ALIBABA CLOUD

阿里云

全球加速

监控与运维

文档版本：20220310

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.查看带宽连接监控

结合阿里云云监控服务，您可以查看全球加速的云监控数据，例如加速地域的出方向和入方向带宽、终端节点组所在地域的出方向和入方向带宽以及加速IP并发连接数。

操作步骤

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，单击**监控**列下的图标查看监控。

   您可以通过以下操作，筛选要查看监控的地域和时间周期。

   - 单击**地域**，在下拉列表中选择要查看的地域。
   - 单击**时间**，在下拉列表中选择要查看的时间周期。

     系统默认为您展示最近一小时内的监控数据。

   监控指标说明如下：

监控指标	说明
加速地域	
加速IP入向带宽	从外部访问全球加速实例一个加速地域所消耗的带宽。单位（默认值）：bps。 您可以单击监控项后的单位**bps**，从单位列表中调整单位为Kbps、Mbps或Gbps。
加速IP出向带宽	全球加速实例一个加速地域访问外部所消耗的带宽。单位（默认值）：bps。 您可以单击监控项后的单位**bps**，从单位列表中调整单位为Kbps、Mbps或Gbps。
加速IP并发连接数	全球加速实例一个加速地域所有的连接数。
终端节点地域	
终端节点组所在地域入方向带宽	全球加速实例访问一个地域的终端节点组所消耗的带宽。单位（默认值）：bps。 您可以单击监控项后的单位**bps**，从单位列表中调整单位为Kbps、Mbps或Gbps。
终端节点组所在地域出方向带宽	一个地域的终端节点组访问全球加速实例所消耗的带宽。单位（默认值）：bps。 您可以单击监控项后的单位**bps**，从单位列表中调整单位为Kbps、Mbps或Gbps。

2.创建阈值报警规则

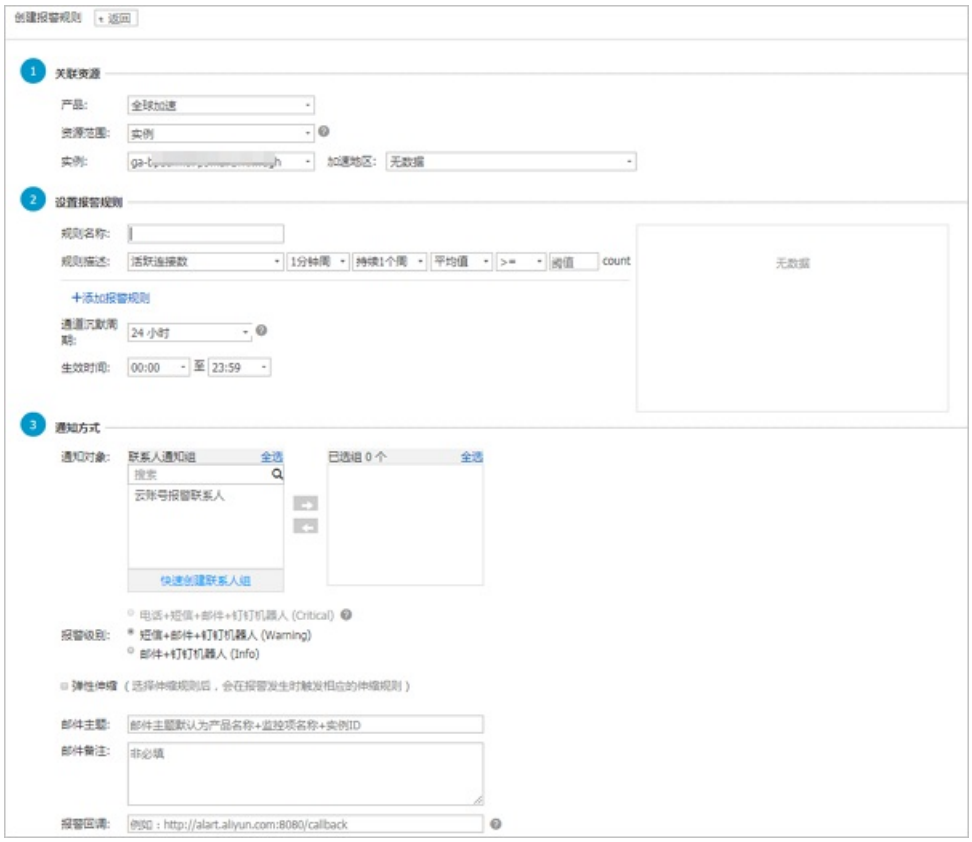
如果您需要监控全球加速实例的使用和运行情况，您可以通过创建阈值报警规则，实时监控全球加速实例运行情况，保证业务的稳定。

