

全球应用加速

操作指南

产品文档





【版权声明】

©2013-2024 腾讯云版权所有

本文档著作权归腾讯云单独所有,未经腾讯云事先书面许可,任何主体不得以任何形式复制、修改、抄袭、传播全部或部分本文档内容。

【商标声明】



及其它腾讯云服务相关的商标均为腾讯云计算(北京)有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标,依法由权利人所有。

【服务声明】

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况,部分产品、服务的内容可能有所调整。您 所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定,除非双方另有约定,否则, 腾讯云对本文档内容不做任何明示或默示的承诺或保证。



文档目录

操作指南

源站管理

接入管理

通道管理(跨境通道)

TCP/UDP 监听器管理

HTTP/HTTPS 监听器管理

安全防护

访问加速通道

通道组管理

统计数据

配置权限

接入腾讯云可观测平台

证书管理

获取访问用户真实 IP

通过 TOA 获取客户端真实 IP(仅针对 TCP 协议)

基本原理

Linux 后端版本调用

步骤一:创建 TCP 监听器并开启 TOA

步骤二:后端服务加载 TOA 模块

步骤三:(可选)查看 TOA 相关的计数状态:

查看 Client IP

常见问题

Windows 后端版本调用

步骤一:创建 TCP 监听器并开启 TOA

步骤二:后端服务加载 TOA 模块

步骤三:使用方法

通过 Proxy Protocol 获取客户端真实 IP(仅针对 TCP 协议)

基本原理

操作步骤

通过 HTTP 请求头获取客户端真实 IP(支持 HTTP/HTTPS 协议)

基本原理

操作步骤

国家与地区映射关系





操作指南 源站管理

最近更新时间:2021-12-10 11:04:29

增加源站

登录 全球应用加速控制台,在"源站管理"页面,单击**新增**,将所有要加速访问的服务器信息添加进来,可填写源站 IP或域名,源站 IP 可支持 IPv4 和 IPv6,多个源站用回车分隔。



Origin Sei	rver Management	All Projects	
Add	Delete		
	Add an origin	×	
	Projects	Default Project 💌	
rs-2	Name	test	
 rs-1 rs-1 rs-2 	Origin IP/Domain name	118.89.5 www.trot.com	
rs-o		Enter multiple public IPs or domain names, one per line	
rs-o	Tag	Tag key Tag value Operation	
T-1-17 ()		No contents found	
		Add	
		OK Cancel	

删除源站

登录 全球应用加速控制台,在"源站管理"页面,选中待删除的源站,单击删除。

注意:

如待删除源站已与现有通道进行绑定,请先进行解绑操作。



Add Delete			Se	eparate keywords with
✓ ID	Name	Origin IP/Domain name	Projects	Operation
r s-ijtl4909	Demo 🧨	demo.com	DEFAULT PROJECT	Edit tag 🎤
Total items: 1			20 🔻 / page 🛛 🗐 🚽	1 / 1 page ▶ ▶

修改名称

1. 登录 全球应用加速控制台,在"源站管理"页面,单击源站名称旁的编辑图标,对源站名称进行编辑。

✓ ID	Name	Origin IP/Domain name	Projects	Operation
v rs-ijtl4909	Dem <mark>e 💉</mark>	demo.com	DEFAULT PROJECT	Edit tag 🌶

2. 在弹出框中,填写新的源站名字,单击确定即可。

Modify Name	1		×
Origin Name	Demo1		
	ОК	Cancel	

查看源站健康状态

1. 登录 全球应用加速控制台,在"源站管理"页面,单击健康状态下的统计图标。

注意:	
如源站尚未绑定监听	器,则无法使用该功能。



D	Name	Health Status	Origin IP/Domain name
rs-mms7k7ct	10° 187 🎤	di	10* 187

2. 在右上角的弹出框, 查看不同时间范围/粒度的源站健康状态, 1代表正常, 0代表异常。

me Period	Today	Yesterday	Last 7 Days	Last 15 days	Last 30 Days	
	2021-09-12	2 ~ 2021-09-26	⊟			
me Granularity	1 hour		•			
Origin Serve	er Health Sta	atus				Ļ
1: Normal; 0: A	Abnormal					
1.25						
1						_
it atus						 -
alth Status 0.22						-
/er Health Status 2.2.0						-
n Server Health Status 2.20 2.20						_
Origin Server Health Status 0.22						
0.rigin Server Health Status 0.5.0 0.22						
0.1gin Server Health Status 0.5.0	·Port 1223	33 2021-09-14	11:0			

编辑标签

1. 登录 全球应用加速控制台,在"源站管理"页面,单击编辑标签。

D	Name	Health Status	Origin IP/Domain name	Project	Operation
rs-mms7k7ct	101.0 10 107	di	101 14 1	DEFAULT PROJECT	<u>Edit Tag</u>





🔗 腾讯云

un lags				
he tag is used to n loes not meet your	nanage resources requirements, p	by category from di lease go to Manage	fferent dimensions. Tags 🔼	If the existing tag
l resource selected				
test	•	123	•	×
- Add				
		OK Cance		



接入管理 通道管理(跨境通道)

最近更新时间:2022-03-16 18:16:01

新增通道

1. 登录 全球应用加速控制台,进入"接入管理"页面,单击新增。



2. 在弹出的窗口中,填写通道信息。

Access N	All Projects			
Add	Add a connection			×
	Projects	Default Project	•	s
Total() its	Connection Name	Please enter the co You can enter 30 cha	nnection name	
	Origin Region	Please select Region of RS	•	
	Acceleration Region	Please select Region of Client	•	
	Bandwidth Cap	Please select	v	
	Max concurrent connections	Please select Maximum number o	▼ f concurrent connections	
	Tag	Tag key	Tag value	Operation
			No contents found	
		Add		
		ОК	Cancel	

- 项目:该通道所属项目(后续可以更换项目)。
- 通道名称:最多30个字符,支持中英文、常规符号。
- IP版本:可根据需要选择 IPv4 或 IPv6,其中 IPv6 暂时只支持中国大陆区域。
- HTTP3特性: 启用后,通道支持HTTP3(QUIC)协议传输,仅支持配置HTTP/HTTPS监听器(通道创建成功 后,暂不支持变更**启用/关闭**)。



• 接入节点:选择客户端所在区域或距离客户端最近区域的节点。

注意:

- 。若您需要提供中国香港的精品 BGP 网络接入,请在"接入节点"选择"香港",选择"Dedicated BGP"。
- 中国大陆提供三网节点网络,如有需要,可通过工单联系我们。
- 回源节点:选择目标服务器所在区域或距离目标服务器最近区域的节点。

注意: 中国台湾无法与中国大陆进行直连。

- 带宽上限:通道的带宽上限,最大值10000Mbps(部分通道最大值为1000Mbps)。
- 并发上限:通道的最大并发连接数,最大值100万(部分通道最大值为30万)。
- 标签:非必填项,可通过设置标签实现对通道的分类管理;
- 费用:根据您选择的带宽与并发数,下方会给出相应的通道费和带宽费。
 a.通道费:按日计算,直到通道被删除为止,请特别注意通道创建后未满一天删除也会按一天计费;
 b.带宽费:按每日实际出入带宽峰值计费。

3. 单击确定,完成新增通道。

4. 在"接入管理"页面中, 查看通道列表信息。

Acces	Guide of GAAP 🖄											
Add	Enable Disable	e Change Project	Delete									
	ID/Channel Name	Projects	VIP	Domain Name(i)	Acceleration	Origin Region	Bandwidth	Conc	Status	Billing Mode	Operation	
	link	Default Project	1176	link apqcl	China (Hong	Japan (Tokyo)	10 Mb	20 K	Enabled	Postpaid	Set	
	link gn	Default Project	118 206	link-user gn.gaapqc Domain Nan	East China	China (Hong	20 Mb	20 K	Enabled	Postpaid	Set	
Total2	items			III K	.gaapqcioud.com			Lines per	page: 20	r II II	↓ × × ×	

- ID/通道名:通道的 ID 和名字,其中通道名可以修改。
- 。 VIP:用于客户端访问的接入 IP 地址。
- 。 域名:用于客户端访问的接入域名(系统分配, 且自动绑定到 VIP)。
- · 状态: 仅"运行中"状态下,加速通道才可以正常使用。



查看通道信息

1. 登录 全球应用加速控制台,进入"接入管理"页面,单击指定通道的 ID/通道名,进入下一级页面。

ID/Connection Name	IP Ver Y	VIP	Domain Name 🛈	Accelerator 🔻	Origin Region 🔻	Bandwidth 🗘	Concur \$	Status Y	Billing Mode	Project	Operation
link tro5	IPv4	5	apqcloud.co	Norway East (Oslo, Partner IDC)	Eastern US (Virginia, Partner IDC)	1000 Mb	20 k	Running	Bill by Bandwidth	DEFAULT PROJECT	Modify Configuration Copy

 在"通道信息"标签页,可以查看通道的详细信息。其中,"转发 IP"是指加速通道末端的转发节点 IP,该转发节点 负责将加速通道的数据通过公网转发给源站。如果您希望多条通道使用同一个域名,可单击未关联跳转至 统一域 名页面进行配置。

Channel Detail	s ()	
Channel Info TCP/	UDP listener management	HTTP/HTTPS listener management
Channel ID	link7	
Channel Name	-	
VIP	11. 6	
Domain Name	link- jaapqcloud.com	
Acceleration Region	China (Hong Kong)	
Origin Region	Japan (Tokyo)	
Bandwidth Cap	10 Mb	
Concurrent connections	20 K	
Forwarding server IP	169. 166;169.5 147;	
Creation Time	2018/06/29 12:39:58	
Project	Default Project	

TCP/UDP 监听器管理

最近更新时间:2023-06-07 15:00:50

新增 TCP/UDP 监听器

1. 登录全球应用加速控制台,进入"接入管理"页面,单击指定通道的 ID/通道名。

2. 进入下一级页面,选择TCP / UDP 监听器管理 > 新建,具体配置如下:

i. 配置监听器信息,用于设置加速协议和端口映射关系。

1 Listener	Info > 2 Configure the Policy	> 3 Origin Health Chee Policy	ck
4 Session	Persistence		
Listener Name	Please enter the listener name		
Origin Type	IP Address 💌		
Protocol	TCP		
Get client IP 🛈	O TOA O Proxy Protocol		
Listening Port	Listening Port 🛈	Operation	
	Enter a listening port	Delete	
	Add Port		



- 源站类型:可以填写 IP 地址或域名,但同一个监听器只支持一种类型。(备注:IPv6通道暂不支持域名类型)
- 获取客户端IP:可选择 TOA 或 Proxy Protocol 两种获取客户端 IP 的方法获取真实用户 IP,具体介绍可参考 获取访问用户真实 IP 页面。
- 监听端口:指加速通道 VIP 的访问端口。端口规范:有效范围1-64999(21端口暂不开放)。支持单个端口或连续端口范围,但端口不能重复,一次最多添加的连续端口20个,如8000-8019。
- ii. 配置源站处理策略。即在同一个监听器绑定多个源站的情况下,选择源站之间的调度策略。

Listener Info	Configure the Policy Configure	>
4 Session Persiste	ence	
Policy	ORR() ○ Weighted RR() ○ Least Connections() ○ Least Latency()	

- 轮询:多个源站按轮询策略回源。
- 轮询加权:多个源站按权重比例回源(可以在绑定监听器时设置各源站的权重)。
- 最小连接数:在所有源站中选择连接数最小的源站优先进行调度。
- 最小时延:选择时延最小的源站优先进行调度。
- 备源:选择是否开启主备源切换(开启该功能会强制要求开启源站健康检查)。

