Ticket: 　<https://redmine.etzone.net/issues/31649>

優化目標:

1. ServicePointManager.ServerCertificateValidationCallback = 需要一個handler去記錄憑證的問題

* 呼叫 ServerCertificateValidationCallback 的時間點

在.NET中，**ServerCertificateValidationCallback** 會在建立SSL/TLS连接時執行。具體來說，當客戶端（即你的應用程序）與服務器完成SSL/TLS握手過程，並且服務器已經提供了其憑證後，該回調函數就會被調用。

* 以下是一些常呼叫ServerCertificateValidationCallback的時間
  + 使用 HttpWebRequest 或 HttpClient 進行 HTTPS 請求。
  + 使用 SslStream 類手動管理SSL/TLS连接。
  + 使用基於SSL/TLS的其他協議，例如FTP over SSL。
* ServerCertificateValidationCallback參數:
  + (object sender, X509Certificate certificate, X509Chain chain, SslPolicyErrors sslPolicyErrors)
* SslPolicyErrors的內容

一張含有 文字, 螢幕擷取畫面, 字型, 行 的圖片

自動產生的描述

* **X509ChainStatusFlags 列表**
* **NoError**: 沒有錯誤。
* **NotTimeValid**: 憑證過期或者還未生效。
* **NotTimeNested**: 上下文中存在一個憑證的有效期不是完全包含在簽發該憑證的上級憑證的有效期內。
* **Revoked**: 憑證被撤銷。
* **NotSignatureValid**: 憑證的數字簽名無效。
* **NotValidForUsage**: 憑證的用途字段不允許其用於當前操作。
* **UntrustedRoot**: 憑證鏈的根憑證不受信任。
* **RevocationStatusUnknown**: 無法檢查憑證是否被撤銷。
* **Cyclic**: 憑證鏈中存在循環。
* **InvalidExtension**: 憑證包含一個無效的擴展。
* **InvalidPolicyConstraints**: 無效或不一致的政策限制。
* **InvalidBasicConstraints**: 基本限制擴展無效或不存在。
* **InvalidNameConstraints**: 名稱限制無效。
* **HasNotSupportedNameConstraint**: 名稱限制不受支持。
* **HasNotDefinedNameConstraint**: 名稱限制未定義。
* **HasNotPermittedNameConstraint**: 名稱限制不允許。
* **HasExcludedNameConstraint**: 名稱限制被排除。
* **PartialChain**: 憑證鏈不完整。
* **CtlNotTimeValid**: 証書信任列表 (CTL) 不在其有效期內。
* **CtlNotSignatureValid**: 証書信任列表 (CTL) 的簽名無效。
* **CtlNotValidForUsage**: 証書信任列表 (CTL) 不適用於這個用途。

每個 **X509ChainStatus** 結構實例都會包含一個 **Status** 屬性（這是一個 **X509ChainStatusFlags** 枚舉）和一個 **StatusInformation** 字符串，用於描述問題的詳細信息。

憑證有問題時則在建立SSL連線會有問題，**此時若沒有**自定義callback則會直接跳Error

一張含有 文字, 軟體, 多媒體軟體, 電腦 的圖片

自動產生的描述

有的話會執行ServerCertificateValidationCallback



**因此可透過chainstatus 判斷憑證沒過的原因 (包含過期等等)**

**再加上自行判斷是否自產生的憑證即可**

Console.WriteLine("SSL certificate error: {0}", chain.ChainStatus);

foreach (X509ChainStatus chainStatus in chain.ChainStatus)

{

Console.WriteLine($"Status: {chainStatus.Status}");

Console.WriteLine($"Status Information: {chainStatus.StatusInformation}");

}

**// 檢查是否是自產生的憑證（檢查鏈的長度和主題）**

**if (chain.ChainElements.Count == 1 &&**

**chain.ChainElements[0].Certificate.Subject == chain.ChainElements[0].Certificate.Issuer)**

**{**

**Console.WriteLine("The certificate is self-signed.");**

**return false; // 通常情況下，您可能不想信任自產生的憑證**

**}**