背景信息

如果全球加速实例被删除，其在云监控设置的阈值报警规则也会随之删除。

操作步骤

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**监控**列单击图标。
3. 在**实例监控**页面，单击**阈值报警设置**。
4. 在**报警规则列表**页面，单击**创建报警规则**。
5. 在**创建报警规则**页面，配置**关联资源**、**设置报警规则**和**通知方式**。



- **产品**：选择**全球加速**。
- **资源范围**：选择报警规则的作用范围。
  - **全部资源**：表示报警规则作用在当前阿里云账号下所有的全球加速实例上。
  - **实例**：表示报警规则只作用在当前阿里云账号下指定的全球加速实例上。

    您还需要进一步选择全球加速实例ID和所在地域。
- **规则描述**：报警规则的主体，定义在监控数据满足何种条件时，触发报警规则。全球加速支持监控以下监控项：

监控项	说明
活跃连接数	全球加速实例所有ESTABLISHED状态的连接个数。
入方向带宽	从外部访问全球加速实例所消耗的带宽。单位：bit/s。
入方向丢弃包速率	全球加速实例每秒丢弃的入方向数据包个数。单位：pps。
入方向包速率	全球加速实例每秒接收的数据包个数。单位：pps。
出方向带宽	全球加速实例访问外部所消耗的带宽。单位：bit/s。
出方向丢弃包速率	全球加速实例每秒丢弃的出方向数据包个数。单位：pps。
出方向包速率	全球加速实例每秒发出的数据包个数。单位：pps。
终端节点组所在地域入方向带宽	全球加速实例访问一个地域的终端节点组所消耗的带宽。单位：bit/s。
终端节点组所在地域入方向丢弃包速率	一个地域的终端节点组每秒丢弃的入方向数据包个数。单位：pps。
终端节点组所在地域入方向包速率	一个地域的终端节点组每秒接收的数据包个数。单位：pps。
终端节点组所在地域出方向带宽	一个地域的终端节点组访问全球加速实例所消耗的带宽。单位：bit/s。
终端节点组所在地域出方向丢弃包速率	一个地域的终端节点组每秒丢弃的出方向数据包个数。单位：pps。
终端节点组所在地域出向包速率	一个地域的终端节点组每秒发出的数据包个数。单位：pps。
全球加速丢弃包速率_目标IP	开启延时监控后，探测报文通过全球加速实例访问目标终端节点每秒丢弃的数据包个数。单位：pps。
全球加速延时_目标IP	开启延时监控后，探测报文通过全球加速实例访问目标终端节点的时延。单位：s。
公网丢弃包速率_目标IP	开启延时监控后，探测报文通过公网访问目标终端节点每秒丢弃的数据包个数。单位：pps。
公网延时_目标IP	开启延时监控后，探测报文通过公网访问目标终端节点的时延。单位：s。

其他参数配置，请参见创建报警规则。

6. 单击**确认**。

相关文档

- PutResourceMetricRule
- CreateGroupMetricRules

3.保持客户端源IP

全球加速GA（Global Accelerator）支持保持客户端源IP功能，后端服务器可以通过该功能获取发起访问的客户端源IP。本文为您介绍在不同场景中如何开启保持客户端源IP功能以及后端服务器如何获取客户端源IP。

