



Table of Contents [show]

Cloudfront是亚马逊AWS(Amazon Web Services)的CDN服务。使用这个cloudfront之前假设你已经使用过cloudflare。我这里有一篇关于使用cloudflare的文章:使用CloudFlare免费cdn加速网站服务。

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白。它的使用跟cloudflare区别很大。我也试了好多坑才搞懂。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，这个额度是够的

1	AWS 免费套餐
2	1TB 流量额度
3	1000 万次 HTTP 或 HTTPS 请求
4	200 万次 CloudFront 函数调用
5	每个月 永久免费

原理解析

Cloudflare的模式

你需要在你的网站的网站(比如可能是阿里云，可能是namesilo，可能是freedom等)那边把你域名服务器(英文NameServer，一般叫称NS)修改为cloudflare的NS服务器，也就是说，需要让cloudflare来接管你的域名。接管后，你想要添加DNS解析(添加A记录)，就需要在cloudflare中添加，而不是在你网站域名的服务商那边添加。添加解析时，把小云云的开关打开，就会变成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、你要做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)存放在哪个服务器上，但不能填ip，只能填域名，所以你需要解析到一个域名到你想要加速的服务器上，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“源域域”中填写B域名。这样cloudfront就知道你要加速的服务是哪个服务器，最后它会自动生成一个“xxx.cloudfront.net”域名作为加速域名。然后你还需要把你的网站域名(你要加速的域名)“aa.test.com”修改为cloudfront的NS服务器，不能直接填ip，所以我们首先需要解析一个域名“xxx.cloudfront.net”(当然是cname，不是301/302跳转)，而“xxx.cloudfront.net”是cloudfront的域名，它会对应前面B域名所对应的两个网站。

由于cloudfront并不是“接管域名”的方式，所以它只能代理80/tcp和443端口(https,包括grpc也能代理，因为grpc基于tcp)。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端口号: 80, 8080, 8880, 2052, 2082, 2086, 2095  
https端口号: 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, 8443.

举例说明

假设你现有如下域名和服务器

1	A域名 aa.test.com
2	B域名 bb.test.com
3	服务器 13.22.33.44

1、假设你想把A域名(aa.test.com)搬到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)解析到你的服务器上(11.22.33.44)；

3、然后把B域名(bb.test.com)填到cloudfront的“源域域”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，需要往下滑动很多才能看到)；

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/img/1.jpg，而用了cdn之后就是: xxx.cloudfront.net/img/1.jpg；

5、按照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，这就需要用到前面第3步说的“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

aa.test.com ==> CNAME ==> xxx.cloudfront.net ==> CDN服务器 ==> bb.test.com ==> 源服务器

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.

这是说用aws一个月后的费用(我用的流量少，所以收费少)



这是我2022年9月份的费用(我用的流量少，而且有免费部分)

0

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“选择源域”中填写一个“源域名”，注意这个域名不是你要加速cdn的域名，这个域名只是用来告诉cloudfront“嘿，你要加速的内容是abc.example.com服务器中，记得给它加速啊”，只不过它只能填域名，不能填直接ip，所以我们首先需要解析一个域名指向这个ip，用域名的方式告诉告诉cloudfront，告诉它要加速哪台服务器的内容加速，这个域名我们叫“源域名”，它指向你要被加速的“源服务器”(就是你的VPS)

创建分配

源域: 选择 AWS 源，或输入源域名称。  
选择源域: 填写源域名，注意这个不是你最终需要 cdn 的域名，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: 填写源路径，或留空以使用默认的路径 (/)。源路径用于指定源域中的特定文件、目录、或子域。

名称: 输入分配的名称。

添加自定义头 - 可选: CloudFront 允许您在分配的源域中添加自定义头。

应用源策略: 选择: 源策略是一个预定义策略，可以减少源域中的流量并保护其内容。

这些控制数就可以

最低协议: 选择: 选择最低协议，或留空以使用默认协议 (SSL)。最低协议: TLSv1.2, TLSv1.1, TLSv1, SSLv3

源策略 - 可选: 选择: 选择源策略，或留空以使用默认策略 (SSL)。源策略: 选择: 选择源策略，或留空以使用默认策略 (SSL)。

名称: 输入分配的名称。

添加自定义头 - 可选: CloudFront 允许您在分配的源域中添加自定义头。

应用源策略: 选择: 源策略是一个预定义策略，可以减少源域中的流量并保护其内容。

还是控制数就好，其中“查看”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成查看的

创建分配

源域: 选择 AWS 源，或输入源域名称。  
选择源域: 填写源域名，注意这个不是你最终需要 cdn 的域名，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: 填写源路径，或留空以使用默认的路径 (/)。源路径用于指定源域中的特定文件、目录、或子域。

