将你的网站解析到1.0.0.1，Cloudflare羊毛薅到底

江风引雨

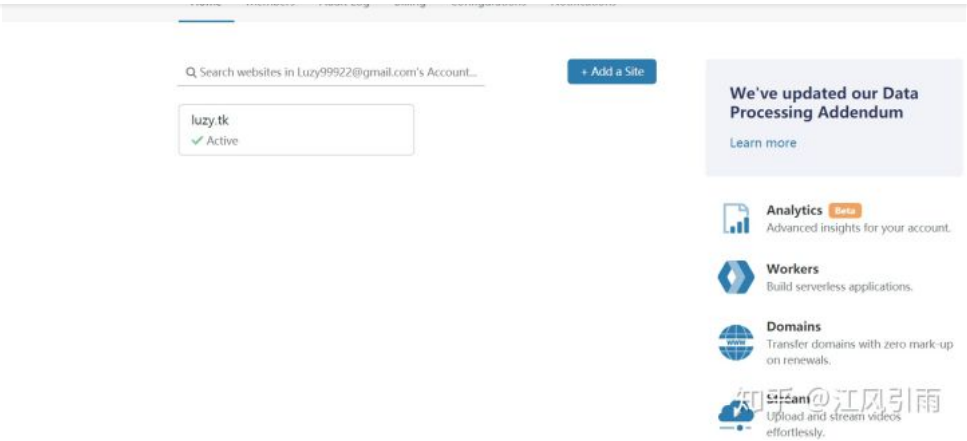
Cloudflare这个域名解析服务商相信很多人一定不陌生，它好像是目前唯一免费提供CDN服务的商家，但由于其cdn服务器多数在国外，在国内的访问速度不佳，甚至起不到加速效果，反而会减速。但通过cdn访问，能是你的服务器匿名性提升不少，也能有效避免DDOS攻击，还能减少服务器流量开支，何乐而不为呢?

那么有没有办法更换DNS服务器地址呢？官网上也确实提供了更改CNAME地址的服务，不过是要收费的。~~作为一个白嫖党怎么可能付钱呢~~ 这两天，我有发现了Cloudflare推出了免费的公共DNS `1.1.1.1` 和 `1.0.0.1` （可真是财大气粗啊，这ip比Google的 `8.8.8.8` 还nb）。

那么下面进入正题，我们有没有办法把域名解析到这个网站上呢？以下就是我的操作步骤：

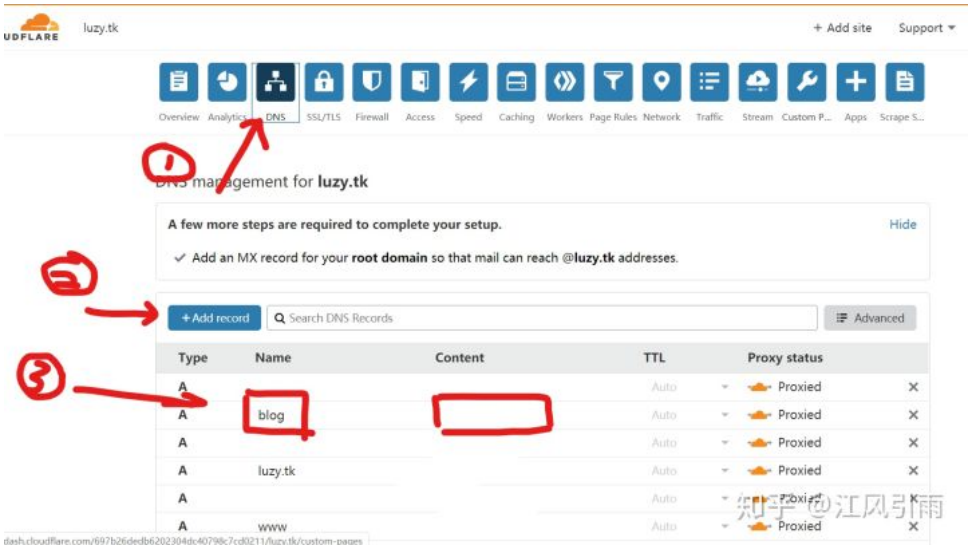
Step 1

当然得先注册Cloudflare账户，点击 `Sign up` 按钮，可以使用邮箱注册，注册完后会让你填写你的二级域名，如本站就是 `luzy.tk` ，可能会让你在原域名商那里验证一下，记不太清了，反正跟着步骤走就行。 显示这样的界面就是注册好了。



