

為具有證書頒發機構(CA)簽名證書的UCCE診斷 框架Portico工具配置HTTPS訪問

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[生成證書簽名請求](#)

[在證書頒發機構上簽署證書](#)

[安裝證書](#)

[複製憑證](#)

[將證書匯入本地電腦儲存](#)

[繫結IIS證書](#)

[驗證](#)

[退出計畫](#)

[疑難排解](#)

[相關文章](#)

簡介

本文檔介紹如何安裝Unified Contact Center Enterprise(UCCE)診斷框架Portico工具的CA簽名證書的配置過程。

必要條件

需求

思科建議您瞭解以下主題：

- Active Directory
- 網域名稱系統(DNS)伺服器
- 為所有伺服器和客戶端部署並工作的CA基礎架構
- 診斷框架門廊

在瀏覽器中鍵入IP地址而不收到證書警告訪問診斷框架Portico工具不屬於本文的範圍。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco UCCE 11.0.1
- Microsoft Windows Server 2012 R2

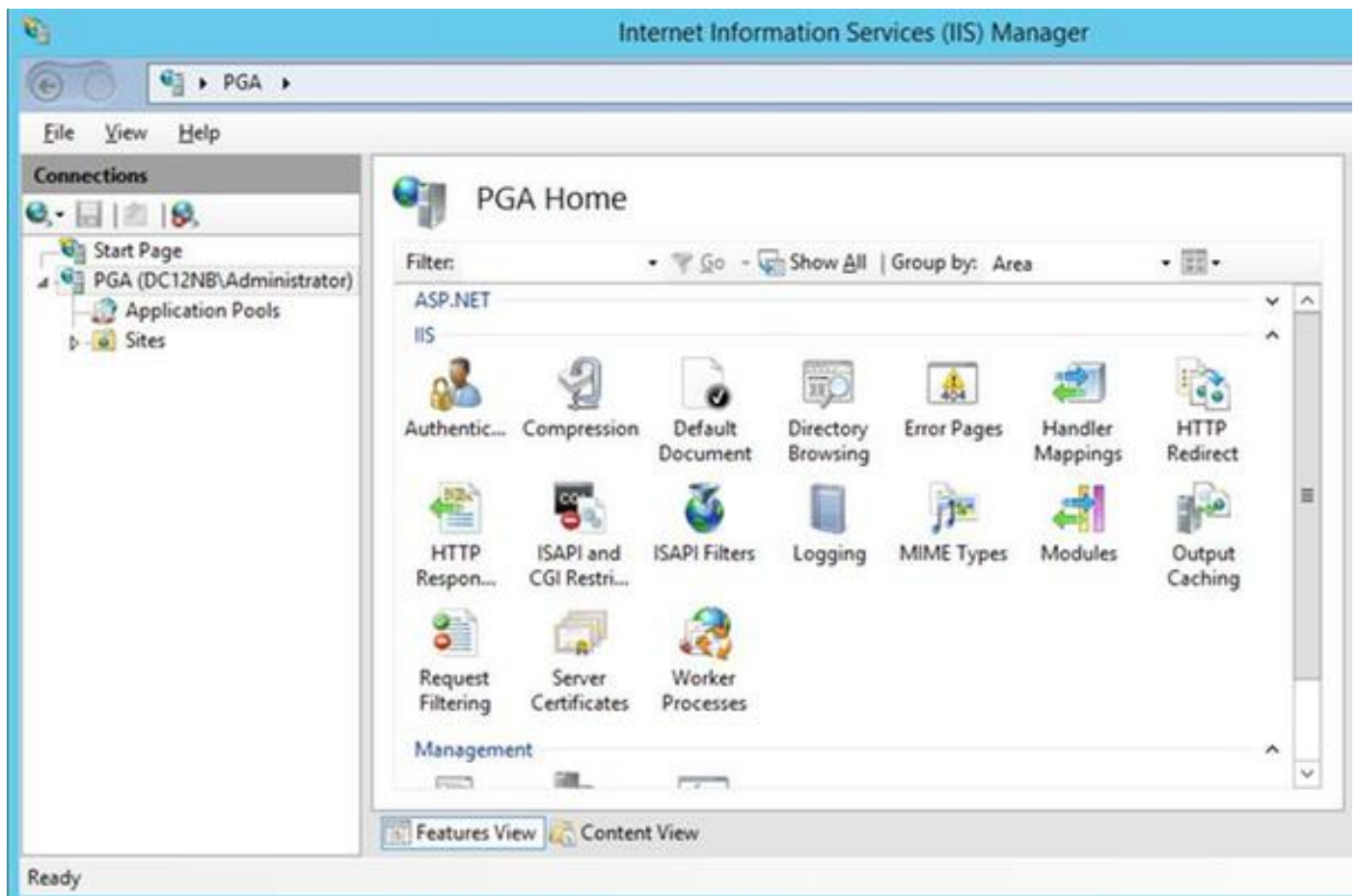
- Microsoft Windows Server 2012 R2證書頒發機構
- Microsoft Windows 7 SP1作業系統

