IBM Tivoli Access Manager Plug-in for Edge Server

使用手冊

第 4.1 版

SC40-1168-00

IBM Tivoli Access Manager Plug-in for Edge Server

使用手冊

第 4.1 版

SC40-1168-00

附註

使用此資訊和它支援的產品前，請先閱讀第 63 頁的附錄 D, 『注意事項』中的資訊。

第二版 (October 2002)

本版本取代 GC40-0839-00。

目錄

前言

IBM® Tivoli®Access Manager (Tivoli Access Manager) plug-in for IBM WebSphere® Edge Server（Edge Server 外掛程式）提供鑑定和授權安全服務。此 Edge Server 外掛程式安裝在 Edge Server 快取 Proxy，是您用戶端和 Web 伺服器間的閘道，實作用以保護您的 Web 資源之安全原則。此外掛程式經由虛擬主機，於快取 Proxy 保全 Web 內容及應用程式伺服器資源，並爲受保護的 Web 伺服器提供單一登入解決方案。

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 軟體與說明文件的使用者而言，專有名詞「*管理伺服器*」現稱爲「*原則伺服器*」。

IBM Tivoli Access Manager Plug-in for Edge Server User's Guide 提供安裝指示、管理程序，以及技術參考手冊，來使用 Edge Server 外掛程式以保護您的 Web 網域。

本書適用對象

本書適用對象爲負責安裝、部署及管理 Edge Server 外掛程式的系統管理者。

讀者必須熟悉以下各項：

- Microsoft® Windows® 和 UNIX® 作業系統
- 安全管理
- 網際網路通訊協定，包括 HTTP、HTTPS 和 TCP/IP
- 「輕裝備目錄存取通訊協定」(LDAP) 和目錄服務
- 鑑定和授權
- Tivoli Access Manager 安全模型和其功能

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 頁的第 1 章, 『簡介 IBM Tivoli Access Manager plug-in for Edge Server』
  說明 Tivoli Access Manager 安全模型及 Edge Server 外掛程式的安全加強功能。
- 第 5 頁的第 2 章, 『安裝 Edge Server 外掛程式』
  提供所有已支援平台的安裝及配置指示。
- 第 9 頁的第 3 章, 『管理 Edge Server 外掛程式』
  說明如何管理使用者帳戶、建立 Tivoli Access Manager 物件空間，以及啓動和停止外掛程式。同時說明 Edge Server 外掛程式之配置和日誌檔。
- 第 21 頁的第 4 章, 『了解 Edge Server 外掛程式配置』
  提供 Edge Server 外掛程式配置概觀。
- 第 27 頁的第 5 章, 『部署 Edge Server 外掛程式』

說明在 Web 商業環境中部署 Edge Server 外掛程式的範例。

- 第 31 頁的第 6 章, 『建立跨網域鑑定服務』

  解釋如何建立「跨網域鑑定服務」(CDAS) 共享程式庫，此程式庫可啓用自訂處理及用戶端鑑定資訊的自訂處理。也說明如何配置 Edge Server 外掛程式來辨識傳送到自訂共享程式庫之特定類型的鑑定資料。

- 第 45 頁的第 7 章, 『移除 Edge Server 外掛程式』

  說明如何從每一種支援的作業系統平台中解除 Edge Server 外掛程式的配置並將它移除。

- 第 49 頁的附錄 A, 『基礎配置檔參照』
- 第 51 頁的附錄 B, 『物件空間定義配置檔參照』
- 第 61 頁的附錄 C, 『wesosm 指令參照』

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』
- 『Base 資訊』
- 第 vii 頁的『WebSEAL 資訊』
- 第 vii 頁的『Web 安全性資訊』
- 第 vii 頁的『程式開發參考手冊』
- 第 viii 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*
  SC32-1131-00 (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 安裝指南*
  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 來管理您安全的 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 安全性資訊

- *IBM Tivoli Access Manager for WebSphere Application Server User's Guide*
  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)

  提供對 Web 伺服器使用外掛程式來保護 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)

  提供指令行公用程式及 Tivoli Access Manager 所提供的 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 Tivoli Access Manager 與定義爲使用者登錄的 IBM Directory 伺服器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。 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 是對電子商務使用 IBM Tivoli Access Manager 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，是對電子商務使用 IBM Tivoli Access Manager 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

本書針對特定的術語和動作、作業系統相關的指令和路徑以及邊距圖形使用數種慣例。

字體使用慣例

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、指令選項必須以斜體字呈現。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 Edge Server

Edge Server 外掛程式新增可爲 IBM WebSphere Edge Server 產品鑑定和授權功能。當此外掛程式在您的安全網域中實作爲授權服務程式時，可以提供單一登入解決方案給該網域中的資源。

本章說明 IBM Tivoli Access Manager 安全模型及 Edge Server 外掛程式的安全加強功能。

系統需求

在安裝及完全發揮功能之前， Tivoli Access Manager 必須具有特定的必備軟硬體。這些要件包括作業系統、硬體平台等等。如需最新資訊，請參閱 *IBM Tivoli Access Manager for e-business Release Notes*。

Tivoli Access Manager 安全模型

Edge Server 外掛程式可爲 Edge Server 快取 Proxy 新增鑑定和授權控制。爲了管理 Edge Server 外掛程式，您需要熟悉 Tivoli Access Manager 模型，以執行安全原則。

Tivoli Access Manager 模型是基於對必須套用到網路環境中的使用者、程式和資料的商業原則的瞭解。爲了建立安全環境，Tivoli Access Manager 需要管理者來定義下列實體：

- 要保全的物件
- 允許對每一個物件執行的動作
- 允許執行動作的使用者

Tivoli Access Manager 會按照下列所述來管理這些實體的每一個：

- 物件會在階層式受保護物件名稱空間或物件空間中定義並列出。
- 標準的動作（例如讀取和寫入）都是定義成許可權。管理者也可以定義自訂的應用程式特定動作。
- 使用者和群組是定義於 Tivoli Access Manager 支援的使用者登錄。

Tivoli Access Manager 將上述的概念合併，形成「存取控制清單」(ACL），這份清單是由特定使用者或群組與許可權（動作）清單組合而成的。管理者可將這些 ACL 連接到物件空間中的物件。

例如，管理者可以藉由將 ACL 連接到 Web 伺服器上階層式檔案系統頂端的檔案，來控制對 Web 伺服器內容的存取。管理者也可以選擇在較低的檔案階層套用更嚴格的 ACL。更嚴格的 ACL 會置換連接到階層頂端的 ACL。 Edge Server 外掛程式會根據所要求的動作，檢查每個所要求物件的讀取（**r**）、修改（**m**）或執行（**x**）許可權，來執行存取控制。

Tivoli Access Manager 安全模型富有彈性，並支援許多不同的配置。使用 Edge Server 外掛程式前，您先要熟悉 Tivoli Access Manager 功能。如需相關資訊，請參閱 *IBM Tivoli Access Manager Base Administrator's Guide*。

Edge Server 外掛程式安全環境

Edge Server 外掛程式與 IBM WebSphere Edge Server 一起使用可提供存取控制。它位於企業網路邊緣，於該處評估來自防火牆外的用戶端的存取要求。

Edge Server 是由兩個關鍵元件組成：

- 快取 Proxy
- 網路分派器

外掛程式是由每一要求上的快取 Proxy 元件呼叫，應要求決定使用者是否經過授權而可以存取所要求的資源。快取 Proxy 接著會執行外掛程式傳回的授權決策。雖然網路分派器元件不需執行外掛程式，但它可用於高容量環境中複寫伺服器間的負載平衡。

通常，當使用者從瀏覽器對網站發出要求時，提供的 URL 中所呈現的物件會對應到 Web 伺服器中的物件。 Edge Server 外掛程式可藉由驗證使用者是否經授權可對 Web 伺服器物件執行所要求的動作，來提供存取控制。外掛程式的做法是對照 Tivoli Access Manager 使用者登錄來驗證使用者身份，對照 Tivoli Access Manager 物件空間來爲使用者授權，如圖 1中所說明。外掛程式傳回狀態資訊到快取 Proxy，指出使用者是否經過授權可對物件執行所要求的動作。快取 Proxy 會使用這項資訊來拒絕或容許所要求的動作。當安全原則許可時，Edge Server 快取 Proxy 會快取所要求的物件，以使效能最佳化。

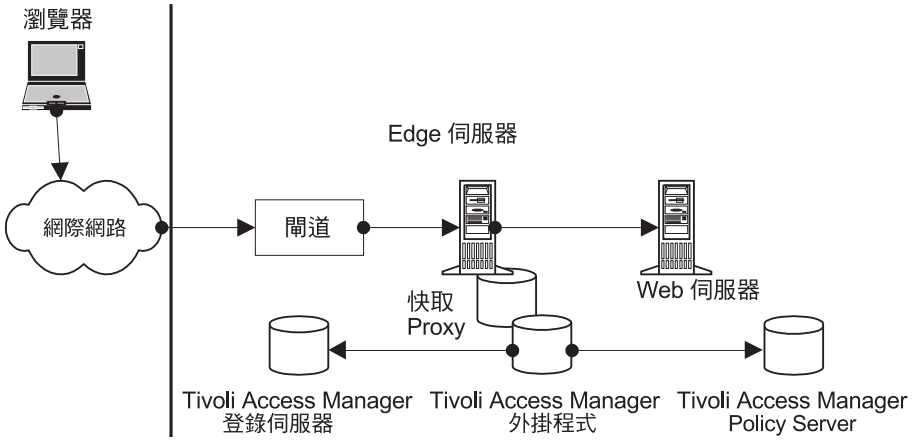

圖 1. Edge Server 外掛程式安全執行的範例

Edge Server 外掛程式對下列快取 Proxy 配置提供存取控制：

- 反向 Proxy
- 順向 Proxy

這些概念將會在下列各節中討論。

反向 Proxy 存取控制

當 Edge Server 快取 Proxy 介於網際網路的用戶端瀏覽器以及防火牆後面的 Web 伺服器之間時，可發揮反向 Proxy 的功能。在擔任這個角色時，快取 Proxy 會截取來自網際網路的使用者要求，將它們轉送到適當的主機 Web 伺服器，快取傳回的資料，然後將該筆資料遞送到網際網路上的用戶端使用者。

Edge Server 外掛程式可用來對這些入埠的用戶端要求提供存取控制。您可以在 Edge Server 快取 Proxy 機器上配置網站的公用網域名稱，然後指定通往對應後端 Web 伺服器的路徑（如圖 2中所述）。

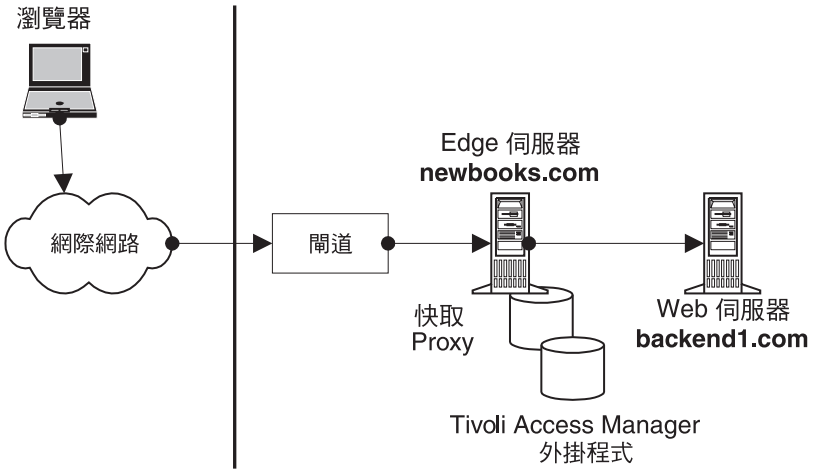

圖 2. 採用反向 Proxy 配置的 Edge Server 外掛程式

在這個範例中，Edge Server 外掛程式是配置成對 newbooks.com 上的物件提供存取控制。在使用者獲得授權後，會由 Edge Server 外掛程式或負載平衡模組（如 Edge Server 網路分派器的內容型遞送模組）將要求遞送到對應的後端伺服器。Edge Server 外掛程式執行 URL 對映，亦即類似在 Edge Server 快取 Proxy 配置檔中 **Proxy** 陳述式所提供的功能。

您可以設定外掛程式配置檔 `osdef.conf` 中的參數值來配置 Edge Server 外掛程式存取控制。在這個網站範例中，您會新增下列項目：

```
[Remote: /ESProxy/reverse/newbooks.com]
domains = newbooks.com www.newbooks.com
login_method = forms
form_login_file = http://newbooks.com/pub/login.html
form_login_errorfile = http://newbooks.com/pub/loginerr.html
form_logout_url = /pub/logout.html
route = http://backend1.com
```

這個項目會配置 Edge Server 外掛程式，以執行下列動作：

- 對 newbooks.com 和 www.newbooks.com 所有的要求授權，方法是查閱 Tivoli Access Manager 保護的物件名稱空間中，位於 `/ESProxy/reverse/newbooks.com` 項目下的物件所連接的 ACL。
- 使用套表型登入作爲登入方法
- 將每一個 URL 對映到下列 Web 伺服器：

  backend1.com

在此範例中，管理者應該將未經鑑定的 ACL 連接於 `/pub` 目錄上。如需如何使用未經鑑定的 ACL 的相關資訊，請參閱 *IBM Tivoli Access Manager Base Administrator's Guide*。

請注意，如果使用者送出的 URL 要求與 `/pub/logout.html` 相符，則使用者會登出。

根據預設，Edge Server 外掛程式會對反向 Proxy 要求來檢查 /ESProxy/reverse/*domain_name*。您可以爲此伺服器定義設定額外的選項。如果您沒有指定選項的設定，則該選項的設定就會繼承 osdef.conf 配置檔的 [Global] 區段的設定。

Edge Server 外掛程式支援數種登入方法。除了配置範例所顯示的套表型登入外，也可以配置 Edge Server 外掛程式來使用下列登入方法：

- 基本鑑定
- 用戶端憑證鑑定

如需有關 osdef.conf 檔案選項的相關資訊，請參閱第 51 頁的附錄 B, 『物件空間定義配置檔參照』。

順向 Proxy 存取控制

當 Edge Server 快取 Proxy 介於用戶端瀏覽器（位於防火牆後）以及網際網路之間時，可當作順向 Proxy 使用。用戶端瀏覽器會配置成把要求導向 Edge Server 快取 Proxy。順向快取 Proxy 會將用戶端的要求轉送到網際網路上的內容主機，快取所擷取的資料，然後將擷取的資料遞送給用戶端。

Edge Server 外掛程式可用來爲這些出埠的用戶端要求提供存取控制，如圖 3 所述。

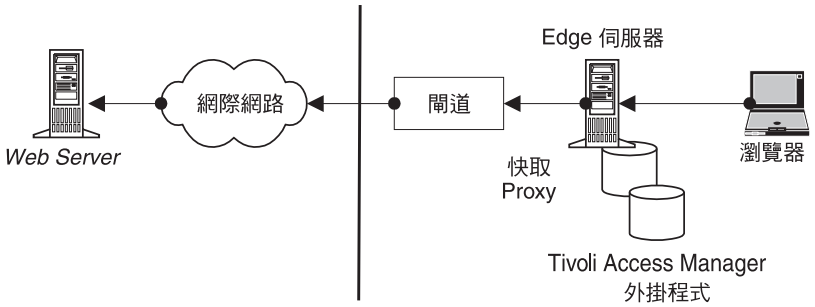

圖 3. 採用順向 Proxy 配置的 Edge Server 外掛程式

根據預設值，Edge Server 外掛程式會爲前向 Proxy 要求檢查 /ESProxy/forward/*domain_name*。您可以置換這個預設設定，方法是在物件空間定義配置檔中建立一或多個伺服器定義（如下所示）：

```
[Remote: /ESProxy/forward/blockedsites]
domains = games.com *.games.com *.competitor.com
route = http://backend2.com /pub/browsepolicy.html
```

在這個範例中，所有與 games.com、*.games.com、或 *.competitor.com 等網域名稱相符的瀏覽器要求，都會被重新導向至公司的瀏覽原則網頁，該網頁位於下列網址：

backend2.com

另外，您可以在物件空間的這個位置中連接一個 Tivoli Access Manager ACL。例如，這個 ACL 可以拒絕存取任何列出網站的所有使用者。

第 2 章 安裝 Edge Server 外掛程式

本章說明如何在 IBM AIX、Red Hat Linux、Sun Solaris Operating Environment（之後稱爲 Solaris）及 Microsoft Windows 等平台上安裝和配置 Edge Server 外掛程式。注意，若您的系統目前是以 GSKit、IBM SecureWay Directory 用戶端和 IBM Tivoli Access Manager runtime environment 等的支援版本所設定的，您僅需安裝外掛程式套件。

本章包含下列各節：

在 AIX 上安裝 Edge Server 外掛程式

下列步驟說明如何安裝 Edge Server 外掛程式之所需元件。

註: 在安裝外掛程式套件前，請確定您安裝了 *IBM Tivoli Access Manager for e-business Release Notes* 中所列的必備軟體。

1. 以 **root** 身份登入系統。
2. 插入 *IBM Tivoli Access Manager Web Security, Version 4.1, for AIX* CD。
3. 若要將 Edge Server 外掛程式套件安裝於預設位置，請輸入下列指令：

