在**带宽**列单击**变配**。
5. 在**变配**页面，修改基础带宽包的带宽峰值或后付费基础带宽包的带宽规格，并选中服务协议，然后单击**立即购买**完成支付。

> **说明** 目前，仅支持标准加速带宽变配到增强加速带宽，而不支持将增强加速带宽和精品加速带宽变配到其他类型的加速带宽。

相关文档

- CreateBandwidthPackage：创建带宽包。
- BandwidthPackageAddAccelerator：将带宽包与全球加速实例绑定。

- ReplaceBandwidthPackage：替换带宽包。
- BandwidthPackageRemoveAccelerator：将带宽包与全球加速实例解绑。
- UpdateBandwidthPackage：修改带宽包的配置。

3.加速区域

3.1. 加速区域概述

创建全球加速实例后，您需要添加加速区域。加速区域是您需要提供访问加速的区域。

加速区域与地域

您需要为哪个区域的用户提供访问加速就将哪个区域添加为加速区域。您可以在加速区域内选择具体的加速地域。

加速区域是阿里云地域的集合，每个加速区域包含一个或多个阿里云的地域，如下表所示。

加速区域	包含的地域
华北	华北1（青岛）、华北2（北京）
华南	华南1（深圳）、华南2（河源）、华南3（广州）
华东	华东1（杭州）、华东2（上海）、华东5（南京）
西南	西南1（成都）
北美洲	美国（硅谷）、美国（弗吉尼亚）
南美洲	巴西（圣保罗）
亚太	中国（香港）、韩国（首尔）、新加坡、马来西亚（吉隆坡）、日本（东京）、印度尼西亚（雅加达）、印度（孟买）、澳大利亚（悉尼）、菲律宾（马尼拉）、泰国（曼谷）、越南（胡志明）
欧洲	德国（法兰克福）、英国（伦敦）
中东	阿联酋（迪拜）

> **说明** 以下加速地域为白名单开放：华南2（河源）、华东5（南京）、巴西（圣保罗）、泰国（曼谷）、越南（胡志明）、阿联酋（迪拜）。如需使用，请提交工单。

加速IP

添加加速区域后，全球加速会根据您在添加加速区域时选择的IP地址协议，为每个接入加速区域的地域分配对应协议的加速IP。客户端通过访问加速IP从就近接入点进入阿里云加速网络。

您可以选择以下IP地址协议：

- IPv4：分配一个IPv4协议的加速IP，用于加速IPv4客户端访问IPv4服务。
- IPv6：分配一个IPv6协议的加速IP，用于加速IPv6客户端访问IPv4服务。

> 说明
> - 目前，仅以下地域支持IPv6客户端接入全球加速服务：华北1（青岛）、华北2（北京）、华东1（杭州）、华东2（上海）、华南1（深圳）、华南2（河源）、华南3（广州）、西南1（成都）、中国（香港）、新加坡、美国（弗吉尼亚）、德国（法兰克福）。
> - 一个全球加速实例下，同一个加速地域不支持同时选择IPv4和IPv6地址协议。

3.2. 添加加速区域

创建全球加速实例后，您需要添加加速区域。加速区域是您需要进行访问加速的区域。

前提条件

开始前，请确保满足以下条件：

- 您已经创建了全球加速实例。具体操作，请参见创建和管理全球加速实例。
- 您已经购买了带宽包。具体操作，请参见购买和管理基础带宽包。

操作步骤

1.
2. 在**实例列表**页面，找到目标全球加速实例，单击实例ID链接。
3. 在实例详情页，单击**加速区域**页签，选择需要进行访问加速的区域，然后单击**添加接入地域**。
4. 在**添加加速区域**对话框，根据以下信息配置加速区域，然后单击**确定**。

配置	说明
地域	选择需要进行访问加速的地域。区域和地域的对应关系请参见加速区域与地域。
带宽	设置加速服务的地域带宽。单位Mbps。 > 说明 > - 每个接入地域支持分配的最小带宽为2 Mbps。 > - 接入地域带宽总额应小于或等于您购买的基础带宽包的带宽。 > 例如，您购买的基础带宽包的带宽为10 Mbps，您已经在华北1（青岛）地域分配了6 Mbps，则您可分配的带宽余量为4 Mbps。

配置	说明
IP地址协议	选择接入全球加速服务的IP地址协议。 ○ IPv4：分配一个IPv4协议的加速IP，用于加速IPv4客户端访问IPv4服务。 ○ IPv6：分配一个IPv6协议的加速IP，用于加速IPv6客户端访问IPv4服务。 **说明** ■ 目前，仅以下地域支持IPv6客户端接入全球加速服务：华北1（青岛）、华北2（北京）、华东1（杭州）、华东2（上海）、华南1（深圳）、华南2（河源）、华南3（广州）、西南1（成都）、中国（香港）、新加坡、美国（弗吉尼亚）、德国（法兰克福）。 ■ 一个全球加速实例下，同一个加速地域不支持同时选择IPv4和IPv6地址协议。

您还可以单击**+添加**为多个地域分配带宽。

说明 可添加地域的数量受带宽总额和全球加速实例规格限制。关于各实例规格支持的接入地域数量，请参见实例规格。

相关文档

- CreateIpSets

3.3. 修改加速区域

本页面后期将不再维护并下线。如何修改加速区域，请参见修改加速区域。

3.4. 删除加速区域

本页面后期将不再维护并下线。如何删除加速区域，请参见删除加速区域。

4.监听

4.1. 监听概述

创建全球加速实例后，您需要为全球加速实例配置监听。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终端节点。

监听协议

每个全球加速实例可以创建10个监听，监听支持TCP、UDP、HTTP和HTTPS协议，您可以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，可靠性高。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。 • 数据传输慢。	• 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，例如文件传输、发送或接收邮件、远程登录。 • 无特殊要求的Web应用。
UDP	• 面向非连接的协议，可靠性低。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机制。 • 数据传输快。	关注实时性而相对不注重可靠性的场景，例如视频聊天、金融实时行情推送。
HTTP	• 面向连接的协议，可靠性高。在正式收发数据前，必须和对方建立可靠的连接。 • 数据传输快。 • 数据明文传输。	• 适用于加速访问HTTP网站的场景，可以提升客户端访问HTTP网站的速度。 • 适用于同时加速多个域名或多个路径访问HTTP网站的场景。
HTTPS	• 面向连接的协议，可靠性高。在正式收发数据前，必须和对方建立可靠的连接。 • 通过绑定SSL证书，保证数据的高可靠性。 **说明** 关于SSL证书更多信息，请参见什么是数字证书管理服务。 • 数据加密传输。	• 适用于加速访问HTTP或HTTPS网站的场景，可以提升客户端访问HTTP或HTTPS网站的速度和安全性。 • 适用于同时加速多个域名或多个路径访问HTTP或HTTPS网站的场景。

监听端口

监听端口是用来接收请求并向终端节点进行转发的端口。根据您为单个监听配置的端口数量，可将监听分为普通端口监听和海量端口监听。

说明 同一全球加速实例下相同监听协议的监听端口不能冲突。

- 普通端口监听

一般情况下，各监听协议支持配置的端口数量和使用限制如下表所示。针对TCP和UDP协议的监听，您还可以通过配额管理提升gaplus_quota_port_per_listener的配额，具体操作，请参见配额管理。

监听协议	可配置的监听端口范围	支持配置的监听端口数量
TCP	1~65499	30个。 ○ 多个端口之间使用半角逗号（,）分隔，例如*80,90,8080*。 ○ 多个连续的端口可以使用半角波浪线（~）表示监听端口范围，例如80,81,82,83端口，可以使用*80~83*表示。
UDP	1~65499	30个。 ○ 多个端口之间使用半角逗号（,）分隔，例如*80,90,8080*。 ○ 多个连续的端口可以使用半角波浪线（~）表示监听端口范围，例如80,81,82,83端口，可以使用*80~83*表示。
HTTP	1~65499	1个。
HTTPS	1~65499	1个。

- 海量端口监听
  针对TCP或UDP协议的监听，支持为单个监听配置超过300个连续的端口。拥有超过300个连续端口的监听可称为海量端口监听。海量端口监听有以下使用限制：
  - 2022年01月08日之后创建的全球加速实例默认支持海量端口功能。如果您的全球加速实例创建于该时间之前，且需使用海量端口功能，请先提交工单进行实例升级。
  - 最少需配置超过300个端口，最多可配置65499个端口。
  - 每个全球加速实例仅支持配置1个海量端口监听。
  - 仅支持配置连续的端口。例如可以配置为*1~350*，不能配置*1,3~350*。
  - 当全球加速实例的加速地域包含阿里云POP点时，不支持为该实例配置海量端口监听。

    说明 查看指定全球加速实例可用的加速地域是否为阿里云POP点，请参见ListAvailableBusiRegions。

例如，您需要为全球加速实例配置如下监听：TCP 1~400、TCP 443、UDP 200~210和UDP 230~240。其中，TCP 1~400为海量端口监听，配置如下图所示。

监听ID/名称	协议	端口	状态	默认终端节点组
lsr-bp[redacted]vz TCP01	TCP	1~400	✓ 运行中	1
lsr-bp1f[redacted] UDP01	UDP	200~210	✓ 运行中	1
lsr-bp1a[redacted] UDP02	UDP	230~240	✓ 运行中	1
lsr-bp1[redacted] TCP02	TCP	443	✓ 运行中	1

4.2. 添加和管理监听

创建全球加速实例后，您需要为全球加速实例配置监听。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终端节点。

前提条件

- 您已经创建了全球加速实例。具体操作，请参见创建和管理全球加速实例。
- 如果您要配置HTTPS协议的监听，请确保您已经购买了SSL证书，并申请了该SSL证书。具体操作，请参见证书选型与购买和提交证书申请。

添加TCP或UDP协议监听

1. 配置监听和协议。
   i. 登录全球加速管理控制台。
   ii. 在**实例列表**页面，找到目标全球加速实例，在**操作**列单击**配置监听**。
   iii. 在**监听**页签下，单击**添加监听**。

> **说明** 如果您是第一次添加监听，或当前全球加速实例下没有监听实例时，请跳过该步骤。

iv. 在**配置监听和协议**配置向导页面，根据以下信息配置监听和协议，然后单击**下一步**。

配置	说明
监听名称	输入监听的名称。 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（_）和短划线（-）。
协议	选择监听的网络传输协议类型，支持以下协议： ■ TCP ■ 面向连接的协议，可靠性高。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。 ■ 数据传输慢。 ■ UDP ■ 面向非连接的协议，可靠性低。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机制。 ■ 数据传输快。
端口	用来接收请求并向终端节点进行转发的监听端口，端口取值范围：**1~65499**。 每个监听可配置30个监听端口，端口之间使用半角逗号（,）分隔，例如80,90,8080。 如果您的端口为多个连续的端口，您可以使用波浪线（~）表示监听端口范围，例如80~85。 说明 ■ 同一全球加速实例下相同监听协议的监听端口不能冲突。 ■ 目前，部分地域支持一个监听可配置超过300个连续的端口。更多信息，请参见海量端口监听。
客户端亲和性	选择是否保持客户端亲和性： ■ **源IP**：保持客户端亲和性，即客户端访问有状态的应用程序时，可以将来自同一客户端的所有请求都定向到同一终端节点。 ■ **关闭**：不保持客户端亲和性，即不能确保来自同一客户端的连接请求始终定向到同一终端节点。

2. 配置终端节点。

每个监听都有与之关联的终端节点组，通过指定要向其分发流量的区域，可以将终端节点组与监听相关联，将流量分配到与监听关联的终端节点组内的最佳终端节点。
在**配置终端节点**配置向导页面，根据以下信息配置终端节点组和终端节点，然后单击**下一步**。
关于终端节点组和终端节点的详细信息，请参见终端节点组与终端节点概述。

配置	说明

配置	说明
节点组名称	输入终端节点组的名称。 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（_）和短划线（-）。
地域	选择终端节点组所属的地域。
流量调配	配置到不同终端节点组的流量比例。单位：%。 取值范围：0~100。 **说明** 您只有在配置TCP或UDP协议监听的终端节点组时，才支持配置**流量调配**。
后端服务部署在	选择后端服务器部署地。 ○ **阿里云**：后端服务器部署在阿里云。 ○ **非阿里云**：后端服务器部署在非阿里云。
保持客户端源IP	开启或关闭保持客户端源IP。 开启后，后端服务器可以通过该功能获取客户端源IP。更多信息，请参见保持客户端源IP。
终端节点	终端节点是客户端请求访问的目标主机。您可以根据以下信息配置终端节点： ○ **后端服务类型**：如果您的服务部署在阿里云，您可以选择**阿里云公网IP**、**ECS**、**CLB**、**ALB**或**OSS**；如果您的服务部署在非阿里云，您可以选择**自定义IP**或**自定义域名**。 **说明** ■ 目前，将ECS、CLB和ALB类型的后端服务作为实例级白名单开放。如果您的全球加速实例需添加ECS、CLB或ALB类型的后端服务，请先提交工单进行实例升级。 ■ 每个全球加速实例的终端节点出公网IP唯一，不与其他全球加速实例用户共享。 ■ 选择ECS、CLB、ALB、OSS作为后端服务类型，如果服务关联角色不存在，系统会自动创建对应的服务关联角色。更多信息，请参见AliyunServiceRoleForGaVpcEndpoint、AliyunServiceRoleForGaAlb和AliyunServiceRoleForGaOss。 ○ **后端服务**：输入后端服务器提供服务的IP地址、域名或实例ID。 ○ **权重**：输入终端节点权重，权重取值范围：0~255。全球加速根据您配置的权重按比例将流量路由到终端节点。 **注意** 如果某个终端节点的权重设置为0，全球加速将终止向该终端节点分发流量，请您谨慎操作。 您可以单击**+添加节点**添加多个终端节点，最多添加4个终端节点。若您需要添加更多终端节点，可在配额管理中提升配额。具体操作，请参见配额管理。

3. 配置审核。

在**配置审核**配置向导页面，确认监听和终端节点配置信息后，单击**提交**。
如果需要修改配置，您可以单击对应区域中的**修改**，返回到之前的配置页面进行修改。

> **说明** 首次配置监听，生效时间约为3分钟；修改监听配置，生效时间约为1分钟，请您耐心等待。

添加HTTP或HTTPS协议监听

1. 配置监听和协议。
   i. 登录全球加速管理控制台。
   ii. 在**实例列表**页面，找到目标全球加速实例，在**操作**列单击**配置监听**。
   iii. 在**监听**页签下，单击**添加监听**。

> **说明** 如果您是第一次添加监听，或当前全球加速实例下没有监听实例时，请跳过该步骤。

iv. 在**配置监听和协议**配置向导页面，根据以下信息配置监听和协议，然后单击**下一步**。

配置	说明
监听名称	输入监听的名称。 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（_）和短划线（-）。
协议	选择监听的网络传输协议类型： ■ **HTTPS**：HTTPS协议具有以下特性： ■ 面向连接的协议，可靠性高。在正式收发数据前，必须和对方建立可靠的连接。 ■ 通过绑定服务器SSL证书，保证数据的高可靠性。 ■ 数据加密传输。 ■ **HTTP**：HTTP协议具有以下特性： ■ 面向连接的协议，可靠性高。在正式收发数据前，必须和对方建立可靠的连接。 ■ 数据传输快。 ■ 数据明文传输。
端口	用来接收请求并向终端节点进行转发的监听端口，端口取值范围：**1~65499**。 HTTP或HTTPS协议的监听只支持配置一个监听端口。
客户端亲和性	选择是否保持客户端亲和性： ■ **源IP**：保持客户端亲和性，即客户端访问有状态的应用程序时，可以将来自同一客户端的所有请求都定向到同一终端节点。 ■ **关闭**：不保持客户端亲和性，即不能确保来自同一客户端的连接请求始终定向到同一终端节点。
高级配置	单击**修改**并选择**附加HTTP头字段**。 ■ 通过 `GA-ID` 头字段获取全球加速实例ID。 ■ 通过 `GA-AP` 头字段获取GA加速地域的信息。 ■ 通过 `GA-X-Forwarded-Proto` 头字段获取GA实例的监听协议。 ■ 通过 `GA-X-Forwarded-Port` 头字段获取GA实例的监听端口。 ■ 通过 `X-Real-IP` 头字段获取真实的客户端IP。

2. （可选）配置SSL证书。

   您只有在配置基于HTTPS协议的监听时，才需要添加服务器SSL证书。SSL证书为全球加速加密传输数据提供保障。

   i. 在**配置SSL证书**页面，选择您已经申请的SSL证书。

   ii. 在**高级配置**右侧单击**修改**，然后在**TLS安全策略**下拉列表选择目标策略。

   关于TLS安全策略，请参见TLS安全策略说明。

   iii. 单击**下一步**。

3. 配置终端节点。

   每个监听都有与之关联的终端节点组，您通过指定要向其分发流量的区域，将终端节点组与监听相关

联，系统自动将流量分配到与监听关联的终端节点组内的最佳终端节点。
在**配置终端节点**配置向导页面，根据以下信息配置终端节点组和终端节点，然后单击**下一步**。
关于终端节点组和终端节点的详细信息，请参见终端节点组与终端节点概述。

配置	说明
节点组名称	输入终端节点组的名称。 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（_）和短划线（-）。
地域	选择终端节点组所属的地域。
后端服务部署在	选择后端服务器部署地。 ○ **阿里云**：后端服务器部署在阿里云。 ○ **非阿里云**：后端服务器部署在非阿里云。
保持客户端源IP	开启或关闭保持客户端源IP。 HTTP和HTTPS监听协议默认开启保持客户端源IP功能，并将客户端源IP保存在HTTP请求头的 `X-Forwarded-For` 字段中。更多信息，请参见保持客户端源IP。
终端节点	终端节点是客户端请求访问的目标主机。您可以根据以下信息配置终端节点： ○ **后端服务类型**：如果您的服务部署在阿里云，您可以选择**阿里云公网IP**、**ECS**、**CLB**、**ALB**或**OSS**；如果您的服务部署在非阿里云，您可以选择**自定义IP**或**自定义域名**。 说明 ■ 目前，将ECS、CLB和ALB类型的后端服务作为实例级白名单开放。如果您的全球加速实例需添加ECS、CLB或ALB类型的后端服务，请先提交工单进行实例升级。 ■ 每个全球加速实例的终端节点出公网IP唯一，不与其他全球加速实例用户共享。 ■ 选择ECS、CLB、ALB、OSS作为后端服务类型，如果服务关联角色不存在，系统会自动创建对应的服务关联角色。更多信息，请参见AliyunServiceRoleForGaVpcEndpoint、AliyunServiceRoleForGaAlb和AliyunServiceRoleForGaOss。 ○ **后端服务**：输入后端服务器提供服务的IP地址、域名或实例ID。 ○ **权重**：输入终端节点权重，权重取值范围：0~255。全球加速根据您配置的权重按比例将流量路由到终端节点。 注意 如果某个终端节点的权重设置为0，全球加速将终止向该终端节点分发流量，请您谨慎操作。 您可以单击**+添加节点**添加多个终端节点，最多添加4个终端节点。