注意:

源站类型为域名的监听器, 仅支持"轮询"及"最小连接数"两种调度策, 暂不支持备源。

iii. 如果使用 TCP 监听器,则可以选择配置健康检查机制,帮助您自动检查并移除异常的源站, 启用备源则无法关闭健康检查。



• 响应超时时间:指源站响应的超时时间。

巻田六

- 健康检查间隔:指前后两次健康检查的时间间隔。
- 不健康阈值:表示监听器连续检查失败多少次后确定源站不健康。当健康检查判断源站不健康时,将不再向 该源站转发数据包,直至该源站健康检查状态恢复正常。
- 健康阈值:表示监听器连续检查成功多少次后确定源站健康。当健康检查判断源站健康时,将重新向该源站 转发数据包。



iv. 选择是否开启会话保持功能。

Cistener lı	nfo >	Configure the Policy	> 🕑	Origin Health Check Policy	>
4 Session Persistence	(i)				
Hold Time 🛈			0	- 2829	+ seconds

- 会话保持:来自同一IP的用户请求保持访问相同源站。
- 保持时间:会话保持的时间。当监听器无请求的持续时间超过保持时间,将会自动断开会话保持。

3. 单击完成,成功新建 TCP/UDP 监听器。

设置TCP/UDP 监听器

单击 TCP/UDP 监听器管理标签页,在操作栏单击设置可以修改监听器名字、调度策略和健康检查参数等。

源站绑定

1. 单击 **TCP/UDP 监听器管理**标签页,选择已建立的 "TCP/UDP监听器"。在操作栏单击**源站绑定**,您可选择多个源 站进行绑定或解绑。如果控制台显示未找到源站信息,可能是由于源站类型不匹配或源站未添加在 源站管理中。



TCP Listeners							
Create Delete Delete ID/Listener Name	Protocol	Listening Port	Bound Origin Server	Origin Type	Service status	Session Persistence	Listening Port/Lister Q Operation
listener-6owz8im1 test	ТСР	-	1(3	IP Address	Normal (j)	Disabled	Set Bind Origin Servers Delete
Total items: 1						20 💌 / page	H 4 1 /1 page 🕨 H

- 2. 选择源站,并配置回源端口。
 - 如果监听器开启主备轮询选项,则需要在源站绑定页面设置"主源站"与"备源站"。
 - 如果您希望对多个源站的端口进行设定,可使用右上角"覆盖端口/补齐端口"功能。无论您之前设定的源站端口 为多少,"覆盖端口"功能都会将您选择的目标源站统一设定为您输入的端口。如果选定的目标源站中存在未设 定端口的情况,您可使用"补齐端口"功能进行统一设定,减少您的重复工作量。
 - 如果监听器策略为"加权轮询",则可以在绑定的同时设置源站的权重,范围1-100,按权重值占总权重的比例 进行调度,如源站1的权重为60,源站2的权重为80,则源站1的调度比例为 60 / (60 + 80) = 42.8%,源站2的调 度比例为57.2%。

	IP/Domain name	Name				
			Primary/S ⁴	econ Real	Ser Weight	
	10		Deine and	- 22	1	0
	R	test	Primary	25		0
	11	test	Primary	22	1	8
↔						
	\leftrightarrow	10 1 [*] ↔	10 test 11 test ↔	10 test Primary 1 11 test Primary 1	10 test Primary ▼ 23 11 test Primary ▼ 22	10 test Primary ▼ 23 1 11 test Primary ▼ 22 1

 如果您开启了健康检查,绑定源站后,健康检查即开始启动。可以通过监听器的状态来判断源站是否正常,加 速通道只会向正常状态的源站进行数据包转发,异常的源站将不再转发数据包,直至该异常源站健康检查状态 恢复正常后才重新转发。



• 如果您未开启健康检查或使用UDP协议监听器,那么不论源站的状态如何,加速通道将始终做数据包转发。

Origin Type	Service status	Session Persistence	Operation
IP Address	Abnormal	Disabled	Set Bind Origin Servers Delete
		20 💌 / page	I /1 page ►

3. 配置确认

源站配置完成后点击下一步到配置确认页面,用户可以查看当前配置的归属通道信息以及监听器详细信息。

Connection ID ink-cb Listener ID listener-ID listener-ID <thlistener-id< th=""> listener-ID</thlistener-id<>	nection Info		Listener Info					
Connection Name test /IP 12 Domain Inining apqcloud.com Accelerator Region Beijing (Former North China) Drigin Region Beijing (Former North China) Dingin Region Beijing (Former North China) Concurrent Connections 20 k Concurrent Connections 20 k Dingin Server IP® 192 Origin Type 192 Origin Type 192 Origin Server IP® 192 Diffed Domain Name 192 Origin Type 192 Origin Server IP® 192 Origin Type 192 Origin Type 192 Origin Server IP® 192 Origin Type 11 Real 1 Arous Diffed Domain Name Name Prime Real Origin Server IP® 1 Opic 1 Treation Time 021/0 Origin Type 1	onnection ID	link-cb	Listener ID	listener-				
IP 12 Protocol TCP omain In apqcloud.com Listening Port 1 occelerator Region Beijing (Former North China) Origin Type IP Address andwidth Cap 10 Mb Get client IP TOA oncurrent Connection 20 k Secondary Origin Server Bable origing Server IP® 19 10 Secondary Origin Server orogict DefAULT PROJECT Bound Origin Server IP/Domain name Name Prim. Real	onnection Name	tes'	Listener Name	test				
Image: selected of Region Beijing (Former North China) Listening Port 1 igin Region Beijing (Former North China) Origin Type IP Address igin Region Beijing (Former North China) Get Client IP TOA indwidth Cap 10 Mb Configure the Policy RR incurrent Connections 20 k Secondary Origin Server Enable infied Domain Name () No associated Origin Server Health Check IP/Domain name Name Prin Real oject DEFAULT PROJECT BETAULT PROJECT Second ary I Itest Second ary ary Second ary	p	12	Protocol	ТСР				
celerator Region Beijing (Former North China) Origin Type IP Address igin Region Beijing (Former North China) Get Client IP TOA ndwidth Cap 10 Mb Configure the Policy RR ncurrent Connections 20 k Secondary Origin Server Enable iffied Domain Name ① No associated Origin Server Health Check Enable warding Server IP ① 192 10; Bound Origin Server oject DEFAULT PROJECT Frim. Real	main	lin apqcloud.com	Listening Port	1				
igin Region Beijing (Former North China) Get client IP TOA ndwidth Cap 10 Mb Configure the Policy RR ncurrent Connections 20 k Secondary Origin Server Enable ified Domain Name ③ No associated Origin Server Health Check Enable warding Server IP ④ 192 10; Bound Origin Server oject DEFAULT PROJECT Frim Real	celerator Region	Beijing (Former North China)	Origin Type	IP Address				
Individit Cap 10 Mb Configure the Policy RR Incurrent Connections 20 k Secondary Origin Server Enable ified Domain Name () No associated Origin Server Health Check Enable warding Server IP() 192 10; Bound Origin Server oject DEFAULT PROJECT Frim Real	igin Region	Beijing (Former North China)	Get client IP	TOA				
Instrument Connections 20 k Secondary Origin Server Enable Ified Domain Name () No associated Origin Server Health Check Enable warding Server IP () 192 10; Bound Origin Server tation Time 2021/C 16 8 oject DEFAULT PROJECT Test Second ary	ndwidth Cap	10 Mb	Configure the Policy	RR				
Instrume No associated Origin Server Health Check Enable warding Server IP() 192 40; Bound Origin Server warding Server IP() 192 40; Bound Origin Server warding Server IP() 16 8 Bound Origin Server warding Server IP() DEFAULT PROJECT 1 test Second ary	ncurrent Connections	20 k	Secondary Origin Server	Enable				
warding Server IP ① 192 40; eation Time 2021/C 16 8 bject DEFAULT PROJECT DEFAULT PROJECT 11 test Second ary 8	ified Domain Name 🛈	No associated	Origin Server Health Check	Enable				
eation Time 2021/C 16 8 oject DEFAULT PROJECT 1 test Second ary 8	rwarding Server IP🛈	192 40;	Bound Origin Server	10/0		. ·		147 -
oject DEFAULT PROJECT 1' test Second ary 8	eation Time	2021/0 18 8		IP/Domain name	Name	Prim	Keal	vvei
	oject 9	DEFAULT PROJECT		17	test	Second ary	8	1
10 test Primar 12 y 12				10	test	Primar y	12	1

4. 单击完成,成功绑定源站。

删除TCP/UDP 监听器

单击 **TCP/UDP 监听器管理**标签页,在操作栏单击**删除**,可以删除指定的监听器,若监听器已绑定源站,则需要选中"允许强制删除绑定有源站的监听器"后,才能删除。删除后,该监听器的端口将停止加速。



Confirm to the delete the listenertest (listener-6owz8im1)?
Allow force deletion of listeners bound with origin server
Confirm Cancel



HTTP/HTTPS 监听器管理

最近更新时间:2023-06-07 17:22:45

新增 HTTP/HTTPS 监听器

- 1. 登录 全球应用加速控制台,进入"接入管理"页面,单击指定通道的ID/通道名。
- 2. 进入到下一级页面,选择 **HTTP/HTTPS 监听器管理 > 新增**,可选的协议有 HTTP 和 HTTPS(备注: IPv6 通道 当前不支持 HTTP/HTTPS 监听器配置)。
- 3. 具体配置如下:
 - i. 当选中 HTTP 时, 仅需要输入监听端口即可, 监听器会默认按照 HTTP 协议进行转发。

Create a lister	er	×
Listener Name		
Protocol	HTTP	
Source port	80 Valid range: 1-64999 (21the port is unavailable)	
	OK Cancel	



ii. 当选中 HTTPS 时,则需要额外配置证书和其他信息,如下图:

Create a listene	· :	×
Listener Name		
Protocol	HTTPS 💌	
	 Listeners communicate with the origin server using HTTP protoco Listeners communicate with the origin server using HTTPS protocol Disteners communicate with the origin server using HTTPS protocol 	
Source port	443	
	Value range: 1 - 64999 (21the port is unavailable)	
SSL Parsing	One-way authentication 🔹	
Server certificate	Please select 💌	
	Upload certificate	
Note: If you upload new certificate. If no certifica certificate uploaded	a new certificate while setting listener rules, the domain name will use the te is uploaded when setting the listener rule, the domain name will use the here.	e ne
	OK Cancel	

- "监听器与源站之间使用 HTTP 协议",指客户端到加速通道 VIP 之间使用 HTTPS 协议,而 VIP 到源站之间 使用 HTTP 协议,需要源站开通HTTP协议端口;
 "监听器与源站之间使用 HTTPS 协议",指客户端到源站之间全程使用 HTTPS 协议,需要源站开通 HTTPS 协议端口。
- SSL 解析方式:支持单向认证、双向认证。
- 服务器证书/客户端证书:需要在全球应用加速控制台的证书管理上传/更新,然后在新建/修改 HTTPS 监听器时从下拉列表中选择对应的证书,详见证书管理。

