

# 边缘安全加速平台 EO

## 常见指南



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

### 常见指南

#### 常见问题

- 产品特性相关问题
- 域名服务与 DNS 相关问题
- 站点加速相关问题
- 安全防护相关问题
- 数据与日志相关问题
- 域名备案相关问题
- 源站配置相关问题

#### 排障指南

- 异常状态码参考
- EdgeOne 4XX/5XX 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

## 常见指南

## 常见问题

## 产品特性相关问题

最近更新时间：2024-09-06 17:01:52

### 边缘安全加速平台 EO 支持哪些接入方式？

支持 NS 接入和 CNAME 接入。

### 边缘安全加速平台 EO 具有哪些安全能力？

支持对 Web 应用层攻击、DDoS 攻击、CC 攻击、BOT/爬虫类攻击进行防护；也支持用户按业务需求，配置自定义复杂访问控制规则。

### 边缘安全加速平台 EO 是否支持各地区线路加速？

对于业务遍及各地的企业，数据传输跨地区、跨网，容易遭遇网络抖动、丢包率高等问题，边缘安全加速平台 EO 在多个地区部署了边缘节点，充分满足用户跨地区的业务需求。有关具体的支持区域，请 [联系我们](#) 获取。

### 边缘安全加速平台 EO 是否支持防御在非腾讯云上的业务？

支持，详情请 [联系我们](#) 获取。

### 边缘安全加速平台 EO 是否支持 API 操作？

支持两种 API 操作，一种为腾讯云原生的 API 操作，一种为 Terraform API 操作。用户可以根据实际需求，选择对应的 API 来进行操作。

### 边缘安全加速平台 EO 是否支持动态加速？

支持。边缘安全加速平台 EO 支持动静混合资源请求加速场景，可以优化请求的响应时间和稳定性，为网站提供优质、流畅的访问体验服务。

### 边缘安全加速平台 EO 支持哪些站点业务安全防护？

边缘安全加速平台 EO 支持对基于 HTTP 和 HTTPS 的网站业务提供 Web 防护和 BOT 防护。其中 Web 防护包括：Web 安全规则（包括 OWASP 规则）、自定义特征规则、频控规则。

### 边缘安全加速平台 EO 支持哪些非站点业务安全防护？

边缘安全加速平台 EO 支持对指定端口 TCP 应用和 UDP 应用提供 DDoS 防护：包括常见 DDoS 攻击类型检测防护，基于端口、协议、源 IP 地区、自定义包特征的过滤规则，和 UDP 水印防护（即将上线）。

# 域名服务与 DNS 相关问题

最近更新时间：2025-01-07 17:54:42

## 添加域名 DNS 解析记录的时候为什么会提示 CNAME 记录与 MX 记录之间冲突？

假设为 `example.com` 有如下记录需配置：

记录类型	主机记录	记录值
MX	www	mx.mail.com
CNAME	www	test.edgeone.com

在进行递归解析查询时，各记录类型之间是有优先级的，根据 [RFC1034](#) 和 [RFC2181](#)，CNAME 优先级最高，所以在解析请求过程中，会优先返回 CNAME 解析记录结果。因此，在主机记录值相同的情况下，域名不允许同时配置 CNAME 记录和 MX 记录，配置时将提示记录冲突。

针对有部分业务场景需要针对主机记录为 @ 时同时添加 CNAME 和 MX 记录，EdgeOne 可允许同时配置 CNAME 和 MX 记录：

记录类型	主机记录	记录值
MX	@	mx.mail.com
CNAME	@	test.edgeone.com

### 警告：

此场景配置方式会导致邮箱无法正常收信、收信时好时坏的问题。若邮箱服务器的 Local DNS 优先进行了 @ 记录的 CNAME 类型解析，此时对 @ 记录的 MX 类型的解析会受到影响，从而产生解析失败或无法达到预期解析结果的现象。主机记录为非 @ 时，MX 与 CNAME 记录依然会提示冲突，具体冲突规则请参考下方其他记录类型冲突的图表。

## 添加域名 DNS 解析记录的时候为什么会提示 CNAME 记录与 TXT 记录之间冲突？

假设为 `example.com` 存在如下记录需配置：

记录类型	主机记录	记录值
TXT	www	edgeone-txt-flag
CNAME	www	test.edgeone.com

与 CNAME 与 MX 记录冲突同理，CNAME 记录优先级最高，所以在主机记录相同的情况下，同时配置 CNAME 记录与 TXT 记录可能会导致 TXT 记录无法正常解析，导致对应的服务不可用。因此 EdgeOne 会通过提示记录冲突的方式来限制这类配置。

