**1，nginx配置HTTPS前置条件**

服务器上已经安装nginx服务，已经具备http访问；

nginx服务器是否已经安装ssl模块得支持；

是否已经拥有ssl证书，如果没有可以去阿里云或者腾讯云免费申请；

## 2，nginx SSL模块是否支持



## 3，nginx安装

3.1 nginx官网地址

下载地址：http://nginx.org/en/download.html

这里下载nginx-1.18.0稳定版tar.gz

3.2 下载tar包到服务器目录

cd /home/somnus

wget http://nginx.org/download/nginx-1.18.0.tar.gz

1

2

3.3 解压安装包

tar -zxvf nginx-1.18.0.tar.gz

1

3.4 配置ssl模块

cd nginx-1.18.0

./configure --prefix=/usr/local/nginx --with-http\_ssl\_module

1

2

我们只需要执行以上命令即可，由于我服务器上还有其他模块依赖

3.5 接下来执行命令编译

使用 make 命令编译（使用make install会重新安装nginx），此时当前目录会出现 objs 文件夹。用新的 nginx 文件覆盖当前的 nginx 文件。

## 4. ssl 证书部署

<https://blog.csdn.net/lw112190/article/details/117320331?utm_medium=distribute.pc_aggpage_search_result.none-task-blog-2~aggregatepage~first_rank_ecpm_v1~rank_v31_ecpm-1-117320331-null-null.pc_agg_new_rank&utm_term=nginx%E6%9C%AC%E5%9C%B0%E9%85%8D%E7%BD%AEhttps&spm=1000.2123.3001.4430>

生成[秘钥](https://so.csdn.net/so/search?q=%E7%A7%98%E9%92%A5&spm=1001.2101.3001.7020)key,运行:

$ openssl genrsa -des3 -out server.key 2048

会有两次要求输入密码,输入同一个即可。输入密码然后你就获得了一个server.key文件。  
以后使用此文件(通过[openssl](https://so.csdn.net/so/search?q=openssl&spm=1001.2101.3001.7020)提供的命令或API)可能经常回要求输入密码,如果想去除输入密码的步骤可以使用以下命令:

$ openssl rsa -in server.key -out server.key

创建服务器证书的申请文件server.csr,运行:

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

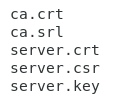
其中Country Name填CN,Common Name填主机名也可以不填,如果不填浏览器会认为不安全.(例如你以后的url为https://abcd/xxxx….这里就可以填abcd),其他的都可以不填.  
创建CA证书:

openssl req -new -x509 -key server.key -out ca.crt -days 3650

此时,你可以得到一个ca.crt的证书,这个证书用来给自己的证书签名.  
创建自当前日期起有效期为期十年的服务器证书server.crt：

openssl x509 -req -days 3650 -in server.csr -CA ca.crt -CAkey server.key -CAcreateserial -out server.crt

ls你的文件夹,可以看到一共生成了5个文件:



其中,server.crt和server.key就是你的[nginx](https://so.csdn.net/so/search?q=nginx&spm=1001.2101.3001.7020)需要的证书文件.

**如何配置nginx**

打开你的nginx配置文件,搜索443找到https的配置,去掉这段代码的注释.或者直接复制我下面的这段配置:

1. server {
3. listen 443;
4. server\_name localhost;
5. ssl on;
6. ssl\_certificate /root/keys/server.crt;*#配置证书位置*
7. ssl\_certificate\_key /root/keys/server.key;*#配置秘钥位置*
8. *#ssl\_client\_certificate ca.crt;#双向认证*
9. *#ssl\_verify\_client on; #双向认证*
10. ssl\_session\_timeout 5m;
11. ssl\_protocols SSLv2 SSLv3 TLSv1;
12. ssl\_ciphers ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP;
13. ssl\_prefer\_server\_ciphers on;

将ssl\_certificate改为server.crt的路径,将ssl\_certificate\_key改为server.key的路径.  
nginx -s reload 重载配置  
至此,nginx的https就可以使用了,默认443端口.

如果出现报错信息：

nginx: [emerg] BIO\_new\_file("/user/local/nginx/temp/server.crt") failed (SSL: error:02001002:system library:fopen:No such file or directory:fopen('/user/local/nginx/temp/server.crt','r') error:2006D080:BIO routines:BIO\_new\_file:no such file)

把server.crt 和server.key 文件放在nginx/conf文件夹下。(和nginx.conf文件同一文件夹)

ssl\_certificate  server.crt;  
ssl\_certificate\_key  server.key;

