

边缘安全加速平台 EO

排障指南



腾讯云

【版权声明】

©2013–2025 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【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。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【服务声明】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。

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。

【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

排障指南

异常状态码参考

EdgeOne 4XX/5XX 状态码排障指南

520/524状态码排障指南

521/522 状态码排障指南

工具指南

诊断工具

自助诊断

协助诊断

自助调试

测速工具

性能监控

IP 归属查询

排障指南

异常状态码参考

最近更新时间：2025-08-14 11:23:51

EdgeOne 响应的异常状态码分为以下几类：

标准状态码

您可以参考 [HTTP 状态码标准](#) 来查看具体的状态码含义，这类状态码通常在以下情况下响应：

- 请求回源后，由源站响应的状态码信息，节点将透传源站响应的状态码返回给客户端。
- 由 EdgeOne 节点直接响应，例如：Token 鉴权不通过，响应 403 状态码。可能由 EdgeOne 节点直接响应的状态码包含以下状态码：

状态码	含义说明
400	客户端请求不合法，如请求 Method 不在 EdgeOne 的允许范围内。详情请参见 HTTP 限制说明 。
403	- 未通过防盗链校验，如规则引擎的 Token 鉴权。 - 触发合规封禁。
416	range 范围异常，如 rangeStart < 0、rangeStart > rangeEnd、rangeStart > FileSize。
418	对于接入 EdgeOne 的域名，系统会自动为域名分配服务节点，且对应的节点均会下发该域名的配置文件，其中文件内容取决于域名的配置，如源站、缓存、头部等。当请求发送给节点时，节点会读取域名的配置文件，当发现配置文件不存在时，则响应 418 状态码。 例如，客户端请求： <code>https://example.com/test.jpg</code> ，则节点会读取域名 <code>example.com</code> 的配置文件，可能由于绑定了非 <code>example.com</code> 域名的服务节点，CNAME 配置错误或者调度系统异常等原因，客户端会接收到 418 响应。
423	触发请求回环，即 CDN-Loop 头部的 Loops 数值 ≥ 16 ，详情请参见 CDN-Loop 。

EdgeOne 自定义的状态码

由 EdgeOne 自定义的特殊含义的状态码，包含 520-599 之间的状态码均为 EdgeOne 保留的自定义非标准状态码响应，建议您在业务中避免使用该范围内状态码，避免与 EdgeOne 的状态码产生混淆。

如下为 EdgeOne 自定义的异常状态码以及含义说明，方便您在业务访问异常时进行自助排障，更多排障详情请参见：[EdgeOne 4XX/5XX 状态码排障指南](#)。

状态码	含义说明
520/550	节点与源站建连成功后，向源站发起请求，但源站直接发送 RST 包，则节点响应客户端 520/550 状态码。
521/551	节点请求到源站，在 TCP 建连阶段，源站直接发送 RST 包，则节点响应客户端 521/551 状态码。
522/552	节点请求到源站，在 TCP 建连阶段，源站一直没有响应导致节点超时，则节点响应客户端 522/552 状态码。
523/553	若域名配置的源站为域名，则节点回源时，需要解析域名获取源站服务器 IP，若解析失败，则节点无法回源，响应客户端 523/553 状态码。
524/554	节点与源站建连成功后，向源站发起请求，源站一直没有响应导致节点超时，则节点响应客户端 524/554 状态码。
525/555	若回源协议为 HTTPS，则节点回源时需要与源站进行 SSL 握手，若握手失败，则节点响应客户端 525/555 状态码。
566	当请求被 Web 防护-托管规则 拦截时，默认使用 566 状态码和默认拦截页面响应请求。若用户配置了 自定义拦截状态码 ，则会使用用户配置的状态码。
567	当请求被 Web 防护-自定义规则 、 Web 防护-速率限制 或 Bot 管理 规则拦截时，默认使用 567 状态码和默认拦截页面响应请求。若用户配置了 自定义拦截状态码 ，则会使用用户配置的状态码。
570	触发平台级访问限频。
545	边缘函数执行异常，如函数引用未定义的变量。

EdgeOne 4XX/5XX 状态码排障指南

最近更新时间：2025-08-27 18:01:32

在接入 EdgeOne 后，如果您的业务请求出现 4XX/5XX 状态码，您可以参照如下的常见原因和解决思路进行排查。

❗ 说明：

若您参照以下排障指南仍然无法解决问题，您可以 [联系我们](#) 进行排查。为了方便定位，请您提供 [EO-LOG-UUID](#) 信息。若没有，请提供以下详细信息：

- 用户 IP、EdgeOne 节点 IP；
- 特定的 4XX、5XX 错误代码和消息；
- 发生 4XX、5XX 错误的时间和时区；
- 导致 HTTP 4XX、5XX 错误的 URL（例如：<https://www.example.com/images/icons/image1.png>）。

HTTP 400

1. 含义：服务器因某些被认为是客户端错误的原因（例如，请求语法错误、无效请求消息格式或者欺骗性请求路由），而无法或不会处理该请求。

2. 可能的原因及解决思路：

- 源站响应：直接访问源站测试，若源站响应 400，则修改源站配置或修改客户端请求行为以获取正确响应。
- EdgeOne 节点响应：
 - 请检查请求方法是否在 EdgeOne 支持的范围内，非以下请求方法，EdgeOne 节点将直接响应 400 状态码。
GET、HEAD、POST、PUT、DELETE、TRACE、CONNECT、OPTIONS、PATCH、COPY、LOCK、MKCOL、MOVE、PROPFIND、PROPPATCH、UNLOCK。
 - 协议格式错误，如使用 443 端口访问 HTTP。
 - HTTP 请求不符合 RFC 规范。

HTTP 403

1. 含义：服务器因某些被认为是客户端错误的原因（例如，请求语法错误、无效请求消息格式或者欺骗性请求路由），而无法或不会处理该请求。

2. 可能的原因及解决思路：

- 源站响应：直接访问源站测试，若源站响应 403，则修改源站配置或修改客户端请求行为以获取正确响应。
- EdgeOne 节点响应：常见的原因是未通过防盗链校验。
 - 请检查是否在规则引擎配置了 [HTTP 应答](#)，若有，看是否命中了如 Referer 黑白名单、IP 黑白名单、User-Agent 黑白名单等基础访问控制。
 - 请检查是否在规则引擎配置了 [Token 鉴权](#)，若有，核对客户端请求的 URL 是否时间戳过期或 MD5 加密串计算错误。
 - 请检查是否通过边缘函数配置了 [远程鉴权](#)，若有，核对客户端请求的 URL 是否符合鉴权服务器的校验放行规则。