   ```
   installp -c -a -g -X -d /dev/cd0 PDPlgES
   ```

4. 若要完成 Edge Server 外掛程式的安裝，請遵循第 6 頁的『配置 Edge Server 外掛程式』中的指示。

在 Linux 上安裝 Edge Server 外掛程式

下列步驟說明如何安裝 Edge Server 外掛程式之所需元件。

註: 在安裝外掛程式套件前，請確定您安裝了 *IBM Tivoli Access Manager for e-business Release Notes* 中所列的必備軟體。

1. 以 **root** 身份登入系統。
2. 插入 *IBM Tivoli Access Manager Web Security, Version 4.1, for Linux* CD。
3. 變換至 `/mnt/cdrom/linux` 目錄，其中 `/mnt/cdrom` 是您 CD 的裝載點。
4. 若要將 Edge Server 外掛程式套件安裝於預設位置，請輸入下列指令：

   ```
   rpm -i PDPlgES-PD-4.1.0-0.i386.rpm
   ```

5. 若要完成 Edge Server 外掛程式的安裝，請遵循第 6 頁的『配置 Edge Server 外掛程式』中的指示。

在 Solaris 上安裝 Edge Server 外掛程式

下列步驟說明如何安裝 Edge Server 外掛程式之所需元件。

註: 在安裝外掛程式套件前，請確定您安裝了 *IBM Tivoli Access Manager for e-business Release Notes* 中所列的必備軟體。

1. 以 **root** 身份登入系統。
2. 插入 *IBM Tivoli Access Manager Web Security, Version 4.1, for Solaris* CD。
3. 變換至 `/cdrom/cdrom0/solaris` 目錄。
4. 若要將 Edge Server 外掛程式套件安裝於預設位置，請輸入下列指令：

   ```
   pkgadd -d /cdrom/cdrom0/solaris -a /cdrom/cdrom0/solaris/pddefault PDPlgES
   ```

5. 若要完成 Edge Server 外掛程式的安裝，請遵循第 6 頁的『配置 Edge Server 外掛程式』中的指示。

在 Windows 上安裝 Edge Server 外掛程式

下列步驟說明如何安裝 Edge Server 外掛程式之所需元件。

註: 在安裝外掛程式套件前，請確定您安裝了 *IBM Tivoli Access Manager for e-business Release Notes* 中所列的必備軟體。

1. 以具備管理者專用權的使用者身份登入系統。
2. 插入 *IBM Tivoli Access Manager Web Security, Version 4.1, for Windows* CD。
3. 在下列位置執行 `setup.exe` 檔案：

   ```
   cdrom_drive\windows\PolicyDirector\Disk Images\Disk1
   ```

4. 從「選取套件」視窗，選取 Edge Server 套件的外掛程式。
5. 若要完成 Edge Server 外掛程式的安裝，請遵循第 6 頁的『配置 Edge Server 外掛程式』中的指示。

配置 Edge Server 外掛程式

Edge Server 外掛程式提供一個配置公用程式，名爲 `wslconfig.sh`（於 UNIX 系統）或 `wslconfig.exe`（於 Windows 系統）。這個公用程式會完成下列作業：

- 爲 Edge Server 外掛程式建立 Tivoli Access Manager 身份。
- 爲 Edge Server 外掛程式建立 Tivoli Access Manager 保護的物件空間。
- 僅在 Windows 平台，配置 Edge Server 快取 Proxy 於應用程式啓動時，自動載入 Edge Server 外掛程式。

若要配置 Edge Server 外掛程式，請遵循下列步驟：

1. 若要啓動配置公用程式，請輸入下列指令：
   - 在 UNIX 系統上：

     ```
     wslconfig.sh
     ```

   - 在 Windows 系統上：

     ```
     wslconfig.exe
     ```

註: 僅有在 Windows 2000 系統上，Active Directory 使用者登錄的外掛程式的配置需要管理者密碼，配置工具才能成功執行。配置時，使用 **wslconfig** 指令以及下列參數：

```
wslconfig -adpwd Active_Directory_admin_password
```

2. 請於提示時，輸入下列資訊：
   - Edge Server 快取 Proxy 的埠號。預設的埠號是 80。
   - Tivoli Access Manager 管理使用者 ID 及密碼。例如，輸入 **sec_master** 和其關聯密碼。

配置公用程式會完成下列作業：

- 爲伺服器建立登錄物件。
- 新增伺服器到安全群組：**ivacld-servers** 和 **SecurityGroup**。
- 建立 SSL 憑證。
- 從 Tivoli Access Manager Policy Server 取得 SSL 簽署的憑證。
- 配置 Edge Server 快取 Proxy 來使用 Edge Server 外掛程式（經由設定 Edge Server 快取 Proxy 設定檔 `ibmProxy.conf` 中的指引）。
- 重新啓動 Edge Server 快取 Proxy 處理程序 **ibmProxy**。

下一步，配置公用程式啓動 Edge Server 物件空間管理程式的外掛程式，方法是使用 **wesosm** 指令。這個公用程式會更新 Tivoli Access Manager 物件空間，爲 Edge Server 外掛程式建立一個新的物件空間配置區。

Edge Server 外掛程式配置現在已經完成。 Edge Server 快取 Proxy 正在執行中，且已載入 Edge Server 外掛程式。管理使用者 sec_master，可用來存取快取 Proxy 的首頁。

升級 Edge Server 外掛程式

早期版本的外掛程式之配置工具在解除配置程序期間，會自動取代使用者配置檔，（這有時會造成使用者配置資訊流失）。在解除配置期間，Edge Server 外掛程式第 4.1 版不會取代使用者配置檔。從 Edge Server 外掛程式的現有版本升級時，您得在解除配置外掛程式前備份所有使用者修改過的配置檔，如 `ibmwesas.conf`、`osdef.conf`、`ibmProxy.conf`。

第 3 章 管理 Edge Server 外掛程式

本章針對使用 Edge Server 外掛程式來管理您安全網域的資源，提供概念、管理程序和技術參考手冊資訊。本章包含下列各節：

管理使用者帳戶

IBM Tivoli Access Manager 是經由 **pdadmin** 指令行介面來維護並管理使用者帳戶 。使用此介面可以建立、刪除和修改使用者和群組。外掛程式藉由驗證所送出的使用者資訊是否與 Tivoli Access Manager 登錄中的使用者項目符合來驗證使用者身份。外掛程式也會驗證使用者帳戶狀態是否有效。

所有使用者密碼原則都是經由 Tivoli Access Manager 設定，然後在鑑定期間傳遞到外掛程式。外掛程式不會維護任何密碼原則資訊，而是靠 Tivoli Access Manager 來維護如最大登入失敗次數、帳戶到期日期和最長密碼時間等的資訊。鑑定期間，外掛程式驗證使用者帳戶是否有效並確定使用者密碼未到期。若使用者帳戶已停用，則使用者授權失敗。然而，若密碼已到期且爲外掛程式配置了變更密碼套表，則會呈現該套表給使用者，來變更到期的密碼。

建立 Tivoli Access Manager 物件空間

Tivoli Access Manager 使用受保護的物件名稱空間來代表需要套用存取控制原則的物件。受保護的物件空間可包含 Web 伺服器上的資源。將 Web 資源加入到物件空間最簡單的方法是匯入 Web 伺服器檔案系統，並在必要時套用 Tivoli Access Manager 存取控制清單 (ACL)。

Edge Server 外掛程式提供了一個物件空間管理程式公用程式，來將資源新增到 Tivoli Access Manager 物件空間中。用 **wesosm** 指令可以呼叫這個公用程式。您可以使用 **wesosm** 來爲 Edge Server 快取 Proxy 以及 Edge Server 外掛程式所保護的 Web 伺服器產生物件空間。

註: 如需關於 **wesosm** 指令的相關資訊，請參閱第 61 頁的附錄 C, 『wesosm 指令參照』。

下列各節說明如何將 Web 資源新增至受保護的物件空間：

為快取 Proxy 建立物件空間

雖然 Edge Server 快取 Proxy 是一 Proxy，當要求是直接針對 Edge Server 快取 Proxy 機器的主要網域名稱時，它也可以作爲 Web 伺服器。通常，參考和錯誤訊息都是儲存在 Proxy 的 Web 空間裡。 Edge Server 外掛程式可對 Edge Server 快取 Proxy 所管理的物件執行存取控制。

每一個需要保護的物件都必須在 Tivoli Access Manager 物件空間中定義。有兩種方法可以新增物件到物件空間。

您可以使用 **pdadmin** 指令，以手動方式將物件新增至物件空間。 **pdadmin** 指令包含可用來建立新的物件空間以及新增、修改和刪除物件的指令行選項。如需相關資訊，請參閱 *IBM Tivoli Access Manager Command Reference*。

您也可以使用 **query_contents** 公用程式來取得 Web 階層中的物件庫存，將一系列的 Web 資源新增至物件空間中。此方法在第 10 頁的『爲其他 Web 伺服器建立物件空間』中有討論。

配置檔 `osdef.conf` 中的下列範例伺服器定義代表名爲 bookProxy.com 的 Edge Server 快取 Proxy：

```
[Local: /ESproxy/bookproxy.com]
domains = bookproxy.com
query_command = http://bookproxy.com/cgi-bin/query_contents?dirlist=/
```

當您在安裝期間配置 Edge Server 外掛程式時，**wsIconfig** 公用程式會執行 **wesosm** 指令，來爲 Edge Server 快取 Proxy 產生預設的物件空間。預設的物件空間包含下列配置區物件：

```
/ESproxy
/Esproxy/proxy_host_name
/ESproxy/forward
/ESproxy/reverse
```

建立物件之後，您可以將 ACL 置於 Edge Server 快取 Proxy 的物件空間中的適當位置。

為其他 Web 伺服器建立物件空間

使用物件空間管理程式 **wesosm** 指令來查詢遠端 Web 伺服器的檔案系統，以便在 Tivoli Access Manager 物件空間中建立對應的項目。物件空間管理程式會讀取 `osdef.conf` 配置檔，並且爲檔案中的每個伺服器定義建立物件項目。

使用 **query_contents** 公用程式來匯入 Web 伺服器的檔案系統到受保護的物件空間。**query_contents** 公用程式位在 Windows 系統上的 *install_dir*`\bin`，或位在 UNIX 系統上的 `/opt/pdweb-lite/bin`。在目標 Web 伺服器上的 `cgi-bin` 目錄中複製這個公用程式。此外，在 Windows 系統上的 `C:\WINNT\query_contents.cfg` 中設定 **DOCROOT** 參數，或在 UNIX 系統上的 `query_contents.sh` 中設定 **DOCROOTDIR** 參數，來指定 Web 伺服器檔案的根目錄位置。如需 **query_contents** 公用程式的相關資訊，請參閱 *IBM Tivoli Access Manager WebSEAL Administrator's Guide*。

配置好 **query_contents** 公用程式之後，請在物件空間定義配置檔中新增一個項目，告知 **wesosm** 指令如何查詢遠端 Web 伺服器的檔案系統。例如，新增下列項目於配置檔：

```
[Remote: /ESproxy/reverse/newbooks.com]
domains = newbooks.com www.newbooks.com
...
query_command = http://backend1.com/cgi-bin/query_contents?dirlist=/
```

將項目新增至配置檔之後，請依下列方式，從 Edge Server 外掛程式機器執行物件空間管理程式：

```
wesosm -run -infile location_of_osdef.conf -verbose
```

wesosm 指令會連接到 Web 伺服器來查詢其檔案系統。接著，它會連接到 Tivoli Access Manager Policy Server，以於 /ESProxy/reverse/newbooks.com 下的物件空間中建立項目。若伺服器定義沒有關聯的 **query_contents** 公用程式，則僅建立根分支。在建立物件空間之後，您可以將 ACL 連接到適當的位置。

您也可以使用 **wesosm** 指令來維護物件空間，方法是刪去任何長期累積的廢棄項目。如果要將已作廢的項目從物件空間移除，請執行含下列選項的 **wesosm** 指令：

```
wesosm -run -infile location_of_osdef.conf -clean -verbose
```

啓動和停止 Edge Server 外掛程式

若要以手動方式來啓動 Edge Server 快取 Proxy 並載入 Edge Server 外掛程式，請進行下列其中一項動作：

- 在 UNIX 系統，使用 **wslstartwte** 指令。

  註: 您可以在每次系統啓動時，新增 **wslstartwte** 公用程式到 UNIX 啓動 Script 以自動啓動 Edge Server 快取 Proxy 和 Edge Server 外掛程式。

- 在 Windows 系統上，啓動 IBM Caching Proxy 服務。

若要停止 Edge Server 快取 Proxy UNIX 系統，請執行下列其中一項動作：

- 在 UNIX 系統，使用 **wslstopwte** 指令：
- 在 Windows 系統，停止 IBM Caching Proxy 服務。

配置檔

在安裝和配置 Edge Server 外掛程式時，就會建立 Edge Server 外掛程式配置檔，並且將它們置於檔案系統中。在起始配置之後，您可以用手動方式來修改這些檔案。

配置檔是位於下列其中一個目錄：

- 在 UNIX 系統上：

  /opt/pdweb-lite/etc

- 在 Windows 系統上：

  install_dir\etc

下列各節分別說明配置檔：

- 第 12 頁的『基本配置檔 (ibmwesas.conf)』
- 第 12 頁的『物件空間定義配置檔 (osdef.conf)』
- 第 14 頁的『使用者對映配置檔 (usermap.conf)』

基本配置檔 (ibmwesas.conf)

基本配置檔名爲 ibmwesas.conf。 **wslconfig** 公用程式會在安裝及配置 Edge Server 外掛程式時，起始設定此檔案。這個檔案包含用來起始設定和啓動 Edge Server 外掛程式的項目。通常在起始配置之後，您並不需要修改這個檔案。

此 ibmwesas.conf 檔案包含指定下列值的項目：

- Tivoli Access Manager 輕裝備目錄存取通訊協定 (LDAP) 配置設定

  這些包括 LDAP 主機和埠號。當 Tivoli Access Manager 與 LDAP 伺服器的通訊是透過「安全 Socket 層 (SSL)」時， SSL 配置值就會包含在這裡。
- Tivoli Access Manager 配置值：
  - 資料庫複寫模式（本端或遠端）
  - 資料庫位置
  - 審核檔位置
  - 快取重新整理間隔
  - 含有憑證資訊的 SSL 配置檔位置
- Lightweight Third Party Authentication (LTPA) cookie 單一登入設定
- WebSEAL cookie 單一登入設定
- osdef.conf 物件空間定義檔案的位置
- usermap.conf 使用者對映檔案的位置

如需 ibmwesas.conf 檔的詳細資訊，請參閱第 49 頁的附錄 A, 『基礎配置檔參照』。

物件空間定義配置檔 (osdef.conf)

物件空間定義設定檔案的名稱是 osdef.conf。osdef.conf 檔案會指定 Edge Server 外掛程式用來對所有用戶端要求執行存取控制的配置設定。物件空間定義配置檔的設定分成下列區段：

- [Global]

  指定適用於所有要求，而且這些要求在另一個區段（[Local] 或 [Remote]）並沒有被明確覆寫的設定。
- [Local]

  指定適用於 Edge Server 快取 Proxy 上物件之要求的設定值。
- [Remote]

  指定適用於遠端 Web 伺服器物件的要求的設定。
- [SSO]

  指定 Edge Server 外掛程式可用來將鑑定資訊傳送到 Web 伺服器的單一登入定義和設定。

此 [Global] 部分（屬於 osdef.conf 檔案）包含下列配置選項：

- 管理者名稱和密碼
- 啓用或停用更新物件空間
- 物件空間 root、前向 Proxy 項目以及反向 Proxy 項目的物件空間位置
- 檔案系統類型
- 使用反向「網域名稱系統（DNS）」查詢的 URL 解析

- 登入方法
  - 無

    我們建議您使用 Tivoli Access Manager 的「未經鑑定 ACL」，而不要使用「無」作爲登入類型。
  - 基本鑑定
  - 套表式登入
  - 憑證
- 套表式登入設定

  包含安全套表登入要使用的套表檔位置、錯誤檔位置、密碼處理以及安全類型。
- 用來儲存已鑑定使用者資訊的快取大小和快取逾時值
- 記載訊息設定

此 [Local] 部分（屬於 the osdef.conf 檔案）包括下列配置選項：
- 網域名稱
- 登入方法
- 查詢指令設定

  這些值是用來收集本端「Edge Server」快取 Proxy 物件的空間資訊。

此 [Remote] 部分（屬於 osdef.conf 檔案）包含 Edge Server 外掛程式保護的每一個遠端伺服器定義。每一個伺服器的此設定都包含下列項目：
- 網域名稱
- 登入方法及支援檔案
- 查詢指令
- SSL 存取需求
- 單一登入選項
- 遞送選項

此 [SSO] 區段（屬於 osdef.conf 檔案）包含單一登入定義和單一登入配置的設定。如果使用者已經通過鑑定，Edge Server 外掛程式可以略過鑑定步驟。Edge Server 外掛程式也可傳送單一登入資訊到 Web 伺服器以作爲 HTTP 標頭或 cookie。

以下是預先定義好的單一登入類型：
- IBM WebSphere LTPA cookie
- Tivoli Access Manager WebSEAL 失效接替 cookie
- CDAS 模組單一登入

