Apache 安装 SSL 证书

1、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

(如果找不到请确认是否编译过 openssl 插件)

#Include conf/extra/httpd\_ssl.conf

删除行首的配置语句注释符号“#”

保存退出。

2、打开 apache 安装目录下 conf/extra 目录中的 httpd-ssl.conf 文件

(注释：安装配置目录有以能存在差异：conf.d/ssl.conf

ubuntu/apache2 安装目录：conf/sites-enabled/\*.conf )

在配置文件中查找以下配置语句：

a. 添加 SSL 协议支持语句，关闭不安全的协议和加密套件

SSLProtocol all –SSLv1 -SSLv2 -SSLv3

b.修改加密套件如下

SSLCipherSuite AESGCM:ALL:!DH:!EXPORT:!RC4:+HIGH:!MEDIUM:!LOW:!aNULL:!eNULL;

c.将服务器证书公钥配置到该路径下(在 conf 目录下创建 ssl 目录，将 for Apache 里面的

SSLCertificateFile conf/ssl/zhengshu.cer (证书公钥)

d.将服务器证书私钥配置到该路径下

SSLCertificateKeyFile conf/ssl/miyao.key (证书私钥)

e.将服务器证书链配置到该路径下

#SSLCertificateChainFile conf/ssl/chain.cer(证书链)删除行首的“#”号注

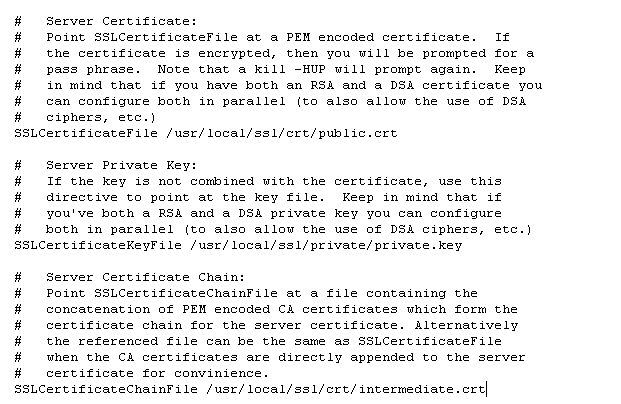
释符

保存退出，并重启 Apache。重启方式：

3、进入 Apache 安装目录下的 bin 目录，运行如下命令

./apachectl -k stop

./apachectl -k start

下附参照图一枚，图中的文件扩展名为.crt和.cer为通用格式。

【补充】

http访问--导向https,

【第一种办法】

http访问转到https,使用Rewrite 模块.

配置如下：

在 httpd.conf 中增加如下语句，如果有就不用加了

LoadModule rewrite\_module modules/mod\_rewrite.so

a)针对整站的

在 VirtualServer 加上如下语句：

RewriteEngine on

RewriteCond %{SERVER\_PORT} !^443$

RewriteRule ^(.\*)?$ https://%{SERVER\_NAME}/$1 [L,R]

b)针对某些目录的

在这个目录内，添加如下

RewriteEngine on

RewriteBase /test

RewriteCond %{SERVER\_PORT} !^443$

RewriteRule ^.\*$ https://%{SERVER\_NAME}%{REQUEST\_URI} [L,R]

【第二种办法】

另也可以在.htaccess添加如下语句来实现

RewriteEngine on

RewriteBase /test

RewriteCond %{SERVER\_PORT} !^443$

RewriteRule ^.\*$ https://%{SERVER\_NAME}%{REQUEST\_URI} [L,R]

最后重新启动apache服务，访问http测试成功转换成httpd