CSR 생성 및 CMS에 인증서 적용

목차

소개

이 문서에서는 CSR(Certificate Signing Request)을 생성하고 Cisco CMS(Meeting Server)에 서명된 인증서를 업로드하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- CMS 서버에 대한 기본 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Putty 소프트웨어 또는 이와 유사한 소프트웨어
- CMS 2.9 이상

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

CSR 생성

CSR을 생성하는 방법에는 두 가지가 있습니다. 그중 하나는 관리자 액세스 권한을 사용하여 CLI(Command Line Interface)에서 CMS 서버에 직접 CSR을 생성하는 것이며, 다른 하나는 Open SSL과 같은 외부 서드파티 CA(Certificate Authority)를 사용하여 생성하는 것입니다.

두 경우 모두 CMS 서비스가 제대로 작동하려면 올바른 구문으로 CSR을 생성해야 합니다.

1단계. 구문 구조

```
pki csr <key/cert basename> <CN:value> [OU:<value>] [O:<value>] [ST:<-value>] [C:<value>] [subjectAltNam
```

- <key/cert basename> 은 새 키와 CSR 이름을 식별하는 문자열입니다. 영숫자, 하이픈 또는 밑줄 문자를 포함할 수 있습니다. 필수 필드입니다.
- <CN:value>는 공용 이름입니다. DNS(Domain Name System)에서 서버의 정확한 위치를 지정하는 FQDN(Fully Qualified Domain Name)입니다. 필수 필드입니다.
- [OU:<값>]은 조직 단위 또는 부서 이름입니다. 예를 들면 지원, IT, 엔지니어, 파이낸스 등입니다. 선택 필드입니다.
- [O:<value>]는 조직 또는 비즈니스 이름입니다. 보통 합법적으로 설립된 회사의 이름입니다. 선택 필드입니다.
- [ST:<값>]은 도, 지역, 군 또는 주입니다. 예를 들면, 버킹엄셔 캘리포니아입니다. 선택 필드입니다.
- [C:<value>]는 국가입니다. 조직이 위치한 국가의 두 글자로 된 국제 표준화 기구(ISO) 코드. 예: US, GB, FR. 선택 필드입니다.
- [subjectAltName:<value>]은(는) SAN(주체 대체 이름)입니다. X509 버전 3(RFC 2459)에서 SSL(Secure Socket Layers) 인증서는 인증서가 일치해야 하는 여러 이름을 지정할 수 있습니다. 이 필드를 사용하면 생성된 인증서가 여러 도메인을 포함할 수 있습니다. IP 주소, 도메인 이름, 이메일 주소, 일반 DNS 호스트 이름 등을 쉼표로 구분하여 포함할 수 있습니다. 지정된 경우 이 목록에 CN도 포함해야 합니다. 이 필드는 선택 사항이지만 XMPP(Extensible Messaging and Presence Protocol) 클라이언트가 인증서를 수락하려면 SAN 필드를 완료해야 합니다. 그렇지 않으면 XMPP 클라이언트가 인증서 오류를 표시합니다.

2단계. callbridge, xmpp, webadmin 및 webbridge CSR을 생성합니다.

1. Putty로 CMS CLI에 액세스하고 admin 계정으로 로그인합니다.
2. CMS에 필요한 모든 서비스에 대해 CSR을 생성하려면 다음 명령을 실행합니다. 와일드카드(*.com)가 있거나 클러스터 FQDN이 CN인 단일 인증서를 생성하고 각 CMS 서버의 FQDN을 사용하며 필요한 경우 URL에 조인하는 것도 허용됩니다.

서비스	코만드
웹 관리자	pki csr <cert name> CN:<server FQDN>

웹브리지	pki csr <cert name> CN:<Server FQDN> subjectAltName:<Join Url>,<XMPP domain>
캘브리지 회전 로드 밸런서	pki csr <cert name> CN:<Server FQDN's>

3. CMS가 클러스터링된 경우 다음 명령을 실행합니다.

서비스	명령을 사용합니다
캘브리지 회전 로드 밸런서	pki csr <cert name> CN:<cluster FQDN> subjectAltName:<Peer FQDN's>
XMPP	pki csr <cert name> CN:<Cluster FQDN> subjectAltName:<XMPP Domain>,<Peer FQDN's>

3단계. 데이터베이스 클러스터 CSR을 생성하고 내장 CA를 사용하여 서명합니다.

