0x00 简介

今日我们讲解一下 nginx 模块ngx\_http\_access\_module 单看这个模块名，很多小伙伴肯定是一脸蒙蔽的状态但是如果我说deny和allow那么小伙伴肯定就知道这是什么东西了，实际上deny和allow指令属于ngx\_http\_access\_module。

allow和deny这两个指令的意思是指，允许ip和限制ip

我们想控制某个路径或是那个url某个ip不让人访问那么就需要靠它了。

水分挤完了，开始干货把！ヽ(✿ﾟ▽ﾟ)ノ

0x01 我开始了哟

nginx中ngx\_http\_access\_module 模块提供了两个用于配置访问权限控制的指令，分别为allow与deny；

allow用于设置允许访问的权限；

deny 用于设置禁止访问的权限；

在使用的时候，权限指令的后面可以跟上允许或禁止的IP/网段/all允许所有的；

语法: allow address |CIDR|unix:|all；

允许一个ip或者ip段访问

语法: deny address |CIDR|unix:|all；

禁止一个ip或者ip段访问

0x02 例子：

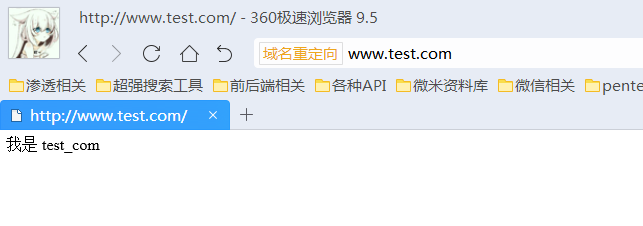
2.1默认访问权限：

确定我们的外网与虚拟机可以ping的通即可

查看我们的某个站点的nginx 服务器配置文件



大概这样以后外网访问一下看看



访问以后返回了对应的 index 内容，表明虚拟机默认没有设置访问权限，允许所有用户的访问，相当于为server设置了allow all！

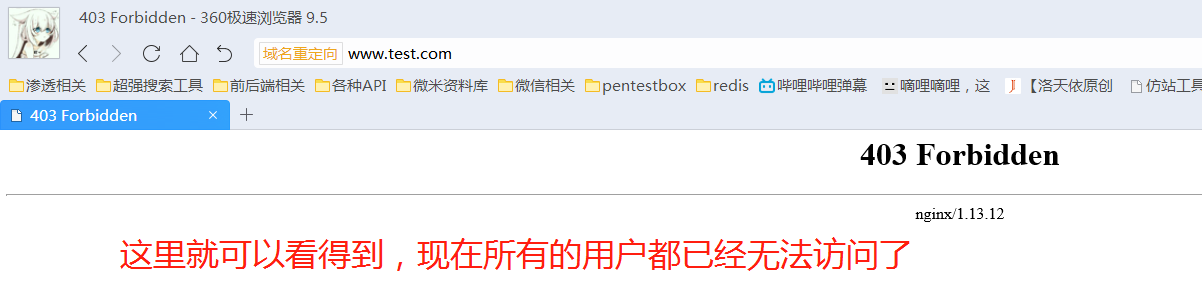
2.2禁止所用用户访问一：

这个时候我们修改一下nginx 的配置

禁止所有用户访问我们的站点

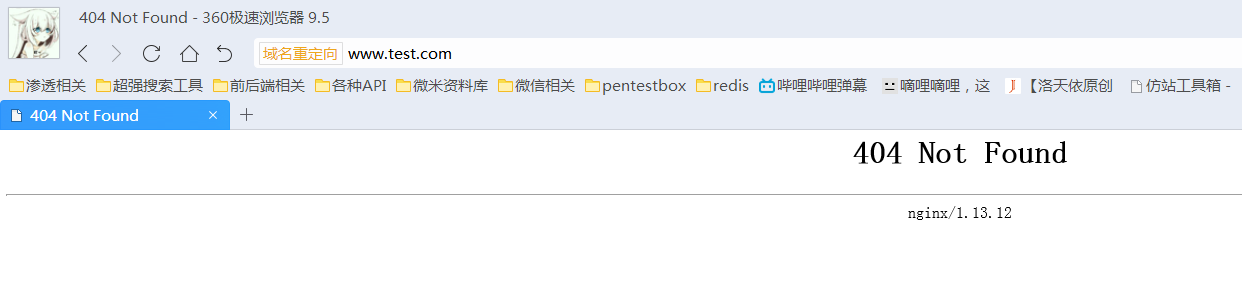
添加代码：deny all;