针对有部分业务场景需要针对主机记录为 @ 时同时添加 CNAME 和 MX 记录，EdgeOne 可允许同时配置 CNAME 和 TXT 记录：

记录类型	主机记录	记录值
TXT	@	edgeone-txt-flag
CNAME	@	test.edgeone.com

### 警告：

此场景配置方式会导致 TXT 校验不通过等问题，如遇到可去掉 CNAME 记录。主机记录为非 @ 时，TXT 与 CNAME 记录依然会冲突。

## 添加域名时有哪些记录类型是冲突的？

域名解析记录之间的冲突说明如下表所示：

- ✓：不冲突，在相同的主机记录下，该两种类型的解析记录可以共存。如：已经设置了 `www.example.com` 的 A 记录，还可以再设置 `www.example.com` 的 MX 记录。

- ✕：冲突，在相同的主机记录下，该两种类型的解析记录不可以共存。如：已经设置了 `www.example.com` 的 A 记录，不可以再设置 `www.example.com` 的 CNAME 记录。

记录类型	A	AAAA	CNAME	MX	NS	TXT	SRV	CAA
A	✓	✓	✕	✓	✕	✓	✓	✓
AAAA	✓	✓	✕	✓	✕	✓	✓	✓
CNAME	✕	✕	✕	✕	✕	✕	✕	✕
MX	✓	✓	✕	✓	✕	✓	✓	✓
NS	✕	✕	✕	✕	✓	✕	✕	✕
TXT	✓	✓	✕	✓	✕	✓	✓	✓
SRV	✓	✓	✕	✓	✕	✓	✓	✓
CAA	✓	✓	✕	✓	✕	✓	✓	✓

**说明**

上表为主机记录为非 @ 时的冲突情况，当主机记录为 @ 时，CNAME 记录与 MX、TXT 记录不冲突，允许配置。

**记录类型为 A/AAAA/CNAME 时，相同的主机记录可以同时存在解析和加速吗？**

假设为 `example.com` 配置如下记录：

记录类型	主机记录	记录值
A	www	1.1.1.1
A	www	2.2.2.2

此时如果想对其中一条主机记录开启加速，则会冲突，相同主机记录不允许同时存在解析和加速。如果需要对主机记录值为 `1.1.1.1` 这条记录开启加速，请先删除主机记录值为 `2.2.2.2` 这条后开启。

**说明：**

A/AAAA/CNAME 这三种记录类型会出现上述冲突情况。

**默认支持哪些端口？**

边缘安全加速平台 EO 默认支持的访问端口为 80、8080、443。回源访问端口配置无限制，源站支持即可。

**未设置权重的时候，如果存在多条同名主机记录的 A/AAAA/CNAME 记录，解析的结果是什么？**

如果存在多条同名主机记录的 A/AAAA 记录，未设置权重的情况下，将返回所有的 A/AAAA 记录；如果存在多条同名主机记录的 CNAME 记录，未设置权重的情况下，将通过轮询的方式返回其中一条 CNAME 记录。

