边缘安全加速平台 EO

实践教程

腾讯云

版权所有：腾讯云计算（北京）有限责任公司

【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】

腾讯云

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

实践教程
- 自动预热/清除缓存
  - EdgeOne + COS 场景实现自动预热缓存
  - EdgeOne + COS 场景实现自动清除缓存
- 防盗刷/盗链实践
  - EdgeOne 防盗刷实践教程
  - EdgeOne 防盗链实践教程
- HTTPS 相关实践
  - 通过 EdgeOne 免费证书快速实现 HTTPS 访问
- 加速优化
  - 跨地域安全加速（海外站点）
- 流量调度
  - 通过流量调度灰度接入 EdgeOne 安全加速
  - 通过流量调度至多厂商服务
- 数据分析与告警
  - 通过腾讯云可观测平台配置 EdgeOne 安全防护事件告警
- 跨域响应配置
- 第三方教程

版权所有：腾讯云计算（北京）有限责任公司

实践教程
自动预热/清除缓存
EdgeOne + COS 场景实现自动预热缓存

最近更新时间：2025-01-14 18:07:53

本文主要介绍了如何通过腾讯云对象存储（Cloud Object Storage，COS）和 云函数服务（Serverless Cloud Function，SCF）实现 EdgeOne 自动预热资源，预热的功能和原理介绍请参考 预热缓存 。

背景介绍

若您的源站为腾讯云对象存储 COS，当源站上传新的热点资源后（例如：APK 安装包、热点视频、课程文件等），通常需通过预热缓存来将资源提前缓存至 EdgeOne 边缘节点，避免客户端首次请求时因节点未缓存资源导致请求回源的情况。但是预热缓存需要您在文件上传到腾讯云 COS 后，人工到 EdgeOne 控制台内提交需预热的 URL，在需预热的 URL 数量很多的情况下，容易遗漏且可能因为人工操作造成未及时预热。

自动预热可以帮助您在文件上传至腾讯云 COS 后，由腾讯云 SCF 自动检测并调用 EdgeOne 的缓存预热 API 接口自动完成文件预热，保证您的文件在上传后立即预热至 EdgeOne 节点，提高缓存命中率，降低回源请求量。

⚠ **注意：**

- 腾讯云对象存储 COS 为收费功能，使用中可能产生的费用由腾讯云 COS 收取，具体收费详情请参考 对象存储计费概述 。
- 云函数 SCF 为收费功能，使用中可能产生的费用由云函数 SCF 收取，具体收费详情请参考 云函数计费概述 。
- 每日预热数量具有限额，不同计费套餐有不同限额，详见 套餐选型对比 。

适用场景

场景1：发布新内容

新版本的安装包或升级包上传至腾讯云 COS 后，资源自动预热至 EdgeOne 加速节点。文件正式发布后，海量用户的下载请求将直接由加速节点响应，提升下载速度的同时，大幅度降低源站压力。

场景2：大型运营活动

运营活动发布前，提前将活动页涉及到的静态资源上传到对象存储 COS，资源自动预热至 EdgeOne 加速节点。活动开始后，用户访问的静态资源均由加速节点响应，降低因高流量导致的延迟和拥塞。

操作步骤

示例场景

假设您是一家游戏厂商，已将站点域名 `www.example.com` 接入到 EdgeOne 加速，源站为腾讯云 COS，地址为： `prefetch-cos-1251558888.cos.ap-guangzhou.myqcloud.com` 。因为有多款游戏 APK 需要经常更新，期望上传 APK 后即可自动将资源预热至 EdgeOne 边缘节点。

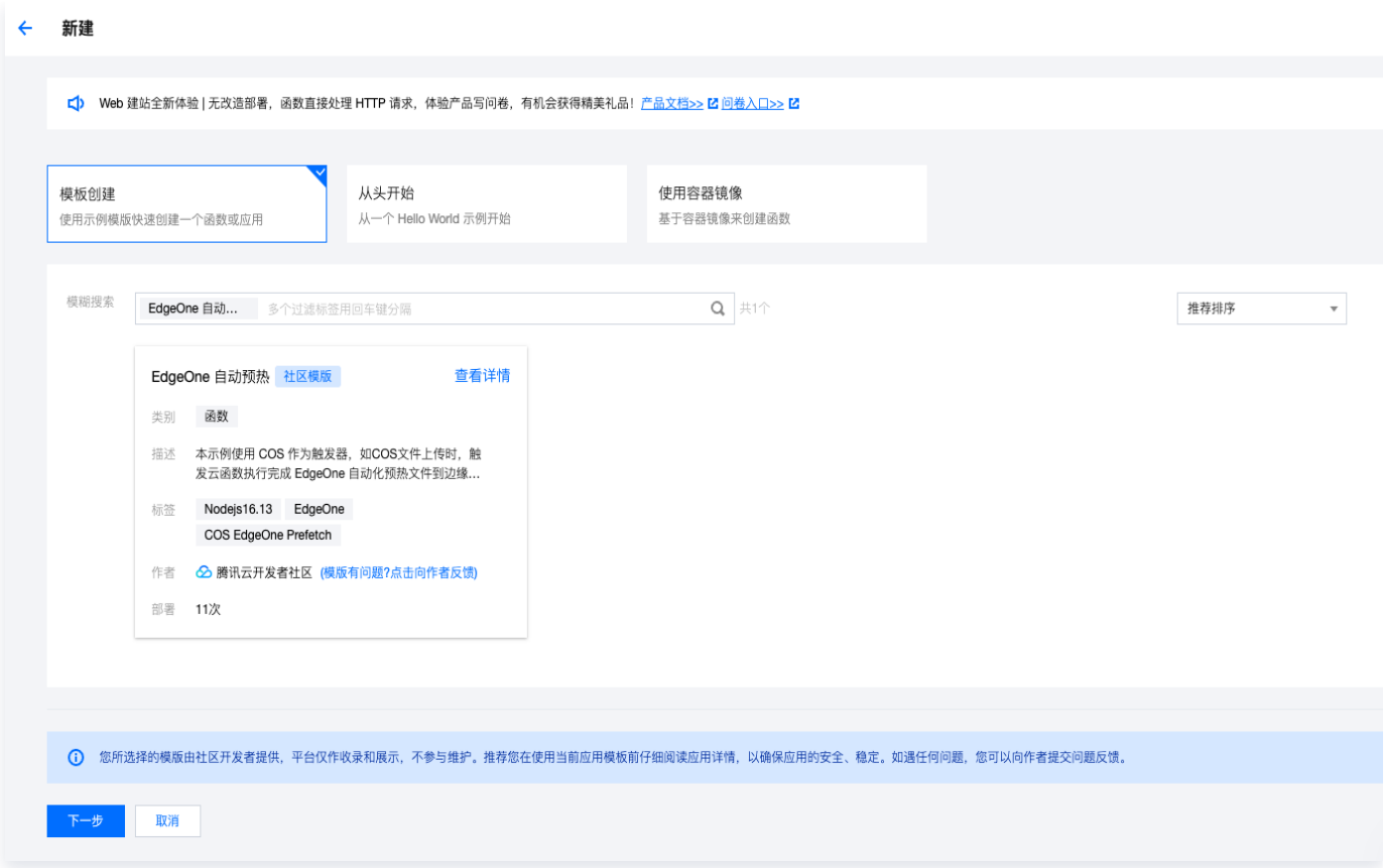
准备工作

1. 已开通 对象存储 COS 和 云函数 SCF，记录该存储桶名称及地域信息。
2. 根据 站点接入 指引添加站点，购买 EdgeOne 套餐，并获取该站点 ID。站点 ID 可通过站点接入后，在站点列表内查看并复制，例如：zone-26v607hq8d3m。

3. 已在 EdgeOne 控制台 添加加速域名 `www.example.com`，且源站配置为腾讯云 COS。

步骤1：创建 EdgeOne 自动预热的云函数并部署

1. 登录 云函数服务控制台，在左侧菜单栏中，单击**函数服务**。
2. 在函数服务页面，单击**新建**，选择**使用模板创建**，在模糊搜索中输入 **EdgeOne 自动预热**并选中，单击**下一步**。

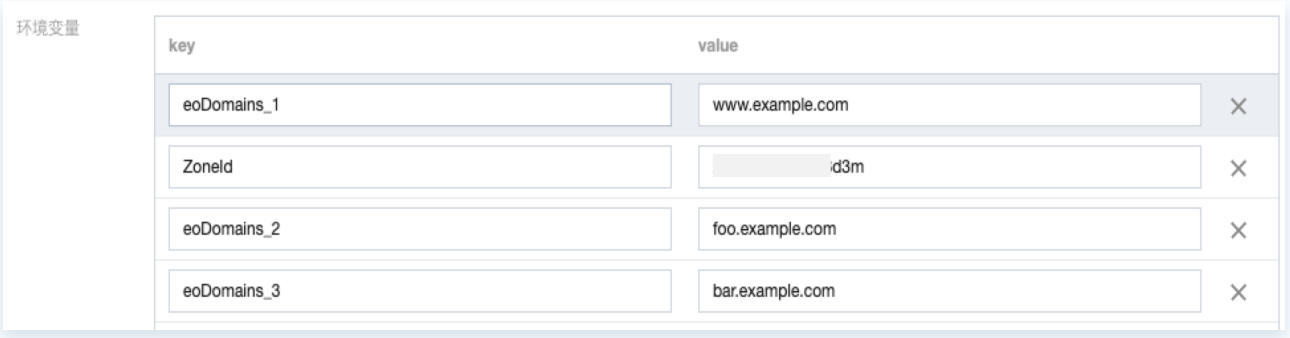


3. 在“函数配置”页面，如下配置为必填项，其他配置项建议保持使用默认配置即可。

- **基础配置**
  - 函数名称：创建函数时将自动生成一个函数名称，您可以选择自定义修改为一个易识别的函数名称。
  - 地域：请选择对象存储桶 COS 的所在地域，例如：广州。
  - 描述：说明此函数的用途，如：本示例使用 COS 作为触发器，如 COS 文件上传时，触发云函数执行完成 EdgeOne 自动化预热文件到边缘节点。
  - 运行角色：默认勾选**启用，配置并使用 SCF 模板运行角色**。如使用**已有角色**，请确保已有角色已包含 QcloudCOSFullAccess 和 QcloudTEOFullAccess 的预设策略。

- **函数代码：**模板已内置默认函数代码实现 EdgeOne 自动预热能力，无需改动。
- **环境配置：**

  单击**高级配置**，选中**环境配置**，您需要在环境变量中添加以下 key 和对应的 value 值，其余配置保持默认即可：
  - ZoneId：请填写对应需进行自动预热的域名站点 `example.com` 的 ZoneId，站点 ID 获取方式请参见 准备工作 。
  - eoDomains：请填写已在 ZoneId 下添加好的加速域名，如：`www.example.com` 。

> **说明：**
> 如果您在当前站点下有多个域名的源站使用了同一个 COS 存储桶，期望多个域名都能触发自动预热，则填写环境配置时，可以填写添加多个环境变量，以 eoDomains 开头，例如：eoDomains_1、eoDomains_2，如下所示：
>
> 
>

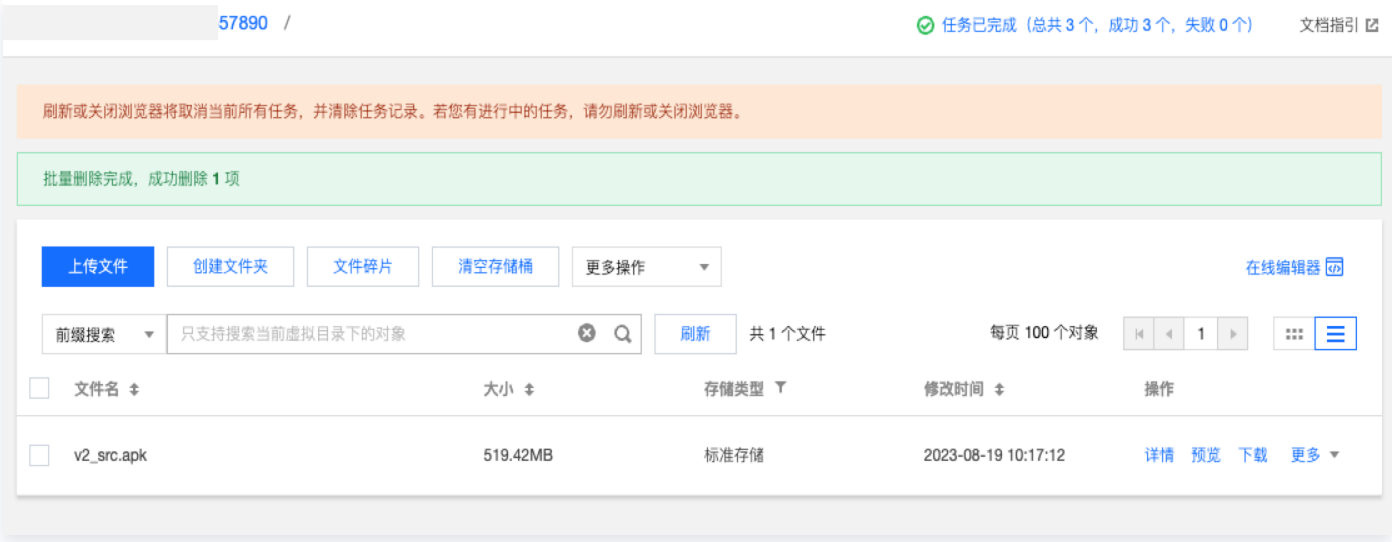
- **触发器配置**

  在触发器配置中，选择 COS Bucket 为与此云函数 SCF 同地域的存储桶，可输入存储桶名称进行模糊查询，例如：`prefetch-cos-1251558888.cos.ap-guangzhou.myqcloud.com`。其余配置项保持为默认配置即可。

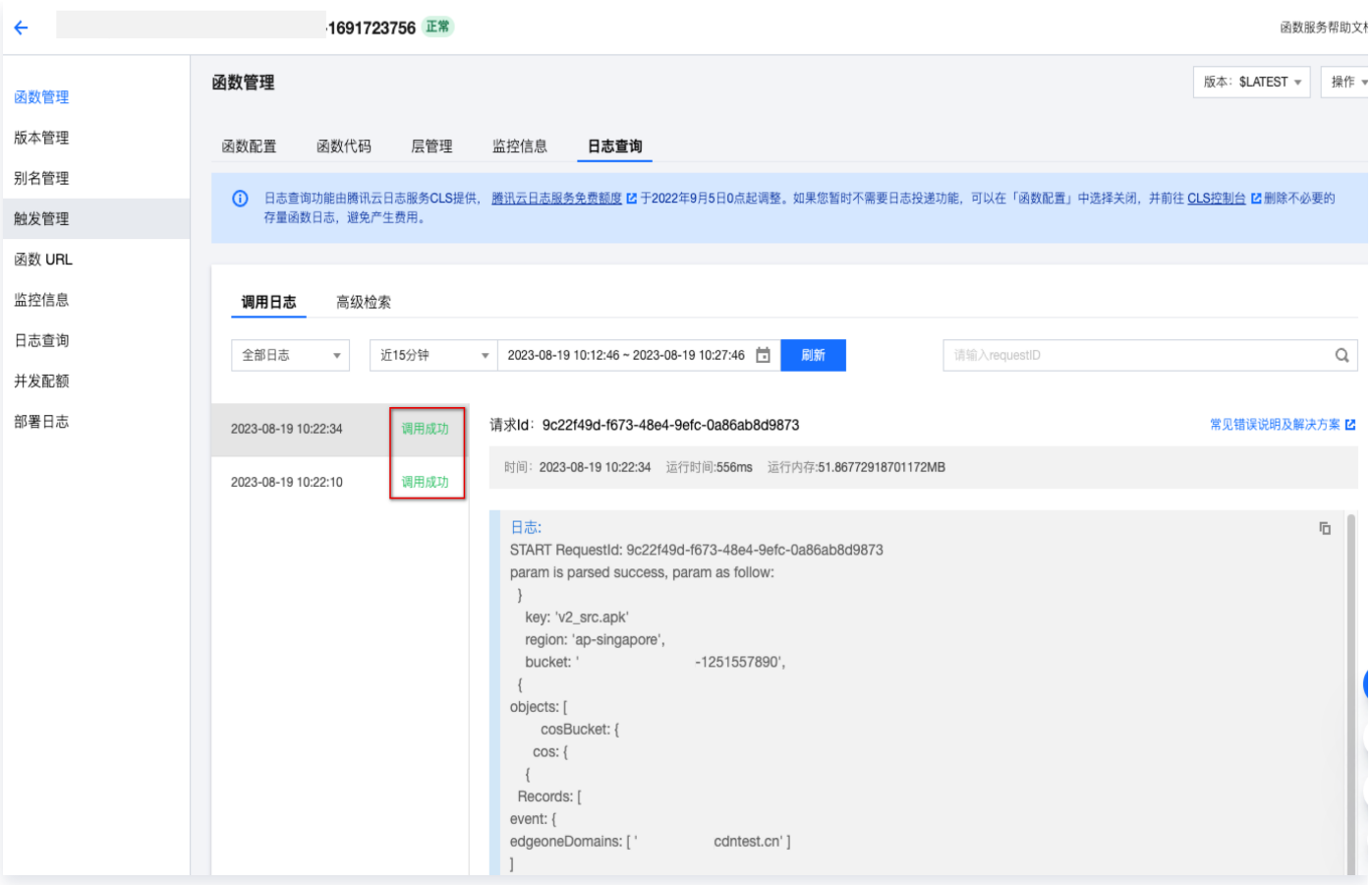
4. 单击**完成**，即可完成 EdgeOne 自动预热函数的创建。

步骤2：验证生效

1. 登录 对象存储 COS 控制台，在左侧菜单栏中，单击**存储桶列表**。
2. 在存储桶列表页面，单击用于**存储 APK 母包**的**存储桶名称**。
3. 在文件列表页面，进入 `prefetch-cos-1251558888.cos.ap-guangzhou.myqcloud.com` **根目录**。
4. 单击**上传文件**，首次上传一个文件，例如：v2_src.apk，单击**上传**。

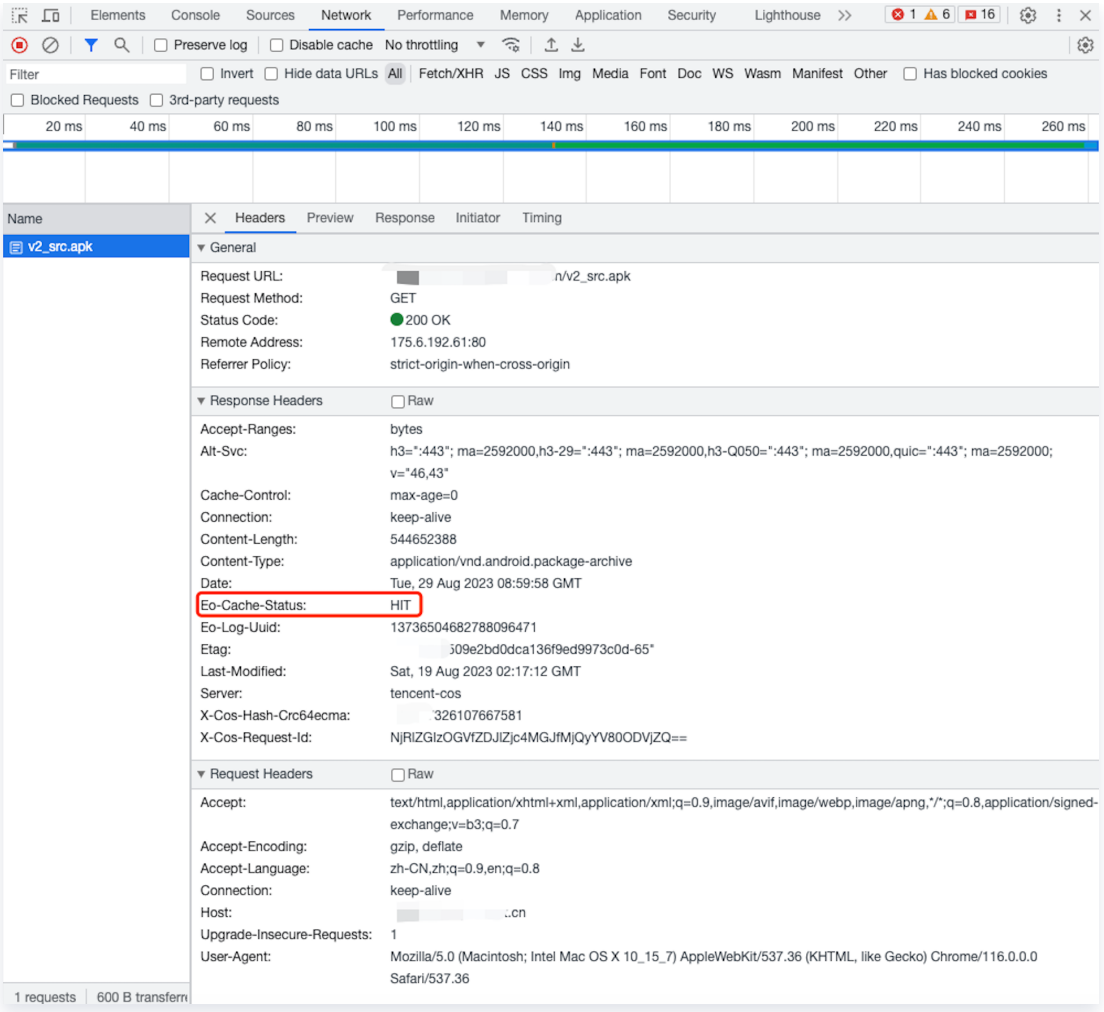


5. 文件上传成功后，在 云函数 SCF 控制台 中，单击 步骤1 创建的**函数名称**。
6. 在函数管理页面，选择**触发管理** > **日志查询** > **调用日志**，通过调用日志获取到函数执行的日志信息，当显示调用成功，且日志内 key 信息与刚才上传的文件名称一致，则表示文件上传到 COS 已触发云函数 SCF 调用 EdgeOne 缓存预热 API 成功。