设置HTTP/HTTPS 监听器

单击 HTTP/HTTPS 监听器管理标签页,在操作栏单击设置规则,可以进入下一级页面,进行域名和 URL 管理。



添加域名

1.为HTTP监听器添加域名只需直接输入域名即可,但须符合域名格式要求,且只支持精确匹配。监听器支持的字符 集有: a-z、0-9、.、-,长度3 - 80。

Create a Di	stribution		×
Domain 🕄]
	Confirm	Cancel	

2. 为 HTTPS 监听器添加域名需输入域名并选择对应服务器证书

Create a Distribu	ution ×
Domain Name	
SSL Phrasing	One-way Authentication
Server Certificate	Default certificate (listener certit 💌
	Upload Certificate
HTTP3 Transfer 🛈	O Disable C Enable
Note: if a certificate can use it directly ar new certificate here,	was uploaded when you created the listener, you nd don't need to upload again. If you upload a the domain name will use the new certificate.
	OK Cancel

- 。 域名:需要符合域名的格式要求,只支持精确匹配,支持字符集如下,长度3-80个字符:a-z 0-9.
- 服务器证书:默认使用创建监听器时选择的证书。如您在此处重新上传证书,则该域名将使用新证书进行认证
- HTTP3 传输:点击**开启**后,支持通过 HTTP3(QUIC)访问,若客户端不支持 HTTP3,规则自动降级为 HTTP2.0 及以下协议访问

添加规则



完成"添加域名"操作后,单击**添加规则**,可以添加对应URL及选择源站类型。同一个域名下可以添加最多20条 URL 规则,具体如下:

1. 基本配置:

1 Basic Conf	iguration >	2 Configure the Policy >	×
3 Origin Hea Policy	lth Check		
Domain name(i)	www.com		
URL	/		
Origin Domain(i)	www com		
Origin Type	IP	v	
		Cancel Next	

- URL:支持字符集如下, a-z、A-Z、0-9、_、.、-、/,长度1 80。
- 。 回源Host:支持修改回源请求中的HOST字段。
- 源站类型:支持 IP 和域名两种类型, 但同一个监听器只支持一种类型。
- 2. 源站处理策略:

设置源站的转发处理规则,即在同一个监听器绑定多个源站的情况下,选择源站之间的调度策略。



3 Origin He Policy	alth Check					
Policy) Weighted RR	C Least (Connections		
Origin-pull SNI						

- 轮询:多个源站按轮询策略回源。
- 轮询加权:多个源站按权重比例回源(源站类型为域名时不支持配置)。
- 最小连接数:在所有源站中选择连接数最小的源站优先进行调度。
- 回源SNI:与源站建立SSL连接之前先发送SNI,源站根据SNI值返回对应的证书。
- 3. 源站健康检查机制:

您可以选择针对当前域名启用监控检查机制。可以设置独立的检查 URL,请求方式可以支持HEAD及GET,检查 状态码可支持 http_1xx, http_2xx, http_3xx, http_4xx, http_5xx,状态码可单选也可多选,即当检测到指定的



状态码时,监听器认为后端源站属于正常状态。如果未检测到任何状态码时,监听器认为后端源站异常。

1 Basic Configuratic 3 Origin Health Ch	n) (2) Config eck Policy	ure the policy	>	×
Enable Health C	heck			
Response Timeout			2	seconds
	2 seconds 31 seconds	60 second	Is	
Health Check Interval	, - III		30	seconds
	5 seconds	300 seco	onds	
Check domain	test			
Test URL	/			
	Specify an URL or directly use	a root directory"	/"	
Request method	HEAD	v		
Status monitoring code	http_1xx http_2xx http_2xx http_4xx http_5xx	http_3xx	c	
	When the status code is http_:	1xx、http_2xx、h	http_3xx、	
	http_4xx、http_5xx, the backe	nd server is cons	idered to	be valid
	Back OK			

修改域名

完成"添加域名"操作后,单击修改域名,可以对域名进行修改。

Modify domain	n name		×
Domain Name	5. /Z		
	ОК	Cancel	



删除域名

完成"添加域名"操作后,单击**删除**可删除域名。如果域名下已有规则绑定源站,则需要勾选"强制删除绑定有源站的 规则"。



HTTP3配置

支持变更对应域名是否开启HTTP3传输(当前仅支持在HTTPS监听器配置,且创建通道时HTTP3特性状态为开启)

HTTP3 Configuration							
Domain HTTP3 Transfer 🛈	qq.com O Disable	C Enable					
1	Confirm	Cancel					

修改规则

参考上文添加规则,主要差别在于域名和源站类型无法修改。

绑定源站

详情请参见绑定源站,可以对不同源站绑定不同的端口。有关"覆盖端口"及"补齐端口"功能,请参见TCP/UDP 监听 器源站绑定。

注意:



一个规则绑定的源站总数最多为100个。

删除规则

完成"添加规则"操作后,单击**删除**可删除规则,如果规则下有绑定的源站,需要先勾选"强制删除绑定有源站的规则"。

			×
(!)	Confirm to de	lete the following rules?	
	Domain Name	gameft01.xyz	
	URL	/	
	Bind origin server	Bound	
	Force delet	ion of listeners bound with origin server	
		OK Cancel	

配置回源请求头

1. 完成"添加规则"操作后,在规则的操作栏选择更多,单击配置回源请求头

÷	HTTP/HTTPS Listener Management (IgI-bysI51f9)									
		Create	e a Distribution							
			Domain		Statu	s		Operation		
		Ŧ	qq.com		Runni	Running Add Rule Modif		Add Rule Modify	ify Domain Name Delete	
			Rule ID	URL		Forwarding Host	Bound Origin Server	Service status	Operation	
			rule-rrly3gfr	/		Default	j	Normal (j)	Modify Rule Bind origin server Delete More 🗸	
									Set Origin-pull Request Header	

2. 单击**新增参数**, 添加请求头的名称参数及取值;如需要携带用户真实IP的头部, 其变量值为\$remote_addr(默认已经有X-Forwarded-For头部携带客户IP回源),携带用户真实端口的变量值为\$remote_por;其余带\$变量默认不支持,如有需求,可提交工单联系我们。

注意:

- 1. HTTP头部的名称Key值长度默认为1 100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,不支持中文;
- 2. 每条规则最多可配置10条回源 HTTP 请求头;
- 3. 部分标准头部不支持自助设置/增加/删除,具体清单请参见以下列表。

www-authenticate	authorization	proxy-authenticate	proxy-authorization
age	cache-control	clear-site-data	expires
pragma	warning	accept-ch	accept-ch-lifetime
early-data	content-dpr	dpr	device-memory
save-data	viewport-width	width	last-modified
etag	if-match	if-none-match	if-modified-since
if-unmodified-since	vary	connection	keep-alive
accept	accept-charset	expect	max-forwards
access-control-allow- origin	access-control-max-age	access-control-allow- headers	access-control-allow- methods
access-control-expose- headers	access-control-allow- credentials	access-control-request- headers	access-control-request- method
origin	timing-allow-origin	dnt	tk
content-disposition	content-length	content-type	content-encoding
content-language	content-location	forwarded	x-forwarded-host
x-forwarded-proto	via	from	host
referer-policy	allow	server	accept-ranges
range	if-range	content-range	cross-origin-embedder- policy
cross-origin-opener- policy	cross-origin-resource- policy	content-security-policy	content-security-policy- report-only
expect-ct	feature-policy	strict-transport-security	upgrade-insecure- requests
x-content-type-options	x-download-options	x-frame-options(xfo)	x-permitted-cross-



			domain-policies
x-powered-by	x-xss-protection	public-key-pins	public-key-pins-report- only
sec-fetch-site	sec-fetch-mode	sec-fetch-user	sec-fetch-dest
last-event-id	nel	ping-from	ping-to
report-to	transfer-encoding	te	trailer
sec-websocket-key	sec-websocket- extensions	sec-websocket-accept	sec-websocket-protocol
sec-websocket-version	accept-push-policy	accept-signature	alt-svc
date	large-allocation	link	push-policy
retry-after	signature	signed-headers	server-timing
service-worker-allowed	sourcemap	upgrade	x-dns-prefetch-control
x-firefox-spdy	x-pingback	x-requested-with	x-robots-tag
x-ua-compatible	max-age		

删除HTTP/HTTPS 监听器

单击 HTTP/HTTPS 监听器管理标签页,在操作栏单击**删除**,可以删除指定的监听器,若监听器已绑定源站,则需要 选中"允许强制删除绑定有源站的监听器"后,才能删除。删除后,该监听器的端口将停止加速。





安全防护

最近更新时间:2023-06-07 15:05:12

GAAP 默认提供基础安全防护策略(普通用户是 2Gbps 带宽, VIP 用户是 10Gbps 带宽)。如需升级到高级防护策略, 可在 DDoS 高防包控制台-云资产升级防护。

另外 GAAP 控制台提供安全防护可支持配置黑白名单。详细配置方法如下:

- 1. 登录 全球应用加速控制台,进入"接入管理"页面,单击指定通道的 ID/通道名。
- 2. 进入到下一级页面,选择**安全防护 > 添加规则**,可进入向导,具体配置如下:
 - i. 添加访问规则,选择默认准许/拒绝所有流量访问通道。

Add Access Rule	×
 Allow all traffic accessing the connection by default Reject all traffic accessing the connection by default 	
Confirm Cancel	

ii. 添加来源IP,选择协议并添加协议端口。之后选择"允许"/"拒绝"该IP的访问。

Add Access Rule	2	×
Source IP 🤅		
Protocol	TCP ·	
Protocol Port 🛈		
Policy	Allow	
Remarks		
- I	Confirm Cancel	



说明:

i. 可添加的访问规则最多为100个。

3. 单击**确定**。



访问加速通道

最近更新时间:2021-12-15 16:00:03

TCP/UDP 协议

您可以通过以下三种方法访问加速通道:

- 客户端直接访问加速通道 VIP+端口。
- 客户端访问加速通道域名+端口。
- 若客户端原来访问的是域名,可以将该域名 cname 到加速通道的域名,或者修改客户端本地 host,将原来访问的域名解析到加速通道 VIP。
 源站如果需要获取客户端真实IP(仅 TCP 协议),需要安装 TOA 模块,具体可参见 服务端获取客户端真实 IP
 (仅针对 TCP 协议)。

HTTP/HTTPS 协议

将客户端访问的域名 cname 到加速通道的接入域名,或者修改客户端本地 host,将客户端要访问的域名解析到加速通道 VIP,然后客户端按照 协议+URL 访问即可实现加速。 源站可以直接从 HTTP 请求头中 x-forward-for 字段中获取客户端真实 IP。



通道组管理

最近更新时间:2021-12-10 11:04:29

新增通道组

当用户需要加速多个区域, 源站区域相同, 且监听器配置相同时, 可以通过通道组实现批量配置管理, 减少管理单 通道时的重复工作。

1. 登录 全球应用加速控制台,进入"通道组管理"页面,单击新增。

2. 在弹出的窗口中,填写通道组信息。

Add Connection Gro	up
Project *	DEFAULT PROJECT 🔹
Connection Group Name	*
IP Version *	
Accelerator Region *	Please select an accelerator reg 💌
Origin Region *	Select the origin region 🔻
	Region of RS
Connection Specification	 Please first select the accelerator region and origin region.
Tag	+ Add
	You can classify and manage resources by setting tags, with up to 50 tags for each resource.Manage Tag 🛂
Fees Connection fees:	Please select the configuration
Bandwidth fees:	Please select the configuration
	Confirm Cancel

- 项目:该通道组所属项目(后续可以更换项目)。
- 。通道组名称:最多30个字符,支持中文。
- 。 IP版本:可根据需要选择 IPv4 或 IPv6,其中 IPv6 暂时只支持国内接入节点。
- · 接入节点:选择客户端所在区域或距离客户端最近区域的节点,支持多选。



注意:

