边缘安全加速平台 EO

常见问题

产品文档

腾讯云

文档目录

常见问题
- 异常状态码参考
- 产品特性相关问题
- 域名服务相关问题
- 站点加速相关问题
- 数据与日志相关问题
- 安全防护相关问题

常见问题
异常状态码参考

最近更新时间：2023-12-06 11:02:46

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。
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：`http://example.com/test.jpg`，则节点会读取域名 `example.com` 的配置文件，可能由于绑定了 `非 example.com` 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，有以下 2 个场景： CDN-Loop 头部的 Loops 数值 ≥ 16，详情请参见 CDN-Loop。 同一个请求，两次经过同一台节点设备。

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。

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	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 状态码。
521	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。
522	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。
523	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。
524	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。
525	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。
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。

产品特性相关问题

最近更新时间：2023-10-13 14:27:08

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，具体详情请 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）。

域名服务相关问题

最近更新时间：2023-11-23 20:30:31

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 M 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。

站点加速相关问题

最近更新时间：2024-05-09 09:11:04

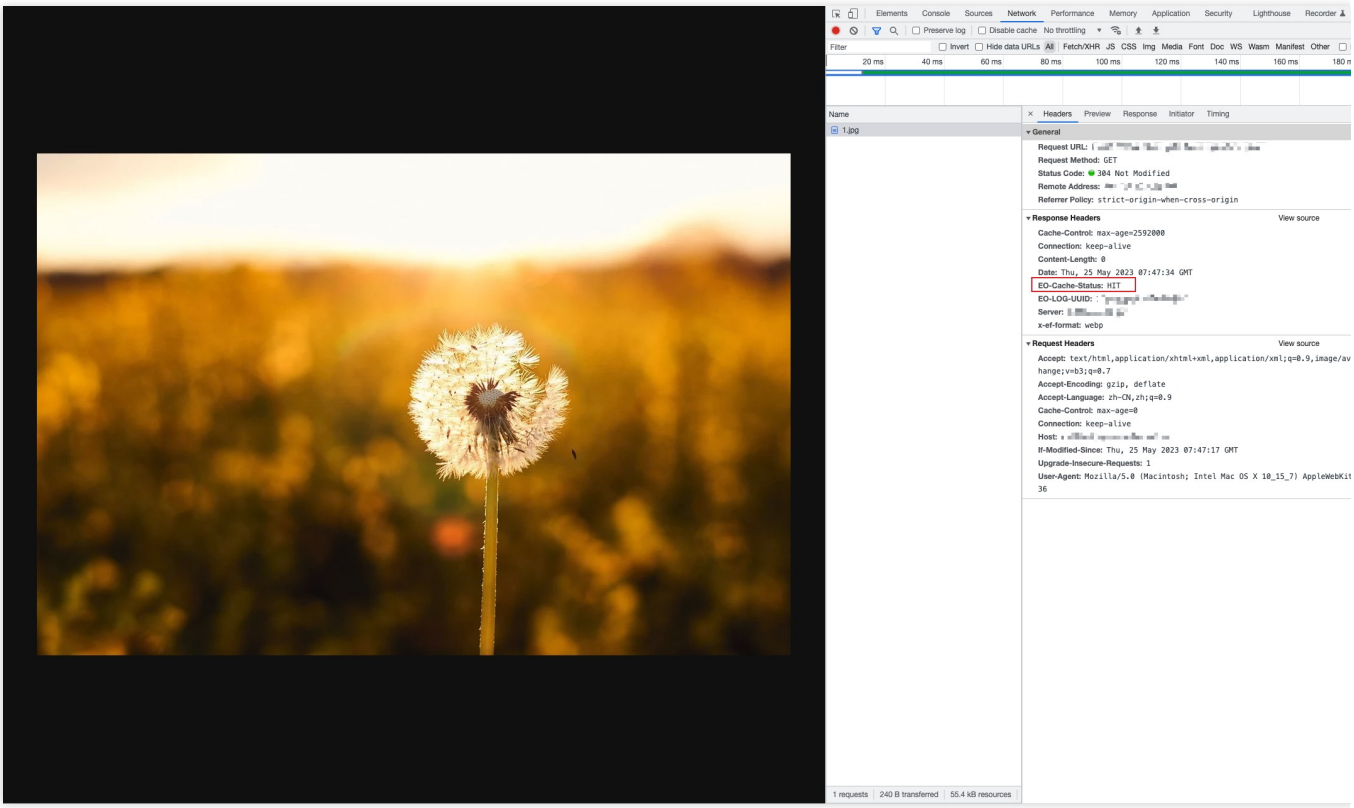
如何判断用户请求是否命中 EdgeOne 节点缓存？

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

通过 curl 请求验证

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。



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。较多大文件（≥100MB）的预热生效时间可能会延长，超过30分钟。

数据与日志相关问题

最近更新时间：2024-07-30 15:25:56

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和产品控制台数据分析的数据波动有时出现不一致的波动幅度？

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，可以保证实时性，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控制台数据在某一分钟粒度上会存在不一致的情况。

安全防护相关问题

最近更新时间：2023-12-05 16:50:57

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）	✓[1]	-	-	-
七层站点（Web 应用服务）	✓[1]	✓	✓	✓[2]

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，因此当您将应用和服务接入 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。

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信息进行采集分析，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[3]，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。

如何配置 IP 黑白名单？能否配置网段黑白名单？

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：

（1）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。

（2）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，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。

注意：

API 无法处理 JavaScript 挑战，因此会被 “JavaScript挑战” 动作拦截。