**域名配置一般多久时间生效？**

域名配置下发后，一般 5 分钟内生效，部分配置可能因为配置任务数量较多，可能需要 5-15 分钟生效，请您耐心等待。

# 站点加速相关问题

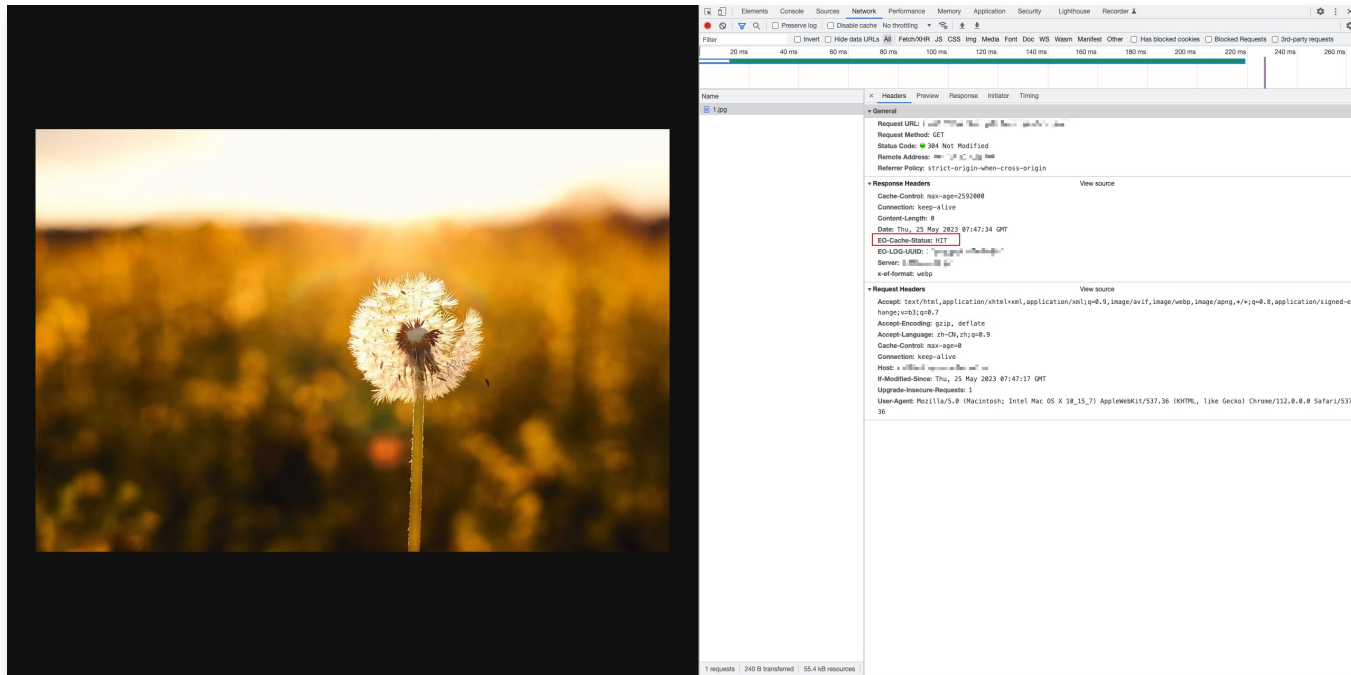
最近更新时间：2024-04-18 14:38:03

## 如何判断用户请求是否命中 EdgeOne 节点缓存？

EdgeOne通过 **EO-Cache-Status** 来标识当前请求是否命中缓存，您可以通过以下两种方式查看该头部进行判断。

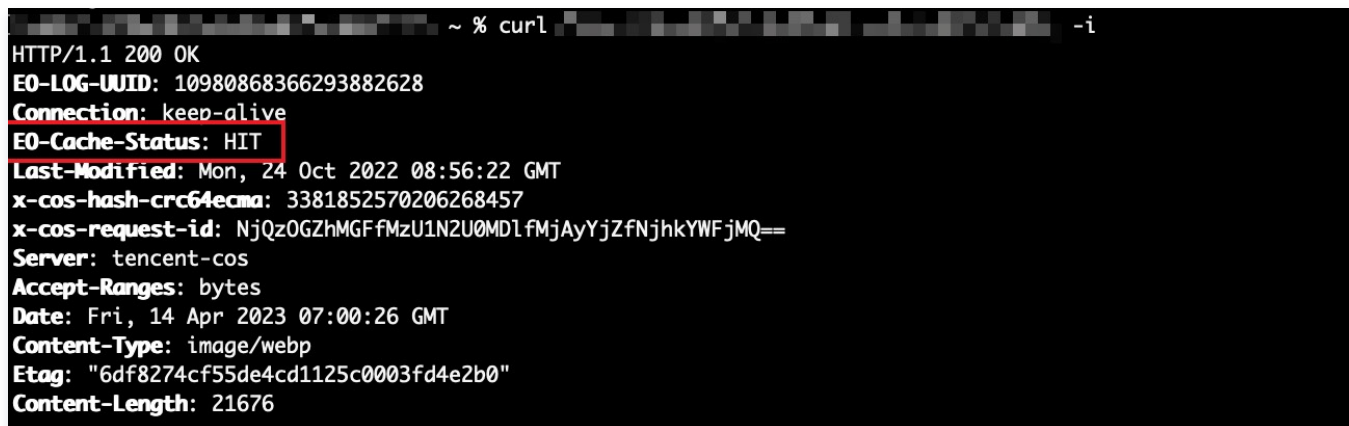
### 浏览器直接访问

在浏览器内打开控制台，直接访问请求 URL，例如：`https://example.com/test.webp`。查看响应头内 **EO-Cache-Status** 的值，如果为 **HIT**，即命中缓存。



### 通过 curl 请求验证

您可以在 Mac/Linux 系统下，通过 curl 请求验证，例如：`curl https://example.com/test.webp -i`。查看响应头内 **EO-Cache-Status** 的值，如果为 **HIT**，即命中缓存。



源站资源配置了跨域响应，资源经预热缓存后跨域响应失败，该如何处理？

预热缓存是直接对提交的 URL 资源发起请求，并非跨域请求，所以不会触发源站的跨域响应配置，预热缓存后的资源将不包含相关的跨域头部，当有用户访问该资源时，将可能出现跨域错误。

因此，如果您的资源需要满足跨域场景访问，且需进行预热缓存，建议通过自定义修改 HTTP 响应头，将跨域响应配置于 EdgeOne 内，由 EdgeOne 响应跨域头部即可。

