全球加速2.0

操作指南

腾讯云

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或95716。

文档目录

操作指南
加速区域

最近更新时间：2026-03-16 16:39:52

概述

加速区域是最靠近终端客户的区域，终端用户通过全球加速2.0（GA2.0）加速区域的接入 IP 就近接入腾讯云全球加速网络。

说明：

- 如终端用户区域不在 GA2.0 支持区域列表内，可选择就近区域实现覆盖。
- 全球加速2.0跨境段由中国联通代运营，如加速区域和终端节点组存在跨境，您的账号需要先通过 跨境资质审核，详情可参见 跨境云专线服务协议 。
- 单次创建，最多添加20个加速地域。

支持的加速区域

地区	包含的区域
中国大陆	北京
	上海
	广州
	成都
	南京
港澳台地区	中国香港
亚太	新加坡
	印尼雅加达
	韩国首尔
	日本东京
	泰国曼谷
欧洲	德国法兰克福

北美	美国西部硅谷
	美国东部弗吉尼亚
南美	巴西圣保罗
中东	利雅得

加速 IP 类型

加速 IP 类型分为常规 BGP IP 及精品 BGP IP，您可按需选择加速 IP 类型。

- 常规 BGP IP：国内多线 BGP 网络覆盖超过二十家网络运营商（三大运营商、教育网、广电等），BGP 公网出口支持秒级跨域切换，保证您的用户无论使用哪种网络，均能享受高速、安全的网络质量。
- 精品 BGP IP：专属线路，避免绕行国际运营商出口网络；延时更低，可有效提升境外业务对中国大陆用户覆盖质量。

> **说明：**
> - 常规 BGP IP：对于中国港澳台地区和其他国家地域的常规 BGP IP，主要面向从中国大陆境外发起的访问；如果您在中国大陆境内访问境外的 IP，可能会有较多的延迟和丢包，
> - 精品 BGP IP：延时更低，适用于中国大陆境内访问境外 IP，且对网络质量敏感的业务场景。目前仅中国香港区域支持选择精品 BGP IP 作为接入 IP。

IP 协议栈

当前仅支持 IPv4 协议接入。

加速区域带宽

- 加速地域带宽是创建加速区域时配置的带宽上限，实际业务带宽无法突破该带宽上限，允许配置的范围是2-1000Mbps，如需突破请 提交工单 咨询。
- 加速地域带宽上限与计费无直接关联，最终会统计实际业务流量作为计费依据。
- 带宽峰值仅作为带宽最高上限峰值，不作为承诺指标。当出现带宽资源争抢时，带宽峰值可能会受到限制。

添加加速区域

1. 登录 全球加速控制台 。
2. 在实例列表页面，单击目标**实例 ID**，进入实例详情页。
3. 单击**加速区域**页签下的**添加加速区域。**（注：单次最多添加20个加速地域）
4. 根据提示配置对应信息。

配置项	说明

区域	所创建的加速区域，全球加速2.0将会在所选区域创建加速IP供终端用户接入。
带宽峰值	用户从该区域接入全球加速2.0可达到的最大业务带宽峰值，带宽峰值仅决定业务带宽上限，与最终费用没有直接关系，创建后将根据实际业务流量统计费用。单位：Mbps。 • 每个加速区域支持分配的带宽范围为2-1000Mbps。 • 带宽峰值仅作为带宽最高上限峰值，不作为承诺指标。当出现带宽资源争抢时，带宽峰值可能会受到限制。
IP 地址协议	终端用户接入全球加速2.0的 IP 地址协议，当前仅支持 IPv4 网络接入。
公网质量类型	终端用户接入全球加速2.0的公网质量类型。 • 普通 BGP：使用腾讯云普通 BGP IP 作为接入 IP，同时接入多家运营商线路，保障最优访问质量。 • 精品 BGP：使用运营商精品公网线路接入，相比普通 BGP，中国大陆用户接入质量更优。选择中国香港作为加速区域时，可选择加速 IP 公网质量类型为精品 BGP。

注意：
如您的业务使用的是全球统一域名，且您的业务通过全局 CNAME 方式接入 GA2.0，如果配置中未包含国内任意加速点，则国内用户的访问请求将被系统默认解析至127.0.0.1。

编辑加速区域

前提条件

已完成实例及 加速区域创建 。您可对已有加速区域进行带宽编辑操作。

注意：
如修改后的带宽上限低于修改前，可能导致业务受损，请谨慎操作。

操作步骤

1. 登录 全球加速控制台 。
2. 在实例列表页面，单击目标**实例 ID**，进入实例详情页，并单击**加速区域**页签。
3. 单击已有加速区域右侧操作栏的**编辑带宽**。
4. 在弹窗中输入目标带宽上限，单击**确定**。

删除加速区域

前提条件

> **注意：**
> 加速区域删除后加速 IP 将被释放，相关配置无法恢复，请充分确认影响后操作。

已完成实例及 加速区域创建 。加速区域删除后，对应加速IP及带宽配置将被释放，全球加速将无法再为该区域提供加速服务。

操作步骤

1. 登录 全球加速控制台 。
2. 在实例列表页面，单击目标**实例 ID**，进入实例详情页，并单击**加速区域**页签。
3. 单击已有加速区域右侧操作栏的**删除**。
4. 在弹窗中单击**确定**。

监听器
配置 TCP 和 UDP 监听器

最近更新时间：2026-03-16 16:39:52

监听器概述

创建全球加速实例后，您需要为实例配置监听器。监听器负责监听客户端请求，并将流量分发至后端终端节点上。
全球加速监听器需配置：

1. 监听协议和监听端口。监听器的监听端口，亦被称为前端端口，用来接收请求并向后端服务器转发请求的端口。
2. 监听策略，如均衡策略、会话保持 等。
3. 添加终端节点组。需创建终端节点组并添加终端节点。

支持的协议类型

全球加速支持监听来自客户端的四层和七层请求，并将这些请求分发到后端终端节点上，而后由后端终端节点处理请求。四层和七层监听器的区别主要体现在：当用户请求到来时，是依据四层协议还是七层协议来转发流量，例如：对 TCP、UDP 等四层协议请求进行四层转发，对 HTTP、HTTPS 等七层协议请求进行七层转发。
四层协议：传输层协议，主要通过 VIP + Port 接收请求并分配流量到后端服务器。
七层协议：应用层协议，基于 URL、HTTP 头部等应用层信息进行流量分发。
腾讯云全球加速支持以下协议的请求转发：

