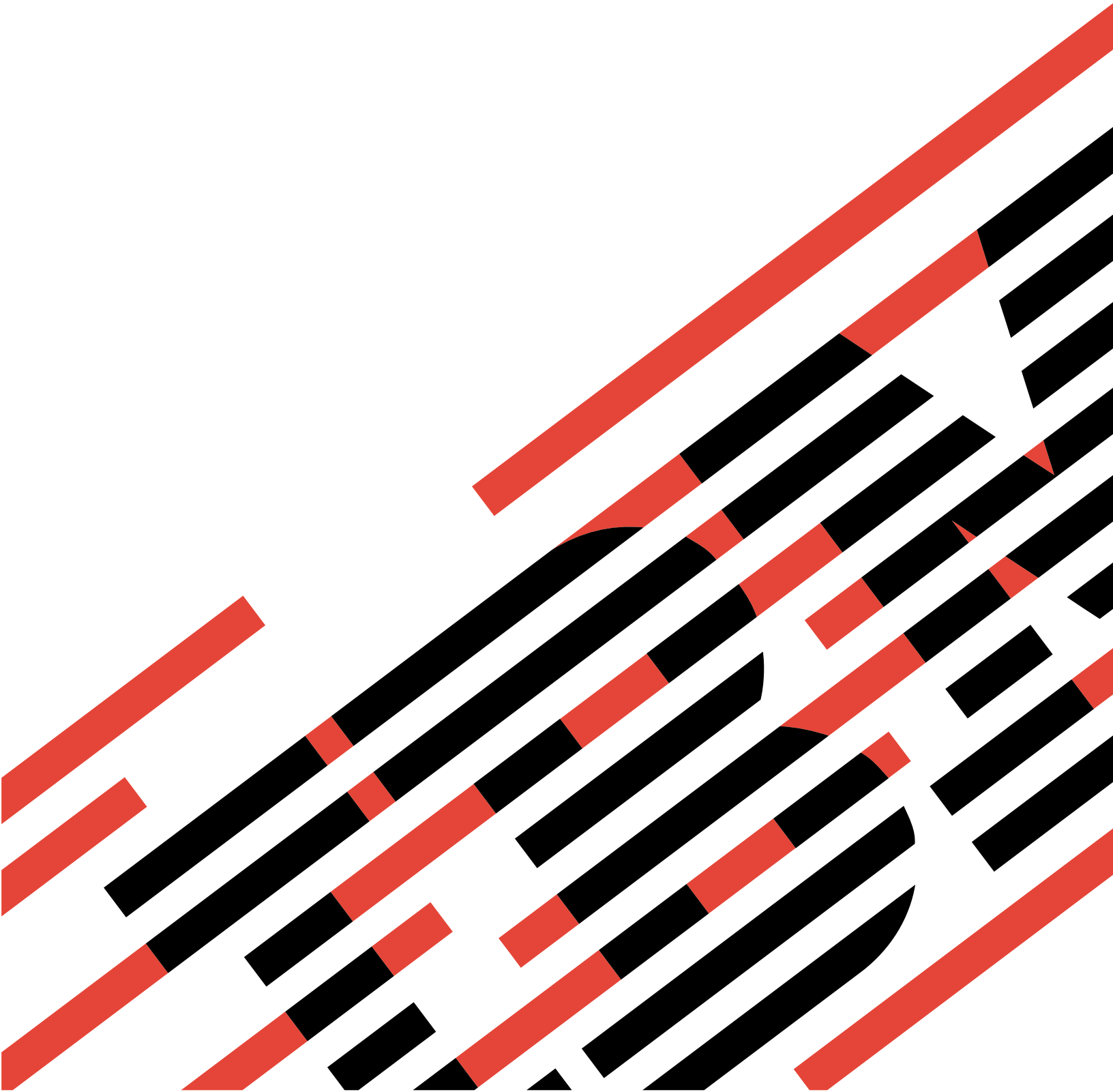
IBM

eserver

iSeries

Secure Sockets Layer (SSL)



IBM

@server

iSeries

Secure Sockets Layer (SSL)

© Copyright International Business Machines Corporation 2000, 2002. All rights reserved.

目錄

© Copyright IBM Corp. 2000, 2002

第 1 篇 Secure Sockets Layer (SSL)

Secure Sockets Layer (SSL) 已成爲業界的標準，可以保障通信階段作業在未受保護之網路 (如：網際網路) 上的安全性。請使用下列鏈結查詢更多有關 SSL 及您 iSeries™ 伺服器應用程式的資訊：

- **V5R2 的新增功能**
  收錄與 SSL 相關，並可供您使用的新功能及新資訊。
- **SSL 實務**
  爲新增加的 SSL 資訊，以提供 SSL 如何運作的相關資訊爲主，加深您對 iSeries 伺服器上之 SSL 的瞭解。
- **SSL 概念**
  涵括部份 Secure Sockets Layer 通信協定基本建置區塊方面的補充資訊。
- **SSL 啓用計畫**
  包括在 iSeries 伺服器上啓用 SSL 的先決條件，以及一些輔助秘訣。
- **使用 SSL 保障應用程式的安全性**
  包含您可以在 iSeries 伺服器上使用 SSL 保護其安全性的應用程式清單。
- **疑難排解 SSL**
  屬基本手冊，主在說明如何著手於 iSeries 伺服器上的 SSL 疑難排解程序。
- **SSL 的相關資訊**
  包含可供您使用的附加資訊資源鏈結。