- 。中国香港提供精品 BGP 网络,如有需要,可提交工单联系我们。
- 中国大陆提供三网节点网络,如有需要,可提交工单联系我们。
- 源站区域:选择目标服务器所在区域或距离目标服务器最近区域的节点。

注意: 中国台湾无法与中国大陆进行直连。

- 通道规格:选择各通道的带宽上限及最大并发数。
- 带宽上限:通道的带宽上限,最大值10000Mbps(部分通道最大值为1000Mbps)。
- 并发上限:通道的最大并发连接数,最大值100万(部分通道最大值为30万)。

注意:

一个通道组下的通道数量不能超过20个。

- 标签:非必填项,可通过设置标签实现对通道的分类管理;
- 费用:根据您选择的带宽与并发数,下方会给出相应的通道费和带宽费。
 a.通道费:按日计算,直到通道被删除为止,请特别注意通道创建后未满一天删除也会按一天计费;
 b.带宽费:按每日实际出入带宽峰值计费。

3. 单击确定,完成新增通道组。

4. 在 通道组管理 页面中, 查看通道组列表信息, 可根据实际需求, 选择对同一通道组下的不同通道进行管理, 监控 不同通道的实时运行状态。



Connection	n Group Management	All Projects 🔻									
General Co	onnection Groups Gam	e Accelerator Conn	ection Groups								
Add	Change Project										Separate keywords with
	ID/Connection group nam	ie IP V	ersion T Origin Region T		Status	Billing Mo	de	Project	Creat	tion Time	Operation
*	lg-Ł test ∋n ∕*	IPv4	West India (Mum	bai)	Running	Bill by Ban	dwidth	DEFAULT PROJECT	2021,	/ 56:07	Configure listener 📊 More 👻
	ID/Connection Name	VIP	Domain Name 🕃	Accelerator Regi	Origin Region	Bandwidth Cap	Concurrent	Status	Billing Mode	Project	Operation
	link-me default 💉	150 5	link-pqcloud.com	Thailand (Bangkok)	West India (Mumbai)	10 Mb	20 k	Running	Bill by Bandwidth	DEFAULT PROJECT	Modify Configuration
	link-345¢ default 🔊	15 57	link- vqcloud.com	Korea (Seoul)	West India (Mumbai)	10 Mb	50 k	Running	Bill by Bandwidth	DEFAULT PROJECT	Modify Configuration
	link-m ^c default	1 29	link apqcloud.com	Singapore	West India (Mumbai)	10 Mb	20 k	Running	Bill by Bandwidth	DEFAULT PROJECT	Modify Configuration

- 。 ID/通道组名:通道的 ID 和名字,其中通道名可以修改。
- VIP:用于客户端访问的接入 IP 地址。
- 。 域名:用于客户端访问的接入域名(系统分配,且自动绑定到 VIP)。
- · 状态:仅"运行中"状态下,加速通道才可以正常使用。

查看通道组信息

1. 登录 全球应用加速控制台,进入"通道组管理"页面,单击指定通道组的 ID/通道名,进入下一级页面。

ID/Connection group name	IP Version T	Origin Region 🔻	Status	Billing Mode	Project	Creation Time	Operation
lg-b test	IPv4	West India (Mumbai)	Running	Bill by Bandwidth	DEFAULT PROJECT	202 6:07	Configure listener 📊 More 🗸

2. 在"通道组信息"标签页,可以查看各通道的详细信息。其中,"转发 IP"是指加速通道末端的转发节点 IP,该转发 节点负责将加速通道的数据通过公网转发给源站。如果您希望多条通道使用同一个域名,可单击**统一域名**选项可



直接跳转至"统一域名"页面进行配置,通道组下不同通道可单独对统一域名进行配置。

Connection group info	TCP/UDP Listener Man	agement HTTP/HTTPS Listene	er Management Attack Defense		
	Connection	Connection Info			
	link- 150	Connection ID	link-		
	link 97h	Connection Name	default		
	15. 0.57	VIP	15 6 link-mexxnlvj.gaapqcloud.com		
	link cxf 10 129	Domain			
		Accelerator Region	Thailand (Bangkok)		
		Network Type	General BGP		
		Origin Region	West India (Mumbai)		
		Bandwidth Cap	10 Mb		
		Max Concurrent Connections	20 k		
		Unified Domain Name()	No associated		
		Forwarding Server IP			
		Creation Time	Connection Group:2021/10, :56:07 Connection: 2021/10/ 59:18		
		Time Modified	Connection: 2021/10/ 59:18		
		Billing Mode	Bill by Bandwidth		
		Project	DEFAULT PROJECT		

TCP/UDP 监听器管理

新增 TCP/UDP 监听器

详情请见 接入管理相关配置页面。

设置 TCP/UDP 监听器


详情请见 接入管理相关配置页面。

HTTP/HTTPS 监听器管理

新增 HTTP/HTTPS 监听器

详情请见 接入管理相关配置页面。

设置 HTTP/HTTPS 监听器

详情请见 接入管理相关配置页面。

安全防护

详情请见 接入管理相关配置页面。



统计数据

最近更新时间:2022-06-20 15:18:55

登录全球应用加速控制台,进入"统计数据"页面。

该页面共提供了以下数据的筛选维度,分别为[通道]、[通道组]、[监听器]、[源站]、[域名]。

通道

查看通道维度的统计数据,如下图所示:

- 通道归属:默认选择为单通道,也可以选择已创建的通道组。
- •选择通道:选择接入管理中的通道,或者通道组内的通道。
- 数据类型:全部、带宽、流量、包量、并发连接数、HTTP QPS、HTTPS QPS、时延、丢包率。
- 时间范围:选择时间范围。
- 时间粒度:选择数据统计粒度,支持1分钟、5分钟、1小时和1天。
 [选择1分钟粒度,最长可查看1天的数据;选择5分钟粒度,最长可查看3天的数据;选择1小时粒度,最长可查看15天数据;选择1天粒度,最长可查看186天数据]

Dimension	Connect	ion Conne	ction group	Listener	Origin					
onnection Type	Single Cor	nection				•				
onnection	test (link-(tt (link-C nox 15C 79)								
ata Range 🛈	By Conr	nection Ove	erall							
ata Type	All	Bandwidth	Traffic	Packet Volume	Conc	urrent Connections	HTTP QPS	HTTPS QPS	Latency	Packet loss rate
ne Period	Today	Yesterday	Last 7 Day	vs Last 15 d	ays	Last 30 Days	2021-09-26 ~ 2021-	.09-26 💼		
me Granularity	5 minutes		~							

通道组

查看通道组维度的统计数据,如下图所示:

• 通道组:选择一条或多条通道组。



- 数据类型:全部、带宽、流量。
- 时间范围:选择时间范围。
- 时间粒度:选择数据统计粒度,支持1分钟、5分钟、1小时和1天。

[选择1分钟粒度,最长可查看1天的数据;选择5分钟粒度,最长可查看3天的数据;选择1小时粒度,最长可查看 15天数据;选择1天粒度,最长可查看186天数据]

Dimension	Connection	Connection	group L	istener Origin	١		
Connection group	test (lg-cic9h)			•		
Data Type	All Band	dwidth Tra	affic				
Time Period	Today Y	'esterday	Last 7 Days	Last 15 days	Last 30 Days	2021-09-26 ~ 2021-09-26	Ċ
Time Granularity	5 minutes		•				

监听器

查看监听器维度的统计数据,如下图所示:

- 通道/通道组:选择监听器所归属的通道/通道组。
- 监听器:选择监听器。
- 数据类型:全部、带宽、包量、并发连接数。
- 时间范围:选择时间范围。
- 时间粒度:选择数据统计粒度,支持1分钟、5分钟、1小时和1天。
 [选择1分钟粒度,最长可查看1天的数据;选择5分钟粒度,最长可查看3天的数据;选择1小时粒度,最长可查看15天数据;选择1天粒度,最长可查看186天数据]



Dimension	Connec	tion Conne	ection group	Listener	Origin		
nnection/Connection Group	test (link-	01 Tiox 15.).59)			•	
ener	test (listen					•	
ata Type	All	Bandwidth	Packet Volume	Concurr	rent Conne	ctions	
ne Period	Today	Yesterday	Last 7 Days	Last 15	days	Last 30 Days	2021-09-26 ~ 2021-09-26
ne Granularity	5 minutes	5	T				

源站

查看通道已绑定的源站中,健康状态的统计数据,如下图所示:

- 通道/通道组:选择源站所归属的通道/通道组。
- 监听器:选择源站所归属的监听器。
- 源站:选择源站。
- 时间范围:选择时间范围。
- 时间粒度:选择数据统计粒度,支持1分钟和5分钟。

[选择1分钟粒度,最长可查看1天的数据;选择5分钟粒度,最长可查看31天的数据]

Dimension	Connection	Connec	tion group	Listener	Origin]		
Connection/Connection Group	test (link-00)		.9)			•		
istener	- m/ (r	ule-eemgscc5)				•		
Origin	10	(rs €⁺g1)				•		
Time Period	Today	Yesterday	Last 7 Days	s Last 1	5 days	Last 30 Days	2021-09-26 ~ 2021-09-26	ö
Time Granularity	5 minutes		•					



域名

查看HTTP/HTTPS监听器配置中,监听域名的统计数据,如下图所示:

- 加速区域:选择中国境内、中国境外。
- 统计域名:支持单选、多选域名。
- HTTP协议:支持单选、全选。
- 数据类型:全部、请求量、状态码、Top10 URL。
- 时间范围:选择时间范围。
- 时间粒度:选择数据统计粒度,支持1分钟、5分钟、1小时和1天。
 [选择1分钟粒度,最长可查看1天的数据;选择5分钟粒度,最长可查看3天的数据;选择1小时粒度,最长可查看
 15天数据;选择1天粒度,最长可查看31天数据]

Dimension	Connection	Connection gro	oup Listener	Origin	Domain nam	ne	
Region	Chinese Mainla	and Overseas	5				
Domains	Please select				•		
HTTP Protocol	HTTP, HTTPS	•					
Acceleration Type	All Atta	ck Requests	Status code To	p10 URL			
Time Period	Today Y	′esterday Las	t 7 days Last 1	5 days	Last 30 days	2022-04-29 ~ 2022-04-29	Ċ
Time Granularity	5 minutes	•					

数据导出



进入"统计数据"页面,点击数据展示页右上角的**下载**图标,即可导出数据。

Dimension	Connectio	n Conne	ction group	Listener	Origin					
Connection Type	Connection	Group: test (၊၂	55)			v				
Connection	All Connecti	ons				*				
Data Range 🛈	By Connec	tion Ov	erall							
Data Type	All	Bandwidth	Traffic	Packet Volume	Concurre	ent Connections	HTTP QPS	HTTPS QPS	Latency	Packet loss rate
Time Period	Today	Yesterday	Last 7 Da	ays Last 15	days La	st 30 Days	2021-09-20 ~ 2021	-09-26 📩		
Time Granularity	1 hour		~							
Bandwidth In (N	/lbps)									

配置告警

0.00175

进入"统计数据"页面,点击右上角"配置告警",即可进行数据报警配置,具体操作流程详见接入云监控。



配置权限

最近更新时间:2021-12-10 11:04:29

拥有 GAAP 权限的主账号或其他账号(AdministratorAccess 权限账号),可通过配置访问管理权限,使协作者账号 拥有 GAAP 全读写或只读访问权限。

用户可通过策略关联用户、用户关联策略两种方式为协作者账号进行授权。更多信息,请参见访问管理 CAM。

准备步骤

1. 使用拥有 GAAP 权限的主账号或其他账号(AdministratorAccess 权限账号),登录 腾讯云控制台。
 2. 在顶部导航中,选择【云产品】>【管理与审计】>【访问管理】,进入访问管理控制台。