- TCP（传输层）
- UDP（传输层）
- HTTP（应用层）
- HTTPS（应用层）

协议分类	协议	说明	应用场景
四层协议	TCP	面向连接的、可靠的传输层协议。 传输的源端和终端需先三次握手建立连接，再传输数据。 支持基于客户端 IP（源 IP）的会话保持。 支持获取客户端源IP。	适用于对可靠性和数据准确性要求高、对传输速度要求较低的场景，如文件传输、收发邮件、远程登录等。
	UDP	无连接的传输层协议。 传输的源端和终端不建立连接，不需维护连接状态。 每一条 UDP 连接都只能是点到点的。	适用于对传输效率要求高、对准确性要求相对较低的场景，如即时通讯、在线视频等。

		支持一对一，一对多，多对一和多对多的交互通信。 支持基于客户端 IP（源 IP）的会话保持。	
七层协议	HTTP	应用层协议。 支持基于请求域名和 URL 的转发。	需要对请求的内容进行识别的应用，例如 Web 应用、App 服务等。详情请参见 配置 HTTP 和 HTTPS 监听器 。
	HTTPS	加密的应用层协议。 支持基于请求域名和 URL 的转发。 统一的证书管理服务，可在全球加速控制台完成证书上传及替换。 支持单向认证和双向认证。	需加密传输的 HTTP 应用。详情请参见 配置 HTTP 和 HTTPS 监听器 。

支持的端口范围

端口类型	说明	限制
监听端口（前端端口）	监听端口是全球加速接收请求并向终端节点转发请求的端口。您可以配置的端口范围为1 - 65499。	在同一个全球加速实例内： UDP 类协议可以和 TCP 类协议的监听端口重复。例如，可以同时创建监听器 TCP:80 和监听器 UDP:80。 同一类协议下监听端口不可重复，TCP/TCP SSL/HTTP/HTTPS 同属于 TCP 类。例如，不可以同时创建监听器 TCP:80 和监听器 HTTP:80。
终端节点端口（后端端口）	七层监听器支持配置终端节点端口，终端节点端口是后端服务器提供服务的端口，接收并处理来自全球加速的流量。 您可以配置的终端节点端口范围为1 - 65499。	在同一个全球加速实例内： 不同监听协议的服务端口可以重复。例如，监听器 HTTP:80 和监听器 HTTPS:443 可以同时绑定同一台后端服务器的同一个端口。
健康检查端口	健康检查端口用于全球加速向后端服务器发送探测请求，以确认服务器是否正常运行。若端口响应正常，则认为服务器健康。您可以配置的健康检查端口范围为1 - 65499。	-

您需要为全球加速实例创建监听器，用于监听用户请求及将流量转发到后端终端节点，全球加速 GA 支持 TCP、UDP、HTTP 及 HTTPS 协议，本章节为您介绍 TCP、UDP 监听器配置及操作指南。

操作步骤

前提条件

已完成 全球加速2.0实例创建 。

创建监听器

1. 登录 全球加速控制台 。
2. 在标准实例列表页面，单击目标**实例 ID**，进入实例详情页。
3. 单击监听器页签下的**添加监听器**。
4. 配置监听器。

配置类型	配置项	说明
基础配置	监听器名称	• 以大小写字母或中文开头。 • 长度2-128字符。 • 支持数字、英文句号 “.” 或短划线 “-” 、下划线 “_” 。
	路由类型	智能路由：根据延时选择最近终端节点组进行转发。
	协议	支持选择 TCP、UDP、HTTP、HTTPS。 • TCP（传输控制协议）：面向连接、可靠传输（确认/重传机制）、保证数据顺序，适用于网页浏览（HTTP/HTTPS）、文件传输（FTP）、电子邮件（SMTP）等对可靠性要求高的场景。 • UDP（用户数据报协议）：无连接、不可靠传输、低延迟，适用于实时音视频（如 VoIP）、在线游戏、DNS 查询等对速度敏感且允许丢包的场景。
	端口	支持端口范围为 1-65499。
高级配置	获取客户端源 IP	• TCP 协议：开启后，可通过 ProxyProtocol 或 ProxyProtocol V2 代理协议获取客户端真实 IP。 • UDP 协议：可通过 ProxyProtocol V2 代理协议获取客户端真实 IP。
	会话保持	• 开启：来自同一个 IP 的用户请求保持访问相同源站。 • 关闭：无法保障来自同一个 IP 的用户请求保持访问相同源站。
	连接空闲超时时间	指定连接空闲超时时间。在超时时间内一直没有数据交互，全球加速会中断当前连接，直到下一次请求来临时重新建立新的连接。监听协议不同，取值范围不同。

		• TCP监听：取值范围为10-900秒，默认值为900秒。 • UDP监听：取值范围是10-20秒，默认是20秒。

5. 配置终端节点组

监听器创建时，您可以为监听器创建默认终端节点组，来承接监听器转发到后端的流量。配置终端节点组时，您需要为节点组添加终端节点并按需开启健康检查。

> **说明：**
> 监听器首次创建时配置的节点组为默认终端节点组，TCP 和 UDP 监听器仅支持创建一个默认终端节点组，不支持创建自定义终端节点组。

配置类型	配置项	说明
终端节点组	节点组名称	• 以大小写字母或中文开头。 • 长度 2-128 字符。 • 支持数字、英文句号 “.” 或短划线 “-” 、下划线 “_” 。
	地域	终端节点组所在地域，全球加速会将来自加速区域的流量转发到终端节点组地域。 **注意：** 如加速区域与终端节点组属于同一地域，可能导致加速效果不佳。
	后端服务类型	终端节点是最终提供服务的后端源站，终端节点类型支持自定义域名及自定义 IP。
	后端服务	最终提供服务的后端源站，您可为一个终端节点组最多添加4个终端节点，支持输入自定义 IP 或自定义域名。例如： • `117.89.1.1` • `example.com`
	权重	终端节点权重，全球加速将按照您配置的终端节点权重来分发业务流量到后端服务器。 • 默认值：100。 • 配置范围：1-100。
	端口映射	监听端口：输入端口须与当前监听所配置的端口一致

	终端节点端口：终端节点提供服务的端口，端口取值范围：1-65499
健康检查	• 开启：全球加速将按配置的健康检查参数来检查后端源站的可用性。 • 关闭：全球加速不对源站进行健康检查探测。