© Copyright IBM Corp. 2000, 2002

第 1 章 V5R2 的新增功能

V5R2M0 上可使用 iSeries 的 2058 加密加速器選項。此加密硬體選項的設計，在提升您 iSeries 伺服器上之 SSL 的效能。請參閱加密硬體，以取得此選項的詳細資訊。

新的 Global Secure Kit (GSKit) 應用程式設計介面 (API)

本版提供新的 OS/400® Global Secure Toolkit (GSKit) API：`gsk_secure_soc_startInit()`。請參閱 Global Secure ToolKit (GSKit) API，以取得詳細資訊。

如需其它本版次新增或變更之功能的相關資訊，請參閱「資訊中心」PDF 中的 使用者備忘錄 

如何找出新增及變更之處

爲協助您瞭解技術變更之處，此資訊採用：

- » 影像來標示新增及變更資訊的起點。
- « 影像來標示新增及變更資訊的結尾。

© Copyright IBM Corp. 2000, 2002

第 2 章 列印此主題

您可以檢視或下載此資訊的 PDF 版本。執行時，請選取 Securing applications with SSL (約 215 KB 或 34 頁)。

其它資訊

您也可以檢視或列印此主題的任何相關資訊。

儲存 PDF 檔案

若要將 PDF 儲存於工作站上以供檢視或列印，請：
1. 在瀏覽器中的 PDF 上按一下右鍵。
2. 按一下**另存目標**。
3. 導覽至您要儲存此 PDF 的目錄。
4. 按一下**儲存**。

下載 Adobe Acrobat Reader

您如需使用 Adobe Acrobat Reader 檢視或列印此資訊，可從「資訊中心」之外的 Adobe 網站 (www.adobe.com/products/acrobat/readstep.html) 上下載之。

© Copyright IBM Corp. 2000, 2002

第 3 章 SSL 實務

下列實務可以協助您將 iSeries 伺服器上所啓用之 SSL 發揮其最大的效益：

- 實務：使用 SSL 保障「管理中心」的安全性
- 實務：使用 SSL 保障 FTP 的安全性
- 實務：使用 SSL 保障 Telnet 的安全性
- 實務範例：加強 iSeries 的 SSL 效能
- 實務：使用加密硬體保護私密金鑰

SSL 實務：使用 SSL 保障「管理中心」的安全性

狀況

某家公司剛安裝了廣域網路 (WAN)，其中包括數台位在遠端 iSeries 伺服器 (端點系統)，由位在總公司的一台 iSeries 伺服器進行集中管理。這家公司的安全專員 Tom 利用其 iSeries 領航員的「管理中心」技術，與總公司的 iSeries 伺服器 (中央系統) 連線。Tom 想要使用 SSL 保障中央系統與所有端點伺服器連線的安全性。

明細

使用 iSeries 領航員 「管理中心」 技術，Tom 可以透過單一中央系統來管理多個系統。並用「管理中心」與 SSL，Tom 便能夠確保這些系統的**安全**。在搭配使用 SSL 與「管理中心」時，Tom 必須先保護「管理中心」執行所在之 PC 上的 iSeries Access for Windows® 及 iSeries 領航員。

在「管理中心」環境中，Tom 擁有兩種鑑別等級：

伺服器鑑別

提供端點系統伺服器憑證的鑑別。在和端點系統連線時，中央系統會以 SSL 從屬站的模式運作。端點系統則會以 SSL 伺服器的模式運作，並須提出中央系統授信之「憑證中心」所簽發的憑證，以證明自己的身份。每一個端點系統皆必須擁有受信任之 CA 所簽發的有效憑證。

從屬站及伺服器鑑別

提供中央系統及端點系統憑證的鑑別。此種方式所提供的安全等級，較伺服器鑑別強。在其它應用程式中，此稱爲從屬站鑑別，因爲從屬站必須提供有效且經過授信的憑證。當中央系統 (SSL 從屬站) 嘗試和端點系統 (SSL 伺服器) 建立連線時，中央系統與端點系統會互相針對憑證權限的確實性進行鑑別。