配置	说明
后端服务协议	选择后端服务器使用的服务协议： ○ **HTTP**（默认值） ○ **HTTPS** **说明** ○ 当您的监听协议为HTTP时，默认您的后端服务使用HTTP服务协议，且不支持更改。 ○ 您只有在配置HTTP或HTTPS协议监听的终端节点组时，才允许配置**后端服务协议**参数。
端口映射	当您监听的端口和您终端节点提供服务的端口不相同时，您需要输入端口映射关系。 ○ **监听端口**：只能填写当前监听的端口。 ○ **终端节点端口**：您终端节点提供服务的端口。 如果您监听的端口和您终端节点提供服务的端口相同，您无需填写端口映射关系，全球加速自动将访问请求发送至终端节点的监听端口。 **说明** 您只有在配置HTTP或HTTPS协议监听的终端节点组时，才允许配置**端口映射**参数。

4. 配置审核。

   在**配置审核**配置向导页面，确认监听和终端节点配置信息后，单击**提交**。
   如果需要修改配置，您可以单击对应区域中的**修改**，返回到之前的配置页面进行修改。

   说明 首次配置监听，生效时间约为3分钟；修改监听配置，生效时间约为1分钟，请您耐心等待。

说明 在您配置HTTP或HTTPS协议的监听后，您可以为该监听配置虚拟终端节点组和转发策略，配置后全球加速可同时加速多个域名或路径访问您后端的HTTP或HTTPS服务。具体操作，请参见添加和管理终端节点组和添加和管理转发策略。
更多信息，请参见单个全球加速实例加速访问多个HTTPS域名。

更多操作

操作	说明
编辑监听	当您的业务发生变化时，您可以修改监听和协议、SSL证书以及终端节点组信息，使监听配置满足您的业务需求。 1. 在**监听**页签下，找到目标监听，在**操作**列单击**编辑监听**。 2. 在**编辑监听**页面，修改监听和协议、SSL证书或终端节点组信息，然后单击**下一步**。 关于监听和协议、SSL证书以及终端节点组的更多信息，请参见添加TCP或UDP协议监听或添加HTTP或HTTPS协议监听。

操作	说明
删除监听	您可以删除监听，删除监听后，监听对应的终端节点组也会被删除。 1. 在**监听**页签下，找到目标监听，在**操作**列单击**删除**。 2. 在**删除监听**对话框中，单击**确定**。

相关文档

- CreateListener：为全球加速实例创建监听。
- UpdateListener：修改全球加速实例下指定监听的配置。
- DeleteListener：删除全球加速实例下指定的监听。

4.3. 绑定和管理证书

全球加速支持为HTTPS协议监听绑定多个证书。本文为您介绍如何为HTTPS协议监听绑定多个证书，并结合虚拟终端节点组和转发策略功能，实现加速访问多个HTTPS域名。

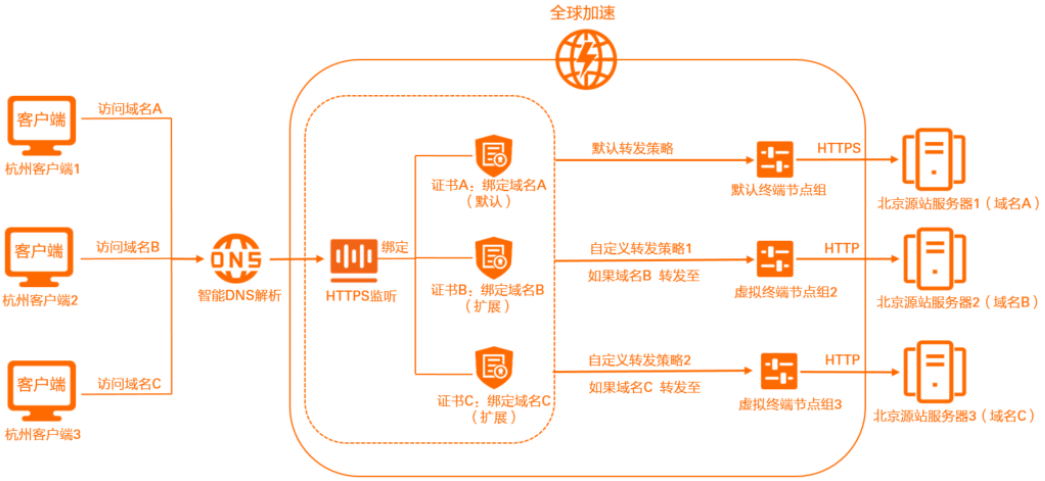
前提条件

- 您已经创建了全球加速实例和基础带宽包。具体操作，请参见创建和管理全球加速实例和购买和管理基础带宽包。
- 您已经添加了加速地域。具体操作，请参见添加加速区域。
- 您的网站已经完成备案。所有对中国内地（大陆）提供服务的网站都必须先进行ICP备案，才可开通服务。更多信息，请参见什么是ICP备案。
- 请确保您已经购买并申请了多个SSL证书。具体操作，请参见证书选型与购买和提交证书申请。

HTTPS协议监听证书管理

为全球加速配置HTTPS协议监听时，需要添加服务器SSL证书以确保您的业务受到加密保护并得到权威机构的身份认证。全球加速的HTTPS协议监听支持绑定多个证书，绑定的证书可分为以下两种类别：

- 默认服务器证书
  创建HTTPS协议监听时绑定的SSL证书为默认服务器证书。默认证书仅支持替换，不支持删除。
- 扩展证书
  对于已创建完成的HTTPS协议监听，您还可以绑定扩展证书。通过为HTTPS协议监听配置扩展证书，可以将多个域名关联到同一个HTTPS协议监听上，再配合基于域名的转发策略可以将不同域名的访问请求转发至不同的虚拟终端节点组。
  每个HTTPS协议监听上最多可绑定3个扩展证书。如需绑定更多扩展证书，可在配额管理提升gaplus_quota_additional_certs_per_listener的配额。配额提升后，一次操作最多可绑定10个扩展证书。具体操作，请参见配额管理。



配置流程

步骤一：绑定默认服务器证书

创建HTTPS协议监听并配置SSL证书，此时配置的证书即为默认服务器证书，配置的终端节点组为默认终端节点组。关于HTTPS协议监听详细信息，请参见添加HTTP或HTTPS协议监听。

1. 登录全球加速管理控制台。
2. 在**实例列表**页面，找到目标全球加速实例，在**操作**列单击**配置监听**。
3. 在**监听**页签下，单击**添加监听**。

> **说明** 如果您是第一次添加监听，或当前全球加速实例下没有监听实例时，请跳过该步骤。

4. 在**配置监听和协议**配置向导页面，配置监听和协议，然后单击**下一步**。
5. 在**配置SSL证书**配置向导页面，选择您已经申请的SSL证书，然后单击**下一步**。

   此处选择的证书即为该HTTPS协议监听的默认服务器证书。
   您还可以根据需要在**高级配置**中选择安全策略，关于TLS安全策略，请参见TLS安全策略说明。
6. 在**配置终端节点**配置向导页面，配置终端节点组和终端节点，然后单击**下一步**。

   此处配置的终端节点组即为该HTTPS协议监听的默认终端节点组。
7. 在**配置审核**配置向导页面，确认配置信息后，单击**提交**。

步骤二：添加虚拟终端节点组

将多个源站服务器分别添加为虚拟终端节点组。具体操作，请参见添加虚拟终端节点组。

步骤三：绑定扩展证书

1. 登录全球加速管理控制台。
2. 在**实例列表**页面，找到目标全球加速实例，在**操作**列单击**配置监听**。
3. 在**监听**页签下，找到目标HTTPS协议监听，单击监听实例ID。
4. 在监听实例详情页面下，单击**证书管理**页签。
5. 在**证书管理**页签下的**扩展证书**区域，单击**绑定证书**。

6. 在**绑定证书**对话框，根据以下信息配置扩展证书，然后单击**确定**。
   - **证书**：选择需要绑定的证书。
   - **关联域名**：选择该证书下需要使用全球加速服务加速访问的域名。您可以选择多个域名进行关联，所有扩展证书最多可关联3个域名。

   您可以单击**+绑定证书**一次绑定多个扩展证书。每个HTTPS协议监听最多可添加3个扩展证书，如需绑定更多扩展证书，可在配额管理提升gaplus_quota_additional_certs_per_listener的配额。具体操作，请参见配额管理。

步骤四：添加转发策略

为多个虚拟终端节点组分别添加基于域名的转发策略。具体操作，请参见添加和管理转发策略。

步骤五：配置CNAME域名解析

为要加速的多个源站服务器域名配置CNAME。域名通过DNS解析到全球加速的CNAME地址，访问请求才能转发到全球加速，实现加速效果。具体操作，请参见配置CNAME。

更多操作

操作	说明
替换默认服务器证书	1. 在**监听**页签下，找到目标HTTPS协议监听，单击监听实例ID。 2. 在监听实例详情页面下，单击**证书管理**页签。 3. 在**证书管理**页签下的**默认服务器证书**区域，在默认服务器证书操作列单击**替换**。 4. 在更换默认服务器证书对话框，选择目标证书，然后单击**确定**。
解绑扩展证书	解绑操作仅将扩展证书和全球加速实例HTTPS监听进行解绑，如果您需要删除证书，请参见删除SSL证书。 1. 在**监听**页签下，找到目标HTTPS协议监听，单击监听实例ID。 2. 在监听实例详情页面下，单击**证书管理**页签。 3. 在**证书管理**页签下的**扩展证书**区域，根据以下信息，解绑单个或多个扩展证书。 ○ 解绑单个扩展证书：找到目标扩展证书，在**操作**列单击**解绑**。 ○ 批量解绑扩展证书：选中多个目标扩展证书，在扩展证书列表下单击**批量解绑**。 4. 在解绑对话框，单击**确定**。

相关文档

- AssociateAdditionalCertificatesWithListener：为HTTPS监听绑定扩展证书。
- DissociateAdditionalCertificatesFromListener：解绑扩展证书。
- ListListenerCertificates：查询监听绑定的证书列表。

4.4. TLS安全策略说明

为全球加速实例配置HTTPS监听时，支持选择TLS安全策略。系统默认选择tls_cipher_policy_1_0安全策略，若您有更高的安全要求，可以根据需要选择更高等级的TLS安全策略。

TLS安全策略

TLS安全策略包含HTTPS可选的TLS协议版本和配套的加密算法套件。TLS协议版本越高，HTTPS通信的安全性越高，但是相较于低版本TLS协议，高版本TLS协议对浏览器的兼容性较差。TLS安全策略对应的TLS协议版本和配套的加密算法套件如下：

安全策略	支持TLS版本	支持加密算法套件
tls_cipher_policy_1_0	TLSv1.0、TLSv1.1和TLSv1.2	• ECDHE-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_cipher_policy_1_1	TLSv1.1和TLSv1.2	• 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

安全策略	支持TLS版本	支持加密算法套件
tls_cipher_policy_1_2	TLSv1.2	• 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_cipher_policy_1_2_strict	TLSv1.2	• ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES128-SHA256 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES128-SHA • ECDHE-RSA-AES256-SHA
tls_cipher_policy_1_2_strict_with_1_3	TLSv1.2及TLSv1.3	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256 • TLS_AES_128_CCM_SHA256 • TLS_AES_128_CCM_8_SHA256 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES128-SHA256 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES128-SHA • ECDHE-ECDSA-AES256-SHA • ECDHE-RSA-AES128-SHA • ECDHE-RSA-AES256-SHA

TLS安全策略支持的加密算法套件

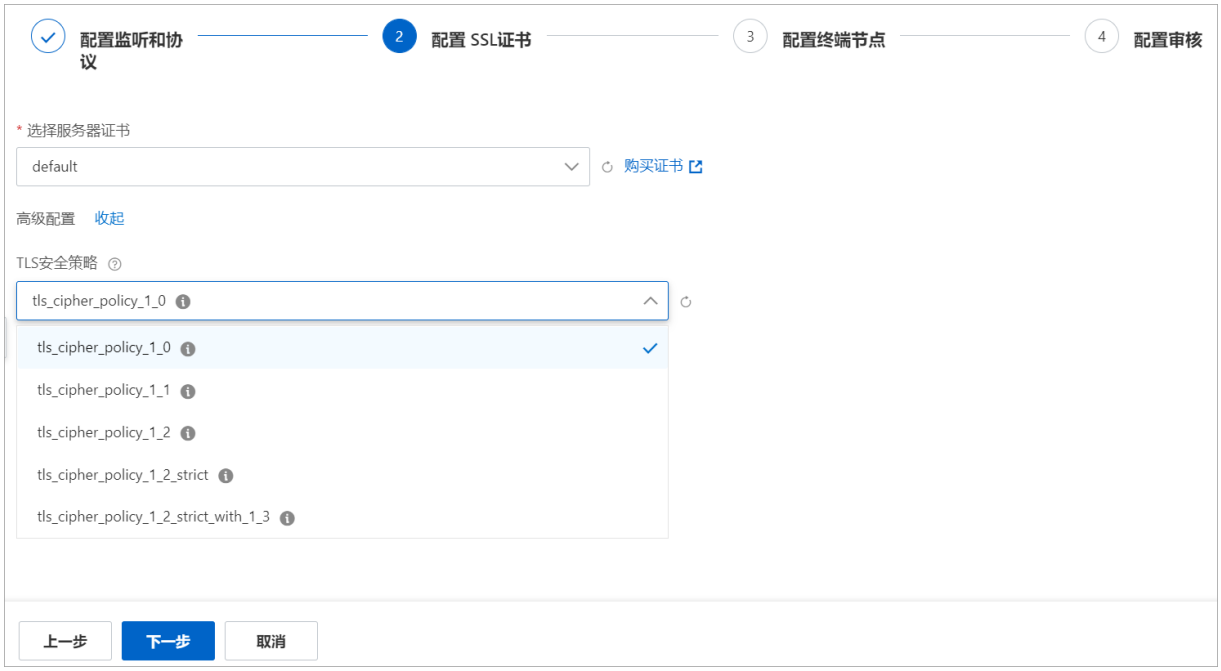
安全策略		tls_cipher_policy_1_0	tls_cipher_policy_1_1	tls_cipher_policy_1_2	tls_cipher_policy_1_2_strict	tls_cipher_policy_1_2_strict_with_1_3
TLS		1.2、1.1及1.0	1.1及1.2	1.2	1.2	1.2及1.3
CIPHER	ECDHE-RSA-AES128-GCM-SHA256	✔	✔	✔	✔	✔
	ECDHE-RSA-AES256-GCM-SHA384	✔	✔	✔	✔	✔
	ECDHE-RSA-AES128-SHA256	✔	✔	✔	✔	✔
	ECDHE-RSA-AES256-SHA384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

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

说明 上表中的✔表示支持，-表示不支持。

选择TLS安全策略

在您添加或者配置HTTPS监听时，系统默认选择tls_cipher_policy_1_0安全策略。您可以通过修改高级配置选择TLS安全策略。具体操作，请参见添加HTTP或HTTPS协议监听。



5.终端节点组与终端节点

5.1. 终端节点组与终端节点概述

每个监听都有与之关联的终端节点组，每个终端节点组都有一个或多个终端节点。

终端节点组

每个终端节点组都与特定的地域关联，通过指定要分发流量的地域，将终端节点组与监听关联。关联后，系统自动将流量分配到与监听关联的终端节点组内的最佳终端节点上。

不同协议的监听支持创建的终端节点组的类型不同：

- TCP或UDP协议的监听
  默认支持创建2个默认终端节点组，如果您需要创建更多默认终端节点组，可在配额管理提升gaplus_quota_epgs_per_listener的配额。具体操作，请参见配额管理。
  每个默认终端节点组的地域必须唯一。您可以为不同地域的默认终端节点组设置流量调配，流量调配确定了全球加速将访问请求定向到各默认终端节点组的流量比例。
- HTTP或HTTPS协议的监听
  默认支持创建1个默认终端节点组和1个虚拟终端节点组，如果您需要创建多个虚拟终端节点组，可在配额管理提升gaplus_quota_vepg_per_listener的配额。具体操作，请参见配额管理。
  - 默认终端节点组：创建HTTP或HTTPS协议的监听时配置的终端节点组为默认终端节点组。
  - 虚拟终端节点组：在您创建监听后，您可以在**终端节点组**页面手动创建虚拟终端节点组。
    在您为HTTP或HTTPS协议的监听创建虚拟终端节点组后，您可以创建转发策略并关联该虚拟终端节点组。关联后，HTTP或HTTPS协议的监听可以根据转发策略将不同域名或不同路径的访问请求转发至对应的默认终端节点组或虚拟终端节点组中，实现一个全球加速实例同时加速多个域名或路径访问后端服务。关于如何创建转发策略，请参见添加和管理转发策略。

终端节点

终端节点是客户端请求访问的目标主机，一个终端节点组可以添加1~4个终端节点。终端节点的后端服务类型如下：

后端服务部署在	网络连接类型	后端服务类型	后端服务
阿里云	公网连接类型	阿里云公网IP	• 弹性公网IP（Elastic IP Address，简称EIP） • 固定公网IP 固定公网IP包括云服务器ECS系统分配的公网IP地址（PublicIP）和经典网络公网CLB的公网IP。
	私网连接类型	ECS	云服务器ECS（Elastic Compute Service）实例 仅支持专有网络类型的ECS。
		CLB	传统型负载均衡CLB（Classic Load Balancer）实例 仅支持专有网络类型的CLB。
		ALB	应用型负载均衡ALB（Application Load Balancer）实例

后端服务部署在	网络连接类型	后端服务类型	后端服务
		OSS	对象存储服务OSS（Object Storage Service）的Bucket实例
非阿里云	公网连接类型	自定义IP	自定义源站IP
		自定义域名	自定义源站域名

> 说明
>
> - 目前，将ECS、CLB和ALB类型的后端服务作为实例级白名单开放。如果您的全球加速实例需添加ECS、CLB或ALB类型的后端服务，请先提交工单进行实例升级。
> - 每个全球加速实例的终端节点出公网IP唯一，不与其他全球加速实例用户共享。

您可以设置终端节点权重，权重确定了全球加速将访问请求定向到终端节点的流量比例。全球加速会计算终端节点组中各个终端节点的权重之和，然后根据每个终端节点的权重与总权重之比将流量定向到终端节点。具体操作，请参见更多操作。

健康检查

通过为全球加速实例的终端节点组开启健康检查功能，可以提高业务的可靠性和可用性、避免异常终端节点对服务的影响。

终端节点组开启健康检查后，当某个终端节点健康检查出现异常时，全球加速会自动将新的请求分发到其它健康检查正常的终端节点上；而当健康检查异常的终端节点恢复正常后，全球加速会将该终端节点自动恢复到请求服务中。更多信息，请参见开启和管理健康检查。

相关文档

- 添加和管理终端节点组
- 添加和管理转发策略
- 开启和管理健康检查

5.2. 多终端节点组流量调配原理及应用场景

全球加速支持为单个TCP和UDP协议的监听配置多个不同地域的终端节点组。您可以为终端节点组设置流量调配值，灵活控制转发到各终端节点组的访问流量比例，同时，您还可以为终端节点组开启健康检查，剔除异常的终端节点组。