检查协议	全球加速用于检测后端服务器是否可用的网络协议。
	• TCP：支持 TCP 与自定义探测。
	  ○ TCP：全球加速通过 TCP 协议检测后端服务器是否可用。
	  ○ 自定义探测：通过手动配置健康检查的检查请求、检查返回结果来对后端服务器进行检测。
	• UDP：支持 PING 与自定义探测。
	  ○ PING：全球加速通过 PING 协议检测后端服务器是否可用。
	  ○ 自定义探测：通过手动配置健康检查的检查请求、检查返回结果来对后端服务器进行检测。

响应超时时间	全球加速向后端服务器发送健康检查请求后，等待服务器响应的最长时间。若超时未收到响应，则判定本次检查失败。 • 默认值：2s。 • 配置范围：2s-60s。
健康检查间隔	两次健康检查之间的时间间隔。 • 默认值：30s。 • 配置范围：5s-300s。
不健康阈值	连续健康检查失败的次数达到该阈值后，后端服务器被标记为不健康，并从流量分发池中移除。 • 默认值：3次。 • 配置范围：1次-10次。
健康阈值	连续健康检查成功的次数达到该阈值后，不健康的服务器被重新标记为健康并恢复流量分发。 • 默认值：3次。 • 配置范围：1次-10次。

编辑监听器

1. 登录 全球加速控制台 。
2. 在实例列表页面，单击目标**实例 ID**，进入实例详情页。
3. 单击**监听器**，进入监听器列表页。

4. 单击**实例 ID**或操作下的**实例详情**，可进入监听器实例详情页。
5. 在已有监听器操作下的**配置管理**下拉列表，单击**管理终端节点组**，进入终端节点组列表页，对终端节点组进行管理。

删除监听器

1. 登录 全球加速控制台 。
2. 在实例列表页面，单击目标**实例 ID**，进入实例详情页。
3. 单击**监听器**，进入监听器列表页。
4. 单击监听器右侧的**删除**。
5. 在弹出提示框中单击**确定**，完成删除。

> **注意：**
> 删除监听器后，将释放组内所有监听和终端节点组的绑定关系，业务将不再进行加速，且删除后无法恢复和访问，请充分确认影响后再进行删除。

配置 HTTP 和 HTTPS 监听器

最近更新时间：2026-03-16 16:39:52

监听器概述

创建全球加速实例后，您需要为实例配置监听器。监听器负责监听客户端请求，并将流量分发至后端终端节点上。
全球加速监听器需配置：

1. 监听协议和监听端口。监听器的监听端口，亦被称为前端端口，用来接收请求并向后端服务器转发请求的端口。
2. 监听策略。如均衡策略、会话保持 等。
3. 添加终端节点组。需创建终端节点组并添加终端节点。

支持的协议类型

全球加速支持监听来自客户端的四层和七层请求，并将这些请求分发到后端终端节点上，而后由后端终端节点处理请求。四层和七层监听器的区别主要体现在：当用户请求到来时，是依据四层协议还是七层协议来进行转发流量，例如：对 TCP、UDP 等四层协议请求进行四层转发，对 HTTP、HTTPS 等七层协议请求进行七层转发。
四层协议：传输层协议，主要通过 VIP + Port 接收请求并分配流量到后端服务器。
七层协议：应用层协议，基于 URL、HTTP 头部等应用层信息进行流量分发。
腾讯云全球加速支持以下协议的请求转发：

- TCP（传输层）
- UDP（传输层）
- HTTP（应用层）
- HTTPS（应用层）

协议分类	协议	说明	应用场景
四层协议	TCP	面向连接的、可靠的传输层协议。 传输的源端和终端需先三次握手建立连接，再传输数据。 支持基于客户端 IP（源 IP）的会话保持。 支持获取客户端源IP。	适用于对可靠性和数据准确性要求高、对传输速度要求较低的场景，如文件传输、收发邮件、远程登录等。详情请参见 配置 TCP 和 UDP 监听器 。
	UDP	无连接的传输层协议。 传输的源端和终端不建立连接，不需维护连接状态。 每一条 UDP 连接都只能是点到点的。 支持一对一，一对多，多对一和多对多的交互通信。	适用于对传输效率要求高、对准确性要求相对较低的场景，如即时通讯、在线视频等。详情请参见 配置 TCP 和 UDP 监听器 。

		支持基于客户端 IP（源 IP）的会话保持。	
七层协议	HTTP	应用层协议。 支持基于请求域名和 URL 的转发。	需要对请求的内容进行识别的应用，例如 Web 应用、App 服务等。
	HTTPS	加密的应用层协议。 支持基于请求域名和 URL 的转发。 统一的证书管理服务，可在全球加速控制台完成证书上传及替换。 支持单向认证和双向认证。	需加密传输的 HTTP 应用。

支持的端口范围

端口类型	说明	限制
监听端口（前端端口）	监听端口是全球加速接收请求并向终端节点转发请求的端口。您可以配置的端口范围为1 - 65499。	在同一个全球加速实例内： UDP 类协议可以和 TCP 类协议的监听端口重复。例如，可以同时创建监听器 TCP:80 和监听器 UDP:80。 同一类协议下监听端口不可重复，TCP/TCP SSL/HTTP/HTTPS 同属于 TCP 类。例如，不可以同时创建监听器 TCP:80 和监听器 HTTP:80。
终端节点端口（后端端口）	七层监听器支持配置终端节点端口，终端节点端口是后端服务器提供服务的端口，接收并处理来自全球加速的流量。 您可以配置的终端节点端口范围为1 - 65499。	在同一个全球加速实例内： 不同监听协议的服务端口可以重复。例如，监听器 HTTP:80 和监听器 HTTPS:443 可以同时绑定同一台后端服务器的同一个端口。
健康检查端口	健康检查端口用于全球加速向后端服务器发送探测请求，以确认服务器是否正常运行。若端口响应正常，则认为服务器健康。您可以配置的终端节点端口范围为1 - 65499。	-

您需要为全球加速实例创建监听器，用于监听用户请求及将流量转发到后端终端节点，全球加速 GA 支持 TCP、UDP、HTTP 及 HTTPS 协议，本章节为您介绍 HTTP 及 HTTPS 监听器配置及操作指南。

操作步骤

前提条件

已完成 全球加速2.0实例创建 。

创建监听器

1. 登录 全球加速控制台 。
2. 在实例列表页面，单击目标**实例 ID**，进入实例详情页。
3. 单击监听器页签下的**添加监听器**。
4. 配置监听器。

