Sun Java System Web Proxy Server 4.0.8 管理指南

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

文件號碼：820–6318
2008 年 8 月

目錄

前言

本指南說明如何配置及管理 Sun Java ™ System Web Proxy Server 4，原稱爲 Sun ONE™ Web Proxy Server 與 iPlanet™ Web Proxy Server (以下通稱爲 Sun Java System Web Proxy Server 或簡稱爲 Proxy Server)。

本書適用對象

本書適用於生產環境下的資訊技術管理員。本指南假定讀者已熟悉下列領域的知識：

- 執行基本的系統管理作業
- 安裝軟體
- 使用 Web 瀏覽器
- 在終端機視窗中發出指令

閱讀本書之前

Sun Java System Web Proxy Server 可以單獨購買或當做 Sun Java Enterprise System (一種軟體基礎架構，可支援分布於網路或網際網路環境上的企業應用程式) 的一個元件來購買。如果當做 Java Enterprise System 的一個元件來購買 Sun Java System Web Proxy Server，請仔細閱讀 `http://docs.sun.com/coll/1286.2` 與 `http://docs.sun.com/coll/1412.2` 上的系統文件。

本書架構

本指南劃分爲若干部分，每一部分探討特定的領域及作業。下表列出本指南的編排及其內容。

表 P–1 指南架構

部分	說明

表 P–1 指南架構 (續)

第 1 部分 伺服器基本知識	提供 Proxy Server 的簡介及其管理： ■ 第 1 章「介紹 Sun Java System Web Proxy Server」 ■ 第 2 章「管理 Sun Java System Web Proxy Server」
第 2 部分 使用 Administration Server	詳細說明如何配置 Administration Server 喜好設定、管理使用者和群組、保護 Proxy Server 的安全，以及使用叢集讓伺服器共用配置： ■ 第 3 章「設定管理喜好設定」 ■ 第 4 章「管理使用者和群組」 ■ 第 5 章「使用憑證和金鑰」 ■ 第 6 章「管理伺服器叢集」
第 3 部分 配置及監視 Proxy Server	詳細說明如何配置伺服器喜好設定、設定存取控制以及監視伺服器作業： ■ 第 7 章「配置伺服器喜好設定」 ■ 第 8 章「控制對伺服器的存取」 ■ 第 9 章「使用記錄檔」 ■ 第 10 章「監視伺服器」
第 4 部分 管理 Proxy Server	詳細說明 Proxy Server 處理請求的相關概念及作業： ■ 第 11 章「代理及路由 URL」 ■ 第 12 章「快取」 ■ 第 13 章「透過代理伺服器篩選內容」 ■ 第 14 章「使用反向代理伺服器」 ■ 第 15 章「使用 SOCKS」 ■ 第 16 章「管理範本和資源」 ■ 第 17 章「使用用戶端自動配置檔案」
第 5 部分 附錄	說明存取控制清單 (ACL) 檔案語法及調校伺服器效能： ■ 第 18 章「ACL 檔案語法」 ■ 第 19 章「調校伺服器效能」

Proxy Server 文件集

此文件集列出與 Proxy Server 相關的 Sun 文件。Proxy Server 文件的 URL 爲 `http://docs.sun.com/coll/1311.8`。如需 Proxy Server 的簡介，請按照表格中列出的順序參閱這些書籍。

表 P–2 Sun Java System Web Proxy Server 文件

文件標題	內容
「Sun Java System Web Proxy Server 4.0.8 版本說明」	Proxy Server 發行版本： ■ 有關軟體和說明文件的最新資訊 ■ 新增功能 ■ 支援的平台及環境 ■ 系統需求 ■ 已知問題及解決方法
「Sun Java System Web Proxy Server 4.0.8 Installation and Migration Guide」	執行安裝和遷移工作： ■ 安裝 Sun Java System Web Proxy Server ■ 從版本 3.6 遷移至版本 4
「Sun Java System Web Proxy Server 4.0.8 管理指南」	執行管理作業： ■ 使用管理介面及指令行介面 ■ 配置伺服器喜好設定 ■ 管理使用者及群組 ■ 監視並記錄伺服器狀態 ■ 使用憑證及公開金鑰加密來保護伺服器 ■ 控制伺服器存取 ■ 代理及路由 URL ■ 快取 ■ 篩選內容 ■ 使用反向代理伺服器 ■ 使用 SOCKS
「Sun Java System Web Proxy Server 4.0.8 Configuration File Reference」	編輯配置檔案
「Sun Java System Web Proxy Server 4.0.8 NSAPI Developer's Guide」	建立自訂 Netscape Server 應用程式設計介面 (NSAPI) 外掛程式

相關書籍

Sun Java Enterprise System (Java ES) 及其元件的所有相關文件的 URL 爲 `http://docs.sun.com/prod/entsys.5` 與 `http://docs.sun.com/prod/entsys.5?l=zh_TW`。

預設路徑及檔案名稱

下表說明本書所使用的預設路徑及檔案名稱。

表 P–3 預設路徑及檔案名稱

預留位置	說明	預設值
install-dir	代表 Sun Java System Web Proxy Server 的基底安裝目錄。	Solaris 及 Linux 安裝：/opt/sun/proxyserver40 Windows 安裝：\Sun\ProxyServer40

印刷排版慣例

下表描述本書中所使用的印刷排版慣例。

表 P–4 印刷排版慣例

字體	意義	範例
`AaBbCc123`	指令、檔案及目錄的名稱；螢幕畫面輸出。	請編輯您的 `.login` 檔案。 請使用 `ls -a` 列出所有檔案。 **電腦名稱**`% you have mail.`
`AaBbCc123`	您所鍵入的內容 (與螢幕畫面輸出相區別)。	**電腦名稱**`% su` `Password:`
`AaBbCc123`	新的字彙或術語、要強調的詞。將用實際的名稱或數值取代的指令行變數。	要刪除檔案，請鍵入 `rm` **檔案名稱**。 **快取**是儲存在本機上的副本。 **不**儲存檔案。
AaBbCc123	保留未譯的新的字彙或術語、要強調的詞。	應謹慎使用 *On Error* 指令。
「AaBbCc123」	用於書名及章節名稱。	請參閱「使用者指南」中的第 6 章。

指令範例中的 Shell 提示符號

下表顯示了預設的系統提示符號和超級使用者提示符號。

表 P–5 Shell 提示符號

Shell	提示符號
UNIX 和 Linux 系統上的 C shell	**電腦名稱**%
UNIX 和 Linux 系統上的 C shell 超級使用者	**電腦名稱**#
UNIX 和 Linux 系統上的 Bourne shell 與 Korn shell	$
UNIX 和 Linux 系統上的 Bourne shell 與 Korn shell 超級使用者	#
Microsoft Windows 指令行	C:\

符號慣例

下表說明本書可能使用的符號。

表 P–6 符號慣例

符號	說明	範例	意義
[ ]	包含選擇性引數與指令選項。	ls [-l]	-l 選項不是必需的。
{ | }	包含所需指令選項的一組選擇。	-d {y|n}	-d 選項需要您使用 y 引數或是 n 引數。
${ }	指出變數參照。	${com.sun.javaRoot}	參照 com.sun.javaRoot 變數的值。
-	結合多個同步按鍵。	Ctrl-A	按下 Control 鍵同時按住 A 鍵。
+	結合多個連續按鍵。	Ctrl+A+N	按下 Control 鍵、放掉然後再按下後續的鍵。
→	指出圖形化使用者介面中的功能表項目選項。	[檔案] → [新增] → [範本]	從 [檔案] 功能表選擇 [新增]。從 [新增] 子功能表選擇 [範本]。

文件、支援與培訓

Sun 網站提供了下列附加資源的相關資訊：

- 文件 (http://www.sun.com/documentation/)
- 支援 (http://www.sun.com/support/)
- 培訓 (http://www.sun.com/training/)

搜尋 Sun 產品文件

除了從 docs.sun.com℠ 網站搜尋 Sun 產品文件外，還可藉由在搜尋欄位中鍵入下列語法來使用搜尋引擎：

search-term `site:docs.sun.com`

例如，若要搜尋「broker」，請鍵入下列語法：

```
broker site:docs.sun.com
```

若要將其他 Sun 網站納入您的搜尋中 (例如，java.sun.com、www.sun.com 與 developers.sun.com)，請在搜尋欄位中用 `sun.com` 取代 `docs.sun.com`。

協力廠商網站參照

本文件提供了協力廠商的 URL 及其他相關資訊做爲參照。

備註 – Sun 對於本文件中所提及之協力廠商網站的使用不承擔任何責任。Sun 對於此類網站或資源中的 (或透過它們所取得的) 任何內容、廣告、產品或其他材料不做背書，也不承擔任何責任。對於因使用或依靠此類網站或資源中的 (或透過它們所取得的) 任何內容、產品或服務而造成的或連帶產生的實際或名義上之損壞或損失，Sun 概不負責，也不承擔任何責任。

Sun 歡迎您提出寶貴意見

Sun 致力於提高文件品質，因此誠心歡迎您提出意見與建議。若要提出您的意見，請至 `http://docs.sun.com` 並按一下 [傳送您的意見] (Send Comments)。請在線上表單中提供完整的文件標題與文件號碼。文件號碼位於書本的標題頁或文件的 URL 中，通常是一組 7 位或 9 位數的數字。例如，本書的文件號碼爲 820-6318。提出意見時您還需要在表格中輸入此文件的英文標題和文件號碼。例如，本文件的英文文件號碼爲 820-5723，完整標題爲「Sun Java System Web Proxy Server 4.0.8 Administration Guide」。

◆ ◆ ◆ 第 1 章

介紹 Sun Java System Web Proxy Server

本章提供 Sun Java System Web Proxy Server 的一般簡介，包括本發行版本新增功能的簡要說明，以及網路型使用者介面 (可用來管理、配置 Proxy Server) 的簡介。

本章包含下列小節：

關於 Sun Java System Web Proxy Server

在高效能網際網路和企業內部網路環境中，Sun Java System Web Proxy Server 代表 HTTP 快取和加速基礎。Proxy Server 爲可快取、篩選 Web 內容並提高網路效能的系統，同時提供與整個網路基礎架構的整合、跨平台支援以及集中管理的功能。它扮演網路流量管理員的角色，能有效分散和管理資訊，以縮短網路流量和使用者的等待時間。Proxy Server 同時也爲內容發行提供安全閘道，並充當網際網路流量的控制點，確保使用者能安全並有效的存取網路資源。

本發行版本的新功能

Sun Java System Web Proxy Server 4 包含下列增強功能：

- 現代型 HTTP 核心
- 支援 Linux 和 Solaris™ x86 平台
- 支援所有平台上的現代型 SSL (安全通訊端層)
- 所有平台上的多重執行緒架構
- 改良過的管理、圖形化使用者介面以及簡易的管理
- 新的 NSAPI (Netscape 伺服器應用程式設計介面) 篩選器
- 提高 LDAP (簡易目錄存取協定) 效能
- 改善延展性與效能

- 改善內容篩選
- `server.xml` 配置檔案的實作

如需有關新功能和增強功能的資訊，請參閱「Sun Java System Web Proxy Server **版本說明**」，網址是：`http://docs.sun.com/coll/1311.8`。

入門

Sun Java System Web Proxy Server 的管理和配置，是透過 Administration Server 和 Server Manager 的網路型使用者介面來進行。系統所安裝之所有 Proxy Server 實例的共用配置由 Administration Server 管理，而 Server Manager 則用來配置各個伺服器實例的設定。

本小節包含以下主題：

- 第 26 頁的 「Administration Server 簡介」
- 第 27 頁的 「Server Manager 簡介」
- 第 28 頁的 「配置檔案」
- 第 29 頁的 「常規表示式」

備註 – 您必須啓用瀏覽器中的 Cookie，才能執行配置伺服器所必需的 CGI 程式。

Administration Server 簡介

Administration Server 爲網路型使用者介面，可用來管理系統上所有已安裝 Sun Java System Web Proxy Server 實例共用的配置。

Administration Server 啓動之後，只要啓動瀏覽器並輸入 URL 就能加以存取。URL 是由安裝期間所指定之主機名稱和連接埠號所決定，例如，
`http://myserver.mycorp.com:1234`。

可以對一名以上的管理員授予管理伺服器的存取權。如需有關分散式管理的更多資訊，請參閱第 38 頁的 「允許多個管理員」。

Administration Server 設定依標籤分門別類，每個標籤對應到特定作業。下表列出 Administration Server 的標籤，後面跟著各標籤可執行作業的簡短說明。

- Servers - 管理、增加、移除、遷移 Proxy Server
- Preferences - 關閉 Administration Server、編輯偵聽通訊端、配置超級使用者存取、配置允許多名管理員的分散式管理、自訂並檢視存取和錯誤記錄
- Global Settings - 配置目錄服務、指定存取控制、配置 SNMP 主代理程式設定
- Users and Groups - 增加並管理使用者、群組和組織單位
- Security - 建立新的信任資料庫、請求並安裝 VeriSign 和其他憑證、變更金鑰對檔案密碼、檢視並管理已安裝憑證、增加或替代憑證撤銷清單 (CRL) 和洩漏金鑰清單 (CKL)、管理 CRL 和 CKL、遷移 3.x 憑證

- Cluster - 控制叢集中的遠端伺服器、增加和移除遠端伺服器、修改伺服器資訊

不論您所在的標籤或頁面爲何，下列按鈕也會顯示出來：

- Version - 顯示有關 Sun Java System Web Proxy Server 的版本資訊
- Refresh - 重新整理目前頁面
- Help - 顯示目前頁面的線上說明

▼ 存取 Administration Server

1 **啓動瀏覽器，並前往反映出 Administration Server 在安裝期間所指定主機名稱和連接埠號的 URL，例如，**`http://myserver.mycorp.com:1234`

2 **當出現提示時，請鍵入安裝期間所指定的使用者名稱和密碼。**

這時會顯示 Administration Server 的使用者介面。

如需有關 Administration Server 的更多資訊，請參閱第 2 章「管理 Sun Java System Web Proxy Server」。另請參閱 Administration Server 標籤和頁面的線上說明。

Server Manager 簡介

Server Manager 爲網路型使用者介面，用於啓動、停止和配置 Sun Java System Web Proxy Server 的個別實例。

Server Manager 設定依標籤分門別類，每個標籤對應到特定作業。以下是 Server Manager 標籤的清單，以及各標籤可執行作業的簡短說明。

- Preferences - 啓動和停止伺服器、檢視伺服器設定、復原配置資訊、配置系統喜好設定、調校 Proxy Server 效能、增加並編輯偵聽通訊端、管理 MIME 類型、管理存取控制、配置 ACL 和 DNS 快取、配置 DNS 本機子網域、配置 HTTP 持續作用設定、設定密碼大小
- Routing - 啓用和停用代理、設定路由喜好設定、轉寄用戶端憑證、啓用 Java IP 位址檢查、建立和編輯自動配置檔案、設定連結模式、變更預設的 FTP 傳輸模式、設定 SOCKS 名稱伺服器 IP 位址、配置 HTTP 請求負載平衡
- SOCKS - 啓動和停止 SOCKS 伺服器、建立並管理 SOCKS 認證、連線和路由項目
- URLs - 檢視、建立並管理 URL 對映和重新導向
- Caching - 設定快取明細、增加和修改快取分割區、在現有分割區間移動區段、設定快取容量、設定資源回收模式、調校快取、排程資源回收、調校資源回收設定、配置特定資源的快取、啓用本地主機的快取、變更檔案快取設定、設定快取批次更新、檢視有關已記錄快取 URL 的資訊、在 ICP 鄰近區域配置代理伺服器、建立和更新代理伺服器陣列成員清單、配置代理伺服器陣列成員、檢視 PAT 檔案中的資訊
- Filters - 建立篩選器檔案、設定內容 URL 重寫、設定使用者代理程式限制和請求阻斷、不列印外寄標頭、設定 MIME 篩選器和 HTML 標記篩選器、視需要壓縮內容

- Server Status - 檢視記錄檔、歸檔記錄、設定記錄喜好設定、產生報告、監視目前的作業、配置並控制 SNMP 子代理程式
- Security - 建立新的信任資料庫、請求並安裝 VeriSign 和其他憑證、變更金鑰對檔案密碼、檢視並管理已安裝憑證、增加或替代憑證撤銷清單 (CRL) 和洩漏金鑰清單 (CKL)、管理 CRL 和 CKL、遷移 3.x 憑證
- Templates - 建立、移除、套用和檢視範本，以及移除資源

不論您所在的標籤或頁面爲何，下列按鈕也會顯示出來：

- Version - 顯示和 Sun Java System Web Proxy Server 相關的版本資訊
- Refresh - 重新整理目前頁面
- Help - 顯示目前頁面的線上說明

  有時在 [Refresh] 按鈕底下，您可能還會看到 [Restart Required] 連結。這個連結表示已完成變更，因此伺服器需要重新啓動。若要套用變更，請按一下連結並指定所需要的動作。

  如需有關使用 Server Manager 的更多資訊，請參閱本指南的相關作業。另請參閱 Server Manager 標籤和頁面的線上說明。

▼ 存取 Server Manager

1 **請依照第 26 頁的 「Administration Server 簡介」所述來存取 Administration Server。**
Administration Server 會出現在 [Servers] 標籤上。

2 **在 [Manage Servers] 頁面上，按一下您要管理的伺服器實例連結。**
這時會出現 Server Manager 使用者介面。

配置檔案

Sun Java System Web Proxy Server 的配置和運作方式是由一組配置檔案所決定。在管理介面中配置的設定會反映在配置檔案中。這些檔案也能以手動方式加以編輯。

配置檔案位於 *instance-dir*/`config` 目錄，其中 *instance-dir* 是伺服器實例。`config` 目錄包含用來控制不同元件的各種配置檔案。配置檔案的數量和名稱視所啓用或載入的元件而定。這個目錄總是包含伺服器作業所需要的四個配置檔案。下表列出這四個必要的配置檔案及其內容。

表 1–1 必要的配置檔案

檔案	內容
`server.xml`	大部分的伺服器配置 (此 Proxy Server 發行版本的新增內容)

表 1–1 必要的配置檔案 (續)

檔案	內容
magnus.conf	全域伺服器初始化資訊
obj.conf	處理用戶端請求的相關說明
mime.types	決定所請求資源內容類型的資訊

如需有關這些檔案和其他配置檔案的詳細資訊，請參閱「Proxy Server 4.0.4 *Configuration File Reference*」。

常規表示式

您可以使用常規表示式來識別資源並對 Proxy Server 進行配置，以不同的方式處理來自不同 URL 的請求。您可以在使用 Administration Server 和 Server Manager 使用者介面執行各種作業時，指定常規表示式。如需有關常規表示式使用方式的詳細資訊，請參閱第 16 章「管理範本和資源」。

◆ ◆ ◆ 第 2 章

2 管理 Sun Java System Web Proxy Server

本章介紹使用 Administration Server 管理 Sun Java System Web Proxy Server 的基本事項。Administration Server 是一種網路型使用者介面，用來管理、增加、移除及遷移伺服器。

本章包含下列小節：

如需有關配置 Administration Server 喜好設定的詳細資訊，請參閱第 3 章「設定管理喜好設定」。如需有關使用伺服器叢集管理多個 Proxy Server 的詳細資訊，請參閱第 6 章「管理伺服器叢集」。

啓動 Administration Server

本小節說明如何在不同的平台上啓動 Administration Server。如需有關停止 Administration Server 的資訊，請參閱第 32 頁的「停止 Administration Server」。

在 UNIX 或 Linux 上啓動 Administration Server

1. 從指令行移至 *server-root*/`proxy-admserv`
2. 鍵入 `./start` 以啓動 Administration Server (或鍵入 `./restart` 以重新啓動 Administration Server)。

在 Windows 上啓動 Administration Server

您可以在 Windows 上用以下任何方式啓動 Administration Server：

- 使用 [開始] -> [程式集] -> [Sun Microsystems] -> [Sun Java System Web Proxy Server *version*] -> [Start Admin]
- 使用 [控制台] -> [系統管理工具] -> [服務] -> [Sun Java System Web Proxy Server 4.0 Administration Server] -> [啓動]
- 從指令提示符號處移至 *server-root* `\proxy-admserv` 並鍵入 `startsvr.bat` 以啓動 Administration Server (或鍵入 `./restart` 以重新啓動 Administration Server)。

啓動 Administration Server 後，您可以啓動瀏覽器並輸入 URL (裡面包含安裝期間爲 Administration Server 指定的主機名稱和連接埠號，例如 `http://myserver.mycorp.com:1234`) 以存取 Administration Server。系統將提示您輸入使用者名稱和密碼，此兩者也是在安裝期間指定的。

可以對一名以上的管理員授予管理伺服器的存取權。如需有關分散式管理的更多資訊，請參閱第 38 頁的 「允許多個管理員」。

停止 Administration Server

本小節說明如何在不同的平台上停止 Administration Server。如需有關啓動 Administration Server 的資訊，請參閱第 31 頁的 「啓動 Administration Server」。

在 UNIX 或 Linux 上停止 Administration Server

在 UNIX 或 Linux 上，您可以用以下兩種方式之一停止 Administration Server：

- 使用管理介面：
  1. 存取 Administration Server。
  2. 選取 [Preferences] 標籤。
  3. 按一下 [Shutdown Server] 連結。
  4. 按一下 [OK]。
- 從指令行移至 *server-root*/ `proxy-admserv/` 並鍵入 `./stop`。

在 Windows 上停止 Administration Server

在 Windows 上，您可以使用以下兩種方式之一停止 Administration Server：

- 使用 [Services] 視窗中的 Sun Java System Proxy Server 4.0 Administration Server 服務：[控制台] -> [系統管理工具] -> [服務] -> [Sun Java System Web Proxy Server 4.0 Administration Server] > [停止]

- 從指令提示符號處移至 *server-root* \proxy-admserv 並鍵入 stopsvr.bat。

執行多個 Proxy Server

若要在您的系統中執行多個 Proxy Server，必須安裝及配置多個伺服器實例。以下程序說明如何增加伺服器實例。

▼ 安裝多個伺服器實例

1. **存取 Administration Server。**
2. **在 [Servers] 標籤中按一下 [Add Server]。**
3. **輸入需要的資訊，然後按一下 [OK]。**
   如需有關特定欄位的更多資訊，請參閱線上說明。
4. **請視需要，在成功增加新的伺服器實例後顯示的 [Success] 頁面上，按一下 [Configure Your New Server] 連結。**
   此時會出現 Server Manager 介面。您可以使用此介面來配置伺服器實例。

移除伺服器實例

可以使用 Administration Server 移除 Proxy Server 實例。此程序無法還原，因此在執行以下程序之前，請確定您的確要移除此伺服器實例。

▼ 移除伺服器實例

1. **存取 Administration Server。**
2. **在 [Servers] 標籤中按一下 [Remove Server]。**
3. **從下拉式清單中，選取要移除的伺服器實例。**
4. **選取 [Confirming Server Removal] 核取方塊並按一下 [OK]。**

從 Proxy Server 3.6 遷移

Sun One Web Proxy Server 3.6 (亦稱爲 iPlanet Web Proxy Server) 可以遷移至 Sun Java System Web Proxy Server 4。此動作會保留 3.6 版伺服器，並建立具有相同設定的第 4 版新伺服器。如需有關將伺服器從版本 3.6 遷移至版本 4 的更多資訊，請參閱「Sun Java System Web Proxy Server 4.0.8 Installation and Migration Guide」。另請參閱 Proxy Server 使用者介面中與遷移相關之頁面的線上說明。如需有關遷移憑證的資訊，請參閱本指南中的第 76 頁的 「遷移先前版本的憑證」。

◆ ◆ ◆ 第 3 章

3 設定管理喜好設定

本章說明如何 Administration Server 配置管理喜好設定。必須在您的瀏覽器中啓用 Cookie，才能執行配置伺服器所需的 CGI 程式。

本章包含下列小節：

建立和管理偵聽通訊端

偵聽通訊端必須先接受請求，再導向至正確的伺服器，然後伺服器才能處理請求。安裝 Proxy Server 時，會自動建立一個偵聽通訊端 (`ls1`)。此偵聽通訊端會使用 IP 位址 `0.0.0.0`，及安裝時指定做爲 Administration Server 連接埠號的相同連接埠號。

可使用 Administration Server 的 [Edit Listen Sockets] 頁面來增加、編輯和刪除偵聽通訊端。您至少必須有一個偵聽通訊端用於存取伺服器。如果這是列出的唯一一個偵聽通訊端，則不能將其刪除。

本小節將說明如何增加、編輯和刪除偵聽通訊端。

▼ 增加偵聽通訊端

1. **存取 Administration Server，然後按一下 [Preferences] 標籤。**
2. **按一下 [Edit Listen Sockets] 連結。**

3. **按一下 [New] 按鈕。**
4. **指定設定，然後按一下 [OK]。**
   如需有關特定欄位的更多資訊，請參閱線上說明。

▼ 編輯偵聽通訊端

1. **存取 Administration Server，然後按一下 [Preferences] 標籤。**
2. **按一下 [Edit Listen Sockets] 連結。**
3. **按一下要編輯的偵聽通訊端之連結。**
4. **進行所需的變更，然後按一下 [OK]。**

▼ 刪除偵聽通訊端

1. **存取 Administration Server，然後按一下 [Preferences] 標籤。**
2. **按一下 [Edit Listen Sockets] 連結。**
3. **選取要刪除的偵聽通訊端旁邊的核取方塊，然後按一下 [OK]。**
4. **出現確認刪除的提示時，按一下 [OK]。**
   您至少必須有一個偵聽通訊端用於存取伺服器。如果這是列出的唯一一個偵聽通訊端，則不能將其刪除。

變更超級使用者設定

可以爲 Administration Server 配置超級使用者存取權。這些設定僅會影響超級使用者帳號。如果 Administration Server 採用分散式管理，則必須爲獲得許可的管理員配置額外存取控制。

注意 – 如果使用 Sun Java System Directory Server 管理使用者和群組，則必須**先**在目錄中更新超級使用者項目，然後才能變更超級使用者的使用者名稱或密碼。如果不先更新目錄，將無法存取 Administration Server 中的 [Users and Groups] 介面。然後，必須使用可以存取目錄的管理員帳號來存取 Administration Server，或使用 Directory Server 的主控台或配置檔案來更新目錄。

▼ 變更 Administration Server 的超級使用者設定

1. **存取 Administration Server，然後按一下 [Preferences] 標籤。**
2. **按一下 [Control Superuser Access] 連結。**
3. **進行所需的變更，然後按一下 [OK]。**

   如需有關特定欄位的更多資訊，請參閱線上說明。

   超級使用者的使用者名稱和密碼存放在名稱爲 `admpw` 的檔案中，此檔案位於 *server-root* `/proxy-admserv/config` 中。檔案的格式爲 *username* :*password*。您可以檢視此檔案以取得使用者名稱，但密碼已加密且不可讀取。如果您忘記密碼，可以改用新密碼。

▼ 變更超級使用者密碼

1. **編輯 `admpw` 檔案並刪除加密的密碼。**
2. **僅藉由使用者名稱而不用密碼存取 Administration Server。**
3. **按一下 [Preferences] 標籤。**
4. **按一下 [Control Superuser Access] 連結。**
5. **提供新密碼，然後按一下 [OK]。**

注意 – 由於 `admpw` 檔案可以進行編輯，因此伺服器電腦必須放置於安全位置，且必須限制他人存取其檔案系統。

在 UNIX 及 Linux 系統上，請考慮變更檔案所有權，以便只讓 root 或執行 Administration Server 常駐程式的任何系統使用者寫入檔案。在 Windows 系統上，將檔案所有權限制爲 Administration Server 使用的使用者帳號。

允許多個管理員

多個管理員可透過分散式管理變更伺服器的特定部分。必須先安裝目錄伺服器，才能啓用分散式管理。預設目錄服務必須以 LDAP 爲基礎。

分散式管理的兩個使用者層級爲超級使用者和管理員。

- 超級使用者是指 *server-root* `/proxy-admserv/config/admpw` 中列出的使用者。這是在安裝時所指定的使用者名稱和密碼。超級使用者對 Administration Server 中的所有表單均有完整的存取權，但 [Users and Groups] 表單除外，需視超級使用者在 LDAP 伺服器中是否有有效帳戶，才可決定能否存取此類表單。
- 管理員可直接移往特定伺服器 (包括 Administration Server) 的 Server Manager 表單。他人 (通常爲超級使用者) 爲管理員配置的存取控制規則，決定該管理員可檢視哪些表單。管理員可以執行有限的管理作業，還可進行影響其他使用者的變更，如增加使用者或變更存取控制。

如需有關存取控制的更多資訊，請參閱第 8 章 「控制對伺服器的存取」。

▼ 啓用分散式管理

1. **確定已安裝目錄伺服器。**
2. **存取 Administration Server。**
3. **(可選) 安裝目錄伺服器之後，可能還需要建立管理群組 (若您尚未建立)。建立群組：**
   a. **按一下 [Users and Groups] 標籤。**
   b. **按一下 [Create Group] 連結。**
   c. **在 LDAP 目錄中建立管理員群組並加入使用者名稱，以便授予這些使用者有足夠權限能配置 Administration Server 或其伺服器根底目錄下所安裝的任何伺服器。**
      如需有關特定欄位的更多資訊，請參閱線上說明。

      管理員群組中的所有使用者對 Administration Server 都具有完整的存取權限，但可以使用存取控制來限制管理員可配置的伺服器和表單。

      建立存取控制清單後，分散式管理群組便會增加至此清單。如果管理員群組的名稱已變更，則必須手動編輯存取控制清單才能變更其參照的群組。
4. **按一下 [Preferences] 標籤。**
5. **按一下 [Configure Distributed Administration] 連結。**

6 **選取 [Yes]、指定管理員群組，然後按一下 [OK]。**

指定記錄檔選項

Administration Server 記錄檔記錄關於 Administration Server 的資料，包括遇到的錯誤類型以及有關伺服器存取的資訊。記錄資訊可用於監視伺服器活動並進行問題疑難排解。使用 [Log Preferences] 頁面中的許多選項，可以指定 Administration Server 記錄中所記錄的資料類型和格式。您可以選擇 [Common Logfile Format] (用於提供固定數量的伺服器資訊)，或建立自訂記錄檔格式，以更好符合您的需求。

若要存取 [Administration Server Log Preferences] 頁面，請按一下 [Preferences] 標籤，然後按一下 [Set Access Log Preferences] 或 [Set Error Log Preferences] 連結。如需有關記錄檔及設定記錄檔選項的詳細資訊，請參閱第 9 章 「使用記錄檔」。另請參閱線上說明。

檢視記錄檔

Administration Server 記錄檔位於 *server-root* `/proxy-admserv/logs` 中。您可透過 Proxy Server 管理主控台或文字編輯器檢視錯誤記錄及存取記錄。

存取記錄檔

存取記錄檔記錄關於請求伺服器以及伺服器回應的資訊。

▼ 檢視存取記錄檔

1 **存取 Administration Server，然後按一下 [Preferences] 標籤。**

2 **按一下 [View Access Log] 連結。**
如需有關特定欄位的更多資訊，請參閱線上說明。另請參閱第 9 章 「使用記錄檔」。

錯誤記錄檔

錯誤記錄檔列出自建立記錄檔以來伺服器遇到的所有錯誤。其中也包含關於伺服器的資訊訊息，如啓動伺服器的時間與嘗試登入伺服器但失敗的使用者。

▼ 檢視錯誤記錄檔

1 **存取 Administration Server，然後按一下 [Preferences] 標籤。**

2 **按一下 [View Error Log] 連結。**
如需有關特定欄位的更多資訊，請參閱線上說明。另請參閱第 9 章 「使用記錄檔」。

使用目錄服務

您可以使用 LDAP 在單一目錄伺服器中儲存並管理諸如使用者名稱和密碼等資訊。您也可以配置伺服器，允許使用者從多個方便存取的網路位置擷取目錄資訊。如需有關使用目錄服務的更多資訊，請參閱第 4 章 「管理使用者和群組」。

限制伺服器存取

Proxy Server 評估內送請求時，會根據名爲存取控制項目 (ACE) 的規則階層確定是否存取，然後使用相符的項目確定應允許還是拒絕該請求。每個 ACE 都會指定伺服器是否應繼續進入階層中的下一個 ACE。ACE 的集合稱爲存取控制清單 (ACL)。

可以針對存取 Administration Server 及伺服器實例內特定資源 (如檔案、目錄和檔案類型) 來配置存取控制。對 Administration Server 的存取控制，需在 Administration Server 的 [Global Settings] 標籤中配置。對伺服器實例內資源的存取控制，需在 Server Manager 的 [Preferences] 標籤中配置。如需有關設定存取控制的更多資訊，請參閱第 8 章 「控制對伺服器的存取」。

備註 – 必須先啓用分散式管理，才能限制伺服器存取。如需更多資訊，請參閱第 38 頁的 「允許多個管理員」。

SNMP 主代理程式設定

簡易網路管理協定 (SNMP) 是一種用於交換有關網路活動資料的協定。此資訊透過使用子代理程式及主代理程式，在網路管理工作站和伺服器之間進行傳輸。

SNMP 主代理程式設定是在 Administration Server 的 [Global Settings] 標籤中配置的。主代理程式隨 Administration Server 一起安裝。如需有關 SNMP 及代理程式設定的詳細資訊，請參閱第 10 章 「監視伺服器」。另請參閱線上說明，以瞭解 Administration Server 之 [Global Settings] 標籤的主代理程式頁面，以及管理伺服器之 [Server Status] 標籤的子代理程式頁面。

◆ ◆ ◆ 第 4 章

管理使用者和群組

本章說明如何增加、刪除、修改及管理可存取 Proxy Server 的使用者和群組。

本章包含下列小節：

存取關於使用者和群組的資訊

使用 Administration Server 可以存取關於使用者帳號、群組清單、存取權限、組織單元以及其他使用者和群組特定資訊的應用程式資料。

使用者和群組資訊會儲存在文字格式的平面檔案中，或是在支援 LDAP (簡易目錄存取協定) 的目錄伺服器 (如 Sun Java System Directory Server) 中。LDAP 是一種在 TCP/IP (傳輸控制通訊協定/網際網路通訊協定) 上執行的開放式目錄存取協定，且可延伸至全域規模及數百萬個項目。

關於目錄服務

目錄服務可以從單一來源管理所有使用者資訊。利用 Proxy Server，可以配置三種不同類型的目錄服務：LDAP、金鑰檔案及摘要檔案。

如果尚未配置其他目錄服務，則第一個建立的新目錄服務會設定爲 `default` 值 (類型不拘)。建立目錄服務時，*server-root* `/userdb/dbswitch.conf` 檔案中會更新目錄服務詳細資訊。

本小節說明 LDAP、金鑰檔案及摘要檔案的目錄服務。

LDAP 目錄服務

利用 LDAP 目錄服務，使用者和群組資訊可儲存在 LDAP 型目錄伺服器中。

如果 LDAP 服務爲預設服務，則會如下列範例所示更新 `dbswitch.conf` 檔案：

```
directory default
ldap://test22.india.sun.com:589/dc%3Dindia%2Cdc%3Dsun%2Cdc%3Dcomdefault:binddn
cn=Directory Managerdefault:encoded bindpw YWRtaW5hZG1pbg==
```

如果 LDAP 服務不是預設服務，則會如下列範例所示更新 `dbswitch.conf` 檔案：

```
directory ldap
ldap://test22.india.sun.com:589/dc%3Dindia%2Cdc%3Dsun%2Cdc%3Dcomldap:binddn
cn=Directory Managerldap:encoded bindpw YWRtaW5hZG1pbg==
```

金鑰檔案目錄服務

金鑰檔案是一個文字檔案，其中包含雜湊格式的使用者密碼以及該使用者所屬群組的清單。只有在打算使用 HTTP 基本認證時才能使用金鑰檔案格式。如需有關此認證方法的更多資訊，請參閱第 146 頁的「指定使用者和群組」。

建立基於金鑰檔案的資料庫時，會如以下範例所示更新 `dbswitch.conf` 檔案：

```
directory keyfile filekeyfile:syntax keyfilekeyfile:keyfile D:\\test22\
\keyfile\\keyfiledb
```

摘要檔案目錄服務

摘要檔案會根據已加密的使用者名稱和密碼來儲存使用者和群組資訊。

摘要檔案格式的功能是支援使用 HTTP 摘要認證，但也支援基本認證，所以同時適用於這兩種認證方法。如需有關這些方法的更多資訊，請參閱第 146 頁的「指定使用者和群組」。

建立基於摘要的資料庫時，會如以下範例所示更新 dbswitch.conf 檔案：

```
directory digest filedigest:syntax digestdigest:digestfile D:\\test22\\digest\
\digestdb
```

備註 – 若要配置分散式管理，則預設目錄服務必須是 LDAP 型目錄服務。

配置目錄服務

在 Administration Server 的 [Global Settings] 標籤上可以建立和配置目錄服務。接著，在 Administration Server 的 [Users and Groups] 標籤上可以建立和管理使用者、群組及組織單元。

本小節說明建立及編輯目錄服務的方法。

▼ 建立目錄服務

1. **存取 Administration Server，然後按一下 [Global Settings] 標籤。**
2. **按一下 [Configure Directory Service] 連結。**
3. **從 [Create New Service of Type] 下拉式清單中，選取您要建立的目錄服務類型，然後按一下 [New]。**
   此時會顯示此目錄服務的配置頁面。
4. **提供配置資訊，然後按一下 [Save Changes]。**
   如需有關特定欄位的更多資訊，請參閱線上說明。

備註 – 如果尚未配置其他目錄服務，則第一個建立的新目錄服務會設定爲 default 值 (類型不拘)。

▼ 編輯目錄服務

1. **存取 Administration Server，然後按一下 [Global Settings] 標籤。**
2. **按一下 [Configure Directory Service] 連結。**
3. **按一下您要編輯的目錄服務的連結。**

4 **進行所需的變更，然後按一下 [Save Changes]。**
如需有關特定欄位的更多資訊，請參閱線上說明。

瞭解辨別名稱 (DN)

Administration Server 中的 [Users and Groups] 標籤可用於建立或修改使用者、群組及組織單元。使用者是 LDAP 資料庫中的個人，例如貴公司的員工。群組是共用某個一般屬性的兩個或多個使用者。組織單元是組織內使用 `organizationalUnit` 物件類別的一個細分單位。本章稍後將詳細說明使用者、群組及組織單元。

您企業內的每個使用者和群組皆以辨別名稱 (DN) 屬性來表示。DN 屬性是一個包含關聯使用者、群組或物件之識別資訊的文字字串。每當使用者或群組目錄項目變更時，您都必須使用 DN。例如，每次建立或修改目錄項目、配置存取控制以及爲應用程式 (如郵件或發佈) 配置使用者帳號時，您都必須提供 DN 資訊。Proxy Server 的 [Users and Groups] 介面可用於建立或修改 DN。

下列範例顯示 Sun Microsystems 員工的典型 DN：

```
uid=doe,e=doe@sun.com,cn=John Doe,o=Sun Microsystems Inc.,c=US
```

此範例中的縮寫有下列意義：

- `uid` 表示使用者 ID
- `e` 表示電子郵件地址
- `cn` 表示使用者的一般名稱
- `o` 表示組織
- `c` 表示國家/地區

DN 可能包含各種「名稱-值」對，且可在支援 LDAP 的目錄中用於識別憑證主體及項目。

使用 LDIF

如果您目前沒有目錄，或您想要在現有目錄中增加新的子樹狀結構，可以使用目錄伺服器的 LDIF (簡易目錄交換格式) 匯入功能。此功能接受包含 LDIF 的檔案，並且會嘗試從 LDIF 項目建立目錄或新子樹。您也可以使用目錄伺服器的 LDIF 匯出功能，將目前目錄匯出至 LDIF。此功能會建立一個代表您目錄的 LDIF 格式的檔案。您可以使用 `ldapmodify` 指令行公用程式 (如果可用) 及適當的 LDIF 更新敘述來增加或編輯項目。

若要使用 LDIF 向資料庫中增加項目，請先在 LDIF 檔案中定義項目，然後從目錄伺服器匯入此 LDIF 檔案。

建立使用者

Administration Server 中的 [Users and Groups] 標籤可用於建立及修改使用者項目。使用者項目包含有關資料庫中個別使用者或物件的資訊。

備註 – 請確定使用者無法未經授權就存取資源，以保護伺服器的安全性。Proxy Server 會使用基於 ACL 的授權及認證模型。如需有關基於 ACL 的安全性的更多資訊，請參閱第 8 章「控制對伺服器的存取」。如需其他安全性資訊，另請參閱第 5 章「使用憑證和金鑰」。

本小節說明在 LDAP 型認證資料庫、金鑰檔案認證資料庫及摘要檔案認證資料庫中建立使用者的方法。

在 LDAP 型認證資料庫中建立使用者

當使用者項目增加到 LDAP 型目錄服務中後，LDAP 型目錄伺服器下的服務即可用於認證及授權這些使用者。本小節列出在使用 LDAP 型認證資料庫時需要考慮的準則，並說明透過 Proxy Server Administration Server 來增加使用者的方法。

建立 LDAP 型使用者項目的準則

當使用 Proxy Server 管理主控台在 LDAP 型目錄服務中建立新的使用者項目時，請考慮下列準則：

- 如果您提供姓名 (或名字) 與姓氏，則會自動填寫使用者的全名及使用者 ID。使用者 ID 由使用者名字的第一個字母後面加上使用者的姓氏所組成。例如，如果使用者名稱爲 Billie Holiday，則使用者 ID 會自動設定爲 `bholiday`。如果您願意，可以用自己選擇的 ID 取代該使用者 ID。
- 使用者 ID 必須是唯一的。Administration Server 會從搜尋庫 (基底 DN) 向下搜尋整個目錄來查看使用者 ID 是否在使用中，以確保該使用者 ID 是唯一的。但請注意，如果您使用目錄伺服器 `ldapmodify` 指令行公用程式 (如果可用) 來建立使用者，則無法確保使用者 ID 爲唯一。如果目錄中存在重複的使用者 ID，則受到影響的使用者將不能認證到該目錄。
- 基底 DN 指定的辨別名稱是目錄查找的預設位置，也是您的目錄樹狀結構中放置所有 Proxy Server Administration Server 項目的位置。辨別名稱 (DN) 是代表目錄伺服器中某個項目名稱的字串。
- 在建立新的使用者項目時，您至少必須指定下列使用者資訊：
  - 姓氏
  - 全名
  - 使用者 ID

如果您的目錄已定義任何組織單元，則您可以在 Administration Server 的 [Create User] 頁面上使用 [Add New User To] 清單，指定您要放置新使用者的位置。預設位置爲您目錄的基底 DN (或根位置)。

Directory Server 使用者項目

請注意下列有關目錄伺服器使用者項目的資訊：

- 使用者項目使用 `inetOrgPerson`、`organizationalPerson` 及 `person` 物件類別。
- 依預設，使用者的辨別名稱爲下列格式：

  `cn=` **全名**`,ou=` **組織** `,...,o=` **基底組織**`,c=` **國家/地區**

  例如，如果 Billie Holiday 的使用者項目是在組織單元 Marketing 內建立，且目錄的基底 DN 是 `o=Ace Industry, c=US`，則此使用者的 DN 爲：

  ```
  cn=Billie Holiday,ou=Marketing,o= Ace Industry,c=US
  ```

  此格式可以變更爲基於使用者 ID (uid) 的辨別名稱。
- 使用者表單欄位的值會儲存爲 LDAP 屬性。

  下表列出在 Proxy Server 介面中建立或編輯新使用者時會顯示的欄位及對應的 LDAP 屬性。

表 4–1 LDAP 屬性 - 建立或編輯使用者項目

使用者欄位	LDAP 屬性
Given Name	`givenName`
Surname	`sn`
Full Name	`cn`
使用者 ID	`uid`
Password	`userPassword`
E-mail Address	`mail`
Title	`title`
Phone Number	`telephoneNumber`

建立 LDAP 型使用者項目

若要建立使用者項目，請參閱第 45 頁的 「建立 LDAP 型使用者項目的準則」中的準則，然後執行下列程序。

▼ 在 LDAP 型認證資料庫中建立使用者

1. **存取 Administration Server，然後按一下 [Users and Groups] 標籤。**
2. **按一下 [Create User] 連結。**
3. **從下拉式清單中選取 LDAP 目錄服務，然後按一下 [Select]。**
4. **在顯示的頁面上提供資訊。**
   如需有關特定欄位的更多資訊，請參閱線上說明。
   另請參閱第 46 頁的 「Directory Server 使用者項目」 。
5. **按一下 [Create] 以建立使用者項目，或按一下 [Create and Edit] 以建立使用者項目，並前進至剛建立之項目的編輯頁面。**

在金鑰檔案認證資料庫中建立使用者

金鑰檔案是一個文字檔案，其中包含雜湊格式的使用者密碼以及該使用者所屬群組的清單。

▼ 在金鑰檔案認證資料庫中建立使用者

1. **存取 Administration Server，然後按一下 [Users and Groups] 標籤。**
2. **按一下 [Create User] 連結。**
3. **從下拉式清單中選取基於金鑰檔案的目錄服務，然後按一下 [Select]。**
4. **在顯示的頁面上鍵入資訊，然後按一下 [Create User]。**
   如需有關特定欄位的更多資訊，請參閱線上說明。

在摘要檔案認證資料庫中建立使用者

摘要檔案認證資料庫會以加密形式來儲存使用者和群組資訊。

▼ 在摘要檔案認證資料庫中建立使用者

1. **存取 Administration Server，然後按一下 [Users and Groups] 標籤。**
2. **按一下 [Create User] 連結。**
3. **從下拉式清單中選取基於摘要檔案的目錄服務，然後按一下 [Select]。**
4. **在顯示的頁面上鍵入資訊，然後按一下 [Create User]。**
   如需有關特定欄位的更多資訊，請參閱線上說明。

備註 – 使用 [Proxy Server ACL] 使用者介面建立使用摘要認證的 ACL 時，必須指定相同的範圍字串。如需更多資訊，請參閱第 142 頁的 「設定存取控制」。

管理使用者

您可以在 [Administration Server Users and Groups] 標籤的 [Manage Users] 頁面上編輯使用者屬性。您可以在此頁面尋找、變更、重新命名及刪除使用者項目。

本小節描述了下列主題：

尋找使用者資訊

您必須先找到並顯示使用者項目，才能編輯此項目。對於基於 LDAP 的目錄服務，您可以爲您要編輯的項目提供描述性的值。

您可以提供下列任何一項資訊：

- 名稱。輸入全名或部分名稱。將傳回所有完全符合該搜尋字串的項目。如果未找到這樣的項目，則將傳回所有包含該搜尋字串的項目。如果未找到包含搜尋字串的項目，則將尋找發音類似搜尋字串的所有項目。
- 使用者 ID。如果只輸入部分使用者 ID，則會傳回包含此字串的所有項目。
- 電話號碼。如果您僅輸入部分號碼，則將傳回包含以搜尋字串結尾的電話號碼的所有項目。
- 電子郵件地址。任何包含 at 符號 (@) 的搜尋字串皆會視爲電子郵件地址。如果找不到完全相符的項目，則會尋找以搜尋字串開頭的所有電子郵件地址。

- 任何 LDAP 搜尋篩選器。包含等號 (=) 的任何字串均被視爲搜尋篩選器。
- 使用星號 (*) 可以查看當前您目錄中的所有項目。將此欄位保留空白也可達到相同的結果。

建立自訂搜尋查詢

對於 LDAP 服務，[Find All Users Whose] 區段可讓您建立自訂搜尋篩選器。請使用欄位來縮小 [Find User] 搜尋所傳回的搜尋結果範圍。

左側的下拉式清單可以指定搜尋所依據的屬性。下表列出可用的搜尋屬性選項。

表 4–2 搜尋屬性選項

選項	搜尋相符項目
全名	每個項目的全名
Last name	每個項目的姓氏
使用者 ID	每個項目的使用者 ID
Phone number	每個項目的電話號碼
E-mail address	每個項目的電子郵件地址

中央的下拉式清單會指定要執行的搜尋類型。下表列出可用的搜尋類型選項。

表 4–3 搜尋類型選項

選項	說明
Contains	導致執行子字串搜尋。傳回屬性值包含指定搜尋字串的項目。例如，如果您知道使用者的名稱可能包含單字「Dylan」，請使用此選項及搜尋字串「Dylan」來尋找此使用者的項目。
Is	能找到完全相符項目 (指定等式搜尋)。當您知道使用者屬性的精確值時，請使用此選項。例如，您知道使用者名稱的正確拼寫。
Isn't	傳回屬性值與搜尋字串不完全相符的所有項目。可以使用此選項在目錄中尋找名稱不是「John Smith」的所有使用者。請注意，使用此選項可能會導致傳回極多項目。
Sounds like	導致執行近似或音形一致的搜尋。如果您知道屬性的值，但不確定拼寫，請使用此選項。例如，您不確定使用者名稱的拼寫是「Sarret」、「Sarette」還是「Sarett」。
Starts with	導致執行子字串搜尋。傳回屬性值以指定搜尋字串開頭的所有項目。例如，您知道使用者的名稱以「Miles」開頭，但不知道名稱的其餘部分。

表 4–3 搜尋類型選項 *(續)*

選項	說明
Ends with	導致執行子字串搜尋。傳回屬性值以指定搜尋字串結尾的所有項目。例如，您知道使用者的名稱以「Dimaggio」結尾，但不知道名稱的其餘部分。

右側的文字欄位可用於輸入搜尋字串。若要顯示 [Look Within] 欄位所指定之目錄中包含的所有使用者項目，請鍵入星號 (*) 或將此欄位保留爲空白。

▼ 尋找使用者資訊

1 **存取 Administration Server，然後按一下 [Users and Groups] 標籤。**

2 **按一下 [Manage Users] 連結。**

3 **從下拉式清單中選取目錄服務，然後按一下 [Select]。**

若選取金鑰檔案或摘要檔案目錄服務，則會顯示使用者的清單。若選取 LDAP 型目錄服務，則會顯示搜尋欄位。

4 **查找使用者資訊：**

若爲金鑰檔案或摘要檔案目錄服務，請按一下使用者的連結來顯示編輯頁面並進行變更。如需有關特定欄位的更多資訊，請參閱線上說明。

若爲 LDAP 型目錄服務，請執行以下動作：

a. **在 [Find User] 欄位中，為您要編輯的項目輸入描述性值。**

或者，您也可以使用 [Find All Users Whose] 區段中的下拉式功能表來縮小搜尋結果範圍。如需更多資訊，請參閱第 49 頁的 「建立自訂搜尋查詢」。

b. **在 [Look Within] 欄位中，選取您要在哪個組織單位下搜尋項目。**

預設爲目錄的根位置 (最上面的項目)。

c. **在 [Format] 欄位中，指定要將輸出格式化以顯示於螢幕，還是列印至印表機。**

d. **在此過程中的任何階段，皆可按一下 [Find] 按鈕。**

螢幕上會顯示符合搜尋條件的所有使用者。

e. **按一下您要顯示的項目的連結。**

編輯使用者資訊

▼ 編輯使用者項目

1. **存取 Administration Server，然後按一下 [Users and Groups] 標籤。**
2. **按一下 [Manage Users] 連結。**
3. **顯示使用者項目，如第 48 頁的 「尋找使用者資訊」中所述。**
4. **依需要變更。**
   如需有關特定欄位的更多資訊，請參閱線上說明。

備註 – 若要變更在編輯使用者頁面中未顯示的屬性值，請使用目錄伺服器 `ldapmodify` 指令行公用程式 (如果可用)。

如需有關變更使用者的使用者 ID 的資訊，請參閱第 51 頁的 「重新命名使用者」。

管理使用者密碼

下列程序說明變更或建立使用者密碼的方法。

▼ 變更或建立使用者密碼

1. **存取 Administration Server，然後按一下 [Users and Groups] 標籤。**
2. **按一下 [Manage Users] 連結。**
3. **顯示使用者項目，如第 48 頁的 「尋找使用者資訊」中所述。**
4. **依需要變更。**
   如需有關特定欄位的更多資訊，請參閱線上說明。

   對於 LDAP 資料庫，您也可以從 [Manage Users] 頁面中存取用於編輯使用者密碼資訊的頁面，然後按一下 [Disable Password] 按鈕來停用使用者的密碼。此動作不必刪除使用者的目錄項目，就可以阻止使用者登入伺服器。您可以提供新的密碼，重新允許使用者存取。

重新命名使用者

對於 LDAP 資料庫，重新命名功能只能變更使用者 ID。其他所有欄位均保持不變。無法使用重新命名功能將項目從一個組織單元移至另一個組織單元。

▼ 重新命名使用者項目

1. **存取 Administration Server，然後按一下 [Users and Groups] 標籤。**
2. **按一下 [Manage Users] 連結。**
3. **顯示使用者項目，如第 48 頁的 「尋找使用者資訊」中所述。**
4. **按一下編輯使用者頁面上的 [Rename User] 按鈕。**
5. **在顯示的頁面上鍵入使用者 ID，然後按一下 [Save Changes]。**

備註 – 透過將 `keepOldValueWhenRenaming` 參數設定爲 `false` (預設值)，可以指定在重新命名項目時，Administration Server 不再保留舊的值。在下列檔案中可以找到此參數：

server-root`/proxy-admserv/config/dsgw-orgperson.conf`

移除使用者

▼ 移除使用者項目

1. **存取 Administration Server，然後按一下 [Users and Groups] 標籤。**
2. **按一下 [Manage Users] 連結。**
3. **顯示使用者項目，如第 48 頁的 「尋找使用者資訊」中所述。**
4. **按一下適當的按鈕。**
   - 若爲 LDAP 伺服器，請按一下 [Delete User]。
   - 若爲金鑰檔案和摘要檔案資料庫，請按一下 [Remove User]。

建立群組

群組是一種物件，用於說明 LDAP 資料庫中的一組物件。Sun Java System Server 群組由共用某個一般屬性的使用者組成。例如，這組物件可能是在貴公司行銷部門工作的一群員工。這些員工可能屬於稱爲 Marketing 的群組。

對於 LDAP 服務，定義群組成員身分有靜態和動態兩種方法。靜態群組明確列舉其成員物件。靜態群組是一般名稱 (CN)，且含有 `uniqueMembers` 或 `memberURLs` 或 `memberCertDescriptions`。對於靜態群組，成員不共用一般屬性，但 `cn=groupname` 屬性除外。

動態群組可讓您使用 LDAP URL 定義僅與群組成員比對的規則集。對於動態群組，成員會共用 memberURL 篩選器中定義的某個一般屬性或屬性集。例如，如果您需要一個群組來包含 Sales 的所有員工，且這些員工已存在於 LDAP 資料庫中的 ou=Sales,o=Airius.com 之下，則您可以使用下列成員 URL 來定義動態群組：

```
ldap:///ou=Sales,o=sun??sub?(uid=*)
```

然後，此群組將包含在樹狀結構的 ou=Sales,o=sun 點下具有 uid 屬性的所有物件。

對於靜態和動態群組，如果使用 memberCertDescription，則成員可以共用憑證中的一般屬性。ACL 必須使用 SSL 方法，才能共用一般屬性。

一旦建立新的群組之後，您就可以在群組中增加使用者 (成員)。

本小節包含以下主題：

- 第 53 頁的 「關於靜態群組」
- 第 54 頁的 「關於動態群組」

關於靜態群組

對於 LDAP 服務，Administration Server 可使您透過在任意數量使用者的 DN 中指定同一群組屬性來建立靜態群組。靜態群組除了增加或刪除使用者之外，完全不會有任何變更。

建立靜態群組的準則

當使用 [Administration Server] 介面來建立新的靜態群組時，請考慮下列準則：

- 靜態群組可以包含其他靜態或動態群組。
- 如果您的目錄已定義組織單元，則您可以在 [Administration Server] 介面的 [Create Group] 頁面上使用 [Add New Group To]，指定您要放置新群組的位置。預設位置爲目錄的根位置 (最上面的項目)。
- 如需有關編輯群組的更多資訊，請參閱第 58 頁的 「編輯群組項目」。

▼ 建立靜態群組

1. **存取 Administration Server，然後按一下 [Users and Groups] 標籤。**
2. **按一下 [Create Group] 連結。**
3. **從 [Type of Group] 下拉式清單中選取 [New Group]，然後按一下 [Go]。**
4. **在 [Create Group] 頁面上鍵入資訊。**
   如需有關特定欄位的更多資訊，請參閱線上說明。

5 **按一下 [Create] 以建立群組，或按一下 [Create and Edit] 以建立群組，並顯示剛建立之群組的編輯頁面。**

關於動態群組

對於 LDAP 服務，如果您想要根據任何屬性來自動將使用者分組，或想要將 ACL 套用至包含相符 DN 的特定群組，Proxy Server 可讓您建立動態群組。例如，您可以建立一個群組來自動包括含有 `department=marketing` 屬性的所有 DN。如果您套用 `department=marketing` 的搜尋篩選器，則搜尋傳回的群組會包括含有屬性 `department=marketing` 的所有 DN。然後，您可以由基於此過濾器的搜尋結果定義動態群組。隨後，您可以針對結果動態群組定義一個 ACL。

動態群組的實作方法

Proxy Server 會在 LDAP 伺服器模式中將動態群組實作爲 `objectclass=groupOfURLs`。一個 `groupOfURLs` 類別可能沒有或有多個 `memberURL` 屬性，每個屬性都是說明目錄中一組物件的 LDAP URL。群組成員將是這些物件集的併集。例如，下列群組只包含一個成員 URL：

```
ldap:///o=mcom.com??sub?(department=marketing)
```

此範例說明的是在 `o=mcom.com` 之下由部門爲 `marketing` 的所有物件所組成的集合。LDAP URL 可以包含搜尋庫 DN、範圍及篩選器，但不能包含主機名稱和連接埠。因此，您只能參照同一 LDAP 伺服器上的物件。支援所有範圍。如需有關 LDAP URL 的更多資訊，請參閱第 55 頁的 「建立動態群組的準則」。

DN 會自動加入群組中，不必在群組中逐一增加。群組會動態變更，因爲每次 ACL 驗證需要群組查詢時，Proxy Server 就會執行 LDAP 伺服器搜尋。ACL 檔案中使用的使用者和群組名稱，與 LDAP 資料庫中物件的 `cn` 屬性相對應。

備註 – Proxy Server 使用 `cn` 屬性作爲 ACL 的群組名稱。

從 ACL 至 LDAP 資料庫的對映在 `dbswitch.conf` 檔案 (它將 ACL 資料庫名稱與實際 LDAP 資料庫 URL 關聯起來) 和 ACL 檔案 (它定義資料庫與 ACL 的對應關係) 中均有定義。例如，如果您想要讓名爲 `staff` 的群組中的成員身分具有基本存取權限，ACL 程式碼會查找物件類別爲 `groupOf`*anything* 且 CN 設定爲 `staff` 的物件。此物件可以明確列舉成員 DN (如同靜態群組的 `groupOfUniqueNames` 一樣) 或指定 LDAP URL (例如，`groupOfURLs`) 來定義群組的成員。

備註 – 群組可以是靜態群組和動態群組。群組物件可以同時有 `objectclass=groupOfUniqueMembers` 和 `objectclass=groupOfURLs`。因此，`uniqueMember` 和 `memberURL` 屬性兩者皆有效。群組的成員身分是靜態和動態成員的併集。

動態群組對伺服器效能的影響

使用動態群組會影響伺服器效能。如果您正在測試群組成員身分，且 DN 不是靜態群組的成員，則 Proxy Server 會檢查資料庫基底 DN 中的所有動態群組。Proxy Server 會比對使用者的 DN 來檢查基底 DN 和範圍，以判斷每個 `memberURL` 是否相符。接著，Proxy Server 會以使用者 DN 做爲基底 DN 和 `memberURL` 的篩選器來執行基本搜尋。此程序可能需要大量的個別搜尋。

建立動態群組的準則

使用 [Administration Server] 介面來建立新的動態群組時，請考慮下列準則：

- 動態群組不能包含其他群組。
- LDAP URL 使用下列格式，其中不含主機和連接埠資訊，因爲會忽略這些參數：

  `ldap:///` *base-dn*`?`*attributes*`?` *scope*`?(`*filter*`)`

`attributes`、`scope` 及 `(filter)` 參數在 URL 中的位置，可作爲識別這些參數的依據。即使您不要指定任何屬性，您仍然必須加上問號 (?) 來分隔此欄位。

- 如果您的目錄已定義組織單元，則您可以在 [Administration Server] 介面的 [Create Group] 頁面上使用 [Add New Group To]，指定您要放置新群組的位置。預設位置爲目錄的根位置 (最上面的項目)。

如需有關編輯群組的更多資訊，請參閱第 58 頁的 「編輯群組項目」。

下表列出 LDAP URL 的必要參數。

表 4–4 LDAP URL 的必要參數

參數名稱	說明
`base_dn`	搜尋庫的 DN，或 LDAP 目錄中所有搜尋的執行起點。此參數經常設定爲目錄的後綴或根，例如 `o=mcom.com`。
`attributes`	搜尋將傳回的屬性清單。若要指定多個屬性，請使用逗號來分隔屬性 (例如，`cn,mail,telephoneNumber`)。如果未指定屬性，則會傳回所有屬性。檢查動態群組成員身分時會忽略此參數。

表 4–4 LDAP URL的必要參數 (續)

參數名稱	說明
scope	此參數是必需的。 搜尋的範圍，可以是下列值之一： ■ base 只針對 URL 中指定的辨別名稱 (base_dn) 來擷取相關資訊。 ■ one 針對 URL 中指定的辨別名稱 (base_dn) 的下一層級項目來擷取相關資訊。此範圍不包括基準項目。 ■ sub 針對 URL 中指定的辨別名稱 (base_dn) 之下的所有層級項目來擷取相關資訊。此範圍包括基準項目。
(filter)	此參數是必需的。 對指定搜尋範圍內的項目所套用的搜尋篩選器。如果您使用 [Administration Server] 介面，則必須指定此屬性。括弧是必要的。

建立動態群組

▼ 建立動態群組

1. **存取 Administration Server，然後按一下 [Users and Groups] 標籤。**
2. **按一下 [Create Group] 連結。**
3. **從 [Type of Group] 下拉式清單中選取 [Dynamic Group]，然後按一下 [Go]。**
4. **在 [Create Group] 頁面上提供資訊。**
   如需有關特定欄位的更多資訊，請參閱線上說明。
5. **按一下 [Create] 以建立群組，或按一下 [Create and Edit] 以建立群組，並顯示剛建立之群組的編輯頁面。**

管理群組

對於 LDAP 服務，Administration Server 可讓您在 [Administration Server Users and Groups] 標籤的 [Manage Groups] 頁面上編輯群組及管理群組成員身分。

本小節描述了下列工作：

- 第 57 頁的 「尋找群組項目」
- 第 58 頁的 「編輯群組項目」
- 第 59 頁的 「增加群組成員」
- 第 60 頁的 「將群組增加至群組成員清單」

尋找群組項目

您必須先找到並顯示群組項目，才能編輯此項目，如下列程序所述。

▼ 尋找群組項目

1. **存取 Administration Server，然後按一下 [Users and Groups] 標籤。**
2. **按一下 [Manage Groups] 連結。**
3. **在 [Find Group] 欄位中鍵入您要尋找的群組名稱。**
   您可以提供下列任何值：
   - 使用星號 (*) 可以查看當前您目錄中的所有群組。將此欄位保留空白也可達到相同的結果。
   - 任何 LDAP 搜尋篩選器。包含等號 (=) 的任何字串均被視爲搜尋篩選器。
     或者，也可以使用 [Find All Groups Whose] 區段來建立自訂搜尋篩選器及縮小搜尋結果範圍。如需更多資訊，請參閱第 57 頁的 「Find All Groups Whose」。
   - 名稱。提供全名或部分名稱。將傳回所有完全符合該搜尋字串的項目。如果未找到這樣的項目，則將傳回所有包含該搜尋字串的項目。如果未找到包含搜尋字串的項目，則將尋找發音類似搜尋字串的所有項目。
4. **在 [Look Within] 欄位中，選取您要在哪個組織單位下搜尋項目。**
   預設爲目錄的根位置 (最上面的項目)。
5. **在 [Format] 欄位中，指定要將輸出格式化以顯示於螢幕，還是列印至印表機。**
6. **若要在此程序的任何階段顯示符合條件的所有群組，請按一下 [Find] 按鈕。**
7. **按一下您要顯示的項目的連結。**

Find All Groups Whose

對於 LDAP 服務，[Find All Groups Whose] 區段可讓您建立自訂搜尋篩選器。請使用此區段中的欄位來縮小 [Find Group] 所傳回的搜尋結果範圍。