多终端节点组流量调配原理

流量调配介绍

全球加速支持设置终端节点组流量调配，调整多个终端节点组的访问流量比例，实现访问流量的合理调配，为用户提供更好的访问体验。

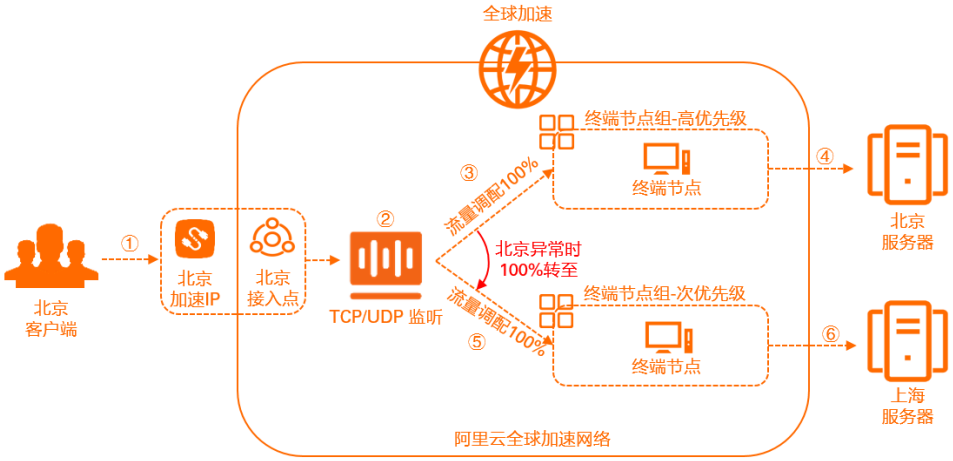
- 流量调配：表示访问流量的调配权重，取值范围为0%~100%，默认值为100%。0%表示忽略此终端节点组，不向该终端节点组转发访问流量，100%表示访问流量全部转发到此终端节点组。
- 调度优先级：终端节点组最终实际的流量分配，不仅取决于设置的终端节点组流量调配，还依赖于终端节点组调度优先级。全球加速基于网络时延（主要依赖于地理位置和网络链路情况）得出调度优先级。一般来说，接入点到每个终端节点组地域的地理位置越近，网络链路越短，调度优先级越高。访问流量会被优先调度至离接入点最近的终端节点组。

> **说明** 为各终端节点组开启了健康检查后，若高优先级的终端节点组健康检查异常，访问流量将全部转发至次优先级终端节点组，此时转发权重与设置的流量调配值无关。

流量调配计算

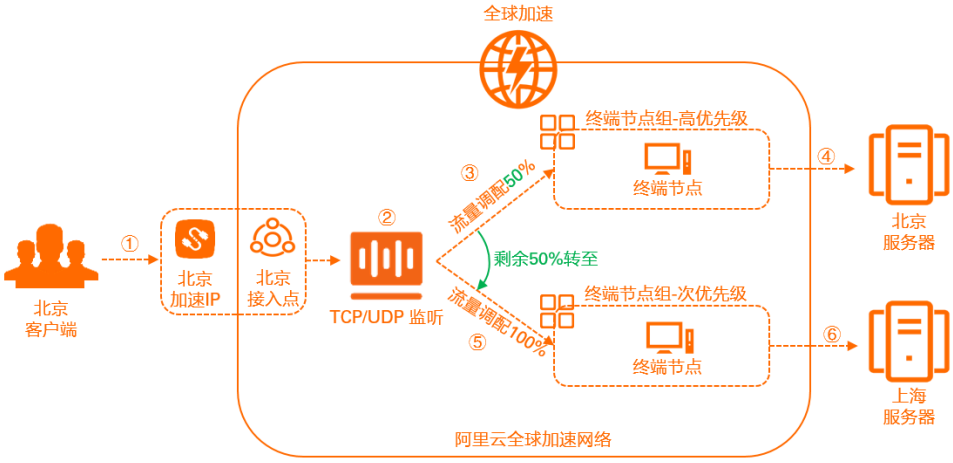
您可以通过以下示例了解流量调配原理：

- 单加速地域对应多终端节点组
  假设某应用的客户端集中在北京地域，服务器部署在北京和上海地域，已通过全球加速添加了北京加速地域、北京地域终端节点组和上海地域终端节点组。现在需要按需分配北京和上海的访问流量比例。
  - 各终端节点组流量调配均设置为100%



序号	调度流程说明
①	客户端访问流量被就近调度到北京接入点，进入阿里云加速网络。
②	监听根据配置的协议与端口检查客户端的连接请求，并根据各个终端节点组的调度优先级与设置的流量调配值选择接收请求的终端节点组。
③	北京终端节点组优先级高于上海终端节点组，健康检查正常且流量调配为100%，访问流量全部被转发到北京终端节点组。
④	客户端请求由北京的服务器处理。
⑤	当北京终端节点组健康检查异常时，次优先级的上海终端节点组健康检查正常，那么监听会将流量全部转发到上海终端节点组。
⑥	客户端请求由上海的服务器处理。

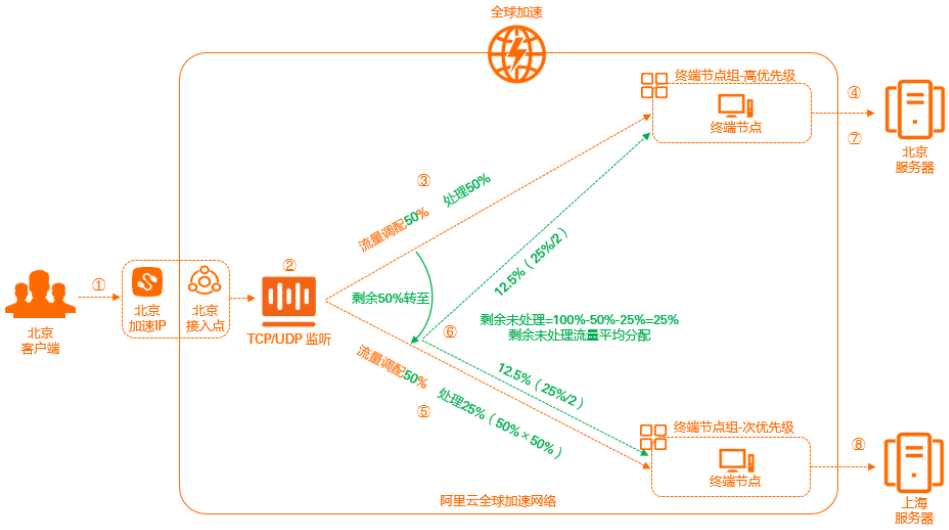
- 北京终端节点组流量调配调整为50%（您也可以按需调整为其他值），上海终端节点组为100%



与流量调配为100%时的调度流程类似，北京客户端访问流量会被优先转发到北京终端节点组。根据流量调配50%，将前50%的访问流量转发至北京终端节点组处理，剩余50%将被转发至上海终端节点组。同样，若流量调配为30%时，将前30%的访问流量转发至北京终端节点组，剩余70%将被转发至上海终端节点组。

同时，上海终端节点组的流量调配为100%，则剩余访问流量（如上剩余50%或70%）将全部由上海终端节点组接收。

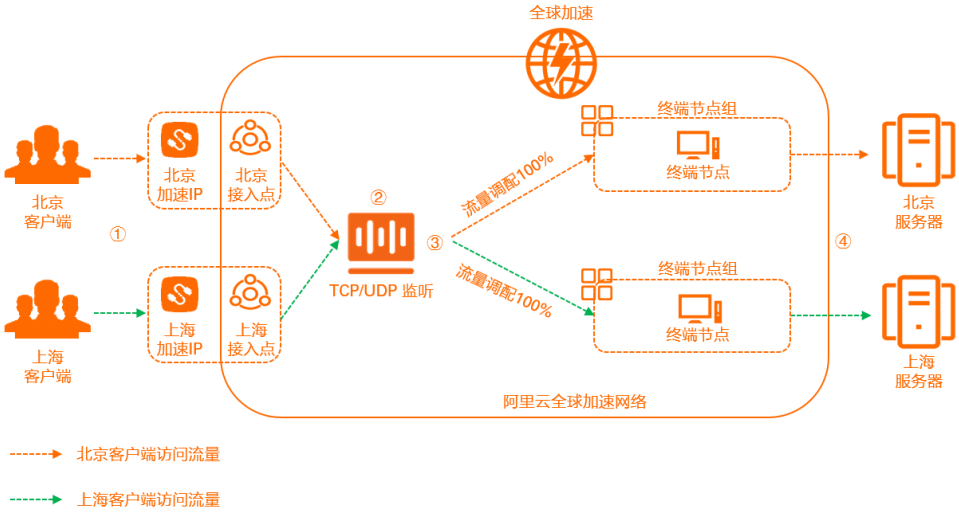
- 各终端节点组流量调配均设置为50%（您也可以按需调整为其他值）



序号	调度流程说明
①	客户端访问流量被就近调度到北京接入点，进入阿里云加速网络。
②	监听根据配置的协议与端口检查客户端的连接请求，并根据各个终端节点组的调度优先级与设置的流量调配值选择接收请求的终端节点组。
③	北京终端节点组优先级高于上海终端节点组，健康检查正常且流量调配为50%，访问流量50%转发到北京终端节点组。
④	北京服务器处理访问流量的50%。
⑤	剩余50%被转至次优先级的上海终端节点组，根据上海终端节点组流量调配50%，则上海终端节点组接收剩余流量的50%，即50%×50%=25%。 此时，北京终端节点组接收50%，上海终端节点组接收25%，还有25%访问流量未被接收。
⑥	对客户端访问流量剩余未被接收部分进行二次调度，二次调度方式为剩余未被接收部分在每个终端节点组平均分配。 剩余未被接收的25%访问流量平均分配至各终端节点组，即北京和上海终端节点组各接收12.5%。
⑦	北京的服务器处理接收的12.5%的访问流量。
⑧	上海的服务器处理37.5%的访问流量，即25%+12.5%=37.5%。

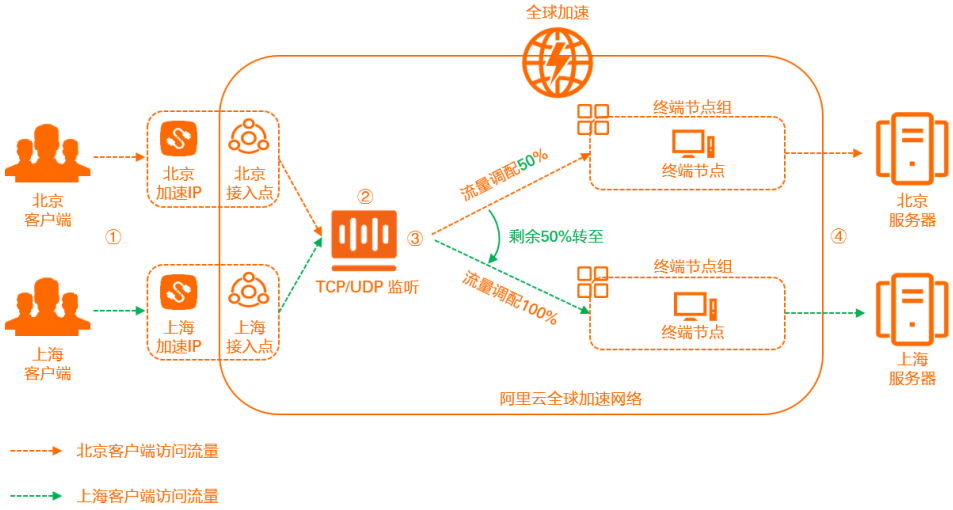
- 多加速地域对应多终端节点组
  当客户端分布在多个地域，即有多个加速地域时，客户端的访问流量通过加速IP从就近接入点进入阿里云加速网络，再根据调度优先级调度至离接入点最近的终端节点组。

- 各终端节点组流量调配均设置为100%



序号	调度流程说明
①	北京和上海客户端的访问流量分别被就近调度到北京和上海接入点，进入阿里云加速网络。
②	监听根据配置的协议与端口检查客户端的连接请求，并根据各个终端节点组的调度优先级与设置的流量调配值选择接收请求的终端节点组。
③	根据流量调配值，对各地域客户端访问流量进行调度。 ■ 北京客户端访问流量调度情况 北京终端节点组优先级高于上海终端节点组，健康检查正常且流量调配为100%，北京客户端的访问流量全部被转发到北京终端节点组。 ■ 上海客户端访问流量调度情况 上海终端节点组优先级高于北京终端节点组，健康检查正常且流量调配为100%，上海客户端的访问流量全部被转发到上海终端节点组。
④	上海和北京的服务器分别处理各自接收到的访问流量。

- 北京终端节点组流量调配调整为50%（您也可以按需调整为其他值），上海终端节点组为100%

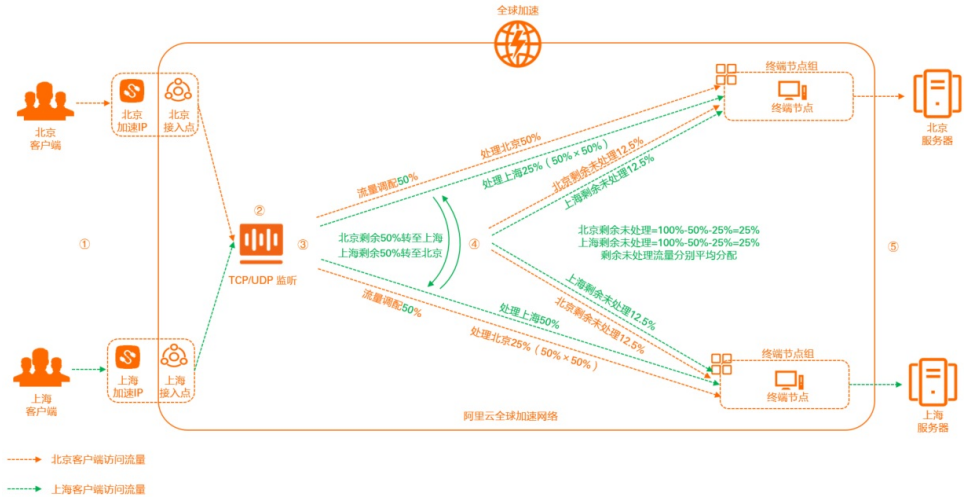


与流量调配为100%时的调度流程类似，北京客户端访问流量会被优先转发到北京终端节点组。根据流量调配50%，将前50%的访问流量转发至北京终端节点组，剩余50%将被转发至上海终端节点组。同样，若流量调配为30%时，将前30%的访问流量转发至北京终端节点组，剩余70%将被转发至上海终端节点组。

上海客户端访问流量会被优先转发到上海终端节点组，根据上海终端节点组流量调配100%，上海客户端访问流量全部被上海终端节点组接收。

最终，北京终端节点组接收50%的北京客户端访问流量，上海终端节点组接收100%上海客户端访问流量和北京客户端剩余50%的访问流量。

- 各终端节点组流量调配均设置为50%（您也可以按需调整为其他值）



序号	调度流程说明
①	北京和上海客户端的访问流量分别被就近调度到北京和上海接入点，进入阿里云加速网络。
②	监听根据配置的协议与端口检查客户端的连接请求，并根据各个终端节点组的调度优先级与设置的流量调配值选择接收请求的终端节点组。
③	根据流量调配值，对各地域客户端访问流量进行首次调度。 ■ 北京客户端访问流量调度情况 北京终端节点组优先级高于上海终端节点组，健康检查正常且流量调配为50%，访问流量50%转发到北京终端节点组，剩余50%转发至上海终端节点组。根据上海终端节点组流量调配50%，则上海终端节点组接收北京剩余流量的50%，即50%×50%=25%。此时，北京剩余25%（100%-50%-25%）访问流量未被接收。 ■ 上海客户端访问流量调度情况 上海终端节点组优先级高于北京终端节点组，健康检查正常且流量调配为50%，访问流量50%转发到上海终端节点组，剩余50%转发至北京终端节点组。根据北京终端节点组流量调配50%，则北京终端节点组接收上海剩余流量的50%，即50%×50%=25%。此时，上海剩余25%（100%-50%-25%）访问流量未被接收。
④	对各地域客户端访问流量剩余未被接收部分进行二次调度，二次调度方式为剩余未被接收部分在每个终端节点组平均分配。 北京剩余未被接收的25%访问流量平均分配到北京终端节点组和上海终端节点组，即各终端节点组分别接收12.5%。同样，上海剩余未被接收的25%访问流量，各终端节点组也分别接收12.5%。
⑤	上海和北京的服务器分别处理各自接收到的访问流量。

应用场景

应用场景概览

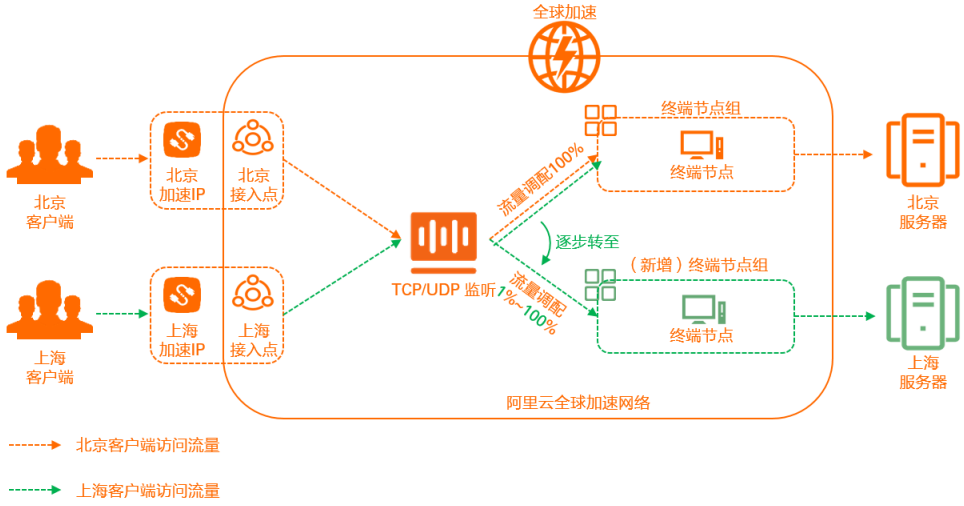
场景	说明
服务多地域部署	针对原有的服务器不满足现有应用需求或部分地域用户群体验不佳时，例如不同的用户群共用一个加速区域，或多个加速区域共用一个终端节点组，需要在新地域上线服务。

场景	说明
访问流量多地域负载	针对单地域部署服务造成的传输线路流量过大或者服务器负载过高问题，可考虑将服务部署在不同地域，将不同地域的后端服务分别配置为终端节点组，再通过流量调配功能调整不同地域访问流量的分配比例，来降低单一地域的访问压力。
服务跨地域容灾	对服务连续性和可靠性有一定要求时，可跨地域部署服务，将不同地域的后端服务分别配置为终端节点组并开启健康检查功能。当某个地域服务出现异常时，可将访问流量转发至正常地域，实现容灾需求。
按地域下线或升级服务	针对地域级业务调整，例如需要平滑下线访问量较小的某地域服务或升级某地域服务，可通过终端节点组的流量调配功能将此地域访问流量进行灵活迁移。

服务多地域部署

当业务扩展，原有的服务器不满足现有应用的需求或部分地域用户体验不佳时，需要在新的地域部署该服务。您可以通过为全球加速新增终端节点组或加速地域，来提升用户访问体验。

- 新增终端节点组，提升服务处理能力
  以下图场景为例。某应用部署在北京地域，原有的北京和上海客户端分别由北京和上海接入点接入，访问请求均由北京终端节点组的服务器进行处理。随着用户量增大，服务器负载越来越高。