Edge Server 外掛程式提供了數個預先定義的巨集，讓您用來格式化單一登入資訊。有關這些巨集的資訊，以及格式化的單一登入資訊範例，請參閱 osdef.conf 檔案中的範例。

Edge Server 外掛程式支援許多不同的配置情況。同樣地，許多配置選項都可以作調整。osdef.conf 配置檔詳細記載了每一個選項，並且爲每一個選項提供一個預設和範例值。

當您對 Edge Server 外掛程式有了基本的瞭解之後，就可以輕易自訂和配置 Edge Server 外掛程式，以便在您的環境中使用。使用預設值的時候，Edge Server 外掛程式可以正常運作。因此，您不必設定每一個選項，就能發揮它的效能。僅設定相關選項。

如需 osdef.conf 檔案上的其他資訊，請參閱第 51 頁的附錄 B, 『物件空間定義配置檔參照』。

使用者對映配置檔 (usermap.conf)

usermap.conf 檔是用來將單一登入使用者和憑證使用者對映到 Tivoli Access Manager 使用者。如需使用者對映檔案的相關資訊，請參閱 usermap.conf 檔中所提供的備註。usermap.conf 檔是位於下列其中一個目錄：

- 在 UNIX 系統：

  /opt/pdweb-lite/etc

- 在 Windows 系統：

  install_dir\etc

日誌檔

Edge Server 外掛程式會將事件記錄到 Edge Server 快取 Proxy 的事件日誌檔中。您可以檢查這個日誌檔，來檢視 Edge Server 外掛程式所採取過的動作。

在 UNIX 系統中，日誌檔是：

/opt/ibm/edge/cp/server_root/logs/event.*date*

在 Windows 系統中，日誌檔是：

C:\Program Files\IBM\edge\cp\Logs\event.*date*

第 15 頁的圖 4 顯示一個來自事件日誌檔的摘錄。

```
[03/15/02 10:04:53 1] ------------------------------------------
[03/15/02 10:04:53 1] 輸入起始設定外掛程式：WTESeal_Init()
[03/15/02 10:04:53 1] 配置設定的起始設定成功
[03/15/02 10:04:55 1] WebSEAL cookie 模組的起始設定成功
[03/15/02 10:04:55 1] 起始設定屬性清單
[03/15/02 10:04:55 1]     [00]: azn_init_audit_file
[03/15/02 10:04:55 1]     [01]: azn_init_cache_refresh_interval
[03/15/02 10:04:55 1]     [02]: azn_init_cfg_file
[03/15/02 10:04:55 1]     [03]: azn_init_db_file
[03/15/02 10:04:55 1]     [04]: azn_init_ldap_bind_dn
[03/15/02 10:04:55 1]     [05]: azn_init_ldap_bind_pwd
[03/15/02 10:04:55 1]     [06]: azn_init_ldap_host
[03/15/02 10:04:55 1]     [07]: azn_init_ldap_port
[03/15/02 10:04:55 1]     [08]: azn_init_listen_flags
[03/15/02 10:04:55 1]     [09]: azn_init_mode
[03/15/02 10:04:55 1] AZN API 用戶端程式庫第 4.1.0 版 (Build 30395)
[03/15/02 10:04:55 1] Access Manager 起始設定成功
[03/15/02 10:04:55 1] 結束起始設定外掛程式：WTESeal_Init()
[03/15/02 10:04:55 1] 等候連線...
[03/15/02 10:06:02 2560]
[03/15/02 10:06:02 2560] --- 接受非安全連線 ---
[03/15/02 10:06:02 2560] 輸入 PreExit 外掛程式：WTESeal_PreExit()
[03/15/02 10:06:02 2560] 來自 110.120.130.140 的使用者送出要求：GET /
[03/15/02 10:06:02 2560] 此要求的登入方法是基本的方法
[03/15/02 10:06:02 2560] 檢查反向 Proxy 模式的授權標頭
[03/15/02 10:06:02 2560] 成功地從授權標頭擷取使用者 'joe'
[03/15/02 10:06:02 2560] 結束 PreExit 外掛程式：WTESeal_PreExit()
[03/15/02 10:06:02 2560]
[03/15/02 10:06:02 2560] 輸入授權外掛程式：WTESeal_Authorize()
[03/15/02 10:06:02 2560]
HTTP 標頭：
主機：newbooks.com
授權：基本 Yah7dglDai84qBXf=

[03/15/02 10:06:02 2560] 經由  Access Manager 鑑定使用者 'joe' 的身份
[03/15/02 10:06:02 2560] 使用者 'joe' 的身份鑑定成功
[03/15/02 10:06:02 2560] 為使用者 'joe' 建立 LDAP 身份
[03/15/02 10:06:02 2560] 載入證明以授權給使用者 'joe'
[03/15/02 10:06:03 2560] 檢查存取 (r) 於 ACL 字串 /ESProxy/reverse/newbooks.com
[03/15/02 10:06:03 2560] 已授與存取物件的許可權
[03/15/02 10:06:03 2560] 已成功授權使用者 'joe' (回覆碼 = 200)
[03/15/02 10:06:03 2560] 使用反向 Proxy 遞送來遞送要求至 http://backend1.com/
[03/15/02 10:06:03 2560] 結束授權外掛程式：WTESeal_Authorize()
```

圖 4. 事件日誌檔摘錄

配置登入方法

登入方法指定使用者將以何種方式呈現證明給外掛程式，以進行鑑定。外掛程式支援下列透過物件空間配置檔 `osdef.conf` 配置的登入方法。

下列幾節將說明登入方法：

- 第 16 頁的『基本鑑定』
- 第 16 頁的『套表登入』
- 第 18 頁的『用戶端憑證』

基本鑑定

當外掛程式查問瀏覽器以取得使用者 ID 及密碼時，使用者會使用基本鑑定來登入。此時瀏覽器會提示使用者提供使用者 ID 及密碼，接著再將這兩者送至外掛程式以進行鑑定。在鑑定成功後，系統可能會呈現一個套表給使用者，來變更到期的密碼。

下列範例說明 newbooks.com 的配置，在這裡使用者使用基本鑑定來進行鑑定，而且當密碼到期時，會呈現一個套表給使用者，以變更該密碼。

```
[Remote: /ESproxy/reverse/newbooks.com]
domains = newbooks.com www.newbooks.com
route = http://backend1.com

# 指定登入方法
login_method = basic

# 變更密碼套表
form_chgpasswd_file = /opt/pdweb-lite/samples/forms/formchgpwd2.html

# 使用變更密碼 URL 來變更密碼
form_chgpasswd_submit_url = /pub/chgpasswd
form_chgpasswd_response_url = /pub/passwdchanged.html
form_chgpasswd_url_recovery = no
```

範例說明下列順序：

1. 使用者使用基本鑑定進行鑑定。
2. 在鑑定成功後，會呈現一個套表給使用者，來變更到期的密碼。
3. 使用者送出變更密碼套表給下列 URL：

   http://newbooks.com/pub/chgpasswd
4. 在外掛程式順利地變更了密碼之後，瀏覽器將重新導向到下列 URL：

   http://newbooks.com/pub/passwdchanged.html

套表登入

當外掛程式傳送一個登入套表給使用者，以取得使用者 ID 及密碼時，使用者會使用套表登入來進行登入。使用者會填寫套表，然後將它送至外掛程式以進行鑑定。當使用者送出登入套表時，外掛程式會使用下列三種方法之一，來偵測是否送出了登入套表。

- 預先登入 cookie
- 套表簽名
- 登入 URL

當既未配置套表簽名，也未配置登入 URL 時，外掛程式會使用預先登入 cookie 來偵測是否送出了登入套表。當傳送登入套表到瀏覽器時，它會建立這個 cookie。當使用者送出鑑定套表以及這個 cookie 時，外掛程式就會驗證使用者身份。

在登入套表中，套表簽名是隱藏的*名稱=值*指定。當使用者送出一個符合已配置之套表簽名的登入套表時，外掛程式就會從套表擷取使用者的資訊，來驗證使用者身份。請注意，僅在配置了外掛程式來遞送要求到後端伺服器，才應該使用套表簽名。

登入 URL 是另一種可供外掛程式偵測是否已送出登入套表的方法。如果已送出的 URL 符合已配置的登入 URL 時，外掛程式就會從套表擷取使用者的資訊，來驗證使用者身份。

如果配置了套表簽名或登入 URL，將不會使用預先登入 cookie。系統會預期登入套表含有套表簽名，或已送至登入 URL。使用這兩種配置之一，使用者都可以送出一個登入套表給外掛程式以進行鑑定，即使使用者目前正在存取的資源不需要已鑑定的存取，也是如此。這可能適用於不需要每一個使用者都要進行鑑定的網站。

同樣地，當使用者送出變更密碼套表給外掛程式時，使用者的密碼可加以變更（即使它未到期）。當外掛程式偵測到已送出變更密碼套表時，它會使用變更密碼套表簽名或變更密碼 URL，來變更使用者的密碼。

當安裝外掛程式時，這些範例中所參照的範例套表將複製到檔案系統。這些套表可加以修改，以含有背景圖片及影像來裝飾套表。確定登入套表中的所有影像參照都不需要鑑定即可存取，並且在參照套表中的影像或背景圖片時，提供絕對 URL。

下列範例說明 newbooks.com 的配置，在這裡使用者使用套表簽名來進行鑑定。

```
[Remote: /ESproxy/reverse/newbooks.com]
domains = newbooks.com www.newbooks.com
route = http://backend1.com

# 指定登入方法
login_method = forms

# 登入及登出套表
form_login_file = /opt/pdweb-lite/samples/forms/formlogin1.html
form_login_errorfile = /opt/pdweb-lite/samples/forms/formerror1.html
form_logout_file = /opt/pdweb-lite/samples/forms/formlogout.html

# 使用登入簽名的套表登入
#form_login_url = /account/greeting
form_signature_login = FormType=LoginForm
form_logout_url = /pub/logout

# 變更密碼套表
form_chgpasswd_file = /opt/pdweb-lite/samples/forms/formchgpwd1.html

# 使用變更密碼簽名來變更密碼
#form_chgpasswd_submit_url = /pub/chgpasswd
form_signature_chgpasswd = FormType=ChangePasswordForm
form_chgpasswd_response_url = /pub/passwdchanged.html
form_chgpasswd_url_recovery = no
```

範例說明下列順序：

1. 使用者送出登入套表給外掛程式。
2. 外掛程式會使用登入套表簽名來偵測是否送出了登入套表。
3. 在鑑定成功後，會呈現一個套表給使用者，來變更到期的密碼。
4. 使用者送出變更密碼套表給外掛程式。
5. 外掛程式會使用變更密碼套表簽名來偵測是否送出了變更密碼套表。
6. 在外掛程式順利地變更了密碼之後，瀏覽器將重新導向到下列 URL：

   http://newbooks.com/pub/passwdchanged.html

下列範例說明 newbooks.com 的配置，在這裡使用者使用登入 URL 來進行鑑定。

```
[Remote: /ESproxy/reverse/newbooks.com]
domains = newbooks.com www.newbooks.com
route = http://backend1.com

# 指定登入方法
login_method = forms
```

```
# 登入及登出套表
form_login_file = /opt/pdweb-lite/samples/forms/formlogin2.html
form_login_errorfile = /opt/pdweb-lite/samples/forms/formerror2.html
form_logout_file = /opt/pdweb-lite/samples/forms/formlogout.html

# 使用登入 URL 的套表登入
#form_signature_login = FormType=LoginForm
form_login_url = /account/greeting
form_logout/url = /pub/logout

# 變更密碼套表
form_chgpasswd_file = /opt/pdweb-lite/samples/forms/formchgpwd2.html

# 使用變更密碼 URL 來變更密碼
#form_signature_chgpasswd = FormType=ChangePasswordForm
form_chgpasswd_submit_url = /pub/chgpasswd
form_chgpasswd_response_url = /pub/passwdchanged.html
form_chgpasswd_url_recovery = no
```

範例說明下列順序：

1. 使用者送出登入套表給下列 URL：

   http://newbooks.com/account/greeting
2. 外掛程式會使用登入 URL 來偵測是否送出了登入套表。
3. 在鑑定成功後，會呈現一個套表給使用者，來變更到期的密碼。
4. 使用者送出變更密碼套表給下列 URL：

   http://newbooks.com/pub/chgpasswd
5. 外掛程式會使用變更密碼 URL 來偵測是否送出了變更密碼套表。
6. 在外掛程式順利地變更了密碼之後，瀏覽器將重新導向到下列 URL：

   http://newbooks.com/pub/passwdchanged.html

用戶端憑證

當快取 proxy 查問瀏覽器以取得用戶端憑證時，使用者就會使用用戶端憑證來進行登入。此時瀏覽器會提示使用者選取已安裝的憑證，接著再將這個憑證送至外掛程式以進行鑑定。

用戶端憑證鑑定的配置包括配置快取 proxy 以接受 SSL 連線，並查問瀏覽器以取得用戶端憑證。外掛程式的登入方法也應該適當地加以設定，而且應該在 `usermap.conf` 配置檔中建立一個對映規則，以將憑證中的識別名稱對映至 Tivoli Access Manager 使用者。如需使用者對映檔的相關資訊，請參閱第 14 頁的『使用者對映配置檔 (usermap.conf)』。

配置標籤值配對支援

外掛程式會支援這樣的功能，在這裡使用者資訊擷取自 LDAP，並在鑑定後放入使用者的證明。使用者資訊擷取自使用者的 LDAP 識別名稱所代表的物件，而且可選擇性地新增至後端伺服器的 HTTP 標頭。

下列範例說明如何使用這些配置參數：

```
[Remote: /ESproxy/reverse/newbooks.com]
domains = newbooks.com
route = http://backend1.com

# 將擷取以放入使用者證明的 LDAP 屬性
tagvalue_creds_registry = lastname:sn email:mail
```

```
tagvalue_creds_registry = account:internationalISDNNumber

# 後端伺服器的標籤值 HTTP 標頭
tagvalue_creds_headers = lastname:X-LastName email:X-Email
tagvalue_creds_headers = account:X-Account

# 若要使用證明屬性名稱作為 HTTP 標頭名稱，
# 將所有標籤值證明放入 HTTP 標頭，請改用這個設定
# tagvalue_creds_headers = *
```

考慮這個實務，其中代表使用者識別名稱的 *inetOrgPerson* 含有 LDAP 中的下列屬性：

```
cn=joe, c=us
uid: Joe
sn: Smith
mail: joe@internet.com
internationalISDNNumber: 123456789
                         987654321
```

下列屬性會新增至使用者的證明。*tagvalue_* prefix 用來區分這些屬性與其他屬性：

```
tagvalue_lastname: Smith
tagvalue_email: joe@internet.com
tagvalue_account: 123456789
                  987654321
```

後端伺服器會在 HTTP 標頭中收到下列額外資訊：

```
X-LastName: Smith
X-Email: joe@internet.com
X-Account: 123456789::987654321
```

總之，tagvalue_creds_registry 設定會從 LDAP 擷取使用者資訊，然後在使用者進行鑑定後，將它儲存在使用者的證明中。您可以使用 tagvalue_creds_headers 設定，將儲存在使用者證明中的資訊新增至預定供後端伺服器使用的 HTTP 標頭，以確定僅有適當的標頭傳送至每一個後端伺服器。

第 4 章 了解 Edge Server 外掛程式配置

本章提供 Edge Server 外掛程式配置的概觀，其中解釋了概念、模型和程序。本章包含下列各節：

伺服器配置模型

Edge Server 外掛程式提供鑑定和授權服務程式給安全網域中之 Web 伺服器，方法是執行在 Edge Server Proxy 的安全性而非在 Web 伺服器的安全性。藉由在 Proxy 實作安全執行，外掛程式會從中央提供安全性服務給所有安全網域中的 Web 伺服器。在使用者經授權後，外掛程式會將要求轉送給對應的 Web 伺服器（含使用者的資訊）。

因爲網站內容可能因效能和內容配送而橫跨多個 Web 伺服器，外掛程式需要提供安全性服務給安全網域中的多重 Web 伺服器。當某些 Web 伺服器可能掌控內容，而其他的伺服器可能掌控廣泛的 Web 應用程式時，兩者皆需要不同的安全基本需求。例如，某些伺服器可能不需要鑑定，但其他的可能需要。需要鑑定的每一個伺服器可能需要使用者資訊以某種專屬格式送出。有些安全性設定對所有伺服器是共通的，如套表階段作業逾時；某些設定對每一伺服器卻是專屬的，如登入方法和單一登入。

外掛程式保護 Web 伺服器多變的陣列，每一個都有其專屬配置需求（經由其物件空間定義配置檔 `osdef.conf`）。此配置檔爲每一個受保護的 Web 伺服器組織設定到伺服器定義中。在每一伺服器定義中，都設好了伺服器特定的設定。有三種類型的伺服器定義用於配置檔，如下表所示。

伺服器定義	說明
[Global]	列於此定義下的設定可套用到所有 Web 伺服器。只有一個此定義的實例。
[Local]	列於此定義下的設定只可套用到 Edge Server 快取 Proxy。只有一個此定義的實例。
[Remote]	列於此定義下的設定可套用到外掛程式所保全的外部或遠端 Web 伺服器。此定義可有多個實例。

