生成CSR並將證書應用到CMS

目錄

簡介

本檔案介紹如何產生憑證簽署請求(CSR)並將簽署的憑證上傳到思科Meeting Server (CMS)。

必要條件

需求

思科建議您瞭解以下主題：

- CMS伺服器基礎知識

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Putty或類似軟體
- CMS 2.9或更高版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

生成CSR

產生CSR的方式有兩種，一種是從具有管理員存取權的指令行介面(CLI)直接在CMS伺服器上產生

CSR，另一種是使用外部第三方憑證授權單位(CA)（例如開啟SSL）來產生CSR。

在這兩種情況下，都必須使用正確的語法生成CSR，CMS服務才能正常工作。

步驟 1.語法結構。

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

- <key/cert basename>是標識新金鑰和CSR名稱的字串。它可以包含英數字元、連字型大小或底線字元。這是必填欄位。
- <CN：value>是公用名。這是完整網域名稱(FQDN)，指定伺服器在網域名稱系統(DNS)中的確切位置。這是必填欄位。
- [OU：<value>]是組織單位或部門名稱。例如，支援、IT、工程師、財務。此為選擇性欄位。
- [O：<value>]是組織或業務名稱。 通常是合法註冊的公司名稱。此為選擇性欄位。
- [ST：<value>]是省、地區、縣或州。 例如，加州白金漢郡。 此為選擇性欄位。
- [C：<value>]是國家/地區。貴組織所在國家/地區的國際標準化組織(ISO)代碼（兩個字母）。例如，US、GB、FR。此為選擇性欄位。
- [subjectAltName：<value>]是主體替代名稱(SAN)。 從X509版本3 (RFC 2459)開始，允許安全通訊端層(SSL)憑證指定憑證必須符合的多個名稱。此欄位可讓產生的憑證涵蓋多個網域。它可以包含IP地址、域名、郵件地址、常規DNS主機名等，以逗號分隔。如果已指定，您也必須在此清單中包含CN。雖然這是可選欄位，但必須填寫SAN欄位才能使可擴展消息傳送和線上狀態協定(XMPP)客戶端接受證書，否則XMPP客戶端將顯示證書錯誤。

步驟 2.生成callbridge、xmpp、webadmin和webbridge CSR。

1. 使用Putty訪問CMS CLI並使用管理員帳戶登入。
2. 運行以下命令，以便為CMS上所需的每項服務建立CSR。也可以建立具有萬用字元(*.com)或群集FQDN作為CN、每個CMS伺服器的FQDN並在必要時加入URL的單個證書。

服務	命令
Webadmin	pki csr <cert name> CN:<server FQDN>
Webbridge	pki csr <cert name> CN:<Server FQDN> subjectAltName:<Join Url>,<XMPP domain>
Callbridge TURN	pki csr <cert name> CN:<Server FQDN's>

負載平衡器	

3. 如果CMS已群集，請運行以下命令。

服務	指令
Callbridge TURN 負載平衡器	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>

步驟 3.生成資料庫群集CSR並使用內建CA對其進行簽名。

從CMS 2.7開始，您必須擁有資料庫叢集的憑證。 在2.7中，我們包括一個可用於簽署資料庫證書的內建CA。

1. 在所有核心上，運行database cluster remove。

- 在主要路由器上，運行pki selfsigned dbca CN。範例： **Pki selfsigned dbca CN:tplab.local**
- 在主要路由器上運行pki csr dbserver CN:cmscore1.example.com subjectAltName。示例：cmscore2.example.com,cmscore3.example.com
- 在「主要」上，為資料庫使用者端建立憑證 pki csr dbclient CN:postgres 。
- 在Primary上，使用dbca簽署dbserver證書 **pki sign dbserver dbca** 。
- 在主要上，使用dbca來簽署dbclient證書pki sign dbclient dbca。
- 將dbclient.crt複製到需要連線到資料庫節點的所有伺服器
- 將dbserver.crt檔案複製到所有已加入資料庫的伺服器（組成資料庫叢集的節點）
- 將dbca.crt檔案複製到所有伺服器。
- 在主DB伺服器上，運行database cluster certs dbserver.key dbserver.crt dbclient.key dbclient.crt dbca.crt。這將使用 dbca.crt作為root ca-cert（在命令列介面上）。
- 在主DB伺服器上，運行database cluster localnode a。
- 在主DB伺服器上，運行database cluster initialize。
- 在主DB伺服器上，運行database cluster status。必須看到節點：(me)：已連線的主節點。

