IBM® SecureWay® Policy Director

啓動與執行

3 .0 版

SC40-0504-00

IBM® SecureWay® Policy Director

啓動與執行

3 .0 版

SC40-0504-00

備註

使用本資訊及其支援的產品之前，請先閱讀第87頁的『附錄. 注意事項』下面的一般資訊。

第一版（1999 年 10 月）

本修訂版適用於 IBM Secureway Policy Director 產品（SC40-0504-00）3.0 版，修訂層次 0；以及所有後續版次和修訂，直到新版中另有指示爲止。

本修訂版將取代 IBM SecureWay Global Sign-On，版本 2.0.200。

目錄

關於本書

本書提供了安裝及架構 IBM® SecureWay® Policy Director（Policy Director）的相關資訊。 Policy Director 伺服器可以安裝在以下的作業系統上：

- Microsoft® Windows NT®
- AIX®
- Solaris®

NetSEAT 從屬站可以安裝在以下的作業系統上：

- Windows® 95
- Windows 98
- Windows NT

本書的適用對象

本書的適用對象是負責計劃與安裝 Policy Director 的管理者。

管理者對於安裝及架構「IBM 分散式計算環境」（DCE）以及 IBM SecureWay Directory 的「輕裝備目錄存取通訊協定」（LDAP）應有所瞭解。 Policy Director 將會使用 IBM SecureWay Directory 以及「IBM 分散式計算環境」（DCE）伺服器，而後兩樣已經包含在 Policy Director 產品中。

本書的架構

本書包含以下章節：

- 第1頁的『第1章 瞭解 Policy Director』提供 Policy Director 及其元件的概觀。
- 第15頁的『第2章 系統需求』提供您的作業系統必須符合的軟硬體需求之相關資訊。
- 第19頁的『第3章 規劃 Policy Director』提供相關資訊以協助您規畫、組織以及管理 Policy Director。
- 第27頁的『第4章 安裝及架構 IBM SecureWay Directory』提供安裝與架構 IBM SecureWay Directory 3.1.1 版（LDAP）之「從屬站 SDK」及伺服器（如果選擇 LDAP 使用者登錄）的相關資訊。您必須先安裝及架構 LDAP 伺服器，然後再安裝 Policy Director。同時，在安裝 Policy Director 之前，LDAP 伺服器必須正在執行中。

- 第41頁的『第5章 安裝 Policy Director for Windows』說明在 Windows NT 作業系統上安裝及架構 Policy Director。
- 第53頁的『第6章 安裝 Policy Director for AIX』說明在 IBM AIX 作業系統上安裝及架構 Policy Director。
- 第69頁的『第7章 安裝 Policy Director for Solaris』說明在 Sun Solaris 作業系統上安裝及架構 Policy Director。
- 第81頁的『第8章 相關文件』告訴您到哪裡尋找 Policy Director 文件以及相關產品的文件。

本版次的新特性

這個版次的 Policy Director 包含以下列新特性：

- 支援 IBM SecureWay Directory 對使用者和群組證明資訊的儲存。
- 「開放群組」對「權限 API 規格」最近的更新。
- 使用 Policy Director「管理主控台」來定義和編輯「IBM 防火牆」Proxy 使用者證明的能力。
- 提供 Policy Director「證明獲取服務程式」（CAS），以支援外部身份驗證服務程式的使用。
- 使用新的 Policy Director「證明獲取服務程式」來對從屬站端進行以憑證爲基礎的身份驗證。
- 讓您使用 WebSEAL 和 Policy Director CAS 之間的「介面定義語言」（IDL）介面，撰寫自己的自訂證明獲取服務程式。 Policy Director 也會提供一般伺服器組織架構，以處理 Policy Director CAS 伺服器功能，像是啓動、伺服器登錄及信號處理。
- 除了同屬安全服務程式（GSS）通道機制外，亦可選擇使用「安全 Sockets 層次」（SSL）通道機制。
- 使用 Policy Director 指令行介面來管理登入及密碼政策。
- 使用 Policy Director「管理主控台」或指令行介面，來管理單一登入使用者、群組或資源（目標檔）。
- Web 型單一登入資源密碼管理工具。
- 整合安裝程序。

2000 年的因應

這些產品皆已完成 2000 年的因應。當您根據這些產品的相關文件來使用產品時，只要和這些產品一起使用的所有產品（例如：硬體、軟體與韌體）能和這些產品適當地交換正確的日期資料，則在跨越 20 世紀與 21 世紀時，這些產品都能正確處理、提供以及接收日期資料。

服務與支援

如要取得 IBM SecureWay FirstSecure 售品中所有產品的服務與支援，請聯絡 IBM。這些產品中有些可能會需要非 IBM 的支援。如果您是從 FirstSecure 售品中取得這些產品，相關服務與支援請聯絡 IBM。

慣用法

本書使用下列的印刷慣例：

慣例	意義
粗體	使用者介面元素，像是列示框中的勾選框、按鈕及項目。
等寬字體	語法、範例碼以及使用者必須鍵入的任何文字。
斜體	在強調與第一次使用 Policy Director 的相關術語時使用。
→	顯示功能表中一系列的選項。例如：按一下**檔案 → 執行**，就表示按一下**檔案**，然後按一下**執行**。

Web 資訊

有關 Policy Director 的最新更新資訊，請造訪下列網址：

http://www.ibm.com/software/security/policy/library

有關其它 IBM SecureWay FirstSecure 產品的更新資訊，請造訪下列網址：

http: //www.ibm.com/software/security/firstsecure/library

第1章 瞭解 Policy Director

IBM SecureWay Policy Director（Policy Director）可以是 IBM SecureWay FirstSecure 的元件，也可以當作獨立的產品。

IBM SecureWay FirstSecure 簡介

IBM SecureWay FirstSecure（FirstSecure）是 IBM 整合安全解決方案的其中一部分。 FirstSecure 是一組廣泛的整合產品，可協助您的公司完成以下的工作：

- 建立安全的電子商業環境。
- 簡化安全規劃，來減少安全所有權的總成本。
- 施行安全政策。
- 建立有效率的電子商業環境。

IBM SecureWay 產品包括：

Policy Director

IBM SecureWay Policy Director（Policy Director）提供身份驗證、授權、資料安全以及 Web 資源的管理。

Boundary Server

IBM SecureWay Boundary Server（Boundary Server）提供以下的功能：

- 過濾、Proxy 和線路層閘道的重要防火牆功能
- 對「IBM 防火牆」的虛擬專用網路（VPN）連線
- 網際網路安全的元件
- 機動碼安全解決方案

架構 GUI 可以將 Policy Director 的 Proxy 使用者功能和 Boundry Server 的「防火牆」產品緊密地整合在一起。

Intrusion Immunity

Intrusion Immunity 提供入侵偵測及防毒保護。

Trust Authority

IBM SecureWay Trust Authority（Trust Authority）支援加密法及互運性的公開金鑰基本設施（PKI）標準。 Trust Authority 提供數位式憑證的發行、重訂以及廢止的支援。這些憑證提供了一種方法來對使用者進行身份驗證，並可確保受信任的通信。

工具箱 「IBM SecureWay 工具箱」（工具箱）是一組應用程式設計介面（API），應用程式程式設計師可以利用這些 API 來將安全性納入軟體中。您可以在 FirstSecure 中取得「工具箱」。 Policy Director 和「工具箱」都包括 Policy Director API 檔案庫及文件。

由於每一個 IBM SecureWay FirstSecure 產品都可以獨立安裝，您可以控制如何規畫一個安全環境。這項功能可以減少保護環境的複雜度與成本，並加速 Web 應用程式及資源的部署。

有關 FirstSecure 元件的其他相關資訊，以及 IBM SecureWay 產品文件的列示，請參閱 FirstSecure *規劃與整合*文件。

IBM SecureWay Policy Director 簡介

Policy Director 是一個獨立的授權及安全管理解決方案，它能爲散佈各地的企業內網路與*企業外網路*提供端對端資源保護。*企業外網路*是一種「虛擬專用網路」（VPN），會使用存取控制與安全特性，限制只有選定的用戶才能使用一或多個與網際網路連接的企業內網路。

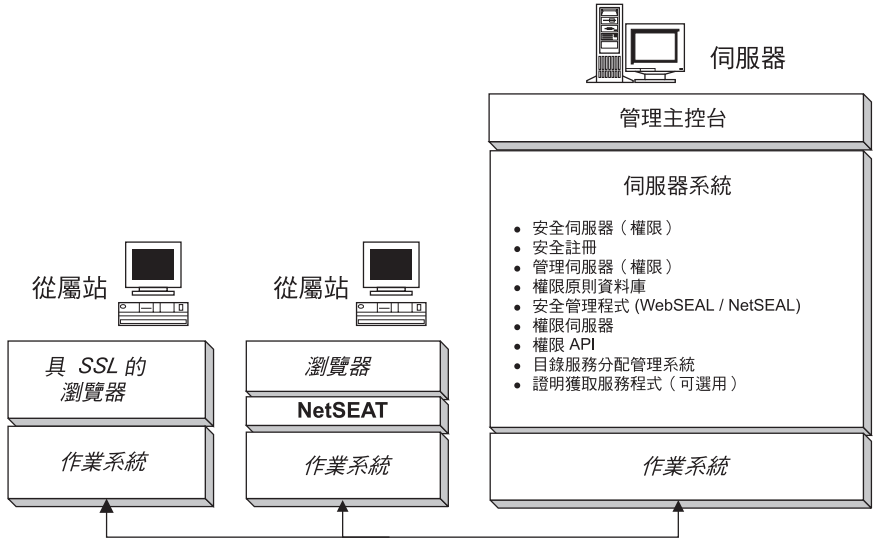
Policy Director 提供身份驗證、授權、資料安全以及資源管理等服務程式。您可使用 Policy Director 和標準的網際網路應用程式，來建置安全及管理良善的企業內網路和企業外網路。

Policy Director 可以在 Windows NT、AIX 和 Solaris 作業系統上執行。

Policy Director 元件

Policy Director 包括以下的元件：

- IBM SecureWay Directory 的「輕裝備目錄存取通訊協定」（LDAP）以及「IBM 分散式計算環境」（DCE）從屬站及伺服器
- Policy Director 基礎
- 管理伺服器
- 安全管理程式（由 WebSEAL 和 NetSEAL 組成）
- 證明獲取服務程式（CAS）
- 權限伺服器
- 授權應用程式設計介面（API）
- NetSEAT 從屬站
- 管理主控台
- 目錄服務分配管理系統（DSB）



在安裝 Policy Director 之前，您必須判斷您的網路需要哪些安全及管理功能。利用以下各節來決定您需要的 Policy Director 元件。

IBM SecureWay Directory 及 DCE 伺服器

Policy Director 將會使用 IBM SecureWay Directory 以及「IBM 分散式計算環境」（DCE）伺服器，後者已經包含在 Policy Director 產品中。

Policy Director 可使用 LDAP 使用者登錄或 DCE 使用者登錄。在安裝 Policy Director 期間，系統會提示您選取使用者登錄類型。

如果您打算使用 LDAP 使用者登錄，則在安裝 Policy Director 之前，就必須先安裝 LDAP 從屬站，並且架構 LDAP 伺服器。請遵循第27頁的『第4章 安裝及架構 IBM SecureWay Directory』中的指示。如果您打算使用 DCE 使用者登錄，就可以略過安裝及架構 LDAP 一節。

IBM SecureWay Directory 伺服器

SecureWay Directory 提供「輕裝備目錄存取通訊協定」（LDAP），將儲存、更新、擷取和交換的目錄資訊維護在一個集中位置。如果您爲使用者登錄使用 LDAP，Policy Director 會使用 LDAP 來授權給使用者。

IBM 分散式計算環境（DCE）伺服器

「分散式計算環境」（DCE）支援在不同的電腦環境中建立、使用以及維護分散式應用程式的服務程式和工具。 DCE 會形成安全領域，在這個領域中， Policy Director 伺服器可以互相對使用者進行身份驗證，並且進行安全的通信。在 Windows NT 作業系統中，NetSEAT 從屬站就是 DCE 從屬站。

Policy Director 基礎

「Policy Director 基礎」（IVBase）元件是所有 Policy Director 元件共同使用的參照軟體。當您安裝其他 Policy Director 元件時，會自動安裝這個元件，但是在您在 Windows 中安裝「管理主控台」時則不會自動安裝。

在 AIX 中，「SMIT 安裝程式」（IV.Smit）元件是屬於 IV.Base 套裝軟體的一部分。這個套裝軟體包含 SMIT 所用的架構資訊。所有的 AIX 伺服器都必須安裝這個套裝軟體。

管理伺服器

「管理」伺服器（IVMgr）是整個安全領域中的主要權限伺服器。「管理」伺服器負責控制及維護主要授權原則資料庫。所有的資料都會流經「管理」伺服器。

在您安裝任何安全管理程式或「權限」伺服器之前，必須將「管理」伺服器安裝到安全領域中的一部電腦上。但是前面二者不一定會在同一部電腦上。在給定的安全領域中，只能安裝一個「管理」伺服器案例。

每一個「管理」伺服器案例都會要求您將以下的元件安裝到「管理」伺服器所在的電腦上：

- DCE 從屬站
- LDAP 從屬站（如果您使用 LDAP 作爲使用者登錄）
- Policy Director 基礎
- 管理伺服器

安全管理程式

「安全管理程式」（IVNet）會引用存取控制原則，而這些原則是根據複本權限原則資料庫的資訊。「安全管理程式」包括以下的元件：

- 供精密的「超文字轉送通信協定」（HTTP）以及「安全 Sockets 層次」（HTTPS）存取控制使用的 WebSEAL。
- 供粗略的「傳輸控制通信協定/網際網路通信協定（TCP/IP）存取控制使用的 NetSEAL

架構及啓用這些功能時，需要 NetSEAL 和 WebSEAL 元件，預設值是停用的。

WebSEAL

WebSEAL（IVWeb）是「安全管理程式」的 HTTP 伺服器元件。 WebSEAL 是一種支援 HTTP、HTTPS 以及 NetSEAT 從屬站的安全 Web 伺服器。 WebSEAL 可以和 Policy Director「證明獲取服務程式」（CAS）合併，以支援對 Policy Director 使用者進行 X.509 憑證式的身份驗證。

NetSEAL

NetSEAL（IVTrap）可爲 TCP/IP 伺服器提供粗略的存取控制。 NetSEAL 負責控制 TCP/IP 伺服器上一組已架構埠的存取。

Policy Director 產品套件可爲網際網路和專用企業內網路上進行的從屬站/伺服器資料交換提供安全保護。 Policy Director NetSEAL 以及 Policy Director WebSEAL 都是伺服器端的產品，可控制及管理 DCE 所定義的安全領域內的網路資料。

權限伺服器

「權限」伺服器（IVAcld）負責處理在遠端模式中使用 Policy Director「權限 API」之協力廠商應用程式所提出的授權要求。您必須將「權限」伺服器安裝到協力廠商應用程式之安全領域內至少一部的電腦中。

授權應用程式設計介面

Policy Director 的「授權應用程式開發套件」或 ADK（IVAuthADK）元件都包含有 「Policy Director 授權」應用程式設計介面（API）。這個 API 可讓您建置使用 Policy Director 授權的應用程式。

Policy Director「應用程式開發套件 (ADK)」包含一個權限 API 伺服器 (AuthAPI™)，可讓開發者將 Policy Director 安全及授權特性直接建置在企業的應用程式中。 Policy Director 權限 API 提供直接存取 Policy Director「權限服務程式」。使用這些權限 API 表示開發者不再需要爲每個應用程式撰寫授權碼。

ADK 包括 C 的範例程式。

ADK 也包含 Policy Director「證明獲取服務程式」（CAS）示範伺服器以及外部權限服務程式示範伺服器的來源。

NetSEAT 從屬站

Policy Director NetSEAT 從屬站是適用於 Windows 95、Windows 98 或 Windows NT 的輕裝備從屬站。 NetSEAT 爲 Policy Director 伺服器提供安全的通信通道。

NetSEAT 從屬站可讓從屬站結合安全領域，並且使用 WebSEAL 和 NetSEAL 伺服器所提供的進階安全服務程式。 NetSEAT 可以保護從屬站所有的網路通信，容許對所有 Web 型的從屬站/伺服器流量進行端對端加密。

NetSEAT 可保護從屬站的 TCP/IP 流量，例如 Telnet 和 POP3 這類的服務程式所產生的流量。 NetSEAT 可讓系統管理者對工作站的網路活動進行粗略的控制。這種控制源自於利用安全領域的功能來對使用者進行身份驗證，以及將授權專用權附加到使用者和資源上。

管理主控台

「管理主控台」（IVConsole）是一種 Java 型的圖形式應用程式，它是用來管理 Policy Director 安全領域的安全原則。您可以使用「管理主控台」來對帳戶登錄和主要授權原則資料庫執行管理作業。「管理主控台」需要 DCE 從屬站來登入安全領域以及對 Policy Director「管理」伺服器執行安全管理遠端程序呼叫（RPC）。「管理主控台」使用 Windows 95、Windows 98 或 Windows NT 上的 NetSEAT 從屬站所提供的輕裝備 DCE 服務程式（執行期服務程式）。

目錄服務分配管理系統

「目錄服務分配管理系統」（DSB）是以「管理」伺服器元件的一部分來分送。在 Windows 95、Windows 98 或 Windows NT 工作站上執行時，「管理主控台」和 NetSEAT 從屬站在安全領域中需要一個 DSB。在起始安裝之後，DSB 通常不需要管理或架構。

證明獲取服務程式（選則性）

Policy Director「證明獲取服務程式」（CAS）是一個選擇性架構的元件。

*證明獲取*是一改變或對映由身份驗證機制提供特定的本體資訊，成爲一般、整領域表示從屬站識別的程序。此一般表示稱爲*從屬站的證明*。

當您需要獲取證明或對映時，您必須將 Policy Director 證明獲取服務程式配置成搭配 Policy Director WebSEAL 伺服器使用。 在此情況下， WebSEAL 會自動將 Policy Director 使用者對映到證明。

使用從屬站端 X.509 憑證來存取 Policy Director 的從屬站，可透過 Policy Director「證明獲取服務程式」或撰寫自己的證明獲取服務程式，將*憑證*資訊對映到 Policy Director 身份。

如果您已經在某些其他外部登錄中定義了使用者，則可以透過自訂的 CAS 伺服器，將使用者名稱對映到 Policy Director 身份。您可以撰寫並自訂自己的 CAS 伺服器，爲安全領域提供特定解決方案，以及處理身份驗證資訊，如：從屬站憑證、使用者名稱及記號。 Policy Director「證明獲取服務程式」的開發者或設計者可完全決定此身份驗證及對映服務程式的細節。 Policy Director 會將對映規則儲存至 Policy Director 外部的資料庫。 Policy Director可在 WebSEAL 和 Policy Director「證明獲取服務程式」間提供「介面定義語言（IDL）」介面。 Policy Director 亦會提供一般伺服器組織配置，以處理 Policy Director「證明獲取服務程式」伺服器功能，像是啓動、伺服器登錄及信號處理。 Policy Director「證明獲取服務程式」開發者有責任擴展證明獲取服務程式的組織配置，以實行特定應用程式所需的身份對映功能。

有關每一個 Policy Director 元件的其他資訊，請參閱 *Policy Director 管理手冊*。

Policy Director 的運作方式

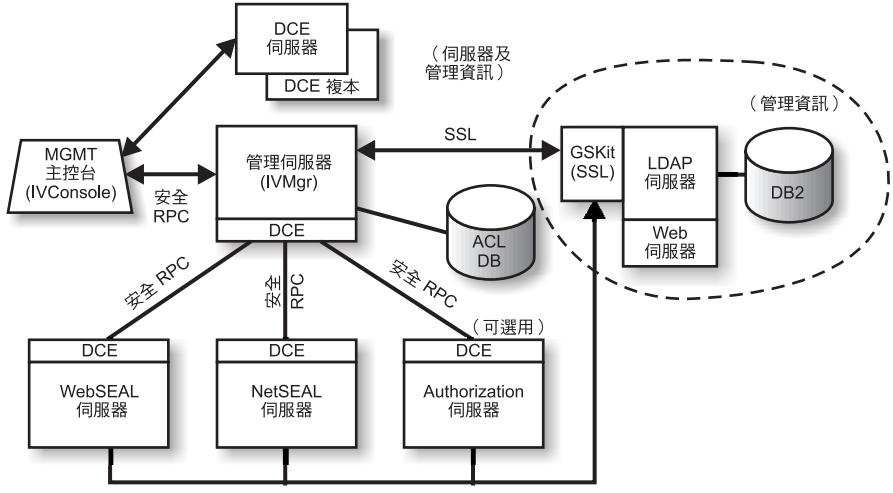
以下各節分別說明了四個實務，爲您示範 Policy Director 的一般用法：

