IBM Tivoli Access Manager
for WebLogic Server

使用手冊

第 4.1 版

SC32-1137-00

IBM Tivoli Access Manager
for WebLogic Server

使用手冊

第 4.1 版

SC32-1137-00

附註

使用此資訊和它支援的產品前，請先閱讀第 43 頁的『注意事項』中的資訊。

第二版 (October 2002)

此版本取代 SC32-0831-00

目錄

前言

歡迎使用 IBM® Tivoli® Access Manager for WebLogic Server （之後稱爲 Tivoli Access Manager for WebLogic）。此項產品擴充了 IBM Tivoli Access Manager，以支援針對 BEA WebLogic Server 撰寫的應用程式。

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 軟體與說明文件的使用者而言，*管理伺服器*現稱爲*原則伺服器*。

*IBM Tivoli Access Manager for WebLogic Server 使用手冊*提供安裝、配置及管理指示，來搭配使用 IBM Tivoli Access Manager 與 WebLogic Server。

本書適用對象

本管理手冊的適用對象爲：

- 安全管理者
- 網路系統管理者
- IT 設計者

讀者應該熟悉：

- 網際網路通訊協定，包括 HTTP、TCP/IP、檔案轉送通訊協定 (FTP) 和 Telnet
- 部署及管理 WebLogic Server 系統
- 安全管理，包括鑑定與授權

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

本文件包含下列章節：

- 第 1 章「簡介及概觀」

  呈現 Tivoli Access Manager for WebLogic 提供的鑑定及授權服務程式的概觀。
- 第 2 章「安裝指示」

  說明如何安裝 Tivoli Access Manager for WebLogic。
- 第 3 章「配置程序」

  說明如何配置 Tivoli Access Manager for WebLogic。
- 第 4 章「管理作業」

說明如何使用示範應用程式，以及提供用法要訣、疑難排解資訊和限制。

- 第 5 章「移除指示」

  說明如何移除 Tivoli Access Manager for WebLogic。

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』
- 『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*
  GI11-4198-00 (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*
  SC32-1133-00 (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 使用手冊*
  SC32-1136-00 (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*
  SC32-1137-00 (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

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 簡介及概觀

IBM Tivoli Access Manager for WebLogic Server（之後稱爲 Tivoli Access Manager for WebLogic）是 IBM Tivoli Access Manager for e-business (Tivoli Access Manager) 的延伸，用以實作 BEA WebLogic Server 的「自訂領域」。「自訂領域」提供一個由 Tivoli Access Manager 管理的使用者登錄。使用者密碼可以加以鑑定以放至 Tivoli Access Manager 使用者登錄，而使用者登錄中的群組成員資格可用來影響 WebLogic Server 所做出的授權決策。「自訂領域」也可與 IBM Tivoli Access Manager WebSEAL (WebSEAL) 一起用來支援一般使用者單一登入。

Tivoli Access Manager for WebLogic 可讓 WebLogic Server 應用程式使用 Tivoli Access Manager 安全性，不需要任何編碼或部署變更。

Tivoli Access Manager for WebLogic 會實作一個使用 Tivoli Access Manager 安全網域提供之安全服務的「自訂領域」。在安裝 Tivoli Access Manager for WebLogic 前，必須先部署安全網域。

在部署安全網域之前，Tivoli Access Manager 的初學者應該檢閱 Tivoli Access Manager 安全模型。這裡會呈現安全模型的簡短摘要。

Tivoli Access Manager 安全模型

Tivoli Access Manager 是一個完整的授權與網路安全原則管理解決方案，可爲遍布各地的企業內部網路和企業外部網路資源提供端對端保護。

Tivoli Access Manager 配有最先進的安全原則管理。此外，它還可支援鑑定、授權、資料安全和資源管理等功能。您可以將 Tivoli Access Manager 和標準的網際網路型應用程式一起使用，以建置高度安全與管理妥善的企業內部網路及外部網路。

Tivoli Access Manager 的核心可提供下列功能：

- 鑑定架構

  Tivoli Access Manager 支援廣泛的鑑定機制。
- 授權架構

  Tivoli Access Manager 提供授權原則管理的架構。授權原則是集中管理、自動配送，以存取企業各處的實施點，包括 Tivoli Access Manager。Tivoli Access Manager 授權服務程式對本機 Tivoli Access Manager 伺服器及協力廠商應用程式的存取要求，提供*允許*及*拒絕*決策。

WebSEAL 是用於 Web 型資源的 Tivoli Access Manager 資源安全管理程式。WebSEAL 是一個高效能、多重執行緒的 Web 伺服器，用以將定義精細的安全性套用至受保護的 Web 資源。WebSEAL 可提供單一登入解決方案，將後端 Web 應用程式伺服器資源納入其安全原則內。

Tivoli Access Manager 產品入門說明文件

您可以藉由檢閱 IBM Tivoli Access Manager 的說明文件，來學到更多有關 Tivoli Access Manager 的資訊，包括做出部署決策所需的資訊。請從下列手冊開始：

- *IBM Tivoli Access Manager Base 安裝手冊*

  本手冊說明如何規劃、安裝及配置 Tivoli Access Manager 安全網域。一系列簡易的安裝 Script 可讓您迅速地部署完整功能的安全網域。當製作安全網域原型，來符合您的安全原則需求時，這些 Script 很有用。

- *IBM Tivoli Access Manager Base Administrator's Guide*

  本文件提供管理受保護的資源之 Tivoli Access Manager 安全模型概觀。本手冊也說明如何配置 Tivoli Access Manager 伺服器來做出存取控制決策。此外，詳細的指示說明如何執行重要的作業，如宣告安全原則、定義受保護的物件名稱空間，以及管理使用者及群組設定檔。

- *IBM Tivoli Access Manager WebSEAL Administrator's Guide*

  本手冊提供一組完備的程序和參考資訊，可用來管理您安全 Web 網域中的資源。 本手冊也呈現概觀及概念資料，以說明廣泛的 WebSEAL 功能。

- *IBM Tivoli Access Manager Authorization C API Developer's Reference*

  本手冊說明如何使用 Tivoli Access Manager 授權 API，將安全性新增至協力廠商應用程式。本文件包括 **svrsslcfg** 公用程式的說明。這個公用程式是在配置 Tivoli Access Manager for WebLogic 期間使用的。

IBM Tivoli Access Manager 說明文件可從「IBM Tivoli 客戶支援中心」網站取得。請參閱第 vi 頁的『IBM Tivoli Access Manager』。

整合 Tivoli Access Manager 及 WebLogic Server

Tivoli Access Manager for WebLogic 第 4.1 版支援下列版次的「自訂領域」：

- WebLogic Server 6.1
- WebLogic Server 7.0（僅在相容性模式中執行）

  相容性模式安全性是用來在 WebLogic Server 7.0 內執行 WebLogic Server 6 安全配置。

  請注意，Tivoli Access Manager for WebLogic 的這個版次不支援 WebLogic Server 7.0 新增的「安全服務提供者介面」。

Tivoli Access Manager 提供 WebLogic Server 的下列整合點：

- 集中式存取控制。
  - Tivoli Access Manager Policy Server 與 WebLogic Server 會共用集中式使用者登錄。 Tivoli Access Manager 產品配送包括 IBM Directory。「Tivoli Access Manager 自訂領域」容許這個登錄，以及 Tivoli Access Manager 支援的其他協力廠商登錄，作爲 WebLogic 登錄。
  - 變更使用者的 Tivoli Access Manager 群組成員資格時，會依照每一個 WebLogic Server 應用程式的部署描述子中含有的群組至角色對映，來改變該使用者對 WebLogic 的 Java™ 2 Enterprise Edition (J2EE) 資源的存取許可權。
  - WebSEAL 會控制對應於 Tivoli Access Manager 原則資料庫中物件的「制式資源定位器 (URL)」的存取權限。這些物件可以是靜態 URL 字串，或可以用型樣相符來代表。
- 整合式授權

WebLogic Server 達成整合式授權的方法爲使用「Tivoli Access Manager 自訂領域」，來判定哪些使用者屬於已對映至 J2EE 應用程式之安全角色的群組。這表示 Tivoli Access Manager 管理者可以透過 Tivoli Access Manager 登錄內的群組成員資格，影響 WebLogic Server 的授權決策。

- 透過使用 WebSEAL 進行單一登入

  達成單一登入的做法爲將 WebSEAL 的一次使用者鑑定與「Tivoli Access Manager 自訂領域」的使用者身份驗證結合一起。

  如此將容許使用許多鑑定機制，包括憑證，而不會影響目標應用程式。

  WebLogic 伺服器信任 WebSEAL 是透過結合 WebSEAL *接合*及使用「Tivoli Access Manager 自訂領域」來達成的。「接合」是 WebSEAL 伺服器與應用程式伺服器之間的網路連線，以便：

  1. WebSEAL 與應用程式伺服器之間能相互信任。
  2. WebSEAL 會同時保護自己的資源，以及已接合之應用程式伺服器上的資源。

使用 Tivoli Access Manager 鑑定

Tivoli Access Manager 可以用來提供對外部使用者或內部使用者的鑑定。外部使用者的鑑定會使用 WebSEAL 單一登入。如需取得最佳的網路安全性，每一個透過 WebSEAL 從外部使用者接收存取要求的 WebLogic Server 不應該接受來自內部使用者的存取要求。下列幾節將說明如何處理外部及內部使用者的鑑定。

鑑定外部使用者

下圖顯示如何處理來自外部使用者，用以存取受保護資源之要求的模型。

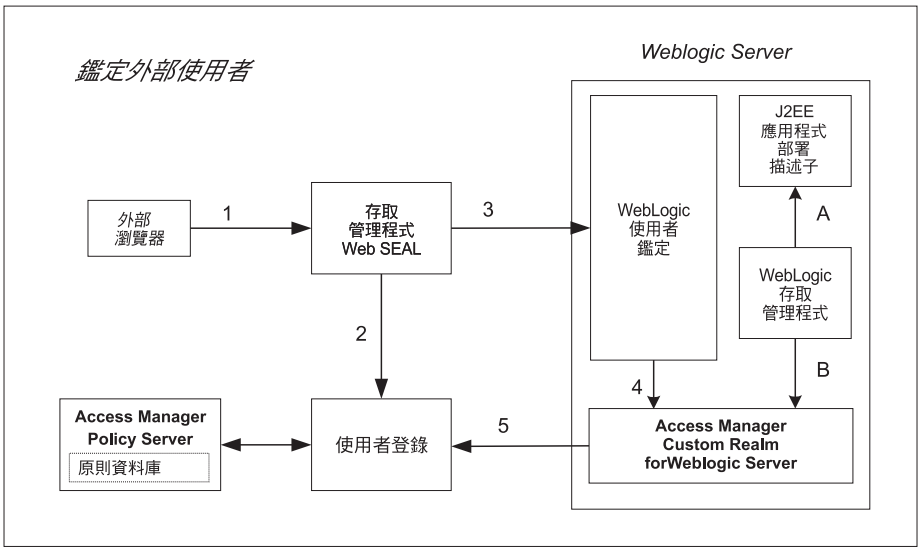

圖 1. Tivoli Access Manager 提供外部使用者的單一登入鑑定

1. 外部使用者要求存取受保護的資源。在進入企業的安全網路之前， WebSEAL 會先收到這個要求。（請看圖 1 中的箭頭 ***1***）
2. WebSEAL 會在 Tivoli Access Manager 安全網域中鑑定使用者。（請看圖 1 中的箭頭 ***2***）

   WebSEAL 支援下列鑑定方法：使用者名稱及密碼、憑證、使用者名稱及 RSA SecureID，或自訂的鑑定機制。

WebSEAL 根據所要求的 URL 及 Tivoli Access Manager 存取原則，來套用它自己的授權決策。WebSEAL 可以套用如帳戶有效性、日期時間，以及鑑定機制等注意事項。

3. 當使用者的要求獲得授權時，WebSEAL 就會將要求轉遞至 WebLogic 伺服器。要求包括基本鑑定標頭內的外部使用者名稱及特殊密碼。特殊密碼屬於 *configured_user*，而且容許「Tivoli Access Manager 自訂領域」確認 WebSEAL，作爲要求的原點。（請看圖 1 中的箭頭 ***3***）