7. 前往 **边缘安全加速平台 EO 控制台**，进入当前站点 `example.com` 后，单击**站点加速 > 预热缓存**。
8. 在预热缓存页面，单击**历史记录**，查看预热结果是否成功，如显示预热成功，表明当前已完成预热。

9. 在浏览器打开开发者工具后，输入该文件的访问路径访问，例如：`www.example.com/v2_src.apk` 。查看响应头内的 EO-Cache-Status 值。如未预热资源，首次访问资源时将显示为 MISS，下图显示为 HIT，则表示资源已提前自动预热到边缘节点，即已实现首次访问也可以命中缓存。



监控告警（建议）

EdgeOne 对于预热任务会设置配额限制，具体配额请参见 套餐选型对比 。

对于超过配额上限的预热缓存任务，在调用预热缓存 API 接口时会触发报错，最终云函数的执行状态为“调用失败”，为了及时关注到该问题，建议您通过云监控配置云函数的监控告警。配置方法请参见：云函数配置告警 、云函数监控指标说明 。

EdgeOne + COS 场景实现自动清除缓存

最近更新时间：2025-01-14 18:07:53

本文主要介绍了如何通过腾讯云 对象存储（Cloud Object Storage，COS）和 云函数服务（Serverless Cloud Function，SCF）实现 EdgeOne 自动清除缓存，清除缓存的功能和原理介绍请参考 清除缓存 。

背景介绍

若您的源站为腾讯云对象存储 COS，当源站有同名文件更新或者违规资源需要删除时，通常需要同步将资源从 EdgeOne 节点删除，避免用户仍访问到旧的资源或者违规内容。但是清除缓存需要您在 COS 上更新或删除文件后，人工进入 EdgeOne 控制台或者调用 API 接口提交需清除缓存的 URL，该方式容易遗漏且可能因为人工操作延迟造成未及时执行清除动作。

自动清除缓存可以帮助您在文件上传至腾讯云 COS 后，由腾讯云 SCF 自动检测并调用 EdgeOne 的清除缓存 API 接口自动完成节点的缓存清除，保障您的文件更新或删除后，用户可立即访问到最新的资源，提升用户体验。

注意：

- 腾讯云对象存储 COS 为收费功能，使用中可能产生的费用由腾讯云 COS 收取，具体收费详情请参考 对象存储计费概述 。
- 云函数 SCF 为收费功能，使用中可能产生的费用由云函数 SCF 收取，具体收费详情请参考 云函数计费概述 。

适用场景

场景1：同名文件更新

文件上传至腾讯云 COS 后，由于文件内容有更新，重新上传同名文件至 COS，在 CDN 缓存过期前，希望用户可以立即访问到最新的资源。

场景2：违规文件删除

上传至 COS 的文件，可能存在内容不合规等问题需要将该文件从 COS 存储桶中删除，在 CDN 缓存过期前，希望用户不再能访问到该资源。

操作步骤

示例场景

假设您是一家游戏厂商，已将站点域名 `www.example.com` 接入到 EdgeOne 加速，源站为腾讯云 COS，地址为： `purge-cos-1251558888.cos.ap-guangzhou.myqcloud.com` 。因为有多款游戏 APK 需要经常更新，期望文件变更时即可自动清除 EdgeOne 节点的缓存。

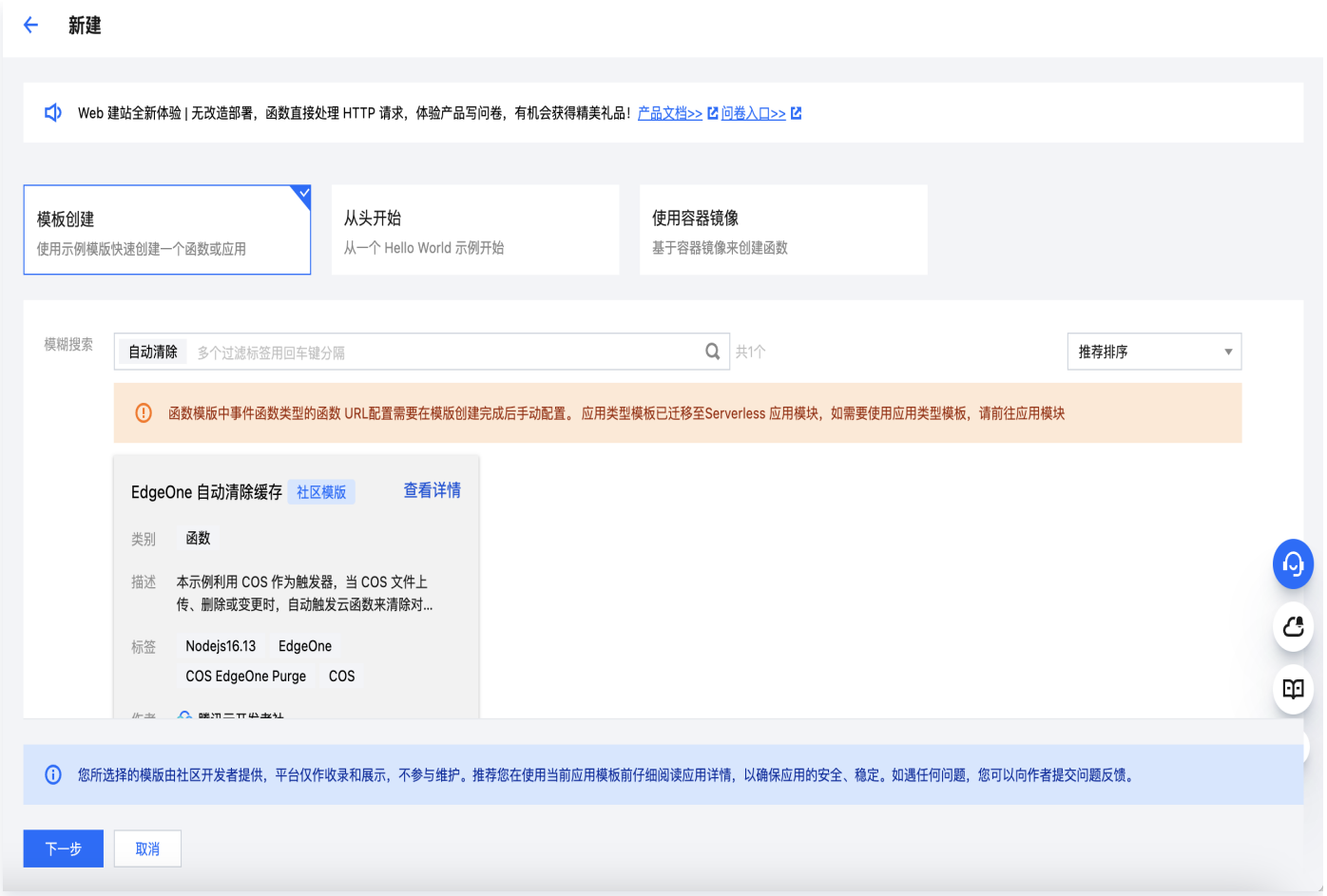
准备工作

1. 已开通 对象存储 COS 和 云函数 SCF，记录该存储桶名称及地域信息。
2. 根据 站点接入 指引添加站点，购买 EdgeOne 套餐，并获取该站点 ID。站点 ID 可通过站点接入后，在站点列表内查看并复制，例如：zone-26v607hq8d3m。

3. 已在 EdgeOne 控制台 添加加速域名 `www.example.com`，且源站配置为腾讯云 COS。

步骤1：创建 EdgeOne 自动清除缓存的云函数并部署

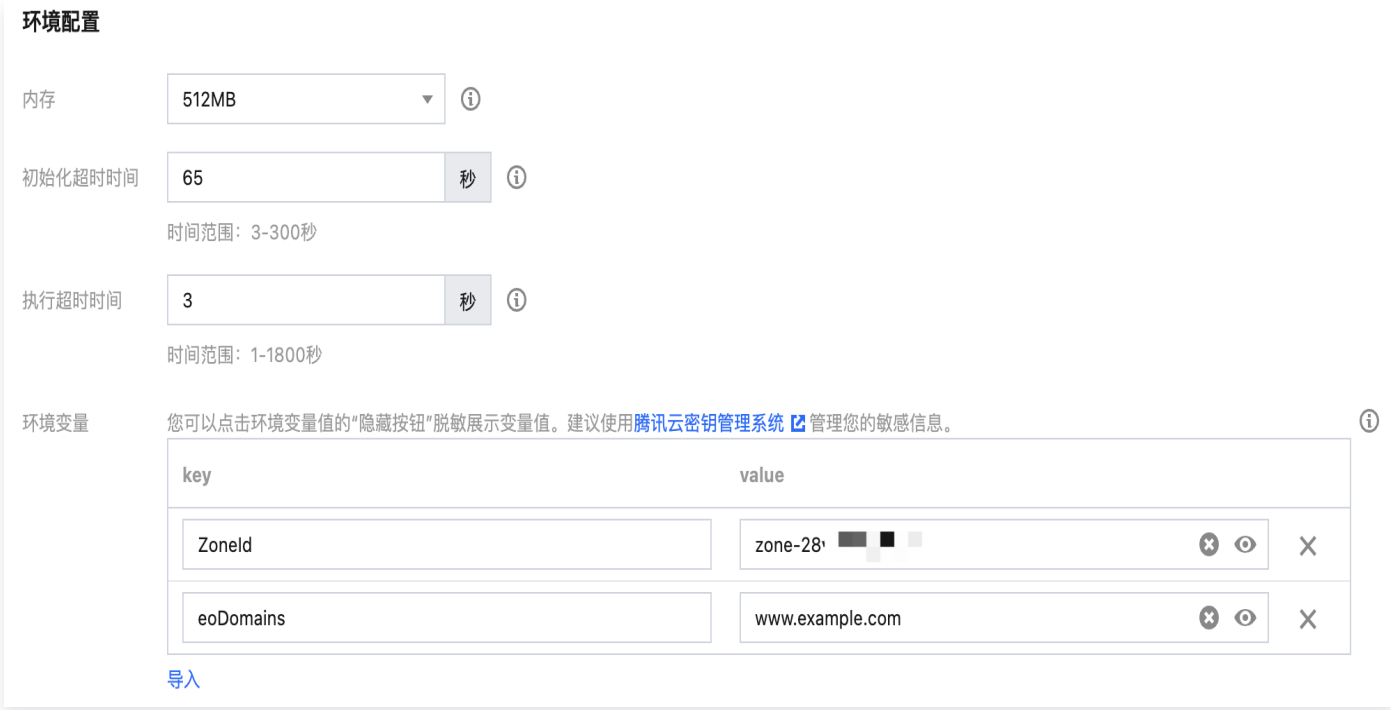
1. 登录 云函数服务控制台，在左侧菜单栏中，单击**函数服务**。
2. 在函数服务页面，单击**新建**，选择**使用模板创建**，在模糊搜索输入框中输入 **EdgeOne 自动清除缓存**并选中，单击**下一步**。



3. 在“函数配置”页面，如下配置为必填项，其他配置项建议保持使用默认配置即可。

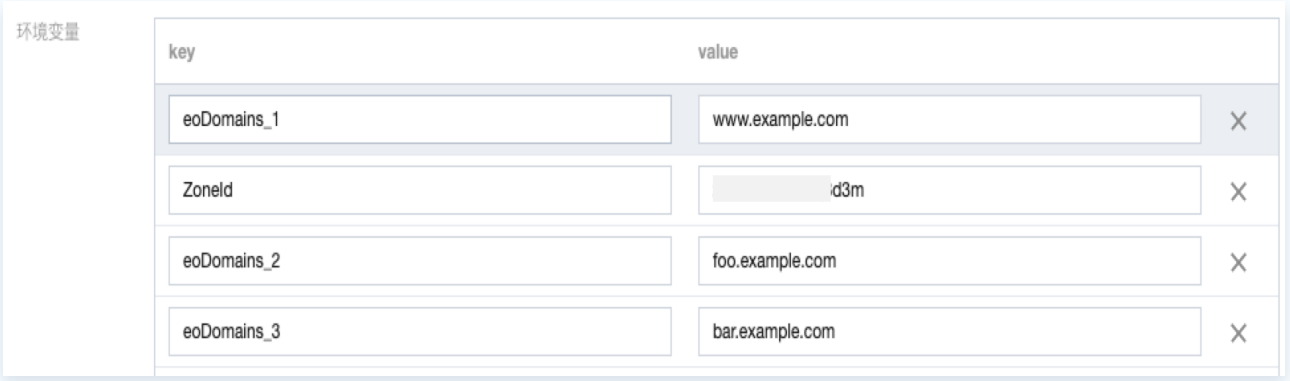
- **基础配置**
  - 函数名称：创建函数时将自动生成一个函数名称，您可以选择自定义修改为一个易识别的函数名称。
  - 地域：请选择对象存储桶 COS 的所在地域，例如：广州。
  - 时区：云函数内默认使用 UTC 时间，您可以通过配置环境变量 TZ 修改。在您选择时区后，将自动添加对应时区的 TZ 环境变量。
- **函数代码：**模板已内置默认函数代码实现 EdgeOne 自动清除缓存的能力，无需改动。
- **高级配置：**

  单击**高级配置**，找到**环境配置**，您需要在环境变量中添加以下 key 和对应的 value 值，其余配置保持默认即可：
  - ZoneId：请填写对应需进行自动清除缓存的域名站点 `example.com` 的 ZoneId，站点 ID 获取方式请参见 准备工作 。
  - eoDomains：请填写已在 ZoneId 下添加好的加速域名，如：`www.example.com` 。

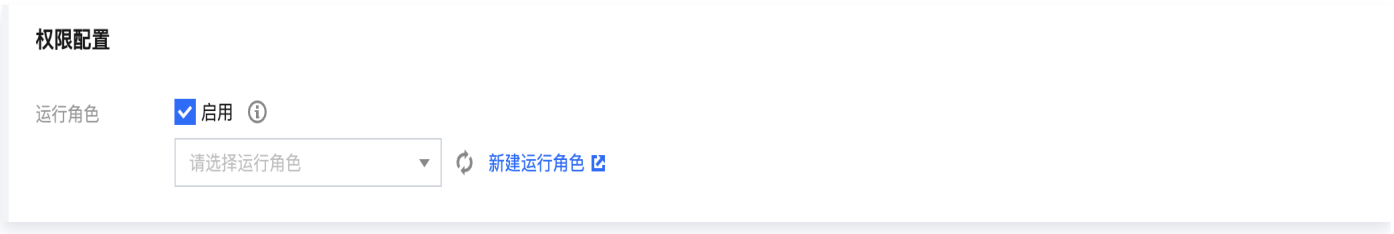


说明：

如果您在当前站点下有多个域名的源站使用了同一个 COS 存储桶，期望多个域名都能触发自动清除缓存，则填写环境配置时，可以填写添加多个环境变量，以 eoDomains 开头，例如：eoDomains_1、eoDomains_2，如下所示：



- 权限配置：运行角色勾选**启用**，通过下拉框选择运行角色（请确保已有角色已包含 QcloudCOSFullAccess 和 QcloudTEOFullAccess 的预设策略），否则请**新建运行角色**。



- **触发器配置**

  以事件类型为 `全部创建` 为例（若需要创建 `全部删除` 事件类型，参照配置即可），在触发器配置中，选择自定义创建，COS Bucket 为与此云函数 SCF 同地域的存储桶，可输入存储桶名称进行模糊查询，例如：`purge-cos-1251558888.cos.ap-guangzhou.myqcloud.com`。其余配置项保持为默认配置即可。

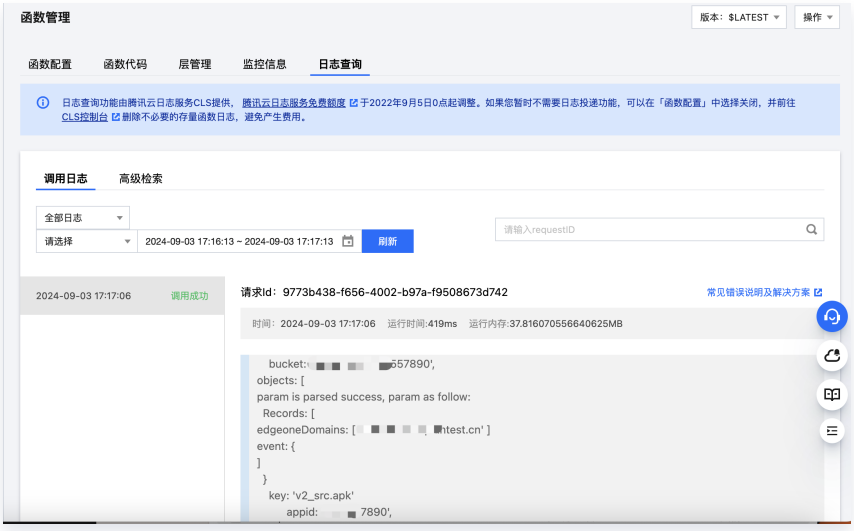
4. 单击**完成**，即可完成 EdgeOne 自动清除缓存函数的创建。

步骤2：验证生效

1. 登录 对象存储 COS 控制台，在左侧菜单栏中，单击**存储桶列表**。
2. 在存储桶列表页面，单击用于**存储 APK 母包**的**存储桶名称**。
3. 在文件列表页面，进入 `purge-cos-1251558888.cos.ap-guangzhou.myqcloud.com` **根目录**。
4. 单击**上传文件**，上传一个同名文件，例如：v2_src.apk，单击**上传**。

