

APACHE INSTALL GUIDE

**2.X.X VERSION
INAMES CO. LTD.**

목차

1. 사전준비

- mod_ssl
- OpenSSL
- 인증서 파일

2. 주의사항

- 신규 및 갱신 구분
- CSR 직접 생성 여부

3. 인증서 설치

- httpd.conf 설정
- httpd-ssl.conf 설정
- 갱신 설치
- 서비스 재시작

4. 확인 및 테스트

- 서비스 구동 확인
- 네트워크 상태 확인
- 방화벽 확인
- 실제 브라우저 테스트

5. 이슈

- *:80
- 443 포트
- VirtualHost 대상
- Error_log

1. 사전준비

1. mod_ssl

- Apache에 SSL을 설정하려면 mod_ssl 이 꼭 필요합니다. 확인 방법은 2가지가 있습니다.

1. statically linking module 로 설치된 mod_ssl 모듈확인

```
[root@web1 root]# $HTTPD/bin/httpd -l
Compiled-in modules:
...
mod_ssl.c
...
[root@web1 root]#
```

웹서버에 설치된 모듈중에 mod_ssl.c 을 확인합니다.

2. DSO module 로 설치된 mod_ssl 모듈확인

```
[root@web1 root]# $HTTPD/bin/httpd -l
Compiled-in modules:
...
mod_so.c
...
[root@web1 root]# ls $HTTPD/module
mod_ssl.so ...
[root@web1 root]#
```

mod_so.c 가 포함되어 있는지 확인 후,
module 폴더 내에 mod_ssl.so 파일이 있는지 확인합니다.

1. 사전준비

2. OpenSSL

- OpenSSL 이 설치되어 있는지 확인합니다. 명령어로 간단히 확인할 수 있습니다.

```
[root@web1 root]# openssl version
OpenSSL 0.9.8e-fips-rhel5 01 Jul 2008
[root@web1 root]#
```

3. 인증서 파일

- 다운받은 인증서 파일을 확인합니다.
- 일반적으로 다음과 같은 파일로 구성되어 있습니다.

www.domain.com.crt (혹은 .cer)

www.domain.com.key

Verisign_bundle.crt (혹은 .cer)

- 1번째 파일이 인증서 파일입니다.
- 2번째 파일은 개인키(비밀키) 파일입니다.
- 3번째 파일은 루트 인증서 파일입니다.

2. 주의사항

1. 신규 및 갱신 구분

- 갱신 설치의 경우 "3-3 갱신 설치"로 건너뛰어 진행하시기 바랍니다.
- 신규 설치는 그대로 진행합니다.

2. CSR 직접 생성 여부

- CSR을 직접 생성하셨다면, Key 파일을 보관하고 있을 것입니다. key 파일의 유무를 먼저 확인하시고 다음으로 진행하시기 바랍니다.
- 다운받은 파일에 확장자가 .key 파일이 있는 경우 CSR을 직접 생성한 것이 아니기 때문에 무시하시고 그대로 진행하시면 됩니다.

3. 인증서 설치

1. httpd.conf

- Apache Conf 폴더에서 httpd.conf 파일을 엽니다.

1. mod_ssl 모듈을 Load하고 있는지 확인

```
...  
#LoadModule spelling_module modules/mod_spelling.so  
LoadModule ssl_module modules/mod_ssl.so  
#LoadModule status_module modules/mod_status.so  
...
```

mod_ssl.so 부분의 주석을 풀어주세요.

2. httpd-ssl.conf 파일을 Include 합니다.

```
# Secure (SSL/TLS) connections  
Include conf/extra/httpd-ssl.conf  
#  
# Note: The following must must be present to support  
# starting without SSL on platforms with no /dev/random equivalent  
# but a statically compiled-in mod_ssl.
```

httpd-ssl.conf 의 주석을 풀어주세요.

저장하고 httpd.conf 파일을 닫습니다.

1번의 mod_ssl 부분이 없는 경우 1-1-1 의 경우일 것입니다.
무시하시고 진행하시면 됩니다.

3. 인증서 설치

2. httpd-ssl.conf

- conf/extra 폴더에서 httpd-ssl.conf 파일을 엽니다.

