KSIDC

KSIDC
Korea Server Hosting Inc

[Apache SSL 설치 메뉴얼]

코리아서버 호스팅
서비스 운영팀
고 현 숙

대한민국 E-Business 대표 브랜드 (주)코리아서버호스팅

@ 문서 개요

작성자 : 고현숙

작성일자 : 2011. 12

버전 : v1.0

개요 : Linux Server SSL인증키 설치 방법 및 신청 방법입니다.

@ 테스트 환경

OS : CentOS 5.6

APP : httpd-2.2.17, openssl-0.9.8e

SSL 이란 ?

- SSL (Secure Socket Layer) 프로토콜은 처음 Netscape 사에서 웹 서버와 브라우저 사이의 보안을 위하여 만들었습니다. SSL은 Certificate Authority(CA) 라 불리는 서드 파티로부터 서버와 클라이언트의 인증을 하는데 사용됩니다.

SSL 통신 절차

① 클라이언트가 서버에 접속하면 서버인증서를 전송 받습니다.

② 클라이언트는 받은 서버 인증서를 분석하여 신뢰할 수 있는 인증서인지를 검토한 뒤, 서버의 공개키를 추출합니다.

③ 클라이언트가 세션키로 사용할 임의의 메시지를 서버의 공개키로 암호화 하여 서버에 전송합니다.

④ 서버에서는 자신의 비밀키로 세션키를 복호화 하여 그 키를 사용하여 대칭키 암호화 방식으로 메시지를 암호화 하여 클라이언트와 통신하게 되며 이것은 "https" 라는 별도의 프로토콜을 사용하게 됩니다.

1. Apache 환경 확인

- Apache 버전 확인

root@localhost# ps –ef |grep httpd

```
[root@localhost SSL]# ps -ef |grep httpd
root     27125     1  0 14:48 ?        00:00:00 /usr/local/apache/bin/httpd -k start
nobody   27127 27125  0 14:48 ?        00:00:00 /usr/local/apache/bin/httpd -k start
nobody   27128 27125  0 14:48 ?        00:00:00 /usr/local/apache/bin/httpd -k start
nobody   27129 27125  0 14:48 ?        00:00:00 /usr/local/apache/bin/httpd -k start
nobody   27130 27125  0 14:48 ?        00:00:00 /usr/local/apache/bin/httpd -k start
nobody   27131 27125  0 14:48 ?        00:00:00 /usr/local/apache/bin/httpd -k start
root     27248 20311  0 15:21 pts/0    00:00:00 grep --color=auto httpd
[root@localhost SSL]#
```

root@localhost# /usr/local/apache/bin/httpd –v

root@localhost# rpm –qa |grep openssl

```
[root@localhost SSL]# /usr/local/apache/bin/httpd -v
Server version: Apache/2.2.17 (Unix)
Server built:   May 23 2011 14:27:35
[root@localhost SSL]# rpm -qa |grep openssl
openssl-0.9.8e-12.el5_5.7
openssl097a-0.9.7a-9.el5_4.2
openssl-devel-0.9.8e-12.el5_5.7
openssl-perl-0.9.8e-12.el5_5.7
openssl-0.9.8e-12.el5_5.7
openssl-devel-0.9.8e-12.el5_5.7
openssl097a-0.9.7a-9.el5_4.2
[root@localhost SSL]#
```

※ openssl 이 설치되어 있지 않은 경우, 설치해 주어야 합니다.

root@localhost# yum –y install openssl-*

- mod_ssl 모듈 확인

root@localhost# /usr/local/apache/bin/httpd –l

<정적으로 설치된 mod_ssl 모듈 확인 법>

```
[root@ns bin]# /usr/local/apache/bin/httpd -l
Compiled-in modules:
  mod_ssl.c
```

<동적으로 설치된 mod_ssl 모듈 확인 법>

```
[root@ns bin]# /usr/local/apache/bin/httpd -l
Compiled-in modules:
  mod_so.c
```

: Apache에 SSL 을 설치하기 위해서는 mod_ssl모듈이 설치되어 있어야 합니다.

Apache는 두 가지 방식으로 모듈 설치를 지원하고 있으며, 정적일 경우와 동적일 경우로 나뉩니다.