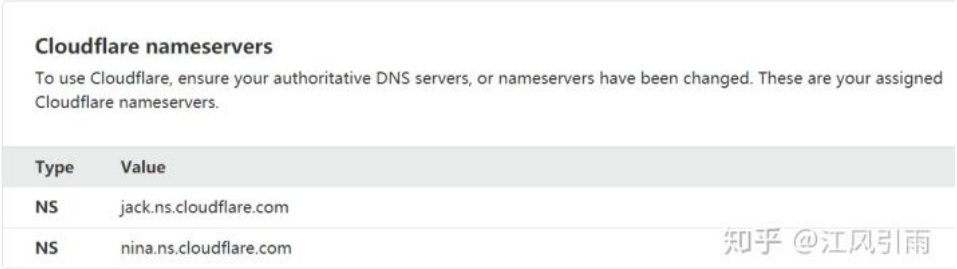
Step 2

点击上图中的你的站点，选择上面DNS菜单，点击 `ADD RECORD` 新增域名解析记录， `Name` 表示域名，只需要填写第三级域名（如下图中 `blog` 即表示 `blog.luzy.tk` ）， `Content` 中填写你的服务器ip。记得再把右边的云朵点亮（灰色表示只使用DNS，橙色表示开启CDN）。



Step 3

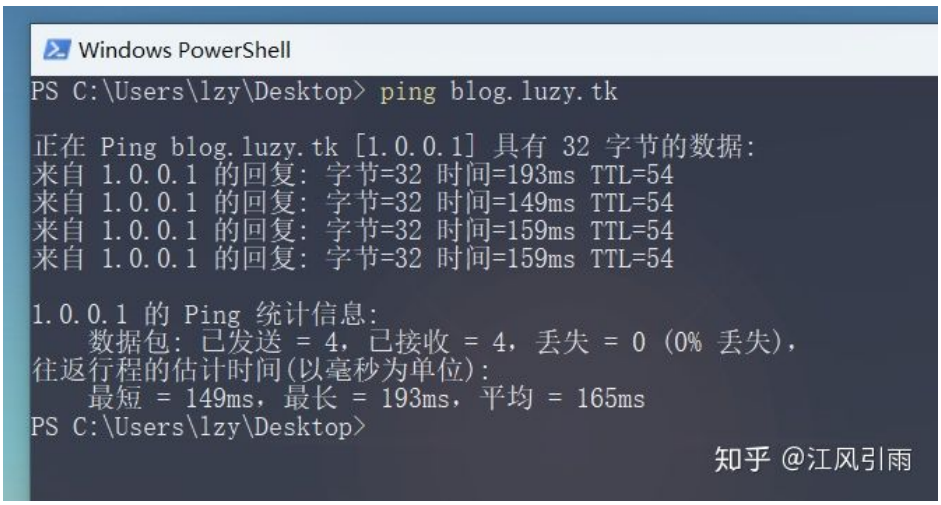
此时，若把下方的 `nameservers` 地址填入你的原始域名服务商上的nameserver地址，就完成了Cloudflare的默认cdn配置。



此时你可以用你的电脑ping一下你的网站域名，会发现它的ip地址变了，不是你原来的地址了。但这不是我们想达到的效果，如果想使其解析到1.0.0.1还需下面的步骤。

Step 4

似，不过要注意的是，**ip地址**那栏，**不要填你的真实ip！ 不要填你的真实ip！ 不要填你的真实ip！ 一律填上 `1.0.0.1` ！**（1.1.1.1被国内各厂商定义为内网网关ip了，用不了，1.0.0.1还是亲测可用的）
至此，就大功告成了！等个十分钟左右，等修改生效，再用你的电脑ping一下。



