IBM Tivoli Access Manager

Plug-in for Web Servers 使用手冊

第 4.1 版

SC40-1158-00

IBM Tivoli Access Manager

Plug-in for Web Servers 使用手冊

第 4.1 版

SC40-1158-00

注意

使用此資訊和它支援的產品前，請先閱讀第 127 頁的附錄 D, 『注意事項』中的資訊。

第一版 (October 2002)

本版本適用於第 4.1 版的 IBM Tivoli Access Manager Plug-in for Web Servers（產品編號 5724-C08），以及所有後續的版次及修訂，除非新版中另有指示。

目錄

圖

表

前言

IBM® Tivoli® Access Manager Plug-in for Web Servers 會藉由充當用戶端與安全 Web 空間之間的閘道，來管理 Web 型資源的安全。外掛程式會實作保護 Web 物件空間的安全原則。外掛程式可提供單一登入解決方案、支援 Web 伺服器當作虛擬主機來執行，以及將 Web 應用程式伺服器資源納入其安全原則內。

IBM® Tivoli® Access Manager (Tivoli Access Manager) 是 IBM Tivoli Access Manager 產品組合中，執行應用程式所需的基礎軟體。它整合了 IBM Tivoli Access Manager 應用程式，以提供廣泛的授權及管理解決方案。這些產品是以整合式解決方案的形式銷售，它們能提供存取控制管理解決方案，集中管理電子商業應用程式的網路和應用程式安全原則。

註: IBM Tivoli Access Manager 是先前上市之軟體 Tivoli SecureWay® Policy Director 的新名稱。同時，對熟悉 Tivoli SecureWay Policy Director 軟體與文件的使用者而言，*管理伺服器*現稱爲*原則伺服器*。

*IBM Tivoli Access Manager Plug-in for Web Servers 使用手冊*提供使用 Plug-in for Web Servers 應用程式來保護 Web 網域的安裝指示、管理程序，以及技術參考資訊。

本書適用對象

本手冊的適用對象是負責安裝、部署及管理 Tivoli Access Manager Plug-in for Web Servers 的系統管理者。

讀者必須熟悉以下各項：

- PC 及 UNIX® 作業系統。
- 資料庫架構和概念
- 安全管理
- 網際網路通信協定，包括 HTTP、HTTPS 及 TCP/IP
- 「輕裝備目錄存取通訊協定」(LDAP) 和目錄服務
- 支援的使用者登錄
- 鑑定和授權

如果您打算啓用「安全 Socket 層」 (SSL) 通訊，您還需熟悉 SSL 通訊協定、金鑰交換（公開和私密）、數位簽章、加密演算法以及憑證管理中心。

本書內容

本書包含下列各節：

- 第 1 章, 『簡介 IBM Tivoli Access Manager Plug-in for Web Servers』

  提供 Access Manager Plug-in for Web Servers 應用程式的簡介，詳述系統架構、功能及操作環境。
- 第 2 章, 『安裝 IBM Tivoli Access Manager Plug-in for Web Servers』

  Access Manager Plug-in for Web Servers 的安裝指示，包括系統需求資訊及移除程序。

- 第 3 章, 『IBM Tivoli Access Manager Plug-in for Web Servers 配置』
  提供 Access Manager Plug-in for Web Servers 的配置需求的相關資訊。
- 第 4 章, 『IBM Tivoli Access Manager Plug-in for Web Servers 鑑定』
  維護階段作業狀態、鑑定要求及支援後置授權處理程序的資訊及配置指示。
- 第 5 章, 『IBM Tivoli Access Manager Plug-in for Web Servers 安全原則』
  關於配置及自訂 Access Manager plug-in for Web Servers 安全原則的資訊。
- 第 6 章, 『Web 單一登入解決方案』
  討論 Access Manager Plug-in for Web Servers 保護的 Web 空間的單一登入解決方案。
- 第 7 章, 『電子社群單一登入』
  討論 Access Manager Plug-in for Web Servers 的電子社群單一登入解決方案。
- 附錄 A, 『pdwebpi.conf 參照』
  列示 Access Manager Plug-in for Web Servers 配置參數及其相關說明。
- 附錄 B, 『模組快速參照』
  列示所有外掛程式鑑定、階段作業及後置授權方法，以及相關說明。
- 附錄 C, 『指令快速參照』
  列示可用的外掛公用程式，以及它們執行之動作的說明。

出版品

本節列出 IBM Tivoli Access Manager 書庫中的出版品和任何其他相關的文件。同時也說明如何由線上存取 Tivoli 出版品、如何訂購 Tivoli 出版品，以及如何提供對 Tivoli 出版品的意見。

IBM Tivoli Access Manager

Tivoli Access Manager 書庫組織成下列的種類：

- 『版次資訊』
- 第 xiii 頁的『Base 資訊』
- 第 xiii 頁的『WebSEAL 資訊』
- 第 xiii 頁的『Web 安全資訊』
- 第 xiii 頁的『程式開發參考手冊』
- 第 xiv 頁的『技術補充』

在「Tivoli 資訊中心」網站上，是以「可攜式文件格式 (PDF)」及 HTML 格式提供產品書庫中的出版品。

http://www.tivoli.com/support/documents/

版次資訊

- *IBM Tivoli Access Manager Read Me First Card*
  GI10-2727-00 (`am41_readme.pdf`)
  提供安裝及開始使用 Tivoli Access Manager 的資訊。
- *IBM Tivoli Access Manager Release Notes*
  SC32-1130-00 (`am41_relnotes.pdf`)

提供最新的資訊，例如軟體限制、暫行解決方法和說明文件更新。

Base 資訊

- *IBM Tivoli Access Manager Base 安裝手冊*
  SC40-1166-00 (am41_install.pdf)

  說明如何安裝、配置和升級 Tivoli Access Manager 軟體，包括 Web Portal Manager 介面。

- *IBM Tivoli Access Manager Base Administrator's Guide*
  SC32-1132-00 (am41_admin.pdf)

  說明使用 Tivoli Access Manager 服務的概念和程序。提供從 Web Portal Manager 介面和使用 **pdadmin** 指令執行作業的指示。

WebSEAL 資訊

- *IBM Tivoli Access Manager WebSEAL 安裝手冊*
  SC40-1167-00 (amweb41_install.pdf)

  提供 WebSEAL 伺服器和 WebSEAL 應用程式開發套件的安裝、配置和移除指示。

- *IBM Tivoli Access Manager WebSEAL Administrator's Guide*
  SC32-1134-00 (amweb41_admin.pdf)

  提供使用 WebSEAL 來管理您安全 Web 網域的資源所需的背景資料、管理程序和技術參考資訊。

Web 安全資訊

- *IBM Tivoli Access Manager for WebSphere Application Server 使用手冊*
  SC40-1155-00 (amwas41_user.pdf)

  提供 Tivoli Access Manager for IBM WebSphere® Application Server 的安裝、移除和管理指示。

- *IBM Tivoli Access Manager for WebLogic Server 使用手冊*
  SC40-1156-00 (amwls41_user.pdf)

  提供 Tivoli Access Manager for BEA WebLogic Server 的安裝、移除和管理指示。

- *IBM Tivoli Access Manager Plug-in for Edge Server 使用手冊*
  SC40-1168-00 (amedge41_user.pdf)

  說明如何安裝、配置和管理 IBM WebSphere Edge Server 應用程式的外掛程式。

- *IBM Tivoli Access Manager Plug-in for Web Servers 使用手冊*
  SC40-1158-00 (amws41_user.pdf)

  提供使用 plug-in for Web Server 來保護 Web 網域的安裝指示、管理程序和技術參考資訊。

程式開發參考手冊

- *IBM Tivoli Access Manager Authorization C API Developer's Reference*
  SC32-1140-00 (am41_authC_devref.pdf)

  提供說明如何使用 Tivoli Access Manager 授權 C API 和 Access Manager 服務外掛程式介面將 Tivoli Access Manager 安全性加入應用程式的參考資料。

- *IBM Tivoli Access Manager Authorization Java Classes Developer's Reference*
  SC32-1141-00 (am41_authJ_devref.pdf)

提供使用 Java™ 語言的授權 API 實作，讓應用程式可以使用 Tivoli Access Manager 安全性的參考資訊。

- *IBM Tivoli Access Manager Administration C API Developer's Reference*
  SC32-1142-00 (am41_adminC_devref.pdf)

  提供有關使用管理 API 讓應用程式可以執行 Tivoli Access Manager 管理作業的參考資訊。此文件說明管理 API 的 C 實作。

- *IBM Tivoli Access Manager Administration Java Classes Developer's Reference*
  SC32-1143-00 (am41_adminJ_devref.pdf)

  提供使用 Java 語言的管理 API 實作，讓應用程式可以執行 Tivoli Access Manager 管理作業的參考資訊。

- *IBM Tivoli Access Manager WebSEAL Developer's Reference*
  SC32-1135-00 (amweb41_devref.pdf)

  提供「跨網域鑑定服務 (CDAS)」、「跨網域對映架構 (CDMF)」和「密碼強度模組」的管理和程式設計資訊。

技術補充

- *IBM Tivoli Access Manager Command Reference*
  GC32-1107-00 (am41_cmdref.pdf)

  提供 Tivoli Access Manager 所提供的指令行公用程式及 Script 的相關資訊。

- *IBM Tivoli Access Manager Error Message Reference*
  SC32-1144-00 (am41_error_ref.pdf)

  提供 Tivoli Access Manager 產生之訊息的說明和建議動作。

- *IBM Tivoli Access Manager Problem Determination Guide*
  GC32-1106-00 (am41_pdg.pdf)

  提供 Tivoli Access Manager 的問題判定資訊。

- *IBM Tivoli Access Manager Performance Tuning Guide*
  SC32-1145-00 (am41_perftune.pdf)

  提供由搭配將 IBM Directory Server 定義爲使用者登錄的 Tivoli Access Manager 所組成之環境的效能調整資訊。

此 *Tivoli 名詞解釋*包括與 Tivoli 軟體相關的許多技術術語的定義。*Tivoli 名詞解釋*僅有英文版，位於：

http://www.tivoli.com/support/documents/glossary/termsm03.htm

如需有關 Tivoli Access Manager 的其他資訊來源以及相關主題，請參閱：

http://www.ibm.com/redbooks
http://www.ibm.com/software/sysmgmt/products/support/Field_Guides.html

相關出版品

本節列出與 Tivoli Access Manager 書庫相關的出版品。

IBM Global Security Toolkit

Tivoli Access Manager 透過使用 IBM Global Security Toolkit (GSKit) 來提供資料加密功能。GSKit 內含在適用於您特殊平台的 IBM Tivoli Access Manager Base CD。

GSKit 套件會安裝 iKeyman 金鑰管理公用程式 (gsk5ikm)，讓您能夠建立金鑰資料庫、公開-私密金鑰對，以及憑證要求。下列文件可在「Tivoli 資訊中心」網站上取得，與 IBM Tivoli Access Manager 產品說明文件位在同一個區段：

- *Secure Sockets Layer Introduction and iKeyman User's Guide* (gskikm5c.pdf)

  提供資訊給計畫要在 Tivoli Access Manager 安全網域中啓用 SSL 通訊的網路或系統安全管理者。

IBM DB2 Universal Database

安裝 IBM Directory Server、z/OS™ 及 OS/390® LDAP 伺服器時，需要 IBM DB2® Universal Database™。下列作業系統平台的產品 CD 會提供 DB2：

- IBM AIX
- Microsoft Windows
- Sun Solaris Operating Environment

DB2 資訊可在下列網站取得：

http://www.ibm.com/software/data/db2/

IBM Directory Server

所有平台（Linux for zSeries 除外）的 IBM Tivoli Access Manager Base CD 都提供 IBM Directory Server 第 4.1 版。您可以在下列網站，取得 Linux for S/390 的 IBM Directory Server 軟體：

http://www.ibm.com/software/network/directory/server/download/

如果您計劃要使用 IBM Directory Server 作爲您的使用者登錄，請參閱下列網站中提供的資訊：

http://www.ibm.com/software/network/directory/library/

IBM WebSphere Application Server

IBM WebSphere Application Server、Advanced Single Server Edition 4.0.3 內含在 Web Portal Manager CD，且會隨著 Web Portal Manager 介面一起安裝。如需 IBM WebSphere Application Server 的相關資訊，請參閱：

http://www.ibm.com/software/webservers/appserv/infocenter.html

IBM Tivoli Access Manager for Business Integration

IBM Tivoli Access Manager for Business Integration 是可以個別訂購的產品，它提供 IBM MQSeries® 第 5.2 版及 IBM WebSphere® MQ 第 5.3 版訊息的安全解決方案全。 IBM Tivoli Access Manager for Business Integration 可讓 WebSphere MQSeries 應用程式使用與傳送及接收應用程式相關聯的金鑰，來傳送具有私密性及完整性的資料。如同 WebSEAL 及 IBM Tivoli Access Manager for Operating Systems 一般，IBM Tivoli Access Manager for Business Integration 是使用 IBM Tivoli Access Manager for e-business 的授權服務程式的其中一個資源管理程式。

下列是與 IBM Tivoli Access Manager for Business Integration 第 4.1 版相關聯的文件，可在「Tivoli 資訊中心」網站取得：

- IBM Tivoli Access Manager for Business Integration Administrator's Guide (SC23-4831-00)
- IBM Tivoli Access Manager for Business Integration Release Notes (GI11-0957-00)
- IBM Tivoli Access Manager for Business Integration Read Me First Card (GI11-0958-00)

IBM Tivoli Access Manager for Operating Systems

IBM Tivoli Access Manager for Operating Systems 是可以個別訂購的產品。除了原始作業系統提供的授權原則外，它還在 UNIX 系統上提供授權原則加強層。IBM Tivoli Access Manager for Operating Systems 如同 WebSEAL 及 IBM Tivoli Access Manager for Business Integration 一般，是使用 IBM Tivoli Access Manager for e-business 的授權服務程式的其中一個資源管理程式。

下列是與 IBM Tivoli Access Manager for Operating Systems 第 4.1 版相關聯的文件，可在「Tivoli 資訊中心」網站取得：

- IBM Tivoli Access Manager for Operating Systems Installation Guide (SC23-4829-00)
- IBM Tivoli Access Manager for Operating Systems Administration Guide (SC23-4827-00)
- IBM Tivoli Access Manager for Operating Systems Problem Determination Guide (SC23-4828-00)
- IBM Tivoli Access Manager for Operating Systems Release Notes (GI11-0951-00)
- IBM Tivoli Access Manager for Operating Systems Read Me First Card (GI11-0949-00)

線上存取出版品

當 IBM 發佈一或多份線上或印刷本出版品的更新版本時，都會將他們公佈在 Tivoli 資訊中心。Tivoli 資訊中心包含產品書庫中出版品的最新版本，其格式爲 PDF、HTML 或兩者兼有。某些產品也有翻譯的文件。

您可以從下列網站存取「Tivoli 資訊中心」中更新的出版品，以及其他技術資訊來源：

http://www.tivoli.com/support/documents/

資訊是依產品來組織分類，包括版本注意事項、安裝手冊、使用手冊、管理手冊和程式開發參考手冊。

註: 若您將 PDF 文件列印於信紙規格以外的紙張上，請選取**適合頁面**勾選框於 Adobe Acrobat 「列印」對話框（當您按一下**「檔案」→「列印」** 就可看見此對話框）以確保頁面完整的列印在您使用的紙張上。

訂購出版品

您可以在下列網站訂購許多 Tivoli 出版品：

http://www.elink.ibmlink.ibm.com/public/applications/ publications/cgibin/pbi.cgi

也可以打電話到下列其中一個號碼來訂購：

- 美國地區：800-879-2755
- 加拿大：800-426-4968
- 在其他國家或地區，如需電話號碼清單，請參閱下列網站：

  http://www.tivoli.com/inside/store/lit_order.html

提供關於出版品的回饋意見

如果您對於 Tivoli 產品及說明文件有任何意見或建議，請填寫位於下列網站的客戶意見調查表：

http://www.tivoli.com/support/survey/

協助工具

協助工具特色可幫助行動不便或視障等身體傷殘的使用者順利使用軟體產品。使用本產品，您可以利用協助技術，靠聽覺來瀏覽介面。您也可以使用鍵盤取代滑鼠來操作圖形式使用者介面的所有功能。

聯絡客戶支援中心

如果您有任何 Tivoli 產品的問題，可以聯絡 Tivoli 產品的「IBM 客戶支援中心」。請參閱下列網站的 *Tivoli 客戶支援手冊*：

http://www.tivoli.com/support/handbook/

這本手冊提供了有關如何聯絡「客戶支援中心」的資訊（根據您問題的嚴重程度而定），以及下列資訊：

- 登記與資格
- 視您所在國家或地區而定的電話號碼和電子郵件
- 聯絡「客戶支援中心」之前應收集的資訊

本書中使用的慣例

本書使用下列字體慣例：

粗體	您必須完全照用的指令名稱和選項、關鍵字和其他資訊是以**粗體**呈現。
斜體	您必須提供的變數、指令選項以及必須提供的值以斜體字呈現。出版品標題和強調的特殊字或詞也是以*斜體*字呈現。
等寬	程式碼範例、指令行、螢幕輸出、檔案和目錄名稱、以及系統訊息是以等寬字型呈現。

第 1 章 簡介 IBM Tivoli Access Manager Plug-in for Web Servers

IBM® Tivoli® Access Manager (Tivoli Access Manager) Plug-in for Web Servers 是一種整合解決方案，可讓您容易地實作及管理受保護 Web 空間的安全原則。與您的 Web 伺服器作爲同一處理程序的一部份一起安裝，外掛程式充當您的用戶端與受保護的 Web 空間的安全閘道。

本簡介章節將概述 Tivoli Access Manager Plug-in for Web Servers 技術，其識別產品的技術需求，以及簡介使用外掛程式來確定 Web 空間安全的處理程序。

主題索引：

Tivoli Access Manager Plug-in for Web Servers 技術

Tivoli Access Manager Plug-in for Web Servers 可以與 Tivoli Access Manager 應用程式整合在一起，以提供 Web 資源的完整安全解決方案。外掛程式是當作您的 Web 伺服器的同一處理程序的一部份來操作，它會截取每一個抵達的要求、判定是否需要授權決策，以及必要時提供使用者鑑定的方法。外掛程式可提供單一登入解決方案，並將 Web 應用程式資源納入其安全原則內。

基本作業元件及架構

兩個基本架構元件構成 Tivoli Access Manager Plug-in for Web Servers – 外掛程式元件及 Authorization Server。外掛程式元件是與 Web 伺服器執行緒一起操作，透過「跨處理通訊 (IPC)」介面，將每一個要求的明細傳送至 Authorization Server。 Authorization Server 對進入的要求執行鑑定及授權。Authorization Server 是本端模式 AZNAPI 應用程式，它會接受並處理來自外掛程式的要求以及回應，同時告訴外掛程式如何處理每一個要求。

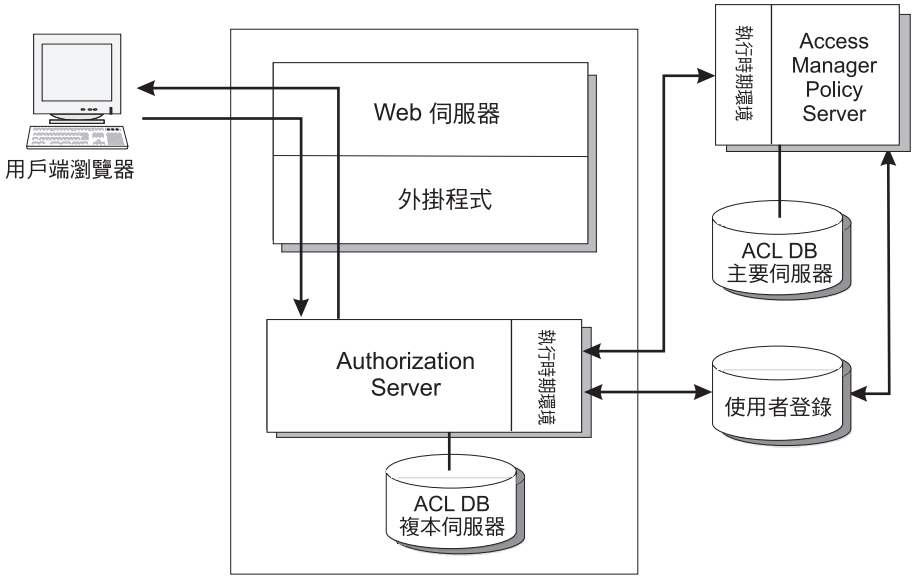

圖 1. 外掛程式及 Tivoli Access Manager 元件互動。

Authorization Server 會判定將要求送至哪一個虛擬主機（如果虛擬主機呈現在 Web 伺服器的話），以及判定要求是否需要授權。不需要授權的要求將直接傳送至 Web 伺服器進行處理。需要授權的要求將由 Authorization Server 以下列方法加以處理：

1. 從先前鑑定的要求擷取階段作業及鑑定資訊。
2. 必要時，起始一個與使用者的鑑定互動。
3. 建立 Tivoli Access Manager 證明。
4. 識別使用者可以存取的資源，而且這些資源會對映至對應的 Tivoli Access Manager 受保護的物件名稱。受保護的物件名稱代表一個電子實體，如網站的安全部份，或僅允許某些使用者存取的應用程式。
5. 判定要求或回應是否需要修改。
6. 產生外掛程式或主機 Web 伺服器需要的回應，方法爲新增 cookie 或標頭至要求或回應，或是產生一個回應（例如，已鑑定的回應或未授權的回應）。

虛擬主機的支援

「虛擬主機」是容許 Web 伺服器被當作網際網路上的多個主機的能力。Tivoli Access Manager Plug-in for Web Servers 支援的 Web 伺服器全都會提供虛擬主機能力。

Tivoli Access Manager Plug-in for Web Servers 提供依照每一虛擬主機基礎來實作安全原則的能力。本文件稍後將討論實作這個能力所需的應用程式設定。

利用 Tivoli Access Manager Plug-in for Web Servers 保護 Web 空間

Tivoli Access Manager Plug-in for Web Servers 提供下列功能：

- 支援多個鑑定方法，包括：基本鑑定、IP 位址、記號、憑證，以及套表，還有其他鑑定方法。
- 接受 HTTP 和 HTTPS 要求。
- 藉由根據組織原則來鑑定及授權使用者要求，以便保護 Web 伺服器資源。

- 支援虛擬主機環境中要求的鑑定及授權。
- 管理 Web 伺服器空間的存取控制。

  支援的資源包括 URL、以 URL 爲基礎的正規表示式、CGI 程式、HTML 檔、Java servlet 和 Java 類別檔。
- 快取階段作業及證明資訊，以避免在授權檢查時重複查詢使用者登錄資料庫。
- 提供單一登入功能

公司安全原則可以識別需要保護的 Web 資源，以及那些 Web 資源每一個所需的保護層次。 Tivoli Access Manager 使用這些 Web 資源的虛擬表現方式，稱爲受保護的物件空間。受保護的物件空間包含代表您網路內之實際實體資源的物件。施行安全原則的方式是對需要保護的物件套用適當的安全機制。

安全機制包括：

- 存取控制清單（ACL）原則

  ACL 原則識別可被考慮存取的使用者類型，以及指定每一使用者類型的物件上所允許的作業。
- 受保護物件原則 (POP)

  POP 指定附加的條件，其支配對受保護的物件之存取，例如私密性、完整性、審核及日期時間存取。
- 延伸屬性

  延伸屬性是置於物件、ACL 或 POP 上，可影響授權決策的額外值。

它是 Tivoli Access Manager Plug-in for Web Servers 的 Authorization Server 元件，這個元件會依據置於物件上的使用者證明及存取控制，來允許或拒絕存取受保護的資源。若要順利實作安全原則，您必須以邏輯方式組織不同的內容類型，並套用適當的 ACL 和 POP 原則。存取控制管理可以是繁複的，若能仔細地將內容類型分門別類，將可使其簡單很多。有關 Tivoli Access Manager 的廣泛資訊，包括設定原則的明細，都可以在 *IBM Tivoli Access Manager Base Administrator's Guide* 中找到。

Tivoli Access Manager Plug-in for Web Servers 鑑定

鑑定是識別試圖登入安全網域之個別處理程序或實體的方法。授權是判定已鑑定的使用者是否有權對特定資源執行作業的方法。鑑定只是確保個人是否確爲其宣稱的身份，但是和對資源執行作業的能力完全無關。

Tivoli Access Manager Plug-in for Web Servers 可強制在安全網域中施行高度安全性，其方法爲要求每一個用戶端提供身份證明。提供廣泛網路安全性的做法爲讓 Tivoli Access Manager Plug-in for Web Servers 控制用戶端的鑑定及授權。

下列條件適用於 Tivoli Access Manager Plug-in for Web Servers 鑑定：

- 外掛程式支援標準的鑑定方法集。您可自訂外掛程式來支援其他鑑定方法。
- 外掛程式處理程序與鑑定方法各自獨立運作。
- 外掛程式只需要用戶端身份。外掛程式透過此身份來取得已鑑定（或未經鑑定）的證明，可供 Authorization Server 用來允許或拒絕對資源的存取。

這項彈性的鑑定方法可讓安全原則以商業需求爲基礎，而非基於實體網路拓蹼。

Tivoli Access Manager Plug-in for Web Servers 鑑定處理程序會導致下列動作：

1. 用戶端鑑定導致一個用戶端身份。

   唯有使用者在 Tivoli Access Manager 使用者登錄中有定義一個帳戶，用戶端鑑定才會順利完成。否則，使用者會被指定爲未經鑑定。

2. Tivoli Access Manager Plug-in for Web Servers 使用用戶端身份，來取得該用戶端的證明。

   外掛程式會比對已鑑定的用戶端身份與已登錄的 Tivoli Access Manager 使用者。然後，外掛程式就會取得適當的使用者證明。這就是所謂的證明取得。

   證明包括使用者名稱，以及使用者在其中具有成員資格的任何群組。這些證明可供外掛程式用來允許或拒絕存取 Tivoli Access Manager 保護的物件空間中的所要求物件。

   證明可供任何需要用戶端相關資訊的 Tivoli Access Manager 服務程式使用。證明可讓 Tivoli Access Manager 安全地執行眾多服務，例如授權、審核及委託。

   關於支援特定鑑定方法的進一步資訊，請參閱第 35 頁的第 4 章, 『IBM Tivoli Access Manager Plug-in for Web Servers 鑑定』。

取得證明

鑑定處理程序的主要目標就是取得說明用戶端使用者的證明資訊。使用者證明是參與安全網域的關鍵需求。

Tivoli Access Manager 會區分使用者的鑑定與證明的取得。使用者身份永遠是固定的。然而，證明 — 其定義使用者在其中參與的群組或角色 — 卻是變動的。環境特有的證明會隨時間改變。例如，當某人升遷時，證明必須反映新的職責層次。

鑑定處理程序會導致方法特有的使用者識別資訊。將對照常駐在 Tivoli Access Manager 使用者登錄（根據預設值，指的是 LDAP）的使用者帳戶資訊，來檢查此資訊。Tivoli Access Manager Plug-in for Web Servers 會將使用者名稱及群組資訊對映至共用的全網域表示法，以及稱爲「延伸專用權屬性憑證 (EPAC)」的格式。

方法特有的身份資訊（例如密碼、記號及憑證）代表使用者的實際身份內容。這項資訊可用來建立與伺服器的安全階段作業。

產生的證明代表使用者在安全網域中的專用權，以特定的環境定義說明使用者，且只對該階段作業的生命週期有效。

Tivoli Access Manager 證明含有使用者身份，以及這個使用者在其中具有成員資格的群組。

證明是供任何需要用戶端相關資訊的 Tivoli Access Manager 服務程式使用。例如，Tivoli Access Manager Authorization Server 利用使用者證明來判定使用者是否獲授權對安全網中受保護的資源執行特定的作業。證明也會用在其他作業，如記載及審核。

EPAC 含有「唯一通用識別字 (UUID)」，Tivoli Access Manager 需要這些識別字，才能使用存取控制清單 (ACL)。

下列 EPAC 欄位適合於 Tivoli Access Manager：

表 1. Tivoli Access Manager EPAC 欄位

屬性	說明
安全網域 ID	主體的起始安全網域識別字
主體 UUID	主體的 UUID
群組 UUID	主體所屬之群組的 UUID

第 2 章 安裝 IBM Tivoli Access Manager Plug-in for Web Servers

本章提供 IBM Tivoli Access Manager (Tivoli Access Manager) Plug-in for Web Servers 的安裝明細。其中包括軟硬體需求的相關資訊，以及詳細的安裝指示。

主題索引：

支援的平台

Tivoli Access Manager Plug-in for Web Servers 可以在下列平台上，與下列 Web 伺服器整合在一起：

- Windows® 2000 Server/Advanced Server – Service pack 2，含有 Internet Information Server (IIS) 第 5.0 版。
- Solaris® Operating Environment (Solaris) 7 (sparc) 及 8，含有 Sun™ ONE Web Server（之前稱爲 iPlanet）6.0 Service Pack 4
- AIX® 4.3.3 及 5L，含有 IBM HTTP Server (IHS) 1.3.19

註: 套用所有來自 Web 伺服器供應商的可用安全性修正檔。

磁碟和記憶體需求

Tivoli Access Manager Plug-in for Web Servers 具有下列硬體需求：

- 如果和必備的 Tivoli Access Manager runtime 環境組合在一起，所需的最小磁碟空間爲 23MB。
- 記憶體：至少 64 MB。建議使用 256 MB。

  請注意：此處所謂至少 64 MB，並不包括必備之 Tivoli Access Manager runtime 環境的需求（至少 64 MB）。要有 256 MB 或以上的記憶體總數，才能產生最佳效能。

必備軟體

Tivoli Access Manager Plug-in for Web Servers 是一種可與 Web 伺服器軟體整合在一起，且在 Tivoli Access Manager 安全網域中執行的應用程式。在安裝外掛程式之前，您必須設定 Web 伺服器，並建立 Tivoli Access Manager 安全網域。

Tivoli Access Manager 安全網域是在安裝 Tivoli Access Manager 軟體時建立的。這個軟體位於 IBM Tivoli Access Manager for e-business Base CD。

下列軟體必須安裝在目標 Web 伺服器後，才能安裝 Tivoli Access Manager Plug-in for Web Servers 軟體：

- Web 伺服器軟體。這將是下列其中一個：
  - IIS 5.0 用於 Windows 2000 Server/Advanced Server 環境
  - Sun ONE Web Server 6.0 (Service Pack 4) for Solaris 7 (sparc)/8
  - IHS 1.3.19 用於 AIX 4.3.3 或 5L 環境。
- IBM Tivoli Access Manager runtime environment v4.1
- IBM Global Security Toolkit (GSKit) 5.0.5.46
- 如果使用 LDAP，則爲 IBM LDAP 4.1 用戶端。

下列應用程式不需要安裝在 Web 伺服器 – 它們會設定成建立 Tivoli Access Manager 安全網域的一部份。它們必須存在網路中可被外掛程式存取的位置。

- IBM Tivoli Access Manager Policy Server v4.1
- IBM Global Security Toolkit (GSKit) 5.0.5.46
- 如果使用 LDAP，則爲支援的 LDAP Server，如 IBM Secure Way Directory 4.1

安裝 Tivoli Access Manager Plug-in for Web Servers

本節提供在三個支援的平台上安裝 Tivoli Access Manager Plug-in for Web Servers 的指示。

在 AIX – IHS 上安裝外掛程式

若要在 AIX 上安裝並配置 Tivoli Access Manager Plug-in for Web Servers：

1. 在 AIX 4.3.3 或 5L Web 伺服器上，確定可在環境中使用下列產品：
   - IBM Tivoli Access Manager for e-business Policy Server v4.1。請參閱 *IBM Tivoli Access Manager Base 安裝手冊*。

     註: Tivoli Access Manager Policy Server 不需要與 Tivoli Access Manager runtime environment 位在同一部機器上。
2. 確定已安裝：
   - IHS Web 伺服器軟體。
   - IBM Tivoli Access Manager for e-business runtime environment v4.1. 請參閱 *IBM Tivoli Access Manager Base 安裝手冊*。
   - IBM Global Security Toolkit (GSKit) 5.0.5.46
   - 如果您正在使用 LDAP 使用者登錄，請安裝 IBM Directory Client 4.1
3. Tivoli Access Manager Plug-in for Web Servers 安裝作業會使解壓縮與套件配置分開。請先使用 **SMIT** 將軟體套件安裝到 AIX 上。接著，使用外掛程式配置公用程式 **pdwpicfg** 來配置安裝作業。

   以 **root** 使用者身份登入。
4. 將 *IBM Tivoli Access Manager Web Security, Version 4.1, for AIX* CD 插入光碟機。
5. 在 Shell 提示中輸入下列指令：

   ```
   # smit
   ```

這時會啓動 **SMIT** 公用程式。

6. 選取**軟體安裝及維護**。選取**安裝及更新軟體**。選取**從最新可用的軟體來安裝及更新軟體**。
7. 出現要求輸入裝置的提示時，請輸入裝載 CD 的位置。
8. 按一下**列示**按鈕來取得**要安裝的軟體**。

   多重選擇清單視窗會顯示 IBM Tivoli Access Manager 軟體套件。
9. 選取 **Access Manager Plug-in for Web Servers** 及 **Access Manager Plug-in for IBM HTTP Server** 軟體套件。按一下**確定**。
10. 畫面上會顯示**從最新可用的軟體來安裝及更新軟體**對話框。
11. 驗證預設值**是**出現在標示有**自動安裝所需的軟體**的欄位中。
12. 根據您的安裝來設定相關的其他欄位值。在大部分的情況下，您可以接受預設值。按一下**確定**。
13. 畫面會顯示一個訊息框，詢問您是否確定安裝這個套件。按一下**確定**。

    系統會安裝套件檔案，同時會顯示幾則狀態訊息。在完成檔案解壓縮時，會出現最後的狀態訊息，指出順利完成。
14. 按一下**完成**。按一下**取消**來結束 SMIT。
15. 如果您尚未配置 Tivoli Access Manager runtime environment，則必須在這個階段中執行配置。請參閱 *IBM Tivoli Access Manager Base 安裝手冊*，以取得配置 Tivoli Access Manager runtime environment 的詳細資訊。
16. 若要配置外掛程式，請移至 `/opt/pdwebpi/bin`，然後執行：

    ```
    # ./pdwpicfg
    ```

    輸入字母 `c`。
17. 畫面會顯示一個清單，列出 Web 伺服器所知的全部虛擬主機。您具有三個選項：
    - 如果您僅想要一部受到外掛程式保護的虛擬主機，請輸入相對於已顯示之清單中虛擬主機的號碼。
    - 若要保護多個虛擬主機的安全，請輸入相對於已顯示之清單中虛擬主機位置的值。以空格隔開所輸入的號碼。
    - 輸入 `all`，讓外掛程式保護伺服器上所有已知的虛擬主機。
18. 輸入 Tivoli Access Manager 管理者 ID 及密碼。
19. AZN 更新是在應用程式作業期間，從授權原則伺服器轉送原則資訊 delta 封包。輸入埠號來監聽 AZN 更新，或按下 **Return** 來接受預設值。
20. 輸入 `Y/N` 來啓用/停用 LDAP Server 的 SSL 通訊。在 Web 伺服器及 LDAP Server 位於同一安全網路的環境中，可能不需要啓用 SSL。如果您可以確定 Web 伺服器與 LDAP 之間傳送的資料的完整性及安全性，則選擇不使用 SSL 將改善網路頻寬，因爲它會移除安全負擔。
21. 如果在外掛程式與 LDAP Server 之間啓用了 SSL 通訊，將提示您輸入 LDAP SSL 用戶端金鑰檔案。輸入用戶端 GSKit 金鑰資料庫檔 `pd_ldapkey.kdb` 位於原則伺服器的完整路徑名稱。

    註: 當 Tivoli Access Manager Plug-in for Web Servers 安裝在 Tivoli Access Manager Policy Server 所在的同一部機器上，且利用 SSL 配置至 LDAP 時， LDAP 用戶端檔案將無法共用。

若要保護檔案避免未經授權的存取，必須有 UNIX 檔案許可權。如果許可權容許「外掛程式」使用者存取檔案，則 LDAP 用戶端金鑰檔案可以共用。

22. Tivoli Access Manager Plug-in for Web Servers 配置應該順利完成了。
23. 重新啓動 Web 伺服器。

在 Solaris – Sun ONE Web Server 上安裝外掛程式

若要在 Solaris 上安裝並配置 Tivoli Access Manager Plug-in for Web Servers：

1. 在 Solaris Web 伺服器上，確定可在您的環境中使用 IBM Tivoli Access Manager for e-business Policy Server v4.1。請參閱 *IBM Tivoli Access Manager Base 安裝手冊*。

   註: Tivoli Access Manager Policy Server 不需要與 Tivoli Access Manager runtime environment 位在同一部機器上。

2. 確定已安裝：
   - Sun ONE Web Server 軟體。
   - IBM Tivoli Access Manager for e-business runtime environment v4.1. 請參閱 *IBM Tivoli Access Manager Base 安裝手冊*。
   - IBM Global Security Toolkit (GSKit) 5.0.5.46
   - 如果您正在使用 LDAP 使用者登錄，請安裝 IBM Directory Client 4.1
3. 進行外掛程式安裝作業時，必須將檔案解壓縮和套件配置分開處理。請先使用 **pkgadd** 將軟體套件安裝到 Solaris 上。接著，使用外掛程式配置公用程式 **pdwpicfg** 來配置外掛程式。

   以 **root** 使用者身份登入。
4. 將 *IBM Tivoli Access Manager Web Security, Version 4.1, for Solaris* CD 裝載在 `/cdrom/cdrom0`
5. 將目錄變換至 `/cdrom/cdrom0/solaris`
6. 進行外掛程式安裝作業時，需要新增兩個套件。請執行下列指令，來安裝外掛程式：

   ```
   # pkgadd -d . PDWPI PDWPIipl
   ```

   提示出現時，請輸入 `y`，然後按下 **Return**。檔案會從 CD 解壓縮，並且安裝到硬碟上。
7. 若要配置外掛程式，請移至 `/opt/pdwebpi/bin`，然後執行：

   ```
   # ./pdwpicfg
   ```
8. 輸入字母 `c` 來配置應用程式。
9. 輸入 Sun ONE Web Server 的根目錄。
10. 畫面會顯示一個清單，列出 Web 伺服器所知的全部虛擬主機。您具有三個選項：
    - 如果您僅想要一部受到外掛程式保護的虛擬主機，請輸入相對於已顯示之清單中虛擬主機的號碼。
    - 若要保護多個虛擬主機的安全，請輸入相對於已顯示之清單中虛擬主機位置的值，以空格隔開所輸入的值。
    - 輸入 `all`，讓外掛程式保護伺服器上所有已知的虛擬主機。
11. 輸入 Tivoli Access Manager 管理者 ID 及密碼。

12. AZN 更新是在應用程式作業期間，從授權原則伺服器轉送原則資訊 delta 封包。輸入埠號來監聽 AZN 更新，或按下 **Return** 來接受預設值。
13. 輸入 `Y/N` 來啓用/停用 LDAP Server 的 SSL 通訊。在 Web 伺服器及 LDAP Server 位於同一安全網路的環境中，可能不需要啓用 SSL。如果您可以確定 Web 伺服器與 LDAP 之間傳送的資料的完整性及安全性，則選擇不使用 SSL 將改善網路頻寬，因爲它會移除安全負擔。
14. 如果在外掛程式與 LDAP Server 之間啓用了 SSL 通訊，將提示您輸入 LDAP SSL 用戶端金鑰檔案。輸入用戶端 GSKit 金鑰資料庫檔 `pd_ldapkey.kdb` 位於原則伺服器的完整路徑名稱。

    註: 當 Tivoli Access Manager Plug-in for Web Servers 安裝在 Tivoli Access Manager Policy Server 所在的同一部機器上，且利用 SSL 配置至 LDAP 時， LDAP 用戶端檔案將無法共用。

    若要保護檔案避免未經授權的存取，必須有 UNIX 檔案許可權。如果許可權容許「外掛程式」使用者存取檔案，則 LDAP 用戶端金鑰檔案可以共用。
15. 輸入 LDAP 使用者名稱及密碼。
16. Tivoli Access Manager Plug-in for Web Servers 配置應該順利完成了。
17. 重新啓動 Web 伺服器。

在 Windows – IIS 上安裝外掛程式

若要在 Windows 2000 Server/Advanced Server Web 伺服器上安裝 Tivoli Access Manager Plug-in for Web Servers：

1. 在 Windows 2000 Web 伺服器上，確定可在您的環境中使用 IBM Tivoli Access Manager for e-business Policy Server v4.1。請參閱 *IBM Tivoli Access Manager Base 安裝手冊*。

    註: Tivoli Access Manager Policy Server 不需要與 Tivoli Access Manager runtime environment 位在同一部機器上。
2. 確定已安裝：
    - IIS Web 伺服器軟體。
    - IBM Tivoli Access Manager for e-business runtime environment v4.1. 請參閱 *IBM Tivoli Access Manager Base 安裝手冊*。
    - IBM Global Security Toolkit (GSKit) 5.0.5.46
    - 如果您正在使用 LDAP 使用者登錄，請安裝 IBM Directory Client 4.1
3. 以具備 Windows 管理者專用權的使用者身份登入 Windows 網域。
4. 將 *IBM Tivoli Access Manager Web Security, Version 4.1, for Windows* CD 插入光碟機。
5. 按兩下下列檔案來執行 Tivoli Access Manager Plug-in for Web Servers InstallShield 安裝程式（其中字母 E: 是光碟機）。

