Apache

SSL 인증서 설치 매뉴얼

- Apache 2.x -

CERT KOREA
씨트코리아

I. 사전 준비

1. 프로세스 및 Apache 버전 확인

✓ Apache 프로세스 확인

```
[root@certkorea  root]# ps  -ef|grep  httpd
root          14321          1      0      00:14:24        /usr/local/apache/bin        -DSSL
```

◎ 프로세스 위치가 /usr/sbin/httpd로 확인되는 경우, 환경설정파일(.conf)은 /etc/httpd/conf 나 /etc/httpd/conf.d 폴더에 있습니다.

✓ Apache 버전 확인

```
[root@certkorea  root]# cd  /usr/local/apache/bin
[root@certkorea  bin]# ./httpd  -v
Server  version : Apache/2.2.24(Unix)
Server built : Oct 24 2009 17:55:06
```

◎ ./httpd -v 명령어로 확인되지 않는 경우, ./apachectl -v 로 확인하시면 됩니다.
◎ Apache 1.3 버전에서는 SHA-1 알고리즘 인증서만 설치 가능합니다.

✓ SHA-2 알고리즘 인증서를 설치하시려면 Apache 2.0.63 이상 / openssl 0.9.8e 이상으로 버전업 하셔야 합니다.

I. 사전 준비

2. mod_ssl 확인 및 설치

✓정적 모듈(Statically)로 설치된 mod_ssl 확인

```
[root@certkorea  bin]# ./apachectl -l
Compiled in modules :
……
mod_ssl.c
……
[root@certkorea  bin]#
```

✓동적 모듈(DSO)로 설치된 mod_ssl 확인

```
[root@certkorea  bin]# ./apachectl -l
Compiled in modules :
……
mod_so.c
……
[root@certkorea  bin]# ls /usr/local/apache/modules
……
mod_ssl.so
……
[root@certkorea  bin]#
```

◎ . bin 폴더에 mod_so.c 파일이 있는지 확인한 후 modules 폴더에 mod_ssl.so 파일이 있는지 확인합니다.

✓ 위의 두가지 방법 모두 확인되지 않은 경우, 저희 써트코리아로 문의해 주시기 바랍니다.

I. 사전 준비

3. openssl 버전 확인

```
[root@certkorea  bin]# openssl version
OpenSSL  0.9.8e  04  May  2007
[root@certkorea  bin]
```

4. 인증서 파일 확인 및 저장

✓ 써트코리아를 통해 발급받은 인증서 파일을 확인합니다.

✓ Apache용 인증서는 다음과 같은 파일로 구성되어 있습니다.

◎ www.domain.com.crt : 인증서 파일(공개키)
◎ www.domain.com.key : 개인키 파일(비밀키)
◎ chainca.crt : 루트/중개인증서 파일(인증서 종류에 따라 다릅니다.)

5. 인증서 갱신 시

✓ 기존 인증서 파일 백업 〉 갱신된 인증서 업데이트 〉 Apache 서비스 재시작만 처리 하시면 됩니다.

Ⅱ. 인증서 설치

1. httpd.conf

✓ mod_ssl 모듈을 Load

```
#동적모듈
LoadModule          ssl_module              modules/mod_ssl.so
#해당 부분 주석을 해제
```

◎ mod_ssl이 정적모듈로 설치된 경우, LoadModule이나 AddModule 설정이 필요하지 않습니다.

✓ httpd-ssl.conf 파일을 Include

```
Include    extra/httpd-ssl.conf
혹은
<IfModule  mod_ssl.c>
Include    extra/httpd-ssl.conf
</IfModule>
#해당 부분 주석을 해제
```

Ⅱ. 인증서 설치

2. httpd-ssl.conf

✓ 443 포트를 Listen

```
Listen 443
```

✓ SSL 관련 VirtualHost 설정

```
<VirtualHost  *:443>
DocumentRoot  "/usr/local/htdocs"          ← DocumentRoot 동기화
ServerName  www.certkorea.co.kr:443        ← ServerName 동기화
……
SSLEngine on
SSLProtocol All -SSLv2 -SSLv3
SSLCipherSuite ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:AES128-SHA:AES256-
SHA:!RC4:HIGH:!MD5:!aNULL:!EDH

#인증서 파일의 위치를 지정합니다.
SSLCertificateFile /usr/local/apache/conf/ssl/www.certkorea.co.kr.crt
#개인키 파일의 위치를 지정합니다.
SSLCertificateKeyFile /usr/local/apache/conf/ssl/www.certkorea.co.kr.key
#루트/중개인증서 파일의 위치를 지정합니다.
SSLCACertificateFile /usr/local/apache/conf/ssl/chainca.crt
……
</VirtualHost>
```

Ⅱ. 인증서 설치

2. httpd-ssl.conf

◎ JkMount(mod_jk.so)를 이용해서 Tomcat과 연동 설정한 경우, SSL 관련 VirtualHost에도 동일하게 설정해주셔야 합니다.