정적인 방식의 경우 mod_ssl.c 이 없을 경우, Apache를 재 설치하여야 합니다.

동적인 방식의 경우 mod_so.c 를 확인 하신 뒤, module 디렉터리 내에 mod_ssl.so 이 있는지 확인하셔야 합니다.

2. 개인키 생성

- SSL 인증서를 보관할 디렉터리로 이동한 뒤, 개인키를 생성합니다.

root@localhost# cd /home/SSL

root@localhost# openssl genrsa -des3 -out [개인키파일명].key 1024

[개인키 암호 입력]

```
[root@localhost ~]# cd /home/SSL
[root@localhost SSL]# openssl genrsa -des3 -out www.ksidc.net.key 1024
Generating RSA private key, 1024 bit long modulus
...++++++
.....................................................++++++
e is 65537 (0x10001)
Enter pass phrase for www.ksidc.net.key:
Verifying - Enter pass phrase for www.ksidc.net.key:
```

- 생성한 개인키로 csr 파일을 생성합니다.

root@localhost# openssl req -new -key [개인키파일명].key -out [CSR파일명].csr

```
[root@localhost SSL]# openssl req -new -key www.ksidc.net.key -out www.ksidc.net.csr
Enter pass phrase for www.ksidc.net.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:KR
State or Province Name (full name) [Berkshire]:Seoul
Locality Name (eg, city) [Newbury]:Seocho
Organization Name (eg, company) [My Company Ltd]:KSIDC
Organizational Unit Name (eg, section) []:IT
Common Name (eg, your name or your server's hostname) []:www.ksidc.net
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

예시) 도메인이 www.ksidc.net 일 경우,

Country Name (국가코드) [] : KR
State or Province Name (지역) [] : Seoul
Locality Name (시/군/구) [] : Seocho
Organization Name (회사명) [] : KSIDC
Organizational Unit Name (부서명) [] : IT
Common Name (서비스도메인명) [] : www.ksidc.net
Email Address [] :

- 개인키 및 CSR 파일 생성이 완료되었습니다.

```
[root@localhost SSL]# pwd
/home/SSL
[root@localhost SSL]# ls -l
합계 8
-rw-r--r-- 1 root root 643 12월  6 15:57 www.ksidc.net.csr
-rw-r--r-- 1 root root 963 12월  6 15:46 www.ksidc.net.key
[root@localhost SSL]#
```

- 생성한 CSR 파일 확인 방법

root@localhost# openssl req -noout -text -in [CSR파일명].csr

```
[root@localhost SSL]# openssl req -noout -text -in www.ksidc.net.csr
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=KR, ST=Seoul, L=Seocho, O=KSIDC, OU=IT, CN=www.ksidc.net
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:c8:fb:ac:9f:37:75:32:e5:af:fb:df:25:c3:39:
                    c8:65:22:8e:20:0f:6e:b8:47:83:e3:5a:4e:45:a2:
                    f5:0b:84:43:ab:80:31:1f:87:55:58:e7:a4:a6:3c:
                    d6:2f:2a:13:d5:86:e9:1b:0c:8f:13:da:d8:a3:0f:
                    30:a4:75:6e:9b:2e:94:0f:6c:66:7e:1d:db:88:9d:
                    76:63:a6:bd:43:b6:1b:27:78:31:57:0b:a6:f1:f3:
                    e7:53:51:87:95:48:87:c9:44:80:92:ee:c7:54:ee:
                    71:f7:b1:37:95:79:10:d5:a9:03:c1:4b:2e:09:52:
                    a0:04:c2:2c:90:58:15:8b:7f
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha1WithRSAEncryption
        9e:d4:56:41:b4:dc:ce:7f:a9:cf:da:0b:62:c1:8b:08:00:68:
        b5:83:b9:52:5e:00:3b:03:19:a4:0e:a1:5d:5a:a8:f3:43:ea:
        fe:bf:25:7f:f5:c0:66:2e:ab:e6:0c:71:a8:1a:82:1d:f7:64:
        31:8d:d9:e5:ff:9c:e3:bd:da:4a:1a:31:8e:6c:c5:f6:06:aa:
        e6:f7:c9:20:84:ae:5c:a9:d6:ca:f2:63:ec:be:b2:52:b3:97:
        75:08:9e:fc:29:d9:0b:56:e1:70:b2:9f:bb:08:da:c3:87:eb:
        33:cd:7e:3a:37:a4:12:bf:b9:d4:f8:ae:d1:23:53:f0:a4:da:
        15:97
```

- 생성한 CSR 파일의 내용을 복사하여, 인증서 발급기관에 발송하도록 합니다.

root@localhost# cat [CSR파일명].csr