CMS 2.7부터는 데이터베이스 클러스터에 대한 인증서가 있어야 합니다. 2.7에서는 데이터베이스 인증서 서명에 사용할 수 있는 내장 CA가 포함되었습니다.

1. 모든 코어에서 를 실행합니다database cluster remove.

- 기본에서 를 실행합니다pki selfsigned dbca CN. 예: **Pki selfsigned dbca CN:tplab.local**
- 기본에서 를 실행합니다pki csr dbserver CN:cmscore1.example.com subjectAltName. 예: cmscore2.example.com,cmscore3.example.com
- Primary에서 데이터베이스 클라이언트에 대한 인증서를 생성합니다 pki csr dbclient CN:postgres .
- Primary에서 dbca를 사용하여 dbserver 인증서를 서명합니다 **pki sign dbserver dbca** .
- 기본에서 dbca를 사용하여 dbclient cert에 서명합니다pki sign dbclient dbca.
- 데이터베이스 노드에 연결해야 하는 모든 서버에 dbclient.crt를 복사합니다
- 데이터베이스(데이터베이스 클러스터를 구성하는 노드)에 조인된 모든 서버에 dbserver.crt 파일을 복사합니다
- dbca.crt 파일을 모든 서버에 복사합니다.

- 기본 DB 서버에서 를 실행합니다database cluster certs dbserver.key dbserver.crt dbclient.key dbclient.crt dbca.crt. 이 경우 를 dbca.crt 로 사용합니다root ca-cert.

- 기본 DB 서버에서 를 실행합니다database cluster localnode a.

- 기본 DB 서버에서 를 실행합니다database cluster initialize.

- 기본 DB 서버에서 를 실행합니다database cluster status. 노드: (me): Connected Primary를 확인해야 합니다.

- 데이터베이스 클러스터에 가입된 다른 모든 코어에서 를 실행합니다database cluster certs dbserver.key dbserver.crt dbclient.key dbclient.crt dbca.crt.

- 데이터베이스 클러스터에 연결된(데이터베이스와 함께 위치하지 않은) 모든 코어에서 다음을 실행합니다 **database cluster certs dbclient.key cbclient.crt dbca.crt** .

- 조인된(데이터베이스와 함께 배치된) 코어에서:

    - 실행. database cluster localnode a

        - 실행.database cluster join

- 연결된 코어(데이터베이스와 함께 위치하지 않음):

    - ru 해당 database cluster localnode a .

        - 실행. database cluster connect

4단계. 서명된 인증서를 확인합니다.

- 인증서 유효성(만료일)은 인증서 검사로 확인할 수 있으며 명령을 실행합니다**pki inspect <filename>** .

    - 인증서가 개인 키와 일치하는지 검증하고 명령을 실행할 수 있습니다pki match <keyfile> <certificate file>.
    - 인증서가 CA에 의해 서명되었는지, 그리고 인증서 번들을 사용하여 인증서를 어설션할 수 있는지 검증하려면 명령을 pki

verify <cert> <certificate bundle/Root CA> 실행합니다.

5단계. 서명된 인증서를 CMS 서버의 구성 요소에 적용합니다.

1. Webadmin에 인증서를 적용하려면 다음 명령을 실행합니다.

```
webadmin disable
webadmin certs <keyfile> <certificate file> <certificate bundle/Root CA>
webadmin enable
```

2. Callbridge에 인증서를 적용하려면 다음 명령을 실행합니다.

```
callbridge certs <keyfile> <certificate file> <certificate bundle/Root CA>
callbridge restart
```

3. Webbridge에 인증서를 적용하려면 다음 명령을 실행합니다.

```
webbridge disable
webbridge certs <keyfile> <certificate file> <certificate bundle/Root CA>
webbridge enable
```

4. 인증서를 XMPP에 적용하려면 다음 명령을 실행합니다.

```
xmpp disable
xmpp certs <keyfile> <certificate file> <certificate bundle/Root CA>
xmpp enable
```

5. 데이터베이스에 인증서를 적용하거나 현재 DB 클러스터에서 만료된 인증서를 바꾸려면 다음 명령을 실행합니다.

```
database cluster remove (on all servers, noting who was primary before beginning)
database cluster certs <server_key> <server_certificate> <client_key> <client_certificate> <Root ca_crt
database cluster initialize     (only on primary node)
database cluster join <FQDN or IP of primary>    (only on slave node)
database cluster connect <FQDN or IP of primary> (only on nodes that are not part of the database clust
```

6. 인증서를 TURN에 적용하려면 다음 명령을 실행합니다.