HTTP 416

1. 含义：服务器无法处理所请求的数据区间。最常见的情况是所请求的数据区间不在文件范围之内，

2. 可能的原因及解决思路：

- 源站响应：直接访问源站测试，若源站响应 416，则修改源站配置或修改客户端请求行为以获取正确响应。
- EdgeOne 节点响应：
 - 异常的 range 范围，如：rangeStart < 0、rangeStart > rangeEnd、rangeStart > FileSize。
 - 客户端请求的 range 头部不标准。如请求 Range: Bytes=0-1023，而非 Range: bytes=0-1023。

HTTP 418

1. 含义：一般服务器使用这个响应来处理它们不想处理的请求。

2. 可能的原因及解决思路：

- 源站响应：直接访问源站测试，若源站响应 418，则修改源站配置或修改客户端请求行为以获取正确响应。
- EdgeOne 节点响应：对于接入 EdgeOne 的域名，系统会自动为域名分配服务节点，且对应的节点均会下发该域名的配置文件，其中文件内容取决于域名的配置，如源站、缓存、头部等。当请求到 EdgeOne 节点时，节点会读取域名的配置文件，当发现配置文件不存在时，则响应 418 状态码。
例如：客户端请求已接入 EdgeOne 的域名 <http://example.com/test.jpg>，该域名的请求配置在节点 [1.1.1.1](#)、[1.1.1.2](#) 上均有相关配置，则当域名请求到这两个节点时节点会读取域名 [example.com](#) 的配置文件，成功响应，如果请求到节点 [2.2.2.2](#) 上时，则会响应 418 状态码。
请检查域名是否绑定了非 [example.com](#) 域名的服务节点，CNAME 配置是否正确，若检查无问题，请 [联系我们](#) 处理。

HTTP 423

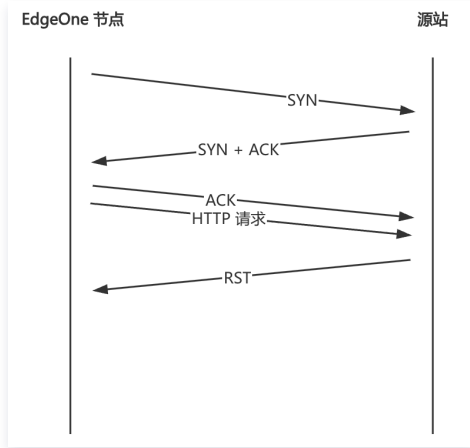
1. 含义：表示 "Locked"（已锁定），在接入 EdgeOne 的场景下，一般表示触发请求回环。

2. 可能的原因及解决思路：

- 源站响应：直接访问源站测试，若源站响应 423，则修改源站配置或修改客户端请求行为以获取正确响应。
- EdgeOne 节点响应：触发请求回环，即 CDN-Loop 头部的 Loops 数值 ≥ 16 ，详情请参见 [CDN-Loop](#)。一般常见于接入 EO 的加速域名，源站也设置为已接入 EO 或 CDN 加速的域名。

HTTP 520

1. 含义：EdgeOne 自定义的状态码。节点与源站 TCP 建连成功后，向源站发起 HTTP 请求，但源站直接发送 RST 包，则节点响应客户端 520 状态码。

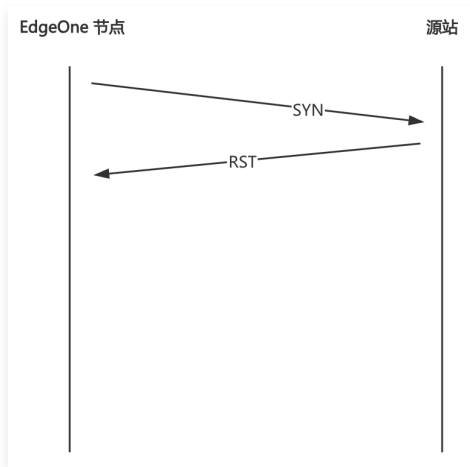


2. 可能的原因及解决思路：

源站服务异常：直接访问源站测试并抓包，查看源站针对 HTTP 请求是否响应 RST 包，可能是源站防火墙或自身服务异常导致。

HTTP 521

1. 含义：EdgeOne 自定义的状态码。节点请求到源站，在 TCP 建连阶段，源站直接发送 RST 包，则节点响应客户端 521 状态码。

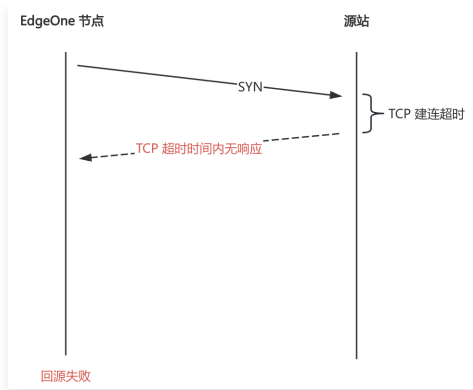


2. 可能的原因及解决思路：

源站服务异常：直接访问源站测试，可使用 curl 或 telnet 等命令工具，查看 TCP 连接是否能建连，通常是源站的某些端口未对公网开放或源站节点网络问题。

HTTP 522

1. 含义：EdgeOne 自定义的状态码。节点请求到源站，在 TCP 建连阶段，源站一直没有响应导致节点超时，则节点响应客户端 522 状态码。



2. 可能的原因及解决思路：

源站服务异常：直接访问源站测试，可使用 curl 或 telnet 等命令工具，查看 TCP 连接是否能建连，通常是源站的某些端口未对公网开放或源站节点网络问题。

HTTP 523

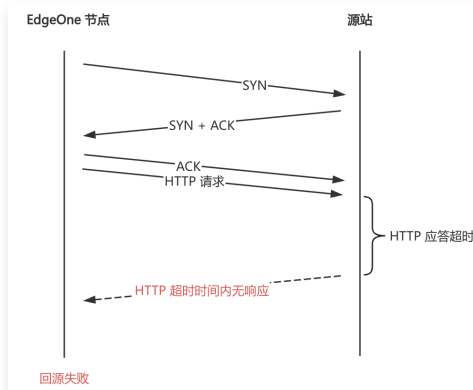
1. 含义：EdgeOne 自定义的状态码。若域名配置的源站为域名，则节点回源时，需要解析域名获取源站服务器 IP，若解析失败，则节点无法回源，响应客户端 523 状态码。