前提条件

您已经在全球加速实例中配置了监听。具体操作，请参见添加和管理监听。

背景信息

通过全球加速服务加速客户端访问后端服务器，默认情况下后端服务器只能获取客户端通过全球加速访问后端服务器的终端节点组出公网IP，不能获取客户端的源IP。如果您需要后端服务器能获取客户端的源IP，您可以开启全球加速的保持客户端源IP功能。全球加速保持客户端源IP功能根据监听协议的不同，支持的情况也不同：

- **HTTP和HTTPS**：支持保持客户端源IP功能。全球加速将客户端源IP保存在HTTP请求头的`X-Forwarded-For`字段中，后端服务器可以通过`X-Forwarded-For`字段获取客户端源IP。
- **UDP**：不支持保持客户端源IP功能。
- **TCP**：支持保持客户端源IP功能。但根据后端服务类型不同，需要后端服务器做相应适配以获取客户端源IP。关于适配说明，请参见下表：

后端服务部署地	后端服务类型	是否支持获取客户端源IP	是否需要后端服务器适配
阿里云	阿里云公网IP	支持	不需要 在您开启保持客户端源IP功能后，后端服务器可直接获取发起访问的客户端源IP，无需添加任何配置。
	阿里云云服务器ECS（Elastic Compute Service）实例	支持	
	传统型负载均衡CLB（Classic Load Balancer）实例	支持 请注意在以下情形中，后端服务器无法获取客户端源IP： ○ 您的CLB实例的后端服务器为经典网络类型的ECS实例。 ○ 您的CLB实例的监听协议为HTTP或HTTPS。	
	应用型负载均衡ALB（Application Load Balancer）实例	支持	
	对象存储服务OSS（Object Storage Service）	不支持	

后端服务部署地	后端服务类型	是否支持获取客户端源IP	是否需要后端服务器适配
非阿里云	自定义IP	支持	需要 在您开启保持客户端源IP功能的情况下，全球加速会使用Proxy Protocol保持客户端源IP，此时需要后端服务器支持解析Proxy Protocol，才能获取到客户端源IP信息。 **注意** 如果您的后端服务器不支持解析Proxy Protocol，则会导致后端服务器无法正确解析加速流量。
	自定义域名	支持	

说明

Proxy Protocol是一种Internet协议，通过为TCP报文添加Proxy Protocol报头来获取客户端源IP。

Proxy Protocol的接收端必须在接收到完整有效的Proxy Protocol头部后才能开始处理连接数据，因此对于服务器中的同一个监听端口，不能同时接收携带Proxy Protocol和未携带Proxy Protocol的连接请求。如果接收到的第一个数据包不符合Proxy Protocol格式，那么服务器会直接终止连接。

通过HTTP或HTTPS监听协议加速访问后端服务

如果您通过HTTP或HTTPS监听协议加速您后端服务的访问，默认开启保持客户端源IP功能，后端服务器可直接通过HTTP请求头的`X-Forwarded-For`字段获取客户端源IP。

1. 开启保持客户端源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，您可以通过`X-Forwarded-For`获取客户端源IP。

2. 获取客户端源IP。

   后端服务器收到的HTTP请求头中的`X-Forwarded-For`字段如下，其中第一个IP即为客户端源IP。

   ```
   X-Forwarded-For: 客户端源IP, 代理服务器1-IP, 代理服务器2-IP, ...
   ```

通过TCP监听协议加速访问阿里云后端服务

如果您通过TCP监听协议加速您的后端服务访问，且您的后端服务部署在阿里云上，那么您开启保持客户端源IP功能后，后端服务器可直接获取客户端源IP信息。

1. 开启保持客户端源IP。
   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，找到目标监听，在**操作**列单击**编辑监听**。
   iv. 在**配置监听和协议**配置向导页面，单击**下一步**。

v. 在**配置终端节点**配置向导页面，打开**保持客户端源IP**开关，然后单击**下一步**。

当后端服务部署在阿里云上时，**获取客户端真实IP方式**默认选择为**自动获取**。

- **自动获取**：IPv4客户端访问后端服务，推荐使用此方式。此方式可以自动获取客户端IP，后端服务无需做任何改动。当后端服务部署在非阿里云时，不支持使用该方式。
- **ProxyProtocol**：IPv6客户端访问后端服务，推荐使用此方式。此方式需要后端服务器支持解析Proxy Protocol，才能获取到客户端源IP信息。