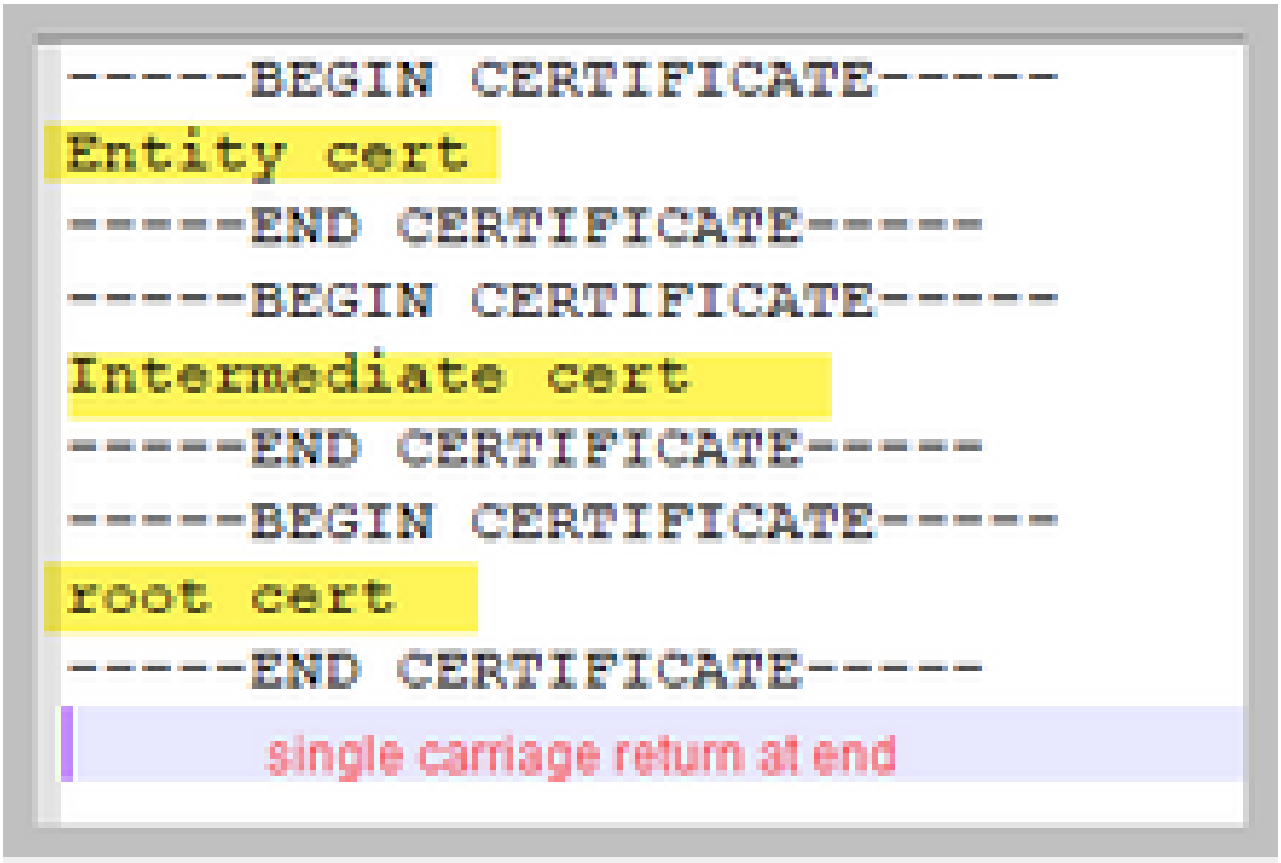
```
turn disable
turn certs <keyfile> <certificate file> <certificate bundle/Root CA>
turn enable
```

인증서 신뢰 체인 및 번들

CMS 3.0부터는 Certificate Trust Chains 또는 Full Chain Trust를 사용해야 합니다. 또한 번들을 만들 때 인증서가 어떻게 구축되는지 인식하는 것은 모든 서비스에 중요합니다.

웹 브리지 3에 필요한 대로 인증서 신뢰 체인을 작성할 때 이미지에 표시된 대로 엔티티 인증서를 위에 두고 중간을 두고 아래쪽에 루

트 CA를 둔 다음 단일 캐리지 리턴을 수행해야 합니다.



