Tivoli SecureWay Policy Director

版次注意事項

3.7/3.7.1 版

Tivoli SecureWay Policy Director

版次注意事項

3.7/3.7.1 版

Tivoli SecureWay Policy Director 版次注意事項

著作權聲明

商標

IBM、IBM 標誌、Tivoli、Tivoli 標誌、AIX、Cross-Site、NetView、OS/2、Planet Tivoli、RS/6000、Tivoli Certified、Tivoli Enterprise、Tivoli Enterprise Console、Tivoli Ready 與 TME 是「國際商業機器股份有限公司 (IBM)」或 Tivoli Systems Inc. 在美國和（或）其他國家內的商標或註冊商標。

Microsoft、Windows、Windows NT 及 Windows 標誌是 Microsoft 公司在美國和（或）其他國家的商標。

UNIX 是 The Open Group 在美國及其他國家的註冊商標。

Java 和所有以 Java 爲基礎的商標和標誌是 Sun Microsystems, Inc. 在美國和（或）其他國家的商標或註冊商標。

其它公司、產品及服務名稱，可能是其他公司的商標或服務標誌。

注意事項

在本出版品中提及 Tivoli Systems 或 IBM 產品、程式或服務並不表示它們在 Tivoli Systems 或 IBM 有營業的所有國家中都有提供。在此提及這些產品、程式或服務並不表示只能使用 Tivoli Systems 或 IBM 的產品、程式或服務。只要不違反 Tivoli System 或 IBM 的相關智慧財產或其他受法律保護的權限，任何功能相等的產品、程式或服務都可用來取代在此提及的產品、程式或服務。但與其他產品連結操作的評估與驗證，除非 Tivoli Systems 或 IBM 特別指定，不然其責任屬於使用者。在本文件中可能包含著 Tivoli Systems 或 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。有關授權方面的查詢，請以書面信函寄至 IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, New York 10504-1785, U.S.A.

目錄

版次注意事項 - 3.7 / 3.7.1 版（2001 年 3 月 30 日）. 1

一般資訊 2
- 版次注意事項修訂歷程 2
- Adobe Acrobat Reader 4.05 版（建議使用） 4
- 導覽 Policy Director PDF 說明文件. 4
- 聯絡客戶支援中心 4
- Policy Director 3.7.1 CD 配送（2001 年 3 月 30 日） 5
- Policy Director 說明文件集 5
- 可從支援站台取得的修訂版說明文件集 6
- Policy Director 公用軟體下載網頁 7

Policy Director 3.7.1 資訊. 8
- 關於 Policy Director 3.7.1 版 8
- 從 Policy Director 3.7 升級至 3.7.1. 8
- 可供 WebSEAL 安裝使用的新 GSKit 套件 8
- 新的 LDAP 3.2 db2ldif 公用程式修補程式. 9
- Policy Director 所支援的 Domino 登錄 10

重要的補充資訊 11

新的 Base 資訊 12
- ACL 修改延遲的影響 12
- 提供 ivadmin 公用程式只是爲了提供向後相容性 12
- 一般備份和復置程序 12
- 讓 Policy Director 伺服器可讀取 SSL 金鑰資料庫檔案. 13
- DCE 需要 Windows 2000 的整合性登入服務. 14
- 審核記錄格式變更. 15
- Base 安裝手冊：新的 5.2.2 節. 17
- 將 Policy Director ACL 套用至新的 LDAP 字尾 17
- Policy Director LDAP 綱目 26

新的 WebSEAL 資訊 27
- 必要的 WebSEAL SSL 架構（GSKit 快取記憶體大小） 27

架構保護層次的預設品質 30
瞭解 GSKit 金鑰資料庫檔案類型 31
不正確的 Step-up 鑑別架構的結果 34
啓動 junctioncp 公用程式 34
AIX i500 單獨版次注意事項 35
AIX i500 單獨版次注意事項 35
修正 2001 年 1 月的說明文件 40
修正安裝手冊 41
不正確的 SSL 憑證檔名 41
Base 安裝手冊：修訂的 4.4.3 節 41
修正 Base 管理手冊 43
Time-of-Day POP 屬性 43
遍訪許可權 43
修正 WebSEAL 管理手冊 45
更新 WebSEAL for Dynamic URL (WebSEAL 6.3.3) 45
WebSEAL 個人化接合 (WebSEAL 5.7) 45
WebSEAL 僅支援 HTTP/1.0 橫跨接合 45
GSKit 階段作業 ID 逾時參數 46
修正 WebSEAL Developer Reference 47
部署範本 CDAS 伺服器（4.4 節） 47
修正主控台管理手冊 48
管理主控台管理手冊修正 48
軟體限制 49
SMP 系統不支援 NetSEAL 核心設陷 49
NetSEAL 和 NetSEAT 的向後相容性 49
管理主控台無法使用 pdadmin 功能 49
對於雙位元組字元的語言限制 50
LDAP 不對使用者名稱區分大小寫 51
pdconfig 公用程式在日文 HP-UX 系統上可能無法運作 51
管理主控台線上說明不一致 51
已翻譯的主控台線上說明中使用了未翻譯的圖形 52

已知的軟體缺陷和暫行解決方法. 53
安裝和升級的缺陷和暫行解決方法 54
升級 Policy Director 3.6 WebSEAL 54
IBM SecureWay Directory 3.2 需要 AIX 4.3.3 修補程式 57
IBM SecureWay Directory DMT 公用程式無法啓動 58
Base 的缺陷和暫行解決方法 59
架構 Solaris 上的「管理伺服器」 59
LDAP 3.1.x 至 LDAP 3.2 移轉程序修訂 59
IBM DCE 3.1 修補程式 3 解決了「管理伺服器」的記憶體泄漏 60
WebSEAL 的缺陷和暫行解決方法 62
額外的 WAP 閘道支援 62
已刪除的使用者證明仍在 WebSEAL 快取中. 63
CDSSO 的憑證鑑別造成 WebSEAL 發生問題 63
NetSEAL 的缺陷和暫行解決方法 64
AIX 設陷缺陷 64
Solaris 修補程式基本要求 64
管理主控台的缺陷和暫行解決方法 65
管理主控台的缺陷和暫行解決方法 65
LDAP 的缺陷和暫行解決方法 67
在架構 LDAP 時，WebSEAL 會變得不穩定 67

1

版次注意事項 - 3.7 / 3.7.1 版（2001 年 3 月 30 日）

本「版次注意事項」說明文件包含了 Policy Director 3.7（版本 3、版次 7、修改 0）和 Policy Director 3.7.1（版本 3、版次 7、修改 1）的最新和經過修訂的技術資訊。

本說明文件會經常性地更新與 Policy Director 相關的最新資訊。修訂歷程表（在「請先讀我」節中）記錄了本文件的所有新增和變更。

目錄：

1. 一般資訊
2. Policy Director 3.7.1 資訊
3. 重要的補充資訊
4. 修正 2001 年 1 月的說明文件
5. 軟體限制
6. 已知的軟體缺陷和暫行解決方法

一般資訊

註: 如果您是 Policy Director 管理者，您需完整地讀完第11頁的『重要的補充資訊』。

- 版次注意事項修訂歷程
- Adobe Acrobat Reader 4.05 版（建議使用）
- 導覽 Policy Director PDF 說明文件
- 聯絡客戶支援中心
- Policy Director 3.7.1 CD 配送（2001 年 3 月 30 日）
- Policy Director 說明文件集
- 可從支援站台取得的修訂版說明文件集
- Policy Director 公用軟體下載網頁

版次注意事項修訂歷程

以下的「修訂歷程」表格列出了從第一次出版日期以來，本說明文件的所有變更：

Policy Director 3.7 版次注意事項修訂歷程	
日期	**主題**
2000年12月15日	隨 CD 配送提供的第一版。
2000年12月16日	一般備份和復置程序
2000年12月16日	LDAP 3.1.x 至 LDAP 3.2 移轉程序修訂
2000年12月16日	已刪除的使用者證明仍在 WebSEAL 快取中
2001年1月17日	可從支援站台取得的修訂版說明文件集
2001年1月17日	提供 ivadmin 公用程式只是爲了提供向後相容性
2001年1月17日	IBM DCE 3.1 修補程式 3 解決了「管理伺服器」的記憶體泄漏
2001年3月7日	導覽 Policy Director PDF 說明文件
2001年3月7日	Policy Director 公用軟體下載網頁
2001年3月7日	讓 Policy Director 伺服器可讀取 SSL 金鑰資料庫檔案
2001年3月7日	DCE 需要 Windows 2000 的整合性登入服務
2001年3月7日	審核記錄格式變更
2001年3月7日	Base 安裝手冊：新的 5.2.2 節
2001年3月7日	將 Policy Director ACL 套用至新的 LDAP 字尾

Policy Director 3.7 版次注意事項修訂歷程	
日期	主題
2001年3月7日	架構保護層次的預設品質
2001年3月7日	瞭解 GSKit 金鑰資料庫檔案類型
2001年3月7日	不正確的 Step-up 鑑別架構的結果
2001年3月7日	啓動 junctioncp 公用程式
2001年3月7日	不正確的 SSL 憑證檔名
2001年3月7日	Base 安裝手冊：修訂的 4.4.3 節
2001年3月7日	Time-of-Day POP 屬性
2001年3月7日	遍訪許可權
2001年3月7日	更新 WebSEAL for Dynamic URL (WebSEAL 6.3.3)
2001年3月7日	WebSEAL 個人化接合 (WebSEAL 5.7)
2001年3月7日	WebSEAL 僅支援 HTTP/1.0 橫跨接合
2001年3月7日	部署範本 CDAS 伺服器（4.4 節）
2001年3月7日	管理主控台管理手冊修正
2001年3月7日	LDAP 不對使用者名稱區分大小寫
2001年3月7日	升級 Policy Director 3.6 WebSEAL
2001年3月7日	IBM SecureWay Directory 3.2 需要 AIX 4.3.3 修補程式
2001年3月7日	IBM SecureWay Directory DMT 公用程式無法啓動
2001年4月1日	Policy Director 3.7.1 資訊
2001年4月1日	Policy Director LDAP 綱目
2001年4月1日	必要的 WebSEAL SSL 架構（GSKit 快取記憶體大小）
2001年4月1日	AIX i500 單獨版次注意事項
2001年4月1日	GSKit 階段作業 ID 逾時參數
2001年4月1日	pdconfig 公用程式在日文 HP-UX 系統上可能無法運作
2001年4月1日	管理主控台線上說明不一致
2001年4月1日	已翻譯的主控台線上說明中使用了未翻譯的圖形
2001年4月1日	CDSSO 的憑證鑑別造成 WebSEAL 發生問題
2001年4月1日	在架構 LDAP 時，WebSEAL 會變得不穩定

Adobe Acrobat Reader 4.05 版（建議使用）

在此強烈建議您使用 Adobe® Acrobat® Reader™ **4.05 版**來檢視和列印 Policy Director PDF 說明文件。

您可從以下的 Adobe 網站免費取得 Adobe Acrobat Reader 4.05 版：

http://www.adobe.com/products/acrobat/readstep2.html

導覽 Policy Director PDF 說明文件

PDF 格式的 Policy Director 說明文件可讓您輕鬆地瀏覽您需要的資訊。Policy Director PDF 檔案中的許多部份包含了可作用的超本文。

當您的游標移動至超本文區域時，滑鼠的游標會變爲「指向手」的圖示。當您按下超本文區域時，PDF 檢視畫面會跳至文件中或文件外的適當位置。

Policy Director PDF 檔案中的以下部份包含了超本文鏈結：

- 所有的書籤（也可以展開和收合）
- 目錄項目
- 索引頁號碼
- URL（以藍色文字顯示）
- 節交互參考（以藍色文字顯示）

聯絡客戶支援中心

Tivoli Customer Support Handbook 位於：

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

提供了關於「Tivoli 客戶支援中心」的完整資訊，並包含了下列項目：

- 登記與資格
- 視您問題的嚴重性，說明如何聯絡支援中心
- 電話號碼和電子郵件位址（各國專屬）
- 在聯絡支援中心前應收集的資訊

Policy Director 3.7.1 CD 配送（2001 年 3 月 30 日）

Policy Director CD 集：

- Tivoli SecureWay Policy Director Base for AIX（3.7.1 版，128 位元）
- Tivoli SecureWay Policy Director Base for Solaris（3.7.1 版，128 位元）
- Tivoli SecureWay Policy Director Base for Windows（3.7.1 版，128 位元）
- Tivoli SecureWay Policy Director Base for HP-UX（3.7.1 版，128 位元）
- Tivoli SecureWay Policy Director WebSEAL/NetSEAL for AIX、Solaris 和 Windows（3.7.1 版，128 位元）
- Tivoli SecureWay Policy Director WebSEAL/NetSEAL for HP-UX（3.7.1 版，128 位元）
- Tivoli SecureWay Policy Director 管理主控台 Windows 版（3.7.1 版，128 位元）