### 清除缓存和预热缓存每次提交内容后需要多久才能生效？

#### 清除缓存：

类型	单次提交数量	生效时间
URL	1-5000 条 URL	5-50分钟
目录	1-1000条目录	5-220分钟
Hostname	1-1000个 Hostname	5-220分钟
Cache-Tag	1-100个 Cache-Tag	5-10分钟
全部缓存	-	5-220分钟

#### 预热缓存：

类型	单次提交数量	生效时间
URL	1-5000条 URL	5-30分钟

#### 说明：

1. 当文件配置的缓存 TTL 少于5分钟时，建议不使用清除工具，而是等待超时更新。
2. 清除缓存中任何类型的实际总耗时主要取决于提交内容的数量，数量越多等待时间越长。
3. 预热缓存的实际总耗时主要取决于文件大小，文件越大等待时间越长。较大文件（ $\geq 100\text{MB}$ ）的预热生效时间可能会延长，超过30分钟。



# 安全防护相关问题

最近更新时间：2024-11-04 20:48:02

## EdgeOne 有哪些安全功能？

EdgeOne 为 Web 应用服务和 TCP/UDP 应用服务提供反向代理和服务对应协议的安全防护。

接入服务类型	L3/L4 DDoS 防护	HTTP DDoS 防护 (七层 CC 攻击防护)	Web 防护	Bot 管理
四层代理 (TCP/UDP 应用服务)	✓ <sup>1</sup>	-	-	-
七层站点 (Web 应用服务)	✓ <sup>1</sup>	✓	✓	✓ <sup>2</sup>

### 说明：

- 注 1：默认提供平台级防护，如您对防护容量有要求，请 [使用独立 DDoS 防护](#)。  
注 2：需要订阅 Bot 管理，详见 [计费概述（新版）](#)。

## 我已经在源站配置了 Web 应用防火墙，是否需要使用 EdgeOne 安全防护？

EdgeOne 旨在提供一体化的加速和安全能力，因此当您应用和服务接入 EdgeOne 时，EdgeOne 即开始提供防护服务。在您源站已有的防护基础上，EdgeOne 提供：

- 分布式安全防护：提供分布在全球可用区的多个独立清洗中心在内的防护资源，通过分布式接入架构提供高效的冗余和灾备。
- WAF 和 Web 站点防护：提供包括漏洞攻击检测、速率限制和 Bot 管理<sup>3</sup>在内的应用安全防护能力。
- 对缓存资源的防护能力：可以同时检查访问已缓存资源的请求。EdgeOne 的安全策略拦截的用量不会计费，减少不必要的内容分发费用。
- 最靠近客户端的威胁识别：EdgeOne 通常由客户端直接发起访问，能够对客户端的四层连接会话特征和 TLS 指纹特征进行采集分析，辅助策略识别恶意访问。
- 兼容您的源站安全策略：支持对回源请求进行标记<sup>3</sup>，您可以在源站对请求进行进一步分析。

### 说明：

- 注 3：需要订阅并启用 [Bot 管理](#)，Bot 管理会在回源请求中携带标识头部，帮助您进一步分析请求。

## EdgeOne 是否支持 IP 黑白名单？

如您需要配置 IP 黑名单，即：拦截指定列表中的客户端 IP，您可以使用 [自定义规则](#) 中的基础访问管控，选择客户端 IP 管控选项，配置需要拦截的 IP 列表，并选择拦截处置方式。

如您需要配置 IP 白名单，即：放行指定列表中的客户端 IP，您可以使用 [防护例外规则](#)，选择客户端 IP 匹配条件，并选择需要跳过的安全模块。

### 注意：

- IP 白名单的可能应用在不同的场景下：
- 放行指定列表中的客户端 IP。在该场景中，需要配置 [防护例外规则](#)，跳过指定安全模块。
  - 仅允许指定列表中的客户端 IP 访问。在该场景中，需要配置 [自定义规则](#) 中的基础访问管控规则，拦截不在指定列表中的客户端 IP。

## 如何配置区域封禁？如何封禁中国大陆以外地区的访问？

您可以使用 [自定义规则](#) 中的基础访问管控，选择区域管控选项，配置需要拦截的客户端地区列表，并选择拦截处置方式。如您需要封禁中国大陆以外地区的访问，可以选择 [区域不匹配选项](#)，匹配内容选择中国大陆地区区域，并选择拦截处置方式。

## 如何配置防盗链？如何仅允许本域名和指定域名的链接访问？

防盗链技术主要用于避免静态资源被外部站点页面加载。

## 常见的防盗链技术

基础的防盗链策略通过请求 Referer 头部判断是否来自页面加载，拦截外部站点引用资源的请求以及不通过页面加载直接访问的请求（例如：在浏览器中输入 URL 直接访问静态资源）。您可以使用 [自定义规则](#) 中的 [基础访问管控](#) 功能，拦截 Referer 头部不在指定域名列表中的请求。