  您可以增加上海终端节点组，将上海客户端的访问流量迁移到上海终端节点组的服务器中，实现应用服务能力提升。实现步骤如下：

  i. 在上海地域部署服务器。

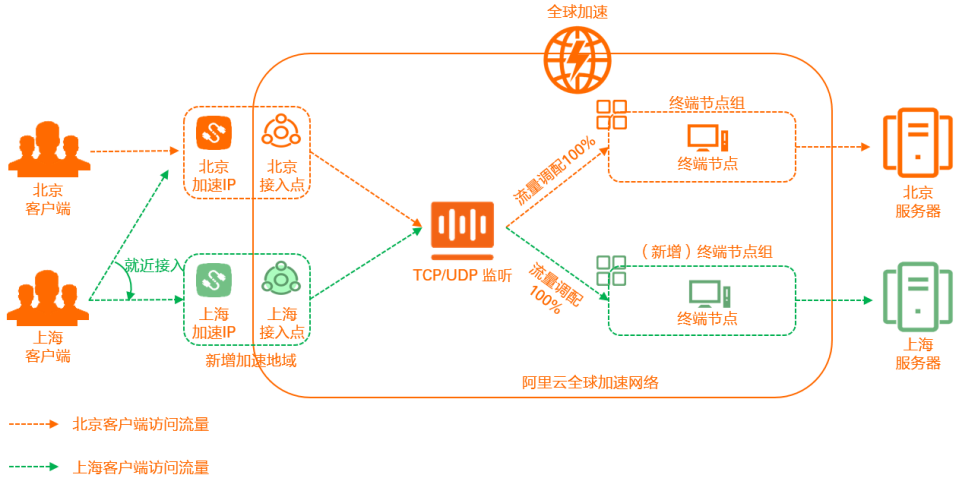
  ii. 在全球加速对应监听中添加上海地域终端节点组。具体操作，请参见添加默认终端节点组。
  添加上海终端节点组时，可先将流量调配配置为一个较小的值，例如1%，以进行调试。

  iii. 调试验证上海客户端访问流量转发情况。
  此时，北京客户端的访问流量继续由北京终端节点组的服务器处理，上海客户端访问流量中1%由上海终端节点组的服务器处理，剩余99%转发至北京终端节点组的服务器处理。

  iv. 调试成功后，修改上海地域终端节点组的流量调配为100%。
  上海客户端的访问流量完全迁移到上海终端节点组的服务器中，北京终端节点组的服务器不再处理上海客户端的访问请求。具体操作，请参见设置终端节点组流量调配。

- 新增加速地域，提升用户访问体验

以下图场景为例。假设某应用部署在北京，客户端集中在北京和上海地域，均通过北京接入点接入全球加速网络，所有访问请求均由北京终端节点组的服务器处理。上海客户端经常出现延迟、抖动等网络问题。

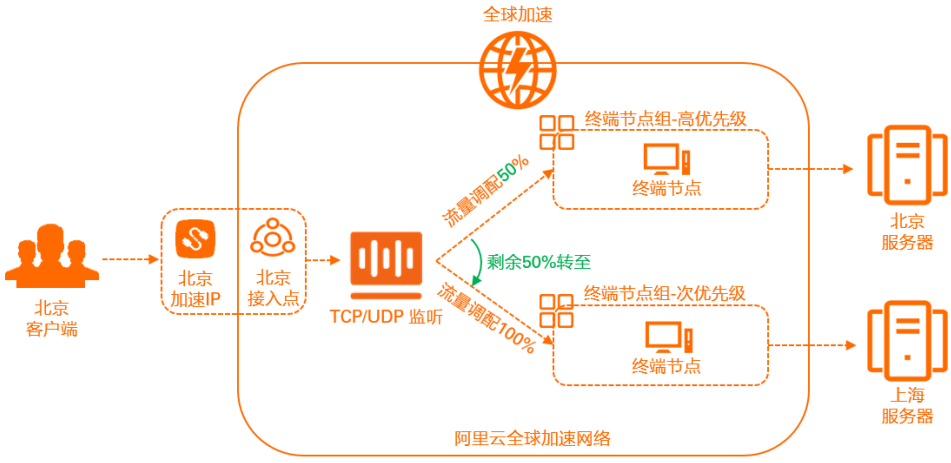


您可以在上海地域部署该服务，为全球加速实例添加上海加速地域和上海地域的终端节点组。上海客户端的访问请求将就近接入上海接入点，经监听检查处理后转发至离上海接入点较近的上海终端节点组。最终实现上海客户端访问体验的提升。具体操作，请参见添加加速区域和添加默认终端节点组。

访问流量多地域负载

您可以通过流量调配功能将某个加速地域的访问流量分配至多个不同地域的终端节点组，从而降低该加速地域对应终端节点组服务器的负载。

如下图场景所示。假设某应用部署在北京和上海，客户端主要集中在北京地域。已通过全球加速添加了北京加速地域、北京地域终端节点组和上海地域终端节点组，全球加速默认将北京客户端的访问流量全部就近转发至北京终端节点组的服务器进行处理。由于北京访问流量较大，导致北京地域终端节点组的服务器负载过大，客户端访问出现卡顿、丢包等情况。

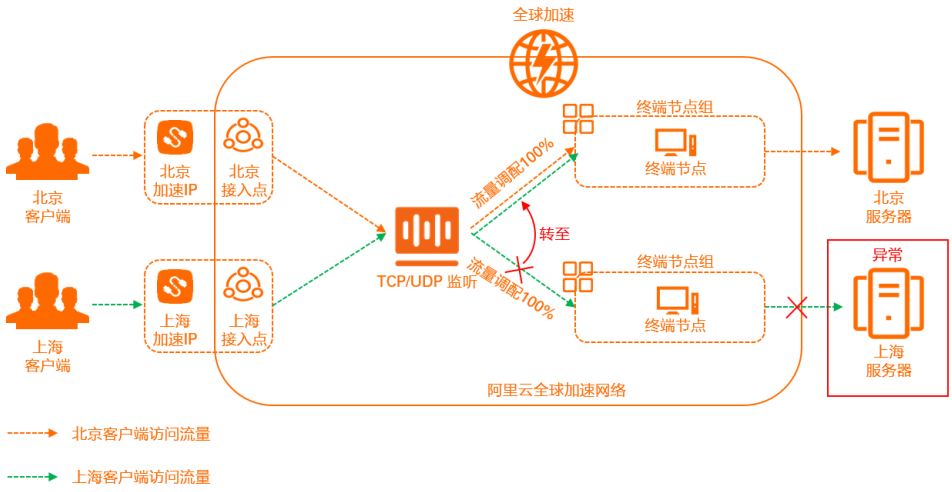


您可以根据需求调整北京和上海地域终端节点组的流量调配值，例如将北京终端节点组的默认流量调配值100%修改为50%，此时，北京客户端的50%访问流量由北京终端节点组的服务器处理，剩余50%访问流量转发至上海终端节点组的服务器处理，实现北京地域访问流量的合理分配，降低北京终端节点组中服务器的压力。修改终端节点组流量调配，请参见设置终端节点组流量调配。

服务跨地域容灾

您可以通过在全球加速中添加多个不同地域的终端节点组，并为多个终端节点组开启健康检查，实现服务跨地域容灾。

如下图场景所示，假设某应用部署在北京和上海，已通过全球加速在上海和北京地域分别添加了对应的加速地域和终端节点组。正常情况下，北京和上海客户端的访问请求会被就近接入对应的加速地域，通过监听检查处理，再根据流量调配值和调度优先级分别转发至对应的终端节点组。为保证应用能持续稳定的对外提供服务，要求北京或上海其中任意一个地域的应用出现异常时，可将异常地域的访问流量自动切换至另一个运行正常的地域。

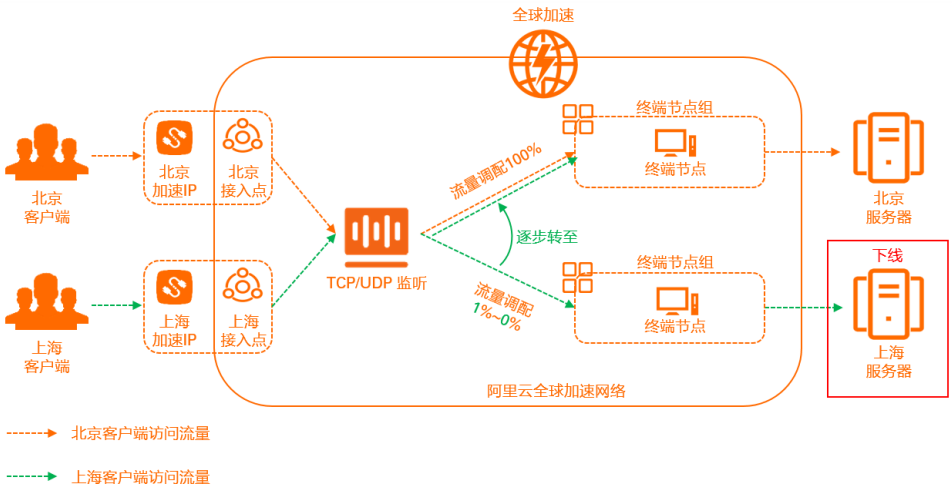


您可以分别为北京和上海地域的终端节点组开启健康检查，当上海地域终端节点组健康检查出现异常时，监听会自动将访问流量调度至健康检查正常的北京地域终端节点组；而当上海地域终端节点组恢复正常后，监听会自动恢复上海客户端的流量调配，将上海客户端的访问流量全部调度至上海地域终端节点组。健康检查的配置，请参见开启和管理健康检查。

按地域下线或升级服务

您可以通过流量调配功能，实现服务按地域下线或升级，降低对客户端访问的影响。

以下图场景为例。假设某公司业务部署在北京和上海地域，已通过全球加速在上海和北京地域分别添加了对应的加速地域和终端节点组。现位于上海的服务因访问量较小，需要暂时下线，要求下线过程中，不会影响上海客户端的正常访问。



您可以先将上海地域终端节点组的流量调配配置为较小的值，例如1%，将剩余99%的访问流量切换至北京地域的终端节点组。待上海地域访问请求量降低至您预期的可下线状态后，再将流量调配配置为0%，此时您可以下线部署在上海地域的服务。

同样，当需要升级上海服务时，可以先按照上述下线过程调整流量调配值，当流量调配值为0%时，上海的客户端访问流量全部被调度至北京终端节点组。升级完成后，再将上海地域终端节点组流量调配配置为100% ，从而恢复上海客户端的流量调度。

5.3. 添加和管理终端节点组

每个监听都有与之关联的终端节点组，通过指定要向其分发流量的地域，可以使终端节点组与监听相关联，系统自动将流量分配到与监听关联的终端节点组内的最佳终端节点。

前提条件

您已经创建了全球加速实例。具体操作，请参见创建和管理全球加速实例。

背景信息

每个终端节点组都与特定的地域关联，通过指定要分发流量的地域，将终端节点组与监听关联。关联后，系统自动将流量分配到与监听关联的终端节点组内的最佳终端节点上。

不同协议的监听支持创建的终端节点组的类型不同：

- TCP或UDP协议的监听
  默认支持创建2个默认终端节点组，如果您需要创建更多默认终端节点组，可在配额管理提升gaplus_quota_epgs_per_listener的配额。具体操作，请参见配额管理。
  每个默认终端节点组的地域必须唯一。您可以为不同地域的默认终端节点组设置流量调配，流量调配确定了全球加速将访问请求定向到各默认终端节点组的流量比例。
- HTTP或HTTPS协议的监听
  默认支持创建1个默认终端节点组和1个虚拟终端节点组，如果您需要创建多个虚拟终端节点组，可在配额管理提升gaplus_quota_vepg_per_listener的配额。具体操作，请参见配额管理。
  - 默认终端节点组：创建HTTP或HTTPS协议的监听时配置的终端节点组为默认终端节点组。
  - 虚拟终端节点组：在您创建监听后，您可以在**终端节点组**页面手动创建虚拟终端节点组。
    在您为HTTP或HTTPS协议的监听创建虚拟终端节点组后，您可以创建转发策略并关联该虚拟终端节点组。关联后，HTTP或HTTPS协议的监听可以根据转发策略将不同域名或不同路径的访问请求转发至对应的默认终端节点组或虚拟终端节点组中，实现一个全球加速实例同时加速多个域名或路径访问后端服务。关于如何创建转发策略，请参见添加和管理转发策略。

添加默认终端节点组

1.
2. 在**实例列表**页面，找到目标全球加速实例，在**操作**列单击**配置监听**。
3. 在**监听**页签下，单击**添加监听**。

   > **说明** 如果您是第一次配置终端节点组，请跳过该步骤。

4. 在**配置监听和协议**配置向导页面，配置监听和协议，然后单击**下一步**。

   如果您在为HTTPS协议的监听配置终端节点组，您还需要配置SSL证书。具体操作，请参见添加和管理监听。
5. 在**配置终端节点**配置向导页面，根据以下信息配置终端节点。

配置	说明
节点组名称	输入终端节点组的名称。 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（_）和短划线（-）。
地域	选择终端节点组所属的地域。

配置	说明
流量调配	配置到不同终端节点组的流量比例。单位：%。 取值范围：0~100。 **说明** 您只有在配置TCP或UDP协议监听的终端节点组时，才支持配置**流量调配**。
后端服务部署在	选择后端服务器部署地。 ○ **阿里云**：后端服务器部署在阿里云。 ○ **非阿里云**：后端服务器部署在非阿里云。
保持客户端源IP	开启或关闭保持客户端源IP。 开启后，后端服务器可以通过该功能获取客户端源IP。更多信息，请参见保持客户端源IP。
终端节点	终端节点是客户端请求访问的目标主机。您可以根据以下信息配置终端节点： ○ **后端服务类型**：如果您的服务部署在阿里云，您可以选择**阿里云公网IP**、**ECS**、**CLB**、**ALB**或**OSS**；如果您的服务部署在非阿里云，您可以选择**自定义IP**或**自定义域名**。 **说明** ■ 目前，将ECS、CLB和ALB类型的后端服务作为实例级白名单开放。如果您的全球加速实例需添加ECS、CLB或ALB类型的后端服务，请先提交工单进行实例升级。 ■ 每个全球加速实例的终端节点出公网IP唯一，不与其他全球加速实例用户共享。 ■ 选择ECS、CLB、ALB、OSS作为后端服务类型，如果服务关联角色不存在，系统会自动创建对应的服务关联角色。更多信息，请参见AliyunServiceRoleForGaVpcEndpoint、AliyunServiceRoleForGaAlb和AliyunServiceRoleForGaOss。 ○ **后端服务**：输入后端服务器提供服务的IP地址、域名或实例ID。 ○ **权重**：输入终端节点权重，权重取值范围：0~255。全球加速根据您配置的权重按比例将流量路由到终端节点。 **注意** 如果某个终端节点的权重设置为0，全球加速将终止向该终端节点分发流量，请您谨慎操作。 您可以单击**+添加节点**添加多个终端节点，最多添加4个终端节点。若您需要添加更多终端节点，可在配额管理中提升配额。具体操作，请参见配额管理。

配置	说明
后端服务协议	选择后端服务使用的服务协议： ○ **HTTP**（默认值）。 ○ **HTTPS**。 **说明** ○ 当您的监听协议为HTTP时，默认您的后端服务使用HTTP服务协议，且不支持更改。 ○ 您只有在配置HTTP或HTTPS协议监听的终端节点组时，才允许配置**后端服务协议**参数。
端口映射	当您监听的端口和您终端节点提供服务的端口不相同时，您需要输入端口映射关系。 ○ **监听端口**：只能填写当前监听的端口。 ○ **终端节点端口**：您终端节点提供服务的端口。 如果您监听的端口和您终端节点提供服务的端口相同，您无需填写端口映射关系，全球加速自动将访问请求发送至终端节点的监听端口。 **说明** 您只有在配置HTTP或HTTPS协议监听的终端节点组时，才允许配置**端口映射**参数。
健康检查	开启或关闭健康检查。 开启后，可以通过健康检查来判断终端节点的运行状态。关于健康检查更多信息，请参见开启和管理健康检查。 **说明** 对于UDP监听，终端节点必须有TCP、HTTP或HTTPS服务才支持健康检查，否则，它将被标记为异常。
健康检查协议	选择健康检查的协议，支持TCP、HTTP和HTTPS协议。 ○ TCP协议的健康检查是基于网络层探测，通过发送SYN握手报文来检测服务器端口是否存活。 ○ HTTP和HTTPS协议的健康检查是基于GET请求，通过发送GET请求模拟浏览器的访问行为来检查服务器应用是否健康。
端口	健康检查服务访问终端节点时的探测端口。 取值范围：1~65535。
健康检查间隔时间	健康检查的时间间隔，单位为秒。 取值范围：1~50秒，默认为2秒。

配置	说明
路径	指定健康检查的路径。 必须以正斜线（/）开头，长度限制为1~80个字符，支持使用字母、数字和短划线（-）、正斜线（/）、英文句点（.）、百分号（%）、问号（?）、井号（#）和and（&）以及扩展字符集 `_;~!()*[]@$^:',+` 。 默认为全球加速系统向后端服务器应用配置的缺省首页发起GET请求。如果您用来进行健康检查的页面并不是应用服务器的缺省首页，需要指定具体的检查路径。 **说明** 仅HTTP和HTTPS协议健康检查显示该项。
健康检查健康阈值	针对健康检查状态变化所需要的连续健康检查次数，即从成功到失败的连续健康检查失败次数或从失败到成功的连续健康检查成功次数。 取值范围：2~10，默认为3次。

6. （可选）单击**+添加终端节点组**，根据上述说明，配置多个终端节点组。

   说明
   - 仅TCP和UDP监听支持添加终端节点组。
   - TCP和UDP监听默认支持创建2个默认终端节点组，如果您需要创建更多默认终端节点组，可在配额管理提升gaplus_quota_epgs_per_listener的配额。具体操作，请参见配额管理。

7. 单击**下一步**。
8. 在**配置审核**配置向导页面，确认信息，然后单击**提交**。

   如果需要修改配置，您可以单击相应区域中的**修改**重新进行配置。

添加虚拟终端节点组

在您添加虚拟终端节点组前，请注意以下说明：

- 只有HTTP或HTTPS协议的监听才支持添加虚拟终端节点组。
- 在您添加虚拟终端节点组前，您需要先添加默认终端节点组。

1.
2. 在**实例列表**页面，找到目标全球加速实例，在**操作**列单击**配置监听**。
3. 在**监听**页签下，找到目标监听，在**默认终端节点组ID/名称**列单击终端节点组ID或数字。
4. 在**终端节点组**页签下的**虚拟终端节点组**区域，单击**添加虚拟终端节点组**。
5. 在**添加虚拟终端节点组**对话框中，配置虚拟终端节点组，然后单击**创建**。

