在Microsoft CA伺服器配置上發佈ISE的證書撤銷列表示例

目錄

簡介

本文檔介紹運行Internet Information Services(IIS)以發佈證書吊銷清單(CRL)更新的Microsoft證書頒發機構(CA)伺服器的配置。還說明了如何配置思科身份服務引擎(ISE)（版本1.1及更高版本）以檢索更新以用於證書驗證。可以將ISE配置為檢索它在證書驗證中使用的各種CA根證書的CRL。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科身分識別服務引擎版本1.1.2.145
- Microsoft Windows® Server® 2008 R2

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。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

設定

本節提供用於設定本文件中所述功能的資訊。

註：使用Command Lookup Tool(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

組態

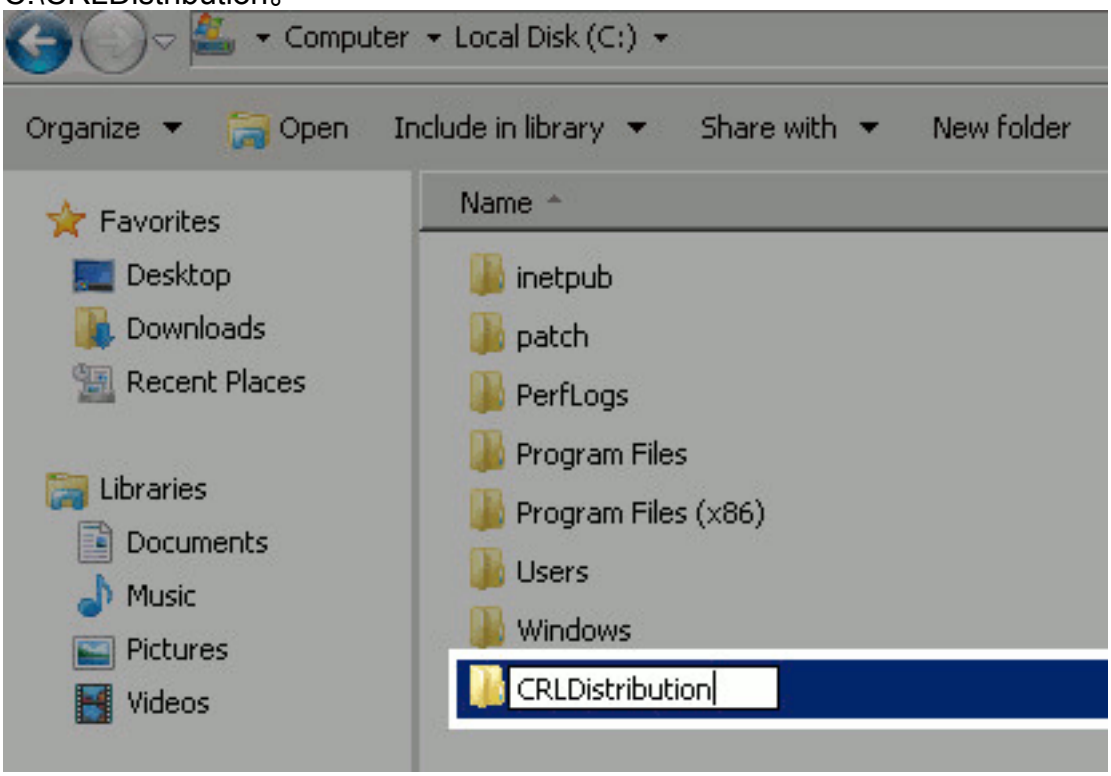
本檔案會使用以下設定：

- 第1部分。在CA上建立並配置資料夾以儲存CRL檔案
- 第2部分。在IIS中建立站點以公開新的CRL分發點
- 第3部分。配置Microsoft CA伺服器以將CRL檔案發佈到分發點
- 第4節：驗證CRL檔案是否存在且可通過IIS訪問
- 第5部分。配置ISE以使用新的CRL分發點

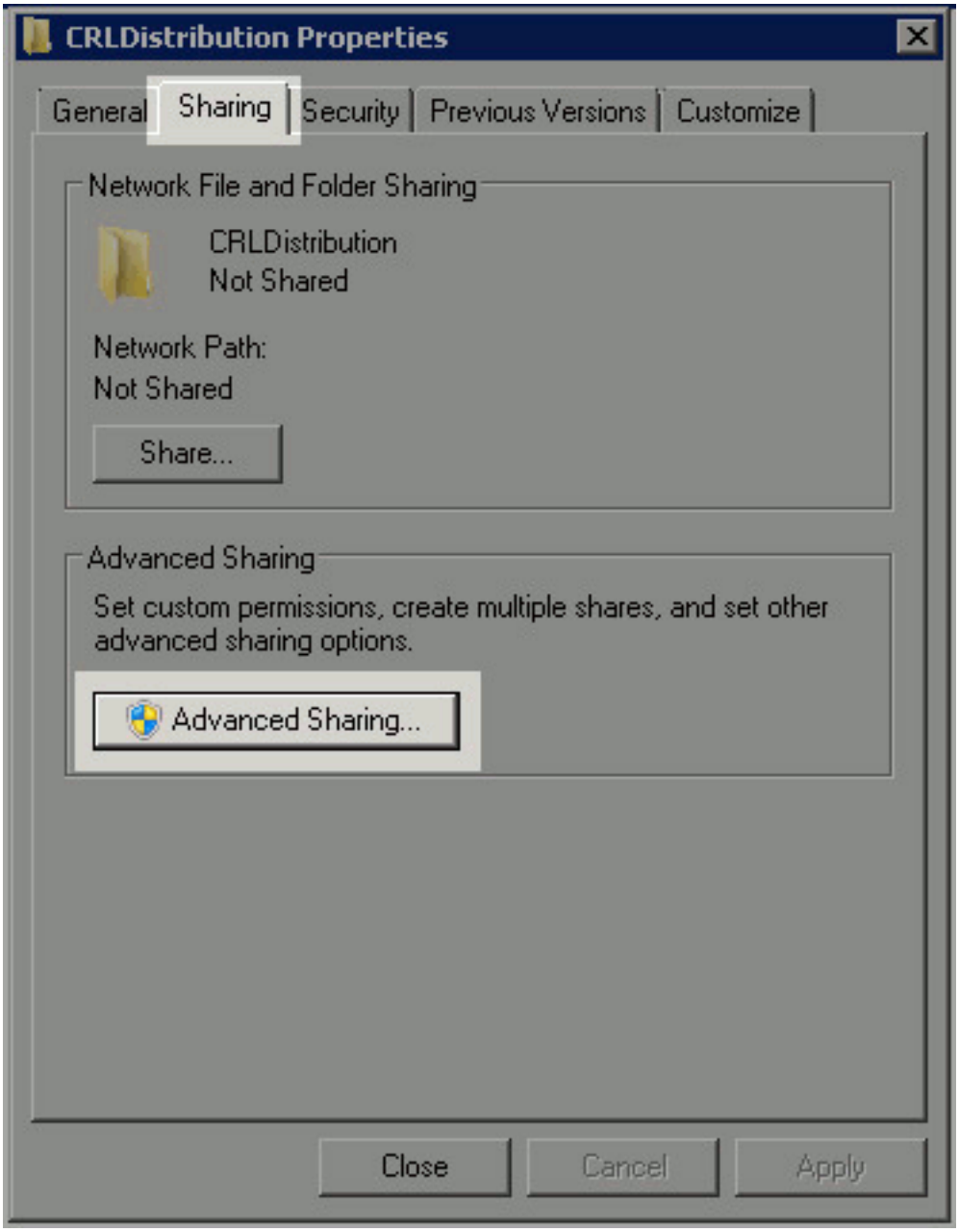
第1部分。在CA上建立並配置資料夾以儲存CRL檔案

第一項任務是配置CA伺服器上的一個位置以儲存CRL檔案。預設情況下，Microsoft CA伺服器將檔案發佈到C:\Windows\system32\CertSrv\CertEnroll\。不要使用此系統資料夾，而是為檔案建立一個新資料夾。

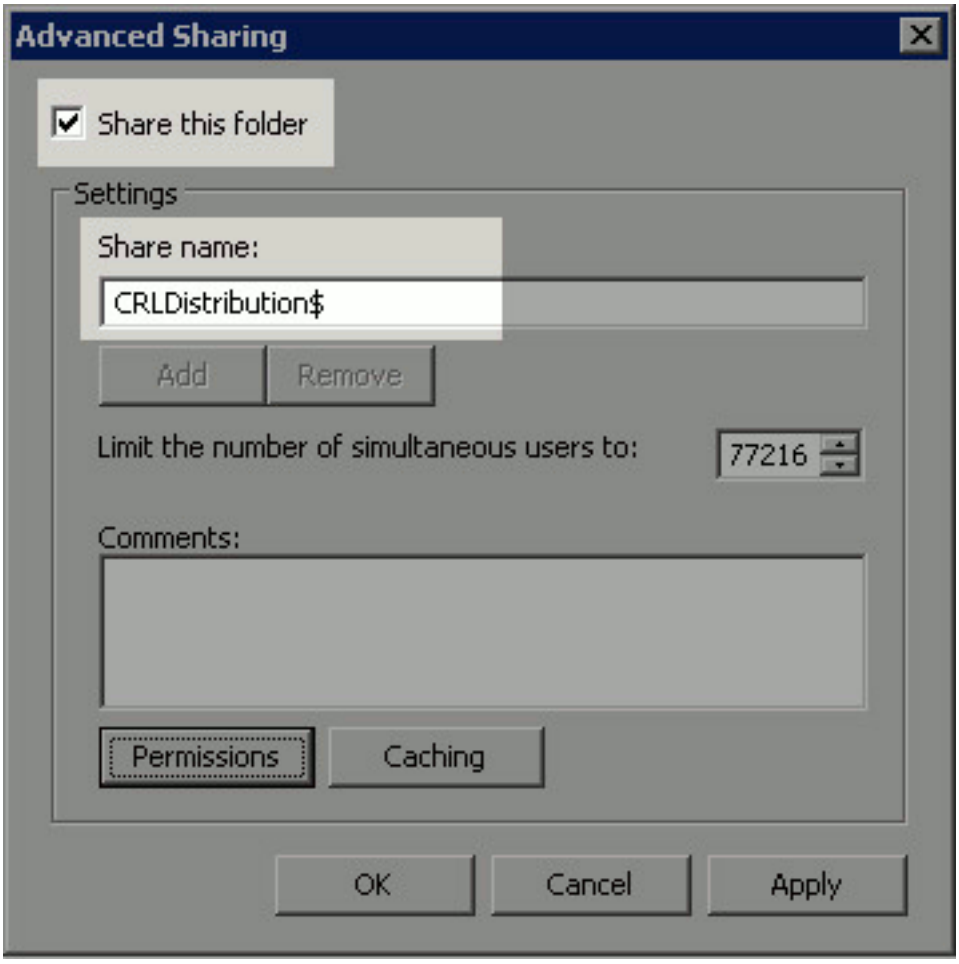
1. 在IIS伺服器上，選擇檔案系統上的位置並建立新資料夾。在此示例中，建立資料夾C:\CRLDistribution。



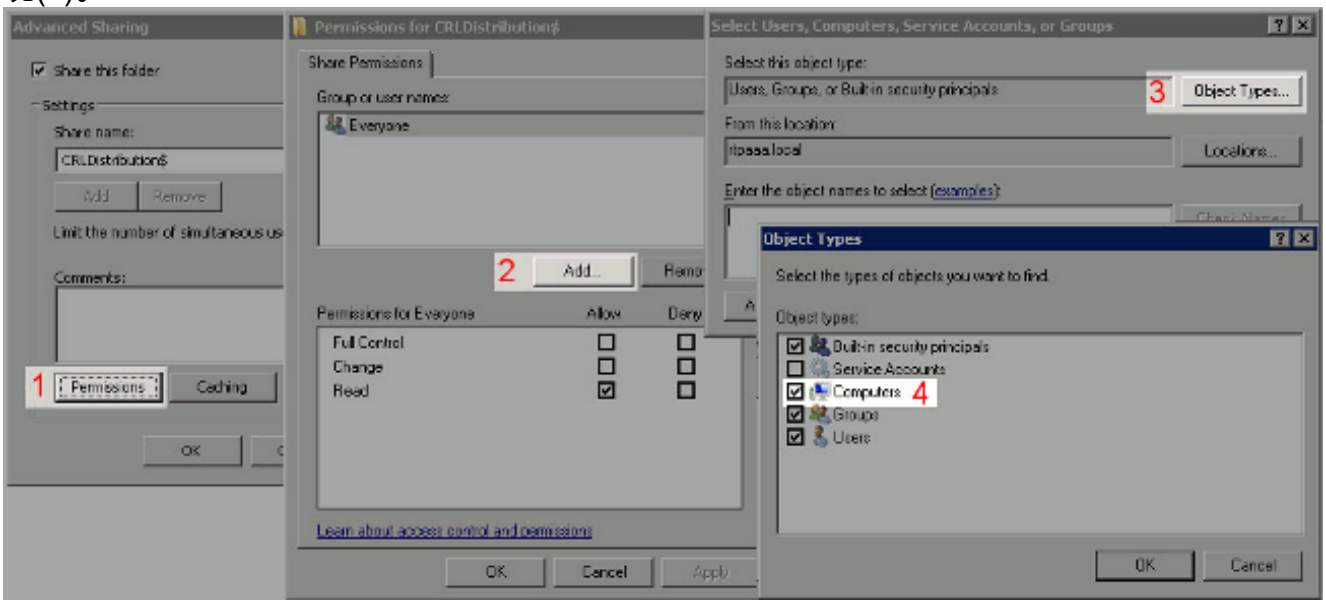
2. 為了使CA將CRL檔案寫入新資料夾，必須啟用共用。按一下右鍵新資料夾，選擇**屬性**，按一下**共用**頁籤，然後按一下**高級共用**。



