```
使用AWS的Cloudfront CDN给你的网站加速
           🕂 😽 🗐 🥒 🊖 人 f 🕒 🕒
Table of Contents [show]
Cloudfront是亚马逊AWS(Amazon Web Services)的CDN服务, 使用这个cloudfront之前我假设你已经使用过cloudflare, 我这里有
一篇关于使用cloudflare的文章:使用CloudFlare免费cdn隐藏服务器ip。
写这篇文章是因为我发现目前网上所有关于cloudfront的文章都写的不清不楚,它的使用跟cloudflare区别很大,我也是踩了好多
坑才搞好,希望给遇到问题的朋友一点帮助!
Cloudfront免费套餐
注册登录aws后, 点击这里, 我们可以看到免费套餐, 个人使用的话, 只要不是下载和老看4k视频, 这个额度是足够的
 1 AMS 免费套餐
2 1TB 的数据传出
3 1000 万次 HTTP 或 HTTPS 请求
4 200 万次 CloudFront 函数调用
5 每个月. 永远免费
原理解析
Cloudflare的模式
你需要在你购买域名的网站(比如可能是阿里云,可能是namesilo,可能是freenom等等)那边把你的域名服务器(英文
NameServer, 一般简称NS)修改为cloudflare的NS服务器, 也就是说, 需要让cloudflare全面接管你的域名, 接管后, 你想要添加
DNS解析(添加A记录), 就需要在cloudflare中添加, 而不是在你购买域名的服务商那边添加, 添加解析时, 把小云朵的开关打开,
就会走cdn, 不打开就不会走cdn。
Cloudfront模式
aws的cloudfront与cloudflare工作模式不同,你无需(也无法)把你的域名交给cloudfront接管,要使用cloudfront做cdn,你需要准备
两个域名:
 • 1、你要套cdn的域名(A域名):假设为"aa.test.com";
 • 2、源域名(B域名):假设为"bb.test.com"。cdn是用于加速用的,你需要告诉cdn你要加速的内容(图片、视频、网站)存放在哪
   台服务器上, 但不能填ip, 只能填域名, 所以你需要解析一个域名到你要加速的服务器上, 这个域名就叫"源域名"。
Cloudfront cdn加速原理: 就是把B域名(bb.test.com)解析到你的服务器上, 然后在cloudfront的"选择源域"中填写B域名, 这样
cloudfront就知道你要加速的服务器是哪个服务器,最后它会自动生成一个"xxx.cloudfront.net"域名作为加速域名,然后你需要把
你的网站域名(即你要套cdn的域名)"aa.test.com"cname到"xxx.cloudfront.net",最终效果就是你访问"aa.test.com"其实是在访
问"xxx.cloudfront.net"(当然这是cname,不是301/302跳转), 而"xxx.cloudfront.net"是cloudfront的域名,它会对应前面B域名所对应
由于cloudfront并不是"接管域名"的方式, 所以它只能代理80(http)和443端口(https,包括grpc也能代理, 因为grpc基于http2), 不像
Cloudflare, 除了80和443, 它还能代理很多端口。
Cloudflare代理的端口请看这里, 下面我也摘抄下来:
   http端口有: 80, 8080, 8880, 2052, 2082,2086, 2095
   https端口有: 443, 2053, 2083, 2087, 2096, 8443
  Cloudflare支持但不做缓存的端口: 2052, 2053, 2082, 2083, 2086, 2087, 2095, 2096, 8880, 8443。
举例说明
假设你现在有如下域名和服务器
 1 A域名:aa.test.com
2 B域名: bb.test.co
  2 B域名: bb.test.com
3 服务器:11.22.33.44
 • 1、假设你想把A域名(aa.test.com)套到cloudflare cdn上,用cdn来加速这个域名;
 • 2、那么你需要先把B域名(bb.test.com)解析到你的服务器(11.22.33.44);
 • 3、然后把B域名(bb.test.com)填到cloudfront的"选择源域"里, 把A域名(aa.test.com)填到"备用域名(CNAME)"里(这一栏与前
   一栏不是挨着,需要往下滚动很多才能看到);
 • 4、然后填好其它选项后, 最终创建好之后, 它会生成一个"xxx.cloudfront.net"格式的域名, 这个域名就是cloudfront给你分配
   的加速域名,比如你之前访问一张图片是这样访问的:aa.test.com/imgs/1.jpg, 而用了cdn之后就是:
   xxx.cloudfront.net/imgs/1.jpg;
 • 5、按第4步的说法,虽然cdn可以加速,可是域名就变了,这是不可接受的,这就要用到前面第3步填的"备用域名"了,其实我
   觉得把它叫"自定义域名"更好一点,你需要添加一条DNS解析(CNAME记录),把你在"备用域名"那一栏填的那个域名
   (aa.test.com)添加一个cname, 对应到cloudfront给你分配的加速域名"xxx.cloudfront.net", 最终的请求的流向为
1 | aa.test.com ====cname===> xxx.cloudfront.net ===> CDN服务器 ===bb.test.com===> 源服务器
cft真的免费吗?
这是我问客服的
   In this case the services "All data transfer out to Origin" this prices are the charges you incur when data is transferred
   to your origin using the Put, Post, Patch, Options and Delete HTTP(s) requests. This process is different to the data
  transfer in free tier, that's why that services charges on demand.
这是我用aws一个月后的费用(我用的流量少, 所以收费少)
AWS Billing Dashboard Info