   如需 *configured_user* 的相關資訊，請參閱第 19 頁的第 3 章, 『配置程序』。

4. WebLogic 伺服器會以透通方式將已鑑定的使用者身份及密碼傳至「Tivoli Access Manager 自訂領域」。（請看圖 1 中的箭頭 ***4***）
5. 「Tivoli Access Manager 自訂領域」會使用 Tivoli Access Manager 鑑定服務，來驗證 WebSEAL 所提供的密碼對上面說明的 *configured_user* 是否正確。亦即，這個密碼提供信任基礎，指出要求的原點是 WebSEAL。（請看圖 1 中的箭頭 ***5***）

現在已準備好授權要求。

鑑定內部使用者

下圖顯示如何處理由未通過 WebSEAL 接合的*內部*使用者提出，用以存取受保護資源之要求的模型。

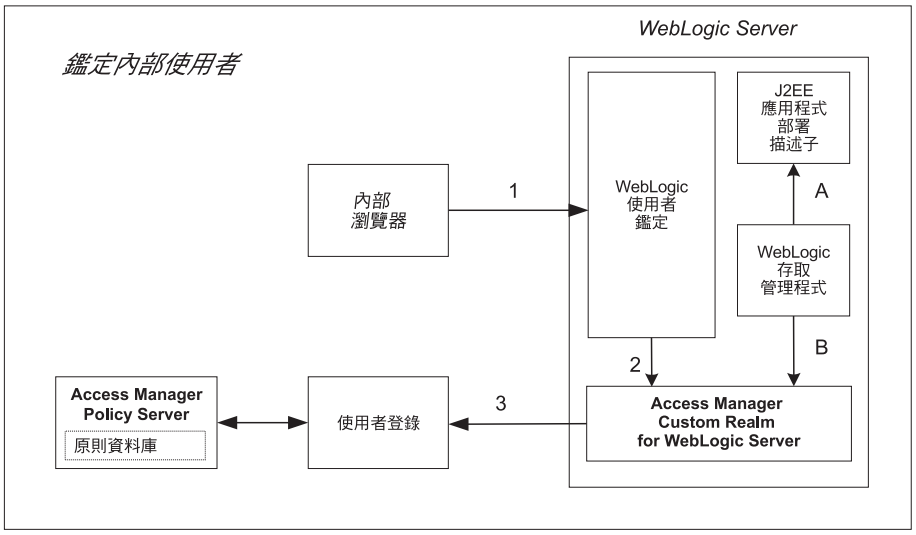

圖 2. 「Tivoli Access Manager 自訂領域」提供內部使用者的鑑定

1. 內部使用者會傳送存取受保護資源的要求。（請看圖 2 中的箭頭 ***1***）
2. WebLogic 使用者鑑定模組會傳送使用者身份至「Tivoli Access Manager 自訂領域」。（請看圖 2 中的箭頭 ***2***）
3. 「Tivoli Access Manager 自訂領域」會傳送鑑定要求至使用者登錄。（請看圖 2 中的箭頭 ***3***）

   如果鑑定成功，「Tivoli Access Manager 自訂領域」會傳回使用者名稱給 WebLogic Server，作爲已鑑定的使用者。

現在已準備好授權要求。

使用 Tivoli Access Manager 授權

授權處理程序發生方式如下：

1. 當 WebLogic Server 收到 J2EE 資源的要求時，它會檢查相關部署描述子資訊，以判定是否要限制某些角色才能存取資源。（請看圖 1 或圖 2 中的箭頭 ***A***）
2. 如果要求需要使用者假設一個角色，則 WebLogic Server 會查詢「Tivoli Access Manager 自訂領域」，來判定要求使用者是否爲已對映至角色的任一群組的成員。（請看圖 1 或圖 2 中的箭頭 ***B***）
3. 「Tivoli Access Manager 自訂領域」會查閱 Tivoli Access Manager Authorization Server，以判定現行使用者是否爲群組的成員。如果使用者是已對映至允許的角色之群組的成員，將授與存取權限。不然，將拒絕存取。（請看圖 1 中的箭頭 ***5***，或圖 2 中的箭頭 **3**）

第 2 章 安裝指示

本章含有下列主題：

支援的平台

Tivoli Access Manager for WebLogic 第 4.1 版支援下列版次的「自訂領域」：

- WebLogic Server 6.1
- WebLogic Server 7.0（僅在相容性模式中執行）。

  相容性模式安全性是用來在 WebLogic Server 7.0 內執行 WebLogic Server 6 安全配置。

  請注意，Tivoli Access Manager for WebLogic 第 4.1 版不支援 WebLogic Server 7.0 新增的「安全服務提供者介面」。

下表中說明的作業系統版次支援 Tivoli Access Manager for WebLogic。請注意，Tivoli Access Manager 第 4.1 版支援的所有作業系統版次目前不支援 WebLogic Server 第 7.0 版。

亦請注意，BEA 會提供 WebLogic Server 適用的一些服務套件。在 BEA 支援的不同作業系統版次中，可能會有不同的服務套件層次。如果要判定每一個作業系統適用的服務套件，使用者應該參閱 BEA 平台認證表格：

`http://www.weblogic.com/platforms/index.html`

表 1. 支援的平台

Tivoli Access Manager for WebLogic 支援的平台	
作業系統版次	**BEA WebLogic Server 版次**
AIX 4.3.3AIX 5.1.0	WebLogic Server 6.1 附註：WebLogic Server 7.0 不支援 AIX 4.3.3 或 AIX 5.1.0。
Solaris Operating Environment 7	WebLogic Server 6.1 附註：WebLogic Server 7.0 不支援 Solaris Operating Environment 7。

表 1. 支援的平台 (繼續)

Solaris Operating Environment 8 HP-UX 11.0 HP-UX 11i Microsoft Windows 2000 Advanced Server（含 Service Pack 2） Microsoft Windows NT 4.0（含 Service Pack 6A） Red Hat Linux 7.2	WebLogic Server 6.1 WebLogic Server 7.0

磁碟和記憶體需求

Tivoli Access Manager for WebLogic 具有下列磁碟及記憶體需求：

- 64 MB RAM

  這是除了 WebLogic Server 及任何其他 Tivoli Access Manager 元件所指定的記憶體需求以外，還需要的記憶體數量。另外使用 64 MB RAM 來取得最佳的快取效能。

  其他 Tivoli Access Manager 元件所需的記憶體數量取決於已安裝在主機系統上的 Tivoli Access Manager 元件而定。如需相關資訊，請參閱 *IBM Tivoli Access Manager Base 安裝手冊*。
- 250 KB（千位元組）磁碟空間

  除了 WebLogic Server 所需的磁碟空間，以及任何其他 Tivoli Access Manager 元件所需的磁碟空間外，還需要這個磁碟空間。

必備軟體

如果要順利地安裝 Tivoli Access Manager for WebLogic，需要下列各節中所說明的先決要件：

- 『Tivoli Access Manager Policy Server』
- 第 9 頁的『Tivoli Access ManagerWebSEAL』
- 第 9 頁的『WebLogic Server』
- 第 9 頁的『Tivoli Access Manager runtime 元件』

Tivoli Access Manager Policy Server

在安裝 Tivoli Access Manager for WebLogic 之前，必須先建立 Tivoli Access Manager 安全網域。

Tivoli Access Manager 安全網域是於安裝 Tivoli Access Manager Policy Server 時建立。適用於您作業系統的 IBM Tivoli Access Manager Base CD 包含此原則伺服器。

通常，安裝 Tivoli Access Manager Policy Server 的系統不同於掌控 Tivoli Access Manager for WebLogic 的系統。

Tivoli Access ManagerWebSEAL

Tivoli Access Manager WebSEAL (WebSEAL) 提供 Tivoli Access Manager for WebLogic 可以使用的 Web 型安全服務。結合 WebSEAL 接合時，Tivoli Access Manager for WebLogic 可以用來提供 WebSEAL 進行 WebLogic Server 單一登入解決方案。

WebSEAL 是啓用 Tivoli Access Manager 單一登入解決方案的先決要件。它不是安裝 Tivoli Access Manager for WebLogic 的先決要件。通常，安裝 WebSEAL 的系統不同於掌控 Tivoli Access Manager for WebLogic 的系統。

如需完整 WebSEAL 安裝指示，請參閱*IBM Tivoli Access Manager WebSEAL 安裝指南*。

WebLogic Server

WebLogic Server 必須安裝並配置在將掌控 Tivoli Access Manager for WebLogic 的系統上。目前 WebLogic Server 在安裝時並不會安裝預設「自訂領域」，而且會使用 **startWebLogic** 指令來加以啓動。

WebLogic Server 是隨著必要的「Java 執行時期環境」一起配送。Tivoli Access Manager for WebLogic 會使用這個相同的「Java 執行時期環境」。如果要順利地安裝 WebLogic Server，必須滿足「Java 執行時期環境」的 Tivoli Access Manager for WebLogic 先決要件。

WebLogic Server 7.0 相容性模式需求

警告: 如果要搭配使用 WebLogic Server 7.0 與 Tivoli Access Manager for WebLogic，**在第一次啓動 WebLogic Server 時，您必須在***相容性模式***中啓動 WebLogic Server 7.0**。如果是在 7.0 模式中啓動 WebLogic Server 7.0，將不能於相容性模式中存取現有的網域。

當您*第一次*啓動 WebLogic Server 7.0 時，請確定遵循 WebLogic Server 說明文件中在相容性模式中啓動的步驟，來起始設定相容性安全。這將確定未來重新啓動 WebLogic Server 7.0 時，會自動在相容性模式中啓動。

AIX 上的 IBM Java Runtime Environment 第 1.3 版

在 AIX 系統上，WebLogic Server 需要 IBM Java Runtime Environment 第 1.3 版。WebLogic Server 會配送這個「Java 執行時期環境」，並在安裝 WebLogic Server 期間安裝它。 Tivoli Access Manager for WebLogic 會使用這個相同版本的「Java 執行時期環境」。

註: WebLogic Server 7.0 不支援 AIX。

Tivoli Access Manager for WebLogic 使用「Java 本機介面」程式碼。請確定已按照下列所述來配置 AIX 環境：

/BEA_installation_directory/jdk130/README.HTML

Tivoli Access Manager runtime 元件

下列執行時期元件來自 Tivoli Access Manager Base，必須安裝在掌控 Tivoli Access Manager for WebLogic 的系統上：

- Tivoli Access Manager runtime environment
- Tivoli Access Manager Java 執行時期環境

在將掌控 Tivoli Access Manager for WebLogic 的系統上配置這些元件之前，必須建立 Tivoli Access Manager 安全網域。

Tivoli Access Manager runtime environment 提供與 Tivoli Access Manager 安全網域的信任、安全通訊，以及提供對照網域使用者登錄來驗證使用者身份的能力。Tivoli Access Manager Java 執行時期環境提供 Java 型管理機能。這些 Java 類別會延伸 WebLogic Server 所使用的 Java 執行時期環境。

每一個支援的作業系統的 IBM Tivoli Access Manager Base CD 上都包括有 Tivoli Access Manager runtime environment 及 Tivoli Access Manager Java 執行時期環境。如需安裝指示，請參閱 *IBM Tivoli Access Manager Base 安裝手冊*。

Tivoli Access Manager 應用程式開發工具箱

Tivoli Access Manager 應用程式開發工具箱含有示範應用程式及範例授權 API 應用程式配置檔。您可以使用這個應用程式及配置檔，來測試是否已正確地配置了 Tivoli Access Manager 授權 API。

不過，請注意，Tivoli Access Manager for WebLogic 會提供一個稱爲 `PDRealm.conf` 的預設配置檔。您可以使用這個配置檔，來驗證授權 API 配置，而不是使用應用程式開發工具箱中提供的範例授權 API 配置檔。因此，安裝應用程式開發工具箱是*選用的*。

每一個支援的作業系統的 IBM Tivoli Access Manager Base CD 都包含此工具箱。如需安裝指示，請參閱 *IBM Tivoli Access Manager Base 安裝手冊*。