- 在已加入資料庫集群的所有其他核心上，運行database cluster certs dbserver.key dbserver.crt dbclient.key dbclient.crt dbca.crt。
- 在連線到資料庫叢集（未與資料庫共置）的所有核心上，執行 **database cluster certs dbclient.key cbclient.crt dbca.crt** .
- 在已連線的核心上（與資料庫共置）：
  - 運行 database cluster localnode a。
    - 運行database cluster join。
- 已連線（未與資料庫共置）的ON核心：
  - ru n database cluster localnode a .
    - 運行 database cluster connect 。

步驟 4.驗證簽署的憑證。

- 證書有效性（到期日期）可以透過證書檢查進行驗證，請運行**pki inspect <filename>** 命令。
  - 您可以驗證證書是否與私鑰匹配，然後運行命令pki match <keyfile> <certificate file>。
  - 要驗證證書是否由CA簽名以及證書捆綁是否可用於宣告證書，請運行命令pki verify <cert> <certificate bundle/Root CA>。

步驟 5.將簽名證書應用於CMS伺服器上的元件。

1. 若要將憑證套用至Webadmin，請執行下列指令：

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

2. 要將證書應用到Callbridge，請運行以下命令：

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

3. 要將證書應用到Webbridge，請運行以下命令：

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

4. 若要將憑證套用至XMPP，請執行下列命令：

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

5. 若要將憑證套用至資料庫或取代目前資料庫叢集上的過期憑證，請執行下列命令：

```
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
```

