SECTIGO

Apache v2.2+ 버전 SSL인증서 설치 가이드 v3.0

2022.03

한국정보인증 KICASSL

KICA 한국정보인증

Contents

01 설치 전 준비 사항

02 SSL인증서 설치

03 SSL 인증서 설치 확인

04 SSL 암호화 통신 적용

05 주의사항 및 자주 발생하는 오류

※ 본 문서는 기본적인 참고용 자료이며, 구성환경에 따라 가이드 내용과 차이가 있을 수 있습니다.

※ SSL 인증서 설치를 위한 설정으로 관련 없는 설정에 대해서는 내용이 생략되어 있습니다.

01 설치 전 준비 사항

01 설치 전 준비 사항

SSL 인증서 준비

- 발급된 인증서는 메일 발송 (인증서 신청 시, 신청서에 기재한 신청자, 기술자에게 메일로 발송)
- 인증서 패스워드는 문자 발송 (패스워드는 별도 지정 요청하지 않을 경우, 임의로 생성)

- **Apache용 인증서 파일** 을 서버에 업로드 : 총 3개의 인증서 파일 제공
  - ① 도메인 인증서 : 도메인_cert.pem
  - ② 개인키 : 도메인_key.pem
  - ③ 루트 중개 인증서 : Chain_RootCA_Bundle.crt

  → 다른 형태로 발급되었다면, 발급 메일 회신으로 Apache용 인증서 파일 요청해주시기 바랍니다.

  참고사항) Chain_RootCA_Bundle.crt 는 ChainCA1.crt , ChainCA2.crt , RootCA.crt 총 3개의 인증서가 합쳐진 인증서 입니다.

FAQ

Q) 패스워드 정보를 못 받았는데 어떻게 해야되나요?
A) webmaster@kicassl.com으로 발급받으신 인증서 도메인명 기재하여, 인증서 패스워드 요청 주시면 확인 후 문자 발송해드립니다.

01 설치 전 준비 사항

확인 사항

- 인증서 타입별 주의사항

  싱글 / 멀티 / 와일드카드 도메인 SSL인증서에 따른 설치 방법 차이점

상품 종류	차이점
싱글 도메인	**한 서버에 복수**로 인증서 설치 시 단일 도메인 인증서는 **포트 공유 불가능**하지만, **Apache 2.2.12 버전 이상**부터는 **SNI 기능을 이용하여 포트 공유 가능**합니다. * SNI 기능 : Server Name Indication(서버 이름 표시) 의 줄임말로 하나의 포트에 2개 이상의 인증서 설정이 가능하게 해주는 기능
멀티 도메인	멀티 인증서에 등록된 도메인은 **포트 공유가 가능**하므로 NameVirtualHost 설정을 추가하시고, **<Virtual Host> ~ </Virtual Host> 구문을 설치할 도메인 수량에 맞추어 설정해주시면 됩니다.** 그 외 다른 내용은 동일합니다.
와일드카드 도메인	와일드카드 인증서는 **모든 서브도메인을 사용할 수 있고, 포트 공유가 가능**하므로 **NameVirtualHost** 설정을 추가하시고, **<Virtual Host>~</Virtual Host> 구문을 도메인에 따라 추가해주시길 바랍니다.** 그 외 다른 내용은 동일합니다.

- Apache 의 경우, 기본적으로 mod_ssl 모듈이 설치되어 있어야 합니다.
  - 정적모듈 or 동적모듈 중 하나로만 확인되면 됩니다.
  - 동적모듈의 경우, mod_sso.c 및 mod_ssl.so 둘 다 확인된 경우에만 SSL 적용 가능합니다.

- Windows 계열의 경우, 설치 방법이 상이 할 수 있으니 참고하시기 바랍니다.