從前一版次升級

您可以從前一版次升級 Tivoli Access Manager for WebLogic。升級處理程序將取代產品檔案，但不會變更現有的自訂領域配置資料。

支援從下列版次升級至 Tivoli Access Manager for WebLogic 第 4.1 版：

- Tivoli Access Manager for WebLogic Server 第 3.9 版
- Tivoli Policy Director for WebLogic Server 第 3.8 版

BEA 支援從 WebLogic Server 第 6.1 版升級至 WebLogic Server 第 7.0 版。

本節說明下列升級實務：

- 『升級 Tivoli Access Manager for WebLogic』
- 第 12 頁的『僅升級 WebLogic Server』

升級 Tivoli Access Manager for WebLogic

本節說明下列升級：

表 2. 升級 Tivoli Access Manager for WebLogic

升級自：	升級至：
Tivoli Access Manager for WebLogic 第 3.9 版，含 WebLogic Server 第 6.1 版	Tivoli Access Manager for WebLogic 第 4.1 版，含 WebLogic Server 第 6.1 版
Policy Director for WebLogic Server 第 3.8 版，含 WebLogic Server 第 6.1 版	

表 2. 升級 Tivoli Access Manager for WebLogic (繼續)

Tivoli Access Manager for WebLogic 第 3.9 版，含 WebLogic Server 第 6.1 版	Tivoli Access Manager for WebLogic 第 4.1 版，含 WebLogic Server 第 7.0 版
Policy Director for WebLogic Server 第 3.8 版，含 WebLogic Server 第 6.1 版	

請完成下列步驟：

1. 停止 WebLogic Server。
2. 如果您不需要升級 WebLogic Server，請略過這個步驟。請跳至下一步驟。

   如果您需要將 WebLogic Server 從第 6.1 版升級至第 7.0 版，請立即執行此步驟。請遵循第 12 頁的『僅升級 WebLogic Server』中的指示。
3. 如果 **svrsslcfg** 產生的 Tivoli Access Manager for WebLogic Authorization Server 檔案位於 Tivoli Access Manager for WebLogic 安裝目錄，請製作它們的備份複本。這些檔案包括：
   - 配置檔 `PDRealm.conf`。
   - 金鑰檔（以 `.kdb` 結尾的檔名）
   - 隱藏檔（以 `.sth` 結尾的檔名）

   請注意，最初利用 **svrsslcfg** 進行配置期間，配置檔是由 **–f** 選項指定的，而含有金鑰檔及隱藏檔的目錄是由 **–d** 選項指定的。
4. 移除 Tivoli Access Manager for WebLogic 第 3.9 版。

   請參閱 *Tivoli Access Manager for WebLogic Version 3.9 User Guide*，以取得您作業系統特有的指示。

   警告: 在移除 Tivoli Access Manager for WebLogic 第 3.9 版之前，不要解除配置自訂領域。
5. 將必備 Tivoli Access Manager 基本套件及安全網域從第 3.9 版升級至第 4.1 版。

   判定哪些 Tivoli Access Manager 基本套件已安裝在掌控 Tivoli Access Manager for WebLogic 的電腦上。每一個部署都包括：
   - Tivoli Access Manager runtime environment
   - Tivoli Access Manager Java 執行時期

   根據 Tivoli Access Manager 安全網域的拓蹼，主機可能也包括：
   - Tivoli Access Manager Policy Server
   - Tivoli Access Manager Authorization Server

   當本端電腦含有原則伺服器及 Authorization Server 時，您可以一次升級所有 Tivoli Access Manager 基本套件。

   當本端電腦系統*不*包括原則伺服器及 Authorization Server 時，首先您必須升級電腦系統上掌控那些伺服器的安全網域。當原則伺服器及 Authorization Server 升級至第 4.1 版時，接著您就可以升級本端電腦上的基本執行時期元件（Tivoli Access Manager runtime environment 及 Java 執行時期）。

如需升級 Tivoli Access Manager 基本套件及安全網域的指示，請參閱*IBM Tivoli Access Manager Base 安裝手冊*。在繼續進行下一個步驟前，請先完成該文件中的指示。

6. Tivoli Access Manager for WebLogic 第 3.9 版部署可選擇性地使用 Tivoli Access Manager WebSEAL 來支援單一登入。如果您的部署使用 WebSEAL，請立即將 WebSEAL 從第 3.9 版升級至第 4.1 版。

   如需升級指示，請參閱*IBM Tivoli Access Manager WebSEAL 安裝指南*。

7. 安裝 Tivoli Access Manager for WebLogic 第 4.1 版。請遵循第 13 頁的『安裝程序』中適用於您作業系統的指示。

8. 不需要配置 Tivoli Access Manager for WebLogic。來自前一版的配置資訊會予以保留。在移除第 3.9 版的 Tivoli Access Manager for WebLogic 之前，如果您備份了 `PDRealm.conf`、金鑰檔或隱藏檔，請立即還原它們。

   遵循第 33 頁的『第 7 部份：測試配置』中的步驟，以驗證是否已正確地配置了自訂領域。

   註: 如果您也要將 WebLogic Server 從 6.1 升級至 7.0，則 BEA 升級指示會確定配置資訊將保留下來。

   警告: 如果要使用 WebLogic Server 7.0 與 Tivoli Access Manager for WebLogic 搭配，**在第一次啓動 WebLogic Server 時，您必須在***相容性模式***中啓動 WebLogic Server 7.0**。如果是在 7.0 模式中啓動 WebLogic Server 7.0，將不再可能於相容性模式中存取現有的網域。

   當您第一次啓動 WebLogic Server 7.0 時，請確定遵循 WebLogic Server 說明文件中在相容性模式中啓動的步驟，來起始設定相容性安全。這將確定 WebLogic Server 7.0 將在未來的重新啓動中，自動在相容性模式中啓動。

僅升級 WebLogic Server

本節說明下列升級：

表 3. 將 WebLogic Server 從 6.1 升級至 7.0

升級自：	升級至：
Tivoli Access Manager for WebLogic 第 4.1 版，含 WebLogic Server 第 6.1 版	Tivoli Access Manager for WebLogic 第 4.1 版，含 WebLogic Server, 第 7.0 版

Tivoli Access Manager for WebLogic 第 4.1 版同時支援 WebLogic Server 第 6.1 版及 WebLogic Server 第 7.0 版（在相容性模式中）。當您配置了含 WebLogic Server 6.1 的 Tivoli Access Manager for WebLogic，且想要將 WebLogic Server 升級至第 7.0 版，請遵循 BEA 提供的升級程序，將 WebLogic 6.x 網域升級至 WebLogic 7.0 網域。

當完成 BEA 升級程序時，第 7.0 版 WebLogic Server 就會在相容性模式中啓動。

在這個升級實務中，不需要對 Tivoli Access Manager for WebLogic 或必備 Tivoli Access Manager 套件，包括選用的 WebSEAL 套件，做任何變更。

警告: 如果要使用 WebLogic Server 7.0 與 Tivoli Access Manager for WebLogic 搭配，**在第一次啓動 WebLogic Server 時，您必須在***相容性模式***中啓動 WebLogic Server 7.0**。如果是在 7.0 模式中啓動 WebLogic Server 7.0，將不再可能於相容性模式中存取現有的網域。

當您*第一次*啓動 WebLogic Server 7.0 時，請確定遵循 WebLogic Server 說明文件中在相容性模式中啓動的步驟，來起始設定相容性安全。這將確定 WebLogic Server 7.0 將在未來的重新啓動中，自動在相容性模式中啓動。

安裝程序

請完成本節中適合於您作業系統的指示：

- 『在 Solaris 上安裝』
- 第 14 頁的『在 AIX 上安裝』
- 第 15 頁的『在 HP-UX 上安裝』
- 第 16 頁的『在 Linux 上安裝』
- 第 17 頁的『在 Windows 上安裝』

在 Solaris 上安裝

進行 Tivoli Access Manager for WebLogic 安裝作業時，必須將檔案解壓縮和套件配置分開處理。使用 **pkgadd**，在 Solaris Operating Environment（之後稱爲 Solaris）上安裝軟體套件。接著，以手動方式配置 Tivoli Access Manager。

註: 安裝及配置 Tivoli Access Manager for WebLogic 之後，如果需要重新安裝，您必須先解除配置並移除它。請參閱第 39 頁的『從 Solaris 移除』。

如果要在 Solaris 上安裝 Tivoli Access Manager for WebLogic，請完成下列指示：

1. 以 *root* 使用者身份登入。
2. 驗證是否滿足了軟體先決要件，包括來自 Tivoli Access Manager Base 的必要元件。請參閱第 8 頁的『必備軟體』。

   警告: 如果要使用 WebLogic Server 7.0 與 Tivoli Access Manager for WebLogic 搭配，**在第一次啓動 WebLogic Server 時，您必須在***相容性模式***中啓動 WebLogic Server 7.0**。如果是在 7.0 模式中啓動 WebLogic Server 7.0，將不再可能於相容性模式中存取現有的網域。

   當您*第一次*啓動 WebLogic Server 7.0 時，請確定遵循 WebLogic Server 說明文件中在相容性模式中啓動的步驟，來起始設定相容性安全。這將確定 WebLogic Server 7.0 將在未來的重新啓動中，自動在相容性模式中啓動。
3. 將 IBM Tivoli Access Manager Web Security CD 裝載在 `/cdrom/cdrom0`。
4. 將目錄切換至 `/cdrom/cdrom0/solaris`。
5. 輸入下列指令來安裝 Tivoli Access Manager for WebLogic 套件：

   ```
   # pkgadd -d . PDWLS
   ```

   當系統詢問您是否要繼續進行時，請鍵入 **y**，然後按 **Enter** 鍵。檔案會從 CD 解壓縮，並且安裝到硬碟上。此時會顯示一則訊息，指出 Tivoli Access Manager 套件的安裝已順利完成。**pkgadd** 公用程式隨即結束。

6. 接著，配置 Tivoli Access Manager for WebLogic。跳至第 19 頁的第 3 章, 『配置程序』。

在 AIX 上安裝

進行 Tivoli Access Manager for WebLogic 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 **SMIT** 將軟體套件安裝到 AIX 上。接著，以手動方式配置 Tivoli Access Manager for WebLogic。

註: 安裝及配置 Tivoli Access Manager for WebLogic 之後，如果需要重新安裝，您必須先解除配置並移除 Tivoli Access Manager for WebLogic 套件。請參閱第 40 頁的『從 AIX 移除』。

如果要在 AIX 上安裝 Tivoli Access Manager for WebLogic，請完成下列指示：

1. 以 *root* 身份登入。
2. 驗證是否滿足了軟體先決要件，包括來自 Tivoli Access Manager Base 的必要元件。請參閱第 8 頁的『必備軟體』。

   警告: 如果要使用 WebLogic Server 7.0 與 Tivoli Access Manager for WebLogic 搭配，**在第一次啓動 WebLogic Server 時，您必須在***相容性模式***中啓動 WebLogic Server 7.0**。如果是在 7.0 模式中啓動 WebLogic Server 7.0，將不再可能於相容性模式中存取現有的網域。

   當您*第一次*啓動 WebLogic Server 7.0 時，請確定遵循 WebLogic Server 說明文件中在相容性模式中啓動的步驟，來起始設定相容性安全。這將確定 WebLogic Server 7.0 將在未來的重新啓動中，自動在相容性模式中啓動。
3. 將 IBM Tivoli Access Manager Web Security CD 插入光碟機。
4. 在 Shell 提示中輸入下列指令：

   ```
   # smit
   ```

   這時會啓動 **SMIT** 公用程式。
5. 選取**軟體安裝及維護**。選取**安裝及更新軟體**。
   - 若爲 AIX 4.3 系統，選取**從最新可用的軟體來安裝及更新軟體**。
   - 若爲 AIX 5.1 系統，選取**安裝軟體**。
6. 當系統提示您提供輸入裝置時：
   - 若爲 AIX 4.3，輸入掛載 CD 的位置
   - 若爲 AIX 5.1，輸入包含安裝套件之 CD 上的目錄。例如：

     /*<mount_point>*/usr/sys/inst.images

     按一下**確定**。
7. 按一下**清單**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 軟體套件的清單。
8. 選取 **Access Manager for WebLogic** 套件 (PDWLS)。按一下**確定**。
9. 此時會開啓「從最新可用的軟體來安裝及更新軟體」視窗。
10. 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。
11. 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**。