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

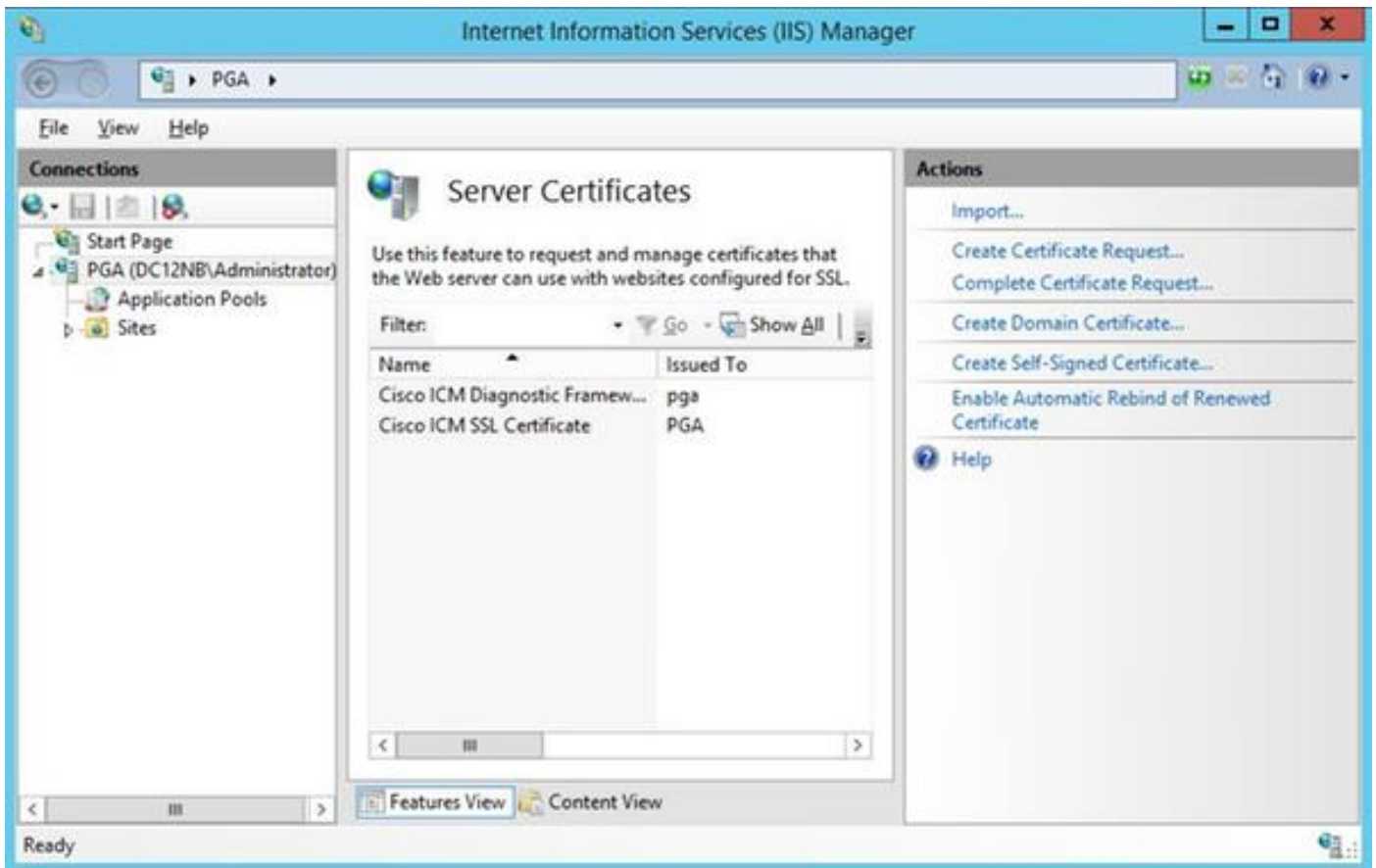
設定

生成證書簽名請求

開啟Internet Information Services(IIS)管理器，選擇站點、示例中的外圍裝置網關A(PGA)和伺服器證書。



在動作面板中選擇Create Certificate Request。



輸入Common name(CN)、Organization(O)、Organization unit(OU)、Locality(L)、State(ST)和Country(C)欄位。公用名必須與完全限定域名(FQDN)主機名+域名相同。

Request Certificate

Distinguished Name Properties

Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

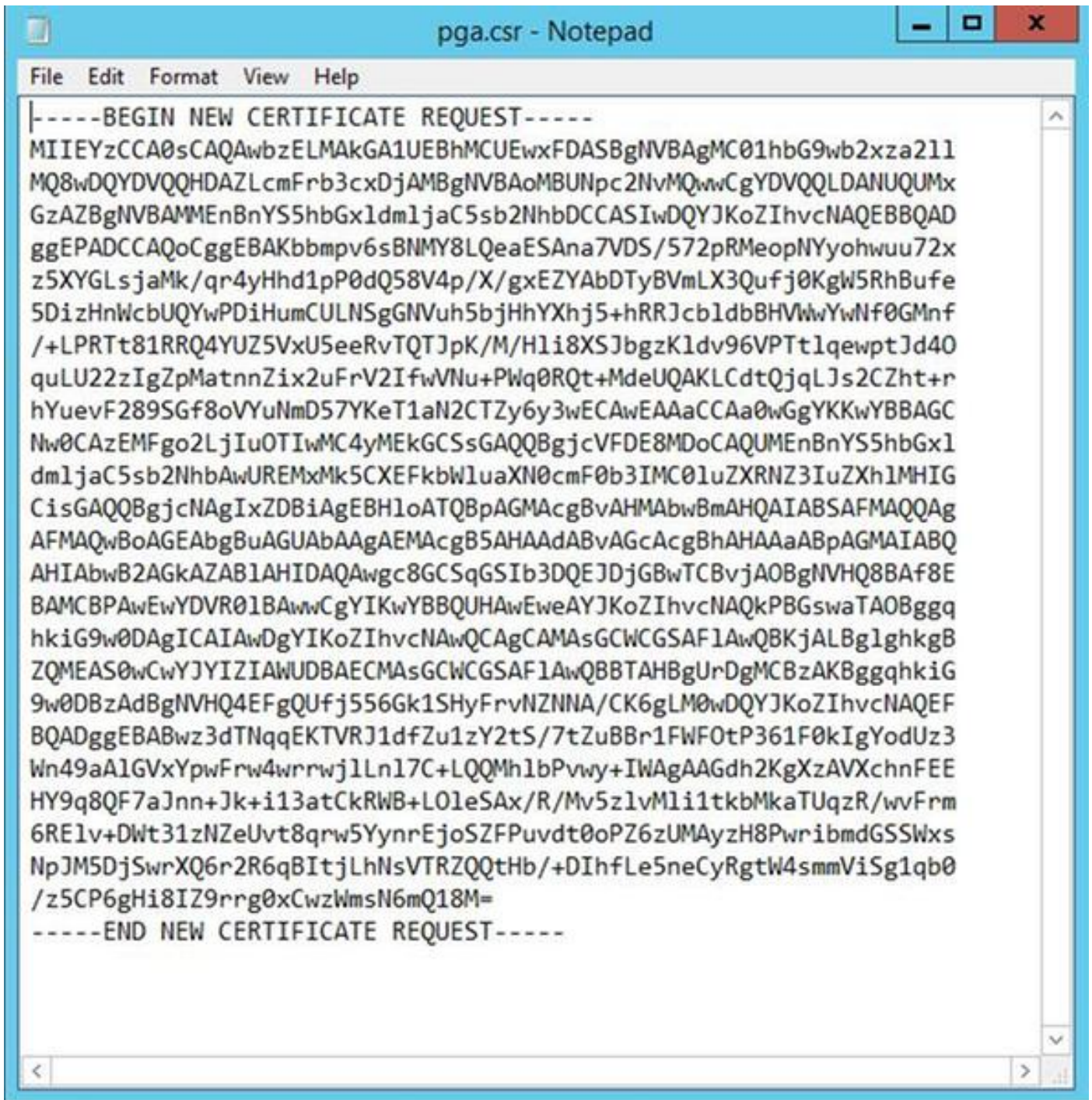
Common name:	<input type="text" value="pga.allevich.local"/>
Organization:	<input type="text" value="Cisco"/>
Organizational unit:	<input type="text" value="TAC"/>
City/locality:	<input type="text" value="Krakow"/>
State/province:	<input type="text" value="Malopolskie"/>
Country/region:	<input type="text" value="PL"/>