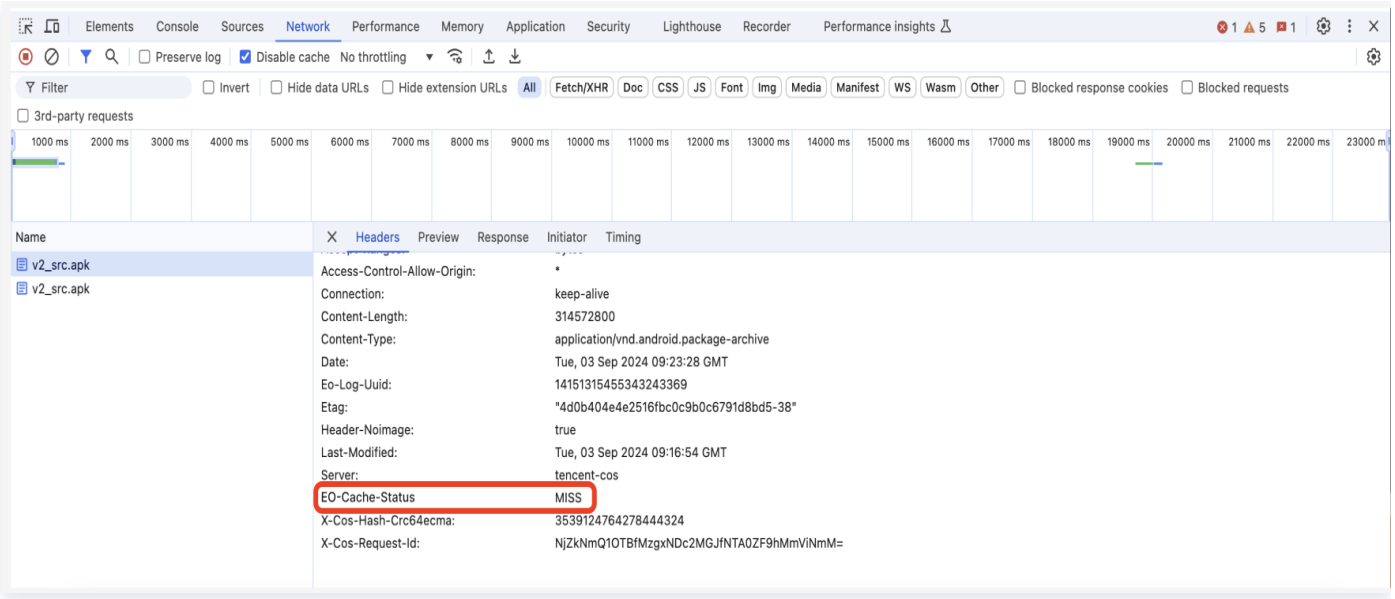
5. 文件上传成功后，在 云函数 SCF 控制台 中，单击 步骤1 创建的**函数名称**。
6. 在函数管理页面，选择**日志查询** > **调用日志**，通过调用日志获取到函数执行的日志信息，当显示调用成功，且日志内 key 信息与刚才上传的文件名称一致，则表示文件上传到 COS 已触发云函数 SCF 调用 EdgeOne 清除

缓存 API 成功。



7. 前往 **边缘安全加速平台 EO 控制台**，在一级导航的**工具集**中单击**清除缓存**。
8. 在清除缓存页面，单击**历史记录**，查清除任务是否成功，如显示清除成功，表明当前已完成清除。

9. 在浏览器打开开发者工具后，输入该文件的访问路径访问，例如：`www.example.com/v2_src.apk` 。查看响应头内的 EO-Cache-Status 值。如未清除缓存，访问资源时会命中之前旧的缓存，下图显示为 MISS，则表示资源已从 EdgeOne 节点清除，用户请求时会回源拉取最新资源。



监控告警（建议）

EdgeOne 对于清除缓存任务会设置配额限制，具体配额请参见 套餐选型对比 。
对于超过配额上限的清除缓存任务，在调用清除缓存 API 接口时会触发报错，最终云函数的执行状态为“调用失败”，为了及时关注到该问题，建议您通过云监控配置云函数的监控告警。配置方法请参见：云函数配置告警 、云函数监控指标说明 。

防盗刷/盗链实践
EdgeOne 防盗刷实践教程

最近更新时间：2025-06-27 10:26:52

本篇文档学习预计需要 20 分钟，通过学习该文档，您可以了解到：

1. 什么是 CDN 盗刷及其常见类型和危害。
2. 如何在 EdgeOne 平台设置流量告警和用量封顶策略，开启实时日志推送，预防 CDN 盗刷。
3. 利用 EdgeOne 的流量分析和日志分析功能，识别和定位盗刷攻击。
4. 针对中小网站平台和企业级业务平台分别给出的 EdgeOne 防盗刷实践教程配置建议。

什么是 CDN 盗刷

CDN 盗刷是指未经授权的用户通过非法手段大量获取网站资源，消耗网站带宽和服务器资源的行为。相比于 DDoS 攻击直接影响网站可用性，CDN 盗刷更多的是消耗网站的带宽等计算资源，产生突发高带宽或者大流量，导致高于日常消费金额的账单，网站运营成本急剧升高。CDN 盗刷的常见手段包括：

- 通过自动化工具、代理服务器或僵尸网络发送大量虚假请求；
- 通过自动化工具不断下载大文件或进行大量数据传输；
- 通过压力测试工具发送大量并发请求，对服务器进行超负荷测试。

> **说明：**
> 如果您当前使用的是腾讯云内容分发网络 CDN，建议升级至 EdgeOne，并在 EdgeOne 上配置相应的防护策略。通过合理配置防护措施，可以有效减少 CDN 盗刷带来的影响，保障业务正常运行，避免高额账单。CDN 服务迁移方式可参考 内容分发网络 CDN 相关服务迁移至 EdgeOne 工具使用指南 。

预防措施

设置用量封顶策略

对网站关键指标（如带宽、流量、请求数等）添加用量封顶策略进行控制，设置合理的用量上限和告警阈值，是防止因盗刷攻击产生高额账单消耗的有效策略。一旦出现告警，立刻根据 排查措施 排查实时请求是否正常，并按 应对措施 进行相应处理。

> **说明：**
> - 用量封顶配置生效存在一定延迟（10分钟左右），期间产生的消耗会正常计费。
> - 封顶策略均根据子域名维度统计用量，生效范围选择站点或全部子域名时表示站点下的所有子域名共用一个封顶策略。
> - 同一个域名流量、带宽或请求数策略同时存在时，只要其中一项达到阈值，则会触发域名停用服务。

- 当前仅支持 L7（应用层）流量/带宽和 HTTP/HTTPS 请求配置封顶策略，L4（传输层 TCP/UDP 应用）流量以及其他增值服务如 QUIC、BOT 等业务暂不支持。

配置示例

配置用量封顶策略，具体操作，请参见 用量封顶策略 。在添加封顶策略窗口中，选择生效站点，并根据以下建议配置封顶策略：

配置维度	配置选项	相应建议	适用场景
统计周期	**5 分钟（推荐选择）**	设置较低的阈值，以便迅速发现并响应异常流量或请求。	能够及时发现短时间内的异常流量或请求峰值，快速采取防护措施，适用于实时监控和即时响应需求。
	小时	设置中等阈值，结合日常正常业务高峰期数据，确保短时间内流量突增时不误触封顶。	能够捕捉到短时间内的流量波动趋势，提供一定的反应时间进行防护调整。
	天（24 小时）	设置较高的阈值，基于正常业务日流量的2-3倍，确保在长时间内异常流量被识别。	能够提供全局视角，识别全天范围内的异常流量或请求模式，适用于制定长时间内的防护策略和资源规划。
封顶配置	**七层流量（推荐选择）**	根据正常业务流量的2-3倍设定流量阈值，以应对流量突增的情况，避免因短时间内的正常流量增长而误触封顶。	有效防止攻击者通过大量下载大文件等方式消耗带宽资源。
	HTTP/HTTPS 请求数	基于正常请求数的2-3倍设定阈值，确保正常业务高峰期不会误触封顶。	有效防止刷请求型攻击，通过大量虚假请求消耗资源。
	七层带宽	根据正常带宽使用量的2-3倍设定带宽阈值，以应对带宽使用突增的情况。	有效防止带宽消耗过高，避免因大流量下载攻击导致的资源浪费。
超出阈值	停止服务，需前往域名列表中重新启用。		
告警阈值	**50%（推荐选择），当访问用量达到配置的告警阈值的 50% 时发出告警消息。**		

说明：
若已开启告警阈值：由于扫描粒度为5分钟，短时间内用量剧增较大时，可能上一次扫描未触发告警阈值，下一次扫描直接达到访问阈值。在此情况下，会同时发送百分比告警和访问阈值告警通知。

开启实时日志推送

为了实现精细化的防护措施，建议开启 实时日志推送 功能。该功能能够以较低的时延将请求访问日志投递到您指定的目的地，支持通过控制台或 API 配置。从请求发起到目的地接收日志的延迟在 5 分钟以内，适合需要实时监控和快速排障的场景，如防范 CDN 盗刷。通过对访问行为进行实时分析，可以及时识别并分析盗刷攻击特征，从而配置相应的策略进行精准拦截。以下是各日志类型记录的请求范围：

- **站点加速日志：**记录域名访问日志，默认仅记录防护后的请求日志，不记录防护拦截请求日志。站点加速日志记录了域名访问日志，包括所有通过 CDN 的L7请求日志。这些日志能够提供全面的访问情况，帮助识别异常高频请求、异常流量和潜在的盗刷行为。

  > **说明：**
  > 实时日志-站点加速日志记录全量 L7 请求日志、包含 L7 防护拦截日志的功能在内测中，如有需求请 联系我们 。

- **速率限制和 CC 攻击防护日志：**仅记录命中 L7 防护-速率限制、CC 攻击防护模块安全规则的请求日志，不论是否被拦截。可帮助识别试图通过高频请求刷流量的行为。
- **托管规则日志：**仅记录命中 L7 防护-托管规则模块安全规则的请求日志，不论是否被拦截。可帮助检测基于托管规则的防护情况，识别潜在的攻击和盗刷行为。
- **自定义规则日志：**仅记录命中 L7 防护-自定义规则模块安全规则的请求日志，不论是否被拦截。可帮助识别符合自定义规则的异常请求，防止特定类型的盗刷行为。
- **Bot 管理日志：**仅记录命中 L7 防护- Bot 管理模块安全规则的请求日志，不论是否被拦截。可帮助识别由自动化脚本或恶意 Bot 引发的盗刷行为。

  > **说明：**
  > Bot 管理日志仅当站点域名开启 Bot 管理能力后支持，开启后，Bot 管理的计费标准详见：增值服务用量单元费用（后付费）。

若您需要推送 HTTP 请求头、HTTP 响应头或 Cookie 中的某些字段值，您可以通过 自定义推送日志字段 功能将此类信息精确记录在日志中。

排查措施

在设置如前文所述的预防措施后，若收到告警并判断用量突增明显，下一步就需要考虑开展深入排查。本节重点介绍如何利用 EdgeOne 的流量分析和日志分析功能，对疑似盗刷流量进行多维度特征分析定位。

流量分析

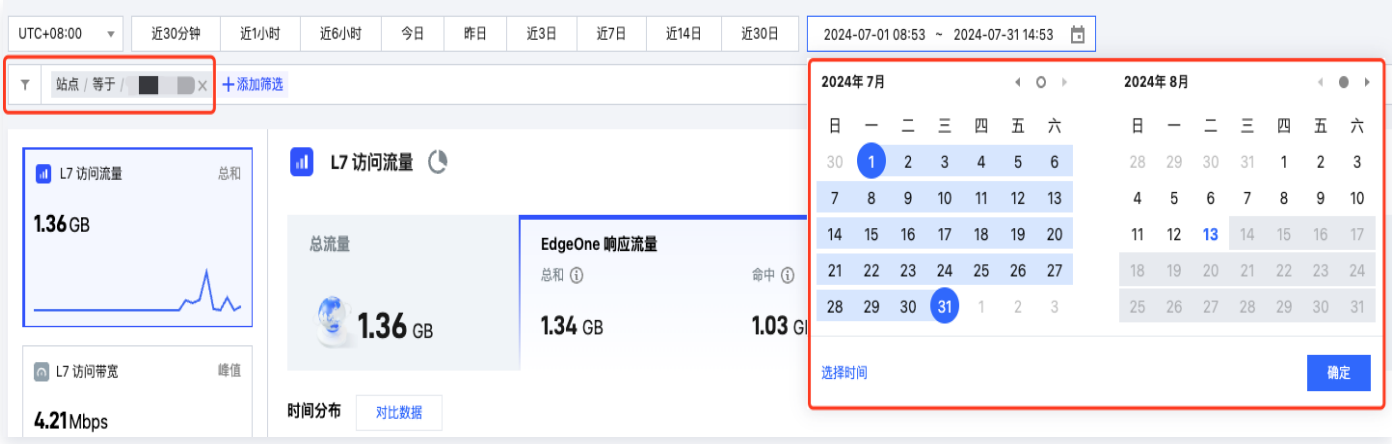
指标分析 是 EdgeOne 提供的一项强大的数据分析服务，旨在帮助用户深入洞察业务运行和安全状况。通过实时监控和分析关键指标，用户可以快速识别问题、优化资源配置，并提升业务的稳定性和安全性。在盗刷攻击排查场景下，建议通过 数据筛选与过滤，结合 TOP 排行，重点关注以下数据：

- Referer 分布：空 Referer 或非法 Referer 的集中出现，往往是撞库、爬虫等恶意请求的标志。
- URLs 资源类型的访问量变化：若少数 URL 或资源类型的请求量突增，远超其他资源，提示可能正遭受针对性的盗刷。

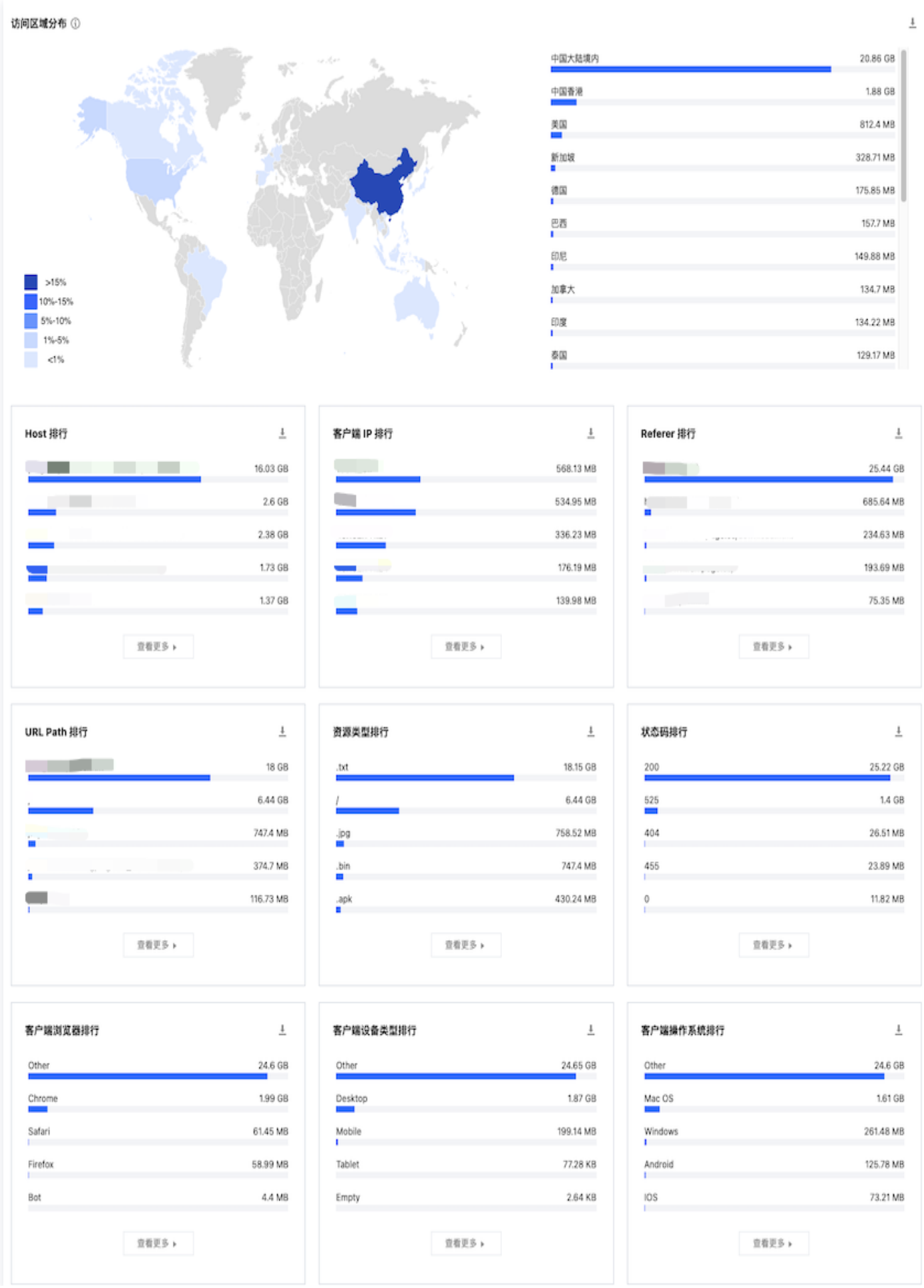
- 客户端 IP TOP：观察是否存在少量 IP 贡献了大部分请求，评估基于 IP 的请求频率控制的可行性。

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**指标分析**。
2. 在指标分析页面，单击**添加筛选**，将出现用量告警的站点加入筛选。
3. 选择日期为疑似遭受盗刷攻击的时间段。



4. 在 L7 访问流量页面，下拉查看以下维度的排行：
   - **Hosts**：客户端请求的子域名。
   - **URLs**：客户端请求的具体资源路径。
   - **资源类型**：客户端请求的资源类型，例如：“.png”“.json”等。
   - **客户端 IP 地址**：客户端请求的具体来源 IP 地址。
   - **Referers**：客户端请求的 Referer 信息。
   - **客户端设备类型**：
     - 设备类型：客户端请求所使用的硬件设备类型，取值有：
       - TV：电视。
       - Tablet：平板电脑。
       - Mobile：手机。
       - Desktop：电脑。
       - Other：其他。
     - 浏览器：客户端请求使用的浏览器类型。
     - 操作系统：客户端请求使用的操作系统类型。


访问区域分布
>15%
10%-15%
5%-10%
1%-5%
<1%
中国大陆境内 20.86 GB
中国香港 1.88 GB
美国 812.4 MB
新加坡 328.71 MB
德国 175.85 MB
巴西 157.7 MB
印尼 149.88 MB
加拿大 134.7 MB
印度 134.22 MB
泰国 129.17 MB
Host 排行
16.03 GB
2.6 GB
2.38 GB
1.73 GB
1.37 GB
查看更多
客户端 IP 排行
568.13 MB
534.95 MB
336.23 MB
176.19 MB
139.98 MB
查看更多
Referer 排行
25.44 GB
685.64 MB
234.63 MB
193.69 MB
75.35 MB
查看更多
URL Path 排行
18 GB
6.44 GB
747.4 MB
374.7 MB
116.73 MB
查看更多
资源类型排行
.txt 18.15 GB
/ 6.44 GB
.jpg 758.52 MB
.bin 747.4 MB
.apk 430.24 MB
查看更多
状态码排行
200 25.22 GB
525 1.4 GB
404 26.51 MB
455 23.89 MB
0 11.82 MB
查看更多
客户端浏览器排行
Other 24.6 GB
Chrome 1.99 GB
Safari 61.45 MB
Firefox 58.99 MB
Bot 4.4 MB
查看更多
客户端设备类型排行
Other 24.65 GB
Desktop 1.87 GB
Mobile 199.14 MB
Tablet 77.28 KB
Empty 2.64 KB
查看更多
客户端操作系统排行
Other 24.6 GB
Mac OS 1.61 GB
Windows 261.48 MB
Android 125.78 MB
IOS 73.21 MB
查看更多

5. 单击**添加筛选**，添加如下建议筛选条件，聚焦异常流量，单击**确定**。
   - Referer：定位空 Referer 请求；
   - URL：包含 TOP 5 URLs，定位可疑的热点资源；
   - 资源类型：包含 TOP 5 资源类型，定位热点资源的类型分布；
   - 设备类型：等于 `Other` 和 `Empty`，定位可疑的非常规客户端。

6. 观察筛选后的各项指标分布，识别明显偏离正常水平的数据，分析其与盗刷的关联性。

离线日志分析

为进一步发现盗刷请求的更多特征，需要对**告警发生时段**的 离线日志 进行深入分析。通过字段进行综合分析，可以从源 IP、URL 路径、请求参数、User-Agent、Referer 来源等多个维度描绘盗刷请求画像，为下一步制定精准的应对措施奠定数据基础。离线日志分析进行盗刷排查中可重点关注的日志字段及相应说明如下：