看，是不是解析成1.0.0.1了呢。😁

> **原理猜测**： **默认cdn的解析路径**： 根据你的顶级和二级域名找到其归属的服务商 -->服务商根据你设置的域名服务器地址，把请求传给Cloudflare -->Cloudflare返回分配的cdn地址 **修改后的解析路径**： 根据你的顶级和二级域名找到其归属的服务商 -->服务商直接把你的域名解析成1.0.0.1返回
> 我们能够如此利用，估计是Cloudflare设置了这两个ip也能作为cdn使用，至于怎么返回真实网站内容的，我也不清楚了。（以上纯属本人个人理解和猜测，如有理解错误请大佬指出 附上对blog.luzy.tk的路由追踪的结果：

序号	IP地址	所在地	耗时(ms)
1	10.59.209.130	本地网络	0ms
2	10.59.243.230	本地网络	0ms
3	--	未知地址	0ms
4	14.18.199.58	广东省广州市 电信IDC机房	2ms
5	--	未知地址	0ms
6	113.96.6.18	广东省广州市 电信	4ms
7	113.96.0.106	广东省广州市 电信	3ms
8	202.97.90.170	中国 中国电信骨干网节点	4ms
9	202.97.91.145	中国 电信骨干网	13ms
10	202.97.98.181	香港 中国电信骨干网接入点	0ms
11	--	未知地址	0ms
12	218.30.54.214	中国电信 美国加利福尼亚州洛杉矶县帕萨迪纳市中国电信美国接入点	172ms
13	1.0.0.1	美国 APNIC&CloudFlare公共DNS服务器	164ms

可以看到，追踪到1.0.0.1就断了，可以说，这招使服务器的安全性提高不少

博客原文链接
blog.luzy.tk

发布于 2020-02-10

CloudFlare CDN DNS 解析

知乎

DNS大全（114DNS 、阿里DNS、百度DNS 、360 DNS...

DNS是什么： DNS是域名系统,Domain Name System的缩写,是一个服务。 DNS就是把域名解析为IP地址，提供我们上网，我们能够上网最终是找到IP地址。比如，http://xxxx.com是域名，那么他的I...

关尔佟

web渗透测试系列 之 信息收集（2）

千锋网络安全学院

switch DNS 推荐 不再花钱 更新无压力

DNS servers in Hong Kong直接上网站，昨天下单的switch，今天就到了，不得不说顺丰在疫情期间依然能保持这种速度是非常可以了so 我找到了很多贴纸，知乎也看了不少推荐的，发现都是重复的...

john

到底什么

小枣君

14 条评论 切换为时间排序

写下你的评论...

少行中 25 天前

太强了。

赞

江风引雨 (作者) 回复 **少行中** 25 天前

你好快

赞

不错兴奋地说 18 天前

这玩意最大的作用是把被墙的ip套一下复活[捂嘴]

赞

江风引雨 (作者) 回复 **不错兴奋地说** 17 天前

没错，搭配ws+tls食用更佳

2

Aa必将势不可挡 回复 **江风引雨** (作者) 17 天前

求教[赞同]

赞

展开其他 1 条回复

kagada 15 天前

太强了。

赞

小樱樱樱樱樱 9 天前

毕竟是BGP Anycast嘛

1

测试签名 6 天前

这样做的速度如何？跟直接套cf相比？

赞

江风引雨 (作者) 回复 **测试签名** 6 天前

其实差不多，可能略微稳定些

赞

貌似杀猪匠 ▲ 赞同 19 ▼ 14 条评论 分享 喜欢 收藏 ...

知乎

江风引雨 (作者) 回复 貌似杀猪匠 4 天前

不是自选，这只能算钻了个空子，不过Cloudflare控制台会显示NS未正确配置

赞

貌似杀猪匠 回复 江风引雨 (作者) 3 天前

效果类似改用cloudflare partner 的cname接入效果。

1

下午茶 回复 江风引雨 (作者) 2 天前

然后过两天 cf 就删除域名了

赞