更多信息，请参见背景信息。

vi. 在**配置审核**页面，确认无误后，单击**提交**。

2. 获取的客户端源IP。

本部分以后端服务类型为阿里云Linux ECS实例为例，介绍如何查看已获取的客户端源IP。

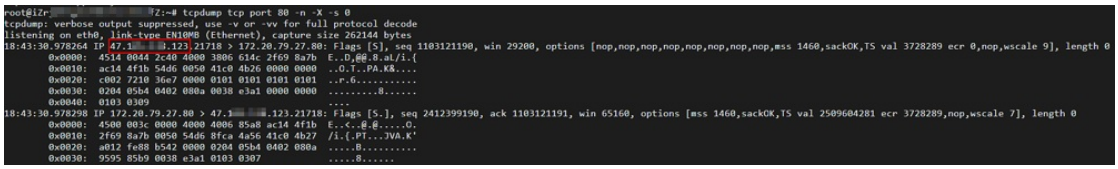
i. 登录后端Linux ECS服务器。

ii. 执行以下命令，抓取HTTP流量。

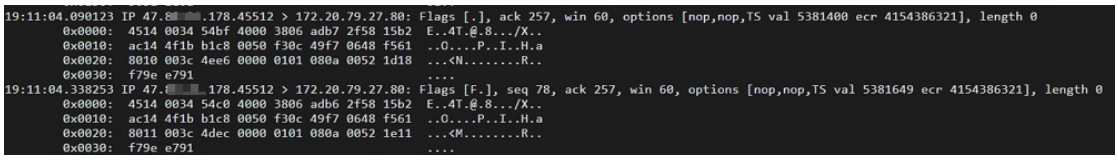
```
tcpdump tcp port [监听端口] -n -X -s 0
```

iii. 从抓取的数据包中筛选信息，查看客户端源IP。

经测试，开启保持客户端源IP功能后，可以在后端服务器查看客户端源IP。



未开启保持客户端源IP功能，只能在后端服务器上查看到客户端通过全球加速访问后端服务器的终端节点组出公网IP。



通过TCP监听协议加速访问非阿里云后端服务

如果您通过TCP监听协议加速您的后端服务访问，且您的后端服务部署在非阿里云上，那么您的后端服务需要支持解析Proxy Protocol，才能获取到客户端源IP。本部分以Nginx为例，为您说明后端服务如何支持解析Proxy Protocol以及如何获取客户端源IP。

1. 开启保持客户端源IP。
   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，找到目标监听，在**操作**列单击**编辑监听**。
   iv. 在**配置监听和协议**配置向导页面，单击**下一步**。

v. 在**配置终端节点**配置向导页面，打开**保持客户端源IP**开关，然后单击**下一步**。

当后端服务部署在非阿里云上时，**获取客户端真实IP方式**默认选择为**ProxyProtocol**。

- **自动获取**：IPv4客户端访问后端服务，推荐使用此方式。此方式可以自动获取客户端IP，后端服务无需做任何改动。当后端服务部署在非阿里云时，不支持使用该方式。
- **ProxyProtocol**：IPv6客户端访问后端服务，推荐使用此方式。此方式需要后端服务器支持解析Proxy Protocol，才能获取到客户端源IP信息。
-

