IBM SecureWay Policy Director 3.0 版管理手冊

IBM SecureWay Policy Director 3.0 版管理手冊

備註

使用本資訊及其支援的產品之前，請先閱讀第271頁的『附錄B. 注意事項』下面的一般資訊。

第 1 版 (October 1999)

本修訂版適用於 IBM® FirstSecure Secureway® Policy Director™ 產品版本 3 版次 0 修訂層次 0 與所有後續版次，直到新修訂版中另有指示爲止。

本修訂版取代 IBM SecureWay Global Sign-On™ 版本 2 版次 2 修訂層次 200。

目錄

關於本書

本書提供 IBM® SecureWay® Policy Director™ 相關資訊，像是：

- Policy Director 概念，如：身份驗證、權限與證明的獲取。
- 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）

本書的適用對象

本書主要寫給將管理 Policy Director 使用者、群組、GSO 資源、GSO 資源群組、Proxy 使用者、存取控制清單與許可權，以及物件空間的管理者看。

由於負責管理 Policy Director 的人員亦必須管理身份驗證、權限與證明獲取事宜，因此對這些程序必須有某些程度的瞭解。

管理者對 IBM Distributed Computing Environment (DCE™) 與 IBM SecureWay Directory 輕裝備目錄存取通信訊協定 (LDAP™) 的管理理應駕輕就熟。Policy Director 會用到 IBM SecureWay Directory 與 IBM Distributed Computing Environment 伺服器，而這些已包含在 Policy Director 產品中。

本書的結構

本書由下列各章節組成：

- 第 1 章到第 3 章，闡述 Policy Director 概念，像是 第1頁的『第1章 歡迎使用 Policy Director』、第15頁的『第2章 身份驗證及證明獲取』 與 第33頁的『第3章 瞭解授權』 爲 Policy Director 概觀。
- 第 4 章到第 12 章，討論 Policy Directory 一般管理作業，如：
  - 第51頁的『第4章 管理主控台簡介』
  - 第65頁的『第5章 管理使用者帳戶及群組』
  - 第71頁的『第6章 管理 GSO 資源、資源群組及資源憑證』
  - 第77頁的『第7章 瞭解存取控制』
  - 第101頁的『第8章 引用存取控制』
  - 第107頁的『第9章 管理 Proxy 使用者』
  - 第117頁的『第10章 管理 Policy Director 伺服器』
  - 第127頁的『第11章 管理權限服務程式』
  - 第137頁的『第12章 登入及審核伺服器活動』

第 13 章到第 16 章，涵蓋 WebSEAL 管理，如：

- 第149頁的『第13章 WebSEAL：設定身份驗證』

- 第167頁的『第14章 WebSEAL：一般管理作業』
- 第175頁的『第15章 WebSEAL：智慧型接合管理』
- 第201頁的『第16章 WebSEAL：應用程式整合』

第 17 章到第 18 章，討論下列這些 NetSEAL 管理主題：

- 第209頁的『第17章 NetSEAL：概觀』
- 第221頁的『第18章 NetSEAL：一般管理作業』

第 19 章到第 21 章，提供 NetSEAT 管理的相關資訊：

- 第229頁的『第19章 NetSEAT：概觀』
- 第233頁的『第20章 NetSEAT：一般管理作業』
- 第247頁的『第21章 NetSEAT：目錄服務分配管理系統』

本書另有附錄，分別是 第251頁的『附錄A. 使用 ivadmin 來進行 Policy Director 管理』與 第271頁的『附錄B. 注意事項』。

本書的使用慣例

本書使用下列的印刷慣例：

慣例	意義
粗體	代表使用者介面元素，像是：功能表名稱、功能表選項、輸入欄位、圖示、資料夾、清單框、動作按鈕、按鈕、圓鈕、旋轉鈕與勾選框。高亮度顯示的粗體亦代表注意與警告事項。
等寬字體	代表語法、範例碼與使用者必須鍵入的文字。
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：選取**檔案 → 執行**，表示先按一下**檔案**，然後再按一下**執行**。

2000 年的因應

這些產品皆已做好 2000 年的因應。當您根據這些產品的相關文件來使用它們，只要這些產品的相關產品（例如，硬體、軟體與韌體）與它們之間能適當交換精確的日期資料，則在 20 世紀與 21 世紀間，這些產品亦能正確處理、提供與接收日期資料。

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參照非 IBM 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。

必備需求與相關資訊

Policy Director 的必備需求與相關產品，請參閱下列文件：

IBM SecureWay Policy Director

PDF 格式的文件：下列是 Policy Director 的相關書籍，以 PDF 格式提供於 *IBM SecureWay Policy Director 3.0 版* CD 中的 /doc 下：

- 本書，*IBM SecureWay Policy Director 管理手冊，3.0 版*
- *IBM SecureWay Policy Director Programming Guide and Reference, Version 3.0*

採印刷本的文件：下列亦是 Policy Director 的相關書籍，以印刷本隨附於產品套裝軟體中：

IBM SecureWay Policy Director 啓動與執行，版本 3.0 (SCT6-3KNA-00)

IBM SecureWay FirstSecure

下列是 IBM SecureWay FirstSecure 的相關文件：

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

  本書說明 FirstSecure 與構成 FirstSecure 的各項產品。本書可協助您初步規劃使用所有的 IBM SecureWay 產品。

IBM Distributed Computing Environment

下列文件說明如何安裝 DCE，這些文件採 PDF 格式，並可在「IBM SecureWay Policy Director 安全服務程式」CD 下的 /doc 或 DCE 網站中找到。

IBM DCE for Windows NT

IBM Distributed Computing Environment for Windows NT 快速入門，2.2 版，可在下列網址中找到：

`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、安裝與配置產品。

IBM DCE for AIX

IBM Distributed Computing for AIX 快速入門 2.2 版，可在下列網址中找到：

`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、安裝與配置產品。

Transarc DCE for Solaris

Transarc DCE 2.0 版最新版本資訊與安裝與配置手冊，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 產品間的差異
- DCE DFS 2.0 版與 1.1 版間的差異
- DCE DFS 的已知瑕疵與相關限制

*安裝與配置手冊*提供有關安裝、配置與升級 DCE DFS 2.0 版產品的指示。

IBM SecureWay Directory

下列亦爲 IBM SecureWay Directory 的參考文件：

- *IBM SecureWay Directory 安裝與配置 3.1.1 版*
  本書針對每一種支援的作業系統提供各自的版本。
- *IBM SecureWay Directory Client SDK Programming Reference*
- *IBM SecureWay Directory Server Plug-ins Reference*

下列書籍含有 IBM SecureWay Directory (LDAP) 的安裝與配置資訊：

- *IBM SecureWay Directory 安裝與配置， 3.1.1 版*
  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）。各作業系統版書籍放在適當的 CD 中。這些 CD 分別是：
  - *IBM SecureWay Directory Version 3.11 for NT*
  - *IBM SecureWay Directory Version 3.11 for AIX*
  - *IBM SecureWay Directory Version 3.11 for Solaris*

下列亦爲 IBM SecureWay Directory 的參考文件：

- *IBM SecureWay Directory Client SDK Programming Reference*
- *IBM SecureWay Directory Server Plug-ins Reference*

傳達意見

您的意見可以幫助我們提供最精確及高品質的資訊。如果您對本書或其它 IBM SecureWay Policy Director 文件有任何意見，請造訪我們的 Policy Director 首頁：

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

您會看到回覆頁，而您可以輸入意見並傳給我們。同時，您還可看到 Policy Director 的最新更新資訊。

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 歡迎使用 Policy Director

IBM SecureWay Policy Director (Policy Director) 是一個完整的權限解決方案，可用來整合 Web、主從架構及大型主機應用程式。 Policy Director 權限可以讓組織安全地控制使用者對保護資訊的存取。 您可使用 Policy Director 和標準的網際網路-應用程式來建置安全性高及管理良善的企業內網路。

本章包括：

瞭解企業網路安全性

需多組織現在認爲公開的網際網路及私人的企業內網路對於廣域通信而言，是十分有效而重要的媒介。電子商務正迅速地成爲許多企業行銷策略的基本元件。教育機構依賴網際網路來進行遠距教學。線上服務可容許個人傳送電子郵件及取得 Web 廣大的資源。傳統的應用程式，如 TELNET 或 POP3，仍然是普遍而重要的網路服務程式。

企業瞭解到他們可以利用網路網路的技術來加強供應鍊的關係、促進與企業伙伴的合作，以及提供增加的客戶連通性。只要企業可以整合具有高度安全性的資源，就能達成這些目的。

企業想要使用網際網路作爲廣域的商業及分送機制。然而，由於缺乏經過證明的安全原則機制以及管理系統，這些企業已經受到阻礙。

Policy Director 是一資訊原則管理解決方案，它提供組織集中式網路安全服務。有了集中式的網路安全服務，您便能維持一致的使用者及原則資訊，並且使之生效。

網路安全性術語及定義

以下的網路安全服務及概念，對於本文中 Policy Director 的探討十分重要：

安全領域 共用共同的服務，而且通常具有共同目的的使用者群組、系統及資源。

身份驗證 識別嘗試登入安全領域之個體的程序。

證明 在身份驗證期間取得的詳細資訊，它說明了使用者、群組連結（如果有的話），以及其他與安全性相關的識別屬性。

權限 決定個體是否有權對受保護的資源執行作業的程序。

密碼化 將電子資料轉換成安全碼，以保護資料不受到未經授權的人取用。

完整性 電子資料在傳送以及接收期間沒有改變。

保護品質 資料安全性的層次，由身份驗證、完整性及私密狀況一起決定。

可調整性 當使用者存取資源時，網路系統回應遞增的使用者數目的能力。

網路安全性的共同考量

全世界的公用網際網路以及公司的專用企業內網路都連接到不同的電腦系統、應用程式及網路。混和不同的硬體及軟體通常會對網路造成以下影響：

- 應用程式的安全性沒有集中控制。
- 沒統一的資源位置命名慣例。
- 缺乏對應用程式高度有用性的共同支援。
- 缺乏對可調整的成長的共同支援。

新的企業運作模式要求組織在某種程度上凸顯他們的資訊資源，這是前所未有的。這些企業需要知道他們可以安全地控制對這些資源的存取。

對於「資訊技術」（IT）管理人員而言，管理分佈在分散式網路上的原則及使用者已經證明是非常困難的。這是因爲個別的應用程式及系統供應商都是以他們自己的方式來使權限生效。

許多公司瞭解到，爲每一個企業應用程式開發新的權限服務程式是項昂貴的程序，這個程序會導致難以管理的基本設施。開發者利用應用程式介面（API）來存取的集中式權限服務可以大幅加快上市的時間，並減少所有權的總成本。

集中式的網路安全管理系統必須滿足下列需求：

- 現存的防火牆及身份驗證配置之共存與 leverage。
- 與網路及應用程式管理組織配置整合或共存。
- 將應用程式獨立。

Policy Director 簡介

Policy Director 是一個有關權限、網路安全、原則管理的完整解決方案，它能爲散佈各地的企業內網路及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。

除了卓越的安全性原則管理特性，Policy Director 還支援身份驗證、權限、資料安全及資源管理功能。您可使用 Policy Director 和標準的網際網路用應用程式來建置安全性高及管理良善的企業內網路。

有了 Policy Director，企業現在可以安全地管理對專用內部網路資源的存取。 同時，企業可以運用公共網際網路廣泛連通性之影響力及簡易使用的能力。Policy Director 如果結合企業的防火牆系統，便能保護企業內網路，使其免於未經授權的存取和入侵。

Policy Director 權限服務程式 API 標準

*權限服務程式*是應用程式安全性配置十分重要的一部分。使用者通過身份驗證程序之後，權限服務程式會判斷使用者可以存取的服務程式及資訊，來繼續強制執行企業原則。

例如，存取 Web 退休金網頁的使用者可以檢視個人帳戶資訊。在這之前，權限伺服器必須驗證該使用者的身份、證明及專用權屬性。

以標準爲基礎的「Policy Director 權限 API」可讓應用程式呼叫集中式的 Policy Director 權限服務程式。使用這些呼叫，讓開發者不必爲每一個新的應用程式撰寫權限程式碼。

「Policy Director 權限 API」能讓企業將受信任的授權組織配置上的所有的應用程式標準化。使用「Policy Director 權限 API」，企業對於存取網路上的資源便能提供更多控制。

請參閱*Policy Director 程式設計及參考手冊*以取得 Policy Director 權限 API 的完整資訊及說明。

Policy Director 核心技術

Policy Director 網路安全性管理解決方案提供並支援以下核心技術：

- 身份驗證
- 權限
- 資料保護的品質
- 可調整性
- 說明性

身份驗證

此核心技術包括支援 Policy Director 使用者名稱與密碼的*身份驗證機制*。

機密金鑰:

- Kerberos
- 輕裝備目錄存取通訊協定（Lightweight Directory Access Protocol，LDAP）

公開金鑰/私密金鑰:

- 利用應用程式特定的使用者名稱及密碼，登入啓用「安全 socket 層次」（SSL）的瀏覽器：
  - 基本身份驗證 (BA) 機制--只有 WebSEAL 及安全 Socket 層次介面 HTTPS。
  - Policy Director 格式基礎機制--只有 WebSEAL 及 HTTPS。
- 使用從屬站端 X.509 憑證透過 SSL 登入 -- Policy Director 支援與 PKIX 相容的公開金鑰基本設施 (PKI) 產品（如 IBM SecureWay Trust Authority 3.1 版）或以 Entrust 爲基礎的 PKI 產品（如 IBM Vault Registry 2.2.2 版）。

  IBM SecureWay Trust Authority 3.1 版包括從屬站軟體、簡單的登錄應用程式、憑證管理中心與整合的目錄，以支援全程的憑證生命週期，包括：登記與初始的憑證、金鑰對更新、憑證更新、憑證與憑證廢止清冊 (CRL) 的發佈，以及憑證的廢除。另提供圖形式使用者介面 (GUI)，用以管理「憑證管理中心 (CA)」、「註冊管理中心（RA）」與「結束實體 (EE)」要求。此外還提供 API 程式庫。

證明獲取:

- 「證明獲取服務程式 (CAS)」-- 自訂身份驗證擴充項

權限

本核心技術提供對下列 Policy Director 權限類型的支援：

- Policy Director 權限服務程式

- 標準的 Policy Director 權限 API
- 外部權限功能

資料保護的品質

*「保護品質」*是指 Policy Director 保護任何在從屬站以及伺服器之間傳輸的資訊的程度。通道機制、加密標準以及修改 --- 偵測演算法的合併效果可以決定保護品質。

爲了增加包括下列的安全性，品質保護層次：

1. 標準傳輸控制通信協定 (TCP) 通信 (無身份驗證)
2. 僅身份驗證--驗證使用者的身份
3. 身份驗證以及資料完整性--避免訊息（資料串流）在網路通信期間被變更
4. 身份驗證 + 資料完整性 + 資料私密性--避免訊息在網路通信期間被變更或視察

您可以爲要使用的特定主電腦及網路指定必要的保護層次。

支援的加密標準: Policy Director 支援以下的資料加密標準 (DES) 及其它 SSL 加密密碼：

- 40 位元 RC2
- 128 位元 RC2
- 40 位元 RC4
- 128 位元 RC4
- 40 位元 DES
- 56 位元 DES
- 168 位元三重 DES

Policy Director NetSEAL 與 Policy Director WebSEAL 在 「DCE 遠端程序呼叫 (DCE-RPC)」上支援 40 位元 DES 與 56 位元 DES 加密。

註: 國際版本會受限於加密技術的出口限制。

通道機制: Policy Director 支援以下傳輸加密資料的通信協定：

- 「安全 SOCKET 層次 (SSL)」通道機制
- 「同屬安全服務 (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：「安全 Socket 層次」（SSL）通信協定可容許信號的交換，以設定兩部數據機之間的通信。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。在 NetSEAT 從屬站作爲安全性特定埠 (例如，TELNET 使用的埠) 之 Policy Director NetSEAL 伺服器的 SSL 從屬站使用時，會使用此配置。

Policy Director WebSEAL 支援 SSL 版本 2 及版本 3。

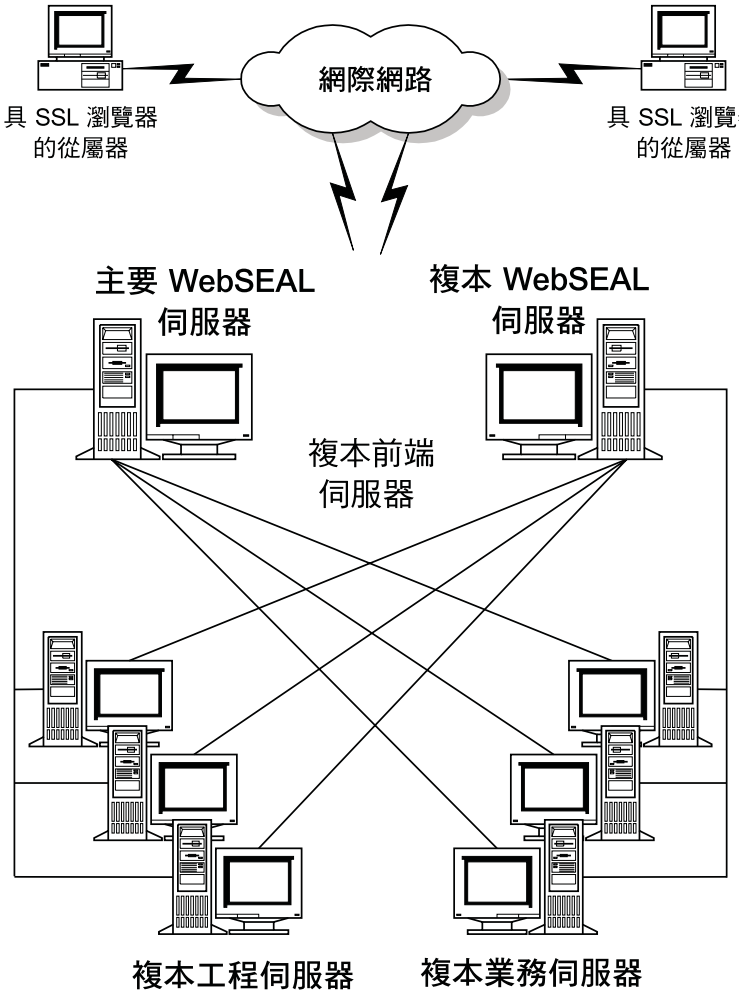
GSS 通道機制：GSS 介面（GSS API）是一種可讓應用程式存取安全服務的標準方法。GSS 通道使用在安全 RPC 上。當您將 NetSEAT 從屬站以支援模組方式安裝在 Policy Director for Microsoft® Windows NT® 或 Policy Director「管理主控台」中時，請啓用此選項。

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。

可調整性

*可調整性*是指當使用者存取安全領域中的資源時，系統回應遞增的使用者數目的能力。Policy Director 使用下列技術來提供可調整性：

- 服務程式複製
  - 身份驗證服務程式
  - 權限服務程式
  - 安全原則
  - 資料加密服務程式
  - 審核服務程式
- 前端複製的 WebSEAL 伺服器
  - 高度有用性的鏡映資源
  - 提供負載平衡的從屬站要求
- 後端複製的伺服器
  - 後端伺服器可以是 WebSEAL 伺服器或協力廠商的 Web 伺服器
  - 高度有用性的鏡映資源（一致的名稱空間）
  - 其他內容及資源
  - 透過智慧型接合™以負載平衡進入的要求
- 藉由將身份驗證及權限服務程式卸載至個別的伺服器，以最佳化效能
- 量化佈署服務程式而不增加管理費用



說明性

Policy Director 提供許多日誌記載及審核功能。日誌檔可以攫取任何由 Policy Director 伺服器及 DCE 伺服器所產生的錯誤訊息和警告訊息。還有審核追蹤檔可以監督 Policy Director 及 DCE 伺服器活動。

日誌檔

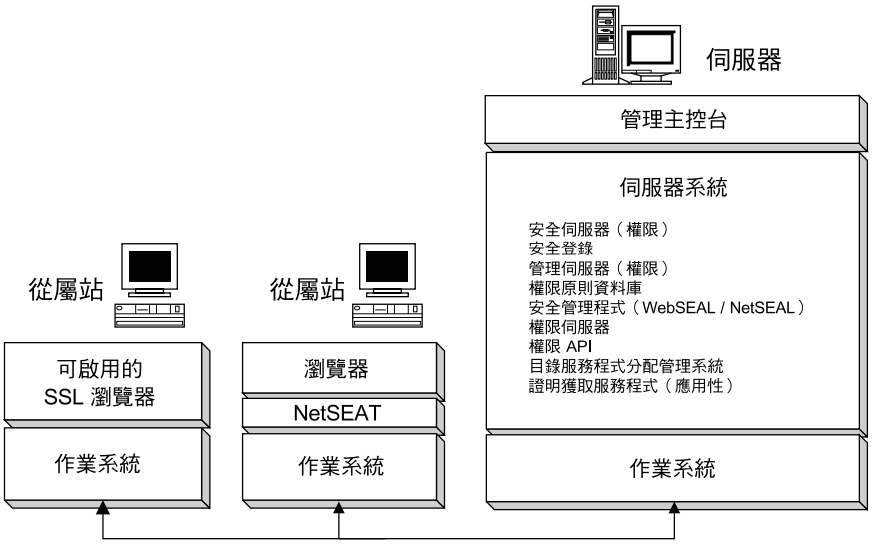
- Policy Director 伺服器日誌檔
- DCE 伺服器日誌檔
- DCE 有用性訊息
- 標準超文體傳送通信協定 (HTTP) 日誌檔

審核追蹤檔

- Policy Director 授權審核追蹤檔
- WebSEAL 審核追蹤檔
- Policy Director 管理審核追蹤檔
- DCE 審核追蹤檔
- LDAP 審核追蹤檔

Policy Director 元件

Policy Director 包含從屬站系統及伺服器系統使用的軟體。 Policy Director 提供 Sun Solaris、IBM AIX 及 Microsoft® Windows NT® 等作業系統平台的支援。



管理主控台

「管理主控台」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。您可以從「管理主控台」來執行帳戶登錄的管理作業以及主要（也就是主）授權原則資料庫。

典型的「管理主控台」作業包括新增及刪除使用者帳戶和群組帳戶，以及引用存取控制清單到名稱空間物件。「管理主控台」使用者可以保護 RPC，以透過安全通信通道來執行這些管理作業。

您可以將管理責任指派至本端層次。例如，您可以指定一位具備有限責任的特定安全管理者。然後，這位安全管理者管理安全原則的對象，只限於受保護物件名稱空間指定部分中的資源。

安全伺服器

安全伺服器 (secd) 可以是 LDAP 伺服器或 DCE 伺服器。「安全」伺服器提供身份驗證服務。它也會維護一個集中式登錄資料庫 (LDAP 或 DCE)，其中包含參與安全領域之所有有效使用者的帳戶項目。

在 DCE 環境中，登錄資料庫使用者有時會以 *Principal* 稱之。

「安全」伺服器扮演兩個重要的角色：

- 「安全」伺服器定義了使用者所屬的群組及組織，以及使用者可假設的角色。 集中式的登錄資料庫負責儲存這項資訊。 「Policy Director 權限服務程式」在進行授權決策時，會考慮這項資訊。
- 「安全」伺服器提供所有登入嘗試的身份驗證服務。

就 DCE 方面，安全伺服器可複製整個安全領域的登錄資料庫，以避免單點失敗。每當主要登錄發生變更時，安全伺服器負責更新所有的複本資料庫。

管理伺服器

「管理」伺服器（ivmgrd）會維護安全領域的主要授權原則資料庫。它也負責更新安全領域上的所有權限資料庫複本。 「管理」伺服器也會維護安全領域中的其他 Policy Director 伺服器的位置資訊。

安全管理程式

「安全管理程式」（secmgrd）引用存取控制原則，而這些原則是以複本、授權原則資料庫的資訊爲根據。安全管理程式包括：

- 一個 NetSEAL 元件，以進行粗略的「傳輸控制通訊協定/網際網路通訊協定」（TCP/IP）存取控制。
- 一個 WebSEAL 元件，以進行細微的 HTTP 及 HTTPS 存取控制。

WebSEAL

WebSEAL 是安全管理程式 (secmgrd) 的兩個元件之一。

WebSEAL 是一個高效能、多緒的 Web 伺服器，它能接受 HTTP、HTTPS 和 NetSEAT 的從屬站要求。 WebSEAL 管理下列資源的存取控制：

- 廣用資源位置 (URL)
- URL 基礎的正規表示式
- 以 Perl、C™ 或 C++ 寫成的通用閘道介面 (CGI) 程式
- 超本文標記語言 (HTML) 檔
- Java Servlet
- Java 類別檔

WebSEAL 是一部接合伺服器，可以透過「智慧型接合」技術，保護及管理協力廠商的 Web 伺服器。*智慧型接合*可讓您將其他的伺服器檔案系統連接到 Web 空間，並且將資源視爲單一、一致的物件名稱空間。

使用 WebSEAL 來爲 Web 型資源提供單一的登入功能。使用者利用標準的 Kerberos 或 SSL 來對 WebSEAL 進行身份驗證。然後 WebSEAL 會使用 HTTP 基本身份驗證及摘要身份驗證來表示使用者。WebSEAL 也可以將使用者的身份傳送成 CGI 變數。

NetSEAL

NetSEAL 是安全管理程式 (secmgrd) 的兩個元件之一。 NetSEAL 是一種虛擬專用網路（VPN）解決方案，可以保護所有進入的 TCP/IP 通信。 NetSEAL 會根據從屬站的目的地埠及身份來執行存取控制。 NetSEAL 是一種安全性解決方案，

- 可授權及保護傳統的網際網路服務程式，如 TELNET 及 POP3。
- 授權及保護不同的應用程式套裝軟體，如資料庫系統及網路管理工具。

NetSEAL 是一種資源管理程式，可控制使用者連接到伺服器上特定埠（例如，埠 23，TELNET）的能力。 NetSEAL 元件亦接受並授權自 NetSEAT 從屬站通過的 TCP/IP 流量。

使用 NetSEAL 伺服器可讓您整合任何網路應用伺服器及 Policy Director 安全性服務程式。 NetSEAL 伺服器爲所有的網路通信提供安全的通道終點。透過這個以 SSL 或 GSS 建立的通道，一併傳送鑑定過的使用者身份和原始的通信協定要求。請使用 NetSEAL SSL 通道來和 NetSEAT 從屬站進行通信。

NetSEAT 從屬站

NetSEAT 是一種網路支援模組。此種模組可透過所有從屬站/伺服器流量的 SSL 或 GSS 通道進行端對端加密，而不露痕跡地扮演從屬站應用程式的安全代理者 (Proxy) 角色。作爲施行安全從屬站的「動態鏈結程式庫」（DLL）， NetSEAT 可容許使用者完全利用 Policy Director 特性的優點。這些特性包括保護資料通信及提供高度有用性的配置。

NetSEAT 可確保與 Policy Director 安全機制的完全整合，並且爲從屬站提供資源管理。NetSEAT 提供了對 TCP/IP 應用程式的保護。 NetSEAT 通透地加密應用資料至 VPN 通道 (如 SSL 或 GSS)，它可以透過沒有安全保護的鏈結傳送 (如公用網際網路)。

它能夠配置成截取所有送出的 HTTP 要求，然後將它們轉遞目的地 WebSEAL 伺服器。它能夠允許重新定位或複製 Web 資源，而不影響一般使用者，以透通方式將邏輯 URL 對映到實體的 WebSEAL 伺服器。

註: 您不需要 NetSEAT 來與 Policy Director 相互作用。例如，從屬站使用者可使用啓用 SSL 的瀏覽器來直接與 WebSEAL 進行通信。

權限 API

「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。

Policy Director 權限 API 會減少應用程式開發的時間以及應用程式開發的成本。因爲權限 API 可提供所有網路安全的中央管理，降低所有權的總成本及安全破壞可能性。

權限伺服器

在遠端快取授權模式中，應用程式使用 Policy Director 權限 API 所提供的函數呼叫來和 Policy Director「授權」伺服器（ivacld）進行通信。 Policy Director「授權」伺服器會維護一份授權原則資料庫的複本，並且擔任授權決策評估者。

Policy Director 權限 API 會將授權決策要求轉遞到 Policy Director「授權」伺服器。Policy Director「授權」伺服器會根據安全原則來傳回建議。伺服器也可以撰寫一份審核記錄，其中包含授權要求的明細。

目錄服務分配管理系統

Policy Director 在 Policy Director 安裝期間，自動地安裝及配置「目錄服務分配管理系統 (DSB)」。Policy Director 提供 DSB 是作爲「管理伺服器」（ivmgrd）的一部分來分送。 使用 DSB 不需要額外的步驟。

如果 NetSEAT 從屬站是當成 Policy Director 伺服器及「管理主控台」的支援模組，則 NetSEAT 從屬站將會用到 DSB。如果 NetSEAT 從屬站只使用 SSL 通道機制，則不會用到 DSB。

DSB 運作方式和 Cell Directory Services (CDS) 中階伺服器一樣。NetSEAT 從屬站會直接向 DSB 要求取得資源位置及服務。接下來， DSB 聯繫安全領域的 CDS，解決要求。然後，DSB 傳回所要求的資訊給執行 NetSEAT 從屬站的系統。

證明獲取服務程式 (可選用)

Policy Director「證明獲取服務程式」（CAS）是一個可選用的元件。 Policy Director 在 Policy Director 安裝期間，自動地安裝「證明獲取服務程式」。

*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。

至於出自外部登錄中的非 Policy Director SSL 從屬站，則可藉由「Policy Director 證明獲取服務程式」（或藉由撰寫自己的證明獲取服務程式），讓*使用者名稱*對映到 Policy Director 身份。而使用從屬站端 X.509 憑證來存取的從屬站，可藉由「Policy Director 證明獲取服務程式」（或藉由撰寫自己的證明獲取服務程式），讓*憑證*對映到 Policy Director 身份。

或者，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，並處理身份驗證資訊，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。

瞭解安全模式

Policy Director 安全性表示對資訊的控制存取。 Policy Director 技術會將組織的安全原則對映到您受保護的名稱空間的物件。

您可以用企業原則作爲存取根據，而不必受限於網路技術。您可以根據使用者的身份以及他們的角色來允許或拒絕他們的存取權，而不必根據他們的實際位置。

Policy Director 元件是主從式基礎的應用程式。使用相互驗證及存取權指定可讓您將特定資源提供給一般有用性使用。同時，您可以將敏感的內部資源限制爲更安全授權的存取。不論授權使用者是從安全領域內或遠端網際網路連線來存取資料，您的資訊都是安全的。

定義安全原則

Policy Director 安全性軟體可讓您建立一個安全領域，這裡所有的通信都是受到保護的，不會有未經授權的存取及未偵測到的損壞。

安全領域的管理者必須識別以下各項：

- 誰可以參與安全領域，並且要求對受保護物件名稱空間中的物件進行存取。
- 您應保護的物件。
- 使用哪些規則來保護這些物件。

Policy Director 會以下列方式來處理從屬站要求：

- 證明那個從屬站正在使用身份驗證。
- 以授權證明的形式來取得權限。
- 根據這些證明來執行授權決策。

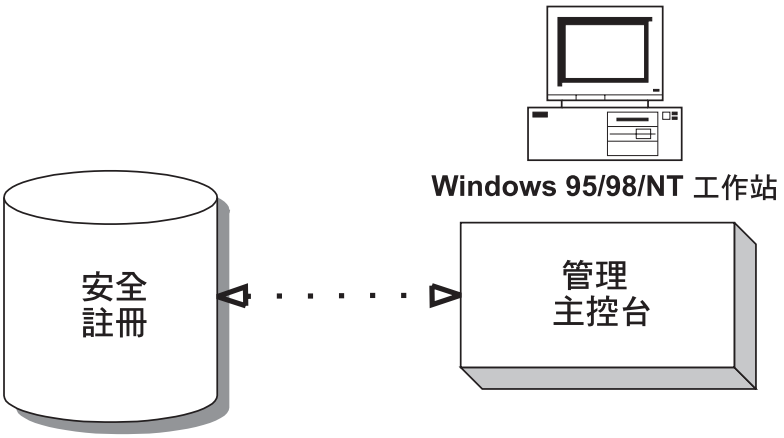
誰可以參與安全領域？

管理者會維護一份正式的清單，其中包含屬於 Policy Director 安全領域成員的使用者 (或在 DCE 環境中稱之爲 *Principal*) 和群組。因此，這些使用者及群組可以參與存取資源。登錄資料庫 (LDAP 或 DCE) 儲存這些使用者和群組的資訊。

一旦您爲該使用者建立帳戶，就可以授權使用者參與安全領域。

管理作業：

- 使用「管理主控台」來建立使用者和群組帳戶。 (或使用 **ivadmin** 指令。



您必須以什麼規則保護什麼物件？

Policy Director 可以保護以下的資源類型：

- Web 物件，例如 HTML 檔、CGI 程式及動態 HTML
- NetSEAL 支援的網路服務程式，如 TELNET、POP3 及自訂應用程式）
- 管理功能

Policy Director 會以物件代表受保護物件名稱空間中的實體資源。您可以將*原則模板*連接到這些物件，來指定特定的存取許可權。 Policy Director 使用的原則模版類型，稱之爲*存取控制清單*（ACL）。 ACL 負責定義以下項目：

- 誰可以存取物件。
- 您可以對物件執行哪些作業。

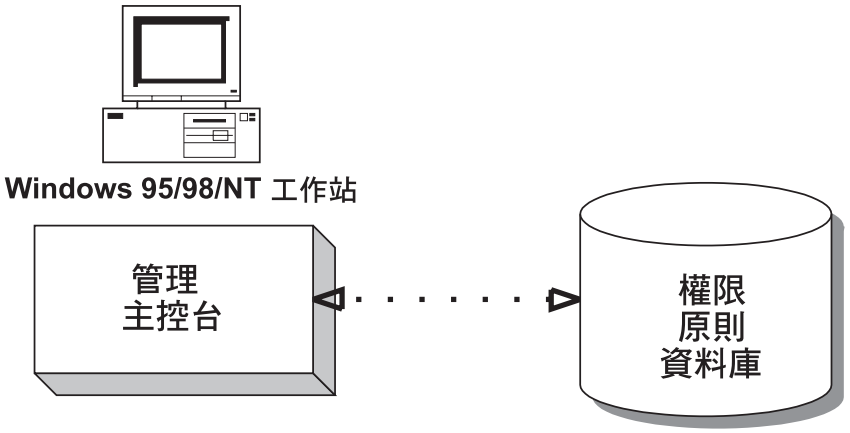
例如，您可以授與物件的檢視專用權給所有的群組，但是只容許一個群組來變更物件。

Policy Director 採用一種機制來設定廣域許可權即爲*稀疏（或承接的）ACL 模式*。在稀疏的 ACL 模式下，ACL 不是直接套用在階層中的每一個物件上。相反地，此模式採用承接 ACL 方式。如果階層中有物件沒有可套用的 ACL，則採用的 ACL 會是下一個出現在階層中較高層的 ACL。根物件 (/) 上必須有一個 ACL，以確保每一個物件皆可承接到 ACL。

當您使用廣域許可權機制時，您不必爲每一個檔案或目錄設定許可權。

管理作業：

- 使用「管理主控台」來對需要保護的物件引用原則模版 (ACL)，以便爲名稱空間定義安全原則。

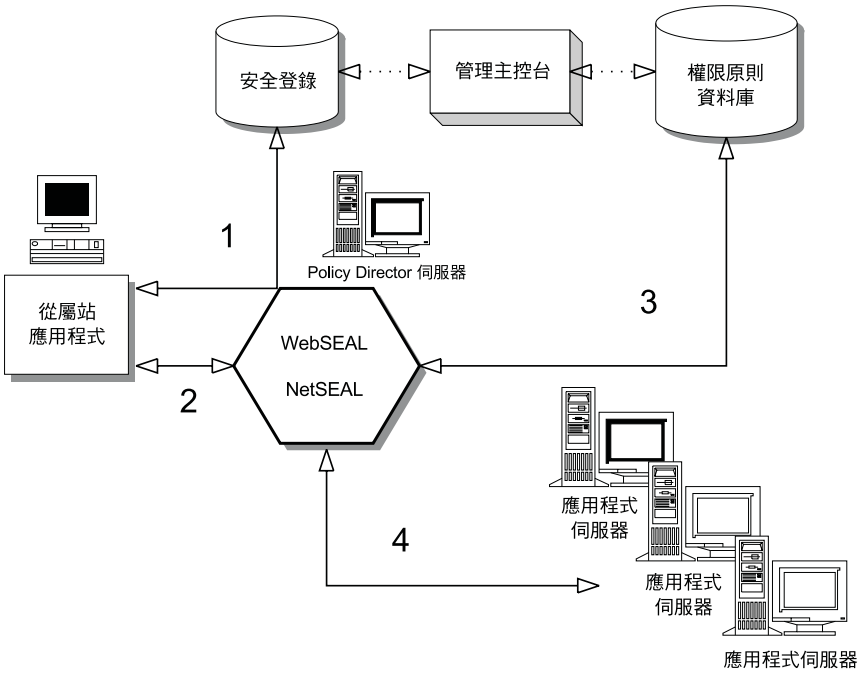


引用安全原則至從屬站要求

當使用者要求存取受保護的物件或應用程式時，在核准要求之前，Policy Director 會引用適當的身份驗證及授權檢查。

1. 從屬站使用者會驗證「安全」伺服器，以建立身份證明。Policy Director 透過公開與機密金鑰兩種方法來支援身份驗證。

   根據這個身份，「安全」伺服器會傳回使用者的授權證明。 證明定義了使用者所屬的群組及組織，以及使用者可假設的角色。



2. 安全通信通道是建立在從屬站使用者以及 Policy Director 伺服器之間。
3. 授權檢查會針對集中及複製的授權原則資料庫。Policy Director 會強制執行基於使用者證明爲基礎的 ACL。
4. 如果使用者證明的許可權，設定是適當的，Policy Director 會將要求傳送到應用伺服器以完成異動。

第2章 身份驗證及證明獲取

身份驗證是指識別嘗試登入安全領域之個體的程序。身份驗證的目標是證明從屬站的身份及取得說明從屬站的證明。證明可以讓 Policy Director 作爲授權、審核及其它服務使用。

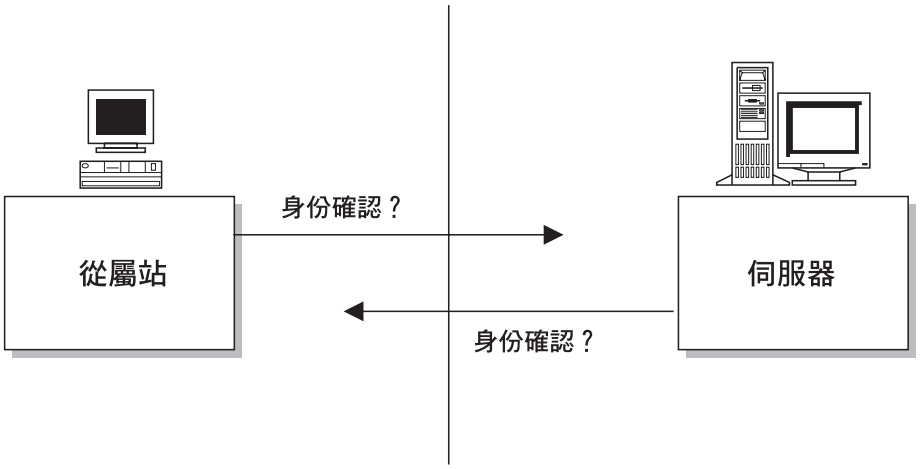
本章包括：

身份驗證基本概念

當伺服器強制執行安全領域中的安全性時，每一個從屬站必須提供其身份證明。安全領域中資源的存取如果是由伺服器控制，伺服器對身份驗證及授權的要求可以提供充分的網路安全性。

*身份驗證*是指識別嘗試登入安全領域之個體的程序。

在安全系統中，身份驗證與授權是有所區別的。*身份驗證*決定已驗證的使用者是否有權對特定資源執行作業。身份驗證可確保個體符合其宣稱的身份，但不指出可對資源執行作業的能力。



Policy Director 支援彈性的接近身份驗證，它可允許安全原則基於商業需求，而不是實體網路拓蹼的需求。

Policy Director 身份驗證在使用者登入安全領域時識別其身份，以存取受保護的資訊。使用者可以假設許多定義的角色 -- 每個角色具有不同的存取許可權。

身份驗證的目標

身份驗證處理程序達成二個重要的目標：

1. 確定從屬站的身份。
2. 取得從屬站的證明。

*身份驗證機制*及*證明獲取機制*是兩個完全不同的處理程序。 Policy Director 支援一些身份驗證機制 (參照『支援的身份驗證機制』)。

Policy Director 也提供獲取證明的預設及可自訂的服務。*證明獲取服務程式*將特定機制的本體資訊對映至 Policy Director 證明。 Policy Director 證明使用「延伸專用權屬性憑證 (EPAC)」格式。

*證明*是由需要關於從屬站資訊的 Policy Director 服務程式所使用。證明可以由 Policy Director 影響，執行多數服務，如：授權、審核及代表。

支援的身份驗證機制

Policy Director 支援私密/公開金鑰基礎的*身份驗證機制*：

秘密金鑰：

- Kerberos 版本 5
- 輕裝備目錄存取通訊協定（Lightweight Directory Access Protocol，LDAP）

公開/私密金鑰：

- 使用從屬站端 X.509 憑證透過 SSL 登入 -- Policy Director 支援與 PKIX 相容的公開金鑰基本設施 (PKI) 產品（如 IBM SecureWay Trust Authority 3.1 版）或以 Entrust 爲基礎的 PKI 產品（如 IBM Vault Registry 2.2.2 版）。

  需要證明獲取服務程式輔助才能獲取證明。

身份驗證類型

Policy Director 支援下列的身份驗證類型：

- SSL 身份驗證--網際網路及企業內網路身份驗證
- 使用者名稱及密碼身份驗證--使用者身份基礎的身份驗證
- Kerberos 身份驗證--網路身份驗證

SSL 身份驗證

安全 Socket 層次 (SSL) 通信協定提供網際網路的身份驗證、安全性及私密性。SSL 使用：

- 公開/私密配對金鑰身份驗證加密法
- 透過 SSL 連接加密資料的金鑰。

作爲身份驗證者，SSL 通信協定支援僅伺服器身份驗證及相互身份驗證。

Policy Director 支援 SSL 第 2 及第 3 版。

通信協定細節

建立在 TCP/IP 之上的 SSL 通信協定，是與應用程式無關的。 SSL 通信協定允許應用程式通信協定 (如 HTTP、FTP 及 TELNET) 通透地放在頂層。 在加密 SSL 通道之上操作的 HTTP Web 通信協定就是 *HTTPS*。

SSL 通信協定可以在資料被高階通信應用程式交換之前，協商加密鎖及驗證伺服器身份。 SSL 通信協定使用加密法、身份驗證及訊息身份驗證碼，維護傳輸通道的安全性及完整性。

協力廠商授信中心及憑證管理中心

SSL 身份驗證依靠身份驗證的主要雙方保證可信賴之協力廠商的基本信任。此可靠的協力廠商也就是*憑證管理中心* (CA)。

CA 是負責發出*數位式憑證* (電子身份識別)，它識別使用網路的個人、群組或系統，並向其他人證明 CA 信任擁有者。

CA 以數位簽字這些憑證，連結憑證的身份擁有者及憑證中的公開金鑰。任何信任 CA 者也應信任使用者。

網路使用者可取得 CA 本身的公開金鑰憑證，並用它來驗證其他使用者的憑證。有了此驗證，他們就有了保證，憑證中的公開金鑰是具名擁有者可信任的金鑰，且 CA (他們透過主要憑證所辨識並信任者) 保證此連結。

在已驗證身份的二方交換公開金鑰憑證之後，他們可以進行加密及對階段作業資料簽字。這個加密及數位簽字移除其他人可能在階段作業竊聽或干涉資料的可能性。

CA 可以爲在網際網路出售憑證的公司，或是爲您公司企業內網路負責發出憑證的部門。您必須決定夠信任那個 CA，以作爲其他人身份的識別者。

IBM SecureWay FirstSecure (FirstSecure) 組的安全性產品之一是 IBM SecureWay Trust Authority (Trust Authority)。此產品提供發出您公司企業內網路自己的憑證的能力。關於 FirstSecure 及其元件最新的資訊可在下列網站中取得：

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

X.509 數位式憑證

透過 SSL 的身份驗證是經由數位式憑證提供的。憑證是一個含有一些識別資訊的檔案。您自一可靠的憑證管理中心 (CA) 購買 (或接收) 憑證。CA 的主要責任是憑證使用者的確實性。

憑證是無法傳輸且無法僞造的檔案，它的作用如一種電子身份識別證或護造的類型。憑證可幫助確定使用者或電腦的確與本身宣稱的身份相符。檔案以 CA 的私密金鑰簽字，以保證其確實性及完整。

啓用 SSL 的瀏覽器使用企業標準的憑證類型，也就是*X.509*。第 3 版的 X.509 含有下列資訊：

- 版本
- 序號
- 簽名演算法 ID

- 發出者姓名
- 有效期間
- 主體 (使用者) 姓名
- 主體公開金鑰資訊
- 發出者唯一的 ID (發出憑證管理中心的識別名稱)
- 主體唯一的 ID (由憑證識別的個別的識別名稱)
- 副檔名 (僅供第 3 版使用)
- 供上列所示所有這些欄位的簽名

X.509 第 3 版標準允許更多的詳細識別資訊，如：憑證擁有者是在什麼企業，及他們在企業中有多久。憑證是由發出者簽字，以驗證主體 (使用者) 的姓名及使用者公開金鑰之間的連結。

憑證不證明最後人員或電腦是他們所宣稱的，但他們確實表示某些 CA 有程度的信任其人或電腦。當您信任發出憑證的 CA 時，當您與憑證持有者交換資訊時，會有某程度的信心。

SSL 身份驗證機制的基本概念

SSL *交握*通信協定是指交換信號以設定通信的程序。 SSL 交握通信協定可由二個階段構成：

- 『伺服器身份驗證使用伺服器端的憑證』
- 第19頁的『使用從屬站端憑證進行從屬站身份驗證』 (可選用)

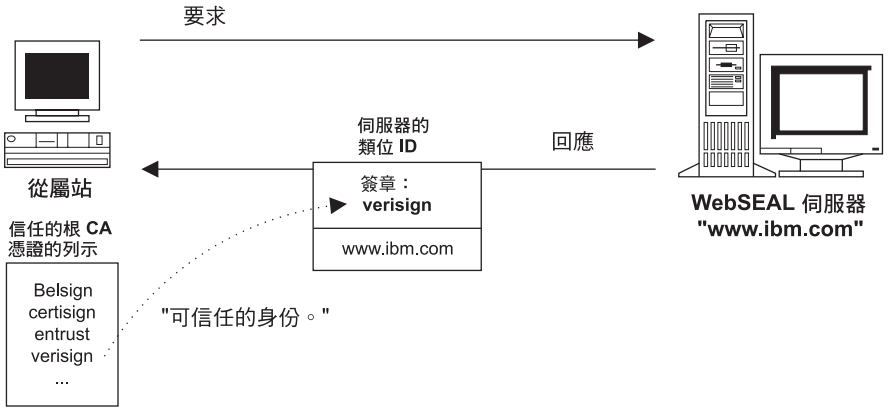
從屬站及伺服器都可以有憑證。伺服器必須恆有透過 SSL 身份驗證的憑證。可以透過 SSL 存取安全領域的從屬站可有或沒有從屬站端的憑證。

當伺服器傳送其憑證給從屬站時，此程序稱爲*伺服器身份驗證*。當從屬站傳送其憑證給伺服器時，此程序稱爲*從屬站身份驗證*。伺服器和從屬站身份驗證的組合也就是*相互驗證*。

伺服器身份驗證使用伺服器端的憑證

伺服器身份驗證是供 SSL 連接所需。透過 SSL 的伺服器身份驗證以下列方式完成：

1. 從屬站需要與啓用 SSL 伺服器的連接。
2. 回應時，伺服器對其憑證簽字 (但不加密)。然後，伺服器傳送含有伺服器公開金鑰的憑證給從屬站。
3. 從屬站使用包含在憑證檔中伺服器的公開金鑰，來驗證憑證所有人是否爲簽字的同一人。
4. 從屬站檢查憑證的發出者，是否其以檢查清單 CA 的瀏覽器之 主要 CA 憑證資料庫所接受。如果爲其接受者，從屬站會進行下一步驟；否則，瀏覽器通知它的使用者，此憑證爲不明未的 CA 所發出。然後，使用者負責接受或拒絕憑證。
5. 然後從屬站產生主要鍵，以伺服器的公開金鑰將它加密，並傳輸加密的主要鍵給伺服器。
6. 伺服器以主要鍵加密傳回訊息，復原主要鍵及給從屬站的身份驗證。後續的資料是以此主要鍵取得的金鑰加密。



使用從屬站端憑證進行從屬站身份驗證

伺服器以從屬站的公開金鑰解除從屬站數位式憑證的鎖定。從屬站公開金鑰憑證遵循 X.509 的語法。

使用透過 SSL 的從屬站端身份驗證以下列方式完成：

1. 在伺服器身份驗證完成之後，伺服器傳送查證給從屬站。
2. 從屬站在查證上傳回其數位簽名及公開金鑰憑證。數位化簽名使用從屬站的私密金鑰計算。
3. 伺服器使用包含在憑證檔中從屬站的公開金鑰，來驗證憑證所有人是否爲簽字的同一人。
4. 伺服器試著拿憑證與可靠的 CA 相比對。若從屬站的 CA 未清單爲可靠的，部份伺服器會結束處理，記載錯誤，並傳回訊息給從屬站。其它的伺服器可能選擇進行不需要此類動作的程序。
5. 當從屬站的 CA 可靠時，伺服器會完成處理。

就 SSL 連線上的身份驗證而言，不見得需要從屬站端的憑證。您仍可以交換加密的資訊。從屬站憑證確實對傳送加密資訊給正確對象的從屬站及伺服器提供額外的保證。 眞正的相互身份驗證是有可能需要從屬站憑證的。

不管那一種情況，當您的 CAS 伺服器已設定爲需要從屬站憑證供存取控制，當從屬站沒有有效的憑證時會被拒絕。

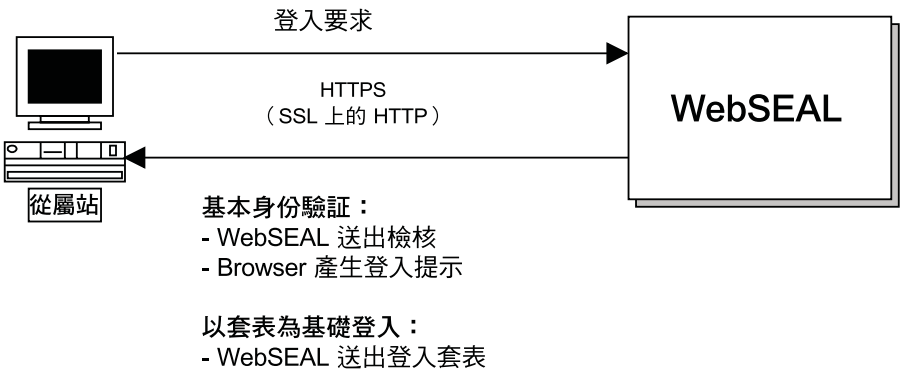
關於由公開及私密金鑰所使用的從屬站端 X.509 憑證的資訊，請參閱 第161頁的『X.509 憑證身份驗證方法』。

使用者名稱及密碼的驗證

身份驗證程序需要從屬站在登入期間提出某些形式的身份資訊。 Policy Director WebSEAL 支援使用者名稱及密碼的驗證。

有兩種使用者名稱及身份驗證方法提供此本體資訊：

- 基本身份驗證
- 基於套表的登入



請參閱第157頁的『使用者名稱和密碼的身份驗證方法』以取得關於使用者名稱及密碼表單中，需要從屬站本體資訊的身份驗證機制的完整資訊。

Kerberos 身份驗證

Kerberos 第 5 版是網路身份驗證的通信協定，它啓用雙方相互驗證，以達跨開放網路安全交換資訊的目的。

Policy Director 可以在下列交換中使用 Kerberos 身份驗證：

- 「管理主控台」對管理伺服器
- 「管理主控台」對安全伺服器
- 權限伺服器對管理伺服器
- WebSEAL 對管理伺服器
- WebSEAL 對 DCE 登錄 (供從屬站身份驗證)

Policy Director 伺服器使用 Kerberos 及 NetSEAT 從屬站網路模組，與其它 Policy Director 安全領域中的伺服器通信。NetSEAT 與 Policy Director 安全服務程式通信，並在交換資訊期間設定安全的 SSL 通道。

Kerberos 身份驗證是倚賴對第三方（可保證鑑定雙方的可信度）的根本信任。這個可靠的協力廠商安全性管理服務程式也就是*安全伺服器*。

Policy Director 安全伺服器 (secd) 實際上是儲存資料庫與安全相關資訊 (如，使用者名稱、群組及密碼) 的安全伺服器，也就是*登錄*。

Kerberos 採用一種共用、特定階段作業的機密金鑰機制（LDAP 機密金鑰），來支援伺服器間的相互身份驗證。Kerberos 的金鑰分送是依賴可靠的安全伺服器。 使用遠端程序呼叫 (RPC) 發生資訊交換。

Kerberos 身份驗證通信協定是複雜的一連串訊息交換。這一連串的訊息交換含有伺服器相互識別所需的金鑰及其它資訊。 Kerberos 的目標是避免所有參與方知道對方的金鑰。事實上，許多金鑰的使用期只限於交換期間。

證明獲取

身份驗證程序的主要目標之一是取得說明從屬站使用者的證明資訊。Policy Director 區分使用者的身份驗證和*獲取證明*。

使用者的身份一定不變。但是，定義使用者參與之群組或角色的憑證是會變的。特定上下文的憑證可因時間而變更。例如，當人員升遷時，憑證必須反映新的責任層次。工作上人員的憑證也和使用者銀行的憑證不同。

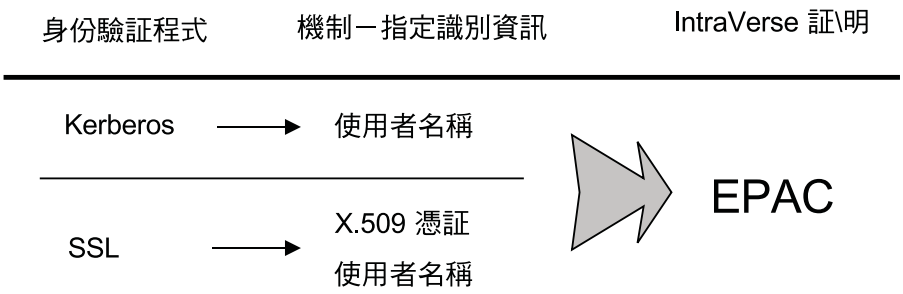
身份驗證程序產生特定機制使用者本體資訊。然後此資訊必須變成 (*對映*) 一般的領域表示及格式。Policy Director 使用 EPAC 格式。

特定機制的本體資訊

對「證明獲取服務程式」，不同的身份驗證機制提供不同的使用者本體資訊：

- Kerberos 是基於使用者名稱 (及密碼)。
- X.509 從屬站端數位式憑證提供 X.509 的欄位資訊。
- 基本的身份驗證及格式基礎的登入方法 (SSL) 是基於使用者名稱 (及密碼)。

下圖說明指定身份驗證機制中可用的識別資訊種類，並說明如何在 SSL 上使用證明獲取服務程式，將資訊轉換爲 EPAC 格式。



特定機制本體資訊 (例如，密碼、配對金鑰及憑證) 代表使用者的實體身份性質。此資訊用來建立伺服器的安全階段作業。

代表安全領域中的使用者角色產生的證明，說明在特定上下文的使用者，且僅對當階段作業之生命週期有效。

EPAC 憑證

證明是由需要關於從屬站資訊的 Policy Director 服務程式所使用。例如，Policy Director 權限服務程式使用憑證來決定使用者是否授權在安全領域中保護的資源上執行特定的作業。

使用 ACL 的方法之一是供 Policy Director 使用包含整體唯一 ID (UUID) 的 EPAC。Policy Director 對其它服務使用憑證，如：

- 審核服務程式
- WebSEAL 及 NetSEAL 接合的代表功能

下列的 EPAC 欄位適合 Policy Director：

屬性	說明
安全領域 ID	使用者的起始安全領域 ID
Principal UUID	使用者（DCE 方面則爲 “Principal”）的 UUID
群組 UUID	使用者所屬群組的 UUID 或 UUID

特定機制身份驗證資訊必須轉換成 EPAC 資訊：

- Policy Director 從屬站自動由 WebSEAL 對映到證明。
- 來自外部登錄的非 Policy Director SSL 從屬站，可透過外部的證明獲取服務程式將使用者名稱對映到 Policy Director 身份。
- 使用從屬站端 X.509 憑證來存取的從屬站，可透過外部的證明獲取服務程式將憑證資訊對映到 Policy Director 身份。

信任鏈

SSL 通信協定在瀏覽器從屬站和 WebSEAL 伺服器之間交換期間,伺服器傳遞伺服器信任之 CA 的憑證的瀏覽器清單。這會導致瀏覽器顯示下列瀏覽器從屬站憑證清單給使用者：

- 由這些 CA 之一所簽字。
- 信任鏈和伺服器信任的 CA 之一間的關係所信任--從屬站憑證是由伺服器所信任之 CA 簽字。

此種程序亦稱爲*憑證鏈*。

瀏覽器使用者選取這些從屬站憑證之一來傳輸給伺服器。若從屬站憑證直接由伺服器信任的 CA 之一所簽章，則瀏覽器只傳輸從屬站的憑證給伺服器（假設伺服器已有負責簽章之 CA 的憑證）。

若從屬站憑證不是直接由伺服器信任的 CA 之一所簽章，則瀏覽器會建構並傳輸一條 CA 憑證鏈，以說明從屬站憑證與伺服器所信任之 CA 之一間的信任鏈。

同樣的，瀏覽器實際上不傳輸伺服器信任 CA 的憑證。它假設伺服器已經有憑證。

Policy Director secmgrd.conf 配置檔中列有 Policy Director 信任的 主要 CA 憑證。所以 Policy Director 信任由這些 CA 發出的從屬站憑證。

伺服器取得由瀏覽器傳輸的每個 CA 憑證，並驗證：

- 憑證爲 CA 憑證。
- 簽字 CA 的簽名。
- 憑證未過期。

當一個 CA 信任第二個 CA (它信任第三個及之後的 CA) 時，已建立*信任鏈*。若 Policy Director 信任任何信任鏈中的 CA，它應可以信任從屬站憑證。

證明獲取服務程式概觀

*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*從屬站證明*。

自身份驗證程序衍生的證明是由需要關於從屬站資訊的 Policy Director 服務程式所使用。這種服務的範例包括授權及審核。Policy Director 的主要工作依每個從屬站可用的憑證而不同。

Policy Director 使用 EPAC 格式來代表由身份驗證程序衍生的證明資訊。

Policy Director 自動爲下列 SSL 從屬站產生憑證：

- 安全領域的成員。
- 以有效的使用者名稱及密碼身份驗證。

在這種情況下，您提供的使用者名稱及密碼必須符合預設登錄 (LDAP) 中現存的帳戶項目。

另有其它可能的情形，從屬站存取不適用以上模式：

- 從屬站不屬於預設的 Policy Director 登錄。
- 從屬站使用從屬站端憑證完成存取。

在這些情形下，Policy Director 必須靠自訂的身份驗證及可達成下列行爲的對映服務程式：

- 在這些從屬站執行身份驗證。
- 參照外部 (協力廠商) 帳戶登錄。
- 對映外部本體資訊至 Policy Director 身份。

此種自訂的身份驗證與對映服務程式亦稱爲*外部證明獲取服務程式* (CAS)。

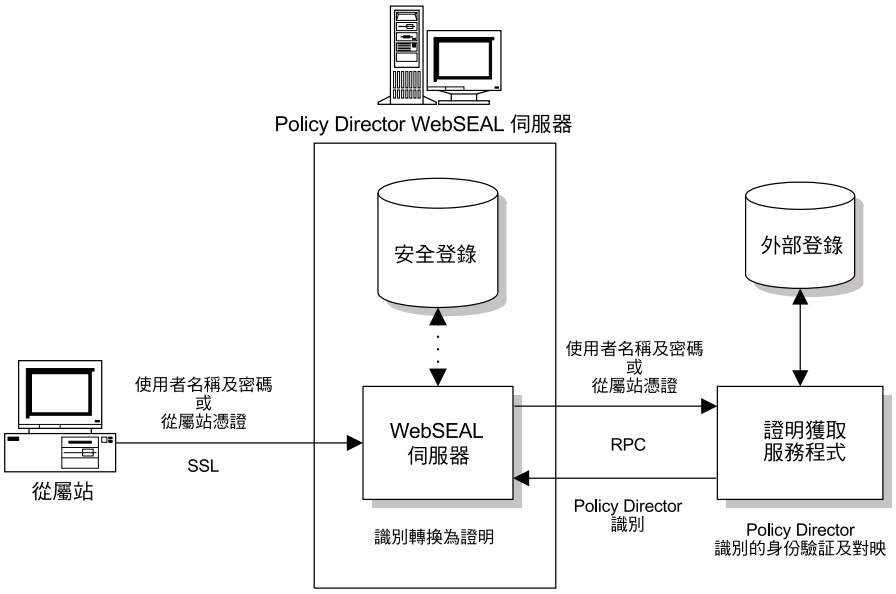
證明獲取服務程式簡介

在「證明獲取服務程式 (CAS)」結構下，您可用自訂的外部身份驗證程序（即參照使用者登錄而非 Policy Director 安全登錄）取代預設的 WebSEAL SSL 身份驗證程序（以使用者名稱與密碼爲依據）。自訂的證明獲取服務程式亦會將任何特殊身份資訊（憑證、記號）適當對映至 Policy Director 身份。

證明獲取服務程式必須由管理者自訂與撰寫，以便爲安全領域提供特定的解決方案。

證明獲取服務程式必須使用 RPC 來保證 WebSEAL 及 CAS 伺服器之間全部的通信安全。

證明獲取服務程式可讓在 Policy Director 登錄中並無帳戶的使用者參與安全領域。證明獲取服務程式可鑑定該使用者（必要時則使用外部登錄）。之後，證明獲取服務程式會將 Policy Director 身份傳回給 WebSEAL 以便轉換爲證明。 Policy Director 使用這些證明讓使用者參與安全領域。



對於很難（或根本不可能）移轉到 Policy Director 平常所用之登錄的傳統使用者資料庫，證明獲取服務程式亦能處理之。範例傳統系統會包含客戶 ID 及 PIN 機制 (記號)。這樣的傳統身份驗證機制透過它自己的登錄資料庫驗證使用者資訊。

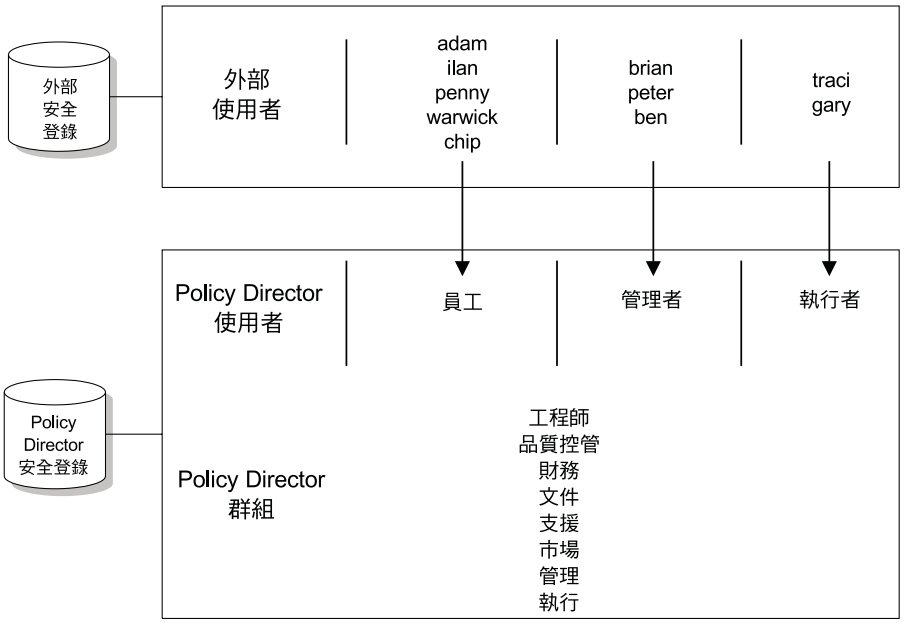
「Policy Director 授權應用程式開發者套件 (IVAuthADK)」中提供了一個示範用 CAS 伺服器。此伺服器定義出 WebSEAL 與證明獲取服務程式間的介面 (IDL)。如果您正在撰寫自己的證明獲取服務程式，ADK 還提供您原始碼。

多對一對映解決方案

證明獲取服務程式適合*多對一*解決方案；亦即，模組可讓您將眾多傳統帳戶對映至一個 Policy Director 使用者。

在多對一對映的情形下，Policy Director 使用者等於扮演整個群組（其成員全是傳統資料庫中的使用者）的角色。多對一對映解決方案對對映相同使用者的全部使用者，產生相同的存取權、可見度及責任。全部對映至特定使用者的使用者有完全相同的許可權。 當決定您的安全原則時，必須正視此項事實。

下圖中，外部登錄的使用者可能對映到單一 Policy Director 使用者。例如， Policy Director 使用者 (員工) 行爲和外部登錄使用者集成的角色相同。雖然使用者對映至相同的 Policy Director 帳戶，他們也可以要指定到一個或以上 Policy Director 群組的成員資格，得到個別的區分。Policy Director 授權決策可以基於使用者身份及群組成員資格。



註: 其多對一對映的責任層次並未仔細規劃。審核服務僅追蹤 Policy Director 使用者--非對映到此使用者的個別使用者。

功能模式

「證明獲取服務程式」可撰寫成處理身份驗證資訊，如從屬站憑證、使用者名稱及記號。須將 WebSEAL，配置爲接受非登錄 SSL 從屬站及爲身份驗證遞送身份驗證資訊給適當的證明獲取服務程式，並對映到 Policy Director 身份。

證明獲取服務程式基於從屬站提供的特定本體資訊，執行其身份驗證及身份對映。因此，證明獲取服務程式可撰寫成在下列一種可能的模式下執行：

- 『X.509 憑證對映模式』
- 第27頁的『使用者名稱對映模式』

有關使用自訂-撰寫之證明獲取服務程式的說明，請參閱第30頁的『自訂證明獲取服務程式』。

X.509 憑證對映模式

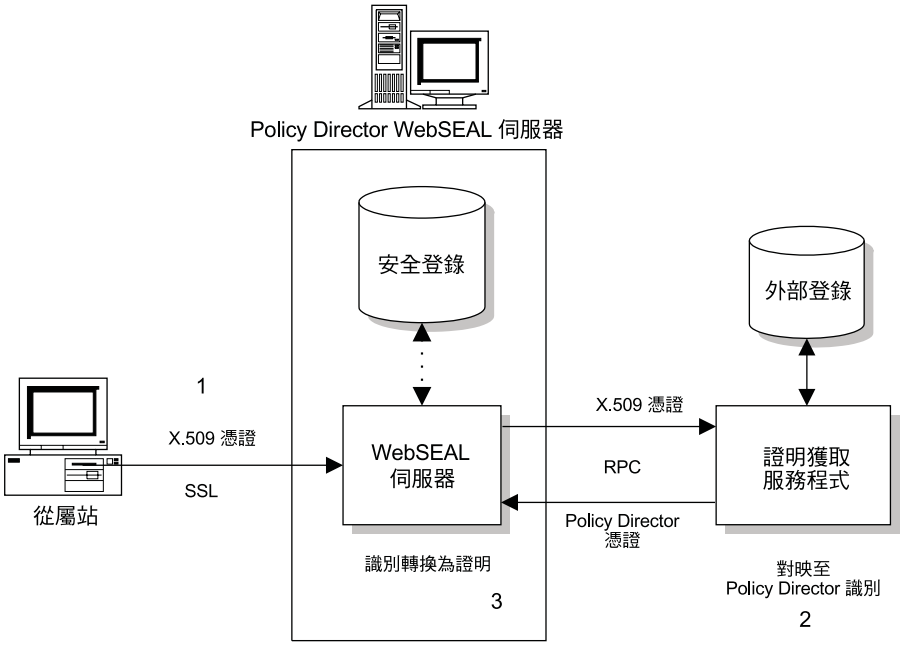
透過任何「證明獲取服務程式」，Policy Director 可以支援透過憑證 SSL 使用數位 X.509 憑證從屬站的身份驗證。「證明獲取服務程式」 X.509 模式將包括在從屬站端 X.509 數位式憑證中特定的資訊，對映至 Policy Director 身份。此 Policy Director 身份會傳回將它轉換成適當憑證的 WebSEAL。

在下列狀況的 X.509 模式是適當的模式：

1. 透過 SSL 通信的從屬站。
2. 使用 X.509 數位式憑證身份驗證的從屬站。
3. 需要存取 Policy Director 安全領域中受保護的資源從屬站。

CAS 伺服器可以用一對一基礎或多對一基礎將憑證資訊對映至 Policy Director 身份。對映服務程式的目標是提供 Policy Director 權限服務程式有用的憑證，以作授權決策。

下圖說明當 WebSEAL 爲 X.509 憑證對映配置成使用「證明獲取服務程式」時之事件順序。



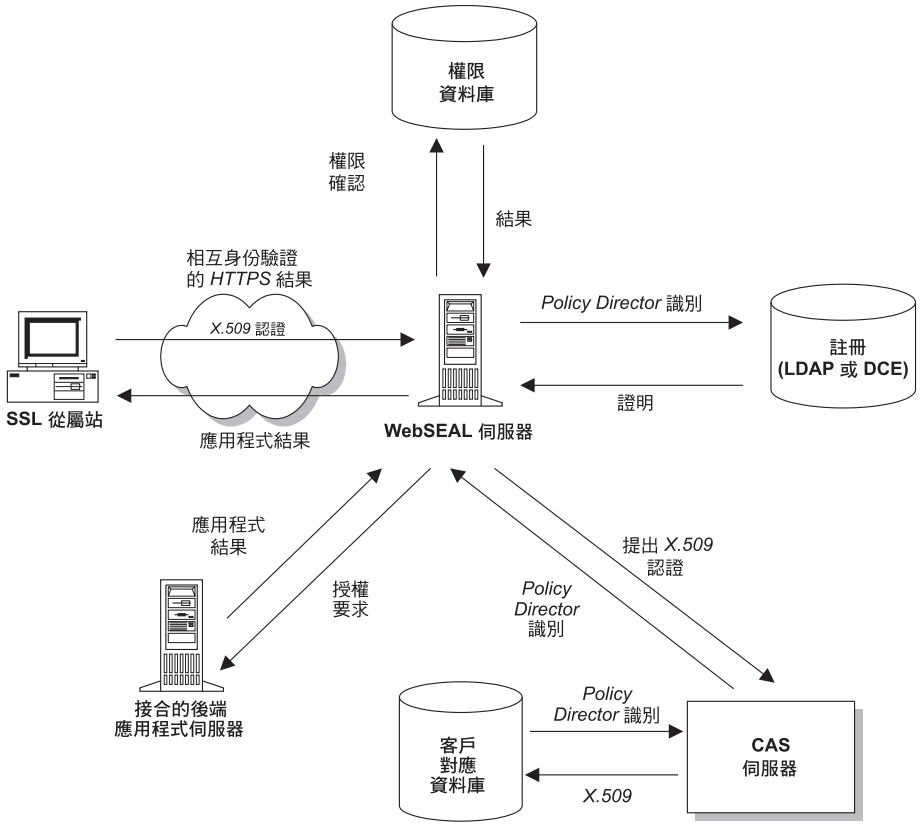
1. 從屬站透過 SSL 及呈現 X.509 憑證存取 WebSEAL。

   請注意身份驗證是在此時透過公開及私密金鑰憑證交換完成。剩下「證明獲取服務程式」唯一的工作是對映使用者憑證。
2. CAS 伺服器從驗證憑證取得本體資訊 (特定的應用程式)，並對映資訊至已知的 Policy Director 身份。CAS 伺服器可使用外部 (協力廠商) 登錄。
3. Policy Director 身份傳回 WebSEAL，然後使用其預設登錄轉換身份爲適當證明。

在 X.509 模式下使用證明獲取服務程式

下圖說明當從屬站 (使用 X.509 憑證存取 WebSEAL) 要求安全領域資源發生時，完整的事件順序。

1. 憑證資訊以傳回 Policy Director 身份至 WebSEAL 的「證明獲取服務程式」，對映到此身份。
2. WebSEAL 從此身份建立證明，並使用證明作對包含結合應用伺服器上受保護資源作授權決策。



使用者名稱對映模式

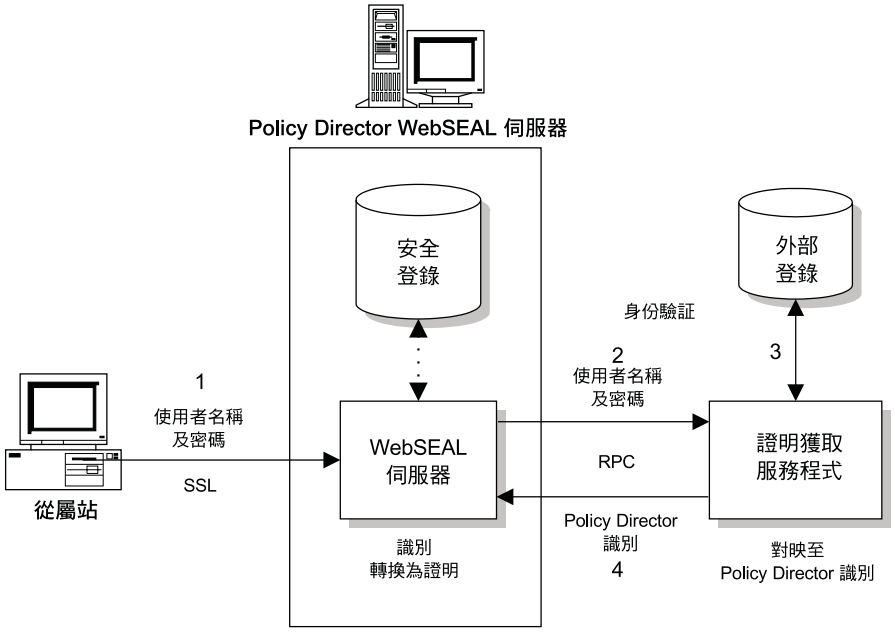
另一種身份驗證與身份對映的類型是「使用者名稱對映」模式。使用使用者名稱對映模式，您可以用參照使用者登錄-- 不同於預設 Policy Director 登錄 (LDAP) 之自訂外部程序代替預設的身份驗證程序。

使用 SSL 的標準 Policy Director 身份驗證需要使用者以使用者名稱及密碼登入。此身份的驗證及憑證獲取是決定於 Policy Director 登錄。

此類型證明獲取服務程式的主要值，是要適應很難或不可能移轉到 Policy Director 登錄的大型主機使用者資料庫。

下圖說明當 WebSEAL 爲使用者名稱對映配置成使用「證明獲取服務程式」時之事件順序。

1. 從屬站透過 SSL 以使用者名稱及密碼存取 WebSEAL。
2. WebSEAL 配置成將使用者名稱及密碼傳給「證明獲取服務程式」，以進行身份驗證及取得憑證。



3. 證明獲取服務程式使用外部 (協力廠商) 登錄來驗證使用者身份，然後對映到 Policy Director 身份。
4. Policy Director 身份傳回 WebSEAL，然後使用其預設登錄轉換身份爲證明。

此模式最好作爲多對一解決方案使用；即模組可讓您對映許多大型主機帳戶至一個 Policy Director 使用者。請參閱第24頁的『多對一對映解決方案』。

身份驗證服務程式的選擇

您可選擇下列一種身份驗證服務程式類型：

- 預設的「Policy Director 證明獲取服務程式」（請參閱『Policy Director 中提供的 CAS』）。
- 自訂-撰寫的證明獲取服務程式（請參閱第30頁的『自訂證明獲取服務程式』）。

Policy Director 中提供的 CAS

Policy Director 會提供自己的從屬站身份驗證服務程式元件 --「Policy Director 證明獲取服務程式」 (Policy Director CAS)。當您以 LDAP 做爲使用者登錄時，可支援 Policy Director CAS。

您必須藉由檢查與更新 iv.conf and the secmgrd.conf 配置檔（請參閱第163頁的『配置「Policy Director 證明獲取服務程式」』），將 WebSEAL 配置成使用 Policy Director CAS 來處理身份驗證。

Policy Director CAS 會將瀏覽器（啓用 SSL）提供的*從屬站數位憑證*對映至 Policy Director 使用者身份。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。 Policy Director CAS 會試著將收到的憑證對映至 Policy Director 所知的使用者身份。

已經撰寫 Policy Director 「證明獲取服務程式」提供支援使用一個或二個從屬站端 X.509 第 3 版的憑證透過 SSL 登入：

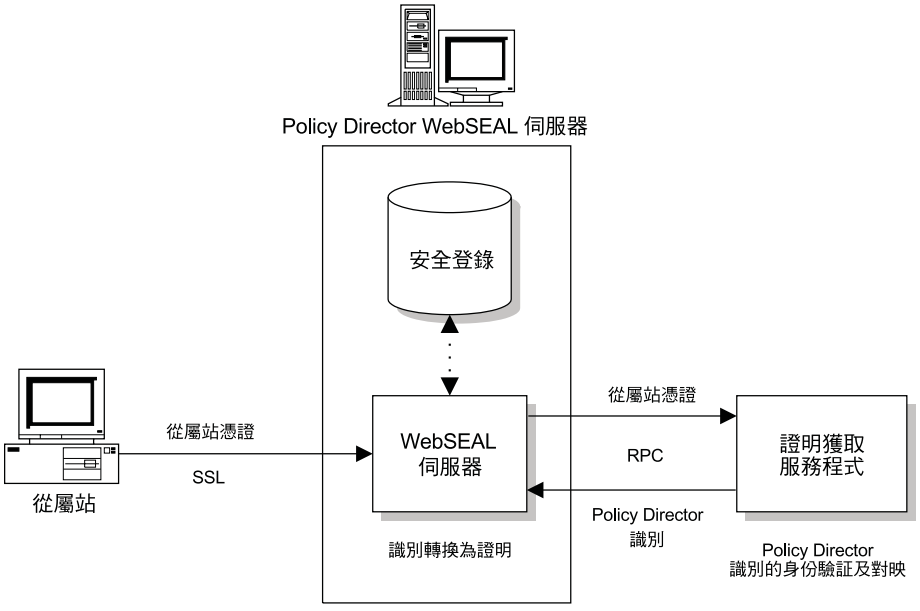
- 與 PKIX 相容的產品（例如，IBM SecureWay Trust Authority 3.1 版）
- 與 Entrust 相容的產品（例如，IBM Vault Registry 2.2.2 版）