左側的下拉式清單可以指定搜尋所依據的屬性。下列爲可用的選項：

- **Name**。搜尋每個項目的全名來尋找相符群組。
- **Description**。搜尋每個群組項目的說明來尋找相符群組。

中央的下拉式清單會指定要執行的搜尋類型。下列爲可用的選項：

- **Contains**。將執行子字串搜尋。傳回屬性值包含指定搜尋字串的項目。例如，如果您知道群組的名稱可能包含單字「Administrator」，請使用此選項及搜尋字串「Administrator」來尋找群組項目。
- **Is**。導致找到完全相符項目。當您知道群組屬性的精確值時，請使用此選項。例如，您知道群組名稱的正確拼寫。
- **Isn't**。傳回屬性值與搜尋字串不完全相符的所有項目。如果您想要在目錄中尋找名稱不包含「administrator」的所有群組，請使用此選項。但是，請注意，使用此選項可能導致傳回大量項目。
- **Sounds like**。導致執行近似或音形一致的搜尋。如果您知道屬性的值，但不確定其拼寫，請使用此選項。例如，您不知道群組名稱的拼寫是「Sarret's list」、「Sarette's list」還是「Sarett's list」
- **Starts with**。將執行子字串搜尋。傳回屬性值以指定搜尋字串開頭的所有項目。例如，您知道群組的名稱以「Product」開頭，但不知道名稱的其餘部分。
- **Ends with**。將執行子字串搜尋。傳回屬性值以指定搜尋字串結尾的所有項目。例如，您知道群組的名稱以「development」結尾，但不知道名稱的其餘部分。

在右側的文字欄位中，輸入搜尋字串。若要顯示 [Look Within] 目錄中包含的所有群組項目，請輸入星號 (*) 或保留此欄位爲空白。

編輯群組項目

▼ 編輯群組項目

下列程序僅適用於 LDAP 服務。

1. **存取 Administration Server，然後按一下 [Users and Groups] 標籤。**
2. **按一下 [Manage Groups] 連結。**
3. **找出您要編輯的群組，如第 57 頁的 「尋找群組項目」中所述。**
4. **依需要變更。**

   如需有關特定欄位及按鈕的更多資訊，請參閱線上說明。

備註 – 您可能想要變更群組編輯頁面未顯示的屬性值。在這種情況下，請使用目錄伺服器 `ldapmodify` 指令行公用程式 (如果可用)。

增加群組成員

▼ 將成員增加至群組

下列程序僅適用於 LDAP 服務。

1. **存取 Administration Server，然後按一下 [Users and Groups] 標籤。**
2. **按一下 [Manage Groups] 連結。**
3. **找出並顯示您要管理的群組，如第 57 頁的 「尋找群組項目」中所述，然後按一下 [Group Members] 旁邊的 [Edit] 按鈕。**

   顯示的頁面上會列出所有現有的群組成員。也會顯示搜尋欄位。

   - 若要將使用者項目增加至成員清單中，必須在 [Find] 下拉式清單中選取 [Users]。
   - 若要將群組項目增加至群組中，則必須選取 [Groups]。

4. **在 [Matching] 文字欄位中，輸入搜尋字串。提供下列任一選項的資訊：**

   - 名稱。輸入全名或部分名稱。將傳回名稱符合搜尋字串的所有項目。如果未找到這樣的項目，則將傳回所有包含該搜尋字串的項目。如果未找到包含搜尋字串的項目，則將尋找發音類似搜尋字串的所有項目。
   - 使用者 ID。如果只輸入部分使用者 ID，則會傳回包含此字串的所有項目。
   - 電話號碼。如果您僅輸入部分號碼，則將傳回包含以搜尋字串結尾的電話號碼的所有項目。
   - 電子郵件地址。任何包含 at 符號 (@) 的搜尋字串皆會視爲電子郵件地址。如果找不到完全相符項目，則會尋找以搜尋字串開頭的所有電子郵件地址。
   - 在此欄位中輸入星號 (*) 或保留爲空白，可以查看當前您目錄中的所有項目或群組。
   - 任意 LDAP 搜尋篩選器。包含等號 (=) 的任何字串均被視爲搜尋篩選器。

5. **按一下 [Add]，尋找 LDAP 資料庫中所有的相符項目，並將其增加至群組。**
6. **(可選) 如果搜尋傳回任何您不想增加至群組中的項目，請在 [Remove From List] 欄中按一下對應的核取方塊。您也可以建構搜尋篩選器來比對您要從群組中移除的項目，然後按一下 [Remove]。如需更多資訊，請參閱第 60 頁的 「從群組成員清單中移除項目」。**

7 **完成群組成員清單後，請按一下 [Save Changes]。項目即會增加至群組成員清單中。**

將群組增加至群組成員清單

對於 LDAP 服務，您可以在群組的成員清單中增加群組，而不是增加個別的成員。如此一來，屬於已包括之群組的所有使用者，都會成爲接收群組的成員。例如，如果 Neil Armstrong 是「Engineering Managers」群組的成員，而您使「Engineering Managers」群組成爲「Engineering Personnel」群組的成員，則 Neil Armstrong 也是「Engineering Personnel」群組的成員。

若要將群組增加至另一群組的成員清單，請像增加使用者項目一樣增加群組。如需更多資訊，請參閱第 59 頁的 「增加群組成員」。

從群組成員清單中移除項目

此程序僅適用於 LDAP 服務。

▼ 從群組成員清單中移除項目

1 **存取 Administration Server，然後按一下 [Users and Groups] 標籤。**

2 **按一下 [Manage Groups] 連結。**

3 **找出您要管理的群組。**
如需更多資訊，請參閱第 57 頁的 「尋找群組項目」。並按一下 [Group Members] 旁邊的 [Edit] 按鈕。

4 **指出您要移除的成員。**

- 若只要移除少數成員，請在 [Remove From List] 欄中按一下對應的核取方塊。
- 若要根據一般條件來移除成員，請建構搜尋篩選器來比對您要從群組中移除的項目，然後按一下 [Remove]。

如需有關建立搜尋篩選器的更多資訊，請參閱第 59 頁的 「增加群組成員」。

5 **按一下 [Save Changes]。**
項目會從群組成員清單中刪除。

管理所有者

對於 LDAP 服務，群組所有者清單的管理方法與群組成員清單相同。

下表列出本指南中提供更多資訊的主題。

表 4–5 管理所有者

主題	請參閱
將所有者增加至群組	第 59 頁的 「增加群組成員」
將群組增加至所有者清單	第 60 頁的 「將群組增加至群組成員清單」
從所有者清單移除項目	第 60 頁的 「從群組成員清單中移除項目」

管理「另請參閱」

「另請參閱」是與目前的群組可能有關的其他目錄項目的參照。這些參照可讓使用者輕鬆找到與目前群組相關的使用者或其他群組的項目。管理「另請參閱」的方法與管理群組成員清單一樣。

下表列出本指南中提供更多資訊的主題。

表 4–6 管理「另請參閱」

主題	請參閱
將使用者增加至「另請參閱」	第 59 頁的 「增加群組成員」
將群組增加至「另請參閱」	第 60 頁的 「將群組增加至群組成員清單」
從「另請參閱」中移除項目	第 60 頁的 「從群組成員清單中移除項目」

重新命名群組

此程序僅適用於 LDAP 服務。重新命名群組項目時，只會變更群組的名稱。「重新命名群組」功能無法將項目從一個組織單元移至另一個組織單元。例如，一個企業可能具有下列組織：

- Marketing 組織單元和 Product Management 組織單元
- Marketing 組織單元下名爲 Online Sales 的群組

在此範例中，您可以將群組從 Online Sales 重新命名爲 Internet Investments，但您不能如此重新命名：將 Marketing 組織單元下的 Online Sales 重新命名爲 Product Management 組織單元下的 Online Sales。

▼ 重新命名群組

1 **存取 Administration Server，然後按一下 [Users and Groups] 標籤。**

2 **按一下 [Manage Groups] 連結，找到您要管理的群組，如第 57 頁的 「尋找群組項目」中所述。**

3. **按一下 [Rename Group] 按鈕。**
4. **在顯示的頁面上指定新的群組名稱，然後按一下 [Save Changes]。**

移除群組

此程序僅適用於 LDAP 服務。

▼ 移除群組

1. **存取 Administration Server，然後按一下 [Users and Groups] 標籤。**
2. **按一下 [Manage Groups] 連結。**
3. **找出您要管理的群組，如第 57 頁的 「尋找群組項目」中所述，然後按一下 [Delete Group]。**

備註 – 群組中個別的成員不會被移除。只會移除群組項目。

建立組織單元

對於 LDAP 服務，一個組織單元可以包括許多群組，且通常可以代表分部、部門或其他獨立的實體。DN 可以存在於多個組織單元中。

- 使用 `organizationalUnit` 物件類別可建立新的組織單元。
- 新組織單元辨別名稱的格式如下：

  `ou=`*new organization* `,ou=`*parent organization*`,...,o=` *base organization*`,c=`*country*

▼ 建立組織單元

1. **存取 Administration Server，然後按一下 [Users and Groups] 標籤。**
2. **按一下 [Create Organizational Unit] 連結。**
3. **輸入資訊，然後按一下 [Create]。**

   如需有關特定欄位的更多資訊，請參閱線上說明。

   例如，如果您在 West Coast 組織單元內建立一個稱爲 Accounting 的新組織，且您的基底 DN 爲 `o=Ace Industry, c=US`，則新組織單元的 DN 爲：

```
ou=Accounting,ou=West Coast,o=Ace Industry,c=US
```

管理組織單元

對於 LDAP 服務，可以從 [Administration Server Users and Groups] 標籤的 [Manage Organizational Units] 頁面中編輯和管理組織單元。

本小節包含以下主題：

尋找組織單元

此程序僅適用於 LDAP 服務。

▼ 尋找組織單元

1. **存取 Administration Server，然後按一下 [Users and Groups] 標籤。**

2. **按一下 [Manage Organizational Units] 連結。**

3. **在 [Find Organizational Unit] 欄位中輸入您要尋找的單元的名稱。**
   您可以輸入下列任何值：
   - 名稱。輸入全名或部分名稱。將傳回所有完全符合該搜尋字串的項目。如果未找到這樣的項目，則將傳回所有包含該搜尋字串的項目。如果未找到包含搜尋字串的項目，則將尋找發音類似搜尋字串的所有項目。
   - 使用星號 (*) 可以查看當前您目錄中的所有群組。將此欄位保留空白也可達到相同的結果。
   - 任意 LDAP 搜尋篩選器。包含等號 (=) 的任何字串均被視爲搜尋篩選器。

     或者，您也可以使用 [Find All Units Whose] 區段中的下拉式功能表來縮小搜尋結果範圍。如需更多資訊，請參閱第 64 頁的 「Find All Units Whose」。

4. **在 [Look Within] 欄位中，選取您要在哪個組織單位下搜尋項目。**
   預設爲目錄的根位置 (最上面的項目)。

5. **在 [Format] 欄位中，指定要將輸出格式化以顯示於螢幕，還是列印至印表機。**

6 **在此過程中的任何階段，皆可按一下 [Find] 按鈕。**
螢幕上會顯示符合搜尋條件的所有組織單元。

7 **按一下您要顯示的項目的連結。**

Find All Units Whose

對於 LDAP 服務，[Find All Units Whose] 區段可讓您建立自訂搜尋篩選器。請使用此區段中的欄位來縮小 [Find Organizational Unit] 所傳回的搜尋結果範圍。

左側的下拉式清單可以指定搜尋所依據的屬性。下列爲可用的選項：

- **Unit name**。搜尋每個項目的全名來尋找相符群組。
- **Description**。搜尋每個組織單元項目的說明來尋找相符項目。

中央的下拉式清單會指定要執行的搜尋類型。下列爲可用的選項：

- **Contains**。將執行子字串搜尋。傳回屬性值包含指定搜尋字串的項目。例如，如果您知道組織單元的名稱可能包含單字「Administrator」，請用此選項及搜尋字串「Administrator」來尋找組織單元項目。
- **Is**。導致找到完全相符項目。當您知道組織單元屬性的精確值時，請使用此選項。例如，您知道組織單元名稱的正確拼寫。
- **Isn't**。傳回屬性值與搜尋字串不完全相符的所有項目。亦即，如果您想要在目錄中尋找名稱不包含「administrator」的所有組織單元，請使用此選項。但是，請注意，使用此選項可能導致傳回大量項目。
- **Sounds like**。導致執行近似或音形一致的搜尋。如果您知道屬性的值，但不確定其拼寫，請使用此選項。例如，您不知道組織單元名稱的拼寫是「Sarret's list」、「Sarette's list」還是「Sarett's list」
- **Starts with**。將執行子字串搜尋。傳回屬性值以指定搜尋字串開頭的所有項目。例如，您知道組織單元的名稱以「Product」開頭，但不知道名稱的其餘部分。
- **Ends with**。將執行子字串搜尋。傳回屬性值以指定搜尋字串結尾的所有項目。例如，您知道組織單元的名稱以「development」結尾，但不知道名稱的其餘部分。

在右側的文字欄位中，輸入搜尋字串。若要顯示 [Look Within] 目錄中包含的所有組織單元項目，請輸入星號 (*) 或保留此欄位爲空白。

編輯組織單元屬性

此程序僅適用於 LDAP 服務。

▼ 編輯組織單元項目

1. **存取 Administration Server，然後按一下 [Users and Groups] 標籤。**
2. **按一下 [Manage Organizational Units] 連結。**
3. **找出您要編輯的組織單元，如第 63 頁的 「尋找組織單元」中所述。**
4. **依需要變更。**
   如需有關特定欄位的更多資訊，請參閱線上說明。

備註 – 若要變更在組織單元編輯頁面中未顯示的屬性值，請使用目錄伺服器 `ldapmodify` 指令行公用程式 (如果可用)。

重新命名組織單元

此程序僅適用於 LDAP 服務。重新命名組織單元項目只會變更組織單元的名稱。無法使用重新命名功能將項目從一個組織單元移至另一個組織單元。

▼ 重新命名組織單元

1. **存取 Administration Server，然後按一下 [Users and Groups] 標籤。**
2. **按一下 [Manage Organizational Units] 連結。**
3. **找出您要編輯的組織單元，如第 63 頁的 「尋找組織單元」中所述。**
4. **按一下 [Rename] 按鈕。**
5. **在顯示的頁面上鍵入新的組織單元名稱，然後按一下 [Save Changes]。**

移除組織單元

此程序僅適用於 LDAP 服務。

▼ 刪除組織單元

1. **存取 Administration Server，然後按一下 [Users and Groups] 標籤。**
2. **按一下 [Manage Organizational Units] 連結。**

3 找出您要刪除的組織單元，如第 63 頁的「尋找組織單元」中所述。

4 按一下 [Delete] 按鈕，然後在出現的確認方塊中按一下 [OK]。

◆ ◆ ◆ 第 5 章

使用憑證和金鑰

本章說明如何使用憑證和金鑰認證來保護 Sun Java System Web Proxy Server 的安全性。Proxy Server 加入了所有 Sun Java System 伺服器的安全性架構，並建立於工業標準和公用協定基礎上，藉此實現最大的互通功能和一致性。

本章假設您對公開金鑰加密的基本概念有一定瞭解，包括加密和解密、公開金鑰和私密金鑰、數位憑證以及加密協定。

本章包含下列小節：

保證 Administration Server 存取的安全性

Administration Server 是一種網路型使用者介面，可用來管理、增加、移除和遷移伺服器，因此需要保護其安全性。

預設的 [Administration Server] 頁面會以 HTTP 模式啓動。[Manage Servers] 標題下列出可用 Proxy Server 實例的清單。若要管理任何 Proxy Server 實例，請按一下清單中的名稱。按一下 Proxy Server 實例的名稱時，即會顯示該實例的 [Server Manager] 頁面。

按一下 [Server Manager] 頁面左上角的 [Manage Servers] 連結，即可從 [Server Manager] 頁面返回至 [Administration Server] 頁面。

安全性功能 (諸如基於憑證的認證，建立信任資料庫、配置 SSL、請求及安裝憑證、設定安全性喜好設定等) 都能套用至 Administration Server 和個別的 Proxy Server 實例。若要對 Administration Server 進行安全性的相關配置，請使用 [Preferences] 標籤，以及出現在 [Administration Server] 頁面上的 [Security] 標籤。若要對 Proxy Server 實例進行安全性的相關配置，請使用 [Preferences] 標籤，以及出現在該代理伺服器實例之 [Server Manager] 頁面上的 [Security] 標籤。

若要以安全模式啓動 Administration Server，必須使用 HTTPS 而非預設的 HTTP 加以存取。

安全性功能將在下列小節中詳細說明。

基於憑證的認證

認證是指確認身分的程序。在網路互動的環境下，認證是一方對另一方進行的信任識別。憑證是支援認證的一種方式。

憑證由數位資料組成，這些資料用於指定個人、公司或其他實體的名稱，並證明憑證中包含的公開金鑰屬於該實體。

用戶端和伺服器都可以擁有憑證。伺服器認證是指用戶端對伺服器所進行的信任識別。亦即識別應負責特定網路位址上伺服器的組織。用戶端認證是由伺服器對用戶端所進行的信任識別，亦即識別應使用用戶端軟體的人。用戶端可以擁有多個憑證，就像使用者可以具有數個不同的識別部分一樣。

憑證是由憑證授權單位 (簡稱 CA) 所核發並加上數位簽名。CA 可以是出售憑證的公司，也可以是負責爲貴公司企業內部網路或企業外部網路核發憑證的部門。您可以決定要將哪些足堪信任的 CA，當作其他使用者身分的驗證者。

憑證所包含的資訊如下。

- 公開金鑰
- 憑證所識別的實體名稱
- 過期日期
- 核發憑證的 CA 名稱
- 核發憑證之 CA 的數位簽名

備註 – 必須首先安裝伺服器憑證，然後才能啓動加密。

建立可信任的資料庫

在請求伺服器憑證之前，您必須建立信任資料庫。在 Proxy Server 中，Administration Server 和每個伺服器實例都可以擁有自己的信任資料庫。信任資料庫只能在本機電腦上建立。

建立信任資料庫時，您需要指定用於金鑰對檔案的密碼。您還需要此密碼來啓動使用加密通訊的伺服器。如需有關選擇密碼時應考量的準則清單，請參閱第 101 頁的「選擇增強式密碼」。

您在信任資料庫中所建立並儲存的公開金鑰和私密金鑰，稱爲金鑰對檔案。金鑰對檔案可用於 SSL 加密。在請求並安裝伺服器憑證時，您需要用到該金鑰對檔案。安裝憑證之後，會將憑證儲存在可信任的資料庫中。

金鑰對檔案會以加密形式儲存於下列目錄中。

server-root/alias/proxy-**serverid**-key3.db

Administration Server 只能有一個信任資料庫。每個伺服器實例都可以擁有自己可信任的資料庫。

▼ 建立信任資料庫

1. **存取 Administration Server 或 Server Manager，然後按一下 [Security] 標籤。**
2. **按一下 [Create Database] 連結。**
3. **鍵入信任資料庫的密碼。**
4. **再次鍵入密碼並按一下 [OK]。**

使用 password.conf

依預設，Proxy Server 會在啓動前，提示管理員鍵入金鑰資料庫密碼。若要重新啓動無人看管狀態的 Proxy Server，您必須將密碼儲存在 `password.conf` 檔案中。僅當您的系統受到適當保護時才能這樣做，以免洩漏該檔案和金鑰資料庫。

一般而言，您無法以 `/etc/ rc.local` 或 `/etc/inittab` 檔案啓動啓用 SSL 的 UNIX 伺服器，因爲該伺服器首先需要密碼，然後才能啓動。儘管將密碼以一般文字格式儲存在

檔案中，即可自動啓動啓用 SSL 的伺服器，但是這種方法並不安全。伺服器的 password.conf 檔案應爲超級使用者或安裝伺服器的使用者所擁有，並且只能讓所有者讀取和寫入。

在 UNIX 上，將啓用 SSL 的伺服器密碼保留在 password.conf 檔案中會帶來很大的安全性風險。任何能夠存取檔案的人，都能存取啓用 SSL 的伺服器密碼。將啓用 SSL 的伺服器密碼保留在 password.conf 檔案中之前，請考量可能帶來的安全性風險。

在 Windows 上，若您有 NTFS 檔案系統，即使您不使用 password.conf 檔案，也應限制存取內含該檔案的目錄以保護此目錄。Administration Server 使用者和 Proxy Server 使用者應該具有該目錄的讀取和寫入權限。保護該目錄可以防止其他使用者建立假的 password.conf 檔案。您無法藉由限制存取的方式，保護 FAT 檔案系統上的目錄或檔案。

自動啓動啓用 SSL 的伺服器

▼ 自動啓動啓用 SSL 的伺服器

1. **請確定 SSL 已經啓用。**
2. **在 Proxy Server 實例的 config 子目錄中，建立新的 password.conf 檔案。**
   - 若您使用的是 Proxy Server 隨附的內部 PKCS #11 軟體加密模組，請鍵入下列資訊：internal: **您的密碼**
   - 如果對硬體加密或硬體加速器使用的是其他 PKCS #11 模組，請指定 PKCS #11 模組名稱，後接密碼，例如：nFast:**您的密碼**

     即使已建立 password.conf 檔案，在啓動 Proxy Server 時，系統仍將一直提示您提供密碼。

使用 Sun Crypto Accelerator 金鑰庫

Sun Crypto Accelerator 4000 卡能夠提供最佳化的可延伸 SSL 操作，速度比系統 CPU 更快。

▼ 配置 Proxy Server 以使用 Sun Crypto Accelerator

1. **安裝 Sun Crypto Accelerator 4000 板。**
2. **初始化 Sun Crypto Accelerator 4000 板。**
3. **安裝 Proxy Server 4.0.8 (最好作為超級使用者)。**

4. **在代理伺服器實例上建立信任資料庫。**
   如需建立信任資料庫的詳細資訊，請參閱第 69 頁的 「建立可信任的資料庫」。

5. **啓用 Sun Crypto Accelerator 4000 板。**

▼ 啓用 Proxy Server 的 Sun Crypto Accelerator 4000 板

1. **使用指令 `secadm` 設定使用者與範圍。**

2. **將目錄「*server-root*`/bin/proxy` 」複製到目錄「*server-root* `/bin/https`」。**
   必須要進行這個步驟來啓用程序檔 `ipsslcfg` 以找出指令 `modutil`。

3. **編輯程序檔 `/opt/SUNWconn/bin/iplsslcfg` 並提供到 `modutil` 的路徑。**

4. **執行 `/opt/SUNWconn/bin/iplsslcfg`。**

5. **選擇選項 `1. 配置 SSL 的 Sun ONE Web Server`。**

   備註 – 選項 `1` 表示 SSL 的 Web Server 配置。也爲 Proxy Server 配置選擇相同的**選項 `1`**。

6. **指定 Proxy Server 4.0.8 安裝目錄並選擇 `y` 來繼續。**
   新增模組 Sun Crypto Accelerator 至資料庫。

7. **重新啓動管理伺服器。**

8. **重新啓動後，選擇 [Security] -> [Request Certificate] -> [Cryptographic Module]。**
   清單會顯示如下：[SUNW acceleration only]、[Internal] 以及 [keystore_name]。清單中每個金鑰庫都有專屬的項目。

9. **選擇金鑰庫。**
   建立伺服器憑證時，請勿選擇選項 [SUNW acceleration only]。

申請和安裝 VeriSign 憑證

VeriSign 是 Proxy Server 首選的憑證授權單位。該公司的技術簡化了憑證請求程序。VeriSign 的優勢在於能夠直接將憑證傳回伺服器。

爲伺服器建立憑證信任資料庫之後，您便可以請求憑證並將其提交給 CA (憑證授權單位)。如果公司有自己的內部 CA，則可以向該部門申請憑證。如果計劃從商業 CA 處購買憑證，請選擇一個 CA 並索要所需的特定格式資訊。

Administration Server 只能有一個伺服器憑證。每個伺服器實例都可以擁有自己的伺服器憑證。

▼ 請求 VeriSign 憑證

1. **存取 Administration Server 或 Server Manager，然後按一下 [Security] 標籤。**
2. **按一下 [Request VeriSign Certificate] 連結。**
3. **檢視所顯示頁面上列出的步驟，然後按一下 [OK]。**
   [VeriSign Enrollment Wizard] 將引導您完成相關程序。

▼ 安裝 VeriSign 憑證

1. **存取 Administration Server 或 Server Manager，然後按一下 [Security] 標籤。**
2. **按一下 [Install VeriSign Certificate] 連結。**
3. **除非您計劃使用外部加密模組，否則請在 [Cryptographic Module] 下拉式清單中選取 [Internal]。**
4. **鍵入金鑰對檔案密碼或 PIN。**
5. **從下拉式清單中選取要擷取的 [Transaction ID]，然後按一下 [OK]。**

申請和安裝其他伺服器憑證

除了 VeriSign 之外，您還可以向其他憑證授權單位請求憑證並加以安裝。貴公司或組織可能會提供自己的內部憑證。本小節說明如何請求和安裝其他類型的伺服器憑證。

本小節包含以下主題：

CA 所需的資訊

在您開始請求程序之前，請確實瞭解 CA 所要求的資訊爲何。CA 所要求的資訊格式雖有不同，但通常會要求您提供下列資訊。這些資訊中的大部分在憑證更新時通常都是不需要的。

- **Requestor name**。核發憑證時接受者的名稱。
- **Telephone number**。請求者的電話號碼。
- **Common name**。用於 DNS 查找的完全合格主機名稱，例如 `www.example.com`。
- **Email address**。您與 CA 進行通訊時所用的公務用電子郵件地址。
- **Organization**。公司、教育機構、組織等的正式法定名稱。大部分的 CA 都要求以法律文件 (如營業執照副本) 驗證此資訊。
- **Organizational unit**。公司內部組織單位的描述。
- **Locality**。組織所在的城市、地區或國家的描述。
- **State or Province**。企業所在的州或省。
- **Country**。ISO 格式的國家或地區名稱的雙字元縮寫。例如，美國的國家代碼爲 US。

所有資訊會合併成一系列的屬性值組合 (稱爲辨別名稱 (DN))，用於唯一識別憑證的主體。

如果從商業 CA 處購買憑證，則必須在 CA 核發憑證之前與之聯絡，以查明他們所需的其他資訊。多數 CA 都要求您提供身分證明。例如，CA 需要驗證您的公司名稱，以及公司授權由誰管理伺服器，並且可能會詢問您是否具有所提供資訊的合法使用權限。

某些商業 CA 向出具較爲詳細身分證明的組織或個人提供內容更爲詳細、準確的憑證。例如，您可以購買一份憑證，宣告 CA 已經驗證您是 `www.example.com` 電腦的合法管理員，此外您的公司已營業三年，並且無尚在審理中的客戶訴訟案件。

申請其他伺服器憑證

▼ 請求其他伺服器憑證

1. **存取 Administration Server 或 Server Manager，然後按一下 [Security] 標籤。**
2. **按一下 [Request Certificate] 連結。**
3. **指定這是新的憑證，還是更新的憑證。**

   許多憑證在固定時間 (例如六個月或一年) 後會過期。某些 CA 會自動給您傳送一個更新的憑證。
4. **指定您要如何提交憑證請求：**
   - 若要使用電子郵件提交請求，請選取 [CA Email Address]，並爲這些請求輸入適用的電子郵件地址。
     - 若要使用 CA 的網站提交請求，請選取 [CA URL]，並爲此類請求鍵入相應的 URL。

5 **從 [Cyptographic Module] 下拉式清單中，選取請求憑證時，要用於金鑰對檔案的加密模組。**

6 **鍵入金鑰對檔案的密碼。**

除非您選取的並非內部加密模組，否則在建立信任資料庫時便會指定此密碼。伺服器會使用該密碼來取得您的私密金鑰，並加密要傳送至 CA 的訊息。接著伺服器會將您的公開金鑰和加密的訊息傳送至 CA。CA 會使用公開金鑰爲您的訊息解密。

7 **提供您的識別資訊，如姓名和電話號碼。**

此資訊的格式因 CA 而異。這些資訊中的大部分在憑證更新時通常都是不需要的。

8 **再次檢查您的資訊以確保準確性，然後按一下 [OK]。**

資訊越準確，批準憑證的速度可能就越快。如果請求是發送至憑證伺服器，則在提交請求前，會提示您驗證表單資訊。

伺服器會產生包含您的資訊之憑證申請。該申請包含透過私密金鑰建立的數位簽名。CA 使用數位簽名來驗證該請求在從伺服器電腦路由至 CA 的過程中未被竄改。只有在極少數情況下請求才會遭到竄改，此時 CA 通常會透過電話與您連絡。

如果選擇以電子郵件傳送請求，則伺服器會傳送一則電子郵件訊息，內含向 CA 提出的請求。一般而言，憑證接著就會以電子郵件方式傳送給您。如果已指定連結至憑證伺服器的 URL，您的伺服器便會使用此 URL 向憑證伺服器提交請求。您可能會收到以電子郵件或其他方式傳來的回應，視 CA 而定。

CA 會通知是否同意將憑證核發給您。多數情況下，CA 透過電子郵件傳送您的憑證。如果您的組織使用的是憑證伺服器，也許可以使用憑證伺服器的表單來搜尋憑證。

備註 – 並非每個從商業 CA 處申請憑證的使用者都會取得憑證。許多 CA 在核發憑證之前，都會要求您提供身分證明。另外，核准時間快則一天，慢則數星期才會完成。您負責向 CA 快速提供所有必要資訊。

收到憑證後立即安裝。在此期間，您仍然可以使用未啓用 SSL 的 Proxy Server。

安裝其他伺服器憑證

CA 所傳來的憑證會以您的公開金鑰加密，因此只有您可以將其解密。只有輸入信任資料庫的正確密碼，才能解密並安裝您的憑證。

憑證包括下列三種類型：

- 您自己伺服器上用於提供給用戶端的憑證
- CA 本身用於憑證鏈的憑證
- 可信任的 CA 憑證

憑證鏈是由連續憑證授權單位簽署的一系列階層式憑證。CA 憑證用於識別憑證授權單位，並用來簽署該授權單位所核發的憑證。反過來，CA 憑證又可以由父 CA 的 CA 憑證簽名，如此類推，直到根 CA。

備註 – 如果 CA 未自動將其憑證傳送給您，請主動提出請求。許多 CA 會在電子郵件中放入他們的憑證和您的憑證，而您的伺服器將同時安裝這兩個憑證。

CA 所傳來的憑證會以您的公開金鑰加密，因此只有您可以將其解密。安裝該憑證時，Proxy Server 將使用您指定的金鑰對檔案密碼將其解密。如以下程序所述，您可以將電子郵件儲存在伺服器可以存取的位置上，也可以複製電子郵件的文字，並準備將其貼到 [Install Certificate] 表單中。

▼ 安裝其他伺服器憑證

1. **存取 Administration Server 或 Server Manager，然後按一下 [Security] 標籤。**
2. **按一下 [Install Certificate] 連結。**
3. **在 [Certificate For] 旁，選取要安裝的憑證類型：**
   - 本伺服器
     - 伺服器憑證鏈
     - 憑證授權單位

     如需有關特定設定的更多資訊，請參閱線上說明。
4. **從下拉式清單中選取加密模組。**
5. **鍵入金鑰對檔案密碼。**
6. **如果您在步驟 3 中選取 [Server Certificate Chain] 或 [Certification Authority]，則請鍵入憑證名稱。**
7. **執行下列任一操作以提供憑證資訊：**
   - 選取 [Message Is In This File]，然後鍵入內含 CA 憑證的檔案的完整路徑名稱。
     - 選取 [Message Text] (含標頭)，然後複製並貼上 CA 憑證的內容。請確實納入 [Begin Certificate] 和 [End Certificate] 標頭，包括開頭和結尾的連字符。
8. **按一下 [OK]。**
9. **指出是要增加新的憑證還是更新現有憑證。**
   - [Add Certificate]，如果要安裝新憑證。

- [Replace Certificate]，如果要安裝更新的憑證。
  憑證將儲存在伺服器的憑證資料庫中。例如：
  server-root/alias/ proxy-*serverid*-cert8.db

遷移先前版本的憑證

從 Sun ONE Web Proxy Server 3.6 (亦稱爲 iPlanet Web Proxy Server) 遷移至 Sun Java System Web Proxy Server 4 時，包括信任資料庫和憑證資料庫在內的檔案都會自動更新。

請確定 Proxy Server 4 Administration Server 對舊的 3.x 資料庫檔案具有讀取權限。這些檔案包括位於 *3.x-server-root*/alias 目錄中的 *alias*-cert.db 和 *alias*-key.db。

只有在伺服器啓用安全性的情況下，才會遷移金鑰對檔案和憑證。您也可以使用 Administration Server 和 Server Manager 中 [Security] 標籤下的 [Migrate 3.x Certificates] 選項，使金鑰和憑證自行遷移。如需有關特定設定的資訊，請參閱線上說明。

在先前版本中，多個伺服器實例是使用別名來參照憑證和金鑰對檔案。Administration Server 管理全部的別名及別名所包含的憑證。在 Sun Java System Web Proxy Server 4 中，Administration Server 和每個伺服器實例都有自己的憑證和金鑰對檔案，稱爲信任資料庫，而非別名。

Administration Server 爲自己管理信任資料庫及資料庫包含的憑證，Server Manager 則爲伺服器實例管理信任資料庫及資料庫包含的憑證。憑證和金鑰對資料庫檔案是根據使用它們的伺服器實例加以命名的。如果是在先前版本中，多個伺服器實例共用同一個別名，則遷移時會根據新的伺服器實例，重新命名憑證和金鑰對檔案。

將遷移與伺服器實例關聯的整個可信任的資料庫。所有列在先前資料庫中的 CA 都會遷移至 Proxy Server 4 資料庫中。如果出現重複的 CA，請使用以前的 CA，直到它過期。請勿嘗試刪除重複的 CA。

Proxy Server 3.x 憑證會遷移至受支援的網路安全性服務 (NSS) 格式。憑證的命名是根據用來存取該憑證的 Proxy Server 頁面而定，也就是從 Administration Server 的 [Security] 標籤或是 Server Manager 的 [Security] 標籤。

▼ 遷移憑證

1. **從本機電腦存取 Administration Server 或 Server Manager，然後選取 [Security] 標籤。**
2. **按一下 [Migrate 3.x Certificates] 連結。**
3. **指定用來安裝 3.6 伺服器的根目錄。**
4. **指定此電腦的別名。**

5 **鍵入管理員的密碼，然後按一下 [OK]。**

使用內建根憑證模組

Proxy Server 隨附的可動態載入根憑證模組，包含多個 CA (包括 VeriSign 在內) 的根憑證。根憑證模組可以讓您將根憑證升級到更高的版本，且方法較以往更容易。以前，您需要逐一刪除舊的根憑證，然後再逐一安裝新的根憑證。若要安裝眾所皆知的 CA 憑證，現在您只要將根憑證模組檔案更新至更高的版本，因爲它在未來版本的 Proxy Server 中都可使用。

由於根憑證已實作爲 PKCS #11 加密模組，因此您永遠無法刪除它所包含的根憑證。管理這些憑證時，並不會出現刪除選項。若要從伺服器實例中移除根憑證，請刪除伺服器 `alias` 目錄中的下列項目，以停用根憑證模組：

- `libnssckbi.so` (在多數 UNIX 平台上)
- `nssckbi.dll` (在 Windows 上)

若要復原根憑證模組，您可以將該延伸從 *server-root*`/bin/proxy/lib` (UNIX) 或 *server-root*`\\ bin\\proxy\\bin` (Windows) 複製到 `alias` 子目錄。

可以修改根憑證的信任資訊。信任資訊將寫入正在編輯的伺服器實例的憑證資料庫中，而非返回至根憑證模組本身。

管理憑證

對於自己的憑證和伺服器上安裝之 CA 所核發的憑證，您可以針對其信任設定加以檢視、刪除或編輯。

▼ 管理憑證

1 **存取 Administration Server 或 Server Manager，然後按一下 [Security] 標籤。**

2 **按一下 [Manage Certificates] 連結。**

- 如果要使用內部加密模組管理預先配置的憑證，將會顯示所有已安裝憑證的清單，其中包括憑證的類型和有效日期。所有憑證都儲存在 *server-root*`/alias` 目錄中。
  - 如果使用的是外部加密模組 (如硬體加速器)，則必須先鍵入每個特定模組的密碼，然後按一下 [OK]。憑證清單將會更新，以便在模組中包含這些憑證。

3 **按一下您要管理的憑證名稱。**

此時會出現內含該憑證類型之管理選項的頁面。只有 CA 憑證才允許您設定或取消設定用戶端信任。某些外部加密模組將不允許刪除憑證。

4 **指定必要的動作**。

下列爲可用的選項：

- [Delete certificate] 或 [Quit]，適用於內部取得的憑證
- [Set client trust]、[Unset server trust] 或 [Quit]，適用於 CA 憑證

憑證資訊中包含所有者和核發憑證的機構。信任設定允許您設定用戶端信任或取消設定伺服器信任。以 LDAP 伺服器憑證來說，您必須設定信任該伺服器。

安裝和管理 CRL 和 CKL

憑證撤銷清單 (CRL) 和洩漏金鑰清單 (CKL) 宣告用戶端或伺服器使用者不應再信任的所有憑證和金鑰。如果憑證中的資料發生變更 (例如某使用者在憑證過期之前調職或離職)，則該憑證將被撤銷，其資料將出現在 CRL 中。如果金鑰被竄改或被洩漏，則該金鑰及其資料將顯示在 CKL 中。CRL 和 CKL 都由 CA 產生並定期更新。請與特定的 CA 連絡以取得這些清單。

本小節說明如何安裝及管理 CRL 和 CKL。

▼ 安裝 CRL 或 CKL

1 **從 CA 取得 CRL 或 CKL 並下載至本機目錄**。

2 **存取 Administration Server 或 Server Manager，然後按一下 [Security] 標籤**。

3 **按一下 [Install CRL/CKL] 連結**。

4 **選取以下任一選項**：

- Certificate Revocation List
- Compromised Key List

5 **鍵入相關檔案的完整路徑名稱，然後按一下 [OK]**。

此時會出現 [Add Certificate Revocation List] 或 [Add Compromised Key List] 頁面，列出 CRL 或 CKL 的資訊。如果資料庫中已存在 CRL 或 CKL，螢幕上會顯示 [Replace Certificate Revocation List] 或 [Replace Compromised Key List] 頁面。

6 **增加或替代 CRL 或 CKL**。

▼ 管理 CRL 和 CKL

1. **存取 Administration Server 或 Server Manager，然後按一下 [Security] 標籤。**
2. **按一下 [Manage CRL/CKL] 連結。**
   此時會出現 [Manage Certificate Revocation Lists /Compromised Key Lists] 頁面，列出所有已安裝的 CRL 和 CKL 及其過期日期。
3. **從 [Server CRLs] 或 [Server CKLs] 清單中選取憑證。**
4. **選取 [Delete CRL] 或 [Delete CKL] 以刪除 CRL 或 CKL。**
5. **退出並返回至管理頁面**

設定安全性喜好設定

一旦取得憑證之後，即可開始保護伺服器的安全性。Sun Java System Web Proxy Server 提供了多種安全性元素，在本小節中將對其加以討論。

加密是指轉換資訊的程序，以便除了指定的收件者之外的其他任何人無法理解此資訊。解密是指轉換加密資訊的程序，讓資訊再次變得能夠理解。Proxy Server 支援安全通訊端層 (SSL) 和傳輸層安全性 (TLS) 加密協定。

密碼是一種加密演算法 (數學函數) ，用於加密或解密。SSL 和 TLS 協定包含大量密碼組。有些密碼會比其他密碼更強、更安全。一般而言，密碼使用的位元越多，解密資料便越困難。

在任何雙向加密程序中，雙方都必須使用相同的密碼。由於有大量密碼可供使用，因此必須讓伺服器使用最常用的密碼。

在安全連線時，用戶端和伺服器一致使用雙方均具有的最強密碼來進行通訊。您可以從 SSL 2.0、SSL 3.0 和 TLS 協定中選擇密碼。

備註 – 在 SSL 2.0 之後，SSL 的安全性和效能進行了各種改進。除非用戶端無法使用 SSL 3.0，否則請勿使用 SSL 2.0。用戶端憑證不一定適用 SSL 2.0 加密。

僅加密程序本身不足以確保伺服器的機密資訊安全。金鑰必須搭配加密密碼一起使用，才能產生實際的加密效果，或是爲先前加密的資訊進行解密。加密程序使用兩個金鑰來達到這個效果：公開金鑰和私密金鑰。使用公開金鑰加密的資訊只能透過相關聯的私密金鑰進行解密。公開金鑰附屬於憑證一起發佈。僅相關聯的私密金鑰才會受到保護。

如需有關各種密碼組的說明以及金鑰和憑證的更多資訊，請參閱「SSL 簡介」。

您可以指定伺服器可以使用的密碼。除非您有不使用特定密碼的充分理由，否則應該選取全部密碼。不過建議您不要啓用未採用最佳化加密的密碼。

注意 – 請勿選取 [Enable No Encryption, Only MD5 Authentication]。如果用戶端沒有其他可用的密碼，伺服器會預設爲使用此設定，因此不進行任何加密。

本小節包含以下主題：

SSL 和 TLS 協定

Proxy Server 支援用於加密通訊的 SSL 和 TLS 協定。SSL 和 TLS 與應用程式無關，並且可以在其上放置更高層級的協定 (不需設定)。

SSL 和 TLS 協定支援多種密碼，這些密碼用於讓伺服器和用戶端互相認證、傳輸憑證以及建立階段作業金鑰。用戶端和伺服器可以支援各種密碼組或密碼集，這取決於各種因素，例如所支援的協定、公司有關加密強度的策略以及政府對加密軟體的出口限定。在其他函式中，SSL 和 TLS 交換協定將決定伺服器和用戶端如何協商以確定將用於通訊的密碼組。

使用 SSL 與 LDAP 通訊

您應該要求 Administration Server 使用 SSL 與 LDAP 進行通訊。

備註 – 在此情況下，Proxy Server 扮演 SSL 用戶端的角色，且必須已匯入用來簽署 SSL 伺服器 LDAP 憑證的根 CA 憑證。若 LDAP 的 SSL 憑證不是由眾所皆知的 CA 核發，則必須將所使用的 CA 根金鑰匯入 Proxy Server 金鑰庫中。

▼ 在 Administration Server 上以 SSL 連線啓用 LDAP

1. **存取 Administration Server，然後按一下 [Global Settings] 標籤。**
2. **按一下 [Configure Directory Service] 連結。**

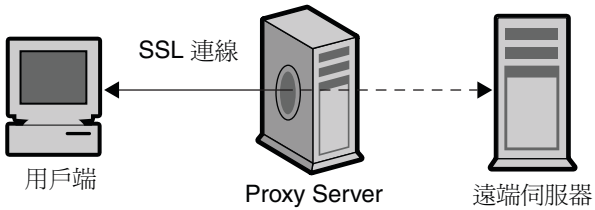
3 **在所顯示的表格中，按一下目錄服務連結。**

此時會顯示 [Configure Directory Service] 頁面。若尚未建立 LDAP 型的目錄服務，請從 [Create New Service of Type] 下拉式清單中選取 [LDAP Server]，然後按一下 [New] 以配置目錄服務。如需有關 LDAP 型目錄服務所顯示之特定欄位的更多資訊，請參閱線上說明。

4 **選取 [Yes]、使用 SSL 進行連線，然後按一下 [Save Changes]。**

經由 Proxy Server 進行 SSL 通道傳輸

向前執行 Proxy Server (代理伺服器)，並且用戶端請求經由代理伺服器與安全伺服器進行 SSL 連線時，代理伺服器會開啓與安全伺服器的連線，並在不干預安全作業事件的情況下，進行雙向資料複製。此程序稱爲 SSL 通道傳輸，並在下圖中說明。



Proxy Server 爲 SSL 作業事件建立通道

圖 5–1 SSL 連線

若要以 HTTPS URL 使用 SSL 通道傳輸，用戶端必須同時支援 SSL 和 HTTPS。HTTPS 是使用 SSL 和一般 HTTP 進行實作的。不支援 HTTPS 的用戶端仍可使用 Proxy Server 的 HTTPS 代理處理功能存取 HTTPS 文件。

SSL 通道傳輸爲較低層級的活動，並不會影響應用程式層級 (HTTPS)。SSL 通道傳輸和沒有使用代理伺服器的 SSL 一樣安全。存在於兩者之間的代理伺服器並不會以任何方式影響安全性，或是降低 SSL 的功能。

使用 SSL 會將資料流加密，以致代理伺服器無法存取實際的作業事件。因此，存取記錄便無法列出來自遠端伺服器的狀態碼或標頭長度。此程序也能防止代理伺服器或任何第三方竊聽作業事件。

由於代理伺服器絕對看不到資料，因此無法驗證用戶端和遠端伺服器之間所使用的通訊協定是否爲 SSL。因此代理伺服器也無法防止其他協定由此通過。您應該限定 SSL 連線僅連接至眾所皆知的 SSL 連接埠，即網際網路網址分配機構 (IANA) 所指定的連接埠 443 (針對 HTTPS) 和 563 (針對 SNEWS)。若網站在其他連接埠上執行安全伺服器，則可以使用 `connect://.*` 資源明訂例外，允許連線至特定主機的其他連接埠。

SSL 通道傳輸功能實際上是與協定無關、類似 SOCKS 的一般功能，因此也可以將此功能用於其他服務。除 HTTPS 和 SNEWS 協定外，Proxy Server 還可以爲支援 SSL 的所有應用程式處理 SSL 通道傳輸。

配置 SSL 通道傳輸

下列程序說明如何配置 Proxy Server 以進行 SSL 通道傳輸。

▼ 配置 SSL 通道傳輸

1. **從 Server Manager 存取伺服器實例，然後按一下 [Routing] 標籤。**
2. **按一下 [Enable/Disable Proxying] 連結。**
3. **從下拉式清單中選取 `connect://.*.443` 資源。**

   `connect://` 方法爲內部代理伺服器表示法，該表示法在代理伺服器外部並不存在。如需有關 `connect` 的更多資訊，請參閱第 82 頁的 「SSL 通道傳輸的技術詳細資訊」。

   若要允許連線至其他連接埠，可以在範本中使用類似的 URL 式樣。如需有關範本的更多資訊，請參閱第 16 章 「管理範本和資源」。
4. **選取 [Enable Proxying Of This Resource]，然後按一下 [OK]。**

注意 – 如果代理伺服器配置錯誤，則可能會有人利用伺服器，使 telnet 連線看似來自代理主機而不是實際的連線主機。因此，請勿使用超過絕對必要數量的連接埠，並請對代理伺服器使用存取控制以限制用戶端主機。

SSL 通道傳輸的技術詳細資訊

SSL 通道傳輸在內部使用 `CONNECT` 方法時，以目標主機名稱和連接埠號爲參數，後跟空白行：

```
CONNECT energy.example.com:443 HTTP/1.0
```

下列範例顯示的是來自 Proxy Server 的成功回應，後跟空白行：

```
HTTP/1.0 200 Connection establishedProxy-agent:
Sun-Java-System-Web-Proxy-Server/4.0
```

接著就會在用戶端和遠端伺服器之間建立連線。資料可進行雙向傳輸，直至其中一方關閉連線。

從內部來看，爲了使根據 URL 式樣的一般配置機制發揮優點，主機名稱和連接埠號會自動對映至 URL，如下所示：

```
connect://energy.example.com:443
```

connect:// 是 Proxy Server 所使用的內部表示法，用於簡化配置，並與其他 URL 式樣更爲一致。在 Proxy Server 的外部，connect URL 並不存在。若 Proxy Server 從網路收到此類 URL，則會將其標記爲無效，並拒絕服務該請求。

為偵聽通訊端啓用安全性

您可以透過執行下列作業來保護伺服器偵聽通訊端的安全性：

- 開啓安全性
- 爲偵聽套接字選取伺服器憑證
- 選取密碼

備註 – 您只能在反向代理模式中啓用安全性，不能在正向代理模式中啓用。

開啓安全性

必須先開啓安全性，然後才能爲偵聽通訊端配置其他安全性設定。您可以在建立新偵聽通訊端或編輯現有偵聽通訊端時開啓安全性。

▼ 建立偵聽通訊端時開啓安全性

1. **存取 Administration Server 或 Server Manager，然後按一下 [Preferences] 標籤。**
2. **按一下 [Add Listen Socket] 連結。**
3. **提供所需的資訊。**

備註 – 建立偵聽通訊端之後，使用 [Edit Listen Sockets] 連結來配置安全性設定。

---

4. **若要開啓安全性，請從 [Security] 下拉式清單中選取 [Enabled]，然後按一下 [OK]。**

   如果尚未安裝伺服器憑證，則只能選擇 [Disabled]。如需有關特定設定的更多資訊，請參閱線上說明。

▼ 編輯偵聽通訊端時開啓安全性

1. **存取 Administration Server 或 Server Manager，然後按一下 [Preferences] 標籤。**
2. **按一下 [Edit Listen Sockets] 連結。**
3. **按一下要編輯的偵聽通訊端之連結。**

4 **從 [Security] 下拉式清單中選取 [Enabled]，然後按一下 [OK]。**
如果尚未安裝伺服器憑證，則只能選擇 [Disabled]。

為偵聽通訊端選取伺服器憑證

您可以在 Administration Server 或 Server Manager 中配置偵聽通訊端，以便使用您已申請並安裝的伺服器憑證。

備註 – 必須至少安裝一份憑證。

▼ 為偵聽通訊端選取伺服器憑證

1 **存取 Administration Server 或 Server Manager，然後按一下 [Preferences] 標籤。**

2 **按一下 [Edit Listen Sockets] 連結。**

3 **按一下要編輯的偵聽通訊端之連結。**

4 **從 [Security] 下拉式清單中選取 [Enabled]，然後按一下 [OK]。**
如果尚未安裝伺服器憑證，則只能選擇 [Disabled]。

5 **從 [Server Certificate Name] 下拉式清單中，為偵聽通訊端選取伺服器憑證，然後按一下 [OK]。**

選取密碼

若要保護 Proxy Server 的安全性，應該啓用 SSL。您可以啓用 SSL 2.0、SSL 3.0 和 TLS 加密協定並選取各種密碼組。可以在 Administration Server 的偵聽通訊端上啓用 SSL 和 TLS 協定。在 Server Manager 的偵聽通訊端上啓用 SSL 和 TLS，即可設定特定伺服器實例的相關安全性喜好設定。必須至少安裝一份憑證。

備註 – 您必須將 Proxy Server 配置爲執行反向代理伺服器功能，才能在偵聽通訊端上啓用 SSL。

預設設定允許大多數常用密碼。除非有充分理由不使用特定密碼組，否則應該選取全部密碼。

[TLS Rollback] 的預設和建議設定皆爲 [Enabled]。此設定可將伺服器配置爲可偵測「中間人版本回復」的攻擊企圖。爲了與某些未正確實作 TLS 規格的用戶端實現互通功能，可能需要將 [TLS Rollback] 設定爲 [Disabled]。

停用 [TLS Rollback] 將導致連線無法抵擋版本回復的攻擊。版本回復攻擊機制讓第三方強制用戶端和伺服器使用較舊、較不安全的協定 (如 SSL 2.0) 進行通訊。由於 SSL 2.0 協定有已知缺陷，若無法偵測「版本回復」的攻擊企圖，第三方便更容易截取已加密的連線並進行解密。

▼ 啓用 SSL 和 TLS

1. **存取 Administration Server 或 Server Manager，然後按一下 [Preferences] 標籤。**
2. **按一下 [Edit Listen Sockets] 連結，然後按一下要編輯的偵聽通訊端連結。**

   對於安全的偵聽通訊端，系統會顯示可用的密碼設定。

   若未啓用偵聽通訊端的安全性，則不會列出 SSL 和 TLS 資訊。若要使用密碼，請確定已在選取的偵聽套接字上啓用了該安全性。如需更多資訊，請參閱第 83 頁的「爲偵聽通訊端啓用安全性」。
3. **選取與所需加密設定對應的核取方塊，然後按一下 [OK]。**
4. **為 Netscape Navigator 6.0 同時選取 TLS 和 SSL 3.0。此外也為 [TLS Rollback] 選取 [TLS]，並確認 SSL 3.0 和 SSL 2.0 皆已停用。**

   一旦在伺服器上啓用 SSL 之後，其 URL 便會使用 `https` 而非 `http`。指向啓用 SSL 伺服器上文件的 URL 格式如下： `https://`*servername*`.`*domain* `.`*dom*`:` *port*，例如 `https://admin.example.com:443`

   如果使用預設的安全 HTTP 連接埠 (443)，則不需要在 URL 中輸入連接埠號。

全域配置安全性

安裝啓用 SSL 的伺服器時，會在 `magnus.conf` 檔案 (全域安全性參數的伺服器主要配置檔案) 中建立指令項目。

SSLSessionTimeout

`SSLSessionTimeout` 指令用於控制 SSL 2.0 階段作業的快取，其語法爲：

`SSLSessionTimeout` *seconds*

其中 *seconds* 是快取的 SSL 階段作業保持有效的秒數。預設值爲 100。如果指定了 `SSLSessionTimeout` 指令，秒數的值將自動限定爲 5 到 100 秒之間。

SSLCacheEntries

指定可以快取的 SSL 階段作業的數目。

SSL3SessionTimeout

SSL3SessionTimeout 指令用於控制 SSL 3.0 和 TLS 階段作業快取，其語法爲：

SSL3SessionTimeout *seconds*

其中 *seconds* 是快取的 SSL 3.0 階段作業保持有效的秒數。預設值爲 86400 秒 (24 小時)。如果指定了 SSL3SessionTimeout 指令，秒數的值將自動限定爲 5 到 86400 秒之間。

▼ 設定 SSL 配置檔案指令的值

1. **從 Server Manager 存取伺服器實例。**
2. **確定為要配置的偵聽套接字啓用了安全性。**
   如需更多資訊，請參閱第 83 頁的 「爲偵聽通訊端啓用安全性」。
3. **手動編輯 magnus.conf 檔案，並為下列設定提供值：**
   - SSLSessionTimeout
   - SSLCacheEntries
   - SSL3SessionTimeout

   如需有關 magnus.conf 的更多資訊，請參閱「Sun Java System Web Proxy Server 4.0.8 Configuration File Reference」。

使用外部加密模組

Proxy Server 支援下列使用外部加密模組 (如智慧卡或記號環網路) 的方法：

- PKCS #11
- FIPS-140

啓動 FIPS-140 加密標準之前，必須增加 PKCS #11 模組。

本小節包含以下主題：

安裝 PKCS #11 模組

Proxy Server 支援公開金鑰加密標準 (PKCS) #11，該標準定義在 SSL 和 PKCS #11 模組之間通訊所使用的介面。PKCS #11 模組用於與 SSL 硬體加速器建立標準連結。所匯入的外部硬體加速器之憑證和金鑰儲存在 secmod.db 檔案中，此檔案是在安裝 PKCS #11 模組時產生的。此檔案位於 *server-root*/alias 目錄中。

使用 modutil 工具安裝 PKCS #11 模組

您可以使用 modutil 工具，以 .jar 檔案或物件檔案的形式安裝 PKCS #11 模組。

▼ 使用 modutil 工具安裝 PKCS #11 模組

1. **確定包括 Administration Server 在內的所有伺服器都已停止。**
2. **移至包含資料庫的** *server-root*/alias **目錄。**
3. **將** *server-root*/bin/proxy/admin/bin **增加到 PATH 中。**
4. **在** *server-root*/bin/proxy/admin/bin **中找到** modutil。
5. **設定環境。**
   - 在 UNIX 上：setenv

     LD_LIBRARY_PATH *server-root*/bin/proxy/lib:${LD_LIBRARY_PATH}
   - 在 Windows 上，將以下內容增加到 PATH 中

     LD_LIBRARY_PATH *server-root*/bin/proxy/bin

     您可以在 *server-root*/proxy-admserv/start 下找到電腦的 PATH。
6. **在終端機視窗中，鍵入** modutil。

   將列出各種選項。
7. **執行所需的動作。**

   例如，若要在 UNIX 中增加 PKCS #11 模組，請輸入：

   modutil -add (*PKCS#11* **檔案的名稱**) -libfile (*PKCS #11* **的** *libfile*) -nocertdb -dbdir . (**您的** *db* **目錄**)

使用 pk12util 工具匯出

使用 pk12util 可讓您從內部資料庫匯出憑證和金鑰，並將其匯入內部或外部 PKCS #11 模組。您可以將憑證和金鑰始終匯出至內部資料庫，但多數外部記號不會允許\您匯出憑證和金鑰。依預設，pk12util 使用名爲 cert8.db 和 key3.db 的憑證和金鑰資料庫。

▼ 從內部資料庫匯出憑證和金鑰

1. **移至包含資料庫的** *server-root*/alias **目錄。**
2. **將** *server-root*/bin/proxy/admin/bin **增加到 PATH 中。**

3. **在** *server-root*/bin/proxy/admin/bin **中找到** pk12util。

4. **設定環境**。
   - 在 UNIX 上：

     setenv LD_LIBRARY_PATH/ *server-root*/bin/proxy/lib:${LD_LIBRARY_PATH}
   - 在 Windows 上，將以下內容增加到 PATH 中

     LD_LIBRARY_PATH *server-root*/bin/proxy/bin

     您可以在下列目錄下找到電腦的 PATH： *server-root*/proxy-admserv/start。

5. **在終端機視窗中，鍵入** pk12util。

   將列出各種選項。

6. **執行所需的動作**。

   例如，在 UNIX 中鍵入

   ```
   pk12util -o certpk12 -n Server-Cert [-d /server/alias] [-P https-test-host]
   ```

7. **鍵入資料庫密碼**。

8. **鍵入** pkcs12 **密碼**。

▼ 將憑證和金鑰匯入內部或外部 PKCS #11 模組

1. **移至包含資料庫的** *server-root*/alias **目錄**。

2. **將** *server-root*/bin/proxy/admin/bin **增加到 PATH 中**。

3. **在** *server-root*/bin/proxy/admin/bin **中找到** pk12util。

4. **設定環境**。

   例如：
   - 在 UNIX 上：

     setenv LD_LIBRARY_PATH/ *server-root*/bin/proxy/lib:${LD_LIBRARY_PATH}
     - 在 Windows 上，將以下內容增加到 PATH 中

       LD_LIBRARY_PATH *server-root*/bin/proxy/bin

       您可以在 *server-root*/proxy-admserv/start 下找到電腦的 PATH。

5. **在終端機視窗中，鍵入** pk12util。

   將列出各種選項。

6. **執行所需的動作。**

   例如，在 UNIX 中輸入：

   ```
   pk12util -i pk12_sunspot [-d certdir][-h “nCipher”][-P
   https-jones.redplanet.com-jones-]
   ```

   `-P` 必須跟在 `-h` 之後，且爲最後一個引數。

   鍵入正確的記號名稱，包括大寫字母和引號之間的空格。

7. **鍵入資料庫密碼。**

8. **鍵入 `pkcs12` 密碼。**

使用外部憑證啓動伺服器

如果伺服器憑證安裝至外部 PKCS #11 模組 (例如硬體加速器) 中，將無法使用該憑證來啓動伺服器，除非編輯 `server.xml` 檔案，或是依下述方式指定憑證名稱。

伺服器會自動嘗試使用名爲 Server-Cert 的憑證進行啓動。然而，外部 PKCS #11 模組中的憑證，會在其識別碼中包括模組的其中一個記號名稱。例如，安裝於外部智慧卡讀取器上名爲 `smartcard0` 的伺服器憑證，就會命名爲 `smartcard0:Server-Cert`。

若要使用安裝在外部模組中的憑證啓動伺服器，必須爲伺服器執行所在的偵聽通訊端指定憑證名稱。

▼ 選取偵聽通訊端的憑證名稱

如果未啓用偵聽通訊端的安全性，則不會列出憑證資訊。若要選取偵聽通訊端的憑證名稱，必須先確定已在該偵聽通訊端上啓用安全性。如需更多資訊，請參閱第 83 頁的「爲偵聽通訊端啓用安全性」。

1. **存取 Administration Server 或 Server Manager，然後按一下 [Preferences] 標籤。**

2. **按一下 [Edit Listen Sockets] 連結。**

3. **按一下要與憑證建立關聯的偵聽通訊端連結。**

4. **從 [Server Certificate Name] 下拉式清單中，選取偵聽通訊端的伺服器憑證，然後按一下 [OK]。**

   該清單包含所有已安裝的內部和外部憑證。

   您也可以藉由手動編輯 `server.xml` 檔案，要求伺服器改用該伺服器憑證啓動。 將 `SSLPARAMS` 中的 `servercertnickname` 屬性變更爲：

   ```
   $TOKENNAME:Server-Cert
   ```

若要尋找 $TOKENNAME 應使用的值，請移至伺服器的 [Security] 標籤，並選取 [Manage Certificates] 連結。登入到儲存 Server-Cert 的外部模組時，$TOKENNAME:$NICKNAME 表單的清單中將顯示其憑證。

如果未建立信任資料庫，則在請求或安裝外部 PKCS #11 模組的憑證時，會自動建立一個。建立的預設資料庫沒有密碼，且無法存取。外部模組可以工作，但您不能申請和安裝伺服器憑證。如果已建立沒有密碼的預設資料庫，請使用 [Security] 標籤上的 [Create Database] 頁面來設定密碼。

FIPS-140 標準

透過 PKCS#11 API，您可以與執行加密作業的軟體或硬體模組進行通訊。一旦將 PKCS #11 安裝在 Proxy Server 上之後，即可將伺服器配置爲遵守 FIPS-140 標準。FIPS 代表聯邦資訊處理標準。只有 SSL 3.0 才包含這些程式庫。

▼ 啓用 FIPS-140

1. **依據 FIPS-140 中的說明安裝該 Plug-in**。
2. **存取 Administration Server 或 Server Manager，然後按一下 [Preferences] 標籤**。
3. **按一下 [Edit Listen Sockets] 連結**。
   對於安全偵聽通訊端，[Edit Listen Sockets] 頁面會顯示可用的安全性設定。
   若要使用 FIPS-140，請確定已在選取的偵聽套接字上啓用了該安全性。如需更多資訊，請參閱第 83 頁的 「爲偵聽通訊端啓用安全性」。
4. **從 [SSL Version 3] 下拉式清單中選取 [Enabled] (如果尚未選取)**。
5. **選取適當的 FIPS-140 密碼組，然後按一下 [OK]**：
   - 啓用168 位元加密的三重 DES 和 SHA 認證 (FIPS)。
     - 啓用 56 位元加密的 DES 和 SHA 認證 (FIPS)。

設定用戶端安全性需求

執行所有步驟保護伺服器的安全性之後，即可爲用戶端設定其他安全性需求。

用戶端認證對於 SSL 連線並非必要，但卻能加強確保加密資訊能傳送給正確的收件人。您可以在反向代理伺服器中使用用戶端認證，以確定您的內容伺服器不會與未經授權的代理伺服器或用戶端共用資訊。

本小節包含以下主題：

要求用戶端認證

您可以爲 Administration Server 和每個伺服器實例啓用偵聽通訊端，以要求用戶端認證。啓用用戶端認證時，需要提供用戶端憑證，然後伺服器才能針對查詢傳送回應。

Proxy Server 支援的用戶端憑證認證方式，是將用戶端憑證中的 CA，與可信任 CA (能簽署用戶端憑證) 加以比對。您可以藉由 [Security] 標籤，在 [Manage Certificates] 頁面上檢視可信任 CA (能簽署用戶端憑證) 的清單。

您可以對 Proxy Server 進行配置，拒絕不具有來自可信任 CA 用戶端憑證的所有用戶端。若要接受或拒絕信任的 CA，必須爲 CA 設定用戶端信任。如需更多資訊，請參閱第 77 頁的 「管理憑證」。

若憑證已過期，Proxy Server 會記錄錯誤、拒絕憑證並向用戶端傳回訊息。您也可以在 [Manage Certificates] 頁面上檢視哪些憑證已經過期。

您可以對伺服器進行配置，以便從用戶端憑證收集資訊並使其與 LDAP 目錄中的使用者項目匹配。此程序可以確定用戶端具有有效的憑證，且在 LDAP 目錄中有對應項目。而且還可以確定用戶端憑證與 LDAP 目錄中的憑證相匹配。若要瞭解如何執行此操作，請參閱第 94 頁的 「將用戶端憑證對映到 LDAP」。

您可以將用戶端憑證和存取控制結合使用，以便除了來自可信任的 CA 以外，與憑證關聯的使用者還必須與存取控制規則 (ACL) 相匹配。如需更多資訊，請參閱第 139 頁的 「使用存取控制檔案」。