    ```
    E:\Windows\PolicyDirector\Disk Images\Disk1\PDWebPI\Disk Images\Disk1\Setup.exe
    ```
6. 從**選取套件**視窗，選取 Plug-in for Web Servers 套件，然後按一下**確定**。
7. 畫面會顯示**選擇安裝語言**對話框。選取適當的語言，然後按一下**確定**。
8. 這時 **InstallShield** 程式就會啓動，並顯示**歡迎使用**對話框。按**下一步**。
9. 畫面會顯示**授權合約**對話框。按一下**是**，接受授權合約的條款。

10. 畫面會顯示**選取套件**對話框。保持這兩個已勾選的選項 **Access Manager Plug-in for Web Servers** 及 **Access Manager Plug-in for Microsoft Internet Information Services**。按**下一步**。
11. 畫面會顯示**選擇目的位置**對話框。接受預設安裝位置或指定替代位置。按**下一步**。

    這時程式檔案就會解壓縮至磁碟。畫面上會顯示一則訊息，指出已安裝軟體。
12. 按一下**完成**來結束安裝程式，並開始檔案解壓縮處理程序。完成時，請按一下**完成**。
13. 從**開始**功能表選取：**程式集** > **Access Manager Plug-in for Web Servers** > **配置**。

    畫面上會顯示 Tivoli Access Manager Plug-in for Web Servers 配置選擇對話框。
14. 畫面上會顯示一個清單，列出 Web 伺服器所知的全部虛擬主機。選取要保護的虛擬主機。按**下一步**。
15. 輸入 Tivoli Access Manager 管理者使用者 ID *sec_master*，以及密碼。按**下一步**。
16. AZN 更新是在應用程式作業期間，從授權原則伺服器轉送原則資訊 delta 封包。輸入埠號來監聽 AZN 更新，或接受預設值。按**下一步**。
17. 選取**是**或**否**來啓用/停用 LDAP Server 的 SSL 通訊。在 Web 伺服器及 LDAP Server 位於同一安全網路的環境中，可能不需要啓用 SSL。如果您可以確定 Web 伺服器與 LDAP 之間傳送的資料的完整性及安全性，則選擇不使用 SSL 將改善網路頻寬，因爲它會移除安全負擔。

    如果您選擇要在外掛程式與 LDAP Server 之間使用 SSL 通訊：

    a. 輸入用戶端 GSKit 金鑰資料庫檔 `pd_ldapkey.kdb` 位於原則伺服器的完整路徑名稱。
    b. 必要時，輸入憑證標籤。
    c. 輸入金鑰檔案密碼。
    d. 選取**下一步**。

    註: 當 Tivoli Access Manager Plug-in for Web Servers 安裝在 Tivoli Access Manager Policy Server 所在的同一部機器上，且利用 SSL 配置至 LDAP 時， LDAP 用戶端檔案將無法共用。

    若要保護檔案避免未經授權的存取，必須有檔案許可權。如果許可權容許「外掛程式」使用者存取檔案，則 LDAP 用戶端金鑰檔案可以共用。
18. 提示出現時，請輸入 LDAP 使用者名稱及密碼。
19. Tivoli Access Manager Plug-in for Web Servers 配置應該順利完成了。
20. 重新啓動 IIS。

註: 如果您已在 Active Directory 的用戶端上安裝並配置了 Access Manager（例如，Access Manager 及 Active Directory 位在不同系統上)，則用戶端系統必須結合網域，而且您必須以「管理者」身份登入網域，才能在用戶端系統上執行 Access Manager 配置。

升級 Tivoli Access Manager Plug-in for Web Servers

本節提供在三個支援的平台上，將 Tivoli Access Manager Plug-in for Web Servers 從第 3.9 版升級至 4.1 版的指示。

升級前，您不需要保留任何 Tivoli Access Manager Plug-in for Web Servers 資訊。然而，請確定在安裝及升級至第 4.1 版軟體前，對 Tivoli Access Manager 系統執行完整的備份。

也將需要升級 LDAP 用戶端及 GSKit。

在 AIX - IHS 上升級外掛程式

若要在 AIX 上升級 Tivoli Access Manager Plug-in for Web Servers：

1. 在 AIX Web 伺服器上，確定您：
   - 已將 Tivoli Access Manager for e-business runtime environment 升級至第 4.1 版。請參閱 *IBM Tivoli Access Manager Base 安裝手冊*，以取得如何進行升級的指示。
   - 已將 IBM Global Security Toolkit (GSKit) 升級至第 5.0.5.46 版。
   - 如果您正在使用 LDAP 使用者登錄，請將 IBM Directory Client 升級至第 4.1 版。
2. 停止「IHS Web 伺服器」。
3. 在 root shell 提示中輸入下列指令，來停止 Tivoli Access Manager Plug-in for Web Servers 處理程序：

   ```
   # /etc/pdwebpi/pdwebpi stop
   ```
4. 使用 **SMIT**，在 AIX 上升級軟體套件。以 **root** 使用者身份登入。
5. 將 *IBM Tivoli Access Manager Web Security, Version 4.1, for AIX* CD 插入光碟機。
6. 在 Shell 提示中輸入下列指令來啓動 SMIT 公用程式：

   ```
   # smit
   ```
7. 選取**軟體安裝及維護**。選取**安裝及更新軟體**。選取**從最新可用的軟體來安裝及更新軟體**。
8. 出現要求輸入裝置的提示時，請輸入裝載 CD 的位置。
9. 按一下**列示**按鈕來取得要安裝的軟體。多重選擇清單視窗會顯示 Tivoli Access Manager 軟體套件。
10. 選取 **Access Manager Plug-in for Web Servers** 軟體套件。按一下**確定**。
11. 畫面上會顯示**從最新可用的軟體來安裝及更新軟體**對話框。
12. 驗證預設值**是**出現在標示有**自動安裝所需的軟體**的欄位中。
13. 根據您的安裝來設定相關的其他欄位值。 在大部分的情況下，您可以接受預設值。按一下**確定**。
14. 畫面會顯示一個訊息框，詢問您是否確定安裝這個套件。按一下**確定**。

    系統會安裝套件檔案，同時會顯示幾則狀態訊息。在完成檔案解壓縮時，會出現最後的狀態訊息，指出順利完成。
15. 對 *Access Manager Plug-in for IBM HTTP Server* 套件重複步驟 9 - 14。
16. 按一下**完成**。按一下**取消**來結束 SMIT。

17. 在 root shell 提示中輸入下列指令，來啓動 Tivoli Access Manager Plug-in for Web Servers 處理程序：

    ```
    # /etc/pdwebpi/pdwebpi start
    ```

18. 重新啓動「IHS Web 伺服器」。

在 Solaris - Sun ONE Web Server 上升級外掛程式

若要在 Solaris 上升級 Tivoli Access Manager Plug-in for Web Servers：

1. 在 Solaris Web 伺服器上，確定您：
   - 已將 Tivoli Access Manager for e-business runtime environment 升級至第 4.1 版。請參閱 *IBM Tivoli Access Manager Base 安裝手冊*，以取得如何進行升級的指示。
   - 已將 IBM Global Security Toolkit (GSKit) 升級至第 5.0.5.46 版。
   - 如果您正在使用 LDAP 使用者登錄，請將 IBM Directory Client 升級至第 4.1 版。
2. 停止 Sun ONE Web Server。
3. 在 root shell 提示中輸入下列指令，來停止 Tivoli Access Manager Plug-in for Web Servers 處理程序：

   ```
   # /etc/init.d/pdwebpi stop
   ```

4. 確定您以 root 使用者身份登入。請先使用 **pkgadd** 將軟體套件安裝到 Solaris 上。

   ```
   # pkgadd -d package directory -a pddefault packages
   ```

   其中：

package directory	含有外掛程式套件的目錄（通常是從 CD 裝載）。
pddefault	在 CD 上找到的回應檔案。
packages	外掛程式套件；如 PDWPI 及 PDWPIipl

5. 將 *IBM Tivoli Access Manager Web Security, Version 4.1, for Solaris* CD 裝載在 `/cdrom/cdrom0`
6. 將目錄變換至 `/cdrom/cdrom0/solaris`
7. 進行外掛程式安裝作業時，需要新增兩個套件。請執行下列指令，來安裝外掛程式：

   ```
   # pkgadd -d . PDWPI PDWPIipl
   ```

   提示出現時，請輸入 **y**，然後按下 **Return**。檔案會從 CD 解壓縮，並且安裝到硬碟上。

8. 在 root shell 提示中輸入下列指令，來啓動 Tivoli Access Manager Plug-in for Web Servers 處理程序：

   ```
   # /etc/init.d/pdwebpi start
   ```

9. 重新啓動 Sun ONE Web Server。

在 Windows - IIS 上升級外掛程式

若要在 Windows 2000 Server/Advanced Server Web 伺服器上升級 Tivoli Access Manager Plug-in for Web Servers：

1. 在 Windows 2000 Web 伺服器上，確定您：

- 已將 Tivoli Access Manager for e-business runtime environment 升級至第 4.1 版。請參閱 *IBM Tivoli Access Manager Base 安裝手冊*，以取得如何進行升級的指示。
- 已將 IBM Global Security Toolkit (GSKit) 升級至第 5.0.5.46 版。
- 如果您正在使用 LDAP 使用者登錄，請將 IBM Directory Client 升級至第 4.1 版。

2. 以具備 Windows 管理者專用權的使用者身份登入 Windows 網域。
3. 停止 Microsoft Internet Information Services Web Server。
4. 透過服務控制台停止 Tivoli Access Manager Plug-in for Web Servers。
5. 將 *IBM Tivoli Access Manager Web Security, Version 4.1, for Windows* CD 插入光碟機。
6. 按兩下下列檔案來執行 Tivoli Access Manager Plug-in for Web Servers InstallShield 安裝程式（其中字母 E: 是光碟機）。

   ```
   E:\Windows\PolicyDirector\Disk Images\Disk1\setup.exe
   ```

7. 從「選取套件」視窗，選取 *Plug-in for Web Servers* 套件，然後按一下**確定**。
8. 畫面會顯示*選擇安裝語言*對話框。選取適當的語言，然後按一下**確定**。
9. 這時 InstallShield 程式就會啓動，顯示*歡迎使用*對話框。按**下一步**。
10. 畫面會顯示*授權合約*對話框。按一下**是**，接受授權合約的條款。
11. 畫面會顯示*選取套件*對話框。保持這兩個已勾選的選項 **Access Manager Plug-in for Web Servers** 及 **Access Manager Plug-in for Microsoft Internet Information Services**。按**下一步**。
12. 畫面上會顯示一則訊息，指定即將進行升級，請按一下**確定**。
13. 這時程式檔案就會解壓縮至磁碟。畫面上會顯示一則訊息，指出已安裝軟體。
14. 對 Tivoli Access Manager Plug-in for Microsoft Internet Information Services 套件重複步驟 12 -13。
15. 按一下**完成**來結束安裝程式。
16. 透過服務控制台啓動 Tivoli Access Manager Plug-in for Web Servers。
17. 啓動 Microsoft Internet Information Services Web Server。

移除 Tivoli Access Manager Plug-in for Web Servers

本節說明移除 Tivoli Access Manager Plug-in for Web Servers 軟體的處理程序。本節不說明移除 Tivoli Access Manager runtime environment 或 Tivoli Access Manager Policy Server 的處理程序。如需移除 runtime environment 及 Policy Server 的詳細資訊，請參閱 *IBM Tivoli Access Manager Base 安裝手冊*。

從 Windows – IIS 移除外掛程式

移除外掛程式前，必須先解除它的配置。

若要在 Windows 上解除外掛程式的配置：

1. 以具有管理專用權的 Windows 使用者身份登入。
2. 從**開始**功能表按一下：**程式集** > **Access Manager Plug-in for Web Servers** > **解除配置**。

註: 如果是從指令提示執行，則在無法到達 Management Server 時，**-f** 選項可用來強制執行解除配置。

3. 畫面上會顯示一個清單，列出外掛程式所保護的全部虛擬主機。選取要解除配置的虛擬主機。按**下一步**。
4. 輸入 Tivoli Access Manager 使用者 ID 及密碼。選取**下一步**。

   一旦順利地解除了外掛程式的配置時，畫面上就會顯示一個狀態訊息。
5. 重新啓動 IIS。

若要從 Windows 移除外掛程式：

1. 從「Windows 控制台」，按一下**新增/移除程式**。

   畫面上會顯示**新增/移除程式**對話框，列出所有已安裝的軟體。
2. 選取代表 **Access Manager Plug-in for Microsoft Internet Information Services** 的項目。按一下**變更/移除**按鈕。
3. 這時 **InstallShield** 程式就會啓動，並移除外掛程式。
4. 按一下**完成**。

從 AIX – IHS 移除外掛程式

移除外掛程式前，需要先解除它的配置。若要在 AIX 平台上解除外掛程式的配置：

1. 以 root 身份登入。
2. 從 bin 目錄執行下列指令，來啓動外掛程式配置公用程式：

   ```
   # pdwpicfg
   ```

   註: 當無法到達 Management Server 時，**-f** 選項可用來強制執行解除配置。
3. 輸入 u 進行解除配置。
4. 畫面上會顯示一個清單，列出受保護的虛擬主機。選取要解除配置的虛擬主機。
5. 輸入 Tivoli Access Manager 管理者 ID 及密碼。
6. 當解除配置完成時，畫面上會顯示一則訊息。
7. 重新啓動 Web 伺服器。

若要移除外掛程式：

1. 以使用者 root 身份啓動 **SMIT**。
2. 選取**通訊應用程式及服務**。
3. 畫面上會顯示**通訊應用程式及服務**功能表。選取 **Access Manager**。
4. 從 **Access Manager** 功能表選取 **Access Manager 解除配置**。畫面上會顯示一個清單，列出已配置的 Tivoli Access Manager 套件。
5. 選取 **Access Manager Plug-in for Web Servers**。

   提示出現時，請輸入 Tivoli Access Manager 密碼。
6. 在所有提示中，按下 **Enter**。
7. 對 **Access Manager Plug-in for Web Servers IHS** 套件重複步驟 3 至 7。

從 Solaris – Sun ONE Web Server 移除外掛程式

在解除外掛程式的配置後，才能移除它。若要在 Solaris 上解除外掛程式的配置：

1. 以 root 身份登入。

2. 從 bin 目錄執行下列指令，來啓動外掛程式配置公用程式：

   ```
   # pdwpicfg
   ```

   註: 當無法到達 Management Server 時，**-f** 選項可用來強制執行解除配置。
3. 輸入 u 進行解除配置。
4. 畫面上會顯示一個清單，列出受保護的虛擬主機。選取要解除配置的虛擬主機。
5. 輸入 Tivoli Access Manager 管理者 ID 及密碼。
6. 當解除配置完成時，畫面上會顯示一則訊息。
7. 重新啓動 Web 伺服器。

若要從 Solaris 移除外掛程式：

1. 輸入指令：

   ```
   # pkgrm PDWPI PDWPIipl
   ```

   系統會提示您確認您的決定。在提示中輸入 y。

   畫面上會顯示一則訊息，指出移除成功。

第 3 章 IBM Tivoli Access Manager Plug-in for Web Servers 配置

本章說明您可以執行以自訂 IBM Tivoli Access Manager (Tivoli Access Manager) Plug-in for Web Servers 的一般管理及配置作業。

主題索引：

一般外掛程式資訊

下列章節說明關於 Tivoli Access Manager Plug-in for Web Servers 配置的一般資訊：

pdwebpi.conf 配置檔

您可以配置位於 `pdwebpi.conf` 配置檔的參數，來自訂外掛程式的作業。檔案是在以下的目錄中：

UNIX：

```
/opt/pdwebpi/etc/
```

Windows：

```
C:\Program Files\Tivoli\PDWebPI\etc\
```

下表將配置檔的段落 (stanza) 分類。

表 2. pdwebpi.conf 區段摘要

區段	段落
GENERAL	[module-mgr] [modules] [wpiconfig] [pdweb-plugins]
AUTHENTICATION	[common-modules] [authentication-levels] [authentication-mechanisms] [BA] [failover] [forms] [ltpa] [tag-value] [token-card] [http-hdr] [iv-headers] [acctmgmt] [ecsso] [ecsso-domain-keys] [login-redirect] [spnego]
VIRTUAL HOSTS	[*virtual-host-name*]
SESSIONS	[sessions] [session-cookie]
LDAP	[ldap]
PROXY	[proxy-if] [proxy]
AUTHORIZATION API	[aznapi-entitlement-services] [aznapi-configuration]
WEB SERVER	[ihs] [iis] [iplanet]

請參閱第 107 頁的附錄 A, 『pdwebpi.conf 參照』，以取得 pdwebpi.conf 配置檔內可配置參數的說明。

註: 每次變更 pdwebpi.conf 檔案時，您都必須以手動方式重新啓動 Tivoli Access Manager Plug-in for Web Servers，讓新的變更生效。請參閱第 21 頁的『啓動及停止 Tivoli Access Manager Plug-in for Web Servers』，以取得啓動及停止應用程式的相關資訊。

pdwebpimgr.conf 配置檔

外掛程式的 UNIX 安裝作業包括配置檔 pdwebpimgr.conf。這個配置檔含有用來自動重新啓動授權常駐程式（若它失敗的話）的參數。

這個檔案位於目錄：

```
/opt/pdwebpi/etc/
```

您根本不需要變更這個檔案中的參數。

Tivoli Access Manager Plug-in for Web Servers 安裝作業的根目錄

Tivoli Access Manager Plug-in for Web Server 的程式檔案會安裝在下列根目錄：

UNIX：

```
/opt/pdwebpi/
```

Windows：

```
C:\Program Files\Tivoli\PDWebPI\
```

在 Windows 上安裝外掛程式期間，您可以配置這個路徑。在 UNIX 上進行安裝時，您無法配置這個路徑。本手冊使用 *install_path* 變數來代表這個根目錄。

在 UNIX 上進行安裝時，以下的獨立目錄包含了可擴充的檔案（例如審核和日誌檔）：

```
/var/pdwebpi/
```

啓動及停止 Tivoli Access Manager Plug-in for Web Servers

若要啓動及停止外掛程式處理程序，在 UNIX 上請使用 **pdwebpi_start** 指令，在 Windows 上請使用「服務控制台」。

UNIX：

```
pdwebpi_start {start|stop|restart|status}
```

例如，若要停止外掛程式，然後再重新啓動，請使用：

```
# pdwebpi_start restart
```

pdwebpi_start 指令位於下列目錄：

```
/opt/pdwebpi/sbin/
```

Windows：

在「服務控制台」中找出外掛程式處理程序，然後使用適當的控制按鈕。

註: pdwebpi 是 Authorization Server 處理程序。在 UNIX 上進行安裝時，處理程序 **pdwebpimgrd** 會自動重新啓動 Authorization Server，如果它失敗的話。在 Windows 上，Windows 服務會自動重新啓動 Authorization Server。

HTTP 錯誤訊息

有時 Tivoli Access Manager Plug-in for Web Servers 會嘗試服務一個要求，但失敗。造成這個失敗有很多種原因。兩個常見的失敗原因如下：

- 檔案不存在
- 許可權設定禁止存取

當服務要求失敗時，外掛程式會傳回一個錯誤碼給 Web 伺服器，然後伺服器就會解譯錯誤碼並顯示對應的錯誤頁。

巨集支援

下列是可在自訂 HTML 錯誤頁時使用的巨集。巨集將會動態置換可用的適當資訊。

表 3. 支援的巨集替代

巨集	說明
%USERNAME%	已登入使用者的名稱
%ERROR_CODE%	與錯誤相關的數字錯誤碼
%ERROR_TEXT%	與錯誤相關的錯誤文字
%URL%	用戶端所要求的 URL
%HOSTNAME%	完整的主機名稱
%HTTP_BASE%	伺服器的基本 HTTP URL： http://*host*:*tcpport*/
%HTTPS_BASE%	伺服器的基本 HTTPS URL： https://*host*:*sslport*/
%REFERER%	來自要求的參照者標頭的值，若沒有，則爲 'Unknown'。
%BACK_URL%	來自要求的參照者標頭的值，若沒有，則爲 '/'。
%BACK_NAME%	如果參照者標頭呈現在要求中，則爲值 'BACK'，若沒有，則爲 'HOME'。

自訂 IIS 錯誤訊息的顯示方式

IIS 可讓您自訂顯示給用戶端之錯誤頁的格式及內容。這有助於顯示更詳細的錯誤資訊給用戶端。外掛程式可以在 IIS 內利用這個錯誤自訂機能。

在 pdwebpi.conf 配置檔的 **[iis]** 段落內使用 **use-error-pages** 參數，您就可以選擇是 IIS 配置的錯誤頁或是標準錯誤碼頁傳回給用戶端瀏覽器。設爲 *yes*， **use-error-pages** 參數會導致外掛程式使用任何自訂的 IIS 錯誤頁。設爲 *no*，就會針對 Authorization Server 遇到的錯誤顯示標準錯誤頁。根據預設值，**use-error-pages** 參數會設爲 *no*。

註: 將 **use-error-pages** 設爲 *yes*，因此容許爲 Authorization Server 錯誤顯示自訂的 IIS 錯誤頁，將導致外掛程式效能的嚴重退化。

配置 Authorization Server

大部份的授權及鑑定處理程序是由 Authorization Server 處理。 Authorization Server 提供工作者執行緒的儲存池，這些執行緒可以：

- 接受來自外掛程式的要求
- 傳送每一個要求的結果回到外掛程式

外掛程式是透過使用共用記憶體實作的 IPC 機制，與 Authorization Server 通訊。pdwebpi.conf 配置檔中的 **[proxy-if]** 段落指定專屬於外掛程式與 Authorization Server 之間通訊的配置參數。

配置工作者執行緒

配置檔的 **[proxy-if]** 段落中的 **number-of-workers** 及 **worker-size** 參數指定可調整以提供最佳外掛程式 Authorization Server 效能的值。當設定這些值時，請考慮網路上通訊的數量及類型。

```
[proxy-if]
number-of-workers = 10
worker-size = 10000
cleanup-interval=300
```

number-of-workers 參數指定外掛程式可服務的並行進入要求數目。在所有的工作者執行緒都在忙碌時到達的要求將置入緩衝區，直到有工作者執行緒可用爲止。這個參數只是指定可供服務可能無限制的工作佇列之執行緒數目。參數應該根據您預期 Web 伺服器同時接受之要求數目上限來增加。在 UNIX 平台上，作業系統可能會對這個值強加限制。

一般而言，增加執行緒的數目即縮減其完成要求所耗費的平均時間。然而，增加執行緒的數目會影響其他因素，其可能對伺服器效能有負面的影響。

worker-size 參數定義預先配置給每一個工作者執行緒的記憶體數量（以位元組爲單位）。

cleanup-interval 是後續清除 Authorization Server 共用記憶體之間的時間（以分鐘爲單位）。

註: 僅變更 **cleanup-interval** 及 **worker-size** 參數，來解決效能問題。

設定 IPC 要求的階段作業生命週期上限

pdwebpi.conf 配置檔的 **[proxy-if]** 段落中的 **max-session-lifetime** 參數設定逾時前，外掛程式將等待來自 Authorization Server 之回應的時間（以秒爲單位）。這個參數僅與短生命週期的「階段作業」相關，這個階段作業是爲了進行要求處理，而在外掛程式與 Authorization Server 之間建立的。如果發生如此的逾時，將有一個錯誤頁傳送至用戶端。如此的逾時是高度不可能。

```
[proxy-if]
max-session-lifetime = 300
```

註: max-session-lifetime 參數不會控制已鑑定之階段作業的生命週期。已鑑定之階段作業生命週期是由 **[sessions]** 段落中的 **timeout** 參數所控制。

配置錯誤頁

位於 pdwebpi.conf 配置檔的 **[proxy]** 段落中的參數，用來指定當 proxy 中發生錯誤時，要顯示的 HTML 頁面。在 **[proxy]** 段落內設定的參數如下：**error-page**、**acct-locked-page**、**retry-limit-reached-page** 及 **login-success**。這些參數都有預設檔案。您可以編輯這些檔案，或指定新的檔案來符合組織的需求。下表彙總這些參數。

表 4. **[proxy]** *錯誤頁配置參數。*

參數	說明
error-page	當非預期伺服器錯誤發生時，顯示在使用者瀏覽器上之頁面的路徑。
acct-locked-page	當使用者嘗試存取已鎖定的帳戶時所顯示之頁面的路徑。
retry-limit-reached-page	當登入嘗試失敗的次數達到了容許的上限時所顯示之頁面的路徑。容許的登入失敗次數上限設定在 LDAP - 請參閱第 77 頁的『三振登入原則』，以取得如何設定此值的詳細資訊。
login-success	指定在套表或記號登入成功後，若外掛程式沒有頁面來重新導向使用者回到其中，將顯示的頁面。當您建置一個登入套表，直接傳送登入 POST 資料回到外掛程式時，就可能發生這種狀況。

根據預設值，範例 HTML 頁面位於下列目錄： *install_directory*/nls/html/*lang*。

其中 *lang* 取自於 NLS 配置。在進行美式英文安裝作業時，*lang* 將設爲 **C**。

配置虛擬主機伺服器

Tivoli Access Manager Plug-in for Web Servers 是以 pdwebpi.conf 配置檔的 **[pdweb-plugins]** 段落中設定的隨意名稱來識別虛擬主機。

外掛程式可以根據要求的兩個性質，來套用不同的安全原則：

- 要求所送至之虛擬主機的 ID
- 要求到達時所用的通訊協定（http 或 https）

虛擬主機 ID 是衍生自主機 Web 伺服器的配置資訊，是 Web 伺服器特有的。它的決定方式如下：

IHS 用來建構虛擬主機 ID 的配置演算法如下：

1. 如果 **ServerName** 指引存在於 *<VirtualHost {hosta}:{port} {hostb}:{port}...>* 區塊內，將使用該名稱，對虛擬主機清單中的每一個主機建構物件空間。不嘗試將提供的 *servername* 解析爲完整的 *hostname*。
2. 如果 **VirtualHost** 區塊內沒有 **ServerName** 指引，而且清單中的主機名稱不是數值 IP 位址，將嘗試完整定義每一個名稱，然後爲每一個不同的主機名稱建立物件空間。
3. 如果 **VirtualHost** 區塊內沒有 **ServerName** 指引，而且清單中的主機名稱是數值 IP 位址，將嘗試把每一個 IP 位址解析爲完整的主機名稱。
4. 如果仍然沒有主機名稱，且在廣域 **ServerName** 指引中指定了一個名稱，將使用該名稱（不解析）。
5. 如果沒有廣域 **ServerName** 指引，將使用完整版的系統主機名稱。

IIS 此 ID 會完全對應於 Internet Information Services 管理嵌入式管理單元中顯示的網站名稱。例如，當配置 IIS 時所建立的預設網站名爲 ″Default Web Site″，這是 Tivoli Access Manager Plug-in for Web Servers 所使用的 ID。

Sun ONE Web Server（之前稱為 iPlanet） 此 ID 完全對應於在 Sun ONE Web Server 配置 GUI 中建立虛擬主機時所指定的虛擬主機名稱。這個名稱儲存在 **server.xml** 檔案的 **<VS id= >** 元素中。

Tivoli Access Manager Plug-in for Web Servers 是按照虛擬主機來定義安全原則。Tivoli Access Manager Plug-in for Web Servers 虛擬主機是以上面定義的虛擬主機 ID，以及它應該保護的通訊協定集（http、https 或兩者）來加以識別。虛擬主機定義鑑定體系集及其優先順序、階段作業識別體系，以及應該透過其中一個相符的通訊協定，套用至 Web 伺服器虛擬主機之要求的後置授權處理。虛擬主機也會定義如何將 URI 對映至 Tivoli Access Manager 的「受保護的物件空間」名稱。

Tivoli Access Manager Plug-in for Web Servers 虛擬主機定義在配置檔的 **[pdweb-plugins]** 段落中。它們可能定義爲受保護的或不受保護的。不受保護的虛擬主機將沒有套用的 Tivoli Access Manager 安全原則。如果收到一個不符合其中一個已定義之受保護或不受保護的虛擬主機的要求，將在 Authorization Server 的日誌檔中產生一則警告訊息，指出要求的虛擬主機 ID 及通訊協定。這將使您容易診斷出配置問題。

受保護的虛擬主機是由 **[pdweb-plugins]** 段落的 **virtual-host** 參數所定義。不受保護的虛擬主機是由 **[pdweb-plugins]** 段落的 **unprotected-virtual-host** 參數所定義。使用的虛擬主機名稱通常會對應於這個虛擬主機比對的虛擬主機 ID，但是情況不一定永遠都是如此。它是定義在 **[pdweb-plugins]** 段落中的虛擬主機名稱，用來定義虛擬主機特有的安全原則。

特殊虛擬主機的安全原則是由含虛擬主機名稱的段落中指定的配置參數來定義。所有可以定義在虛擬主機段落中的參數都具有適當的預設值，因此不需要每一個虛擬主機都有一個段落。僅在虛擬主機的安全原則不同於預設值時，才需要具有如此段落。

虛擬主機有兩個參數是用來比對進入的要求與定義應該套用至要求之安全原則的虛擬主機。這兩個參數是 **id** 及 **protocols**。

id 參數將定義爲這個虛擬主機將比對的虛擬主機 ID。 **id** 參數的預設值是虛擬主機名稱本身。

protocols 參數定義虛擬主機將比對的通訊協定集。這個值可能是 **http**、**https** 或 **both**。預設值是 **both**。

虛擬主機的剩餘參數用來定義應該套用至符合這個虛擬主機之要求的安全原則。

虛擬主機與受保護的物件空間的特殊子分支有關聯。要求的 URI 是以這個子分支爲字首，以建構受保護的物件空間名稱。這個受保護的物件空間名稱是用於做出授權決策。**branch** 配置參數定義這個受保護的物件空間的名稱。

```
[virtual_host_name]
branch = virtual_host_id
```

如果虛擬主機 ID 值沒有前導反斜線 (/)，項目將以 /PDWebPI/ 爲字首。

branch 參數將預設爲 **id** 參數的值，因而導致預設物件名稱字首 /PDWebPI/*virtual-host-id*。

已解釋的虛擬主機分支

在外掛程式配置期間，將建立稱爲 /PDWebPI 的物件儲存區。在這個物件儲存區內，會爲外掛程式所保護的每一個虛擬主機建立項目。虛擬主機物件下的物件儲存區是由外掛程式 Authorization Server 所擁有，這個伺服器會爲虛擬主機物件空間中的資源執行授權決策。根據預設值，針對虛擬主機使用的物件儲存區分支會從虛擬主機 ID 取得它的名稱。如果將使用 /PDWebPI 物件儲存區的不同分支，則分支延伸會用來指定這個分支。分支可以在虛擬主機之間共用。當虛擬主機是彼此的別名時，就可能發生這種情況。

註: 當分支變更時，需要以新名稱建立物件。任何在舊分支下連接的 ACL 仍會連接至新的未存在物件。

下列範例顯示一個具有四個虛擬主機之 Web 伺服器所需的配置參數：ibm.com、lotus.com-HTTP、lotus.com-HTTPS 及 domino.com。虛擬主機 lotus.com-HTTP 及 lotus.com-HTTPS 是眞正相同的虛擬主機，因爲它們共用相同的分支；然而，它們是藉由存取類型（HTTP 或 HTTPS）來區分。在這種情況中，可以根據存取類型，以不同方式設定鑑定配置。domino.com 不受外掛程式保護，而且 ibm.com 是同一伺服器上的另一個虛擬主機。

```
[pdweb-plugins]
virtual-host = ibm.com
virtual-host = lotus.com-HTTPS
virtual-host = lotus.com-HTTP
unprotected-virtual-host = domino.com

web-server = iplanet

[lotus.com-HTTPS]
id = lotus.com
protocols = https
branch = lotus.com

[lotus.com-HTTP]
id = lotus.com
protocols = http
branch = lotus.com

[ibm.com]
id = ibm.com
protocols = http, https
branch = ibm.com
```

若要設定每一個個別虛擬主機的鑑定參數，需要每一虛擬主機的進一步配置。請參閱第 39 頁的『配置虛擬主機的鑑定』，以取得配置虛擬主機的鑑定方法的詳細資訊。

Web 伺服器特有的配置

外掛程式的部份動作是 Web 伺服器特有的，所以根據外掛程式操作所在的 Web 伺服器類型，將需要特殊配置。請在 pdwebpi.conf 配置檔的 **[pdweb-plugins]** 段落中使用 **web-server** 參數，來定義您的 Web 伺服器類型。有效值是 **ihs**、**iplanet** 或 **iis**。例如：

```
[pdweb-plugins]
web-server = ihs
```

Web 伺服器特有的配置項目存在於 pdwebpi.conf 配置檔的 **[iis]**、**[ihs]** 及 **[iplanet]** 段落中。

您可以依照每一分支來設定部份 Web 伺服器配置參數，方法爲將完整的虛擬主機分支附加至段落；例如，**[iplanet:/PDWebPI/lotus.com]**。與瀏覽 Web 空間相關的參數可用這種方法加以配置。

下表說明特定 Web 伺服器類型的可配置參數。

表 5. Web 伺服器特有的配置參數

參數	說明
[ihs]	
query-contents	指定要用於透過 'pdadmin> object list' 指令瀏覽 IBM HTTP Server Web 空間的查詢內容程式。這個參數可以依照每一分支來置換，方法爲在名爲 **[ihs:*branch*]** 的段落（例如，[ihs:/PDWebPI/lotus.com]）中，指定一值給它
query-log-file	可取得查詢內容程式所遇到之錯誤的日誌檔的位置。
doc-root	指定說明文件 root，它會提供執行 'pdadmin> object list' 指令所需的 Web 空間瀏覽能力。當設定虛擬主機時，這個參數是由配置公用程式所設定的 - 它是依照每一原則分支在 **[ihs:*branch*]** 段落（例如，[ihs:/PDWebPI/lotus.com]）中指定的。
[iis]	
query-contents	指定用於透過 pdadmin 瀏覽 IIS Web 空間的查詢內容程式。這個參數可以依照每一分支來置換，方法爲在名爲 **[iis:*branch*]** 的段落（例如，[iis:/PDWebPI/lotus.com]）中，指定一值給它
query-log-file	可取得查詢內容程式所遇到之錯誤的日誌檔的位置。
log-file	定義日誌檔，以取得來自 IIS 外掛程式的錯誤及追蹤訊息，這些訊息會個別保存在 Authorization Server 日誌檔以外的日誌檔。如果指定爲相對路徑，位置將相對於安裝目錄的 log 子目錄。如果指定爲絕對路徑，將使用絕對路徑。
[iplanet]	
query-contents	指定用於透過 pdadmin 瀏覽 Sun ONE (iPlanet) Web 空間的查詢內容程式。這個參數可以依照每一分支來置換，方法爲在名爲 **[iplanet:*branch*]** 的段落（例如，[iplanet:/PDWebPI/lotus.com]）中，指定一值給它
query-log-file	可取得查詢內容程式所遇到之錯誤的日誌檔的位置。
doc-root	指定說明文件 root，它會提供執行 'pdadmin> object list' 指令所需的 Web 空間瀏覽能力。當設定虛擬主機時，這個參數是由配置公用程式所設定的 - 它是依照每一原則分支在 **[iplanet:*branch*]** 段落（例如，[iplanet:/PDWebPI/lotus.com]）中指定的。

在下面範例中，虛擬主機 ibm.com 及 lotus.com 兩者在配置檔：[iplanet:/PDWebPI/ibm.com] 及 [iplanet:/PDWebPI/lotus.com] 中都具有對應的段落，這是特定的配置參數定義所在。

```
[pdweb-plugins]
virtual-host = ibm.com
virtual-host = lotus.com
web-server = iplanet

[iplanet]
query-contents = /opt/pdweb/bin/wpi_iplanet_ls
```

```
[iplanet:/PDWebPI/ibm.com]
doc-root = /usr/local/ibm.com/doc/root

[iplanet:/PDWebPI/lotus.com]
doc-root = /usr/local/lotus.com/doc/root
```

註: 在 Web 伺服器**內容**對話框中，使用*目錄安全*標籤來配置 IIS 安全設定時，必須記住部份可配置安全設定是可透過 Web 空間階層來繼承。

外掛程式會動態地建立「虛擬」Web 空間物件，來處理各種函數。這些物件上的安全設定通常都是重要的。這些物件上的安全內容不得變更。

一旦在**內容**對話框的*目錄安全*標籤內，修改了 IIS 安全設定，畫面上就會顯示*繼承置換*對話框。*繼承置換*對話框會列示置換您剛設定之值的*子節點*。您具有選擇哪些節點應該使用新值的選項。在這個對話框中，**不得**選取 *PDWebPI* 節點。

配置 LDAP 伺服器的失效接替

啓動時，Tivoli Access Manager plug-in for Web Servers 會連接至任何可用的 LDAP Server（主要或複本，視優先順序而定）。如果 LDAP 主要伺服器因故當機，外掛程式必須能夠連接到可用的 LDAP 複本伺服器，以進行任何讀取作業。這是標準 Tivoli Access Manager LDAP 複本配置。如需進一步的詳細資訊，請參閱 *IBM Tivoli Access Manager Base Administrator's Guide*。

IBM Directory (LDAP) 支援一個或多個唯讀複本 LDAP 伺服器的存在。 Sun ONE（之前稱爲 iPlanet）Directory Server (LDAP) 允許同時存在一或多個稱爲 ″consumers″ 的唯讀複本 LDAP 伺服器。您必須新增幾行到 `pdwebpi.conf` 配置檔的 **[ldap]** 段落中，以識別可供外掛程式使用的任何複本伺服器。請對每一個複本使用下列語法：

```
replica = ldap_server,port,type,preference
```

其中：

ldap-server	LDAP 複本伺服器的網路名稱。
port	此伺服器所接聽的埠。通常是使用 389 或 636。
type	複本伺服器的功能 - 亦即 ″read-only″ 或 ″read-write″。在一般情況下請使用 ″read-only″。″read-write″ 這個類型代表的是主要伺服器。
preference	從 1 到 10 的數字。具有最高喜好設定值的伺服器會被選來進行 LDAP 連線。請參閱 *IBM Tivoli Access Manager Base Administrator's Guide* 中的 ″Setting preference values for replica LDAP servers″。

範例：

```
replica =replica1.ldap.tivoli.com,389,readonly,5
replica =replica2.ldap.tivoli.com,389,readonly,5
```

配置外掛程式審核、記載、追蹤及快取資料庫

記載及審核提供的資訊將可協助您識別任何可能因爲外掛程式而遭遇的問題。如果您發現遭遇麻煩，而且需要即時檢視錯誤訊息，請使用 **-foreground** 選項，在前景中啓動外掛程式；亦即，

```
pdwebpi -foreground
```

註: 若要在 IIS 進行安裝，請在前景模式中啓動外掛程式之前，先重新啓動 IIS，再釋出任何現有的共用記憶體。

狀態及錯誤訊息都會記載在 **log-file**、**logs** 及 **log-entries** 參數中所配置的檔案，這些參數位於 pdwebpi.conf 配置檔的 **[pdweb-plugins]** 段落中。

外掛程式審核及基本快取資料庫配置是使用在 pdwebpi.conf 配置檔的 **[aznapi-configuration]** 段落中的參數來執行。

審核記錄

授權 API 的基本服務容許攫取鑑定 (authn) 及授權 (azn) 審核事件。

然而，標準 'authn' 審核事件不會封裝關於鑑定嘗試的足夠資訊，這個嘗試容許這些事件與特定虛擬主機（在這裡外掛程式正在保護多個單一主機）相關。基於這個理由，外掛程式會實作它自己的審核事件種類，以攫取虛擬主機特有的鑑定資訊。

藉由以 /PDWebPI/*virtual_host_name* 字首建立的受保護物件名稱，標準 'azn' 審核事件的確會攫取外掛程式相關虛擬主機資訊。

外掛程式特有的鑑定審核事件會記錄在如下建構的虛擬主機特有的審核事件儲存池：

wpi.*virtual_host_name*.authn.*authentication_module_name*

外掛程式特有的鑑定審核事件符合 *IBM Tivoli Access Manager Base Administrator's Guide* 中所說明的 DTD 定義。

下表會說明 XML 樣式 'wpi' 審核記錄的元素。

表 6. 鑑定審核記錄欄位定義。

XML 標籤	說明
<event>	封裝審核記錄的標籤。元素包括說明記錄的 doc 類型定義修訂的屬性。
<date>	發生事件的日期及時間的記錄。
<outcome>	標籤元素包括一個 **status** 參數，來識別 Tivoli Access Manager 或外掛程式錯誤碼。元素說明事件的廣泛結果。可能值如下： • 0 = 成功 • 1 = 失敗 • 2 = 擱置 • 3 = 不明
<originator>	審核記錄的起始者區段的標頭標籤。標籤元素包括一個 **blade** 參數，來識別負責事件的 Tivoli Access Manager blade。
<component>	標籤識別已攫取審核記錄的元件。元件會以這種格式記錄： wpi.*virtual_host_name.type_of_event.module_name*