   关于参数的配置信息，请参见添加默认终端节点组。

更多操作

操作	说明

操作	说明
修改终端节点组	1. 在**监听**页签下，找到目标监听，然后在**默认终端节点组ID/名称**列单击终端节点组ID或数字。 2. 在**终端节点组**页签下，找到目标默认终端节点组或虚拟终端节点组，在**操作**列单击**编辑**。 3. 在**编辑默认终端节点组**或**编辑虚拟终端节点组**对话框，修改终端节点组的名称、终端节点等信息，然后单击**保存**。 默认终端节点组的配置详情，请参见添加默认终端节点组。 **说明** 目前仅HTTP或HTTPS协议的监听支持配置和修改虚拟终端节点组。关于虚拟终端节点组的更多信息，请参见终端节点组与终端节点概述。
设置终端节点组流量调配	设置到不同终端节点组的流量比例。 1. 在**监听**页签下，找到目标监听，然后在单击**编辑节点组**。 2. 在**配置终端节点**配置向导页面，找到目标终端节点组，设置流量调配值，然后单击**下一步**。流量调配取值范围：0~100。单位：%。 3. 确认终端节点组的信息后，单击**提交**。 **说明** 仅TCP或UDP协议的监听支持设置终端节点组的流量调配。
设置终端节点权重	终端节点权重确定了全球加速将访问请求定向到终端节点组内各终端节点的流量比例。 全球加速会计算终端节点组中各个终端节点的权重之和，然后根据每个终端节点的权重与总权重之比将流量定向到终端节点。例如，如果您要将三分之一的流量分发到终端节点EP1上，将流量的三分之二分发到终端节点EP2上，则可以配置EP1和EP2的权重分别为1和2。如果您希望全球加速停止向某个终端节点分发流量，则可以将该终端节点的权重配置为0。 1. 在**监听**页签下，找到目标监听，然后在**默认终端节点组ID/名称**列单击终端节点组ID或数字。 2. 在**终端节点组**页签下，找到待设置权重的终端节点所在的终端节点组，在**操作**列单击**编辑**。 3. 在**编辑虚拟终端节点组**或**编辑虚拟终端节点组**对话框的**终端节点**区域，找目标终端节点，设置权重值，然后单击**保存**。 权重取值范围：0~255。
删除终端节点组	您可以删除不需要的终端节点组，删除后，全球加速将不再向该终端节点组转发流量。 1. 在**监听**页签下，找到目标监听，然后在**默认终端节点组ID/名称**列单击终端节点组ID或数字。 2. 在**终端节点组**页签下，找到待删除的默认终端节点组或虚拟终端节点组，在**操作**列单击**删除**。 3. 在弹出的对话框中单击**确定**。 **说明** 如果删除的终端节点组为监听下唯一的终端节点组，则该监听将不可用。

操作	说明
删除终端节点	您可以删除不需要的终端节点，删除后，全球加速将不再向该终端节点转发流量 。终端节点组下只有一个终端节点时，该终端节点无法删除。 1. 在**监听**页签下，找到目标监听，然后在**默认终端节点组ID/名称**列单击终端节点组ID或数字。 2. 在**终端节点组**页签下，找到待删除终端节点的默认终端节点组或虚拟终端节点组，在**操作**列单击**编辑**。 3. 在**编辑默认终端节点组**或**编辑默认终端节点组**对话框的**终端节点**区域，找到待删除的终端节点，在**操作**列单击**删除**，然后单击**保存**。

相关文档

- CreateEndpointGroup：创建终端节点组。
- CreateEndpointGroups：创建多个终端节点组。
- UpdateEndpointGroup：修改终端节点组配置信息。
- DeleteEndpointGroup：删除终端节点组。

5.4. 添加和管理转发策略

HTTP或HTTPS协议的监听支持配置基于域名或基于路径的转发策略。HTTP或HTTPS协议的监听接收到访问请求后会根据转发策略将不同域名或不同路径的访问请求转发至后端对应的终端节点组中。本文为您介绍转发策略功能原理以及如何添加、管理转发策略。

转发策略介绍

转发策略类型

转发策略分为默认转发策略和自定义转发策略：

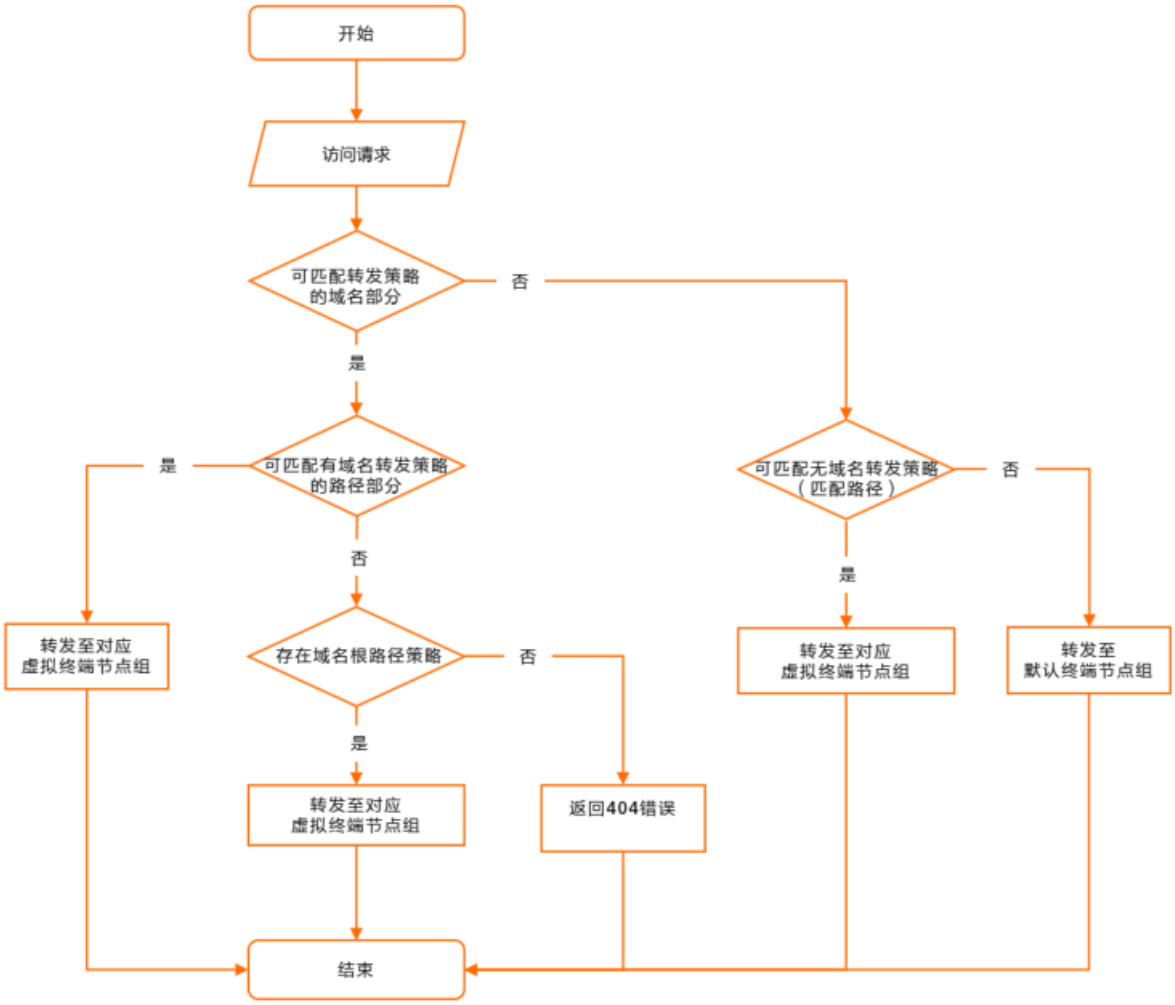
- 默认转发策略：在您创建HTTP或HTTPS监听后，系统自动创建一条默认转发策略并关联到默认终端节点组。一个监听中只有一条默认转发策略，且默认转发策略不支持更改和删除。
- 自定义转发策略：在您创建HTTP或HTTPS监听后，您可以根据实际需求手动创建自定义转发策略。一个监听中可以创建多个自定义转发策略。

转发策略组成

每条转发策略均包含转发条件和转发动作两个部分：

- 转发条件：访问请求只有匹配转发条件后，才会被转发至对应的终端节点组。
  您可以通过以下三种方式配置自定义转发策略的转发条件：
  - 只配置域名：一个转发策略只支持配置一个域名作为转发条件，访问请求匹配到域名后才可被转发至对应的虚拟终端节点组。
  - 只配置路径：一个转发策略可以配置多个路径作为转发条件，访问请求只要匹配到其中一个路径即可被转发至对应的虚拟终端节点组。
  - 同时配置域名和路径：一个转发策略可以同时配置一个域名和多个路径作为转发条件，访问请求只要匹配到域名和其中的一个路径即可被转发至对应的虚拟终端节点组。
- 转发动作：转发动作指向终端节点组。一个转发策略只允许指向一个终端节点组。

转发策略匹配规则



访问请求将通过以下顺序匹配转发策略：

1. 访问请求中存在域名，则先根据域名匹配转发策略。
   若存在匹配该域名的转发策略，则继续匹配路径部分。若路径部分也能匹配，则将访问请求转发到对应的虚拟终端节点组；若路径部分未能匹配该域名下的任何路径转发条件，则将访问请求转发给该域名的根路径转发策略（即只配置了该域名作为转发条件，没有配置路径的转发策略），若当前监听没有配置该域名的根路径转发策略时，则向客户端返回404错误。
2. 访问请求中不存在域名或者监听中不存在匹配该域名的转发策略，则直接匹配无域名转发策略（即只配置了路径作为转发条件，没有配置域名的转发策略）。
3. 访问请求未能匹配到转发策略时，将直接通过默认转发策略被转发到默认终端节点组。

前提条件

- 您已经添加了HTTP或HTTPS协议的监听。具体操作，请参见添加HTTP或HTTPS协议监听。
- 您已经添加了虚拟终端节点组。具体操作，请参见添加虚拟终端节点组。

添加转发策略

您可以通过以下步骤添加自定义转发策略，将匹配策略的请求转发至对应的虚拟终端节点组。

1.
2. 在**实例列表**页面，找到目标全球加速实例，在**操作**列单击**配置监听**。
3. 在**监听**页签下，找到目标监听，然后单击监听ID。

4. 在监听详情页面下，单击**转发策略**页签。
5. 在**转发策略**页签下，单击**插入新策略**，根据以下信息配置转发策略，然后单击**确定**。

参数	说明
策略名称	自定义转发策略的名称。 长度为2~128个英文或中文字符，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（-）。不填则自动生成。
如果（条件全部匹配）	配置转发条件。 ○ **域名** 域名长度为3~128个字符，允许包含字母、数字、短划线（-）和半角句号（.），支持使用星号（*）和半角问号（?）作为通配符。 示例：`*.example.com` ○ **路径** 路径长度为1~128个字符，必须以正斜线（/）开头，只允许包含字母、数字、美元符号（$）、短划线（-）、下划线（_）、半角句号（.）、加号（+）、正斜线（/）、and（&）、波浪线（~）、at（@）、半角冒号（:）、半角单引号（'），支持使用星号（*）和半角问号（?）作为通配符。 示例：URL为`www.example.com/test/test1?x=1&y=2`时可配置为`/test/*`。
那么转发至虚拟终端节点组	选择目标虚拟终端节点组。

6. 如果您需要添加多个转发策略，可继续单击**插入新策略**进行添加。

编辑转发策略

1.
2. 在**实例列表**页面，找到目标全球加速实例，在**操作**列单击**配置监听**。
3. 在**监听**页签下，找到目标监听，然后单击监听ID。
4. 在监听详情页面下，单击**转发策略**页签。
5. 在**转发策略**页签下，找到目标转发策略，单击右上角的图标，编辑转发策略，然后单击**保存**。

> **说明** 不支持编辑默认转发策略。

删除转发策略

1.
2. 在**实例列表**页面，找到目标全球加速实例，在**操作**列单击**配置监听**。
3. 在**监听**页签下，找到目标监听，然后单击监听ID。
4. 在监听详情页面下，单击**转发策略**页签。
5. 在**转发策略**页签下，找到目标转发策略，单击右上角的图标。
6. 在弹出的对话框中，确认转发策略ID信息，然后单击**确定删除**。

相关文档

- CreateForwardingRules：创建转发策略。
- UpdateForwardingRules：更新转发策略。
- ListForwardingRules：查看已经创建的转发策略信息。
- DeleteForwardingRules：删除转发策略。

5.5. 开启和管理健康检查

全球加速通过健康检查来判断终端节点的运行状态，健康检查机制提高了业务的可靠性和可用性，避免了异常终端节点对服务的影响。

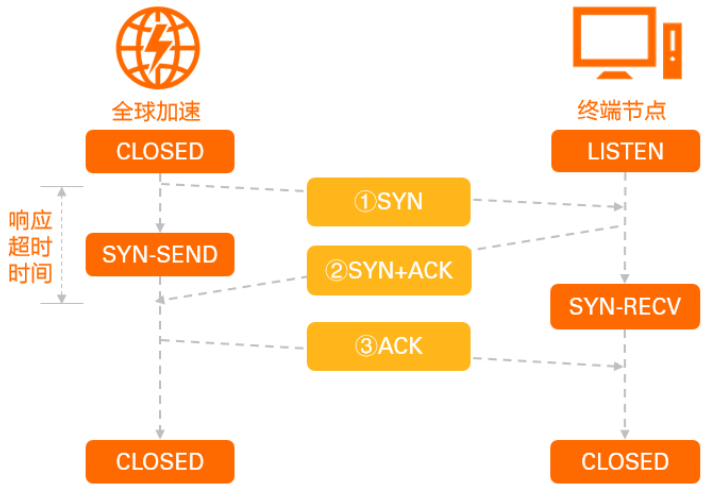
健康检查介绍

您可以为全球加速实例的终端节点组开启健康检查。开启健康检查后，当某个终端节点健康检查出现异常时，全球加速会自动将新的请求分发到其它健康检查正常的终端节点上；而当健康检查异常的终端节点恢复正常后，全球加速会将该终端节点自动恢复到请求服务中。

全球加速支持TCP、HTTP和HTTPS协议的健康检查。

TCP协议健康检查

TCP协议的健康检查是基于网络层探测，通过发送SYN握手报文来检测服务器端口是否存活。检查流程如下图：



序号	描述
①	全球加速实例根据监听的健康检查配置，向终端节点的IP和健康检查端口发送TCP SYN数据包。
②	根据终端节点是否返回SYN+ACK数据包，判定健康检查是否成功。 • 如果在响应超时时间（3秒）之内，全球加速实例成功收到终端节点返回的SYN+ACK数据包，则认为终端节点正常运行，判定健康检查成功。 • 如果在响应超时时间（3秒）之内，全球加速实例收到终端节点返回的RST数据包，则认为终端节点未响应健康检查端口，判定健康检查失败。 • 如果已超出响应超时时间（3秒），全球加速实例还未收到终端节点返回的SYN+ACK数据包，则认为网络无法到达终端节点，终端节点无法响应，判定健康检查失败。 **说明** 响应超时时间为接收来自运行状况检查的响应需要等待的最大时间。如果终端节点在响应超时时间内没有正确响应，则判定为健康检查失败。系统默认为3秒，不支持配置。

序号	描述
③	全球加速实例成功收到终端节点返回的SYN+ACK数据包后，向终端节点发送ACK数据包，确认连接。

HTTP和HTTPS协议的健康检查

HTTP和HTTPS协议的健康检查是基于GET请求，通过发送GET请求模拟浏览器的访问行为来检查终端节点的服务器应用是否健康。检查流程如下图：

序号	描述
①	全球加速实例根据监听的健康检查配置，向终端节点的IP、健康检查端口、检查路径发送HTTP GET请求。
②	终端节点收到请求后，根据相应服务的运行情况，确定是否返回HTTP状态码。 • 如果在响应超时时间（3秒）之内，全球加速实例成功收到终端节点返回的状态码 `200` ，则认为终端节点正常运行，判定健康检查成功。 • 如果在响应超时时间（3秒）之内，全球加速实例收到终端节点返回状态码不为 `200` ，则认为终端节点异常，判定健康检查失败。 • 如果已超出响应超时时间（3秒），全球加速实例还未收到终端节点返回状态码，则认为网络无法到达终端节点，终端节点无法响应，判定健康检查失败。 **说明** 响应超时时间为接收来自运行状况检查的响应需要等待的最大时间。如果终端节点在响应超时时间内没有正确响应，则判定为健康检查失败。系统默认为3秒，不支持配置。

健康检查时间窗

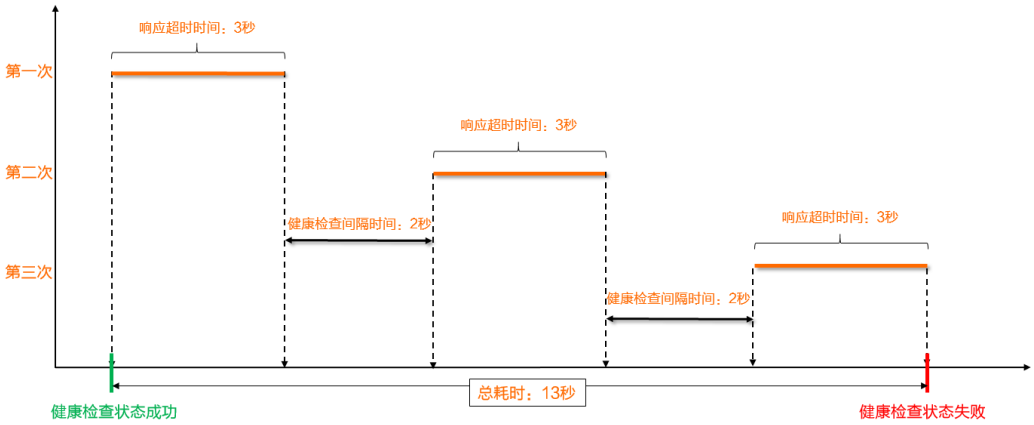
健康检查机制的引入，有效提高了业务服务的可用性。但是，为了避免频繁的健康检查失败引起的切换对系统可用性的冲击，健康检查只有在健康检查时间窗内连续多次检查成功或失败后，才会进行状态切换。健康检查时间窗由以下三个因素决定：

- 健康检查间隔时间：每隔多久进行一次健康检查。
- 响应超时时间：等待后端服务返回健康检查的最大时间。
- 健康检查健康阈值：针对健康检查状态变化所需要的连续健康检查次数。

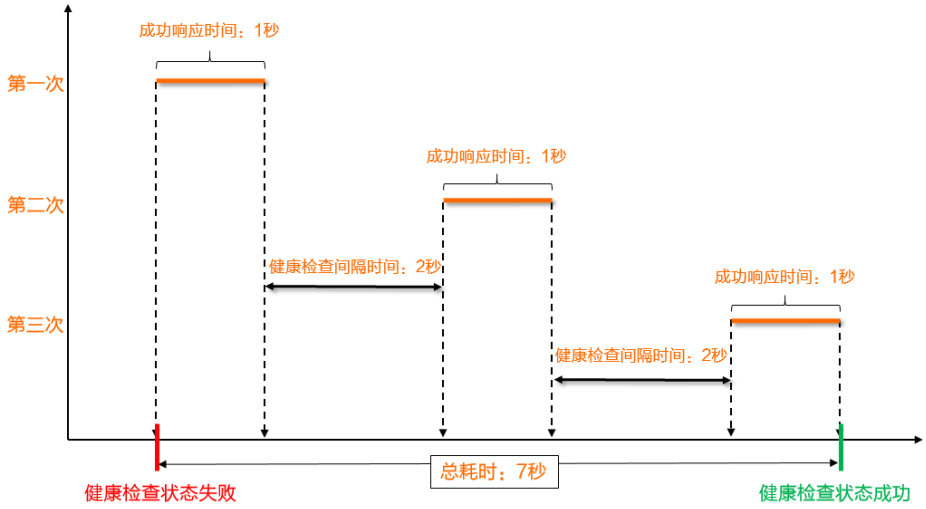
健康检查时间窗的计算方法如下：

- 健康检查失败时间窗=响应超时时间×健康检查健康阈值+健康检查间隔时间×(健康检查健康阈值-1)

