边缘安全加速平台 EO

数据分析与日志服务

腾讯云

文档目录

数据分析与日志服务
日志服务
概述

最近更新时间：2025-04-24 17:00:42

EdgeOne 全球可用区节点的 L4/7 加速、Web 防护、边缘函数等功能模块在处理访问您业务的请求时会记录详细日志，日志服务模块将各功能模块产生的日志收集并汇聚后提供给用户。您可以利用日志明细来进行故障排查、检查更新配置的影响、生成监控指标等。

支持的功能

- **实时日志推送**：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；从发起请求开始至目的地收到日志的延迟在 5 分钟以内，适合实时排障、监控等对时效性要求较高的场景；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。

    > **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 。

  - **四层代理日志**：记录四层代理实例访问日志，仅记录防护后的访问日志，不记录 DDoS 防护拦截的日志。
  - **边缘函数运行日志**：记录边缘函数执行情况的日志。
  - **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。
  - **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。
  - **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。
  - **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。
- **离线日志**：默认为您存储 30 天访问日志，支持通过控制台或 API 获取日志包的下载链接；通常发起请求 3 小时后可以获取日志包下载链接，24 小时后保障日志包内的日志完整性。适合长时间日志留存、周期性对账等对时效性要求不高的场景。
  - **站点加速日志**：记录域名访问日志，仅记录防护后的请求日志，不记录防护拦截请求日志。
  - **四层代理日志**：记录四层代理实例访问日志，仅记录防护后的访问日志，不记录 DDoS 防护拦截的日志。

> **说明：**
> 实时日志、离线日志字段说明请参考 字段说明 。

套餐支持差异

子功能	个人版	基础版	标准版	企业版
实时日志推送	2 个任务/日志类型	2 个任务/日志类型	3 个任务/日志类型	5 个任务/日志类型
离线日志	支持，日志留存时长为 31 天。		支持，默认日志留存时长为 31 天，最长可留存 183 天。	

计费说明

实时日志推送

接入 EdgeOne 后，您将默认获得实时日志推送功能，不需要额外付费。
需要注意的是，当您配置实时日志推送任务之后，日志投递的目的地处也有可能产生费用。例如：配置日志推送至腾讯云 CLS 后，可能在腾讯云 CLS 产品产生流量和存储费用，详情请参见 日志服务 CLS 计费说明 。

离线日志

接入 EdgeOne 后，您将默认获得离线日志功能，不需要额外付费。

实时日志
实时日志概述

最近更新时间：2025-01-09 16:46:42

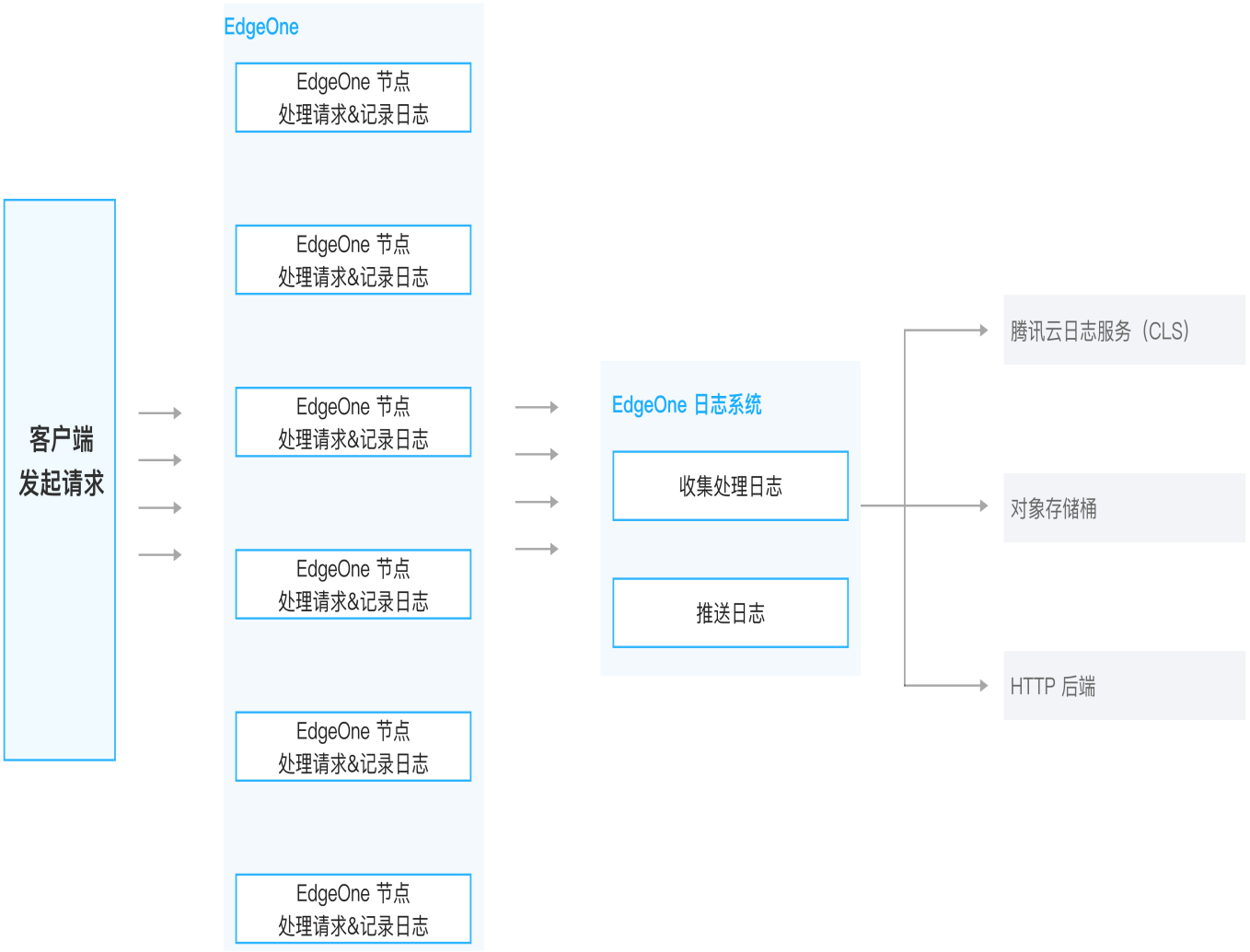
功能概述

当您的站点接入 EdgeOne 后，EdgeOne 为您提供了丰富的预设报表，帮助您监控、分析业务的运行情况。您可能会存在更加个性化的数据分析诉求，例如以下数据分析场景：

场景	场景诉求
深度数据分析	需要指定一个或者多个条件，查找符合条件的日志。例如： • 通过指定客户端 IP 查询指定时间范围内的访问统计（访问 URL、访问次数等）。 • 通过筛选状态码、时间、URL 细化分析状态码的分布情况。 • 通过筛选处置方式为观察的日志，汇总携带的请求头内容及其他请求特征信息，调整安全策略。
监控服务指标	分析 EdgeOne 服务的质量以及用户的访问效率，以便及时发现异常。访问效率包括 EdgeOne 整体响应耗时、下载速度、回源响应耗时等。
鉴别盗刷	通过分析流量异常、访问模式、访问频率，鉴别存在盗刷等行为客户端 IP 。
统一多厂商监控数据	自建数据大屏，统一监控多个云厂商的应用数据。
存储日志	需要保留全量用户访问日志（包括攻击拦截日志）30 天以上。

针对以上场景诉求，EdgeOne 实时日志服务提供了日志的实时采集与推送的能力，可将您的日志推送到腾讯云日志服务（CLS）或您自建的数据中心内，帮助您自行实现对日志数据的灵活检索与分析。目前 EdgeOne 支持将日志推送到以下目的地：

- 推送至腾讯云 CLS：推送至腾讯云提供的一站式日志处理服务（CLS），可用于在 CLS 上进一步对日志做检索分析。
- 推送至 AWS S3 兼容对象存储：兼容 AWS Signature V4 鉴权方法的对象存储。
- 推送至 HTTP 服务器：通过 HTTP POST 请求将日志推送到指定的后端服务器。



说明：

1. 通常情况下，日志投递的延迟在 5 分钟内。为了确保日志投递的实时性，EdgeOne 将固定的日志数量或者固定时间周期为一个批次，将日志推送到相应的目的地。默认策略为优先按日志条数 1000 条/批次；当日志条数不满 1000 条，但距上次推送时间间隔 5 秒时，也将触发第二次推送。
2. 实时日志字段说明请参考 字段说明 。

计费和配额说明

详见 套餐支持差异 、计费说明 。

推送至腾讯云 CLS

最近更新时间：2025-06-26 11:21:23

EdgeOne 实时日志推送支持将日志推送至腾讯云日志服务 CLS 中，您可通过控制台或 API 进行配置。如您希望了解更多有关 CLS 的信息，请参见 日志服务 CLS 产品文档 。

前提条件

1. 登录 腾讯云日志服务控制台 ，开通日志服务 CLS。
2. 若您期望使用子用户账号来进行日志服务相关操作，请参照 CLS 权限管理指引 完成子账号授权，确保子账号拥有 CLS 日志集和日志主题相关读写权限。

> ⚠ **注意：**
> 需要您授权 EdgeOne 通过服务角色 `TEO_QCSLinkedRoleInRealTimeLogCLS` 访问您的日志集和日志主题， EdgeOne 将通过服务角色进行查询日志集和日志主题、修改索引配置、推送日志等操作。

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，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**日志服务** > **实时日志**。
3. 在实时日志页面，单击**新建推送任务**。
4. 在选择日志源页面，填写任务名称、选择日志类型、服务区域、需推送日志的域名/四层代理实例，单击**下一步**。
5. 在定义推送内容页面：
   - （必选）在预设字段列表中勾选需要推送的日志字段；
   - （可选）添加 自定义日志字段 ，支持从请求头、响应头、Cookie 头中提取指定字段名称的值；
   - （可选）配置 推送日志筛选条件 ，默认推送全量日志；
   - （可选）在高级配置中，配置采样比例，默认不开启采样，推送 100% 日志至目的地。
   - （可选）在高级配置中，配置 日志输出格式 ，默认格式为 JSON Lines 。

   > ⚠ **注意：**
   > 推送至 CLS 时，仅支持选择 JSON 格式，且前后缀、分隔符等配置不生效。

6. 在选择目的地页面，选择**腾讯云日志服务（CLS）**，单击**下一步**。
7. 在目的地信息页面，选择目标日志集所在地域、日志集、日志主题。

> ⚠ **注意：**
> 由于云函数（SCF）等其他云产品对于 CLS 日志主题的写操作权限限制，配置 EO 实时日志投递目的地时**无法选择** SCF 默认日志主题 或其他云产品默认日志主题，以免出现投递失败或无法检索日志的情

况。

8. 单击**推送**。
9. 在弹窗中选择索引配置方式，推荐单击**一键配置索引**，EdgeOne 将为您此前选择的日志主题创建键值索引；您也可以选择自行前往 CLS 控制台进行索引配置；需要注意的是，若您未开启键值索引，将导致无法检索日志。

> ⚠ **注意：**
> 当日志量过大，同时 CLS 日志主题自动分裂功能关闭、或者分区值已达上限时，CLS 将限制日志推送请求频率，可能导致您的日志数据丢失。为了避免此类问题，请参考 CLS 日志主题分区分裂 进行相关配置。

推送至 AWS S3 兼容对象存储

最近更新时间：2025-06-26 11:21:23

EdgeOne 实时日志推送支持通过控制台或 API 进行配置，将日志推送至 AWS S3 Signature Version 4 鉴权算法 兼容的对象存储中，例如：

- 腾讯云 COS
- AWS S3
- Google Cloud Storage
- IBM Cloud Object Storage
- Linode Object Storage
- Oracle Cloud Object Storage 等

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，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**日志服务** > **实时日志**。
3. 在实时日志页面，单击**新建推送任务**。
4. 在选择日志源页面，填写任务名称、选择日志类型、服务区域、需推送日志的域名/四层代理实例/边缘函数实例，单击**下一步**。

> **说明：**
> 目前仅支持将站点加速日志、四层代理日志、边缘函数运行日志推送至 S3 兼容对象存储。

5. 在定义推送内容页面：
   - （必选）在 预设字段列表 中勾选需要推送的日志字段；
   - （可选）添加 自定义日志字段，支持从请求头、响应头、Cookie 头中提取指定字段名称的值；
   - （可选）配置 推送日志筛选条件，默认推送全量日志；
   - （可选）在高级配置中，配置采样比例，默认不开启采样，推送 100% 日志至目的地。
   - （可选）在高级配置中，配置 日志输出格式，默认格式为 JSON Lines。
6. 在选择目的地页面，选择 **S3 兼容**，单击**下一步**。
7. 在目的地信息页面，填写相关目的地及参数信息。

参数名称	说明
端点 URL	不包含存储桶名称或路径的 URL，例如：`https://cos.ap-nanjing.myqcloud.com` 。

存储桶地域	存储桶所在的地域，例如：`ap-nanjing`。
存储桶	存储桶名称以及日志存储目录，例如：`your_bucket_name/EO-logs/`。无论您是否填写以 `/` 结尾的目录，都将被正确解析处理。
文件压缩	勾选后，将使用 gzip 压缩日志文件。
SecretId	访问存储桶使用的 Access Key ID。
SecretKey	访问存储桶使用的 Secret key。

8. 单击**推送**。
9. 下发实时日志推送任务后，EdgeOne 将推送一个测试文件至目标存储桶目录以校验连通性，例如 `1699874755_edgeone_push_test.txt`，文件内容为固定字符串“test”。

文件名称说明

日志将会在指定存储桶目录下以 `{{UploadTime}}_{{Random}}.log` 格式存储，且会以日期（UTC+8）为一个文件夹归档日志，例如：`20230331/20230331T185917Z_2aadf5ce.log`。当您开启 gzip 压缩时，文件名称为 `20230331/20230331T185917Z_2aadf5ce.log.gz`。

- UploadTime：日志文件上传时间，格式形如 `{{YYYYMMDD}}T{{HHMMSS}}Z`，UTC+8 时区。
- Random：随机字符，当日志量较大的情况，可能会出现同一个上传时间有多个日志文件，通过此串随机字符来标识不同的文件。

推送至 HTTP 服务器

最近更新时间：2025-06-26 11:21:23

EdgeOne 实时日志推送支持将日志推送至自定义接口地址，您可通过控制台或 API 进行配置。EdgeOne 可通过 HTTP POST 请求调用您提供的后端接口地址，将日志在 HTTP Body 中传输到您指定的服务器上。

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，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**日志服务** > **实时日志**。
3. 在实时日志页面，单击**新建推送任务**。
4. 在选择日志源页面，填写任务名称、选择日志类型、服务区域、需推送日志的域名/四层代理实例/边缘函数，单击**下一步**。
5. 在定义推送内容页面：
   - （必选）在预设字段列表中勾选需要推送的日志字段；
   - （可选）添加自定义日志字段，支持从请求头、响应头、Cookie 头中提取指定字段名称的值；
   - （可选）配置推送日志筛选条件，默认推送全量日志；
   - （可选）在高级配置中，配置采样比例，默认不开启采样，推送 100% 日志至目的地。
   - （可选）在高级配置中，配置日志输出格式，默认格式为 JSON Lines。
6. 在选择目的地页面，选择 **HTTP 服务（POST）**，单击**下一步**。
7. 在目的地信息页面，填写相关目的地及参数信息。

参数名称	说明
接口地址	填入您的日志接收接口地址，例如：`https://www.example.com/edgeone-logs`
内容压缩	为减少日志内容的大小，节约流量开销，您可以通过勾选**使用 gzip 压缩日志文件**开启内容压缩，EdgeOne 将会使用 gzip 格式压缩日志后再传输日志，并且会增加 HTTP 头部 `Content-Encoding: gzip` 来标明压缩格式。
源站鉴权	选择为加密鉴权时，推送日志时将携带鉴权信息供源站进行验证，保证数据来源身份的安全性。鉴权算法见：鉴权算法参考 。
自定义 HTTP 请求头	添加需要 EdgeOne 发起请求时携带的 HTTP 头部。例如： • 通过添加头部 `log-source: EdgeOne` 来识别日志来源为 EdgeOne。 • 通过添加头部 `BatchSize: ${batchSize}` 来获取每次 POST 请求内推送的日志条数。 **说明：**