```
[root@localhost SSL]# cat www.ksidc.net.csr
-----BEGIN CERTIFICATE REQUEST-----
MIIBozCCAQwCAQAwYzELMAkGA1UEBhMCS1IxDjAMBgNVBAgTBVNlb3VsMQ8wDQYD
VQQHEwZTZW9jaG8xDjAMBgNVBAoTBUtTSURDMQswCQYDVQQLEwJJVDEWMBQGA1UE
AxMNd3d3LmtzaWRjLm5ldDCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAyPus
nzd1MuWv+98lwznIZSKOIA9uuEeD41pORaL1C4RDq4AxH4dVwOekpjzWLyoT1Ybp
GwyPE9rYow8wpHVumy6UD2xmfh3biJ12Y6a9Q7YbJ3gxVwum8fPnU1GHlUiHyUSA
ku7HVO5x97E3lXkQ1akDwUsuCVKgBMIskFgVi38CAwEAAaAAMA0GCSqGSIb3DQEB
BQUAA4GBAJ7UVkGO3M5/qc/aC2LBiwgAaLWDuVJeADsDGaQOoV1aqPND6v6/JX/1
wGYuq+YMcagagh33ZDGN2eX/nOO92koaMY5sxfYGqub3ySCErlyp1sryY+y+slKz
l3UInvwp2QtW4XCyn7sI2sOH6zPNfjo3pBK/udT4rtEjU/Ck2hWX
-----END CERTIFICATE REQUEST-----
```

※ 복사한 CSR 파일 내용을 인증기관의 메일로 붙여 넣기 하여 보냅니다.
또는, 고객이 신청한 신청서와 인증서(CSR) 파일을 같이 첨부하여 인증기관 메일로 보냅니다.

※ 복사하여 붙여 넣을 때엔 '-----BEGIN' 부터 'REQUEST-----' 까지 모두 복사하여야 합니다.

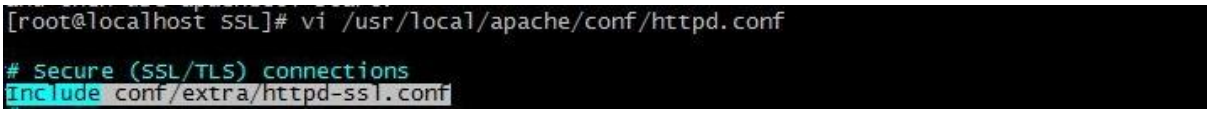
3. 인증서 설치

- 인증기관에서 발급 받은 인증서를 서버에 업로드 한 뒤, httpd.conf와 httpd-ssl.conf 을 수정합니다.

※ SSL 설정 파일 경로의 경우, Apache 버전 및 설치 환경에 따라 다르며, yum 으로 설치하셨을 경우, /etc/httpd/conf.d/ssl.conf 에 위치하고 있습니다.

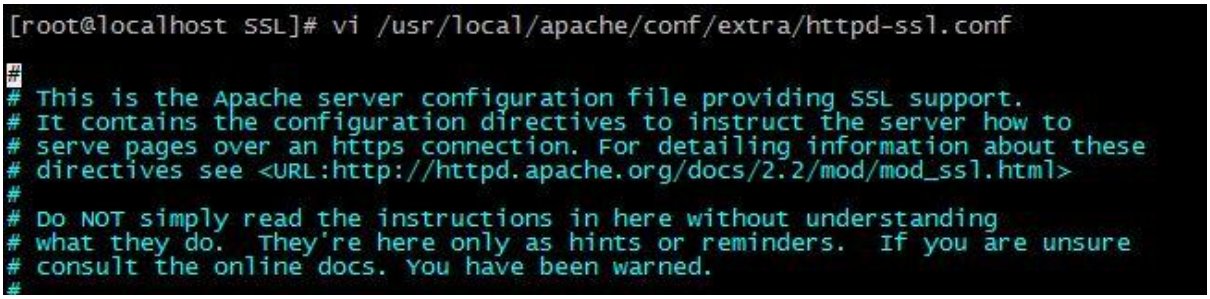
root@localhost# vi /usr/local/apache/conf/httpd.conf

Include conf/extra/httpd-ssl.conf 내용의 # 설정을 제거 하여 주석 처리된 부분 해제



- httpd-ssl.conf 파일에 인증서 경로 및 파일을 설정합니다.

root@localhost# vi /usr/local/apache/conf/extra/httpd-ssl.conf



예시) 기본 443포트로 인증서를 설치할 경우 httpd-ssl.conf 설정

Listen 443

---------- 중 략 ----------

<VirtualHost _default_:443>

---------- 중 략 ----------

DocumentRoot "/home/KSIDC" # 웹사이트의 홈디렉터리

ServerName www.ksidc.net:443 # 도메인:443

ServerAdmin ksidc@ksidc.net

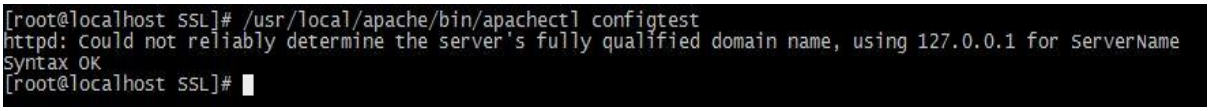
```
---------------------------------- 중 략 ----------------------------------