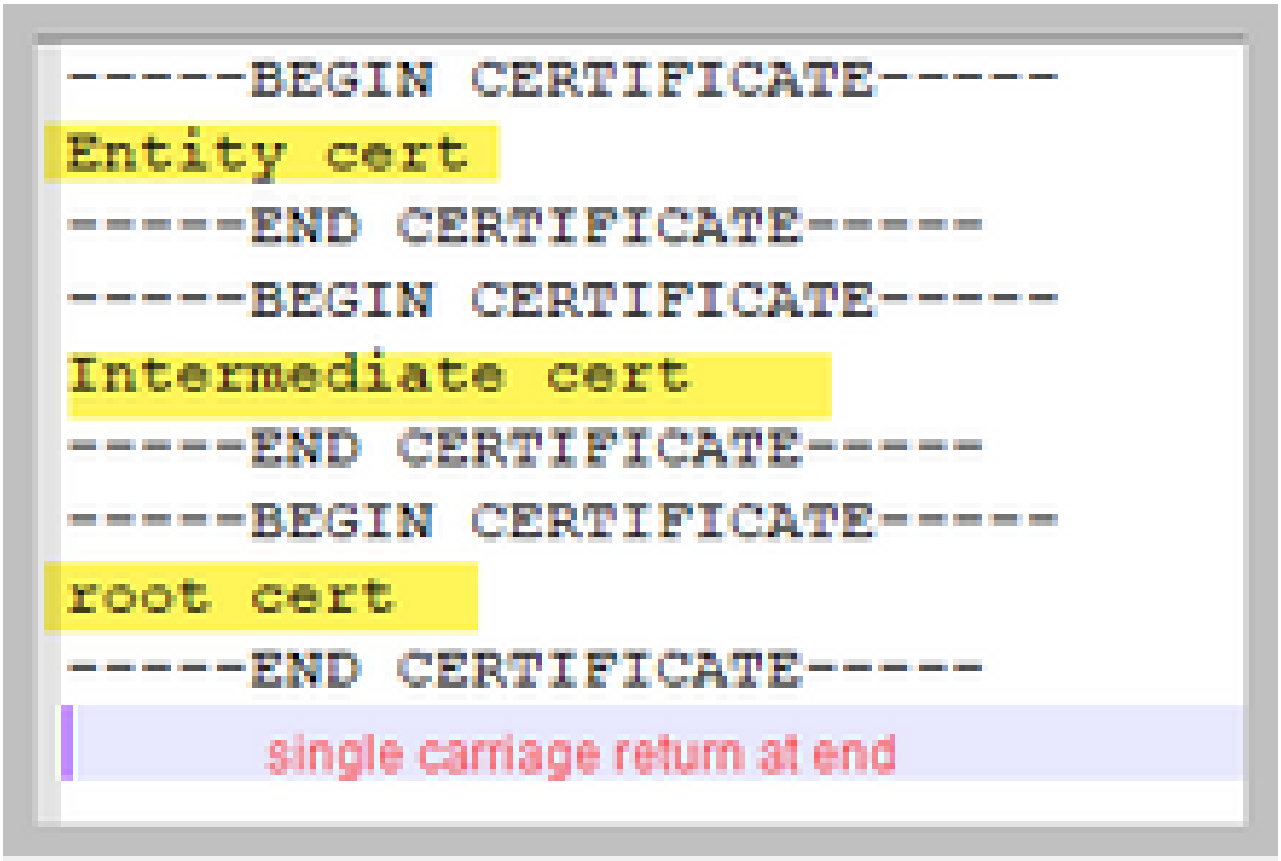
6. 要將證書應用到TURN，請運行以下命令：

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

證書信任鏈和捆綁包

從CMS 3.0開始，您需要使用證書信任鏈或完整鏈信任。 此外，對於任何服務而言，當您製作捆綁包時，您必須瞭解證書的構建方式，這一點非常重要。

建立證書信任鏈時，如Web Bridge 3要求的那樣，必須構建證書信任鏈（如圖所示），其中entity cert位於頂部，intermediates位於中間，root CA位於底部，然後返回一個回車。



無論何時建立捆綁，證書的末尾只能返回一個回車。

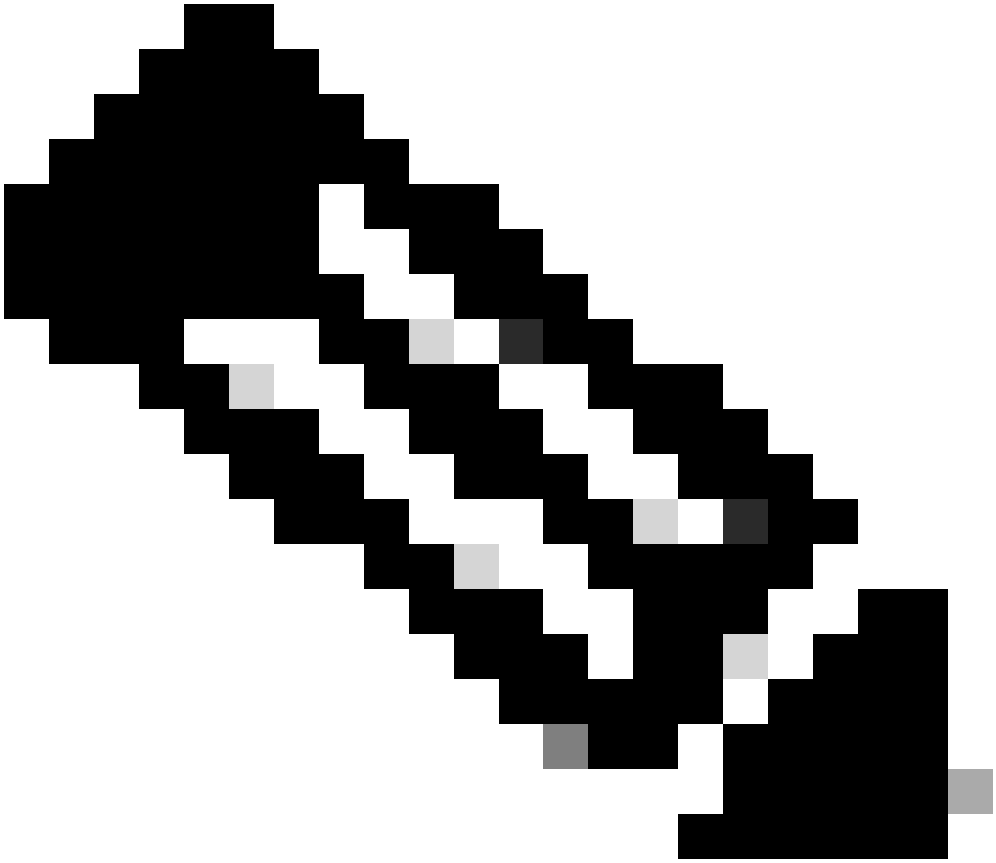
CA捆綁包與圖中所示相同，只是沒有實體證書。

疑難排解

如果需要替換除資料庫證書之外的所有服務的過期證書，最簡單的方法就是上傳與舊證書同名的新證書。如果這樣做，則只需重新啟動服務，而無需重新配置服務。

如果執行pki csr ... ，並且證書名稱與當前金鑰相匹配，則它會立即中斷服務。 如果生產處於活動狀態，並且您主動建立了新的CSR和金鑰，請使用新名稱。 在將新證書上載到伺服器之前，可以重新命名當前活動名稱。

如果資料庫證書已過期，您需要檢查資料庫Primary **database cluster status** 是誰，並在所有節點上運行命令 database cluster remove。然後您可以使用步驟3中的說明。生成資料庫集群CSR並使用內建CA對其進行簽名。



注意：如果需要續訂思科會議管理器(CMM)證書，請參閱下一個影片：更新思科會議管理SSL證書

相關資訊

- **思科技術支援與下載**

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。