Nginx之Https配置

nginx的https协议需要ssl模块的支持，我们在编译nginx时使用–with-http\_ssl\_module参数加入SSL模块。还需要服务器私钥，服务器证书，如果是公司对外环境，这个证书需要购买第三方的权威证书，否则用户体验得不到保障；这里我仅仅在我的vps上使用并测试。

注意：如果你购买的是第三方服务证书,那么只需要参考1.3-1.4的配置信息即可完整企业ssl配置实践。

1.1检查Nginx的SSL模块是否安装

[root@web-node1~]# /application/nginx/sbin/nginx -V

nginx version: nginx/1.6.3

built by gcc 4.4.7 20120313 (Red Hat 4.4.7-16) (GCC)

TLS SNI support enabled

configure arguments: –prefix=/application/nginx-1.6.3 –user=nginx –group=nginx –with-http\_ssl\_module –with-http\_stub\_status\_module

1.2准备私钥和证书

1.2.1创建服务器私钥

[root@web-node1~]# cd /application/nginx/conf/

[root@web-node1 conf]# mkdir key

[root@web-node1 conf]# cd key/

[root@web-node1 key]# openssl genrsa -des3 -out server.key 1024

Generating RSA private key, 1024 bit long modulus

..++++++

…++++++

e is 65537 (0x10001)

Enter pass phrase for server.key:

Verifying – Enter pass phrase for server.key:

1.2.2签发证书

[root@web-node1 key]# openssl req -new -key server.key -out server.csr

Enter pass phrase for server.key:

You are about to be asked to enter information that will be incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter ‘.’, the field will be left blank.

—–

Country Name (2 letter code) [XX]:CN

State or Province Name (full name) []:BJ

Locality Name (eg, city) [Default City]:BJ

Organization Name (eg, company) [Default Company Ltd]:SDU

Organizational Unit Name (eg, section) []:SA

Common Name (eg, your name or your server’s hostname) []:XuBuSi

Email Address []:xubusi@xuliangwei.com

Please enter the following ‘extra’ attributes

to be sent with your certificate request

A challenge password []:

An optional company name []:

1.2.3删除服务器私钥口令

[root@web-node1 key]# cp server.key server.key.ori

[root@web-node1 key]# openssl rsa -in server.key.ori -out server.key

Enter pass phrase for server.key.ori:

writing RSA key

1.2.4生成使用签名请求证书和私钥生成自签证书

[root@web-node1 key]# openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt

Signature ok

subject=/C=CN/ST=BJ/L=BJ/O=SDU/OU=SA/CN=XuBuSi/emailAddress=xubusi@xuliangwei.com

Getting Private key

1.3开启Nginx SSL

[root@web-node1 ~]# cat /application/nginx/conf/vhosts/www.conf

server {

server\_nameblog.xuliangwei.com;

#listen 80;

listen 443;

ssl on;

ssl\_certificate key/server.crt;

ssl\_certificate\_key key/server.key;

location / {

roothtml/blog;

index index.php index.html index.htm;

access\_log /app/logs/blog.xuliangwei.log main;

}

}

1.3.1重启nginx生效

[root@web-node1 ~]# /application/nginx/sbin/nginx -s reload

[root@web-node1 ~]# netstat -lntup|grep 443

tcp 0 0 0.0.0.0:443 0.0.0.0:\* LISTEN 1711/nginx

1.3.2测试https

由于该证书非第三方权威机构颁发，而是我们自己签发的，所以浏览器会警告，如果是对外的业务需要加密，必须使用商用第三方签名证书。

1.4配置重定向80端口转443端口

以上配置有个不好的地方，如果用户使用时忘了使用https或者443端口，那么将会报错，所以我们需要80端口的访问转到443端口并使用ssl加密访问。

只需要增加一个server段，使用301永久重定向。

[root@web-node1 ~]# tail -5 /application/nginx/conf/vhosts/www.conf

server {

listen 80;

server\_name blog.xuliangwei.com;

rewrite ^(.\*) https://$server\_name$1 permanent;

}

[root@web-node1 ~]# /application/nginx/sbin/nginx -t

nginx: the configuration file /application/nginx-1.6.3/conf/nginx.conf syntax is ok

nginx: configuration file /application/nginx-1.6.3/conf/nginx.conf test is successful

[root@web-node1 ~]# /application/nginx/sbin/nginx -s reload