字段名称	数据类型	说明	离线日志是否支持该字段	实时日志是否支持该字段
RequestUrl	String	客户端请求的 URL 路径，不含查询参数。对于刷量攻击，该字段是关键分析维度。	✓	✓
RequestUrlQueryString	String	客户端请求 URL 中的查询参数。若被刷请求的查询参数固定或特征明显，可对请求的源 IP 或匹配该参数的请求设置黑名单。	✓	✓
RequestUA	String	客户端请求的 User-Agent 信息。简单的刷量工具常使用相同 User-Agent。若某个 User-Agent 的访问集中且为非常见类型，可考虑封禁。	✓	✓
RequestReferer	String	客户端请求的 Referer 信息。正常请求的 Referer 通常为该站点的其他页面 URL 或搜索引擎 URL，而 curl 等命令行工具可能伪造 Referer。若被刷页面实际不会被其他站点引用但出现 Referer，可判定	✓	✓

		为异常。可通过配置 Referer 防盗链 阻断。		
ClientIP	String	与 EdgeOne 节点建连的客户端 IP，即请求的源 IP。若少量IP 的访问量远超其他 IP，可考虑封禁。	✓	✓
EdgeResponseBodyBytes	Integer	节点返回给客户端的响应体大小，单位：Byte。恶意刷量常反复下载大文件，从 EdgeResponseBodyBytes 的统计结果分析是刷量分析的关键一步。	✓	✓

更多字段及相应说明，请参见 七层访问日志字段说明 。下载离线日志的详细操作请参见 离线日志 。

应对措施

针对网站盗刷这一复杂多变的攻击场景，没有一招鲜吃遍天的招式。EdgeOne 提供了丰富的访问控制、速率限制等防护功能，可灵活组合应用，因此需要根据攻击特征、业务实际情况等因素，选择最优的防护配置组合。下面从个人站点运营者和线上业务站点的不同视角，给出具体的 EdgeOne 防盗刷实践教程。

中小网站平台

场景一：基于指标分析的异常来源 IP 快速拦截

场景示例

在疑似盗刷时间段内，通过分析 L7 访问流量资源类型排行指标，发现一个 5MB 大小的文件访问占比异常偏高。进一步排查该文件路径为 `/test/installer.apk` ，且其请求主要来自 `1.1.1.0/24` 网段的客户端 IP。基于以上线索，可迅速创建 IP 黑名单策略，拦截该恶意网段，遏制潜在的盗刷行为。

配置推荐

推荐您使用 EdgeOne Web 防护功能的自定义规则，配置防护策略，具体操作，请参见 自定义规则 。

- 对于个人版用户，可以在**基础访问管控**中，配置规则类型为**客户端 IP 管控**，匹配方式选择为**客户端 IP 等于**，匹配内容为 `1.1.1.0/24` ，处置方式为拦截。

- 对于基础版及以上用户，可以在**精准匹配规则**中，配置匹配字段为**客户端 IP 匹配** `1.1.1.0/24` **AND 请求路径（Path）包含** `/test/installer.apk` **的请求，处置方式为 JavaScript 挑战**。

场景二：基于日志分析的异常 User-Agent 快速拦截

场景示例

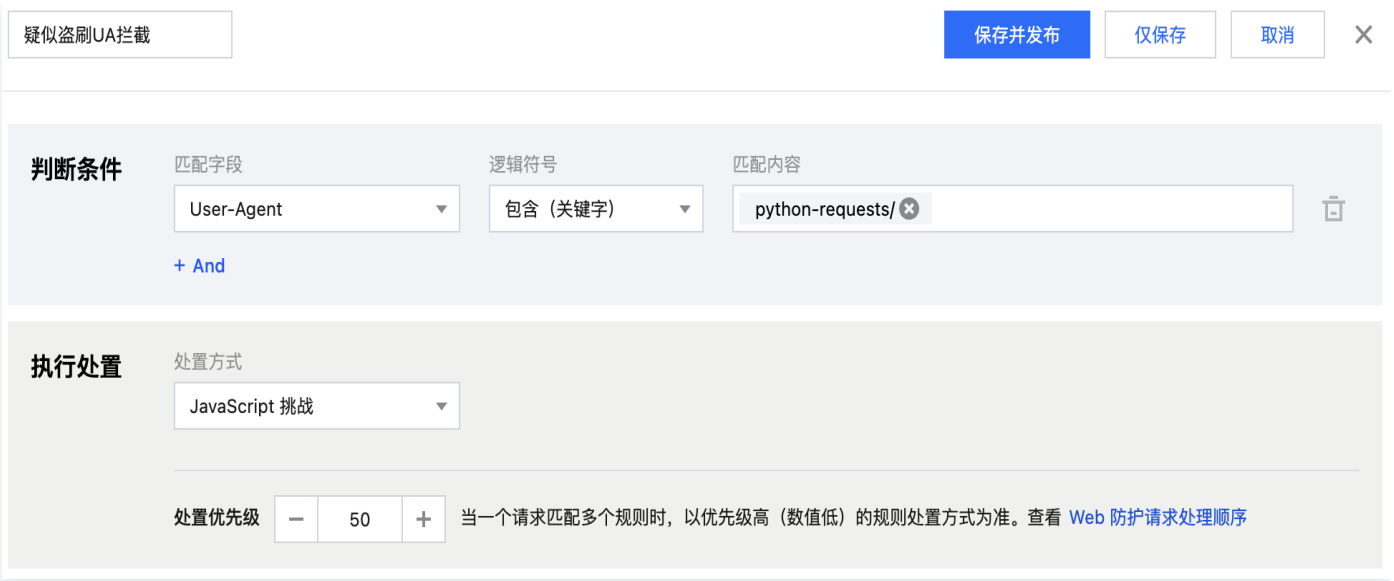
实时日志显示，某时段内 RequestUA 分布异常集中，进一步分析发现访问次数最高的是 `python-requests/2.22.0`，并同时有大量请求使用了含 python-requests/ 等 Python 脚本特有的 User-Agent 标识。由于这类请求明显偏离常规浏览器的 User-Agent 特征，可判定为自动化请求，甚至是恶意爬虫。据此可配置 User-Agent 黑名单规则，精准拦截含特定 User-Agent 标识的可疑请求。

配置推荐

推荐您使用 EdgeOne Web 防护功能的自定义规则，配置防护策略，具体操作，请参见 自定义规则 。

- 对于个人版用户，可以在基础访问管控中，配置规则类型为 **User-Agent 管控**，匹配方式为 **User-Agent 通配符匹配**，匹配内容为 `*python-requests*`，处置方式为**拦截**。

- 对于基础版及以上用户，可以在精准匹配规则中，配置判断条件为 **User-Agent 包含** `python-requests/` 的请求，处置方式为 **JavaScript 挑战**。



场景三：基于已知恶意 User-Agent 预防拦截

场景示例

对于已知的常见盗刷工具，可提前配置其特征 User-Agent 字符串到自定义规则中。在站点全局或重点路径下预防性开启该规则，可最大程度降低被此类工具盗刷的风险。常见盗刷 User-Agent 如：空 `User-Agent` `curl/xx.xx` `Wget/xx.xx` `ApacheBench/xx.xx` `python-requests/xx.xx` 。

配置推荐

推荐您使用 EdgeOne Web 防护功能的自定义规则，配置防护策略，具体操作，请参见 自定义规则 。

- 对于个人版用户，可以在**基础访问管控**中配置两条规则；
  - 规则 1：配置规则类型为 **User-Agent 管控**，匹配方式为请求 **User-Agent 为空**，执行动作为**拦截**。
  - 规则 2：在基础访问管控中，配置规则类型为 **User-Agent 管控**，匹配方式为**请求 User-Agent 通配符匹配** `*curl/*` 、 `*Wget/*` 、 `*ApacheBench/*` 和 `*python-requests/*` ，处置方式为**拦截**。

- 对于基础版及以上用户，可以在**精准匹配规则**中配置如下两条规则：
  - 规则 1：在**精准匹配规则**中，配置匹配字段为 **User-Agent 包含** `curl/` 、 `Wget/` 、 `ApacheBench/` 和 `python-requests/` 的请求，处置方式为 **JavaScript 挑战**。

- 规则 2：**在精准匹配规则中，配置匹配字段为 User-Agent 内容为空的请求，处置方式为 JavaScript 挑战。**

场景四：仅放行常见 User-Agent（临时高防）

在遭受大规模 User-Agent 分散式盗刷时，若难以逐一梳理恶意 User-Agent 的特征，可利用反向逻辑，仅允许常见正常浏览器、App 的合法 User-Agent 访问。该方式可一次性过滤大量可疑请求，**但因规则力度大，存在一定误判风险，应结合其他维度特征谨慎使用。**

配置推荐

推荐您使用 EdgeOne Web 防护功能的自定义规则，配置防护策略，具体操作，请参见 自定义规则 。

- **对于个人版用户，可以在基础访问管控中，配置规则类型为 User-Agent 管控，匹配方式为请求 User-Agent 通配符不匹配，匹配内容为** `*Linux*` 、 `*Macintosh*` 、 `*Android*` 、 `*iPhone*` 、 `*iPad*` **和** `*Windows*` **，处置方式为拦截。**

- **对于基础版及以上用户，可以在精准匹配规则中，配置匹配字段为 User-Agent 通配符不匹配 `*Linux*` 、`*Macintosh*` 、`*Android*` 、`*iPhone*` 、`*iPad*` 和 `*Windows*` 的请求，处置方式为 JavaScript 挑战。**

说明：

- 针对 App 场景，正常业务为空 User-Agent，则无需使用该策略。
- 如果 User-Agent 取值是 App 名称，需要将 User-Agent 中正常业务的 App 名称加入匹配内容。
- **强度较高，谨慎配置，为避免误拦截，请结合其他维度特征进行联合判断。**

场景五：设置 CC 攻击单 IP 高频访问限制（临时高防）

平台托管的速率限制规则 通过速率基线学习、头部特征统计分析和客户端 IP 情报等方式识别 CC 攻击，并进行处置。EdgeOne 提供了三种预设 CC 攻击防护策略：

- **自适应频控：**用于应对通过高频和大量并发的连接请求占用服务器资源的 CC 攻击行为，可基于单 IP 源限制访问频次限制。
- **慢速攻击防护：**用于应对通过大量慢速连接请求占用服务器资源的 CC 攻击行为，可基于单会话限制访问连接最低速率，淘汰慢速连接客户端。

- **智能客户端过滤：**融合了速率基线学习、头部特征统计分析和客户端 IP 情报，实时动态生成防护规则。针对来自高危客户端、或者携带高危头部特征的请求进行人机验证。智能客户端过滤默认开启且对符合规则的客户端执行 JavaScript 挑战。

在发生网站疑似遭受盗刷攻击或出现异常用量告警时，建议临时将自适应频控设置为**自适应 – 紧急**级别，处置方式为 **JavaScript 挑战**。此举可高效阻止恶意 IP 的大量请求，有效防范盗刷和其他攻击行为。具体操作，请参见 CC 攻击防护 。

> **说明：**
> 请在应对完盗刷攻击后及时恢复高频访问请求限制等级为推荐配置：**自适应 – 宽松**，以确保正常业务流量的顺畅访问。详细了解各限制等级的说明，请参考 平台托管的速率限制规则 。

场景六：基于业务水位进行个性化频次控制

在与 DDoS 强攻击的区别是，盗刷往往更加隐蔽，需要结合特定业务场景来进行判断，制定**个性化的频次限制策略**，以避免误拦截合法用户。无论是针对 IP 还是 User-Agent 的拦截策略都属于精准拦截。然而，在实际攻击中，攻击特征可能不会明显，特别是源 IP 的请求量可能高达数十万。
结合业务场景的防御策略首先需要网站管理者**评估业务的正常访问模式，确定业务流量基线**。例如在 App 的下载或升级场景下，大多数 IP 通常只会进行一两次下载，少数情况下可能因失败而多次尝试，但通常在合理的频次范围内。如果出现异常的高频率访问，很可能是攻击或恶意刷量的迹象。
在网站遭受盗刷攻击时，域名的带宽将显著增加。为了应对这种情况，推荐您使用 EdgeOne Web 防护功能的速率限制，根据正常业务水位设定阈值，配置限速策略，或通过 实时日志 监控和调整策略。具体操作，请参见 速率限制 。

> **注意：**
> 配置频次控制规则时应根据实际防御效果动态调整。初期可以基于经验值设定频次阈值以快速实现防御，如果发现效果不佳，则可以逐步收紧；反之，如果规则影响了正常业务，就需要适当放宽。

基于业务基线的游戏包下载限频

场景示例

某游戏平台提供多款游戏的安装包和更新包下载服务，通过 EdgeOne 加速分发。游戏包的下载 URL 具有固定的模式，例如：

- 游戏 A 安装包：`https://cdn.example.com/games/A/installer_v1.0.zip`
- 游戏 A 更新包：`https://cdn.example.com/games/A/patch_v1.1.zip`
- 游戏 B 安装包：`https://cdn.example.com/games/B/installer_v2.0.exe`
- 游戏 B 更新包：`https://cdn.example.com/games/B/patch_v2.1.exe`

游戏版本发布当天，单 IP 下载次数通常为 1 次，个别网络问题导致的重试下载不超过 3 次。但某些 IP 在版本发布后频繁下载安装包和更新包，远超正常用户的行为，触发用量告警。推测可能是盗版网站或分享社区在抓取游戏包，或攻击者意图消耗带宽，可通过配置 速率限制 规则及时阻断这些恶意请求。

配置推荐

在**精准速率限制**中，配置匹配对象为**自定义防护对象**，匹配字段为**请求 URL 包含** `games/` 、 `installer/` 、 `patch/` **AND 请求方式（Method）等于** `GET` 。统计**单个客户端 IP 请求到 EdgeOne 节点**的请求速率，计数值在 **10 分钟**内，超过 3 次时触发，处置方式为 **JavaScript 挑战**，处置持续时间为 **1 小时**。详细操作步骤，请参见 速率限制 。

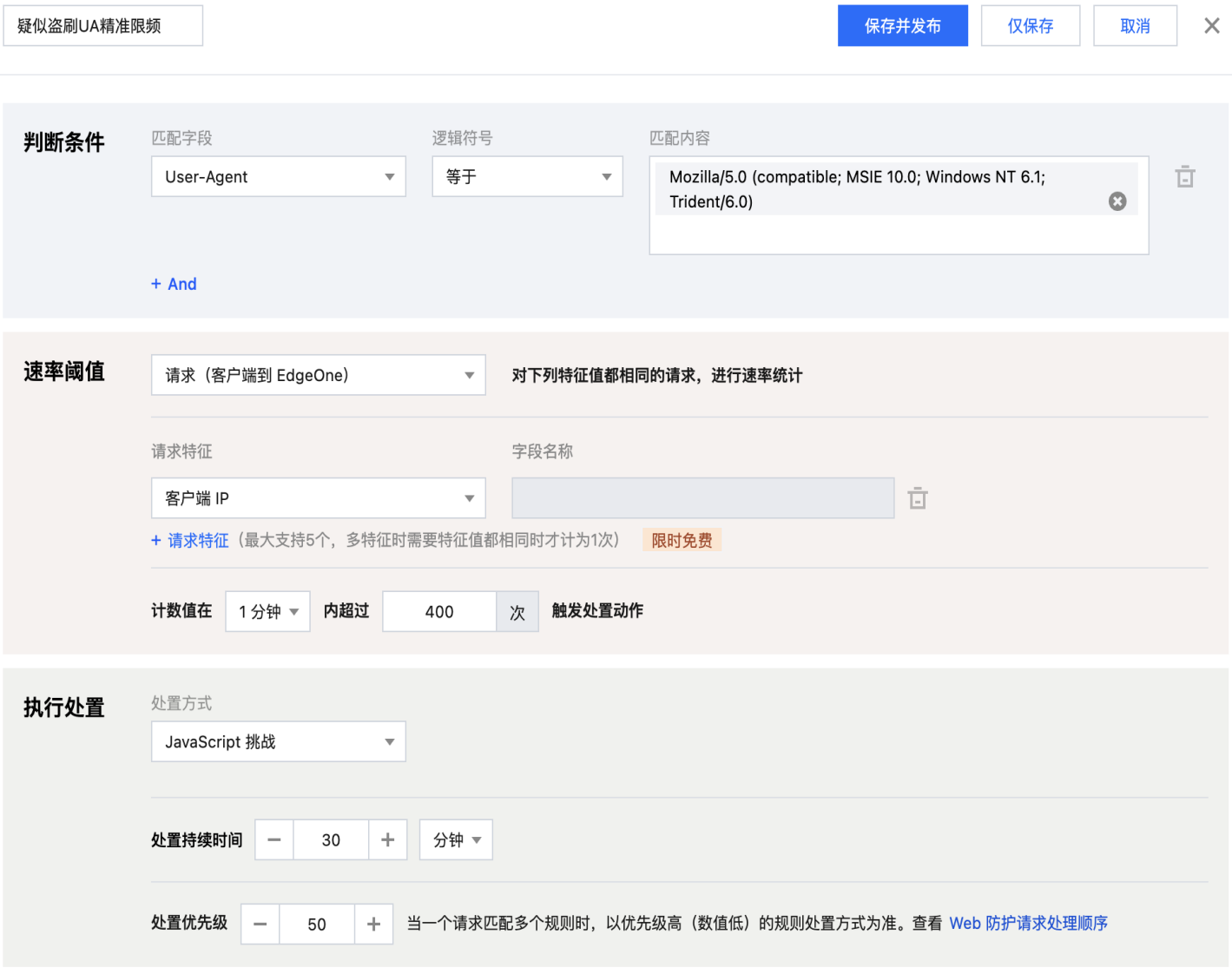
基于日志分析的异常 User-Agent 限频

场景示例

某站点被攻击者大量访问导致用量告警，通过查看实时日志发现访问 IP 分散，可能是分布式攻击，但 User-Agent 非常集中，如：`Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; Trident/6.0)`，与正常业务不符。对比平常未被攻击的时间段，发现正常 User-Agent 多样化，覆盖不同浏览器和设备。该可疑 User-Agent 平时访问量极低，此次激增占据大部分流量，基本可判定为 CDN 盗刷攻击，可通过配置 速率限制 规则及时阻断这些恶意请求。

配置推荐

在**精准速率限制规则**中，配置匹配对象为**自定义防护对象**，匹配字段为 User-Agent 等于 `Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; Trident/6.0)`，统计**单个客户端 IP 请求到 EdgeOne 节点**的请求速率，计数值在 **1 分钟**内，超过 **400** 次时触发，处置方式为 **JavaScript 挑战**，处置持续时间为 **30 分钟**。详细操作步骤，请参见 速率限制 。



说明：

您需要根据自身业务正常水位和实时日志中攻击者特征和频次评估，调整触发防护的阈值和处置时长。

EdgeOne 防盗链实践教程

除了针对盗刷本身的直接防护措施外，网站还应重视对资源本身的保护，采取主动防御。防盗链是避免网站资源被未授权使用的重要手段。

盗链是指未经网站所有者许可，在其他网站上非法引用、使用原站点的资源（如图片、视频、软件包等），消耗原站点的带宽和资源的行为。它不仅侵犯了原站点的合法权益，也可能对其产生不利的 SEO 影响。因此积极采取防盗链措施十分必要。

EdgeOne 提供了完善的防盗链解决方案，可从 Referer 防盗链、Token 防盗链、远程鉴权等多个角度对盗链行为进行管控，保护您的内容免受未经授权的盗链访问，提升加速服务的安全性。更多详情，可参考 EdgeOne 防盗链实践教程 。

企业级业务平台

对于面临盗刷威胁的线上业务站点，除了采用个人站点常用的通用防护手段外，建议选择 EdgeOne 标准版或企业版，并开通 Bot 管理 功能，利用其内置的人工智能引擎和丰富的行为特征分析，您将获得更智能、更省心的 Bot 管理体验，从容应对各类盗刷攻击。