◎ Wildcard / MDC(Multi-Domain) 인증서
-〉 Wildcard / MDC 인증서의 경우, ssl.conf 파일에 각 도메인의 VirtualHost 설정을 하고, 인증서 파일, 개인키 파일, 루트/중개인증서 파일, SSL 포트등 SSL관련 설정을 동일하게 처리하시면 됩니다.

3. 갱신설치

✓ 갱신 설치의 경우, 갱신 발급된 인증서 파일, 개인키 파일, 루트/중개인증서 파일로 교체하신 후, Apache 서비스만 재시작 하시면 됩니다.

Ⅱ. 인증서 설치

4. 서비스 재시작

✓ 구문 오류 체크

```
[root@certkorea  bin]# ./apachectl configtest
Syntax OK
```

◎ 구문 오류 체크 시 error가 발생하면, 해당 error에 대한 처리를 완료하신 후 Apache 서비스를 재시작 해야합니다. 에러 메세지를 저희 써트코리아로 보내주시면 처리 방법을 안내해 드리겠습니다.

✓ Apache 재시작

```
[root@certkorea  bin]# ./httpd  stop
/usr/local/apache/bin/apachectl stop : httpd stopped
[root@certkorea  bin]# ./httpd  start
```

◎ 1.3.x 버전에서 Apache 재시작 시 ./apachectl start 로 시작하시는 경우, SSL서비스가 같이 시작되지 않습니다. 반드시 ./apachectl startssl 로 재시작 하시기 바랍니다.

Ⅲ. 확인 및 테스트

1. 서비스 구동 확인

✓ ps -ef|grep httpd 명령어로 서비스가 정상 구동되었는지 확인합니다.

```
[root@certkorea  bin]# ps -ef|grep httpd
root      14321     1     0     00:00:12      /usr/local/apache/bin/httpd  -DSSL
```

2. SSL 포트 확인

✓ netstat 명령어로 SSL포트(기본 443)가 LISTEN 중인지 확인합니다.

```
[root@certkorea  bin]# netstat  -nap|grep  httpd
tcp      0     0:0:0:0:80          0:0:0:0:*         LISTEN      14321/httpd
tcp      0     0:0:0:0:443         0:0:0:0:*         LISTEN      14321/httpd
```

3. 방화벽 확인

✓ 사용하고 있는 방화벽에서 SSL포트(기본 443)를 80포트와 동일한 조건으로 OPEN 해주시기 바랍니다.

Ⅲ. 확인 및 테스트

4. 브라우저 테스트

✓ https로 사이트에 접속하여 자물쇠 및 인증서를 확인합니다.

Internet Explorer

Chrome

FireFox

◎ 영문회사명 표기 및 그린바는 EV 제품만 표시됩니다.
일반 SSL 인증서는 자물쇠 모양만 표시됩니다.

CERT KOREA 씨트코리아

Ⅳ. 문제해결

✓서비스 재시작 후 443 포트가 Listen 되지 않는 경우

◎ httpd.conf 에서 ssl_module이 Load 되었는지 확인합니다.
◎ httpd.conf 에서 httpd-ssl.conf 파일이 Include 되었는지 확인합니다.
◎ ssl.conf 에서 Listen 443이 설정되었는지 확인합니다.

✓서비스 재시작 후 http로 확인되는 페이지가 https로 접속 시 “403 Not Found” 오류가 발생하는 경우

◎ httpd.conf의 80포트 관련 Directory 설정을 ssl.conf 파일의 443포트 관련 VirtualHost에 복사해 주시면 됩니다.

✓Error_log

◎ 그 외의 문제가 발생할 경우 logs 폴더의 error_log를 확인하시고 오류구문을 써트코리아(support@certkorea.co.kr)로 보내주시기 바랍니다.

THANK YOU!

CERT KOREA
씨트코리아