▼ 申請用戶端認證

1. **存取 Administration Server 或 Server Manager，然後按一下 [Preferences] 標籤。**
2. **按一下 [Edit Listen Sockets] 連結。**
3. **按一下要求用戶端認證的偵聽通訊端連結。**
4. **使用 [Client Authentication] 下拉式清單要求針對偵聽通訊端進行用戶端認證，然後按一下 [OK]。**

反向代理伺服器中的用戶端認證

在反向代理伺服器中，您可以根據下列任一分析藍本配置用戶端認證：

- **Proxy-Authenticates-Client**。在此分析藍本下，您可允許具有可接受憑證的所有用戶端進行存取，或是僅允許具有可接受憑證，且爲 Proxy Server 存取控制清單上可辨識之使用者的用戶端進行存取。

  備註 – 代理伺服器必須具有 CA 的使用者根金鑰，或已簽署使用者憑證之自我簽署應用程式的使用者根金鑰。使用者必須已載入 CA 的 Proxy Server 根金鑰，或已簽署 Proxy Server 憑證之自我簽署應用程式的 Proxy Server 根金鑰。

- **Content-Server-Authenticates-Proxy**。在此分析藍本下，您可確保內容伺服器是連接至 Proxy Server 而非其他伺服器。

  備註 – 代理伺服器必須具有 CA 的內容伺服器根金鑰，或已簽署內容伺服器憑證之自我簽署應用程式的內容伺服器根金鑰。內容伺服器必須具有 CA 的 Proxy Server 根金鑰，或已簽署 Proxy Server 憑證之自我簽署應用程式的 Proxy Server 根金鑰。

- **Proxy-Authenticates-Client and Content-Server-Authenticates-Proxy**。此分析藍本可爲您的反向代理伺服器提供最佳的安全性和認證。

如需有關如何配置這些分析藍本的資訊，請參閱第 92 頁的 「在反向代理伺服器中設定用戶端認證」 。

在反向代理伺服器中設定用戶端認證

安全反向代理伺服器中的用戶端認證可以進一步確保連線的安全。下列指示說明如何根據所選擇的分析藍本配置用戶端認證。

備註 – 每個分析藍本都假設您同時具有安全的用戶端至代理伺服器連線，以及代理伺服器至內容伺服器連線。

▼ 配置 Proxy-Authenticates-Client 分析藍本

1. **請依照第 14 章 「使用反向代理伺服器」 中「設定反向代理伺服器」的指示，配置安全的用戶端至代理伺服器以及安全的代理伺服器至內容伺服器分析藍本。**
2. **從 Server Manager 存取伺服器實例，然後按一下 [Preferences] 標籤。**
3. **按一下 [Edit Listen Sockets] 連結，然後在所顯示的表格中，按一下所需偵聽通訊端的連結。**

   (使用 [Add Listen Socket] 連結可配置和增加偵聽通訊端。)

4 **指定用戶端認證需求：**

a. **若要允許具有有效憑證之所有使用者進行存取，請執行下列操作：**

在 [Security] 區段中，使用 [Client Authentication] 設定來要求對此偵聽通訊端進行用戶端認證。如果尚未安裝伺服器憑證，則不會顯示此設定。

b. **若要僅允許具有有效憑證，且在存取控制中指定為可接受使用者的使用者進行存取，請執行下列操作：**

i. **在 [Security] 區段中，保持 [Client Authentication] 設定為關閉狀態。如果尚未安裝伺服器憑證，則不會顯示此設定。**

ii. **在此伺服器實例的 Server Manager [Preferences] 標籤上，按一下 [Administer Access Control] 連結。**

iii. **選取 [ACL]，然後按一下 [Edit] 按鈕。**

此時會顯示 [Access Control Rules For] 頁面 (若出現提示則請先認證)。

iv. **開啓存取控制 (若尚未選取 [Access control Is On] 核取方塊，請加以選取)。**

v. **將 Proxy Server 設定為以反向代理伺服器身分進行認證。**

如需更多資訊，請參閱第 288 頁的 「設定反向代理伺服器」。

vi. **在所需的存取控制規則上按一下 [Rights] 連結，於下方框架內指定存取權限，然後按一下 [Update] 更新此項目。**

vii. **按一下 [Users/Groups] 連結。在下方框架中，指定使用者和群組、選取 SSL 做為認證方法，然後按一下 [Update] 更新此項目。**

viii. **在上方框架中按一下 [Submit] 以儲存項目。**

如需有關設定存取控制的更多資訊，請參閱第 8 章 「控制對伺服器的存取」。

▼ 配置 Content Server-Authenticates-Proxy 分析藍本

1 **請依照第 288 頁的 「設定反向代理伺服器」中的指示，配置安全的用戶端至代理伺服器以及安全的代理伺服器至內容伺服器分析藍本。**

2 **在內容伺服器上開啓用戶端認證。**

您可以修改此分析藍本，建立用戶端與 Proxy Server 之間的不安全連線，以及與內容伺服器的安全連線，這樣內容伺服器便會對此 Proxy Server 進行認證。若要執行上述操作，必須關閉加密功能，並要求代理伺服器僅依照以下所述的程序初始化憑證。

▼ 配置 Proxy-Authenticates-Client and Content Server-Authenticates-Proxy 分析藍本

1 **請依照第 92 頁的「配置 Proxy-Authenticates-Client 分析藍本」中的指示，配置 Proxy-Authenticates-Client 分析藍本。**

2 **在內容伺服器上開啓用戶端認證。**

將用戶端憑證對映到 LDAP

本小節說明 Proxy Server 採用何種程序，將用戶端憑證對映至 LDAP 目錄中的項目。將用戶端憑證對映至 LDAP 之前，還必須配置必要的 ACL。如需更多資訊，請參閱第 8 章「控制對伺服器的存取」。

伺服器收到來自用戶端的請求時，會在處理前索取用戶端的憑證。某些用戶端會在向伺服器傳送申請的同時傳送用戶端憑證。

伺服器將嘗試檢視該 CA 是否與 Administration Server 中的某個可信任 CA 匹配。如果不存在相符的項目，Proxy Server 將會結束連線。如果存在相符的項目，伺服器將繼續處理請求。

伺服器驗證憑證是來自可信任的 CA 之後，便會透過執行下列操作將憑證對映至 LDAP 項目：

- 將核發者和主體 DN 從用戶端憑證對映至 LDAP 目錄中的分支點。
- 在 LDAP 目錄中，搜尋與用戶端憑證的主體 (一般使用者) 相關資訊相符的項目。
- (可選) 驗證用戶端憑證是否與 LDAP 項目中對應於 DN 的憑證相符。

伺服器使用憑證對映檔案 (稱爲 `certmap.conf`) 來確定 LDAP 搜尋的執行方式。對映檔案將告知伺服器要採用用戶端憑證中的哪些值，如一般使用者名稱、電子郵件地址等。伺服器將使用這些值來搜尋 LDAP 目錄中的使用者項目，但伺服器必須先確定要從 LDAP 目錄中的何處開始搜尋。憑證對映檔案也會告訴伺服器開始搜尋的位置。

一旦伺服器知道從何處開始搜尋以及所搜尋的內容之後，便會在 LDAP 目錄 (第二個點) 中執行搜尋。如果找不到任何相符項目或找到多個相符項目，並且**未**設定對映必須驗證憑證，則搜尋將會失敗。

下表列出了預期的搜尋結果運作方式。您可以在 ACL 中指定預期的運作方式。例如，您可以指定找不到相符憑證時，Proxy Server 就只接受您。如需有關如何設定 ACL 喜好設定的更多資訊，請參閱第 139 頁的「使用存取控制檔案」。

表 5–1 LDAP 搜尋結果

LDAP 搜尋結果	憑證驗證「開啓」	憑證驗證「關閉」
未找到項目	認證失敗	認證失敗
恰好找到一個項目	認證失敗	認證成功
找到多個項目	認證失敗	授權失敗

伺服器在 LDAP 目錄中找到相符的項目和憑證之後，即可使用該資訊處理作業事件。例如，某些伺服器使用憑證到 LDAP 的對映來確定對某個伺服器的存取權限。

使用 certmap.conf 檔案

憑證對映用於確定伺服器在 LDAP 目錄中查找使用者項目的方式。您可以使用 certmap.conf 檔案來配置將憑證 (依名稱指定) 對映至 LDAP 項目的方式。您可以編輯此檔案並增加項目，以便與 LDAP 目錄的組織相符，並列出您希望使用者擁有的憑證。您可根據 subjectDN 中所使用的使用者 ID、電子郵件地址或其他值，對使用者進行認證。特別是，對映檔案可定義以下資訊：

- 伺服器應從 LDAP 樹狀結構中開始搜尋的位置
- 在 LDAP 目錄中進行搜尋時，伺服器應該做爲搜尋條件的憑證屬性
- 伺服器是否要執行其他驗證程序

憑證對映檔案位於以下位置：

server-root/userdb/certmap.conf

該檔案包含了一個或多個已命名對映，每個對映都套用於不同的 CA。對映具有下列語法：

certmap *name issuerDNname* :*property* [*value*]

第一行用於指定項目的名稱以及形成 CA 憑證中區別名稱的屬性。*name* 爲任意名稱，可依照您的喜好加以定義。不過，*issuerDN* 必須與核發用戶端憑證之 CA 的核發者 DN 完全相符。例如，以下兩個核發者 DN 行僅在分隔屬性的空格上有所差異，但伺服器將其視爲兩個不同的項目：

```
certmap sun1 ou=Sun Certificate Authority,o=Sun,c=UScertmap sun2 ou=Sun
Certificate Authority, o=Sun, c=US
```

備註 – 如果您使用的是 Sun Java System Directory Server，在確定核發者 DN 符合情況遇到問題時，請檢查 Directory Server 錯誤記錄以取得有用的資訊。

已命名對映中的第二行和隨後的行可以使屬性與值相匹配。certmap.conf 檔案具有六項預設特性。您也可以使用憑證 API 來自訂特性。預設特性爲：

- DNComps 是逗號分隔的屬性清單，用於確定伺服器從 LDAP 目錄中的何處開始搜尋與使用者 (即用戶端憑證的所有者) 資訊相符的項目。伺服器從用戶端憑證中收集這些屬性的值，並用這些值形成 LDAP DN，然後即可確定伺服器從 LDAP 目錄的哪個位置開始搜尋。例如，如果 DNComps 設定爲要使用 DN 的 o 和 c 屬性，伺服器就會從 LDAP 目錄中的 o=*org*, c= *country* 項目開始搜尋，其中 *org* 和 *country* 會以憑證中 DN 的值替代。

  請注意以下情形：

  - 如果對映中沒有 DNComps 項目，則伺服器會使用 CmapLdapAttr 設定或用戶端憑證中的整個主體 DN，也就是一般使用者的資訊。
  - 如果 DNComps 項目存在但沒有對應的值，伺服器將在整個 LDAP 樹狀結構中搜尋與篩選器相符的項目。

  FilterComps 是逗號分隔的屬性清單，藉由收集用戶端憑證中使用者 DN 的資訊來建立篩選器。伺服器將使用這些屬性的值，以形成匹配 LDAP 目錄中各項目的搜尋條件。如果伺服器在 LDAP 目錄中找到的一個或多個項目，與從憑證中收集到的使用者資訊相符，則表示搜尋成功，且伺服器選擇性地執行驗證。

  例如，如果將 FilterComps 設定爲要使用電子郵件地址和使用者 ID 屬性 (FilterComps=e,uid)，伺服器會在目錄中搜尋這樣的項目：其電子郵件及使用者 ID 值與從用戶端憑證所收集的一般使用者資訊相符合。電子郵件地址和使用者 ID 是很好的篩選器，因爲它們在目錄中通常是唯一的項目。篩選器必須夠具體，才能在 LDAP 資料庫中找到一個 (且只有一個) 符合項目。

  篩選器的屬性名稱必須是來自憑證 (而非來自 LDAP 目錄) 的屬性名稱。例如，某些憑證以 e 屬性代表使用者的電子郵件地址，而 LDAP 將此屬性稱爲 mail。

  下表列出了 x509v3 憑證的屬性。

表 5–2 x509v3 憑證的屬性

屬性	說明
c	國家/地區
o	組織
cn	共用名稱
l	位置
st	狀態
ou	組織單元
uid	UNIX/Linux 使用者 ID
電子郵件	電子郵件地址

- `verifycert` 會告知伺服器是否應將用戶端憑證與 LDAP 目錄中的憑證相比對。此特性採用以下兩個值：[on] 和 [off]。只有當 LDAP 目錄中包含憑證時才使用此特性。此功能有助於確定一般使用者所具有的憑證是否有效且未被撤銷。
- `CmapLdapAttr` 是 LDAP 目錄中包含使用者全部憑證之主體 DN 的屬性名稱。該特性的預設值爲 `certSubjectDN`。該屬性不是標準的 LDAP 屬性，因此要使用該特性，您必須延伸 LDAP 模式。如需更多資訊，請參閱「SSL 簡介」。

  如果 `certmap.conf` 檔案中存在此特性，伺服器將在整個 LDAP 目錄中，搜尋其屬性 (以此特性命名) 與主體之完整 DN (從憑證中取得) 相符的項目。如果找不到任何項目，伺服器會使用 `DNComps` 和 `FilterComps` 對映重試搜尋。

  如果使用 `DNComps` 和 `FilterComps` 進行項目比對非常困難，這就是比對憑證和 LDAP 項目的實用方式。
- `Library` 是共用程式庫或 DLL 的路徑名稱。只有在使用憑證 API 建立您自己的特性時，才使用此特性。
- `InitFn` 爲自訂程式庫中 `init` 函數的名稱。只有在使用憑證 API 建立您自己的特性時，才使用此特性。

如需有關這些特性的更多資訊，請參閱第 97 頁的 「對映範例」中所述範例。

建立自訂特性

用戶端憑證 API 可用來建立您自己的特性。建立自訂對映後，就可以參照以下格式的對映：

name`:library` *path_to_shared_libraryname* `:InitFN` *name_of_ init_function*

例如：

```
certmap default1 o=Sun Microsystems, c=US default1:library
/usr/sun/userdb/plugin.so default1:InitFn plugin_init_fn default1:DNComps ou o
c default1:FilterComps l default1:verifycert on
```

對映範例

`certmap.conf` 檔案中應至少包含一個項目。下列範例說明了 `certmap.conf` 的不同使用方式。

範例 #1 只有一個預設對映的 `certmap.conf` 檔案

```
certmap default defaultdefault:DNComps ou, o, cdefault:FilterComps e,
uiddefault:verifycert on
```

以此爲例，伺服器在包含 `ou=`*orgunit*, `o=`*org*, `c=`*country* 項目的 LDAP 分支點開始搜尋，其中斜體文字將由用戶端憑證中主體 DN 的值所替代。

然後，伺服器會使用憑證上電子郵件地址和使用者 ID 的值，在 LDAP 目錄中搜尋相符的項目。找到相符的項目時，伺服器會比對用戶端傳送的憑證與儲存在目錄中的憑證，以驗證該憑證。

範例 #2 具有兩個對映的 certmap.conf 檔案

以下範例檔案中包括兩個對映：一個用於預設，另一個用於美國郵政局。

```
certmap default defaultdefault:DNCompsdefault:FilterComps e, uid

certmap usps ou=United States Postal Service, o=usps, c=USusps:DNComps
ou,o,cusps:FilterComps eusps:verifycert on
```

伺服器收到美國郵政局以外的人傳來憑證時會使用預設對映，該對映會從 LDAP 樹狀結構的頂層開始，搜尋與用戶端電子郵件地址和使用者 ID 相符的項目。如果憑證來自美國郵政服務，則伺服器會從包含組織單位的 LDAP 分支開始搜尋相符的電子郵件地址。此外，伺服器還會驗證該憑證。其他憑證則不加以驗證。

注意 – 憑證中的核發者 DN (即 CA 的資訊) 必須與對映第一行中所列的核發者 DN 相同。在前一個範例中，來自核發者 DN (即 `o=United States Postal Service,c=US`) 的憑證就不相符，因爲 DN 中 `o` 和 `c` 屬性之間沒有空格。

範例 #3 搜尋 LDAP 資料庫

下列範例使用 `CmapLdapAttr` 特性在 LDAP 資料庫中搜尋名爲 `certSubjectDN` 的屬性，該屬性的值與用戶端憑證中的整個主體 DN 完全相符。本範例假設 LDAP 目錄中包含具有 `certSubjectDN` 屬性的項目。

```
certmap myco ou=My Company Inc, o=myco, c=USmyco:CmapLdapAttr
certSubjectDNmyco:DNComps o, c myco:FilterComps mail, uid myco:verifycert on
```

如果用戶端憑證的主題爲：

```
uid=Walt Whitman, o=LeavesOfGrass Inc, c=US
```

伺服器將首先搜尋包含以下資訊的項目：

```
certSubjectDN=uid=Walt Whitman, o=LeavesOfGrass Inc, c=US
```

如果找到一個或多個匹配的項目，伺服器將繼續驗證各項目。如果找不到相符的項目，伺服器會使用 `DNComps` 和 `FilterComps` 來搜尋相符的項目。在本範例中，伺服器會在 `o=LeavesOfGrass Inc, c=US` 之下的所有項目中搜尋 `uid=Walt Whitman`。

設定更強密碼

透過 Server Manager [Preferences] 標籤中的 [Set Cipher Size] 選項可以選擇使用 168 位元、128 位元或 56 位元大小的祕密金鑰進行存取，或者不予限制。您可以指定不符合限定條件時使用的檔案。如果未指定檔案，Proxy Server 會傳回「Forbidden」狀態。

如果所選取的存取用金鑰大小與 [Security Preferences] 下目前的密碼設定不一致，Proxy Server 會警告您需要啓用金鑰大小更大的密碼。

金鑰大小限制的實作是根據 `obj.conf` 中的 NSAPI `PathCheck` 指令，而不是 `Service fn=key-toosmall`。該指令爲：

```
PathCheck fn="ssl-check" [secret-keysize=nbits ] [bong-file=filename ]
```

其中，*nbits* 是所需的最小秘密金鑰位元數，*filename* 是不符合限定條件時所提供的檔案名稱。

若未啓用 SSL，或是未指定 `secret-keysize` 參數，則 `PathCheck` 會傳回 `REQ_NOACTION`。如果目前階段作業的秘密金鑰大小小於指定的 `secret-keysize`，在未指定 `bong-file` 的情況下，函數會傳回 `REQ_ABORTED` 以及 `PROTOCOL_FORBIDDEN` 狀態。如果指定了 `bong-file`，則函數會傳回 `REQ_PROCEED`，而路徑變數會設定爲 `bong-file` *filename*。而且，如果不符合金鑰大小限制，目前階段作業的 SSL 階段作業快取項目將失效，這樣下次當同一個用戶端連線到伺服器時，將發生完整的 SSL 訊號交換。

備註 – 在 [Set Cipher Size] 表單中增加 `PathCheck fn=ssl-check` 時，表單會移除在物件中找到的所有 `Service fn=key-toosmall` 指令。

▼ 設定更強的加密

1. **從 Server Manager 存取伺服器實例，然後按一下 [Preferences] 標籤。**
2. **按一下 [Set Cipher Size] 連結。**
3. **從下拉式清單中選取要套用更強密碼的資源，然後按一下 [Select]。您也可以指定常規表示式。**
   如需更多資訊，請參閱第 16 章「管理範本和資源」。
4. **選取金鑰大小的限定：**
   - 168 位元或更大
     - 128 位元或更大
     - 56 位元或更大
     - 無限定

5 **指定要拒絕存取的訊息檔案所在位置，然後按一下 [OK]。**

如需有關密碼的更多資訊，請參閱「SSL 簡介」。

其他安全性考量

除了某些人會嘗試破解您的加密外，還有其他安全性風險存在。網路面臨的風險來自外部和內部的駭客，他們使用各種方法嘗試存取您的伺服器以及伺服器上的資訊。除了在伺服器上啓用加密外，還應採取額外的安全防護措施。例如，將伺服器電腦放在安全的房間內，不允許任何不可信任的使用者將程式上傳至您的伺服器。本小節說明幾項能讓伺服器更安全無虞的重要措施。

本小節包含以下主題：

限制實體存取

這種簡單的安全方法經常會被遺忘。將伺服器電腦放在上鎖的房間中，只有經過授權的人才能進入。此一策略可以防止任何人攻擊伺服器電腦本身。而且要保護好電腦的管理 (root) 密碼 (如果有)。

限制管理存取權

如果使用遠端配置，請確定設定了存取控制，以便只對少數使用者和電腦進行管理。如果您要讓 Administration Server 提供一般使用者對 LDAP 伺服器或本機目錄資訊的存取權限，請考慮維護兩部 Administration Server，並使用叢集管理。這樣，啓用 SSL 的 Administration Server 就能當做主伺服器，而另一部 Administration Server 則可提供一般使用者存取。如需有關叢集的更多資訊，請參閱第 6 章 「管理伺服器叢集」。

您還應爲 Administration Server 開啓加密功能。如果未將 SSL 連線用於管理，則透過不安全的網路執行遠端伺服器管理時應該格外小心。因爲任何人都可以截取您的管理密碼並重新配置您的伺服器。

選擇增強式密碼

您可以在伺服器中使用多個密碼：管理密碼、私密金鑰密碼、資料庫密碼等等。管理密碼是最重要的密碼，因爲任何具有該密碼的使用者都可配置電腦上的任何 (和所有) 伺服器。私密金鑰密碼則是次重要的密碼。任何取得私密金鑰和私密金鑰密碼的人，都能建立假伺服器 (僞裝成您的伺服器)，或者截取和變更進出伺服器的通訊資訊。

密碼最好是便於自己記住，他人又無法猜到。例如，您可以將 *MCi12!mo* 記爲「My Child is 12 months old!」小孩的名字或生日則是不良密碼的範例。

建立難以破解的密碼

使用這些準則來建立較強的密碼。不必對一個密碼套用以下所有規則，但使用的規則越多，您的密碼就越難以被破解。提供下列幾個提示：

- 密碼的長度應該介於 6-14 個字元
- 請勿使用非法字元：*、“或空格
- 請勿使用辭典單詞 (任何語言)
- 請勿以常見的方式替換字母，例如以 3 替代 E，或以 1 替代 L
- 盡可能多地包含以下字元：
  - 大寫字母
  - 小寫字母
  - 數字
  - 符號

變更密碼或 PIN

定期變更您的信任資料庫/金鑰對檔案密碼或 PIN。如果在 Administration Server 中啓用 SSL，則啓動伺服器時需要此密碼。定期變更密碼可以增加對伺服器的額外保護。

您只能在本機電腦上變更此密碼。如需變更密碼時應考量的準則清單，請參閱第 101 頁的 「建立難以破解的密碼」。

▼ 變更信任資料庫/金鑰對檔案密碼

1. **存取 Administration Server 或 Server Manager，然後按一下 [Security] 標籤。**
2. **按一下 [Change Key Pair File Password] 連結。**
3. **從 [Cryptographic Module] 下拉式清單中，選取您要變更密碼的安全性代表字元。**
   依預設，內部金鑰資料庫的記號爲 [Internal]。若已安裝 PKCS #11模組，則將列出所有安全性代表字元。

4. **鍵入您目前的密碼。**
5. **鍵入您的新密碼。**
6. **再次鍵入新密碼並按一下 [OK]。**

   請確定您的金鑰對檔案已受到保護。Administration Server 將金鑰對檔案儲存在 *server-root*/alias 目錄中。

   瞭解檔案是否儲存在備份磁帶上，或是否能被其他人截取。如果儲存了該檔案，則必須像保護伺服器一樣盡力保護您的備份。

限制伺服器上的其他應用程式

仔細檢查與伺服器在同一部電腦上執行的所有應用程式。有人可能利用伺服器上執行的其他程式漏洞，避開伺服器的安全性功能。請停用所有不必要的程式和服務。例如，UNIX sendmail 常駐程式很難有安全的配置，因此可將其設定爲在伺服器電腦上執行其他可能有害的程式。

UNIX 和 Linux

仔細選擇從 inittab 和 rc 程序檔啓動的程序。請勿從伺服器電腦執行 telnet 或 rlogin。您亦不應在伺服器電腦上執行 rdist。這除了可用來分布檔案之外，也能用來更新伺服器電腦上的檔案。

Windows

仔細考慮哪些磁碟機和目錄要與其他電腦共用。而且，要考量哪些使用者具有帳號或 Guest 權限。請特別留意在伺服器上安裝的程式，允許其他人在伺服器上安裝程式時也要特別小心。其他人員的程式可能會有安全漏洞。更糟的是有人可能會上傳惡意程式，目的就是破壞您的安全性。在您的伺服器上安裝程式之前一定要仔細檢查這些程式。

防止用戶端快取 SSL 檔案

透過在 HTML 檔案的 <HEAD> 區段中增加以下行，可以防止用戶端快取加密前的檔案：

```
<meta http-equiv="pragma" content="no-cache">
```

限制連接埠

停用電腦上未使用的所有連接埠。使用路由器或防火牆配置以防止與絕對最小連接埠集以外的任何連接埠進行進來的連線。這種保護方法意味著要取得電腦上的 Shell，就只能實際操作已經位於管制區域中的伺服器電腦。

瞭解伺服器的限制

伺服器提供了伺服器和用戶端之間的安全連線。用戶端取得資訊之後，伺服器既無法控制資訊的安全性，也無法控制誰能實際操作伺服器電腦本身及存取其目錄和檔案。

瞭解這些限制有助於您理解要避免哪些情形。例如，您可以透過 SSL 連線取得信用卡號，但這些號碼是否儲存在伺服器電腦上的安全檔案中呢？SSL 連線終止後，這些號碼會怎樣呢？請務必對用戶端透過 SSL 傳送給您的任何資訊實施安全保護。

◆ ◆ ◆ 第 6 章

管理伺服器叢集

本章說明叢集 Sun Java System Web Proxy Server 的概念，並說明如何使用叢集以在伺服器之間共用配置。

本章包含下列小節：

關於伺服器叢集

叢集是指一組 Sun Java System Web Proxy Server，可以從單一 Administration Server 對它們進行管理。每個叢集均必須包含一台指定做爲主 Administration Server 的伺服器。

將伺服器劃分爲幾個叢集可以讓您執行下列動作：

- 建立一個可以集中管理所有 Proxy Server 的位置
- 在伺服器之間共用一個或多個配置檔案
- 由一個主 Administration Server 來啓動與停止所有伺服器
- 檢視特定伺服器的存取記錄與錯誤記錄

叢集的使用準則

請遵循下列使用準則，將 Proxy Server 群組配置爲叢集：

- 必須先安裝要包括在特定叢集內的所有伺服器，才能開始建立叢集。
- 叢集中所有伺服器的類型必須相同 (UNIX 或 Windows)。 叢集必須爲同質叢集。
- 叢集內的所有伺服器均必須爲 Proxy Server 第 4 版。目前僅支援將 Proxy Server 第 4 版伺服器增加至叢集。
- 所有 Administration Server 均必須使用相同的協定 (HTTP 或 HTTPS)。如果變更叢集中某個 Administration Server 的協定，則必須變更所有 Administration Server 的協定。如需更多資訊，請參閱第 108 頁的 「修改伺服器資訊」。
- 所有的特定叢集 Administration Server 必須與主 Administration Server 有相同的使用者名稱與密碼。可以使用分散式管理在各 Administration Server 上配置多個管理員。
- 必須指定一個特定叢集的 Administration Server 做爲主 Administration Server；選擇哪一部伺服器都可以。
- 主 Administration Server 必須對每個特定叢集的 Administration Server 均具有存取權限。主 Administration Server 會擷取所有已安裝 Sun Java System Web Proxy Server 的相關資訊。

設定叢集

以下爲設定 Proxy Server 叢集的一般步驟。

1. 安裝要納入叢集的 Proxy Server。

   請確定此叢集的 Administration Server 之使用者名稱和密碼，可供主 Administration Server 用於認證。您可以使用預設的使用者名稱與密碼，或者配置分散式管理來達到此目的。
2. 安裝將包含主 Administration Server 的 Proxy Server，並確定其使用者名稱與密碼符合步驟 1 中的設定。
3. 將伺服器增加至叢集清單。

   如需更多資訊，請參閱第 107 頁的 「將伺服器增加至叢集」。
4. 管理遠端伺服器有兩種方式：從 [Control Cluster] 頁面存取該伺服器的 Server Manager 介面；或將叢集中某個伺服器的配置檔案複製到另一個伺服器。

將伺服器增加至叢集

將 Proxy Server 增加至叢集時，該伺服器的 Administration Server 及連接埠號就已指定。如果該 Administration Server 包含關於多個伺服器的資訊，則其所有伺服器均會增加至叢集。稍後可個別將伺服器移除。

如果遠端 Administration Server 包含關於叢集的資訊，則不會增加遠端叢集中的伺服器。主 Administration Server 僅增加實際安裝在遠端電腦中的那些伺服器。

▼ 將遠端伺服器增加至叢集

1 **確定已開啓主 Administration Server 的電源。**

2 **存取主 Administration Server，然後按一下 [Cluster] 標籤。**

3 **按一下 [Add Server] 連結。**

4 **選擇遠端 Administration Server 使用的協定。**

- HTTP 用於一般 Administration Server
- HTTPS 用於安全 Administration Server

5 **依照 `magnus.conf` 檔案中的顯示，鍵入遠端 Administration Server 之完整合格的主機名稱，例如 `plaza.example.com`。**

6 **鍵入遠端 Administration Server 的連接埠號。**

7 **鍵入遠端 Administration Server 的管理員使用者名稱與密碼，然後按一下 [OK]。**

主 Administration Server 會嘗試與遠端伺服器連絡。如果連絡成功，就會提示您確認將伺服器增加至叢集。

備註 – 啓用叢集控制時，叢集的主伺服器即會於叢集內每個從屬伺服器的 `proxy-`*`serverid`*`/config/cluster/`*`server-name`*`/proxy-`*`serverid`* 目錄內建立一些檔案。這些檔案均不可配置。

修改伺服器資訊

僅在從屬伺服器上的從屬管理連接埠資訊變更後要加以更新時，才使用 Administration Server 中 [Cluster] 標籤下的 [Modify Server] 選項。如果您變更叢集中遠端 Administration Server 的連接埠號，則還需要修改儲存於叢集中的關於該 Administration Server 的資訊。若從屬 Administration Server 有其他任何變更，則您必須將該伺服器移除，完成變更後再將其重新增加至叢集。

▼ 修改叢集內的伺服器資訊

1. **存取主 Administration Server，然後按一下 [Cluster] 標籤。**
2. **按一下 [Modify Server] 連結。所有伺服器會依唯一的伺服器識別碼順序顯示。**
3. **選取要修改的伺服器，進行必要的變更，然後按一下 [OK]。**

從叢集中移除伺服器

▼ 從叢集中移除伺服器

1. **存取主 Administration Server，然後按一下 [Cluster] 標籤。**
2. **按一下 [Remove Server] 連結。**
3. **選取要從叢集中移除的遠端伺服器，然後按一下 [OK]。**
   移除的伺服器將無法再透過叢集存取。只能透過該伺服器本身的 Administration Server 存取。

控制伺服器叢集

您可利用 Proxy Server 以下列動作控制您叢集內的遠端伺服器：

- 啓動與停止伺服器
- 檢視其存取與錯誤記錄
- 傳輸配置檔案。如果主 Administration Server 具有的 Proxy Server 實例超過一個，則可從這些伺服器中的任意一個，將檔案傳輸到增加至叢集的任何從屬伺服器。叢集必須爲同質叢集。叢集中的所有伺服器必須爲相同類型 (UNIX 或 Windows)。從其他平台傳輸配置檔案可能導致伺服器掛起或當機。配置檔案包括：

- server.xml
- magnus.conf
- obj.conf
- mime.types
- socks5.conf
- bu.conf
- icp.conf
- parray.pat
- parent.pat

▼ 控制叢集中的伺服器

1 **存取主 Administration Server，然後按一下 [Cluster] 標籤。**

2 **按一下 [Control Cluster] 連結。**

3 **選取要控制的伺服器，進行必要的選擇。**

您可以隨時按一下 [Reset] 按鈕，將元素重設爲進行變更之前所包含的值。

- 從下拉式清單中選取 [Start]、[Stop] 或 [Restart]，然後按一下 [Go]。系統會提示您確認動作。
- 從下拉式清單中選取 [View Access] 或 [View Error]，然後輸入記錄檔中，您要檢視的從末端算起行數。按一下 [Go] 以顯示資訊。在所顯示的 [Cluster Execution Report] 中按一下 [View] 按鈕。
- 傳輸配置檔案：
  - 選取要傳輸的配置檔案
  - 選取檔案所在的伺服器
  - 按一下 [Go] 以傳輸資訊

◆ ◆ ◆ 第 7 章

7 配置伺服器喜好設定

本章說明 Proxy Server 的系統設定以及配置方式。系統設定會影響整個 Proxy Server。設定項目包括諸如代理伺服器所使用的使用者帳號及其偵聽的連接埠等選項。

本章包含下列小節：

啓動 Proxy Server

本小節說明如何在不同平台上啓動 Proxy Server。伺服器安裝後，便會偵聽並接受請求。

▼ 從管理介面啓動 Proxy Server

1. **存取 [Server Manager]，然後按一下 [Preferences] 標籤。**
2. **按一下 [Start/Stop Server] 連結。**
   此時會顯示 [Start/Stop Server] 頁面。
3. **按一下 [On] 按鈕。**
   伺服器的狀態會顯示在 [Start/Stop Server] 頁面中。

在 UNIX 或 Linux 上啓動 Proxy Server

您可以使用下列任一方式，在 UNIX 或 Linux 上啓動 Proxy Server：

- 在指令行中，移至 *server-root* `/proxy-server`*id* 並鍵入 `./start` 以啓動 Proxy Server。
- 使用 `start`。若要將此程序檔與 `init` 搭配使用，必須將 `prxy:2: respawn:` *server-root*`/proxy-server`*id* `/start -start -i` 啓動指令納入 `/etc/inittab` 中。

在 Windows 上啓動 Proxy Server

您可以使用下列任一方式，在 Windows 上啓動 Proxy Server

- 使用 [開始] > [程式集] > [Sun Microsystems] > [Sun Java System Web Proxy Server *version*] > [Start Proxy Server]
- 使用 [控制台] > [系統管理工具] > [服務] > [Sun Java System Web Proxy Server 4.0 (proxy-server*id*)] > [啓動]
- 在指令提示符號中，移至 *server-root* `\proxy-server`*id* 並鍵入 `startsvr.bat` 以啓動 Proxy Server。

啓動啓用 SSL 的伺服器

啓動啓用 SSL 的伺服器需要密碼。雖然將密碼以一般文字存放在檔案中可以自動啓動啓用 SSL 的伺服器，但是這種做法有極大的安全性風險。任何能夠存取檔案的人，都能存取啓用 SSL 的伺服器密碼。在將啓用 SSL 的伺服器密碼以一般文字保存之前，請先考慮安全性風險。

伺服器的啓動程序檔、金鑰組檔案及金鑰密碼應由超級使用者所有，或是由安裝此伺服器的非超級使用者之使用者帳號所有，因爲僅只有所有者才可讀取和寫入這些項目。

停止 Proxy Server

本小節說明在不同平台上停止 Proxy Server 的各種方法。

▼ 從管理介面停止 Proxy Server

1. **存取 [Server Manager]，然後按一下 [Preferences] 標籤。**
2. **按一下 [Start/Stop Server] 連結。**
   此時會顯示 [Start/Stop Server] 頁面。
3. **按一下 [Off] 按鈕。**
   伺服器的狀態會顯示在 [Start/Stop Server] 頁面中。

在 UNIX 或 Linux 上停止 Proxy Server

您可以使用下列任一方式，在 UNIX 或 Linux 上停止 Proxy Server：

- 在指令行中，移至 *server-root* `/proxy-server`*id* 並鍵入 `./stop`。

備註 – 如果是使用 `etc/inittab` 檔案重新啓動伺服器，在嘗試停止伺服器之前，必須從 `/etc/inittab` 中移除啓動伺服器的指令行，並鍵入 `kill -1 1`。否則，伺服器在停止後會自動重新啓動。

- 使用 `stop` 可以完全關閉伺服器並中斷服務，直到伺服器重新啓動爲止。如果將 `etc/inittab` 檔案設定爲使用 `respawn` 自動重新啓動，則在關閉伺服器之前，必須移除 `etc/inittab` 中與代理伺服器有關的指令行，否則伺服器會自動重新啓動。

關閉伺服器之後，可能會經過幾秒鐘，伺服器才會完成關機程序，然後其狀態會變更爲 [Off]。

如果發生系統當機或離線的情形，伺服器會停止運作，而其所處理的任何請求都可能會遺失。

備註 – 如果伺服器安裝了安全性模組，則在啓動或停止伺服器之前，需要提供正確的密碼。

在 Windows 上停止 Proxy Server

您可以使用下列任一方式，在 Windows 上停止 Proxy Server：

- 使用 [開始] > [程式集] > [Sun Microsystems] > [Sun Java System Web Proxy Server *version*] > [Stop Proxy Server]
- 在指令提示符號中，移至 *server-root* `\proxy-server`*id* 並鍵入 `stopsvr.bat` 以停止 Proxy Server。
- 在 [服務] 視窗中，使用 Sun Java System Proxy Server 4.0 (proxy-server *id*) 服務：[控制台] > [系統管理工具] > [服務]

重新啓動 Proxy Server

本小節說明在不同平台上重新啓動 Proxy Server 的各種方法。

重新啓動伺服器 (UNIX 或 Linux)

您可以使用下列方法之一重新啓動伺服器：

- 手動重新啓動伺服器。
- 從 `inittab` 檔案自動重新啓動伺服器

  如果使用的 UNIX 或 Linux 版本不是源自 System V (如 SunOS™ 4.1.3)，就不能使用 `inittab` 檔案。
- 在系統重新開機時，使用 `/etc/rc2.d` 中的常駐程式自動重新啓動伺服器。

由於安裝程序檔無法編輯 `/etc/rc.local` 或 `/etc/inittab` 檔案，因此必須使用文字編輯器編輯這些檔案。如果您不瞭解如何編輯這些檔案，請洽詢您的系統管理員或參考系統文件。

▼ 從指令行重新啓動 Proxy Server

1 如果伺服器在編號低於 1024 的連接埠上執行，請以超級使用者身分登入；否則，請以超級使用者身分或使用伺服器使用者帳號登入。

2 在指令行提示處，鍵入下列行並按下 Enter 鍵：

server-root`/proxy-server`*id*`/restart`

其中，*server-root* 是安裝伺服器的目錄。

- 您可以在該行結尾使用選擇性參數 `-i`。如果伺服器程序遭強制結束或當機，`-i` 選項便會以 `inittab` 模式執行伺服器，`inittab` 將爲您重新啓動伺服器。該選項也可防止伺服器將其本身放入後台程序中。

使用 inittab 重新啓動伺服器

在 /etc/inittab 檔案中的一行上增加下列文字：

prxy:23:respawn:*server-root* /proxy-server*id*/start -start -i

其中 *server-root* 是安裝伺服器的目錄，而 proxy-server*id* 則是伺服器的目錄。

-i 選項可防止伺服器將其自身放置在背景程序中。

在停止伺服器之前，您必須移除該行。

使用系統 RC 程序檔重新啓動伺服器

如果使用 /etc/rc.local 或系統中的等效檔案，請將下列一行置入 /etc/rc.local 中：

server-root/proxy-server *id*/start

使用安裝伺服器的目錄替代 *server-root*。

重新啓動伺服器 (Windows)

您可以使用服務控制台或透過完成下列作業來重新啓動伺服器。

▼ 在 Windows 上重新啓動伺服器

1. **使用 [控制台] > [系統管理工具] > [服務]**
2. **從服務清單中，選取 [Sun Java System Web Proxy Server 4.0 (proxy-server *id*)]。**
3. **在 [內容] 視窗中，將 [啓動類型] 變更為 [自動]。這樣系統便會在每次電腦啓動或重新開機時，同時啓動伺服器。**
4. **按一下 [OK]。**

設定終止逾時

當伺服器停止時，將會停止接受新連線。然後，伺服器會等待所有未執行的連線完成。可以在 magnus.conf 檔案中配置伺服器逾時前的等待時間。依預設，該值設定爲 30 秒。若要變更該值，請在 magnus.conf 檔案中增加下列行：

TerminateTimeout *seconds*

其中，*seconds* 表示伺服器在逾時前將等待的秒數。

配置該值的優點是伺服器將等待更長的時間以讓連線完成。然而，由於伺服器經常會開啓與無回應用戶端的連線，因此增加終止逾時可能會增加伺服器關機所需要的時間。

檢視伺服器設定

您在安裝期間爲 Proxy Server 配置了某些設定。您可以從 Server Manager 檢視這些設定和其他系統設定。[View Server Settings] 頁面會列出 Proxy Server 的所有設定。透過此頁面，可以瞭解是否有尚未儲存及尚未套用的變更。如果有尚未儲存的變更，請儲存變更並重新啓動 Proxy Server，以便可以開始使用新配置。

伺服器設定包括技術設定和內容設定兩種類型。伺服器的內容設定是依據伺服器的配置方式而定。一般而言，代理伺服器會列出所有範本、URL 對映和存取控制。對於個別範本，[View Server Settings] 頁面會列出範本名稱、其常規表示式及範本設定，如快取設定。

代理伺服器的技術設定來自 `magnus.conf` 檔案和 `server.xml` 檔案，而內容設定則來自 `obj.conf` 檔案。這些檔案位於伺服器根目錄的 `proxy-`*id*`/config` 子目錄中。

▼ 檢視 Proxy Server 的設定

1. **存取 [Server Manager]，然後按一下 [Preferences] 標籤。**
2. **按一下 [View Server Settings] 連結。**
   此時會顯示 [View Server Settings] 頁面。

檢視並復原配置檔案的備份

您可以檢視或復原配置檔案的備份副本：`server.xml`、`magnus.conf`、`obj.conf`、`mime.types`、`server.xml.clfilter`、`magnus.conf.clfilter`、`obj.conf.clfilter`、`socks5.conf`、`bu.conf`、`icp.conf`、`parray.pat`、`parent.pat`、`proxy-id.acl`。這項功能可以讓您在目前配置出現問題時，返回到先前的配置。例如，如果已對代理伺服器的配置進行數項變更，但之後發現其並未依照預期的方式運作 (例如，您已拒絕對某個 URL 的存取，但是代理伺服器仍處理該請求)，則可以復原至先前的配置，然後重新進行配置變更。

▼ 檢視先前的配置

1. **存取 [Server Manager]，然後按一下 [Preferences] 標籤。**
2. **按一下 [Restore Configuration] 連結。**
   此時會顯示 [Restore Configuration] 頁面。此頁面會依照日期和時間順序，列出先前的所有配置。
3. **按一下 [View] 連結，顯示特定版本的技術和內容設定清單。**

▼ 復原配置檔案的備份副本

1. **存取 [Server Manager]，然後按一下 [Preferences] 標籤。**
2. **按一下 [Restore Configuration] 連結。**
   此時會顯示 [Restore Configuration] 頁面。此頁面會依照日期和時間順序，列出先前的所有配置。
3. **針對要復原的版本，按一下 [Restore] 連結。**
   若要將所有檔案復原至特定時間的狀態，請按一下表格左欄中的 [Restore to *time*] 連結。*time* 是復原的目標日期和時間。

▼ 設定顯示的備份數量

1. **存取 [Server Manager]，然後按一下 [Preferences] 標籤。**
2. **按一下 [Restore Configuration] 連結。**
   此時會顯示 [Restore Configuration] 頁面。
3. **在 [Set Number Of Sets Of Backups] 欄位中，鍵入要顯示的備份數量。**
4. **按一下 [Change] 按鈕。**

配置系統喜好設定

您可以藉由 [Configure System Preferences] 頁面對伺服器的基本層面進行設定或變更。此頁面可以讓您執行下列作業：

- 變更代理伺服器的伺服器使用者、程序數量、偵聽佇列大小、代理逾時以及中斷後的逾時
- 啓用 DNS、ICP、代理伺服器陣列和父系陣列

喜好設定選項包括：

- **Server User**。[Server User] 是指代理伺服器所使用的使用者帳號。您輸入做爲代理伺服器使用者的使用者名稱，應已經以一般使用者帳號的形式存在。伺服器啓動時，其執行方式就像是由該使用者所啓動一樣。

  若要避免建立新的使用者帳號，您可以選擇在相同主機上執行的另一部伺服器所使用的帳號。如果您執行的是 UNIX 代理伺服器，則可以選擇 `nobody` 使用者。然而，在某些系統上，`nobody` 使用者可以擁有檔案但無法執行程式，因此不適合做爲代理伺服器的使用者名稱。

  在 UNIX 系統上，代理伺服器產生的所有程序都會指定給伺服器使用者帳號。
- **Processes**。[Processes] 欄位顯示可用於處理請求的程序數量。預設值爲 1。除非必要，否則請勿修改此設定。
- **Listen Queue Size**。[Listen Queue Size] 欄位用於指定偵聽通訊端上擱置連線的最大數量。
- **DNS**。網域名稱服務 (DNS) 可將 IP 位址復原爲主機名稱。當 Web 瀏覽器連線至伺服器時，伺服器僅會取得用戶端的 IP 位址，例如 `198.18.251.30`。伺服器沒有主機名稱資訊，如 `www.example.com`。進行存取記錄和存取控制時，伺服器可以將 IP 位址解析爲主機名稱。在 [Configure System Preferences] 頁面上，可以指定伺服器是否要將 IP 位址解析爲主機名稱。
- **ICP**。網際網路快取協定 (ICP) 爲訊息傳遞協定，可讓快取記憶體相互進行通訊。快取可以使用 ICP 來傳送有關快取 URL 是否存在，以及擷取這些 URL 最佳位置的查詢與回覆。您可以在 [Configure System Preferences] 頁面上啓用 ICP。如需有關 ICP 的更多資訊，請參閱第 249 頁的 「透過 ICP 鄰近區域路由」。
- **Proxy Array**。代理伺服器陣列是由代理伺服器組成的陣列，它做爲一個快取來達到分散式快取之目的。如果啓用 [Configure System Preferences] 頁面上的代理伺服器陣列選項，表示您所配置的代理伺服器爲代理伺服器陣列的成員，而陣列中其他所有成員都是它的同層代理伺服器。如需有關使用代理伺服器陣列的更多資訊，請參閱第 256 頁的 「透過代理伺服器陣列路由」。
- **Parent Array**。父系陣列是指代理伺服器或代理伺服器陣列成員路經的代理伺服器陣列。因此，如果代理伺服器在存取遠端伺服器之前，路由通過上游代理伺服器陣列，則上游代理伺服器陣列就視爲父系陣列。如需有關將父系陣列與代理伺服器搭配使用的更多資訊，請參閱第 268 頁的 「透過父系陣列路由」。

- **Proxy Timeout**。代理伺服器逾時是指來自遠端伺服器的連續網路資料封包的最大間隔時間，過了這段時間，Proxy Server 就會使請求逾時。代理伺服器逾時的預設值爲 5 分鐘。

備註 – 如果遠端伺服器使用 server-push 且頁面之間的延遲長於代理伺服器逾時，則在完成傳輸之前，便可能會終止連線。請改用 client-pull，它可傳送多項請求至代理伺服器。

▼ 修改系統喜好設定

1. **存取 [Server Manager]，然後按一下 [Preferences] 標籤。**
2. **按一下 [Configure System Preferences] 連結。**
   此時會顯示 [Configure System Preferences] 頁面。
3. **變更選項，然後按一下 [OK]。**
4. **按一下 [Restart Required]。**
   此時會顯示 [Apply Changes] 頁面。
5. **按一下 [Restart Proxy Server] 按鈕以套用變更。**

調校 Proxy Server

您可以藉由 [Tune Proxy] 頁面來變更預設參數，以調校代理伺服器的效能。

▼ 變更預設的調校參數

1. **存取 [Server Manager]，然後按一下 [Preferences] 標籤。**
2. **按一下 [Tune Proxy] 連結。**
   此時會顯示 [Tune Proxy] 頁面。
3. **(可選) 修改 FTP 的清單寬度，以顯示較長的檔案名稱，避免出現檔案名稱截斷的情形。**
   預設寬度爲 80 個字元。
4. **按一下 [OK]。**

5 **按一下 [Restart Required]**。
此時會顯示 [Apply Changes] 頁面。

6 **按一下 [Restart Proxy Server] 按鈕以套用變更**。

增加與編輯偵聽通訊端

伺服器必須透過偵聽通訊端接受請求，然後將請求導向至正確的伺服器，之後才能處理該請求。安裝 Proxy Server 時，會自動建立一個偵聽通訊端 ls1。該偵聽通訊端會使用 IP 位址 `0.0.0.0`，以及在安裝期間指定做爲代理伺服器連接埠號的連接埠號。您無法刪除預設的偵聽通訊端。

- **General**
  - **Listen Socket ID**。偵聽通訊端的內部名稱。建立偵聽通訊端之後，便無法變更該名稱。
  - **IP Address**。偵聽通訊端的 IP 位址。這個位址可用「點對」或是 IPv6 表示法來表示。也可以使用 `0.0.0.0`、`any`、`ANY` 或 `INADDR_ANY` (所有 IP 位址) 表示。
  - **Port**。要在其上建立偵聽通訊端的連接埠之號碼。允許使用 1-65535 之間的數值。在 UNIX 上，若要在連接埠 1-1024 上建立偵聽通訊端，需要有超級使用者權限。請將 SSL 偵聽通訊端配置爲偵聽連接埠 443。
  - **Server Name**。此偵聽通訊端的預設伺服器。

Security

如果停用安全性，將僅顯示下列參數：

- **Security**。啓用或停用選取的偵聽通訊端的安全性。

如果啓用安全性，將顯示下列參數：

- **Security**。啓用或停用選取的偵聽通訊端的安全性。
  - **Server Certificate Name**。從下拉式清單中選取要用於此偵聽通訊端的已安裝的憑證。
  - **Client Authentication**。指定此偵聽通訊端上是否需要用戶端認證。此設定預設爲 [Optional]。
  - **SSL Version 2**。啓用或停用 SSL 第 2 版。此設定預設爲停用狀態。
  - **SSL Version 2 Ciphers**。列出此套裝軟體中的所有密碼。透過選取或取消選取核取方塊，可選取要爲所編輯的偵聽通訊端啓用的密碼。預設版本爲取消選取的狀態。
  - **SSL Version 3**。啓用或停用 SSL 第 3 版。此設定預設爲啓用狀態。
  - **TLS**。啓用或停用 TLS (用於加密通訊的傳輸層安全性協定)。此設定預設爲啓用狀態。

- **TLS Rollback**。啓用或停用 [TLS Rollback]。請注意，停用 [TLS Rollback] 將導致連線容易受到版本回復攻擊。此設定預設爲啓用狀態。
- **SSL Version 3 and TLS Ciphers**。列出此套裝軟體中的所有密碼。透過選取或取消選取核取方塊，可選取要爲所編輯的偵聽通訊端啓用的密碼。預設版本爲選取狀態。

Advanced

- **Number Of Acceptor Threads**。偵聽通訊端的接收器執行緒數目。建議值爲機器中處理器的數目。預設值爲 1。有效值爲 1-1024。

  Protocol Family。套接字家族類型。允許使用的值包括 `inet`、`inet6` 和 `nca`。對於 IPv6 偵聽通訊端，請使用值 `inet6`。指定 `nca` 可使用 Solaris 網路快取記憶體及加速器。

可以使用 Server Manager 的 [Add Listen Socket] 和 [Edit Listen Sockets] 頁面，來增加、編輯和刪除偵聽通訊端。

僅當安裝所需的憑證之後，偵聽通訊端的安全性才能 [Enabled] 做爲選項，屆時下拉式方塊中將僅出現 [Disabled]。

本小節包含以下主題：

- 第 92 頁的 「配置 Proxy-Authenticates-Client 分析藍本」
- 第 93 頁的 「配置 Content Server-Authenticates-Proxy 分析藍本」
- 第 94 頁的 「配置 Proxy-Authenticates-Client and Content Server-Authenticates-Proxy 分析藍本」

▼ 增加偵聽通訊端

1. **存取 [Server Manager]，然後按一下 [Preferences] 標籤。**
2. **按一下 [Add Listen Socket] 連結。**

   此時會顯示 [Add Listen Socket] 頁面。
3. **指定偵聽通訊端的內部名稱。**

   建立偵聽通訊端之後，便無法變更該名稱。
4. **指定偵聽通訊端的 IP 位址。**

   IP 位址可用「點對」或是 IPv6 表示法來表示。也可以使用 `0.0.0.0`、`any`、`ANY` 或 `INADDR_ANY` (所有 IP 位址) 表示。
5. **指定要在其上建立偵聽通訊端的連接埠之號碼。允許使用的值包括 `1 - 65535`。**

   在 UNIX 上，若要在連接埠 1 - 1024 上建立偵聽通訊端，需要有超級使用者權限。請將 SSL 偵聽通訊端配置爲偵聽連接埠 443。

6. **指定伺服器傳送至用戶端的所有 URL 之主機名稱區段中使用的伺服器名稱。**
   此設定會影響伺服器自動產生的 URL；但不會影響儲存在伺服器中的目錄和檔案的 URL。如果您的伺服器使用一個別名，則該名稱應爲此別名。
7. **從下拉式清單中，指定應啓用還是應停用偵聽通訊端的安全性。**
8. **按一下 [OK]。**
9. **按一下 [Restart Required]。**
   此時會顯示 [Apply Changes] 頁面。
10. **按一下 [Restart Proxy Server] 按鈕以套用變更。**

▼ 編輯偵聽通訊端

1. **存取 [Server Manager]，然後按一下 [Preferences] 標籤。**
2. **按一下 [Edit Listen Sockets] 連結。**
   此時會顯示 [Add Listen Socket] 頁面。
3. **在 [Configured Sockets] 表格中，按一下要編輯的偵聽通訊端連結。**
   此時會顯示 [Add Listen Socket] 頁面。
4. **對選項進行所需的變更。**
   如需有關選項的說明，請參閱本小節開頭部分。
5. **按一下 [OK]。**
6. **按一下 [Restart Required]。**
   此時會顯示 [Apply Changes] 頁面。
7. **按一下 [Restart Proxy Server] 按鈕以套用變更。**

▼ 刪除偵聽通訊端

1. **存取 [Server Manager]，然後按一下 [Preferences] 標籤。**
2. **按一下 [Edit Listen Sockets] 連結。**

3. **選取要刪除的偵聽通訊端旁的核取方塊，然後按一下 [OK]。**
   系統將提示您確認刪除。只要不是該實例的唯一偵聽通訊端，任何偵聽通訊端皆可刪除。

4. **按一下 [Restart Required]。**
   此時會顯示 [Apply Changes] 頁面。

5. **按一下 [Restart Proxy Server] 按鈕以套用變更。**

選取目錄服務

[Select Directory Services] 頁面列出了指定代理伺服器實例的所有目錄服務。您可以藉由該頁面來選取與特定代理伺服器實例搭配使用的目錄服務。如需更多資訊，請參閱第 43 頁的 「配置目錄服務」。

▼ 選取目錄服務

1. **存取 Server Manager，然後按一下 [Preferences] 標籤。**

2. **按一下 [Select Directory Services] 連結。**
   此時將顯示 [Select Directory Services] 頁面，其中顯示了指定代理伺服器實例的所有目錄服務。

3. **從清單中選取目錄服務。**

4. **按一下 [OK]。**

5. **按一下 [Restart Required]。**
   此時會顯示 [Apply Changes] 頁面。

MIME 類型

多用途網際網路郵件延伸 (MIME) 類型爲多媒體電子郵件和郵件傳送的標準。因此您可以依照檔案的 MIME 類型進行篩選，代理伺服器將提供頁面，供您建立與伺服器搭配使用的新 MIME 類型。代理伺服器會將新類型增加至 `mime.types` 檔案中。如需有關依照 MIME 類型封鎖檔案的更多資訊，請參閱第 278 頁的 「依 MIME 類型進行篩選」。

本小節說明如何建立、編輯或移除 MIME 類型。

建立 MIME 類型

▼ 建立 MIME 類型

1. **存取 Server Manager，然後按一下 [Preferences] 標籤。**
2. **按一下 [Create/Edit MIME Types] 連結。**
   此時會顯示 [Create/Edit MIME Types] 頁面，其中顯示了代理伺服器的 `mime.types` 檔案所列的所有 MIME 類型。
3. **從下拉式清單中指定 MIME 類型的種類。可以是 `type`、`enc` 或 `lang`。`type` 為檔案或應用程式類型，`enc` 是用於壓縮的編碼，`lang` 則為語言編碼。**
   如需有關種類的更多資訊，請參閱線上說明。
4. **指定將出現在 HTTP 標頭中的內容類型。**
5. **指定檔案後綴。**
   檔案後綴是指對映至 MIME 類型的副檔名。若要指定一個以上的副檔名，請以逗號分隔各項目。副檔名必須是唯一的，也就是說，不可以將一個副檔名對映至兩種 MIME 類型。
6. **按一下 [New] 按鈕以增加 MIME 類型。**

▼ 編輯 MIME 類型

1. **存取 Server Manager，然後按一下 [Preferences] 標籤。**
2. **按一下 [Create/Edit MIME Types] 連結。**
   出現的 [Create/Edit MIME Types] 頁面將顯示代理伺服器的 `mime.types` 檔案中所列的所有 MIME 類型。
3. **對於要編輯的 MIME 類型按一下 [Edit] 連結。**
4. **依需要變更。按一下 [Change MIME Type] 按鈕。**

▼ 移除 MIME 類型

1. **存取 Server Manager，然後按一下 [Preferences] 標籤。**
2. **按一下 [Create/Edit MIME Types] 連結。**
   出現的 [Create/Edit MIME Types] 頁面將顯示代理伺服器的 `mime.types` 檔案中所列的所有 MIME 類型。
3. **對於要移除的 MIME 類型按一下 [Remove] 連結。**

管理存取控制

您可以藉由 [Administer Access Control] 頁面來管理存取控制清單 (ACL)。 ACL 可以讓您控制哪些用戶端可以存取伺服器。ACL 可以篩選掉特定的使用者、群組或主機，以允許或拒絕其存取伺服器的某些部分。ACL 還可設定認證，以便僅有效的使用者和群組才能存取伺服器的某些部分。 如需有關存取控制的更多資訊，請參閱第 8 章「控制對伺服器的存取」。

▼ 管理存取控制清單

1. **存取 Server Manager，然後按一下 [Preferences] 標籤。**
2. **按一下 [Administer Access Control] 連結。**
   此時會顯示 [Administer Access Control] 頁面。
3. **選取資源或現有的 ACL，或是鍵入 ACL 名稱，然後按一下 [Edit] 按鈕。**
   此時會顯示 [Access Control Rules for] 頁面。
4. **進行所需的變更，然後按一下 [Submit]。**
   如需有關存取控制的更多資訊，請參閱第 8 章「控制對伺服器的存取」中的「設定伺服器實例的存取控制」。

配置 ACL 快取

您可以藉由 [Configure ACL Cache] 頁面來啓用或停用代理伺服器認證快取、設定代理伺服器認證快取目錄、配置快取表格大小及設定項目的過期時間。

▼ 配置 ACL 快取

1. **存取 [Server Manager]，然後按一下 [Preferences] 標籤。**
2. **按一下 [Configure ACL Cache] 連結。**
   此時會顯示 [Configure ACL Cache] 頁面。
3. **啓用或停用代理伺服器認證快取。**
4. **從 [Proxy Auth User Cache Size] 下拉式清單中，選取使用者快取中的使用者人數。**
   預設大小爲 200。
5. **從 [Proxy Auth User Cache Size] 下拉式清單中，選取可為單一 UID/快取項目進行快取的群組 ID 數量。**
   預設大小是 4。
6. **選取快取項目過期前的秒數。**
   每次參照快取中的項目時，都將計算其作用時間並依該值進行檢查。如果項目的作用時間大於或等於 [Proxy Auth Cache Expiration] 值，則不予以採用。如果將該值設定爲 0，則會關閉快取。

   如果該值使用較大的數字，則對 LDAP 項目進行變更時，可能需要重新啓動 Proxy Server。例如，如果將該值設定爲 120 秒，Proxy Server 可能與 LDAP 伺服器不同步達兩分鐘之久。如果 LDAP 項目可能不會經常變更，請使用較大的數字。預設的過期值爲兩分鐘。
7. **按一下 [OK]。**
8. **按一下 [Restart Required]。**
   此時會顯示 [Apply Changes] 頁面。
9. **按一下 [Restart Proxy Server] 按鈕以套用變更。**

瞭解 DNS 快取

Proxy Server 支援 DNS 快取，以減少代理伺服器在將 DNS 主機名稱解析爲 IP 位址時，所執行的 DNS 查找數量。

配置 DNS 快取

您可以使用 [Configure DNS Cache] 頁面來啓用或停用 DNS 快取、設定 DNS 快取的大小、設定 DNS 快取項目的過期時間，以及啓用或停用反 DNS 快取。

▼ 配置 DNS 快取

1. **存取 [Server Manager]，然後按一下 [Preferences] 標籤。**
2. **按一下 [Configure DNS Cache] 連結。**
   此時會顯示 [Configure DNS Cache] 頁面。
3. **啓用或停用 DNS 快取。**
4. **從 [DNS Cache Size] 下拉式清單中，選取 DNS 快取可儲存的項目數量。**
   預設大小爲 1024。
5. **設定 DNS 快取過期時間。**
   Proxy Server 會在 DNS 快取達到預設的過期時間時，清除快取中的項目。預設的 DNS 過期時間爲 20 分鐘。
6. **啓用或停用在找不到主機名稱時對錯誤的快取。**
7. **按一下 [OK]。**
8. **按一下 [Restart Required]。**
   此時會顯示 [Apply Changes] 頁面。
9. **按一下 [Restart Proxy Server] 按鈕以套用變更。**

配置 DNS 子網域

有些 URL 所包含的主機名稱具有許多子網域層級。如果第一部 DNS 伺服器無法解析主機名稱，則代理伺服器可能需要較長的時間來進行 DNS 檢查。您可以設定 Proxy Server 在將「host not found」訊息傳回用戶端之前，所要檢查的層級數量。

例如，如果用戶端對 `http://www.sj.ca.example.com/index.html` 提出請求，代理伺服器可能需要很長的時間才能將該主機解析爲 IP 位址，因爲它可能要遍查四部 DNS 伺服器，才能取得主機的 IP 位址。由於上述查找較爲費時，因此您可以對代理伺服器進行配置，使其在必須使用的 DNS 伺服器超過一定數量時，即停止查找 IP 位址。

▼ 為代理伺服器設定查詢的子網域層級

1. **存取 [Server Manager]，然後按一下 [Preferences] 標籤。**
2. **按一下 [Configure DNS Subdomains] 連結。**
   此時會顯示 [Configure DNS Subdomains] 頁面。
3. **從下拉式清單中選取一個資源，或指定常規表示式。**
4. **從 [Local Subdomain Depth] 下拉式清單中選取層級數量。**
5. **按一下 [OK]。**
6. **按一下 [Restart Required]。**
   此時會顯示 [Apply Changes] 頁面。
7. **按一下 [Restart Proxy Server] 按鈕以套用變更。**

配置 HTTP 持續作用

您可以使用 [Configure HTTP Client] 頁面在代理伺服器上啓用持續作用。

持續作用是一項TCP/IP 功能，可在請求完成後使連線保持可用狀態，以便用戶端可以很快地重複使用可用的連線。依預設，代理伺服器並不使用持續作用的連線，但是對某些系統而言，使用持續作用功能可改善代理伺服器的效能。

在 Web 上一般的主從式作業事件中，請求多份文件的用戶端可能會多次連線至伺服器。例如，如果用戶端所請求的網頁包含數個圖形影像，則必須針對每個圖形檔分別提出請求。重新建立連線相當費時。因此，持續作用封包就相當有用。

▼ 配置 HTTP 持續作用

1. **存取 [Server Manager]，然後按一下 [Preferences] 標籤。**
2. **按一下 [Configure HTTP Client] 連結。**
   此時會顯示 [Configure HTTP Client] 頁面。
3. **從下拉式清單中選取資源。**
   選取 HTTP 或 HTTPS 資源，以在 Proxy Server 上配置持續作用功能或指定常規表示式。
4. **透過選取適當的 [Keep Alive] 選項，指定 HTTP 用戶端是否應使用持續連線。**