2.3禁止所用用户访问二：





2.4只允许指定用户访问设置一：

添加代码：

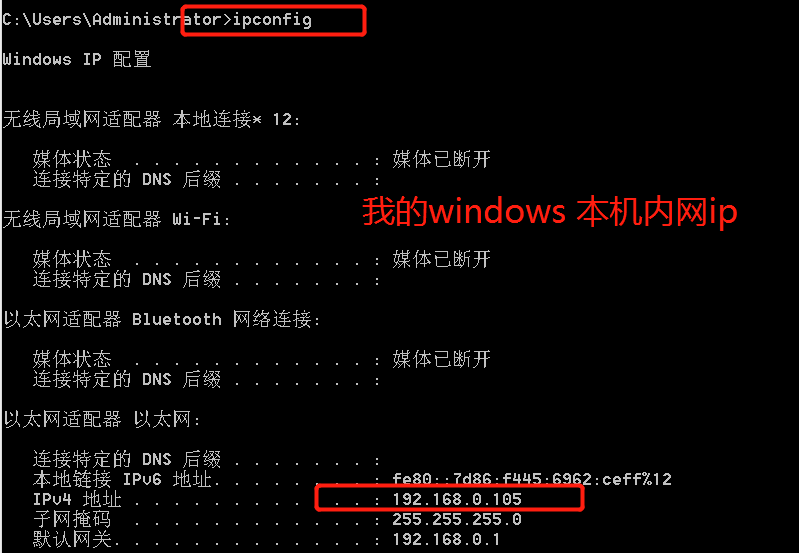
allow 192.168.0.105;

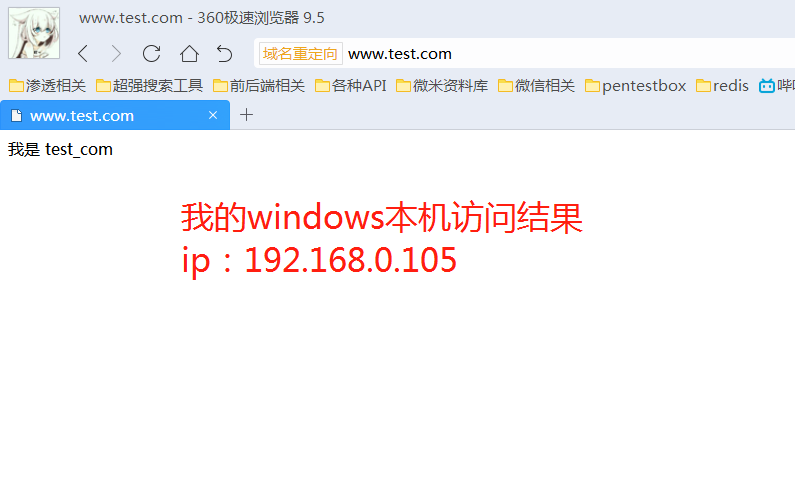
deny all;