## 进一步验证数据访问安全性

通过 HTTP 头部字段可以应对常见盗链场景，但是恶意请求仍可通过技术手段生成合法 HTTP 请求，从而获取站点资源。为了进一步提升站点资源访问安全性，您可以通过动态生成 URL，在 URL 中包含具有时效性的随机签名。在提供资源访问之前，确认签名合法性和有效性，从而识别请求是否有访问资源的权限。EdgeOne 的 [规则引擎](#) 功能提供了 [Token 鉴权](#) 选项，可帮助您生成签名 URL，并提供签名验证机制。您也可以使用 [边缘函数](#) 实现自定义的动态访问鉴权。

## 什么是“观察”，“观察”处置动作会进行拦截吗？

“观察”处置动作仅记录日志，不会拦截请求。这对于评估策略很有帮助，设置为“观察”的规则不会对您的业务造成影响，因此您可以通过检查日志中该规则的匹配情况判断它对正常业务的影响，以及对恶意请求的匹配情况，帮助您判断是否需要启用为拦截。详见 [处置方式](#)。

## 什么是“JavaScript 挑战”，“JavaScript 挑战”处置动作会对业务有什么影响？

“JavaScript 挑战”处置动作会响应一个页面，该页面会校验请求客户端是否支持 Cookie 和 JavaScript 运行环境，满足校验条件的浏览器可以继续访问，其他工具（例如：cURL 等）会被拦截。该方式可以识别一些非浏览器的工具。详见 [处置方式](#)。

### ⚠ 注意：

1. 大部分 API 接口无法处理 JavaScript 响应，因此会被“JavaScript挑战”动作拦截。
2. 原生 APP、小程序请求也属于 API 请求，无法处理 JavaScript 响应，因此会被“JavaScript挑战”动作拦截。如需兼容 JavaScript 挑战，客户端可以在访问 API 接口之前，先通过 web-view 或者 H5 框架完成 JavaScript 挑战，避免访问 API 接口的请求被“JavaScript 挑战”拦截。

## EdgeOne 开放的端口都可以访问到源站吗？

EdgeOne 的开放端口默认不提供站点业务访问。根据已接入站点的协议和端口配置，EdgeOne 会解析访问请求，并根据安全和加速配置决定是否处理来自指定端口的请求，并根据配置响应、拦截或回源。

如果您的业务未启用端口，或未配置接入协议，客户端将无法通过该端口或协议访问业务域名资源或源站：

- 未完成接入流程的站点域名，无法通过 EdgeOne 的 HTTP、HTTP/2、QUIC 等协议访问域名业务；
- 如果未启用或配置 HTTPS、HTTP/2、QUIC 服务或相应证书，客户端将无法通过 HTTPS、HTTP/2、QUIC 等协议访问对应域名资源或源站；
- 如果四层代理未配置指定端口的转发规则，将无法通过该端口访问源站的对应端口业务。

### 📌 说明：

接入域名服务后，EdgeOne 默认支持指定端口访问站点 HTTP 服务，详见 [域名服务相关问题](#)。

# 数据与日志相关问题

最近更新时间：2024-03-15 17:33:41

## 为什么控制台流量数据与从日志中统计而来的流量数据对不上？

通过站点加速访问日志 `EdgeResponseBytes` 字段中记录的字节数统计而来的流量数据与控制台展示的流量数据、计费流量数据可能不一致。原因如下：

- 访问日志中仅可记录应用层数据，在实际网络传输中，产生的网络流量要比纯应用层流量多 5% - 15%。由两部分组成：
  - TCP/IP 包头消耗，基于 TCP/IP 协议的 HTTP 请求，每一个包的大小最大是1500个字节，包含了 TCP 和 IP 协议的 40-60 个字节的包头，包头部分会产生流量，但是无法被应用层统计到，这部分的开销大致为 3-4 % 左右。
  - TCP 重传，正常网络传输过程中，发送的网络包会有 3-10% 左右会被互联网丢掉，丢掉后服务器会对丢弃的部分进行重传，此部分流量应用层也无法统计，占比约为3% - 7%。

## 为何腾讯云可观测平台告警和产品控制台内数据分析有时会出现不一致的波动？

腾讯云可观测平台告警要求较高的实时性，而产品控制台的数据分析模块要求较丰富的多维度统计分析。为了分别满足这两种数据需求，EdgeOne 分别采用了不同的数据采集和统计方式，两个数据源在整体指标趋势上保持一致，但是在一分钟粒度的指标值可能存在不一致的情况，具体差异点参考如下示例：