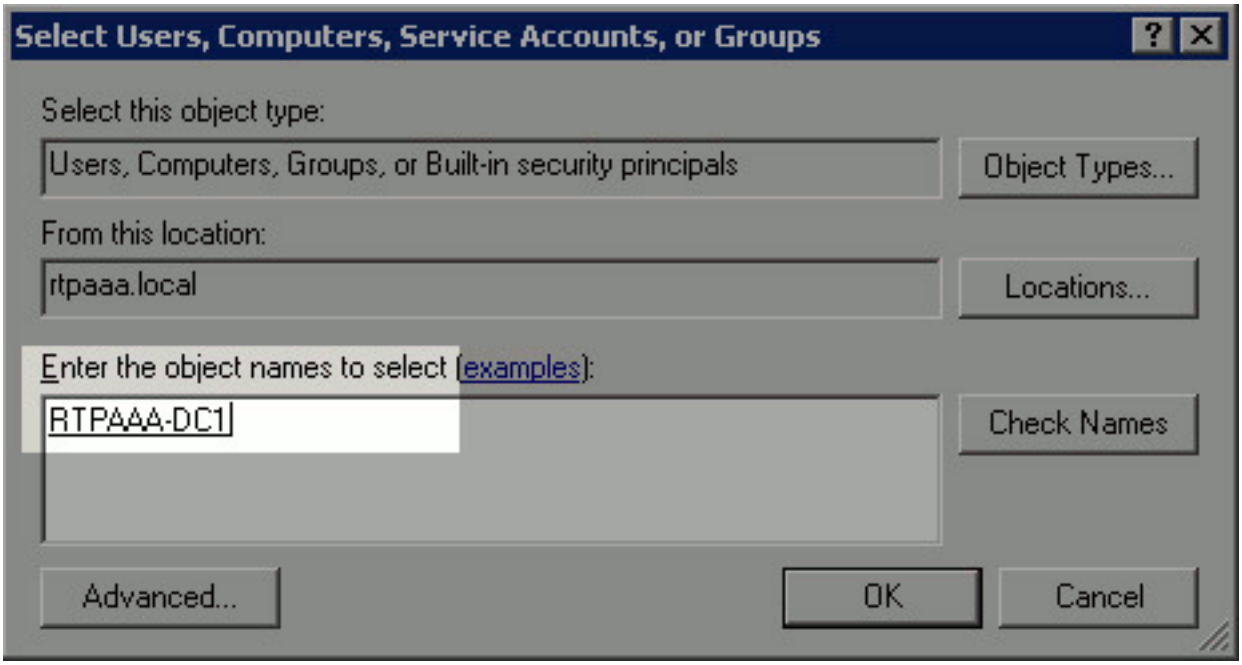
3. 若要共用資料夾，請選中**共用此資料夾**覈取方塊，然後在「共用名稱」欄位中為共用名稱末尾新增一個美元符號($)以隱藏共用。



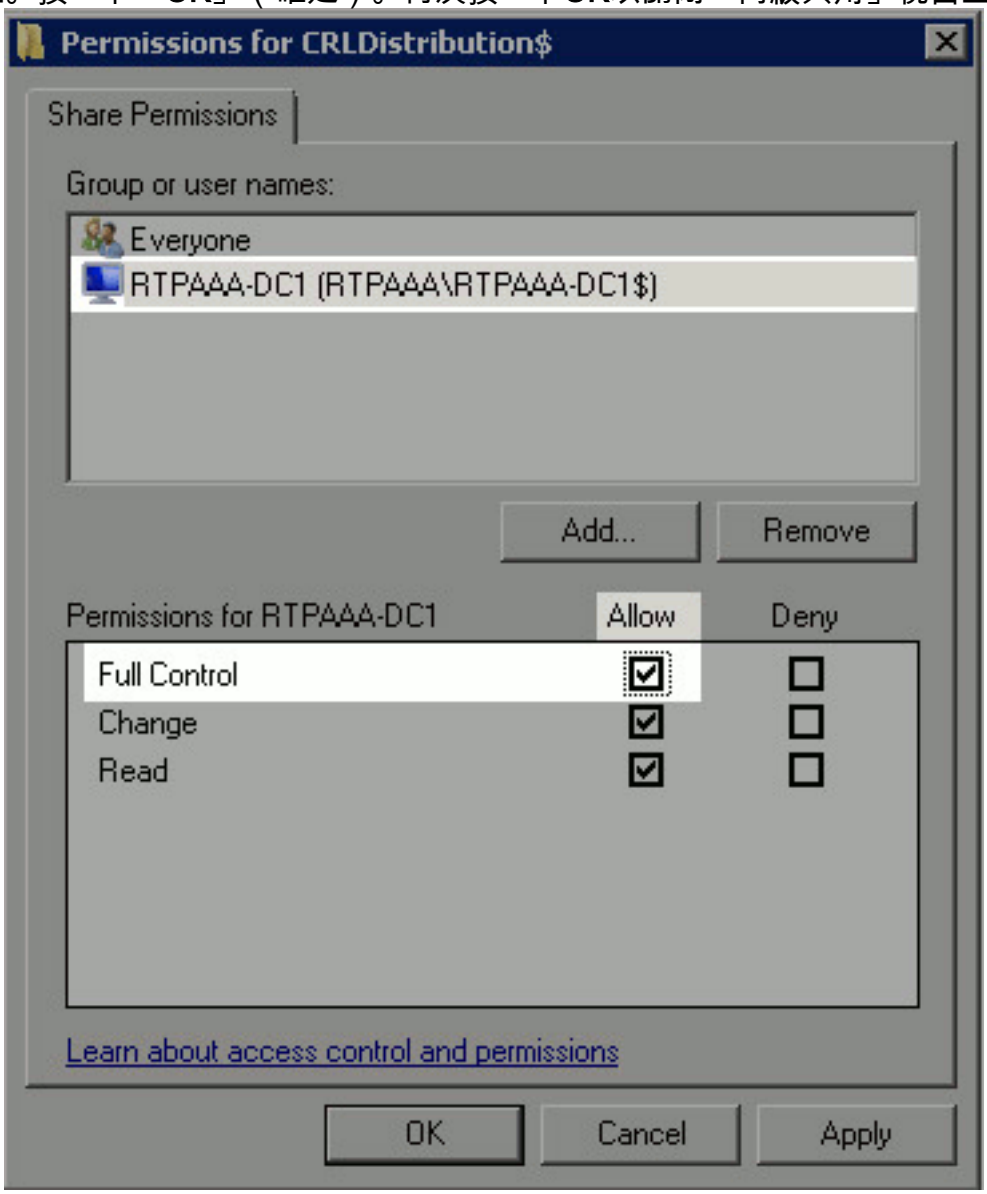
4. 按一下**Permissions**(1)，按一下**Add**(2)，按一下**Object Types**(3)，然後選中**Computers**覈取方塊(4)。



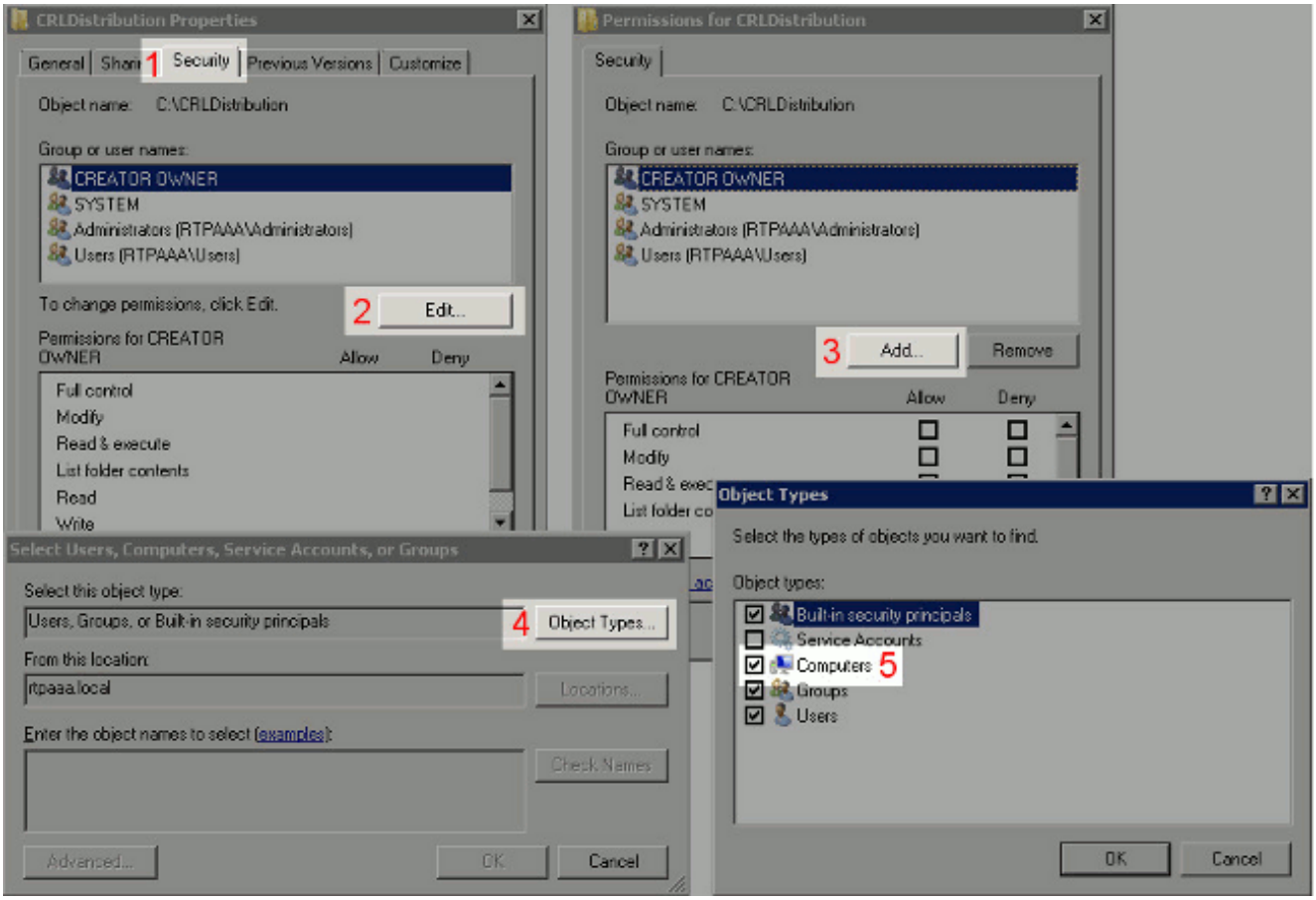
5. 要返回「選擇使用者」、「電腦」、「服務帳戶」或「組」視窗，請按一下**確定**。在「輸入要選擇的對象名稱」欄位中，輸入CA伺服器的電腦名稱，然後按一下**檢查名稱**。如果輸入的名稱有效，該名稱將刷新並帶有下劃線。按一下「**OK**」（確定）。



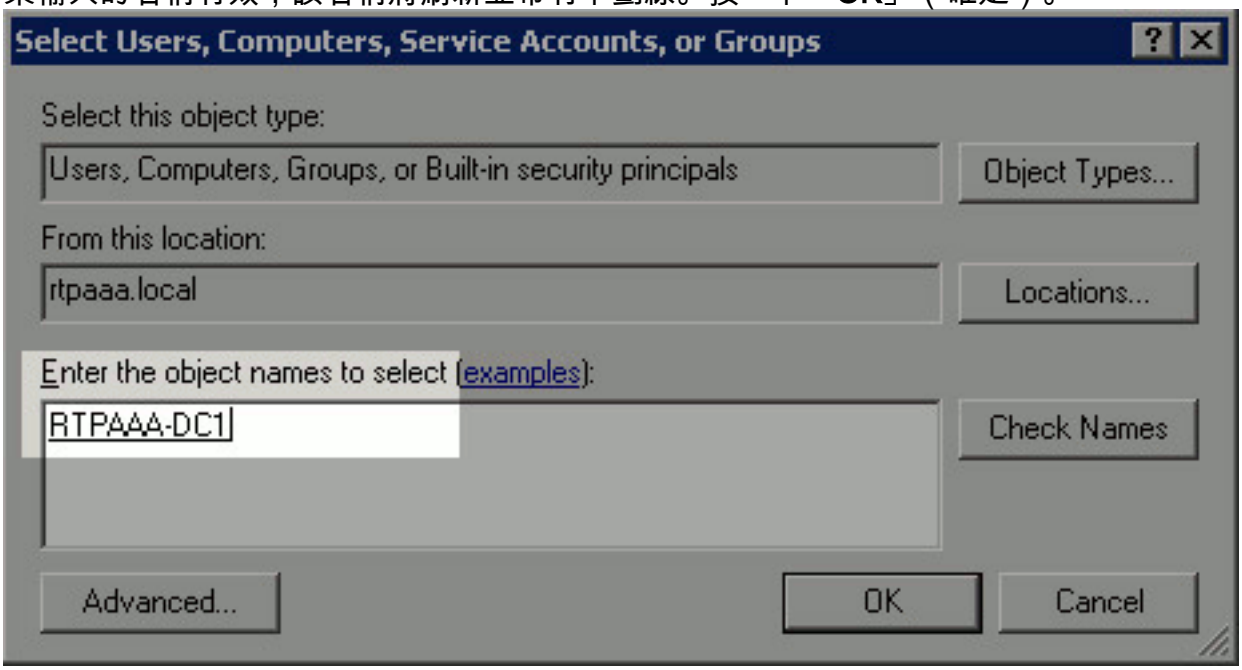
6. 在「組或使用者名稱」欄位中，選擇CA電腦。選中**Allow** for Full Control以授予對CA的完全訪問許可權。按一下「**OK**」（確定）。再次按一下**OK**以關閉「高級共用」視窗並返回到「屬性」視窗。