- 使用「管理主控台」進行管理
- 使用者從 Web 瀏覽器存取受保護的 Web 資源
- 使用者利用 NetSEAT 從屬站存取受保護的 TCP/IP 伺服器

- 使用者存取受保護的協力廠商伺服器

使用「管理主控台」進行管理

下圖說明使用者使用「管理主控台」來管理 Policy Director 時的資料流程。以點虛線顯示的 LDAP 元件只有在使用 LDAP 作爲使用者登錄時才需要。



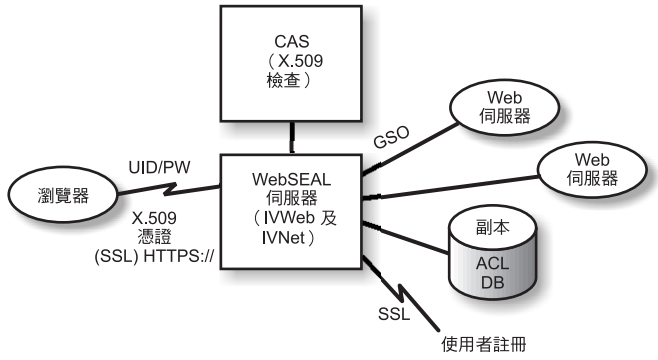
位於「管理主控台」的管理者會對安全領域進行身份驗證，並且接收證明。

當管理者從「管理主控台」來管理使用者或群組時， 「管理主控台」會透過 RPC 將要求傳送給「管理」伺服器。「管理」伺服器會透過先前使用「管理」伺服器的識別名稱（DN）和密碼所建立的 SSL 連線，將對應的變更傳送到 LDAP 伺服器。

當管理者新增、修改或引用存取控制列示（ACL）時， 「管理主控台」會透過安全 RPC 將資料傳送給「管理」伺服器。然後「管理」伺服器會將變更儲存在 ACL 資料庫的本端副本中。在修改必要的 ACL 資料庫時，「管理」伺服器會透過安全 RPC，通知所有其他的伺服器 ACL 已經變更。 WebSEAL、NetSEAL 和「權限」伺服器也會定期和「管理」伺服器進行核對，以取得 ACL 資料庫中的更新。

使用者從 Web 瀏覽器存取受保護的 Web 資源

下圖說明當使用者從 Web 瀏覽器存取受保護的 Web 資源時的資料流程。



當使用者試著存取受保護的網頁時，啓用 SSL 的瀏覽器會聯絡 WebSEAL 伺服器。 如果 WebSEAL 被配置成以從屬站憑證做爲身份驗證的依據，則 WebSEAL 會向瀏覽器要求提供 X.509 憑證。 當 WebSEAL 收到瀏覽器提供的憑證時，會將憑證傳遞給 CAS 伺服器。 CAS 會試著將收到的憑證對映至 Policy Director 所知的使用者身份。在 CAS 的配置檔中， Policy Director 管理者可建立一份表格，將憑證 DN 連結 Policy Director 使用者的 DN。當 WebSEAL 使用憑證呼叫 CAS 時， CAS 會先擷取憑證中的 DN，並在表格中尋找相符項。如果找到相符項目，CAS 會將相關的 Policy Director 使用者 DN 傳回給 WebSEAL。之後，WebSEAL 會使用這個 DN 來識別 Policy Director 使用者。如找不到相符項， CAS 會將憑證中的 DN 傳回給 WebSEAL。 在此情況下，會以憑證中的 DN 來識別 Policy Director 使用者。而 WebSEAL 伺服器會使用傳回的 DN 來擷取使用者的證明。

有關 X.509 憑證的其他資訊，請參閱以下的網址：

`http://www.ietf.org`

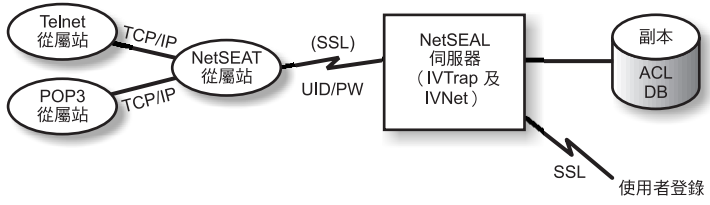
當 WebSEAL 順利完成使用者身份驗證時， WebSEAL 會使用 ACL 資料庫的本端複本來判斷使用者是否被授權用所要求的方式來存取 Web 物件。

如果 WebSEAL 伺服器與包含被存取 Web 資源的後端伺服器之間的連線是「廣域登入」（GSO）接合， WebSEAL 會爲 LDAP 中的該接合查閱 GSO 證明，並且將使用者名稱和密碼傳送給 Web 伺服器。

有關管理 GSO 資源以及 GSO 資源群組的資訊，請參閱 *Policy Director 管理手冊*中的「管理主控台」資訊。

使用者利用 NetSEAT 從屬站來存取受保護的 TCP/IP 伺服器

下圖說明當使用者利用 NetSEAT 從屬站來存取受保護的 TCP/IP 資源時的資料流程。



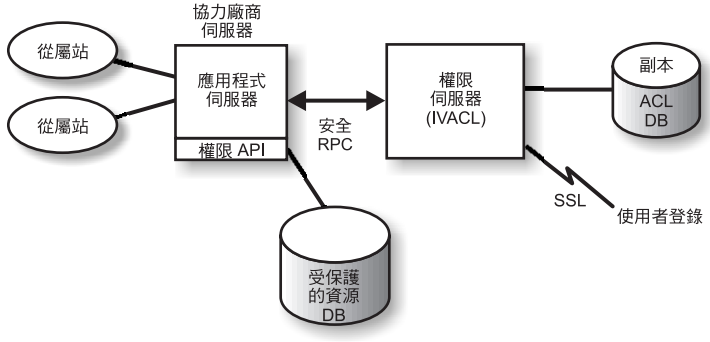
位於 Telnet 從屬站的使用者利用 Telnet 連線到由 NetSEAL 保護的伺服器，後者會指出使用者正在要求存取。 NetSEAL 會要求使用者名稱和密碼，並且藉由提供使用者資訊，然後將它和使用者登錄中儲存的值加以比較，來驗證使用者的身份。 NetSEAL 會驗證使用者可以透過指定的埠來存取電腦。

NetSEAT 會以透通方式將要求重新導向至安全 Policy Director 伺服器，透過安全 SSL 通道來傳送資訊。 NetSEAT 會使用其架構資訊來辨識同屬 TCP/IP 應用程式（如 Telnet、POP3 或 HTTP）對安全伺服器所提出的要求。 NetSEAT 透過 SSL 來使用基本的身份驗證，以建立 NetSEAT 使用者的身份和證明。建立授權之後，安全 SSL 會根據適用的安全設定來封裝及完成所要求的交易。

例如：當 Web 瀏覽器要求存取由 Policy Director「安全管理程式」保護的服務程式或資源時， NetSEAT 會以透通方式截取要求，並且將它遞送到適當的伺服器。如果這是對 Policy Director 提出的第一個要求，而且要求需經過身份驗證，NetSEAT 會提示使用者在登入對話框中輸入資訊。驗證使用者身份後，Policy Director 會以透通方式，將適當的證明連接到未來提出的每一個資訊要求。這個程序會爲 Policy Director 管理的所有 Winsock 應用程式建立一個單一登入環境。此外，Policy Director 會使用這些證明來判斷使用者是否能存取所要求的 Policy Director 保護資源。

使用者存取受保護的協力廠商伺服器

下圖說明當使用者存取受保護的協力廠商伺服器時的資料流程。



當從屬站嘗試存取協力廠商保護的伺服器上的受保護資料時，協力廠商伺服器會驗證使用者身份，並且將使用者對映到 Policy Director 使用者。應用程式伺服器會將 Policy Director 使用者資訊傳送到「權限」伺服器，後者即聯絡 LDAP（或另一個用於使用者登錄的產品，例如 DCE），並擷取使用者的證明。然後應用程式伺服器會將證明、使用者要存取的物件名稱，以及使用者要執行的作業傳送到「權限」伺服器，而後者會傳回是否應容許作業的指示。然後應用程式伺服器會容許或拒絕存取。

Policy Director 套裝軟體的內容

IBM SecureWay Policy Director 產品 3.0 版共有五張 CD。下表是這五張 CD 的標題和內容。

CD 標題	內容
IBM SecureWay Policy Director 3.0 版	• IBM Policy Director 3.0 版
IBM SecureWay Policy Director Security Service	• IBM DCE for AIX，2.2 版 • IBM DCE for Windows NT，2.2 版 • Transarc DCE for Solaris，2.0 版
IBM SecureWay Directory Version 3.1.1 for AIX	• IBM SecureWay Directory，3.1.1 版 • IBM DB2 5.2 版，含 Fix Pack 7 • IBM Global Security Kit SSL Runtime Toolkit，3.0.1 版（GSKit）
IBM SecureWay Directory Version 3.1.1 for NT	• IBM SecureWay Directory，3.1.1 版 • IBM DB2 5.2 版，含 Fix Pack 7 • IBM Global Security Kit SSL Runtime Toolkit，3.0.1 版（GSKit）
IBM SecureWay Directory Version 3.1.1 for Solaris	• IBM SecureWay Directory，3.1.1 版 • IBM DB2 5.2 版，含 Fix Pack 8 • IBM Global Security Kit SSL Runtime Toolkit，3.0.1 版（GSKit）

第2章 系統需求

您的作業環境必須符合下列章節中所討論的軟硬體基本需求。如需系統基本需求的最新相關資訊，請參閱 Policy Director 的 README 檔案。 README 檔案含有代替產品出版品的資訊。

如果要取得最新的 README 檔案，請存取 IBM SecureWay Policy Director 網站的檔案庫頁面。

`http://www.ibm.com/software/security/policy/library`

在安裝 Policy Director DCE、LDAP、NetSEAT 以及伺服器元件之前，請確定您有必要的軟硬體（列示於以下各節）。

硬體基本需求

記憶體的使用、緩衝區和快取記憶體的管理以及控制結構等，都是可以調整的。然而，基本作業系統的基礎需求、先決的 DCE 和 LDAP 從屬站的需求以及從屬站應用程式的需求，可以決定架構所需的最小磁碟空間和記憶體。

以下是 Policy Director 伺服器的硬體需求：

平台	最小磁碟空間	最小記憶體
Windows NT Server、使用 Intel 或 Intel 相容的 80486、133 MHz 或更快的速度	16MB	64MB
AIX 伺服器、執行 AIX 4.3.1 的硬體	16MB	64MB
Solaris 伺服器、執行 Solaris 2.6 的硬體	16MB	64MB

以下是 Policy Director 從屬站的硬體需求：

平台	最小磁碟空間	最小記憶體
Windows NT 從屬站，使用 Intel 或 Intel 相容的 80486，133 MHz 或更快的速度	16MB	32MB
AIX 伺服器，執行 AIX 4.3.1 的硬體	16MB	32MB
Solaris 伺服器，以及執行 Solaris 2.6 的硬體	16MB	24MB

軟體基本需求

在規畫 Policy Director 安裝時，請確定您有正確的作業系統版本以及其他必備軟體（列示於以下各節）。以下是 Policy Director 伺服器、NetSEAT 從屬站以及「管理主控台」的作業系統需求：

Policy Director 伺服器

Policy Director 伺服器可以安裝在以下的作業系統上：

- Windows NT Server 4.0 版，含 Service Pack 4 或更新的版本
- AIX 4.3.1 版或更新的版本
- Sun Solaris 2.6 版

NetSEAT 從屬站

Policy Director 從屬站可以安裝在以下的作業系統上：

- Windows NT 4.0 版，含 Service Pack 4 或更新的版本
- Windows 98
- Windows 95

管理主控台

Policy Director「管理主控台」可以安裝在以下的作業系統上：

- Windows NT Server，4.0 版，含 Service Pack 4 或更新的版本
- Windows NT、Windows 95 或 Windows 98
- AIX 4.3.1 版或更新的版本，包含 Java 執行期 1.1.6 或更新的版本
- Sun Solaris 2.6 版

其他軟體基本需求

Policy Director 需要一個 DCE 伺服器，而如果您使用 LDAP 作爲使用者登錄時，它需要一個 LDAP 伺服器。安全領域中至少有一部電腦上要有一個伺服器（不論是 LDAP 或 DCE）。 DCE 和 LDAP 從屬站以及伺服器都是 Policy Director 產品的一部分。您可以在安裝 Policy Director 之前安裝它們，或者使用正確層次的現有 DCE 和 LDAP 安裝。

Windows NT 及 AIX

在 Windows NT 和 AIX 平台上， Policy Director 伺服器需要以下的軟體：

- Windows NT Server 適用的 IBM DCE for Windows NT 2.2 版或更新的版本，或 AIX 伺服器適用的 IBM DCE for AIX，2.2 版或更新的版本
- IBM SecureWay Directory 3.1.1 版（LDAP），其中包含 DB2® 5.2 版，Fix Pack 7。只有當您使用 LDAP 作爲使用者登錄時，才需要 LDAP。
- 安全 Sockets 層次（SSL）3.0 版或更新的版本。
- Policy Director「證明獲取服務程式」（CAS）以及 WebSEAL 需要以下其中一種 Web 瀏覽器：
  - Microsoft Internet Explorer 第 4 版或更新的版本
  - Netscape Communicator 4.5 版或更新的版本
  - Netscape Navigator 4.5 版或更新的版本
- 對於 Windows 95 上的 Policy Director 從屬站，您必須具備 Winsock 2.0 版或更新的版本。

Solaris

在 Solaris 平台上，Policy Director 伺服器需要以下的軟體：

- Transarc DCE 2.0 版。
- IBM SecureWay Directory（LDAP）3.1.1 版，其中包含 DB2 5.2 版，Fix Pack 8。只有當您使用 LDAP 作爲使用者登錄時，才需要 LDAP。
- 安全 Sockets 層次 3.0 版或更新的版本。
- Policy Director CAS 以及 WebSEAL 需要以下其中一種 Web 瀏覽器：
  - Microsoft Internet Explorer 第 4 版或更新的版本
  - Netscape Communicator 4.5 版或更新的版本
  - Netscape Navigator 4.5 版或更新的版本

第3章 規劃 Policy Director

以下各節提供了準備及規畫 Policy Director 安裝與架構時所需的資訊。在規畫您的安裝前，請務必閱讀第1頁的『第1章 瞭解 Policy Director』，並且決定您需要的 Policy Director 元件。

共通架構

本節中的架構可協助您決定您的網路適用的架構。請使用第20頁的『共通架構所需的元件』中的表格來決定您的架構所需的元件。然後在 Policy Director 安裝期間選取這些元件。請注意，WebSEAL 和 NetSEAL 可以安裝在任何電腦上。以下的列示顯示了部分共通的 Policy Director 元件架構：

僅管理伺服器

執行安全領域之單一「管理」伺服器案例的伺服器。在這個實務中，「管理」伺服器本身是常駐在自己的系統中。「管理」伺服器會維護安全領域的主要授權資料庫、複製整個安全領域的資料庫，以及維護安全領域中其他 Policy Director 伺服器電腦的位置資訊。

安全管理程式以及 WebSEAL 伺服器

WebSEAL 提供兩個元件--安全管理程式（IVNet）以及 WebSEAL（IVWeb）。 WebSEAL 伺服器可保護 Web 空間。 WebSEAL 透過*智慧型接合*（或稱爲接合），來支援後端伺服器的高度可用性及容錯。

安全管理程式以及 NetSEAL 伺服器

NetSEAL 提供兩個元件--安全管理程式（IVNet）以及 NetSEAL（IVTrap）。 NetSEAL 伺服器可保護虛擬專用網路（VPN），並提供大型主機（legacy）和協力廠商網路服務程式的存取控制。

安全管理程式以及 WebSEAL 和 NetSEAL 伺服器

WebSEAL 和 NetSEAL 伺服器的組合。

權限伺服器

利用 Policy Director「權限 API」爲協力廠商應用程式提供 Policy Director 權限服務程式之存取控制的伺服器。

權限伺服器及 ADK

爲想要建置協力廠商應用程式（使用 Policy Director「權限 API」來呼叫權限服務程式）的開發者提供開發環境的伺服器。

管理主控台

一種 Java 型的圖形式應用程式，它是用來管理 Policy Director 安全領域的安全原則。在 Windows 中的「管理主控台」是不需要 IVBase 的。

全部的元件

提供所有上述架構的合併服務程式的伺服器。

共通架構所需的元件

下表列出第19頁的『共通架構』中所說明的 Policy Director 架構。這個表格顯示了每一種架構必須安裝的元件。從左向右閱讀時，指出的元件即爲正確的安裝次序。

請注意，有兩個元件會組成 WebSEAL 和 NetSEAL：

WebSEAL	安全管理程式（IVNet）和 WebSEAL（IVWeb）
NetSEAL	安全管理程式（IVNet）和 NetSEAL（IVTrap）

IVBase 的附註：

- 在 Windows 中的「管理主控台」是不需要 IVBase 的。
- 在 AIX 中，IV.Smit 會隨著 IV.Base 自動安裝。

實務	安裝套裝軟體							
	IVBase	IVMgr	IVNet	IVWeb	IVTrap	IVAcld	IVAuthADK	IVConsole
僅「管理伺服器」的單一案例	X	X						
安全管理程式以及 WebSEAL	X	X***	X	X				
安全管理程式以及 NetSEAL	X	X***	X		X			
安全管理程式以及 WebSEAL 和 NetSEAL	X	X***	X	X	X			
權限伺服器	X	X***				X		
權限伺服器以及 ADK	X	X***				X	X	
管理主控台	X							X
全部的元件	X	X***	X	X	X	X	X	X

*** 如果這是安全領域中的第一部或唯一的電腦，您就必須安裝「管理」伺服器（IVMgr）。如果這是具備現有「管理」伺服器的現有安全領域中附加的電腦，就不應該安裝另一個「管理」伺服器。任何給定的安全領域中必須只有一個「管理」伺服器。

安裝前所需的資訊

在開始安裝 Policy Director 之前，請記下安裝 Policy Director 軟體所需的系統資訊：

Policy Director 伺服器

- Cell 管理者（cell_admin）的使用者名稱
- Cell 管理者（cell_admin）的密碼
- WebSEAL：HTTP 埠（預設值）
- WebSEAL：Web 文件起始目錄

NetSEAT 從屬站（限 Windows）

- Cell 名稱
- 安全伺服器主電腦名稱
- 時間伺服器主電腦名稱
- 目錄服務分配管理系統主電腦名稱

通道機制

Policy Director 支援以下傳輸加密資料的通信協定：

- 安全 Sockets 層次（SSL）通道機制
- 同屬安全服務程式（GSS）通道機制

WebSEAL 支援 SSL加密通道所提供的資料完整性及資料私密性。 WebSEAL 及 NetSEAL 都支援 RPC。RPC 的完整性及時間戳記可避免遭到*重現式侵犯*。當流動於使用者從屬站與伺服器間的使用者資料被攫取時，即發生重現式侵犯情況。之後，即以該首位使用者之姿將該資料重映或重現於伺服器上。

SSL 通道機制：SSL 通信協定可容許信號的交換，以設定兩個工作站之間的通信。此通信協定提供網際網路的安全性及私密性。 SSL 的運作方式是利用身份驗證所使用的公開金鑰以及機密金鑰，將透過 SSL 連線轉送的資料加密。

對 Policy Director NetSEAL 伺服器使用 SSL 通道機制時，啓用 SSL。當 NetSEAT 從屬站是作爲用來保護特定埠（例如：Telnet 使用的埠）的 Policy Director NetSEAL 伺服器時，會使用這個架構。