> 若您填写的头部名称为 Content-Type 等 EdgeOne 日志推送默认携带的头部，那么您填写的头部值将覆盖默认值。

8. 单击**推送**。
9. 实时日志推送任务在配置阶段为了校验接口连通性，将向接口地址发送测试数据进行验证，数据格式如下所示：

```
{
    "ClientState": "CH-AH",
    "EdgeResponseTime": 366,
    "RequestID": "13515444256055847385",
    "ClientRegion": "CN",
    "RemotePort": 443,
    "RequestHost": "www.tencent.com",
    "RequestMethod": "GET",
    "RequestUrlQueryString": "-",
    "RequestUrl": "/en-us/about.html",
    "RequestProtocol": "HTTP/2.0",
    "EdgeServerID": "336d5ebc5436534e61d16e63ddfca327-
d41d8cd98f00b204e9800998ecf8427e",
    "RequestTime": "2022-07-01T02:37:13Z",
    "EdgeCacheStatus": "-",
    "EdgeResponseBytes": 39430,
    "EdgeResponseStatusCode": 200,
    "ClientIP": "0.0.0.0",
    "RequestReferer": "https://www.tencent.com/",
    "RequestUA": "Mozilla/5.0 (iPhone; CPU iPhone OS 15_5 like Mac OS
X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.5 Mobile/15E148
Safari/604.1",
    "EdgeServerIP": "0.0.0.0",
    "RequestRange": "0-100/200",
    "EdgeInternalTime": 334,
    "RequestBytes": 237
}
```

相关参考

服务端解析日志代码示例

当您未开启源站鉴权时，可参考以下 Python 代码在服务端解析请求正文中的日志内容。

```
# 导入Python标准库中的模块
```

```
import time  # 用于获取当前时间
import gzip  # 用于处理gzip压缩的数据


# 从http.server模块导入HTTPServer和BaseHTTPRequestHandler类
from http.server import HTTPServer, BaseHTTPRequestHandler
import json  # 用于处理JSON数据格式


# 定义一个继承自BaseHTTPRequestHandler的类，用于处理HTTP请求
class Resquest(BaseHTTPRequestHandler):
    # 重写do_POST方法，该方法会在服务器接收到POST请求时被调用
    def do_POST(self):
        # 打印请求头信息
        print(str(self.headers))
        # 打印HTTP请求的命令（如POST）
        print(self.command)
        # 读取请求体内容，根据请求头中的Content-Length字段确定读取的长度
        req_datas = self.rfile.read(int(self.headers['content-length']))
        try:
            # 尝试解码请求体内容并打印
            print(req_datas.decode())
        except Exception as e:
            # 如果解码过程中发生异常，打印异常信息
            print(e)
            # 检查请求头中是否有Content-Encoding: gzip，如果有，则解压请求体
            if self.headers['Content-Encoding'] == 'gzip':
                data = gzip.decompress(req_datas)
                # 打印解压后的gzip内容
                print('---------------decompress gzip content-----------
--------------')
                print(data.decode())
        # 检查请求的路径是否为 '/edgeone-logs'，如果不是，则返回404错误
        if self.path != '/edgeone-logs':
            self.send_error(404, "Page not Found!")
            return
        # 如果请求路径正确，准备响应数据
        data = {
            'result_code': '1',
            'result_desc': 'Success',
            'timestamp': int(time.time())  # 响应当前时间戳
        }
        # 发送HTTP响应状态码200，表示请求成功
```

```
        self.send_response(200)
        # 设置响应头Content-type为application/json
        self.send_header('Content-type', 'application/json')
        # 结束响应头的发送
        self.end_headers()
        # 将响应数据以JSON格式写入到响应体中
        self.wfile.write(json.dumps(data).encode('utf-8'))


# 检查当前脚本是否作为主程序运行
if __name__ == '__main__':
    # 定义服务器监听的地址和端口，您可将9002替换为自定义端口
    host = ('', 9002)
    # 创建HTTPServer对象，传入监听地址和端口以及处理请求的请求处理器类
    server = HTTPServer(host, Resquest)
    # 打印服务器启动信息
    print("Starting server, listen at: %s:%s" % host)
    # 启动服务器，使其持续运行直到外部中断
    server.serve_forever()
```

请求鉴权算法

如果您在推送目的地信息中，源站鉴权内选择了**加密签名**，可输入您自定义配置 SecretId 和 SecretKey，EdgeOne 将在请求 URL 中增加签名 `auth_key` 和 `access_key`，签名算法详情如下：

1. **请求 URL 构成**

   如下所示，请求 URL 将在 `?` 后携带 `auth_key` 和 `access_key` 。

   ```
   http://DomainName[:port]/[uri]?auth_key=timestamp-rand-
   md5hash&access_key=SecretId
   ```

   参数说明：

   - **timestamp**：请求当前时间，使用 Unix 秒级10位时间戳。
   - **rand**：随机数。
   - **access_key**：用于标识接口请求方的身份，即您所自定义配置的 SecretId。
   - **SecretKey**：固定长度 32 位，即您所自定义配置的 SecretKey。
   - **uri**：资源标识符，例如：`/access_log/post` 。
   - **md5hash**：md5hash = `md5sum(string_to_sign)` ，其中 string_to_sign = `"uri-timestamp-rand-SecretKey"` 。通过md5算法计算出的验证串，数字0-9和小写英文字母 a-z 混合，固定长度为32个字符。

2. **计算示例**

假定填入参数为：
接口地址：`https://www.example.com/access_log/post`
SecretId = `YourID`
SecretKey = `YourKey`
uri = `/access_log/post`
timestamp = `1571587200`
rand = `0`

```
string_to_sign = "/access_log/post-1571587200-0-YourKey"
```

基于该字符串计算出：

```
md5hash=md5sum("/access_log/post-1571587200-0-
YourKey")=1f7ffa7bff8f06bbfbe2ace0f14b7e16
```

最终推送时的请求 url 为：

```
https://www.example.com/cdnlog/post?auth_key=1571587200-0-
1f7ffa7bff8f06bbfbe2ace0f14b7e16&access_key=YourID
```

服务端在接收到推送请求后，提取 `auth_key` 的值. 对 auth_key 的值进行拆分，获取 `timestamp`， `rand` 和 `md5hash`。可先检查 `timestamp` 是否过期，过期时间建议为 `300s`，并基于上述规则拼装加密字符串，利用 SecretKey 拼装出需加密的字符串，加密后与 `auth_key` 中的 `md5hash` 值进行比较，相同则说明鉴权通过。

3. 服务端解析鉴权请求代码示例

Python

```python
import hashlib

from flask import Flask, request

app = Flask(__name__)


def get_rsp(msg, result={}, code=0):
    return {
        "respCode": code,
        "respMsg": msg,
        "result": result
```

```
    }


def get_secret_key(access_key):
    return "secret_key"


@app.route("/access_log/post", methods=['POST'])
def access_log():
    if request.method == 'POST':
        if request.content_type.startswith('application/json'):
            current_time_ts, rand_num, md5hash =
request.args.get("auth_key").split("-")
             # 判断请求时间是否是在有效期内
            if time.time() - int(current_time_ts) > 300:
                return get_rsp(msg="The request is out of time",
code=-1)

            access_key = request.args.get("access_key")
            # 通过access_key(SecretId)获取secret_key
            secret_key = get_secret_key(access_key)
            raw_str = "%s-%s-%s-%s" % (request.path, current_time_ts,
rand_num, secret_key)
            auth_md5hash = hashlib.md5(raw_str.encode("utf-
8")).hexdigest()
            if auth_md5hash == md5hash:
                # 认证通过
                if request.headers['content-encoding'] == 'gzip':
                    # 解压数据
                    pass
                # 数据处理
            return get_rsp("ok")
        return get_rsp(msg="Please use content_type by
application/json", code=-1)
    return get_rsp(msg="The request method not find, method == %s" %
request.method, code=-1)

if __name__ == '__main__':
    app.run(host='0.0.0.0', port=8888, debug=True)
```

Golang

```
package main

import (
    "context"
    "crypto/md5"
    "fmt"
    "log"
    "net/http"
    "os"
    "os/signal"
    "strings"
    "syscall"
)

func main() {
    mux := http.NewServeMux()
    mux.Handle("/access_log/post", &logHandler{})

    server := &http.Server{
        Addr:    ":5000",
        Handler: mux,
    }

    // 创建系统信号接收器
    done := make(chan os.Signal)
    signal.Notify(done, os.Interrupt, syscall.SIGINT, syscall.SIGTERM)
    go func() {
        <-done

        if err := server.Shutdown(context.Background()); err != nil {
            log.Fatal("Shutdown server:", err)
        }
    }()

    err := server.ListenAndServe()
    if err != nil {
        if err == http.ErrServerClosed {
            log.Print("Server closed under request")
        } else {
            log.Fatal("Server closed unexpected")
        }
    }
```

```
}

type logHandler struct{}

func (*logHandler) ServeHTTP(w http.ResponseWriter, r *http.Request) {
    if r.Method == "POST" {
        query := r.URL.Query()
        authKey := query.Get("auth_key")
        accessKey := query.Get("access_key")//access_key 即您提供的
SecretId
        authKeys := strings.Split(authKey, "-")
        if len(authKeys) == 3 {
            currentTimeTs := authKeys[0]

            //进行时间戳有效期判断
            RandNum := authKeys[1]
            md5Hash := authKeys[2]
            secretKey := getSecretKey(accessKey)
            authStr := fmt.Sprintf("%s-%s-%s-%s", "/access_log/post",
currentTimeTs, RandNum, secretKey)
            data := []byte(authStr)
            has := md5.Sum(data)
            authMd5 := fmt.Sprintf("%x", has) //转换成字符串进行比较
            if authMd5 == md5Hash {
                // todo 认证成功
                if r.Header.Get("Content-Encoding") == "gzip" {
                    //解压数据
                }
                //数据处理
            }
        } else {
            //异常处理
        }
    }
}

// 获取SecretKey
func getSecretKey(accessKey string) string {
    if accessKey != "" {
        // 通过Access_key(SecretI)获取Secret_Key
        return "secret_key"
    }
    return ""
```

```
}
```

离线日志

最近更新时间：2025-06-26 11:21:23

功能概述

为了方便客户对用户访问进行分析，EdgeOne 对访问日志进行了小时粒度打包，并且提供下载服务。

离线日志格式

- 日志默认按照 JSON Lines 格式存储，一行 JSON 即为一条日志。
- 日志包通过 gzip 压缩为 .gz 格式。由于 MacOS 系统的目录系统缺陷，在 MacOS 系统下双击解压可能会报错，如出现这种情况，您可以进入日志所在的目录下，通过如下 Terminal 命令进行解压。

```
gunzip {your_file_name}.log
```

日志打包规则

- 默认按小时粒度打包，若某个小时里无任何请求访问您的业务，则不会产生该时间区间的日志包。
- 由于 EdgeOne 节点分布在各地，为同步所有时区，离线日志的存储时间（日志包文件名称的时间）默认为：UTC +00:00。
- 离线日志从各 EdgeOne 节点收集而来，因此延迟上各有差异，一般情况下延迟 3 小时左右后可查询、下载日志包，日志包会不断追加，一般 24 小时左右趋于稳定。

日志存储时长

离线日志默认存储时长为 31 天，对于标准版、企业版站点，可选调整离线日志存储时长为 183 天，以满足相关合规诉求。详见 套餐支持差异 。

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，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**日志服务** > **离线日志**。
3. 在离线日志页面，筛选栏右侧选择**设置**图形按钮 。

4. 在弹窗中，修改离线日志存储时长，并单击**保存**。修改日志存储时长后，修改前存储的日志将按原存储时长淘汰，新存储的日志按修改后的存储时长淘汰。

示例：查询指定域名在指定时间段内的离线日志

示例场景

当您通过 添加加速域名 将 `www.example.com` 添加至 EdgeOne 服务后，您需要下载 `www.example.com` 在 2023-08-07 至 2023-08-10 的所有站点加速日志进行数据分析，您可以参考以下步骤操作。

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，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**日志服务** > **离线日志**。
3. 在离线日志页面，筛选时间范围，选择日期为 2023-08-07 至 2023-08-10，右侧日志类型选择为站点加速日志，域名选择为 www.example.com 。筛选完成后，页面将自动查询符合条件的日志信息。

4. 在查询到的日志列表内，您可以按需通过以下三种方法来进行下载：
   - 通过单击**操作列下载**，即可下载对应域名/四层代理实例、对应时间段的日志包。
   - 通过单击**获取下载链接**，即可复制相应的日志包下载链接。
   - 通过勾选需要的日志包，并单击**批量获取下载链接**，可以批量复制所需的所有日志包下载链接。

相关 API

- 下载七层离线日志 DownloadL7Logs
- 下载四层离线日志 DownloadL4Logs

相关参考
字段说明
七层访问日志

最近更新时间：2025-04-25 15:12:12

以下是七层访问日志（站点加速日志、速率限制和 CC 攻击防护日志、自定义规则日志、Bot 管理日志、托管规则日志）的详细字段说明。

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、自定义规则日志、Bot 管理日志即将下线，建议您使用站点加速日志来获取全量 L7 防护日志。

字段说明

通用字段

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
ContentID	String	与请求相关的内容标识符，用于识别 EO 平台上提供的计费、报告和监控的特定流量和内容子集。若该请求关联到内容标识符则为 `eocontentid`；若无则为 `zoneid`。	✓	✓
EdgeEndTime	Timestamp ISO8601	完成响应客户端请求的时间。示例值：2024-10-14T05:13:43Z，表示 2024年10月14日 UTC+0 时区时间 05:13:43，等同于 2024年10月14日 UTC+8 时区（北京时间）13:13:43。	×	✓

EdgeFunctionSubrequest	Integer	标识此条日志是否属于边缘函数发起的子请求，取值有： • 1：边缘函数发起的子请求。 • 0：非边缘函数发起的子请求。	✓	✓
LogTime	Timestamp ISO8601	日志生成的时间。示例值：2024-10-14T05:13:43Z。	×	✓
ParentRequestID	String	当该请求是使用边缘函数发起时，记录父请求的 `RequestID`；否则记录为“-”。	✓	✓
RequestID	String	客户端请求的唯一标识 ID。	✓	✓

客户端信息

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
ClientConnectionID	String	客户端与边缘节点之间连接的唯一标识。示例值："5692760165714882237"。	×	✓
ClientDeviceType	String	客户端请求设备类型，取值有： • TV：电视 • Tablet：平板电脑 • Mobile：手机 • Desktop：电脑 • Other：其他	×	✓
ClientIP	String	与 EdgeOne 节点建连的客户端 IP。	✓	✓
ClientISP	String	客户端 IP 解析出的运营商信息。 • 中国大陆境内数据，记录为 ISP 中文名称； • 全球可用区（不含中国大陆）数据，记录为 自治系统编号（ASN）。	✓	✓

ClientPort	Integer	与 EdgeOne 节点建连的客户端端口。	×	✓
ClientRegion	String	客户端 IP 解析出来的国家/地区。格式标准：ISO 3166-1 alpha-2 。	✓	✓
ClientState	String	客户端 IP 解析出的国家下一级的行政划分。目前仅支持中国大陆境内数据。格式标准：ISO-3166-2 。	✓	✓

请求信息

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
RemotePort	Integer	TCP 协议下与客户端建立连接的 EdgeOne 节点端口。	✓	✓
RequestBodyBytes	Integer	客户端请求发送给 EdgeOne 节点的请求体大小，单位：Byte。	×	✓
RequestBytes	Integer	客户端请求过程中向 EdgeOne 节点发送的总流量，根据请求头大小、请求体大小、SSL 握手中客户端向 EdgeOne 节点发送的数据统计而来。单位：Byte。	✓	✓
RequestHost	String	客户端请求的 Host。	✓	✓
RequestMethod	String	客户端请求的 HTTP Method，取值有： • GET • POST • HEAD • PUT • DELETE • CONNECT • OPTIONS • TRACE • PATCH	✓	✓