5 **在 [Keep Alive Timeout] 欄位中，指定保持持續連線開啓的最大秒數。**
預設值爲 29。

6 **透過選取適當的 [Persistent Connection Reuse] 選項，指定 HTTP 用戶端是否可針對所有類型的請求，重複使用現有的持續連線。**
預設值爲 [off]，表示不允許對非 GET 請求或具有內文的請求，重複使用持續連線。

7 **在 [HTTP Version String] 欄位中，指定 HTTP 通訊協定的版本字串。**
除非遇到特定的協定互通功能問題，否則請勿指定此參數。

8 **在 [Proxy Agent Header] 欄位中，指定 Proxy Server 的產品名稱和版本。**

9 **在 [SSL Client Certificate Nickname] 欄位中，指定要提供給遠端伺服器的用戶端憑證暱稱。**

10 **選取適當的 [SSL Server Certificate Validation] 選項，指出 Proxy Server 是否必須驗證遠端伺服器所提供的憑證。**

11 **按一下 [OK]。**

12 **按一下 [Restart Required]。**
此時會顯示 [Apply Changes] 頁面。

13 **按一下 [Restart Proxy Server] 按鈕以套用變更。**

◆ ◆ ◆ 第 8 章

8 控制對伺服器的存取

本章說明如何控制存取 Administration Server 以及 Proxy Server 所提供資料的行爲。您可針對伺服器提供的所有資料或伺服器處理的特定 URL，限制對其存取的行爲。例如，您可以指定僅某些人員可以存取特定的 URL，或指定除這些人員之外的所有人員均可看到檔案。您可以允許所有用戶端均可存取 HTTP 的 URL，但針對 FTP 則限定存取行爲。您也可以依據主機名稱或網域名稱來限制對 URL 進行存取，例如當您使用一部 Proxy Server 來爲許多內部網路伺服器提供服務時，可以僅允許特定人員存取其中一部伺服器所儲存的機密研究專案。

您必須先啓用分散式管理，並在您的 LDAP 資料庫中配置一個管理群組，才能在 Administration Server 上使用存取控制功能。本章包含的資訊假設已執行過這些作業。

本章包含下列小節：

何為存取控制？

存取控制可讓您決定可存取 Proxy Server 的人員，以及他們可存取伺服器的哪些部分。您可以控制讓使用者存取整個伺服器或只存取伺服器的某些部分 (如目錄、檔案、檔案類型等)。在評估內送請求時，會依據稱爲存取控制項目 (ACE) 的規則階層來決定存取。Proxy Server 將尋找相符的項目，以決定應授予存取權還是拒絕。每個 ACE 都會指定伺服器是否應該繼續到階層中的下一個項目。ACE 的集合稱爲存取控制清單 (ACL)。當收到請求時，系統會檢查 `obj.conf` 檔案查看其中是否有參照 ACL 來判斷存取權。依預設，伺服器具有一個包含多個 ACL 的 ACL 檔案。

存取權是允許還是拒絕，需依下列項目決定：

- 使用者/群組的存取控制
- 發出請求的位置 (主機 IP)
- 請求發生的時間 (例如一天中的某個時間)
- 使用的連線類型 (SSL)

本小節包含以下主題：

使用者/群組的存取控制

您可以限制只讓特定使用者或群組存取您的伺服器。使用者/群組存取控制會要求使用者先提供使用者名稱和密碼，之後才能存取伺服器。伺服器會將用戶端憑證中的資訊或用戶端憑證本身，與某個目錄伺服器項目進行比對。

Administration Server 只使用基本認證。如果需要在 Administration Server 上進行用戶端認證，您必須在 `obj.conf` 中手動編輯 ACL 檔案，將此方法變更爲 SSL。

使用者/群組認證是由爲伺服器配置的目錄服務執行的。如需更多資訊，請參閱第 43 頁的 「配置目錄服務」。

目錄服務實作存取控制時使用的資訊，可以從下列任一來源取得：

- 內部平面檔案類型資料庫
- 外部 LDAP 資料庫

當伺服器使用外部 LDAP 型的目錄服務時，伺服器實例支援以下類型的使用者/群組認證方法：

- 預設值
- 基本
- SSL
- 摘要
- 其他

當伺服器使用內部檔案型目錄服務時，針對伺服器實例支援的使用者/群組認證方法包括：

- 預設值
- 基本
- 摘要

使用者/群組認證機制要求使用者先通過認證驗證，之後才能取得存取權。使用者在認證時須提供使用者名稱和密碼、使用用戶端憑證或使用摘要式認證外掛程式，以驗證自己的身分。使用用戶端憑證時需要加密。

預設認證

預設認證是首選方法。[Default] 設定使用 `obj.conf` 檔案中的預設方法，如果 `obj.conf` 中沒有任何設定，則使用 [Basic] 方法。如果選取 [Default]，ACL 規則不會指定 ACL 檔案中的方法。如果選擇 [Default]，您只需編輯 `obj.conf` 檔案中的一行文字，就可以輕鬆變更所有 ACL 的方法。

基本認證

基本認證會要求使用者先提供使用者名稱和密碼，之後才能存取伺服器。基本認證爲預設的設定。您必須在 LDAP 資料庫 (如 Sun Java System Directory Server) 或檔案中建立及儲存使用者和群組的清單。您所使用的目錄伺服器不能與您的 Proxy Server 安裝在相同的伺服器根目錄下，不過您可以使用安裝在遠端電腦上的目錄伺服器。

當使用者嘗試存取具有使用者/群組認證機制的資源時，系統會提示使用者提供使用者名稱和密碼。伺服器所收到的資訊是否加密，取決於您的伺服器是否開啓了加密功能 (啓用 SSL)。

備註 – 如果使用不具 SSL 加密的基本認證，就會在網路上以未加密的文字傳送使用者名稱和密碼。網路封包可能會被截取，因而使用者名稱和密碼可能會被盜用。基本認證與 SSL 加密、主機/IP 認證或這兩者一起使用時的效果最佳。使用摘要式認證可以避免此問題。

如果認證成功，使用者會看到所請求的資源。如果使用者名稱或密碼無效，系統將會發出一則訊息並拒絕存取。

您可以自訂未經授權的使用者可收到的訊息。如需更多資訊，請參閱第 150 頁的「拒絕存取時的回應」。

SSL 認證

伺服器可以利用下列兩種方法，以安全憑證確認使用者的身分：

- 使用用戶端憑證中的資訊做爲身分的證明
- 驗證 LDAP 目錄中發佈的用戶端憑證 (附加)

如果將伺服器配置爲使用憑證資訊來認證用戶端，則伺服器會執行下列動作：

- 檢查以判斷憑證是否來自可信任的CA (憑證授權單位)。如果不是，則認證會失敗，且作業事件會結束。若要瞭解如何啓用用戶端認證，請參閱第 79 頁的「設定安全性喜好設定」。

- 如果憑證是來自可信任的 CA，則會使用 `certmap.conf` 檔案將憑證對映至使用者項目。若要瞭解如何配置憑證對映檔案，請參閱第 95 頁的 「使用 certmap.conf 檔案」。
- 如果憑證正確進行了對映，請檢查爲該使用者指定的 ACL 規則。即使憑證正確進行了對映，ACL 規則也可能會拒絕該使用者的存取。

要求用戶端認證以控制對特定資源進行存取的作法，與要求所有針對伺服器的連線需經用戶端認證不同。如果將伺服器配置爲要求對所有連線進行用戶端認證，則用戶端必須只能提供由可信任的 CA 核發的有效憑證。如果將伺服器配置爲使用 SSL 方法來認證使用者和群組，則必須執行下列動作：

- 用戶端必須出示由可信任的 CA 所核發的有效憑證
- 憑證必須對映到 LDAP 中的有效使用者
- 存取控制清單必須進行正確評估

當您需要具有存取控制的用戶端認證時，您的 Proxy Server 必須啓用 SSL 加密。請參閱第 5 章 「使用憑證和金鑰」以取得有關啓用 SSL 的更多資訊。

若要成功地對採用 SSL 認證的資源進行存取，用戶端憑證必須來自 Proxy Server 所信任的 CA。如果將 Proxy Server 的 `certmap.conf` 檔案配置爲將瀏覽器中的用戶端憑證與目錄伺服器中的用戶端憑證進行比對，則必須在此目錄伺服器中發佈用戶端憑證。不過，您也可以將 `certmap.conf` 檔案配置爲只將憑證中所選取的資訊與目錄伺服器項目進行比對。例如，您可以將 `certmap.conf` 配置爲只將瀏覽器憑證中的使用者 ID 和電子郵件地址，與目錄伺服器項目進行比對。如需有關 `certmap.conf` 和憑證對映的更多資訊，請參閱第 5 章 「使用憑證和金鑰」。另請參閱「Sun Java System Web Proxy Server 4.0.8 Configuration File Reference」。

摘要式認證

您可以將 Proxy Server 配置爲使用 LDAP 型或檔案型目錄服務來執行摘要式認證。

摘要式認證可讓使用者依據使用者名稱和密碼進行認證，但不需要以明文方式傳送使用者名稱和密碼。瀏覽器會利用使用者密碼和 Proxy Server 提供的某些資訊，使用 MD5 演算法來建立摘要值。

當伺服器使用 LDAP 型的目錄服務執行摘要式認證時，也會使用摘要式認證外掛程式在伺服器端計算此摘要值，並將計算結果與用戶端提供的摘要值進行比對。如果兩個摘要值相符，該使用者便通過認證。爲了使這項功能得以正常運作，您的目錄伺服器必須能存取明文的使用者密碼。Sun Java System Directory Server 包含一個反向密碼外掛程式，使用對稱式加密演算法以加密形式儲存資料，稍後可解密成原來的形式。只有 Directory Server 保存了資料的金鑰。

對於 LDAP 型的摘要式認證，您必須啓用隨附於 Proxy Server 的反向密碼外掛程式和摘要式認證專用外掛程式。若要配置您的 Proxy Server 以處理摘要式認證，請設定 `dbswitch.conf` 檔案中資料庫定義的 `digestauth` 特性，該檔案位於 *server-root*`/userdb/`。

以下是 dbswitch.conf 檔案的範例。

```
directory default ldap://<host_name>:<port>
default:binddn cn=Directory Manager
default:encoded bindpw ***********
default:digestauth on
```

或

```
directory default ldap://<host_name>:<port>/
default:binddn cn=Directory Manager
default:encoded bindpw ***********
default:digestauthstate on
```

伺服器會嘗試依據指定的 ACL 方法來認證 LDAP 資料庫，如第 134 頁的 「摘要式認證」所示。如果您未指定 ACL 方法，當需要進行認證時，伺服器會使用摘要式認證或基本認證；當不需要進行認證時，伺服器則會使用基本認證。

下表列示認證資料庫支援和不支援的摘要式認證。

表 8–1 產生摘要式認證挑戰

ACL 方法	認證資料庫支援	認證資料庫不支援
預設值 未指定	摘要和基本	基本
基本	基本	基本
摘要	摘要	錯誤

當處理設定 `method=digest` 的 ACL 時，伺服器會嘗試執行下列動作以進行驗證：

- 檢查授權請求標頭。如果找不到標頭，則會產生帶有摘要挑戰的 401 回應，並且停止處理。
- 檢查授權類型。如果授權類型爲「摘要」，則伺服器會執行下列動作：
  - 檢查 nonce。如果 nonce 不是由此伺服器所產生的有效且未過期的 nonce，則會產生 401 回應，並且會停止處理。如果 nonce 已過期，則會產生 401 回應 (並設定 `stale=true`)，並且會停止處理。

    您可以配置 nonce 的有效時間，方法是變更 `magnus.conf` 檔案中的 `DigestStaleTimeout` 參數值，此檔案位於 *server-root* `/proxy-server_name/config/`。若要設定該值，請將以下行增加至 `magnus.conf`：

    `DigestStaleTimeout` *seconds*

    其中 *seconds* 代表 nonce 有效的秒數。指定的秒數過後，目前認證將過期並要求使用者進行新的認證。
  - 檢查範圍。如果範圍不相符，則會產生 401 回應，並且會停止處理。

- 如果認證目錄是 LDAP 型的，請檢查使用者是否在 LDAP 目錄中；或者，如果認證目錄是檔案型的，則請檢查使用者是否在檔案資料庫中。如果找不到使用者，則會產生 401 回應，並且會停止處理。
- 從目錄伺服器或檔案資料庫取得 `request-digest` 值，並檢查是否與用戶端的 `request-digest` 值相符。如果找不到相符項目，則會產生 401 回應，並且會停止處理。
- 建構 `Authorization-Info` 標頭並將此標頭插入到伺服器標頭中。

安裝摘要式認證外掛程式

對於使用 LDAP 型之目錄服務的摘要式認證，您必須安裝摘要式認證外掛程式。此外掛程式會在伺服器端計算出一個摘要值，並將此摘要值與用戶端提供的摘要值進行比對。如果兩個摘要值相符，該使用者便通過認證。

如果您使用的是檔案型的認證資料庫，便不需要安裝摘要式認證外掛程式。

在 UNIX 上安裝摘要式認證外掛程式

摘要式認證外掛程式包括一個共用程式庫和一個 ldif 檔案：

- `libdigest-plugin.lib`
- `libdigest-plugin.ldif`

▼ 在 UNIX 上安裝摘要式認證外掛程式

開始之前

- 請確定此共用程式庫所在的伺服器電腦與安裝 Sun Java System Directory Server 的伺服器電腦相同。
- 確定您知道 Directory Manager 密碼。
- 修改 `libdigest-plugin.ldif` 檔案會將對 `/path/to` 的所有參照，變更爲指向安裝摘要外掛程式共用程式庫的位置。

● **若要安裝外掛程式，請鍵入以下指令：**

```
% ldapmodify -D "cn=Directory Manager" -w password -a < libdigest-plugin.ldif
```

在 Windows 上安裝摘要式認證外掛程式

您必須將數個 `.dll` 檔案從 Proxy Server 安裝複製到您的 Sun Java System Directory Server 伺服器電腦上，具備摘要外掛程式的 Directory Server 才能正確啓動。

▼ 在 Windows 上安裝摘要式認證外掛程式

1. 存取 Proxy Server 中的共用程式庫，位於 *server-root* \bin\proxy\bin。
2. 將 nsldap32v50.dll、libspnr4.dll 和 libplds4.dll 檔案複製到適當的目錄中：
3. 將這些檔案貼上到以下任一位置：
   - \Winnt\system32
   - Sun Java System Directory Server 安裝目錄： *server-root*\bin\sldap\server

將 Sun Java System Directory Server 設定為使用 DES 演算法

將儲存摘要密碼的屬性加密時，需要 DES 演算法。

▼ 將 Directory Server 設定為使用 DES 演算法

1. 啓動 Sun Java System Directory Server 主控台。
2. 開啓您的 Sun ONE Directory Server 5.1 SP1 (或更高版本) 實例。
3. 選擇 [Configuration] 標籤。
4. 按一下外掛程式旁邊的 + 號。
5. 選取 DES Plug-in。
6. 選擇 [Add] 以增加一個新屬性。
7. 鍵入 iplanetReversiblePassword。
8. 按一下 [Save]。
9. 設定摘要式認證密碼。

備註 – 伺服器會使用位於物件類別 iplanetReversiblePassword 中的 iplanetReversiblePassword 屬性。若要在使用者的 iplanetReversiblePassword 屬性中使用摘要式認證密碼，輸入的項目中必須包括 iplanetReversiblePasswordobject 物件。

您可以使用 ldapmodify 或 Directory Server 管理介面完成此作業。

使用 ldapmodify —

建立 digest.ldif 檔案以儲存 LDAP 指令。增加密碼的程序共有兩個步驟。

a. 將物件類別增加至 digest.ldif。

該檔案如下所示 (您可以根據 Directory Server 的使用者和 ACL 建立多個 ldif 檔案)：

```
dn:uid=user1,dc=india,dc=sun,dc=com
changetype:modify
add:objectclass
objectclass:iplanetReversiblePasswordobject

dn:uid=user1,dc=india,dc=india,dc=sun,dc=com
changetype:modify
add:iplanetReversiblePassword
iplanetReversiblePassword:user1
```

b. `# ldapmodify -D “cn={CN_Value}” -w <password> -a <ldif_file_name>`

10 重新啓動您的 Sun Java System Directory Server 實例，並驗證使用者屬性是否已增加至 Directory Server 資料庫。

其他認證

您可以使用存取控制 API 來建立自訂認證方法。

對主機/IP 的存取控制

您可以限制對 Administration Server 及其檔案和目錄的存取，方法爲限定只有使用特定電腦的用戶端才能加以存取。您可以指定要允許或拒絕其存取的電腦主機名稱或 IP 位址。使用主機/IP 認證機制存取檔案或目錄，對使用者來說幾乎毫不費力。使用者可以立即存取檔案和目錄，且無需輸入使用者名稱或密碼。

由於可能會有多人同時使用一台特定的電腦，因此將主機/IP 認證和使用者/群組認證結合在一起使用的效果會更好。如果同時使用這兩種認證方法，則在進行存取時會要求提供使用者名稱和密碼。

主機/IP 認證不需要在伺服器上配置 DNS (網域名稱服務)。但如果選擇使用主機/IP 認證，您的網路中必須執行 DNS，並且將您的伺服器配置爲使用該 DNS。若要啓用 DNS，請存取伺服器的 Server Manager，並按一下 [Preferences] 標籤，然後按一下 [Configure System Preferences]。您就會看到 DNS 設定。

啓用 DNS 會降低 Proxy Server 的效能，因爲伺服器被迫執行 DNS 查找作業。 若要降低 DNS 查找作業對伺服器效能的影響，請只針對存取控制和 CGI 請求解譯 IP 位址，而不要針對每項請求解譯 IP 位址。若要設定此項限制，請在 obj.conf 中指定下列項目：

```
AddLog fn="flex-log" name="access" iponly=1
```

使用存取控制檔案

當您對 Administration Server 或伺服器上的檔案或目錄使用存取控制時，這些設定會儲存在副檔名爲 .acl 的檔案中。存取控制檔案儲存在 *server-root*/httpacl 目錄中，其中 *server-root* 是伺服器的安裝位置。例如，如果將伺服器安裝在 /usr/Sun/Servers 中，則 Administration Server 和伺服器上所配置的每個伺服器實例的 ACL 檔案，都將位在 /usr/Sun/Servers/httpacl/ 中。

主要 ACL 檔案是 generated-proxy-*serverid*.acl。暫存工作檔案是 genwork-proxy-*serverid*.acl。若您使用 Administration Server 來配置存取，您就會有這兩個檔案。不過，如果您希望實施更複雜的限制，您可以建立多個檔案並從 server.xml 檔案參照這些檔案。有幾個功能只能透過編輯檔案的方式才能發揮功效，例如根據一天中的時間或一週中的日期限制存取伺服器的行爲。

如需有關存取控制檔案及其語法的更多資訊，請參閱第 18 章 「ACL 檔案語法」。如需有關 server.xml 的更多資訊，請參閱 「Sun Java System Web Proxy Server 4.0.8 Configuration File Reference」。

配置 ACL 使用者快取記憶體

依預設，Proxy Server 會將使用者和群組認證結果快取到 ACL 使用者快取記憶體中。您可以控制 ACL 使用者快取的有效時間長度，方法是在 magnus.conf 檔案中使用 ACLCacheLifetime 指令。每次參照快取中的某個項目時，都會計算其有效時間並與 ACLCacheLifetime 比對檢查。如果該項目的有效時間大於或等於 ACLCacheLifetime，則不使用該項目。預設值爲 120 秒。將該值設定爲 0 (零) 將關閉快取記憶體。如果將其設定爲一個較大的值，則每次變更 LDAP 項目時，都可能需要重新啓動 Proxy Server。例如，如果將該值設定爲 120 秒，Proxy Server 可能在兩分鐘的時間內，與 LDAP 伺服器不同步。僅當 LDAP 目錄不經常變更時才設定一個較大的值。

使用 magnus.conf 參數 ACLUserCacheSize，就可以配置快取記憶體中可保留的項目上限。此參數的預設值爲 200。新的項目會增加至清單開頭，而且當快取記憶體的大小達到最大值時，位於此清單尾端的項目會回收以建立新的項目。

您也可以使用 magnus.conf 參數 ACLGroupCacheSize，設定每個使用者項目可以在快取記憶體內保留的最大群組成員數。此參數的預設值爲 4。如果某使用者不是群組中的成員，就不會將其快取至記憶體中，如此將導致每次有請求時都需要存取數次 LDAP 目錄。

使用用戶端憑證控制存取

如果您的伺服器上已啓用 SSL，就可以將用戶端憑證與存取控制結合使用。您必須指定需要有用戶端憑證才能存取特定資源。當在您的伺服器上啓用這項功能時，擁有憑證的使用者只有在第一次嘗試存取限定資源時，才需要輸入使用者名稱和密碼。一旦建

立使用者身分之後，伺服器便會將其登入名稱和密碼對映至該特定的憑證。此後，當使用者存取需要有用戶端認證才能存取的資源時，就不需要再輸入其登入名稱或密碼。

當使用者嘗試存取限定資源時，其用戶端就會將用戶端憑證傳送給伺服器，伺服器便會將該憑證與對映清單檢查核對。如果該憑證屬於您已授予存取權的使用者，則該使用者即可存取資源。

要求用戶端認證以控制對特定資源進行存取的作法，與要求所有針對伺服器的連線需經用戶端認證不同。此外請注意，對所有 SSL 連線要求用戶端憑證，並不會自動將憑證對映至資料庫內的使用者。若要設定此對映，您必須指定需要有用戶端憑證才能存取指定的資源。

存取控制的工作方式

當伺服器收到對某個網頁的請求時，它會使用 ACL 檔案中的規則來判斷是否應授予存取權。這些規則可以參照傳送請求的電腦主機名稱或 IP 位址。還可以參照儲存在 LDAP 目錄中的使用者和群組。

下列範例顯示 ACL 檔案可能包含的內容，並提供存取控制規則範例。

```
version 3.0;
# The following "es-internal" rules protect files such
# as icons and images related to Sun Java System Web Proxy Server.
# These "es-internal" rules should not be modified.
  acl "es-internal";
  allow (read, list, execute,info) user = "anyone";
  deny (write, delete) user = "anyone";

# The following rules deny access to the directory "web"
# to everyone not in the directory server and deny everyone
# in the directory server who is not in GroupB.
# Only the users in GroupB are allowed read, execute, list,
# and info permissions. GroupA cannot gain access to the
# directory "web" even though (in the ACL rule below) they
# can access the directory “my_stuff”. Furthermore, members
# of GroupB cannot write or delete files.
  acl "path=/export/user/990628.1/docs/my_stuff/web/";
  authenticate (user,group) {
     database = "default";
     method = "basic";
  };
  deny (all)
  (user = "anyone");

  allow (read,execute,list,info)
```

```
  (group = "GroupB");

# The following rule denies everyone not in the directory
# server and denies everyone in the directory server except
# users with the ID of "SpecificMemberOfGroupB". The ACL rule
# in this setting also has a requirement that the user
# connect from a specific IP address. The IP address setting
# in the rule is optional, and has been added for extra
# security. Also, this ACL rule has a Customized prompt
# of "Presentation Owner". This Customized prompt appears
# in the username and password dialog box in the client's
# browser.

  acl "path=/export/user/990628.1/docs/my_stuff/web/presentation.html";
  authenticate (user,group) {
     database = "default";
     method = "basic";
     prompt = "Presentation Owner";
  };
  deny (all)
  (user = "anyone" or group = "my_group");
  allow (all)
  (user = "SpecificMemberOfGroupB") and
  (ip = "208.12.54.76");

# The following ACL rule denies everyone not in the directory
# server and everyone in the directory server except for
# GroupA and GroupB access to the directory  "my_stuff"
  acl "path=/export/user/990628.1/docs/my_stuff/";
  authenticate (user,group) {
     database = "default";
     method = "basic";
  };
  deny (all)
  (user = "anyone");
  allow (read,execute,list,info)
  (group = "GroupA,GroupB");
```

例如，如果使用者請求 URL `http://server_name/my_stuff/web/presentation.html`，Proxy Server 便會先檢查對整個伺服器的存取控制。如果整個伺服器的 ACL 設定爲 [Continue]，則伺服器會檢查 `my_stuff` 目錄中有無 ACL。如果有 ACL 存在，伺服器便會檢查該 ACL 內的 ACE，然後檢查下一個目錄。此程序持續到找出拒絕存取的 ACL 爲止，或者到達所請求 URL 的最後一個 ACL 爲止，在本例中是到達 `presentation.html` 檔案。

若要使用 Server Manager 設定對此範例的存取控制，您可以只針對該檔案建立一個 ACL，或針對指向該檔案的每項資源各建立一個 ACL，亦即整個伺服器一個 ACL、`my_stuff` 目錄一個 ACL、`my_stuff/web` 目錄一個 ACL，以及該檔案一個 ACL。

如果有一個以上相符的 ACL 存在，則伺服器會使用相符的最後一個 ACL 敘述。

設定存取控制

本節說明限制存取的程序。您可以對所有伺服器設定全域存取控制規則，也可以對特定的伺服器設定個別的存取控制規則。例如，人力資源部門可以建立 ACL，允許所有通過認證的使用者檢視自己的薪資資料，但僅限負責薪資的人力資源部門人員可以更新資料。

本小節包含以下主題：

- 第 142 頁的 「設定全域存取控制」
- 第 144 頁的 「設定對伺服器實例的存取控制」

備註 – 您必須先配置並啓動分散式管理，才能設定全域存取控制。

設定全域存取控制

▼ 設定對所有伺服器的存取控制

1. **存取 Administration Server，然後按一下 [Global Settings] 標籤。**
2. **按一下 [Administer Access Control] 連結。**
3. **從下拉式清單選取管理伺服器 (`proxy-admserv`)、按一下 [Go] 以載入資料，然後按一下 [New ACL] (或 [Edit ACL])。**
4. **如果出現提示，則進行驗證。**

   此時會顯示 [Access Control Rules For] 頁面。Administration Server 具有兩行不可編輯的預設存取控制規則。
5. **選取 [Access Control Is On] (如果尚未選取)。**
6. **若要將一個預設 ACL 規則增加至該表的底部一列，請按一下 [New Line] 按鈕。**

   若要變更存取控制限制的位置，請按一下向上或向下箭頭。

7. **按一下 [Users/Groups] 欄中的 [Anyone]。**
   [User/Group] 頁面會顯示在下方框架中。

8. **選取您要允許其存取的使用者和群組，然後按一下 [Update]。**
   按一下 [Group or User] 的 [List] 按鈕，即可提供一份清單供您選擇。如需有關設定的更多資訊，請參閱線上說明。另請參閱第 146 頁的 「指定使用者和群組」。

9. **按一下 [From Host] 欄中的 [Anyplace]。**
   [From Host] 頁面會顯示在下方框架中。

10. **指定允許其存取的主機名稱和 IP 位址，然後按一下 [Update]。**
    如需有關設定的更多資訊，請參閱線上說明。另請參閱第 148 頁的 「指定 [From Host]」。

11. **按一下 [Programs] 欄中的 [All]。**
    [Programs] 頁面會顯示在下方框架中。

12. **選取 [Program Groups]，或在 [Program Items] 欄位中鍵入您要允許存取的特定檔案名稱，然後按一下 [Update]。**
    如需有關設定的更多資訊，請參閱線上說明。另請參閱第 149 頁的 「限制對程式的存取」。

13. **(可選) 按一下 [Extra] 欄中的 X 符號可以增加一個自訂的 ACL 表示式。**
    [Customized Expressions] 頁面會顯示在下方框架中。如需更多資訊，請參閱第 150 頁的 「撰寫自訂表示式」。

14. **選取 [Continue] 欄中的核取方塊 (如果尚未選取)。**
    伺服器會先評估下一行，之後才決定是否允許該使用者進行存取。建立多行限制時，請將限制依一般到特定的順序排列。

15. **(可選) 按一下回收筒圖示，以刪除存取控制規則對應的那一行。**

16. **(可選) 按一下 [Response When Denied] 連結，以指定使用者遭到拒絕存取時會收到的回應。**
    [Access Deny Response] 頁面會顯示在下方框架中。

    a. **請選取所需的回應。**

    b. **指定附加資訊 (如果適用)。**

    c. **按一下 [Update]。**

    如需有關設定的更多資訊，請參閱第 150 頁的 「拒絕存取時的回應」。

17 **按一下 [Submit] 以將新的存取控制規則儲存在 ACL 檔案中，或按一下 [Revert] 以將該頁面中的元素重設為變更之前所包含的值。**

設定對伺服器實例的存取控制

使用 Server Manager 可以建立、編輯或刪除對特定伺服器實例的存取控制。若要刪除，請勿刪除 ACL 檔案中的所有 ACL 規則。至少要保留一個 ACL 檔案，並且其中至少要包含一個 ACL 規則，才能啓動伺服器。刪除所有 ACL 規則並重新啓動伺服器將導致語法錯誤。

▼ 設定對伺服器實例的存取控制

1 **存取伺服器實例的 Server Manager 並按一下 [Preferences] 標籤。**

2 **按一下 [Administer Access Control] 連結。**

3 **使用下列其中一種方法來選取 ACL：**

- 從 [Select A Resource] 下拉式清單中選取使用 ACL 以限制存取的資源，或按一下 [Regular Expression] 以指定常規表示式。如需更多資訊，請參閱「Proxy Server **管理指南**」中的第 16 章「管理範本和資源」。
- 選取 [Existing ACL]，將列出所有已啓用的 ACL。

  尚未啓用的現有 ACL 不會顯示在此清單中。從下拉式清單選取 ACL。
- 鍵入 [ACL Name]。此選項可讓您建立已命名的 ACL。除非您很熟悉 ACL 檔案，否則不建議您使用此選項。若要將已命名的 ACL 套用至多項資源，您必須手動編輯 `obj.conf`。如需更多資訊，請參閱第 18 章「ACL 檔案語法」。

4 **按一下對應的 [Edit] 按鈕。**

此時會顯示 [Access Control Rules For] 頁面。

5 **選取 [Access Control Is On] (如果尚未選取)。**

6 **若要將一個預設 ACL 規則增加至該表的底部一列，請按一下 [New Line] 按鈕。**

若要變更存取控制限制的位置，請按一下向上或向下箭頭。

7 **若要編輯此伺服器實例的 ACL，請按一下 [Action] 欄中的動作。**

[Allow/Deny] 頁面會顯示在下方框架中。

8 **選取 [Allow] (如果尚未依預設選取)，然後按一下 [Update]。**

如需有關 [Allow] 或 [Deny] 的更多資訊，請參閱第 146 頁的「設定動作」。

9 **按一下 [Users/Groups] 欄中的 [Anyone]。[User/Group] 頁面會顯示在下方框架中。**

10 **選取要對其授予存取權的使用者和群組、指定認證資訊，然後按一下 [Update]。**

按一下 [Group or User] 的 [List] 按鈕，即可提供一份清單供您選擇。如需有關設定的更多資訊，請參閱線上說明。另請參閱第 146 頁的 「指定使用者和群組」。

11 **按一下 [From Host] 欄中的 [Anyplace]。**

[From Host] 頁面會顯示在下方框架中。

12 **指定允許其存取的主機名稱和 IP 位址，然後按一下 [Update]。**

如需有關設定的更多資訊，請參閱線上說明。另請參閱第 148 頁的 「指定 [From Host]」。

13 **按一下 [Rights] 欄中的 [All]。**

[Access Rights] 頁面會顯示在下方框架中。

14 **指定此使用者的存取權限，然後按一下 [Update]。**

如需更多資訊，請參閱第 149 頁的 「限制對程式的存取」。

15 **(可選) 按一下 [Extra] 欄下的 X 符號以增加自訂的 ACL 表示式。**

[Customized Expressions] 頁面會顯示在下方框架中。如需更多資訊，請參閱第 150 頁的 「撰寫自訂表示式」。

16 **選取 [Continue] 欄中的核取方塊 (如果尚未選取)。**

伺服器會先評估下一行，之後才決定是否允許該使用者進行存取。建立多行限制時，請將限制依一般到特定的順序排列。

17 **(可選) 按一下回收筒圖示，以刪除存取控制規則對應的那一行。**

請勿刪除 ACL 檔案中的所有 ACL 規則。必須至少有一個 ACL 檔案包含至少一個 ACL 規則，才能啓動伺服器。如果刪除 ACL 檔案中的所有 ACL 規則，並嘗試重新啓動伺服器，您就會收到語法錯誤訊息。

18 **(可選) 按一下 [Response When Denied] 連結，以指定使用者遭到拒絕存取時會收到的回應。**

[Access Deny Response] 頁面會顯示在下方框架中。選取所需的回應，並指定附加資訊 (如果適用)，然後按一下 [Update]。如需有關設定的更多資訊，請參閱第 150 頁的 「拒絕存取時的回應」。

19 **按一下 [Submit] 以將新的存取控制規則儲存在 ACL 檔案中，或按一下 [Revert] 以將該頁面中的元素重設為變更之前所包含的值。**

選取存取控制選項

下列主題說明您在設定存取控制時可以選取的各種選項。針對 Administration Server，前兩行爲預設設定，無法編輯。

本小節包含以下主題：

設定動作

您可以指定當請求匹配存取控制規則時伺服器要執行的動作。

- [**Allow**] 表示使用者或系統可以存取請求的資源
- [**Deny**] 表示使用者或系統不能存取該項資源

伺服器會檢查所有存取控制項目 (ACE) 清單，以決定存取權限。例如，第一個 ACE 通常爲拒絕所有使用者。如果第一個 ACE 設爲 [Continue]，伺服器便會檢查清單中的第二個 ACE。如果該 ACE 相符，就會使用下一個 ACE。如果未選取 [Continue]，則會拒絕所有使用者存取該項資源。伺服器會繼續檢查清單，直到找到不相符的 ACE 或相符但未設定爲 [Continue] 的 ACE 爲止。最後一個相符的 ACE 將確定是允許還是拒絕存取。

指定使用者和群組

使用使用者和群組認證時，系統會提示使用者提供使用者名稱和密碼，之後才能存取在存取控制規則中指定的資源。

Proxy Server 會檢查儲存在 LDAP 伺服器 (如 Sun Java System Directory Server) 或內部檔案型之認證資料庫中的使用者和群組清單。

您可以允許或拒絕資料庫中的任何人進行存取，也可以使用萬用字元式樣以允許或拒絕特定的人員，或從使用者和群組清單中選取要允許或拒絕的人員。

下列爲使用者介面中 [Access Control Rules For] 頁面上，針對 [Users/Groups] 所顯示的元素：

- [**Anyone (No Authentication)**] 是預設設定，表示任何使用者都可以存取該資源而不必提供使用者名稱或密碼。但是，基於其他設定 (例如主機名稱或 IP 位址) 的不同，也可能會拒絕該使用者進行存取。針對 Administration Server，這項設定表示您爲分散式管理所指定的管理者群組中，任何人都可以存取這些頁面。
- **Authenticated People Only**
  - [**All In The Authentication Database**] 會比對與資料庫項目相符的任何使用者。
  - [**Only The following People**] 可讓您指定要比對的使用者和群組。您可以用逗號分隔各個項目來個別列出使用者或使用者群組，也可以使用萬用字元式樣，還可以從儲存在資料庫中的使用者和群組清單進行選取。[**Group**] 可比對指定群組中的所有使用者。[**User**] 可比對您指定的個別使用者。針對 Administration Server，使用者還必須位於您爲分散式管理所指定的管理員群組中。

  [**Prompt For Authentication**] 指定在認證對話方塊中顯示的訊息文字。您可以使用此文字來說明使用者需要鍵入的內容。使用者大約可以看到該提示的前 40 個字元，視作業系統而定。大多數瀏覽器都會快取使用者名稱和密碼，並將其與提示文字相關聯。如果使用者存取的伺服器檔案與目錄區域具有相同的提示，使用者就不需要重新鍵入使用者名稱和密碼。相反，如果要強制使用者重新認證後才可存取不同區域，您必須變更此資源上的 ACL 提示。
- [*Authentication Methods*] 指定伺服器從用戶端取得認證資訊時所使用的方法。Administration Server 僅提供了基本認證方法。Server Manager 則提供下列方法：
  - [*Default*] 會使用 `obj.conf` 檔案中指定的預設方法，如果 `obj.conf` 中沒有任何設定，則會使用 [Basic]。如果選取 [Default]，ACL 規則不會指定 ACL 檔案中的方法。如果選擇 [Default]，您只需編輯 `obj.conf` 檔案中的一行文字，就可以輕鬆變更所有 ACL 的方法。
  - [*Basic*] 使用 HTTP 方法，從用戶端取得認證資訊。僅當爲伺服器啓用了加密 (啓用 SSL) 後，才會對使用者名稱和密碼進行加密。否則，名稱和密碼會以明文方式傳送，如果遭到截取，他人就會看到這些內容。
  - [*SSL*] 使用用戶端憑證來認證使用者。若要使用此方法，必須爲伺服器啓用 SSL。如果啓用加密，則可以合併 [Basic] 和 [SSL] 兩種方法。

    備註 – 您只能在反向代理模式中啓用安全性，不能在正向代理模式中啓用。

  - [*Digest*] 所使用的認證機制讓瀏覽器根據使用者名稱和密碼認證使用者，不以明文方式傳送使用者名稱和密碼。瀏覽器透過使用者的密碼和 Proxy Server 提供的一些資訊，使用 MD5 演算法來建立摘要值。伺服器端也會使用摘要式認證外掛程式計算此摘要值，並與用戶端提供的摘要值進行比對。

備註 – [Prompt For Authentication] 是摘要式認證的必要參數。變更值以符合範圍 (摘要檔案的必要項目)。例如，如果您在摘要檔案中將所有使用者都配置爲位於 *test* 範圍內，則 [Prompt For Authentication] 欄位應包含文字 *test*。

- [*Other*] 使用您透過存取控制 API 建立的自訂方法。

[*Authentication Database*] 指定伺服器將用來認證使用者的資料庫。此選項僅在 Server Manager 中可用。如果選擇 [Default]，伺服器將查找配置爲預設的目錄服務中的使用者和群組。如果要配置讓個別的 ACL 使用不同資料庫，請選取 [Other] 並指定資料庫。您必須在 *server-root*`/userdb/dbswitch.conf` 中指定非預設資料庫和 LDAP 目錄。如果將存取控制 API 用於自訂資料庫，請選取 [Other] 並鍵入資料庫名稱。

指定 [From Host]

您可以根據發出請求的電腦來限制對 Administration Server 的存取。

下列爲使用者介面中 [Access Control Rules For] 頁面上，[From Host] 所顯示的元素：

- [Anyplace] 允許存取所有使用者和系統。
- [Only From] 可讓您限制對特定主機名稱或 IP 位址的存取

如果選取 [Only From] 選項，請在 [Host Names] 或 [IP Addresses] 欄位中鍵入萬用字元式樣或以逗號分隔的清單。依主機名稱限制比依 IP 位址限制更具有彈性。如果使用者的 IP 位址發生變更，您就無需更新此清單。但是依 IP 位址限制比較可靠。如果對連線用戶端進行 DNS 查找失敗，將無法使用主機名稱限制。

您只能使用與電腦的主機名稱或 IP 位址相符之萬用字元式樣的 * 萬用字元表示法。例如，若要允許或拒絕特定網域內的所有電腦，您需要輸入與該網域內所有主機相符的萬用字元式樣，例如 `*.example.com`。您可以爲存取 Administration Server 的超級使用者設定不同的主機名稱和 IP 位址。

對於主機名稱，* 必須替代名稱中的整個元件，亦即 `*.example.com` 有效，但 `*users.example.com` 則無效。* 出現在主機名稱中時，必須是最左側的字元。例如 `*.example.com` 有效，但 `users.*.com` 則無效。

對於 IP 位址，* 必須替代位址中的整個位元組，例如 `198.95.251.*` 有效，但 `198.95.251.3*` 則無效。* 出現在 IP 位址中時，必須是最右側的字元。例如 `198.*` 有效，但 `198.*.251.30` 則無效。

限制對程式的存取

只有 Administration Server 才能限制對程式的存取行爲。限制對程式的存取行爲，即可僅讓指定的使用者檢視 Server Manager 頁面，並決定這些使用者是否可以配置該伺服器。例如，您可能允許幾個管理員配置 Administration Server 的 [Users and Groups] 區段，但拒絕他們存取 [Global Settings] 區段。

您可以配置不同的使用者存取不同的功能領域。一旦允許使用者存取已選取的功能性網域，則該使用者登入後，僅能看到開放給該使用者的功能性網域之 Administration Server 頁面。

下列爲使用者介面中 [Access Control Rules For] 頁面上， [Programs] 所顯示的元素：

- [All Programs]，允許或拒絕存取所有程式。依預設，管理員可以存取伺服器的所有程式。
- [Only The Following] 讓您可以指定使用者可以存取的程式。
  - [**Program Groups**] 顯示 Administration Server 的標籤 (例如，[Preferences] 和 [Global Settings])，並顯示對這些頁面的存取情形。當管理員存取 Administration Server 時，伺服器將使用他們的使用者名稱、主機和 IP 位址來決定他們能檢視的頁面。
  - [Program Items] 讓您可以在欄位中鍵入頁面名稱，即可限制對程式內特定頁面的存取。

設定存取權限

伺服器實例的存取權限只能由 Server Manager 設定。存取權限可以限制對伺服器上檔案和目錄的存取。除了允許或拒絕所有存取權限外，您還可以指定一個允許或拒絕部分存取權限的規則。例如，您可以允許使用者對檔案具有唯讀存取權限，讓他們可以檢視資訊，但無法變更檔案。

下列爲使用者介面中 [Access Control Rules For] 頁面上， [Rights] 所顯示的元素：

- [All Access Rights] 是預設設定，可允許或拒絕所有權限。
- [**Only The following Rights**] 讓您可以選取要允許或要拒絕的權限組合：
  - [*Read*] 允許使用者檢視檔案，包括 HTTP 方法 GET、HEAD、POST 和 INDEX。
  - [*Write*] 允許使用者變更或刪除檔案，包括 HTTP 方法 PUT、DELETE、MKDIR、RMDIR 和 MOVE。若要刪除檔案，使用者必須同時具有寫入和刪除權限。
  - [*Execute*] 允許使用者執行伺服器端應用程式，例如 CGI 程式、Java Applet 及代理程式。
  - [*Delete*] 允許同時具有寫入權限的使用者刪除檔案或目錄。
  - [*List*] 允許使用者存取不包含 `index.html` 檔案之目錄中的檔案清單。

- [*Info*] 允許使用者接收有關 URI 的資訊，例如 `http_head`。

撰寫自訂表示式

您可以爲 ACL 輸入自訂表示式。僅當您瞭解 ACL 檔案的語法和結構時，才可以選取此選項。有幾個功能只有透過編輯 ACL 檔案或建立自訂表示式的方式才能發揮功效。例如，您可以根據一天中的時間和/或一週中的日期限制存取伺服器的行爲。

以下自訂表示式顯示如何依據一天中的時間和一週中的日期來限制存取。本範例假定您的 LDAP 目錄中有兩個群組存在。[Regular] 群組可以在星期一到星期五的上午 8:00 到下午 5:00 進行存取。[Critical] 群組可以隨時進行存取。

```
allow (read){(group=regular and dayofweek=” mon,tue,wed,thu,fri” );
(group=regular and (timeofday>=0800 and timeofday<=1700));(group=critical)}
```

如需有關有效語法及 ACL 檔案的更多資訊，請參閱第 18 章 「ACL 檔案語法」。

關閉存取控制

當您取消選取 [Access Control Rules For] 頁面上標示爲 [Access Control Is On] 的選項時，會出現提示詢問您是否要消除 ACL 中的記錄。當您按一下 [OK] 時，將會從 ACL 檔案中刪除該資源的 ACL 項目。

如果您想要停用 ACL，可在檔案 `generated-proxy-`*`serverid`*`.acl` 中的每一行開頭使用 # 號，爲 ACL 行加入註釋。

在 Administration Server 中，您可以針對特定伺服器實例建立並開啓存取控制，但對其他伺服器仍保留關閉存取控制 (預設值)。例如，您可以透過 Administration Server 拒絕對 Server Manager 頁面的所有存取。當任何其他伺服器依預設開啓了分散式管理且關閉存取控制時，管理員仍可以存取和配置那些伺服器，但不能配置 Administration Server。

拒絕存取時的回應

Proxy Server 在拒絕存取時提供一則預設訊息，您可以視需要自訂回應。也可以爲每個存取控制物件建立不同的訊息。

對於 Administration Server，依預設使用者會收到 *server-root*`/httpacl/admin-denymsg.html` 中的 [Permission Denied] 訊息。

▼ 變更拒絕存取訊息

1 **按一下 [Access Control Rules For] 頁面上的 [When Denied] 連結。**

2. **選取所需的回應並提供附加資訊 (如果適用)，然後按一下 [Update]。請確定使用者對重新導向後的回應擁有存取權限。**

3. **按一下 [Submit] 以儲存變更，或按一下 [Revert] 以將該頁面中的元素重設為變更之前所包含的值。**

限制對伺服器中區域的存取

本節說明一些對伺服器及其內容的常用限制。每個程序的步驟都會詳細記載必須採取的特定動作。不過，您仍舊要完成第 144 頁的 「設定對伺服器實例的存取控制」中所描述的步驟。

本小節包含以下主題：

限制對整個伺服器的存取

您可能希望允許群組中的使用者，從子網域中的電腦存取伺服器。例如，公司某部門有一部伺服器，您只希望使用者透過網路特定子網域中的電腦加以存取。

▼ 限制對整個伺服器的存取

1. **存取伺服器實例的 Server Manager。**

2. **在 [Preferences] 標籤上，按一下 [Administer Access Control] 連結。**

3. **從下拉式清單選取整個伺服器、按一下 [Select]，再按一下對應的 [Edit] 按鈕。**
   此時會顯示 [Access Control Rules For] 頁面。

4. **增加一個新規則以拒絕所有人存取。**

5. **增加另一個新規則以允許特定群組存取。**

6. **使用 [From Host] 指定要限制的主機名稱和 IP 位址。**

7 **按一下 [Submit] 以儲存變更。**

限制對目錄的存取

您可以允許某個群組的使用者讀取或執行由該群組的所有者控制的目錄及其子目錄中的應用程式和檔案。例如，專案經理可以更新狀態資訊，供專案團隊複查。

▼ 限制對目錄的存取

依照對伺服器實例的存取控制設定步驟 (請參閱第 144 頁的 「設定對伺服器實例的存取控制」)，執行下列動作：

1 **存取伺服器實例的 Server Manager。**

2 **在 [Preferences] 標籤上，按一下 [Administer Access Control] 連結。**

3 **從下拉式清單選取所需的資源，然後按一下 [Edit]。**

4 **建立一個規則，其預設值為拒絕任何人從任何位置進行存取。**

5 **建立另一個規則，允許某個特定群組中的使用者僅具有讀取和執行權限。**

6 **建立第三個規則，允許某個特定使用者具有所有權限。**

7 **對後兩個規則取消選取 [Continue]。**

8 **按一下 [Submit] 以儲存變更。**

限制對檔案類型的存取

您可以限制對檔案類型的存取。例如，您可能只想允許特定使用者建立在伺服器上執行的程式。任何使用者都可以執行程式，但僅有群組中的特定使用者可以建立或刪除程式。

▼ 限制對檔案類型的存取

1 **存取伺服器實例的 Server Manager。**

2 **在 [Preferences] 標籤上，按一下 [Administer Access Control] 連結。**

3 **在 [Select A Resource] 區段中，按一下 [Regular Expression] 並指定常規表示式，例如** `*.cgi`。

4. **按一下 [Edit]。**
5. **建立一個規則，允許所有使用者進行讀取。**
6. **建立另一個規則，僅允許某個特定群組進行寫入和刪除。**
7. **按一下 [Submit] 以儲存變更。**

   對於檔案類型限制，您可以讓兩個規則的 [Continue] 方塊均保持在選取狀態。當傳入對檔案的請求時，伺服器將先檢查該檔案類型的 ACL。

   `obj.conf` 檔案中會建立一個 `Pathcheck` 函數，可能包含檔案或目錄的萬用字元式樣。ACL 檔案中的項目將如下所示：`acl"*.cgi";`

根據一天中的時間限制存取

您可以將對伺服器的寫入和刪除存取限制爲僅允許在指定的時間或指定的日期進行。

▼ 基於一天中的時間限制存取

1. **存取伺服器實例的 Server Manager。**
2. **在 [Preferences] 標籤上，按一下 [Administer Access Control] 連結。**
3. **在 [Select A Resource] 區段中，從下拉式清單選取整個伺服器，然後按一下 [Edit]。**
4. **建立一個規則，授予所有使用者讀取和執行權限。**

   如果使用者要增加、更新或刪除檔案或目錄，則此規則不再適用，伺服器將搜尋另一個相符的規則。
5. **建立另一個規則，拒絕所有使用者進行寫入和刪除。**
6. **按一下 X 連結，以建立自訂表示式。**
7. **鍵入允許進行存取的一週中的哪些天以及一天中的哪些時間，例如：**

   ```
   user = "anyone" anddayofweek = "sat,sun" or(timeofday >= 1800
   andtimeofday <= 600)
   ```
8. **按一下 [Submit] 以儲存變更。**

   自訂表示式中的任何錯誤都會產生一則錯誤訊息。請進行更正並再次提交。

基於安全性限制存取

您可以爲同一伺服器實例配置 SSL 及非 SSL 偵聽通訊端。基於安全性限制存取，可讓您爲僅應透過安全通道傳輸的資源建立保護。

▼ 基於安全性限制存取

1. **存取伺服器實例的 Server Manager。**
2. **在 [Preferences] 標籤上，按一下 [Administer Access Control] 連結。**
3. **在 [Select A Resource] 區段中，從下拉式清單選取整個伺服器，然後按一下 [Edit]。**
4. **建立一個規則，授予所有使用者讀取和執行權限。**
   如果使用者要增加、更新或刪除檔案或目錄，則此規則不再適用，伺服器將搜尋另一個相符的規則。
5. **建立另一個規則，拒絕所有使用者進行寫入和刪除。**
6. **按一下 X 連結，以建立自訂表示式。**
7. **鍵入** `ssl="on"`**。例如：**
   ```
   user = "anyone" and ssl="on"
   ```
8. **按一下 [Submit] 以儲存變更。**
   自訂表示式中的任何錯誤都會產生一則錯誤訊息。請進行更正並再次提交。

保證資源的存取安全

本節說明在啓用分散式管理後，爲保證 Proxy Server 存取控制安全性而必須執行的其他作業。

保證伺服器實例的存取安全

若要配置 Proxy Server 以控制對伺服器實例的存取，請編輯 *server-roob*`/httpacl/*.proxy-admserv.acl` 檔案，以指定要授予哪個使用者存取控制權限。例如：

```
acl "proxy-server_instance "; authenticate (user,group) { database = "default";
method = "basic"; }; deny absolute (all) user != "UserA";
```

啓用基於 IP 的存取控制

如果參照 ip 屬性的存取控制項目位於與 Administration Server 相關的 ACL 檔案中 (gen*.proxy-admserv.acl)，請完成下列步驟 1 和 2。

如果有關 ip 屬性的存取控制項目位於與伺服器實例相關的 ACL 檔案中，則僅需爲該特定 ACL 完成下列步驟 1。

▼ 啓用基於 IP 的存取控制

1 **編輯 *server-root*/httpacl/gen*.proxy-admserv.acl 檔案，以便讓認證清單除了 user 和 group 之外還增加 ip，如下所示。**

```
acl "proxy-admserv"; authenticate (user,group,ip) { database = "default"; method =
"basic"; };
```

2 **增加以下存取控制項目：**

```
deny absolute (all) ip !="ip_for_which_access_is_allowed ";
```

例如：

```
acl "proxy-admserv"; authenticate (user,group,ip) { database = "default"; method =
"basic"; }; deny absolute (all) ip !="205.217.243.119";
```

為檔案型認證建立 ACL

Proxy Server 支援使用檔案型的認證資料庫，這些資料庫將使用者和群組資訊以文字格式儲存在平面檔案中。ACL 架構的設計原本就是要搭配檔案型認證資料庫。

備註 – Proxy Server 不支援動態平面檔案。平面檔資料庫將在伺服器啓動時載入。對這些檔案所做的任何變更僅在重新啓動伺服器時才能生效。

本節說明如何根據檔案認證和摘要式認證，建立目錄服務的 ACL。

ACL 項目可以使用 database 關鍵字來參照使用者資料庫。例如：

```
acl "default";    authenticate (user) {...    database="myfile";...};
```

server-root/userdb/dbswitch.conf 檔案中包含的項目可定義檔案認證資料庫及其配置。例如：

```
directory myfiledb filemyfiledb:syntax keyfilemyfiledb:keyfile
/path/to/config/keyfile
```

下表列示檔案認證資料庫支援的參數。

表 8–2 檔案認證資料庫支援的參數

參數	說明
`syntax`	(可選) 值爲 `keyfile` 或 `digest`。如果未指定，則預設爲 `keyfile`。
`keyfile`	(如果 `syntax=digest`，則爲必要參數) 包含摘要式認證之使用者資料的檔案路徑。
`digestfile`	(如果 `syntax=digest`，則爲必要參數) 包含摘要式認證使用者資料的檔案路徑。

注意 – 檔案認證資料庫檔案中每一行的長度上限爲 255。如果有任何一行超出此限制，伺服器將無法啓動，並將錯誤記錄到記錄檔中。

請確定在嘗試使用檔案型的認證資料庫設定 ACL 前，已經配置好檔案型的認證目錄服務。如需更多資訊，請參閱第 43 頁的「配置目錄服務」。

為基於檔案認證的目錄服務建立 ACL

▼ 為基於檔案認證的目錄服務建立 ACL

1. **存取伺服器實例的 Server Manager。**
2. **在 [Preferences] 標籤上，按一下 [Administer Access Control] 連結。**
3. **從下拉式清單選取 ACL 檔案，然後按一下 [Edit]。**
4. **在 [Access Control Rules For] 頁面中，按一下要編輯之 ACL 項目的 [Users/Groups] 連結。**
   [User/Group] 頁面會顯示在下方框架中。
5. **從 [Authentication Database] 下的下拉式清單，指定金鑰檔案資料庫。**
6. **按一下 [Update]，再按一下 [Submit] 以儲存變更。**
   當您依據金鑰檔案型的檔案認證資料庫設定 ACL 時，將使用相應的 ACL 項目更新 `dbswitch.conf` 檔案，例如以下所提供的範例項目：

```
version 3.0;acl "default";authenticate (user) {prompt =
"Sun Java System Proxy Server 4.0";database = "mykeyfile";
method = "basic";};deny (all) user = "anyone";
allow (all) user = "all";
```

為基於摘要式認證的目錄服務建立 ACL

檔案認證資料庫也支援適於和摘要式認證一起使用的檔案格式 (根據 RFC 2617)。此舉會儲存基於密碼和範圍產生的雜湊。不會維護明文密碼。

▼ 為基於摘要式認證的目錄服務建立 ACL

1. **存取伺服器實例的 Server Manager。**
2. **在 [Preferences] 標籤上，按一下 [Administer Access Control] 連結。**
3. **從下拉式清單選取 ACL 檔案，然後按一下 [Edit]。**
4. **在 [Access Control Rules For] 頁面，按一下要編輯之 ACL 的 [Users/Groups] 連結。**
   [User/Group] 頁面會顯示在下方框架中。
5. **在 [Authentication Database] 下的下拉式清單中，指定摘要資料庫。**
6. **按一下 [Update]，再按一下 [Submit] 以儲存變更。**
   當您依據摘要式認證型檔案認證資料庫設定 ACL 時，將使用相應的 ACL 項目更新 `dbswitch.conf` 檔案，例如以下所提供的範例項目。

```
version 3.0;acl "default";authenticate (user) {prompt = "filerealm";
database = "mydigestfile";method = "digest";}; deny (all) user = "anyone";
allow (all) user = "all";
```

◆ ◆ ◆ 第 9 章

9 使用記錄檔

您可以使用幾種不同的方法來監視伺服器的作業。本章論述了透過記錄和檢視記錄檔監視伺服器的方式。如需有關使用內建效能監視服務或 SNMP 的資訊，請參閱第 10 章「監視伺服器」。

本章包含下列小節：

關於記錄檔

伺服器記錄檔可記錄伺服器的作業。可以使用這些記錄來監視伺服器以及幫助您進行疑難排解。錯誤記錄檔位於伺服器根目錄的 `proxy-server_name/logs/errors` 中，其中列出了伺服器遇到的所有錯誤。存取記錄位於伺服器根目錄的 `proxy-server_name/logs/access` 中，其中記錄了有關向伺服器提出的請求及伺服器做出的回應的資訊。您可以配置 Proxy Server `access` 記錄檔中記錄的資訊。請使用記錄分析器來產生伺服器統計資料。您可以透過歸檔伺服器的錯誤記錄檔和存取記錄檔，對其進行備份。

備註 – 由於作業系統的限制，Proxy Server 在 Linux 上無法處理超過 2 GB 的記錄檔。一旦達到最大的檔案大小，記錄將停止。

在 UNIX 和 Windows 平台上記錄

本小節論述記錄檔的建立方法。另外，本小節還包括下列主題：

- 第 160 頁的 「預設錯誤記錄」
- 第 160 頁的 「使用 syslog 進行記錄」

備註 – 如需關於 Windows 作業環境使用的事件記錄機制的更多資訊，請參閱 Windows 說明系統索引，查找關鍵字「事件記錄」。

預設錯誤記錄

在 UNIX 和 Windows 平台上，Administration Server 的記錄都會收集在管理 `proxy-admserv/logs/` 目錄中。伺服器實例的記錄收集在 `proxy-server_name/logs/` 目錄中。

可以爲整部伺服器設定預設的記錄層級。您可以將 `stdout` 和 `stderr` 重新導向至伺服器的事件記錄，並將記錄輸出導向至作業系統的系統記錄檔中。此外，您也可將 stdout 和 stderr 內容導向至伺服器的事件記錄中。依預設，記錄訊息除傳送至指定的伺服器記錄檔以外，也傳送至 stderr。

使用 `syslog` 進行記錄

對於需要進行集中記錄的穩定作業環境而言，`syslog` 是適用的。對於經常需要輸出記錄以便診斷和除錯的環境而言，個別伺服器實例記錄可能更容易管理。

由於若將伺服器實例和 Administration Server 的記錄資料儲存在一個檔案內，可能會造成不易閱讀和除錯，因此只適合對穩定執行的已部署應用程式使用 `syslog` 主記錄檔。

已記錄的訊息會和 Solaris 常駐程式應用程式中的所有其他記錄混雜在一起。

使用 `syslog` 記錄檔，並結合 `syslogd` 及系統記錄常駐程式，您可以配置 `syslog.conf` 檔案以執行下列動作：

- 將訊息記錄到適當的系統記錄中
- 將訊息寫入至系統主控台
- 將記錄的訊息轉寄至使用者清單，或透過網路將其轉寄至另一台主機上的另一個 `syslogd`

由於記錄至 syslog 表示來自 Proxy Server 和其他常駐程式應用程式的記錄都要集中在同一個檔案裡，因此下列資訊會增強已記錄的訊息，以識別特定伺服器實例的特定 Proxy Server 訊息：

- 唯一的訊息 ID
- 時間戳記
- 實例名稱
- 程式名稱 (proxyd 或 proxyd-wdog)
- 程序 ID (proxyd 程序的 PID)
- 執行緒 ID (可選)
- 伺服器 ID

可以在 server.xml 檔案中爲 Administration Server 和伺服器實例配置 LOG 元素。

如需有關 UNIX 作業環境中使用的 syslog 記錄機制的更多資訊，請在終端機提示符號處使用下列 man 指令：

```
man syslog
man syslogd
man syslog.conf
```

記錄層級

下表依嚴重性遞增順序定義了 Proxy Server 中的記錄層級與訊息。

表 9–1 記錄層級

記錄層級	說明
finest	訊息指示除錯訊息的詳細度範圍。finest 提供最高詳細度。
finer	
fine	
info	訊息實際上是有益的，通常與伺服器配置或伺服器狀態有關。這些訊息不指示需要立即採取動作的錯誤。
warning	訊息表示一條警告。該訊息可能伴有異常。
failure	訊息指示發生相當嚴重的故障，可能會阻止應用程式正常執行。
config	訊息與各種靜態配置資訊有關，可協助對可能與特定配置關聯的問題進行除錯。
security	訊息指示發生安全問題。
catastrophe	訊息指示發生嚴重錯誤。

歸檔記錄檔

您可以將存取和錯誤記錄檔設定爲自動歸檔。記錄會在特定的時間或指定的間隔後自動重建。Proxy Server 會儲存舊記錄檔，並使用包含儲存日期和時間的名稱，爲已儲存的檔案加上戳記。

例如，您可以設定您的存取記錄檔於每小時自動重建一次。Proxy Server 會儲存檔案並將檔案命名爲「`access.200505160000`」，其中的記錄檔名稱、年、月、日和 24 小時制時間均會鏈結成一個字元串。依據您設定的記錄自動重建類型的不同，記錄歸檔檔案的格式也會不同。

Proxy Server 提供兩種用於歸檔檔案的記錄自動重建類型：內部常駐程式記錄自動重建及基於 cron 的記錄自動重建。

內部常駐程式記錄自動重建

內部常駐程式記錄自動重建會在 HTTP 常駐程式中發生，且只能在啓動時配置。伺服器會於內部自動重建記錄，不需要重新啓動伺服器。使用此方法重新記錄的記錄將以下列格式儲存：

```
access.<YYYY><MM><DD><HHMM>
```

```
errors.<YYYY><MM><DD><HHMM>
```

您可以指定用作自動重建記錄檔和啓動新記錄檔的時間依據。例如，如果自動重建開始時間爲上午 12:00，且自動重建間隔爲 1440 分鐘 (一天)，則當您儲存及套用變更時，不論當時是幾點，都會立即建立一個新的記錄檔。記錄檔會在每天上午 12:00 自動重建，並會在上午 12:00 將存取記錄加上戳記，並且另存新檔爲 `access.200505172400`。同樣地，如果設定間隔爲 240 分鐘 (4 小時)，4 個小時間隔會從上午 12:00 開始起算，因此存取記錄檔會包含從上午 12:00 到上午 4:00、上午 4:00 到上午 8:00 之間收集的資訊，依此類推。

如果有啓用記錄自動重建，則記錄檔自動重建會從伺服器啓動時開始。要循環的第一個記錄檔將從目前時間到下一個循環時間收集資訊。以上述範例爲例，如果設定開始時間爲上午 12:00，自動重建間隔爲 240 分鐘，且目前時間爲上午 6:00，則自動重建的第一個記錄檔會包含從上午 6:00 到上午 8:00 之間收集的資訊；下一個記錄檔會包含從上午 8:00 到下午 12:00 (中午) 收集的資訊，依此類推。

基於排程程式的記錄自動重建

基於排程程式的記錄自動重建是依據 `server.xml` 檔案內儲存的時間和日期進行的，該檔案位於 *server-root*`/proxy-` *server_name*`/config/` 目錄。這種方法可讓您立即歸檔記錄檔或在特定日期的特定時間使用伺服器來歸檔記錄檔。伺服器的排程程式配置選項均儲存在 `server-root/proxy-`*server_name*`/config/` 目錄中的 `server.xml` 中。使用基於排程程式的方法自動重建的記錄將以下列格式儲存：

<original_filename>.<YYYY><MM><DD><HHMM>

例如，若在下午 4:30 自動重建 access，其可能成爲 access.200505171630。

伺服器啓動時，將初始化記錄循環。如果自動重建已開啓，Proxy Server 會建立帶有時間戳記的存取記錄檔，並且會在伺服器啓動時開始自動重建。

一旦自動重建啓動，每當在需要記錄至存取記錄檔或錯誤記錄檔之預先排定的「下次自動重建時間」之後發生請求或錯誤時，Proxy Server 就會建立一個包含新時間戳記的記錄檔。

備註 – 執行記錄分析器之前，應歸檔伺服器記錄。

若要歸檔記錄檔，並指定使用內部常駐程式方法，還是使用基於排程程式的方法，請使用 Server Manager 中的 [Archive Log] 頁面。

設定存取記錄偏好設定

在安裝期間，會爲伺服器建立一個名稱爲 access 的存取記錄檔。透過指定是否要記錄存取、要使用的記錄格式，以及伺服器是否應在用戶端存取資源時花費時間查詢它們的網域名稱，您可以爲任何資源自訂存取記錄。

您可以使用 Server Manager 中的 [Set Access Log Preferences] 頁面來指定記錄喜好設定，也可以手動配置 obj.conf 檔案中的指令。在 obj.conf 中，伺服器會呼叫函數 flex-init 來初始化彈性記錄系統，並呼叫函數 flex-log 以彈性記錄格式記錄請求特定的資料。若要使用共用記錄檔格式來記錄請求，伺服器會呼叫 init-clf 來初始化 obj.conf 中使用的「共用記錄」子系統，並呼叫 common-log 以大多數 HTTP 伺服器使用的共用記錄格式來記錄請求特定的資料。