以下图为例，健康检查响应超时时间为3秒，健康检查间隔时间为2秒，健康检查健康阈值为3次，健康检查失败时间窗=3×3+2×(3-1)=13秒。



- 健康检查成功时间窗=(健康检查成功响应时间x健康检查健康阈值)+健康检查间隔时间x(健康检查健康阈值-1)
  以下图为例，健康检查成功响应时间为1秒，健康检查间隔时间为2秒，健康检查健康阈值为3次，健康检查成功时间窗=1×3+2×(3-1)=7秒。



使用限制

对于UDP监听，终端节点必须有TCP、HTTP或HTTPS服务才支持健康检查，否则，它将被标记为异常。

开启健康检查

1.
2. 在**实例列表**页面，找到目标全球加速实例，在**操作**列单击**配置监听**。
3. 在**监听**页签下，找到目标监听，在**操作**列单击**编辑监听**。
4. 在**编辑监听**页面，单击**下一步**。
5. 在**配置终端节点**配置向导页面的**健康检查**区域，打开**健康检查**的开关，然后根据以下信息配置健康检查。

配置	说明

配置	说明
健康检查协议	选择健康检查的协议，支持TCP、HTTP和HTTPS协议。 ○ TCP协议的健康检查是基于网络层探测，通过发送SYN握手报文来检测服务器端口是否存活。 ○ HTTP和HTTPS协议的健康检查是基于GET请求，通过发送GET请求模拟浏览器的访问行为来检查终端节点的服务器应用是否健康。
端口	健康检查服务访问终端节点时的探测端口。 取值范围：1~65535。
健康检查间隔时间	健康检查的时间间隔，单位为秒。 取值范围：1~50秒，默认为2秒。
路径	指定健康检查的路径。 必须以正斜线（/）开头，长度限制为1~80个字符，支持使用字母、数字和短划线（-）、正斜线（/）、英文句点（.）、百分号（%）、问号（?）、井号（#）和and（&）以及扩展字符集 `_;~!()*[]@$^:',+` 。 默认为全球加速系统向后端服务器应用配置的缺省首页发起GET请求。如果您用来进行健康检查的页面并不是应用服务器的缺省首页，需要指定具体的检查路径。 **说明** 仅HTTP和HTTPS协议健康检查显示该项。
健康检查健康阈值	针对健康检查状态变化所需要的连续健康检查次数，即从成功到失败的连续健康检查失败次数或从失败到成功的连续健康检查成功次数。 取值范围：2~10，默认为3次。

6. 单击**下一步**，在**配置审核**配置向导页面确认健康检查信息，然后单击**提交**。

更多操作

操作	说明
修改健康检查配置	1. 在**监听**页签下，找到目标监听，在**操作**列单击**编辑节点组**。 2. 在**配置终端节点**配置向导页面的**健康检查**区域，您可以修改健康检查协议、端口、健康检查间隔时间等各配置项信息，然后单击**下一步**。 关于配置项信息，请参见开启健康检查。 3. 在**配置审核**配置向导页面，单击**下一步**。
关闭健康检查	1. 在**监听**页签下，找到目标监听，在**操作**列单击**编辑节点组**。 2. 在**配置终端节点**配置向导页面的**健康检查**区域，关闭**健康检查**的开关，然后单击**下一步**。 3. 在**配置审核**配置向导页面，单击**下一步**。

相关文档

- CreateEndpointGroup：创建终端节点组（可配置健康检查）。
- UpdateEndpointGroup：修改终端节点组配置信息（可配置健康检查）。

- GetHealthStatus：查看终端节点的健康检查信息。

5.6. 多终端节点组流量调配使用示例

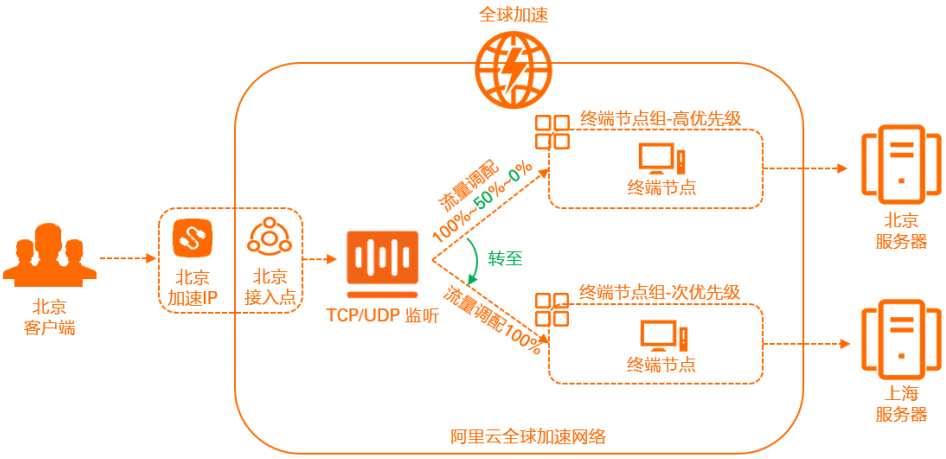
跨地域服务流量调度

本文为您介绍如何通过流量调配功能控制不同地域终端节点组的访问比例。

场景示例

假设某公司业务部署在北京和上海，服务协议与端口为TCP 80，客户端主要集中在北京地域。该公司已通过全球加速添加了北京加速地域、北京地域终端节点组和上海地域终端节点组。全球加速默认将北京客户端的访问流量全部就近转发至北京终端节点组的服务器进行处理，上海终端节点组作为北京地域异常时的备用终端节点组。因公司业务调整，要求北京客户端的访问流量先暂时切换至上海地域终端节点组的服务器进行处理，切换过程客户端不感知。

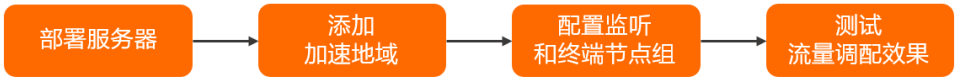
您可以调整北京终端节点组的流量调配值，例如将默认的100%先调整至50%，此时北京客户端50%的访问流量会被调度到上海终端节点组的服务器处理。测试访问流量转发不受影响后，进一步调整为0%，北京客户端的访问流量会被全部调度到上海终端节点组的服务器处理，从而实现北京客户端访问流量的平滑切换。



前提条件

请确保您已购买全球加速实例和基础带宽包。更多信息，请参见购买与选型。

配置步骤



步骤一：部署服务器

本文以Alibaba Cloud Linux 3.2104 64位操作系统为例。不同类型的操作系统测试命令会有差异，具体测试命令请参见您操作系统的操作指南。

1. 分别在北京和上海地域部署服务器，并开启TCP 80协议端口。
2. 登录北京客户端，打开命令行窗口，通过curl命令分别访问北京和上海地域的服务器。

   ```
   curl <源站IP>
   ```

   如下图所示，分别可返回各自的地域信息。

   访问北京服务器

访问上海服务器

步骤二：添加加速地域

1.
2. 在**实例列表**页面，找到已创建的全球加速实例，单击实例ID。
3. 单击**加速区域**页签，然后在**华北**页签下单击**添加接入地域**。
4. 在**添加加速区域**对话框，根据以下信息进行配置，然后单击**确定**。

配置	说明
地域	选择访问加速服务用户的所属地域。 本文选择**北京**。
带宽	输入加速服务的地域带宽。 本文输入*2* Mbps。
IP地址协议	选择用户接入全球加速服务的IP地址协议。 本文选择**IPv4**。

添加成功后，全球加速会在接入地域分配一个加速IP，用来加速用户访问。

步骤三：添加监听和终端节点组

1. 在实例详情页面，单击**监听**页签，然后单击**添加监听**。
2. 在**配置监听和协议**配置向导页面，根据以下信息配置监听，然后单击**下一步**。

配置	说明
监听名称	输入监听的名称。 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（_）和短划线（-）。
协议	选择监听的协议类型。 本文选择**TCP**。
端口	指定用来接收请求并向终端节点进行转发的监听端口，端口取值范围：**1~65499**。 本文输入*80*。
客户端亲和性	选择是否保持客户端亲和性。保持客户端亲和性，即客户端访问有状态的应用程序时，可以将来自同一客户端的所有请求都定向到同一终端节点。 本文选择**关闭**。

3. 在**配置终端节点**配置向导页面，根据以下信息配置北京终端节点组。

配置	说明
节点组名称	输入终端节点组的名称。
地域	选择终端节点组所属的地域，即请求要访问的目标服务器的所属地域。 本文选择**北京**。
流量调配	配置到不同终端节点组的流量比例。单位：%。取值范围：0~100。 本文保持默认值**100**。 **说明** 您只有在配置TCP或UDP协议监听的终端节点组时，才支持配置**流量调配**。
后端服务部署在	选择后端服务部署位置。 本文选择**非阿里云**。
保持客户端源IP	选择开启或关闭保持客户端源IP。开启后，后端服务器可以通过该功能获取客户端源IP。 本文选择关闭保持客户端源IP。

配置	说明
终端节点	终端节点是客户端请求访问的目标主机。您可以根据以下信息配置终端节点： ○ **后端服务类型**：选择**自定义IP**。 ○ **后端服务**：输入后端服务的公网IP地址。 ○ **权重**：输入终端节点的权重，权重取值范围：0~255。全球加速根据您配置的权重按比例将流量路由到终端节点。 **注意** 如果某个终端节点的权重配置为0，全球加速将终止向该终端节点分发流量，请您谨慎操作。
健康检查	开启或关闭健康检查。 开启后，可以通过健康检查来判断终端节点的运行状态。关于健康检查相关配置项更多信息，请参见开启和管理健康检查。 本文开启健康检查。

4. 单击**+添加终端节点组**，根据步骤的配置项说明，配置上海终端节点组，然后单击**下一步**。

5. 在**配置审核**配置向导页面，确认监听和终端节点配置信息后，单击**提交**。

步骤四：测试流量调配效果

本文使用以下命令模拟客户端发送访问请求，测试流量调配效果。

```
echo > curl.txt; for ((i=0;i<<请求数>;i++)); do curl -s <加速IP> >> curl.txt; done; beijing_count=`grep Beijing curl.txt | wc -l`;echo "Beijing count: ${beijing_count}";shanghai_count=`grep Shanghai curl.txt | wc -l`;echo "shanghai count: ${shanghai_count}";
```

其中：

- `请求数`：模拟的访问请求量，例如`请求数`为100时，表示模拟有100个访问请求。
- `加速IP`：全球加速分配的加速IP。
- `Beijing count`：北京地域服务器处理的访问请求量。
- `Shanghai count`：上海地域服务器处理的访问请求量。

1. 测试高优先级的北京终端节点组流量调配为100%时的访问请求调度情况。

   登录北京客户端，打开命令行窗口，在北京客户端发送100个请求，查看北京和上海地域服务器处理的访问请求量。

   ```
   [root@iZ2ze ~]# echo > curl.txt; for ((i=0;i<100;i++)); do curl -s 123. >> curl.txt; done; b
   eijing_count=`grep Beijing curl.txt | wc -l`;echo "Beijing count: ${beijing_count}";shanghai_count=`grep shanghai curl.t
   xt | wc -l`;echo "shanghai count: ${shanghai_count}";
   Beijing count: 100
   shanghai count: 0
   [root@iZ2ze ~]#
   ```

   经验证，北京客户端的访问请求全部转发至北京地域的终端节点组处理。

2. 测试高优先级的北京终端节点组流量调配为50%时的访问请求调度情况。

   i. 修改北京地域终端节点组的流量调配为50%。具体操作，请参见设置终端节点组流量调配。

   ii. 在北京客户端发送100个请求，查看北京和上海地域服务器处理的访问请求量。

   ```
   [root@iZ ~]# echo > curl.txt; for ((i=0;i<100;i++)); do curl -s 123. >> curl.txt; done; b
   eijing_count=`grep Beijing curl.txt | wc -l`;echo "Beijing count: ${beijing_count}";shanghai_count=`grep Shanghai curl.t
   xt | wc -l`;echo "shanghai count: ${shanghai_count}";
   Beijing count: 50
   shanghai count: 50
   [root@iZ ~]#
   ```

   经验证，北京和上海地域终端节点组各处理了北京客户端总请求量的50%，即北京终端节点组处理50个，上海终端节点组处理50个。

3. 测试高优先级的北京终端节点组流量调配值为0%时的访问请求调度情况。

   i. 修改北京地域终端节点组的流量调配为0%。具体操作，请参见设置终端节点组流量调配。

   ii. 在北京客户端发送100个请求，查看北京和上海地域服务器处理的访问请求量。

   ```
   [root@iZ2ze ~]# echo > curl.txt; for ((i=0;i<100;i++)); do curl -s 123. >> curl.txt; done; b
   eijing_count=`grep Beijing curl.txt | wc -l`;echo "Beijing count: ${beijing_count}";shanghai_count=`grep Shanghai curl.t
   xt | wc -l`;echo "shanghai count: ${shanghai_count}";
   Beijing count: 0
   shanghai count: 100
   [root@iZ2 ~]#
   ```

   经验证，北京客户端的访问请求全部转发至上海地域的终端节点组处理。

6.配置CNAME

如果您是通过域名方式加速访问服务，则您需要配置源站的智能DNS，将加速域名指向CNAME地址。本文以阿里云云解析DNS（Alibaba Cloud DNS）服务为例，为您介绍如何配置CNAME。

步骤一：获取加速域名的CNAME地址

1.
2. 在**实例列表**页面，找到目标全球加速实例，单击实例ID。
3. 单击**实例信息**页签。
4. 在**基本信息**区域，找到**CNAME**，然后单击CNAME值右侧的**复制**。

步骤二：添加CNAME记录

1. 登录域名解析控制台。
2. 如果您是非阿里云注册的域名且需要在阿里云云解析DNS控制台进行CNAME配置，添加域名到云解析控制台。

> **说明** 如果您的域名是在阿里云注册的，请跳过该步骤。如果您的域名是非阿里云注册，您可以通过以下两种方式进行域名解析设置：
>
> - 使用阿里云DNS解析服务时，需要先在阿里云云解析DNS控制台完成域名添加。具体操作，请参见添加域名。
> - 使用非阿里云DNS解析服务时，请登录您的DNS服务商系统修改网站域名的解析记录。

3. 在**域名解析**页面，找到目标域名，在**操作**列单击**解析设置**。
4. 在**解析设置**页面，单击**添加记录**。
5. 在**添加记录**面板，根据以下信息配置CNAME记录，然后单击**确认**。

配置	说明
记录类型	选择**CNAME**。

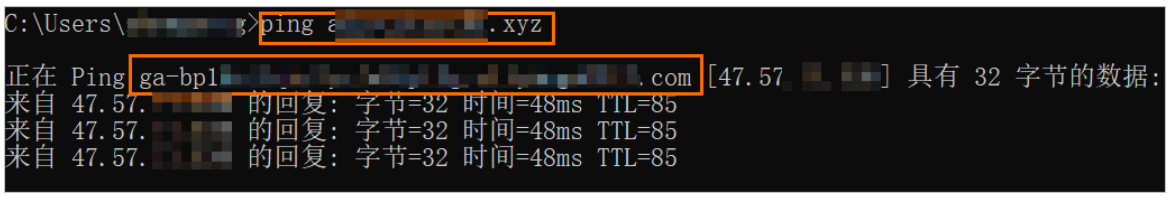
配置	说明
主机记录	加速域名的前缀。 ○ 如果您的加速域名为 `www.aliyun.com` ，主机记录为 `www` 。 ○ 如果您的加速域名为 `aliyun.com` ，主机记录为 `@` 。 ○ 如果您的加速域名为 `*.aliyun.com` ，主机记录为 `*` 。 ○ 如果您的加速域名为 `mail.aliyun.com` ，主机记录为 `mail` 。
解析线路	选择**默认**。
记录值	粘贴在步骤一：获取加速域名的CNAME地址中复制的CNAME值。
TTL	选择**10分钟**。

> **说明**
>
> ○ 新增CNAME记录会实时生效，修改CNAME记录72小时之内生效。
>
> ○ 如果您遇到添加冲突问题，可以换一个加速域名或者调整冲突的记录，请参见解析记录冲突。
>
> ○ 配置完CNAME后，由于状态更新约有10分钟延迟，控制台的域名列表页可能仍提示“未配置CNAME”，请您耐心等待。

步骤三：验证CNAME配置

本文以Windows系统为例，验证CNAME配置是否生效。

1. 打开Windows的命令行窗口。
2. 执行**ping**命令，**ping**加速域名。
   如果返回的解析结果与全球加速的CNAME值一致，则表示CNAME配置已经生效。



7.访问控制

全球加速提供监听级别的访问控制。您可以针对不同的监听实例配置不同的访问控制方式和访问控制策略组。

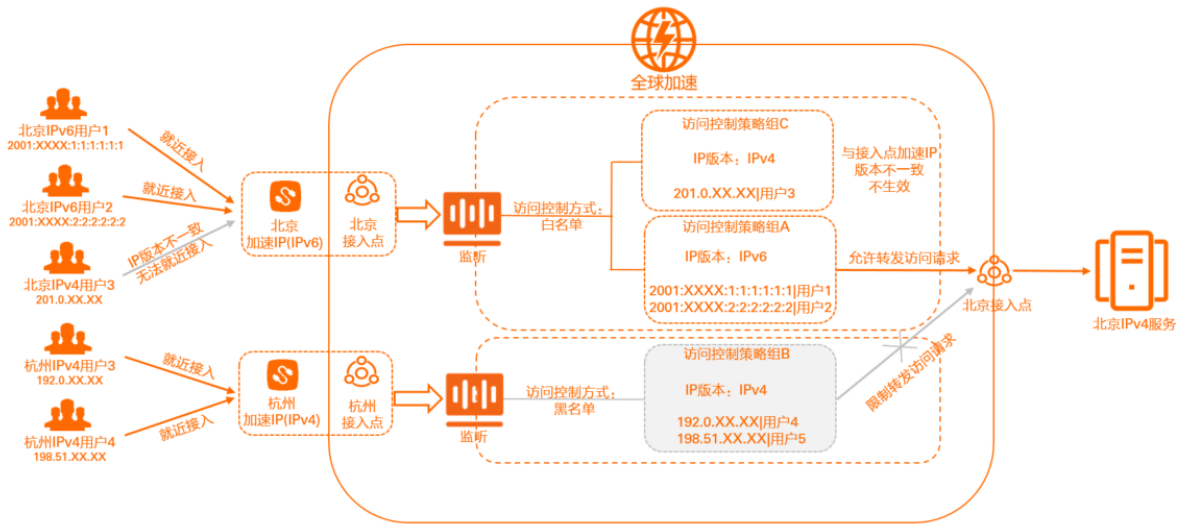
访问控制介绍

访问控制功能由访问控制方式和访问控制策略组组成，访问控制方式包括白名单和黑名单，访问控制策略组可以添加多个IP地址条目或IP地址段条目。您可以针对不同的监听设置访问白名单或黑名单：

- 白名单：仅转发来自所选访问控制策略组中设置的IP地址或地址段的所有请求，白名单适用于只允许特定IP访问的场景。
- 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，黑名单适用于应用只限制某些特定IP访问的场景。

> 注意
>
> - 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地址可以访问全球加速监听。如果开启了白名单访问，但访问策略组中没有添加任何IP，则全球加速监听会屏蔽所有转发请求。
> - 如果开启了黑名单访问，但访问策略组中没有添加任何IP，则全球加速监听会转发全部请求。