CD 目錄內容說明：

註: 特定平台所使用的 Policy Director CD 可能不會完全包含這些目錄。

- **/Doc** 包含了 Policy Director 的基本技術資訊
  （您可以在 Tivoli 支援網站取得本說明文件和額外的資訊）。
- **/Policy_Director** 包含了 Policy Director 安裝映像檔
- **/GSKIT** 是 IBM 的 SSL 實作。
- **/Schema** 包含了 Policy Director 所需的 LDAP 綱目檔
- **/SecureWay_Directory** 包含了 IBM LDAP 3.2 安裝映像檔
- **/Security_Services** 包含了 IBM DCE 安裝映像檔
- **/Security_Service_Client** 是在 WebSEAL/NetSEAL CD 中，而 Console CD 中的是 NetSEAT 從屬站

Policy Director 說明文件集

所有最新版本的 Tivoli SecureWay Policy Director 說明文件是放在 Policy Director 3.7 / 3.7.1 的支援頁中。

安裝手冊
Policy Director Base for AIX 安裝手冊
Policy Director Base for HP-UX 安裝手冊
Policy Director Base for Solaris 安裝手冊
Policy Director Base for Windows 安裝手冊
Policy Director WebSEAL 安裝手冊
Policy Director NetSEAL 安裝手冊
Policy Director 管理主控台（Windows 版）安裝手冊
管理手冊
Policy Director Base 管理手冊
Policy Director WebSEAL 管理手冊
Policy Director NetSEAL 管理手冊
Policy Director 管理主控台（Windows 版）管理手冊
程式開發者參考手冊
Policy Director Authorization ADK Developer Reference
Policy Director Authorization API Java Wrappers Developer Reference
Policy Director WebSEAL Developer Reference
Policy Director Administration API Developer Reference
Policy Director CDAS API Developer Reference
Policy Director CDMF API Developer Reference
補充說明文件
Policy Director Performance Tuning Guide
Policy Director Lotus Domino Registry Supplement
Policy Director Migration Tool Administration Guide

可從支援站台取得的修訂版說明文件集

Policy Director 3.7 / 3.7.1 支援站台包含了「Policy Director 安裝手冊」、「管理手冊」和「程式開發者參考手冊」的修訂版本。新的修訂版可取代原始（2000 年 12 月）Policy Director 3.7 CD-ROM 中所內含的說明文件。新修訂版的日期爲 2001 年 1 月。

所有的出版品和經過翻譯的 Policy Director 3.7 說明文件都是根據 2001 年 1 月的版本。配送的 Policy Director 3.7.1 CD 也包含了這個在 2001 年 1 月更新的說明文件。

Policy Director 公用軟體下載網頁

Tivoli 支援站台中的下列網頁，包含了所有 Policy Director 補充軟體下載的鏈結：

http://www.tivoli.com/support/secureway/policy_dir/downloads.html

Policy Director 3.7.1 資訊

- 關於 Policy Director 3.7.1 版
- 從 Policy Director 3.7 升級至 3.7.1
- 可供 WebSEAL 安裝使用的新 GSKit 套件
- 新的 LDAP 3.2 db2ldif 公用程式修補程式
- Policy Director 所支援的 Domino 登錄

關於 Policy Director 3.7.1 版

Policy Director 3.7.1 是提供「國家語言支援 (NLS)」的版次。本產品提供了九種語言的資料處理和訊息顯示：西班牙文、德文、法文、義大利文、巴西葡萄牙文、日文、韓文、簡體中文和繁體中文。

Policy Director 軟體下載網頁中所公佈的個別語言套件，則提供了這些語言版本的所有訊息：

http://www.tivoli.com/support/secureway/policy_dir/downloads.html

從 Policy Director 3.7 升級至 3.7.1

- 所配送的 Policy Director 3.7.1 CD 不支援將 3.7 版的程式碼自動升級至 3.7.1 版。
- 對於要將現存的 3.7 安裝升級至 3.7.1 層次而不重新架構的客戶，則必須下載 Policy Director 3.7 FixPack 2，並且安裝至現存的 Policy Director 3.7 安裝目錄。本程序會保留所有的架構資料。

  您可以從 Tivoli 支援網站取得 FixPack 2 套件：

  https://www.tivoli.com/secure/support/patches/

可供 WebSEAL 安裝使用的新 GSKit 套件

以下的討論內容可適用於 Policy Director 3.7.1 WebSEAL 安裝。

Policy Director 3.7.1 包含了數個版本的 GSKit：

- GSKit 版本 61 (Policy Director 3.7.1 Base for AIX CD)
- GSKit 版本 57 (Policy Director 3.7.1 Base for Solaris CD)

- GSKit 版本 65 (Policy Director 3.7.1 Base for HP-UX CD)
- GSKit 版本 58 (Policy Director 3.7.1 Base for Windows CD)
- GSKit 版本 126 (Policy Director 3.7.1 WebSEAL CD)

最新版本的 GSKit (126) 包含的加強功能可增進 WebSEAL 的效能，並且可解決在 Solaris 安裝上的 LDAP 伺服器的 SSL 連線問題。您必須在所有的 WebSEAL 安裝上使用此版本的 GSKit。

如果您沒有安裝 WebSEAL，則仍可使用原始平台特定 Base CD 中的 GSKit 套件。

新的 LDAP 3.2 db2ldif 公用程式修補程式

最近與 Policy Director 3.7.1 CD 一同分送的 IBM SecureWay Directory (LDAP) 效能增進修補程式會造成 **db2ldif** LDAP 管理公用程式無法使用。**db2ldif** 公用程式並未更新，因而無法辨識正確的成員群組使用者儲存體格式。

針對每個 LDAP 伺服器平台的新 **db2ldif** 修補程式已放在 Policy Director 3.7.1 CD 的 **/Patch** 目錄中，並已更正此問題。

亦請參閱第7頁的『Policy Director 公用軟體下載網頁』。

Policy Director 所支援的 Domino 登錄

僅有 Policy Director 3.7.1 for Windows NT 支援 Domino 登錄。Domino 伺服器本身可以安裝在任何支援的平台上，但是 Policy Director 3.7.1 必須在 Windows NT 上安裝和架構。

Domino 登錄支援所需要的 Policy Director meta 資料庫範本 (**PDMdata.ntf**) 是放在 Policy Director 3.7.1 Base CD 的 **/schema** 目錄中。

您可以在 Policy Director 3.7 / 3.7.1 支援頁中找到修訂過的 *Lotus Domino 登錄補充*說明文件。

Policy Director 3.7.1 for Windows NT 支援 Domino 4.6.x 和 5.0.x 版次。 Policy Director 3.7.1 上的 Domino 登錄架構會用到下列的 Policy Director 套件：PDRTE、PDMgr 和 PDWeb。

架構了 Domino 登錄的 Policy Directoir 3.7.1 不支援從屬站端的憑證鑑別或「跨網域單一登入 (CDSSO)」功能。

重要的補充資訊

- 新的 **Base** 資訊
- 新的 **WebSEAL** 資訊
- **AIX i500** 單獨版次注意事項

新的 Base 資訊

- ACL 修改延遲的影響
- 提供 ivadmin 公用程式只是爲了提供向後相容性
- 一般備份和復置程序
- 讓 Policy Director 伺服器可讀取 SSL 金鑰資料庫檔案
- DCE 需要 Windows 2000 的整合性登入服務
- 審核記錄格式變更
- Base 安裝手冊：新的 5.2.2 節
- 將 Policy Director ACL 套用至新的 LDAP 字尾
- Policy Director LDAP 綱目

ACL 修改延遲的影響

ACL 原則更新程序現在會在 15 秒的閒置逾時期間後被觸發。

您可以在 *ivmgrd.conf* 架構檔的 **[ivmgrd]** 段落中，加入 **notifier-wait-time** 參數，以便手動架構逾時值（秒數）。例如：

```
notifier-wait-time = 25
```

亦請參閱 2001 年 1 月 *Tivoli SecureWay Policy Director Base 管理手冊*中的「6.6.2 節」。

提供 ivadmin 公用程式只是為了提供向後相容性

在 Policy Director 3.7 中，**ivadmin** 公用程式已被 **pdadmin** 公用程式所取代。兩個公用程式的功能完全相同。在 Policy Director 3.7 中，**ivadmin** 公用程式的存在僅是爲了提供向後相容性。

變更公用程式名稱是因爲產品名稱的變更。在 Policy Director (“pd”) 前，本產品被稱爲 IntraVerse (“iv”)。

一般備份和復置程序

一般而言，Policy Director 的詳細備份和復置程序是以每個客戶爲基礎，按照架構的不同所研發。每一個都是開始於相同的基本原則：

- 對於 DCE 備份和復置，請參照適當的的 DCE 說明文件。特別是 **dceback** 指令參照中有值得注意的資訊。

  下列的鏈結可找出 Transarc DCE 的此種資訊：

  http://www.transarc.ibm.com/Library/documentation/dce/1.1/dceback.html

- 對於 Policy Director，備份主要安裝檔案系統（UNIX 系統上的 */opt/PolicyDirector*，以及 Windows NT 系統上的 *\Program Files\Tivoli\Policy Director*）。
- 因爲多重 Policy Director 環境中的備援和高可用性，讓即時災害的可能性降到最低，所以可以在系統不停止處理交易的狀態下，完成復置作業。

讓 Policy Director 伺服器可讀取 SSL 金鑰資料庫檔案

問題：

在無法讀取 LDAP 從屬站鑑別所要使用的 SSL 金鑰資料庫檔案時，Policy Director 會無法運作，並且不作任何反應。

由管理者所建立，用來啓用 IBM SecureWay Directory 從屬站和伺服器間 SSL 通信的 SSL 金鑰資料庫檔案，才適用於此問題。

在架構 Policy Director 管理伺服器和 Policy Director WebSEAL 時所建立的兩個 SSL 金鑰資料庫檔案，並不適用於此問題。

說明：

IBM SecureWay Directory 從屬站可選擇使用「安全 Socket 層 (SSL)」通信協定，來和 IBM SecureWay Directory LDAP 伺服器通信。Policy Director 會使用此通訊通道作爲建立鑑別和鑑別決策程序的一部分。

要能順利地使用 SSL 通信，則需仰賴金鑰資料庫檔案的使用。Policy Director 的使用者必須可以讀取此金鑰資料庫檔案，而此使用者通常是 **ivmgr**。當管理者在建立供 LDAP 從屬站和伺服器間使用的金鑰資料庫檔案時，並未預設指定此許可權。

解決方案：

所有「Base 安裝手冊」的下列章節中說明了 SSL 金鑰資料庫檔案的建立：

文件	節
Policy Director Base for Solaris 安裝手冊	7.3.1, 7.4.1
Policy Director Base for AIX 安裝手冊	6.3.1, 6.4.1
Policy Director Base for Windows 安裝手冊	7.3.1, 7.4.1
Policy Director Base for HP-UX 安裝手冊	6.3.1, 7.4.1

在所有的手冊中，**建立金鑰資料庫檔案和憑證**節包含了從 1 到 10 的作業項目編號清單，並說明了如何使用 **gsk4ikm** GUI 工具來建立金鑰資料庫檔案。請在清單的結尾加入下列文字，作爲步驟 11：

11. 在建立金鑰資料庫檔案後，將金鑰資料庫檔案的檔案所有權變更爲 **ivmgr**。使用適當的作業系統指令來變更檔案所有權。

例如，在 UNIX 中輸入：

```
# chown ivmgr <keyfile>
```

DCE 需要 Windows 2000 的整合性登入服務

問題：

在 Windows 2000 上安裝 NetSEAT 和 Policy Director 後，使用者無法登入至 DCE 元件。

說明：

Windows 2000 導入了名爲「整合性登入服務」的新服務。您必須啓用此服務才能成功地使用 DCE 登入。

解決方案：

啓用「Windows 2000 整合性登入服務」。DCE 登入現在就可以使用。

註: 「Windows 2000 整合性登入服務」和 NetSEAT 整合性登入功能無關。NetSEAT 整合性登入功能**不應**啓用。NetSEAT 整合性登入預設**不**啓用。