名称: 输入分配的名称。

添加自定义头 - 可选: CloudFront 允许您在分配的源域中添加自定义头。

应用源策略: 选择: 源策略是一个预定义策略，可以减少源域中的流量并保护其内容。

选择源域和所有策略

源域: 选择 AWS 源，或输入源域名称。  
选择源域: 填写源域名，注意这个不是你最终需要 cdn 的域名，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: 填写源路径，或留空以使用默认的路径 (/)。源路径用于指定源域中的特定文件、目录、或子域。

名称: 输入分配的名称。

添加自定义头 - 可选: CloudFront 允许您在分配的源域中添加自定义头。

应用源策略: 选择: 源策略是一个预定义策略，可以减少源域中的流量并保护其内容。

这些都不填，默认就好

源域: 选择 AWS 源，或输入源域名称。  
选择源域: 填写源域名，注意这个不是你最终需要 cdn 的域名，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: 填写源路径，或留空以使用默认的路径 (/)。源路径用于指定源域中的特定文件、目录、或子域。

名称: 输入分配的名称。

添加自定义头 - 可选: CloudFront 允许您在分配的源域中添加自定义头。

应用源策略: 选择: 源策略是一个预定义策略，可以减少源域中的流量并保护其内容。

函数关联 - 可选

选择源域: 选择 AWS 源，或输入源域名称。  
选择源域: 填写源域名，注意这个不是你最终需要 cdn 的域名，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: 填写源路径，或留空以使用默认的路径 (/)。源路径用于指定源域中的特定文件、目录、或子域。

名称: 输入分配的名称。

添加自定义头 - 可选: CloudFront 允许您在分配的源域中添加自定义头。

应用源策略: 选择: 源策略是一个预定义策略，可以减少源域中的流量并保护其内容。

设置

价格计划: 选择: 选择价格计划，或留空以使用默认价格计划 (标准)。价格计划: 选择: 选择价格计划，或留空以使用默认价格计划 (标准)。

源域: 选择 AWS 源，或输入源域名称。  
选择源域: 填写源域名，注意这个不是你最终需要 cdn 的域名，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: 填写源路径，或留空以使用默认的路径 (/)。源路径用于指定源域中的特定文件、目录、或子域。

名称: 输入分配的名称。

添加自定义头 - 可选: CloudFront 允许您在分配的源域中添加自定义头。

应用源策略: 选择: 源策略是一个预定义策略，可以减少源域中的流量并保护其内容。

这“价格”看不懂，看你的服务器在哪儿，一般来说一个标准三个都可以，仅北美和欧洲肯定不行，因为你在国内是亚洲，不对应到亚洲的话，你要它来干嘛。这个价格可以不关注它，因为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)”栏要填“你真正需要加速cdn的域名”(就是你的网站域名，就是你要加速的域名)

源域: 选择 AWS 源，或输入源域名称。  
选择源域: 填写源域名，注意这个不是你最终需要 cdn 的域名，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: 填写源路径，或留空以使用默认的路径 (/)。源路径用于指定源域中的特定文件、目录、或子域。

名称: 输入分配的名称。

添加自定义头 - 可选: CloudFront 允许您在分配的源域中添加自定义头。

应用源策略: 选择: 源策略是一个预定义策略，可以减少源域中的流量并保护其内容。

请求公共证书

源域: 选择 AWS 源，或输入源域名称。  
选择源域: 填写源域名，注意这个不是你最终需要 cdn 的域名，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: 填写源路径，或留空以使用默认的路径 (/)。源路径用于指定源域中的特定文件、目录、或子域。

名称: 输入分配的名称。

添加自定义头 - 可选: CloudFront 允许您在分配的源域中添加自定义头。

应用源策略: 选择: 源策略是一个预定义策略，可以减少源域中的流量并保护其内容。

选择验证方式

源域: 选择 AWS 源，或输入源域名称。  
选择源域: 填写源域名，注意这个不是你最终需要 cdn 的域名，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: 填写源路径，或留空以使用默认的路径 (/)。源路径用于指定源域中的特定文件、目录、或子域。

名称: 输入分配的名称。

添加自定义头 - 可选: CloudFront 允许您在分配的源域中添加自定义头。

应用源策略: 选择: 源策略是一个预定义策略，可以减少源域中的流量并保护其内容。

请求成功，点击“查看证书”