除了記錄於 `osdef.conf` 檔案中的一些例外，任何設定都可以放置於任何定義下。例如，**form_session_timeout** 設定，可放於 [Global] 定義下或 [Remote] 定義下，如下所示：

```
[Global]
login_method = forms
form_login_file = /opt/pdweb-lite/samples/forms/welcome.html
form_session_timeout = 10

[Remote: /ESProxy/reverse/anyother.com]
domains = anyother.com
```

```
[Remote: /ESProxy/reverse/verysecure.com]
domains = verysecure.com
form_session_timeout = 1
```

在此範例，任何登入 verysecure.com 的使用者都不被允許持續閒置超過一分鐘，否則階段作業就會過期。然而，對任何登入 anyother.com 和所有其他網域的使用者而言，閒置逾時是 10 分鐘，此乃由於它是被設於 [Global] 定義中。除了一些例外（[SSO] 設定），此承接模型可被用於配置檔中的任何伺服器設定，如圖 5中說明的。

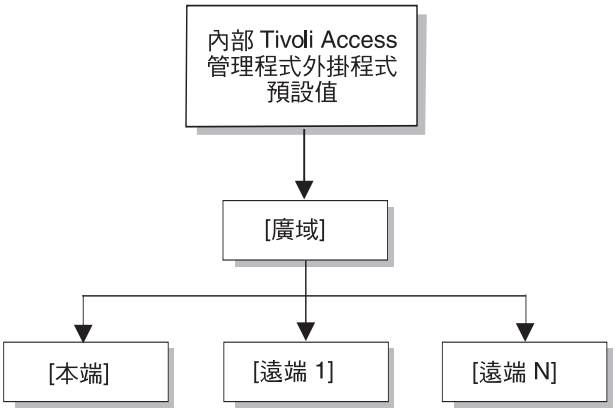

圖 5. 使用承接模型的 Edge Server 外掛程式

使用此承接模型，每一 Web 伺服器都相同的設定不需要在每一伺服器定義下重複，只要在配置檔下的 [Global] 定義下列出一次即可。例如，若所有伺服器使用相同的套表登入檔案，則設定可以被列於 [Global] 定義。

套用的伺服器配置概念

對配置檔有基本了解，就比較容易了解外掛程式如何使用配置檔來執行安全性。當要求被外掛程式接收到後，它會遵循基本步驟來授權使用者。

1. 若使用者已經過鑑定，例如（經由一個受信任的閘道）接受使用者單一登入資訊並繼續 4 步驟。
2. 根據下列其中一項登入方法取得使用者身份：
   - 對基本鑑定和套表登入，取得使用者 ID 和密碼。
   - 對憑證登入，取得憑證識別名稱。
3. 對照 Tivoli Access Manager 使用者登錄驗證使用者身份。
4. 對照 Tivoli Access Manager 物件空間授權使用者。
5. 送出使用者的單一登入資訊。
6. 轉送要求給對應的 Web 伺服器。

若要執行這些授權步驟，外掛程式必須查閱配置檔以取得關於要求的配置資訊。每一個步驟都需要從 `osdef.conf` 配置檔中擷取一個或多個設定。例如， 2步驟需要擷取 **login_method** 設定。

若要爲要求擷取一設定，外掛程式需要先決定先從哪一個定義開始擷取設定。這必須將要求與配置檔中的特定伺服器定義關聯。儘管外掛程式可以對反向和前向 Proxy 要求執行安全，外掛程式不會考慮該要求是一反向或前向的 Proxy 要求。

此網域名稱是掌控受保護的資源的對應 Web 伺服器之公用 ID。在反向 Proxy 方案中，這需要在外掛程式系統上建立別名或公用網域名稱，如圖 6 中所說明的。

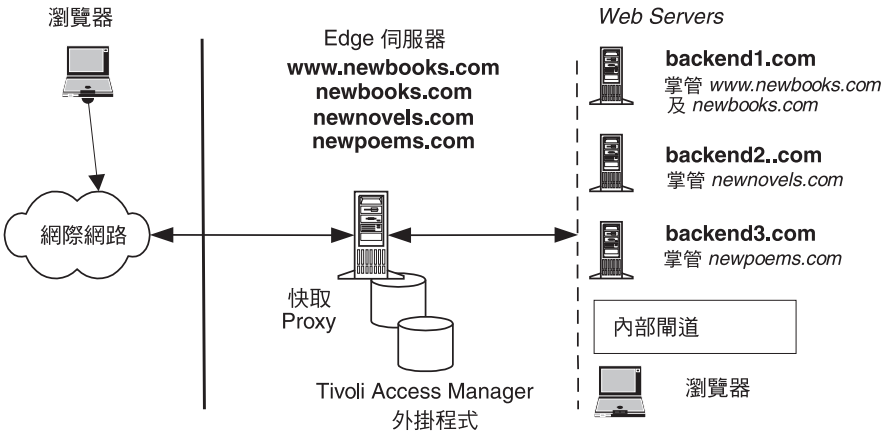

圖 6. 在外掛程式系統上建立別名

在此配置中，所有對 www.newbooks.com、newbooks.com、newnovels.com 和 newpoems.com 的要求會到達 Edge Server Proxy 且由外掛程式保護。使用網域名稱作爲要求的專屬 ID，外掛程式現在可以搜尋配置檔以取得符合網域名稱的伺服器定義。

考慮下列 `osdef.conf` 配置檔：

```
[Global]
login_method = basic

# Definition 1
[Remote: /ESProxy/reverse/newbooks.com]
domains = newbooks.com *.newbooks.com
login_method = forms
route = http://backend1.com

# Definition 2
[Remote: /ESProxy/reverse/label2]
domains = newnovels.com
login_method = certificate
route = http://backend2.com

# Definition 3
[Remote: /ESProxy/check_here/this_is_just_a_label]
domains = newpoems.com
route = http://backend3.com
```

考慮下列要求，外掛程式決定登入方法的地方、使用者被授權的物件空間位置、以及要求被轉送的目標 Web 伺服器：

- 若使用者鍵入下列 URL，此外掛程式會將要求與定義 1 比對，因爲網域設定包含值 *.newbooks.com：

  http://www.newbooks.com/private.html

  此登入方法是套表，因爲它在此定義下已明確地設定。針對授權檢查，網域名稱會被授權字串取代而 URL 路徑會被附加上去。在此範例，讀取許可權的授權檢查會在 `/ESProxy/reverse/newbooks.com/private.html` 執行。要求會轉送至 backend1.com 是因爲遞送設定。
- 如果使用者鍵入下列 URL，此外掛程式首先會在 IP 位址上執行反向 DNS 查閱，然後將要求與定義 2 比對，因爲網域設定包含值 newnovels.com：

http://*IP_address_of_newnovels.com*/gifs/private.html

此登入方法是憑證，因爲它在此定義下已明確地設定。讀取許可權的授權檢查是在 /ESProxy/reverse/label2/gifs/private.html 執行。要求會轉送至 backend2.com 是因爲遞送設定。

- 若使用者鍵入下列 URL，此外掛程式會將要求與定義 3 比對，因爲網域設定包含值 newpoems.com：

  http://newpoems.com/logo.gif

  此登入方法是基本，因爲它在此定義下並未明確地設定且是從 [Global] 定義中擷協取。讀取許可權的授權檢查是在 /ESProxy/check_here/this_is_just_a_label/logo.gif 執行。要求會轉送至 backend3.com 是因爲遞送設定。

- 若使用者配置他們的瀏覽器來使用 Edge Server 作爲 Proxy 並鍵入下列 URL，外掛程式不會爲要求找尋符合值而會使用 [Global] 定義：

  http://internet.com/mail/logo.gif

  登入方法是基本。針對授權檢查，會使用預設轉遞 Proxy 範本，/ESProxy/forward/*domain*/*path*。在此範例，讀取許可權的授權檢查會在 /ESProxy/forward/internet.com/mail/logo.gif 執行。既然此物件可能不存在於物件空間，此有效的許可是從連接於 /ESProxy/forward 的 ACL 沿用而來。要求會自動轉遞到 internet.com，因爲它曾是一個前向 Proxy 要求。然而，於（在物件空間中另一位置執行授權檢查並轉遞 internet.com 要求到別處的）配置檔中建立一個定義是可能的。外掛程式不會考慮要求是一前向或反向要求。在這兩種配置，都會以相同的方式處理要求。

物件空間配置模型

當外掛程式於 Tivoli Access Manager 物件空間中的分支下執行授權檢查時，它會對映所要求的資源或 URL 到物件空間。例如，在伺服器定義 1，會對授權檢查執行下列對映：

```
URL 物件：http://www.newbooks.com/private.html
Tivoli Access Manager 物件：/ESproxy/reverse/newbooks.com/private.html
```

爲了使用 Tivoli Access Manager ACL 將存取控制套用到特定的物件，必須以一種方式建構物件空間，在這種方式中，使用者在他們的 URL 中所要求的物件集與 Web 伺服器提供的物件集之間有一直接對映。最簡單的情況是 URL 中被參考到的檔案和 Web 伺服器上的實際檔案間的一直接對映，如說明：

```
Tivoli Access Manager 物件：/ESproxy/reverse/newbooks.com/伺服器檔案
/ESProxy/reverse/newbooks.com/private.html
/ESProxy/reverse/newbooks.com/public.html
/ESProxy/reverse/newbooks.com/gifs
/ESProxy/reverse/newbooks.com/gifs/logo.gif

URL 物件：http://www.newbooks.com/伺服器檔案
http://www.newbooks.com/private.html
http://www.newbooks.com/public.html
http://www.newbooks.com/gifs
http://www.newbooks.com/gifs/logo.gif
```

範例 **query_contents** 公用程式會提供 Web 伺服器上所有檔案的路徑給 **wesosm** 公用程式。檔案資訊會複製到物件空間，所以當外掛程式執行授權檢查，在 URL 物件和伺服器物件間有一直接對映。

若 URL 物件集將一直是 **query_contents** 公用程式尋找到的目標 Web 伺服器上的實體檔，則此模型運作良好。在某些情況下，URL 物件集可能不會直接對應到 Web 伺服器上的實體檔案。在此情況下，**query_contents** 公用程式可被修改來傳回由 Web 伺服器所提供的虛擬物件，如下所示：

```
Tivoli Access Manager 物件：/ESproxy/reverse/newbooks.com/虛擬物件
/ESProxy/reverse/newbooks.com/object1
/ESProxy/reverse/newbooks.com/object2
/ESProxy/reverse/newbooks.com/object3
/ESProxy/reverse/newbooks.com/object3/object3.1

URL 物件：http://www.newbooks.com/虛擬物件
http://www.newbooks.com/object1
http://www.newbooks.com/object2
http://www.newbooks.com/object3
http://www.newbooks.com/object3/object3.1
```

在此情況下，Web 伺服器所供應的物件可能不會直接對應到 Web 伺服器上的實體檔案。然而，Web 伺服器了解這些物件爲何，也知道如何擷取他們。只要 **query_contents** 公用程式可以爲 **wesosm** 公用程式列舉這些虛擬物件，外掛程式就可以對這些虛擬物件執行授權檢查。

外掛程式藉由驗證在 Tivoli Access Manager 物件空間中是否有適當的許可權來執行授權檢查。它對映 URL 到物件空間以決定執行授權檢查的確切位置。爲了套用 ACL 於外掛程式所保全的特定的物件，必須確定物件空間中所代表的物件集合對應到受保護的 Web 安全的伺服器之 URL 要求中所代表的物件集合。

單一登入配置模型

外掛程式支援在物件空間定義配置檔的 [SSO] 種類下所建立的可自訂單一登入記號，如下表所指出的。

伺服器定義	說明
[SSO]	列於此定義下的設定是用來定義單一登入記號。此定義可有多個實例。

列於此定義的設定與列於 [Global]、[Local] 和 [Remote] 伺服器定義的設定無關。例如， **trust_list** 設定，在配置檔中任何伺服器定義下都是無效的。然而，藉由在一地方定義單一登入記號，他們可被用作 **accept_sso** 和 **submit_sso** （這些在伺服器種類下是有效的）的參數。下列範例顯示 iv-user 記號（兩個 Web 伺服器所需的記號）的定義：

```
[Remote: /ESProxy/reverse/newbooks.com]
domains = newbooks.com
accept_sso = mysso
submit_sso = mysso
route = http://backend1.com

[Remote: /ESProxy/reverse/newnovels.com]
domains = newnovels.com
submit_sso = mysso
route = http://backend2.com

[SSO: mysso]
```

```
name = iv-user
format = <userid>
trust_basis = IP_Address
trust_list = 0.0.0.0/0.0.0.0
```

在此範例，外掛程式會從對 newbooks.com 作要求的任何 IP 位址檢查 iv-user 記號的存在。若找到 iv-user 記號，它會從記號擷取使用者 ID 並授權使用者。外掛程式也將各別後端伺服器的 iv-user 記號送出給 newbooks.com 和 newnovels.com。

彙總的配置程序

Edge Server 外掛程式提供彈性的架構來對您的 Web 伺服器上的受保護的資源進行配置存取控制。它允許您設定伺服器特定的配置項目，如登入方法、單一登入記號和目的地伺服器。套用到每一個伺服器的設定僅可於一個地方設定，而伺服器特定的設定值，則可爲每一各別伺服器設定。

配置外掛程式的一般方法如下：

1. 對反向 Proxy 配置，爲每一需要授權服務程式的 Web 伺服器在外掛程式機器建立別名網域。
2. 爲每一個別伺服器建立對應 [Remote] 伺服器定義，並指派別名網域給該定義。
3. 在該伺服器定義下設定伺服器特定的設定，並於配置檔的 [Global] 定義中設定廣域設定值。對多數設定使用預設內部外掛程式值是足夠的。
4. 執行 **wesosm** 公用程式來產生物件空間，並於 Tivoli Access Manager 物件空間設定合適的 ACL 以控制該伺服器的存取。

在變更配置後，一定要重新啓動外掛程式。若您無法判定配置錯誤的原因，請檢查事件日誌檔以取得說明外掛程式如何處理要求的相關資訊。執行 UNIX 追蹤 **-f** 指令於事件日誌檔上，可在事件發生時，即時幫助觀察事件。在觀察事件日誌後再判定配置問題的原因比較容易。

第 5 章 部署 Edge Server 外掛程式

本章說明 IBM Tivoli Access Manager Plug-in for Edge Server 的範例部署。這個部署動作說明必須控制訪客存取之商業網站的範例。下列各節分別說明本範例：

- 第 27 頁的『設計網站』
- 第 28 頁的『配置網站』

設計網站

本節中，設計了 newbooks.com 的 Edge Server 配置之完整的外掛程式。此網站允許使用者瀏覽和採購書本。Edge Server 之外掛程式的許多關鍵功能在此範例中都有說明。網站的設計可分爲下列幾個元件：

- 第 27 頁的『內容配送』
- 第 27 頁的『單一登入』

內容配送

在這個設計活動中，不會將整個網站的內容儲存在 Web 伺服器上，而是分送到數個 Web 伺服器上。 Web 的內容可分成下列各部分：

- newbooks.com
- catalog.newbooks.com
- account.newbooks.com
- payment.newbooks.com

此 newbooks.com 網域包含招呼頁面和連到網站的其他部分的連結。catalog.newbooks.com 子網域包含在此網站售出的所有書籍的儲存庫。網站的這些部分並不需要存取控制，因此沒有受到保護。

account.newbooks.com 目錄包含 HTML 和 Java 程式碼（用來管理使用者的帳戶）。payment.newbooks.com 目錄也包含 HTML 和 Java 程式碼以接收使用者的買書所付的書款。網站的這些部分大多是受保護的。 account.newbooks.com 下的目錄是用來登記新使用者。這個目錄並沒有受保護。

單一登入

此設計中，在掌控 account.newbooks.com 子網域的 Web 伺服器上執行的一應用程式會需要加密過的 Lightweight Third Party Authentication (LTPA) cookie 來識別經鑑定的使用者。在掌控 payment.newbooks.com 子網域的 Web 伺服器上執行的另一個應用程式需要 HTTP 標頭、App-User（內有使用者 ID）。它也需要來自 Edge Server 的基本鑑定，以作爲接受已鑑定使用者的信任基礎。在對此應用程式以使用者 ID **plugin**和密碼 **bookworm** 鑑定其自身時，Edge Server 外掛程式是需要的。

在本範例中，已經和另一個廠商 newnovels.com 建立關係以便將經鑑定的使用者經由 Edge Server 外掛程式轉送到 newbooks.com. 的受保護的區域。位於 newnovels.com 的

閘道必須使用含有使用者 ID **novelgateway** 和密碼 **bookworm** 的授權標頭對 Edge Server 外掛程式進行自我鑑定。閘道會將已經鑑定的使用者 ID 置於 cookie Novel-User 中，如圖 7 中圖所示。