一旦建立了資源的存取記錄，您便無法變更其格式，除非將其歸檔或爲該資源建立新的存取記錄檔。

表 9–2 Administration Server 的記錄檔格式

記錄格式項目	說明
Client Hostname	請求存取的用戶端主機名稱 (如果已停用 DNS，則爲 IP 位址)。
Authenticate User Name	如果需要進行認證，您可以在存取記錄中列出通過認證的使用者名稱。
System Date	用戶端請求的日期與時間。

表 9–2 Administration Server 的記錄檔格式 *(續)*

記錄格式項目	說明
Full Request	用戶端發出的確切請求。
Status	伺服器傳回用戶端的狀態碼。
Content Length	傳送給用戶端的文件內容長度 (以位元組爲單位)。
HTTP Header, "referer"	參考指定一個頁面，用戶端從此頁面存取目前頁面。例如，如果使用者是從文字搜尋查詢查看結果，則參考者就是使用者從中存取文字搜尋引擎的頁面。參考者允許伺服器建立回溯的連結清單。
HTTP Header, "user-agent"	使用者代理程式資訊，包括用戶端使用的瀏覽器類型、版本及瀏覽器執行所在的作業系統。此項資訊來自用戶端傳送給伺服器的 HTTP 標頭資訊內的 [User-agent] 欄位。
Method	使用的 HTTP 請求方法，例如 GET、PUT 或 POST。
URI	通用資源識別碼。伺服器上資源的位置。例如，對於 `http://www.a.com:8080/special/docs`，其 URI 爲 `special/docs`。
Query String Of The URI	URI 中問號之後的所有文字。例如，在 `http://www.a.com:8080/special/docs?find_this` 中，URI 的查詢字串爲 `find_this`。
Protocol	使用的傳輸協定和版本。

當變更現有記錄檔的格式時，應該先將現有記錄檔刪除/重新命名，或是改用不同的檔案名稱。

▼ 設定 Administration Server 的存取記錄喜好設定

1. **存取 Administration Server，然後按一下 [Preferences] 標籤。**
2. **按一下 [Set Access Log Preferences] 連結。**
   此時會顯示 [Set Access Log Preferences] 頁面。
3. **從下拉式清單中選取資源，或按一下 [Regular Expression] 按鈕，然後鍵入常規表示式並按一下 [OK]。**

4. **指定是否要記錄用戶端存取。**

   此設定要求啓用 Domain Name Service (DNS)。

5. **為存取記錄檔指定絕對路徑。**

   依預設，記錄檔會儲存在伺服器根目錄的 `logs` 目錄中。如果指定部分路徑，伺服器將假設此路徑是伺服器根目錄中 `logs` 目錄的相對路徑。

   如果您是在編輯整個伺服器，則此欄位的預設值爲 `$accesslog`，它是配置檔案中表示伺服器存取記錄檔的變數。

6. **選擇是否要在存取記錄中記錄存取伺服器的系統之網域名稱或 IP 位址。**

7. **選擇要在存取記錄中使用的記錄檔格式類型。**

   下列爲可用的選項：

   - **Use Common** *LogFile Format*。包括用戶端的主機名稱、通過認證的使用者名稱、請求日期及時間、HTTP 標頭、傳回用戶端的狀態碼以及傳送至用戶端的文件內容長度。
   - **Only Log**。讓您決定要記錄哪些資訊。您可以從表 9–2 列出的彈性記錄格式項目中進行選擇。
   - 如果您選擇自訂格式，請在 [Custom Format] 欄位中鍵入格式。

8. **按一下 [OK]。**

9. **按一下 [Restart Required]。**

   此時會顯示 [Apply Changes] 頁面。

10. **按一下 [Restart Proxy Server] 按鈕以套用變更。**

設定伺服器實例的存取記錄喜好設定

下表列出的彈性記錄格式，可讓您用來設定伺服器實例的存取記錄喜好設定。

表 9–3 伺服器實例的記錄檔格式

記錄格式項目	說明
Client Hostname	請求存取的用戶端主機名稱 (如果已停用 DNS，則爲 IP 位址)。
Authenticate User Name	如果需要進行認證，您可以在存取記錄中列示經認證的使用者名稱。

表 9–3 伺服器實例的記錄檔格式 (續)

記錄格式項目	說明
System Date	用戶端請求的日期與時間。
Full Request	用戶端發出的確切請求。
Status	伺服器傳回用戶端的狀態碼。
Content Length	傳送給用戶端的文件內容長度 (以位元組爲單位)。
HTTP Header, "referer"	參考指定一個頁面，用戶端從此頁面存取目前頁面。例如，如果使用者是從文字搜尋查詢查看結果，則參考者就是使用者從中存取文字搜尋引擎的頁面。參考者允許伺服器建立回溯的連結清單。
HTTP Header, "user-agent"	使用者代理程式資訊，包括用戶端使用的瀏覽器類型、版本及瀏覽器執行所在的作業系統。此項資訊來自用戶端傳送給伺服器的 HTTP 標頭資訊內的 [User-agent] 欄位。
Method	使用的 HTTP 請求方法，例如 GET、PUT 或 POST。
URI	通用資源識別碼。伺服器上資源的位置。例如，對於 `http://www.a.com:8080/special/docs`，其 URI 爲 `special/docs`。
Query String Of The URI	URI 中問號之後的所有文字。例如，在 `http://www.a.com:8080/special/docs?find_this` 中，URI 的查詢字串爲 `find_this`。
Protocol	使用的傳輸協定和版本。

表 9–3 伺服器實例的記錄檔格式 *(續)*

記錄格式項目	說明
Cache Finish Status	此欄位指定快取檔案是被寫入、重新整理，還是由最新狀態檢查傳回。 cs 欄位可保留以下內容之一： - 表示資源不可快取。 WRITTEN 表示已建立快取檔案。 REFRESHED 表示已更新或重新整理快取檔案。 NO-CHECK 表示在傳回快取檔案時未進行最新狀態檢查。 UP-TO-DATE 表示在傳回快取檔案時進行了最新狀態檢查。 HOST-NOT-AVAILABLE 表示遠端伺服器不可用於進行最新狀態檢查，因此未檢查就傳回了快取檔案。 CL-MISMATCH 表示因內容長度不符而中斷了快取檔案寫入。 ABORTED 表示因特殊緣由而中斷了快取。例如，缺少有效的 Last-Modified 標頭。
Remote Server Finish Status	此欄位指出向遠端伺服器提出的請求是順利執行完成、在用戶端按一下瀏覽器中的 [Stop] 按鈕後被中斷，或因錯誤狀況而中斷。
Status Code From Server	伺服器傳回的狀態碼。
Route To Proxy (PROXY, SOCKS, DIRECT)	用於擷取資源的路由。文件可以透過代理伺服器或透過 SOCKS 伺服器直接擷取。
Transfer Time	傳輸時間長度 (以秒或毫秒爲單位)。
Header-length From Server Response	來自伺服器回應的標頭長度。
Request Header Size From Proxy To Server	自代理伺服器傳送至伺服器的請求標頭大小。
Response Header Size Sent To Client	傳送至用戶端的回應標頭大小。
Request Header Size Received From Client	自用戶端收到的請求標頭大小。
Content-length From Proxy To Server Request	自代理伺服器傳送至伺服器的文件長度 (以位元組爲單位)。
Content-length Received From Client	來自用戶端的文件長度 (以位元組爲單位)。
Content-length From Server Response	來自伺服器的文件長度 (以位元組爲單位)。
Unverified User From Client	認證期間向遠端伺服器提供的使用者名稱。

▼ 設定伺服器實例的存取記錄喜好設定

1. **存取 Server Manager，然後按一下 [Server Status] 標籤。**

2. **按一下 [Set Access Log Preferences] 連結。**
   此時會顯示 [Set Access Log Preferences] 頁面。

3. **從下拉式清單中選取資源，或按一下 [Regular Expression] 按鈕，然後鍵入常規表示式並按一下 [OK]。**

4. **指定是否要記錄用戶端存取。**
   此設定要求啓用 Domain Name Service (DNS)。

5. **為存取記錄檔指定絕對路徑。**
   依預設，記錄檔會儲存在伺服器根目錄的 `logs` 目錄中。如果指定部分路徑，伺服器將假設此路徑是伺服器根目錄中 `logs` 目錄的相對路徑。

   如果您是在編輯整個伺服器，則此欄位的預設值爲 `$accesslog`，它是配置檔案中表示伺服器存取記錄檔的變數。

6. **選擇是否要在存取記錄中記錄存取伺服器的系統之網域名稱或 IP 位址。**

7. **選擇記錄檔應使用的格式：共用、延伸、延伸-2、僅指定的資訊 ([Only log] 單選按鈕) 或自訂。**
   如果您按一下 [Only log]，將可以使用下列彈性記錄格式項目：

8. **選擇要在存取記錄中使用的記錄檔格式類型。**
   伺服器存取記錄可以使用共用記錄檔格式、延伸記錄檔格式、延伸 2 記錄檔格式、彈性記錄格式，或您自己的自訂格式。共用記錄檔格式爲通常受支援的格式，可提供固定數量的伺服器資訊。彈性記錄格式可讓您從 Proxy Server 選擇所要記錄的內容。可自訂格式使用您指定的參數區段來控制記錄的內容。

   - **Use Common** *LogFile Format*。包括用戶端的主機名稱、通過認證的使用者名稱、請求日期及時間、HTTP 標頭、傳回用戶端的狀態碼以及傳送至用戶端的文件內容長度。
   - **Use Extended** *LogFile Format*。包括共用記錄檔格式的所有欄位，加上一些額外欄位，諸如遠端狀態、代理伺服器至用戶端的內容長度、遠端至代理伺服器的內容長度、代理伺服器至遠端的內容長度、用戶端至代理伺服器的標頭長度、代理伺服器至用戶端的標頭長度、代理伺服器至遠端的標頭長度、遠端至代理伺服器的標頭長度以及傳輸時間。
   - **Use Extended2** *LogFile Format*。包括延伸記錄檔格式的所有欄位，加上一些額外欄位，諸如用戶端狀態、伺服器狀態、遠端狀態、快取完成狀態以及實際路由。

- **Only Log**。可讓您選擇要記錄的資訊。您可以從表 9–3 列出的彈性記錄格式項目中進行選擇。
- 如果您選擇自訂格式，請在 [Custom Format] 欄位中鍵入格式。

9 **如果您不想記錄來自特定主機名稱或 IP 位址的用戶端存取，請在 [host names] 及 [IP Addresses] 欄位中鍵入該主機名稱與 IP 位址。**

請鍵入伺服器不應記錄存取的主機萬用字元式樣。例如，`*.example.com` 將不會記錄網域名稱爲 example.com 的人員存取。您可以鍵入主機名稱、IP 位址或兩者的萬用字元式樣。

10 **選擇是否要在記錄檔中包括格式字串。**

如果您要使用 Proxy Server 的記錄分析器，就應該包括格式字串。如果您要使用協力廠商的分析器，最好不要在記錄檔中包括格式字串。

11 **按一下 [OK]。**

12 **按一下 [Restart Required]。**

此時會顯示 [Apply Changes] 頁面。

13 **按一下 [Restart Proxy Server] 按鈕以套用變更。**

簡便的 Cookie 記錄

Proxy Server 提供了使用 flexlog 功能記錄特定 cookie 的簡便方式。將 `Req->headers.cookie.cookie_name` 增加到初始化 `flex-log` 子系統的行中，此行位於 `obj.conf` 配置檔中。如果請求標頭提供了 cookie 變數，則指令將記錄 `cookie_name` 變數的值，如果未提供，則記錄爲 -。

設定錯誤記錄選項

您可以配置要在伺服器的錯誤記錄中記錄的資訊。

▼ 設定錯誤記錄選項

1 **若要從 Administration Server 設定錯誤記錄選項，請選擇 [Preferences] 標籤，然後按一下 [Set Error Log Preferences] 連結。**

若要從 Server Manager 設定伺服器實例的錯誤記錄選項，請選擇 [Server Status] 標籤，然後按一下 [Set Error Log Preferences] 連結。

2 **在 [Error Log File Name] 欄位中，指定儲存伺服器訊息的檔案。**

3. **從記錄層級下拉式清單中，指定要在錯誤記錄中記錄的資訊量。下列為可用的選項：**
4. **若要將 stdout 輸出重新導向至錯誤記錄，請選取 [Log Stdout]。**
5. **若要將 stderr 輸出重新導向至錯誤記錄，請選取 [Log Stderr]。**
6. **若要將記錄訊息重新導向至主控台，請選取 [Log To Console]。**
7. **若要使用 UNIX syslog 服務或 Windows 事件記錄來產生和管理記錄，請選取 [Use System Logging]。**
8. **按一下 [OK]。**
9. **按一下 [Restart Required]。**
   此時會顯示 [Apply Changes] 頁面。
10. **按一下 [Restart Proxy Server] 按鈕以套用變更。**

配置 LOG 元素

下表說明可以在 `server.xml` 檔案中配置的 LOG 元素屬性。

表 9–4 LOG 屬性

屬性	預設值	說明
`file`	`errors`	指定儲存伺服器訊息的檔案。
`loglevel`	`info`	控制由其他元素記錄到錯誤記錄中的訊息的預設類型。允許\值依從最高到最低的次序，列示如下： `finest`、`fine`、`fine`、 `info`、`warning`、`failure`、`config`、`security` 及 `catastrophe`。
`logstdout`	`true`	(可選) 如果是 `true`，則將 `stdout` 輸出重新導向至錯誤記錄。有效值包括 `on`、 `off`、`yes`、`no`、`1`、 `0`、`true`、 `false`。
`logstderr`	`true`	(可選) 如果是 `true`，則將 `stderr` 輸出重新導向至錯誤記錄。有效值包括 `on`、 `off`、`yes`、`no`、`1`、 `0`、`true`、 `false`。
`logtoconsole`	`true`	(可選，僅限於 UNIX) 如果爲 `true`，則將記錄訊息重新導向至主控台。

表 9–4 LOG 屬性 (續)

屬性	預設值	說明
createconsole	false	(可選，僅限於 Windows) 如果爲 true，則針對 stderr 輸出建立一個 Windows 主控台。有效值包括 on、off、yes、no、1、0、true、false。
usesyslog	false	(可選) 如果爲 true，則使用 UNIX syslog 服務或 Windows 事件記錄來產生和管理記錄。有效值包括 on、off、yes、no、1、0、true、false。

檢視存取記錄檔

您可以檢視伺服器的使用中存取記錄檔和已歸檔存取記錄檔。

若要從 Administration Server 檢視它的存取記錄，請選擇 [Preferences] 標籤，然後按一下 [View Access Log] 連結。

若要從 Server Manager 檢視伺服器實例的存取記錄，請選擇 [Server Status] 標籤，然後按一下 [View Access Log] 連結。

下列範例顯示了共用記錄檔格式的存取記錄。

```
198.18.17.222 - - [20/May/2005:14:15:49 +0530]
"GET http://www.example.com/ HTTP/1.1" 504 622 198.18.17.222 - abc
[20/May/2005:14:16:09 +0530] "GET http://www.test.com/report.zip HTTP/1.1"
504 630
```

下表說明此範例存取記錄的最後一行。

存取記錄欄位	範例
用戶端主機名稱或 IP 位址	198.18.17.222 (在此範例中顯示的是用戶端的 IP 位址，因爲代理伺服器已停用 DNS 查找設定；如果有啓用 DNS 查找，則會顯示用戶端的主機名稱)。
RFC 931 資訊	- (未執行 RFC 931 識別)
使用者名稱	*abc* (用戶端進行認證時輸入的使用者名稱)
請求的日期/時間	20/May/2005:14:16:09 +0530
請求	GET
協定	HTTP/1.1

存取記錄欄位	範例
狀態碼	504
傳輸的位元組	630

檢視錯誤記錄檔

錯誤記錄檔中包含自建立記錄檔以來，伺服器所遇到的錯誤。此檔案中亦包含有關伺服器的資訊訊息，例如伺服器啓動時間。錯誤記錄中還記錄未成功的使用者認證。請使用錯誤記錄尋找中斷的 URL 路徑或遺漏的檔案。

若要檢視 Administration Server 的錯誤記錄檔，請從 Administration Server 中，選擇 [Preferences] 標籤，並按一下 [View Error Log] 連結。

若要檢視伺服器實例的錯誤記錄檔，請從 Server Manager 中，選擇 [Server Status] 標籤，並按一下 [View Error Log] 連結。

以下錯誤記錄範例共包含三個項目：

```
20/May/2005:14:08:37] info ( 6141): CORE1116: Sun Java System Web Proxy
Server 4.0 B05/10/2005 01:26 20/May/2005:14:08:37] info ( 6142): CORE3274:
successful server startup 20/May/2005:14:08:37] security (23246):
for host 198.18.148.89 trying to GET /, deny-service reports:
 denying service of /
```

使用記錄分析器

server-root/extras/log_anly 目錄中包含透過 Server Manager 使用者介面執行的記錄分析工具。此記錄分析器僅分析使用共用記錄格式的檔案。log_anly 目錄中的 HTML 文件對工具的參數進行了說明。server-install/extras/flexanlg 目錄中包含針對彈性記錄檔格式的指令行記錄分析器。但是不論您選取的記錄檔格式爲何，Server Manager 均會預設爲使用彈性記錄檔報告工具。

使用記錄分析器可以產生關於預設伺服器的統計資料，例如活動摘要、最常存取的 URL、一日內反復存取伺服器的次數，等等。您可以從 Proxy Server 或從指令行執行記錄分析器。

您必須先設定程式庫路徑，然後才可以嘗試執行 flexanlg 指令行公用程式。各種平台的設定如下：

Solaris 和 Linux：

```
LD_LIBRARY_PATH=server-root/bin/proxy/lib:$LD_LIBRARY_PATH
```

AIX：

```
LIBPATH=server-root/bin/proxy/lib:$LIBPATH
```

HP-UX：

```
SHLIB_PATH=server-root/bin/proxy/lib:$SHLIB_PATH
```

Windows：

```
path=server-root\\bin\\proxy\\bin;%path%
```

備註 – 執行記錄分析器之前，應先將伺服器記錄歸檔。如需有關歸檔伺服器記錄的更多資訊，請參閱第 162 頁的 「歸檔記錄檔」。

您也可以先轉到 `server-root/proxy-server`*id* 目錄，然後於指令提示符號處鍵入 `./start -shell`，而不用設定程式庫路徑。

如果您使用延伸或延伸-2 記錄格式，則除了您指定要報告的資訊外，記錄分析器還會在輸出檔案中產生數項報告。下列幾個小節說明這些報告。

傳輸時間分配報告

傳輸時間分配報告會顯示代理伺服器傳輸請求所用的時間。此報告依服務時間和完成百分比將資訊分類顯示。以下範例爲傳輸時間分配報告的範例。

By service time category:

```
< 1 sec [644%] ....................................
< 2 sec [33.3%] ...................
< 3 sec [ 2.7%] .
< 4 sec [ 1.7%] .
< 5 sec [ 0.6%]
< 6 sec [ 0.4%]
< 7 sec [ 0.2%]
< 8 sec [ 0.0%]
< 9 sec [ 0.0%]
```

By percentage finished:

```
< 1 sec [64.4%] ....................................

< 2 sec [97.7%] ....................................

< 3 sec [100.4%]..........................................
```

資料流量報告

資料流量報告顯示從用戶端到代理伺服器、從代理伺服器到用戶端、從代理伺服器到遠端伺服器，以及從遠端伺服器到代理伺服器之間的資料流量 (所傳輸的位元組數)。報告會針對每種分析藍本，顯示以標頭與內容形式傳輸的資料量。資料流量報告也會顯示從快取記憶體到用戶端之間的資料流量。以下是資料流量報告的範例。

	Headers	Content	Total
- Client -> Proxy.....	0 MB	0 MB	0 MB
- Proxy -> Client.....	0 MB	2 MB	3 MB
- Proxy -> Remote.....	0 MB	0 MB	0 MB
- Remote -> Proxy.....	0 MB	2 MB	2 MB
Approx:			
- Cache -> Client.....	0 MB	0 MB	0 MB

狀態碼報告

狀態碼報告顯示代理伺服器自遠端伺服器收到，及傳送至用戶端的狀態碼項目與數目。狀態碼報告也會提供所有這些狀態碼的說明。以下是狀態碼報告的範例。

Code	-From remote-	-To client-	-Explanation-
200	338 [70.7%]	352 [73.6%]	OK
302	33 [6.9%]	36 [7.5%]	Redirect
304	90 [18.8%]	99 [20.7%]	Not modified
404	3 [0.6%]	3 [0.6%]	Not found

Code	-From remote-	-To client-	-Explanation-
407		5 [1.0%]	Proxy authorization required
500		2 [0.4%]	Internal server error
504		6 [1.3%]	Gateway timeout

請求與連線報告

請求與連線報告顯示代理伺服器收到的用戶端請求數目、代理伺服器向遠端伺服器發出的連線數目 (初始擷取、最新狀態檢查及重新整理)，以及代理伺服器使用快取文件而避免的遠端連線數目。以下是請求與連線報告的範例。

```
- Total requests.............     478
- Remote connections.........     439
- Avoided remote connects....      39 [ 8.2%]
```

快取效能報告

快取效能報告顯示用戶端快取、代理伺服器快取以及直接連線的效能。

用戶端快取

當用戶端對文件執行最新狀態檢查時，如果遠端伺服器傳回 304 訊息，告知用戶端此文件並未修改，就表示有用戶端快取符合項目。若用戶端啓動最新狀態檢查，即表示用戶端在快取記憶體中擁有自己的文件副本。

對於用戶端快取，此報告會顯示：

- **Client and proxy cache hits:**一種用戶端快取符合項目，在這種符合項目中，代理伺服器和用戶端皆擁有所請求文件的副本，並且查詢遠端伺服器，以進行代理伺服器副本的最新狀態檢查，並依代理伺服器的副本來評估用戶端請求。快取效能報告會顯示代理伺服器處理的這類請求數目，及代理伺服器處理這類請求所花的平均時間。
- **Proxy shortcut no-check:**一種用戶端快取符合項目，在這種符合項目中，代理伺服器和用戶端皆擁有所請求文件的副本，代理伺服器將告知用戶端 (無需和遠端伺服器確認) 在用戶端快取記憶體中的文件爲最新版本。快取效能報告可顯示代理伺服器處理的這類請求數目，及代理伺服器用於處理這類請求的平均時間。
- **Client cache hits only:**一種用戶端快取符合項目，在這種符合項目中，僅用戶端擁有所請求文件的快取副本。在這類請求中，代理伺服器直接爲用戶端的 If-modified-since GET 標頭建立通道。快取效能報告可顯示代理伺服器處理的這類請求數目，及代理伺服器用於處理這類請求的平均時間。

- **Total client cache hits:**用戶端快取符合項目總數及用於服務此類請求的平均時間。

代理伺服器快取

當用戶端向代理伺服器請求文件，且該代理伺服器的快取中具備此份文件時，就表示有代理伺服器快取符合項目。對於代理伺服器的快取符合項目，此報告會顯示：

- **Proxy cache hits with check:**一種代理伺服器快取符合項目，在這種符合項目中，代理伺服器會查詢遠端伺服器，以對文件進行最新狀態檢查。快取效能報告可顯示代理伺服器處理的這類請求數目，及代理伺服器用於處理這類請求的平均時間。
- **Proxy cache hits without check:**一種代理伺服器快取符合項目，在這種符合項目中，代理伺服器**不會**查詢遠端伺服器，所以不會對文件進行最新狀態檢查。快取效能報告可顯示代理伺服器處理的這類請求數目，及代理伺服器用於處理這類請求的平均時間。
- **pure proxy cache hits:**一種代理伺服器快取符合項目，在這種符合項目中，用戶端沒有所請求文件的快取副本。快取效能報告可顯示代理伺服器處理的這類請求數目，及代理伺服器用於處理這類請求的平均時間。

合併的代理伺服器快取符合項目

對於合併的代理伺服器快取符合項目，報告會顯示代理伺服器快取的符合項目總數，以及代理伺服器服務這些請求所花費的平均時間。

直接作業事件

直接作業事件是指無任何快取符合項目而直接從遠端伺服器到代理伺服器再到用戶端的作業事件。對於直接作業事件，報告將顯示：

- **Retrieved documents:**直接從遠端伺服器擷取的文件。快取效能報告會顯示代理伺服器服務此類型請求的數目、服務這些請求所花費的平均時間，以及總作業事件的百分比。
- **Other transactions:**導致所傳回之狀態碼非 200 或 304 的作業事件。快取效能報告顯示代理伺服器服務此類型請求的數目和服務這些請求所花費的平均時間。
- **Total direct traffic:**直接從用戶端到遠端伺服器的請求 (包括失敗的請求與成功擷取的文件)。快取效能報告會顯示代理伺服器服務此類型請求的數目、服務這些請求所使用的平均時間，以及總作業事件的百分比。

以下是快取效能報告的範例。

```
                    CLIENT CACHE:
- Client & proxy cache hits... 86 reqs [18.0%] 0.21 sec/req- Proxy shortcut
no-check........ 13 reqs [ 2.7%] 0.00 sec/req- Client cache hits only.....
- TOTAL client cache hits.......... 99 reqs [20.7%] 0.18 sec/req

                    PROXY CACHE:
```

```
- Proxy cache hits w/check........ 4 reqs [ 0.8%] 0.50 sec/req- Proxy cache
hits w/o check.. 10 reqs [ 2.1%] 0.00 sec/req- Pure proxy cache hits......
14 reqs [ 2.9%] 0.14 sec/req

                    PROXY CACHE HITS COMBINED:
- TOTAL proxy cache hits....... 113 reqs [23.6%] 0.18 sec/req

                    DIRECT TRANSACTIONS:
- Retrieved documents..313 reqs [65.5%]  0.90 sec/req 2 MB- Other
transactions.. 52 reqs [10.9%] 7.79 sec/req- TOTAL direct traffic..
365 reqs [76.4%] 1.88 sec/req 2 MB
```

傳輸時間報告

傳輸時間報告顯示關於代理伺服器處理作業事件所用時間的資訊。此報告顯示下列類別的值：

Average transaction time:記錄的所有傳輸時間的平均值。

Average transfer time without caching:不是從快取傳回之作業事件 (導致遠端伺服器傳送 200 回應) 的平均傳輸時間。

Average with caching, without errors:所有無錯誤作業事件 (狀態碼爲 2xx 和 3xx) 的平均傳輸時間。

Average transfer time improvement:平均作業事件時間減去包含快取且無錯誤情況的平均傳輸時間。

以下是傳輸時間報告的範例。

```
- Average transaction time... 1.48 sec/req- Ave xfer time w/o caching..
    0.90 sec/req- Ave w/caching, w/o errors.. 0.71 sec/req - Ave xfer
    time improvement.. 0.19 sec/req
```

每小時作業報告

對於已分析的每個小時，每小時作業報告會顯示：

- 平均負載
- 不向遠端伺服器進行最新狀態檢查的快取符合項目數目
- 對遠端伺服器進行最新狀態檢查 (證明文件是最新的且位於用戶端快取記憶體中) 的代理伺服器快取符合項目數目
- 對遠端伺服器進行最新狀態檢查 (證明文件是最新的且**不**位於用戶端快取記憶體中) 的代理伺服器快取符合項目數目

- 對遠端伺服器進行最新狀態檢查 (導致文件的部分被更新) 的代理伺服器快取符合項目數目
- 對遠端伺服器進行最新狀態檢查 (傳回請求文件的新副本與 200 狀態碼) 的代理伺服器快取符合項目數目
- 從遠端伺服器直接擷取文件，且沒有任何代理伺服器快取符合項目的請求數目

▼ 從 Server Manager 執行記錄分析器

1. **存取 Server Manager，然後按一下 [Server Status] 標籤。**
2. **按一下 [Generate Report] 連結。**
   此時會顯示 [Generate Report] 頁面。
3. **鍵入您的伺服器名稱。此名稱會出現在產生的報告中。**
4. **選擇報告是以 HTML 格式還是 ASCII 格式顯示。**
5. **選取您要分析的記錄檔。**
6. **如果您想要將結果儲存於檔案中，請在 [Output File] 欄位中鍵入輸出檔案名稱。**
   如果保留此欄位爲空白，則報告結果將在螢幕上顯示。對於大型記錄檔，您應將結果儲存到檔案中，因爲將輸出顯示到螢幕上可能需要很長時間。
7. **選取是否為某些伺服器的統計資料產生小計。**
   可以產生以下小計：
   - **Total Hits**－啓用存取記錄以來伺服器接收的符合項目總數。
   - **304 (Not Modified) Status Codes**－所請求文件之本機副本的使用次數，而非伺服器傳回頁面的次數。
   - **302 (Redirects) Status Codes**－因原始 URL 移動而將伺服器重新導向至新 URL 的次數。
   - **404 (Not Found) Status Codes**－伺服器找不到所請求文件，或由於用戶端不是授權的使用者而未提供文件的次數。
   - **500 (Server Error) Status Codes**－發生與伺服器相關的錯誤次數。
   - **Total Unique URLs**－啓用存取記錄以來所存取的唯一 URL 之數目。
   - **Total Unique Hosts**－啓用存取記錄以來存取過伺服器的唯一主機數目。
   - **Total Kilobytes Transferred**－啓用存取記錄以來伺服器傳輸的千位元組數目。
8. **選擇是否產生一般統計資料。如果您選擇產生一般統計資料，請從以下選項中選擇：**

- **Find Top** *Number* **Seconds Of Log**－基於最近幾秒內的資訊產生統計資料。
- **Find Top** *Number* **Minutes Of Log**－
- 基於最近幾分鐘內的資訊產生統計資料。
- **Find Top** *Number* **Hours Of Log**－基於最近幾小時內的資訊產生統計資料。
- **Find** *Number* **Users (If Logged)**－基於使用者數目的資訊產生統計資料。
- **Find Top** *Number* **Referers (If Logged)**－基於參考者數目的資訊產生統計資料。
- **Find Top** *Number* **User Agents (If Logged)**－基於使用者代理程式的資訊 (例如瀏覽器類型、瀏覽器版本及作業系統) 產生統計資料。
- **Find Top** *Number* **Miscellaneous Logged Items (If Logged)**－基於使用者數目的資訊產生統計資料。

9 選擇是否產生清單。

如果您選擇產生清單，請指定要產生清單的項目：

- **URLs Accessed**－顯示已存取的 URL
- *Number* **Most Commonly Accessed URL**－顯示最常存取的 URL 或存取次數超過指定次數的 URL
- **URLs That Were Accessed More Than** *Number* **Times**－顯示存取次數超過指定次數的 URL
- **Hosts Accessing Your Server**－顯示存取 Proxy Server 的主機
- *Number* **Hosts Most Often Accessing Your Server**－顯示最常存取伺服器的主機，或存取伺服器的次數超過指定次數的主機
- **Hosts That Accessed Your Server More Than** *Number* **Times**－顯示存取伺服器次數超過指定次數的主機

10 指定察看結果的順序

按照您希望各部分在報告中顯示的順序，爲其指定從 1 至 3 的優先權。如果您選擇不產生任何優先權，此部分將自動被忽略。這些部分包括：

- 尋找小計
- 一般統計資料
- 產生清單

11 按一下 [OK]。

報告會在新視窗中顯示。

從指令行執行記錄分析器

若要從指令行分析存取記錄檔，請執行 `flexanlg` 工具 (位於 `server-install/extras/flexanlg` 目錄中)。

若要執行 flexanlg，請在指令提示符號處鍵入下列指令和選項：

```
./flexanlg [-n name] [-x] [-r] [-p order] [-i file]* [ -m metafile ]* [-o file]
[-c opts] [-t opts] [-l opts]
```

標記 * 的選項可以重複。

鍵入 `./flexanlg -h` 可以在線上取得此資訊。

```
-P: proxy log format                                    Default: no
-n servername: The name of the server
-x : Output in HTML                                     Default: no
-r : Resolve IP addresses to hostnames                  Default: no
-p [c,t,l]: Output order (counts, time stats, lists)  Default: ctl
-i filename: Input log file                             Default: none
-o filename: Output log file                            Default: stdout
-m filename: Meta file                                  Default: none
-c [h,n,r,f,e,u,o,k,c,z]: Count these item(s) -       Default: hnreuokc
    h: total hits
    n: 304 Not Modified status codes (Use Local Copy)
    r: 302 Found status codes (Redirects)
    f: 404 Not Found status codes (Document Not Found)
    e: 500 Server Error status codes (Misconfiguration)
    u: total unique URL's
    o: total unique hosts
    k: total kilobytes transferred
    c: total kilobytes saved by caches
    z: Do not count any items.
-t [sx,mx,hx, xx,z]: Find time stats -      Default:s5m5h10u10a10r10x10
    s(number): Find top (number) seconds of log
    m(number): Find top (number) minutes of log
    h(number): Find top (number) hours of log
    u(number): Find top (number) users of log
    a(number): Find top (number) user agents of log
    r(number): Find top (number) referers of log
    x(number): Find top (number) for miscellaneous keywords
    z: Do not find any time stats.
-l [cx,hx]: Make a list of -                            Default: c+3h5
    c(x,+x): Most commonly accessed URL's
             (x: Only list x entries)
             (+x: Only list if accessed more than x times)
    h(x,+x): Hosts (or IP addresses) most often accessing your server
             (x: Only list x entries)
             (+x: Only list if accessed more than x times)
    z: Do not make any lists.
```

檢視事件 (Windows)

除了將錯誤記錄到伺服器錯誤記錄之外，Proxy Server 還會將嚴重的系統錯誤記錄至事件檢視器。事件檢視器可讓您監視系統上的事件。使用事件檢視器，可查看開啓錯誤記錄之前可能發生的基礎配置問題所導致的錯誤。

▼ 使用時間事件檢視器

1 **從 [開始] 功能表中，選取 [程式集]，然後選取 [系統管理工具]。**

在 [系統管理工具] 程式群組中選擇 [事件檢視器]。

2 **從 [記錄] 功能表中選擇 [應用程式]。**

[應用程式] 記錄將顯示於 [事件檢視器] 中。Proxy Server 中的錯誤具有 `proxy-server`*id* 來源標籤。

3 **從 [檢視] 功能表中選擇 [尋找]，以在記錄中搜尋其中一個標籤。**

從 [檢視] 功能表中選擇 [重新顯示]，查看更新後的記錄項目。

如需關於事件檢視器的更多資訊，請參考您的系統文件。

◆ ◆ ◆ 第 10 章

10 監視伺服器

本章包含有關用於監視伺服器的方法資訊，包括使用內建監視工具及簡易網路管理協定 (SNMP)。

您可以將 SNMP 和 Sun Java System 管理資訊庫 (MIB) 以及網路管理軟體 (如 HP OpenView) 一起使用，以進行伺服器即時監視，就像您監視網路上的其他裝置一樣。

備註 – 在 Windows 上安裝 Proxy Server 4 之前，請確定您的系統上已安裝 Windows SNMP 元件。

您可以使用統計資料功能或 SNMP，即時檢視伺服器的狀態。如果您使用的是 UNIX 或 Linux，並且打算使用 SNMP，則必須針對 SNMP 配置您的 Proxy Server。

本章包含下列小節：

使用統計資料監視伺服器

您可以使用統計資料功能監視伺服器的目前作業。統計資料會顯示伺服器所處理的請求數，以及對這些請求的處理程度。如果互動式伺服器監視器報告該伺服器正在處理大量請求，則可能需要您調整伺服器配置或系統的網路核心以容納這些請求。依預設，統計資料爲停用狀態，因爲收集統計資料會增加 Proxy Server 的經常性耗用時間。啓用統計資料會使伺服器開始收集和儲存統計資訊。

一旦啓用統計資料之後，您將可以檢視下列方面的統計資料：

- 連線
- DNS
- KeepAlive
- 快取
- 伺服器請求

如需有關各種伺服器統計資料 (互動式伺服器監視器報告這些統計資料的總數) 的描述，請參閱\線上說明中的 [Monitor Current Activity] 頁面。

處理 Proxy Server 統計資料

系統會使用名稱爲 `stats-xml` 的內建函數來收集 Proxy Server 統計資料。必須啓用此函數，才能從 Server Manager 檢視統計資料，或使用 `perfdump` 函數來產生報告。`stats-xml` 函數亦用於啓用效能評測，它是透過使用自訂 NSAPI 函數監視統計資料所必需的。若在伺服器上啓用統計資料與效能評測，將會初始化 `obj.conf` 檔案中名爲 `stats-init` 的伺服器函數，使其開始收集統計資料。

```
Init profiling="on" fn="stats-init"
```

此指示也會建立一個 `NameTrans` 指令，讓您用來從瀏覽器視窗存取統計資料。

```
NameTrans fn="assign-name" name="stats-xml" from="(/stats-xml|/stats-xml/.*)
```

最後，當啓用統計資料時，會增加一個 `Service` 指令，以在選取 `NameTrans` 指令時用來處理 `stats-xml` 函數。

```
<Object name="stats-xml">

Service fn="stats-xml"

</Object>
```

收集統計資料時會更新 `obj.conf` 中的 Init 函數。因此，您必須停止並重新啓動伺服器，使這些變更開始生效。

下列範例顯示 `obj.conf` 檔案中的 `stats-init`：

```
Init profiling="on" fn="stats-init" update-interval="5"
```

您也可以指定下列值：

- **update-interval**。更新統計資料的間隔秒數。設定值較高時 (較不頻繁) 可以獲得較佳效能。最小值爲 1；預設值爲 5。
- **profiling**。是否要啓動 NSAPI 效能設定檔。預設值爲 *no*，這樣可稍微提升伺服器的效能。但是，若您是透過使用者介面啓動統計資料，則依預設會啓用設定檔。

您可以使用下列 URL 來擷取 `stats-xml` 輸出：

```
http://computer_name:proxyport /stats-xml/proxystats.xml
```

此請求會傳回一個 XML 頁面，其中包含 Proxy Server 統計資料。某些瀏覽器可讓您在瀏覽器視窗中檢視該資料；但有些瀏覽器則會要求您將資料儲存至外部檔案，再以外部檢視器檢視其內容。若無法剖析欲分析資料的不同檢視之統計，則此資訊的用途無法完全發揮。使用協力廠商工具將可以協助執行此程序。若無剖析工具，則最好透過 Server Manager 或 `perfdump` SAF 來觀察 `stats-xml` 輸出。

限制存取 `stats-xml` 輸出

若您想限制可從瀏覽器檢視伺服器 `stats-xml` 統計的使用者，則應爲 `/stats-xml` URI 建立 ACL。

`obj.conf` 檔案中的 `stats-xml` 物件定義也必須參照此 ACL 檔案。例如，如果您已爲 `/stats-xml` URI 建立了一個已命名的 ACL，就必須在物件定義中的 `PathCheck` 敘述內參照該 ACL 檔案，如下所示：

```
<Object name="stats-xml">

PathCheck fn="check-acl" acl="stats.acl"

Service fn="stats-xml"

</Object>
```

啓用統計資料

您必須先在 Proxy Server 上啓動統計資料，之後才能監視效能。您可以透過 Server Manager 來啓動統計資料，也可以編輯 `obj.conf` 和 `magnus.conf` 檔案來加以啓動。負責建立自動化工具或撰寫自訂程式以進行監視和調校的使用者，可能會偏好直接使用 `stats-xml`。

注意 – 啓用統計資料/設定檔時，伺服器的所有使用者都可使用統計資料資訊。

▼ 從 Server Manager 啓用統計資料

1. **存取 Server Manager，然後按一下 [Server Status] 標籤。**
2. **按一下 [Monitor Current Activity] 連結。**
   這時會顯示 [Monitor Current Activity] 頁面。
3. **在 [Activate Statistics/Profiling] 中選取 [Yes] 選項，以啓用統計資料。**
4. **按一下 [OK]。**
5. **按一下 [Restart Required]。**
   此時會顯示 [Apply Changes] 頁面。
6. **按一下 [Restart Proxy Server] 按鈕以套用變更。**

▼ 使用 stats-xml 啓用統計資料

1. **在 obj.conf 檔案的預設物件下，增加下列行：**

```
NameTrans fn="assign-name" name="stats-xml" from="
(/stats-xml|/stats-xml/.*)"
```

2. **將下列 Service 函數增加至 obj.conf 中：**

```
<Object name="stats-xml">

Service fn="stats-xml"

</Object>
```

3. **將 stats-init SAF 增加至 obj.conf 中。**

使用統計資料

一旦啓用統計資料，您就可以取得有關您的伺服器實例運作狀況的各項資訊。統計資料被分爲多個功能區域。

在 Server Manager 中顯示統計資料

本小節說明如何在 Server Manager 中檢視 proxystats.xml 資料的子集。

您可以檢視 Proxy Server 連線、DNS 處理、持續作用值、快取及伺服器請求等相關資訊之總數、最大值、尖峰值及長條圖。

以下小節說明可以在這些區域取得的資訊類型。

連線統計資料

下列連線統計資料可從 Server Manager 取得：

- 連線總數
- 最大佇列中連線數
- 佇列中連線之尖峰數
- 目前佇列中連線數
- 程序數目

DNS 統計資料

下列 DNS 統計資料可從 Server Manager 取得：

- 最大 DNS 快取項目數
- 程序數目
- DNS 快取符合項目數 (亦顯示爲長條圖)
- DNS 快取不符合項目數 (亦顯示爲長條圖)

持續作用統計資料

下列持續作用統計資料可從 Server Manager 取得：

- 最大持續作用連線數
- 持續作用逾時
- 程序數目
- 持續作用符合項目數 (亦顯示爲長條圖)
- 持續作用更新次數 (亦顯示爲長條圖)
- 持續作用拒絕次數 (亦顯示爲長條圖)
- 持續作用逾時次數 (亦顯示爲長條圖)

伺服器請求統計資料

下列伺服器統計資料可從 Server Manager 取得。

- 請求總數。
- 收到的位元組數。
- 傳送的位元組數。
- 程序數目。
- 每一 HTTP 伺服器代碼的請求細項 (亦顯示爲長條圖)。例如，HTTP 伺服器代碼 200 表示已執行的請求。

▼ 存取統計資料

1. **存取 Server Manager，然後按一下 [Server Status] 標籤。**
2. **按一下 [Monitor Current Activity] 連結。**
3. **從 [Select Refresh Interval] 下拉式清單中選擇重新整理間隔。**
   重新整理間隔是指所顯示統計資訊的更新間隔秒數。
4. **從 [Select Statistics To Be Displayed] 下拉式清單中選擇要顯示的統計資料類型。**
   如需有關統計資料類型的更多資訊，請參閱第 186 頁的 「在 Server Manager 中顯示統計資料」。
5. **按一下 [Submit]。**
   如果伺服器實例正在執行中，並且已經啓用統計/效能評測，您就會看到顯示所選取統計資料類型的頁面。此頁面每隔 5 到 15 秒更新一次，視重新整理間隔值而定。
6. **從下拉式清單中選取程序 ID。**
   您可以透過 Server Manager 檢視目前作業，但這些種類與調校伺服器的關係不大。建議您使用 `perfdump` 統計資料來調校伺服器。如需更多資訊，請參閱下一節。

使用 perfdump 公用程式監視目前作業

`perfdump` 公用程式是內建在 Proxy Server 中的一種伺服器應用程式函數 (SAF)，可以從 Proxy Server 內部統計資料收集各種效能資料，並將其以 ASCII 文字格式顯示出來。與使用 Server Manager 相比，使用 `perfdump` 公用程式可監視的統計資料類型更多。

利用 `perfdump` 可將統計資料統一。此公用程式並不只是監視單一程序，而是將統計資料與程序數相乘，這樣可從整體上更精確地瞭解伺服器狀況。

啓用 perfdump 公用程式

必須先啓用 `stats-xml` 函數，之後才能啓用 `perfdump` SAF。

▼ 啓用 perfdump SAF

1. **在 `obj.conf` 檔案內的預設物件之後增加以下物件：**

```
<Object name="perf">

Service fn="service-dump"

</Object>
```

2. **在預設物件中增加以下一行：**

   ```
   NameTrans fn=assign-name from="/.perf" name="perf"
   ```

3. **重新啓動伺服器軟體。**

4. **轉至** `http://` *computer_name:proxyport*`/.perf` **以存取** `perfdump`。

   您可請求 `perfdump` 統計資料，並指定瀏覽器自動重新整理的頻率 (以秒爲單位)。下列範例設定每隔 5 秒重新整理一次：

   ```
   http:// computer_name:proxyport/.perf?refresh=5
   ```

`perfdump` 輸出範例

以下顯示 `perfdump` 輸出的範例

```
proxyd pid: 6751

Sun Java System Web Proxy Server 4.0 B05/02/2005 15:32 (SunOS DOMESTIC)

Server started Thu May 19 13:15:14 2005
Process 6751 started Thu May 19 13:15:14 2005

ConnectionQueue:
----------------------------------------
Current/Peak/Limit Queue Length            0/1/4096
Total Connections Queued                   1
Average Queue Length (1, 5, 15 minutes)    0.00, 0.00, 0.00
Average Queueing Delay                     0.09 milliseconds

ListenSocket ls1:
-----------------------
Address                    http://0.0.0.0:8081
Acceptor Threads           1

KeepAliveInfo:
--------------------
KeepAliveCount        0/256
KeepAliveHits         0
KeepAliveFlushes      0
KeepAliveRefusals     0
KeepAliveTimeouts     0
KeepAliveTimeout      30 seconds

SessionCreationInfo:
-----------------------
Active Sessions           1
```

```
Keep-Alive Sessions       0
Total Sessions Created    48/128

DiskCacheInfo:
------------------
Hit Ratio               0/0 (  0.00%)
Misses                  0
Cache files at startup  0
Cache files created     0
Cache files cleaned up  0

Native pools:
--------------------------
NativePool:
Idle/Peak/Limit               1/1/128
Work Queue Length/Peak/Limit  0/0/0

Server DNS cache disabled

Async DNS disabled

Performance Counters:
------------------------------------------------
 ......................Average         Total      Percent

Total number of requests:                    1
Request processing time:    0.2559        0.2559

default-bucket (Default bucket)
Number of Requests:                          1    (100.00%)
Number of Invocations:                       7    (100.00%)
Latency:                    0.2483        0.2483    ( 97.04%)
Function Processing Time:   0.0076        0.0076    (  2.96%)
Total Response Time:        0.2559        0.2559    (100.00%)

Sessions:
---------------------------
Process  Status     Function
6751     response   service-dump
```

如需有關這些參數的更多資訊，請參閱「Sun ONE Web Server 6.1 *Performance Tuning, Sizing, and Scaling Guide*」的第 2 章「Using Statistics to Tune Your Server」。

限制存取 perfdump 輸出

若您想限制可從瀏覽器檢視伺服器 perfdump 統計的使用者，則需爲 /.perf URI 建立 ACL。

obj.conf 檔案中的 perf 物件定義也必須參照此 ACL 檔案。例如，如果您已爲 >/.perf URI 建立了一個已命名的 ACL，就必須在物件定義中的 PathCheck 敘述內參照該 ACL 檔案，如下所示：

```
<Object name="perf">

PathCheck fn="check-acl" acl="perf.acl"

Service fn="service-dump"

</Object>
```

使用效能儲存區

您可利用效能儲存區來定義儲存區，並將之連結至多種伺服器函數。每當呼叫其中一種函數時，伺服器就會收集統計資料，並將資料增加至儲存區中。例如，send-cgi 和NSServletService 是分別用來服務 CGI 和 Java servlet 請求的函數。您可以定義兩個儲存區來維護 CGI 和 servlet 請求的個別計數，或建立一個儲存區以計算這兩種動態內容的請求數目。收集這項資訊的成本很低，且對於伺服器效能的影響通常微乎其微。稍後您可以利用 perfdump 公用程式來存取這項資訊。

下列資訊儲存在儲存區中：

- **Name of the bucket**－此名稱用於將儲存區與函數相關聯
- **Description**－與儲存區相關聯的函數說明
- **Number of requests for this function**－造成呼叫此函數的請求總數
- **Number of times the function was invoked**－由於一個請求可能會使某些函數執行多次，因此這個數字可能與請求該函數的請求數目不相等
- **Function latency or the dispatch time**－伺服器呼叫該函數所耗費的時間
- **Function time**－函數本身所耗費的時間

default-bucket 是由伺服器預先定義。其中記錄未與任何使用者定義的儲存區產生關聯的函數統計資料。

配置

您必須在 magnus.conf 和 obj.conf 檔案中指定效能儲存區的所有配置資訊。只有預設儲存區會自動啓用。

首先，您必須依照第 188 頁的 「使用 perfdump 公用程式監視目前作業」中的說明，啓用效能測量。

下列範例顯示如何在 magnus.conf 檔案中定義新的儲存區：

```
Init fn="define-perf-bucket" name="acl-bucket" description="ACL bucket"

Init fn="define-perf-bucket" name="file-bucket" description="Non-cached
responses"

Init fn="define-perf-bucket" name="cgi-bucket" description="CGI Stats"
```

此範例共建立三個儲存區：acl-bucket、file-bucket 和 cgi-bucket。若要將這些儲存區與函數建立關聯，請將 bucket=*bucket-name* 增加至您要進行效能測量的 obj.conf 函數中。

範例

```
PathCheck fn="check-acl" acl="default" bucket="acl-bucket"

...

Service method="(GET|HEAD|POST)" type="*~magnus-internal/*" fn="send-file"
bucket="file-bucket"

...

<Object name="cgi">

ObjectType fn="force-type" type="magnus-internal/cgi"

Service fn="send-cgi" bucket="cgi-bucket"

</Object>
```

效能報告

您可以利用 perfdump 公用程式來存取儲存區中的伺服器統計資料。效能儲存區資訊位於 perfdump 所傳回報告的最後一部分。

該報告中包含下列資訊：

- [Average]、[Total] 和 [Percent] 欄提供每項已請求的統計資料。
- [Request Processing Time] 是伺服器用於處理其到目前爲止所有已接收請求的時間總數。
- [Number of Requests] 是此函數的請求總數。
- [Number of Invocations] 是函數被呼叫的總次數。此值與請求數不同，因爲處理一個請求時可能會多次呼叫某函數。此列的百分比欄是參照所有儲存區的呼叫總數計算得出。
- [Latency] 是 Proxy Server 用於準備呼叫函數的時間 (以秒爲單位)。

- [Function Processing Time] 是 Proxy Server 在函數內耗費的時間 (以秒爲單位)。[Function Processing Time] 和 [Total Response Time] 的百分比是參照 [Request Processing Time] 總數計算得出。
- [Total Response Time] 是 [Function Processing Time] 和 [Latency] 的總和 (以秒爲單位)。

以下爲可透過 `perfdump` 取得的效能儲存區資訊之範例：

```
Performance Counters:
------------------------------------------------
                           Average         Total      Percent

Total number of requests:                      1
Request processing time:    0.2559        0.2559

default-bucket (Default bucket)
Number of Requests:                            1    (100.00%)
Number of Invocations:                         7    (100.00%)
Latency:                    0.2483        0.2483    ( 97.04%)
Function Processing Time:   0.0076        0.0076    (  2.96%)
Total Response Time:        0.2559        0.2559    (100.00%)
```

SNMP 基本原理

SNMP 是用來交換網路作業相關資料的協定。透過 SNMP，資料可在管理裝置和網路管理工作站 (NMS) 之間進行傳輸。管理裝置是指所有執行 SNMP 的裝置：主機、路由器、代理伺服器以及網路上的其他伺服器。NMS 是用於對該網路進行遠端管理的系統。通常，NMS 軟體會提供圖形來顯示收集到的資料，或使用此資料確定伺服器在特定的容許度下作業。

NMS 通常是指功能強大，且安裝了一或多個網路管理應用程式的工作站。網路管理應用程式 (例如 HP OpenView) 會以圖形方式顯示有關管理裝置 (例如您的 Web 伺服器) 的資訊。此項資訊可能包括企業中運作和當機的伺服器，或收到的錯誤訊息數目與類型。當您將 SNMP 與代理伺服器一起使用時，會使用兩種代理程式 (子代理程式和主代理程式) 在 NMS 與伺服器之間傳輸此資訊。

子代理程式會收集有關伺服器的資訊，並將該資訊傳送給伺服器的主代理程式。除了 Administration Server 之外的每部伺服器都具有子代理程式。

備註 – 對 SNMP 配置進行任何變更之後，您必須按一下 [Apply Required]，然後重新啓動 SNMP 子代理程式。

主代理程式會與 NMS 進行通訊。主代理程式隨 Administration Server 一起安裝。

每部主機上都可以安裝多個子代理程式，但是只能安裝一個主代理程式。例如，如果您在同一部主機上安裝了 Directory Server、Proxy Server 和 Messaging Server，則這些伺服器的子代理程式都會與同一個主代理程式進行通訊。

管理資訊庫

Proxy Server 儲存了與網路管理相關的變數。主代理程式可以存取的變數稱爲管理物件。這些物件都定義在樹狀結構中，此結構稱爲管理資訊庫 (MIB)。使用 MIB，您可以存取 Proxy Server 的網路配置、狀態以及統計資料。使用 SNMP，您可以從 NMS 檢視此項資訊。

MIB 樹狀結構頂層顯示網際網路物件識別碼具有以下四個子樹狀結構：directory、mgmt、experimental 和 private。private 子樹狀結構包含 enterprises 節點。enterprises 節點中的每個子樹狀結構被指定給個別的企業，該企業爲已註冊其自身特定 MIB 延伸的組織。企業然後便可以在其子樹下建立產品特定子樹。公司建立的 MIB 位於 enterprises 節點之下。Sun Java System 伺服器 MIB 也位於 enterprises 節點之下。每個 Sun Java System 伺服器子代理程式都會提供一個 MIB，用於 SNMP 通訊。伺服器藉由傳送包含這些變數的訊息或陷阱，將重要事件報告給 NMS。NMS 也可以查詢伺服器的 MIB 以獲取資料，或者從遠端變更 MIB 中的變數。每部 Sun Java System 伺服器都有其各自的 MIB。所有 Sun Java System 伺服器 MIB 都位於

```
server-root/plugins/snmp
```

Proxy Server 的 MIB 是一個名稱爲 `proxyserv40.mib` 的檔案。此 MIB 包含有關 Proxy Server 網路管理中各種變數的定義。您可以使用 Proxy Server MIB 來查看有關 Proxy Server 的管理資訊，並即時監視伺服器。

設定 SNMP

若要使用 SNMP，您的系統上必須已安裝一個主代理程式和至少一個子代理程式，且已開始運作。在啓用子代理程式之前首先需要安裝主代理程式。

由於系統不同，因此，設定 SNMP 的程序也不盡相同。

開始之前，應該確認兩個事項：

- 您的系統是否已在執行 SNMP 代理程式 (作業系統的本機代理程式)？

- 若是如此，您的本機 SNMP 代理程式是否支援 SMUX 通訊？(如果您使用的是 AIX 平台，則您的系統支援 SMUX。)

請參閱您的系統文件，以瞭解如何確認此資訊。

備註 – 變更 Administration Server 中的 SNMP 設定、安裝新伺服器或刪除現有的伺服器之後，您必須執行以下步驟：

- (Windows) 重新啓動 Windows SNMP 服務或重新啓動系統。
- (UNIX) 使用 Administration Server 重新啓動 SNMP 主代理程式。

表 10–1 啓用 SNMP 主代理程式和子代理程式的程序簡介

如果您的伺服器符合這些條件...	...請按照這些程序執行。在後面的小節中詳細地論述它們。
■ 目前尚未執行任何本機代理程式	1. 啓動主代理程式。 2. 爲系統上安裝的每個伺服器啓用子代理程式。
■ 目前正在執行本機代理程式 ■ 無 SMUX ■ 無需繼續使用本機代理程式	1. 爲 Administration Server 安裝主代理程式時，請停止本機代理程式。 2. 啓動主代理程式。 3. 爲系統上安裝的每個伺服器啓用子代理程式。
■ 目前正在執行本機代理程式 ■ 無 SMUX ■ 需要繼續使用本機代理程式	1. 安裝 SNMP 代理程式。 2. 啓動主代理程式。 3. 啓動 SNMP 代理程式。 4. 使用主代理程式的連接埠號之外的連接埠號，重新啓動本機代理程式。 5. 爲系統上安裝的每個伺服器啓用子代理程式。
■ 目前正在執行本機代理程式 ■ 支援 SMUX	1. 重新配置本機 SNMP 代理程式。 2. 爲系統上安裝的每個伺服器啓用子代理程式。

使用 Proxy SNMP 代理程式 (UNIX)

當您已經在執行本機代理程式，且要使其繼續與 Proxy Server 主代理程式同步運作時，就必須使用代理伺服器 SNMP 代理程式。在啓動之前，一定要停止本端主代理程式。請參閱您的系統文件，以取得詳細資訊。

備註 – 若要使用代理伺服器代理程式，您必須安裝然後將其啓動。您還必須使用不同於 Proxy Server 主代理程式執行所用的連接埠號，來重新啓動本機 SNMP 主代理程式。

本小節包括下列主題：

- 第 196 頁的「安裝 SNMP 代理程式」

- 第 196 頁的「啓動 SNMP 代理程式」
- 第 197 頁的「重新啓動本端 SNMP 常駐程式」

安裝 SNMP 代理程式

如果您的系統上正在執行 SNMP 代理程式，且您要繼續使用本機 SNMP 常駐程式，請遵循下列小節中的步驟：

▼ 安裝代理伺服器 SNMP 代理程式

1 **安裝 SNMP 主代理程式**。

請參閱第 197 頁的「安裝 SNMP 主代理程式」。

2 **安裝及啓動代理伺服器 SNMP 代理程式，並重新啓動本機 SNMP 常駐程式**。

請參閱第 195 頁的「使用 Proxy SNMP 代理程式 (UNIX)」。

3 **啓動 SNMP 主代理程式**。

請參閱第 198 頁的「啓用與啓動 SNMP 主代理程式」。

4 **啓用子代理程式**。

請參閱第 203 頁的「啓用子代理程式」。

若要安裝 SNMP 代理伺服器代理程式，請編輯 `CONFIG` 檔案，該檔案位於伺服器根目錄內的 `plugins/snmp/sagt` 中。增加 SNMP 常駐程式要偵聽的連接埠。此檔案也應該包含代理伺服器 SNMP 代理程式將轉寄的 MIB 樹狀結構和陷阱。

下列範例顯示 `CONFIG` 檔案。

```
AGENT AT PORT 1161 WITH COMMUNITY public
SUBTREES       1.3.6.1.2.1.1,
               3.6.1.2.1.2,
               1.3.6.1.2.1.3,
               1.3.6.1.2.1.4,
               1.3.6.1.2.1.5,
               1.3.6.1.2.1.6,
               1.3.6.1.2.1.7,
               1.3.6.1.2.1.8
FORWARD ALL TRAPS;
```

啓動 SNMP 代理程式

若要啓動代理伺服器 SNMP 代理程式，請在指令提示符號處鍵入：

```
# sagt -c CONFIG&
```

重新啓動本端 SNMP 常駐程式

啓動代理伺服器 SNMP 代理程式之後，您需要從 CONFIG 檔案中指定的連接埠處重新啓動本機 SNMP 常駐程式。若要重新啓動本機 SNMP 常駐程式，請在指令提示符號處鍵入：

```
# snmpd -P port-number
```

其中 *port-number* 是在 CONFIG 檔案中指定的連接埠號。例如，若您要在 Solaris 平台上使用先前提及的 CONFIG 檔案範例中的連接埠，請鍵入：

```
# snmpd -P 1161
```

重新配置本端 SNMP 代理程式

如果您的 SNMP 常駐程式是在 AIX 上執行，則它支援 SMUX。因此，您無需安裝主代理程式。不過，您需要變更 AIX SNMP 常駐程式的配置。

AIX 使用數個配置檔案來檢查其通訊。您必須編輯 snmpd.conf 檔案，使 SNMP 常駐程式接受來自 SMUX 子代理程式的內送訊息。如需更多資訊，請參閱線上手冊中有關 snmpd.conf 的內容。在此檔案中增加一行，以定義每個子代理程式。

例如，您可能會將此行增加至 snmpd.conf：

```
smux 1.3.6.1.4.1.1.1450.1 “ “ IP-address net-mask
```

IP_address 爲執行子代理程式的主機 IP 位址，net_mask 爲該主機的網路遮罩。

備註 – 請勿使用回送位址 127.0.0.1。請改用實際的 IP 位址。

安裝 SNMP 主代理程式

若要配置 SNMP 主代理程式，您必須以**超級**使用者身分安裝 Administration Server 實例。不過，即使不是**超級**使用者也可以透過將 SNMP 子代理程式配置爲與主代理程式一起使用，而完成一些基本的 SNMP 作業，例如 MIB 瀏覽。

▼ 安裝 SNMP 主代理程式

1. **以 root 身分登入。**
2. **檢查連接埠 161 上是否正在執行 SNMP 常駐程式 (snmpd)。**
   - **如果尚未執行任何 SNMP 常駐程式，請轉至第 197 頁的 「安裝 SNMP 主代理程式」。**

- **如果已經執行 SNMP 常駐程式，請確定您瞭解如何重新啓動此常駐程式，並瞭解其支援哪些 MIB 樹狀結構。然後強制結束其程序。**

3. **在 Administration Server 中，按一下 [Global Settings] 標籤中的 [Set SNMP Master Agent Trap] 連結。**
4. **鍵入執行網路管理軟體的系統名稱。**
5. **鍵入網路管理系統偵聽陷阱的連接埠號。(衆所周知的連接埠為 162。)**
   如需有關陷阱的更多資訊，請參閱第 203 頁的 「配置陷阱目標」。
6. **鍵入您要在陷阱中使用的社群字串。**
   如需有關社群字串的更多資訊，請參閱第 202 頁的 「配置社群字串」。
7. **按一下 [OK]。**
8. **在 Administration Server 中，按一下 [Global Settings] 標籤中的 [Set SNMP Master Agent Community] 連結。**
9. **鍵入主代理程式的社群字串。**
10. **為社群選擇一項作業。**
11. **按一下 [New]。**

啓用與啓動 SNMP 主代理程式

主代理程式的作業是在名稱爲 `CONFIG` 的代理程式配置檔案中定義。您可以使用 Server Manager 編輯 `CONFIG` 檔案，也可以手動編輯該檔案。您必須先安裝 SNMP 主代理程式，之後才能啓用 SNMP 子代理程式。

當重新啓動主代理程式時，若出現類似 `System Error:Could not bind to port` 的連結錯誤訊息，請在重新啓動主代理程式時，使用 `ps -ef | grep snmp` 來檢查 `magt` 是否正在執行。如果正在執行，請使用 `kill -9 pid` 指令來結束該程序。SNMP 的 CGI 即會開始重新運作。

本小節包括下列主題：

在其他連接埠上啓動主代理程式

管理介面不會在 161 以外的連接埠上啓動 SNMP 主代理程式。

▼ 在另一個連接埠上手動啓動主代理程式

1. **在 /*server-root* /plugins/snmp/magt/CONFIG 檔案中指定所需的連接埠。**
2. **依下列方式執行啓動程序檔：**

   ```
   cd / server-root/proxy-admserv

   ./start -shell /server-root/plugins/snmp/magt/magt

   /server-root /plugins/snmp/magt/CONFIG

   / server-root/plugins/snmp/magt/INIT
   ```

   然後會在所需的連接埠上啓動主代理程式。使用者介面就可以偵測出主代理程式正在執行。

手動配置 SNMP 主代理程式

▼ 手動配置 SNMP 主代理程式

1. **以超級使用者身分登入。**
2. **檢查連接埠 161 上是否正在執行 SNMP 常駐程式 (snmpd)。**

   如果已經執行 SNMP 常駐程式，請確定您瞭解如何重新啓動此常駐程式，並瞭解其支援哪些 MIB 樹狀結構。然後終止其程序。
3. **編輯 CONFIG 檔案，該檔案位於伺服器根目錄的 plugins/snmp/magt 中。**
4. **(可選) 在 CONFIG 檔案中定義 sysContact 變數和 sysLocation 變數。**

編輯主代理程式 CONFIG 檔案

▼ 手動配置 SNMP 主代理程式

1. **以超級使用者身分登入。**
2. **檢查連接埠 161 上是否正在執行 SNMP 常駐程式 (`snmpd`)。**
   如果已經執行 SNMP 常駐程式，請確定您瞭解如何重新啓動此常駐程式，並瞭解其支援哪些 MIB 樹狀結構。然後終止其程序。
3. **編輯 `CONFIG` 檔案，該檔案位於伺服器根目錄的 `plugins/snmp/magt` 中。**
4. **(可選) 在 `CONFIG` 檔案中定義 `sysContact` 變數和 `sysLocation` 變數。**