- **腾讯云可观测平台数据源**：采集自边缘节点机器根据用户请求汇聚成域名维度的分钟粒度数据，不受用户数突发影响，量级稳定，具有更高的实时性，但统计指标仅覆盖域名维度的关键用量指标，例如域名维度的流量，请求数等指标。
- **控制台数据分析**：采集自用户每次请求产生的原始日志进行实时分析，请求会在用户请求完成后打印，受用户数突发的影响，量级不稳定，实时性较弱，但包括丰富的数据维度指标，例如设备类型，浏览器类型维度的流量、请求数等指标。

例如：一个用户请求一个1GB文件，假设用户10:00:00开始下载，100秒下载完成。

- **腾讯云可观测平台数据**：每台边缘机器会在每分钟内的某个时刻上报一次监控指标，该请求的统计指标会落在10:01，10:02两个分钟内。
- **控制台数据**：每台边缘机器会在用户请求结束时间10:01:40打印一条日志，最终统计值会落在10:01分钟上。

因此，由于统计规则的差异，导致腾讯云可观测平台数据和产品控制台数据在某一分钟粒度上会存在不一致的情况。

# 域名备案相关问题

最近更新时间：2025-02-26 15:46:02

## 一、ICP备案要求说明

1. 依据中国《互联网信息服务管理办法》、《非经营性互联网信息服务备案管理办法》等相关法律法规，使用腾讯云 EdgeOne 产品加速服务时，当加速区域为“全球可用区”或“中国大陆可用区”的域名必须完成 ICP 备案，更多法规要求或指引可参见 [ICP 备案](#)。
2. 未 ICP 备案域名，加速区域不可选全球可用区或中国大陆可用区，仅可选择全球可用区（不含中国大陆）。

## 二、接入备案说明

1. 接入备案是指域名已在其他接入服务商（非腾讯云）完成备案并取得 ICP 备案号，现将域名指向腾讯云服务器（如：CVM, LightHouse），则需要在腾讯云进行接入备案，更多的接入备案说明可参见 [接入备案](#)。
2. 源站为腾讯云服务器，如 CVM 或 Lighthouse，域名接入时，EdgeOne 会检测是否已在腾讯云完成接入备案，检测结果仅作为提醒，不强制限制接入，您须尽快完成腾讯云接入备案，否则所有请求到源站时（包括回源请求）将被会拦截，从而影响您在 EdgeOne 的加速服务。

## 三、备案失效的处理机制

1. 若您站点加速区域为“全球可用区”或“中国大陆可用区”时的域名备案失效时，腾讯云 EdgeOne 会停止其站点下所有域名的加速服务、域名解析服务等，同时会通过短信、邮件、站内信等方式进行提醒。
2. 域名备案失效可能包括但不限于如下原因：
  - 主动注销备案。
  - 备案信息不真实或不准确被管局注销。
  - 域名因违法违规原因被管局注销。

## 四、恢复备案后加速服务启用方法

1. 若您的加速域名因未备案被停止加速服务，在完成域名备案后，您需要在 EdgeOne 控制台的域名管理重新启用域名即可。
2. 如果您已恢复完成备案，建议在管局备案审核时间后1-2小时再到控制台重新启用，若超过2小时仍提示域名未备案情形，请您联系 [在线客服](#) 寻求帮助。

## 五、其它常见问题

### 如何查看域名是否完成 ICP 备案，是否可以提供云 API 查询服务？

域名备案信息查询可到工信部 [ICP/IP地址/域名信息备案管理系统](#) 查询。

### 工信部官网显示已完成备案，在域名接入时仍提示未备案？

由于备案信息同步存在一定数据延迟，建议您在工信部备案审核通过后2小时再做接入，若超过2小时仍提示域名未备案，请您联系 [在线客服](#) 寻求帮助。

### 域名已完成备案，为何仍提示需腾讯云完成接入备案？

当您的源站为腾讯云服务器，如 CVM 或 Lighthouse，需要将域名的备案信息同步到腾讯云，即需要做腾讯云接入备案，详情请参见 [接入备案指引](#)。

#### 提示：

更多的备案相关问题，请参见：[备案相关问题](#)。

# 源站配置相关问题

最近更新时间：2025-01-06 17:56:12

## 源站组中权重应该如何填写？

当源站组中某个源站设定了权重，则其余源站都需设置权重，权重支持填写 0-100 的整数。不支持仅对部分源站设置权重。

## 源站组中某个源站权重设置为 0 时如何生效？

当您源站组中某个源站权重设置为 0 时，将不会有流量进入到该源站，EO 将按照其他源站加权为 100 分比例回源。

## 源站组中针对多个源站配置不同权重且对应域名开启智能加速时回源逻辑如何生效？

[智能加速](#) 和源站组权重两部分能力组合使用时，将按照以下逻辑生效：

场景	生效逻辑
源站组中多源站配置权重，对应域名开启智能加速	优先按照权重选择源站，然后智能加速会对回源链路做优化。
源站组中多源站配置权重，对应域名不开启智能加速	按照权重比例回源。
源站组中多源站不配置权重，对应域名开启智能加速	按照智能加速选择的最优源站回源。
源站组中多源站不配置权重，对应域名不开启智能加速	轮询源站组中每个源站，等比例回源。