2. 可能的原因及解决思路：

- 尝试 dig 解析源站域名，确认是否能正常解析。
- 若源站域名能正常解析，请 [联系我们](#) 处理。

HTTP 524

1. 含义：EdgeOne 自定义的状态码。节点与源站建连成功后，向源站发起请求，源站一直没有响应导致节点超时，则节点响应客户端 524 状态码。

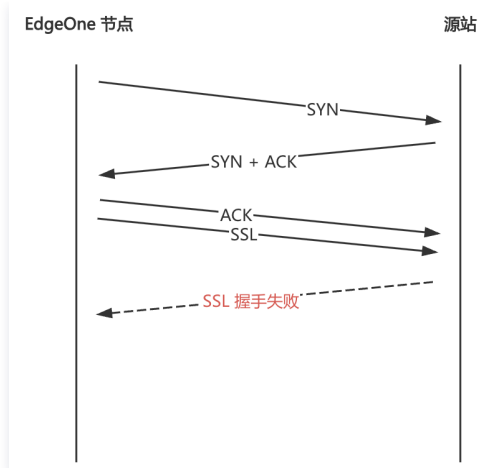


2. 可能的原因及解决思路：

源站服务异常：直接访问源站测试，查看针对 HTTP 请求是否有响应，若源站正常响应，可以尝试调整 [回源超时时间](#)。如果仍然有问题，请 [联系我们](#) 处理。

HTTP 525

1. 含义：EdgeOne 自定义的状态码。若回源协议为 HTTPS，则节点回源时需要与源站进行 SSL 握手，若握手失败，则节点响应客户端 525 状态码。



2. 可能的原因及解决思路：

- 请检查是否域名回源协议配置为 HTTPS，但源站没有部署证书。若是，可在域名管理处将回源协议修改为 HTTP，或者在源站部署对应域名的证书。
- 节点和源站 SSL 握手时由于网络原因出现丢包。

520/524状态码排障指南

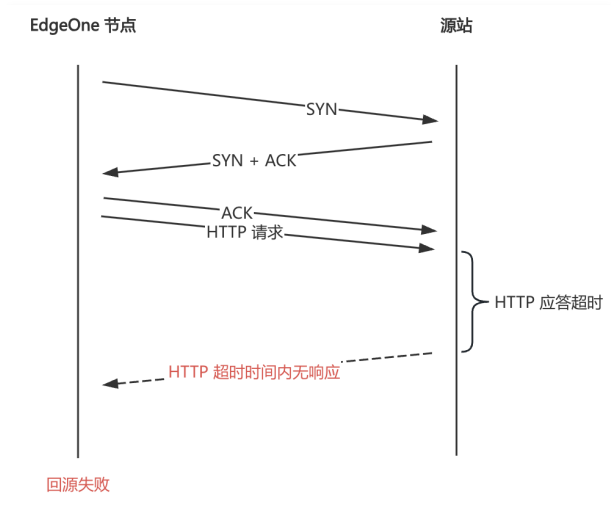
最近更新时间：2025-08-27 18:01:32

当您使用腾讯云 EdgeOne 加速站点访问资源后，客户端的请求将发送至 EdgeOne 节点，再回源到源站。因此如果访问过程中出现问题，可能涉及到多层网络链路的问题。当 EdgeOne 回源源站失败时则会出现 52x 的错误，本文档将为您介绍当出现 520/524 状态码时，您应该如何排查。

如下，以 524 状态码为例：

定义

524 状态码是 EdgeOne 自定义的状态码。节点与源站 TCP 建连成功后，向源站发起请求，源站一直没有响应导致节点超时，则节点响应客户端 524 状态码。其它状态码的含义请参考 [异常状态码参考](#)。



现象

```
curl -v http://www.example.com/test.jpg
* Trying 43.152.167.17...
* Connected to www.example.com (43.152.167.17) port 80 (#0)
> GET /test.jpg HTTP/1.1
> Host: www.example.com
> User-Agent: curl/7.79.1
> Accept: */*
> Proxy-Connection: Keep-Alive

* Mark bundle as not supporting multiuse
< HTTP/1.1 524 Receive timeout from origin
< Server: Edgeone_Spectrum_OCMID
< Date: Wed, 25 Oct 2023 10:16:27 GMT
< Content-Length: 0
< Connection: keep-alive
< Cache-Control: max-age=0
< EO-LOG-UUID: 16221131381683531888
<
* Connection #0 to host 43.152.162.17 left intact
```

可能的原因

- 源站自身服务异常
- 源站安全策略导致
- 运营商限制（HTTP）

排查方法

从第三方（非 CDN、源站）发起 HTTP/HTTPS 请求，指向源站测试，第三方可以是个人 PC、服务器、监测平台等。可以通过在服务器上使用命令行工具 CURL 来排查。

步骤一：确定回源配置信息

若您无特殊配置，则仅以「域名管理」处设置的源站、协议、以及端口为准即可。若有特殊配置，则可参照如下方法进行确定：

1. 源站 IP：源站 IP 需要根据「域名管理」配置的源站、源站组、负载均衡以及规则引擎「修改源站」的配置综合确定；
2. 回源协议：回源协议需要根据「域名管理」、规则引擎「回源 HTTPS」以及「修改源站」里的回源协议综合确定。
3. 回源端口：若无特殊配置，则为 80 或 443，若您在规则引擎「修改源站」操作中有修改回源端口，则以修改后的为准。
4. 回源 HOST：默认跟随加速域名，若您在规则引擎「Host Header 重写」操作中有进行设置，则以设置的为准。
5. 回源 Path：默认跟随请求 URL，若您在规则引擎「回源 URL 重写」操作中有进行修改，则以修改的为准。

步骤二：源站自身服务异常排查

使用命令行工具 curl，从第三方平台指向源站发起 HTTP/HTTPS 请求，测试方式为：

```
curl -vo/dev/null [协议]://[域名][path] --resolve [域名]:[端口]:[源ip]
```

注：CURL 版本保证在 7.21.3 版本以上。

假设回源使用 HTTP 协议、80 端口、源站 IP 为 1.1.1.1、回源 HOST 为 www.test.com、URL Path 为 /test.jpg，测试命令如下：

```
curl -vo/dev/null http://www.test.com/test.jpg --resolve www.test.com:80:1.1.1.1
```

从第三方客户端访问源站，如果源站返回空响应，则可能源站服务有问题，可自查源站服务是否有问题。如果源站返回正常或自查源站服务正常，则进入下一步继续排查。

步骤三：源站安全策略导致排查

可能的原因如下：

1. 源站有设置防火墙，EdgeOne 回源节点 IP 不在 IP 白名单里。

在源站上抓包或日志确认 EdgeOne 回源节点 IP 是否在源站 IP 白名单里，或者 CURL 获取 EO-LOG-UUID，提交给腾讯云技术支持，由技术支持查询 EdgeOne 回源节点的 IP，源站自查回源节点 IP 是否在源站的 IP 白名单里。其中，UUID 获取方法如下：

```
< Last-Modified: Mon, 24 Oct 2022 08:21:54 GMT
< Etag: "63564b22-264"
< Server: nginx/1.20.2
< Content-Type: text/html
< Content-Length: 612
< Accept-Ranges: bytes
< Connection: keep-alive
< Date: Wed, 08 Jan 2025 12:29:57 GMT
< EO-LOG-UUID: 4745437539590071077
```