定義 sysContact 變數和 sysLocation 變數

`CONFIG` 檔案中的 `sysContact` 和 `sysLocation` 項目分別指定 `sysContact` 變數和 `sysLocation` MIB-II 變數。在本範例中，`sysContact` 和 `sysLocation` 的字串均用引號括住。任何含有空格、行中斷、標籤等等的字串均必須用引號括住。您也可以使用十六進制表示法指定值。

下列範例顯示已定義 `sysContract` 變數和 `sysLocation` 變數的 `CONFIG` 檔案：

```
COMMUNITY public

ALLOW ALL OPERATIONS

MANAGER nms2

SEND ALL TRAPS TO PORT 162

WITH COMMUNITY public

INITIAL sysLocation "Server room

987 East Cannon RoadMountain View, CA 94043 USA" INITIAL sysContact "Jill Dawson
email: jdawson@example.com"
```

配置 SNMP 子代理程式

您可以配置 SNMP 子代理程式來監視您的伺服器。

▼ 配置 SNMP 子代理程式

1. **存取 Server Manager，然後按一下 [Server Status] 標籤。**
2. **按一下 [Configure SNMP Subagent] 連結。**
   這時會顯示 [Configure SNMP Subagent] 頁面。
3. **在 [Master Host] 欄位中鍵入伺服器的名稱和網域。**
4. **鍵入伺服器的說明，包含作業系統資訊。**
5. **鍵入負責管理此伺服器的組織。**
6. **在 [Location] 欄位中鍵入伺服器的絕對路徑。**
7. **在 [Contact] 欄位中，鍵入伺服器負責人的姓名及其連絡資訊。**
8. **選取 [On] 以啓用 SNMP 統計資料集合。**
9. **按一下 [OK]。**
10. **按一下 [Restart Required]。**
    此時會顯示 [Apply Changes] 頁面。
11. **按一下 [Restart Proxy Server] 按鈕以套用變更。**

啓動 SNMP 主代理程式

一旦安裝 SNMP 主代理程式，您就可以手動或使用 Administration Server 將其啓動。

手動啓動 SNMP 主代理程式

若要手動啓動主代理程式，請在指令提示符號處鍵入下列指令：

```
# magt CONFIG INIT&
```

`INIT` 檔案是一個永久性的檔案，其中包含來自 MIB-II 系統群組的資訊 (包括系統位置和連絡資訊)。如果 `INIT` 尚不存在，則在首次啓動主代理程式時會建立該檔案。`CONFIG` 檔案中若包含無效管理員名稱，將會導致主代理程式啓動程序失敗。

若要在非標準連接埠上啓動主代理程式，您可以採用下列兩種方法之一：

方法一：在 CONFIG 檔案中，爲每個介面指定一個傳輸對映，主代理程式會經由此對映偵聽來自管理員的 SNMP 請求。傳輸對映可讓主代理程式在標準連接埠和非標準連接埠接受連線。主代理程式也可以在非標準連接埠接受 SNMP 通訊。目標系統對開放式通訊端數目或每個程序中檔案描述元數目的限制會限制 SNMP 的最大同步運作數目。下列範例顯示傳輸對映項目：

```
TRANSPORT extraordinary SNMP

OVER UDP SOCKET

AT PORT 11161
```

手動編輯 CONFIG 檔案之後，您應該在指令提示符號處鍵入下列指令，以手動啓動主代理程式：

```
# magt CONFIG INIT&
```

方法二：請編輯 /etc/services 檔案，讓主代理程式可在標準連接埠和非標準連接埠接受連線。

▼ 使用 Administration Server 啓動 SNMP 主代理程式

1. **登入 Administration Server**。
2. **從 Administration Server 中，按一下 [Global Settings] 標籤上的 [Control SNMP Master Agent] 連結**。
3. **按一下 [Start]**。
   您也可以從 [Control SNMP Master Agent] 頁面停止並重新啓動 SNMP 主代理程式。

配置 SNMP 主代理程式

啓用了主機上的主代理程式與子代理程式之後，便需要配置主機的 Administration Server。在此配置中，您要指定社群字串和陷阱目標。

配置社群字串

社群字串是 SNMP 代理程式用於授權的文字字串。這表示網路管理工作站將訊息傳送至代理程式的同時，會隨附傳送一個社群字串。然後，代理程式可以驗證網路管理站是否被授權取得資訊。社群字串在以 SNMP 封包傳送時，並不會隱藏起來。字串將會以 ASCII 文字格式傳送。

您可以從 Administration Server 的 [Set SNMP Master Agent Community] 頁面中，配置 SNMP 主代理程式的社群字串。您也可以定義特定社群所能夠執行的相關 SNMP 作業。您也可以從 Administration Server 中檢視、編輯和移除已配置的社群。

配置陷阱目標

SNMP 陷阱是 SNMP 代理程式傳送給網路管理工作站的一則訊息。例如，當介面的狀態由運作中變更爲當機，則 SNMP 代理程式會傳送一個陷阱。SNMP 代理程式必須知道網路管理工作站的位址，才會知道傳送陷阱的目標位置。您可以從 Proxy Server 中爲 SNMP 主代理程式配置此陷阱目標。也可以檢視、編輯、移除已經配置的陷阱目標。當使用 Proxy Server 配置陷阱目標時，實際上就是在編輯 `CONFIG` 檔案。

啓用子代理程式

安裝好隨附於 Administration Server 的主代理程式之後，您必須先爲您的伺服器實例啓用子代理程式，之後才能將其啓動。如需更多資訊，請參閱第 197 頁的 「安裝 SNMP 主代理程式」。您可以使用 Server Manager 來啓用子代理程式。

若要停止 UNIX 或 Linux 平台上的 SNMP 功能，您必須先停止子代理程式，然後再停止主代理程式。若您先停止主代理程式，則可能無法停止子代理程式。發生此情況後，請重新啓動主代理程式，然後停止子代理程式，接著停止主代理程式。

若要啓用 SNMP 子代理程式，請使用 Server Manager 中的 [Configure SNMP Subagent] 頁面，並從 [Control SNMP Subagent] 頁面來啓動子代理程式。如需更多資訊，請參閱線上說明中的相應小節。

一旦啓用子代理程式，您就可以從 [*Control SNMP Subagent*] 頁面或 Windows 的 [Services Control Panel]，將其啓動、停止或重新啓動。

備註 – 對 SNMP 配置進行任何變更之後，您必須按一下 [Apply Required]，然後重新啓動 SNMP 子代理程式。

瞭解 SNMP 訊息

GET 和 SET 是 SNMP 定義的兩種訊息類型。GET 和 SET 訊息都是由網路管理工作站 (NMS) 傳送給主代理程式的訊息。您可以將這些訊息和 Administration Server 一起使用。

SNMP 會以協定資料單元 (PDU) 格式交換網路資訊。這些單元包含有關儲存於管理裝置上的變數資訊，如 Web 伺服器。這些變數亦稱爲管理物件，其值和標題都會視需要報告給 NMS。由伺服器傳送至 NMS 的協定資料單元稱爲「陷阱」。下列範例顯示在由 NMS 或伺服器啓動的通訊中，使用 GET、SET 和陷阱訊息。

NMS 啓動式通訊。NMS 或者從伺服器請求資訊，或者變更儲存在伺服器 MIB 中的變數值。例如：

1. NMS 傳送訊息給 Administration Server 主代理程式。該訊息可能是對資料的請求 (一則 GET 訊息)，或者是一條設定 MIB 內變數的指令 (一則 SET 訊息)

2. 主代理程式將訊息轉寄至適當的子代理程式。
3. 子代理程式擷取資料或變更 MIB 中的變數。
4. 子代理程式向主代理程式報告資料或狀態，然後主代理程式將 GET 訊息轉寄回 NMS。
5. NMS 透過其網路管理應用程式，以文字或圖形顯示資料。

   伺服器啓動式通訊。發生了重要事件之後，伺服器子代理程式便會發送一則訊息或一個陷阱至 NMS。例如：
6. 子代理程式通知主代理程式伺服器已經停止。
7. 主代理程式會傳送一則訊息或一個陷阱，將事件報告給 NMS。
8. NMS 透過其網路管理應用程式，以文字或圖形顯示資訊。

◆ ◆ ◆ 第 11 章

11 代理及路由 URL

本章說明代理伺服器如何處理請求，也說明如何對特定的資源啓用代理。本章也說明如何配置代理伺服器將 URL 路由至不同的 URL 或伺服器。

本章包含下列小節：

對資源啓用/停用代理

您可以開啓或關閉資源的代理。資源可能爲單一 URL、一組具有共同點的 URL，或整個協定。您可以控制是要針對整個伺服器、各種資源或範本檔案中指定的資源開啓代理。您可以關閉資源的代理，以拒絕對一或多個 URL 的存取。此設定是完全拒絕或允許存取某項資源的通用方法。您也可以使用 URL 篩選器來允許或拒絕對資源的存取。如需有關 URL 篩選器的更多資訊，請參閱第 271 頁的 「篩選 URL」。

▼ 對資源啓用代理

1. **存取 Server Manager，然後按一下 [Routing] 標籤。**
2. **按一下 [Enable/Disable Proxying] 連結。**
   此時會顯示 [Enable/Disable Proxying] 頁面。
3. **從下拉式清單選取資源，或按一下 [Regular Expression] 按鈕、鍵入常規表示式，然後按一下 [OK]。**
4. **您可以為您指定的資源選擇預設設定。**
   - **Use Default Setting Derived From A More General Resource**。此資源會使用更一般性資源的設定 (包含此設定)。
   - **Do Not Proxy This Resource**。無法透過代理伺服器來存取此資源。
   - **Enable Proxying Of This Resource**。代理伺服器可允許用戶端存取此資源 (倘若通過其他安全檢查及授權檢查)。對資源啓用代理伺服器時，也會啓用所有方法。此資源的讀取方法 (包括 GET、HEAD、INDEX、POST 及用於 SSL 通道傳輸的 CONNECT) 及寫入方法 (包括 PUT、MKDIR、RMDIR、MOVE 及 DELETE) 都會啓用。如無任何其他的安全檢查，則用戶端都有讀取和寫入存取權。
5. **按一下 [OK]。**
6. **按一下 [Restart Required]。**
   此時會顯示 [Apply Changes] 頁面。
7. **按一下 [Restart Proxy Server] 按鈕以套用變更。**

透過另一個代理伺服器路由

[Set Routing Preferences] 頁面可用於配置代理伺服器來路由某些資源，路由方式可以指定使用衍生的預設配置或直接連線；或使用代理伺服器陣列、ICP 鄰近區域、另一個代理伺服器或 SOCKS 伺服器。

配置資源的路由

▼ 配置資源的路由

1 **存取 Server Manager，然後按一下 [Routing] 標籤。**

2 **按一下 [Set Routing Preferences] 連結。**
此時會顯示 [Set Routing Preferences] 頁面。

3 **從下拉式清單中選取資源，或按一下 [Regular Expression] 按鈕、鍵入常規表示式，然後按一下 [OK]。**

4 **為正在配置的資源選取您要的路由類型。**
可用選項如下：：

- **Derived Default Configuration**。代理伺服器會使用較常用的範本 (亦即具有較短、相符之常規表示式的範本)，以決定要使用遠端伺服器或是另一個代理伺服器。例如，如果代理伺服器將所有 `http://.*` 請求路由至另一個代理伺服器，並將所有 `http://www.*` 請求路由至遠端伺服器，您可以爲 `http://www.example.*` 請求建立一個衍生的預設配置路由，否則，由於 `http://www.*` 範本的設定，這些請求都會直接送往遠端伺服器。
- **Direct Connections**。請求將自動直接送往遠端伺服器，而不透過代理伺服器。
- **Route Through A SOCKS Server**。對指定資源的請求將透過 SOCKS Server 路由。如果選擇此選項，請指定代理伺服器要做爲路由途徑之 SOCKS 伺服器的名稱或 IP 位址及連接埠號。
- **Route Through**。可讓您指定要以代理伺服器陣列、ICP 鄰近區域、父系陣列或代理伺服器做爲路由途徑。若選擇多種路由方法，則代理伺服器將按照表單上所顯示的階層來執行：代理伺服器陣列、重新導向、ICP、父系陣列或另一個代理伺服器。如需有關透過代理伺服器路由的更多資訊，請參閱第 208 頁的 「鏈接 Proxy Server」。

  如需有關透過 SOCKS Server 路由的資訊，請參閱第 208 頁的 「透過 SOCKS 伺服器路由」。如需有關透過代理伺服器陣列、父系陣列或 ICP 鄰近區域路由的資訊，請參閱第 12 章 「快取」。

備註 – 若要在 443 以外的連接埠上啓用連線請求的路由，請在 `obj.conf` 檔案中將 `ppath` 參數變更爲 `connect://.*`。

---

5 **按一下 [OK]。**

6 **按一下 [Restart Required]。**
此時會顯示 [Apply Changes] 頁面。

7 **按一下 [Restart Proxy Server] 按鈕以套用變更。**

鏈接 Proxy Server

您可以讓代理伺服器存取另一個代理伺服器以取得某些資源，而非存取遠端伺服器。鏈接是在防火牆後組織數個代理伺服器的一種好方法。鏈接也可讓您建立階層式快取。

▼ 透過另一個 Proxy Server 路由

1 **存取 Server Manager，然後按一下 [Routing] 標籤。**

2 **按一下 [Set Routing Preferences] 連結。**
此時會顯示 [Set Routing Preferences] 頁面。

3 **從下拉式清單選取資源，或按一下 [Regular Expression] 按鈕、鍵入常規表示式，然後按一下 [OK]。**

4 **在頁面的 [Routing Through Another Proxy] 區段中，選取 [Route Through] 選項。**

5 **選取 [Another Proxy] 核取方塊。**

6 **在 [Another Proxy] 欄位中，可鍵入您要做為路由途徑之代理伺服器的伺服器名稱及連接埠號。**
鍵入伺服器名稱及連接埠號的格式爲：伺服器名稱:連接埠

7 **按一下 [OK]。**

8 **按一下 [Restart Required]。**
此時會顯示 [Apply Changes] 頁面。

9 **按一下 [Restart Proxy Server] 按鈕以套用變更。**

透過 SOCKS 伺服器路由

如果您的網路上已有遠端 SOCKS 伺服器在執行，您可以配置代理伺服器來連線至 SOCKS 伺服器，以取得特定的資源。

▼ 透過 SOCKS 伺服器路由

1. **存取 Server Manager，然後按一下 [Routing] 標籤。**
2. **按一下 [Set Routing Preferences] 連結。**
   此時會顯示 [Set Routing Preferences] 頁面。
3. **從下拉式清單選取資源，或按一下 [Regular Expression] 按鈕、鍵入常規表示式，然後按一下 [OK]。**
4. **在頁面的 [Routing Through Another Proxy] 區段中，選取 [Route Through] 選項。**
5. **選取 [Route Through SOCKS Server] 選項。**
6. **指定代理伺服器要做為路由途徑之 SOCKS 伺服器的名稱或 IP 位址及連接埠號。**
7. **按一下 [OK]。**
8. **按一下 [Restart Required]。**
   此時會顯示 [Apply Changes] 頁面。
9. **按一下 [Restart Proxy Server] 按鈕以套用變更。**

後續步驟

一旦啓用透過 SOCKS Server 路由之後，您便應該使用 [SOCKS v5 Routing] 頁面來建立代理路由。代理路由會識別可透過做爲代理路由途徑之 SOCKS 伺服器存取的 IP 位址。代理路由也可指定此 SOCKS 伺服器 是否直接連線至主機。

將用戶端 IP 位址轉寄至伺服器

可使用 [Forward Client Credentials] 頁面配置代理伺服器，將用戶端憑證傳送至遠端伺服器。

▼ 配置代理伺服器來傳送用戶端 IP 位址

1. **存取 Server Manager，然後按一下 [Routing] 標籤。**
2. **按一下 [Forward Client Credentials] 連結。**
   此時會顯示 [Forward Client Credentials] 頁面。

3. **從下拉式清單選取資源，或按一下 [Regular Expression] 按鈕、鍵入常規表示式，然後按一下 [OK]。**

4. **設定轉寄選項：**

   - **Client IP Addressing Forwarding**。當用戶端提出文件請求時，Proxy Server 不會將用戶端的 IP 位址傳送至遠端伺服器。而是由代理伺服器扮演用戶端的角色，將自己的 IP 位址傳送至遠端伺服器。但是在下列情況下，您最好傳送用戶端的 IP 位址：
     - 如果您的代理伺服器是內部代理伺服器鏈的其中一員。
     - 如果您的用戶端需存取的伺服器必須知道用戶端 IP 位址。您可以透過使用範本，只將用戶端的 IP 位址傳送至特定的伺服器。

     設定選項，以配置代理伺服器來傳送用戶端 IP 位址：
     - **Default**。允許 Proxy Server 轉寄用戶端的 IP 位址。
     - **Blocked**。不允許代理伺服器轉寄用戶端的 IP 位址。
     - **Enabled Using HTTP Header**。您可以指定 HTTP 標頭供代理伺服器在轉寄 IP 位址時使用。預設的 HTTP 標頭名爲 `Client-ip`，但您可以任意選擇標頭來傳送 IP 位址。
   - **Client Proxy Authentication Forwarding**。 設定選項，以配置代理伺服器來傳送用戶端的認證詳細資訊：
     - **Default**。允許 Proxy Server 轉寄用戶端的認證詳細資訊。
     - **Blocked**。不允許代理伺服器轉寄用戶端的認證詳細資訊。
     - **Enabled Using HTTP Header**。您可以指定 HTTP 標頭供代理伺服器在轉寄認證詳細資訊時使用。
   - **Client Cipher Forwarding**。設定該選項，以配置代理伺服器將用戶端的 SSL/TLS 加密套裝軟體名稱傳送至遠端伺服器。
     - **Default**。允許 Proxy Server 將用戶端的 SSL/TLS 加密套裝軟體名稱轉寄至遠端伺服器。
     - **Blocked**。不允許代理伺服器將用戶端的 SSL/TLS 加密套裝軟體名稱轉寄至遠端伺服器。
     - **Enabled Using HTTP Header**。您可以指定 HTTP 標頭，以供代理伺服器將用戶端的 SSL/TLS 加密套裝軟體名稱轉寄至遠端伺服器時使用。預設的 HTTP 標頭名爲 `Proxy-cipher`，但您可以任意選擇標頭來傳送用戶端的 SSL/TLS 加密套裝軟體名稱。
   - **Client Keysize Forwarding**。設定選項，以配置代理伺服器將用戶端的 SSL/TLS 金鑰大小傳送至遠端伺服器。
     - **Default**。允許 Proxy Server 將用戶端的 SSL/TLS 金鑰大小轉寄至遠端伺服器。
     - **Blocked**。不允許代理伺服器將用戶端的 SSL/TLS 金鑰大小轉寄至遠端伺服器。

- **Enabled Using HTTP Header**。您可以指定 HTTP 標頭，以供代理伺服器將用戶端的 SSL/TLS 金鑰大小轉寄至遠端伺服器時使用。預設的 HTTP 標頭名爲 `Proxy-keysize`，但您可以任意選擇標頭來傳送用戶端的 SSL/TLS 金鑰大小。

- **Client Secret Keysize Forwarding**。設定選項，以配置代理伺服器將用戶端的 SSL/TLS 私密金鑰大小傳送至遠端伺服器：
  - **Default**。允許 Proxy Server 將用戶端的 SSL/TLS 私密金鑰大小轉寄至遠端伺服器。
  - **Blocked**。不允許代理伺服器將用戶端的 SSL/TLS 私密金鑰大小轉寄至遠端伺服器。
  - **Enabled Using HTTP Header**。您可以指定 HTTP 標頭，以供代理伺服器將用戶端的 SSL/TLS 私密金鑰大小轉寄至遠端伺服器時使用。預設的 HTTP 標頭名爲 `Proxy-secret-keysize`，但您可以任意選擇標頭來傳送用戶端的 SSL/TLS 私密金鑰大小。

- **Client SSL Session ID Forwarding**。設定選項，以配置代理伺服器將用戶端的 SSL/TLS 階段作業 ID 傳送至遠端伺服器。
  - **Default**。允許 Proxy Server 將用戶端的 SSL/TLS 階段作業 ID 轉寄至遠端伺服器。
  - **Blocked**。不允許代理伺服器將用戶端的 SSL/TLS 階段作業 ID 轉寄至遠端伺服器。
  - **Enabled Using HTTP Header**。您可以指定 HTTP 標頭，以供代理伺服器將用戶端的 SSL/TLS 階段作業 ID 轉寄至遠端伺服器時使用。預設的 HTTP 標頭名爲 `Proxy-ssl-id`，但您可以任意選擇標頭來傳送用戶端的 SSL/TLS 階段作業 ID。

- **Client Issuer DN Forwarding**。設定選項，以配置代理伺服器將用戶端之 SSL/TLS 憑證的核發者辨別名稱傳送至遠端伺服器。
  - **Default**。允許 Proxy Server 將用戶端之 SSL/TLS 憑證的核發者辨別名稱轉寄至遠端伺服器。
  - **Blocked**。不允許代理伺服器將用戶端之 SSL/TLS 憑證的核發者辨別名稱轉寄至遠端伺服器。
  - **Enabled Using HTTP Header**。您可以指定 HTTP 標頭，以供代理伺服器將用戶端之 SSL/TLS 憑證的核發者辨別名稱轉寄至遠端伺服器時使用。預設的 HTTP 標頭名爲 `Proxy-issuer-dn`，但您可以任意選擇標頭來傳送用戶端之 SSL/TLS 憑證的核發者名稱。

- **Client User DN Forwarding**。設定選項，以配置代理伺服器將用戶端的 SSL/TLS 憑證主體辨別名稱傳送至遠端伺服器。
  - **Default**。允許 Proxy Server 將用戶端的 SSL/TLS 憑證主體辨別名稱轉寄至遠端伺服器。
  - **Blocked**。不允許代理伺服器將用戶端的 SSL/TLS 憑證主體辨別名稱轉寄至遠端伺服器。

- **Enabled Using HTTP Header**。您可以指定 HTTP 標頭，以供代理伺服器將用戶端之 SSL/TLS 憑證主體辨別名稱轉寄至遠端伺服器時使用。預設的 HTTP 標頭名爲 `Proxy-user-dn`，但您可以任意選擇標頭來傳送用戶端的 SSL/TLS 憑證主體名稱。

- **Client SSL/TLS Certificate Forwarding**。設定選項，以配置代理伺服器將用戶端的 SSL/TLS 憑證傳送至遠端伺服器。
  - **Default**。允許 Proxy Server 將用戶端的 SSL/TLS 憑證轉寄至遠端伺服器。
  - **Blocked**。不允許代理伺服器將用戶端的 SSL/TLS 憑證轉寄至遠端伺服器。
  - **Enabled Using HTTP Header**。您可以指定 HTTP 標頭，以供代理伺服器將用戶端的 SSL/TLS 憑證轉寄至遠端伺服器時使用。預設的 HTTP 標頭名爲 `Proxy-auth-cert`，但您可以任意選擇標頭來傳送用戶端的 SSL/TLS 憑證。
- **Client Cache Information Forwarding**。選取其中一個選項，以配置代理伺服器將有關本機快取符合項目的資訊傳送至遠端伺服器：
  - **Default**。允許 Proxy Server 將有關本機快取符合項目的資訊轉寄至遠端伺服器。
  - **Blocked**。不允許代理伺服器將有關本機快取符合項目的資訊轉寄至遠端伺服器。
  - **Enabled Using HTTP Header**。您可以指定 HTTP 標頭，以供代理伺服器將有關本機快取符合項目的資訊轉寄至遠端伺服器時使用。預設的 HTTP 標頭名爲 `Cache-info`，但您可以任意選擇標頭來傳送有關本機快取符合項目的資訊。
- **Set Basic Authentication Credentials**。設定選項，以配置代理伺服器來傳送 HTTP 請求。
  - **User**。指定要認證的使用者。
  - **Password**。指定使用者的密碼。
  - **Using HTTP Header**。您可以指定 HTTP 標頭，以供代理伺服器用來傳送憑證。

5. **按一下 [OK]**。
6. **按一下 [Restart Required]。此時會顯示 [Apply Changes] 頁面**。
7. **按一下 [Restart Proxy Server] 按鈕以套用變更**。

允許用戶端檢查 IP 位址

爲了維護網路的安全性，用戶端可能會有限制僅能存取某些 IP 位址的功能。爲了讓您的用戶端可以使用此功能，Proxy Server 提供了對於檢查 Java IP 位址的支援。

藉由檢查 Java IP 位址，用戶端可以向 Proxy Server 查詢用於重新路由資源的 IP 位址。由於 Java Applet 經常發生 DNS 盜用情況，因此利用此功能，用戶端便可查看原始伺服器的眞實 IP 位址。

當啓用此功能時，Proxy Server 會附加一個標頭，其中包含用於連線至目標原始伺服器的 IP 位址。例如，如果啓用此功能，且請求包含「Pragma: dest-ip」標頭，則 Proxy Server 就會加入原始伺服器的 IP 位址做爲「Dest-ip:」標頭的值。

如需有關用於檢查 Java IP 位址之伺服器應用程式功能 (SAF) 的資訊，請參閱「Sun Java System Web Proxy Server 4.0.8 Configuration File Reference」中的「ObjectType」一節中的 `java-ip-check`。

▼ 檢查 Java IP 位址

1. **存取 Server Manager，然後按一下 [Routing] 標籤。**
2. **按一下 [Java IP Address] 連結。**
   此時會顯示 [Java IP Address] 頁面。
3. **從下拉式清單選取資源，或按一下 [Regular Expression] 按鈕、鍵入常規表示式，然後按一下 [OK]。**
4. **啓用、停用或使用 Java IP 位址檢查的預設配置。**

   備註 – 預設選項會使用從較常用範本導出的衍生預設配置。一般範本使用較短、相符的常規表示式來決定是否啓用或停用 Java IP 位址檢查。
5. **按一下 [OK]。**
6. **按一下 [Restart Required]。**
   此時會顯示 [Apply Changes] 頁面。
7. **按一下 [Restart Proxy Server] 按鈕以套用變更。**

用戶端自動配置

如果您的 Proxy Server 支援許多用戶端，則您可能想要使用用戶端自動配置檔案來配置所有的瀏覽器用戶端。自動配置檔案包含一個 JavaScript™ 函數，可以決定瀏覽器存取不同 URL 時所使用的代理伺服器 (如果存在)。如需有關此功能的更多資訊，請參閱第 17 章「使用用戶端自動配置檔案」。

設定網路連結模式

您可以讓代理伺服器電腦與網路連線，或中斷代理伺服電腦與網路的連線。此功能表示您可以輕鬆地將代理伺服器安裝在您用於示範的可攜式電腦上。

當代理伺服器與網路中斷連線時，將直接從快取中傳回文件。代理伺服器無法執行最新狀態檢查，所以擷取文件的速度非常快。不過，文件可能不是最新文件。如需有關快取的更多資訊，請參閱第 12 章 「快取」。

若您未連線至網路，也不會出現連線當機的情況，因爲代理伺服器知道網路連線不存在，也就永遠不會嘗試連線至遠端伺服器。如果網路不通，但代理伺服器電腦還在執行，則您可以使用這種無網路設定。執行與網路中斷連線的代理伺服器表示您將最終存取快取內過時的資料。此外，在無網路的情況下執行也會讓代理伺服器的安全性功能顯得多餘。

Proxy Server 提供四種網路連結模式：

- 預設模式源自最常用之相符物件的配置。
- 正常模式是代理伺服器的正常作業模式。如果文件不存在快取中，則代理伺服器會從內容伺服器擷取文件。如果文件在快取中，則會比對內容伺服器來判斷是否爲最新文件。如果快取的檔案已變更，則會以目前的副本將其替代。
- 快速示範模式可讓您在有網路可用的情況下順暢地展示示範。如果在快取中找到文件，則不會連絡內容伺服器，甚至不會檢查文件是否已變更。此模式可防止因爲等待內容伺服器回應所造成的任何延時。如果文件不在快取中，則會從內容伺服器擷取，然後存入快取中。快速示範模式的延時現象少於正常模式，但偶爾會傳回過時的資料，因爲一旦伺服器有文件的副本，就不會對文件執行最新狀態檢查。
- 無網路模式是專爲可攜式電腦在未連線至網路期間所設計的。如果文件在快取中，則代理伺服器會傳回文件；如果不在快取中，則會傳回錯誤。代理伺服器絕對不會嘗試連絡內容伺服器，這可以避免代理伺服器因爲嘗試取得不存在的連線而逾時。

▼ 變更 Proxy Server 的執行模式

1. **存取 Server Manager，然後按一下 [Routing] 標籤。**
2. **按一下 [Set Connectivity Mode] 連結。此時會顯示 [Set Connectivity Mode] 頁面。**
3. **從下拉式清單選取資源，或按一下 [Regular Expression] 按鈕、鍵入常規表示式，然後按一下 [OK]。**
4. **選取您要的模式。**
5. **按一下 [OK]。**
6. **按一下 [Restart Required]。此時會顯示 [Apply Changes] 頁面。**

7 **按一下 [Restart Proxy Server] 按鈕以套用變更。**

變更預設的 FTP 傳輸模式

FTP 有兩種不同的方法可建立 FTP 伺服器與用戶端之間的資料連線，由代理伺服器扮演用戶端的角色。這兩種模式稱爲 PASV 和 PORT 模式 FTP。

- **被動模式** *(PASV)*。資料連線由代理伺服器啓動，由 FTP 伺服器接受連線。對於執行代理伺服器的網站，如此較爲安全，因爲伺服器不必接受傳入連線。
- **主動模式** *(PORT)*。資料連線由遠端 FTP 伺服器啓動，由代理伺服器接受內送連線。如果代理伺服器在防火牆內，則防火牆可能會封鎖來自 FTP 伺服器的內送 FTP 資料連線，這表示 PORT 模式可能無法運作。

有些 FTP 網站是在防火牆內執行，導致代理伺服器無法使用 PASV 模式。因此，可以配置代理伺服器來使用 PORT 模式 FTP。您可以對整個伺服器開啓 PORT 模式，或只針對特定的 FTP 伺服器來開啓此模式。

即使已開啓 PASV 模式，如果遠端 FTP 伺服器不支援 PASV 模式，則代理伺服器還是會使用 PORT 模式。

如果代理伺服器在防火牆後，以致於無法使用 PORT 模式 FTP，則您無法啓用 PORT 模式。如果爲資源選取預設模式，則代理伺服器會使用較常用資源的模式。如果沒有指定模式，則會使用 PASV 模式。

▼ 設定 FTP 模式

1 **存取 Server Manager，然後按一下 [Routing] 標籤。**

2 **按一下 [Set FTP Mode] 連結。此時會顯示 [Set FTP Mode] 頁面。**

3 **從下拉式清單選取資源，或按一下 [Regular Expression] 按鈕、鍵入常規表示式，然後按一下 [OK]。**

4 **選取 FTP 傳輸模式。**

5 **按一下 [OK]。**

6 **按一下 [Restart Required]。此時會顯示 [Apply Changes] 頁面。**

7 **按一下 [Restart Proxy Server] 按鈕以套用變更。**

指定 SOCKS 名稱伺服器 IP 位址

如果您的代理伺服器配置爲透過 SOCKS 伺服器來建立傳出連線，則您可能需要明確指定用於 SOCKS 之名稱伺服器的 IP 位址。

如果您使用 DNS 伺服器來解析外部主機名稱，而不是使用防火牆內的內部 DNS 服務來解析，則應該指定名稱伺服器的 IP 位址。

▼ 指定 SOCKS 名稱伺服器的 IP 位址

1. **存取 Server Manager，然後按一下 [Routing] 標籤。**
2. **按一下 [Set SOCKS Name Server] 連結。**
   此時會顯示 [Set SOCKS Name Server] 頁面。
3. **在欄位中鍵入 DNS 名稱伺服器的 IP 位址。**
4. **按一下 [OK]。**

備註 – 以前只能透過 SOCKS_NS 環境變數來指定 SOCKS 名稱伺服器的 IP 位址。如果您設定此環境變數，並使用 [SOCKS Name Server Setting] 表單來指定名稱伺服器 IP 位址，則代理伺服器將使用表單上指定的 IP 位址，而不是此環境變數。

---

5. **按一下 [Restart Required]。**
   此時會顯示 [Apply Changes] 頁面。
6. **按一下 [Restart Proxy Server] 按鈕以套用變更。**

配置 HTTP 請求負載平衡

[Configure HTTP Request Load Balancing] 頁面可用於將負載分散於指定的原始伺服器之間。

▼ 配置 HTTP 請求負載平衡

1. **存取 Server Manager，然後按一下 [Routing] 標籤。**
2. **按一下 [Configure HTTP Request Load Balancing] 連結。**
   此時會顯示 [Configure HTTP Request Load Balancing] 頁面。

3. 從下拉式清單選取資源，或按一下 **[Regular Expression]** 按鈕、鍵入常規表示式，然後按一下 **[OK]**。

4. 在 **[Server]** 欄位中指定原始伺服器的 **URL**。如果指定多個伺服器參數，則 **Proxy Server** 會將負載分散於指定的原始伺服器之間。

5. 在 **[Sticky Cookie]** 欄位中指定 **cookie** 的名稱，當其出現在回應中時，將導致隨後的請求固定使用此原始伺服器。預設值是 `JSESSIONID`。

6. 在 **[Sticky Parameter]** 欄位中，指定用於檢查路由資訊的 **URI** 參數名稱。如果此 **URI** 參數出現在請求 **URI** 中，且值含有一個冒號後面跟著路由 **ID**，則請求會「居留」於此路由 **ID** 所識別的原始伺服器。預設值是 `jsessionid`。

7. 在 **[Route Header]** 欄位中，指定將路由 **ID** 傳達給原始伺服器時所用的 **HTTP** 請求標頭名稱。預設值是 `proxy-jroute`。

8. 在 **[Route Cookie]** 欄位中，指定當 **Proxy Server** 在回應中遇到居留式 **cookie** 時所會產生的 **cookie** 名稱。

   預設值是 `JROUTE`。

9. 設定 **[Rewrite Host]** 選項，指出是否重寫 **Host HTTP** 請求標頭以符合伺服器參數所指定的主機。

10. 設定 **[Rewrite Location]** 選項，指出是否重寫符合伺服器參數的 **Location HTTP** 回應標頭。

11. 設定 **[Rewrite Content Location]** 選項，指出是否重寫符合伺服器參數的 **Content-location HTTP** 回應標頭。

12. 指出是否重寫符合伺服器參數的 *headername* **HTTP** 回應標頭，其中 *headername* 是使用者定義的標頭名稱。在 **[Headername]** 欄位中指定標頭名稱。

13. 按一下 **[OK]**。

14. 按一下 **[Restart Required]**。

    此時會顯示 [Apply Changes] 頁面。

15. 按一下 **[Restart Proxy Server]** 按鈕以套用變更。

管理 URL 和 URL 對映

使用 Server Manager 將 URL 對映至另一個伺服器，有時稱爲鏡像伺服器。當用戶端使用鏡像 URL 來存取代理伺服器時，代理伺服器會從鏡像伺服器中擷取請求的文件，而不是從 URL 中指定的伺服器擷取。用戶端永遠不知道請求會送往不同的伺服器。您也可以重新導向 URL。在此情況下，代理伺服器只會將重新導向的 URL 傳回給用戶端，而不會傳回文件，所以用戶端可以繼續請求新的文件。對映也可讓您將 URL 對映至檔案，如同在 PAC 和 PAT 對映中一樣。

建立及修改 URL 對映

若要對映 URL，請指定 URL 前綴及對映位置。下列幾節說明各種 URL 對映。您可以建立下列 URL 對映類型：

- 標準對映可將一個 URL 前綴對映至另一個 URL 前綴。例如，您可以配置代理伺服器在收到以 `http://www.example.com` 開頭的請求時一律連線至特定的 URL。
- 反向對映可將重新導向的 URL 前綴對映至另一個 URL 前綴。當內部伺服器傳送至代理伺服器的是重新導向的回應，而不是文件時，這種對映就會與反向代理伺服器搭配使用。請參閱第 14 章 「使用反向代理伺服器」以取得更多資訊。
- 常規表示式可將所有符合表示式的 URL 對映至單一 URL。例如，您可以將所有符合 .*job.* 的 URL 對映至特定的 URL，此 URL 可能說明代理伺服器不讓使用者連線至特定 URL 的原因。
- 用戶端自動配置可將 URL 對映至代理伺服器上儲存的特定 `.pac` 檔案。如需有關自動配置檔案的更多資訊，請參閱第 17 章 「使用用戶端自動配置檔案」。
- 代理伺服器陣列表格 (PAT) 可將 URL 對映至 Proxy Server 上儲存的特定 `.pat` 檔案。您應該只從主代理伺服器建立這種類型的對映。如需有關 PAT 檔案及代理伺服器陣列的更多資訊，請參閱第 256 頁的 「透過代理伺服器陣列路由」。

存取 URL 的用戶端會傳送至相同或不同伺服器上的另一個位置。在不以尾隨斜線來存取目錄時，如果有一項資源已移動，或您需要維護相關連結的完整性，此功能非常有用。

例如，假設您有一個工作量沈重的 Web 伺服器，名爲 `hi.load.com` ，但您想要鏡像至另一個名爲 `mirror.load.com` 的伺服器。對於連線至 `hi.load.com` 電腦的 URL，您可以配置代理伺服器來使用 `mirror.load.com` 電腦。

來源 URL 前綴不能換碼，但在目標 (鏡像) URL 中，只有在 HTTP 請求中非法的字元才需要換碼。

請勿在前綴中使用尾隨斜線！

▼ 建立 URL 對映

1 **存取 Server Manager，然後按一下 [URL] 標籤。**

2 **按一下 [Create Mapping] 連結。**
這時會顯示 [Create Mapping] 頁面。

3 **選擇您要建立的對映類型。**

- **Regular Mappings**。如果選取此選項，則頁面的下方區段會顯示下列選項：
  - *Rewrite Host*。指出是否重寫 Host HTTP 標頭以符合 `to` 參數所指定的主機。
  - **Reverse Mappings**。將重新導向的 URL 前綴對映至另一個 URL 前綴。如果選取此選項，則頁面的下方區段會顯示下列選項：
    - *Rewrite Location*。指出是否重寫 Location HTTP 回應標頭。
    - *Rewrite Content Location*。指出是否重寫 Content-location HTTP 回應標頭。
    - *Rewrite Headername*。選取此核取方塊，以指出是否應重寫 *headername* HTTP 回應標頭，其中 *headernam* 是使用者定義的標頭名稱。

    Regular Expressions。將所有符合表示式的 URL 對映至單一 URL。如需有關常規表示式的更多資訊，請參閱第 16 章「管理範本和資源」。
  - **Client Autoconfiguration**。將 URL 對映至 Proxy Server 上儲存的特定 `.pac` 檔案。如需有關自動配置檔案的更多資訊，請參閱第 17 章「使用用戶端自動配置檔案」。
  - **代理伺服器陣列表格 (PAT)**。將 URL 對映至 Proxy Server 上儲存的特定 `.pat` 檔案。您應該只從主代理伺服器建立這種類型的對映。如需有關 PAT 檔案和代理伺服器陣列的更多資訊，請參閱第 12 章「快取」中的「透過代理伺服器陣列路由」。

4 **鍵入對映來源前綴。**
以標準及反向對映而言，前綴應該是您要取代的 URL 部分。

以常規表示式對映而言，URL 前綴應該是您要比對的所有 URL 的常規表示式。如果您也選擇了對映的範本，則此常規表示式僅適用於範本之常規表示式內的 URL。

以用戶端自動配置對映及代理伺服器陣列表格對映而言，URL 前綴應該是用戶端所存取的完整 URL。

5 **鍵入對映目標。**
以用戶端自動配置及代理伺服器陣列表格之外的所有對映類型而言，此宣告應該是對映目標的完整 URL。以用戶端自動配置對映而言，此值應該是 `.pac` 檔案在代理伺服器硬碟上的絕對路徑。以代理伺服器陣列對映而言，此值應該是 `.pat` 檔案在主代理伺服器本機磁碟上的絕對路徑。

6. **從下拉式清單中選取範本名稱，如果您不要套用範本，請讓值保留為 [NONE]。**
7. **按一下 [OK] 來建立對映。**
8. **按一下 [Restart Required]。**
   此時會顯示 [Apply Changes] 頁面。
9. **按一下 [Restart Proxy Server] 按鈕以套用變更。**

▼ 變更現有的對映

1. **存取 Server Manager，然後按一下 [URL] 標籤。**
2. **按一下 [View/Edit Mappings] 連結。**
   此時會顯示 [View/Edit Mappings] 頁面。
3. **在要修改的對映旁邊按一下 [Edit] 連結。您可以編輯前綴、對映的 URL 及對映所影響的範本。按一下 [OK] 以確認變更。**
4. **按一下 [Restart Required]。此時會顯示 [Apply Changes] 頁面。**
5. **按一下 [Restart Proxy Server] 按鈕以套用變更。**

▼ 移除對映

1. **存取 Server Manager，然後按一下 [URL] 標籤。**
2. **按一下 [View/Edit Mappings] 連結。**
   此時會顯示 [View/Edit Mappings] 頁面。
3. **選取要移除的對映，然後按一下旁邊的 [Remove] 連結。**
4. **按一下 [Restart Required]。此時會顯示 [Apply Changes] 頁面。**
5. **按一下 [Restart Proxy Server] 按鈕以套用變更。**

重新導向 URL

您可以配置代理伺服器將重新導向的 URL 傳回給用戶端，而不是取得並傳回文件。透過重新導向，用戶端可知道最初請求的 URL 已重新導向不同的 URL。用戶端通常會立即請求重新導向的 URL。Netscape Navigator 會自動請求重新導向的 URL。使用者不必特別再次請求文件。

當您想要拒絕存取某個區域時，URL 重新導向非常有用，因爲您可以將使用者重新導向一個說明拒絕存取理由的 URL。

▼ 重新導向一或多個 URL

1. **存取 Server Manager，然後按一下 [URLs] 標籤。**
2. **按一下 [Redirect URLs] 連結。此時會顯示 [Redirect URLs] 頁面。**
3. **鍵入一個為 URL 前綴的來源 URL。**
4. **鍵入重新導向的目標 URL。此 URL 可以是 URL 前綴或固定 URL。**
   - 如果選擇使用 URL 前綴做爲要重新導向的目標 URL，請選取 URL 前綴欄位旁邊的單選按鈕，然後鍵入 URL 前綴。
   - 如果選擇使用固定 URL，請選取 [Fixed URL] 欄位旁邊的單選按鈕，然後鍵入固定 URL。
5. **按一下 [OK]。**
6. **按一下 [Restart Required]。**
   此時會顯示 [Apply Changes] 頁面。
7. **按一下 [Restart Proxy Server] 按鈕以套用變更。**

◆ ◆ ◆ 第 12 章

12 快取

本章說明 Sun Java System Web Proxy Server 快取文件的方式。同時說明如何使用線上頁面來配置快取。

本章包含下列小節：

快取的運作方式

對於使用 Proxy Server (而非直接存取遠端伺服器) 的用戶端，快取可以降低網路流量並提供更短的回應時間。

當用戶端向代理伺服器請求網頁或文件時，代理伺服器將文件傳送給用戶端的同時，會從遠端伺服器將文件複製到其本機快取目錄結構。

當用戶端請求之前請求過並已複製到代理伺服器快取的文件時，代理伺服器會從快取傳回此文件，而不會再次從遠端伺服器擷取此文件，如下圖所示。若代理伺服器判斷檔案並不是最新的，則會從遠端伺服器更新此文件，並在將文件傳送給用戶端之前，更新其快取。

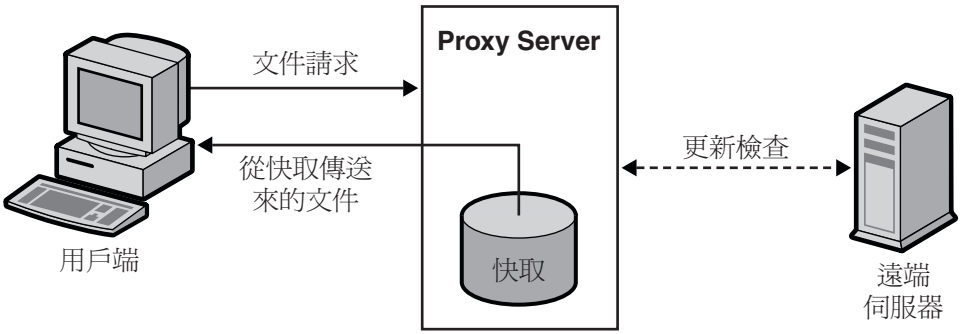


圖 12–1 代理伺服器文件擷取

Sun Java System Web Proxy Server 資源回收公用程式 (CacheGC) 會自動維護快取中的檔案。CacheGC 會定期自動清理快取以確保快取不會因過期文件而出現混亂。

瞭解快取結構

快取由一或多個分割區組成。就概念上而言，分割區是磁碟上留作快取用途的儲存區域。若要讓快取跨越數個磁碟，請至少爲每個磁碟配置一個快取分割區。每個分割區均可獨立管理。換句話說，可以單獨對某個分割區進行啓用、停用和配置，其他分割區不受影響。

在單一位置儲存大量快取檔案會使得效能降低；因此，建議您在每個分割區中建立數個目錄或區段。在快取結構中，區段是分割區的下一個層級。在跨越所有分割區的快取中最多可以有 256 個區段。快取區段的數目必須是 2 的乘冪 (例如，1、2、4、8、16、...、256)。

快取結構階層中的最低層級是子區段。子區段是區段內的目錄。每個區段具有 64 個子區段。快取檔案儲存在快取中最低層級的子區段中。

下圖顯示了一個具有分割區與區段的快取結構範例。在此圖中，快取目錄結構將整個快取分爲三個分割區。第一個分割區包含四個快取區段，而其餘兩個分割區各包含兩個區段。

每個快取區段的標註方式是：以「s」表示區段，其後爲區段號碼。對於顯示爲 s3.4 的區段，3 表示快取區段號碼是 2 的 3 乘冪 ($2^3 = 8$)，而 4 表示區段號碼 (共有 8 個區段，標示爲 0 到 7)。因此，s3.4 表示 8 個區段的第 5 個。

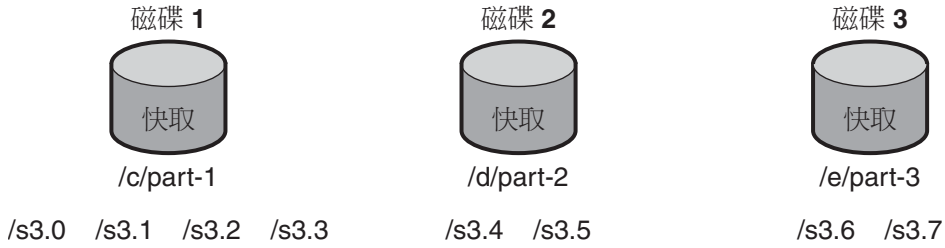


圖 12–2 快取結構範例

分配快取中的檔案

Proxy Server 使用特定演算法來確定文件應儲存於哪個目錄。此演算法可確保將文件平均分配在各目錄中。平均分配非常重要，因爲包含大量文件的目錄可能會導致效能問題。

Proxy Server 使用 RSA MD5 演算法 (訊息摘要 5) 將 URL 簡化爲 16 位元組的二進位資料，並使用此資料的 8 個位元組來計算 16 個字元的十六進位檔案名稱，以此將文件儲存在快取中。

設定快取明細

您可以藉由設定快取明細來啓用快取並控制 Proxy Server 將快取的協定類型。快取明細包含下列項目：

- 快取是啓用還是停用狀態
- 快取儲存其暫存檔案的工作目錄
- 將記錄快取 URL 的目錄之名稱
- 快取大小
- 快取容量
- 將快取的協定類型
- 重新整理快取文件的時機
- 代理伺服器是否要追蹤文件的存取次數並向遠端伺服器回報該值

備註 – 設定大型快取的明細非常耗時，而且可能導致管理介面逾時。因此，若要建立大型快取，請使用指令行公用程式來設定快取明細。如需有關快取指令行公用程式的更多資訊，請參閱第 242 頁的 「使用快取指令行介面」。

▼ 設定快取明細

1. **存取 Server Manager，然後按一下 [Caching] 標籤。**

2. **按一下 [Set Cache Specifics] 連結。**
   此時會顯示 [Set Cache Specifics] 頁面。

3. **您可以選取適當的選項來啓用或停用快取。**
   依預設，快取爲啓用狀態。

4. **提供工作目錄。**
   依預設，工作目錄位於代理伺服器實例下。您無法變更此位置。如需更多資訊，請參閱第 227 頁的「建立快取工作目錄」。

5. **按一下 [partition configuration] 連結。**
   此時會顯示 [Add/Edit Cache Partitions] 頁面。您可以增加新的快取分割區，或編輯現有的快取分割區。快取大小是允許快取擴充到的最大值。快取大小最大值是 32 GB。如需更多資訊，請參閱第 227 頁的「設定快取大小」。

6. **按一下 [cache capacity configuration] 連結。**
   此時會顯示 [Set Cache Capacity] 頁面。您可以在 [Set Cache Capacity] 頁面上設定快取容量。

7. **選取 [Cache HTTP] 以啓用 HTTP 文件的快取。**
   如果確定要讓代理伺服器快取 HTTP 文件，則必須確定應讓其一直對快取內的文件進行最新狀態檢查，還是讓它每隔一段時間進行檢查。您也可以啓用或停用 Proxy Server 向遠端伺服器報告快取符合項目的功能。如需更多資訊，請參閱第 227 頁的「快取 HTTP 文件」。可用選項如下：

   - 選取 [Always Check That The Document Is Up To Date] 選項來確保 HTTP 文件永遠是最新的。
     - 從 [Check Only If Last Check More Than] 下拉式清單選取小時數，以指定代理伺服器的重新整理間隔。使用下列選項之一可執行最新狀態檢查：
       - **Use Last-modified Factor**。這是原始伺服器連同文件一起傳送的上次修改的標頭。
       - **Use Only Explicit Expiration Information**。代理伺服器會使用 Expires 標頭來判斷快取項目爲最新還是過期。

       選取 [Never Report Accesses To Remote Server] 選項來避免代理伺服器向遠端伺服器報告存取次數。
     - 選取 [Report Cache Hits To Remote Server] 選項來追蹤文件的存取次數並向遠端伺服器回報。

8 選取 [Yes; Reload If Older Than] 核取方塊以設定快取 FTP 文件的重新整理間隔，並從下拉式清單中選取值以設定時間間隔。如需更多資訊，請參閱第 229 頁的 「快取 FTP 與 Gopher 文件」。

9 可以為快取 Gopher 文件設定重新整理間隔。選取 [Yes; Reload If Older Than] 核取方塊，並從下拉式清單中選取值以設定時間間隔。如需更多資訊，請參閱第 229 頁的 「快取 FTP 與 Gopher 文件」。

10 按一下 [OK]。

11 按一下 [Restart Required]。此時會顯示 [Apply Changes] 頁面。

12 按一下 [Restart Proxy Server] 按鈕以套用變更。

建立快取工作目錄

快取檔案位於快取分割區下。您在 [Set Cache Specifics] 頁面上指定的工作目錄通常是快取的父系目錄。所有快取的檔案會出現在快取目錄下的組織化目錄結構中。若變更快取目錄名稱或將它移動到另一個位置，則必須爲代理伺服器提供新位置。

您可以將快取目錄結構延伸到多個檔案系統上，以便將大型快取結構分散到多個較小的磁碟上，而不是完全儲存在一個大型磁碟上。每個代理伺服器都必須有自己的快取目錄結構，也就是說，多部代理伺服器無法同時共用快取目錄。

設定快取大小

快取大小指的是分割區大小。快取大小永遠都應小於快取容量，因爲快取容量是快取可擴充到的最大值。所有分割區大小的總和必須小於或等於快取大小。

代理伺服器快取可用的磁碟空間對於快取效能有重大影響。若快取太小，Cache GC 必須更頻繁地移除快取文件以挪出磁碟空間，而且必須更頻繁地從內容伺服器擷取文件，從而會使效能降低。

使用較大的快取效率比較高，因爲快取的文件越多，網路流量負載就越小，且代理伺服器可提供的回應時間也越短。此外，GC 會移除使用者不再需要的快取文件。如果排除檔案系統本身的限制，快取大小絕不會有過大之慮。多餘的空間只是維持原狀而已。

您也可以將快取設定爲分散於多個磁碟分割區。

快取 HTTP 文件

HTTP 文件能提供其他協定的文件無法提供的快取功能。然而，透過正確地設定並配置快取，可確保 Proxy Server 能有效快取 HTTP、FTP 與 Gopher 文件。

備註 – Proxy Server 4 不支援快取 HTTPS 文件。

所有 HTTP 文件都具有描述性標頭區段，Proxy Server 可使用該區段來比較並評估代理伺服器快取中的文件與遠端伺服器上的文件。當代理伺服器針對 HTTP 文件執行最新狀態檢查時，代理伺服器會傳送一個請求給伺服器，告知伺服器若發現快取中的版本過期則傳回文件。通常，文件在上次請求後並無變更，因此不會進行傳輸。此種透過檢查 HTTP 文件是否爲最新的方式可節省頻寬並減少延時。

爲降低與遠端伺服器之間的作業事件，Proxy Server 可讓您針對 HTTP 文件設定 [Cache Expiration] 設定。[Cache Expiration] 設定提供資訊給代理伺服器，以判斷傳送請求給伺服器之前，是否需要爲 HTTP 文件執行最新狀態檢查。代理伺服器會根據在 HTTP 文件標頭中找到的 Last-Modified 日期來進行估計。

對於 HTTP 文件，您也可以使用 [Cache Refresh] 設定。此選項指定代理伺服器是否一直進行最新狀態檢查 (這會置換過期設定)，或代理伺服器是否等待特定時間間隔後再進行檢查。下表顯示同時指定過期設定與重新整理設定時，代理伺服器的動作。使用重新整理設定可顯著降低延時並節省頻寬。

表 12–1 對 HTTP 使用 [Cache Expiration] 與 [Cache Refresh] 設定

重新整理設定	過期設定	結果
一直執行最新狀態檢查	(不適用)	一直執行最新狀態檢查
使用者指定的間隔	使用文件的「Expires」標頭	間隔過期時進行最新狀態檢查
	使用文件的 Last-Modified 標頭來估計	估計值與 Expires 標頭值兩者中較小者*

備註 – * 對於經常變更的文件，使用較小的值可避免從快取取得過期的資料。

設定 HTTP 快取重新整理間隔

如果確定要讓 Proxy Server 快取 HTTP 文件，則必須確定是讓 Proxy Server 一直對快取內的文件進行最新狀態檢查，還是讓它根據 [Cache Refresh] 設定 (最新狀態檢查間隔) 來進行檢查。例如，對 HTTP 文件合理的重新整理間隔是四到八小時。重新整理間隔越久，代理伺服器連線到遠端伺服器的次數就越少。即使代理伺服器未在重新整理間隔時間內執行最新狀態檢查，使用者也可以按一下用戶端中的 [Reload] 按鈕強制重新整理。此動作可讓代理伺服器對遠端伺服器執行強制最新狀態檢查。

您可以在 [Set Cache Specifics] 頁面或 [Set Caching Configuration] 頁面設定 HTTP 文件的重新整理間隔。使用 [Set Cache Specifics] 頁面可以配置全域快取程序，而使用 [Set Caching Configuration] 頁面可以控制特定 URL 與資源的快取程序。

設定 HTTP 快取過期策略

您也可以設定伺服器以使用 Last-modified 因子或只使用明確的過期資訊來檢查快取文件是否爲最新。

明確的過期資訊是見於某些 HTTP 文件中的一種標頭，指定檔案的過期日期與時間。使用明確的 Expires 標頭的 HTTP 文件並不是很多，因此您應該根據 Last-modified 標頭來決定何時執行最新狀態檢查。

若決定根據 Last-modified 標頭來快取您的 HTTP 文件，必須選取要在過期估計中使用的分數。此分數稱爲 LM 因子，將與文件的上次修改時間和上次對文件執行最新狀態檢查的時間之間的間隔相乘。將所得數字和自上次執行最新狀態檢查以來的時間做比較。若此數字小於時間間隔，表示文件尚未過期。較小的分數會讓代理伺服器更頻繁地檢查文件。

例如，假設有一個文件的上次變更時間是十天前。若將 Last-modified 因子設定爲 0.1，代理伺服器會將其解釋爲該文件可能會有一天時間不會變更 (10 * 0.1 = 1)。在這種情況下，如果在不到一天前檢查過此文件，代理伺服器會從快取中傳回文件。

同樣以此爲例，若 HTTP 文件的快取重新整理設定是設定爲小於一天，則代理伺服器在一天中會執行一次以上的最新狀態檢查。代理伺服器會一直使用需要其更頻繁地更新檔案的值 ([Cache Refresh] 或 [Cache Expiration])。

您可以在 [Set Cache Specifics] 頁面或 [Set Caching Configuration] 頁面設定 HTTP 文件的過期設定。使用 [Set Cache Specifics] 頁面可以配置全域快取程序，而使用 [Set Caching Configuration] 頁面可以控制特定 URL 與資源的快取程序。

向遠端伺服器報告 HTTP 存取次數

Sun Java System Web Proxy Server 快取文件後到再次重新整理前，文件可被存取多次。對於遠端伺服器而言，傳送一份副本給加以快取的代理伺服器僅表示存取一次，也就是一個「符合項目」。Proxy Server 可以針對兩次最新狀態檢查期間，計算從代理伺服器快取存取指定文件的計數，然後將此符合項目的計數在下次重新整理此文件時，透過附加 HTTP 請求標頭 (Cache-Info) 傳回遠端伺服器。如此一來，若遠端伺服器是配置爲識別此標頭類型，遠端伺服器就能接收到某文件存取次數的更準確記錄。

快取 FTP 與 Gopher 文件

FTP 與 Gopher 不包含檢查文件是否爲最新的方法。因此，最佳化 FTP 與 Gopher 文件快取的唯一方式是設定 [Cache Refresh] 間隔。[Cache Refresh] 間隔是 Proxy Server 從遠端伺服器擷取最新版文件之前的等待時間。若未設定 [Cache Refresh] 間隔，即使快取中的文件已是最新版本，代理伺服器也會擷取這些文件。

若要設定 FTP 與 Gopher 的快取重新整理間隔，請爲代理伺服器取得的文件選擇您認爲最安全的間隔。例如，如果儲存的資訊很少變更，請使用較大的數字 (幾天)。若資料

經常變更，最好每隔幾小時就擷取檔案。在重新整理期間，您有可能會把過期檔案傳送給用戶端。若重新整理間隔足夠短 (例如幾小時)，可以降低上述風險，同時回應時間也會明顯縮短。

您可以在 [Set Cache Specifics] 頁面或 [Set Caching Configuration] 頁面設定 FTP 與 Gopher 文件的快取重新整理間隔。使用 [Set Cache Specifics] 頁面可以配置全域快取程序，而使用 [Set Caching Configuration] 頁面可以控制特定 URL 與資源的快取程序。如需有關使用 [Set Cache Specifics] 頁面的更多資訊，請參閱第 225 頁的「設定快取明細」。如需有關使用 [Set Caching Configuration] 頁面的更多資訊，請參閱第 233 頁的「配置快取」。

備註 – 若您的 FTP 與 Gopher 文件差異性很大 (有些經常變更，有些很少變更)，請使用 [Set Caching Configuration] 頁面爲每種類型的文件建立個別範本 (例如，建立資源 `ftp://.*.gif` 的範本)，然後爲該資源設定適合的重新整理間隔。

建立與修改快取

快取分割區是磁碟或記憶體中保留的部分，此保留部分是用於快取用途。若快取容量變更，最好變更或增加分割區。

▼ 增加快取分割區

1. **存取 Server Manager，然後按一下 [Caching] 標籤。**
2. **按一下 [Add/Edit Cache Partitions] 連結。**
   此時會顯示 [Add/Edit Cache Partitions] 頁面。
3. **按一下 [Add Cache Partition] 按鈕。**
   此時會顯示 [Cache Partition Configuration] 頁面。
4. **為新分割區提供適當的值。**
5. **按一下 [OK]。**
6. **按一下 [Restart Required]。**
   此時會顯示 [Apply Changes] 頁面。
7. **按一下 [Restart Proxy Server] 按鈕以套用變更。**

▼ 修改快取分割區

1. **存取 Server Manager，然後按一下 [Caching] 標籤。**
2. **按一下 [Add/Edit Cache Partitions] 連結。**
   此時會顯示 [Add/Edit Cache Partitions] 頁面。
3. **按一下要變更的分割區名稱。**
4. **編輯資訊。**
5. **按一下 [OK]。**
6. **按一下 [Restart Required]。**
   此時會顯示 [Apply Changes] 頁面。
7. **按一下 [Restart Proxy Server] 按鈕以套用變更。**

設定快取容量

快取容量值用來導出快取目錄結構。快取目錄中可容納的區段數目源自快取容量。快取容量與快取目錄中的快取階層有直接關聯。容量越大，階層就越大。快取容量應該等於或大於快取大小。若計劃未來將增加快取大小 (例如，透過增加外接式磁碟的方式)，將容量設定爲大於快取大小將很有幫助。快取容量最大值是 32 GB，設定爲此容量時可建立 256 個區段。

▼ 設定快取容量

1. **存取 Server Manager，然後按一下 [Caching] 標籤。**
2. **按一下 [Set Cache Capacity] 連結。**
   此時會顯示 [Set Cache Capacity] 頁面。
3. **從 [New Capacity Range] 下拉式清單選擇容量。**
4. **按一下 [OK]。**
5. **按一下 [Restart Required]。**
   此時會顯示 [Apply Changes] 頁面。

6 **按一下 [Restart Proxy Server] 按鈕以套用變更。**

管理快取區段

代理伺服器快取分爲一或多個快取區段。區段數目上限爲 256 個。快取區段的數目必須是 2 的乘冪 (例如，1、2、4、8、16、...、256)。快取容量最大值爲 32 GB (最佳值)，具有 256 個快取區段。

若選擇 500 MB 的快取容量，安裝程式會建立 4 個快取區段 (500 d6 125 = 4)；若選擇 2 GB 的快取容量，安裝程式會建立 16 個區段 (2000 d6 125 = 16)。選擇 125 MB 做爲每個區段的最佳值以取得區段的數目。區段數目越多，跨區段儲存與分配的 URL 數目就越多。

▼ 管理快取區段

1 **存取 Server Manager，然後按一下 [Caching] 標籤。**

2 **按一下 [Manage Sections] 連結。**
此時會顯示 [Manage Sections] 頁面。

3 **變更該表格上的資訊。**
可以在現有的分割區之間移動區段。

4 **按一下 [OK]。**

5 **按一下 [Restart Required]。**
此時會顯示 [Apply Changes] 頁面。

6 **按一下 [Restart Proxy Server] 按鈕以套用變更。**

設定資源回收喜好設定

您可以使用快取回收收集器從快取中刪除檔案。資源回收可以自動模式或明確模式執行。明確模式是指由管理員在外部設定排程。選取其中一種模式，然後按一下 [OK]。按一下 [Restart Required]。此時會顯示 [Apply Changes] 頁面。按一下 [Restart Proxy Server] 按鈕以套用變更。

排程資源回收

[Schedule Garbage Collection] 頁面可指定執行資源回收的日期與時間。

▼ 設定資源回收

1. **存取 Server Manager，然後按一下 [Caching] 標籤。**
2. **按一下 [Schedule Garbage Collection] 連結。**
   此時會顯示 [Schedule Garbage Collection] 頁面。
3. **從 [Schedule Garbage Collection At list] 清單選取執行資源回收的時間。**
4. **指定要在星期幾執行資源回收。**
5. **按一下 [OK]。**
6. **按一下 [Restart Required]。**
   此時會顯示 [Apply Changes] 頁面。
7. **按一下 [Restart Proxy Server] 按鈕以套用變更。**

配置快取

您可以針對符合所指定之常規表示式模式的 URL，指定數個配置參數值。透過此功能，您可以根據已快取的文件類型更精確地控制代理伺服器快取。配置快取可能包括確定下列項目：

- 快取預設值
- 如何快取需要認證的頁面
- 如何快取查詢
- 快取檔案大小的最小值與最大值
- 重新整理快取文件的時機
- 快取過期策略
- 用戶端中斷時的快取運作方式
- 無法連線到來源伺服器時的快取運作方式