说明:

您也可以在腾讯云控制台右上角,选择您的账户名称>【访问管理】,进入访问管理控制台。

操作步骤

策略关联用户

- 1. 在左侧菜单中,单击【策略】,进入管理页面。
- 2. 在搜索栏中,检索"GAAP",找到2条结果。选择策略权限,单击【关联用户/组】。

olicy	All Policies 🔻			
Bind	users or user groups with the policy to as	isign them related permissions.		
Creat	e Custom Policy Delete		GAAP	Q,
	Policy Name	Description	Service Type 🔻	Operation
		Search"GAAP", 2 results are found.Back to Original List		
	QcloudGAAPFullAccess	Full read-write access to Global Application Acceleration Platform	Global Application Acceleration Platform	Bind User/Group
	QcloudGAAPReadOnlyAccess	Read-only access to Global Application Acceleration Platform	Global Application Acceleration Platform	Bind User/Group



3. 勾选需要授权的用户,单击【确定】,即授权成功。

关联用户/用户组					×
关联用户			已选择(2条)		
		論語 Q	用户名/组名	类型	
用户	切换成用户组 ▼		£.	用户	×
一 走	用户	Â	z,	田户	~
✓ 2;	用户	E	HU	, 11,	^
	用户		\Leftrightarrow		
	用户				
一五	用户				
<u>并一下</u>	用户				
支持按住shift键进行多选					
		确定	取消		

用户关联策略

1. 在左侧菜单中,选择【用户】>【用户列表】,进入管理页面。

2. 在列表中,找到需要授权的用户所在行,单击操作栏中的【授权】。

详情	用户名称	用户类型	账号ID	关联信息	操作
Þ	X.	主账号	3299785925		授权
Þ	1.	子用户	100004619964		授权
×	6	子用户	100003407227		授权



3. 在关联列表中,检索"GAAP",勾选策略权限,单击【确定】,即授权成功。

ААР		0	Q,		Policy Name	Policy Type	
Po	olicy Name	Policy Ty	Ŧ		OcloudGAAPFullAccess		
Qa	cloudGAAPFullAccess Ill read-write access to Global Application	Preset policy			Full read-write access to Global Application Acceleration Platform	Preset policy	
Ad	cceleration Platform				QcloudGAAPReadOnlyAccess		
Qa Re Ad	cloudGAAPReadOnlyAccess ead-only access to Global Application cceleration Platform	Preset policy		\Leftrightarrow	Read-only access to Global Application Acceleration Platform	Preset policy	
ss Shift	t to select multiple items						

查看和解除权限

授权成功的用户,可在用户列表中,单击用户名称,查看权限、解除权限。

权限(3) 用户组(0) 安全	t 🕕 API 密钥			
关联策略以获取策略包含的操作权	限。解除策略将失去策略包含的操	作权限。特别的,解除随组关联类型	的策略是通过将用户从关联该策略的用户	组中移出。
关联策略 解除策略				
策略名	关联类型 ▼	策略类型 ▼	关联时间	操作
	直接关联	预设策略	2019-04-15 15:21:38	解除
Q.	3 直接关联	预设策略	2019-04-15 15:21:38	解除



接入腾讯云可观测平台

最近更新时间:2023-05-09 18:46:16

应用场景

为提升使用体验,您可以在腾讯云可观测平台产品中配置对应的告警规则,当加速通道达到告警条件时,第一时间触发告警。

操作步骤

登录 腾讯云可观测平台控制台,进行如下操作。

通道监控

1. 在左侧目录中,选择"告警策略",单击新建,进入新建策略页面。



2. 在"策略类型"中,选择 全球应用加速 > 通道监控。

Create Ala	m Policy
Basic Info	
Policy Name	It can contain up to 30 characters
Remarks	It can contain up to 100 characters
Monitoring Type	Cloud Product Monitoring
Policy Type	Cloud Virtual Machine 🔻
Project 🚯	Data Transmission Service
Alarm Policy	Cloud Database Channel docker service L4_Listener_rs_status
Alarm Object 🚯	docker cluster
	docker container tag now, allowing newly
	GAAP >

3. 在"配置告警规则"中,选择"告警对象",您可根据需要添加通道进行监控。

在"配置触发条件"中,您可选择"使用模板"或进行"手动配置"。

如选择"使用模板",您可使用之前已经配置的告警策略。如无合适模板,您可通过新建模板的方式进行配置。该 模板会存储在控制台中,方便您的后续使用。新建模板具体配置过程如下:



i. 单击"新增触发条件模板", 进入模板配置页面。

Trigger Condition	O Select template O Configure manually
	Please select 🔹 🗘 If there is no suitable template, you can Add Trigger Condition Template 🗹 or Change Template 🖾
	Metric Alarm
	When meeting any • of the following metric conditions, the metric will trigger an alarm.

ii. 单击新建, 在弹出的窗口中配置触发条件, 条件说明如下。

- 模板名称:输入模板名称。
- 备注:输入模板备注。
- 策略类型:选择监控的服务,如全球应用加速 **> **通道监控。
- 使用预置触发条件:腾讯云可观测平台内置对应监控项的触发条件,勾选则开启。
- 触发条件:分为指标告警和事件告警。在其下方单击添加,可以设置多个告警项。
 如选择使用"手动配置",您可根据需要添加多个告警触发条件。

Alarm Policy	
Alarm Object 🚯	Instance ID v 1(link-mxgqu4ab) v
Trigger Condition	Select template O Configure manually (✔ Use preset trigger conditions ③)
	Metric Alarm
	When meeting any • of the following metric conditions, the metric will trigger an alarm.
	Threshold Ostatic Opynamic () Type ()
	If Inbound bandwidth ▼ (statistical perioc ▼) > ▼ 70 Mbps at 5 consecutive c ▼ then Alarm every 5 minut ▼ ③ 前
	Threshold O Static O Dynamic (1) Type (1)
	If Outbound bandwi ▼ (statistical perior ▼ > TO Mbps at 5 consecutive (▼ then Alarm every 5 minut ▼ ① III
	Add Metric

4. 在"配置告警通知"中,单击新建模板,添加通知模板名称并选择接收对象及渠道。





New Notification Templat	te	×
Notification Template Name *	It can contain up to 30 Chinese characters, letters, digits, underscores, or syı	
Recipient Object *	User v	🗘 🛛 Add User
Receiving Channel *	🛩 Email 🔽 SMS	
For more configurations, please	go to notification template page 🛂	
	Confirm Cancel	

单击**选择模板**,选择相应模板即可完成设置。

selected. more	can be selected.		
Search for not	ification template		Q, Q
	Notification Templat	Included Operations	
<u>~</u>	Preset Notification Te	Recipient: 1	
Total items: 1	10 🔻 / page	◀ 1 /1	page 🕨 🕨
	Confirm	Cancel	

监听器监控

1. 在左侧目录中,选择**告警策略**,单击**新建**,进入新建策略页面。



2. 在"策略类型"中,选择全球应用加速 > 4层监听器源站状态/7层监听器源站状态。

Create Ala	w Deller			
Create Ala	rm Policy			
Basic Info				
Policy Name	It can contain up to 30 c	haracte	rs	
Remarks	It can contain up to 100	charact	ers	
Monitoring Type				
5.77	Cloud Product Monito	ring		
Policy Type	GAAP / L4_Listener_rs_st	atus	•	
Project 🕢	Cloud Virtual Machine		L7_Listener_rs_status	ate 300 more static threshold policiesThe current account has 0 policies for dynamic alarm thresholds, and 20 more policies can be created.
	Cloud Block Storage	_	Channel	
Alarm Policy	CDB	+	L4_Listener_rs_status	
Alarm Object 🚯	docker(new)	+		v
	ckafka	•		

3. 在"配置告警规则"中,选择"告警对象"。在"配置触发条件"中,选择"使用模板"或进行"手动配置"。如选择使用"手动配置",您可设置"监听器源站状态异常"触发条件。

Alarm Policy	
Alarm Object 🚯	Instance ID 🔻 Select object 🔻
Trigger Condition	○ Select template O Configure manually (✓ Use preset trigger conditions (i))
	Metric Alarm
	When meeting any • of the following metric conditions, the metric will trigger an alarm.
	Threshold Ostatic Opynamic () Type ()
	► If Origin server status ▼ (statistical perior ▼ Please select ▼ then an alarm is triggerer ▼ ①
	Add Metric

4. 在"配置告警通知"中,单击新建模板,添加通知模板名称并选择接收对象及渠道。

注意:

接收对象需绑定对应渠道,否则将无法收到告警通知。



New Notification Templa	te		×
Notification Template Name *	It can contain up to 30 Chinese characters, letters, digits, underscores, or sy		
Recipient Object *	User 🔻	φ	Add User
Receiving Channel *	🖌 Email 🔽 SMS		
For more configurations, please	e go to notification template page 🛂		
	Confirm		

单击**选择模板**,选择相应模板即可完成设置。

l selected. more	can be selected.	
Search for not	fication template	Q, Q
	Notification Templat Included C	Operations
~	Preset Notification Te Recipient: 1	1
Total items: 1	10 🔻 / page 🛛 🗐 🚽	1 / 1 page 🕨 🕅
	Confirm Cano	cel



证书管理

最近更新时间:2021-12-10 11:04:30

证书新增

1. 登录 全球应用加速控制台,进入"证书管理"页面,单击**新增**。

2. 填写证书信息。

Create a new cer	tificate	×
Certificate Name		
Certificate Type	Server SSL certificate	
Certificate Content	Format: please enter in PEM format View Example	
Key Content	Format: please enter in PEM format View Example	
	Confirm Cancel	

• 证书名称:用户自定义配置该证书的别名。



- 证书类型:分为[基础认证配置]、[客户端CA证书]、[服务器SSL证书]、[源站CA证书]、[通道SSL证书]五种类型, 其中[服务器SSL证书]、[通道SSL证书]需要配置密钥,密钥需要在腾讯云的 SSL 证书管理产品中进行购买。
- 证书内容:采用 pem 格式填写证书内容。
- 密钥内容:采用 pem 格式填写密钥内容。

证书详情

进入"证书管理"页面,单击证书"ID/名称"或单击该证书详情按钮即可查看该证书的详细信息。

证书删除

进入"证书管理"页面,单击证书**删除**按钮,然后单击弹窗确定按钮即可删除该证书。

() Are you hwfvgt	ı sure you wa st) ?	× ant to delete test(cert-
	Confirm	Cancel



获取访问用户真实 IP 通过 TOA 获取客户端真实 IP (仅针对 TCP 协议) 基本原理

最近更新时间:2022-07-13 15:43:30

加速通道转发数据包时,数据包同时会做 SNAT 和 DNAT,即数据包的源地址和目标地址均修改。源站看到的数据 包的源地址是加速通道转发 IP 地址,而并非是客户端的真实 IP。为了将客户端 IP 传给服务器,加速通道将客户端 的 IP 和 Port 在转发时放入了自定义的 tcp option 字段中。如下:

```
#define TCPOPT_ADDR 200
#define TCPOLEN_ADDR 8 /* /opcode/size/ip+port/ = 1 + 1 + 6 */
/*
 * insert client ip in tcp option.
 * must be 4 bytes alignment.
 */
struct ip_vs_tcpo_addr{
    __u8 opcode;
    __u8 opsize;
    __u16 port;
    __u32 addr;
};
```