表 6. 鑑定審核記錄欄位定義。 (繼續)

XML 標籤	說明
<action>	識別已嘗試的鑑定方法。動作碼及其對應的鑑定機制如下： 16961 - BA 17236 - 用戶端憑證 17731 - Ecsso 17999 - 失效接替 cookie 17997 - 套表 18504 - Http 標頭 18768 - IP 位址 4806211 - IV 標頭：PAC 證明 4806229 - IV 標頭：使用者名稱 4806220 - IV 標頭：識別名稱 300609 - IV 標頭：IP 位址 21579 - 記號
<location>	定義起始事件的伺服器名稱。
<accessor>	審核記錄的存取者 (accessor) 區段的標頭標籤。標籤元素可以包括存取者的名稱。
<主體>	主體標籤包括參數 **auth**，來識別鑑定目錄服務。標籤定義已驗證的使用者名稱。
<target>	目標標籤包括可以是下列其中一值的參數 **resource**： • 0 = 授權 • 1 = 處理 • 2 = TCB • 3 = 證明 • 4 = 一般 鑑定審核記錄永遠都會將這個值設爲 3 - 證明。
<object>	保留與鑑定處理程序稍有相關的審核資料。
<data>	額外的鑑定失敗資訊。例如，在使用 HTTP 標頭資訊進行鑑定嘗試期間若失敗，將導致審核日誌記錄，將失敗的 HTTP 標頭記錄在這個欄位中。

審核配置

下表顯示審核配置參數及說明其函數。

表 7. 審核配置參數定義

參數	說明
logsize	日誌檔轉換至新檔案的大小（以位元組爲單位）。如果設爲 0，日誌檔將不會轉換。負數將每天轉換日誌，不管其大小爲何。
logflush	清除日誌的間隔（以秒爲單位）。最多 6 小時，預設值是 20 秒。
logaudit	啓用或停用審核。
auditlog	指定審核檔案的名稱。
auditcfg	啓用或停用授權及/或鑑定審核。

例如：

```
[aznapi-configuration]
logsize = 2000000logflush = 20logaudit = no
auditlog = audit.log
auditcfg = azn
#auditcfg = authn
auditcfg = wpi
```

追蹤外掛程式動作

Tivoli Access Manager Plug-in for Web Servers 會基於除錯的目的，提供追蹤動作並將結果儲存在檔案的能力。追蹤主要是分析及問題診斷工具，被應用程式支援用來取得導致錯誤之動作的完整檢視。作爲使用者的您可能會發現部份外掛程式追蹤機能很有用，但是大部份機能的用處不大，除非您正在診斷複雜的問題。

在外掛程式中追蹤 HTTP 訊息是可能的。這可能非常有用，因爲它會完全地顯示從使用者收到的資料，以及傳回給使用者的資料 - 即使通訊是透過 HTTPS，也是一樣。追蹤是使用標準 **pdadmin** 追蹤指令來開啓及關閉。

pdadmin 追蹤指令

列示追蹤元件

list 指令會產生一個清單，列出所有可以追蹤的外掛程式動作。

語法：

```
pdadmin> server task PDWebPI-server-name trace list [component]
```

所列出的大部份追蹤作業都是 Tivoli Access Manager 特有的。外掛程式特有的追蹤項目是以 **pdwebpi** 爲字首。

設定追蹤元件

有兩個您可能發現有助於除錯的主要追蹤項目：

- pdwebpi.request
- pdwebpi.plugin

pdwebpi.request 設爲 2，來追蹤每一個透過外掛程式傳送的要求。當 **pdwebpi.request** 設爲 9 時，要求標頭將併入在追蹤中。**pdwebpi.plugin** 會在外掛程式伺服器中啓動追蹤。所有訊息都會傳送至 Web 伺服器的日誌檔，在 IIS 的情況中，則傳送至不同於針對 Authorization Server 使用之日誌的日誌。

trace **set** 指令具有下列語法：

```
pdadmin> server task PDWebPI-server-name trace set component
 level [file path=file|other-log-agent-config]
```

其中 *component* 是 list 指令所顯示的追蹤元件的名稱。追蹤是針對這個元件而設定的。*層次*是針對追蹤而收集的明細數量。範圍爲 1 到 9。1 是最不詳細，9 是最詳細。選用的 **file path** 參數指定追蹤輸出的位置。根據預設值，追蹤輸出將傳送至標準配置的外掛程式日誌檔（使用元件 **pdwebpi.plugin** 時除外）。對於 IIS 安裝，永遠都在配置檔中 **[iis]** 段落下使用 **log-file** 參數來配置外掛程式元件追蹤將傳送至的檔名。

您可以使用 **-foreground** 選項，將輸出傳送至螢幕。亦即：

```
pdwebpi -foreground
```

顯示追蹤元件

若要顯示追蹤元件，請以下列格式使用 **show** 指令：

```
pdadmin> server task PDWebPI-server-name trace show [component]
```

快取資料庫設定

您可以配置外掛程式定期輪詢主要授權資料庫，以便了解是否有更新資訊。**cache-refresh-interval** 參數可以設爲 ″default″、″disable″ 或特定的間隔（以秒爲單位）。預設設定是 **disable**。

```
[aznapi-configuration]
cache-refresh-interval = 60
```

db-file 參數定義 ACL 快取資料庫的完整路徑。根據預設值，不設定這個參數。

```
[aznapi-configuration]
db-file = /var/pdwebpi/db/pdwebpi.db
```

listen-flags 參數啓用或停用原則快取更新通知的接收。″disable″ 值會停用通知接收器。這個參數是 `svrsslcfg` 公用程式設定的。

```
[aznapi-configuration]
listen-flags = disable
```

配置授權 API 服務

`pdwebpi.conf` 配置檔的 **[aznapi-entitlement-services]** 段落會指定服務 ID 給服務。每一個段落項目定義不同類型的 aznAPI 服務。如需相關資訊，請參閱 *IBM Tivoli Access Manager Administration C API Developer's Reference*。

每一個項目都具有這樣的格式：

```
service_id = path_to_dll [ & params ... ]
```

服務 ID 是被 aznAPI 用戶端用來識別服務。您可以指定當 aznAPI 起始設定服務時，要傳送給這個服務的參數。參數是在項目中 ″&″ 符號之後。

語言支援

Tivoli Access Manager Plug-in for Web Servers 可以用客戶偏好的語言顯示 Tivoli Access Manager 產生的 HTML 頁面。用於顯示在 HTML 頁面的語言是取自於 HTTP 要求內找到的 *Accept-Language* 標頭。語言值是以兩個字元代表。位置特有的值是以兩個部份格式來表示，分別指出語言以及使用這個語言版本的國家或地區。範例包括：

- es（西班牙文）
- de（德文）
- en（英文）
- it（義大利文）
- en-US（美式英文）
- en-GR（英式英文）
- es-ES（西班牙文/西班牙）
- es-MX（西班牙文/墨西哥）
- pt-BR (葡萄牙文/巴西）

如果外掛程式在 HTTP 要求中找不到適當的語言碼，它會重新嘗試語言清單，不限定方言（如 es-MX 會當作 es 來重試）。如果仍然找不到適當的語言，伺服器將使用英文。

僅有 Tivoli Access Manager 產生的頁面，包含在 *install directory*/nls/html/*lang* 內，才有多語言服務。這些頁面的範例包括所有 Tivoli Access Manager 鑑定套表，以及 Tivoli Access Manager 帳戶管理頁面。

在 HTTP 標頭中的*接受語言*欄位內指定的語言會直接對映至 *install directory*/nls/html 目錄內找到的目錄。您可以複製語言目錄，來修改伺服器，以顧及語言指定程式變量。若要修改伺服器，應該複製的眞正語言目錄是：

am base install directory/nls/msg/*lang*
am webpi install directory/nls/html/*lang*
am webpi install directory/nls/msg/*lang*

下表列出外掛程式支援的語言，以及相關聯的子目錄名稱：

表 8. 外掛程式支援的語言，以及支援的目錄。

語言	系統目錄
英文（預設值）	C
捷克文	cs
德文	de
西班牙文	es
法文	fr
匈牙利文	hu
義大利文	it
日文	ja
韓文	ko
波蘭文	pl
葡萄牙文，巴西	pt_BR
俄文	ru
中文，中國	zh_CN
中文，台灣	zh_TW

最多可在 HTTP 標頭的*接受語言*欄位中辨識 10 種語言規格。

第 4 章 IBM Tivoli Access Manager Plug-in for Web Servers 鑑定

本章討論 IBM Tivoli Access Manager (Tivoli Access Manager) Plug-in for Web Servers 如何維護階段作業狀態、處理鑑定處理程序，以及對已授權階段作業執行任何必要的後置授權處理程序。

主題索引：

鑑定處理程序

鑑定是識別試圖登入安全網域之個別處理程序或實體的方法。 順利完成鑑定會產生代表使用者的 Tivoli Access Manager 身份。外掛程式會使用這個身份來取得該使用者的證明。授權服務程式在評估掌控每一個物件之原則的 ACL 許可權和 POP 條件之後，使用這些證明來允許或拒絕對受保護資源的存取權限。

註: ACL = 存取控制清單原則
POP = 受保護的物件原則

Tivoli Access Manager Plug-in for Web Servers 預設支援數種鑑定方法，並可被自訂來使用其他方法。

在鑑定期間，外掛程式會檢查用戶端要求，以取得下列資訊：

- **虛擬主機資訊**

  要求將導向至其中的虛擬主機身份是從 Web 伺服器決定的。 Authorization Server 會使用虛擬主機資訊，來識別定址的虛擬主機，以及比對要求與 Tivoli Access Manager 原則資訊。

- **階段作業資料**

  階段作業資料是用來在用戶端和外掛程式伺服器間識別特定連線的資訊。階段作業資料是從要求的內容決定的。資料是用來重新識別傳送至外掛程式伺服器的用戶端階段作業，以及避免爲每一個要求建立新階段作業時所產生的負擔。階段作業資料的範例是「SSL 階段作業 ID」，或階段作業 cookie 中的值。

  它是從要求擷取階段作業資料的階段作業模組，這些模組會使用階段作業資料當作索引，在階段作業快取記憶體中儲存/擷取階段作業資訊（例如，使用者證明）。

- **鑑定資料**

  鑑定資料是來自用戶端而讓外掛程式識別用戶端的資訊。鑑定資料類型包含了用戶端憑證、密碼以及記號碼。

  鑑定模組可以執行兩個函數。它們會從要求擷取鑑定資訊並驗證它。鑑定資訊可能是來自套表的使用者 ID/密碼資訊，或是來自 X.509 憑證的 DN。模組也許能夠產生鑑定暗號，可透過外掛程式傳回給一般使用者。並非所有鑑定模組都可以產生暗號。

- **後置授權資料**

  某些進入要求可能是針對需要不同於正常情況之處理程序的 URI。後置授權處理程序會處理需要特殊鑑定方法的要求。這個處理程序通常會重新導向到設計來鑑定此類要求的特殊處理程序。後置授權模組是用來提供這些額外的函數。在授權要求後，將呼叫這些模組，然後就有機會來指示外掛程式，修改要求或回應。後置授權模組可能會新增「IV 標頭」至要求，以達成單一登入，或它們可能截取特殊 URL，並開始特定的處理程序。

對於到達 Web 伺服器的每一個要求，外掛程式會判定要求所針對的虛擬主機，並判定是否要配置虛擬主機來進行保護。

未配置來進行保護之虛擬主機的要求容許通過，不需進一步處理。對於配置來進行保護之虛擬主機的要求，外掛程式會判定做出要求之使用者的身份。可能的話，使用者的識別是使用要求內的資料來執行，此資料可能是已指定證明之現有階段作業的一部份。在這種情況中，可以使用現有的證明來執行授權。如果沒有呈現證明，將授與要求**未經鑑定**證明。

如果已授權要求，則 Authorization Server 會判定是否需要修改要求或回應。這個處理程序是由後置授權模組所執行，這些模組會執行如新增標頭或 cookie 至要求，或將使用者重新導向至適當頁面等作業。如果未使用現行證明來授權要求，則 proxy 會嘗試在要求中使用鑑定資訊（例如，BA 標頭）來建置新的證明。如果成功，則這個鑑定資訊可以用來重新嘗試授權。如果沒有鑑定資訊，則 proxy 將嘗試對外掛程式建置一個鑑定暗號回應。如果不可能送給使用者一個鑑定暗號，將傳回禁止存取的頁面。

下列流程圖顯示針對處理要求做出的決策。

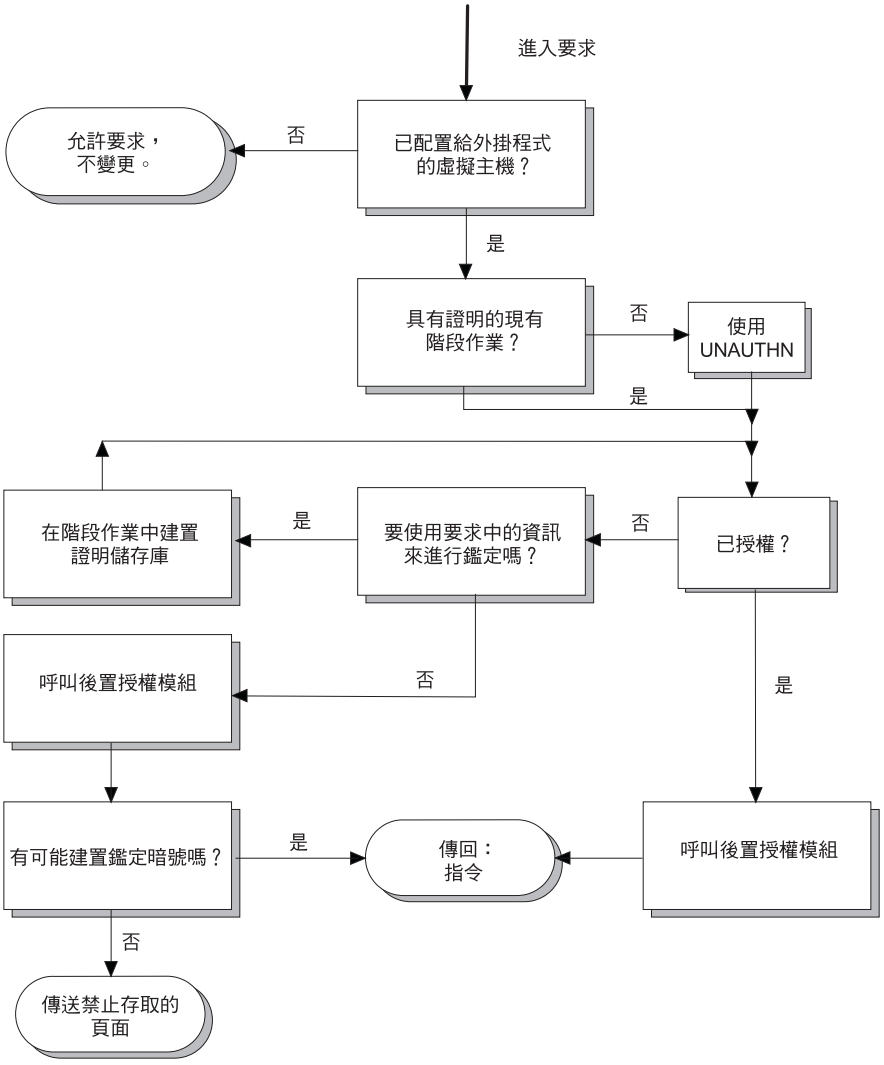

圖 2. Web 伺服器存取決策。

配置鑑定

所有可用的鑑定方法及其相關聯的共用程式庫名稱都定義在 pdwebpi.conf 配置檔的 **[modules]** 段落中。 **[modules]** 段落也會列示針對階段作業識別及後置授權處理而使用的模組。稍後將說明這些模組。共用程式庫必須存在於 pdwebpi/lib 目錄中。指定共用程式庫名稱時，沒有任何作業系統特有的字首（如 lib），以及任何作業系統特有的字尾（如 dll）。例如：

```
BA = pdwpi-ba-module
```

在前述範例中，已給與 BA 模組程式庫作爲 pdwpi-ba-module。在 Windows 上，外掛程式會尋找一個稱爲 pdwpi-ba-module.dll 的檔案，在 Solaris 上，它將尋找一個稱爲 libpdwpi-ba-module.so 的檔案，以及在 AIX 上，它將尋找一個稱爲 libpdwpi-ba-module.a 的檔案。

註: 程式庫檔案的預設搜尋路徑的替代路徑可以定義在 **[module-mgr]** 段落中。

每一個定義在 **[modules]** 段落中的標籤都具有它自己對應的段落，例如，**[BA]**、**[cert]** 及 **[token]**。每一個鑑定方法的特定配置資訊都是在這些段落中指定的，並且套用至該鑑定方法，與從哪一個虛擬主機呼叫它無關。如果每一個虛擬主機都需要特殊配置，則可以使用以虛擬主機標籤定義模組標籤的段落，來置換預設配置。例如：

```
[BA]
basic-auth-realm = "Access Manager"

[BA:ibm.com]
basic-auth-realm = "ibm.com"
```

在上面範例中，使用「基本鑑定」存取虛擬主機 ibm.com 的使用者將受到段落 **[BA:ibm.com]** 中指定的配置參數來支配。

模組的標準配置僅允許一個模組程式庫實例指定給一個指定的鑑定方法，例如：

```
[modules]
BA = pdwpi-ba-module
```

部份安裝作業可能需要指定多個鑑定程式庫實例。當不同的鑑定層次需要不同的模組行爲時，情況可能就是如此。下列範例顯示兩個套表鑑定模組實例的配置。

```
[modules]
ba = pdwpi-ba-module
forms-authn-level1 = pdwpi-forms-module
forms-authn-level2 = pdwpi-forms-module

[common-modules]
authentication = forms-authn-level1
authentication = forms-authn-level2
authentication = BA

[forms-authn-level1]
login-form = level1-form

[forms-authn-level2]
login-form = level2-form

[BA]
...
```

配置鑑定方法的最後一個步驟就是指定鑑定方法。這些都是按它們的偏好次序，設定在配置檔的 **[common-modules]** 段落中。例如：

```
[common-modules]
session = ssl-id
session = BA
session = session-cookie

authentication = cert
authentication = BA

post-authzn = ltpa
```

在上面範例中，配置設定確定：

- SSL 階段作業 ID 是用來維護作爲首選的階段作業資訊。
- 當 SSL 階段作業 ID 無法使用時，BA 標頭（如果可用的話）是用來維護階段作業資訊。

- 當 SSL 階段作業 ID 及 BA 標頭無法使用時，階段作業 cookie 將作爲維護階段作業資訊的最後手段。
- 憑證是作爲首選的鑑定方法。
- 當憑證無法使用時，將使用 BA 進行鑑定。
- LTPA cookie 將新增至要求，作爲後置授權處理程序的一部份。

配置虛擬主機的鑑定

您可以直接在每一個虛擬主機段落中指定方法，來達成鑑定方法的配置。例如：

```
[pdweb-plugins]
virtual-host = ibm.com

[ibm.com]
....
session = ssl-id
session = BA
session = session-cookie

authentication = cert
authentication = BA

post-authzn = ltpa
```

指定虛擬主機之鑑定方法的替代方法就是爲鑑定方法配置定義一個段落。如此將容許多個虛擬主機共用模組配置。模組配置段落是由虛擬主機段落中的 **modules** 參數加以指定。例如：

```
[pdweb-plugins]
virtual-host = ibm.com
virtual-host = lotus.com

[ibm.com]
modules = ibm-lotus-module-stanza

[lotus.com]
modules = ibm-lotus-module-stanza

[ibm-lotus-module-stanza]
authentication = ba
session = ba
post-authzn = ltpa
```

當每一虛擬主機上鑑定方法配置的個別段落未定義在配置檔時，所有虛擬主機都會使用 **[common-modules]** 段落中配置的參數；亦即，**modules** 參數的預設值是 *common modules*。

下列範例設定一個稱爲 ibm.com 的虛擬主機，它會在適當之處使用 SSL 階段作業 ID、在無法使用 SSL ID 之處使用 BA 標頭，以及具有 BA 標頭，然後使用階段作業 cookie，作爲維護階段作業資訊的最後手段。它支援在基本鑑定之前的憑證鑑定，並在鑑定成功時，新增 LTPA cookie 至要由 Web 伺服器處理的要求。此範例僅顯示這裡定義的參數。

```
[pdweb-plugins]
virtual-host = ibm.com

[modules]
ssl-id = pdwpi-ssl-id
session-cookie = pdwpi-session-cookie
ba = pdwpi-ba
cert = pdwpi-cert
```

```
ltpa = pdwpi-ltpa

[ibm.com]
session = ssl-id
session = ba
session = session-cookie

authenitcation = cert

post-authzn = ltpa
```

您可以建立虛擬主機特有的鑑定配置段落，來依照每一虛擬主機達成鑑定參數的進一步配置。底下的範例顯示這兩個虛擬配置：ibm.com 及 lotus.com。每一個虛擬主機都有模組特有的鑑定配置。

```
[pdweb-plugins]
virtual-host = ibm.com
virtual-host = lotus.com

[modules]
...

[ibm.com]
session = ba
session = session-cookie

authenitcation = ba
authentication = forms

[lotus.com]
session = session-cookie

authenitcation = ba
authentication = cert

[BA:ibm.com]
basic-auth-realm = "Access Manager - ibm.com"

[BA:lotus.com]
basic-auth-realm = "Access Manager - lotus.com"
```

配置鑑定方法的次序

已配置的鑑定方法顯示在配置檔中的次序是正確操作外掛程式軟體所不可缺的。您需要以免於失敗並達成安全目標的方法，來仔細考慮並實作您選擇的鑑定方法類型。

Tivoli Access Manager Plug-in for Web Servers 以可以基於不同安全需求來調整，以符合不同客戶需求的方法，支援各種鑑定方法。

如同在本文件的前幾節中所看到的一般，pdwebpi.conf 配置檔的 **[common-modules]** 段落是您指定要使用之鑑定方法的位置。配置檔的 **[authentication-levels]** 段落定義設定鑑定層次（請參閱 第 80 頁的『鑑定強度的受保護的物件原則（進階）』），以及排序 **[common-modules]** 段落中所配置的鑑定方法。

在 **[authentication-levels]** 段落中沒有定義任何項目給鑑定方法時，它會預設爲層次 1。接著，鑑定次序會判定爲由最高鑑定層次，向下至 **[authentication-levels]** 段落中已定義的鑑定方法的最低鑑定層次。如果數個模組共用一個鑑定層次，則子次序將由模組出現在 **[common-modules]** 段落內的次序來加以決定。

若要瞭解外掛程式鑑定，請考慮外掛程式如何回答它所處理的每一個要求的兩個問題，這是很有用的：

1. 我可以使用已配置的鑑定方法來鑑定這個要求嗎？

   如果這個問題的答案爲否，外掛程式將要求下一個問題。
2. 我可以使用已配置的鑑定方法來產生一個鑑定要求嗎？

請考慮下列配置。

```
[common-modules]
authentication = BA
```

對於進入要求，如果 ACL 不允許未經鑑定的使用者，將需要鑑定使用者。將 BA 看成唯一已配置的鑑定方法的外掛程式會問「我可以使用基本鑑定來鑑定這個要求嗎？」。如果要求是新的，則答案爲否—外掛程式不認識這個使用者。接著，外掛程式會問「我可以使用基本鑑定來產生鑑定要求嗎？」。如果已正確地配置基本鑑定，則答案爲是。外掛程式將提示使用者輸入 ID 及密碼。

這是使用「基本鑑定」進行鑑定的簡單範例。您可能想要配置多個鑑定方法，視您物件空間的安全需求而定。

底下是外掛程式用來給與特殊鑑定方法優先順序之邏輯的更詳細範例。

下列幾個段落中所討論的邏輯假設不允許未經鑑定的使用者存取資源，以及假設已對 pdwebpi.conf 配置檔做了下列配置。

```
[common-modules]
authentication = BA
authentication = failover
authentication = forms

post-authzn = failover

[authentication-levels]
1 = BA
2 = failover
```

之前的配置指定三種鑑定方法：BA、失效接替 cookie 及含失效接替 cookie 的套表，來進行後置授權處理程序。 **[authentication-levels]** 段落中設定的層次決定將呼叫哪一種鑑定方法來鑑定要求。套表鑑定的層次將預設爲 1，因爲在 **[authentication-levels]** 段落沒有定義任何層次給它。

在接收要求時，外掛程式會使用上面的配置在要求標頭中尋找失效接替 cookie。外掛程式會在尋找 BA 資料之前，先尋找失效接替 cookie，因爲在 **[authentication-levels]** 段落中，失效接替已指定在層次 2。**[authentication-levels]** 段落比 **[common-modules]** 段落中鑑定模組定義的次序更具優先順序。

外掛程式會問「我可以使用失效接替 cookie 來鑑定這個要求嗎？」。如果先前並未鑑定要求，則答案爲否，因爲外掛程式先前並未建構要求的失效接替 cookie。接著，外掛程式會問「我可以使用失效接替 cookie 來產生鑑定要求嗎？」。答案爲否，因爲失效接替 cookie 模組沒有產生要求來進行鑑定的方法。

外掛程式會移至 **[authentication-levels]** 段落中下一個配置的鑑定方法，亦即範例中的 BA。外掛程式會問「我可以使用 BA 標頭來鑑定這個要求嗎？」。答案是否，因爲先前並未鑑定要求。接著，外掛程式會問「我可以使用 BA 來產生鑑定要求嗎？」。答案可能爲是，而且將提示使用者輸入使用者 ID 及密碼。成功的鑑定會產生一個已獲授權的階段作業，而且有一個失效接替 cookie 會插入要求標頭，作爲同一階段作業期間後續要求的第一個鑑定方法。

萬一 BA 模組無法產生一個鑑定使用者的方法，外掛程式將預設爲配置檔的 **[common-modules]** 段落中所列示的方法排序。在上面的配置範例中，外掛程式將指定鑑定方法的優先順序，因此次序爲：

level 1 = BA, 套表
level 2 = 失效接替 cookie

如果失效接替 cookie 及 BA 無法提供使用者鑑定方法，則外掛程式將使用套表來鑑定使用者。

底下的流程圖顯示用來選取鑑定模組的外掛程式邏輯。

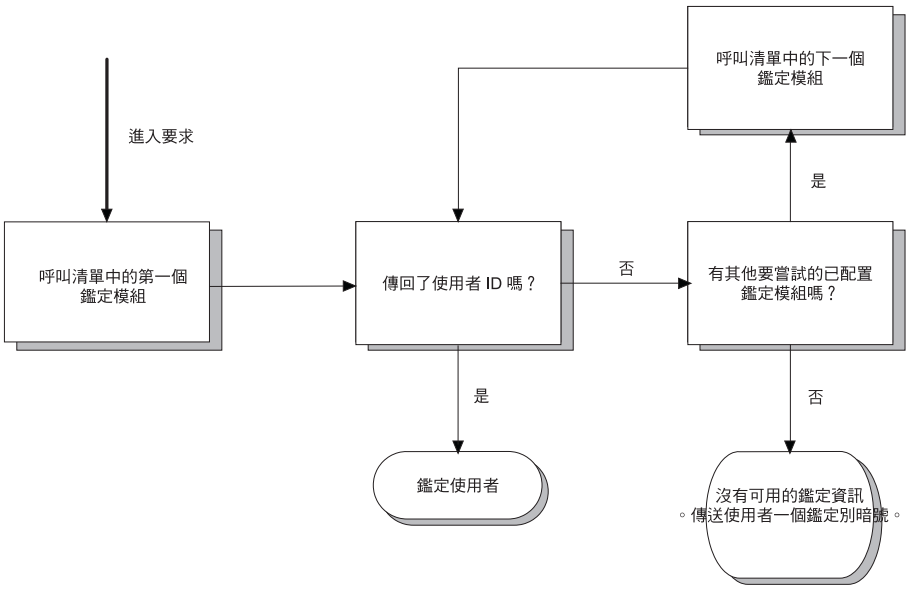

圖 3. 決定鑑定模組的外掛程式處理流程。

外掛程式會按它的配置次序來呼叫每一個鑑定模組，直到其中一個模組傳回使用者的證明爲止。如果沒有一個已配置的鑑定模組能夠產生證明，則鑑定暗號會傳送至使用者，以提示他們提供鑑定資訊。

如果需要鑑定暗號，將呼叫來自已配置清單之第一個適合的鑑定模組，來產生所需的指令以產生暗號。並非所有鑑定模組都可以產生暗號。例如，沒有要求「HTTP 標頭」的暗號 — 這些不是呈現在要求中，就是根本不存在。此外，鑑定模組可能無法使用，因爲它已用來識別正要轉遞要求至外掛程式的 proxy 代理站。可爲使用者產生暗號的最常用鑑定機制就是「基本鑑定」（有一個 BA 暗號會傳送至使用者），以及套表型鑑定（有一個登入套表會傳送至使用者）。如果沒有可用的鑑定方法，將無法鑑定使用者，而且外掛程式將傳回禁止存取的頁面。

圖 4 中的流程圖顯示選取一個鑑定方法來傳送暗號至使用者的處理程序。

每一個已配置的鑑定方法都會按它的配置次序來加以檢查，直到找到其中一個鑑定方法滿足所需的鑑定層次爲止。如果找到一個滿足鑑定準則的模組，將呼叫它以建立要傳送至使用者的暗號。如果已配置的鑑定方法都不適合，則可能不進行任何鑑定。外掛程式會傳回「禁止存取」頁面給使用者，因爲使用者沒有必要的許可權，來存取所要求的資源，而且也不可能傳送他們一個要在必要層次鑑定的暗號。

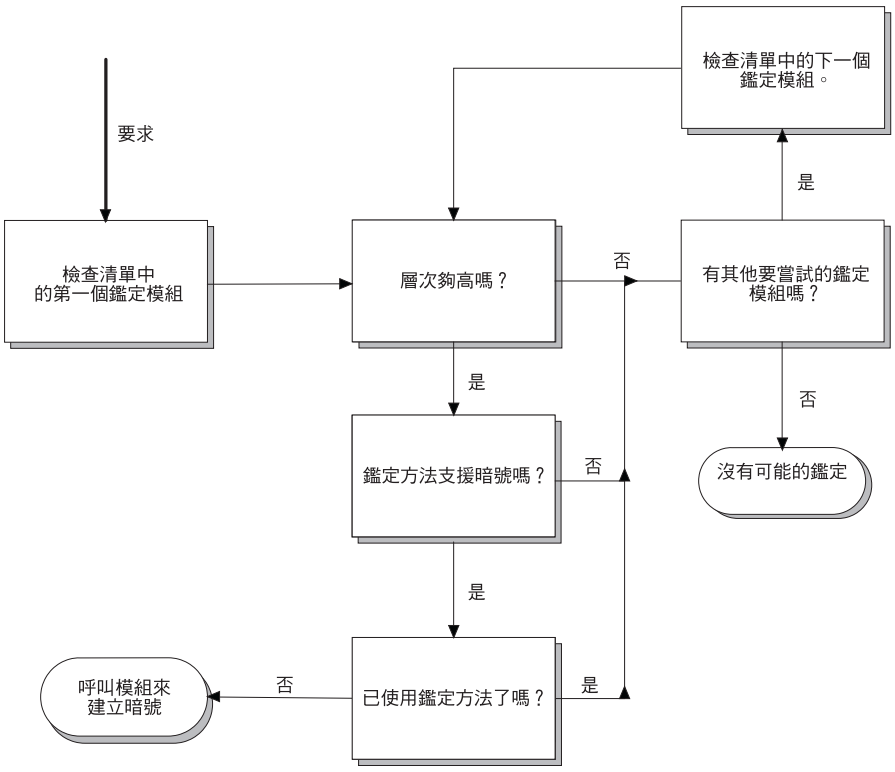

圖 4. 鑑定暗號處理邏輯。

配置後置授權處理程序

在要求獲得授權後，將呼叫已配置的後置授權模組。後置授權模組會決定在要求傳回給外掛程式，以供 Web 伺服器處理之前，是否需要採取任何其他動作。所有已配置的後置授權模組將被呼叫，以決定是否有需要對要求採取動作。

「後置授權」模組可以分類爲：

- **修改 SSO 的要求** — 這些後置授權模組會新增 Web 應用程式所使用的資訊（cookie 或標頭)，以識別不需要第二個鑑定的使用者。
- **修改回應** — 這些後置授權模組通常會藉由加入標頭或 cookie，來修改回應。例如，失效接替模組會新增失效接替 cookie 至回應。
- **特殊函數** — 這些後置授權模組會辨識被要求作爲部份特殊函數之觸發程式的 URI。特殊函數指出外掛程式會處理要求。範例爲 eCSSO「擔保」要求。

後置授權模組會按它們出現在配置檔的次序來加以呼叫。在清單中「較後」指定的後置授權模組能夠還原或覆寫先前的後置授權模組所做的變更。

例如，下列配置檔將導致不同的外掛程式行爲，視 *BA* 及 *討表* 在 **[common-modules]** 段落中指定的次序而定。

```
[common-modules]
...
post-authzn = BA
post-authzn = 套表
```

```
[BA]
...
strip-hdr = always

[forms]
...
create-ba-hdr = yes
```

上面的配置是一個簡單的範例，它指出透過後置授權模組及模組配置的排序，可以達成多大的彈性。

管理階段作業狀態

外掛程式會使用階段作業狀態資訊來識別進入要求的來源。當用戶端在一個階段作業內執行許多要求時，外掛程式就會使用要求來源的身份，來維護用戶端與伺服器之間階段作業狀態。若用戶端和伺服器之間未建立階段作業狀態，用戶端和伺服器間必須針對所有後續要求進行通訊上的協調。 階段作業狀態資訊可以改進效能，因爲它會消除重複鑑定的需求。用戶端可以登入一次然後進行多次要求，而不需要針對每個要求進行另外的登入。

Tivoli Access Manager Plug-in for Web Servers 可同時處理 HTTP 及 HTTPS 通訊。外掛程式的設計是使用以下任何資訊類型來維護用戶端的階段作業狀態：

1. SSL 階段作業 ID
2. 基本鑑定
3. 伺服器特有的階段作業 cookie
4. HTTP 標頭資料
5. IP 位址
6. LTPA cookie
7. IV 標頭
8. SPNEGO

外掛程式會輪流呼叫每一個已配置的階段作業模組。外掛程式會繼續搜尋已配置的階段作業模組類型，直到有一個傳回證明爲止。然後，外掛程式會判定應用程式是否參照「多工 Proxy 代理站」。如果它是「Proxy 代理站」，則眞正一般使用者的另一個階段作業必須存在。爲了尋找這個其他階段作業，外掛程式會繼續呼叫已配置之階段作業模組的其餘部份。當找到已發生使用者鑑定的現有階段作業時，將傳回使用者證明。這個證明是用來授權要求。如果沒有任何已配置的階段作業模組傳回使用者證

明，則階段作業是新的，或是沒有建立證明的階段作業。

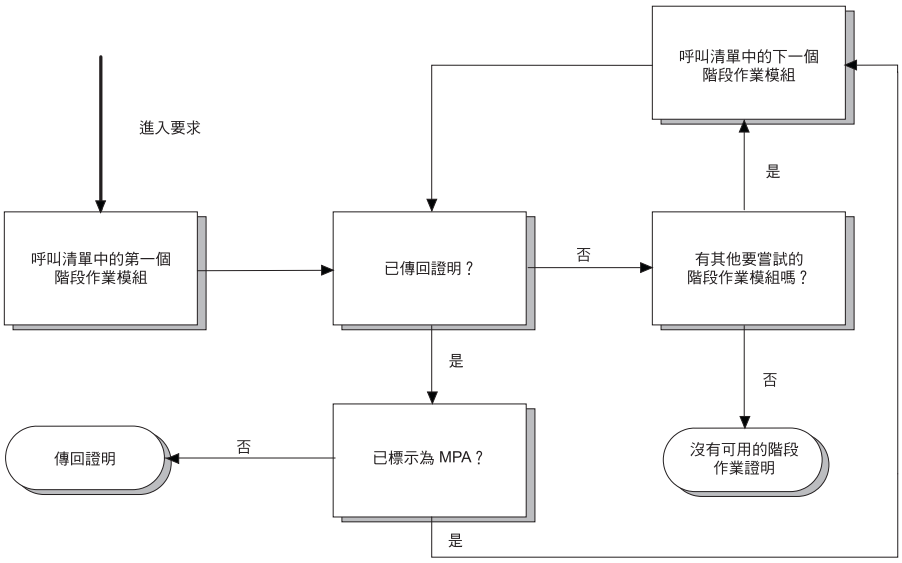

圖 5. 決定階段作業模組的外掛程式處理流程。

配置外掛程式階段作業/證明快取

外掛程式階段作業快取可讓伺服器儲存來自多個用戶端的階段作業 ID 資訊。階段作業快取可以同時容納 HTTPS 及 HTTP 階段作業狀態資訊。

外掛程式快取儲存階段作業 ID 資訊，以及針對每一個用戶端取得的證明資訊。證明資訊會被暫存在快取中，以避免在授權檢查時重複查詢使用者登錄資料庫。外掛程式快取也會維護外掛程式與 LDAP 使用者登錄之間 SSL 連線的階段作業狀態資訊。

外掛程式快取都有數種可用的配置參數，可讓您調整快取的效能。

註: 在 pdwebpi.conf 配置檔的 **[sessions]** 段落中配置的值可在 **[***module_name***]** 段落中加以置換，而且有些值可以依照每一虛擬主機而在 **[***module_name:virtual_host_name***]** 段落中進一步的置換。

設定並行項目數上限值

位於 pdwebpi.conf 配置檔的 **[sessions]** 段落的 **max-entries** 參數，可設定每一個階段作業模組的階段作業/證明快取中的並行項目數上限。

此值對應於特殊階段作業模組的並行登入階段作業數目。當快取大小到達此值時，則會根據最近最少使用的演算法，從快取移除項目，以便接受新的進入登入。

並行登入階段作業的預設數目爲 4096：

```
[sessions]
max-entries = 4096
```

設定快取項目逾時值

位於 pdwebpi.conf 配置檔的 **[sessions]** 段落的 **timeout** 參數，可設定外掛程式階段作業/證明快取中項目的生命週期逾時上限。

外掛程式會在內部快取證明資訊。階段作業快取逾時參數指定保留在記憶體中的授權證明資訊之時間長度。

此參數不是停止活動逾時。 值會對映至「證明生命週期」而不是「證明逾時」。其目的在於提升安全性，其方法是在到達指定的逾時限制時，強制使用者重新鑑定。

預設登入階段作業逾時（以秒爲單位）爲 3600：

```
[sessions]
timeout = 3600
```

您可以配置在每次發生重新鑑定時重設階段作業快取生命週期。每次發生重新鑑定時，階段作業快取**逾時**值即會重設。若要配置階段作業快取生命週期重設，請在 pdwebpi.conf 配置檔的 **[sessions]** 段落中使用 **reauth-lifetime-reset** 參數：

```
[sessions]
reauth-lifetime-reset = yes
```

預設值是 *NO*。

當使用者正在執行重新鑑定時，有可能讓階段作業快取生命週期值到期。在重新鑑定登入套表傳送給使用者之後，並在傳回完成的登入套表之前，階段作業快取生命週期可能會到期。當階段作業快取生命週期值到期時，即會刪除階段作業快取項目。當登入套表傳回外掛程式時，不再有該使用者的階段作業。此外，所有快取的使用者要求資料也會遺失。如果在重新鑑定期間，階段作業快取生命週期到期，則可以爲階段作業快取生命週期配置時間展延或「寬限期」。

pdwebpi.conf 配置檔的 **[sessions]** 段落中的 **reauth-grace-period** 參數提供此時間展延（以秒爲單位)。例如：

```
[reauthentication]
reauth-grace-period = 20
```

預設值 *0* 不提供階段作業快取逾時值展延。 **reauth-grace-period** 參數適用具有現存的階段作業快取項目而且需要重新鑑定的使用者。例如：

- 因爲 POP 安全原則而執行重新鑑定的使用者
- 因爲階段作業快取無活動而執行重新鑑定的使用者
- 執行進階鑑定的使用者

reauth-grace-period 選項通常會配合 **reauth-lifetime-reset** = *yes* 選項使用。

設定快取項目無活動逾時值

inactive-timeout 參數（位於 pdwebpi.conf 配置檔的 **[sessions]** 段落中）可設定登入階段作業無活動的逾時值。

預設登入階段作業無活動逾時（以秒爲單位）爲 600：

```
[sessions]
inactive-timeout = 600
```

若要停用此逾時功能，請將參數值設定爲 *0*。

利用 SSL 階段作業 ID 維護階段作業狀態

Tivoli Access Manager Plug-in for Web Servers 可以利用進入的 HTTPS 要求的 SSL 階段作業 ID，來追蹤階段作業。這種機能不能在 IIS 上使用，因爲 IIS 不會讓外掛程式使用 SSL 階段作業 ID。

註: SSL 階段作業 ID 不是針對鑑定要求而使用的。

pdwebpi.conf 配置檔中的 **[common-modules]** 段落定義如何利用格式 *module_type* = *module-name*，來使用所有階段作業、鑑定及後置授權方法。若要使用 SSL 階段作業 ID 來維護階段作業狀態，請指定 **ssl-id** 一字給 **session** 參數，如下所示：

```
[common-modules]
session = ssl-id
```

