使用OpenSSL為加密配置CMS的CSR

目錄

簡介

本文說明如何使用開放安全套接字層(OpenSSL)為思科會議伺服器(CMS)建立證書。

作者：Moises Martinez，思科TAC工程師。

必要條件

思科建議您瞭解以下主題：

- 開啟SSL。
- CMS配置。

採用元件

本檔案中的資訊是根據以下軟體：

- OpenSSL精簡版1.1

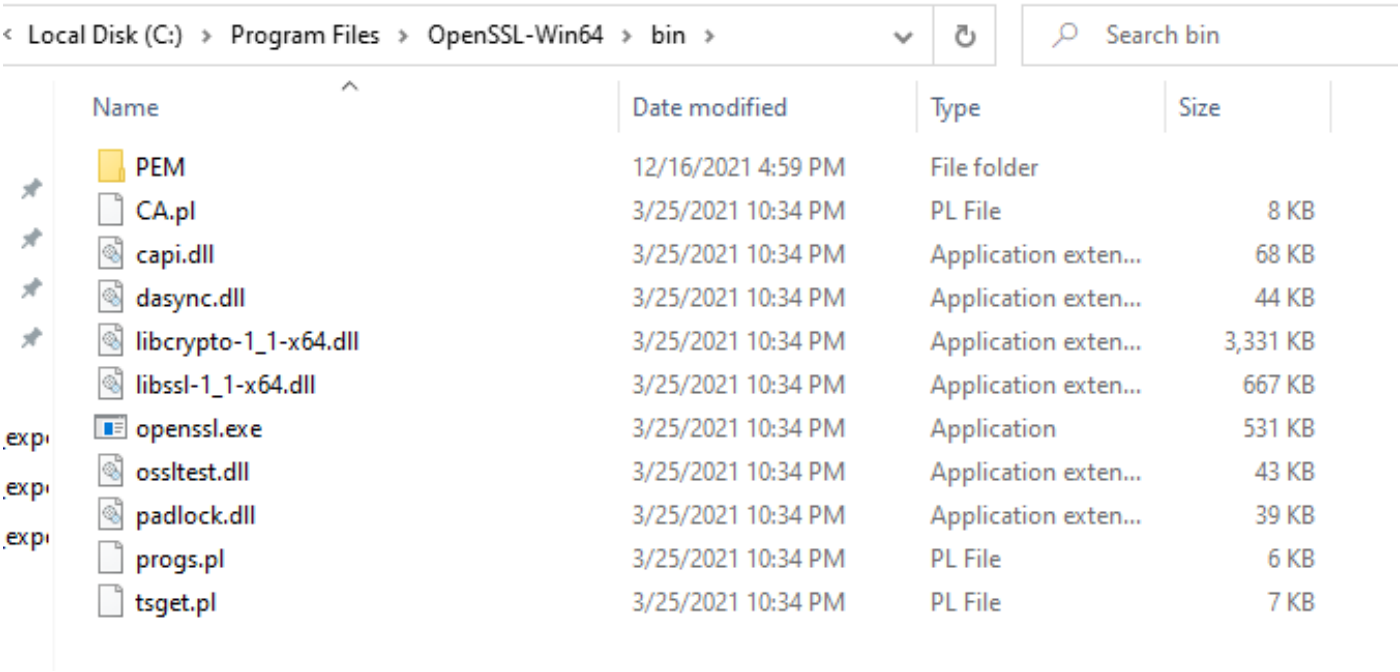
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