Linux 内核在监听套接字收到三次握手的 ACK 包之后,会从 SYN_REVC 状态进入到 TCP_ESTABLISHED 状态。这时内核会调用 tcp_v4_syn_recv_sock 函数。Hook 函数 tcp_v4_syn_recv_sock_toa首先调用原有的 tcp_v4_syn_recv_sock函数,然后调用 get_toa_data 函数从 TCP OPTION 中提取出 TOA OPTION,并存储在 sk_user_data 字段中。再用 inet_getname_toa hook inet_getname,在获取源 IP 地址和端口时,首先调用原来的 inet_getname,然后判断 sk_user_data 是否为空,如果有数据从其中提取真实的 IP 和 port,替换 inet_getname 的 返回。

服务端程序在用户态调用 getpeername, 返回的 IP 和 port 即为客户端的原始 IP。



Linux 后端版本调用 步骤一:创建 TCP 监听器并开启 TOA

最近更新时间:2022-06-20 10:48:45

注意:

若您在后端适配过程中遇到无法解决的问题,可通过工单联系我们。

仅四层 TCP 支持 TOA 获取客户端真实 IP,请根据以下指引,在加速通道中选择开启 TOA。

控制台步骤:登录 腾讯云 GAAP 控制台 > 进入加速通道(监听器配置) > 新增 TCP 监听器管理 > 勾选 TOA > 按照 指引完成监听器、通道创建。



Add a listener						
1 Listener	Info > 2 Configure t	he Policy	3 Origin Health Check Policy	>		
4 Session	Persistence					
Listener Name	Please enter the listener name					
Origin Type	IP address					
Protocol	TCP					
Get client IP	• TOA Proxy Protocol					
Listening Port	Listening Port		Operation			
	Enter a listening port		Delete			
	Add Port					
		Next				



步骤二:后端服务加载 TOA 模块

最近更新时间:2022-07-13 15:09:53

方法一:直接下载源码并加载模块

1. 根据腾讯云上 Linux 的版本,下载对应的 TOA 包并解压。

- arm64
 - kernel-4.18.0.rar
- centos
 - CentOS 6.5 64.rar
 - CentOS 7.2 64.rar
 - CentOS 7.3 64.rar
 - CentOS 7.4 64.rar
 - CentOS 7.5 64.rar
 - CentOS 7.6 64.rar
 - CentOS 7.7 64.rar
 - CentOS 7.8 64.rar
 - CentOS 7.9 64.rar
 - CentOS 8.0 64.rar
 - CentOS 8.2 64.rar
- debian
 - Debian 10.2 64.rar
 - Debian 8.2 64.rar
 - Debian 9.0 64.rar
- suse linux
 - SUSE Linux Enterprise Server 12 SP3 64.rar
- ubuntu
 - Ubuntu Server 14.04.1 LTS 64.rar
 - Ubuntu Server 16.04.1 LTS 64.rar
 - Ubuntu Server 18.04.1 LTS 64.rar
 - Ubuntu Server 20.04.1 LTS 64.rar

2. 解压完成后,执行 cd 命令进入刚解压的文件夹里,执行加载模块的指令:

insmod toa.ko



3. 执行下面指令确认是否已加载成功:

lsmod | grep toa

root@VM-16-42-centos ~]# lsmod | grep toa 278528 0

4. 加载成功,在启动脚本里面加载 toa.ko 文件(重启机器 ko 文件需要重新加载)。

```
echo "insmod xxxxx /toa.ko" >> /etc/rc.local
```

5. (可选)临时关闭 TOA : rmmod 路径/模块名。

```
rmmod toa.ko
```

6. (可选)若不再需要使用 TOA 模块,执行以下命令进行卸载。

```
rmmod toa
```

7. (可选)执行以下命令确认 TOA 模块是否卸载成功。若提示"TOA unloaded",则说明卸载成功。

dmesg -T

方法二:自行编码并加载模块

若上述下载文件中没有您的操作系统版本对应的安装包,请下载 Linux 通用版的源码包,进行编译后获取(以 CentOS 环境为例)。

1. 获取源码包

```
wget "https://thunder-pro-mainland-1258348367.cos.ap-guangzhou.myqcloud.com/gaa
p-toa.rar"
```

2. 安装编译环境。

```
yum install gcc
yum install make
yum install kernel-headers kernel-devel -y
```



3. 解压源码包。

tar zxf gaap-toa.rar

4. 进入 TOA 目录。

cd toa

5. 编译 make。

make

6. 移动并加载模块。

```
mv toa.ko /lib/modules/`uname -r`/kernel/net/netfilter/ipvs/toa.ko
insmod /lib/modules/`uname
¬-r`/kernel/netfilter/ipvs/toa.ko
```

7. 查看是否加载成功。

lsmod | grep toa



步骤三:(可选)查看 TOA 相关的计数状

态:

最近更新时间:2022-06-17 18:49:37

为保障 TOA 内核模块运行的稳定性, TOA 内核模块还提供了监控功能。在插入 toa.ko 内核模块后,可以通过以下 两种方式监控 TOA 模块的工作状态。

执行以下命令查看 TOA 相关的计数状态。

cat /proc/net/toa_stats

HORD TOWING THE -			
[root@VM-16-42-centos	~]# cat	/proc/net/	toa_stats
		CPU0	CPU1
syn_recv_sock_toa		865	858
syn_recv_sock_no_toa		1011	1035
getname_toa_ok		0	0
getname_toa_mismatch		831	892
getname_toa_bypass		0	0
getname_toa_empty		12897	12757
ip6_address_alloc		865	858
ip6_address_free	:	819	904

其中主要的监控指标对应的含义如下所示:

指标名称	说明
syn_recv_sock_toa	接收带有 TOA 信息的连接个数。
syn_recv_sock_no_toa	接收并不带有 TOA 信息的连接个数。
getname_toa_ok	调用 getsockopt 获取源 IP 成功即会增加此计数,另外调用 accept 函数接收客户端 请求时也会增加此计数。
getname_toa_mismatch	调用 getsockopt 获取源 IP 时,当类型不匹配时,此计数增加。例如某条客户端连接内存放的是 IPv4 源 IP,并非为 IPv6 地址时,此计数便会增加。
getname_toa_empty	对某一个不含有 TOA 的客户端文件描述符调用 getsockopt 函数时,此计数便会增加。
ip6_address_alloc	当 TOA 内核模块获取 TCP 数据包中保存的源 IP、源 Port 时,会申请空间保存信息。



指标名称	说明
ip6_address_free	当连接释放时, toa 内核模块会释放先前用于保存源 IP、源 port 的内存,在所有连接都关闭的情况下,所有 CPU 的此计数相加应等于 ip6_address_alloc 的计数。



查看 Client IP

最近更新时间:2022-06-17 18:49:37

参考方法一:直接在 nginx 日志中查看(日志路径:/var/log/nginx/access.log)

参考方法二:使用 wireshark 查看 tcpdump 抓包获取为。

1. 在后端服务器执行以下命令进行抓包

sudo tcpdump -i eth0 -w dump.pcap

-i 指定要抓取的网卡
-w 指定结果保存位置
2. 客户端访问测试地址后,按下 ctrl + c 停止抓包

```
[root@VM-16-42-centos ~]# sudo tcpdump -i eth0 -w dump.pcap
dropped privs to tcpdump
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C361 packets captured
362 packets received by filter
0 packets dropped by kernel
```

3. 用 sz 命令或其他方式把 dump.pcap 文件下载到本地

sz **dump.**pcap

4. wireshark 打开下载的 dump.pcap 文件,从 TCP Option 中查看客户端真实 IP。 此字段后4个字节(十六进制)即为客户端真实 IP





常见问题

最近更新时间:2022-06-17 18:49:37

签名报错,例如 module verification failed: signature and/or required key missing - tainting kernel

- 解决:linux 内核会有对模块有签名校验, 取决于编译内核时候是否开启此特性
- 解决方法一:编译内核时,去掉签名支持 CONFIG_MODULE_SIG=n
- 解决方法二:有证书的情况下,可进行签名,举个例子:
 /usr/src/linux-4.9.61/scripts/sign-file sha512/usr/src/linux-4.9.61/certs/signing_key.pem /usr/src/linux-4.9.61/certs/signing_key.x509 toa.ko

编译时报错没有 /lib/modules 目录

- 解决:常见以下三种情况
- 没安装有内核包
- 路径被修改过,需要自行纠正下
- 安装的内核没有 build 目录,需手动软连接到对应版本内核的 header,例如 cd /lib/modules/4.9.0-13-amd64 && In -s /usr/src/linux-headers-4.9.0-13-amd64 build



Windows 后端版本调用 步骤一:创建 TCP 监听器并开启 TOA

最近更新时间:2022-06-20 10:54:55

注意:

若您在后端适配过程中遇到无法解决的问题,可通过工单联系我们。

仅四层 TCP 支持 TOA 获取客户端真实 IP,请根据以下指引,在加速通道中选择开启 TOA。

控制台操作步骤:登录 腾讯云 GAAP 控制台 > 加速通道(监听器配置) > 新增 TCP 监听器管理 > 勾选 TOA > 按照 指引完成监听器、通道创建。



Add a listener					
1 Listener	1 Listener Info > 2 Configure the Policy > 3 Origin Health Check > Policy				
4 Session	Persistence				
Listener Name	Please enter the listener name				
Origin Type	IP address				
Protocol	TCP				
Get client IP	• TOA Proxy Protocol				
Listening Port	Listening Port		Operation		
	Enter a listening port		Delete		
	Add Port				
		Next			



步骤二:后端服务加载 TOA 模块

最近更新时间:2022-06-17 18:49:37

下载文件

获取文件。

通用版本

文件说明

文件	说明
WinPcap_4_1_3.exe	winpcap 驱动,详情见 WinPcap 文档。
lib_toa.lib	TOA 静态库。
toa_fetcher.h	静态库依赖的头文件。
pcap.h	静态库依赖的头文件。

环境准备

1. 安装 winpcap 驱动:双击 WinPcap_4_1_3.exe(不需重启)。

- 2. 添加 lib_toa.lib 到工程的 lib 库路径下。
- 3. 添加 toa_fetcher.h, pcap.h 到工程的头文件中。

Go 版本

文件说明

文件	说明	
WinPcap_4_1_3.exe	winpcap 驱动,详情请参见 WinPcap 官网。	
toa_win.exe	Windows 服务器端 TOA 服务程序。	
toa_win.conf	Windows 服务器端 TOA 服务程序配置文件。	
program_auto_up.bat	Windows 服务器端服务监控 bat 脚本。	



文件	说明	
demo.go	Go语言编写的示例程序,用于访问 TOA 服务程序。	

部署步骤

1. 修改配置文件 toa_win.conf,参数说明如下:

参数	是否必选	说明
ToaWinPort	是	toa_win.exe 的服务端口,用于与 TOA 获取客户端通信,默认为 9999。
NetworkCardIP	是	用于识别网络接口的 IP 地址字符串,例如:10.75.132.39,该网卡为 与客户端通信的网卡。
ServerListenIP	是	服务器的 IP 地址字符串,例如:10.75.132.39,用于过滤 TCP 流。
ServerListenPortList	否	服务器的端口列表,用于过滤 TCP 流,最多可以填三个端口。 ServerListenPortList 和 PortRange 必须至少设置一个。
PortRange	否	服务器端口范围列表,用于过滤 TCP 流,最多可以填三个端口。 ServerListenPortList 和 PortRange 必须至少设置一个。
CacheSeconds	否	缓存的时长,单位:秒,默认为15秒。