RequestProtocol	String	客户端请求的应用层协议，取值有： • HTTP/1.0 • HTTP/1.1 • HTTP/2.0 • HTTP/3 • WebSocket	✓	✓
RequestRange	String	客户端请求的 Range 参数信息。	✓	✓
RequestReferer	String	客户端请求的 Referer 信息。	✓	✓
RequestScheme	String	客户端请求的 HTTP 协议。取值有：HTTP、HTTPS。	×	✓
RequestSSLProtocol	String	客户端的使用的 SSL（TLS）协议，若取值为“-”，则表示请求没有 SSL 握手；取值有： • TLS1.0 • TLS1.1 • TLS1.2 • TLS1.3	×	✓
RequestStatus	String	客户端请求的状态，若使用 WebSocket 协议的请求，EdgeOne 会周期打印日志，可以使用此字段确定连接状态，取值有： • 0：未结束 • 1：请求正常结束 • 2：WebSocket 协议下，表示同连接的首条日志 • 3：WebSocket 协议下，表示同连接的非首条、非末条日志	✓	✓
RequestTime	Timestamp ISO8601	EdgeOne 节点收到客户端请求的时间，时区：UTC +0。示例值：2024-10-14T05:13:43Z。	✓	✓
RequestUA	String	客户端请求的 User-Agent 信息。	✓	✓
RequestUrl	String	客户端请求的 URL Path ，不包含查询参数。	✓	✓

RequestUrlQueryString	String	客户端请求的 URL 携带的查询参数。	✓	✓

响应信息

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
EdgeCacheStatus	String	客户端请求是否命中节点缓存，取值有： • hit：资源由节点缓存提供 • miss：资源可缓存，但由源站提供 • dynamic：资源不可缓存 • other：无法被识别的缓存状态	✓	✓
EdgeInternalTime	Integer	从 EdgeOne 接收到客户端发起的请求开始，到响应给客户端的第一个字节，整个过程的耗时；单位：ms。	✓	✓
EdgeResponseBodyBytes	Integer	节点返回给客户端的响应体大小，单位：Byte。	✓	✓
EdgeResponseBytes	Integer	节点返回给客户端的总流量，根据响应头大小、响应体大小、SSL 握手中 EdgeOne 节点向客户端发送的数据统计而来。单位：Byte。	✓	✓
EdgeResponseStatusCode	Integer	节点响应返回给客户端的状态码。	✓	✓
EdgeResponseTime	Integer	从 EdgeOne 接收到客户端发起的请求开始，到响应给客户端的最后一个字节，整个过程的耗时；单位：ms。	✓	✓

边缘服务端信息

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

EdgeException	String	描述 EO 边缘节点处理请求时遇到的问题。字段取值含义详见 EdgeException 字段说明 。	×	✓
EdgeServerID	String	客户端访问到的 EdgeOne 服务器唯一标识。示例值："28a1672eeaa86c145501d3950bff06cc-501d3fb0abce346ac9a5598b665bfcfe"。	✓	✓
EdgeServerIP	String	DNS 解析 Host 得到的 EdgeOne 服务器 IP 地址。	✓	✓
EdgeServerRegionTopDivision	String	边缘服务端接入 IP 解析出的国家下一级的行政划分。目前仅支持中国大陆境内数据。格式标准：ISO-3166-2 。	×	✓
EdgeSeverRegion	String	边缘服务端接入 IP 解析出来的国家/地区，格式标准参考：ISO 3166-1 alpha-2 。	×	✓

源站信息

说明：

- **EdgeCacheStatus 为 `miss` 或 `dynamic` 时： 源站信息字段反映实际的回源请求信息。**
- **EdgeCacheStatus 为 `hit` 时： 源站信息字段可能显示的是节点缓存中的回源信息，这并不代表实际的回源情况。**

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
OriginDNSResponseDuration	Float	接收到源站 DNS 解析响应的耗时，若没有获取到值，记录为 -1 ，单位：ms。	×	✓
OriginIP	String	回源访问的源站 IP，若没有获取到值，记录为“-”。	×	✓
OriginRequestHeaderSendDuration	Float	向源站发送请求头的耗时，一般是 0，若没有获取到值，记录为 -1 ，单位：ms。	×	✓

OriginResponseHeaderDuration	Float	向源站发送请求头到接受到源站响应头的耗时，若没有获取到值，记录为 -1 ，单位：ms。	×	✓
OriginResponseStatusCode	Integer	源站响应状态码，若没有获取到值，记录为 -1。	×	✓
OriginSSLProtocol	String	请求源站使用的 SSL 协议版本，若没有获取到值，记录为“-”；取值有： • TLS 1.0 • TLS 1.1 • TLS 1.2 • TLS 1.3	×	✓
OriginTCPHandshakeDuration	Float	请求源站时，完成 TCP 握手的耗时，若没有获取到值，记录为 -1 ，单位：ms；**注意：当连接重复利用时为0。**	×	✓
OriginTLSHandshakeDuration	Float	请求源站时，完成 TLS 握手的耗时，若没有获取到值或回源协议为 HTTP，记录为 -1 ，单位：ms；**注意：当连接重复利用时为0。**	×	✓

安全防护相关字段

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
BotCharacteristic	String	EO Bot 智能分析引擎发现该请求具备的特征，仅提供给已启用 Bot 管理 - Bot 智能分析 功能的域名。字段取值含义详见 BotCharacteristic 字段说明 。	×	✓
BotClassAccountTakeOver	String	基于近期 IP 情报数据，请求客户端 IP 有恶意破解登录、发起账号接管攻击的风险等级，取值有： • high：高风险 • medium：中等风险	×	✓

		• low：一般风险 • -：无历史数据或域名没有开启 客户端画像分析 功能		
BotClassAttacker	String	基于近期 IP 情报数据，请求客户端 IP 有攻击（如 DDoS，高频恶意请求、站点攻击等）行为的风险等级，取值有： • high：高风险 • medium：中等风险 • low：一般风险 • -：无历史数据或域名没有开启 客户端画像分析 功能	×	✓
BotClassMaliciousBot	String	基于近期 IP 情报数据，请求客户端 IP 有恶意爬虫、刷量和暴力破解行为的风险等级，取值有： • high：高风险 • medium：中等风险 • low：一般风险 • -：无历史数据或域名没有开启 客户端画像分析 功能	×	✓
BotClassProxy	String	基于近期 IP 情报数据，请求客户端 IP 开放可疑代理端口、并且被用作网络代理（包括秒拨IP）的风险等级，取值有： • high：高风险 • medium：中等风险 • low：一般风险 • -：无历史数据或域名没有开启 客户端画像分析 功能	×	✓
BotClassScanner	String	基于近期 IP 情报数据，请求客户端 IP 有攻击已知漏洞的扫描器行为的风险等级，取值有： • high：高风险 • medium：中等风险 • low：一般风险 • -：无历史数据或域名没有开启 客户端画像分析 功能	×	✓
BotTag	String	EO Bot 智能分析引擎根据请求速率、IP 情报库等因素对请求进行综合评估分类，仅提供	×	✓

		给已启用 Bot 管理 - Bot 智能分析 功能的域名。取值有： • evil_bot：恶意 Bot 请求 • suspect_bot：疑似 Bot 请求 • good_bot：正常 Bot 请求 • normal：正常请求 • -：未分类		
JA3Hash	String	用于分析 SSL/TLS 客户端的 JA3 指纹的 MD5 哈希值，仅提供给已启用 Bot 管理 的域名。	×	✓
SecurityAction	String	请求命中安全规则后的最终处置动作，取值有： • -：未知/未命中 • Monitor：观察 • JSChallenge：JavaScript 挑战 • Deny：拦截 • Allow：放行 • BlockIP：IP 封禁 • Redirect：重定向 • ReturnCustomPage：返回自定义页面 • ManagedChallenge：托管挑战 • Silence：静默 • LongDelay：长时间等待后响应 • ShortDelay：短时间等待后响应	×	✓
SecurityModule	String	最终处置请求的安全模块名称，与 `SecurityAction` 对应，取值有： • -：未知/未命中 • CustomRule：Web防护 - 自定义规则 • RateLimitingCustomRule：Web防护 - 速率限制规则 • ManagedRule：Web防护 - 托管规则 • L7DDoS：Web防护 - CC攻击防护 • BotManagement：Bot管理 - Bot基础管理 • BotClientReputation：Bot管理 - 客户端画像分析	×	✓

		• BotBehaviorAnalysis：Bot管理 – Bot智能分析 • BotCustomRule：Bot管理 – 自定义Bot规则 • BotActiveDetection：Bot管理 – 主动特征识别		
SecurityRuleID	String	最终处置请求的安全规则 ID，与 `SecurityAction` 对应。	×	✓

相关参考

日志示例

以下是默认情况下单条七层访问日志示例。您可以根据下游日志分析系统的具体要求自定义配置 EdgeOne 日志输出格式，更多请参见 自定义日志输出格式 。


```
{
    "ClientState": "CN-LN",
    "BotTag": "normal",
    "EdgeSeverRegion": "US",
    "RequestID": "13719873400522703510",
    "EdgeException": "client_request_exception.upstream_failed",
    "RequestMethod": "GET",
    "RequestUrlQueryString": "-",
    "LogTime": "2024-10-13T23:30:39Z",
    "RequestUrl": "/app/",
    "ClientPort": 62389,
    "RequestBodyBytes": 0,
    "SecurityRuleID": "-",
    "ContentID": "zone-2mxigizoh600",
    "OriginRequestHeaderSendDuration": 0.001,
    "EdgeResponseTime": 379,
    "ParentRequestID": "-",
    "EdgeServerRegionTopDivision": "CN-LN",
    "RequestSSLProtocol": "-",
    "RequestScheme": "HTTPS",
    "RequestTime": "2024-10-13T23:30:39Z",
    "EdgeResponseStatusCode": 404,
    "ClientIP": "0.0.0.0",
    "BotCharacteristic": "-",
    "SecurityAction": "-",
    "EdgeEndTime": "2024-10-13T23:30:39Z",
```

```
    "RequestRange": "-",
    "BotClassScanner": "-",
    "BotClassProxy": "-",
    "ClientDeviceType": "Desktop",
    "RequestHost": "www.example.com",
    "OriginSSLProtocol": "-",
    "EdgeResponseBodyBytes": 548,
    "RequestProtocol": "HTTP/1.1",
    "EdgeServerID": "b3da9837137ad37f8e430b1d6de51dc5-
d41d8cd98f00b204e9800998ecf8427e",
    "EdgeCacheStatus": "miss",
    "EdgeFunctionSubrequest": 0,
    "EdgeResponseBytes": 825,
    "OriginTCPHandshakeDuration": 182.485,
    "SecurityModule": "-",
    "ClientConnectionID": "5692760165714882237",
    "EdgeInternalTime": 378,
    "RequestBytes": 769,
    "OriginIP": "0.0.0.0",
    "JA3Hash": "-",
    "OriginResponseHeaderDuration": 182.676,
    "OriginResponseStatusCode": 404,
    "ClientRegion": "US",
    "RemotePort": 80,
    "ClientISP": "AS396982",
    "BotClassMaliciousBot": "-",
    "BotClassAccountTakeOver": "-",
    "OriginDNSResponseDuration": 0.0,
    "RequestReferer": "-",
    "BotClassAttacker": "-",
    "RequestUA": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36",
    "EdgeServerIP": "0.0.0.0",
    "OriginTLSHandshakeDuration": -1,
    "RequestStatus": "1"
}
```


EdgeException 字段说明

- **字段格式：** `[请求阶段].[异常描述]`
- **若无异常，则字段值为** `no_exception`

请求阶段

请求阶段取值	含义
client_request_exception	客户端向 EdgeOne 边缘节点发起请求过程中发生异常。
edge_response_exception	EdgeOne 边缘节点向客户端响应请求过程中发生异常。

异常描述

> **说明：**
> 以下仅列出常见异常情况，后续 EdgeOne 有可能追加新的异常情况描述。

异常描述取值	含义
timeout	超时
peer_close	对端关闭（对端关闭以是否收到 FIN 包为准）；对于 EdgeOne 边缘服务端来说，对端指的是客户端。
closed	本端主动关闭
read_buffer_full	读 buffer 满
package_write_failed	写失败（仅针对 UDP）
peer_error	读写数据出现异常（RST 等）
peers_is_empty	回源 peers 为空
module_load_failed	HTTP 模块加载失败
header_too_large	HTTP 头部过大
parse_header_failed	HTTP 解析头部失败
read_offset_out_of_upstream_range	读取回源数据的偏移超出了回源响应的 range
no_cache	不使用缓存
partial_compress_cache	仅包含部分压缩缓存
upstream_no_mtime	回源响应无 mtime
cache_no_mtime	本地缓存无 mtime
upstream_mtime_change	回源 mtime 变化
upstream_no_etag	回源响应无 etag

cache_no_etag	本地缓存无 etag
upstream_etag_change	回源 etag 变化
upstream_length_change	回源长度变化
upstream_status_change	回源状态码变化
upstream_data_not_set	回源模块数据未初始化
upstream_respond_extra_data	源站响应多余数据
domain_resolve_failed	回源域名解析失败
domain_resolve_none	回源域名解析结果为空
upstream_server_is_empty	源站列表为空
upstream_failed	回源失败
upstream_content_range_with_content_encoding	源站响应同时包含 Content-Range 和 Content-Encoding
upstream_unknown_transfer_encoding	源站响应未知 Transfer-Encoding
upstream_transfer_encoding_with_content_length	源站响应同时包含 Transfer-Encoding 和 Content-Length
upstream_keepalive_without_length	源站响应未知长度文件并要求 keep-alive
chunked_error	chunked 解析失败
read_file_info_failed	缓存文件信息读取失败
set_cache_data_failed	尝试设置缓存数据失败
unknown_compress_method	未知压缩算法
compress_size_too_large	压缩文件过大
compress_error	压缩异常
upstream_verify_failed	UUID 防劫持校验失败
scheme_error	未知 schema
empty_domain	域名为空

reset_client	需 RST 客户端
blacklist_fatal_error	封禁名单异常
range_index_error	多 Range 下标异常
upstream_respond_206_without_content_range	源站响应 206 未携带 Range
upstream_respond_content_range_without_size	源站响应 Content-Range 未携带文件总大小
upstream_respond_error_content_range	源站响应 Range 异常

BotCharacteristic 字段说明

> **说明：**
> 该字段仅提供给已启用 Bot 管理 - Bot 智能分析 功能的域名。

字段取值	对应规则名称	详细描述	映射 Bot 标签（`BotTag`）	可能命中攻击或业务场景
Client Inconsistency	客户端不一致	请求头部和特征不一致，或四层操作系统指纹与 User-Agent 不匹配	恶意 Bot	• 伪造 UA，例如 Linux 服务器请求却声明为 Windows UA； • 某些用户使用代理、办公网/校园网等出口时，四层指纹来自代理机器，与用户 UA 不匹配。
Irregular TLS Fingerprint	TLS 指纹异常	工具的 TLS 指纹异常	恶意 Bot，疑似 Bot	• 脚本工具发起的请求； • 某些客户端用工具/组件调用 API、静态资源。

High Frequency	高频请求	同一或几个 IP/User-Agent 发送大量请求	恶意 Bot，疑似 Bot	/
Irregular Path Access	非常规路径访问	请求路径出现随机或集中在特定接口，可能是扫描或数据抓取	恶意 Bot，疑似 Bot	• 某些站点资源少或做活动时，用户请求在短时间内高频集中访问某特定路径。
Real-time Proxy Detection	实时代理检测	基于实时流量模式，判断请求是否可能经由代理转发	恶意 Bot，疑似 Bot	• 黑产用秒拨代理换 IP 绕风控策略； • 用户用代理 VPN、办公网/校园网出口 IP； • 网络波动较大。
TLS Fingerprint Inconsistency	TLS 指纹不一致	TLS 指纹与 User-Agent 不匹配	恶意 Bot，疑似 Bot	• 某些小众客户端（非常见 UA）； • 脚本工具请求； • 篡改 UA 请求； • 办公网/校园网出口。
UA with Bot Identifier	UA 含 Bot 标识	User-Agent 中包含常见的 bot 工具标识	恶意 Bot	• 用户 UA 含常见脚本工具标识字符串。
Python-Requests	Python-requests 请求	使用 python-requests 工具发送请求	恶意 Bot	• 用户 UA 含 `python-requests` 字符串。
Python-Urllib	Python-urllib 请求	使用 python-urllib 工具发送请求	恶意 Bot	• 用户 UA 含 `python-urllib`