12. 這時會顯示一個訊息框，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。

13. 按一下**完成**。按一下**取消**來結束 **SMIT**。
14. 接著，配置 Tivoli Access Manager for WebLogic。請跳至：第 19 頁的第 3 章, 『配置程序』。

在 HP-UX 上安裝

進行 Tivoli Access Manager for WebLogic 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 **swinstall** 將軟體套件安裝到 HP-UX 上。接著，以手動方式配置 Tivoli Access Manager for WebLogic。

註: 安裝及配置 Tivoli Access Manager for WebLogic 之後，如果需要重新安裝，您必須先解除配置並移除它。請參閱第 41 頁的『從 HP-UX 移除』。

如果要在 HP-UX 上安裝 Tivoli Access Manager for WebLogic，請完成下列步驟：

1. 以 *root* 使用者身份登入。
2. 驗證是否滿足了軟體先決要件，包括來自 Tivoli Access Manager Base 的必要元件。請參閱第 8 頁的『必備軟體』。

   警告: 如果要使用 WebLogic Server 7.0 與 Tivoli Access Manager for WebLogic 搭配，**在第一次啓動 WebLogic Server 時，您必須在*相容性模式*中啓動 WebLogic Server 7.0**。如果是在 7.0 模式中啓動 WebLogic Server 7.0，將不再可能於相容性模式中存取現有的網域。

   當您*第一次*啓動 WebLogic Server 7.0 時，請確定遵循 WebLogic Server 說明文件中在相容性模式中啓動的步驟，來起始設定相容性安全。這將確定 WebLogic Server 7.0 將在未來的重新啓動中，自動在相容性模式中啓動。

3. 將 IBM Tivoli Access Manager Web Security CD 插入光碟機。使用下列指令來掛載 CD：

   ```
   # nohup /usr/sbin/pfs_mountd &
   # nohup /usr/sbin/pfsd &
   # /usr/sbin/pfs_mount <mount_device> <mount_point>
   ```

   例如：

   ```
   # /usr/sbin/pfs_mount /dev/dsk/c0t0d0 /cdrom
   ```

4. 將目錄切換至 `hp`。
5. 輸入下列指令來安裝 Tivoli Access Manager for WebLogic 套件：

   ```
   # swinstall -s /temp_directory PDWLS
   ```

   這時會顯示一則訊息，指出分析階段已經順利完成。然後會顯示另一則訊息，指出執行階段正在開始。檔案會從 CD 解壓縮，並且安裝到硬碟上。這時會顯示一則訊息，指出執行階段已經順利完成。**swinstall** 公用程式隨即結束。

6. 驗證 `SHLIB_PATH` 已設爲 `/usr/lib` 或 `/opt/ibm/gsk5/lib`。如果未設定它，請輸入：

   ```
   export SHLIB_PATH=/opt/ibm/gsk5/lib
   ```

   當未設定這個變數時， Tivoli Access Manager 授權服務程式可能無法存取 IBM Global Security Toolkit (GSKIT) 程式庫。

7. 接著，配置 Tivoli Access Manager for WebLogic。請跳至：第 19 頁的第 3 章, 『配置程序』。

在 Linux 上安裝

進行 Tivoli Access Manager for WebLogic 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 **rpm** 將軟體套件安裝到 Linux 上。接著以手動方式配置 Tivoli Access Manager for WebLogic。

註: 安裝及配置 Tivoli Access Manager for WebLogic 之後，如果需要重新安裝，您必須先解除配置並移除它。請參閱第 41 頁的『從 Linux 移除』。

如果要在 Linux 上安裝 Tivoli Access Manager for WebLogic，請完成下列步驟：

1. 以 *root* 使用者身份登入。
2. 驗證是否滿足了軟體先決要件，包括來自 Tivoli Access Manager Base 的必要元件。請參閱第 8 頁的『必備軟體』。

   警告: 如果要使用 WebLogic Server 7.0 與 Tivoli Access Manager for WebLogic 搭配，**在第一次啓動 WebLogic Server 時，您必須在*相容性模式*中啓動 WebLogic Server 7.0**。如果是在 7.0 模式中啓動 WebLogic Server 7.0，將不再可能於相容性模式中存取現有的網域。

   當您*第一次*啓動 WebLogic Server 7.0 時，請確定遵循 WebLogic Server 說明文件中在相容性模式中啓動的步驟，來起始設定相容性安全。這將確定 WebLogic Server 7.0 將在未來的重新啓動中，自動在相容性模式中啓動。
3. 設定下列環境變數：

```
# export LD_PRELOAD=/usr/lib/libstdc++-libc6.1-2.so.3:/usr/lib/libstdc++-3-libc6.2-2-2.10.0.so
```

   註: 您必須設定這個環境變數，才能避免 Tivoli Access Manager 所使用的 C++ 程式庫版本與 IBM Global Security Toolkit 之間發生衝突。
4. 設定下列環境變數，以便確定「Java 本機介面」可以尋找適當的 Tivoli Access Manager for WebLogic C 程式庫：

```
# export LD_LIBRARY_PATH=/opt/pdwls/lib
```

5. 裝載 IBM Tivoli Access Manager Web Security CD。
6. 將目錄切換至 */mount_point*/linux。
7. 輸入下列指令來安裝 Tivoli Access Manager for WebLogic 套件：

   ```
   # rpm -i PDWLS-PD-4.1.0-0.i386.rpm
   ```

   當系統詢問您是否要繼續進行時，請鍵入 y，然後按 **Enter** 鍵。此時會將檔案解壓縮，並且安裝到硬碟上。 **rpm** 公用程式隨即結束。
8. 接著，配置 Tivoli Access Manager for WebLogic。跳至第 19 頁的第 3 章, 『配置程序』。

在 Windows 上安裝

進行 Tivoli Access Manager for WebLogic 安裝作業時，必須將檔案解壓縮和套件配置分開處理。請使用 InstallShield **setup.exe** 來安裝 Tivoli Access Manager for WebLogic 檔案。當 InstallShield 完成時，請以手動方式配置 Tivoli Access Manager for WebLogic。

註: 安裝及配置 Tivoli Access Manager for WebLogic 之後，如果需要重新安裝，您必須先解除配置並移除它。請參閱第 39 頁的『從 Windows 移除』。

如果要在 Windows 上安裝及配置 Tivoli Access Manager for WebLogic，請完成下列指示：

1. 以具備 Windows 管理者專用權的使用者身份登入 Windows 網域。
2. 驗證是否滿足了軟體先決要件，包括來自 Tivoli Access Manager Base 的必要元件。請參閱第 8 頁的『必備軟體』。

   警告: 如果要使用 WebLogic Server 7.0 與 Tivoli Access Manager for WebLogic 搭配，**在第一次啓動 WebLogic Server 時，您必須在***相容性模式***中啓動 WebLogic Server 7.0**。如果是在 7.0 模式中啓動 WebLogic Server 7.0，將不再可能於相容性模式中存取現有的網域。

   當您*第一次*啓動 WebLogic Server 7.0 時，請確定遵循 WebLogic Server 說明文件中在相容性模式中啓動的步驟，來起始設定相容性安全。這將確定 WebLogic Server 7.0 將在未來的重新啓動中，自動在相容性模式中啓動。
3. 將 IBM Tivoli Access Manager Web Security CD 插入光碟機。
4. 執行 Tivoli Access Manager for WebLogic InstallShield 安裝程式，方法爲按兩下以下檔案，其中下列指令中的字母 `E:` 代表光碟機：

   ```
   E:\Windows\AccessManager\Disk Images\Disk1\PDWLS\Disk Images\Disk 1\setup.exe
   ```

   這時會開啓「選擇安裝語言」視窗。
5. 選取適當的語言，然後按一下**確定**。

   這時會啓動 InstallShield 程式且開啓「歡迎使用」視窗。
6. 按一下**下一步**。

   這時會開啓「授權合約」視窗。
7. 按一下**是**，接受「授權合約」。

   這時會開啓「選擇目的位置」視窗。
8. 接受預設值或指定替代位置。按**下一步**。

   這時檔案就會解壓縮至磁碟。這時會顯示一則訊息，指出這些檔案已經安裝完畢。
9. 按一下**完成**來結束安裝程式。
10. 接著，配置 Tivoli Access Manager for WebLogic。移至第 19 頁的第 3 章, 『配置程序』。

第 3 章 配置程序

如果要配置 Tivoli Access Manager for WebLogic，請完成下列各節中的指示：

- 『第 1 部份：配置 Tivoli Access Manager Java 執行時期環境』
- 第 21 頁的『第 2 部份：結合 Tivoli Access Manager 安全網域』
- 第 23 頁的『第 3 部份：建立使用者帳戶』
- 第 24 頁的『第 4 部份：設定 startWebLogic 的 CLASSPATH』
- 第 26 頁的『第 5 部份：配置自訂領域』
- 第 31 頁的『第 6 部份：配置 WebLogic Server 的 WebSEAL 接合』
- 第 33 頁的『第 7 部份：測試配置』

註: 本章中的指示會假設您已安裝了 Tivoli Access Manager for WebLogic 及必備軟體，包括 Tivoli Access Manager 基本元件的配置。如果您未安裝軟體，請遵循第 7 頁的第 2 章, 『安裝指示』中的指示，立即安裝它。

第 1 部份：配置 Tivoli Access Manager Java 執行時期環境

Tivoli Access Manager Java 執行時期環境是 Tivoli Access Manager for WebLogic 的先決要件。您必須正確地配置了 Java 執行時期元件後，才能配置「WebLogic Server 自訂領域」。請使用 Tivoli Access Manager 公用程式 **pdjrtecfg**，來更新 WebLogic Server 所使用的「Java 執行時期環境」。此外，如果系統含有多個 Java 執行時期，請確定 WebLogic Server 所使用的「Java 執行時期環境」是用來執行 **pdjrtecfg** 公用程式。

1. 驗證您已安裝並配置了 Tivoli Access Manager Base runtime 元件。
2. 驗證已安裝了 Tivoli Access Manager Base Java 執行時期環境。

   如需相關資訊，請參閱第 8 頁的『必備軟體』。
3. 驗證當執行 **pdjrtecfg** 時，將存取正確版本的 Java：
   a. 判定 WebLogic Server 所使用的 Java 執行時期環境的位置。

      確切的目錄位置與作業系統類型有關。此外，在安裝 WebLogic Server 後，部份 WebLogic Server 部署（如 WebLogic Server 7.0 for Linux）會使用必須下載的 JDK。在這些情況中，JDK 的位置是由安裝程式來決定。

      例如：

      UNIX：*/WebLogic_install_directory/jdk_release*/jre/bin/java
      Windows：C:*WebLogic_install_directory**jdk_release*\jre

      Windows 上的預設 WebLogic 安裝目錄是 C:\bea。

      UNIX 上的預設 WebLogic 安裝目錄是 /opt/bea。

      註: 請參閱 WebLogic Server 說明文件，以取得建議的方法，來確定 PATH 環境變數已設定來使用 WebLogic Server 所提供的 Java 開發套件（JDK）。
   b. 選擇下列適用於您作業系統的指示：
      - 在 Windows 系統上，驗證 %PATH% 變數將 WebLogic Server 提供的 Java 執行時期環境列示爲路徑中的第一個。

- 在 UNIX 系統上，輸入下列指令：

  ```
  # which java
  ```

  回應應該符合您在前一個步驟中所決定的位置。

  – 大部份 WebLogic Server 6.1 UNIX 安裝作業的預設位置是：

    /WebLogic_install_directory/jdk131/jre/bin/java

  – 大部份 WebLogic Server 7.0 UNIX 安裝作業的預設位置會隨著該平台的 JDK 修訂層次而有所改變。請注意， WebLogic Server 7.0 目前不支援 AIX。

4. 將目錄切換至 Tivoli Access Manager 安裝路徑中的 sbin 目錄。例如：

   (UNIX) /opt/PolicyDirector/sbin

   (Windows) C:\Program Files\Tivoli\Policy Director\sbin

5. 執行 **pdjrtecfg** 指令。例如，請以*連續一行*輸入下列指令：

   ```
   Windows:
   MSDOS> pdjrtecfg -action config
    -java_home C:\WebLogic_install_directory\JDK131\jre
   ```