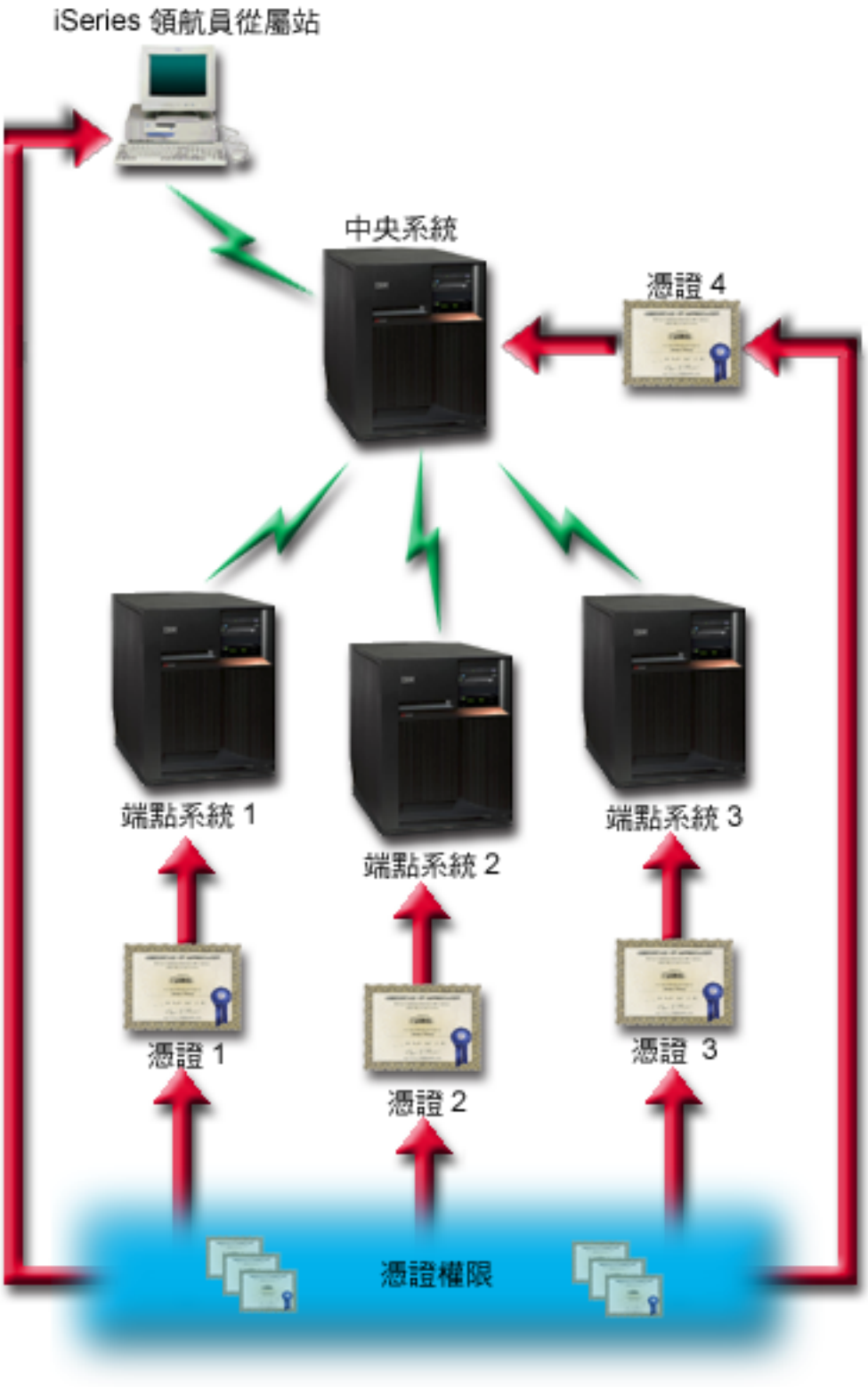
與其它應用程式不同的是，「管理中心」也能夠利用「授信群組」驗證清單提供鑑別。一般來說，驗證清單所儲存的資訊包括：使用者的識別資訊 (如：使用者的身份)、鑑別資訊 (如：密碼)、個人識別碼或數位憑證。這些鑑別資訊都會予以加密。

大部份的應用程式多不會同時啓用伺服器及從屬站鑑別。因爲伺服器鑑別大都發生在 SSL 階段作業的啓動期間。許多應用程式具有從屬站鑑別配置選項。而由於中央系統在網路上的雙重身份，因此「管理中心」會稱此爲「伺服器及從屬站鑑別」，而不會稱爲從屬站鑑別。當 PC 使用者連線至中央系統並啓用 SSL 時，中央系