Bot 智能分析 模块采用先进的机器学习算法，通过海量数据训练形成威胁识别模型。该模型从请求速率、IP 情报、URL 序列、SSL/TLS 指纹等多维度提取请求的关键行为特征，通过聚类分析、相似度比对等技术，准确判断请求来源是否为自动化程序，以及是否具有恶意目的，以全方位、立体化的分析方法降低了对合法请求的误伤。

此外，EdgeOne 企业版还支持 JA3 指纹特征，网站管理员可针对自身业务场景，预设高危 Bot 的指纹条件，实现对特定攻击工具的精准拦截。例如，将恶意爬虫常用的 Python 库、无头浏览器等指纹纳入盗刷防御规则，即可自动拦截相关流量，让防护更加主动和高效。

> **说明：**
> Bot 管理功能仅当站点域名开启 Bot 管理能力后支持，开启后，Bot 管理的计费标准详见：增值服务用量单元费用（后付费）。

EdgeOne 防盗链实践教程

最近更新时间：2025-06-26 11:21:23

本文为您介绍如何通过 EdgeOne 提供的防盗链能力，保护您的内容免受未经授权的盗链访问，提升加速服务的安全性。

背景介绍

盗链指的是其他网站或应用程序直接链接到您的资源，而未经您的授权。这种行为可能对您的网站造成严重影响。首先，盗链会消耗您的带宽和服务器资源，导致网站速度变慢，甚至可能导致服务器崩溃。其次，盗链可能导致您的内容被滥用或未经授权传播，这将严重损害您的品牌形象和声誉。
为了应对这些问题，EdgeOne 提供了一系列强大的防盗链能力。通过使用 EdgeOne 的防盗链功能，您可以确保只有经过授权的用户才能访问和使用您的内容。您可以设置白名单，仅允许特定的域名或 IP 地址访问您的资源，从而阻止未经授权的盗链行为。此外，您还可以根据需要灵活配置自定义的防盗链规则。
借助 EdgeOne 的防盗链能力，可以有效保护您的内容安全。您可以放心提供高质量的内容，而无需担心盗链和滥用问题。这将有助于维护您的品牌形象和声誉，同时节省带宽和服务器资源，提升网站的性能和可靠性。

实现方式

1. **HTTP 应答：**实现基础访问控制，如 IP 黑白名单、Referer 黑白名单、UserAgent 黑白名单、区域访问控制。详情请参见 HTTP 应答 。该方式存在的问题是：
   - IP 地址可以被伪造或隐藏，使攻击者能够绕过 IP 黑白名单的限制。他们可以使用代理服务器、虚拟专用网络（VPN）或其他技术来隐藏真实的 IP 地址，从而绕过访问限制。这使得 IP 黑白名单在防止未经授权访问方面变得不够可靠；
   - Referer 头部也容易被伪造。攻击者可以通过修改 HTTP 请求头部中的 Referer 字段来绕过 Referer 黑白名单的限制。他们可以使用浏览器插件、代理工具或其他技术来修改 Referer 字段，使其看起来像是来自受信任的来源，从而绕过访问限制；
   - User-Agent 头部的问题和 Referer 头部类似，同样存在容易被伪造的风险。
2. **Token 鉴权：**即时间戳防盗链，安全性更高，更可靠。详情请参见 Token 鉴权 。该方式相对上述基础访问控制，优势及问题如下：
   - 防止链接的重复使用：每个链接都包含时间戳参数，即使链接被转发分享，一旦时间戳过期，则其他人无法使用该链接获取到资源。
   - 难以伪造：时间戳防盗链增加了对盗链的难度，因为攻击者需要知道鉴权算法、鉴权密钥、时间戳格式等信息方可构造出可通过校验的 URL，而这些信息攻击者很难猜测或伪造；
   - 客户端需改造：该功能的使用需要客户端和 EdgeOne 配合，客户端发起加密的 URL 请求后，EdgeOne 负责根据预先设定的规则对 URL 进行合法性验证。因此在实施时需要考虑一些额外的开销和复杂性。
3. **边缘函数：**定制化的防盗链能力，如远程鉴权等，可通过 边缘函数 支持。该方式的优势及问题如下：

版权所有：腾讯云计算（北京）有限责任公司

- 高度安全性：远程鉴权可以提供更高的安全性。鉴权过程由客户提供的远程服务器完成，而非 EdgeOne 节点服务器，减少了被攻击者窃取的风险；
- 灵活性和可扩展性：远程鉴权提供了更大的灵活性和可扩展性。客户可以灵活控制鉴权逻辑，从而适应不断变化的业务需求和用户访问模式。
- 客户需改造：客户需要部署远程鉴权服务，并确保远程服务器的可靠性、安全性和性能，以避免鉴权延迟增加，从而影响服务质量。此外，为了应对可能的异常情况，需要设置适当的鉴权超时时间。通常情况下，如果鉴权超时，则直接放行请求。然而，如果鉴权服务出现异常，可能会导致非法请求被放行，从而增加安全风险。

操作指南

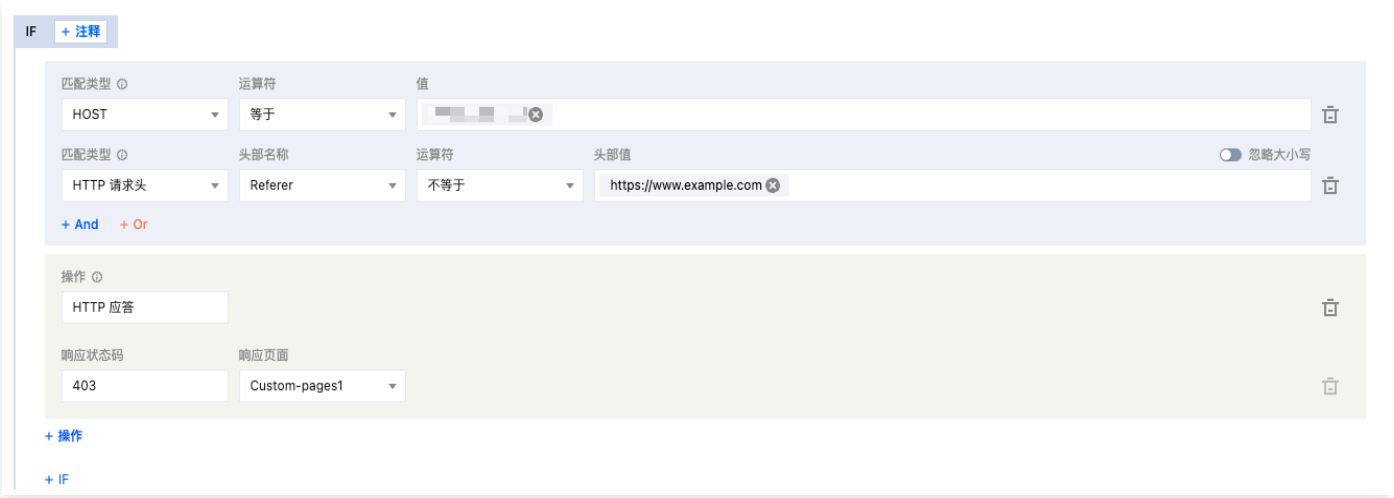
Referer 防盗链

基于 HTTP 请求头中的 Referer 字段设置访问控制规则，实现对访客的身份识别和过滤，防止网站资源被非法盗用。配置 Referer 黑白名单，EdgeOne 会根据名单识别请求身份，允许或拒绝访问请求。允许访问请求，EdgeOne 会返回资源链接；拒绝访问请求，EdgeOne 会返回 403 响应码。

配置示例

若您 `example.com` 站点下的 `www.example.com` 域名业务仅允许 Referer 为 `https://www.example.com` 的访问，其它请求则直接 403 拒绝，可参考以下步骤：

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，单击**规则引擎** Tab 页。
3. 在规则引擎页面，单击**创建规则**，选择**新增空白规则**。
   3.1 在规则编辑页面，匹配类型选择为 HOST 等于 `www.example.com`，同时设置匹配类型 HTTP 请求头 Referer 头部值不等于 `https://www.example.com`。
   3.2 单击**操作**，在弹出的操作列表内，选择操作为 **HTTP 应答**。
   3.3 配置响应状态码 403，响应页面通过下拉框选择，若当前无页面，则需要单击**新建页面**先创建，创建完成再引用。
4. 完整的规则配置如下所示，单击**保存并发布**，即可完成该规则配置。



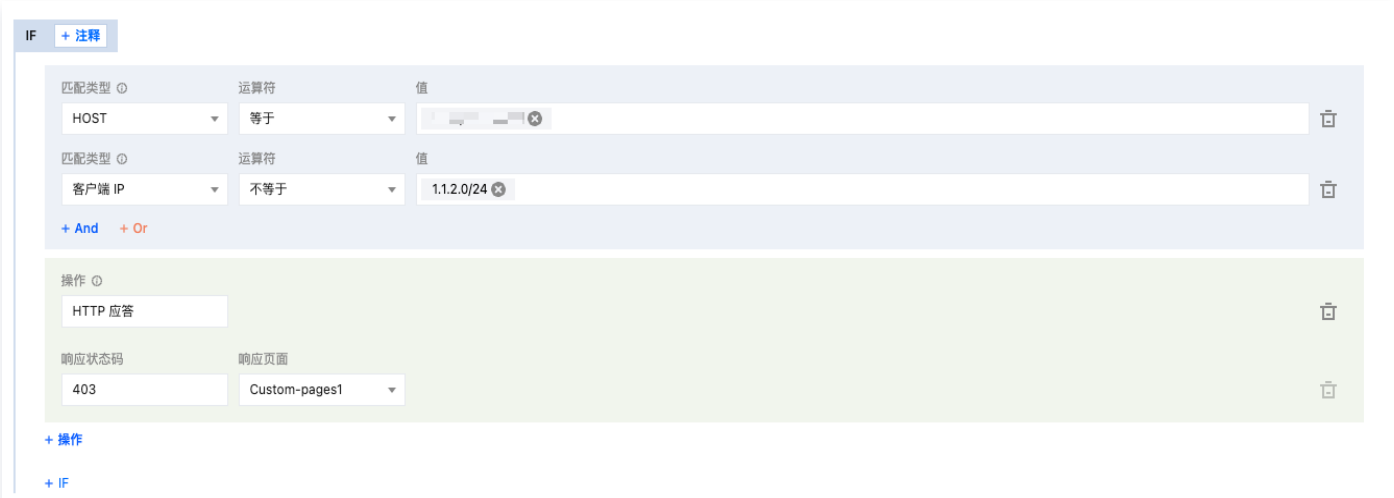
IP 黑白名单

通过配置 IP 黑白名单过滤用户请求，拦截或允许特定 IP 的访问，可以有效限制访问来源，解决恶意 IP 盗刷、攻击等问题。

配置示例

若您 `example.com` 站点下的 `www.example.com` 域名业务仅允许客户端 IP 在 1.1.2.1~1.1.2.254 地址范围（包含 1.1.2.1 和 1.1.2.254）时，才能访问该加速域名下的资源，否则直接 403 拒绝，可参考以下步骤：

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，单击**规则引擎** Tab 页。
3. 在规则引擎页面，单击**创建规则**，选择**新增空白规则**。
   3.1 在规则编辑页面，匹配类型选择为 HOST 等于 `www.example.com`，同时设置匹配类型客户端 IP 等于 `1.1.2.0/24`。
   3.2 单击**操作**，在弹出的操作列表内，选择操作为 **HTTP 应答**。
   3.3 配置响应状态码 403，响应页面通过下拉框选择，若当前无页面，则需要单击**新建页面**先创建，创建完成再引用。
4. 完整的规则配置如下所示，单击**保存并发布**，即可完成该规则配置。



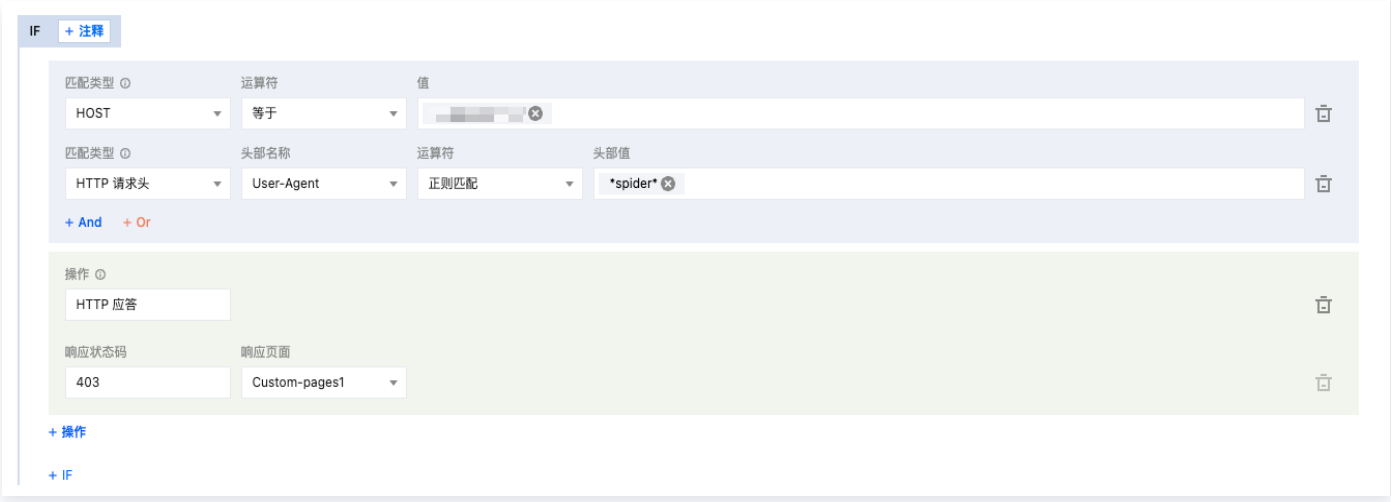
UserAgent 黑白名单

User-Agent 是 HTTP 请求头的一部分，包含用户访问时所使用的操作系统及版本、浏览器类型及版本等标识信息。您可以通过配置 User-Agent 黑白名单规则，限制访问业务资源的用户来源，提升加速的安全性。

配置示例：

若您 `example.com` 站点下的 `www.example.com` 域名业务被谷歌爬虫恶意爬取资源，导致域名带宽突增，严重影响账单。通过分析，发现爬虫请求 User-Agent 包含 `spider`，您希望拦截该类请求，可参考以下步骤：

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，单击**规则引擎** Tab 页。
3. 在规则引擎页面，单击**创建规则**，选择**新增空白规则**。
   3.1 在规则编辑页面，匹配类型选择为 HOST 等于 `www.example.com` 。
   3.2 单击**操作**，在弹出的操作列表内，选择操作为 **HTTP 应答**，同时设置匹配类型 HTTP 请求头 User-Agent 头部值正则匹配 `*spider*` 。
   3.3 配置响应状态码 403，响应页面通过下拉框选择，若当前无页面，则需要单击**新建页面**先创建，创建完成再引用。
4. 完整的规则配置如下所示，单击**保存并发布**，即可完成该规则配置。



Token 鉴权

Token 鉴权是一种实现原理简单、可靠性高的访问控制策略，通过配置鉴权规则进行 URL 访问校验，可有效防止站点资源被恶意盗刷。该功能的使用需要客户端和 EdgeOne 配合，客户端负责发起加密的 URL 请求，EdgeOne 负责根据预先设定的规则对 URL 进行合法性验证。详细的配置使用方式，您可以参考 Token 鉴权 。

远程鉴权

如果您有自己的鉴权服务器，可以通过配置远程鉴权，将用户请求转发至您指定的鉴权服务器，由鉴权服务器对用户请求进行校验，适用于需要精确控制访问权限和实时鉴权验证的场景。EdgeOne 可通过边缘函数实现远程鉴权能力，示例函数可参考 远程鉴权 。

HTTPS 相关实践
通过 EdgeOne 免费证书快速实现 HTTPS 访问

最近更新时间：2025-07-03 10:29:21

本文为您介绍如何通过 EdgeOne 提供的免费证书服务，帮助您的网站快速实现 HTTPS 访问，并且减少后续在证书的更新及维护工作量。

背景介绍

HTTPS 访问已经是目前互联网的主流需求，HTTPS 访问不仅能够更有效地保障用户在访问到网站时的数据安全传输，防止信息泄露、消息劫持等问题，在搜索引擎中，未实现 HTTPS 还会被浏览器提示为不安全网站，并影响搜索权重。因此，网站必须要能够具有 HTTPS 访问能力。

为了实现 HTTPS 访问，需要用户寻找合适的免费证书机构申请免费证书，或者采购可信度更高的付费证书。存在以下的难题：

1. **申请流程复杂：**证书申请需要逐个域名申请，并根据证书颁发机构要求完成 DNS 验证或者 HTTP 验证，在域名数量众多的情况下，需要逐个域名添加 DNS 完成验证，工作量较高。
2. **部署及维护成本高：**证书申请完成后，需要自行在服务器内完成证书部署，证书数量多的情况下，需要逐个域名对应并维护正确的证书，避免出现 HTTPS 访问错误，更新维护工作量较重。
3. **容易过期失效：**证书在过期前必须完成证书更新，否则会出现 HTTPS 访问告警，尤其针对免费证书，当前有效期一般为 3 个月，需要频繁更新。
4. **付费证书使用成本高：**付费证书虽然可以通过申请泛域名证书来减少证书数量并支持自动续期，但是使用成本较高，不适用于小型网站或者域名数量多的业务。

方案优势

EdgeOne 提供的免费证书服务简化了 HTTPS 访问的实现，免去了手动申请、部署和维护证书的繁琐过程。用户只需通过简单的操作即可为网站启用 HTTPS，同时享受自动续期和额外的访问加速及安全防护服务。相比采购付费的 SSL 证书或者自行申请其它机构提供的免费证书，具有以下优势：

1. **申请简单：**只需要在控制台上单击**申请免费证书**即可，EdgeOne 将自动完成后续的证书申请和验证流程。
2. **部署简单：**证书申请完成后将自动下发部署，无需手工下载、部署证书的操作。
3. **自动续期：**免费证书可自动续期，无需人工维护，避免因证书过期导致网站 HTTPS 访问不可用。
4. **同时享受更多服务：**接入 EdgeOne 后，除了具备了 HTTPS 访问的能力，可同时为您的站点提供访问加速及安全防护的相关能力，更进一步提供网站的访问体验。

证书类型	EdgeOne 免费	付费 SSL 证书	自行申请的免费证书

	证书		
费用	**免费**	需额外付费	免费
申请方式	**自动申请并完成验证**	申请时需进行 DNS 验证或者 HTTP 验证	申请时需进行 DNS 验证或者 HTTP 验证
部署方式	**自动部署**	相同云资源内支持一键部署，其它资源需人工部署	需人工进行部署
更新方式	**自动更新**	腾讯云购买的 SSL 证书可支持托管后自动续费/更新，其它来源证书需人工更新	方式一：在到期前自行申请免费证书后手工更新； 方式二：自行维护代码脚本来实现免费证书的自动申请/更新
签发速度	**验证完成后立即签发**	根据证书类型不同，最快1个工作日	验证完成后立即签发
证书公信力	一般	高	一般

说明：

1. 免费证书由 TrustAsia 和 Let's Encrypt 机构颁发，如果您的站点当前为 NS 接入的方式，可申请泛域名证书，如果当前为 CNAME 接入，EdgeOne 只支持申请单域名证书，不支持申请泛域名证书。
2. 证书有效期为 90 天，到期前 15 天平台将自动为您申请续期，无需您手动更新。如果您当前是 NS 接入，切换至 CNAME 接入后，申请的泛域名证书到期后将无法自动续期。
3. 免费证书不支持下载。
4. 如果域名是 CNAME 接入或者 DNSPod 托管接入，您还需要完成 CNAME 配置并等待 CNAME 状态生效，才可以为该域名申请免费 SSL 证书。在 CNAME 接入或者 DNSPod 托管接入模式下，EO 将通过 HTTP 验证的方式申请免费证书，在验证时，由 EO 节点直接响应校验值，建议在配置 CNAME 记录时避免使用分线路/分区域解析，否则可能导致无法获取到正确的校验值导致免费证书申请失败。

场景示例

例如：当前网站计划使用 `example.com` 、`www.example.com` 、`api.example.com` 、`image.example.com` 、`video.example.com` 五个域名服务，均需要实现 HTTPS 访问。以下是未接入 EdgeOne 时和接入 EdgeOne 的 HTTPS 访问实现路径差异对比。