審核記錄格式變更

註: 下列資訊更新了 *Tivoli SecureWay Policy Director Base 管理手冊*中的「8.5 節」和「8.6 節」內容。

原始的 Policy Director 3.7 XML 格式審核紀錄不愼重複使用了元素標籤名稱<event>。開始使用<event>時，含括了整個「審核事件」文件。巢狀使用<event>是要表示事件動作識別字。

第二個元素標籤名稱現已變更爲<action>。事件紀錄的版本號碼已經增加，而且新的版本屬性已加入至<component>元素。

新格式事件的範本外觀如下：

```
<event rev="1.1">
<date>2001-02-22-01:25:54.452+00:00I-----</date>
<outcome status="0">0</outcome>
<originator blade="ivmgrd"><component
rev="1.1">azn</component>
<action>0</action>
<location>azn_id_get_creds</location>
</originator>
<accessor name="unauthenticated">
<principal auth="IV_UNAUTH_V3.0">Unauth</principal>
</accessor>
<target
resource="3"><object>IV_UNAUTH_V3.0:unauthenticated
</object></target>
<data>
</data>
</event>
```

Base 安裝手冊：新的 5.2.2 節

摘要：

所有的「Policy Director Base 安裝手冊」均新增了「5.2.2 節」。在這些安裝手冊的「版次注意事項」中，新增下列文字段落：

- 5.2.2 將 ACL 新增至 Policy Director 字尾

說明：

所有的「Policy Director Base 安裝手冊」包含了第 5 章；它的標題爲「架構 Netscape LDAP 伺服器」。本章說明了如何指定供 Netscape LDAP 伺服器使用的 Policy Director 資訊。此章中的指示需在安裝和架構 Policy Director 伺服器前執行。

「5.2 節」說明了 Netscape Directory Server 的額外新字尾。未討論如何處理這些新字尾的「存取控制清單 (ACLs)」。

建立包含下列文字的新「5.2.2 節」：

5.2.2 將 ACL 新增至 Policy Director 字尾

在架構 Policy Director 的時候，它會自動嘗試將適當的 ACL 新增至 LDAP Server 的每個字尾，以便讓 Policy Director 建立和更新那些字尾中的使用者和群組資訊。

若要在起始架構 Policy Director 之後，由 LDAP 管理者新增任何字尾，管理者必須手動新增適當的 ACL。

關於在架構 Policy Director 後將適當的 ACL 新增至字尾的指示，請參閱以下的「Policy Director 3.7 版次注意事項」節：

將 Policy Director ACL 套用至新的 LDAP 字尾.

將 Policy Director ACL 套用至新的 LDAP 字尾

簡介

註: 下列資訊可適用於 IBM SecureWay Directory Server 和 Netscape LDAP Server。

當 LDAP 管理者在起始架構 Policy Director 之後新增 LDAP 字尾時，管理者必須套用適當的「存取控制清單 (ACL)」，以便讓 Policy Director 管理這些新字尾中所定義的使用者和群組。

對於 IBM SecureWay Directory，請使用「目錄管理工具」來套用 ACL。對於 Netscape LDAP 伺服器，請使用 Netscape Console。

請使用適當的 LDAP 管理介面來將下列 ACL 套用至每個新的 Policy Director 字尾：

LDAP 群組	存取控制
cn=SecurityGroup,secAuthority=Default	
	■ 完整存取
cn=ivacld-servers,cn=SecurityGroup,secAuthority=Default	
	■ 讀取 ■ 搜尋 ■ 比較
cn=remote-acl-users,cn=SecurityGroups,secAuthority=Default	
	■ 讀取 ■ 搜尋 ■ 比較

這些控制只有在管理者選取 Policy Director 使用者登錄的 LDAP，而且在起始架構 Policy Director 後建立新 LDAP 字尾時適用。它假設您是 Policy Director 管理者，而且熟悉 Policy Director 和 LDAP。它進一步地假設管理者有適當的權限來更新「LDAP 目錄資訊樹」。

在架構 Policy Director 的時候，它會嘗試將適當的 ACL 套用至那時存在於 LDAP 伺服器中的每個 LDAP 字尾。此存取控制可讓 Policy Director 建立和管理這些 LDAP 字尾中的使用者和群組資訊。

然而，如果在架構 Policy Director 後才建立字尾，則 Policy Director 必須在稍後才能建立和管理此新字尾中的使用者和群組資訊，然後手動套用適當的存取控制。若沒有這些存取控制，Policy Director 會沒有適當的 LDAP 許可權，來建立和管理此新字尾中所指定的使用者和群組資訊。

若要將適當的存取控制套用至新建立的 LDAP 字尾，請根據所使用的 LDAP 伺服器類型，對 IBM SecureWay Directory 或 Netscape Directory Server 執行下列步驟。

請注意，該程序假設新建立的字尾名稱爲「**o=neworg,c=us**」。您應用實際上新建立的字尾來取代下列說明中的此值。

IBM SecureWay Directory Server 的程序

若要將適當的 Policy Director 存取控制套用至 IBM SecureWay Directory Server 中新建立的字尾，請遵循下列步驟：

1. 啓動「LDAP 目錄管理工具 (DMT)」。

   Windows：開始 > 程式集 > IBM SecureWay Directory > 目錄管理工具

   UNIX：# /usr/bin/dmt

2. 以下的警告可能會出現：

   警告：o=neworg,c=us 登錄未包含任何資料。

   如果出現了此警告，它是指出新建立的字尾所代表的登錄不存在。除非建立了字尾所代表的登錄，否則存取控制無法套用至新建立的字尾。

   跳出警告並且繼續執行「步驟 3」。您會在步驟 6 中建立新字尾中所指定的組織登錄。

   如果此警告未出現，則新建立的字尾中所指定的組織登錄已存在。

   請繼續進行「步驟 3」並且略過「步驟 6」。

3. 按一下左框底端的「新增伺服器」按鈕。

   「新增伺服器」視窗將會出現。

4. 請在下列欄位中輸入值：

欄位	值	備註
伺服器名稱：	ldap://<hostname>	例如 ibm007.ibm.com
埠：	389	389 爲預設埠

欄位	值	備註
使用者 DN：	cn=root	LDAP 管理者的 DN
使用者密碼：	abc123	LDAP 管理者的密碼

5. 按一下「確定」。

   會出現「目錄管理工具」頁面。

6. 如果新建立的字尾中所指定的組織登錄不存在（也就是您收到了步驟 2 中所說明的警告訊息），請依照 *Tivoli SecureWay Policy Director Base 安裝手冊*中的「4.4.2 節」來建立登錄。

   當您完成建立登錄時，請略過「Base 安裝手冊」中的「步驟 9」，然後繼續執行以下的「步驟 7」。

   如果組織登錄已存在，請繼續執行以下的「步驟」。

7. 請在「目錄管理工具」的左窗格中選取：

   目錄樹 > 瀏覽樹

8. 請在右邊的「瀏覽樹」窗格中亮顯標示新建立的字尾。

9. 按下窗格上方的 ACL 按鈕。

   該字尾目前的「存取控制清單」設定會顯示在「編輯 LDAP ACL」視窗中。

10. 請在「編輯 LDAP ACL」視窗中的「主題」區域輸入下列的「識別名稱」：

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

    勾選群組類型然後按下「新增」按鈕。

11. 當重新顯示窗格時，請選擇下列設定：

    授與「新增」子項和「刪除」登錄權限。

    所有的許可權（讀取、寫入、搜尋和比較）應授與所有的「安全」等級。

    若要這樣做，請確定在每個所有等級中的「讀取」、「寫入」、「搜尋」和「比較」直欄選項均指示「授與」。

    請確定已在 DN 登錄窗格頂端選取了「下一代目錄樹登錄繼承此登錄」。

在完成所有選項後，請按下窗格底端的「確定」。

12. 再一次在右邊的「瀏覽樹」窗格中標示新建立的字尾。
13. 按下窗格上方的 ACL 按鈕。

    請驗證列出了 **cn=SecurityGroup,secAuthority=Default** 群組，而且群組的設定正確。請注意，群組名稱不分大小寫。
14. 請在「編輯 LDAP ACL」視窗中的「主題」區域輸入下列的「識別名稱」：

    ```
    cn=ivacld-servers,cn=SecurityGroups,secAuthority=Default
    ```

    勾選群組類型然後按下「新增」按鈕。
15. 當重新顯示窗格時，請選擇下列設定：

    不指定「新增」子項和「刪除」登錄的權限。

    「讀取」、「搜尋」和「比較」許可權僅可授與「正常安全」等級。

    若要這樣做，請在「正常安全」等級的所有「讀取」、「搜尋」和「比較」直欄中選取「授與」。

    不指定「正常安全」等級的「寫入」許可權。

    不指定「敏感和重要安全」等級的所有許可權。

    請確定已在 DN 登錄窗格頂端選取了「下一代目錄樹登錄繼承此登錄」。

    在完成所有選項後，請按下窗格底端的「確定」。
16. 再一次在右邊的「瀏覽樹」窗格中標示新建立的字尾。
17. 按下窗格上方的 ACL 按鈕。

    請驗證列出了 **cn=ivacld-servers,cn=SecurityGroups,secAuthority=Default** 群組，而且群組的設定正確。請注意，群組名稱不分大小寫。
18. 請在「編輯 LDAP ACL」視窗中的「主題」區域輸入下列的「識別名稱」：

    ```
    cn=remote-acl-users,cn=SecurityGroups,secAuthority=Default
    ```

    勾選群組類型然後按下「新增」按鈕。

19. 當重新顯示窗格時，請選擇下列設定：

    不指定「新增」子項和「刪除」登錄的權限。

    「讀取」、「搜尋」和「比較」許可權僅可授與「正常安全」等級。

    若要這樣做，請僅在「正常安全」等級的所有「讀取」、「搜尋」和「比較」直欄中選取「授與」。

    不指定「正常安全」等級的「寫入」許可權。

    不指定「敏感和重要安全」等級的所有許可權。

    請確定已在 DN 登錄窗格頂端選取了「下一代目錄樹登錄繼承此登錄」。

    在完成所有選項後，請按下窗格底端的「確定」。

20. 「存取控制清單」的變更到此完成。

    請選取「結束」按鈕以便完成「目錄管理工具」。

Netscape Directory Server 的程序

若要將適當的 Policy Director 存取控制套用至 Netscape Directory Server 中新建立的字尾，請遵循下列步驟：

1. 啓動 Netscape Directory Console

   開始 > 程式集 > Netscape Server Products > Netscape Console

   在 Netscape 伺服器安裝目錄中：

   ```
   # ./startconsole
   ```

2. 請在 Netscape Console 登入視窗中，輸入管理者 ID、密碼和 URL，以便存取 Netscape 管理網頁。

   例如：

使用者 ID：	cn=Directory Manager
密碼：	abc123
管理 URL：	http://ibm007.ibm.com:<port number>

   按下 OK 按鈕以便登入。

3. 將網域中架構爲您所使用的 Netscape Directory Server 的伺服器名稱展開。

然後展開 Server Group，並且標示您所使用的 Directory Server。

按下右窗格中的 Open 按鈕。

其他的視窗會顯示一組標籤展示 Directory Server 正在執行的作業。

4. 選取 Directory 標籤。
5. 如果新建的字尾出現在左窗格，請繼續執行「步驟 6」。

   如果新建的字尾 (**o=neworg,c=us**) 未出現在左窗格中，這表示新字尾的登錄不存在。除非建立了登錄，否則存取控制無法套用至新建立的字尾。

   如果是這樣，請在視窗頂端的工作列中選許 Object，然後選取：

   ```
   New > Other...
   ```

   New Object 選項視窗會出現。向下捲動，並且標示 "Organization" 作爲新的物件登錄類型。然後按下 OK。

   Property Editor 視窗將會出現。請在 Organization 欄位中填入 "**neworg,c=us**"，然後按下 OK。請記得這些指示是假設使用範例字尾。請建立與實際字尾對應的登錄類型和名稱。

   現在請在視窗的頂端選取工作列中的 View，然後選取 Refresh。

   新的字尾登錄應會顯示在左窗格中。
6. 在左窗格中標示 **neworg** 登錄，然後在視窗頂端的工作列中選取 Object。然後按下 Set Access Permissions...