備註 – 若將特定資源的快取預設值設定爲 [Derived configuration] 或 [Don't cache]，則 [Set Caching Configuration] 頁面將不會顯示快取配置選項。然而，若爲資源選擇快取預設值 Cache，則可以指定數個其他配置項目。

▼ 配置快取

1. **存取 Server Manager，然後按一下 [Caching] 標籤。**
2. **按一下 [Set Caching Configuration] 頁面。**
   此時會顯示 [Set Caching Configuration] 頁面。
3. **從下拉式清單中選取資源，或按一下 [Regular Expression] 按鈕，然後鍵入常規表示式並按一下 [OK]。**
4. **變更配置資訊。**
5. **按一下 [OK]。**
6. **按一下 [Restart Required]。**
   此時會顯示 [Apply Changes] 頁面。
7. **按一下 [Restart Proxy Server] 按鈕以套用變更。**

快取配置元素

以下各節包含的資訊將協助您確定最符合您需求的配置。

設定快取預設值

代理伺服器可讓您確定特定資源的快取預設值。此處所稱資源是指符合您所指定的某些條件的檔案類型。例如，若要讓您的伺服器自動快取來自網域 `company.com` 的所有文件，可以建立以下常規表示式

`[a-z] *://[^/:]\\.company\\.com.*`。

依預設，將選取 [Cache] 選項。您的伺服器會自動快取來自該網域的所有可快取文件。

備註 – 若將特定資源的快取預設值設定爲 [Derived configuration] 或 [Don't cache]，則不需要爲該資源配置快取。然而，若爲資源選擇快取預設值 Cache，則可以指定數個其他配置項目。如需這些項目的清單，請參閱第 233 頁的 「配置快取」。

也可以設定 HTTP、FTP 與 Gopher 的快取預設值。

快取需要認證的頁面

您可以讓伺服器快取需要使用者認證的檔案。Proxy Server 會爲快取中的檔案加上標籤，如此一來，當使用者請求檔案時，Proxy Server 可以向遠端伺服器要求認證。

因爲 Proxy Server 無法決定遠端伺服器的認證方式，而且沒有使用者 ID 或密碼清單，所以它只會在每次收到對需要認證的文件的請求時強制對遠端伺服器執行最新狀態檢查。 因此，使用者必須鍵入 ID 與密碼才能取得檔案的存取權。若使用者在瀏覽器階段作業中的初期存取過該伺服器，則瀏覽器會自動傳送認證資訊，而不會提示使用者。

若不啓用對需要認證的頁面的快取，則代理伺服器會採取預設的運作方式，即不會對它們進行快取。

快取查詢

快取查詢只適用於 HTTP 文件。您可以限制所快取查詢的長度，也可完全禁止快取查詢。查詢越長，重複的機會就越低，快取的效用也越低。

以下快取限制適用於查詢：

- 存取方法必須是 GET、文件不能有保護 (除非已啓用快取需要認證之頁面的功能)，且回應中至少必須有一個 Last-modified 標頭。這需要查詢引擎指明查詢結果文件可以快取才行。
- 若有 Last-modified 標頭，則查詢引擎應該支援條件式 GET 方法 (使用 If-modified-since 標頭) 才能使快取生效；否則，查詢引擎應該傳回 Expires 標頭。

設定快取檔案大小的最小值與最大值

可以爲 Proxy Server 快取的檔案大小設定最小值與最大值。若您的網路連線速度很快，最好設定最小值。若連線速度很快，擷取小型檔案的速度可能會快到讓伺服器不需要快取這些檔案。在此情況下，您可以只快取較大的檔案。您可能想要設定檔案大小的最大值，以確定大型檔案不會佔用太多代理伺服器磁碟空間。

設定最新狀態檢查策略

最新狀態檢查策略可確保 HTTP 文件永遠是最新的。您也可以指定 Proxy Server 的重新整理間隔。

設定過期策略

您可以使用 Last-Modified 因子或明確的過期資訊來設定過期策略。

設定用戶端中斷時的快取運作方式

若文件只擷取了一部分時用戶端就中斷了資料傳輸，則代理伺服器可以爲了快取的目的而完成文件擷取程序。代理伺服器的預設值是爲了快取，而針對已擷取至少 25% 的文件完成擷取文件的動作。否則，代理伺服器會終止遠端伺服器連線，並移除未完成擷取的檔案。您可以視需要提高或降低用戶端中斷百分比。

無法連線到伺服器時的運作方式

若由於無法與原始伺服器連線，致使對過期文件進行的最新狀態檢查失敗，您可以指定代理伺服器是否傳送快取中的過期文件。

快取本地主機

若從本地主機請求的 URL 缺少網域名稱，Proxy Server 將不會快取它。此運作方式可避免重複快取。例如，若使用者從本機伺服器請求 `http://machine/filename.html` 與 `http://machine.example.com/filename.html`，兩個 URL 可能都會出現在快取中。因爲這些檔案是來自本機伺服器，擷取這些檔案的速度很快，因此沒有必要快取這些檔案。

然而，若您的公司在許多遠端位置都有伺服器，您可能想要快取來自所有主機的文件，以降低網路流量並縮短存取檔案所需的時間。

▼ 啓用對本地主機的快取

1. **存取 Server Manager，然後按一下 [Caching] 標籤。**
2. **按一下 [Cache Local Hosts] 連結。**
   此時會顯示 [Cache Local Hosts] 頁面。
3. **從下拉式清單中選取資源，或按一下 [Regular Expression] 按鈕，然後鍵入常規表示式並按一下 [OK]。**
   如需有關常規表示式的更多資訊，請參閱第 16 章 「管理範本和資源」。
4. **按一下 [Enabled] 按鈕。**
5. **按一下 [OK]。**

6 **按一下 [Restart Required]。**
此時會顯示 [Apply Changes] 頁面。

7 **按一下 [Restart Proxy Server] 按鈕以套用變更。**

配置檔案快取記憶體

依預設，檔案快取總處於開啓狀態。檔案快取設定包含在 `server.xml` 檔案中。您可以使用 Server Manager 變更檔案快取記憶體的設定。

備註 – 使用者介面會顯示 [Configure File Cache] 頁面，但此頁面在 Proxy Server 4 的此發行版本中並未實作

▼ 配置檔案快取

1 **按一下 Server Manager 的 [Caching] 標籤。**

2 **按一下 [File Cache Configuration] 連結。**
此時會顯示 [File Cache Configuration] 頁面。

3 **選取 [Enable File Cache] (如果尚未選取)。**

4 **選擇是否傳輸檔案。**
當您啓用 [Transmit File] 時，伺服器會快取檔案快取 (而非檔案內容) 中檔案的開啓檔案描述元。`PR_TransmitFile` 用於將檔案內容傳送給用戶端。啓用 [Transmit File] 時，由於僅快取開啓檔案描述元，因此檔案快取不再像平常一樣區別小型、中型和大型檔案。依預設，[Transmit File] 在 Windows 上啓用，而在 UNIX 上停用。在 UNIX 系統上，您只應該針對本機作業系統已經支援 PR_TransmitFile 的平台 (目前包括 HP-UX 和 AIX) 啓用 [Transmit File]。不建議在 UNIX/Linux 平台上啓用此選項。

5 **鍵入雜湊表格的大小。**
預設大小是檔案最大數目的兩倍加 1。例如，如果檔案的最大數目設定爲 1024，則預設的隨機表格大小爲 2049。

6 **鍵入有效快取項目的最長作用時間 (以秒為單位)。**
預設設定是 30。此設定控制快取檔案後可以繼續使用快取資訊的時間。比 MaxAge 舊的項目將由相同檔案的新項目替代 (如果快取參照相同的檔案)。您可以根據內容是否定期更新來設定最長作用時間。例如，如果一天以固定時間間隔更新內容四次，則可將最長作用時間設定爲 21600 秒 (6 小時)。否則，請考慮將最長存在時間設定爲要在檔案經過修改後仍願意提供內容檔案之先前版本的最長時間。

7. **鍵入要快取的最多檔案數量：[Maximum Number of Files]。**
   預設設定是 1024。

8. **鍵入中型與小型檔案大小限制 (以位元組為單位)。**
   [Medium File Size Limit] 的預設值是 537600。[Small File Size Limit] 的預設值是 2048。

   快取對於小型、中型與大型檔案的處理方式不一樣。透過將檔案對映到虛擬記憶體來快取中型檔案的內容 (僅限於 UNIX/Linux 平台)。透過配置堆疊儲存區空間，然後將檔案讀入此空間，來快取小型檔案的內容。對於大型檔案，只會快取檔案的相關資訊，而不會快取檔案內容。區分小型檔案與中型檔案的好處，在於小型檔案的數目很多時，可避免浪費虛擬記憶體眾多頁面的一部分。因此，[Small File Size Limit] 的值通常略低於 VM 頁面大小。

9. **設定中型與小型檔案空間。**
   中型檔案空間是用於對映所有中等大小檔案的虛擬記憶體大小 (以位元組爲單位)。此大小預設爲 10485760。小型檔案空間是用於快取的堆疊儲存區空間大小 (以位元組爲單位)，包括用於快取小型檔案的堆疊儲存區空間。在 UNIX/Linux 中，此大小預設爲 1048576。

10. **按一下 [OK]。**

11. **按一下 [Restart Required]。**
    此時會顯示 [Apply Changes] 頁面。

12. **按一下 [Restart Proxy Server] 按鈕以套用變更。**

檢視 URL 資料庫

您可以檢視所有已記錄之快取 URL (依照存取協定與網站名稱分組) 的名稱與屬性。您可以透過存取此資訊而執行各種快取管理功能，例如將快取中的文件設定爲過期與將快取中的文件移除。

▼ 檢視資料庫中的 URL

1. **存取 Server Manager，然後按一下 [Caching] 標籤。**

2. **按一下 [View URL Database] 連結。**
   此時會顯示 [View URL Database] 頁面。

3. **按一下 [Regenerate] 按鈕以產生最新的快取 URL 清單。**

4 (可選) 若要檢視特定 URL 的資訊，請在 [Search] 欄位鍵入 URL 或常規表示式，然後按一下 [Search] 按鈕。

5 若要檢視依網域名稱與主機分組的快取資料庫資訊：

a. 請從清單中選取一個網域名稱。
此時會顯示該網域的主機清單。按一下主機名稱，此時會顯示 URL 清單。

b. 按一下 URL 名稱。
此時會顯示關於該 URL 的詳細資訊。

c. 按一下 URL 名稱可查看關於該 URL 的詳細資訊。

▼ 將快取 URL 設定為過期或移除快取 URL

1 存取 Server Manager，然後按一下 [Caching] 標籤。

2 按一下 [View URL Database] 連結。
此時會顯示 [View URL Database] 頁面。

3 按一下 [Regenerate] 按鈕以產生快取資料庫的快照。
此快照爲後續步驟的基礎。

4 若知道要設定為過期或移除的特定 URL，請在 [Search] 欄位中鍵入 URL 或符合此 URL 的常規表示式，然後按一下 [Search] 按鈕。

5 如果想處理依照網域名稱與主機分組的 URL：

a. 請從清單中選取一個網域名稱。
此時會顯示該網域的主機清單。

b. 按一下主機名稱，此時會顯示 URL 清單。

6 若要將個別檔案設定為過期：

a. 請選取這些檔案之 URL 旁的 [Ex] 選項。

b. 然後按一下 [Exp/Rem Marked] 按鈕。

7 若要將清單中的所有檔案設定為過期，請按一下表單底部的 [Exp All] 按鈕。

8. **若要從快取中移除個別檔案：**

   a. **請選取要移除之檔案的 URL 旁的 [Rm] 選項。**

   b. **然後按一下 [Exp/Rem Marked] 按鈕。**

9. **若要移除清單中的所有檔案，請按一下 [Rem All] 按鈕。**

10. **按一下 [Regenerate] 按鈕以重新產生快照。**

備註 – 當您使用 [Ex] 或 [Rm] 選項時，會處理關聯的檔案，但所做的變更不會反映在快照中。您必須重新產生快照，才能看到所做的變更。

使用快取批次更新

您可以在代理伺服器不忙碌的時候預先載入指定網站中的檔案，或對已存在於快取中的文件執行最新狀態檢查。您可以建立、編輯與刪除 URL 批次，以及啓用與停用批次更新。

建立批次更新

您可以透過指定要批次更新的檔案來主動快取檔案。您可以針對已存在於快取中的數個檔案執行最新狀態檢查，或預先載入特定網站中的多個檔案。

▼ 建立批次更新

1. **存取 Server Manager，然後按一下 [Caching] 標籤。**

2. **按一下 [Set Cache Batch Updates] 連結。**
   此時會顯示 [Set Cache Batch Updates] 頁面。

3. **從 [Create/Select a Batch Update Configuration] 旁的下拉式清單中選取 [New and Create]。**

4. **按一下 [OK]。此時會顯示 [Set Cache Batch Updates] 頁面。**

5. **在 [Name] 區段中，鍵入新批次更新項目的名稱。**

6. **在該頁面的 [Source] 區段中，選取要建立的批次更新類型。**
   若要針對快取中的所有文件執行最新狀態檢查，請按一下第一個單選按鈕。若要從指定的來源 URL 以遞迴方式快取 URL，請按一下第二個單選按鈕。

7 **在 [Source] 區段欄位中，指定要在批次更新中使用的文件。**

8 **在 [Exceptions] 區段中，指定要從批次更新排除的任何檔案。**

9 **在 [Resources] 區段中，鍵入最大同步式連線數以及遍歷的最大文件數。**

10 **按一下 [OK]。**
選取新增的批次名稱，並從 [Create/Select a Batch Update Configuration] 旁的下拉式清單中選取 [Schedule]。

11 **按一下 [OK]。**

備註 – 您可以在不開啓批次更新的情況下建立、編輯與刪除批次更新配置。然而，如果希望批次更新根據您在 [Set Cache Batch Updates] 頁面所設定的時間執行，則必須開啓更新。

---

12 **此時會顯示 [Schedule Batch Updates] 頁面。**

13 **選取 [Update On] 或 [Update Off] 選項。**

14 **在下拉式清單中選取時間，然後選取要執行更新的日期。**

15 **按一下 [OK]。**

16 **按一下 [Restart Required]。**
此時會顯示 [Apply Changes] 頁面。

17 **按一下 [Restart Proxy Server] 按鈕以套用變更。**

編輯或刪除批次更新配置

若要排除特定檔案或更頻繁地更新批次，可以編輯批次更新。也能想要完全刪除某個批次更新配置。

▼ 編輯或刪除批次更新配置

1 **存取 Server Manager，然後按一下 [Caching] 標籤。**

2 **按一下 [Set Cache Batch Updates] 連結。**
此時會顯示 [Set Cache Batch Updates] 頁面。

3. **若要編輯批次，請選取批次名稱，然後從 [Create/Select a Batch Update Configuration] 旁的下拉式清單中選取 [Edit]。**
4. **按一下 [OK]。**
   此時會顯示 [Set Cache Batch Updates] 頁面。
5. **視需要修改資訊。**
6. **按一下 [OK]。**
7. **按一下 [Restart Required]。**
   此時會顯示 [Apply Changes] 頁面。
8. **按一下 [Restart Proxy Server] 按鈕以套用變更。**

▼ 刪除批次更新配置

1. **存取 Server Manager，然後按一下 [Caching] 標籤。**
2. **按一下 [Set Cache Batch Updates] 連結。**
3. **若要刪除批次，請選取批次名稱，然後從 [Create/Select a Batch Update Configuration] 旁的下拉式清單中選取 [Delete]。**
4. **按一下 [OK]。**
5. **按一下 [Restart Required]。**
   此時會顯示 [Apply Changes] 頁面。
6. **按一下 [Restart Proxy Server] 按鈕以套用變更。**

使用快取指令行介面

代理伺服器提供數個指令行公用程式，您可以使用這些公用程式來配置、變更、產生與修復您的快取目錄結構。這些公用程式的功能大部分都與 Server Manager 頁面上的功能重複。若需要對維護 (例如 cron 工作) 進行排程，您可能需要使用這些公用程式。所有公用程式都位於 `extras` 目錄。

▼ 執行指令行公用程式

1 **從指令行提示符號移至** *server_root* `/proxy-server`*id* **目錄**。

2 **鍵入** `./start -shell`
以下各節說明各種公用程式。

建立快取目錄結構

名爲 `cbuild` 的代理伺服器公用程式是一個離線快取資料庫管理程式。此公用程式可讓您使用指令行介面來建立新的快取結構或修改現有的快取結構。您可以使用 Server Manager 頁面來啓用代理伺服器以使用新建立的快取。

備註 – 此公用程式不會更新 `server.xml` 檔案。`cbuild` 無法對具有多個分割區的快取調整大小。透過 `cbuild` 建立或修改快取時，應該手動更新 `server.xml` 檔案中的 `cachecapacity` 參數。

```
<PARTITION partitionname="part1" partitiondir="/home/build/install9
/proxy-server1/cache" maxsize="1600" minspace="5" enabled="true"/>
<CACHE enabled="true" cachecapacity="2000" cachedir="/tmp/cache">
```

您可以使用兩種模式來呼叫 `cbuild` 公用程式。第一種模式是：

```
cbuild -d conf-dir -c cache-dir -s cache size
cbuild -d conf-dir -c cache-dir -s cache size -r
```

例如：

```
cbuild -d server_root/proxy-serverid/config
    -c server_root/proxy-serverid/cache -s 512
cbuild -d server_root/proxy-serverid/config
    -c server_root/proxy-serverid/cache -s 512 -r
```

其中

- *conf-dir* 是代理伺服器實例的配置目錄，它位於 *server_root* `/proxy-server`*id*`/config` 目錄中。
- *cache-dir* 是快取結構的目錄。
- *cache size* 是快取可擴充到的最大值。此選項不能與 *cache-dim* 參數一起使用。上限大小是 65135 MB。
- `-r` 可調整現有快取結構的大小 (假設該快取結構只有單一分割區)。建立新快取時不需要此選項。

第二種模式是：

```
cbuild -d conf-dir -c cache-dir -n cache-dim
cbuild -d conf-dir -c cache-dir -n cache-dim -r
```

例如：

```
cbuild -d server_root/proxy-serverid/config
    -c server_root/proxy-serverid/cache -n 3
cbuild -d server_root/proxy-serverid/config
    -c server_root/proxy-serverid/cache -n 3 -r
```

其中

- *conf-dir* 是代理伺服器實例的配置目錄，它位於 *server_root* `/proxy-server`*id*`/config` 目錄中。
- *cache-dir* 是快取結構的目錄。
- *cache-dim* 決定區段數目。例如，在圖 12–2 中，區段顯示爲 s3.4，其中 3 表示大小。*cache-dim* 的預設值是 0，最大值是 8。
- `-r` 可調整現有快取結構的大小 (假設該快取結構只有單一分割區)。建立新快取時不需要此選項。

管理快取 URL 清單

代理伺服器公用程式 `urldb` 用於管理快取中的 URL 清單。您可以使用此公用程式來列出已快取的 URL。您也可以從快取資料庫選取性地移除已快取的物件，或將它設定爲過期。

`urldb` 指令可根據 `-o` 選項分爲三個群組：

- 網域
- 網站
- URL
- 若要列出網域，請在指令行中鍵入以下指令：

  ```
  urldb -o matching_domains -e reg-exp -d conf-dir
  ```

  例如：

  ```
  urldb -o matching_domains -e “.*phoenix.*” -d server-root/proxy-serverid/config
  ```

  其中

  - *matching_domains* 可列出符合常規表示式的網域
  - *reg-exp* 是所使用的常規表示式

- *conf-dir* 是代理伺服器實例的配置目錄，它位於 *server-root* `/proxy-server`*id*`/config` 目錄中。

- 若要列出網域中所有符合的網站，請在指令行中鍵入以下指令：

  ```
  urldb -o matching_sites_in_domain -e reg-exp -m domain_name -d conf-dir
  ```

  例如：

  ```
  urldb -o matching_sites_in_domain -e ".*atlas" -m phoenix.com
      -d server-root/proxy-serverid/config
  ```

  其中

  - `matching_sites_in_domain` 可列出網域中所有符合常規表示式的網站
  - *reg-exp* 是所使用的常規表示式
  - *domain_name* 是網域的名稱
  - *conf-dir* 是代理伺服器實例的配置目錄，它位於 *server-root* `/proxy-server`*id*`/config` 目錄中。

- 若要列出所有符合的網站，請在指令行中間鍵入以下指令：

  ```
  urldb -o all_matching_sites -e reg-exp -d conf-dir
  ```

  例如：

  ```
  urldb -o all_matching_sites -e ".*atlas.*" -d server-root/proxy-serverid/config
  ```

  其中

  - `all_matching_sites` 可列出所有符合常規表示式的網站
  - *reg-exp* 是所使用的常規表示式
  - *conf-dir* 是代理伺服器實例的配置目錄，它位於 *server-root* `/proxy-server`*id*`/config` 目錄中。

- 若要列出網站中符合的 URL，請在指令行中鍵入以下指令：

  ```
  urldb -o matching_urls_from_site -e reg-exp -s site_name -d conf-dir
  ```

  例如：

  ```
  urldb -o matching_urls_from_site -e "http://.*atlas.*" -s atlas.phoenix.com
      -d server-root/proxy-serverid/config
  ```

  其中

  - `matching_urls_from_site` 可列出網站中所有符合常規表示式的 URL
  - *reg-exp* 是所使用的常規表示式
  - *site_name* 是網站的名稱

- *conf-dir* 是代理伺服器實例的配置目錄，它位於 *server-root* `/proxy-server`*id*`/config` 目錄中。

- 若要將網站中符合的 URL 設定爲過期或將它移除，請在指令行中鍵入以下指令：

```
urldb -o matching_urls_from_site -e reg-exp -s site_name -x e -d conf-dir
urldb -o matching_urls_from_site -e reg-exp -s site_name -x r -d conf-dir
```

  例如：

```
urldb -o matching_urls_from_site -e “http://.*atlas.*” -s atlas.phoenix.com
    -x e -d server-root/proxy-serverid/config
```

  其中

  - `matching_urls_from_site` 可列出網站中所有符合常規表示式的 URL
  - *reg-exp* 是所使用的常規表示式
  - *site_name* 是網站的名稱
  - `-x e` 選項可將快取資料庫中符合的 URL 設定爲過期。此選項無法與網域和網站模式一起使用
  - `-x r` 選項可從快取資料庫移除符合的 URL
  - *conf-dir* 是代理伺服器實例的配置目錄，它位於 *server-root* `/proxy-server`*id*`/config` 目錄中。

- 若要列出所有符合的 URL，請在指令行中鍵入以下指令：

```
urldb -o all_matching_urls -e reg-exp -d conf-dir
```

  例如：

```
urldb -o all_matching_urls -e “.*cgi-bin.*” -d
    server-root/proxy-serverid/config
```

  其中

  - `all_matching_urls` 可列出所有符合常規表示式的 URL
  - *reg-exp* 是所使用的常規表示式
  - *conf-dir* 是代理伺服器實例的配置目錄，它位於 *server-root* `/proxy-server`*id*`/config` 目錄中。

- 若要將所有符合的 URL 設定爲過期，或要移除所有符合的 URL，請在指令行中鍵入以下指令：

```
urldb -o all_matching_urls -e reg-exp -x e -d conf-dir
urldb -o all_matching_urls -e reg-exp -x r -d conf-dir
```

  例如：

```
urldb -o all_matching_urls -e “.*cgi-bin.*” -x e -d server-root/proxy-serverid/config
```

其中

- `all_matching_urls` 可列出所有符合常規表示式的 URL
- *reg-exp* 是所使用的常規表示式
- `-x e` 選項可將快取資料庫中所有符合的 URL 設定爲過期
- `-x r` 選項可從快取資料庫移除符合的 URL
- *conf-dir* 是代理伺服器實例的配置目錄，它位於 *server-root* `/proxy-server`*id*`/config` 目錄中。

- 若要將 URL 清單設定爲過期或移除 URL 清單，請在指令行中鍵入以下指令：

```
urldb -l url-list -x e -e reg-exp -d conf-dir
urldb -l url-list -x r -e reg-exp -d conf-dir
```

例如：

```
urldb -l url.lst -x e -e “.*cgi-bin.*” -d server-root/proxy-serverid/config
```

其中

- `url-list` 是需要設定爲過期的 URL 清單。此選項可用於提供 URL 清單。
- `-x e` 選項可將快取資料庫中符合的 URL 設定爲過期。
- `-x r` 選項可從快取資料庫移除符合的 URL。
- *reg-exp* 是所使用的常規表示式
- *conf-dir* 是代理伺服器實例的配置目錄，它位於 *server-root* `/proxy-server`*id*`/config` 目錄中。

管理快取資源回收

`cachegc` 公用程式可讓您從快取資料庫中移除受快取大小限制，可能已過期或過舊以致於無法快取的物件。

備註 – 使用 `cachegc` 公用程式時，請確定 CacheGC 並未在代理伺服器實例中執行。

`cachegc` 公用程式的使用方式如下：

```
cachegc -f leave-fs-full-percent -u gc-high-margin-percent -l gc-low-margin-percent -e
    extra-margin-percent -d conf-dir
```

例如：

```
cachegc -f 50 -u 80 -l 60 -e 5 -d server-root/proxy-serverid/config
```

其中

- *leave-fs-full-percent* 可判斷快取分割區大小的百分比，當快取分割區大小低於此值時，將不會執行資源回收
- *gc-high-margin-percent* 可控制最大快取大小的百分比，當達到此值時，會觸發資源回收
- *gc-low-margin-percent* 可控制回收收集器目標的最大快取大小百分比
- *extra-margin-percent* 是由回收收集器用來確定要移除的快取部分。
- *conf-dir* 是代理伺服器實例的配置目錄，它位於 *server-root* `/proxy-server`*id*`/config` 目錄中。

管理批次更新

`bu` 公用程式用於更新快取，它有兩種運作模式。在第一種模式中，它會反覆檢查快取資料庫，並透過爲每個 URL 傳送 HTTP 請求來更新快取中現存的所有 URL。在第二種模式中，它會從指定的 URL 開始對從此 URL 至所指定層級的所有連結執行廣度優先遍歷，並將頁面擷取到快取中。`bu` 是與 RFC 相容的網頁抓取程式。

`bu -n` *hostname* `-p` *port* `-t` *time-lmt* `-f` *contact-address* `-s` *sleep-time* `-o` *object* `-r n -d` *conf-dir*

例如：

```
bu -n phoenix -p 80 -t 3600 -f admin@phoenix.com -s 60 -o nova -r n
    -d server-root/proxy-serverid/config
```

其中

- *hostname* 是執行代理伺服器的機器的主機名稱。預設值是 localhost。
- *port* 是代理伺服器執行時所用的連接埠。預設連接埠是 `8080`。
- *time-lmt* 是執行公用程式的時間限制
- *contact-address* 決定將透過 `bu` 傳送的 HTTP 請求傳送的連絡位址。預設值是 `worm@proxy-name`。
- *sleep-time* 是兩個連續請求之間的暫停時間。預設值是 5 秒。
- *object* 是目前正在執行的 `bu.conf` 中指定的物件。
- `-r n` 選項決定是否遵循 `robot.txt` 策略。預設值是 `y`。
- *conf-dir* 是代理伺服器實例的配置目錄，它位於 *server-root* `/proxy-server`*id*`/config` 目錄中。

使用網際網路快取協定 (ICP)

網際網路快取協定 (ICP) 是物件位置協定，它可以讓快取彼此進行通訊。快取可以使用 ICP 來傳送有關快取 URL 是否存在，以及擷取這些 URL 最佳位置的查詢與回覆。在典型的 ICP 交換中，一個快取會將有關特定 URL 的 ICP 查詢傳送給所有相鄰的快取。接著，那些快取會傳回 ICP 回覆，指出它們是否包含該 URL。若它們不包含該 URL，則會傳回 [MISS]。若包含該 URL，則會傳回 [HIT]。

透過 ICP 鄰近區域路由

ICP 可用來讓位於不同管理網域中的代理伺服器進行通訊。它可讓位於不同管理網域中的代理伺服器快取相互通訊。對於數個代理伺服器需要進行通訊，但無法從一部主代理伺服器配置所有伺服器 (因爲它們位於代理伺服器陣列中) 的情形而言，使用 ICP 是有效的。圖 12–3 顯示了不同管理網域中各代理伺服器之間的 ICP 交換。

透過 ICP 相互通訊的代理伺服器稱爲**芳鄰**。ICP 鄰近區域中的芳鄰不能超過 64 個。ICP 鄰近區域中的兩種芳鄰類型分別是 **父系芳鄰**與**同層芳鄰**。如果沒有其他芳鄰具有請求的 URL，則只有父系芳鄰可存取遠端伺服器。 您的 ICP 鄰近區域可以沒有任何父系芳鄰，也可以有一個以上的父系芳鄰。ICP 鄰近區域中的任何芳鄰如果**不是**父系芳鄰，就會被視爲同層芳鄰。同層芳鄰無法擷取遠端伺服器中的文件，除非同層芳鄰被標示爲 ICP 的預設路由，且 ICP 使用預設值。

您可以使用**輪詢循環**來決定芳鄰接收查詢的順序。輪詢循環就是 ICP 查詢循環。您必須爲每個芳鄰指定輪詢循環。若將所有芳鄰配置於輪詢循環一，則會同時在一個循環中查詢所有芳鄰。若將某些芳鄰配置於輪詢循環 2，則會先查詢輪詢循環 1 中的所有芳鄰，如果都沒有傳回「符合項目」，則會查詢循環 2 中的所有代理伺服器。輪詢循環的最大值是二。

因爲 ICP 父系芳鄰可能會成爲網路瓶頸，您可以使用輪詢循環來減輕其負載。常見的設定方式是將所有同層芳鄰配置在輪詢循環 1，並將所有父系芳鄰配置在輪詢循環 2。如此一來，若本機代理伺服器請求 URL，該請求會先傳送至鄰近區域中的所有同層芳鄰。若沒有任何同層芳鄰具有請求的 URL，則請求會傳送至父系芳鄰。若父系芳鄰沒有該 URL，則會從遠端伺服器擷取。

ICP 鄰近區域中的每個芳鄰必須至少有一個執行中的 ICP 伺服器。若芳鄰沒有執行任何 ICP 伺服器，則無法回覆來自芳鄰的 ICP 請求。啓用代理伺服器上的 ICP 時會啓動 ICP 伺服器 (若 ICP 尚未執行)。

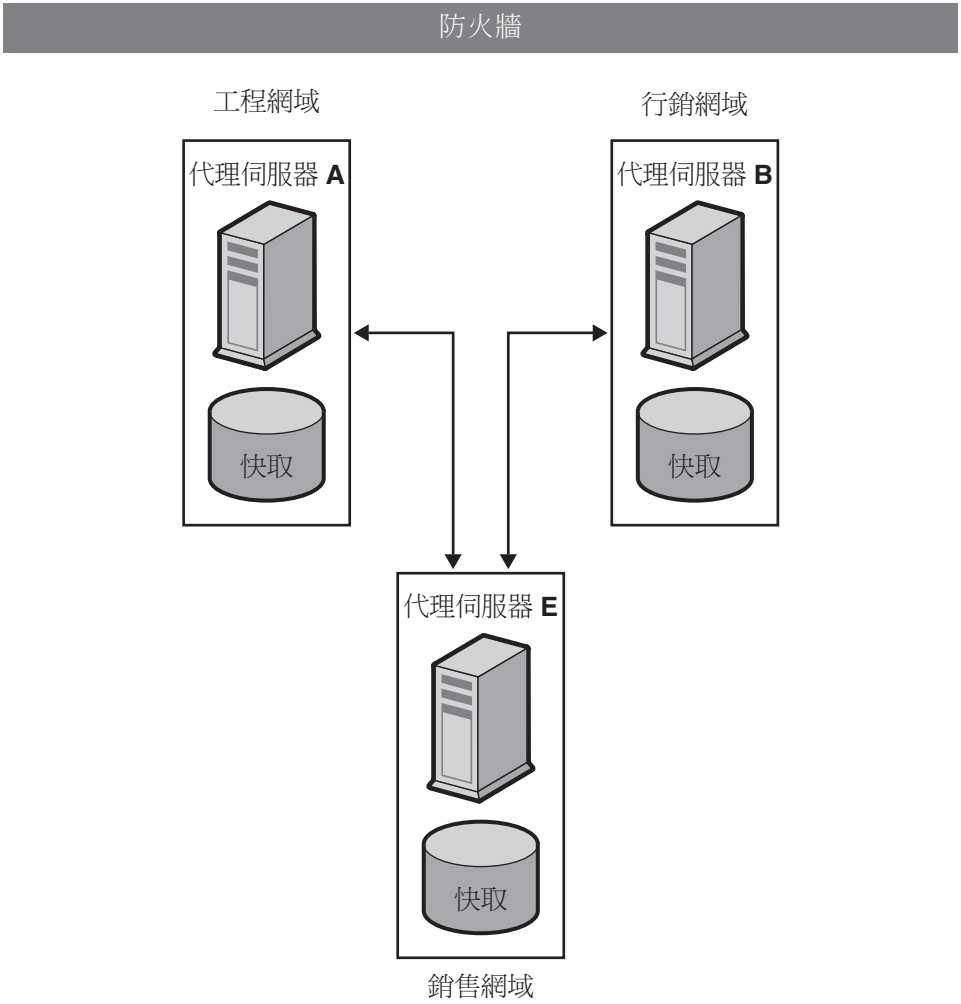


圖 12–3 ICP 交換

設定 ICP

本小節提供有關設定 ICP 的詳細資訊。設定 ICP 的一般步驟如下：

1. (可選) 將父系增加到您的 ICP 鄰近區域。

   如需更多資訊，請參閱第 251 頁的 「將父系或同層代理伺服器增加到 ICP 鄰近區域」。

2. 將同層芳鄰增加到您的 ICP 鄰近區域。

如需更多資訊，請參閱第 251 頁的 「將父系或同層代理伺服器增加到 ICP 鄰近區域」。

3. 配置 ICP 鄰近區域中的每個芳鄰。

   如需更多資訊，請參閱第 252 頁的 「編輯 ICP 鄰近區域的配置」。

4. 啓用 ICP。

   如需更多資訊，請參閱第 254 頁的 「啓用 ICP」。

5. 若您的代理伺服器在其 ICP 鄰近區域中具有同層芳鄰或父系芳鄰，請啓用透過 ICP 鄰近區域路由的功能。

   如需更多資訊，請參閱第 255 頁的 「啓用透過 ICP 鄰近區域路由」。

▼ 將父系或同層代理伺服器增加到 ICP 鄰近區域

1 存取 Server Manager，然後按一下 [Caching] 標籤。

2 按一下 [Configure ICP] 連結。

此時會顯示 [Configure ICP] 頁面。

3 在該頁面的 [Parent List] 區段，按一下 [Add] 按鈕。

此時會顯示 [ICP Parent] 頁面。

- 若要增加父系代理伺服器，請按一下該頁面上 [Parent List] 區段中的 [Add]。

  此時會顯示 [ICP Parent] 頁面。
- 若要增加同層代理伺服器，請按一下該頁面上 [Sibling List] 區段中的 [Add]。

  此時會顯示 [ICP Sibling] 頁面。

4 在 [Machine Address] 欄位中，鍵入要增加到 ICP 鄰近區域之代理伺服器的 IP 位址或主機名稱。

5 在 [ICP Port] 欄位中，鍵入代理伺服器將用來偵聽 ICP 訊息的連接埠號。

6 (可選) 在 [Multicast Address] 欄位中，鍵入父系要偵聽的多重播送位址。多重播送位址是可讓多部伺服器偵聽的 IP 位址。

使用多重播送位址後，代理伺服器就能將一個查詢，傳送到偵聽該多重播送位址之所有芳鄰都能查看的網路中。如此一來，就不需要將查詢分別傳送至每個芳鄰。使用多重播送是選擇性的。

備註 – 不同輪詢循環中的芳鄰不應該偵聽相同的多重播送位址。

---

7. **在 [TTL] 欄位中，將多重播送訊息轉寄至的子網路數目。**
   若將 TTL 設定爲 1，就只能將多重播送訊息轉寄到本機子網路。若將 TTL 設定爲 2，就會將訊息轉寄到相差一個層級的所有子網路，依此類推。

   備註 – 多重播送可讓兩個不相關的芳鄰彼此傳送 ICP 訊息。因此，爲避免不相關的芳鄰接收來自您的 ICP 鄰近區域中代理伺服器的 ICP 訊息，請在 [TTL] 欄位中設定較低的 TTL 值。

8. **在 [Proxy Port] 欄位中，鍵入父系代理伺服器的連接埠。**
9. **從 [Polling Round] 下拉式清單中，選擇您希望父系代理伺服器位於哪個輪詢循環。預設的輪詢循環是 1。**
10. **按一下 [OK]。**
11. **按一下 [Restart Required]。**
    此時會顯示 [Apply Changes] 頁面。
12. **按一下 [Restart Proxy Server] 按鈕以套用變更。**

▼ 編輯 ICP 鄰近區域的配置

1. **存取 Server Manager，然後按一下 [Caching] 標籤。**
2. **選取 [Configure ICP] 連結。此時會顯示 [Configure ICP] 頁面。**
3. **選取您要編輯之代理伺服器旁的單選按鈕。**
4. **按一下 [Edit] 按鈕。**
5. **視需要修改資訊。**
6. **按一下 [OK]。**
7. **按一下 [Restart Required]。**
   此時會顯示 [Apply Changes] 頁面。
8. **按一下 [Restart Proxy Server] 按鈕以套用變更。**

▼ 移除 ICP 鄰近區域中的代理伺服器

1 **存取 Server Manager，然後按一下 [Caching] 標籤。**

2 **選取 [Configure ICP] 連結。此時會顯示 [Configure ICP] 頁面。**

3 **選取您要移除之代理伺服器旁的單選按鈕。**

4 **按一下 [Delete] 按鈕。**

5 **按一下 [Restart Required]。**
此時會顯示 [Apply Changes] 頁面。

6 **按一下 [Restart Proxy Server] 按鈕以套用變更。**

▼ 配置 ICP 鄰近區域中的本機代理伺服器

您必須配置 ICP 鄰近區域中的每個芳鄰 (或本機代理伺服器)。

1 **存取 Server Manager，然後按一下 [Caching] 標籤。**

2 **選取 [Configure ICP] 連結。**
此時會顯示 [Configure ICP] 頁面。

3 **在 [Binding Address] 欄位中，鍵入芳鄰伺服器將連結的 IP 位址。**

4 **在 [Port] 欄位中，鍵入芳鄰伺服器將用來偵聽 ICP 的連接埠號。**

5 **在 [Multicast Address] 欄位中，鍵入芳鄰要偵聽的多重播送位址。**
多重播送位址是可讓多部伺服器偵聽的 IP 位址。使用多重播送位址後，代理伺服器就能將一個查詢，傳送到偵聽該多重播送位址之所有芳鄰都能查看的網路中。如此一來，就不需要將查詢分別傳送至每個芳鄰。

若同時爲芳鄰指定多重播送位址與連結位址，芳鄰會使用連結位址來傳送回覆，並使用多重播送位址來偵聽。若未指定連結位址也未決定多重播送位址，作業系統會決定要使用哪個位址來傳送資料。

6 **在 [Default Route] 欄位中鍵入的代理伺服器名稱或 IP 位址，屬於鄰近代理伺服器的回應都沒有符合項目時，芳鄰應將請求路由至的目標代理伺服器。**
若在此欄位中鍵入「origin」，或將此欄位保留爲空白，預設路由就會是原始伺服器。

若從 [No Hit Behavior] 下拉式清單中選擇 [first responding parent]，您在 [Default Route] 欄位中鍵入的路由將不會有作用。只有在選擇預設的「無符合項目」運作方式時，代理伺服器才會使用此路由。

7. **在第二個 [Port] 欄位中，鍵入您在 [Default Route] 欄位鍵入之預設路由機器的連接埠號。**

8. **從 [On No Hits, Route Through] 下拉式清單中選擇當 ICP 鄰近區域內所有同層芳鄰的快取內都沒有請求的 URL 時芳鄰所要採取的運作方式。**
   可用選項如下：
   - **first responding parent**。芳鄰將透過第一個以 [miss] 回應的父系芳鄰擷取請求的 URL。
   - **default route**。芳鄰將透過 [Default Route] 欄位中指定的機器來擷取請求的 URL。

9. **在 [Server Count] 欄位中，鍵入將用來服務 ICP 請求的程序數目。**

10. **在 [Timeout] 欄位中，鍵入芳鄰將在每個循環中等待 ICP 回應的最長時間。**

11. **按一下 [OK]。**

12. **按一下 [Restart Required]。**
    此時會顯示 [Apply Changes] 頁面。

13. **按一下 [Restart Proxy Server] 按鈕以套用變更。**

▼ 啓用 ICP

1. **存取 Server Manager，然後按一下 [Preferences] 標籤。**

2. **按一下 [Configure System Preferences] 連結。**
   此時會顯示 [Configure System Preferences] 頁面。

3. **選取 ICP 的 [Yes] 單選按鈕，然後按一下 [OK]。**

4. **按一下 [Restart Required]。**
   此時會顯示 [Apply Changes] 頁面。

5. **按一下 [Restart Proxy Server] 按鈕以套用變更。**

▼ 啓用透過 ICP 鄰近區域路由

只有當代理伺服器在 ICP 鄰近區域中有其他同層芳鄰或父系芳鄰時，才需要啓用透過 ICP 鄰近區域路由。若代理伺服器是其他代理伺服器的父系，且沒有自己的同層芳鄰或父系芳鄰，則只需要爲該代理伺服器啓用 ICP。不需要啓用透過 ICP 鄰近區域路由。

1. **存取 Server Manager，然後按一下 [Routing] 標籤。**
2. **按一下 [Set Routing Preferences] 連結。**
   此時會顯示 [Set Routing Preferences] 頁面。
3. **從下拉式清單中選取資源，或按一下 [Regular Expression] 按鈕，然後鍵入常規表示式並按一下 [OK]。**
4. **選取 [Route Through] 選項旁的單選按鈕。**
5. **選取 ICP 旁的核取方塊。**
6. **(可選) 若要讓用戶端直接從具有此文件的 ICP 芳鄰擷取文件，而不是透過其他芳鄰取得該文件，請選取 [Text Redirect] 選項旁的核取方塊。**
7. **按一下 [OK]。**

注意 – 目前沒有用戶端支援重新導向，因此現在請不要使用此功能。

8. **按一下 [Restart Required]。**
   此時會顯示 [Apply Changes] 頁面。
9. **按一下 [Restart Proxy Server] 按鈕以套用變更。**

使用代理伺服器陣列

分散式快取的代理伺服器陣列，可讓多部代理伺服器的運作方式如同單一快取。陣列中的每部代理伺服器將會包含不同的快取 URL，這些 URL 可以由瀏覽器或下游代理伺服器擷取。代理伺服器陣列可避免多部代理伺服器常有的快取重複問題。透過基於雜湊的路由，代理伺服器陣列可將請求路由至代理伺服器陣列中正確的快取。

代理伺服器陣列也提供增量延展性功能。如果決定將另一個代理伺服器增加到您的代理伺服器陣列，每個成員的快取並不會失效。在每個成員的快取中，只有 1/*n* 的 URL 會重新指定給其他成員，其中 *n* 是陣列中代理伺服器的數目。

透過代理伺服器陣列路由

對於每個透過代理伺服器陣列的請求，雜湊函數會爲陣列中的每個代理伺服器指定一個分數，此分數是以所請求的 URL、代理伺服器名稱與代理伺服器的負載因子爲依據。以後請求就會路由至分數最高的代理伺服器。

因爲 URL 請求可能來自用戶端與代理伺服器，所以透過代理伺服器陣列的路由有兩種類型：用戶端至代理伺服器路由與代理伺服器至代理伺服器路由。

在用戶端至代理伺服器路由中，用戶端會使用代理伺服器自動配置 (PAC) 機制來決定應該通過哪部代理伺服器。然而，用戶端不是使用標準的 PAC 檔案，而是使用一種計算雜湊演算法的特殊 PAC 檔案，以決定所請求之 URL 的適當路由。圖 12–4 顯示了用戶端至代理伺服器路由。在這張圖中，代理伺服器陣列的每個成員會載入並輪詢主代理伺服器，以判斷 PAT 檔案是否有更新。一旦用戶端擁有 PAC 檔案，如果配置變更，用戶端只要再次下載此檔案即可。一般而言，用戶端將會在重新啓動時下載 PAC 檔案。

代理伺服器可透過使用管理介面決定的「代理伺服器陣列成員身分表格 (PAT)」規格來自動產生特殊的 PAC 檔案。

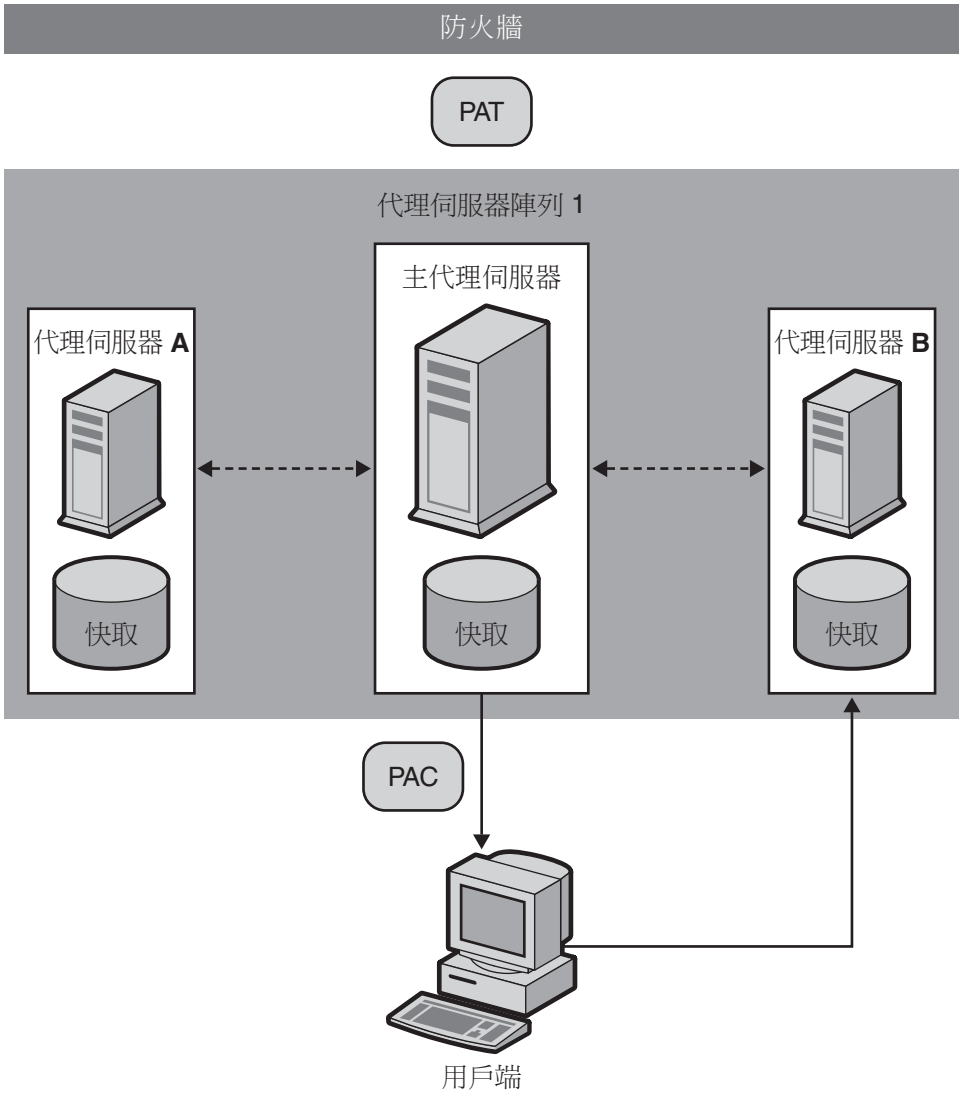


圖 12–4 用戶端至代理伺服器路由

在代理伺服器至代理伺服器路由中，代理伺服器會使用 PAT (代理伺服器陣列表格) 檔案 (而非用戶端所使用的 PAC 檔案) 來計算雜湊演算法。PAT 檔案是 ASCII 檔案，它包含代理伺服器陣列的相關資訊，包括代理伺服器的機器名稱、IP 位址、連接埠、負載因子與快取大小等。在伺服器計算雜湊演算法時，使用 PAT 檔案比使用 PAC 檔案 (必須在執行階段解譯的 JavaScript 檔案) 有效率得多。然而，大部分用戶端無法識別 PAT 檔案格式，因此必須使用 PAC 檔案。圖 12–5 顯示了代理伺服器至代理伺服器路由。

PAT 檔案是在代理伺服器陣列中的主代理伺服器建立。代理伺服器管理員必須決定要使用哪部代理伺服器做爲主代理伺服器。管理員可以從這一部主代理伺服器變更 PAT 檔案。以後代理伺服器陣列的所有其他成員，就可以手動或自動輪詢主代理伺服器以取得這些變更。您可以將每個成員配置爲自動根據這些變更產生 PAC 檔案。

您也可以將代理伺服器陣列鏈接在一起，以進行階層式路由。若某部代理伺服器透過上游代理伺服器陣列以路由內送請求，則該上游代理伺服器陣列即稱爲父系陣列。換句話說，若用戶端向代理伺服器 X 請求文件，且代理伺服器 X 沒有該文件，它會將請求傳送到代理伺服器陣列 Y，而非將請求直接傳送到遠端伺服器。因此代理伺服器陣列 Y 是父系陣列。

在圖 12–5 中，代理伺服器陣列 1 是代理伺服器陣列 2 的父系陣列。代理伺服器陣列 2 的成員會載入並進行輪詢，以確定父系代理伺服器陣列的 PAT 檔案是否有更新。通常，該成員會輪詢父系陣列中的主代理伺服器。所請求 URL 的雜湊演算法，要以所下載的 PAT 檔案來計算。接著，代理伺服器陣列 2 中的成員會從代理伺服器陣列 1 中最高分數的代理伺服器，擷取所請求的 URL。在這張圖中，對於用戶端所請求的 URL，代理伺服器 B 具有最高的分數。

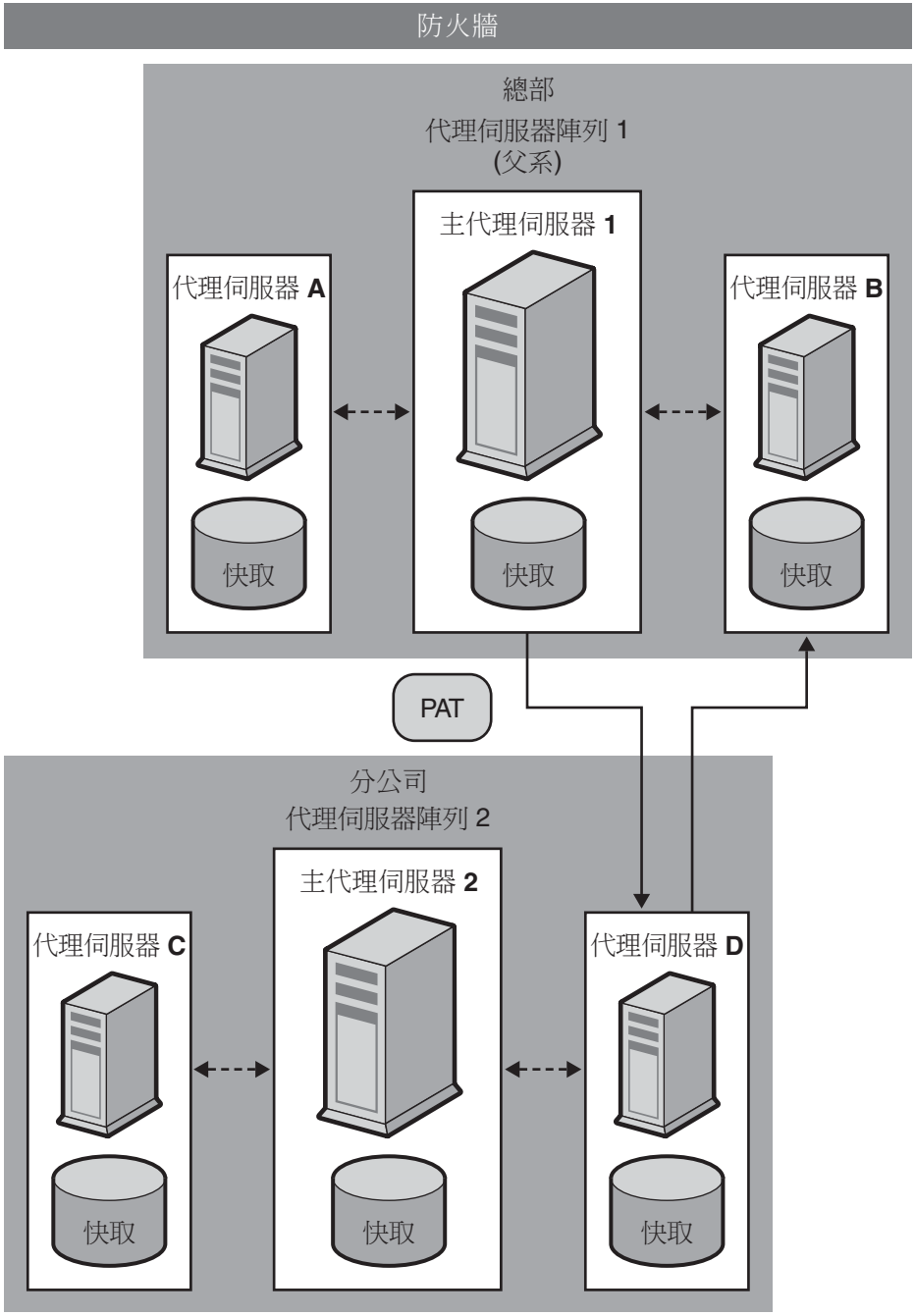


圖 12–5 代理伺服器至代理伺服器路由

設定代理伺服器陣列的一般步驟如下所示。

從主代理伺服器執行下列步驟：

1. 建立代理伺服器陣列。

   如需有關建立成員清單的更多資訊，請參閱第 260 頁的 「建立代理伺服器陣列成員清單」。
2. 從您的 PAT 檔案產生 PAC 檔案。

   只有在使用用戶端至代理伺服器路由時，才需要產生 PAC 檔案。如需更多資訊，請參閱第 266 頁的 「使用 PAT 檔案產生 PAC 檔案」。
3. 配置陣列的主成員。如需更多資訊，請參閱第 263 頁的 「配置代理伺服器陣列成員」。
4. 啓用透過代理伺服器陣列路由。如需更多資訊，請參閱第 264 頁的 「啓用透過代理伺服器陣列路由」。
5. 建立 PAT 對映，將 URL `/pat` 對映到 PAT 檔案。
6. 啓用您的代理伺服器陣列。

   如需更多資訊，請參閱第 265 頁的 「啓用或停用代理伺服器陣列」。

從每個非主代理伺服器執行下列步驟：

1. 配置陣列的非主成員。

   如需更多資訊，請參閱第 263 頁的 「配置代理伺服器陣列成員」
2. 啓用透過代理伺服器陣列路由。

   如需更多資訊，請參閱第 264 頁的 「啓用透過代理伺服器陣列路由」。
3. 啓用您的代理伺服器陣列。

   如需更多資訊，請參閱第 265 頁的 「啓用或停用代理伺服器陣列」。

備註 – 若代理伺服器陣列將透過父系陣列路由，則還必須啓用該父系陣列，並配置每個成員透過父系陣列路由來取得所需的 URL。如需更多資訊，請參閱第 268 頁的 「透過父系陣列路由」。

建立代理伺服器陣列成員清單

您應該只從陣列的主代理伺服器，來建立與更新代理伺服器陣列成員清單。您只需要建立代理伺服器陣列成員清單一次，但可隨時修改。建立代理伺服器陣列成員清單時會產生 PAT 檔案，可將此檔案分發給陣列中的所有代理伺服器以及所有下游代理伺服器。

備註 – 若要對代理伺服器陣列成員清單進行變更或增加，只能透過陣列中的主代理伺服器來執行。陣列中的所有其他成員只能讀取成員清單。

▼ 建立代理伺服器陣列成員清單

1. **存取 Server Manager，然後按一下 [Caching] 標籤。**
2. **按一下 [Configure Proxy Array] 連結。**
   此時會顯示 [Configure Proxy Array] 頁面。
3. **在 [Array name] 欄位中，鍵入陣列的名稱。**
4. **在 [Reload Configuration Every] 欄位中，鍵入每次針對 PAT 檔案進行輪詢的相隔分鐘數。**
5. **按一下 [Array Enabled] 核取方塊。**
6. **按一下 [Create] 按鈕。**
   建立代理伺服器陣列之後，[Create] 按鈕會變更爲 [OK] 按鈕。

   備註 – 開始增加成員到成員清單之前，請務必按一下 [OK]。
7. **按一下 [OK]。**
8. **按一下 [Restart Required]。**
   此時會顯示 [Apply Changes] 頁面。
9. **為代理伺服器陣列中的每個成員提供下列資訊，然後按一下 [OK]。**
   必須先增加主成員，才能增加其他成員。
   - **Name**。您要增加到成員清單之代理伺服器的名稱
   - **IP Address**。您要增加到成員清單之代理伺服器的 IP 位址
   - **Port**。此爲成員用來輪詢 PAT 檔案的連接埠。
   - **Load Factor**。此整數表示應透過此成員進行路由的相關負載。
   - **Status**。成員的狀態。此值可以是 [on] 或 [off]。若停用某個代理伺服器陣列成員，將會透過其他成員重新路由該成員的請求。

   備註 – 爲要增加的每個代理伺服器陣列成員鍵入資訊之後，請務必按一下 [OK]。

10 **按一下 [Restart Required]。**
此時會顯示 [Apply Changes] 頁面。

11 **按一下 [Restart Proxy Server] 按鈕以套用變更。**

編輯代理伺服器陣列成員清單資訊

您可以隨時變更代理伺服器陣列成員清單中的成員資訊。您只能從主代理伺服器編輯代理伺服器陣列成員清單。

備註 – 若要對代理伺服器陣列成員清單進行變更或增加，只能透過陣列中的主代理伺服器來執行。若從陣列中的其他成員修改此清單，所有變更都會遺失。

▼ 編輯成員清單資訊

1 **存取 Server Manager，然後按一下 [Caching] 標籤。**

2 **按一下 [Configure Proxy Array] 連結。**
此時會顯示 [Configure Proxy Array] 頁面。

3 **在 [Member List] 中，選取您要編輯之成員旁的單選按鈕。**

4 **按一下 [Edit] 按鈕。**
此時會顯示 [Configure Proxy Array Member] 頁面。

5 **編輯相關資訊。**

6 **按一下 [OK]。**

7 **按一下 [Restart Required]。**
此時會顯示 [Apply Changes] 頁面。

8 **按一下 [Restart Proxy Server] 按鈕以套用變更。**

備註 – 若要讓變更生效並將變更分發給代理伺服器陣列中的成員，請更新 [Configure Proxy Array] 頁面上的 [Configuration ID]，然後按一下 [OK]。若要更新配置 ID，只需將 ID 加 1 即可。

刪除代理伺服器陣列成員

刪除代理伺服器陣列成員會將它們從代理伺服器陣列移除。您只能從主代理伺服器刪除代理伺服器陣列成員。

▼ 刪除代理伺服器陣列成員

1. **存取 Server Manager，然後按一下 [Caching] 標籤。**
2. **按一下 [Configure Proxy Array] 連結。**
   此時會顯示 [Configure Proxy Array] 頁面。
3. **在 [Member List] 中，選取您要刪除之成員旁的單選按鈕。**
4. **按一下 [Delete] 按鈕。**

備註 – 若要讓變更生效並將變更分發給代理伺服器陣列中的成員，請更新 [Configure Proxy Array] 頁面上的 [Configuration ID]，然後按一下 [OK]。若要更新配置 ID，只需將 ID 加 1 即可。

---

5. **按一下 [Restart Required]。**
   此時會顯示 [Apply Changes] 頁面。
6. **按一下 [Restart Proxy Server] 按鈕以套用變更。**

配置代理伺服器陣列成員

只需對代理伺服器陣列中的每個成員進行一次配置，且必須從成員本身進行配置。無法從其他成員處配置。還必須配置主代理伺服器。

▼ 配置代理伺服器陣列的每個成員

1. **存取 Server Manager，然後按一下 [Caching] 標籤。**
2. **按一下 [Configure Proxy Array Member] 連結。**
   此時會顯示 [Configure Proxy Array Member] 頁面。
3. **在 [Proxy Array] 區段，選取適當的單選按鈕以指定成員是否需要針對 PAT 檔案進行輪詢。**

- **Non-Master Member**。若您要配置的成員**不是**主代理伺服器，請選取此選項。主代理伺服器以外的所有代理伺服器陣列成員都必須針對 PAT 檔案進行輪詢，以便從主代理伺服器擷取該檔案。
- **Master Member**。若您要配置主代理伺服器，請選取此選項。若您要配置主代理伺服器，PAT 檔案將位於本機，因此不需要輪詢。

4. **在 [Poll Host] 欄位中，鍵入要向其輪詢 PAT 檔案的主代理伺服器名稱。**
5. **在 [Port] 欄位中，鍵入主代理伺服器用來接受 HTTP 請求的連接埠。**
6. **在 [URL] 欄位中，鍵入主代理伺服器上之 PAT 檔案的 URL。若已在主代理伺服器上建立 PAT 對映，以將 PAT 檔案對映到 URL `/pat`，則應該在 [URL] 欄位中鍵入 `/pat`。**
7. **(可選) 在 [Headers File] 欄位中，鍵入檔案的完整路徑，此檔案包含必須與 PAT 檔案的 HTTP 請求一起傳送的所有特殊標頭，例如認證資訊。**
8. **按一下 [OK]。**
9. **按一下 [Restart Required]。**
   此時會顯示 [Apply Changes] 頁面。
10. **按一下 [Restart Proxy Server] 按鈕以套用變更。**

啓用透過代理伺服器陣列路由

▼ 啓用透過代理伺服器陣列路由

1. **存取 Server Manager，然後按一下 [Routing] 標籤。**
2. **按一下 [Set Routing Preferences] 連結。**
   此時會顯示 [Set Routing Preferences] 頁面。
3. **從下拉式清單中選取資源，或按一下 [Regular Expression] 按鈕，然後鍵入常規表示式並按一下 [OK]。**
4. **選取 [Route Through] 選項。**
5. **選取代理伺服器陣列或父系陣列的核取方塊。**
   只有在配置的代理伺服器是代理伺服器陣列的成員時，才能啓用代理伺服器陣列路由。只有當父系陣列存在時，才能啓用父系路由。上述兩個路由選項彼此獨立。

6 **若選擇透過代理伺服器陣列路由，且想要將請求重新導向到另一個 URL，請選取 [Redirect] 核取方塊。**

重新導向表示若代理伺服器陣列的某個成員收到不應由它服務的請求，則會告知用戶端應連絡哪部代理伺服器來處理該請求。

7 **按一下 [OK]。**

8 **按一下 [Restart Required]。**

此時會顯示 [Apply Changes] 頁面。

9 **按一下 [Restart Proxy Server] 按鈕以套用變更。**

啓用或停用代理伺服器陣列

若不是透過代理伺服器陣列進行路由，則停用代理伺服器陣列選項之前，應先確定所有用戶端都使用特殊 PAC 檔案以使路由正確。若停用父系陣列選項，則應該在 [Set Routing Preferences] 頁面上設定有效的替代路由選項，例如明確的代理伺服器或直接連線。

▼ 啓用或停用代理伺服器陣列

1 **存取 Server Manager，然後按一下 [Preferences] 標籤。**

2 **按一下 [Configure System Preferences] 連結。**

此時會顯示 [Configure System Preferences] 頁面。

3 **啓用或停用代理伺服器陣列。**

- 若要啓用代理伺服器陣列，請按一下要啓用之陣列類型或特定陣列的 [Yes] 選項：一般代理伺服器陣列或父系陣列。
- 若要停用代理伺服器陣列，請按一下 [No]。

4 **按一下 [OK]。**

5 **按一下 [Restart Required]。**

此時會顯示 [Apply Changes] 頁面。

6 **按一下 [Restart Proxy Server] 按鈕以套用變更。**

重新導向代理伺服器陣列中的請求

若選擇透過代理伺服器陣列路由，則必須指定是否要將請求重新導向到另一個 URL。重新導向表示若代理伺服器陣列的某個成員收到不應由它服務的請求，則會告知用戶端應連絡哪部代理伺服器來處理該請求。