確定已在 pdwebpi.conf 配置檔的 **[modules]** 段落配置了 ssl-id 的共用程式庫。亦即：

```
[modules]
ssl-id = pdwpi-sslsessid-module
```

利用基本鑑定來維護階段作業狀態

「基本鑑定 (BA)」是透過輸入使用者名稱及密碼，來鑑定使用者及維護階段作業狀態的方法。 BA 是由 HTTP 通訊協定所定義，並可透過 HTTP 及 HTTPS 實作。

「基本鑑定」是藉由快取「基本鑑定」標頭的內容記錄來維護階段作業狀態。

若要配置外掛程式，以利用「基本鑑定」來維護階段作業狀態，請在 pdwebpi.conf 配置檔中使用 **[common-modules]** 段落。將參數 **session** 輸入爲值 *BA*，如下所示：

```
[common-modules]
session = BA
```

如果 BA 是用來維護階段作業狀態，則也需要使用它來進行使用者鑑定。配置檔的 **[common modules]** 段落也應該爲鑑定設定 BA。

```
[common-modules]
session = BA
authentication = BA
```

利用階段作業 Cookie 來維護階段作業狀態

使用階段作業 cookie 來保留階段作業資訊是一種維護外掛程式階段作業狀態的方法。伺服器先將特定用戶端的狀態資訊封裝在 cookie 中，然後傳送給用戶端的瀏覽器。 針對每一個新的要求，瀏覽器都會將該 cookie（含有階段作業 ID）傳回給伺服器，以便重新識別自身。

當用戶端的瀏覽器會在很短的時間間隔內，重新協議其 SSL 階段作業時，階段作業 Cookie 可以爲此狀況提供可能的解決方案。 例如，某些版本的 Microsoft Internet Explorer 瀏覽器會每隔兩或三分鐘即重新協議 SSL 階段作業。

階段作業 cookie 僅對用戶端已在一個短暫時段內（大約 10 分鐘）鑑定的伺服器，提供用戶端的重新鑑定。此機制是基於一個「伺服器 cookie」無法傳送至產生該 cookie 之機器以外的機器。

此外，階段作業 cookie 包含一個亂數 ID，其用來製成伺服器階段作業快取中 cookie 的索引 —沒有其他資訊會外曝在階段作業 cookie 中。階段作業 cookie 不會危及安全原則。

Tivoli Access Manager Plug-in for Web Servers 使用安全伺服器特有的階段作業 cookie。下列條件適用於此 cookie 機制：

- Cookie 僅包含階段作業資訊；它並不包含身份資訊。
- Cookie 只位在瀏覽器記憶體中（不會寫入磁碟上的瀏覽器 cookie jar）。
- Cookie 具有一個有限的生命週期（可配置）。
- Cookie 具有路徑和網域參數，可禁止被其他伺服器使用。

若要配置外掛程式，使用階段作業 cookie 來維護階段作業狀態，請在 pdwebpi.conf 配置檔中使用 **[common-modules]** 段落。將參數 **session** 輸入爲值 *session-cookie*，如下所示：

```
[common-modules]
session = session-cookie
```

resend-pdwebpi-cookies 參數（位於 pdwebpi.conf 配置檔的 **[sessions]** 段落中）可啓用或停用在每次回應時將階段作業 cookie 傳送至瀏覽器。這個動作可以協助確保階段作業 cookie 仍留在瀏覽器的記憶體中。 **resend-pdwebpi-cookies** 參數具有預設設定 no：

```
[sessions]
resend-pdwebpi-cookies = no
```

將預設設定變更爲 *yes*，以便在每次回應時傳送外掛程式階段作業 cookie。

利用 HTTP 標頭來維護階段作業狀態

您可以配置 Tivoli Access Manager Plug-in for Web Servers，來使用 HTTP 標頭資訊，以識別階段作業及維護階段作業狀態。

外掛程式可以使用 HTTP 標頭，來追蹤階段作業，以及鑑定使用者。如果配置外掛程式，使用 HTTP 標頭來追蹤階段作業，則也須配置它，使用 HTTP 標頭來鑑定使用者。然而，如果配置外掛程式，使用 HTTP 標頭來鑑定進入的要求，則不需要配置外掛程式，就可追蹤階段作業。請參閱第 65 頁的『配置 HTTP 標頭鑑定』，以取得如何配置外掛程式，使用 HTTP 標頭進行用戶端鑑定。

當使用 HTTP 標頭來維護階段作業狀態時，必須利用下列值，來配置 pdwebpi.conf 配置檔的 **[common-modules]** 段落：

```
[common-modules]
authentication = http-hdr
session = http-hdr
```

HTTP 標頭的標準配置僅允許指定一個標頭，例如：

```
[modules]
http-hdr = pdwpi-httphdr-module
```

若要指定多個 HTTP 標頭，必須配置多個 HTTP 標頭模組實例。

例如：

```
[modules]
entrust-client-header = pdwpi-httphdr-module
some-other-header     = pdwpi-httphdr-module

[entrust-client-header]
```

```
header = entrust-client

[some-other-header]
header = some-other
```

利用 IP 位址來維護階段作業狀態

Tivoli Access Manager Plug-in for Web Servers 可以使用 IP 位址來識別及追蹤階段作業。

若要配置外掛程式，使用 IP 位址來追蹤階段作業狀態，請在 pdwebpi.conf 中使用 **[common-modules]** 段落。將參數 **session** 輸入爲值 *ip-addr*。亦即：

```
[common-modules]
session = ip-addr
```

確定已在 pdwebpi.conf 配置檔的 **[modules]** 段落配置了 IP 位址鑑定的共用程式庫。亦即：

```
[modules]
ip-addr = pdwpi-ipaddr-module
```

如果 IP 位址是用來維護階段作業狀態，則它們也須用來鑑定進入的要求。請參閱第 67 頁的『配置 IP 位址鑑定』，以取得如何配置 Tivoli Access Manager Plug-in for Web Servers，使用 IP 位址作爲用戶端鑑定方法的詳細資訊。然而，當使用 IP 位址鑑定用戶端時，並不需要它們作爲識別階段作業的方法。

利用 LTPA cookie 標頭來維護階段作業狀態

LTPA 鑑定可用來根據 LTPA cookie 進行接受及鑑定。「LTPA 鑑定」可以利用每一個 HTTP 要求內找到的 LTPA cookie 來維護階段作業狀態。

若要配置外掛程式，以利用「LTPA 鑑定」來維護階段作業狀態，請在 pdwebpi.conf 配置檔中使用 **[common-modules]** 段落。將參數 **session** 輸入爲值 *ltpa*，如下所示：

```
[common-modules]
session = ltpa
```

如果 LTPA 是用來維護階段作業狀態，則也需要配置它來進行使用者鑑定。配置檔的 **[common modules]** 段落也應該爲鑑定 (authentication)設定 LTPA。

```
[common-modules]
authentication = ltpa
session = ltpa
```

利用 iv-headers 位址來維護階段作業狀態

Tivoli Access Manager Plug-in for Web Servers 可以快取 iv-header 資訊，來改進系統效能。

pdwebpi.conf 配置檔中的 **[common-modules]** 段落定義如何利用格式 *module_type* = *module-name*，來使用所有階段作業、鑑定及後置授權方法。若要快取 iv-headers 資訊，請指定值 **iv-headers** 給 **session** 階段作業，如下所示：

```
[common-modules]
session = iv-headers
```

確定已在 pdwebpi.conf 配置檔的 **[modules]** 段落配置了 iv-headers 的共用程式庫。亦即：

```
[modules]
iv-headers = pdwpi-iv-headers-module
```

利用 SPNEGO 來維護階段作業狀態

請參閱第 60 頁的『配置安全提供者 NEGOtiation (SPNEGO) 鑑定』

鑑定配置概觀

如同在第 37 頁的『配置鑑定』 節中看到的一般，鑑定模組是用來執行從要求擷取鑑定資訊的處理程序。驗證鑑定資訊的鑑定機制會執行要求的眞正鑑定。隔離鑑定模組與鑑定機制之間的角色，可讓針對 WebSEAL 撰寫的自訂 CDAS 程式庫與外掛程式一起使用。

Tivoli Access Manager Plug-in for Web Servers 支援的所有鑑定方法的機制都配置在 pdwebpi.conf 配置檔的 **[authentication-mechanisms]** 段落中。受支援的鑑定方法參數包括：

- 本端（內建）鑑定程式

  本端鑑定程式的參數指定了正確的內建共用程式庫 (UNIX) 或 DLL (Windows) 檔。
- 自訂外部鑑定程式

  外掛程式提供伺服器程式碼範本，您可用來建置及指定自訂的外部「跨網域鑑定服務 (CDAS)」伺服器。

  外部 CDAS 鑑定程式會指定正確的自訂共用程式庫。

註: 不同於 **[modules]** 段落的配置，在 **[authentication-mechanisms]** 段落中配置機制時，請新增完整的檔名。亦即，包括檔案字首及作業系統特有的副檔名。

本端鑑定機制

下列鑑定機制參數指定本端內建鑑定程式：

表 9. 本端內建鑑定程式.

參數	說明
套表和基本鑑定	
passwd-ldap	以 LDAP 使用者名稱和密碼進行用戶端存取。
用戶端憑證式鑑定	
cert-ssl	透過 SSL 利用用戶端憑證進行用戶端存取。
「HTTP 標頭」、「IP 位址鑑定」、已啓動 iv-remote-address 的「IV 標頭」。	
http-request	透過特殊的 HTTP 標頭、IP 位址鑑定或已啓動 iv-remote-address 的「IV 標頭」，來進行用戶端存取。

使用 **[authentication-mechanisms]** 段落，以下列格式來配置鑑定方法及實作方式：

authentication_method_parameter = shared_library

外部自訂 CDAS 鑑定參數

以下的參數可用來指定外部 CDAS 伺服器的自訂共用程式庫：

表 10. 外部 CDAS 伺服器參數.

參數	說明
passwd-cdas	以第三方登錄的使用者名稱和密碼進行用戶端存取。
token-cdas	以 LDAP 使用者名稱和記號通行代碼進行用戶端存取。
cert-cdas	透過 SSL 利用用戶端憑證進行用戶端存取。

除了鑑定程式庫外，還有兩個可在外掛程式中使用的其他標準 Tivoli Access Manager 程式庫：

- **passwd-strength**

  這個程式庫會檢查在密碼變更套表上所輸入的新密碼。

- **cred-ext-attrs**

  這個程式庫容許指定自訂的屬性（名稱/值配對），以併入證明。

請參閱 *IBM Tivoli Access Manager WebSEAL Developer's Reference*，以取得有關建置和配置實作 CDAS 伺服器的自訂共用程式庫的詳細資訊。

外掛程式的預設配置

根據預設值，會設定外掛程式，使用「基本鑑定 (BA)」使用者名稱和密碼（LDAP 登錄）來鑑定用戶端。

通常會對 TCP 及 SSL 存取同時啓用外掛程式。因此， **[authentication-mechanisms]** 段落的典型配置包含了使用者名稱和密碼的支援（LDAP 登錄）以及透過 SSL 之用戶端憑證的支援。

下列範例代表 Solaris 上 **[authentication-mechanisms]** 段落的典型配置：

```
[authentication-mechanisms]passwd-ldap = libldapauthn.so
cert-ssl = pdwpi-sslauthn.so
```

若要配置其他鑑定方法，請新增適當的參數與其共用程式庫（或 CDAS 模組）。

配置多個鑑定方法

您可以修改 `pdwebpi.conf` 配置檔的 **[authentication-mechanisms]** 段落，來指定將用於任何可支援的鑑定方法的共用程式庫。當您配置多個鑑定方法時，以下的狀況均可適用：

1. 所有的鑑定方法都可各自獨立運作。 您也可以試著爲每個可支援的方法配置一個共用程式庫。
2. 當 **cert-cdas** 方法和 **cert-ssl** 方法都已配置時，前者優先於後者。您必須啓用這兩個方法之一，才能支援用戶端憑證。
3. 在配置多個密碼類型鑑定程式時，實際上只會使用其中一個。 外掛程式使用下列優先順序，來解析多個配置的密碼鑑定程式：
   a. **passwd-cdas**
   b. **passwd-ldap**
4. 您可以試著爲兩個不同的鑑定方法配置相同的自訂程式庫。 例如，您可以寫入一個自訂共用程式庫來處理使用者名稱/密碼和 HTTP 標頭鑑定。 在此範例中，您可爲 **passwd-cdas** 和 **http-request** 參數配置相同的共用程式庫。 程式開發人員必須負責維護階段作業狀態，並且避免兩種方法發生衝突。

登出、密碼變更及說明指令

Tivoli Access Manager 提供了以下指令，支援透過 HTTP 或 HTTPS 鑑定的用戶端。

pkmslogout

當用戶端所使用的鑑定方法，不會針對所有的要求提供鑑定資料時，用戶端可以使用 **pkmslogout** 指令從現行階段作業登出。當使用鑑定方法來提供每一個要求的鑑定資料時， **pkmslogout** 指令雖然會清除階段作業快取，但是證明資訊仍包含在要求標頭中。在此情況下，使用者必須關閉瀏覽器，才能完全登出階段作業。

pkmslogout 指令適用於使用以下的鑑定方式：用戶端憑證、記號通行代碼、「套表」鑑定，以及 HTTP 標頭鑑定的某些實作方式。

按照以下的方式來執行指令：

```
https://www.tivoli.com/pkmslogout
```

瀏覽器會顯示 pdwebpi.conf 配置檔中所定義的登出套表：

```
[acctmgmt]
logout-success = logout_success.html
```

logout-success 項目可以指定預先定義的 HTML 檔（內含在基本 *install*/nls/html/C 目錄內）或 URI。指定的 URI 可以是相對 URI 或絕對 URI。

當網路配置需要不同的結束畫面，供使用者登出明顯不同的虛擬系統時， **pkmslogout** 公用程式也支援多個登出回應頁面。

pkmspasswd

當您使用「基本鑑定 (BA)」或「套表」鑑定時，您可以使用此指令來變更登入密碼。這個指令適用於透過 HTTP 或 HTTPS。

例如：

```
https://www.tivoli.com/pkmspasswd
```

瀏覽器會顯示 pdwebpi.conf 配置檔中所定義的密碼變更套表：

```
[acctmgmt]
password-change-form-uri = /pkmspasswd.form
password-change-uri = /pkmspasswd
password-change-success = password_change_success.html
password-change-failure = password_change_failure.html
```

您可以修改 password_change_success.html 及 password_change_failure.html 檔來符合您的需求。

pkmshelp

您可以使用這個指令來存取說明頁面。這個指令適用於透過 HTTP 或 HTTPS。

說明頁面的名稱及位置定義在 pdwebpi.conf 配置檔中：

```
[acctmgmt]
help-uri = /pkmshelp
help-page = help.html
```

您可以修改 help.html 檔來符合您的需求。

配置基本鑑定

「基本鑑定 (BA)」是對鑑定機制提供使用者名稱和密碼的標準方法。 BA 是由 HTTP 通訊協定所定義，並透過 HTTP 及透過 HTTPS 實作。

啓用基本鑑定

根據預設值，外掛程式是針對 BA 使用者名稱及密碼而配置的。pdwebpi.conf 配置檔中的 **[common-modules]** 段落定義如何使用 BA 鑑定使用者。亦即：

```
[common-modules]
authentication = BA
```

pdwebpi.conf 配置檔中的 **[modules]** 段落定義所有可用的鑑定機制，以及它們相關聯的共用程式庫名稱。確定基本鑑定的項目存在；亦即：

```
[modules]
BA = pdwpi-ba-module
```

根據預設值，在配置檔的 **[authentication levels]** 段落中， BA 鑑定機制的層次會指定爲 1。對於進入的要求，這個設定與鑑定機制的優先順序相關。

配置基本鑑定機制

passwd-ldap 參數可指定用來處理使用者名稱和密碼鑑定的共用程式庫。

- 在 UNIX 上，提供內建對映功能的檔案是一個稱爲 libldapauthn 的共用程式庫。
- 在 Windows 上，提供內建對映功能的檔案是一個稱爲 ldapauthn 的 DLL。

表 11. BA 共用程式庫鑑定機制

	共用程式庫		
鑑定機制	**Solaris**	**AIX**	**Windows**
passwd-ldap	libldapauthn.so	libldapauthn.a	ldapauthn.dll

您可以在 pdwebpi.conf 配置檔的 **[authentication-mechanisms]** 段落中，將 **passwd-ldap** 參數輸入爲共用程式庫檔案的平台特有名稱，來配置使用者名稱和密碼鑑定機制 – 如下所示：

Solaris：

```
[authentication-mechanisms]passwd-ldap = libldapauthn.so
```

Windows：>

```
[authentication-mechanisms]passwd-ldap = ldapauthn.dll
```

設定領域名稱

領域會顯示在瀏覽器呈現給使用者，以要求使用者名稱及密碼的對話框中。領域名稱會指定給 **basic-auth-realm** 參數（位於 pdwebpi.conf 配置檔的 **[BA]** 段落中）。

```
[BA]
basic-auth-realm = realm_name
```

操作 BA 標頭

您可以配置外掛程式，藉由控制傳送至 Web 伺服器的 BA 標頭內容，以原始或修改過的用戶端身份資訊提供受保護的應用程式。用戶端送來的現有標頭可以：

- 刪掉所有要求、
- 刪掉未經鑑定的要求、
- 傳送未經變更的所有要求。

對於未提供 BA 標頭的用戶端，或對於傳送至 Web 伺服器的現有用戶端標頭資訊，標頭資訊可以：

- 設爲固定的使用者名稱及密碼、
- 具有固定的已傳送密碼（含有以已鑑定使用者名稱傳送的使用者名稱）、
- 利用來自 Tivoli Access Manager GSO 鎖定框的資訊加以設定。

若要操作進入要求的 BA 標頭，外掛程式必須加以配置，以容許使用「基本鑑定」來進行後置授權處理程序。若要這樣做，請在 pdwebpi.conf 配置檔的 *[common-modules]* 段落中，新增參數 **post-authzn** 並將它設爲 **BA** 值。亦即：

```
[common-modules]
post-authzn = BA
```

strip-hdr 參數會指示外掛程式：

值	結果
ignore	將標頭保持原狀。外掛程式會傳送原始的用戶端 BA 標頭至資源，沒有任何干預。基本上，這會建構資源的直接登入，透通至外掛程式。 **註:** 這個選項可能容許未經鑑定的使用者傳送 BA 標頭至 Web 伺服器。僅在確定您需要它並瞭解安全暗示時，才應該使用這個選項。
always	在轉遞要求至 Web 伺服器之前， Always 會從任何用戶端要求中移除「基本鑑定」標頭資訊。在此情況下，外掛程式變成單一安全提供者。如果您需要對 Web 伺服器提供某些用戶端資訊，您可將此選項與 IV 標頭鑑定結合，將 Tivoli Access Manager 用戶端身份資訊放入 HTTP 標頭欄位。 **註:** 一旦啓用了這個選項，如果受保護的伺服器傳送一個 BA 暗號，則用戶端會看到一個鑑定蹦現視窗，但無法登入，因爲它們的回應永遠都會遭到移除。
unauth	從用戶端收到的 BA 標頭將從所有要求中移除，但來自使用者的要求除外，因爲外掛程式已使用「基本鑑定」鑑定了他們。這允許已鑑定的使用者傳送已鑑定的 BA 標頭至 Web 伺服器，但阻止未經鑑定的使用者這樣做。

配置檔的 **[BA]** 段落中的 **add-hdr** 參數可讓您在「HTTP 基本鑑定 (BA)」標頭中提供用戶端識別資訊。使用 **add-hdr** 參數在 HTTP BA 標頭中提供用戶端識別資訊是發生在利用 **strip-hdr** 參數功能進行任何處理程序之後。 **add-hdr** 參數可以設爲：*none*、*gso* 或 *supply*。

- 設爲 *none*，BA 標頭就不會新增至要求。
- 設爲 *gso*，有一個 GSO BA 標頭就會新增至要求 — 請參閱第 94 頁的『使用廣域單一登入 (GSO)』，以取得如何配置外掛程式 GSO 功能的詳細資訊。
- 設爲 *supply*，有一個靜態密碼及使用者名稱就會新增至 BA 標頭。這些靜態密碼及使用者名稱都定義在 **supply-password** 及 **supply-username** 參數（位於配置檔的 **[BA]** 段落）中。 **supply-username** 參數可以設爲固定的使用者名稱值。如果未設定 **supply-username** 參數，將使用 Tivoli Access Manager 的已鑑定名稱，來建立 BA 標頭中的使用者名稱。在此情況下，外掛程式保護的資源需要來自 Tivoli Access Manager 身份的鑑定。

當 **add-hdr** 參數設爲 *supply* 及 **supply-password**，而且設定了 **supply-username** 參數，則所有要求都將使用指定的使用者名稱及密碼。使用共同使用者名稱及密碼，並不足以向應用程式伺服器證明，可用該使用者名稱合法登入用戶端。如果用戶端永遠通過外掛程式來存取資源，則這個解決方案不會出現任何安全問題。不過，利用其他可能的存取方法實際保護資源是非常重要的。由於此實務沒有密碼層次的安全，因此外掛程式保護的資源必須隱含地信任外掛程式，以驗證用戶端的合法性。使用者登錄也必須辨識 Tivoli Access Manager 身份，才能夠接受它。

如果未設定 **supply-username**，且使用者未經鑑定，則沒有 BA 標頭會新增至要求。

配置套表鑑定

Tivoli Access Manager 所提供的「套表」鑑定，是標準「基本鑑定」機制以外的另一種選擇。這種方法會自 Tivoli Access Manager 產生自訂的 HTML 登入套表，而不是因「基本鑑定」暗號產生的標準登入提示。

當您使用「套表」型登入時，瀏覽器不會如同其在「基本鑑定」中一樣快取使用者名稱和密碼資訊。

啓用套表鑑定

pdwebpi.conf 配置檔中的 **[common-modules]** 段落定義如何使用所有鑑定方法。若要使用套表啓用鑑定，請指定 *forms* 一字給 authentication 參數；亦即：

```
[common-modules]
authentication = forms
```

當使用套表進行鑑定時，也會配置外掛程式，以使用套表進行後置授權處理程序。使用套表可讓外掛程式重新導向已鑑定的使用者回到原始要求 URL。在 pdwebpi.conf 配置檔的 **[common-modules]** 段落中，新增參數 **post-authzn**，如下所示：

```
[common-modules]
authentication = forms
post-authzn = forms
```

pdwebpi.conf 配置檔中的 **[modules]** 段落定義所有可用的鑑定機制，以及它們相關聯的共用程式庫名稱。確定套表鑑定的項目存在；亦即：

```
[modules]
forms = pdwpi-forms-module
```

配置套表鑑定機制

passwd-ldap 參數可指定用來處理使用者名稱和密碼鑑定的共用程式庫。

- 在 UNIX 上，提供內建對映功能的檔案是一個稱爲 libldapauthn 的共用程式庫。
- 在 Windows 上，提供內建對映功能的檔案是一個稱爲 ldapauthn 的 DLL。

表 12. 套表共用程式庫鑑定機制

	共用程式庫		
鑑定機制	**Solaris**	**AIX**	**Windows**
passwd-ldap	libldapauthn.so	libldapauthn.a	ldapauthn.dll

您可以在 pdwebpi.conf 配置檔的 **[authentication-mechanisms]** 段落中，將 **passwd-ldap** 參數輸入爲共用程式庫檔案的平台特有名稱，來配置使用者名稱和密碼鑑定機制，如下所示：

Solaris：

```
[authentication-mechanisms]passwd-ldap = libldapauthn.so
```

Windows：

```
[authentication-mechanisms]passwd-ldap = ldapauthn.dll
```

自訂 HTML 回應套表

套表鑑定需要您使用自訂登入套表。根據預設值，範例 login.html 套表位於下列目錄：*install_directory*/nls/html/*lang*

其中 *lang* 取自於 NLS 配置。在進行美式英文安裝作業時，*lang* 將設爲 **C**。

配置檔的 **[forms]** 段落中的 **login-form** 參數定義在登入期間呈現給使用者之套表的檔名。檔案的路徑應該相對於已轉換的 pdwebpi HTML 目錄；例如，*pdwebpi*/nls/html/*lang*。

```
[forms]
login-form = login.html
```

自訂套表登入 URI

您可以具有在單一虛擬主機內使用之套表登入模組的多個實例。在如此的實例中，需要變更當爲套表登入模組的每一個別實例送出登入套表時已張貼的 URI。 **[forms]** 段落中的 **login-uri** 參數會控制這個 URI。如果是從預設值變更，則 **login-form** 參數（請參閱『自訂 HTML 回應套表』）必須更新，才能反映變更。

建立 BA 標頭

套表鑑定可讓您根據登入套表中提供的使用者名稱及密碼，來建立 BA 標頭。建立標頭會提供一個簡易登入機制，當後端應用程式需要基本鑑定，且使用者名稱及密碼符合 Tivoli Access Manager 使用的使用者名稱及密碼時，就可以使用這個機制。

配置檔的 **[forms]** 段落內的 **create-ba-hdr** 參數可啓用或停用建立 BA 標頭，例如：

```
[forms]
create-ba-hdr = yes
```

根據預設值，鑑定並不會建立 BA 標頭 - **create-ba-hdr** 設爲 *no*。不管如何設定參數，當未順利鑑定使用者時，不會建立 BA 標頭，當使用者的密碼到期時，也不會建立標頭。

註: 如果 **post-authzn** 清單中在套表模組後的另一個模組覆寫了 BA 標頭（或移除了它），則這個功能將無法運作。建議您應該將套表模組指定爲 **post-authzn** 清單中的最後一項。

配置憑證鑑定

Tivoli Access Manager Plug-in for Web Servers 支援透過 SSL 使用用戶端數位憑證，進行與用戶端的安全通訊。在此鑑定方法中，憑證資訊（例如「識別名稱」或 DN）會對應至 Tivoli Access Manager 身份。

使用憑證互相鑑定

在兩個階段中，會使用數位憑證來進行鑑定：

- 外掛程式所在的 Web 伺服器以其伺服器端憑證，對 SSL 用戶端識別其本身。
- Web 伺服器使用其「憑證管理中心 (CA)」主要憑證的資料庫，驗證以用戶端憑證存取伺服器的用戶端。

1. SSL 用戶端需要透過外掛程式與 Web 伺服器建立連線。
2. 在回應中，Web 伺服器會使用已簽署的伺服器端憑證傳送其公用金鑰。這個憑證先前已由受信任的第三方憑證機構 (CA) 所簽署。
3. 用戶端檢查該憑證的發證者是否可爲其所信任及接受。 用戶端的瀏覽器通常含有受信任 CA 所發出的主要憑證清單。如果 Web 伺服器的憑證上的簽名符合這些主要憑證之一，則伺服器是可信任的。
4. 如果簽名不符，瀏覽器即通知其使用者，指出此憑證是由不明憑證機構所發出。 接著，接受或拒絕該憑證是使用者的責任。
5. 如果簽名符合瀏覽器的主要憑證資料庫中的項目，則會安全地協議用戶端與 Web 伺服器之間的階段作業金鑰。

   這項處理程序的最終結果就是安全頻道，用戶端可以透過這個頻道來進行鑑定（例如，使用使用者名稱及密碼）。在順利地鑑定後，用戶端與伺服器可以繼續透過這個頻道進行安全的通訊。
6. 現在，用戶端將透過外掛程式傳送其公用金鑰憑證給 Web 伺服器。
7. Web 伺服器將嘗試使用 Web 伺服器的憑證儲存區，將用戶端憑證上的簽名與已知 CA 比對。
8. 如果簽名不符，將產生 SSL 錯誤碼，並將它傳送給用戶端。
9. 如果簽名相符，則可信任用戶端。將發生用戶端鑑定，因而導致 Tivoli Access Manager 身份。
10. 安全地協議用戶端與 Web 伺服器之間的階段作業金鑰。這項處理程序的最終結果就是手動鑑定的用戶端與伺服器之間安全且信任的通訊頻道。

啓用憑證鑑定

`pdwebpi.conf` 配置檔中的 **[common-modules]** 段落定義如何使用所有鑑定方法。若要使用憑證啓用鑑定，請指定 'cert' 一字給 **authentication** 參數；亦即：

```
[common-modules]
authentication = cert
```

`pdwebpi.conf` 配置檔中的 **[modules]** 段落定義所有可用的鑑定機制，以及相關聯的共用程式庫名稱。確定憑證鑑定的項目存在；亦即：

```
[modules]
cert = pdwpi-certificate-module
```

註: 對於 IHS 上的安裝作業，您必須配置 Web 伺服器，向用戶端要求憑證。

配置憑證鑑定機制

cert-ssl 參數可指定對映憑證鑑定資訊的共用程式庫。

在 UNIX 上，提供內建對映功能的檔案是一個稱爲 `libpdwpi-sslauthn` 的共用程式庫。在 Windows 上，提供內建對映功能的檔案是一個稱爲 `sslauthn` 的 DLL。

表 13. 憑證共用程式庫鑑定機制

鑑定機制	共用程式庫		
	Solaris	**AIX**	**Windows**
cert-ssl	libpdwpi-sslauthn.so	libpdwpi-sslauthn.a	pdwpi-sslauthn.dll

您可以在 pdwebpi.conf 配置檔的 **[authentication-mechanisms]** 段落中，將 **cert-ssl** 參數輸入爲共用程式庫檔案的平台特有名稱，來配置憑證鑑定機制。

Solaris：

```
[authentication-mechanisms]cert-ssl= libpdwpi-sslauthn.so
```

Windows：>

```
[authentication-mechanisms]cert-ssl = pdwpi-sslauthn.dll
```

註: pdwpi-sslauthn CDAS 需要使用者憑證中的主題 DN 完全符合使用的 LDAP DN。如果您需要使用更複雜的對映，將需要開發一個自訂的 CDAS。請參閱 *WebSEAL Developer's Reference*，取得如何建置 CDAS 模組的指示，這些指示也適用於 Plug-in for Web Servers。

配置記號鑑定

Tivoli Access Manager Plug-in for Web Servers 可支援透過用戶端提供的記號通行代碼進行鑑定。這種鑑定會使用兩個以 RSA SecureID™ 墜飾爲基礎的因子登入。

啓用記號鑑定

pdwebpi.conf 配置檔中的 **[common-modules]** 段落定義如何使用所有鑑定方法。若要使用「記號啓用鑑定」，請指定 'token' 一字給 **authentication** 參數。

當啓用了使用記號來鑑定時，也必須配置記號，來進行後置授權處理程序。在配置檔的 **[modules]** 段落中，請建構一個 **post-authzn** 參數，並指定 'token' 一值給它。**[common-modules]** 段落應該包括下列兩個項目：

```
[common-modules]
authentication = token
post-authzn = token
```

pdwebpi.conf 配置檔中的 **[modules]** 段落定義所有可用的鑑定機制，以及相關聯的共用程式庫名稱。確定記號鑑定的項目存在；亦即：

```
[modules]
token = pdwpi-token-module
```

配置記號鑑定機制

token-cdas 參數可指定對映記號通行代碼鑑定資訊的共用程式庫。

- 在 UNIX 上，提供內建對映功能的檔案是名稱爲 libtokenauthn 的共用程式庫。
- 在 Windows 上，提供內建對映功能的檔案是一個稱爲 tokenauthn 的 DLL。

表 14. 記號共用程式庫鑑定機制

鑑定機制	共用程式庫		
	Solaris	**AIX**	**Windows**
token-cdas	libtokenauthn.so	libtokenauthn.a	tokenauthn.dll

根據預設值，此內建共用程式庫是寫在程式內，以對映 SecureID 記號通行代碼資料。您可以自訂這個檔案來鑑定其他類型的特殊記號資料，並（選用性）將此資料對映至 Tivoli Access Manager 身份。請參閱 *IBM Tivoli Access Manager WebSEAL Developer Reference*，以取得 API 資源。

您可以在 pdwebpi.conf 配置檔的 **[authentication-mechanisms]** 段落中，將 **token-cdas** 參數輸入爲共用程式庫檔案的平台特有名稱，來配置記號鑑定機制。

例如：

Solaris：

```
[authentication-mechanisms]token-cdas = libtokenauthn.so
```

Windows：

```
[authentication-mechanisms]token-cdas = tokenauthn.dll
```

自訂記號回應頁面

配置檔的 **[token-card]** 段落中的 **token-login-form** 參數定義在記號登入期間呈現給使用者用戶端之套表的檔名。檔案的路徑應該相對於已轉換的 pdwebpi HTML 目錄；例如， *pdwebpi*/nls/html/*lang*。其中 *lang* 取自於 NLS 配置。在進行美式英文安裝作業時，*lang* 會設爲 **C**。

[token-card] 段落中的 **next-token-form** 參數定義顯示給使用者用戶端以要求下一個記號的套表。當伺服器無法順利地從第一個記號鑑定使用者時，將要求用戶端輸入另一個記號。有一些理由可能導致無法鑑定使用者。但是，最常發生此錯誤的原因是用戶端與伺服器時鐘不同步。當使用第一個記號無法順利地鑑定時，就會顯示 **next-token-form** 參數中所指定的頁面，來提示輸入下一個記號。

token-card 段落具有下列格式：

```
[token-card]
token-login-form = tokenlogin.html
next-token-form = nexttoken.html
```

配置安全提供者 NEGOtiation (SPNEGO) 鑑定

對於 Windows 用戶端（如 Microsoft Internet Explorer）， Tivoli Access Manager Plug-in for Web Servers 支援使用 SPNEGO 標準鑑定通訊協定，作爲外掛程式保護的 IIS 伺服器的鑑定機制。 SPNEGO 鑑定機制提供「單一登入 (SSO)」能力，以允許使用者從僅需要起始登入的 Windows 用戶端，存取安全 IIS Web 伺服器上的資源。Web 伺服器或外掛程式（視外掛程式配置而定）會在鑑定網域控制站及用戶端瀏覽器之間傳送要求。

當使用者存取安全 Web 伺服器時，將對照網路的網域控制站所儲存的使用者 ID 及密碼，來檢查使用者 ID 及密碼，並在下列情況時，授與使用者存取權：

- 使用者是網域的成員
- 已在 Authorization Server 中啓用了 SPNEGO
- Authorization Server 允許存取

使用者若存取外掛程式 SPNEGO 鑑定所保護的資源，且不是網域的成員，或正在使用 Internet Explorer 以外的瀏覽器，則必須使用另一種方法（例如，「基本鑑定」或套表）來進行鑑定。

註: SPNEGO 外掛程式功能與 IIS 安全配置無關。

使用 SPNEGO 啓用鑑定

若要使用 SPNEGO 啓用鑑定，請指定參照 *spnego* 給 **authentication** 及 **session** 參數（位於 pdwebpi.conf 配置檔的 **[common-modules]** 段落中）。SPNEGO 鑑定功能將不會正確地操作，除非 **authentication** 及 **session** 參數兩者都設爲 *spnego*。

```
[common-modules]
authentication = spnego
session = spnego
```

pdwebpi.conf 配置檔中的 **[modules]** 段落定義所有可用的鑑定機制，以及它們相關聯的共用程式庫名稱。確定 SPNEGO 鑑定的項目存在；亦即：

```
[modules]
spnego = pdwpi-spnego-module
```

配置 SPNEGO 參數

SPNEGO 鑑定參數是配置在 pdwebpi.conf 配置檔的 **[spnego]** 段落中。

web-server-does-authn 參數指定用來執行 SPNEGO 鑑定的機制。設爲 **true**，IIS 將執行鑑定並明白使用者身份。所有要求都是在使用者的環境定義中執行。對於許多應用程式，這是想要的動作，但是對於某些應用程式，在匿名使用者的環境定義以外的任何環境定義中具有 Web 伺服器所處理的要求，可能會被視爲安全風險。將 **web-server-does-authn** 參數設爲 **false** 容許額外的安全。當參數設爲 false 時， IIS 在處理要求時將不明白使用者的身份，因此，將以匿名使用者的身份來處理要求。

設定此參數就是您想要決定已鑑定使用者的專用權的地方。根據預設值，**web-server-does-authn** 參數會設爲 **true**。

```
[spnego]
web-server-does-authn = true
```

使用者第一次存取 SPNEGO 鑑定保護的安全 HTTP Web 空間時，系統會提示他們輸入他們的使用者名稱、密碼及網域。在這個起始登入後，他們可以在外掛程式保護的 Web 空間之間瀏覽，不需要重新登入。HTTPS 用戶端不會出現登入提示，因爲網域已從它們的起始登入知道它們的使用者名稱及密碼。

如果利用目標 Web 伺服器作爲 *本端內部網路網站*或*受信任的網站*，來配置您的 Internet Explorer 瀏覽器，則您可以避免使用者名稱及密碼的起始要求。若要在 Internet Explorer 中進行如此的配置：

1. 從 Internet Explorer 功能表列，選取**工具** > **網際網路選項**，來顯示*網際網路選項*對話框。
2. 選取**安全性**標籤。

3. 選取**本端內部網路**圖示或**信任的網站**圖示，再按一下**網站...** 按鈕。
4. 如果在步驟 3 中選取了**本端內部網路**，請按一下**進階**按鈕。
5. 輸入目標 Web 伺服器（IP 位址或主機名稱），再按一下**新增**按鈕。
6. 按一下**確定**。

配置失效接替 cookie 鑑定

失效接替 cookie 功能通常是用於透過負載平衡機制連接至已抄寫的前端 Web 伺服器的用戶端。當伺服器與用戶端之間的原始階段作業變成無法使用時，失效接替 cookie 會阻止強制的重新鑑定。

當配置失效接替 cookie 來進行後置授權處理程序時，外掛程式就會以伺服器特有的或全網域的 cookie 來加密證明資料。當用戶端第一次連接時，此 cookie 會被放在瀏覽器中。如果失去了起始 Web 伺服器階段作業，則 cookie 會呈現至用戶端重新導向至的下一個伺服器。 cookie 是用於自動重新鑑定，所以會替用戶端省掉手動重新鑑定的作業。已抄寫之伺服器上的外掛程式會共用一個共同的金鑰，此金鑰是用來解密 cookie 中所保留的證明資訊，以及建立新的階段作業。

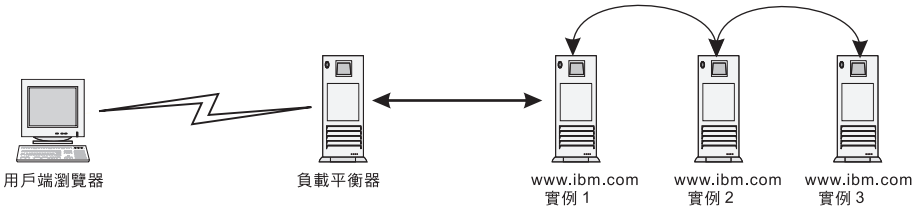

圖 6. 失效接替 cookie 的典型伺服器架構。

上圖顯示將因使用失效接替 cookie 而受益的典型架構。同一 Web 伺服器的三個相同實例都位在負載平衡伺服器之後，這個伺服器會將要求導向至這三個伺服器之一，視負荷及可用性而定。例如，假設您配置 www.ibm.com 的每一個實例，利用失效接替cookie來鑑定用戶端，而且也配置這些實例，使用失效接替 cookie 進行後置授權處理程序。用戶端會存取 www.ibm.com，然後導向至伺服器的實例 1，並順利地完成鑑定。用戶端的證明是加密的，並且儲存在用戶端瀏覽器中所儲存的全網域 cookie。在階段作業期間，如果用戶端需要存取 www.ibm.com 的實例 2 或實例 3（例如，如果實例 1 失敗，或需求變得太大），用戶端瀏覽器中所儲存的失效接替 cookie 將用於自動重新鑑定，不需要使用者的介入。

使用失效接替 cookie 啓用鑑定

`pdwebpi.conf` 配置檔中的 **[common-modules]** 段落定義如何使用所有鑑定方法。您可以配置失效接替 cookie，來執行鑑定及後置授權作業。

爲了使用失效接替 cookie 進行後置授權處理程序而配置的外掛程式會加密證明，並將它儲存爲異動回應中的失效接替 cookie。

外掛程式（配置來使用失效接替 cookie 執行鑑定）會使用加密的證明（來自證明要求中找到的失效接替 cookie），來重新鑑定用戶端。

若要使用失效接替r cookie 來啓用鑑定及後置授權，請指定參照 'failover' 給 **authentication** 及 **post-authzn** 參數；亦即：

```
[common-modules]
authentication = failover
post-authzn = failover
```

註: 當配置其他鑑定機制，以及失效接替 cookie 時，必須將失效接替 cookie 鑑定配置成起始鑑定方法。

pdwebpi.conf 配置檔中的 **[modules]** 段落定義所有可用的鑑定機制，以及它們相關聯的共用程式庫名稱。確定失效接替鑑定的項目存在；亦即：

```
[modules]
failover = pdwpi-failovercookie-module
```

配置失效接替 cookie 參數

失效接替 cookie 鑑定參數是配置在 pdwebpi.conf 配置檔的 **[failover]** 段落中。

failover-cookies-keyfile 參數指定用來在失效接替 cookie 中加密及解密證明資料的檔案。例如：

```
[failover]
failover-cookies-keyfile = failover.key
```