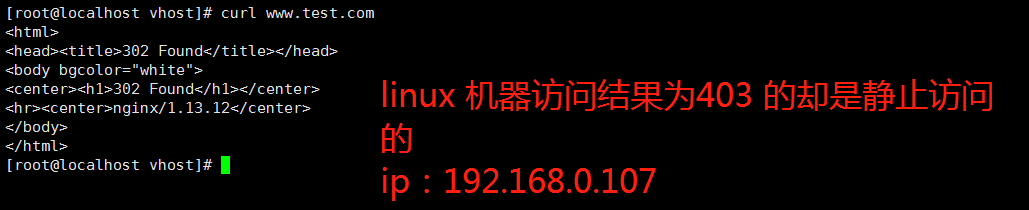
记得重启nginx；

命令：service nginx restart



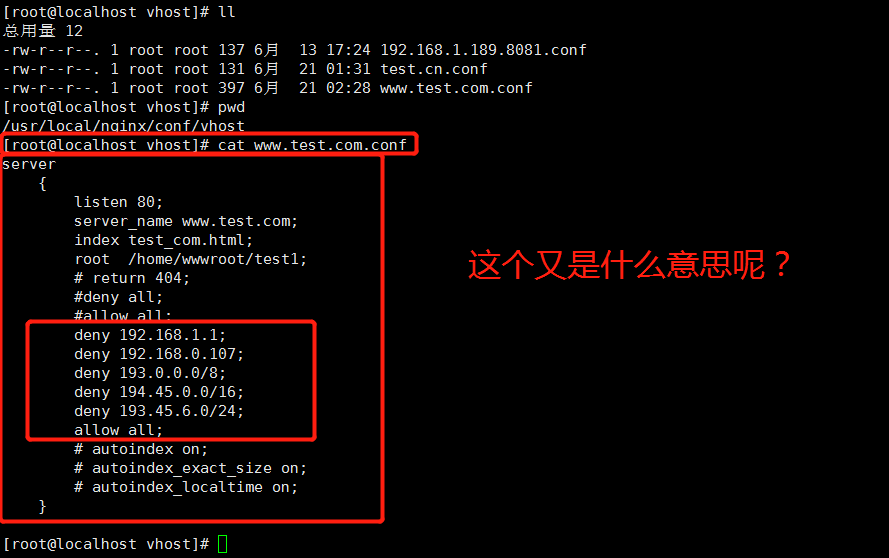






2.5只允许指定用户访问设置二：

我现在要做个功能，要禁止一些IP 或是ip段的访问 其他的都放行，这样的功能，就可以使用nginx 像下面这样配置了



````

#屏蔽192.168.1.1这个IP的访问

deny 192.168.1.1;

#屏蔽192.168.0.107这个IP的访问

deny 192.168.0.107;

#封整个段即从193.0.0.0到193.255.255.254的命令

deny 193.0.0.0/8;

#封IP段即从194.45.0.0到194.45.255.254的命令

deny 194.45.0.0/16;

#封IP段即从193.45.6.0到193.45.6.254的命令是

deny 193.45.6.0/24;

#运行剩下的ip访问

allow all;

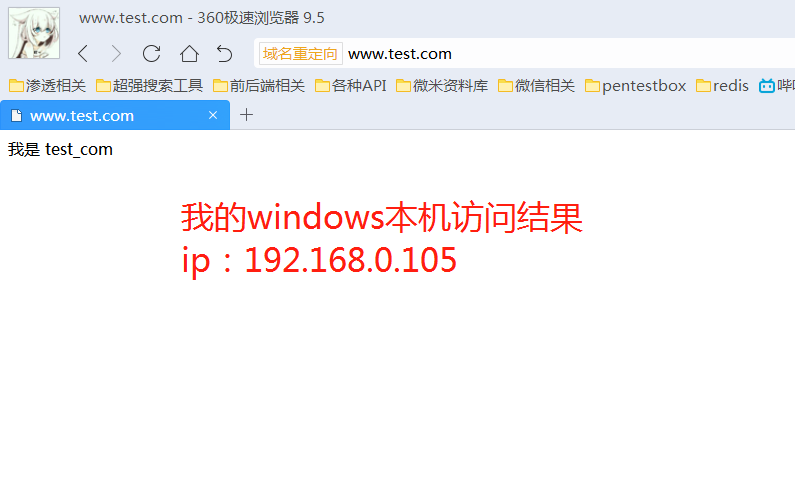
````