配置类型	配置项	说明
基础配置	监听器名称	• 以大小写字母或中文开头 • 长度 2-128 字符 • 支持数字、英文句号 “.” 或短划线 “-” 、下划线 “_” 。
	路由类型	当前支持智能路由，GA2.0会根据时延选择最近终端节点组进行转发。
	协议	支持选择 TCP、UDP、HTTP、HTTPS • HTTP（超文本传输协议）：应用层协议，明文传输、无加密，适用于普通网页浏览、数据抓取等非敏感信息传输。 • HTTPS（安全超文本传输协议）：HTTP+SSL/TLS 加密，提供数据加密和身份认证，适用于在线支付、登录认证等需要安全传输的场景。
	端口	支持端口范围为 1-65499
	SSL 解析方式	HTTPS 监听器与客户端的认证方式。 • 单向认证：仅客户端验证服务端身份，服务端不验证客户端身份，选择该认证方式，仅需上传服务器证书到全球加速。 • 双向认证：客户端和服务端互相验证身份，客户端需提供证书供服务端验证。选择该认证方式时，需同时上传服务器证书及 CA 证书到全球加速。
	服务器证书	由 CA 机构颁发给网站的数字证书，用于验证服务器身份并建立加密连接。选择单向认证并完成上传后，全球加速会将该证书返回给客户端用于建立加密连接。

	客户端 CA 证书	由根 CA 或中间 CA 持有的证书，用于签发和验证服务器证书的合法性，上传后，全球加速将用该证书验证客户端的合法性。 **说明：** 仅在认证模式选择双向认证时需上传客户端 CA 证书。
	TLS 安全策略组	创建 HTTPS 监听器时支持按需选择不同 TLS 安全策略组（tls_policy_1.0-2、tls_policy_1.1-2、tls_policy_1.2、tls_policy_1.2_strict），不同策略组包含不同 TLS 版本及加密算法套件，详情可参见 TLS 安全策略组 。
高级配置	获取客户端源 IP	开启后，默认携带 X-Forwarded-For、X-Forwarded-Ip、X-Forwarded-Proto、X-Real-IP 字段。
	连接空闲超时时间	指定连接空闲超时时间。在超时时间内一直没有数据交互，全球加速会中断当前连接，直到下一次请求来临时重新建立新的连接。 • 默认值：15s。 • 配置范围：1-60s。
	连接请求超时时间	指定连接请求超时时间，客户端与服务器建立连接所需的最大等待时间，如果超过这个时间仍未建立连接，则认为连接请求超时。 • 默认值：60s。 • 配置范围：1s-180s。

5. 配置终端节点组

监听器创建时，您可以为监听器创建默认终端节点组，来承接监听器转发到后端的流量。配置终端节点组时，您需要为节点组添加终端节点并按需开启健康检查。

说明：
监听器首次创建时配置的节点组为默认终端节点组，HTTP/HTTPS 监听器支持创建自定义终端节点组。

配置类型	配置项	说明
终端节点组	节点组名称	• 以大小写字母或中文开头 • 长度 2-128 字符 • 支持数字、英文句号 “.” 或短划线 “-” 、下划线 “_” 。
	地域	终端节点组所在地域，全球加速会将来自加速区域的流量转发到终端节点组地域。

	注意： 如加速区域与终端节点组属于同一地域，可能导致加速效果不佳。
后端服务类型	终端节点是最终提供服务的后端源站，终端节点类型支持自定义域名及自定义 IP。
后端服务	最终提供服务的后端源站，您可为一个终端节点组最多添加4个终端节点，支持输入自定义 IP 或自定义域名。例如： • `117.89.1.1` • `example.com`
权重	终端节点权重，权重取值范围为：1-100。全球加速将按照您配置的终端节点权重来分发业务流量到后端服务器。
回源协议	全球加速回源到终端节点时所使用的协议。 • 监听协议为 HTTP：回源协议仅支持 HTTP。 • 监听协议为 HTTPS：回源协议支持选择 HTTP 或 HTTPS。
端口映射	支持配置监听端口与后端服务端口的映射关系。全球加速将根据配置转发数据包到终端节点对应端口。 • 监听端口：不支持修改，与监听器端口保持一致。 • 终端节点端口：支持修改配置范围为1-65499。
健康检查	• 开启：全球加速将按配置的健康检查参数来检查后端源站的可用性。 • 关闭：全球加速不对源站进行健康检查探测。
检查协议	全球加速用于检测后端服务器是否可用的网络协议，对于 HTTP 和 HTTPS 监听器，均只支持通过 HTTP 协议进行健康检查。
响应超时时间	全球加速向后端服务器发送健康检查请求后，等待服务器响应的最长时间。若超时未收到响应，则判定本次检查失败。 • 默认值：2s • 配置范围：2s-60s
健康检查间隔	两次健康检查之间的时间间隔。 • 默认值：30s • 配置范围：5s-300s
不健康阈值	连续健康检查失败的次数达到该阈值后，后端服务器被标记为不健康，并从流量分发池中移除。 • 默认值：3次

		• 配置范围：1次-10次
	健康阈值	连续健康检查成功的次数达到该阈值后，不健康的服务器被重新标记为健康并恢复流量分发。 • 默认值：3次 • 配置范围：1次-10次
	检查域名	指健康检查时请求的域名。
	检查路径	指定健康检查的 URL 路径（如/checkHealth），全球加速会向该路径发送 HTTP 请求，根据返回状态码判断服务是否健康。
	请求方式	支持 HEAD 或 GET 方法： • HEAD：仅请求响应头，轻量高效。 • GET：获取完整响应，适用于需检查内容完整性的场景。
	状态监测码	健康检查通过 HEAD 或 GET 请求访问指定路径（如/health），若返回状态码在预设范围内且未超时，则标记服务为健康，否则触发隔离机制，支持配置以下状态监测码： http_2xx、http_3xx、http_4xx、http_5xx。

相关文档

- 证书管理
- 转发策略
- TLS 安全策略组

终端节点组

最近更新时间：2026-03-16 16:39:52

概述

终端节点组（Endpoint Group）是指一组位于特定地域的终端节点（Endpoint）的集合，用于接收并处理通过腾讯云全球加速网络转发的客户端请求。其核心作用是将流量从加速入口（加速 IP）高效分发到后端服务（如 ECS、CLB 等），实现跨地域的低延迟访问。终端节点组的主要功能如下：

- 流量分发：全球加速监听器（Listener）根据路由规则（当前仅支持智能路由）将客户端请求转发到关联的终端节点组，再由终端节点组内的终端节点将请求送达后端服务。
- 地域关联：每个终端节点组绑定一个特定地域（如北京、上海），确保流量就近接入后端服务，减少网络延迟。
- 多节点容灾：一个终端节点组通常可添加至多4个终端节点，通过健康检查实现高可用，故障时自动切换。