Policy Director WebSEAL 支援 SSL 版本 2 及版本 3。

GSS 通道機制：GSS 介面（GSS API）是一種可讓應用程式存取安全服務的標準方法。 GSS 通道機制是在安全 RPC 上使用。將 NetSEAT 從屬站以支援模組方式安裝在 Policy Director for Microsoft® Windows NT® 或 Policy Director「管理主控台」時，請啓用這個選項。

GSS 通道機制是以同屬型式提供各種安全服務。它可支援基礎機制與技術範圍。它容許將應用程式攜至不同的環境中（來源層次）。 GSS 通道機制可控制雙向（彼此不相依）資料流通上的保護層次。例如：當資料自從屬站流往伺服器時，可透過大量資料加密方式加以完整保護，而當資料從伺服器流往從屬站時可能就未受到保護。

安全領域的安裝需求

Policy Director 是高度分散的安全系統，其元件可以用不同的架構安裝到一或多部電腦上。以下列示說明安全領域必須安裝哪些元件。

- DCE 服務程式
- 使用者登錄（IBM SecureWay Directory 只有在利用 LDAP 作爲使用者登錄時才需要）。
- Policy Director 伺服器
- Policy Director 管理主控台
- Policy Director 權限 ADK

如果您使用現有的 DCE 或 LDAP 安裝，請確定現有的安裝層次正確。請參閱第16頁的『其他軟體基本需求』以取得正確的層次。安裝 Policy Director 產品前，請觀察以下的相依關係。

分散式計算環境（DCE）服務程式

每一個 Policy Director 安全領域（DCE Cell）都必須在至少一部的電腦上安裝完整的 DCE 服務程式安裝，以確保 Policy Director 伺服器之間的通信。 DCE 服務程式可以常駐和 Policy Director 伺服器相同的主電腦上，或者安裝在網路的遠端主電腦上。

有關安裝 DCE 的資訊，請參閱安裝及管理手冊，以及您的平台所需的技術支援資源。請參閱第82頁的『IBM 分散式計算環境文件』以取得 DCE 文件列示。

使用以下的指引來安裝 DCE：

- 如果您要在單一主電腦系統上建立新的 Policy Director 安全領域，請執行完整的 DCE 伺服器安裝
- 如果 DCE 伺服器是位於遠端主電腦上，請將 Policy Director 安裝在區域主電腦上來建立新的安全領域。
- 如果您要將 Policy Director for Windows NT 安裝在現有的 Policy Director 安全領域中，請使用 NetSEAT 從屬站來提供對必要 DCE 服務程式的存取。請將 NetSEAT 從屬站安裝在 Windows NT Server 的 Policy Director 相同的主電腦上。

使用者登錄

Policy Director 可使用 IBM SecureWay Directory（LDAP）使用者登錄或 DCE 使用者登錄作爲其使用者登錄。

如果您使用 LDAP 作爲使用者登錄，則必須在安裝 Policy Director 之前安裝及架構 LDAP 伺服器，而且您必須同時將 LDAP 從屬站安裝在每一個 Policy Director 電腦上。

請參閱 *IBM SecureWay Directory 安裝與架構，版本 3.1.1*，以取得 LDAP 安裝資訊。請參閱第84頁的『IBM SecureWay Directory 文件』以取得此 LDAP 文件的位置。

或者請參閱 DCE 產品資訊（列示於第82頁的『IBM 分散式計算環境文件』），以取得安裝 DCE 的相關資訊。

Policy Director 伺服器

以下的基本需求適用於安裝 Policy Director 伺服器。

- 如果要適當地進行通信，所有的 Policy Director Windows NT 伺服器都需要 Policy Director NetSEAT 從屬站。
- 所有的 Policy Director 伺服器安裝都需要基礎元件，這個元件會自動安裝。
- 如果您要在安全領域中安裝*第一部*或*唯一的*電腦，就必須在電腦上安裝「管理」伺服器。
- 如果您要在具備現存「管理」伺服器的現有安全領域中安裝*附加的*電腦，請勿安裝另一個「管理」伺服器。任何給定安全領域中必須只有一個「管理」伺服器案例。
- WebSEAL、NetSEAL 以及協力廠商「權限」伺服器元件都是選用的。
- 「安全管理程式」可與 WebSEAL 合併，提供 WebSEAL HTTP 伺服器元件以及精密的 HTTP 存取控制，和 NetSEAL 合併時，則可提供 NetSEAL 粗略的 TCP/IP 存取控制元件。
- AIX 和 Solaris 上的所有 Policy Director 伺服器都需要一個完全的 DCE 從屬站，而如果您使用 LDAP 作爲使用者登錄時，則需要一個 LDAP 從屬站。

管理主控台

「管理主控台」需要安裝及架構安全領域和「管理」伺服器。「管理主控台」也需要 DCE 從屬站，而如果它是在 Windows 電腦上，則需要 NetSEAT 從屬站。

權限 ADK

請將 Policy Director 權限 ADK 安裝在應用程式開發的電腦上。「權限 ADK」可用來開發應用程式，以容許使用者存取受保護的協力廠商伺服器。「權限 ADK」需要基礎元件，這個元件是在安裝「權限 ADK」時自動安裝。

用來執行應用程式的安全領域至少必須在一部電腦上安裝「權限」伺服器。典型的開發環境會將「權限」伺服器併入與「權限 ADK」相同的系統上。

Policy Director 逐步安裝概觀

安裝 Policy Director 需要以下的步驟：

1. 如果您已經安裝前一版的 IBM SecureWay Policy Director，而且您要移轉安裝，請參閱 Policy Director 網頁的移轉資訊（請參閱第viii頁的『Web 資訊』）。
2. 驗證您的作業系統有支援 Policy Director。

   請參閱第16頁的『Policy Director 伺服器』來取得已支援作業系統的資訊。
3. 判斷哪一個伺服器元件最適合您的基本需求，以及要將這些元件安裝到哪些電腦上。

   請參閱第19頁的『共通架構』以取得協助。
4. 決定安全領域將使用 SSL 通道機制或 GSS 通道機制。

   請參閱第22頁的『通道機制』以取得其他資訊。
5. 安裝及架構 DCE 基本設施（如果不存在的話）。

   請參閱第23頁的『分散式計算環境（DCE）服務程式』以取得必要的 DCE 服務程式的概觀。
6. 決定安全領域將使用 LDAP 使用者登錄或 DCE 使用者登錄。如果您使用 IBM SecureWay Directory（LDAP）作爲使用者登錄，而且不要使用現存的 LDAP，請安裝並架構 LDAP。

   請參閱第27頁的『第4章 安裝及架構 IBM SecureWay Directory』以取得安裝 LDAP 的指示。
7. 將 DCE 和 LDAP 從屬站安裝在 Policy Director 伺服器要使用的電腦上。

   請參閱 DCE 產品資訊（列示於第82頁的『IBM 分散式計算環境文件』）以取得安裝 DCE 的資訊。
8. 安裝 Policy Director 伺服器元件。

   請參閱您要使用的作業系統平台所屬的章節。請使用下列其中一項：

   - 第41頁的『第5章 安裝 Policy Director for Windows』
   - 第53頁的『第6章 安裝 Policy Director for AIX』
   - 第69頁的『第7章 安裝 Policy Director for Solaris』
9. 如果您要使用 Policy Director CAS來進行從屬站憑證的身份驗證，請架構 Policy Director「證明獲取服務程式」（CAS）。

請參閱『架構證明獲取服務程式』以取得 Policy Director CAS 的相關資訊。

10. 安裝「管理主控台」。

    請參閱您要使用的作業系統平台所屬的章節。請使用下列其中一項：

    - 若是 Windows NT，請參閱第49頁的『在 Windows 上安裝管理主空台』。
    - 在 AIX 上，如果您要使用 DCE 使用者登錄，請參閱第64頁的『安裝管理主控台』；如果您要使用 LDAP 使用者登錄，請參閱第57頁的『架構及啓動管理主控台』。
    - 若是 Solaris，請參閱第78頁的『安裝管理主控台』。

重新安裝 Policy Director

如果您需要重新安裝任何套裝軟體，就必須先移除現存的套裝軟體，然後重新安裝想要的套裝軟體。請參閱第65頁的『移除 Policy Director』以取得指示。

架構證明獲取服務程式

Policy Director 證明獲取服務程式（CAS）是 Policy Director 其中一個可自訂的元件，可讓您用來延伸 WebSEAL 所支援的標準身份驗證機制。

Policy Director 會自動安裝。如果您要使用 Policy Director CAS 作爲證明獲取服務程式，就必須架構它。請參閱 *Policy Director 管理手冊*中的第 2 章和第 13 章，以取得瞭解和架構 Policy Director CAS 的資訊。

第4章 安裝及架構 IBM SecureWay Directory

如果您打算使用 DCE 使用者登錄，就可以略過安裝及架構 IBM SecureWay Directory（LDAP）（本節）。

在安裝 Policy Director 期間，系統會要求您選擇 LDAP 使用者登錄或 DCE 使用者登錄。

- 如果您選擇 LDAP，在安裝 Policy Director 之前，就必須安裝 IBM SecureWay Directory 3.1.1 版（LDAP）從屬站 SDK 和伺服器，然後再架構 LDAP 伺服器。
- 如果您使用 SSL 來存取 LDAP 伺服器，也必須架構 LDAP 從屬站。

安裝 LDAP 伺服器及從屬站

如果您使用 LDAP 作爲使用者登錄， Policy Director 需要一個 LDAP 伺服器以及從屬站。

安全領域中至少有一部電腦上要有一個 LDAP 伺服器。 LDAP 從屬站及伺服器是 Policy Director 產品的一部分。安裝 Policy Director 之前，您必須安裝這些元件，或者您可以使用屬於正確層次的現有 LDAP 安裝。

在安裝 LDAP 期間，請選擇安裝 **SecureWay Directory 及從屬站 SDK**。

有關安裝及架構 LDAP 的其他資訊，請參閱 *>IBM SecureWay Directory Installation and Configuration, Version 3.1.1* 文件。這本書還針對支援的作業系統，在個別作業系統 CD 中提供 HTML 格式的版本。請參閱第84頁的『IBM SecureWay Directory 文件』，以取得如何存取文件的資訊。

僅安裝 LDAP 從屬站

如果您使用 LDAP 作爲使用者登錄，就必須在即將執行 Policy Director 的每一個系統上安裝 LDAP 從屬站。 LDAP 從屬站是 Policy Director 產品的一部分。安裝 Policy Director 之前，請安裝 LDAP 從屬站。

在安裝 LDAP 期間，只有當您已經爲 Policy Director 安裝及架構正確層次的 LDAP 伺服器安裝時，才選擇要安裝 **SecureWay 從屬站 SDK**。

架構 LDAP 伺服器

如果您使用 LDAP 作爲使用者登錄，就必須在安裝第一個 Policy Director 伺服器之前架構 LDAP 伺服器。在架構 LDAP 伺服器作爲第一個 Policy Director 系統之後，在新增額外的 Policy Director 伺服器時，您不需要重新架構 LDAP 伺服器。

如果在 LDAP 伺服器架構期間啓用對 LDAP 伺服器的 SSL 存取，您需要將從屬站及伺服器金鑰環配對複製到每一部使用 SSL 存取的額外電腦上。請參閱第31頁的『啓用 SSL 存取（選則性）』以取得其他資訊

如果要架構 LDAP 伺服器，您必須爲每一個安全領域完成以下列示中的架構步驟（僅需要進行一次）：

1. 新增必需的字尾。請參閱『新增字尾』以取得指示。
2. 安裝安全綱目物件及屬性。請參閱第29頁的『安裝安全綱目物件及屬性』。
3. 啓用 LDAP 存取控制。請參閱第38頁的『啓用 LDAP 存取控制』以取得指示。
4. 啓用 SSL 存取。請參閱第31頁的『啓用 SSL 存取（選則性）』以取得指示。

如果您啓用 SSL 存取，在每次新增利用 SSL 來存取 LDAP 伺服器的 LDAP 從屬站（Policy Director 伺服器）時，請完成第35頁的『設定 SSL 存取的 LDAP 從屬站』中的步驟。

註: LDAP 管理者可指定 LDAP 資料庫中的密碼加密設定。 LDAP 容許將密碼儲存爲可讀取的文字，這可能會造成安全上的風險。請參閱您的 LDAP 文件，以取得將使用者密碼屬性設定爲適當加密層次的指示。

新增字尾

在 IBM SecureWay Directory 中，完成以下的步驟來建立新的字尾：

1. 使用 Web 瀏覽器來存取 IBM SecureWay Directory Server「Web 管理」工具，網址是

   `http://servername/ldap`

透過 Web 介面，以 LDAP 管理者的身份登入（例如：cn=root）。

2. 按一下：**字尾 → 新增字尾**。
3. 您必須在**字尾 DN** 欄位中新增以下的字尾：

   ```
   secAuthority=Default
   ```

   secAuthority=Default 的物件是在架構「管理」伺服器期間建立的。
4. 按一下**新增字尾**按鈕。
5. 如果要新增另一個字尾，按一下**新增字尾**鏈結來回到前一個視窗。
6. 必要時，爲您的 Policy Director 使用者和「廣域登入」（GSO）資料新增字尾。例如：

   ```
   o=IBM,c=US
   ```

   您可以用想要的方法來指名適用於安裝的字尾。其中 o= 是您自己的組織縮寫名稱，而 c= 是指國家。

   這個步驟會爲您的 GSO 資料以及您的使用者和群組建立字尾。這些字尾是使用 LDAP「Web 管理」工具來建立。
7. 按一下**新增字尾**按鈕。
8. 爲您要新增以及組織所需的每一個字尾重複這個步驟。
9. 當您完成新增字尾時，在目前的 LDAP「管理」工具網頁上，按一下**重新啓動伺服器**鏈結來重新啓動 LDAP 伺服器。

安裝安全綱目物件及屬性

Policy Director 使用一組 LDAP 物件和屬性來維護 LDAP 伺服器中的使用者證明。

使用 IBM SecureWay「目錄管理工具」（DMT）來判斷是否已安裝安全物件及屬性。如果尚未安裝，請安裝它們。 DMT 是隨著 IBM SecureWay Directory 套裝軟體一起安裝的。

如果要判斷是否已安裝 Policy Director 安全物件及屬性，請完成以下步驟：

1. 在 LDAP 從屬站上啓動「目錄管理工具」。

   註: 如果您收到一則訊息，指出沒有 secAuthority=Default 字尾的項目，您就可以放心地繼續進行。 secAuthority=Default 字尾的物件是在架構「管理」伺服器期間建立的。
2. 按一下**綱目 → 物件類別 → 檢視物件類別**。
3. 驗證以下所有的 Policy Director 物件和屬性都存在：

物件類別
secAuthorityInfo
secGroup
secMap
secPolicy
secPolicyData
secUser

4. 按一下**網目 → 屬性 → 檢視屬性**
5. 驗證以下所有的 Policy Director 物件和屬性都存在：

   屬性
   secUUID
   secLoginType
   secAuthority
   secAcctValid
   secPwdValid
   secDN
   secPwdMgmtBind
   secAcctExpires
   secAcctInactivity
   secAcctLife
   secPwdAlpha
   secPwdSpaces
   secPwdFailures
   secPwdLastChanged
   secPwdLastUsed

6. 根據第 29 頁步驟 3 及步驟 5 中找到的項目，執行下列其中一項。
   - 如果所有的物件都存在，就不需要進一步的動作。請繼續第31頁的『啓用 SSL 存取（選則性）』。
   - 如果*部分*（並非全部）的物件存在，請跳至步驟7。
   - 如果*沒有*物件存在，請跳至步驟8。
7. 如果找到部分（並非全部）的 Policy Director 物件及屬性，請移除現有的 Policy Director 物件及屬性。

   在 DMT 中，按一下：

   網目 → 物件類別 → 刪除物件類別，然後移除物件類別。

   然後按一下**網目 → 屬性 → 刪除屬性**，然後移除屬性。
8. 如果找不到 Policy Director 物件及屬性，請插入*IBM SecureWay Policy Director 3.0 版* CD。
9. 在指令行中，使用 **ldapmodify** 來載入網目檔。例如鍵入：

   UNIX：

```
ldapmodify -h hostname -p 389 -D cn=root -w password -f /schema/secschema.def
```

Windows：

```
ldapmodify -h hostname -p 389 -D cn=root -w password -f x:\schema\secschema.def
```

其中 *x:* 是 Windows 光碟機的代號。

10. 如果您打算使用 Policy Director 來管理 SecureWay Boundary Server 使用者，也必須從 Policy Director 綱目檔新增物件及屬性：

    在指令行中，使用 **ldapmodify** 指令來載入綱目檔。例如鍵入：

    Windows：

    ```
    ldapmodify -h hostname -p 389 -D cn=root -w password -f x:\schema\puschema.def
    ```

    UNIX：

    ```
    ldapmodify -h hostname -p 389 -D cn=root -w password -f /schema/puschema.def
    ```

    其中 *x:* 是光碟機的代號。

啓用 SSL 存取（選則性）

如果不需要對 LDAP 伺服器進行 SSL 存取，請略過本節。請跳至第38頁的『啓用 LDAP 存取控制』。

如果您的 LDAP 伺服器需要 SSL 存取，請繼續閱讀本節。只有第一次設定 LDAP 伺服器和 LDAP 從屬站之間的 SSL 通信時，才需要執行這個程序。

您可以選擇啓用 SSL 來保護 Policy Director 伺服器和 LDAP 伺服器之間的通信。

IBM 廣域安全套件（GSKit）SSL 執行期工具集 3.0.1 版是在安裝 LDAP 期間安裝。 GSKit 提供兩種版本的「金鑰管理工具」--一個是視窗化的版本 **ikmguiw**，另一個是非視窗化的版本 **ikmgui**。在以下的程序中，每次呼叫 **ikmguiw** 時，您可以使用任一版本。

有關如何使用這個工具的完整指示，可以在 LDAP 文件中取得。請參閱第84頁的『IBM SecureWay Directory 文件』。

或者，您可以遵循這些簡化的程序，特別啓用 Policy Director 來進行 SSL 存取。

建立金鑰資料庫檔案及憑證

如果要在 LDAP 上啓用 SSL 支援，伺服器必須具備一個憑證來指出這項支援，而且憑證可作爲*個人憑證*使用。這個個人憑證就是伺服器傳送給從屬站來容許從屬

站對伺服器進行身份驗證的憑證。憑證和公用及私密金鑰配對是儲存在金鑰資料庫檔案中。通常，客戶會向「憑證管理中心」（CA）（例如 VeriSign）取得*已簽名的憑證*。

然而，您也可以使用*自行簽名*的憑證。如果使用自行簽名的憑證，則產生憑證的機器會成爲 CA。

使用 GSKit 的「金鑰管理工具」（**ikmguiw**）來建立金鑰資料庫檔案及憑證。建立金鑰資料庫檔案及憑證（自行簽名或已簽名的）：

1. 請確定「IBM 廣域安全套件（GSKit）SSL 執行期工具集 3.0.1 版」以及 Java 型「金鑰管理工具」已同時安裝在 LDAP 伺服器以及即將使用 SSL 的任何 LDAP 從屬站上。

   Windows： `C:\Program Files\IBM\GSK\bin\ikmguiw.exe`

   Solaris： `/opt/IBM/GSK/bin/ikmguiw`

   AIX： `/usr/lpp/ibm/gsk/bin/ikmguiw`
2. 啓動「IBM 金鑰管理」工具（**ikmguiw**）。
3. 按一下**金鑰資料庫檔案 → 新增**。
4. 驗證 **CMS 金鑰資料庫檔案**是選取的金鑰資料庫類型。
5. 將您要放置金鑰資料庫檔案的位置資訊鍵入**檔名**及**位置**欄位中。金鑰資料庫檔案的副檔名是 *.kdb*。
6. 按一下**確定**。
7. 輸入金鑰資料庫檔案的密碼，然後予以確認。

   請記住這個密碼，因爲在編輯金鑰資料庫檔案時會需要它。
8. 接受預設的到期時間，或者根據組織的需求來改變它。
9. 如果您想要遮住密碼，並且將它儲存到隱藏檔中，請按一下**將密碼隱藏到檔案中**。

   某些應用程式可以使用隱藏檔，所以應用程式不必知道密碼就能使用金鑰資料庫檔案。隱藏檔的位置和名稱和金鑰資料庫檔案相同，而其副檔名爲 *.sth*。
10. 按一下**確定**。

