服务器 SSL 证书安装配置指南

Nginx

更新日期：2016-11-7

第一步：生成证书请求文件(CSR)

进入 OpenSSL 安装的目录，运行如下命令生成私钥：

```
openssl genrsa -out server.key 2048
Loading 'screen' into random state - done
Generating RSA private key, 2048 bit long modulus
.....++++++
.....++++++
e is 65537 (0x10001)
```

该命令执行后将会生成 server.key 私钥文件

运行如下命令生成证书请求文件（CSR）

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

如是 Windows 系统，请使用下面命令生成证书请求文件（CSR）

```
set OPENSSL_CONF=openssl.cnf
openssl req -new -key server.key -out server.csr
```

接下来提提示输入申请证书的详细信息

```
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) []:CN
State or Province Name (full name) []:Shanghai
Locality Name (eg, city) []:Shanghai
Organization Name (eg, company) []:GlobalSign China Co., Ltd.

Organizational Unit Name (eg, section) []:IT Dept.
Common Name (eg, your websites domain name) []:cn.globalsign.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
```

从 Email 地址开始，下面的信息都不需要，请保留为空，直接回车即可。

需要输入的信息说明请见下表：

字段	说明	示例
Country Name	ISO 国家代码（两位字符）	CN
State or Province Name	所在省份	Shanghai
Locality Name	所在城市	Shanghai
Organization Name	公司名称	GlobalSign China Co., Ltd.
Organizational Unit Name	部门名称	IT Dept.
Common Name	申请证书的域名	cn.globalsign.com
Email Address	不需要输入	
A challenge password	不需要输入	

完成以上的操作后会在对应的目录下生成 server.key 和 server.csr，请妥善保存这两个文件。

第二步：提交 CSR，申请证书

递交证书申请表及相关资料，并把证书请求文件（CSR）提交给我们。
我们确认资料齐全后，三个工作日内完成证书颁发。

第三步：获取服务器证书

1. 获取 SSL 证书（此证书由 GlobalSign 系统通过 Email 方式发送给用户，邮件中第一段代码），证书文件的内容为（包括“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”），请把此内容保存为 server.cer（文本格式）。

2. 获取中级证书（此证书由 GlobalSign 系统通过 Email 方式发送给用户，邮件中第二段代码），证书文件的内容为（包括“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”），请把此内容追加到 server.cer 内容后。最终 server.cer 内容如下：

```
-----BEGIN CERTIFICATE-----
MIIE3zCCA8egAwIBAgIMZaTH1OGecTk1fJSsMA0GCSqGSIb3DQEBCwUAMEw
BgNVBAYTAkJFMRkwFwYDVQQKExBHbG9iYWxTaWduIG52LXNhMSIwIAYDVQQ
bHBoYVNTTCBDQSAtIFNIQTI1NiAtIEcyMB4XDTE2MDgxNTAzNDgyM1oXDTE
NjAzNDgyM1owPTEhMB8GA1UECxMYRG9tYWluIENvbnRyb2wgVmFsaWRhdGV
FgYDVQQDDA8qLmdsb2JhbHNpZ24uY24wggEiMA0GCSqGSIb3DQEBAQUAA4I
ggEKAoIBAQDagY7pJ3DYOgdOpdMdCtHj2ERP0eCINzhd1bAZnSwL46fFwt6
5e41IjryiypSVIHodzaGfrg3t48IRnxtYMxmmeUAA8j3QGFComLdNANEYV3
+rFWzXvKqYaWNP/ru9SGgtB4Y0/dPBbNdGw7FcfRFUgG04D8V1toNu0NtTa
4nXhXERQmsnMfSY8z5fL4eAWJ0CNqEp94Qq1IARLFw1XBVrDPy6qcXJu0pL
pmjooGp72B0LqCUxXEkZPWAKj9GfkwqI1dTg9mKSNZdoeHR8311JLPdRKGh
NuxZ7Hu3M/9CKnYro51gJHHV8zOHULWNAgMBAAGjggHOMIIByjAOBgNVHQ8
BAMCBaAwgYkGCCsGAQUFBwEBBH0wezBCBggrBgEFBQcwAoY2aHR0cDovL3N
ZTIuYWxwaGFzc2wuY29tL2NhY2VydC9nc2FscGhhc2hhMmcycjEuY3J0MDU
AQUFBzABhilodHRwOi8vb2NzcDIuZ2xvYmFsc2lnbi5jb20vZ3NhbHBoYXN
MjBXBgNVHSAEUDBOMEIGCisGAQQBoDIBCgowNDAyBggrBgEFBQcCARYmaHR
Ly93d3cuZ2xvYmFsc2lnbi5jb20vcmVwb3NpdG9yeS8wCAYGZ4EMAQIBMAk
EwQCMAAwPgYDVR0fBDcwNTAzoDGgL4YtaHR0cDovL2NybDIuYWxwaGFzc2w
L2dzL2dzYWxwaGFzaGEyZzIuY3JsMCkGA1UdEQQiMCCCDyouZ2xvYmFsc21
boINZ2xvYmFsc2lnbi5jbjAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQU
HQYDVR0OBBYEFF6Mmd8Oj2peJlBS/+W7spDvBkWUMB8GA1UdIwQYMBaAFPX
UP1qTzq319pWg+Zp0mj3MA0GCSqGSIb3DQEBCwUAA4IBAQAqtbem7sW/m74
SjcN+sJ8F8b2ozSCu4doULg37zjfNhHXL/F8XzsLzPnN1XHkzmgaWAaOSnu
Jx5Don6BrVQuXY7Rn4Qy8bicU3aY530+UsV45U5ErZZ/43z4y5Wj7I/mCC9
SaYeRB1V6c79hD8HtbwZkmywxyVy3V21Rm7WRIlQ1cnTLmynIPhs0uVyl1d
9XJyG4CSkUrijPEJXvmJAtaldbbdctEikb2jNS+MdrIbYmsIYWQwWESW60d
XCnHBv46wuxSuDyypcOrzDvJj+hUYN5s3F1pH/Tj5bTXXeS/RTTfuW4SY6G
PKNg
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIETTCCAzWgAwIBAgILBAAAAAABRE7wNjEwDQYJKoZIhvcNAQELBQAwVzE
A1UEBhMCQkUxGTAXBgNVBAoTEEdsb2JhbFNpZ24gbnYtc2ExEDAOBgNVBAs
b3QgQ0ExGzAZBgNVBAMTEkdsb2JhbFNpZ24gUm9vdCBDQTAeFw0xNDAyMjA
```

请把 server.cer 和 server.key 这两个文件保存到同一个目录下，例如放到/etc/ssl/crt/目录下。

第四步：更新 nginx.conf 配置文件

用文本编辑器打开 nginx.conf 并更新以下内容

```
server
{ listen
443;
server_name www.domain.com;
ssl on;
ssl_certificate /etc/ssl/crt/server.cer; // 公钥文件 (Globalsign 颁发的证书 )
ssl_certificate_key /etc/ssl/crt/server.key; //私钥文件
ssl_session_timeout 5m;
ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
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; }
}
```

按照以上的步骤配置完成后，重新启动 Nginx（如果有设置 server.key 私钥密码，这时会提示输入） 后就可以使用 https://www.domain.com 来访问了。

如有任何问题或疑问请直接与我们联系，谢谢！