2. 源站设置访问限频，EdgeOne 回源频率过高。

可指向源站并发起多个请求，验证能否复现源站返回空响应或超时的情况。如果可复现，通过源站日志排查频繁回源的请求（包含时间点、EdgeOne 回源节点 IP、URL），并将信息反馈给腾讯云技术支持排查。

3. EdgeOne 回源携带的标准头部触发源站安全策略。

EdgeOne 回源默认会携带 特定的 HTTP 请求头，可以通过 CURL 指向源站的同时携带这几个头部验证，测试方式如下：

```
curl -vo/dev/null [协议]://[域名][path] --resolve [域名]:[端口]:[源ip] -H "[头部名称]:[头部值]"
```

步骤四：运营商劫持限制

若以上排查均是正常的，且域名回源协议为 HTTP，则有可能是被运营商劫持或限制，需要在源站上抓包确认请求是否有正常回源，排查方法如下：

找一个现网无访问或访问频率较低的 URL，经由 EdgeOne 节点发起请求，同时在源站上抓包，如果源站上未收到该 HTTP 请求，则说明是被运营商劫持或限制，可直接找运营商反馈或保留现象通过腾讯云技术支持反馈给运营商。

客户端测试命令：

```
curl -vo/dev/null [协议]://[域名][path] --resolve [域名]:[端口]:[cdn ip]
```

源站测试命令：

```
tcpflow -cp port 80 -i [网卡] > src_80.flow
```

注：由于回源是 HTTP 协议，因此请求信息会以明文的形式保存在 `src_80.flow` 里，可通过 `vi` 或 `vim` 编辑器打开查找是否有客户端请求的 URL。

解决思路

对于 524 状态码，如果明确源站处理耗时长（EdgeOne 默认读/写超时时间为 15 s），可以尝试调整「HTTP 应答超时时间」，超时时间的设置建议不超过客户端超时时间，避免 EdgeOne 回源节点在等待源站响应的过程中，触发客户端超时断开。具体调整步骤可参考：[回源超时时间](#)。

521/522 状态码排障指南

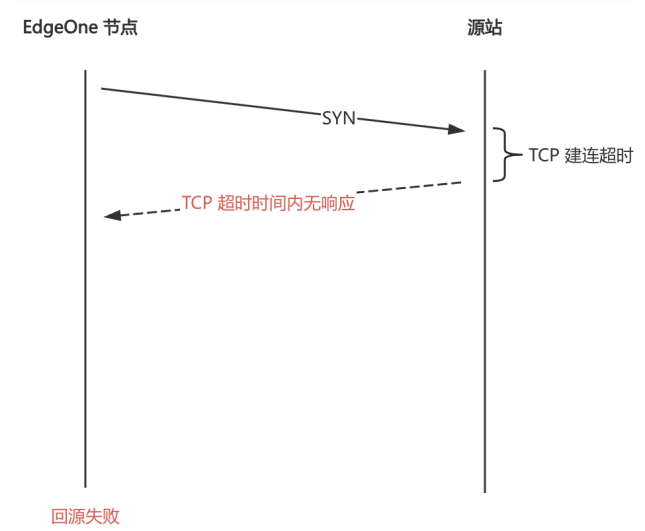
最近更新时间：2025-08-27 18:01:32

当您使用腾讯云 EdgeOne 加速站点访问资源后，客户端的请求将发送至 EdgeOne 边缘节点，再回源到中间层节点，最终再回源到源站。因此如果访问过程中出现问题，可能涉及到多层网络链路的问题。当 EdgeOne 回源源站失败时则会出现 52x 的错误，本文档将为您介绍当出现 521/522 状态码时，您应该如何排查。

如下，以 522 状态码为例：

定义

522 状态码是 EdgeOne 自定义的状态码，指节点请求到源站，在 TCP 建连阶段，源站一直没有响应导致节点超时，则节点响应客户端 522 状态码。其它状态码的含义请参考 [异常状态码参考](#)。



现象

```
curl -v http://www.example.com/test.jpg
* Trying 43.152.167.17...
* Connected to www.example.com (43.152.167.17) port 80 (#0)
> GET /test.jpg HTTP/1.1
> Host: www.example.com
> User-Agent: curl/7.79.1
> Accept: */*
> Proxy-Connection: Keep-Alive
* Mark bundle as not supporting multiuse
< HTTP/1.1 522 Connect origin timed out
< Server: Edgeone_Spectrum_OCMID
< Date: Wed, 25 Oct 2023 10:16:27 GMT
< Content-Length: 0
< Connection: keep-alive < Cache-Control: max-age=0
< EO-LOG-UUID: 16221131381683531888
<
* Connection #0 to host 43.152.162.17 left intact
```

可能的原因

- 源站自身服务问题
- 源站安全策略导致
- 运营商限制（HTTP）

排查方法

从第三方（非 CDN、源站）发起 HTTP/HTTPS 请求，指向源站测试，第三方可以是个人 pc、服务器、监测平台等。可以通过在服务器上使用命令行工具 CURL 来排查。

步骤一：确定回源配置信息

若您无特殊配置，则仅以「域名管理」处设置的源站、协议、以及端口为准即可。若有特殊配置，则可参照如下方法进行确定：

1. 源站 IP：源站 IP 需要根据「域名管理」配置的源站、源站组、负载均衡以及规则引擎「修改源站」的配置综合确定。
2. 回源协议：回源协议需要根据「域名管理」、规则引擎「回源 HTTPS」以及「修改源站」里的回源协议综合确定。
3. 回源端口：若无特殊配置，则为 80 或 443，若您在规则引擎「修改源站」操作中有修改回源端口，则以修改后的为准。
4. 回源 HOST：默认跟随加速域名，若您在规则引擎「Host Header 重写」操作中有进行设置，则以设置的为准。
5. 回源 Path：默认跟随请求 URL，若您在规则引擎「回源 URL 重写」操作中有进行修改，则以修改的为准。

步骤二：源站自身服务问题排查

可能是源站服务异常，比如端口侦听未开启，可使用命令行工具 telnet，从第三方平台指向源站端口发起 telnet 请求，测试方法如下：

```
telnet [源ip] [端口]
```

注：CURL 版本保证在 7.21.3 版本以上。

假设回源使用 80 端口、源 ip 为 1.1.1.1。

```
telnet 1.1.1.1 80
```

从第三方平台 telnet 源站的 80 端口，如果 TCP 连接被断开或一直在连接中，可在源站上执行如下命令确认源站 80 端口是否开启，测试示例如下：

```
netstat -tnlp|grep -w 80
```