© Copyright IBM Corp. 2000, 2002

統即會以伺服器的模式運作；但當中央系統連線至端點系統時，其又會改以從屬站的模式運作。下列圖例說明了中央系統如何同時在網路上擔任伺服器及從屬站的角色。

註: 圖例中，連結至「憑證中心」的憑證必須儲存在中央系統的金鑰資料庫與所有的端點系統中。



先決條件及假設

Tom 必須執行以下的管理及配置作業 (請參閱影像，受 SSL 保護的「管理中心 WAN」)，讓已啓用 SSL 的「管理中心」能夠運作：

1. 使用「管理中心」的 iSeries 伺服器符合 SSL 的先決條件 (請參閱 SSL 的先決條件)。
2. 中央系統及所有端點 iSeries 伺服器上執行的是 OS/400 V5R2 版本。如果版本爲 V5R1，請安裝下列 OS/400 (5722-SS1) 的修訂程式 (PTFs)：
   a. SI01375
   b. SI01376
   c. SI01377
   d. SI01378
   e. SI01838
3. iSeries 領航員 PC 從屬站上執行的是 iSeries Access for Windows V5R2 版本。如果從屬站爲 V5R1 版本，請安裝 iSeries Access for Windows (5722-XE1) 的服務修正程式包 PTF SI01907 (或更新的版本)。請參閱 V5R1 資訊中心，「保護管理中心」頁，以取得相關資訊。
4. 取得 iSeries 伺服器的「憑證權限 (CA)」。
5. 在每一個 iSeries 伺服器上建立由 CA 簽訂的憑證，讓啓用 SSL 的「管理中心伺服器」管理之。
6. 傳送 CA 和憑證至每一個 iSeries 伺服器，並將其匯入金鑰資料庫。
7. 使用「管理中心」應用程式識別，以及 iSeries 領航員所使用的所有端點伺服器之應用程式識別，來指派憑證：
   a. 在中心伺服器上啓動 IBM® 數位憑證管理程式。若 Tom 要取得或建立憑證，亦或設定及改變憑證系統，他現在必須如此做 (請參閱使用「數位憑證管理程式」以獲得憑證系統設定的資訊)。
   b. 按一下 **選取「憑證庫」**。
   c. 選取 ***SYSTEM**，再按一下**繼續**。
   d. 輸入 *SYSTEM **「憑證庫」密碼**，再按一下**繼續**。功能表重新載入後，請展開**管理應用程式**。
   e. 按一下**更新憑證分派**。
   f. 選取**伺服器** ，再按一下**繼續**。
   g. 選取**管理中心伺服器**，再按一下**更新憑證分派**。 如此便可指派憑證給「管理中心」伺服器使用，目的在建立 iSeries Access for Windows 從屬站的識別。
   h. 按一下**指派新憑證**。DCM 會重新載入**更新憑證分派**頁，並發送確認的訊息。
   i. 按一下**完成**。
   j. 對 iSeries 領航員使用的所有端點伺服器，重複以上程序。
8. 設定 iSeries 領航員：
   a. 選擇性地安裝 iSeries 領航員的 SSL 元件。
   b. 從 CA 建立所在的系統下載它。

   註: 若 Tom 所選擇之 iSeries Access for Windows 從屬站的金鑰資料庫中沒有 CA 憑證，他必須先將憑證新增至資料庫中，才能使用 SSL。

配置步驟

| 「管理中心」可以啓用 SSL 之前， Tom 必須在 iSeries 伺服器上先安裝先決條件程式與設定數位憑證 (繼續之前，請參閱此實務手冊的假設與先決條件。 一旦符合先決條件，Tom 即可遵循以下程序來啓用「管理中心」的 SSL。

| **註:** 若 iSeries 領航員中的 SSL 已啓用，Tom 必須先將之停用以啓用「管理中心」的 SSL。若啓用 SSL 的爲 iSeries 領航員而非「管理中心」，則 iSeries 領航員欲嘗試連接至「管理中心」中央系統會失敗。

| **伺服器鑑別方面 (必要的)：**

| 1. 配置伺服器鑑別的中央系統
| 2. 配置伺服器鑑別的端點系統

| **從屬站鑑別方面 (可選用)：**

| **註:** 除非伺服器鑑別已配置完成，否則無法進行從屬站鑑別的配置。

| 1. 配置從屬站鑑別的中央系統
| 2. 配置從屬站鑑別的端點系統

配置伺服器鑑別的中央系統

SSL 可讓 Tom 保護中央系統與端點系統間的傳輸安全，在 iSeries 領航員從屬站與中央系統間也同樣受到保護。 SSL 提供憑證的傳送及鑑別與資料加密。只有在同時啓用 SSL 的中央系統與端點系統間，才能進行 SSL 連線。 Tom 必須先設定伺服器鑑別，才能設定從屬站鑑別。

1. iSeries 領航員 中，在**管理中心**上按一下右鍵，再選取**內容**。
2. 按一下**安全性**標籤，再選取**使用 Secure Sockets Layer (SSL)**
3. 鑑別等級方面，選取**伺服器**。
4. 按一下**確定**在中央系統上設此值。

   註: 請勿重新啓動「管理中心伺服器」，除非端點系統中的伺服器鑑別已完成配置。
5. 配置伺服器鑑別的端點系統。

配置伺服器鑑別的端點系統

啓用中央系統伺服器鑑別的 SSL 之後，Tom 必須接著啓用所有端點系統伺服器鑑別的 SSL。爲配置端點系統使用 SSL 及伺服器鑑別，Tom 需完成以下作業：

1. 展開**管理中心**檢視畫面。
2. **端點系統系統值的比較與更新**：
   a. 在**端點系統**之下於中央系統上按一下右鍵，再選取**庫存-->收集**。
   b. 在收集對話框上勾選 **系統值**選項，以收集中央系統的系統值庫存。請勿勾選其它選項。
   c. 以右鍵按一下**系統群組-->新系統群組**。
   d. 使用 SSL 定義所有端點系統欲連接的新系統群組。
   e. 展開系統群組清單來顯示新的群組。
   f. 收集完成之後，在新系統群組上按一下右鍵，再選取**系統值-->比較與更新**。
   g. 驗證顯示在**模型系統**欄位中的中央系統。
   h. 選取**管理中心**類別並驗證以下的值，再勾選旁邊的方框：
      - 「使用 Secure Sockets Layer」設定爲**是**。
      - SSL 鑑別等級設定爲**伺服器**。