创建访问控制策略组时，支持选择IPv4版本和IPv6版本。您可以根据接入点加速IP版本，为监听开启对应IP版本的访问控制策略组。



使用限制

- 一个监听挂载的访问控制策略组包含的访问控制条目IP总数上限为200，且控制条目IP不能重复。
- 一个访问控制策略组能够关联的监听总数为10。
- 一个监听最多只支持添加2个访问控制策略组，且必须分别为IPv4和IPv6版本的访问控制策略组，不能同时为IPv4访问控制策略组或IPv6访问控制策略组。
- 当监听同时添加了一个IPv4和一个IPv6版本的访问控制策略组时，仅可生效与加速IP版本一致的访问控制策略组。

配置流程

访问控制配置流程如下图所示：

访问控制配置流程说明如下：

1. 创建访问控制策略组：在开启访问控制前，需要先创建访问控制策略组。
2. 添加策略组条目：每个策略组可以添加多个IP地址条目或IP地址段条目。
3. 为监听开启访问控制：为监听开启访问控制，选择访问控制方式，并绑定访问控制策略组。

创建访问控制策略组

在开启访问控制前，您需要先配置访问控制策略组。

1.
2. 在左侧导航栏，单击**访问控制**。
3. 在**访问控制**页面，单击**创建访问控制策略组**，输入**策略组名称**并选择**IP版本**。

   您可以根据需求选择访问控制策略组的IP版本，包括**IPv4**和**IPv6**。
   - 选择**IPv4**时，该访问控制策略组仅针对加速IP为IPv4地址协议的加速地域生效。
   - 选择**IPv6**时，该访问控制策略组仅针对加速IP为IPv6地址协议的加速地域生效。
4. 单击**确定**。

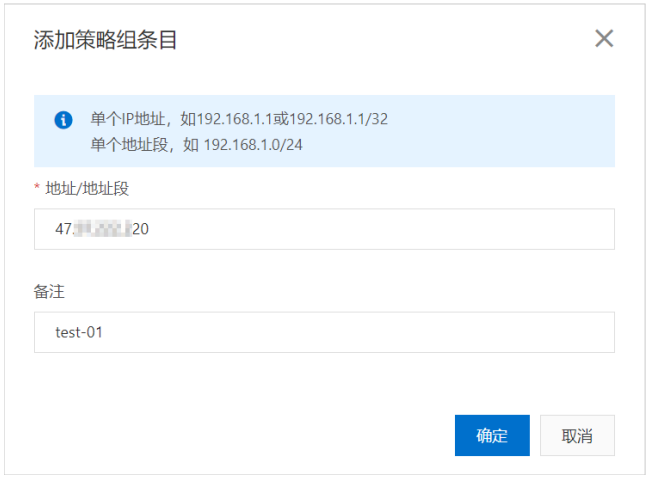
添加策略组条目

创建完访问控制策略组后，每个策略组可添加多个IP地址条目或IP地址段条目，从而实现允许或者限制全球加速监听对这些IP条目访问请求的转发。

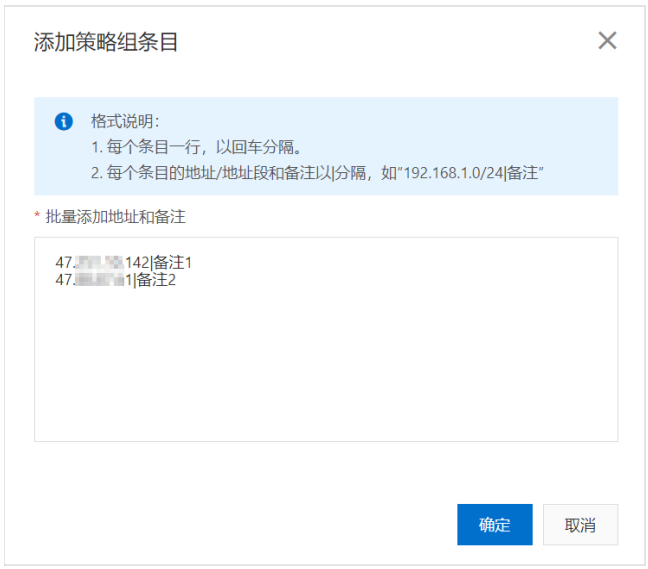
1.
2. 在左侧导航栏，单击**访问控制**。
3. 找到目标访问控制策略组，在**操作**列单击**管理访问控制策略组**。
4. 添加策略组条目。
   - 单个添加策略组条目

     单击**添加条目**，在**添加策略组条目**对话框，输入要添加的IP地址或IP地址段条目和备注，单击**确定**。

     备注长度为2~256个字符，支持中文、字母、数字、短划线（-）、正斜线（/）、半角句号（.）、下划线（_）、半角逗号（,）、半角分号（;）和at（@）。



- 批量添加策略组条目
  单击**批量添加条目**，在**批量添加策略组条目**对话框，批量添加IP地址或IP地址段，单击**确定**。
  在添加条目时注意：
  - 每个条目一行，以回车分隔。
  - 每个条目中IP地址或IP地址段与备注之间用竖线（|）分隔，例如：47.57.XX.XX|备注。
  - 备注长度为2~256个字符，支持中文、字母、数字、短划线（-）、正斜线（/）、半角句号（.）、下划线（_）、半角逗号（,）、半角分号（;）和at（@）。



为监听开启访问控制

全球加速提供监听级别的访问控制。您可以针对不同的监听设置访问白名单或黑名单。

在开启访问控制前，请确保您已创建监听。更多信息，请参见添加和管理监听。

1.
2. 在**实例列表**页面，找到目标全球加速实例，然后在**操作**列单击**配置监听**。
3. 在**监听**页签下，单击待开启访问控制的监听ID。
4. 在**监听详情**页签下，打开**访问控制**开关。
5. 在**开启访问控制**对话框配置以下参数，然后单击**确定开启**。

配置	说明

配置	说明
访问控制方式	选择一种访问控制方式： ○ **白名单**：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。 ○ **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。 **注意** ○ 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地址可以访问全球加速监听。如果开启了白名单访问，但访问策略组中没有添加任何IP，则全球加速监听会屏蔽所有转发请求。 ○ 如果开启了黑名单访问，但访问策略组中没有添加任何IP，则全球加速监听会转发全部请求。
选择访问控制策略组	选择一个访问控制策略组。

删除策略组条目

您可以删除访问控制策略组中的IP地址条目。

1.
2. 在左侧导航栏，单击**访问控制**。
3. 找到目标访问控制策略组，在**操作**列单击**管理访问控制策略组**。
4. 在目标IP条目的**操作**列下单击**删除**，或选中多个IP条目，然后在条目列表下方单击**删除**。
5. 在弹出的对话框中，单击**确定**。

关闭访问控制

如果不需要对监听设置访问限制，您可以对监听关闭访问控制。

1.
2. 在**实例列表**页面，找到目标全球加速实例，然后在**操作**列单击**配置监听**。
3. 在**监听**页签下，单击待关闭访问控制的监听ID。
4. 在**监听详情**页签下，关闭**访问控制**开关。

8.日志管理

背景信息

1.

8.1. 查看操作日志

全球加速实例的所有操作都会保存到操作日志中，您可以在操作日志中查看和搜索包括事件时间、操作用户、相关资源等日志信息，您可以通过这些信息追踪实例相关的变更信息。

操作步骤

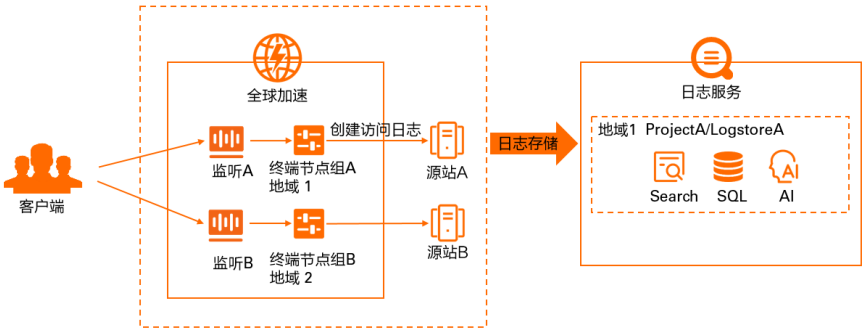
1.
2. 在左侧导航栏，选择**日志管理 > 操作日志**。
3. 在**操作日志**页面设置查询条件，然后单击图标。
   - 选择**服务名称**：系统默认为**全球加速（GA）**。
   - 选择事件类型：支持类型为**读写类型**、**用户名**和**资源类型**。
   - 选择时间范围：支持选择控制台显示的时间范围，也可以自定义时间范围。
4. 在需要查看的操作日志前，单击图标，查看详细信息。

8.2. 使用访问日志

全球加速提供访问日志功能，可以记录所有访问终端节点的流量信息，帮助您检查访问控制规则、排查网络故障等。

访问日志介绍

您可以选择为全球加速实例的一个或者多个终端节点组创建访问日志，采集到的访问日志将会投递到终端节点组所在地域SLS的日志库中。访问日志包括：客户端源IP、客户端源端口、目的IP、目的端口、加速地域等字段信息。



- 故障定位
  您可以根据访问日志快速定位和解决故障。
  例如，您可以根据status字段查看全球加速应答报文的状态，排查访问请求未获得预期响应的原因。
- 业务规划
  您可以根据访问日志进行数据分析，提前规划业务规格。

例如，您可以根据加速区域的访问流量趋势，提前进行带宽升级以满足业务发展，或者进行带宽降级以节省成本；您可以根据访问日志中的http_host字段，查看某段时间内访问应用的host列表，为应用更新做储备。

全球加速的访问日志功能无需额外付费，您仅需要支付SLS的费用。更多信息，请参见日志服务计费。

- 访问日志功能仅支持在SLS开服地域使用。更多信息，请参见开服地域。
- 仅标准型全球加速实例支持使用访问日志功能，基础型全球加速实例不支持。本文所有操作中的全球加速实例均指标准型全球加速实例。
- 当终端节点组所在地域为阿里云POP点时，不支持获取该终端节点组的访问日志。
- 暂不支持查询终端节点的域名。
- 2022年01月08日之后创建的GA实例可直接使用访问日志功能。如果您的全球加速实例创建于该时间之前，且需使用访问日志功能，请先提交工单进行实例升级。

单击此处，查看更多访问日志字段信息。❯

使用场景

费用说明

使用限制

创建访问日志

创建访问日志前，请确保已为全球加速实例添加了监听和终端节点组。具体操作，请参见添加和管理监听。

1.
2. 在**实例列表**页面，单击目标全球加速实例ID。
3. 在实例详情页面，单击**访问日志**页签。
4. 在**访问日志**页签下，单击**创建访问日志**，在**访问日志存储设置**对话框配置以下参数，然后单击**确定**。

配置		说明
选择存储内容	**监听ID/名称**	选择已创建的监听实例。
	终端节点组ID/名称	选择目标终端节点组。
存储设置	**日志服务地域**	系统默认选择为终端节点组所在地域。
	日志服务Project	日志服务中的资源管理单元，用于资源隔离和控制。 您可以**选择现有Project**，也可以**新建Project**。
	日志库Logstore	日志服务中日志数据的采集、存储和查询单元。 您可以**选择现有Logstore**，也可以**新建Logstore**。

> **说明** 执行此操作时，系统会判断全球加速是否拥有服务关联角色AliyunServiceRoleForGaFlowlog：
>
> - 如果全球加速不存在服务关联角色AliyunServiceRoleForGaFlowlog，系统会自动创建该服务关联角色，并为该服务关联角色添加名称为AliyunServiceRolePolicyForGaFlowlog的权限策略，授予全球加速拥有访问SLS并将流日志投递到SLS的权限。
> - 如果全球加速已经拥有服务关联角色AliyunServiceRoleForGaFlowlog，则不会重复创建该服务关联角色。
>
> 更多信息，请参见AliyunServiceRoleForGaFlowlog。

创建完成后，您可以在**访问日志**页签下查看已创建的访问日志。

更多操作

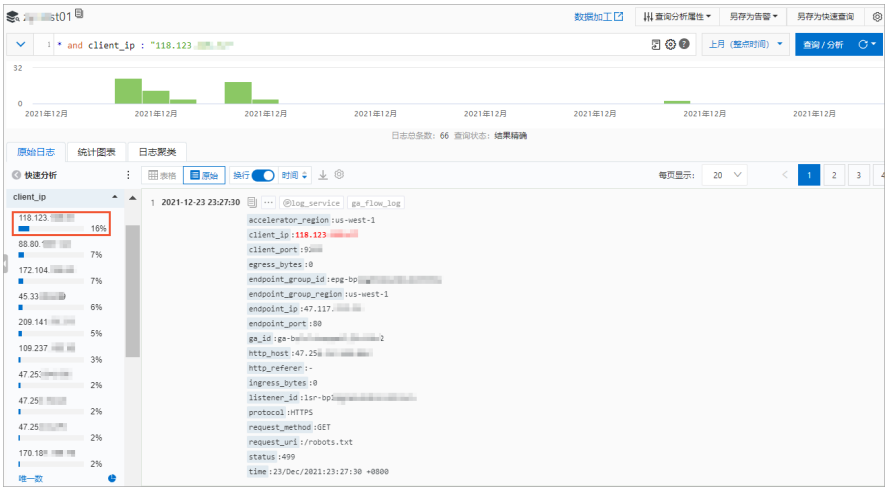
操作	说明
查看访问日志	1. 在**访问日志**页签下，找到目标访问日志，在其右侧的**操作**列，单击**查看日志**打开SLS控制台。 2. 查看并分析访问日志，更多信息，请参见使用示例。
删除访问日志	1. 在**访问日志**页签下，找到目标访问日志，在其右侧的**操作**列，单击**删除**。 2. 在弹出的**删除日志**对话框，单击**确定**。

SLS采集到访问日志后，您还可以下载、投递、加工日志、创建告警等操作。具体操作，请参见云产品日志通用操作。

使用示例

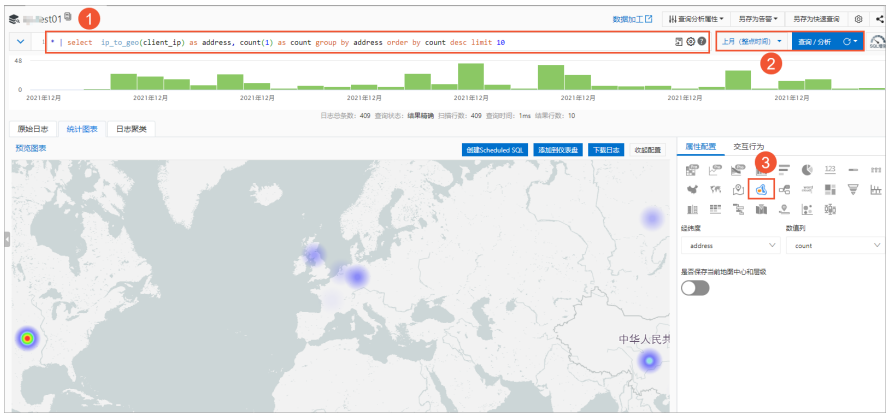
在对应日志库页面的**原始日志**页签下，查看对应的日志信息。

例如，单击**client_ip**字段，查看客户端源IP的访问请求信息。



在对应日志库页面的查询和分析语句输入框中输入SQL语句，查询特定的访问日志。

例如，根据下图示例顺序，查询客户端IP分布情况。



序号	步骤描述
①	输入如下SQL语句查询客户端IP分布热力图，查看Top10的分布地域，辅助业务规划。 `* | select ip_to_geo(client_ip) as address, count(1) as count group by address order by count desc limit 10`
②	选择要查看访问日志的时间范围，并单击**查询/分析**。
③	在**统计图表>属性配置**页签下，单击图标，即可查看客户端IP的分布情况。

查看原始访问日志

查询特定的访问日志

9.配额管理

您可以通过配额管理查询当前全球加速的资源配额使用情况。如果某个资源的剩余配额不满足业务需求，您可以申请提升配额。

操作步骤

1.
2. 在左侧导航栏，单击**配额管理**。
3. 在**配额管理**页面，查看当前账号下全球加速的资源配额使用情况。

配额名称	描述	类型	用量/配额	操作
gaplus_quota_accelerator	每个用户可以保有的全球加速实例个数	配额	10	申请
gaplus_quota_endpoint	每个终端节点组的最大终端节点数	配额	4	申请
gaplus_quota_listener_per_accelerator	每个加速实例的监听个数	配额	10	申请

4. 如果需要提升配额，在**操作**列下单击**申请**，提交配额申请，然后单击**确定**。
   - **申请数量**：需要的资源配额数量，申请数量必须为数字且大于当前配额。全球加速的资源默认使用限制，请参见使用限制。
   - **申请原因**：请详细描述申请配额的原因、业务场景和必要性。
   - **手机/固话**：申请配额的用户电话号码。
   - **电子邮箱**：申请配额的用户电子邮箱。

执行结果

提交配额申请后，您可以单击**操作**列下的**申请历史**，查看配额申请情况。
系统会自动审批配额申请是否合理：

- 如果您申请的配额超过可申请的配额数量时，系统会自动拒绝您的申请，申请状态变更为**拒绝**。
  如果申请被拒绝，请降低预申请的配额数量，然后再提交申请。
- 如果您申请的配额在可申请的配额数量范围内，系统会自动同意您的申请，申请状态变更为**通过**，配额立即自动提升为申请的数量。

10.权限管理

10.1. 服务关联角色

10.1.1. AliyunServiceRoleForGaVpcEndpoint

如果您的全球加速不存在服务关联角色AliyunServiceRoleForGaVpcEndpoint，您在配置云服务器ECS或传统型负载均衡CLB（原SLB）为全球加速终端节点时，系统会自动创建服务关联角色AliyunServiceRoleForGaVpcEndpoint。

AliyunServiceRoleForGaVpcEndpoint简介

AliyunServiceRoleForGaVpcEndpoint是全球加速的一种服务关联角色SLR（Service Linked Role），在配置全球加速终端节点时，全球加速需要拥有该服务关联角色才能将云服务器ECS和传统型负载均衡CLB添加为全球加速的终端节点。

> **说明** 服务关联角色是指与某个云服务关联的访问控制（RAM）角色。在某些场景下，为了完成云服务的某个功能，需要获取访问其他云服务的权限。通过服务关联角色，您可以更好地创建云服务正常操作所需的权限，避免误操作带来的风险。更多关于服务关联角色的信息，请参见服务关联角色。

创建服务关联角色AliyunServiceRoleForGaVpcEndpoint所需的权限

阿里云账号（主账号）默认拥有创建服务关联角色AliyunServiceRoleForGaVpcEndpoint的权限，RAM用户（子账号）必须拥有以下权限，才可以创建服务关联角色AliyunServiceRoleForGaVpcEndpoint：

```
{
      "Action": "ram:CreateServiceLinkedRole",
      "Resource": "*",
      "Effect": "Allow",
      "Condition": {
        "StringEquals": {
          "ram:ServiceName": "vpcendpoint.ga.aliyuncs.com"
        }
      }
}
```

您可以通过以下两种方式为RAM用户（子账号）授予创建AliyunServiceRoleForGaVpcEndpoint所需的权限：

- 为RAM用户（子账号）添加管理员权限策略AliyunGlobalAccelerationFullAccess。具体操作，请参见为RAM角色授权。

  > **说明** 创建全球加速服务关联角色AliyunServiceRoleForGaVpcEndpoint的权限通常包含在管理员权限策略AliyunGlobalAccelerationFullAccess中，因此只要拥有全球加速的管理员权限，就可以为全球加速创建服务关联角色AliyunServiceRoleForGaVpcEndpoint。

