SSL 证书- Apache

设置 OCSP 装订

RegSSL

设置 OCSP 装订

OCSP 装订（英语：OCSP Stapling），是一个 TLS 证书状态查询扩展，作为在线证书状态协议的代替方法对 X.509 证书状态进行查询。服务器在 TLS 握手时发送事先缓存的 OCSP 响应，用户只需验证该响应的有效性而不用再向数字证书认证机构（CA）发送请求。

OCSP 装订需求 **Apache2.3.3** 版本或以上。

检测 Apache 版本

apache2 –v

1 设定

在设定档底下加入两行指令：

```
SSLUseStapling on
SSLStaplingCache "shmcb:/var/run/ocsp(128000)"
```

第二行 **SSLStaplingCache 指定快取的装置路径和记忆体大小。注意：如果 Apache 是安装在微软，**第二行指令设为 "*shmcb:C:/xampp/apache/logs/ocsp(128000)*"

以上二行指令必须在 <VirtualHost> … </VirtualHost> 挂号以外，避免 **Apache 无法重启。**

注意：若在服务器配置 OCSP 装订，终端服务器的 OCSP 请求必须默认允许连接到赛门铁克 OCSP 服务器。若您的服务器是安装在防火墙后端，则必须创建防火墙策略外接链接允许赛门铁克 OCSP。

使用 Openssl 工具验证终端服务器 ssl 证书与赛门铁克 OCSP 链接，请参考以下文档：

https://knowledge.symantec.com/support/mpki-for-ssl-support/index?page=content&actp=CROSSLINK&id=HOWTO111088

保存设定档，**重启 Apache。**

2 验证 OCSP 装订

只有 openssl 工具版本 0.9.8k 或以上才能验证 OCSP 装订。

```
# openssl s_client -connect yourdomain.com:443 -tls1 -tlsextdebug -status
```

范例显示结果：

```
OCSP response:
======================================
OCSP Response Data:
OCSP Response Status: successful (0x0)
```

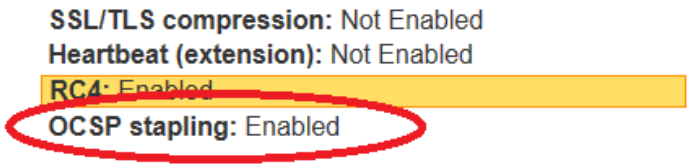
若显示以上结果说明 OCSP 装订已经配置成功，不成功则显示：

```
OCSP response:
======================================
OCSP response: no response sent
```

另一个验证是透过赛门铁克官网

https://cryptoreport.websecurity.symantec.com/checker/

OCSP 装订将显示 "**Enabled**" 或 "**Not Enabled**"



原本参考：https://knowledge.symantec.com/support/mpki-for-ssl-support/index?page=content&id=INFO2085&actp=search&viewlocale=en_US&searchid=1476953219028