02 SSL 인증서 설치

02 SSL 인증서 설치

Apache Config 파일(httpd.conf) 수정

› httpd.conf : 일반적으로 “apache 홈/conf ” 하위에 위치
(해당 위치에 없을 경우, 내부적으로 위치 확인 必)

1) httpd.conf 파일에서 mod_ssl 모듈을 Load

- LoadModule - mod_ssl.so 주석 제거

```
LoadModule ssl_module modules/mod_ssl.so
```

※ mod_ssl이 정적모듈로 설치된 경우, 이 부분은 생략 됩니다.

2) httpd.conf 파일에서 httpd-ssl.conf 파일을 Include

- Include - httpd-ssl.conf 주석 제거

```
Include conf/extra/httpd-ssl.conf
```

3) <IfModule ssl_module> ~ </IfModule> 주석 제거

```
<IfModule ssl_module>
SSLRandomSeed startup builtin
SSLRandomSeed connect builtin
</IfModule>
```

※ httpd.conf 파일에서 해당 부분을 주석해제 하거나, 추가합니다.

02 SSL 인증서 설치

Apache Config 파일(httpd-ssl.conf) 수정

› httpd-ssl.conf : 일반적으로 “apache 홈/conf/extra” 하위에 위치 (앞장에서 include한 ssl.conf파일)

1) Listen 포트

- SSL 사용 포트 설정(default port = 443)
- 다른 포트로 변경하셔도 되며, 지정하신 포트가 방화벽 등에 차단 포트 인지 확인해주시길 바랍니다.

```
Listen 443        ← 포트 설정
```

FAQ

Q) 패스워드 자동 설정은 어떻게 하나요?(OS가 리눅스일 경우)

A) 서버 재기동시 패스워드 입력 없이 자동 시작을 원하실 경우, shell script 파일을 생성하고 httpd-ssl.conf 파일에서 SSLPassPhraseDialog “경로/ssl_pass.sh” 를 추가하여 설정하면 됩니다.

```
[root@localhost bin]# vi 경로/ssl_pass.sh

#!/bin/sh
echo “인증서 패스워드”

:wq
```

.sh 파일은 chmod 700으로 파일권한 변경을 해야합니다.
복호화(패드워드 없는) 인증서 파일을 받으셨다면 해당 작업은 불필요합니다.

※ **OS가 윈도우일 경우**, 인증서 패스워드가 없는 복호화 키파일로 인증서 설치가 필요합니다.
복호화 인증서 파일은 webmaster@kicassl.com으로 도메인명 기재하여 요청주시면 됩니다.

02 SSL 인증서 설치

Apache Config 파일(httpd-ssl.conf) 수정

› httpd-ssl.conf : 일반적으로 “apache 홈/conf/extra” 하위에 위치 (앞장에서 include한 ssl.conf파일)

2) Virtual Host 설정

- Virtual Host, SSLEngine, SSLProtocol, SSLCipherSuite, SSLCertificateFile, SSLCertificateKeyFile, SSLCACertificateFile

```
NameVirtualHost *:443  ← IP기반일 시 제거

<VirtualHost *:443>
DocumentRoot "/usr/local/test/ "        ← http 설정과 동일한 디렉토리 (도메인 홈 디렉토리 설정)
ServerName www.kicassl.com:443          ← 해당 서버의 도메인
.....

#SSL 환경설정
SSLEngine on                            ← SSL 엔진 사용을 활성화
SSLProtocol –All +TLSv1.2 +TLSv1.3      ← 프로토콜 설정
.....

#발급받은 인증서 경로와 파일명을 지정
SSLCertificateFile “경로/인증서파일”      ← 도메인인증서(도메인명_cert.pem) 설정
SSLC                ertificateKeyFile “경로/개인키파일”      ← 개인키(도메인명_key.pem) 설정
SSLCertificateChainFile “경로/Chain_RootCA_Bundle.crt”   ← 중개루트인증서(Chain_RootCA_Bundle.crt) 설정
.....
</VirtualHost>
```

※ 멀티/와일드카드 인증서 설정 시, 각 도메인 별로 SSL VirtualHost를 설정하고, SSL 관련 설정을 동일하게 설정하시면 됩니다.