這樣便可建立金鑰資料庫檔案。此外還有一組預設的簽名者憑證。這些簽名者憑證是已辨識的預設「憑證管理中心」。

建立個人憑證

如果您打算使用「憑證管理中心」（如 VeriSign）的憑證，您必須從 CA 要求憑證，然後在完成之後予以接收。完成第33頁的『接收憑證』中的步驟。

接收憑證: 如果您使用來自「憑證管理中心」（如 VeriSign）的憑證，而非自行簽名的憑證，請完成以下的步驟：

1. 使用 **ikmguiw** 來向 CA 要求憑證，然後將新的憑證接收到您的金鑰資料庫檔案中。
2. 按一下金鑰資料庫檔案的**個人憑證申請要求**區段。
3. 按一下**新增**。
4. 填入所有的資訊以產生可傳送至「憑證管理中心」的要求。
5. 按一下**確定**。
6. 在 CA 傳回憑證後，您可以將它安裝到您的金鑰資料庫檔案中，方法是按一下**個人憑證**區段，然後按一下**接收**。
7. 在將 LDAP 伺服器的憑證置於金鑰資料庫檔案中後，您可以架構 LDAP 伺服器來啓用 SSL。

如果您的憑證尚無法辨識，請將 CA 的憑證複製到從屬站機器。

如果您的憑證是由已辨識的 CA（如 VeriSign）所產生，則不需要採取任何進一步的動作。請跳至 第34頁的『架構 LDAP 伺服器來啓用 SSL』。

建立自行簽名的憑證: 如果您打算使用來自「憑證管理中心」（如 VeriSign）的憑證，而非自行簽名的憑證，請完成以下的步驟。『接收憑證』。

新建自行簽名的憑證，並將它儲存到資料庫檔案中：

1. 按一下**建立 → 新的自行簽名憑證**。
2. 在**金鑰標籤**欄位中鍵入 GSKit 可在「金鑰資料庫」中用來指出這個新憑證的名稱。

   例如：標籤可以是 LDAP 伺服器的機器名稱。
3. 接受**版本**欄位的預設值（這個值是 X509 V3）以及**金鑰大小**欄位的預設值。
4. 接受預設的機器名稱，或是在這個憑證的**共通名稱**欄位中輸入不同的識別名稱。
5. 在**組織**欄位中輸入公司名稱。
6. 完成任何選用的欄位，或保持欄位空白。
7. 接受**國家**欄位的預設值，以及**有效期間**欄位的預設值（365），或變更它們以符合您本身組織的需求。
8. 按一下**確定**。

   GSKit 會產生一個新的公用及私密金鑰配對，然後建立憑證。

如果您在金鑰資料庫檔案中有一個以上的個人憑證， GSKit 會查詢您是否要將這個金鑰當作資料庫中的預設金鑰。您可以接受其中一個作爲預設值。在選取要使用的憑證實，如果沒有提供標籤，則執行期會使用預設的憑證。

這樣便可建立 LDAP 伺服器的個人憑證。它應該會出現在金鑰資料庫檔案的「個人憑證」區段中。請使用「金鑰管理工具」中間的功能表列來選取金鑰資料庫檔案中保留的憑證類型。

接下來，您必須將 LDAP 伺服器的憑證擷取到以 Base64 編碼的 ASCII 資料檔。

擷取自行簽名的憑證

如果您的憑證是自行簽名的，您必須從金鑰資料庫檔案中擷取簽名者的憑證。請繼續執行這個擷取程式。

解壓縮是用來設定從屬站機器。如果您在第33頁的『建立自行簽名的憑證』中建立了自行簽名的憑證，它也會出現在金鑰資料庫檔案的**簽名者憑證**區段中，因爲它是自行簽名的憑證。當您位於「金鑰資料庫」的「簽名者憑證」區段中時，請驗證新的憑證出現在此。

解開簽名者憑證的壓縮：

1. 使用 **ikmguiw** 來將 LDAP 伺服器的憑證解壓縮到以 Base64 編碼的 ASCII 資料檔。這個檔案將在第35頁的『設定 SSL 存取的 LDAP 從屬站』的程序中使用。
2. 選取您剛才第33頁的『建立自行簽名的憑證』中新增的自行簽名憑證。
3. 按一下**解開憑證**。
4. 按一下**Base64 編碼的 ASCII 資料**作爲資料類型。
5. 爲新解開的憑證鍵入一個憑證檔名。憑證檔的副檔名是 *.arm*。
6. 鍵入您要儲存解開憑證的位置。
7. 按一下**確定**。
8. 將這個解開的憑證複製到 LDAP 從屬站機器。
9. 您可以架構 LDAP 伺服器來啓用 SSL。

架構 LDAP 伺服器來啓用 SSL

架構 LDAP 伺服器來啓用 SSL：

1. 如果您要使用 LDAP 作爲使用者登錄，請確定您已經安裝 LDAP 伺服器，而且它正在執行中。請參閱第27頁的『第4章 安裝及架構 IBM SecureWay Directory』以取得完整指示。
2. 利用以下的 URL 來使用 Web 型的 LDAP 管理工具：

   `http://servername/ldap`

其中 *servername* 是 LDAP 伺服器機器的名稱。

3. 如果您尚未登入，請以 LDAP 管理者的身份登入（例如：cn=root）。
4. 按一下**伺服器 → SSL**。
5. 按一下**開啓 SSL**，它是用來啓用 SSL 以及非 SSL，或按一下 **僅 SSL**，作爲您要設定的 SSL 狀態。
6. 按一下**伺服器身份驗證**作爲身份驗證方法的類型。
7. 鍵入一個埠號，或接受預設的埠號 636。
8. 鍵入您在建立金鑰資料庫檔案及憑證的步驟 5 中指定的金鑰資料庫路徑和檔案名稱。

   金鑰資料庫檔案的副檔名是 *.kdb*。
9. 在**金鑰標籤**欄位中，鍵入您將 LDAP 伺服器的憑證儲存到「金鑰資料庫」中時，用來指出這個新憑證的名稱。例如：標籤可以是 LDAP 伺服器的機器名稱。
10. 輸入金鑰資料庫檔案的密碼，然後予以確認。或者，如果您要 LDAP 伺服器使用隱藏檔，您可以將密碼欄位保持空白。
11. 按一下**引用**。
12. 按一下**重新啓動伺服器**鏈結來重新啓動 LDAP 伺服器，以容許變更生效。

測試 SSL 存取: 如果要測試 SSL 已經啓用，請從 LDAP 伺服器指令行輸入以下指令：

```
ldapsearch -h servername -Z -K keyfile -P key_pw -b "" -s base \
objectclass=*
```

無法將指令都輸入到同一行時，才需要這個指令中的反斜線（\）。

其中：

選項	說明
servername	LDAP 伺服器的 DNS 主電腦名稱。
keyfile	產生的金鑰環的完整路徑名稱。
key_pw	產生的金鑰環的密碼。

這個指令會傳回 LDAP 基本資訊，包括 LDAP 伺服器的字尾。

伺服器 SSL 的設定已經完成。接下來，請設定 SSL 存取的 LDAP 從屬站。

設定 SSL 存取的 LDAP 從屬站

在設定 SSL 存取的 LDAP 伺服器後，您必須設定 SSL 存取的 LDAP 從屬站。

建立金鑰資料庫檔案: 確定 GSKit 已經安裝在從屬站上，然後使用第31頁的『建立金鑰資料庫檔案及憑證』中所說明的「IBM 金鑰管理工具」來建立新的金鑰資料庫檔案。

爲了讓從屬站能夠對 LDAP 伺服器進行身份驗證，從屬站必須辨識建立 LDAP 伺服器憑證的「憑證管理中心」（簽名者）。如果 LDAP 伺服器使用自行簽名的憑證，則必須啓用從屬站來辨識之前產生 LDAP 伺服器憑證作爲受信的根鑰匙（憑證管理中心）的機器。

新增簽名者憑證: 在建立金鑰資料庫檔案後新增簽名者憑證：

1. 確定在第34頁的『擷取自行簽名的憑證』中從金鑰資料庫檔案解壓縮的憑證已經複製到從屬站機器上。如果尚未複製它，請現在複製它。
2. 按一下從屬站 CMS 金鑰資料庫檔案的**簽名者憑證**區段。
3. 按一下**新增**。
4. 按一下**Base64 編碼的 ASCII 資料**來設定資料類型。
5. 指出憑證的檔名及其位置。憑證檔的副檔名是 *.arm*。
6. 按一下**確定**。
7. 爲您要新增的簽名者憑證鍵入一個標籤。例如：您可能要使用 LDAP 伺服器的機器名稱作爲標籤。
8. 按一下**確定**。

   自行簽名的憑證會出現在從屬站的「金鑰資料庫」中，以作爲簽名者憑證。
9. 強調顯示新增的簽名者憑證，然後按一下**檢視/編輯**。
10. 確定**將憑證設定為受信的根鑰匙**已經選取，以確定它已經標示爲受信的根鑰匙。

    如果 LDAP 伺服器的憑證是由一般的「憑證管理中心」所產生，請確定「憑證管理中心」是列爲簽名者憑證，並且標示爲受信的根鑰匙。如果不是，則新增「憑證管理中心」的憑證作爲簽名者憑證，然後指出它是受信的根鑰匙。

此時，從屬站應該可以建立對 LDAP 伺服器的 SSL 階段作業。

測試 SSL 的啓用: 如果要測試 SSL 已經啓用，請從 LDAP 從屬站指令行輸入以下指令：

```
ldapsearch -h servername -Z -K client_keyfile -P key_pw -b "" \
-s base objectclass=*
```

無法將指令都輸入到同一行時，才需要這個指令中的反斜線（\）。

其中：

選項	說明
servername	LDAP 伺服器的 DNS 主電腦名稱。
client_keyfile	產生的金鑰環的完整路徑名稱。
key_pw	產生的金鑰環的密碼。

這個指令會傳回 LDAP 基本資訊，包括 LDAP 伺服器的字尾。

SSL 的設定已經完成。

使用 LDAP 伺服器及從屬站的身份驗證類型（選則性）

這個架構區段是可選擇的：

1. 完成第34頁的『架構 LDAP 伺服器來啓用 SSL』中說明的程序。但是，請勿將 LDAP 伺服器架構爲**伺服器身份驗證**，而是選取要執行**伺服器及從屬站身份驗證**。

   在此情形下，在伺服器將其憑證傳送至從屬站，而從屬站也已經對其進行身份驗證之後，伺服器會要求從屬站的憑證。如果爲從屬站和伺服器二者架構 LDAP 伺服器，則您也必須爲從屬站機器建立憑證。
2. 在從屬站機器上，根據這些程序中的說明，爲從屬站機器建立憑證：
   - 第31頁的『建立金鑰資料庫檔案及憑證』
   - 第33頁的『建立自行簽名的憑證』（如果您的憑證是自行簽名的憑證），或者 第33頁的『接收憑證』（如果憑證是簽名者憑證）。
   - 第34頁的『擷取自行簽名的憑證』
   - 第34頁的『架構 LDAP 伺服器來啓用 SSL』
3. 在 LDAP 伺服器上，當從屬站的個人憑證建立完成，並且新增到從屬站的金鑰資料庫檔案之後，建立從屬站憑證的「憑證管理中心」必須被視爲簽名者憑證（受信的根鑰匙）。根據第36頁的『新增簽名者憑證』中的說明，「憑證管理中心」憑證會新增至 LDAP 伺服器的「金鑰資料庫」。

測試 SSL 存取: 在 LDAP 伺服器辨識建立從屬站個人憑證的「憑證管理中心」後，便可使用以下的指令來測試設定：

```
ldapsearch -h servername -Z -K client_keyfile -P key_pw -N client_label \
-b "" \ -s base objectclass=*
```

無法將指令都輸入到同一行時，才需要這個指令中的反斜線（\）。

其中：

選項	說明
servername	LDAP 伺服器的 DNS 主電腦名稱。
client_keyfile	產生從屬站金鑰環的完整路徑名稱。
key_pw	產生的金鑰環的密碼。
client_label	與金鑰相關聯的標籤（如果有的話）。這個欄位是選用的，而且只有將 LDAP 伺服器架構爲同時執行伺服器和從屬站身份驗證時才需要。

這個指令會傳回 LDAP 基本資訊，包括 LDAP 伺服器的字尾。請注意，**-N** 參數會指定將從屬站個人憑證新增至從屬站金鑰資料庫檔案時所指定的標籤。

請勿指定 LDAP 伺服器的簽名者憑證標籤。 **-N** 參數會對 GSKit 指定在要求時要將哪一個從屬站憑證傳送給伺服器。如果沒有指定標籤，則當伺服器要求從屬站憑證時，會傳送預設的個人憑證。

SSL 的設定已經完成。

啓用 LDAP 存取控制

如果要完成 Policy Director 安全以及 LDAP 使用者登錄的整合，請完成以下的步驟來更新負責控制使用者登錄的 LDAP ACL：

1. 從 LDAP 從屬站或 LDAP 伺服器啓動「目錄管理工具」，方法是按一下**開始 → 程式集 → IBM SecureWay Directory → 目錄管理工具**。
2. 重新連結伺服器：
   a. 按一下**伺服器 → 重新連結**。
   b. 按一下**已驗證身份**。
   c. 鍵入使用者 DN（例如：cn=root）。
   d. 鍵入您的密碼。
   e. 按一下**確定**。
3. 對於每一個出現的警告訊息，按一下**確定**或關閉警告訊息視窗。
4. 對於您在第28頁的『新增字尾』之下建立的字尾，提供完整的控制給 Policy Director 安全常駐程式群組。
   a. 按一下**項目 → 新增項目**。

b. 在**項目 RDN** 中，爲您的 Policy Director 使用者及 GSO 使用者資料庫鍵入字尾。例如：

```
o=IBM,c=US
```

c. 按一下**組織**。

d. 按一下**下一步**。

此時會出現「建立 LDAP 項目」視窗。

e. 爲您的組織新增適當的資訊，然後按一下**建立**按鈕。

f. 按一下**樹狀結構 → 重新整理樹狀結構**，然後新的項目應該會出現在「瀏覽」目錄樹中。

5. 新增以下的項目到每一個負責控制 LDAP ACL 的擁有者列示中，以提供完整的控制權給 Policy Director 安全常駐程式群組：

```
cn=SecurityGroup,secAuthority=Default
```

按一下 **ACL** 標籤。

此時會出現**編輯 LDAP ACL** 視窗。

a. 在 DN 欄位中鍵入 `cn=SecurityGroup,secAuthority=Default`，然後從下拉清單中按一下**群組**。

b. 按一下**新增**按鈕。

c. 選取「授與新增、刪除及分類的權利」之下的所有勾選框。

d. 完成時，按一下**變更**，然後 `cn=SecurityGroup,secAuthority=Default` 應該會出現在您的字尾 DN 的 ACK 列示中。

e. 如果您要將一個以上的字尾新增至擁有者列示中，請爲每一個字尾重複這個程序。

您現在已經完成 LDAP 架構。

第5章 安裝 Policy Director for Windows

本章中的這幾節將告訴您如何在支援的 Windows 和 Windows NT 平台上安裝及架構 Policy Director。

在開始安裝 Policy Director 之前，確定您已經閱讀過『安裝 Policy Director for Windows 之前』中的資訊。

安裝 Policy Director for Windows 之前

在開始安裝 NetSEAT 及 Policy Director 之前，請閱讀以下的資訊：

- 在安裝 NetSEAT 和 Policy Director 之前，您必須先安裝及架構 Windows NT 伺服器。
- 您必須知道 Windows NT 領域管理者以及安全領域管理者（例如：cell_admin 帳戶）的密碼。請務必取得管理者專用權。
- 在 Windows NT 作業系統上安裝 Policy Director 伺服器時，如果您要建立新的 DCE Cell：
  - 您也必須安裝及架構 DCE 伺服器。
  - 如果您使用 LDAP 作爲使用者登錄，您也必須安裝及架構 LDAP 伺服器。
- 請熟悉與 Policy Director 部署有關的所有資訊（在第23頁的『安全領域的安裝需求』中有說明）。

安裝 NetSEAT 及 Policy Director

在開始安裝 Policy Director 之前，請務必關閉所有的應用程式。完成安裝 Policy Director 之後，您必須關機並重新啓動電腦。

完成安全領域庫存

在安裝期間，您必須提供架構安全領域的特定資訊：

- 您的安全領域名稱（DCE Cell），例如 cell_admin。
- 提供以下服務程式的電腦的名稱：
  - 安全
  - 時間
  - Cell 目錄服務程式（CDS）
  - 目錄服務分配管理系統 (DSB)

安裝 NetSEAT

Policy Director NetSEAT 設定檔會將 NetSEAT 檔案複製到您的硬碟，然後自動啓動 NetSEAT 架構公用程式。

安裝 NetSEAT：

1. 以具備管理者專用權的使用者名稱登入。
2. 將 *IBM SecureWay Policy Director 3.0 版* CD 插入光碟機。
3. 變更至 CD 的 \win32\從屬站目錄。
4. 按兩下 Setup.exe 檔，然後 InstallShield 程式會啓動。
5. 當「選擇安裝語言」視窗出現時，請選取適當的語言。
6. 按一下**下一步**，然後會出現 Policy Director「歡迎使用」視窗。
7. 按一下**下一步**。
8. 當「選擇要安裝的元件」視窗出現時，按一下**Policy Director 伺服器產品的從屬站**。
9. 按一下**下一步**。
10. 當「選擇安裝類型」視窗出現時，按一下**典型**。

    典型安裝的預設位置是：

    ```
    c:\Program Files\ibm\netseat\
    ```

    或者按一下**自訂**來指定您要安裝 NetSEAT 的磁碟機和目錄。

    此時會出現「選擇目的地位置」視窗。
11. 按一下**下一步**。

    NetSEAT 檔案會複製到您硬碟上的預設 NetSEAT 位置。此時會出現「NetSEAT 架構」視窗。

架構 NetSEAT

NetSEAT 架構作業可提供與安全領域相關的資訊給 NetSEAT，例如 DCE 伺服器名稱、位置及服務程式。

在將所有的 NetSEAT 檔案複製到硬碟之後，會出現「NetSEAT 架構」視窗（**安全領域**標籤）。

架構 NetSEAT：

1. 如果要爲新的安全領域新增項目，請按一下**新增**。

   此時會出現「新增安全領域」視窗。
2. 鍵入 NetSEAT 所屬的安全領域（DCE Cell）名稱，例如 cell_admin。
3. 選取**啓用 GSS** 或**啓用 SSL** 勾選框。
4. 按一下**確定**。

   出現「安全領域內容」視窗。
5. 如果要新增 DCE 伺服器以及它所提供的服務程式，請按一下**新增**。

   此時會出現「新增 DCE 伺服器」視窗。

   使用這個視窗來通知 NetSEAT 安全領域中現有的 DCE 伺服器，以及每一個伺服器所提供的服務程式。您可能需要新增一個以上的 DCE 伺服器。所有的服務程式都可以在一部電腦上，或者分散在數台電腦上。

   可能的實務包括：

   - **新增安全領域（一個主電腦系統）**

     如果您要建立的新安全領域只是由一個主電腦系統組成，您的主電腦系統會提供所有的 DCE 服務程式。將您的主電腦系統名稱鍵入**機器名稱**欄位中。選取一或多個服務程式。選取 DSB（即使您尚未安裝它）。
   - **新增安全領域（一個以上的主電腦）**

     如果您要建立一個新的安全領域，而 DCE 服務程式是位於另一個主電腦上，您的區域主電腦將只提供 DSB 服務程式。在此情形下，請先新增提供 DCE 服務程式（安全、時間、CDS）的 DCE 伺服器。然後，新增另一個指名爲 `localhost` 的 DCE 伺服器來代表您的區域系統，然後選取 DSB 勾選框。即使尚未安裝 DSB，您仍然可以選取它。
   - **現有的安全領域**

     如果您要在現有的安全領域中新增 Policy Director，請新增提供「安全」、「時間」以及 CDS 的 DCE 伺服器之名稱。然後新增含有可自動安裝 DSB 的 Policy Director「管理」伺服器的 DCE 伺服器名稱。選取這個系統的 DSB 勾選框。在這個實務中，所有的服務程式（包括 DSB）都可以位於同一個主電腦系統中。