## 变更源站组配置时，会对存量连接造成什么影响？

当您源站组中某个源站的权重从一个大于 0 的值调整到 0 或直接删除某个源站时，存量已经建联的回源连接不会受到影响，新增连接将不会被转发到权重为 0 或者被删除的源站上。

# 排障指南

## 异常状态码参考

最近更新时间：2024-12-25 10:43:53

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 <a href="#">HTTP 限制说明</a> 。
403	未通过防盗链校验，如规则引擎的 Token 鉴权。
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 $\geq 16$ ，详情请参见 <a href="#">CDN-Loop</a> 。

### EdgeOne 自定义的状态码

由 EdgeOne 自定义的特殊含义的状态码，包含 499、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
499	客户端请求到节点，还没等到节点响应就主动断开请求，如关闭请求页面等，则日志&监控会记录为 499 状态码。
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 <a href="#">Web 防护-托管规则</a> 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 <a href="#">Web 防护-自定义规则</a> 、 <a href="#">Web 防护-速率限制</a> 或 <a href="#">Bot 管理</a> 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。

# EdgeOne 4XX/5XX 状态码排障指南

最近更新时间：2025-01-17 11:49:12

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

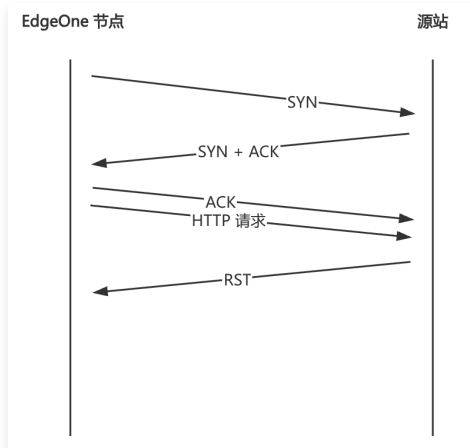
1. 含义：表示 "Locked"（已锁定），在接入 EdgeOne 的场景下，一般表示触发请求回环。

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  $\geq 16$ ，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。

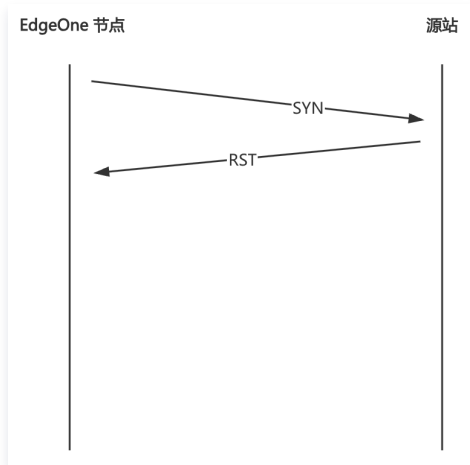


2. 可能的原因及解决思路：

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。



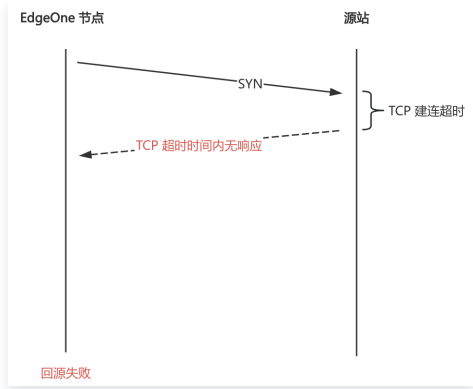
2. 可能的原因及解决思路：

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

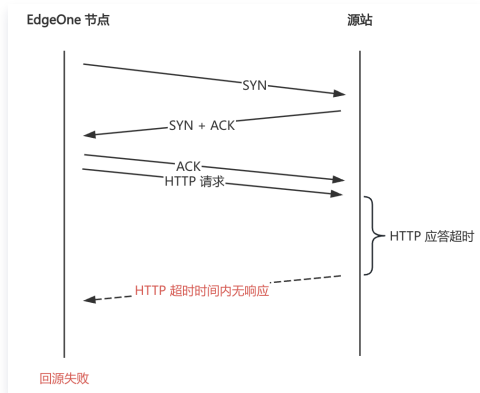
1. 含义：EdgeOne 自定义的状态码。若域名配置的源站为域名，则节点回源时，需要解析域名获取源站服务器 IP，若解析失败，则节点无法回源，响应客户端 523 状态码。