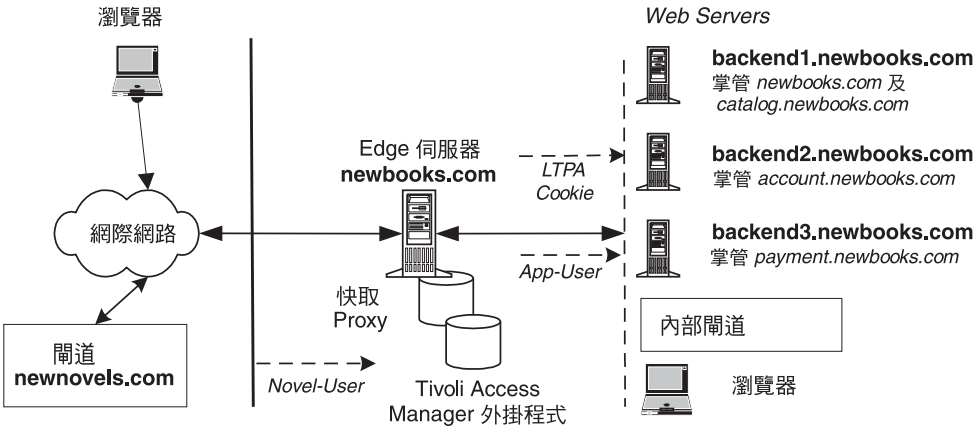

圖 7. newbooks.com 的網站設計

配置網站

爲了提供 newbooks.com 存取控制，必須配置 Edge Server 外掛程式。配置是從在 `osdef.conf` 配置檔中定義廣域設定開始，如下例所示：

```
[Global]
# 執行 wesosm 所需的管理者使用者 ID 和密碼
update_admin_userid = sec_master
update_admin_password = secret5

# 指出需要 SSL 的錯誤訊息
require_ssl_errorfile = /opt/pdweb-lite/samples/errorpages/require_ssl.htmls

# 套表登入及登出資訊
login_method = forms
form_login_file = http://newbooks.com/pub/login.html
form_login_errorfile = http://newbooks.com/pub/loginerr.html
form_logout_url = /pub/logout.html

# 變更密碼資訊
form_chgpasswd_file = http://newbooks.com/pub/chgpasswd.html
form_chgpasswd_submit_url = /pub/chgpasswd
form_chgpasswd_response_url = /pub/passwdchanged.html

# 要尋找的單一登入記號
accept_sso = NovelSSO
```

配置檔中的 `[Global]` 定義會指定要套用到 Edge Server 外掛程式所處理的每一個要求的設定。在此配置中，會提供管理者使用者 ID 和密碼，使得 **wesosm** 公用程式可以建立和更新物件空間。同時，如果要求需要安全連線，但是又沒有提供安全連線，就會將指定的錯誤頁面傳給使用者。但是，如果可能的話，瀏覽器會自動被重新導向到安全站台。

此配置也會也會將登入方法指定爲套表並列出登入套表。登入套表可以從遠端 Web 伺服器（以 http 開頭）來擷取，或者從本端檔案系統擷取。如果套表內有參照影像，則套表中關於這些影像的 URL 連結應該包含影像的完整 URL，例如：

http://newbooks.com/pub/gifs/banner.gif

當所要求的 URL 路徑與指定的登出 URL 路徑相同時，就會讓使用者登出。同時，根據配置所示，當使用者的密碼過期時，也會傳送變更密碼套表給已經鑑定過的使用者。

會從位於 newnovels.com 的閘道來接受單一登入的使用者（使用 NovelSSO 單一登入定義）。這個單一登入定義必須在配置檔中定義。

配置檔中的 [Local] 定義會指定要套用到檔案系統上受到 Edge Server 快取 Proxy 管理之物件的設定。配置檔中只能有其中一個定義。這個伺服器定義是由配置工具建立，其內容類似下列範例：

```
[Local: /ESProxy/bookProxy.com]
domains = bookProxy.com
query_command = http://bookProxy.com/cgi-bin/query_contents?dirlist=/
login_method = basic
```

在本範例中，bookProxy.com 是執行「Edge Server 快取 Proxy」的機器主要的網域名稱。別名 newbooks.com 則是指定給同一部機器的另一個網域名稱（以及其關聯的 IP 位址）。Edge Server 外掛程式會區別對「Edge Server 快取 Proxy」所屬物件以及屬於 newbooks.com 的物件的要求，方法是將所要求的網域名稱和配置檔中的伺服器定義加以比對。此**網域**設定會指出伺服器定義套用的網域。

配置檔中的 [Remote] 定義會指定要套用到外部 Web 伺服器的設定。您可使用的伺服器定義數目並沒有限制。例如，下列定義就很適合 newbooks.com:

```
[Remote: /ESProxy/reverse/newbooks.com]
domains = newbooks.com www.newbooks.com

# 建立物件空間的查詢指定
query_command = http://backend1.newbooks.com/cgi-bin/query_contents?dirlist=/home

# 對映要求的伺服器
route = http://backend1.newbooks.com/home
```

下列子網域定義是針對網站其他部分所定義的：

```
[Remote: /ESProxy/reverse/catalog.newbooks.com]
domains = catalog.newbooks.com
query_command = http://backend1.newbooks.com/cgi-bin/query_contents?dirlist=/catalog
route = http://backend1.newbooks.com/catalog

[Remote: /ESProxy/reverse/account.newbooks.com]
domains = account.newbooks.com
query_command = http://backend2.newbooks.com/cgi-bin/query_contents?dirlist=/
require_ssl = yes
submit_sso = LTPA-COOKIE
route = https://backend2.newbooks.com

[Remote: /ESProxy/reverse/payment.newbooks.com]
domains = payment.newbooks.com
query_command = http://backend3.newbooks.com/cgi-bin/query_contents?dirlist=/
require_ssl = yes
submit_sso = PayAppSSO PayAppAuth
route = https://backend3.newbooks.com
```

這些伺服器定義會指定要送出給每一個需要單一登入記號之 Web 伺服器的單一登入記號。這些定義也會告知 Edge Server 外掛程式，將 URL 對映到掌控所要求的內容的對應的 Web 伺服器。如果要使用另一部遞送模組於 Edge Server 外掛程式的 URL 對映之處，只要從配置檔中刪除對 **遞送 (route)** 關鍵字的所有參照即可。

配置檔中的 [SSO] 定義會定義可被接受或被送出的單一登入記號，如下所示：

```
[SSO: PayAppSSO]
type = header
name = App-User
format = "<userid>"

[SSO: PayAppAuth]
type = auth_header
format = plugin:bookworm

[SSO: NovelSSO]
type = cookie
name = Novel-User
format = "<userid>"
trust_basis = basic_auth
trust_list = novelgateway:bookworm
```

在您建立單一登入定義後，它們可提供作爲 **accept_sso** 和 **submit_sso** 關鍵字的選項。這樣就滿足了此例中的單一登入基本需求。

第 6 章 建立跨網域鑑定服務

本章解釋如何建立「跨網域鑑定服務 (CDAS)」共享程式庫，此程式庫可啓用自訂處理和用戶端鑑定資訊的處理程序。它也說明如何配置 Edge Server 外掛程式來針對鑑定使用自訂共享程式庫。

示範 CDAS 程式庫與說明 CDAS 功能之實作的 Edge Server 外掛程式包裝在一起。您可以重新編譯並修改此示範程式庫以建立自訂共享程式庫。

本章包含下列各節：

鑑定模型

本節說明兩種 CDAS 鑑定模型類型：

當 IBM Tivoli Access Manager plug-in for Edge Server 收到用戶端要求時，它會傳送適當的鑑定資料給自訂共享程式庫。不會依據 Tivoli Access Manager 使用者登錄對使用者進行身份驗證， CDAS 共享程式庫反而會使用外部鑑定機制依據替代使用者登錄對使用者進行身份驗證。最終， CDAS 傳回 Tivoli Access Manager 身份給外掛程式用以對 Tivoli Access Manager 物件空間進行鑑定。

若您建立自訂 CDAS 共享程式庫來處理使用者名稱和密碼鑑定，用戶端鑑定資料必須包含使用者的名稱和密碼。然而，若共享程式庫是寫來處理憑證鑑定，用戶端鑑定資料必須包含用戶端的憑證。

單一鑑定模型

第 32 頁的圖 8說明單一鑑定 CDAS 功能的範例。

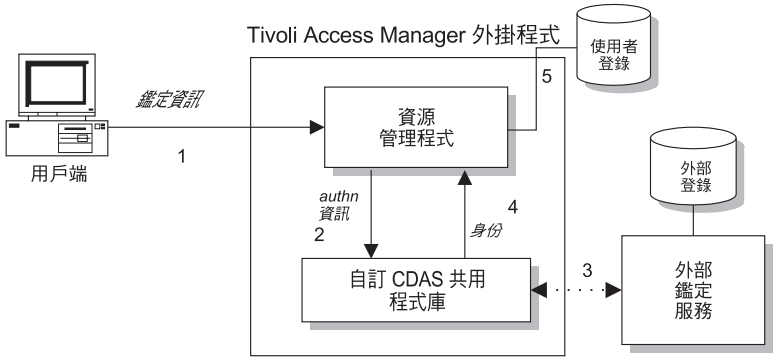

圖 8. CDAS 鑑定模型範例

圖 8 中說明的步驟如下所示：

1. 用戶端提供鑑定資訊給外掛程式。
2. 在此範例，外掛程式是配置來使用自訂 CDAS 共享程式庫以供鑑定。

   此 CDAS 共享程式庫可於內部驗證使用者身份並將產生的 Tivoli Access Manager 身份傳回外掛程式（ 4 步驟）。例如，共享程式庫可以接受數位憑證，修改「識別名稱 (DN)」資料，並將修改的 DN 如 Tivoli Access Manager 身份般傳回。
3. 自訂共享程式庫可傳送資料到執行其用戶端自身鑑定外部鑑定服務（也許使用協力廠商（遺留的）使用者登錄）。
4. CDAS 傳回下列狀態碼之一到外掛程式：
   - 一個成功的狀態碼（指出成功的鑑定企圖）和 Tivoli Access Manager 身份。
   - 一個不成功的狀態碼，指出失敗的鑑定企圖。

   此外，自訂 CDAS 可以被寫來提供延伸的屬性資料給外掛程式（以內含於使用者證明中）。
5. 若傳回了成功的狀態碼，外掛程式試著比對身份與 Tivoli Access Manager 使用者登錄中的項目。若找到符合項目，外掛程式會將用戶端當作已鑑定的。否則，它會將用戶端視爲未經授權的。

有一個成功鑑定會產生在使用者的 Tivoli Access Manager 證明中。任何延伸的屬性資料都包含於證明中，可於之後擷取來適當使用。證明可讓使用者參與 Tivoli Access Manager 安全網域。

分派的鑑定模型

您可建立根據外掛程式傳進來的關聯參數分派鑑定要求到其他 CDAS 模組的 CDAS 模組。此分派 CDAS 模組本身不會執行任何鑑定，而會委派鑑定和延伸屬性的建立給其他 CDAS 模組並將從 CDAS 模組傳回的身份傳遞給外掛程式。使用此模型，外掛程式可根據 URL 對不同的使用者登錄進行身份驗證。

第 33 頁的圖 9 說明 CDAS 分派的功能之範例。

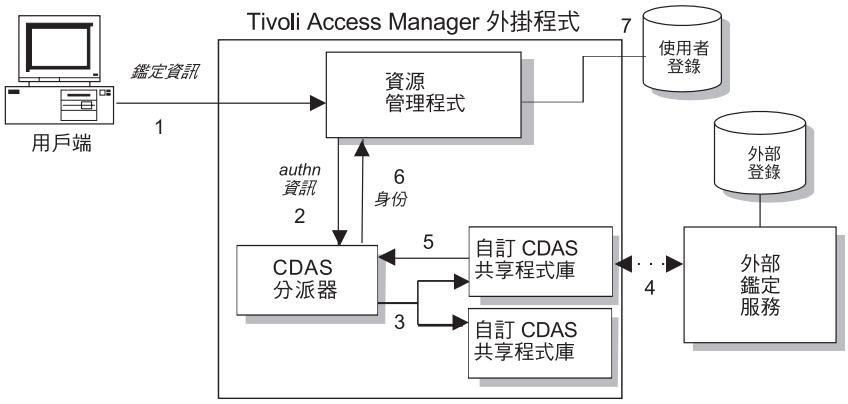

圖 9. 分派的鑑定模型範例

圖 9 中說明的步驟如下：

1. 用戶端提供鑑定資訊給外掛程式。
2. 在此範例中，外掛程式是配置來使用自訂 CDAS 共享程式庫以處理此類鑑定的資料。
3. 根據從外掛程式傳來的參數，CDAS 模組會爲要求分派鑑定到適當的 CDAS 模組。

   此 CDAS 共享程式庫可於內部驗證使用者身份並將產生的 Tivoli Access Manager 身份傳回 CDAS 分派器。例如，共享程式庫可以接受數位憑證，修改「識別名稱 (DN)」資料，並將修改的 DN 如 Tivoli Access Manager 身份般傳回。
4. 自訂共享程式庫可傳送資料到執行其用戶端自身鑑定外部鑑定服務（也許使用協力廠商（遺留的）使用者登錄）。
5. 適當的 CDAS 模組傳回 Tivoli Access Manager 身份和延伸屬性到 CDAS 分派器。
6. CDAS 分派器模組傳回下列狀態碼之一到外掛程式：
   - 一個成功的狀態碼（指出成功的鑑定企圖）和 Tivoli Access Manager 身份。
   - 一個不成功的狀態碼，指出失敗的鑑定企圖。

   此外，自訂 CDAS 可以被寫來提供延伸的屬性資料給外掛程式（以內含於使用者證明中）。
7. 若傳回了成功的狀態碼，外掛程式試著比對身份與 Tivoli Access Manager 使用者登錄中的項目。若找到符合項目，外掛程式會將用戶端當作已鑑定的。否則，它會將用戶端視爲未經授權的。

建置一自訂共享程式庫

在建置自訂 CDAS 程式庫前，您必須決定想以什麼方式讓特定的鑑定和對映服務在您的安全網域中操作。使用示範資源 CDAS 來實作您的自訂 CDAS 程式庫。

本節包含下列主題：

CDAS 應用程式開發工具箱

此 CDAS 應用程式開發工具箱 (ADK) 包含下列元件：

- API 程式庫（公用程式函數）
- API 標頭檔
- CDAS 原始檔範例（僅供示範）
- Make 檔

CDAS ADK 檔案是位於下列其中一項目錄：

- 在 UNIX 系統：

  `/opt/pdweb-lite/samples/cdas_adk`

- 在 Windows 系統上：

  install_dir`\samples\cdas_adk`

ADK 元件是包含在下列子目錄中。

目錄	內容
`include`	此目錄含有 C 標頭檔。 請參閱『標頭檔』。
`lib`	此目錄含有靜態 CDAS API 公用程式程式庫： - 在 UNIX 系統：`libpdxauthn.a` - 在 Windows 系統：`pdxauthn.lib`
`example`	example 目錄包含： - 原始檔 (`xauthn.c`) - Makefile - 一個預先建立的特定平台範例共享程式庫，用以示範功能性的 CDAS

標頭檔

下列標頭檔是包含在 `include` 目錄中。

檔案	內容
`pdxauthn.h`	函數原型的定義、用戶端身份和鑑定 CDAS API 函數所用的錯誤碼。
`xnvlist.h`	使用者鑑定資料公用程式功能
`xattr.h`	使用者延伸的屬性資料結構公用程式功能

程式設計自訂共享程式庫

自訂 CDAS 共享程式庫必須包含下列 API：

- xauthn_initialize

  如需相關資訊，請參閱第 35 頁的『起始設定：xauthn_initialize』

- xauthn_shutdown

  如需相關資訊，請參閱第 35 頁的『關機：xauthn_shutdown』

- xauthn_authenticate

  如需相關資訊，請參閱第 35 頁的『鑑定：xauthn_authenticate』

- xauthn_change_password

如需相關資訊，請參閱第 35 頁的『密碼變更：xauthn_change_password』

註: 這些 API 函數在第 40 頁的『CDAS API 核心函數參照』 中有詳細說明。

起始設定：xauthn_initialize

外掛程式載入 CDAS 共享程式庫並起始設定它，方法是呼叫 **xauthn_initialize**。

此函數包含 **argc** 和 **argv** 選項。這些選項包含 `osdef.conf` 配置檔中所指定的值。不像 C 語言 **argv**， **argv[0]** 陣列項目是第一個選項。

關機：xauthn_shutdown

關機期間，外掛程式會呼叫 **xauthn_shutdown** 函數以停止 CDAS 共享程式庫處理程序。

此 **xauthn_shutdown** 函數是以與傳送到 **xauthn_initialize** 函數相同的 **argc** 和 **argv** 選項來呼叫（在第一次起始設定共享程式庫時）。

鑑定：xauthn_authenticate

在配置了 CDAS 共享程式庫以及收到要求後，外掛程式會傳入使用者的資訊到共享程式庫，方法是經由 **xauthn_authenticate** 函數。

使用者鑑定資訊會傳入位於名稱/值資料清單 (**xnvlist_t**) 中的此函數。名稱/值資料清單的內容可改變，且這些內容對配置的鑑定方法而言是特定的。

此 **xauthn_authenticate** 函數根據資料清單中所找到的鑑定資訊，執行應用程式特定鑑定處理程序並傳回產生的用戶端身份 (**xauthn_identity_t**) 給外掛程式。

很重要的是要注意，經由此函數傳回的用戶端身份可含有延伸的屬性資料。

密碼變更：xauthn_change_password

此函數讓使用者對儲存在替代使用者登錄中的帳戶密碼進行變更。僅使用者名稱和密碼鑑定方法支援此函數。若外部鑑定機制不支援密碼變更，此函數傳回：

```
XAUTHN_S_UNSUPPORTED_AUTHN_METHOD
```