※ JkMount(mod_jk.so)를 이용해서 Tomcat과 연동되는 경우, 80포트의 JkMount 설정을 SSL 관련 VirtualHost에 동일하게 복사해야 합니다.

※ 갱신 설치 시, 기존 파일을 백업한 후 갱신된 인증서파일로 업로드 및 Apache 서비스 재시작 하시면됩니다.

FAQ

Q) 기존에 crt 확장자로 적용하였는데 어떻게 해야되나요?
A) Apache는 pem, crt 확장자 모두 설치 가능합니다.
crt 확장자로 설치를 원하실 경우,
오른쪽 마우스 클릭 - [이름바꾸기] 로 확장자 변경하여 설치 진행해주시면 됩니다.

Q) Chain_RootCA_Bundle.crt 도 교체해야되나요?
A) 네, 도메인 인증서, 개인키, 중개루트인증서 모두 발급받으신 인증서로 교체해주시기 바랍니다.

02 SSL 인증서 설치

Apache 웹서버 재기동

- 재기동 명령어로 서비스 재시작

```
[root@localhost bin]# ./apachectl stop
[root@localhost bin]# ./apachectl start
```

```
[root@localhost bin]# ./apachectl restart
```

  - 재기동 명령어는 서버마다 상이하며, 명령어 확인 후 진행 필

- 재기동시 오류가 발생하신다면 SSL 오류 로그 또는 오류 로그 확인 必

FAQ

Q) 서버 재기동 꼭 해야되나요?
A) 인증서파일과 설정파일을 변경하는 작업이므로 재기동이 필요 합니다.

03 SSL 인증서 설치 확인

03 SSL 인증서 설치 확인

서버에서 확인하는 방법

- 서비스 구동 확인
  - 아래 명령어로 서비스가 정상 구동되었는지 확인

```
[root@localhost bin]# ps-ef|grep httpd
root     14321   1        0        12:17:13        /usr/local/test/        -DSSL
```

- SSL 포트 확인
  - 아래 명령어로 SSL포트가 LISTEN 되는지 확인

```
[root@localhost 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
```

- Openssl 명령어로 확인
  - 아래 명령어로 서버에서 인증서 적용 여부를 확인
  - 명령어 : openssl s_client -connect 도메인:포트 | openssl x509 -noout -dates