若 TCP 连接建立成功或自查源站端口有正常开启，则进入步骤三。

步骤三：源站安全策略排查

可能的原因如下：

1. 源站有设置防火墙，EdgeOne 回源节点 IP 不在 IP 白名单里。

CURL 获取 EO-LOG-UUID，提交给腾讯云技术支持，由技术支持查询 EdgeOne 回源节点的 IP，源站自查回源节点 IP 是否在源站的 IP 白名单里。其中，UUID 获取方法如下：

```
< Last-Modified: Mon, 24 Oct 2022 08:21:54 GMT
< Etag: "63564b22-264"
< Server: nginx/1.20.2
< Content-Type: text/html
< Content-Length: 612
< Accept-Ranges: bytes
< Connection: keep-alive
< Date: Wed, 08 Jan 2025 12:29:57 GMT
< EO-LOG-UUID: 4745437539590071077
```

2. 源站设置访问限频，EdgeOne 回源频率过高。

可指向源站并发起多个请求，验证能否复现与源站建连失败或超时的现象。

步骤四：运营商限制

若以上排查均是正常的，则有可能是被运营商限制，需要在源站上抓包确认是否有收到 TCP SYN 包，排查方法如下：

在 EdgeOne 回源节点和源站上同时抓包，并在 EdgeOne 回源节点上发起 telnet 请求至源站（由腾讯云技术支持操作）。测试命令如下：EdgeOne 回源节点：

```
telnet [源ip] [端口]

# 抓包
tcpdump -nn -s0 -i [网卡] -w src_port.pcap
```

源站：

```
tcpdump -nn -s0 -i [网卡] -w src_port.pcap
```

通过对比 EdgeOne 回源节点与源站的数据包，确认 EdgeOne 回源节点的 SYN 包源站是否有收到。

解决思路

对于 522 状态码，如果明确源站建连响应耗时长（EdgeOne 默认建连超时时间为 5 s），可以尝试调整「TCP 建连超时时间」，超时时间的设置建议不超过客户端超时时间，避免 EdgeOne 回源节点在等待源站响应的过程中，触发客户端超时断开。当前「TCP 建连超时时间」暂不支持控制台标准能力，如有需要，可 [联系我们](#)。

工具指南

诊断工具

自助诊断

最近更新时间：2024-04-18 14:38:03

功能简介

自助诊断工具是腾讯云 EdgeOne 为用户提供的 Web 工具，可用于加速域名访问慢、访问失败等场景的自助诊断排查，以及日常的业务健康巡检。您可以在工具页面输入诊断链接，单击检测后，会模拟用户请求进行智能诊断，检测完成即可查看报告，或发起重新诊断，帮助您快速定位可能的问题原因，并提供解决指引。

⚠ 注意：

- 自助诊断是模拟用户对诊断链接发起请求，因此会产生请求数和流量。建议诊断资源的文件大小控制在10MB 以下。
- 诊断链接的所属域名必须是同个站点下已配置的域名。
- 诊断链接的资源内容必须符合国家法律法规。
- 账号必须处于非欠费停服状态。

使用场景

域名访问慢

域名访问效果提升不明显，通过自助诊断工具可以定位出如域名配置不合理、未缓存命中，访问链路异常等可能的原因，并提供相应的解决指引。

域名访问失败

域名访问失败，通过自助诊断工具可以定位出如域名配置错误，源站异常等可能的原因，并提供相应的解决指引。

全面健康巡检

希望全面了解域名访问的健康状态，通过自助诊断工具可以进行域名 DNS 检测、获取节点及源站的运行状态，并提供相应的优化建议。

操作步骤

- 登录 [边缘安全加速平台 EO 控制台](#)，在左侧菜单栏中，单击**诊断工具** > **自助诊断**。
- 在自助诊断页面的输入框，按输入格式填写需要诊断的资源链接，单击**检测**，将弹出诊断页面。

⚠ 注意：

诊断过程中，请不要关闭页面。

自助诊断

访问诊断工具可帮助您及时发现因域名配置不当和网络链路等引起的域名访问异常、加速效果未生效等问题。通过检测DNS、节点、源站等状态，及时定位问题并给出解决建议和技术支持。[功能详细介绍](#)

诊断报告

今天

近7天

近30天

2022-10-19 ~ 2022-10-19

输入域名关键字过滤

报告ID	诊断URL	诊断状态	诊断结果	客户端IP	所在区域	诊断时间	操作
暂无数据							

共 0 条

10 / 页

1 / 1 页

使用场景

加速效果未生效
接入域名后加速效果不佳或未生效等情况，可使用「访问诊断」我们将排查出错误配置或提供配置建议

域名访问异常
域名访问异常或遇到问题，可使用诊断帮助定位问题、排查故障，并根据检测出异常情况给出相应处理建议。

全面健康诊断
日常管理域名，可使用诊断域名DNS检测、节点及源站的运行状态，及时发现问题并保障业务正常运行。

3. 检测完成后，即可查看诊断结果报告，您可根据诊断报告的异常项以及排查指南，自助定位并修复问题。

诊断正常

诊断详情

客户端检测

客户端 IP

中国-福建省-中国联通 (58.)

域名

com.cn

接入模式

CNAME 接入模式

Local DNS

中国-福建省-中国联通 (36.)

CNAME 域名

正常 (edgeonedy1.com)

节点检测

加速节点

中国香港-香港特别行政区-其他 (43.152)

状态码

访问正常 (200)

命中状态

已命中，正为您提供加速效果

文件大小

正常 (21 KB)

下载速率

正常 (12 KB/s)

重新诊断

我知道了

4. 在诊断报告列表中，支持查询历史诊断记录，以及查看报告，或发起重新诊断。

自助诊断

访问诊断工具可帮助您及时发现因域名配置不当和网络链路等引起的域名访问异常、加速效果未生效等问题。通过检测DNS、节点、源站等状态，及时定位问题并给出解决建议和技术支持。[功能详情介绍](#)

诊断报告

今天 近7天 近30天 2022-10-21 ~ 2022-10-21

报告ID	诊断URL	诊断状态	诊断结果	客户端IP	所在区域	诊断时间	操作
xd-6b	http://pic.jpg	已完成	异常	58.2	中国-福建省	2022-10-21 11:24:03	查看报告 重新诊断

共 1 条

10 条 / 页

1 / 1 页

诊断示例

问题示例

假设您的站点以 CNAME 模式接入，但未在域名注册商处配置 EdgeOne 提供的 CNAME 记录。如下所示，[域名服务页面](#) 提示“未在域名解析商添加此 CNAME 记录”。

CNAME 接入

添加域名 更多操作

服务域名	服务类型	操作				
@	负载均衡	前往负载均衡				
☐ 加速域名	源站类型	源站地址	代理模式	CNAME	HTTPS 证书	操作
☐ com.cn	IPv4	12	代理加速	未在域名解析商添加此CNAME记录	未配置	配置 编辑 新建别称域名 删除
☐ .cn	域名	www	代理加速	acc.edgeone...	未配置	配置 编辑 新建别称域名 删除
☐ com.cn	IPv4	1.1	代理加速	om.cn.ac...	未配置	配置 编辑 新建别称域名 删除