   Multi-value ACI Selector 視窗將會出現。

   按下 New 按鈕以便顯示 Set Access Permissions 視窗。
7. 按下 Allow/Deny 欄位並且將它設定爲 Allow。
8. 按兩下 User/Group 欄位。Select Users and Groups 視窗將會出現。

   將類型設定爲 Add Group to List，然後輸入以下的群組名稱：

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

   按下 Add 按鈕。

   然後按下畫面底端的 OK。

9. 當重新顯示 Set Access Permissions 視窗時，請確定 User/Group 欄位中正確地列出了群組名稱，而且 Rights 欄位指示了 All。
10. 按下 Add Rule 按鈕。以預設值新增另一個規則。
11. 在新增的規則中，按下 Allow/Deny 欄位，然後將它設定爲 Allow。
12. 按兩下 User/Group 欄位。Select Users and Groups 視窗將會出現。

    將類型設定爲 Add Group to List，然後輸入以下的群組名稱：

    ```
    cn=ivacld-servers,cn=SecurityGroups,secAuthority=Default
    ```

    按下 Add 按鈕。

    然後按下畫面底端的 OK。
13. 當重新顯示 Set Access Permissions 視窗時，請確定 User/Group 欄位中正確地列出了群組名稱。
14. 按兩下 Rights 欄位，而且只勾選「讀取」、「搜尋」和「比較」等受影響的權限。所有其他的權限都不應選取。

    然後按下 OK。
15. 按下 Add Rule 按鈕。另一個規則爲使用預設值新增。
16. 在新增的規則中，按下 Allow/Deny 欄位，然後將它設定爲 Allow。
17. 按兩下 User/Group 欄位。Select Users and Groups 視窗將會出現。

    將類型設定爲 Add Group to List，然後輸入以下的群組名稱：

    ```
    cn=remote-acl-users,cn=SecurityGroups,secAuthority=Default
    ```

    按下 Add 按鈕。

    然後按下畫面底端的 OK。
18. 當重新顯示 Set Access Permissions 視窗時，請確定 User/Group 欄位中正確地列出了群組名稱。
19. 按兩下 Rights 欄位，而且只勾選「讀取」、「搜尋」和「比較」等受影響的權限。所有其他的權限都不應選取。

    然後按下 OK。
20. 當重新顯示 Set Access Permissions 視窗時，三個群組規則都應顯示。

按下畫面底端的 OK。

21. 存取控制即已新增。

    您可以選取下列項目（從工作列）來結束 Netscape Console：

    ```
    Console > Exit
    ```

Policy Director LDAP 綱目

Policy Director 使用標準的 LDAP 綱目來實作所有的使用者登錄功能。此綱目可讓 Policy Director 與其他大多數的 LDAP 應用程式的使用者和群組管理功能相容。

因爲 Policy Director 支援廣泛的授權功能，自定的 Policy Director LDAP 物件定義可延伸此標準的綱目。這些自定物件的綱目會在安裝 Policy Director 時發佈於 LDAP 目錄，而可讓其他 LDAP 應用程式使用。

您有時會需要修改這些自訂物件的綱目定義，以及增加新物件的定義。雖然升級 Policy Director 時可以隱藏這些變更，其他應用程式還是會察覺這些變更。所以，在此建議協力廠商的應用程式不要使用安裝時所提供的自訂 Policy Director LDAP 物件定義。

需要獨立於 Policy Director 管理工具之外，來維護授權資訊的協力廠商應用程式可以使用 API。請參照 *Tivoli SecureWay Policy Director Administration API Developer Reference*（可從 Policy Director 支援網頁取得）。

新的 WebSEAL 資訊

- 必要的 WebSEAL SSL 架構（GSKit 快取記憶體大小）
- 架構保護層次的預設品質
- 瞭解 GSKit 金鑰資料庫檔案類型
- 不正確的 Step-up 鑑別架構的結果
- 啓動 junctioncp 公用程式

必要的 WebSEAL SSL 架構（GSKit 快取記憶體大小）

背景：

WebSEAL 預設 SSL 快取記憶體大小的限制爲：

- 512 項目 (SSL V3)
- 256 項目 (SSL V2)

此大小對大部份的產品部署是不足的。

Policy Director 的 GSKit 元件提供了 WebSEAL SSL 服務。當 GSKit SSL 階段作業快取用盡時，WebSEAL 會拒絕所有新的 SSL 鑑別。

您可以使用環境變數來架構 GSKit SSL 階段作業快取的大小。

GSKit SSL 階段作業快取的空間基本要求，主要是取決於兩個因素的相互影響：

- 每秒鑑別的數量
  此鑑別速率會使快取中的登錄增加。
- 階段作業 ID 生命週期值（**ssl-v2-timeout** 或 **ssl-v3-timeout** 參數）
  此參數可減少快取中的登錄。

架構指引：

環境變數 (**GSK_V3_SIDCACHE_SIZE**) 可指定 GSKit SSL 階段作業快取大小。您可以經由以下方法來預估快取的最佳大小：

1. 判斷鑑別存取率的每秒平均值，以及

2. 在 **ssl-v2-timeout** 或 **ssl-v3-timeout** 參數（在 *secmgrd.conf* 架構檔中）中設定適當的階段作業 ID 逾時值。

安裝時的預設值：

```
GSK_V3_SIDCACHE_SIZE = 512（登錄）
ssl-v2-timeout = 100（秒）
ssl-v3-timeout = 7200（秒，或 2 小時）
```

WebSEAL 階段作業 ID 管理會牽涉到 GSKit 階段作業 ID 快取和 WebSEAL 證明快取之間的組合互動。因此，您應另外設定 WebSEAL 證明快取逾時 (**ssl-cache-timeout**)，使它與 GSKit **ssl-v2-timeout** 或 **ssl-v3-timeout** 值相等。

ssl-cache-timeout 參數是在 *secmgrd.conf* 架構檔中。安裝時的預設值爲：

```
ssl-cache-timeout = 3600（秒，或 1 小時）
```

以下的公式可讓您決定 GSKit SSL 階段作業快取的適當大小：

```
鑑別次數/秒 * ssl-v3-timeout 值 = 快取大小
```

例如，單一 WebSEAL 伺服器每秒鑑別速率的保守估計爲每秒 40 個。如果您保留了 **ssl-v3-timeout** 參數的預設值 (7200)，則快取大小爲：

```
40 個登錄/秒 * 7200 秒 = 288000 個登錄
```

在啓動 Policy Director 前修改此變數：

1. 停止 Policy Director：

   ```
   # iv stop
   ```

2. 設定 **GSK_V3_SIDCACHE_SIZE** 環境變數：

   ```
   # GSK_V3_SIDCACHE_SIZE=288000
   # export GSK_V3_SIDCACHE_SIZE
   ```

3. 啓動 Policy Director：

   ```
   # iv start
   ```

註: GSKit 程式碼會將 GSK_V3_SIDCACHE_SIZE 值向下修正爲最接近的 2 的次方值。例如 24000 會減少至 16384、144000 減少至 131072、4096 爲 4096，以此類推。

如果您重新啓動 WebSEAL 機器，此環境變數值會遺失，而會重設爲預設值 (512)。若要避免此問題，請將適當的 **export** 指令插入至 **iv start** Script。

增加 GSKit SSL 階段作業快取大小的結果會讓 WebSEAL 程序 (**secmgrd**) 使用更多的記憶體。144000 的 GSKit SSL 階段作業快取大小會使 WebSEAL 增加使用多達 100MB 的記憶體。若相同機器上存在 **ivmgrd** 和 **ivacld**，則也會增加記憶體的使用量。

經由減少 **ssl-v3-timeout** (或 **ssl-v2-timeout**) 參數（減少每個快取登錄的最大生命週期）的值，可讓您指定較小的快取大小。

支援 Internet Explorer 的特別注意事項：

Microsoft Internet Explorer 的使用者會遇到一個特別的狀況，就是現在有一個問題會導致大約每兩分鐘就會重新協調階段作業。如果您使用 Internet Explorer，您很可能會架構 WebSEAL 來利用 SSL 的 HTTP 階段作業狀態 cookie 機制 (**ssl-cookie-sessions**)，以便維護登入階段作業。

然而，重新協調的階段作業 ID 會不斷地產生 GSKit 階段作業 ID 快取。先前所討論的階段作業 ID 逾時是由 **ssl-v2-timeout** 或 **ssl-v3-timeout** 參數的值所決定。如果鑑別速率很高，在此參數使用大的值會使快取被很快地用盡。

在這個狀態下，您可能會考慮將 **ssl-v2-timeout** 或 **ssl-v3-timeout** 參數設定爲 3 或 4 分鐘。這相當符合 Internet Explorer 的重新協調速率，而且可讓 GSKit 快取不被這些重新協調的階段作業 ID 所填滿。

相關議題：

另一個相關的議題爲架構 WebSEAL SSL 證明快取的大小。指定此值的參數爲 **ssl-cache-max-sessions**（位於 *secmgrd.conf* 檔中）。

此參數控制了此快取可容許多少個同時存在的 SSL 階段作業。該參數會影響 SSL 階段作業的效能，而且請先考慮這個事實，再決定是否要增加。如果您要變更此參數，請使用多個設定來執行一些效能測試。

關於管理 WebSEAL 階段作業狀態的進一步資訊，請參閱 *Tivoli SecureWay Policy Director 3.7 WebSEAL 管理手冊* 的「4.2 節」。

架構保護層次的預設品質

您可以透過管理保護的品質，來控制 WebSEAL SSL 存取所需的加密預設層次。保護管理的預設品質是透過 *iv.conf* 架構檔中的兩個參數來控制：

- **ssl-qop-mgmt**
- **[ssl-qop-mgmt-default]** 段落中的項目

1. 啓用保護管理的品質：

```
[wand]
ssl-qop-mgmt = yes
```

2. 指定 SSL 存取的預設加密層次：

```
[ssl-qop-mgmt-default]
# default = ALL | NONE | cipher-level
# ALL（啓用所有的密碼）# NONE（停用所有的密碼並且使用 MD5 MAC 總合檢查）
# DES-40
# DES-56
# DES-168
# RC2-40
# RC2-128
# RC4-40
# RC4-128
default = ALL
```

請注意，您也可以指定所選取群組的密碼：

```
[ssl-qop-mgmt-default]
default = RC4-128
default = RC2-128
default = DES-168
```

註: **ssl-qop-mgmt = yes** 參數也可以啓用 **[ssl-qop-mgmt-hosts]** 和 **[ssl-qop-mgmt-networks]** 段落中的任何設定。這些段落可容許特定主機/網路/網路遮罩 IP 位址的保護管理品質。**[ssl-qop-mgmt-default]** 段落則列出了所有不符合 **[ssl-qop-mgmt-hosts]** 和 **[ssl-qop-mgmt-networks]** 段落的所有 IP 位址所使用的密碼。

[ssl-qop-mgmt-hosts] 和 **[ssl-qop-mgmt-networks]** 段落僅是要提供向後相容性。在此不建議您使用這些 Policy Director 3.7 架構中的段落。

瞭解 GSKit 金鑰資料庫檔案類型

註: 以下的資訊可增強 *Tivoli SecureWay Policy Director WebSEAL 管理手冊*中的「2.6 節」內容。

「IBM 金鑰管理工具 (iKeyman)」使用了下表中彙總的數個檔案類型。

CMS 金鑰資料庫包含了副檔名爲 .kdb 的檔案，而且可能有兩個以上的其他檔案。在建立新的金鑰資料庫時，就會建立 .kdb 檔。.kdb 檔案中的金鑰紀錄可以是憑證或具有加密的私有金鑰資訊的憑證。