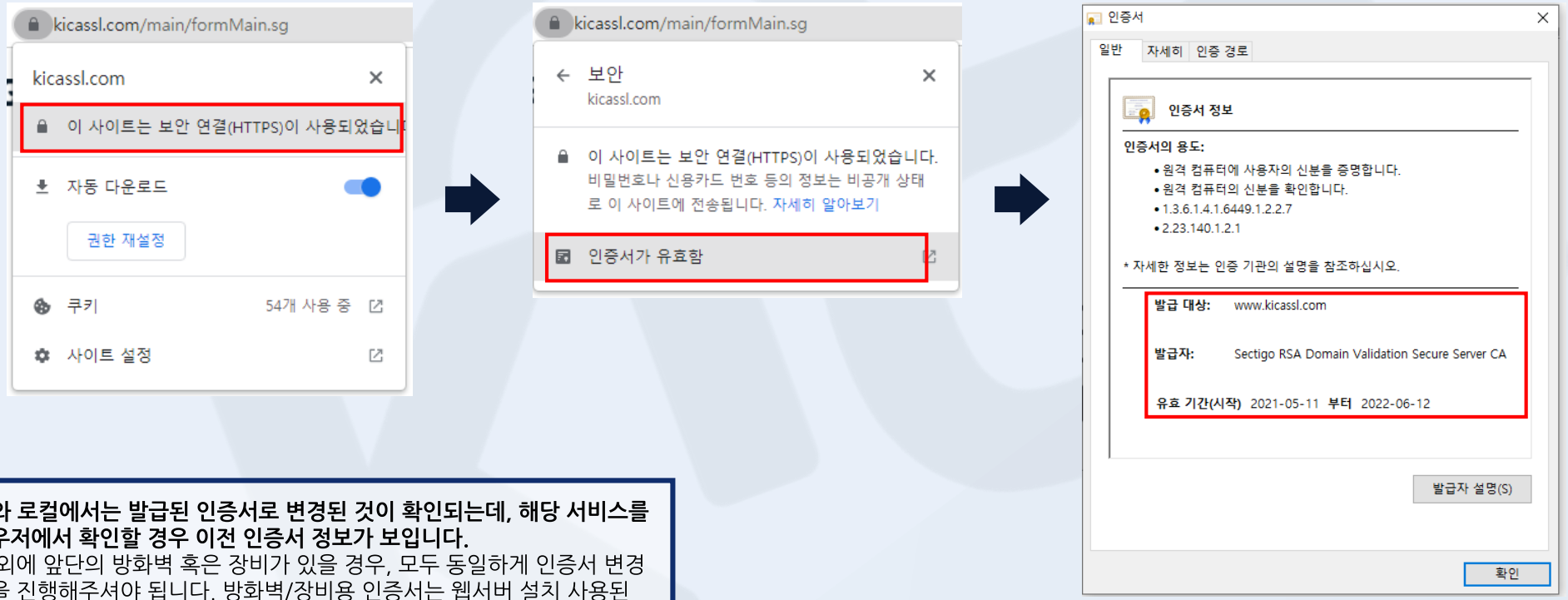
```
[root@localhost bin]# openssl s_client -connect www.kicassl.com:443 | openssl x509 -noout –dates
---
---

#발급받은 인증서 유효기간 일치 여부 확인
notBefore=May 11 00:00:00 2021 GMT
notAfter=Jun 12 23:59:59 2022 GMT
```

03 SSL 인증서 설치 확인

브라우저에서 확인하는 방법

› “https://도메인:포트” 로 접속 후, 자물쇠 및 https 통신 확인

- Chrome 브라우저 기준 인증서 정보 확인하는 방법



FAQ

Q) 서버와 로컬에서는 발급된 인증서로 변경된 것이 확인되는데, 해당 서비스를 브라우저에서 확인할 경우 이전 인증서 정보가 보입니다.

A) 서버 외에 앞단의 방화벽 혹은 장비가 있을 경우, 모두 동일하게 인증서 변경 작업을 진행해주셔야 됩니다. 방화벽/장비용 인증서는 웹서버 설치 사용된 인증서 형태와 상이할 수 있습니다. webmaster@kicassl.com으로 필요하신 인증서 확장자명 및 도메인명을 기재하여 요청주시면 변환하여 전달드립니다.

04 SSL 암호화 통신 적용

04 SSL 암호화 통신 적용

SSL 암호화 통신 웹 페이지 적용

› 부분 페이지 암호화

2) Virtual Host 설정

- 멀티/와일드카드 인증서 혹은 싱글 인증서 여러 개를 동일 포트에 설정 TIP
  - 나머지 도메인에 대한 Virtual Host 설정 :
    ① 기존 완성한 하나의 <VirtualHost> 블록을 복사
    ② DocumentRoot, ServerName, ServerAdmin, ErrorLog, TransferLog 항목만 적절하게 수정
  - 동일 포트로 설정하는 경우, Virtualhost 바깥쪽에 **NameVirtualHost 옵션**을 추가하여야 합니다.

```
NameVirtualHost *:443

<VirtualHost *:443>
DocumentRoot "/usr/local/test/ "
ServerName *.kicassl.com
ServerAlias  test.kicassl.com
.....
</VirtualHost>

<VirtualHost *:443>
DocumentRoot "/usr/local/test/ "
ServerName *.kicassl.com
ServerAlias  test2.kicassl.com
.....
</VirtualHost>
```

05 주의사항 및 자주 발생하는 오류

05 주의사항 및 자주 발생하는 오류

주의사항 (1/2)

윈도우 OS버전의 아파치에서 SSL인증서 작업 후 프로세스 기동이 안되는 경우

- mod-ssl 유무와 인증서 파일 확인 필요.
- Win32에서 SSLPassPhraseDialog 지시문 지원하지않아 패스워드가 지정되지않은 복호화파일로 인증서 설치 진행
- 복호화 인증서 파일은 KICASSL로 도메인명 기재하여 요청해주시기 바랍니다.