SSLCertificateFile /home/SSL/www.ksidc.net.crt   # 발급 받은 인증서
SSLCertificateKeyFile /home/SSL /www.ksidc.net.key   # 개인키
SSLCertificateChainFile /home/SSL /bundle.crt   # 체인인증서

---------------------------------- 중 략 ----------------------------------

</VirtualHost>
```

4. 서비스 재실행

- SSL에 대한 설정이 완료되었으며, 서비스를 재실행하여, 적용시킵니다.

- 서비스 재실행 전, 환경설정에 오류가 있는지 확인합니다.

root@localhost# /usr/local/apache/bin/apachectl configtest



※ Syntax OK 라고 메시지가 나와야 설정에 문제가 없을 경우 나오는 메시지, 아닐 경우 error 메시지 출력

- 설정 파일에 문제가 없을 경우, 아래 명령어를 실행하여 서비스를 재실행합니다.

root@localhost# /usr/local/apache/bin/apachectl restart

또는

root@localhost# /usr/local/apache/bin/apachectl startssl

5. 인증서 확인

- 웹 브라우저에서 https://도메인 입력시 인증서가 보이는지 확인해 주시기 바랍니다.

[추가 TIP]

1. 서버 개인키와 인증서 관련 명령어

구 분	명 령 어
Key 생성	openssl genrsa -dec3 -out 도메인.key 1024
Key 확인	openssl rsa -noout -text -in 도메인.key
CSR 생성	openssl req -new -key 도메인.key -out 도메인.csr
CSR 확인	openssl req -noout -text -in 도메인.csr
인증서 내용 확인	openssl x509 -noout -text -in 도메인.crt
원격지 인증서 확인	openssl s_client -connect URL:Port
Key 패스워드 변경	openssl rsa -des3 -in 도메인.key -out 도메인_new.key
Key 패스워드 삭제	openssl rsa -in 도메인.key -out 도메인_new.key
삭제한 패스워드 복구	openssl rsa -in 도메인.key -des3 -out 도메인_new.key

2. 인증서 형식 변환 명령어

구 분	명 령 어
DER을 PEM형식으로	x509 -in cert.cer -inform DER -out cert.pem -outform PEM
PEM을 DER형식으로	x509 -in cert.pem -inform PEM -out cert.der -outform DER
PFX에서 키 추출	pkcs12 -in filename.pfx -nocerts -out key.pem
PFX에서 인증서 추출	pkcs12 -in filename.pfx -clcerts -nokeys -out cert.pem