未接入 EdgeOne

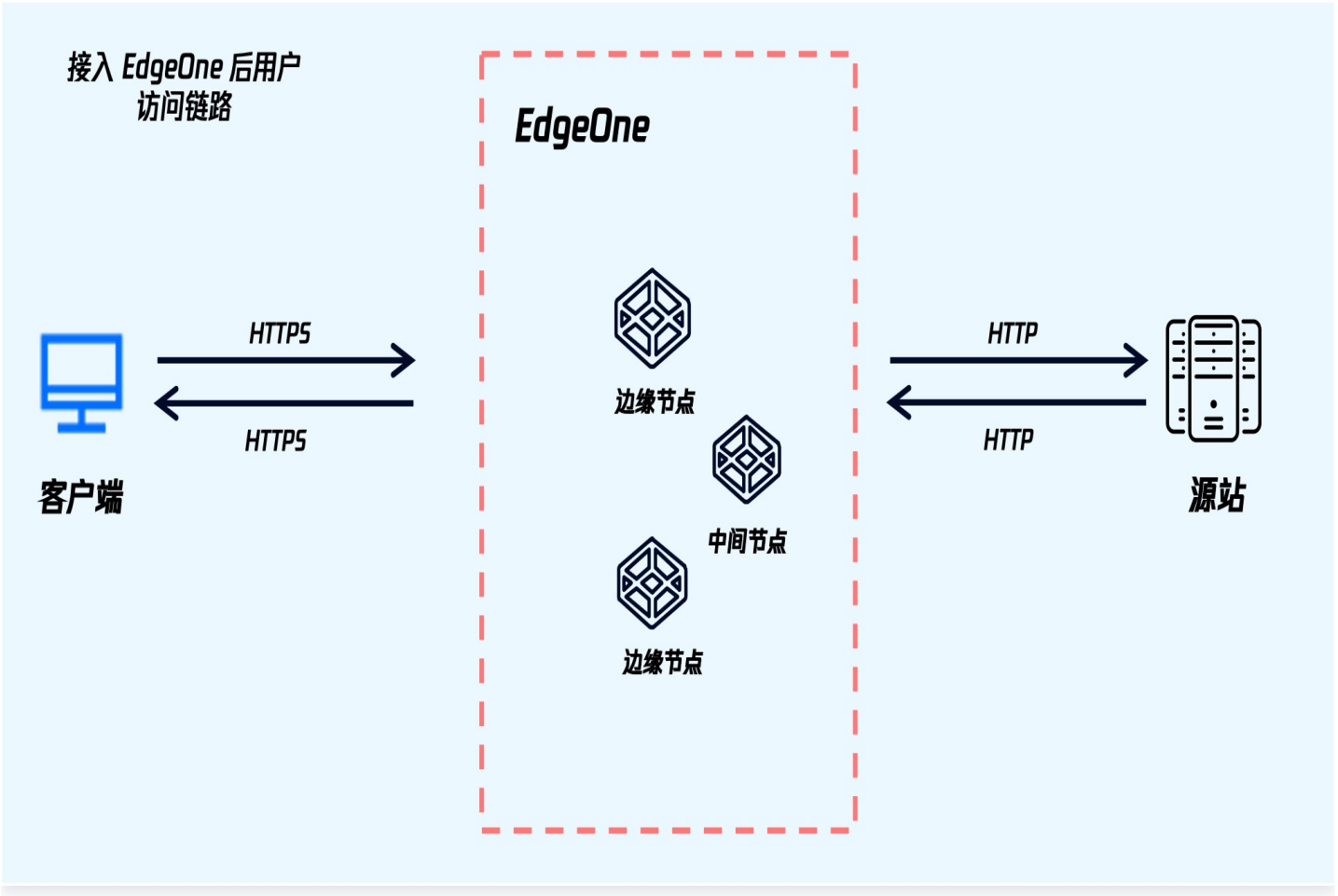
在不接入 EdgeOne 的情况下，为了实现网站的 HTTPS 访问，用户需要注册域名并部署好源站服务后，选择合适的证书机构申请指定证书，如果有多个域名，需要为每个域名单独申请证书或者直接购买泛域名证书。然后在源站服

务器内分别部署证书并启用 HTTPS 服务，才能实现 HTTPS 访问。

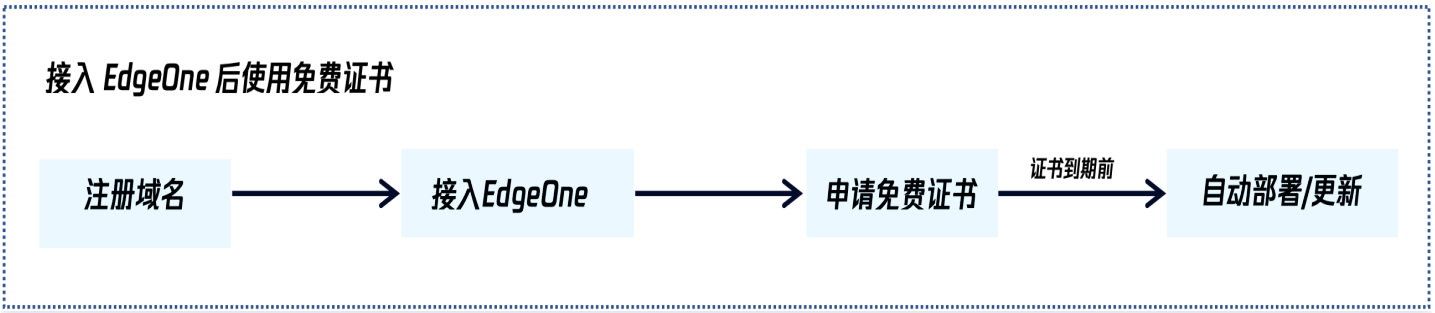
而在证书到期前，需要提前向证书颁发机构重新申请一本新的证书进行续期，并将该证书继续更新部署至服务器内。在域名数量众多的情况下，可能出现证书未及时更新导致的 HTTPS 访问出错。因此，需要在 HTTPS 证书中投入更多的维护工作。

接入 EdgeOne 免费证书

EdgeOne 可让用户将域名接入至 EdgeOne 后，通过 EdgeOne 申请免费证书，自动完成证书申请、下发部署，快速实现 HTTPS 访问。您的源站可无需部署 HTTPS 证书，回源仍然使用 HTTP 访问即可。



在证书到期前，EdgeOne 会自动进行证书续期更新并部署至 EdgeOne 内，可以免去您大量的维护工作量。



操作步骤

1. 参照 从零快速开始接入 EdgeOne，完成站点接入及域名接入。
2. 域名接入后，如果您的站点是 CNAME 接入，需要您的域名完成 CNAME 配置 并等待 CNAME 状态生效；如果您的站点是 NS 接入，需要您完成 NS 服务器切换 并等待解析生效后，再进入下一步。
3. 在域名管理内，选择 `example.com` ，在 HTTPS 配置一列，单击**编辑**，在弹出的 HTTPS 证书配置中选择**申请免费证书**，单击**确定**。

4. 等待免费证书申请完成并下发部署。
5. 部署完成后，再次访问当前站点，即可实现 HTTPS 访问。
6. 重复步骤2-4，对域名 `www.example.com` 、 `api.example.com` 、 `image.example.com` 、 `video.example.com` 同样申请免费证书即可。

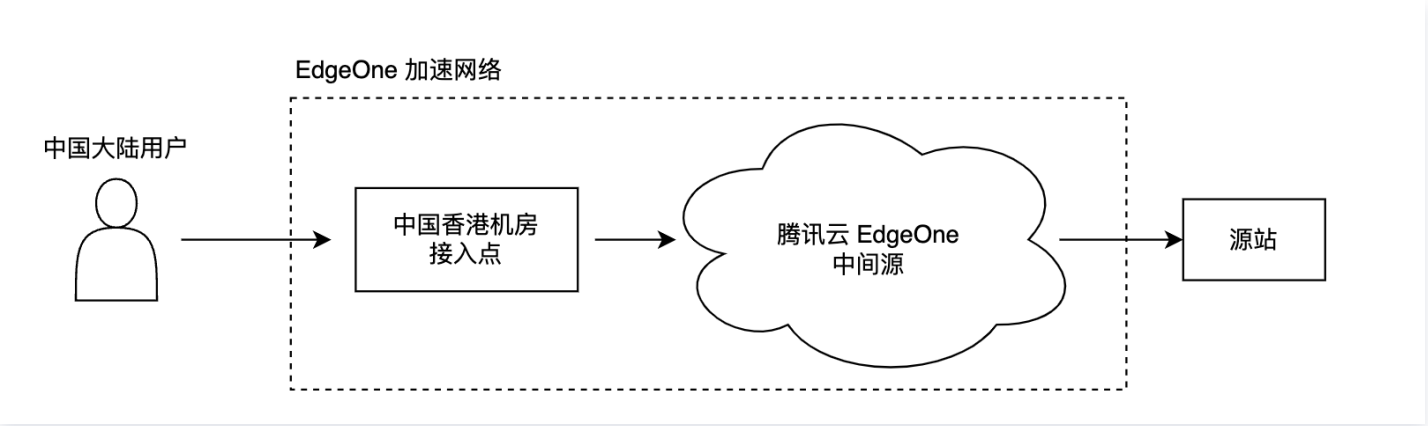
加速优化
跨地域安全加速（海外站点）

最近更新时间：2025-06-26 11:21:23

中国大陆网络优化（国际加速）功能通过 EdgeOne 全球可用区加速网络，为服务商提供跨地域的安全加速方案。

背景介绍

某 Web 服务部署在海外，服务通过 www.example.us（海外站点）对外提供服务。由于站点在海外，暂不能托管在中国内地的服务器上，但客户访问主要来自中国大陆地区，服务面临延迟、抖动、丢包等网络问题，存在中断的风险。为优化中国大陆用户的访问体验，EdgeOne 提供了中国大陆网络优化（国际加速）功能，利用中国香港机房接入点及腾讯云加速网络，有效解决跨地域服务面临的问题。



前提条件

您需要根据 站点接入 指引添加站点，购买 EdgeOne 企业版套餐，七层域名/四层实例加速区域为全球可用区（不含中国大陆）。

> ⚠ **注意：**
>
> 1. 该功能仅在 EdgeOne 企业版套餐中提供。
> 2. 如果您同时购买了**独立 DDoS 防护**，当您的域名遭受攻击时，中国大陆地区访问流量将优先使用独立 DDoS 防护资源，中国大陆网络优化将短暂失效；攻击结束后，恢复中国大陆网络优化效果。切换过程中，客户端连接可能重置。
> 3. 中国大陆网络优化（国际加速）功能将额外收取中国大陆网络优化流量费用，详情参考 中国大陆网络优化服务费用（后付费）。

开启中国大陆网络优化（国际加速）

场景一：配置七层站点全局加速

如需针对站点全局开启中国大陆网络优化（国际加速）功能，请前往站点加速配置，操作步骤如下：

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**网络优化**。
3. 找到中国大陆网络优化（国际加速）功能配置卡片，单击**开关**，站点全局开启中国大陆网络优化（国际加速）功能。

4. 在确认开启窗口中，单击**确认开启**即可开启配置。

场景二：配置单个四层代理加速

如需针对单个四层代理实例开启中国大陆网络优化（国际加速）功能，请前往四层代理配置，如下：

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**四层代理 > 目标实例名称**。
3. 找到中国大陆网络优化（国际加速）功能，单击**开关**，为该实例开启中国大陆网络优化（国际加速）功能。

4. 在弹出的确认窗口中，单击**确定开启**即可完成配置。

访问测试

场景一：配置七层站点全局加速

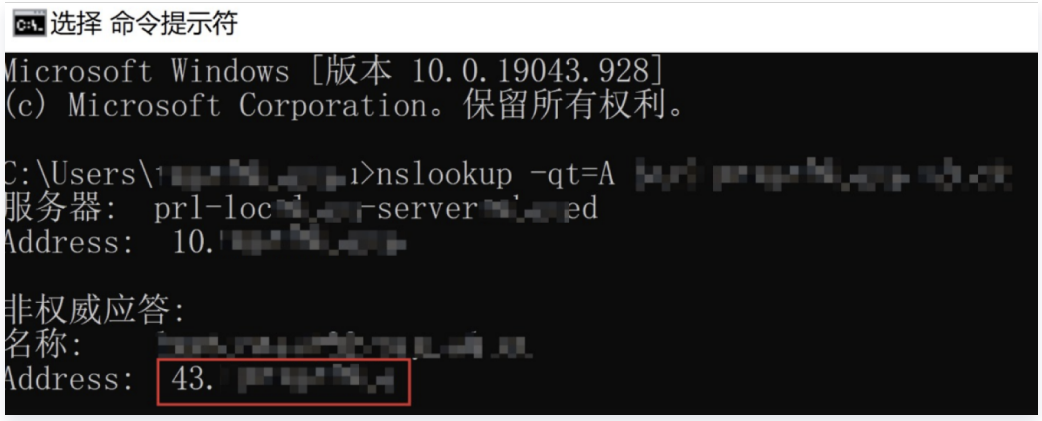
针对已开启中国大陆网络优化（国际加速）的域名，客户端从中国大陆发起访问时，EdgeOne 将自动调度至中国香港接入节点，您可以通过验证当前所分配节点的归属地是否为中国香港来进行验证。

1. 测试获取当前访问节点 IP，可通过以下方式手动获取。

> **注意：**
> 由于中国大陆网络优化（国际加速）功能作用的是从中国大陆发出的用户请求，您需要注意访问测试也应从中国大陆发出。

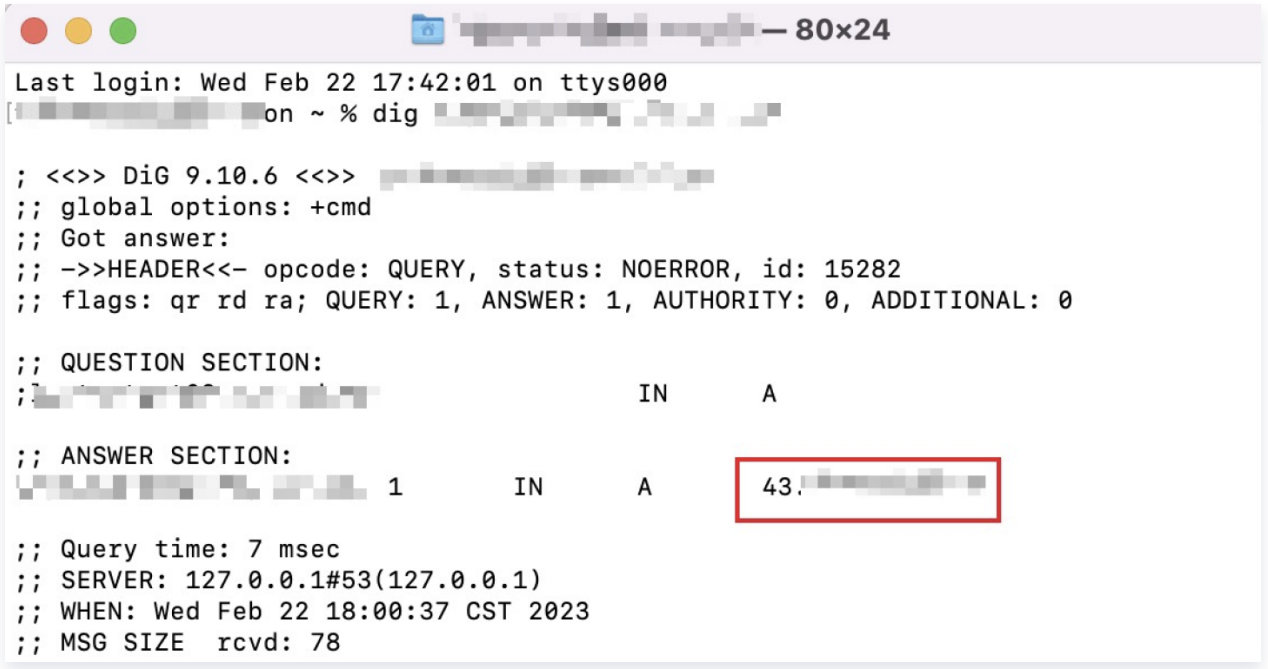
Windows

在 Windows 系统中，打开 cmd 运行程序，以域名 www.example.com 为例，您可以在 cmd 内运行：nslookup -qt=A www.example.com，在运行的解析结果内，可以获取到当前域名 A 记录解析的 IP 地址。



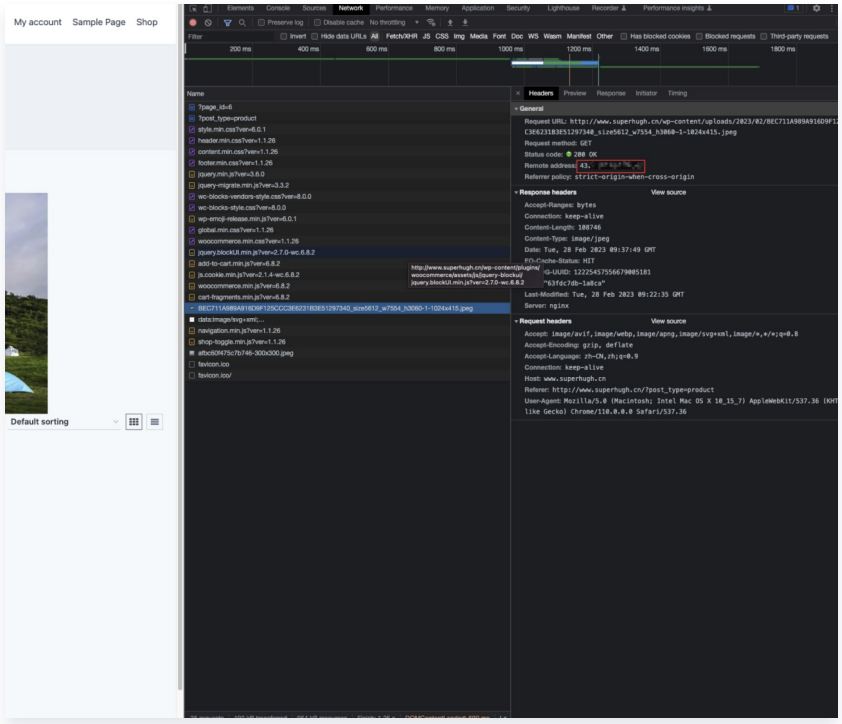
Mac/Linux

在 Mac/Linux 系统中，可以使用 dig 命令进行验证，以域名 www.example.com 为例，您可以在终端内运行命令：dig www.example.com，在运行的解析结果内，可以获取到当前域名 A 记录解析的 IP 地址。



访问站点获取

您也可以通过访问当前站点，例如：www.example.com，访问该站点时，在浏览器内按 F12 打开开发者工具。单击任意的请求记录，可以查看该请求指向的 IP 地址。



2. 您可以通过任一 IP 查询工具查询其归属信息，如果是腾讯中国香港，则中国大陆网络优化（国际加速）功能已生效。

场景二：配置单个四层代理加速

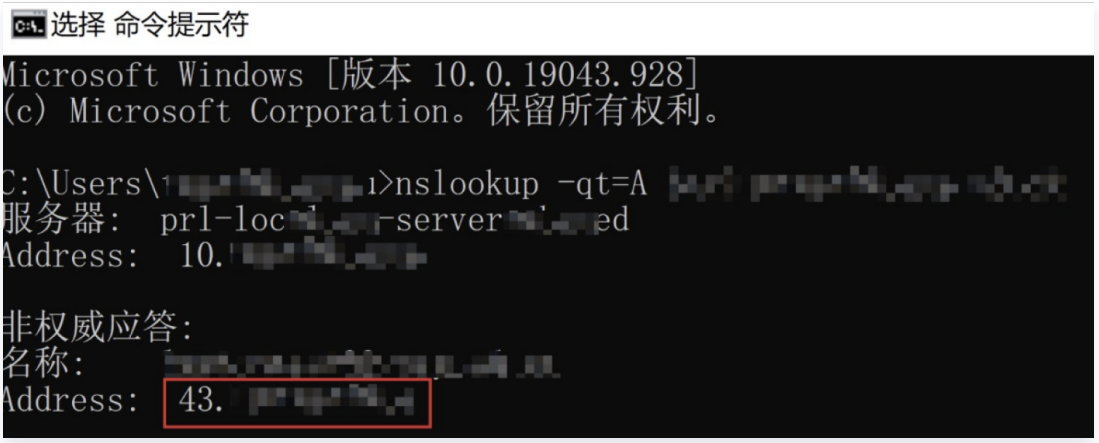
针对已开启中国大陆网络优化（国际加速）的四层代理实例，客户端从中国大陆发起访问时，EdgeOne 将自动调度至香港接入节点，您可以通过验证当前所分配节点的归属地是否为中国香港来进行验证。

