Nginx 限制IP并发数

原创 2016-01-28 杜亦舒 [性能与架构](javascript:void(0);)

前几天介绍了[CC攻击及其防护方法](http://mp.weixin.qq.com/s?__biz=MzA4Nzc4MjI4MQ==&mid=402282033&idx=1&sn=14ac48d8176c35f7e83d959a329a5760&scene=21#wechat_redirect)，其中有一个方法是限制同一个IP的并发请求数量，以防止来自同一IP的大量高并发攻击

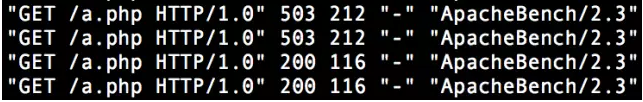
我的服务器一直没有配置这个限制，今天实验了一下，下面是配置过程

配置

示例

limit\_conn addr **2**; 表示限制并发数量最高为**2** 这个数字可以根据自己实际情况设置

测试

写了一个测试用的 a.php  
  
在另一台服务器用**ab**命令测试并发效果  
  
# ab -c 5 -t 10 http://192.2.4.31/a.php  
  
这里指定并发数为**5**，大于上面配置的最高限制  
  
回到nginx服务器查看访问日志  
  
# tail -f access.log  
  
  
  
可以看到很多请求的返回状态为503

增加 limit\_conn addr 的值为**10**，再次用**ab**测试

会看到返回状态都为200了，说明配置生效

配置说明

其中有两个关键指令的定义  
  
**（1）limit\_conn\_zone**   
  
limit\_conn\_zone $binary\_remote\_addr zone=addr:10m;  
  
limit\_conn\_zone 指令用来定义会话状态存储区域  
  
$binary\_remote\_addr 表示以客户端的IP作为键  
  
zone=addr:10m 表示分配一个名为 '**addr**' 的区域，空间大小为 **10M**  
  
相当于这个区域记录了IP的会话状态信息  
  
**（2）limit\_conn**   
  
limit\_conn 指令用来限制并发连接数  
  
limit\_conn addr 2; 表示到名为 '**addr**' 这个区域中检索IP键，不允许有超过**2**个的会话状态，超过的话会返回**503**  
  
  
通过这两项配置，就可以实现IP并发限制