6. 對於每一個伺服器，鍵入安全領域中現有伺服器的完整 DN 機器名稱（例如 SFF98732.austin.ibm.com）。
7. 對於每一個伺服器，選取伺服器的一或多個服務程式：
   - 安全
   - DSB
   - 時間
   - CDS
8. 按一下**確定**。

   「安全領域內容」視窗會顯示新的項目。
9. 必要時，重複第 43 頁的步驟 5 到步驟 8 來新增額外的伺服器和服務程式。
10. 從「安全領域內容」視窗中，接受**僅 DCE 登入**的預設進階登入架構。

    NetSEAT 安裝時不會使用「安全領域內容」視窗的整合登入區域。
11. 按一下**確定**。

    此時會出現「NetSEAT 架構」視窗。
12. 按一下**確定**。

    此時會出現「需要重新啓動系統」視窗。
13. 按一下**是**來重新啓動電腦。
14. 按一下**確定**。

    當電腦重新啓動時，會自動啓動 NetSEAT。 NetSEAT 圖示會出現在 Windows 工作列中。

    NetSEAT 安裝及架構已經完成。

驗證 NetSEAT 從屬站架構

在安裝 Policy Director 伺服器前，請驗證 NetSEAT 從屬站已順利架構到指定的安全領域中。 **netseat_ping** 可用來判斷下列服務程式是否可用：

- 安全服務程式
- 時間服務程式
- Cell 目錄服務程式
- 目錄服務分配管理系統 (DSB)

如果要驗證 NetSEAT 從屬站可以和必要的服務程式進行通信，請完成以下的步驟：

1. 按一下**開始 → 程式集 → NetSEAT → NetSEAT 登入**來以 cell_admin 的身份登入。

   或者，您可在指令行使用 **netseat_login** 指令來登入。
2. 請勿選取「PKI 登入」，除非這是您的架構特別需要的。
3. 鍵入 Policy Director 管理者的使用者名稱和密碼。
4. 按一下**確定**。
5. 在指令行中，使用 **netseat_ping** 指令來取得架構狀態。

   例如：如果將 NetSEAT 從屬站架構到稱爲 ″redback″ 的安全領域中，請在 DOS 指令提示下鍵入這個指令來取得狀態：

   ```
   netseat_ping -C redback
   ```

   此時會出現類似以下的輸出資訊：

   ```
   /.../redback:
          SecurityServers:
                       ncacn_ip_tcp:redback[ ] 可用
                       ncadg_ip_udp:redback[ ] 可用
          CdsServers:
                       ncacn_ip_tcp:redback[ ] 可用
                       ncadg_ip_udp:redback[ ] 可用
          TimeServers:
                       ncacn_ip_tcp:redback[ ] 可用
                       ncadg_ip_udp:redback[ ] 可用
          DsbServers:
                       ncacn_ip_tcp:redback[ ] 無法選用
                       ncacn_ip_udp:redback[ ] 無法選用
   ```

   然而，請注意如果您打算建立新的安全領域，則 DSB 將不會執行。在此情形下，DSB 的 **netseat_ping** 輸出會顯示成**無法選用**。在這個實務中，這是預期的輸出結果。您可以放心繼續進行 Policy Director 安裝，因爲 Policy Director 「管理」伺服器元件的安裝會自動安裝、架構以及啓動 DSB。如果 DSB 已經在執行中， DSB 的輸出會顯示成**可用**（v3.1）。
6. 如果任何 DSB 以外的服務程式無法選用，請在安裝 Policy Director 伺服器之前解決問題。

安裝 Policy Director 伺服器

在您開始安裝 Policy Director 伺服器前，請確定您知道管理者的使用者名稱和密碼。

安裝 Policy Director 伺服器元件：

1. 如果您要使用 LDAP 作爲使用者登錄，請確定您已經安裝 LDAP 伺服器，而且它正在執行中。請參閱第27頁的『第4章 安裝及架構 IBM SecureWay Directory』以取得完整指示。
2. 將 *IBM SecureWay Policy Director 3.0 版* CD 插入光碟機。
3. 變更至 CD 的 \win32\ 伺服器目錄。
4. 按一下 Setup.exe 檔，然後 InstallShield 程式會啓動。
5. 當「選擇安裝語言」視窗出現時，請選取適當的語言。
6. 按一下**下一步**，然後會出現 Policy Director「歡迎使用」視窗。
7. 按一下**下一步**。

   此時會出現「選擇目的地位置」視窗。
8. 接受程式檔的預設目錄位置，或按一下**瀏覽**按鈕來建立或選取另一個目錄。

   預設位置是： `C:\Program Files\IBM\`

   如果您將 NetSEAT 安裝在非預設的位置，請在同一位置安裝 Policy Director 伺服器。
9. 按一下**下一步**。

   此時會出現「選取元件」視窗。
10. 選取適當的 Policy Director 伺服器元件。如需選項方面的協助，請參閱第19頁的『共通架構』。

    安全領域中應該只能有一個 Policy Director「管理」伺服器（IVMgr）的案例。
11. 按一下**下一步**。
12. 如果您並未選取 WebSEAL，請跳至14。

    如果您已經選取 WebSEAL（IVWeb）元件，則出現「選擇 Web 文件起始位置」視窗。這個視窗會詢問您 Web 空間的根目錄位置。所有屬於您網站的資源都會常駐在這個目錄下。
13. 接受預設的根目錄位置，或按一下**瀏覽**按鈕來建立或選取另一個目錄。預設的位置是：

    ```
    C:\...\IBM\Policy Director\www\docs
    ```

    Policy Director 檔案現在會從 CD 複製到您的硬碟上。此時會出現安全領域「管理者登入」視窗。對於建立安全證明以及完成架構程序而言，這個步驟是必要的。
14. 完成「DCE Cell 管理者」名稱及密碼。
15. 如果您選取了「管理」伺服器元件（IVMgr），系統會提示您選取 **LDAP 登錄** 或 **DCE 登錄**。

如果您並未選取「管理」伺服器，則自動偵測現有安全領域的「使用者登錄」類型：

- 如果偵測到 LDAP 使用者登錄，安裝會依『使用 LDAP 使用者登錄』中的說明繼續進行。
- 如果偵測到 DCE 使用者登錄，安裝會依第48頁的『使用 DCE 使用者登錄』中的說明繼續進行。

16. 爲您的使用者登錄按一下下列其中一項：
    - 如果您選取 **LDAP 使用者登錄**，請跳至『使用 LDAP 使用者登錄』。
    - 如果您選取 **DCE 使用者登錄**，請跳至第48頁的『使用 DCE 使用者登錄』。

使用 LDAP 使用者登錄

如果您的 Policy Director 安全領域使用 LDAP 使用者登錄，或者您要安裝 IVMgr，而且已經選取 **LDAP 登錄**，就會出現「LDAP 伺服器資訊」視窗。

1. 鍵入 LDAP 伺服器架構的必要資訊：
    - LDAP 主電腦名稱
    - 埠號
    - SSL 埠號（只有在使用 SSL 來存取 LDAP 伺服器時才需要）
    - GSO 資料庫的 LDAP DN（例如：o=ibm,c=us）
2. 按一下**下一步**。

    此時會出現「與 LDAP 伺服器進行通信」視窗。
3. 選擇要啓用或停用 Policy Director 和 LDAP 伺服器之間的 SSL 通信。按一下**是**來啓用 SSL 通信，或按一下**否**來停用 SSL 通信。

    在 Windows NT 上，主電腦系統和 LDAP 伺服器上的所有 Policy Director 伺服器之間的 SSL 通信會啓用一次。

    如果您已經啓用 SSL 通信，請跳至步驟 4。

    如果您已經停用 SSL 通信，請跳至步驟 5。
4. 提供下列提示的值：
    - SSL 金鑰檔位置
    - SSL 檔 DN（金鑰標籤）
    - SSL 金鑰檔密碼

    請參閱第31頁的『建立金鑰資料庫檔案及憑證』以取得相關資訊。
5. 按一下**下一步**。

此時會出現「LDAP 管理者登入」視窗。

6. 完成「LDAP 管理者」名稱（例如：cn=root）以及密碼資訊，然後按一下**確定**。

   伺服器現在已經架構完成並且啓動。這可能需要花上幾分鐘。「系統資訊」視窗會出現，並且顯示伺服器的狀態，包括登錄資訊。

7. 按一下**下一步**。

   此時會出現 Policy Director「設定完成」視窗。

8. 按一下**是**來重新啓動。

   如果您選擇**否**來重新啓動選項，您稍後必須重新啓動 Windows NT 來完成架構程序。此步驟會完成 Policy Director 安裝。

9. 按一下**完成**。

   此時會提示您重新啓動系統。

使用 DCE 使用者登錄

如果您的 Policy Director 安全領域使用 DCE 使用者登錄，或者您要安裝 IVMgr，而且已經選取 **DCE 登錄**，安裝會以下列方式繼續進行：

1. 如果您已經選取 WebSEAL（IVWeb）元件，則出現「選擇 Web 文件起始位置」視窗。 這個視窗會要求您輸入 Web 空間的根目錄位置。所有屬於您網站的資源都會常駐在這個目錄下。

   如果您並未選取 WebSEAL，請跳至3。

2. 接受預設的根目錄位置，或按一下**瀏覽**按鈕來建立或選取另一個目錄。 預設的位置是：

   ```
   C:\Program Files\IBM\Policy Director\www\docs
   ```

3. 按一下**下一步**。

   Policy Director 檔案現在會從 CD 複製到您的硬碟上。 此時會出現安全領域「管理者登入」視窗。

4. 完成「LDAP 管理者」名稱及密碼資訊，然後按一下**確定**。

   伺服器現在已經架構完成並且啓動。 這可能需要花上幾分鐘。 「系統資訊」視窗會出現，並且顯示伺服器的狀態，包括登錄資訊。

5. 按一下**下一步**。

   此時會出現 Policy Director「設定完成」視窗。

6. 按一下**完成**。

   此時會提示您重新啓動系統。

7. 按一下**是**來重新啓動。

如果您選擇**否**來重新啓動選項，您稍後必須重新啓動 Windows NT 來完成架構程序。此步驟會完成 Policy Director 安裝。

架構證明獲取服務程式

Policy Director CAS CAS 會自動安裝。如果您要使用 CAS 作爲證明獲取服務程式，就必須架構它。請參閱 *Policy Director 管理手冊*中有關架構證明獲取服務程式的資訊，以取得進一步的指示。

在 Windows NT 上使用 NetSEAL 設陷

Policy Director NetSEAL（IVTrap）會設陷對特定埠所進行的要求。如果要使用 NetSEAL 設陷，您必須停止並重新啓動所有使用指定埠的應用程式。

有關架構 Policy Director NetSEAL 來設陷特定埠的其他資訊，請參閱 *Policy Director 管理手冊* 中有關 NetSEAL 的概觀資訊。

在 Windows 上安裝管理主空台

Policy Director 提供「管理主控台」來從 Windows 從屬站桌面管理 Policy Director 安全系統的許多元件。「管理主控台」可以安裝在以下的作業系統上：

- Windows 95
- Windows 98
- Windows NT 4.0 版，含 Service Pack 4 或更新的版本

每一個執行 Policy Director 的 Windows 作業系統都需要 Policy Director NetSEAT 從屬站。

NetSEAT 從屬站可以架構爲 DCE 執行期從屬站或 Policy Director 伺服器的從屬站。雖然任何一種架構對於「管理主控台」而言都是可以接受的， Policy Director 伺服器需要 Policy Director 伺服器的完整從屬站。

如果您需要重新安裝任何元件，就必須在重新安裝之前移除現有的元件。

安裝管理主控台以及伺服器元件

當您在第45頁的『安裝 Policy Director 伺服器』中安裝及架構 Policy Director 伺服器元件後，請完成以下的步驟：

1. 將 *IBM SecureWay Policy Director 3.0 版* CD 插入光碟機。
2. 變更至 \win32\ 主控台目錄。
3. 按兩下 Setup.exe 檔，然後 InstallShield 程式會啓動。

4. 當「選擇安裝語言」視窗出現時，請選取適當的語言。
5. 按一下**下一步**，然後會出現 Policy Director「歡迎使用」視窗。
6. 按一下**下一步**，然後「選擇目的地位置」視窗就會出現。
7. 指出您要安裝檔案的位置。

   檔案會複製到 Windows 電腦上的適當位置。此時會出現一個資訊視窗，指出安裝順利完成。
8. 如果系統詢問您是否要重新啓動 Windows，請按一下**是**。
9. 按一下**確定**。
10. 請跳至第51頁的『啓動管理主控台』。

安裝管理主控台，但不含伺服器元件

如果要從其他的 Windows 系統啓用 Policy Director 安全的管理，您可以將「管理主控台」安裝在沒有安裝 Policy Director 伺服器元件的 Windows 系統上。當您以這種方式安裝「管理主控台」時，可以將 NetSEAT 從屬站架構爲 DCE 執行期從屬站或 Policy Director 伺服器的從屬站。

如果要安裝「管理主控台」，但是不要安裝伺服器元件，請跳至 Windows 桌面系統，並且完成以下的步驟：

1. 驗證 Windows 作業系統是已支援的平台。請參閱第16頁的『Policy Director 伺服器』。
2. 安裝 Policy Director NetSEAT 從屬站。請遵循第42頁的『安裝 NetSEAT』中的指示
3. 驗證 NetSEAT 從屬站已經適當地架構到您將執行「管理主控台」的安全領域中。請參閱第44頁的『驗證 NetSEAT 從屬站架構』。
4. 將 *IBM SecureWay Policy Director 3.0 版* CD 插入光碟機。
5. 變更至 \win32\ 主控台目錄
6. 按兩下 Setup.exe 檔，然後 InstallShield 程式會啓動。
7. 當「選擇安裝語言」視窗出現時，請選取適當的語言。
8. 按一下**下一步**，然後會出現 Policy Director「歡迎使用」視窗。
9. 按一下**下一步**，然後「選擇目的地位置」視窗就會出現
10. 指出您要安裝檔案的位置。

    檔案會複製到 Windows 電腦上的適當位置。此時會出現一個資訊視窗，指出安裝順利完成。
11. 按一下**確定**以完成安裝。
12. 如果要啓動「管理主控台」，請跳至第51頁的『啓動管理主控台』。

啓動管理主控台

啓動「管理主控台」：

1. 確定 Policy Director 伺服器已經安裝好，而且正在執行中。
2. 按一下**開始 → 程式集 → Policy Director → 管理主控台**。

   此時會出現 Policy Director「管理主控台」視窗。
3. 以具備管理者專用權的使用者身份登入「管理主控台」，如 cell_admin。

移除 Policy Director

如果要移除 Policy Director 元件，請務必以管理者身份登入。以具備管理者證明的使用者身份登入 Windows 領域。例如：

```
dce_login cell_admin password
```

如果您嘗試移除元件，但是您沒有適當的安全領域證明，就會出現「授權失敗」訊息視窗。

您必須採取和安裝順序完全相反的順序來移除 Policy Director 元件。請使用「控制台」中的**新增/移除程式**圖示來移除 Policy Director。

如果要解除安裝整個 Policy Director，請依照以下的順序來執行以下的程序：

1. 移除「管理主控台」。
2. 移除伺服器元件。
3. 移除 NetSEAT 從屬站。

移除管理主控台

移除「管理主控台」：

1. 如果「管理主控台」正在執行中，請關閉它。
2. 跳至「控制台」中的**新增/移除程式**，然後按一下 **Policy Director 管理主控台**。
3. 按一下**新增/移除**按鈕。
4. 當系統詢問時，按一下**是**以確認您要移除程式。
5. 按一下**確定**。

移除伺服器元件

如果要移除 Policy Director 伺服器元件，您必須取得專用權及證明，然後移除這些元件。

移除伺服器元件：

1. 確定 Policy Director 伺服器已經安裝好，而且正在執行中。
2. 跳至「控制台」中的**新增/移除程式**，然後選取第一個要移除的 Policy Director 伺服器元件。
3. 依照與之前安裝時完全相反的順序，移除 Policy Director 伺服器元件。

   例如，如果您安裝所有的元件，請依照以下的次序來移除它們：

   - 權限 ADK（IVAuthADK）
   - 權限伺服器（IVAcld）。
   - NetSEAL（IVTrap）。
   - WebSEAL（IVWeb）。
   - 安全管理程式（IVNet）。
   - 管理伺服器（IVMgr）。
   - 基礎（IVBase）。這個元件一定會自動安裝。

   您可以隨時移除 Policy Director「管理主控台」。有關您安裝元件的次序的其他資訊，請參閱第25頁的『Policy Director 逐步安裝概觀』。
4. 按一下**新增/移除**按鈕。
5. 要求時，輸入「LDAP 管理者」的使用者名稱和密碼。
6. 對每一個 Policy Director 伺服器元件重複步驟 2 到步驟 5。
7. 完成時請按一下**確定**。

移除 NetSEAT 從屬站

您必須擁有 Windows NT 管理者專用權，才能移除 Policy Director NetSEAT 元件。

1. 跳至「控制台」中的**新增/移除程式**，然後按一下**安裝/解除安裝**標籤。
2. 從標籤的列示視窗中，按一下 **Policy Director NetSEAT 從屬站**。
3. 按一下**新增/移除**。
4. 按一下**確定**。

第6章 安裝 Policy Director for AIX

本章中的這幾節將告訴您如何在 AIX 作業系統上安裝及架構 Policy Director。

在開始安裝 Policy Director 之前，確定您已經閱讀過『安裝 Policy Director for AIX 之前』中的資訊

安裝 Policy Director for AIX 之前

在開始安裝 NetSEAT 及 Policy Director 之前，請閱讀以下的資訊：

- 安裝 Policy Director 伺服器時，如果您要建立新的 DCE Cell：
  - 您也必須安裝及架構 DCE 伺服器。
  - 如果您使用 LDAP 作爲使用者登錄，您也必須安裝及架構 LDAP 伺服器。
- 請熟悉與 Policy Director 部署有關的所有資訊（在第23頁的『安全領域的安裝需求』中有說明）。

安裝管理主控台

Policy Director 提供一個「管理主控台」，可用來管理 Policy Director 系統的所有元件。管理者可以選擇將「管理主控台」安裝在 AIX 系統，Windows 系統，或同時安裝在兩者上。

AIX 的「管理主控台」是以指名爲 IV.Console 的套裝軟體來分送。請使用 SMIT 來安裝及架構套裝軟體。

安裝 Policy Director

如果要在 AIX 上安裝 Policy Director，請使用以下的指示：

1. 如果您要使用 LDAP 作爲使用者登錄，請確定您已經安裝 LDAP 伺服器，而且它正在執行中。請參閱第27頁的『第4章 安裝及架構 IBM SecureWay Directory』以取得完整指示。
2. 以 root 的身份登入。
3. 將 *IBM SecureWay Policy Director 3.0 版* CD 插入光碟機。
4. 啓動 SMIT。
5. 按一下**軟體的安裝與維護**。

   此時會出現「軟體的安裝與維護」功能表。
6. 按一下**安裝與更新軟體**。

   此時會出現「安裝與更新軟體」功能表。
7. 按一下**依套裝軟體名稱安裝與更新軟體**。

   此時會出現「依套裝軟體名稱安裝與更新軟體」視窗。
8. 鍵入您要用來安裝軟體的裝置名稱。

   例如：

   - 如果您是從 CD 裝置進行安裝，可以鍵入：`/dev/cd0`
   - 如果您是從已裝載伺服器的目錄來安裝，可以鍵入：`/mnt/user/lpp/IV`

     在鍵入裝置名稱後，會出現「多重選取列示」視窗。
9. 按一下 **IV**。

   「多重選取列示」視窗會顯示 Policy Director 套裝軟體的列示。
10. 選取您要安裝的套裝軟體。

    - 如果要安裝所有的 Policy Director 套裝軟體，請按一下項目 **IV**。
    - 只有安裝部分 Policy Director 套裝軟體時，請務必觀察第23頁的『安全領域的安裝需求』中所說明的安裝相依關係。
11. 按一下**確定**。

    此時會出現 SMIT 功能表的「依套裝軟體名稱安裝與更新軟體」視窗。
12. 在標示的欄位上按一下**是**：

    自動安裝必備的軟體嗎？

    這個步驟可確定會安裝 Policy Director 基礎（IV.Base）以及 SMIT 設定（IV.smit）套裝軟體。這些套裝軟體是其他 Policy Director 套裝軟體的必備軟體。如果您選擇將這個欄位設定成**否**，請返回選擇套裝軟體功能表。請確定您已經選取 IV.Base 以及 IV.Smit。