更多信息，请参见背景信息。

vi. 在**配置审核**页面，确认无误后，单击**提交**。

2. 配置Nginx使其支持解析Proxy Protocol。

Nginx的 `http{}` 和 `stream{}` 模块均可以接收Proxy Protocol，在 `http{}` 模块或 `stream{}` 模块中添加相应处理Proxy Protocol的端口即可。

```
http {
    #...
    server {
        listen 8080 proxy_protocol;     #在8080端口，开启解析proxy protocol。
        #...
    }
}
stream {
    #...
    server {
        listen 1235 proxy_protocol;     #在1235端口，开启解析proxy protocol。
        #...
    }
}
```

3. 获取客户端源IP。

在开始解析Proxy Protocol后，Nginx会将客户端源IP保存在变量proxy_protocol_addr中。因此，您可

以通过以下两种方式获取客户端源IP：

- 对于HTTP流量，您可以将客户端源IP保存在HTTP请求头字段中：

```
http {
    proxy_set_header X-Real-IP       $proxy_protocol_addr;
    proxy_set_header X-Forwarded-For $proxy_protocol_addr;
}
```

后端服务器通过HTTP请求头中的 `X-Forwarded-For` 字段获取源IP，其中第一个IP即为客户端源IP。

```
X-Forwarded-For: 客户端源IP，代理服务器1-IP， 代理服务器2-IP，...
```

- 对于HTTP流量或TCP流量，您也可以将客户端源IP保存在日志中，然后通过日志信息获取客户端源IP。

  a. 设置 `http{}` 模块和 `stream{}` 模块的日志格式，将客户端源IP信息保存到日志中。

```
http {
    #...
    log_format combined '$proxy_protocol_addr - $remote_user [$time_local] ' ##在http{}模块的日志格式中添加保存客户端源IP的变量proxy_protocol_addr。
                        '"$request" $status $body_bytes_sent '
                        '"$http_referer" "$http_user_agent"';
}
#...
stream {
    #...
    log_format basic '$proxy_protocol_addr - [$time_local] '                  ##在stream{}模块的日志格式中添加保存客户端源IP的变量proxy_protocol_addr。
                     '$protocol $status $bytes_sent $bytes_received '
                     '$session_time';
}
```

  b. 通过以下命令查看日志信息，获取客户端源IP。

```
tail -n -5 <日志路径>
```

以下内容为您展示一个完整的配置示例：

```
worker_processes  4;
events {
    worker_connections  1024;
}
http {
    include       mime.types;
    default_type  application/octet-stream;
    log_format  main  '$proxy_protocol_addr $remote_addr - $remote_user [$time_local] "
$request" '##在http{}模块日志格式中添加保存客户端源IP的变量proxy_protocol_addr。
                      '$status $body_bytes_sent "$http_referer" '
                      '"$http_user_agent" "$http_x_forwarded_for"';
    sendfile        on;
    keepalive_timeout  65;
    upstream backend {
        server 192.XX.XX.36:8080;
        server 192.XX.XX.37:8080;
        keepalive 2000;
    }
    server {
        listen       80 proxy_protocol;                          ##在80端口，开启解析prox
y protocol。
        server_name  example.com;
        proxy_set_header X-Real-IP       $proxy_protocol_addr;   ##在发给后端服务时，将客
户端源IP信息插入到HTTP中。
        proxy_set_header X-Forwarded-For $proxy_protocol_addr;
        access_log  /var/log/nginx/access.log  main;
        location / {
            proxy_pass http://backend;
            proxy_http_version 1.1;
            proxy_set_header Connection "";
        }
    }
}
stream {
    log_format tcp_basic '$proxy_protocol_addr - [$time_local] '  ##在stream{}模块的日志
格式中添加保存客户端源IP的变量proxy_protocol_addr。
                      '$protocol $status $bytes_sent $bytes_received '
                      '$session_time';
    upstream stream_backend {
        server 192.XX.XX.36:2003;
        server 192.XX.XX.37:2003;
    }
    server {
        listen 1234 proxy_protocol;                               ##在1234端口，开启解析p
roxy protocol。
        access_log  /var/log/nginx/access_tcp.log  tcp_basic;
        proxy_pass stream_backend;
    }
}
```