1. 查看四层代理实例接入域名，在站点详情页面，单击**四层代理**。在四层代理目标实例下，查看接入域名。

2. 测试获取当前接入域名的 IP，可通过以下方式手动获取。（注：由于中国大陆网络优化（国际加速）功能作用的是从中国大陆发出的用户请求，您需要注意访问测试也应从中国大陆发出）

Windows

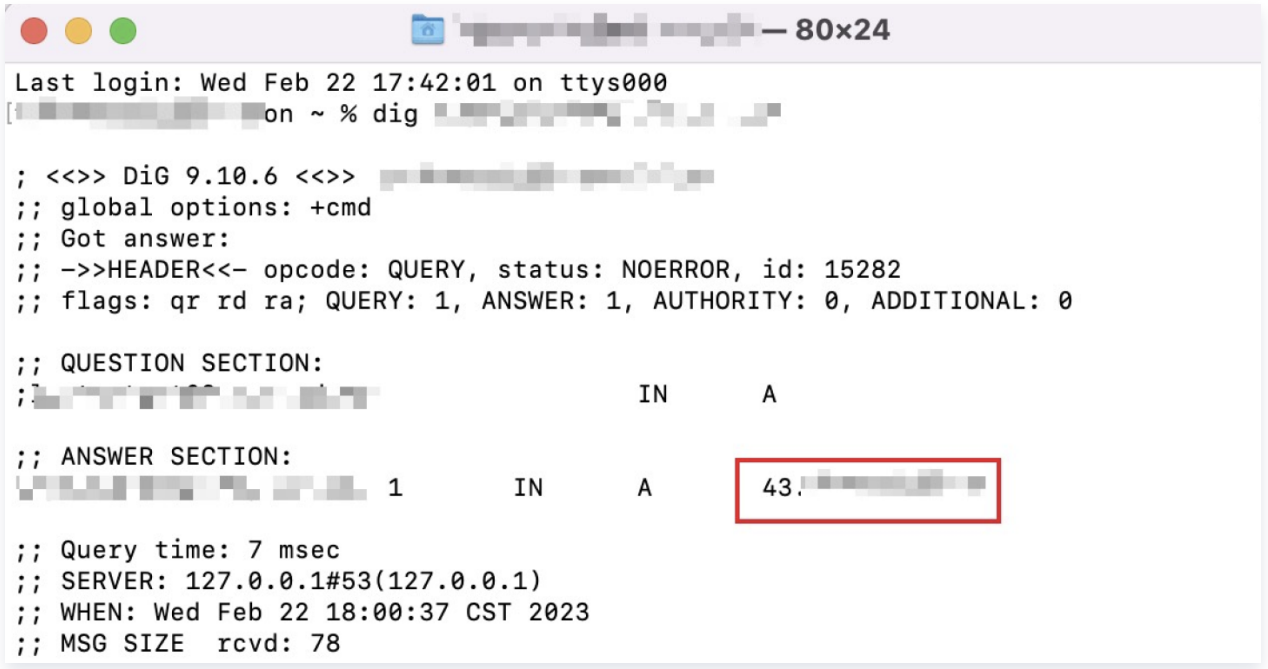
在 Windows 系统中，打开 cmd 运行程序，以 example.com.eo.dnse.com 为例，您可以在 cmd 内运行：nslookup -qt=A example.com.eo.dnse.com，在运行的解析结果内，可以获取到当前域名 A 记录解析的 IP 地址。



Mac/Linux

在 Mac/Linux 系统中，可以使用 dig 命令进行验证，以 example.com.eo.dnse.com 为例，您可以在终端内运行命令：dig example.com.eo.dnse.com，在运行的解析结果内，可以获取到当前域

名 A 记录解析的 IP 地址。

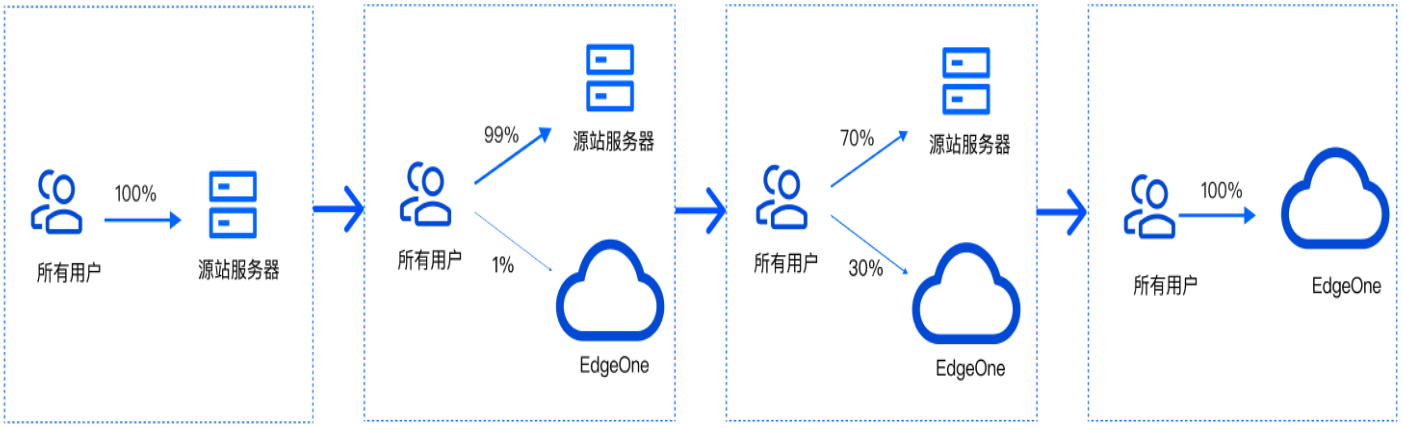


3. 您可以通过任一 IP 查询工具查询其归属信息，如果是腾讯中国香港，则中国大陆网络优化（国际加速）功能已生效。

流量调度
通过流量调度灰度接入 EdgeOne 安全加速

最近更新时间：2025-06-26 11:21:24

本文介绍了如何通过 EdgeOne 的流量调度功能，来帮助您实现将一个域名的流量从源站服务器灰度切换到 EdgeOne，保障业务平稳迁移。



文档目标

本篇文档学习预计需要10分钟，通过学习该文档，您可以了解到：

1. 什么是流量调度管理?
2. 如何使用流量调度来灰度迁移流量并保障服务的高可用性。

背景介绍

购买 EdgeOne 安全加速服务后，网站需要将流量从源站或者其他服务厂商切换至 EdgeOne 。传统方案为用户通过工具指向访问某个节点进行测试，测试确认服务正常之后，一键将所有流量进行切换，可能存在局部区域有问题的风险，造成可用性下降或者源站流量突发等问题。

为了保证服务高可用性，较好的方案是进行灰度切换，实现业务平滑迁移。 EdgeOne 通过提供流量调度管理工具，可自定义灰度切换比例和时间节奏，按需切换控制 EdgeOne 加速流量的比例，保证服务平滑迁移。

前置条件

1. 根据 站点接入 指引添加站点，购买 EdgeOne 企业版套餐，并通过 CNAME 接入站点。
2. 已在 EdgeOne 控制台添加需要进行灰度切换的域名，配置可参考 CNAME 接入模式 添加域名指引 。

预设场景

假设需要迁移的域名为 `huidu.example.com`，当前所有流量直接指向源站服务器，源站地址为 `origin.example.com`。
制定分三阶段灰度切换至 EdgeOne：首先灰度1%，其次30%，最后100%。

操作步骤

步骤1：添加初始灰度策略

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. 进入站点后，菜单栏单击**域名服务 > 流量调度管理**，进入流量调度管理页面，单击**添加调度策略**。
3. 在选择域名页面，选择需要进行灰度切换的域名 `huidu.example.com`，单击**创建**。

4. 在添加服务商页面，本场景因为是从源站迁移，则输入源站域名 `origin.example.com`，服务名称可自定义填写，如“源站域名”，添加完成后单击**下一步**。

5. 在配置策略页面，添加初始灰度策略并提交配置，考虑先将1%流量从源站切换到 EdgeOne，服务一段时间无问题之后再增加灰度比例，则默认策略添加服务商源站域名权重99，EdgeOne 权重1。

image

步骤2：切换解析开始灰度

1. 切换解析

添加策略完成后，EdgeOne 会给域名分配一个流量调度 CNAME，该 CNAME 与域名的默认 CNAME 一致，您还需要前往您的 DNS 解析服务商完成 CNAME 配置，方可触发流量调度策略生效。域名解析切换指引可参见 CNAME 接入 第4部分。

2. 验证生效情况

可以使用 nslookup 或 dig 命令来查看当前域名的解析生效状态。

Windows 系统

在 Window 系统中打开 cmd 运行程序，以域名 `huidu.example.com` 为例，您可以在 cmd 内运行：`nslookup -qt=cname huidu.example.com`，根据运行的解析结果内，可以查看该域名的 CNAME 信息。

因为只有1%灰度，所以约有1%的比例会出现 EdgeOne 提供的 CNAME 地址，可尝试多次运行命令，若出现 EdgeOne 分配的 CNAME ，即流量切换成功。

```
C:\Users\[redacted]>nslookup -qt=cname [redacted].com
服务器: [redacted].com
Address: [redacted]56.23

非权威应答:
[redacted].com canonical name = [redacted]m.acc.edgeonedy1.com
```

Mac 或 Linux 系统

可以使用 dig 命令进行验证，以域名 `huidu.example.com` 为例，您可以在终端内运行命令：`dig huidu.example.com` ，根据运行的解析结果内，可以查看该域名的 CNAME 信息。

因为只有1%灰度，所以约有1%的比例会出现 EdgeOne 提供的 CNAME 地址，可尝试多次运行命令，若出现 EdgeOne 分配的 CNAME ，即流量切换成功。

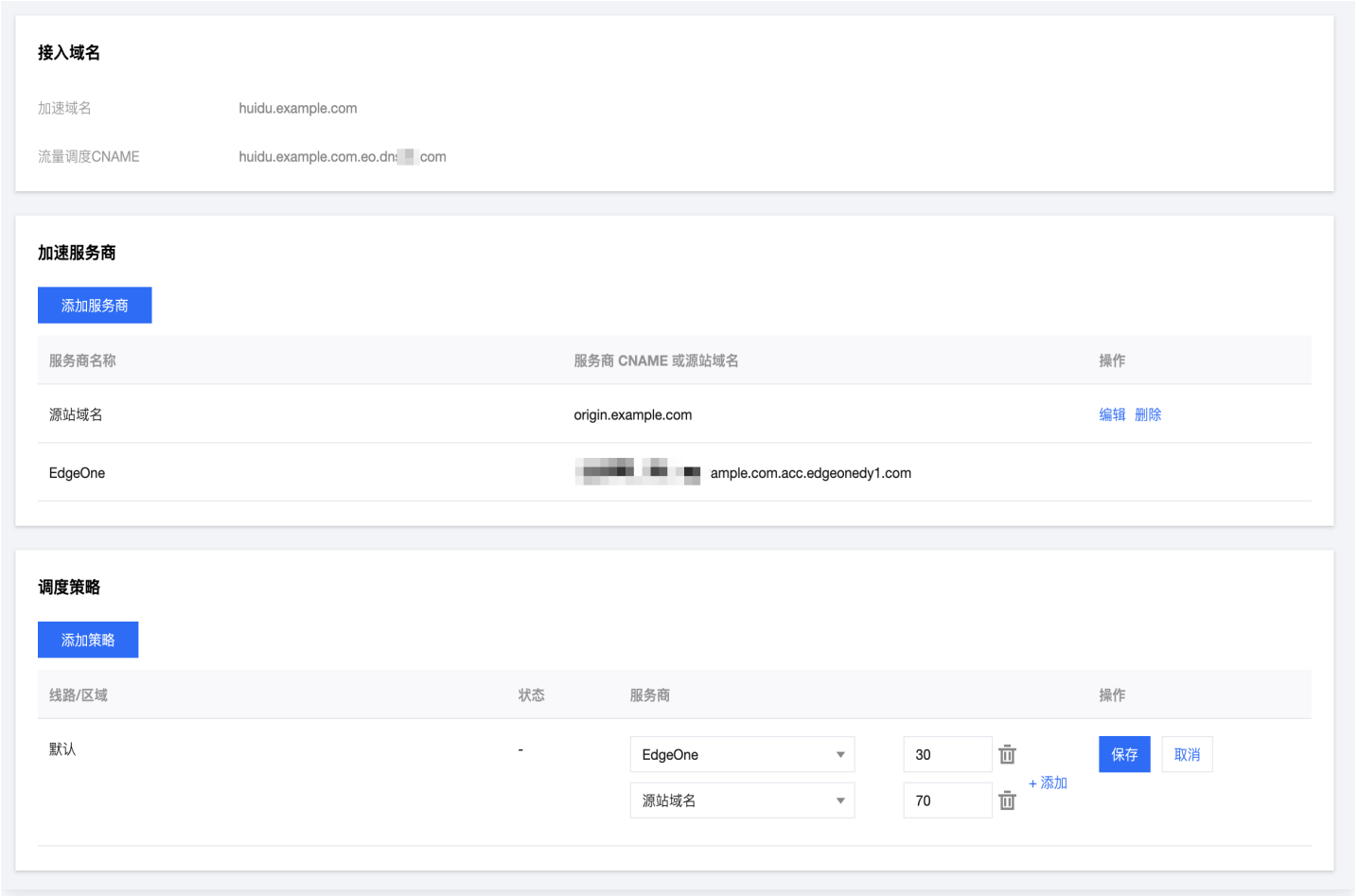
```
(base) [redacted] % dig [redacted]

; <<>> DiG 9.10.6 <<>> [redacted]
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46159
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;w[redacted] IN A

;; ANSWER SECTION:
[redacted] 298 IN CNAME w[redacted]eo.dnse2.com.
[redacted].eo.dnse2.com. 298 IN CNAME w[redacted].acc.edgeonedy1.com.
[redacted].acc.edgeonedy1.com. 58 IN A 175.99.198.121
```

3. 查看流量变化

单击**数据分析 > 流量分析**，流量添加筛选条件 host 等于 `huidu.example.com` ，查看流量趋势曲线变化。例如当前总带宽为100Mpbs ，当切换1%到 EdgeOne 时，EdgeOne 控制台带宽曲线将增长至1Mbps带宽。

步骤3：增加灰度比例

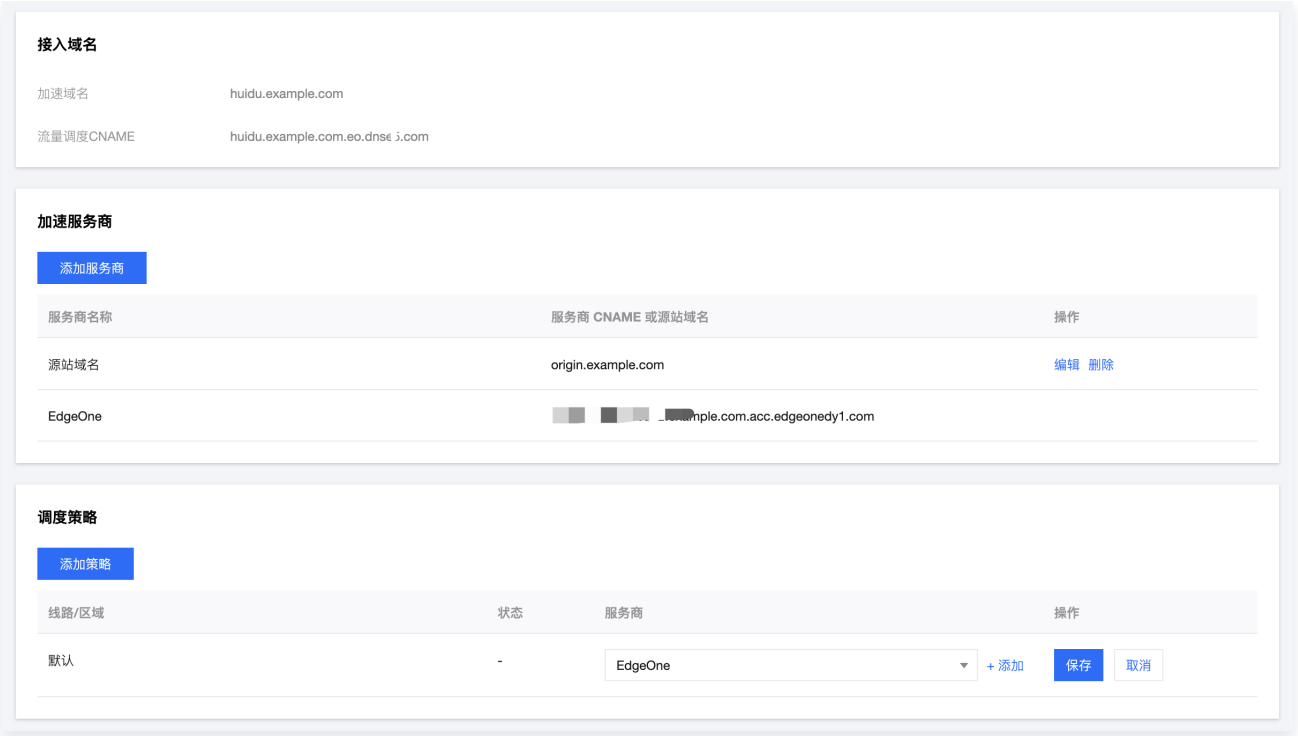
需要增加灰度流量比例至30%时，可进入流量调度管理页面，选择 `huidu.example.com` ，单击操作列**管理**进入编辑页面；在编辑页面内，将 EdgeOne 权重变更为30，源站域名变更为70，单击**保存**则策略立即生效，现网等待 DNS 缓存过期后生效。验证方案同 步骤2：切换解析开始灰度–验证生效情况 。



步骤4：完成灰度流程

增加灰度比例至100%流量切换至 EdgeOne。

1. 编辑默认策略，删除源站域名，只保留 EdgeOne，单击**保存**策略立即生效，现网等待 DNS 缓存过期后生效，则是100%流量切换至 EdgeOne。验证方案同 步骤2：切换解析开始灰度–验证生效情况 。



2. 100%灰度服务一段时间，确认服务没问题后，可以选择停用和删除流量调度策略，停用和删除对您的服务没有影响，流量依然全部采用 EdgeOne 服务，即完成整个流量切换的灰度流程。