源域: 选择 AWS 源，或输入源域名称。  
选择源域: 填写源域名，注意这个不是你最终需要 cdn 的域名，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: 填写源路径，或留空以使用默认的路径 (/)。源路径用于指定源域中的特定文件、目录、或子域。

名称: 输入分配的名称。

添加自定义头 - 可选: CloudFront 允许您在分配的源域中添加自定义头。

应用源策略: 选择: 源策略是一个预定义策略，可以减少源域中的流量并保护其内容。

在你域名名称解析站边添加一个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

源域: 选择 AWS 源，或输入源域名称。  
选择源域: 填写源域名，注意这个不是你最终需要 cdn 的域名，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: 填写源路径，或留空以使用默认的路径 (/)。源路径用于指定源域中的特定文件、目录、或子域。

名称: 输入分配的名称。

添加自定义头 - 可选: CloudFront 允许您在分配的源域中添加自定义头。

应用源策略: 选择: 源策略是一个预定义策略，可以减少源域中的流量并保护其内容。

添加之后，稍候一会儿你再刷新下图这个页面，“等待验证”会变成“成功”

源域: 选择 AWS 源，或输入源域名称。  
选择源域: 填写源域名，注意这个不是你最终需要 cdn 的域名，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: 填写源路径，或留空以使用默认的路径 (/)。源路径用于指定源域中的特定文件、目录、或子域。

名称: 输入分配的名称。

添加自定义头 - 可选: CloudFront 允许您在分配的源域中添加自定义头。

应用源策略: 选择: 源策略是一个预定义策略，可以减少源域中的流量并保护其内容。

回到之前请求证书的地方，点击右侧的“关联”按钮，然后下拉菜单中就可以选择刚刚请求的证书了

源域: 选择 AWS 源，或输入源域名称。  
选择源域: 填写源域名，注意这个不是你最终需要 cdn 的域名，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: 填写源路径，或留空以使用默认的路径 (/)。源路径用于指定源域中的特定文件、目录、或子域。

名称: 输入分配的名称。

添加自定义头 - 可选: CloudFront 允许您在分配的源域中添加自定义头。

应用源策略: 选择: 源策略是一个预定义策略，可以减少源域中的流量并保护其内容。

下图都默认就行，或者把Cdn也选上

源域: 选择 AWS 源，或输入源域名称。  
选择源域: 填写源域名，注意这个不是你最终需要 cdn 的域名，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: 填写源路径，或留空以使用默认的路径 (/)。源路径用于指定源域中的特定文件、目录、或子域。

名称: 输入分配的名称。

添加自定义头 - 可选: CloudFront 允许您在分配的源域中添加自定义头。

应用源策略: 选择: 源策略是一个预定义策略，可以减少源域中的流量并保护其内容。

如果前面没有证书就点击“创建分配”，它就会报这个错

源域: 选择 AWS 源，或输入源域名称。  
选择源域: 填写源域名，注意这个不是你最终需要 cdn 的域名，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: 填写源路径，或留空以使用默认的路径 (/)。源路径用于指定源域中的特定文件、目录、或子域。

名称: 输入分配的名称。

添加自定义头 - 可选: CloudFront 允许您在分配的源域中添加自定义头。

应用源策略: 选择: 源策略是一个预定义策略，可以减少源域中的流量并保护其内容。

最后点击“创建分配”

源域: 选择 AWS 源，或输入源域名称。  
选择源域: 填写源域名，注意这个不是你最终需要 cdn 的域名，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: 填写源路径，或留空以使用默认的路径 (/)。源路径用于指定源域中的特定文件、目录、或子域。

名称: 输入分配的名称。

添加自定义头 - 可选: CloudFront 允许您在分配的源域中添加自定义头。

应用源策略: 选择: 源策略是一个预定义策略，可以减少源域中的流量并保护其内容。

可以看到已经创建成功，它会给你分配一个“分配域名”，然后下边还会有一个“备用域名”，这时你就会比较明白什么叫备用域名了，因为它已经给你分配了，你直接用它分配的域名就能用，但是用我们自己的域名通过添加cname值，也是可以走cdn加速的。所以叫“备用域名”

源域: 选择 AWS 源，或输入源域名称。  
选择源域: 填写源域名，注意这个不是你最终需要 cdn 的域名，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: 填写源路径，或留空以使用默认的路径 (/)。源路径用于指定源域中的特定文件、目录、或子域。

名称: 输入分配的名称。

添加自定义头 - 可选: CloudFront 允许您在分配的源域中添加自定义头。

应用源策略: 选择: 源策略是一个预定义策略，可以减少源域中的流量并保护其内容。

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，就是可能自己用的域名，而自动分配的域名就是一cloudfront的域名(都是代理使用的，用cloudfront的域名好处也没什么，就是可能不能自己使用)。