13. 設定您的安裝所適用的其他欄位值。
14. 按一下**確定**。

    SMIT 會顯示狀態訊息，包括：

    - Policy Director 套裝軟體的前置安裝驗證。
    - 解除套裝軟體檔案壓縮期間，每一個套裝軟體的名稱。
    - 爲每一個套裝軟體建立架構功能表。
    - 指出順利完成檔案解壓縮的狀態訊息。
15. 完成檔案解壓縮時，請使用『架構 Policy Director 以及 LDAP 使用者登錄』中的資訊來架構 Policy Director 套裝軟體。如果您使用 DCE 登錄，請參閱第61頁的『架構 Policy Director 以及 DCE 使用者登錄』。

架構 Policy Director 以及 LDAP 使用者登錄

您必須安裝 Policy Director 套裝軟體，才能架構它們。如果您尚未安裝 Policy Director 套裝軟體，請參閱第54頁的『安裝 Policy Director』。

如果您安裝了 Policy Director 以及 DCE 使用者登錄，請跳至第61頁的『架構 Policy Director 以及 DCE 使用者登錄』。

您必須架構每一個已安裝的 Policy Director 套裝軟體，但是「SMIT 設定」除外。請一次架構一個套裝軟體。某些 Policy Director 套裝軟體在架構期間需要管理者來回應螢幕提示。

架構 Policy Director 套裝軟體：

1. 啓動 SMIT。

   此時會出現「系統管理」功能表。
2. 按一下**通信應用程式及服務程式**。

   此時會出現已安裝的套裝軟體列示。例如：

   - TCP/IP
   - NFS
   - DCE（分散式計算環境）
   - Policy Director
3. 按一下 **Policy Director**。

   此時會出現 Policy Director 功能表，並且提供以下選項：

   - Policy Director 架構
   - Policy Director 解除架構

4. 按一下 **Policy Director 架構**。

   此時會出現已安裝的 Policy Director 套裝軟體列示，例如：

   - Policy Director 基礎架構
   - Policy Director 管理伺服器架構
   - Policy Director 管理主控台架構
   - Policy Director 安全管理程式架構
   - Policy Director WebSEAL 架構
   - Policy Director 權限伺服器架構
   - Policy Director NetSEAL 架構
   - Policy Director 權限 ADK 架構

5. 按一下每一個套裝軟體來進行架構，一次架構一個。

   您必須根據 Policy Director 架構列示中呈現的順序來架構 Policy Director 套裝軟體。依序選取每一個套裝軟體，從頂端的項目到底端的項目。

您現在必須使用下列各節中的架構指示來架構您所選取的 Policy Director 套裝軟體。

架構基礎套裝軟體

每次您安裝任何套裝軟體時，都會將「基礎」套裝軟體安裝到電腦上。如果要架構「基礎」套裝軟體，請按一下 Policy Director 架構列示中的 **Policy Director 基礎**。

Policy Director「基礎」套裝軟體架構不需要任何使用者輸入即可完成。

架構管理伺服器

架構「管理」伺服器：

1. 按一下 Policy Director 架構列示中的 **Policy Director 管理伺服器**。

   此時會出現提示，要求您選擇使用者登錄類型。

2. 如果您使用 LDAP 作爲使用者登錄，請鍵入 2 來代表 LDAP 使用者登錄。

   此時會出現提示，要求輸入「DCE Cell 管理者」名稱及密碼。

3. 提示時，請鍵入「DCE Cell 管理者」帳戶名稱及密碼。

   如果您使用 LDAP 作爲使用者登錄，會出現一系列提示，來架構「管理」伺服器以及 LDAP 伺服器之間的通信。

4. 鍵入 LDAP 架構的必要資訊：

   - LDAP 伺服器主電腦名稱
   - LDAP 伺服器埠號

- LDAP 伺服器 SSL 埠號（選則性）

5. 鍵入 LDAP 管理使用者（例如：cn=root）的使用者名稱和密碼。 Policy Director 安全資訊現在是登錄爲 LDAP 伺服器。
6. 選擇要啓用或停用「管理」伺服器和 LDAP 伺服器之間的 SSL 通信。

   註: 您可以個別啓用或停用每一個伺服器和 LDAP 伺服器之間的 SSL 通信。在目前的情況下，您正在設定「管理伺服器」（IVMgr）和 LDAP 伺服器之間的 SSL 通信。
7. 如果您已經停用 SSL 通信，請跳至步驟 8。如果您已經啓用 SSL 通信，請爲以下的提示個別的值：
   - SSL 金鑰環檔案位置
   - SSL 金鑰標籤
   - SSL 金鑰的密碼
8. 提供 GSO 資料庫字尾的 DN（您已經在第28頁的『新增字尾』中新增）來啓用 GSO 資料庫存取。

   例如：

   ```
   o=IBM,c=US
   ```

   在架構 GSO 資料庫存取之後， Policy Director「架構管理程式」會自動架構「目錄服務分配管理系統」。此時會出現一系列的訊息，在每一個步驟完成時列出每一個自動化的步驟。

   此時會出現一則訊息，指出 IVMgr 套裝軟體安裝已經順利完成。

   可用的套裝軟體列示會重新出現。

架構及啓動管理主控台

如果要架構「管理主控台」，請按一下 Policy Director 架構列示中的 **Policy Director 管理主控台**。

Policy Director「管理主控台」架構不需要任何使用者輸入即可完成。

啓動 AIX 版的「管理主控台」：

1. 確定 Policy Director 伺服器已經安裝好，而且正在執行中。
2. 鍵入以下的指令：

```
$ /opt/intraverse/bin/ivconsole
```

或者，如果您使用 Windows 從屬站版本的「管理主控台」，請遵循第51頁的『啓動管理主控台』中的指示。

架構安全管理程式

架構安全管理程式（IVNet）：

1. 按一下 Policy Director 架構列示中的 **Policy Director 安全管理程式**。

   此時會出現一系列的提示，以整合「安全管理程式」和 LDAP 伺服器。
2. 提示時，請鍵入 LDAP 伺服器架構的必要資訊：
   - LDAP 伺服器主電腦名稱
   - LDAP 伺服器埠號
   - LDAP 伺服器 SSL 埠號（選則性）

   如果先前已經架構 Policy Director「管理」伺服器或「權限」伺服器，這些提示就不會出現。
3. 鍵入 LDAP 管理使用者的使用者名稱和密碼。 Policy Director 安全資訊現在是登錄爲 LDAP 伺服器。
4. 選擇要啓用或停用「安全管理程式」和 LDAP 伺服器之間的 SSL 通信。

   註: 您可以個別啓用或停用每一個 Policy Director 伺服器和 LDAP 伺服器之間的 SSL 通信。在目前的情況下，您正在設定「安全管理程式」（IVNet，供 WebSEAL 和 NetSEAL 使用）和 LDAP 伺服器之間的 SSL 通信。
5. 如果您已經停用 SSL 通信，請跳至步驟 6。如果您已經啓用 SSL 通信，請爲以下的提示個別的值：
   - SSL 金鑰環檔案位置
   - SSL 金鑰標籤
   - SSL 金鑰的密碼
6. 提供 GSO 資料庫字尾的 DN（您已經在第28頁的『新增字尾』中新增）來啓用 GSO 資料庫存取。

   例如：

   ```
   o=IBM,c=US
   ```

   如果先前已經架構 Policy Director「管理」伺服器或「權限」伺服器，這個提示就不會出現。

   此時會出現提示，要求輸入「DCE Cell 管理者」的名稱及密碼。
7. 提示時，請鍵入「DCE Cell 管理者」帳戶名稱及密碼。

   「安全管理程式」現在已經架構完成並且啓動。 CAS 伺服器也已經啓動。

此時會出現一則訊息，指出「安全管理程式」套裝軟體安裝已經順利完成。

架構 Policy Director WebSEAL

架構 Policy Director WebSEAL（IVWeb）：

1. 按一下 Policy Director 架構列示中的 **Policy Director WebSEAL**。

   Policy Director WebSEAL 架構功能表會出現，並顯示用來確認以下項目的值：

   - HTTP 以及 HTTPS 從屬站存取
   - 必要的傳輸控制通信協定（TCP）埠
   - 預設的 Web 文件起始目錄

2. 確認現行的架構值：

```
請檢查 Web 伺服器架構：
1. 啓用 TCP HTTP？                    是
2. HTTP 埠                            80
3. 啓用 HTTPS？                       是
4. HTTPS 埠                           443
5. Web 文件起始目錄                   /opt/Policy Director/www/docs
a. 接受架構並繼續執行安裝
x. 結束安裝
選取要變更的項目：a
```

3. 鍵入 a 以接受架構並繼續執行安裝，或輸入要變更的值的號碼。

   Policy Director「安全管理程式」架構會提示您輸入「DCE Cell 管理者」的名稱及密碼。

4. 鍵入「DCE Cell 管理者」帳戶名稱及密碼。

   Policy Director「安全管理程式」會重新啓動。

   安裝程式會架構及啓用電腦上的 Policy Director WebSEAL。

架構 Policy Director 權限伺服器

架構 Policy Director 權限伺服器（IVAcld）：

1. 按一下 Policy Director 架構列示中的 **Policy Director 權限伺服器**。

   此時會出現一或多個提示，以整合 Policy Director「權限」伺服器和 LDAP 伺服器。

2. 提示時，請鍵入 LDAP 伺服器架構的必要資訊：

   - LDAP 伺服器主電腦名稱
   - LDAP 伺服器埠號
   - LDAP 伺服器 SSL 埠號（選則性）

   如果先前已經架構 Policy Director「管理」伺服器或「權限」伺服器，這些提示就不會出現。

3. 鍵入 LDAP 管理使用者的使用者名稱和密碼。 Policy Director 安全資訊現在是登錄爲 LDAP 伺服器。
4. 選擇要啓用或停用「安全管理程式」和 LDAP 伺服器之間的 SSL 通信。

   註: 您可以個別啓用或停用每一個 Policy Director 伺服器和 LDAP 伺服器之間的 SSL 通信。在目前的情況下，您正在設定「權限」伺服器（IVAcld）和 LDAP 伺服器之間的 SSL 通信。
5. 如果您已經停用 SSL 通信，請跳至步驟 6。 如果您已經啓用 SSL 通信，請爲以下的提示個別的值：
   - SSL 金鑰環檔案位置
   - SSL 金鑰標籤
   - SSL 金鑰的密碼
6. 提供 GSO 資料庫字尾的 DN（您已經在第28頁的『新增字尾』中新增）來啓用 GSO 資料庫存取。

   例如：

   ```
   o=IBM,c=US
   ```

   如果先前已經架構 Policy Director「管理」伺服器或「權限」伺服器，這個提示就不會出現。

   此時會出現提示，要求輸入「DCE Cell 管理」的名稱及密碼。
7. 提示時，請鍵入「DCE Cell 管理者」帳戶名稱及密碼。

   「權限伺服器」現在已經架構完成並且啓動。

   此時會出現一則訊息，指出「權限」伺服器套裝軟體安裝已經順利完成。

架構 Policy Director NetSEAL

架構 Policy Director NetSEAL：

1. 按一下 Policy Director 架構列示中的 **Policy Director NetSEAL**。

   此時會出現提示，要求輸入「DCE Cell 管理者」名稱及密碼。
2. 鍵入 LDAP 管理使用者的使用者名稱和密碼。 Policy Director 安全資訊現在是登錄爲 LDAP 伺服器。

   Policy Director NetSEAL 套裝軟體的架構已完成。

Policy Director NetSEAL 會設陷對特定埠所提出的要求。如果要使用 NetSEAL 設陷，您必須停止並重新啓動所有使用指定埠的應用程式。有關使用 Policy Director NetSEAL 的其他資訊，請參閱第65頁的『在 AIX 上使用 NetSEAL 設陷』。

架構 Policy Director 權限 ADK

如果要架構 Policy Director「權限 ADK」，請按一下 Policy Director 架構列示中的 **Policy Director 權限 ADK**。

Policy Director「權限」套裝軟體架構不需要任何使用者輸入即可完成。

架構 Policy Director 證明獲取服務程式

Policy Director CAS CAS 會自動安裝。如果您要使用 Policy Director CAS作爲證明獲取服務程式，就必須架構它。如需 Policy Director CAS 的相關資訊以及如何爲 WebSEAL 伺服器架構它的資訊，請參閱 *Policy Director 管理手冊*。

架構 Policy Director 以及 DCE 使用者登錄

您必須安裝 Policy Director 套裝軟體，才能架構它們。如果您尚未安裝 Policy Director 套裝軟體，請先參閱第54頁的『安裝 Policy Director』。

如果您安裝了 Policy Director 以及 LDAP 使用者登錄，請跳至第55頁的『架構 Policy Director 以及 LDAP 使用者登錄』。

您必須架構每一個已安裝的 Policy Director 套裝軟體，但是「SMIT 設定」除外。請一次架構一個套裝軟體。某些 Policy Director 套裝軟體在架構期間需要管理者來回應螢幕提示。

架構 Policy Director 套裝軟體：

1. 啓動 SMIT。

   此時會出現「系統管理」功能表。
2. 按一下**通信應用程式及服務程式**。

   此時會出現已安裝的套裝軟體列示。例如：

   - TCP/IP
   - NFS
   - DCE（分散式計算環境）
   - Policy Director
3. 按一下 **Policy Director**。

   此時會出現 Policy Director 功能表，並且提供以下選項：

   - Policy Director 架構
   - Policy Director 解除架構
4. 按一下 **Policy Director 架構**。

此時會出現已安裝的 Policy Director 套裝軟體列示，例如：

- Policy Director 基礎架構
- Policy Director 管理伺服器架構
- Policy Director 管理主控台架構
- Policy Director 安全管理程式架構
- Policy Director WebSEAL 架構
- Policy Director 權限伺服器架構
- Policy Director NetSEAL 架構
- Policy Director 權限 ADK 架構

5. 按一下每一個套裝軟體來進行架構，一次架構一個。

   您必須根據 Policy Director 架構列示中呈現的順序來架構 Policy Director 套裝軟體。 依序選取每一個套裝軟體，從頂端的項目到底端的項目。

您現在必須使用下列各節中的架構指示來架構您所選取的 Policy Director 套裝軟體。

架構「基礎」套裝軟體

每次您安裝任何套裝軟體時，都會將「基礎」套裝軟體安裝到電腦上。如果要架構「基礎」套裝軟體，請按一下 Policy Director 架構列示中的 **Policy Director 基礎**。

Policy Director「基礎」套裝軟體架構不需要任何使用者輸入即可完成。

架構「管理」伺服器

架構「管理」伺服器：

1. 按一下 Policy Director 架構列示中的 **Policy Director 管理伺服器**。

   此時會出現提示，要求輸入「DCE Cell 管理者」名稱及密碼。

2. 提示時，請鍵入「DCE Cell 管理者」帳戶名稱及密碼。

   安裝程式會架構並啟動「管理」伺服器。

架構及啟動管理主控台

如果要架構「管理主控台」，請按一下 Policy Director 架構列示中的 **Policy Director 管理主控台**。

Policy Director「管理主控台」架構不需要任何使用者輸入即可完成。

啓動 AIX 版的「管理主控台」：

1. 確定 Policy Director 伺服器已經安裝好，而且正在執行中。
2. 鍵入以下的指令：

```
$ /opt/intraverse/bin/ivconsole
```

架構安全管理程式

架構安全管理程式（IVNet）：

1. 按一下 Policy Director 架構列示中的 **Policy Director 安全管理程式**。
2. 提示時，請鍵入「DCE Cell 管理者」帳戶名稱及密碼。

安裝程式會架構並啓動「安全管理程式」。

架構 Policy Director WebSEAL

架構 Policy Director WebSEAL（IVWeb）：

1. 按一下 Policy Director 架構列示中的 **Policy Director WebSEAL**。

   Policy Director WebSEAL 架構功能表會出現，並顯示用來確認以下項目的值：

   - HTTP 以及 HTTPS 從屬站存取
   - 必要的傳輸控制通信協定（TCP）埠
   - 預設的 Web 文件起始目錄

2. 確認現行的架構值：

```
請檢查 Web 伺服器架構：
1. 啓用 TCP HTTP？                    是
2. HTTP 埠                            80
3. 啓用 HTTPS？                       是
4. HTTPS 埠                           443
5. Web 文件起始目錄                   /opt/Policy Director/www/docs
a. 接受架構並繼續執行安裝
x. 結束安裝
選取要變更的項目：a
```

3. 鍵入 a 以接受架構並繼續執行安裝，或輸入要變更的值的號碼。

   Policy Director「安全管理程式」架構會提示您輸入「DCE Cell 管理者」的名稱及密碼。

4. 鍵入「DCE Cell 管理者」帳戶名稱及密碼。

   Policy Director「安全管理程式」會重新啓動。

   安裝程式會架構及啓用電腦上的 Policy Director WebSEAL。

架構 Policy Director 權限伺服器

架構 Policy Director 權限伺服器（IVAcld）：

1. 按一下 Policy Director 架構列示中的 **Policy Director 權限伺服器**。

此時會出現提示，要求輸入「DCE Cell 管理」的名稱及密碼。

2. 鍵入「DCE Cell 管理者」帳戶名稱及密碼。

   「權限伺服器」現在已經架構完成並且啓動。

架構 Policy Director NetSEAL

架構 Policy Director NetSEAL：

1. 按一下 Policy Director 架構列示中的 **Policy Director NetSEAL**。

   此時會出現提示，要求輸入「DCE Cell 管理者」名稱及密碼。

2. 鍵入 LDAP 管理使用者的使用者名稱和密碼。 Policy Director 安全資訊現在是登錄爲 LDAP 伺服器。

   Policy Director NetSEAL 架構已完成。

Policy Director NetSEAL 會設陷對特定埠所提出的要求。如果要使用 NetSEAL 設陷，您必須停止並重新啓動所有使用指定埠的應用程式。有關使用 Policy Director NetSEAL 的其他資訊，請參閱第65頁的『在 AIX 上使用 NetSEAL 設陷』。

架構 Policy Director 權限 ADK

如果要架構 Policy Director「權限 ADK」，請按一下 Policy Director 架構列示中的 **Policy Director 權限 ADK**。

Policy Director「權限」套裝軟體架構不需要任何使用者輸入即可完成。

架構 Policy Director 證明獲取服務程式

Policy Director CAS CAS 會自動安裝。如果您要使用 Policy Director CAS作爲證明獲取服務程式，就必須架構它。如需 Policy Director CAS 的相關資訊以及如何爲 WebSEAL 伺服器架構它的資訊，請參閱 *Policy Director 管理手冊*。

安裝管理主控台

Policy Director 提供「管理主控台」來從 Windows 從屬站桌面管理 Policy Director 安全系統的許多元件。「管理主控台」可以安裝在以下的作業系統上：

- Windows 95
- Windows 98
- Windows NT 4.0 版，含 Service Pack 4 或更新的版本
- AIX 4.3.1.0 版或更新的版本

每一個執行 Policy Director 的 Windows 作業系統都需要 Policy Director NetSEAT 從屬站。

NetSEAT 從屬站可以架構爲 DCE 執行期從屬站或 Policy Director 伺服器的從屬站。雖然任何一種架構對於「管理主控台」而言都是可以接受的， Policy Director 伺服器需要 Policy Director 伺服器的完整從屬站。

如果您需要重新安裝任何元件，就必須在重新安裝之前移除現有的元件。

在 AIX 上使用 NetSEAL 設陷

如果要使用 Policy Director NetSEAL 設陷，就必須在任何存取安全埠（已設陷）的應用程式前，先啓動 NetSEAL 常駐程式「安全管理程式」（secmgrd）。使用 /etc/inittab 項目來確保在啓動程序期間， secmgrd 是在應用程式之前啓動。

請將 NetSEAL 設陷和網路應用程式一起使用，如 Telnet、RLOGIN 以及 POP3。**inetd** 常駐程式會控制這些應用程式。 Policy Director 啓動設定 Script（/etc/iv/iv）會啓動 secmgrd，然後停止並重新啓動 inetd 常駐程式。這個程序可確保系統重新啓動後順利設陷這些應用程式。