在程序期間，中央系統中會設定這些值，請配置伺服器鑑別的中央系統。

i. 按一下**確定**來設定新系統群組中端點系統的值。

j. 完成**比較與更新**的處理後，您才能重新啓動「管理中心伺服器」。這會花費您一些時間。

3. **重新啓動中央系統的管理中心伺服器：**

   a. 在 iSeries 領航員中，展開**我的連線**。

   b. 展開中央系統檢視畫面。

   c. 展開**網路--> 伺服器**，再選取 **TCP/IP**。

   d. 在**管理中心**上按一下右鍵，再選取**停止**。中央系統檢視畫面會隱藏起來並顯示一個訊息，說明您不再與伺服器連線。

   e. 一旦「管理中心」伺服器已停止，請按一下**啓動**以重新啓動之。

4. **重新啓動所有端點系統的管理中心伺服器：**

   a. 展開要重新啓動的端點系統。

   b. 展開**網路--> 伺服器**，再選取 **TCP/IP**。

   c. 在**管理中心**上按一下右鍵，再選取**停止**。

   d. 一旦「管理中心」伺服器已停止，請按一下**啓動**以重新啓動之。

   e. 對每一個端點系統重複以上程序。

5. **啓動 iSeries 領航員從屬站的 SSL：**

   a. 在 iSeries 領航員中，展開**我的連線**。

   b. 在中央系統上按一下右鍵，再選取**內容**。

   c. 按一下 **Secure Sockets** 標籤，再選取**使用 Secure Sockets Layer (SSL) 建立連線**。

   d. 結束 iSeries 領航員並重新啓動之。

現在 Tom 已完成伺服器鑑別的配置，他便可執行以下的從屬站鑑別程序 (可選用)：

- 配置從屬站鑑別的中央系統
- 配置從屬站鑑別的端點系統

從屬站鑑別能提供「憑證權限」及可靠群組之驗證給中央系統及端點系統。

配置從屬站鑑別的中央系統

當中央系統 (SSL 從屬站) 嘗試使用 SSL 連線至端點系統 (SSL 伺服器) 時，兩者可透過從屬站鑑別來鑑別彼此的憑證 (「管理中心」中稱爲「憑證權限」與「可靠群組」鑑別)。

1. 在iSeries 領航員中，於**管理中心**上按一下右鍵，再選取**內容**。
2. 按一下**安全性** 標籤，再選取**使用 Secure Sockets Layer (SSL)** 。
3. 鑑別等級方面，選取**從屬站與伺服器** 。
4. 按一下**確定**，在中央系統上設定此值。

   註: 請勿重新啓動「管理中心伺服器」，除非所有端點系統已完成使用 SSL 的從屬站與伺服器鑑別之配置。

5. 配置從屬站鑑別的端點系統。

配置從屬站鑑別的端點系統

1. **端點系統系統值的比較與更新：**

註: 若您的端點 iSeries 伺服器上執行的是 V4R5 版本，則此項作業將無法運作。請參閱「V4R4 紅皮書」，Management Central: A Smart Way to Manage AS/400® Systems  。

a. 在**端點系統**之下，於中央系統上按一下右鍵，再選取**庫存-->收集**。
b. 在收集對話框上勾選**系統值**選項，以收集中央系統的系統值庫存。請勿勾選其它選項。
c. 以右鍵按一下**系統群組-->新系統群組**。
d. 使用 SSL 定義所有端點系統欲連接的新系統群組。
e. 展開系統群組清單來顯示新的群組。
f. 收集完成之後，在新系統群組上按一下右鍵，再選取**系統值-->比較與更新**。
g. 驗證顯示在**模型系統**欄位中的中央系統。
h. 選取**管理中心**類別並驗證以下選項：
   - 「使用 Secure Sockets Layer」設定爲**是**。
   - SSL 鑑別等級設定爲**從屬站與伺服器**。

   在程序期間，中央系統中會設定這些值，請「配置從屬站鑑別的中央系統」。勾選每一個值旁邊的**更新**方框。
i. 按一下**確定**來設定新系統群組中端點系統的值。

2. **複製驗證清單至端點系統**：
   a. 在 iSeries 領航員中，展開**管理中心-->定義**。
   b. 在**套裝軟體**上按一下右鍵，再選取**新的定義**。
   c. 在**新的定義**視窗中，使用以下項目:
      - **名稱**：鍵入定義的名稱。
      - **來源系統**：選取中央系統的名稱。
      - **所選取的檔案及資料夾**：在欄位上按一下，再鍵入 `/QSYS.LIB/QUSRSYS.LIB/QYPSVLDL.VLDL`。
   d. 按一下**選項**標籤，再選擇**用已傳送檔案置換現有檔案**。
   e. 按一下**進階**。
   f. 在**進階選項**視窗，指定**是**以允許復置時的物件差異。
   g. 按一下**確定**來重新整理定義清單及顯示新的套裝軟體。
   h. 在新的套裝軟體上按一下右鍵，再選取**傳送**。
   i. 在**傳送**對話框中：新增可靠群組，移除其它選項，再選取**確定**。「可靠」群組是您在此程序步驟 1 所定義的系統群組。

   註: 中央系統爲來源系統，因此無法執行**傳送**作業。**傳送**作業應在所有端點系統上順利完成。

3. **重新啓動中央系統的管理中心伺服器**：
   a. 在 iSeries 領航員中，展開**我的連線**。
   b. 展開中央系統。
   c. 展開**網路--> 伺服器**，再選取 **TCP/IP**。
   d. 在**管理中心**上按一下右鍵，再選取**停止**。中央系統檢視畫面會隱藏起來並顯示一個訊息，說明你不再與伺服器連線。
   e. 一旦「管理中心」伺服器已停止，請按一下**啓動**以重新啓動之。