所有憑證在傳輸時全以「識別編碼規則 (DER)」編碼而成。

RPC 介面使用在 Policy Director 「證明獲取服務程式」及 WebSEAL 之間。Policy Director 「證明獲取服務程式」使用 RPC 來保證 WebSEAL 及 CAS 伺服器之間全部的通信安全。因爲 Policy Director 「證明獲取服務程式」是 DCE-RPC 應用程式，需要 DCE 從屬站執行相關的從屬站身份對映。

預設的「Policy Director 證明獲取服務程式」：

- 可讓您使用從屬站端的憑證或將其指定爲選用的。
- 不執行任何相關憑證廢止清冊 (CRL) 的檢查。
- 支援憑證鏈
- 支援一對一對映的解決方案



一對一對映解決方案

Policy Director「證明獲取服務程式」使用一對一對映模式。採一*對*一模式將個別的傳統帳戶對映至單一使用者，需要高度的帳戶維護。不過，在 Policy Director CAS cdas.conf 配置檔中， Policy Director 管理者可建立一份表格，讓憑證的識別名稱 (DN) 連結 Policy Director (LDAP) 使用者的 DN。

當 WebSEAL 拿著憑證呼叫 Policy Director CAS 時， CAS 會先擷取憑證中的 DN，並在表格中尋找相符項。如找到相符項， 「Policy Director 證明獲取服務程式」會將 Policy Director 使用者的正確 DN 格式，傳回給 WebSEAL。之後，WebSEAL 即以這個 DN 來識別 Policy Director (LDAP) 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 (LDAP) 使用者。而 WebSEAL 伺服器會使用傳回的 DN 來擷取使用者的證明。

必要的管理作業

需要爲 Policy Director 「證明獲取服務程式」設定的管理作業包括：

1. 必要時藉由檢查與更新 iv.conf 與 secmgrd.conf 配置檔將 WebSEAL 配置成使用 CAS 來處理身份驗證（請參閱第163頁的『配置「Policy Director 證明獲取服務程式」』）。
2. 視需要更新 cdas.conf 配置檔中的 DN 對映表區段（請參閱第165頁的『識別名稱對映』）。

「證明獲取服務程式」機能

Policy Director「證明獲取服務程式」可以用來提供下列功能：

- 由 WebSEAL 拿著憑證呼叫 Policy Director CAS。
- Policy Director CAS 擷取憑證中的 DN，並在 DN 對映表中尋找相符項。
- 如找到相符項：
  - 「Policy Director 證明獲取服務程式」將相關的 Policy Director 使用者 DN 傳回給 WebSEAL。
  - 之後，WebSEAL 即以這個 DN 來識別 Policy Director 使用者。
- 如找不到相符項：
  - CAS 將憑證中的 DN 傳回給 WebSEAL。
  - 以憑證中的 DN 來識別 Policy Director 使用者。
  - WebSEAL 伺服器使用傳回的 DN 來擷取使用者的證明。

自訂證明獲取服務程式

因爲每個應用伺服器及其相關的身份驗證組織配置的不同，無法撰寫一個證明獲取服務程式，可以適合所有的需求。因此，我們在 Policy Director 的 IVAuthADK 套裝軟體中提供了一個示範 CAS 伺服器原始碼。這個示範的 CAS 伺服器可以採用作爲生產 CAS 伺服器基本的組織配置--有新增的特定應用程式使用者名稱對映及對映管理功能。

WebSEAL，以接受非登錄 SSL 從屬站及爲身份驗證遞送身份驗證資訊給適當的證明獲取服務程式，並對映到 Policy Director 身份。

自訂-撰寫的 CAS 必須使用 RPC 來保護 WebSEAL 與 CAS 伺服器間的所有通信。

對映 X.509 憑證資訊至 Policy Director 身份的基本要求，因客戶的不同，而有很大的差異。雖然 Policy Director 在定義對映服務程式上並未制訂任何一般規則，但 Policy Director 中的兩項規定將有助於想設定自訂對映服務程式的管理者：

1. Policy Director 會定義一種 IDL 介面讓開發者可撰寫自己的服務程式，用以將 X.509 憑證資訊對映到 Policy Director 身份。此 IDL 介面詳細內容可在*Policy Director 程式設計及參考手冊*中找到。
2. Policy Director 包括施行對映服務程式的範例，此服務程式提供僅傳回每個失敗要求的 CAS 伺服器組織配置。此組織配置可以進一步發展至產生 CAS 伺服器。

   範例服務程式原始程式包括在 Policy Director IVAuthADK 安裝套裝軟體中。

必要的管理作業

設定自訂 CAS 必要的管理作業包括：

1. 撰寫由 Policy Director 提供，使用 IDL 介面的自訂 CAS。
2. 配置 WebSEAL 來使用身份驗證的外部證明獲取服務程式。

自訂 CAS 機能

自訂 CAS 介面可以用來提供下列功能：

- 對與預設 Policy Director 不同的使用者登錄，執行使用者名稱及密碼驗證。
- 對映許多使用者至相同的 Policy Director 身份。
- 管理外部使用者密碼。
- 加入自訂審核資訊至證明。Policy Director 將整個證明寫入其審核日誌中。

第3章 瞭解授權

*授權*是決定識別的實體是否有權執行以下項目的程序：

- 啓動特定的服務程式。
- 對安全領域中的特定資源執行作業。

「Policy Director 權限服務程式」可藉由控制授權決策進行的程序，來協助強制執行網路的安全原則。

本章包括：

授權的概念模式

當伺服器強制執行安全領域中的安全性時，每一個從屬站必須提供其身份證明。反之，安全原則決定該從屬站對要求的資源是否有執行作業的許可權。伺服器控制對安全領域中的每一個資源的存取。基於這個原因，伺服器對身份驗證及授權的要求可以提供充分的網路安全性。

*身份驗證*是指識別嘗試登入安全領域之個體的程序。

在安全系統中，身份驗證與授權是有所區別的：

- *身份驗證*是指識別嘗試登入安全領域之個體的程序。身份驗證可確保個體符合其宣稱的身份，但是不指出可對受保護資源執行作業的權力。
- *權限*決定已驗證的從屬站是否有權對安全領域中的特定資源執行作業。在授權模式中，Policy Director 可完成授權原則，不依賴使用者身份驗證所使用的機制。使用者可利用公開/私密金鑰或機密金鑰，或客戶定義的機制來驗證其身份。

身份驗證程序的其中一部分涉及證明的獲取，這份證明說明了從屬站的身份。權限服務程式會根據使用者的證明來進行授權決策。

安全領域中的資源會接收由領域的安全原則所指定的保護層次。安全原則定義了可容許的安全領域參與者，以及每一個要求保護的資源周圍的保護程度。

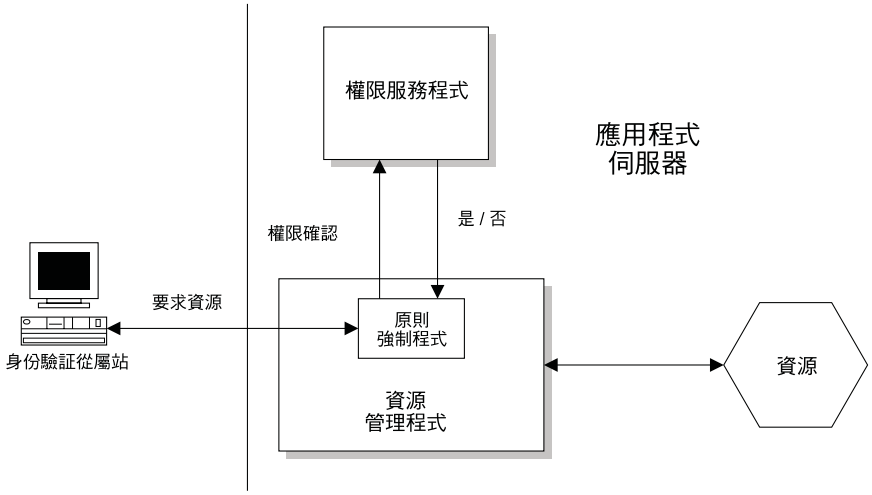
授權程序的基本元件包括：

資源管理程式

當 Policy Director 授與權限時，資源管理程式負責執行所要求的作業。資源管理程式的其中一個元件是負責將要求導入權限服務程式以進行處理程序的「原則強制執行程式」。

權限服務程式

權限服務程式應要求來執行決策動作。



傳統的應用程式會將原則強制執行程式以及資源管理程式連結到一個程序中。這個結構的範例包括 Policy Director WebSEAL 及協力廠商應用程式。 這些授權元件的獨立功能，在設計安全性強制執行策略時可有更多彈性。

例如，此類獨立性可讓安全管理程式控制下列項目：

- 程序的位置。
- 爲程序撰寫程式碼的人員。
- 程序執行作業的方式。

標準權限服務程式的優點

在大部分的系統中（大型主機或新型系統），授權和個別的應用程式是緊密相關的。公司通常會持續建置應用程式來滿足企業需求。許多應用程式需要某些特定形式的授權。

因此常常導致很多應用程式具有不同的授權施行方法。這些所有人授權施行方法需要個別的管理，它們難以整合，因而導致所有權需要更高的成本。

分散式權限服務程式可以提供這些獨立的應用程式一個標準的授權決策機制。

標準的權限服務程式可提供下列好處：

- 減少開發及對應用程式管理存取權的成本。
- 減少擁有及管理個別授權系統的總成本。
- 對於現存安全基本設施的影響力。
- 容許新的企業更安全地進行開放。
- 啓用更新、更不一樣的應用程式類型。
- 容許較短的開發週期。
- 安全地共用資訊。

Policy Director 權限服務程式的優點

Policy Director 可以將現存的大型主機及與現有的基本設施整合在一起。 Policy Director 提供安全、集中式原則管理能力。 「Policy Director 權限服務程式」--和 WebSEAL 以及 NetSEAL 資源管理程式--可爲企業網路系統提供一個標準的授權機制。

現存的應用程式可以利用權限服務程式的優點，而不必修改應用程式本身。 Policy Director 會根據使用者角色或群組角色執行它的授權原則。您可以將授權原則引用至以下各項：

- 網路伺服器
- 個別交易或資料庫要求
- 特定的 Web 型資訊
- 管理活動
- 使用者定義的物件

Policy Director 權限 API 可容許現存的應用程式呼叫「Policy Director 權限服務程式」。反之，權限服務程式會根據企業的安全原則來進行決策。請參閱第42頁的『Policy Director 權限 API』。

Policy Director 權限服務程式也可以擴充。您可以配置權限服務程式，以使用外部 Policy Director 權限 API，呼叫其他的權限服務程式來進行其他的處理。

「Policy Director 權限服務程式」提供下列好處：

- 和應用程式無關。
- 使用標準的授權編碼樣式，且其樣式和語言無關（Policy Director 權限 API）。
- 它是集中管理的，因此很容易管理。例如，加入一位新員工需要變更某個中央位置的專用權資料庫，而不必跨越多個系統。
- 它是針對跨平台之異質環境中，提供安全服務的應用程式。
- 它會透過外部權限服務程式功能，整合現存非 Policy Director 的授權系統。
- 它具有可調整及彈性的配置，可輕易整合現存的基本設施。
- 它啓用多層次的授權--服務程式會透過應用程式程序或異動的多重層次來傳送證明封包。
- 它使用共同及有效的審核模式。
- 它與任何身份驗證機制無關。

Policy Director 權限服務程式

「Policy Director 權限服務程式」負責授權決策的程序，以協助強制執行網路安全原則。由權限服務程式所進行的授權決策可核准或拒絕從屬站對安全領域中受保護資源執行作業的要求。

Policy Director 權限服務程式元件

「Policy Director 權限服務程式」是由三個基本元件組成：

- 主要（主）授權原則資料庫
- 管理伺服器

- 授權決策評估程式

主要授權原則資料庫

主要授權原則資料庫包含安全領域中所有資源的安全原則資訊。資料庫也包含與安全領域參與者相關的所有必要證明資訊。

使用「Policy Director 管理主控台」來輸入及變更這個資料庫的內容。

管理伺服器

管理伺服器（ivmgrd）會執行以下的作業：

- 維護主要授權原則資料庫。
- 將這份原則資訊複製到整個安全領域中。
- 每次變更主要授權原則資料庫時，即更新資料庫複本。

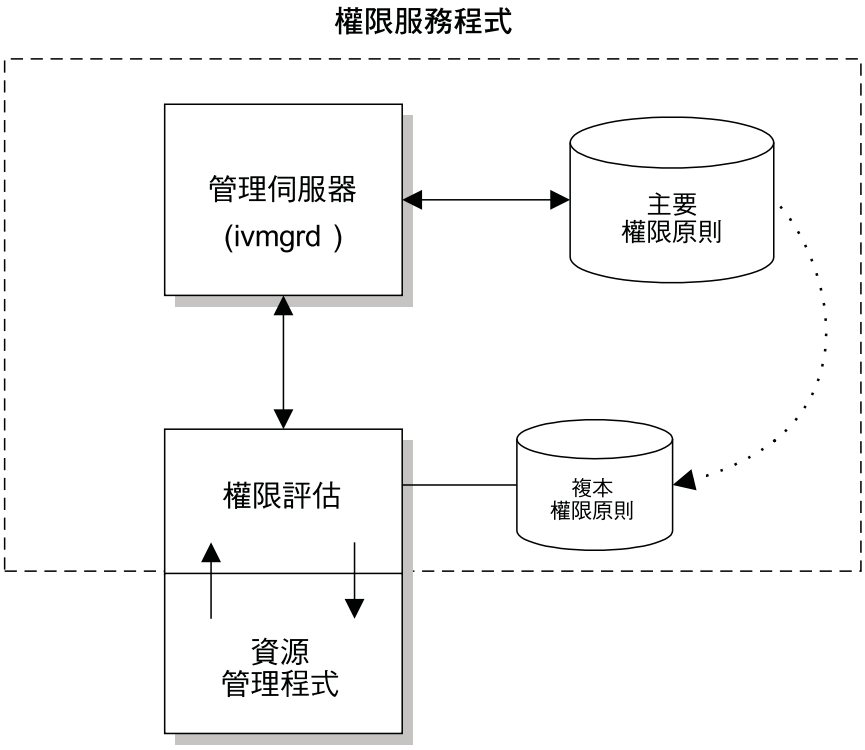
「管理」伺服器也會維護在安全領域中作業的其他 Policy Director 以及非 Policy Director 伺服器的位置資訊。

註: 任何安全領域中必須只有一個「管理」伺服器案例。

授權評估程式

授權評估程式是根據安全原則來決定從屬站存取受保護資源之能力的決策程序。評估程式會爲資源管理程式提供建議，而後者則依此回應。

下圖說明「Policy Director 權限服務程式」的主要元件：



Policy Director 權限服務程式介面

「Policy Director 權限服務程式」有兩種介面可供互動發生：

管理介面

安全管理者會管理網路的安全原則。安全管理者使用「Policy Director 管理主控台」，或 **ivadmin** 公用程式，來執行以下各項：

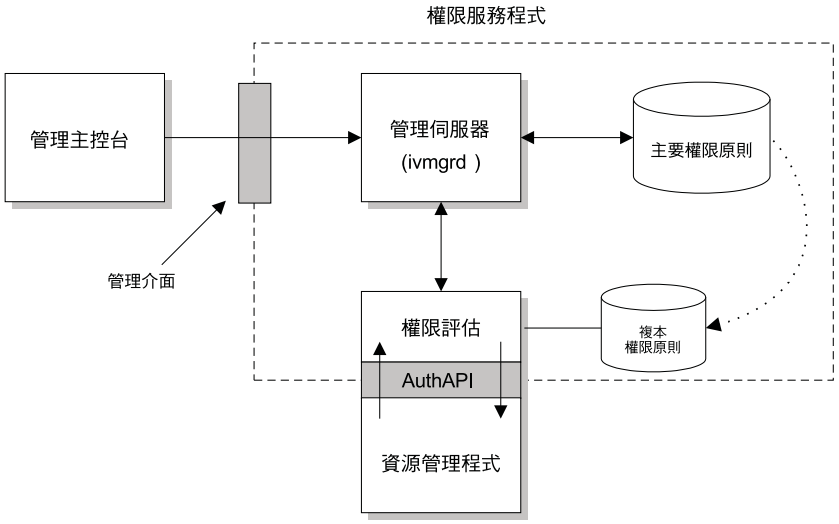
- 對網路資源引用原則規則（模版）。
- 登錄安全領域中的參與者之證明。

「管理主控台」會使用「管理」伺服器，將這個安全原則資料引用至主要授權原則資料庫。

這個介面涉及名稱空間、原則模板及證明的詳細知識。

權限 API

Policy Director 權限 API 會將授權決策的要求從資源管理程式傳送到授權評估程式，然後後者會傳回建議。*Policy Director 程式設計及參考手冊*包含此 API 的詳細資料。



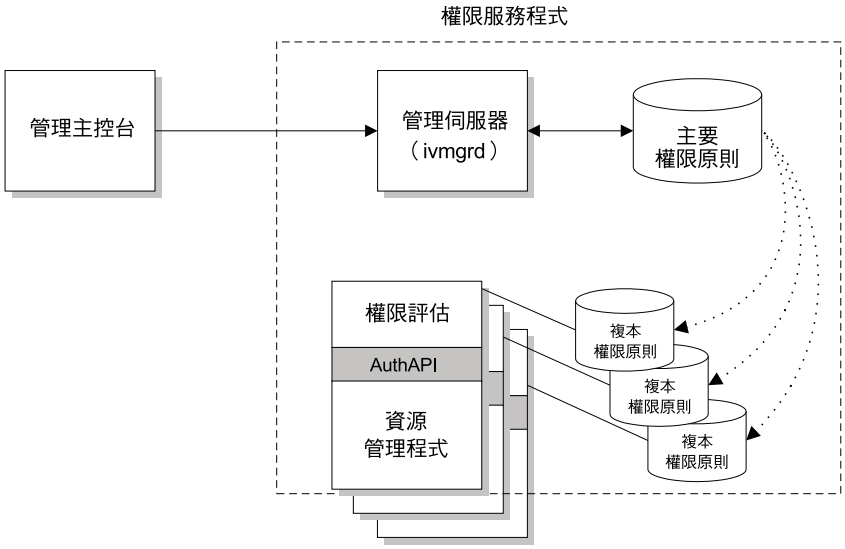
複製以達到可調整性及效能

您可以複製 Policy Director 權限服務程式元件，以增加大量需求的環境中的有用性。

Policy Director 一定會自動複製主要授權原則資料庫，其中包含原則規則及證明資訊。呼叫權限服務程式的應用程式有兩個選項參照至這份資料庫資訊：

- 應用程式在配置成與授權評估程式一起使用時，會使用資料庫的本端快取。在本端快取模式中使用權限服務程式的每一個應用程式都會發生資料庫的複製。
- 應用程式使用一個共用的複本，這個複本是由遠端 Policy Director「授權」伺服器元件來進行快取。 每一個 Policy Director「授權」伺服器實例都會發生資料庫的複製。有許多應用程式可以存取單一的權限伺服器。

來自「管理」伺服器的更新通知會觸發快取程序來更新所有的複本。每當主要的授權原則資料庫發生變更時，就會發出更新通知。



效能備註：

- 應用伺服器收到直接來自管理伺服器的更新通知。應用伺服器每隔幾分鐘會檢查主要授權原則資料庫的版本。 檢查可確保應用伺服器不會遺漏更新通知。

  如果更新通知無法抵達伺服器， Policy Director 會建立日誌登錄。在這兩種情況下，重試機制也可以確保更新將會發生。
- 快取的授權原則資訊會導致較高的系統效能。 例如，當 WebSEAL 執行授權檢查時，它會檢查本身資料庫快取版本中的原則模版。 WebSEAL 不必存取網路，即可從主要資料庫取得這項資訊。 所以是授權檢查的回應時間（效能）可變得很快。
- 用來呼叫的應用伺服器不會快取個別的授權結果。

網路安全原則

您控制領域中的使用者及群組的參與方式，會決定安全領域的安全原則。安全原則是將規則套用在需要保護的資源上。這些規則稱爲*原則模版*。

「Policy Director 權限服務程式」會強制執行這項原則，方法是將使用者的身份及證明與指定給要求資源的原則模版做對比。Policy Director 會將產生的建議傳送至資源管理程式，後者會完成對原始要求的回應。

網路安全原則的定義

「Policy Director 權限服務程式」使用一個集中式資料庫，可列出安全領域中的所有資源，以及指定給每一個資源的原則模版。這個主要授權原則資料庫以及安全性登錄是協助定義網路安全原則的主要元件。安全性登錄包含使用者帳戶及群組帳戶。

總結來說，網路安全原則負責控制以下各項：

- 可容許參與安全領域的使用者及群組。安全性登錄會包含並維護此資訊。
- 安全領域中所有物件的保護層次。主要授權原則資料庫會維護這項資訊。

受保護的物件名稱空間

*受保護的物件名稱空間*是隸屬安全領域之資源的階層式描述。出現在階層式名稱空間中的物件代表實際的網路資源。

- **系統資源** -- 實際的實體檔、網路服務程式或應用程式。
- **受保護的物件** -- 「Policy Director 權限服務程式」、「管理主控台」及其他 Policy Director 管理公用程式所使用的實際系統資源的邏輯呈現。

您可以將原則模版連接到名稱空間中的物件，以提供資源的保護。「Policy Director 權限服務程式」會根據這些模版來執行授權決策。

Policy Director 使用以下的名稱空間種類：

Web 物件

這些物件代表 HTTP URL 可定址的任何項目，如靜態 Web 網頁及動態 URL。您可以將靜態 Web 網頁及動態 URL 轉換成成資料庫查詢或其他類型的應用程式。

網路物件

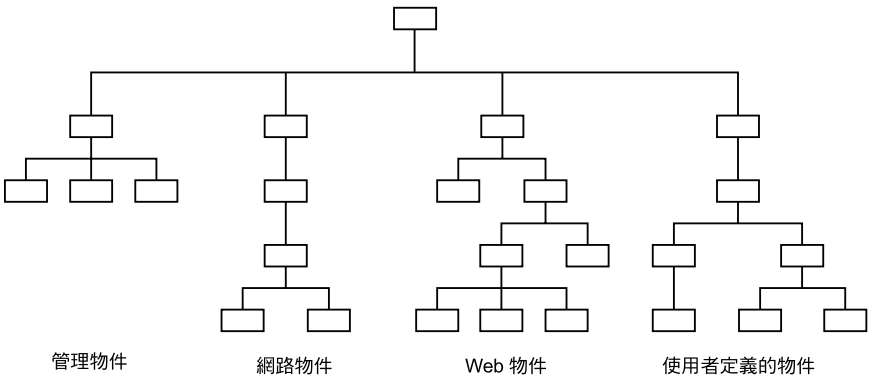
這些物件代表對映到應用程式將要使用的 TCP 網路位址（埠）的 TCP 應用程式（如 TELNET 及 FTP）。

管理物件

這些物件代表您可以利用「Policy Director 管理主控台」來執行的管理活動。物件代表定義使用者及設定安全原則所需的作業。 Policy Director 支援管理活動的指定，並且可以限制管理者將安全原則設定至名稱空間子集的能力。

使用者定義的物件

這些物件代表由使用「Policy Director 權限服務程式」（利用 Policy Director 權限 API）的應用程式所保護的作業或網路資源。



原則模版的定義及應用程式

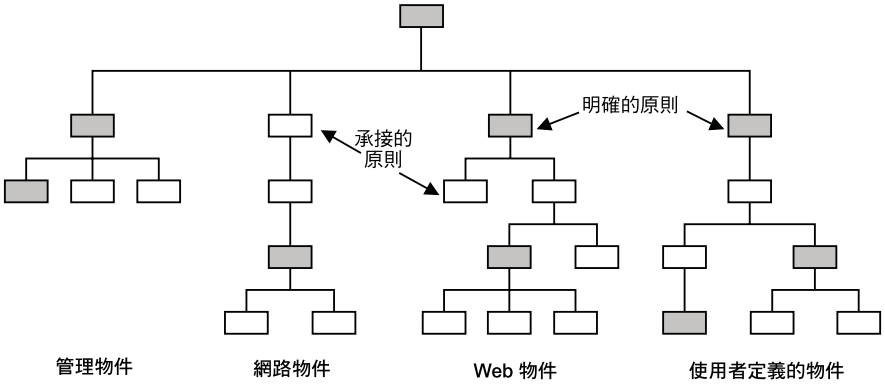
安全管理者會保護系統資源，方法是定義 (原則模版) 規則，然後將這些模版引用至名稱空間中資源的物件表示法。

「Policy Director 權限服務程式」會執行授權決策，這些決策是基於引用於這些物件的原則模版。當 Policy Director 允許對受保護的物件進行所要求的作業時，負責資源的應用程式會執行這項作業。

一個原則模版可以指定許多物件的保護參數。對規則的任何變更都會影響模版所連接的全部物件。

明確及承接的原則

您可以明確地引用或承接原則。 Policy Director 受保護的物件名稱空間支援對安全原則屬性的承接。對於負責管理名稱空間的安全管理者而言，這是一個很重要的考量。管理者只需要在階層中必須改變規則的地方引用明確的原則模版。



原則模版的類型範例包括：

- 寫死在程式中的規則
- 外部授權功能
- 特殊安全標籤
- 存取控制清單

存取控制清單

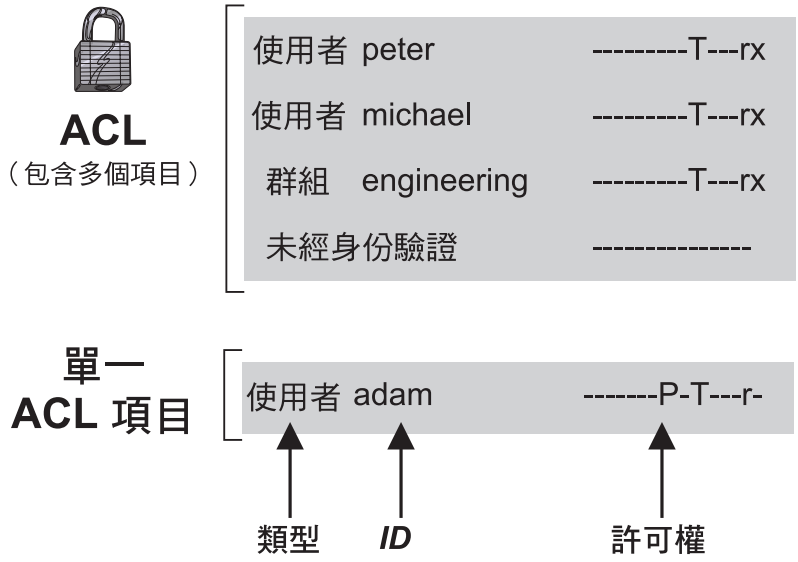
存取控制清單 (ACL) 是原則模板的範例。Policy Director 使用 ACL 作爲它的主要原則模版。

ACL 是指定對該資源執行特定作業時所需條件的控制集（許可權）。 ACL 定義是爲安全領域建立安全原則的重要元件。如同所有的原則模版一樣，您使用 ACL 將組織的安全原則戳印在受保護的物件名稱空間中所代表的資源上。

ACL 特別是用來控制以下各項：

- 對資源所執行的作業。
- 可執行這些作業的人員。

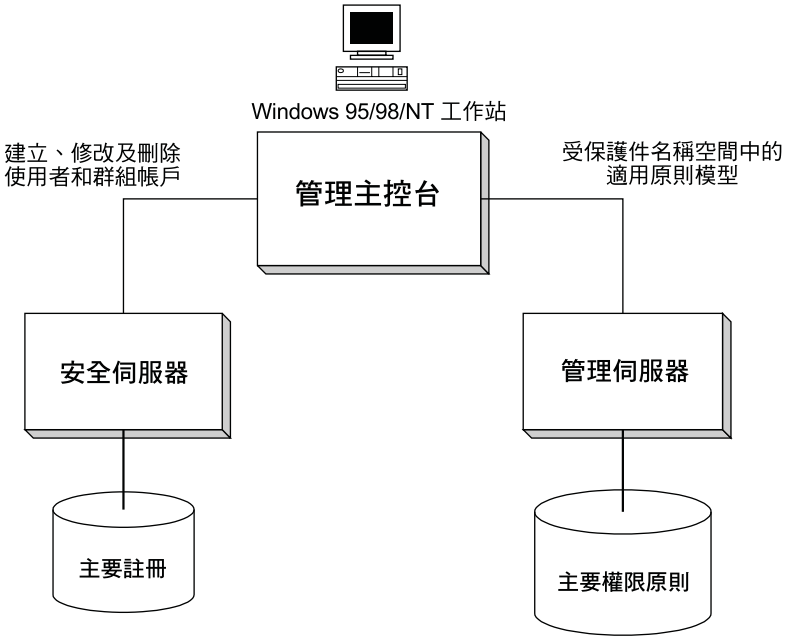
ACL 是由一或多個項目（包括使用者指定及群組指定），加上它們的特定許可權或權限所組成。



原則管理

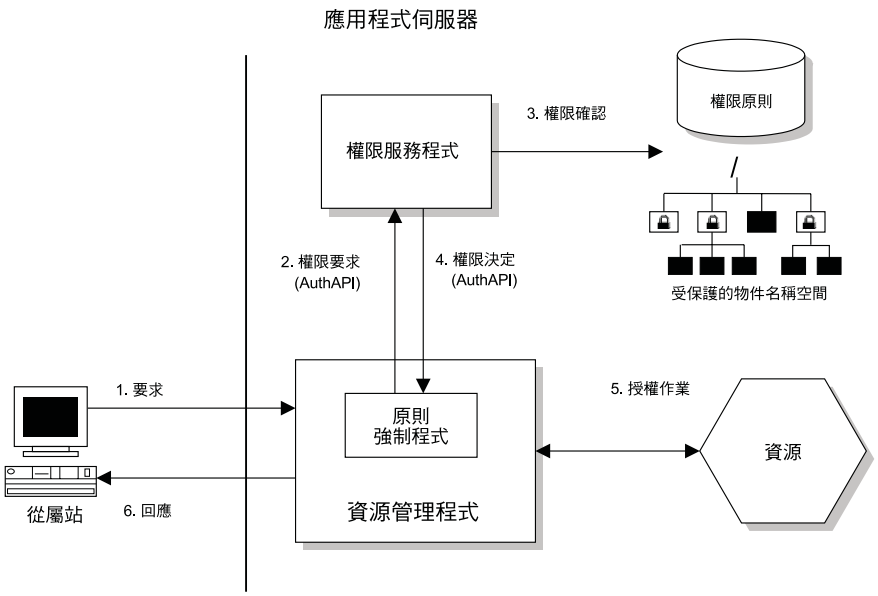
「Policy Director 管理主控台」是一種 Java 型的圖形式應用程式，它是用來管理 Policy Director 安全領域中的安全原則。選用性的 **ivadmin** 指令行公用程式提供和「管理主控台」相同的管理功能。

您可以從「管理主控台」或利用 **ivadmin** 公用程式，來管理「安全」伺服器登錄、主要授權原則資料庫，以及所有的 Policy Director 伺服器。 您也可以新增或刪除使用者及群組，並且將原則模版或 ACL 引用至網路物件。



逐步的授權程序

以下圖解說明完整的授權程序：



1. Policy Director 將對資源的已驗證從屬站要求導入資源管理程式伺服器。原則強制執行程序會截取要求。

   資源管理程式可以是 WebSEAL（用於 HTTP 及 HTTPS 存取）、 NetSEAL（用於 TCP/IP 網路存取）或協力廠商應用程式。
2. 原則強制執行程序使用 Policy Director 權限 API（請參閱『Policy Director 權限 API』）來呼叫「Policy Director 權限服務程式」以進行授權決策。
3. 權限服務程式對資源（在 Policy Director 受保護的物件名稱空間中是以物件爲代表）執行授權檢查。將引用至物件的原則模板比對從屬站的證明。
4. 傳回對資源管理程式的建議（使用原則強制執行程式），以決定要接收或拒絕要求。
5. 如果授權檢查核准要求，資源管理程式會將要求傳送至負責資源的應用程式。
6. 從屬站接收所要求的作業結果。

Policy Director 權限 API

「Policy Director 授權*應用程式介面*」（API）可容許 Policy Director 應用程式及協力廠商應用程式查詢 「Policy Director 權限服務程式」以執行授權決策。

Policy Director 權限 API 是介於資源管理程式（要求授權檢查）以及權限服務程式本身之間的介面。Policy Director 權限 API 可容許強制執行原則的應用程式要求授權決策。然而，Policy Director 權限 API 可以防止應用程式免於實際決策程序的複雜性。

Policy Director 權限 API 提供一個標準的程式設計模式以進行編碼授權要求及決策。Policy Director 權限 API 可讓您從任何大型主機或新開發的應用程式，對集中管理的權限服務程式進行標準化的呼叫。

您可以在以下其中一種模式中使用 Policy Director 權限 API：

遠端快取模式

在這個模式中，Policy Director 會起始設定 API 以呼叫遠端「Policy Director 權限伺服器」（ivacld）來代替應用程式執行授權決策。 Policy Director「授權」伺服器會維護它本身的授權原則資料庫複本快取。使用這個模式來處理應用程式從屬站的授權要求。

請參閱第44頁的『遠端快取模式』。

本端快取模式

在這個模式中，Policy Director 會起始設定 API，以下載及維護應用程式權限資料庫的本端複本。本端快取模式可容許應用程式在本端執行所有的授權決策，因而達到更佳的效能及可靠性。

然而，資料庫複製的額外需要以及使用這個模式的安全性施行方式，使它適用於授信的應用伺服器。可靠的應用伺服器包括 WebSEAL 及 NetSEAL。

請參閱第45頁的『本端快取模式』。

Policy Director 權限 API 的主要意義及好處是它有能力防止使用者面對權限服務程式機制本身的複雜性。 Policy Director 會將管理、儲存體、快取、複製、證明格式，以及身份驗證方法等課題隱藏到 Policy Director 權限 API 之後。

Policy Director 權限 API 也可以獨立於基礎安全性基本設施、證明格式及評估機制之外運作。 Policy Director 權限 API 讓您可以要求授權檢查，並取得簡單的"是"或"否"等建議。 使用者看不到授權檢查機制的明細。

「Policy Director 權限 API」可支援下列平台：

- Microsoft Windows NT、Windows 98 及 Windows 95
- IBM AIX 版本 4.3
- Sun Solaris 版本 2.6

權限 API 範例

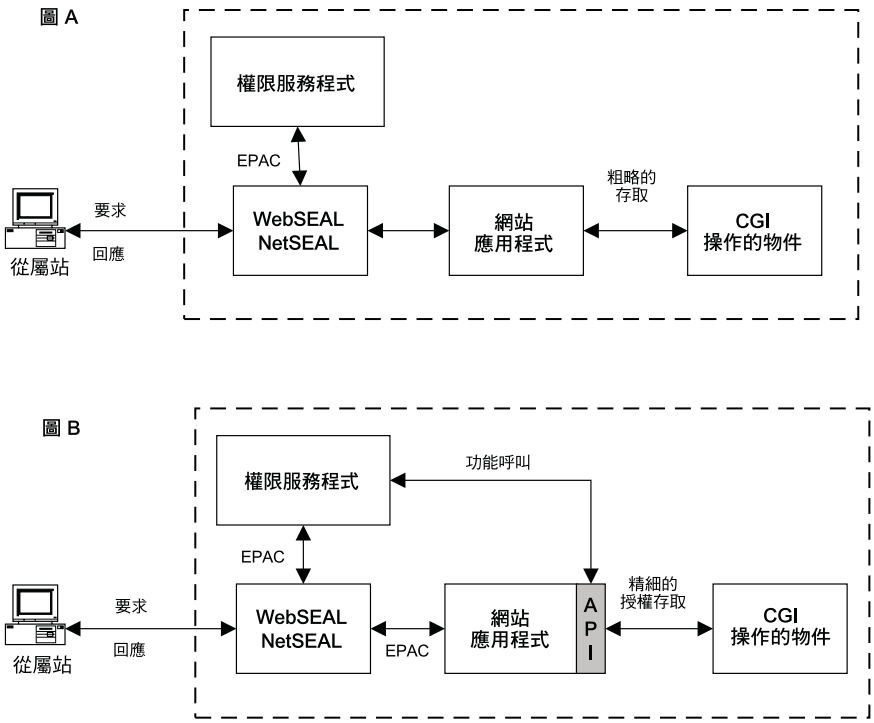
WebSEAL 及 NetSEAL 權限服務程式可分別對 URL 及埠執行存取控制。協力廠商的應用程式可使用 Policy Director 權限 API 來執行非常特別及特殊程序的存取控制。

範例 1：您可以指定一個圖形式使用者介面（GUI），根據授權檢查的結果，以動態方式將作業按鈕顯示成作用中或非作用中。

範例 2：下圖說明另一個 Policy Director 權限 API 的使用。本圖說明 Web 應用程式對 CGI 異動的要求。

圖 A 中所說明的最低層次授權涉及對 URL "非有即無"（all-or-nothing）的存取控制。這個粗略的授權層次只會決定從屬站是否能執行 CGI 程式。藉由容許存取 CGI 應用程式，對於 CGI 應用程式所操作的資源將無進一步的控制權。

在圖 B 中，存取控制是 CGI 程式所操作的一組資源。 Web 應用程式是配置成使用 Policy Director 權限 API。現在，CGI 程式可以呼叫「Policy Director 權限服務程式」來對它所操作的資源進行授權決策。 授權決策可以根據要求從屬站的身份爲基礎。

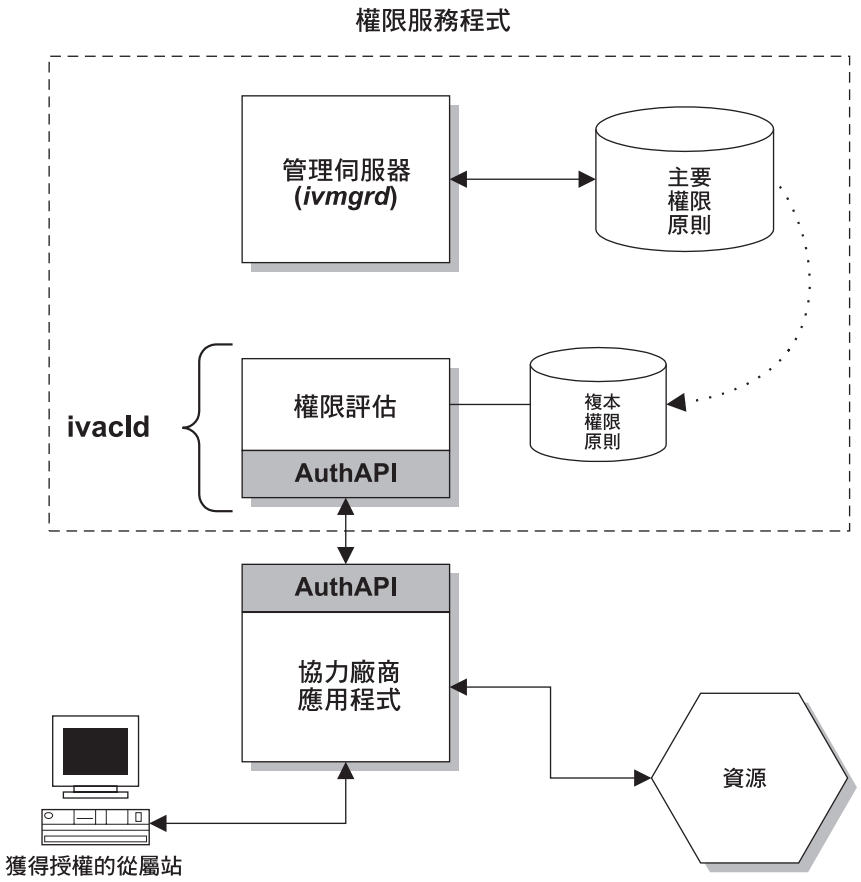


遠端快取模式

在*遠端快取授權模*式中，應用程式使用 Policy Director 權限 API 所提供的函數呼叫來和遠端 Policy Director「授權」伺服器（ivacld）進行通信。 Policy Director「授權」伺服器的作用是授權決策評估程式，它會維護自己的授權原則資料庫複本。

Policy Director「授權」伺服器會進行決定，並使用 API 將建議傳回應用程式。伺服器也可以撰寫一份審核記錄，其中包含授權決定要求的明細。

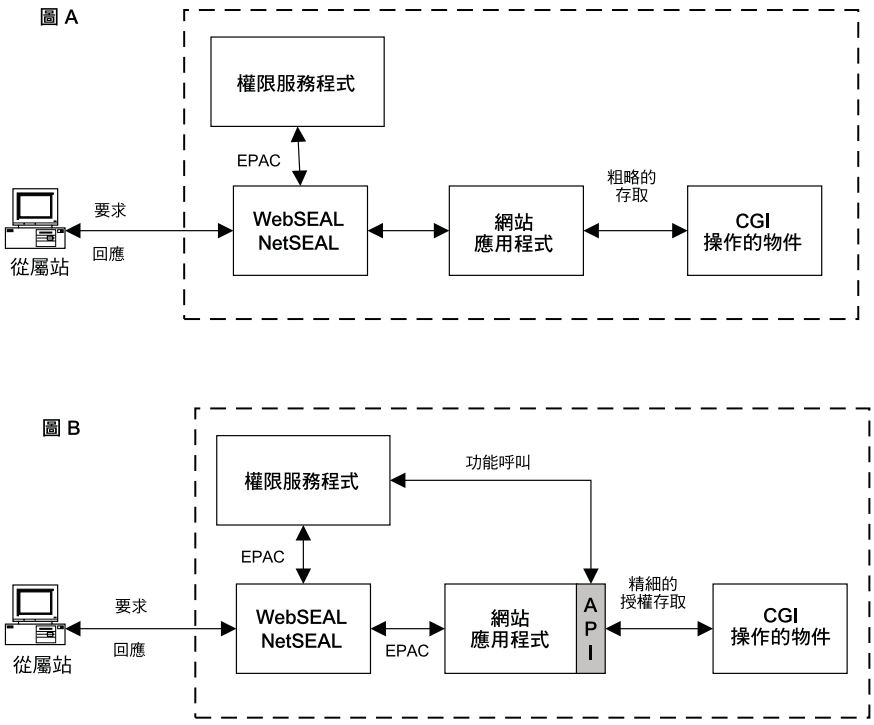
安全領域中必須有一個 Policy Director「授權」伺服器正在執行中。 Policy Director「授權」伺服器可以常駐在和應用程式相同的機器，或是在另一部機器上。您也可以將 Policy Director「授權」伺服器安裝在安全領域中一部以上的機器上，以容許更高的有用性。當特定的 Policy Director「授權」伺服器失效時，Policy Director 權限 API 會明顯失效。



本端快取模式

在*本端快取模式*中， API 會下載並且在應用程式本端的檔案系統中維護授權原則資料庫的複本。它會在記憶體中執行所有的授權決策，而產生較高的效能及較佳的可靠性。

本端複本在應用程式的不同呼叫之間都是持續的。 API 會以複本模式啓動。啓動時，它會檢查主要「授權原則」資料庫是否有任何更新。這些更新是自從建置本端複本以來可能發生的更新。



外部授權功能

在某些情況下，標準的 Policy Director 許可權集可能無法表示組織的安全原則所需的全部授權角色。 Policy Director 提供選用的外部授權功能，以容納任何其他的授權需求。

外部權限服務程式可讓您強制執行由個別的外部權限伺服器程式所指定的其它授權控制及條件。

權限服務程式的延伸

「Policy Director 權限服務程式」會自動建置一個外部授權功能。 如果您配置一個外部權限服務程式， 「Policy Director 權限服務程式」只會將新的控制及條件納入其評估程序。

使用「Policy Director 權限服務程式」的應用程式包括 WebSEAL、 NetSEAL，以及任何使用「Policy Director 權限 API」 的應用程式。 這些應用程式可以獲得已配置外部權限服務程式的其他好處。透過使用外部權限服務程式來新增的安全原則，對於這些應用程式而言都是透通的，因此不需要變更應用程式。

外部權限服務程式配置可完全整合組織現有的安全服務程式。外部權限服務程式會保留公司在安全機制上的起始投資。這個外部權限服務程式可讓大型主機伺服器納入 Policy Director 授權決策程序。

設定外部權限服務程式需要這些一般步驟：

1. 撰寫一個伺服器程式，以便在授權決策期間參照。
2. 將外部權限服務程式登錄到 Policy Director。

在登錄服務程式之後，代表此服務程式的新許可權會出現在「Policy Director 管理主控台」中。您現在可以在任何 ACL 項目中使用這個許可權。

在授權檢查期間發現許可權時，會參照外部權限服務程式以進行其他的授權決策。

*Policy Director 程式設計及參考手冊*中有說明安裝外部權限服務程式的詳細明細。

資源要求的條件

您也可以使用外部權限服務程式，對順利完成或未順利完成的存取強制施行特定的條件。

範例包括許多條件，例如：

- 導致外部審核機制記錄順利完成或未順利完成的存取嘗試。
- 主動監督存取嘗試以及爲無法接受的行爲偵測產生警示或警告聲。
- 記帳及 micro-payment 交易。

授權評估程序

納入外部權限服務程式的授權決策會以下列方式發生：

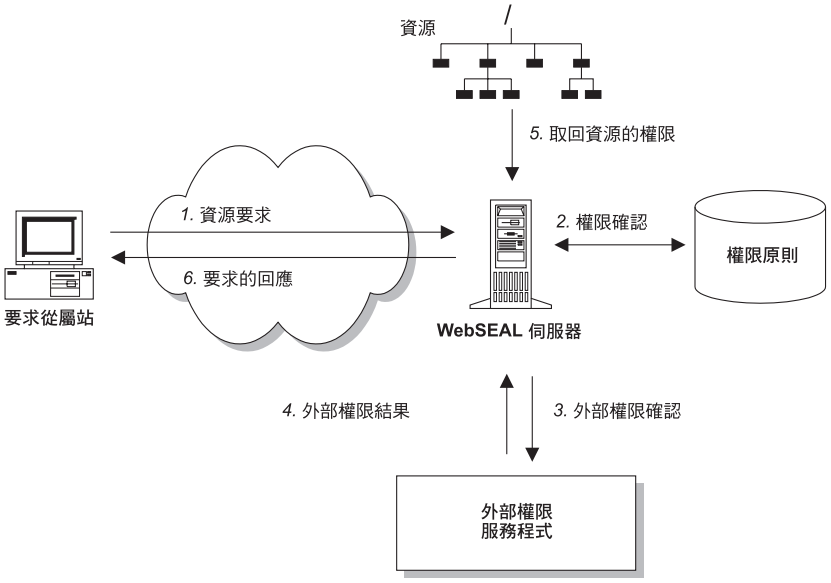
1. 執行 ACL 檢查以決定授與要求的使用者的許可權集。
2. 傳送使用已驗證 RPC 的授權要求給許可權出現在 ACL 中的每一個外部權限服務程式。

   不論是否將必要的許可權授與使用者，這個外部授權檢查都會發生。
3. 總結所有的授權決策結果。

   拒絕可能來自 Policy Director ACL 檢查或任何外部授權檢查。如果有任何拒絕發生，「Policy Director 權限服務程式」將會拒絕授權要求。

範例：

下圖說明涉及 WebSEAL 伺服器及外部權限服務程式的授權決策。



在本例中，外部權限服務程式的目的是強制存取物件的時間限制。在「管理主控台」中，指定爲代表許可權的字元是 k。

1. Policy Director WebSEAL 伺服器接收來自從屬站的要求，以存取敏感的工程文件。從屬站是「工程」群組的成員之一。
2. WebSEAL 伺服器會先檢查複本授權原則資料庫，以決定指定給該文件物件的許可權。

   ```
   group engineering rk
   ```

   如果 ACL 項目不含外部權限服務程式許可權，最終的授權決策將會完全根據這項資訊。

   在上述的範例中，ACL 項目包含標準的讀取許可權。項目也包含一個附加的 (k) 許可權，它會參照外部權限伺服器以提供授權評估。
3. Policy Director 使用已對外部權限伺服器驗證的 RPC 來傳送要求。授與的許可權集是在步驟 2 中決定。 Policy Director 會將這個許可權集與這個要求一起傳送，使外部權限伺服器可以根據這項資訊來進行決策。

   在本例中，外部權限伺服器的設計可讓您對存取這份文件的能力設定時間界線。當要求是在星期一到星期五的 8AM 和 6PM 之間發生時，對文件的存取才會發生。
4. 本例中的從屬站已經在星期二早上十點鐘提出要求。伺服器將順利完成的回應傳回 WebSEAL 伺服器。

   所有上述授權決策的總和會導致最終的建議，以容許對文件物件的存取。
5. WebSEAL 伺服器擷取文件資源。
6. WebSEAL 伺服器容許從屬站檢視文件。

請參閱*Policy Director 程式設計及參考手冊*以取得外部權限服務程式生效的進階明細。

施行策略

Policy Director 可讓您以數種方式完成外部權限服務程式：

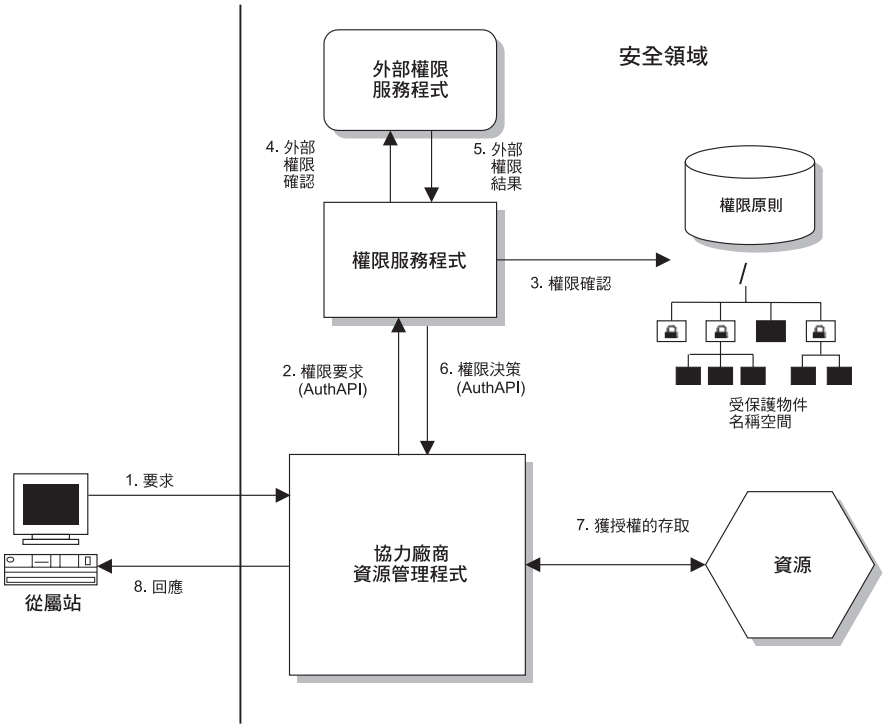
- 您可以新增任何數目的外部權限服務程式給您的安全領域，以完成許多不同的授權評估。 ACL 中每一個不同的許可權都代表一個服務程式。
- 您可以將多個外部權限伺服器連鎖在一起，爲給定的許可權呼叫一個以上的外部伺服器。每一個伺服器都會將已驗證的身份傳送給連鎖中的下一個伺服器，並且從下游伺服器收集結果。
- 您可以複製整個安全領域中的外部權限服務程式。

這些施行方式的每一個都是彼此獨立的，並且可以任意合併使用。

延伸性及彈性

Policy Director 權限 API 及外部權限服務程式的組合，可提供高度延伸及彈性的解決方案，以執行安全原則。

下圖說明可能爲協力廠商應用程式及外部權限服務程式使用 Policy Director 權限 API 之組合特性的可延伸配置：


安全領域
外部權限
服務程式
4. 外部
權限
確認
5. 外部
權限
結果
權限原則
權限服務程式
3. 權限確認
2. 權限要求
(AuthAPI)
6. 權限決策
(AuthAPI)
受保護物件
名稱空間
1. 要求
協力廠商
資源管理程式
7. 獲授權的存取
資源
8. 回應
從屬站

第4章 管理主控台簡介

「Policy Director 管理主控台」是以 Java 型的圖形式應用程式，它是在分散式網路中使用，以便管理所有的 Policy Director 元件的安全。您可以從「管理主控台」來管理「安全」伺服器登錄、主要授權原則資料庫，以及所有的 Policy Director 伺服器。「管理主控台」也能讓您新增及刪除使用者或群組，以及引用 ACL。

本章包括：

管理主控台概觀

「Policy Director 管理主控台」是一種 Java 型的圖形式應用程式，它是用來管理 Policy Director 安全領域中的安全原則。選用的 **ivadmin** 指令行公用程式提供和「管理主控台」相同的管理功能。

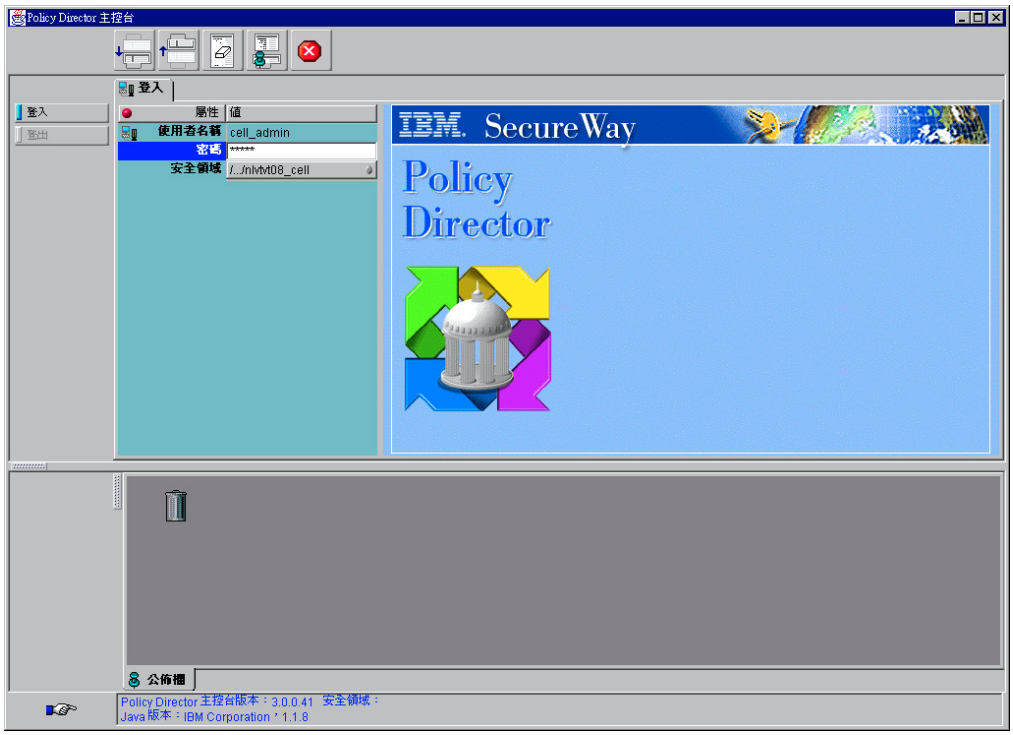
您可以從「管理主控台」或利用 **ivadmin** 公用程式，來執行以下功能：

- 變更登錄資料庫（帳戶）。
- 變更主要授權原則（ACL）資料庫。
- 新增及刪除使用者。
- 新增及刪除群組。
- 新增原則模版或 ACL 至物件。
- 新增、刪除或變更「廣域登入」（GSO）資源、資源群組及資源憑證。
- 新增、刪除或變更 Proxy 使用者 (可選用的)

管理主控台特性

「管理主控台」提供了許多工具來執行作業，並且會在「管理主控台」視窗的區分範圍中顯示資訊。主要工具及顯示範圍包括：

- 作業標籤
- 管理作業畫面（頂端及底端畫面）
- 動作按鈕
- 工具列
- 公佈欄（預設底端畫面）
- 狀態列
- 標題列



管理作業畫面工具

這些工具是爲管理作業畫面提供的：

- 作業標籤
- 管理作業標籤畫面（頂端及底端畫面）
- 動作按鈕

作業標籤

「管理主控台」提供這些主要*作業標籤*來執行管理作業：

- 登入
- 使用者

- 群組
- GSO 資源
- GSO 資源群組
- ACL
- 物件空間
- Proxy 使用者（選用）

管理作業畫面

每一個作業標籤會產生一個管理作業畫面，其中包括「管理主控台」頂端畫面中所呈現的資訊檢視畫面的集成。

管理作業包括：

登入	「登入」是用來登入及登出「管理主控台」的進入點。
使用者	讓您建立及維護安全領域中的使用者。
群組	讓您建立及維護安全領域中的群組。
GSO 資源	讓您建立及維護 GSO 資源資訊。
GSO 資源群組	讓您建立及維護 GSO 資源群組資訊。
ACL	讓您建立及維護原則模版或 ACL。
物件空間	讓您將原則模版連接到名稱空間中的物件，或是從後者移除原則模版。
Proxy 使用者	讓您建立及維護 Proxy 使用者資訊。

動作按鈕

每一個作業標籤都有一組特定的動作按鈕。使用這些動作按鈕來執行管理作業。這些按鈕會出現在畫面左邊。動作按鈕可以變更及更新適當的資料庫。

畫面檢視類型

您可以用下列三種檢視畫面的其中一種來顯示管理作業畫面中的資訊。每一個檢視類型都有特定的性質：

明細檢視畫面

明細檢視畫面包含資料項目的動態欄位。

清單檢視畫面

您可以按一下適當直欄的標題列，以升冪或降冪次序來排序清單檢視。某些清單具有查詢功能。

樹狀檢視畫面

您可以展開及收縮樹狀檢視畫面。

當項目被選取，並且在任何檢視畫面中作用時，強調顯示會呈現藍色。

當項目被選取，但是目前不在作用中時，則使用灰色。

工具列

工具列出現在「管理主控台」視窗頂端，其中的按鈕可用來啓動特定的「管理主控台」功能。

將作業移至底端按鈕會將目前在頂端畫面中的管理作業重新定位到底端畫面。

將作業移至頂端按鈕會將目前在底端畫面中的管理作業重新定位至至頂端畫面。

圖釘檢視畫面按鈕會取用頂端畫面目前作用中的資訊，然後將這項資訊的副本放置到底端畫面中。 頂端畫面目前作用中的資訊包括如群組或使用者清單等資訊。 畫面的新標籤也會出現。 這個畫面中的資訊只是靜態副本，而非動態。 然而，您仍然可以展開及收縮樹狀檢視畫面，如物件空間樹狀組織及群組清單。

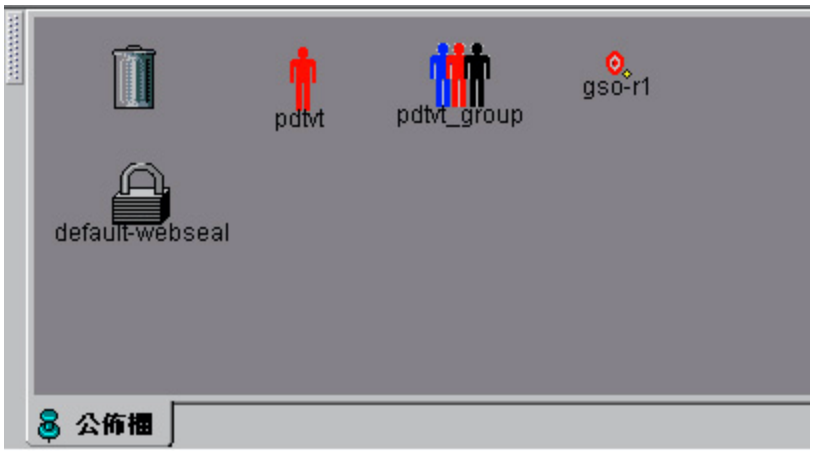
消除按鈕會從「管理主控台」清除目前選取的檢視畫面。 這個動作只會清除檢視畫面；實際的資料庫資訊不受影響。

停止按鈕會停止目前進行中的動作，並且將「管理主控台」的控制傳回給管理者。 實際上，它會忽略現行動作的結果，而「管理主控台」會假設作業失敗。

公佈欄

「公佈欄」是「管理主控台」的預設下方畫面。您使用「公佈欄」作爲您在管理階段作業期間要多次使用的任何物件之暫時儲存體位置。物件可包括檔案、ACL、使用者和群組清單，以及屬性。您可以將物件圖示拖放到「公佈欄」，並且視需要在管理作業中使用它們。

「公佈欄」上的標準圖示包括**垃圾桶**圖示及**圖釘檢視畫面**圖示。



垃圾桶圖示

您可以移除儲存在「公佈欄」的圖示，方法是將它們拖曳到**垃圾桶**圖示。

圖釘檢視畫面

您可以從任何其他管理作業畫面中，選取（強調顯示）特定的物件及資訊，然後將它們拖放到「公佈欄」的**圖釘檢視畫面**圖示。

這個動作會產生一個新的畫面出現在下方，並且顯示選取資訊的副本。新標籤也會出現。

這個畫面中的資訊只是靜態副本，而非動態。然而，您仍然可以展開及收縮樹狀檢視畫面，如「物件空間」樹狀組織及「群組」清單。

如果作用中的資訊是群組清單，只有選取（強調顯示）的群組會在「圖釘檢視畫面」畫面中。

如果要關閉「圖釘檢視畫面」畫面，請按一下視窗右上角的關閉框。

註: 當您選取資訊並按一下「工具列」中的**圖釘檢視畫面**按鈕時，會出現相同動作。

狀態列

「管理主控台」底端的「狀態列」會顯示狀態及錯誤訊息。

- 一般狀態資訊會以**黑色**顯示。
- 警告會以**藍色**顯示。
- 錯誤會以**紅色**顯示。

狀態指示圖示會顯示在訊息區左邊：

順利完成狀態圖示

警告狀態圖示

錯誤狀態圖示

如果您按兩下狀態指示圖示，狀態列會顯示：

- 「管理主控台」版本
- 受到「管理主控台」活動影響的安全領域
- Java 版本

標題列

「管理主控台」的標題列會顯示兩個重要資訊：

- 目前受到「管理主控台」活動影響的安全領域。
- 使用者的登入狀態（UPDATE 或 READ-ONLY）。

如無法使用主要「安全」伺服器登錄，您將無法透過「管理主控台」來修改帳戶資料。如果這種少見的情況發生，「管理主控台」會從登錄複本取得現行帳戶資訊。當您嘗試變更會影響登錄的資訊時，會出現錯誤訊息。

登入管理作業

「登入」作業畫面是已驗證使用者的「管理主控台」進入點。如果此事件順利完成，將會出現完整的管理作業標籤集。

當使用者登出時，所有的上下文都會遺失，而作業標籤會被移除。

作業標籤

作業標籤：**登入**

管理作業

「登入」管理作業畫面包含**使用者名稱**及**密碼**項目的欄位。**安全領域**欄位最初會顯示爲 NetSEAT 所配置的預設安全領域。

「登入」下拉功能表可讓您選取不同的安全領域，以執行「管理主控台」作業。

動作按鈕

登入的動作按鈕有：

- 登入
- 登出

使用者管理作業

「使用者」管理作業畫面可讓您建立及維護安全領域中的使用者。當您從清單檢視畫面或樹狀檢視畫面選取使用者時，明細檢視畫面中的欄位會輸入現行資料。

作業標籤

作業標籤：**使用者**

管理作業

「使用者」管理作業畫面包含「使用者」清單檢視畫面、「使用者明細」檢視畫面，以及「群組」清單檢視畫面。

「群組」檢視畫面含有 GSO 資源與 GSO 資源群組的其它標籤。

動作按鈕

使用者的動作按鈕有：

- 新增
- 取得
- 儲存
- 刪除

群組管理作業

「群組」管理作業畫面可讓您建立及維護安全領域中的群組。當您從清單檢視畫面或樹狀檢視畫面選取群組時，明細檢視畫面中的欄位會輸入現行資料。

作業標籤

作業標籤：**群組**

管理作業

「群組」管理作業畫面包含「群組」清單檢視畫面、「群組明細」檢視畫面，以及「使用者 ID」清單檢視畫面。

動作按鈕

群組的動作按鈕有：

- 新增
- 取得
- 儲存
- 刪除

GSO 資源管理作業

GSO 資源管理作業畫面可讓您建立及維護安全領域中的 GSO 資源。GSO 資源恆爲 Web 資源。當您從清單或樹狀檢視畫面選取 GSO 資源時，明細檢視畫面中的欄位會大量輸入資料現行資料。

作業標籤

作業標籤：**GSO 資源**

管理作業

「GSO 資源」管理作業畫面含有「資源」清單檢視畫面及「資源明細」檢視畫面。

動作按鈕

GSO 資源的動作按鈕有：

- 新增
- 取得
- 儲存
- 刪除

GSO 資源群組管理作業

「GSO 資源群組」管理作業畫面可讓您建立及維護安全領域中的 GSO 資源群組。*資源群組*參照 Web 伺服器的群組，其中群組中的全部伺服器會有同一組使用者 ID (userids) 及密碼。當您從清單或樹狀檢視畫面選取 GSO 資源群組時，明細檢視畫面中的欄位會大量輸入資料現行資料。

您可以建立資源群組中全部資源的單一資源證明。Policy Director 使用資源群組的單一資源證明，而不是資源群組中每個資源的資源證明。

作業標籤

作業標籤：**GSO 資源群組**

管理作業

「GSO 資源」群組管理作業畫面包含「資源群組」清單檢視畫面、「資源群組明細」檢視畫面，以及「GSO 資源」清單檢視畫面。

動作按鈕

GSO 資源群組的動作按鈕有：

- 新增
- 取得
- 儲存
- 刪除

ACL 管理作業

ACL 管理作業畫面可讓您建立及維護 ACL 原則模板。當您選取 **ACL 清單**檢視畫面中的 ACL 時， 「ACL 定義」檢視畫面中的欄位中會移入現行資料。

作業標籤

作業標籤：**ACL**

管理作業

ACL 管理作業畫面中會有一個「ACL 清單」檢視畫面、一個「ACL 定義」明細檢視畫面，以及一個內含許可權樹狀檢視畫面的「ACL 項目」明細檢視畫面。

動作按鈕

ACL 的動作按鈕有：

- 新 ACL
- 新項目
- 儲存
- 刪除
- 取得
- 清單
- 使用處

物件空間管理作業

「物件空間」管理作業畫面可讓您將 ACL 連接到名稱空間中的物件，或是從後者移除 ACL。

當您選取「物件空間」樹狀檢視畫面中的物件時，承接的 ACL 順序會出現在「承接的 ACL」樹狀檢視畫面。 這份清單代表具有明確設定的 ACL，並且會因爲承接而影響選取物件許可權的所有物件。

作業標籤

作業標籤：**物件空間**

管理作業

「物件空間」管理作業畫面提供從畫面子標籤選取的三個明確資訊檢視畫面：

- **承接的 ACL** 檢視畫面（預設值）

  這個檢視畫面是預設的檢視畫面。 它顯示影響選取物件的 ACL 連鎖。有一個箭頭恆會指向立即影響「物件空間」樹狀檢視畫面中選取物件的 ACL。
- **編輯 ACL** 檢視畫面

  這個檢視畫面提供了可讓您直接變更 ACL 屬性的 ACL 管理畫面部分。
- **承接**樹狀檢視畫面

  這個檢視畫面會顯示直接影響選取物件的 ACL 承接連鎖的樹狀檢視畫面。

動作按鈕

物件空間的動作按鈕有：

- 連接 ACL
- 移除 ACL
- 尋找 ACL

- 儲存 ACL
- 清單

Proxy 使用者管理作業

Policy Director 如果結合企業的防火牆系統，便能完全保護企業內網路，使其免於未經授權的存取和入侵。 「Proxy 使用者」管理作業畫面可讓您建立及維護安全領域中的 Proxy 使用者。當您從樹狀檢視畫面選取 Proxy 使用者時，明細檢視畫面中的欄位會輸入現行資料。

作業標籤

作業標籤：**Proxy 使用者**

管理作業

「Proxy 使用者」管理作業畫面包含「Proxy 使用者」清單檢視畫面及「Proxy 使用者明細」檢視畫面。

「Proxy 使用者明細」管理作業畫面包含顯示預設Proxy 使用者資訊的欄位。

動作按鈕

Proxy 使用者的動作按鈕有：

- 儲存
- 刪除

管理主控台的性質及控制項

「管理主控台」需要 Microsoft Window NT 或 Microsoft 95 或 98 平台上的 Policy Director NetSEAT 從屬站，才能透過安全通信通道來執行管理作業。如果是 AIX 和 Solaris，「管理主控台」使用系統的 DCE 從屬站來執行管理作業。

拖放

您可以使用滑鼠來執行許多「管理主控台」作業，從一個位置拖曳物件，然後放置到另一個位置。例如，您可以新增使用者至群組，方法是從「使用者清單」的「使用者」圖示，然後，您只要將它放置到「群組」樹狀檢視畫面中的群組即可。

當游標位於您可拖曳的圖示上時，游標的形狀會改變爲手型。

您可以拖放以下物件：

- 使用者
- 群組
- ACL
- ACL 項目
- 名稱空間中的物件
- GSO 資源及GSO 資源群組
- Proxy 使用者

註: 可導致資料庫更新的所有拖放會產生確認警示對話框。

您可以用拖放方式來執行資料查詢。例如，當您將「公佈欄」中的 **ACL** 圖示拖曳到「ACL 定義」檢視畫面中時，欄位中會移入現行資料。

如果您將物件（圖示）放置到不接受這項作業的位置，物件（圖示）會以動畫方式回到它的原始位置。

註: 拖放作業只能在「管理主控台」的上下文中使用。

執行頂端及底端畫面活動

「管理主控台」更新作業會在頂端及底端畫面中發生。您可以從底端畫面拖曳物件，然後將它們放置在頂端畫面。將任何畫面中的修改儲存到資料庫中。

Policy Director 一定會將「物件空間」畫面以及 ACL 畫面中顯示的 ACL 資訊同步化。

選取清單中的多個項目

您可以使用這些標準的 Windows 選擇技巧來選取清單及表格中的項目：

- 在項目上按一下以選取項目。
- 按住 Ctrl 鍵以同時選取其他的項目。
- 按一下，然後按 Shift + 按一下以選取兩次按鍵之間所形成的文字區塊。
- 清單中的所有項目可利用 **Ctrl + a** 來選取。

編輯資料登錄欄位

編輯資料登錄欄位時，請記得：

- 您可以使用 Enter 鍵來輪換開啓和關閉文字編輯欄位。
- 編輯時，您可以使用 Esc 鍵來復置欄位先前的資料登錄。
- 在 Windows 從屬站機器上，您可以使用標準的 Windows 按鍵來執行「管理主控台」特定的複製、剪下及貼上。
- 結束資料已變更的欄位之後，檢視畫面左上角會出現紅色指示器。按一下**儲存**按鈕來確定對資料庫的所有變更。
- 您可以使用拖放來將資料輸入到某些資料欄位中。

從清單查詢

許多清單檢視畫面都有查詢功能。查詢圖示會出現在清單檢視畫面視窗的左上角。

導覽

如果要在欄位之間進行導覽：

- 在明細檢視畫面中，Tab 鍵可以將游標從一個資料登錄欄位移至下一個。
- 當游標位於明細檢視畫面的最後一個欄位時。Tab 鍵會將游標移至下一個檢視畫面。游標會從左移至右邊。
- 當游標位於清單或樹狀檢視畫面時，Tab 鍵會將游標移至下一個檢視畫面。游標會從左移至右邊。

- Shift + Tab 會將游標從右往左移至下一個檢視畫面。
- Home 鍵會將游標移至檢視畫面頂端。 End 鍵會將游標移至檢視畫面底端。

在明細檢視畫面中，當所有欄位都不在作用中時， Home + End 鍵會將游標移至檢視畫面頂端及底端。如果有任何欄位正在作用中， Home + End 會將游標移至作用中欄位的開頭和結尾。

使用物件圖示

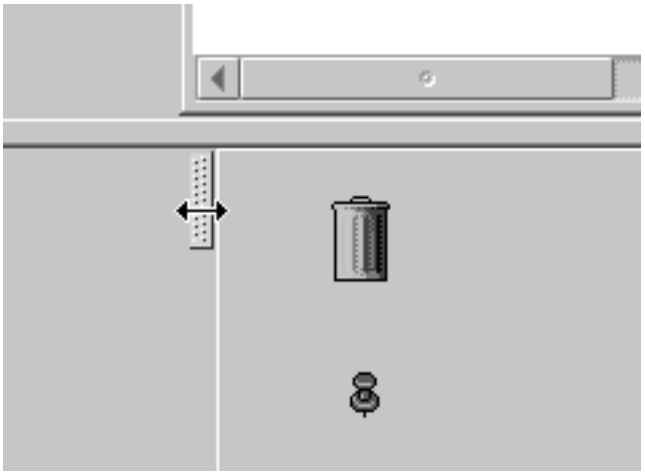
使用物件圖示時，請記得：

- 只能有一個唯一圖示來代表名稱空間中的每一個物件類型。
- 每一個作業標籤會顯示該管理作業所影響的物件圖示。
- 明細檢視畫面會顯示檢視畫面左上角中所編輯的物件之圖示。
- 拖放作業會顯示選取物件的圖示。
- 必須利用物件圖示來拖曳物件。
- 當游標位於您可拖曳的圖示上時，游標的形狀會變成手形。

使用分割圖示來調整檢視畫面大小

每一個管理作業畫面包含一或多個檢視畫面。使用檢視畫面左邊邊框頂端的分割圖示來調整這些檢視畫面的大小。同時，您也可以將游標移至兩個直欄標題之間的分割圖示，來調整清單檢視畫面中的直欄大小。

當您將游標移到分割器上時，游標形狀會變成雙向箭頭，指出您可以調整檢視畫面大小。



排序清單

您可以按一下直欄標題列，以升冪或降冪排序次序來輪換清單檢視畫面中的資訊。標題列右邊的圖示指出目前的排序次序。

排序清單後，清單中的選取項目會維持選取狀態。

展開及收縮樹狀檢視畫面

樹狀檢視畫面類似「Windows® 檔案總管」顯示檔案與目錄的方式。如果要展開或收縮節點，您必須察看圖示--具有加號或減號的方塊。按兩下這個圖示來輪換展開或收縮的樹狀檢視畫面。在鍵盤上就等於 **Ctrl + e**。

如果節點之下沒有物件或節點，在按一下節點之後，展開/收縮指示器會消失。

您可以展開或收縮根節點來復新整個樹狀組織。

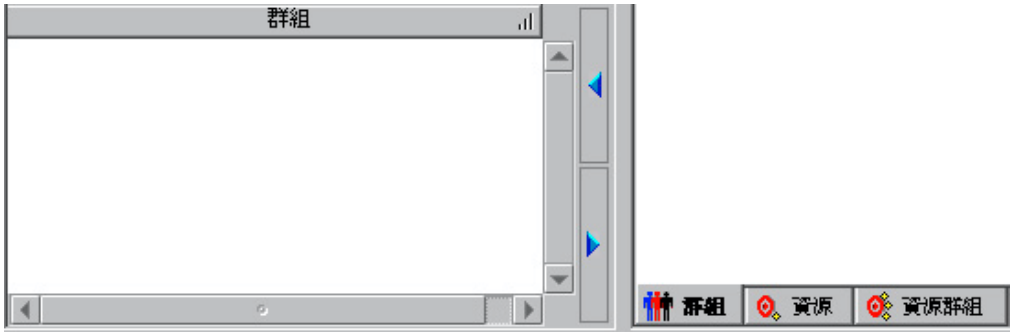
使用物件空間將節點箭頭移位

物件空間檢視畫面的標題列包含兩個藍色箭頭。這兩個藍色箭頭可讓您將樹狀檢視畫面的焦點限制到樹的分支上。

- **左箭號** -- 這個箭頭會將選取的節點或物件完全移至左邊，使它出現在在根的位置。
- **右箭號** -- 每按一下，這個箭頭就會將樹狀組織往回移動一個節點。 使用左箭號之後，請使用右箭號（一或多個按鍵）來將樹狀組織復置爲正常方位。

使用選擇箭號

選擇箭號會將選取的資訊從一個視窗檢視畫面移至另一個視窗檢視畫面。效果是將新的資訊輸入第二個視窗的欄位。



第5章 管理使用者帳戶及群組

Policy Director 安全模式在授與對物件的存取權之前，需要對使用者的身份進行身份驗證。您可以將使用者身份及加密的密碼和主要登錄資料庫中的帳戶資訊相比對，以完成使用者身份的驗證。根據預設， Policy Director 會使用 LDAP 登錄。 安全管理者可以使用「管理主控台」來建立及管理參與安全領域的使用者和群組。

本章包括：

瞭解使用者、群組及帳戶

Policy Director 安全服務程式依賴主要帳戶登錄--一個包含安全領域之使用者、群組及帳戶相關資訊的資料庫。根據預設， Policy Director 會使用 LDAP 登錄。

使用者

*使用者*是爲安全領域的 Principal 或參與者。使用者可以包括人類使用者、伺服器程序、機器或其他安全領域。

使用者是指可參與和另一位使用者之間的身份驗證交換的實體。*身份驗證*是指驗證使用者所宣稱之身份的程序。每一位使用者都有一個密碼（或機密金鑰），以便用於身份驗證。

您可以將使用者和存取控制許可權連結。每一位使用者都有自己的「廣用唯一識別碼」（UUID），這個識別碼一定會保持一致，即使使用者的名稱改變。 Policy Director 會將 UUID 當作安全證明傳送至安全服務程式。

群組

*群組*是藉由群組名稱來識別的使用者集成。群組可以代表不同層次的安全規則（或責任）。 爲了安全起見，Policy Director 會以相同方式對待屬於同一群組的使用者。 使用者可以屬於一個以上的群組，端視使用者的角色及職責而定。

群組可以讓您更容易管理以及處理安全原則。請使用 ACL 來定義群組的安全原則。當使用者的角色、責任或存在已經改變，這位使用者的所有 ACL 項目也必須改變。如果沒有群組，如果要改變含有個別使用者項目的所有 ACL，幾乎是不可能完成的作業。

群組 ACL 項目可以代表使用者的角色或責任。如果是以這種方式代表，則唯一需要的管理作業是新增或移除使用者在群組中的成員身份。

如同使用者一樣，除了群組名稱之外，群組還有 UUID。這個群組 UUID 代表使用者安全證明的其中一個元件。

帳戶

*帳戶*是涉及使用者、相關群組，以及相關安全資訊的一種關係。登錄中的帳戶會定義使用者的網路身份。 帳戶定義網路身份的方法是將使用者和一或多個群組及任何相關的安全資訊連結，例如用於身份驗證的密碼。

您必須爲跨越安全領域而進行通信的所有使用者建立一個帳戶，不論通信是否經過身份驗證。

您可以將使用者帳戶和使用者的密碼，以及當使用者登入安全領域時使用的任何資訊連結起來。帳戶資訊可以包括使用者的起始目錄、登入 Shell 及身份驗證原則（密碼）。這項資訊可以協助控制使用者對安全領域的存取。

註: 您必須先將群組新增至登錄，才能在使用者帳戶中使用它。

管理群組

群組是一或多個使用者的集成。您通常會建立群組來代表一個組織內的共同部門。（例如，業務、訓練及工程）。 您也可以建立以作業爲基礎的群組種類（例如，執行定期備份的系統管理者或使用者群組）。

群組種類可以簡化 Policy Director 安全領域中的存取控制管理。您可以爲使用者指定適當群組種類的成員身份，以容許新使用者存取資訊。這個方法可以減少爲每一位新使用者建立新 ACL 項目的需求。