如果您停止並重新啓動 Policy Director，您也必須停止並重新啓動任何對設陷埠提出要求的應用程式。如果要使這個程序自動化，您可以新增程式碼到 /etc/iv/iv，以便在 secmgrd 啓動後停止並啓動應用程式。使用 /etc/iv/iv Script 的技巧來停止及重新啓動 **inetd**，作爲停止和啓動其他應用程式的模版。

有關架構 Policy Director NetSEAL 來設陷特定埠的其他資訊，請參閱 *Policy Director 管理手冊* 中有關 NetSEAL 的資訊。

移除 Policy Director

在移除 Policy Director for AIX 之前，您必須先將它解除架構。

- 有關解除架構 Policy Director 的資訊，請參閱『解除架構 Policy Director 套裝軟體』。
- 有關移除 Policy Director 的資訊，請參閱第66頁的『移除 Policy Director 套裝軟體』。

如果要移除 Windows 版的「管理主控台」，請參閱

解除架構 Policy Director 套裝軟體

如果要解除架構 Policy Director 伺服器，請完成下列步驟：

1. 啓動 SMIT。
2. 按一下**通信應用程式及服務程式**。

   此時會出現「Communications 應用程式及服務程式」功能表。

3. 按一下 **Policy Director**。

   此時會出現 Policy Director 功能表。

4. 從功能表中，按一下 **Policy Director 解除架構**。

   此時會出現已架構的 Policy Director 套裝軟體列示。

   選取要解除架構的套裝軟體。可能的套裝軟體包括：

   - Policy Director 權限伺服器解除架構
   - Policy Director 權限 ADK 解除架構
   - Policy Director NetSEAL 解除架構
   - Policy Director WebSEAL 解除架構
   - Policy Director 安全管理程式解除架構
   - Policy Director 管理伺服器解除架構
   - Policy Director 管理主控台解除架構
   - Policy Director 基礎解除架構
   - IV Smit 功能表解除架構

5. 請一次解除架構一個套裝軟體。

   註: 您必須依照安裝套裝軟體的相反順序來將它們解除架構。如果要確定這個次序，請由功能表頂端的套裝軟體開始，往功能表底端逐一解除架構。

6. 如果您要解除架構 Policy Director 套裝軟體是因爲您要從電腦移除所有的 Policy Director，在解除架構所有其他的 Policy Director 套裝軟體後，請按一下 **Policy Director Smit 功能表解除架構**。

   這個步驟會從 SMIT 資料庫移除 Policy Director 套裝軟體資訊。

7. 請參閱『移除 Policy Director 套裝軟體』來移除 Policy Director。

移除 Policy Director 套裝軟體

在您嘗試移除 Policy Director 之前，請先驗證您已經取消架構 Policy Director 軟體。 第65頁的『解除架構 Policy Director 套裝軟體』提供了解除架構的指示。

移除 Policy Director：

1. 啓動 SMIT。
2. 按一下**軟體的安裝與維護**。

   此時會出現「軟體的安裝與維護」功能表。

3. 按一下**軟體維護及公用程式**。

   此時會出現「軟體維護及公用程式」功能表。

4. 按一下**移除已安裝的軟體**。

此時會出現「移除已安裝的軟體」視窗。

5. 選取要移除的 Policy Director 套裝軟體。您可以同時選取一個以上的套裝軟體。如果要移除所有的 Policy Director 套裝軟體，請鍵入 IV。

Policy Director 軟體會被移除。

移除管理主控台及 NetSEAT

Windows 上的「管理主控台」以及 NetSEAT 從屬站可以利用 InstallShield 解除安裝功能來移除：

- 移除「管理主控台」。請參閱第51頁的『移除管理主控台』以取得指示。
- 移除 NetSEAT 從屬站。請參閱第52頁的『移除 NetSEAT 從屬站』以取得指示。

第7章 安裝 Policy Director for Solaris

本章中的這幾節將告訴您如何在 Solaris 作業系統上安裝及架構 Policy Director。

在開始安裝 Policy Director 之前，確定您已經閱讀過『安裝 Policy Director for Solaris 之前』中的資訊

安裝 Policy Director for Solaris 之前

在開始安裝 Policy Director 之前，請閱讀以下的資訊：

這個版次的 Policy Director 所用的安裝程序需要使用 **pkgadd** 指令。如果要執行 **pkgadd** 指令，請在指令提示下鍵入下列指令：

```
# pkgadd -d /cdrom/cdrom0/solaris
```

請使用 **pkgadd** 指令來安裝 Policy Director 軟體。 **pkgadd** 指令通常會顯示標準的程序指示中沒有指出的補充提示。這些提示的出現是爲了回應您的系統設定及架構特定的情況。對於標準程序以外的提示，請務必回答 y。

安裝 Policy Director 之前：

- 您必須安裝 DCE 從屬站。
- 如果您使用 LDAP 作爲使用者登錄，您也必須安裝 LDAP 從屬站。

您必須在開始安裝 Policy Director 之前啓用 Transarc DCE 遠端管理特性。如果沒有啓用遠端管理特性，您就無法完成 Policy Director 安裝。

使用某些遠端管理特性可以讓「Cell 管理者」相當於本端的 Root 帳戶。 Transarc DCE 通常會停用這些遠端管理特性。然而，Policy Director 軟體需要這些特性。

請參閱 *Transarc 版本注意事項，版次 1.1*（DCE-D1002-01）的第 4.2.1 節，以取得如何啓用遠端管理特性的資訊。

安裝畫面輸出

本文件中的標準程序並未指出 **pkgadd** 指令所有可能的畫面輸出。大部分未記載的畫面輸出可提供您正在執行的作業的其他資訊。一般而言，本文件中的標準程序只會顯示需要使用者回應的訊息。

以 LDAP 使用者登錄安裝 Policy Director 伺服器

如果您要以 DCE 使用者登錄安裝 Policy Director ，請跳至第75頁的『以 DCE 使用者登錄安裝 Policy Director 伺服器』。

伺服器套裝軟體是位於 *IBM SecureWay Policy Director 3.0 版* CD 的 /solaris 目錄。

您必須以使用者 root 的身份登入，才能安裝 Policy Director 套裝軟體。

如果您需要重新安裝任何套裝軟體，就必須先移除現有的套裝軟體（**pkgrm**），然後重新安裝想要的套裝軟體。

安裝「管理」伺服器：

1. 如果您要使用 LDAP 作爲使用者登錄，請確定您已經安裝 LDAP 伺服器，而且它正在執行中。請參閱第27頁的『第4章 安裝及架構 IBM SecureWay Directory』以取得完整指示。
2. 鍵入 **pkgadd** 指令來列出 CD 上可用的套裝軟體：

   ```
   # pkgadd -d /cdrom/cdrom0/solaris
   ```

   可用的套裝軟體列示會出現在顯示畫面上。

   如果您使用不同的 CD-ROM 裝載點，請在上述指令中替代成您的裝載點。
3. 鍵入 IVBase 的選擇號碼來安裝 Policy Director「基礎」檔案，然後按 Enter 鍵。

   這個指令會將檔案從 CD 解壓縮，然後安裝到您指定的硬碟位置。

   此時會出現一則提示，指出 IVBase 套裝軟體安裝已經順利完成。可用的套裝軟體列示會重新出現。

   在繼續下一步之前，請記住，安全領域中只能有一個「管理」伺服器（IVMgr）案例。如果這是獨立式系統安裝，請繼續執行下一步。如果您是安裝在次要的伺服器上，請確定您已經檢視過第23頁的『安全領域的安裝需求』。
4. 鍵入 IVMgr 的選擇號碼來安裝 Policy Director「管理」伺服器檔案。按 Enter 鍵。

   這個指令會將檔案從 CD 解壓縮，然後安裝到您指定的硬碟位置。

   此時會出現提示，要求您選擇使用者登錄類型。
5. 如果您使用 LDAP 作爲使用者登錄，請鍵入 2 來代表 LDAP 使用者登錄。

   此時會出現提示，要求輸入「DCE Cell 管理者」名稱及密碼。
6. 鍵入必要的資訊來存取「DCE Cell 管理」帳戶。

```
輸入「Cell 管理者」[cell_admin] 的使用者名稱：
輸入「Cell 管理者」的密碼：
```

此時會出現一系列提示，來架構「管理」伺服器以及 LDAP 伺服器之間的通信。

7. 鍵入 LDAP 架構的必要資訊：
   - LDAP 伺服器主電腦名稱
   - LDAP 伺服器埠號
   - LDAP 伺服器 SSL 埠號
8. 鍵入 LDAP 管理使用者（例如，cn=root）的 DN 和密碼。 LDAP 伺服器現在包含 Policy Director 安全資訊。
9. 選擇要啓用或停用「管理」伺服器和 LDAP 伺服器之間的 SSL 通信。

   您可以個別啓用或停用每一個 Policy Director 伺服器和 LDAP 伺服器之間的 SSL 通信。在目前的情況下，您正在設定「管理」伺服器和 LDAP 伺服器之間的 SSL 通信。
10. 如果您已經停用 SSL 通信，請略過這個步驟。如果您已經啓用 SSL 通信，請爲以下的提示提供個別的值：
    - SSL 金鑰環檔案位置
    - SSL 金鑰標籤
    - SSL 金鑰的密碼
11. 提供 GSO 資料庫字尾的 DN（您已經在第28頁的『新增字尾』中新增）來啓用 GSO 資料庫存取。

    例如：

    ```
    o=IBM,c=US
    ```

    在架構 GSO 資料庫存取之後， Policy Director「架構管理程式」會自動架構 DSB。此時會出現一系列的訊息，在每一個步驟完成時列出每一個自動化的步驟。

    此時會出現一則訊息，指出 IVMgr 套裝軟體安裝已經順利完成。可用的套裝軟體列示會重新出現。

安裝 WebSEAL 以及 NetSEAL 的安全管理程式

「安全管理程式」套裝軟體（IVNet）需要使用「基礎」套裝軟體的資源。在安裝 IVNet 之前，請確定您已經安裝「基礎」元件。

1. 鍵入 IVNet 的選擇號碼來安裝 Policy Director「安全管理程式」檔案，然後按 Enter 鍵。

檔案會從 CD 解壓縮，並且安裝到硬碟上的預設目錄中。

如果您使用 LDAP 作爲使用者登錄，就會出現一系列提示，來整合「安全管理程式」和 LDAP 伺服器。

2. 提示時，請鍵入 LDAP 伺服器架構的必要資訊：
   - LDAP 伺服器主電腦名稱
   - LDAP 伺服器埠號
   - LDAP 伺服器 SSL 埠號

   只有先前未曾在這個系統上爲任何其他 Policy Director 套裝軟體架構與 LDAP 伺服器之間的通信時，才會出現上述的 LDAP 伺服器架構提示。如果已經在這個系統上架構「管理」伺服器（IVMgr）或權限伺服器（IVAcld），則之前的提示就不會出現在這個步驟中。
3. 鍵入 LDAP 管理使用者的 DN 和密碼。

   LDAP 伺服器現在包含 Policy Director 安全資訊。
4. 選擇要啓用或停用「安全管理程式」和 LDAP 伺服器之間的 SSL 通信。

   您可以個別啓用或停用每一個 Policy Director 伺服器和 LDAP 伺服器之間的 SSL 通信。在目前的情況下，您正在設定「安全管理程式」以及 LDAP 伺服器之間的 SSL 通信。
5. 如果您已經停用 SSL 通信，請略過這個步驟。如果您已經啓用 SSL 通信，請爲以下的提示提供個別的值：
   - SSL 金鑰環檔案位置
   - SSL 金鑰標籤
   - SSL 金鑰的密碼
6. 提供 GSO 資料庫字尾的 DN（您已經在第28頁的『新增字尾』中新增）來啓用 GSO 資料庫存取。

   例如：

   ```
   o=IBM,c=US
   ```

   此時會出現提示，要求輸入「DCE Cell 管理者」名稱及密碼。
7. 鍵入必要的資訊來存取「DCE Cell 管理」帳戶。

   ```
   輸入「Cell 管理者」[cell_admin] 的使用者名稱：
   輸入「Cell 管理者」的密碼：
   ```

   「安全管理程式」現在已經架構完成並且啓動。

   CAS 伺服器現在已經架構完成並且啓動。

此時會出現一則提示，指出 IVNet 套裝軟體安裝已經順利完成。可用的套裝軟體列示會重新出現。

啓用 WebSEAL 元件

如果您要啓用 WebSEAL 元件，請安裝 WebSEAL（IVWeb）套裝軟體。

1. 鍵入 IVWeb 的選擇號碼來安裝啓用 WebSEAL HTTP 伺服器元件所需的檔案。
2. 按 Enter 鍵以繼續。

   檔案會從 CD 解壓縮，並且安裝到硬碟上。

   此時會出現架構列示，並且包含許多值來確認 HTTP 以及 HTTPS 從屬站存取、必要的 TCP 埠，以及預設的 Web 文件起始目錄。
3. 確認現行的架構值：

```
請檢查 Web 伺服器架構：
1. 啓用 TCP HTTP？ 是
2. HTTP 埠 80
3. 啓用 HTTPS？ 是
4. HTTPS 埠 443
5. Web 文件起始目錄 /opt/Policy Director/www/docs
a. 接受架構並繼續執行安裝
x. 結束安裝
選取要變更的項目：a
```

4. 鍵入 a 以接受架構並繼續執行安裝，然後按 Enter 鍵。
5. 鍵入必要的資訊來存取「DCE Cell 管理」帳戶。

```
輸入「Cell 管理者」[cell_admin] 的使用者名稱：
輸入「Cell 管理者」的密碼：
```

   安裝程式會架構及啓用電腦上的 WebSEAL。「安全管理程式」會自動重新啓動。

啓用 NetSEAL 元件

如果您要啓用 NetSEAL 元件，請安裝 NetSEAL（IVTrap）套裝軟體。

1. 鍵入 IVTrap 的選擇號碼來安裝啓用 NetSEAL 粗略 TCP/IP 存取控制元件所需的檔案，然後按 Enter 鍵。

   NetSEAL 已經架構完成並且啓用。

   此時會出現一個提示，要求輸入「DCE Cell 管理者」的名稱及密碼。
2. 輸入必要的資訊來存取「DCE Cell 管理」帳戶。

   此時會出現一則訊息，指出您需要使用 **ivadmin** 指令來指定受保護埠。

   此時會出現另一則訊息，指出您需要重新啓動（重新開機）系統，以確保所有的受保護埠都是在 NetSEAL 的控制下。

   此時會出現一個提示，指出 IVTrap 套裝軟體安裝已經順利完成。可用的套裝軟體列示會重新出現。

Policy Director NetSEAL 會設陷對特定埠所提出的要求。 如果要使用 NetSEAL 設陷，您必須停止並重新啓動所有使用指定埠的應用程式。有關架構 Policy Director NetSEAL 的其他資訊，請參閱 *Policy Director 管理手冊*中有關 NetSEAL 的概觀資訊。

安裝權限伺服器

安裝「權限」伺服器：

1. 鍵入 IVAcld 的選擇號碼來安裝 Policy Director「權限伺服器」檔案，然後按 Enter 鍵。

   檔案會從 CD 解壓縮，並且安裝到硬碟上的預設目錄中。

   如果您使用 LDAP 作爲使用者登錄，就會出現一系列提示，來整合「權限」伺服器和 LDAP 伺服器。

2. 提示時，請鍵入 LDAP 伺服器架構的必要資訊：
   - LDAP 伺服器主電腦名稱
   - LDAP 伺服器埠號
   - LDAP 伺服器 SSL 埠號

   只有先前未曾在這個系統上爲任何其他 Policy Director 套裝軟體架構與 LDAP 伺服器之間的通信時，才會出現上述的 LDAP 伺服器架構提示。如果已經在這個系統上架構「管理」伺服器（IVMgr）或「安全管理程式」（IVNet），則之前的提示就不會出現在這個步驟中。

3. 鍵入 LDAP 管理使用者的 DN 和密碼。

   LDAP 伺服器現在包含 Policy Director 安全資訊。

4. 選擇要啓用或停用「管理」伺服器和 LDAP 伺服器之間的 SSL 通信。

   您可以個別啓用或停用每一個 Policy Director 伺服器和 LDAP 伺服器之間的 SSL 通信。 在目前的情況下，您正在設定「管理」伺服器和 LDAP 伺服器之間的 SSL 通信。

5. 如果您已經停用 SSL 通信，請略過這個步驟。如果您已經啓用 SSL 通信，請爲以下的提示提供個別的值：
   - SSL 金鑰環檔案位置
   - SSL 金鑰標籤
   - SSL 金鑰的密碼

6. 提供 GSO 資料庫字尾的 DN（您已經在第28頁的『新增字尾』中新增）來啓用 GSO 資料庫存取。

   例如：

   ```
   o=IBM,c=US
   ```

此時會出現提示，要求輸入「DCE Cell 管理者」名稱及密碼。

7. 鍵入必要的資訊來存取「DCE Cell 管理」帳戶。

```
輸入「Cell 管理者」[cell_admin] 的使用者名稱：
輸入「Cell 管理者」的密碼：
```

「權限」伺服器已經架構完成並且啓動。

此時會出現一個提示，指出 IVAcld 套裝軟體安裝已經順利完成。可用的套裝軟體列示會重新出現。

安裝權限 API 元件

如果要安裝 C 檔案的「權限 API」，請鍵入 IVAuthADK 的選擇號碼，然後按 Enter 鍵。

檔案會從 CD 解壓縮，並且安裝到硬碟上的預設目錄中。

此時會出現一個提示，指出 IVAuthADK 套裝軟體安裝已經順利完成。可用的套裝軟體列示會重新出現。

以 DCE 使用者登錄安裝 Policy Director 伺服器

如果您要以 LDAP 使用者登錄安裝 Policy Director ，請跳至第70頁的『以 LDAP 使用者登錄安裝 Policy Director 伺服器』。

伺服器套裝軟體是位於 *IBM SecureWay Policy Director 3.0 版* CD 的 /solaris 目錄。

您必須以使用者 root 的身份登入，才能安裝 Policy Director 套裝軟體。

如果您需要重新安裝任何套裝軟體，就必須先移除現有的套裝軟體（**pkgrm**），然後重新安裝想要的套裝軟體。

安裝「管理」伺服器：

1. 鍵入 **pkgadd** 指令來列出 CD 上可用的套裝軟體：

   ```
   # pkgadd -d /cdrom/cdrom0/solaris
   ```

   可用的套裝軟體列示會出現在顯示畫面上。

   如果您使用不同的 CD-ROM 裝載點，請在上述指令中替代成您的裝載點。

2. 鍵入 IVBase 的選擇號碼來安裝 Policy Director「基礎」檔案，然後按 Enter 鍵。

   這個指令會將檔案從 CD 解壓縮，然後安裝到您指定的硬碟位置。

此時會出現一則提示，指出 IVBase 套裝軟體安裝已經順利完成。 可用的套裝軟體列示會重新出現。

在繼續下一步之前，請記住，安全領域中只能有一個「管理」伺服器（IVMgr）案例。 如果這是獨立式系統安裝，請繼續執行下一步。 如果您是安裝在次要的伺服器上，請確定您已經檢視過第23頁的『安全領域的安裝需求』。