인증서와 개인키 keypair(키쌍)이 안 맞으면 인증서가 정상 로드되지 않음

- 발급 신청 시, 생성된 CSR과 매칭되는 개인키만 인증서와 사용가능

→ 개인키를 여러 번 생성 시, 신청 당시 기입한 최종 CSR과 매칭되는 개인키만 사용 가능

05 주의사항 및 자주 발생하는 오류

주의사항 (2/2)

1개의 서버에 여러 도메인(인증서) 사용시 주의사항”

- https(SSL)을 사용하는 포트는 설치한 인증서 수량과 같아야 합니다.

→ 2개의 인증서를 설치 시 2개의 각각 다른 포트가 필요함

- 와일드카드 SSL인증서 (*.kicassl.com), 멀티도메인 SSL인증서는 동일한 포트 공유가 가능한 SSL 인증서 입니다.

→ 멀티도메인 인증서 설치 후 인증서에 도메인을 추가 신청 시 인증서는 재설치 해야 합니다.

https 사용 포트를 “443”이 아닌 다른 포트를 지정하면 URL 입력 시 포트까지 입력

- 예시1) https://www.kicassl.com:**443**

→ “443’포트는 기본 SSL 포트이므로 생략이 가능함2개의 인증서를 설치 시 2개의 각각 다른 포트가 필요함

- 예시2) https://www.kicassl.com:**442**

→ “442’포트로 SSL 포트 설정 시 URL에 포트번호 필수 기입

※ 위에 기재된 포트는 예시로 입력한 포트로 사용하시려는 포트로 변경하시면 됩니다.

05 주의사항 및 자주 발생하는 오류

자주 발생하는 오류 (1/3)

```
[error] Init: Pass phrase incorrect
[error] SSL Library Error: 218529960 error:0D0680A8:asn1 encoding routines:ASN1_CHECK_TLEN:wrong tag
[error] SSL Library Error: 218640442 error:0D08303A:asn1 encoding routines:ASN1_TEMPLATE_NOEXP_D2I:nested asn1 error
[error] SSL Library Error: 218529960 error:0D0680A8:asn1 encoding routines:ASN1_CHECK_TLEN:wrong tag
[error] SSL Library Error: 218595386 error:0D07803A:asn1 encoding routines:ASN1_ITEM_EX_D2I:nested asn1 error
[error] SSL Library Error: 67710980 error:04093004:rsa routines:OLD_RSA_PRIV_DECODE:RSA lib
[error] SSL Library Error: 218529960 error:0D0680A8:asn1 encoding routines:ASN1_CHECK_TLEN:wrong tag
[error] SSL Library Error: 218595386 error:0D07803A:asn1 encoding routines:ASN1_ITEM_EX_D2I:nested asn1 error
```

인증서 갱신 후 서버 기동시 에러 메시지 발생

- 원인 : 패스워드를 자동 입력하여 서버를 시작하는 환경에서, 패스워드를 잘못 적은 경우 발생

→ 해결방법 : 패스워드 입력 부분을 확인하여 문자로 안내받은 패스워드 입력

(문자로 패스워드 수신 못하셨을 경우, KICASSL로 도메인 기재하여 문의주시기 바랍니다.)

안드로이드 v.5.0(롤리팝)+ 또는 구글 크롬 브라우저에서 https 접속 안될 시

- 원인 : SSL인증서가 아닌 TLS 프로토콜 확인

→ 해결방법 : 웹 서버에 SSL Protocol 중 TLS v1.2를 사용 가능하도록 수정하고 해당 웹 서버의 최신 보안패치 설치

(브라우저사 정책 변경으로 인하여 TLS v1.2이상 사용이 권고되어 해당 프로토콜 미지원 시 접속 안될 수 있습니다.)