4. **重新啓動所有端點系統的管理中心伺服器**：

   註: 對每一個端點系統重複此程序。

| a. 展開要重新啓動的端點系統。
| b. 展開**網路--> 伺服器**，再選取**TCP/IP**。
| c. 在**管理中心**上按一下右鍵，再選取**停止**。
| d. 一旦「管理中心」伺服器已停止，請按一下**啓動**以重新啓動之。

| 

第 4 章 SSL 概念

使用 SSL 通信協定，您可以在從屬站與伺服器應用程式間建立安全的連線，因爲這些應用程式能夠在通信階段作業中，提供一個或兩個端點的鑑別。 SSL 也提供從屬站與伺服器應用程式交換資料時的隱密性及整合性。

以下的概念資訊可讓您更瞭解 SSL 與 iSeries 伺服器間的關係：

- SSL 之歷程
- SSL 如何運作
- 支援的 SSL 與 Transport Layer Security (TLS) 通信協定
- 伺服器鑑別
- 從屬站鑑別

SSL 之歷程

»

Netscape 於 1994 年開發「Secure Sockets Layer (SSL) 通信協定」，旨在回應當時網際網路上對安全性的關注。雖然 SSL 最初是針對保護 Web 瀏覽器及伺服器通信的安全而開發，但透過此規格設計，其它的應用程式 (如：TELNET 與 FTP) 亦能使用 SSL。請參閱 支援的 SSL 與「傳輸層安全 (TLS)」通信協定 ，以獲得更多 SSL 或相關通信協定的資訊。 «

SSL 如何運作

實際上 SSL 有兩種通信協定：記錄式通信協定與交握式通信協定。記錄式通信協定能夠在 SSL 階段作業期間，控制兩端點之間的資料流程。

交握式通信協定能夠在 SSL 階段作業期間鑑別一個或兩個端點，並建立唯一且對稱的金鑰，產生的金鑰可以在該 SSL 階段作業期間進行資料的加密及解密。 SSL 使用非對稱加密法、數位憑證及 SSL 交握式流程，來鑑別 SSL 階段作業期間的一個或兩個端點。一般來說，伺服器需要鑑別而從屬站的鑑別則可選用。由「憑證權限」發出的數位憑證以被指派至每一個端點，或至每一個連線端點上使用 SSL 的應用程式。

數位憑證是由公開金鑰及可靠的「憑證權限 (CA)」數位簽訂的一些識別資訊所組成。每一個公開金鑰皆有其相關的私密金鑰。私密金鑰並非儲存於憑證中或屬於憑證的一部分。伺服器與從屬站鑑別中，受鑑別的端點必須證明其有權限存取數位憑證中與公開金鑰相關的私密金鑰。

加密作業使用了公開與私密金鑰，使 SSL 的交握成爲效能極高的作業。兩端點間的起始 SSL 階段作業建立後，安全記憶體會快取兩個端點及應用程式的 SSL 階段作業資訊，以加速後續 SSL 階段作業的啓用。 SSL 階段作業如已回復，兩個端點會使用縮短的交握式流程，來鑑別每一個端點是否有權限存取不使用公開及私密金鑰的唯一資訊。若兩者皆能證明擁有此唯一資訊的存取權限，新的對稱金鑰會被建立，SSL 階段作業便會「回復」。對於 TLS 1.0 版本與 SSL 3.0 版本的階段作業，保留於安全記憶體的快取資訊不會超過 24 小時。V5R2M0 中，可以藉著使用加密硬體，將 SSL 交握式效能對主要 CPU 的衝擊降至最小。

© Copyright IBM Corp. 2000, 2002

支援的 SSL 與 Transport Layer Security (TLS) 通信協定

SSL 通信協定有多種定義版本。最新的版本爲「傳輸層安全通信協定 (TLS)」，此版本以 SSL 3.0 爲基礎，且爲 IETF 的產品。 OS/400 實作支援下列的 SSL 與 TLS 通信協定版本：

- TLS 1.0 版本
- TLS 1.0 版本 (相容於 SSL 3.0 版本)

  註:

  1. 指定相容於 SSL 3.0 版本的 TLS 1.0 版本，表示 TLS 會盡可能地溝通，若 TLS 無法溝通，SSL 3.0 版本便會取而代之進行溝通。若 SSL 3.0 版本仍無法進行溝通，則 SSL 的交握將會失敗。
  2. 我們也支援相容於 SSL 3.0 及 2.0 版本的 TLS 1.0 版本。這是以**全部**的通信協定值指定，意即 TLS 會盡可能地溝通，若 TLS 無法溝通，則 SSL 3.0 版本便會取而代之進行溝通。若 SSL 3.0 版本無法進行溝通，則 SSL 2.0 版本會取而代之進行溝通。若 SSL 2.0 版本仍無法進行溝通，則 SSL 的交握將會失敗。
- SSL 3.0 版本
- SSL 2.0 版本
- SSL 3.0 版本 (相容於 SSL 2.0 版本)

SSL 3.0 版本與 SSL 2.0 版本

SSL 3.0 版本是幾乎完全異於 SSL 2.0 版本的通信協定・兩種通信協定一些主要的差異點包含：

- SSL 3.0 版本的交握式通信協定流程異於 SSL 2.0 版本。
- SSL 3.0 版本使用來自「RSA 資料安全公司」的 BASFE 3.0 實作。 BASFE 3.0 包含了一些計時攻擊修訂程式與 SHA-1 雜湊演算法。一般認爲 SHA-1 雜湊演算法比 MD5 雜湊演算法更具安全性。使用 SHA-1 而不用 MD5 可讓 SSL 3.0 版本支援附加的密碼套件。
- 在 SSL 交握處理程序期間， SSL 3.0 版本的通信協定會減少人爲介入 (MITM) 攻擊類型的發生。在 SSL 2.0 版本中，MITM 攻擊可能會讓密碼規格減弱，儘管這種情況未必會發生。密碼減弱會造成無權限的使用者能夠破解階段作業密碼鎖。