例如，當新的人員加入工程部門時，您會建立一個包括**工程**群組種類成員身份的新使用者帳戶。新使用者現在可以讀取**工程**群組所允許的所有工程文件。您不需要在工程 ACL 模版中爲這個使用者建立新的 ACL 項目。

您可以利用「管理主控台」來新增、變更或移除 Policy Director 安全登錄中的群組項目。

在您建立一或多個群組項目之後，您可以指定使用者到群組中。使用者可以屬於一個以上的群組，反映出使用者不同的角色及責任。

使用「群組」管理畫面

安全領域的安全管理者使用「管理主控台」來建立群組：

1. 以管理者身份登入「管理主控台」，如 `cell_admin`。
2. 按一下**群組**作業標籤。

   此時會出現「群組」管理作業畫面。

使用動作按鈕來進行群組管理作業

您可以使用**群組**動作按鈕來執行「群組」管理作業。下表說明每一個動作按鈕所執行的作業：

動作按鈕	說明
新增	爲安全領域建立一個新的群組項目。

取得	擷取特別指定之群組的相關資訊，並且輸入明細檢視畫面視窗。
儲存	儲存此一群組項目。新的項目會出現在適當的清單視窗。
刪除	從登錄資料庫移除選取的群組。

使用群組明細欄位

下表說明「管理主控台」的**群組明細**檢視畫面中的欄位：

欄位	說明
群組名稱	指定給安全領域的群組的主要名稱。「群組名稱」是對登錄進行查詢時使用的主要欄位。
說明	說明群組的參考用文字字串。「說明」是一個選用的資料欄位，登錄並不會用到此欄位。
LDAP	如果是 LDAP： • 若是 cn =，請鍵入共通名稱，如 `credit` • 若是 dn=，請鍵入識別名稱，如 `cn=credit,o=IBM,ou=Austin,c=US`

建立新的群組

建立新的群組：

1. 按一下**新增**動作按鈕。

   啓動「群組明細」區域中的**群組名稱**及**說明**輸入欄位。
2. 鍵入新的群組名稱，並且在**說明**欄位中選擇性鍵入群組說明。
3. 若 LDAP 是您預設的登錄，加入必要的 LDAP 登錄資訊。
4. 您可以從「群組明細」檢視畫面的「使用者 ID」清單檢視畫面中，拖曳使用者圖示到使用者 ID 視窗來將使用者新增至群組。

   同時，您可以使用選擇箭頭來將使用者移出及移入「使用者 ID」畫面。
5. 按一下**儲存**動作按鈕。

   新的群組項目會出現在「群組」清單檢視畫面中。

變更群組明細

變更使用者成員身份或現存群組的名稱：

1. 從「群組」清單檢視畫面中選取一個群組。

   「群組明細」檢視畫面會輸入群組目前的相關資訊。
2. 在「群組明細」區域中，選取要變更的欄位（請參照『使用群組明細欄位』），然後鍵入新的值。
3. 您也可以將新的使用者加入到群組，或者從群組刪除使用者。

   從「使用者 ID」直欄，按兩下使用者圖示。然後，將新使用者 ID 拖放到「群組明細」檢視畫面中的「使用者 ID」視窗。您也可以使用選擇箭頭。
4. 按一下**儲存**。

移除群組

移除群組：

1. 從「群組」清單檢視畫面，選取您要刪除的群組名稱。
   群組成員清單會出現在「群組明細」檢視畫面中。
2. 選取每一個群組成員，每次選取一個，然後從群組中移除每一位使用者。
3. 從「群組」清單檢視畫面中選取群組。
4. 按一下**刪除**以完全移除群組項目。

管理使用者帳戶

要求存取安全領域中的服務程式及物件的使用者必須自行對 Policy Director 驗證其身份。想要參與 Policy Director 安全領域的每一位使用者都必須有一個已向 LDAP 登錄的帳戶。

使用使用者管理畫面

安全領域的安全管理者使用「管理主控台」來建立使用者帳戶：

1. 以管理者身份登入「管理主控台」（例如 `cell_admin`）。
2. 按一下**使用者**作業標籤。
   此時會出現「使用者」管理作業畫面。

使用動作按鈕來進行使用者管理作業

您使用**使用者**動作按鈕來執行「使用者」管理作業。下表說明每一個動作按鈕所執行的作業：

動作按鈕	說明
新增	爲安全領域建立一個新的使用者帳戶。
取得	擷取特別指定之使用者的相關資訊，並且輸入明細檢視畫面視窗。
儲存	儲存這個使用者帳戶。新的項目會出現在適當的清單視窗。
刪除	從登錄資料庫移除選取的使用者。

使用使用者明細欄位

下表說明「管理主控台」的**使用者明細**檢視畫面中的欄位：

欄位	說明
使用者 ID	指定給安全領域使用者的主要名稱。「使用者 ID」是對登錄進行查詢時使用的主要欄位。
說明	說明使用者的參考用文字字串。「說明」只是一個選用性資料欄位，登錄並不會使用它。
帳戶有效	這個勾選框可讓您控制使用者參與（或不參與）安全領域的能力。清除方框時，帳戶就不再有效。但是，帳戶資訊仍會保留在登錄中。
密碼有效	這個勾選框可讓您強制使用者在下次登錄安全領域時，一定要變更密碼。清除方框時，就會通知使用者他（她）的密碼已經過期。

GSO 使用者	這個勾選框指出使用者具有 GSO 功能。
LDAP	如果是 LDAP： • 若是 cn =，請鍵入一個共通名稱，如 Diana Lucas • 若是 sn=，請鍵入一個次名稱（姓），如 Lucas • 若是 dn=，請鍵入一個識別名稱，如 cn=Diana Lucas,o=IBM,ou=Austin,c=US

新增使用者帳戶

新增使用者帳戶：

1. 按一下**新增**動作按鈕。

   空白的輸入欄位會出現在「使用者明細」檢視畫面。
2. 在欄位中鍵入適當的資料。請參閱第68頁的『使用使用者明細欄位』以取得這些欄位的完整資訊。

   您可以從「群組」樹狀檢視畫面拖放**群組**圖示，將資料輸入「群組成員」視窗--或使用選擇箭頭。
3. 若 LDAP 是您預設的登錄，加入必要的 LDAP 登錄資訊。
4. 按一下**儲存**。

變更帳戶性質

變更現存帳戶的性質：

1. 從「使用者 ID」清單檢視畫面選取使用者。

   「使用者明細」區域會輸入現行資料。
2. 在「使用者明細」檢視畫面中，按一下您要變更的欄位。
3. 輸入新的資料。
4. 按一下**儲存**。

移除使用者帳戶

欲移除使用者帳戶：

1. 從「使用者 ID」清單檢視畫面選取使用者。
2. 按一下**刪除**。

建立多重管理帳戶

管理使用者必須位於以下群組中。當管理使用者位於這些群組中的時候，他（她）有權新增、變更或移除安全領域中的使用者、群組及組織：

- acct-admin
- subsys/dce/sec-admin
- subsys/dce/cds-admin

當您最初建立安全領域時，唯一包含這個群組組合的帳戶是 cell_admin。

在安全領域抵達特定大小後，如果一位管理者必須管理不斷增加的作業數目，就會造成很多問題。管理大型的安全領域時，需要指定管理責任。

您可以建立其他的管理帳戶，使他們具有相同的能力來操作「管理主控台」，方法是在列出的三個群組中指定他們的成員身份。規畫和組織這個權限的指派時，必須配合這些帳戶一起建立。

從其他來源匯入資訊

您可以將使用者資料和群組資料從其他來源輸入到登錄中。

第6章 管理 GSO 資源、資源群組及資源憑證

Policy Director 可藉由整合 IBM Global Sign-on（GSO）技術來支援更具彈性的單一登入解決方案。 您可以藉由建立 Policy Director 智慧型接合來達成整合。有關智慧型接合的完整資訊，請參閱第175頁的『第15章 WebSEAL：智慧型接合管理』。

當 WebSEAL 收到一則要取得所接合伺服器上之資源的要求時， WebSEAL 會使用 GSO 來擷取適當的身份驗證資訊。GSO 包含每一個已登錄使用者的對映資料庫，這些使用者爲特定的資源和應用程式提供了使用者名稱和密碼。 Policy Director 直接將 GSO 資料儲存在 IBM SecureWay Directory (LDAP) 中。

合併 WebSEAL 及 GSO 可提供一個完整的單一登入 Web 解決方案，並且具有資料加密、高度有用性及可調整性等額外好處。

進一步的資訊請參照第194頁的『整合 GSO 與 WebSEAL 的單一登入』。

瞭解 GSO 資源及 GSO 資源群組

GSO 包含特定的使用者*資源證明*，其使用者對映 GSO 資源至特定的使用者身份 (使用者名稱) 及密碼組合。 資源證明對 GSO 特定使用者 (如 Web 伺服器或 Web 伺服器群組) 提供此使用者名稱及密碼。

GSO 提供身份驗證資訊給 WebSEAL。當使用者想要執行應用程式資源時， WebSEAL 詢問 GSO 有關使用者的身份驗證資訊。GSO 維護著一個完整的身份驗證資訊資料庫，並採會對映到特定身份驗證資訊的資源形式。應用程式資源以及使用者名稱和密碼合併的對映稱爲 *GSO 資源證明*。 您只能爲登錄的使用者建立 GSO 資源證明。

註: 在您引用 GSO 資源證明到 GSO 資源或 GSO 資源群組之前，它們必須存在。

管理 GSO 資源

*GSO 資源*是 Web 伺服器。您可以對 Web 資源命名以識別之。

使用 GSO 資源管理畫面

要求存取安全領域中的服務程式及物件的 GSO 資源必須自行對 Policy Director 驗證其身份。想要參與 Policy Director 安全領域的每一位 GSO 資源都必須對 LDAP 登錄一個帳戶。

GSO 資源管理作業使用的動作按鈕

您使用 **GSO 資源**動作按鈕來執行 GSO 資源管理作業。下表說明每一個動作按鈕所執行的作業：

動作按鈕	說明
新增	爲安全領域建立一個新的 GSO 資源帳戶。
取得	擷取特別指定之 GSO 資源的相關資訊，並且輸入明細檢視畫面視窗。

儲存	儲存此 GSO 資源帳戶。新的項目會出現在適當的清單視窗。
刪除	從登錄資料庫移除選取的 GSO 資源。

使用 GSO 資源明細欄位

下表說明「管理主控台」的**資源明細**檢視畫面中的欄位：

欄位	說明
資源名稱	指定給安全領域的 GSO 資源的名稱。「資源名稱」是對登錄進行查詢時使用的主要欄位。
說明	說明資源的參考用文字字串。「說明」只是一個選用性資料欄位，登錄並不會使用它。

新增 GSO 資源

如果要新增 GSO 資源：

1. 按一下**新增**動作按鈕。

   空白的輸入欄位會出現在「資源明細」檢視畫面。
2. 在欄位中鍵入適當的資料。請參閱『使用 GSO 資源明細欄位』以取得這些欄位的完整資訊

   您可以從「資源群組」樹狀檢視畫面拖放**資源群組**圖示，將資料輸入「GSO 資源群組」視窗--或使用選擇箭號。
3. 按一下**儲存**動作按鈕。

建立 GSO 資源的資源證明

在您建立資源定義後，可爲使用者建立資源證明：

要建立資源證明時請：

1. 選取**使用者**標籤。
2. 標明出使用者名稱，以便爲該使用者建立資源證明。
3. 在「使用者明細 GSO 資源」檢視畫面中，選取**資源**標籤，列出目前可用的資源。
4. 選取要套用證明的資源。
5. 將所選資源拖曳到「使用者明細」檢視畫面的資源窗格中。

   新資源證明的登入 ID 與密碼值會預設爲與使用者帳戶的值相同。
6. 您可將此使用者資源證明的登入 ID 與密碼變更爲適當值，其方法是按一下**登入 ID** 或**密碼**按鈕，並填入適當值。
7. 按一下**儲存**動作按鈕。

變更 GSO 資源資訊

變更現存帳戶的性質：

1. 自「資源」清單檢視畫面選取 GSO 資源。

   「資源明細」區域會輸入現行資料。
2. 在「資源明細」檢視畫面中，按一下您要變更的欄位。
3. 變更現存的資料或輸入新資料。

4. 按一下**儲存**動作按鈕。

移除 GSO 資源

移除使用者帳戶：

1. 自「資源」清單檢視畫面選取 GSO 資源。
2. 按一下**刪除**。

管理 GSO 資源群組

*資源群組*是指 Web 伺服器群組，而群組中的所有伺服器會有同一組使用者 ID 及密碼。

使用 GSO 資源群組管理畫面

安全領域的安全管理者使用「管理主控台」來建立 GSO 資源群組：

1. 以管理者身份登入「管理主控台」，如 `cell_admin`。
2. 按一下 **GSO 資源群組**作業標籤。
   此時會出現「GSO 資源群組」管理作業畫面。

使用 GSO 資源群組管理作業的動作按鈕

您使用「GSO 資源群組」動作按鈕來執行資源管理作業。下表說明每一個動作按鈕所執行的作業：

動作按鈕	說明
新增	爲安全領域建立一個新的 GSO 資源群組項目。
取得	擷取特別指定之 GSO 資源群組的相關資訊，並且輸入明細檢視畫面視窗。
儲存	儲存此 GSO 資源群組項目。新的項目會出現在適當的清單視窗。
刪除	從登錄資料庫移除選取的 GSO 資源群組。

使用 GSO 資源群組明細欄位

下表說明「管理主控台」的**資源群組明細**檢視畫面中的欄位：

欄位	說明
資源群組名稱	指定給安全領域的 GSO 資源群組的主要名稱。GSO 資源群組名稱是對登錄進行查詢時使用的主要欄位。
說明	說明GSO 資源群組的參考用文字字串。說明只是一個選用性資料欄位，登錄並不會使用它。

新增 GSO 資源群組

如果要建立新的 GSO 資源群組：

1. 按一下**新增**動作按鈕。
   啓動「資源群組明細」區域中的**資源群組名稱**及**說明**輸入欄位。
2. 鍵入新的資源群組名稱，並且在**說明**欄位中選擇性鍵入資源群組說明。

3. 您可以將 GSO 資源圖示從「GSO 資源」清單檢視畫面拖移到「資源群組明細」檢視畫面的 GSO 資源視窗，新增 GSO 資源至新的 GSO 資源群組。

   同時，您可使用選擇箭頭移出及移入「GSO 資源」畫面中的資源。
4. 按一下**儲存**動作按鈕。

   新的 GSO 群組項目會出現在「資源群組」清單檢視畫面中。

建立 GSO 資源證明

您可以建立資源群組中全部資源的單一資源證明。 Policy Director 使用資源群組的單一資源證明，而不是資源群組中每個資源的資源證明。首先，您必須先建立資源群組，才能建立 GSO 資源證明。

要在建立資源群組定義後，建立使用者的 GSO 資源證明時請：

1. 選取**使用者**標籤，並選取所要的使用者，以便爲該使用者建立資源證明。
2. 在「使用者明細 GSO 資源群組」檢視畫面中，選取**資源群組**標籤，列出目前可用的資源群組。
3. 選取要套用證明的資源群組。
4. 將所選的資源群組拖曳到「使用者明細」檢視畫面的「資源群組」窗格中。

   新資源證明的登入 ID 與密碼值會預設爲與使用者帳戶的值相同。
5. 您可將此使用者資源證明的登入 ID 與密碼變更爲適當值，其方法是按一下**登入 ID** 或**密碼**按鈕，並填入適當值。
6. 按一下**儲存**動作按鈕。

變更 GSO 資源群組資訊

變更資源成員身份或現存資源群組的名稱：

1. 從「資源群組」清單檢視畫面中選取一個資源群組。

   「資源群組明細」檢視畫面會輸入資源群組目前的相關資訊。
2. 在「資源群組明細」區域中，選取要變更的欄位（**資源群組名稱**或**說明**），然後鍵入新的值。鍵入新值。
3. 您也可以將新的資源加入到資源群組，或者從群組刪除資源。

   從「資源群組」直欄，按兩下使用者圖示。然後，將新資源拖放到「資源群組明細」檢視畫面中的「GSO 資源」視窗中。您也可以使用選擇箭頭。
4. 按一下**儲存**動作按鈕。

移除 GSO 資源群組

如果要移除 GSO 資源群組：

1. 從「資源群組」清單檢視畫面，選取您要刪除的 GSO 資源群組名稱。

   GSO 資源群組成員清單會出現在「資源群組明細」檢視畫面中。
2. 選取每一個 GSO 資源，並將它從 GSO 資源群組中移除。
3. 從「資源群組」清單檢視畫面，選取 GSO 資源群組。
4. 按一下**刪除**以完全移除 GSO 資源群組項目。

移轉 GSO 資料

若您有來自 IBM SecureWay Global Sign-on 版本 2.0.200 或前一版 IBM Global Sign-On 的 GSO 資料，您會需要移轉 GSO 資料，它才能在這個版本的 Policy Director 使用。

最新的資訊及工具 (例如，移轉工具) 可以在 IBM SecureWay Policy Director 網站找到：

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

變更 GSO 資源證明密碼

使用者可使用 Policy Director Web 用密碼工具 (chpwd.exe)，更新所儲存的 GSO 資源或 GSO 資源群組密碼。必須已建立資源證明，才能使用此工具。請在第一次變更資源上的密碼後才使用此工具。

下列處可以找到這個檔：

UNIX： `/opt/intraverse/www/docs/cgi-bin/chpwd`

Windows： `c:\Program Files\www\docs\cgi-bin\chpwd.exe`

如要使用 Web 工具來變更 GSO 資源證明密碼時請：

1. 開啓一個安全瀏覽器案例。
2. 輸入下列 URL 位置：

   `https://`*`webseal server`*`/cgi-bin/chpwd.exe`

   其中 *webseal server* 是您 WebSEAL 伺服器的名稱。若使用 Windows，必須在指定的 URL 中鍵入 .exe 副檔名。
3. 按一下「資源名稱」直欄中的資源名稱，以選取它。
4. 在**使用者 ID** 欄位中鍵入您的使用者名稱。
5. 在**新密碼**欄位中鍵入您想要變成的密碼。然後，在**確認新密碼**欄位中重新鍵入加以確認。
6. 按一下**更新**。

第7章 瞭解存取控制

您可以保護安全領域中的資源。您可以藉由定義特殊規則以及將這些模版連接到資源的物件表示法來保護資源。這些特殊規則稱爲*原則模版*。 Policy Director 可以辨識以及使用稱爲*存取控制清單*（ACL）的原則模版。使用 ACL 來將組織的安全原則戳印到屬於安全領域的資源。

本章包括：

受保護的物件名稱空間

Policy Director 安全模式會根據規則（或許可權）來保護安全領域中的資源。有一組特定的許可權稱爲*原則模版*。

連接到資源時，原則模版會有效地將企業安全原則引用至資源。如果要完成這個安全模式， Policy Director 會使用安全領域的實體資源庫存的邏輯物件表示法。

如果要提供實際實體資源的保護，請將原則模版連接到名稱空間中的邏輯物件。 「Policy Director 權限服務程式」會藉由比較在身份驗證期間取得的使用者證明，以及在這些模版中定義的許可權，來進行授權決策。

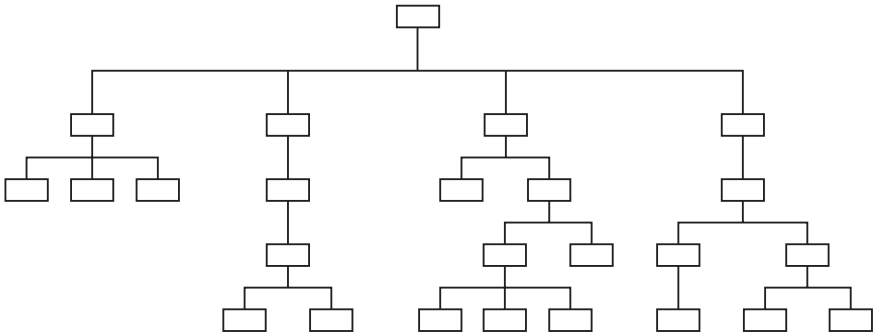
Policy Director *受保護的物件名稱空間*是屬於安全領域的的資源的邏輯與階層式呈現。出現在階層式名稱空間中的物件代表實際的實體網路資源。

系統資源

實際的實體檔、網路服務程式或應用程式。

受保護的物件

「Policy Director 權限服務程式」、「管理主控台」及其他 Policy Director 管理公用程式所使用的實際系統資源的邏輯呈現。



受保護的物件名稱空間使用兩種物件類型：

配置區物件

配置區物件是結構性的指定，可讓您以階層方式將名稱空間組織成個別的功能範圍。配置區物件包含資源物件。

資源物件

資源物件是您安全領域中實際網路資源的表示法（如服務程式、檔案及程式）。

受保護的物件名稱空間階層

受保護物件名稱空間的結構頂端是**根**配置區物件。在「Policy Director 管理主控台」中，根的符號是向前的斜線（/）。

以下的名稱空間種類是緊接著根物件之後：

Web 物件（/WebSEAL 配置區）

WebSEAL 配置區物件是安全領域的邏輯 Web 空間根。 Policy Director 可對這個次目錄樹中的部分物件授權所有的 HTTP 作業。

*Web 物件*代表 URL 可定址的任何項目，包括靜態 Web 網業及動態 URL。 Web 對應用程式的閘道會將這些靜態 Web 網頁或動態 URL 轉換成資料庫查詢或某些其他類型的應用程式呼叫。

網路應用程式物件（/NetSEAL 配置區）

NetSEAL 配置區物件是安全領域中包含 NetSEAL 受保護服務程式的邏輯空間根。 這些物件代表對映到 TCP 網路位址（埠）的 TCP 應用程式（如 TELNET 及 FTP）。應用程式會使用這些埠。

Policy Director 管理物件（/Management 配置區）

「管理」配置區物件是控制所有 Policy Director 管理作業的邏輯空間根。 管理物件代表定義使用者及設定安全原則所需的服務程式。 請使用「Policy Director 管理主控台」或 **ivadmin** 公用程式來執行這些作業。

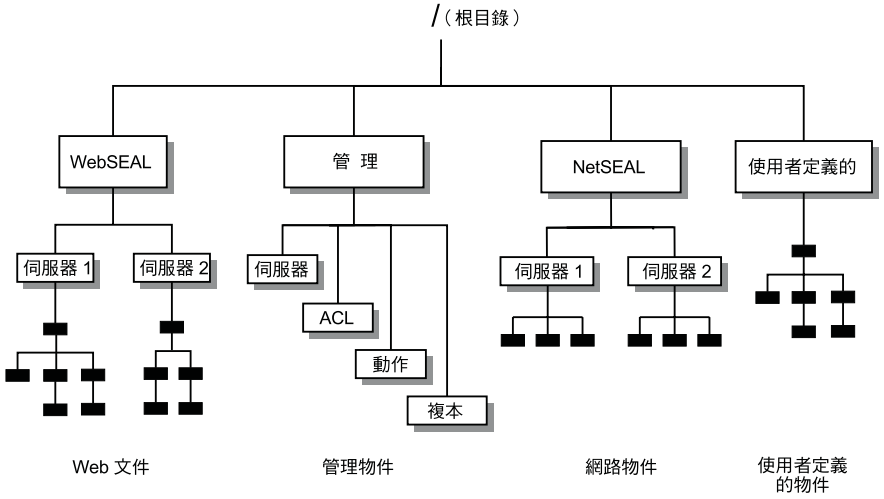
這個範圍的子分區包括：

- 伺服器管理作業（/伺服器）
- 安全原則作業（/ACL）
- 協力廠商授權控制（/動作）
- 權限資料庫複製控制（/複本）

Policy Director 支援管理活動的指定，並且可以限制管理者將安全原則設定至名稱空間子集的能力。

使用者定義的物件

這些物件代表由使用「Policy Director 權限服務程式」（利用 Policy Director 權限 API）的協力廠商應用程式所保護的作業或網路資源。



協力廠商應用程式名稱空間

Policy Director 可提供授權服務給受保護的物件名稱空間所定義的任何應用程式物件。屬於 Policy Director 系列一部分的應用程式包括 WebSEAL（用於 Web 應用程式）以及 NetSEAL（用於 TCP 應用程式）。

Policy Director 以及協力廠商應用程式會透過權限 API 來呼叫「Policy Director 權限服務程式」。 如果要將協力廠商的應用程式和「Policy Director 權限服務程式」整合在一起，請使用以下兩個步驟：

1. 說明協力廠商應用程式的名稱空間。
2. 對需要保護的任何名稱空間物件引用許可權。

可選用的使用者定義物件配置區，是指您可以建置協力廠商應用程式名稱空間所在的受保護物件名稱空間的範圍。

您必須在「受保護物件名稱空間」中定義這個協力廠商名稱空間開始的根（*接合點*）。詳細資訊請參閱 第127頁的『定義協力廠商應用程式名稱空間』。

然後您可以使用「管理主控台」或 **ivadmin** 公用程式來建立、連接，以及刪除這個名稱空間中的物件中的 ACL。

存取控制清單

存取控制清單（ACL）是 Policy Director 爲安全領域中的資源提供保護時所用的原則模版類型。

ACL 是一組規則或許可權，可指定對受保護資源執行作業時所需的條件。 ACL 可識別受保護的資源可允許的作業，並且列出可執行這些作業的人員之身分（使用者、群組，或兩者皆是），例如：

- 在安全登錄中，使用者身份以及群組身份的定義。
- 在授權原則資料庫中，受保護的物件名稱空間以及原則模版的定義。

作爲原則模版，每一個 Policy Director ACL 都有一個唯一的名稱（或*標籤*），以反應它所代表的安全原則。然後，您可以將 ACL 引用至受保護物件名稱空間中的資源之物件表示法。

ACL 是由一或多個項目（包括使用者指定及群組指定）及其特定許可權所組成。

ACL 項目

ACL 是由一或多個項目所組成，這些項目分別說明：

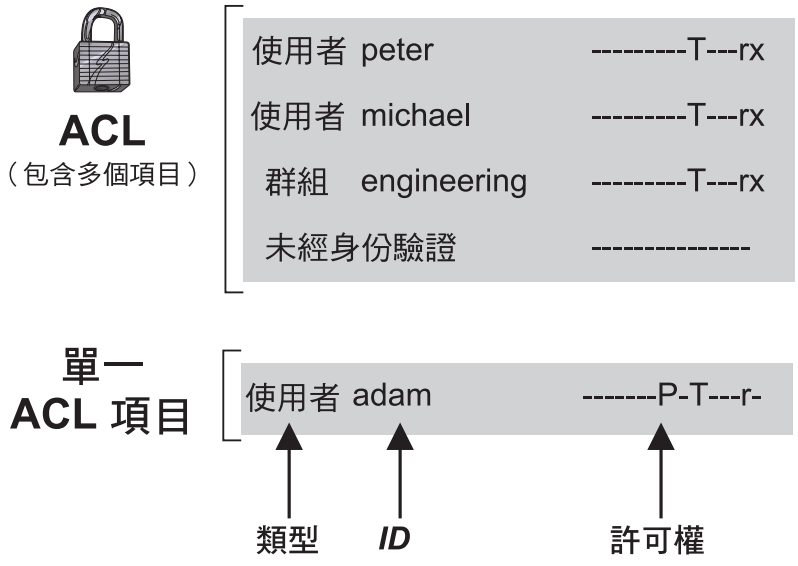
- 其物件存取權已受到明確控制的使用者和群組之 UUID
- 每一個使用者、群組或角色所允許的特定作業
- 特殊的 “任何” 及 “未經身份驗證” 使用者種類所允許的特定作業

使用者（或 Principal）代表由「Policy Director 安全伺服器」進行驗證的所有身份。通常，使用者代表網路使用者或應用伺服器。

*群組*是一或多個使用者的集成。網路管理者可以使用群組 ACL 項目來指定相同的許可權給多個使用者。新使用者可藉由變成適當群組的成員，來取得物件的存取權。這個方法可以減少爲每一位新使用者建立新 ACL 項目的需求。群組可以代表安全領域內的組織分支或部門。群組對於定義角色或功能連結也很有幫助。

總括來說，使用者和群組都是*實體*。

您可以使用「Policy Director 管理主控台」（**ACL** 管理標籤）來建立、變更及刪除 ACL 項目。



以 ACL 作為原則模板

「管理主控台」可讓您：

- 建立特定的 ACL。
- 將它以標籤來儲存。
- 將它以安全原則模版引用到名稱空間中的物件。

ACL 會變成單一來源模版，如同公式或秘訣。 ACL 包含爲任何連結物件提供正確保護層次的特定項目。

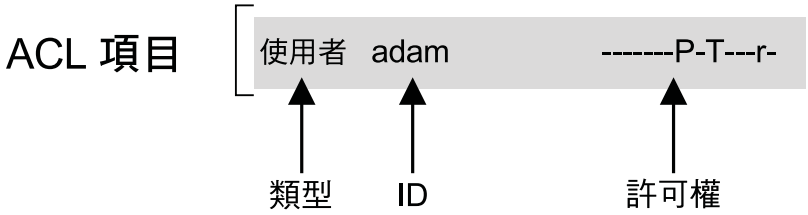
舉例來說，ACL 清單中可包含：

```
ACL 名稱
預設管理
預設 netseal
預設複製
預設根
預設 webseal
```

ACL 模版提供了和文字處理文件中的段落格式化樣式相同的單一資源參照品質。如果安全原則需求變更，您只能編輯單一 ACL。 Policy Director 會立即使連接 ACL 的所有物件的新安全定義生效。

ACL 項目語法

ACL 項目包含兩個或三個屬性，端視 ACL 項目類型而定，並且以下列格式出現：



類型

建立 ACL 的實體種類（使用者或群組）。

ID（身份）

實體的唯一識別碼（名稱）。

任何經身分驗證的 ACL 項目類型或未經身份驗證 ACL 項目類型都不需要 ID 屬性。

許可權

此一使用者或群組可對物件執行的作業集。

大部分的許可權會指定從屬站對資源執行特定作業的能力。每當容許對資源執行一個動作時，有幾個許可權會強制某些條件。後者的範例可能包括強制資料加密、保護資料的完整性、撰寫報告記錄至審核服務程式，或需要某些外部授權條件。

在本例中，Adam（類型=user，ID=adam）有權讀取（檢視）與含有此項目之 ACL 相關的物件。 讀取（r）許可權可容許進行讀取作業。 加密（P）許可權會強制通信通道使用資料加密。 遍訪（T）許可權會強制執行遍訪權屬性。

類型屬性

ACL 項目類型可指定 ACL 項目的實體。ACL 項目類型有四種：

類型	說明
使用者	爲安全領域中的特定使用者設定許可權。使用者項目類型需要帳戶名稱（ID）。項目格式爲：user ID 許可權。例如： `user greg -------------r-`
群組	爲安全領域中的特定群組設定許可權。群組項目類型需要群組名稱（ID）。項目格式爲：group ID 許可權。例如： `group engineering -------------r-`
任何經身分驗證的	爲所有經過身份驗證的使用者設定許可權。不需要指定 ID。項目格式爲： `any-authenticated -------------r-`

未經身份驗證	替尙未經「安全」伺服器身份驗證的使用者設定許可權。不需要指定 ID。項目格式爲：unauthenticated 許可權。例如：
	`unauthenticated ---------T---r-`
	此 ACL 項目是根據任何經身分驗證的 ACL 項目的遮罩（按位元"及"作業）來決定許可權集。例如，以下的未經身份驗證 ACL 項目：
	`unauthenticated -------------r-`
	是針對此任何經身分驗證的 ACL 項目的遮罩：
	`any-authenticated ---------T---r-`
	結果會產生這些許可權：
	`-------------r-`（唯讀）。

ID 屬性

ACL ID 是使用者項目或群組項目類型的*唯一識別碼*或名稱。 ID 必須代表爲安全領域建立，並且儲存在登錄資料庫中的有效使用者和群組。

下列是唯一的 ID 的範例：

```
user michael
user greg
group engineering
group documentation
group accounting
```

註: 請勿在任何經身分驗證的及未經身份驗證的 ACL 項目類型上使用 ID 屬性。

許可權屬性

每一個 ACL 項目都包含一組*許可權*，以用來說明：

- 使用者或群組可對物件執行的特定作業

- 對物件存取權類型的任何限制，例如：
  - 在通信通道上強制使用資料私密性或完整性
  - 經審核的存取
  - 外部（協力廠商）授權基本要求

ACL 藉由以下方式來控制受保護的資源：

- 使用者對受保護物件執行作業的能力
- 管理者變更物件及任何子物件之存取控制規則的能力
- Policy Director 伺服器指定使用者證明的能力

許可權順序

ACL 許可權是*切合當時情況需要的*許可權。 切合當時情況需要的許可權表示特定許可權的行爲會隨之改變。 行爲會根據引用許可權的受保護物件空間範圍而改變。 例如，m 許可權對於 WebSEAL 物件和「管理」物件的意義就不相同。

在 ACL 項目中使用許可權時，有十七個標準的許可權，它們可分成四個種類，並且以下列次序出現：

基本	同屬	NetSEAL	WebSEAL
a A b c g I P T	d m s v	C p	l r x

「ACL 定義/ACL 項目」視窗顯示您可以選取的許可權清單。選取這些許可權旁邊的勾選框，來選擇它們：

基本
(a) 連接
(A) 審核
(b) 瀏覽
(c) 控制
(g) 指定
(I) 完整
(P) 私有
(T) 遍訪權

同屬
(d) 刪除
(m) 修改
(s) 伺服器管理
(v) 檢視畫面

NetSEAL
(C) 連接
(p) Proxy

WebSEAL
(l) 清單目錄
(r) 讀取
(x) 執行

名稱空間的範圍

配置區物件代表受保護物件名稱空間的特定範圍，並且提供這些重要的安全功能：

1. 在並未引用其他明確的 ACL 時，您可以使用配置區物件的 ACL 來爲範圍內的所有子物件定義高層次原則。
2. 您可以使用配置區物件的 ACL 來爲範圍內的所有子物件定義高層次原則。在並未引用其他明確的 ACL 時，您可以定義高層次原則。

3. 您可以快速拒絕對範圍中所有物件的存取，方法是從配置區物件的 ACL 移除遍訪許可權。

遍訪許可權

遍訪許可權是一個同屬許可權，可引用至整個受保護的物件名稱空間：

遍訪許可權：	存取	說明
T	遍訪權	可容許要求程式在傳送至所要求的物件時，以階層方式傳送物件。它不容許對物件進行任何其他類型的存取。所要求的物件本身也需要遍訪權。

存取條件

存取條件是引用至整個受保護物件名稱空間的同屬許可權：

所有受保護物件的存取條件：	存取	說明
A	審核	每次存取物件時，會導致 Policy Director 伺服器撰寫一筆審核記錄到審核服務程式。審核所有的存取嘗試，包括授權失敗
I	完整性	如果要存取這個物件，則從屬站及 Policy Director 伺服器之間需要資料完整性保護。
P	私密性	如果要存取這個物件，則從屬站及 Policy Director 伺服器之間需要資料加密。

控制許可權

控制許可權是一個威力強大的許可權，可提供您 ACL 的所有權。控制權可讓您改變 ACL 中的項目。控制權表示您有權建立項目、刪除項目、授與許可權，以及移除許可權。

控制許可權：	存取	說明
c	控制	ACL 模版的所有權；可讓您建立、刪除及修改這個 ACL 的項目

管理者可以從這個 ACL 模版的清單中刪除這個 ACL。在刪除前，管理者在這個 ACL 中必須具備一個項目。同時，管理者必須在該項目中具有控制許可權集。

控制許可權可讓您將管理權授與給另一位使用者。例如，您可以授與將 ACL 連接到物件的能力。您可以使用連接（a）許可權來將 ACL 連接到物件。

您必須小心使用控制（c）許可權，因爲它具備強大的所有權性質。

根配置區物件

以下的安全考量適用於 *根* (/) 配置區物件：

- 根物件是整個受保護物件名稱空間的 ACL 承接連鎖的開頭。
- 如果您沒有引用任何其他明確的 ACL，根物件會定義（透過承接）整個名稱空間的安全原則。

- 您必須使用遍訪許可權（T）來存取根以下的所有物件。

WebSEAL 名稱空間

以下的安全考量適用於 /WebSEAL 配置區物件：

- WebSEAL 物件是名稱空間 WebSEAL 範圍的 ACL 承接連鎖的開頭。
- 如果您沒有引用任何其他明確的 ACL，這個物件會定義（透過承接）整個 Web 空間的安全原則。
- 您必須使用遍訪許可權（T）來存取這個物件以及這個點以下的所有物件。

/WebSEAL/host

這個次目錄樹包含特定 Policy Director WebSEAL 伺服器的 Web 空間。以下的安全考量適用於這個物件：

- 您必須使用遍訪許可權（T）來存取這個點以下的所有物件。
- 如果您沒有引用任何其他明確的 ACL，這個物件會定義（透過承接）這部機器上整個名稱空間的安全原則。

/WebSEAL/host/file

這個次目錄樹是用來檢查 HTTP 存取的資源物件。檢查的許可權是根據所要求的作業而定。

WebSEAL 許可權

下表說明適用於名稱空間 WebSEAL 範圍的許可權：

WebSEAL 名稱空間許可權：	存取	說明
r	讀取	檢視 HTTP 物件
x	執行	執行 CGI 程式
d	刪除	移除 HTTP 物件
m	修改	放置（PUT）HTTP 物件（放置 - 發行 - HTTP 物件到 WebSEAL 名稱空間中）
l	清單	產生 HTTP 目錄自動清單
g	指定	指定信任 WebSEAL 伺服器代表從屬站行動，並且將要求傳送給接合的 WebSEAL 伺服器

NetSEAL 名稱空間

以下的安全考量適用於 /NetSEAL 物件：

- NetSEAL 物件是物件名稱空間 NetSEAL 範圍的 ACL 承接連鎖的開頭。
- 如果您沒有引用任何其他明確的 ACL，這個物件會透過承接，定義名稱空間中所有 NetSEAL 受保護服務程式的安全原則。
- 您必須使用遍訪許可權（T）來存取這個物件以及這個點以下的所有物件。

/NetSEAL/host

這個次目錄樹包含特定伺服器機器上的所有 NetSEAL 受保護服務程式。以下的安全考量適用於這個物件：

- 您必須使用遍訪許可權（T）來存取這個點以下的任何資源。
- 如果您沒有引用任何其他明確的 ACL，這個物件會定義（透過承接）這部機器上所有 NetSEAL 受保護服務程式的安全原則。

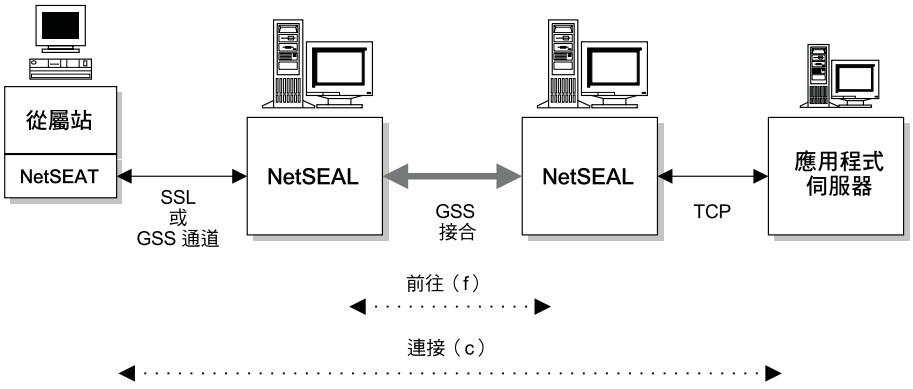
/NetSEAL/host/service

這個次目錄樹是用來檢查的物件，以便存取它所代表的受保護服務程式。檢查的許可權是根據所要求的作業而定。

NetSEAL 許可權

下表說明適用於名稱空間 NetSEAL 範圍的許可權：

NetSEAL 受保護的物件許可權：	存取	說明
C	連接	連接至 NetSEAL 伺服器
f	轉遞	允許跨越 NetSEAL 接合送出的連接；遍訪接合。



管理名稱空間

以下的安全考量適用於 /Management 物件：

- 「管理」物件是物件名稱空間「管理」範圍的 ACL 承接連鎖的開頭。
- 如果您沒有引用任何其他明確的 ACL，這個物件會定義（透過承接）整個「管理」名稱空間的安全原則。
- 您必須具備這個物件的遍訪（T）許可權。

/Management/server

Policy Director 受保護物件名稱空間的 /Management/server 配置區物件可讓管理者執行伺服器管理作業（如果已設定適當的許可權）。

使用伺服器管理控制項來決定使用者是否有許可權來建立、變更或刪除伺服器定義。伺服器定義包含可容許其他 Policy Director 伺服器（特別是「管理」伺服器，ivmgrd）尋找以及與該伺服器通信的相關資訊。

在安全程序期間，您可以爲特定的「安全管理程式」（secmgrd）或「權限伺服器」（ivacld）建立伺服器定義。當您解除安裝伺服器時，Policy Director 也會刪除伺服器的定義。

定義的建立與刪除會自動發生；安裝管理者不必執行任何特殊步驟來建立定義。然而，在安裝期間，管理者必須具備 /Management/Server 物件的（m）許可權才能建立定義。

此外，在解除安裝期間，管理者必須具備 /Management/Server 物件的（d）許可權才能刪除定義。

可對伺服器定義執行的其他作業還包括容許使用者執行以下各項：

- 透過 **ivadmin** 公用程式來檢視定義。使用者必須被授與伺服器物件的檢視（v）許可權。
- 執行伺服器管理作業，如啓動、停止、暫停、回復伺服器，或刪除日誌。使用者必須被授與伺服器物件的伺服器管理（s）許可權。
- 請使用 **ivadmin server modify** 指令來變更定義。使用者必須被授與伺服器物件的修改（m）許可權。

伺服器管理許可權：	存取	說明
s	伺服器	執行伺服器管理作業（如啓動、停止、暫停、回復）
v	檢視	列出伺服器
m	修改	建立新的伺服器定義
d	刪除	刪除伺服器定義

/Management/ACL

這個物件可讓管理使用者執行會影響安全領域之安全原則的高層次 ACL 管理作業。

ACL 管理許可權：	存取	說明
b	瀏覽	檢視物件之下的名稱空間內容
a	連接	將 ACL 模版連接到物件；從物件移除 ACL 模版
m	修改	建立新的 ACL 模板
d	刪除	刪除現存的 ACL 模板。對於相同的使用者，ACL 必須包含一個項目，並且具有控制（c）許可權。
v	檢視	列出或檢視 ACL

您必須定義預設 ACL 管理物件中的 ACL 管理者。管理者的 ACL 項目可以包含上述任何許可權。這些許可權可以提供管理者建立新的 ACL 模版、將 ACL 連接至物件，以及刪除 ACL 模版。

ACL 管理者無法變更現存的 ACL，除非含有控制（c）許可權的管理者在這個 ACL 中有一個項目。只有 ACL 的擁有者才能變更 ACL 的項目。

請注意，新的 ACL 模版的建立者會成爲該 ACL 中的第一個項目，並且具有預設值所設定的 abcT 許可權。

例如，如果 cell_admin 是預設管理 ACL 中的項目，並且具備（m）許可權，則 cell_admin 可以建立新的 ACL 模版。使用者 cell_admin 會成爲新 ACL 中的第一個項目，並且具有 abcT 許可權。控制（c）許可權會提供 ACL 的所有權給 cell_admin，並且容許 cell_admin 變更 ACL。然後，使用者 cell_admin 會將管理許可權授與該 ACL 中的其他使用者項目。

根據預設，預設管理 ACL 本身的所有權會提供給使用者 cell-admin 及群組 iv-admin。

/Management/action

這個物件可容許管理使用者在協力廠商名稱空間中執行 ACL 管理作業。動作作業和相關的許可權包括：

動作管理許可權（協力廠商授權）：	存取	說明
m	修改	建立新的動作
d	刪除	刪除現存的動作

Policy Director 會提供權限服務程式給應用程式。屬於 Policy Director 系列一部分的應用程式包括 WebSEAL（用於 Web 應用程式）以及 NetSEAL（用於 TCP 應用程式）。

協力廠商應用程式會透過權限 API 來呼叫「Policy Director 權限服務程式」。 如果要將協力廠商的應用程式和「Policy Director 權限服務程式」整合在一起，則需要以下兩個步驟：

- 定義應用程式的名稱空間。
- 對需要保護的物件（資源）引用許可權。

協力廠商應用程式名稱空間的管理者可以使用 **ivadmin** 公用程式來定義新的許可權和動作。管理者必須具備「管理」和「動作」許可權，才能建立及刪除這些許可權和動作。

/Management/replica

Policy Director 受保護物件名稱空間的 /Management/Replica 配置區物件會控制權限資料庫的複製。對這個物件的高層次控制會影響安全領域中「管理」伺服器及「安全管理程式」的作業。

複本管理控制是用來決定可容許哪些程序讀取或更新主要授權原則資料庫，以便讓複製順利發生。

控制和相關的許可權包括：

複本管理許可權：	存取	說明
v	檢視	讀取主要權限資料庫
m	修改	授權對複本資料庫進行修改

所有的 Policy Director 伺服器都會維護一份權限資料庫的本端複本。 Policy Director 伺服器包括所有「安全管理程式」（secmgrd）以及「授權」伺服器（ivacld）。 所有的 Policy Director 伺服器對於 /Management/Replica 物件都有檢視（v）許可權。

複製程序可讓這些程序檢視及存取主要授權原則資料庫以外的項目。 Policy Director 安裝會自動授與讀取（r）許可權給需要存取授權原則資料庫的任何伺服器。

Policy Director 目前不使用修改（m）許可權。目前，您可以透過「管理主控台」或 **ivadmin** 公用程式來變更主要原則權限資料庫。這些工具受限於其他更精密的檢查。

安全名稱空間指引

這些指引提供許多可協助您保護名稱空間的資訊：

- 在名稱空間之上的配置區物件設定高層次安全原則。 設定這個原則的例外，使明確的 ACL 位於階層中較低的物件。
- 排列受保護的物件空間，讓大部份的物件受承接的 ACL（而非明確的 ACL）保護。

  承接的 ACL 可簡化樹狀組織的維護，因爲它們會減少您必須維護的 ACL 數目。較少的維護可以減少錯誤的風險，後者可能會連累您的網路。
- 將新的物件放置在它們承接適當許可權所在的樹狀組織中。

  將您的物件樹狀組織排列成次目錄樹，而每一個次目錄樹都是由特定存取原則所支配。您可以在次目錄樹根設定明確的 ACL，以決定整個次目錄樹的存取原則。
- 建立 ACL 模版的核心集，並且在必要時重覆使用這些 ACL。

  由於 ACL 模版是單一來源的定義，對於模版的任何修改都會影響與這個 ACL 相關的所有物件。
- 透過群組的使用來控制使用者存取。

  ACL 可能只是由群組項目組成。新增或從這些群組移除使用者，可以有效控制個別使用者對物件的存取。

標準的管理 ACL 模板

建議您使用以下的預設管理 ACL 模版來開始保護安全領域的特定範圍。

您可以新增使用者、群組、任何經身分驗證的，以及未經身份驗證的項目。這些項目提供更廣的控制範圍，更能符合受保護物件空間的需要。

請注意每一個包含控制（c）許可權的 ACL 中的使用者和群組。具有控制許可權的使用者、群組（或兩者皆是）可*擁有* ACL，並且可以變更 ACL 項目。

根

預設根 ACL（預設根）的核心項目包括：

user cell_admin	abcT
group iv-admin	abcT
任何經身分驗證的	T
unauthenticated	T

根 ACL 是非常基本的。每一位都可以遍訪名稱空間，但無法執行任何其他動作。您通常不需要變更這部分。但是，根 ACL 有一個很有用的功能，它能夠快速拒絕個別使用者或群組對整個名稱空間的存取。

請考量根 ACL 中的下列項目：

```
user john -----------------
```

這個項目（無許可權）的結果是 user john 甚至無法遍訪根配置區物件。這位使用者完全無法存取受保護的物件空間，不論授與給樹狀組織底下的許可權爲何。

您可以對 WebSEAL 及 NetSEAL 物件空間引用相同的方法。例如，您可以移除特定使用者在 /WebSEAL 配置區物件的遍訪（T）許可權。移除後，使用者就完全無法進入 WebSEAL 名稱空間。不管授與哪些許可權給這些範圍內的物件，使用者都無法進入。

WebSEAL 物件空間

WebSEAL ACL（預設 webseal）的核心項目包括：

```
user cell_admin                    abcTdmlrx
group iv-admin                     abcTdmlrx
group webseal-servers              gTdmlrx
group ivmgrd-servers               Tl
```

安裝時，這個預設的 ACL 是連接到名稱空間中的 /WebSEAL 配置區物件。

群組 webseal-servers 爲安全領域中的每一個 WebSEAL 伺服器包含一個項目。預設的許可權可讓伺服器回應瀏覽器的要求。

群組 ivmgrd-servers 只包含一個代表「管理」伺服器的項目。「管理主控台」大部分的管理要求都是利用「管理」伺服器來對目標 WebSEAL 伺服器啓動。因此，「管理」伺服器必須具備在目標伺服器上執行要求的許可權。

遍訪許可權可容許在「管理主控台」中所呈現的 Web 空間之擴充。清單許可權可讓「管理主控台」顯示 Web 空間的內容。

NetSEAL 物件空間

NetSEAL ACL（預設 netseal）的核心項目包括：

```
user cell_admin                    abcTC
group iv-admin                     abcTC
```

安裝時，這個 ACL 是連接到名稱空間中的 /NetSEAL 配置區物件。您必須授與控制（c）許可權以存取受保護的服務程式。

管理物件空間

「管理」ACL（預設管理）的核心項目包括：

```
user cell_admin                    abcTdmsv
group iv-admin                     abcTdmsv
group ivmgrd-servers               Ts
任何經身分驗證的                   Tv
```

```
unauthenticated                         Tv
```

安裝時，這個 ACL 是連接到名稱空間中的 /Management 配置區物件。

複本管理物件

「複本」管理 ACL（預設複本）的核心項目包括：

```
group secmgrd-servers                   dmv
group ivacld-servers                    dmv
group ivmgrd-servers                    m
group iv-admin                          abcTv
user cell_admin                         abcTv
```

ACL 的評估

Policy Director 遵循一個特定的評估程序，以決定 ACL 授與特定使用者的許可權。

經身份驗證的要求之評估

Policy Director 會以下列次序評估經身份驗證的使用者：

1. 將使用者 ID 與 ACL 的使用者項目做比對。授與的許可權就是比對項目中的許可權。

   順利完成：評估在此停止。未順利完成：繼續下一步。

2. 決定使用者所屬的群組，並且將它與 ACL 的群組項目比對：

   如果有一個以上的群組項目相符，則產生的許可權是每一個相符項目所授與的邏輯"或"（最寬大的）許可權。

   順利完成：評估在此停止
   未順利完成：繼續下一步。

3. 授與任何經身分驗證項目的許可權（如果存在）。

   順利完成：評估在此停止
   未順利完成：繼續下一步。

4. 如果沒有任何經身分驗證的 ACL 項目，則有隱含的任何經身分驗證的實體存在。這表示項目沒有授與任何許可權。

   順利完成：未授與許可權。
   評估程序結束。

未經身份驗證的要求之評估

Policy Director 會從 ACL 的未經身份驗證項目來授與許可權，以評估未經身份驗證的使用者。

在決定許可權時，*未經身份驗證項目*是針對經身份驗證項目的遮罩（按位元"及"作業）。只有當許可權也出現在任何經身分驗證的項目時，才會授與未經身份驗證的許可權。

由於未經身份驗證是根據任何經身分驗證的而定，當 ACL 包含未經身份驗證，而不含任何經身分驗證的時，則沒有太大意義。如果 ACL 確實包含未經身份驗證，而不含任何經身分驗證的，則預設的回應是不授與許可權給未經身份驗證。

ACL 項目範例

您可以藉由指定適當的 ACL 項目類型，來爲特定使用者、群組（或兩者皆是）設定許可權。在以下範例中，群組 documentation 具有完整的存取專用權：

```
group documentation --bcg--TdmsvC-lrx
```

您可以利用任何經身分驗證的項目類型，以限制對安全領域中其他經身份驗證之使用者（不屬於 documentation 群組）的存取權：

```
any-authenticated -------T-------rx
```

您可以進一步限制不屬於安全領域成員的使用者對未經身份驗證項目類型的存取：

```
unauthenticated -------T-------r-
```

註: 如果沒有未經身份驗證 ACL 項目，未經身份驗證的使用者就無法存取 Policy Director 安全領域中任何安全文件。

ACL 承接的稀疏（Sparse）ACL 模式

如果要保護受保護物件空間中的網路資源，您必須將 ACL 連接到每一個物件。

您可以用下列一種方法將 ACL 指定給物件：

- 在物件上連接*明確的* ACL
- 容許物件從之前階層中的配置區物件*承接*其 ACL

採用承接的 ACL 綱目可以大幅減少安全領域的管理作業。本節討論承接或稀疏 ACL 的概念。

稀疏 ACL 模式概觀

這個原則是 ACL 承接的威力基礎：任何未明確連接 ACL 的物件會承接其最接近的配置區物件（具有明確設定的 ACL）的 ACL。換言之，所有*並未*明確連接 ACL 的物件會從*具有*明確連接 ACL 的配置區物件來承接 ACL。當您在物件上連接明確的 ACL 時，就會*岔斷*特定的承接連鎖。

ACL 承接可簡化在大型受保護的物件空間上設定及維護存取控制的作業。在典型的物件空間中，您只需要連接位於關鍵位置的少數 ACL，就能保護整個物件空間。位於關鍵位置的少數 ACL 即表示這是一個*稀疏* ACL 模式。

典型的 Policy Director 名稱空間會以連接到根配置區物件的單一明確 ACL 作爲開頭。根 ACL 一定要存在，絕對不可以移除。通常，這是一個限制很少的 ACL。所有位於其下的物件都會承接這個 ACL。

當名稱空間中的範圍或次目錄樹需要不同的存取控制限制時，您可以在該次目錄樹的根連接明確的 ACL。此動作會*岔斷*從主要名稱空間根到該次目錄樹的承接 ACL 串流。新的承接連鎖會從這個新建的明確 ACL 開始。

預設的根 ACL 模板

Policy Director 會從受保護的物件空間的根開始檢查承接。 如果您沒有明確地在樹狀組織中的任何其他物件上設定 ACL，則整個樹狀組織都會承接這個根 ACL。

在根設定的一定是明確的 ACL 模板。管理者可以將這個 ACL 取代成另一個含有不同項目及許可權設定的 ACL。 但是根 ACL 絕不能完全移除。

在 Policy Director 初始安裝及配置期間，在「ACL 定義/ACL 項目」視窗，Policy Director 會明確設定根 ACL 模板：

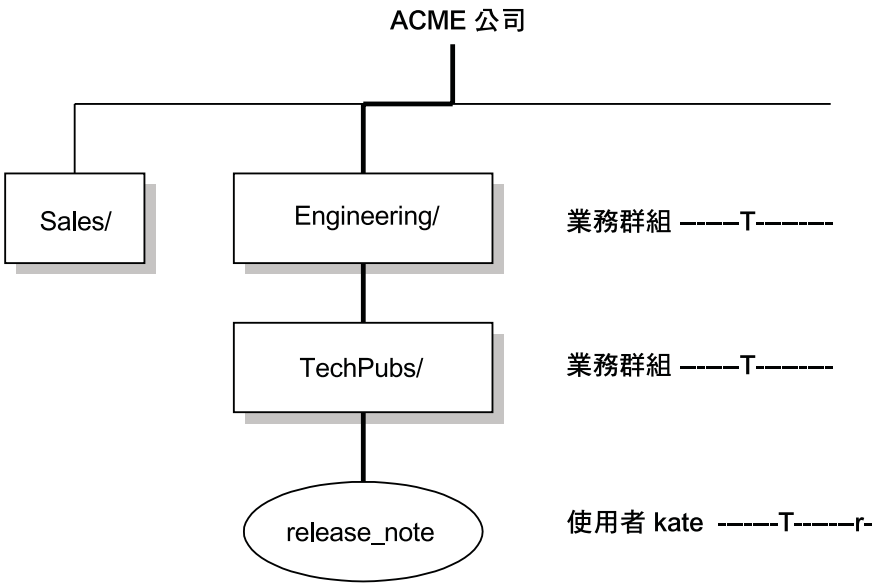
ACL 名稱 預設根
說明 預設根 ACL

遍訪許可權

遍訪（T）許可權指定 ACL 項目中已識別的實體有權傳送至該物件。項目需要許可權才能傳送至該物件，以取得對階層以下的物件之存取權。遍訪許可權並不會爲該物件授與其他許可權。您必須對所要求的物件本身提供遍訪許可權。

下圖說明遍訪許可權的運作方式。在 ACME 公司中有一個 Engineering 目錄，其中也包含一個 TechPubs 子目錄。 Kate（使用者 kate）是 Sales（業務）部門的成員之一，她需要存取 /Engineering/TechPubs 目錄，以檢視版本注意事項檔案。

管理者在 /Engineering 和 /TechPubs 目錄上都放置了一個群組 sales ACL 項目，並且具備遍訪（T）許可權。 雖然使用者 kate 在這兩個目錄中沒有其他許可權，她仍可以進入這些目錄以存取 release_note 檔。由於這個檔案同時具有使用者 kate 的遍訪（T）及讀取（r）許可權，因此她可以檢視檔案。



您可以輕易對給定配置區物件之下的階層限制存取--而不必在這些物件上重設個別的許可權。您只要從適當的 ACL 項目移除遍訪許可權即可。移除目錄物件上的遍訪許可權可以保護階層中較低的所有物件，即使這些物件包含其他限制較少的 ACL。

例如，群組 sales 必須具有 Engineering 目錄的遍訪（T）許可權。如果群組 sales 不具備，Kate 就無法存取 release_note 檔，即使她具備檔案的讀取（r）許可權。

存取要求的解決方案

承接會以根 ACL 作爲開頭，並且會影響名稱空間中的所有物件，直到它到達具有明確 ACL 的物件。此時會開始新的承接連鎖。

明確設定的 ACL 以下的物件會承接新的存取控制。如果您刪除明確的 ACL，所有物件的存取控制將回到最接近的目錄，或具有明確設定的 ACL 的配置區物件。

當使用者嘗試存取安全物件時，Policy Director 會檢查使用者是否有權存取物件。例如，安全物件可能是一份 Web 文件。它會檢查物件階層中的每一個物件，以取得適當承接或明確設定的許可權。

您可以拒絕使用者對物件的存取權。當階層之上的任何目錄物件或配置區物件不含該使用者的遍訪（T）許可權時， Policy Director 會拒絕存取。同時，當目標物件沒有足夠的許可權來執行所要求的作業時， Policy Director 會拒絕存取。

爲了順利進行存取檢查，要求程式必須具備以下兩者：

1. 遍訪至所要求物件之路徑的許可權。
2. 所要求物件的適當許可權。

以下範例說明當解決使用者是否能讀取（檢視）物件的程序：

```
/acme/engineering/project_Y/current/report.html
```

Policy Director 會檢查以下各項：

1. 明確設定的根 ACL（/）的遍訪許可權。
2. 對連接目錄的任何明確 ACL 遍訪許可權：`acme`、`engineering`、`project_Y` 及 `current`。
3. 檔案本身（report.html）的讀取許可權。

當使用者無法通過物件階層任一點的存取檢查時，Policy Director 會拒絕使用者存取。

引用至不同物件類型的 ACL 模版

您可以在 ACL 模版中爲許多作業設定許可權。 對於連接 ACL 的特定物件，只有這些可行作業的子集可能相關。

這個行爲的原因和 Policy Director 的兩種特性有關，其設計是爲了使管理更方便：

- ACL 模版
- ACL 承接

ACL 模版可讓您將相同的 ACL 定義連接到受保護物件名稱空間中的多個物件。 ACL 定義是由數量足以符合將引用 ACL 的所有物件基本要求的項目所組成。然而，只有少數項目會影響每一個個別的物件。

在 ACL 承接模式中，任何不含已連接的明確 ACL 的物件將會承接原則定義。這些承接的原則定義來自最接近的 ACL（引用至階層中在它之上的物件）。

總結來說，ACL 模版必須爲它將引用的所有物件類型說明所有必要的許可權。 ACL 模版不只會說明它所連接的物件。

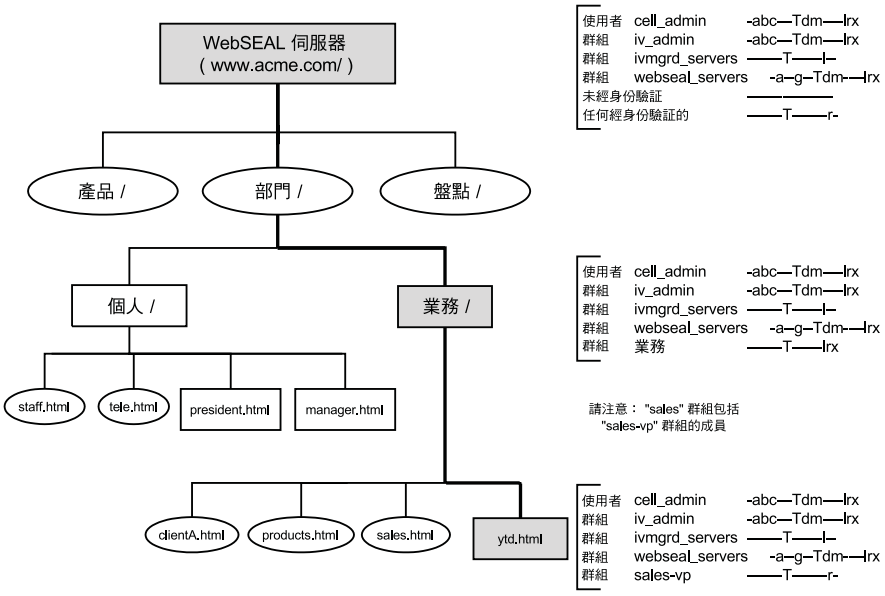
ACL 承接的範例

下圖說明在企業名稱空間中，混合承接以及明確的 ACL 所造成的影響。

企業物件空間在根物件已經設定了一般安全原則。根之後緊接著 /WebSEAL 配置區物件以及個別控制的部門此目錄樹。

在本例中，sales 群組對於它們的部門次目錄樹具有所有權。請注意，這個次目錄樹上的 ACL 已不再認可未經身份驗證或任何經身分驗證的項目類型。「迄今年份」業務檔（ytd.html）有一個明確的 ACL。這個明確的 ACL 會授與讀取（r）許可權給 sales-vp 群組的成員；這些 sales-vp 群組成員也是 sales 群組的成員。

註: 這個 ACL 綱目不需要藉由新增或刪除安全領域中的使用者來加以改變。只要將新使用者加入適當的群組即可。同樣地，您也可以從這些群組移除使用者。



ACL 管理指定

在安全領域中，管理責任的分送稱爲管理指定。管理指定的需求通常是源自大型網站（其中包含特殊的部門和資源部門）的成長需求。

通常，大型的物件空間可以組織成代表這些部門或分支的範圍。領域的每一個區分範圍都可以組織得更好。同時，每一個區分範圍都可以由熟悉課題以及該分支的需求的管理者來維護。

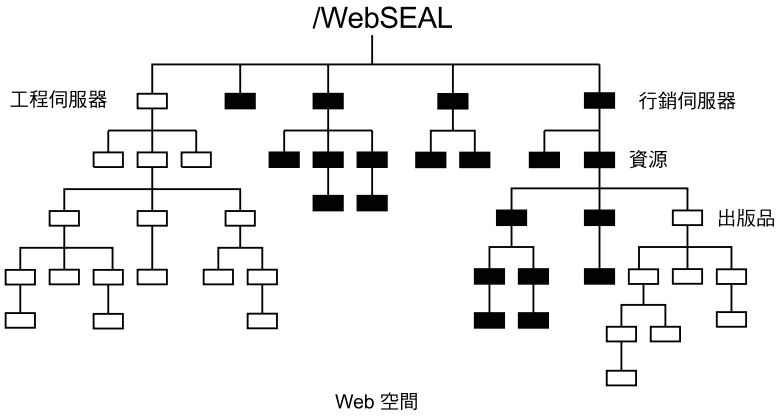
領域的每一個區分範圍通常會組織得更好。由熟悉課題以及該分支的需求的管理者來維護每一個區分範圍。

在 Policy Director 安全領域中， cell_admin 帳戶是一開始就具備管理許可權的唯一帳戶。身爲 cell_admin，您可以建立管理帳戶，並且爲物件空間的特定範圍指定適當的控制給這些帳戶。

為管理指定建構名稱空間

建構您的物件空間來包含區分範圍或分支，以便執行該分支特定的次管理責任。

在以下的範例中，物件空間的 Engineering 及 Publications 範圍需要個別的管理控制。這些範圍的控制是從每一個範圍的根開始，並且延伸到其下的所有物件。



使用預設的管理使用者和群組

Policy Director 會建立數個重要的管理群組。根據預設，這些使用者、群組（或兩者皆是）都會具有特殊許可權，以控制及管理安全領域中的所有作業。這個預設的安全原則是由安裝期間所建立的 ACL 定義。

以下各節詳細說明在安裝時指定給每一個使用者和群組的特殊角色。管理者可以在稍後自行設定這些專用權，以容納改變的管理原則。

user cell_admin

這個使用者代表安全領域的管理者，他會被授與在安全領域中執行所有作業的完整權利。

這個原則可以隨著物件空間的成長改變。您可以藉由指定管理許可權給其他使用者來改變原則。或者，您可以從 cell_admin 取消某些（或全部）許可權來變更原則。

group iv-admin

這個群組代表管理者群組。如同 cell_admin 一樣，這個群組的所有成員都會被預設原則視爲安全領域的管理者。所有預設的 ACL 會授與使用者 cell_admin 及群組 iv-admin 完全相同的許可權。

您可以將使用者新增至 iv-admin 群組，就能輕易地將使用者安置成管理角色。請注意，這個程序具有某種程度的危險性。當使用者變成這個群組的成員時，這個使用者就具備預設的 ACL。有了預設的 ACL，使用者現在就有權對整個名稱空間中的任何物件執行任何動作。

這個群組的預設原則可以改變。例如，您可以將管理許可權指定給其他使用者，來變更預設的原則。或者，您可以從 iv-admin 取消部分或全部的管理許可權來變更預設原則。

group ivmgrd-servers

這個群組包含「管理」伺服器。目前，Policy Director 需要安全領域中剛好有一個「管理」伺服器存在。因此，這個群組只包含這一個項目。

主控台大部分的管理要求都是利用「管理」伺服器來對目標 Policy Director 伺服器執行。由於這個處理程序，「管理」伺服器必須具備在目標伺服器上執行要求的許可權。因此，這個群組會被授與在預設管理 ACL 中的伺服器管理（s）許可權，以及整個 Web 空間的清單（l）許可權。

group webseal-servers

這個群組包含安全領域中的所有 WebSEAL 伺服器。預設的 WebSEAL ACL 會授與這些伺服器完整的 HTTP 特定許可權及指定許可權集。這個原則可讓所有的 WebSEAL 伺服器接合到所有其他的 WebSEAL 伺服器。您可以修改這個原則，以便根據伺服器對伺服器的基礎來授與這些許可權。

建立管理使用者

有了 Policy Director，您可以建立具有不同程度責任的管理帳戶。責任是透過策略性的安置管理 ACL 來指定。以下的清單說明了可能的管理角色：

ACL 管理責任

ACL 管理者可控制整個或部份的受保護物件名稱空間範圍（此視管理 ACL 所在的位置而定）。管理者的 ACL 項目可以包含 b、a 及 T 等許可權，加上適用於對該範圍中物件所執行之作業的任何其他許可權。

管理者可以使用「管理主控台」來將 ACL 連接到指定名稱空間中的物件。管理者可以使用現存的 ACL 模版集。您可以使用連接（a）許可權來將連接 ACL。這個管理者沒有建立、變更或刪除 ACL 模版的許可權。

ACL 原則的責任

ACL 原則管理者應該負責控制所有在安全領域中使用的 ACL 模版的建立及修改。 ACL 原則管理者應該被授與對 /Management 或 /Management/ACL 物件的 d、b、m 及 v 許可權。

這個 ACL 原則管理者可以使用（m）許可權來建立新的 ACL 模版。身爲新模版的建立者，根據預設，管理者會變成新 ACL 模版中的第一個項目，並且具有 abcT 許可權。控制（c）許可權可有效地提供 ACL 的所有權給管理者，因此可以變更 ACL。

身爲 ACL 的擁有者，管理者可以使用在管理 ACL 中授與的刪除（d）許可權。 管理者使用這個許可權來將 ACL 從模版清單中移除。 除非您是該 ACL 的擁有者，否則您不能刪除 ACL 模版。

伺服器管理責任

此管理者會被授與對 /Management/Server 物件的 d、m、s 以及 v 許可權。這個管理者可以執行有關 Policy Director 伺服器的作業。

授權動作責任

這個管理者會被授與 /Management/Action 物件的（d）及（m）許可權。這個管理者可以建立或刪除所有爲協力廠商應用程式建立的許可權。

請參閱第86頁的『管理名稱空間』以取得管理名稱空間的其餘資訊。

管理 ACL 模版範例

以下範例說明使用者如何取得管理權利。

- /WebSEAL 的下列 ACL 會提供管理權利給 user adam：

```
user cell_admin                 abcTdmlrx
group iv-admin                  abcTdmlrx
group webseal-servers           gTdmlrx
group ivmgrd-servers            Tl
user adam                       abcTdmlrx
any-authenticated               Trx
unauthenticated                 Trx
```

- /NetSEAL 的下列 ACL 會提供管理權利給 user adam：

```
user cell_admin                                 abcTC
group iv-admin                                  abcTC
user adam                                       abcTC
any-authenticated                               TC
unauthenticated                                 TC
```

管理指定範例

較大的物件空間可能會要求管理使用者管理各種不同的子分支。在這個實務中，通往每一個分支的路徑目錄的 ACL 必須包含每一個帳戶的項目，並且具備遍訪許可權。 對於具備許多管理使用者的網站，這些 ACL 可能包含很長的項目清單，以代表所有的管理帳戶。

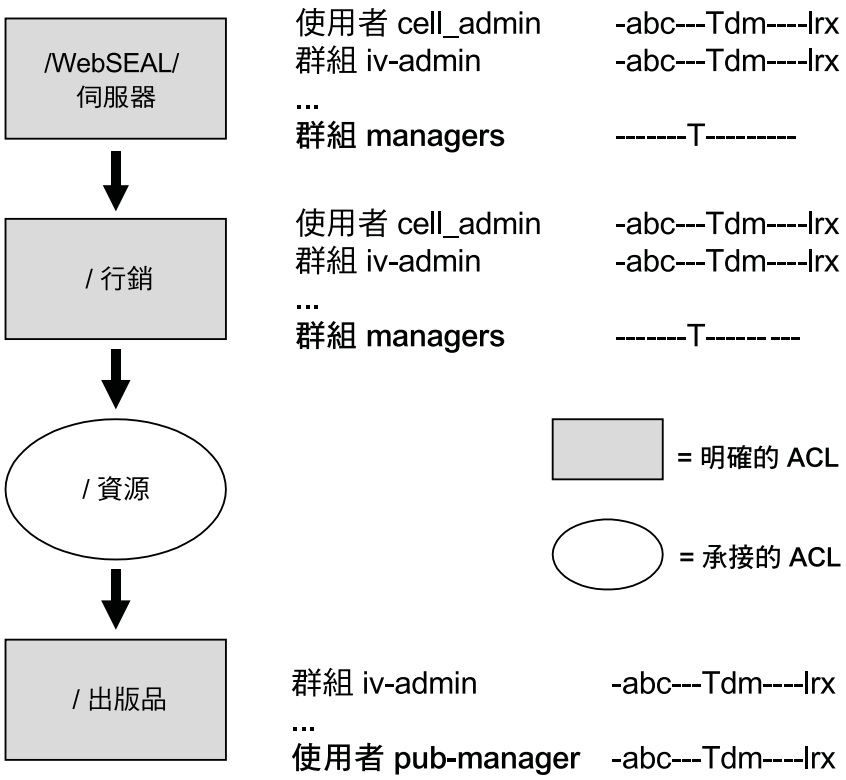
以下的技術可以爲管理者解決過多 ACL 項目的問題：

1. 建立一個管理群組帳戶。
2. 新增所有的新管理使用者至這個群組。
3. 將此群組當成一筆 ACL 項目（具備遍訪權）新增到每一個子分支前頭的目錄中，以及新增到需要管理委任的目錄中。
4. 在每一個分支根 ACL，新增適當的管理使用者項目（具有 b、c、T，加上其他適當的許可權）。
5. 管理者現在可以從根移除管理群組 ACL 項目（以及任何其他項目）。

   現在只有該使用者具備對根以及其下所有物件的控制權。

在以下的範例中，已經建立 managers 群組來包含所有的管理使用者。使用者 pub-manager 是這個群組的成員，因此具備瀏覽 Publications 目錄所需的遍訪許可權。

Publications 目錄將使用者 pub-manager 項目併入其 ACL 中。 pub-manager 是這個分支的指定管理者，並且具備適當的許可權。身爲指定的管理者，pub-manager 可以從 Publications ACL 移除 manager 群組帳戶（以及任何其他 ACL 項目）。藉由移除群組帳戶及任何其他 ACL 項目，指定的管理者可以對 Web 空間的分支取得完全控制。


/WebSEAL/
伺服器
/ 行銷
/ 資源
/ 出版品
使用者 cell_admin -abc---Tdm----lrx
群組 iv-admin -abc---Tdm----lrx
...
群組 managers -------T---------
使用者 cell_admin -abc---Tdm----lrx
群組 iv-admin -abc---Tdm----lrx
...
群組 managers -------T----------
= 明確的 ACL
= 承接的 ACL
群組 iv-admin -abc---Tdm----lrx
...
使用者 pub-manager -abc---Tdm----lrx

第8章 引用存取控制

在安全領域中，您可以透過原則模版的使用來保護資源。原則模版包含控制資源使用的許可權。您必須將原則模版連接到需要保護的資源的名稱空間物件表示法。

Policy Director 可以辨識以及使用稱爲 ACL 的原則模版類型。 ACL 是用來將組織的安全原則戳印到屬於安全領域的資源上。

本章討論管理物件空間以及引用存取控制所需的共同作業。

本章包括：

ACL 管理概觀

您可以使用「管理主控台」的 ACL 管理作業畫面來建立、變更及刪除 ACL 模版。

1. 以 ACL 管理者身份登入「管理主控台」，如 `cell_admin`。
2. 按一下 **ACL** 作業標籤。

   此時會出現 ACL 管理作業畫面。

ACL 管理作業的動作按鈕

您可以使用 **ACL** 動作按鈕來執行 ACL 管理作業。下表說明每一個動作按鈕所執行的作業：

動作按鈕	說明
新增 ACL	建立新的 ACL 模板。
新增項目	新增項目至選取的 ACL 模版。
儲存	儲存這個 ACL 模板。 ACL 會出現在「ACL 名稱」清單檢視畫面中。
刪除	刪除選取的 ACL 模板。
取得	擷取特別指定的 ACL 模版的相關資訊，並且輸入 ACL 明細檢視畫面。在「ACL 定義」區段的「ACL 名稱欄位中指定 ACL。
列出	復新清單檢視畫面。
使用處	顯示連接選取的 ACL 模版所在的受保護物件的完整清單。這個顯示畫面會出現在「主控台」的「公佈欄」區段中。

ACL 管理作業

您可以執行這些 ACL 管理作業的方式有：

- 建立新的 ACL 模板。
- 新增 ACL 項目。
- 編輯 ACL 項目的許可權。
- 刪除 ACL 模板。

建立新的 ACL 模板

如果要建立新的 ACL 模版，您可以從其中一個現存的預設 ACL 模版開始，然後將這個 ACL 變更成您要的規格。

1. 從 **ACL 名稱**清單中，拖曳您要使用的預設 ACL 模版圖示。然後您可以在「公佈欄」中使用模版來作爲新 ACL 的基礎。
2. 從 ACL 動作按鈕中，按一下**新增 ACL**。

   此時會清除「ACL 定義」區中的先前資訊，並且準備欄位給新的項目。

   根據預設，您的登入身份會變成第一個 ACL 項目，並且具有 abcT 許可權。 控制（c）許可權會提供您這個 ACL 的所有權。
3. 在 **ACL 名稱**欄位中鍵入 ACL 的名稱。
4. 按 Tab 鍵以跳至**說明**欄位，並且鍵入一個段落，說明這個 ACL 的目的（您將如何引用它）。
5. 將「公佈欄」中預設的 **ACL** 圖示拖曳到新的「ACL 定義」中的「ACL 項目」區域。

   新的 ACL 現在包含來自預設 ACL 的項目。
6. 對項目進行適當的修改。
7. 按一下**儲存**。

新增 ACL 項目

欲新增 ACL 項目：

1. 從 **ACL 名稱**清單中，選取一個 ACL 模版。
2. 按一下**新增項目**動作按鈕。

   「ACL 項目」區域會清除，並且自行重設以接受新的項目。
3. 在**類型**欄位中按住滑鼠按鈕。

   此時會出現一個下拉式功能表。
4. 選取使用者、群組、任何經身分驗證的或未經身份驗證類型。
5. 按一下 **ID** 欄位並鍵入適當的 ID。

   您也可以從**帳戶管理**檢視畫面來拖放使用者和群組圖示。按一下**帳戶**作業標籤，並且將**帳戶管理**檢視畫面移至「主控台」較低的畫面區域。
6. 使用許可權勾選框來將適當的許可權引用至這個項目。
7. 按一下**儲存**按鈕來對 ACL 確定這個項目。

編輯 ACL 項目的許可權

欲編輯 ACL 項目的許可權：

1. 在「ACL 定義」區中，選取項目。
2. 在「ACL 項目」區中，藉由選取或不選取許可權勾選框，來選取適當的許可權。
3. 按一下**儲存**按鈕來確定變更。

刪除 ACL 模版

如果要刪除 ACL 模板：

1. 從 **ACL 名稱**清單中，選取您要刪除的 ACL 模版。
2. 按一下**刪除**按鈕。

   此時會出現一個警告方塊。
3. 按一下**繼續**。

   「管理主控台」不會刪除仍然連接到物件的 ACL。 狀態列中會出現一則訊息，警告您發生這個情況。

範例：

您已經連接爲 `webtest` 群組成員所設計的 ACL。 `webtest` 群組是負責開發及測試新 HTML 網頁的小組。 在測試後，您可以移除這個明確的 ACL，使網頁可供安全領域其他成員使用。

建立新 ACL 模版的範例程序

如果要建立新的 ACL 模板：

1. 按一下**新增 ACL** 動作按鈕。

   此時會清除「ACL 定義」區中的先前資訊，並且準備欄位給新的項目。

   根據預設，您的登入身份會變成第一個 ACL 項目，並且具有 abcT 許可權。
2. 在 **ACL 名稱**欄位中鍵入 ACL 的名稱。
3. 按 Tab 鍵以跳至**說明**欄位，並且鍵入一個段落，說明這個 ACL 的目的（您將如何引用它）。
4. 按一下**儲存**按鈕來對「 ACL 清單」確定這個新 ACL。
5. 按一下**新增項目**按鈕。

