



服务器证书安装配置指南

Nginx

Q/ GlobalSign China-QI-XX-YY

GlobalSign 数字证书颁发机构
环玺信息科技（上海）有限公司

2018 年 1 月

目 录

1. 生成证书请求.....	3
1.1 安装 OpenSSL 工具.....	3
1.2 生成服务器证书私钥.....	3
1.3 生成服务器证书请求文件.....	3
1.4 备份私钥并提交证书请求.....	3
2. 安装服务器证书.....	3
2.1 获取服务器证书文件.....	3
2.2 安装服务器证书.....	4
3. 安装服务器证书.....	5
3.1 服务器证书的备份.....	5
3.2 服务器证书的恢复.....	5

服务器证书安装配置指南 (Nginx)

1. 生成证书请求

1.1 安装 OpenSSL 工具

您需要使用 openssl 工具来创建证书请求。

下载 OpenSSL:

<http://www.globalsign.cn/Openssl/openssl-1.0.2p.tar.gz>

1.2 生成服务器证书私钥

安装 OpenSSL 到 C:\openssl

命令行进入 C:\openssl\bin, 运行如下命令:

```
openssl genrsa -out server.key 2048
```

您还可以选择下载 CSR 自动创建程序, 快速创建证书请求。

1.3 生成服务器证书请求文件

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

1.4 备份私钥并提交证书请求

请妥善保存证书私钥文件 server.key, 并将证书请求文件 certreq.csr 提交给 GlobalSign。

2. 安装服务器证书

2.1 获取服务器证书文件

将证书签发邮件中的包含服务器证书代码的文本复制出来 (包括 “-----BEGIN CERTIFICATE-----” 和 “-----END CERTIFICATE-----”) 粘贴到记事本等文本编辑器中。

为保障 EV 服务器证书在 IE7 以下客户端的兼容性, EV 服务器证书需要安装两张中级 CA 证书。

在服务器证书代码文本结尾, 回车换行, 并分别粘贴两张中级 CA 证书代码 (包括 “-----BEGIN CERTIFICATE-----” 和 “-----END CERTIFICATE-----”, 每串证书代码之间均

使用回车换行分隔)，修改文件扩展名，保存为 server.pem 文件。

2.2 安装服务器证书

打开 Nginx 安装目录下 conf 目录中的 nginx.conf 文件找到

```
# 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;
#    }
#}
```

将其修改为

```
server {
    listen          443;
    server_name     localhost;
    ssl              on;
    ssl_certificate  server.pem;
    ssl_certificate_key server.key;
    ssl_session_timeout 5m;
    ssl_protocols   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;
    }
}
```

保存退出，并重启 Nginx。

通过 https 方式访问您的站点，测试站点证书的安装配置。

3. 安装服务器证书

在您成功的安装和配置了服务器证书之后，请务必依据下面的操作流程，备份好您的服务器证书，以防证书丢失给您的系统应用带来不便。

3.1 服务器证书的备份

备份服务器证书私钥文件 `server.key`，以及服务器证书文件 `server.pem` 即可完成服务器证书的备份操作。

3.2 服务器证书的恢复

请参照服务器证书配置部分，将服务器证书密钥文件恢复到您的服务器上，并修改配置文件，恢复服务器证书的应用。