1. VirtualHost 를 서버 구성에 맞게 수정합니다.

아래 예시를 참조하여 설정하시기 바랍니다.

```
<VirtualHost *:443>

#   General setup for the virtual host
DocumentRoot "/usr/local/apache2/htdocs"
#설명 : 루트가 되는 폴더의 위치를 지정해 줍니다.
ServerName www.domain.com:443
#설명 : 서버의 도메인을 입력해 줍니다.
ServerAdmin admin@domain.com
ErrorLog "/usr/local/apache2/logs/error.log"
TransferLog "/usr/local/apache2/logs/access.log"

...
중략
...

SSLCertificateFile "/usr/local/apache2/ssl/www.domain.com.crt"
#설명 : 인증서 파일의 위치를 지정해 줍니다.
SSLCertificateKeyFile "/usr/local/apache2/ssl/www.domain.com.key"
#설명 : 개인키 파일의 위치를 지정해 줍니다.
SSLCertificateChainFile "/usr/local/apache2/ssl/Verisign_bundle.crt"
#설명 : 루트 인증서 파일의 위치를 지정해 줍니다.

...
중략
...
</VirtualHost>
```

3. 인증서 설치

3. 갱신 설치

- 갱신 설치의 경우, 기존에 설치되어 있던 인증서 파일들을 새로 다운 받은 파일로 교체만 하시면 됩니다. 그 외에 수정할 부분은 없습니다.

4. 서비스 재시작

- 마지막으로 Apache를 재시작 하여 줍니다. (서버를 통째로 재시작 할 필요는 없습니다.)
- 재시작 하는 방법은 여러 가지가 있을 수 있습니다. 잘 동작하는 것으로 사용하시기 바랍니다.

```
[root@web1 root]# /usr/local/apache2/bin/httpd -t
```

```
Syntax OK
```

설명 : 설정에 구문 오류가 없는지 테스트

1번 방법

```
[root@web1 root]# /usr/local/apache2/bin/apachectl restart
```

```
[root@web1 root]# ps -ef | grep httpd
```

```
root 5465 5345 pts/1 00:00:00 grep httpd
```

```
root 2724 1 ? 00:00:13 /usr/local/apache2/bin/httpd -k start -DSSL
```

2번 방법

```
[root@web1 root]# /usr/local/apache2/bin/httpd -k stop
```

```
[root@web1 root]# /usr/local/apache2/bin/httpd -k start -DSSL
```

```
[root@web1 root]# ps -ef | grep httpd
```

```
root 5465 5345 pts/1 00:00:00 grep httpd
```

```
root 2724 1 ? 00:00:13 /usr/local/apache2/bin/httpd -k start -DSSL
```


4. 확인 및 테스트

1. 서비스 구동 확인

- `ps -ef | grep httpd` 명령어로 서비스가 구동되었는지 확인합니다. 아울러 `-DSSL` 옵션이 적용되었는지도 확인합니다.

```
[root@www bin]# ps -ef | grep httpd
root      5568      1   0 16:09 ?        00:00:00 /dotname/local/bin/httpd -k start -DSSL
nobody    5595    5568   0 16:11 ?        00:00:00 /dotname/local/bin/httpd -k start -DSSL
nobody    5602    5568   0 16:14 ?        00:00:00 /dotname/local/bin/httpd -k start -DSSL
root      5618    5345   0 16:18 pts/1    00:00:00 grep httpd
```

2. 네트워크 상태 확인

- `netstat` 명령어로 **443** 포트가 **LISTEN** 중인지 확인합니다.

```
[root@www bin]# netstat -anp | grep httpd
tcp        0      0 0.0.0.0:80          0.0.0.0:*        LISTEN      5568/httpd
tcp        0      0 0.0.0.0:443        0.0.0.0:*        LISTEN      5568/httpd
```