   「ACL 項目」區域會清除，並且自行重設以接受新的項目。
6. 在**類型**欄位中按住滑鼠按鈕。

   此時會出現一個下拉式功能表。
7. 按一下 **unauthenticated**，並且不授與任何許可權。
8. 按一下**儲存**按鈕。

   項目會出現在「ACL 定義」區中。
9. 遵循相同的程序來新增不具備許可權的任何經身分驗證的項目。
10. 按一下**帳戶**作業標籤。

    「帳戶」管理畫面會變成最頂端的畫面。

11. 按一下**將作業往下移動**按鈕來將「帳戶」管理畫面置於「主控台」底端的部分。
12. 如果要建立新的群組項目，請按一下**新增項目**（ACL 畫面）。
13. 從「帳戶」畫面的**群組**清單中，將**群組**圖示拖放到「ACL 項目」區域的 **ID** 欄位。**類型**及 **ID** 欄位會填入適當的資訊。
14. 勾選適當的許可權。
15. 按一下**儲存**按鈕來對 ACL 確定這個項目。

物件空間管理概觀

您可以使用「管理主控台」的「物件空間」管理作業畫面，將 ACL 連接到物件，或是從後者移除 ACL。

1. 以具備 ACL 管理許可權的使用者身份登入「管理主控台」，如 `cell_admin`。
2. 按一下**物件空間**作業標籤。

   此時會出現「物件空間」管理作業畫面。

物件空間管理作業的動作按鈕

您可以使用**物件空間**動作按鈕來執行物件空間管理作業。下表說明每一個動作按鈕所執行的作業：

動作按鈕	說明
連接 ACL	指定 ACL 至物件。
移除 ACL	從物件移除 ACL。
尋找 ACL	尋找明確標記有特定 ACL 的所有物件。物件會清單在「主控台」底端的畫面中。
儲存 ACL	使用「編輯 ACL」檢視畫面時，可提供儲存對 ACL 的變更之能力。
列出	復新「物件空間」樹狀組織。

物件空間管理作業

您可以執行這些物件空間管理作業：

- 連接 ACL 至物件。
- 從物件移除明確的 ACL。

讓 ACL 連接物件

您必須具備適當的管理許可權來連接及移除 ACL。特別是，您必須具備連接（a）許可權來將 ACL 引用至物件，以及從物件移除 ACL。

1. 將 ACL 管理作業畫面置於「主控台」底端的區段。
2. 按一下「主控台」頂端畫面中的「物件空間」畫面。
3. 展開「物件空間」樹狀組織的適當範圍，並選取要連接明確的 ACL 所在的目標物件。
4. 從 **ACL 名稱**清單拖曳適當的 ACL 模版圖示，然後放置在「物件空間」樹狀組織的選取物件上。

移除物件中的明確 ACL

您必須具備適當的管理許可權來連接及移除 ACL。特別是，您必須具備連接（a）許可權來將 ACL 引用至物件，以及從物件移除 ACL。

1. 按一下**物件空間**作業標籤。
2. 展開「物件空間」樹狀組織的適當範圍，並選取目標物件以及連接的明確 ACL。
3. 按一下**移除 ACL** 按鈕。

第9章 管理 Proxy 使用者

IBM SecureWay FirstSecure (FirstSecure) 組的安全性產品之一是 IBM SecureWay Boundary Server for Windows NT 與 AIX (Boundary Server)。如果您的預設使用者登錄爲 LDAP，您可以在整合的 IBM Firewall 及 Policy Director Proxy 使用者解決方案中，結合使用 Policy Director 與 Boundary Server。

關於 FirstSecure 及其元件最新的資訊可在下列網站中取得：

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

簡介界限安全性

和 Policy Director 一樣，Boundary Server 是 IBM SecureWay FirstSecure 產品安全性套裝軟體提供的元件。或者，您可以個別地購買 Boundary Server 或 Policy Director，然後以獨立的產品方式執行它們--不需要購買完整的 FirstSecure 套裝軟體。

界限安全性不只保護您的網路、應用程式及資訊，它也延伸它們的觸角。適當的界限安全性需要您控制可以存取網路的人員及進入及離開網路的資訊。界限伺服器提供防火牆保護、內容安全性及 VPN。界限伺服器建立網際網路的界限，您可以使用此界限防阻可能有害的病毒、Java Script、Applet、ActiveX 控制、甚至垃圾電子郵件 (SPAM)。

有關 Boundary Server 的規劃、安裝、配置、使用與疑難排解，請參閱 IBM SecureWay Boundary Server 產品中隨附的 *IBM SecureWay Boundary Server 啓動與執行*書籍。

Boundary Server 是產品的套件。Boundary Server 將安全性產業的最佳生產技術帶入整合的解決方案。解決方案包括您可以選用購買的 IBM 支援及服務。

Boundary Server 的其中一個元件是 IBM SecureWay Firewall 版本 4.1 (防火牆)。

與 IBM Firewall 整合

*防火牆*的目的是要防止不想要或未授權的通信進入或流出安全的網路。防火牆作爲一個或多個安全內部專用網路及其它 (不安全) 網路或公用網際網路之間的障礙物。

IBM Firewall 是一個網路安全性的程式。IBM SecureWay Firewall 版本 4.1 包括這些新特性：

- 增強安全郵件 Proxy
- 增強 Socks 通信協定 (第 5 版)
- 遠端存取服務程式 (RAS)
- HTTP Proxy

HTTP Proxy 透過消除瀏覽 Web 的 sock 伺服器需求之 SecureWay Firewall 來處理瀏覽器要求。使用者可以存取網際網路上有用的資訊，而不需對它們的內部網路妥協，且不需要它們的從屬站環境施行 HTTP Proxy。

您必須先確定已安裝與配置必備需求，才能安裝 SecureWay Firewall。您也必須定義安全介面，確定並設定您的安全原則，及定義網路物件。 必須定義下列主要的網路物件：

- 防火牆的安全介面。

- 防火牆的非安全介面。
- 安全網路
- 您的安全網路上的每一個子網路。
- 您的「安全性動態」伺服器及您的 Windows NT 領域伺服器之主電腦物件，如果有的話。

完整的安裝及配置資訊可以在 Boundary Server 提供的 *IBM SecureWay Boundary Server 啓動與執行*一書中找到。

使用者類型說明

IBM Firewall 管理者負責爲 Proxy 使用者配置建立及變更定義，但他們不能建立或修改其他防火牆管理者的定義。

防火牆管理者執行這些管理作業：

- 新增使用者至 IBM Firewall，使他們可以從受保護的網路外存取主電腦。
- 變更存取防火牆使用者的屬性。
- 刪除不再從網路外存取的使用者。

就整合的 IBM Firewall 與 Policy Director 解決方案而言，此爲負責管理 Proxy 使用者的 Policy Director 管理者。

防火牆使用者

在安全網路內的使用者可以使用網路功能機制存取非安全網路 (如 Socks 或 Proxy)。如果您想要讓您的安全使用者使用非安全網路 (Proxy)，您需要配置並設定適當的連接，來使用此類流量。

進行那種服務是依您規劃階段作的決策而定。讓服務程式有效通常需要設定一些連接配置，以允許特定的流量類型。例如，若您要讓您的安全使用者以 HTTP Proxy 使用網際網路上的 Web，您不只需要在 Firewall 配置 HTTP Proxy 常駐程式，還需要設定允許 HTTP 流量。

若您需要像出埠 Web 存取功能的身份驗證，定義這些使用者至 IBM Firewall。

Proxy 使用者

Policy Director 管理可配置成將 Proxy 使用者當成 Policy Director 使用者的延伸來管理。就整合的 Policy Director 及 IBM Firewall 解決方案而言， Policy Director 管理者必須將使用者設定爲 Policy Director Proxy 使用者。

Proxy 使用者是使用防火牆服務程式 (HTTP Proxy 服務程式) ，來從公司網路內存取網際網路上網站的人員。 Proxy 使用者可以透過防火牆使用服務，但不能存取防火牆機器且不能執行本端登入至防火牆機器。

啓用 Proxy 使用者管理

在您可以進行 Proxy 使用者管理之前，必須啓用「管理主控台」上的此功能。如果要啓用「Proxy 使用者」能力，必須編輯 console.properties 檔。

您可以在下列處找到 console.properties 檔：

Windows： `C:\Program Files\IBM\IVConsole\console.properties`

UNIX： `/opt/intraverse/ivconsole/console.properties`

如果要設定 Proxy 使用者管理：

1. 使用文字編輯器，開啓 console.properties 檔。
2. 移除下列行開頭的註解符號 (#)：

   ```
   #6, ProxyUsersTaskView              = IV.ProxyUserTask.ProxyUsersTaskView
   ```

3. 重新啓動「管理主控台」，以啓用「Proxy 使用者」管理特性。

介紹 Proxy 使用者管理

對於 Policy Director，防火牆使用者就是 *Proxy 使用者*。Policy Director「管理主控台」可讓您管理 Proxy 使用者。

Policy Director 管理者執行這些管理作業：

- 新增使用者作爲 Proxy 使用者，使他們可以使用防火牆服務。
- 變更使用防火牆服務 Proxy 使用者的屬性。
- 刪除不再需要使用防火牆服務的 Proxy 使用者。

防火牆管理者應參照 IBM Firewall 文件，以取得更多執行這些管理作業方法的資訊。

使用 Proxy 使用者管理畫面

「使用者」管理作業畫面包含**使用者**樹狀檢視畫面及**Proxy 使用者** 明細檢視畫面。

使用 Proxy 使用者管理作業的動作按鈕

您可以使用 **Proxy 使用者**動作按鈕來執行 Proxy 使用者管理作業。下表說明每一個動作按鈕所執行的作業：

動作按鈕	說明
儲存	若在使用者樹狀檢視畫面選取 Policy Director 使用者，則建立新的 Proxy 使用者。或者，若在使用者樹狀檢視畫面選取現存的 Proxy 使用者，則變更現存的 Proxy 使用者。
刪除	移除選取的 Proxy 使用者

使用 Proxy 使用者明細欄位

下表說明「管理主控台」的**Proxy 使用者明細**檢視畫面中的欄位：

欄位	說明

Proxy 使用者	要指定將爲 Proxy 存取定義的使用者的名稱。這是將登入 IBM Firewall 的 TELNET 或 FTP 伺服器的使用者名稱。此使用者沒有管理權限。
Proxy 領域	指定防火牆 Proxy 領域的名稱。
密碼	指定用來登入防火牆 Proxy 領域的密碼。
說明	說明 Proxy 使用者的指定參考用資訊文字字串。說明只是一個選用性資料欄位，登錄並不會使用它。
遠端 Shell	指定針對 Proxy 使用者使用遠端登入 Shell。您可選擇：**/bin/restrict.sh**、**/bin/csh**、**/bin/ksh** **/bin/bsh**、**/bin/oneact.sh** 與空字串。
本端 Shell	指定針對 Proxy 使用者使用本端登入 Shell。您可選擇：**/bin/restrict.sh**、**/bin/csh**、**/bin/ksh** **/bin/bsh**、**/bin/oneact.sh** 與空字串。
預設群組	指定 Proxy 使用者所屬的預設群組。管理者可從顯示的群組清單中選取群組，讓 Proxy 使用者成爲其中的成員。
安全 FTP 身份驗證	指定此使用者需要使用安全網路的 FTP 存取防火牆的身份驗證層次。您可以選擇：**防火牆密碼**、**全部容許**、**全部拒絕**、**安全 ID 卡**、**NT 登入密碼**、**使用者提供之 1**、**使用者提供之 2**、**使用者提供之 3**、**AIX 登入密碼** 與空字串。
遠端 FTP 身份驗證	指定此使用者需要使用非安全網路的 FTP 存取防火牆的身份驗證層次。您可以選擇：**防火牆密碼**、**全部容許**、**全部拒絕**、**安全 ID 卡**、**NT 登入密碼**、**使用者提供之 1**、**使用者提供之 2**、**使用者提供之 3**、**AIX 登入密碼** 與空字串。
安全 Telnet 身份驗證	當從安全網路登入時，指示此使用者的身份，必須以某種方法身份驗證。您可以選擇：**防火牆密碼**、**全部容許**、**全部拒絕**、**安全 ID 卡**、**NT 登入密碼**、**使用者提供之 1**、**使用者提供之 2**、**使用者提供之 3**、**AIX 登入密碼** 與空字串。
遠端 Telnet 身份驗證	當從非安全網路登入時，指示此使用者的身份，必須以某種方法身份驗證。 您可以選擇：**防火牆密碼**、**全部容許**、**全部拒絕**、**安全 ID 卡**、**NT 登入密碼**、**使用者提供之 1**、**使用者提供之 2**、**使用者提供之 3**、**AIX 登入密碼** 與空字串。
安全 SOCK 身份驗證	指定 Socks (第 5 版) 對來自防火牆安全端 Socks 從屬站連線的身份驗證方法。您可以選擇：**防火牆密碼**、**全部容許**、**全部拒絕**、**安全 ID 卡**、**NT 登入密碼**、**使用者提供之 1**、**使用者提供之 2**、**使用者提供之 3**、**AIX 登入密碼** 與空字串。
遠端 SOCK 身份驗證	指定 Socks (第 5 版) 對來自防火牆非安全端 Socks 從屬站連線的身份驗證方法。您可以選擇：**防火牆密碼**、**全部容許**、**全部拒絕**、**安全 ID 卡**、**NT 登入密碼**、**使用者提供之 1**、**使用者提供之 2**、**使用者提供之 3**、**AIX 登入密碼** 與空字串。

安全 HTTP 身份驗證	指定出埠 HTTP Proxy 要求上，身份驗證的使用者 ID 及密碼配對類型。您可以選擇：**防火牆密碼**、**全部容許**、**全部拒絕**、**安全 ID 卡**、**NT 登入密碼**、**使用者提供之 1**、**使用者提供之 2**、**使用者提供之 3**、**AIX 登入密碼** 與空字串。
本端身份驗證	指定本端身份驗證方法。您可以選擇：**防火牆密碼**、**全部容許**、**全部拒絕**、**安全 ID 卡**、**NT 登入密碼**、**使用者提供之 1**、**使用者提供之 2**、**使用者提供之 3**、**AIX 登入密碼** 與空字串。
閒置切斷時間	指定切斷連接之前允許閒置時間。
警告切斷時間	指定切斷連接之前使用者允許警告次數。
密碼有效	指定是否使用者應被提示及要求輸入有效的密碼。IBM Firewall 將會提示此使用者的密碼。
密碼已鎖定	指定是否密碼已鎖定。管理者可將此欄位設爲 yes，避免使用者使用密碼身份驗證。

新增 Proxy 使用者

如果要建立 Proxy 使用者：

1. 按一下 **Proxy 使用者**作業標籤。
2. 展開適當的**使用者**樹範圍，並選取您要製作 Proxy 使用者的 Policy Director 使用者。
3. 填寫 **Proxy 使用者明細**檢視畫面中的欄位。
4. 按一下**儲存**按鈕。

變更 Proxy 使用者資訊

如果要變更 Proxy 使用者資訊：

1. 按一下 **Proxy 使用者**作業標籤。
2. 展開適當的**使用者**樹狀檢視畫面範圍，並選取清單中現存的 Proxy 使用者。「Proxy 使用者明細」區域會輸入現行資料。
3. 輸入新的資料。
4. 按一下**儲存**按鈕。

移除 Proxy 使用者

如果要刪除 Proxy 使用者：

1. 按一下 **Proxy 使用者**作業標籤。
2. 展開適當的**使用者**樹狀檢視畫面範圍，並選取現存的 Proxy 使用者。
3. 按一下**刪除**按鈕。

使用 ivadmin policy 指令來管理 Proxy 使用者

特定的**ivadmin policy** 指令只對 Policy Director Proxy 使用者使用。這些 **ivadmin policy** 指令爲一組管理指令，用以控制 Policy Director 使用者與 Proxy 使用者的一般原則資訊。管理者可以管理下列的原則屬性：

- 『管理登入原則』.
- 『管理密碼原則』

*原則*定義使用者帳戶及密碼的限制設定，以增進系統的整體安全性。這些限制可以一般強制 (對系統中每個使用者) 或指定強制 (僅對指定的使用者)。如果使用者引用特定的原則，此特定的原則優先於任何定義的一般原則。優先引用的原則，不管是否爲特定的原則，多少會限制一般原則。

管理登入原則

下列的 **ivadmin policy** 指令可以讓 IBM SecureWay Boundary Server 管理者管理與登入相關的原則。

使用與登入相關的**原則**管理作業，建立新的登入原則。這些原則引用至全部的使用者。

對於與登入相關的原則，當參照**原則**管理作業指令時，Policy Director 定義相對時間爲 DDD-hh:mm:ss，並定義絕對時間爲 YYYY-MM-DD-hh:mm:ss。

指令	說明
policy {set | get} disable-time-interval [*number*]	

	指出一旦抵達失敗登入重試次數上限後，經過多久即應停用帳戶（以秒爲單位）。
	
	number 引數爲帳戶應停用之秒數。
	
	例如：
	
	`ivadmin> policy set disable-time-interval 3`
	
	或：
	
	`ivadmin> policy get disable-time-interval`

policy {set | get} max-login-failures [*number*]	

	對允許試圖登入失敗的最大數值，建立新的原則或顯示現存的原則。
	number 引數是允許試圖登入的最大數值。
	
	例如：
	
	`ivadmin> policy set max-login-failures 5`
	
	或：
	
	`ivadmin> policy get max-login-failures`

管理密碼原則

下列的 **ivadmin policy** 指令可以讓 IBM SecureWay Boundary Server 管理者管理密碼的原則。

對於與密碼相關的原則，當參照**原則**管理作業指令時，Policy Director 定義相對時間爲 DDD-hh:mm:ss。

指令	說明
policy {set | get} max-password-age [*relative-time*]	

	在密碼必須變更之前，管理控制最大時間的原則。*relative-time* 引數是指定的時間--以日、小時及分鐘表示，格示如下：`DDD-hh:mm:ss`
	
	例如：
	`ivadmin> policy set max-password-age 031-08:30:00`
	
	或：
	`ivadmin> policy get max-password-age`

policy {set | get} max-password-repeated-chars [*number*]	

	指定使用者密碼中可以依序重複最大字元值。
	
	例如：
	`ivadmin> policy set max-password-repeated-chars 3`
	
	如按本例採用 3 個重複字元（此爲上限），則 `deptfff` 密碼可設爲密碼，這是因爲其中的重複字元 “f” 並未超過 3 個。而密碼 `deptffff` 則無法設爲密碼，因爲 4 個 “f” 字元已超過 3 個重複字元上限。
	
	或：
	`ivadmin> policy get max-password-repeated-chars`

policy {set | get} min-password-alphas [*number*]	

	指定使用者密碼中必須至少使用多少個英文字母字元。
	
	例如：
	`ivadmin> policy set min-password-alphas 5`
	
	若按本範例，則密碼至少得含 5 個英文字母字元。
	
	或：
	`ivadmin> policy get min-password-alphas`

policy {set | get} min-password-non-alphas [*number*]	

	指定必須使用作爲使用者密碼的最小非 alpha 字元值。
	
	例如：
	`ivadmin> policy set min-password-non-alphas 1`
	
	使用此範例，密碼必須最少含有五個非 alpha 字元才有效。
	
	或：
	`ivadmin> policy get min-password-non-alphas`

policy {set | get} min-password-different-chars [*number*]	

	指定必須使用作爲使用者密碼的不同字元最小值。
	
	例如：
	
	`ivadmin> policy set min-password-different-chars 3`
	
	使用此範例，密碼必須最少含有三個不同字元才有效。 若指定的密碼爲 ddddyyyy，密碼爲無效，因爲它只含有二個不同的字元 (d 和 y)。
	
	或：
	
	`ivadmin> policy get min-password-different-chars`

policy {set | get} min-password-length [*number*]	

	指定密碼的最小長度 (以字元計)。*number* 引數爲密碼允許的最小長度。
	
	例如：
	
	`ivadmin> policy set min-password-length 8`
	
	或：
	
	`ivadmin> policy get min-password-length`

policy {set | get} min-password-reuse-num [*number*]	

	指定先前已使用的密碼可以重新使用之前，密碼必須變更的次數。
	
	例如：
	
	`ivadmin> policy set min-password-reuse-num 3`
	
	或：
	
	`ivadmin> policy get min-password-reuse-num`

policy {set | get} min-password-reuse-time [*relative-time*]	

	指定密碼可以重覆使用之前，必須經過的最小時間值。
	
	relative-time 引數是時間的最小值，以日、小時及分鐘表示，格示如 (DDD-hh:mm:ss)。使用者不能在指定的時間限制之內重新使用相同的密碼 (例如，60 天或 060-00:00:00)。
	
	例如：
	
	`ivadmin> policy set min-password-reuse-time 060-00:00:00`
	
	或：
	
	`ivadmin> policy get min-password-reuse-time`

policy {set | get} password-expiry-date [*relative-time*]	

	指定密碼到期的日期和時間。
	
	例如：
	
	`ivadmin> policy set password-expiry-date 031-08:30:00`
	
	或：
	
	`ivadmin> policy get password-expiry-date`

policy {set | get} password-expiry-warn [*number*]	

	警告使用者密碼將要到期。*number* 引數是到期日期之前開始警告的日數 (例如，還有四天密碼就要到期)。
	
	例如：
	
	`ivadmin> policy set password-expiry-warn 4`
	
	或：
	
	`ivadmin> policy get password-expiry-warn`

第10章 管理 Policy Director 伺服器

本章包括管理及配置 Policy Director 伺服器組的一般作業。支援每一個伺服器的配置檔也一併在此討論。

本章包括：

Policy Director 伺服器簡介

Policy Director 伺服器是由以下的伺服器程序（常駐程式）所組成：

- 安全伺服器（secd）
- 安全管理程式（secmgrd）
- 權限伺服器（ivacld）
- 管理伺服器（ivmgrd）
- 目錄服務分配管理系統 (DSB)

在安裝產品期間，會自動配置這些伺服器。

Policy Director **「安全」伺服器 (secd)** 僅爲一種 DCE 伺服器。「安全」伺服器提供身份驗證服務。同時，「安全」伺服器會維護一個集中式登錄資料庫。使用者登錄可爲 LDAP 或 DCE，如果使用者登錄爲 DCE，此集中式登錄資料庫中可含有參與安全領域之所有有效使用者的帳戶資訊。

安全管理程式 (secmgrd) 包含 WebSEAL 及 NetSEAL 「安全」伺服器。

Policy Director**「權限」伺服器**（**ivacld**）服務程式權限會向任何以遠端模式使用「Policy Director 權限 API」的協力廠商應用程式進行要求。「權限」伺服器通常需要極少的管理或配置。

「管理」伺服器（**ivmgrd**）會管理主要的 ACL 資料庫，並且維護安全領域中的其他 WebSEAL 及 NetSEAL 伺服器的位置資訊。「管理」伺服器通常需要極少的管理或配置。

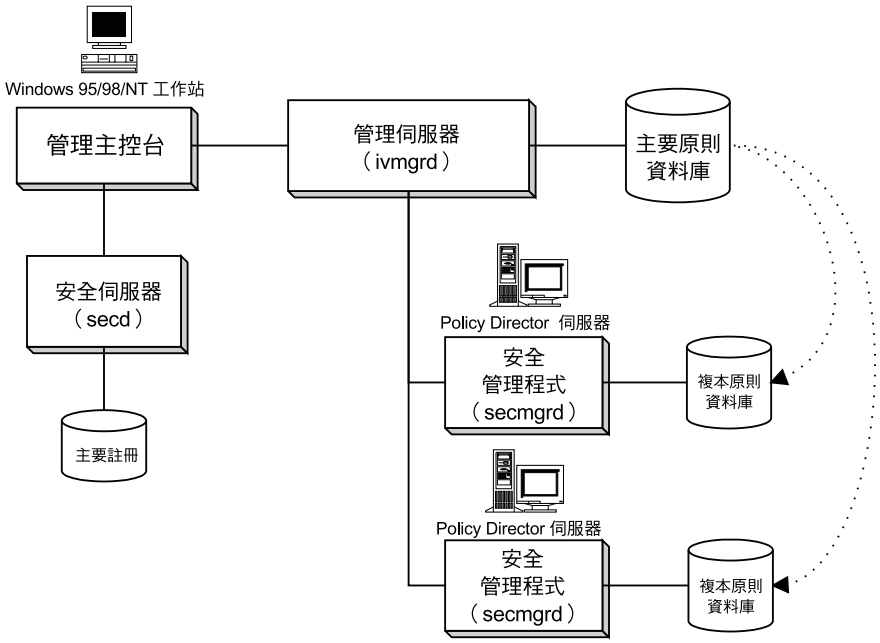
「目錄服務分配管理系統」（**DSB**）是作爲「管理伺服器」（ivmgrd）的一部分來分送。 在 Windows NT、Windows 95 或 Windows 98 工作站上執行時，「管理主控台」在安全領域中需要一個「目錄服務分配管理系統」。 在起始安裝之後，「目錄服務分配管理系統」通常不需要管理或配置。

伺服器相依關係

Policy Director 伺服器的相依關係包括：

- 任何安全領域中必須只有一個「管理」伺服器以其主要權限（ACL）資料庫案例。

- 「管理」伺服器會將其 ACL 資料庫複製到安全領域中的所有其他 Policy Director 伺服器。
- 具有 WebSEAL 及 NetSEAL 設陷的「安全管理程式」會常駐在每一個 Policy Director 伺服器上。
- 每一個「安全管理程式」會引用存取控制原則，而這些原則是根據複製的權限或 ACL 資料庫的資訊。



伺服器管理工具概觀

您可以透過以下的介面來執行伺服器管理：

- **ivadmin** 公用程式
- **wandmgr** 公用程式（限 WebSEAL）
- UNIX Script
- Windows NT 服務控制台

本章說明如何使用這些介面。

ivadmin、**wandmgr** 以及啓動 Script 都提供指令行介面。在 Shell Script 中自動化伺服器管理作業時，這些介面非常有用。

「管理主控台」、ivadmin 及 wandmgr 都可以從遠端或本端來使用。啓動 Script 必須從本端管理。

在尋找及更正問題時，指令行公用程式可以提供狀態資訊以及控制個別的伺服器。

ivadmin 公用程式

Policy Director 提供 **ivadmin** 指令行公用程式來完成更進階的伺服器作業。使用 **ivadmin** 來完成以下各項：

- 執行前一節列出的所有「管理主控台」作業

- 顯示伺服器狀態

wandmgr 公用程式

wandmgr 指令行公用程式是一個 Policy Director WebSEAL 工具，它是用來執行進階的 Web 從屬站授權及快取管理作業，例如：
- 顯示 Web 物件快取狀態。
- 從記憶體刪除 Web 物件快取。

UNIX Script

在系統啓動期間，Policy Director 使用 Script 來自動停止及啓動伺服器以及顯示伺服器狀態。 這些 Script 可以用手動方式啓動：
- 停止伺服器。
- 顯示伺服器狀態。
- 啓動伺服器。

Windows NT 服務控制台

使用 Windows NT 服務控制台：
- 啓動伺服器。
- 停止伺服器。
- 暫停伺服器。
- 繼續（回復）已暫停的伺服器。
- 列出已配置的伺服器。

伺服器配置檔

Policy Director 伺服器使用配置檔來指定功能：

伺服器名稱	程序	配置檔
安全管理程式	secmgrd	**UNIX**： /opt/intraverse/secmgr/lib/secmgrd.conf **Windows**： \Program Files\ibm\Policy Director\secmgr\lib\secmgrd.conf
管理伺服器	ivmgrd	**UNIX**： /opt/intraverse/ivmgrd/lib/ivmgrd.conf **Windows**： \Program Files\ibm\Policy Director\ivmgrd\lib\ivmgrd.conf
權限伺服器	ivacld	**UNIX**： /opt/intraverse/ivacld/lib/ivacld.conf **Windows**： \Program Files\ibm\Policy Director\ivacld\lib\ivacld.conf

配置檔是根據「美國國家標準交換碼」（ASCII），並且可以用常用的編輯程式來加以編輯。檔案登錄的格式如下：

```
parameter=value
```

Policy Director 伺服器的起始設定安裝會爲大部分的參數設定預設值。某些參數是靜態的，從來不會改變；您可以調整或新增其他的參數，以便配置伺服器功能及最佳化效能。

註: 在編輯配置檔後，您必須先停止並重新啓動 Policy Director 伺服器，才能使變更生效。

每一個檔案都包含許多區段（或**段落**），並且爲特定配置種類提供許多設定。段落標籤會出現在方括弧（[]）中。

例如，iv.conf 中的 [intraverse] 段落定義了一般的 Policy Director 配置設定，它們適用於整個安全領域。段落 [wand-mime-types] 定義了本端系統上的 Policy Director WebSEAL 所支援的 MIME-type 定義。

這些檔案都已加上註解，以說明每一個參數的用法。若您必須變更任何配置設定時，請小心編輯檔案，以確保它們的完整性。

UNIX：停止及啓動 Policy Director 伺服器

啓動及停止伺服器程序通常是透過在系統啓動及關機時執行的自動化 Script 來完成。

管理者也可以利用 Script 來以手動方式啓動及停止伺服器程序。在自訂安裝或尋找及更正問題時，這個技巧非常有用。您只能將 Script 引用至本端機器。使用「管理主控台」或 **ivadmin** 公用程式來從遠端停止及啓動伺服器。

您可以一次啓動及停止所有的 Policy Director 伺服器，或是一次一個將它們個別停止。一般而言，您必須以正確的次序來停止及啓動伺服器。

當代替 NetSEAT 從屬站來處理「Cell 目錄服務程式 (CDS)」要求時，需用到「目錄服務分配管理系統」。（Windows 版的「管理主控台」使用 NetSEAT 從屬站。）

使用 iv Script 來停止

使用 iv Script 來以正確的次序停止特定機器上的所有 Policy Director 伺服器：

AIX：

```
# /etc/iv/iv stop
```

Solaris：

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

這個 Script 只會以下列次序來停止伺服器：ivacld、secmgrd 及 ivmgrd。 Script 會等待所有的伺服器停止後，才會傳回提示。

手動關機

您也可以利用 **kill** 指令，將伺服器個別停止：

```
# kill <pid>          強制伺服器完全關機。
# kill -9 <pid>       突然終止伺服器，不進行任何清除。
```

以下列次序將 Policy Director 伺服器關機：

1. 目錄服務分配管理系統 (DSB)
2. 權限伺服器（ivacld）
3. 安全管理程式（secmgrd）
4. 管理伺服器（ivmgrd）

使用 iv Script 來啓動伺服器

使用 iv Script 來以正確的次序啓動特定機器上的所有 Policy Director 伺服器：

AIX：

```
# /etc/iv/iv start
```

Solaris：

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

這個 Script 只會以下列次序啓動伺服器：ivmgrd、secmgrd 及 ivacld。 Script 會等待所有的伺服器啓動後，才會傳回提示。

手動啓動

您可以直接啓動伺服器，以手動方式個別啓動伺服器。伺服器會自行起始設定。如果順利完成，伺服器會自行常駐。

您必須以管理使用者的身份執行啓動指令，例如 root 或 ivmgr。以下列次序來啓動 Policy Director 伺服器：

1. 管理伺服器（ivmgrd）：

   ```
   # /opt/intraverse/ivmgrd/bin/ivmgrd
   ```

2. 安全管理程式（secmgrd）：

   ```
   # /opt/intraverse/secmgr/bin/secmgrd
   ```

3. 權限伺服器（ivacld）：

   ```
   # /opt/intraverse/ivacld/bin/ivacld
   ```

4. 目錄服務分配管理系統 (DSB)：

   ```
   # /opt/intraverse/broker/bin/dsb
   ```

顯示伺服器狀態

如果要檢查伺服器是否正在執行，請使用以下指令：

AIX：

```
# /etc/iv/iv status
```

Solaris：

```
# /etc/init.d/iv status
```

```
DCE 伺服器：
伺服器                    已啓用                  執行中
dced                      是                      是
secd                      -                       是
cdsd                      -                       是
```

```
dtsd                            -                       是
dsb                             -                       是

Policy Director 伺服器：
伺服器                          已啓用                  執行中
ivmgrd                          是                      是
secmgrd                         是                      是
ivacld                          是                      是
```

Windows：停止及啓動 Policy Director 伺服器

使用 Windows NT 服務控制台，以手動方式啓動及停止伺服器程序。在自訂安裝或尋找及更正問題時，這可能非常有用。 您必須具備管理專用權，才能使用這個公用程式。

您可以一次啓動及停止所有的 Policy Director 伺服器，或是一次一個將它們個別停止。通常您必須以正確的次序來停止及啓動伺服器。

每當您重新啓動（重新開機）系統時， Policy Director 自動啓動服務程式會自動啓動每一個 Policy Director 伺服器。在伺服器啓動後，「自動啓動服務程式」會結束。

使用 Windows NT 服務控制台，手動啓動及停止個別的 Policy Director 伺服器：

1. 開啓 Windows 控制台。
2. 按兩下**服務**圖示。

   「服務」對話框會出現。 您會看到的服務的範例包括：

   ```
   服務程式                                 狀態          啓動
   目錄服務分配管理系統                     啓動          自動
   Policy Director 權限伺服器               啓動          手動
   Policy Director 自動啓動服務程式         啓動          自動
   Policy Director 管理伺服器               啓動          手動
   Policy Director 安全管理程式             啓動          手動
   Policy Director X.509 權限伺服器         啓動          手動
   ```
3. 根據步驟 4 及 5 中指示的順序，從清單框中選取 Policy Director 伺服器。
4. 以下列次序來停止伺服器：
   - 安全管理程式
   - 管理伺服器
   - 目錄服務分配管理系統
5. 以下列次序來啓動伺服器：
   - 目錄服務分配管理系統
   - 管理伺服器
   - 安全管理程式
   - 權限伺服器
6. 從方框的右手邊，按一下適當的控制選項按鈕（**起始**、**停止**、**啓動**）。
7. 如果要防止 Policy Director「自動啓動服務程式」自動啓動 Policy Director 伺服器，請使用**啓動**選項按鈕。這個按鈕會將 Policy Director 伺服器設定成停用。

啓動時自動化伺服器的啓動

iv.conf 配置檔的 [intraverse] 段落包含自動化（或不自動化）伺服器啓動的參數。

當您安裝時，可以將「安全」伺服器常駐程式（secmgrd）配置成每次重新啓動系統後即自動啓動。

```
[intraverse]
boot-start-secmgrd = yes
```

如果要防止 secmgrd 自動啓動，請設定：

```
boot-start-secmgrd = no
```

當您安裝 IVMgr 套裝軟體時，Policy Director「管理」伺服器常駐程式 （ivmgrd）會在每次重新啓動系統後自動啓動。

```
[intraverse]
boot-start-ivmgrd = yes
```

如果要防止 ivmgrd 自動啓動，請設定：

```
boot-start-ivmgrd = no
```

註: 每一個安全領域（Cell）都剛好需要一個 Policy Director「管理」伺服器常駐程式。請勿在一部以上的伺服器上，對每一個 Cell 安裝及執行 **ivmgrd**。

當您安裝 IVAcld 套裝軟體時，Policy Director「授權」伺服器常駐程式會在每次重新啓動系統後自動啓動。

```
[intraverse]
boot-start-ivacld = yes
```

如果要防止 **ivacld** 自動啓動，請設定：

```
boot-start-ivacld = no
```

配置 RPC 工作者緒

已配置的工作者緒數目會指定伺服器可服務的並行進入要求數目。當所有的工作者緒都在忙碌時， Policy Director 會將其他抵達的連線置於緩衝區中，直到有工作者緒可用爲止。

您可以設定可提供服務給進入連線的緒數目。請小心配置工作者緒的數目，因爲可能會對效能產生影響。

配置參數不會對同時連線的數目強制上限。這些參數僅指定服務無限制的工作佇列時可用的緒數目。

爲了選擇最佳的工作者緒數目，您必須瞭解您網路流量的數量及類型。

藉由增加工作者緒的數目，完成要求所需的平均時間會減少。然而，增加工作者緒的數目會增加伺服器負擔，導致提供服務給要求的平均時間再度增加。

secmgrd、ivmgrd 及 ivacld 伺服器的每一個配置檔都包含以下的參數，以便配置 RPC 工作者緒：

- RPC 工作者緒的最大值
- 接收進入 RPC 的 TCP 埠
- 接收進入 RPC 的「使用者資料圖通信協定」（UDP）埠

伺服器名稱	程序	配置檔
安全管理程式	**secmgrd**	secmgrd.conf
管理伺服器	**ivmgrd**	ivmgrd.conf
權限伺服器	**ivacld**	ivacld.conf

設定 RPC 工作者緒儲存池

Policy Director 伺服器使用 RPC 工作者緒來處理以下各項：

- 自 NetSEAT 從屬站進入的 RPC 要求
- 從「管理主控台」執行的管理作業所產生的資料庫更新

RPC 工作者緒參數的最大值（位於每一個伺服器配置檔中）包含以下的預設值：

```
max-rpc-worker-threads = 10
```

當 Policy Director 伺服器處理大量的 NetSEAT 從屬站時，請考慮增加這個值。

配置伺服器以處理進入的 RPC 要求

下表列出每一個伺服器用於 RPC 接收的預設埠值：

伺服器	配置檔	具有預設值的埠參數
secmgrd	secmgrd.conf	`rpc-tcp-port = 6052 rpc-udp-port = 0`
ivmgrd	ivmgrd.conf	`tcp-rpc-port = 6032 udp-rpc-port = 0`
ivacld	ivacld.conf	`tcp-rpc-port = 6031 udp-rpc-port = 0`

零（0）的埠值會停用該埠的 RPC 接收。建議您使用 TCP 監聽。只有非常必要時，才啓動 UDP 埠。

您可以視需要來設定不同的埠，

secmgrd 的範例：

```
rpc-udp-port = 6052
```

TCP 及 UDP 現在是在相同的埠上接收。

第11章 管理權限服務程式

「Policy Director 權限服務程式」可藉由控制授權決策進行的程序，強制執行網路的安全原則。 您可以有一些方法延伸 Polic Director 授權功能：定義並納入附加的名稱空間，定義新的存取控制許可權，及適應協力廠商的*外部權限服務程式*。本章討論需要配置、維護及延伸 Policy Director 權限服務程式的作業。

本章包括：

定義協力廠商應用程式名稱空間

這些要素定義 Policy Director 安全原則：

- 誰被允許參與安全領域？
- 必須受保護的的物件是什麼？
- 什麼規則必須保護那些物件？

Policy Director 受保護的物件名稱空間是屬於安全領域的的資源的邏輯與階層式呈現。在名稱空間中的物件代表受保護的系統資源 (如檔案及埠)。如果要保護任何安全領域中的資源，請您連接原則模板 (ACL) 至那些資源的物件代表。

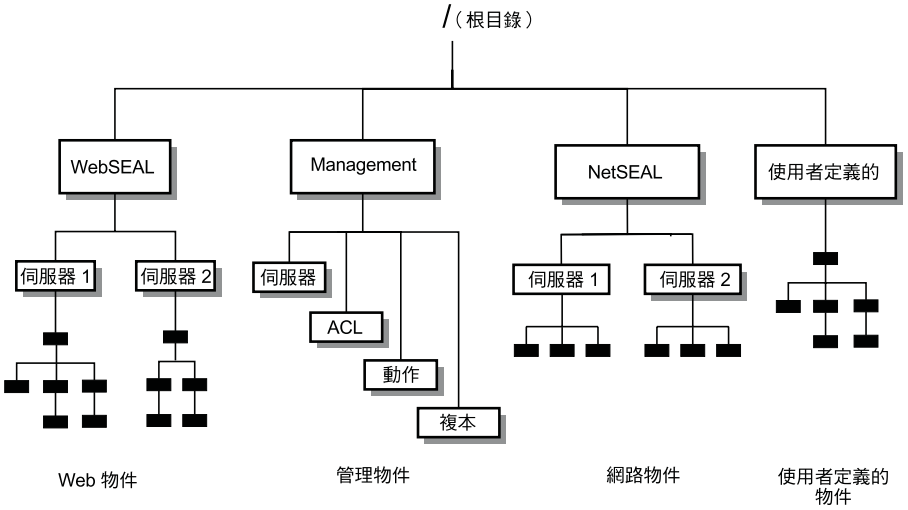
受保護的物件名稱空間使用兩種物件類型：

配置區物件

配置區物件是結構性的指定，可讓您以階層方式將名稱空間組織成區分功能範圍。配置區物件包含資源物件。

資源物件

資源物件是您安全領域中實際系統資源的表示法（如服務程式、檔案及程式）。



Policy Director 可讓您延伸其權限服務程式至屬於協力廠商名稱空間的物件。整合協力廠商名稱空間與 Policy Director 需要這些步驟：

- 對 Policy Director 說明協力廠商應用程式的名稱空間。
- 引用原則模板 (ACL) 至任何需要保護的名稱空間物件。

您透過特殊的對映檔案，對 Policy Director 說明協力廠商名稱空間的內容。這些檔案清單屬於協力廠商名稱空間特定的資源物件，並指示它的階層式關係。

另外，您必須定義保留此協力廠商名稱空間的根配置區物件。當名稱空間由「管理主控台」(物件空間標籤) 顯示時，根配置區物件名稱會出現，作爲 Policy Director 名稱空間的一部份。現存的標準 Policy Director 配置區物件包括 /WebSEAL、/NetSEAL 及 /Management。

管理伺服器配置檔 (ivmgrd.conf) 定義協力廠商配置區物件的名稱及對映檔的位置。

根配置區物件名稱及對映檔位置

「管理」伺服器配置檔 (ivmgrd.conf) 的[object-spaces] 段落定義這兩個項目：

- 物件協力廠商的根配置區物件名稱。
- 對映檔的位置。

每一個項目有下列格式：

object-space-root = map-file

其中：

object-space-root	保留協力廠商名稱空間的配置區物件名稱。
map-file	對映檔的完整路徑名稱。對映檔可以位在任意處。

下列範例定義協力廠商配置區物件 (附註) 及對映檔(notemap.txt) 位置：

UNIX: `/Notes = /opt/intraverse/lib/notemap.txt`

Windows： `/Notes = C:\Program Files\IBM\Policy Director\lib\notemap.txt`

註: 您必須停止並重新啓動「管理」伺服器，以納入任何 ivmgrd.conf 檔的編輯。

對映檔格式

說明協力廠商名稱空間爲 ASCII 文字檔的對映檔。檔案中的每一行是代表名稱空間中每一個資源物件的絕對路徑名稱。對映檔僅清單資源物件；Policy Director 表示路徑名稱的配置區物件。

其它的對映檔規則包括：

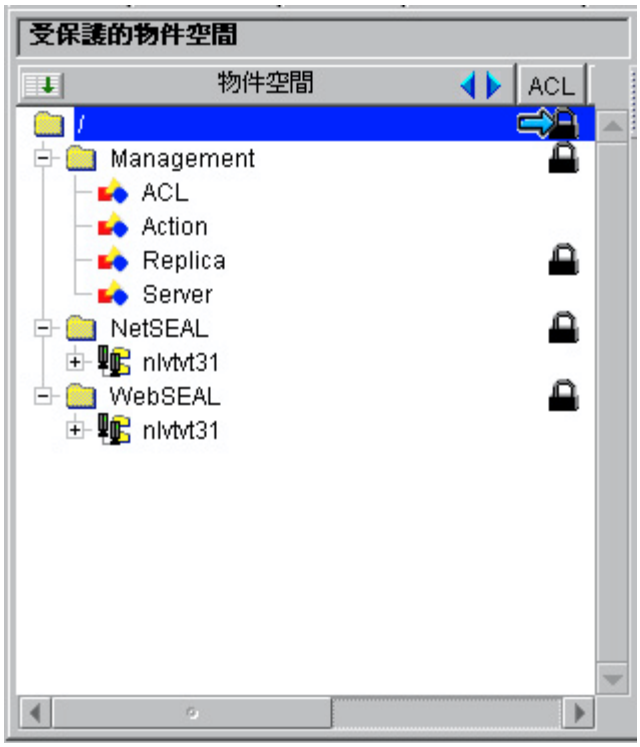
- 僅清單一個物件及每行的路徑名稱。
- 物件路徑名稱恆以斜線 (/) 開始。

範例對映檔：

```
/Forum/public/mail
/Forum/public/reference
/Forum/public/chat
/Forum/documents/style
/Forum/documents/guide
/Forum/documents/manual
/Forum/private/mail
/Forum/private/notes
/Forum/private/bulletins
```

「管理主控台」的階層式顯示

下列的「管理主控台」顯示說明於 『對映檔格式』 中，範例對映檔的結果。



定義自訂 ACL 許可權

Policy Director 依原則模板指定對受保護物件執行作業時所需的條件。 Policy Director 使用特定的原則模板類型，也就是存取控制清單 (ACL)。

ACL 項目

您可以連接 ACL 至物件。當連接時，ACL 中的項目指定 Policy Director 允許此物件的那個作業，及誰可以執行那些作業。ACL 項目包括：

- 使用者類型或群組類型

  未經身份驗證及皆經身份驗證使用者也有類型。
- 唯一的使用者識別或群組識別
- 許可權

許可權

Policy Director 使用包含大範圍作業的許可權標準集。單一可列印 ASCII 字元代表許可權。在「管理主控台」 (**ACL** 標籤)，Policy Director 以說明其支配作業的標籤，顯示每一個許可權。另外，Policy Director 依照它們在特定名稱空間中的使用，或整個名稱空間的使用， 將 ACL 群組在一起。群組種類範例包括：基本、同屬、WebSEAL、NetSEAL。

物件上的作業

應用軟體通常包含一個或以上受保護物件執行的作業。這些應用程式在要求作業允許進行之前，呼叫權限服務程式。此呼叫是要使用 Policy Director 及協力廠商應用程式的 Policy Director 權限 API。

資訊包含在 保護物件的 ACL 中。權限服務程式使用資訊，以簡單的 yes/ no 回答問題：使用者 (群組) 此是否有要求物件的 "r" 許可權 (範例)？

特別注意，權限服務程式不知道關於需要讀取 (r) 許可權作業的任何事項。它只關心讀取 (r) 許可權的存在 (或不存在)。讀取 (r) 許可權在要求使用者或群組的 ACL 項目中。

此許可權是很有力的 Policy Director 權限服務程式功能。服務程式完全獨立於要求的作業之外，這就是它可以輕易延伸權限服務程式的優點至協力廠商應用程式的原因。

自訂許可權的基本要求

標準 Policy Director 許可權的整個功能都可用在協力廠商的應用程式。讓協力廠商應用程式可以使用 Policy Director 許可權。如果完成了，相關的作業應會非常接近一般 Policy Director 執行的實際的作業。例如，需要唯讀存取受保護的物件作業，應只使用讀取 (r) 許可權。

註: 協力廠商應用程式可以使用完全不相關作業的標準 Policy Director 許可權，它不需知道或關心其作業。但是，這會導致管理者必須在二個不同者使用相同許可權間區分的困難。

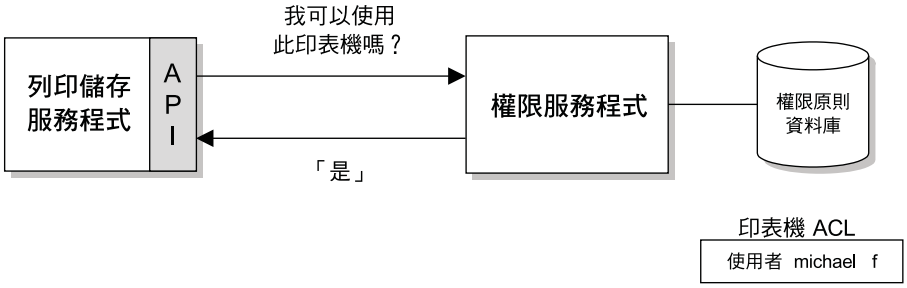
協力廠商應用程式會使用許可權標準集中未表示的作業。若使用了，Policy Director 會讓您定義新的許可權。這個應用程式使用這個權限服務程式辨識的許可權。

範例：

這個範例中基本要求是保護一些未經授權使用的印表機裝置。協力廠商列印排存作業服務程式已以 Policy Director 權限 API 撰寫。這個列印排存作業服務程式會呼叫權限服務程式，依印表機要求執行 ACL 檢查。

標準的 Policy Director 許可權不包括保護印表機的許可權。範例中新建的列印許可權應會保護印表機。

ACL 現在已連接至印表機物件。若使用者要求使用受保護的印表機，該使用者的 ACL 項目中必須有列印許可權。如出現列印許可權，權限服務程式會傳回一則同意回應，並繼續進行列印作業。若權限服務程式找不到列印許可權，將不容許進行列印作業。



管理許可權

做爲 Policy Director 管理者，您可以下列方式來管理許可權：

- 新增自訂許可權
- 移除自訂許可權
- 檢視所有可用的許可權

建立自訂許可權

您使用 **ivadmin action** 指令來建立、刪除及清單新的許可權。您必須以 Policy Director 管理者身份登入，才能使用 **ivadmin** 公用程式。

使用下列指令語法來建立新的自訂許可權：

```
ivadmin> action create name description action-type
```

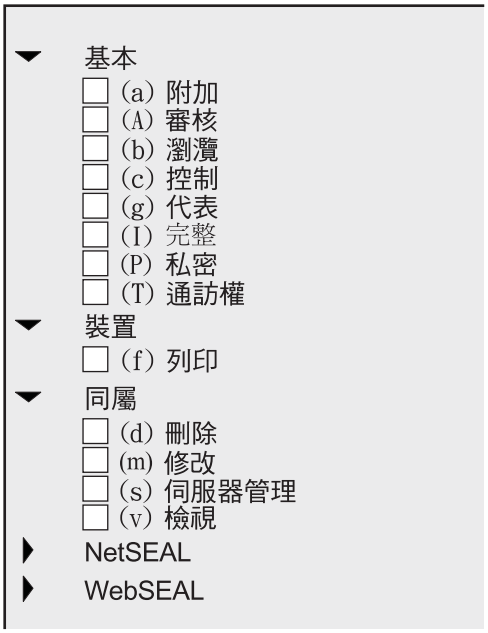
其中：

名稱	代表許可權的可列印 ASCII 字元。
說明	出現在「管理主控台」顯示畫面 (ACL 標籤) 中，字元右方的說明標籤。
action-type	出現在「管理主控台」顯示畫面 (ACL 標籤) 中，這個許可權的組織種類。

例如，鍵入：

```
ivadmin> action create f print Devices
```

在「管理主控台」的 ACL 管理中，產生這個新的項目。



刪除自訂許可權

使用下列指令語法來刪除自訂許可權：

```
ivadmin> action delete name
```

例如：

```
ivadmin> action delete f
```

清單全部可用的許可權

使用下列指令語法來清單全部可用的許可權：

```
ivadmin> action list
```

您會看到如下的許可權清單：

```
p "Proxy" NetSEAL
r "Read" WebSEAL
v "View" Generic
x "Execute" WebSEAL
A "Audit" Base
a "Attach" Base
b "Browse" Base
c "Control" Base
C "Connect" NetSEAL
d "Delete" Generic
f "Print" Devices
g "Delegation" Base
I "Integrity" Base
l "List Directory" WebSEAL
m "Modify" Generic
```

```
P "Privacy" Base
s "Server Admin" Generic
T "Traverse" Base
...
```

定義外部權限服務程式

*外部權限服務程式*可讓您強制執行其它授權控制及條件，來補充標準 Policy Director 授權程序。分別的權限伺服器程式指定這些外加的控制及條件。

「Policy Director 權限服務程式」會自動建置一個外部授權功能。如果您配置一個外部權限服務程式， 「Policy Director 權限服務程式」只會將新的控制及條件納入其評估程序。

設定外部權限服務程式需要這些一般步驟：

1. 撰寫一個伺服器程式，以便在授權決策期間參照。

   請參閱*Policy Director 程式設計及參考手冊*。

2. 將外部權限服務程式登錄到 Policy Director。

   參照 『登錄外部權限服務程式』。

在登錄服務程式之後，代表此服務程式的新許可權會出現在「Policy Director 管理主控台」中。 您現在可以在任何 ACL 項目中使用這個許可權。

當 Policy Director 在授權檢查期間發現許可權時，會參照外部權限服務程式以進行其他的授權決策。

進一步的背景資訊，請參照 第46頁的『外部授權功能』。

登錄外部權限服務程式

使用 **ivadmin server register** 指令，通知 Policy Director 權限服務程式，關於外部權限服務程式的存在及位置。

引用下列語法：

```
ivadmin> server register externauth server-name ns-location server-principal
         action-char action-name
```

其中：

server-name	這個外部權限服務程式的名稱 (或標籤)。這是出現在「管理主控台」上及 ivadmin server list 指令中，物件空間顯示畫面的名稱。
ns-location	在外部權限伺服器匯出其 RPC 連結的 CDS 名稱空間中的 RPC 項目。
server-principal	外部權限伺服器程序的 LDAP 名稱或 DCE Principal 名稱。
action-char	用在 ACL 的許可權字元，指定補充授權決策之外部權限服務程式的使用。
action-name	出現在「管理主控台」顯示畫面 (ACL 標籤) 中，字元右方的說明標籤。

此指令會產生預設的 ACL 組織種類，稱爲*外部授權*。當顯示 ACL 時，「管理主控台」使用預設的 ACL 組織種類。 全部登錄的外部權限服務程式的許可權出現在這個種類之下。

例如，鍵入：

```
ivadmin> server register externauth timechecker /.:/subsys/timechk
         t-checker k time-check
```

向名爲 timechecker 的外部權限伺服器登錄權限服務程式。在 timechecker 匯出其 RPC 連結的 CDS 名稱空間中的 RPC 項目，爲 /.:/subsys/timechk。伺服器的 DCE Principal 名稱是 t-checker。與這個服務程式相關的許可權是時間檢查 (k) 許可權。

這個出現在「管理主控台」的登錄的外部權限伺服器的許可權，類似如下：

基本
  (a) 附加
  (A) 審核
  (b) 瀏覽
  (c) 控制
  (g) 代表
  (I) 完整
  (P) 私密
  (T) 遍訪權
同屬
  (k) 時間檢查
同屬
  (d) 刪除
  (m) 修改
  (s) 伺服器管理
  (v) 檢視
NetSEAL
WebSEAL

刪除外部權限伺服器

使用 **ivadmin server delete** 指令，移除登錄的外部權限服務程式。引用下列語法：

```
ivadmin> server delete /ExternAuthzn/server-name
```

其中：

server-name	這個外部權限服務程式的名稱 (或標籤)。這是出現在「管理主控台」上，物件空間顯示畫面的名稱。

例如：

```
ivadmin> server delete /ExternAuthzn/timechecker
```

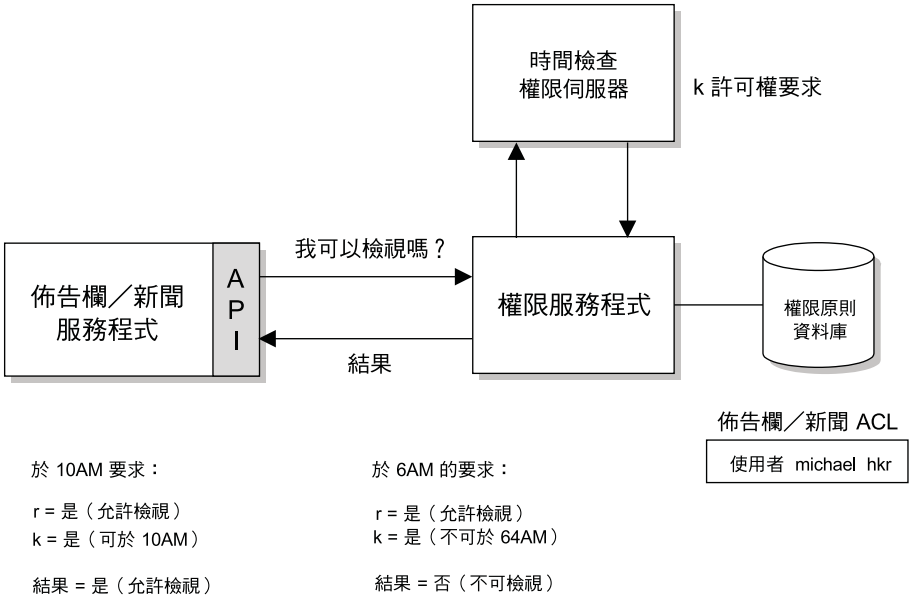
範例 1：

協力廠商公佈欄及新聞服務程式在作業上具有時間限制。使用者可以檢視由這個服務程式，僅在 8AM 到 5PM 之間提供的資訊。撰寫外部權限服務程式，來執行在公佈欄及新聞服務程式上，所作要求的時間檢查。

使用 **ivadmin** 指令來設定外部權限服務程式。

下圖說明授權處理程序的可能情形。使用者必須有讀取 (r) 許可權，才能檢視公佈欄及新聞資訊。新聞服務程式上的 ACL 也包括時間檢查 (k) 許可權。時間檢查 (k) 許可權指定 Policy Director 權限服務程式，它在最終決策中包括時間檢查器權限伺服器。

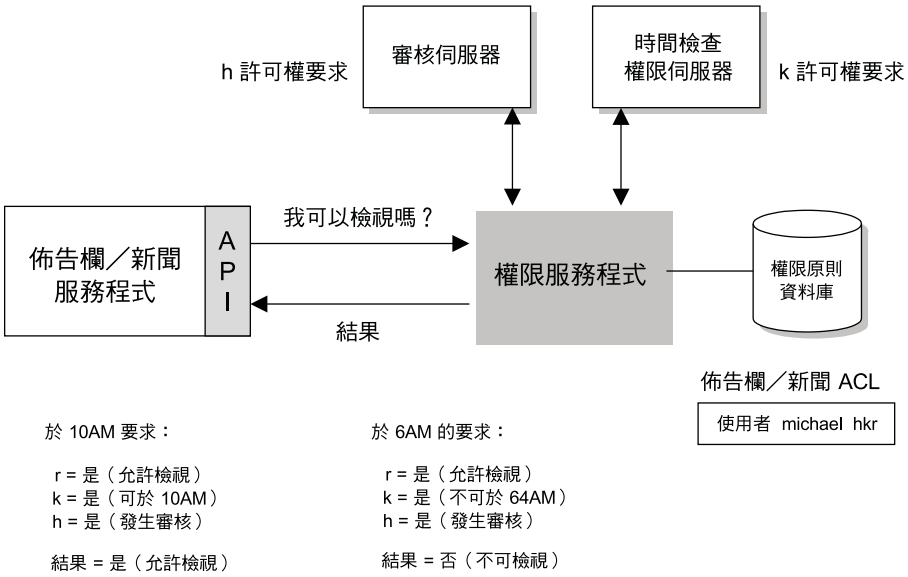
Policy Director 基於總和全部權限伺服器決策的最終的授權決策。



範例 2：

這個範例和範例 1 相同。但是這個範例加入了第二個外部權限服務程式，它審核公佈欄及新聞服務程式的活動。

請注意，當時間檢查器權限服務程式不允許檢視時，活動的審核仍會發生。**h** 許可權的出現，需要在 ACL 期間審核權限伺服器的加入。



「伺服器管理」之管理

Policy Director 管理伺服器 (ivmgrd) 管理主要的 (主) 授權原則資料庫。它也維護關於其它在安全領域中 WebSEAL 及 NetSEAL 伺服器的位置資訊。「管理」伺服器通常需要極少的管理或配置。 這一節包括管理者可用的作業。

設定更新通知者緒數目

「管理」伺服器（ivmgrd）負責維護主要授權原則資料庫。「安全性管理程式」(secmgrd) 及「權限伺服器」(ivacld) 負責建立這個主要的資料庫的複製。

「管理」伺服器則負責安全領域中資料庫複製的同步。當主要資料庫變更時，通知緒進行發表這個變更給所有的複製資料庫的工作。每一個複製資料庫有責任從主要的資料庫下載新資訊。

「管理」伺服器配置檔 (ivmgrd.conf) 含有設定最大更新通知者緒數目的參數。這個緒的儲存池允許同時 (平行) 的通知。

例如，同時通知 30 個複製資料庫關於資料庫的變更，最少將緒儲存池設定爲 30。如果有超過 30 個複製資料庫，會發生另一回合的通知 (在這個例子中如果是一次 30 個)。全部的複製資料庫保證會被通知到，不管這個參數的值爲何。

變更通知緒者值的效能目標是要儘快發表資料庫的變更。一般設定值爲等於現存的複製資料庫數目。設定此值可擁有單一緒儲存池的效能，而能一次即通知完所有複製資料庫。

預設的事件通知者緒儲存池設定爲：

```
[ivmgrd]
max-notifier-threads = 10
```

第12章 登入及審核伺服器活動

Policy Director 提供許多日誌記載及審核功能。日誌檔可以攫取任何由 Policy Director 及 DCE 伺服器所產生的錯誤訊息和警告訊息。還有審核追蹤檔可以監督 Policy Director 及 DCE 伺服器活動。

本章包括：
- 登入及審核簡介。
- 每一個日誌檔的說明。
- 每一個審核檔的說明。

登入及審核概觀

日誌及審核追蹤檔的內容可以是很有用的資訊來源。您可以使用日誌及審核追蹤檔的內容，來監督及找出及修正 Policy Director 和 DCE 伺服器活動的問題。

日誌檔

Policy Director 及 DCE 伺服器使用日誌檔來儲存警告及錯誤訊息。所有的日誌檔都是使用文字格式。

Policy Director 提供以下的日誌檔：

- Policy Director 伺服器日誌檔

  請參閱第138頁的『Policy Director 伺服器日誌檔』。
- DCE 伺服器日誌檔

  請參閱第139頁的『DCE 伺服器日誌檔』。
- DCE 有用性訊息

  請參閱第139頁的『DCE 有用性訊息』。
- 標準 HTTP 日誌檔

  請參閱第140頁的『標準的 HTTP 日誌記載』。

審核追蹤檔

Policy Director 及 DCE 伺服器使用審核追蹤檔來儲存伺服器活動的記錄。*記錄*是指特定伺服器事件的輸出。審核追蹤是記載伺服器活動的多筆記錄的集成。大部分的審核檔都是 ASCII 格式。 DCE 審核追蹤檔是二進位格式。您必須使用 **dcecp** 公用程式來檢視這些檔案。

以下的審核追蹤檔提供了 Policy Director 或 DCE 伺服器的事件資訊：

- 三個 Policy Director 授權審核追蹤檔（audit.log）：
  - 管理伺服器（ivmgrd）
  - 安全管理程式（secmgrd）
  - 權限伺服器（ivacld）

  請參閱第143頁的『Policy Director 授權審核追蹤檔』。
- WebSEAL 審核追蹤檔（wand_audit_log）

請參閱第145頁的『WebSEAL 審核追蹤檔』。

- Policy Director 管理審核追蹤檔

  請參閱第147頁的『Policy Director 管理指令審核追蹤檔』。
- DCE 審核追蹤檔

  請參閱第148頁的『DCE 伺服器審核追蹤檔』。

install-path 變數的使用慣例

根據不同的作業系統平台而定，本章中所使用的 *install-path* 變數具有以下的解譯：

UNIX：

```
/opt/intraverse/
```

Windows：

```
C:\Program Files\IBM\
```

您無法在 UNIX 中改變這個路徑名稱，因爲它是固定的。

Windows 平台可讓您在安裝 Policy Director 軟體期間定義 *install-path*。

Policy Director 伺服器日誌檔

每一個 Policy Director 伺服器都會以動態方式產生警告及錯誤訊息，它們會導入至標準的錯誤，然後重新導向特定的日誌檔。

伺服器	程序	日誌檔位置
管理伺服器	**ivmgrd**	定義於 ivmgrd.conf 中： log-file=*install-path*/ivmgrd/log/ivmgrd.log
安全管理程式	**secmgrd**	定義於 secmgrd.conf 中： log-file=*install-path*/secmgr/log/secmgrd.log
權限伺服器	**ivacld**	定義於 ivacld.conf 中： log-file=*install-path*/ivacld/log/ivacld.log
目錄服務分配管理系統	**nsid**	*install-path*/broker/nsid.log

啓用及停用伺服器日誌檔

配置檔已定義日誌檔時，Policy Director 就會啓用日誌記載。

secmgrd.log 範例

secmgrd.log 檔所含的內容和以下類似：

```
1998-09-22-21:56:36.898-04:00I----- secmgrd FATAL ivc general
exec.c 344 0x00000006
Caught signal (15)
1998-09-22-21:56:37.309-04:00I----- secmgrd ERROR ivc rpc
IVServer.cpp 1039 0x00000001
Could not unexport bindings from name service
(/.:/subsys/ibm/secmgr/server/sun,0x16c9a093
```

```
1998-09-22-21:56:37.354-04:00I----- secmgrd ERROR ivc rpc
IVServer.cpp 1048 0x00000001
Could not unregister RPC endpoints (0x16c9a042)
```

DCE 伺服器日誌檔

每一個 DCE 伺服器都會以動態方式產生警告及錯誤訊息，它們會導入至標準的錯誤，然後重新導向特定的日誌檔。在尋找及更正問題時，這些日誌檔可以是很有用的資訊來源。

DCE 伺服器日誌檔包括：

安全伺服器：

UNIX： `/opt/dcelocal/var/security/secd.log`

Windows： `\Program Files\IBM\dcelocal\var\security\secd.log`

DCE 伺服器：

UNIX： `/opt/dcelocal/var/dced/dced.log`

Windows： `\Program Files\IBM\dcelocal\var\dced\dced.log`

DCE 有用性訊息

遞送檔負責控制 DCE 有用性訊息：

UNIX： `/opt/dcelocal/var/svc/routing`

Windows： `\Program Files\IBM\NetSEAT\var\svc\routing`

註： 就 Windows 系統而言，安裝路徑在安裝期間爲可配置的： `\Program Files\IBM\NetSEAT\`。環境變數 (%NETSEAT%) 會解析爲所配置的路徑。

遞送檔中的預設項目

這個配置檔中的項目會決定記載的資訊類型。 *遞送檔*包括以下的預設項目：

UNIX：

```
FATAL:STDERR:-;FILE:/opt/dcelocal/var/svc/fatal.log
ERROR:STDERR:-;FILE:/opt/dcelocal/var/svc/error.log
WARNING:STDERR:-;FILE:/opt/dcelocal/var/svc/warning.log
```

Windows：

```
FATAL:STDERR:-;FILE:%NETSEAT%\var\svc\fatal.log
ERROR:STDERR:-;FILE:%NETSEAT%\var\svc\error.log
WARNING:STDERR:-;FILE:%NETSEAT%\var\svc\warning.log
```

NOTICE（注意）訊息可提供伺服器活動的額外相關資訊。根據預設，Policy Director 不會啓用（檔案中沒有項目存在）NOTICE 訊息。

如果要啓用 NOTICE 訊息（並且將它們導入標準錯誤），請將以下的 NOTICE 新增至遞送檔結尾：

UNIX：
```
FATAL:STDERR:-;FILE:/opt/dcelocal/var/svc/fatal.log
ERROR:STDERR:-;FILE:/opt/dcelocal/var/svc/error.log
WARNING:STDERR:-;FILE:/opt/dcelocal/var/svc/warning.log
NOTICE:STDERR:-;FILE:/opt/dcelocal/var/svc/notice.log
```

Windows：
```
FATAL:STDERR:-;FILE:%NETSEAT%\var\svc\fatal.log
ERROR:STDERR:-;FILE:%NETSEAT%\var\svc\error.log
WARNING:STDERR:-;FILE:%NETSEAT%\var\svc\warning.log
NOTICE:STDERR:-;FILE:%NETSEAT%\var\svc\notice.log
```

將訊息導入標準輸出的除錯模式

通常 Policy Director 會將警告及錯誤訊息 (包括 NOTICE 訊息) 重新導入適當的日誌檔。

如果要將這些訊息導入標準輸出（終端機），啓動伺服器時請使用 **-debug** 指令選項。這個選項可讓伺服器在前景中執行（亦即，伺服器本身不會成爲常駐程式）。 Policy Director 會將警告及錯誤訊息寫入標準輸出。

例如，如果要在除錯模式中啓動「安全管理程式」(secmgrd)，請使用以下的指令：

```
# /opt/intraverse/secmgr/bin/secmgrd -debug
```

您也可以使用 UNIX 的 **tee** 指令，將伺服器輸出攫取成單一檔案。

以下範例說明在這個模式中啓動 Policy Director「安全管理程式」：

```
# secmgrd -debug 2>&1 | tee /tmp/secmgrd.log
```

除錯備註

除錯時，請記住以下事項：

1. 當您取得伺服器活動資訊時，請務必將遞送檔復置成一般狀況。移除 NOTICE 項目。NOTICE 會產生大量的資訊，而這些資訊可能會快速累積。
2. 您可以使用 **Ctrl + c** 來岔斷以除錯模式啓動的伺服器程序。伺服器程序會正確關機並結束。

標準的 HTTP 日誌記載

Policy Director WebSEAL 伺服器也會維護三個傳統的 HTTP 日誌檔，它們記錄的是活動，而非訊息：

wand_request_log
請參閱第142頁的『顯示 wand_request_log』。

wand_agent_log
請參閱第142頁的『顯示 wand_agent_log』。

wand_referer_log
請參閱第143頁的『顯示 wand_referer_log』。

根據預設，Policy Director 會在以下的目錄中維護這些日誌檔：

UNIX： `/opt/intraverse/www/log`

Windows： `\Program Files\IBM\Policy Director\www\log`

配置標準的 HTTP 日誌記載

配置檔 iv.conf 中的 [wand] 段落包含了配置標準 HTTP 日誌記載的參數。

下表說明 HTTP 日誌檔和配置檔參數之間的關係：

日誌檔	位置參數	啓用/停用參數（= yes 或 no）
wand_request_log	reqlog =	logreqs =
wand_referer_log	reflog =	logrefs =
wand_agent_log	agentlog =	logagents =

例如，iv.conf 中有關 **wand_request_log** 預設位置的項目如下：

```
reqlog = log/wand_request_log
```

這個位置的根目錄是：

UNIX： `/opt/intraverse/www/`

Windows： `\Program Files\IBM\Policy Director\www\`

啓用及停用 HTTP 日誌記載

根據預設， Policy Director 會啓用所有的 HTTP 日誌記載：

```
[wand]
logreqs = yes
logrefs = yes
logagents = yes
```

如果要停用日誌記載，請設定：

```
<enable-parameter> = no
```

指定時間戳記類型

您可以選擇在每一個日誌檔中加上時間戳記，也可以使用格林威治標準時間（GMT），而非本地時區。根據預設，Policy Director 會使用本地時區：

```
[wand]
loggmttime = no
```

如果要使用 GMT 時間戳記，請設定：

```
loggmttime = yes
```

註: 讓所有日誌檔的時間維持同步，可讓所有相關安全產品中之審核與日誌檔的讀取更形容易。

指定日誌檔大小最大值

根據預設，每一個 HTTP 日誌檔大小的最大值是：

```
[wand]
logsize = 2000000
```

當日誌到達這個大小時，Policy Director 會備份日誌檔。

請注意，這個參數也會影響 Policy Director 的 **wand_audit_log** 審核追蹤檔。

請經常檢查日誌檔的大小，確定它們不會變得太大，而佔據太多空間。在一般系統維護時，請定期保存日誌檔。

使用 HTTP 共同日誌格式

Policy Director 伺服器所傳回的每一個回應（順利完成或失敗），都會用以下的「HTTP 共同日誌格式」記錄成一行的項目：

```
host - authuser [date] request status bytes
```

其中：

host	指定提出要求的機器的網際網路通信協定（IP）位址。
authuser	採用所接收之 HTTP 要求的**自**：標頭值。此外，這個欄位也會將值設定成 dce-rpc，以傳遞安全的 RPC 要求。對於未經身份驗證的使用者，這個欄位是空白的。
date	指定要求的日期和時間。
request	將要求的第一行指定成來自從屬站。
status	指定傳送回提出要求的機器的 HTTP 狀態碼。
bytes	指定傳送回提出要求的機器的位元組數目。換言之，轉送文件的內容長度。

顯示 wand_request_log

wand_request_log 記錄了標準的 HTTP 要求日誌記載。標準的日誌記載範例包括已經要求的 URL 資訊，以及提出要求的從屬站資訊（例如，IP 位址）。

wand_request_log 檔所含的內容和以下類似：

```
130.105.1.90 - - [Tue, 23 Apr 1996 17:23:33 EDT]
  "GET /~smith/private_html/ HTTP/1.0" 403 77
130.105.1.90 - - [Tue, 23 Apr 1996 17:23:47 EDT]
  "GET /icons HTTP/1.0" 302 93
130.105.1.90 - - [Tue, 23 Apr 1996 17:23:59 EDT]
  "GET /icons/ HTTP/1.0" 403 77
130.105.1.90 - - [Tue,  23 Apr 1996 17:24:04 EDT]
  "GET /~smith/private_html/ HTTP/1.0" 403 77
130.105.1.90 - - [Tue, 23 Apr 1996 17:24:11 EDT]
  "GET /~smith/ HTTP/1.0" 403 77
dce-rpc - - [Tue, 23 Apr 1996 17:24:51 EDT]
  "GET / HTTP/1.0" 200 919
```

顯示 wand_agent_log

wand_agent_log 記錄了 HTTP 要求中的 User_Agent：標頭內容。這個日誌顯示了每一個要求的從屬站瀏覽器相關資訊，例如配置或版本號碼。

以下範例顯示 wand_agent_log 檔的範例版本：

```
Mozilla/4.01 [en] (WinNT; U)
Mozilla/4.01 [en] (WinNT; U)
Mozilla/4.01 [en] (WinNT; U)
Mozilla/4.01 [en] (WinNT; U)
```

顯示 wand_referer_log

wand_referer_log 記錄了 HTTP 要求的標頭。對於每一個要求，日誌會記錄含有對所要求文件之鏈結的文件。

日誌使用以下格式：

```
referer -> object
```

這項資訊對於追蹤 Web 空間中文件的外部鏈結非常有用。日誌顯示 `referer` 所指出的來源包含對頁面*物件*的鏈結。這個日誌可讓您追蹤陳舊的鏈結，以及找出誰正在對您的文件建立鏈結。

以下範例顯示 wand_referer_log 檔的範例版本：

```
http://manuel/maybam/index.html -> /pics/ibm_logo.gif
http://manuel/maybam/ivdl/index.html -> /pics/ibm_logo.gif
http://manuel/maybam/ -> /ivdl/index.html
http://manuel/maybam/ -> /ivdl/index.html
http://manuel/maybam/ivdl/index.html -> /pics/ibm_logo.gif
http://manuel/maybam/ -> /ivdl/index.html
```

Policy Director 授權審核追蹤檔

有任何與安全相關的可審核活動發生時，每一個 Policy Director 伺服器都可以攫取審核事件。 Policy Director 會將審核事件儲存爲記載該伺服器特定活動的審核記錄。 多個審核記錄會組成一個審核追蹤檔。

下表說明 Policy Director 伺服器與其相關審核追蹤檔之間的關係：

伺服器	程序	授權審核檔
管理伺服器	**ivmgrd**	在 ivmgrd.conf 中定義：audit-file= *install-path*/ivmgrd/log/audit.log
安全管理程式	**secmgrd**	在 secmgrd.conf 中定義：authzn-audit-file= *install-path*/secmgr/log/audit.log
權限伺服器	**ivacld**	在 ivacld.conf 中定義：audit-file= *install-path*/ivacld/log/audit.log

每當您爲 ACL 中的使用者或群組設定審核（A）許可權時， Policy Director 會將「授權」資訊寫入適當的審核追蹤檔。產生的審核記錄包含所有的存取嘗試，包括授權失敗。

審核追蹤管理

ACL 項目中的審核 (A) 許可權會觸發 Policy Director 授權審核追蹤檔記錄活動資訊。透過審核（A）許可權來啓動審核是很容易完成的。

以下條件適用於管理授權審核追蹤檔：

- 連接 ACL 所在的物件決定了三個 audit.log 檔案中的哪一個要收集資料。

  例如，您可以將一或多個項目上包含審核（A）許可權的 ACL，連接到受保護物件名稱空間的 /Management 物件。 如果已連接，則會爲「管理」伺服器（ivmgrd）將資料收集到 audit.log 檔案中。「管理」伺服器會控制授權原則資料庫（ACL）及資料庫複製（複本）。
- 當您在適當的 ACL 項目中設定審核（A）許可權時，只會爲使用者、群組（或兩者皆是）收集活動資訊。

  例如，您可以在連接 HTML 頁面物件的 ACL 中，爲 unauthenticated 項目給定審核（A）許可權。 有了這個許可權，「安全管理程式」的 audit.log 檔會收集嘗試對不容許存取的物件進行存取時的所有資訊。

範例：以下的 ACL 代表預設的 webseal ACL。 cell_admin 使用者項目及 authenticated 項目具有審核（A）許可權集。

```
user cell_admin                 aAbcTdmlrx
group iv-admin                  abdTdmlrx
group ivmgrd-servers            Tl
group webseal-servers           gTdmlrx
any-authenticated               Tr
unauthenticated                 ATr
```

連接到 /WebSEAL 物件的 ACL 表示它是連接到受保護物件名稱空間的 WebSEAL 範圍的根。如果連接，Policy Director 會將有關「安全管理程式」伺服器（WebSEAL 及 NetSEAL）的活動記錄到「安全管理程式」audit.log 檔。

WebSEAL 名稱空間可能不含變更許可權條件的其他明確 ACL，如果沒有其他明確的 ACL，則對 Web 空間內任何物件的所有要求都會被審核。

審核追蹤檔只會記錄 cell_admin 使用者及任何未經身份驗證的存取嘗試所起始的活動。

如果明確的 ACL 是連接到 /WebSEAL 物件之下的物件，則會岔斷 ACL 承接的連鎖。這個明確的 ACL 中的項目可能不含任何審核許可權，如果項目不含任何審核許可權，則不會爲這個物件或這個點以下的任何其他物件產生審核追蹤。

註: 您必須記得將審核許可權加入任何 ACL（您要明確地連接到 /WebSEAL 物件之下的物件）的相關項目。

管理伺服器審核追蹤檔範例

「管理」伺服器審核追蹤檔所含的內容和以下類似：

```
START RECORD
  Protected object: /WebSEAL
  Requested permissions: 0x00000100
  Principals:
principal 0: DCE principal 00000064-35ee-21d2-a000-0800207b48c5
  quality of protection: none    result: authorized
```

```
END RECORD
START RECORD
  Protected object: /WebSEAL/sun
  Requested permissions: 0x00000100
  Principals:
principal 0: DCE principal 00000064-35ee-21d2-a000-0800207b48c5
  quality of protection: none    result: authorize
END RECORD
START RECORD
  Protected object: /WebSEAL/sun/icons
  Requested permissions: 0x00000100
  Principals:
principal 0: DCE principal 00000064-35ee-21d2-a000-0800207b48c5
  quality of protection: none    result: authorize
END RECORD
START RECORD
  Protected object: /WebSEAL
  Requested permissions: 0x00000100
  Principals:
principal 0: DCE principal 00000064-35ee-21d2-a000-0800207b48c5
  quality of protection: none    result: authorize
END RECORD
```

WebSEAL 審核追蹤檔

您也可以監督 Policy Director WebSEAL 伺服器活動。 Policy Director 會將審核事件儲存爲記載該伺服器特定活動的審核記錄。 多個審核記錄會組成一個審核追蹤檔。

WebSEAL 審核

配置 WebSEAL 審核追蹤檔的參數是在配置檔 iv.conf 中的 [wand] 段落中

下表說明 WebSEAL 和審核追蹤檔之間的關係：

伺服器	審核檔
WebSEAL	在 iv.conf 中定義：auditlog= *install-path*/www/log/wand_audit_log

啓用及停用 WebSEAL 審核

預設值是停用 WebSEAL 審核：

```
[wand]
logaudit = no
```

如果要開啓審核，請設定：

```
logaudit = yes
```

註: 在編輯 iv.conf 配置檔中的這個參數時， yes 或 no 之後不能有空格。

指定日誌檔位置

WebSEAL 審核檔的預設位置是：

```
[wand]
auditlog = log/wand-audit-log
```

指定日誌檔大小最大值

Policy Director 會設定審核日誌檔的預設最大值：

```
[wand]
logsize = 2000000
```

當日誌抵達這個大小時，Policy Director 會將日誌檔備份成備份副本。而新與空的審核日誌檔即成爲預設的審核日誌檔。請注意，這個參數也會影響以下的標準 HTTP 日誌檔：

- wand_request_log
- wand_referer_log
- wand_agent_log

WebSEAL 審核追蹤檔語法

WebSEAL 伺服器所傳回的每一個回應（順利完成或失敗），都會用以下格式記錄成一行的項目：

```
host call_type uri iv_status_code [date] uuid group_uuid_list
```

主電腦（及終點）	遠端主電腦的 IP 位址及終點資訊。如果沒有終點資訊，則顯示 [-]。
call_type	0 代表 TCP 連線， 1 代表 UNAUTH RPC， 2 代表 AUTH RPC
uri	要求的「廣用要求指示器」。
iv_status_code	標準審核機能的這個 Policy Director 子集的狀態碼。
date	要求的日期與時間。
uuid（以 **-p** 旗號指示）	從屬站的 UUID。如果沒有 UUID 資訊，則不予顯示。
group_uuid_list （以 **-g** 旗號指示）	群組 UUID 的清單。如果沒有群組 UUID 資訊，則不予顯示。

審核追蹤檔內容範例

審核追蹤檔所含的內容和以下類似：

```
204.30.81.188[33380] 2 /audit_report.html 0x18a2141a
[21/Aug/1997:14:36:23 -0700]
-p 00000064-0f4c-21d1-9300-00c078500371
-g 0000000c-0f4c-21d1-9301-00c078500371
-g 0000044c-0f4c-21d1-8601-00c078500371
-g 0000044d-0f4c-21d1-8601-00c078500371
```

明細：

主電腦：	204.30.81.188
終點：	[33380]
call_type：	2
uri:	/audit_report.html
iv_status_code:	0x18a2141a

date:	[21/Aug/1997:14:36:23 -0700]
uuid:	-p 00000064-0f4c-21d1-9300-00c078500371
group_uuid_list:	-g 0000000c-0f4c-21d1-9301-00c078500371 -g 0000044c-0f4c-21d1-8601-00c078500371 -g 0000044d-0f4c-21d1-8601-00c078500371

註: URI 字串可能只會顯示成連字號。這個情況可能是因爲要求過早結束或格式不正確的要求字串。

Policy Director 管理指令審核追蹤檔

有任何與管理相關的可審核活動發生時，每一個 Policy Director 伺服器都可以攫取審核事件。 Policy Director 會將審核事件儲存爲記載該伺服器特定活動的審核記錄。 多個審核記錄會組成一個審核追蹤檔。

下表說明 Policy Director 伺服器與其相關審核追蹤檔之間的關係：

伺服器	程序	管理審核檔
管理伺服器	**ivmgrd**	在 ivmgrd.conf 中定義：mgr-audit-file= *install-path*/ivmgrd/log/mgraudit.log

「管理」伺服器的責任包括維護主要授權原則資料庫。

這個資料庫包括安全領域之受保護物件名稱空間的說明、 ACL 原則模板，以及將 ACL 連接到物件的地方。

這個資料庫包括：

- 安全領域之受保護物件名稱空間的說明。
- ACL 原則模板。
- 將 ACL 連接到物件所在的相關資訊。

您可以從「管理主控台」或利用 **ivadmin** 公用程式，將任何管理指令事件攫取到 mgraduit.log 檔案中：

審核記錄內容

審核記錄會寫入記錄中，並且以 XML 樣式的方括弧作爲標示語言。 審核事件會攫取以下資訊：

發送端 ID

衍生自進入的 RPC 從屬站控點，並且列印成 UUID 清單或 unauthenticated 字串。

標示：P

事件 ID

用來唯一識別管理指令的數字，它是在 ../ivmgrd/cmdConst.h 標頭中定義。

標示：I

指令輸出

對應至呼叫程式所傳回之狀態碼的數字。

標示：O

時間戳記

完成指令的時間記錄，其格式和 ACL 位元審核目前使用的相同。

標示：D

指令引數向量

指令輸入引數的表示法。

標示：V 及 A

管理伺服器審核追蹤檔範例

「管理」伺服器審核追蹤檔所含的內容和以下類似：

```
<E><D>Fri May 30 00:00:00 1999<\D><I>3008</I><O>0</O><P>[1]
069d9fb6-943e-11cd-a35c-0000c08adf56</P><V><A> argument
1</A><A>argument 2</A></V></E>
```

DCE 伺服器審核追蹤檔

以下的 DCE 伺服器審核追蹤檔使用 DCE 審核服務程式。檔案格式是二進位格式。您必須使用 **dcecp** 公用程式來檢視檔案。

1. DCE 安全服務程式（secd）審核追蹤

   /opt/dcelocal/var/security/sec_audit_trail

   /opt/dcelocal/var/security/sec_audit_trail.md_index
2. DCE 審核服務程式（auditd）審核追蹤

   /opt/dcelocal/var/security/central_trail

   /opt/dcelocal/var/security/central_trail.md_index
3. DCE 時間服務程式（dtsd）審核追蹤

   /opt/dcelocal/var/security/dts_aud_trail

   /opt/dcelocal/var/security/dts_aud_trail.md_index

sec_audit_trail 範例

```
dcecp> login cell_admin
Enter Password:
dcecp>
--- Event Record number 261 ---
o Event Information:
   - Event Number:          0x101 /* 257 */
   - Event Name:          AS_Request
   - Event Outcome:          success
o Server:          /.:/hosts/eggman
o Client:          /.../eggman_cell/cell_admin
o Number of groups:          0
o Authorization Status:          Authorized with a name
o Date and Time recorded: 1998-10-20-10:42:56.248-04:00I-----
--- End of Event record number 261 ---
```

第13章 WebSEAL：設定身份驗證

Policy Director WebSEAL 支援 LDAP、Kerberos，以及公開與私密金鑰身份驗證機制。身份驗證的一個重要副產品是使用者證明的取得。在授權要求（即要求存取受保護的資源）期間，會用到使用者證明。

本章包括：

WebSEAL 身份驗證概觀

本節討論如下的 WebSEAL 支援：

- 透過 SSL 通信協定支援安全通信。
- 身份驗證機制。
- 提供身份資訊的方法。
- 標準身份驗證機制的擴充。

SSL 支援

WebSEAL 支援透過安全 socket 層次（SSL）通信協定的安全通信。 以下各節討論透過 SSL 通信協定的安全通信：

- 第150頁的『爲 SSL 配置 WebSEAL』.
- 第152頁的『爲 WebSEAL 設定伺服器端的憑證』.