在您建立新憑證要求時，就會建立 .rdb 和 .crl 檔。整個 CA 憑證要求程序都需要 .rdb 檔。

檔案類型	說明
.kdb	「金鑰資料庫」檔。儲存了個人憑證、個人憑證要求和簽章憑證。例如，WebSEAL 的預設金鑰資料庫檔爲 pdsrv.kdb。
.sth	「隱藏」檔。儲存了金鑰資料庫密碼的加密版本。此檔的起源名稱與相關的 .kdb 檔相同。
.rdb	「要求」資料庫檔。在建立 .kdb 金鑰資料庫檔時會自動建立。此檔的起源名稱與相關的 .kdb 檔相同。此檔包含了未執行和未從 CA 接收到的憑證要求。 當 CA 傳回憑證時，會搜尋 .rdb 檔以便比對憑證要求（根據公開金鑰）。如果找到符合的項目，則會接收憑證，而對應的憑證要求會從 .rdb 檔中刪除。 如果找不到符合的項目，則會拒絕接收憑證。憑證要求中包含了一般名稱、組織、街道地址和其他在要求時所指定的資訊，以及與要求相關的公開和私密金鑰。
.crl	「憑證廢止清單」檔。此檔一般包含了因爲某些原因被取消的憑證清單。然而，iKeyman 不對憑證廢止清單提供任何支援，所以它是空的。
.arm	已編碼的 ASCII 二進位檔。.arm 檔包含了以 base-64 編碼 ASCII 表示的憑證，並包含了其公開金鑰，而不含私密金鑰。原始的二進位憑證資料會被轉換爲 ASCII 表示方式。 當使用者收到 .arm 檔形式的憑證時，iKeyman 會對 ASCII 表示方式做解碼動作，然後以二進位表示方式置入適當的 .kdb 檔。同樣地，當使用者從 .kdb 檔取出憑證時，iKeyman 會將資料從二進位轉換爲 ASCII，然後將它置入 .arm 檔。 .arm 檔中的 ASCII 資料就是您在憑證要求程序中所傳送給 CA 的資料。 請注意：只要檔案是 Base64 編碼的檔案，任何檔案類型（包含 .arm 以外）都可以使用。
.der	「識別編碼規則」檔。.der 檔包含了以二進位表示的憑證，並包含了其公開金鑰，而不含私密金鑰。除了表示方式是二進位而不是 ASCII 以外，它和 .arm 檔非常類似。

檔案類型	說明
.p12	「PKCS 12 檔；PKCS 是指「公開金鑰加密標準」。.p12 檔包含了以二進位表示的憑證，並包含了公開和私密金鑰。 .p12 檔也可能包含了多個憑證；例如，憑證、發出憑證的 CA 本身的憑證、CA 憑證的發出者以及其發出者等等。因爲 .p12 檔包含了私密金鑰，它受到密碼保護。

不正確的 Step-up 鑑別架構的結果

如果在 *iv.conf* 架構檔的 **[authentication-levels]** 段落中，不正確地架構了 step-up 鑑別層次，會使 WebSEAL 中的 step-up 功能停用。此狀況會導致非預期的鑑別行爲，例如由 POP 保護的物件所發出的密碼登入頁，需要標記卡鑑別層次。

在修改 step-up 鑑別層次後，請檢查 *secmgrd.log* 檔案以取得任何架構錯誤的報告。

啓動 junctioncp 公用程式

註: 下列資訊更新了 *Tivoli SecureWay Policy Director WebSEAL 管理手冊* 中的「5.2.1 節」和「C.1 節」內容。

在使用 **junctioncp** 公用程式前，您必須：

1. 以 **root** 使用者或 **ivmgr** 使用者來登入。

   junctioncp 公用程式必須可以讀取 **ivmgr** 所擁有的 *secmgrd.conf* 檔。

2. 此外，您必須執行 **dce_login**（UNIX 或 Windows）或 **netseat_login**（Windows）。

3. 最後，請依說明文件中所述，呼叫 **junctioncp** 指令。

AIX i500 單獨版次注意事項

■ AIX i500 單獨版次注意事項

AIX i500 單獨版次注意事項

簡介

這些注意事項是根據並參照 *Tivoli SecureWay Policy Director 3.7 Base for Solaris 安裝手冊*中的第 6 章（架構 LiveContent Server）。

在 LiveContent(i500) 的目錄中安裝和架構 AIX 上的 Policy Director 3.7.1，是需要多個步驟的作業。以下是必要步驟的摘要。

1. 在 AIX 主機上安裝 Policy Director 3.7.1 套件。
2. 將 i500 特定的架構檔複製至 i500 主機。
3. 架構除了 PDAcld 以外的必要 Policy Director 3.7.1 元件。只有在 i500 目錄中架構了 PDMgr 後，才能架構 PDAcld。
4. 將前一步驟中所產生的 i500 架構資料檔複製至 i500 主機。
5. 使用 i500 的外部架構 Script 來執行 i500 主機的 i500 目錄中的架構。
6. 重複步驟 3、4 和 5 來安裝 PDAcld 或任何其他的伺服器。

您可以重複步驟 3、4 和 5 來解除架構任何或全部的 Policy Director 3.7 元件。

軟體需求

此次的配送僅支援將 AIX 上的 Policy Director 安裝至 Solaris 上的 i500 目錄。i500 所支援的版本和 Policy Director 3.7 相同：

- LiveContent DSA V8.3.1.12
- LDAP Server V8.2.4.8

在 AIX 上安裝 Policy Director 3.7.1

請依照 *Tivoli SecureWay Policy Director 3.7 Base for AIX 安裝手冊*以及「Policy Director 版次注意事項」來安裝 Policy Director

3.7.1。*/opt/PolicyDirectory/i500_external* 目錄會被建立。因爲此目錄中的內容包含了 i500 特定的架構檔，故需轉送至 i500 伺服器的目錄：

```
<any-i500o-host-directory>/i500_external
```

架構 LiveContent 目錄

請遵循 *Tivoli SecureWay Policy Director 3.7 Base for Solaris 安裝手冊* 中的「6.2 節」。「步驟 2」中的條件在 Policy Director 3.7.1 中是可選用的。

I500_DAP_PORT 環境變數可以定義來包含 DAP 埠號。否則 DAP 埠會被預設爲 LDAP 埠號的前一號。

載入 Policy Director 綱目

請遵循 *Tivoli SecureWay Policy Director 3.7 Base for Solaris 安裝手冊* 中的「6.3 節」。包含綱目檔的目錄爲：

```
<any-i500-host-directory>/i500_external/lib
```

在 AIX 上安裝時會複製至 *i500_external* 目錄。

Policy Director 主機系統的架構

請遵循 *Tivoli SecureWay Policy Director 3.7 Base for Solaris 安裝手冊* 中的「6.4 節」。該作業是在 i500 的 Solaris 主機上執行，而不是在 Policy Director 的 AIX 主機上執行。若 i500 已架構，則「6.4.1 節」的步驟 1 至 5 不適用。請在 i500 主機上執行下列作業：

- 將 $ODSRELEASE/<*dsa-name*>/oidslocal 複製/附加至 $ODSRELEASE/scripts。

架構 IBM LDAP 從屬站

請遵循 *Tivoli SecureWay Policy Director 3.7 Base for Solaris 安裝手冊* 中的「6.5 節」。

使 LiveContent 綱目同步化

請遵循 *Tivoli SecureWay Policy Director 3.7 Base for Solaris 安裝手冊* 中的「6.6 節」。DAC 檔可以從以下位置複製：

```
/opt/PolicyDirector/i500_external/lib
或
<any-i500-host-directory>/i500_external/lib
```

架構 AIX 上的 Policy Director

您可以根據 *Tivoli SecureWay Policy Director 3.7 Base for AIX 安裝手冊*中的第 7 章來架構 AIX 機器上的 Policy Director。

這時可以架構除了 PDAcld 以外的所有元件。在正確地架構 PDAcld 前，您必須在 i500 主機上完整地架構 PDMgr。

如果架構順利完成，則會產生 */tmp/aaa_details.cfg* 檔。此檔包含了 Policy Director 安全常駐程式的密碼，因此只有 "root" 才有讀取和寫入的許可權。此檔必須傳送至 i500 主機以便繼續架構。

架構 i500 主機上的 Policy Director

1. 移至目錄：

   <any-i500-host-directory>/i500_external/bin

2. 輸入下列：

   Perl i500_ext_config -h *<hostname>* -p *<LDAP-port#>* -P *<DAP-port#>* -D *<i500-admin-DN>* -w *<i500-admin-pwd>*

   以下的功能表會顯示：

   ```
   Policy Director i500 外部架構
   1. 新增存取控制資訊至 Policy Director  DIT
   2. 自 Policy Director  DIT 移除存取控制資訊
   3. 新增作為管理代理程式的伺服器常駐程式
   4. 移除作為管理代理程式的伺服器常駐程式
   5. 刪除 AAA 檔
   6. 結束
   選取功能表項目：
   ```

3. 選取項目 1。下列要求將會出現：

   輸入 GSO 字尾的「識別名稱」：

4. 請輸入 GSO 字尾的名稱；該名稱與架構 Policy Director 時要求輸入者相同。當作業完成時，功能表會再次出現。

5. 請取項目 3。下列的要求會出現：

   輸入 AAA 檔的目錄/檔案路徑：

6. 請輸入從 AIX 主機上的 */tmp/aaa_details.cfg* 複製的檔案名稱和路徑。預設爲相同的檔案路徑。

此檔的內容爲 AIX 機器上架構的伺服器 DN 和密碼。當作業完成時，功能表會再次出現。

7. 請選取項目 5。下列要求將會出現：

   輸入 AAA 檔的目錄/檔案路徑：

8. 重新輸入 *aaa_details.cfg* 檔的名稱。

   因爲安全性的考量，該檔案會被刪除。當作業完成時，功能表會再次出現。

9. 選取項目 6 以便結束架構工具。

   您現在可以安全地在 AIX 主機上架構 PDAcld 或必要時在其他的主機上架構其他的 Policy Director 分支。

解除架構 AIX 上的 Policy Director

您可以根據 *Tivoli SecureWay Policy Director 3.7 Base for AIX 安裝手冊*中的第 7 章來解除架構 AIX 主機上的 Policy Director。

當解除架構順利完成，則會建立 /tmp/aaa_details.cfg 檔。此檔必須傳送至 i500 主機以便繼續解除架構。

解除架構 i500 主機上的 Policy Director

1. 移至目錄：

   <any-i500-host-directory>/i500_external/bin

2. 輸入下列：

   Perl i500_ext_config -h *<hostname>* -p *<LDAP-port#>* -P *<DAP-port#>* -D *<i500-admin-DN>* -w *<i500-admin-pwd>*

   以下的功能表會顯示：

   ```
   Policy Director i500 外部架構
   1. 新增存取控制資訊至 Policy Director  DIT
   2. 自 Policy Director  DIT 移除存取控制資訊
   3. 新增作為管理代理程式的伺服器常駐程式
   4. 移除作為管理代理程式的伺服器常駐程式
   5. 刪除 AAA 檔
   6. 結束
   選取功能表項目：
   ```

3. 選取項目 2。

   當作業完成時，功能表會再次出現。

4. 選取項目 4。下列要求將會出現：

   輸入 AAA 檔的目錄/檔案路徑：

5. 請輸入從 AIX 主機上的 */tmp/aaa_details.cfg* 複製的檔案名稱和路徑。預設爲相同的檔案路徑。

   此檔的內容爲 AIX 機器上架構的伺服器 DN 。當作業完成時，功能表會再次出現。

6. 請選取項目 5。下列要求將會出現：

   輸入 AAA 檔的目錄/檔案路徑：

7. 重新輸入 *aaa_details.cfg* 檔的名稱。

   因爲安全性的考量，該檔案會被刪除。當作業完成時，功能表會再次出現。

8. 選取項目 6 以便結束架構工具。

   Policy Director 或任何 Policy Director 的元件現已解除架構。

修正 2001 年 1 月的說明文件

- 修正安裝手冊
- 修正 **Base** 管理手冊
- 修正 **WebSEAL** 管理手冊
- 修正 **WebSEAL Developer Reference**
- 修正主控台管理手冊

修正安裝手冊

- 不正確的 SSL 憑證檔名
- Base 安裝手冊：修訂的 4.4.3 節

不正確的 SSL 憑證檔名

Policy Director 3.7 Base for AIX、Solaris、HP-UX 和 Windows 的安裝手冊中，包含了不正確的文字檔檔名；該文字檔是用來儲存在安裝「Policy Director 管理伺服器」時所建立和架構的 SSL 憑證。