   ```
   UNIX:# pdjrtecfg -action config -java_home /WebLogic_install_directory/jdk131/jre
   ```

   註: 上面顯示的 JDK 目錄名稱可能需要稍作修改，才能反映您作業系統專有的 JDK 1.3.1 版本所使用的目錄。

   如需如何使用 **pdjrtecfg** 的相關資訊，請參閱 *IBM Tivoli Access Manager Base 安裝手冊* 中此指令的參考頁。

6. 新增下列項目到 CLASSPATH 變數：

表 4. UNIX 作業系統的 CLASSPATH 項目。

UNIX
/opt/PolicyDirector/java/export/pdjrte/PD.jar
/opt/PolicyDirector/java/export/pdjrte/ibmjceprovider.jar
/opt/PolicyDirector/java/export/pdjrte/jaas.jar
/opt/PolicyDirector/java/export/pdjrte/US_export_policy.jar
/opt/PolicyDirector/java/export/pdjrte/ibmjsse.jar
/opt/PolicyDirector/java/export/pdjrte/local_policy.jar
/opt/PolicyDirector/java/export/pdjrte/ibmjcefw.jar
/opt/PolicyDirector/java/export/pdjrte/ibmpkcs.jar

表 5. Windows 作業系統的 CLASSPATH 項目。

Windows
C:\Program Files\Tivoli\PolicyDirector\java\export\pdjrte\PD.jar
C:\Program Files\Tivoli\PolicyDirector\java\export\pdjrte\ibmjceprovider.jar
C:\Program Files\Tivoli\PolicyDirector\java\export\pdjrte\jaas.jar
C:\Program Files\Tivoli\PolicyDirector\java\export\pdjrte\US_export_policy.jar
C:\Program Files\Tivoli\PolicyDirector\java\export\pdjrte\ibmjsse.jar
C:\Program Files\Tivoli\PolicyDirector\java\export\pdjrte\local_policy.jar
C:\Program Files\Tivoli\PolicyDirector\java\export\pdjrte\ibmjcefw.jar
C:\Program Files\Tivoli\PolicyDirector\java\export\ibmpkcs.jar

第 2 部份：結合 Tivoli Access Manager 安全網域

Tivoli Access Manager for WebLogic 結合 Tivoli Access Manager 安全網域，方法爲登記 Tivoli Access Manager 授權 API 應用程式，並自訂部份配置檔設定。配置步驟彙總如下：

- 將範例配置檔複製到將用來儲存 Tivoli Access Manager for WebLogic 檔的位置。
- 使用 Java 類別 SvrSslCfg，提供與原則伺服器的連通性。

  註: 如何使用這個類別取決於 Tivoli Access Manager Java 執行時期的適當配置而定，其說明在第 19 頁的『第 1 部份：配置 Tivoli Access Manager Java 執行時期環境』中。
- 使用 **svrsslcfg** 公用程式來建立必要的使用者，並調整配置檔設定。

每一個步驟都會在下列指示中加以詳細說明。如果要將 Tivoli Access Manager for WebLogic 配置到 Tivoli Access Manager 安全網域，請完成下列每一個步驟：

1. Tivoli Access Manager for WebLogic 包括範例配置檔 `PDRealm.conf`。這個檔案包含在 `etc` 目錄（位於 Tivoli Access Manager for WebLogic 安裝目錄）。

   將範例配置檔複製到您選擇的目錄。例如，如果您在 WebLogic Server 安裝目錄下建立 `PDRealm` 目錄，請以*連續一行*輸入下列指令：

表 6. 如何在 UNIX 作業系統上複製範例配置檔

UNIX
`# cp /opt/pdwls/etc/PDRealm.conf \` ` /WebLogic_install_directory/PDRealm/PDRealm.conf`

表 7. 如何在 Windows 作業系統上複製範例配置檔

Windows
`> copy \C:\Program Files\Tivoli\pdwls\etc\PDRealm.conf` ` C:\WebLogic_install_directory\PDRealm\PDRealm.conf`

2. 使用 Tivoli Access Manager SvrSslCfg Java 類別來配置與遠端 Tivoli Access Manager 伺服器的 SSL 通訊。*以連續一行指令方式*輸入的語法如下：

   ```
   java com.tivoli.mts.SvrSslCfg Name sec_master_password
    Access_Manager_policy_server_hostname
    Access_Manager_policy_server_hostname
   ```

   選項如下：

   - *Name*

     要建立並與 SSL 通訊產生關聯之 Tivoli Access Manager for WebLogic 應用程式的名稱。這個應用程式是伺服器。例如：

     ```
     amwlsserver
     ```
   - *sec_master_password*

     sec_master 使用者的密碼。
   - *Access_Manager_policy_server_hostname*

     Tivoli Access Manager Policy Server 執行所在的系統名稱。
   - *Access_Manager_policy_server_hostname*

     Tivoli Access Manager Policy Server 執行所在的系統名稱。

Tivoli Access Manager Policy Server 主機名稱指定了*兩次*。第二個項目是必要的，因爲 SvrSslCfg 類別需要一個項目指出 Authorization Server 的主機名稱。當 Tivoli Access Manager 安全網域不包括一個 Authorization Server 時，您必須改爲指定原則伺服器的主機名稱。請注意，Tivoli Access Manager for WebLogic 不需要 Authorization Server。因此，在典型 Tivoli Access Manager for WebLogic 安裝作業中，您必須指定原則伺服器主機名稱兩次。

如需 `com.tivoli.mts.SvrSslCfg` 的相關資訊，請參閱 *IBM Tivoli Access Manager Administration Java Classes Developer's Reference*。

3. *以連續一行*輸入下列 **svrsslcfg** 指令：

表 8. UNIX 作業系統上 svrsslcfg 的指令行參數。

UNIX

`# svrsslcfg -config -f /WebLogic_install_directory/PDRealm/PDRealm.conf`
`-d /WebLogic_install_directory/PDRealm -n amwlsserver -s remote`
`-P sec_master_password -S amwlsserver_password -r 0`

表 9. Windows 作業系統上 svrsslcfg 的指令行參數。

Windows

`svrsslcfg -config -f c:\WebLogic_install_directory\PDRealm\PDRealm.conf`
`-d c:\WebLogic_install_directory\PDRealm -n amwlsserver -s remote`
`-P sec_master_password -S amwlsserver_password -r 0`

svrsslcfg 的這個範例呼叫會完成下列作業：

- 建立一個稱爲 `amwlsserver` 的使用者。當透過 SSL 與 Tivoli Access Manager Policy Server 通訊時，應用程式將使用這個使用者身份。
- 按照 **-S** 選項的指定，來建立 amwlsserver 的密碼。
- 建立該使用者的 SSL 金鑰檔，然後將它放在 **-d** 選項所指定的目錄中。
- 新增使用者至 remote-acl-users 群組（根據 **-s** `remote` 選項而定）

  註: 使用這個 `remote` 引數表示已在遠端模式中配置了授權。這表示必須在 Tivoli Access Manager 安全網域內的另一個主機系統上配置 Authorization Server。
- 修改指定的配置檔 `PDRealm.conf` 中的設定。請注意，必須提供配置檔的絕對路徑名稱給 **-f** 選項。

如需 **svrsslcfg** 的相關資訊，請參閱 *IBM Tivoli Access Manager Administration C API Developer's Reference*。

4. 驗證您是否可以連接原則伺服器。以管理者 sec_master 身份登入 **pdadmin**，再輸入下列指令：

```
pdadmin> server list
```

來自這個指令的回應會顯示兩個伺服器。其中一個是與主機名稱結合的 Tivoli Access Manager for WebLogic 應用程式的名稱，這是您在前一節呼叫 `java com.tivoli.mts.SvrSslCfg` 時所輸入的名稱。另一個是 **svrsslcfg** 公用程式執行配置步驟的結果。

註: 這兩個伺服器不能同名。

下列範例顯示兩個以**粗體**字型顯示的伺服器：

```
pdadmin> server list
 pdwls-securix
 amwlsserver-securix.ibm.com
 webseald-securix.ibm.com
 ivacld-securix.ibm.com
```

第 3 部份：建立使用者帳戶

當呼叫 Tivoli Access Manager 管理 API 介面時，Tivoli Access Manager for WebLogic 需要一個帳戶，供「自訂領域」使用。當透過 WebSEAL 配置單一登入能力時，需要額外的帳戶。

如果您要建立必要的帳戶，請完成下列指示。

1. 使用 **pdadmin**，來建立*pdadmin_context_user*。

   例如，*以連續一行*輸入下列指令來建立使用者：

   ```
   pdadmin> user create pdadmin_context_user
   cn=pdadmin_context_user,o=ibm,c=au
   pdadmin_context_user pdadmin_context_user
   pdadmin_context_user_password iv-admin
   ```

   > *pdadmin_context_user* 是將用來建立 **pdadmin** 環境定義的使用者名稱。這是「自訂領域」與 Tivoli Access Manager 管理 API 一起使用的環境定義。
   >
   > 使用者必須位在 **iv-admin** 使用者群組，或指定有足夠的許可權，可建立、刪除、修改及列示使用者和群組。做法爲在連接至 /Management 物件空間內適當物件的存取控制清單 (ACL) 上，給與使用者下列許可權：
   >
   > ```
   > TcmdbsvatNWA
   > ```
   >
   > 連接至 /Management 物件的預設 ACL 名稱是 `default-management`

2. 使用 **pdadmin** 來啓動新的 *pdadmin_context_user* 帳戶。例如：

   ```
   pdadmin> user modify pdadmin_context_user account-valid yes
   ```

3. 如果您不想使用 WebSEAL 來提供單一登入能力，請略過這個步驟。跳至第 24 頁的『第 4 部份：設定 startWebLogic 的 CLASSPATH』。

   如果您想要使用 WebSEAL 來提供單一登入能力，請使用 Tivoli Access Manager Web Portal Manager 或 Tivoli Access Manager 公用程式 **pdadmin** 來建立 WebSEAL *configured_user*。

   > *configured_user* 是特殊的 Tivoli Access Manager 使用者，用來在 WebSEAL 與 WebLogic Server 之間形成信任關係。這個使用者的名稱可以是任何有效的 Tivoli Access Manager 使用者名稱。

   例如，如果 *configured_user* 是 `websealsso`，且 `websealsso` 的密碼是 `pdwebwlssso`，請輸入下列 **pdadmin** 指令。每一個指令都應該*以連續一行*輸入：

```
pdadmin> user create websealsso cn=websealsso,o=ibm,c=au
websealsso websealsso pdwebwlssso

pdadmin> user modify websealsso account-valid yes
```

註: 以適當的值取代上面指令中的組織 (o=ibm) 及國家或地區 (c=au)。

若要得到最佳安全性，請保護 *configured_user* 密碼。
定期變更密碼。建議使用 Tivoli Access Manager 隨機密碼產生器：

UNIX：/opt/PolicyDirector/sbin/genpass

第 4 部份：設定 startWebLogic 的 CLASSPATH

startWebLogic 指令是用來啓動 WebLogic Server。您需要修改 CLASSPATH 環境變數，以啓用 **startWebLogic** 來存取並載入正確的 Java 類別。

請完成下列指示：

1. 如果 WebLogic Server 正在執行，請立即停止它。
2. 新增下列檔名至 **startWebLogic** 指令的 CLASSPATH 變數。

表 10. 要在 UNIX 作業系統上新增至 CLASSPATH 的檔名。

UNIX
/opt/pdwls/lib/PDWASAuthzManager.jar
/opt/pdwls/lib/pdAuthzn.jar
/opt/pdwls/lib/PDRealm.jar

表 11. 要在 Windows 作業系統上新增至 CLASSPATH 的檔名。

Windows
C:\Progra~1\Tivoli\pdwls\lib\PDWASAuthzManager.jar
C:\Progra~1\Tivoli\pdwls\lib\pdAuthzn.jar
C:\Progra~1\Tivoli\pdwls\lib\PDRealm.jar

startWebLogic 指令是位在已安裝的 WebLogic Server 網域的目錄中。在標準安裝中，這是：

- WebLogic Server 6.1

  (Windows) C:\bea\wlserver6.1\config\mydomain
  (UNIX) /bea/wlserver6.1/config/mydomain