金鑰檔案必須使用程式 **pdwpi-cdsso-key-gen**（位於 *install_path*/bin 目錄）來加以建立。用法：

```
./pdwpi-cdsso-key-gen key_file_name_to_create
```

failover-cookies-lifetime 參數定義 failover-cookie 的有效生命週期（以分鐘爲單位）。這是建立 cookie 及停用 cookie 之間的時間。預設值是 30 分鐘。

```
[failover]
failover-cookies-lifetime = 30
```

enable-failover-cookie-for-domain 參數啓用或停用整個網域內的 cookie 有效性。

例如：

```
[failover]
enable-failover-cookie-for-domain = false
```

配置 IV 標頭鑑定

Tivoli Access Manager 支援使用內部產生且由相容用戶端或 proxy 代理站提供的標頭資訊，來進行鑑定。基於歷程理由，這些稱爲 IV (IntraVerse) 標頭。當外掛程式強化的 Web 伺服器從受信任的應用程式（如 WebSEAL 或多工 proxy 代理站）接收要求時，IV 標頭可插入至已傳送至外掛程式 proxy 伺服器的要求。 IV 標頭含有識別起源用戶端而不是傳送伺服器的資訊。標頭中的資訊是基於授權目的而用來建構起源用戶端證明。同樣地，如果外掛程式強化的 Web 伺服器傳送要求至另一個能辨識 IV 標頭的 Tivoli Access Manager 伺服器，則外掛程式 proxy 可以插入 IV 標頭，以識別起源用戶端。

您可以配置外掛程式，以使用 IV 標頭進行後置授權處理程序或鑑定要求。針對後置授權處理程序而配置的外掛程式，在順利配置後，會修改異動要求，方法爲插入用戶端的眞正身份作爲 IV 標頭。然後，起源 Web 伺服器可能會將這些標頭轉遞至另一個伺服器。

如果您配置外掛程式，使用「IV 標頭」來執行用戶端鑑定，則外掛程式會使用從異動要求中找到的 IV 標頭擷取的身份，來建立一個用戶端證明。因爲用戶端容易僞造 IV 標頭，所以僅在 proxy 伺服器在鑑定要求中設定 'use secondary authenticator' 旗標，來指定標頭的信任，才能建立如此的證明。

對於鑑定，您可以配置 IV 標頭，當透過 proxy 接收時，在要求中接受一個、一些或所有 iv-user、iv-user-l、iv-creds 或 iv-remote-address 標頭，作爲鑑定的證明。iv-remote-address 標頭是用來記錄使用者的眞正遠端位址。

針對後置授權處理程序而配置的 IV 標頭，會與一個、一些或所有 iv-user、iv-user-l、iv-creds 及/或 iv-remote-address、HTTP 標頭一起插入要求中。

表 15. IV 標頭欄位說明

IV 標頭欄位	說明
iv-user	Access Manger 使用者的簡稱。如果用戶端是未經鑑定（不明），將預設爲 unauthenticated。
iv-user-l	使用者的完整網域名稱（長型）。例如， LDAP 識別名稱。
iv-groups	使用者所屬的群組清單。
iv-creds	已編碼的不透明資料結構，代表使用者的 Tivoli Access Manager 證明。
iv-remote-address	用戶端的 IP 位址。 此值可能代表 Proxy 伺服器或網路位址轉換器 (NAT) 的 IP 位址。

使用 IV 標頭啓用鑑定

pdwebpi.conf 配置檔中的 **[common-modules]** 段落定義如何使用所有鑑定方法。若要使用 IV 標頭啓用鑑定，請指定參照 **iv-headers** 給 **authentication** 參數；亦即：

```
[common-modules]
authentication = iv-headers
```

若要啓用 IV 標頭進行後置授權處理程序，請指定 *iv-headers* 一值給 **post-authzn** 參數（位於 pdwebpi.conf 配置檔的 **[common-modules]** 段落中）。亦即：

```
[common-modules]
post-authzn = iv-headers
```

pdwebpi.conf 配置檔中的 **[modules]** 段落定義所有可用的鑑定機制，以及它們相關聯的共用程式庫名稱。確定 IV 標頭鑑定的項目存在；亦即：

```
[modules]
iv-headers = pdwpi-iv-headers-module
```

配置 IV 標頭參數

IV 標頭鑑定參數是配置在 pdwebpi.conf 配置檔的 **[iv-headers]** 段落中。

accept 參數指定執行 IV 標頭鑑定時所接受的 IV 標頭類型。根據預設值，外掛程式接受所有類型的 IV 標頭。有效選項爲 all、iv-creds、iv-user、iv-user-l、iv-remote-address。若要輸入多個標頭類型，請以逗點隔開值。

例如：

```
[iv-headers]
accept = iv-creds,iv-user
```

generate 參數指定當轉遞 proxy 要求時將產生的 IV 標頭類型。根據預設值，當轉遞 proxy 要求時，外掛程式將產生所有類型的 IV 標頭。有效選項爲：all、iv-creds、iv-user、iv-user-l、iv-remote-address。若要輸入多個標頭類型，請以逗點隔開值。

配置 for iv-remote-address 的 IV 標頭鑑定機制

在「IV 標頭」中使用 **iv-remote-address** 時，您將需要指定對映 HTTP 鑑定標頭資訊的共用程式庫。 **http-request** 鑑定機制會指定對映 HTTP 鑑定標頭資訊的共用程式庫。

- 在 UNIX 上，提供內建對映功能的檔案是一個稱爲 `libpdwpi-http-cdas` 的共用程式庫。
- 在 Windows 上，提供內建對映功能的檔案是一個稱爲 `pdwpi-http-cdas` 的 DLL。

表 16. IV 標頭共用程式庫鑑定機制

	共用程式庫		
鑑定機制	**Solaris**	**AIX**	**Windows**
http-request	`libpdwpi-http-cdas.so`	`libpdwpi-http-cdas.a`	`pdwpi-http-cdas.dll`

您可以在 `pdwebpi.conf` 配置檔的 **[authentication-mechanisms]** 段落中，將 http-request 參數輸入爲共用程式庫檔案的平台特有名稱，來配置 HTTP 標頭鑑定機制。

Solaris：

```
[authentication-mechanisms]http-request = libpdwpi-http-cdas.so
```

Windows：

```
[authentication-mechanisms]http-request = pdwpi-http-cdas.dll
```

配置 HTTP 標頭鑑定

Tivoli Access Manager 支援透過用戶端或 proxy 代理站所提供的自訂 HTTP 標頭資訊進行鑑定。

此機制需要對映功能（共用程式庫），將受信任的（經預先鑑定）標頭資料對映至 Tivoli Access Manager 身份。外掛程式可取得此身份，然後爲使用者建立證明。

外掛程式假設 proxy 代理站先前已鑑定自訂 HTTP 標頭資料。基於這個理由，僅在外掛程式位在已鑑定的 Web proxy 代理站之後，且 **[pdweb-plugins]** 段落內的 **mpa-enabled** 參數設爲 *true* 時，這個模組才能運作。

根據預設值，會建置此共用程式庫，以便從 Entrust Proxy 標頭對映資料。

使用 HTTP 標頭啓用鑑定

pdwebpi.conf 配置檔中的 **[common-modules]** 段落定義如何使用所有鑑定方法。若要使用 HTTP 標頭啓用鑑定，請指定參照 *http-hdr* 給 **authentication** 參數；亦即：

```
[common-modules]
authentication = http-hdr
```

pdwebpi.conf 配置檔中的 **[modules]** 段落定義所有可用的鑑定機制，以及它們相關聯的共用程式庫名稱。確定 HTTP 標頭鑑定的項目存在；亦即：

```
[modules]
http-hdr = pdwpi-httphdr-module
```

指定標頭類型

您必須在 pdwebpi.conf 配置檔的 **[http-hdr]** 段落中指定所有支援的 HTTP 標頭類型。

```
[http-hdr]
header = header_type
```

HTTP 標頭的標準配置僅允許指定一個標頭，例如：

```
[modules]
http-hdr = pdwpi-httphdr-module
```

若要指定多個 HTTP 標頭，必須配置多個 HTTP 標頭模組實例。

例如：

```
[modules]
entrust-client-header = pdwpi-httphdr-module
some-other-header     = pdwpi-httphdr-module

[entrust-client-header]
header = entrust-client

[some-other-header]
header = some-other
```

配置 HTTP 標頭鑑定機制

http-request 參數會指定對映 HTTP 鑑定標頭資訊的共用程式庫。

- 在 UNIX 上，提供內建對映功能的檔案是一個稱爲 libpdwpi-http-cdas 的共用程式庫。
- 在 Windows 上，提供內建對映功能的檔案是一個稱爲 pdwpi-http-cdas 的 DLL。

表 17. HTTP 標頭共用程式庫鑑定機制

	共用程式庫		
鑑定機制	**Solaris**	**AIX**	**Windows**
http-request	libpdwpi-http-cdas.so	libpdwpi-http-cdas.a	pdwpi-http-cdas.dll

根據預設值，此內建共用程式庫已寫在程式內，而會將 Entrust Proxy 標頭資料對映至有效的 Tivoli Access Manager 身份。您必須自訂這個檔案來鑑定其他類型的特殊記號資料，並（選用性）將此資料對映至 Tivoli Access Manager 身份。請參閱 *IBM Tivoli Access Manager WebSEAL Developer Reference*，以取得 API 資源。

您可以在 pdwebpi.conf 配置檔的 **[authentication-mechanisms]** 段落中，將 http-request 參數輸入爲共用程式庫檔案的平台特有名稱，來配置 HTTP 標頭鑑定機制。

例如：

Solaris：

```
[authentication-mechanisms]http-request = libpdwpi-http-cdas.so
```

Windows：

```
[authentication-mechanisms]http-request = pdwpi-http-cdas.dll
```

配置 IP 位址鑑定

進入要求的 IP 位址可以用來維護階段作業狀態，並使用用戶端位址標頭來鑑定用戶端要求。

若沒有同時也配置外掛程式來使用 IP 位址鑑定用戶端要求，將無法配置外掛程式，使用 IP 位址來維護階段作業狀態。然而，如果外掛程式不使用 IP 位址來追蹤使用者階段作業，則可以使用 IP 位址來鑑定使用者。

使用 IP 位址啓用鑑定

pdwebpi.conf 配置檔中的 **[common-modules]** 段落定義如何使用所有鑑定方法。若要使用要求起始者的「IP 位址」來啓用鑑定，請指定參照 *ip-addr* 給 **authentication** 參數，如下所示：

```
[common-modules]
authentication = ip-addr
```

若要啓用使用「IP 位址」來追蹤使用者階段作業，請指定參照 *ip-addr* 給 **session** 參數，如下所示：

```
[common-modules]
session = ip-addr
```

pdwebpi.conf 配置檔中的 **[modules]** 段落定義所有可用的鑑定機制，以及它們相關聯的共用程式庫名稱。確定「IP 位址」鑑定的項目存在，如下所示：

```
[modules]
ip-addr = pdwpi-ipaddr-module
```

配置 IP 位址鑑定機制

「IP 位址鑑定機制」同於「HTTP 標頭」的鑑定機制。 **http-request** 參數會指定「IP 位址」鑑定機制的共用程式庫。

- 在 UNIX 上，提供內建對映功能的檔案是一個稱爲 libpdwpi-http-cdas 的共用程式庫。
- 在 Windows 上，提供內建對映功能的檔案是一個稱爲 pdwpi-http-cdas 的 DLL。

表 18. IP 位址共用程式庫鑑定機制

鑑定機制	共用程式庫		
	Solaris	**AIX**	**Windows**
http-request	libpdwpi-http-cdas.so	libpdwpi-http-cdas.a	pdwpi-http-cdas.dll

您可以在 pdwebpi.conf 配置檔的 **[authentication-mechanisms]** 段落中，將 http-request 參數輸入爲共用程式庫檔案的平台特有名稱，來配置 IP 位址鑑定機制。

例如：

Solaris：

```
[authentication-mechanisms]http-request = libpdwpi-http-cdas.so
```

Windows：

```
[authentication-mechanisms]http-request = pdwpi-http-cdas.dll
```

配置 LTPA 鑑定

外掛程式可以使用 LTPA cookie 來鑑定使用者。LTPA cookie 可以由 Tivoli Access Manager WebSEAL 或 IBM WebSphere 伺服器提供。

啓用 LTPA 鑑定

pdwebpi.conf 配置檔中的 **[common-modules]** 段落定義如何使用 LTPA 鑑定要求。亦即：

```
[common-modules]
authentication = ltpa
```

pdwebpi.conf 配置檔中的 **[modules]** 段落定義所有可用的鑑定機制，以及它們相關聯的共用程式庫名稱。確定 LTPA 鑑定的項目存在；亦即：

```
[modules]
ltpa = pdwpi-ltpa-module
```

設定金鑰明細

所收到的眞正 LTPA cookie 已被傳送者加密。因此，cookie 必須先解密後，才能發生鑑定。pdwebpi.conf 配置檔中的 **[ltpa]** 段落含有解密處理程序所需的金鑰明細：

```
[ltpa]
ltpa-keyfile = full path of keyfile
ltpa-stash-file = password stash file location
ltpa-password = password in lieu of the stash file
```

其中：

ltpa-keyfile 項目指定起始機器所提供之金鑰檔的名稱。金鑰檔項目是必要的。

ltpa-stash-file 項目指定含有金鑰檔密碼之檔案的名稱。這個項目是選用的，但是，如果它不存在，**ltpa-password** 項目必須存在。這個項目較任何指定的 **ltpa-password** 更具優先順序。

僅在 **ltpa-stash-file** 項目不存在時，才需要 **ltpa-password** 項目。它應該含有已指定的金鑰檔的純文字密碼。

配置 LTPA 後置授權處理程序

LTPA 模組是針對後置授權處理程序而配置的，以作爲 WebSphere 應用程式伺服器的單一登入解決方案的一部份。請參閱第 90 頁的『使用 LTPA cookie 單一登入至 WebSphere 應用程式伺服器』，以取得配置明細。

配置登入後使用者的重新導向

使用 **login-redirect** 模組，您可以配置外掛程式，在使用者順利地完成鑑定後，將他們重新導向至特定的 URL。如果您想要所有使用者重新導向至的入口不是他們所要求的網頁，或想要呈給現使用者一個歡迎頁面，或線上應用程式的起始頁，這樣做可能很有用。

外掛程式登入重新導向功能是獨立運作的，與用於鑑定使用者的方法無關。重新導向不會針對設定鑑定或重新鑑定而發生。

啓用使用者重新導向

pdwebpi.conf 配置檔中的 **[common-modules]** 段落定義如何使用所有鑑定方法。若要在使用者起始登入及鑑定後，將他們重新導向至特定的 URI，請指定參照 *login-redirect* 給 **post-authzn** 參數；如下所示：

```
[common-modules]
post-authzn = login-redirect
```

註: 使用時，建議 **login-redirect** 參數應該置於後置授權模組清單中的第一個位置；不然，另一個鑑定模組重新導向（例如，套表後置授權模組）可能會取得優先權。

pdwebpi.conf 配置檔中的 **[modules]** 段落定義所有可用的鑑定機制，以及它們相關聯的共用程式庫名稱。確定 **login-redirect** 的項目存在，如下所示：

```
[modules]
login-redirect = pdwpi-loginredirect-module
```

配置使用者重新導向參數

使用者重新導向參數是配置在 pdwebpi.conf 配置檔的 **[login-redirect]** 段落中。

```
[login-redirect]
redirect-uri = redirect uri
```

使用 **redirect-uri** 參數，來指定您想要使用者在順利登入後導向至哪一個 URI。指定的 URI 可以是相對 URI 或絕對 URI。

新增 LDAP 延伸屬性至 HTTP 標頭（標籤值）

通常，將使用者特有的資訊（例如，電話號碼、電子郵件位址）從 LDAP 連接至 HTTP 鑑定的要求的標頭是很有用的。這容許多個應用程式存取連接的資訊，而不必時常地查詢 LDAP 伺服器。此資訊的本質就是它是相當靜態的，任何使用它的應用程式從不會更新它。資料置於使用者證明，作爲 **ivauthn** 鑑定處理程序的一部份。此資訊也會透過使用者實作的 CDAS 鑑定模組，連接至使用者證明。

下列處理流程說明事件的順序：

- 來自使用者 LDAP 登錄帳戶中任何欄位的使用者定義的補充資料，會被作爲延伸屬性資料而新增至使用者的 Access Manager 證明。
- 被配置來進行標籤值後置授權處理程序時，外掛程式會擷取 LDAP 延伸屬性資料，並將它置於要求的 HTTP 標頭中。
- 後端應用程式可以從標頭中擷取資料，而不需要特別的程式碼或授權 API。

配置外掛程式，將 LDAP 延伸屬性資訊插入 HTTP 標頭包括下列步驟：

1. 在「Web 外掛程式」中配置標籤值後置授權。請參閱第 71 頁的『啓用標籤值處理程序』，以取得如何做的詳細資訊。
2. 編輯 Tivoli Access Manager 配置檔 (pd.conf)，然後在 **[ldap-ext-cred-tags]** 段落中指定要擷取的屬性。

   在證明中，pd.conf 配置檔中定義的每一個 **cred-ext-attr-name** 項目，都會在字首加上 ″tagvalue_″ 一字。此字首可避免與證明中的其他現存資訊發生衝突。 例如：

來自 inetOrgPerson 物件類別的名稱及值：	employeeNumber:09876
證明延伸屬性名稱：	ldap-employee-number
使屬性名稱與 pd.conf **[ldap-ext-cred-tags]** 段落中的 LDAP 資料名稱產生關聯：	[ldap-ext-cred-tags] ldap-employee-number = employeeNumber
出現在使用者證明的屬性名稱及值：	tagvalue_ldap-employee-number:09876

3. 重新啓動外掛程式。
4. 新增延伸屬性至 Access Manager 中的 /PDWebPI/*host* 物件。例如（以一行輸入）：

```
pdadmin> object modify /PDWebPI/host
set attribute HTTP-Tag-Value ldap-home-phone=homePhone
```

影響證明中 LDAP 延伸屬性的狀況

- LDAP 資料可以來自 inetOrgPerson 物件類別中的標準或自訂欄位。
- 您可以在 **[ldap-ext-cred-tags]** 段落中放置多個屬性項目。
- **[ldap-ext-cred-tags]** 段落中指定的所有延伸屬性都會在使用者順利登入時置入證明中。
- LDAP 資料名稱不區分大小寫。
- 證明延伸屬性名稱區分大小寫。
- 透過 **[ldap-ext-cred-tags]** 段落，將延伸屬性插入使用者證明的方法不提供處理及編寫特殊字元（包括雙位元組字集 (DBCS)）的方式。自訂的 CDAS 可用來編寫延伸屬性，以使用 DBCS 並將它們插入證明中。此外，如果這些屬性是當作 HTTP 標頭來傳送，則後端應用程式必須能夠處理已編碼的特殊字元。

您也可以建立新的 Tivoli Access Manager 延伸證明 CDAS，並將這個證明指定爲外掛程式中的鑑定機制。例如：

1. 將 **[authentication-mechanisms]** 段落中的 **cred-ext-attrs** 參數設爲新的 CDAS。例如（以一行輸入）：

```
[authentication-mechanisms]cred-ext-attrs = /opt/PolicyDirector/lib/libextcredtags.so
& /opt/pdwebpi/etc/pdwebpi.conf
```

   （預設配置檔是 pd.conf）
2. 編輯 pdwebpi.conf，並新增段落： **[ldap-ext-attr-cdas-tags]** 及必要的 LDAP 延伸屬性。例如：

```
[ldap-ext-attr-cdas-tags]
ldap-home-phone = homePhone
```

3. 重新啓動外掛程式
4. 新增延伸屬性至 Tivoli Access Manager 中的 /PDWebPI/*host* 物件。例如（以一行輸入）：

```
pdadmin> object modify /PDWebPI/host
set attribute HTTP-Tag-Value ldap-home-phone=homePhone
```

啓用標籤值處理程序

pdwebpi.conf 配置檔中的 **[common-modules]** 段落定義如何使用所有鑑定方法。若要使用標籤值來啓用處理程序，請指定參照 *tag-value* 給 **post-authzn** 參數；如下所示：

```
[common-modules]
post-authzn = tag-value
```

pdwebpi.conf 配置檔中的 **[modules]** 段落定義所有可用的鑑定機制，以及它們相關聯的共用程式庫名稱。確定標籤值的項目存在，如下所示：

```
[modules]
tag-value = pdwpi-tag-value-module
```

配置標籤值參數

標籤值參數是配置在 pdwebpi.conf 配置檔的 **[tag-value]** 段落中。

```
[tag-value]
cache-definitions = yes
cache-refresh-interval = 60
```

cache-definitions 參數啓用或停用快取已連接至物件空間的標籤值定義。**cache-refresh-interval** 定義重新整理定義的快取記憶體的間隔（以秒爲單位）。

支援多工 Proxy 代理站 (MPA)

Tivoli Access Manager 提供保全使用「多工 Proxy 代理站 (MPA)」之網路的解決方案。「多工 Proxy 代理站 (MPA)」是調適多重用戶端存取的閘道。 這些閘道會建立單一鑑定頻道到安全的伺服器，並透過此頻道「穿通」所有的用戶端要求和回應。對外掛程式而言，通過此頻道的資訊最初是以來自一個用戶端的多重要求出現。 外掛程式必須區分 MPA 伺服器鑑定與每一個個別用戶端的額外鑑定。此種閘道的常見範例是「無線存取通訊協定 (WAP)」閘道。接合主機 Web 伺服器一起配置，以容許 WebSEAL 與外掛程式之間的單一登入時， Tivoli Access Manager WebSEAL 也會充當 MPA。若要配置此種的解決方案，可以使用 iv-header 鑑定模組。請參閱第 89 頁的第 6 章, 『Web 單一登入解決方案』，以取得如何配置 SSO 的詳細資訊。

有效的階段作業資料類型和鑑定方法

因爲 Tivoli Access Manager Plug-in for Web Servers 會爲 MPA 維護經過鑑定的階段作業，它也必須同時維護每一個用戶端的個別階段作業。因此，MPA 所使用的階段作業資料和鑑定方法，必須和用戶端所使用的階段作業資料和鑑定方法有所區別。下表列出了 MPA 和用戶端的有效階段作業類型：

表 19. MPA 的有效階段作業資料類型

有效的階段作業類型	
MPA-to-plug-in	**Client-to-plug-in**
SSL 階段作業 ID	
HTTP 標頭	HTTP 標頭
BA 標頭	BA 標頭
IP 位址	
Cookie	Cookie

- 用戶端不可使用 SSL 階段作業 ID 作爲階段作業資料類型。
- 舉例來說，如果 MPA 使用 BA 標頭作爲階段作業資料類型，用戶端就只能選擇 HTTP 標頭和 cookie 作爲階段作業資料類型。
- 如果 MPA 使用 HTTP 標頭作爲階段作業資料，用戶端可以使用不同的 HTTP 標頭類型。
- 伺服器特有 cookie 只包含了階段作業資訊；它沒有身份資訊。
- 如果啓用了 MPA 支援，使用 SSL 階段作業 ID 來維護階段作業狀態就會變更。一般而言，如果已配置 SSL 階段作業 ID 來維護階段作業狀態，則只有 SSL 階段作業 ID 可用來維護 HTTPS 用戶端的階段作業。若要讓 MPA 使用 SSL 階段作業 ID 來維護階段作業，並且讓用戶端使用其他方法來維護階段作業，則此限制就不存在。

MPA-to-plug-in 所使用的鑑定方法必須不同於 client-to-plug-in 所使用的鑑定方法。下表列出了 MPA 和用戶端的有效鑑定方法：

表 20. 有效的 MPA 鑑定類型

有效的鑑定類型	
MPA-to-plug-in	**Client-to-plug-in**
基本鑑定	基本鑑定
套表	套表
記號	記號
HTTP 標頭	HTTP 標頭
憑證	
IP 位址	

- 舉例來說，如果 MPA 使用「基本鑑定」，用戶端可以選擇「套表」、記號以及 HTTP 標頭作爲鑑定方法。
- 用戶端不能使用憑證和 IP 位址鑑定方法。
- 一般而言，若某種傳輸方式已啓用了「套表」（或記號）鑑定，該傳輸方式的「基本鑑定」會自動停用。如果啓用了 MPA 支援，則此限制不存在。 這樣可以讓 MPA 以「套表」（或記號）登入，而用戶端也可使用經由「基本鑑定」，透過相同的傳輸方式登入。

MPA 和多個用戶端的鑑定處理程序

1. 進行下列配置變更：
   - 在配置檔中啓用「多工化 Proxy 代理站」支援。
   - 爲特定的 MPA 閘道建立 Tivoli Access Manager 帳戶。
   - 授與這個帳戶 Proxy ([PDWebPI]p) 存取權，以存取 proxy 要求將導向至的虛擬主機的「MPA 保護的物件」。在預設配置中，可以讓使用者成爲 **pdwebpi-mpa-servers** 群組的成員，來達成這個目的。
2. 用戶端連接至 MPA 閘道。
3. 閘道將要求轉換成 HTTP 要求。
4. 閘道鑑定用戶端。
5. 閘道使用用戶端要求建立與外掛程式的連線。

6. MPA 會向外掛程式鑑定（使用與用戶端不同的方法），並且會取得 MPA 的身份（已有外掛程式帳戶）。
7. 外掛程式驗證 **pdwebpi-mpa-servers** 群組中的 MPA 成員資格。
8. 建立了 MPA 證明，並在快取中標示爲特殊 MPA 類型。

   雖然此 MPA 證明伴隨每一個用戶端要求，但它並不用於對這些要求的授權檢查。
9. 現在，外掛程式必須進一步識別要求的擁有者。

   MPA 能夠區分多個用戶端，以適當地遞送登入提示。
10. 用戶端會登入，並且使用與 MPA 不同的鑑定方法來進行鑑定。
11. 外掛程式會根據用戶端的鑑定資料建立證明。
12. 每一個用戶端使用的階段作業資料類型必須與 MPA 所使用的不同。
13. Authorization Server 根據使用者證明和物件的 ACL 許可權，允許或拒絕存取受保護的物件。

啓用 MPA 鑑定

mpa-enabled 參數（位於 **pdwebpi.conf** 配置檔的 [pdweb-plugins] 段落中）可啓用或停用 MPA 鑑定。有效設定爲 *true* 及 *false*，分別用於啓用及停用 MPA 鑑定。根據預設值，MPA 鑑定是停用的。您可以爲個別虛擬主機設定 MPA 鑑定，方法爲在配置檔的 [*virtual_host*] 段落中指定 **mpa-enabled** 參數。

若要將新的階段作業識別爲 MPA 所建立的主要階段作業，將做出一個授權決策，測試 MPA 保護的物件上是否有 Proxy ([PDWebPI]p) 許可權。根據預設值，MPA 保護的物件會定義爲 /PDWebPI。若要置換這個預設設定，例如，若要定義不同的主體集來代表每一個虛擬主機的 MPA，則可以對 **mpa-protected-object** 配置參數指定一值。您可以對每一個虛擬主機置換這個參數，方法爲在配置檔的 [*virtual_host*] 段落中指定它的值。例如，若要啓用 ibm.com 虛擬主機，但不是 lotus.com 虛擬主機的 MPA 存取權，請在 pdwebpi.conf 配置檔中使用下列設定：

```
[pdmweb-plugins]
virtual-host = ibm.com
virtual-host = lotus.com

[ibm.com]
mpa-enabled = yes
```

若要爲 ibm.com 虛擬主機的要求，將 ibm-mpa-servers 群組的成員定義爲 MPA，以及爲 lotus.com 虛擬主機的要求，將 lotus-mpa-servers 群組定義爲 MPA，請使用下列配置：

```
[pdweb-plugins]
virtual-host = ibm.com
virtual-host = lotus.com

[ibm.com]
mpa-enabled = yes
mpa-protected-object = /PDWebPI/ibm.com

[lotus.com]
mpa-enabled = yes
mpa-protected-object = /PDWebPI/lotus.com
```

並定義下列 Tivoli Access Manager 原則：

```
pdadmin> acl create ibm-mpa
pdadmin> acl modify ibm-mpa set group ibm-mpa-servers T[PDWebPI]p
pdadmin> acl create lotus-mpa
pdadmin> acl modify lotus-mpa set group lotus-mpa-servers T[PDWebPI]p
pdadmin> acl attach /PDWebPI/ibm.com ibm-mpa
pdadmin> acl attach /PDWebPI/lotus.com lotus-mpa
```

mpa-protected-object 配置參數指定在做出授權決策時所對照的物件。

為 MPA 建立使用者帳戶

請參閱 *IBM Tivoli Access Manager Base Administration Guide* 及 *IBM Tivoli Access Manager Web Portal Manager Administration Guide*，以取得如何建立使用者帳戶的相關資訊。

新增 MPA 帳戶至 pdwebpi-mpa-servers 群組

Tivoli Access Manager Plug-in for Web Servers 會建立一個易於管理 MPA 伺服器的群組。這個群組稱之爲 **pdwebpi-mpa-servers**。連接至 /PDWebPI 的 default-pdwebpi ACL 會授與 Proxy ([PDWebPI]p) 許可權給 **pdwebpi-mpa-servers** 群組的成員。當安裝在已配置至少一個 WebSEAL 的 Tivoli Access Manager 安裝網域時，將配置 default-pdwebpi ACL，以便它也授與 Proxy 許可權給 **webseal-servers** 及 **webseal-mpa-servers** 群組的成員。您可以選擇自己的群組及 ACL，以用來控制作爲「多工 Proxy 代理站」之主體的識別。

請參閱 *IBM Tivoli Access Manager Base Administration Guide* 及 *IBM Tivoli Access Manager Web Portal Manager Administration Guide*，以取得關於管理群組的資訊。

第 5 章 IBM Tivoli Access Manager Plug-in for Web Servers 安全原則

本章含有的資訊用以說明如何配置及自訂 IBM Tivoli Access Manager (Tivoli Access Manager) Plug-in for Web Servers 安全原則。

主題索引：

外掛程式特有的存取控制清單 (ACL) 原則

下列安全考量適用於受保護的物件空間中的 `/PDWebPI`：

- Tivoli Access Manager Plug-in for Web Servers 物件起始物件空間之外掛程式區域的 ACL 繼承鏈。
- 如果您不套用其他明確的 ACL，則這個物件會定義（透過繼承）整個 Web 空間的安全原則。
- 存取此物件及此點以下的任何物件都需要遍訪許可權。

請參閱 *IBM Tivoli Access Manager Base Administrator's Guide*，以取得有關 Tivoli Access Manager ACL 原則的完整資訊。

註: Microsoft IIS Web 伺服器可讓您在目錄內指定一個預設網頁，當使用者要求含有一個僅包括目錄路徑的 URL 時，就會顯示這個網頁。

由 Plug-in for Web Servers 執行的 ACL 檢查僅適用於要求 URL 中指定的目錄，不適用於 IIS 在回應這個要求時所服務的預設網頁。

在 IIS 平台上實作您的安全原則時，您應該納入這個 ACL 檢查限制。

/PDWebPI/host 或 virtual_host

/PDWebPI/*host* 或 *virtual_host* 子目錄樹含有特殊外掛程式實例的物件空間。下列安全考量適用於此物件：

- 存取此點以下的任何物件都需要遍訪權。
- 如果您不套用其他任何明確的 ACL，則這個物件定義（透過繼承）此機器上整個物件空間的安全原則。

外掛程式 ACL 許可權

下表說明適用於物件空間之 Tivoli Access Manager Plug-in for Web Servers 區域的 ACL 許可權：

表 21. 外掛程式 ACL 許可權

許可權	作業	說明
[PDWebPI]**r**	讀取	檢視目錄以外的任何元素。任何 HTTP GET 或 POST 要求都需要這個許可權。沒有特定的「列示」權，可要求目錄列示（以 / 結尾的 URL 的 GET）。
[PDWebPI]**d**	刪除	從 Web 空間中移除 Web 物件。HTTP DELETE 指令需要這個許可權。
[PDWebPI]**m**	修改	在外掛程式物件空間中放置/發佈 HTTP 物件。 HTTP PUT 要求需要這個許可權。
[PDWebPI]**p**	proxy	判定使用者是否可以充當「多工 Proxy」代理站。請參閱第 74 頁的『新增 MPA 帳戶至 pdwebpi-mpa-servers 群組』，以取得詳細資訊。
T	遍訪	存取此點以下的任何物件都需要它。

外掛程式也支援底下所顯示的 WebDAV 作業。

表 22. 外掛程式 WebDAV 許可權

作業	必要的許可權
PROPFIND	[PDWebPI]**R**
PROPPATCH	[PDWebPI]**M**
MKCOL	[PDWebPI]**N**

WebDAV 作業是根據要求 URI 來授權 – 不是根據集合的個別成員。此外，也部份支援一些其他 WebDAV 作業：

- **COPY** - 集合上需要 [PDWebPI]**R**，以便可以讀取「複製來源」。不會檢查目標的許可權。
- **MOVE** - 這視爲先複製再刪除。在要從中移動的集合上需要 [PDWebPI]**Rd**。不會檢查目標的許可權。

預設 /PDWebPI ACL 原則

Tivoli Access Manager Plug-in for Web Servers ACL (**default-pdwebpi**) 的核心項目包括：

```
群組 iv-admin                    Tcmdbva[PDWebPI]rmdNRM
使用者 sec_master                Tcmdbva[PDWebPI]rmdNRM
其他                             [PDWebPI]rR
未經鑑定                         T
群組 pdwebpi-mpa-servers         T[PDWebPI]p
群組 webseal-servers             T[PDWebPI]p
群組 webseal-mpa-servers         T[PDWebPI]p
```

安裝時，此預設 ACL 會連接到物件空間的 /PDWebPI 配置區物件。

遍訪權容許擴增 Web Portal Manager 中代表的 Web 空間。列示許可權可讓 Web Portal Manager 顯示 Web 空間的內容。

三振登入原則

用於 LDAP 型 Tivoli Access Manager 安裝的三振登入原則可讓您阻止電腦密碼攻擊，方法爲指定登入失敗嘗試次數上限以及懲罰鎖定時間。此原則建立一個條件，即使用者必須等候一段時間，然後才能進行更多原先失敗的登入嘗試。例如，原則可能會指定 3 次失敗嘗試後，有 180 秒的懲罰。 這種類型的登入原則可防止一秒內發生多次的電腦隨機產生的登入嘗試。

三振登入原則需要兩個 **pdadmin** policy 指令設定的結合作用：

- 登入失敗嘗試次數上限
  policy set max-login-failures
- 超出失敗登入嘗試設定的懲罰
  policy set disable-time-interval
  懲罰設定可併入帳戶鎖定時間間隔或完全停用帳戶。

如果設定了在三次失敗嘗試之後採取特定的鎖定時間懲罰之登入原則（如範例），則第四次的嘗試（不論正確或不正確）將會導致一個錯誤頁，指出由於密碼原則而暫時無法使用帳戶。

時間間隔是以秒數指定 - 建議的最小時間間隔爲 60 秒。

如果 **disable-time-interval** 原則設爲 disable，則使用者會被鎖定無法存取帳戶，且此使用者的 LDAP **account valid** 屬性會設爲 no。管理者可透過 Web Portal Manager 重新啓用帳戶。

註: 將 **disable-time-interval** 設爲 disable 會導致額外的管理成本。您可觀察將**有效帳戶**資訊抄寫到外掛程式時的延遲。這種情況取決於您的 LDAP 環境。此外，**有效帳戶**更新作業會導致某些 LDAP 實作可能遇到效能退化。基於此原因，建議您使用逾時間隔。

下列 **pdadmin** 指令僅適合與 LDAP 登錄一起使用。

表 23. pdadmin LDAP 登入原則指令

指令	說明
policy set max-login-failures {*number***|unset} [-user** *username***]**	
policy get max-login-failures [-user *username***]**	
	管理強制實施懲罰之前控制登入失敗嘗試次數上限的原則。這個視 policy set disable-time-interval 指令中設定的懲罰而定。 身爲一位管理者，您可將此原則套用至特定的使用者，或將此原則整體套用至 LDAP 登錄中所列示的所有使用者。 預設設定爲 10 次嘗試。
policy set disable-time-interval {*number***|unset|disable} [-user** *username***]**	
policy get disable-time-interval [-user *username***]**	
	管理懲罰原則，這個原則控制在到達登入失敗嘗試次數上限時，應停用帳戶的時期。 身爲一位管理者，您可將此懲罰原則套用至特定的使用者，或將此原則整體套用至 LDAP 登錄中所列示的所有使用者。 預設設定爲 180 秒。

密碼強度原則

Tivoli Access Manager LDAP 型安裝作業提供兩種控制密碼建構的方法：

- 五個 **pdadmin** 密碼原則指令
- 可外掛的鑑定模組（PAM），其可讓您自訂密碼原則

  請參閱 *Tivoli Access Manager Authorization C API Developer's Reference*

pdadmin 公用程式所設定的密碼強度原則

透過 **pdadmin** 公用程式實作的五個密碼強度屬性包括：

- 最小密碼長度
- 最小英文字母
- 最小非英文字母
- 最大重複字元
- 容許的空格

當您以 **pdadmin** 或 Web Portal Manager 建立使用者，以及以 **pdadmin**、Web Portal Manager 或 **pkmspasswd** 公用程式變更密碼時，會強制這些原則。

下列 pdadmin 指令僅適合與 LDAP 登錄一起使用。 unset 選項會停用這個原則屬性 – 亦即，不強制該原則。

表 24. pdadmin LDAP 密碼強度指令

指令	說明
policy set min-password-length {*number***|unset} [-user** *username***]**	
policy get min-password-length [-user *username***]**	
	管理其控制最小密碼長度的原則。 身爲一位管理者，您可將此原則套用至特定的使用者，或將此原則整體套用至預設登錄中所列示的所有使用者。 預設設定爲 8。
policy set min-password-alphas {*number***|unset} [-user** *username***]**	
policy get min-password-alphas [-user *username***]**	
	管理其控制在密碼中容許的最小英文字母數的原則。 身爲一位管理者，您可將此懲罰原則套用至特定的使用者，或將此原則整體套用至預設登錄中所列示的所有使用者。 預設設定爲 4。
policy set min-password-non-alphas {*number***|unset} [-user** *username***]**	
policy get min-password-non-alphas [-user *username***]**	
	管理其控制在密碼中容許的最小非英文字母（數字）數的原則。 身爲一位管理者，您可將此原則套用至特定的使用者，或將此原則整體套用至預設登錄中所列示的所有使用者。 預設設定爲 1。
policy set max-password-repeated-chars {*number***|unset} [-user** *username***]**	
policy get max-password-repeated-chars [-user *username***]**	
	管理其控制在密碼中容許的最大重複字元數的原則。 身爲一位管理者，您可將此原則套用至特定的使用者，或將此原則整體套用至預設登錄中所列示的所有使用者。 預設設定爲 2。
policy set password-spaces {yes|no|unset} [-user *username***]**	
policy get password-spaces [-user *username***]**	
	管理其控制密碼是否可包含空格的原則。 身爲一位管理者，您可將此原則套用至特定的使用者，或將此原則整體套用至預設登錄中所列示的所有使用者。 預設設定爲未設定。

下表說明以五個 pdadmin 參數之預設值爲基礎的數個密碼範例和原則結果：

表 25. 密碼範例

範例	結果
密碼	無效：必須至少包含一個非英文字母。
pass	無效：必須至少包含 8 個字元。
passs1234	無效：包含兩個以上的重複字元。
12345678	無效：必須至少包含 4 個英文字母。
password3	有效。

特定使用者和廣域設定

pdadmin policy 指令可以針對特定使用者（利用 - user 選項）或廣域（不使用 - user 選項） 來加以設定。任何使用者特有的設定都會置換原則的整體設定。您也可以停用 (unset) 原則參數，表示該參數不含任何值。帶有 unset 選項的任何原則都不會被檢查及強制。

例如：

```
pdadmin> policy set min-password-length 8
pdadmin> policy set min-password-length 4 -user matt
pdadmin> policy get min-password-length
最小密碼長度：8
pdadmin> policy get min-password-length -user matt
最小密碼長度：4
```

使用者 matt 具有 4 個字元的最小密碼長度原則；其他所有的使用者具有 8 個字元的最小密碼長度原則。

```
pdadmin> policy set min-password-length unset -user matt
```

現在，使用者 matt 受限於 8 個字元的整體最小密碼長度原則。

```
pdadmin> policy set min-password-length unset
```

現在，包括 matt 在內的所有使用者都沒有最小密碼長度原則。

鑑定強度的受保護的物件原則（進階）

鑑定強度的「受保護的物件原則」(POP) 使您可以根據它們使用的鑑定方法來控制物件的存取。

您可使用這項功能（有時又稱爲進階鑑定）來確保使用者使用較強的鑑定機制存取較機密的資源。您可以在特定資源有較大的威脅時使用這個條件。

例如，您可對 Web 空間的區域提供更高的安全性，方法爲套用其鑑定層次高於起始進入 WebSEAL 網域時使用的用戶端的進階 POP 原則。

進階鑑定也可以針對 Web 伺服器上每一個特定虛擬主機來加以設定，以容許個別虛擬主機攜帶它們自己的進階層次的鑑定，不受全伺服器原則實作的管制。

鑑定強度原則是在 POP 原則的「IP 端點鑑定方法」屬性中設定

配置進階授權的層次

配置鑑定特有的存取權限的第一個步驟是配置支援的鑑定方法，並決定考慮加強這些鑑定方法的順序。 請參閱第 35 頁的第 4 章, 『IBM Tivoli Access Manager Plug-in for Web Servers 鑑定』，以取得如何配置鑑定機制的詳細資訊。