                                                                        Unhide
Page refresh time: 2022年10月15日星期六 GMT+8 22:52:17
                                                          CNY - Chinese Yuan
                                                                         ▼ ⊚ ×
 AWS summary Info
                             Current MTD balance
                             No data to display
 CNY 0.08
                                                          CNY 0.14 ↓ 100.0%
                              Total number of active AWS accounts
                                                          7
 3
这是我2022年9月份的费用(我用的流量少, 而且有免费部分)
实际操作
Cloudfront网页端操作
从这里点击"创建CloudFront分配"。
然后在下图的"洗择源域"中填写一个"源域名"。注意这个域名不能是你要套cdn的域名。这个域名只是用来告诉cloudfront:"喂 你
要加速的内容是abc.examle.com服务器中,记得给它加速哟",只不过它只能填域名,不能直接填ip. 所以我们需要要解析一个域
名指向这个ip,用域名的方式来告诉cloudfront,告诉它要给哪台服务器的内容加速,这个域名我们叫"源域名",它指向将要被加
速的"源服务器"(就是你的VPS)
  创建分配
    源
    選城
這其MMS夏,或者輸入運的域名。
以
包
遊样遊域
它只是用来告诉 cdn:你要给谁加速,你要缓存谁的数据
    源路径 - 可选 信息
輸入要附加到源请求的源域名的 URL 路径。
    输入源路径
    输入源名称
    添加自定义标头 - 可选
CloudFront 在发送到源的所有请求中都包含此标头。
    添加标头
    启用源护盾 信息
源护盾是一个附加缓存层,可以帮助减少源的负载并帮助保护其可用性。
这些按默认就可以
        - 最低源 SSL 协议 信息
CloudFront 与源一起使用的最低 SSL 协议
         CloudFront 与源

TLSv1.2
        O TLSv1.1
        ○ TLSv1
○ SSLv3
       源路径 - 可选 信息
输入要附加到源请求的源域名的 URL 路径。
       输入源路径
       職入此源的名称。
前面选择源域中填了之后,这一栏自
动跟它一样,我们默认就行,不用改
       添加标头
       启用源护盾 信息
零炉质是一个附加螺存层,可以帮助减少源的负载并帮助保护其可用性。
还是按默认就好,其中"查看器"其实是browser的翻译,本来应该翻译为浏览器的,这aws的翻译也是厉害,不知道为什么会翻译
  CloudFront > 分配 > create
   创建分配
    源
    選輯

选择源域

□ 透样源域

□ 以 透样源域

□ で只是用来告诉でdn: 你要给谁加速,你要缓存谁的数据
    源路径 - 可选 信息
輸入要附加到源请求的源域名的 URL 路径。
    输入源路径
    输入源名称
    添加自定义标头 - 可选
CloudFront 在发送到源的所有请求中都包含此标头。
    添加标头
    启用源护盾 信息
源护盾是一个附加缓存层,可以帮助减少源的负载并帮助保护其可用性。
O GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE
    缓存 HTTP 方法

"哈尔",将会缓存 GET 和 HEAD 方法。
    ○ Yes
    缓存键和源请求
~~=====>以使用缓存策略和源请求策略来控制缓存键和源请求。
    O Cache policy and origin request policy (recommended)
     CachingDisabled Policy with caching disabled 创建策略 亿 查看策略 亿
                                                ▼ C
       选择现有源请求策略或创建新的源请求策略。
                                                ▼ C
      AllViewer
Policy with forward all parameters in viewer requests
       创建策略 🖸 查看策略 🖸
这里都不用填, 默认就好
      源清求策略 - 可选
选择现有源请求策略或创建新的源请求策略。
       AllViewer
                                                ▼ C
      创建策略[2] 查看策略[2]
             大策略或创建一个新的响应标头策略。
                                                ▼ C
     选择购应标头
     创建策略 🖸
     ▶ 其他设置
     函数关联 - 可洗 (6.8)
                的 Edge 函数,以及调用此函数的 CloudFront 事件。
      查看器请求 无关联
                     ▼
      查看器响应
              无关联
       源请求 无关联 ▼
这里"价格与级别",看你的服务器在哪儿,一般来说第一个和第三个都可以,仅北美和欧洲肯定不行,因为你在国内是亚洲,它不
对亚洲加速的话, 你要它来干嘛。这个价格可以不用太在意, 因为你个人使用不超过免费用量是不会收费的。特别注意这里的"备
用域名(CNAME)"一栏要填"你真正要套cdn的域名"(就是你的网站域名,就是你要加速的域名)
      源响应 无关联 ▼
    设置
    使用所有边缘站点(最佳性能)