使用者鑑定資訊會傳入位於名稱/值資料清單 (**xnvlist_t**) 中的此函數。資料清單包含使用者名稱、舊密碼和新密碼。

使用者鑑定資料

外掛程式傳送各種用戶端鑑定資訊到共享程式庫。此資訊是使用名稱/值清單格式來傳送，其中的名稱是指定值類型的識別符。

此資訊是儲存在 **xnvlist_t** 資料類型。可使用公用程式函數 **xnvlist_get** 來存取這些值。

下列表格列出外掛程式傳送到 CDAS 模組的使用者鑑定選項。

鑑定方法	名稱	值
使用者名稱/密碼	**xauthn_username** **xauthn_password** **xauthn_new_password** **xauthn_ipaddr** **xauthn_browser_info** **xauthn_extended_handle** **xauthn_extended_parameter**	- 使用者名稱 - 使用者密碼 - 使用者新密碼 - 使用者 IP 位址 - 瀏覽器資訊 - 快取 Proxy 控點 - 配置檔選項
憑證	**xauthn_cert_dn** **xauthn_ipaddr** **xauthn_browser_info** **xauthn_extended_handle** **xauthn_extended_parameter**	- 憑證的 DN - 使用者 IP 位址 - 瀏覽器資訊 - 快取 Proxy 控點 - 配置檔選項
單一登入	**xauthn_ipaddr** **xauthn_browser_info** ″**Request-URI**″ ″**Request-Headers**″ **xauthn_extended_handle** **xauthn_extended_parameter**	- 使用者 IP 位址 - 瀏覽器資訊 - 要求 URL - 要求標頭 - 快取 Proxy 控點 - 配置檔選項

雖然 Edge Server 外掛程式的 CDAS 實作與 WebSEAL 類似，仍有些微差異。差異如下：

- **xauthn_extended_handle** 和 **xauthn_extended_parameter** Edge Server 是外掛程式傳送給 CDAS 模組的選項。
- **xauthn_extended_handle** 提供 CDAS 模組擷取使用快取 Proxy 的 API 來擷取其他的 HTTP 標頭所需要的快取 Proxy 的控點。
- **xauthn_extended_parameter** 從 `osdef.conf` 配置檔提供相關聯的選項給 CDAS 模組。

傳回用戶端身份

對傳回產生的用戶端身份到外掛程式而言，CDAS 共享程式庫是必要的。 用戶端身份是由 **xauthn_identity_t** 資料結構所定義的。

如需相關資訊，請參閱 *IBM Tivoli Access Manager WebSEAL Developer's Guide*。

編譯自訂共享程式庫

CDAS 示範程式庫的原始碼是位於下列目錄之一：

- 在 UNIX 系統：

  `/opt/pdweb-lite/samples/cdas_adk/example`

- 在 Windows 系統：

  install_dir`\samples\cdas_adk\example`

原始檔 `xauthn.c` 和 `xauthn.h` 是用來建立 CDAS 共享物件。

若要自訂和編譯自訂 CDAS 共享程式庫，請執行下列動作：

1. 自訂原始檔來實作對您的使用者登錄進行身份驗證所需的邏輯。

2. 若要重新編譯程式碼，使用下列其中一項 make 檔：
   - 在 UNIX 系統：

     `/opt/pdweb-lite/samples/cdas_adk/example/Makefile.in`
   - 在 Windows 系統：

     install_dir`\samples\cdas_adk\example\Makefile.in`

   在每一平台上編譯的指示是包含於 `Makefile.in` 中。makefile 假設您的編譯器和鏈結指令可從現行目錄呼叫且已經在系統的路徑中。
3. 成功建置自訂 CDAS 模組後，出現的共享程式庫命名如下：
   - 若爲 AIX 系統：`libwslcdas.a`
   - 若爲 Linux 系統：`libwslcdas.so`
   - 若爲 Solaris 系統：`libwslcdas.so`
   - 若爲 Windows 系統：`wslcdas.dll`
4. 停止外掛程式並將新 CDAS 模組複製到位於下列其中一目錄的現有 CDAS 模組：
   - 在 UNIX 系統：

     `/opt/pdweb-lite/lib`
   - 若爲 Windows 系統：*install_dir*`\bin`

   註: 如需關於啓動和停止外掛程式的相關資訊，請參閱第 11 頁的『啓動和停止 Edge Server 外掛程式』。

配置 Edge Server 外掛程式來使用自訂共享程式庫

本節討論特定的配置步驟，您必須執行這些步驟，Edge Server 外掛程式才可使用 CDAS 介面。

本節包含下列主題：

配置自訂共享程式庫

若要配置自訂 CDAS 共享程式庫，請修改包含在 `osdef.conf` 檔案中的配置選項。如需關於 `osdef.conf` 配置選項的資訊，請參閱第 51 頁的附錄 B, 『物件空間定義配置檔參照』。

自訂共享程式庫配置方案

下列方案說明配置選項的使用。此方案顯示三個使用 CDAS 的網站。第一個網站使用套表作爲登入方法，但第二個網站使用憑證。第三個網站使用 CDAS 來進行單一登入，但使用 Tivoli Access Manager 來進行基本鑑定。

```
[Global]
...
cdas_loaded = yes
cdas_init_parameter = ldap /etc/ldap.conf
cdas_init_parameter = cert /etc/cert.conf
```

```
[Remote: /ESProxy/reverse/newnovels.com]
domains = newnovels.com
login_method = forms
cdas_enabled = yes
cdas_auth_parameter = ldap

[Remote: /ESProxy/reverse/newpoems.com]
domains = newpoems.com
login_method = certificate
cdas_enabled = yes
cdas_auth_parameter = cert

[Remote: /ESProxy/reverse/newbooks.com]
domains = newbooks.com
login_method = basic
accept_sso = CDAS-MODULE
```

在此方案中，**xauthn_init** 被呼叫兩次，第一次是以 **argv[0]** = **ldap**, **argv[1]** = **/etc/ldap.conf** 起始設定選項，第二次是以 **argv[0]** = **cert**, **argv[1]** = **/etc/cert/conf** 起始設定選項。存取 newnovels.com 的使用者是以 **xauthn_extended_parameter** = **ldap** 鑑定，但存取 newpoems.com 的使用者是以 **xauthn_extended_parameter** = **cert** 鑑定。CDAS 模組也被呼叫來偵測存取 newbooks.com 之預先鑑定過的使用者。

CDAS 共享程式庫可同步支援多個使用者儲存庫並根據其接收到的 **xauthn_extended_parameter** 值，執行切換。也可根據 **argv[0]** 選項執行多重起始設定，允許一個 CDAS 共享程式庫來執行另外需要多個 CDAS 程式庫之功能。

配置示範程式庫

若要配置 CDAS 示範程式庫，請修改 osdef.conf 檔案中的配置選項。例如，考慮顯示在圖 10 中的選項。

```
[Global]
...
cdas_loaded=yes
cdas_init_parameter=demouser userid demopassword password democertdn CertDN validpddn validpdDN

[Local]
cdas_enabled=yes
cdas_auth_parameter=basic_auth
```

圖 10. osdef.conf 中配置選項的範例

註: 對於示範模組，**basic _auth** 和 **cert** 都是 **cdas_auth_parameter** 的有效值。

在此範例，對示範模組配置了使用者 ID 和密碼、對應 Tivoli Access Manager 的識別名稱和憑證的識別名稱。由 **cdas_init_parameter** 指定的引數會傳送到示範模組（當呼叫 **xauthn_initialize** 函數時）。下列值會傳送到 **xauthn_initialize** 常式：

```
argc = 8
argv[0] = demouser
argv[1] = userid
argv[2] = demopassword
argv[3] = password
argv[4] = democertdn
argv[5] = CertDN
argv[6] = validpddn
argv[7] = validpdDN
```

當本端 Web 伺服器上受保護的資源被存取時，會使用 **xauthn_authenticate** 函數執行鑑定。當 **xauthn_authenticate** 函數被呼叫時，範例模組會檢查

xauthn_extended_parameter 值。若傳入 **basic_auth**，則會對照起始設定時間所傳入的用者 ID 和密碼來檢查傳入的使用者 ID 和密碼。若傳入 **cert** ，則會對起始設定時傳入的 *CertDN* 來檢查傳入的 *CertDN*。若鑑定成功，有效的 Tivoli Access Manager 識別名稱會傳回外掛程式以進行授權。

載入自訂共享程式庫

CDAS 共享程式庫會在外掛程式的起始設定期間載入。CDAS 程式庫檔案可在下列其中一位置找到：

- 在 UNIX 系統：

  `/opt/pdweb-lite/lib/libwslcdas.`*`ext`*

  其中 *ext* 是下列其中一項：

  – 在 AIX 系統：`a`
  – 在 Linux 系統：`so`
  – 在 Solaris 系統： `so`
- 在 Windows 系統：

  `install_dir``\bin\wslcdas.dll`

若您想要外掛程式使用包裝的示範 CDAS 程式庫，請執行下列其中一項：

- 若爲 UNIX 系統，將 `ibwe.idas.`*`ext`* 檔案換成 `libcdasdemo.`*`ext`* 檔案，可在下列位置找到它：

  `/opt/pdweb-lite/samples/cdas_adk/example/libcdasdemo.`*`ext`*

  其中 *ext* 是下列其中一項：

  – 在 AIX 系統：`a`
  – 在 Linux 系統：`so`
  – 在 Solaris 系統： `so`
- 若爲 Windows 系統，將 `wescdas.dll` 檔案換成 `cdasdemo.dll` 檔案，可在下列位置找到它：

  `install_dir``\samples\cdas_adk\example\cdasdemo.dll`

若您想要外掛程式使用自訂的 CDAS 共享程式庫，請進行下列其中一項：

- 若爲 UNIX 系統，將 `ibwe.idas.`*`ext`* 檔案換成自訂 CDAS 共享程式庫檔案（其中 *ext* 是下列其中一項）：

  – 在 AIX 系統：`a`
  – 在 Linux 系統：`so`
  – 在 Solaris 系統： `so`
- 若爲 Windows 系統，將 `wescdas.dll` 檔案換成自訂 CDAS 共享程式庫檔案。

註: 若在載入您的自訂 CDAS 共享程式庫時發生問題，您可以回復到示範 CDAS 程式庫。

CDAS 核心和公用程式函數

下列核心 API 函數必須在您的自訂 CDAS 共享程式庫中實作：

- **xauthn_initialize**
- **xauthn_shutdown**
- **xauthn_authenticate**
- **xauthn_change_password**

CDAS 公用程式程式庫是位於下列其中一個目錄中：

- 在 UNIX 系統：

  `/opt/pdweb-lite/samples/cdas_adk/lib`

- 在 Windows 系統：

  `install_dir\samples\cdas_adk\lib`

AIX、Linux 和 Solaris 版的 `libpdxauthn.a` 或 Windows 版的 `pdxauthn.lib` 等靜態程式庫檔案都包含了公用程式函數。若要使用這些函數，您必須將您的自訂共享程式庫連結到此檔案。

下列公用程式函數有助於資料操作：

- **xnvlist_get**
- **xattr_malloc**
- **xattr_free**
- **xattr_get**
- **xattr_set**
- **xattr_dup**

此 **xnvlist_get** 函數接收從外掛程式傳入的鑑定資料。剩餘的公用程式允許您建構 Tivoli Access Manager 身份的延伸屬性。

如需相關資訊，請參閱第 40 頁的『CDAS API 核心函數參照』。如需公用程式函數的相關資訊，請參閱 *IBM Tivoli Access Manager WebSEAL Developer's Reference*。

CDAS API 核心函數參照

此節列出用來實作您的 CDAS 共享程式庫之下列核心 API 函數：

- **xauthn_authenticate**
- **xauthn_change_password**
- **xauthn_initialize**
- **xauthn_shutdown**

xauthn_authenticate

執行 CDAS 鑑定。

上下文

```
xauthn_status_t
xauthn_authenticate(
   xnvlist_t *authnInfo,
   xauthn_identity_t *ident
);
```

說明

外掛程式呼叫此介面來執行客戶特定外部鑑定。用戶端鑑定資訊是經外掛程式藉由輸入引數 **authnInfo** 來傳送。

參考第 35 頁的『使用者鑑定資料』 以取得 **authnInfo** 可以包含的鑑定選項清單。

根據鑑定資訊，此函數實作特定的鑑定機制並儲存產生的用戶端資訊於 **ident**。此資訊稍後會傳回外掛程式。

請謹記用戶端身份 **ident** 可包含額外的使用者資訊。

選項

輸入

authnInfo
此 **authnInfo** 選項是含有用戶端鑑定資訊的名稱/值資料清單。

輸入/輸出

ident
此 **ident** 選項包含鑑定過的使用者資訊。

回覆碼

若成功，此函數會傳回 XAUTHN_S_COMPLETE。

可能的錯誤碼可以在 `pdxauthn.h` 標頭檔中找到。

xauthn_change_password

執行 CDAS 密碼變更。

上下文

```
xauthn_status_t
xauthn_change_password(
   xnvlist_t *authnInfo
);
```

說明

外掛程式呼叫此介面來實作自訂密碼變更機制。此介面僅支援使用者名稱和密碼鑑定機制。用戶端密碼變更資訊是經外掛程式藉由輸入引數 **authnInfo** 傳送。

請參考第 35 頁的『使用者鑑定資料』 以取得 **authnInfo** 包含的鑑定資料的清單。

選項

輸入

authnInfo

此 **authnInfo** 選項是含有用戶端鑑定資訊的名稱/值資料清單。

回覆碼

若成功，函數會傳回 XAUTHN_S_COMPLETE。

若外部鑑定處理不支援密碼變更就會傳回 XAUTHN_S_UNSUPPORTED_AUTHN_METHOD。

可能的錯誤碼可以在 `pdxauthn.h` 標頭檔中找到。

xauthn_initialize

起始設定 CDAS 共享程式庫。

上下文

```
xauthn_status_t
xauthn_initialize(
   int argc,
   const char **argv
);
```

說明

使用此函數來起始設定鑑定共享程式庫。此輸入選項 **argc** 和 **argv** 是從 osdef.conf 配置檔中 **cdas_init_parameter** 所指定的選項所建置的。下列範例定義說明範例 CDAS 共享程式庫的起始設定：

```
cdas_init_parameter = -dbms sys.db
```

在此範例，**xauthn_initialize** 被呼叫時的 **argc** 值爲 2。此 **argv** 陣列含下列值：

```
argv[0] = "-dbms"
argv[1] = "sys.db"
```

請勿修改輸入選項。

選項

輸入

argc
在 **argv** 陣列中含的引數數目。

argv
針對此服務實例傳入服務定義的字串引數。

回覆碼

若成功，此函數會傳回 XAUTHN_S_COMPLETE。

可能的錯誤碼可以在 pdxauthn.h 標頭檔中找到。

xauthn_shutdown

關閉 CDAS 共享程式庫。

上下文

```
xauthn_status_t
xauthn_shutdown(
   int argc,
   const char **argv
);
```

說明

正常關機期間，外掛程式會呼叫此介面來執行任何自訂環境所必須的關機處理程序。輸入選項 **argc** 和 **argv** 是從 `osdef.conf` 配置檔中以 **cdas_init_parameter** 指引指定的選項建置的。下列範例說明範例 CDAS 共享程式庫的終止：

```
cdas_init_parameter = -dbms sys.db
```

在此範例，**xauthn_shutdown** 被呼叫時的 **argc** 值爲 2。此 **argv** 陣列含下列值：

```
argv[0] = "-dbms"
argv[1] = "sys.db"
```

選項

輸入

argc
在 **argv** 陣列中含的引數數目。

argv
針對此服務實例傳入服務定義的字串引數。

回覆碼

若成功，此函數會傳回 XAUTHN_S_COMPLETE。

可能的錯誤碼可以在 `pdxauthn.h` 標頭檔中找到。

第 7 章 移除 Edge Server 外掛程式

本章說明如何解除配置以及移除 Edge Server 外掛程式。要解除配置以及移除外掛程式，請完成下列其中一節的指示：

在 AIX 上移除 Edge Server 外掛程式

在 AIX 上的 Edge Server 外掛程式之移除作業是兩部分的處理程序。您必須先解除配置外掛程式套件然後將它移除。

若要在 AIX 上解除配置外掛程式，請執行下列動作：

1. 以 **root** 身份登入。
2. 請輸入以下指令：

   ```
   wslconfig.sh -u
   ```

3. 輸入 IBM Tivoli Access Manager 管理使用者的使用者 ID。您可以按下 Enter 鍵來接受 **sec_master** 的預設使用者。

   此時會出現提示，要求您輸入 Tivoli Access Manager 管理者的密碼。
4. 請輸入 **sec_master** 的密碼。

   這時會出現一系列的狀態訊息。Edge Server 外掛程式登入 Tivoli Access Manager Policy Server 並解除自身的配置。

   解除配置完成且 **wslconfig** 公用程式存在。

如要在 AIX 上移除外掛程式套件和任何相依軟體，請輸入下列指令：

```
installp -u -g PDPlgES
```

註: 僅在您想移除指定的套件的相依軟體時，使用 **–g** 選項。

Edge Server 外掛程式檔案已移除。**installp** 公用程式隨即結束。在 AIX 上的 Edge Server 外掛程式之移除作業已完成。

如果您想要移除必備 Tivoli Access Manager 元件，請遵循 *IBM Tivoli Access Manager Base 安裝手冊*中的移除指示。