注意: 配置文件必须和 toa_win.exe 放在同一个目录下。

```
#ToaWinPort
9999
#NetworkCardIP
172.19.0.9
#ServerListenIP
172.19.0.9
#ServerListenPortList
9102;5555;6666
#PortRange
6666-7777;7777-8888
#CacheSeconds
15
```



2. 修改 program_auto_up.bat。

修改路径为程序所在的目录,将脚本添加到定时任务中,周期性执行该脚本用于监控 toa_win.exe 程序,当程序退出时,自动拉起。



3. 启动 toa_win.exe 程序, log 日志将存在同一目录下的 toa_win.log。此时,可以通过 udp 通信的方式向 TOA 服务 获取真实的 IP 地址,详情请参见 使用方法。



步骤三:使用方法

最近更新时间:2022-06-17 18:49:37

通用版本

数据结构和函数说明

- class ToaFetcher 主体类,用于管理 TOA 的获取和释放。
- InitUpToaFetcher
- 1. 函数说明

该函数用于初始化 TOA fetcher。

```
bool InitUpToaFetcher(char *ncard_ip_str, char *svr_ip_str, u_short svr_port[],
u_short svr_port_num, u_short cache_secs=TIMER_CACHE_SECS)
```

2. 入参说明

- ncard_ip_str: 用于识别网络接口的 IP 地址字符串,例如: 10.75.132.39,该网卡为与客户端通信的网卡。
- svr_ip_str:服务器的 IP 地址字符串,例如:10.75.132.39,用于过滤 TCP 流。
- svr_port:服务器的端口列表,用于过滤TCP流,最多可以填三个端口,svr_port和port_range_ptr至少设置 其中一个。
- 。 svr_port_num: 服务器的端口个数。
- port_range_ptr:服务器的端口范围数组指针,其中元素为指向一个字符串的指针,端口范围字符串格式: 10001-10005,用于过滤TCP流,最多填三个范围,svr_port和port_range_ptr至少设置其中一个。
- port_range_num:服务器的端口范围个数。
- cache_secs:缓存的时长,单位:秒,默认15秒,详见 toa_fetcher.h:TIMER_CACHE_SECS,缓存时间到 期后,将不再保存该 TOA。

3. 返回值

- 。 TRUE:表示创建 TOA 获取旁路线程成功。
- FALSE:表示创建 TOA 获取旁路线程失败。

FetchToaValue



1. 函数说明

该函数用于获取 TOA 值, tcp-syn 包交互后, 最长需要等待 1ms 后可以获取到 TOA, 正常情况下三次握手需要消耗1ms以上。

bool FetchToaValue(u_long fake_client_ip_addr, u_short fake_client_port, u_long &real_client_ip_addr, u_short &real_client_port)

2. 入参说明

- 。 fake_client_ip_addr:客户端伪 IP 地址,采用网络序存储,从服务器 accept 函数返回的对端地址中获取。
- 。 fake_client_port:客户端伪端口号,采用网络序存储,从服务器 accept 函数返回的对端地址中获取。
- real_client_ip_addr:客户端真实 IP 地址,采用网络序存储,从 TOA 中获取。
- real_client_port:客户端真实端口号,采用网络序存储,从 TOA 中获取。

3. 返回值

- TRUE: 获取 TOA 成功。
- FALSE:未获取到 TOA,一般是超过缓存时间导致 TOA 被清掉。

StopToaFetcher

1. 函数说明

该函数用于停止 TOA fetcher。

void StopToaFetcher()

2. 入参说明

无。

3. 返回值

无。

- GetFetcherStatus
- 1. 函数说明

该函数用于获取 Fetcher 状态。

int GetFetcherStatus()



2. 入参说明

无。

3. 返回值

- 0:表示初始状态。创建实例后,初始状态处于该状态,Fetcher 初始化中,该状态保持不变,当中间出现错误时,返回-1,当成功运行时,返回1。
- -1:表示异常状态。
- •1:表示正常运行中。
- FetchThreadHandler
- 1. 函数说明

该函数用于获取 TOA 旁路线程句柄。

HANDLE FetchThreadHandler()

2. 入参说明

无。

3. 返回值

TOA 旁路线程句柄,当 ToaFetcher 实例被销毁时,将主动关闭该句柄。

FetchErrorInfo

1. 函数说明

该函数用于获取错误码。

bool FetchErrorInfo(int* err_code_ptr, char* err_msg_ptr)

2. 入参说明

- 。 err_code_ptr:一个整型指针指向错误码,用于返回错误码。
- 。 err_msg_ptr : 一个字符指针指向字符串缓冲区, 至少50字节, 用于返回错误信息。

3. 返回值

- TRUE:获取正常。
- FALSE:获取异常。



错误码

错误码	错误信息	说明
0	Ok	正常
-1001	Exceed max server port number	超过最大的端口数,请检查 InitUpToaFetcher:svr_port_num。
-1002	Invalid IP address	非法的 IPv4 地址。
-1003	No suitable network interface	未找到合适的网络接口。
-1004	System Error: find dev error	系统错误:未找到 dev,请联系 lib 开发者。
-1005	System Error: start timer error	系统错误:定时器启动错误,请联系 lib 开发者。
-1006	System Error: compile filter error	系统错误:过滤规则编译错误,请联系lib开发者。
-1007	System Error: set filter error	系统错误:过滤规则设置错误,请联系 lib 开发者。
-1008	System Error: open pcap error	系统错误:打开 dev 错误,请联系 lib 开发者。
-1009	System Error: start pcap error	系统错误:启动监听错误,请联系 lib 开发者。
-1010	System Error: begin thread error	系统错误:启动线程错误,请联系 lib 开发者。
-1999	Unknown error	未知错误,请联系 lib 开发者。

示例

• 初始化 ToaFetcher:

```
char ncard_ip_str[] = "1.1.1.1";
char svr_ip_str[] = "1.1.1.1";
char port_range[3][100] = {"10001-10005", "20001-20005", "30001-30005"};
char* port_range_ptr[3] = {port_range[0], port_range[1], port_range[2]};
u_short svr_port_list[3] = {1111, 2222, 3333};
ToaFetcher inst = ToaFetcher();
inst.InitUpToaFetcher((char*)ncard_ip_str, (char*)svr_ip_str, svr_port_list, 3);
```

• 获取 TOA:

void GetToa(SOCKADDR_IN client_addr, ToaFetcher * toa_fetcher_ptr)
{


```
u_long fake_client_ip_addr = 0;
u_short fake_client_port = 0;
u long real client ip addr = 0;
u_short real_client_port = 0;
memcpy(&fake_client_ip_addr, &client_addr.sin_addr, 4);
memcpy(&fake_client_port, &client_addr.sin_port, 2);
bool ret = toa_fetcher_ptr->FetchToaValue(fake_client_ip_addr, fake_client_port
, real_client_ip_addr, real_client_port);
if(ret == FALSE) {
printf("No toa found\n");
}else{
//fpp: 自定义的打印函数
fpp("real_client_ip_addr", &real_client_ip_addr, 4);
 fpp("real_client_port", &real_client_port, 2);
}
}
```

Go版本

TOA 获取端通过本机 UDP 通信的方式向 toa_win.exe 获取真实 IP 地址。

协议格式

• 请求: | ID(4Bytes)| FakeIPAddress(4Bytes)| FakePort(2Bytes)|

字段说明如下:

- ID:4字节,用于唯一标识一个请求,响应中将原始返回。
- FakelPAddrss: 4字节,客户端伪 IP 地址,采用网络序存储,从服务器 accept 函数返回的对端地址中获取。
- FakePort:2字节,客户端伪端口号,采用网络序存储,从服务器 accept 函数返回的对端地址中获取。
- 响应: | ID(4Bytes)| Code(1Byte)| RealIPAddress(4Bytes)| RealPort(2Bytes)|

字段说明如下:

- ID:4字节,用于唯一标识一个请求,和请求携带上来的一致。
- Code:1字节,0:成功获取到真实 IP 和 Port,1:获取失败。
- ReallPAddress:4字节,网络序,当Code=0时存在,表示真实的客户端IP地址。
- RealPort: 2字节, 网络序, 当 Code=0 时存在, 表示真实的客户端 Port。



示例

详情请参见 demo.go,可以自行开发 TOA 获取客户端程序,也可以使用 demo.go 中的 queryToa 函数进行获取。

1. 函数说明

func queryToa(serverAddr string, fakeIp string, fakePort uint16)(int32, string, uint16)

2. 入参说明

- serverAddr:字符串类型, toa_win.exe 的服务通信地址, 格式:127.0.0.1:9999。
- fakelp:字符串类型, 伪 IP 地址, 格式:1.2.3.4。
- fakePort: uint16类型, 伪 Port, 格式: 8899。

3. 返回值

- 第一个返回值:int32类型,用于表示 error code。
 - 。 0:成功获取
 - 。-1: toa 获取失败,可能因为 fakeIP 和 fakePort 不对或者 cache 到期。
 - -2:网络通信导致的失败。
- 第二个返回值:字符串类型,当 toa 获取成功时,返回真实的 IP,否则为空字符串。
- 第三个返回值: uint16 类型,当 toa 获取成功时,返回真实的 Port,否则为0。



通过 Proxy Protocol 获取客户端真实 IP(仅针 对 TCP 协议) 基本原理

最近更新时间:2022-06-17 18:49:37

Proxy Protocol 是通过为 TCP 添加一个头部信息,来方便的传递客户端信息(协议栈、源 IP、目的 IP、源端口、目的端口等),在网络情况复杂又需要获取用户真实 IP 时非常有用。其本质是在三次握手结束后由代理在连接中插入一个携带了原始连接四元组信息的数据包。

Proxy Protocol 方式获取客户端 IP 需要先在控制台配置开启使用(当前仅支持协议为 TCP 的监听器使用),加速服务 在和源站建立连接后,会在传输的第一个 payload 的报文前插入 Proxy Protocol 协议文本。



操作步骤

最近更新时间:2022-06-20 10:30:22

注意:

若您在后端适配过程中遇到无法解决的问题,可通过工单联系我们。

步骤一:创建TCP监听器并开启 Proxy Protocol

仅四层 TCP 支持 Proxy Protocol 获取客户端真实 IP,请根据以下指引,在加速通道中选择开启 Proxy Protocol。 控制台操作步骤:登录 腾讯云 GAAP 控制台 > 加速通道(监听器配置) > 新增 TCP 监听器管理 > 勾选 Proxy Protocol > 按照指引完成监听器、通道创建。

Add a listener				×
1 Listener In	fo > 2 Configure t	he Policy 💙	3 Origin Health Check Policy	
Listener Name	Please enter the listener name			
Origin Type	IP address			
Protocol	TCP			
Get client IP	TOA Proxy Protocol			
Listening Port	Listening Port (j)		Operation	
	Enter a listening port		Delete	
	Add Port			

步骤二:后端服务适配 Proxy Protocol 协议

当前 Nginx 和 HaProxy 都已经支持 Proxy Protocol 协议。 以 Nginx 为例, 配置支持 Proxy Protocol 协议只需要将参数 proxy_protocol 添加在 server 块中的 listen 指令后:

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



不支持 Proxy Protocol 的应用程序, 需要在 TCP 连接建立后, 读取 Proxy Protocol 的文本行并进行字符串解析来获取 客户端 IP, 字符示例如下所示:

PROXY TCP4 1.1.1.2 2.2.2.2 12345 80\r\n

步骤三:查看 Client IP

参考方法一:直接在 nginx 日志中查看(日志路径:/var/log/nginx/access.log)

