CSRの生成とCMSへの証明書の適用

内容

はじめに

このドキュメントでは、証明書署名要求(CSR)を生成し、署名付き証明書をCisco Meeting Server(CMS)にアップロードする方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- CMSサーバの基礎知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Puttyまたは同様のソフトウェア
- CMS 2.9以降

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

CSRの生成

CSRを生成するには2つの方法があります。1つは、管理アクセス権を持つコマンドラインインターフェイス(CLI)からCMSサーバ上に直接CSRを生成する方法で、もう1つは、Open SSLなどの外部サードパーティ認証局(CA)を使用する方法です。

どちらの場合も、CMSサービスが正しく動作するためには、正しい構文を使用してCSRを生成する必要があります。

ステップ 1：構文構造。

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

- <key/cert basename>は、新しいキーとCSR名を識別する文字列です。英数字、ハイフン、アンダースコアを含めることができます。これは必須フィールドです。
- <CN:value>は共通名です。これは、ドメインネームシステム(DNS)内のサーバの正確な場所を指定する完全修飾ドメイン名(FQDN)です。これは必須フィールドです。
- [OU:<value>]は組織単位(OU)または部署名です。たとえば、サポート、IT、エンジニア、財務などです。これはオプションのフィールドです。
- [O:<value>]は組織名または会社名です。 通常は、法的に設立された会社の名前。これはオプションのフィールドです。
- [ST:<value>]は、州、地域、郡、または州です。 たとえば、Buckinghamshire Californiaです。 これはオプションのフィールドです。
- [C:<value>]は国です。貴社が所在する国の2文字の国際標準化機構(ISO)コード。たとえば、US、GB、FRなどです。これはオプションのフィールドです。
- [subjectAltName:<value>]は、サブジェクト代替名(SAN)です。 X509バージョン3(RFC 2459)からは、Secure Socket Layer(SSL)証明書は、証明書が一致する必要がある複数の名前を指定できます。このフィールドにより、生成された証明書が複数のドメインをカバーできるようになります。これには、IPアドレス、ドメイン名、電子メールアドレス、通常のDNSホスト名などをカンマで区切って含めることができます。指定する場合は、このリストにCNも含める必要があります。このフィールドはオプションですが、Extensible Messaging and Presence Protocol(XMPP)クライアントが証明書を受け入れるようにするには、SANフィールドに入力する必要があります。入力しない場合は、XMPPクライアントに証明書エラーが表示されます。

ステップ 2：callbridge、xmpp、webadmin、およびwebbridge CSRを生成します。

1. Puttyを使用してCMS CLIにアクセスし、管理者アカウントでログインします。
2. 次のコマンドを実行して、CMSで必要なすべてのサービスに対してCSRを作成します。必要に応じて、ワイルドカード(*.com)またはクラスタFQDNをCNとして持つ単一の証明書、各CMSサーバのFQDN、および参加URLを作成することもできます。

サービス	コマンド
Web管理者	pki csr <cert name> CN:<server FQDN>
Webブリッジ	pki csr <cert name> CN:<Server FQDN> subjectAltName:<Join Url>,<XMPP domain>
コールブリッジ 回転 ロードバランサ	pki csr <cert name> CN:<Server FQDN's>

3. CMSがクラスタ化されている場合は、次のコマンドを実行します。

サービス	コマンド
コールブリッジ 回転 ロードバランサ	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>

ステップ 3：データベースクラスタCSRを生成し、組み込みCAを使用して署名します。

CMS 2.7以降では、データベースクラスタ用の証明書が必要です。 2.7では、データベース証明書の署名に使用できる組み込みCAを組み込みました。

1. すべてのコアで、 database cluster removeを実行します。

   - プライマリで、pki selfsigned dbca CNを実行します。以下に例を挙げます。 **Pki selfsigned dbca CN:tplab.local**

   - プライマリで、pki csr dbserver CN:cmscore1.example.com subjectAltNameを実行します。例：cmscore2.example.com,cmscore3.example.com

- プライマリで、データベースクライアントの証明書を作成します pki csr dbclient CN:postgres 。
- プライマリで、dbcaを使用してdbserver証明書に署名します **pki sign dbserver dbca** 。
- プライマリで、dbcaを使用してdbclient certpki sign dbclient dbcaに署名します。
- dbclient.crtを、データベース・ノードに接続する必要があるすべてのサーバにコピーします
- データベースに参加しているすべてのサーバ（データベース・クラスタを構成するノード）にdbserver.crtファイルをコピーします
- dbca.crtファイルをすべてのサーバにコピーします。
- プライマリDBサーバで、database cluster certs dbserver.key dbserver.crt dbclient.key dbclient.crt dbca.crtを実行します。ここでは、 dbca.crtをroot ca-certとして使用します。
- プライマリDBサーバで、database cluster localnode aを実行します。
- プライマリDBサーバで、database cluster initializeを実行します。
- プライマリDBサーバで、database cluster statusを実行します。「Must see Nodes: (me): Connected Primary」というメッセージが表示されます。
- データベースクラスタに参加している他のすべてのコアで、database cluster certs dbserver.key dbserver.crt dbclient.key dbclient.crt dbca.crtを実行します。
- データベースクラスタに接続されているすべてのコア（データベースと共存していないコア）で、を実行します。**database cluster certs dbclient.key cbclient.crt dbca.crt** .
- 参加している（データベースと同じ場所に配置されている）コア：
    - run. database cluster localnode a
        - run.database cluster join
- 接続されている（データベースと同じ場所に配置されていない）コア：
    - ru n database cluster localnode a 。
        - run. database cluster connect