步驟1.下載OpenSSL Light 1.1。

步驟2.在電腦上安裝OpenSSL。

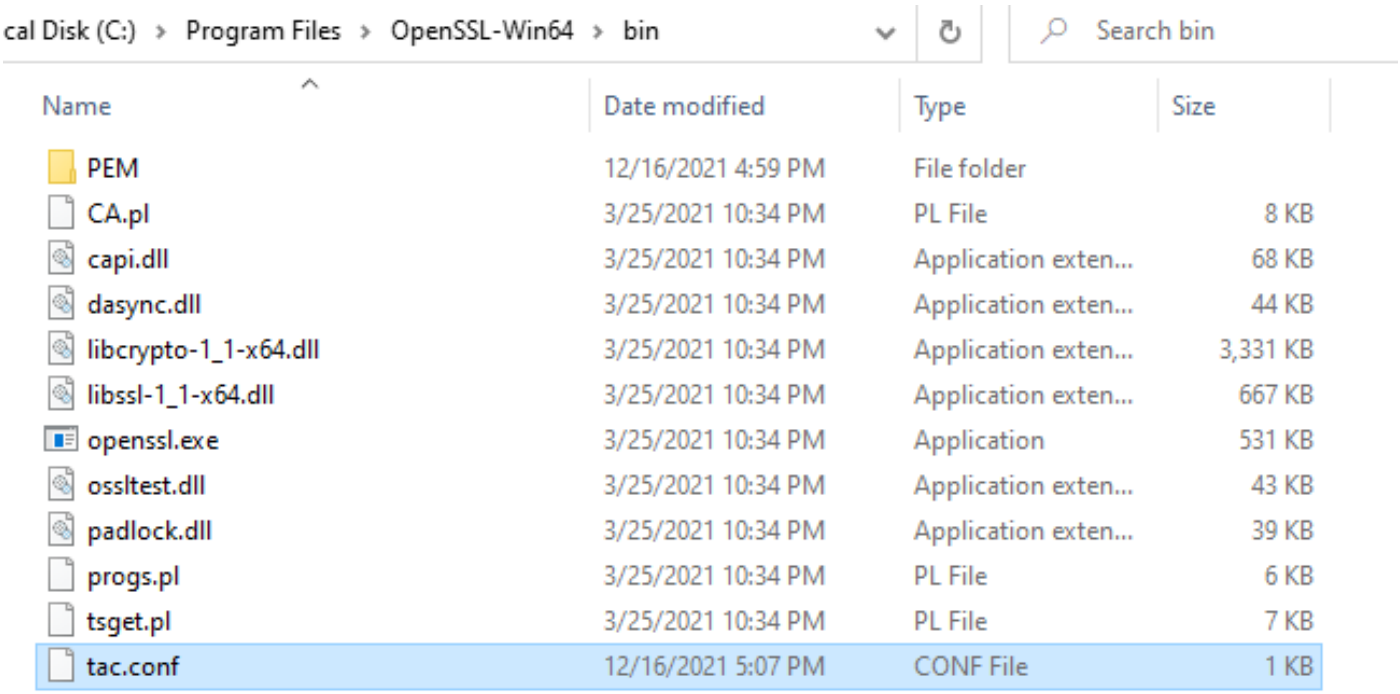
步驟3.導航到安裝SSL的資料夾。通常安裝在**C:\Program Files\OpenSSL-Win64\bin**上。



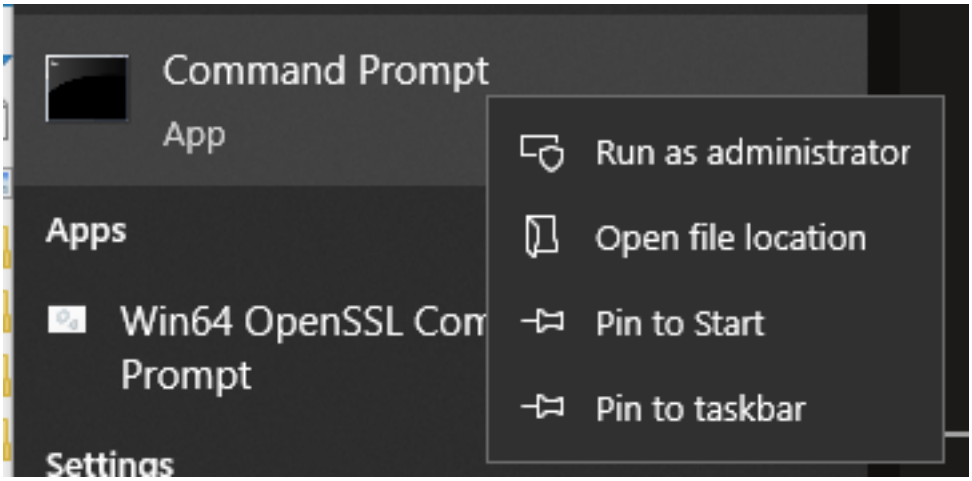
步驟4.開啟**記事本**，並輸入憑證簽署請求(CSR)所需的資訊，如下例所示：

```
[req] distinguished_name = req_distinguished_name req_extensions = v3_req prompt = no
[req_distinguished_name] C = US ST = California L = San Jose O = TAC OU = IT CN =
cms.tac.cisco.com [v3_req] extendedKeyUsage = serverAuth, clientAuth subjectAltName = @alt_names
[alt_names] DNS.1 = webbridge3.tac.cisco.com DNS.2 = webadmin.tac.cisco.com DNS.3 =
xmpp.tac.cisco.com
```

步驟5.一旦為CSR輸入資訊，此檔案就會儲存在**tac.conf**的下一個路徑中：**C:\Program Files\OpenSSL-Win64\bin**。