> **说明：**
> 全球加速跨境段由中国联通代运营，如加速区域和终端节点组存在跨境，您的账号需要先通过 跨境资质审核 ，详情可参见 跨境云专线服务协议 。

终端节点组类型

终端节点组分为默认终端节点组及自定义终端节点组两种类型，首次创建监听器时创建的节点组即为默认终端节点组。

- 默认终端节点组：
  - TCP/UDP 监听：仅支持创建1个默认终端节点组，创建后将根据配置的健康检查策略将业务流量转发到健康的终端节点。
  - HTTP/HTTPS 监听：仅支持创建1个默认组。
- 自定义终端节点组：
  - 适用于HTTP/HTTPS监听，支持创建最多10个自定义节点组，可通过转发策略（如基于 URL）将部分流量定向到特定自定义节点组。

> **说明：**
> - 默认终端节点组创建后即绑定默认转发策略。
> - 仅 HTTP 和 HTTPS 监听器支持配置转发策略并绑定自定义终端节点组，详情可参见 转发策略 。

终端节点类型

终端节点（Endpoint）是指客户端请求最终到达并处理的后端服务实例，它是全球加速网络中将加速流量转发到实际业务服务器的代理节点。配置完成后全球加速通过公网将业务流量转发到终端节点。终端节点支持以下类型：

- 自定义公网 IP 地址

- 自定义域名

回源协议

回源协议是指全球加速将客户端请求转发到后端服务器（终端节点）时所使用的应用层协议。例如：客户端通过 HTTPS 访问负载均衡器，但负载均衡器回源时可能使用 HTTP。仅在七层监听器创建终端节点组时支持选择回源协议。

端口映射

端口映射是指全球加速服务在应用层（HTTP/HTTPS）将客户端请求的前端监听端口与后端服务器的实际服务端口进行关联和转发。

- 前端端口：客户端访问全球加速的端口（如80或443）。
- 后端端口：全球加速将请求转发到后端终端节点的端口（如8080或8443）。
- 映射关系：创建终端节点组时，通过配置端口映射将前端端口的请求定向到后端指定端口，实现协议转换或端口解耦。

> **说明：**
> 终端节点组配置端口映射时，监听端口需要与监听器端口保持一致，不支持修改。

健康检查

健康检查是全球加速服务中用于检测后端终端节点是否可用的机制。通过定期发送探测请求，判断后端服务的运行状态，确保流量只被分发到健康的节点，从而保障业务的高可用性。支持对终端节点组配置健康检查，详情可参见 配置HTTP和HTTPS监听器 。

相关文档

- 配置HTTP和HTTPS监听器
- 转发策略
- 证书管理

转发策略

最近更新时间：2026-03-16 16:39:52

概述

转发策略是指全球加速服务基于应用层（HTTP/HTTPS）的请求内容（如域名、URL 路径、请求头等）将流量智能分发到不同终端节点组的规则集合。您可通过创建转发策略并绑定自定义终端节点组，实现精细化的流量控制和路由。

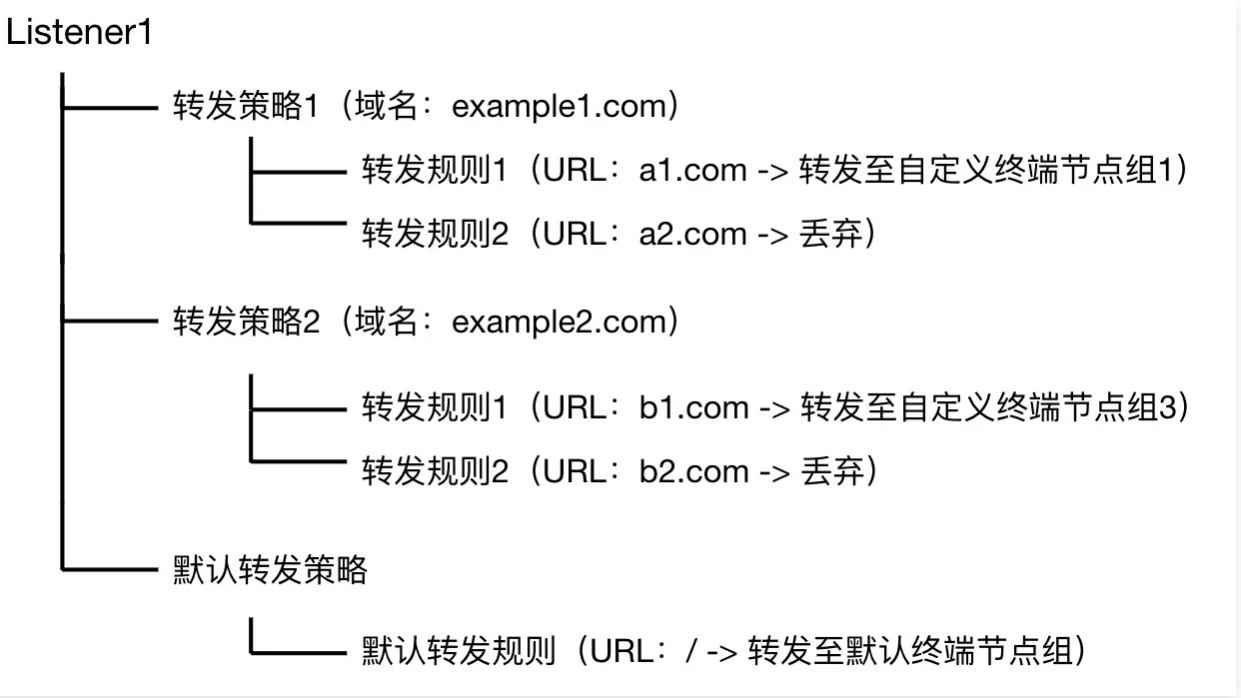
策略类型

转发策略类型包括默认策略与自定义策略：

- 默认策略：监听器创建时自动创建，与默认终端节点组自动关联，不支持编辑或者删除，且无法绑定其他自定义终端节点组。默认终端节点组删除后，默认策略将被联动删除。
- 自定义策略：用户可基于域名、路径定义精细化路由规则。自定义策略可绑定到自定义终端节点组实现流量分配，但无法绑定默认终端节点组。