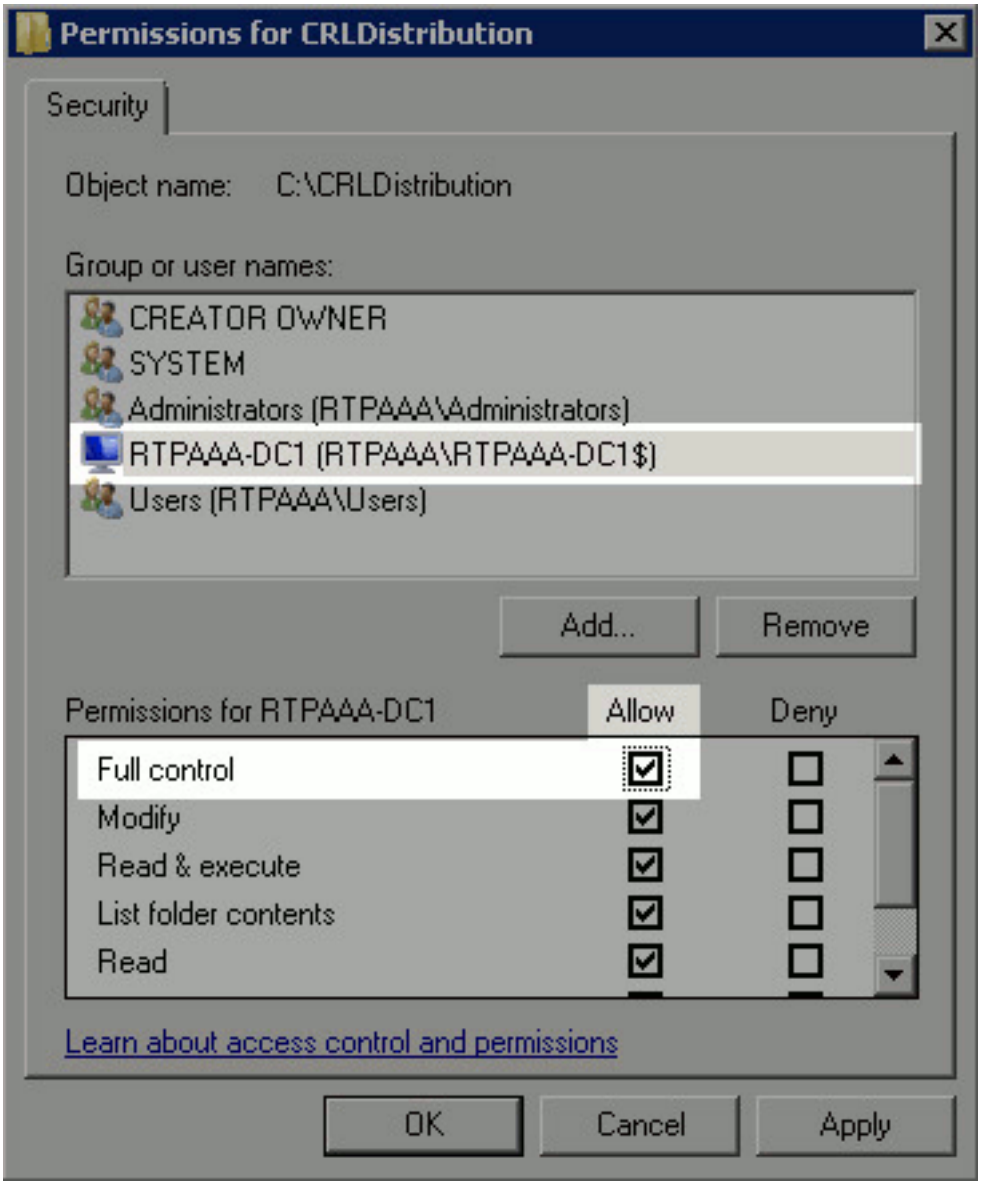
7. 為了允許CA將CRL檔案寫入新資料夾，請配置相應的安全許可權。按一下Security頁籤(1)，按一下**Edit**(2)，按一下**Add**(3)，按一下**Object Types**(4)，然後選中**Computers**覈取方塊(5)。



8. 在「輸入要選擇的對象名稱」欄位中，輸入CA伺服器的電腦名稱，然後按一下**檢查名稱**。如果輸入的名稱有效，該名稱將刷新並帶有下劃線。按一下「**OK**」（確定）。



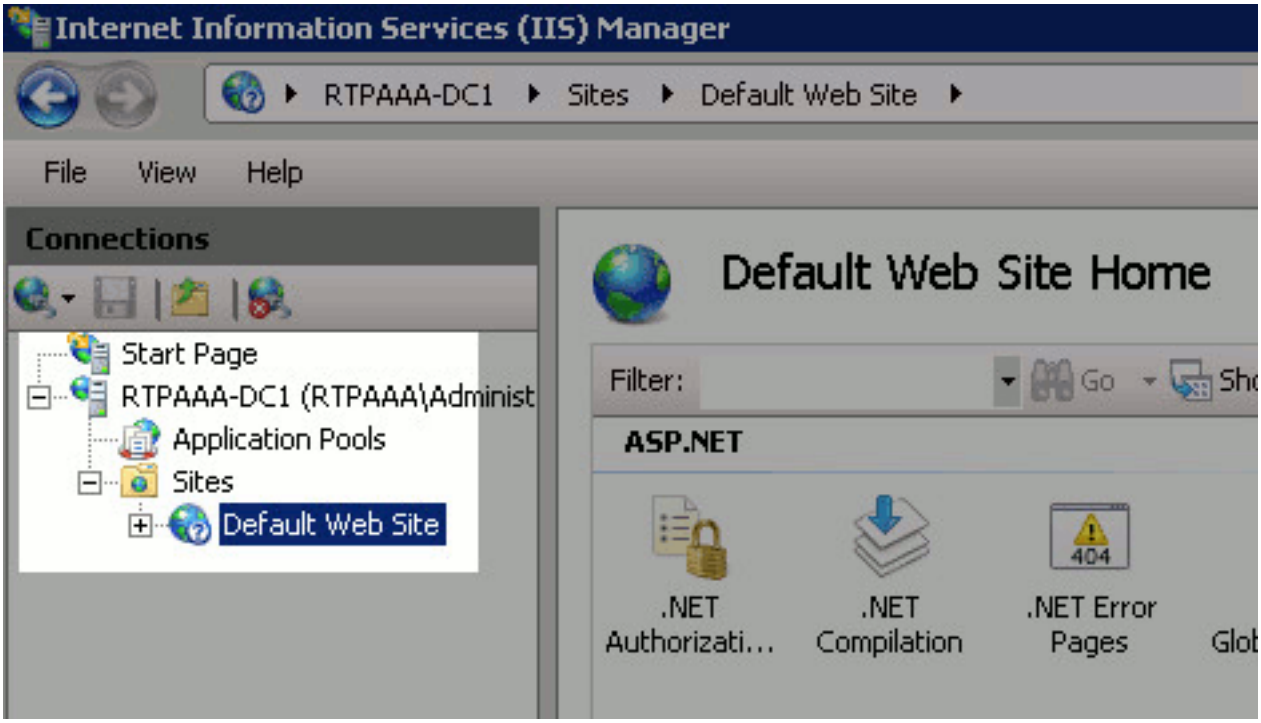
9. 在「組或使用者名稱」欄位中選擇CA電腦，然後選中**Allow**以授予對CA的完全訪問許可權。按一下**OK**，然後按一下**Close**以完成任務。



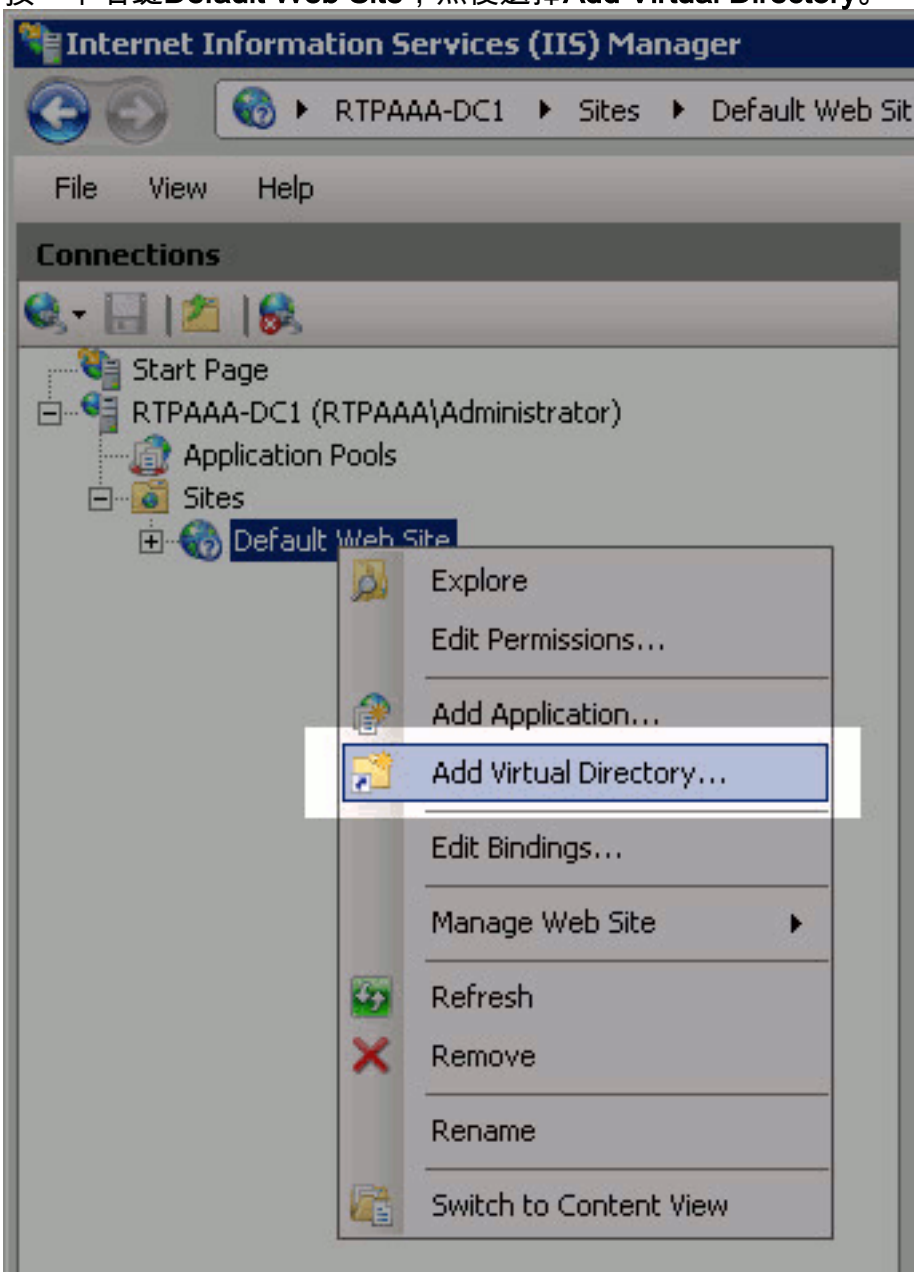
第2部分。在IIS中建立站點以公開新的CRL分發點

為了讓ISE訪問CRL檔案，請通過IIS訪問包含CRL檔案的目錄。

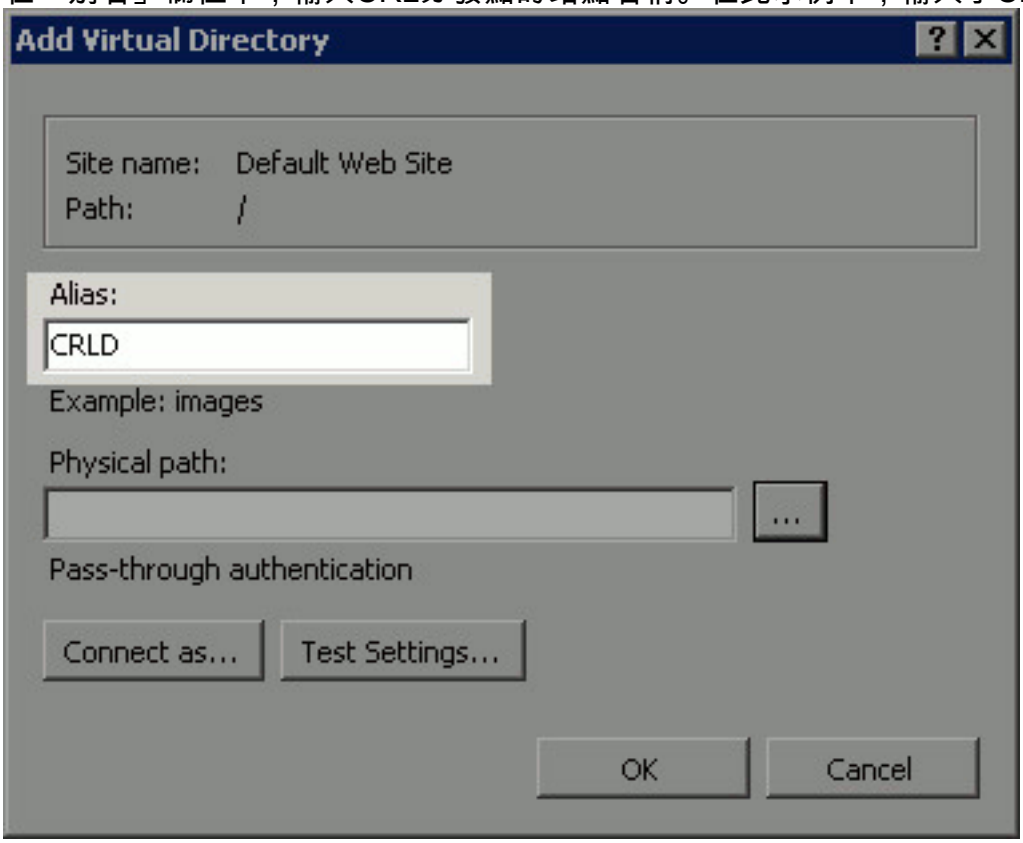
1. 在IIS伺服器工作列上，按一下**開始**。選擇**管理工具> Internet資訊服務(IIS)管理器**。
2. 在左側窗格（稱為控制檯樹）中，展開IIS伺服器名稱，然後展開**站點**。