05 주의사항 및 자주 발생하는 오류

자주 발생하는 오류 (2/3)

https 접속 시 딜레이가 길거나, 경고 메시지("인증서 해지 목록을 확인 할 수 없습니다.") 표시 오류

- 원인 : 사용자의 환경이 공용망이 아닌 경우, 외부 CRL 및 OCSP URL로 접속이 제한되어 있다면 브라우저가 SSL 인증서 관련 정보 탐색을 하지 못하여 발생

→ 해결방법 : 방화벽 등 네트워크 장비에서 관련 접속 URL(또는 IP) 및 port 를 open 하여 사용자가 원활히 접속하여 사용 할 수 있도록 작업 필요

(CRL, OCSP URL 정보는 인증서마다 다르므로 인증서 파일 상세 정보에서 "자세히" 탭 내용 중 "CRL 배포 지점", 기관 정보 액세스"에 기입된 URL을 확인하시길 바랍니다)

https접속 시 SSL 인증서가 웹 서버에 설치한 SSL 인증서가 아닌 다른 SSL 인증서가 로드 되는 오류

- 원인 : 설치하신 웹서버로 직접 접속하여 어떤 인증서를 로드 했는지 확인 필요

→ 해결방법 :

① 웹 서버 IP주소로 https://아이피:포트로 접속 후 표시되는 인증서 오류 화면에서 "계속 탐색" 클릭

② 웹브라우저에 로드된 SSL 인증서 정보를 확인 합니다.

③ 설치된 인증서가 표시된다면 L4, 방화벽 또는 웹 서버 앞 단에 장비에도 SSL 인증서 설치가 필요한지 확인이 필요합니다.

05 주의사항 및 자주 발생하는 오류

자주 발생하는 오류 (3/3)

해당 도메인 접속 시 "유효하지 않은 인증서" 라는 표시 발생 시

1) 폐쇄망 등 특정 환경의 사용자만 발생할 시

- 원인 : 중개인증서가 웹 서버에 설치의 문제가 있어서 사용자(접속자)에게 중개인증서를 전달해주지 못 할 때 발생할 수 있음
- 해결방법 : 중개인증서 본 가이드의 설치 부분을 확인해 주시길 바랍니다.

2) WIN XP, IE 8이하 등 낮은 버전 환경 또는 윈도우 업데이트를 하지 않은 사용자

- 원인 : 사용자(접속자)의 환경에 루트인증서가 존재하지 않아 발생할 수 있음
- 해결방법 : 윈도우에 내장된 윈도우 업데이트를 통해 윈도우 업데이트를 하거나, 첨부한 RootCA.crt 파일을 직접 사용자PC에 수동 설치해야 합니다.

해당 도메인 접속 시 "만료된 인증서" 라는 표시 발생 시

- 해결방법 :
  ① 해당 도메인의 접속한 사용자 PC의 시간이 현재 시간인지 확인해주시길 바랍니다.
  ② 해당 도메인에 설치된 인증서 정보창을 띄워 해당 인증서의 만료일을 확인해주시기 바랍니다.
  ※ 도메인 인증서 갱신을 했는데도 발생한 경우, 방화벽 또는 L4 등 다른 장비에 인증서 설치가 필요한지 확인해주시길 바랍니다.

해당 도메인 접속 시 "폐기된 인증서" 라는 표시 발생 시

- 해결방법 : 인증서가 폐기 또는 해지된 경우 KICASSL에 발급받으신 인증서 도메인명 기재하여 문의 해주시길 바랍니다.

감사합니다.

KICA 한국정보인증

www.kicassl.com ☎ 대표전화 : 02-360-3065 ✉ 이메일 : webmaster@kicassl.com