Previous Next Finish Cancel

保留加密服務提供程式的預設設定並指定位長度：2048。

選擇要儲存的路徑。例如，在具有pga.csr名稱的案頭上。

在記事本中開啟新建立的請求。



```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIEYzCCA0sCAQAwbzELMAKGA1UEBhMCUEwxFDASBgNVBAGMC01hbG9wb2xza211
MQ8wDQYDVQQHDAZLcmFr3cxDjAMBgNVBAoMBUNpc2NvMQwwCgYDVQQLDANUQUx
GzAZBgNVBAMMEnBnYS5hbGxldm1jaC5sb2NhbDCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAKbbmpv6sBNMY8LQeaESAna7VDS/572pRMeopNYyohwuu72x
z5XYGLsjaMk/qr4yHhd1pP0dQ58V4p/X/gxEZYAbDTyBVmLX3Qufj0KgW5RhBufe
5DizHnWcbUQYwPDiHumCULNSgGNVuh5bjHhYXhj5+hRRJcbldbBHVWwYwNf0GMnf
/+LPRTt81RRQ4YUZ5VxU5eeRvTQTJpK/M/Hli8XSJbgzK1dv96VPTt1qewptJd40
quLU22zIgZpMatnnZix2uFrV2IfwVNu+Pwq0RQt+MdeUQAKLCdtQjqLJs2CZht+r
hYuevF289SGf8oVYuNmD57YKeT1aN2CTZy6y3wECAwEAaCCAA0wGgYKKwYBBAGC
Nw0CAzEMFgo2LjIu0TIwMC4yMEkGCSsGAQQBgjcVFDE8MDoCAQUMEnBnYS5hbGx1
dmljaC5sb2NhbAwUREMxMk5CXEFkbWluaXN0cmF0b3IMC0luZXRNZ3IuZXh1MHIG
CisGAQQBgjcNAgIxZDBiAgEBHloATQBpAGMAcGvAHMAbwBmAHQAIABSAFMAQQAg
AFMAQwBoAGEAbgBuAGUAbAAgAEMAcb5AHAAdABvAGcAcgBhAHAAaABpAGMAIABQ
AHIAbwB2AGkAZABlAHIDAQAawgc8GCSqGSIb3DQEJJDjGBwTCBvjA0BgNVHQ8BAf8E
BAMCBPAwEwYDVR01BAwwCgYIKwYBBQUHAwEweAYJKoZIhvcNAQkPBGswaTA0Bggq
hkiG9w0DAGICAIAwDgYIKoZIhvcNAwQCAgCAMAsGCWCGSAF1AwQBKjALBglghkgB
ZQMEAS0wCwYJYIZIAWUDBAECMA5GCWCGSAF1AwQBBTAHBgUrDgMCBzAKBggqhkiG
9w0DBzAdBgNVHQ4EFgQUfj556Gk1SHyFrvNZNNA/CK6gLM0wDQYJKoZIhvcNAQEF
BQADggEBABwz3dTNqqEKTVRJ1dfZu1zY2tS/7tZuBBn1FWF0tP361F0kIgYodUz3
Wn49aA1GVxYpwFrw4wrrwj1Ln17C+LQQMh1bPvwy+IWAgaAGdh2KgXzAVXchnFEE
HY9q8QF7aJnn+Jk+i13atCkRWB+L0leSAx/R/Mv5z1vMli1tkbMkaTUqzR/wvFrm
6RElv+Dwt31zNZeUvt8qrw5YynrEjoSZFPuvdt0oPZ6zUMAYzH8PwribmdGSSWxs
NpJM5DjSwrXQ6r2R6qBItjLhNsVTRZQQtHb/+DIhfLe5neCyRgtW4smmViSg1qb0
/z5CP6gHi8IZ9rrg0xCwzWmsN6mQ18M=
-----END NEW CERTIFICATE REQUEST-----
```