任何透過外掛程式存取 Web 伺服器的用戶端都有一個鑑定層次，例如「未經鑑定」或「密碼」，其指出前次透過外掛程式來鑑定用戶端的方法。

在某些情況下，您可能必須採行存取特定資源時所需要的最低「安全」層次。例如，在某個環境中，使用記號密碼進行鑑定可會被視爲比以使用者名稱和密碼進行鑑定更爲安全。另一個環境可能具有不同的標準。

當用戶端不符合所需的鑑定層次時，進階鑑定機制並不會強制用戶端重新啓動它們的階段作業，而是提供用戶端第二次機會使用必要的方法（層次）重新鑑定。

進階鑑定方法表示，當使用者嘗試存取需要「較高」鑑定層次（高於其登入的層次）時，不會馬上看到「拒絕」訊息。相反的，會有一個新的鑑定提示呈現給使用者，要求支援較高鑑定層次的資訊。 如果他們能夠提供此鑑定層次，則將會允許其原始要求。

您可在 `pdwebpi.conf` 配置檔的 **[authentication-levels]** 或 **[authentication-levels:***virtual_host_label***]** 段落中配置鑑定層次。例如：

```
[authentication-levels]
1 = BA
2 = iv-headers
3 = cert
```

根據方法在清單中的順序，指定一個層次索引給每一種方法。

- 未經鑑定的層次假設爲 0。
- 您可以任何順序來放置後續的方法。 請參閱第 82 頁的『進階鑑定注意事項和限制』
- 至少必須有兩個項目才能啓用進階鑑定。
- 鑑定機制的層次可以針對特定虛擬主機來加以設定，方法爲使用具有下列格式的段落來指定層次：**[authentication-levels:***virtual_host_name***]**

註: 關於設定必要的鑑定機制之詳細資訊，請參閱第 35 頁的第 4 章, 『IBM Tivoli Access Manager Plug-in for Web Servers 鑑定』。

啓用進階鑑定

進階鑑定是使用置於需要區分鑑定授權之物件上的 POP 原則來實作。您可使用 POP 原則的「IP 端點鑑定方法」屬性。

pdadmin pop modify set ipauth 指令可指定 **IP 端點鑑定方法**屬性容許的網路以及必要的鑑定層次。

經配置的鑑定層次可鏈結至 IP 位址範圍。 這個方法的目的在提供管理彈性。如果依 IP 位址過濾使用者不重要，則您可對 **anyothernw**（其他任何網路）設定單一項目。這項設定將會影響所有的存取使用者（無論 IP 位址爲何），並要求他們在指定的層次鑑定。這是實施進階鑑定最常用的方法。

語法：

```
pdadmin> pop modify pop_name set ipauth anyothernw level_index
```

anyothernw 項目用來作爲一個將會符合除 POP 中指定的網路外的任何網路之網路範圍。 這個方法是用來建立預設項目，以拒絕所有不符合的 IP 位址，或是容許符合鑑定層次需求的任何使用者進行存取動作。

根據預設值，**anyothernw** 以鑑定層次索引 0 出現在 POP 中。此項目以「任何其他的網路」出現在 **pop show** 指令中：

```
pdadmin> pop show test
       受保護物件的原則：  test
       說明：  Test POP
       警告：  無
       審核層次：  無
       保護品質：  無
       存取日期時間：星期日、星期一、星期二、星期三、星期四、星期五、星期六：
            隨時：當地
       IP 端點鑑定方法原則
           任何其他的網路 0
```

範例

1. 在 pdwebpi.conf 中配置鑑定層次：

   ```
   [authentication-levels] 或 [authentication-levels:virtual_host_label]
   1 = BA
   2 = token
   ```

2. 配置「IP 端點鑑定方法 POP」屬性：

   ```
   pdadmin> pop modify test set ipauth anyothernw 2
   pdadmin> pop show test
          受保護的物件原則：  test
          說明：  Test POP
          警告：  無
          審核層次：  無
          保護品質：  無
          存取日期時間：星期一、星期三、星期五：任何時間：當地
          IP 端點鑑定方法原則
              任何其他的網路 2
   ```

   因此，存取測試 POP 所保護之物件的使用者需要層次 2 鑑定，或將被迫利用記號方法來進行鑑定。
   另請參閱第 84 頁的『網路型鑑定的受保護的物件原則』。

進階鑑定注意事項和限制

- 進階鑑定可透過 HTTP 和 HTTPS 支援。
- 您無法從 HTTP 協定進階至 HTTPS。
- 未在 **[authentication-levels]** 段落中指定的鑑定方法將預設爲層次 1。
- 鑑定方法僅能在層次清單中指定一次。
- SPNEGO 不會進階至任何使用 POST 套表的鑑定。使用 SPNEGO 鑑定模組配置進階行爲會導致一個錯誤頁面傳回給用戶端。
- 進階鑑定層次的不正確配置會導致停用外掛程式內的進階功能。此狀況會導致非預期的鑑定行爲，例如爲受 POP 保護的物件所發出的密碼登入頁面，會要求使用記號通行代碼鑑定方法。

  在配置了進階鑑定機制後，請檢查 pdwebpi.log 檔，看看是否有回報任何配置錯誤。

重新鑑定的受保護的物件原則

Tivoli Access Manager Plug-in for Web Servers 可以強制使用者執行額外的登入（重新鑑定)，以確保存取受保護資源的使用者和階段作業開始時鑑定的是同一人。重新鑑定可以由受保護物件上的「受保護的物件原則 (POP)」或超過階段作業快取無活動逾時值的方式來啓動。本節根據 POP 延伸屬性指定的安全原則來討論重新鑑定。請參閱第 46 頁的『配置外掛程式階段作業/證明快取』，以取得如何配置「階段作業/證明快取」的詳細資訊。

影響 POP 重新鑑定的條件

強制的重新鑑定提供安全網域中敏感性資源的額外保護。基於安全原則的重新鑑定方式，是由保護要求資源物件的 POP 中的特定延伸屬性來啓動。POP 可以直接連接在物件，或者物件可以繼承上層物件的 POP 條件。下列的外掛程式鑑定方法支援重新鑑定：

- 套表式（使用者名稱和密碼）鑑定
- 記號鑑定

此外，可以寫入自訂使用者名稱/密碼 CDAS 以支援重新鑑定。

重新鑑定假設使用者初始時已登入安全網域，而且使用者存在有效的證明。在重新鑑定時，使用者必須以產生現有證明的相同身份來登入。Tivoli Access Manager 會在重新鑑定期間保留使用者原來的階段作業資訊，包括證明。重新鑑定時，證明不會被取代。

重新鑑定時，外掛程式也會快取提示重新鑑定的要求。當順利完成重新鑑定時，快取的資料會用來重新建置要求。

如果重新鑑定失敗，外掛程式會重新傳回登入提示。如果重新鑑定成功，但是該資源的 ACL 檢查失敗，則會傳回 403「禁止存取」訊息並拒絕使用者存取要求的資源。在任一種情況下，使用者都不會登出。利用仍然有效的證明，使用者可以結束重新鑑定處理程序（要求另一個 URL)，並且可以存取不需要重新鑑定的其它資源而仍然可參與安全網域。

建立和套用重新鑑定 POP

根據安全原則的強制重新鑑定配置是藉由使用名稱爲 ″reauth″ 的特殊延伸屬性來建立受保護的物件原則 (POP)。您可以連接此 POP 到需要強制重新鑑定所提供之額外保護的任何物件。

請記得所有具備 POP 的物件的所有子項也會繼承 POP 條件。每一個要求的子物件都需要個別的重新鑑定。

使用 **pdadmin pop create**、**pdadmin pop modify** 和 **pdadmin pop attach** 指令。下列範例說明使用 reauth 延伸屬性建立名稱爲 ″secure″ 的 POP，並將它連接到物件：

```
pdadmin>pop create secure
pdadmin>pop modify secure set attribute reauth true
pdadmin>pop attach /PDWebPI/hostA/budget.html secure
```

任何人嘗試存取 budget.html 都會使用與產生現存證明相同的身份和鑑定方法來強制重新鑑定。

如果使用者要求資源是未經鑑定，POP 會強制使用者進行鑑定。每次存取重新鑑定原則所保護的物件時，都需要重新鑑定。

在目錄中大部份但非全部物件需要重新鑑定的狀況中，最好將 POP 連接至整個目錄，包括 ″reauth″ 延伸屬性。對於那些不需要重新鑑定的物件，連接與目錄的 POP 相同的 POP，但不包括 ″reauth″ 延伸屬性。

有關 **pdadmin** 指令行公用程式的詳細資訊可在 *IBM Tivoli Access Manager Base Administrator's Guide* 中找到。

網路型鑑定的受保護的物件原則

網路型鑑定的「受保護的物件原則 (POP)」使您可依據使用者的 IP 位址來控制物件的存取。您可使用這個功能來防止特定的 IP 位址（或 IP 位址範圍）存取您安全網域內的任何資源。

您也可以將進階鑑定配置套用到此原則，以及對每一個指定的 IP 位址範圍要求特定的鑑定方法。

網路型鑑定原則設定於 POP 原則的「IP 端點鑑定方法」屬性中。 您必須在此屬性中指定兩個基本要求：

- 鑑定層次
- 容許的網路

如需指定配置層次的詳細資訊，請參閱第 81 頁的『配置進階授權的層次』

指定 IP 位址與範圍

在配置鑑定層次之後，您必須指定此 POP 原則容許的 IP 位址與 IP 位址範圍。

pdadmin pop modify set ipauth add 指令指定「IP 端點鑑定方法」屬性中的網路（或網路範圍）和必要的鑑定層次。

語法：

```
pdadmin> pop modify pop_name set ipauth add network netmask level_index
```

配置的鑑定層次鏈結至 IP 位址範圍。 這個方法的目的在提供彈性。 如果依 IP 位址過濾使用者不重要，則您可設定 **anyothernw**（其他任何網路）的單一項目。這項設定會影響所有的存取使用者（無論 IP 位址爲何），並需要他們在指定的層次鑑定。

語法：

```
pdadmin> pop modify pop_name set ipauth anyothernw level_index
```

反之，如果您想要忽略鑑定層次且只想依據 IP 位址來容許或拒絕，您就可以在想容許的範圍上使用層次 0，並針對您想拒絕的範圍使用 ″forbidden″。

anyothernw 項目用來作爲一個將會符合除 POP 中指定的網路外的任何網路之網路範圍。這個方法可用來建立預設項目，以拒絕所有不符合的 IP 位址，或是容許符合鑑定層次需求的任何使用者進行存取動作。

根據預設值，**anyothernw** 以鑑定層次索引 0 出現在 POP 中。此項目以「任何其他的網路」出現在 **pop show** 指令中：

```
pdadmin> pop show test
       受保護的物件原則：  test
       說明：  Test POP
```

```
警告：  無
審核層次：  無
保護品質：  無
存取日期時間：星期日、星期一、星期二、星期三、星期四、星期五、星期六：
      隨時：當地
IP 端點鑑定方法原則
     任何其他的網路 0
```

請參閱第 81 頁的『配置進階授權的層次』，以取得關於設定鑑定層次的詳細討論。

範例

需要來自 IP 位址範圍 9.0.0.0 及網路遮罩 255.0.0.0 的使用者使用層次 1 的鑑定（預設爲「密碼」）：

```
pdadmin> pop modify test set ipauth add 9.0.0.0 255.0.0.0 1
```

要求特定的使用者使用層次 0 鑑定：

```
pdadmin> pop modify test set ipauth add 9.1.2.3 255.255.255.255 0
```

防止所有的使用者（在上述範例中指定的使用者除外）存取物件：

```
pdadmin> pop modify test set ipauth anyothernw forbidden
```

以 IP 位址停用進階鑑定

語法：

```
pdadmin> pop modify pop_name set ipauth remove network netmask
```

例如：

```
pdadmin> pop modify test set ipauth remove 9.0.0.0 255.0.0.0
```

網路型鑑定演算法

Tivoli Access Manager Plug-in for Web Servers 使用以下演算法來處理 POP 中的狀況：

1. 檢查 POP 上的 IP 端點鑑定方法原則。
2. 檢查 ACL 許可權。
3. 檢查 POP 上的日期時間原則。
4. 檢查 POP 上的審核層次原則。

保護品質的受保護的物件原則

保護品質的「受保護的物件原則 (POP)」屬性可讓您指定在對物件執行作業時，需要什麼層次的資料保護。

```
pdadmin> pop modify pop_name set qop {none|integrity|privacy}
```

表 26. QOP level descriptions

QOP 層次	說明
privacy	資料加密是必要的 (SSL)。
integrity	使用某些機制來確保資料未變更。
none	不使用任何資料保護方法。

例如：

```
pdadmin> pop modify test set qop privacy
```

當 ACL 決策的 ″yes″ 回應也包含必要的保護品質層次時，保護品質 POP 屬性容許單一異動。如果外掛程式無法保證提供必要的保護層次，要求就會被拒絕。

處理未經鑑定的使用者 (HTTP/HTTPS)

Tivoli Access Manager Plug-in for Web Servers 接受經過鑑定及未經鑑定使用者透過 HTTP 和 HTTPS 發出的要求。隨後，外掛程式會依賴 Authorization Server，藉由允許或拒絕對受保護的資源之存取，來施行安全原則。

下列狀況適用於透過 SSL 存取的未經鑑定使用者：

- 對未經鑑定使用者與外掛程式之間的資訊交換加密 – 作法就如同對經過鑑定的使用者所做一般。
- 未經鑑定使用者與外掛程式之間的 SSL 連線只需要伺服器端鑑定。

處理匿名用戶端所發出的要求

1. 匿名用戶端會透過外掛程式（使用 HTTP 或 HTTPS）對 Web 伺服器發出要求。
2. 外掛程式爲這個用戶端建立未經鑑定的證明。
3. 要求連同此證明傳送至受保護的 Web 物件。
4. Authorization Server 會檢查在 ACL 的未經鑑定項目上是否有此物件的許可權，然後允許或拒絕所要求的作業。
5. 是否能順利存取此物件，視至少包含讀取權 (r) 的未經鑑定 ACL 項目而定。
6. 如果要求無法通過授權決定，用戶端會收到一份登入套表（BA 或「套表型」）。

強制使用者登入

您可強制未經鑑定的使用者登入，方法爲對保護所要求的物件之 ACL 原則中的未經鑑定項目設定適當的許可權。

讀取 [PDWebPI]**r** 許可權容許對物件進行未經鑑定的存取。

若要強制未經鑑定的使用者登入，請從保護該物件之 ACL 原則中的未經鑑定項目中，移除讀取 [PDWebPI]**r** 許可權。

套用未經鑑定的 HTTPS

有很多實際商業理由用以支援透過 HTTPS 對外掛程式強化的 Web 伺服器進行未經鑑定的存取：

- 某些應用程式不需要個人登入，但需要敏感資訊，例如地址和信用卡號碼。舉例而言，包括線上購買機票及其他商品。
- 某些應用程式會要求您先向公司登記帳戶，然後才能進行進一步的交易。 敏感資訊又再度必須通過網路。

以 ACL/POP 原則控制未經鑑定的使用者

註: ″any-other″ 項目類型也稱爲 ″any-authenticated″ 項目類型。

1. 若要允許未經鑑定使用者存取公用物件，請以至少包含對未經鑑定及 any-other 項目的讀取 [PDWebPI]**r** 許可權的 ACL 來保護公用內容：

```
unauthenticated [PDWebPI]r
any-other [PDWebPI]r
```

註: **unauthenticated** 項目是一個根據 **any-other** 項目來判定許可權的遮罩（按位元 ″and″ 作業）。只有當 **unauthenticated** 許可權也出現在 **any-other** 項目中時，才會授與該許可權。由於 **unauthenticated** 取決於 **any-other**，因此，如果 ACL 包含 **unauthenticated** 但不包含 **any-other**，就不大合乎邏輯了。如果 ACL 包含 **unauthenticated** 但不包含 **any-other**，預設回應就是不授與許可權給 **unauthenticated**。

2. 若要要求加密 (SSL)，請以指定私密性爲條件的「受保護的物件原則（Protected Object Policy, POP）」來保護內容。
   請參閱第 85 頁的『保護品質的受保護的物件原則』。

第 6 章 Web 單一登入解決方案

將 Tivoli Access Manager Plug-in for Web Servers 當作授權服務程式來實作，以便爲安全網域提供保護時，您通常必須提供該網域內資源的單一登入解決方案。本章討論 Tivoli Access Manager Plug-in for Web Servers 保護的 Web 空間單一登入解決方案。

主題索引：

單一登入概念

當受保護的資源位於外掛程式強化的 Web 應用程式伺服器上時，若要在存取不同安全應用程式時，執行多個登入，需要一個要求該資源的用戶端。每一個登入可能都需要不同的登入身份。

管理及維護多個登入身份的問題經常可以單一登入 (SSO) 機制獲得解決。 SSO 容許使用者僅使用起始的登入，就可以存取資源。 Web 伺服器上資源的任何進一步登入需求在處理時，使用者是看不到的。

Tivoli Access Manager Plug-in for Web Servers 支援若干不同的單一登入架構。如下：

1. 提供單一登入給伺服器上多個安全應用程式的外掛程式實例。
2. 從 WebSEAL 或其他 proxy 代理站（如 WAP 閘道）單一登入至外掛程式。
3. 使用失效接替 cookie 來提供不同網域之間的單一登入。
4. 使用「廣域單一登入 (GSO)」鎖定框模組，利用儲存的使用者證明資訊來提供應用程式的存取。
5. 使用「安全提供者 NEGOtiation (SPNEGO)」，允許存取 IIS 型 Web 伺服器上的資源。
6. 電子社群單一登入，在這裡使用者會鑑定一次，並發給他一個記號，以允許他們存取虛擬網域社群內的其他網域，不需要重新鑑定。

最先五個 SSO 實務範例會在本章中加以討論。第六個實務範例是下一章的主題。

自動登入至安全的應用程式

HTTP 標頭及 LTPA cookie（當應用程式是 WebSphere Application Server 時）可用來完成伺服器上受到某個外掛程式保護之應用程式的 SSO。

在起始鑑定用戶端後，外掛程式可以建置一個含有用戶端識別資訊的 HTTP 標頭，這個識別資訊可用於自動鑑定，以保護伺服器上執行的應用程式。利用同樣的方式，您可使用 LTPA cookie 來完成 Web 應用程式伺服器（如 WebSphere）的 SSO。

配置單一登入以使用 HTTP 標頭來保護應用程式

用於登入至應用程式的 HTTP 標頭是由 iv-header 後置授權模組所產生的。可產生的標頭集統稱爲 IV 標頭。

在順利地授權使用者要求後，外掛程式可以將定義用戶端之身份的 IV 標頭，插入由應用程式處理的要求。當安全 Web 伺服器掌控的應用程式處理要求時，這個標頭資訊可作爲使用者身份的證明。因此，可以免除使用者每次存取新應用程式時都要登入的需求。

針對後置授權處理程序而配置的 IV 標頭，會與一個、一些或所有 iv-user、iv-user-l、iv-creds、iv-remote-address HTTP 標頭一起插入。下表將說明這些標頭類型。

表 27. IV 標頭欄位說明

IV 標頭欄位	說明
iv-user	Tivoli Access Manager 使用者的簡稱。如果用戶端是未經鑑定（不明），將預設爲 unauthenticated。
iv-user-l	使用者的完整網域名稱（長套表），例如，LDAP 識別名稱。
iv-groups	使用者所屬的群組清單。
iv-creds	已編碼的不透明資料結構，代表使用者的 Tivoli Access Manager 證明。
iv-remote-address	用戶端的 IP 位址。 此值可能代表 Proxy 伺服器或網路位址轉換器 (NAT) 的 IP 位址。

啓用及停用產生 IV 標頭

若要啓用外掛程式，將 IV 標頭插入已獲授權的要求，需要配置外掛程式以使用 IV 標頭來進行後置授權處理程序。 pdwebpi.conf 配置檔中的 **[common-modules]** 段落定義如何使用所有鑑定方法。若要啓用 IV 標頭進行後置授權處理程序，請在 pdwebpi.conf 配置檔中的 **[common-modules]** 段落中，將參數 **post-authzn** 指定爲關鍵字值 *iv-headers*。亦即：

```
[common-modules]
post-authzn = iv-headers
```

配置 IV 標頭參數

IV 標頭鑑定參數是配置在 pdwebpi.conf 配置檔的 **[iv-headers]** 段落中。

generate 參數指定當轉遞 proxy 要求時將產生的 IV 標頭類型。根據預設值，當轉遞 proxy 要求時，外掛程式將產生所有類型的 IV 標頭。有效選項爲 all、iv-creds、iv-user、iv-user-l 及 iv-remote-address。若要輸入多個標頭類型，請以逗點隔開值。

例如：

```
[iv-headers]
generate = iv-creds,iv-user,iv-user-l
```

使用 LTPA cookie 單一登入至 WebSphere 應用程式伺服器

當外掛程式安裝爲 WebSphere 應用程式伺服器上的保護層時，存取用戶端時會面對兩個可能的登入點 – WebSphere 所服務的外掛程式及安全應用程式。若要在這種情況中提

供單一登入點，您可以配置外掛程式，以產生並傳送 cookie 型輕裝備協力廠商鑑定 (LTPA) 機制至支援 LTPA cookie 的 Web 應用程式伺服器。

當使用者對伺服器上的資源做出要求時，使用者首先必須通過外掛程式的鑑定。在順利鑑定後，外掛程式就會產生代表使用者的 LTPA cookie。充當 Web 應用程式伺服器之鑑定記號的 LTPA cookie 含有使用者身份及密碼資訊。此資訊會使用外掛程式與應用程式伺服器間共用的密碼保護秘密金鑰來進行加密。

外掛程式會在傳送至 Web 應用程式伺服器之要求的 HTTP 標頭中插入 cookie。應用程式伺服器會收到要求，並且爲 cookie 解密，然後根據 cookie 所提供的身份資訊來鑑定使用者。

若要增進效能，外掛程式會在階段作業快取中儲存 LTPA cookie，並且在相同的使用者階段作業中，將儲存在快取中的 LTPA cookie 用於後續的要求。如需設定階段作業快取的參數的詳細資訊，請參閱第 46 頁的『配置外掛程式階段作業/證明快取』

使用 LTPA cookie 配置 WebSphere 的單一登入

使用 LTPA cookie 來完成支援 LTPA cookie 之應用程式伺服器的單一登入，是外掛程式的後置授權處理程序的一部份。若要啓用這個功能，請在 `pdwebpi.conf` 配置檔的 **[common-modules]** 段落中，將關鍵值 **ltpa** 輸入給參數 **post-authzn**；亦即：

```
[common-modules]
post-authzn = ltpa
```

LTPA cookie 配置是在 `pdwebpi.conf` 配置檔的 **[ltpa]** 段落中執行。下列參數需要配置。

表 28. LTPA 配置參數

參數	說明
ltpa-keyfile	用來爲 cookie 中所包含之身份資訊加密的金鑰檔的完整路徑名稱。
ltpa-stash-file	密碼隱藏檔案的位置。如果沒有密碼隱藏檔案存在，這個項目應該變成備註。
ltpa-password	當密碼隱藏檔案不存在時要使用的密碼。
ltpa-lifetime	LTPA cookie 的生命週期（以秒爲單位）。

LTPA 單一登入的技術注意事項

- 金鑰檔包含了特定 Web 應用程式伺服器的相關資訊。如果您新增多個應用程式伺服器至同一外掛程式，所有的伺服器會共用相同的金鑰檔。
- 若要讓單一登入成功，外掛程式與應用程式伺服器必須以某種方式來共用相同的登錄資訊。
- 應用程式伺服器會負責設定 LTPA 以及建立共用的秘密金鑰。

從 WebSEAL 或其他 proxy 單一登入至外掛程式

當外掛程式強化的 Web 伺服器從受信任的應用程式（如 WebSEAL 或多工 proxy 代理站）接收要求時， IV 標頭可插入已傳送至外掛程式的要求。 IV 標頭含有識別起源用戶端而不是傳送伺服器的資訊。標頭中的資訊是基於授權目的而用來建構起源用戶端證明。

如果您配置外掛程式，使用「IV 標頭」來執行用戶端鑑定，則外掛程式會使用從異動要求中找到的 IV 標頭擷取的身份，來建立一個用戶端證明。因爲用戶端容易僞造 IV 標頭，所以僅在鑑定要求中設定 'use secondary authenticator' 旗標，才建立如此的證明。

對於鑑定，您可以配置 IV 標頭，當透過 proxy 接收時，在要求中接受一個、一些或所有 iv-user、iv-user-l、iv-creds 或 iv-remote-address 標頭，作爲鑑定的證明。iv-remote-address 標頭是用來記錄使用者的眞正遠端位址。這些 IV 標頭類型是由 Tivoli Access Manager 及 WebSEAL 加以識別。

表 29. IV 標頭欄位說明

IV 標頭欄位	說明
iv-user	用戶端的簡稱。如果用戶端是未經鑑定（不明），將預設爲 unauthenticated。
iv-user-l	使用者的完整網域名稱（長套表）。
iv-groups	用戶端所屬的群組清單。
iv-creds	已編碼的不透明資料結構，代表 Tivoli Access Manager 證明。
iv-remote-address	用戶端的 IP 位址。 此值可能代表 Proxy 伺服器或網路位址轉換器 (NAT) 的 IP 位址。

爲了能夠當作用戶端身份的證明來接受，WebSEAL 或其他 proxy 本身必須通過外掛程式的鑑定。通常，這是透過外掛程式所保護的 proxy 與 Web 伺服器之間的互相鑑定 SSL 連線來完成。

使用 IV 標頭啓用及停用鑑定

pdwebpi.conf 配置檔中的 **[common-modules]** 段落定義如何使用所有鑑定方法。若要使用 IV 標頭啓用鑑定，請指定參照 'iv-header' 給 **authentication** 參數；亦即：

```
[common-modules]
authentication = iv-header
```

配置 IV 標頭參數

IV 標頭鑑定參數是配置在 pdwebpi.conf 配置檔的 **[iv-headers]** 段落中。

accept 參數指定執行 IV 標頭鑑定時所接受的 IV 標頭類型。根據預設值，外掛程式接受所有類型的 IV 標頭。有效選項爲 all、iv-creds、iv-user、iv-user-l 及 iv-remote-address。若要輸入多個標頭類型，請以逗點隔開值。

例如：

```
[iv-headers]
accept = iv-creds,iv-user
```

使用失效接替 cookie 進行單一登入

當配置失效接替 cookie 來進行後置授權處理程序時，外掛程式就會以伺服器特有的或全網域的 cookie 來加密用戶端的證明資料。當用戶端第一次連接時，此 cookie 會被放在瀏覽器中。當用戶端嘗試存取網域內的另一個安全伺服器時， cookie 會呈現至用戶端重新導向至的下一個伺服器。 cookie 是用於自動重新鑑定，所以會替用戶端省掉手動重新鑑定的作業。已抄寫之伺服器上的外掛程式會共用一個共同的金鑰，此金鑰是用來解密 cookie 中所保留的證明資訊，以建立新的階段作業。

註: 在外掛程式 4.1 版中已改進了產生失效接替 cookie 時的記號安全性。這些改進無法與 Tivoli Access Manager 3.9 記號編碼架構交互作業。若要繼續能夠與 3.9 Tivoli Access Manager Web Security 產品交互作業，請將 **[pdweb-plugins]** 段落中的 **pre-410-compatible-tokens** 配置參數設成 **true**。這個參數適用於整個處理程序，而且無法依照每一虛擬主機基礎來指定。

使用失效接替 cookie 啓用單一登入

您可以配置失效接替 cookie，來執行鑑定及後置授權作業。

爲了使用失效接替 cookie 進行後置授權處理程序而配置的外掛程式會加密證明，並將它儲存爲異動回應中的失效接替 cookie。

外掛程式（配置來使用失效接替 cookie 執行鑑定）會使用加密的證明（來自異動要求中找到的失效接替 cookie），來重新鑑定用戶端。

若要使用失效接替 cookie 來啓用 SSO，請在配置檔的 **[common-modules]** 段落中，指定參照「失效接替」給 **authentication** 及 **post-authzn** 參數；亦即：

```
[common-modules]
authentication = failover
post-authzn = failover
```

註: 當配置其他鑑定機制，以及失效接替 cookie 時，必須將失效接替 cookie 鑑定配置成起始鑑定方法。

配置失效接替 cookie 參數

失效接替 cookie 鑑定參數是配置在 pdwebpi.conf 配置檔的 **[failover]** 段落中。

failover-cookies-keyfile 參數指定用來在失效接替 cookie 中加密及解密證明資料的檔案。例如：

```
[failover]
failover-cookies-keyfile = failover.key
```

金鑰檔案必須使用程式 **pdwpi-cdsso-key-gen**（位於 *install_path*/bin 目錄）來加以建立。

用法：

```
./pdwpi-cdsso-key-gen key_file_name_to_create
```

failover-cookies-lifetime 參數定義 failover-cookie 的有效生命週期（以分鐘爲單位）。這是建立 cookie 及停用 cookie 之間的時間。預設值是 30 分鐘。

```
[failover]
failover-cookies-lifetime = 30
```

enable-failover-cookie-for-domain 參數啓用或停用整個網域內的 cookie 有效性。若要對網域內的所有伺服器完成 SSO，請將這個參數設爲 true。

例如：

```
[failover]
enable-failover-cookie-for-domain = true
```

使用廣域單一登入 (GSO)

您可以配置 Tivoli Access Manager Plug-in for Web Servers，授與使用者他們透過單一登入獲權使用之運算資源的存取權。GSO 係針對由異質、分散式運算環境內的多部系統和應用程式所組成之大型企業而設計，其消弭一般使用者管理多個使用者名稱和密碼之需。

若要建立 GSO 解決方案，必須先使用 Web 入口管理程式或 **pdadmin** 公用程式建立 Tivoli Access Manager GSO 資源及 GSO 資源群組。如需建立 GSO 資源及 GSO 資源群組的詳細資訊，請參閱 *IBM Tivoli Access Manager Base Administrator's Guide*。

在授權要求後，將呼叫「基本鑑定 (BA)」後置授權模組，來判定所要求的資源是否有可用的資源證明。資源證明是對映至每一個資源並儲存在使用者登錄的使用者名稱/密碼組合。 BA 後置授權模組會擷取適合於使用者及所要求之應用程式資源的資源證明，然後使用擷取的資源證明來建立「HTTP 基本鑑定」標頭，並將這個 BA 標頭新增至 HTTP 要求。資源證明僅擷取自第一個要求的使用者登錄，對於所有後續的要求，資源證明將當作階段作業資訊來擷取。

下圖說明如何使用 GSO 機制擷取後端應用程式資源之使用者名稱和密碼。

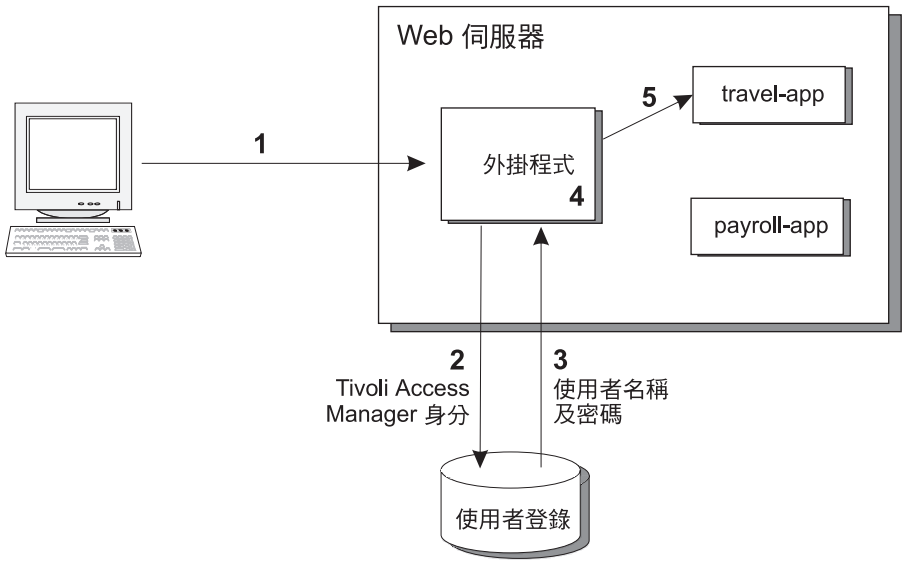

圖 7. 透過 GSO 保護應用程式的使用者存取權。

1. 使用者 Michael 要求受保護的後端 Web 伺服器應用程式 (*travel-app*) 的存取權。Tivoli Access Manager 鑑定用戶端，並取得一個 Tivoli Access Manager 身份。如果所要求的資源並未受到保護，則要求將轉遞至 Web 伺服器進行處理。

   註: 單一登入處理與起始鑑定方法各自獨立運作。
2. 外掛程式將 Tivoli Access Manager 身份傳給使用者登錄伺服器（LDAP 或 URAF）。使用者登錄伺服器維護一個完整的鑑定資訊資料庫，其資訊的形式是資源對特定鑑定資訊的對映。該鑑定資訊是使用者名稱 / 密碼的組合，又稱爲資源證明。只能爲已登記的使用者建立資源證明。

下表說明 GSO 資源證明資料庫的結構：

Michael	Jane
resource: travel-app username=mike password=123	resource: travel-app username=Jane password=abc
resource: payroll-app username=smith password=456	resource: payroll-app username=Jones password=xyz

3. 登錄會傳回使用者名稱 ″mike″ 及密碼 ″123″ 給外掛程式。
4. 外掛程式會將 Michael 的使用者名稱及密碼資訊插入要求的 HTTP 基本鑑定 (BA) 標頭，然後，再將要求傳回給 Web 伺服器。
5. Web 伺服器會根據要求中所插入的 BA 標頭中的證明（來自步驟 4）來鑑定 Michael（針對他所要求的資源），如同它是來自用戶端一般。

配置廣域單一登入

若要啓用「廣域單一登入」功能，您需要配置 pdwebpi.conf。在 **[common-modules]** 段落中，請指定 *BA* 一值給 **post-authzn** 參數，如下所示：

```
[common-modules]
authentication = ...
session = ...
post-authzn = BA
```

確定在模組段落中，參數 **BA** 已指定爲至少預設模組；亦即：

```
[modules]
BA = pdwpi-ba-module
```

在 pdwebpi.conf 配置檔的 **[BA]** 段落內，有一些參數是用於配置 BA 後置授權模組。如下：

- **basic-auth-realm**
- **strip-hdr**
- **add-hdr**
- **gso-resource-name**
- **supply-password**
- **supply-username**

若要對後端應用程式完成 GSO，參數 **add-hdr** 及 **gso-resource-name** 需要配置。在 第 54 頁的『配置基本鑑定』中將更詳細地討論其他 BA 參數。

add-hdr 控制一旦鑑定了要求，將如何新增 BA 標頭。若要完成 GSO，請將這個參數設爲 *gso* 一值，例如：

```
[BA:virtual_host1]
...
add-hdr = gso
```

將 **add-hdr** 參數設爲 *gso* 一值表示新的 BA 標頭將根據使用者登錄中所儲存的資源資訊來新增至 HTTP 要求。配置檔的 **[BA]** 段落中的 **gso-resource-name** 參數指定將

啓用 GSO 的 Web 伺服器資源的名稱。這可以依照每一虛擬主機基礎來指定。使用者登錄中所儲存的資源證明會對映至使用者登錄中所儲存的每一個資源。

將 **gso-resource-name** 參數設爲將啓用 GSO 之 Tivoli Access Manager 資源的名稱。例如：

```
[BA:virtual_host1]
...
gso-resource-name = payroll-app
```

每一虛擬主機僅能指定一個 GSO 資源名稱。如果未指定任何值給 **gso-resource-name**，則虛擬主機名稱將作爲 GSO 資源名稱。

註: 如果正在 Sun ONE（之前稱爲 iPlanet）與 Tivoli Access Manager 之間共用 LDAP 登錄，您將無法在 Tivoli Access Manager 內，以目標使用者名稱（同於預期要向「Sun ONE Web 伺服器」鑑定的使用者名稱）建立 GSO 資源證明。這是因爲當鑑定使用者來僅搜尋正確 LDAP 物件類別的物件時，「Sun ONE Web 伺服器」無法限制 LDAP 搜尋準則。

安全提供者 NEGOtiation (SPNEGO) 單一登入

使用 SPNEGO 作爲外掛程式內的鑑定機制，可提供單一登入功能，以允許使用者從 Windows 用戶端存取安全 IIS Web 伺服器上的資源，而且在起始登入至網域後，就不需再次鑑定。第 60 頁的『配置安全提供者 NEGOtiation (SPNEGO) 鑑定』包括有 SPNEGO 單一登入的作業及配置詳細資訊。

第 7 章 電子社群單一登入

當實作 Tivoli Access Manager Plug-in for Web Servers 來提供安全網域的保護時，通常必須提供資源的單一登入解決方案。本章將討論外掛程式電子社群單一登入解決方案。

主題索引：

概觀

Tivoli Access Manager Plug-in for Web Servers 電子社群單一登入功能可讓使用者不需重新鑑定的情況下，在多個網域內多個伺服器之間存取資源。

「電子社群」是成員間有商務關係而由不同網域（Tivoli Access Manager 或 DNS）所組成的群組。這些加入的網域可以配置爲單一企業的一部分（並且依照地域使用不同的 DNS 名稱），或有共用關係的不同企業（例如企業總部、壽險公司以及財務管理公司）。

在所有的實務中，固定會有一個網域被指定爲「起始」或「擁有者」網域。在加入的企業中，起始網域會擁有管理電子社群的企業協議。

在兩個實務中，加入電子社群的使用者鑑定資訊是由起始網域來維護。這樣的安排可容許因爲管理議題而生的單一參照點，例如，電子社群中的諮詢呼叫都會指向起始網域。

另外，您可以使用 Tivoli Access Manager Web Portal Manager 來委派此資訊的管理權，讓加入的網域可負責管理自身的使用者。

起始網域「擁有」使用者 – 也就是可以控制使用者的鑑定資訊。不論使用者在何處要求資源，均需由起始網域鑑定。

鑑定活動會發生在主要鑑定伺服器 (MAS) – 位於起始網域中而配置的目的爲鑑定所有使用者的伺服器（或一組複本伺服器）。MAS 的任務限制於提供鑑定服務。 MAS 上不應有可讓使用者使用的資源。

在使用者順利通過 MAS 的鑑定後，MAS 會產生「擔保」記號。這個記號會傳回使用者發出要求所在的伺服器。 伺服器會將此「擔保」記號視爲使用者已順利通過 MAS 鑑定的證明，並且可以參與電子社群。

『電子社群單一登入處理流程』章節中會詳細說明電子社群網域間的資訊轉送。

電子社群單一登入功能及需求

- 「電子社群」功能支援使用直接 URL（書籤）存取資源。
- 實作「電子社群」時，所有參與電子社群的網域的所有外掛程式都需要一致的配置。
- 加入電子社群的所有使用者都要通過起始網域中的單一主要鑑定伺服器 (MAS) 的鑑定。
- 如果使用者在 MAS 上沒有有效的帳戶，則「電子社群」在實作時可容許在遠端網域上進行「本端」鑑定。

  當使用者在要求非 MAS（但是已加入）網域中的資源，但未通過 MAS 的鑑定時，使用者可以選擇向要求所在的本端伺服器進行鑑定。
- MAS（以及最後在遠端網域中選取的其他伺服器）會「擔保」使用者的鑑定身份。
- 網域特有的 Cookie 是用在識別可以提供「擔保」服務的伺服器。這樣可容許遠端網域中的伺服器在本端要求「擔保」資訊。電子社群 cookie 的加密內容並未包含使用者身份或安全資訊。
- 特殊記號是用來傳遞已加密的「擔保」使用者身份。「擔保」記號不包含眞正的使用者鑑定資訊。共用的秘密金鑰（三重 DES 演算法）可以提供完整性。 該記號包含了逾時值（生命週期）以便限制記號有效的持續時間。
- 電子社群在實作上支援 HTTP 和 HTTPS。
- 電子社群的配置是設定於每一個參與之外掛程式的 `webseald.conf` 檔中。

電子社群單一登入處理流程

電子社群是由外掛程式強化的主要鑑定伺服器 (MAS) 及其他充當電子社群之外掛程式強化的伺服器所組成。電子社群單一登入解決方案也可以與 WebSEAL 保護的資源交互作業。

電子社群在實作時是根據「擔保」系統。通常，當未經鑑定的使用者透過外掛程式來要求資源時，將提示他們提供鑑定資訊。在電子社群配置中，外掛程式伺服器會識別「擔保」伺服器，並且向使用者通過鑑定的「擔保」伺服器要求驗證。擔保伺服器會儲存使用者的有效證明資訊。

針對使用者的第一次要求，「擔保」伺服器固定爲 MAS。MAS 會繼續作爲起始網域資源的「擔保」伺服器。當使用者繼續要求電子社群中的資源時，每一個遠端網域中的獨立伺服器可以自行建立針對使用者的證明（根據來自 MAS 的使用者身份資訊），並且擔任自身所在網域資源的「擔保」伺服器角色。