				字符串。
Curl	cURL 请求	使用 curl 工具发送请求	恶意 Bot	• 用户 UA 含 `curl` 字符串。
Go HTTP Client	Go HTTP 客户端请求	使用 go-http-client 工具发送请求	恶意 Bot	• 用户 UA 含 `go-http-client` 字符串。
Phpcrawl	phpcrawl 请求	使用 phpcrawl 工具发送请求	恶意 Bot	• 用户 UA 含 `phpcrawl` 字符串。
Libcurl	libcurl 请求	使用 libcurl 工具发送请求	恶意 Bot	• 用户 UA 含 `libcurl` 字符串。
WinHTTP Client	WinHTTP 请求	使用 WinHttpClient 工具发送请求	恶意 Bot	• 用户 UA 含 `WinHttpClient` 字符串。
Headless Browser	无头浏览器	使用无头浏览器（如 Puppeteer，Selenium 等）发送请求	恶意 Bot	• 用户 UA 含 `headless` 字符串。
Triggered by Known Tool# {Num}	特定工具特征# {Num}	特定工具或行为触发的规则。`{Num}` 用于标识不同的工具或行为。暂不支持自助查询/管理这一类特征，若有疑问请 联系我们 。	恶意 Bot，疑似 Bot	/

四层代理日志

最近更新时间：2024-04-30 14:36:11

以下是四层代理日志的详细字段说明。

说明：

- 在 TCP 长连接的场景下，EdgeOne 会周期记录日志，并且在连接结束的时候记录最后一条日志，您可以通过 `DisconnetReason` 字段是否为空来判定连接是否断开；同时也可以使用 `SessionID` 来标识连接，相同的 `SessionID` 的日志记录的是相同连接的行为。
- 四层代理日志类型下，实时日志和离线日志所记录的字段相同。

字段名称	数据类型	说明
ClientRealIP	String	客户端真实 IP。
ClientRegion	String	客户端所在国家/地域 2 位字母编码，符合 ISO-3166 alpha-2 规范。
ConnectTimeStamp	Timestamp ISO8601	建连时间，默认UTC +0 时区。

DisconnetReason	String	断连原因，若当前日志周期内未断连，则值为“-”。
		• 格式为「方向：原因」
		• 方向取值有：
		  ○ up：源站方向
		  ○ down：客户端方向
		• 原因取值有：
		  ○ net_exception_peer_error：读写对端返回错误
		  ○ net_exception_peer_close：对端已关闭连接
		  ○ create_peer_channel_exception：创建到下一跳的 channel 失败
		  ○ channel_eof_exception：channel 已结束（请求结束时，结束请求的节点会给相邻节点发送 channel_eof 告知相邻节点请求已结束）
		  ○ net_exception_closed：连接已关闭
		  ○ net_exception_timeout：读写超时

DisconnetTimeStamp	Timestamp ISO8601	断连时间，默认 UTC +0 时区。若当前日志周期内未断连，则值为“-”。

EdgeIP	String	访问的 EdgeOne 服务器 IP 地址。
ForwardPort	Integer	客户配置的转发端口。
ForwardProtocol	String	客户配置的转发协议 TCP/UDP。
LogTimeStamp	Timestamp ISO8601	日志生成时间；默认 UTC +0 时区。
ReceivedBytes	Integer	上一条日志记录时间至本条日志记录期间产生的出流量，单位：Byte。
SentBytes	Integer	上一条日志记录时间至本条日志记录期间产生的入流量，单位：Byte。
ServiceID	String	四层代理服务唯一标识 ID。
SessionID	String	TCP 连接或 UDP 会话的唯一标识 ID。

边缘函数运行日志

最近更新时间：2025-04-22 15:10:42

字段说明

字段名称	数据类型	说明
EdgeFunctionName	String	此次被触发的边缘函数名称。
RequestHost	String	客户端请求的 Host（主请求访问的域名）。
RequestID	String	客户端请求的唯一标识 ID（主请求的 UUID）。
EventTimestamp	Integer	函数触发的时间戳。格式：UNIX，精确到毫秒。
Logs	Array[object]	用户在 JS 代码中 console.log() 方法打印的指定信息。
Outcome	String	函数执行是否成功，取值有： • ok：无异常或错误 • exception：有异常或错误，若需了解错误详情，请参考 Exceptions 字段。
Exceptions	Array[object]	函数执行中遇到的异常和错误详情。
CpuTime	Integer	占用 CPU 的耗时，单位：微秒。
WallTime	Integer	墙钟耗时，从函数触发到结束所经历的耗时，单位：微秒。

日志示例

以下是默认情况下单条边缘函数运行日志示例。您可以根据下游日志分析系统的具体要求自定义配置 EdgeOne 日志输出格式，更多请参见 自定义日志输出格式 。

```
{
    "WallTime": 125221,
    "RequestID": 8254903099116445190,
```

```
    "EventTimestamp": 1727251229247,
    "EdgeFunctionName": "testtracelog-zone-2rdnikn6zjck-251255070",
    "Outcome": "ok",
    "RequestHost": "www.example.com",
    "Exceptions": [],
    "Logs": [
        {
            "level": "INFO",
            "message": "test log from function",
            "timestamp": 1727251229247
        }
    ],
    "CpuTime": 547
}
```

推送实时日志筛选条件

最近更新时间：2025-06-26 11:21:23

实时日志推送任务支持配置筛选条件，帮助您过滤特定类型日志、减少下游日志处理量。以下为支持的日志字段、比较运算符。

说明

- 目前仅实时日志-**站点加速日志**支持配置推送日志筛选条件。
- 实时日志推送筛选条件功能内测中，如您需要使用请 联系我们 。

支持的日志字段

字段名称	数据类型	说明
SecurityAction	String	请求命中安全规则后的最终处置动作，取值有： • -：未知/未命中 • Monitor：观察 • JSChallenge：JavaScript 挑战 • Deny：拦截 • Allow：放行 • BlockIP：IP 封禁 • Redirect：重定向 • ReturnCustomPage：返回自定义页面 • ManagedChallenge：托管挑战 • Silence：静默 • LongDelay：长时间等待后响应 • ShortDelay：短时间等待后响应
SecurityModule	String	最终处置请求的安全模块名称，与 `SecurityAction` 对应，取值有： • -：未知/未命中 • CustomRule：Web 防护 - 自定义规则 • RateLimitingCustomRule：Web 防护 - 速率限制规则 • ManagedRule：Web 防护 - 托管规则 • L7DDoS：Web 防护 - CC 攻击防护 • BotManagement：Bot 管理 - Bot 基础管理 • BotClientReputation：Bot 管理 - 客户端画像分析 • BotBehaviorAnalysis：Bot 管理 - Bot 智能分析

		• BotCustomRule：Bot 管理 – 自定义 Bot 规则 • BotActiveDetection：Bot 管理 – 主动特征识别
EdgeResponseStatusCode	Integer	节点响应返回给客户端的状态码。
OriginResponseStatusCode	Integer	源站响应状态码，若没有回源，记录为 -1。

支持的比较运算符

比较运算符名称	是否支持该数据类型	
	String	Integer
等于（匹配列表中任意值）	✓	✓
大于	×	✓
小于	×	✓
大于等于	×	✓
小于等于	×	✓

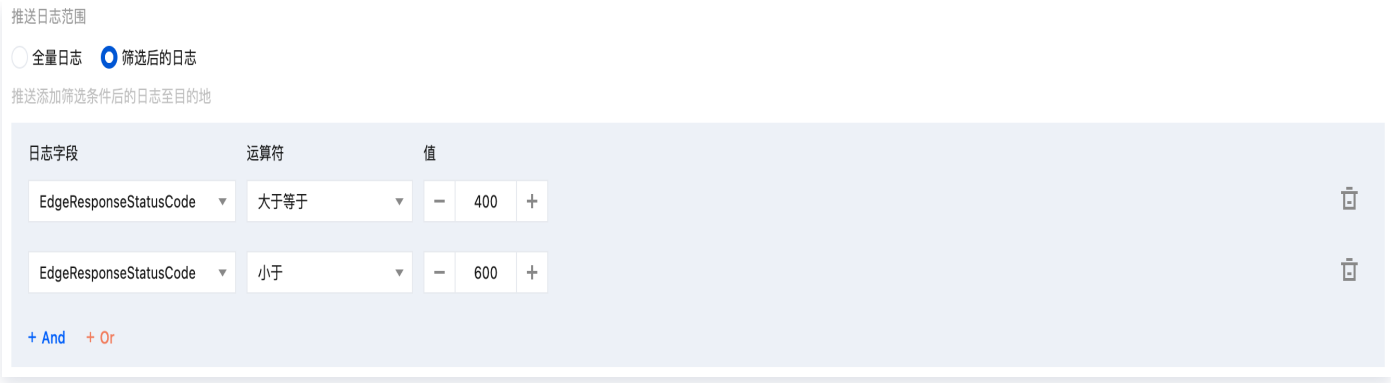
示例：筛选推送 HTTP 状态码为 4xx/5xx 的日志

示例场景

在一家大型电商平台的 IT 运维团队中，您负责监控和分析网站的实时日志。由于网站的访问量巨大，日志数据量也非常庞大，因此您希望通过设置过滤规则来减少不必要的日志数据推送，从而避免对分析平台造成不必要的负担。例如：您可以配置仅推送 HTTP 状态码为 4xx/5xx 的访问日志，这些状态码通常表示出现了某种错误。通过这种方式，您可以专注于那些可能指向用户体验问题或需要立即关注的系统故障的日志。您可以参考以下步骤进行配置。

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，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**日志服务 > 实时日志**。
3. 在实时日志页面，单击**新建推送任务**。
4. 在选择日志源页面，填写任务名称、选择日志类型、服务区域、需推送日志的域名/四层代理实例，单击**下一步**。
5. 在定义推送内容页面，配置推送日志范围。
   5.1 选中**筛选后的日志**。
   5.2 填写筛选条件如下图所示：



6. 完成目的地配置后，单击**推送**。

自定义推送日志字段

最近更新时间：2025-06-26 11:21:23

如果您需要推送 HTTP 请求头、HTTP 响应头、Cookie、HTTP 请求正文中的某些字段值，您可以通过自定义日志字段功能将此类信息精确记录在日志中。

使用限制说明

- 目前仅**实时日志-站点加速日志**支持添加自定义字段；
- 同一个实时日志推送任务中，自定义字段名称不能重复；
- 最多配置 200 个自定义字段；
- 字段名称区分大小写，需要与 HTTP 行为中的原始字段名称完全匹配；
- 字段类型选择请求头、响应头、Cookie 时，字段名称可输入 1-100 个字符，允许的字符开头为字母，中间为字母、数字、-，结尾为字母、数字；
- 字段类型选择请求正文时，支持通过 Google RE2 正则表达式提取指定内容；
  - 单个请求正文类型字段，正则表达式长度上限为 4KB；
  - 单个请求正文类型字段，提取内容的长度上限为 1000 Bytes，超过此上限的内容将会被截断丢弃；
  - 单个实时日志推送任务最多添加 5 个请求正文类型的自定义字段。

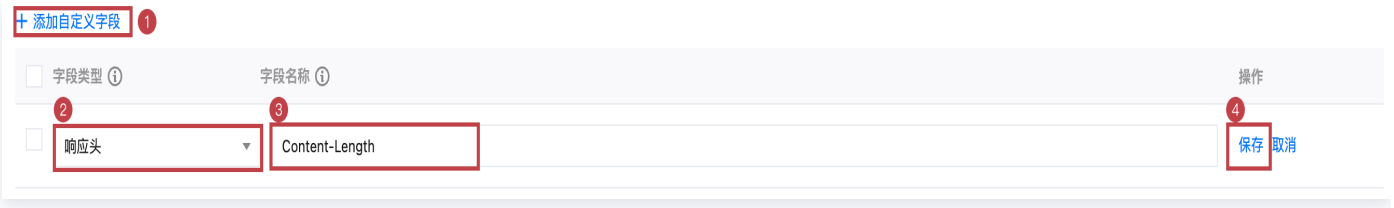
示例一：在日志中记录指定响应头部的值

示例场景

在某些业务场景下，了解响应体的大小对于监控网络流量和优化性能至关重要。为了实现这一目的，可以配置自定义日志字段来记录每个响应的 `Content-Length` 头部的值。

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，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**日志服务 > 实时日志**。
3. 在实时日志页面，单击**新建推送任务**。
4. 在选择日志源页面，填写任务名称、选择日志类型、服务区域、需推送日志的域名，单击**下一步**。
5. 在定义推送内容页面，单击**添加自定义字段**。
   5.1 选择字段类型为响应头；
   5.2 填写字段名称为 `Content-Length`；
   5.3 单击**保存**。



6. 完成目的地配置后，单击**推送**。

示例二：在日志中记录请求正文中的指定内容

示例场景

假设您需要从 POST 请求中提取请求正文 JSON 对象中的 `account` 字段，用于分析不同账号用户的访问行为。

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，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**日志服务 > 实时日志**。
3. 在实时日志页面，单击**新建推送任务**。
4. 在选择日志源页面，填写任务名称、选择日志类型、服务区域、需推送日志的域名，单击**下一步**。
5. 在定义推送内容页面，单击**添加自定义字段**。
   5.1 选择字段类型为请求正文；
   5.2 填写字段名称为 `"account": "(.*?)"`
   5.3 单击**保存**。

6. 完成目的地配置后，单击**推送**。
7. 发送测试请求检查日志记录行为是否符合预期，测试命令如下：

```
curl -X POST https://www.example.com -H "Content-Type:
application/json" -d '{"account": "user123", "password": "pass456"}'
```

8. 接收到的日志将会增加 `RequestBodyCustom1` 字段，示例以键值对形式展示如下。若您在单个实时日志推送任务中添加多个请求正文类型自定义字段，则接收到的日志将会依次增加 `RequestBodyCustom1` 、`RequestBodyCustom2` ……多个字段。

```
{"RequestBodyCustom1":"\"account\": \"user123\""}
```

参考资料

如您希望了解各种 HTTP 请求头和响应头的释义，以决定是否将它们记录至日志中，请参考 HTTP 标准头部说明 。

自定义日志输出格式

最近更新时间：2024-08-28 17:30:01

功能简介

支持用户自定义日志数据的输出格式，包括选择不同的日志记录风格（如 JSON Lines 或 CSV）以及定义批次和单条日志的前后缀、日志记录或字段之间的分隔符。实时日志和离线日志的默认格式为 JSON Lines 。

> **说明：**
> 目前仅实时日志-**站点加速日志**支持配置日志输出格式。

配置项

- **日志输出格式**：日志投递的预设输出格式类型。
  - **JSON Lines**：单条日志中的字段以键值对方式呈现。
  - **CSV**：单条日志中仅呈现字段值，不呈现字段名称。
- **批次前后缀**：用户可以为日志批次定义前缀和后缀。“一个批次”指的是一次日志推送请求。每个日志投递批次可能包含多条日志记录。
  - **前缀**：在每个日志投递批次之前添加的字符串。
  - **后缀**：在每个日志投递批次后附加的字符串。
- **单条日志前后缀**：
  - **前缀**：在每条日志记录之前添加的字符串。
  - **后缀**：在每条日志记录后附加的字符串。

> **说明：**
> 在未开启日志采样或 筛选 的情况下，对于域名业务而言，一次 HTTP 请求对应一条日志记录。

- **日志分隔符**：插入日志记录之间作为分隔符的字符串。
- **字段分隔符**：单条日志记录内，插入字段之间作为分隔符的字符串。

示例配置

以下是不同日志输出格式配置对应的日志样本。

JSON Lines

配置示例

配置项	值

日志输出格式	JSON Lines
单条日志前缀	{
单条日志后缀	}
日志分隔符	\n
字段分隔符	,

输出日志样本

```
{"SecurityAction":"Deny","RequestID":"14941044941971548881","RequestTime
":"2024-08-12T08:12:15Z","ClientIP":"1.1.1.1"}
{"SecurityAction":"Deny","RequestID":"14941045941971548882","RequestTime
":"2024-08-12T08:12:30Z","ClientIP":"2.2.2.2"}
```

csv

配置示例

配置项	值
日志输出格式	csv
日志分隔符	\n
字段分隔符	,

输出日志样本

```
Deny,14941044941971548881,2024-08-12T08:12:15Z,1.1.1.1
Deny,14941045941971548882,2024-08-12T08:12:30Z,2.2.2.2
```