- 添加自定义权限策略，并为RAM用户（子账号）授权。自定义权限策略包含以下权限：

```
{
      "Action": "ram:CreateServiceLinkedRole",
      "Resource": "*",
      "Effect": "Allow",
      "Condition": {
        "StringEquals": {
          "ram:ServiceName": "vpcendpoint.ga.aliyuncs.com"
        }
      }
}
```

具体操作，请参见创建自定义权限策略和为RAM角色授权。

创建服务关联角色AliyunServiceRoleForGaVpcEndpoint

您在配置云服务器ECS或传统型负载均衡CLB为全球加速终端节点时，系统会判断全球加速是否拥有服务关联角色AliyunServiceRoleForGaVpcEndpoint：

- 如果全球加速不存在服务关联角色AliyunServiceRoleForGaVpcEndpoint，系统会自动创建该服务关联角色，并为该服务关联角色添加名称为AliyunServiceRoleForGaVpcEndpoint的权限策略，授予全球加速拥有访问云服务器ECS和传统型负载均衡CLB的权限，策略内容如下：

```
{
  "Version": "1",
  "Statement": [
    {
      "Effect": "Allow",
      "Resource": "*",
      "Action": [
        "ecs:CreateNetworkInterface",
        "ecs:DeleteNetworkInterface",
        "ecs:DescribeNetworkInterfaces",
        "ecs:ModifyNetworkInterfaceAttribute",
        "ecs:DescribeSecurityGroups",
        "ecs:CreateSecurityGroup",
        "ecs:AuthorizeSecurityGroup",
        "ecs:AuthorizeSecurityGroupEgress",
        "ecs:RevokeSecurityGroup",
        "ecs:RevokeSecurityGroupEgress",
        "ecs:JoinSecurityGroup",
        "ecs:LeaveSecurityGroup",
        "ecs:DeleteSecurityGroup",
        "ecs:DescribeSecurityGroupAttribute",
        "ecs:DescribeSecurityGroups",
        "ecs:DescribeSecurityGroupReferences",
        "ecs:ModifySecurityGroupAttribute",
        "ecs:ModifySecurityGroupEgressRule",
        "ecs:ModifySecurityGroupPolicy",
        "ecs:ModifySecurityGroupRule",
        "vpc:DescribeVSwitches"
      ]
    },
    {
      "Action": "ram:DeleteServiceLinkedRole",
      "Resource": "*",
      "Effect": "Allow",
      "Condition": {
        "StringEquals": {
          "ram:ServiceName": "vpcendpoint.ga.aliyuncs.com"
        }
      }
    }
  ]
}
```

- 如果全球加速已经拥有服务关联角色AliyunServiceRoleForGaVpcEndpoint，则不会重复创建该服务关联角色。

删除服务关联角色AliyunServiceRoleForGaVpcEndpoint

系统不会自动删除全球加速的服务关联角色AliyunServiceRoleForGaVpcEndpoint，如果您要删除该服务关联角色，请先删除终端节点类型为云服务器ECS和传统型负载均衡CLB的终端节点，然后再删除服务关联角色AliyunServiceRoleForGaVpcEndpoint。具体操作，请参见：

1. 删除终端节点
2. 删除服务关联角色

10.1.2. AliyunServiceRoleForGaAntiDdos

如果您的全球加速不存在服务关联角色AliyunServiceRoleForGaVpcEndpoint，您在为全球加速提升DDoS阈值时，系统会自动创建服务关联角色AliyunServiceRoleForGaVpcEndpoint，以获取访问DDoS高防实例的权限。

AliyunServiceRoleForGaAntiDdos简介

AliyunServiceRoleForGaAntiDdos是全球加速的一种服务关联角色SLR（Service Linked Role），在为全球加速提升DDoS阈值时，需要拥有该服务关联角色才能访问DDoS高防实例。如何提升DDoS阈值，请参见提升DDoS阈值。

> **说明** 服务关联角色是指与某个云服务关联的访问控制（RAM）角色。在某些场景下，为了完成云服务的某个功能，需要获取访问其他云服务的权限。通过服务关联角色，您可以更好地创建云服务正常操作所需的权限，避免误操作带来的风险。更多关于服务关联角色的信息，请参见服务关联角色。

创建服务关联角色AliyunServiceRoleForGaAntiDdos所需的权限

阿里云账号默认拥有创建服务关联角色AliyunServiceRoleForGaAntiDdos的权限，RAM用户必须拥有以下权限，才可以创建服务关联角色AliyunServiceRoleForGaAntiDdos：

```
{
    "Action": "ram:CreateServiceLinkedRole",
    "Resource": "*",
    "Effect": "Allow",
    "Condition": {
        "StringEquals": {
            "ram:ServiceName": "ddos.ga.aliyuncs.com"
        }
    }
}
```

您可以通过以下两种方式为RAM用户授予创建AliyunServiceRoleForGaAntiDdos所需的权限：

- 为RAM用户添加管理员权限策略AliyunGlobalAccelerationFullAccess。具体操作，请参见为RAM角色授权。

  > **说明** 创建全球加速服务关联角色AliyunServiceRoleForGaAntiDdos的权限通常包含在管理员权限策略AliyunGlobalAccelerationFullAccess中，因此只要拥有全球加速的管理员权限，就可以为全球加速创建服务关联角色AliyunServiceRoleForGaAntiDdos。

- 添加自定义权限策略，并为RAM用户授权。自定义权限策略包含以下权限：

```
{
    "Action": "ram:CreateServiceLinkedRole",
    "Resource": "*",
    "Effect": "Allow",
    "Condition": {
        "StringEquals": {
            "ram:ServiceName": "ddos.ga.aliyuncs.com"
        }
    }
}
```

具体操作，请参见创建自定义权限策略和为RAM角色授权。

创建服务关联角色AliyunServiceRoleForGaAntiDdos

您在为全球加速提升DDoS阈值时，系统会判断全球加速是否拥有服务关联角色AliyunServiceRoleForGaAntiDdos：

- 如果全球加速不存在服务关联角色AliyunServiceRoleForGaAntiDdos，系统会自动创建该服务关联角色，并为该服务关联角色添加名称为AliyunServiceRolePolicyForGaAntiDdos的权限策略，授予全球加速拥有访问DDoS高防实例的权限，策略内容如下：

```
{
  "Version": "1",
  "Statement": [
    {
      "Effect": "Allow",
      "Resource": "*",
      "Action": [
        "yundun-ddoscoo:DescribeInstanceDetails"
      ]
    },
    {
      "Action": "ram:DeleteServiceLinkedRole",
      "Resource": "*",
      "Effect": "Allow",
      "Condition": {
        "StringEquals": {
          "ram:ServiceName": "ddos.ga.aliyuncs.com"
        }
      }
    }
  ]
}
```

- 如果全球加速已经拥有服务关联角色AliyunServiceRoleForGaAntiDdos，则不会重复创建该服务关联角色。

删除服务关联角色AliyunServiceRoleForGaAntiDdos

系统不会自动删除全球加速的服务关联角色AliyunServiceRoleForGaAntiDdos，如果您要删除该服务关联角色，请先删除全球加速与DDoS高防实例的绑定关系。具体操作，请参见：

1. 重置DDoS阈值
2. 删除服务关联角色

10.1.3. AliyunServiceRoleForGaFlowlog

本文为您介绍全球加速服务关联角色AliyunServiceRoleForGaFlowlog的应用场景，以及如何创建删除服务关联角色。

AliyunServiceRoleForGaFlowlog简介

AliyunServiceRoleForGaFlowlog是全球加速的一种服务关联角色SLR（Service Linked Role）。拥有该角色后，阿里云全球加速服务可以访问您的日志服务（SLS），将流日志投递到您的SLS。

> **说明** 服务关联角色是指与某个云服务关联的访问控制（RAM）角色。在某些场景下，为了完成云服务的某个功能，需要获取访问其他云服务的权限。通过服务关联角色，您可以更好地创建云服务正常操作所需的权限，避免误操作带来的风险。更多信息，请参见服务关联角色。

创建服务关联角色AliyunServiceRoleForGaFlowlog所需的权限

阿里云账号默认拥有创建服务关联角色AliyunServiceRoleForGaFlowlog的权限，RAM用户必须拥有以下权限，才可以进行创建：

```
{
      "Action": "ram:CreateServiceLinkedRole",
      "Resource": "*",
      "Effect": "Allow",
      "Condition": {
        "StringEquals": {
          "ram:ServiceName": "flowlog.ga.aliyuncs.com"
        }
      }
}
```

您可以通过以下两种方式为RAM用户授予创建AliyunServiceRoleForGaFlowlog所需的权限：

- 为RAM用户添加管理员权限策略AliyunGlobalAccelerationFullAccess。具体操作，请参见为RAM角色授权。

  > **说明** 创建全球加速服务关联角色的权限通常包含在管理员权限策略AliyunGlobalAccelerationFullAccess中，因此只要拥有全球加速的管理员权限，就可以为全球加速创建服务关联角色。

- 添加自定义权限策略，并为RAM用户授权。自定义权限策略包含以下权限：

  ```
  {
        "Action": "ram:CreateServiceLinkedRole",
        "Resource": "*",
        "Effect": "Allow",
        "Condition": {
          "StringEquals": {
            "ram:ServiceName": "flowlog.ga.aliyuncs.com"
          }
        }
  }
  ```

  具体操作，请参见创建自定义权限策略和为RAM角色授权。

创建服务关联角色AliyunServiceRoleForGaFlowlog

为全球加速实例开启流日志的投递功能，系统会自动创建服务关联角色AliyunServiceRoleForGaFlowlog，并为该服务关联角色添加名称为AliyunServiceRolePolicyForGaFlowlog的权限策略，授予全球加速拥有访问用户流日志的权限，策略内容如下：

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "log:PostLogStoreLogs"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": "ram:DeleteServiceLinkedRole",
      "Resource": "*",
      "Effect": "Allow",
      "Condition": {
        "StringEquals": {
          "ram:ServiceName": "flowlog.ga.aliyuncs.com"
        }
      }
    }
  ]
}
```

删除服务关联角色AliyunServiceRoleForGaFlowlog

系统不会自动删除全球加速的服务关联角色AliyunServiceRoleForGaFlowlog，如果您要删除该服务关联角色，请先删除所有全球加速实例，然后再删除服务关联角色AliyunServiceRolePolicyForGaFlowlog。具体操作，请参见删除服务关联角色。

10.1.4. AliyunServiceRoleForGaAlb

如果您的全球加速不存在服务关联角色AliyunServiceRoleForGaAlb，您在配置负载均衡ALB为全球加速终端节点时，系统会自动创建服务关联角色AliyunServiceRoleForGaAlb。

AliyunServiceRoleForGaAlb简介

AliyunServiceRoleForGaAlb是全球加速的一种服务关联角色SLR（Service Linked Role），在配置全球加速终端节点时，全球加速需要拥有该服务关联角色才能将负载均衡ALB添加为全球加速的终端节点。

> **说明** 服务关联角色是指与某个云服务关联的访问控制（RAM）角色。在某些场景下，为了完成云服务的某个功能，需要获取访问其他云服务的权限。通过服务关联角色，您可以更好地创建云服务正常操作所需的权限，避免误操作带来的风险。更多关于服务关联角色的信息，请参见服务关联角色。

创建服务关联角色AliyunServiceRoleForGaAlb所需的权限

阿里云账号（主账号）默认拥有创建服务关联角色AliyunServiceRoleForGaAlb的权限，RAM用户（子账号）必须拥有以下权限，才可以创建服务关联角色AliyunServiceRoleForGaAlb：

```
{
      "Action": "ram:CreateServiceLinkedRole",
      "Resource": "*",
      "Effect": "Allow",
      "Condition": {
        "StringEquals": {
          "ram:ServiceName": "alb.ga.aliyuncs.com"
        }
      }
}
```

您可以通过以下两种方式为RAM用户（子账号）授予创建AliyunServiceRoleForGaAlb所需的权限：

- 为RAM用户（子账号）添加管理员权限策略AliyunGlobalAccelerationFullAccess。详细信息，请参见为RAM角色授权。

  > **说明** 创建全球加速服务关联角色AliyunServiceRoleForGaAlb的权限通常包含在管理员权限策略AliyunGlobalAccelerationFullAccess中，因此只要拥有全球加速的管理员权限，就可以为全球加速创建服务关联角色AliyunServiceRoleForGaAlb。

- 添加自定义权限策略，并为RAM用户（子账号）授权。自定义权限策略包含以下权限：

  ```
  {
        "Action": "ram:CreateServiceLinkedRole",
        "Resource": "*",
        "Effect": "Allow",
        "Condition": {
          "StringEquals": {
            "ram:ServiceName": "alb.ga.aliyuncs.com"
          }
        }
  }
  ```

  具体操作，请参见创建自定义权限策略和为RAM角色授权。

创建服务关联角色AliyunServiceRoleForGaAlb

您在配置负载均衡ALB为全球加速终端节点时，系统会判断全球加速是否拥有服务关联角色AliyunServiceRoleForGaAlb：

- 如果全球加速不存在服务关联角色AliyunServiceRoleForGaAlb，系统会自动创建该服务关联角色，并为该服务关联角色添加名称为AliyunServiceRoleForGaAlb的权限策略，授予全球加速拥有访问负载均衡ALB的权限，策略内容如下：

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "alb:GetLoadBalancerAttribute",
      "Resource": "*"
    },
    {
      "Action": "ram:DeleteServiceLinkedRole",
      "Resource": "*",
      "Effect": "Allow",
      "Condition": {
        "StringEquals": {
          "ram:ServiceName": "alb.ga.aliyuncs.com"
        }
      }
    }
  ],
  "Version": "1"
}
```

- 如果全球加速已经拥有服务关联角色AliyunServiceRoleForGaAlb，则不会重复创建该服务关联角色。

删除服务关联角色AliyunServiceRoleForGaAlb

系统不会自动删除全球加速的服务关联角色AliyunServiceRoleForGaAlb，如果您要删除该服务关联角色，请先删除终端节点类型为负载均衡ALB的终端节点，然后再删除服务关联角色AliyunServiceRoleForGaAlb。具体操作，请参见：

1. 删除终端节点
2. 删除服务关联角色

10.1.5. AliyunServiceRoleForGaOss

如果您的全球加速不存在服务关联角色AliyunServiceRoleForGaOss，您在配置对象存储服务OSS为全球加速终端节点时，系统会自动创建服务关联角色AliyunServiceRoleForGaOss。

AliyunServiceRoleForGaOss简介

AliyunServiceRoleForGaOss是全球加速的一种服务关联角色SLR（Service Linked Role），在配置全球加速终端节点时，全球加速需要拥有该服务关联角色才能将对象存储服务OSS添加为全球加速的终端节点。

> **说明** 服务关联角色是指与某个云服务关联的访问控制（RAM）角色。在某些场景下，为了完成云服务的某个功能，需要获取访问其他云服务的权限。通过服务关联角色，您可以更好地创建云服务正常操作所需的权限，避免误操作带来的风险。更多关于服务关联角色的信息，请参见服务关联角色。

创建服务关联角色AliyunServiceRoleForGaOss所需的权限

阿里云账号（主账号）默认拥有创建服务关联角色AliyunServiceRoleForGaOss的权限，RAM用户（子账号）必须拥有以下权限，才可以创建服务关联角色AliyunServiceRoleForGaOss：

```
{
      "Action": "ram:CreateServiceLinkedRole",
      "Resource": "*",
      "Effect": "Allow",
      "Condition": {
        "StringEquals": {
          "ram:ServiceName": "oss.ga.aliyuncs.com"
        }
      }
}
```

您可以通过以下两种方式为RAM用户（子账号）授予创建AliyunServiceRoleForGaOss所需的权限：

- 为RAM用户（子账号）添加管理员权限策略AliyunGlobalAccelerationFullAccess。具体操作，请参见为RAM角色授权。

  > **说明** 创建全球加速服务关联角色AliyunServiceRoleForGaOss的权限通常包含在管理员权限策略AliyunGlobalAccelerationFullAccess中，因此只要拥有全球加速的管理员权限，就可以为全球加速创建服务关联角色AliyunServiceRoleForGaOss。

- 添加自定义权限策略，并为RAM用户（子账号）授权。自定义权限策略包含以下权限：

  ```
  {
        "Action": "ram:CreateServiceLinkedRole",
        "Resource": "*",
        "Effect": "Allow",
        "Condition": {
          "StringEquals": {
            "ram:ServiceName": "oss.ga.aliyuncs.com"
          }
        }
  }
  ```

  具体操作，请参见创建自定义权限策略和为RAM角色授权。

创建服务关联角色AliyunServiceRoleForGaOss

您在配置对象存储服务OSS为全球加速终端节点时，系统会判断全球加速是否拥有服务关联角色AliyunServiceRoleForGaOss：

- 如果全球加速不存在服务关联角色AliyunServiceRoleForGaOss，系统会自动创建该服务关联角色，并为该服务关联角色添加名称为AliyunServiceRoleForGaOss的权限策略，授予全球加速拥有访问对象存储服务OSS的权限，策略内容如下：

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "oss:getBucketInfo",
      "Resource": "*"
    },
    {
      "Action": "ram:DeleteServiceLinkedRole",
      "Resource": "*",
      "Effect": "Allow",
      "Condition": {
        "StringEquals": {
          "ram:ServiceName": "oss.ga.aliyuncs.com"
        }
      }
    }
  ],
  "Version": "1"
}
```

- 如果全球加速已经拥有服务关联角色AliyunServiceRoleForGaOss，则不会重复创建该服务关联角色。

删除服务关联角色AliyunServiceRoleForGaOss

系统不会自动删除全球加速的服务关联角色AliyunServiceRoleForGaOss，如果您要删除该服务关联角色，请先删除终端节点类型为对象存储服务OSS的终端节点，然后再删除服务关联角色AliyunServiceRoleForGaOss。具体操作，请参见：

1. 删除终端节点
2. 删除服务关联角色

10.2. 为RAM用户授权

RAM用户（子账号）默认情况下不能创建全球加速资源，也不能访问和管理阿里云账号（主账号）下的全球加速资源。如果您希望RAM用户可以访问或操作全球加速资源，您需要为RAM用户授权。

前提条件

您已经创建了RAM用户。详细信息，请参见创建RAM用户。

操作步骤

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，选择**身份管理 > 用户**。
3. 在**用户**页面，找到目标RAM用户，在**操作**列单击**添加权限**。
4. 在**添加权限**面板，根据以下信息添加权限，然后单击**确定**。

配置	说明
授权范围	根据需要选择权限的生效范围： ○ **整个云账号**：权限在当前阿里云账号内生效。 ○ **指定资源组**：权限在指定的资源组内生效。

配置	说明
授权主体	系统会将步骤中的目标RAM用户自动填入被授权主体。
选择权限	选择**系统策略**，然后选择要授予RAM用户的权限策略。 您可以为RAM用户授予以下全球加速系统策略： ○ **AliyunGlobalAccelerationReadOnlyAccess**：只读访问全球加速的权限。 ○ **AliyunGlobalAccelerationFullAccess**：管理全球加速的权限。

5. 确认授权应用范围和权限策略，然后单击**完成**。