      仅使用北美洲和欧洲
     ○ 使用北美洲、欧洲、亚洲、中东和非洲
     选择 Web ACL
    - - d - - - e.cf
    滋加项目 这个域名就是你要套cdn的域名
    要添加备用域名列表,请使用批量编辑器。
    自定义 SSL 证书 - 可进
关联来自 AWS Certificate Manager 的证书。证书必须位于美国东部(弗吉尼亚北部)区域(us-east-1)。
这里一定要选择证书,可上传你自己域名的证书,也可在这边直接申请,由于我自己的域名是acme.sh自动获取的letsencrypt证
书,有效期3个月,如果上传这个证书,代表你每三个月就要上传一次,非常麻烦。所以我们直接在这里申请就行,点击"请求证
书"来申请一个证书,点击后它会在另一个标签中打开新页面,这个证书不需要我们源域名(bb.test.com)或网站域名(bb.test.com)
的证书,就是说这个证书归这个证书,你自己服务器那边用acme.sh申请的证书之前不套cdn的时候怎么申请,现在套了,你还是
跟以前的方法一样申请就行,也就是说你acme.sh申请的域名证书跟套不套cdn是无关的
                  anager 的证书,证书必须位于美国东部(弗吉尼亚北部)区域(us-east-1),

▼

C
     自定义 SSL 证书 - 可选
      选择证书
     支持的 HTTP 版本
添加对其他 HTTP 版本的支持。默认情况下,支持 HTTP/1.0 和 HTTP/1.1。
     默认根对象 - 可选
当查看器请求根 URL (/)而不是特定对象时返回的对象(文件名)。
     标准日志记录
            azon S3 存储桶的查看器请求的日志。
     ○ 关闭
     〇 关闭
     说明 – 可选
以下页面是在新标签中打开的, 其中"完全限定域名", 其实就是填"你要获取证书的域名", 如果你要申请单域名证书, 那就填你要
套cdn的那个域名, 比如"aa.test.com", 当然你也可以填写"*.test.com"表示获取"test.com"的通配符证书, 这样无论
是"aa.test.com"还是"bb.test.com"都以用,我是强烈建议填通配符证书,因为如果你还要添加要套cdn的域名,是可以选择同一个
  AWS Certificate Manager > 证书 > 请求证书 > 请求公有证书
  请求公有证书
   域名
   完全限定域名 個惠

这里填写你要套 cdn 的那个域名或通配符域名
比如"aa.test.com"或 "test.com"
   为此证书游加另一个名称
您可以向此证书添加其他名称、例如,如果要请求"www.example.com"的证书,您可能需要添加名称
    选择验证方法 [48]

    DNS 验证・推荐
如果您已获得投权可以待改证书请求中域的 DNS 配置。请选择此选项。

    电子邮件验证
如果您没有权限或无法获得修改证书请求中域的 DNS 配置的权限,请选择此选项。

    标签 信息
    为此证书添加另一个名称
      选择验证方法 信息
    O DNS 验证 - 推荐

    电子邮件验证
如果您没有权限或无法获得传改证书请求中域的QNS 配置的权限、请选择此选项。

                                 标签值 - 可选
                        Q、输入值
    Q輸入鍵
                                                              删除标签
    添加标签
请求成功, 点击"查看证书"
aws III 服务 Q 搜索服务、功能、
                                                                          查看证书
                                                    ご 訓除 管理到期事件 导入 请求
                                      您的账户中没有证书。
您的账户中没有证书。
在你域名解析网站那边添加一个cname解析,cname解析需要一个"cname名称"和一个"cname值",这两个数据在下图中可以看到
    6a9b9 1 P 2 2 1 L 5cbc
    详細状态 详細状态 此证书请求的状态为"等待验证",需要进一步采取措施来验证和批准证书。 4c77-b624 4 4 4 4 4 4
    Amazon 已颁发
    域 (1)
                                                        在 Route 53 中创建记录 导出为 CSV
              状态
                         续订状态
                                        类型
              ② 等待验证
                                                   _22( 1083a8
    详细信息
    使用中?
                        序列号
                                            请求时间
                                                                续订资格
                                            八月 28, 2022, 00:09:02
(UTC+08:00)
                                                                不符合条件
添加之后,稍微过一会儿你再刷新下图这个页面,"等待验证"会变成"成功"
                                          ❷已颁发
                                          证书颁发时间 八月 28, 2022, 00:11:27 (UTC+08:00)
                                                            在 Route 53 中创建记录 导出为 CSV
 域 (1)
```