JSON Lines 变体

JSON 数组格式配置示例

配置项	值
日志输出格式	JSON Lines
批次前缀	[

批次后缀	]
单条日志前缀	{
单条日志后缀	}
日志分隔符	,
字段分隔符	,

JSON 数组格式输出日志样本

```
[

{"SecurityAction":"Deny","RequestID":"14941044941971548881","RequestTime
":"2024-08-12T08:12:15Z","ClientIP":"1.1.1.1"},

{"SecurityAction":"Deny","RequestID":"14941045941971548882","RequestTime
":"2024-08-12T08:12:30Z","ClientIP":"2.2.2.2"},

{"SecurityAction":"Allow","RequestID":"14941046941971548883","RequestTim
e":"2024-08-12T08:12:45Z","ClientIP":"3.3.3.3"}
]
```

内嵌 JSON 对象格式配置示例

配置项	值
日志输出格式	JSON Lines
批次前缀	{"events":[
批次后缀	]}
单条日志前缀	{"info":{
单条日志后缀	}}
日志分隔符	,
字段分隔符	,

内嵌 JSON 对象格式输出日志样本

```
{"events": [
```

```
        {"info":
{"SecurityAction":"Deny","RequestID":"14941044941971548881","RequestTime
":"2024-08-12T08:12:15Z","ClientIP":"1.1.1.1"}},
        {"info":
{"SecurityAction":"Deny","RequestID":"14941045941971548882","RequestTime
":"2024-08-12T08:12:30Z","ClientIP":"2.2.2.2"}}
]}
```

csv 变体

csv 携带表头格式配置示例

配置项	值
日志输出格式	csv
批次前缀	SecurityAction,RequestID,RequestTime,ClientIP\n
日志分隔符	\n
字段分隔符	,

csv 携带表头格式输出日志样本

```
SecurityAction,RequestID,RequestTime,ClientIP
Deny,14941044941971548881,2024-08-12T08:12:15Z,1.1.1.1
Deny,14941045941971548882,2024-08-12T08:12:30Z,2.2.2.2
Allow,14941046941971548883,2024-08-12T08:12:45Z,3.3.3.3
```

tsv 格式配置示例

配置项	值
日志输出格式	csv
日志分隔符	\n
字段分隔符	\t

tsv 格式输出日志样本

```
Deny  14941044941971548881  2024-08-12T08:12:15Z  1.1.1.1
Deny  14941045941971548882  2024-08-12T08:12:30Z  2.2.2.2
```

```
Allow  1494104694197154888 3  2024-08-12T08:12:45Z  3.3.3.3
```

数据分析
概述

最近更新时间：2024-07-30 16:32:11

腾讯云边缘安全加速平台 EdgeOne 通过分析访问日志数据，在数据分析页面中提供多种数据指标，供您多维度了解业务数据。

适用场景

场景	具体诉求
日常监控巡检	通过观察加速域名/四层代理实例的各项数据指标走势和分布，持续监控 EdgeOne 是否存在高延迟或故障等问题。
故障排查分析	通过分析访问日志，了解报障用户访问的路径、内容等信息，从而定位问题并进行排查。
业务数据洞察	通过对客户端数据进行分析和挖掘，了解用户画像。

功能详情

数据分析功能	功能介绍
指标分析	提供流量、带宽、请求数等汇聚后的指标数据，支持查看访问区域分布、缓存命中情况、安全防护情况、状态码情况，助您了解各类已接入 EdgeOne 业务的运行状况。
Web 安全分析	通过对命中 Web 安全防护规则的访问日志进行分析，了解与您业务有关的攻击面数据，包括攻击来源、攻击方式等，帮助您更好地了解攻击情况，制定更有效的安全策略。支持直接查看样本日志，了解攻击请求上下文。

指标分析

最近更新时间：2025-07-03 10:29:21

功能简介

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。

支持查看的指标

指标分析支持用户自定义展示数据指标，具体包括以下操作：

1. **展示和排序指标**：用户可以在**指标设置**中选择是否展示某个指标，并通过拖放的方式对指标进行排序，以确定指标在仪表板上的展示顺序。
2. **选择时间范围**：用户可以 修改查询时间范围 来查看数据，如近30分钟、近1小时、今日等。单次筛选的时间跨度不超过31天。
3. **设置筛选条件**：用户可以 使用筛选条件 来细化查看的数据，例如根据域名、状态码、国家/地区等进行筛选。

> **注意：**
> 1. 历史时间范围的支持情况可能因您的套餐版本而有所区别，具体请参考 套餐选型对比 。若控制台抛出“查询时间范围超过限制”错误，请缩短查询时间窗口至您的套餐所支持的范围之内。
> 2. 部分分析维度下的数据（如：客户端 IP、状态码、URL Path、Referer 等）仅保留 30 天。例如：当您查询一个月前指定客户端 IP 数据时，可能出现查询不到数据的情况。
> 3. 为了优化用户体验，EdgeOne 数据分析中引入了 抽样数据统计 技术，以确保即使在处理大量数据时，也能保持查询的准确性和及时性。
> 4. 当拥有部分站点权限且拥有权限的站点数超过 100 个的子用户访问数据查询相关页面时，控制台将抛出“权限不足（ `Cam no permission` ）”错误，此时请筛选具体站点列表来查询数据，且单次查询所筛选的站点数量最大 100 个。

指标分析支持查看以下指标：

域名业务相关指标

- **L7 访问流量**：客户端与 EdgeOne 之间传输的流量统计；单击 **EdgeOne 响应流量**后，支持查看访问区域分布、Host、客户端 IP、Referer、URL Path、资源类型、状态码、客户端浏览器、客户端设备类型、客户端操作系统排行等。
- **L7 访问带宽**：客户端与 EdgeOne 之间传输的带宽统计。

> **说明：**

在 不同时间统计颗粒度 下，带宽指标的计算方式会有所区别。该计算方式适用于 L7 访问带宽、L7 回源带宽、L4 访问带宽指标。
- 1 分钟颗粒度：1 分钟内的总流量 * 8 / 60 秒。
- 5 分钟颗粒度：5 分钟内的总流量 * 8 / 300 秒。
- 1 小时颗粒度：所有的 5 分钟颗粒度带宽峰值点中的最大值。
- 1 天颗粒度：所有的 5 分钟颗粒度带宽峰值点中的最大值。

- **L7 访问请求数**：EdgeOne 收到客户端请求数统计。
- **L7 防护命中次数**：请求命中 EdgeOne Web 防护安全规则的次数统计；点击某一类安全规则（如：自定义规则）后，支持查看更多维度数据，例如命中规则排行、客户端 IP 排行、URL Path 排行、客户端分布、最近事件等。
- **L7 回源流量**：EdgeOne 与源站之间传输的流量统计。
- **L7 回源带宽**：EdgeOne 与源站之间传输的带宽统计。
- **L7 回源请求数**：EdgeOne 向源站发起的请求数统计。
- **缓存命中率**：EdgeOne 边缘节点响应流量中，未从源站获取而直接提供服务的百分比。统计公式：`缓存命中率 = 1 - （源站响应流量 / EdgeOne 响应流量）`

> **说明：**
> L7 回源相关指标、缓存命中率指标展示功能在内测中，如您需要使用请 联系我们 。

- **L7 访问响应耗时**：
  - **L7 访问平均响应耗时**：从 EdgeOne 接收到客户端请求到响应客户端完整文件的平均耗时，不包含 TCP 建连和 TLS 握手耗时。统计公式：`所有请求的响应耗时总和 / 访问请求数总和` 。
  - **L7 访问平均首字节响应耗时**：从 EdgeOne 接收到客户端请求到响应客户端第一个字节的平均耗时，不包含 TCP 建连和 TLS 握手耗时。统计公式：`所有请求的首字节响应耗时总和 / 访问请求数总和` 。
- **DNS 解析次数**： EdgeOne DNS 接收到解析请求的数量。仅支持 NS 模式接入的站点数据。

边缘函数相关指标

- **边缘函数执行次数**：
  - **总执行次数**：触发边缘函数执行的次数。当客户端请求满足触发规则或请求边缘函数默认访问域名时，将触发边缘函数执行。
  - **执行成功次数**：边缘函数执行结果为成功的次数。
  - **执行失败次数**：边缘函数执行结果为失败的次数。
- **边缘函数执行 CPU 耗时**：边缘函数在执行过程中占用 CPU 的时长。展示的统计方式包括平均值和分位值（P50、P90、P99）。
- **边缘函数执行墙钟耗时**：边缘函数从开始执行到结束的耗时。墙钟耗时包括函数的实际执行时间以及可能的等待时间（如 I/O 操作等）。展示的统计方式包括平均值和分位值（P50、P90、P99）。

说明：

1. P50、P90、P99 分位值是通过以下方式计算的：
   - P50（中位数）：表示数据中有50%的值小于或等于该值。
   - P90：表示数据中有90%的值小于或等于该值。
   - P99：表示数据中有99%的值小于或等于该值。
2. 请注意，查看分位值统计数据时，您需要通过筛选条件指定某一个具体边缘函数实例。

TCP/UDP 应用业务相关指标

- **L4 访问流量**：客户端与 EdgeOne 之间传输的流量统计。
- **L4 访问带宽**：客户端与 EdgeOne 之间传输的带宽统计。
- **L4 并发连接数**：客户端与 EdgeOne 之间同时建立的传输层连接数量。支持查看并发连接数的访问区域分布。

说明：

在 不同时间统计颗粒度 下，并发连接数指标的计算方式会有所区别。

- 1 分钟颗粒度：1 分钟内所有活跃过的连接数。
- 5 分钟颗粒度：所有 1 分钟颗粒度并发连接数点中的最大值。
- 1 小时颗粒度：所有 1 分钟颗粒度并发连接数点中的最大值。
- 1 天颗粒度：所有 1 分钟颗粒度并发连接数点中的最大值。

L3/4 DDoS 攻击防护相关指标

- **L3/4 DDoS 攻击防护带宽**：针对网络层和传输层 DDoS 攻击的防护带宽、包速率、攻击事件数。支持查看防护流量、包数的协议排行。支持查看历史攻击事件、攻击来源分布、攻击类型排行。

EdgeOne Shield 相关指标

- **EdgeOne Shield 响应流量**：EdgeOne Shield 服务响应的流量。
- **EdgeOne Shield 响应请求数**：EdgeOne Shield 服务响应的请求次数。

说明：

EdgeOne Shield 功能在内测中，如您需要使用请 联系我们 。

Web 安全分析

最近更新时间：2024-11-04 20:48:02

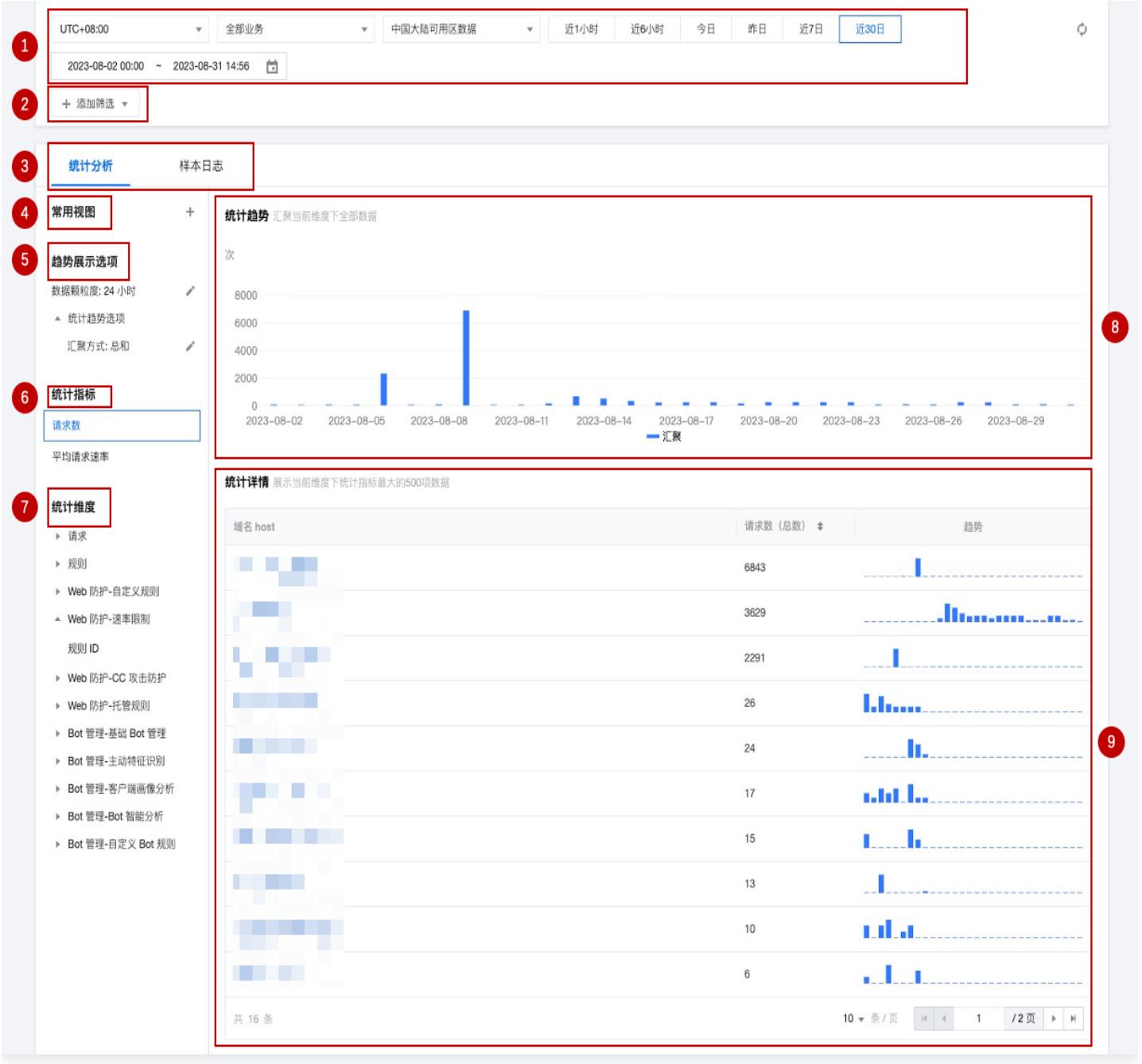
概述

Web 安全分析提供了安全事件精细化分析工具，为您制定或调整安全策略提供参考。您不仅可以查看近期安全事件在数十个维度下的统计分析和分布趋势，还可以通过查看样本日志，进一步了解某一事件的具体内容和详细信息。Web 安全分析为经过 EdgeOne Web 防护功能的请求数据提供了多个分析维度，帮助您制定高效的安全策略。

支持的能力

说明：

1. 由于一个安全事件中，单个请求可能命中多个安全规则。在进行筛选或选择统计维度时，请注意区分规则的处置方式和请求的处置结果。例如：一个请求命中了多条**处置方式**为观察的规则，同时命中了一条**处置方式**为拦截的规则，导致该请求最终的**处置结果**为拦截。
2. 为了优化用户体验，EdgeOne 数据分析中引入了 抽样数据统计 技术，以确保即使在处理大量数据时，也能保持查询的准确性和及时性。



1. 数据时间范围

通过调整查询时间范围，您可以查询某一特定时间段的安全事件。

> **说明：**
> 不同版本套餐可支持的查询时间范围请参见 套餐选型对比 。

2. 添加筛选

支持的根据请求特征、规则 ID 等多种维度筛选需要统计的 Web 安全数据，Web 安全分析支持的筛选项可参考 如何使用筛选条件 。

> **说明：**
> 1. 同一个请求可能命中多条规则，因此当使用规则 ID 筛选时，会展示同时命中的其他规则的统计详情和趋势分布。
> 2. 您可以在统计详情中点击需要筛选的特征值，快速添加到筛选。

3. 分析维度

- **统计分析：**帮助您按所选维度展示指标排名，发现异常访问量和异常访问趋势。例如：当您选择按 User-Agent 头部维度展示时，您可以查看访问的设备分布和访问指标趋势，从而鉴别出访问量异常的设备类型，以及匀速周期访问的可疑访问行为。
- **样本日志：**帮助您进一步查看安全事件详情，判断请求命中的安全策略是否符合预期。例如：您可以通过样本日志查看请求命中的托管规则，以及托管规则匹配的字段内容，从而帮助您判断是否为误杀，并据此调优安全策略。