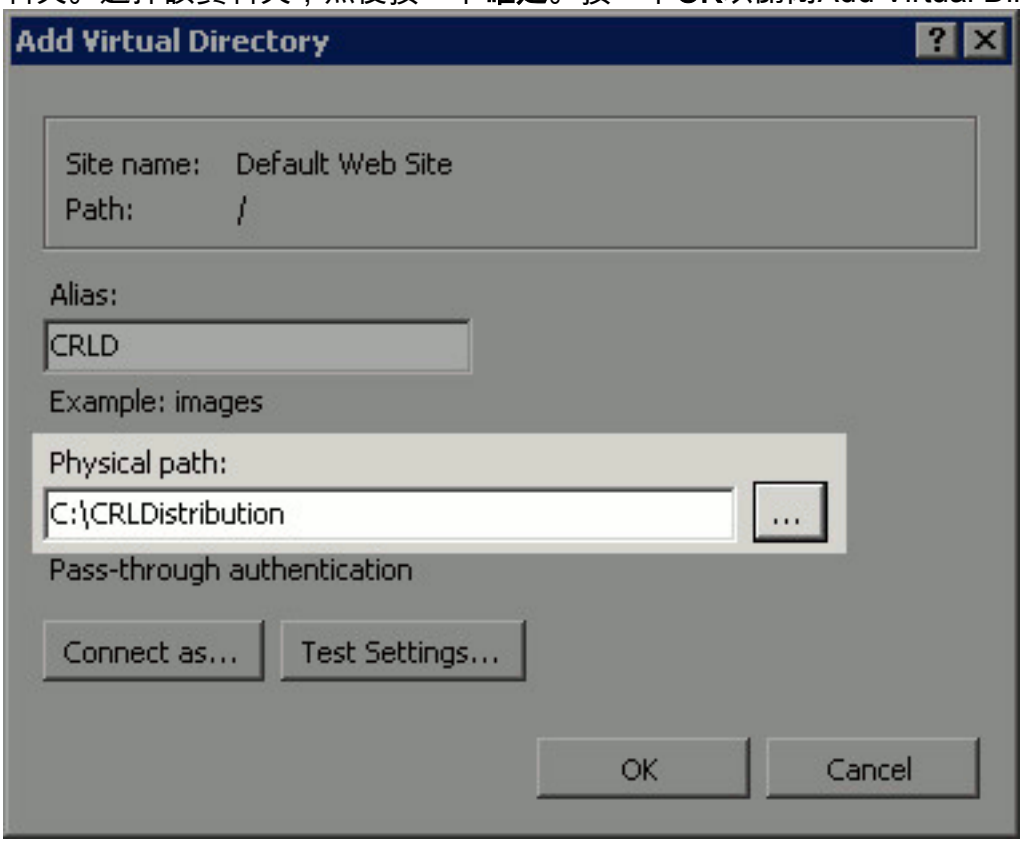
3. 按一下右鍵**Default Web Site**，然後選擇**Add Virtual Directory**。



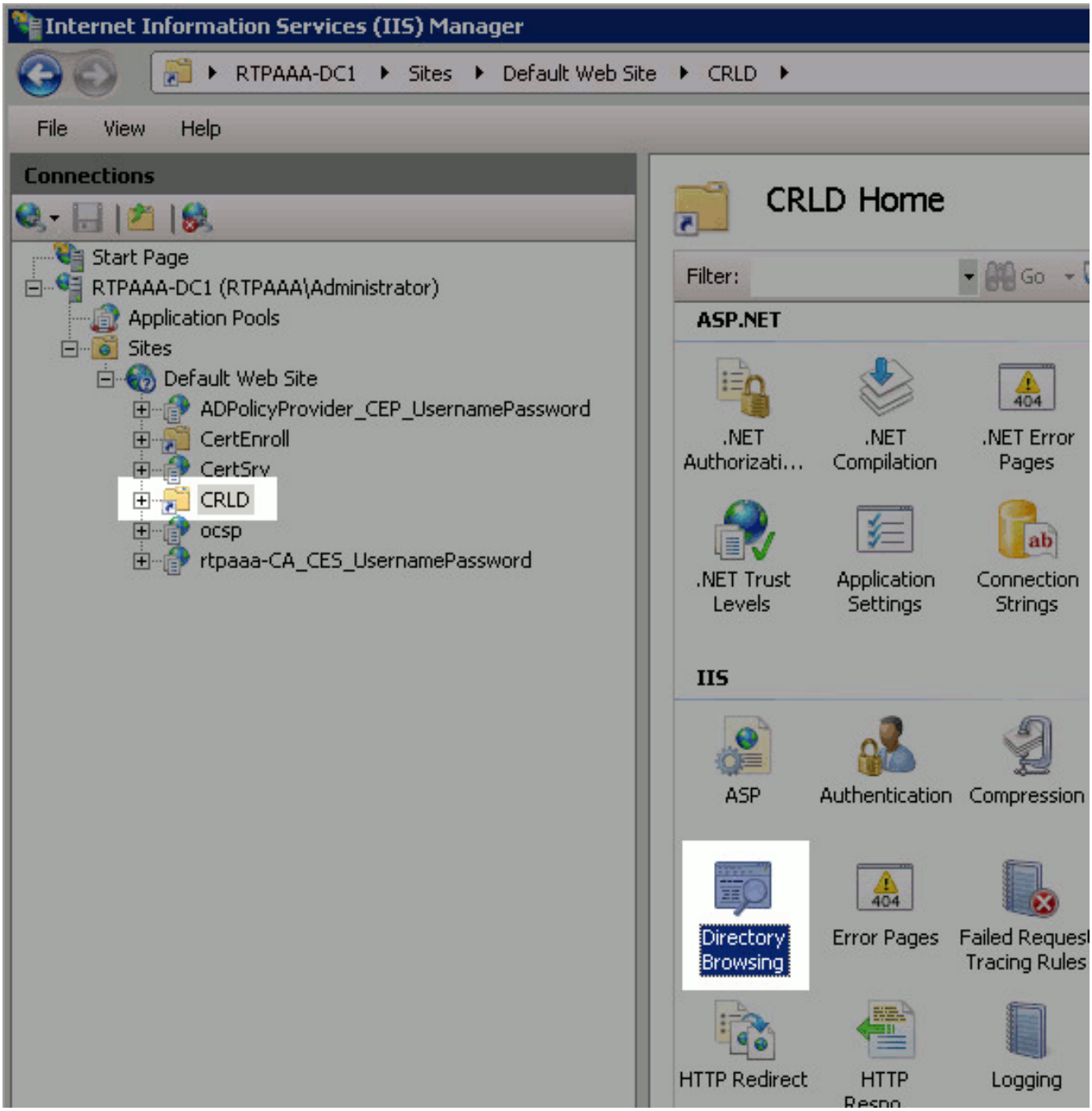
4. 在「別名」欄位中，輸入CRL分發點的站點名稱。在此示例中，輸入了CRLD。



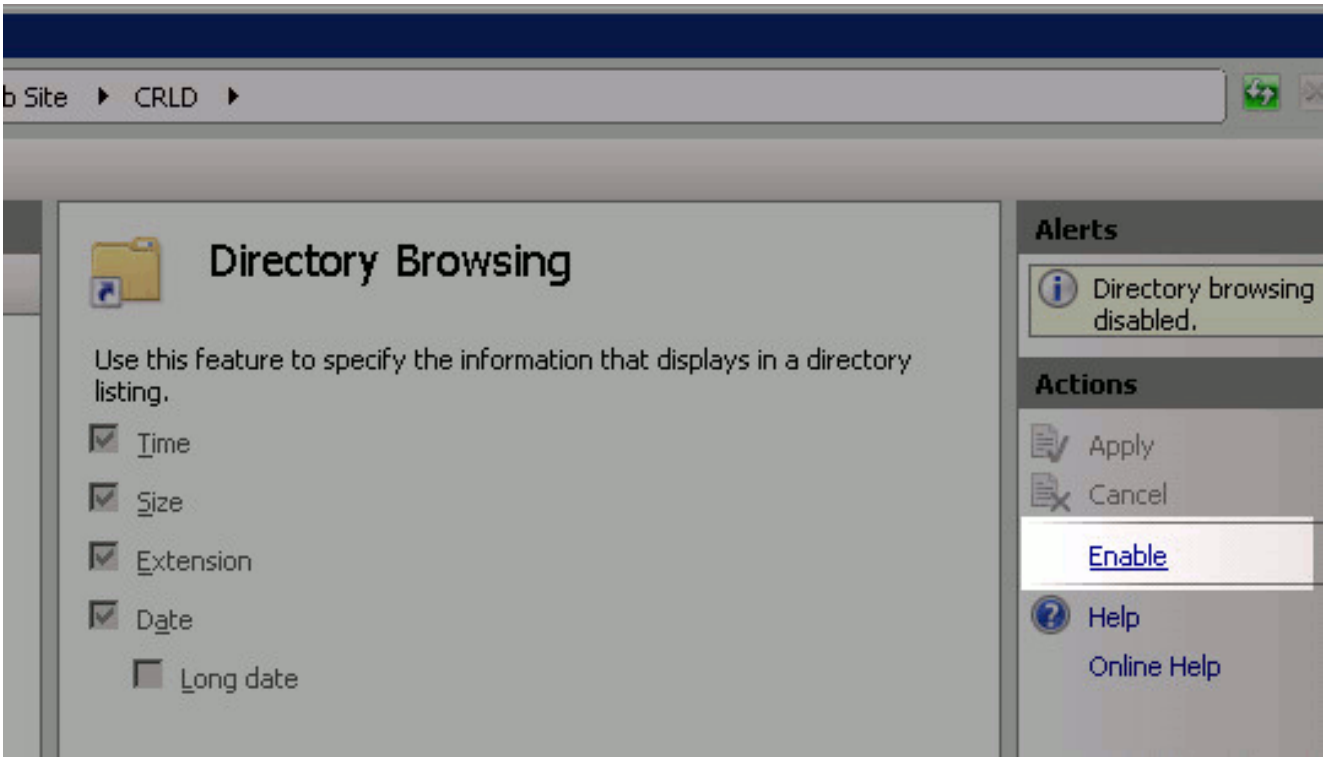
5. 按一下省略號(。..)在「物理路徑」(Physical path)欄位的右側，瀏覽到在第1部分中建立的資料夾。選擇該資料夾，然後按一下**確定**。按一下**OK**以關閉Add Virtual Directory視窗。