当查看器请求根 URL (/)而不是特定对象时返回的对象(文件名)。

标准日志记录 ○ 关闭 〇 打开 IPv6 〇 关闭 ○ 打开

下图都默认就行,或者把http3也选上

❷ xiebruce.cf ☑ 请求证书 ☑

O TLSv1.2_2021 (推荐)

■ ■ ■ ■ ■ f (6a9b989e-41ce-4c77-b624-46a1ea905cbc)

旧式客户端支持 – 按比例分摊的费用为 600 USD/月。大多数客户不需要此支持。

全策略确定 SSL 或 TLS 协议以及 CloudFront 用于与查看器(客户端)进行 HTTPS 连接的特定密码。

自定义 SSL 证书 - 可洗

安全策略

支持的 HTTP 版本

来中转用的域名, 真实使用的时候并不使用它



1 aa.test.com ====cname===> xxx.cloudfront.net ===> CDN服务器 ===bb.test.com===> 源服务器 你可以创建很多"分配"来分别代理到你的不同机器, 这都是可以的。 C 启用 禁用 删除 创建分配 < 1 > ⊚ ▽ 説明 ▽ 域名 ▽ 無用域名 ▽ 源 ▽ 状态 ▽ 上次修改时间 ▼ 如果你想删除一个分配,必须先禁用它,然后等待它生效,当"部署中"变成日期时(不用刷新网页,它会自动变),禁用就生效了,然 后你才能再次选中去删除它, 而且删除后, 如果再去分配, 如果是同一个源域或同一个备用域名, 都是无法直接分配的, 需要等 DNS缓存没了才行, 一般要等一小时以上。

你的网站域名(即要套cdn的那个域名)

安全策略

cloudfront的域名(如果是做代理用的话,用cloudfront分配的域名也没什么,就是可能不容易记住)。

作为名称, 而把cloudfront给你分配的域名作为"目标", 添加之后就可以使用它了。

备用域名

这两个域名都可以用来访问你的网站,只不过备用域名的好处就是自定义,更像是你自己的域名,而自动分配的域名就统一是

如果你想使用自定义域名(即上图的"备用域名"),**你需要在域名解析服务商那边添加一个cname记录,把自己要套cdn的域名**

按照本例的示例域名, aa.test.com就是套了cdn的域名, 你用aa.test.com访问你的网站就是走了cdn的, 而bb.test.com则是一个用

标准日志记录 关闭

默认根对象

server_name aa.test.com bb.test.com; bb.test.com作为源域名,不用说肯定要配置的,不然CDN服务器没法通过这个域名获取到源站的内容,而aa.test.com是cname到 xxx.cloudfront.net, 理论上来说aa.test.com并没有直接参与访问你服务器的内容,为什么它也要在nginx中配置呢? 原因是, 你在浏览器(或其它客户端)发起请求的时候, 用的是aa.test.com, 虽然DNS那边最终会把cname的域名(即 xxx.cloudfront.net)对应的ip返回,但浏览器并不知道这个ip是cname那边的,所以GET请求中header中的Host值还是aa.test.com, 这个请求最终会被CDN服务器转发到你的VPS中,那么VPS中的nginx接收到这个请求,就会根据Host值判断应该用哪个server模

块来处理你的请求(如果你同一个端口有多个模块的话),当然如果同一端口只有一个模块,其实server_name可以不写

另外,server模块中的证书,一般来说用通配符证书都是能匹配上,如果是单独指定多个域名,申请证书时记得把aa.test.com和

Cloudfront会通过443端口和80端口,即https和http协议去请求你的服务器,你必须在你的服务器配置前面所说的"A域名"(套cdn的

域名)和"B域名"(源域名), 如果是nginx, 则server_name应该把aa.test.com和bb.test.com都写上

bb.test.com,因为只有一个它默认就进去了,但建议还是写比较好。

一般报错502都是由于源站域名不包含在证书里(或证书过期)造成的,详见:如何排查来自 CloudFront 的 502:"无法满足请求"错 参考: https://www.banzhuti.com/free-cdn-amazon-cloudfront-setting.html