策略组成

- 匹配域名：需要匹配的域名，一条转发策略对应一个域名匹配，基于域名添加匹配 URL。
- URL 路径：需要匹配的路径，一个域名下支持配置多条转发规则，一条转发规则对应一个 URL。
- 转发动作：命中转发策略后全球加速对应执行的策略动作，转发至策略绑定的自定义终端节点组或丢弃。
- 回源 HOST：全球加速向源站发起请求时，在 HTTP 头部 Host 字段中携带的域名标识，支持修改回源请求中的 HOST 字段，如不填写则使用默认 HOST。
- 回源 SNI：全球加速在 HTTPS 回源握手阶段告知源站请求的目标域名，仅 HTTPS 转发策略支持修改。



工作原理

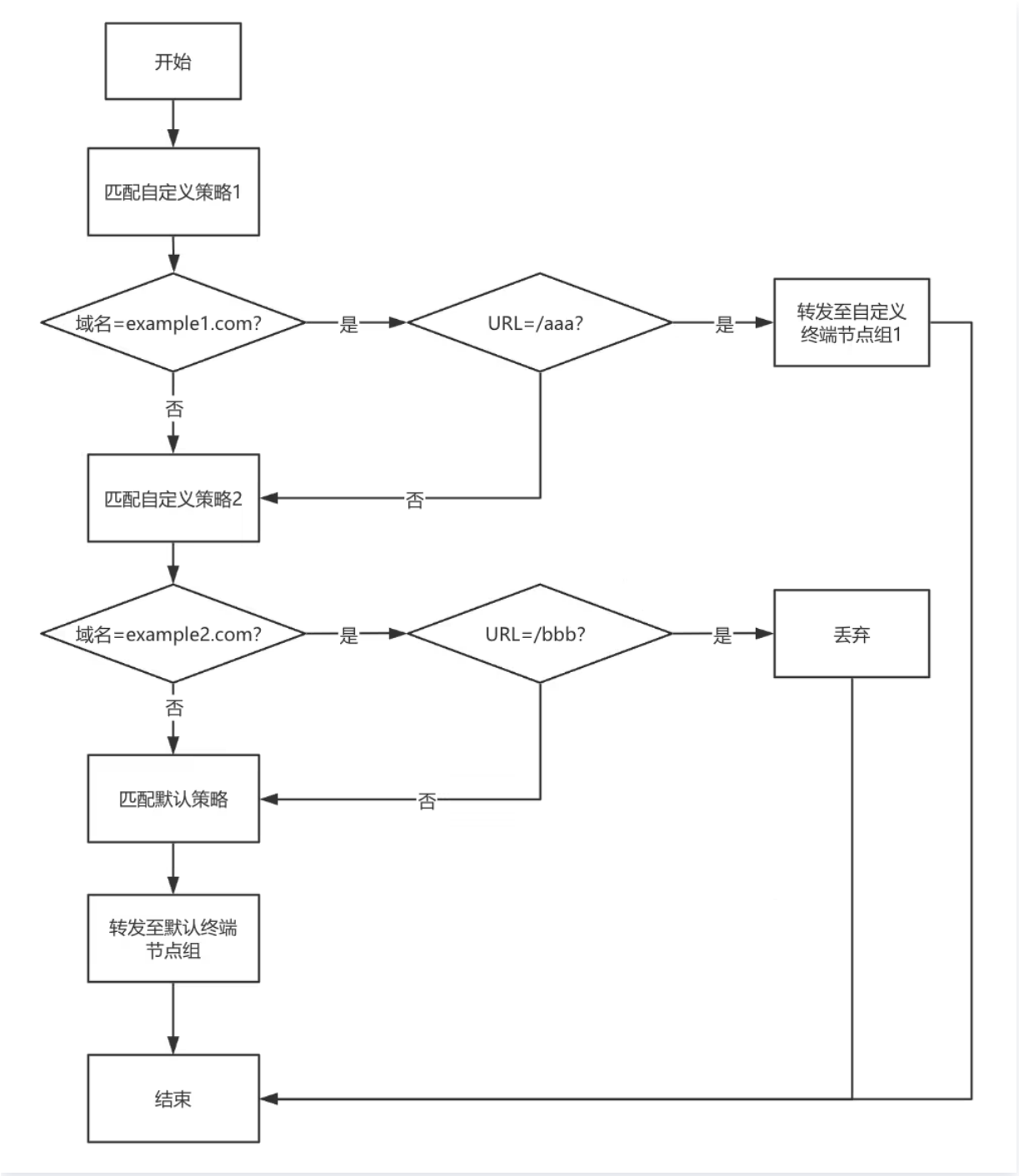
1. 请求解析

   全球加速节点接收用户请求后，解析 HTTP/HTTPS 头部、URL 路径、域名等信息。
2. 按优先级对自定义转发策略逐条匹配：

   条件组合：转发策略匹配条件包含域名+路径，需全部满足才会触发动作。
3. 动作执行

- 匹配成功：立即执行策略对应动作（转发至指定终端节点组或丢弃）。
- 匹配失败：继续匹配其余的自定义策略，如未匹配上任何自定义策略，最终按默认策略动作执行，将请求发送至默认终端节点组。

例如：
一个监听器下配置了两条自定义转发策略，自定义策略1匹配域名为 example1.com，匹配 URL 为/aaa，转发动作为 转发至自定义终端节点组1；自定义策略2匹配域名为 example2.com，匹配 URL 为/bbb，转发动作为 丢弃；则该监听器匹配流程如下：



配置转发策略

前提条件

已完成 全球加速实例创建 及 HTTP&HTTPS 监听器创建 。

操作步骤

1. 登录 全球加速控制台 。
2. 在实例列表页面，单击目标**实例 ID**，进入实例详情页。
3. 单击监听器页签下的**监听器 ID**，进入监听器详情页。

4. 单击**转发策略**进入转发策略页签，单击**添加 HTTP 转发策略**。
5. 在弹窗中输入希望匹配的域名。
6. 单击域名右侧的**添加转发规则**并按下表指引完成对应配置。

- **域名**：客户端访问加速服务时使用的域名（如www.example.com），全球加速会基于该域名匹配预设的转发规则。
- **URL**：转发路径，必填，长度1-80，支持字符集如下：a-z A-Z 0-9 _ . - /。全球加速会基于该域名+URL对业务流量进行精确匹配。
- **转发动作**：流量命中转发规则配置的域名及 URL 后，全球加速会执行对应的转发动作。
  - 转发至：将命中的流量转发至规则绑定的自定义终端节点组。
  - 丢弃：全球加速将丢弃命中规则的流量，不进行转发
- **回源 SNI**：当全球加速以 HTTPS 协议回源时，通过 SNI 在 TLS 握手阶段明确告知源站请求的目标域名，源站据此返回对应的SSL 证书。对命中规则的流量，支持修改回源请求中的 SNI 字段。