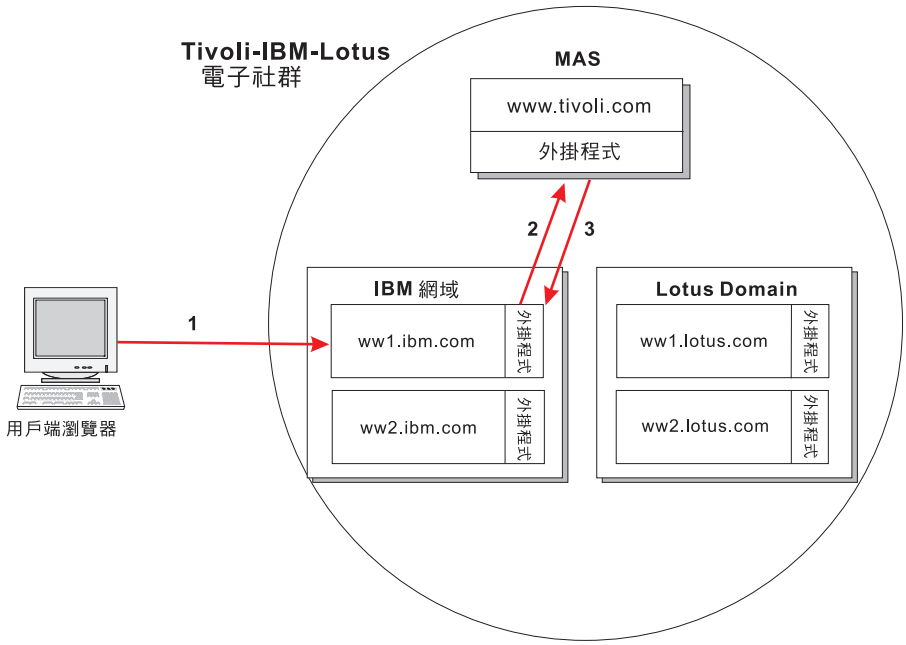

圖 8. 登入至電子社群

上面的範例顯示兩個網域（IBM 網域及 Lotus 網域）存在於電子社群內。當使用者第一次登入至電子社群內的安全網站時，將發生下列處理程序：

1. 使用者要求 Web 伺服器 ww1.ibm.com 上資源的存取權。外掛程式會截取要求，並確認 ww1.ibm.com 已配置爲 Tivoli-IBM-Lotus 電子社群的一部份。電子社群中的 MAS 伺服器是從 ww1.ibm.com 配置中識別的。
2. 要求將傳遞至 MAS - www.tivoli.com。MAS 會代表 ww1.ibm.com 來鑑定要求，並發出一個變成使用者電子社群身份的擔保記號。記號中的使用者身份資訊會被加密。
3. MAS 伺服器將傳送「擔保」記號至 ww1.ibm.com。 ww1.ibm.com 會將此「擔保」記號視爲使用者已順利通過 MAS 鑑定的證明，因此，現在可以根據正常授權控制，來存取所要求的資源。

電子社群 cookie

- 電子社群 cookie 是由一個外掛程式所設定的網域特有 cookie；它會儲存在使用者的瀏覽器記憶體中，並且會在後續的要求中傳送給其他的外掛程式實例（在相同的網域中）。
- 網域特有 cookie 包含了「擔保」伺服器的名稱、電子社群身份、「擔保」伺服器和功能的位置 (URL)，以及生命週期值。cookie 中沒有使用者資訊。
- 電子社群 cookie 可讓參與網域中的伺服器在本端要求「擔保」資訊。 MAS 所在網域的電子社群 cookie 是扮演較次要的角色。
- cookie 中所具有的生命週期（逾時）值是設定於 `pdwebpi.conf` 配置檔。此生命週期值可指定遠端伺服器要花多久的時間，才能提供使用者的「擔保」資訊。當 cookie 的生命週期到期時，使用者必須重新導向至 MAS 以便取得鑑定。

- 當瀏覽器關閉時，記憶體中的 cookie 會被清除。如果使用者登出了特定網域，電子社群 cookie 會被改寫爲空白。此動作可有效地將它從瀏覽器中移除。

擔保要求及回覆

電子社群「擔保」作業需要透過兩個特別建構的 URL 來存取專用功能：「擔保」要求和「擔保」回覆。這些 URL 是在進行電子社群「擔保」HTTP 重新導向時，根據 pdwebpi.conf 中的配置資訊所建構的。

擔保要求

當使用者向目標伺服器要求資源（針對電子社群所配置），而該伺服器沒有該使用者的證明資訊時，就會觸發「擔保」要求。伺服器會傳送 HTTP 重新導向至「擔保」伺服器（MAS 或電子社群 cookie 中所識別的伺服器）。

「擔保」要求包含了以下資訊：

https://*vouch_for_server*/pkmsvouchfor?*ecommunity_name*&*target_url*

接收的伺服器會檢查 *ecommunity_name*，以驗證電子社群身份。接收的伺服器會在「擔保」回覆中使用 *target_url*，將瀏覽器重新導向回到原始要求的頁面。

pkmsvouchfor 擔保 URL 是可配置的。

例如：

https://www.tivoli.com/pkmsvouchfor?companyABC&https://ww2.lotus.com/index.html

擔保回覆

「擔保」回覆是指「擔保」伺服器對目標伺服器的回應。

「擔保」回覆包含了以下資訊：

https://*target_url*?PD-VFHOST=*vouch_for_server*&PD-VF=*encrypted_token*

PD-VFHOST 參數識別執行了擔保作業的伺服器。接收的（目標）伺服器會使用此資訊來選擇爲「擔保」記號 (PD-VF) 解密的正確金鑰。 **PD-VF** 參數代表了加密的「擔保」記號。

例如：

https://ww2.lotus.com/index.html?PD-VFHOST=www.tivoli.com&PD-VF=3qhe9fjkp...ge56wgb

擔保記號

爲了達到跨網域的單一登入，部分使用者身份資訊必須在伺服器間傳輸。這種敏感資訊會透過重新導向來處理；而重新導向會包含加密爲 URL 一部分的身份資訊。這種加密的資料稱之爲「擔保」記號。

- 該記號包含了「擔保」成功或失敗的狀態、使用者的身份（在擔保成功時）、建立記號的伺服器完整名稱、電子社群身份，以及建立時間值。
- 有效「擔保」記號的持有者可以使用此記號在伺服器上建立階段作業（以及證明集），而不需要經過該伺服器的鑑定。
- 該記號會使用共用三重 DES 演算法的秘密金鑰來加密，因此可以驗證其確實性。
- 加密的記號資訊不會儲存在瀏覽器中。

- 記號只會傳送一次。接收的伺服器會使用此資訊在快取中建立該使用者的證明。 當使用者在相同的階段作業中作出後續的要求時，伺服器就會使用這些證明。
- 記號中所具有的生命週期（逾時）值是設定於 pdwebpi.conf 配置檔。此值可以是很短（秒）以便減少 re-play 攻擊的風險。

註: 在外掛程式 4.1 版中已改進了記號安全性。這些改進無法與 Tivoli Access Manager 3.9 記號編碼架構交互作業。若要繼續能夠與 3.9 Tivoli Access Manager Web Security 產品交互作業，請將 **[pdweb-plugins]** 段落中的 **pre-410-compatible-tokens** 配置參數設成 **true**。這個參數適用於整個處理程序，而且無法依照每一虛擬主機基礎來指定。

加密擔保記號

Tivoli Access Manager Plug-in for Web Servers 必須使用 **pdwpi-cdsso-key-gen** 公用程式（位於 /bin 目錄）所產生的金鑰來加密置於記號中的鑑定資料。您必須與每一個參與的網域內的每一部外掛程式伺服器共用金鑰檔，來「同步化」這個金鑰。每一個網域內的每一部參與的外掛程式伺服器都必須使用相同的金鑰。

註: 金鑰檔的建立和分送並非 Tivoli Access Manager 電子社群處理程序的一部份。您必須自行安全地將金鑰複製至所有的分享伺服器。

當您執行 **pdwpi-cdsso-key-gen** 公用程式時，此公用程式會要求您指定金鑰檔的位置（絕對路徑名稱）：

UNIX：

```
# pdwpi-cdsso-key-gen absolute_pathname
```

Windows：

```
MSDOS> pdwpi-cdsso-key-gen absolute_pathname
```

加密金鑰是配置在 pdwebpi.conf 配置檔的 **[ecsso-domain-keys]** 段落中。這個配置將詳述在下一節 『配置電子社群』

配置電子社群

本節會檢閱實作電子社群所需要的所有配置參數。這些參數是在 pdwebpi.conf 檔中。您必須對電子社群中每一個參與的外掛程式仔細配置這個檔案。

啓用及停用電子社群成員

pdwebpi.conf 配置檔中的 **[common-modules]** 段落定義如何使用所有鑑定方法。若要啓用外掛程式伺服器，在電子社群內操作，請指定 *ecsso* 一詞給 **authentication** 及 **post-authzn** 參數，如下所示：

```
[common-modules]
authentication = ecsso
post-authzn = ecsso
```

pdwebpi.conf 配置檔中的 **[modules]** 段落定義所有可用的鑑定機制，以及它們相關聯的共用程式庫名稱。確定電子社群 SSO 的項目存在；亦即：

```
[modules]
ecsso = pdwpi-ecsso
```

e-community-name

e-community-name 參數識別伺服器所屬之電子社群的名稱。例如：

```
[ecsso]
e-community-name = companyABC
```

對於電子社群的所有成員，**e-community-name** 值必須是相同的。

is-master-authn-server

此參數可識別此伺服器是否爲 MAS。其值包括 *yes* 或 *no*。電子社群 MAS 的參數將設定如下：

```
[ecsso]
is-master-authn-server = yes
```

多個外掛程式可以配置爲主要鑑定伺服器，然後置於負載平衡器之後。在此情況中，負載平衡器會被電子社群中所有其他外掛程式伺服器識別爲 MAS。

如果 **is-master-authn-server** 設爲 *yes*，則這個伺服器將接受來自其他外掛程式實例的「擔保」要求，不過，這些實例的 **e-community-name** 必須相同，而且它們的網域金鑰必須列示在 **[ecsso-domain-keys]** 段落中。

master-authn-server

如果 **is-master-authn-server** 參數設定爲 *no*，您必須消除 **master-authn-server** 參數的標註，並且加以指定。此參數可識別電子社群 MAS 的完整網域名稱。例如：

```
[ecsso]
 master-authn-server = www.tivoli.com
```

master-http-port

指定主要鑑定伺服器用來接收 HTTP 要求的埠號。如果埠號不是標準埠 80，則必須在這裡指定非標準埠號。

```
[ecsso]
master-http-port = port_number
```

master-https-port

指定主要鑑定伺服器用來接收 HTTSP 要求的埠號。如果埠號不是標準埠 443 則必須在這裡指定非標準埠號。

```
[ecsso]
master-https-port = port_number
```

vf-token-lifetime

此參數設定「擔保」記號的生命週期逾時值（秒）。此值會根據 cookie 上的建立時間戳記來進行檢查。 預設值爲 180 秒。 您必須將分享伺服器間的時間偏差列入考量。根據預設值，參數將設爲：

```
[ecsso]
vf-token-lifetime = 180
```

vf-url

此參數指定「擔保」URL。此值必須以斜線 (*/*) 開頭。預設設定值爲：

```
[ecsso]
vf-url = /pkmsvouchfor
```

您也可以表示延伸的 URL：

```
vf-url = /ecommA/pkmsvouchfor
```

allow-login-retry
當使用者執行了不成功的登入時，使用使用者名稱/密碼型鑑定架構的 MAS 具有兩個選項：它可以提示使用者重新輸入他們的證明，或它可以立即重新導向使用者回到他們原先嘗試存取的伺服器，而需擔保使用者。在後面的情況中，使用者被迫直接接受從屬伺服器的鑑定。 **allow-login-retry** 參數控制 MAS 中的這個行爲。這個參數僅適用於 ecsso 社群內 MAS 的配置。

註: 使用者可以嘗試重設到期的密碼。

其他發生在 MAS 的登入失敗（如帳戶鎖定）會導致立即重新導向至從屬伺服器，不管 **allow-login-retry** 參數的值。根據預設值，參數將設爲：

```
[ecsso]
allow-login-retry = true
```

ecsso Domain Keys
定義在配置檔的 **[ecsso-domain-keys]** 段落中的值是金鑰檔的位置，需有這些金鑰檔，才能在 MAS 與遠端網域中參與的伺服器之間加密及解密記號。 MAS 的配置包括定義每一個網域（本身是主要網域）的金鑰。 MAS 以外的電子社群成員的配置包括定義網域及 MAS 的金鑰。您必須指定伺服器的完整網域名稱以及金鑰檔位置的絕對路徑名稱。

以下的 MAS 配置範例提供了 MAS 使用金鑰檔與兩個遠端網域通訊：

```
[ecsso-domain-keys]
ibm.com = /abc/xyz/ibm-lotus.key
lotus.com = /abc/xyz/lotus-tivoli.key
```

網域中伺服器的配置包括指定 MAS 網域，以及用來與 MAS 交換資訊的對應金鑰。在網域中的伺服器之間交換資料時，也需要金鑰。例如，參與電子社群的網域中的 **[ecsso-domain-keys]** 段落的樣子可能如下：

```
[ecsso-domain-keys]
#the key for data exchange between the MAS (tivoli.com)
#and the ibm.com domain servers
tivoli.com = /abc/xyz/ibm-tivoli.key
#the key for data exchange between servers in the ibm.com domain
ibm.com = /abc/xyz/ibm.key
```

配置電子社群單一登入 - 範例

在下列範例中，有兩個已配置的電子社群 – lotus-domino 及 ibm-db2 – 且具有單一 MAS 來鑑定這兩個社群的要求。

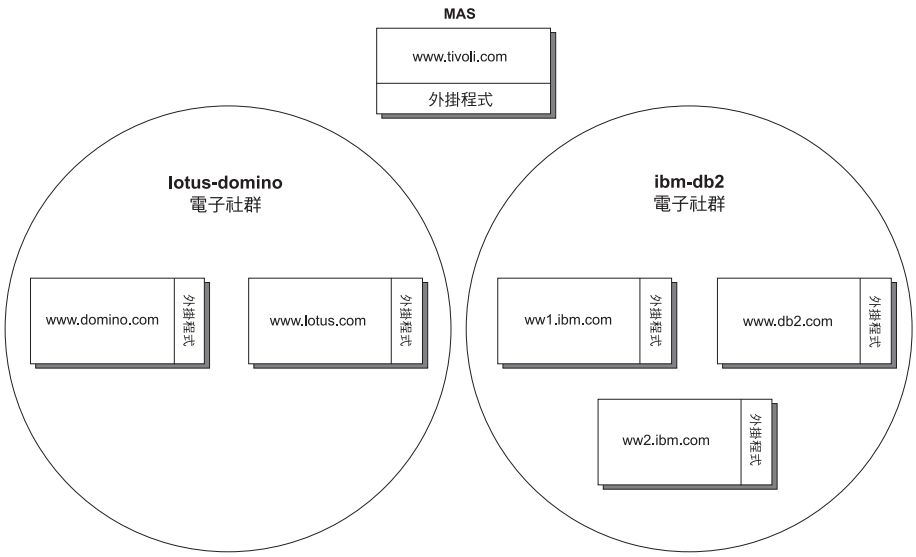

圖 9. 電子社群單一登入配置範例

下列條件適用於這個範例：

- www.tivoli.com 是這兩個電子社群的 MAS。
- 有兩個不同的網域（爲了簡化，每一個網域有一個伺服器）存在於 lotus-domino 電子社群 – domino.com 及 lotus.com。存取這些網域之一的使用者不需重新鑑定，就可以存取其他網域，因爲已透過 MAS 授與所有存取權。
- ibm-db2 電子社群含有兩個不同的網域 – ibm.com 及 db2.com。存取這些網域之一的使用者不需重新鑑定，就可以存取其他網域。
- 存取其中一個 ibm.com 伺服器的使用者可以存取其他使用「擔保」記號的伺服器。在此情況下，不需要 MAS 授與存取權，就能完成單一登入。

在上面的範例中，將套用下列配置條件：

MAS 的配置 – www.tivoli.com

當 MAS 是多個電子社群的控制中心時，需要配置 ecsso 模組的兩個不同實例，以及需要定義 MAS 控制的電子社群名稱。MAS 需要在它控制的所有社群內，指定了主要網域的所有金鑰。將套用下列配置條件：

```
[modules]
ecsso1 = pdwpi-ecsso-module
ecsso2 = pdwpi-ecsso-module

[common-modules]
authentication = ecsso1
authentication = ecsso2

post-authzn = ecsso1
post-authzn = ecsso2

[ecsso1]
e-community-name = lotus-domino
is-master-authn-server = yes
.....etc

[ecsso2]
e-community-name = ibm-db2
```

```
is-master-authn-server = yes
.....etc

[ecsso1-domain-keys]
# one key for each domain the MAS controls
domino.com = /abc/tivolikeys/tivoli-domino.key
lotus.com = /abc/tivolikeys/tivoli-lotus.key
db2.com = /abc/tivolikeys/tivoli-db2.key
ibm.com = /abc/tivolikeys/tivoli-ibm.key
```

www.domino.com 的配置

```
[modules]
ecsso = pdwpi-ecsso-module

[common-modules]
authentication = ecsso

post-authzn = ecsso

[ecsso]
e-community-name = lotus-domino
is-master-authn-server = no
master-authn-server = www.tivoli.com
.....etc

[ecsso-domain-keys]
#key for encrypting/decrypting data
#between servers in the domino.com domain
domino.com = /abc/domino-keys/domino.key
#key for encrypting/decrypting data between
#servers in the domino.com domain and the MAS
tivoli.com = /abc/domino-keys/tivoli-domino.key
```

www.lotus.com 的配置

完成 www.lotus.com 單一登入的配置參數將同於配置給 www.domino.com 的參數，但網域金鑰將有所不同。www.lotus.com 的網域金鑰配置如下：

```
[ecsso-domain-keys]
#key for encrypting/decrypting data
#between servers in the lotus.com domain
lotus.com = /abc/lotus-keys/lotus.key
#key for encrypting/decrypting data
#between servers in the lotus.com domain and the MAS
tivoli.com = /abc/lotus-keys/tivoli-lotus.key
```

www.db2.com 的配置

```
[modules]
ecsso = pdwpi-ecsso-module

[common-modules]
authentication = ecsso

post-authzn = ecsso

[ecsso]
e-community-name = ibm-db2
is-master-authn-server = no
master-authn-server = www.tivoli.com
.....etc

[ecsso-domain-keys]
#key for encrypting/decrypting data
#between servers in the db2.com domain
db2.com = /abc/db2-keys/db2.key
```

```
#key for encrypting/decrypting data between
#servers in the db2.com domain and the MAS
tivoli.com = /abc/db2-keys/tivoli-db2.key
```

ww1.ibm.com 的配置

ww1.ibm.com 的電子社群單一登入配置同於 www.db2.com 的配置。需要兩個金鑰，一個用於在 MAS 與 ibm.com 網域之間加密/解密資料，另一個則用於在 ibm.com 網域內伺服器（如這個範例中的 ww1.ibm.com 及 ww2.ibm.com）之間加密/解密資料。

```
[ecsso-domain-keys]
ibm.com = /abc/ibm-keys/ibm.key
tivoli.com = /abc/ibm-keys/tivoli-ibm.key
```

ww2.ibm.com 的配置

ww2.ibm.com 的金鑰定義將同於 ww1.ibm.com 的金鑰定義。

```
[ecsso-domain-keys]
ibm.com = /abc/ibm-keys/ibm.key
tivoli.com = /abc/ibm-keys/tivoli-ibm.key
```

附錄 A. pdwebpi.conf 參照

Tivoli Access Manager Plug-in for Web Servers 是使用位在 pdwebpi.conf 配置檔中的參數來加以配置的。檔案是在以下的目錄中：

UNIX：

```
/opt/pdwebpi/etc/
```

Windows：

```
C:\Program Files\Tivoli\PDWebPI\etc\
```

底下是可在 pdwebpi.conf 配置檔內配置的每一個參數的說明。參數將根據它們的用途而分成不同的表格群組。

表 30. 一般配置參數

一般	
參數	**說明**
[pdweb-plugins]	
virtual-host	識別含有關於特定虛擬主機之配置資訊的子層段落。
unprotected-virtual-host	識別外掛程式不提供安全保護的虛擬主機。外掛程式允許不需要對要求執行鑑定及授權，就可以存取這些虛擬主機。
web-server	識別使用中的 Web 伺服器類型。可接受的值如下： • *iis* 代表 Microsoft Internet Information Services • *ihs* 代表 IBM HTTP Server • *iplanet* 代表 Sun ONE（之前稱爲 iPlanet）Web Server 安裝期間，會自動設定這個參數。
windows-file-system	向 Authorization Server 指出，應該採取預防措施，以避免與代表 Windows 檔案系統資源的 URI 相關的安全問題。 設爲 *true*，將禁止存取含路徑元素（如 Windows 2000 短路徑名稱）的 URI。尤其，將拒絕以 *~digit* 結尾的路徑元素。在 Windows 系統上，這個參數依預設會設爲 *true*。在 UNIX 系統上，則會設爲 *false*。 這個參數可以依照每一虛擬主機基礎來置換，方法爲在適當的 **[***virtual_host***]** 段落指定它。

表 30. 一般配置參數 (繼續)

一般	
參數	**說明**
case-sensitive	告訴 Authorization Server 如何處理 URI 的字體。 設爲 *false*，當對照做出授權決策的物件名稱，建構對應的 Tivoli Access Manager 物件名稱時，URI 就會轉換成小寫字體。 在 UNIX 系統上，這個參數會設爲 *true*。在 Windows 系統上，則會設爲 *false*。 當 **windows-file-system** 參數設爲 *true*，且未定義 **case-sensitive**，則 URI 依預設會轉換成小寫字體。 請注意，並未轉換物件名稱的 /PDWebPI/*branch* 部份。 這個參數可以依照每一虛擬主機基礎來置換，方法爲在適當的 **[***virtual_host***]** 段落指定它。
utf8-url-support-enabled	控制在建置對應的 Tivoli Access Manager 的「受保護的物件名稱」時，解譯 URL 所依據的字碼頁。 設爲 *true*，呈現給 Authorization Server 的 URI 將假設以 UTF8 編碼，並且轉換成 Authorization Server 在用來建構 Tivoli Access Manager 的受保護的物件名稱之前，執行時所依據的字碼頁。 設爲 *false*，呈現給 Authorization Server 的 URI 將假設以 Authorization Server 執行時所依據的字碼頁來編碼。 設爲 *auto*，將檢查每一個 URI 是否有多位元組 UTF8 順序。如果找到的話，URI 將假設以 UTF8 編碼。如果偵測到無效的 UTF8 字元順序，URI 將假設以 Authorization Server 執行時所依據的字碼頁來編碼。 這個參數可以依照每一虛擬主機基礎來置換，方法爲在適當的 **[***virtual_host***]** 段落指定它。
log-file	識別所有 Authorization Server 作業攫取所在之日誌檔的檔名及路徑。
logs	指定在重複使用第一個日誌檔之前，要建立的日誌檔數目。
log-entries	指定建立新的日誌檔之前，要寫入的日誌項目數目。
mpa-enabled	「多工 Proxy 代理站 (MPA)」是調適多重用戶端存取的閘道。 系統會建立至源點伺服器的單一鑑定頻道，所有用戶端及回應通訊都會透過這個頻道來傳送。 設爲 *true*，就會啓用 MPA 能力。 設爲 *false*，就會停用 MPA 能力。 這個參數可以依照每一虛擬主機基礎來置換，方法爲在 **[***virtual_host***]** 段落定義它。

表 30. 一般配置參數 (繼續)

一般	
參數	**說明**
mpa-protected-object	定義 MPA 物件以便對其做出授權決策。 這個參數可以依照每一虛擬主機基礎來置換，方法爲在 **[***virtual_host***]** 段落定義它。
user	在 UNIX 系統上，這個參數含有使用者名稱，管理程式及 proxy 處理程序將以這個使用者名稱來執行。
group	在 UNIX 系統上，這個參數含有群組名稱，管理程式及 proxy 處理程序將以這個群組名稱來執行。
pre-410-compatible-tokens	啓用或停用 Tivoli Access Manager 第 4.1 版與 Tivoli Access Manager 3.9 中記號加強功能之間的相容性。設爲 true，電子社群單一登入及失效接替 cookie 產生的記號安全性將與 Tivoli Access Manager 3.9 記號編碼架構交互作業。這個參數適用於整個處理程序，而且無法依照每一虛擬主機基礎來指定。
[module-mgr]	
path	含有模組共用程式庫檔案的路徑。當外掛程式將搜尋全部項目時，允許多個路徑項目。
[wpiconfig]	
server-type	配置期間設定以協助解除配置。
install-dir	配置期間設定以協助解除配置。
vhosts	配置期間設定以協助解除配置。

表 31. 鑑定配置參數

鑑定	
參數	**說明**
[modules]	
module_name **=** *shared_library_name*	宣告可用的鑑定方法及相關聯的程式庫。
acctmgmt	帳戶管理
BA	基本鑑定
cert	憑證
failover	失效接替
forms	套表
ip-addr	IP 位址
iv-headers	IV 標頭
session-cookie	階段作業 Cookie
ssl-id	SSL ID
tag-value	標籤值
http-hdr	HTTP 標頭
token	記號
ltpa	LTPA Cookie

表 31. 鑑定配置參數 (繼續)

鑑定	
參數	**說明**
ecsso	電子社群單一登入
login-redirect	登入重新導向
spnego	安全提供者協議
[common-modules]	
authentication	指定要用於使用者鑑定的方法。
session	指定要用於維護階段作業狀態的方法。
post-authzn	指定要用於後置授權處理程序的方法。
[authentication-levels]	
level **=** *module_name*	**[authentication-levels]** 段落定義進階鑑定層次，以及 **[modules]**段落中定義的鑑定方法的排次。 當沒有定義任何項目給鑑定方法時，它會預設爲層次 **1**。鑑定次序會判定爲由最高鑑定層次，向下至已定義的鑑定方法的最低鑑定層次。如果數個鑑定方法共用一個鑑定層次，則子次序將由模組出現在 **[modules]** 段落內的次序來加以決定。
[authentication-mechanisms]	
passwd-cdaspasswd-ldap passwd-uraf token-cdas cert-sslcert-cdas http-requestcdssopasswd-strength cred-ext-attrs	列示支援的其他鑑定機制及相關聯的共用程式庫，它們會外掛至 Tivoli Access Manager 的鑑定子系統。
[BA]	
basic-auth-realm	宣告在基本鑑定登入期間，將出現在呈現給使用者之對話的領域名稱。
strip-hdr	控制如何從要求移除 BA 標頭。有效的選項如下： • *ignore* - 不對 BA 標頭執行任何動作。 • *always* - 從要求移除 BA 標頭。 • *unauth* - 如果標頭未經鑑定，將從要求移除 BA 標頭。
add-hdr	控制如何新增 BA 標頭至要求。這個項目的有效選項如下： • *none* - 不要新增 BA 標頭至要求。 • *gso* - 新增 GSO BA 標頭至要求。 • *supply* - 在 BA 標頭中提供靜態密碼或使用者名稱，或是同時提供這兩者
gso-resource-name	含有用來建立 GSO BA 標頭的 GSO 資源名稱。當 **add-hdr** 設爲 *gso* 時，指定值是選用的。當 **add-hdr** 設爲 i*gso*，但未設定 **gso-resource-name** 時，將使用處理要求之虛擬主機的名稱。
supply-password	如果 **add-hdr** 設爲 *supply*，將需要一值。設定時，參數會指定在已建立的 BA 標頭中使用的靜態密碼。

表 31. 鑑定配置參數 (繼續)

鑑定	
參數	**說明**
supply-username	含有在已建立的 BA 標頭中使用的靜態使用者名稱。當 **add-hdr** 參數設爲 *supply* 時，這個參數的設定是選用的。當設定 **supply** 參數，但未設定 **supply-username**（亦即，它仍然是註解）時，將在已建立的 BA 標頭中使用已鑑定使用者的名稱。
[failover]	
failover-cookie-keyfile	宣告用來加密及解密失效接替 cookie 中的證明資料之金鑰檔的路徑。
failover-cookie-lifetime	失效接替 cookie 的有效生命週期（以分鐘爲單位）。
enable-failover-cookie-for-domain	啓用/停用整個網域延伸範圍的失效接替 cookie。
[ltpa]	
ltpa-keyfile	LTPA 金鑰檔的完整路徑名稱。
ltpa-stash-file	密碼隱藏檔案的位置
ltpa-password	要在隱藏檔所在使用的密碼。
ltpa-lifetime	LTPA cookie 的生命週期（以秒爲單位）。
[forms]	
login-form	登入套表的檔名。
login-uri	登入套表將登入明細送至的 URI。登入明細必須送至這個 URI，其中使用者的名稱在 POST 資料屬性 'username' 中指定，而使用者的密碼則在 POST 資料屬性 'password' 中指定。
create-ba-hdr	啓用或停用當使用套表鑑定時建立 BA 標頭。
[tag-value]	
cache-definitions	指出是否要快取已連接至物件空間的標籤值的布林值。如果已快取的話，將需要重新啓動 proxy，以挑選標籤/值定義的任何變更。
cache-refresh-interval	定義的快取記憶體的重新整理間隔（以秒爲單位）。
[token-card]	
token-login-form	記號登入頁面的檔名。
next-token-form	定義顯示給使用者用戶端以要求下一個記號的套表。當伺服器無法順利地從第一個記號鑑定使用者時，將要求用戶端輸入另一個記號。
[http-hdr]	
header	傳至「跨網域鑑定服務 (CDAS)」進行鑑定的標頭名稱。
[iv-headers]	

表 31. 鑑定配置參數 (繼續)

鑑定	
參數	**說明**
accept	當作來自 proxy 的鑑定證明而接受的標頭清單。有效的選項如下： • *all* - 接受所有標頭類型。 • *iv-creds* - 使用者證明資訊。 • *iv-user* - 短使用者名稱。 • *iv-user-l* - 長使用者名稱。 • *iv-remote-address* - 用戶端的 IP 位址。
generate	從 proxy 轉遞要求時將產生的標頭清單。有效的選項如下： • *all* - 產生所有標頭類型。 • *iv-creds* - 使用者證明資訊。 • *iv-user* - 短使用者名稱。 • *iv-user-l* - 長使用者名稱。 • *iv-remote-address* - 用戶端的 IP 位址。
[acctmgmt]	
password-change-form	當使用者要求密碼變更時所顯示的套表。
password-change-form-uri	當使用者要求密碼變更時所存取的 URI。
password-change-uri	密碼變更後的 URI 目的地。
password-change-success	當使用者順利地完成密碼變更時所顯示的頁面。
password-change-failure	當使用者無法順利登入時所顯示的頁面。
logout-uri	使用者登出後的 URI 目的地。
help-uri	說明頁面的位置。
help-page	當使用者要求說明時所顯示的說明頁面的檔名。
logout-success	當使用者順利登出時所顯示的 URI 或檔案。
[ecsso]	
e-community-name	出現在擔保記號和要求中的電子社群名稱。
is-master-authn-server	指定伺服器是主要伺服器或不在電子社群中。設爲 *yes*，這個伺服器將接受來自其他外掛程式實例的擔保需求，這些實例的網域金鑰列示在 **[ecsso-domain-keys]** 段落中。
master-authn-server	電子社群中主要伺服器的名稱。如果 *is-master-authn-server* 設爲 no，則這個參數是必要的。
master-http-port	指定主要鑑定伺服器上監聽 HTTP 要求的埠（不同於標準埠 80）。如果此伺服器爲主要鑑定伺服器，則會忽略此參數。
master-https-port	指定主要鑑定伺服器上監聽 HTTPS 要求的埠（不同於標準埠 443）。如果此伺服器爲主要鑑定伺服器，則會忽略此參數。
vf-token-lifetime	擔保記號生命週期（以秒爲單位）。
vf-url	擔保 URL。

表 31. 鑑定配置參數 (繼續)

鑑定	
參數	**說明**
allow-login-retry	當未經鑑定的使用者被重新導向至主要伺服器進行鑑定時，啓用或停用使用者登入的重試。設爲 *true*，主要伺服器將容許使用者在起始嘗試失敗後，重新輸入他們的使用者名稱/密碼。設爲 *false*，使用者將被重新導向回從屬伺服器，而不擔保使用者。
[ecsso-domain-keys]	
domain-name* = *key-file	定義當與來自電子社群內指定的網域的參與者通訊時要使用的金鑰。 這個段落的名稱衍生自定義在 **[modules]** 段落的 **pdwpi-ecsso-module** 的模組名稱。它的格式是 **[*ecsso-module-name*-domain-keys]**。
[login-redirect]	
redirect-uri	鑑定成功時使用者將重新導向至的 URI。
[spnego]	
web-server-does-authn	指出是由 Authorization Server 或「Web 伺服器」處理整合性登入交換。 *true* 值指出由 Web 伺服器處理交換， *false* 則指出由 Authorization Server 處理交換。

表 32. 階段作業配置參數

階段作業	
參數	**說明**
[sessions]	
max-entries	單一階段作業模組實例內所儲存的階段作業數目上限。每一虛擬主機的每一階段作業模組的階段作業數目上限。
timeout	階段作業生命週期上限（以秒爲單位）。
inactive-timeout	在階段作業逾時前，階段作業所需的閒置時間長度（以秒爲單位）。
resend-pdwebpi-cookie	啓用或停用對每一個要求傳送「Web 外掛程式」cookie。
reauth-lifetime-reset	控制階段作業生命週期計時器。設爲 *yes*，則在重新鑑定成功時，將重設階段作業生命週期計時器（亦即，timeout 參數中設定的值）。設爲 *no*，則在重新鑑定成功時，將不會執行重設。
reauth-grace-period	以秒爲單位設定用戶端具有多少時間作爲寬限期，以便順利地執行重新鑑定，不然，證明將到期。
[session-cookie]	
use-same-session	指定 HTTP 及 HTTPS 通訊協定是否應該使用相同的階段作業。

表 33. LDAP 配置參數

LDAP	
參數	**說明**
[ldap]	
bind-pwd	Web Plug-in 常駐程式的密碼（在配置期間設定）。
enabled	啓用或停用 LDAP 通訊（在配置期間設定）。
host	LDAP Server 的名稱（在配置期間設定）。
port	LDAP 的埠號（在配置期間設定）。
replica	失效接替 LDAP 實例的複本 LDAP 規格。當主要 LDAP 伺服器無法使用時，就會使用它。
cache-enabled	啓用和停用本端 LDAP 快取。

表 34. Proxy 配置參數

Proxy	
參數	**說明**
[proxy-if]	
id	指定 proxy 介面的 ID 或共用記憶體檔案名稱。 ID 必須符合外掛程式所使用的 ID。
number-of-workers	處理外掛程式要求之工作者執行緒的數目。
worker-size	預先配置給每一個處理外掛程式要求之工作者執行緒的記憶體數量。
cleanup-interval	每一次清除記憶體的間距（以秒爲單位）。
max-session-lifetime	逾時前，外掛程式等待來自 Authorization Server 之回應的時間（以秒爲單位）。
[proxy]	
error-page	當非預期伺服器錯誤發生時，顯示在使用者瀏覽器上之頁面的路徑。
acct-locked-page	當使用者嘗試存取已鎖定的帳戶時所顯示之頁面的路徑。
retry-limit-reached-page	當登入嘗試失敗的次數達到了容許的上限時所顯示之頁面的路徑。容許的登入失敗次數上限是使用 **policy** 指令設定在 LDAP。
login-success	指定在套表或記號登入成功後，若外掛程式沒有頁面來重新導向使用者回到其中，將顯示的頁面。當您建置的登入套表是直接傳送登入 POST 資料回到外掛程式時，就可能發生這種狀況。

表 35. 授權 API 配置參數

授權 API	
參數	**說明**
[aznapi-configuration]	
審核及記載參數及配置	

表 35. 授權 API 配置參數 (繼續)

授權 API	
參數	**說明**
logsize	建立新日誌檔時檔案的大小（以位元組爲單位）。 如果設爲 *0*，將不建立新的日誌檔。 如果設爲負數，將每天建立新的日誌檔，不管大小爲何。
logflush	清除日誌的間隔（以秒爲單位）。 最大值是 21600（6 小時）。
logaudit	啓用或停用審核記載。
auditlog	審核檔案的名稱。
auditcfg	啓用或停用元件特有的審核記錄。有效值如下： *authn* - 攫取鑑定事件。 *azn* - 攫取授權事件。
db-file	ACL 資料庫快取檔案的位置。
cache-refresh-interval	檢查主要授權伺服器是否更新的間隔（以秒爲單位）。
listen-flags	啓用或停用原則快取更新通知的接收旗號。
授權 API 服務定義	
[aznapi-entitlement-services]	
service_id	每一個段落項目定義不同類型的 aznAPI 服務。如需相關資訊，請參閱 *IBM Tivoli Access Manager Authorization C API Developer's Reference*。
AZN_ENT_EXT_ATTR	這是不應該變更的系統層次參數。它容許在物件空間上使用延伸屬性。

表 36. Web 伺服器特有的配置參數

Web 伺服器特有的	
參數	**說明**
[ihs]	
query-contents	指定要用於透過 'pdadmin> object list' 指令瀏覽 IBM HTTP Server Web 空間的查詢內容程式。這個參數可以依照每一分支來置換，方法爲在名爲 **[ihs:***branch***]** 的段落（例如，[ihs:/PDWebPI/foo.bar.com]）中，指定一值給它
query-log-file	可取得查詢內容程式所遇到之錯誤的日誌檔的位置。
doc-root	指定說明文件 root，它會提供執行 'pdadmin> object list' 指令所需的 Web 空間瀏覽能力。當設定虛擬主機時，這個參數是由配置公用程式所設定的 - 它是依照每一原則分支在 **[ihs:***branch***]** 段落（例如，[ihs:/PDWebPI/foo.bar.com]）中指定的。
[iis]	

表 36. Web 伺服器特有的配置參數 (繼續)

Web 伺服器特有的	
參數	**說明**
query-contents	指定用於透過 pdadmin 瀏覽 IIS Web 空間的查詢內容程式。這個參數可以依照每一分支來置換，方法爲在名爲 **[iis:*branch*]** 的段落（例如，[iis:/PDWebPI/foo.bar.com]）中，指定一值給它
query-log-file	可取得查詢內容程式所遇到之錯誤的日誌檔的位置。
log-file	定義日誌檔，以取得來自 IIS 外掛程式的錯誤及追蹤訊息。訊息會個別保存在 Authorization Server 日誌檔以外的日誌檔，以確定檔案的一致性。如果指定爲相對路徑，位置將相對於安裝目錄的 log 子目錄。如果指定爲絕對路徑，將使用絕對路徑。
[iplanet]	
query-contents	指定用於透過 pdadmin 瀏覽 Sun ONE Web 空間的查詢內容程式。這個參數可以依照每一分支來置換，方法爲在名爲 **[iplanet:*branch*]** 的段落（例如，[iplanet:/PDWebPI/foo.bar.com]）中，指定一值給它
query-log-file	可取得查詢內容程式所遇到之錯誤的日誌檔的位置。
doc-root	指定說明文件 root，它會提供執行 'pdadmin> object list' 指令所需的 Web 空間瀏覽能力。當設定虛擬主機時，這個參數是由配置公用程式所設定的 - 它是依照每一原則分支在 **[iplanet:*branch*]** 段落（例如，[iplanet:/PDWebPI/foo.bar.com]）中指定的。

附錄 B. 模組快速參照

鑑定是識別試圖登入安全網域之個別處理程序或實體的方法。 個人或處理程序用來存取外掛程式的受保護網域的鑑定方法可以採用許多種形式。 IBM Tivoli Access Manager Plug-in for Web Servers 支援一些鑑定方法。下表將列出這些鑑定方法及其適當說明。

表 37. 外掛程式鑑定方法/模組參照

鑑定方法/模組	說明
BA `pdwpi-ba-module`	「基本鑑定」鑑定模組。 也可能配置爲階段作業及後置授權模組。
forms `pdwpi-forms-module`	「HTML 套表」鑑定模組。 使用透過套表送出的使用者名稱及密碼來進行鑑定。 使用時，這個模組也必須配置爲後置授權模組。
ip-addr `pdwpi-ipaddr-module`	「用戶端 IP 位址」鑑定模組。 提供完全以用戶端的 IP 位址爲基礎的鑑定。 http 要求鑑定機制必須由客戶提供，才能將 IP 位址資訊對映至 Tivoli Access Manager 主體。 也可配置爲階段作業模組。
http-hdr `pdwpi-httphdr-module`	「HTTP 標頭」鑑定模組。 提供完全以要求中指定的 HTTP 標頭值爲基礎的鑑定。 http 要求鑑定機制必須由客戶提供，才能將標頭資訊對映至 Tivoli Access Manager 主體。 也可配置爲階段作業模組。
token `pdwpi-token-module`	記號鑑定模組。 Tivoli Access Manager Plug-in for Web Servers 可支援利用用戶端提供的記號通行代碼進行鑑定。這種鑑定會使用兩個以 RSA SecureID 墜飾爲基礎的因子登入。 使用時，也必須配置爲後置授權模組。
cert `pdwpi-certificate-module`	「用戶端憑證」鑑定模組。 用戶端憑證的主題 DN 是由 cert-ssl 鑑定機制對映至 Tivoli Access Manager Principa 名稱。 cert-ssl 鑑定機制需要用戶端憑證的主題 DN 直接對映至使用者登錄中 Tivoli Access Manager 使用者的 DN。 這個模組將忽略這些要求，以鑑定未透過 SSL 階段作業抵達的要求，以便可以安全地配置它們，供處理 HTTP 及 HTTPS 要求授權的虛擬主機使用。