使用CTRL+C將憑證複製到緩衝區中。

在證書頒發機構上簽署證書

附註：如果您使用外部憑證授權單位（例如GoDaddy），則需在產生CSR檔案後聯絡他們。

登入到CA伺服器證書註冊頁面。

<https://<CA-server-address>/certsrv>

選擇Request Certificate、Advanced Certificate Request，然後將憑證簽署請求(CSR)內容貼上到緩衝區。然後選擇Certificate Template as Web Server。

下載Base 64編碼證書。

開啟證書並複製指紋欄位的內容供以後使用。從指紋中刪除空格。

安裝證書

複製憑證

將新生成的證書檔案複製到Portico工具所在的UCCE VM中。

將證書匯入本地電腦儲存

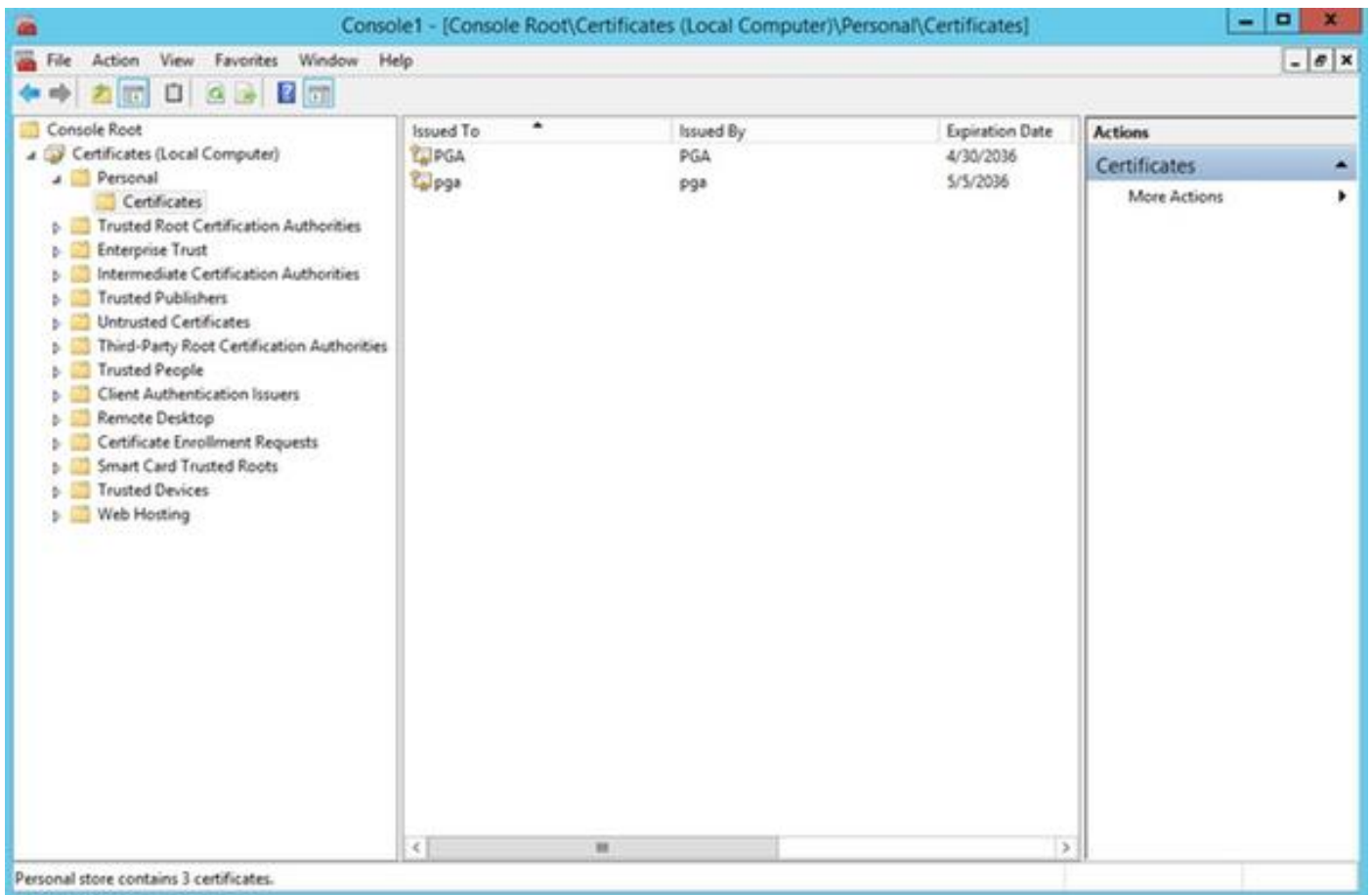
在同一UCCE伺服器上，通過選擇「開始」選單啟動Microsoft管理控制檯(MMC)控制檯，鍵入run和mmc。