> **说明：**
> - 仅 HTTPS 监听器支持通过 HTTPS 协议回源。
> - 如配置了回源 SNI 的转发规则绑定到回源协议为 HTTP 的终端节点组，全球加速2.0将仍使用 HTTP 协议回源，此时 SNI 配置无实际使用意义。

- **回源 HOST**：全球加速向源站发起请求时，会在 HTTP 头部 Host 字段中携带域名标识。对命中规则的流量，支持修改回源请求中的 HOST 字段。如不填写则使用默认 HOST。
- **回源请求头**：支持在 HTTPS 转发规则中配置回源请求头，用于自定义全球加速向源站发起请求时携带的 HTTP 头部信息。

> **说明：**
> - HTTP 头部的名称 Key 值长度默认为1 - 20个字符，由数字0 - 9、字符a - z、A - Z，及特殊符 - _ : 空格 组成。Value 长度为1 - 100个字符。
> - 每条规则最多可配置10条回源 HTTP 请求头。
> - 部分标准头部不支持自助设置/增加/删除，即 Key 不允许配置的字段，具体清单请参见下表。

www-authenticate	authorization	proxy-authenticate	proxy-authorization	range	if-range	content-range	cross-origin-embedder-policy
age	cache-	clear-site-	expires	cross-	cross-	content-	content-

	control	data		origin-opener-policy	origin-resource-policy	security-policy	security-policy-report-only
pragma	warning	accept-ch	accept-ch-lifetime	expect-ct	feature-policy	strict-transport-security	upgrade-insecure-requests
early-data	content-dpr	dpr	device-memory	x-content-type-options	x-download-options	x-frame-options(xfo)	x-permitted-cross-domain-policies
save-data	viewport-width	width	last-modified	x-powered-by	x-xss-protection	public-key-pins	public-key-pins-report-only
etag	if-match	if-none-match	if-modified-since	sec-fetch-site	sec-fetch-mode	sec-fetch-user	sec-fetch-dest
if-unmodified-since	vary	connection	keep-alive	last-event-id	nel	ping-from	ping-to
accept	accept-charset	expect	max-forwards	report-to	transfer-encoding	te	trailer

access-control-allow-origin	access-control-max-age	access-control-allow-headers	access-control-allow-methods	sec-websocket-key	sec-websocket-extensions	sec-websocket-accept	sec-websocket-protocol
access-control-expose-headers	access-control-allow-credentials	access-control-request-headers	access-control-request-method	sec-websocket-version	accept-push-policy	accept-signature	alt-svc
origin	timing-allow-origin	dnt	tk	date	large-allocation	link	push-policy
content-disposition	content-length	content-type	content-encoding	retry-after	signature	signed-headers	server-timing
content-language	content-location	forwarded	x-forwarded-host	service-worker-allowed	sourcemap	upgrade	x-dns-prefetch-control
x-forwarded-proto	via	from	host	x-firefox-spdy	x-pingback	x-requested-with	x-robots-tag
referer-policy	allow	server	accept-ranges	x-ua-compatible	max-age	-	-

编辑转发策略

1. 登录 全球加速控制台 。
2. 在实例列表页面，单击目标**实例 ID**，进入实例详情页。
3. 单击监听器页签下的**监听器 ID**，进入监听器详情页。
4. 单击**转发策略**进入转发策略页签。
5. 单击已有规则右侧的**编辑转发规则**进行修改

删除转发策略

1. 登录 全球加速控制台 。
2. 在实例列表页面，单击目标**实例 ID**，进入实例详情页。
3. 单击监听器页签下的**监听器 ID**，进入监听器详情页。
4. 单击**转发策略**进入转发策略页签。
5. 单击已有规则右侧的**删除**进行删除。

> **说明：**
> 默认转发策略不支持编辑或删除，默认终端节点组删除后，默认策略联动删除，可通过再次创建默认终端节点组来恢复默认策略。

相关文档

- 配置 HTTP 和 HTTPS 监听器
- 证书管理

证书管理

最近更新时间：2026-03-16 16:39:52

概述

HTTPS 证书（也称为 SSL/TLS 证书）是一种由受信任的证书颁发机构（CA）签发的数字证书，用于验证网站身份并启用加密连接。它通过 SSL/TLS 协议在客户端（如浏览器）和服务器之间建立安全通道，确保数据传输的机密性（防止窃听）、完整性（防止篡改）和真实性（防止冒充）。证书包含网站的公钥、域名、颁发机构信息及有效期。使用全球加速创建 HTTPS 监听器时，您需要进行证书上传与管理。

认证模式

您可按需为全球加速监听器实例选择 HTTPS 认证模式，支持单向认证及双向认证，单向认证和双向认证的核心区别在于身份验证的方向和严格程度。

- 单向认证：仅客户端验证服务器身份，服务器不验证客户端，该认证模式下，您仅需上传服务器证书到全球加速。适用于普通网站浏览、电商平台等公开服务，用户无需预先配置证书。
- 双向认证：客户端和服务器互相验证身份，该认证模式下，您需同时上传服务器证书及客户端证书到全球加速。适用于企业内网、金融系统、医疗数据交换等高安全需求场景，仅允许持有合法证书的客户端访问。

对比项	单向认证	双向认证
验证方	仅客户端验证服务器	双方互相验证
客户端证书	不需要	必须配置
安全性	中等（防窃听、篡改）	更高（防冒充、中间人攻击）
复杂度	配置简单，仅需上传服务器证书	需上传服务器证书与客户端证书
典型应用	普通网站	银行系统、内部 API

证书类型

证书类型分为默认服务器证书、自定义服务器证书以及 CA 证书，仅在认证模式选择双向认证时需要上传和管理 CA 证书。

证书类型	说明
默认服务器证书	监听器创建时上传的服务器证书即为默认证书，当客户端请求未匹配上其他任何自定义服务器证书时，全球加速将返回默认证书用于 HTTPS 认证。 • 默认证书仅支持替换，不支持删除或添加。 • 一个 HTTPS 监听器有且仅有一本默认证书。

自定义服务器证书	当需要通过一个全球加速实例加速多个 HTTPS 域名时，可为监听器添加多个自定义证书，每个证书对应不同域名。 **说明：** 自定义证书支持替换，所替换的新证书域名需与老证书域名保持一致，否则无法完成替换。
CA 证书	认证模式选择双向认证时，除服务器证书外，还需要上传 CA 证书，用于验证客户端身份的合法性。 • CA 证书支持替换，不支持删除或添加。 • 一个 HTTPS 监听器有且仅有一本 CA 证书。