表 37. 外掛程式鑑定方法/模組參照 (繼續)

鑑定方法/模組	說明
Failover pdwpi-failovercookie-module	失效接替 Cookie 鑑定模組。 這個接受失效接替 cookie 來鑑定使用者。 使用時，這個模組也必須配置爲後置授權模組。
iv-headers pdwpi-iv-headers-module	「IV 標頭」鑑定模組。 提供以要求中的 iv-user、 iv-user-l、iv-creds 或 iv-remote-address HTTP 標頭值爲基礎的鑑定。當使用者已通過前端 proxy 伺服器的鑑定時，這個模組有助於對 Tivoli Access Manager Plug-in for Web Servers 使用單一登入。 爲了能夠取得信任，必須使用已鑑定階段作業與前端 proxy 伺服器（例如，WebSEAL 接合）搭配，要求才能到達。proxy 必須當作使用者來進行鑑定，而且這個使用者必須對正在存取之虛擬主機的受保護物件空間具有 Proxy ([PDWebPI]p) 許可權。 對於使用 iv-remote-address 標頭的鑑定，http 要求鑑定機制必須由客戶提供，才能將 IP 位址資訊對映至 Tivoli Access Manager 主體。 這個模組也可能配置爲後置授權模組及階段作業模組。
ecsso pdwpi-ecsso-module	「電子社群單一登入」鑑定模組。 這個模組必須配置爲虛擬主機的鑑定模組，而非正在參與電子社群之主要鑑定伺服器的鑑定模組。 使用時，這個模組也必須配置爲後置授權模組。
unauth pdpwi-unauth-module	未經鑑定使用者鑑定模組。 這個模組是基於完整性而列示在這裡。它永遠隱含地配置爲最低優先順序的鑑定模組，而且用來產生未經鑑定使用者的證明。
ltpa pdwpi-ltpa-module	LTPA 鑑定模組 接受並鑑定以 LTPA cookie 爲基礎的使用者。 LTPA cookie 可以由 WebSEAL 或由 WebSphere 伺服器提供。
spnego pdwpi-spnego-module	SPNEGO 鑑定模組 利用 Windows LAN 網域內的標準 SPNEGO 鑑定通訊協定，來達成「單一登入」解決方案，以便在 IIS 上實作外掛程式。

表 38. 外掛程式階段作業模組參照

模組	說明
BA pdwpi-ba-module	「基本鑑定」階段作業模組。 使用「基本鑑定授權」標頭值作爲階段作業金鑰。 使用時，也必須配置爲鑑定模組。 也可配置爲後置授權模組。
ip-addr pdwpi-ipaddr-module	「IP 位址」階段作業模組。 使用已鑑定用戶端 IP 位址作爲階段作業金鑰。 使用時，它也必須配置爲鑑定模組。
http-hdr pdwpi-httphdr-module	「HTTP 標頭」階段作業模組。 使用已鑑定用戶端標頭作爲階段作業金鑰。 使用時，它也必須配置爲鑑定模組。
session-cookie pdwpi-sesscookie-module	「階段作業 Cookie」階段作業模組。 這個模組會產生並接受用來識別階段作業的 cookie。通常僅作爲低優先順序的階段作業識別機制。
ssl-id pdwpi-sslsessid-module	「SSL 階段作業 ID」階段作業模組。 使用「SSL 階段作業 ID」作爲階段作業金鑰。請注意，雖然這個模組是在 Tivoli Access Manager Plug-in for Web Servers 的 Windows 配送中提供的，但是 Microsoft Internet Information Services Web Server 不會提供「SSL 階段作業 ID」資訊給外掛程式，所以「SSL 階段作業 ID」無法作爲 IIS 的階段作業金鑰。
iv-headers pdwpi-iv-headers-module	IV 標頭階段作業模組
spnego pdwpi-spnego-module	SPNEGO 階段作業模組 利用 Windows LAN 網域內的標準 SPNEGO 鑑定通訊協定，來達成「單一登入」解決方案，以便在 IIS 上實作外掛程式。 僅在鑑定處理期間，才會使用這個模組，在鑑定完成後，至少有一個其他階段作業模組必須用來維護階段作業。

表 39. 外掛程式後置授權模組參照

模組	說明
套表 pdwpi-forms-module	「HTML 套表」後置授權模組。 在「HTML 套表型」登入期間，這個模組會處理套表資料的送出。 使用時，它也必須配置爲鑑定模組。 這個模組也可以從送出的使用者名稱及密碼來設定 BA 標頭。
BA pdwpi-ba-module	「基本鑑定」後置授權模組。 修改 Web 伺服器所看到的 BA 標頭，或從 GSO 鎖定框資料建立它，來修改此標頭。
token pdwpi-token-module	記號後置授權模組。 Tivoli Access Manager Plug-in for Web Servers 可支援利用用戶端提供的記號通行代碼進行鑑定。這種鑑定會使用兩個以 RSA SecureID 墜飾爲基礎的因子登入。 使用時，記號模組也必須配置爲鑑定模組。
failover pdwpi-failovercookie-module	失效接替 Cookie 後置授權模組。 這個模組會爲用戶端建立一個失效接替 cookie。 使用時，失效接替 cookie 模組也必須配置爲鑑定模組。
iv-headers pdwpi-iv-headers-module	「IV 標頭」後置授權模組。 在容許 Web 伺服器處理要求前，這個模組會將使用者識別資訊，當作 IV 標頭插入至要求中。這有助於提供單一登入至 Web 伺服器所掌控的應用程式。可以新增的標頭是 iv-user、iv-user-l、iv-groups、iv-creds 及 iv-remote-address。 這個模組也可配置爲鑑定模組及階段作業模組。
tag-value pdwpi-tag-value-module	標籤/值後置授權模組。 在容許 Web 伺服器處理要求前，這個模組會將來自使用者證明的額外延伸屬性，當作 IV 標頭插入至要求中。這些延伸屬性通常會對映至來自使用者登錄的使用者屬性。
acctmgmt pdwpi-acct-mgmt-module	「帳戶管理」後置授權模組。 這個模組會提供登出 (/pkmslogout)、變更密碼 (/pkmspasswd)、說明 (/pkmshelp) 功能。
ltpa pdwpi-ltpa-module	LTPA Cookie 後置授權模組。 在容許 Web 伺服器處理要求前，這個模組會將 WebSphere Application Server (WAS) 的「輕裝備協力廠商鑑定 (LTPA)」cookie 插入至要求。這會提供單一登入至正被 Web 伺服器掌控的應用程式。

表 39. 外掛程式後置授權模組參照 (繼續)

模組	說明
ecsso pdpwi-ecsso-module	「電子社群單一登入」後置授權模組。 所有參與電子社群的虛擬主機必須具有配置爲後置授權模組的 ecsso 模組。 這個模組也必須配置爲所有參與者的鑑定模組，但主要鑑定伺服器除外。
login-redirect pdwpi-loginredirect-module	「登入重新導向」後置授權模組。 當使用任一個外掛程式支援的方法，來執行登入時，一旦鑑定成功，使用者就會重新導向至已配置的頁面。

附錄 C. 指令快速參照

下列是可被執行以執行各種 IBM Tivoli Access Manager Plug-in for Web Server 作業之指令的說明。

pdwebpi_start

在 UNIX 上進行安裝時，啓動及停止外掛程式處理程序。

有效的選項如下：

```
pdwebpi_start {start|stop|restart|status}
```

若要停止外掛程式，再重新啓動它，請使用：

```
# pdwebpi_start restart
```

pdwebpi_start 指令位於下列目錄：

```
/opt/pdwebpi/sbin/
```

若要啓動及停止外掛程式 Windows 安裝，請在「服務控制台」中找出外掛程式處理程序，然後使用適當的控制按鈕。

pdwpi-cdsso-key-gen

建立用於加密及解密外掛程式資料（如失效接替 cookie 資訊及擔保記號）的金鑰檔案。

用法：

```
./pdwpi-cdsso-key-gen key_file_name_to_create
```

pdwpi-cdsso-key-gen 指令位於 `/bin` 目錄中。

pdwpi-version

列示安裝作業的版本及著作權資訊。

用法：

```
./pdwpi-version
```

pdwpi-version 指令位於 `/bin` 目錄中。

pdwpicfg

啓動配置及解除配置外掛程式的公用程式。

pdwpicfg 指令位於 `/bin` 目錄中。

用法：
UNIX:

```
./pdwpicfg
```

Windows 指令行：

```
pdwpicfg-cl
```

選項：

```
pdwpicfg -a [configure|unconfigure] -A
admin_id -P admin_pwd
parameter1 parameter2 ...
```

其中：

-A *admin_id* 是「Tivoli Access Manager 管理者」名稱。

-P *admin_pwd* 是「Tivoli Access Manager 管理者」密碼。

配置用法

```
pdwpicfg -a configure -A admin_id -P admin_pwd -p port_num
-t server_type -d ldap_admin_dn -m ldap_admin_pwd -s
[ -k key_file -w key_file_pwd -c cert_label -l ssl_port ]
{ -iis options- } { -iplanet options- } { -ihs options- }
```

選項：

-p *port_num*	伺服器的接聽埠號（預設值是 7237）
-t *server_type*	Web 伺服器類型，如 IIS、iPlanet 或 IHS
-d *ldap_admin_dn*	LDAP 管理者 DN（預設值是 cn=root）
-m *ldap_admin_pwd*	LDAP 管理者密碼
-s	啓用與 LDAP Server 的 SSL 通訊
-k *key_file*	LDAP SSL 金鑰檔案
-w *key_file_pwd*	LDAP SSL 金鑰檔案密碼
-c *cert_label*	LDAP 用戶端憑證標籤（如果需要的話）
-l *ssl_port*	LDAP SSL 埠（預設值是 636）
-v *vhosts*	將受到保護的虛擬主機。此值的格式應爲列出各虛擬主機 ID，其間並以逗點隔開。虛擬主機 ID 之間不應有空格。

IIS 選項：

-d	啓用 IIS 過濾器。

iPlanet 選項：

-i iplanet_dir	iPlanet 安裝根目錄。如果沒有指定任何目錄，將預設爲 /usr/iplanet/servers

IHS 選項：

-i ihs_dir	IHS 安裝根目錄。

解除配置用法

```
pdwpicfg -a unconfigure -A admin_id -P admin_pwd -f -D {acls|objspace|all}
```

選項：

-f	強制解除配置，忽略所有錯誤
-D	從原則資料庫移除指定的資料，其中： acls: 僅移除 pdwebpi default ACL 及 pdwebpi 動作群組。 objspace: 移除 /PDWebPI/*vhost* 物件空間。 all: 同時移除 acls 及物件空間。

附錄 D. 注意事項

本資訊是針對 IBM 在美國所提供之產品與服務開發出來的。 而在其他國家或地區中，IBM 不見得有提供本書中所提的各項產品、服務、或功能。如果要了解您所在的地區目前是否可使用這些產品與服務，請向當地的 IBM 服務代表查詢。本書在提及 IBM 的產品、程式或服務時，不表示或暗示只能使用 IBM 的產品、程式或服務。只要未侵犯 IBM 的智慧財產權，任何功能相當的產品、程式或服務都可以取代 IBM 的產品、程式或服務。不過，其他非 IBM 產品、程式、或服務在運作上的評價與驗證，其責任屬於使用者。

在這本書或文件中可能包含著 IBM 所擁有之專利或專利申請案。本書使用者並不享有前述專利之任何授權。您可以用書面方式來查詢授權，來函請寄到：

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

若要查詢有關二位元組 (DBCS) 資訊的特許權限事宜，請聯絡您國家或地區的 IBM 智慧財產部門，或者用書面方式寄到：

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

下列段落若與該國之法律條款抵觸，即視為不適用： IBM 僅以「現狀」提供本書，而不提供任何明示或默示之保證（包括但不限於可商用性或符合特定效用的保證）。若有些地區在某些交易上並不允許排除上述保證，則該排除無效。

本資訊中可能會有技術上或排版印刷上的訛誤。因此，IBM 會定期修訂；並將修訂後的內容納入新版中。同時，IBM 得隨時改進並/或變動本書中所提及的產品及/或程式。

本資訊中任何對非 IBM 網站的敘述僅供參考，IBM 對該網站並不提供保證。該網站上的資料，並非本 IBM 產品所用資料的一部分，如因使用該網站而造成損害，其責任由貴客戶自行負責。

IBM 得以各種適當的方式使用或散佈由 貴客戶提供的任何資訊，而無需對您負責。

本程式之獲授權者若希望取得相關資料，以便使用下列資訊者可洽詢 IBM。其下列資訊指的是： (1) 獨立建立的程式與其他程式（包括此程式）之間更換資訊的方式 (2) 相互使用已交換之資訊方法 若有任何問題請聯絡：

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758
U.S.A.

上述資料之取得有其特殊要件，在某些情況下必須付費方得使用。

IBM 基於雙方之「IBM 客戶合約」、「IBM 國際程式授權合約」或任何同等合約之條款，提供本書中所說的授權程式與其所有適用的授權資料。

任何此處涵蓋的執行效能資料都是在一個受控制的環境下決定出來的。因此，若在其他作業環境下，所得的結果可能會大大不同。有些測定已在開發階段系統上做過，不過這並不保證在一般系統上會出現相同結果。再者，有些測量可能已透過推測方式評估過。但實際結果可能並非如此。本書的使用者應依自己的特定環境，查證適用的資料。

本書所提及之非 IBM 產品資訊，係一由產品的供應商，或其出版的聲明或其他公開管道取得。IBM 並未測試過這些產品，也無法確認這些非 IBM 產品的執行效能、相容性、或任何對產品的其他主張是否完全無誤。如果您對非 IBM 產品的性能有任何的疑問，請逕向該產品的供應商查詢。

有關 IBM 未來動向的任何陳述，僅代表 IBM 的目標而已，並可能於未事先聲明的情況下有所變動或撤回。

此資訊僅適用於規劃目的。在所說明的產品推出前，這裡的資訊隨時都有可能更改。

此資訊包含日常商業行爲之資料和報告的範例。爲了儘可能的說明這些範例，其包括有個人、公司、品牌和產品。此等名稱皆屬虛構，凡有類似實際企業所用之名稱及地址者，皆屬巧合。

若您檢視的是本資訊的電子檔，其中的圖片和圖例可能不會顯現。

商標

下列專有名詞是 IBM 公司在美國和/或其他國家或地區的商標或註冊商標：

AIX
DB2
IBM
IBM（標誌）
Java
OS/390
SecureWay
Tivoli
Tivoli（標誌）
Universal Database
WebSphere
z/OS
zSeries

Microsoft 和 Windows 是 Microsoft Corporation 在美國和/或其他國家或地區的商標。

UNIX 是 The Open Group 在美國和其他國家或地區的註冊商標。

其他公司、產品及服務名稱，可能是第三者的商標或服務標誌。

名詞解釋

二劃

入口網站（portal）. 一種整合的網站，它會根據某一使用者的存取權，以動態方式產生自訂的 Web 資源清單（如鏈結、內容或服務），供特定使用者使用。

四劃

公開金鑰（public key）. 在電腦安全中，每一個人都可使用的金鑰。請對照*私密金鑰（private key）*。

五劃

主機（host）. 連接到網路（例如網際網路或 SNA 網路），並可提供對該網路之存取點的電腦。同時，視環境而定，主機可以提供對網路的集中控制。主機可以是用戶端、伺服器或同時爲用戶端和伺服器。

加密（encryption）. 在電腦安全中，將資料轉換成無法辨識的格式的程序，以防止取得原始資料或僅能由解密程序來取得資料。

可調性（scalability）. 網路系統回應漸增的存取資源使用者數量的能力。

外部授權服務程式（external authorization service）. 一種授權 API 執行時期外掛程式，可用來使應用程式或環境特有的授權決策成爲 Access Manager 授權決策鏈的一部份。客戶可以使用「授權 ADK」來開發這些服務。

目錄綱目（directory schema）. 可以出現在目錄中的有效屬性類型及物件類別。屬性類型及物件類別定義屬性值的語法。必須呈現的屬性及目錄可以呈現的屬性。

六劃

企業應得權力（business entitlement）. 使用者證明的補充屬性，用來說明定義精細的條件，這些都是可用在資源的授權要求中的條件。

回應檔（response file）. 一種檔案，這個檔案包含一組預先定義的問題（由程式提出）解答，可使用它而不必一次又一次地輸入其中一值。

多工 proxy 代理站（multiplexing proxy agent (MPA)）. 容納多個用戶端存取的閘道。當用戶端使用 WAP 存取安全網域時，這些閘道有時又稱爲「無線存取通訊協定（WAP）」閘道。該閘道會建立單一鑑定頻道到原始伺服器，並透過此頻道「穿通」所有的用戶端要求和回應。

多重因子鑑定（multi-factor authentication）. 一種受保護的物件原則（POP），強制使用者使用兩個或以上的鑑定層次來進行鑑定。例如，受保護資源上的存取控制可以要求使用者同時以名稱/密碼及使用者名稱/記號通行碼來進行鑑定。另請參閱*受保護的物件原則*。

字尾（suffixes）. 一種識別名稱，可用來識別本端環境所保留的目錄階層中的頂端項目。由於「輕裝備目錄存取通訊協定（LDAP）」使用相對命名綱目，所以此字尾適用於該目錄階層內的其他每一個項目。目錄伺服器可以有多個字尾，每一個分別指出本端環境所保留的目錄階層。

存取控制清單（access control list）. (1) (2) 在電腦安全中，這是與某個物件相關的一份清單，這份清單指出可存取物件的所有主題以及這些主題的存取權。例如，存取控制清單就是與檔案相關的一份清單，這份清單會指出可存取檔案的使用者，並指出使用者對於該檔案的存取權。

存取控制群組（access control groups）. 用於存取控制的群組。每一個群組包含由許多值組成的屬性，這些屬性中含有許多成員識別名稱。存取控制群組的物件類別爲 `AccessGroup`。

存取控制（access control）. 在電腦安全中，這是指確定電腦系統的資源只能由獲得授權的使用者以授權的方式來加以存取的程序。

存取權（access permission）. 套用至整個物件的存取專用權。或是，套用至屬性存取類別的許可權。

安全 Socket 層（secure sockets layer (SSL)）. 可提供通訊私密的安全性通訊協定。SSL 可避免用戶端/伺服器應用程式之間的通訊遭到竊取、竄改或僞造。 SSL 是由 Netscape Communications Corp. 和 RSA Data Security, Inc. 所開發。

安全管理（security management）. 專門解決組織對重要的應用程式和資料的存取控制能力的管理原則。

安全網域（secure domain）. 共用共同服務的使用者、系統和資源群組，通常有共同目的的運作。

自行註冊（self-registration）. 這是一種處理程序，使用者可使用它來輸入必要的資料並成爲已註冊的 Tivoli Access Manager 使用者，而不需管理者的介入。

七劃

私密金鑰（private key）. 在電腦安全中，只有擁有者才知道的金鑰。請對照*公開金鑰（public key）*。

角色指定（role assignment）. 指定角色給使用者的處理程序，如此使用者就會對定義給該角色的物件具有適當的存取權。

角色啓動（role activation）. 將存取權套用至角色的處理程序。

八劃

使用者登錄（user registry）. 請參閱*登錄*。

使用者（User）. 使用他方所提供之服務的人員、組織、處理程序、裝置、程式、通訊協定或系統。

制式資源 ID（uniform resource identifier (URI)）. 用來識別網際網路上位置內容的方法。 URL（制式資源定位器）是特殊形式的 URI，用來識別網頁位址。 URI 通常說明 (a) 用來存取資源（例如，HTTP、HTTPS、FTP）的機制、 (b) 資源儲存所在的特定電腦（例如，www.webserver.org），以及電腦上資源的特定名稱（例如，/products/images/serv.jpg）。

制式資源定位器（uniform resource locator (URL)）. 一連串字元，代表電腦上或網路（網際網路）中的資訊資源。這一連串的字元包括 (a) 用來存取資訊資源之通訊協定的縮寫名稱，以及 (b) 通訊協定用來尋找資訊資源的資訊。例如，在網際網路的環境定義中，這些是部份用來存取各種資訊資源之通訊協定的縮寫：
http、ftp、gopher、telnet，以及 news；下列是 IBM 首頁的 URL：http://www.ibm.com。

受保護的物件空間（protected object space）. 使用於套用授權服務程式使用的 ACL 和 POP 的實際系統資源的虛擬物件表示式。

受保護的物件原則（protected object policy，POP）. 一種安全原則的類型，指出順利完成 ACL 原則檢查之後存取受保護資源的額外條件。POP 的範例包括日期時間存取和保護品質的層次。

服務（service）. 由伺服器所執行的工作。服務可以是讓資料傳送或儲存的簡單要求（例如，利用檔案伺服器、HTTP 伺服器、電子郵件伺服器和 finger 伺服器），也可以是更複雜的工作，例如，列印伺服器或處理程序伺服器。

金鑰資料庫檔案（key database file）. 請參閱*金鑰環（key ring）*.

金鑰對（key pair）. 在電腦安全中，指公開金鑰及私密金鑰。將金鑰配對用於加密時，傳送者會使用公開金鑰將訊息加密，收件人則使用私密金鑰將訊息解密。將金鑰配對用於簽章時，簽章者會使用私密金鑰將訊息表示法加密，收件人則使用公開金鑰將訊息表示法解密，以便驗證簽章。

金鑰檔（key file）. 請參閱*金鑰環（key ring）*。

金鑰環（key ring）. 在電腦安全中，含有公開金鑰、私密金鑰、最高授信使用者和憑證的檔案。

金鑰（key）. 在電腦安全中，和密碼演算法一起使用的一組符號順序，可用來將資料加密或解密。請參閱*私密金鑰*及*公開金鑰*。

九劃

保護的品質（quality of protection）. 資料安全性的層級，由鑑定、完整性和私密性條件的組合來決定。

十劃

原則伺服器（policy server）. 維護關於其他伺服器在安全網域中的位置資訊的 Tivoli Access Manager 伺服器。

原則資料（policy data）. 同時包含密碼強度原則資料和登入資料。

原則（policy）. 套用到受管理資源的一組規則。

記號（token）. (1) 在區域網路中，從某個資料站持續傳送到另一個資料站的權限的符號，以表示該站暫時控制了傳輸媒體。每一個資料站都有機會取得和使用記號來控制媒體。記號是一種特定的訊息或位元型樣，可表示傳輸許可權。 (2) 在區域網路（LAN）中，透過傳輸媒體，從一個裝置傳送到另一個裝置的位元順序。當記號已附加資料時，記號就變成訊框。

配置區物件（container object）. 將物件空間組織成不同功能區的結構化指定。

配置（configuration）. (1) 組織和交互連接資訊處理系統之軟硬體的方式。 (2) 組成系統、子系統或網路的裝置和程式。

十一劃

動作（action）. 存取控制清單（ACL）許可權屬性。

基本鑑定（basic authentication）. 鑑定方法之一，需要使用者輸入有效的使用者名稱及密碼後，才授與安全線上資源的存取權限。

執行時期（run time）. 執行電腦程式的期間。執行時期環境是一個執行環境。

密碼（cipher）. 加密的資料是無法讀取的，除非用金鑰將它轉換成純資料（解密）。

專用權屬性憑證服務（privilege attribute certificate service）. (1) 在 Tivoli Access Manager 中，專用權屬性憑證服務是用來以可在僅文字環境中傳輸的格式，對 Tivoli Access Manager 證明進行編碼或解碼。格式是 ASN1 及 MIME 編碼的組合。服務是內建在 Tivoli Access Manager 授權 API。 (2) 將以預先決定的格式表示的 PAC 轉換成 Access Manager 證明（或反之）的授權 API 執行時期用戶端外掛程式。這些服務也可以用來包裝或配置 Access Manager 證明，以傳輸至安全網域的其他成員。客戶可以使用「授權 ADK」來開發這些服務。 (3) 另請參閱*專用權屬性憑證*。 (4) Michelle, this term has two definitions, which one do you think should be used?

專用權屬性憑證（privilege attribute certificate）. 說明在外部定義給 Tivoli Access Manager 安全網域的資料配置區，它含有主體的鑑定及授權，以及能力。

常駐程式（daemon）. 用來執行標準服務的自動執行程式。有些常駐程式會自動觸發，以執行其作業；其他常駐程式則是定期執行。

接合（junction）. 前端 WebSEAL 伺服器與後端 Web 應用程式伺服器之間的 HTTP 或 HTTPS 連線。接合會以邏輯方式將後端伺服器的 Web 空間與 WebSEAL 伺服器的 Web 空間結合，讓您能以一致方式檢視整個 Web 物件空間。接合可讓 WebSEAL 代表後端伺服器提供保護服務。WebSEAL 在透過接合將資源的所有要求傳遞至後端伺服器之前，會對那些要求執行鑑定及授權檢查。接合同時也容許用戶端與已接合的後端應用程式之間有各種單一登入解決方案。

授權服務外掛程式（authorization service plug-in）. 一種可動態載入的程式庫（DLL 或共用程式庫），可由 Access Manager 授權 API 執行時期用戶端在起始設定時載入，以執行在「授權 API」內延伸服務介面的作業。目前可用的服務介面包括「管理」、「外部授權」、「證明修改」、「應得權力」以及 PAC 操作介面。客戶可以使用「授權 ADK」來開發這些服務。

授權（authorization）. (1) 在電腦安全中，指授與使用者與電腦系統通訊或使用電腦系統的權利。 (2) 授與使用者對物件、資源或功能的完整或有限存取權的程序。

移轉（migration）. 安裝新版本或新版次的程式，以取代較早的版本或版次。

許可權（permission）. 存取受保護的物件（如檔案或目錄）的能力。物件許可權的號碼及意義是由存取控制清單所定義。

通用閘道介面（common gateway interface (CGI)）. 一種在 Web 伺服器上執行的電腦程式，它會使用「通用閘道介面（CGI）」，來執行通常不是由 Web 伺服器執行的作業（例如，資料庫存取及表格處理）。 CGI Script 是一種以 Scripting 語言（如 Perl）撰寫的 CGI 程式。

連結（bind）. 將識別字與程式中的另一個物件相關聯；例如，將識別字與某個值、位址或另一個識別字關聯，或者將正式的參數與實際的參數相關聯。

連線（connection）. (1) 在資料通訊中，指功能單元之間所建立的關聯，以用於傳遞資訊。 (2) 在 TCP/IP 中，指提供可靠的資料匯流遞送服務的兩個通訊協定應用程式之間的路徑。在網際網路中，連線會從某個系統的 TCP 應用程式延伸到另一個系統上的 TCP 應用程式。 (3) 在系統通訊中，指可在兩個系統間或系統和裝置間傳送資料的線路。

十二劃

最高授信使用者（trusted root）. 在「安全 Socket 層（SSL）」，公開金鑰和憑證管理中心（CA）的關聯識別名稱。

單一登入（single signon (SSO)）. 指使用者能夠登入一次，並且可存取多個應用程式，不需個別地登入至每一個應用程式。另請參閱*廣域登入*。

無聲安裝（silent installation）. 一種安裝方式，它不會傳送訊息給主控台，而是將訊息和錯誤儲存在日誌檔中。此外，自動安裝可以使用回應檔來輸入資料。另請參閱*回應檔*。

登錄（registry）. (1) 維護允許參與安全網域的使用者和群組之帳戶資訊的資料儲存處。 (2) 含有系統配置資訊的資料庫，這些資訊與使用者、硬體和已安裝的程式和應用程式有關。

虛擬主機（virtual hosting）. 容許 Web 伺服器被當作網際網路上的多個主機的能力。

超文字轉送通訊協定（hypertext transfer protocol (HTTP)）. 在網際網路通訊協定組中，指用來轉送和顯示超本文文件的通訊協定。

進階鑑定（step-up authentication）. 一種受保護的物件原則（POP），它會依賴已預先配置的鑑定層次，並依據資源上所設定的原則來執行特定的鑑定層次。進階鑑定 POP 雖然不會強制使用者使用多個鑑定層次來進行鑑定，以存取任何給定的資源，但是需要使用者在與保護資源的原則所需的層次一樣高的層次中進行鑑定。

十三劃

傳送選擇器（transport selector (TSEL)）. 與 TCP/IP 中的埠號相當的 Open Systems Interconnection（OSI）。亦稱爲 TSEL 號碼。

資源物件（resource object）. 代表眞正的網路資源，如服務、檔案及程式。

跨處理通訊（interprocess communication (IPC)）. 可讓程式同時處理許多使用者要求的方法，做法爲建立及管理同時在作業系統中執行的個別程式程序。

跨網域對映架構（cross domain mapping framework (CDMF)）. 一種程式設計介面，可讓程式開發者自訂如何對映使用者的身份，以及當使用 WebSEAL e-Community SSO 功能時，如何處理使用者屬性。

跨網域鑑定服務（cross domain authentication service (CDAS)）. 一種提供共用程式庫機制的 WebSEAL 服務，這種機制可讓您將預設 WebSEAL 鑑定機制換成一個可傳回 Tivoli Access Manager 身份給 WebSEAL 的自訂程序。另請參閱 *WebSeal*。

十四劃

管理伺服器（management server）. 已作廢。請參閱*原則伺服器*。

管理服務（administration service）. 一種授權 API 執行時期外掛程式，可用來對 Access Manager 資源管理程式執行管理要求。管理服務將回應來自 pdadmin 指令的遠端要求，以執行如下的作業：列示受保護的物件樹狀結構中葉節點下的物件。客戶可以使用「授權 ADK」來開發這些服務。

網域名稱（domain name）. 在網際網路通訊協定組中，指主機系統名稱。網域名稱是由一組子名稱順序所組成，並且以區隔字元隔開。例如，如果主機系統的完整網域名稱是 ralvm7.vnet.ibm.com，則下列每一個都是網域名稱：

- ralvm7.vnet.ibm.com
- vnet.ibm.com
- ibm.com

網域（domain）. (1) 電腦網路中負責控制資料處理資源的部分。 (2) 請參閱*網域名稱（domain name）*。

網路型鑑定（network-based authentication）. 一種受保護的物件原則（POP），用來依據使用者的網際網路通訊協定（IP）位址來控制物件存取。另請參閱*受保護的物件原則*。

網際網路通信協定組（Internet suite of protocols）. 一組爲了網際網路使用所開發的通訊協定，並透過 Internet Engineering Task Force（IETF）發佈爲「備註要求（RFC）」。

網際網路通信協定（Internet protocol (IP)）. 在網際網路通信協定組中，指一種無須連線的通訊協定，可透過網路或交互連接的網路來遞送資料，並且可作爲較高通訊協定層與實體網路之間的媒介。

綱目（schema）. 以資料定義語言表示的陳述式，以完整說明資料庫的結構。

輕裝備目錄存取通訊協定（lightweight directory access protocol (LDAP)）. 一種開放式通訊協定，(a) 使用 TCP/IP 來提供對支援 X.500 模式之目錄的存取 (b) 不必具備更複雜的 X.500 目錄存取通訊協定（DAP）所需要的資源。使用 LDAP（亦稱爲啓用目錄的應用程式）的應用程式可以使用目錄來作爲通用的資料儲存庫以及擷取人員或服務的相關資訊，例如電子郵件位址、公開金鑰或服務特定的配置參數。LDAP 原先是在 RFC 1777 中指定的。LDAP 第 3 版是在 RFC 2251 中指定，而 IETF 仍在繼續處理其他的標準功能。在 RFC 2256 中可以找到某些由 IETF 定義的 LDAP 標準綱目。

輕裝備協力廠商鑑定（lightweight third party authentication (LTPA)）. 一種鑑定架構，容許跨過一組落在網際網路網域內的 Web 伺服器進行單一登入。

遞送檔（routing file）. 一個含有指令的 ASCII 檔，這些指令係用來控制訊息的配置。

十五劃

廣域登入（global signon (GSO)）. 彈性的單一登入解決方案，可讓使用者提供替代使用者名稱和密碼給後端 Web 應用程式伺服器。廣域登入可讓使用者存取他們獲權使用的計算資源 — 透過單一登入。 GSO 係針對由異質、分散式運算環境內的多部系統和應用程式所組成之大型企業而設計，用來消弭使用者管理多個使用者名稱和密碼之需。另請參閱單一登入。

數位簽章（digital signature）. 在電子商務中，附加到資料單位的資料，或資料單位的加密轉換，可讓資料單位的收件人驗證單位的來源和完整性，並且辨識可能的僞造資料。

複本（replica）. 含有另一個伺服器的目錄複本的伺服器。複本會備份伺服器，以便加強效能或縮短回應時間，並確定資料的完整性。

輪詢（polling）. 在其中做出資料要求的頻道存取方法（CAM）。在主要/從屬實務範例中，主要裝置會輪流查詢每一個從屬裝置，是否具有任何要傳輸的資料。如果從

屬裝置回答有，將允許裝置傳輸它的資料。如果從屬裝置回答沒有，則主要裝置將離開，並輪詢下一個從屬裝置。這個處理程序會持續的重複。對於 Tivoli Access Manager，您可以配置 WebSEAL 伺服器，以定期輪詢主要授權（原則）資料庫，來取得更新資料。

十六劃

憑證管理中心（certificate authority (CA））. 在電子商務中，指負責發出憑證的組織。憑證管理中心會鑑定憑證擁有者的身份以及所有者被授權使用的服務、發出新的憑證、更新現有的憑證，以及將不再被授權使用憑證的使用者的憑證加以取消。

憑證（certificate）. 在電腦安全中，指一種數位文件，可將公開金鑰連結到憑證擁有者的身份，因此可對憑證擁有者進行鑑定。憑證是由憑證管理中心所發出。

十七劃

應得權力服務（entitlements service）. 一種授權 API 執行時期外掛程式，可用來從主體或一組條件的外部來源傳回應得權力。應得權力通常是應用程式特有的資料，將由資源管理程式以某種方式來加以使用，或新增至主體的證明，以便在授權程序中進一步的使用。客戶可以使用「授權 ADK」來開發這些服務。

應得權力（entitlement）. 含有外部化安全原則資訊的資料結構。應得權力含有原則資料，或以特定應用程式可以瞭解的方式來加以格式化的能力。

檔案轉送通訊協定（file transfer protocol (FTP)）. 在網際網路通訊協定組中，指利用「傳輸控制通訊協定（TCP）」和 Telnet 等服務在機器或主機之間轉送大量資料檔的應用程式層的通訊協定。

十九劃

識別名稱（distinguished name，DN）. 可唯一識別目錄中之項目的名稱。識別名稱是由*屬性:值*配對所組成，這些配對是以逗點區隔。

證明修改服務（credentials modification service）. 一種授權 API 執行時期外掛程式，可用來修改 Access Manager 證明。由客戶在外部開發的證明修改服務僅限於執行從證明屬性清單新增及移除的作業，以及僅限於那些被視爲可更改的屬性。

證明（credentials）. 在鑑定期間所取得，說明使用者、任何的群組關聯及其他安全相關的身份屬性的詳細資訊。證明可用來安全地執行許多服務，例如授權、審核和委任。

二十一劃

屬性清單（attribute list）. 在 Tivoli Access Manager 中，含有延伸資訊的已鏈結清單，這些資訊係用來做出授權決策。屬性清單是由一組 *keyword = value* 配對所構成。

二十二劃

鑑定（authentication）. (1) 在電腦安全中，指驗證使用者的身份或使用者存取物件的資格。 (2) 在電腦安全中，指驗證訊息尚未更改或損毀。 (3) 在電腦安全中，指用來驗證資訊系統或受保護資源之使用者的程序。另請參閱*多重因子鑑定*、*網路型鑑定*，以及*進階鑑定*。

A

ACL. 請參閱*存取控制清單*。

B

BA. 請參閱*基本鑑定*。

blade. 提供應用程式特有的服務及元件的元件。

C

CA. 請參閱*憑證管理中心*。

CDAS. 請參閱*跨網域鑑定服務*。

CDMF. 請參閱*跨網域對映架構*。

CGI. 請參閱*通用閘道介面*。

cookie. 伺服器儲存在用戶端機器，並在後續的階段作業期間存取的資訊。cookie 容許伺服器記住關於用戶端的特定資訊。

D

DN. 請參閱*識別名稱（distinguished name）*。

E

EAS. 請參閱*外部授權服務程式*。

G

GSO. 請參閱*廣域登入*。

H

HTTP. 請參閱*超文字轉送通訊協定*。

I

IP. 請參閱*網際網路通信協定（Internet Protocol）*。

IPC. 請參閱*跨處理通訊*。

L

LDAP. 請參閱 *輕裝備目錄存取通訊協定（Lightweight Directory Access Protocol）*。

LTPA. 請參閱 *輕裝備協力廠商鑑定*。

M

meta 資料（metadata）. 說明已儲存資料之性質的資料。

P

PAC. 請參閱*專用權屬性憑證*。

POP. 請參閱*受保護的物件原則（protected object policy）*。

R

RSA 加密（RSA encryption）. 用於加密和鑑定的公開金鑰加密法系統。此系統是在 1977 年由 Ron Rivest、Adi Shamir 和 Leonard Adleman 所發明。系統的安全是根據對兩大質數的乘積所取的因數難度而定。

S

SSL. 請參閱*安全 Socket 層（Secure Sockets Layer）*。

SSO. 請參閱*單一登入*。

T

TSEL. 請參閱**傳送選擇器（transport selector）**。

U

URI. 請參閱*制式資源 ID*。

URL. 請參閱*制式資源定位器*。

W

WebSEAL. 一種 Tivoli Access Manager blade。WebSEAL 是一個高效能、多重執行緒的 Web 伺服器，它會將安全原則套用至受保護的物件空間。WebSEAL 可提供單一登入解決方案，將後端 Web 應用程式資源納入其安全原則內。

WPM. 請參閱*Web Portal Manager*。

特殊字元

Tivoli Access Manager for Business Integration. 一種 Tivoli Access Manager blade，它會提供廣泛的安全服務給 IBM MQSeries。它會延伸 MQSeries 環境，以支援跨佇列的端對端安全性。

Tivoli Access Manager for Operating Systems. 一種 Tivoli Access Manager blade，它會提供安全引擎給 Tivoli Identity Director 產品。這種安全引擎會截取需要授權檢查的作業系統呼叫，如檔案存取。

Web Portal Manager（WPM）. 用來管理安全網域中之 Tivoli Access Manager Base 及 WebSEAL 安全原則的 Web 型圖形式應用程式。這個 GUI 可代替 **pdadmin** 指令行介面，讓遠端管理者能夠存取，並且讓管理者能夠建立委任的使用者網域，以及指定委任管理者給這些網域。

索引

索引順序以中文字，英文字，及特殊符號之次序排列。

〔三劃〕

〔四劃〕

〔五劃〕

〔六劃〕

〔七劃〕

〔八劃〕

〔九劃〕

〔十劃〕

〔十一劃〕

〔十二劃〕

〔十三劃〕

〔十四劃〕

〔十五劃〕

〔十六劃〕

〔十九劃〕

〔二十二劃〕

A

B

C

D

E

F

G

H

I

L

M

N

P

Q

R

S

T

U

V

W

讀者意見表

爲使本書盡善盡美，本公司極需您寶貴的意見；懇請您使用過後，撥冗填寫下表，惠予指教。

請於下表適當空格內，填入記號（∨）；我們會在下一版中，作適當修訂，謝謝您的合作!

評估項目	評 估 意 見		備 註
正 確 性	內容說明與實際程序是否符合	□是□否	
	參考書目是否正確	□是□否	
一 致 性	文句用語及風格，前後是否一致	□是□否	
	實際畫面訊息與本書所提之畫面訊息是否一致	□是□否	
完 整 性	是否遺漏您想知道的項目	□是□否	
	字句、章節是否有遺漏	□是□否	
術語使用	術語之使用是否恰當	□是□否	
	術語之使用，前後是否一致	□是□否	
可 讀 性	文句用語是否通順	□是□否	
	有否不知所云之處	□是□否	
內容說明	內容說明是否詳盡	□是□否	
	例題說明是否詳盡	□是□否	
排版方式	本書的形狀大小，版面安排是否方便使用	□是□否	
	字體大小，顏色編排，是否有助於閱讀	□是□否	
目錄索引	目錄內容之編排，是否便於查考	□是□否	
	索引語錄之排定，是否便於查考	□是□否	
	※評估意見爲 "否" 者，請於備註欄說明。		

其他：（篇幅不夠時，請另紙說明。）

上述改正意見，一經採用，本公司有合法之使用及發佈權利，特此聲明。

IBM Tivoli Access Manager SC40-1158-00

Plug-in for Web Servers 使用手冊

第 4.1 版

折疊線

台北市 110 基隆路一段 206 號

大臺灣中華研發中心國際商業機器股份有限公司

軟體國際部 啟

廣告回信

台灣北區郵政管理局登記證

北台字第0587號

（免貼郵票）

寄件人 姓名：

地址：

寄

折疊線

讀者意見表

Printed in Australia

SC40-1158-00