身份驗證機制

身份驗證是指識別嘗試登入安全領域之個體的程序。 WebSEAL 支援以下的身份驗證機制：

- LDAP 機密金鑰
- Kerberos 版本 5
- 公開與私密金鑰

從屬站身份資訊

身份驗證程序需要從屬站在登入期間提出某些形式的身份資訊。 WebSEAL 支援以下的方法來提出這項身份資訊：

1. 使用者名稱與密碼（供 LDAP 與 Kerberos 使用）
   - 基本身份驗證

- 基於套表的登入

請參閱第157頁的『使用者名稱和密碼的身份驗證方法』。

2. 從屬站端 X.509 憑證（供公開/私密金鑰使用）

請參閱第161頁的『X.509 憑證身份驗證方法』。

證明獲取

您可以使用「證明獲取服務程式（CAS）」，擴充 WebSEAL 支援的標準身份驗證機制。請參閱第163頁的『配置「Policy Director 證明獲取服務程式」』。

為 SSL 配置 WebSEAL

Policy Director WebSEAL 伺服器支援和使用安全 socket 層次（SSL）的從屬站瀏覽器之間的安全通信。

使用這個通信協定時，從屬站可使用兩個方法的其中一個來傳送身份資訊到 WebSEAL：

- 使用者名稱和密碼
- 從屬站端的 X.509 數位式憑證

在兩種模式中，WebSEAL 會藉由其伺服器端的數位式憑證，自行對從屬站進行身份驗證。「憑證管理中心」（CA）會發出此一 X.509 憑證。 Policy Director 會將憑證及相關的私密金鑰儲存在 PEM 格式檔或 PKCS#12 格式檔。

使用 PEM 格式時，Policy Director 會將伺服器的私密金鑰以及簽名的公開金鑰儲存在個別的檔案中。當使用 PKCS#12 格式時，則產生與儲存的金鑰對同位於一個檔案中。

建議您讓憑證中的共通名稱（CN）與 WebSEAL 伺服器的完整主電腦名稱相同。

雖然不是必要的，大部分的從屬站瀏覽器會驗證有效的「憑證管理中心」是否已經發出伺服器憑證。 驗證是透過主要 CA 憑證資料庫來完成的。如果憑證的簽名者不符合主要 CA 憑證資料庫中的項目，則會出現警告。 使用者必須接受或拒絕與該伺服器的連接。

請參閱第152頁的『爲 WebSEAL 設定伺服器端的憑證』以取得爲 WebSEAL 取得及安裝伺服器端 X.509 憑證的完整資訊。

在從屬站端憑證模式中，如上所述，WebSEAL 會使用其伺服器端的數位式憑證，自行對從屬站進行身份驗證。此外，WebSEAL 會要求需有 CA 所發的 X.509 主要 CA 憑證，以驗證從屬站端的憑證。從屬站端所發出的從屬站要求可提供眞實的相互身份驗證。

使用伺服器端憑證及主要 CA 憑證

伺服器端的 X.509 憑證可對從屬站識別特定的 WebSEAL 伺服器。 Policy Director 會以 PEM 或 PKCS#12 格式來儲存伺服器端的憑證，方式如下：

- PEM 格式 -- 儲存伺服器之私密金鑰與已簽章之公開金鑰的個別檔案
- PKCS#12 格式 -- 內含伺服器之私密與公開金鑰的單一檔案。

註: WebSEAL 一次只能包含及支援一個伺服器憑證。 WebSEAL 不支援同一部機器上的多個邏輯 Web 伺服器案例。

*主要 CA 憑證*用以代表一個特定的「憑證管理中心 (CA)」。WebSEAL 需要主要 CA 憑證來驗證從屬站端的憑證。 WebSEAL 可以用 PEM、PKCS#12 或合併兩者的格式，來維護 主要 CA 憑證的清單，方式如下：

- PEM 格式--將主要憑證累積在一個單一檔案中
- PKCS#12 格式--將主要憑證以個別的檔案儲存在一個共同目錄下

儲存憑證

secmgrd.conf 配置檔負責定義憑證儲存參數。這些參數是不同的，端視您使用的參數是供 UNIX 或 Windows 使用。

參數	說明
UNIX： `ca-directory = /opt/intraverse/lib/certs` **Windows**： `ca-directory = C:\Program Files\ibm\Policy Director\lib\certs`	
	憑證儲存體的基本目錄。
UNIX： `ca-cert-file = /lib/certs/cacert.pem` **Windows**： `ca-cert-file = C:\Program Files\ibm\Policy Director\lib\certs\cacert.pem`	
	認可之「憑證管理中心」的 X.509 主要 CA 憑證（PEM 格式）。WebSEAL 可接受可靠 CA 所發出而採 PEM 格式的從屬站端 X.509 憑證。您可以將其他 CA 的主要憑證附加到這個檔案。
UNIX： `ca-cert-p12-dir = /opt/intraverse/lib/certs/ca_p12` **Windows**： `ca-cert-p12-dir = C:\Program Files\ibm\Policy Director\lib\certs\ca_p12`	
	檔案的指定目錄，此檔案中含有認可之「憑證管理中心」的 X.509 主要憑證（PEM 格式）。WebSEAL 可接受可靠 CA 所發出而採 PKCS#12 格式的從屬站端 X.509 憑證。您可以將其他 CA 的主要憑證檔儲存在這個目錄中。
UNIX： `certificate-file = /opt/intraverse/lib/certs/svrcert.pem` **Windows**： `certificate-file = C:\Program Files\ibm\Policy Director\lib\certs\svrcert.pem`	
	向 CA 取得的 X.509 伺服器憑證（PEM 格式）。這個憑證是提出給 SSL 從屬站。此檔案中的憑證範例，應換成可靠 CA 所發的合法憑證。
UNIX： `key-file = /opt/intraverse/lib/certs/srvkey.pem` **Windows**： `key-file = C:\Program Files\ibm\Policy Director\lib\certs\srvkey.pem`	
	採 PEM 格式的伺服器私密金鑰。安裝時，此檔案中所含的金鑰範例應換成您產生的合法金鑰。
UNIX： `certificate-file = /opt/intraverse/lib/certs/svrcert.p12` **Windows**： `certificate-file = C:\Program Files\ibm\Policy Director\lib\certs\svrcert.p12`	

	向 CA 取得的 X.509 伺服器憑證（PKCS#12 格式）。檔案包括私密金鑰。此檔案中的憑證與金鑰範例，應換成可靠 CA 所發的合法憑證與金鑰。
UNIX 及 Windows： **pass-key =***passphrase*	
	用來解除鎖定私密金鑰檔的金鑰密碼（*passphrase*）。

配置憑證處理

配置檔 iv.conf 中的 [wand] 段落包含了處理從屬站端 X.509 憑證的參數。您可以藉由設定 **verify-clients** 參數，來指定 WebSEAL 如何處理從屬站端的 X.509 憑證。verify-clients 的容許值包括：

值	說明
never	不向從屬站要求 X.509 憑證。強制從屬站使用使用者名稱和密碼來進行存取。
optional	向從屬站要求 X.509 憑證，並且在提供憑證時使用基於憑證的身份驗證。當從屬站未提出憑證時，強制從屬站使用基本身份驗證。
required	向從屬站要求 X.509 憑證，並且使用基於憑證的身份驗證。當從屬站未提出憑證時，不容許連接。

根據預設，WebSEAL 不會要求從屬站端的憑證：

```
[wand]
verify-clients = never
```

設定 SSL 階段作業快取逾時

secmgrd.conf 配置檔的 [ssl] 段落包含設定靜態 SSL 階段作業快取逾時的參數。

WebSEAL 會在內部快取證明資訊。這個證明期滿參數指定在 WebSEAL 記憶體中維持授權證明資訊的時間長度。

參數不是指非作用逾時。此值對映的是 “證明的使用期限” 而非 ”證明的逾時”。其目的是當 Policy Director 抵達指定的逾時上限時，強迫使用者重新鑑定，藉以強化安全性。

預設快取逾時值（以秒計）爲：

```
[ssl]
ssl-cache-timeout = 3600
```

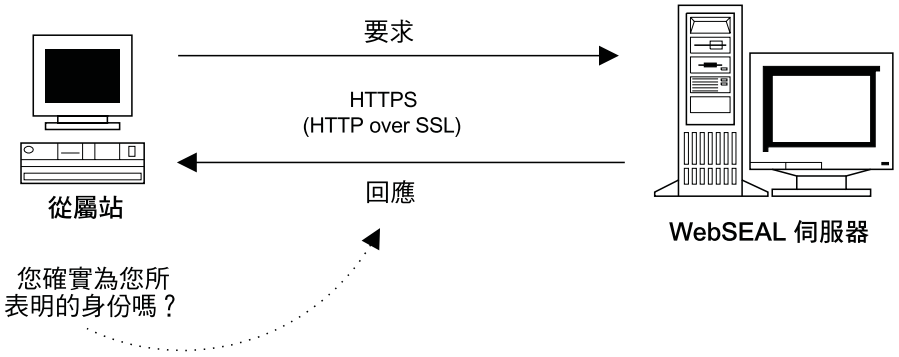
調整這個值來平衡伺服器效能以及使用者便利性二者，端視伺服器必須處理的 SSL 要求數量而定。

註: 某些瀏覽器會執行自動階段作業協調。如果您的瀏覽器是屬於這種情況，這個參數將是無效的。

為 WebSEAL 設定伺服器端的憑證

您可以設定 Policy Director WebSEAL 伺服器，以容許啓用 SSL 的從屬站驗證伺服器的確實性。本節將引導您執行一遍管理作業；如果您是以 PEM 格式來設定伺服器端憑證，則需執行這些作業。

特別是作業涉及到登錄有效的 CA 或內部控制的憑證產生產品。登錄必須取得網站伺服器憑證，以容許 Policy Director 適當地接受及回應來自啓用 SSL 的瀏覽器之要求。

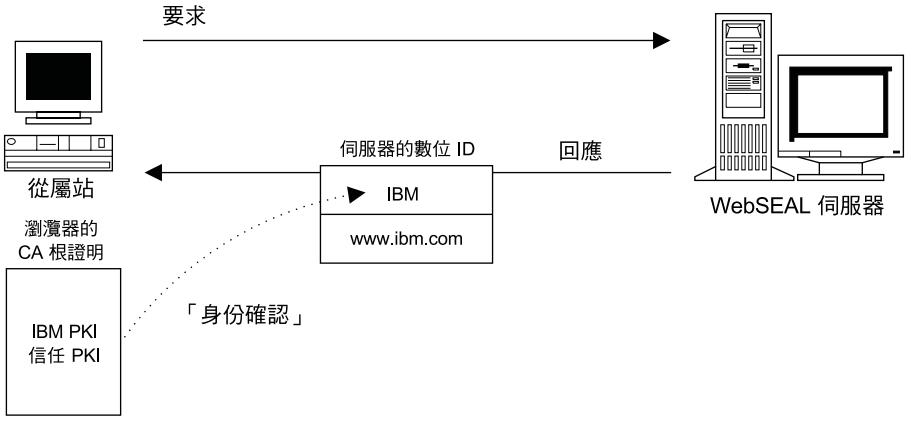


確定透過 SSL 的安全通信

Policy Director WebSEAL 伺服器支援對透過 SSL（HTTPS），並且利用 HTTP 進行存取的從屬站進行身份驗證。 WebSEAL 必須具備安裝好的伺服器端公用 X.509 憑證，以便用來回應這些從屬站。 X.509 憑證可對從屬站證明，來自 WebSEAL 的回應是來自容許的伺服器。

對於透過網際網路的安全 SSL 通信，瀏覽器必須驗證伺服器的身份。瀏覽器會檢查伺服器的公開金鑰憑證和相符的主要 CA 憑證，來進行身份驗證。相符的 CA 憑證是和瀏覽器隨附在一起，或是由瀏覽器取得。

一份經由 CA 簽章的獲准伺服器憑證，可杜防可能的僞造。



WebSEAL 附有一個伺服器憑證範例，它是由 IBM 憑證管理中心範例所簽名。這個範例憑證可讓 WebSEAL 回應來自啓用 SSL 之瀏覽器的要求。然而，瀏覽器無法驗證範例憑證，因爲憑證不含 IBM 主要 CA 憑證。 因此，它不能提供安全通信。

爲了確保透過 SSL 的安全通信，從信任的「憑證管理中心」登錄站台伺服器憑證是非常重要的。您可向認可的 CA 取得網站伺服器憑證，或使用 IBM SecureWay Trust Authority 之類的軟體產生 “自家的” 憑證。

設定 Policy Director 以透過 SSL 進行通信時，牽涉到以下的作業：

- 『產生公開金鑰及私密金鑰』.
- 『使用 gencsr 公用程式 (選用性)』（可選用）。
- 第156頁的『向憑證管理中心登錄 CSR』.
- 第156頁的『安裝伺服器憑證』.
- 第156頁的『更新安全管理程式配置檔』.
- 第157頁的『測試新的憑證安裝』.

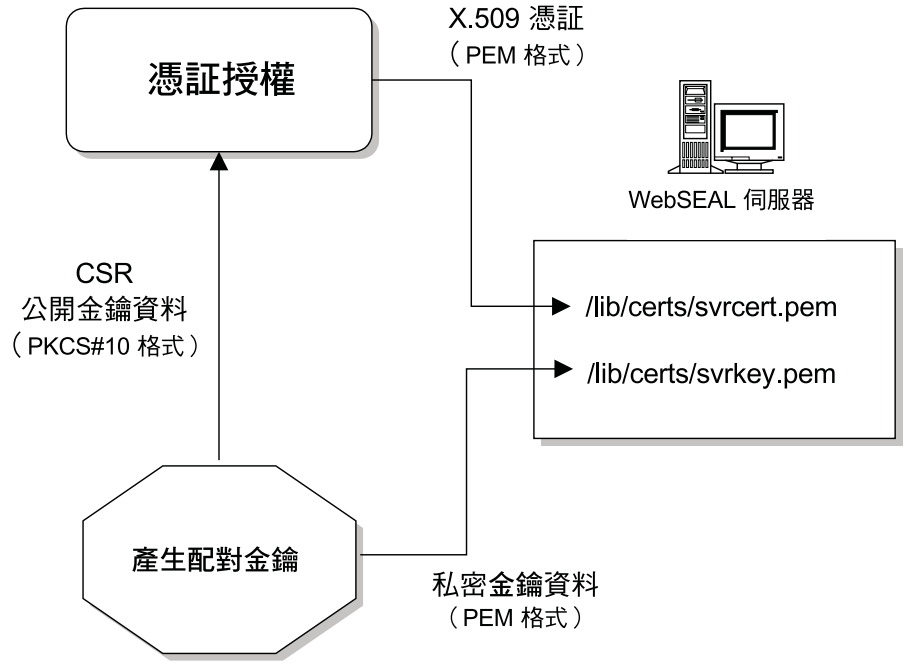
產生公開金鑰及私密金鑰

如果要從 CA 取得站台伺服器憑證，您必須先爲您的伺服器產生公開/私密配對金鑰。

您保留的是私密金鑰的部分。

公開金鑰的部分（包含使用者身份資訊）稱爲「憑證簽章要求」（CSR）。 CSR 是您在登錄取得網站伺服器憑證時必須傳給 CA 的資訊。 CA 使用這項資訊來建構您的 X.509 伺服器端憑證，它是用來回應啓用 SSL 的從屬站。

您必須將私密金鑰以及來自 CA 的伺服器端 X.509 憑證儲存在特別指定的位置。 Policy Director secmgrd.conf 配置檔會定義這些位置。



如要產生公開與私密金鑰對，請使用 CA 提供的產生工具與指示。 Policy Director 提供了一個公用程式（**gencsr**），在沒有其他公用程式可用時，您可以使用這個公用程式。 『使用 gencsr 公用程式 (選用性)』說明了使用 **gencsr** 來產生配對金鑰的作業。

使用 gencsr 公用程式 (選用性)

Policy Director 提供一種選用公用程式，**gencsr**，用以產生公開與私密金鑰對。公用程式是屬於 Policy Director 安裝的一部分，它位於 /bin 目錄中：

UNIX： *install-path*/bin/gencsr

Windows： *install-path*\bin\gencsr

PKCS#10 格式

gencsr 公用程式可產生配對金鑰。這個公用程式可以 PEM 格式將私密金鑰資訊寫入檔案。這個公用程式可將公開金鑰和其他憑證簽名要求資訊一起儲存在一個檔案中。公用程式是以 PKCS#10 格式來儲存公開金鑰資訊。

公開金鑰加密標準（PKCS）說明了憑證要求的語法。憑證要求是由識別名稱、公開金鑰和選用的屬性集所組成，並且由要求憑證的組織一起簽名。憑證簽名要求會傳送到「憑證管理中心」。然後，CA 會爲您的伺服器產生一個唯一的 X.509 公開金鑰憑證。

gencsr 公用程式指令語法

gencsr [-csrfile *csr_filename*] [-keyfile *key_filename*] [-keylen *key_length*] [-version]

選項	說明
-csrfile	指定將公開金鑰（CSR）輸出至檔案（PKCS#10 格式）。指定的檔案（*csr_filename*）會以「美國國家標準交換碼」（ASCII）格式來保留 CSR。預設值是標準輸出。
-keyfile	指定將私密金鑰輸出（PEM 格式）至檔案。預設值是標準輸出。
-keylen	指定公開/私密配對金鑰的金鑰長度（以位元組爲單位）。預設值爲 512。
-version	顯示公用程式版本號碼及版權資訊。
-help	顯示指令語法及選項說明。

Gencsr 公用程式程序

如果要使用 Policy Director 的 **gencsr** 公用程式：

1. 爲 CSR 檔名、私密金鑰及金鑰長度（選用性）使用適當的引數，以啓動 **gencsr** 公用程式：

   UNIX： $ gencsr -csrfile *filename* -keyfile *filename* -keylen 1024

   Windows： gencsr -csrfile *filename* -keyfile *filename* -keylen 1024

   您可以使用任何檔名作爲公開及私密金鑰；您在稍後的步驟中會將它們重新命名。

   註: 預設的金鑰長度是 512 的位元組。

2. 公用程式會提示您輸入個人資訊，其中包括 *PEM 通行詞彙*。

   您必須記住這個通行詞彙。在稍後的步驟中，會將這個通行詞彙儲存在 secmgrd.conf 配置檔中。通行詞彙可爲您的私密金鑰提供保護。

3. 公用程式會產生一個 CSR 檔及私密金鑰檔。 第156頁的『向憑證管理中心登錄 CSR』說明如何將 CSR 傳給憑證管理中心。

4. 備份 Policy Director 所附的範例私密金鑰檔：

   UNIX： # cp svrkey.pem svrkey.pem.orig

   Windows： copy svrkey.pem svrkey.pem.orig

5. 將新產生的私密金鑰檔儲存在這個相同的目錄，並且將它命名爲 svrkey.pem：

   UNIX： # cp newkey.txt svrkey.pem

Windows： `copy newkey.txt svrkey.pem`

註: 您必須保護這個私密金鑰。您只能有一個私密金鑰案例，它對於驗證從屬站與從屬站之間的通信非常重要。

向憑證管理中心登錄 CSR

如果要向憑證管理中心登錄 CSR：

1. 「憑證管理中心」通常具有一個線上登錄套表。請使用 Web 瀏覽器來填入這個套表。端視 CA 而定，確實的程序可能會有所不同。
2. 登錄套表要求您提供在第154頁的『產生公開金鑰及私密金鑰』或第154頁的『使用 gencsr 公用程式 (選用性)』中產生的 CSR。您可以將 CSR 檔內容貼在套表上，或以電子郵件寄送檔案。
3. CA 會傳給您 PEM 格式的新 X.509 伺服器端公用憑證。這個程序會花上數天。

WebSEAL 要求憑證爲 PEM 格式。PEM 編碼制是一種適用於二進位憑證的 base64 轉換。PEM 格式是一種 ASCII 檔案，其中每行長度限制在 64 個字元內。此種 ASCII 檔的開頭爲：

```
-----BEGIN CERTIFICATE----
```

結尾爲：

```
-----END CERTIFICATE----
```

安裝伺服器憑證

如果要安裝伺服器憑證：

1. 備份 Policy Director 所附的範例伺服器憑證檔：

   PEM 格式方面：

   UNIX： `# cp svrcert.pem svrcert.pem.orig`

   Windows： `copy svrcert.pem svrcert.pem.orig`
2. 將來自 CA 的新伺服器憑證檔儲存在這個相同的目錄中，並且將它命名爲 svrkey.pem（改寫舊的值）：

   UNIX： `# cp newcert.txt svrcert.pem`

   Windows： `copy newcert.txt svrcert.pem`

更新安全管理程式配置檔

必要時檢查並更新 secmgrd.conf 配置檔中的下列項目：

`certificate-file =`	從 CA 接收的包含 PEM 格式憑證的檔案之路徑名稱。 預設值：lib/certs/svrcert.pem
`key-file =`	本端產生的私密金鑰檔的路徑名稱。 預設值：lib/certs/svrkey.pem
`pass-key =`	用來保護私密金鑰的 PEM 通行詞彙。

當您使用列出的預設檔名以外的檔名時，只變更 `certificate-file` 項目以及 `key-file` 項目。

測試新的憑證安裝

如果要測試新的憑證安裝：

1. 停止並重新啓動 Policy Director 來開始使用新的憑證：

   UNIX：

   ```
   # /etc/init.d/iv stop
   # /etc/init.d/iv start
   # /etc/init.d/iv status
   ```

   Windows：使用「服務程式控制台」。

2. 確定「安全管理程式」（secmgrd）已經順利啓動。

   當 secmgrd 無法啓動時，請檢查以下的日誌檔來察看失敗的原因：

   UNIX： *install-path*/secmgr/log/secmgrd.log

   Windows： *install-path*\secmgr\log\secmgrd.log

   當您找不到有意義的錯誤訊息，請在除錯模式中以手動方式啓動 secmgrd。請參照 第140頁的『將訊息導入標準輸出的除錯模式』。此外您可在下列的 IBM SecureWay Policy Director 網站中找到有關更正問題的最新資訊：

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

3. 從瀏覽器，連接到使用 HTTPS 的伺服器，並且確定瀏覽器接受伺服器憑證。

   例如，瀏覽器應該已經預設儲存了廣爲認知的 VeriSign 主要憑證。因此，在 Policy Director 登入提示之前，您不應該會收到任何警告訊息或對話框。

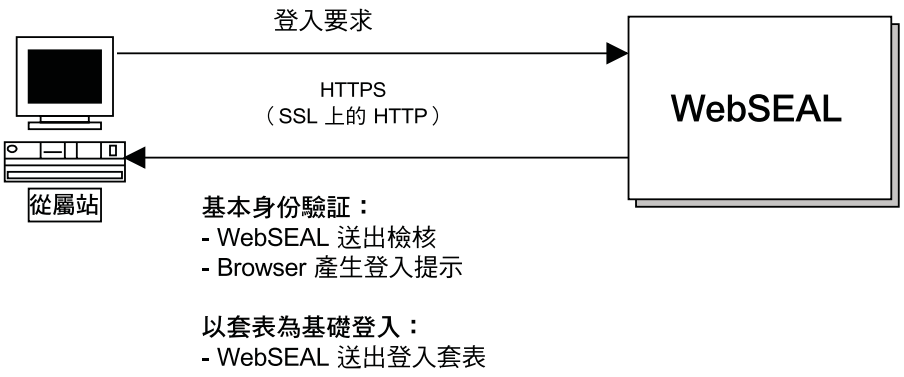
   如果您使用 Policy Director 所附的範例憑證，則會出現警告訊息。 出現警告訊息是因爲瀏覽器不含 IBM 主要憑證，以便驗證範例伺服器憑證。 這些訊息會提示您接受或拒絕伺服器憑證。 如果沒有主要憑證，瀏覽器就無法驗證伺服器憑證的合法性。因此，瀏覽器必須將接受或拒絕憑證的責任交給您。

   您現在已經有一個由信任的「憑證管理中心」所驗證的站台伺服器憑證。有了經過驗證的伺服器憑證，啓用 SSL 的從屬站可以順利及安全地驗證您的 Policy Director WebSEAL 伺服器身份。

使用者名稱和密碼的身份驗證方法

Kerberos 及「LDAP 機密金鑰」身份驗證機制需要使用者名稱和密碼形式的從屬站身份資訊。 WebSEAL 支援兩種證明利用使用者名稱和密碼進行身份驗證的方法。

- 第158頁的『基本身份驗證方法』.
- 第159頁的『Policy Director 套表式登入方法』.



基本身份驗證方法

WebSEAL 支援 Netscape® Communicator/Netscape Navigator® 與 Microsoft Internet Explorer™ (IE) 所用的 SSL 通信協定，來取得使用者名稱和密碼之類的使用者資訊。根據慣例，以**https:**而非**http:**） 開頭的 URL 表示使用了安全 SSL 連接。

爲了登入成功，Policy Director 要求從屬站使用它們記錄在安全登錄中的 Policy Director 身份。*基本身份驗證*是一種提供使用者名稱和密碼給身份驗證機制的標準方法。

第一步，伺服器會使用其伺服器端的憑證對從屬站進行身份驗證。 如果從屬站接受憑證，伺服器會對從屬站發出一則檢核。瀏覽器會產生一個登入提示，要求輸入使用者名稱及密碼。

註: 瀏覽器會快取這項登入資訊。標準的基本身份驗證在每一個後續的要求中，會要求提供使用者名稱資訊及密碼資訊。快取的身份驗證資訊會以透通方式傳送給使用者。

基本身份驗證的重點包括：

- Policy Director 使用 SSL 作爲安全通信通道。
- Policy Director 會跨越安全 SSL 通道來傳輸使用者名稱和密碼。

您會看到登入提示，它由基本身份驗證查問題，如下所示：

```
輸入位於 www.ibm.com 之 Policy Director [/.../www.ibm.com] 的使用者名稱
使用者名稱：
密碼：
```

您必須在**使用者名稱**及**密碼**欄位輸入所需的資訊。

基本身份驗證模式

基本身份驗證模式的程序包括：

1. 從屬站瀏覽器會使用 SSL 來聯絡伺服器。
2. 伺服器會傳回其簽名的公開金鑰伺服器憑證，這是從 CA 取得。
3. 從屬站瀏覽器會採取以下其中一項動作：
   - 在其資料庫中尋找相關的主要 CA 憑證，並且接受伺服器的憑證。
   - 在其資料庫中找不到相關的主要 CA 憑證，並且以警告提示使用者。使用者現在必須接受或拒絕憑證。

4. 接受時，伺服器會對瀏覽器發出一則查證。
5. 瀏覽器會產生一個登入提示，要求輸入使用者名稱及密碼。
6. 在使用者鍵入使用者名稱與密碼資訊後，瀏覽器會將資訊傳給 Policy Director 伺服器。
7. 當使用者名稱和密碼資訊符合 Policy Director 使用者登錄中的現存資訊時， Policy Director 會產生一個證明。 Policy Director 使用此證明來進行授權決策。 WebSEAL 會在 SSL 階段作業期間快取這項證明。
8. 瀏覽器會快取使用者名稱資訊及密碼資訊。

   標準的基本身份驗證會要求每一個後續瀏覽器登入或要求的使用者名稱和密碼。這項要求可使用快取的身份驗證資訊來滿足。

   註: 由於在基本身份驗證中，瀏覽器會快取使用者名稱及密碼資訊， **pkmslogout** 指令便無法正確作用。 如果要完全登出，您必須關閉瀏覽器階段作業。當您需要 **pkmslogout** 特性時，請使用基於套表的登入。

必要的管理作業

管理者必須執行以下的作業來準備 WebSEAL 伺服器，以便在基本身份驗證模式中進行 SSL 存取：

- 將伺服器端的 X.509 憑證安裝到 WebSEAL 伺服器。
- 爲即將參與安全領域的每一個使用者建立一個 Policy Director 帳戶。

Policy Director 套表式登入方法

Policy Director 提供了標準基本身份驗證機制以外的另一個選擇方案： Policy Director *套表式登入*。這種方法會從 Policy Director 產生一個 HTML 登入套表，不像基本身份驗證的深入問題所產生的標準登入提示。

當您使用套表式登入時，瀏覽器並不像基本身份驗證會快取使用者名稱和密碼資訊。 如此便可順利使用特殊 SSL 階段作業登出指令 **pkmslogout**。 由於 Policy Director 只需要證明資訊一次（並且會予以快取），就不需要在每一個瀏覽器要求時重複登入要求。

在 iv.conf 配置檔中的 [wand] 段落中，使用 **https-forms-auth** 參數來完成套表式登入。這個參數可以設定成 yes 或 no。預設值是 no。

```
[wand]
https-forms-auth = no
```

Policy Director 包括七個範例 HTML 套表。您可以自訂這些 HTML 套表，以包含站台特定的訊息，或執行站台特定的動作。

配置檔 iv.conf 中的 [wand] 段落在 SSL HTML 頁面位置之下定義了這些套表的檔案位置。

預設目錄位置是：

UNIX： *install-path*/www/lib/html/

Windows： *install-path*\www\lib\html\

套表	說明
login.html	要求取得使用者名稱與密碼
login_rep.html	登入錯誤訊息
logout.html	從 SSL 階段作業順利登出的訊息
passwd.html	變更密碼套表
passwd_exp.html	密碼期滿訊息
passwd_rep.html	變更密碼錯誤訊息
help.html	指令說明

還有兩個巨集可用於這些頁面。您可以將這些巨集字串置於模版檔中。常式會以動態方式替代適當的值。

巨集	說明
%USERNAME%	登入使用者的名稱。
%ERROR%	從 Policy Director 傳回的寫在程式內的錯誤訊息。

套表式身份驗證模式

格式基礎的身份驗證模式程序如下：

1. 從屬站瀏覽器會使用 SSL 來聯絡伺服器。
2. 伺服器會傳回其簽名的公開金鑰伺服器憑證，這是從 CA 取得。
3. 從屬站瀏覽器會採取以下其中一項動作：
   - 在其資料庫中尋找相關的 CA 憑證，並且接受伺服器的憑證。
   - 在其資料庫中找不到相關的 CA 憑證，並且以警告提示使用者。使用者現在必須接受或拒絕憑證。
4. 當從屬站接受時，WebSEAL 會使用自訂的 Policy Director HTML 套表，提示從屬站輸入使用者名稱和密碼。

   Policy Director 使用這個套表來將使用者名稱和密碼資訊傳回 WebSEAL。
5. 當使用者名稱和密碼資訊符合 Policy Director 使用者登錄中的現存資訊時， Policy Director 會產生一個證明。 Policy Director 使用證明來進行授權決策。 WebSEAL 會在 SSL 階段作業期間快取這項證明。

   和基本身份驗證不同，瀏覽器*不會*快取使用者名稱和密碼資訊。 **pkmslogout** 指令現在可以正常作用。

必要的管理作業

管理者必須執行以下的作業來準備 WebSEAL 伺服器，以便在套表式登入模式中進行 SSL 存取：

1. 將 X.509 伺服器端 CA 憑證安裝到 WebSEAL 伺服器。
2. 爲即將參與安全領域的每一個使用者建立一個 Policy Director 帳戶。
3. 自訂 Policy Director 套表，並且在 iv.conf 配置檔中定義它們的位置。

使用者名稱和密碼方法的指令

Policy Director 提供以下的指令來支援對啓用 SSL 以及利用使用者名稱和密碼方法的從屬站進行身份驗證：

- pkmslogout
- pkmspasswd

pkmslogout

使用 pkmslogout 指令來從現行 SSL 階段作業登出套表。這個指令適用於套表式登入方法。

```
https: //Web URL install-path/pkmslogout
```

例如：

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

您在 iv.conf 配置檔中定義爲了回應這個登出所顯示的檔案：

```
# SSL HTML 頁面位置
pkms-logout-page = lib/html/logout.html
```

您可以根據自我需求來變更 logout.html 檔。

當網路配置需要爲登出不同後端系統的使用者提供不同的結束螢幕時， **pkmslogout** 公用程式也支援多個登出回應頁面。

以下的表示式定義了一個特定的回應檔：

```
https://pkmslogout?filename=custom_logout_file
```

其中 *custom_logout_file* 是登出回應的檔名。這個檔案必須常駐在爲預設 logout.html 檔所定義的同一個 /lib/html/ 目錄中。

pkmspasswd

執行這個指令來變更您的密碼。

```
https://Web URL install-path/pkmspasswd
```

例如：

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

X.509 憑證身份驗證方法

WebSEAL 支援透過 SSL 使用從屬站端 X.509 憑證來進行身份驗證。不同於使用者名稱和密碼，X.509 憑證可提供從屬站的身份資訊。

設定從屬站端 X.509 憑證支援的作業

執行以下的作業來將 WebSEAL 設定成支援從屬站端的 X.509 數位式憑證：

從屬站作業

如果要執行從屬站作業：

1. 從 CA 取得 X.509 從屬站端數位式憑證（已簽名的公開金鑰）。
2. 將憑證安裝到從屬站系統。

WebSEAL 伺服器作業

如果要執行 WebSEAL 伺服器作業：

1. 取得同一個「憑證管理中心」的主要 CA 憑證。

   憑證格式可以是 PEM 或 PKCS#12。
2. 將主要 CA 憑證複製到系統中的適當位置，並在 secmgrd.conf 配置檔中指出這個位置：

   PEM 格式：

   將主要憑證附加到以下的檔案：

   UNIX： `ca-cert-file = lib/certs/cacert.pem`

   Windows： `ca-cert-file = lib\certs\cacert.pem`

   PKCS#12 格式：

   將每一個主要憑證以個別的檔案新增至以下目錄：

   UNIX： `ca-cert-p12-dir = lib/certs/ca_p12`

   Windows： `ca-cert-p12-dir = lib\certs\ca_p12`

   註: 這些 PEM 格式與 PKCS#12 格式的憑證，皆是 Policy Director 所信任之憑證管理中心的憑證。
3. 設定 **verify-clients** 參數，藉以指定 WebSEAL 如何處理從屬站端 X.509 憑證。請在 iv.conf 配置檔的 `[wand]` 段落中，輸入 verify-clients 的容許值之一：never、optional 或 required。

   這些值的說明請參閱第152頁的『配置憑證處理』。
4. 將 WebSEAL 配置成使用 CAS 伺服器；方法是編輯 iv.conf 檔，並視需要根據您的適當平台來變更 [authentication-mechanisms] 段落中的 **cert-cdas** 參數：

   ```
   [authentication-mechanisms]
   cert-cdas = &entry=/.:/subsys/intraverse/cdas/servers/hostname
   ```

   cas module 的選項包括：cdasauthn.dll（若爲 Windows NT）、libcdasauthn.a （若爲 AIX）與 libcdasauthn.so（若爲 Solaris）。

   有關 **cert-cdas** 參數的詳細說明，請參閱第164頁的『基本 Policy Director CAS 配置』。
5. 使用 secmgrd.conf 配置檔中的 **certificate-file** 與 **key-file** 參數，定義伺服器身份。請注意：伺服器私密金鑰採 PEM 格式。參數因您所用的平台而異：

   PEM 格式下的 certificate-file 參數：

   UNIX： `certificate-file = /opt/intraverse/lib/certs/svrcert.pem`

   Windows： `certificate-file = C:\Program Files\ibm\Policy Director\lib\certs\svrcert.pem`

   PEM 格式下的 key-file 參數：

   UNIX： `key-file = /opt/intraverse/lib/certs/srvkey.pem`

Windows： `key-file = C:\Program Files\ibm\Policy Director\lib\certs\srvkey.pem`

有關 secmgrd.conf 憑證儲存參數的說明，請參閱第151頁的『儲存憑證』。

6. 使用 secmgrd.conf 配置檔中的 certificate-file 參數，定義伺服器身份。請注意：伺服器憑證採 PKCS#12 格式。

   PKCS#12 格式下的 certificate-file 參數：

   UNIX： `certificate-file = /opt/intraverse/lib/certs/svrcert.p12`

   Windows： `certificate-file = C:\Program Files\ibm\Policy Director\lib\certs\svrcert.p12`

7. 使用「Policy Director 證明獲取服務程式 (CAS)」，來進行證明的獲取與對映。

   或者，您可以在伺服器系統上撰寫及安裝您自己的證明獲取及對映服務程式。請參閱*Policy Director 程式設計及參考手冊*及『配置「Policy Director 證明獲取服務程式」』以取得進一步資訊。

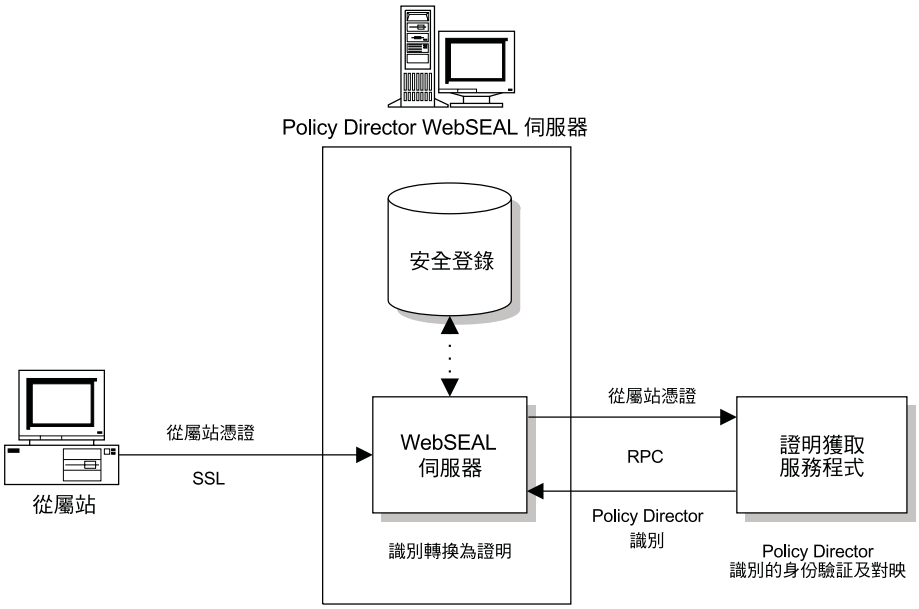
配置「Policy Director 證明獲取服務程式」

Policy Director「證明獲取服務程式」(CAS) 是可自訂的元件，可以用來延伸 WebSEAL 所支援的標準身份驗證機制。預設的「Policy Director 證明獲取服務程式」使用 cdas_server(.exe) 檔。請參照 第164頁的『將 WebSEAL 配置成使用 Policy Director CAS』。

或者，您可以在伺服器系統上撰寫及安裝您自己的證明獲取及對映服務程式。有關撰寫與安裝證明獲取服務程式的說明，請參閱 *Policy Director 程式設計及參考手冊*。

介紹 Policy Director CAS

「Policy Director 證明獲取服務程式 (CAS)」可鑑定使用者身份資訊（像是 X.509 憑證）並對映至 Policy Director 使用者身份。「安全管理程式」（使用其預設登錄）會傳回這個身份的證明。



有關 Policy Director CAS 資訊，請參閱第28頁的『Policy Director 中提供的 CAS』與『將 WebSEAL 配置成使用 Policy Director CAS』。

將 WebSEAL 配置成使用 Policy Director CAS

您可以在 iv.conf 配置檔的 authentication-mechanisms 段落中，配置 WebSEAL 所支援的全部身份驗證機制。WebSEAL 所支援的全部身份驗證機制代表 CAS 伺服器使之生效的本端（程序中）身份驗證程式及所有自訂遠端身份驗證程式。

本端外掛程式模組

在配置檔中，您可以將每一個身份驗證程式和本端外掛程式模組連結。 在 UNIX 平台上，這些模組是共用檔案庫。在 Windows NT 上，這些模組是「動態鏈結程式庫」（DLL）。這些模組屬於 Policy Director 分送中的標準組件，且無法讓您自訂。

Policy Director 提供一個標準的外掛程式模組。使用這個標準的外掛程式模組來作爲與任何協力廠商 CAS 伺服器之間的介面：

平台	CAS 模組名稱
Solaris	libcdasauthn.so
AIX	libcdasauthn.a
Windows NT	cdasauthn.dll

基本 Policy Director CAS 配置

您可以配置一個用以回應 X.509 憑證資訊的「Policy Director 證明獲取服務程式」，以實行 WebSEAL CAS 介面的從屬站端身份驗證工作。 Policy Director CAS 配置需用到一個額外的引數，以指出 CAS 伺服器連結資訊儲存在 DCE CDS 名稱空間中的位置。

如要將 WebSEAL 配置成使用 CAS 伺服器，請編輯 iv.conf 檔，並視需要根據您的適當平台，變更 [authentication-mechanisms] 段落中的 cert-cdas 參數。

例如，下列的配置順序（Windows NT 方面）定義出支援 X.509 憑證身份驗證方式的單一 CAS 伺服器：

```
[authentication-mechanisms]
cert-cdas = cdasauthn.dll&entry=/.:/subsys/intraverse/cdas/servers/hostname
```

其中 cdasauthn.dll 代表適當平台的 CAS 模組， *hostname* 爲簡單的主電腦名稱，&entry=/.:/subsys/intraverse/cdas/servers/*hostname* 代表 CAS 伺服器連結資訊儲存在 DCE CDS 名稱空間中的位置。

配置項目語法

身份驗證配置項目使用以下格式：

authn-mechanism = *module*[&*arg1*[*arg2*]...[*argN*]]

多個 Policy Director CAS 伺服器

單一「Policy Director 證明獲取服務程式」可支援一個以上的身份驗證機制。在這種情形下，每一個機制都具有重複的配置資訊。

識別名稱對映

Policy Director CAS 會將瀏覽器（啓用 SSL）提供的*從屬站數位憑證*對映至 Policy Director 使用者身份。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。 Policy Director CAS 會試著將收到的憑證對映至 Policy Director 所知的使用者身份。

在 Policy Director CAS cdas.conf 配置檔中， Policy Director 管理者可建立一份表格，讓憑證的識別名稱 (DN) 連結 Policy Director 使用者的 DN。當 WebSEAL 拿著憑證呼叫 Policy Director CAS 時， CAS 會先擷取憑證中的 DN，並在表格中尋找相符項。如找到相符項， 「Policy Director 證明獲取服務程式」會將 Policy Director 使用者的正確 DN 格式，傳回給 WebSEAL。這個方法亦稱爲 *DN 對映*。

之後，WebSEAL 即以這個 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。

用以對應識別名稱的 cdas.conf 配置檔可在下列中找到：

UNIX: /opt/intraverse/cdas_server/lib/cdas.conf

Windows: C:\Program Files\IBM\Policy Director\cdas_server\lib\cdas.conf

cdas.conf 配置中含有下列資訊：

```
# DN mapping
# If the certificate DN is in the following table, use the corresponding LDAP
# DN.  Otherwise, use the certificate DN as is.
# Each entry should be on a single line with the following format:
# [DN in the certificate]LDAP DN to map to
```

```
# For example:
# [/C=US/O=IBM/CN=Policy Director User] cn=Policy Director User,o=IBM,c=US
# [/C=US/O=IBM/CN=User1] cn=IBM Policy Director User,o=IBM,c=US
```

憑證識別名稱 (DN) 固定位於表格左邊，且會括在方括弧中：`[/C=US/O=IBM/CN=Policy Director User]`。Policy Director 使用者的 DN（與 LDAP 登錄 DN 一樣）固定位於表格右邊：`cn=Policy Director User,o=IBM,c=US`。Policy Director 使用者的 DN 固定跟在憑證 DN 右方括弧 ( ]) 之後，且兩者間必須空一格。對映表項目兩邊皆必須完成，才能適當運作。

啓用 SSL 的瀏覽器（如 Netscape® Communicator/Netscape Navigator® 與 Microsoft Internet Explorer™）可讓您檢視憑證 DN 資訊。這些瀏覽器中顯示的 DN 資訊可能不同；但這兩種瀏覽器中的憑證資訊應該都含有所有的識別名稱元素。

第14章 WebSEAL：一般管理作業

本章包含的資訊說明了爲您的網路自訂 WebSEAL 時，您可以執行的一般管理作業及配置作業。

本章包括：

啓用及停用 WebSEAL 安全性

請使用 **ivadmin** 公用程式來啓用及停用 WebSEAL。

在特定 Policy Director 伺服器上啓用 WebSEAL：

```
ivadmin> server enable /WebSEAL/
```

其中 *hostname* 是伺服器名稱，但是不含領域名稱

當服務程式已經啓用，或者服務程式指定無效， Policy Director 會傳回錯誤。

根據預設，Policy Director 會啓用 WebSEAL。

如要在特定 Policy Director 伺服器中停用 WebSEAL，請使用 **ivadmin server disable** 指令：

```
ivadmin> server disable /WebSEAL/
```

如果要檢查 WebSEAL 伺服器狀態，請使用 **ivadmin server status** 指令：

```
ivadmin> server status hostname
```

狀態報告會顯示以下資訊：

- WebSEAL 伺服器已啓用或停用。
- WebSEAL 伺服器是否可偵測到（Ping）。
- WebSEAL 配置資料庫的狀態。

管理 Web 空間

本節說明管理 WebSEAL 名稱空間所需的作業，包括：

指定 Web 文件樹的位置

Web 文件樹的位置是指伺服器所提供的文件之文件樹根的絕對路徑。預設位置是在安裝「安全管理程式」期間所建立：

UNIX： *install-path*/www/docs

Windows： *install-path*\www\docs

您可以透過安裝 Script 來變更這個位置。安裝後，您必須使用 **junctioncp** 公用程式來變更這個位置。有關完整的指令資訊，請參閱第181頁的『使用 junctioncp 來管理智慧型接合』。

下列的 UNIX 範例說明如何使用 **junctioncp** 公用程式來變更位置：

1. 執行 **junctioncp**：

```
# junctioncp -e hostA
嘗試連接到 hostA 於
/.:/subsys/intraverse/secmgr/server/hostA
junctioncp>
```

2. 使用 **list** 指令來顯示所有現行的接合點：

```
junctioncp> list
/
```

3. 使用 **show** 指令來顯示接合的明細：

```
junctioncp> show /
接合點：/
類型：本端根
目錄：/opt/intraverse/www/docs
```

4. 建立一個新的本端接合來取代現行接合點：

```
junctioncp> create -t local -d /tmp/docs /
警告：junction 已存在於 /
您是否要取代它 [no]？yes
接合已建立於 /
```

5. 列出新的接合點：

```
junctioncp> list
/
```

6. 顯示此接合的明細：

```
junctioncp> show /
接合點：/
類型：本端根
目錄：/tmp/docs
```

配置目錄索引

您可以指定伺服器所傳回的預設檔名稱。當您提供目錄名稱作爲 URL 時，就會指定這個名稱。當檔案存在時，Policy Director 會將這個預設檔傳給從屬站。如果檔案不存在，Policy Director 會以動態方式產生目錄索引並將它傳給從屬站。

註: Policy Director 不會將產生的索引儲存至磁碟。 Policy Director 會從伺服器的 wand 或 dirindex 快取擷取索引，或是在每次存取目錄時重新產生索引。

配置目錄索引的參數是位於 iv.conf 配置檔的 [wand-indexing] 段落。

預設檔的值是：

```
[wand-indexing]
dirindex = index.html
```

如果您的站台使用不同的慣例，您將必須變更這個檔名：

```
[wand-indexing]
dirindex = default.html
```

用於索引目錄的每一個參數都有一個預設圖示（.gif 檔），每次找到文件類型及 MIME 類型時就會顯示圖示：

```
[wand-indexing]
image/*= /icons/image2.gif
video/* = /icons/movie.gif
audio/* = /icons/sound2.gif
text/html = /icons/html.gif
text/* = /icons/text.gif
application/* = /icons/binary.gif
```

您可以爲每一個參數指定其他圖示。同時，您可以從遠端找到圖示，也可以使用 URL 作爲參數值。例如：

```
application/* = http://www.acme.com/icons/binary.gif
```

指定 CGI 程式的檔案副檔名類型

iv.conf 配置檔的 [wand-cgi-types] 段落中所含的參數，可讓您指定 Windows 副檔名類型。 Policy Director 會辨識可以 CGI 程式啓動的 Windows 副檔名類型。

UNIX 作業系統沒有副檔名的需求。然而，您必須爲 Windows NT 定義副檔名類型。[wand-cgi-types] 段落會列出全部有效的副檔名類型，並且在必要時將每一個副檔名對映到適當的 CGI 程式。

根據預設，Policy Director 只會將其副檔名與段落中所列的副檔名相符的檔案啓動成 CGI 程式。 根據預設，Policy Director 會將副檔名爲 .exe 的檔案啓動爲程式，而這些檔案不需要對映。 您必須爲代表解譯 Script 檔的副檔名提供適當的解譯程式。副檔名類型的範例有：Shell script（.sh 與 .ksh）、Perl script (.pl) 與 Tcl script (.tcl)。

以下範例說明典型的 [wand-cgi-types] 段落配置：

```
#
# CGI 副檔名對指令的對映（限 Windows NT）
#
# 若是 WIN32 伺服器，我們提供 CGI 副檔名以及用來執行它們的程式。
# 如果 CGI 的副檔名不在
# 這份清單中，則不會執行它。
#
[wand-cgi-types]
.exe =
.bat =
.cmd =
.pl = perl
.sh = sh
.tcl = tclsh76
```

註: 使用 .bat 檔牽涉到許多嚴重的安全課題。 請勿使用 .bat 檔。

配置 HTTP 及 HTTPS 工作者緒

已配置的工作者緒數目會指定伺服器可服務的並行進入要求數目。當所有的工作者緒都在忙碌時， Policy Director 會將其他抵達的連線置於緩衝區中，直到有工作者緒可用爲止。

您可以設定可提供服務給進入連線的緒數目。請小心配置工作者緒的數目，因爲可能會對效能產生影響。

這個配置參數不會對同時連線的數目強制上限。這個參數只會指定服務無限制的工作佇列時可用的緒數目。

爲了選擇最佳的工作者緒數目，您必須瞭解您網路流量的數量及類型。

一般而言，藉由增加緒的數目，您就會減少完成要求所需的平均時間。然而，增加緒的數目會影響其他因素，可能會對您的效能有不良的影響。

設定 WebSEAL 的工作者緒儲存池值

WebSEAL 會維護一個單一、同屬的工作者清單，亦會維護一個工作者緒儲存池，以處理從屬站使用 TCP、SSL 通道機制或 GSS 通道機制所提出的要求。這項強化機制可讓 WebSEAL 在處理更重大的負載時，使用較少的系統資源。

您可以設定 iv.conf 配置檔 [wand] 段落部分的 worker-threads 參數，來控制工作者緒儲存池大小。

```
worker-threads = 50
```

配置 WebSEAL 以處理 HTTP 要求

WebSEAL 通常會處理來自未經身份驗證的使用者的許多 HTTP 要求。例如，建議您容許不明的（未經身份驗證）使用者以唯讀方式存取公用網站上的選取題材。

iv.conf 配置檔中的 [wand] 段落包含了處理透過 TCP 進行的 HTTP 要求的參數。

啓用及停用 HTTP 接收

根據預設，Policy Director 會啓用（容許）接收透過 TCP 進行的 HTTP 要求：

```
allow-tcp-http = yes
```

將參數值設定成 no 會停用 HTTP 接收。

設定埠值

透過 TCP 監聽的 HTTP 的預設埠是 80：

```
http-tcp-port = 80
```

如果要變更至埠 8080，設定：

```
http-tcp-port = 8080
```

配置 WebSEAL 以處理 HTTPS 要求

iv.conf 配置檔的 [wand] 段落包含了處理透過 SSL 進行的 HTTPS 要求的參數。

啓用及停用 HTTPS 接收

根據預設，Policy Director 會啓用（容許）接收透過 SSL 進行的 HTTPS 要求：

```
allow-ssl-http = yes
```

將參數值設定成 no 會藉由接收來停用 HTTPS。

設定埠值

透過 SSL 接收所進行的 HTTPS 的預設埠是 443：

```
ssl-port = 443
```

如果要變更至埠 4343，設定：

```
ssl-port = 4343
```

指定逾時參數

可設定的 Policy Director 逾時參數如下：

- 設定 HTTP 通信的逾時參數
- iv.conf 配置檔之 [wand] 段落中的其它 WebSEAL 伺服器逾時參數

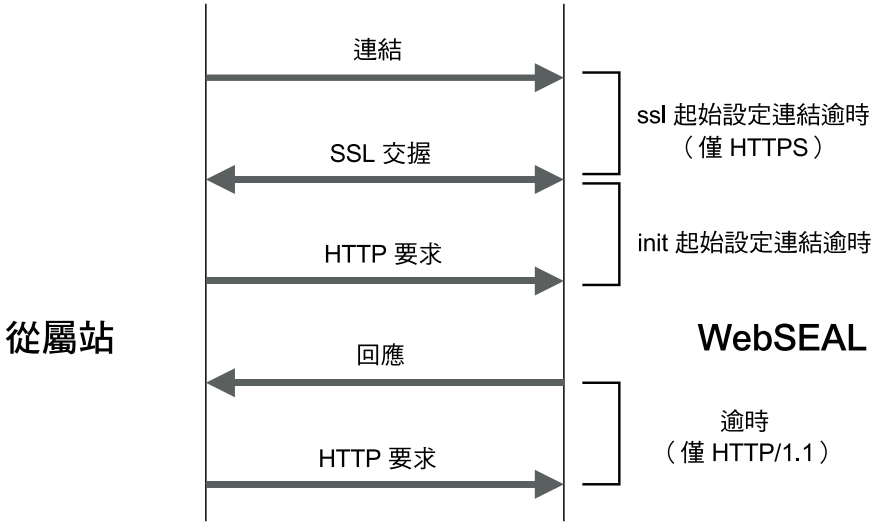
HTTP 通信的逾時參數

WebSEAL 支援以下的 HTTPS 通信逾時參數：

ssl-init-connect-timeout（限 HTTPS）
當 WebSEAL 接受來自瀏覽器的 SSL 連線時，必須發生 SSL 通信協定交握。交握是指交換信號以設定兩個數據機之間的通信的程序。這個參數控制「安全管理程式」等待 SSL 瀏覽器起始 SSL 交握的時間長度。這個起始設定會發生在 SSL 連線開始時，以及關閉連線之前。

init-connect-timeout
在 SSL 交握發生後，這個參數會指定 WebSEAL 等待起始 HTTP 要求的時間。這個連線可能是 HTTP、HTTPS 或 NetSEAT（HTTP 及 GSS）。

tcptimeout
這個參數是 HTTP/1.1（非 HTTP/1.0）連線特有的參數。在第一個 HTTP/1.1 要求以及伺服器回應之後，這個參數會控制伺服器保持 HTTP/1.1 持續連線開啓的最大秒數。在到達最大秒數後就會關閉連線。



參數	配置檔	預設值 （秒）
ssl-init-connect-timeout	secmgrd.conf [ssl] 段落	120
init-connect-timeout	iv.conf [wand] 段落	120
tcptimeout	iv.conf [wand] 段落	5

其他的 WebSEAL 伺服器逾時參數

iv.conf 配置檔的 [wand] 段落是您設定以下逾時值的地方：

參數	說明	預設值 （秒）
tcp-junction-timeout	透過 TCP 接合，讀取與傳送至後端伺服器的逾時時間。	120
ssl-junction-timeout	透過 SSL 接合，讀取及傳送到後端伺服器的逾時時間。	120
cgi-timeout	讀取及傳送到本端 CGI 程序的逾時時間。	120
junction-ping-time	WebSEAL 會對每一個接合的伺服器執行定期背景偵測（Ping），不管伺服器是否正在執行中。 WebSEAL 最多每隔 300 秒（或任何設定的值）會嘗試執行一次。	300

配置 HTTP 錯誤訊息

有時候 WebSEAL 伺服器會嘗試提供服務給要求，但是會失敗。這類失敗可能有許多原因。例如：

- 檔案不存在。
- 許可權設定禁止存取。
- 不正確的 UNIX 檔案許可權或類似情況，使 CGI 程式無法啓動。

發生無法提供服務給要求的情況時，伺服器會以 HTML 錯誤頁面將錯誤訊息傳回給瀏覽器，例如 403 Forbidden。錯誤訊息有好幾種。 每一個訊息都儲存在個別的 HTML 檔案中。

以下的目錄包含這些檔案：

UNIX：

install-path/www/lib/errors/*locale-dir*

Windows：

install-path\www\lib\errors/*locale-dir*

errors 目錄包含許多語言環境子目錄。子目錄包含錯誤訊息檔的本土化版本。

這個目錄中的訊息是使用 HTML 格式，所以它們可以正確顯示在瀏覽器中。您可以編輯這些 HTML 頁面來自訂它們的內容。檔名是作業失效時傳回的內部錯誤碼的十六進位值。請勿變更這些檔名。

下表包含某些常見錯誤訊息的檔名及內容清單：

檔名	標題	說明	HTTP 錯誤碼
1354a2fa.html	非空白的目錄	所要求的作業需要移除非空的目錄。 這項作業不符規定。	
1898d25a.html	無法登入使用者	所要求的資源需要 WebSEAL 伺服器將使用者登入另一個 Web 伺服器。不過，當 WebSEAL 試著擷取資訊時卻發生問題。	
1898d25b.html	使用者無單一登入資訊	WebSEAL 找不到所要求資源的 GSO 使用者。	
1898d25c.html	缺乏使用者的單一登入目標	WebSEAL 找不到所要求資源的 GSO 目標。	
1898d25d.html	使用者有多個登入目標	爲所要求的使用者定義了多個 GSO 目標。GSO 目標檔配置錯誤。	
1898d25e.html	需要登入	所要求的資源是受到接合後端 Web 伺服器的保護，需要 WebSEAL 將使用者登入至該 Web 伺服器。如要登入，使用者必須先登入 WebSEAL。	
1898d25f.html	無法登入使用者	所要求的資源需要 WebSEAL 伺服器將使用者登入另一個 Web 伺服器。不過，使用者帳戶的登入資訊不正確。	
1898d260.html	非預期的身份驗證深入問題	WebSEAL 從接合的後端 Web 伺服器接收到非預期的身份驗證深入問題。	
1898d421.html	暫時移動	所要求的資源已經暫時移走，這通常是因爲錯誤的重新導向而發生。	302
1898d424.html	要求不正確	WebSEAL 收到無效的 HTTP 要求。	400
1898d425.html	需要登入	您所要求的資源是由 WebSEAL 保護，如要存取該資源，您必須先登入。	
1898d427.html	禁止	使用者沒有許可權存取所要的資源。	403
1898d428.html	找不到	找不到所要求的資源。	404
1898d432.html	服務程式無法使用	WebSEAL 完成要求所需的服務程式目前無法使用。	503

1898d437.html	伺服器已暫停	「系統管理者」暫停了 WebSEAL 伺服器。在「管理者」讓伺服器返回服務狀態前，將無法處理任何要求。	
1898d439.html	階段作業資訊遺失	瀏覽器及伺服器間的交互作用，是與接合的後端伺服器之間的*有狀態的階段作業*，但是該伺服器已不再做出回應。WebSEAL 需用位於這個伺服器上的服務程式才能完成您的要求。 請參閱第186頁的『維護狀態（-s 選項）』。	
1898d7af.html	CGI 程式失敗	CGI 程式無法適當地執行。	
default.html	伺服器錯誤	因爲異常錯誤，WebSEAL 無法完成您的要求。	500

巨集支援

以下的巨集可用於自訂的 HTML 錯誤訊息頁面。巨集可以動態方式替代適當的可用資訊。

巨集	說明
ERROR_CODE	錯誤碼的數值。
ERROR_TEXT	與訊息型錄錯誤碼中的相關的文字。
METHOD	從屬站所要求的 HTTP 方法。
URL	從屬站所要求的 URL。
HOSTNAME	完整的主電腦名稱。
HTTP_BASE	伺服器的基礎位置 HTTP URL `http://`*`host`*`:`*`tcpport`*`/`
HTTPS_BASE	伺服器的基礎位置 HTTPS URL：`https://`*`host`*`:`*`sslport`*`/`
REFERER	來自要求的參照者標頭值或 `Unknown`（如果沒有的話）。
BACK_URL	來自要求的參照者標頭值或 `/`（如果沒有的話）。
BACK_NAME	如果要求中出現參照標頭，則爲 `BACK` 值，若未出現則是 `HOME`。

第15章 WebSEAL：智慧型接合管理

WebSEAL 可以作爲基本的獨立式 Web 伺服器或作爲接合伺服器，以便爲後端應用伺服器提供身份驗證及權限服務程式。WebSEAL 的主要優點是能整合及保護後端應用伺服器上的其他 Web 資源。 WebSEAL 使用「智慧型接合」技術，整合並保護 Web 資源。

本章包含：

使用 WebSEAL 作為智慧型接合伺服器

Policy Director 提供網路的身份驗證、授權及管理服務程式。在 Web 型的網路中，這些服務程式最好是由前端 WebSEAL 伺服器來提供。前端 WebSEAL 伺服器可保護位於後端應用伺服器的 Web 資源。

WebSEAL 伺服器與後端伺服器之間的連線稱爲*智慧接合*或接合。使用接合來合併 WebSEAL 以及後端伺服器的實體 Web 空間，以建置單一的邏輯 Web 空間表示。

從屬站不必知道 Web 資源的實體位置。 WebSEAL 會將邏輯 URL 位址轉換成後端伺服器可接受的實體位址。您可以將 Web 物件從伺服器移至另一個伺服器，而不會影響從屬站定址這些物件的方式。

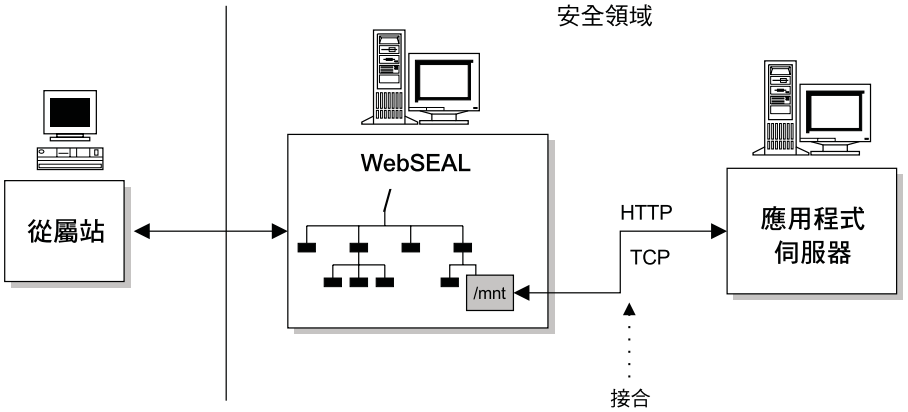
作爲接合伺服器，WebSEAL 可以對所有的要求執行身份驗證及授權檢查，然後再將這些要求傳送到後端伺服器。接合能提供一個可調整而安全的環境，以容許負載平衡、高度有用性，以及狀態管理等功能--這些都是以透通方式對從屬站來執行。 對名稱空間採取集中式管理可嘉惠管理者。

大部分的商業 Web 伺服器無法定義邏輯 Web 名稱空間。反之，它們的存取控制是連接到實體檔以及目錄結構。智慧型接合可以透通方式定義名稱空間，以反映組織結構（而非實體機器）和標準 Web 伺服器常見的目錄結構。

智慧型接合可讓您建立單一登入解決方案。不論資源的位置爲何，單一登入配置可讓使用者只利用一次初始登入來存取資源。從後端伺服器的任何進一步登入要求，對使用者而言都是以透通方式來處理。

瞭解智慧型接合

*智慧型接合*是介於前端 WebSEAL 伺服器以及後端應用伺服器之間的一種實體 TCP/IP 連線。後端伺服器可以是另一部 WebSEAL 伺服器或協力廠商應用伺服器。 後端應用程式 Web 空間會在 WebSEAL Web 空間中特別指定的 *接合點*（裝載點）*連接* WebSEAL 伺服器。

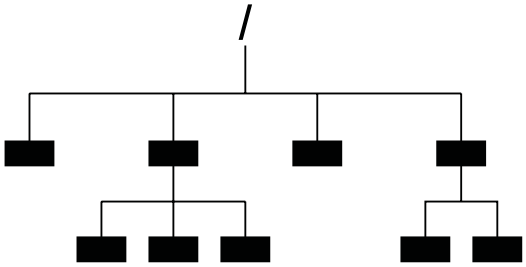


智慧型接合可讓 WebSEAL 代表後端應用伺服器來提供保護性服務程式。後端伺服器對於其物件需要精密的存取控制。當它要求這個控制時，您必須執行其他的配置步驟來對 Policy Director 安全服務程式說明協力廠商 Web 空間。

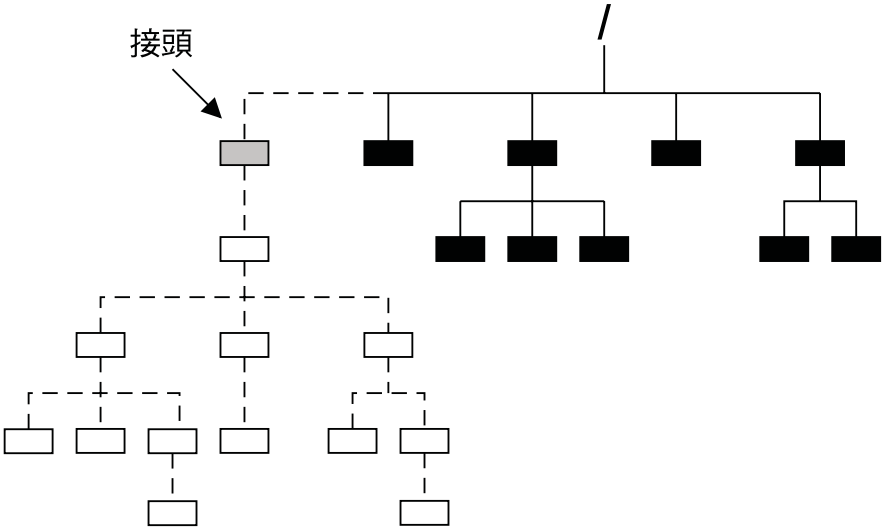
配置正確時，WebSEAL 會保護它自己的資源以及接合的伺服器上的資源，方法是執行如身份驗證、授權及審核之類的安全服務程式。

智慧型接合可提供一個附加價值，也就是以邏輯方式將 WebSEAL 伺服器的空間與後端伺服器的 Web 空間合併。合作的伺服器之間的接合會導致一個單獨、統一的分散式 Web 空間，這對於使用者而言是透通而無縫的。

統一的 Web 空間可簡化系統管理者對於所有資源的管理。其他管理方面的優點包括可調整性、負載平衡和高度有用性。



WebSEAL Web 空間



結合 Web 空間：
WebSEAL 加上接合的伺服器

智慧型接合對於網站的可調整性而言是非常重要的工具。接合可讓您藉由連接伺服器來回應網站不斷增加的需求。

智慧型接合及網站的可調整性

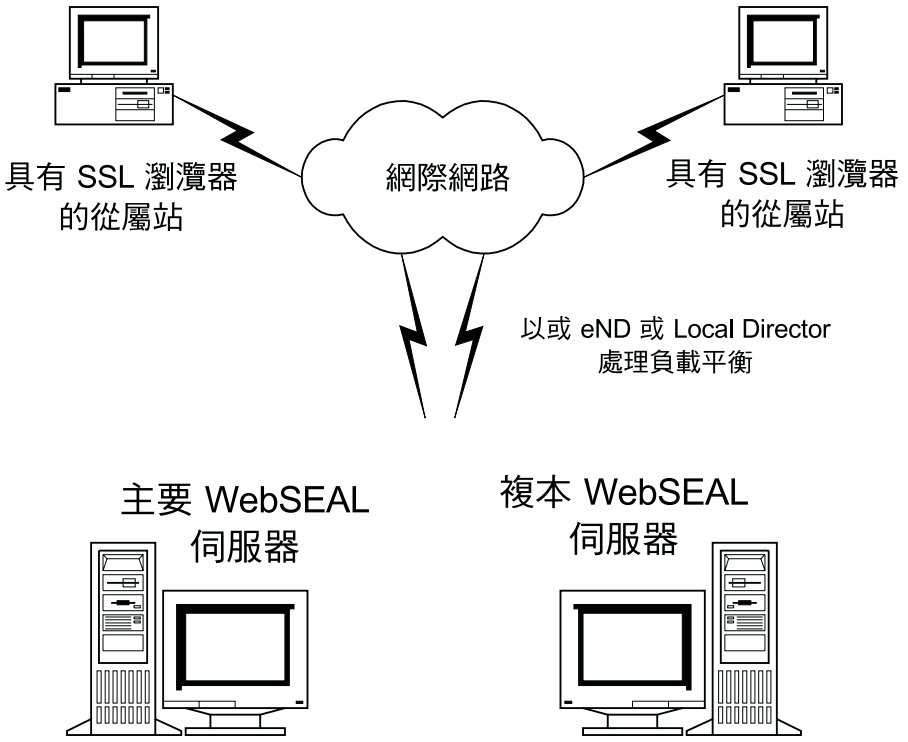
請使用智慧型接合來建立一個可調整的網站。當網站的需求增加時，您可以輕易新增其他的伺服器來擴充網站的功能。您可以根據以下的理由來新增額外伺服器：

- 想增加內容擴充網站
- 想複製現存內容，以達負載平衡、失效接手及高度有用性功能。

複製的前端 WebSEAL 伺服器

後端伺服器的接合支援是至少從一個前端 WebSEAL 伺服器開始。複製的前端 WebSEAL 伺服器可在需求量大的期間爲站台提供負載平衡。應用程式（如 Policy Director eND 或 Cisco Local Director）負責處理負載平衡機制。

前端複製也可以爲站台提供免於失敗功能。如果伺服器因爲某些原因失效，剩餘的複本伺服器會繼續提供對站台的存取。順利完成的負載平衡及免於失敗功能可爲站台使用者提供高度有用性。



複製前端 WebSEAL 伺服器時，必須記住兩個關鍵點：

- 每一個伺服器必須包含一個 Web 空間副本。
- 您必須複製使用者帳戶資料庫以進行持續的身份驗證。

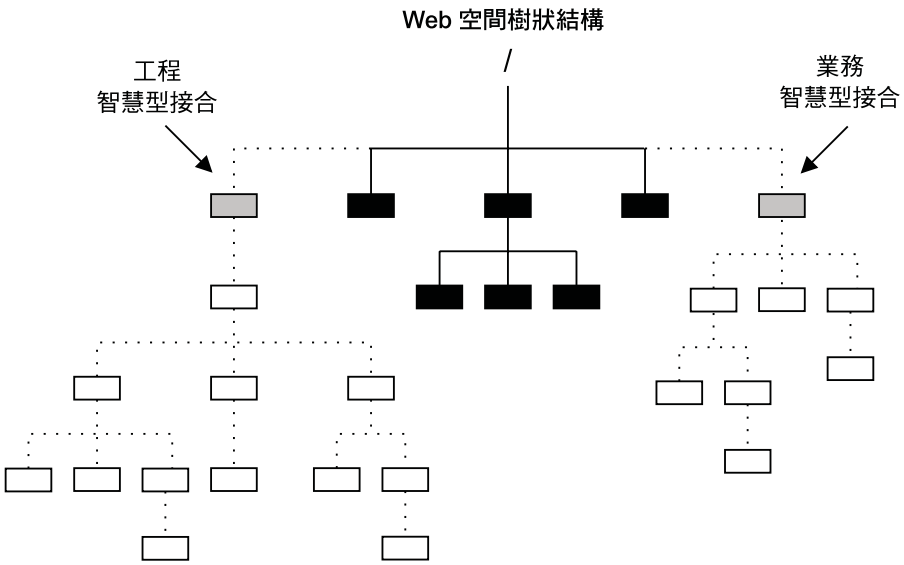
必要時，「Policy Director 權限服務程式」會自動複製授權資料庫資訊。

支援後端伺服器

WebSEAL 伺服器本身、後端伺服器或 WebSEAL 伺服器與後端伺服器組合，都可以提供網站內容的服務。後端伺服器的智慧型接合支援可讓您透過附加的內容及資源來調整網站的大小。

每一個唯一的後端伺服器必須接合到個別的接合（裝載）點。當附加內容及資源的需求成長時，請使用智慧型接合來新增其他的伺服器。這個實務爲投資大量協力廠商 Web 伺服器的現有網路提供了一個解決方案。