4. 常用视图

您可以根据需要，将当前视图选项保存为常用视图，便于后续快捷使用。您可以为常用视图命名，视图将保存当前趋势展示选项、统计指标和 统计维度信息。

5. 趋势展示统计方式

> **说明：**
> 当调整数据筛选时间范围时，数据颗粒度会对应调整，以确保有合适的趋势图表展示。

您可以按需要调整趋势图的展示选项：

- 数据颗粒度：趋势图中每个柱对应的数据统计时长。
- 汇聚方式：趋势图中每个柱对应数据的计算方式。
  - 总和：展示按所选维度过滤数据后，该时间段段内所有统计项的指标总和。例如：趋势图中一个柱对应的统计时段中，有 6000 个请求，则该柱展示数据为 6000。
  - 平均值：展示按所选维度过滤数据后，该时间段段内所有统计项指标的平均值。例如：按 Host 维度展示统计数据时，数据共包含 5 个 Host 数据，趋势图中一个柱对应的统计时段中，有 6000 个请求，则该柱展示数据为 6000 / 5 = 1200。
  - 最大值：展示按所选维度分拆数据后，该时间段内的最大数据项。
  - 99 分位值：展示按所选维度分拆数据后，该时间段内大于 99% 数据项的最小数值，即：该值大于其他 99% 的统计项指标值。
  - 99.9 分位值：展示按所选维度分拆数据后，该时间段内大于 99.9% 数据项的最小数值，即：该值大于其他 99.9% 的统计项指标值。

6. 统计指标

您可以选择展示 请求数 或者 平均请求速率 指标，来展示需要的统计特征（如：速率特征或请求数特征）。

- 请求数：按当前统计维度展示总请求数，用于区分大量请求的访客特征。例如：按 请求 `Host` 维度分析，可以区分出访问较集中的业务域名。
- 平均请求速率：按当前统计维度统计平均请求速率，用于区分访问频次较高的访客特征。例如：按 `User-Agent` 头部维度分析，可区分出访问频率异常的设备类型。

7. 统计维度

Web 安全分析提供了下列分析维度分类，您可以选择按所选维度调整统计对象和分组方式：

- 按**请求**属性分类的统计维度有：
  - 客户端 IP：统计来自不同客户端 IP 的请求数。
  - 客户端 IP（XFF 头部优先）：统计来自不同客户端 IP 的请求数。如果客户端经过 Web 代理访问，将按 XFF 头部中最近一跳的 IP 统计。
  - User-Agent：统计来自不同设备类型（通过 HTTP User-Agent 头部区分）的请求。
  - 请求 URL：统计访问不同 URL（包括访问路径和查询参数）的请求。
  - 域名 Host：统计访问不同域名（通过 HTTP 头部 Hostname 区分）的请求。
  - 来源 Referer：统计使用不同引用方式（通过 HTTP Referer 头部区分）访问资源的请求。
- 按**规则**属性分类的统计维度有：
  - 类型：统计命中不同安全模块（如：自定义规则、托管规则等）的请求。
  - 规则 ID：统计命中不同规则的请求。

> **说明：**
> 1. 您可以使用规则分类中规则 ID 选项合并展示命中所有安全防护规则的请求。
> 2. 您也可以使用具体安全功能分类中的规则 ID 选项，仅查看命中该模块中规则的情况。如：按命中 Web 防护自定义规则的规则 ID 来统计请求。
> 3. 不同版本套餐可支持的统计维度不同，详情请参见 套餐选型对比 。

您也可以选择其他按防护功能提供的分析选项。如：托管规则的命中字段、Bot 智能分析的 Bot 标签等，来进行统计分析。

8. 统计趋势图

统计趋势图将根据您的趋势展示选项和筛选条件，展示对应的汇聚数据柱状图。

9. 统计详情

根据您的统计维度和统计指标选项，展示不同维度的请求特征值，以及对应的指标。例如：当选择了 请求数 指标和 `User-Agent` 分析维度时，统计详情部分将展示不同客户端设备类型（User-Agent 头部取值）的请求数，按请求数从大到小排列展示，并展示各个设备类型的请求趋势。

分析示例

场景一：分析近 1 天内 CC 攻击防护的请求趋势

场景示例

假设您的站点 `example.com` 发现可疑的访问量突增，命中了 CC 攻击防护规则。需要分析在近 1 天内所有命中 CC 攻击防护的请求是否为正常请求，您可以参考以下步骤进行分析。

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 **Web 安全分析**。
2. 筛选查看需要分析的站点域名、时间范围以及聚合条件，以当前场景为例，可选择过去 1 天的时间范围内。
3. 在统度分析中，单击 **Web 防护-CC 攻击防护 > 规则 ID**。

4. 查看数据结果，以上图为例，智能客户端过滤触发的请求数非常高（规则 ID：4294967293）可单击该**规则 ID** 加入筛选。然后单击左侧统计维度内的**请求 > User Agent**，即可查看命中该规则的所有 User-Agent 头部汇总信息。您可以根据 User-Agent 值判断是否符合您正常客户端预期。您也可以在统计维度中继续添加其它统计维度，例如：客户端 IP 和 请求 URL 来进一步缩小筛选范围。

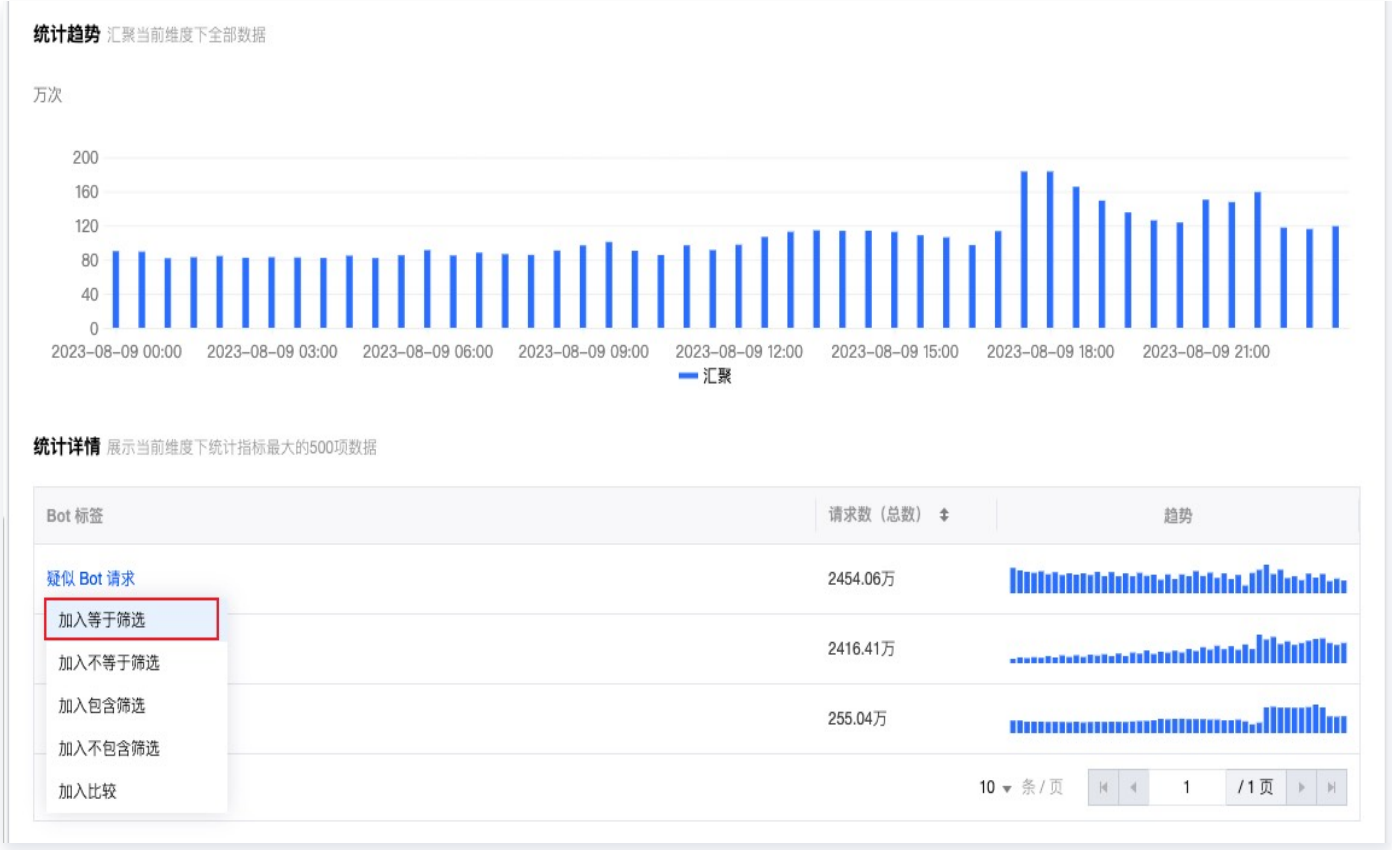
场景二：分析近 1 天内疑似 Bot 请求是否存在异常请求

场景示例

假设您的站点 `example.com` 近期频繁遭遇疑似 Bot 访问，需要分析在过去1天内所有疑似 Bot 请求访问的是否为正常请求，您可以参考以下步骤进行分析。

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 **Web 安全分析**。
2. 筛选查看需要分析的站点域名、时间范围以及聚合条件，以当前场景为例，可选择过去 1 天的时间范围内。
3. 在统计分析中，单击 **Bot 管理-Bot 智能分析 > Bot 标签**。
4. 查询数据结果，在统计详情内，可以看到相应 Bot 标签的请求次数。以当前场景为例，可以单击**疑似 Bot 请求 > 加入等于筛选**做进一步分析，加入筛选条件后，您也可以在统计维度中继续添加其它统计维度，例如：User-Agent 来进一步缩小筛选范围。



5. 单击**样本日志**，切换至详细样本日志分析，单击每条日志左侧的箭头可展开查看详细的请求头以及命中规则情况，来用于判断该请求是否为正常请求。

数据服务报表

最近更新时间：2025-05-29 17:56:43

功能简介

本功能旨在为用户提供发送数据服务报表邮件的能力。通过该功能，用户可以接收到关于 EdgeOne 服务使用情况的详细报表，帮助用户更好地监控和分析服务性能和站点安全情况。报表可以通过邮件即时下载或定时发送（每天/每周/每月）以满足不同场景需求。

套餐支持差异

数据服务报表功能仅在标准版和企业版中可用。

功能	个人版	基础版	标准版	企业版
数据服务报表	不支持		10个任务/站点	20个任务/站点

报表订阅任务配置说明

配置项目	说明
服务报表名称	用于填充邮件标题。支持中文、字母、数字、连字符、下划线，长度限制为2-120个字符，不能以连字符开头。
归属站点	选择期望推送报表数据的站点。
报表格式	选择报表的格式，可选值包括： • **HTML**：报表内容将内嵌于邮件正文。
发送频率	选择报表发送的频率，可选值包括： • **立即发送**：配置后立即发送报表； • **每天**：每天固定时间发送前一天数据； • **每周**：每周一固定时间发送前一周数据； • **每月**：每月1日固定时间发送前一月数据。 **说明：** • 发送报表的固定时间为 8:00-10:00，若出现报表堆积等现象，可能导致报表实际推送时间延迟。

	• 发送时间点将跟随报表任务配置的时区。例如：某报表任务配置发送频率为每天，时区为 UTC+9，则预计发送报表时间点为每天 UTC+9 时区的 8:00-10:00。
接收渠道	选择报表接收的渠道，可选值包括： • **腾讯云用户**：按照 访问管理子用户 配置接收对象； • **腾讯云用户组**：按照 访问管理用户组 配置接收对象。
接收对象	指定报表接收的对象。 ⚠ **注意：** 请确保接收对象中配置的用户已在 访问管理配置联系邮箱 ，否则将导致报表推送失败。
时区	设置报表发送的时区。
数据时间范围	设置生成报表时的数据时间范围。仅当发送频率选择**立即发送**时，支持配置数据时间范围。更多信息请参考 修改查询时间范围 。
数据筛选条件	添加生成报表时的数据筛选条件。仅当服务报表内容选择**域名业务流量服务**时，支持配置数据筛选条件。更多信息请参考 使用筛选条件 。
服务报表内容	选择报表内容模板，可选值包括： • **域名业务流量服务报表**：内容包括 L7 访问流量、L7 访问带宽、L7 访问请求数等相关数据。 • **域名业务安全加速服务报表**：内容包括 L7 访问流量、L7 访问带宽、L7 访问请求数、L7 防护命中次数、L3/4 DDoS 攻击防护带宽等相关数据。 • **TCP/UDP 应用安全加速服务报表**：内容包括 L4 访问流量、L4 访问带宽、L4 并发连接数、L3/4 DDoS 攻击防护带宽等相关数据。

场景示例

示例一：定期发送服务报表以监控业务性能

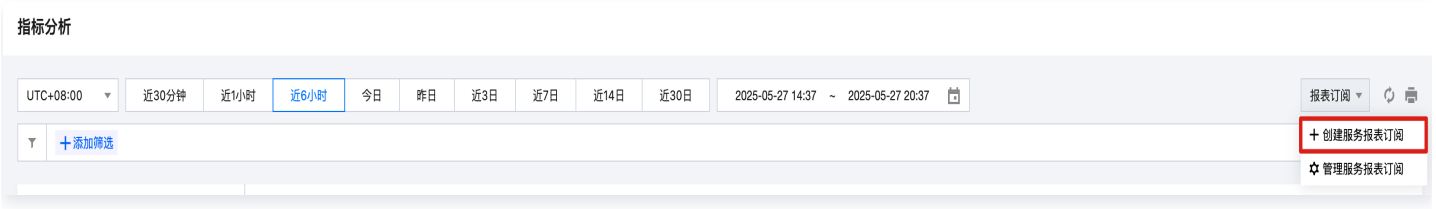
场景描述

一家大型电商客户需要定期监控其网站在全球不同区域的性能，包括访问流量、带宽、请求数和状态码分布等关键指标。为了确保业务连续性和优化用户体验，该客户希望通过电子邮件每天接收包含这些关键指标的服务报表。

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. 点击右上角**报表订阅 > 创建服务报表订阅**。



3. 在创建服务报表订阅页面中，完成相关配置，其中发送频率选择**每天**。其他配置请参考 配置项目说明 。
4. 单击**创建**保存配置，系统将根据配置于第二天开始自动发送报表邮件。
5. 如需修改报表订阅任务配置，可在**指标分析 > 报表订阅 > 管理服务报表订阅**中选择相应任务进行编辑。

示例二：通过即时发送报表邮件来留存历史时间的数据服务报表

场景描述

某公司需要留存历史时间的数据服务报表，例如过去三个月的月度报表，以便进行内部审计和业务回顾。用户可通过立即发送服务报表以满足该项需求。

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. 点击右上角**报表订阅 > 创建服务报表订阅**。
3. 在创建服务报表订阅页面中，完成相关配置，其中发送频率选择**立即发送**。其他配置请参考 配置项目说明 。
4. 数据时间范围选择某个完整的历史月份，例如4月1日00:00-4月30日23:59。

5. 单击**创建**保存配置，系统将根据配置立即生成并发送报表邮件。
6. 如需修改报表订阅任务配置，可在**指标分析 > 报表订阅 > 管理服务报表订阅**中选择相应任务进行编辑。

相关参考
如何使用筛选条件

最近更新时间：2025-04-22 15:10:42

EdgeOne 数据分析支持的筛选条件分为两种类型：

1. 时间筛选条件（必选）：查看所选的时间范围内的数据，详情请参见 如何修改查询时间范围 。
2. 其他筛选条件：根据每个页面支持的筛选项，自定义筛选需要的数据。下文针对这部分详细说明。

支持的运算符

运算符	说明
等于	查询筛选项等于任一指定值的数据
不等于	查询筛选项不等于任一指定值的数据
包含	查询 URL、Referer、资源类型等字段包含指定字符串的数据（例如：查询 `URL 包含/example` 数据）
不包含	查询 URL、Referer、资源类型等字段不包含指定字符串的数据（例如：查询 `URL 不包含/example` 的数据）
开始于	查询 URL、Referer、资源类型等字段的前缀匹配指定字符串的数据
不开始于	查询 URL、Referer、资源类型等字段的前缀不匹配指定字符串的数据
结尾是	查询 URL、Referer、资源类型等字段的后缀匹配指定字符串的数据
结尾不是	查询 URL、Referer、资源类型等字段的后缀不匹配指定字符串的数据

多个筛选条件之间的关系

多个筛选条件之间的关系为“且”关系，同一个筛选条件内的多个取值之间的关系为“或”关系。
例如：同时添加筛选条件 `国家/地区=新加坡;泰国` 和 `状态码=404` ，意味着查询满足**来自新加坡或泰国客户端的访问且边缘响应状态码为 404** 的数据。