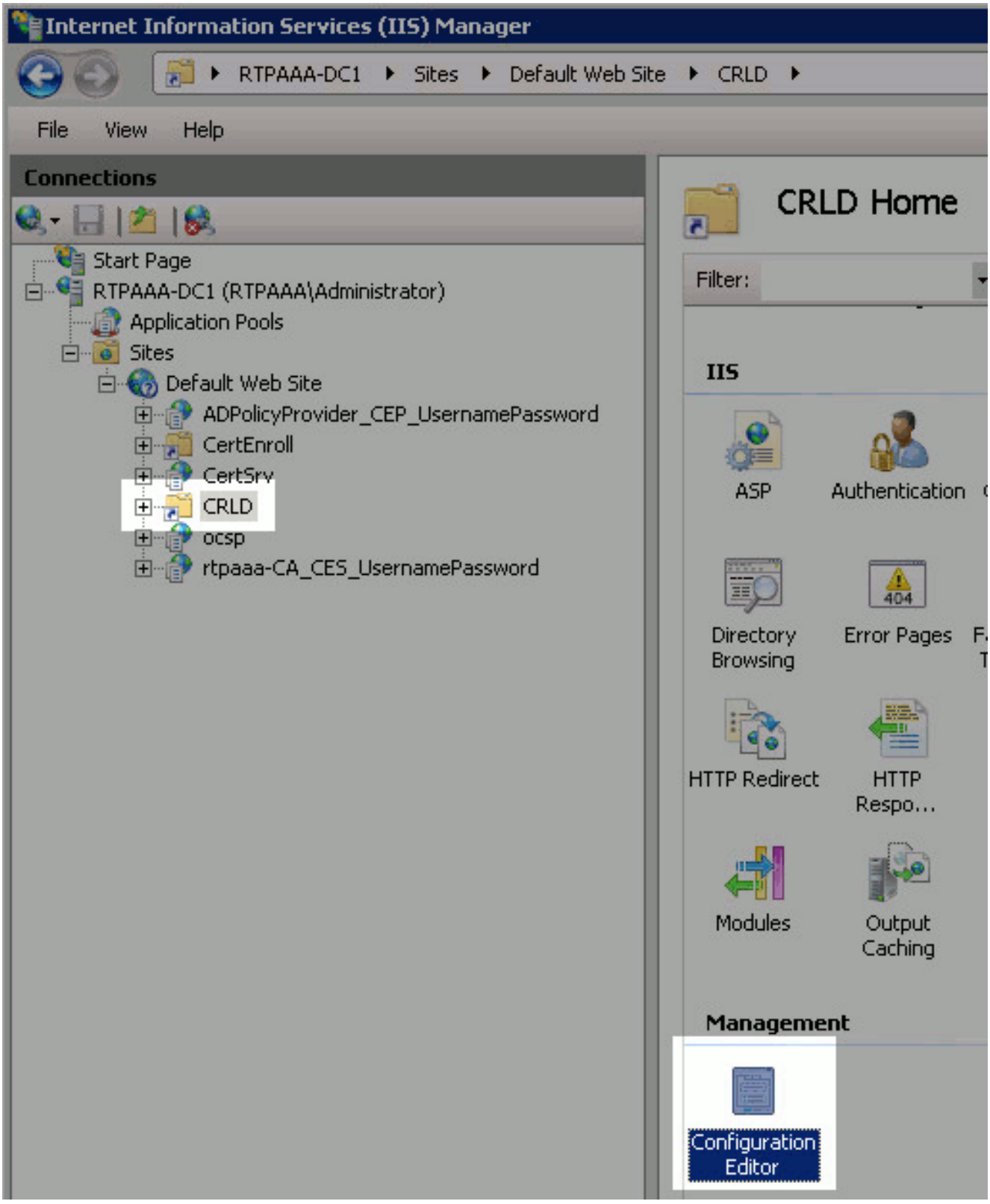
6. 在步驟4中輸入的站點名稱應在左窗格中突出顯示。如果沒有，現在就選擇。在中心窗格中，按兩下**Directory Browsing**。



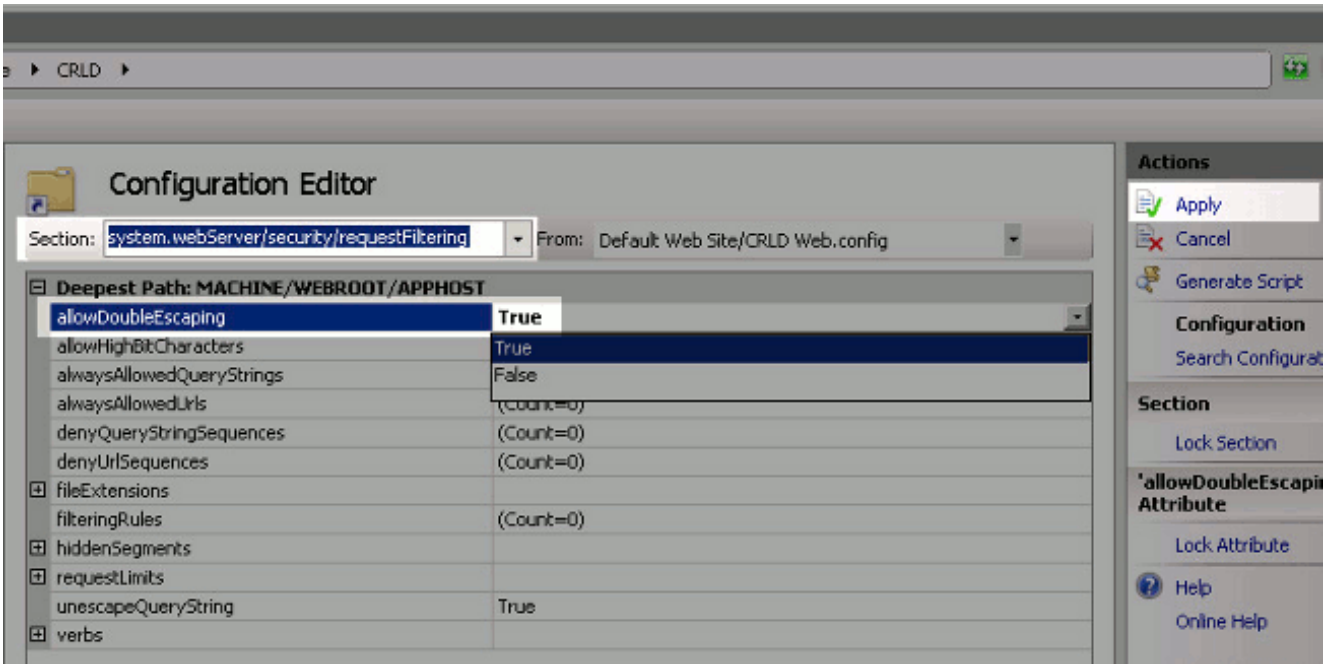
7. 在右窗格中，按一下**Enable**以啟用目錄瀏覽。



8. 在左窗格中，再次選擇站點名稱。在中心窗格中，按兩下**Configuration Editor**。



9. 在「部分」下拉選單中，選擇**system.webServer/security/requestFiltering**。在allowDoubleEscaping下拉選單中，選擇**True**。在右窗格中，按一下**Apply**。