按一下 **新增/刪除管理單元**，然後在對話方塊中按一下 **新增**。

然後選擇**Certificates**選單並新增。

在「證書」管理單元對話方塊中，按一下**電腦帳戶>本地電腦>完成**。

導航到個人證書資料夾。



在操作窗格中，選擇**更多操作> 所有任務> 匯入**。

按一下**Next**、**Browse**並選擇之前生成的證書，在下一個選單中確保將證書儲存設定為個人。在最後

一個螢幕上，驗證已選中Certificate Store和Certificate File，然後按一下Finish。

繫結IIS證書

開啟CMD應用程式。

導航到Diagnostic Portico主資料夾。

```
cd c:\icm\serviceability\diagnostics\bin
```

刪除Portico工具的當前證書繫結。

```
DiagFwCertMgr /task:UnbindCert
```

繫結CA簽名的證書。

提示：使用某些文本編輯器(++記本)刪除雜湊中的空格。

使用之前儲存的雜湊並刪除空格。

```
DiagFwCertMgr /task:BindCertFromStore /certhash:bc6bbe23b8b3a26d8446c252400f9264c5c30a29
```

如果成功繫結證書，您應該看到輸出中的類似行。

"證書繫結有效"

使用此命令確保證書繫結成功。

```
DiagFwCertMgr /task:ValidateCertBinding
```

同樣，輸出中也應顯示類似的消息。

"證書繫結有效"

附註：預設情況下，DiagFwCertMgr將使用埠7890。

重新啟動診斷框架服務。

```
sc stop "diagfwsvc"  
sc start "diagfwsvc"
```

提示：可通過CMD工具中的tasklist命令檢查服務清單，特別是Portico服務名稱。

```
tasklist /v
```

驗證

使用FQDN開啟「診斷框架」頁，該頁不應提示證書警告消息。

退出計畫

如果您無法訪問Portico工具，可以重新生成自簽名證書並新增例外。
可以使用以下命令完成。

```
DiagFwCertMgr /task:CreateAndBindCert
```

疑難排解

在登入到Diagnostic Framework Portico工具時不要使用IP地址。您仍會收到證書警告，因為FQDN必須與證書CN欄位中指定的值匹配。

驗證所有伺服器是否都與NTP源同步。

```
w32tm /monitor
```

如果您嘗試使用主體替代名稱(SAN)或橢圓曲線數位簽章演算法(EC DSA)或4096金鑰長度證書 — 首先確定它不是特定於這些功能之一。

相關文章

[UCCE/PCCE — 在2008伺服器上獲取和上傳Windows Server自簽名證書或證書頒發機構\(CA\)證書的過程](#)

[在思科語音作業系統\(VOS\)中通過CLI配置CA簽名的證書](#)