- WebLogic Server 7.0

  (Windows) C:*WebLogic_install_directory*\user_projects*domain_name*
  (UNIX) */WebLogic_install_directory*/user_projects/*domain_name*

  變數 *domain_name* 是您在建立 WebLogic Server 7.0 網域時所選取的名稱。

3. 完成本步驟中的指示，以確定 WebLogic Server 載入正確的 Java 類別。

   警告: 您必須完成這個步驟，不然 WebLogic Server 將不會重新啓動。

   從 Java 執行時期環境（已安裝成 WebLogic Server 的先決要件）的程式庫延伸目錄移除 Tivoli Access Manager Base Java 執行時期環境檔案。

程式庫延伸目錄如下：

UNIX：/*Java_runtime_environment_path*/lib/ext
Windows：C:*Java_runtime_environment_path*\lib\ext

Java 執行時期環境路徑的位置應該符合您在第 19 頁的『第 1 部份：配置 Tivoli Access Manager Java 執行時期環境』中所決定的路徑。

從程式庫延伸目錄移除下列檔案：

表 12. 要從延伸目錄移除的檔案清單

PD.jar	ibmjsse.jar
US_export_policy.jar	ibmpkcs.jar
ibmjcefw.jar	jaas.jar
ibmjceprovider.jar	local_policy.jar

註： 在配置 Tivoli Access Manager Base Java 執行時期環境期間，這些檔案已複製至這個目錄。您移除的是檔案複本。但不會移除原始檔案。

4. 新增下列項目到 **startWebLogic** 指令中定義的 CLASSPATH 變數。確定這些項目放在 WebLogic Server 項目*之後*。

   警告： 您必須完成這個步驟，不然 WebLogic Server 將不會重新啓動。

表 13. UNIX 作業系統上的新 CLASSPATH 項目

UNIX
/opt/PolicyDirector/java/export/pdjrte/PD.jar
/opt/PolicyDirector/java/export/pdjrte/US_export_policy.jar
/opt/PolicyDirector/java/export/pdjrte/ibmjcefw.jar
/opt/PolicyDirector/java/export/pdjrte/ibmjceprovider.jar
/opt/PolicyDirector/java/export/pdjrte/ibmjsse.jar
/opt/PolicyDirector/java/export/pdjrte/ibmpkcs.jar
/opt/PolicyDirector/java/export/pdjrte/jaas.jar
/opt/PolicyDirector/java/export/pdjrte/local_policy.jar

表 14. Windows 作業系統上的新 CLASSPATH 項目

Windows
C:\Progra~1\Tivoli\Policy~1\java\export\pdjrte\PD.jar
C:\Progra~1\Tivoli\Policy~1\java\export\pdjrte\US_export_policy.jar
C:\Progra~1\Tivoli\Policy~1\java\export\pdjrte\ibmjcefw.jar
C:\Progra~1\Tivoli\Policy~1\java\export\pdjrte\ibmjceprovider.jar
C:\Progra~1\Tivoli\Policy~1\java\export\pdjrte\ibmjsse.jar
C:\Progra~1\Tivoli\Policy~1\java\export\pdjrte\ibmpkcs.jar
C:\Progra~1\Tivoli\Policy~1\java\export\pdjrte\jaas.jar
C:\Progra~1\Tivoli\Policy~1\java\export\pdjrte\local_policy.jar

5. 如果您要使用預設語言（英文），請略過這個步驟。跳至第 26 頁的『第 5 部份：配置自訂領域』。

   如果您要使用支援非預設語言（英文）的語言套件，則您必須新增下列路徑到 **startWebLogic** Script 中定義的 CLASSPATH：

   - UNIX 系統：

     /opt/pdwls/nls/java

- Windows 系統：

  ```
  C:\Progra~1\Tivoli\pdwls\nls\java
  ```

註： 新增這個目錄將可讓您存取語言套件安裝作業安裝在 `/opt/pdwls/nls/java/com/tivoli/pdwls/nls/` 的資源組。

第 5 部份：配置自訂領域

請完成下列各節中的指示：

- 『第 5A 部份：建立新的自訂領域』
- 第 29 頁的『第 5B 部份：配置新的快取領域』
- 第 30 頁的『第 5C 部份：快取證明及群組名稱對映』

第 5A 部份：建立新的自訂領域

1. 使用 **startWebLogic** 來啓動 WebLogic 伺服器。

   如果您正要使用 WebLogic Server 7.0，但尚未第一次啓動伺服器，請閱讀下列注意事項：

   警告： 如果要使用 WebLogic Server 7.0 與 Tivoli Access Manager for WebLogic 搭配，**在第一次啓動 WebLogic Server 時，您必須在***相容性模式***中啓動 WebLogic Server 7.0**。如果是在 7.0 模式中啓動 WebLogic Server 7.0，將不再可能於相容性模式中存取現有的網域。

   當您第一次啓動 WebLogic Server 7.0 時，請確定遵循 WebLogic Server 說明文件中在相容性模式中啓動的步驟，來啓動 WebLogic Server 7.0。這將確定 WebLogic Server 7.0 將在未來的重新啓動中，自動在相容性模式中啓動。

2. 在瀏覽器中啓動 WebLogic Server 主控台。做法爲存取下列 URL：

   `http://`*`WebLogic_Server_host`*`:`*`WebLogic_Server_listening_port`*`/console`

   > *WebLogic_Server_host* 是 WebLogic Server 系統的名稱。
   >
   > *WebLogic_Server_listening_port* 是 WebLogic Server 監聽所在的埠。這個埠的預設值是 7001。

3. 選取適當的功能表項目：
   - 對於相容性模式中的 WebLogic Server 7.0，請選取：

     相容性安全模式 > 領域 > 配置新的自訂領域
   - 對於 WebLogic Server 6.1，請選取：

     按一下**安全性 -> 領域 -> 配置新的自訂領域**
4. 建立「自訂領域」。指定下列值：
   - 名稱：`PDRealm`

     這是將新增至 WebLogic Server 的「Tivoli Access Manager 自訂領域」的名稱。這個名稱可以是您選擇的任何名稱。這裡提供的名稱 `PDRealm` 僅做範例之用。
   - 領域類別名稱：`com.tivoli.pdwls.realm.PDRealm`
   - 密碼：（不需要）。

在 WebLogic Server 7.0 中建立新的網域期間，「網域配置精靈」會提供一個選項，來指定預設名稱 system 以外的系統使用者名稱。如果選擇要這樣做，則您也須按照下一個步驟中的說明，指定內容 wls.configurable.user.name。

在 WebLogic Server 7.0 中，如果您指定 system 以外的系統使用者名稱，且您未設定 wls.configurable.user.name，Tivoli Access Manager for WebLogic 將使用預設名稱 system。如此將使得您的非預設系統使用者名稱處於無效狀態。

例如，如果建立了網域，且在建立網域期間，已將使用者名稱 myuser 指定成系統使用者，則 wls.configurable.system.user=myuser 必須新增至自訂領域配置。略過這個配置項目會導致 Tivoli Access Manager for WebLogic 將系統使用者預設爲 system。這將使得 myuser 處於無效狀態，以致無法加以管理。當使用者無效時，將無法刪除使用者，也無法變更密碼。

當您在 WebLogic Server 7.0 上啓用相容性模式時，在建立網域期間，會自動建立 system 使用者（如果沒有指定的話）。使用者 system 的密碼起初會和指定給系統使用者（在建立網域時設定的）的密碼一樣。

例如，假設已用系統使用者名稱 myuser 及密碼 mypassword 建立了網域。啓用相容性模式會自動建立一個密碼是 mypassword 的 system 使用者。然後，就可以使用者 myuser 或使用者 system 的身份，來啓動 WebLogic 伺服器及存取 WebLogic Web 型主控台。

5. 輸入「自訂領域」內容設定的適當配置資料。當設定所有內容值時，請參閱本步驟中所包含的資訊，然後按一下**建立**。

   如何判定內容設定

   Tivoli Access Manager for WebLogic 包括一個範例文字檔，其中含有所有必要的配置設定。您可以將這個檔案複製至 WebLogic 主控台視窗，然後修改這些值以符合您的環境。

   範例文字檔位於下列位置：

   - UNIX 系統：

     /opt/pdwls/sbin/DefaultConfig.txt

   - Windows 系統：

     C:\Progam Files\Tivoli\pdwls\sbin\DefaultConfig.txt

   下表說明範例配置檔中所包括的內容。使用這個表格中的定義，來協助您判定這些值中有哪些應該位於您的環境中。

表 15. 自訂領域內容設定

領域內容：webseal.sso.configured **有效值**：true 或 false **說明**：定義是否將配置 WebSEAL，以及判定「Tivoli Access Manager 自訂安全領域」是否將嘗試執行單一登入。
領域內容：pdadmin.user.name **有效值**：*pdadmin_context_user* **說明**：pdamin.user.name 是 *pdadmin_context_user*，而且是將用來建立 **pdadmin** 環境定義的使用者名稱。 這是「自訂領域」與 Tivoli Access Manager 管理 API 一起使用的環境定義。這個使用者名稱已依照這些配置指示定義在前一個步驟中。

表 15. 自訂領域內容設定 (繼續)

領域內容：pdadmin.password **有效值**：*pdadmin_context_user_password* **說明**：pdadmin.user.name 的密碼。 這應該符合在上面已依照這些配置指示在前一個步驟中定義的密碼。
領域內容：pdrealm.registry.listing **有效值**：true 或 false **說明**：定義「Tivoli Access Manager 自訂領域」是否應該將使用者和群組（包括 群組成員資格）列示至 WebLogic Server 主控台應用程式。在生產環境中，這應該設爲 false。 僅在測試環境中，才將它設成 true。
領域內容：connection.pool **有效值**：: 1 -*n* **說明**：其中 *n* 是一個整數，用來定義要在「領域」儲存池中實例化的「領域」物件數目。
領域內容：pdrealm.tracing **有效值**：true 或 false **說明**：開啓或關閉「Tivoli Access Manager for WebLogic 領域」追蹤。追蹤將傳送至 WebLogic Server 日誌。
領域內容：wls.admin.user **有效值**： *configured_user* **說明**：被配置來在 WebSEAL 與 WebLogic Server 之間形成信任關係的特殊使用者。 這個項目必須符合您先前依照這些配置指示所建立的 *configured_user* 身份。
領域內容：group.dn **有效值**：有效的識別名稱 (DN) **說明**：群組定義所在的 LDAP 命名環境定義。例如，o=ibm,c=aux。
領域內容：user.dn **有效值**：有效的識別名稱 (DN) **說明**：使用者定義所在的 LDAP 命名環境定義。例如，o=ibm,c=aux。

表 15. 自訂領域內容設定 (繼續)

領域內容：aznapi.conf.file **有效值**： *authorization_api_configuration_file_path* **說明**：Tivoli Access Manager 授權配置檔 PDRealm.conf 的完整路徑， 這是當使用 **svrsslcfg** 來配置 Tivoli Access Manager 授權 API 應用程式時所產生的配置檔。
領域內容：wls.configurable.system.user **有效值**： **說明**：這個設定指定系統使用者名稱。當建立了 WebLogic Server 7.0 網域，而且該網域的系統使用者名稱已指定爲預設名稱 system 以外的值時， 將需要這個設定。這個內容的值應該是當建立 WebLogic Server 7.0 網域時輸入給系統使用者的使用者名稱。 請注意，當配置 WebLogic Server 6.1 網域時，或從現有 WebLogic Server 6.1 網域升級至 WebLogic Server :break>7.0 網域時， 不需要這個配置項目。
領域內容：wls.admin.user.password.expiry **有效值**： *number_of_minutes* **說明**：指定快取版的 *configured_user* 密碼何時到期。此值是以分鐘爲單位指定的。 如果您不想要密碼到期，請不要設定這個內容，或將它設爲少於 1 的值。 當 configured_user 的密碼到期時，「自訂領域」將重新鑑定從 WebSEAL 收到的密碼，:break>並放至 Tivoli Access Manager 使用者登錄 如果已在使用者登錄中變更了密碼，則必須以新的密碼更新 WebSEAL 配置， 而且必須重新啓動 WebSEAL。