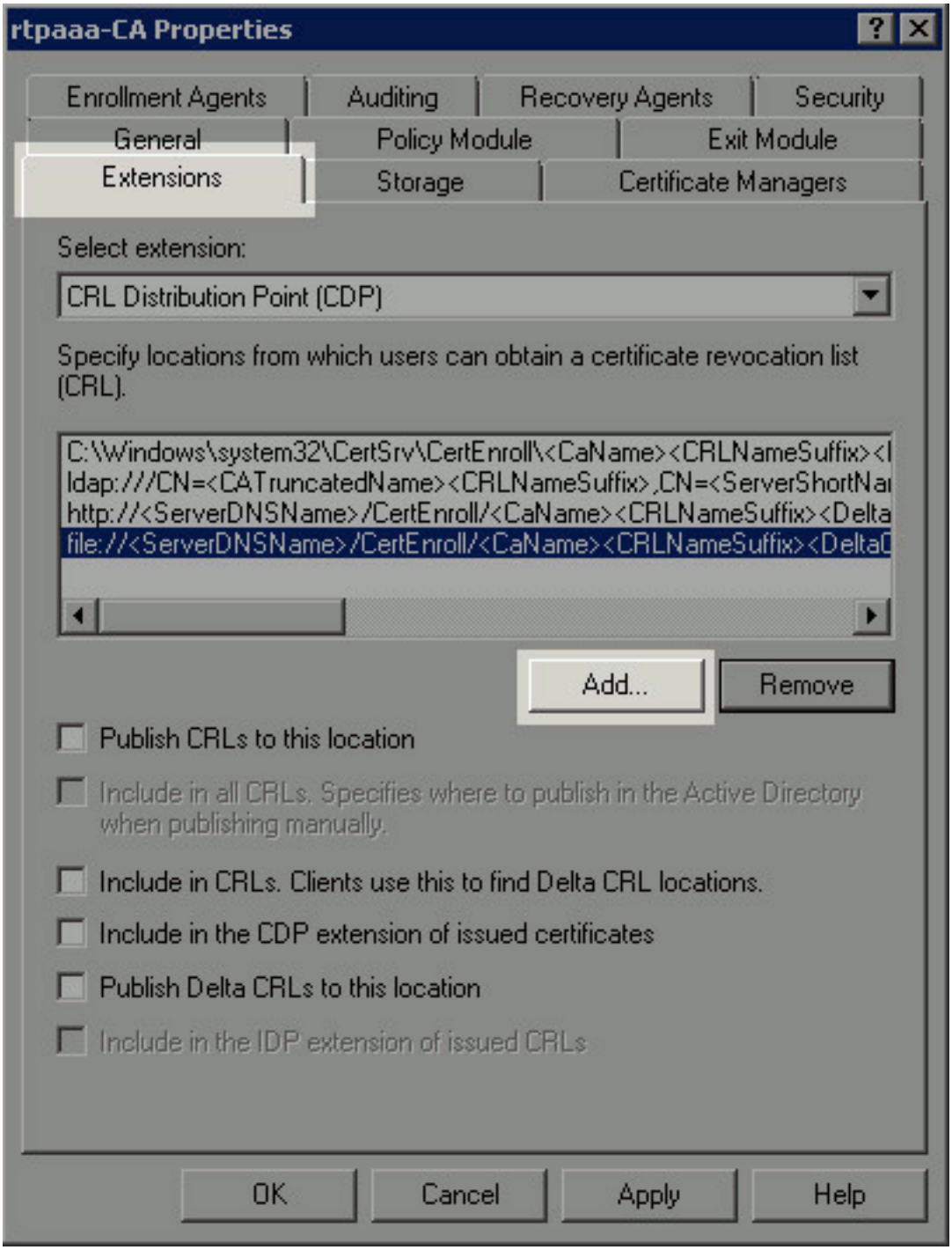


現在應可通過IIS訪問該資料夾。

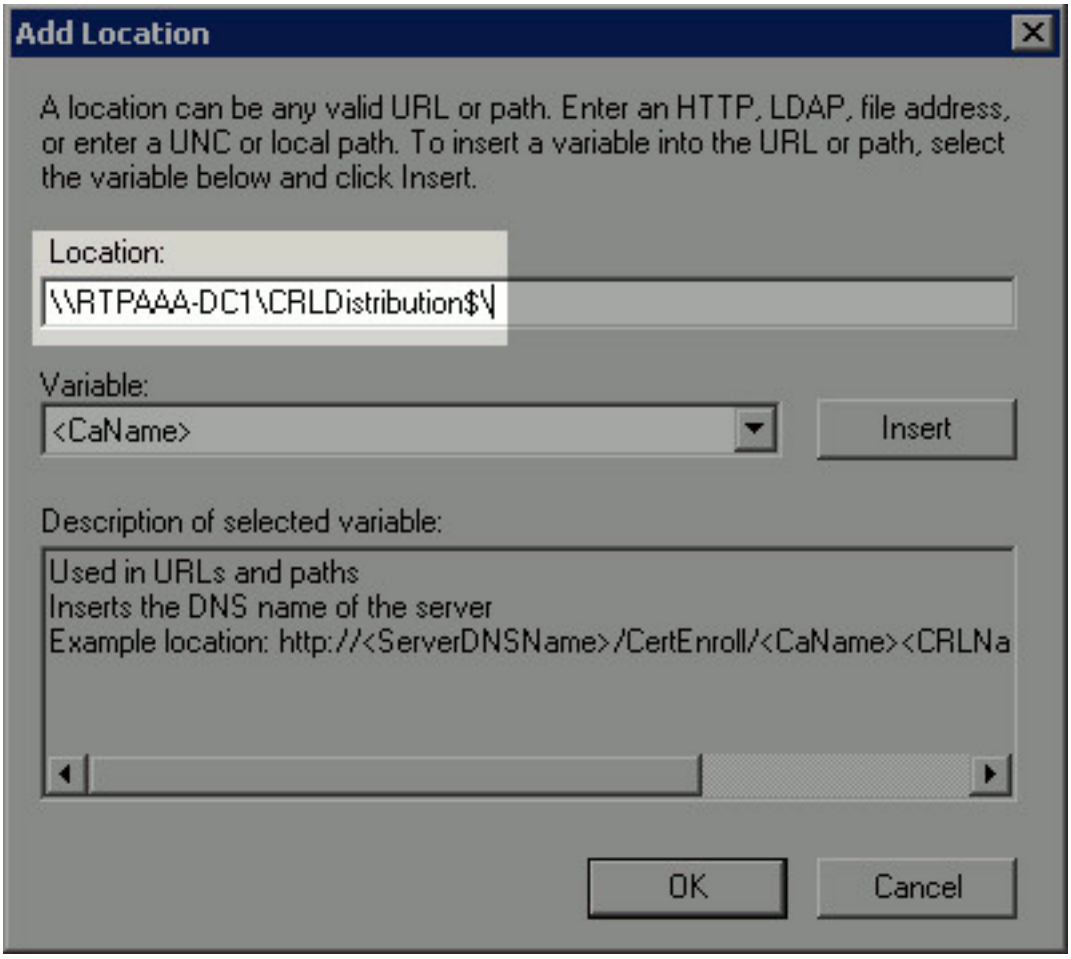
第3部分。配置Microsoft CA伺服器以將CRL檔案發佈到分發點

現在，已配置了一個新資料夾來容納CRL檔案，並且該資料夾已在IIS中公開，請配置Microsoft CA伺服器以將CRL檔案發佈到新位置。

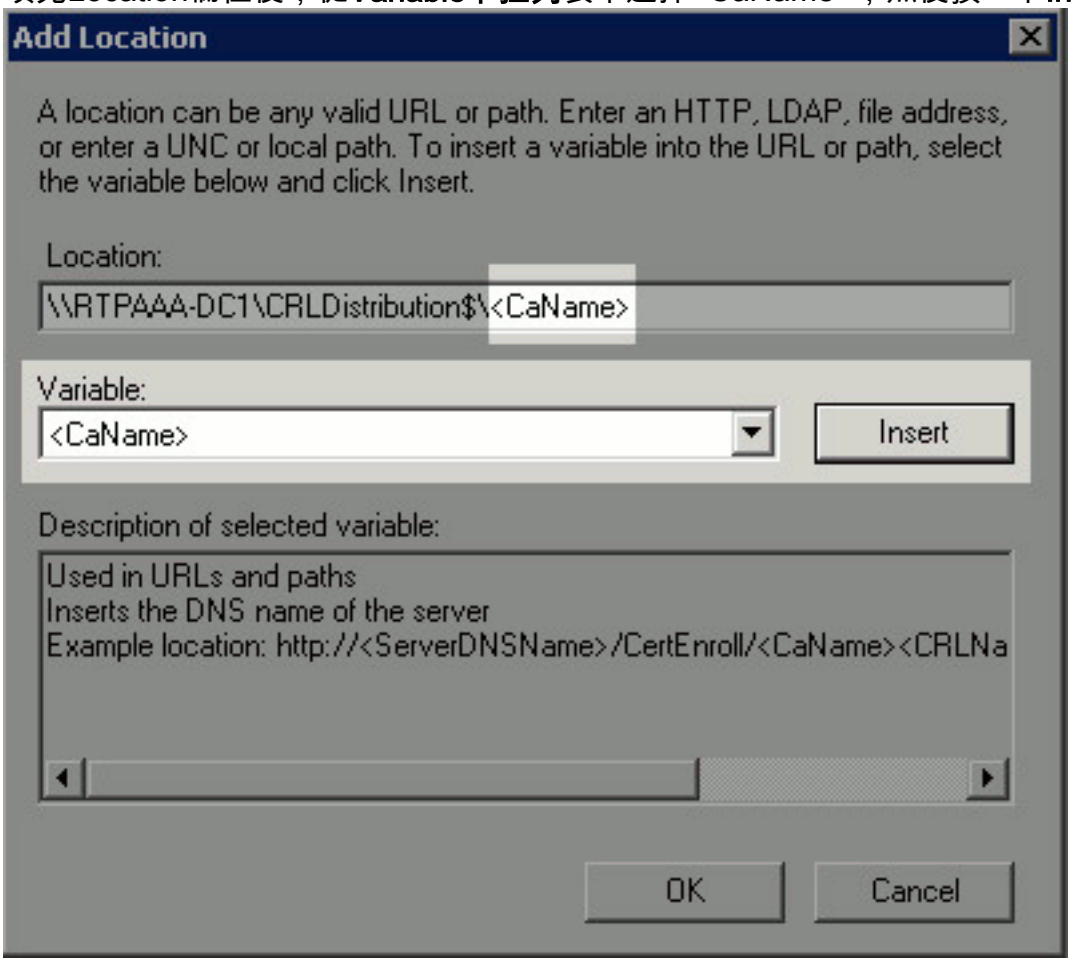
1. 在CA伺服器工作列上，按一下**開始**。選擇**Administrative Tools > Certificate Authority**。
2. 在左窗格中，按一下右鍵CA名稱。選擇**Properties**，然後按一下**Extensions**頁籤。要新增新的CRL分發點，請按一下**Add**。



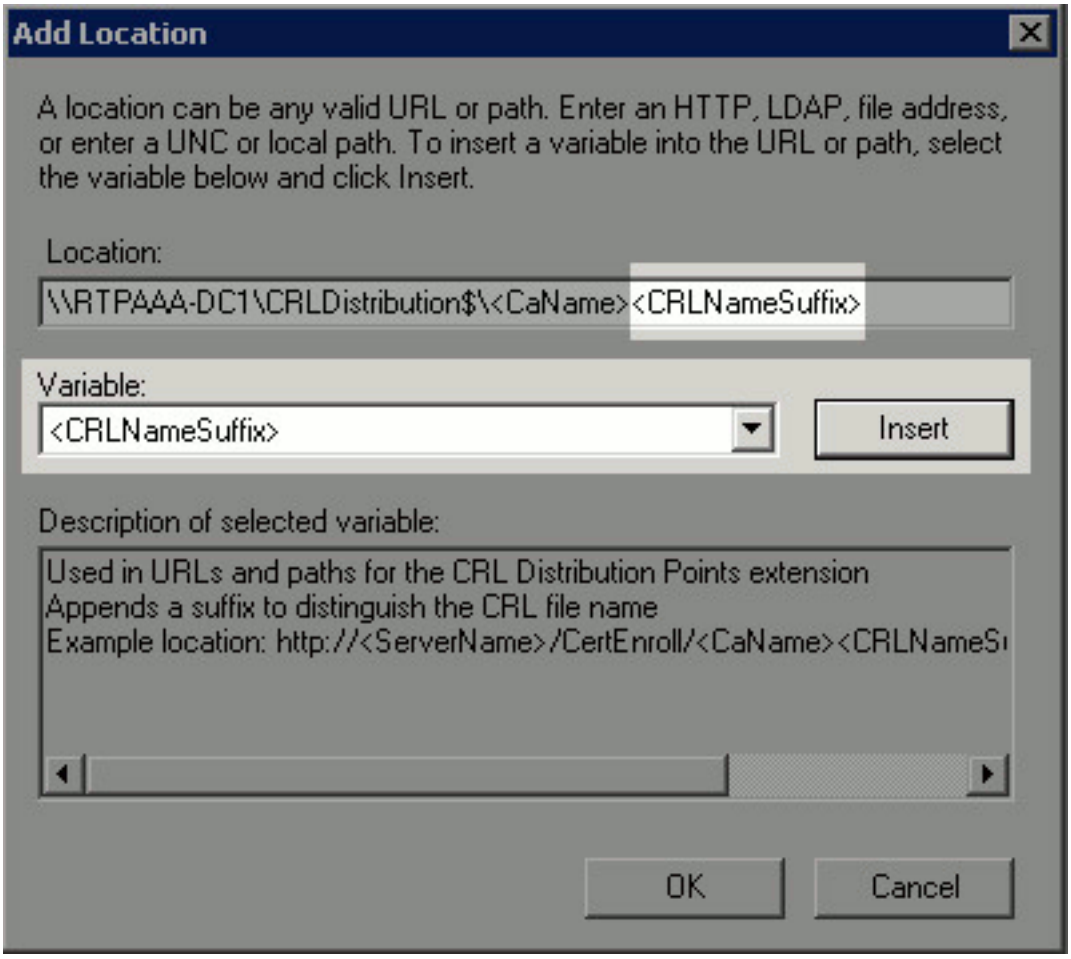
3. 在「位置」欄位中，輸入在第1部分中建立和共用的資料夾的路徑。在第1部分的示例中，路徑為：
   `\\RTPAAA-DC1\CRLDistribution$\`



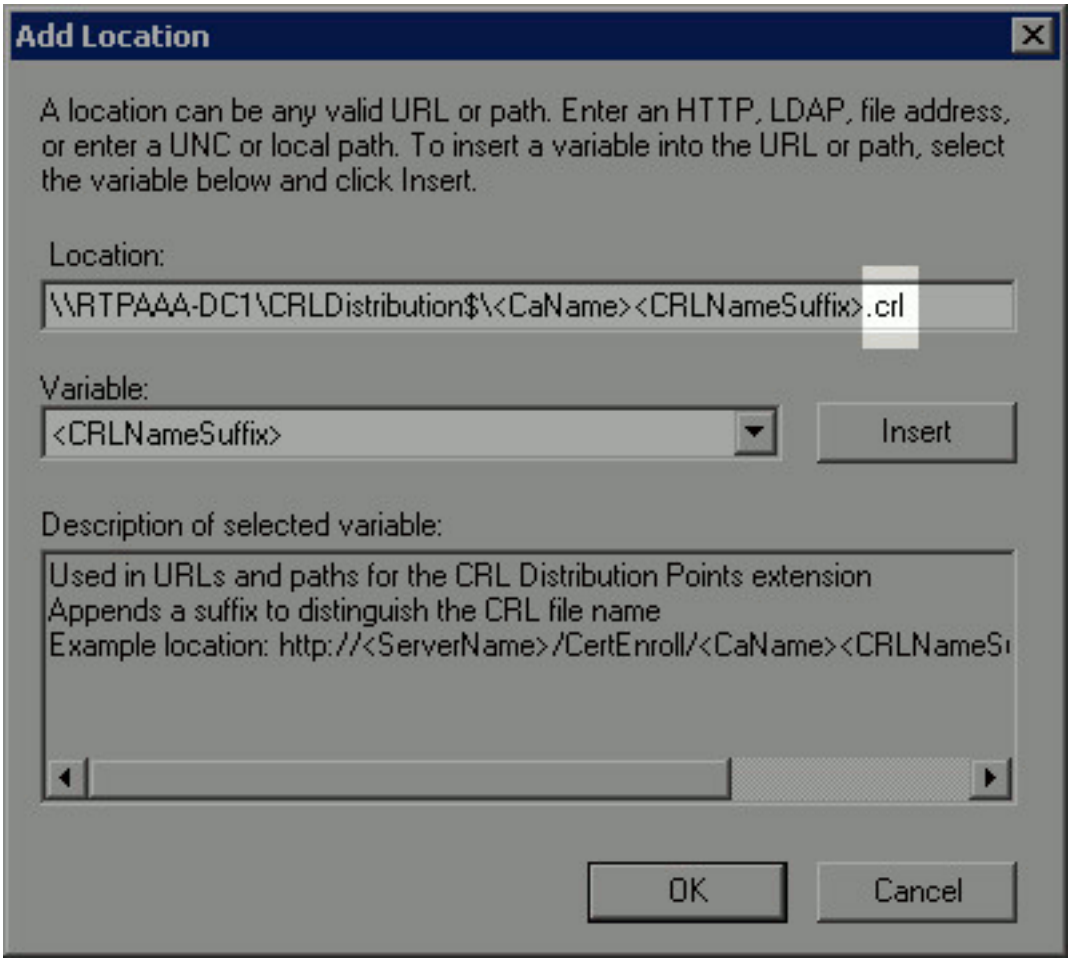
4. 填充Location欄位後，從**Variable下拉列**表中選擇<CaName>，然後按一下**Insert。**



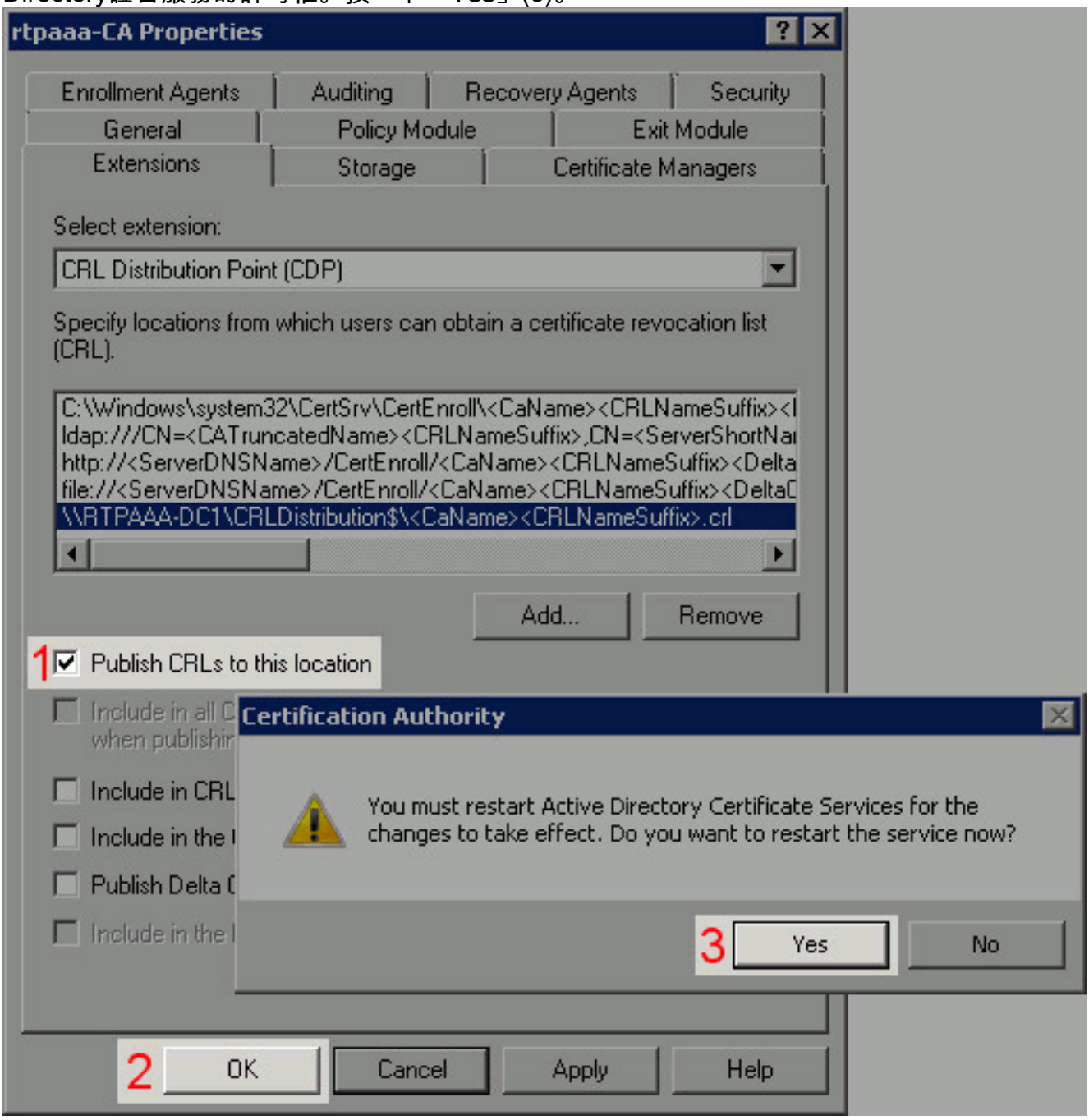
5. 從「變數」下拉選單中，選擇**<CRLNameSuffix>,**然後按一下**插入。**