支持筛选项

指标分析

- **站点：** EdgeOne 站点。
- **Host：** 客户端请求的 host。
- **国家/地区：** 客户端请求来源的国家或地区。

- **状态码：**EdgeOne 响应客户端的状态码。
- **HTTP 协议版本：**客户端请求使用的 HTTP 版本，取值有：
  - HTTP/1.0
  - HTTP/1.1
  - HTTP/2.0
  - HTTP/3.0（QUIC 协议）
  - WebSocket Over HTTP/1.1（由 HTTP/1.1 发起的 WebSocket 协议）
- **运营商：**客户端请求来源的运营商，仅支持中国大陆可用区站点数据。
- **省份：**客户端请求来源的省份，仅支持中国大陆可用区站点数据。
- **TLS 版本：**客户端请求使用的 TLS 协议版本。取值有：
  - TLS 1.0
  - TLS 1.1
  - TLS 1.2
  - TLS 1.3
- **URL Path：**客户端请求的 URL 路径（path），支持输入多个值，不同值使用半角分号进行分隔。例如：`/example1;/example2`
- **Referer：**客户端请求的 Referer 头部值，支持输入多个值，不同值使用半角分号进行分隔。
- **资源类型：**客户端请求的资源类型，支持输入多个值，不同值使用半角分号进行分隔。例如：`.txt;.jpg`
- **设备类型：**客户端请求的设备类型，由 HTTP 请求头中的 User-Agent 解析得出。取值有：
  - TV：电视
  - Tablet：平板电脑
  - Mobile：手机
  - Desktop：电脑
  - Other：其他
  - Empty：空
- **浏览器类型：**客户端请求使用的浏览器类型。取值有：
  - Firefox
  - Chrome
  - Safari
  - Opera
  - QQBrowser
  - LBBrowser
  - MaxthonBrowser
  - SouGouBrowser

- BIDUBrowser
- TaoBrowser
- UBrowser
- IE
- Microsoft Edge
- Bot
- Empty
- Other

- **系统类型：**客户端请求使用的操作系统类型。取值有：
  - Empty
  - Android
  - IOS
  - MacOS
  - Linux
  - Windows
  - ChromiumOS
  - NetBSD
  - Bot
  - Other
- **IP 版本：**客户端请求使用的 IP 地址版本，取值有：
  - IPv4
  - IPv6
- **HTTP/HTTPS：**客户端请求使用的 HTTP 协议类型，取值有：
  - HTTP
  - HTTPS
- **缓存状态：**客户端请求的缓存状态，取值有：
  - hit：请求命中 EdgeOne 节点缓存，资源由节点缓存提供。资源部分命中缓存也会记录为 hit。
  - miss：请求未命中 EdgeOne 节点缓存，资源由源站提供。
  - dynamic：请求的资源无法缓存/未配置被节点缓存，资源由源站提供。
  - other：无法被识别的缓存状态。边缘函数响应的请求会记录为 other。
- **客户端 IP：**仅查看来自指定客户端 IP 的请求数据。运算符为等于/不等于时，支持输入多个值，不同值使用回车进行分隔。
- **User-Agent：**客户端请求的 User-Agent 头部值。支持输入多个值，不同值使用回车进行分隔。
- **四层代理转发规则：**四层代理实例具体的转发规则。

- **四层代理实例：**四层代理实例名称。
- **DNS 返回码：**DNS 解析应答状态码。取值有：
  - NOError：无错误，成功响应。
  - NXDomain：不存在的记录。
  - NotImp：未实现，DNS 服务器不支持所请求的查询类型；已实现的请求查询类型参考 记录类型 。
  - Refused：拒绝，DNS 服务器由于策略拒绝执行指定的操作。
- **DNS 记录：**DNS 记录类型，取值请参考 记录类型 。
- **DNS 地区：**客户端请求来源的大洲，目前支持如下选项：
  - 亚洲
  - 欧洲
  - 非洲
  - 大洋洲
  - 美洲
- **请求处置结果：**仅查看命中安全规则并按指定方式处置的请求（不包括放行或例外规则）。取值有：
  - 观察
- **规则 ID：**仅查看命中指定 Web 防护规则 ID的请求数据。
- **DDoS 防护实例：**查看指定企业版 DDoS 防护实例的数据。
- **EdgeOne Shield 空间：**查看指定 EdgeOne Shield 空间的数据。
- **内容标识符：**查看指定内容标识符的数据。仅支持 L7 访问相关指标数据。内容标识符功能在内测中，如需使用请 联系我们 。
- **边缘函数名称：**查看指定边缘函数实例的数据。仅支持边缘函数相关指标数据。
- **边缘函数执行结果：**查看指定边缘函数执行结果的数据。仅支持边缘函数相关指标数据。

> **说明：**
> - 当指标选择“L7 访问相关指标”“L7 回源相关指标”“缓存命中率”时，不支持“四层代理转发规则”“四层代理实例”“DNS 返回码”“DNS 记录”“DNS 地区”“请求处置结果”“规则 ID”“DDoS 防护实例”“EdgeOne Shield 空间”筛选项。
> - 当指标选择“L7 防护命中次数”时，仅支持“Host”“请求处置结果”“规则 ID”“客户端 IP”筛选项。

Web 安全分析

支持的根据请求特征、规则特征以及各详细的 Web 防护规则和 Bot 管理策略特征来进行筛选，具体筛选项说明如下：

- **站点：**EdgeOne 站点。
- **客户端 IP：**仅查看来自指定客户端 IP 的请求数据，支持输入多个值，不同值使用回车进行分隔。

- **客户端 IP 地区：**客户端 IP 来源于指定国家或地区。
- **客户端 IP（优先匹配 XFF 头部）：**仅查看来自指定客户端 IP（优先匹配 XFF 头部）的请求数据，支持输入多个值，不同值使用回车进行分隔。
- **客户端 IP 地区（优先匹配 XFF 头部）：**客户端 IP（优先匹配 XFF 头部）来源于指定国家或地区。
- **User-Agent：**客户端请求中携带的 User-Agent 头部信息，支持输入多个值，不同值使用回车进行分隔。
- **请求 URL：**客户端请求的 URL（不包括 Host，仅包含请求路径和查询参数），支持输入多个值，不同值使用回车进行分隔。
- **域名 host：**客户端请求的 Host，支持输入多个值，不同值使用回车进行分隔。
- **来源 Referer：**客户端请求携带的 Referer，支持输入多个值，不同值使用回车进行分隔。
- **处置结果：**Web 防护模块对于请求的最终处置结果，详细说明请参考**处置方式**。处置结果“未知”代表没有执行任何其他已经定义的处置方式，仅用作数据统计过程中的兜底归类，日常分析中可忽略该选项。
- **请求路径（Path）：**客户端请求的 URL Path（HTTP 请求路径，不包括 Host 和查询参数）。支持填入多个值，不同值使用回车进行分隔。
- **请求 JA3 指纹：**根据客户端请求 TLS 握手时相关参数计算得出的 JA3 指纹。仅支持开启 **Bot 管理**的域名数据。
- **请求方式（Method）：**客户端请求的 HTTP Method。
- **请求 ID：**用于唯一标识请求，即默认拦截页面的 `Request ID`、**自定义响应页面**的 `{{ EO_REQ_ID }}`、**EdgeOne 默认响应头部**中的 `EO-LOG-UUID`、**七层访问日志**中的 `RequestID`。
- **规则类别：**仅查看命中指定类别 Web 防护规则的请求数据。
- **规则 ID：**仅查看命中指定 Web 防护规则 ID 的请求数据。

如何修改查询时间范围

最近更新时间：2024-07-30 16:32:11

EdgeOne 数据分析页面支持用户自定义筛选时间范围，下文主要介绍筛选时间范围的两种方式。

说明：

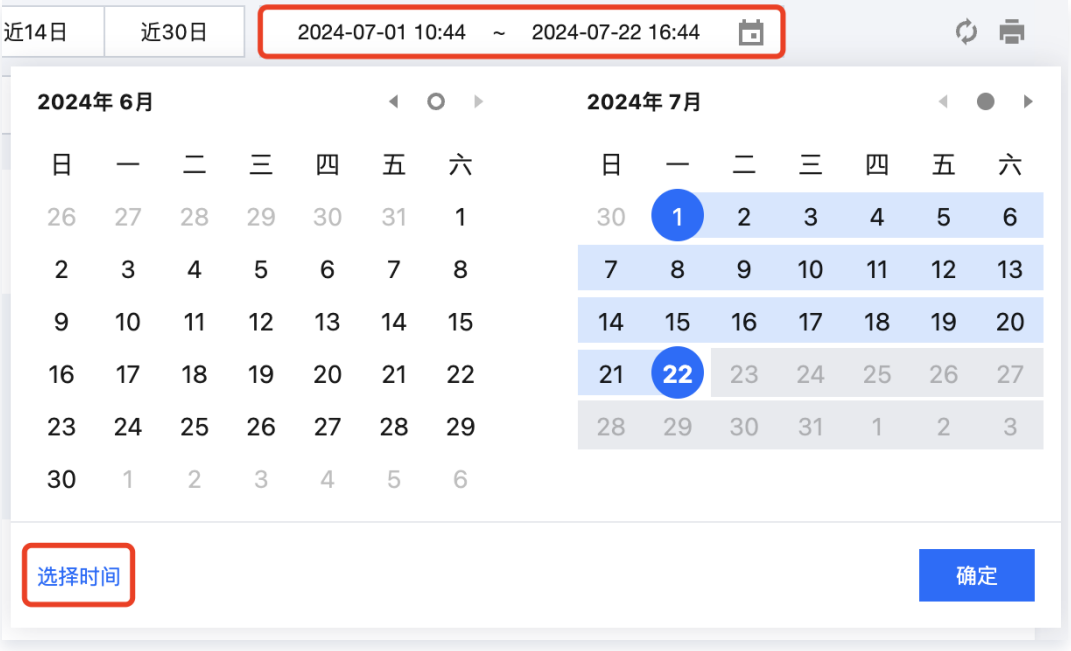
为了提升查询效率，不同时间范围的数据颗粒度如下：

- 时间范围 ≤ 2 小时：1 分钟。
- 2 小时 < 时间范围 ≤ 48 小时：5 分钟。
- 48 小时 < 时间范围 ≤ 7 天：1 小时。
- 时间范围 > 7 天：1 天。

方式 1：通过筛选栏设置查询时间范围

- 快速查询：通过单击**近 30 分钟**、**近 1 小时**、**近 6 小时**、**今日**、**昨日**、**近 3 日**、**近 7 日**等按钮快速查询对应的时间范围数据。

- 自定义查询：您也可以通过选择具体的日期和时间范围，查询自定义时间范围内的数据。



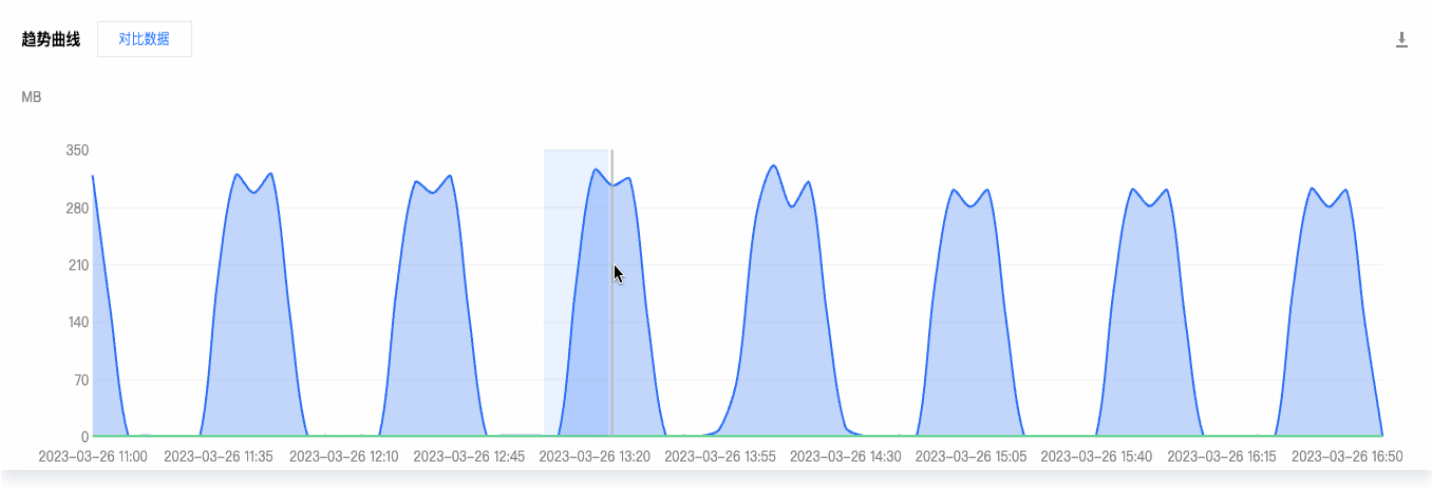
说明：

- 当您选择“近 30 分钟”“近 1 小时”“近 6 小时”“今日”时，页面会显示最近 30 分钟、1 小时、6 小时、当日（从 00:00 开始）的数据，并以每 5 分钟的频率刷新。

- 单次查询的最大时间范围为 31 天。
- 由于套餐版本不同，支持的可查询最大时间跨度不同，详情请见 套餐选型对比 。

方式 2：在时间趋势图上选择查询时间范围

若您想查看曲线上特定的时间段，如下图所示，可以通过鼠标在曲线上点击滑动选取曲线的特定区域。该区域所对应的时间范围将会回填至顶部筛选栏，并影响页面中其他数据统计。



如何导出统计数据与报告

最近更新时间：2024-07-30 16:32:11

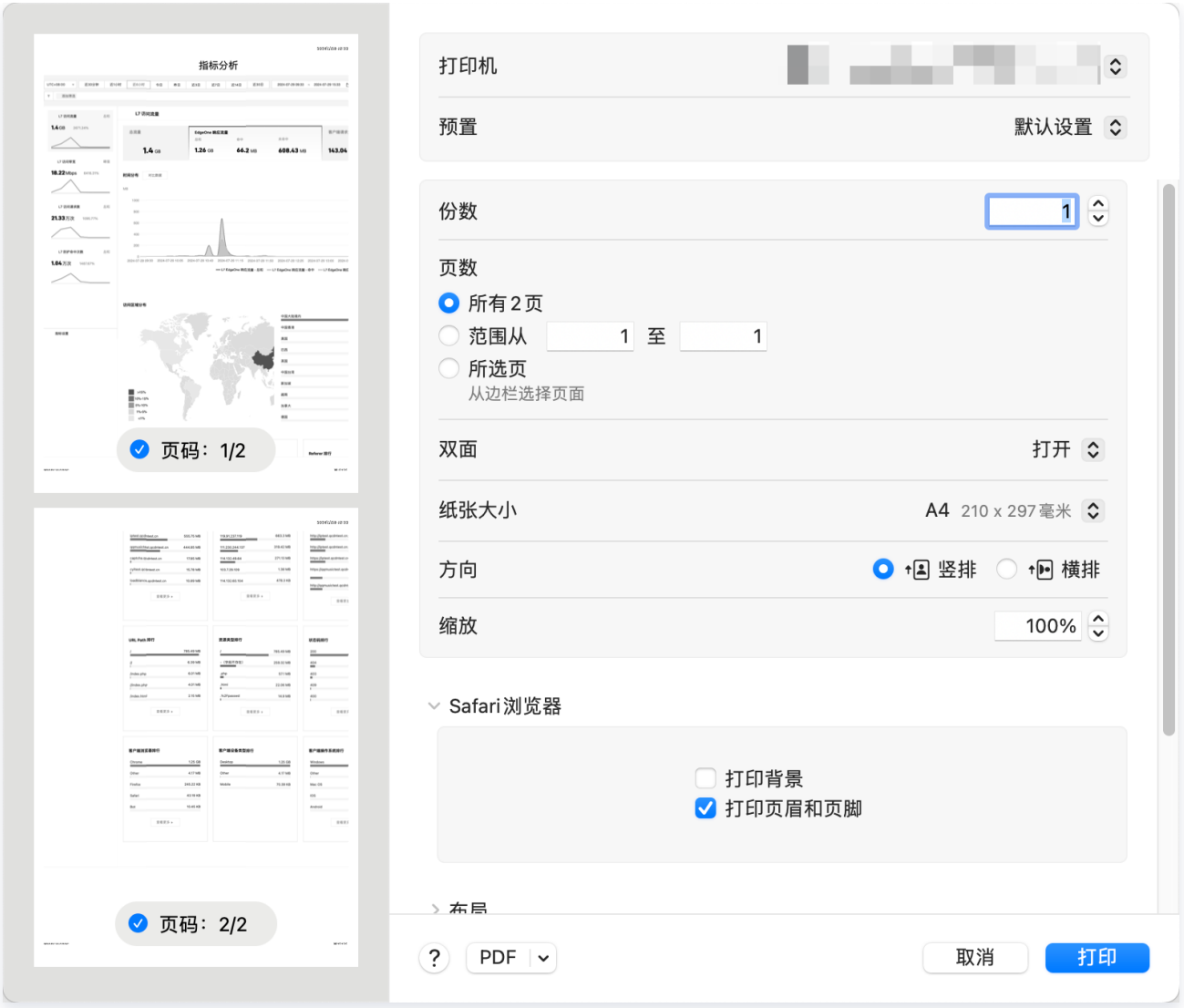
本文档介绍了 EdgeOne 数据分析页面如何导出统计数据和报告，具体操作步骤如下。