第 5B 部份：配置新的快取領域

請完成本節中的步驟，以配置新的快取領域。這些指示假設您的 WebLogic 主控台正在執行中。

1. 選取適當的功能表項目：
   - 對於相容性模式中的 WebLogic Server 7.0，請選取：
     相容性安全模式 > 快取領域 > 配置新的快取領域
   - 對於 WebLogic Server 6.1，請選取：
     安全性 -> 領域 -> 配置新的快取領域
2. 指定下列值：
   a. 名稱：PD_Caching_Realm
      這是將新增至 WebLogic Server 的「Tivoli Access Manager 快取領域」的名稱。這個名稱可以是您選擇的任何名稱。這裡提供的名稱 PD_Caching_Realm 僅做範例之用。
   b. 基本領域：PDRealm

這個名稱應該符合您在前一個步驟中指定的「自訂領域」名稱。先前使用的範例是 PDRealm。

c. 區分大小寫：否

3. 按一下**建立**。
4. 繼續進行『第 5C 部份：快取證明及群組名稱對映』。

第 5C 部份：快取證明及群組名稱對映

Tivoli Access Manager for WebLogic 提供要與 Tivoli Access Manager 安全性一起使用的額外快取設定。這些設定是用來配置下列的快取：

- 使用者證明
- 群組名稱對映

請完成下列指示：

1. 如果您想要對快取使用者證明使用預設設定，請略過這個步驟，然後繼續進行下一個步驟。

   使用本節中的設定來啓用使用者證明的快取。使用證明快取可取得最佳的效能。下表中所說明的項目應該新增至「Access Manager 安全領域」的配置資料。

表 16. 使用者證明快取設定

證明快取
領域內容：credential.cache.entry.lifetime **有效值**： *number_of_minutes* **說明**：指定要將使用者證明保留在快取記憶體中多久時間（分鐘）。 例如，5。如果未指定此值，或此值少於 1，將停用證明快取。 請注意，這個參數應該設爲使群組成員資格變更生效所需的時間。 「自訂領域」將不會偵測到使用者證明中的變更，直到過了這個時間量。
領域內容： credential.cache.max.entries **有效值**： *整數* **說明**：指定快取記憶體中最多可有多少個項目。 例如，10000。如果未指定此值，或此值少於 1，將停用證明快取。
領域內容： credential.cache.num.buckets **有效值**：*整數* **說明**：指定快取記憶體內將具有多少個快取記憶體（儲存區）。 例如，20。使用多個儲存區將在快取記憶體中取得最佳的證明查閱效能。 如果未指定此值，或此值少於 1，將停用證明快取。

2. 如果您想要對群組名稱對映使用預設設定，請略過這個步驟，然後繼續進行下一個步驟。

群組名稱對映快取

這個快取會儲存群組「識別名稱」或 UUID 與 Tivoli Access Manager 簡稱之間的對映。這個對映是用來比較 J2EE 部署描述子的群組資訊與使用者登錄中所含有的群組資訊。當根據角色成員資格處理存取（授權）要求時，快取這個資訊將得到最佳效能。下表中所說明的項目應該新增至「Tivoli Access Manager for WebLogic 安全領域」的配置資料。

表 17. 群組名稱對映的快取設定

群組名稱對映快取
領域內容：group.mapping.cache.entry.lifetime **有效值**：*number_of_minutes* **說明**：指定每一個快取項目的生命週期（分鐘）。 例如，720。
領域內容：group.mapping.cache.max.entries **有效值**：*integer* **說明**：指定快取記憶體中最多可有多少個項目。 例如，500。請使用此值來確定含有非常多群組的安裝作業不會用光可用的系統記憶體。

3. 選擇符合您 WebLogic Server 版本號碼的指示：

   WebLogic Server 6.1

   a. 移至**安全性 -> FileRealm**，然後

   b. 將它設成您已在前一個步驟中指定的快取領域名稱。前一個步驟中的範例快取領域名稱是 PD_Caching_Realm。將其他所有欄位保持原狀。

   WebLogic Server 7.0

   a. 按一下 *mydomain* **-> 安全性**

   b. 按一下**一般**標籤。對於**預設領域**，選取 **CompatibilityRealm**。

   c. 按一下 **FileRealm** 標籤。對於**快取領域**，選取您已建立的領域名稱。

   d. 按一下**套用**。

4. 重新啓動 WebLogic Server。

   安全設定現在將生效。

第 6 部份：配置 WebLogic Server 的 WebSEAL 接合

如果您想要使用 WebSEAL 來提供單一登入服務，請使用本節中的指示來配置必要的 WebSEAL 接合。如果您未使用 WebSEAL 單一登入，請略過本節，跳至第 33 頁的『第 7 部份：測試配置』。

警告: 當使用單一登入服務時，請拒絕內部使用者直接存取 WebLogic Server。

如果您的 WebLogic Server 安裝作業需要處理來自您區域網路外的使用者的存取要求，使用 WebSEAL 來提供單一登入服務有很大的優點。在此情況下，WebSEAL 將提供所有鑑定服務給 WebLogic Server。

不過，當使用 WebSEAL 來提供單一登入服務給外部使用者時，**不**容許外部使用者不經過 WebSEAL 存取 WebLogic Server。 WebSEAL 在操作每一個要求的使用者名稱及密碼項目時，會將它們當作 WebLogic Server 信任關係的一部份。信任關係需要對特殊 WebSEAL 使用者 *configured_user* 停用鑑定鎖定（登入失敗次數上限）。

因爲對 *configured_user* 停用了鑑定鎖定，所以惡意內部使用者可能會嘗試冒充 WebLogic Server 的 WebSEAL，並強行嘗試蠻橫的密碼攻擊。對於這種破壞信任關係（未必會發生，但可能很嚴重的情況）的最佳防禦就是用 WebSEAL 執行所有的鑑定。因此，當使用單一登入時， WebLogic Server 應該會拒絕所有來自內部使用者的直接存取要求。

如果要配置 WebLogic Server 的 WebSEAL 接合，請在掌控 WebSEAL 伺服器的系統上完成下列步驟：

1. 在 WebSEAL 配置檔 `webseald.conf` 中，更新下列配置項目：

   ```
   basicauth-dummy-passwd = configured_user_password
   ```

2. 停止並重新啓動 WebSEAL，以使配置變更生效。
3. 使用 **pdadmin** 指令，來停用特殊 WebSEAL 使用者 *configured_user* 的鑑定鎖定：

   ```
   pdadmin> policy set max-login-failures unset -user configured_user
   ```

4. 使用 **pdadmin** 指令來建立 WebSEAL 接合。

   註: 這個步驟可以在 Tivoli Access Manager 安全網域中的任何機器上進行。您不一定要在 WebSEAL 系統上執行它。例如，您可以在 Tivoli Access Manager Policy Server 系統上執行它。

   請確定使用 `-b` 選項，來提供接合目標 URL。對於單一登入，這是必要的。

   例如，*以連續一行*輸入下列指令：

   ```
   pdadmin> server task webseald_server_name create -t tcp
   -p WebLogic_Server_listen_port -h WebLogic_Server
   -b supply junction_target
   ```

   下表定義上述 **pdadmin** 指令中的變數：

表 18. pdadmin 指令的選項

選項	說明

表 18. pdadmin 指令的選項 (繼續)

webseald_server_name	WebSEAL 伺服器的名稱。 名稱是由這兩個部份所組成： webseald-*WebSEAL_server_instance*。 對 *WebSEAL_server_instance* 使用您的系統主機名稱。 例如，如果主機名稱是 cruz， 則 *webseald_server_name* 將是： webseald-cruz 附註：如果已在同一伺服器上安裝了多個 WebSEAL 實例， 則您也需要指定伺服器實例。如需利用多個伺服器實例建立接合:break>的指示， 請參閱 *IBM Tivoli Access Manager WebSEAL Administrator's Guide*。
WebLogic_Server	WebLogic Server 的主機名稱
WebLogic_Server_listen_port	WebLogic Server 監聽所在的埠
junction_target	接合的 URL 目標

如需建立及使用 WebSEAL 接合的完整資訊，請參閱*IBM Tivoli Access Manager WebSEAL Administrator's Guide*。

第 7 部份：測試配置

完成下列步驟來驗證已正確地配置了「Tivoli Access Manager 自訂領域」：

1. 使用 WebLogic Server 主控台來建立新的測試使用者。
2. 執行下列 **pdadmin** 指令：

   ```
   pdadmin> user show test_user
   ```

   - 驗證 account-valid 是 yes。
   - 驗證 password-valid 是 yes。

「Tivoli Access Manager 自訂領域」單一登入解決方案容許透過 WebSEAL 進行單一鑑定步驟，以透通方式向 WebLogic Server 驗證使用者身份。您可以執行示範應用程式，來確認已正確地配置了鑑定。示範應用程式的說明在第 35 頁的『使用示範應用程式』中。

第 4 章 管理作業

本章含有關於 Tivoli Access Manager for WebLogic 的下列資訊：

使用示範應用程式

您可以使用示範應用程式，來查看兩種授權類型的範例，以及運用 WebSEAL 單一登入能力。

兩種授權類型如下：

- 宣告

  使用「部署描述子」來授與使用者及群組特定的角色。根據預設值，PDDemoApp 應用程式不會授與存取權限給任何使用者。

- 程式

  使用程式安全性，Enterprise Java Bean 可確定僅有每一個帳戶的擁有者有權檢視他們自己的帳戶餘額。例如，使用者 Mark 無法檢視使用者 Luke 的餘額。

如果要執行示範應用程式，請完成下列步驟：

1. 將示範應用程式 PDDemoApp.ear 複製至 *WebLogic_domain_directory*\applications。請注意，不需要使用這個目錄。您可以將 EAR 檔放入您檔案系統上的任何目錄。
2. 使用 WebLogic Server 主控台來安裝示範應用程式。
3. 使用 WebLogic Server 主控台來建立下列使用者：

   ```
   Banker1
   Banker2
   Banker3
   Banker4
   ```

4. 使用 WebLogic Server 主控台來新增群組至 PDDemoApp 中的 BankMembersRole。這可以是已存在的群組，或您可以使用 WebLogic Server 主控台來建立新的群組。另外，將上面建立的使用者新增至 BankMembersRole。

   如需使用 WebLogic Server 主控台的指示，請參閱 WebLogic Server 說明文件。

5. 如果您已在上面的步驟，將群組新增至 BankMembersRole，請將上面建立的所有使用者（Banker1、Banker2、Banker3、Banker4）新增至群組。如果您已個別地將使用者加入 BankMembersRole，請略過這個步驟。
6. 如果要存取示範應用程式，請存取下列 URL。

   http://*WebLogic_Server_host*:*WebLogic_Server_listening_port*/pddemo/PDDemo

利用上面定義的使用者之一來進行身份驗證。

WebLogic_Server_host 是 WebLogic Server 系統的主機名稱。

WebLogic_Server_listening_port 是 WebLogic Server 監聽所在的埠。

7. 驗證僅有已授與給 BankMembersRole 的使用者可以存取 Servlet。
8. 驗證已鑑定的使用者可以檢視他們自己的餘額，但不能檢視任何其他使用者的餘額。

如果要測試 WebSEAL 單一登入，請完成下列步驟：

1. 存取下列 URL：

   `https://webseald_server_name/junction_target/pddemo/PDDemo`

   WebSEAL 將提示您進行身份驗證。

   如需變數 *webseald_server_name* 及 *junction_target* 的說明，請參閱第 31 頁的『第 6 部份：配置 WebLogic Server 的 WebSEAL 接合』。

   註: 請在這裡使用 HTTPS，因爲預設 WebSEAL 行爲會阻止透過 HTTP 進行「基本」或「套表型」鑑定。
2. 以上面定義的使用者之一來進行身份驗證。

   這個處理程序可讓使用者對 WebLogic Server 進行單一登入，而且不需第二次鑑定，就可以呼叫 Servlet。當透過 WebSEAL 存取時，PDDemo 示範應用程式將顯示與直接存取 WebLogic Server 時所顯示的相同行爲。
3. 驗證已鑑定的使用者可以檢視他們自己的餘額，但不能檢視任何其他使用者的餘額。