查看日志信息，其中日志信息中的第一个IP地址即为客户端源IP。

```
[root@iZ2zefu      sf638txqeZ ~]# tail -n 5 /var/log/nginx/access.log
42.      .128 123      .195 - - [19/Nov/2020:15:34:00 +0800] "GET /info HTTP/1.1" 200 115 "-" "curl/7.64.1" "-"
42.      .128 123      .158 - - [19/Nov/2020:15:34:01 +0800] "GET /info HTTP/1.1" 200 115 "-" "curl/7.64.1" "-"
42.      .128 123.      .50 - - [19/Nov/2020:15:34:59 +0800] "GET /info HTTP/1.1" 200 115 "-" "curl/7.64.1" "-"
42.      .128 39.      5.250 - - [19/Nov/2020:15:35:40 +0800] "GET /info HTTP/1.1" 200 115 "-" "curl/7.64.1" "-"
42.      .128 123.      .158 - - [19/Nov/2020:15:35:45 +0800] "GET /info HTTP/1.1" 200 115 "-" "curl/7.64.1" "-"
[root@iZ2zefu      f638txqeZ ~]# tail -n 5 /var/log/nginx/access_tcp.log
42.      .128 - [19/Nov/2020:15:39:10 +0800] TCP 200 12 12 0.046
42.      .128 - [19/Nov/2020:15:39:21 +0800] TCP 200 12 12 0.041
```

4.测试TCP监听协议的加速效果

如果您的全球加速配置的监听协议是TCP协议，您可以通过curl命令测试全球加速的加速效果。

前提条件

开始前，请确保满足以下条件。

- 您已经添加了监听，且监听协议为TCP协议。详细信息，请参见添加和管理监听。
- 您已经在终端节点服务器上将监听端口添加到安全配置（例如安全组）白名单中。

背景信息

全球加速采用四层（TCP/UDP协议）转发模式，无法使用ICMP Ping和TCPing测试TCP监听协议的加速效果，但您可以通过curl命令测试TCP监听协议的加速效果。

操作步骤

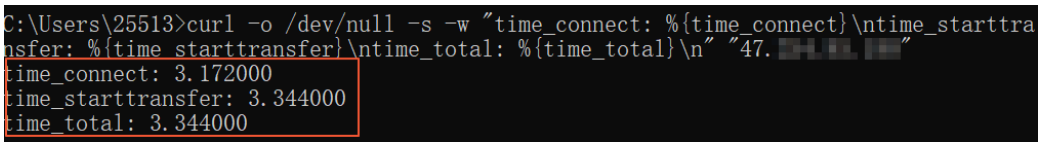
1. 在加速地域的电脑中打开命令行窗口。
2. 在配置全球加速前后分别执行以下命令，对比数据包延迟情况。

```
curl -o /dev/null -s -w "time_connect: %{time_connect}\ntime_starttransfer: %{time_starttransfer}\ntime_total: %{time_total}\n" "http[s]://<IP或域名>[:<端口>]"
```

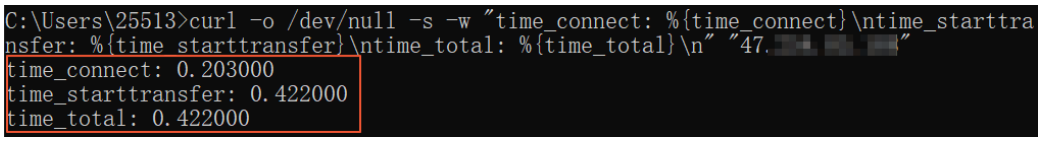
其中：

- time_connect：连接时间，从开始到建立TCP连接完成所用的时间，单位为秒。
- time_starttransfer：开始传输时间。在客户端发出请求后，到后端服务器响应第一个字节所用的时间，单位为秒。
- time_total：连接总时间。客户端发出请求后，到后端服务器响应会话所用的时间，单位为秒。