移除 Linux 上的 Edge Server 外掛程式

移除在 Linux 上的 Edge Server 外掛程式之作業是兩部分的處理程序。您必須先解除配置外掛程式套件然後將它移除。

若要在 Linux 上解除配置外掛程式，請執行下列動作：

1. 以 **root** 身份登入。

2. 請輸入以下指令：

   ```
   wslconfig.sh -u
   ```

3. 輸入 Tivoli Access Manager 管理使用者的使用者 ID。您可以按下 Enter 鍵來接受 **sec_master** 的預設使用者。

   此時會出現提示，要求您輸入 Tivoli Access Manager 管理者的密碼。

4. 請輸入 **sec_master** 的密碼。

   這時會出現一系列的狀態訊息。Edge Server 外掛程式登入 Tivoli Access Manager Policy Server 並解除自身的配置。

   解除配置完成且 **wslconfig** 公用程式存在。

如要在 Linux 上移除外掛程式檔案，請輸入下列指令：

```
rpm -e PDPlgES-PD
```

Edge Server 外掛程式檔案已移除。**rpm** 公用程式存在。在 Linux 上的 Edge Server 外掛程式之移除作業已完成。

如果您想要移除 Tivoli Access Manager runtime environment 或其他 Tivoli Access Manager 元件，請遵循 *IBM Tivoli Access Manager Base 安裝手冊*中的指示。

在 Solaris 上的移除 Edge Server 外掛程式

移除在 Solaris 上的 Edge Server 外掛程式之作業是兩部分的處理程序。您必須先解除配置外掛程式套件然後將它移除。

若要在 Solaris 上解除配置外掛程式，請執行下列動作：

1. 以 **root** 身份登入。
2. 請輸入以下指令：

   ```
   wslconfig.sh -u
   ```

3. 輸入 Tivoli Access Manager 管理使用者的使用者 ID。您可以按下 Enter 鍵來接受 **sec_master** 的預設使用者。

   此時會出現提示，要求您輸入 Tivoli Access Manager 管理者的密碼。

4. 請輸入 **sec_master** 的密碼。

   這時會出現一系列的狀態訊息。Edge Server 外掛程式登入 Tivoli Access Manager Policy Server 並解除自身的配置。

   解除配置完成且 **wslconfig** 公用程式存在。

如要在 Solaris 上移除外掛程式檔案，請輸入下列指令：

```
pkgrm PDPlgES
```

Edge Server 外掛程式檔案已移除。**pkgrm** 公用程式隨即結束。在 Solaris 上的 Edge Server 外掛程式之移除作業已完成。

如果您想要移除 Tivoli Access Manager runtime environment 或其他 Tivoli Access Manager 元件，請遵循 *IBM Tivoli Access Manager Base 安裝手冊*中的指示。

移除 Windows 上的 Edge Server 外掛程式

移除在 Windows 上的 Edge Server 外掛程式之作業是兩部分的處理程序。您必須先解除配置外掛程式套件然後將它移除。

若要在 Windows 上解除配置外掛程式，請執行下列動作：

1. 以 **Administrator** 身份登入。
2. 請輸入以下指令：

   ```
   wslconfig -u
   ```

3. 輸入 Tivoli Access Manager 管理使用者的使用者 ID。您可以按下 Enter 鍵來接受 **sec_master** 的預設使用者。

   此時會出現提示，要求您輸入 Tivoli Access Manager 管理者的密碼。

4. 請輸入 **sec_master** 的密碼。

   這時會出現一系列的狀態訊息。Edge Server 外掛程式登入 Tivoli Access Manager Policy Server 並解除自身的配置。

   解除配置完成且 **wslconfig** 公用程式存在。

若要在 Windows 上解除配置外掛程式，請執行下列動作：

1. 選取**開始 → 設定 → 控制台**。按一下**新增/移除程式**。會顯示「新增/移除程式」對話，列出所有已安裝的軟體。
2. 選取 **Tivoli Access Manager Plug-in for Edge Server**。按一下**新增/移除程式**。畫面上會顯示「選擇語言設定」對話框。
3. 選取移除程序要使用的語言，然後按一下**確定**。
4. 從「確認元件移除」訊息框，按一下**是**。 Edge Server 檔案的外掛程式已移除。
5. 按一下**確定**來結束程式。

在 Windows 上的 Edge Server 外掛程式之移除作業已完成。

如果您想要移除 Tivoli Access Manager runtime environment 或其他 Tivoli Access Manager 元件，請遵循 *IBM Tivoli Access Manager Base 安裝手冊*中的指示。

附錄 A. 基礎配置檔參照

ibmwesas.conf 檔案包含用來起始設定外掛程式的設定值。這些設定值包括 Tivoli Access Manager 配置設定值以及 LTPA & WebSEAL 失效接替 cookie 模組配置設定值。其他的配置可經由物件空間定義配置檔來取得。僅有需要使用者修改的設定會列在下表中。所有其他的設定都經由配置工具適當地設定，通常不需使用者修改。

選項	說明
LTPA_Cookie_Enabled	指出 LTPA cookie 模組是否使用金鑰檔和金鑰檔密碼來起始設定。預設值是 YES。
LTPA_Cookie_Keyfile	指出含有用來加密和解密的密碼金鑰之 LTPA 金鑰檔。可由 WebSphere Application Server 針對外掛程式和伺服器間的單一登入來產生此檔案。
LTPA_Cookie_Keyfile_Password	指出存取 LTPA 金鑰檔所需的密碼。
LTPA_Cookie_TTL	指出外掛程式不會重新整理的 LTPA cookie 的閒置到期期間。預設值是 20 分鐘。
LTPA_Cookie_Validation	指出 LTPA cookie 的簽名在外掛程式解密 cookie 時，是否經過加強的安全驗證。注意此驗證可以比僅解密 cookie 更耗 CPU 資源。預設值是 YES。
WebSEAL_Cookie_Enabled	指出 WebSEAL 失效接替 cookie 模組是否使用金鑰檔和金鑰檔標籤來起始設定。預設值是 YES。
WebSEAL_Cookie_Keyfile	指出 WebSEAL 失效接替 cookie 金鑰檔含有用來加密和解密的密碼金鑰。此檔案是在配置外掛程式期間產生的。
WebSEAL_Cookie_Keylabel	指出用來從 WebSEAL 失效接替 cookie 金鑰檔中擷取密碼金鑰的標籤。
WebSEAL_Cookie_TTL	指出外掛程式不會重新整理的 WebSEAL Fail Over cookie 的閒置到期期間。預設值是 20 分鐘。
ObjectSpace_File	指出物件空間定義配置檔的位置。此檔案根據 URL 中所指定的網域名稱告訴外掛程式 Tivoli Access Manager 物件空間的哪一分支是用於授權。此檔案也指定網域特定的配置設定。
UserMap_File	指出使用者對映檔案的位置。此檔案告訴外掛程式如何將一般使用者 ID 或憑證識別名稱對映到 Tivoli Access Manager 使用者。此檔案是用於判定憑證使用者的證明和抵達外掛程式之前經過鑑定的使用者。

附錄 B. 物件空間定義配置檔參照

此附錄提供物件空間定義配置檔上的參考資訊並包含下列部分：

- 『伺服器定義』
- 第 59 頁的『單一登入定義』

伺服器定義

osdef.conf 檔案定義受保護的物件 (URL) 和 Tivoli Access Manager 物件空間之間的對映。受保護的 Web 伺服器之設定會被組織到伺服器定義中。在伺服器定義中，伺服器特定的設定，如網域、登入方法、應被用來對使用者執行授權檢查的物件空間分支和其他網域特定的設定都會被配置。

選項	說明
物件空間（僅 wesosm）	
update_objectspace	指出外掛程式的此實例是否負責以每一個 Web 伺服器的檔案系統資訊更新 Tivoli Access Manager 物件空間。預設值是 YES。
update_admin_userid	指出修改物件空間所需的 Tivoli Access Manager 管理者使用者 ID。
update_admin_password	指出修改物件空間所需的 Tivoli Access Manager 管理者密碼。
query_command	指出所發出來以取得物件空間資訊的 HTTP 要求。此要求傳回的資料格式應與 WebSEAL **query_contents** 公用程式符合。
query_authentication	指出傳到掌管 **query_contents** 之 Web 伺服器的 HTTP 授權標頭參數。若未指定此選項，不會傳送任何授權標頭。
query_interval	指出在此分支下被更新的物件空間比率。若此值設爲 0，就不會對此 Tivoli Access Manager 物件空間分支執行任何更新。預設值是1440 分鐘（1 天）。
query_files	指出是否也要進入 Tivoli Access Manager 物件空間查詢每一目錄中的檔案。如果您僅想連接 ACL 到目錄，那 Tivoli Access Manager 就沒必要將 Web 檔案儲存在物件空間中。預設值是 YES。
query_depth	指出進入 Tivoli Access Manager 物件空間查詢的子目錄深度。既然物件空間是儲存在授權資料庫中，不要將非必要的檔案系統資訊儲存在此資料庫中是有利的。只將物件儲存在 Web 空間（應該讓 ACL 連接到他們）就足夠了。將此值設爲 0 會停用物件空間中此分支的深度限制。預設值是 0。

選項	說明
query_removal	指出無法識別或未知項目是否會從物件空間中移除。若已啓用，在 Web 伺服器上找不到的此分支下的所有現有的項目都會從物件空間中移除。預設值是 YES。
物件空間（wesosm 和外掛程式）	
objectspace_branch_reverse	指出物件空間分支在哪個授權要求下，會取代此檔案中未明確定義的反向 proxy 要求。預設值是 /reverse。
objectspace_branch_forward	指出物件空間分支在哪個授權要求下，會取代此檔案中未明確定義的反向 proxy 要求。預設值是 /forward。
objectspace_filesystem_type	指出內容 Web 伺服器在哪種檔案系統類型上執行。此設定會判定每一個 URL 對映到 ACL 字串以授權使用者的方式。預設值是 unix。 檔案系統類型： • unix - 區分大小寫的 UNIX 檔案系統 • win32 - 不區分大小寫的 WIN32 檔案系統
一般	
domains	指出伺服器定義套用的網域清單。若所要求的 URL 中的網域名稱符合任一所指定的網域名稱，則會從該伺服器定義擷取要求的配置設定。
login_method	指出此網域的登入方法。登入方法可以與特定的裝置設定檔（僅 WebSphere EveryPlace Suite）關聯。若未指定任何裝置，則所有裝置使用相同的登入方法。預設值是 basic。 登入方法： • nome - 使用者沒必要登入。 • basic - 使用者使用基本鑑定登入。 • forms - 使用者使用套表登入。 • certificate - 使用者使用用戶端憑證登入。 語法：*login method* [device profile list]
reverse_dns_lookup	若 URL 含有一 IP 位址或不完整網域名稱，此選項會告訴外掛程式去執行反向 DNS 查閱以判定完整網域名稱並根據展開的名稱作出授權決定。僅有在此檔案的 [Global] 區段，此選項才有效。預設值是 YES。
使用者資訊	

選項	說明
realm	在對使用者進行身份驗證之前指出要連接到每一個使用者 ID 的領域。例如，如果領域是 bank_a，則使用者 joe 會被鑑定爲 joe@bank_a。因爲 Tivoli Access Manager 對所有的使用者 ID 使用單一名稱空間，所以在 Tivoli Access Manager 中必須建立使用者 ID 以及連接到他們的領域。這麼做，屬於不同網域的相同的使用者 ID 可以在 Tivoli Access Manager 的使用者登錄（例如：joe@bank_a, joe@bank_b）中同時存在。
錯誤頁	
require_ssl_errorfile	若網域需要 SSL 連線，而建立的連線不是 SSL，則此錯誤會傳回給使用者。
require_cert_errorfile	若網域需要憑證，而使用者的瀏覽器並沒有提供，則此錯誤會傳回給使用者。
套表登入	
form_login_file	指出用來鑑定的套表登入檔案。此檔案可以本端環境的方式存在，或以 URL 中所指定的遠端檔的方式存在。若未指定此選項，則不會對此網域使用套表登入。套表登入可以與特定的裝置設定檔關聯。若未指定任何裝置，則所有裝置使用相同的套表。 語法：*local path* | *URL* [device profile list]
form_login_errorfile	指示當使用者之套表鑑定失敗時，要發送套表錯誤檔案。此檔可與登入檔案相同，含有指出使用者登入失敗的異常錯誤訊息。 語法：*local path* | *URL* [device profile list]
form_logout_file	指示當使用者送出登出 URL 時，要發送套表登出檔案。此檔可含告知使用者階段作業已經結束的訊息。若未經指定，要求傳送到後端伺服器。 語法：*local path* | *URL* [device profile list]
form_type	指出套表 MIME 內容類型，指定套表檔案的格式。無線裝置可能需要特殊類型。若未指定類型，就會採用 `text/html`。 語法：*type* [device profile list]
form_signature_login	套表簽名是套表中值指派的隱藏屬性。當套表被選作登入方法時，若外掛程式接收到包含此指派之套表送出，它會從套表中擷取使用者 ID 和密碼來驗證使用者身份。對套表登入使用此方法，即使該使用者之前並未試著存取受保護的網頁，外掛程式仍可對使用者進行身份驗證。若指定了此選項，套表中必可找到簽名，除非另外指定，否則不會檢查套表簽名。 語法：*name=value*

選項	說明
form_login_url	指出使用者在哪一個套表登入 URL 中送出鑑定套表。當套表被選作登入方法時，如果外掛程式收到一個套表送出作業，其符合此 URL，則它會從套表中擷取使用者 ID 和密碼來驗證使用者身份。請注意，配置套表登入簽名是另一種可供外掛程式偵測是否已送出登入套表的方法。如果既未配置 **form_login_url**，也未配置 **form_signature_login** 選項，則外掛程式會使用 cookie 來偵測是否已送出登入套表。 語法：*URL* [device profile list]
form_logout_url	指出由要登出的使用者所提出的套表登出 URL。外掛程式在使用者作出符合此 URL 的要求時，刪除使用者的階段作業資訊。 語法：*URL* [device profile list]
form_login_url_recovery	指出當使用者使用套表登入 URL 來進行鑑定時，外掛程式是否要在鑑定後，將瀏覽器重新導向到原始 URL。預設值是 `YES`。
form_session_size	指出使用套表登入可同步登入的最大使用者數。僅有在此檔案的 [Global] 區段，此選項才有效。預設值是 `10000` 個使用者。
form_session_timeout	指出在使用套表登入時，使用者可以保持閒置而不送出要求的時間長度。在此逾時期間後，使用者必須再登入一次。預設值是 `20` 分鐘。
form_ssl_security	指出用來保全套表登入的安全性類型。當套表登入用在安全性的連線上時，使用者 ID 和密碼會儲存在本端環境並伴隨著一個安全的階段作業 ID。預設值是 `cookie_sessionId`。 套表登入安全性選項： • `ssl_sessionId` - SSL 階段作業 ID 與 使用者 ID 和密碼相關聯。 • `cookie_sessionId` - 一暫時無法譯解的值，儲存在階段作業 cookie 中，與使用者 ID 和密碼關聯。
form_client_validation	指出使用者的 IP 位址在使用者使用套表登入來進行身份驗證時，是否被允許變更。 若已啓用，在套表登入階段作業的期間就會驗證使用者的 IP 位址。預設值是 `YES`。
form_fieldname_userid	指出 POST 作業所送出的使用者 ID 資料的欄位名稱。預設值是 `UserID`。
form_fieldname_password	指出 POST 作業所送出的密碼資料的欄位名稱。此設定值套用到登入和變更密碼套表兩者。 預設值是 `Password`。
form_fieldname_newpassword	指出當使用者的密碼有變更時，POST 作業所送出的新密碼資料的欄位名稱。預設值是 `NewPassword`。

選項	說明
form_fieldname_verifynewpassword	指出當使用者的密碼有變更時，POST 作業所送出的新密碼驗證資料的欄位名稱。預設值是 VerifyNewPassword。
form_fieldname_requestdata	指出鑑定套表中儲存要求資訊的隱藏欄位名稱。當送出套表進行鑑定時，外掛程式會從這個欄位擷取要求資訊。預設值是 RequestData。
form_fieldvalue_requestdata	指出鑑定套表中外掛程式將以要求資訊取代的隱藏欄位值。當鑑定套表傳回給使用者時，外掛程式會將此值換成要求資訊。預設值是 INSERT.REQUEST.DATA.HERE。
form_fieldname_postdata	指出儲存了已儲存 POST 資料的內容之鑑定套表中隱藏欄位名稱。當套表已送出待鑑定時，外掛程式會從此欄位擷取已儲存的 POST 資料。預設值是 PostCacheData。
form_fieldvalue_postdata	指出鑑定套表中的隱藏欄位值（外掛程式會以 POST 資料取代之）。當鑑定套表傳回給送出 POST 要求的使用者時，外掛程式以送出的 POST 資料取代此值。預設值是 INSERT.POST.DATA.HERE。
form_fieldvalue_url	指出鑑定套表中外掛程式將以 URL 取代的隱藏欄位值。預設值是 INSERT.URL.HERE。
form_fieldvalue_secure_url	指出鑑定套表中外掛程式將以安全 URL 取代的隱藏欄位值。預設值是 INSERT.SECURE.URL.HERE。
form_fieldvalue_method	指出鑑定套表中外掛程式將以方法取代的隱藏欄位值。預設值是 INSERT.METHOD.HERE。
變更密碼	
form_chgpasswd_file	指出當登入方法是基本或套表時，傳送到使用者以變更到期密碼的套表。當使用者的密碼到期時，此套表會傳送給使用者來變更到期的密碼。若未指定此選項，就不會執行任何密碼到期檢查。 語法：*local path* | *URL*
form_chgpasswd_generic_errorfile	指出傳送給使用者的錯誤檔案，該檔案指明當使用者的密碼被變更時發生的一般錯誤。 語法：*local path* | *URL*
form_chgpasswd_oldpasswd_errorfile	指出傳送給使用者的錯誤檔案，該檔案指明舊密碼密碼是錯誤的。 語法：*local path* | *URL*
form_chgpasswd_newpasswd_errorfile	指出傳送給使用者的錯誤檔案，該檔案指明新密碼未通過密碼原則驗證檢查。 語法：*local path* | *URL*