3. 鍵入 IVMgr 的選擇號碼來安裝 Policy Director「管理」伺服器檔案。按 Enter 鍵。

   這個指令會將檔案從 CD 解壓縮，然後安裝到您指定的硬碟位置。

   此時會出現提示，要求您選擇使用者登錄類型。

4. 如果您使用 DCE 作爲使用者登錄，請鍵入 1。

   此時會出現提示，要求輸入「DCE Cell 管理者」名稱及密碼。

5. 鍵入必要的資訊來存取「DCE Cell 管理」帳戶。

   ```
   輸入「Cell 管理者」[cell_admin] 的使用者名稱：
   輸入「Cell 管理者」的密碼：
   ```

   此時會出現一則訊息，指出 IVMgr 套裝軟體安裝已經順利完成。 可用的套裝軟體列示會重新出現。

安裝 WebSEAL 以及 NetSEAL 的安全管理程式

「安全管理程式」套裝軟體（IVNet）需要使用「基礎」套裝軟體的資源。在安裝 IVNet 之前，請確定您已經安裝「基礎」元件。

1. 鍵入 IVNet 的選擇號碼來安裝 Policy Director「安全管理程式」檔案，然後按 Enter 鍵。

   檔案會從 CD 解壓縮，並且安裝到硬碟上的預設目錄中。此時會出現提示，要求輸入「DCE Cell 管理者」名稱及密碼。

2. 鍵入必要的資訊來存取「DCE Cell 管理」帳戶。

   ```
   輸入「Cell 管理者」[cell_admin] 的使用者名稱：
   輸入「Cell 管理者」的密碼：
   ```

   「安全管理程式」現在已經架構完成並且啓動。

   此時會出現一則提示，指出 IVNet 套裝軟體安裝已經順利完成。可用的套裝軟體列示會重新出現。

啓用 WebSEAL 元件

如果您要啓用 WebSEAL 元件，請安裝 WebSEAL（IVWeb）套裝軟體。

1. 鍵入 IVWeb 的選擇號碼來安裝啓用 WebSEAL HTTP 伺服器元件所需的檔案。

2. 按 Enter 鍵以繼續。

   檔案會從 CD 解壓縮，並且安裝到硬碟上。

   此時會出現架構列示，並且包含許多值來確認 HTTP 以及 HTTPS 從屬站存取、必要的 TCP 埠，以及預設的 Web 文件起始目錄。

3. 確認現行的架構值：

```
請檢查 Web 伺服器架構：
1. 啓用 TCP HTTP？ 是
2. HTTP 埠 80
3. 啓用 HTTPS？ 是
4. HTTPS 埠 443
5. Web 文件起始目錄 /opt/Policy Director/www/docs
a. 接受架構並繼續執行安裝
x. 結束安裝
選取要變更的項目：a
```

4. 鍵入 a 以接受架構並繼續執行安裝，然後按 Enter 鍵。
5. 鍵入必要的資訊來存取「DCE Cell 管理」帳戶。

```
輸入「Cell 管理者」[cell_admin] 的使用者名稱：
輸入「Cell 管理者」的密碼：
```

   安裝程式會架構及啓用電腦上的 WebSEAL。「安全管理程式」會自動重新啓動。

啓用 NetSEAL 元件

如果您要啓用 NetSEAL 元件，請安裝 NetSEAL（IVTrap）套裝軟體。

1. 鍵入 IVTrap 的選擇號碼來安裝啓用 NetSEAL 粗略 TCP/IP 存取控制元件所需的檔案，然後按 Enter 鍵。

   NetSEAL 已經架構完成並且啓用。

   此時會出現一個提示，要求輸入「DCE Cell 管理者」的名稱及密碼。

2. 輸入必要的資訊來存取「DCE Cell 管理」帳戶。

   此時會出現一則訊息，指出您需要使用 **ivadmin** 指令來指定受保護埠。

   此時會出現另一則訊息，指出您需要重新啓動（重新開機）系統，以確保所有的受保護埠都是在 NetSEAL 的控制下。

   此時會出現一個提示，指出 IVTrap 套裝軟體安裝已經順利完成。可用的套裝軟體列示會重新出現。

Policy Director NetSEAL 會設陷對特定埠所提出的要求。 如果要使用 NetSEAL 設陷，您必須停止並重新啓動所有使用指定埠的應用程式。有關架構 Policy Director NetSEAL 的其他資訊，請參閱 *Policy Director 管理手冊*中有關 NetSEAL 的概觀資訊。

安裝權限伺服器

安裝「權限」伺服器：

1. 鍵入 IVAcld 的選擇號碼來安裝 Policy Director「權限伺服器」檔案，然後按 Enter 鍵。

   檔案會從 CD 解壓縮，並且安裝到硬碟上的預設目錄中。此時會出現提示，要求輸入「DCE Cell 管理者」名稱及密碼。

2. 鍵入必要的資訊來存取「DCE Cell 管理」帳戶。

   ```
   輸入「Cell 管理者」[cell_admin] 的使用者名稱：
   輸入「Cell 管理者」的密碼：
   ```

   「權限」伺服器已經架構完成並且啓動。

   此時會出現一個提示，指出 IVAcld 套裝軟體安裝已經順利完成。可用的套裝軟體列示會重新出現。

安裝權限 API 元件

如果要安裝 C 檔案的「權限 API」，請鍵入 IVAuthADK 的選擇號碼，然後按 Enter 鍵。

檔案會從 CD 解壓縮，並且安裝到硬碟上的預設目錄中。

此時會出現一個提示，指出 IVAuthADK 套裝軟體安裝已經順利完成。可用的套裝軟體列示會重新出現。

架構證明獲取服務程式

Policy Director CAS 會自動安裝。如果您要使用 Policy Director CAS作爲證明獲取服務程式，就必須架構它。請參閱 *Policy Director 管理手冊*中有關架構證明獲取服務程式的資訊，以取得進一步的指示。

安裝管理主控台

Policy Director 提供「管理主控台」來管理許多 Policy Director 元件。

Solaris 的「管理主控台」是使用 IVConsole 安裝套裝軟體來安裝。請使用 **pkgadd** 來安裝及架構套裝軟體。

1. 以 root 的身份登入。
2. 將 *IBM SecureWay Policy Director 3.0 版* CD 插入 Policy Director 伺服器系統的光碟機，並予以裝載。
3. 顯示可用的套裝軟體列示：

```
# pkgadd -d /cdrom/cdrom0/solaris
```

4. 鍵入 IVBase 的選擇號碼（如果尚未安裝的話）。如果已經安裝 IVBase，請跳至步驟 6。
5. 鍵入 y 以繼續。

   此時會出現套裝軟體列示。
6. 鍵入 IVConsole 的選擇號碼。
7. 鍵入 y 以繼續。

   此時會出現一個提示，指出安裝順利完成。「管理主控台」現在已經準備啓動。

啓動管理主控台

啓動「管理主控台」：

1. 確定 Policy Director 伺服器已經安裝好，而且正在執行中。
2. 鍵入以下的指令：

```
$ /opt/intraverse/bin/ivconsole
```

移除 Policy Director

使用 **pkgrm** 公用程式從電腦移除 Policy Director 伺服器。套裝軟體必須以和安全期間相反的次序來移除。 **pkgrm** 和 **pkgadd** 指令都是同一個公用程式系列的成員，而且具有相同的使用者介面。 root 使用者會執行 **pkgrm** 公用程式。

有數種方法可以使用這個指令：

- 啓動 **pkgrm** 指令，但不要加上任何引數。

  此時會出現您電腦上目前的套裝軟體編號列示。鍵入您要移除的套裝軟體的單一選擇號碼。
- 啓動 **pkgrm** 指令並指定一個單一套裝軟體名稱作爲指令的引數。例如：

  ```
  # pkgrm IVBase
  ```
- 啓動 **pkgrm** 指令並指定一系列套裝軟體名稱作爲指令的多重引數。例如：

  ```
  # pkgrm IVAuthADK IVAcld IVTrap IVWeb IVNet IVMgr IVBase
  ```

請查詢 Solaris 作業系統文件，以取得 **pkgrm** 指令的詳細資訊。

註: 您移除 Policy Director 套裝軟體的順序應該和安全所需的順序完全相反。

移除 Policy Director：

1. 以 root 身份登入 Solaris 作業系統。

使用其中一個之前啓動 **pkgrm** 指令的方法。

2. Policy Director 元件必須用以下的順序來移除：
   - IVTrap
   - IVWeb
   - IVNet
   - IVAuthADK
   - IVAcld
   - IVMgr
   - IVBase

   您的電腦系統架構可能不含之前的列示所顯示的每一個套裝軟體。 Policy Director「管理主控台」（IVConsole）可以在 IVBase 之前隨時移除。

移除管理主控台

移除「管理主控台」：

1. 以使用者 root 的身份登入。
2. 鍵入以下的指令：

   ```
   # pkgrm ivconsole
   ```

第8章 相關文件

您可以使用本章中所列出的文件來尋找 Policy Director 3.0 版及相關產品的其他資訊。

Policy Director 文件

*啓動與執行 IBM SecureWay Policy Director，3.0 版*這本書除了隨附於 Policy Director 產品之外，在文件包中也有提供。 Policy Director 文件包括本書和 Policy Director 著作權資訊。

除了本書外，以下的文件包含 Policy Director 的相關資訊，並且提供「PostScript 文件格式」（PDF）格式的文件，這些文件位於 *IBM SecureWay Policy Director 3.0 版* CD 的 /doc 子目錄下：

- *IBM SecureWay Policy Director 管理手冊，3.0 版*

  本書提供管理 Policy Director 的詳細指示。本書提供 IBM SecureWay Policy Director 相關資訊，例如：

  - Policy Director 概念，如：身份驗證、授權以及證明的獲取。
  - 使用「管理主控台」來執行的一般管理作業
  - WebSEAL 管理
  - NetSEAL 管理
  - NetSEAT 管理
  - 管理資源（**ivadmin** 指令）

- *IBM SecureWay Policy Director Programming Guide and Reference, Version 3.0*

  本書探討「權限 API」元件，以及執行下列作業的方法：
  - 使用權限 API 來建置應用程式
  - 起始設定 Policy Director 權限服務程式
  - 對應用程式伺服器或從屬站進行身份驗證
  - 取得使用者證明
  - 進行授權決策
  - 執行選用的作業
  - 清除和關機
  - 使用「權限 API」來部署應用程式

Policy Director README 檔可能含有替代產品出版品的最新 Policy Director 相關資訊。

如果要取得最新的 README 檔案，請存取 IBM SecureWay Policy Director 網站的檔案庫頁面。

http://www.ibm.com/software/security/policy/library

IBM SecureWay FirstSecure 文件

以下的書籍包含 FirstSecure 的相關資訊：

- *IBM SecureWay FirstSecure Planning and Integration， 2.0 版（S564-8D11-00）*

  本書說明 FirstSecure 以及組成 FirstSecure 的產品，並協助您開始規畫，以使用所有的 IBM SecureWay 產品。

IBM SecureWay Policy Director（Policy Director）可以是 IBM SecureWay FirstSecure 的元件，也可以當作獨立的產品。如果您的 Policy Director 版本是包含在 FirstSecure 中，則 FirstSecure 會提供本書。如果您的 Policy Director 版本是單獨購買的產品，您可以在 FirstSecure 網頁找到本書：

http: //www.ibm.com/software/security/firstsecure/library

IBM 分散式計算環境文件

下列文件說明如何安裝 DCE，您可以從 *IBM SecureWay Policy Director 安全服務程式* CD 取得這些文件，它們採用 PDF 格式，並且位於 /doc 目錄下，您也可以在 DCE 網站取得它們：

http://www.ibm.com/network/dce/library/

IBM DCE for Windows NT

*IBM Distributed Computing Environment for Windows NT 快速入門，2.2 版*可從以下的網址取得：

http://www.software.ibm.com/network/dce/library/publications/dcent.html

本書說明 Distributed Computing Environment (DCE) for Windows NT, 2.2 版，並解釋如何規劃、安裝與架構產品。

*IBM Distributed Computing Environment for Windows NT 快速入門，2.2 版*一書也可以從 *IBM SecureWay Policy Director 安全服務程式* CD 取得，檔案位於 /doc/DCE22_QuickBeginnings_NT.pdf。

IBM DCE for AIX

IBM Distributed Computing for AIX 快速入門，2.2 版，可從以下的網址取得：

http://www.software.ibm.com/network/dce/library/publications/dceaix.html

本書說明 IBM Distributed Computing Environment (DCE) for AIX， 2.2 版，並解釋如何規劃、安裝與架構產品。

*IBM Distributed Computing Environment for AIX NT 快速入門， 2.2 版*一書也可以從 *IBM SecureWay Policy Director 安全服務程式* CD 取得，檔案位於 /doc/DCE22_QuickBeginnings_AIX.pdf。

Transarc DCE for Solaris

*Transarc DCE 2.0 版最新版本資訊*與*安裝與架構手冊*，可在下列網址中找到：

`http://www.transarc.com/Library/documentation/dce/2.0/index.html`

*Transarc DCE 2.0 版最新版本資訊*提供 Transarc DCE 軟體與文件的如下相關資訊：

- OSF DCE 與 DCE * DFS 產品之間的差異
- DCE * DFS 的 2.0 版與 1.1 版之間的差異
- 與 DCE * DFS 相關的已知問題和限制

*Transarc DCE，2.0 版版本注意事項*也可以從 *IBM SecureWay Policy Director 安全服務程式* CD 取得，檔案是 /doc/DCE20_ReleaseNotes_Solaris.pdf。

*安裝與架構手冊*提供安裝、架構以及更新 DCE DFS 2.0 產品的指示。

*安裝與架構手冊*也可以從 *IBM SecureWay Policy Director 安全服務程式* CD 取得，檔案是 /doc/DCE20_InstallGuide_Solaris.pdf。

IBM SecureWay Directory 文件

下列書籍含有 IBM SecureWay Directory (LDAP) 的安裝與架構資訊：

- *IBM SecureWay Directory Installation and Configuration, Version 3.1.1*

  本書針對每一種支援的作業系統提供各自的版本（採 HTML 格式）。每一個作業系統的書籍都位於各版本 CD 的 /doc/wparent.htm 中。這些 CD 分別是：

  – *IBM SecureWay Directory Version 3.1.1 for NT*

  – *IBM SecureWay Directory Version 3.1.1 for AIX*

  – *IBM SecureWay Directory Version 3.1.1 for Solaris*

  在 LDAP 安裝後，安裝與架構的 .HTM 文件檔位置是：

  ```
  C:\Program Files\IBM\LDAP\nls\html\enUS1252\config\wparent.htm
  ```

以下的 HTML 格式書籍包含如何管理 IBM SecureWay 的資訊：

- *IBM SecureWay Directory 管理手冊， 3.1.1 版*

  1. 在 LDAP 預設安裝之後，使用 Web 瀏覽器來存取在下列網址中找到的文件：

     ```
     C:\Program Files\IBM\LDAP\nls\html\enUS1252\config\wparent.ht
     ```

以下的 HTML 格式書籍含有 IBM SecureWay Directory 從屬站的資訊：

- *IBM SecureWay Directory Client SDK Programming Reference，3.1.1 版*

  本書包含這份 LDAP 資訊的鏈結：

  – LDAP Client SDK Plugin Programming Reference 資訊

    1. 在 LDAP 預設安裝之後，使用 Web 瀏覽器來存取在下列網址中找到的文件：

       ```
       C:\Program Files\IBM\doc\progref.htm
       ```

    2. 開啓 *IBM SecureWay Directory Client SDK Programming Reference* 文件。
    3. 按一下 **Appendices**。
    4. 按一下 **LDAP Client SDK Plugin Programming Reference**

  – 有關如何使用 GSKit 以及「金鑰管理工具」**ikmguiw** 來架構 LDAP 伺服器，以便支援 SSL 存取的資訊

    1. 如果本書尚未開啓，請開啓 *IBM SecureWay Directory Client SDK Programming Reference* 文件。
    2. 按一下 **API categories**。
    3. 按一下 **SSL**。
    4. 按一下 **LDAP_SSL API**。
    5. 找出並按一下 **Using IKMGUI** 鏈結來開啓適當的 HTML 檔。

IBM SecureWay Directory 伺服器也提供以下的文件：

- *IBM SecureWay Directory Server Plug-ins Reference*

附錄. 注意事項

本資訊是針對 IBM 在美國所提供之產與服務開發出來的。 而在其他國家中，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 產品、程式或服務時，不表示或暗示只能使用 IBM 產品、程式或服務。 只要未侵犯 IBM 的智慧財產權，任何功能、產品或服務都可以取代 IBM 的產品。 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）資訊的特許權限事直，請聯絡您國家的 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（包括但不限於可售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。

本書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。

資料中提供的非 IBM 網站僅供用戶參考方便，絕不代表爲那些網站背書。那些網站上的內容並非本 IBM 產品內容的一部份，用戶使用該網站時應自行承擔風險。

IBM 可能使用或散佈您提供的任何資料，然因合理得宜，可不須對您負責。

本程式之授權者若欲取得相關資訊，以便使用下列資訊者可洽詢 IBM。其下列資訊指的是： (i) 獨立建立的程式與其他程式（包括此程式）之間交換資訊的方式， (ii) 互相使用已交換之資訊方法。若有任何問題請聯絡：

IBM Corporation
Department LZKS
11400 Burnet Road
Austin, TX 78758
U.S.A.

上述資料之取得有其特殊要件，在某些情況下必須付費方得使用。

IBM 基於雙方之「IBM 客戶合約」、「IBM 國際程式授權合約」（或任何同等合約）條款，提供本資訊中所述的授權程式與其所有適用的授權資料。

這裡提到的任何性能資料均限定在一控制環境下。因此從其它操作環境所取得的結果可能差異很大。我們可能已對發展層次系統採取某些措施，但不保證這些措施與一般現有的系統相同。再者，某些措施可能是推斷而來，與實際結果可能有異。本文件的用戶應查證所屬環境是否適用這些資料。

關於非 IBM 產品的資料是來自該產品供應商、公開說明或其它公開來源。IBM 並未測試那些產品，所以無法確認性能準確度、相容性或任何其它與非 IBM 產品有關的索賠。有關非 IBM 產品的性能問題應直接洽詢該產品供應商。

所有關於 IBM 未來的方向或企圖可能未經通知逕行修正或撤回，僅代表目標和方針。

所有列出的 IBM 價格只是 IBM 目前的建議售價，可能未經通知逕行變更。經銷商的價格可能有所差異。

本資訊含有日常業務運作所用的資料報告範例。 爲使這些範例儘可能完整，其中有個人、公司、品牌和產品的名稱。 所有名稱純屬虛構，如有雷同純屬巧合。

商標

下列詞彙是 International Business Machines 公司在美國和其他國家的商標：

AIX
DB2
FirstSecure
IBM
Policy Director
SecureWay

其他公司、產品和服務名稱可能是第三者的商標或服務標記。

AuthAPI	DASCOM, Inc.
DASCOM	DASCOM, Inc.
Internet Explorer	Microsoft Corporation
Netscape 與 Netscape 標誌圖	Netscape Communications Corporation
Netscape Communicator	Netscape Communications Corporation
Netscape Navigator	Netscape Communications Corporation
NetSEAL	DASCOM, Inc.
NetSEAT	DASCOM, Inc.
Solaris	Sun Microsystems, Inc.
WebSEAL	DASCOM, Inc.

Java 及所有 Java 型商標及標誌都是 Sun Microsystems, Inc. 在美國及/或其它國家的商標。

Microsoft、Windows、Windows NT 及 Windows 標誌是 Microsoft Corporation 在美國及/或其它國家的商標。

UNIX 是 X/Open Company Limited 在美國及/或其它國家獨家授權的註冊商標。

索引

索引順序以中文字，英文字，及特殊符號之次序排列。

〔三劃〕

〔四劃〕

〔五劃〕

〔六劃〕

〔七劃〕

〔八劃〕

〔九劃〕

〔十劃〕

〔十一劃〕

〔十二劃〕

〔十三劃〕

〔十四劃〕

〔十五劃〕

〔十六劃〕

〔十七劃〕

〔十八劃〕

〔十九劃〕

〔二十二劃〕

〔數字〕

A

B

C

D

F

G

I

L

N

P

S

T

W

IBM® SecureWay® Policy Director
啟動與執行
3.0 版

SC40-0504-00

折疊線

台北市敦化南路一段二號十二樓

中華民國國際商業機器股份有限公司 啟

寄

折疊線

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：

讀者意見表

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!

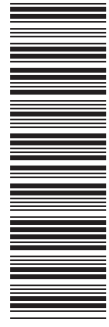
評估項目	評　估　意　見		備　註
正確性	內容說明與實際程序是否符合	□是□否	
	參考書目是否正確	□是□否	
一致性	文句用語及風格，前後是否一致	□是□否	
	實際畫面訊息與本書所提之畫面訊息是否一致	□是□否	
完整性	是否遺漏您想知道的項目	□是□否	
	字句、章節是否有遺漏	□是□否	
術語使用	術語之使用是否恰當	□是□否	
	術語之使用，前後是否一致	□是□否	
可讀性	文句用語是否通順	□是□否	
	有否不知所云之處	□是□否	
內容說明	內容說明是否詳盡	□是□否	
	例題說明是否詳盡	□是□否	
排版方式	本書的形狀大小，版面安排是否方便使用	□是□否	
	字體大小，顏色編排，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。

Part Number: CT63KTC

Printed in Singapore



CT63KTC

SC40-0504-00