ステップ 4：署名付き証明書を確認します。

- 証明書の有効性（有効期限）は、証明書インスペクションを使用して確認できます。**pki inspect <filename>** コマンドを実行します。

  - 証明書が秘密キーと一致することを検証するには、pki match <keyfile> <certificate file>コマンドを実行します。

  - 証明書がCAによって署名されており、証明書バンドルをその証明書のアサートに使用できることを検証するには、pki verify <cert> <certificate bundle/Root CA>コマンドを実行します。

ステップ 5：CMSサーバのコンポーネントに署名付き証明書を適用します。

1. 証明書をWebadminに適用するには、次のコマンドを実行します。

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

2. 証明書をCallbridgeに適用するには、次のコマンドを実行します。

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

3. 証明書をWebbridgeに適用するには、次のコマンドを実行します。

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

4. 証明書をXMPPに適用するには、次のコマンドを実行します。

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

5. 証明書をデータベースに適用するか、現在のDBクラスタで期限切れの証明書を置き換えるには、次のコマンドを実行します。

```
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
```

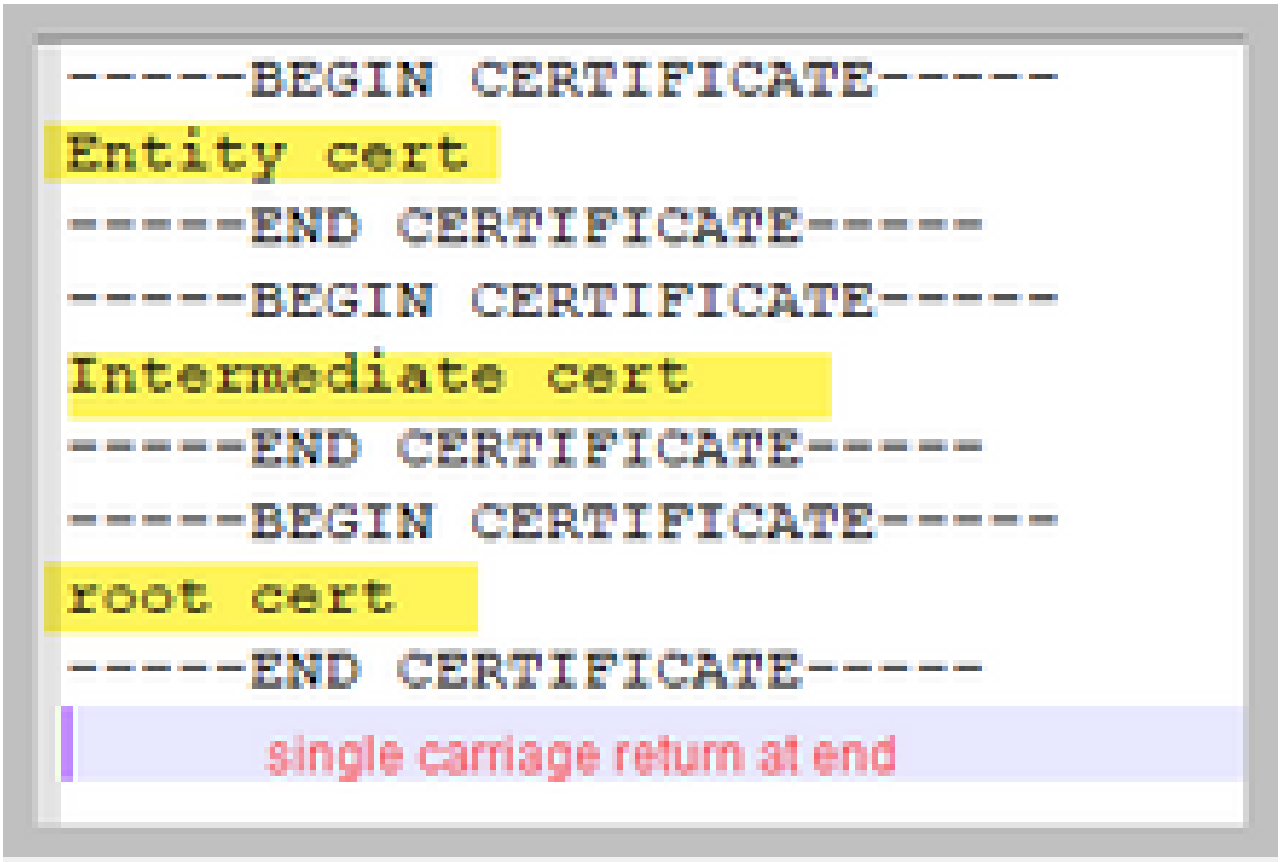
6. 証明書をTURNに適用するには、次のコマンドを実行します。

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

証明書信頼チェーンおよびバンドル

CMS 3.0以降では、証明書信頼チェーンまたは完全なチェーンの信頼を使用する必要があります。 また、バンドルの作成時に証明書がどのように構築されるかを認識するサービスを作成することも重要です。