加速前的访问延迟情况



加速后的访问延迟情况



相关文档

- 测试UDP监听协议的加速效果

5.测试UDP监听协议的加速效果

如果您的全球加速配置的监听协议是UDP协议，您可以通过UDPing测试全球加速的加速效果，UDPing使用特定的端口号将UDP ping发送到特定的IP地址。本文以终端节点服务器和客户端都为CentOS系统为例，介绍如何通过UDPing测试UDP监听协议的网络加速效果。

前提条件

开始前，请确保满足以下条件。

- 您已经添加了监听，且监听协议为UDP协议。详细信息，请参见添加和管理监听。
- 您已经在终端节点服务器上将监听端口添加到安全配置（例如安全组）白名单中。

背景信息

全球加速采用四层（TCP/UDP协议）转发模式，无法使用ICMP Ping和TCPing测试UDP监听协议的加速效果，但您可以使用UDPing测试UDP监听协议的加速效果。

UDP是数据报机制，无会话连接，直接将UDP报文转发给终端节点组中的终端节点。

步骤一：在终端节点服务器上部署UDP Echo服务

要使用UDPing测试加速效果，终端节点服务器必须部署UDP Echo服务。本示例使用Socat模拟UDP服务端为例，介绍如何部署UDP Echo服务。

1. 执行以下命令，安装Socat。
   ```
   yum install socat
   ```
2. 执行以下命令，启动Socat。
   ```
   nohup socat -v UDP-LISTEN:<监听端口>,fork PIPE 2>/dev/null &
   ```

步骤二：在客户端部署UDPing工具

完成以下操作，在客户端部署UDPing工具。

1. 执行以下命令，下载UDPing工具。
   ```
   wget https://networktools-public.oss-cn-hangzhou.aliyuncs.com/ga/udping/udping.py
   ```
2. 执行以下命令，赋予UDPing工具执行权限。
   ```
   chmod +x udping.py
   ```

步骤三：测试加速效果

1. 登录客户端。
2. 执行 `./udping.py <后端服务器IP> <监听端口>` ，查看未使用全球加速客户端访问后端服务器的网络延迟。
3. 执行 `./udping.py <加速IP> <监听端口>` ，查看使用全球加速后客户端通过加速IP访问后端服务器的网络延迟。

> 说明
>
> - 全球加速的加速效果以您的实际业务测试为准。
> - 加速IP是您添加加速区域后为加速地域分配的加速IP。
> - 下图以上海到美国（弗吉尼亚）的加速效果作为示例。

未使用全球加速，客户端访问后端服务器的网络延迟

```
[root@ gwx4wqrjjn9Z ~]# ./udping.py 47.  .73 4000
udping 47  .73 via port 4000 with 64 bytes of payload
Reply from 47.  .73 seq=0 time=265.93 ms
Reply from 47.  .73 seq=1 time=265.50 ms
Reply from 47.  .73 seq=2 time=265.50 ms
Reply from 47.  .73 seq=3 time=265.52 ms
Reply from 47.  .73 seq=4 time=265.49 ms
^C
--- ping statistics ---
5 packets transmitted, 5 received, 0.00% packet loss
rtt min/avg/max = 265.49/265.59/265.93 ms
```

使用全球加速后，客户端通过加速IP访问后端服务器的网络延迟

```
[root@ x4wqrjjn9Z ~]# ./udping.py 47.  .59 4000
udping 47  .59 via port 4000 with 64 bytes of payload
Reply from 47.  .59 seq=0 time=182.39 ms
Reply from 47.  .59 seq=1 time=181.74 ms
Reply from 47.  .59 seq=2 time=181.43 ms
Reply from 47.  .59 seq=3 time=181.42 ms
Reply from 47.  .59 seq=4 time=181.46 ms
^C
--- ping statistics ---
5 packets transmitted, 5 received, 0.00% packet loss
rtt min/avg/max = 181.42/181.69/182.39 ms
```

相关文档

- 测试TCP监听协议的加速效果