Ngnix SSL Certificate Deployment Guide

沃通电子认证服务有限公司

WoSignCA Limited

Content

Contact information of technical support

Email of technical support：support@wosign.com

Hotline of technical support：+86-755-8600 8688

Website of technical support：https://bbs.wosign.com

Company official website address：https://www.wosign.com

1. The environment for installing the SSL certificate

1.1 Brief introduction of SSL certificate installation environment

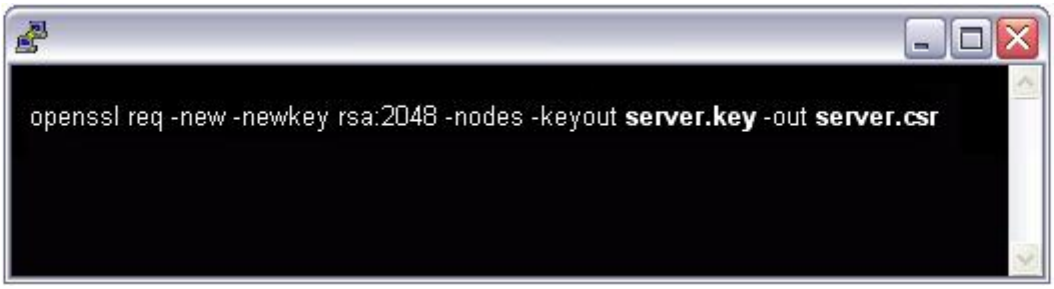
Cnetos 6.4;
Nginx 1.9.1;
Openssl 1.0.1+;
SSL certificate（Note: this guide uses the OV SSL certificate which the domain name is s.wosign.com to operate, other version of the certificate are also common.）.

1.2 Network environment requirements

Please ensure the site is a legitimate e domain address, which can normal access by typing it’s domain name http://XXX.

2. Created a Certificate Signing Request (CSR)

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



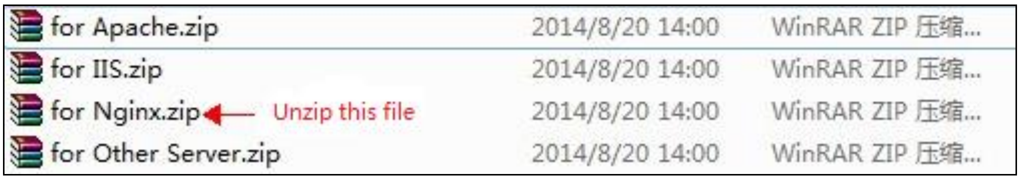
```
openssl req -new -newkey rsa:2048 -nodes -keyout server.key -out server.csr
```

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. Installation of SSL certificate

3.1 Get SSL certificate

You will get a zip file with password after you apply the certificate from wosign successfully. You need to enter the password to extract the file, after extract the file you will get 4 files: for Apache、for IIS、for Nginx、for Other Servert. These are different formats for different servers. We will need to use the certificate from for Ngnix.



```
for Apache.zip                              2014/8/20 14:00    WinRAR ZIP 压缩...
for IIS.zip                                 2014/8/20 14:00    WinRAR ZIP 压缩...
for Nginx.zip ← Unzip this file             2014/8/20 14:00    WinRAR ZIP 压缩...
for Other Server.zip                        2014/8/20 14:00    WinRAR ZIP 压缩...
```

Figure 1

3.2 Extract SSL certificate

Open the file for Nginx, you can see a file, including public key, as shown in Figure 2

```
1_test.wosign.com_bundle.crt ← Public key 2014/8/20 14:00
```

Figure 2

3.3 Install SSL certificate

Open the file nginx.conf which is under the file conf in Nginx directory, and you can find the code below.

```
# HTTPS server
 #
 #server {
 #       listen          443;
 #       server_name   localhost;
 #       ssl                        on;
 #       ssl_certificate      cert.pem;
 #       ssl_certificate_key   cert.key;
 #       ssl_session_timeout   5m;
 #       ssl_protocols   SSLv2 SSLv3 TLSv1;
 #                                                                      ssl_ciphers
ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP;
    #     ssl_prefer_server_ciphers    on;
    #     location / {
    #         root    html;
    #         index   index.html index.htm;
    #     }
    #}
```

Modify it to:

```
    server {
        listen          443;
        server_name   localhost;
        ssl                          on;
        ssl_certificate          sslkey/wosign.com.crt;          （public key of SSL certificate）
        ssl_certificate_key          sslkey/wosign.com.key;  （private key of SSL certificate）
        ssl_session_timeout   5m;
        ssl_protocols   TLSv1 TLSv1.1 TLSv1.2;
        ssl_ciphers    ALL:!DH:!EXPORT:!RC4:+HIGH:+MEDIUM:-LOW:!aNULL:!eNULL;
        ssl_prefer_server_ciphers    on;
        location / {
            root    html;
            index   index.html index.htm;
        }
    }
```

Save exit and restart Nginx.

Access your site through HTTPS, test the installation configuration of SSL certificate.

4. Install Secure signature

（Secure signature only works on OV and EV SSL certificate now）

After you purchased the SSL WoSign certificate, you can get a trusted website security certification logo which shows your company’s certificate information freely. It can greatly enhance the user's online trust, to facilitate more online transactions. So we suggest you to add the following code which can dynamically display the trusted site security certification logo on your homepage or other page.

If you want display the certificate logo on Enlgish website, add the code on the English web page below:

```
<SCRIPT LANGUAGE="JavaScript" TYPE="text/javascript" SRC="https://seal.wosign.com/tws-en.js"></SCRIPT>
```

Secured
2013-03-07 13 : 34
OV

Secured
2013-03-07 13 : 34
EV

5. Backup of SSL certificate

Please save the file and password you receive.

6. Restore of SSL certificate

Repeat 2.3 operation。