下圖說明智慧型接合如何提供統一的邏輯 Web 空間。這個 Web 空間對於使用者而言是透通的，並且容許集中式的管理。



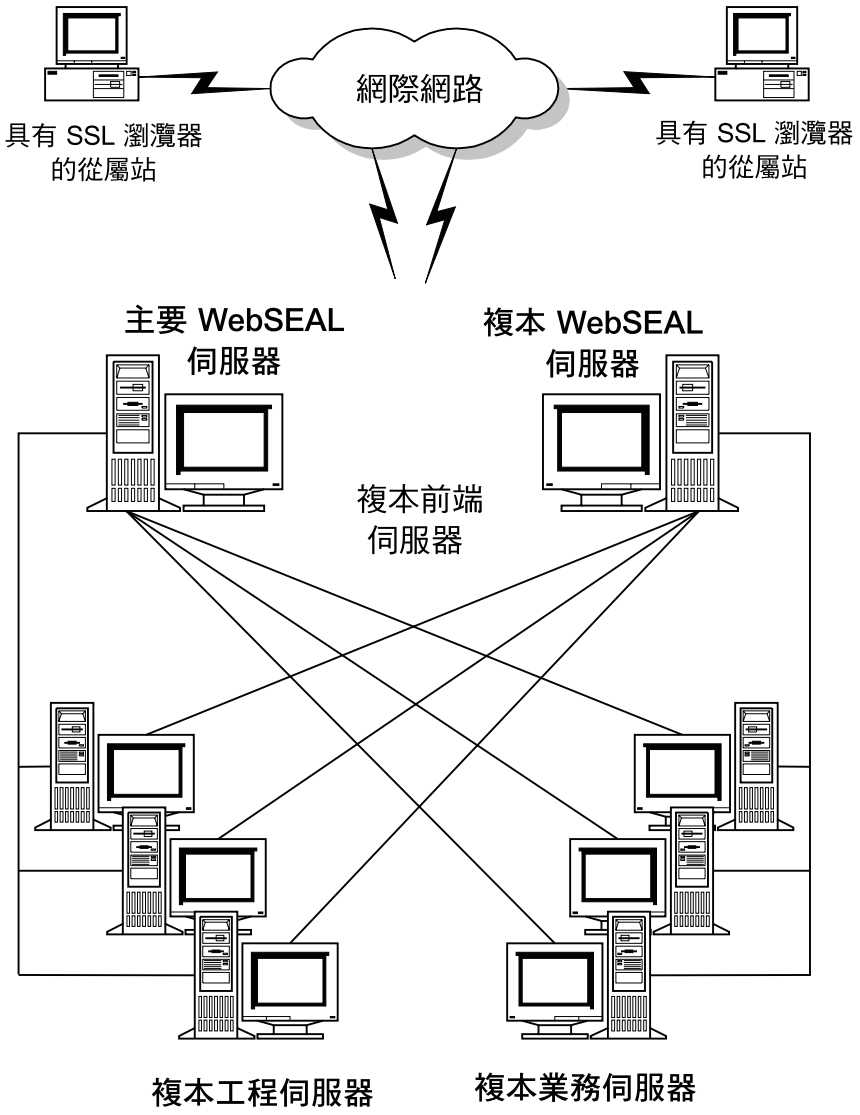
如同『複製的後端伺服器』中所論及，複製的後端伺服器是接合到相同的接合點。

複製的後端伺服器

如果要擴充後端伺服器配置的可調整特性，您可以複製後端伺服器。複製的前端伺服器可以這麼做，但複製的後端伺服器必須包含屬於彼此鏡映影像的 Web 空間。

WebSEAL 使用 “最不忙碌”（least-busy）排程演算法，來平衡複製之伺服器間的負載。當伺服器當機，並且再次使用重新啓動之伺服器時， WebSEAL 也可以正確地免於失敗。

如果後端應用程式需要在數個頁面中維持相同的狀態，您可以使用狀態接合。*狀態接合*可確保每一個階段作業傳回給同一個後端伺服器。請參閱第186頁的『維護狀態（-s 選項）』。



建立接合的作業總結

您可以建立以下的接合類型：

- Policy Director 對協力廠商; TCP 連線
- Policy Director 對協力廠商; SSL 連線
- Policy Director 對本端檔案系統

以下的步驟總結了將後端應用程式 Web 空間接合到 WebSEAL Web 空間時，必須執行的作業：

1. 決定在 WebSEAL Web 空間中接合（裝載）額外伺服器的地方。
2. 決定確保網路的完整性時所需的安全條件。

粗略的存取控制

如要提供粗略的存取控制請：

1. 使用 Policy Director **junctioncp** 公用程式，在後端協力廠商應用程式 Web 空間以及前端 WebSEAL 伺服器之間建立一個智慧型接合。
2. 將適當的原則模版（ACL）置於接合點，以提供對後端伺服器的粗略控制。

精密的存取控制

如要提供細密的存取控制請：

1. 使用 **junctioncp** 公用程式，在後端協力廠商應用程式 Web 空間以及前端 WebSEAL 伺服器之間建立一個智慧型接合。

   WebSEAL 無法自動察看及瞭解協力廠商檔案系統。您必須使用 **query_contents**，通知 WebSEAL 有關協力廠商的名稱空間。這個特殊的應用程式會庫存協力廠商 Web 空間，並且將結構報告給 WebSEAL。
2. 將 **query_contents** 程式複製到協力廠商伺服器。
3. 使用「管理主控台」來將原則模版（ACL）引用至統一的 Web 空間中的適當物件。

建立智慧型接合的指引

以下指引總結了智慧型接合的規則：

- 您可以在主要 WebSEAL 名稱空間中的任何地方新增智慧型接合。
- 您可以在相同的裝載點 (接合點) 接合多個複製伺服器。
- 在同一接合點裝載的多個複本伺服器必須屬於同一類型（TCP 或 SSL）。
- 您不能連鎖協力廠商伺服器（如：Policy Director - 協力廠商 - 協力廠商）。

存取控制及管理專用權

根據預設，Cell 管理者帳戶對於整個 Web 空間具有完整的權利，其中包括接合的伺服器。接合伺服器的管理者只會爲該伺服器維護 Web 空間。 必要時，這個管理者可以從 Cell 管理者移除伺服器的管理專用權。

Policy Director 會跨越智慧型接合，將 ACL 承接到協力廠商伺服器。

使用 junctioncp 來管理智慧型接合

使用 **junctioncp** 公用程式來執行所有的接合管理作業：

- 建立新的接合點
- 新增伺服器至接合點
- 從接合點移除伺服器
- 刪除接合點
- 顯示接合點清單
- 顯示接合明細

junctioncp 公用程式提供一個交談式指令提示，讓您執行接合作業。

在啓動 **junctioncp** 之前，您必須以管理使用者的身份登入安全領域。您可以在 UNIX 或 Windows 環境中使用 dce_login。 您可以在 Windows 環境中使用 netseat_login。

啓動 **junctioncp** 公用程式，並且加上 **-e** 選項，來指定您要執行接合作業的伺服器（主電腦名稱）。 此時會出現 **junctioncp** 指令提示。

例如：

UNIX：

```
#
# junctioncp -e server-name
junctioncp>
```

Windows：

```
junctioncp -e <server-name>
junctioncp>
```

使用 junctioncp 指令

以下的指令可以和 **junctioncp** 一起使用：

指令	說明
create	爲起始伺服器建立新的接合。
add	新增額外的伺服器至現存的接合點。
remove	從接合點移除伺服器。
delete	移除接合點。
list	列出此伺服器上的所有接合點
show	顯示接合明細
help	列出 **junctioncp** 指令。
help *command*	顯示特定 **junctioncp** 指令的詳細說明。
exit	結束 **junctioncp** 公用程式。

請參閱『爲起始伺服器建立新的接合』這些指令以及相關選項的討論。

為起始伺服器建立新的接合

作業：建立新的接合點以及接合起始伺服器。

語法： `create -t type -h hostname options junction-point`

類型		
其中之一： • **tcp** • **ssl** • **local**		*必要的*。 定義接合的類型。 後端協力廠商伺服器請使用 **tcp**。 當您使用 **ssl** 選項時，預設的 TCP 埠會從 80 變成 443。 請參閱第187頁的『建立安全的 SSL 智慧型接合』。
選項		
	TCP 及 SSL 接合選項 （搭配使用 **-t tcp** 或 **-t ssl**）	
	-2	強制僅使用 SSL 第 2 版與後端伺服器進行通信。 請參閱第187頁的『建立安全的 SSL 智慧型接合』。

	-b *ba-value* 其中之一： • **filter**（預設值） • **ignore** • **supply** • **gso**	定義 WebSEAL 伺服器如何將身份驗證資訊傳送到後端伺服器。 請參閱第191頁的『提供身份驗證資訊給接合的伺服器』。
	-c	將 Policy Director 從屬站身份插入 HTTP 標頭。 請參閱第186頁的『插入從屬站身份資訊（-c 選項）』。
	-i	導致 WebSEAL 伺服器將 URL 視爲不區分大小寫。 請參閱第185頁的『支援不區分大小寫的 URL（-i 選項）』。
	-h *hostname*	*必要的*。 定義目標後端伺服器的主電腦名稱 (DNS)。您也可以提供它的 IP 位址。
	-p *port*	定義後端協力廠商伺服器的 TCP 埠。 TCP 接合的預設值是 80；SSL 接合的預設值是 443。
	-q *url*	定義 **query_contents** Script 的 URL。 Policy Director 會在 /cgi_bin/ 目錄中尋找 **query_contents**。 當這個目錄不同時，或者 **query_contents** 檔案已經更名，請使用這個選項來對 WebSEAL 指出檔案的新 URL。 當您爲協力廠商 Win32 伺服器建立智慧型接合時，請使用這個 **-q** 選項。請參閱第199頁的『將智慧型接合配置成尋找查詢內容』。
	-s	指定接合應支援有狀態的應用程式。根據預設，接合不是*有狀態的*。 請參閱第186頁的『維護狀態（-s 選項）』。
	-T *resource*	定義 GSO 資源證明 的應用程式資源名稱。這是必要選項，且只能搭配 **-b gso** 選項使用。 請參閱第194頁的『整合 GSO 與 WebSEAL 的單一登入』。
	-v *hostname*	定義伺服器的虛擬主電腦名稱。
	-w	定義 Win32 檔案系統支援。 請參閱第185頁的『不容許短檔名格式（-w 選項）』。
	本端及 DFS 接合選項（與 **-t dfs** 或 **local** 一起使用）	
	-d *dir*	定義分散式檔案系統（DFS）或接合的本端目錄。這是必要的。
junction-point		
	定義在 WebSEAL 名稱空間中建立接合的位置。	

新增額外的伺服器至現存的接合

作業：新增額外的伺服器現存的接合點。

語法： `add -h hostname options junction-point`

選項

	TCP 及 SSL 接合選項	
	-i	導致 WebSEAL 伺服器將 URL 視爲不區分大小寫。 請參閱第185頁的『支援不區分大小寫的 URL（-i 選項）』。
	-h *hostname*	*必要的*。 定義目標後端伺服器主電腦名稱 (DNS)。您也可以提供它的 IP 位址。
	-p *port*	定義後端協力廠商伺服器的 TCP 埠。TCP 接合的預設值是 80；SSL 接合的預設值是 443。
	-q *url*	定義 **query_contents** Script 的 URL。 Policy Director 會在 /cgi_bin/ 目錄中尋找 **query_contents**。 當這個目錄不同時，或者 **query_contents** 檔案已經更名，請使用這個選項來對 WebSEAL 指出檔案的新 URL。
	-v *hostname*	定義伺服器的虛擬主電腦名稱。
	-w	定義 Win32 檔案系統支援。 請參閱第185頁的『不容許短檔名格式（-w 選項）』。
junction-point		
	新增伺服器到這個現存的接合點。	

使用其他的 junctioncp 指令

第182頁的『爲起始伺服器建立新的接合』 以及 第183頁的『新增額外的伺服器至現存的接合』 討論了 **junctioncp create** 和 **junctioncp add** 指令。下表列出了其他可用的 **junctioncp** 指令：

指令	說明
remove	**作業**：從接合點移除後端伺服器。 **語法**： `remove -i server-id junction-point` **選項**： **-i** *server-id* 要移除的伺服器的身份。 使用 show 指令來判斷特定伺服器的 ID。
delete	**作業**：移除接合點。 **語法**： `delete junction-point`
show	**作業**：顯示接合明細。 **語法**： `show junction-point`
list	**作業**：列出所有的接合。 **語法**： `list`
help	**作業**：顯示 **junctioncp** 指令的清單。 **語法**： `help`
help *command*	**作業**：顯示特定 **junctioncp** 指令的資訊，包括可用的選項。 **語法**： `help command`

exit	**作業**：結束 **junctioncp** 公用程式並返回作業系統提示。 **語法**： `exit`

支援不區分大小寫的 URL（-i 選項）

接合協力廠商伺服器時，使用 **-i** 選項來指定 WebSEAL 不要區分 URL 的大小寫。這表示伺服器在剖析 URL 時，不會區分大小寫字元。根據預設，伺服器是區分大小寫的。

雖然大部分的 HTTP 伺服器支援 HTTP 規格（定義 URL 是區分大小寫的），某些 HTTP 伺服器會將 URL 視爲不區分大小寫。

例如，在不區分大小寫的伺服器上，您可以將這兩個 URL 視爲同一個 URL：

```
http://server/sales/index.htm
http://server/SALES/index.HTM
```

這種行爲需要 Policy Director 將相同的存取控制（ACL）置於兩個 URL 上。根據預設，在引用存取控制時， Policy Director 會將 URL 視爲區分大小寫。當使用 **-i** 選項接合某個協力廠商伺服器時， WebSEAL 會將導向該伺服器的 URL 視爲不區分大小寫。

不容許短檔名格式（-w 選項）

目標只是要限制對一個物件表示法的存取控制。不容許使用會略過安全機制的*後門*。

WebSEAL 會根據 URL 中指定的檔案路徑，針對從屬站對接合的後端伺服器的要求執行安全檢查。由於 Win32 檔案系統提供存取長檔名的兩種不同方法，這項安全檢查可能會有所妥協。

第一個方法認可整個檔名（`abcdefghijkl.txt`）。第二個方法使用舊的 8.3 檔名格式，以容許向後相容性（`abcdef~1.txt`）。

junctioncp 指令的 **-w** 選項不容許 8.3 檔名格式。使用者使用檔名的短（8.3）格式時，將無法避免長檔名上明確的 ACL。伺服器會在任何輸入的短格式檔名上，傳回一則 `403 禁止錯誤`。

Windows 會將 “foo.” 檔名看成沒有尾端之點的 “foo” 檔名。**-w** 選項會從 URL 中的檔名移除尾端的點，然後才會將要求傳送至後端伺服器。Policy Director 基礎 ACL 會檢查沒有尾端之點的檔名。

註： **-i** 選項指出 Win32 不區分大小寫的問題（`abced.txt = AbCdE.txt`）。

範例：

在 Windows NT 4.0 中，下列這些方式皆可存取到 \Program Files\ibm corp\readme.txt 檔：

1. \program files\ibm corp.\readme.txt
2. \program files\ibm corp\readme.txt
3. \progra~1\ibm~2\readm~3.txt

上述範例 1 說明 “不區分大小寫” 的結果。**-i**選項（而非 **-w** 選項）指出這個影響。

範例 2 說明 Windows NT 如何忽略了尾端的擴充點。

範例 3 說明 Windows NT 如何建立別名，以便與「磁碟作業系統 (DOS)」相容。別名的檔名中不能包含空格，而且必須符合 8.3 格式。

-w 選項指出範例 2 與 3 所說明的潛在安全漏洞。 **-w** 選項會指定 Policy Director 忽略尾端的點。此選項亦指出 Policy Director 不容許存取短檔名（亦即在這個接合伺服器的要求 URL 中使用 ~ 字元）。

維護狀態（-s 選項）

大部分啓用 Web 的應用程式會跨越每一個從屬站階段作業中所含的一系列 HTTP 要求，來維護一個*狀態*。例如，使用這個狀態來執行以下各項：

- 透過 CGI 程式所產生的資料輸入表格中的欄位，來追蹤使用者的進度。
- 在執行一系列資料庫查詢時，維護使用者的上下文。
- 當使用者隨機瀏覽並選取要購買的項目時，維護線上購物籃車應用程式中的項目清單

如同任何伺服器一樣，您可以複製執行 Web 應用程式的伺服器，以透過載入共用元件來增進效能。 Policy Director 伺服器可以提供智慧型接合給這些複製的伺服器。在此情形下，它必須確定從屬站階段作業中所含的全部要求都會轉遞到正確的伺服器。同時，根據載入平衡規則，它必須確定所有的要求不會分送到複製的伺服器之間。

根據預設，Policy Director 會藉由將要求分送到所有可用的複製伺服器，來平衡伺服器負載。Policy Director 採用 “最不忙碌” 演算法。

如要置換此負載平衡，並建立*狀態接合*，請使用 **junctioncp** 指令與 **-s** 選項。狀態接合可確保在整個階段作業期間從屬站要求皆轉遞到同一伺服器中。

插入從屬站身份資訊（-c 選項）

-c 選項可讓您將 Policy Director 特定的從屬站身份及群組成員身份資訊插入 HTTP 要求的標頭。 HTTP 要求的目的是接合的協力廠商伺服器。 Policy Director 特定的 HTTP 標頭可讓位於接合協力廠商伺服器上的應用程式執行使用者特定的動作。使用者特定的動作是根據從屬站的 Policy Director 身份。

您必須將 HTTP 標頭資訊轉換成環境變數格式，以供後端伺服器上的服務程式使用。藉由將所有的連字號（-）換成底線（_），並在字串開頭之前附加 “HTTP”，以便將標頭資訊轉換成 CGI 環境變數格式。HTTP 標頭的值會成爲新環境變數的值。

Policy Director 特定的 HTTP 標頭項目包括：

Policy Director 特定的 HTTP 標頭	CGI 環境變數格式	說明
iv-user	HTTP_IV_USER	從屬站的名稱。如果從屬站未經身份驗證（不明），則預設值爲 **Unauthenticated**。
iv-groups	HTTP_IV_GROUPS	從屬站所屬的群組清單。這是由以空格分開的項目所組成。

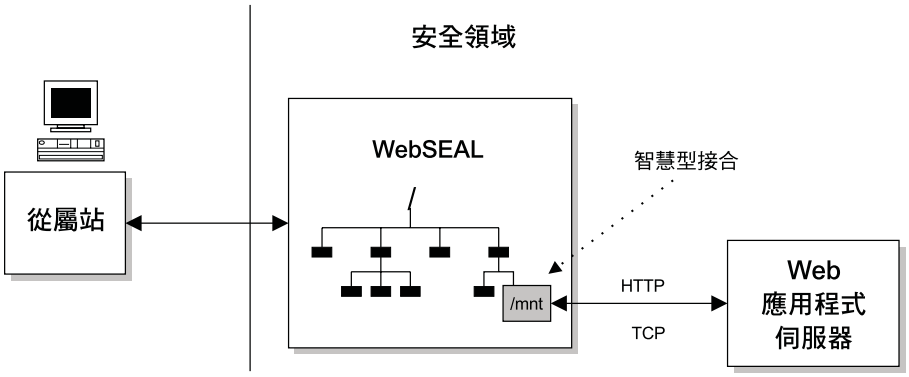
iv-creds	HTTP_IV_CREDS	代表 Policy Director 證明之已編碼的不透明資料結構。與「Policy Director 權限 API」一起使用。詳細說明請參閱 *Policy Director 程式設計及參考手冊*。

HTTP 標頭項目可讓 CGI 程式作爲環境變數 HTTP_IV_USER、 HTTP_IV_GROUP 和 HTTP_IV_CREDS 使用。若是其他的應用系統配置產品，請參閱產品文件，以取得從 HTTP 要求擷取標頭的指示。

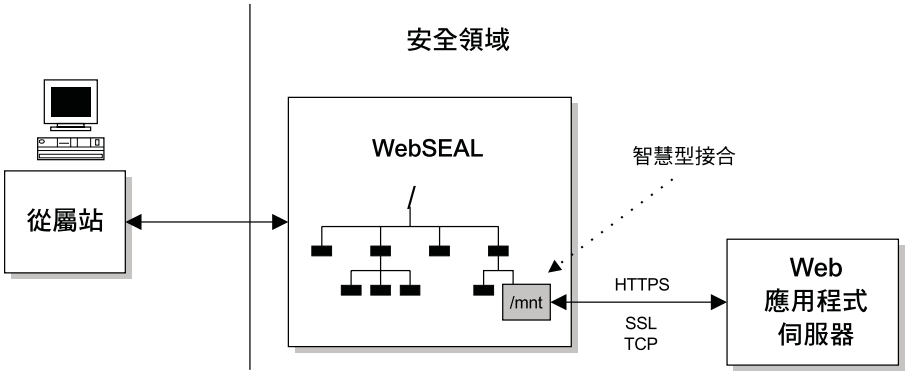
建立安全的 SSL 智慧型接合

WebSEAL 支援介於 WebSEAL 和後端伺服器之間的標準 TCP（HTTP）及安全的 SSL（HTTPS）接合。 SSL 接合功能和 TCP 接合完全相同，其附加價值在於 WebSEAL 和後端伺服器之間的所有通信都是加密的。

下圖代表不安全的 TCP (HTTP) 接合。



下圖代表安全的 SSL（HTTPS）接合。



WebSEAL 和後端伺服器之間的接合是獨立於從屬站和 WebSEAL 伺服器之間的連線類型（及其安全層次）之外。

SSL 接合可容許安全的端點對端點、瀏覽器對應用程式的交易。使用 SSL 來保護自從屬站到 WebSEAL，以及自 WebSEAL 到後端伺服器的通信。

配置安全的 SSL 接合

SSL 智慧型接合功能會要求後端 Web 伺服器必須啓用 HTTPS。

您可以使用 **junctioncp** 公用程式來建立智慧型接合。 第181頁的『使用 junctioncp 來管理智慧型接合』說明了 **junctioncp** 公用程式的明細。

如果要建立安全的 SSL 接合以及新增起始伺服器，請使用 **junctioncp create** 指令。以下範例說明了使用 create 指令來建立安全的 SSL 接合的語法：

```
junctioncp> create -t ssl [-2] -h hostname [-p port] junction-point
```

-2 選項可強制 Policy Director 僅使用 SSL 版本 2 來和後端伺服器進行通信。

通常 Policy Director 會自動協定 SSL 通信協定（版本 2 或 3）的版本。 Policy Director 引用了 **-2** 選項，因爲某些 IIS 伺服器在嘗試協議 SSL 版本 3 的時候會導致 Policy Director 失效。發生這種情形時，裝載將會失敗。強制使用版本 2 即可解決這個問題。

檢視 SSL 接合的範例

使用 SSL 通信協定，位於接合點 /sales 的接合主電腦 sales.ibm.com：

```
create -t ssl -h sales.ibm.com /sales
```

僅使用 SSL 版本 2 通信協定，位於接合點 /admin 的接合主電腦 admin.ibm.com：

```
create -t ssl -2 -h admin.ibm.com /admin
```

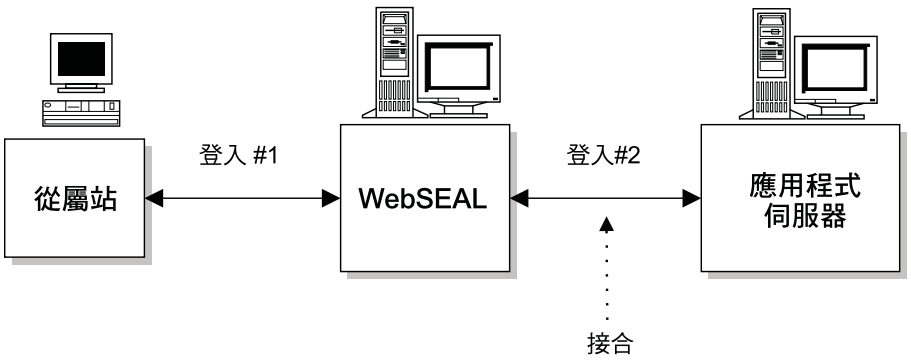
註: 在以上兩個範例中，**-t ssl** 選項指定了預設埠 443。

使用 SSL 通信協定，位於接合點 /travel，埠 4343 的接合主電腦 travel_svr：

```
create -t ssl -p 4343 -h travel_svr /travel
```

使用 Policy Director 單一登入解決方案

當您尋找後端伺服器上的受保護資源時，要求該項資源的從屬站可能必須執行多重登入。多重登入包括登入 WebSEAL 伺服器一次，以及登入每一個後端伺服器各一次。每一個登入都可能需要不同的登入身份。



您可以使用單一登入機制來解決管理及維護多重登入身份的問題。不論資源的位置爲何，單一登入解決方案可讓使用者只利用一次初始登入來存取資源。從後端伺服器的任何進一步登入要求，對使用者而言都是以透通方式來處理。

在配置 Policy Director 單一登入機制時，網路安全管理者必須執行三個重要決策：

1. 後端伺服器是否需要身份驗證資訊？

   WebSEAL 使用 HTTP *基本身份驗證*標頭來傳遞身份驗證資訊。
2. 如果後端伺服器需要身份驗證資訊，這項資訊來自何處？（WebSEAL 將哪些資訊置於 HTTP 標頭中？）
3. WebSEAL 和後端伺服器之間的連線是否需要保護？（TCP 接合或 SSL 接合？）

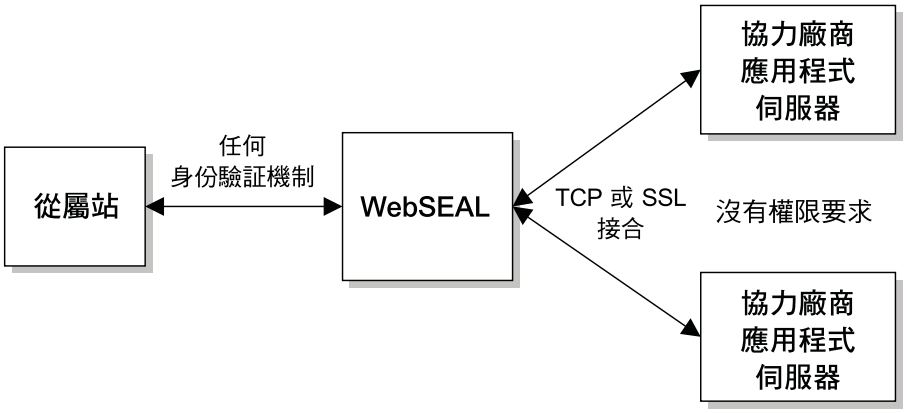
以下各節說明某些典型的 WebSEAL 單一登入配置。

後端伺服器不需要身份驗證

當後端伺服器不需要身份驗證資訊時，則以下條件成立：

- 您不需要將 WebSEAL 配置成跨越接合以傳送身份驗證資訊。
- 您只能透過 WebSEAL 來存取後端伺服器。
- WebSEAL 會代替所有的後端伺服器來處理身份驗證。
- 必要時，仍有一個特殊選項可將使用者身份資訊傳送到後端伺服器，以進行進一步的授權動作。此特殊選項爲 **junctioncp** 公用程式中的 **-c** 選項。

請參閱第193頁的『無身份驗證資訊』。

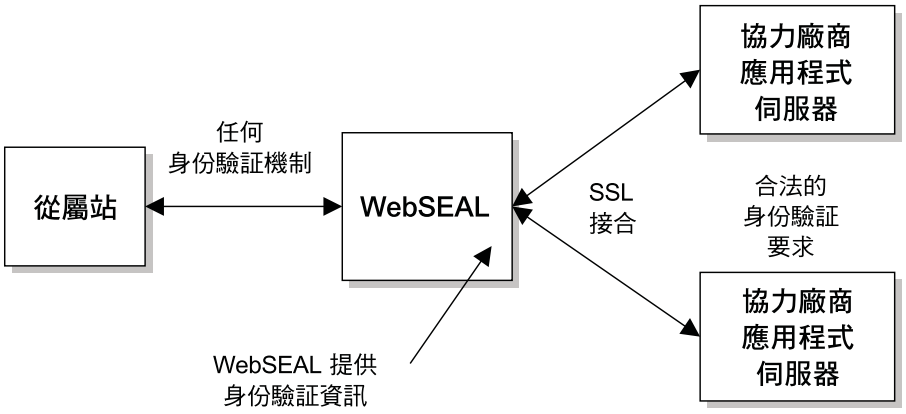


需要舊型身份驗證的後端伺服器

當後端伺服器含有必須支援的舊型身份驗證機制時，則以下條件成立：

- 您必須配置 WebSEAL 以提供適當的身份驗證資訊給後端伺服器。
- 身份驗證資訊很可能來自如 GSO 這類的機制。

  請參閱第194頁的『整合 GSO 與 WebSEAL 的單一登入』。
- 由於 Policy Director 會跨越接合來傳送敏感的身份驗證資訊（使用者名稱和密碼），接合的安全性是非常重要的。因此，Policy Director 建議使用 SSL 接合。

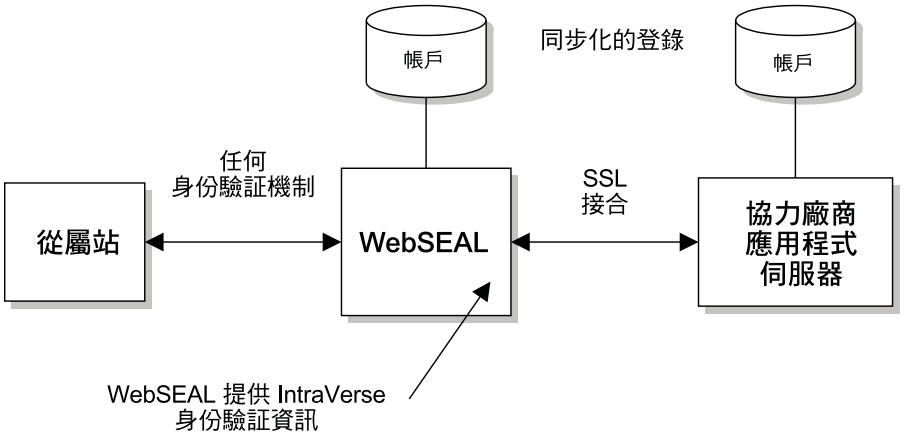


Policy Director 單一登入

當後端伺服器需要身份驗證資訊時，則以下條件成立：

- 您必須配置 WebSEAL，將原始從屬站要求中所含的使用者名稱和密碼提供給後端伺服器。
- 後端伺服器必須瞭解 HTTP 基本身份驗證（BA）標頭中所提供的 Policy Director 身份及密碼。因此，WebSEAL 及後端伺服器必須具備同步化的使用者登錄。
- 由於 Policy Director 會跨越接合來傳送敏感的身份驗證資訊（使用者名稱和密碼），接合的安全性是非常重要的。 Policy Director 建議使用 SSL 接合。

請參閱第192頁的『原始的從屬站 BA 標頭資訊』。



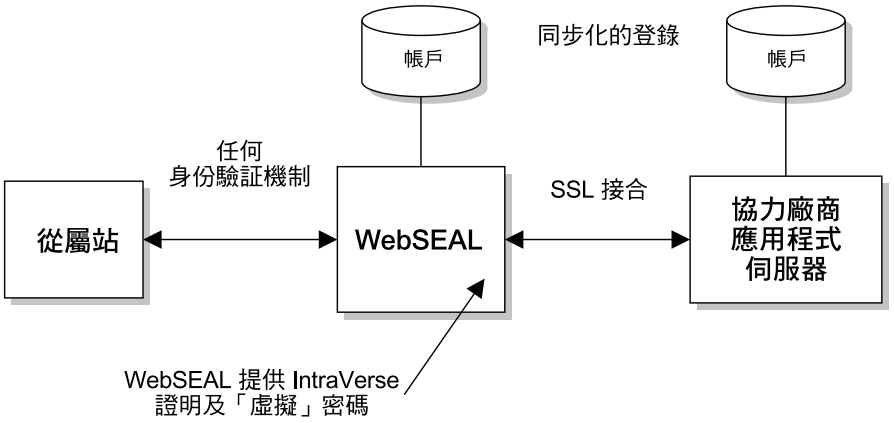
有限的 Policy Director 單一登入

您可用到有限的 Policy Director 單一登入方式；在單一登入中，HTTP BA 標頭提供了 Policy Director 身份（使用者名稱）。同時亦提供靜態、同屬的密碼。此種情況適合每一種使用者應用程式的使用。這種解決方案可能有好處，因爲它不需要持續的密碼管理。但是以下的條件存在：

- 您必須配置 WebSEAL，將原始從屬站要求中所含的使用者名稱以及同屬（虛擬）密碼提供給後端伺服器。
- 在 iv.conf 配置檔中配置虛擬密碼。

- 後端伺服器必須能理解 HTTP BA 標頭中提供的 Policy Director 身份。因此，WebSEAL 及後端伺服器必須具備同步化的帳戶登錄。
- 由於 Policy Director 會跨越接合來傳送敏感的身份驗證資訊（使用者名稱和密碼），接合的安全性是非常重要的。 Policy Director 建議使用 SSL 接合。

請參閱『Policy Director 身份及同屬密碼』。



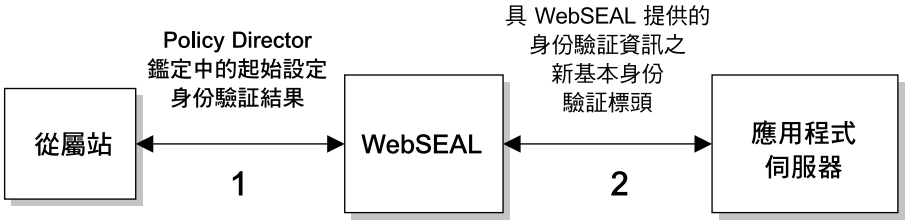
提供身份驗證資訊給接合的伺服器

將身份驗證資訊從 WebSEAL 傳給後端伺服器的情況可能很多。做爲管理者，您必須判斷是否要將 HTTP 基本身份驗證標頭中的身份驗證資訊傳送給後端伺服器。

這項身份驗證資訊的來源爲何？

進行從屬站及 WebSEAL 之間的起始身份驗證之後， WebSEAL 會建置一個新的基本身份驗證標頭。要求會使用這個新的標頭來跨越接合到後端伺服器。您使用 **junctioncp** 公用程式所提供的選項來指定這個新的標頭中要提供哪些身份驗證資訊。

您必須分析您的網路配置以及安全需求，然後決定哪些標頭資訊（如果有的話）必須跨越接合。

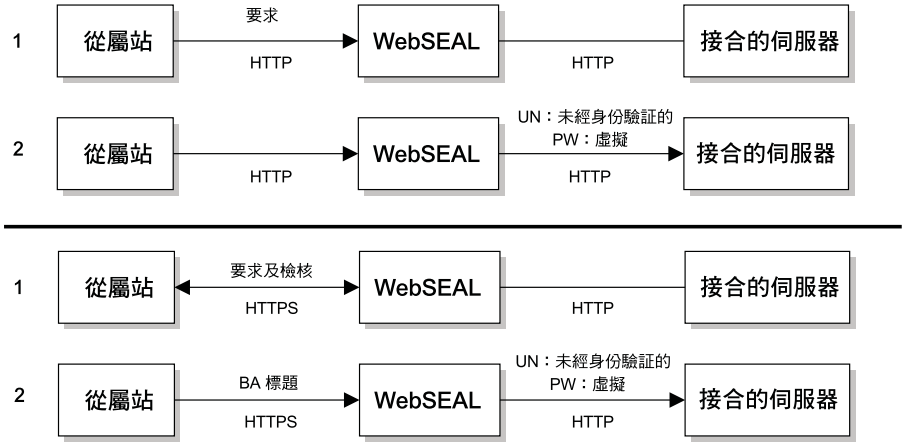


Policy Director 身份及同屬密碼

junctioncp 選項：-b supply

此選項指示 WebSEAL 提供經鑑定的 Policy Director 使用者名稱（從屬站的原始身份）與同屬（虛擬）密碼。這個實務不會使用原始的從屬站密碼。

這個實務會假設後端伺服器會對 Policy Director 的身份要求身份驗證。藉由將從屬站使用者對映到已知的 Policy Director 使用者， Policy Director 可以管理後端伺服器的身份驗證。同時，Policy Director 亦提供單純的領域型、單一登入解決方案。



限制：

Policy Director 在所有的要求中使用相同的虛擬密碼；所有的使用者在後端登錄中都有相同的密碼。如果從屬站一定會經過 WebSEAL 來存取接合的伺服器，這項安排將不會出現任何安全問題。

同屬密碼可以省去密碼管理，並且支援以每一使用者（per-user）爲基礎的應用程式。iv.conf 配置檔中的 **basic_auth_passwd** 參數用以設定虛擬密碼。

```
basic_auth_passwd = password
```

由於這個實務沒有密碼層次的安全性，後端伺服器必須隱含地信任 WebSEAL 來驗證從屬站的合法性。

伺服器也必須瞭解 Policy Director 身份才能接受它。因此，後端伺服器登錄與 WebSEAL 登錄必須同步化。

使用共同的虛擬密碼並不會爲後端伺服器提供任何基礎來證明使用該名稱登入的從屬站之合法性。 因此，您也必須以實體方式保護後端伺服器，防止其他可能的存取。

原始的從屬站 BA 標頭資訊

junctioncp 選項：-b ignore

此選項指示 WebSEAL 忽略從屬站提供的基本身份驗證 (BA) 標頭。這個選項指示 WebSEAL 在不修改的情況下，將標頭轉遞到協力廠商伺服器。WebSEAL 伺服器上不會執行任何登入。

這個實務適用於符合以下條件的後端伺服器：

- 支援基本身份驗證
- 未配置成使用 Policy Director 安全特性
- 必須維護從屬站所提供的密碼

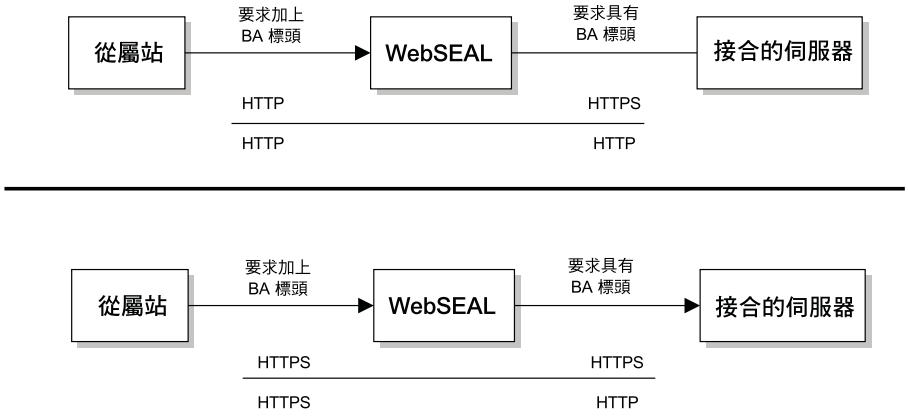
WebSEAL 會將原始的從屬站要求直接傳送到後端伺服器，而不會加以干涉。

後端伺服器會將基本身份驗證查證傳回給從屬站。從屬站回以使用者名稱及密碼資訊，而 WebSEAL 伺服器只負責傳遞而不加以修改。

這不是眞正的單一登入機制 -- 但更確切地說，是透通 WebSEAL 而直接登入協力廠商伺服器。

注意:
當從屬站已經使用 SSL（基本身份驗證）對 WebSEAL 進行身份驗證後，這個選項無法運作。在此情形下，基本身份驗證標頭會被移除（如同在 -b filter 選項中），然後再跨越可能並不安全的接合來傳送。

如果後端伺服器使用基本身份驗證，它會將深入的問題傳回給從屬站。然而，從屬站所傳回的基本身份驗證資訊將會再次被移除。因此，要求永遠不會抵達後端伺服器。

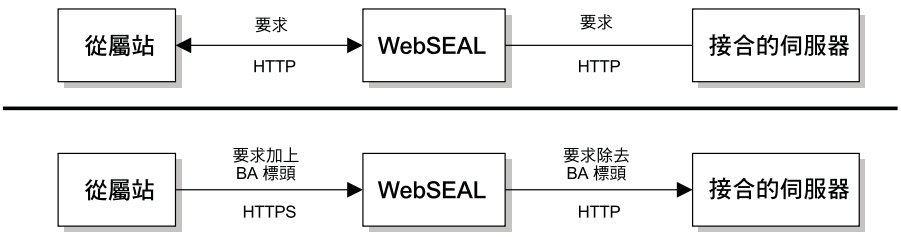


無身份驗證資訊

junctioncp 選項：-b filter

這個選項會指示 WebSEAL 在將要求轉遞到後端伺服器之前，從所有從屬站要求移除全部的基本身份驗證標頭。 WebSEAL 會成爲單一的安全提供者。當您知道後端伺服器不需要基本身份驗證時，可使用這個選項。

您可以將這個選項和 **-c** 選項合併，以便將 Policy Director 從屬站身份資訊插入 HTTP 標頭。請參閱第186頁的『插入從屬站身份資訊（-c 選項）』。



來自 GSO 的使用者名稱和密碼

junctioncp 選項：-b gso

這個選項會指示 WebSEAL 將從 GSO 取得的身份驗證資訊（使用者名稱和密碼）提供給後端伺服器。當您對於 WebSEAL 和後端伺服器的安全性感興趣時，便適用這個實務。後端伺服器應用程式也需要 WebSEAL 登錄中未包含的其他使用者名稱和密碼。

『整合 GSO 與 WebSEAL 的單一登入』有關於這個機制的完整說明。

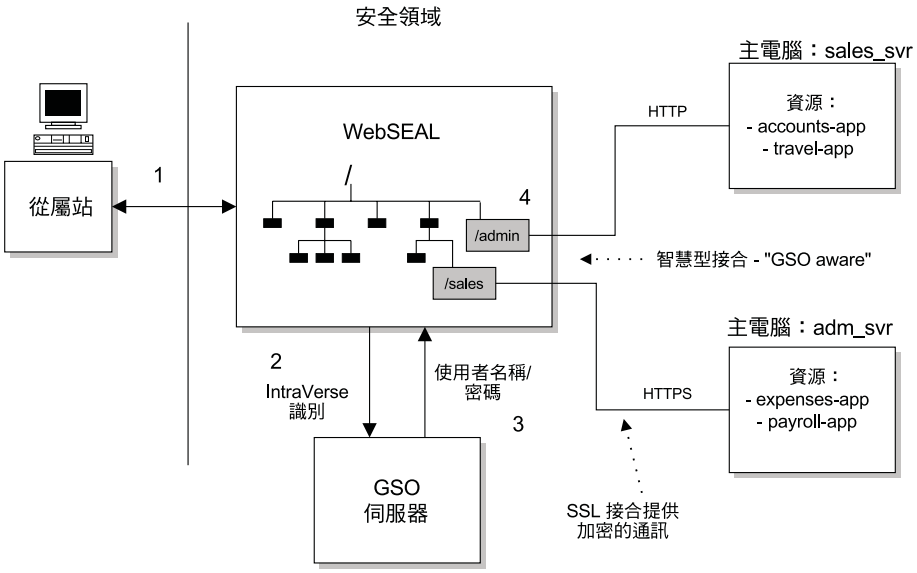
整合 GSO 與 WebSEAL 的單一登入

Policy Director 可藉由整合 IBM Global Sign-on（GSO）來支援更具彈性的單一登入解決方案。IBM Global Sign-On 是 IBM SecureWay 技術的其中一個元件。 合併 WebSEAL 及 GSO 可提供一個完整的單一登入 Web 解決方案，並且具有資料加密、高度有用性及可調整性等額外好處。

下圖說明整合 WebSEAL 與 GSO 來擷取後端應用程式資源所需的使用者名稱和密碼。

1. 從屬站對 WebSEAL 進行身份驗證，並且要求存取後端伺服器上的應用程式資源。此時會取得 Policy Director 身份。

   註: 單一登入程序是獨立於起始身份驗證方法之外。
2. WebSEAL 會將 Policy Director 身份傳給 GSO。
3. GSO 會傳回適合使用者的使用者名稱和密碼，以及所要求的應用程式資源。
4. WebSEAL 會將使用者名稱和密碼資訊插入要求的 HTTP 基本身份驗證標頭。WebSEAL 會行經接合，將要求傳送到後端伺服器。



自 GSO 取得身份驗證資訊

以下範例說明 GSO 如何提供身份驗證資訊給 WebSEAL。使用者 Michael 想執行 travel-app 應用程式資源， WebSEAL 向 GSO 詢問有關 Michael 的身份驗證資訊。

GSO 維護一個完整的身份驗證資訊資料庫，其形式爲針對特定身份驗證資訊的資源對映。應用程式資源以及使用者名稱和密碼合併的對映稱爲 *GSO 資源證明*。您只能爲登錄的使用者建立 GSO 資源證明。

GSO 含有 Michael 的特定資源證明，且將 “travel-app” 資源對映至特定的使用者名稱與密碼組合。

下表說明 GSO 資源資料庫的結構：

Michael	**Paul**

`resource: travel-app`
`username=mike`
`password=123`
`resource: payroll-app`
`username=powell`
`password=456`
	`resource: travel-app`
	`username=bundy`
	`password=abc`
	`resource: payroll-app`
	`username=jensen`
	`password=xyz`

在本例中，GSO 傳回使用者名稱 `mike` 與密碼 `123` 給 WebSEAL。WebSEAL 在跨越接合傳送的要求中建構 HTTP 基本身份驗證標頭時，會使用這項資訊。

配置啓用 GSO 的智慧型接合

您可將 WebSEAL 配置成在 WebSEAL 與後端應用伺服器間的智慧型接合上支援 GSO。

如果要建立啓用 GSO 的接合，請使用 **junctioncp create** 指令以及 **-b gso** 選項。以下範例說明了 create 指令的語法：

```
create -t tcp -h hostname -b gso -T resource jct-point
```

下表列出設定 GSO 智慧型接合的選項：

選項	**說明**
-b gso	指定 GSO 應該爲所有跨越這個接合的要求提供身份驗證資訊。
-T *resource*	指定應用程式資源的名稱。作爲這個選項引數的資源名稱必須和 GSO 資料庫中所列出的資源名稱完全相符。 GSO 接合需用到此選項。

如同在第187頁的『建立安全的 SSL 智慧型接合』中所提到，您可以透過 SSL，使 WebSEAL 和 GSO 解決方案中使用的接合更安全。建立接合時，引用 **-t ssl** 選項來保護接合。

請務必將 SSL 接合和 GSO 一起使用，以確保 GSO 資源證明 和所有資料的加密。

啓用 GSO 智慧型接合的範例：

將 “sales_svr” 主電腦上的 “travel-app” 應用程式資源與 “/sales” 接合點接合：

```
create -t tcp -b gso -T travel-app -h sales_svr /sales
```

將 “adm_svr” 主電腦上的 “payroll-app” 應用程式資源，與 “/admin” 接合點接合，並使用 SSL 做好接合的安全性：

```
create -t ssl -b gso -T payroll-app -h adm_svr /admin
```

註: 在上述範例中，**-t ssl** 選項指定了預設埠 443。

使用智慧型接合

每一個唯一的後端伺服器必須接合到個別的接合（裝載）點。隨著對其它內容的需求與資源的擴展，您可使用智慧型接合來增加更多的伺服器。

使用智慧型接合的相關程序如下：

- 『在相同的接合裝載多重伺服器』.
- 『透過接合的伺服器來過濾 URL』.
- 第197頁的『控制 CGI 處理（x 許可權）』

在相同的接合裝載多重伺服器

您可以在相同接合點裝載多個複製的伺服器。同一個接合點上可以裝載任何數目的伺服器。

裝載在同一個接合點上的所有伺服器都必須是複本（鏡映的 Web 空間），而且必須使用相同的通信協定--HTTP 或 HTTPS。請勿在相同的接合點上裝載不同的伺服器。

從主要 Policy Director 伺服器 Web 空間，存取屬於接合伺服器的頁面。您應該可以存取這些頁面（當然，必須視許可權而定），而出現的頁面應該會一致。有時候，當您找不到頁面或頁面變更時，就表示 Policy Director 未正確複製該頁面。

請檢查文件已存在，而且兩個複製的伺服器中的文件樹狀結構是完全相同的。

透過接合的伺服器來過濾 URL

只有在收到的文件（接合伺服器所送）屬於 MIME 類型 “text” 或 “html” 時，才會加以過濾。

WebSEAL 可變更的兩組 URL 爲：絕對 (Absolute) 與主電腦相對 (Host Relative)。

相對於主電腦的 URL

相對於主電腦的 URL 是指相對於接合伺服器之文件根目錄的 URI 位置，例如：

```
/dir/file.html
```

變更這些 URL 以反映出接合伺服器的接合點。例如：

```
/jct/dir/file.html
```

絕對 URL

「絕對 URL」是指一個相對 HOST 名稱或 IP 位址的 URI 位置外加網路埠。例如：

```
http://servername[:port]/file.html
```

或：

```
https://servername[:port]/file.html
```

您可以根據以下規則來變更這些 URL：

1. 當 URL 是 HTTP，而主電腦或埠符合 TCP 接合的伺服器， URL 會改變以反映接合點。例如：

   ```
   /jct/...
   ```

2. 當 URL 是 HTTPS，而主電腦或埠符合 SSL 接合的伺服器， URL 會改變以反映接合點。例如：

   ```
   jct...
   ```

3. 只有定義於 iv.conf 配置檔中之「TAG - 屬性」對的 URL 才會加以過濾。
4. 請務必過濾 META 標示以復新要求。例如：

   ```
   META HTTP-EQUIV="Refresh" CONTENT="5;URL=http://server/url"
   ```

5. 如果 BASE 標示含有 HREF 屬性，則對從屬站的回應會移除標示。

iv.conf 配置檔的 [url-filter] 段落包含了透過接合伺服器來過濾 URL 的參數。

[url-filter] 段落包含 HTML 標示的清單。 WebSEAL 伺服器會過濾或變更這些標籤，以調整透過所接合伺服器取得的絕對 URL。

根據預設，Policy Director 會配置所有常用的 HTML 標示。管理者可能需要新增含有 URL 的其他 HTML 標示。

控制 CGI 處理（x 許可權）

Policy Director 的執行 (x) 許可權在接合間並無意義。您不能以 x 許可權來控制 CGI Script 的處理。 WebSEAL 沒有任何方法可以正確地判斷位於後端伺服器上的要求物件是 CGI 程式檔或一般 HTTP 物件。經由接合存取物件（包括 CGI 程式），往往是使用讀取 (r) 許可權來控制。

對協力廠商伺服器使用 query_contents

您可使用 Policy Director 安全服務程式，來保護協力廠商應用程式 Web 空間的資源。如果要這麼做，您必須爲 WebSEAL 提供協力廠商 Web 空間的內容相關資訊。

一個稱爲 **query_contents** 的 CGI 程式提供了這項資訊。 **query_contents** 程式會搜尋協力廠商 Web 空間的內容，並且提供這項庫存資訊給 WebSEAL 上的「管理主控台」。這個程式包含在 WebSEAL 安裝中，但是您必須以手動方式將程式安裝到協力廠商伺服器上。程式檔類型有很多種，端視您將協力廠商伺服器置於 UNIX 或 Windows 上而定。

「管理主控台」的「物件空間」管理程式可以自動執行 **query_contents**。只要受保護物件空間部份（代表接合）展開於「物件空間」管理畫面中，該管理程式即會執行 query_contents。現在「主控台」已經知道協力廠商應用程式空間的內容，您可以顯示這項資訊，並且將原則模版引用到適當的物件。

安裝 query_contents

在安裝 **query_contents** 的過程中，需將 Policy Director 伺服器中的一或多個檔案複製到協力廠商伺服器中，並編輯配置檔。

以下的 Policy Director 目錄包含一個程式模版：

UNIX： *root-directory*/www/lib/query_contents

Windows： *root-directory*\www\lib\query_contents

目錄內容包括：

檔案	說明
query_contents.exe	Win32 系統的主要可執行程式。它應該安裝到協力廠商 Web 伺服器的 cgi-bin 目錄中。
query_contents.sh	UNIX 系統的主要可執行程式。它應該安裝到協力廠商 Web 伺服器的 cgi-bin 目錄中。
query_contents.c	原始程式碼。提供原始碼是因爲您可能需要變更 **query_contents** 的行爲。在大部分的情形下，這是不必要的。
query_contents.html	HTML 格式的說明檔。
query_contents.cfg	指出 Web 伺服器之文件根目錄的範例配置檔。

安裝 query_contents 到協力廠商 UNIX 伺服器

在以下的目錄中找出指名爲 query_contents.sh 的 Shell Script：

UNIX： *install-dir*/www/lib/query_contents

如要將 **query_contents** 公用程式安裝於協力廠商 UNIX 伺服器中時請：

1. 將 query_contents.sh 複製到協力廠商 Web 伺服器可作用的 /cgi-bin 目錄。
2. 移除 .sh 副檔名。
3. 爲擁有 Web 伺服器的使用者設定 UNIX “execute” 位元。

安裝 query_contents 到協力廠商 Win32 伺服器

在以下的目錄中找出指名爲 query_contents.exe 的可執行程式以及指名爲 query_contents.cfg 的配置檔：

Windows： *install-dir*\www\lib\query_contents

如要將 **query_contents** 公用程式安裝於協力廠商 Win32 伺服器中時請：

1. 確定協力廠商 Web 伺服器已正確配置一個 CGI 目錄。
2. 確定協力廠商 Web 伺服器的文件根目錄中有一份有效的文件存在。
3. 將 query_contents.exe 複製到協力廠商 Web 伺服器的 CGI 目錄中。
4. 將 query_contents.cfg 複製到 Windows 目錄中。
   下表顯示了這個目錄的預設值：

作業系統	Windows 目錄
Windows 95	c:\windows
Windows NT 3.5x	c:\winnt35
Windows NT 4.x	c:\winnt

5. 編輯 query_contents.cfg 檔，以正確指定協力廠商 Web 伺服器的文件根目錄。

檔案目前含有 Microsoft Internet Information Server™ 以及 Netscape® FastTrack 伺服器的範例項目。這個檔案中以分號（;）作爲開頭的程式行爲說明，**query_contents** 程式會忽略它。

測試配置

要測試配置時請：

1. 在 Win32 伺服器中，變更至內含 **query_contents** 程式的目錄。
2. 從 Win32 伺服器的 DOS 提示中，執行下列程式：

   ```
   query_contents dirlist=/
   ```

   您應該會看到類似以下的輸出：

   ```
   100
   index.html
   cgi-bin//
   pics//
   ```

   數字 100 爲指出順利完成的傳回狀態。最重要的是察看數字 100 是第一個（或許是唯一的）值。

   當您看到錯誤碼時，表示配置檔不在正確的位置，或者不含有效的文件根項目。請檢查 query_contents.cfg 檔的配置，並確定文件根目錄存在。
3. 從瀏覽器中，輸入以下的 URL：

   ```
   http://Win32 machine name/cgi-bin/query_contents.exe?dirlist=/
   ```

   此指令應會傳回與前一步驟相同的結果。如不是傳回此結果，您 Web 伺服器的 CGI 配置將不正確。請參閱伺服器的文件來更正問題。

將智慧型接合配置成尋找查詢內容

您可以爲 **query_contents** script 定義 URL。 Policy Director 會在 /cgi_bin/ 目錄中尋找 **query_contents**。當這個目錄不同時，或者 **query_contents** 檔案已更名時，請使用這個選項將此檔案的新 URL 告知 WebSEAL。

如果您爲協力廠商 Win32 伺服器建立智慧型接合，請使用 **junctioncp** 指令與 **-q** 選項：

```
junctioncp> create -t tcp -h hostname -q /cgi-bin/query_contents.exe /jct_mount_point
```

有關所有 **junctioncp** 指令選項的摘要說明，請參閱第182頁的『爲起始伺服器建立新的接合』。

執行 query_contents

query_contents 可傳回 URL 要求中之目錄的內容。例如，如果要取得伺服器 Web 空間的根目錄內容，瀏覽器必須在以下這類的 URL 上執行 **query_contents**：

```
http://third-party-server/cgi-bin/query_contents?dirlist=/
```

query_contents Script 會執行以下動作：

1. 讀取 $SERVER_SOFTWARE（一個標準的 CGI 環境變數），以決定伺服器類型。

Policy Director 會根據 Web 伺服器類型，將變數 $DOCROOTDIR 設定爲典型的文件根目錄位置。

2. 從所要求的 URL 讀取環境變數 $QUERY_STRING，以取得要求的作業及物件路徑。

   變數 $OPERATION 會儲存作業值，而 $OBJPATH 會儲存選項路徑。在本例中，$OPERATION 爲 dirlist， $OBJPATH 爲 “ / ”。

3. 在物件路徑上執行目錄列表（ls），並且將結果置於標準輸出，以供 Policy Director 伺服器使用。代表子目錄的項目其後會加上一個雙斜線 (//)。

   典型的輸出如下：

   ```
   100
   index.html
   cgi-bin//
   pics//
   ```

   數字 100 爲指出順利完成的傳回狀態。

自訂 query_contents

如果要爲您的伺服器自訂 **query_contents**，您可能需要變更文件根目錄的設定。

如果 **query_contents** 傳回錯誤狀態（100 以外的數字），而且沒有列出任何檔案，請檢查 Script。必要時，請變更 $DOCROOTDIR 變數，以符合您伺服器的配置。

如果您指定了正確的文件根目錄，而 Script 仍然失效，則 cgi-bin 位置的指定可能不正確。請檢查 $FULLOBJPATH 變數，並且變更指定給它的值，以反映正確的 cgi-bin 位置。

其他功能

query_contents 程式 (query_contents.c) 的原始碼會隨 Policy Director 一起分送。

您可以在這個程式中加入其他功能，以支援某些協力廠商 Web 伺服器的特殊特性。這些特性包括：

1. 目錄對映--不在文件根目錄下的次目錄會對映到 Web 空間。
2. 產生並非以檔案系統爲基礎的 Web 空間。

   這可能是針對以資料庫爲主導的 Web 伺服器。

第16章 WebSEAL：應用程式整合

WebSEAL 支援透過變數及動態 URL 功能來整合協力廠商應用程式。 WebSEAL 可擴充環境變數及 HTTP 標頭的範圍，讓協力廠商應用程式執行基於從屬站身份的作業。此外，WebSEAL 可提供對動態 URL（例如，含有查詢文字）的存取控制。

本章包括：

支援 CGI 程式設計

爲了支援 CGI 程式設計，WebSEAL 在標準的 CGI 變數集中加入三個額外的環境變數。 CGI 應用程式可使用在本端 WebSEAL 伺服器或接合的後端伺服器上所執行的這些環境變數。變數將 Policy Director 特定的使用者、群組及證明資訊提供給 CGI 應用程式。

在本端的 WebSEAL 伺服器上，提出要求的從屬站的 Policy Director 證明資訊可直接產生這些環境變數。

執行於接合之協力廠商伺服器上的 CGI 應用程式所用的環境變數，是從 HTTP 標頭資訊中產生。 WebSEAL 會將 HTTP 標頭資訊傳送至伺服器。您必須使用 **junctioncp -c** 選項來建立*接合*。 之後，接合會將 Policy Director 特定標頭資訊插入到 HTTP 要求中，然後將這些 HTTP 要求送往後端伺服器。

請參閱第186頁的『插入從屬站身份資訊（-c 選項）』。

其他的 Policy Director 特定環境變數

以下是其它的 Policy Director 特定 CGI 環境變數格式：

CGI 環境變數格式	說明
HTTP_IV_USER	要求程式的 Policy Director 使用者帳戶名稱。
HTTP_IV_GROUPS	要求程式所屬的 Policy Director 群組。以雙引號括住，並且以逗號隔開群組名稱的清單。
HTTP_IV_CREDS	代表 Policy Director 證明的已編碼不透明資料結構。提供證明給遠端伺服器，使中間層的應用程式可以使用「權限 API」來呼叫「權限服務程式」。請參閱 *Policy Director 程式設計及參考手冊*。

本端 WebSEAL 伺服器中的 REMOTE_USER 變數

在 WebSEAL 所控制的本端伺服器環境中，HTTP_IV_USER 變數值是提供作爲標準的 REMOTE_USER 變數值。請注意，REMOTE_USER 變數也可以出現在於接合的後端伺服器上執行的 CGI 程式的環境中。然而，在這種情況下， WebSEAL 不會控制它的值。

CGI 環境變數格式	說明
REMOTE_USER	包含與 HTTP_IV_USER 欄位相同的值。

支援後端伺服器端的應用程式

WebSEAL 也支援作爲後端 Web 伺服器內含元件來執行的可執行碼。此類伺服器端可執行碼的範例包括：

- Java Servlet
- Oracle Web Listener 的卡匣
- 伺服器端的外掛程式

您可使用 **junctioncp** 公用程式中的 **-c** 選項，建立與後端伺服器間的接合。接著，WebSEAL 會將 Policy Director 特定從屬站身份與群組成員資訊插入到 HTTP 要求的標頭中，然後將這些 HTTP 要求送給該伺服器。

請參閱第186頁的『插入從屬站身份資訊（-c 選項）』。

Policy Director 特定的 HTTP 標頭可讓位於接合的、協力廠商伺服器上的應用程式執行使用者特定的動作（基於從屬站的 Policy Director 身份）。

WebSEAL 提供以下的 Policy Director 特定 HTTP 標頭資訊：

Policy Director 特定的 HTTP 標頭	說明
iv-user	從屬站的名稱。如果從屬站未經身份驗證（不明），則預設值爲 “Unauthenticated”。
iv-groups	從屬站所屬的群組清單。由以雙引號括住、並且以逗號隔開的群組名稱清單所組成。
iv-creds	代表 Policy Director 證明的已編碼不透明資料結構。提供證明給遠端伺服器，使中間層的應用程式可以使用「權限 API」來呼叫「權限服務程式」。請參閱*Policy Director 程式設計及參考手冊*。

HTTP 標頭項目可讓 CGI 程式作爲環境變數 HTTP_IV_USER、 HTTP_IV_GROUP 和 HTTP_IV_CREDS 使用。若是其他非 CGI 的應用系統配置，請參閱相關的產品文件，以取得從 HTTP 要求擷取標頭的指示。

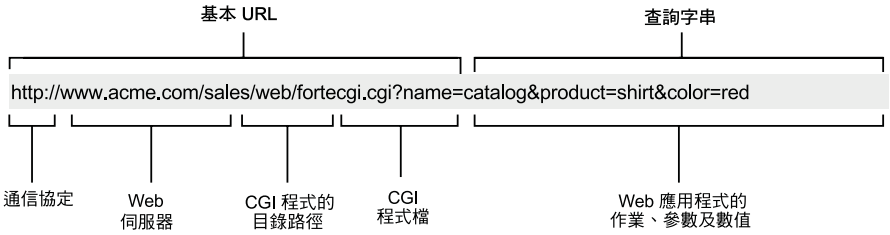
提供對動態 URL 的存取控制

現行的 Web 環境可讓使用者立即存取快速變更的資訊。許多 Web 應用程式會以動態方式產生「統一資源定位器」（URL）來回應每一個使用者要求。這些動態 URL 可能只會存在一段很短的時間。儘管它們短暫的特性，動態 URL 仍然需要強大的保護，以免遭到不當的使用或存取。

瞭解動態 URL

某些較複雜的 Web 應用程式工具使用標準的 Web 瀏覽器，透過 Web 伺服器的 CGI 介面來與應用伺服器通信。

這些工具使用動態 URL 以及隱藏的套表元件，將所要求的作業（及其參數值）告知應用伺服器。動態 URL 會將標準的 URL 位址擴大，加入特定作業的相關資訊及其參數值。 URL 的查詢字串部分可將作業、參數和值提供給 Web 應用程式介面。



將 ACL 名稱空間物件對映至動態 URL

WebSEAL 採用受保護的物件名稱空間模式與原則模版 (ACL) 來保護動態產生的 URL（如資料庫要求產生的這些 URL）。和授權程序的第一步相同，每一個對 WebSEAL 的要求都會解析成特定的名稱空間物件。引用至名稱空間物件的 ACL 會指出對映至該物件的所有動態 URL 所需要的保護。

由於動態 URL 只是暫時存在，您不可能在預先配置的授權原則資料庫中備有它們的項目。 WebSEAL 解決這個問題的方法是提供一種機制，將許多動態 URL 對映至單一、靜態的受保護物件。

文字檔中含有「物件 -> 名稱空間」的對映型式。

UNIX： `/opt/intraverse/www/lib/dynurl.conf`

Windows： `C:\Program Files\IBM\Policy Director\www\lib\dynurl.conf`

編輯這個檔案來變更這些對映。您必須建立這個檔案；預設值沒有這個檔案。檔案中的項目格式如下：

object pattern

WebSEAL 使用 UNIX Shell 型樣（包括萬用字元）的子集，以定義在名稱空間中組成一個物件的參數集。 WebSEAL 會將所有符合這些參數的動態 URL 對映至該物件。 WebSEAL 支援以下的 UNIX Shell 型樣相符字元：

字元	說明
****	反斜線後面的字元是特殊順序的一部分。例如，爲 TAB 字元。
?	符合單一字元的萬用字元。例如，`abcde` 字串符合 `ab?de` 表示式。
*****	符合零個或更多字元的萬用字元。
[ ]	定義任何字元均可相符的字元集。例如，`abcde` 字串符合 `ab[cty]de` 正規表示式。
^	指出反相。例如，表示式 ^[ab] 符合 ″a″ 或 ″b″ 字元以外的任何項目。

以下範例說明執行信用餘額查閱的動態 URL 格式：

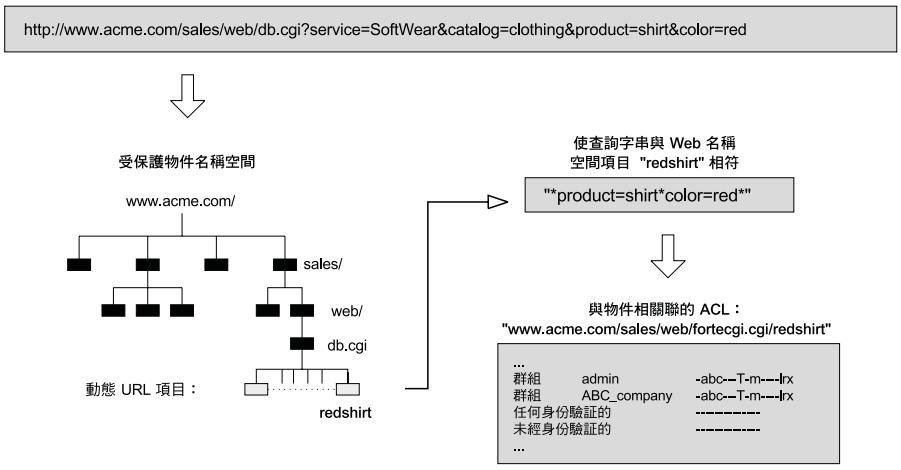
`http://`*`server-name`*`/home-bank/owa/acct.bal?acc=`*`account-number`*

代表這個動態 URL 的名稱空間物件會以下列方式出現：

`http://<server-name>/home-bank/owa/acct.bal?acc=*`

小心檢查本例中的動態 URL，您可發現它說明了一個特定的帳號。名稱空間物件在 home-bank 的帳戶餘額，顯示出 ACL 許可權適用於所有帳戶。它們適用於所有帳戶，因爲項目的最後一部分（acc=*）使用星號萬用字元，後者與所有的字元相符。

本圖說明一個對映到特定受保護名稱空間物件的特定動態 URL 的完整實務--這個範例沒有使用任何萬用字元：



為動態 URL 更新 WebSEAL

使用 **dynurlcp** 公用程式，將 WebSEAL 受保護的物件名稱空間更新成 dynurl.conf 配置檔中的項目。您必須使用 dce_login 來登入安全領域。

如要使用 **dynurlcp** 公用程式以更新 WebSEAL 受保護的物件名稱空間時請：

1. 在 dynurl.conf 配置檔中建立、編輯或刪除動態 URL 項目。
2. 製作變更後，使用 **dynurlcp** 公用程式來更新伺服器：

   ```
   dynurlcp -e /.:/subsys/intraverse/secmgr/server/ host update
   ```

解析名稱空間中的動態 URL

將動態 URL 解析成名稱空間物件是根據 dynurl.conf 配置檔中的項目次序而定。

在嘗試將動態 URL 對映到名稱空間項目時，會掃描 dynurl.conf 配置檔中的對映清單。檔案是從頂端掃描到底端，直到發現第一個相符的型樣爲止。

發現第一個相符的項目時，WebSEAL 使用對應的名稱空間項目來進行後續授權檢查。找不到相符的項目時，WebSEAL 使用 URL 本身，再減去路徑的 http://*server* 部分。

將對應到最具限制性之 ACL 的對映保持在清單頂端。例如，書籍銷售程序（屬於銷售訂單應用程式）被限制爲讀書會群組。然而，所有的使用者都能存取其餘的銷售訂單應用程式。因此，對映的順序應如下表所示：

名稱空間項目	URL 型樣
/ows/sales/bksale	/ows/db-apps/owa/book.sales*
/ows/sales/general	/ows/db-apps/owa/*

請注意，如果對映項目的次序相反，則 /ows/db-apps/owa 目錄中的所有已儲存程序都會對映到 /ows/sales/general 名稱空間物件。這可能會破壞安全性，這是因爲此種名稱空間處理方式不正確。

GET 和 POST 資料傳輸方法

當您將 URL 正規表示式對映到名稱空間項目時， URL 格式應該假定爲 GET 方法所產生的格式。在此種假設下，便無關乎所用的是 POST 或 GET 方法。

在 GET 資料傳輸方法中，WebSEAL 會將*動態資料*附加到 URL。使用者在套表中提供的資料就是動態資料的範例。

在 POST 資料傳輸方法中，WebSEAL 會將動態資料併入要求本體。

ACL 評估

在將動態 URL 解析成名稱空間項目後，會使用標準的 Policy Director ACL 承接模式。此模式下會決定應處理或禁止（因專用權不足）要求。

動態 URL 的說明：Travel Kingdom

下列範例說明企業內部網路如何保護 Oracle Web 接聽器產生的 URL。

本範例中所使用的動態 URL Web 伺服器是 Oracle Web Listener。您可以將這個技術同樣引用到其他的動態 URL Web 伺服器。

應用程式

Travel Kingdom 組織專門透過網際網路爲客戶提供旅遊訂票服務。這家企業打算在它們的 Web 伺服器上使用兩個 Oracle 資料庫應用程式 --可以從企業防火牆內存取，也可從網際網路來存取。

- **旅遊預訂系統**

  被授權的客戶可以從遠端預約，並且查詢他們目前的預約狀況。 Travel Kingdom 員工也可以爲電話客戶進行預約、處理變更，並且執行許多其他交易。由於外部客戶是利用信用卡來付款， WebSEAL 必須保護這些資訊的傳輸。
- **管理程式**

  和大部分的公司一樣， Travel Kingdom 維護一個管理資料庫，其中包含薪資、職位及經驗資訊。這項資料同時附有每一位員工的照片。

介面

您可以配置 Oracle Web 伺服器，以便對資料庫中的下列儲存程序進行存取：

/db-apps/owa/tr.browse	讓所有的使用者查詢旅遊目的地、價格等等。
/db-apps/owa/tr.book	用來進行預約（旅行社員工或未經身份驗證的客戶）。
/db-apps/owa/tr.change	用來檢視或變更目前的預約。
/db-apps/owa/admin.browse	由任何員工使用，以檢視未限制的員工資訊，如分機號碼、電子郵件地址及照片。

/db-apps/owa/admin.resume	讓員工檢視或變更他們在「管理」資料庫中的履歷資訊。
/db-apps/owa/admin.update	由「管理」員工用來更新員工資訊。

Web 空間結構

利用 WebSEAL 伺服器爲 Travel Kingdom 統一的 Web 空間提供一個安全的介面。

您可以接合（/ows）執行旅遊預約應用程式及管理應用程式的 Oracle Web 伺服器。

安全原則

爲了提供適當的安全性給 Web 資源，同時又能維持一個易於使用的系統，這家企業已經建立以下的安全目標：

- 旅行社員工可以完全控制所有的預約。
- 已通過身份驗證的客戶可以變更自己的預約，但不能干擾其他通過身份驗證客戶的旅遊資料。
- 管理員工可以完整存取所有的管理資訊。
- Travel Kingdom 員工（非「管理部門」）可以變更自己的履歷資訊，並且檢視其他員工的部分資訊。

動態 URL 對名稱空間的對映

如要達到安全原則目標，則需配置「動態 URL -> ACL 名稱空間」的對映型式。請記住，這些對映的次序是達成安全目標很重要的一部分。

對映應該以下表所顯示的方法來配置：

名稱空間項目	URL 型樣
/ows/tr/browse	/ows/db-apps/owa/tr.browse\?dest=*&date=??/??/????
/ows/tr/auth	/ows/db-apps/owa/tr.book\?dest=*&depart=??/??/????&return=??/??/????
/ows/tr/auth	/ows/db-apps/owa/tr.change
/ows/admin/forall	/ows/db-apps/owa/admin.resume
/ows/admin/forall	/ows/db-apps/owa/admin.browse\?empid=[th]???
/ows/admin/auth	/ows/db-apps/owa/admin.update\?empid=????