正確的名稱爲：

```
pdcacert.b64
```

而不是：

```
pdacert.b64.
```

檔案的完整路徑爲：

Solaris、AIX 和 HP-UX：

```
/opt/PolicyDirector/ivmgrd/keytabs/pdcacert.b64
```

Windows：

```
C:\Program Files\Tivoli\Policy Director\ivmgrd\keytabs\pdcacert.b64
```

Base 安裝手冊：修訂的 4.4.3 節

摘要：

所有「Policy Director Base 安裝手冊」中的「4.4.3 節」內容均已修訂。請使用以下列爲標題的資訊來取代「4.4.3 節」：

- **4.4.3 新增 ACL 至 Policy Director 字尾**

說明：

所有的「Policy Director Base 安裝手冊」包含了第 4 章；它的標題爲「架構 IBM LDAP」。本章說明了如何指定供 IBM SecureWay Directory 伺服器使用的 Policy Director 資訊。此章中的指示需在安裝和架構 Policy Director 伺服器前執行。

「第 4 章」包含了「4.4.3 節 新增 Policy Director 群組至 LDAP ACL」。本節說明了如何使 Policy Director 成爲「LDAP 目錄資訊樹 (DIT)」中的 Policy Director 字尾擁有者。

「4.4.3 節」中的指示已修訂。Policy Director 不需要成爲 Policy Director 字尾的擁有者。Policy Director 可以完整地使用 LDAP，而不需要成爲 Policy Director 字尾的擁有者。

如果 Policy Director 擁有字尾，則可能會在日後造成 LDAP 管理上的困難。例如，如果在從 DIT 移除字尾前就移除了 Policy Director 伺服器，LDAP 管理者將無法完全控制剩餘的字尾。

使用下列文字來取代整個「4.4.3 節」：

4.4.3 新增 ACL 至 Policy Director 字尾

在架構 Policy Director 的時候，它會自動嘗試將適當的 ACL 新增至 LDAP Server 的每個字尾，以便讓 Policy Director 建立和更新那些字尾中的使用者和群組資訊。

若要在起始架構 Policy Director *之後*，由 LDAP 管理者新增任何字尾，管理者必須手動新增適當的 ACL。

關於在架構 Policy Director 後將適當的 ACL 新增至字尾的指示，請參閱以下的「Policy Director 3.7 版次注意事項」節：

將 Policy Director ACL 套用至新的 LDAP 字尾.

修正 Base 管理手冊

- Time-of-Day POP 屬性
- 遍訪許可權

Time-of-Day POP 屬性

以下的注意事項是用來說明 *Tivoli SecureWay Policy Director Base 管理手冊*的「4.2.3 節」：

可選用的時區參數（*代表了 Policy Director 伺服器的時區*）會被預設爲 **local**。

遍訪許可權

註: 以下的資訊是用來取代 *Tivoli SecureWay Policy Director Base 管理手冊*中「3.5.3 節」的文字和圖形。相同文件中的「3.7.2」節也已作適當的修訂。

遍訪 (**T**) 許可權可適用於 WebSEAL 階層性物件空間中的配置區物件。遍訪許可權可指定 ACL 登錄中可識別的使用者或群組，具有通過此配置區物件的許可權，以便取得階層下的資源物件的存取權。遍訪許可權不會授與該配置區物件任何其他的許可權。所要求的資源物件本身不需要遍訪許可權。然而，該資源物件的上層配置區物件（目錄）需要它。

以下的範例說明了遍訪許可權的運作方式。在 ACME 公司中，有一個 *Engineering* 配置區物件（目錄），而它也包含了一個 *TechPubs* 配置區物件（子目錄）。**銷售**部門的成員**使用者 kate** 需遍訪 *Engineering/TechPubs* 目錄以便檢視版次注意事項檔。

管理者在 *Engineering* 和 *TechPubs* 目錄中放置了具有 **T** 許可權的 **sales 群組** ACL 登錄。雖然 Kate 對這兩個目錄沒有其他許可權，她可以通過（遍訪）這些目錄，以便存取 *release_note* 檔。因爲**使用者 kate** 有此檔的讀取許可權，她可以檢視該檔。

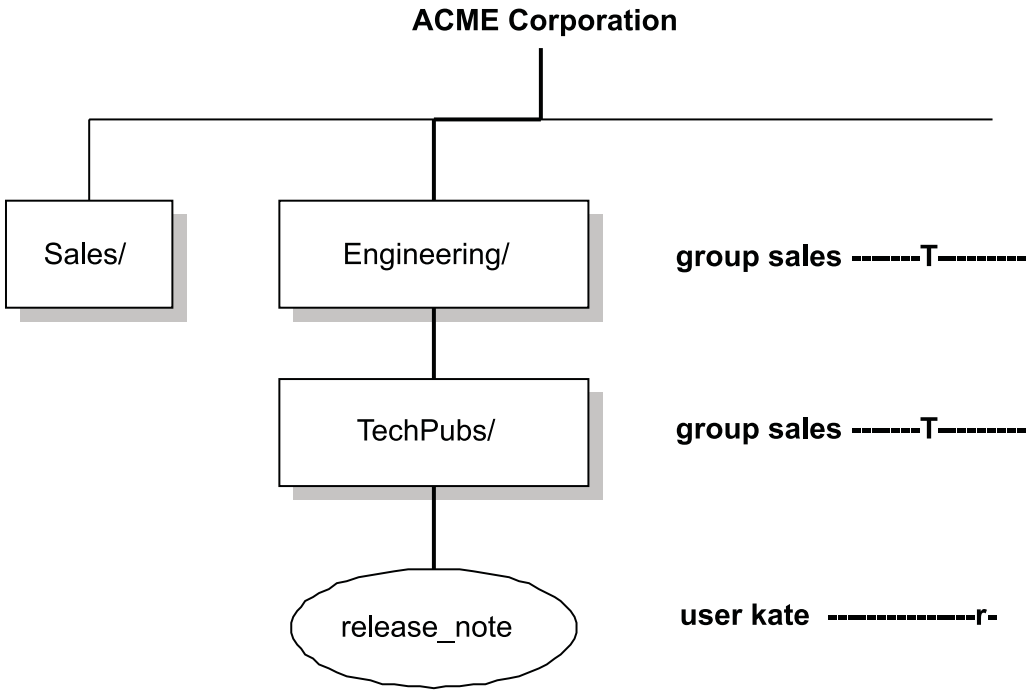

圖 1. 遍訪許可權

您可以輕鬆地將階層的存取權限制在指定的配置區物件—而不需要重設這些物件的個別許可權。您只需從適當的 ACL 登錄中移除遍訪許可權。不論那些物件是否包含了其他限制較少的 ACL，移除目錄物件的遍訪許可權可保護階層中較低的所有物件。

例如，如果 **sales 群組**沒有 *Engineering* 目錄的遍訪許可權，則不論 Kate 是否有該檔的讀取許可權，她都無法存取該版次注意事項檔案。

修正 WebSEAL 管理手冊

- 更新 WebSEAL for Dynamic URL (WebSEAL 6.3.3)
- WebSEAL 個人化接合 (WebSEAL 5.7)
- WebSEAL 僅支援 HTTP/1.0 橫跨接合
- GSKit 階段作業 ID 逾時參數

更新 WebSEAL for Dynamic URL (WebSEAL 6.3.3)

在 2001 年 1 月 *Tivoli SecureWay Policy Director WebSEAL 管理手冊* 的「6.3.3 節」中所陳述的，要在使用 **dynurlcp** 公用程式時找出 WebSEAL 伺服器的路徑名稱不正確。

將 **PolicyDirector** 目錄變更爲 **intraverse**：

```
dynurlcp -e /.:/subsys/intraverse/secmgr/server/<host> update
```

WebSEAL 個人化接合 (WebSEAL 5.7)

在 2001 年 1 月的 *Tivoli SecureWay Policy Director WebSEAL 管理手冊*的「5.7 節」中所指定爲 HTTP_PD_PORTAL 的 HTTP 標頭變數不正確。該變數爲 **PD_PORTAL**。

此外，「注意事項」的「5.7.2 節」中的第二個註解：

「在架構檔中將相同的後端 URL 對映至多個物件：許可權對，會造成一連串的物件清單」

是錯的。

WebSEAL 僅支援 HTTP/1.0 橫跨接合

*Tivoli SecureWay Policy Director WebSEAL 管理手冊*的「5.1.2 節」中的表格，包含了不正確的支援通信協定 RFC 號碼。以下的表格包含了正確的參照：

連線	支援的通信協定	RFC 號碼
前端（從屬站-至-WebSEAL）	HTTP/1.0 和 HTTP/1.1	RFC2068
後端（WebSEAL-至-接合的伺服器）	僅 HTTP/1.0	RFC1945

GSKit 階段作業 ID 逾時參數

2001 年 1 月的 *Tivoli SecureWay Policy Director WebSEAL 管理手冊*的「2.3 節」（「架構逾時值」）不正確地分類和定義了 **ssl-v2-timeout** 和 **ssl-v3-timeout** 參數。

這兩個參數不是 HTTP/HTTPS 連線的逾時參數。它們是用來定義 GSKit 階段作業 ID 快取中，階段作業 ID 生命週期的參數。這些參數中其一的值集和鑑別速率的組合，可以判斷 GSKit 階段作業快取被填滿的速度。這兩個參數是在 *secmgrd.conf* 架構檔中的 **[ssl]** 段落：

這些參數在 4.2 節「管理階段作業狀態」中有更詳盡的討論。

- **ssl-v2-timeout**

  對於 SSL v2 通信，此參數定義了階段作業 ID 會停留在 GSKit 階段作業快取中的時間長度。預設值爲 100（秒）。

- **ssl-v3-timeout**

  對於 SSL v3 通信，此參數定義了階段作業 ID 會停留在 GSKit 階段作業快取中的時間長度。預設值爲 7200（秒）。

修正 WebSEAL Developer Reference

- 部署範本 CDAS 伺服器（4.4 節）

部署範本 CDAS 伺服器（4.4 節）

註: 以下的資料說明了原始文件中的指示。此節和發展自訂的 CDAS 伺服器有關。

Tivoli SecureWay Policy Director WebSEAL Developer Reference 中經修改的「4.4 節」（「架構 WebSEAL 使用範本 CDAS 伺服器」）如下：

4.4.1 節

範本 CDAS 伺服器只是示範的程式碼。程式中已固定僅識別 **cdas_test** 使用者（密碼： “tivoli”），並且將此使用者對映至 Policy Director **test-user**。

1. 遵循原始的指示。
2. 遵循原始的指示。
3. 依照 **default-webseal** ACL 來建立測試的 ACL 原則。此 ACL 原則應包含測試使用者的登錄，並且授與 T、r 和 x 許可權。
4. 將此測試原則連接至 WebSEAL 物件空間中的部份物件。
5. 繼續「4.4.2 節」以便測試 CDAS 伺服器存取此受保護物件的能力。

4.4.2 節

1. 遵循原始的指示。
2. 使用下列來存取受保護的物件，以測試 CDAS 伺服器：

   使用者名稱：`cdas_test`

   密碼：`tivoli`
3. 範本 CDAS 伺服器應可成功地將此使用者對映至 **test_user** Policy Director 本身，並且讓您存取受保護的物件。

修正主控台管理手冊

■ 管理主控台管理手冊修正

管理主控台管理手冊修正

「管理主控台」線上說明系統包含了「主控台」說明文件的修正清單。

軟體限制

- SMP 系統不支援 NetSEAL 核心設陷
- NetSEAL 和 NetSEAT 的向後相容性
- 管理主控台無法使用 pdadmin 功能
- 對於雙位元組字元的語言限制
- LDAP 不對使用者名稱區分大小寫
- pdconfig 公用程式在日文 HP-UX 系統上可能無法運作
- 管理主控台線上說明不一致
- 已翻譯的主控台線上說明中使用了未翻譯的圖形

SMP 系統不支援 NetSEAL 核心設陷

SMP 系統不支援 NetSEAL 核心設陷。

在多重處理器的系統上架構 PDNet 時，請勿啓用核心設陷。

NetSEAL 和 NetSEAT 的向後相容性

NetSEAL 3.7 不能和前一版本的 NetSEAT 從屬站一同使用。

管理主控台無法使用 pdadmin 功能

以下的 Policy Director 3.7 功能存在於 **pdadmin** 公用程式，而不在「管理主控台」：

- 伺服器管理功能
- NetSEAL 管理
- ACL 動作/動作群組管理
- 物件空間和物件管理
- 密碼原則管理
- 授權管理功能
- 使用者和群組匯入指令