選項	說明
form_chgpasswd_verifypasswd_errorfile	指出傳送給使用者的錯誤檔案，該檔案指明新密碼並未經過使用者正確驗證。 語法：*local path* | *URL*
form_signature_chgpasswd	指出用來偵測是否已送出變更密碼套表的套表簽名。如果外掛程式收到一個套表送出作業，其中包括這個簽名，它會從套表中擷取使用者資訊來變更使用者的密碼。
form_chgpasswd_submit_url	指出密碼變更要求送達處的 URL。當密碼變更要求送出到此 URL，外掛程式會以送出的資訊來更新使用者的密碼。在外掛程式變更使用者的密碼之前，使用者必須已經過鑑定。請注意，配置套表變更密碼簽名是另一種可供外掛程式偵測是否已送出變更密碼套表的方法。僅對 Tivoli Access Manager 使用者登錄支援此功能。 語法：*URL* [device profile list]
form_chgpasswd_response_url	指出當成功變更密碼時，傳送到使用者的回應 URL。此頁面告訴使用者密碼已成功變更。預設值是/。 語法：*URL*
form_chgpasswd_url_recovery	指出在使用者變更了到期的密碼之後，外掛程式是否要將瀏覽器重新導向到原始 URL，而不是將瀏覽器重新導向到回應 URL。預設值是 YES。
安全性	
cookie_security_enabled	指出在安全的連線上建立的 cookies 是否被允許略過不安全的連線。若已啓用，安全的 cookies 不會被允許略過不安全的連線。預設值是 YES。
require_ssl	指出存取此網域是否須要安全的連線。若安全的連線是必要的，瀏覽器會自動重新導向到安全站台。
單一登入	
accept_sso	指出要爲此網域接受的單一登入記號。若使用者已經過鑑定，外掛程式可以略過鑑定。外掛程式搜尋此清單直到它找到單一登入記號。請參閱 SSO 區段以取得更多關於單一登入的資訊。
submit_sso	指出要爲此網域送出的單一登入記號。外掛程式可以送出已經過鑑定的使用者的資訊到後端伺服器。外掛程式送出清單中的每一個單一登入記號到後端伺服器。請參閱 SSO 區段以取得更多關於單一登入的資訊。
遞送	

選項	說明
route	指出反向 Proxy 配置中的要求所要轉遞到的目標伺服器。在此配置中，DNS 會被配置來對映多個網域名稱到外掛程式。遞送選項告訴外掛程式將要求遞送到對應的內容 Web 伺服器。若此配置中並未指定任何遞送選項，快取 Proxy 會使用其配置的對映規則來遞送要求。 語法：*URL* [default page]
Proxy	指出所有要求都經由其代理的 HTTP Proxy 伺服器的 URL。例如，transcoder Proxy 伺服器可以用來將 HTML 檔案轉換爲裝置相容的檔案。僅當遞送要求時，此選項才適用。 語法：*URL*
快取	
user_cache_size	指出鑑定過的使用者的快取表格中所儲存的最大使用者數。當驗證使用者身份成功時，使用者的證明會儲存在此快取中。對相同的使用者的後續的要求，會從此快取擷取使用者證明。在此時間過去後，會對使用者登錄驗證使用者的證明。僅有在此檔案的 [Global] 區段，此選項才有效。預設值是 `20000`。啓用 WES 支援時，請於 **ibmwesas.conf** 設定 `MaxSessionCache` 參數。
user_cache_timeout	指出鑑定過的使用者儲存在快取中的最長時間。在指定的時間後，會對使用者登錄驗證使用者的快取證明。若驗證失敗，使用者必須再登入一次。預設值是 `10` 分鐘。啓用 WES 支援時，請於 **ibmwesas.conf** 設定 `MaxSessionAge` 參數。
記載	
logging_flags	指出外掛程式傳送給事件日誌檔的記載訊息種類。僅符合指定的種類的訊息會傳送給日誌檔。僅有在此檔案的 [Global] 區段，此選項才有效。預設值是 `EWI`。 日誌訊息旗標選項： • `E` - 錯誤訊息 • `W` - 警告訊息 • `I` - 參考訊息 • `D` - 除錯訊息
logging_level	指出參考和除錯日誌訊息的冗長層次。此值範圍可從 0 到 5。較高的數字表示記載了較多的訊息。僅有在此檔案的 [Global] 區段，此選項才有效。預設值是 `3`。
CDAS 支援	
cdas_loaded	指出 CDAS 模組是否已載入和已起始設定。僅有在此檔案的 [Global] 區段，此選項才有效。預設值是 `YES`。

選項	說明
cdas_init_parameter	指出傳至 CDAS 模組的起始設定參數。若定義了多重項目則會多次呼叫 CDAS 起始設定函數。僅有在此檔案的 [Global] 區段，此選項才有效。
cdas_enabled	指出當登入方法是基本、套表、或憑證時，是否會呼叫 CDAS 模組。使用此選項，可對某些 URL 啓用 CDAS，對其他的停用。注意，不需對單一登入支援啓用 CDAS。預設值是 YES。
cdas_tagvalue_enabled	指出當使用 Tivoli Access Manager 使用者登錄進行鑑定時，是否僅呼叫 CDAS 模組，來新增延伸屬性到使用者的證明。使用這個選項，外掛程式會執行鑑定，但呼叫 CDAS 模組來新增延伸的使用者屬性。預設值是 YES。
cdas_auth_parameter	指出傳送至 CDAS 模組的關聯參數（對符合配置檔中伺服器定義的所有要求）。使用此選項，CDAS 模組可以根據此參數選擇鑑定方法。沒有預設值。
cdas_sso_headers	指出是否會爲從 CDAS 鑑定模組所傳回的每一個延伸屬性產生 HTTP 標頭。若已啓用，則會爲有此格式 tagvalue_*name* 的名稱之延伸屬性清單中的每一個名稱/值配對項目產生 HTTP 標頭。產生的 HTTP 標頭會根據 **tagvalue_creds_headers** 選項的設定來加以格式化。預設值是 YES。
cdas_sso_mapping	指出是否送出對應 Tivoli Access Manager 使用者 ID 到後端伺服器，進行單一登入。如果停用，則會爲單一登入送出原始 CDAS 使用者 ID。預設值是 YES。
標籤值	
tagvalue_creds_registry	指出在鑑定後新增至使用者證明的 LDAP 屬性。這個設定可能有多個實例。如果未指定，沒有 LDAP 屬性會新增至使用者的證明。 語法：*credential attribute name:ldap attribute name*
tagvalue_creds_headers	指出將新增至預定供後端伺服器使用之 HTTP 標頭的標籤值證明屬性。這個設定可能有多個實例。如果指定了特殊字元 *，將使用證明屬性名稱作爲 HTTP 標頭名稱，把所有標籤值證明屬性新增至 HTTP 標頭。請注意，這個設定也適用於 CDAS 延伸屬性。 語法：*credential attribute name:HTTP header name*

單一登入定義

如果使用者已經通過鑑定，外掛程式可以略過鑑定步驟。外掛程式也可傳送單一登入資訊到 Web 伺服器以作爲 HTTP 標頭或 cookie。外掛程式僅可接受來自受信任的鑑定伺服器之預先鑑定的使用者。

下列單一登入定義是預先定義的，可用作 **accept_sso** 和 **submit_sso** 的參數：

- **CDAS-MODULE**: CDAS 模組單一登入（僅 SSO 接受）
- **LTPA-COOKIE**: WebSphere LTPA Cookie
- **WEBSEAL-COOKIE**: WebSEAL 的失效接替 Cookie

選項	說明
type	指出單一登入類型： • `cookie` - Cookie 標頭 • `header` - HTTP 標頭 • `auth_header` - 授權標頭（僅 SSO 送出） • `IP_address` - IP 位址（僅 SSO 接受）
name	指出 cookie 的名稱或包含使用者的 SSO 資訊的 HTTP 標頭。此選項是預設爲 auth_header 的 SSO 類型的 授權，且不適合 IP_address 的 SSO 類型。
format	指出 cookie 或標頭值的格式。下列列出的巨集可用來指定使用者 ID 在標頭或 cookie 中的位置。此選項不適用於 IP_address 的 SSO 類型。 下列預設巨集可用來格式化單一登入資訊： • `<userid>` - 使用者的 ID • `<userdn>` - 使用者的 Tivoli Access Manager 識別名稱 • `<pd_cred>` - 使用者的 Tivoli Access Manager EPAC 證明（僅 SSO 送出） • `<opaque>` - 外掛程式無法辨識的資料（僅 SSO 接受）
sso_realm	在使用者 ID 對映到 Tivoli Access Manager 識別名稱前，使用單一登入定義，指出連接到預先鑑定的使用者 ID 的領域。此領域的目的是從此預先鑑定的伺服器，爲所有使用者 ID 專屬識別對映規則。請參閱使用者對映檔案以獲取更多資訊。當送出了 SSO 資訊後，此選項不適用。
default_user	指出預設 Tivoli Access Manager 使用者（其證明被用來授權給已使用此單一登入定義來鑑定的使用者）。若找不到預先鑑定過的使用者 ID 的對映項目，則此使用者的證明會用來執行授權。如果找不到預先鑑定過的使用者 ID 的對映項目，且未指定此選項，則外掛程式會引導 Tivoli Access Manager 查閱登錄中的使用者 ID。當送出了 SSO 資訊後，此選項不適用。

選項	說明
trust_basis	指出外掛程式可以信任預先鑑定的伺服器的基準。只有在外掛程式信任預先鑑定的伺服器時，外掛程式才接受預先鑑定的使用者。預設值是 IP_address。當送出了 SSO 資訊後，此選項不適用。 信任基準選項： • IP_address - 預先鑑定的伺服器的 IP 位址必須符合 trust_list 設定值中的項目。若沒有爲 trust_list 指定 IP 位址，則不會接受任何預先鑑定的使用者（使用此單一登入定義）。 • basic_auth - 預先鑑定的伺服器必須使用「授權」標頭來進行身份驗證。送出的使用者 ID 和密碼必須符合 trust_list 設定值中的項目。 • Proxy_auth - 預先鑑定的伺服器必須使用「Proxy 授權」標頭來進行身份驗證。送出的使用者 ID 和密碼必須符合 trust_list 設定值中的項目。 • certificate - 預先鑑定的伺服器必須使用用戶端憑證來進行身份驗證。憑證 DN 必須符合 trust_list 設定中的項目。
trust_list	指出可由預先鑑定的伺服器展示給外掛程式之可接受的識別的清單。當送出了 SSO 資訊後，此選項不適用。

附錄 C. wesosm 指令參照

本附錄列出與 **wesosm** 公用程式有關的指令。

指令語法

本附錄中的指令使用下列特殊字元來定義指令語法：

[ ] 識別選用的元素。方括弧（[ ]）外的那些是必要的。

... 指出您可以爲前一個元素指定多個值。除非指令資訊另有指示，否則是以空格來分隔多個值。

若元素的省略符號接著右方括弧，請使用方括弧中的語法來指定多個值。例如，爲選項 [**–a** *admin*]...指定兩個管理者，請使用 **–a admin1 –a admin2**。

若元素的省略符號在方括弧中，請使用最後一個元素的語法來指定多個值。例如，若要指定兩個主機於 [**–h** *host...*]，請使用 **–h host1 host2**。

| 指出互斥的資訊。您可以使用位於垂直的條欄左邊或右邊上的元素。

{ } 限定一組互斥的元素（如果這些元素其中之一是必要時）。若元素是選用的，他們會被置於括弧 ([ ]) 中。

除了特殊字元外，會使用第 xi 頁的『字體使用慣例』中所說明的字體使用慣例。

wesosm

目的

建立和維護 Edge Server 外掛程式的 Tivoli Access Manager 物件空間

語法

wesosm {**–start** | **–stop** | **–run** | **–file** [*output_file*]}

[**–infile** *input_file*] [**–logging** [*log_file*] [**-clean**]

[**–force** [*branch*]] [**–fast**] [**–skiperrors**] [**–verbose**]

選項

–clean 從 /ESProxy（在配置檔 osdef.conf 中找不到）底下的物件空間移除所有項目。請小心使用此選項，因爲在刪除物件空間時，任何連接的 ACL 都會不見。

–fast 當檢查 Tivoli Access Manager 物件空間和 Web 伺服器的檔案系統間的差異時，此參數會告訴公用程式僅去比較物件名稱而不要比較類型。Tivoli Access Manager 物件類型會指出物件空間項目是檔案或目錄。例如，若在 Web 伺服器上的現有檔案變更目錄但名稱仍相同時，公用程式不會偵測到此現象（當指定了此參數時）。

–file 啓動物件空間管理程來更新物件空間一次，然後終止公用程式。不是更新 Tivoli Access Manager 物件空間，而是將物件空間資訊寫入指定的檔案。

–force 當以 daemon 啓動物件空間管理程式，強迫公用程式起始更新物件空間（在等候下次更新之間隔時）。若有指定，僅物件空間中指出的分支會被更新。萬用字元可用來指定分支。

–infile 指出配置檔 osdef.conf（用來更新物件空間）的位置。

–logging 指出物件空間管理程式是否應將物件空間記載到日誌檔。若沒有指定日誌檔，就會使用預設的日誌檔 wesosm.log。

–run 啓動物件空間管理程來更新物件空間一次，然後終止公用程式。

–skiperrors 當更新物件空間時，如果在更新 Tivoli Access Manager 物件空間時碰到錯誤，公用程式不會中斷。若物件空間含有錯誤項目，這就很有用。

–start 以 daemon 啓動物件空間管理程式。daemon 將自身安裝在記憶體中以 osdef.conf 配置檔中所配置的間隔，更新物件空間。這可確保物件空間與對應的 Web 伺服器上的內容是同步化的。

–stop 停止物件空間管理程式 daemon。此 daemon 會將它自身從記憶體中移除並停止對物件空間執行進一步更新。

–verbose 在更新物件空間時，顯示關於確切的項目（在物件空間中建立、刪除和修改的項目）的資訊。

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。要知道在您所在地區是否可用到這些產品與服務時，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, 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 Web 站上的資料，並非本 IBM 產品所用資料的一部分，因使用該 Web 站造成之損害，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」、「國際程式授權合約」或任何同等合約之條款，提供本文件中所述之授權程式與其所有適用的授權資料。

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。

著作權授權：

本資訊包含原始語言的範例應用程式，用以說明各種作業平台上的程式設計技術。 貴客戶得爲開發、使用、銷售或散佈運用樣本程式之作業平台的應用程式程式介面所撰寫的應用程式之目的，免費複製、修改並散佈這些樣本程式。此些範例並未在所有情況下完整測試。故 IBM 不保證或默示保證此些程式之可靠性、服務性或功能。您可以基於研發、使用、銷售或散佈符合 IBM 應用程式介面之應用程式等目的，以任何形式複製、修改及散佈這些範例程式，而不必向 IBM 付費。

每份複本或任何這些範例程式的部份或任何衍生工作，例如下列的版權聲明：

©（ 貴公司名稱）（年份）。本程式碼之一部份係衍生自「IBM Corp. 樣本程式」。© Copyright IBM Corp. _輸入年份_. All rights reserved.

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 logo
OS/390
SecureWay
Tivoli
Tivoli logo
Universal Database
WebSphere
zSeries
z/OS

Java 和所有以 Java 爲基礎的商標和標誌是 Sun Microsystems, Inc. 在美國和/或其他國家或地區的商標或註冊商標。

Microsoft 和 Windows 是 Microsoft Corporation 在美國和/或其他國家或地區的商標。
Java 及所有以 Java 爲基礎的商標與標誌是 Sun Microsystems, Inc. 在美國及/或其他國家或地區的商標或註冊商標。

UNIX 是 The Open Group 在美國及其他國家或地區的註冊商標。

其他公司、產品或服務名稱，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。

I

O

P

T

U

W

X

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 Plug-in for Edge Server
使用手冊
第 4.1 版

SC40-1168-00

折疊線

台北市 110 基隆路一段 206 號

大臺灣國際商業機器股份有限公司
中華研發中心
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

SC40-1168-00