**[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

另一篇申请ssl的说明：https://www.freessl.com/

### Solution

This document provides instructions for generating a Certificate Signing Request (CSR) for Nginx Server. If you are unable to use these instructions for your server, RapidSSL recommends that you contact a compnay that supports Nginx.

**NOTE:** To generate a CSR, you will need to create a key pair for your server. These two items are a digital certificate key pair and cannot be separated. If you lose your public/private key file or your password and generate a new one, your SSL Certificate will no longer match.

**NOTE:** **All certificates that will expire after October 2013 must have a 2048 bit key size.**

**To generate a CSR on Nginx, please do the following:**

    1.    Login to your server via your terminal client (ssh). At the prompt, type:  
 **openssl req -new -newkey rsa:2048 -nodes -keyout server.key -out server.csr**    2.    This will begin the process of generating two files: the **Private-Key** file for the decryption  
           of your SSL Certificate,   
           and a certificate signing request (**CSR**) file used to apply for your SSL Certificate.   
    3.    The command from **Step 1** will prompt for the following X.509 attributes of the certificate

* **Country Name (C):** Use the two-letter code without punctuation for country, for example: US or CA.
* **State or Province (S):** Spell out the state completely; do not abbreviate the state or province name, for example: California.
* **Locality or City (L):** The Locality field is the city or town name, for example: Berkeley.
* **Organization (O):** If your company or department has an &, @, or any other symbol using the  
  shift key in its name, you must spell out the symbol or omit it to enroll, for example:   
  XY & Z Corporation would be XYZ Corportation or XY and Z Corportation.
* **Organizational Unit (OU):** This field is the name of the department or   
  organization unit making the request.
* **Common Name (CN):** The Common Name is the Host + Domain Name.   
  **NOTE**: RapidSSL certificates can only be used on Web servers using the Common Name  
  specified during enrollment. For example, a certificate for the domain "domain.com" will  
  receive a warning if accessing a site named [www.domain.com](http://www.domain.com/) or "secure.domain.com",   
  because "www.domain.com" and "secure.domain.com" are different from "domain.com."

    4.    When promted, please do not enter your email address, challenge password or an optional  
           company name when generating the CSR.Leave out this fields blank.  
    5.    Your .csr file will then be created.  
    6.    Proceed to Enrollment and paste the CSR in the enrollment form when required.  
  
**Once the certificate has been issued, refer to this link for installation instructions:**[**SO17664**](https://knowledge.rapidssl.com/support/ssl-certificate-support/index?page=content&actp=CROSSLINK&id=SO17664)