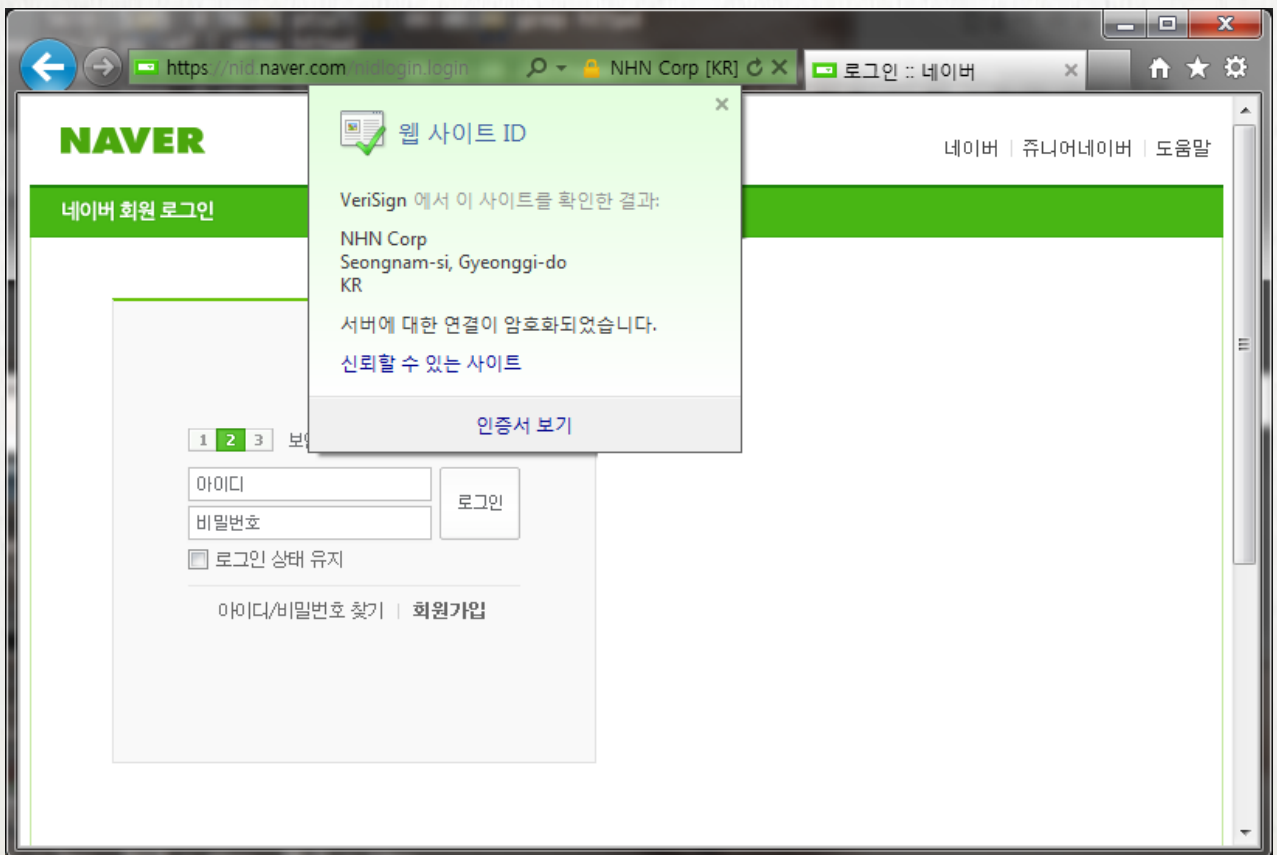
3. 방화벽 확인

- 사용하고 있는 방화벽 제어 프로그램(혹은 장비)에서 443 포트를 80포트와 동일하게 OPEN 하여 주시기 바랍니다.

4. 확인 및 테스트

4. 실제 브라우저 테스트

- 이제 인터넷 브라우저에서 HTTPS 접속을 테스트하여 보시기 바랍니다.
- 아래 이미지는 예시입니다.



4. 확인 및 테스트

4. 실제 브라우저 테스트

- <http://www.ssltest.net> 에서 좀 더 자세한 정보를 확인할 수 있습니다.



5. 이슈

1. *:80

- 설정을 마쳤으나 페이지가 열리지 않고 "페이지를 표시할 수 없습니다" (IE) ,
SSL 연결 오류입니다.(Chrome) 이라는 문구가 뜰 경우,
<http://www.domain.com:443> 으로 연결이 되는지 접속하여 보시기 바랍니다. 만일 연결이 된다면 VirtualHost 문제입니다.
사용중인 VirtualHost 들이
 <VirtualHost 192.168.1.5>
와 같이 설정되어 있을 것입니다. 이것을
 <VirtualHost 192.168.1.5:80>
와 같이 포트를 입력하여 주시기 바랍니다.

2. 443 포트

- 설정을 마치고 서비스는 시작되었지만 netstat 에서 443 포트가 LISTEN을 하지 않는 경우, 다음을 확인하여 보십시오
 1. httpd.conf 에서 Include 가 주석 해제 되었는지 (3.1 참조)
 2. httpd-ssl.conf 파일에 Listen 443 부분이 없는지 확인

3. VirtualHost 대상

- 설정은 모두 정상이나 아파치 서비스가 정상 구동이 되지 않을 경우 다음을 확인하여 보십시오
 1. httpd-ssl.conf 에 기술된 <VirtualHost *:443> 부분을
 <VirtualHost 192.168.1.5:443> 와 같이 IP로 변경하거나
 <VirtualHost www.domain.com:443> 같이 도메인으로 변경하거나
 <VirtualHost _default_:443> 로 설정하고 재시작하여 보십시오.

5. 이슈

5. Error_log

- 그 외의 문제가 발생할 경우 logs 폴더에 기록된 error_log 를 확인하여 문제점을 확인하여 주시기 바랍니다.
- 아래는 예시입니다.

[Error log]

Syntax error on line 117 of /usr/local/apache2/conf/extra/httpd-ssl.conf:
SSLCertificateFile: file '/usr/local/apache2/conf/www.domain.com.crt' does
not exist or is empty

#설명 : 파일명 기입에 오차가 발생하여 Syntax Error 가 발생하였다.