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。

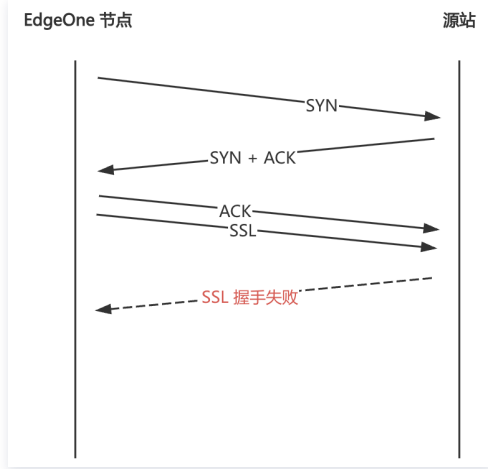


2. 可能的原因及解决思路：

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。
- 回源证书合法性校验不通过，目前 EdgeOne 默认会校验证书有效期。

# 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](#)

检测

### 诊断报告

今天
近7天
近30天
2022-10-19 ~ 2022-10-19

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 条 / 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 ([ ] 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 [ ])
- 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。[功能详细介绍](#)

输入检测URL，例如：http://www.example.com/example.html 检测

---

### 诊断报告

今天 | 近7天 | 近30天 | 2022-10-21 ~ 2022-10-21 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
xd-6b	http://...pic.jpg	✔ 已完成	异常	58.2...	中国-福建省	2022-10-21 11:24:03	<a href="#">查看报告</a> <a href="#">重新诊断</a>

共 1 条 10 条 / 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 输入加速域名/源站类型/源站地址

服务域名	服务类型						操作
@	负载均衡						<a href="#">前往负载均衡</a>
<input type="checkbox"/> 加速域名	源站类型	源站地址	代理模式	CNAME	HTTPS 证书	操作	
<input type="checkbox"/> ...com.cn	IPv4	12...	✔ 代理加速	✘ 未在域名解析商添加此CNAME记录	未配置	<a href="#">配置</a> <a href="#">编辑</a> <a href="#">新建别称域名</a> <a href="#">删除</a>	
<input type="checkbox"/> ...	域名	www...	✔ 代理加速	✘	未配置	<a href="#">配置</a> <a href="#">编辑</a> <a href="#">新建别称域名</a> <a href="#">删除</a>	
<input type="checkbox"/> ...com.cn	IPv4	1.1...	✔ 代理加速	✘	未配置	<a href="#">配置</a> <a href="#">编辑</a> <a href="#">新建别称域名</a> <a href="#">删除</a>	

### 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...)

域名 ✔ ...

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 '...y1.com'。

### 节点检测

加速节点 ✔ 中国香港-香港特别行政区-其他 (...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 ✔ ...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，可以获得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     请将诊断链接分享给协助者，收集协助者客户端网络信息，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

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

**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。

- 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URL: http://[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	<a href="#">查看报告</a>

共 1 条 10 条 / 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.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 )
- 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

最近更新時間：2024-08-23 15:07:21

### 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 -voa 'http://www.example.com/test.jpg?a=1' -H 'EO-Debug-Headers: all'
% Total % Received % Xferd Average Speed Time Time Time Current
         Dload Upload Total Spent Left Speed
  0     0     0     0     0     0     0     0  --:--:-- --:--:-- --:--:--    0*   Trying ██████████
* TCP_NODELAY set
* Connected to www.example.com (██████████) 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，单击 [站点列表](#)，在站点列表内单击需配置的站点。
2. 在站点详情页面，单击 [诊断工具](#) > [自助调试](#)。
3. 在自助调试页面，单击“开关”，开启自助调试功能。



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。



EO-Debug- CacheKey	本次请求的 URL，按照 <a href="#">自定义 Cache key</a> ，最终该请求 URL 资源在 EdgeOne 节点内生成的 Cache key。	例如： <code>www.example.com/test.jpg a=1</code> ，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 <a href="#">配置节点缓存 TTL</a> 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： <ul style="list-style-type: none"> <li>• 3d0h0m0s 表示缓存TTL是 3 天；</li> <li>• 0d0h5m0s 表示缓存是 5 分钟；</li> <li>• 0d0h0m5s 表示缓存是 5 秒。</li> </ul>

# 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** ✕

✔ 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。



### 应用接入

创建应用 > 应用接入

#### 接入指引

接入类型  <script> 标签引入  npm 安装

```
// 在应用支持 NPM 时使用 NPM 安装 Aegis SDK。
npm install --save aegis-web-sdk

// 引入后进行初始化
import Aegis from 'aegis-web-sdk';

const aegis = new Aegis({
  id: 'r5-xxxx-xxxx-ZDx', // 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
});
```

完成

## 数据监控

完成上述步骤接入后即可前往页面性能、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：2024-04-18 14:38:03


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。