步驟6.在PC上開啟**Command Promt**，然後選擇**Run as administrator**。



步驟7.透過命令提示導航至儲存檔案的路徑，輸入**openssl.exe**指令，然後選擇enter。

```
C:\Program Files\OpenSSL-Win64\bin>openssl.exe
```

步驟8.執行下一個命令：**req -new -newkey rsa:4096 - nodes -keyout cms.key -out cms.csr -config tac.conf**。

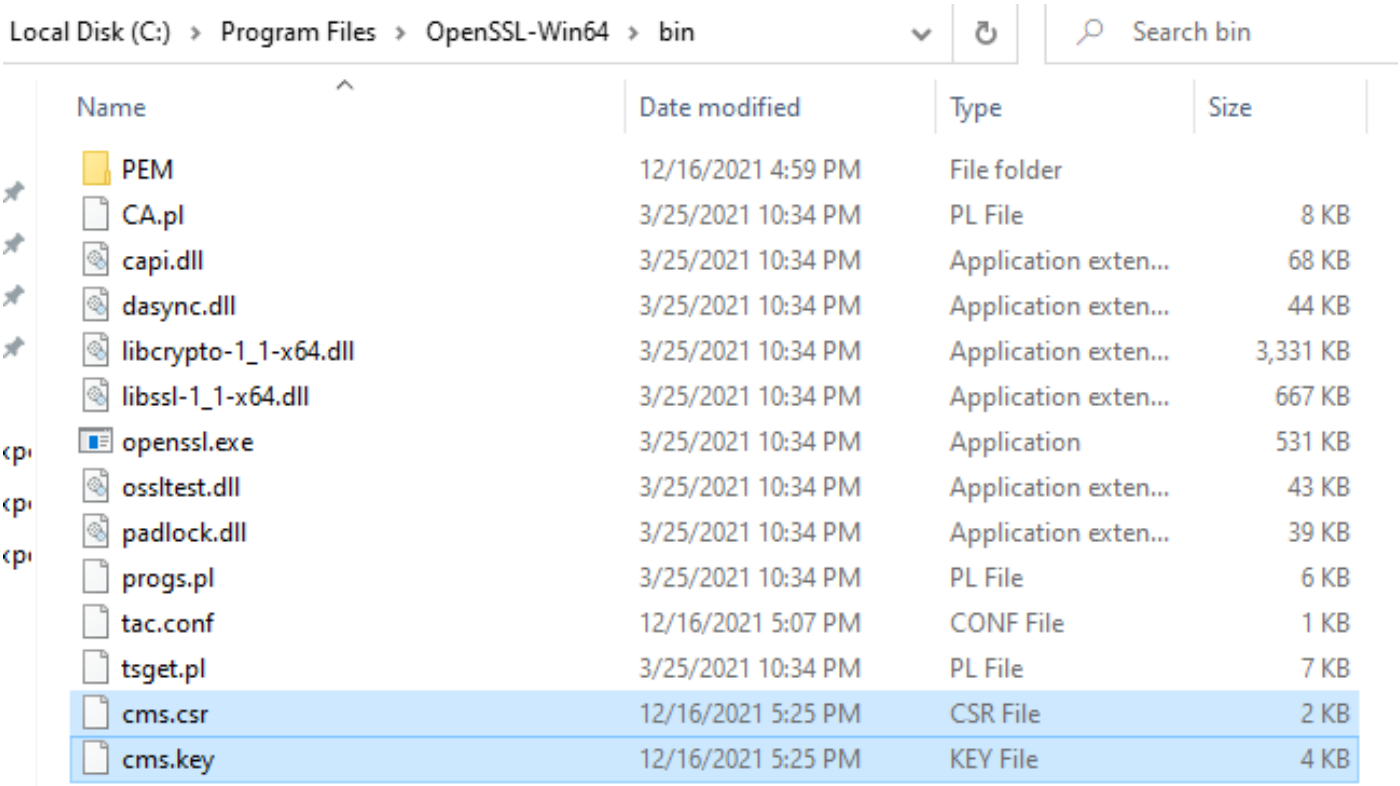
```
C:\Program Files\OpenSSL-Win64\bin>openssl.exe
OpenSSL> req -new -newkey rsa:4096 -nodes -keyout cms.key -out cms.csr -config tac.conf
```

```
C:\Program Files\OpenSSL-Win64\bin>openssl.exe
OpenSSL> req -new -newkey rsa:4096 -nodes -keyout cms.key -out cms.csr -config tac.conf
Generating a RSA private key
.....++++
.....
writing new private key to 'cms.key'
-----
```

驗證

如果未顯示錯誤，則會在同一資料夾中生成兩個新檔案：

- **cms.key**
- **cms.csr**



此新檔案**cms.csr**可由憑證授權單位(CA)簽署。