导出统计数据

1. 登录 边缘安全加速平台 EO 控制台，进入**指标分析**或 **Web 安全分析**页面。
2. 单击  即可下载相应统计数据表，文件格式为 .csv，当前页面上的筛选条件将会应用到导出数据上。

导出报告

1. 登录 边缘安全加速平台 EO 控制台，进入**指标分析**或 **Web 安全分析**页面。
2. 单击筛选栏右上角的  ，EdgeOne 将会唤起浏览器的打印窗口，您可选择打印或另存为 PDF 报告。当前页面上的筛选条件将会同步打印在报告中。


指标分析
页码：1/2
页码：2/2
打印机
预置
默认设置
份数
1
页数
所有 2 页
范围从
1
至
1
所选页
从边栏选择页面
双面
打开
纸张大小
A4 210 x 297 毫米
方向
竖排
横排
缩放
100%
Safari 浏览器
打印背景
打印页眉和页脚
布局
PDF
取消
打印

抽样数据统计

最近更新时间：2024-12-18 17:26:32

EdgeOne 数据分析模块通过深入分析 EdgeOne 产品持续记录的海量日志数据，帮助用户分析流量特征。为了优化用户体验，EdgeOne 数据分析中引入了抽样数据统计技术，以确保即使在处理大量数据时，也能保持查询的准确性和及时性。

什么是抽样数据统计

数据分析中，抽样是指从全部数据中选取一个代表性的子集进行分析，以便从中提取有价值的信息。例如，进行社会调查时，研究者无法对每个人进行调查，因此他们会挑选一部分人群作为代表样本，用这些样本的回答来反映整个人群的倾向。

什么时候 EdgeOne 会应用抽样数据统计

EdgeOne 运用动态抽样技术来适应不同用户的日志数据量级，确保数据分析的准确性和效率。在以下数据查询场景中，EdgeOne 相关页面所展示的数据可能会经过抽样处理。

- 在 指标分析页面 查询 L7 访问相关指标，且添加如下筛选条件时：状态码、运营商、省份、TLS 版本、URL Path、Referer、资源类型、设备类型、浏览器类型、系统类型、IP 版本、客户端 IP、User-Agent。这是因为当用户在查询整体流量时，我们会为用户提供提前聚合好的统计表，帮助用户快速得到精确的统计结果。但是当用户需要按照某些特定维度进行下钻分析时，查询就会切换到体量庞大的多维统计表，此时便需要通过抽样机制来减少底层数据扫描量，为用户提供快速的查询体验。
- 在 指标分析页面 查询 L7 防护相关指标或在 Web 安全分析页面 进行**统计分析**或查看**样本日志**时，如果查询的时间范围内发生了大规模的 CC 攻击，您看到的数据也可能是抽样结果。在这种情况下，可能会存在无法检索到特定请求 ID 对应日志的情况。

> **说明：**
> 请注意，EdgeOne 会根据平台日志数据的规模和用户的实际需求，不断优化和调整抽样策略。如果您对 EdgeOne 提供的数据分析查询结果有任何疑问，欢迎随时 联系我们 的支持团队。

对使用 EdgeOne 是否有影响

抽样统计技术仅应用于数据分析模块，不会对站点加速、四层代理或安全防护等其他服务配置产生任何影响。通过抽样数据统计技术，EdgeOne 能够更快速地为您提供统计分析结果，协助您在页面内能够获得查询结果的同时提升查询效率。这确保了即使面对海量数据，EdgeOne 也能保持查询的响应速度和准确性。

如何查询全量数据

如果您的业务需求需要对全量日志数据进行深入分析，我们推荐您使用 EdgeOne 的 实时日志推送 功能。实时日志推送可以将详尽的完整日志数据转存到您指定的日志分析系统中（如腾讯云 CLS、第三方日志解决方案或自建的

ELK 栈），您可以通过获取全量数据来进行精细的数据处理。通过实时日志功能，您可以确保在需要更高数据精度的场景中，获得更加准确的数据分析结果，从而为您的业务决策提供更加准确的数据支持。

了解更多

抽样数据统计的工作原理

抽样策略

EdgeOne 采用动态分级策略。该策略会周期性分析您的域名请求量级与对应的查询性能，来判定您的域名是否符合抽样条件。当抽样系统判定您的域名符合抽样条件时，会根据判定周期内的请求量级大小从 10%、1%、0.1%、0.01% 这 4 种抽样比例为您选取合适的抽样等级，各抽样比例的触发规则如下：

- 10%：日均请求量级达 1000 万次以上；
- 1%：日均请求量级达 1 亿次以上；
- 0.1%：日均请求量级达 10 亿次以上；
- 0.01%：日均请求量级达 100 亿次以上。

在触发抽样后，您的抽样等级并非是一成不变的。若您的域名请求量级持续上升，EdgeOne 会相应地升级您的抽样等级，采取更低的抽样比例；若您的域名请求量级持续下降，EdgeOne 会相应地下降您的抽样等级，采取更高的抽样比例，甚至为您取消抽样机制。

数据代表性

EdgeOne 会为您的每条请求日志提供唯一标识（Request ID），抽样系统会基于该唯一标识对您的数据进行抽样分析，以保证抽样因子的随机性。经过我们的测试，当您需要分析的特征在整体数据中占比较高时，采用抽样分析可以为您提供快速且准确的结果。但我们也需要指出，当您需要分析的特征在整体数据中占比较小时，由于样本数较少，抽样分析的结果可能会偏大或偏小。
举例说明，您有量级为 10000 的数据集，该数据集包含 3 个 URL Path A、B、C，其数量分布分别为 7000(70%)、2900(29%)、100(1%)，在最理想的情况下，经过 10% 的抽样后，URL Path A、B、C 的样本数分别为 700、290、10，其中，由于 URL C 对应的样本数太少，基于样本估算总体的准确性将大幅降低，此时您对 URL C 进行下钻分析时的结果可能不符合预期。

告警服务
自定义统计指标

最近更新时间：2025-06-26 11:21:23

功能简介

自定义统计指标功能支持用户通过灵活的配置方式满足个性化的业务监控需求。通过这一功能，用户能够精确定制并追踪网站或 API 的关键流量与性能指标，从而获得深入的业务洞察。EdgeOne 将用户定义的统计指标推送至 腾讯云可观测平台，并允许用户基于这些指标构建定制化的告警策略（例如，监控来自特定国家地区的访问流量），以便用户实时监控业务状态，及时发现并响应潜在问题，确保业务的连续性和稳定性。

使用限制说明

支持的指标范围

目前支持的基础指标如下：

- L7 访问流量
  - 总流量
  - EdgeOne 响应流量
  - 客户端请求流量
- L7 访问带宽
  - 总带宽
  - EdgeOne 响应带宽
  - 客户端请求带宽
- L7 访问请求数

> **说明：**
> 1. 各基础指标的含义请参见 指标分析 。
> 2. 支持的筛选条件参见 如何使用筛选条件 。

数据上报时延说明

在 EdgeOne 服务中，数据的收集与处理是一个涉及多个环节的复杂过程。具体来说，EdgeOne 会从遍布全球的各个节点实时搜集日志信息。随后，系统会根据用户在自定义统计指标功能中设定的特定过滤条件，对这些数据进行细致的处理。处理完成的数据将被推送至腾讯云可观测平台，以便用户能够进行进一步的分析和监控。由于这一流程涵盖了数据的收集、处理和传输等多个步骤，因此存在一定的数据处理时延。**目前，从数据收集到最终在可观测平台显示，整个过程的延迟大约为10分钟。这意味着，当告警策略被触发时，告警通知的推送可能会在实际触发事件之后10 – 12分钟送达。**

这种时延对于大多数监控场景来说是可接受的，因为它不会显著影响用户对流量趋势的把握和对异常情况的响应。然而，对于需要极短时间内响应的紧急情况，用户可能需要考虑这种时延并相应地调整告警策略，以确保能够及时采取必要的应对措施。

套餐支持差异

自定义统计指标功能仅在试用版、标准版和企业版中可用。对于试用版而言，配额限制为10个。完整套餐支持差异请参见 套餐选型对比 。

功能	个人版	基础版	标准版	企业版
自定义统计指标	不支持		100个/站点	100个/站点

场景示例

示例一：监控特定国家地区的访问流量

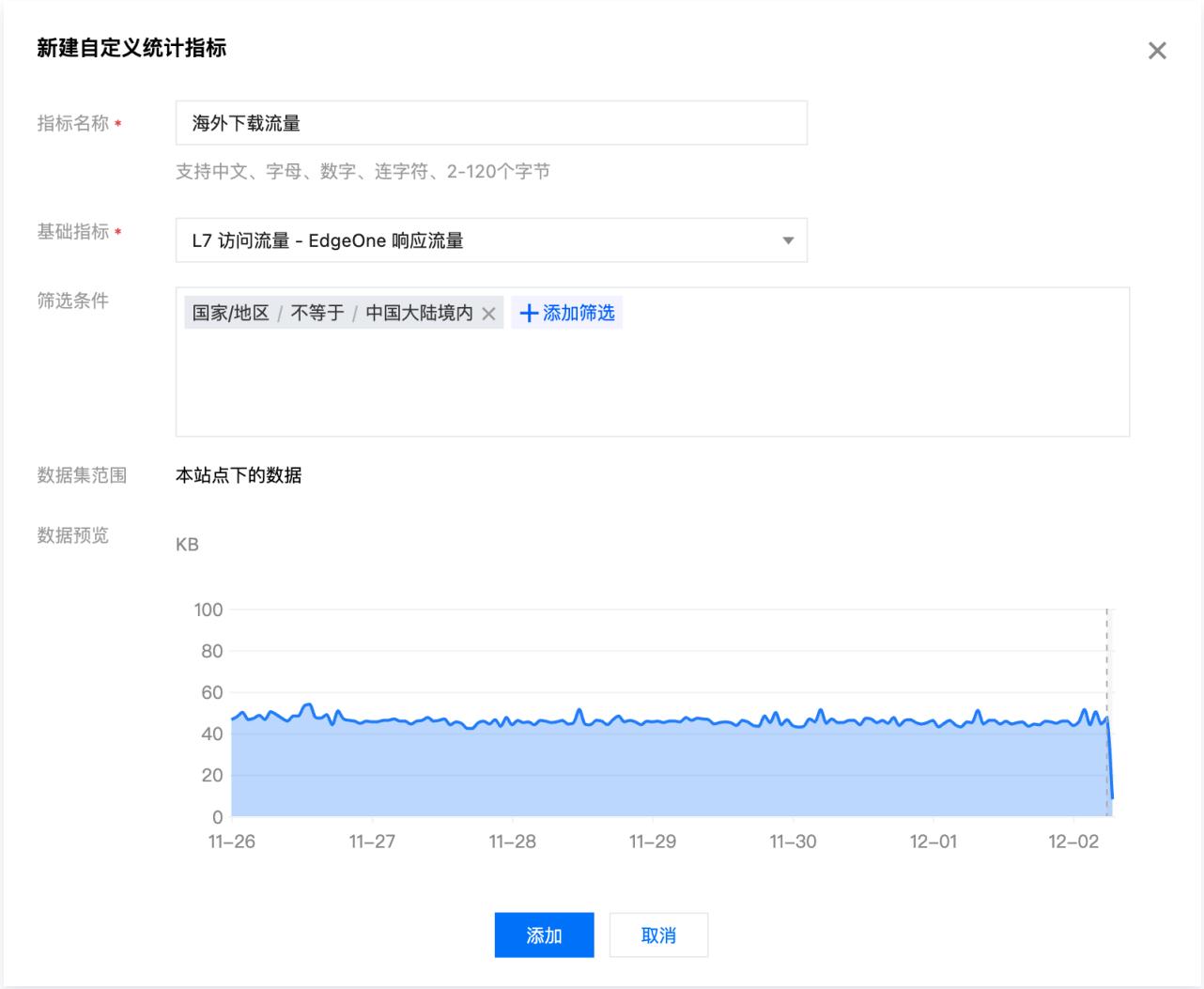
场景描述

在全球化的商业环境中，针对特定国家或地区的流量进行监控并配置告警对于企业至关重要。这不仅涉及到对市场动态的快速响应，还包括对服务质量的持续保障。通过自定义统计指标功能，用户能够实现对关键地区流量的细致监控，并基于这些数据设置告警机制，以便在流量异常时迅速采取行动。

操作步骤

步骤1：创建 EdgeOne 自定义统计指标

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**告警服务** > **自定义统计指标**。
3. 在自定义统计指标页面，单击**新建自定义统计指标**。
4. 在弹出的窗口中，填写指标名称，支持输入中文、字母、数字、连字符，2 - 120字节。
5. 选择基础指标为**“L7 访问流量 - EdgeOne 响应流量”**。
6. 设置筛选条件，指定国家/地区，例如**“国家/地区不等于中国大陆境内”**。数据预览区域将会根据用户配置的基础指标和筛选条件展示近7天的数据。
7. 单击**添加**保存配置，系统将开始收集上述条件下的访问数据，并开始推送至腾讯云可观测平台。



步骤2：创建告警策略

1. 创建自定义统计指标后，在自定义统计指标列表操作列，单击**配置告警策略**。弹出的新页面将跳转至腾讯云可观测平台-告警管理-告警配置-新建策略，并自动选中相应 EO 自定义统计指标作为告警对象。
2. 填写**告警策略名称**。
3. 根据实际业务需求，配置 告警触发条件 。
4. 单击**下一步：配置告警通知**。
   4.1 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，可参见 新建通知模板 。
   4.2 选择所需通知模板后，单击**完成**，保存配置。

示例二：排除特定 User-Agent 对于监控告警的影响

场景描述

在监控网站流量时，有时需要排除某些特定 User-Agent 的访问，如爬虫或测试工具，以避免这些访问影响正常的业务分析和告警触发。通过自定义统计指标，您可以创建排除特定 User-Agent 的监控指标并配置相应告警策略。

操作步骤

步骤1：创建 EdgeOne 自定义统计指标

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**告警服务** > **自定义统计指标**。
3. 在自定义统计指标页面，单击**新建自定义统计指标**。
4. 在弹出的窗口中，填写指标名称，支持输入中文、字母、数字、连字符，2 - 120字节。
5. 选择基础指标为“**L7 访问请求数**”。
6. 设置筛选条件，例如“**User-Agent 不等于** `tget` ”且“**状态码等于** `4xx` ”。数据预览区域将会根据用户配置的基础指标和筛选条件展示近7天的数据。
7. 单击**添加**保存配置，系统将开始收集上述条件下的访问数据，并开始推送至腾讯云可观测平台。

步骤2：创建告警策略

1. 创建自定义统计指标后，在自定义统计指标列表操作列，单击**配置告警策略**。弹出的新页面将跳转至**腾讯云可观测平台** > **告警管理** > **告警配置** > **新建策略**，并自动选中相应 EO 自定义统计指标作为告警对象。
2. 填写**告警策略名称**。
3. 根据实际业务需求，配置 告警触发条件 。
4. 单击**下一步：配置告警通知**。
   4.1 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，可参见 新建通知模板 。
   4.2 选择所需通知模板后，单击**完成**，保存配置。