自助诊断

在自助诊断页面输入对应的资源链接进行诊断，诊断完成后，查看诊断报告可以发现，CNAME 域名处提示配置异常，以及“请在域名解析商添加 CNAME 记录”的解决指引文案。

存在异常

检测出该域名存在以下异常,可能会影响加速效果,请根据实际情况处理

[诊断详情](#) ▾

客户端检测

客户端 IP ✓ 中国-福建省-中国联通 (58.2 [REDACTED])

域名 ✓ [REDACTED]

接入模式 ✓ CNAME 接入模式

Local DNS ! 未知

CNAME 域名 ! 配置异常 [排查指南](#) ▾

请在域名解析商添加 CNAME 记录 [REDACTED]y1.com'。

节点检测

加速节点 ✓ 中国香港-香港特别行政区-其他 ([REDACTED]157)

状态码 ! 访问异常 (403) [排查指南](#) ▲

命中状态 ! 未知

文件大小 ! 未知

下载速率 ! 未知

回源检测

源站地址 ✓ [REDACTED].94

状态码 ! 访问异常 (403) [排查指南](#) ▲

下载速率 ! 未知

协助诊断

最近更新时间：2024-04-22 14:51:31

功能简介

协助诊断工具是对自助诊断工具的补充，可用于解决您的用户访问慢、访问失败等问题。您可以通过协助诊断邀请用户进行访问诊断，目前支持微信二维码和页面链接的分享方式。通过协助诊断，可以获取保障用户的网络环境信息，以及访问的诊断详情，帮助您快速定位可能的问题原因，并提供解决指引。

⚠ 注意：

- 协助诊断是模拟用户对诊断链接发起请求，因此会产生请求数和流量。建议诊断资源的文件大小控制在10MB 以下。
- 诊断 URL分享的有效期为 24 小时，诊断次数上限为 10 次。
- 诊断链接的所属域名必须是同个站点下已配置的域名。
- 诊断链接的资源内容必须符合国家法律法规。
- 账号必须处于非欠费停服状态。

使用场景

客户端网络环境异常

个别用户访问慢或访问失败，可使用协助诊断，获取客户端网络信息；

部分区域访问异常

同个资源链接，部分区域访问异常，可使用协助诊断获取节点或访问链路的运行状态，并提供相应的解决指引。

操作步骤

- 登录 [边缘安全加速平台 EO 控制台](#)，在左侧菜单栏中，单击**诊断工具 > 协助诊断**。
- 在协助诊断页面的输入框，按输入格式填写需要诊断的链接和协助人数。单击**分享**，即可将诊断链接分享给协助者。

诊断URL

协助人数

-

10

+

分享

请将诊断链接分享给协助人，收集协助人客户端网络信息，生成诊断报告。[更多功能介绍](#)

诊断列表

今天近7天近30天2022-10-19 ~ 2022-10-19

输入域名关键字过滤

诊断URL	诊断ID	创建时间	已诊断数/最大可诊断数	正常报告数	异常报告数	操作
暂无数据						

共 0 条

10 条 / 页

1 / 1 页

使用场景

接入域名后加速效果不佳或未生效等情况，可使用「访问诊断」我们将排查出错误配置或提供配置建议

域名访问异常或遇到问题，可使用诊断帮助定位问题、排查故障，并根据检测出异常情况给出相应处理建议。

日常管理域名，可使用诊断域名DNS检测、节点及源站的运行状态，及时发现并保障业务正常运行。

- 在分享方式弹窗中，您可以自行选择微信二维码或页面链接的方式。移动端环境建议复制微信二维码进行分享、PC 端环境建议复制链接进行分享。单击**复制二维码或复制链接**，即可将二维码图片或链接发送给协助者。



4. 协助者在手机移动端扫描二维码或点击链接，即可进行客户端网络环境检测。



5. 您可以在诊断报告列表查看协助者网络环境信息以及分享情况。

诊断信息

诊断URLhttp://[redacted].com.cn/plc.jpg

创建时间2022-10-20 19:37:09

最大诊断人数2

分享

诊断结果预览



已诊断人数: 1

未诊断人数: 1

诊断报告

报告ID	诊断状态	诊断结果	客户端 IP	所在区域	诊断时间	操作
tdiag-2ahx7q6jzk43	已完成	正常	58.23.[redacted]	中国-福建省	2022-10-20 19:37:17	查看报告

共 1 条

10 条 / 页

1 / 1 页

6. 在诊断报告列表中，单击查看报告，即可查看诊断详情。

诊断正常

诊断详情

客户端检测

客户端 IP

中国-福建省-中国联通 (58.23.[redacted])

域名

[redacted].com.cn

接入模式

CNAME 接入模式

Local DNS

中国香港-香港特别行政区-其他 (172.[redacted])

CNAME 域名

正常 ([redacted].com.cn.acc.edgeoned1.com)

节点检测

加速节点

中国香港-香港特别行政区-其他 (43.152.[redacted])

状态码

访问正常 (200)

命中状态

已命中，正为您提供加速效果

文件大小

正常 (21 KB)

下载速率

正常 (11 KB/s)

我知道了

诊断示例

问题示例

假设您的用户反馈业务资源访问慢或访问失败，但无法提供客户端网络信息用于定位问题，您可以使用协助诊断工具，将诊断链接分享给您的用户进行诊断。

诊断排查

进入协助诊断页面，在诊断URL输入框中填写用户反馈的资源链接，设置协助人数，单击分享，将诊断链接或微信二维码发送给协助者，协助者可自行选择诊断方式。

- 客户端诊断信息

尊敬的用户，您好：

本次检测已完成，感谢您的帮助，您现在可以关闭页面，祝您生活愉快！



诊断已完成，感谢您的支持



客户端环境检测



- ①

公网出口IP
- 获取失败
- ✓

操作系统
- iPhone
- ✓

浏览器
- WeixinBrowser
- ✓

域名测试结果
- cloud.tencent.com 网络正常，
延时518毫秒

● 控制台诊断报告

诊断正常

诊断详情

客户端检测

客户端 IP

✓ 中国-福建省-中国联通 (58.23)

域名

✓ .com.cn

接入模式

✓ CNAME 接入模式

Local DNS

✓ 中国香港-香港特别行政区-其他 (172)

CNAME 域名

✓ 正常 (.com.cn.acc.edgeoneddy1.com)

节点检测

加速节点

✓ 中国香港-香港特别行政区-其他 (43.152)

状态码

✓ 访问正常 (200)

命中状态

✓ 已命中, 正为您提供加速效果

文件大小

✓ 正常 (21 KB)