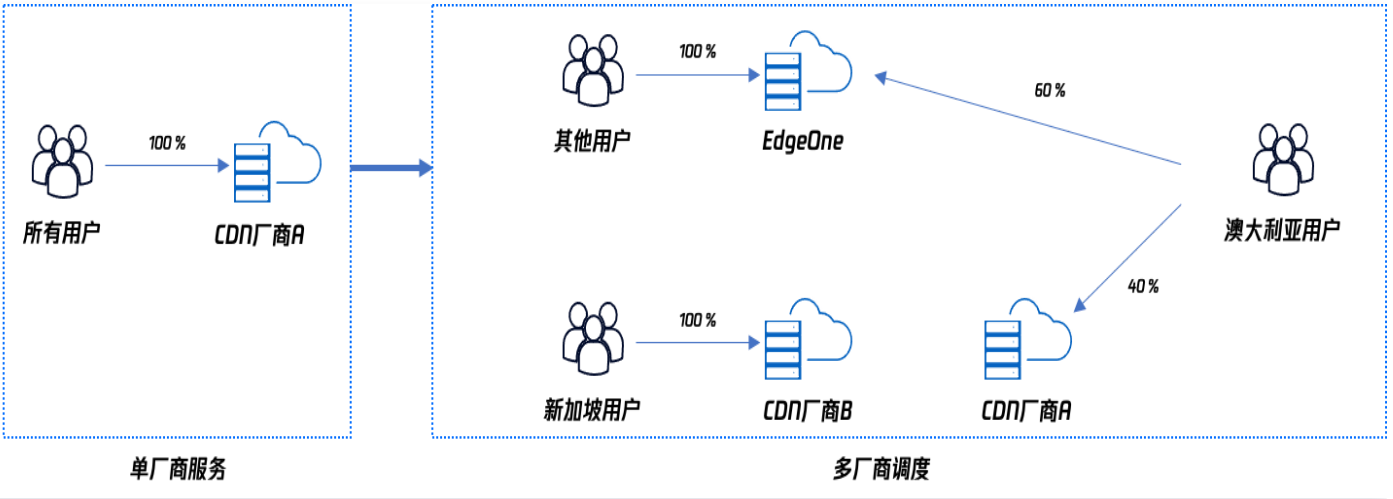
了解更多

- 如何添加站点
- 如何切换 CNAME
- 通过流量调度至多厂商服务

通过流量调度至多厂商服务

最近更新时间：2025-06-26 11:21:24

本文介绍了如何通过 EdgeOne 的流量调度功能，来帮助您实现将一个域名的流量灵活分配给多家服务商共同服务，分散风险实现业务容灾高可用。



文档目标

本篇文档学习预计需要10分钟，通过学习该文档，您可以了解到：

1. 什么是流量调度管理?
2. 如何使用流量调度来实现将流量调度到多家厂商共同服务。
3. 如何通过流量调度来保障服务高可用性。

背景介绍

网站通过购买安全加速服务，提升用户访问体验和业务安全，但不期望将流量全部调度到一家服务商，一旦发生故障影响较大，需要将流量灵活的分配到多家厂商共同服务，降低风险实现服务高可用。传统方案为用户通过自己的 DNS 解析商，针对域名进行复杂的配置指向，例如根据区域、运营商等线路设定不同的服务商，操作和管理较为复杂。EdgeOne 通过提供流量调度管理工具，用户可以按照国家、省份区域、运营商等方式分配流量，可以快速变更和切换服务，保障业务容灾高可用。

前置条件

1. 根据 站点接入 指引添加站点，购买 EdgeOne 企业版套餐，以及通过 CNAME 接入站点。
2. 已在 EdgeOne 控制台添加需要进行流量调度切换的域名，配置可参考 CNAME 接入模式 添加域名指引 。

预设场景

假设域名 `a.exampe.com` 当前所有流量使用 CDN 厂商 B，考虑引入其他厂商共同调度，同时某厂商出现问题时，可以进行流量调度切换。

整体调度策略：

- 将新加坡用户切换使用 CDN 厂商 B 服务。
- 澳大利亚用户采用 EdgeOne 和 CDN 厂商 A 共同服务，EdgeOne 占比60%，CDN 厂商 A 占比40%。
- 其他地区采用默认调度，统一使用 EdgeOne 服务。

操作步骤

步骤1：选择域名

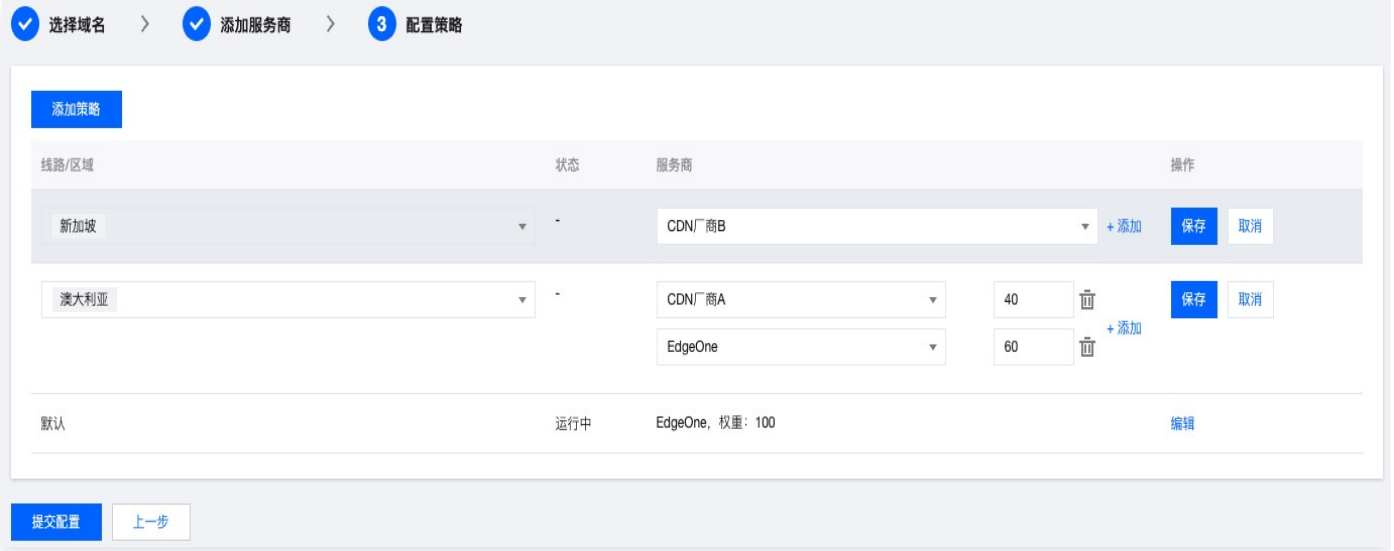
1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，进入**服务总览**，单击**网站安全加速**内需配置的**站点**。
2. 进入站点后，菜单栏单击**域名服务 > 流量调度管理**，进入流量调度管理页面，单击**添加调度策略**。
3. 在流量调度管理页面，单击**添加调度策略**，选择 `a.example.com` ，单击**创建**。

步骤2：设置策略

1. 添加服务商，本场景因为是多厂商共同服务，默认有 EdgeOne 的调度 CNAME，可再分别添加 CDN 厂商 A、CDN 厂商 B 的 CNAME 域名。

2. 添加策略提交配置，添加两条策略，分别在线路/区域中添加中国大陆及新加坡区域：
   - 新加坡：服务商选择 CDN 厂商 B 。
   - 澳大利亚：服务商处**单击添加**一个服务，分别选择 EdgeOne 和 CDN 厂商 A ，其中 EdgeOne 设置权重 60 ， CDN 厂商 A 设置权重 40。

- 默认：默认其他采用 EdgeOne 服务。



步骤3：切换解析

1. 添加策略提交配置后，返回流量调度管理列表页面，EdgeOne 会给域名分配一个流量调度 CNAME，该 CNAME 与域名的默认 CNAME 一致。
2. 如果域名解析已切换至 EdgeOne，则无需变更，现网策略立即生效。若域名解析还未切换，您还需要前往您的 DNS 解析服务商完成 CNAME 配置，方可触发流量调度策略生效，域名解析切换可参见 CNAME 接入 第4部分。

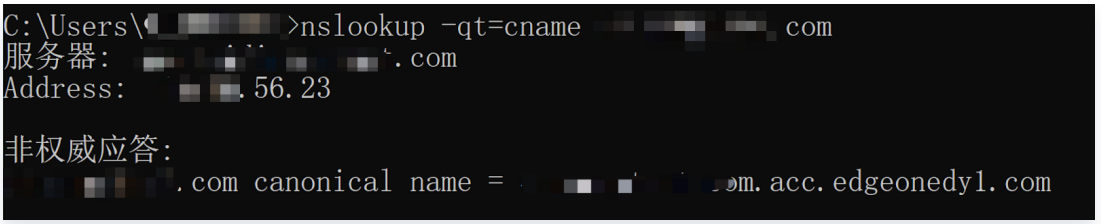
步骤4：验证生效

1. DNS 解析生效查看

可以使用 nslookup 或 dig 命令来查看当前域名的解析生效状态。

Windows 系统

在 Window 系统中打开 cmd 运行程序，以域名 `a.example.com` 为例，判断中国大陆区域生效情况，您可以在 cmd 内运行：`nslookup -qt=cname a.example.com`，根据运行的解析结果内，可以查看该域名的 CNAME 信息。若出现 EdgeOne 分配的 CNAME ，即流量切换成功。



Mac 或 Linux 系统

可以使用 dig 命令进行验证，以域名 `a.example.com` 为例，您可以在终端内运行命令：`dig a.example.com`，根据运行的解析结果内，可以查看该域名的 CNAME 信息。若出现 EdgeOne 分配的 CNAME ，即流量切换成功。

```
(base)  [redacted] % dig [redacted]

; <<>> DiG 9.10.6 <<>> [redacted]
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46159
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;[redacted]                    IN      A

;; ANSWER SECTION:
[redacted]  298 IN      CNAME   [redacted]eo.dnse2.com.
[redacted]eo.dnse2.com. 298 IN CNAME [redacted]..acc.edgeonedy1.com.
[redacted].acc.edgeonedy1.com. 58 IN A 175.99.198.121
```

2. 流量统计变化

以中国大陆区域为例，单击**数据分析 > 流量分析**，流量添加筛选条件 host 等于 `a.example.com` ，查看流量趋势曲线变化。
例如：当前中国大陆带宽为100Mpbs ，当中国大陆切换到 EdgeOne 时，EdgeOne 控制台带宽曲线将增长至100Mbps带宽。

了解更多

- 如何添加站点
- 如何切换 CNAME
- 通过流量调度灰度接入 EdgeOne 安全加速

数据分析与告警
通过腾讯云可观测平台配置 EdgeOne 安全防护事件告警

最近更新时间：2024-09-02 10:45:41

背景介绍

EdgeOne 联合 腾讯云可观测平台 提供针对 DDoS 攻击、CC 攻击、DDoS 攻击封禁等安全事件的灵活告警解决方案。用户可以利用腾讯云可观测平台的告警能力，设置详细的告警触发规则，并通过 多种通知渠道 接收告警，包括电话、短信、邮件、微信、客户售后 VIP 群等，从而有效提升对安全威胁的响应速度和处理效率。

> **注意：**
> 当您在腾讯云可观测平台选择 电话 、短信 告警渠道时，可能产生相关费用，由腾讯云可观测平台收取。

适用场景

本文档适用于已经接入 EdgeOne，且需要配置安全防护事件告警的所有用户。

默认告警策略

当您将域名/四层代理实例接入 EdgeOne 后，一旦发生安全防护事件，腾讯云可观测平台将默认推送告警消息至您腾讯云 主账号 设置的邮箱、短信。您可在 腾讯云可观测平台-事件总线-事件规则 查看 云服务事件默认告警 规则。

操作步骤

步骤1：配置告警

1. 登录 腾讯云可观测平台控制台 ，在左侧导航中，选择**告警管理** > **告警配置**，单击**新建策略**。
2. 告警策略配置细项如下：
   2.1 监控类型选择**云产品监控**。

2.2 策略类型选择**边缘安全加速平台EdgeOne / 站点加速 / 域名**；不同安全防护事件的告警配置需要选择不同策略类型，详见下表：

EO 安全防护事件类型	腾讯云可观测平台告警策略类型	配置含义
HTTP 请求突增	边缘安全加速平台EdgeOne / 站点加速 / 域名	针对**指定域名**遭受到的 CC 攻击事件进行告警
DDoS 攻击 / DDoS 攻击封禁	边缘安全加速平台EdgeOne / 四层代理 / 实例	针对**指定四层代理实例**遭受到的 DDoS 攻击/封禁事件进行告警
	边缘安全加速平台EdgeOne / 套餐	针对**指定七层业务所属** EO 套餐 遭受到的 DDoS 攻击/封禁事件进行告警

2.3 告警对象选择您期望监控的域名列表。

2.4 触发条件选择**事件告警**。

2.5 下拉框选择 **HTTP 请求突增**。

2.6 其他相关配置请参考 新建告警策略 。

3. 单击**下一步：配置告警通知**。

步骤2：配置告警通知

1. 确认**系统预设通知模板**是否符合预期，若需自定义通知模板，可参考 新建通知模板 。
2. 选择所需通知模板后，单击**完成**，保存配置。

参考资料

EO 安全防护事件及对应处置建议

以下是 EdgeOne 可能触发的安全防护事件列表，包括事件类型、事件说明、处置建议等。

事件类型	事件说明	处置建议
HTTP 请求突增	EdgeOne 检测到域名 HTTP 请求突增，疑似遭受 CC 攻击。 **说明：** 触发条件为当 HTTP 请求的速率超过 1000 次每秒（QPS），并且这一增长超出	1. 请关注您的业务可用性，同时您可在 EdgeOne 控制台-指标分析 页面查看近期流量、请求数详情，判断突增流量是否属于正常业务。 2. 若您判断突增流量不属于正常业务，且当前安全策略并未覆盖此次攻击所携带的特征，建议修改收紧 Web 防护策略 。

	了平台通过智能学习算法对业务正常流量基线所预测的范围。	3. 若您判断突增流量属于正常业务，则您可以忽略此条告警，同时建议您放宽 Web 防护-自适应频控限制等级 或改为观察模式。
DDoS 攻击	EdgeOne 检测到为您提供服务的 IP 遭受 DDoS 攻击。 **说明：** 触发条件为 DDoS 攻击检测带宽超过客户在 EO 控制台配置的 DDoS 攻击流量告警阈值（默认 100Mbps）。	请关注您的业务可用性，同时您可在 EdgeOne 控制台-指标分析 页面查看 **L3/4 DDoS 攻击防护带宽**指标卡片，单击顶部 **DDoS 攻击事件数** tab，查看对应攻击事件详情。
DDoS 攻击导致封禁	由于遭受到 DDoS 攻击，为您提供服务的 IP 已被运营商封禁。	请 联系我们 。

跨域响应配置

最近更新时间：2025-07-03 18:00:32

背景介绍

跨源资源共享（CORS，或通俗地译为跨域资源共享）是一种基于 HTTP 头的机制，该机制通过允许服务器标示除了它自己以外的其他源（域、协议或端口），使得浏览器允许这些源访问加载自己的资源。目前许多 HTML 页面都会加载来自不同域下的 CSS 样式表，图像和脚本等资源。因此，解决跨域问题显得尤为重要。
跨源资源共享标准通过新增一系列 HTTP 响应头部，使得服务器能声明哪些来源可以通过浏览器访问该服务器上的资源。

跨域响应头部

头部字段	说明
Access-Control-Allow-Origin	值支持常量以及变量。其中： • 常量：支持输入 `*` ，或多个 域名 、 `IP` 、以及 域名与 `IP` 混填（必须包含 `http://` 或 `https://` ，例如：`http://test.com,http://1.1.1.1` ， 多值可通过英文逗号分隔，最多可输入 `1000` 字符。 • 变量：将需要支持的跨域来源域名通过 `Origin` 请求头进行匹配，头部值使用 `${http.request.headers["Origin"]}` 。
Access-Control-Allow-Methods	用于设置跨域允许的 HTTP 请求方法，可同时设置多个方法，例如 `POST` 、 `GET` 、 `OPTIONS` ，多值可通过英文逗号分隔，最多可输入 `1000` 字符。
Access-Control-Max-Age	用于指定预请求的有效时间，单位为 秒 ，支持输入 `0 ~ 2147483647` 的整型数值。 非简单的跨域请求，在正式通信之前，需要增加一次 `HTTP` 查询请求，称为“预请求”，用来查明这个跨域请求是不是安全可以接受的，如下请求会被视为非简单的跨域请求：以 `GET` 、 `HEAD` 或者 `POST` 以外的方式发起，或者使用 `POST` ，但是请求数据类型为 `application/x-www-form-urlencoded` 、 `multipart/form-data` 、 `text/plain` 以外的数据类型，如 `application/xml` 或者 `text/xml` 。使用自定义请求头为：`Access-Control-Max-Age: 1728000` ，表明在 `1728000` 秒内，对该资源的跨域访问不再发送另外一条预请求。

说明：

- 若在 EdgeOne 上设置跨域响应头，那么响应 `Access-Control-Allow-Origin` 头部的前提条件为客户端请求携带 `Origin` 头部，且该头部与设置的 `Access-Control-Allow-Origin` 任意一个值精确匹配。
- 若源站有设置跨域响应头，则 EdgeOne 上无需配置，否则出现两个跨域响应头部，会导致跨域报错。另外，若由源站来实现跨域响应，需要源站响应 `Vary: Origin` 头部，且在 EdgeOne 上开启 Vary 特性 。

配置示例

场景一：跨域头响应仅允许指定的域名访问页面资源

若您的业务场景涉及跨域访问，当前业务域名为 `www.example.com` 的资源仅允许来自 `example.com` 、`site.com` 的页面访问加速域名，可参考以下步骤。

1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**站点加速** > **规则引擎**，进入规则引擎页面。
3. 在规则引擎页面，单击**创建规则**，选择**新增空白规则**。
4. 在规则编辑页面，匹配类型选择为 HOST 等于 `www.example.com` ，
   同时设置匹配类型 HTTP 请求头 Origin 头部值等于 `*.example.com`、`*.site.com` 。
5. 单击**操作** > **选择框**，在弹出的操作列表内，选择操作为**修改 HTTP 节点响应头**。
6. 选择类型为**设置**，头部名称为 `Access-Control-Allow-Origin` ，头部值设置为 `${http.request.headers["Origin"]}` 。

7. 单击**保存并发布**，即可完成该规则配置。
8. 生效行为说明。

- 当客户端请求中携带 Origin: `http://www.example.com` 时，则 EdgeOne 会响应 `Access-Control-Allow-Origin: http://www.example.com`
- 当客户端请求中携带 Origin: `http://www.site.com` 时，则 EdgeOne 会响应 `Access-Control-Allow-Origin: http://www.site.com`
- 当客户端请求中携带 Origin: `http://www.abc.com` 时，则 EdgeOne 不会响应跨域响应头部 `Access-Control-Allow-Origin`
- 当客户端请求未携带 Origin 时，则 EdgeOne 不会响应跨域响应头部 `Access-Control-Allow-Origin`

场景二：跨域头响应支持所有域名访问页面资源

若您的业务场景涉及跨域访问，当前业务域名为 `www.example.com` 的资源允许所有页面访问加速域名，可参考以下步骤。

1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**站点加速 > 规则引擎**，进入规则引擎页面。
3. 在规则引擎页面，单击**创建规则**，选择**新增空白规则**。
4. 在规则编辑页面，匹配类型选择为 HOST 等于 `www.example.com` 。
5. 单击**操作 > 选择框**，在弹出的操作列表内，选择操作为**修改 HTTP 节点响应头**。
6. 选择类型为设置，头部名称为 `Access-Control-Allow-Origin` ，头部值设置为 `*` 。

7. 单击**保存并发布**，即可完成该规则配置。
8. 生效行为说明。
   - 当客户端请求中携带 `Origin` 时，则 EdgeOne 会响应 `Access-Control-Allow-Origin: *`
   - 当客户端请求未携带 `Origin` 时，则 EdgeOne 不会响应跨域响应头部 `Access-Control-Allow-Origin`

第三方教程

最近更新时间：2025-02-10 11:54:42

本文提供了边缘安全加速平台 EO 不同场景下的第三方教程，您可参考教程进行相关实践操作。

说明：

- 由于边缘安全加速平台 EO 产品在持续的更新与迭代，教程中的步骤由于时效性原因可能与产品最新的操作步骤不一致。
- 第三方教程均来自 腾讯云开发者社区，仅供学习和参考。

站点加速

- PHP 实现无 SDK 依赖的 EdgeOne 缓存刷新

边缘函数

- 纯 EdgeOne 打造 IP 信息查询接口
- 使用 EdgeOne 边缘函数搭建无服务器 AI 绘图站
- 在边缘函数实现腾讯云 API 3.0签名
- 图片渲染 API：极速生成电商、社媒、营销、横幅、证书等图片！

安全防护

- 设置防盗刷规则与针对盗刷 IP 进行反制

版权所有：腾讯云计算（北京）有限责任公司