安全從屬站

從屬站是透過安全、加密的通道來對 WebSEAL 進行身份驗證。

想使用 Web 介面的客戶必須另外向 Travel Kingdom Web 經營者登錄，才能收到帳戶。

帳戶結構及群組結構

在系統中建立以下的群組：

Staff Travel Kingdom 組織的成員。

TKStaff Travel Kingdom 旅行社。

AdminStaff Travel Kingdom 管理部門的成員。請注意，「管理」員工也包含在「Staff」群組中。

Customer 想透過網際網路進行旅遊訂票的 Travel Kingdom 客戶。

在安全領域中提供每一個使用者一個帳戶，使 WebSEAL 伺服器能單獨識別他們。WebSEAL 會將使用者的身份傳送到 Oracle Web 伺服器，並且爲所有的 Web 資源提供一個單一登入解決方案。

存取控制

下表列出了之前的資訊中的應用程式所產生的存取控制：

/ows/tr/browse	unauthenticated	Tr
	any_authenticated	Tr
/ows/tr/auth	unauthenticated	-
	any_authenticated	-
	group TKStaff	Tr
	group Customer	PTr
/ows/admin/forall	unauthenticated	-
	any_authenticated	-
	group Staff	Tr
/ows/admin/auth	unauthenticated	-
	any_authenticated	-
	group AdminStaff	Tr

客戶與 TKStaff 對於預約和旅遊計畫維護物件都具有相同的專用權，但是有一點例外。這個例外是客戶必須將資訊加密（私密許可權），以便在將*敏感資料*提出到不可靠的網路網路時，能提供進一步的安全性。敏感的資料包括信用卡之類的資訊。

結論

這個簡單的範例說明了佈署具備可執行下列功能的系統的概念：

- 保護敏感資訊
- 驗證使用者身份
- 授權對敏感資訊的存取

此外，WebSEAL 和 Oracle Web 伺服器兩者都知道系統中通過身份驗證的使用者身份。這項身份資訊是用來提供可審核的單一登入解決方案。

第17章 NetSEAL：概觀

Policy Director NetSEAL 是一種「虛擬專用網路（VPN）」解決方案，可保護所有傳入的 TCP/IP 通信。NetSEAL，此種資源管理程式，可控制使用者連接特定 TCP 應用程式的能力。 NetSEAL 是根據目的地埠與從屬站身份來執行存取控制。 NetSEAL 可將任何網路應用伺服器與 Policy Director 安全服務程式整合在一起。

本章包括：

介紹 NetSEAL

NetSEAL 可控制存取 Policy Director 安全領域中各種以 TCP 爲基礎的應用程式與服務程式。 Windows 從屬站可透過 Policy Director NetSEAT 從屬站與 NetSEAL 進行安全通信。

NetSEAT 與 NetSEAL 間的通信可利用 SSL 通道或 GSS 通道來保護。在每一種情況中，會使用提出要求之從屬站的使用者名稱與密碼，來鑑定 NetSEAT 從屬站和 Policy Director 伺服器間的安全鏈結之建立。

- *SSL 通道*用以保護 NetSEAT 與 NetSEAL 間的通信。
- *GSS 通道*或 NetSEAL 接合用以保護 NetSEAL 伺服器到 NetSEAL 伺服器間的通信。恆使用代表提出要求之從屬站來建立連線的 Policy Director 伺服器使用者，來鑑定建於 Policy Director 伺服器之間的 GSS 通道。透過 GSS 通道，兩個伺服器間相互鑑定；而恆由第二個伺服器對從屬站執行存取控制。

NetSEAL 接合會建立一種經由 Policy Director 伺服器到另一個 Policy Director 伺服器或網路的前進通信方向。 GSS 通道可用來保護跨過 NetSEAL 接合的安全通信。

NetSEAL 存取控制是粗略的。最多是控制應用程式所監聽之特定埠。細密的存取控制方式對應用程式所操作的資源並沒有幫襯效果。

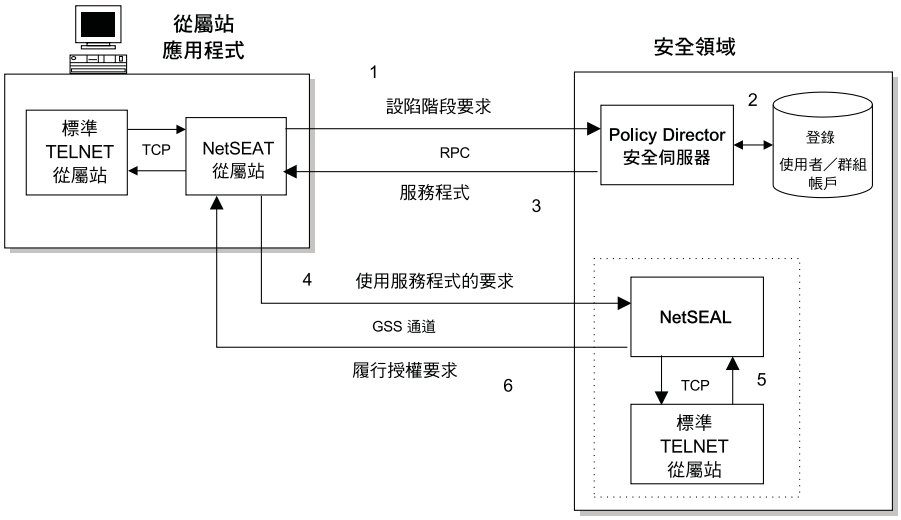
本章說明一些使用 NetSEAL 的網路情況。圖解中是以 TELNET 遠端登入應用程式做爲 TCP 應用程式範例。在每一種情況中，NetSEAL 是根據下列來回應要求：

- 要求的來源
- 對受影響物件（像是目的地埠與 NetSEAL 接合）的許可權
- 參與連線的 Principal

NetSEAT 從屬站經由 GSS 通道到 NetSEAL

當 NetSEAT 配置成使用 GSS 通道時， NetSEAT 會設陷截下送出的要求，並使用 RPC，向 Policy Director 安全伺服器求證從屬站的身份。此外，並針對所要求之應用程式的相關特定埠，執行授權檢查。

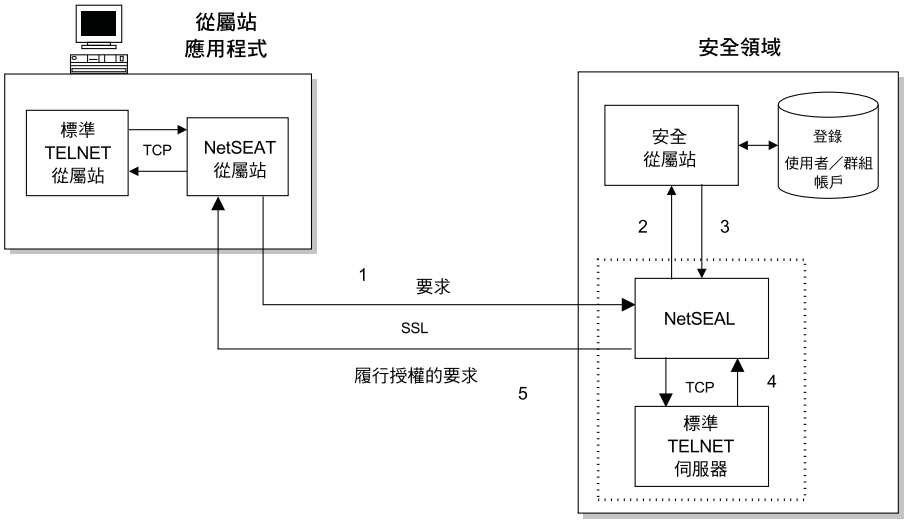
若身份驗證與授權程序證明無誤，即會在 NetSEAT 與 NetSEAL 伺服器間建立一條 GSS 通道。之後會使用 TCP 從 NetSEAL 存取所要求的 TCP 應用程式。



NetSEAT 從屬站經由 SSL 通道到 NetSEAL

當您將 NetSEAT 配置成使用 SSL 時，是在 NetSEAL 與 Policy Director 安全服務程式間處理身份驗證與授權程序。NetSEAL 可接受代表從屬站身份的使用者名稱與密碼。

如果身份驗證與授權程序證明無誤， Policy Director 將處理要求。並使用 TCP 從 NetSEAL 來存取所要求的 TCP 應用程式。

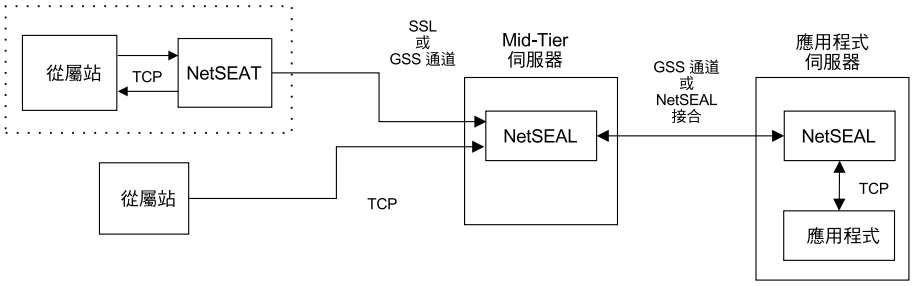


NetSEAL 網路區段

NetSEAL 交易中的連線要求會沿著網路路徑經歷各種不同的保護層次。如同第210頁的『NetSEAT 從屬站經由 SSL 通道到 NetSEAL』中的說明， NetSEAT 從屬站支援和 NetSEAL 伺服器間的 SSL 或 GSS 連線。

註: 依照設計，NetSEAL 伺服器連接 NetSEAL 伺服器時，*恆採用* GSS。請勿在兩個 NetSEAL 伺服器間採用 SSL 連線。

從 NetSEAL 到本端或遠端 TCP 應用程式埠間的最終路徑，則恆使用 TCP。



下表摘要說明每一個連線區段的保護層次：

連線區段	保護
NetSEAT 從屬站到 NetSEAL 伺服器	SSL 或 GSS 通道
TCP 從屬站到 NetSEAL 伺服器	無
NetSEAL 伺服器到 NetSEAL 伺服器	GSS 通道
NetSEAL 接合	GSS 通道
NetSEAL 伺服器到 TCP 應用程式埠	無

不論是本端或遠端應用程式，NetSEAL 皆採同一連線決策程序：

- 所要求之埠受到保護（使用 ACL）嗎？
- 若該埠受到保護，使用者有適當許可權來存取嗎？
- 若該埠未受保護，則容許外傳的連線。

NetSEAL 也會區隔出「安全管理程式」所要求之傳入資訊與外傳連線程序。換句話說，「安全管理程式」不需要知道 NetSEAT 從屬站是在本端或遠端設陷截下連線要求。

說明從屬站到 NetSEAL 的服務

下列情況說明從屬站與受 NetSEAL 保護之 TCP 應用程式間可能發生的交談類型。從屬站可包括 NetSEAT 從屬站與非 NetSEAT 從屬站。

這些情況有：

- 第212頁的『接往 Policy Director 伺服器的傳入通道連線』。
- 第212頁的『接往受保護主電腦的傳入通道連線』。
- 第213頁的『接往 Policy Director 伺服器的傳入 TCP 連線』。

接往 Policy Director 伺服器的傳入通道連線

在這個第一種基本情況中，您將 NetSEAT 從屬站配置成設陷截下送往 Policy Director 伺服器中之應用程式的連線。在 NetSEAT 從屬站設陷截下通信後，即會與 Policy Director 伺服器上的 NetSEAL 間建立一條安全通道。本例中將送往埠 23 的要求，即會透過此通道加以轉遞。

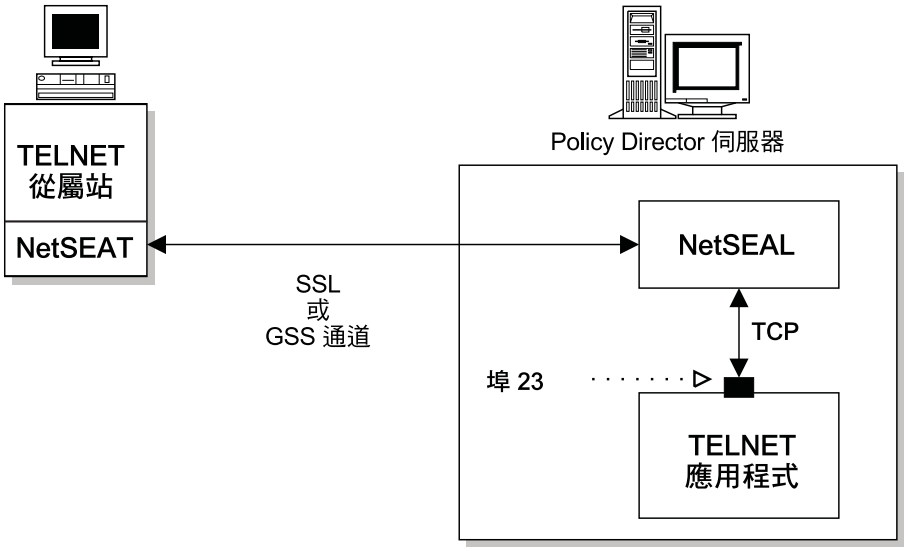
身份驗證程序對使用者是透通的。

NetSEAL 伺服器會以下列方式完成交易：

1. 根據埠的 ACL，使用者能不能連接所要求之埠？

   是-- 與所要求之埠間建立一條 TCP 連線。

   否-- 拒絕連線要求。



接往受保護主電腦的傳入通道連線

本情況顧及到位於受保護之遠端伺服器上的應用程式。應用伺服器可以是 Policy Director 或協力廠商伺服器。對於兩個 NetSEAL 伺服器間的通信，Policy Director 恆使用 GSS。

在本情況中，NetSEAL 可保護執行於 Policy Director 不支援之平台上的 TCP 應用程式。

NetSEAL 伺服器會以下列方式完成交易：

1. 使用者能否連接目的地伺服器上的所要求之埠（根據其 ACL 而定）？

   是-- 繼續進行。

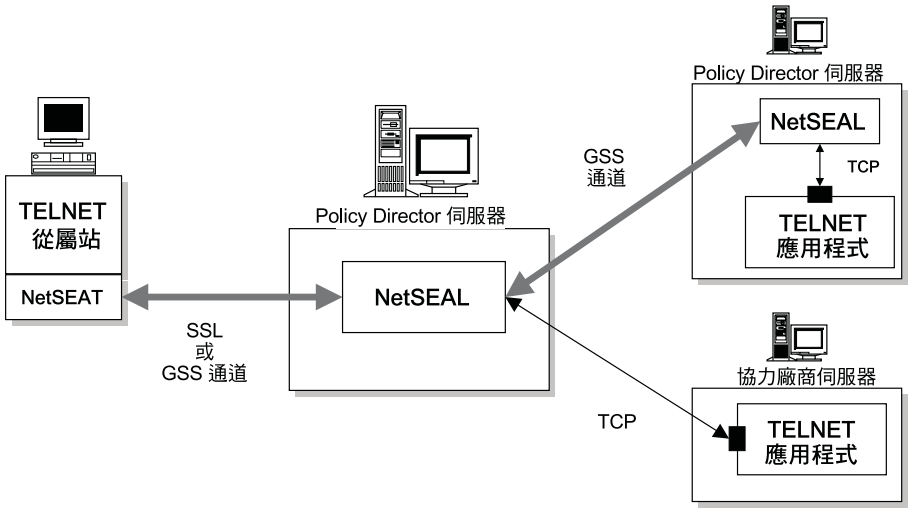
   否-- 拒絕連線要求。

2. 目的地是否爲 Policy Director 伺服器？

   是-- 建立與伺服器間的安全通道。與所要求之埠間建立一條 TCP 連線。

   否-- 與所要求之埠間建立一條 TCP 連線（不安全）。

協力廠商應用伺服器的 TCP 連線往往未到受保護。請在可靠的網路環境中使用此類配置。



接往 Policy Director 伺服器的傳入 TCP 連線

本情況顧及非 NetSEAT TCP 從屬站使用者的狀況。 Policy Director 將此類的從屬站視爲未經身份驗證的。如所要求之埠未受到保護（無 ACL），Policy Director 將容許存取該埠。如有 ACL 保護該埠，「安全管理程式」將檢查 ACL 看看有無未經身份驗證的存取情況。

此種配置可保護對網路服務程式的直接存取。外部權限服務程式可使用從屬站的 IP 位址，來判斷存取權限。

NetSEAL 伺服器會以下列方式完成交易：

1. 該要求是否被 Policy Director 設陷截下（根據埠上的 ACL）？

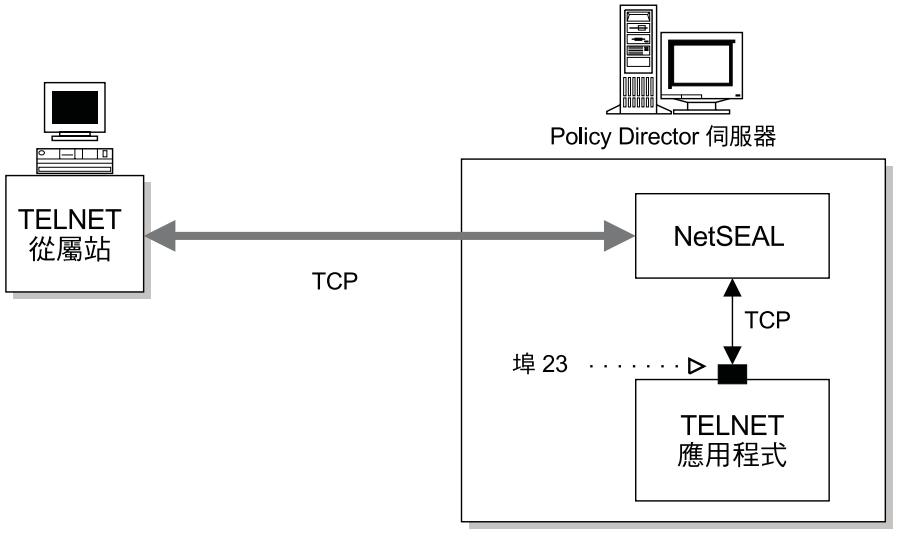
   是-- 將要求傳給「安全管理程式」 (secmgrd)。

   否-- 容許傳入的連線。

2. 是否容許埠上的未經身份驗證要求？

   是-- 與所要求之埠間建立一條 TCP 連線。

   否-- 拒絕連線要求。



說明 NetSEAL 到 NetSEAL 的服務

下列情況說明兩個伺服器間可能發生的交談類型。在這些情況中，是由第一個 NetSEAL 伺服器（與本端從屬站）起始連線，而非由遠端 NetSEAT 從屬站起始連線。

在這些情況中，是由第一個 NetSEAL 伺服器（與本端從屬站）起始連線，而非由遠端 NetSEAT 從屬站起始連線。這個本端從屬站可從伺服器的主控台來操作，或從遠端位置 TELNET 到此伺服器。後端 NetSEAL 伺服器可保護 TCP 應用程式。

這些情況有：

- 『接往 Policy Director 伺服器的外傳連線』.
- 第215頁的『接往受保護主電腦的外傳連線』.

接往 Policy Director 伺服器的外傳連線

請使用 GSS 通道來建立兩個 Policy Director NetSEAL 伺服器間的連線。並且是由第一個 NetSEAL 伺服器（與本端從屬站）起始連線，而非從遠端 NetSEAT 從屬站起始連線。Policy Director 可允許或拒絕連線，並保護任何獲准的通信。

Policy Director 伺服器會以下列方式完成交易：

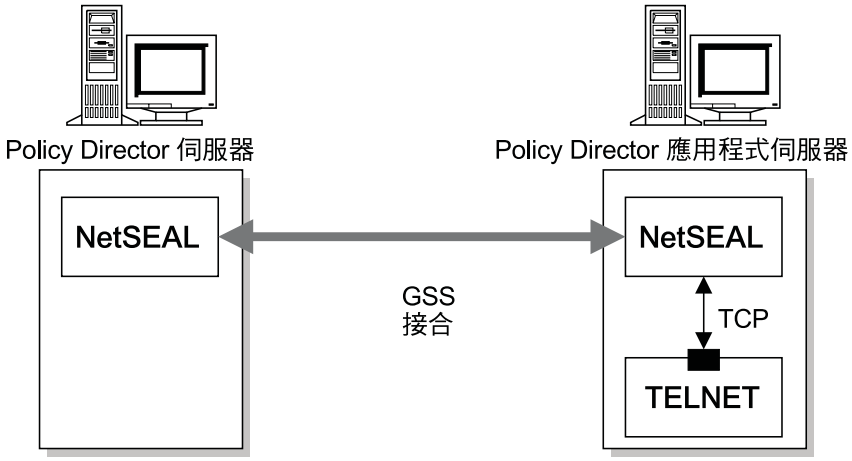
1. 位於目的地機器中的所要求之埠是否受到保護 (ACL)？

   是-- 將要求傳給「安全管理程式」 (secmgrd)。

   否-- 容許外傳的連線。
2. 是否容許埠上的未經身份驗證要求？

   是-- 建立與伺服器間的安全通道。與所要求之埠間建立一條 TCP 連線。

   否-- 拒絕連線要求。



接往受保護主電腦的外傳連線

您可使用 TCP 來建立 Policy Director NetSEAL 伺服器與協力廠商伺服器間的連線。不過，任何經由 TCP 建立的連線並不是安全連線。後端協力廠商伺服器上並無 NetSEAL 伺服器。 Policy Director 只能做到允許或拒絕與後端伺服器間的連線； Policy Director 不能保護經由此種連線的通信。

Policy Director 伺服器會以下列方式完成交易：

1. 位於目的地機器中的所要求之埠是否受到保護 (ACL)？

   是-- 將要求傳給「安全管理程式」 (secmgrd)。

   否-- 容許外傳的連線。
2. 使用者是否有權存取目的地伺服器中的所要求之埠？

   是-- 繼續進行。

   否-- 拒絕連線要求。
3. 埠中是否設定資料完整性與資料隱私性？

   是-- 拒絕連線要求。

   否 -- 與所要求之埠間建立一條 TCP 連線。

介紹 NetSEAL 接合

*NetSEAL 接合*藉經由 Policy Director 伺服器網路將通信轉遞到目的地伺服器或網路，來提供安全的轉遞機制。 NetSEAL 接合會決定經由 Policy Director 伺服器的封包轉遞方向。

NetSEAL 接合是單向的靜態路徑。單向接合可讓每一個 Policy Director 伺服器的管理程式更能做好其網路的控制存取。每一種旅程方向各需要一個個別的 NetSEAL 接合。不過，流經 NetSEAL 接合的資料往往是雙向的。

GSS 通道可保護行經 NetSEAL 接合的通信。之後，通信路徑中的最終 Policy Director 伺服器會使用 TCP 與目的地埠連線。此目的地埠可位於 Policy Director 伺服器本身上。

NetSEAL 接合可經由組織爲通信提供資料保護與安全性。您可根據地理位置或功能性，來劃分組織。例如，當兩個依地理位置分隔之 Policy Director 伺服器間的網路不可靠時，採用 NetSEAL 接合相當有幫助。此外，這兩個 Policy Director 伺服器爲同一安全領域中的成員。

每一個接合各有一個來源 Policy Director 伺服器、一個目的地與一個遞送方向。目的地可以是另一個 Policy Director 伺服器或網路規格。接合可接受簡易的防火牆配置，這是因爲所有行經接合的流量只需要一條經過防火牆的路徑。

配置 NetSEAL 接合

管理者可使用 **ivadmin** 公用程式來建立 NetSEAL 接合。**ivadmin** 公用程式包含各種用以新增、刪除與列出 NetSEAL 接合的指令。您可在兩個 Policy Director 伺服器間建立接合，或在 Policy Director 伺服器與網路間建立接合。

請參閱第251頁的『附錄A. 使用 ivadmin 來進行 Policy Director 管理』。

NetSEAL 接合與存取控制

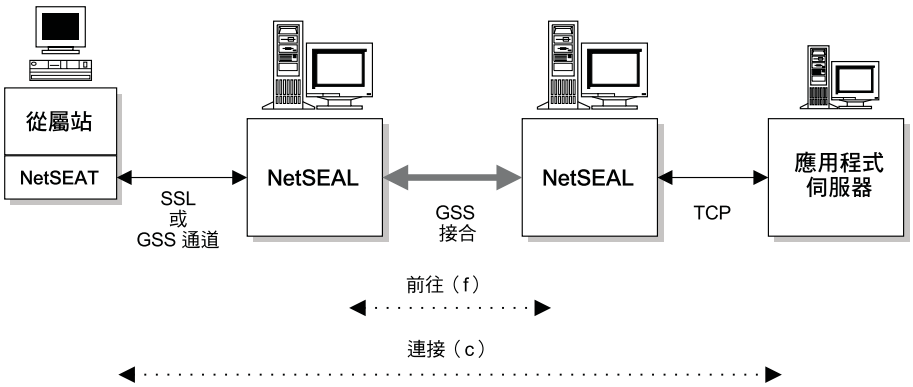
NetSEAL 在有關控制存取應用伺服器上的埠方面，認可兩種 ACL 許可權。

目的地埠物件上的 ACL 會控制對該埠的存取。ACL 項目中必須含有連接 (C) 許可權以容許使用者或群組存取該埠。

負責外傳連線之 Policy Director 伺服器上的 ACL 會控制經由 NetSEAL 接合的遍訪。ACL 項目中必須含有轉遞 (f) 許可權以容許使用者或群組經由接合存取。

請使用與檢查接合伺服器鏈中每一個中間 Policy Director 伺服器物件上的轉遞 (f) 許可權。

NetSEAL 受保護的物件許可權：	存取	說明
C	連接	經由 NetSEAL 伺服器連接本端或遠端受保護的服務程式
f	轉遞	容許外傳的連線行經 NetSEAL 接合；遍訪接合



說明 NetSEAL 接合所控制的服務

NetSEAL 接合可經由組織爲通信提供資料保護與安全性。您可根據地理位置或功能性，來劃分組織。例如，當兩個依地理位置分隔之 Policy Director 伺服器間的網路不可靠時，採用 NetSEAL 接合相當有幫助。此外，這兩個 Policy Director 伺服器爲同一安全領域中的成員。

這些情況有：

- 『接往 Policy Director 伺服器的傳入接合連線』.
- 『接往受保護主電腦的傳入接合連線』.
- 第218頁的『接往所接合之 Policy Director 伺服器的外傳連線』.
- 第219頁的『接往所接合之受保護主電腦的外傳連線』.

接往 Policy Director 伺服器的傳入接合連線

本情況顧及到位於受保護之遠端 Policy Director 伺服器上的應用程式。本情況會在 Policy Director 伺服器間將 GSS 通道明確建立爲 NetSEAL 接合。如今目的地埠的存取控制已將轉遞許可權納入考量。

Policy Director 伺服器會以下列方式完成交易：

1. 使用者能否連接目的地伺服器上的所要求之埠（根據其 ACL 而定）？

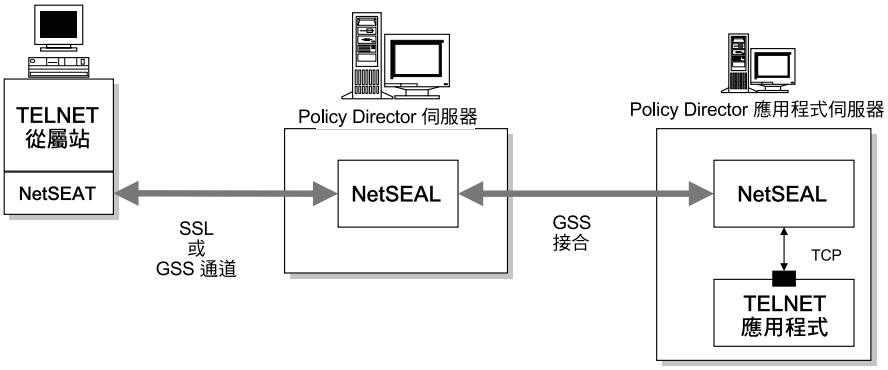
   是-- 繼續進行。

   否-- 拒絕連線要求。

2. 使用者可經由接合加以轉遞嗎？

   是-- 經由 GSS 接合轉遞要求。與所要求之埠間建立一條 TCP 連線。

   否-- 拒絕連線要求。



接往受保護主電腦的傳入接合連線

本情況顧及到位於受保護之遠端協力廠商伺服器上的應用程式。本情況會在 Policy Director 伺服器間將 GSS 通道明確建立爲 NetSEAL 接合。如今目的地埠的存取控制已將轉遞許可權納入考量。

Policy Director 伺服器會以下列方式完成交易：

1. 使用者能否連接目的地伺服器上的所要求之埠（根據其 ACL 而定）？

是-- 繼續進行。

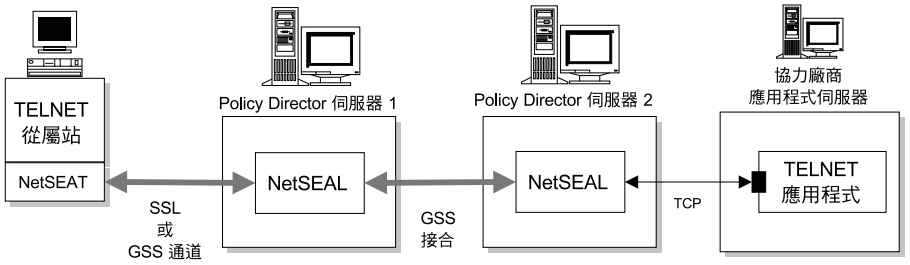
否-- 拒絕連線要求。

2. 使用者可經由接合加以轉遞嗎？

   是-- 經由接合轉遞要求。與所要求之埠間建立一條 TCP 連線。

   否-- 拒絕連線要求。

協力廠商應用伺服器的 TCP 連線往往未到受保護。請在可靠的網路環境中使用此類配置。



接往所接合之 Policy Director 伺服器的外傳連線

本情況顧及到位於受保護之遠端 Policy Director 伺服器上的應用程式。本情況會在 Policy Director 伺服器間將 GSS 通道明確建立爲 NetSEAL 接合。如今對目的地埠的存取控制已將轉遞許可權（可提供理想的中階伺服器保護）納入考量。

Policy Director 伺服器會以下列方式完成交易：

1. 位於目的地機器中的所要求之埠是否受到保護 (ACL)？

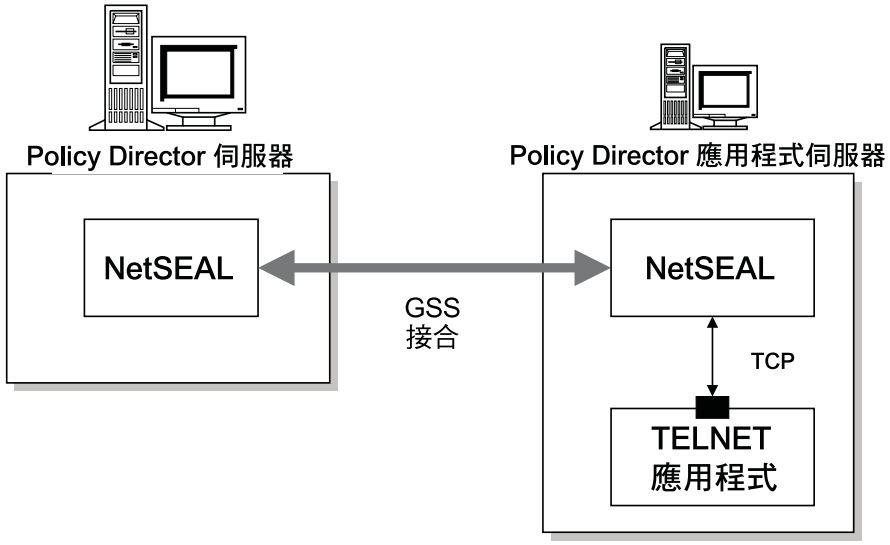
   是-- 將要求傳給「安全管理程式」 (secmgrd)。

   否-- 容許外傳的連線。

2. 使用者可經由接合加以轉遞嗎？

   是-- 經由接合轉遞要求。與所要求之埠間建立一條 TCP 連線。

   否-- 拒絕連線要求。



接往所接合之受保護主電腦的外傳連線

本情況顧及到位於受保護之遠端協力廠商伺服器上的應用程式。本情況會在 Policy Director 伺服器間將 GSS 通道明確建立爲 NetSEAL 接合。如今目的地埠的存取控制已將轉遞許可權納入考量。

Policy Director 伺服器會以下列方式完成交易：

1. 位於目的地機器中的所要求之埠是否受到保護 (ACL)？

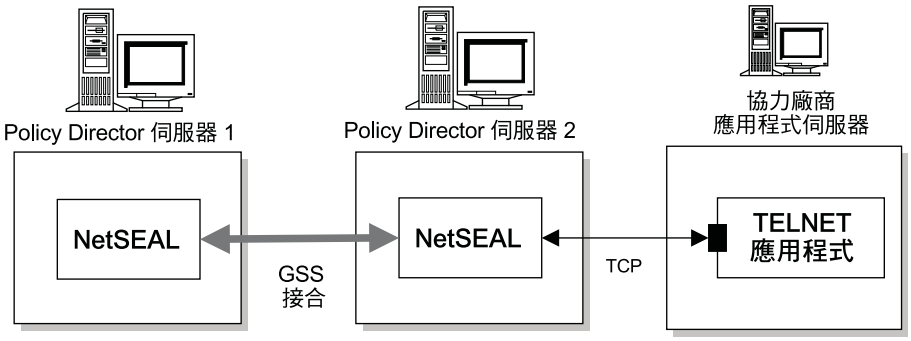
   是-- 將要求傳給「安全管理程式」 (secmgrd)。

   否-- 容許外傳的連線。

2. 使用者可經由接合加以轉遞嗎？

   是-- 經由接合轉遞要求。與所要求之埠間建立一條 TCP 連線。

   否-- 拒絕連線要求。



保護 TCP 服務程式

TCP 服務程式埠上的 ACL 會控制對這些埠的存取。當埠物件上的 ACL 含有 NetSEAL 從屬站使用者的連接 (C) 許可權時，該使用者即可存取特定的 TCP 服務程式。

管理者只需將連接許可權自 ACL 的適當項目中移除，即可拒絕存取 TCP 服務程式。

ACL 許可權也可以控制 NetSEAL 通信的保護品質。有些資料完整與資料隱私許可權組合會決定保護品質。您可控制經由 NetSEAL 接合之外傳通信的保護品質。如要控制保護品質，目的地埠物件上之 ACL 中的項目必須包含資料完整許可權與資料隱私許可權。

依據物件的網址與網路遮罩，測試過的 ACL 最爲明確。當正在尋找之所要求的物件以進行 ACL 檢查時，目的地埠上有無 ACL 便無關緊要。

例如，從屬站正在 TELNET 到配置了如下 ACL 的 10.0.0.1；而依據 ACL3，將授與這個從屬站存取權。Policy Director 會授與存取權，即使相符網路上的埠 23 含有明確的 ACL。

10.0.0.0:255.255.255.0	ACL1
10.0.0.0:255.255.255.0/埠 23	ACL2
10.0.0.1:255.255.255.255	ACL3

第18章 NetSEAL：一般管理作業

Policy Director NetSEAL 是一種「虛擬專用網路（VPN）」解決方案，可保護所有傳入的 TCP/IP 通信。NetSEAL，此種資源管理程式，可控制使用者連接特定 TCP 應用程式的能力。本章將說明您可執行的一般管理作業，以爲您的網路自訂 NetSEAL。

本章包括：

啓用與停用 NetSEAL 安全

請使用 **ivadmin** 公用程式來啓用及停用 NetSEAL。

啓用 NetSEAL

要在特定 Policy Director 伺服器上啓用 NetSEAL 時請輸入：

```
ivadmin> server enable /NetSEAL/hostname
```

其中 *hostname* 是伺服器的主電腦名稱，但不含領域名稱。

當服務程式已啓用，或者服務程式規格無效時， Policy Director 會傳回錯誤。

除非您安裝了 Policy Director 分送中的 NetSEAL 設陷 (IVTrap) 元件，否則依預設，Policy Director 是停用 NetSEAL。

停用 NetSEAL

要在特定 Policy Director 伺服器上停用 NetSEAL 時請輸入：

```
ivadmin> server disable /NetSEAL/hostname
```

NetSEAL 狀態

如要檢查 NetSEAL 伺服器狀態，請使用 **server status** 指令：

```
ivadmin> server status /NetSEAL/hostname
```

狀態報告會顯示以下資訊：

- NetSEAL 伺服器啓用或停用。
- NetSEAL 伺服器可用。

- 副本 NetSEAL 配置資料庫已（或尚未）更新。

使用 NetSEAL 存取控制

基於如下的安全考量，NetSEAL 連線中可使用 Policy Director ACL 許可權：

- 允許存取 TCP 服務程式，像是目的地埠
- 允許行經 NetSEAL 接合轉遞封包
- 確定資料完整與資料隱私

目的地埠物件上的 ACL 會控制對該埠的存取。ACL 項目中必須含有連接 (C) 許可權以容許使用者或群組存取該埠。連接許可權也可管制對受保護網路上之應用伺服器的存取。

負責外傳連線控制之 Policy Director 伺服器上的 ACL 會控制經由 NetSEAL 接合的遍訪。ACL 項目中必須含有轉遞 (f) 許可權以容許使用者或群組經由接合存取。

請使用與檢查接合伺服器鏈中每一個中間 Policy Director 伺服器物件上的轉遞 (f) 許可權。

	存取	說明
C	連接	經由 NetSEAL 伺服器連接本端或遠端受保護的服務程式
f	轉遞	容許外傳的連線行經 NetSEAL 接合；遍訪接合

ACL 許可權也可以控制 NetSEAL 通信的保護品質。有些資料完整許可權與資料隱私許可權的組合會決定保護品質。

您可控制經由 NetSEAL 接合之外傳通信的保護品質。目的地埠物件上之 ACL 中的項目必須含有資料完整 (I) 與資料隱私 (P) 許可權。您無法將資料完整與資料隱私延伸到可靠網路中之協力廠商（非 Policy Director）應用伺服器中。

管理受保護的網路

您可將網路視爲一個受 NetSEAL 保護的非 Policy Director 伺服器。請使用 **ivadmin** 公用程式來定義與管理網路。指令包括新增、刪除與列出受保護的網路。

指令	說明
netseal network add *network netmask* **[***network-alias***]**	
	建立一個受 NetSEAL 保護的新網路。網路/網路遮罩配對爲標準的 IP 網址號碼與網路遮罩。網路別名（選用）可用來識別此網路。如未指定別名，則必須使用網路與網路遮罩配對來識別網路。如網路已存在則會傳回錯誤。
netseal network delete *network-id*	
	將指定的網路從系統中刪除，其中 *network-id* 可對應下列之一： • *network/netmask*（*網路/網路遮罩*）配對 • *network-alias*（*網路別名*） network-id 引數可對應網路/網路遮罩配對或網路別名。系統中所有對此網路的參照將會被移除，包括 NetSEAL 接合。如在資料庫中找不到網路，將會傳回錯誤。
netseal network list	

	顯示資料庫中所有的網路，包括網路與網路遮罩配對以及任何所定義的別名。

範例：

```
ivadmin> netseal network add 10.125.0.0 255.255.255.0 west
```

此指令是在 NetSEAL 保護的網路規格中新增網路節點 10.125.0.0 到 10.125.0.255。同時，此指令指定 `west` 別名給網路規格。

管理 NetSEAL 接合

NetSEAL 接合會決定通信經由 Policy Director 伺服器應行經的方向。您可在兩個 Policy Director 伺服器間或 Policy Director 伺服器與網路間建立接合。請使用 GSS 通道來保護行經兩個 Policy Director 伺服器間之接合的通信。

ivadmin 公用程式用以定義與管理 NetSEAL 接合。指令包括新增、刪除與列出 NetSEAL 接合。

指令	說明
netseal junction add *hostname destination*	
	建立一個由 NetSEAL 伺服器到指定目的地的接合，其中 *hostname* 爲 NetSEAL 伺服器名稱（扣掉領域名稱），*destination* 可對應下列之一： • *pd-server（Policy Director 伺服器）* • *network/netmask（網路/網路遮罩）*配組 • *network-alias（網路別名）* 如接合已存在、主電腦伺服器不存在或目的地不存在，則會傳回錯誤。
netseal junction delete *hostnamedestination*	
	刪除由 NetSEAL 伺服器到指定目的地的接合，其中 *hostname* 爲 NetSEAL 伺服器名稱（扣掉領域名稱），*destination* 可對應下列之一： • *pd-server（Policy Director 伺服器）* • *network/netmask（網路/網路遮罩）*配組 • *network-alias（網路別名）* 若接合目前不存在，則會傳回錯誤。指令對目前的連線不會產生影響。
netseal junction list *hostname*	
	顯示指定 NetSEAL 伺服器的所有 NetSEAL 接合。

範例：

```
ivadmin> netseal junction add clipper west
```

此指令會建立一個由 NetSEAL 伺服器 `clipper` 到別名爲 `west` 網路的接合。同時，指令定義遞送方向（`clipper` 到 `west`）；NetSEAL 接合爲單向的。

管理受保護之埠

Policy Director NetSEAL 伺服器可爲特定埠、主電腦與網路，提供安全服務程式。例如，您可以將 NetSEAL 伺服器配置成保護特定埠上的 TELNET 流量。

ivadmin netseal 公用程式用以定義您想讓 NetSEAL 保護的埠清單。指令包括新增、刪除與列出受保護之埠。您可指定埠給 Policy Director 伺服器或網路。

指令	說明
netseal port add *destination port-id*	
	保護與指定 *port-id* 上之指定目的地的連線，其中 *destination* 可對應下列之一： • *pd-server（Policy Director 伺服器）* • *network netmask（網路/網路遮罩）* • *network-alias（網路別名）* *port-id* 可對應下列之一： • *port（埠）* • *port-range（埠範圍）* • *port-alias（埠別名）* 如果埠已受保護、伺服器不存在或埠別名不存在，則會傳回錯誤。
netseal port delete *destination port-id*	
	停止與指定埠上之指定目的地的保護中連線，其中 *destination* 可對應下列之一： • *pd-server（Policy Director 伺服器）* • *network netmask（網路/網路遮罩）* • *network-alias（網路別名）* *port-id* 可對應下列之一： • *port（埠）* • *port-range（埠範圍）* • *port-alias（埠別名）* 如果埠尚未受到保護、伺服器不存在或埠別名不存在，則會傳回錯誤。
netseal port list *destination*	
	列出指定目的地的所有埠，其中 *destination* 可對應下列之一： • *pd-server（Policy Director 伺服器）* • *network netmask（網路/網路遮罩）* • *network-alias（網路別名）* 如伺服器不存在，則會傳回錯誤。

註: 請以兩個埠號其間以連字符號隔開，來表示埠範圍（例如 22-88）。

範例：

```
ivadmin> port add west 23
```

此指定是將網路（別名爲 “west”）上的埠號 23 定義成受 NetSEAL 保護之埠。

管理受保護的埠別名

ivadmin 公用程式用以定義與管理埠別名。指令包括新增、刪除與列出埠別名。請使用埠別名，以較有意義的方法來識別設陷的埠範圍。

指令	說明

netseal port-alias add *port-spec port-alias*	
	爲指定的埠規格建立新的埠別名，其中 *port-spec* 可對應下列之一： • *port（埠）* • *port-range（埠範圍）* 如果該埠範圍已有其它別名，將會傳回錯誤。
netseal port-alias delete *port-id*	
	將指定 port-id 的埠別名從系統中刪除，其中 *port-id* 可對應下列之一： • *port（埠）* • *port-range（埠範圍）* • *port-alias（埠別名）* 如在資料庫中找不到埠別名，將會傳回錯誤。
netseal port-alias list	
	列出在資料庫中找到的所有埠別名。

範例：

```
ivadmin> netseal port-alias add 23 telnet
```

此指令會爲埠號 23 建立埠別名 telnet。

```
ivadmin> netseal port-alias add 5000-5010 pilot
```

此指令會爲埠範圍 5000 到 5010 建立埠別名 “pilot”。

配置可靠的主電腦與可靠的網路

Policy Director NetSEAL 伺服器可爲特定埠、主電腦與網路，提供安全服務程式。例如，您可以將 NetSEAL 伺服器配置成保護 Policy Director 伺服器中之特定埠上的 TELNET 流量。此外，NetSEAL 伺服器可信任某些系統（可靠的主電腦）與某些主電腦集合（可靠的網路）。

在 secmgrd.conf 配置檔之 [trusted_hosts] 或 [trusted_networks] 段落中，含有用以識別可靠主電腦與可靠網路的參數。

可靠的主電腦

通常您的 NetSEAL 伺服器會與特定之高可靠度伺服器（主電腦）通信。您可讓 NetSEAL 將這些伺服器所發出的傳入要求免受存取控制的制約，藉以讓效能最佳化。

註: 識別可靠的主電腦會讓您的系統易受 IP 捏造的侵犯。請確定您可保護任何可靠的主電腦免遭此類侵犯。 attacks.

依預設，Policy Director 不會識別任何可靠的主電腦。

如要識別可靠的主電腦，請跳至 [trusted_hosts] 段落，並列出 IP 位址與伺服器名稱。

例如，要信任名爲 “typhoon”，IP 位址爲 220.12.35.102 之伺服器所發出的所有要求時，請鍵入：

```
[trusted_hosts]
220.12.35.102 = typhoon
```

當使用 NetSEAL 設陷來保護機器時，通常需要信任本端機器。信任本端機器可讓執行於此機器上的服務程式繼續運作。即使對某一埠或某個埠範圍停用未經身份驗證的存取特性，這些服務程式仍照常執行。

Policy Director 需要下列這些項目，以*信任*本端機器：

- 一筆本端主電腦的項目
- 每一個與該機器有關之 IP 位址的項目

例如，NetSEAL 伺服器 typhoon 的 IP 位址可爲 220.12.35.102。同一伺服器中之另一個程序的本端主電腦 IP 位址爲 127.0.0.1。如要信任同位於 NetSEAL 伺服器 typhoon 之其它程序所發出的本端要求時，可鍵入：

```
[trusted_hosts]
220.12.35.102 = typhoon
127.0.0.1 = localhost
```

一般而言，一部機器只會有一個 IP 位址，不過，由於有些機器會與一個以上的網路連接，因此可能會有一個以上的位址。

可靠的網路

如果您的網路含有整個子網路或可靠系統的區域網路，則可指定整個子網路而不必列出每一個主電腦。

依預設，Policy Director 不會定義任何可靠的網路。

如要識別可靠的網路，請跳至 [trusted_networks] 段落，並列出子網路 IP 位址與網路遮罩。

例如，要信任子網路 192.96.32.0 所發出的所有要求時，請鍵入：

```
[trusted_networks]
192.96.32.0 = 255.255.255.0
```

設定 SSL 逾時參數

有關您可設定的 SSL 逾時包括：

- 『設定 SSL 階段作業快取逾時』.
- 第227頁的『設定 SSL 連線逾時』.

設定 SSL 階段作業快取逾時

secmgrd.conf 配置檔的 [ssl] 段落包含設定靜態 SSL 階段作業快取逾時的參數。

NetSEAL 會在內部快取證明資訊。階段作業快取逾時參數用以指出身份驗證證明資訊可留在 NetSEAL 記憶體中多久。

參數不是指非作用逾時。此值對映的是*證明的使用期限*（Credential Lifetime）*證明的逾時*（Credential Timeout）。其目的是當抵達指定的逾時上限時，強迫使用者重新鑑定，藉以強化安全性。

預設快取逾時值（以秒計）爲：

```
[ssl]
ssl-cache-timeout = 3600
```

調整這個值來平衡伺服器效能以及使用者便利性，端視伺服器必須處理的 SSL 要求數量而定。

設定 SSL 連線逾時

在 secmgrd.conf 配置檔的 [ssl] 段落中，含有用以設定 SSL 連線逾時的參數。

一旦 NetSEAL 接受 NetSEAT 從屬站經由 NetSEAL SSL 通道所發出的 SSL 連線，即會發生 SSL 通信協定交握。此參數用以控制當 SSL 連線開始時，「安全管理程式」在等待 NetSEAT 起始 SSL 交握上要等多久。待過了此時間後，「安全管理程式」即會關閉連線。

預設的 SSL 連線逾時（以秒計）爲：

```
[ssl]
ssl-init-connect-timeout = 120
```

配置 NetSEAL 連線

配置 NetSEAL 連線的相關參數位於 secmgrd.conf 配置檔的 [netseal] 段落中。

max-connections 用以指定 NetSEAL 容許的同時連線數上限。

Policy Director 安裝會設定如下的預設值：

```
[netseal]
max-connections = 32
```

您可能想增加此值，以符合您網路中的流量情況。如果 max-connections 設得過低，則在負載繁重下將會拒絕連線。若設得過高，則是浪費資源與降低伺服器效能。

註: 此配置參數的下限爲 20。即使想設定低於 20 的值，系統仍只會採用預設值 20。

第19章 NetSEAT：概觀

Policy Director NetSEAT 從屬站可讓 Windows 從屬站參與 Policy Director 安全領域。NetSEAT 可在 Windows 從屬站與 Policy Director 伺服器間提供安全通道機制。NetSEAT 使用通道機制或 GSS 通道機制來加密通信。

本章包括：

介紹 NetSEAT 從屬站

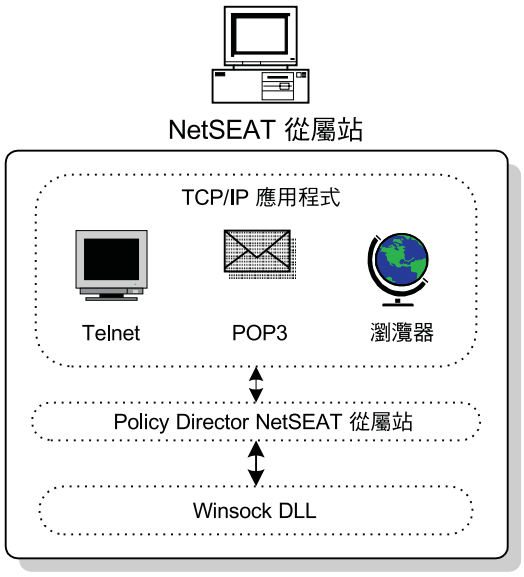
Policy Director NetSEAT 從屬站可讓 Windows 從屬站安全無虞地與 Policy Director WebSEAL 及 NetSEAL 伺服器通信。當您新增 NetSEAT 至 Windows 工作站中時，即會將該工作站配置到 Policy Director 安全領域中。在安全領域中，NetSEAT 可用到 Policy Director 的身份驗證與授權安全服務程式。

NetSEAT 可提供網路通信協定層次的身份驗證與訊息保護。應用程式不必爲了使用 NetSEAT 而重新編譯或重新鏈結。

NetSEAT 會在網路要求行經 Winsock 層前加以攔截，藉以保護 Windows 從屬站與 Policy Director 伺服器間的網路流量。 NetSEAT 會使用其配置資訊，來辨識同屬 TCP/IP 應用程式產生的要求。這些同屬 TCP/IP 應用程式包括 TELNET、POP3 或 HTTP。

當有從屬站對 Policy Director 伺服器上的應用程式發出要求時， NetSEAT 即會建立一條通往 Policy Director 伺服器的透明、安全通道。接著 NetSEAT 即經由通道重導從屬站要求。

NetSEAT 是以下列兩法方法之一來保護與加密和 Policy Director 伺服器間的通信： SSL 通道與 GSS 通道。 SSL 通道是以 SSL 來加密通信。而 GSS 通道則採 GSS API 來加密通信。



支援的配置

您可以按下列中的說明，根據各種不同的目的來佈署 NetSEAT 從屬站：

- 『「虛擬專用網路」從屬站』。
- 『Windows NT 上之 Policy Director 的支援模組』。
- 第231頁的『Policy Director「管理主控台」的支援模組』。

「虛擬專用網路」從屬站

您可將 NetSEAT 配置成一種「虛擬專用網路 (VPN)」從屬站，以使用安全通道，與 Policy Director NetSEAL 伺服器之間進行安全的通信鏈結。

在扮演 VPN 從屬站角色下，NetSEAT 可使用下列通道類型來加密通信：

- SSL
- GSS

Windows NT 上之 Policy Director 的支援模組

在每次安裝 Policy Director for Windows NT 伺服器元件時， Policy Director 會將 NetSEAT 安裝成支援模組。 Policy Director for Solaris 與 AIX 則不要求 NetSEAT 從屬站提供此支援。

在這種角色下，NetSEAT 從屬站會提供核心設陷，供 Policy Director 安全服務程式內部使用。

做爲 Policy Director for Windows NT 支援模組， NetSEAT 需用到下列服務程式：

- 目錄服務分配管理系統
- GSS 通道

當您將 NetSEAT 從屬站以支援模組方式安裝在 Policy Director for Windows NT 或 Windows 上的 Policy Director「管理主控台」中時，請使用 GSS 通道機制。

Policy Director「管理主控台」的支援模組

當在 Windows 從屬站中執行 Policy Director「管理主控台」時，您必須將 NetSEAT 安裝成支援模組。在此種配置下， NetSEAT 可讓管理者從 Windows 系統使用「管理主控台」來執行管理作業。 Windows 系統用不著安裝任何 Policy Director 伺服器元件。

做爲「管理主控台」的支援模組，NetSEAT 需用到如下的服務程式：

- 目錄服務分配管理系統
- GSS 通道

當您將 NetSEAT 從屬站以支援模組方式安裝在 Policy Director for Windows NT 或 Windows 上的 Policy Director「管理主控台」中時，請使用 GSS 通道機制。

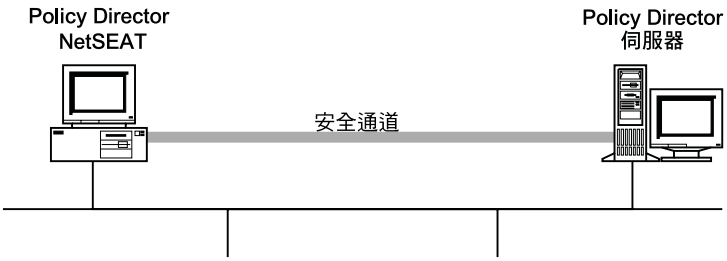
安全通道機制

在轉遞從屬站要求前，NetSEAT 會透過安全通道聯絡 Policy Director 安全伺服器（針對適當的安全領域）。此外，NetSEAT 也會使用安全通道來建立從屬站的身份與證明。當從屬站身份驗證成功時，NetSEAT 即會封裝所要求的交易於另一條安全通道中。同時，NetSEAT 會根據適用的安全設定來完成所要的交易。

例如，當 Web 瀏覽器要求存取一項受 WebSEAL 保護的服務程式或資源時， NetSEAT 即透通地截下該要求。如果這是第一次向 Policy Director 提出要求，而您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。

在 Policy Director 鑑定使用者後， NetSEAT 即透通地放行以這些初始證明爲基礎的後續要求與安全通道。 NetSEAT 對於每一項要求便是根據這些證明來決定是否授權。

NetSEAT 可建立兩種不同的安全通道類型；請參閱『使用 SSL 通道機制』與第232頁的『使用 GSS 通道機制』。



使用 SSL 通道機制

*SSL 通道機制*是指採用 SSL 通信協定的安全通道。當佈署成 Policy Director NetSEAL 的 VPN 從屬站時， NetSEAT 所用的是 SSL 通道機制。使用 SSL 通道可簡化 NetSEAT 配置。在此情況下，管理者不必在 Policy Director 安全領域中指定 DCE 服務程式的配置。

當從屬站想存取受防火牆保護的資料時，SSL 通道相當好用。在此模式下，NetSEAT 是以單一埠來應付所有與防火牆後之 Policy Director 伺服器間的通信。 Policy Director 會封裝所有經由埠的通信於一條安全通道中。

在 NetSEAT 配置期間，您可在通過防火牆時指定想用的埠號。埠號必須與配置在 NetSEAL 伺服器上之埠相符。

凡經由 LDAP 使用者登錄或 DCE 使用者登錄鑑定過的使用者，可使用 SSL 通道機制。

使用 GSS 通道機制

*GSS 通道機制*一詞是指採用「同屬安全服務 API (GSS API)」的一種安全通道。NetSEAT 在與 DCE cell 通信時使用的是 GSS 通道。

在此模式下，NetSEAT 從屬站會使用 DCE cell 中之其它伺服器上的「安全管理程式 (secd)」與「時間伺服器 (dtsd)」。NetSEAT 也使用 Policy Director 的「目錄服務分配管理系統」，代理向 DCE cell 中的 「Cell 目錄服務程式 (cdsd)」提出名稱空間查閱要求。

當使用者 PKI 登入經由 Entrust 從屬站與 Policy Director 安全領域中的使用者身份整合在一起時，是採用安全 GSS 通道。在此情況下，使用者是透過 Entrust PKI 從屬站登入其工作站。當使用者試著使用 Policy Director 身份驗證與權限服務程式時，即會在 NetSEAT 與 Policy Director 伺服器間建立一條安全通道。 Policy Director 伺服器會自動將 PKI 登入身份對映至使用者的 Policy Director 身份，做爲身份驗證與授權的判別。

GSS 通道機制不適用於經由 LDAP 使用者登錄鑑定的使用者。

存取受保護的伺服器

NetSEAT 從屬站可使用它與 Policy Director NetSEAL 伺服器間的安全通道，將要求傳給任何遠端應用伺服器。這些遠端應用伺服器受 NetSEAL 伺服器的保護。在 NetSEAT 配置期間，管理者可指定：

- 應用伺服器的名稱。
- 負責保護的 NetSEAL 伺服器。
- NetSEAT 與 NetSEAL 間所用的安全通道類型（SSL 或 GSS 通道）。

如有配置此資訊，NetSEAT 會截下 Windows 從屬站向應用伺服器提出的要求。接著，NetSEAT 會將這些要求經由安全通道遞給 Policy Director NetSEAL 伺服器。

如 Policy Director NetSEAL 有保護子網路，您也可以將 NetSEAT 配置成存取整個受保護的子網路。像受 Policy Director NetSEAL 伺服器保護免被網際網路侵入的企業內部網路即是一例。

目錄服務分配管理系統

當做爲 Policy Director 伺服器與 Windows 中之「管理主控台」之支援模組（GSS 通道機制）時， NetSEAT 需要「目錄服務分配管理系統 (DSB)」服務程式。在與 Policy Director 伺服器通信時需用到 DSB。 DSB 會代理同安全領域中之「Cell 目錄服務程式」的名稱空間查閱工作。

Policy Director 會自動將 DSB 視爲「Policy Director 管理伺服器 (IVMgr)」套裝軟體的一部份加以安裝。您必須將 NetSEAT 配置成清楚主導「目錄服務分配管理系統」之伺服器系統的名稱。

第20章 NetSEAT：一般管理作業

本章說明系統管理作業，包括配置 NetSEAT 從屬站、管理安全上下文，以及尋找並更正問題（*疑難排解*）。

本章包括：

配置 NetSEAT 從屬站

請將每一個 NetSEAT 從屬站配置到 Policy Director 安全領域中。您可在安裝時配置 NetSEAT 從屬站，或在安裝後擇期配置。 NetSEAT 配置工具（公用程式）提供一種圖形式使用者介面，可讓管理者輕鬆配置從屬站。

請在 NetSEAT 參與的安全領域上下文中執行所有的配置作業。

有些配置作業只適用於其中一種安全通道類型（GSS 或 SSL）的配置。NetSEAT 會使用這些安全通道來與 Policy Director 伺服器通信。對 NetSEAL 伺服器而言純粹配置成 SSL 從屬站的 NetSEAT 從屬站則只需要有限的配置作業子集。

下表顯示對應每一種安全通道類型的配置作業：

通道類型	配置作業
GSS 與 SSL 兩者	• 第234頁的『新增 NetSEAT 到安全領域中』 • 第236頁的『配置 NetSEAL 伺服器』 • 第242頁的『拒絕存取網路資源』
限 GSS	• 第234頁的『新增 DCE 伺服器』 • 第235頁的『設定 DCE 伺服器內容』 • 第238頁的『配置整合登入』 • 第240頁的『配置進階登入（PKI 整合）』. • 第242頁的『設定時差上限』

限 SSL	第242頁的『配置 SSL Proxy』

NetSEAT 提供數種 DCE 安全公用程式的擴充，也提供一種公用程式用以檢查 DCE 服務程式的有用性。

只有在您將 NetSEAT 配置成使用 GSS 通道機制時，才能使用這些公用程式。

下列各節說明這些公用程式：

- 使用 NetSEAT 安全公用程式（請參閱第243頁的『使用 NetSEAT 安全公用程式』）。
- 使用 **netseat_ping** 來尋找與更正問題（請參閱第244頁的『使用 netseat_ping 解決問題』）。

啓動 NetSEAT 配置工具

在完成初次安裝與配置後，如要重新配置 NetSEAT，請使用 NetSEAT 配置工具。或者，如果您在初次安裝期間延後配置，而今要配置 NetSEAT，請使用 NetSEAT 配置工具。

啓動 NetSEAT 配置工具的方法有二：

- 要從 Windows 桌面啓動 NetSEAT 配置工具時，請按一下**開始 → 程式集 → Policy Director → NetSEAT → NetSEAT 配置**
- 如要從「系統匣」中的 **NetSEAT** 圖示啓動 NetSEAT 配置工具時，請以右滑鼠按鈕按一下 **NetSEAT** 圖示，然後選取**內容**。

新增 NetSEAT 到安全領域中

如要新增 NetSEAT 到安全領域中，請完成下列步驟：

1. 啓動 NetSEAT 配置工具。當啓動時，NetSEAT 配置工具會在 NetSEAT 配置視窗中顯示**安全領域**標籤。
2. 按一下**新增**。

   出現「新安全領域」對話框。
3. 鍵入 NetSEAT 隸屬的安全領域名稱。
4. 爲此領域選取支援通信協定，然後按一下**確定**。
   - 如果您選取**啓用 GSS**，請跳至『新增 DCE 伺服器』。
   - 如果您選取**僅啓用 SSL**，請跳至第236頁的『配置 NetSEAL 伺服器』。
5. **僅 GSS 通道機制**--如果您配置了一個以上的領域，請回到**安全領域**標籤。請標明出使用者登入的預設領域。然後按一下**設為預設值**。

   如果您只配置一個領域，領域會自動變爲預設值。
6. 按一下**確定**。

新增 DCE 伺服器

如果您將領域配置成啓用 GSS 安全通道，您還必須設定其它的配置選項。

對於 NetSEAT 接合的安全領域（或 *cell*），請取得 cell 中 Policy Director 安全伺服器的名稱。請指出每一個所提供之系統的基本安全 (DCE) 服務程式。請針對每一個伺服器，判斷它是否提供：

- **安全** -- 安全服務程式 (secd)
- **時間** -- 時間服務程式 (dtsd)
- **DSB** -- 目錄服務分配管理系統 (dsb)
- **CDS** -- Cell 目錄服務程式 (cdsd)

  只有在「目錄服務分配管理系統 (DSB)」執行於 NetSEAT 從屬站中時， NetSEAT 才需要知道 CDS 的位置。通常您是將 DSB 配置成執行於「Policy Director 管理伺服器 (IVMgr)」所在的同一伺服器上。

在建立新安全領域的項目並按下**確定**後，會出現「安全領域內容」對話框。

1. 按一下**新增**。

   出現「新增 DCE 伺服器」對話框。
2. 鍵入此安全領域中提供 DCE 服務程式的伺服器名稱。
3. 爲每一個伺服器選出下列一或多個服務程式：**安全**、**時間**、**DSB** 或 **CDS**。
4. 如果您想爲這個 DCE 伺服器設定任何進階內容，可按一下**進階**（選用）。

   請參閱『設定 DCE 伺服器內容』。
5. 按一下**確定**完成指定 DCE 伺服器上之所支援服務程式的設定。

   回到「安全領域內容」對話框。
6. 接受下列預設值：
   - 整合登入支援：**停用**
   - 進階登入：**限 DCE 登入**

   如果您想選擇性地爲安全領域配置整合登入支援與進階登入，請參閱下列各節：
   - 配置整合登入（請參閱第238頁的『配置整合登入』）。
   - 配置進階登入（請參閱第240頁的『配置進階登入（PKI 整合）』）。
7. 當您完成此 DCE 伺服器的配置後，請按一下**確定**。

   重新出現「安全領域」視窗。此時，您已完成新增 DCE 伺服器所需的配置作業。

設定 DCE 伺服器內容

您可在配置 DCE 伺服器期間，在「進階 DCE 伺服器內容」對話框中配置下列各值。此配置作業爲選用的。

通信協定與埠

對於每一個 DCE 伺服器，您可選擇性地指定每一個安全服務程式所用的通信協定（TCP 或 UDP）。您可使用此特性來配置經由防火牆（如 IBM SecureWay Firewall 4.1 版，此爲 IBM SecureWay Boundary Server 產品的元件）的作業。

例如，您可取消選取 DCE 服務程式的 UDP 存取，並指定防火牆管理者已配置的 TCP 埠號。

優先順序層次

當您在定義有一或多個服務程式之多個副本可用的領域時，可指定 NetSEAT 存取每一種服務程式的順序。您可爲各服務程式指定一個正整數，以設定其優先順序。數值越大優先順序越高。

管理者可藉由此特性來最佳化效能，亦即讓 NetSEAT 最先跳至最近（就電子而言）的服務程式。如果該服務程式無法使用，依預設，NetSEAT 將跳至優先順序次高之服務程式的副本。

1. 如要配置進階內容，請跳至「新增 DCE 伺服器」對話框。
2. 選取 **DCE 伺服器**。
3. 按一下**進階**。

   出現「進階 DCE 伺服器內容」對話框。
4. 如要限制聯絡 DCE 服務程式時所用的通信協定，請取消選取適當 DCE 服務程式旁的勾選框。取消選取勾選框會移除您不想啓用的通信協定。
5. 如有需要請在適當 DCE 服務程式旁的欄位中鍵入埠號。
6. 設定每一種 DCE 服務程式的優先順序層次。
7. 按一下**確定**。

配置 NetSEAL 伺服器

如要將 NetSEAT 配置成與 NetSEAL 伺服器通信，請完成下列步驟：

1. 跳至 **NetSEAL 伺服器**標籤，並選取下拉清單中的安全領域。
2. 按一下**新增**。

   出現「新增 NetSEAL 伺服器」對話框。
3. 鍵入 NetSEAL 伺服器的機器名稱。
4. 如果 NetSEAL 在 GSS 或 SSL 通道機制方面不是使用預設埠，請在適當欄位中鍵入這些埠號。否則，則接受預設值。
   - 在建立安全領域項目期間未啓用的通信協定將變成灰色。
   - 如果啓用了 GSS 通道機制，請勿選取**指定 Principal 名稱**勾選框。只有在求與舊版相容（後相容性）時，才使用此特性。
5. 如果您使用的是 SSL 通道機制，且您的 NetSEAT 配置中配置了 SSL Proxy 伺服器， Policy Director 會自動選取**使用 Proxy 伺服器**勾選框。

   當您未啓用 SSL Proxy 伺服器時，**使用 Proxy 伺服器**勾選框不會起作用（未勾選且變成灰色）。如要在 NetSEAT 配置中啓用 SSL Proxy 伺服器，請參閱第242頁的『配置 SSL Proxy』。
6. 按一下**確定**。

   再次出現 **NetSEAL 伺服器**標籤。此時， NetSEAL 伺服器已新增到 NetSEAT 配置中。

新增受保護的伺服器

您可將 NetSEAT 配置成指定一條與應用伺服器（受 NetSEAL 伺服器保護）間的通信通道。

當 NetSEAT 從屬站採用 GSS 或 SSL 通道機制時，即可使用此選項。

當您在 NetSEAT 配置中加入應用伺服器後， NetSEAT 會攔截 Windows 從屬站向應用伺服器所提的要求。接著， NetSEAT 會將這些要求經由安全通道遞給 NetSEAL 伺服器。

如要在 NetSEAT 配置中新增受保護的伺服器時，請提供下列資訊：

欄位	定義
機器名稱	在 TCP/IP 領域中用以識別應用伺服器的名稱。
通道目的地	負責保護應用伺服器的 NetSEAL 伺服器名稱。
埠範圍	受 NetSEAL 伺服器保護之受保護伺服器上的埠號。此埠（或埠範圍）是透過 ivadmin 指令指定於 NetSEAL 伺服器中。
選取的通信協定	通道機制通信協定。安全領域中可啓用 GSS 與 SSL 兩種。Policy Director 方面請指定 SSL 通道機制。 GSS 通道機制則是用於 NetSEAL 對 NetSEAL 的連線。

如要將 NetSEAT 配置成能辨識送給受保護伺服器的要求，請完成下列步驟：

1. 按一下**主電腦安全性**標籤。
2. 按一下**新增**。

   出現「新增受保護的伺服器」對話框。
3. 「機器名稱」方面，請鍵入受 NetSEAL 保護之伺服器的機器名稱。

   只有一個 NetSEAL 伺服器能保護應用伺服器。
4. 在「通道目的地」方面，請使用下拉清單選出保護伺服器的 NetSEAL 伺服器。
5. 必要時使用下拉清單，選出適當的通道機制通信協定。
6. 按一下**新增**。

   出現「新增埠範圍」對話框。
7. 指定 NetSEAL 伺服器上 NetSEAL 和受保護應用伺服器通信時所用之埠或埠範圍。
8. 按一下**確定**。

   傳回「新增受保護的伺服器」對話框。

   例如，下列對話框項目所設的值如下：
   - 名爲 “sunshine” 的 NetSEAL 伺服器負責保護一個名爲 “thunder” 的受保護伺服器。
   - sunshine 伺服器會保護和 thunder 間之埠 5000-5005 範圍的通信。
   - Policy Director 在 NetSEAT 從屬站與 NetSEAL 伺服器 “sunshine” 間定義一條安全通道。
   - 安全通道的類型爲 SSL 通道機制。
9. 按一下**確定**。

   再次出現**主電腦安全性**標籤。

   Policy Director 在 NetSEAT 配置中加入受保護的伺服器。

新增受保護的子網路

您可將 NetSEAT 配置成指定一條與子網路（受 NetSEAL 伺服器保護）間的通信通道。當 NetSEAT 從屬站採用 GSS 或 SSL 通道機制時，即可使用此選項。

當您在 NetSEAT 配置中加入應用程式子網路時， NetSEAT 會攔截 Windows 從屬站向應用程式子網路所提的要求。接著，NetSEAT 會將這些要求經由安全通道遞給 NetSEAL 伺服器。

如要在 NetSEAT 配置中新增受保護的子網路時，請提供下列資訊：

欄位	定義
子網路中任何機器的名稱	受保護子網路中任何伺服器的名稱。
網路遮罩	子網路的網路遮罩（例如 255.255.0.0）。
通道目的地	負責保護子網路的 NetSEAL 伺服器名稱。
選取通信協定	通道機制通信協定。安全領域中可啓用 GSS 與 SSL 兩種。Policy Director 方面請指定 SSL 通道機制。 GSS 通道機制則是用於 NetSEAL 對 NetSEAL 的連線。

如要將 NetSEAT 配置成能辨識送給受 NetSEAL 伺服器保護之子網路的要求，請完成下列步驟：

1. 按一下**子網路安全性**標籤。
2. 選取內含 NetSEAL 伺服器（負責保護子網路）的安全領域。
3. 按一下**新增**。

   出現「新增受保護的子網路」對話框。
4. 鍵入受 NetSEAL 伺服器保護之子網路上的任何機器名稱。

   只有一個 NetSEAL 伺服器能保護應用程式子網路。
5. 鍵入子網路的網路遮罩。
6. 在「通道目的地」方面，請使用下拉清單選出保護子網路的 NetSEAL 伺服器。
7. 必要時使用下拉清單，選出適當的通道機制通信協定。

   例如，下列項目是讓 NetSEAT 存取網路遮罩爲 255.255.0.0 的子網路。子網路中系統名稱爲 “thunder”。負責保護子網路的 NetSEAL 伺服器名爲 “sunshine”，它也是 SSL 通道目的地。

   子網路中任何機器的名稱： `thunder`

   網路遮罩： `255.255.0.0`

   通道目的地 `sunshine`

   選取通信協定 `SSL`
8. 按一下**確定**。

   再次出現**子網路安全性**標籤。

   Policy Director 已將 NetSEAT 從屬站配置成與受保護的子網路通信。

配置整合登入

您可在安裝 NetSEAT 期間，選擇安裝整合登入支援。 NetSEAT 安裝作業會將 Windows NT 登錄變更爲可支援整合登入。

在您安裝整合登入後， NetSEAT 配置工具可針對每一個安全領域啓用或停用整合登入。

您可在初次安裝與配置 NetSEAT 期間配置整合登入。或者，您可日後再配置之。您得針對各個安全領域個別設定整合登入配置。

在配置整合登入之前，NetSEAT 使用者應完成下列作業：

- 取得需要自動登入之各安全領域中的帳戶。
- 將 NetSEAT 從屬站配置成每一個安全領域中的成員。
- 讓登入安全領域時所用的使用者名稱與密碼，和 Windows NT 領域中所用的同步。

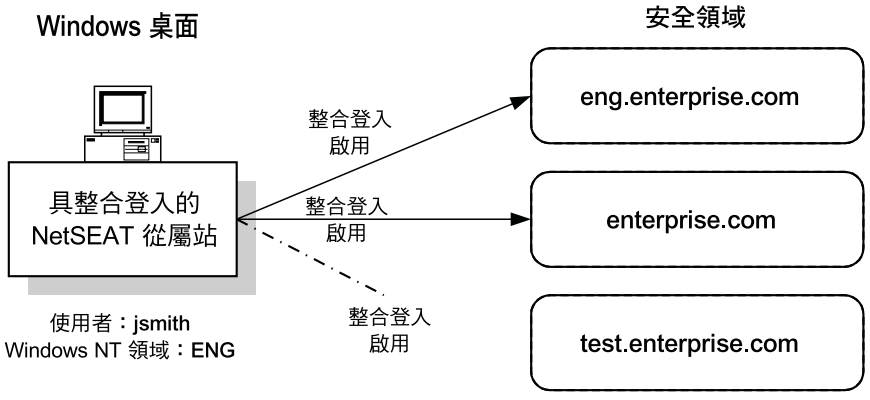
檢視整合登入配置範例

John Smith 工程師在 Windows 中的使用者名稱爲 jsmith，通常是登入 Windows NT 領域 ENG。他以如下方式登入數個安全領域：

安全領域名稱	安全領域使用者帳戶	安全領域的說明
eng.enterprise.com	jsmith	工程部門的安全領域
enterprise.com	ENG/jsmith	整個公司的安全領域
test.enterprise.com	test_user	僅供測試用的小型安全領域。測試 Cell 不會維護完整的使用者名稱登錄。反而，使用者是以 test_user 登入。

John Smith 使用 NetSEAT 配置工具，按如下爲每一個安全領域配置整合登入：

安全領域	整合登入配置
eng.enterprise.com	啓用整合登入，並配置成將 Microsoft Windows NT 使用者 jsmith 對映至安全領域使用者 jsmith，並自動將 jsmith 登入到 eng.enterprise.com 中。
enterprise.com	啓用整合登入，並配置成將 Microsoft Windows NT 使用者 jsmith 對映至安全領域使用者 ENG/jsmith，並自動將 ENG/jsmith 登入到 enterprise.com 中。
test.enterprise.com	停用整合登入，這是因爲 jsmith 必須以使用者 test_user 自行登入此 Cell 中。



配置整合登入

如要配置整合登入請：

1. 啓動 NetSEAT 配置工具。

   出現**安全領域**標籤。

2. 選取您想配置整合登入的安全領域。

3. 按一下**編輯**。

   出現「安全領域內容」視窗。

4. 選取其中一個**整合登入支援**功能表選項。

   如果**整合登入支援**變成灰色，則無法在這個安全領域中啓用整合登入，這是因爲您未安裝整合登入支援。

   - 選取**停用**，停用此安全領域的整合登入支援。
   - 如果此安全領域中的使用者名稱與 Windows 使用者名稱相符，請選取**啓用 -- DCE 使用者名稱為 Windows 使用者名稱**。
   - 如果此安全領域中的使用者名稱包含 Windows 領域名稱，請選取**啓用 -- DCE 使用者名稱為 Windows 領域名稱/Windows 使用者名稱**。

5. 按一下**確定**。

   出現**安全領域**標籤。

6. 按一下**確定**。

配置整合登入通知模式

安全領域密碼可能與 Windows NT 領域密碼不相符。如果不相符，Windows 登錄項目會判斷安全領域的登入是否悄悄失敗（*無聲模式*）。或者，它會提示使用者輸入安全領域的現行密碼（*交談模式*）。在無聲模式下， Policy Director 是將使用者登入到 Windows NT 領域中，而非登入到安全領域中。在交談模式下，您可讓安全領域密碼與 Windows 密碼同步。

如要變更通知模式，請使用「登錄編輯程式」編輯這項 Windows 登錄項目：

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetSEAT\Parameters
```

變更下列之值：

```
InfoLevel:
0x00000001 (1)
```

InfoLevel 值可爲下列之一：

登錄值	模式	說明
0	無聲	在嘗試登入後，不論登入成功或失敗，皆不會向使用者報告。
1	交談	在嘗試登入後，向使用者報告失敗的登入，並提示使用者輸入動作。
2	贅述	在嘗試登入後，不論登入成功或失敗，皆向使用者報告。

配置進階登入（PKI 整合）

這項配置作業爲選用的，並且只適用於已啓用 GSS 通道機制的 NetSEAT 從屬站。

您可將 NetSEAT 配置成讓使用者的「公開金鑰基礎構造 (PKI)」登入，與使用者的 NetSEAT (Kerberos) 登入整合在一起。

依預設，是停用與 PKI 登入間的整合。如要啓用 PKI 登入，請執行 NetSEAT 配置工具。您得針對 NetSEAT 從屬站參與的每一個安全領域，個別啓用或停用 PKI 登入。

支援的 PKI 版次

NetSEAT 只支援與 Entrust 4.0 版間的使用者登入整合。

註: 在配置 NetSEAT PKI 登入前，必須先安裝 Entrust 4.0 版從屬站。

使用 NetSEAT 登入公用程式

當從 Windows **開始**功能表中呼叫 **NetSEAT 登入**公用程式時，會在登入期間出現 **PKI 登入**勾選框。此勾選框中顯示配置給現行安全領域的進階登入設定。

使用「PKI 登入」勾選框

在 NetSEAT 登入期間，使用者可使用 **PKI 登入**勾選框，置換「PKI 登入」配置（以每次的登入爲基礎）。如在配置期間選取的是**採 PKI 登入，後備為 DCE 登入**設定，則採取置換相當有用。若使用者想跳過 PKI 登入嘗試，而直接執行 DCE 登入，可選擇置換。在此情況下，使用者可取消選取 **PKI 登入**勾選框，強制進行 DCE 登入。

如果在配置期間使用者配置的是**限 PKI 登入**，即使在登入期間取消選取 **PKI 登入**，此動作亦不會生效。

如果在配置期間使用者配置的是**限 DCE 登入**，當登入期間選取 **PKI 登入**時，將會產生錯誤訊息。

使用系統匣登入

您可使用「系統匣」中的 **NetSEAT** 圖示，來執行 NetSEAT 登入。請使用下拉清單，選取您想登入的領域。如已配置 PKI 登入，則會出現 Entrust 登入提示。

如 PKI 登入失敗，而您配置的是**採 PKI 登入，後備為 DCE 登入**， Policy Director 會提示您完成 DCE 登入。

配置進階登入

如要將 PKI 登入與 NetSEAT 登入整合在一起請：

1. 啓動 NetSEAT 配置工具。
   出現**安全領域**標籤。
2. 選取您想配置 PKI 登入的安全領域。
3. 按一下**編輯**。
   出現「新安全領域」對話框。
4. 按一下**配置**。
   出現「安全領域內容」視窗。
5. 在「進階登入」區中，選取其中一個進階登入下拉清單選項。
   - 選取**限 DCE 登入**，讓使用者以使用者名稱與密碼（Kerberos 登入）來登入 Policy Director 安全領域。
   - 選取**採 PKI 登入，後備為 DCE 登入**，讓使用者嘗試 PKI 登入。如果登入失敗，NetSEAT 將提示使用者輸入使用者名稱與密碼以進行 DCE 登入。
   - 選取**限 PKI 登入**，要求使用者使用 X.509 憑證來登入。

6. 按一下**確定**。
   出現「新安全領域」對話框。
7. 按一下**確定**。
   出現**安全領域**標籤。

設定時差上限

這項配置作業爲選用的，並且只適用於 Policy Director「管理主控台」中的 NetSEAT 從屬站，以及安裝 Policy Director 的 Windows NT 伺服器。

NetSEAT 若配置成使用 GSS 通道機制，則會用到遠端時間服務程式。您可配置安全領域時間與 NetSEAT 系統時鐘間所能容許的時差上限。或者，可採用預設值 15 分鐘。

如要設定時差上限請：

1. 按一下**一般事項**標籤。
2. 視需要在**時差上限**欄位中鍵入一值。
3. 按一下**確定**或**套用**。

拒絕存取網路資源

這項配置作業爲選用的，並且適用於已啓用 GSS 或 SSL 通道機制的 NetSEAT 從屬站。

您可防止使用者從工作站發出不安全的 TELNET、RLOGIN 或 HTTP 要求。請將 NetSEAT 從屬站配置成拒絕或限制存取這些網路服務程式。拒絕或限制存取，可強迫從屬工作站在進行網路交談時，只能使用安全、加密的 Policy Director 通信通道。

依預設，此特性爲停用的。只有講究高度安全與特殊用途的網路，才應啓用此特性。

要拒絕存取未受保護的網路服務程式時請：

1. 選取**一般事項**標籤。
2. 如有需要，請選取**拒絕存取未受保護的網路服務程式**勾選框。
3. 按一下**確定**或**套用**。

配置 SSL Proxy

這項配置作業爲選用的，並且只適用於已啓用 SSL 通道機制的 NetSEAT 從屬站。

如果 NetSEAT 從屬站所發出的要求必須行經您網路的 SSL Proxy 伺服器時，可將 NetSEAT 從屬站配置成使用 Proxy 伺服器。**一般事項**標籤中的 **啓用 Proxy 伺服器**勾選框，可讓所有 NetSEAL 伺服器皆能用到 Proxy 伺服器。

如取消選取這個勾選框，則新增於 NetSEAT 配置中的 NetSEAL 伺服器沒有一個能存取 Proxy 伺服器。

如要指定 SSL Proxy 伺服器，請完成下列步驟：

1. 按一下**一般事項**標籤。

2. 必要時可變更**時差上限**欄位中的分鐘數。預設值爲 15 分鐘。
3. 請確定您未選取**拒絕存取未受保護的網路服務程式**勾選框。
4. 選取**啓用 Proxy 伺服器**勾選框。
5. 在 **Proxy 伺服器的機器名稱**欄位中鍵入名稱。
6. 在 **Proxy 伺服器之埠**欄位中鍵入埠號。
7. 按一下**確定**或**套用**。

使用 NetSEAT 安全公用程式

NetSEAT 從屬站提供了 DCE 安全服務公用程式，您可在傳統的 DCE 施行中找到。在 NetSEAT 獨一無二的結構下，足以擴充下列每一種公用程式的標準功能：**klist**、**kdestroy** 與 **dce_login**。

klist

klist 指令用以列出保留於預設證明快取中的主要使用者（*Principal*）與通行證。或者，如果您使用 **-c** 選項，此指令將會列出保留於所識別快取名稱中的使用者與通行證。

NetSEAT 可實行標準 **klist** 指令選項，另新增擴充選項。

標準選項有：

選項	說明
-c *cachename*	應顯示快取名稱所識別之快取內容，而非預設快取的內容。
-e	顯示畫面中包含過期的通行證。如不使用此選項，則只會顯示現行的通行證。
-f	顯示通行證中的選項設定。

擴充選項有：

選項	說明
-C *cellname*	說明使用者保留於 *cellname* 所識別 DCE cell 中的主要使用者與通行證。
-m	說明使用者保留於所有 DCE cell（使用者有其相關的 DCE 登入上下文）中的主要使用者與通行證。
-s	顯示一則簡短摘要，其中記錄著使用者所登入的所有 cell 以及這些 cell 的使用者登入名稱。

kdestroy

kdestroy 指令用以摧毀使用者的登入上下文與使用者的證明。在 Policy Director 重建證明前，使用者以及該使用者所建立的任何程序會受限在未經身份驗證的存取上。

NetSEAT 從屬站支援標準 **kdestroy** 選項，另新增擴充選項。

標準選項爲：

選項	說明

-c *cachename*	應摧毀的是所指快取名稱的登入上下文與相關證明，而非預設快取中的這些。

擴充選項有：

選項	說明
-C *cellname*	摧毀所指 cell *cellname* 的登入上下文與相關證明。
-m	摧毀所有 cell（使用者有其登入上下文）的使用者登入上下文與相關證明。

dce_login

dce_login 指令可驗證使用者的身份，取得使用者的網路證明，以及建立 DCE 登入上下文。

使用者必須提供 principal_name（使用者名稱）與密碼。如未將這些值當成指令行引數提供， **dce_login** 將提示使用者輸入這些。

NetSEAT 從屬站支援下列的標準 **dce_login** 選項：

選項	說明
-exec *command_string*	登入後執行 *command_string* 指定的指令。如指定 *command_string*，但未提供完整路徑名稱，則會根據 PATH 變數來搜尋目錄，藉以取得路徑字首。
-k *keytab_file_name*	指示 **dce_login** 從 keytab 檔 *keytab_file_name* 中取得使用者（Principal）名稱與密碼。
-r	在使用者通行證過期前，重新整理使用者的 DCE 登入上下文。

Policy Director 支援如下的 dce_login 擴充選項：

選項	說明
-C *cellname*	指出使用者是登入 cell *cellname*，而非登入預設 cell。

註: NetSEAT 從屬站不支援 **dce_login -c** 選項。

使用 netseat_ping 解決問題

NetSEAT 從屬站提供 **netseat_ping** 公用程式，可讓使用者取得一或多個 cell 中之 DCE 服務程式的狀態資訊。 **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

如要取得使用者維護登入上下文所在之所有 cell 中的服務程式狀態，請鍵入：