對於雙位元組字元的語言限制

當您在英文以外的環境中執行 Policy Director 時，適用於以下的限制和條件：

- 當在 Netscape 瀏覽器中使用「基本鑑別」來鑑別 WebSEAL 時，您必須在使用者名稱和密碼中使用可攜性字元集（7 位元 US-ASCII）。

  對於使用者名稱包含雙位元組字元的環境，請設定 WebSEAL 使用表單式登入，以便傳遞從屬站的本體資訊。

  當使用表單式登入時，用來建立表單的字碼頁必須與 WebSEAL 正在執行的字碼頁相同。

- 如果使用者資料包含了可攜性字元集（7 位元 US-ASCII）以外的字元，您必須確定所有的 Policy Director 元件是使用相同的字碼頁來執行，以便正常地在這些元件間共享資料。

- 當 Policy Director 是架構於英文以外的平台上，而且需要建立非可攜性字元集的資料時，只能使用 IBM SecureWay Directory 作爲使用者登錄。

- 當使用 junctioncp 公用程式來建立新接合時，接合點的名稱必須限制爲可攜性字元集。

  每個「亞洲」語言都有多個字碼集。HTTP 並不定義 URL 所要使用的字碼集。所以，若 URL 使用可攜性字碼集（7 位元 US-ASCII）以外的字元碼，則會導致相容性的問題。

LDAP 不對使用者名稱區分大小寫

此資訊適用於 IBM 和 Netscape LDAP。

Policy Director 會在 LDAP 登錄的 **secUser** 物件中，將使用者的名稱儲存於 **principalName** 屬性中。

LDAP 綱目將 **principalName** 定義爲區分大小寫的字串。然而，使用者名稱中所指示的原始大小寫會在將被儲存至 LDAP 資料庫時被保留。

因此，「Test User」會被視爲與「test user」相同。

pdconfig 公用程式在日文 HP-UX 系統上可能無法運作

如果您是使用 ja_JP.SJIS 語言環境或 ja_JP.eucJP 語言環境來登入系統，則在您嘗試架構 Policy Director 時，**pdconfig** 可能會無法執行。此問題的暫行解決方法爲使用「C」語言環境來登入至系統，然後使用「英文」來架構 Policy Director。

如果您使用此暫行解決方法，Policy Director 會在起始時認爲是在「C」語言環境中執行。在使用 ja_JP.SJIS 或 ja_JP.eucJP 語言環境來登出再登入系統後，Policy Director 應會停止，然後重新啓動以便能識別 ja_JP.SJIS（或 ja_JP.eucJP）語言環境。

此問題僅會出現在 HP-UX 系統上。

管理主控台線上說明不一致

「管理主控台」所提供的線上說明文件，和「主控台」本身顯示的實際畫面/標籤之間有部分不一致。

第一種類型的不一致是因爲在「主控台」的程式碼中，採用了最新的 Java swing 類別。線上說明中所使用的螢幕攫取（.gif 檔）是在該程式碼變更前所取得。因此變更所造成的畫面/標籤外觀上的變更相當小，並且應不會造成任何功能問題或困擾。

第二種類型的不一致是因爲「主控台」的程式碼基礎爲「元件管理程式」；它在 Tivoli 專案中是原始設計來作爲整合多種產品的管理主控台架構。「元件管理程式」所管理的每個產品都需要用來外掛至架構的轉換程式。線上說明中所顯示的部分功能畫面/標籤顯示了「元件管理程

式」架構的外掛程式能力。然而，「管理主控台」本身實際上是 Policy Director 轉換程式的結果，而且只能提供與 Policy Director 相關的功能。

已翻譯的主控台線上說明中使用了未翻譯的圖形

「管理主控台」線上說明（HTML 檔）以及程式碼所使用的訊息，已被翻譯爲九國語言。然而，已翻譯的線上說明中所使用的圖形，還未經過翻譯。目前是使用「英文」的圖形。

已知的軟體缺陷和暫行解決方法

- 安裝和升級的缺陷和暫行解決方法
- **Base** 的缺陷和暫行解決方法
- **WebSEAL** 的缺陷和暫行解決方法
- **NetSEAL** 的缺陷和暫行解決方法
- 管理主控台的缺陷和暫行解決方法
- **LDAP** 的缺陷和暫行解決方法

安裝和升級的缺陷和暫行解決方法

- 升級 Policy Director 3.6 WebSEAL
- IBM SecureWay Directory 3.2 需要 AIX 4.3.3 修補程式
- IBM SecureWay Directory DMT 公用程式無法啓動

升級 Policy Director 3.6 WebSEAL

註: 此問題發生在 Solaris、AIX 和 HP-UX 系統上。此問題不會發生在 Windows 系統。

問題：

當在升級 Policy Director 3.6 時架構 Policy Director 3.7 WebSEAL 伺服器，WebSEAL 伺服器可能會無法啓動。以下的錯誤訊息可能會出現：

```
symbol IV_URAF: 找不到參照的符號
```

說明：

如果在嘗試啓動 Policy Director 3.7 WebSEAL 伺服器時，還在執行任何 Policy Director 3.6 伺服器處理程序，新的 WebSEAL 伺服器可能會存取到快取在記憶體中的 Policy Director 3.6 共享程式庫。

Policy Director 3.6 共享程式庫中，未包含 Policy Director 3.7 WebSEAL 伺服器所需的所有程式庫常式。這會使新的 WebSEAL 伺服器無法啓動。

如果在嘗試啓動 Policy Director 3.7 WebSEAL 伺服器時，Policy Director 3.6 Authorization API Client 程式仍在執行中，則也會發生此問題。

暫行解決方法：

如果您在架構 Policy Director 3.7 WebSEAL 伺服器時遭遇此錯誤，請完成下列步驟：

1. 選取「x」來結束「Policy Director 架構功能表」。
2. 選取「x」來結束「Policy Director 設定功能表」。
3. 停止所有的 Policy Director 伺服器，以及使用 Policy Director 3.6 Authorization API 的從屬站程式。若要停止 Policy Director 伺服器，請輸入下列指令：

- AIX

```
# /etc/iv/iv stop
```

- Solaris

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

- HP-UX

```
# /sbin/init.d/iv stop
```

4. 請驗證已安裝了 Policy Director 3.6 授權程式庫，然後再移除它：

   - AIX

   ```
   # ls -l /usr/lib/libivauthzn.a
   # rm -f /usr/lib/libivauthzn.a
   ```

   - Solaris

   ```
   # ls -l /usr/lib/libivauthzn.so
   # rm -f /usr/lib/libivauthzn.so
   ```

   - HPUX

   ```
   # ls -l /usr/lib/libivauthzn.sl
   # rm -f /usr/lib/libivauthzn.sl
   ```

5. 使用新的 Policy Director 3.7 授權程式庫來建立符號鏈結：

   - AIX

```
# ln –s /opt/PolicyDirector/lib/libivauthzn.a /usr/lib/libivauthzn.a
```

   - Solaris

```
# ln –s /opt/PolicyDirector/lib/libivauthzn.so /usr/lib/libivauthzn.so
```

   - HPUX

```
# ln –s /opt/PolicyDirector/lib/libivauthzn.sl /usr/lib/libivauthzn.sl
```

6. 重新啓動 Policy Director 伺服器（以及任何 Authorization API 從屬站）：

- AIX

```
# /etc/iv/iv start
```

- Solaris

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

- HP-UX

```
# /sbin/init.d/iv start
```

7. 啓動 Policy Director 架構公用程式：

```
# pdconfig
```

8. 選取 **Policy Director 架構**。
9. 選取 **Policy Director WebSEAL (PDWeb) 架構**。
10. 按照提示，完成 WebSEAL 架構。

解決方案：

若要預防此問題的發生，請在準備將 Policy Director 3.6 系統升級至 Policy Director 3.7 時，手動停止 Policy Director 3.6 WebSEAL 伺服器。

請先備份 Policy Director 3.6 ACL 資料庫和 WebSEAL 接合資料庫後，再執行此動作。

註: 如果 Policy Director 3.6 系統中有 NetSEAL 伺服器，請在停止其他 Policy Director 3.6 伺服器前，先行移除 NetSEAL 伺服器。

若要停止 AIX 系統上的 WebSEAL 伺服器，請在 Shell 提示中輸入下列指令：

```
# /etc/iv/iv stop
```

若要停止 Solaris 系統上的 WebSEAL 伺服器，請在 Shell 提示中輸入下列指令：

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

若要停止 HP-UX 系統上的 WebSEAL 伺服器，請在 Shell 提示中輸入下列指令：

```
# /sbin/init.d/iv stop
```

IBM SecureWay Directory 3.2 需要 AIX 4.3.3 修補程式

問題：

只有在 AIX 系統上，IBM SecureWay Directory 3.2 才會因爲未安裝作爲先決條件的 AIX 作業系統軟體，而導致安裝失敗。

說明：

Policy Director 3.7 支援 LDAP 使用者登錄。Policy Director 使用者可以選擇安裝 IBM SecureWay Directory 3.2 版，來提供 LDAP 使用者登錄支援。Policy Director Base CD 包含了 SecureWay Directory 3.2 版。

只有在 AIX 上，SecureWay Directory 3.2 版才需要數個 AIX 作業系統修補程式；而在安裝 AIX 4.3.3 時，並未預設安裝這些檔案集。如果缺少了這些相關項目的任何一個，SecureWay Directory 3.2 版的安裝會失敗。

解決方案：

1. 在安裝 SecureWay Directory 3.2 版之前，請使用 **smit** 公用程式來驗證是否安裝了下列修補程式：
   - X11.Dt.lib 4.3.3.2
   - X11.Dt.rte 4.3.3.3
   - X11.adt.motif 4.3.3.1
   - X11.base.lib 4.3.3.2
   - X11.base.rte 4.3.3.2
   - X11.compat.lib.X11R5 4.3.3.2
   - X11.motif.lib 4.3.3.2
   - X11.motif.mwm 4.3.3.1
   - bos.adt.include 4.3.3.1
   - bos.adt.prof 4.3.3.3
   - bos.net.tcp.client 4.3.3.3

- bos.rte.libpthreads 4.3.3.3
- bos.sysmgt.serv_aid 4.3.3.2
- bos.mp 4.3.3.3
- bos.up 4.3.3.3

2. 使用 **smit** 來安裝任何缺少的修補程式。

IBM SecureWay Directory DMT 公用程式無法啓動

問題：

平台：僅 AIX

在使用者第一次架構 IBM SecureWay Directory 3.2 版時，「目錄管理程式 (DMT)」可能會無法啓動。此失敗會讓控制使用者登錄的 LDAP ACL 無法更新。此架構步驟會在 *Tivoli SecureWay Policy Director Base for AIX 安裝手冊*的「4.4.1 節」和「A.7.3 節」中說明。

說明：

DMT 公用程式是 IBM SecureWay Directory 3.2 版的一部分。Policy Director 3.7 Base for AIX CD 包含了 IBM SecureWay Directory。使用 LDAP 使用者登錄的 Policy Director 使用者通常會安裝 IBM SecureWay Directory 作爲 Policy Director 的必備軟體。

DMT 公用程式則視 AIX 4.3.3 作業系統檔案集 **X11.adt.lib** 而定。**X11.adt.lib** 檔案集則未包含在指定必備軟體相依關係（檔案集）的 SecureWay Directory **.TOC** 檔中。因此，不論是否缺少了軟體相依關係，IBM SecureWay Directory 3.2 版都會完成安裝。

解決方案：

1. 使用 **smit** 公用程式來安裝 AIX 4.3.3 檔案集 **X11.adt.lib**。
2. 重新啓動 DMT 公用程式。

Base 的缺陷和暫行解決方法

- 架構 Solaris 上的「管理伺服器」
- LDAP 3.1.x 至 LDAP 3.2 移轉程序修訂
- IBM DCE 3.1 修補程式 3 解決了「管理伺服器」的記憶體泄漏

架構 Solaris 上的「管理伺服器」

問題：

此問題僅針對 Solaris。當 LDAP 伺服器在相同主機時，架構爲 SSL 的「Policy Director 管理伺服器」(**ivmgrd**) 會無法啓動。