下载速率

✓ 正常 (11 KB/s)

我知道了

自助调试

最近更新时间：2025-06-26 11:21:24

功能简介

如果您需要确认当前在 EdgeOne 内配置的节点缓存规则、自定义 Cache Key 等配置是否已针对您的资源生效，EdgeOne 提供了自助调试工具来帮助您获取节点缓存 TTL，资源是否可缓存，Cache key 等信息，方便您进行业务配置调试。开启自助调试后，您可以通过指定的客户端 IP 来发起 URL 请求，在请求中携带 `EO-Debug-Headers: all` 头部，即可根据返回的响应头来查看该资源在节点内是否缓存、对应的 Cache Key 值、缓存时间。

```
curl -v -o/a 'http://www.example.com/test.jpg?a=1' -H 'EO-Debug-Headers: all'
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           % Done    0         0             0          0      0     0    0*   Trying 192.168.1.1...
* TCP_NODELAY set
* Connected to www.example.com (192.168.1.1) port 80 (#0)
> GET /test.jpg?a=1 HTTP/1.1
> Host: www.example.com
> User-Agent: curl/7.62.0
> Accept: */*
> EO-Debug-Headers: all
>
< HTTP/1.1 200 OK
< Last-Modified: Wed, 07 Dec 2022 12:32:32 GMT
< Etag: "639087e0-4"
< Server: nginx/1.20.2
< Date: Thu, 29 Jun 2023 12:19:58 GMT
< Content-Type: image/jpeg
< Content-Length: 4
< Accept-Ranges: bytes
< Connection: keep-alive
< EO-LOG-UUID: 6570353728066144953
< EO-Cache-Status: HIT
< EO-Debug-Status: on
< EO-Debug-CacheKey: www.example.com/test.jpg a=1
< EO-Debug-Cacheable: yes
< EO-Debug-CacheTTL: 00d00h10m00s
{ [4 bytes data]
100    4  100    4    0    0    47    0  --:--:-- --:--:-- --:--:--    47
* Connection #0 to host www.example.com left intact
```

使用场景

若您在控制台规则引擎里配置了较复杂的缓存策略、自定义 cache key，需要验证配置是否生效，可以通过该功能进行验证。

操作步骤

例如：当前站点 `example.com` 下的域名 `www.example.com`，当前已针对 `.jpg` 后缀文件配置需要在 EdgeOne 节点内缓存 600 秒；缓存 Cache Key 配置为保留指定参数 `a` 作为缓存键。配置完成后，需要验证当前配置是否已生效，可按照如下操作步骤验证：

1. 登录 [边缘安全加速平台 EO 控制台](#)，在左侧菜单栏中，进入 **服务总览**，单击 **网站安全加速** 内需配置的站点。
2. 在站点详情页面，单击 **站点加速**，进入站点全局配置页面，在右侧导航栏中，单击 **自助调试**。
3. 找到 **自助调试** 配置卡片中，单击“开关”，开启自助调试功能。

自助调试

自助调试

调试模式开启后，可以在 HTTP 请求头中携带 EO-Debug-Headers 头，来获取部分域名配置信息（例如节点缓存 TTL，CacheKey 等）。

- 调试信息结果将通过 EO-XXXX 头返回。
- 调试模式仅在有效期内生效。
- 为避免不必要的配置信息泄露，调试模式会对访问的客户端 IP 或 IP 段进行白名单限制，支持 IPv4 及 IPv6 网段。0.0.0.0/0 表示允许所有 IPv4 客户端进行调试，::/0 表示允许所有 IPv6 客户端进行调试。



4. 开启调试模式后，需要设置有效期，以及允许访问的客户端来源。其中，时间范围为 1-365 天，默认 7 天。客户端 IP 可输入 100 个，支持填写 IPv4 以及 IPv6 的 IP/IP 段，0.0.0.0/0 表示允许所有 IPv4 客户端进行调试；::/0 表示允许所有 IPv6 客户端进行调试。
5. 单击 **保存**，则配置允许的客户端 IP 在有效期内可进行 debug 调试。

自助调试

自助调试

调试模式开启后，可以在 HTTP 请求头中携带 EO-Debug-Headers 头，来获取部分域名配置信息（例如节点缓存 TTL，CacheKey 等）。

- 调试信息结果将通过 EO-XXXX 头返回。
- 调试模式仅在有效时间内生效。
- 为避免不必要的配置信息泄露，调试模式会对访问的客户端 IP 或 IP 段进行白名单限制，支持 IPv4 及 IPv6 网段。0.0.0.0/0 表示允许所有 IPv4 客户端进行调试，::/0 表示允许所有 IPv6 客户端进行调试。



有效时间: 2025-03-31 17:44:05

允许的 IP/IP 段: 1

编辑

6. 通过以上指定的客户端 IP 来源，在 Mac/Linux 环境下，发起 curl 请求进行验证，例如：

curl -voa 'http://www.example.com/test.jpg?a=1' -H 'EO-Debug-Headers: all'。请求结果如下：

```
curl -voa 'http://www.example.com/test.jpg?a=1' -H 'EO-Debug-Headers: all'
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
   0      0     0     0         0             0      0      0  0*    Trying 192.168.1.1...
* TCP_NODELAY set
* Connected to www.example.com (192.168.1.1) port 80 (#0)
> GET /test.jpg?a=1 HTTP/1.1
> Host: www.example.com
> User-Agent: curl/7.62.0
> Accept: */*
> EO-Debug-Headers: all
>
< HTTP/1.1 200 OK
< Last-Modified: Wed, 07 Dec 2022 12:32:32 GMT
< Etag: "639087e0-4"
< Server: nginx/1.20.2
< Date: Thu, 29 Jun 2023 12:19:58 GMT
< Content-Type: image/jpeg
< Content-Length: 4
< Accept-Ranges: bytes
< Connection: keep-alive
< EO-LOG-UUID: 6570353728066144953
< EO-Cache-Status: HIT
< EO-Debug-Status: on
< EO-Debug-CacheKey: www.example.com/test.jpg a=1
< EO-Debug-Cacheable: yes
< EO-Debug-CacheTTL: 00d00h10m00s
{ [4 bytes data]
100   4  100   4    0     0    47     0  --:--:-- --:--:-- --:--:--    47
* Connection #0 to host www.example.com left intact
```