源域: 选择 AWS 源，或输入源域名称。  
选择源域: 填写源域名，注意这个不是你最终需要 cdn 的域名，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: 填写源路径，或留空以使用默认的路径 (/)。源路径用于指定源域中的特定文件、目录、或子域。

名称: 输入分配的名称。

添加自定义头 - 可选: CloudFront 允许您在分配的源域中添加自定义头。

应用源策略: 选择: 源策略是一个预定义策略，可以减少源域中的流量并保护其内容。

如果你想使用自定义域名(即上图的“备用域名”)，就需要在域名解析服务商那边添加一个cname记录，把自己要加速的域名作为目标，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。

源域: 选择 AWS 源，或输入源域名称。  
选择源域: 填写源域名，注意这个不是你最终需要 cdn 的域名，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: 填写源路径，或留空以使用默认的路径 (/)。源路径用于指定源域中的特定文件、目录、或子域。

名称: 输入分配的名称。

添加自定义头 - 可选: CloudFront 允许您在分配的源域中添加自定义头。

应用源策略: 选择: 源策略是一个预定义策略，可以减少源域中的流量并保护其内容。

按照本例的示例域名，aa.test.com就是源域，你用aa.test.com访问的网站就是走了cdn的，而bb.test.com则是一个用来中利用的域名，真实使用的时候并不使用它

源域: 选择 AWS 源，或输入源域名称。  
选择源域: 填写源域名，注意这个不是你最终需要 cdn 的域名，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: 填写源路径，或留空以使用默认的路径 (/)。源路径用于指定源域中的特定文件、目录、或子域。

名称: 输入分配的名称。

添加自定义头 - 可选: CloudFront 允许您在分配的源域中添加自定义头。

应用源策略: 选择: 源策略是一个预定义策略，可以减少源域中的流量并保护其内容。

你可以创建很多“分配”来分别代理到不同的服务器，这都是可以的。

源域: 选择 AWS 源，或输入源域名称。  
选择源域: 填写源域名，注意这个不是你最终需要 cdn 的域名，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: 填写源路径，或留空以使用默认的路径 (/)。源路径用于指定源域中的特定文件、目录、或子域。

名称: 输入分配的名称。

添加自定义头 - 可选: CloudFront 允许您在分配的源域中添加自定义头。

应用源策略: 选择: 源策略是一个预定义策略，可以减少源域中的流量并保护其内容。

如果你想要删除一个分配，必须先禁用它，然后等待它生效，当“禁用”变成“完成日期”(不用刷新网页，它会自动)，禁用就生效了，然后你才能再次去它中删除它，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，都是无法直接删除的，需要等DNS缓存没了才行，一般要等一两个小时以上。

源域: 选择 AWS 源，或输入源域名称。  
选择源域: 填写源域名，注意这个不是你最终需要 cdn 的域名，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: 填写源路径，或留空以使用默认的路径 (/)。源路径用于指定源域中的特定文件、目录、或子域。

名称: 输入分配的名称。

添加自定义头 - 可选: CloudFront 允许您在分配的源域中添加自定义头。

应用源策略: 选择: 源策略是一个预定义策略，可以减少源域中的流量并保护其内容。

服务器端操作

Cloudfront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页面前面说的“A域名”(即cdn的域名)和“B域名”(源域名)，如果是nginx，则server\_name应该设aaa.test.com和bbb.test.com都写上

```
server {
    listen 80;
    server_name aa.test.com bb.test.com;
}
```

bb.test.com作为源域名，不用设置需要配置的，不设置CDN服务无法通过这个域名获取到源站的内容，而aaa.test.com是cname到xxx.cloudfront.net，理论上说aaa.test.com并没有直接参与访问你服务器内容的内容，所以它也会在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aaa.test.com，虽然CDN那边最终会拿到cname的域名(即xxx.cloudfront.net)的ip地址，但浏览器并不知道这个ip是aaa.test.com的，所以CDN请求来自header中的Host值还是aaa.test.com，这个请求最终会请求到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判断应该用哪个server块来处理这个请求(如果你同一个端口有多个server块的话)，当然如果同一端口只有一个server块，其实server\_name可以不写bb.test.com，因为只有一个它就不存在了，但建议还是写比较保险。

另外，server模块中的证书，一般来说是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aaa.test.com和bbb.test.com的证书都加上。

一般用letsencrypt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：如何搭建来自 CloudFront 的 502 “无法满足请求”错误？

参考: https://www.banzhul.com/free-cdn-amazon-cloudfront-setting.html