若要正常地透過 SSL 來鑑別，「管理伺服器」必須可以讀取 */opt/ibm/gsk4/bin/ldapsslclient.kdb* 金鑰資料庫檔。只有起始建立該檔的 **root** 使用者，才對此檔有讀取/寫入許可權。在啓動「管理伺服器」時，它會使用 **ivmgr** 使用者來執行。**ivmgr** 使用者無法讀取該檔。

暫行解決方法：

將 *ldapsslclient.kdb* 檔的所有權變更爲 **ivmgr** 使用者。

LDAP 3.1.x 至 LDAP 3.2 移轉程序修訂

此資訊是在討論現存 IBM SecureWay Directory (LDAP) 說明文件中，屬於 Policy Director 3.6 升級至 Policy Director 3.7 程序的問題。此處主要討論的議題爲保留 LDAP 綱目。

註: 此討論是基於 Windows NT 平台。然而，此議題和所說明的更正也適用於 UNIX 平台。

1. LDAP Server 3.2 版 Readme 文件指定了說明將 LDAP 3.1.1.5 移轉至 LDAP 3.2 的說明文件。
2. 此文件的標題爲 *Directory 3.2 安裝和架構手冊（Windows NT 版）*，而且位置在 IBM 支援網站：

   http://www-4.ibm.com/software/network/directory/library/
3. 請按下標題爲「安裝、架構和移轉」的節。完整的鏈結如下：

   http://www-4.ibm.com/software/network/directory/library/publications/ldap32in/wparent.htm

4. 請展開此節的目錄，然後按下「移轉」。
5. 向下捲動至標題爲「移轉現存綱目和保留的資料庫」的子節。在從 Policy Director 3.6 移轉至 3.7 時，此程序是必要的。
6. 「步驟 1」和「步驟 2」是正確的。停止 LDAP 和 DB2 案例。
7. 「步驟 5」並未提供關於停止複製的正確次序。

   它應也說明直接將 LDAP 3.2 覆蓋安裝在 3.1.1.5 上。
8. 步驟 6 之後的段落建議「綱目內容更新」。

   此結論與標題爲「移轉現存綱目和保留的資料庫」的節相衝突。事實上，Policy Director 在改變綱目後會無法運作。因此，下列的額外步驟是必要的（根據下列「從 V3.1 移轉至 V3.2」節中步驟 3 的複製指令」）：
9. 使用下列指令來復原綱目：

   ```
   MSDOS> copy
   <install_directory>\etc\ldapV31\V3.modifiedschema
   <install_directory>\etc
   ```
10. 使用 DMT 工具來驗證升級後的 LDAP 資料仍可使用。

備註：

- 此討論是針對 Windows。然而，UNIX 可能會有相同的問題。
- Solaris 平台上的資料必須手動儲存。

IBM DCE 3.1 修補程式 3 解決了「管理伺服器」的記憶體泄漏

問題：

下列問題可適用於同時在 Solaris 上使用 IBM DCE 3.1 的 Policy Director 3.7。

使用 **pdadmin** 或「管理主控台」等管理工具來修改原則，會導致「管理伺服器」(ivmgrd) 的記憶體泄漏。

解決方案：

安裝 IBM DCE 3.1 的修補程式可修復此記憶體泄漏。取得並且安裝 IBM DCE 3.1 的「修補程式 3 (IDCE31-03)」。

IBM DCE 軟體首頁：

http://www-4.ibm.com/software/network/dce/

修補程式集 3：

http://www-4.ibm.com/software/network/dce/support/patches/dce310/patchsummary_current.html

WebSEAL 的缺陷和暫行解決方法

- 額外的 WAP 閘道支援
- 已刪除的使用者證明仍在 WebSEAL 快取中
- CDSSO 的憑證鑑別造成 WebSEAL 發生問題

額外的 WAP 閘道支援

當您使用 WebSEAL 並且特別藉由其他的 Proxy 或閘道伺服器來通信時，您可以利用 WebSEAL 所支援的 HTTP over SSL 鑑別方法。

例如，當您要在 WAP 環境中提供授權服務時，此方法相當有用。

1. 請在 *iv.conf* 架構檔的 **[wand]** 段落中輸入下列的架構參數：

   ```
   use-http-auth-for-ssl = yes
   ```

2. 架構 **enable-http-auth-forms** 參數以便指定是否要使用「基本鑑別」或「表單式登入」。

   使用 *iv.conf* 架構檔中的 **[http-auth-headers]** 段落，來指定任何特別的 HTTP 標頭，作爲鑑別資料。

當您將 WebSEAL 設定爲此模式時，WebSEAL 會忽略 SSL 階段作業 ID，然後使用標準的 HTTP 階段作業管理機制。請參照 *Tivoli SecureWay Policy Director WebSEAL 管理手冊*，以取得關於這些鑑別機制的明細資訊。

已刪除的使用者證明仍在 WebSEAL 快取中

問題：

當您從使用者登錄（DCE 或 LDAP）刪除使用者時，WebSEAL 證明快取中的使用者證明（如果有的話）不會被移除。

註: 此快取的目的是限制使用者登錄的呼叫。

如果在刪除帳戶時，使用者有作用中的瀏覽器階段作業，基於未刪除的證明，使用者可以繼續瀏覽。

當刪除使用者時，只有登錄會受影響。在作用中的瀏覽器階段作業，如果有該使用者的合法證明，則不會查詢登錄。登錄查閱（以反映刪除的帳戶）只會在新的登入或目前的證明到期時，才會發生。

暫行解決方法：

在使用者登出瀏覽器階段作業後，快取中的證明會被清除。

如果您是安全管理者，而且需要立刻停止安全網域中的使用者活動，您可以在特定使用者的預設 WebSEAL ACL 原則中加入項目，以移除遍訪 (T) 許可權。

CDSSO 的憑證鑑別造成 WebSEAL 發生問題

問題：

如果在 CDSSO 環境中，從屬站透過從屬站端的憑證來進行對網域 A 的鑑別，然後啓動對網域 B 的鏈結，則記憶體泄漏會使 **secmgrd** (WebSEAL) 程序過度成長。

暫行解決方法：

要使用 CDSSO 功能的從屬站不應透過從屬站端的憑證來鑑別起始網域。例如，「基本鑑別」和「表單式登入」都是可接受的鑑別方法。

請查詢「Tivoli 支援中心」來取得修正套件，以便容許透過從屬站端憑證來鑑別。

NetSEAL 的缺陷和暫行解決方法

- AIX 設陷缺陷
- Solaris 修補程式基本要求

AIX 設陷缺陷

AIX 核心設陷有一個明顯的缺陷。您不能將 NetSEAL 架構來對暫時埠設陷（例如，1025 至 5000 範圍中的埠）。

如果您將 NetSEAL 架構來對暫時埠設陷，所有的外送網路連線都會失效，而使得伺服器失去效用。

Solaris 修補程式基本要求

NetSEAL 設陷需要 Solaris 的最新 O/S 修補程式。

O/S 修補程式位於：

http://sunsolve.Sun.COM

請查看 Sunsolve 中的內容：「Recommended and Security patches」。

管理主控台的缺陷和暫行解決方法

■ 管理主控台的缺陷和暫行解決方法

管理主控台的缺陷和暫行解決方法

當您執行 Policy Director 管理主控台（Windows 版）時，以下的限制和條件均適用：

- 對於 LDAP 使用者登錄，「帳戶管理程式」不能複製和貼上來自「使用者」配置區，或自現行群組移動至其他群組的使用者。

  暫行解決方法爲拖放使用者。

- 對於 LDAP 登錄，在「建立 GSO 資源群組」或「GSO 群組內容」檢視畫面中，按下 「...」按鈕所出現的「帳戶管理程式」檢視畫面，應會帶出「GSO 資源」檢視畫面。然而，「GSO 資源」檢視畫面不會列出任何資源。

  此問題的暫行解決方法爲從「GSO 資源」配置區中拖放資源。

- 對於 DCE 登錄，在帶出「許可權」檢視畫面時，DCE SecRgy 檢視畫面會使「主控台」跳出。請用滑鼠右鍵點選「群組」或「Principals」，然後按下「新增」，則也會使「主控台」跳出。

  此外，部份說明文件有缺少或尚未更新（品牌未更新）。

- 您需選取配置區物件，才能使「重新整理」按鈕生效。否則，將不會執行任何重新整理的動作。

- 對於 DCE 登錄，「項目」和「物件」標籤與「編輯 Principal」視窗中的相同。

- 「帳戶管理程式」檢視畫面中的「物件」下拉功能表應已停用。它不提供此檢視畫面中的任何功能表選項。它先前僅是列出不支援的「自訂指令」選項，而且已被移除。

- 在「物件空間」檢視畫面中將 ACL 或 POP 連接至物件，或分離 ACL 與物件時，「主控台」會沒有回應。該動作則應已成功完成。此無回應問題的暫行解決方法爲重新啓動「主控台」。

- 「主控台」有時會在啓動時立刻跳出。暫行解決方法爲登入然後再次登入。

- 「主控台」必須重新啓動，才能察覺動作群組的變更（例如，新增或移除許可權位元）。
- 如果重新架構 PDRTE 來使用不同的使用者登錄類型（例如，從 DCE 使用者登錄切換至 LDAP 使用者登錄）時，「主控台」必須重新安裝。

LDAP 的缺陷和暫行解決方法

- 在架構 LDAP 時，WebSEAL 會變得不穩定

在架構 LDAP 時，WebSEAL 會變得不穩定

背景：

對於 IBM LDAP，Policy Director 透過 *iv.conf* 架構檔中，**[ldap]** 段落的 **auth-using-compare** 參數，來提供增進鑑別效能的選項。

此選項對 Netscape LDAP 沒有作用，WebSEAL 會因此而忽略它。此參數的說明文件在 *Tivoli SecureWay Policy Director Performance Tuning Guide* 中的「4.2 節」。

auth-using-compare 的預設值爲「yes」。對於 IBM LDAP，WebSEAL 可以使用此參數並且按照預期來執行。

問題：

然而，當在 IBM LDAP 中將 **auth-using-compare** 設定爲 「no」時，WebSEAL 會因爲沉重的鑑別負荷而變得不穩定。

此外，當 Policy Director 架構了 Netscape LDAP，不論是否忽略 **auth-using-compare** 參數，相同的缺陷會使 WebSEAL 因爲沉重的鑑別負荷而變得不穩定。

相同的問題會影響 Policy Director 所使用的 IBM LDAP 從屬站。

暫行解決方法：

請勿對 IBM LDAP 將 **auth-using-compare** 設定爲「no」。

對於 Netscape LDAP 則沒有暫行解決方法。

修補程式下載將會盡快提供給您。

讀者意見表

爲使本書盡善盡美，本公司極需您寶貴的意見；懇請您使用過後，撥冗填寫下表，惠予指教。

請於下表適當空格內，填入記號（∨）；我們會在下一版中，作適當修訂，謝謝您的合作!

評估項目	評　估　意　見		備　註
正確性	內容說明與實際程序是否符合	□是□否	
	參考書目是否正確	□是□否	
一致性	文句用語及風格，前後是否一致	□是□否	
	實際畫面訊息與本書所提之畫面訊息是否一致	□是□否	
完整性	是否遺漏您想知道的項目	□是□否	
	字句、章節是否有遺漏	□是□否	
術語使用	術語之使用是否恰當	□是□否	
	術語之使用，前後是否一致	□是□否	
可讀性	文句用語是否通順	□是□否	
	有否不知所云之處	□是□否	
內容說明	內容說明是否詳盡	□是□否	
	例題說明是否詳盡	□是□否	
排版方式	本書的形狀大小，版面安排是否方便使用	□是□否	
	字體大小，顏色編排，是否有助於閱讀	□是□否	
目錄索引	目錄內容之編排，是否便於查考	□是□否	
	索引語錄之排定，是否便於查考	□是□否	
	※評估意見爲"否"者，請於備註欄說明。		

其他：（篇幅不夠時，請另紙說明。）

上述改正意見，一經採用，本公司有合法之使用及發佈權利，特此聲明。

Policy Director
版次注意事項

GI10-6374-00

讀者意見表

寄

台北市115南港區三重路十九之十一號E棟九樓

折疊線

大臺灣國際商業機器股份有限公司
中華研發中心
軟體國際部
啟

寄件人
姓名：
地址：

免貼郵票

廣告回信
台灣北區郵政管理局
登記證
北台字第　號

折疊線

Printed in Australia

GI10-6374-00