服务器证书安装配置指南

Apache

二〇二一年一月

GlobalSign
GMO INTERNET GROUP

目 录

服务器证书安装配置指南（Apache）

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

您还可以选择在线CSR 创建程序，快速创建证书请求。

1.3 生成服务器证书请求（CSR）文件

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

Country Name：	//您所在国家的ISO 标准代号，中国为CN
State or Province Name：	//您单位所在地省/自治区/直辖市
Locality Name：	//您单位所在地的市/县/区
Organization Name：	//您单位/机构/企业合法的名称
Organizational Unit Name：	//部门名称
Common Name：	//通用名，例如：cn.globalsign.com。此项必须与访问提供 SSL 服务的服务器时所应用的域名完全匹配。
Email Address：	//您的邮件地址，不必输入，直接回车跳过
"extra"attributes：	//以下信息不必输入，回车跳过直到命令执行完毕。

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CA 证书

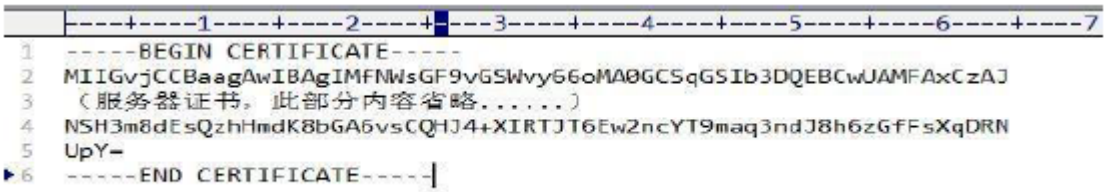
为保障服务器证书在 IE7 以下客户端的兼容性，服务器证书需要安装 CA 证书（CA证书包含中级证书，交叉证书（重要））。

从邮件中获取 CA证书：

将证书签发邮件中的从 BEGIN 到 END 结束的两段 CA证书内容（包括“-----BEGIN CERTIFICATE-----”和“----- ENDCERTIFICATE -----”）粘贴到同一个记事本等文本编辑器中。修改文件扩展名，保存为 intermediate.cer 文件。如下

2.2 获取服务器证书

将证书签发邮件中的从BEGIN 到END 结束的服务器证书内容（包括“--------BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”）粘贴到记事本等文本编辑器中，保存为 server.cer 文件，如下



Apache 2.0.63 的配置

打开apache 安装目录下conf 目录中的httpd.conf 文件，找到172 行

#LoadModulessl_module modules/mod_ssl.so

删除行首的配置语句注释符号“#”

保存退出。

打开apache 安装目录下conf 目录中的ssl.conf 文件，找到35 行<IfDefine SSL>

在行首添加注释符号“#”找到文件末行（246 行）</IfDefine>在行首添加注释符号“#”在配置文件中查找以下配置语句

SSLCertificateFile conf/ssl.crt/server.cer (108 行）将服务器证书配置到该路径

SSLCertificateKeyFile conf/ssl.key/server.key (116 行) 将服务器证书私钥配置到该路径下

#SSLCertificateChainFile conf/ssl.crt/intermediate.cer (126 行) 删除行首的“#”号注释符， 并将CA 证书intermediate.cer 配置到该路径下

保存退出，并重启 Apache

Apache 2.2.* 的配置

打开 apache 安装目录下 conf 目录中的 httpd.conf 文件，找到

#LoadModule ssl_module modules/mod_ssl.so

#Include conf/extra/httpd-ssl.conf 删除行首的配置语句注释符号“#”

保存退出。

打开 apache 安装目录下 conf/extra 目录中的 httpd_ssl.conf 文件在配置文件中查找以下配置语句

SSLCertificateFile conf/ssl.crt/server.cer 将服务器证书配置到该路径下

SSLCertificateKeyFile conf/ssl.key/server.key 将服务器证书私钥配置到该路径下

#SSLCertificateChainFile conf/ssl.crt/intermediate.cer 删除行首的“#”号注释符

并将 CA 证书intermediate.cer 配置到该路径下

保存退出，并重启 Apache

通过 https 方式访问您的站点，测试站点证书的安装配置。

3. 服务器证书的备份及恢复

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，服务器证书文件 server.cer，以及服务器证书CA 证书文件 intermediate.cer 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。

GlobalSign China Co., Ltd

环玺信息科技（上海）有限公司

2021年 1 月