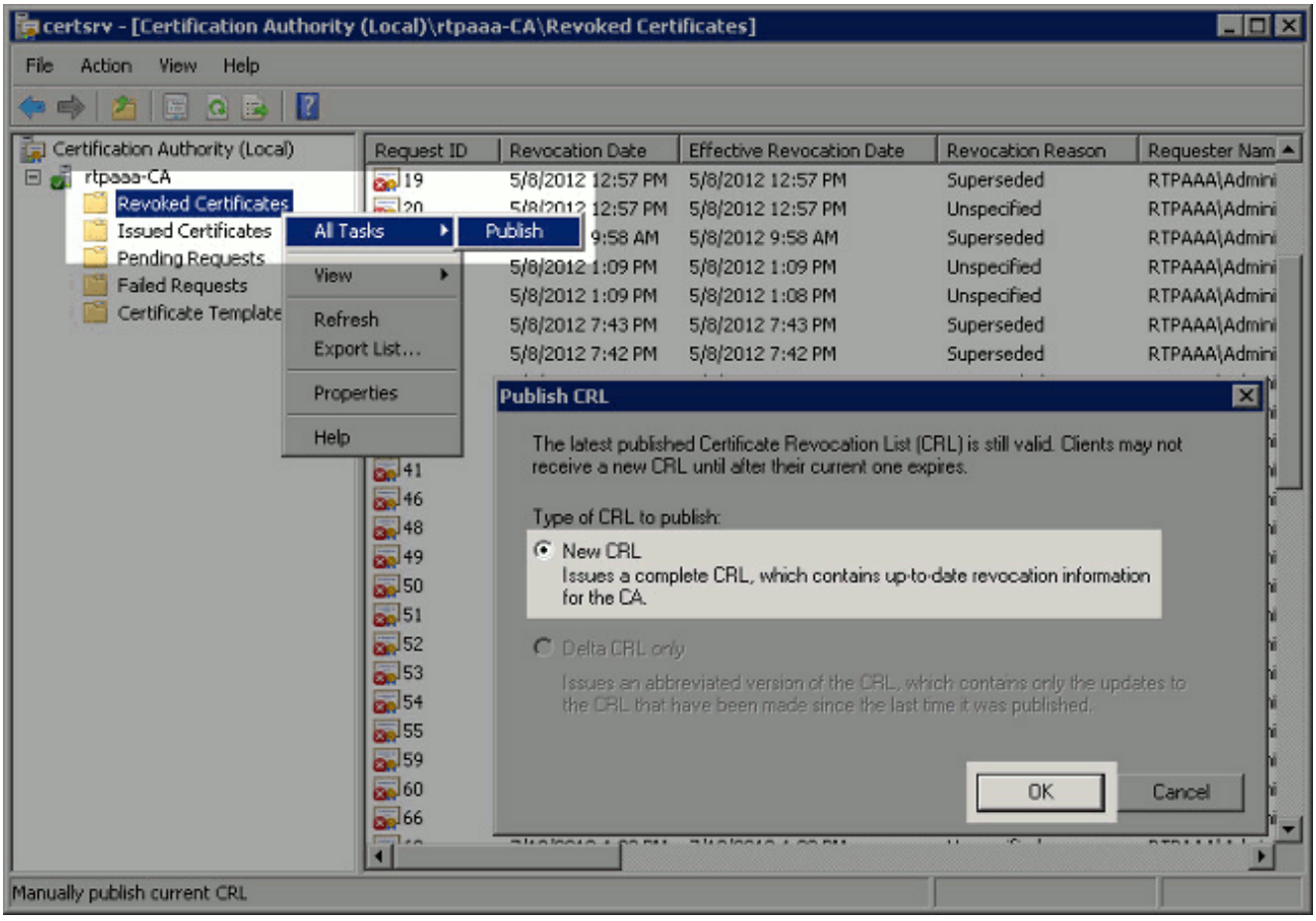
6. 在Location欄位中，將.crl附加到路徑的末尾。在此示例中，位置為：
`\\RTPAAA-DC1\CRLDistribution$\<CaName><CRLNameSuffix>.crl`



7. 按一下**OK**返回到「擴展」頁籤。選中**Publish CRLs to this location**覈取方塊(1)，然後按一下**OK**(2)以關閉「Properties（屬性）」視窗。出現一個提示符，提示獲得重新啟動Active Directory證書服務的許可權。按一下「**Yes**」(3)。



8. 在左窗格中，按一下右鍵**Revoked Certificates**。選擇**所有任務>發佈**。確保選中「New CRL（新建CRL）」，然後按一下**「OK（確定）」**。

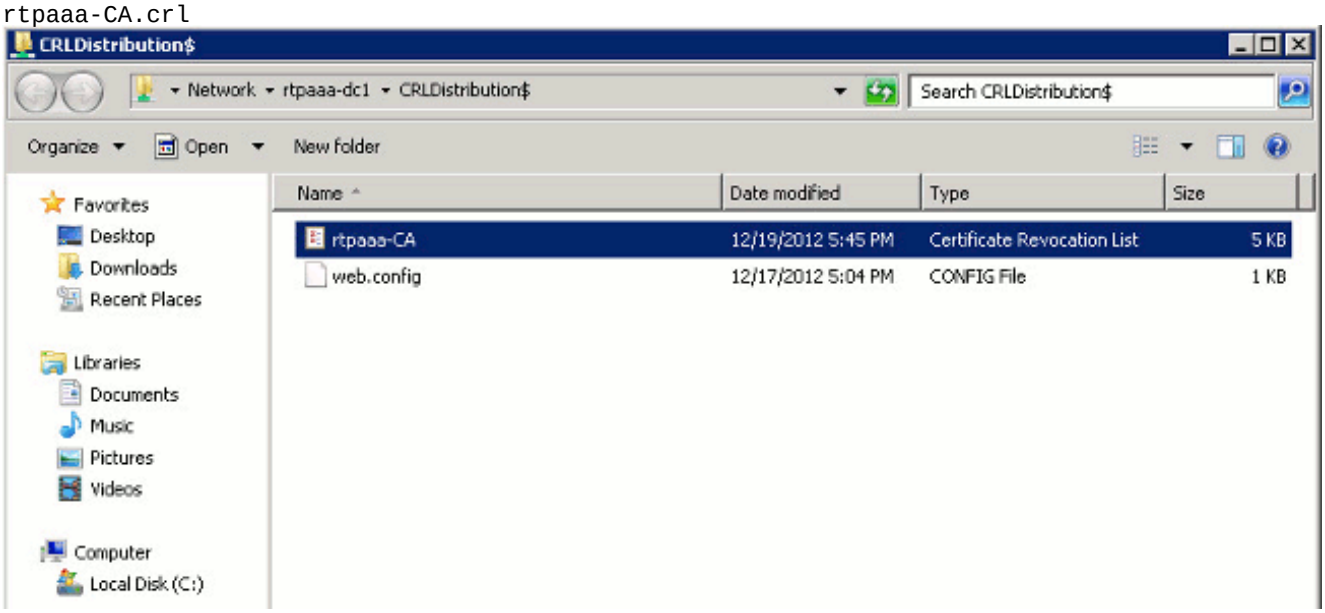


Microsoft CA伺服器應在第1節中建立的資料夾中建立新的.crl檔案。如果成功建立新的CRL檔案，則按一下「確定」後將不會出現對話方塊。如果返回有關新分發點資料夾的錯誤，請仔細重複本節中的步驟。

第4節：驗證CRL檔案是否存在且可通過IIS訪問

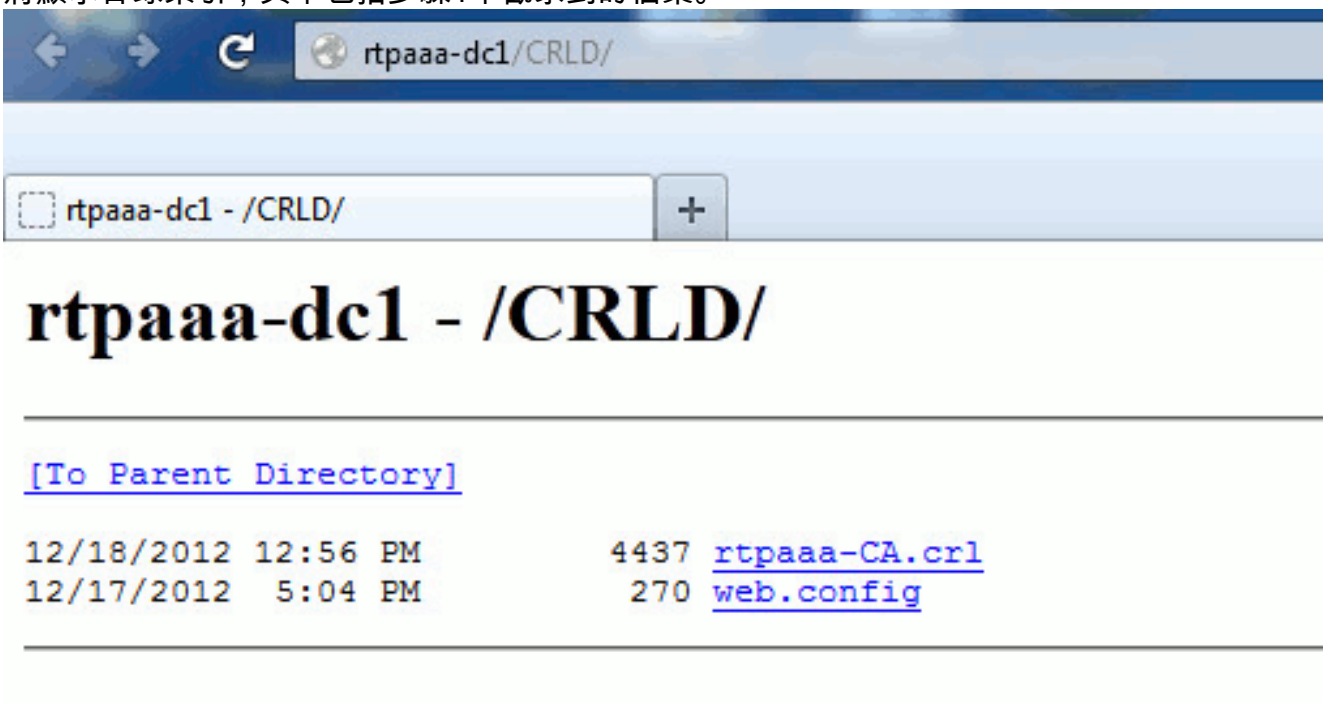
開始本節之前，請確認新的CRL檔案是否存在，以及是否可以通過另一工作站的IIS訪問這些檔案。

1. 在IIS伺服器上，開啟第1部分中建立的資料夾。應存在一個.crl檔案，其格式為<CANAME>.crl，其中<CANAME>是CA伺服器的名稱。在此範例中，檔案名稱為：`rtpaaa-CA.crl`



2. 從網路上的工作站（最好與ISE主管理節點位於同一網路），開啟Web瀏覽器並瀏覽到http://<SERVER>/<CRLSITE>，其中<SERVER>是在第2部分中配置的IIS伺服器的伺服器名

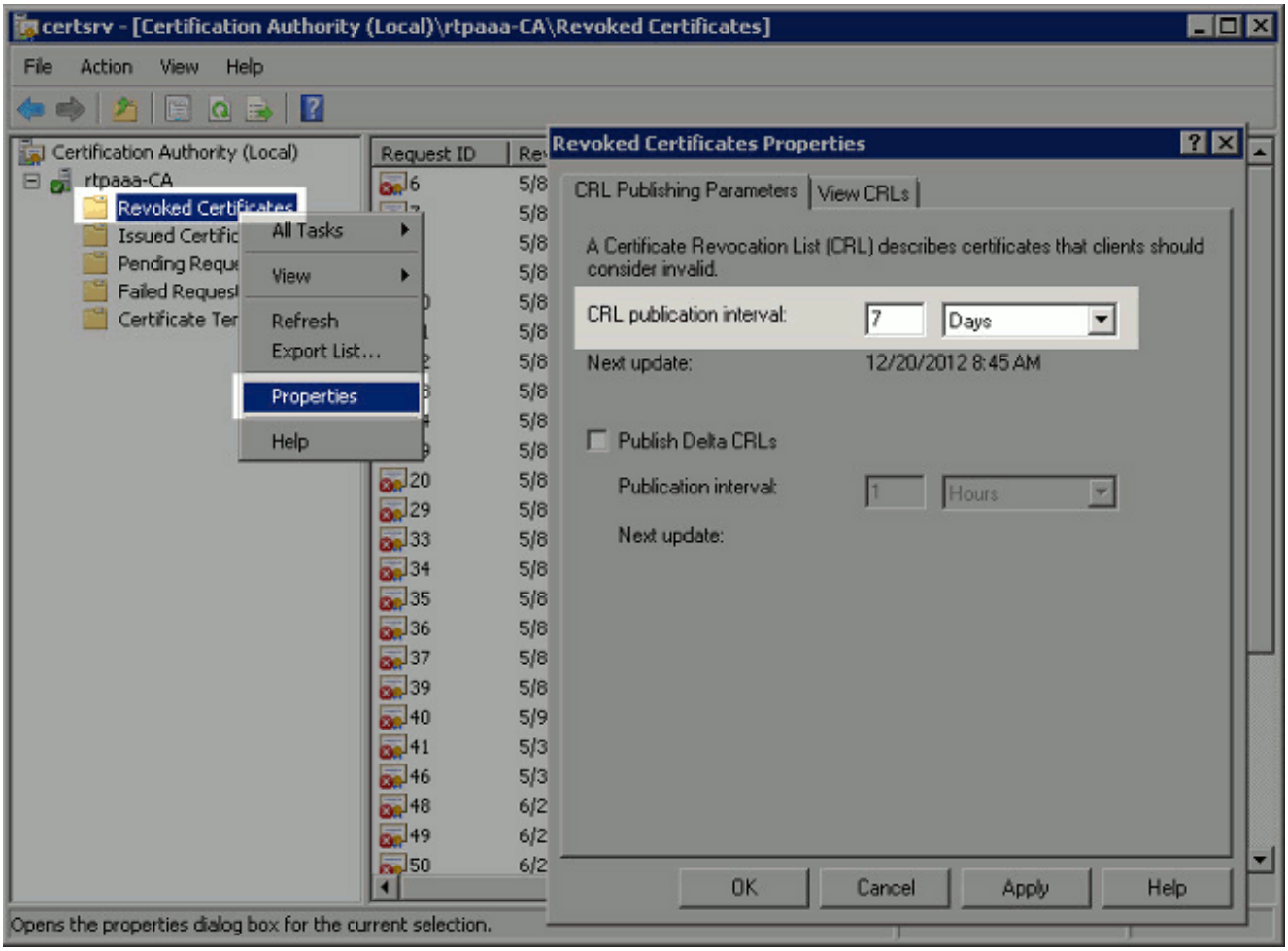
稱，<CRLSITE>是在第2部分中為分發點選擇的站點名稱。在此示例中，URL為：
`http://RTPAAA-DC1/CRLD`
將顯示目錄索引，其中包括步驟1中觀察到的檔案。