TLS 1.0 版本與 SSL 3.0 版本

「傳輸層安全性 (TLS)」 1.0 版本以 SSL 3.0 版本爲基礎，爲最新產業標準 SSL 通信協定。它的規格由 IETF 在 RFC 2246 中定義，「TLS 通信協定。」 

TLS 的主要目標是讓 SSL 更具安全性，以及讓通信協定的規格更加精確與完整。 TLS 提供 SSL 3.0 版本的加強功能如下：

- 更安全的 MAC 演算法
- 更清楚的警示
- 對「灰色區域」有更詳細的定義

任何一個啓用 SSL 的 iSeries 伺服器應用程式會自動取得 TLS 支援，除非該應用程式已特別要求只使用 SSL 3.0 版本或 SSL 2.0 版本。

TLS 在安全性上改善之處如下：

- **訊息鑑別的金鑰雜湊**
  TLS 使用「訊息鑑別碼的金鑰雜湊 (HMAC)」，如此可以確定通過開放的網路 (如：網際網路) 時，記錄無法被改變。 SSL 3.0 版本也有金鑰訊息鑑別的功能，但一般認爲 HMAC 比 SSL 3.0 版本使用的 (「訊息鑑別碼」) MAC 功能更具安全性。
- **強化的偽隨機功能 (PRF)**
  PRF 用來產生金鑰資料。在 TLS 中，PRF 是與 HMAC 一起定義的。 PRF 使用兩種雜湊演算法，能夠確保安全性。只要第二個演算法不外曝，即使其中一個演算法外曝，此時資料仍具安全性。
- **改良的完成訊息驗證**
  TLS 1.0 版本與 SSL 3.0 版本提供兩端點完成訊息，如此可以鑑別所交換的訊息不被改變。然而，TLS 以 PRF 上的完成訊息與 HMAC 值爲基礎，再度比 SSL 3.0 版本更具安全性。
- **一致的憑證處理**
  不同於 SSL 3.0 版本， TLS 會嘗試指定必須在 TLS 實作間交換的憑證類型。
- **特定的警示訊息**
  TLS 提供更特定及附加的警示，能在任一階段作業端點偵測並指出問題。 TLS 也能在傳送某個警示時將其記錄下來。

伺服器鑑別

擁有伺服器鑑別，從屬站可以確定伺服器憑證有效，意即該憑證是從屬站信任並由憑證權限 (CA) 所簽訂的。SSL 使用非對稱加密法與交握式通信協定流程，來產生只給此唯一 SSL 階段作業使用的對稱金鑰。此金鑰會產生一組金鑰，使 SSL 階段作業流程中的資料能夠加密與解密。而後，當 SSL 的交握完成，一端或兩端的通信鏈結會被鑑別，並產生唯一金鑰來加密與解密資料。交握一旦完成，SSL 階段作業中的應用程式層資料流程便會加密。

從屬站鑑別

許多應用程式提供啓用從屬站鑑別的選項。擁有從屬站鑑別，伺服器可以確保從屬站憑證有效，意即該憑證是伺服器信任並由「憑證權限」所簽訂的。支援從屬站鑑別的 iSeries 伺服器應用程式如下：

- IBM HTTP 伺服器 (原始)
- IBM HTTP Server (Apache 驅動)
- FTP 伺服器
- Telnet 伺服器
- 「管理中心」端點系統
- 目錄服務 (LDAP)

第 5 章 SSL 啓用計畫

計畫啓用 iSeries 伺服器上的 SSL 時，請注意以下兩點：

- SSL 的先決條件
- 你要何種數位憑證，以及要從何處取得

SSL 的先決條件：

- IBM 數位憑證管理程式 (DCM)，OS/400 (5722-SS1) 的選項 34。
- TCP/IP Connectivity Utilities for iSeries (5722-TC1)
- IBM HTTP Server for iSeries (5722-DG1)
- 若您要在 HTTP 伺服器上使用 DCM，請確定您已安裝 IBM Developer Kit for Java™(5722-JV1)，否則 HTTP 管理伺服器將不會啓動。
- IBM Cryptographic Access Provider 產品，5722-AC3 (128 位元)。此產品的位元大小，是指在加密作業中對稱金鑰裡密鑰大小的最大值。這樣的大小可讓對稱金鑰接受每一個國家出及入法律的控制。較高的位元大小可提供更安全的連線。
- 您亦可在使用 SSL 時安裝加密硬體，以加速 SSL 交握處理的時間。 V5R2M0 版次提供您在使用 iSeries 伺服器時的加密硬體選項如下：
  - 2058 加密加速器 (「硬體特性碼」4805)
  - 4758 加密輔助處理器 (「硬體特性碼」4801 或 4802)