번들을 생성할 때마다 인증서에는 끝에 캐리지 리턴이 하나만 있어야 합니다.

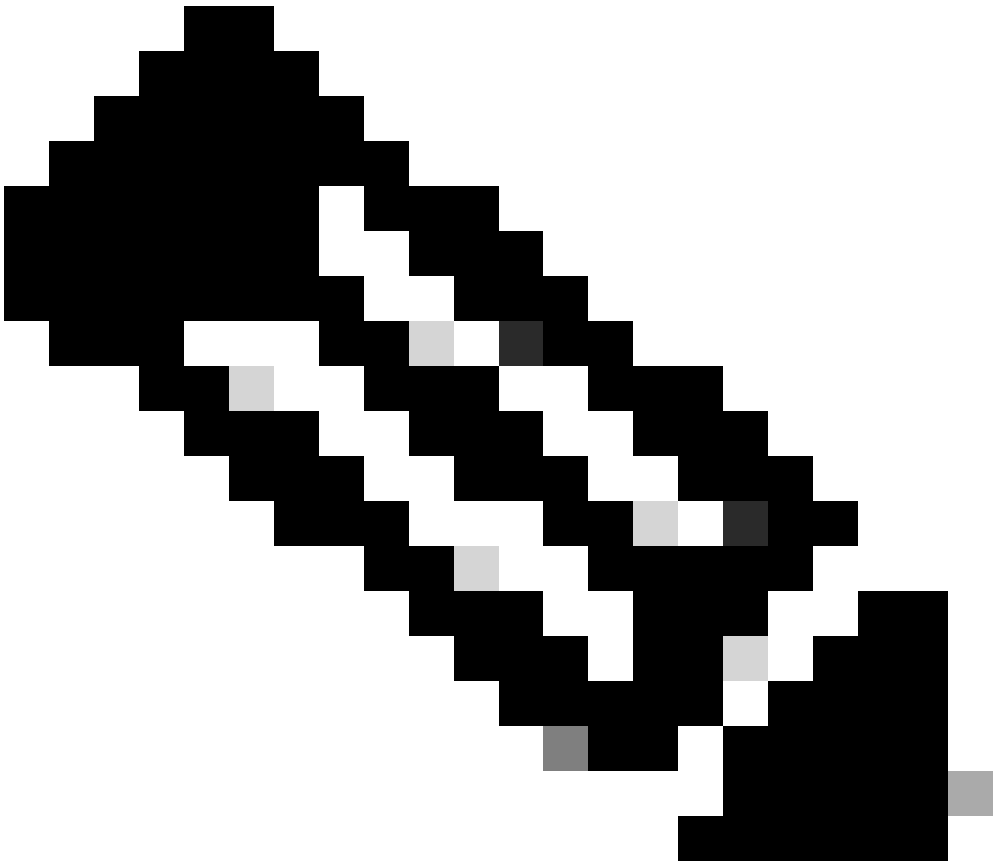
CA 번들은 이미지에 표시된 것과 동일하며, 물론 엔티티 인증서가 없습니다.

문제 해결

데이터베이스 인증서를 제외한 모든 서비스에 대해 만료된 인증서를 교체해야 하는 경우 가장 쉬운 방법은 이전 인증서와 이름이 같은 새 인증서를 업로드하는 것입니다. 이렇게 하면 서비스를 다시 시작해야 하며 서비스를 재구성할 필요가 없습니다.

인증서 이름이 현재 키와 일치하면 수행pki csr ... 즉시 서비스가 중단됩니다. 프로덕션이 라이브 상태이고 사전 대응적으로 새 CSR 및 키를 생성하는 경우 새 이름을 사용합니다. 서버에 새 인증서를 업로드하기 전에 현재 활성 이름의 이름을 변경할 수 있습니다.

데이터베이스 인증서가 만료 된 경우 기본 데이터베이스가 **database cluster status** 누구인지를 확인 하고 모든 노드에서 명령을 실행 database cluster remove 합니다. 그런 다음 3 단계의 지침을 사용 할 수 있습니다. 데이터베이스 클러스터 CSR을 생성하고 내장 CA를 사용하여 서명합니다.



참고: CMM(Cisco Meeting Manager) 인증서를 갱신해야 하는 경우 다음 비디오인 Cisco Meeting Management SSL 인증서 업데이트를 참조하십시오.

관련 정보

- **Cisco 기술 지원 및 다운로드**

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.