第5部分。配置ISE以使用新的CRL分發點

在將ISE配置為檢索CRL之前，定義發佈CRL的時間間隔。確定此間隔的策略不在本檔案的範圍之內。潛在值（在Microsoft CA中）為1小時到411年（含）。預設值為1週。確定適合您環境的間隔後，請使用以下說明設定間隔：

1. 在CA伺服器工作列上，按一下**開始**。選擇**Administrative Tools > Certificate Authority**。
2. 在左窗格中，展開CA。按一下右鍵**Revoked Certificates**資料夾，然後選擇**Properties**。
3. 在「CRL發佈間隔」欄位中，輸入所需的數字並選擇時間段。按一下**OK**關閉視窗並應用更改。在本示例中，配置了7天的發佈間隔。



您現在應該確認幾個登錄檔值，這將有助於確定ISE中的CRL檢索設定。

4. 輸入**certutil -getreg CA\Clock***命令以確認ClockSkew值。預設值為10分鐘。輸出示例：

```
Values:
    ClockSkewMinutes        REG_DWORS = a (10)
CertUtil: -getreg command completed successfully.
```

5. 輸入**certutil -getreg CA\CRLov*命令**以驗證是否已手動設定CRLOverlapPeriod。預設情況下，CRLOverlapUnit值為0，表示未設定手動值。如果該值不是0，請記錄該值和單位。輸出示例：

```
Values:
    CRLOverlapPeriod      REG_SZ = Hours
    CRLOverlapUnits        REG_DWORD = 0
CertUtil: -getreg command completed successfully.
```

6. 輸入**certutil -getreg CA\CRLpe***命令以驗證CRLeriod（已在步驟3中設定）。輸出示例：

```
Values:
    CRLPeriod      REG_SZ = Days
    CRLUnits        REG_DWORD = 7
CertUtil: -getreg command completed successfully.
```

7. 按如下方式計算CRL寬限期：如果在步驟5中設定CRLOverlapPeriod:重疊= CRLOverlapPeriod（分鐘）；其他：重疊=(CRLeriod / 10)，分鐘如果重疊大於720，則重疊= 720如果重疊<(1.5 * ClockSkewMinutes)，則重疊=(1.5 * ClockSkewMinutes)如果OVERLAP > CRLPeriod，則重疊= CRLPeriod，以分鐘為單位寬限期= 720分鐘+ 10分鐘= 730分鐘範例：

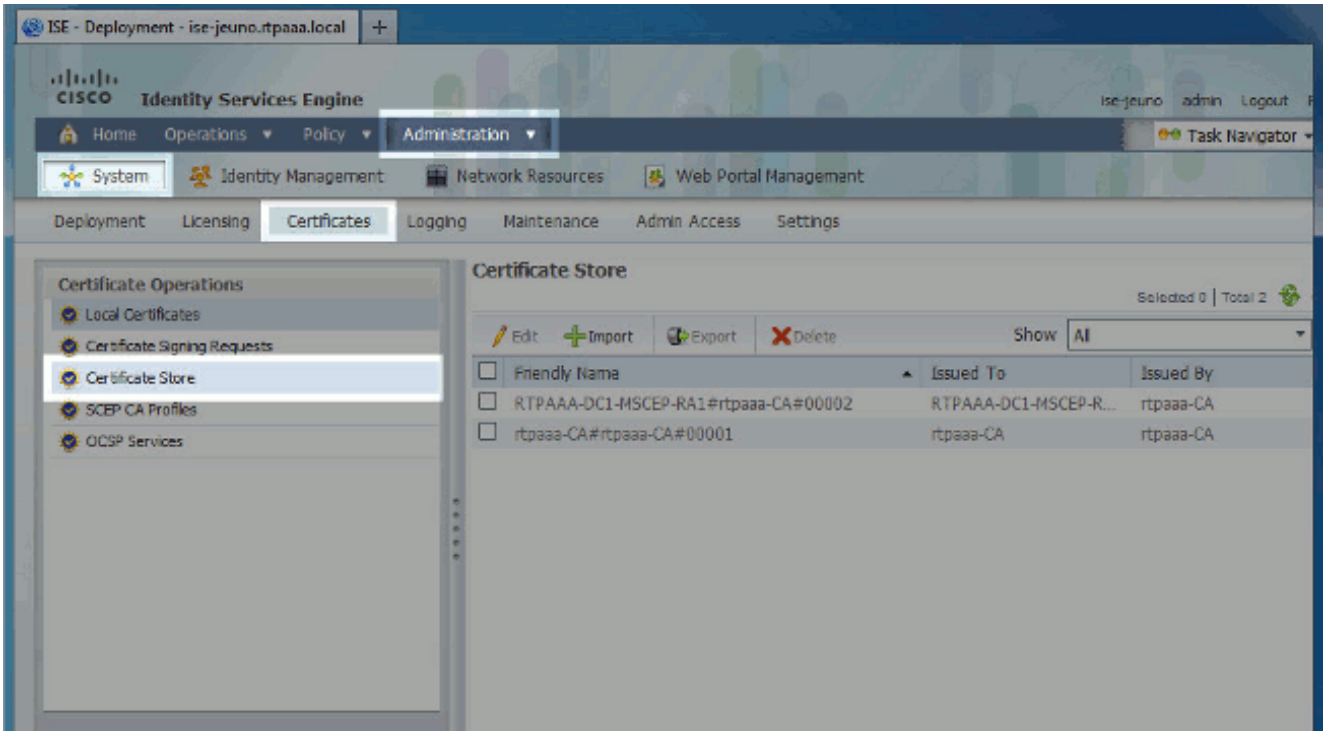
```
As stated above, CRLPeriod was set to 7 days, or 10248 minutes and
CRLOverlapPeriod was not set.

a. OVERLAP = (10248 / 10) = 1024.8 minutes
```

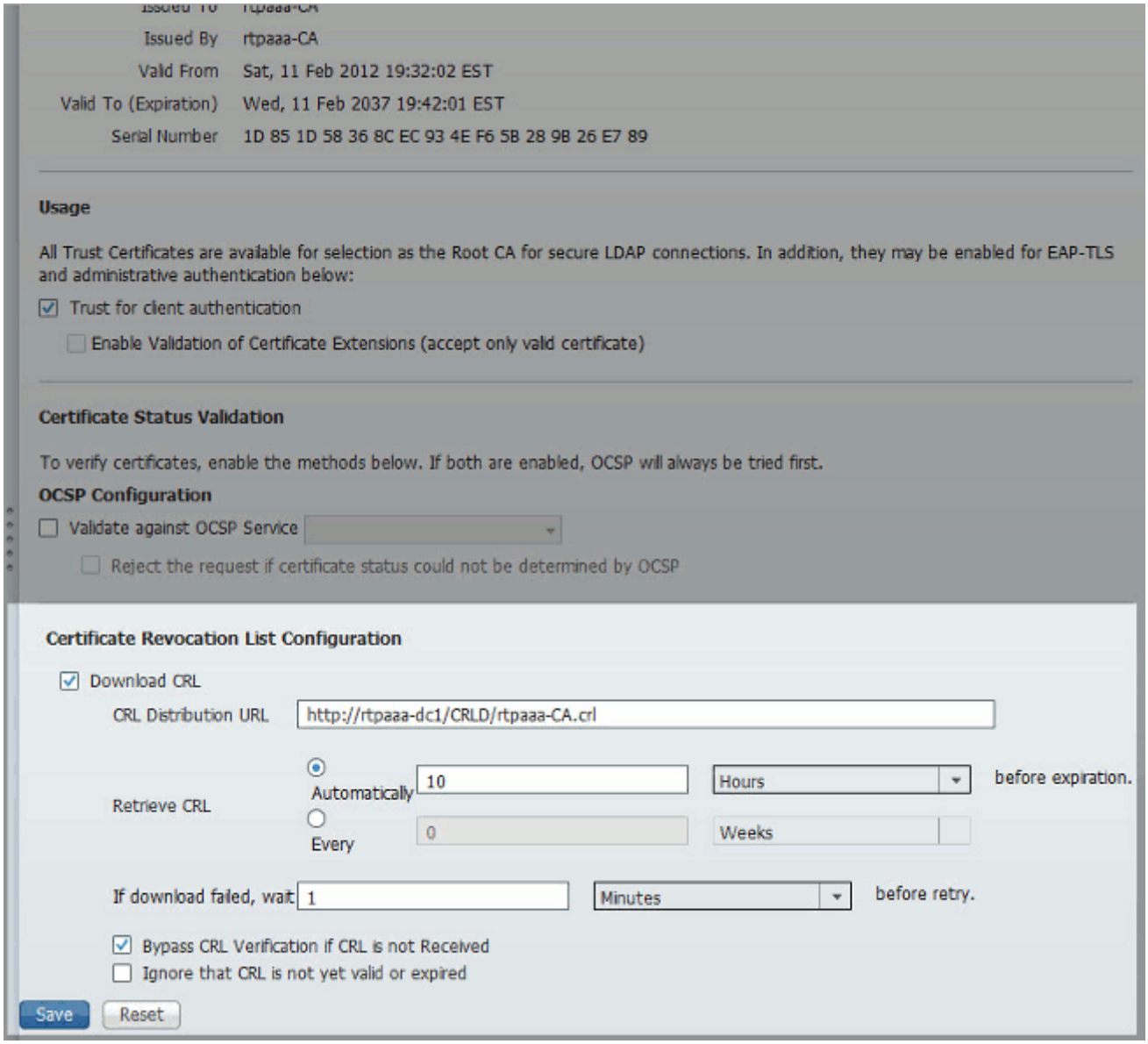
```
b. 1024.8 minutes is > 720 minutes : OVERLAP = 720 minutes
c. 720 minutes is NOT < 15 minutes : OVERLAP = 720 minutes
d. 720 minutes is NOT > 10248 minutes : OVERLAP = 720 minutes
e. Grace Period = 720 minutes + 10 minutes = 730 minutes
```

計算出的寬限期是CA發佈下一個CRL到當前CRL到期之間的時間量。需要配置ISE以相應地檢索CRL。

8. 登入到主Admin節點，然後選擇**Administration > System > Certificates**。在左窗格中，選擇**Certificate Store**。



9. 選中要為其配置CRL的CA證書旁邊的證書儲存覈取方塊。按一下「**Edit**」。
10. 在視窗底部附近，選中**Download CRL**覈取方塊。
11. 在「CRL分發URL」欄位中，輸入CRL分發點的路徑，該分發點包括第2部分建立的.crl檔案。在此示例中，URL為：
    `http://RTPAAA-DC1/CRLD/rtpaaa-ca.crl`
12. 可以將ISE配置為定期或根據過期時間（通常也是定期間隔）檢索CRL。 當CRL發佈間隔為靜態時，使用後一個選項可獲得更及時的CRL更新。按一下**Automatically**單選按鈕。
13. 將檢索的值設定為小於在步驟7中計算的寬限期的值。如果值集大於寬限期，ISE將在CA發佈下一個CRL之前檢查CRL分發點。在此示例中，寬限期計算為730分鐘或12小時10分鐘。檢索將使用10小時的值。
14. 根據您的環境設定重試間隔。如果ISE無法按上一步中配置的間隔檢索CRL，它將按此較短間隔重試。
15. 選中**Bypass CRL Verification if CRL is not Received**覈取方塊，如果ISE在其上次下載嘗試中無法檢索此CA的CRL，則允許基於證書的身份驗證正常進行（並且不進行CRL檢查）。如果未選中此覈取方塊，則如果無法檢索CRL，則此CA頒發的證書的所有基於證書的身份驗證都將失敗。
16. 選中**Ignore that CRL is not not valid or expired**覈取方塊，以允許ISE使用已過期（或尚未有效）的CRL檔案，就好像這些檔案有效。如果未選中此覈取方塊，則ISE會將CRL視為在其生效日期之前和下次更新時間之後無效。按一下「**Save**」以完成設定。



驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- 技術支援與文件 - Cisco Systems