  若您要安裝加密硬體，必須先安裝選項 35 的「密碼服務提供程式」。

若您要在任何的 iSeries Access for Windows 或 IBM Toolbox for Java 元件中使用 SSL，必須先安裝 iSeries Client Encryption 產品，5722-CE3 (128 位元)。iSeries Access for Windows 需要該產品來建立安全連線。

註: PC5250 模擬器與 Personal Communications 產品一起出貨，因此若要使用 PC5250 模擬器，您毋需安裝 Client Encryption Product。 Personal Communications 有其內建加密碼。

數位憑證

請參閱使用公開憑證與發出私密憑證，以更瞭解公開憑證與私密數位憑證間之差異，以及可供您取得的選項。

IBM 數位憑證管理程式 (DCM) 爲 iSeries 伺服器管理數位憑證的解決方案。更多 DCM 的相關資訊，請參閱「資訊中心」主題使用數位憑證管理程式。

© Copyright IBM Corp. 2000, 2002

第 6 章 使用 SSL 保護應用程式安全

您可以使用 SSL 來保護以下的 iSeries 伺服器應用程式：

- IBM HTTP Server for iSeries (原始)
- IBM HTTP Server for iSeries (Apache 驅動)
- FTP 伺服器
- Telnet 伺服器
- 分散式關連資料庫架構 (DRDA®) 與分散式資料管理 (DDM) 伺服器
- 管理中心
- 目錄服務伺服器 (LDAP)
- 企業識別對映 (EIM)
- iSeries Access for Windows 應用程式，包含 iSeries 領航員
- 以一組 iSeries Access for Windows 應用程式設計介面 (API) 撰寫的應用程式
- 以 Developer Kit for Java 及使用 IBM Toolbox for Java 而開發的程式
- 使用 iSeries 伺服器所支援的 Secure Sockets 「應用程式設計介面 (API)」而開發的應用程式。 支援的 API 包括「廣域安全工具程式 (GSKit) 」及 SSL_ iSeries 原有的 API。 請參閱 Secure Sockets API ，以取得 GSKit 與 SSL_API 的資訊。

© Copyright IBM Corp. 2000, 2002

第 7 章 SSL 疑難排解

此基本的疑難排解資訊能夠幫你減少使用 SSL 時 iSeries 伺服器可能發現的問題清單。您必須瞭解這些只是個指引，並非疑難排解資訊的全部來源。

驗證下列的陳述式爲眞：

- 您已符合 iSeries 伺服器上使用 SSL 的先決條件 (請參閱 「SSL 的先決條件」)。
- 若您在 V5R1 系統內使用「iSeries 領航員」的「管理中心」技術，您便已在系統內安裝下列的 PTF：
  - si01375
  - si01376
  - si01377
  - si01378
  - si01838
- 您的憑證權限及憑證有效且尚未過期。

若您已驗證系統中上述的陳述式爲眞，但在 iSeries 伺服器上仍有 SSL 相關的問題，您可以嘗試以下的選項：

- 伺服器工作日誌中的 SSL 錯誤碼能夠在錯誤表格中交互參照，以尋找該錯誤的更多資訊。請參閱 Secure Socket API 錯誤碼訊息頁面，以獲得 Secure Socket 錯誤碼訊息資訊。例如，這個表格對映 -93，在伺服器工作日誌出現的則是常數 SSL_ERROR_SSL_NOT_AVAILABLE 。
  - 負的回覆碼 (在代號前以破折號表示)，代表您正在使用 SSL_ API。
  - 正的回覆碼代表您正在使用 GSKit API。程式設計師可在程式中撰寫 gsk_strerror()or SSL_Strerror() API 程式碼，以取得錯誤回覆碼的簡短說明。部份應用程式使用此 API 並列印訊息至含有該句子的工作日誌。

  如需要更詳細的資訊，iSeries 伺服器上會顯示出表格提供的訊息 ID，以顯示此錯誤的潛伏原因及其回復方法。解譯這些錯誤碼的附加文件會位於傳回錯誤的個別 Secure Socket API 中。
- 以下兩個標頭檔包含相同的系統 SSL 回覆碼常數名稱 (視爲表格)，但沒有訊息 ID 交互參照：
  - QSYSINC/H.GSKSSL
  - QSYSINC/H.SSL

  請記得在此兩個檔案中系統 SSL 回覆碼名稱雖爲常數，但每一個回覆碼仍可與一個以上的唯一錯誤結合。

關於更多 iSeries 伺服器的疑難排解資訊，請參閱疑難排解與服務頁面。 

© Copyright IBM Corp. 2000, 2002

第 8 章 相關資訊

您可以在以下的來源獲得其它 SSL 資訊：

IBM 來源

- SSL 及 Java Secure Socket Extension (JSSE) 頁面：包含 JSSE 的簡短說明，以及您可以使用的方式。
- Java Secure Socket Layer (JSSL) 頁面：包含 JSSL 的簡短說明，以及您可以使用的方式。
- IBM Toolbox for Java 頁面：提供 Java 類別的簡短說明，以及您可以使用的方式。

說明的要求

- RFC 2246：「TLS 通信協定 1.0 版本」，  詳細地說明 TLS 通信協定。
- RFC2818：HTTP Over TLS，  說明如何使用 TLS 來確保網際網路上 HTTP 連線的安全性。

其它來源

- 「SSL 通信協定 3.0 版本」 文件，  對「SSL 通信協定 3.0 版本」有更詳細的說明。

© Copyright IBM Corp. 2000, 2002