証明書信頼チェーンを構築する場合、Web Bridge 3の要件に従って、図に示すように、エンティティ証明書を上、中間に中間証明書、下部にルートCA、単一のキャリッジリターンを指定して構築する必要があります。



バンドルを作成する場合は、証明書の末尾にキャリッジリターンが1つだけ必要です。

CAバンドルは図に示すように同じですが、当然、エンティティ証明書はありません。

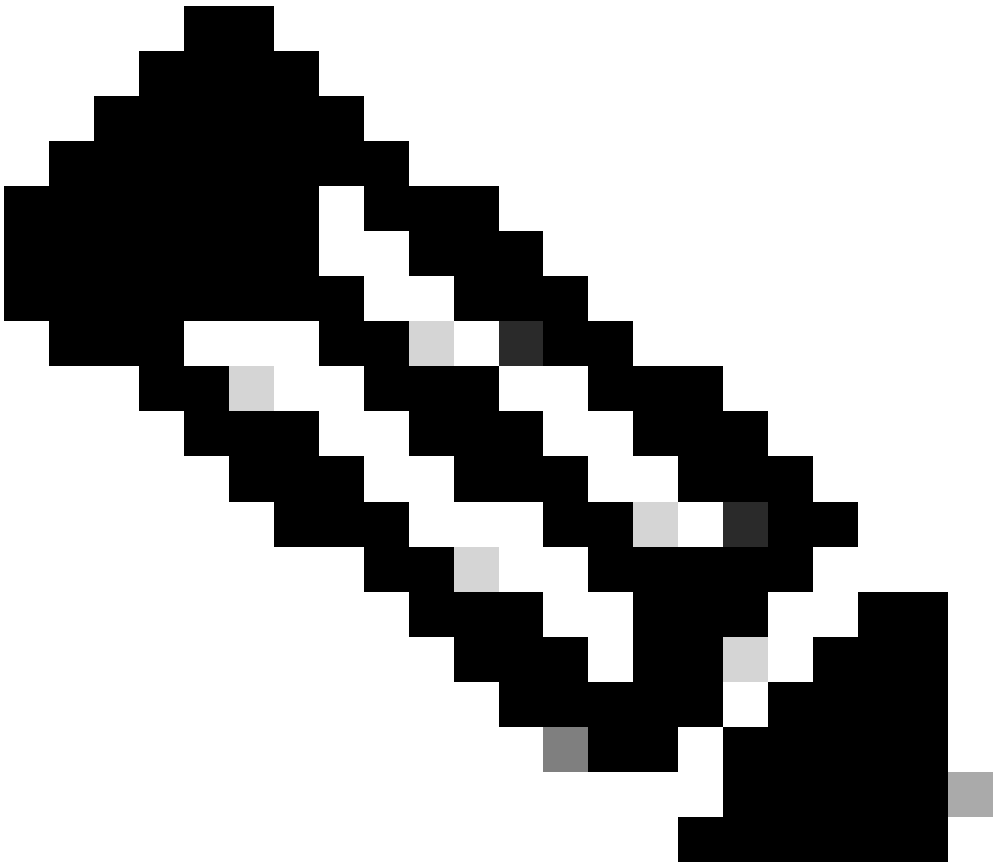
トラブルシュート

データベース証明書を除くすべてのサービスで期限切れの証明書を置き換える必要がある場合、最も簡単な方法は、古い証明書と同じ名前で新しい証明書をアップロードすることです。この場合、サービスを再起動するだけで、サービスを再設定する必要はありません。

pki csr ...

を実行し、その証明書名が現在のキーと一致する場合、サービスは直ちに中断されます。 実稼働環境で、新しいCSRとキーを予防的に作成する場合は、新しい名前を使用します。 新しい証明書をサーバにアップロードする前に、現在アクティブな名前を変更できます。

データベース証明書の期限が切れている場合は、データベースのプライマリが **database cluster status** 誰であるかを確認し、すべてのノードで database cluster removeコマンドを実行する必要があります。その後、手順3の手順を使用できます。データベースクラスタCSRを生成し、組み込みCAを使用して署名する。



注:Cisco Meeting Manager(CMM)証明書を更新する必要がある場合は、次のビデオ「Updating the Cisco Meeting Management SSL Certificate」を参照してください。

関連情報

- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。