关联域名

全球加速支持单个 HTTPS 监听器下添加多个域名证书，实现多域名加速时的灵活管理。在添加自定义服务器证书时，您需要创建证书与域名的关联关系，关联后，全球加速将根据客户端请求域名返回对应证书，如没有匹配到任何自定义证书包含的域名，将返回默认证书。

上传证书

前提条件

已完成 全球加速实例创建 及 HTTPS 监听器创建 。

操作步骤

1. 登录 全球加速控制台 。
2. 在实例列表页面，单击目标**实例 ID**，进入实例详情页。
3. 单击监听器页签下的**监听器 ID**，进入监听器详情页。
4. 单击**证书管理**，进入证书管理页签。
5. 单击**添加证书**，在弹窗中完成添加配置。

配置项	说明
证书类型	所添加的证书类型，仅支持添加自定义服务器证书。
服务器证书	选择所需添加的证书，您可在 SSL 控制台 对证书进行统一管理。
关联域名	服务器证书包含的域名，全球加速根据客户端请求域名返回对应证书。

替换证书

1. 登录 全球加速控制台 。
2. 在实例列表页面，单击目标**实例 ID**，进入实例详情页。
3. 单击监听器页签下的**监听器 ID**，进入监听器详情页。
4. 单击**证书管理**，进入证书管理页签。
5. 单击已有证书右侧的**更换证书**，进行证书替换。

> **说明：**
> 自定义服务器证书替换时，所替换的新证书域名需与老证书域名保持一致，否则无法完成替换。默认证书及 CA 证书替换时，无需域名一致。

删除证书

1. 登录 全球加速控制台 。
2. 在实例列表页面，单击目标**实例 ID**，进入实例详情页。
3. 单击监听器页签下的**监听器 ID**，进入监听器详情页。
4. 单击**证书管理**，进入证书管理页签。
5. 单击已有自定义服务器证书右侧的**删除**。
6. 在弹窗中，单击**确定**，完成删除。

> **说明：**
> 默认证书不支持删除。

相关文档

- 配置HTTP和HTTPS监听器

访问控制

最近更新时间：2026-03-16 16:39:52

概述

全球加速支持通过设置安全访问策略，对加速实例进行外网访问权限控制，提高网络访问的安全性。可通过来源IP、协议、端口对流量进行访问限制。

- 全球加速默认不对客户端流量进行防控，需在访问控制页签开启该功能。
- 功能开启需选择默认处理策略，准许或拒绝全部流量进入全球加速实例，并通过访问规则进一步控制。

创建访问控制

前提条件

已完成全球加速实例创建。

创建访问控制策略

1. 登录 全球加速控制台 。
2. 在实例列表页面，单击目标**实例 ID**，进入实例详情页。
3. 单击**访问控制**页签，进入访问控制配置页。
4. 单击**创建访问控制**，选择默认处理策略，完成访问控制策略的创建。
5. 单击**状态**开关，启用控制策略。

创建访问规则

1. 登录 全球加速控制台 。
2. 在实例列表页面，单击目标**实例 ID**，进入实例详情页。
3. 单击**访问控制**页签，进入访问控制配置页。
4. 单击**添加规则**，在弹窗中对访问规则进行配置。

配置项	说明
来源 IP	客户端流量源 IP，来源支持以下格式 • 单个 IP: 192.168.0.1 • CIDR: 192.168.1.0/24
协议	客户端来源协议，支持 TCP、UDP。
协议端口	来源协议端口，支持以下格式 • 单个端口: 80 • 多个端口: 80,443

	• 连续端口: 3306-20000 • 所有端口: ALL
策略	允许：全球加速放通命中规则的流量。 拒绝：全球加速将拒绝命中规则的流量访问。
备注	规则备注，非必填。

5. 单击**确定**，完成规则配置。

编辑规则

1. 登录 全球加速控制台 。
2. 在实例列表页面，单击目标**实例 ID**，进入实例详情页。
3. 单击监听器页签下的**访问控制**，进入访问控制配置页。
4. 在已有规则右侧，单击**编辑**。
5. 在弹窗中完成对应配置，单击**确定**，完成编辑。

删除规则

1. 登录 全球加速控制台 。
2. 在实例列表页面，单击目标**实例 ID**，进入实例详情页。
3. 单击监听器页签下的**访问控制**，进入访问控制配置页。
4. 选中需要删除的规则，单击**删除**。
5. 在弹窗中单击**确定**，完成删除。

删除访问控制策略

1. 登录 全球加速控制台 。
2. 在实例列表页面，单击目标**实例 ID**，进入实例详情页。
3. 单击监听器页签下的**访问控制**，进入访问控制配置页。
4. 单击访问安全控制右侧的**删除**，并点击弹窗中的**确定**，完成删除。

> **注意：**
> 策略删除后，全部访问规则也会对应删除，全球加速将不再对业务进行访问控制，请充分确认影响后再操作。

TLS安全策略组

最近更新时间：2026-03-16 16:39:52

概述

TLS（Transport Layer Security）是一种用于保障网络通信安全的加密协议，其前身是 SSL（Secure Sockets Layer）。TLS 通过加密、身份验证和数据完整性保护，确保客户端（如浏览器）与服务器之间的数据传输不被窃听或篡改。它广泛应用于 HTTPS、电子邮件、VPN 等场景，是互联网保密通信的工业标准。TLS 协议经历了多个版本的迭代，每个版本在安全性和性能上有所改进：

- TLS 1.0（1999年）：首个版本，基于 SSL 3.0，但存在安全漏洞（如易受 BEAST 攻击），已逐渐被弃用。
- TLS 1.1（2006年）：修复了 TLS 1.0的部分漏洞，但仍使用较弱的加密算法（如 SHA-1），目前也不推荐使用。
- TLS 1.2（2008年）：主流版本，支持更强的加密算法（如 AES-GCM、SHA-256），提供更好的安全性和效率。
- TLS 1.3（2018年）：最新版本，简化握手流程（减少延迟）、移除不安全算法（如 RC4），并强制使用前向保密（PFS），安全性最高。

密码套件是 TLS 握手时协商的一组算法组合，用于定义加密、身份验证和密钥交换方式。创建 HTTPS 监听器时支持按需选择 TLS 安全策略组，不同安全策略组对 TLS 版本、加密套件包的支持度不同。详情如下：

TLS 安全策略组	支持 TLS 版本	支持加密算法套件
tls_policy_1.0-2	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_policy_1.1-2	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_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_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_policy_1.2_strict-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

相关文档

配置 HTTP 和 HTTPS 监听器。