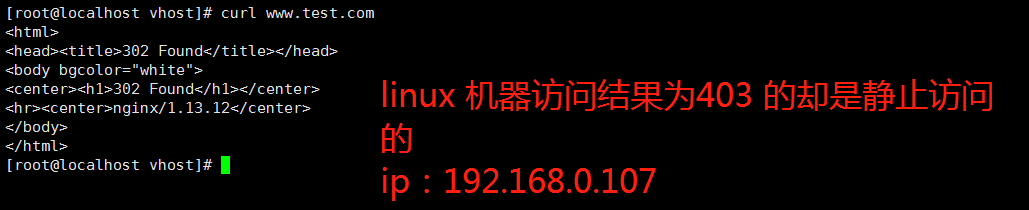
也就是说，如果最后的斜杠后的数值：

8：匹配后三位最大值的

16：匹配后两位最大值的

24：匹配后一位最大值的



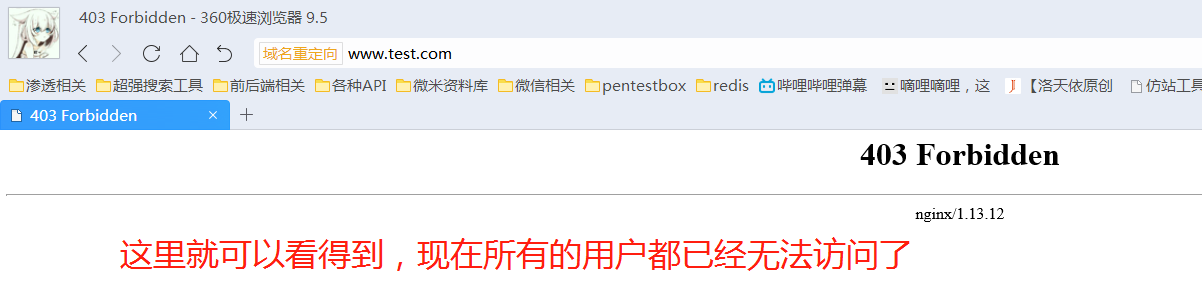


2.6不同块的访问权限指令优先级探讨：

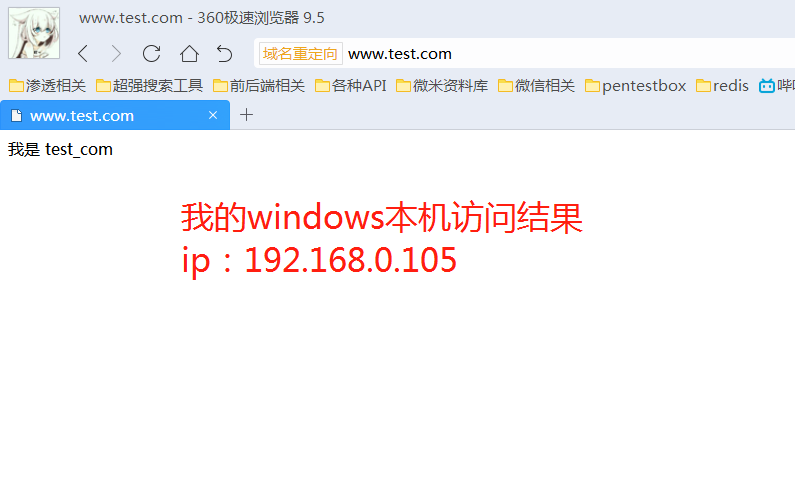
这里的话，我就有一个疑问了呀，假如我们在不同的模块下面 设置不同的 访问权限那么他最终会执行的是那个呢？

那么如果我是相同模块下设置不同的访问权限那又会显示那个呢？

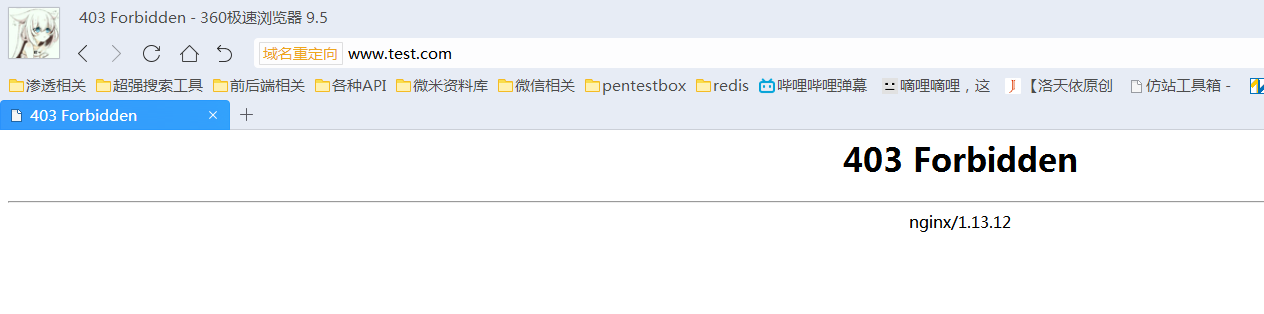












---2.6结论：

上面就是Nginx配置文件中在各个块嵌套的情况下的结果。

最终可以得出**内层块内的指令比外层块内的指令执行优先级高**，因此，当内外层中同时出现权限指令时，则**内层块中的allow all会覆盖外层块的deny all的设置**；

而**当同一个模块都出现了权限指令时，则第一个出现的权限指令优先级最高**