```
netseat_ping
```

例如，如果您將 NetSEAT 從屬站配置成參與 cell redback，將會出現如下輸出：

```
/.../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[ ] 可用 (v3.0)
                    ncacn_ip_udp:redback[ ] 可用 (v3.0)
```

Policy Director 支援如下的 **netseat_ping** 選項：

選項	說明
-C *cellname*	產生使用者已配置給 cell *cellname* 之所有伺服器的相關連結清單。
-t -C *cellname*	顯示 cell *cellname* 中之時間伺服器的連結。
-s -C *cellname*	顯示 cell *cellname* 中之安全伺服器的連結。
-c -C *cellname*	顯示 cell *cellname* 中之 CDS 伺服器的連結。
-d -C *cellname*	顯示 cell *cellname* 中之 DSB 伺服器的連結。

如果 cell 中有一個以上的安全伺服器、時間伺服器、Cell 目錄伺服器或 DSB，**netseat_ping** 會試著全偵測之。

第21章 NetSEAT：目錄服務分配管理系統

本章提供「目錄服務分配管理系統 (DSB)」的概觀，並說明如何針對自己的環境自訂 DSB 配置。

本章包括：

目錄服務分配管理系統的概觀

Policy Director NetSEAT 從屬站會將「RPC 名稱服務程式介面」功能轉交給「目錄服務分配管理系統 (DSB)」負責。DSB 運作方式和 Cell Directory Services (CDS) 中階伺服器一樣。

NetSEAT 從屬站直接要求到 DSB 的資源位置及服務。接下來，DSB 聯繫安全領域的 CDS，解決要求。 然後，DSB 傳回所要求的資訊給執行 NetSEAT 從屬站的系統。

在安裝 Policy Director 期間，Policy Director 會自動安裝與配置 DSB。 Policy Director 提供 DSB 是作爲「管理伺服器」（ivmgrd）資料包的一部分來分送。使用 DSB 不需要額外的步驟。

- 做爲 Policy Director 伺服器與「管理主控台」之支援模組的 NetSEAT 從屬站會用到 DSB。
- 而使用 SSL 通道機制的 NetSEAT 從屬站則不會用到 DSB。

DSB 可支援數量龐大的 NetSEAT 從屬站。如安全領域較大，您可在提供「Cell 目錄服務程式」的伺服器上執行 DSB，藉以讓效能最佳化。

爲了提供高有用性或平衡龐大網路中的工作負載，管理者可能想在安全領域中佈署一個以上的 DSB。您可自行安裝與配置附加的 DSB。

「目錄服務分配管理系統」配置選項

DSB 採常駐程式或服務程式方式執行。您可將 DSB 配置成隨系統開機而自動啓動。在大部份的情況下，DSB 不需進行任何管理。

請參閱下列各節，其中會說明管理者如何調整 DSB 配置參數：

設定 DSB 埠

DSB 會在埠上監聽要求。依預設，DSB 是隨機選擇一埠。

管理者可在下列欄位之一鍵入一值以指定埠號（選用）：

UNIX： /etc/services

Windows： *install-path*\system32\drivers\etc\services

例如，如要告訴 UNIX 系統上的 DSB 在埠 5000 上監聽，請在 /etc/services 中加入下列項目：

```
dsb                 5000/tcp                # Directory Services Broker
```

指定 DSB 日誌檔位置

DSB 會採用 DCE 有用性日誌檔來記載通知、錯誤、警告與無法恢復（嚴重）的錯誤。如果您的 DCE 安裝採用 DSB 有用性， DSB 會將輸出寫到一或多個有用性日誌檔中。DCE 有用性日誌檔可在 *DCELOCAL*/var/svc 目錄中找到。*DCELOCAL* 代表 DCE 安裝目錄。

您可使用多個檔案來反映訊息的狀態，像是：通知、錯誤或警告。您可在 *DCELOCAL*/var/svc/routing 遞送檔中加入項目，藉以指定這些檔案的位置。

例如：

```
NOTICE:FILE:DCELOCAL/var/svc/notice
```

或者，您可使用 *SVC_NOTICE* 環境變數來指定位置。環境變數的定義會蓋掉遞送檔規格。例如，您可按如下所示爲通知檔規格定義一個 UNIX 環境變數：

```
export SVC_NOTICE=FILE:DCELOCAL/var/svc/notice
```

指令行範例：

如果您在遞送檔中定義 NOTICE，並按如下從指令行啓動 DSB：

```
SVC_NOTICE=FILE:DCELOCAL/var/dsb/dsb.log dsb -q -f -U cell_admin -P *****
```

DSB 將會執行下列作業：

- 在無聲下自我配置與啓動。
- 將所有通知記載到 *DCELOCAL*/var/dsb/dsb.log 中。
- 根據遞送檔中的規格，來記載所有的錯誤、警告與無法恢復（嚴重）的錯誤。
- 不顯示任何記載的輸出。

有關遞送檔格式與 SVC_* 環境變數群組的使用，完整資訊請參閱 DCE 有用性資訊。您可在 IBM Policy Director Security Services CD 的 /doc 目錄中，找到如下有關 DCE 的安裝與配置文件：

- DCE22_QuickBeginnings_AIX.pdf
- DCE22_QuickBeginnings_NT.pdf
- DCE20_InstallGuide_Solaris.pdf
- DCE20_ReleaseNotes_Solaris.pdf

目錄服務分配管理系統指令行選項

下表說明 DSB 指令行選項：

選項	說明

-d	在前景中執行，而非採 UNIX 常駐程式或 Microsoft Windows NT 服務程式方式執行。此選項主要用來除錯。
-f	強迫重新配置 DSB 的 DCE 安全項目。 此旗號會建立 Policy Director/dsb-servers 群組（除非已建立該群組）、鍵值表格檔、intraverse/dsb/default/*fully_qualified_DNS_name* Principal （使用者），其中 *fully_qualified_DNS_name* 爲 DSB 執行所在的系統。 此選項是在 DSB 初次啓動時使用。它可呼叫多次，而不必先移除 Principal（使用者）項目、群組項目與鍵值表格檔。
-h	指令行用法訊息。
-q	傳送標準輸出到日誌檔中，而非到 stdout 或 stderr 中。螢幕中不顯示任何通知。
-r	解除配置 DSB。 此選項會移除 DSB 的 DCE 安全項目（如前面 **-f** 選項中所述）。 **-r** 旗號可單獨使用或與 **-q** 一起使用。其它的指令行旗號則不能與 **-r** 一起使用。
-t	爲 DSB 指定所能使用的伺服器緒數目。 緒數目是指同時間所能處理的從屬站要求數目。
-P *password*	指定 DCE 登入 Principal（使用者）的密碼。 只能與 **-U** 旗號一起使用。
-U *principal_name*	執行 DSB 配置時所用的 DCE 登入 Principal（使用者）。 此選項用以指定任何獲授權建立 DSB 安全項目的使用者（如前面 **-f** 選項中所述）。
-b	*限 Microsoft Windows*--指定可執行檔 DSB 二進位的檔名。 如果 DSB 安裝於非預設位置中，請使用此選項。 此選項會將 DSB 位置儲存在 Microsoft Windows NT 登錄中。當 DSB 配置成 Microsoft Windows NT 服務程式時，則 Microsoft Windows NT 會使用登錄設定。
-v	*限 Microsoft Windows*--顯示 DSB 版本與 DCE 供應商訊息。

附錄A. 使用 ivadmin 來進行 Policy Director 管理

ivadmin 公用程式是一種可用來執行 Policy Director 管理作業，且相當於「管理主控台」的指令行。

本章包括：

- 『介紹 ivadmin 公用程式』在本頁
- 『使用 ivadmin 指令』.

介紹 ivadmin 公用程式

ivadmin 公用程式是一種可代替「管理主控台」的指令行。對於想讓某些管理功能自動執行的管理者而言，可藉由使用 **ivadmin** 撰寫 Script 達到此目的。

很多 **ivadmin** 指令與「管理主控台」提供的功能重複。此外，**ivadmin** 還提供幾種無法透過「管理主控台」用到的進階管理功能。 IVBase 套裝軟體（安裝於任何執行 Policy Director 的系統中）也會連帶安裝此公用程式。

啓動 ivadmin 公用程式

如要啓動 **ivadmin** 公用程式，請使用 **dce_login** 登入安全領域。然後鍵入：

UNIX： `# ivadmin`

Windows： `ivadmin`

出現 **ivadmin** 提示：

```
ivadmin>
```

請在此提示中，鍵入適當的指令、選項與引數。請參閱『使用 ivadmin 指令』中的指令表。

例如，如想查看 **ivadmin** 說明訊息時，請鍵入：

```
ivadmin> help
```

結束 ivadmin 公用程式

如要結束公用程式並回到指令提示中，請鍵入 **ivadmin exit** 指令：

```
ivadmin> exit
```

使用 ivadmin 指令

ivadmin 指令包括：

- 第252頁的『Server（伺服器）指令』
- 第253頁的『Object（物件）指令』
- 第254頁的『Action（動作）指令』
- 第254頁的『ACL 指令』

- 第256頁的『NetSEAL 指令』
- 第258頁的『配置管理指令』
- 第258頁的『使用者管理指令』
- 第262頁的『群組管理指令』
- 第264頁的『資源管理指令』
- 第268頁的『登錄原則管理指令』

註: 所有的 **ivadmin** 指令皆必須輸入於同一行，而當成單一指令。本書中有些範例較長，因而在顯示時會折到下一行。

Server（伺服器）指令

ivadmin server 指令提供目前無法透過「管理主控台」來處理的功能：

指令	說明
server flush_logs *server-name*	
	將 WebSEAL 伺服器日誌從記憶體寫到硬碟中。啓用對伺服器事件的立即追蹤特性。
server list	
	列出所有已配置的伺服器。
server resume *server-name*	
	回復已暫停的 WebSEAL 伺服器。
server show *server-name*	
	顯示指定伺服器的內容，像是名稱、說明、主電腦名稱、NS 位置、Principal 與 root URL。
server start *server-name*	
	啓動指定的伺服器。啓動 secmgrd （NetSEAL 與 WebSEAL）與 ivacld。
server stop *server-name*	
	停止指定的伺服器。停止 secmgrd （NetSEAL 與 WebSEAL）與 ivacld。
server suspend *server-name*	
	暫停指定的 WebSEAL 伺服器。對執行伺服器的維護工作相當有助益。

下列 **ivadmin server** 指令可擴充「管理主控台」的功能：

指令	說明
server delete /ExternAuthzn/*server-name*	
	只顯示外部權限伺服器。通常此指令是由解除安裝程式在非交談方式下使用。 **註:** 此指令不應用來刪除其它任何伺服器。
server modify *server-name* **baseurl** *mount-point*	

	指定伺服器要使用的 ACL 空間分支。用以搭配複製的 WebSEAL 伺服器使用。指定所指的分支 *mount-point* 做爲「管理主控台」在管理 ACL 時所用的主要分支。此分支中的 ACL 會套用在與此裝載點（接合點）接合之所有複製的伺服器上；而複製的伺服器會立即反映所有的 ACL 變更資訊。 請注意：*mount-point* 相對於 /WebSEAL 配置區物件，且必須位於 WebSEAL 目錄中（而非任何子目錄中）。
server register externauth *server-name ns-location server-principal action-char action-name*	
	登錄外部權限伺服器的存在。此指令用以告知 Policy Director 權限服務程式有外部權限伺服器存在，因而在解析受保護物件上的授權專用權時，必須查詢此外部權限伺服器。
server status *server-name*	
	判斷伺服器正在執行或已停止，且伺服器的 ACL 資料庫副本是否已以最新的變更資訊加以更新。

技術上的注意事項：

如要顯示 chevelle 機器上之 WebSEAL 伺服器的內容，請鍵入：

```
ivadmin> server show /WebSEAL/chevelle
類型：WebSEAL 伺服器
名稱：/WebSEAL/chevelle
說明：chevelle
主電腦名稱：chevelle
NS 位置：/.:/subsys/intraverse/secmgr/server/chevelle
Principal: secmgr/chevelle Root URL: /chevelle
```

請注意：您必須完全遵照 **ivadmin server list** 指令輸出中所示的格式，來鍵入 *server-name* 引數。

例如：

```
ivadmin> server list
         /WebSEAL/chevelle
         /NetSEAL/chevelle
         /ExternAuthzn/timechecker
```

Object（物件）指令

下列 **ivadmin object** 指令所提供的功能，相當於「管理主控台」中的「物件空間」管理作業指令。

指令	說明
object list *directory-name*	
	列出分組於所指目錄下的物件，並顯示各物件的任何相關 ACL 名稱。 請注意：此指令不會展開此目錄之上的目錄樹。
object show *object-name*	
	顯示 *object-name* 資訊與任何相關的 ACL 名稱。 如沒有相關的 ACL，會出現沒有 ACL 字眼。

Action（動作）指令

下列 **ivadmin action** 指令用以將額外的 Policy Director 授權動作（許可權）定義在「管理主控台」中。

例如，透過 **ivadmin action** 指令在可用的 ACL 許可權清單加入外部授權機制。

ivadmin action 指令可提供目前無法透過「管理主控台」來處理的功能：

指令	說明
action create *name description action-type*	
	定義新 Policy Director 授權動作（許可權）。新建一個在「管理主控台」中代表此動作的新 ACL 許可權碼。 *name* 引數用以指定新的許可權碼（單一字母）。 *description* 引數提供將出現在「管理主控台」中的新勾選框標籤。 *action-type* 引數用以提供出現在「管理主控台」中的動作種類標籤。 範例： `ivadmin> action create k time Ext-Authzn`
action delete *name*	
	刪除 **action create** 指令所建之現有授權動作（許可權）。 範例： `ivadmin> action delete k`
action list	

	以下列格式列出所有現有的 ACL 動作（許可權）：
	permission name permission description action type
	
	範例：
	
	`ivadmin> action list`
	
	顯示的資訊類似如下：
	
	`r read WebSEAL`
	`...`

ACL 指令

下列 **ivadmin acl** 指令提供的功能相當於「管理主控台」中的 **ACL** 管理作業指令。

指令	說明
acl attach *obj-name acl-name*	
	讓 ACL 模版連接某物件。
acl create *acl-name*	
	在 ACL 模版資料庫中建立新 ACL 模版。請注意：此指令不會建立 ACL 項目。
acl delete *acl-name*	
	將 ACL 模版從 ACL 模版資料庫中刪除。
acl detach *obj-name*	

	讓現行 ACL 模版與所指物件脫離關聯。請注意：此指令不會將 ACL 模版從 ACL 模版資料庫中刪除。
acl find *acl-name*	
	尋找並列出連接所指 ACL 模版的所有物件。
acl list	
	列出 ACL 模版資料庫中的所有 ACL 模版。
acl modify *acl-name* **description** *desc*	
	可讓您建立或編輯所指 ACL 模版的相關說明欄位。會出現此說明的一個地方是「管理主控台」之 ACL 管理作業畫面中的「ACL 定義」區。
acl modify *acl-name* **remove user** *user-name*	
	可讓您將現有的使用者 ACL 項目從所指 ACL 模版定義中移除。
acl modify *acl-name* **remove group** *group-name*	
	可讓您將現有的群組 ACL 項目從所指 ACL 模版定義中移除。
acl modify *acl-name* **remove any-other**	
	可讓您將任何已身份驗證的 ACL 項目從所指 ACL 模版定義中移除。
acl modify *acl-name* **remove unauthenticated**	
	可讓您將任何未經身份驗證的 ACL 項目從所指 ACL 模版定義中移除。
acl modify *acl-name* **set user** *user-name perms*	
	可讓您在所指 ACL 模版定義中建立或編輯使用者 ACL 項目 (pubs)，其中許可權 (*perms*) 爲 bPTr。 範例： `ivadmin> acl modify pubs set user peter bPTr`
acl modify *acl-name* **set group** *group-name perms*	
	可讓您在所指 ACL 模版定義中建立或編輯群組 ACL 項目。 範例： `ivadmin> acl modify pubs set group sales Tr`
acl modify *acl-name* **set any-other** *perms*	
	可讓您在所指 ACL 模版定義中建立或編輯任何已身份驗證之 ACL 項目 (pubs)。 範例： `ivadmin> acl modify pubs set any-other r`
acl modify *acl-name* **set unauthenticated** *perms*	
	可讓您在所指 ACL 模版定義中建立或編輯未經身份驗證的 ACL 項目。 範例： `ivadmin> acl modify pubs set unauthenticated r`
acl show *acl-name*	
	列出構成所指 ACL 模版定義之完整的一組項目。 `ivadmin> acl show pubs`

NetSEAL 指令

您可使用 **ivadmin** 公用程式來執行下列的 NetSEAL 管理作業：

- 『管理受保護的網路』。
- 『管理 NetSEAL 接合』。
- 第257頁的『管理受保護之埠』。
- 第258頁的『管理受保護的埠別名』。

管理受保護的網路

您可將*網路*視爲一個受 NetSEAL 保護的非 Policy Director 伺服器。**ivadmin netseal** 指令可用來新增、刪除與列出受保護的網路。

指令	說明
netseal network add *network netmask* **[***network-alias***]**	
	建立一個受 NetSEAL 保護的新網路。網路與網路遮罩配對爲標準的 IP 網址號碼與網路遮罩。網路別名（選用）可用來識別此網路。如未指定別名，則必須使用網路與網路遮罩配對來識別網路。如網路已存在則會傳回錯誤。
netseal network delete *network-id*	
	將指定的網路從系統中刪除，其中 *network-id* 可對應下列之一： • *network/netmask*（*網路/網路遮罩*）配對 • *network-alias*（*網路別名*） 如在資料庫中找不到網路，將會傳回錯誤。
netseal network list	
	顯示資料庫中所有的網路，包括網路與網路遮罩配對以及任何所定義的別名。

管理 NetSEAL 接合

NetSEAL 接合會決定通信經由 Policy Director 伺服器應行經的方向。您可在兩個 Policy Director 伺服器間或 Policy Director 伺服器伺服器與網路間建立接合。請使用 GSS 通道來保護行經兩個 Policy Director 伺服器間之接合的通信。

ivadmin netseal junction 指令可用來新增、刪除與列出 NetSEAL 接合。

指令	說明
netseal junction add *hostname destination*	
	建立一個由 NetSEAL 伺服器到指定目的地的接合，其中 *hostname* 爲 NetSEAL 伺服器名稱（扣掉領域名稱），*destination* 可對應下列之一： • *pd-server*（*Policy Director 伺服器*） • *network/netmask*（*網路/網路遮罩*）配對 • *network-alias*（*網路別名*） 如接合已存在、主電腦伺服器不存在或目的地不存在，則會傳回錯誤。
netseal junction delete *hostname* **destination**	

	刪除由 NetSEAL 伺服器到指定目的地的接合，其中 *hostname* 爲 NetSEAL 伺服器名稱（扣掉領域名稱），*destination* 可對應下列之一： • *pd-server（Policy Director 伺服器）* • *network/netmask（網路/網路遮罩）*配對 • *network-alias（網路別名）* 若接合目前不存在，則會傳回錯誤。指令對目前的連線不會產生影響。
netseal junction list *hostname*	
	顯示指定 NetSEAL 伺服器的所有 NetSEAL 接合。

管理受保護之埠

Policy Director NetSEAL 伺服器可爲特定埠、主電腦與網路，提供安全服務程式。例如，您可以將 NetSEAL 伺服器配置成保護特定埠上的 TELNET 流量。

ivadmin netseal port 指令可用來新增、刪除與列出受保護之埠。您可指定埠給 Policy Director 伺服器或網路。

指令	說明
netseal port add *destination port-id*	
	保護與所指 port-id 上之指定目的地的連線，其中 *destination* 可對應下列之一： • *pd-server（Policy Director 伺服器）* • *network/netmask（網路/網路遮罩）*配對 • *network-alias（網路別名）* *port-id* 可對應下列之一： • *port（埠）* • *port-range（埠範圍）* • *port-alias（埠別名）* 如果埠已受保護、伺服器不存在或埠別名不存在，則會傳回錯誤。
netseal port delete *destination port-id*	
	停止與指定埠上之指定目的地的保護中連線，其中 *destination* 可對應下列之一： • *pd-server（Policy Director 伺服器）* • *network/netmask（網路/網路遮罩）*配對 • *network-alias（網路別名）* *port-id* 可對應下列之一： • *port（埠）* • *port-range（埠範圍）* • *port-alias（埠別名）* 如果埠尚未受到保護、伺服器不存在或埠別名不存在，則會傳回錯誤。
netseal port list *destination*	
	列出指定目的地的所有埠，其中 *destination* 可對應下列之一： • *pd-server（Policy Director 伺服器）* • *network/netmask（網路/網路遮罩）*配對 • *network-alias（網路別名）* 如伺服器不存在，則會傳回錯誤。

註: 埠範圍的表示方式應爲：指定兩個埠號，其間以連字符號隔開（例如 22-88）。

管理受保護的埠別名

ivadmin port-alias 指令可用來新增、刪除與列出埠別名。請使用*埠別名*，以較有意義的方式來識別設陷的埠範圍。

指令	說明
netseal port-alias add *port-spec port-alias*	
	爲指定的埠規格建立新的埠別名，其中 *port-spec* 可對應下列之一： • *port（埠）* • *port-range（埠範圍）* 如果該埠範圍已有其它別名，將會傳回錯誤。
netseal port-alias delete *port-id*	
	將所指 port-id 的埠別名從系統中刪除，其中 *port-id* 可對應下列之一： • *port（埠）* • *port-range（埠範圍）* • *port-alias（埠別名）* *port-id* 可以是某一埠、埠範圍、或某個埠別名。如在資料庫中找不到埠別名，將會傳回錯誤。
netseal port-alias list	
	列出在資料庫中找到的所有埠別名。

配置管理指令

ivadmin admin 配置管理指令用以顯示伺服器的相關資訊。

指令	說明
admin show configuration	

	顯示使用者登錄位於 LDAP 或 DCE 中的相關資訊。
	
	範例：
	
	`ivadmin> admin show configuration`
	
	產生的輸出類似如下：
	
	`LDAP: TRUE`
	`SECAUTHORITY: 預設值`
	`GSO: TRUE`

使用者管理指令

下列 **ivadmin user** 指令所提供的功能，相當於「管理主控台」中的**使用者**管理作業指令。此組管理指令用以控制預設 LDAP 登錄中的使用者項目。

*使用者*指的是 Policy Director 使用者。*GSO 使用者*爲 Policy Director 使用者，只是此種使用者還多了使用 Web 資源（如 Web 伺服器）的權限。

指令	說明
user create [-gsouser] ***user-name dn cn sn pwd***	

	在 LDAP 使用者登錄中建立新 Policy Director 使用者 (secUser) 帳戶（該使用者的識別名稱尚未存在於預設的 LDAP 登錄資料庫中）。 **-gsouser** 引數爲選用的。對選用指令而言，需用到連字符號 (-)。當指定 -gsouser 引數時，使用者亦會成爲 GSO 使用者 (gsouser)。 *user-name* 引數爲所要建立的使用者名稱。此名稱必須是唯一的。 *dn* 引數爲指定給所要建立之使用者的 LDAP 識別名稱（例如，`cn=Diana Lucas,ou=Austin,o=Wesley Inc,c=US`）。DN 必須是唯一的。 *cn* 引數爲指定給所要建立之使用者的共通名稱（例如，`Diana Lucas`）。 *sn* 引數爲所要建立之使用者的姓氏（例如，`Lucas`）。 *pwd* 引數爲您設給這位新使用者的密碼。密碼必須遵守 Policy Director 管理者所設的原則集（例如，`mypasswd`）。 範例： `ivadmin> user create -gsouser dlucas cn=Diana Lucas,ou=Austin,o=Wesley Inc,c=US "Diana Lucas" Lucas mypasswd` 如要讓使用者帳戶生效，您必須自行修改使用者資訊，啓用這位使用者。如要變更資訊，您必須將 account-valid 旗號設爲 “yes”。 如要新增使用者的說明，您必須使用 **ivadmin modify user** 指令變更使用者帳戶資訊。
user import [-gsouser] ***user-name dn***	
	以 Policy Director 資訊更新其識別名稱已存在於預設 LDAP 登錄資料庫中的現有使用者，讓使用者可參與安全領域。 範例： `ivadmin> user import -gsouser mlucaser cn=Mike Lucaser,ou=Austin,o=Wesley Inc,c=US`
user modify ***user-name*** **description** *description*	
	新增說明資訊，讓管理者較易識別此位使用者。 範例： `ivadmin> user modify dlucas description "Diana Lucas, Credit Dept HCUS`
user modify ***user-name*** **password** *password*	
	將使用者密碼從現行密碼改爲新密碼。將不會要求您確認密碼。 範例： `ivadmin> user modify dlucas password newpasswd`
user modify ***user-name*** **authentication-mechanism** *mech*	

	變更所用的身份驗證機制。 範例： `ivadmin> user modify dlucas authentication-mechanism dce`
user modify *user-name* account-valid {yes | no}	
	指定帳戶爲作用中或非作用中。如要啓用帳戶，請選取 “yes”;；如要停用帳戶，請選取 “no”。 範例： `ivadmin> user modify dlucas account-valid yes`
user modify *user-name* password-valid {yes | no}	
	指定密碼爲作用中或非作用中。如要啓用帳戶，請選取 “yes”;；如要停用帳戶，請選取 “no”。 範例： `ivadmin> user modify dlucas password-valid no`
user modify *user-name* gsouser {yes | no}	
	指出所指的 Policy Director 使用者是否亦爲 GSO 使用者。如要新增亦是 GSO 使用者的使用者，請選取 “yes”；如要移除同時爲 GSO 使用者的使用者，請選取 “no”。 範例： `ivadmin> user modify dlucas gsouser no`
user delete *user-name*	
	將現有的使用者帳戶從 LDAP 使用者登錄中刪除。當刪除 Policy Director 使用者帳戶時，亦會連帶刪除預設 LDAP 登錄中的 GSO 使用者帳戶資訊。 範例： `ivadmin> user delete dlucas` 在刪除使用者帳戶的同時，亦會移除該使用者帳戶的任何相關資源證明。
user show *user-name*	
	顯示指定使用者的使用者帳戶資訊。 範例： `ivadmin> user show dlucas`
user show-dn *dn*	

	在您指定識別名稱 (DN) 時提供該使用者的其它相關資訊。
	
	範例：
	
	`ivadmin> user show-dn`
	`cn=Diana Lucas,ou=Austin,o=Wesley Inc,c=US`

user show-groups *username*	

	顯示使用者所隸屬的群組。
	
	範例：
	`ivadmin> user show-groups dlucas`
	
	產生的清單類似如下：
	`sales`
	`credit`
	`engineering`

user list *pattern max-return*	

	根據您指定的比對型樣，依使用者名稱列出所有已配置的使用者帳戶。清單中會按使用者帳戶的建立順序來顯示。
	
	pattern 引數可讓您指定一種比對型樣，以據此列出您想要的。會拿使用者名稱與萬用字元相比對。比對型樣中可混合使用萬用字元與字串常數，且區分大小寫（例如，`*luca*`）。
	
	max-return 引數用以限制針對單一要求所能找出並傳回的項目數（例如，`2`）。此數目亦受 LDAP 伺服器中的配置管制。其中您可指定搜尋過程中最多能傳回多少結果。 Policy Director 會傳回 *max-return* 的最小值與 LDAP 伺服器中所配置的值。
	
	範例：
	`ivadmin> user list *luca* 2`
	
	產生的清單類似如下：
	`dlucas`
	`mlucaser`

user list-dn *pattern max-return*	

	如果只知道部份的識別名稱，則會依識別名稱列出所有已配置的使用者帳戶。清單中會按使用者名稱的建立順序來顯示。
	
	會拿使用者識別名稱中的 CN 部份（但不含 `cn=` 部份）來比對萬用字元。
	
	max-return 數亦受 LDAP 伺服器中的配置管制。其中您可指定搜尋過程中最多能傳回多少結果。Policy Director 會傳回 *max-return* 的最小值與 LDAP 伺服器中所配置的值。
	
	範例：
	`ivadmin> user list-dn *luca* 2`
	
	產生的清單類似如下：
	`Diana Lucas,ou=Austin,o=Wesley Inc,c=US`
	`Mike Lucaser,ou=Austin,o=Wesley Inc,c=US`

技術上的注意事項：

請注意：當您在 **user show-dn** 指令與 **user show-groups-dn** 指令中輸入 *dn* 引數時，請嚴守格式。當 *dn* 引數內含空格時，請使用雙引號 (″)。

例如：

```
cn=Diana Lucas,ou=Austin,o=Wesley Inc,c=US
```

user show 與 **user show-dn** 指令顯示的資訊，類似如下 Diana Lucas 使用者的相關資訊：

```
登入 ID：dlucas
LDAP dn：cn=Diana Lucas,ou=Austin,o=Wesley Inc,c=US
LDAP cn：Diana Lucas
LDAP sn：Lucas
說明：Diana Lucas, Credit Dept HCUS
為 SecUser：true
為 GSO 使用者：false
帳戶有效：true
密碼有效：true
授權機制：
預設值：LDAP
```

群組管理指令

下列 **ivadmin group** 指令相當於「管理主控台」中的**群組**管理作業指令。這組管理指令用以控制 LDAP 目錄登錄中的群組項目。

所謂*群組*是指一組具類似屬性的 Policy Director 使用者帳戶。群組可讓管理者在「存取控制清單 (ACL)」中使用群組名稱，而用不著一個個列出所有的使用者。

您可刪除或變更任何群組項目。此外，您可顯示群組或群組成員的相關資訊。做爲管理者的您也可以列出所有已配置的群組。

指令	說明
group create *groupname dn cn*	

	在 LDAP 使用者登錄中建立新 Policy Director 群組 (SecGroup)。
	
	groupname 引數爲所要建立的群組名稱。此名稱必須是唯一的。
	
	dn 引數爲指定給所要建立之存取群組的 LDAP 識別名稱（例如，cn=credit,ou=Austin,o=Wesley Inc,c=US）。
	
	cn 引數爲指定給群組的共通名稱（例如 Credit）。
	
	範例：
	
	`ivadmin> group create credit`
	`cn=credit,ou=Austin,o=Wesley Inc,c=US`
	`Credit`

group import *groupname dn*	

	匯入現有 LDAP 登錄群組的相關資訊以建立 Policy Director 群組。群組必須已存在於 LDAP 登錄中， Policy Director 群組才能匯入資訊並建立群組。所要建立的群組名稱必須是唯一的。
	
	範例：
	
	`ivadmin> group import engineering`
	`cn=engineering,ou=Austin,o=Wesley Inc,c=US`

group modify *groupname* description *description*	
	新增所指群組的相關說明，讓 Policy Director 管理者更容易識別之。 範例： `ivadmin> group modify credit description "Credit, Dept HCUS`
group modify *groupname* add *user-name*	

	新增使用者到指定的群組中。 範例： `ivadmin> group modify engineering add dlucas`
group modify *groupname* remove *user-name*	
	將現有的使用者從指定的群組中刪除。 範例： `ivadmin> group modify engineering remove dlucas`
group delete *groupname*	
	刪除現有的群組與該群組的任何相關項目。 範例： `ivadmin> group delete engineering`
group show *groupname*	
	顯示指定群組的相關明細。 範例： `ivadmin> group show credit`
group show-dn *dn*	
	爲群組名稱提供指定的識別名稱。 範例： `ivadmin> group show-dn cn=credit,ou=Austin,o=Wesley Inc,c=US`
group show-members *groupname*	

	顯示指定群組的成員，並依識別名稱列出。
	
	範例：
	
	`ivadmin> group show-members credit`
	
	顯示的資訊類似如下：
	
	`dlucas`
	`mlucaser`

group list *pattern max-return*	

	依群組名稱，列出其名稱符合指定之比對型樣的所有已配置群組。
	
	pattern 引數可讓您指定一種比對型樣，以據此列出您想要的。會拿群組名稱與萬用字元相比對。比對型樣中可混合使用萬用字元與字串常數，且區分大小寫（例如，`*Austin*`）。
	
	max-return 引數用以限制針對單一要求所能找出並傳回的項目數（例如，2）。此數目亦受 LDAP 伺服器中的配置管制。其中您可指定搜尋過程中最多能傳回多少結果。Policy Director 會傳回 *max-return* 的最小值與 LDAP 伺服器中所配置的值。
	
	顯示的資訊類似如下：
	
	`credit`
	`marketing`

group list-dn *pattern max-return*	

	如果只知道部份的識別名稱，則會根據指定的比對型樣，依識別名稱列出所有已配置的群組。
	
	會拿群組識別名稱中的 CN 部份（但不含 cn= 部份）來比對萬用字元。
	
	max-return 數亦受 LDAP 伺服器中的配置管制。其中您可指定搜尋過程中最多能傳回多少結果。 Policy Director 會傳回 *max-return* 的最小值與 LDAP 伺服器中所配置的值。
	
	範例：
	
	`ivadmin> group list-dn *t* 2`
	
	顯示的資訊類似如下：
	
	`cn=credit,ou=Austin,o=Wesley Inc,c=US`
	`cn=marketing,ou=Boston,o=Austin Sale,c=US marketing`

技術上的注意事項：

請注意：您必須完全遵照 **group show-dn** 指令輸出中所示的格式，來輸入 *dn* 引數。當 *dn* 內含空格時，請使用雙引號 (″)。

例如：

```
cn=credit,ou=Austin,o=Wesley Inc,c=US
```

group show 與 **group show-dn** 指令顯示的資訊，類似如下 credit 群組的相關資訊：

```
群組 ID：credit
LDAP dn：cn=credit,ou=Austin,o=Wesley Inc,c=US
說明：Credit, Dept HCUS
LDAP cn：credit
為 SecGroup：true
```

資源管理指令

下列的 Policy Director **ivadmin** 指令爲一組管理指令，用以控制資源的相關資訊。

資訊的相關資訊包括：

- 『管理資源』
- 第265頁的『管理資源群組』
- 第267頁的『管理資源證明』

管理資源

下列 **ivadmin rsrc** 指令可讓管理者管理各種不同的資源，像是 GSO 使用者的 Web 伺服器。

所謂*資源*是指 Web 伺服器。智慧型接合定義中的 **-T** 識別碼用以識別 Web 伺服器。

ivadmin rsrc 指令用以指出 Web 資源的名稱。

下列 **ivadmin rsrc** 指令所提供的功能，相當於「管理主控台」中的 **GSO 資源**管理作業指令。

指令	說明
rsrc create *resource-name* [-desc *description*]	
	將 Web 伺服器當成一項資源來建立與命名。 *resource-name* 引數爲提供給 Web 資源的識別名稱（例如 engwebs01）。 *description* 引數爲一可新增的說明（選用），用以讓 Policy Director 管理者更容易識別此資源。任何選用參數皆必須在前頭加上連字符號 (-)。內含空格的說明則必須以雙引號 (″) 括住。 `ivadmin> rsrc create engwebs01 -desc "Engineering Web server - Room 4807"`
rsrc delete *resource-name*	
	刪除指名的資源，包括說明資訊在內。資源必須存在，否則將顯示錯誤。 範例： `ivadmin> rsrc delete engwebs01`
rsrc list	

	顯示定義於 LDAP 目錄中的所有 Web 資源名稱，並依資源名稱列出。
	
	範例：
	
	`ivadmin> rsrc list`
	
	提供的資訊類似如下：
	
	`engwebs01`
	`engwebs02`
	`engwebs03`

rsrc show *resource-name*	

	顯示指名資源的 Web 資源資訊。
	
	資源必須存在，否則將顯示錯誤訊息。
	
	範例：
	
	`ivadmin> rsrc show engwebs01`
	
	顯示的資訊類似如下：
	
	`Web 資源名稱：engwebs01`
	`說明：Engineering Web server - Room 4807`

管理資源群組

下列 **ivadmin rsrcgroup** 指令相當於 **GSO 資源群組**管理作業指令，用以控制「GSO 資源」資訊。這些指令可讓管理者管理資源群組的各種相關屬性。

*資源群組*參照 Web 伺服器的群組，其中群組中的全部伺服器會有同一組使用者 ID (userids) 及密碼。 您可以建立資源群組中全部資源的單一資源證明。Policy Director 使用資源群組的單一資源證明，而不是資源群組中每個資源的資源證明。

下列 **ivadmin rsrcgroup** 指令所提供的功能，相當於「管理主控台」中的 **GSO 資源群組**管理作業指令。

指令	說明
rsrcgroup create *resource-group-name* [-desc *description*]	
	建立與命名 Web 資源群組。 *resource-group-name* 引數爲資源群組的名稱。 *description* 引數爲一則可新增的說明（選用），用以識別此資源群組。**-desc** 選用參數前面必須加上連字符號 (-)。內含空格的說明必須以雙引號括住。 範例： `ivadmin> rsrcgroup create webs4807 -desc "Web servers, Room 4807"`
rsrcgroup delete *resource-group-name*	
	刪除指名的資源群組，包括說明資訊在內。資源群組必須存在。 範例： `ivadmin> rsrcgroup delete webs4807`
rsrcgroup modify *resource-group-name* add rsrcname *resource-name*	
	新增 Web 資源到現有的資源群組中。資源群組必須存在。 範例： `ivadmin> rsrcgroup modify webs4807 add rsrcname engwebs02`
rsrcgroup modify *resource-group-name* remove rsrcname *resource-name*	
	將 Web 資源名稱從現有的資源群組中刪除。 範例： `ivadmin> rsrcgroup modify webs4807 remove rsrcname engwebs02`
rsrcgroup list	

	顯示定義於 LDAP 目錄中的所有 Web 資源群組的名稱。跟在 “list” 後的資訊將忽略之。
	
	範例：
	
	`ivadmin> rsrcgroup list`
	
	顯示的資訊類似如下：
	
	`webs4807`
	`websbld3`
	`websbld4`

rsrcgroup show *resource-group-name*	

	顯示指定資源群組的 Web 資源群組資訊。
	
	資源群組必須存在，否則將顯示錯誤訊息。
	
	範例：
	
	`ivadmin> rsrcgroup show webs4807`
	
	顯示的資訊類似如下：
	
	`資源群組名稱：webs4807`
	`說明：Web servers, Room 4807`
	`資源成員：`
	`engwebs01`
	`engwebs02`
	`engwebs03`

管理資源證明

下列 **ivadmin rsrccred** 指令可讓管理者管理資源證明的各種相關屬性。

*資源證明*中提供特定 GSO 使用者資源（像是一個 Web 伺服器或一群 Web 伺服器）的使用者識別與密碼。

當您使用 **ivadmin rsrccred** 指令時，在資源類型方面，您只能指定 “web” 或 “group”。

註: 資源或資源群組必須存在，您才能將資源證明套用在其上。

指令	說明
rsrccred create *resource-name* rsrcuser *resource-userid* rsrcpwd *resource-password* rsrctype {web | group} user *user-name*	

	建立與命名資源證明。使用者與資源（或資源群組）必須已存在，才能建立資源證明。如果使用者、資源或資源群組不存在或未指定，則會顯示錯誤訊息。
	
	當參照資源證明管理指令時，資源類型只能是 “web” 或 “group” 資源。
	
	resource-name 引數爲當初建立資源時提供給資源的名稱（例如 `engwebs01`）。
	
	resource-userid 引數爲使用者在 Web 伺服器上的唯一使用者識別方式（使用者 ID），例如 `4807ws01`。
	
	resource-password 引數爲使用者在 Web 伺服器中的密碼（例如 *`rsrcpwd`*）。
	
	user-name 引數爲將套用資源證明資訊的使用者名稱（例如 `dlucas`）。
	
	範例：
	
	`ivadmin> rsrccred create engwebs01 rsrcuser 4807ws01`
	`rsrcpwd` *`rsrcpwd`* `rsrctype web user dlucas`

rsrccred modify *resource-name* rsrctype {web | group} set [-rsrcuser *resource-userid*] [-rsrcpwd *resource-password*] user *user-name*	

	變更指名資源的使用者 ID 與密碼資源證明資訊。
	
	如要變更或重設使用者或密碼資訊中的資源使用者 ID，則必須在這些選用指令前面加上連字符號 (-)。資源（或資源群組）與使用者必須已存在，才能變更資源證明資訊。
	
	您指定的資源類型必須符合初次建立該資源時所指定的類型，像是 “web” 或 “group”。
	
	範例：
	
	`ivadmin> rsrccred modify engwebs01 rsrctype group`
	`set -rsrcuser 4807ws01 -rsrcpwd` ***newrsrpw***
	`user dlucas`

rsrccred delete *resource-name* rsrctype {web | group} user *user-name*	

	只刪除現有使用者的資源證明資訊。
	
	資源類型必須符合初次建立該資源時所指定的類型，像是 “web” 或 “group”。
	
	範例：
	
	`ivadmin> rsrccred delete engwebs01 rsrctype group`
	`user dlucas`

rsrccred list user *user-name*	
	顯示所指使用者之所有已定義的資源名稱與其類型。 範例： `ivadmin> rsrccred list user dlucas` 顯示的資訊類似如下： 資源名稱：engwebs01 資源類型：group 資源名稱：engwebs02 資源類型：web
rsrccred show *resource-name* rsrctype {web | group} user *user-name*	
	顯示指定使用者的資源證明資訊。 資源證明與使用者皆必須存在，否則會出現錯誤訊息。 範例： `ivadmin> rsrccred show webs4807 rsrctype group user dlucas` 顯示的資訊類似如下： 資源名稱：engwebs01 資源類型：group 資源使用者 ID：dlucas

登錄原則管理指令

ivadmin policy 指令爲一組管理指令，用以控制 Policy Director 使用者的一般原則資訊。管理者可以管理下列的原則屬性：

- 第269頁的『管理登入原則』.
- 第269頁的『管理密碼原則』

*原則*定義使用者帳戶及密碼的限制設定，以增進系統的整體安全性。這些限制可以一般強制 (對系統中每個使用者) 或指定強制 (僅對指定的使用者)。如果使用者引用特定的原則，此特定的原則優先順序高於任何定義的一般原則。優先引用的原則，不管是否爲特定的原則，多少會限制一般原則。

管理登入原則

ivadmin policy 指令可讓管理者管理登入的相關原則。

請使用與登入有關的 **policy** 管理作業指令，來建立新登入原則或複製現有的登入原則。此外，您可顯示使用者帳戶的登入原則資訊。

對於與登入相關的原則，當參照**原則**管理作業指令時，Policy Director 定義相對時間爲 DDD-hh:mm:ss，並定義絕對時間爲 YYYY-MM-DD-hh:mm:ss。

指令	說明
policy {set | get} max-account-age [*relative-time*] [-user *user-name*]	

	管理用以控制時段的原則，像是最長過了幾天與幾小時後，使用者的帳戶便宣告過期。
	例如：
	`ivadmin> policy set max-account-age 031-12:30:00 dlucas`
	或：
	`ivadmin> policy get max-account-age dlucas`

policy {set | get} account-expiry-date [*absolute-time*] [-user *user-name*]	

	指定個別使用者帳戶即將過期的絕對日期與時間。也可用來指出所有使用者帳戶會在何時同時過期。
	例如：
	`ivadmin> policy set account-expiry-date 1999-12-30-23:30:00 dlucas`
	或：
	`ivadmin> policy get account-expiry-date dlucas`

管理密碼原則

下列 **ivadmin policy** 指令可讓管理者管理密碼的各種相關原則屬性。

對於與密碼相關的原則，當參照**原則**管理作業指令時，Policy Director 定義相對時間爲 DDD-hh:mm:ss。

指令	說明
policy {set | get} min-password-length [*number*]	

	指定密碼的最小長度 (以字元計)。*number* 引數爲密碼允許的最小長度。
	
	例如：
	
	`ivadmin> policy set min-password-length 8`
	
	或：
	
	`ivadmin> policy get min-password-length`

附錄B. 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 (DBCS0）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。

本資訊只供規劃之用。在交付所說明的產品之前，此處所提供之資訊有可能改變。

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。

著作權授權：

本資訊含有原始語言的應用程式樣本，用以說明各種作業平台上的程式設計技術。 您可以基於開發、使用、行銷和發行應用程式（這些應用程式符合應用程式設計介面且適用於程式樣本所針對的作業平台）之目的，以任何形式來複製、修改和發行這些程式樣本，不必向 IBM 付費。

這些範例未經過所有狀況下的完整測試。 因此，IBM 對這些程式的可靠性、實用性或功能，不提供任何保證或暗示。您可以基於開發、使用、行銷和發行應用程式（符合 IBM 應用程式設計介面者）之目的，以任何形式來複製、修改和發行這些程式樣本，不必向 IBM 付費。

這些範例程式的每一個副本或任何部分，或是任何衍生的作品，都必須包括以下的版權聲明：

©（您的公司名稱）（年份）。這個部分的程式碼是衍生自 IBM Corp. 範例程式。 © Copyright IBM Corp. *enter the year or years.* All rights reserved.

如果您檢視本資訊的軟體版本，可能不會看到照片和彩色圖例。

商標

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

AIX
DCE
IBM
FirstSecure
Global Sign-On
GSO

LDAP
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.
IntraVerse	DASCOM, Inc.
Internet Information Server (IIS)	Microsoft Corporation
Internet Explorer	Microsoft Corporation
Netscape 與 Netscape 標誌圖	Netscape Communications Corporation
Netscape 標誌圖	Netscape Communications Corporation
Netscape FastTrack	Netscape Communications Corporation
Netscape Navigator	Netscape Communications Corporation
NetSEAL	DASCOM, Inc.
NetSEAT	DASCOM, Inc.
智慧型接合	DASCOM, Inc.
Solaris	Sun Microsystems, Inc
WebSEAL	DASCOM, Inc.

Java 和所有以 Java 爲基礎的商標，是 Sun Microsystems, Inc. 在美國和其他國家的商標。

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。

〔一劃〕

〔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〕

〔二十劃〕

〔二十二劃〕

〔二十三劃〕

〔數字〕

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

X

〔特殊字元〕

名詞解釋

這份名詞解釋定義了本書中的術語及縮寫，它們可能是全新的，或是您不熟悉以及可能會感興趣的術語。它包括來自下列書籍的術語及定義：

- IBM Dictionary of Computing，New York：McGraw-Hill，1994。
- The American National Standard Dictionary for Information Systems，ANSI X3.172-1990，American National Standards Institute (ANSI)，1990。
- The Answers to Frequently Asked Questions, Version 3.0, California: RSA Data Security, Inc., 1998.

一劃

一般實體. 非 CA 之憑證的主旨。

三劃

三重 DES. 一種對稱的演算法，用來將純文字加密三次。雖然有很多方法可以這樣做，但最安全多次加密形式就是具有三個不同金鑰的三重 DES。

四劃

內部結構. *請參閱*綱目。

公開金鑰. 其它人可以使用的公開/私密金鑰對。 它可讓它們將交易導向到金鑰的擁有者，或驗證數位簽章。 以公開金鑰加密的資料只能使用對應的私密金鑰解密。 *請對照*私密金鑰。 *亦請參閱*公開/私密金鑰對

公開金鑰基本設施 (PKI). 安全軟體的一個標準，它是根據公開金鑰加密法。 PKI 是數位式憑證、憑證管理中心、註冊管理中心（RA）、憑證管理服務及分散式目錄服務的一個系統。它是用來驗證網際網路上參與任何交易之每一方的身份與權限。這些交易可能涉及會要求身份驗證的作業。例如，它們可能會確認原始的企劃書招標、電子郵件訊息的作者或金融交易。

PKI 是藉由建立可供有效個人或組織鑑定的使用者公開加密金鑰及憑證，來達到此目的。它提供含有公開加密金鑰及憑證的線上目錄，用來驗證數位式憑證、證明及數位簽章。

PKI 提供了一種方法，來迅速及有效率地回應公開加密金鑰的驗證查詢及要求。它也會識別系統的潛伏安全威脅，而且會維護資源來處理安全性的侵泛。最後，PKI 會提供數位時間戳記服務給重要的商務交易。

公開金鑰密碼化標準 (PKCS). 非正式供應商之間的標準，在 1991 年由代表許多電腦供應商的 RSA 實驗室所開發出來的。這些標準涵蓋 RSA 加密、Diffie-Hellman 法合約、密碼型加密、擴充憑證語法、加密訊息語法、私密金鑰資訊語法及憑證語法。

- PKCS #10 是指定憑證要求的標準語法。
- PKCS #12 是指定一個可攜性格式，用來儲存或傳送使用者的私密金鑰、憑證及雜項秘密等。

公開/私密金鑰對. 公開/私密配對金鑰是金鑰配對加密法概念（由 Diffie 及 Hellman 在 1976 年所提，用來解決金鑰管理問題）的一部份。在它們的概念中，每一個人會取得一對金鑰，其中一個稱爲公開金鑰，而另一個稱爲私密金鑰。當私密金鑰保密時，則每一個人的公開金鑰都是公開的。傳送者及接收者不需要共用機密資訊：所有通信只牽涉到公開金鑰，而私密金鑰永遠不會傳輸或共用。相較於竊聽或洩密，它不再需要相信某些通信頻道是安全的。唯一的基本要求就是公開金鑰必須以可靠的（經過身份驗證）方法（例如，放在可靠的目錄中），建立和其使用者間的關聯性。任何一個人都可使用公用資訊，來傳送機密的訊息。然而，訊息只能使用只有接受者擁有的私密金鑰解密。因此，金鑰配對加密法不僅可用在資料隱私（加密）上，也可用在身份驗證（數位簽章）上。

文件加密金鑰 (document encrypting key). 一般而言，係指對稱的加密/解密金鑰，像是 DES。

五劃

主從架構（client/server）. 分散式處理中的模型，其中在某一個站台的程式會傳送要求給另一個站台上的程式，並且等待回應。發出要求的程式稱爲從屬站；而回答的一方稱爲伺服器。

加密. 將資訊亂數化，只讓具有適當解密字碼的人可以透過解密來取得原始資訊。

加密. 有關隱藏資料意義的資料轉換。

加密法. 在電腦安全中，係指用來加密純文字及解密加密文字的原則、手段及方法。

加密/解密. 使用接受者的公開金鑰，將接受者的資料鎖碼，然後接受者再使用成對的私密金鑰來將資料解碼。

加強私密性的郵件 (PEM). Internet 加強私密性的郵件標準，係由「Internet 配置委員會」（IAB）採用，以透過 Internet 提供安全的電子郵件。 PEM 通信協定提供了加密、身份驗證、訊息資料完整性，以及金鎖管理。

六劃

交互憑證. 藉由信任模式，一個 CA 發出包含一個與其私密簽章金鑰相關之公開金鑰的憑證給另一個 CA。交叉證明的憑證可讓一個管理領域中的從屬站系統或一般實體安全地與另一個領域中的從屬站系統或一般實體通信。

全球資訊網（World Wide Web，WWW）. Internet 的一部分，其網路連接是建立在包含超媒體資料的電腦之間。這些資料提供許多資訊，而且能提供對全球資訊網及 Internet 中其它資料的鏈結。全球資訊網資源是經由 Web 瀏覽器程式來存取。

共同密碼配置 (CCA). 可讓主要 IBM 運算平台上的加密一致的 IBM 軟體。它支援以各種程式設計語言來撰寫的應用軟體。 應用軟體可在 CCA 服務上呼叫，來執行廣範圍的加密功能，包括 DES 及 RSA 加密。

多目標 Internet 郵件擴充（Multipurpose Internet Mail Extensions, MIME）. 一組可自由使用的規格，可互相交換以不同字元集的語言書寫的文字。允許在使用 Internet 郵件標準的許多不同電腦系統中交換多媒體電子郵件。例如，電子郵件訊息可包含非 US-ASCII 的字集、豐富文字、影像以及聲音。

存取控制清單（access control list，ACL）. 一種用來限制授權使用者使用特定資源的機制。

安全 Socket 層次（Secure Sockets Layer、SSL）. 一種 IETF 標準通信的通信協定，具有內建的安全性服務，並且儘可能對一般使用者透明化。它提供數位化的安全通信通道。

啓用 SSL 的伺服器通常會接受與標準 HTTP 要求之要求不同埠的 SSL 連線要求。 SSL 會在交換信號來設定兩個數據機 (一次只需一個) 之間的通信期間建立一個階段作業。之後，就會加密通信。訊息完整性檢查會一直繼續到 SSL 階段作業過期爲止。

安全領域（security domain）. 其憑證已經由同一 CA 證明的一個群組（公司、工作小組或團隊、教育或政府單位）。其憑證已經過 CA 簽章的使用者，可以信任他位具有同一 CA 所簽章之憑證的使用者身份。

七劃

伺服器憑證（server certificate）. 由 CA 所發出的數位式憑證，可讓 Web 伺服器處理各種以 SSL 爲基礎的交易。當瀏覽器使用 SSL 通信協定連接伺服器時，伺服器會將它的公開金鑰傳送給瀏覽器。這會鑑定伺服器的身份。它也會讓加密的資訊送到伺服器。*亦請參閱* CA 憑證、數位式憑證及瀏覽器憑證。

伺服器（server）. （1）在網路中提供功能給其他工作站的資料工作站；例如，檔案伺服器。（2）在 TCP/IP 中，指網路中負責處理另一個站台之系統要求的系統，稱爲主從架構。

完整性. 系統會保護資料的完整性，以免未授權修改 (另一方面也會保護資料的保密性，以免未授權洩授)。

完整性檢查. 檢查與外部元件交易所產生的審核記錄。

私密金鑰. 只有擁有者可以使用的公開/私密金鑰對。它可讓擁有者接收私密的交易，或進行數位簽章。以私密金鑰簽名的資料只可使用對應的公開金鑰驗證。 *請對照*公開金鑰。 *亦請參閱*公開/私密金鑰對。

身份驗證（authentication）. 用以決定通信方之身份的可靠程序。

防火牆. 網路之間的閘道，用來限制網路之間的資訊流量。基本上，防火牆的目的是爲了保護內部網路，以免外界未授權使用。

八劃

事先登錄. 在 IBM SecureWay Trust Authority 中，一種可讓使用者（通常是管理者）登記其它使用者的程序。如要求獲准，「註冊管理中心（RA）」會提供可讓使用者在稍後使用 Trust Authority 從屬站應用程式來取得憑證的資訊。

使用者身份驗證（user authentication）. 此程序用以驗證訊息發出者確實符合其身份，且是訊息的合法擁有者。也可以驗證您要與之通信的一般使用者或系統。

拒絕. 以不正確的方式拒絕；例如，拒絕您傳送特定訊息，或提出特定的要求。

物件類型（object type）. 一種可儲存在 IBM SecureWay Directory 中的物件種類。例如，組織、會議室、裝置、人員、程式或處理。

物件（object）. 在物件導向的設計或程式設計中，摘要封裝的資料以及和該資料連結的作業。*亦請參閱*類別。

金鑰. 一種表量的數字或符號，在加密法中用來將資訊鎖碼及解碼。

金鑰對. 對應的金鑰，用於非對稱加密法。其中一個金鑰是用來加密，而另一個金鑰是用來解密。

九劃

信任領域（trust domain）. 其憑證已經由同一個 CA 所證明的一組實體。

信任模式（trust model）. 管制憑證管理中心如何證實其它憑證管理中心的結構慣例。

保密性. 不洩漏給未授權團體的性質。

美國國家標準局（American National Standards Institute，ANSI）. 在美國的一個組織，它負責建立許多程序，其認可的組織可藉由這些程序來建立及維護自發性的工業標準。它是由生產者、消費者，以及一般利益團體所組成。

美國國家標準資訊交換碼（American National Standard Code for Information Interchange, ASCII）. 在資料處理系統、資料通信系統，以及相關設備之間進行資訊交換的標準碼。 ASCII 集是使用編碼字集，它是由 7 位元的編碼字元（8 位元時包括同位檢查）所組成。該字集是由控制字元及圖形字元所組成。

要求 ID. 24 到 32 字元 ASCII 值，唯一用來識別對 CA 的憑證申請。這個值可以用在憑證申請交易上，來擷取與它相關的申請或憑證的狀態。

十劃

案例. 在 DB2 中，案例是一個邏輯資料庫管理環境，用來儲存資料及執行應用程式。它允許爲多個資料庫定義一組共通的配置參數。

站台憑證（site certificate）. 類似 CA 憑證，但只適用特定的網站。*亦請參閱* CA 憑證。

純文字. 未加密的資料。cleartext 的*同義字*。

十一劃

動作歷程（action history）. 累計在證明生命週期中的事件。

國家安全部 (NSA). 美國政府的官方安全主體。

國家語言支援（National Language Support，NLS）. 產品對不同語言環境的支援，包括語言、幣別、日期與時間格式以及數字表示法。

常駐程式（daemon）. 在背景執行作業的程式。當需要其協助的狀況發生時，就會暗中被呼叫。使用者不需要注意常駐程式的存在，因爲系統通常會自動啓動它。常駐程式可能一直存在，或系統可能會常常重新產生它。

這個術語（發音爲 *demon*）是取自於神話後來被合理化成爲 DAEMON 的頭字語，即「磁碟與執行監視程式」（Disk And Execution MONitor）。

從屬站（client）. （1）一種功能性單元，它會從伺服器接收共用的服務。（2）對另一部電腦或程式要求服務的電腦或程式。

授權（authorization）. 存取資源的許可。

統一資源定位器（Uniform Resource Locator，URL）. 在 Internet 上定址資源的體制。URL 是指定通信協定、主電腦名稱或 IP 位址。它也包括從特定機器存取資源時所需的埠號、路徑及資源明細。

統一資源指示符 (Uniform Resource Indicator, URI). 絕對 URL 是指相對於 HOST 名稱或 IP 位址的 URI 位置，以及網路埠。

通用閘道介面 (CGI). 在網頁與 Web 伺服器之間傳輸資訊的標準方法。

通信協定（protocol）. 電腦之間協議的通信慣例。

通道（tunnel）. 在 VPN 技術中，係指透過網際網路來進行的一種隨選虛擬點對點連線。連接時，遠端使用者可以使用通道來與企業專用網路交換安全、加密以及封裝的資訊。

頂端 CA. 位於 PKI CA 階層頂端的 CA。

十二劃

單位碼. 由 ISO 10646 定義的一種 16 位元字集。單位碼字元編碼標準是資訊處理的一種國際字元碼。單位碼標準包含世界的 Principal Script，並提供軟體國際化及本土化的基礎。 Java 程式設計環境中的所有原始程式都是以單位碼撰寫的。

無法否認. 使用數位私密金鑰來避免文件的簽名者錯誤地拒絕簽名它。

登錄資料庫. 包含有關憑證申請及發出憑證的資訊。資料庫會儲存登記資料，以及在它整個生命週期內對該憑證資料所做的所有變更。

登錄領域. 與特定憑證登錄程序有關的一組資源、原則和配置選項。領域名稱是一個用來執行登錄應用程式的 URL 子集。

發出的憑證清冊 (ICL). 已發出的憑證及其現行狀態的一個完整清單。 憑證是依序號及狀態編製索引的。 這個清單是由 CA 維護，且儲存在 CA 資料庫中。

程式碼簽名. 以數位簽章簽名可執行檔的一種技術。程式碼簽名的設計是爲了改善透過網際網路分送的軟體穩定性。

虛擬專用網路（Virtual Private Network，VPN）. 一種採用網際網路而非電話線來建立遠端連線的專用資料網

路。由於使用者是透過「Internet 服務提供者」（ISP）來存取企業網路資源，而不是透過電話公司，因此組織可以大幅地減少遠端存取的成本。 VPN 也能加強資料交換的安全性。 在傳統的防火牆技術中，訊息內容可以加密，但是來源及目的地位址則不能。 在 VPN 技術中，使用者可以建立通道連線，其中的整個資訊封包（內容及標頭）都是加密與封裝的。

註冊管理中心 (registration authority, RA). IBM SecureWay Trust Authority 軟體，用以管理數位式憑證，以確定從一開始接收登記要求到廢止憑證，都會套用組織的商務原則。

超本文傳輸通信協定（Hypertext Transaction Protocol，HTTP）. 用來跨越 Web 轉送超本文檔案的網際網路主從架構通信協定。

超本文標記語言（Hypertext Markup Language，HTML）. 用來撰寫 Web 網頁程式碼的標記語言。它是以 SGML 爲基礎。

超本文（hypertext）. 包含字詞、詞組或圖形的文字，並且能夠讓讀者用滑鼠按一下文字來取出或顯示另一份文件。這些字詞、詞組或圖形稱爲超鏈結。取出它們即爲我們平常所說的鏈結。

十三劃

傳輸控制通信協定/Internet 通信協定（Transmission Control Protocol/Internet Protocol，TCP/IP）. 一組支援區域及廣域網路之對等式連結性功能的通信協定。

解密. 還原加密處理。

資料儲存庫 (data storage library). 一個模組，提供憑證、CRL、金鑰、原則及其它安全相關物件之永存資料庫的存取權。

資料隱私. 避免洩漏未獲授權的資料。

閘道. 一種功能單位，可讓不相容的網路或應用程式彼此通信。

電子商務（e-commerce）. 商業與商業之間的交易。包括購買及銷售物品與服務，（對象爲網際網路上的買主、供應商、廠商及其他）。它是電子商業的主要元素。

電子商業（e-business）. 在網路上經由電腦所進行的商務交易。包括購買和銷售貨品與服務，也包括經由數位通信的轉帳。

十四劃

綱目. 與 IBM SecureWay Directory 有關，一種定義出各種物件類型間之關係的內部結構。

輕裝備目錄存取通信協定（Lightweight Directory Access Protocol，LDAP）. 它是一種用來存取 Directory 的通訊協定。

領域（domain）. *請參閱*安全性領域及登錄領域。

十五劃

審核日誌 (audit log). 資料庫中用以儲存審核事件記錄（一個審核事件一筆記錄）的表格。

審核伺服器 (audit server). 此種伺服器負責接收來自審核從屬站的審核事件，並將之寫入審核日誌中。

審核追蹤（audit trail）. 一種資料，它是以鏈結事件順序的邏輯路徑形式存在。一種可用來追蹤交易或給定活動行程的審核追蹤。

數位式憑證 (digital certificate). 具公信力的第三者發放給個人或實體的電子證明。每一個憑證都是以 CA 的私密金鑰簽名的。它是用來保證個人、企業或組織的身份。

端視 CA 的角色而定，憑證可以證明持有者的權限，以便在網際網路上執行電子商業。就某方面來說，數位式憑證所扮演的角色類似於駕駛執照或醫療執照。它可以證明對應的私密金鑰的擁有者已獲得授權，來處理電子商業活動或組織內的其他功能。

憑證包含它所證明之實體（不論是個人、機器或電腦程式）的相關資訊。這份資訊中也包含了該實體之已證明的公開金鑰。

數位式憑證程序（digital certification）. *請參閱*憑證。

數位簽章. 新增到文件或資料的一則編碼訊息，用來保證傳送者的身份。

數位簽章可以提供比實體簽章大的安全層次。理由爲數位簽章不是加密名稱，或一系列的簡式識別程式碼。反之，它是簽名之訊息的加密摘要。 因此，在訊息上數位簽章可提供傳送者的可靠識別。（只有傳送者的金鑰才能建立簽章）。其中亦混合著簽章訊息的內容（加密過的訊息摘要必須符合訊息內容，否則簽章無效）。因此，數位簽章無法從一個訊息複製，並引用到另一個訊息，因爲摘要或雜湊不相符。簽名訊息的任何變更也會使簽章失效。

數位簽章演算法 (digital signature algorithm). 作爲部份「數位簽章標準」的一種公開金鑰演算法。它無法用於加密，只用於數位簽章。

數據加密標準（DES）. 一種加密區塊密碼，美國政府在 1977 年定義及簽署爲正式標準。 IBM 是最先發展的。從 DES 的出版品中，DES 已被廣泛地研究，而且是知名且廣泛使用的加密系統。

DES 是一種對稱的加密系統。當它用來通信時，傳送者及接收者兩者都必須知道同一個機密金鑰。 這個金鑰是用來

加密及解密訊息。DES 也可用於單一使用者加密，像是將檔案以加密格式儲存在硬碟中。 DES 具有 64 位元區塊大小，而且會使用 56 位元金鑰來加密。 它一開始的設計是爲了在硬體中施行。 NIST 每 5 年會以美國政府加密標準來重新證明 DES。

標準一般標示語言 (SGML). 用來說明標示語言的一種標準。HTML 是根據 SGML。

十六劃

憑證原則. 一組具名的規則，代表對具有共通安全需求之特定應用程式類別的憑證的適用性。例如，憑證原則可能會指示特定的憑證類型可讓使用者在一定的售價範圍內處理貨品的交易。

憑證設定檔. 用來定義所要之憑證類型（像是 SSL 憑證或 IPSec 憑證）的一組性質。設定檔可協助您管理憑證規格及登錄。發行者可變更設定檔名稱，並指定所要憑證的性質，像是有效期、金鑰用法及識別名稱 (DN) 限制等等。

憑證程序. 在此程序中，具公信力的第三者會發出電子證明來保證個人、企業或組織的身份。

憑證管理中心 (CA）. 負責遵循組織的安全性原則，並以憑證的格式指定安全電子身份的軟體。 CA 可處理「註冊管理中心（RA）」所提的要求，以發出、重訂與廢除憑證。CA 會與 IBM SecureWay Trust Authority 產品的 RA 互動，以便在 Directory 中發佈憑證與 CRL。*另請參閱*數位式憑證 (digital certificate)。

憑證廢止清冊（certificate revocation list, CRL）. 以數位方式簽名、加上時間戳記，並且已被憑證管理中心廢止的憑證清單。此清單中的憑證應視爲無法接受。*另請參閱*數位式憑證 (digital certificate)。

憑證擴充欄位. X.509v3 憑證格式的一種選用特性，用來將其它的欄位併入憑證中。共有標準的擴充欄位及使用者定義的擴充欄位。標準擴充欄位的存在有各種目的，包括金鑰及原則資訊、主旨及發出者屬性，以及憑證路徑限制。

十七劃

應用程式介面 (application program interface, API). 爲 Policy Director 中的一種運作介面，可讓以高階語言寫成的應用程式使用特定的 Policy Director 功能。以標準爲基礎的「Policy Director 權限 API」可讓應用程式呼叫集中式的 Policy Director 權限服務程式。使用這些呼叫，讓開發者不必爲每一個新的應用程式撰寫授權程式碼。 「Policy Director 權限 API」能讓企業將可靠的授權組織配置上的所有的應用程式標準化。使用「Policy Director 權限 API」，企業對於存取網路上的資源便能提供更多控制。 請參閱 *Policy Director 程式設計及參考手冊*以取得 Policy Director 權限 API 的完整資訊及說明。

檔案轉送通信協定 (FTP). 一種網際網路主從架構通信協定，用以在電腦間轉送檔案。

十八劃

瀏覽器憑證（browser certificate）. 一種數位式憑證，也稱之爲從屬端憑證。它是由 CA 透過 SSL 啓用的 Web 伺服器所發出的。加密檔中可讓憑證持有人將資料加密、解密及簽名的金鑰。基本上， Web 瀏覽器會儲存這些金鑰。部份應用程式可將金鑰儲存在智慧型卡片或其它媒體上。*另請參閱*數位式憑證 (digital certificate)。

瀏覽器（browser）. *請參照*「Web 瀏覽器（Web browser）」。

簡易郵件轉送通信協定（Simple Mail Transfer Protocol，SMTP）. 透過 Internet 轉送電子郵件的通信協定。

十九劃

簽名. 使用私密金鑰來產生簽章。簽章是確定您負責並核准您簽名之訊息的一種方法。

簽章與驗證 (signing and verifying). 簽章就是使用私密金鑰來產生簽章。驗證就是使用對應的公開金鑰來驗證簽章。

識別名稱（distinguished name，DN）. 它是一個儲存在 Directory 中資料項目的唯一名稱。DN 可用來唯一識別項目在 Directory 階層結構中的位置。

識別編碼規則 (DER). DER 只會從編碼規則允許的那些中選取其中一個編碼類型，來評估所有傳送者選項。

證明獲取服務程式 (Credentials Acquisition Service, CAS). 「Policy Director 證明獲取服務程式 (CAS)」元件。

證明（credential）. 在身份驗證交換中，用來證明某人身份的機密資訊。在網路運算環境中，最普遍的證明類型是一種經由 CA 建立且簽章的憑證。

鏈結驗證. 驗證信任階層發出已知憑證的所有 CA 簽章。例如，如果某個 CA 藉由另一個 CA 發出簽名憑證，則這兩個簽章在由使用者提出的憑證驗證期間都是有效的。

類別. 在物件導向的設計或程式設計中，係指一群共用共通定義並進一步共用共通性質、作業及行爲的物件。

類型. *請參照*「物件類型（object type）」

A

ACL. 全文爲 ″Access control list″，意指「存取控制清單」。

ANSI. 全文爲 ″American National Standards Institute″，意指「美國國家標準局」。

API. 應用程式介面 (Application program interface)。

Applet. 一種以 Java 撰寫，並且在 Java 相容的瀏覽器內執行的電腦程式。 亦稱爲 Java Applet。

ASCII. 全文爲 ″American National Standard Code for Information Interchange″，意指「美國國家標準交換碼 」。

B

base64 encoding. 一種以 MIME 轉換二進位資料一般方法。

C

CA. 憑證管理中心 (Certificate authority)。

CA 憑證. Web 瀏覽器在您申請時，從它無法辨識的 CA 接受的一個憑證。瀏覽器可使用此憑證來鑑定與伺服器（持有該 CA 所發出的憑證）間的通信。

CAS. 證明獲取服務程式 (Credentials Acquisition Service)。

CAS 伺服器 (CAS server). 「Policy Director 證明獲取服務程式 (CAS)」元件的伺服器。

CGI. 通用閘道介面，原文爲 Common Gateway Interface。

cleartext. 未經加密的資料。純文字的*同義字*。

CRL. 全文爲 ″Certificate revocation list″，意指「憑證廢止清冊」。

CRL 出版品間隔. 設定在 CA 配置檔中，係指定期將 CRL 發行給 Directory 之間的時間間隔。

D

DER. 識別的編碼規則。

DES. 數據加密標準。

Directory. 它是一種階層式結構，意指一種與通信（如：電子郵件或密碼化交換）相關資訊的廣域儲存庫。Directory 會儲存 PKI 結構不可或缺的特定項目，包括公開金鑰、憑證及憑證廢止清冊（CRL）。

Directory 中的資料是以樹狀的階層來加以組織，樹狀結構的頂端是根。通常，較高層次的組織代表個別的國家、政府或公司。一般而言，使用者以及裝置是以每一棵樹枝的樹葉來代表。這些使用者、組織、地區、國家，以及裝置在「目錄資訊樹」（DIT）中各有它們自己的項目。每一個項目是由鍵入的屬性所組成的。這些提供項目代表之物件的相關資訊。

Directory 中的每一個使用者項目都會連結到一個相關的識別名稱（DN）。當項目包括對實際物件而言是唯一的屬性時，則這是唯一的名稱。 請考慮下列範例 DN。 其中，國家 (C) 是 US (美國)、組織 (O) 是 IBM、組織單位 (OU) 是 Trust，而一般名稱 (CN) 爲 CA1。

```
C=US/O=vnet/OU=Trust/CN=CA1
```

DN. 全文爲 ″Distinguished name″，意指「識別名稱」。

E

extranet. 它是網際網路的衍生網路，使用類似的技術。公司正開始應用 Web 發佈、電子商務、訊息傳輸，以及對客戶、伙伴及內部員工等多樣社區的群體。

F

FTP. 檔案轉送通信協定。

H

HTML. 全文爲 ″Hypertext Markup Language″，意指「超本文標記語言」。

HTTP. 全文爲 ″Hypertext Transaction Protocol″，意指「超本文傳輸通訊協定」。

HTTP 伺服器 (HTTP server). 一種伺服器，用來處理瀏覽器與網路中其他程式間的 Web 型通信。

I

ICL. 發出的憑證清冊。

Internet. 世界性的網路集成，提供電腦之間的電子連線。這可讓它們經由軟體裝置彼此通信，例如電子郵件或 Web 瀏覽器。例如，某些網路上的大學院校會與其他類似的網路鏈結，來形成 Internet。

intranet. 企業內部的網路，通常位於防火牆內。它是 Internet 的衍生網路，使用類似的技術。就技術上而言，intranet 只是 Internet 的延伸而已。HTML 及 HTTP 是部份的法人團體。

IPSec. IETF 所發展的一種「Internet 通信協定安全性」(Internet Protocol Security）標準。 IPSec 是一種網路層通信協定，用以提供加密的安全服務，以便能彈性地支援身份驗證、資料完整、存取控制以及保密性的組合。由於它強大的身份驗證特性，已有眾多 VPN 產品供應商採用，用來做爲在網際網路上建立安全點對點連線時的通信協定。

J

Java. 由 Sun Microsystems 公司所發展的一組可感應網路，未針對特定平台的電腦技術。Java 環境是由 Java OS、不同平台的「虛擬機器」、物件導向的 Java 程式設計語言，以及數個類別程式庫所組成。

Java Applet. *請參照* Applet。*請與*「Java 應用程式（Java application）」對照。

Java 虛擬機器 (JVM). 負責解譯 bytecode 的部份 Java 執行環境。

Java 應用程式（Java application）. 以 Jave 語言寫成的一種獨立式程式。它可以在 Web 瀏覽器的環境之外執行。

Jave 語言（Java language）. 由 Sun Microsystems 所開發的程式語言，它是專門爲了在 applet 以及代理程式應用程式中使用而設計。

L

LDAP. 全文爲 ″Lightweight Directory Access Protocol″，意指「輕裝備目錄存取通訊協定」。

N

NLS. 全文爲 ″National language support″，意指「國家語言支援」。

P

PEM. 加強私密性的郵件，全文爲 Privacy-enhanced mail。

PKCS. 公開金鑰密碼化標準，全文爲 Public Key Cryptography Standards。

PKCS#10. *請參閱*公開金鑰密碼化標準。

PKCS#12. *請參閱*公開金鑰密碼化標準 (Public Key Cryptography Standards)。

PKI. 公開金鑰基本設施，全文爲 Public key infrastructure。

PKIX. X.509v3 型 PKI。

PKIX 憑證管理通信協定 (CMP). 可和 PKIX 相容之應用程式連線的通信協定。 PKIX CMP 會以 TCP/IP 作爲它的主要傳送機制，但 socket 上會有一個摘要層。這可啓用其它輪詢傳送的支援。

Proxy 伺服器. 要求存取的電腦（電腦 A）與被存取的電腦 (電腦 B) 之間的中繼站。因此，如果一般使用者向電腦 A 要求資源，則這個要求會導向到 Proxy 伺服器。 Proxy 伺服器會提出該要求，並從電腦 B 取得回應後，再將回應轉遞給一般使用者。 Proxy 伺服器有助於從防火牆內存取全球資訊網。

R

RA. 全文爲 ″Registration authority″，意指「註冊管理中心（RA）」。

RC2. 一種可變的金鑰大小區塊密碼，由 Ron Rivest 針對「RSA 資料安全」而設計出。*RC* 代表 *Ron's Code* 或 *Rivest's Cipher*。 它的速度比 DES 快，而且它的設計也可以直接替換 DES。 相較於徹底的金鑰搜尋，使用適當的金鑰大小可以用來設定比 DES 較安全或較不安全的等級。它具有 64 位元的區塊大小，而且速度比軟體的 DES 快兩到三倍。 RC2 可以用於與 DES 相同的模式中。

Software Publishers Association (SPA) 與美國政府之間的合約，給予 RC2 特殊的狀態。這可讓出口核准處理比有用的加密出口處理簡單且快速。然而，在某些例外情況下，限制 RC2 金鑰大小爲 40 位元來取得產品快速出口核准的資格。附加字串可用以阻撓試圖預先計算出可能加密之龐大查詢表的入侵者。

RC4. 一種可變的金鑰大小區塊密碼，由 Ron Rivest 針對「RSA 資料安全」而設計出。*RC* 代表 *Ron's Code* 或 *Rivest's Cipher*。 與 RC2 類似，只不過其區塊大小爲 128 個位元。

S

servlet. 一種伺服端程式，可提供其它功能給 Java 啓用的伺服器。

SGML. 標準一般標示語言，全文爲 Standard Generalized Markup Language。

SMTP. 全文爲 ″Simple Mail Transfer Protocol″，意指「簡單郵件轉送通信協定」。

SSL. 全文爲 ″Secure Sockets Layer″，意指「安全 Socket 層次」。

S/MIME. 支援在 Internet 上傳輸之電子郵件的簽名和加密的標準。*請參照* MIME。

T

TCP/IP. 全文爲 ″Transmission Control Protocol/Internet Protocol″，意指「傳輸控制通訊協定/Internet 通訊協定」。

Trust Authority. 一種整合的 IBM SecureWay 安全解決方案，支援數位式憑證的發出、重訂及廢止。這些憑證可以在 Internet 上被廣泛地使用，而且提供了一個方法來驗證使用者及確定可信託的通信。

U

URI. 統一資源指示符 (Uniform Resource Indicator)。

URL. 全文爲 ″Uniform Resource Locator″，意指「統一資源定位器」。

UTF-8. 一種轉換格式。它可讓資訊處理系統只處理 8 位元字集，將 16 位元單位碼轉換爲相當的 8 位元，並再將它轉換回去，而不會流失資料。

V

VPN. 全文爲 ″Virtual Private Network″，意指「虛擬專用網路」。

W

Web 伺服器（Web server）. 一種伺服器程式，負責回應瀏覽器程式所提的資訊資源要求。*另請參照*「伺服器（server）」。

Web 瀏覽器（Web browser）. 在桌上型 PC 上執行的從屬站軟體，可讓使用者瀏覽「全球資訊網」或本端的 HTML 頁面。它是一個擷取工具，可提供對 Web 及 Internet 上可用的大量超媒體資料集合進行廣泛的存取。某些瀏覽器可以顯示文字與圖形，而某些瀏覽器僅能顯示文字。大部分的瀏覽器可以處理主要的 Internet 通信格式，如 FTP 異動。

X

X.509 第 3 版憑證（X.509 Version 3 certificate）. X.509v3 憑證擁有擴充的資料結構來儲存和擷取憑證申請資訊、憑證分送資訊、憑證取消資訊、原則資訊和數位化簽名。

X.509 v3 處理會爲所有的憑證建立加上時間戳記的 CRL。每次使用憑證時， X.509 v3 的功能可讓應用程式檢查憑證的有效性。同時也可讓應用程式判斷應用程式是否位於 CRL 上。X.509v3 CRL 可以建構一段特定的有效期間。它們也會根據其它情況來讓憑證失效。 例如，如果員工離開組織，則它們的憑證就會放在 CRL 上。

X.509 憑證（X.509 certificate）. 一種被廣泛接受的憑證標準，其設計是爲了支援安全管理，以及跨越安全的 Internet 網路來分送以數位方式簽名的憑證。 X.509 憑證定義了許多資料結構，來納入用來分送具公信力第三者數位簽名之公開金鑰的程序。

Printed in Singapore