建立測試使用者

爲了方便，如果需要許多測試使用者，將提供名爲 `users.sh` 的 Script。這個工具可用來建立或刪除多個測試使用者，方法爲建立適當的 **pdadmin** Script：

- 執行 `users.sh` 來產生兩個文字檔，**pdadmin** 可以使用它們來新增一組使用者至使用者登錄，或從其中移除一組使用者。
- 如果要使用 `users.sh` Script，請編輯此 Script，然後定義您環境適用的變數。

  這時會產生兩個檔案：`add_users.txt` 及 `remove_users.txt`。 使用這些檔案作爲 **pdadmin** Script 的輸入，如下所示：

  ```
  pdadmin -a sec_master -p <password> <add_users.txt
  pdadmin -a sec_master -p <password> <remove_users.txt
  ```

用法要訣

1. 對外部使用者啓用單一登入時，請遵守良好的安全守則。確定僅由 WebSEAL 伺服器執行鑑定。如果要達成這個目的，請停用沒有通過 WebSEAL 伺服器的內部使用者存取 WebLogic Server。

2. 在生產環境中，「Tivoli Access Manager 自訂領域」清單應該設爲 `false`。僅在測試以驗證領域是否可作業時，才將這個內容設爲 `true`。
3. 如果要透過 WebSEAL 使用 WebLogic Server *system* 及 *guest* 使用者，您必須在 Tivoli Access Manager 建立一個虛擬的 *guest*，然後設定眞正的 Guest 及 System 密碼，以符合 *configured_user* 密碼。

   不過，請注意，這表示如果您想要容許 guest 使用者不通過 WebSEAL 就可登入（如存取內部網路），您將需要外曝 *configured_user* 密碼。
4. 請明白，Tivoli Access Manager 及 WebLogic Server 兩者都會追蹤失敗的鑑定嘗試。每一項產品都會維護一個安全配置設定，來指定在鎖定使用者帳戶之前，可容許的失敗嘗試次數的上限。使用者將被這兩個設定中的較少者加以鎖定。例如，如果將 WebLogic Server 配置爲容許 5 次登入失敗，但將 Tivoli Access Manager 配置爲僅容許 3 次登入失敗，則在 3 次登入失敗後，將鎖定使用者。

疑難排解要訣

主題索引：

- 『使用套表型登入時發生單一登入失敗』
- 『無法在 HP-UX 上啓動授權服務程式』
- 『WebLogic Server 丟出記憶體異常狀況』

使用套表型登入時發生單一登入失敗

當使用者透過套表型登入來進行鑑定，且嘗試存取他們無權存取的資源時，可能會出現下列錯誤訊息：

```
來自 WebSEAL 的無法登入訊息
```

這種情況可能發生，因爲即使使用者實際上通過了鑑定，他們仍然無權存取 Web 配置區中的 Servlet。

當使用「基本鑑定」時，如果發生這種錯誤，將重新提示使用者提供鑑定明細，而不會看到上面所說明的頁面。這是預設 WebLogic Server 行爲，如果使用者直接或透過 WebSEAL 來存取頁面，將看到這種行爲。

無法在 HP-UX 上啓動授權服務程式

僅在 HP-UX 11i 上，如果 Tivoli Access Manager 授權服務程式無法啓動，請檢查 `SHLIB_PATH` 環境變數是否設定正確。這個變數必須包括 IBM Global Security Toolkit (GSKIT) 程式庫的位置。位置可以是 `/usr/lib` 或 `/opt/ibm/gsk5/lib`。

如果未設定 `SHLIB_PATH`，請輸入：

```
export SHLIB_PATH=/opt/ibm/gsk5/lib
```

如果設定了 `SHLIB_PATH`，但沒有包含這兩個目錄之一，請新增其中一個目錄至路徑。

WebLogic Server 丟出記憶體異常狀況

問題：丟出了 `java.lang.OutofMemory` 異常狀況。

說明：當執行大量的 Access Manager for WebLogic Server 階段作業時， BEA WebLogic Server 可能會用光資料堆空間。

解決方案：在 startWebLogic script 中，加大 Java Virtual Machine (JVM) 的資料堆大小上限選項。例如：

```
%JAVA_HOME%\bin\java -ms64m -mx128m
```

參閱 BEA 產品說明文件，根據應用程式架構及在主機系統上執行的處理程序（使用大量記憶體者）數目，以取得建議的資料堆大小。應用程式應該加以嚴格測試，以判定它們的環境所適用的資料堆大小。請參閱下列 URL，以取得執行緒數量及資料堆大小的效能調整注意事項：

```
http://edocs.bea.com/wls/docs61/perform/index.html
```

限制

1. Tivoli Access Manager for WebLogic 不支援遞迴的群組成員資格（群組內的群組）。
2. 集中控制使用者對 WebLogic 的 J2EE 資源的存取權限將限制爲群組之間移動中的使用者，這些使用者已指定給應用程式部署描述子中的角色。
3. Tivoli Access Manager for WebLogic 不會實作 `java.security.ACL` 介面。請注意，Tivoli Access Manager ACL 不會對應至 WebLogic Server ACL。

第 5 章 移除指示

本章說明如何解除配置以及移除 IBM Tivoli Access Manager for WebLogic Server。

請完成下列其中一節中的指示：

- 『從 Solaris 移除』
- 『從 Windows 移除』
- 第 40 頁的『從 AIX 移除』
- 第 41 頁的『從 HP-UX 移除』
- 第 41 頁的『從 Linux 移除』

從 Solaris 移除

使用 **pkgrm** 來移除 Solaris 檔案上的 Tivoli Access Manager for WebLogic。請完成下列指示：

1. 以 *root* 身份登入。
2. 使用 WebLogic Server 主控台來解除 `PDRealm` 的配置。
3. 如果要移除 Tivoli Access Manager for WebLogic，請輸入以下指令：

   ```
   # pkgrm PDWLS
   ```

   這時會出現提示，要求您確認是否要移除您選取的套件。
4. 輸入字母 **y**。

狀態訊息隨即逐一列出被移除的檔案。後移除 Script 開始執行後，畫面上會出現一則狀態訊息，指出軟體套件的移除作業已順利完成。**pkgrm** 公用程式隨即結束。

這樣就完成 Tivoli Access Manager for WebLogic 套件的移除作業了。

如果您想要移除 IBM Tivoli Access Manager Base 先決要件（Tivoli Access Manager Base runtime environment、Tivoli Access Manager Base Java 執行時期環境，以及選用的 Tivoli Access Manager 應用程式開發工具箱），請遵循 *IBM Tivoli Access Manager Base 安裝手冊*中的指示。

從 Windows 移除

使用「Windows 新增/移除程式」圖示介面，來移除 Tivoli Access Manager for WebLogic 檔案。請完成下列指示：

1. 以具備管理者專用權的 Windows 使用者登入。
2. 使用 WebLogic Server 主控台來解除配置 `PDRealm`。
3. 按兩下**新增/移除程式**圖示。
4. 選取 **Access Manager for WebLogic Application Server**。
5. 按一下**變更/移除**。

   這時會出現「選擇安裝語言」對話框。
6. 選取一種語言，然後按一下**確定**。

7. 選取**移除**圓鈕。按**下一步**。
   隨即出現「確認檔案刪除」對話框。
8. 按一下**確定**。
   這時會移除 Tivoli Access Manager for WebLogic 檔。
   此時會出現「維護完成」對話框。
9. 按一下**完成**。

這樣就完成 Tivoli Access Manager for WebLogic 的移除作業了。

如果您想要移除 IBM Tivoli Access Manager Base 先決要件（Tivoli Access Manager Base runtime environment、Tivoli Access Manager Base Java 執行時期環境，以及選用的 Tivoli Access Manager 應用程式開發工具箱），請遵循 *IBM Tivoli Access Manager Base 安裝手冊*中的指示。

從 AIX 移除

使用 **SMIT** 公用程式來移除 AIX 套件的 Tivoli Access Manager for WebLogic。請完成下列指示：

1. 以 *root* 身份登入。
2. 使用 WebLogic Server 主控台來解除 `PDRealm` 的配置。
3. 啓動 **SMIT**。選取**軟體安裝及維護**。
4. 選取**軟體維護及公用程式**。
5. 選取**移除安裝的軟體**。
6. 按一下**軟體名稱**旁邊的**列示**按鈕。
   隨即出現「多重選擇清單」視窗。這時會顯示套件名稱 **PDWLS**。
7. 選取 **PDWLS** 套件：**Access Manager for WebLogic**。
   此時會出現「移除已安裝的軟體」對話框。
8. 將**僅預覽**欄位的值變更爲**否**。
9. 在所有其他欄位中，接受預設值**否**。按一下**確定**。
10. 此時會出現「您確定嗎？」訊息視窗。按一下**確定**。
    這時會出現一則狀態訊息，指出正在安裝軟體。然後有另一則狀態訊息，列出所有已被移除的套件。
11. 按一下**完成**。
    此時會出現「移除已安裝的軟體」對話框。
12. 按一下**取消**。按一下**結束**來結束 **SMIT**。

這樣就完成 Tivoli Access Manager for WebLogic 的移除作業了。

如果您想要移除 IBM Tivoli Access Manager Base 先決要件（Tivoli Access Manager Base runtime environment、Tivoli Access Manager Base Java 執行時期環境，以及選用的 Tivoli Access Manager 應用程式開發工具箱），請遵循 *IBM Tivoli Access Manager Base 安裝手冊*中的指示。

從 HP-UX 移除

使用 **swremove** 來移除 Tivoli Access Manager for WebLogic 檔案。請完成下列指示：

1. 以 *root* 身份登入。
2. 使用 WebLogic Server 主控台來解除 `PDRealm` 的配置。
3. 如果要移除 Tivoli Access Manager for WebLogic，請輸入以下指令：

   ```
   # swremove PDWLS
   ```

   這時會出現一系列的狀態訊息。這時會出現一則狀態訊息，指出分析階段已經順利完成。 **swremove** 公用程式會將 Tivoli Access Manager for WebLogic 檔從硬碟中移除。

   移除作業完成時，**swremove** 公用程式便會結束。

這樣就在 HP-UX 上完成 Tivoli Access Manager for WebLogic 的移除作業了。

如果您想要移除 IBM Tivoli Access Manager Base 先決要件（Tivoli Access Manager Base runtime environment、Tivoli Access Manager Base Java 執行時期環境，以及選用的 Tivoli Access Manager 應用程式開發工具箱），請遵循 *IBM Tivoli Access Manager Base 安裝手冊*中的指示。

從 Linux 移除

使用 **rpm** 來移除 Tivoli Access Manager for WebLogic 檔案。請完成下列指示：

1. 以 *root* 身份登入。
2. 使用 WebLogic Server 主控台來解除 `PDRealm` 的配置。
3. 如果要移除 Tivoli Access Manager for WebLogic，請輸入以下指令：

   ```
   # rpm -e PDWLS-PD-4.1.0-0.i386.rpm
   ```

   這時會移除檔案。**rpm** 公用程式存在。

這樣就在 Linux 上完成 Tivoli Access Manager for WebLogic 的移除作業了。

如果您想要移除 IBM Tivoli Access Manager Base 先決要件（Tivoli Access Manager Base runtime environment、Tivoli Access Manager Base Java 執行時期環境，以及選用的 Tivoli Access Manager 應用程式開發工具箱），請遵循 *IBM Tivoli Access Manager Base 安裝手冊*中的指示。

附錄. 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估與驗證，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
500 Columbus Avenue
Thornwood, NY 10594
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
USA

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，有些測定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 logo
SecureWay
Tivoli
Tivoli logo

Microsoft、Windows、Windows NT 及 Windows 標誌是 Microsoft 公司在美國和（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。

〔十劃〕

〔十一劃〕

〔十二劃〕

〔十三劃〕

〔十四劃〕

〔十五劃〕

〔十七劃〕

〔十九劃〕

〔二十二劃〕

A

C

D

G

H

J

L

P

R

S

T

U

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 for WebLogic Server
使用手冊
第 4.1 版

SC40-1156-00

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

SC32-1137-00