在响应头中，可以看到该请求对应的 Cache Key、缓存状态、缓存时间，与示例中的配置一致，即当前配置已生效。

相关参考

在开启自助调试模式下时，响应的 debug 头部说明如下：

头部名称	功能说明	返回值的含义说明
EO-Debug-Status	用于标识自助调试模式是否开启。	• on: 开启状态，且请求客户端 IP 在白名单内&请求时间在有效期内； • off: 关闭状态，或开启状态但请求时间超出有效期； • forbidden: 开启状态，但请求客户端 IP 不在白名单内。
EO-Debug-ClientIp	发起 Debug 请求的 ClientIp。	发起 Debug 请求的客户端 IP。当开启自助调试但 EO-Debug-Status 值为 forbidden 时，可以检查下是否请求的客户端 IP 不在允许的 IP/IP 段范围内。
EO-Debug-Cacheable	本次请求的 URL，按照配置节点缓存 TTL 的配置，最终该请求 URL 资源在 EdgeOne 节点内是否可缓存的状态。	• yes: 可缓存内容 • no: 不可缓存内容
EO-Debug-CacheKey	本次请求的 URL，按照自定义 Cache key，最终该请求 URL 资源在 EdgeOne 节点内生成的 Cache key。	例如：www.example.com/test.jpg a=1，指该请求 URL 资源在 EdgeOne 内生成的 Cache Key

EO-Debug- CacheTTL	本次请求的 URL，按照 配置节点缓存 TTL 的配置，最终该请求 URL 资源在 EdgeOne 节点缓存 TTL 时长。	列表值，包括数字和时间单位。d 表示天，h 表示小时，m 表示分钟，s 表示秒，例如： • 3d0h0m0s 表示缓存TTL是 3 天； • 0d0h5m0s 表示缓存是 5 分钟； • 0d0h0m5s 表示缓存是 5 秒。
-----------------------	--	--

测速工具

性能监控

最近更新时间：2024-12-02 15:13:01

注意：

EdgeOne 性能监控页面已于2024年11月21日下线。请注意，这一变更并不影响您现有的性能监控服务和数据。您可以继续在 [腾讯云可观测平台-前端性能监控-应用管理](#) 页面查看和使用相关服务，无需担心服务中断或数据丢失。

功能概述

性能监控是一站式前端监控解决方案，该功能为 EdgeOne 与 [前端性能监控](#) 的联动功能，专注于 Web 等前端场景监控。用户只需要将 SDK 安装到自己的项目中，通过简单配置，即可全方位守护用户页面质量。实现低成本使用和无侵入的监控，确保页面性能和前端质量的实时可观测。

说明：

性能监控每个应用每天50万免费上报数据量额度，对超过50万上报次数的部分进行计费，该功能费用不计入 EdgeOne 套餐，由前端性能监控侧收取。计费详情请参见 [前端性能监控-购买指南](#)。

适用场景

- 页面性能分析：包括首屏耗时、建立 TCP 连接耗时、TTFB 耗时、SSL 耗时等。同时还支持最新的 Web Vitals（谷歌针对网页加载速度和体验所提出的一套指标）标准。全方位协助您优化用户体验。
- 用户访问分析：支持查看业务 PV/UV 数据，每个页面访问的 TOP 数据等，支持通过网络、浏览器、地区等多维度分析用户访问数据，实时了解并分析用户访问情况。
- 静态资源测速：支持资源测速，包括图片加载耗时和 CDN 资源耗时等。开发者可以查看某个页面下具体使用了哪些资源，每个资源的耗时情况等信息。

操作步骤

1. 登录 [边缘安全加速平台 EO 控制台](#)，在左侧导航中，单击 [测速工具 > 性能监控](#)。
2. 首次进入性能监控页面时，由于性能监控是与腾讯云前端性能监控联动功能，需要您单击 [开启](#)，开启对应权限。



3. 在性能监控页面，单击 [应用接入](#)。
4. 在应用接入对话框中，输入应用名称和描述，并勾选“我已知悉费用详情”框，单击 [下一步](#)。

应用接入

1 创建应用

>

2 应用接入

应用名称

应用描述

☐ 我已知悉费用详情

下一步

取消

5. 根据接入类型安装 SDK。

5.1 `<script>` 标签引入的方式安装 SDK

5.1.1 在接入指引页面，复制提供的 `<script>` 标签代码。

5.1.2 把 `<script>` 标签引入类型下的代码引入到需要监控的网站的标签 `<head></head>` 中即可。

应用接入

1 创建应用

>

2 应用接入

接入指引

接入类型 ☒ `<script>` 标签引入 ☐ npm 安装

```
// 直接在页面<head></head>标签中引入，将会在 window 上挂载 Aegis 构造函数
<script src="https://cdn-go.cn/aegis/aegis-sdk/latest/aegis.min.js"></script>
<script>
  const aegis = new Aegis({
    id: 'r', // 上报 id
    uin: 'xxx', // 用户唯一 ID (可选)
    reportApiSpeed: true, // 接口测速
    reportAssetSpeed: true, // 静态资源测速
    spa: true // spa 应用页面跳转的时候开启 pv 计算
  });
</script>
```

完成

④ 说明

该接入方式使用“h3-Q050”协议，默认 cache-control 为 max-age=666，如果需要修改 cache-control，可以添加参数 max_age，例如：

```
<script src="https://cdn-go.cn/aegis/aegis-sdk/latest/aegis.min.js?max_age=3600"></script>。
```

5.2 npm 方式安装 SDK

5.2.1 在接入指引页面，复制提供的首行命令，在您的开发环境中引入 aegis sdk。

5.2.2 引入之后，复制提供的代码，在您的 js 代码中初始化 SDK 即可。



数据监控

完成上述步骤接入后即可以前往页面性能、页面访问和静态资源界面查看相关数据。

页面性能

页面性能模块支持多维度分析页面性能情况，您可以通过性能变化趋势图、页面加载瀑布图、地区视图等维度分析首屏时间、请求响应等页面性能关键指标。详情请参见 [页面性能](#)。

页面访问

页面访问用于展示页面访问量情况（UV、PV、WAU、MAU），并支持多维度分析页面访问情况。详情请参见 [页面访问](#)。

静态资源

前端 HTML 页面中主要包含的静态资源有：JS 文件、CSS 文件和图片文件，若这些文件加载耗时较长、失败等，将直接对页面造成影响甚至瘫痪，静态资源监控将协助您分析前端静态资源情况。详情请参见 [静态资源](#)。

IP 归属查询

最近更新时间：2025-09-04 15:10:12

本文介绍了如何使用 IP 归属查询工具来验证 IP 是否为腾讯云 EdgeOne 节点 IP，以及 IP 归属地信息。

操作步骤

1. 登录 [边缘安全加速平台 EO 控制台](#)，在左侧菜单栏中，单击 IP 归属查询。



2. 在 IP 归属查询页面，查询框内输入需要查询的 IP，一行一个，单次查询最多支持 100 个 IP，支持输入 IPv6 地址。
3. 单击查询，查询结果可展示当前查询的 IP 是否为腾讯云 EdgeOne 节点 IP，以及 IP 归属地信息。单击查询结果右上角 ，可导出查询结果，导出为 CSV 文件。