参考办法二:执行命令 nc -l port 查看

[root@VM-16-42-centos `]# nc -l 80
PROXY TCP4 112.97. ; 1 172.16.9.142 41131 80
GET / HTTP/1.1
Host: link-cfs4lo35.gaapqcloud.com.cn
Upgrade-Insecure-Requests: l
Accept: text/html,application/xmtl+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 14_8 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.1.2 Mobile/15E148 Safari/604.1
Accept-Language: zh-tw
Accept-Encoding: gzip, deflate
Connection: keep-alive



通过 HTTP 请求头获取客户端真实 IP(支持 HTTP/HTTPS 协议) 基本原理

最近更新时间:2022-06-17 18:49:37

使用 HTTP/HTTPS 监听器后,源站可直接从 HTTP 请求头中 X-Real-IP 或 X-Forwarded-For 字段中获取客户端真实 IP,此为默认生效功能。

同时支持从 "回源 HTTP 请求头配置" 自定义,若从源站到程序还有中间链路 (如 CLB,自建 nginx),则需要自行配置,以防字段被中间链路覆盖。



操作步骤

最近更新时间:2022-06-20 10:40:00

注意:

若您在后端适配过程中遇到无法解决的问题,可通过工单联系我们。

步骤一:创建 HTTP/HTTPS 监听器

控制台操作步骤:登录 腾讯云 GAAP 控制台 > 加速通道(监听器配置) > 新增 HTTP/HTTPS 监听器管理 > 按照指引完成监听器、通道创建。



er Management	HTTP/HTTPS Liste	Management	TCP/UDP Listener N	Connection Info
Service status The cu	Listening Port		P Listeners eate Delete ID/Listener Name	HTTP Cre
Client cer The cu	Server certificate	Authenticat	PS Listeners eate Delete ID/Listener Name	

步骤二:后端服务适配

以下对常见的应用服务器 X-Forwarded-For 配置方案进行举例介绍:

- IIS 7 配置方案
- Apache 配置方案
- Nginx 配置方案

IIS 7 配置方案



- 下载与安装插件 F5XForwardedFor 模块,根据自己的服务器操作系统版本将 x86\Release 或者 x64\Release 目录 下的 F5XFFHttpModule.dll和F5XFFHttpModule.ini 拷贝到某个目录,这里假设为 C:\F5XForwardedFor,确保 IIS 进程对该目录有读取权限。
- 2. 选择 IIS 服务器,双击模块功能。

3. 单击**配置本机模块**。

4. 在弹出框中单击注册。

5. 添加下载的 DLL 文件, 如下图所示:

6. 添加完成后,勾选并单击确定。

7. 在 IIS 服务器的 "ISAPI 和 CGI 限制"中,添加如上两个 DLL,并将限制设置为允许。

8. 重启 IIS 服务器,等待配置生效。

Apache 配置方案

1. 安装 Apache 第三方模块"mod_rpaf", 需执行如下命令:

```
wget http://stderr.net/apache/rpaf/download/mod_rpaf-0.6.tar.gz
tar zxvf mod_rpaf-0.6.tar.gz
cd mod_rpaf-0.6
/usr/bin/apxs -i -c -n mod_rpaf-2.0.so mod_rpaf-2.0.c
```

2. 修改 Apache 配置 /etc/httpd/conf/httpd.conf, 需在最末尾添加:

```
LoadModule rpaf_module modules/mod_rpaf-2.0.so
RPAFenable On
RPAFsethostname On
RPAFproxy_ips IP地址 //IP 地址为通道的转发IP
RPAFheader X-Forwarded-For
```



3. 添加完成后,重启 Apache。

/usr/sbin/apachectl restart

Nginx 配置方案

 当 Nginx 作为服务器时,获取客户端真实 IP,需使用 http_realip_module 模块,默认安装的 Nginx 是没有编译 http_realip_module 模块的,需要重新编译 Nginx,在configure 增加 --with-http_realip_module 选项,确保 http_realip_module 模块编译进 nginx 中。编译代码如下:

```
wget http://nginx.org/download/nginx-1.14.0.tar.gz
tar zxvf nginx-1.14.0.tar.gz
cd nginx-1.14.0
./configure --user=www --group=www --with-http_stub_status_module --without-htt
p-cache --with-http_ssl_module --with-http_realip_module
make
make install
```

2. 修改 nginx.conf。

```
vi /etc/nginx/nginx.conf
修改如下红色部分:
fastcgi connect_timeout 300;
fastcgi send_timeout 300;
fastcgi read_timeout 300;
fastcgi buffer_size 64k;
fastcgi buffers 4 64k;
fastcgi busy_buffers_size 128k;
fastcgi temp_file_write_size 128k;
set_real_ip_from IP地址; //IP 地址为通道转发IP
real_ip_header X-Forwarded-For;
```

3. 重启 Nginx。

service nginx restart



国家与地区映射关系

最近更新时间:2023-06-30 11:48:24

由于世界各国疆域面积各异,为了方便数据展示及加速点广泛覆盖,全球应用加速对一些距离相近的国家进行加速 区域合并。同时,对一些疆域面积较大的国家,全球应用加速进行区域拆分,以提高用户使用体验。当您使用"**全球** 统一域名接入"功能,选择加速点覆盖区域时,可参照下表的国家与地区映射关系,配置全球加速点的覆盖区域。

大洲	地理分区	国家/地区	省/州
亚洲		中国大陆-华东	山东、江苏、安徽、浙江、江西、福建、上海
		中国大陆-华南	广东、广西、海南
		中国大陆-华中	湖北、湖南、河南
		中国大陆-华北	北京、天津、河北、山西、内蒙古
		中国大陆-西北	宁夏、新疆、青海、陕西、甘肃
	东亚	中国大陆-西南	四川、云南、贵州、西藏、重庆
		中国大陆-东北	辽宁、吉林、黑龙江
		蒙古国	
		朝鲜	
东西		韩国	
		日本	
	东南亚	文莱	
		中国澳门	
		柬埔寨	
		东帝汶	
		印度尼西亚	
		老挝	
		马来西亚	
		缅甸	



	菲律宾	
	中国香港	
	新加坡	
	中国台湾	
	泰国	
	越南	
	孟加拉	
	不丹	
	印度	
南亚	马尔代夫	
	尼泊尔	
	巴基斯坦	
	斯里兰卡	
	哈萨克斯坦	
	吉尔吉斯斯坦	
中亚	塔吉克斯坦	
	土库曼斯坦	
	乌兹别克斯坦	
西亚	阿富汗	
	伊拉克	
	伊朗	
	叙利亚	
	约旦	
	黎巴嫩	
	以色列	



		巴勒斯坦	
		沙特阿拉伯	
		巴林	
		卡塔尔	
		科威特	
		阿联酋	
		阿曼	
		也门	
		格鲁吉亚	
		亚美尼亚	
		阿塞拜疆	
		土耳其	
		塞浦路斯	
欧洲		芬兰	
		瑞典	
	-1レ <i>び</i> /2	挪威	
	1664	冰岛	
		丹麦	
		法罗群岛	
		爱沙尼亚	
		拉脱维亚	
		立陶宛	
	示以	白俄罗斯	
		乌克兰	
		摩尔多瓦	



中欧	波兰	
	捷克	
	斯洛伐克	
	匈牙利	
	德国	
	奥地利	
	瑞士	
	列支敦士登	
	英国	
	爱尔兰	
	荷兰	
西欧	比利时	
	卢森堡	
	法国	
	摩纳哥	
南欧	罗马尼亚	
	保加利亚	
	塞尔维亚	
	马其顿	
	阿尔巴尼亚	
	希腊	
	斯洛文尼亚	
	克罗地亚	
	波斯尼亚和墨塞哥 维那	
	意大利	



		梵蒂冈	
		圣马力诺	
		马耳他	
		西班牙	
		葡萄牙	
		安道尔	
非洲		埃及	
		利比亚	
		苏丹	
	北非	突尼斯	
		阿尔及利亚	
		摩洛哥	
		马德拉群岛	
		埃塞俄比亚	
		厄立特里亚	
	左出	索马里	
		吉布提	
		肯尼亚	
	21/21	坦桑尼亚	
		乌干达	
		卢旺达	
		布隆迪	
		塞舌尔	
	中非	乍得	
		中非	



	喀麦隆
	赤道几内亚
	加蓬
	刚果(布)
	刚果(金)
	圣多美及普林西比
	毛里塔尼亚
	塞内加尔
	冈比亚
	马里
	布基纳法索
	几内亚
	几内亚比绍
而非	佛得角
	塞拉利昂
	利比里亚
	科特迪瓦
	加纳
	多哥
	尼日利亚
	贝宁
	尼日尔
南非	赞比亚
	安哥拉
	津巴布韦



		马拉维	
		莫桑比克	
		博茨瓦纳	
		纳米比亚	
		南非	
		斯威士兰	
		莱索托	
		马达加斯加	
		科摩罗	
		毛里求斯	
		留尼旺	
大洋洲	大洋洲	澳大利亚	
		新西兰	
		巴布亚新几内亚	
		所罗门群岛	
		瓦努阿图	
		密克罗尼西亚	
		马绍尔群岛	
		帕劳	
		瑙鲁	
		基里巴斯	
		图瓦卢	
		萨摩亚	
		斐济群岛	
		汤加	



		库克群岛	
		关岛	
		新克里多尼亚	
		瓦利斯与富图纳	
		纽埃	
		托克劳	
		美属萨摩亚	
		北马里亚纳	
北美洲		加拿大	
	北美	美国东部	缅因州、新罕布什尔州、佛蒙特州、马萨诸塞州、罗得岛 州、康涅狄格州、纽约州、宾夕法尼亚州、新泽西州、特 拉华州、马里兰州、华盛顿哥伦比亚特区、弗吉尼亚州、 西弗吉尼亚州、北卡罗来纳州、南卡羅萊納州、佐治亚 州、佛罗里达州、肯塔基州、田纳西州、密西西比州、亚 拉巴马州
		美国西部	爱达荷州、蒙大拿州、怀俄明州、内华达州、犹他州、科 罗拉多州、亚利桑那州、新墨西哥州、阿拉斯加州、华盛 顿州、俄勒冈州、加利福尼亚州、夏威夷州
		美国中部	威斯康星州、密歇根州、伊利诺伊州、印第安纳州、俄亥 俄州、密苏里州、北达科他州、南达科他州、内布拉斯加 州、堪萨斯州、明尼苏达州、艾奥瓦州、俄克拉何马州、 德克薩斯州、阿肯色州、路易斯安那州
		墨西哥	
		格陵兰	
	中美洲	危地马拉	
		伯利兹	
		萨尔瓦多	
		洪都拉斯	
		尼加拉瓜	
		哥斯达黎加	



	巴拿马	
加勒比海区	巴哈马	
	古巴	
	牙买加	
	海地	
	多米尼加	
	安提瓜和巴布达	
	圣基茨和尼维斯	
	多米尼克	
	圣卢西亚	
	圣文森特和格林纳 丁斯	
	格林纳达	
	巴巴多斯	
	特立尼达和多巴哥	
	波多黎各	
	英属维尔京群岛	
	美属维尔京群岛	
	安圭拉	
	蒙特塞拉特	
	瓜德罗普	
	马提尼克	
	荷兰加勒比区	
	阿鲁巴	
	特克斯和凯科斯群	



		开曼群岛	
		百慕大	
		哥伦比亚	
		委内瑞拉	
	南美洲北部	圭亚那	
		法属圭亚那	
		苏里南	
		厄瓜多尔	
南美洲	南美洲中西 部	秘鲁	
		玻利维亚	
	南美洲东部	巴西	
		智利	
		阿根廷	
	的天伽的印	乌拉圭	
		巴拉圭	