[**丁丁的开发日记**](http://www.cnblogs.com/tintin1926/)

**一所懸命**

[**使用nginx搭建https服务器**](http://www.cnblogs.com/tintin1926/archive/2012/07/12/2587311.html)

最近在研究nginx，整好遇到一个需求就是希望服务器与客户端之间传输内容是加密的，防止中间监听泄露信息，但是去证书服务商那边申请证书又不合算，因为访问服务器的都是内部人士，所以自己给自己颁发证书，忽略掉浏览器的不信任警报即可。下面是颁发证书和配置过程。

首先确保机器上安装了openssl和openssl-devel

#yum install openssl

#yum install openssl-devel

然后就是自己颁发证书给自己

#cd /usr/local/nginx/conf

#openssl genrsa -des3 -out server.key 1024

#openssl req -new -key server.key -out server.csr

#openssl rsa -in server.key -out server\_nopwd.key

#openssl x509 -req -days 365 -in server.csr -signkey server\_nopwd.key -out server.crt

至此证书已经生成完毕，下面就是配置nginx

server {

listen 443;

ssl on;

ssl\_certificate /usr/local/nginx/conf/server.crt;

ssl\_certificate\_key /usr/local/nginx/conf/server\_nopwd.key;

}

然后重启nginx即可。

ps： 如果出现“[emerg] 10464#0: unknown directive "ssl" in /usr/local/nginx-0.6.32/conf/nginx.conf:74”则说明没有将ssl模块编译进nginx，在configure的时候加上“--with-http\_ssl\_module”即可^^

至此已经完成了https服务器搭建，但如何让浏览器信任自己颁发的证书呢？

今天终于研究捣鼓出来了，只要将之前生成的server.crt文件导入到系统的证书管理器就行了，具体方法：

控制面板 -> Internet选项 -> 内容 -> 发行者 -> 受信任的根证书颁发机构 -> 导入 -》选择server.crt