使用 PAT 檔案產生 PAC 檔案

因爲大多數用戶端都無法識別 PAT 檔案格式，所以用戶端至代理伺服器路由中的用戶端會使用代理伺服器自動配置 (PAC) 機制來接收有關應該通過哪個代理伺服器的資訊。然而，用戶端不會使用標準的 PAC 檔案，而是使用源自 PAT 檔案的特殊 PAC 檔案。這個特殊 PAC 檔案會計算雜湊演算法，以決定所請求之 URL 的適當路由。

您可以從 PAT 檔案手動或自動產生 PAC 檔案。若從代理伺服器陣列的特定成員處手動產生 PAC 檔案，該成員將會根據目前 PAT 檔案中的資訊立即重新產生 PAC 檔案。若將代理伺服器陣列成員配置爲自動產生 PAC 檔案，則成員在每次偵測到 PAT 檔案有修改版本時，就會自動重新產生檔案。

備註 – 若您沒有使用代理伺服器的代理伺服器陣列功能，請使用 [Create/Edit Autoconfiguration File] 頁面來產生 PAC 檔案。如需更多資訊，請參閱第 17 章 「使用用戶端自動配置檔案」。

▼ 使用 PAT 檔案手動產生 PAC 檔案

PAC 檔案只能從主代理伺服器產生。

1. **存取主代理伺服器的 Server Manager，然後按一下 [Caching] 標籤。**
2. **按一下 [Configure Proxy Array] 連結。**
   此時會顯示 [Configure Proxy Array] 頁面。
3. **按一下 [Generate PAC] 按鈕。**
   此時會顯示 [PAC Generation] 頁面。
4. **若要在 PAC 檔案中使用自訂邏輯，請在 [Custom logic file] 欄位中鍵入包含自訂邏輯 (要在 PAC 檔案產生程序執行期間加入的邏輯) 之檔案的名稱。**
   此邏輯會插入 `FindProxyForURL` 函數中，代理伺服器陣列選取邏輯之前。此函數通常用於不需要通過代理伺服器陣列的本機請求。

   若已在配置代理伺服器陣列成員時提供自訂邏輯檔案，此欄位會自動寫入該資訊。您可以在此編輯自訂邏輯檔案名稱。

5 **在 [Default Route] 欄位中，鍵入陣列中的代理伺服器無法使用時，用戶端應採用的路由。**

若已在配置代理伺服器陣列成員時提供預設路由，此欄位會自動寫入該資訊。您可以在此編輯預設路由。

6 **按一下 [OK]。**

7 **按一下 [Restart Required]。**

此時會顯示 [Apply Changes] 頁面。

8 **按一下 [Restart Proxy Server] 按鈕以套用變更。**

▼ 自動產生 PAC 檔案

1 **存取 Server Manager，然後按一下 [Caching] 標籤。**

2 **按一下 [Configure Proxy Array Member] 連結。**

此時會顯示 [Configure Proxy Array Member] 頁面。

3 **選取 [Auto-generate PAC File] 核取方塊。**

4 **若要在 PAC 檔案中使用自訂邏輯，請在 [Custom Logic File] 欄位中鍵入包含您想要在 PAC 檔案產生時加入之自訂邏輯的檔案名稱。**

將此邏輯插入 `FindProxyFor URL` 函數中代理伺服器陣列選取邏輯之前。

若已在配置代理伺服器陣列時提供並儲存自訂邏輯檔案，此欄位會自動寫入該資訊。您可以在此編輯自訂邏輯檔案名稱。

5 **在 [Default Route] 欄位中，鍵入陣列中的代理伺服器無法使用時，用戶端應採用的路由。**

若已在配置代理伺服器陣列時提供預設路由，此欄位會自動寫入該資訊。您可以編輯預設路由。

6 **按一下 [OK]。**

7 **按一下 [Restart Required]。**

此時會顯示 [Apply Changes] 頁面。

8 **按一下 [Restart Proxy Server] 按鈕以套用變更。**

透過父系陣列路由

您可以將代理伺服器或代理伺服器陣列成員配置爲透過上游父系陣列路由，而非直接連線到遠端伺服器。

▼ 透過父系陣列路由

1. **啓用父系陣列**。
   如需更多資訊，請參閱第 265 頁的「啓用或停用代理伺服器陣列」。
2. **啓用透過父系陣列路由**。
   如需更多資訊，請參閱第 264 頁的「啓用透過代理伺服器陣列路由」。
3. **存取 Server Manager，然後按一下 [Caching] 標籤**。
4. **按一下 [Configure Proxy Array Member] 連結**。
   此時會顯示 [Configure Proxy Array Member] 頁面。
5. **在頁面中 [Parent Array] 區段的 [Poll Host] 欄位裡，鍵入父系陣列中代理伺服器的主機名稱，以便針對 PAT 檔案進行輪詢**。
   此代理伺服器通常是該父系陣列的主代理伺服器。
6. **在頁面中 [Parent Array] 區段的 [Port] 欄位，鍵入要針對 PAT 檔案進行輪詢的父系陣列中代理伺服器的連接埠號**。
7. **在 [URL] 欄位中，鍵入主代理伺服器上之 PAT 檔案的 URL**。
   若已在主代理伺服器上建立 PAT 對映，請在 [URL] 欄位中鍵入該對映。
8. **(可選) 在表單上 [Parent Array] 區段的 [Headers File] 欄位中，鍵入檔案的完整路徑，此檔案包含必須與 PAT 檔案的 HTTP 請求一起傳送的所有特殊標頭，例如認證資訊**。
   此欄位是選擇性的。
9. **按一下 [OK]**。
10. **按一下 [Restart Required]**。
    此時會顯示 [Apply Changes] 頁面。
11. **按一下 [Restart Proxy Server] 按鈕以套用變更**。

檢視父系陣列資訊

若您的代理伺服器陣列是透過父系陣列進行路由，則需要父系陣列成員的相關資訊。父系陣列會以 PAT 檔案形式傳送此資訊。

▼ 檢視父系陣列資訊

1. **存取 Server Manager，然後按一下 [Caching] 標籤。**
2. **按一下 [View Parent Array Configuration] 連結。**
   此時會顯示 [View Parent Array Configuration] 頁面。
3. **檢視該資訊。**

◆ ◆ ◆ 第 13 章

13 透過代理伺服器篩選內容

本章說明如何篩選 URL，讓代理伺服器拒絕存取 URL，或修改代理伺服器傳回給用戶端的 HTML 和 JavaScript 內容。本章也說明如何依據用戶端使用的 Web 瀏覽器 (使用者代理程式)，限制透過代理伺服器進行存取。

您可以使用 URL 篩選檔案來決定伺服器可支援的 URL。例如，您可以建立或購買文字檔，裡面包含要限制的 URL，而無需手動鍵入要支援的 URL 萬用字元式樣。此項功能讓您只須建立一個 URL 檔案，即可在許多不同的代理伺服器上使用。

您也可以依據 MIME 類型來篩選 URL。例如，您可以允許代理伺服器快取及傳送 HTML 和 GIF 檔案，但不允許其取得二進位檔或可執行檔，因爲這樣可能會招致電腦病毒的風險。

本章包含下列小節：

篩選 URL

您可以使用包含 URL 的檔案來配置代理伺服器要擷取的內容。您可以設定一份代理伺服器一定支援的 URL 清單，以及一份絕不支援的 URL 清單。

例如，如果您是網際網路服務提供者，所執行的代理伺服器提供適合兒童的內容，則可設定一份 URL 清單，包含經核准適合兒童檢視的 URL。然後您可以讓代理伺服器僅

擷取經過核准的 URL。如果用戶端試圖連線至不受支援的 URL，您可以讓代理伺服器傳回預設的「Forbidden」訊息，或是建立一則自訂訊息，說明用戶端無法存取該 URL 的原因。

若要依 URL 來限制存取，請透過 Server Manager 建立一個包含 URL 的檔案以允許或限制存取。您可以透過 Server Manager 完成此動作。建立好檔案後，就可以設定限制。後面幾節會討論這些程序。

建立 URL 篩選檔案

篩選檔案是一個包含 URL 清單的檔案。代理伺服器使用的篩選檔案爲純文字檔案，其中包含多行採用以下式樣的 URL：

```
protocol://host:port/path/filename
```

在以下三個區段的每個區段中都可以使用常規表示式：`protocol`、`host:port` 及 `path/filename`。例如，若要爲連線至 `netscape.com` 網域的所有協定建立一個 URL 式樣，則您應在檔案中增加以下一行：

```
.*://.*\\.example\\.com/.*
```

這一行僅在不指定連接埠號時才會作用。如需有關常規表示式的更多資訊，請參閱第 16 章 「管理範本和資源」中的「瞭解常規表示式」。

如果您不想使用 Server Manager 而要自己建立檔案，請使用 [Server Manager] 頁面建立一個空的檔案，然後在該檔案中自行增加文字，或以包含常規表示式的檔案來取代該檔案。

▼ 建立篩選檔案

1. **存取 Server Manager，然後按一下 [Filters] 標籤。**
2. **按一下 [Restrict URL Filter Access] 連結。**
   此時會顯示 [Restrict URL Filter Access] 頁面。
3. **從 [Create/Edit] 按鈕旁的下拉式清單中選擇 [New Filter]。**
4. **在下拉式清單右邊的文字方塊中鍵入篩選檔案的名稱，然後按一下 [Create/Edit] 按鈕。**
   此時會顯示 [Filter Editor] 頁面。
5. **在 [Filter Content] 可捲動文字方塊中鍵入 URL 及 URL 的常規表示式。**
   [Reset] 按鈕可清除欄位內的所有文字。

   如需有關常規表示式的更多資訊，請參閱第 16 章 「管理範本和資源」中的「瞭解常規表示式」。

6 **按一下 [OK]。**
代理伺服器即會建立檔案，並使您返回 [Restrict URL Filter Access] 頁面。篩選檔案建立在 `proxy-server`*id*`/conf_bk` 目錄中。

設定篩選檔案的預設存取

備妥內含要使用的 URL 之篩選檔案後，即可設定這些 URL 的預設存取。

▼ 設定篩選檔案的預設存取

1 **存取 Server Manager，然後按一下 [Filters] 標籤。**

2 **按一下 [Restrict URL Filter Access] 連結。**
此時會顯示 [Restrict URL Filter Access] 頁面。

3 **選擇要與篩選器一起使用的範本。**
通常您會希望建立的篩選檔案可以用於整個代理伺服器，但是您可能需要針對 HTTP 和 FTP 分別建立一組篩選檔案。

4 **請使用 [URL Filter To Allow] 清單選擇一個篩選檔案，其中包含您要代理伺服器支援的 URL。**

5 **請使用 [URL Filter To Deny] 清單選擇一個篩選檔案，其中包含您要代理伺服器拒絕存取的 URL。**

6 **選擇用戶端請求遭到拒絕的 URL 時，您希望代理伺服器傳回的文字。**
   - 傳送代理伺服器產生的預設「Forbidden」回應。
   - 傳送含有自訂文字的文字檔或 HTML 檔案。在文字方塊中鍵入此檔案的絕對路徑。

7 **按一下 [OK]。**

8 **按一下 [Restart Required]。此時會顯示 [Apply Changes] 頁面。**

9 **按一下 [Restart Proxy Server] 按鈕以套用變更。**

內容 URL 重寫

Proxy Server 可以檢視傳回給用戶端的內容，並用別的字串來替代諸如 URL 之類的式樣。有兩種參數可以配置：來源字串及目標字串。Proxy Server 會尋找符合來源字串的文字，並取代目標字串中的文字。此功能僅在反向代理伺服器模式中才有作用。

▼ 建立 URL 重寫式樣

1. **存取 Server Manager，然後按一下 [Filters] 標籤。**
2. **按一下 [Set Content URL Rewriting] 連結。**
   此時會顯示 [Set Content URL Rewriting] 頁面。
3. **從下拉式清單中選取一個資源，或指定常規表示式。**
   如需有關常規表示式的更多資訊，請參閱第 16 章 「管理範本和資源」中的「瞭解常規表示式」。
4. **在 [Source Pattern] 文字方塊中指定來源字串。**
5. **在 [Destination Pattern] 文字方塊中指定目標字串。**
6. **在 [MIME Pattern] 文字方塊中指定內容類型。**
7. **按一下 [OK]。**
8. **按一下 [Restart Required]。**
   此時會顯示 [Apply Changes] 頁面。
9. **按一下 [Restart Proxy Server] 按鈕以套用變更。**

▼ 編輯 URL 重寫式樣

1. **存取 Server Manager，然後按一下 [Filters] 標籤。**
2. **按一下 [Set Content URL Rewriting] 連結。**
   此時會顯示 [Set Content URL Rewriting] 頁面。
3. **按一下您要編輯的 URL 重新寫入式樣旁的 [Edit] 連結。**
4. **按一下 [OK]。**

5 **按一下 [Restart Required]。**
此時會顯示 [Apply Changes] 頁面。

6 **按一下 [Restart Proxy Server] 按鈕以套用變更。**

▼ 刪除 URL 重寫式樣

1 **存取 Server Manager，然後按一下 [Filters] 標籤。**

2 **按一下 [Set Content URL Rewriting] 連結。**
此時會顯示 [Set Content URL Rewriting] 頁面。

3 **按一下您要刪除的 URL 重寫式樣旁的 [Remove] 連結。**
按一下 [OK] 以確認刪除。

4 **按一下 [Restart Required]。**
此時會顯示 [Apply Changes] 頁面。

5 **按一下 [Restart Proxy Server] 按鈕以套用變更。**

限制特定 Web 瀏覽器的存取

您可以依據用戶端 Web 瀏覽器的類型及版本來限制對 Proxy Server 的存取。限制的依據爲所有 Web 瀏覽器在發出請求時，傳送給伺服器的使用者代理程式標頭。

▼ 依據用戶端的 Web 瀏覽器限制對代理伺服器存取

1 **存取 Server Manager，然後按一下 [Filters] 標籤。**

2 **按一下 [Set User-Agent Restriction] 連結。**
此時會顯示 [Set User-Agent Restriction] 頁面。

3 **從下拉式清單選取資源，或鍵入常規表示式，以符合您要 Proxy Server 支援的瀏覽器之使用者代理程式字串。**
如果您希望指定多個用戶端，請用括弧括住常規表示式，並使用 | 字元來分隔多個項目。如需有關常規表示式的更多資訊，請參閱第 16 章 「管理範本和資源」中的「瞭解常規表示式」。

4 **按一下 [Allow Only User-Agents Matching] 選項。**

5 **按一下 [OK]。**

6 **按一下 [Restart Required]。**
此時會顯示 [Apply Changes] 頁面。

7 **按一下 [Restart Proxy Server] 按鈕以套用變更。**

阻斷請求

您可能想要依據上傳內容類型來阻斷檔案上傳及其他請求。

▼ 依據 MIME 類型阻斷請求

1 **存取 Server Manager，然後按一下 [Filters] 標籤。**

2 **按一下 [Set Request Blocking] 連結。**
此時會顯示 [Set Request Blocking] 頁面。

3 **從下拉式清單選取資源，或按一下 [Regular Expression] 按鈕、鍵入常規表示式，然後按一下 [OK]。**

4 **選取您想要的請求阻斷類型。**

- [Disabled] — 停用請求阻斷
- [Multipart MIME (File Upload)] — 阻斷所有檔案上傳
- [MIME Types Matching Regular Expression] — 阻斷符合您鍵入的常規表示式的 MIME 類型請求。如需有關常規表示式的更多資訊，請參閱第 16 章 「管理範本和資源」中的「瞭解常規表示式」。

5 **選擇是要阻斷所有用戶端的請求，還是只阻斷符合您輸入的常規表示式之使用者代理程式的請求。**

6 **選取要阻斷請求的方法。**
選項包括：

- [Any Method With Request Body] — 阻斷所有含請求內文的請求，不論其使用的方法爲何
- 僅適用於：
  - [POST] — 阻斷使用 POST 方法的檔案上傳請求
  - [PUT] — 阻斷使用 PUT 方法的檔案上傳請求

- [Methods Matching Regular Expression] — 阻斷使用所輸入方法的所有檔案上傳請求

7 **按一下 [OK]**。

8 **按一下 [Restart Required]**。
此時會顯示 [Apply Changes] 頁面。

9 **按一下 [Restart Proxy Server] 按鈕以套用變更**。

不列印外寄標頭

您可以配置代理伺服器，使其移除請求中的外寄標頭，這通常是爲了安全性的考量。例如，您可能要防止顯示 From 標頭，因爲此標頭會洩漏使用者的電子郵件地址。或者，您可能要篩選掉使用者代理程式標頭，讓外部伺服器無法得知貴組織使用的 Web 瀏覽器。您也可能想要在將請求轉寄至網際網路之前，移除僅在企業內部網路中使用的記錄或與用戶端相關的標頭。

此功能不會影響經過特別處理的標頭，或由代理伺服器本身產生的標頭，或使協定正常運作的必要標頭，例如 If-Modified-Since 和 Forwarded。

源自代理伺服器的轉寄標頭並不會造成安全性問題。遠端伺服器可以從連線偵測出連線的代理伺服器主機。在代理伺服器鏈中，外部代理伺服器不會列印來自內部代理伺服器的轉寄標頭。如果您不希望向遠端伺服器顯示內部代理伺服器或用戶端主機名稱，我們建議您以此方式設定您的伺服器。

▼ 不列印外寄標頭

1 **存取 Server Manager，然後按一下 [Filters] 標籤**。

2 **按一下 [Suppress Outgoing Headers] 連結**。
此時會顯示 [Suppress Outgoing Headers] 頁面。

3 **在 [Suppress Headers] 文字方塊中，鍵入不要列印的請求標頭清單，並以逗點分隔**。

4 **按一下 [Restart Required]**。
此時會顯示 [Apply Changes] 頁面。

5 **按一下 [Restart Proxy Server] 按鈕以套用變更**。

依 MIME 類型進行篩選

您可以配置代理伺服器，使其阻斷符合 MIME 類型的某些檔案。例如，您可以設定您的代理伺服器，使其阻斷任何可執行檔或二進位檔，如此一來，所有使用您的代理伺服器的用戶端都不會下載到潛在的電腦病毒。

若您要代理伺服器支援新的 MIME 類型，可以在 Server Manager 中選擇 [Preferences] > [Create/Edit MIME]，然後增加類型。如需有關建立 MIME 類型的更多資訊，請參閱第 124 頁的 「建立 MIME 類型」。

您可以將篩選 MIME 類型與範本合併使用，如此一來，只有特定 URL 的某些 MIME 類型會被阻斷。例如，您可以阻斷來自 .edu 網域內任何電腦的可執行檔。

▼ 依 MIME 類型進行篩選

1. **存取 Server Manager，然後按一下 [Filters] 標籤。**
2. **按一下 [Set MIME Filters] 連結。**
   此時會顯示 [Set MIME Filters] 頁面。
3. **選擇要用來篩選 MIME 類型的範本，或者確定您正在編輯整個伺服器。**
4. **您可以在 [Current filter] 文字方塊中鍵入符合要阻斷的 MIME 類型的常規表示式。**
   例如，若要篩選掉所有應用程式，您可以鍵入 **`application/.*`** 做爲常規表示式。這比針對每種應用程式類型來檢查每一 MIME 類型速度要快。常規表示式不區分大小寫。如需有關常規表示式的更多資訊，請參閱第 16 章 「管理範本和資源」中的「瞭解常規表示式」。
5. **核取要篩選的 MIME 類型。**
   當用戶端試圖存取被阻斷的檔案時，代理伺服器會傳回「403 Forbidden」訊息。
6. **按一下 [OK]。**
7. **按一下 [Restart Required]。**
   此時會顯示 [Apply Changes] 頁面。
8. **按一下 [Restart Proxy Server] 按鈕以套用變更。**

依 HTML 標記進行篩選

您可以在傳送檔案至用戶端之前，先指定要篩選掉的 HTML 標記。這個方法可讓您篩選掉內嵌在 HTML 檔案中的物件，例如 Java Applet 及 JavaScript。若要篩選 HTML 標記，請指定開頭和結尾 HTML 標記。如此一來，代理伺服器就會在傳送檔案至用戶端之前，將那些標記內的所有文字和物件都取代成空白。

如果代理伺服器配置爲快取資源，則代理伺服器會將原始 (未編輯) 的檔案儲存在快取記憶體中。

▼ 篩選掉 HTML 標記

1. **存取 Server Manager，然後按一下 [Filters] 標籤。**
2. **按一下 [Set HTML Tag Filters] 連結。**
   此時會顯示 [Set HTML Tag Filters] 頁面。
3. **選擇您要修改的範本。**
   您可以選擇 HTTP，也可以選擇僅指定特定 URL 的範本，例如來自 .edu 網域內主機的 URL。
4. **選取要篩選的預設 HTML 標記。**
   - APPLET 通常包圍著 Java Applet。
   - SCRIPT 指示 JavaScript 程式碼的開頭。
   - IMG 用於指定內嵌影像檔。
5. **您可以鍵入任何要篩選的 HTML 標記。**
   鍵入開頭及結尾的 HTML 標記。

   例如，若要篩選掉表單，可以在 [Start Tag] 方塊中鍵入 **FORM**，並在 [End Tag] 方塊中鍵入 **/FORM**。HTML 標記不區分大小寫。如果您要篩選的標記沒有結尾標記，例如 OBJECT 和 IMG，則可以將 [End Tag] 方塊保留空白。
6. **按一下 [OK]。**
7. **按一下 [Restart Required]。**
   此時會顯示 [Apply Changes] 頁面。
8. **按一下 [Restart Proxy Server] 按鈕以套用變更。**

為內容壓縮配置伺服器

Proxy Server 支援 HTTP 內容壓縮。透過內容壓縮，您可以加快對用戶端的傳送速度，並且可以在不增加硬體費用的情況下提供更高的內容量。內容壓縮縮短了內容的下載時間，使需要撥號與多次連線的使用者明顯受益。

透過內容壓縮，您的 Proxy Server 可以傳送壓縮過的資料，並指示瀏覽器即時將資料解壓縮。壓縮可以減少傳送的資料量，並加快頁面顯示速度。

將伺服器配置為依需要壓縮內容

您可以將 Proxy Server 配置爲即時壓縮傳輸資料。動態產生的 HTML 頁面只有在使用者提出請求時才會存在。

▼ 將伺服器配置為依需要壓縮內容

1. **存取 Server Manager，然後按一下 [Filters] 標籤。**
2. **按一下 [Compress Content on Demand] 連結。**
   此時會顯示 [Compress Content on Demand] 頁面。
3. **從下拉式清單中選取資源，或鍵入常規表示式。**
   如需有關常規表示式的更多資訊，請參閱第 16 章 「管理範本和資源」中的「瞭解常規表示式」。
4. **指定下列資訊：**
   - **Activate Compress Content on Demand?** 選擇伺服器是否應該爲選取的資源提供預先壓縮的內容。
   - **Vary Header**。指定是否插入 Vary: Accept-encoding 標頭。選取 [yes] 或 [no]。若設定爲 [yes]，則當選取檔案的壓縮版本時，一律會插入 Vary: Accept-encoding 標頭。

     如果設定爲 no，則永遠不會插入 Vary: Accept-encoding 標頭。

     依預設，該值設定爲 yes。
   - **Fragment Size**。指定壓縮程式庫 (`zlib`) 使用的記憶體分段大小 (以位元組爲單位)，以控制每次要壓縮的內容量。預設值爲 8096。
   - **Compression Level**。指定壓縮的層級。選擇 1 至 9 之間的值。數值 1 會產生最快的速度；數值 9 產生最佳壓縮效果。預設值爲 6，在速度和壓縮效果上比較適中。
5. **按一下 [OK]。**
6. **按一下 [Restart Required]。**
   此時會顯示 [Apply Changes] 頁面。

7 按一下 [Restart Proxy Server] 按鈕以套用變更。

◆ ◆ ◆ 第 14 章

使用反向代理伺服器

本章說明將 Proxy Server 當成反向代理伺服器使用的方式。反向代理伺服器可用於防火牆之外，以做爲外部用戶端的安全內容伺服器，避免在未受監視的情況下，從公司外部直接存取您的伺服器資料。反向代理伺服器也能用於複製；也就是說，可以將多部代理伺服器連接於使用頻繁的伺服器之前，以發揮負載平衡之功效。本章說明將 Proxy Server 用於防火牆內外部的替代方法。

本章包含下列小節：

反向代理的運作方式

您可以使用兩種不同的方法，來進行反向代理。第一種方法是利用 Proxy Server 的安全性功能來處理作業事件。第二種方法是利用快取在使用頻繁的伺服器上提供負載平衡功能。這兩種方法不限於在防火牆上運作，因此其使用方法與傳統的代理伺服器不同。

做為替代伺服器的代理伺服器

如果您的內容伺服器上有必須妥善保護的機密資訊，如信用卡號資料庫等，您可以在防火牆外設置代理伺服器做爲內容伺服器的替代伺服器。當外部用戶端嘗試存取內容伺服器時，就會被改送至代理伺服器，而內容伺服器上眞正的內容則會安全地保留在防火牆內。代理伺服器位於防火牆之外，而用戶端會將其視爲內容伺服器。

當用戶端對網站提出請求時，該請求會被送至代理伺服器。接著代理伺服器會經由防火牆的特定通道，將用戶端的請求傳送至內容伺服器。內容伺服器會經由通道將結果送回代理伺服器。代理伺服器會將所擷取的資訊傳送至用戶端，就像代理伺服器是實際的內容伺服器一般，如圖 14–1 所示。若內容伺服器傳回錯誤訊息，則代理伺服器可

截取訊息，並在將訊息傳送至用戶端之前，變更標頭所列的任何 URL。此運作方式可防止外部用戶端取得連結至內部內容伺服器的重新導向 URL。

代理伺服器以這種方式，在安全的資料庫和可能的惡意攻擊之間多加一道屏障。即使攻擊成功 (雖然不太可能)，攻擊者所能擷取的內容也很可能僅限於單一作業事件的資訊，不太可能取得整個資料庫的存取權。未經授權的使用者無法進入實際的內容伺服器，因爲防火牆通道僅允許代理伺服器存取實際的內容伺服器。

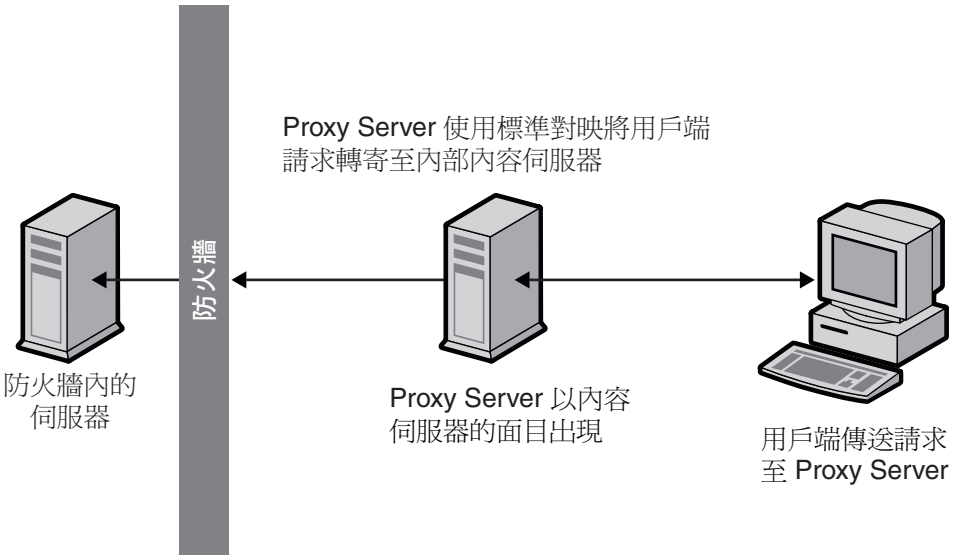


圖 14–1 反向代理伺服器的程序

您可以對防火牆路由器進行配置，允許特定連接埠上的特定伺服器 (在此例中是指其指定連接埠上的代理伺服器) 取得通過防火牆的存取權，但不允許其他機器出入防火牆。

安全的反向代理

當代理伺服器和其他機器之間有一或多個連線採用安全通訊端層 (SSL) 協定來加密資料時，就能確保安全的反向代理。

安全的反向代理有多種用途：

- 爲防火牆外的代理伺服器與防火牆內的安全內容伺服器之間，提供加密的連線
- 讓用戶端以安全的方式連線至代理伺服器，增強資訊 (如信用卡號) 傳輸的安全性

安全的反向代理會因資料加密時需要經常性耗用時間，而使每個安全連線的速度減緩。不過，因 SSL 提供快取機制，連線的雙方可重複使用先前所協議的安全性參數，而大幅縮短後續連線的經常性耗用時間。

三種配置安全反向代理伺服器的方法如下：

- **用戶端與代理伺服器之間的安全連線**。如果代理伺服器和內容伺服器之間所交換的資訊，不太可能或不可能遭未經授權的使用者存取 (如下圖所示)，則這個方案就很有用。

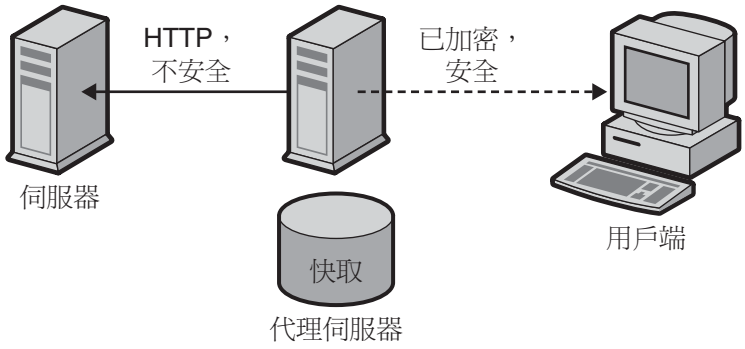


圖 14–2 用戶端與代理伺服器之間的安全連線

- **代理伺服器與內容伺服器之間的安全連線**。如果您的用戶端位於防火牆內部，而內容伺服器位於防火牆外部，則這個方案就很有用。在此方案中，您的代理伺服器可做爲網站之間的安全通道，如下圖所示。

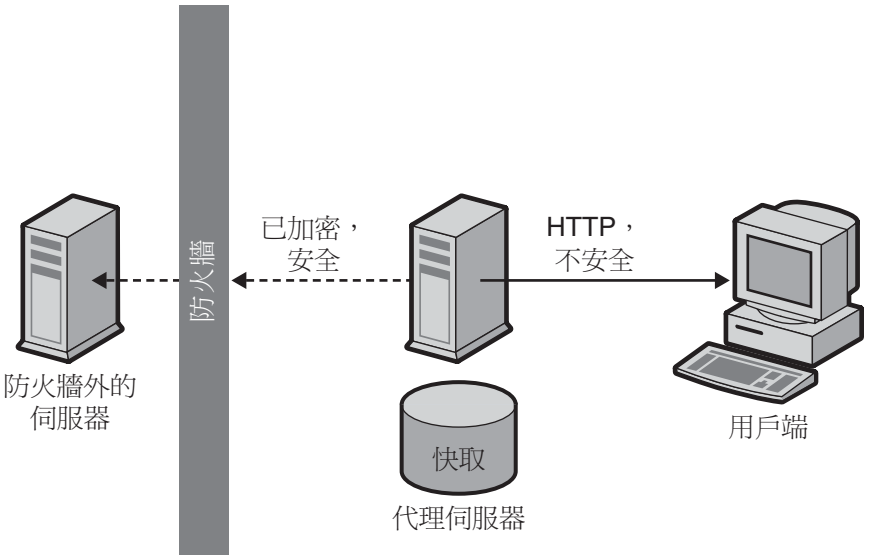


圖 14–3 代理伺服器與內容伺服器之間的安全連線

- **用戶端與代理伺服器以及代理伺服器與內容伺服器之間的安全連線**。如果伺服器、代理伺服器和用戶端之間所交換的資訊都需要保密，則這個方案就很有用。在此方案中，您的代理伺服器由於有用戶端認證提供額外的安全性，因此能做爲網站之間的安全通道，如下圖所示。

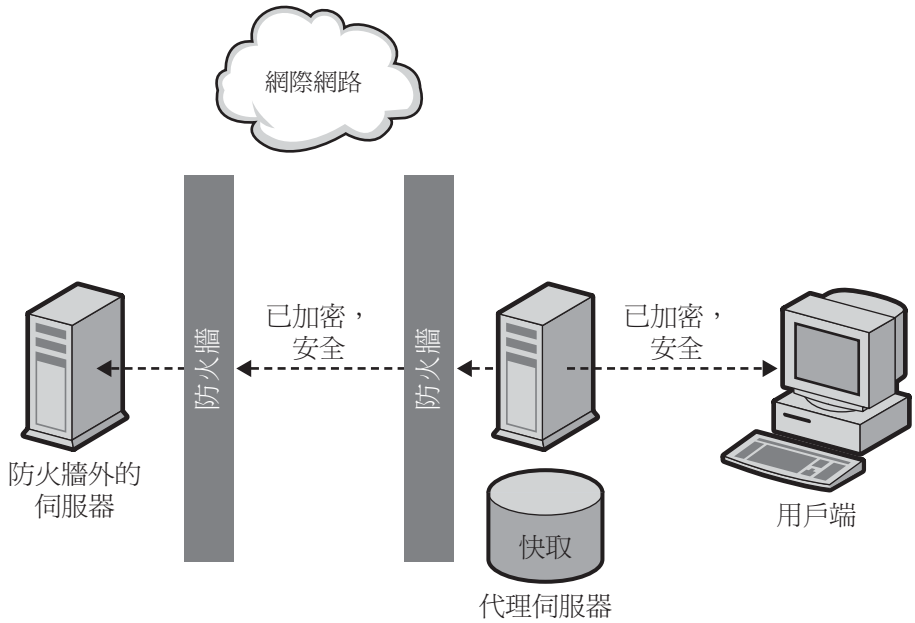


圖 14–4 用戶端與代理伺服器以及代理伺服器與內容伺服器之間的安全連線

如需有關如何設定各項配置的資訊，請參閱第 288 頁的 「設定反向代理伺服器」。

除了 SSL 之外，代理伺服器也可以使用用戶端認證，此認證要求向代理伺服器提出請求的電腦提供憑證或其他形式的識別以驗證其身分。

用於負載平衡的代理

您可以在組織內使用多部代理伺服器，以平衡 Web 伺服器之間的網路負載。此模型利用 Proxy Server 的快取功能來建立伺服器池，以進行負載平衡。在此例中，代理伺服器可以位於防火牆的任一側。若您的 Web 伺服器每天都會收到大量請求，則可以利用代理伺服器來分擔 Web 伺服器的負載，以提高網路存取的效率。

代理伺服器相當於用戶端請求與眞實伺服器之間的媒介。代理伺服器會快取所請求的文件。若您有一部以上的代理伺服器，DNS 可以「循環」選取請求的 IP 位址，對各項請求進行隨機路由。用戶端每次都使用相同的 URL，但是每次請求所採取的路由可能每次都透過不同的代理伺服器。

使用多部代理伺服器來處理傳送至使用頻繁的內容伺服器之請求的優點是，伺服器可以更有效率的方式處理更大的負載，這是單一代理伺服器無法比擬的。代理伺服器在初次啓動期間會從內容伺服器擷取文件，之後傳送至內容伺服器的請求數量就會大幅減少。

只有 CGI 請求和偶而發生的新請求才必須送至內容伺服器。其餘請求都可由代理伺服器來處理。例如，假設傳送至伺服器的請求中有 90% 都不是 CGI 請求，表示您可以快取這些請求，而您的內容伺服器每天會接收 2 百萬次點閱。在此情況下，若您連接三部反向代理伺服器，而每部每天可處理 2 百萬次點閱，那麼每天總共可接收 6 百萬次點閱。至於每天從每部代理伺服器傳送至內容伺服器的 10% 請求約爲 20 萬次點閱，表示總點閱次數只有 60 萬次，如此自然可以大幅提升處理效率。點閱次數可以從大約 2 百萬次增加爲 6 百萬次，而內容伺服器的負載則相對從 2 百萬次減少爲 60 萬次。但實際的結果會依照您的狀況而有所不同。

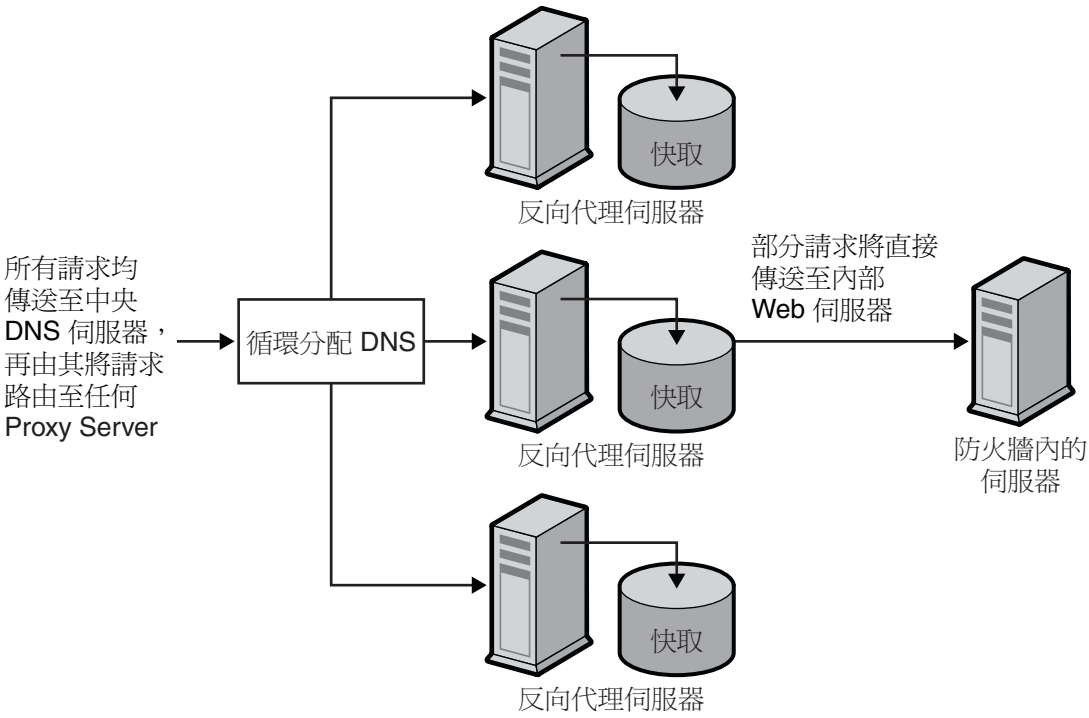


圖 14–5 用於負載平衡的代理伺服器

設定反向代理伺服器

若要設定反向代理伺服器，則需要兩種對映：標準對映和反向對映。

- 標準對映會將請求重新導向至內容伺服器。當用戶端向代理伺服器請求文件時，代理伺服器會需要標準對映告知實際文件的取得位置。

注意 – 請勿將反向代理伺服器和提供自動配置檔案的代理伺服器一起使用，因爲代理伺服器可能會傳回錯誤的結果。

- 反向對映會指示代理伺服器針對從內容伺服器傳來的重新導向設置陷阱。代理伺服器會截取重新導向，然後變更重新導向的 URL 以對映到代理伺服器。例如，若用戶端所請求的文件已經移動或是找不到，則內容伺服器會將訊息傳回至用戶端，說明在所請求的 URL 上找不到文件。在傳回的訊息中，內容伺服器會增加 HTTP 標頭，列出要用來取得已移動檔案的 URL。爲維護內部內容伺服器的私密性，代理伺服器可以使用反向對映以重新導向 URL。

假設您有一部名爲 `http://http.site.com/` 的 Web 伺服器，而您要爲這部 Web 伺服器設定反向代理伺服器。您可以將反向代理伺服器稱爲 `http://proxy.site.com/`。

▼ 建立標準或反向對映

1 **存取 Server Manager，然後按一下 [URL] 標籤。**

2 **按一下 [Create Mapping] 連結。**
這時會顯示 [Create Mapping] 頁面。

3 **在所出現的頁面中，提供標準對映的來源前綴和來源目標，**
例如，

來源前綴：`http://proxy.site.com`

來源目標：`http://http.site.com/`

4 **按一下 [OK]。**
返回頁面並建立反向對映，例如，

反向對映：

來源前綴：`http://http.site.com/`

來源目標：`http://proxy.site.com/`

5 **若要變更，請按一下 [OK]。**
當您按下 [OK] 按鈕時，代理伺服器就會增加一或多個附加對映。若要查看對映，請按一下 [View/Edit Mappings] 連結。附加對映的格式如下：

from: `/`

to: `http://http.site.com/`

這些附加的自動對映，適用於將反向代理伺服器當作一般伺服器連線的使用者。第一個對映用來擷取連線至反向代理伺服器以做爲標準代理伺服器的使用者。只有當使用者未變更由管理 GUI 自動提供之 [Map Source Prefix] 文字方塊的內容時，才會增加「/」對映。依據設定，通常只需要第二個對映，但是額外的對映並不會導致代理伺服器發生問題。

備註 – 若 Web 伺服器具有多個 DNS 別名，則每個別名都必須具有對應的標準對映。若 Web 伺服器以其自身的數個 DNS 別名產生重新導向，則每個別名都應有一個對應的反向對映。

CGI 應用程式仍在原始伺服器上執行。代理伺服器本身決不會執行 CGI 應用程式。然而，若 CGI 程序檔指出，可發出 Last-modified 或 Expires 標頭暗示非零的存留時間以快取結果，則代理伺服器將會快取結果。

撰寫 Web 伺服器的內容時，請記住內容也是由反向代理伺服器提供服務的，因此 Web 伺服器上的所有檔案連結都應該是相對連結。請勿在 HTML 檔案中參照主機名稱。所有連結必須只包含頁面：

```
/abc/def
```

而非完全合格的主機名稱，如：

```
http://http.site.com/abc/def
```

備註 – 您可以針對在反向代理伺服器模式中所發生的錯誤，提供自訂的錯誤頁面。這些錯誤頁面會置換代理伺服器所產生的錯誤。這樣可以防止用戶端得知您已配置代理伺服器。

設定安全的反向代理伺服器

設定安全的反向代理之前，您必須先熟悉數位憑證、憑證授權單位和認證。

設定安全的反向代理伺服器和設定不安全的反向代理伺服器，操作大致相同。唯一的差別是您必須爲要加密的檔案，指定 HTTPS 做爲通訊協定。

用戶端與代理伺服器之間的安全連線

這個程序說明如何根據您所選擇的配置方案，設定安全的反向代理伺服器。下面示範對映的設定方式，這些說明假設您有一部名爲 `http.site.com` 的 Web 伺服器，而您要設定名爲 `proxy.site.com` 的安全反向代理伺服器。當您執行這些步驟時，請以您的 Web 伺服器和代理伺服器的名稱，取代指示中所使用的範例名稱。

▼ 設定用戶端與代理伺服器之間安全連線的對映

1. **存取 Server Manager，然後按一下 [URL] 標籤。**
2. **按一下 [Create Mapping] 連結。**
   這時會顯示 [Create Mapping] 頁面。
3. **在所出現的頁面上，以下列方式設定標準對映和反向對映：**
   標準對映：

   來源前綴：`https://proxy.mysite.com`

   來源目標：`http://http.mysite.com/`

   反向對映：

   來源前綴：`http://http.mysite.com/`

   來源目標：`https://proxy.mysite.com/`
4. **儲存並套用變更。**
   若要查看您剛才所建立的對映，請按一下 [View/Edit Mappings] 連結。

備註 – 您的代理伺服器必須在安全模式下運作，這項配置才會有作用。換句話說，必須啓用加密，且必須從指令行重新啓動代理伺服器。若要從指令行重新啓動代理伺服器，請移至代理伺服器目錄並鍵入 **`./start`**。

▼ 設定代理伺服器與內容伺服器之間安全連線的對映

1. **存取 Server Manager，然後按一下 [URL] 標籤。**
2. **按一下 [Create Mapping] 連結。**
   這時會顯示 [Create Mapping] 頁面。
3. **在所出現的頁面上，以下列方式設定標準對映和反向對映：**
   標準對映：

   來源前綴：`http://proxy.mysite.com`

   來源目標：`https://http.mysite.com/`

   反向對映：

   來源前綴：`https://http.mysite.com/`

   來源目標：`http://proxy.mysite.com/`

4 **儲存並套用變更**。
若要查看您剛才所建立的對映，請按一下名爲 [View/Edit Mappings] 的連結。

備註 – 您的內容伺服器必須在安全模式下運作，這項配置才會有作用。

▼ 設定用戶端與代理伺服器之間以及代理伺服器與內容伺服器之間的安全連線

1 **存取 Server Manager，然後按一下 [URL] 標籤**。

2 **按一下 [Create Mapping] 連結**。
這時會顯示 [Create Mapping] 頁面。

3 **在所出現的頁面上，以下列方式設定標準對映和反向對映：**
標準對映：

來源前綴：`https://proxy.mysite.com`

來源目標：`https://http.mysite.com/`

反向對映：

來源前綴：`https://http.mysite.com/`

來源目標：`https://proxy.mysite.com/`

4 **儲存並套用變更**。
若要查看您剛才所建立的對映，請按一下名爲 [View/Edit Mappings] 的連結。

備註 – 您的代理伺服器和內容伺服器必須在安全模式下運作，這項配置才會有作用。換句話說，必須對代理伺服器啓用加密，且必須從指令行重新啓動代理伺服器。若要從指令行重新啓動代理伺服器，請移至代理伺服器目錄並鍵入 **`./restart`**。

停用反向代理伺服器設定中的正向代理功能

當將 Proxy Server 配置爲反向代理伺服器時，依預設，它不會停止正向代理伺服器的作用。這樣的伺服器實例既接受反向代理請求又接受正向代理請求，並爲其提供服務。需要進一步配置才能停用正向代理功能。您可以設定 ACL 配置，拒絕 URI 符合正向代理格式的請求。您可以使用用戶端指令來達到這個目的：

```
<Client uri="http://.*">
PathCheck fn="check-acl" acl="http://.*"
<Client>
.
```

```
.
.
The "http://.*" ACL can be a deny all ACL as follows:
.
.
acl "http://.*";
deny (all) user="anyone";
```

反向代理伺服器中的虛擬多重主機

虛擬多重主機可以讓原始伺服器，如反向代理伺服器，回應多個 DNS 別名，如同在每個位址上安裝了不同的伺服器。舉例來說，假設您的 DNS 主機名稱爲：

- www
- specs
- phones

這三個主機名稱都可對映至相同的 IP 位址，即反向代理伺服器的 IP 位址。接著反向代理伺服器可依據存取其本身時所使用的 DNS 名稱，而做出不同的回應。

另外，虛擬多重主機也能讓您在單一反向代理伺服器中，放置多個不同的 *網域*。例如：

- www.domain-1.com
- www.domain-2.com
- www.domain-3.com

您可以將多個本地主機名稱和多個網域組合在單一代理伺服器中：

- www
- specs
- phones
- www.domain-1.com
- www.domain-2.com
- www.domain-3.com

虛擬多重主機功能的詳細資訊

虛擬多重主機的運作方式，是指定 DNS 主機和網域名稱或別名，然後再指定傳送至該主機名稱的請求，所應導向的目標 URL 前綴。舉例來說，假設您有兩個對映：

- engr.domain.com -> http://int-engr.domain.com
- mktg.domain.com -> http://int-mktg.domain.com

對映不一定是從根目錄到根目錄。您可以在目標 URL 中指定附加的 URL 路徑前綴：

- engr.domain.com -> http://internal.domain.com/engr
- mktg.domain.com -> http://internal.domain.com/mktg

這同樣適用於虛擬網域對映。例如，您可以使用：

- `www.domain-1.com -> http://int-engr.domain.com`
- `www.domain-2.com -> http://int-mktg.domain.com`

系統會查看 HTTP「Host:」標頭。系統會根據該標頭，選擇相符的虛擬多重主機對映。如果沒有相符的多重主機對映，伺服器會依據對映出現在配置檔案中的順序繼續查看其他對映。如果仍找不到相符的對映，伺服器將不執行對映。如果找不到相符的對映，代理伺服器通常會發出「代理拒絕執行請求」的回應。

▼ 配置虛擬多重主機功能

1. **存取 Server Manager，然後按一下 [URL] 標籤。**
2. **按一下 [Configure Virtual Multihosting] 連結。**
   這時會顯示 [Configure Virtual Multihosting] 頁面。
3. **在 [Source Hostname (alias)] 欄位中，指定要套用此對映的本地主機名稱 (或 DNS 別名)。**
4. **在 [Source Domain Name] 欄位中，鍵入應套用此對映的本機網域名稱。**
   一般而言，這個名稱是您網路的網域名稱，除非您要針對多個不同的 DNS 網域使用多重主機。
5. **在 [Destination URL Prefix] 欄位中，鍵入當主機和網域名稱與上述規格相符時，要將請求導向至的目標 URL 前綴。**
6. **若您使用範本，請在 [Use This Template] 下拉式清單中選擇範本名稱，若您不想套用範本，則將此值保留為 NONE。**
7. **按一下 [OK]。**
8. **按一下 [Restart Required]。**
   此時會顯示 [Apply Changes] 頁面。
9. **按一下 [Restart Proxy Server] 按鈕以套用變更。**
   針對您要建立的每個虛擬多重主機對映，重複執行上述步驟。

   所有虛擬多重主機對映都會出現在 [Configure Virtual Multihosting] 頁面的底端。[Source Hostname (alias)] 和 [Source Domain Name] 欄位以及代理伺服器的連接埠號會合併起來，成爲單一的常規表示式，以用來比對「主機：」標頭。

   例如，若您的主機名稱爲 `www`，網域爲 `example.com`，連接埠號爲 8080，則會出現下列常規表示式：

   ```
   www(|.example.com)(|:8080)
   ```

此常規表示式保證與使用者可能鍵入的下列所有可能組合，或用戶端可能傳送的下列所有可能組合相符。即使該連接埠號並非 80，有些用戶端軟體仍可能加以省略，因爲伺服器已經在該連接埠上進行偵聽。

- `www`
- `www:8080`
- `www.example.com`
- `www.example.com:8080`

虛擬多重主機功能的相關說明

- 在配置反向代理伺服器對映之前，您必須先停用用戶端自動配置功能。用戶端自動配置功能適用於正向代理伺服器作業，而非反向代理伺服器。
- 虛擬多重主機功能會建立自動反向對映。請勿針對使用 [Virtual Multihosting] 頁面所提供的對映建立反向對映。
- 虛擬對映是以 `obj.conf` 檔案中的 `virt-map` 函數指定。
- 虛擬對映是依據 `obj.conf` 配置檔案中所指定的順序進行比對。若標準對映、反向對映、常規表示式對映或用戶端自動配置對映出現在虛擬對映之前，則會優先套用這些對映。同樣地，若未在虛擬對映中找到相符對映，則會繼續對 `obj.conf` 中虛擬對映區段之後的下一個對映進行轉換。

  備註 – 依照規格的順序，反向對映應出現在其他對映之前。

- 若代理伺服器的連接埠號有所變更，則必須重新建立虛擬多重主機對映，以採用新的連接埠號。

◆ ◆ ◆ 第 15 章

15 使用 SOCKS

本章說明如何配置並使用 Sun Java System Web Proxy Server 所附的 SOCKS 伺服器。Proxy Server 支援 SOCKS 版本 4 和 5。

本章包含下列小節：

關於 SOCKS

SOCKS 是一種網路代理伺服器協定，可將 SOCKS 伺服器另一端主機所傳來的連線請求予以重新導向，讓一端的主機無需直接連線至 IP，就能完全存取另一端主機。SOCKS 通常用來當做網路防火牆，讓 SOCKS 伺服器之後的主機能夠完全存取網際網路，同時防止他人在未經授權的情況下，經由網際網路存取內部主機。

SOCKS 伺服器爲通用的防火牆常駐程式，以點對點的方式控制通過防火牆的存取。SOCKS 伺服器會認證並授權請求、建立代理伺服器連線並轉送資料。SOCKS 伺服器是在網路層級而非應用程式層級上運作，因此不識別用於傳輸請求的協定或方法。由於 SOCKS 伺服器不識別這些協定，因此可用來傳送不受 Proxy Server 支援的協定，如 Telnet。

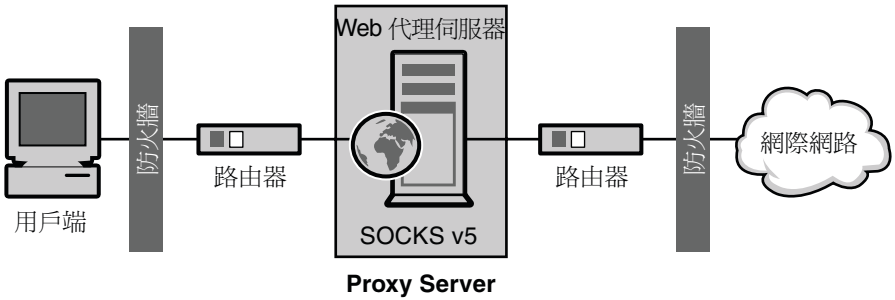


圖 15–1 SOCKS 伺服器在網路中的位置

使用隨附的 SOCKS v5 伺服器

Sun Java System Web Proxy Server 包含本身的 SOCKS 常駐程式，可瞭解其他 SOCKS 常駐程式所使用的標準 `socks5.conf` 檔案格式。Proxy Server 可以使用此常駐程式來路由請求，或是執行此常駐程式，爲網路提供附加功能。如需有關配置 Proxy Server，以透過 SOCKS 伺服器路由請求的更多資訊，請參閱第 307 頁的 「配置路由項目」。

Proxy Server 隨附的 SOCKS 常駐程式依預設爲停用狀態。您可以從 Server Manager 介面的 [SOCKS] 標籤或指令行，啓用此常駐程式。如需更多資訊，請參閱第 300 頁的 「啓動並停止 SOCKS v5 伺服器」。

備註 – 在 Proxy Server 4 中，SOCKS 常駐程式的名稱已從 `ns-sockd` 變更爲 `sockd`。

爲使用 Proxy Server 隨附的 SOCKS 伺服器，必須採取下列完整步驟：

▼ 使用 SOCKS

1. **配置 SOCKS 伺服器。請參閱第 300 頁的 「配置 SOCKS v5 伺服器」。**
2. **若 SOCKS 伺服器會執行於具有多重介面的電腦上，請建立 SOCKS 路由項目。請參閱第 307 頁的 「配置路由項目」。**
3. **建立認證項目。請參閱第 302 頁的 「配置 SOCKS v5 認證項目」。**
4. **建立連線項目。請參閱第 304 頁的 「配置 SOCKS v5 連線項目」。**
5. **啓用 SOCKS 伺服器。請參閱第 300 頁的 「啓動並停止 SOCKS v5 伺服器」。**

關於 socks5.conf

Sun Java System Web Proxy Server 使用 `socks5.conf` 檔案來控制對 SOCKS 伺服器及其服務的存取。每個項目都定義當收到與該項目相符的請求時，Proxy Server 會採取什麼行動。在 Server Manager 中所做的選擇會寫入 `socks5.conf`。此檔案也能以手動方式加以編輯。`socks5.conf` 檔案位於安裝根目錄 *server-root*，如下所示：

server-root`/proxy-`*serverid*`/config` 目錄

本小節提供和 `socks5.conf` 有關的一般資訊。如需有關該檔案、其指令和語法的詳細資訊，請參閱「Proxy Server *Configuration File Reference*」。

認證

可將 SOCKS 常駐程式配置爲需經過認證才能使用其服務。認證是基於連線用戶端的主機名稱和連接埠。若您選擇需要使用者名稱和密碼，則會根據 `socks5.conf` 檔案所參照的使用者名稱和密碼檔案，對這些資訊加以認證。如果所提供的使用者名稱和密碼不同於密碼檔案所列項目，則會拒絕存取。密碼檔案中的使用者名稱和密碼格式爲**使用者名稱 密碼**，使用者名稱和密碼之間並以空格區隔。

您也可以禁止使用者。若要要求使用者名稱和密碼認證，必須將 `SOCKS5_PWDFILE` 指令增加到 `socks5.conf` 中。如需有關指令及其語法的更多資訊，請參閱「Proxy Server *Configuration File Reference*」中的 `socks5.conf` 部分。

使用者名稱與密碼認證也可以依據配置的LDAP 伺服器而不僅是檔案來執行。

存取控制

存取控制是使用 `socks5.conf` 檔案中的一組有序行來執行的。每行中包含一個指令，用於允許或拒絕對資源的存取。處理指令時，會依照這些指令在配置檔案中的順序依次處理。不符合任何允許指令的請求，其存取權都會遭到拒絕。

記錄

SOCKS 常駐程式會將錯誤和存取訊息記錄在 SOCKS 記錄檔中。記錄檔的位置和記錄類型可在 `socks5.conf` 中加以指定。

SOCKS 常駐程式也會每小時產生統計項目，爲常駐程式提供統計。

調校

您可以使用 `socks5.conf` 檔案來決定 SOCKS 伺服器所使用的工作執行緒和接受執行緒數量。此數量會影響 SOCKS 伺服器的效能。

如需有關工作執行緒和接受執行緒設定及其對效能之影響的更多資訊，請參閱第 300 頁的「配置 SOCKS v5 伺服器」中的相關章節。

啓動並停止 SOCKS v5 伺服器

SOCKS 伺服器可從 Server Manager 或從指令行啓動和停止。

▼ 從 Server Manager 啓動或停止 SOCKS 伺服器

1. **從 Server Manager 存取伺服器實例，然後按一下 [SOCKS] 標籤。**
2. **按一下 [Start/Stop SOCKS] 連結。**
3. **啓動或停止 SOCKS 伺服器。**

從指令行啓動和停止 SOCKS 伺服器

執行在 *server-root*/proxy- *serverid* 目錄中找到的程序檔，其中 *server-root* 是安裝根目錄：

- `start-sockd` 啓動 SOCKS 常駐程式
- `stop-sockd` 停止 SOCKS 常駐程式
- `restart-sockd` 重新啓動 SOCKS 常駐程式

配置 SOCKS v5 伺服器

▼ 配置 SOCKS 伺服器

1. **從 Server Manager 存取伺服器實例，然後按一下 [SOCKS] 標籤。**
2. **按一下 [Configure SOCKS v5] 連結。**
3. **在 [SOCKS Port] 欄位中，鍵入 SOCKS 伺服器所要偵聽的連接埠號。預設為 1080。**
4. **選取您要使用的 SOCKS 選項。**

   下列爲可用的選項：

   - *Disable Reverse DNS Lookup*。停用 SOCKS 伺服器的反向 DNS 查找。反向 DNS 會將 IP 位址轉譯爲主機名稱。停用反向 DNS 查找可以節省網路資源。DNS 查找依預設爲停用狀態。在停用反向 DNS 查找的狀態下，若以主機名稱請求 URL，則伺服器不會將主機名稱對映至 IP 位址。若啓用反向 DNS 查找，則伺服器會執行對映，SOCKS 記錄檔中也會增加一個項目，以列出此 DNS 轉譯事件。

- **Use Client-specific Bind Port**。允許用戶端在 BIND 請求中指定連接埠。若停用此選項，SOCKS 會忽略用戶端所請求的連接埠，並隨機指定連接埠。此選項依預設爲停用狀態。
- **Allow** *Wildcard As Bind IP Address*。允許用戶端在 BIND 請求中，指定全都是零 (0.0.0.0) 的 IP 位址，表示任何 IP 位址都能連線。在停用此選項的情況下，用戶端必須指定要連線至連結連接埠的 IP 位址，而 SOCKS 伺服器會拒絕連結至 0.0.0.0 的請求。此選項依預設爲停用狀態。
- *Quench Updates*。停用每小時一次的自動統計檔案寫入。若停用此選項，則會在每次請求時寫入。如需更多資訊，請參閱第 299 頁的 「記錄」。

[Quench Updates] 元素會顯示在使用者介面上，但是此 Proxy Server 4 發行版本未實作此功能。

5 在 [Log File] 欄位中，鍵入 SOCKS 記錄檔的完整路徑名稱。

預設爲 *server-root*/proxy- *serverid*/logs/socks5.log。

6 從 [Log Level] 下拉式清單中，選取記錄檔是應該只包含警告與錯誤、包含所有請求，或是包含除錯訊息。

7 選取 RFC 1413 ident 回應。

Ident 允許 SOCKS 伺服器決定用戶端的使用者名稱。一般而言，這項功能只有在用戶端執行特定版本的 UNIX 時才會有作用。可供使用的項目如下

- **Don't Ask**。絕對不要使用 ident 來決定用戶端的使用者名稱。這是建議使用的預設設定。
  - **Ask But Don't Require**。詢問所有用戶端的使用者名稱但不加以要求。此選項僅將 ident 用於記錄用途。
  - **Require**。詢問所有用戶端的使用者名稱，只允許傳送有效回應的用戶端進行存取。

8 在 [SOCKS Tuning] 區段中，指定 SOCKS 伺服器應該使用的工作執行緒和接受執行緒數量。這些數量會影響 SOCKS 伺服器的效能。按一下 [OK]。

- **Number Of Worker Threads**。預設值是 40。若 SOCKS 伺服器速度太慢，請增加工作執行緒數量。若伺服器不穩定，請減少數量。變更此數量時，一開始先採用預設值，並視需要進行增減。工作執行緒的數量通常介於 10 到 150 之間，絕對最大值是 512，但是超過 150 後容易造成浪費和不穩定。
  - **Number Of Posted Accepts**。預設值是 1。若 SOCKS 伺服器斷線，請增加接受執行緒的數量。如果伺服器不穩定，請減少伺服器數量。變更此數量時，一開始先採用預設值，並視需要進行增減。接受執行緒的數量通常介於 1 到 10 之間，絕對最大值是 512，但是超過 60 後容易造成浪費和不穩定。當 SOCKS 伺服器欠載且連線中斷，並因而造成請求失敗時，請調校此設定。

配置 SOCKS v5 認證項目

SOCKS 認證項目會識別 SOCKS 常駐程式應接受來自哪些主機的連線，以及 SOCKS 常駐程式應使用何種認證類型來認證這些主機。

▼ 建立 SOCKS 認證項目

1. **從 Server Manager 存取伺服器實例，然後按一下 [SOCKS] 標籤。**
2. **按一下 [Set SOCKS v5 Authentication] 連結。**
3. **按一下 [Add] 按鈕。**
4. **在 [Host Mask] 欄位中，鍵入 SOCKS 伺服器要認證的主機之 IP 位址或主機名稱。**

   若您鍵入 IP 位址，請在位址後面加上正斜線，以及要套用至內送 IP 位址的遮罩。SOCKS 伺服器會將此遮罩套用至 IP 位址，以確定是否爲有效主機。主機遮罩項目中請勿使用空格。若您未鍵入主機遮罩，則認證項目會套用至所有主機。

   例如，您可以在主機遮罩欄位中鍵入 155.25.0.0/255.255.0.0。若主機的 IP 位址是 155.25.3.5，SOCKS 伺服器會將遮罩套用至此 IP 位址，然後確定主機的 IP 位址符合認證記錄所適用的 IP 位址 (155.25.0.0)。
5. **在 [Port Range] 欄位中，鍵入 SOCKS 伺服器要認證之主機上的連接埠。**

   連接埠範圍項目中請勿使用空格。若您未提供連接埠範圍，則認證項目會套用至所有連接埠。

   您可以使用方括號 [ ] 以包含兩端的連接埠，或是使用括弧 ( ) 以排除兩端的連接埠。例如，[1000-1010] 表示這兩個數值之間的所有連接埠號，包括 1000 和 1010，而 (1000-1010) 則表示這兩個數值之間的所有連接埠號，但是不包括 1000 和 1010。您也可以混合使用方括號和括弧。例如，(1000-1010] 表示 1000 和 1010 之間的所有號碼，不包括 1000，但包括 1010。
6. **在 [Authentication Type] 下拉式清單中，選取認證類型。**

   下列爲可用的選項：

   - **Require user-password**。存取 SOCKS 伺服器時，需要使用者名稱和密碼。
   - **User-password, if available**。如果有可供使用的使用者名稱和密碼，則應用來存取 SOCKS 伺服器，但它們並非存取所必需。
   - **Ban**。禁止使用 SOCKS 伺服器。
   - **None**。存取 SOCKS 伺服器時不需要認證。

7 **從 [Insert] 下拉式清單中，選取這個項目在 `socks5.conf` 檔案中的位置，然後按一下 [OK]。**

因爲認證方法可以有多種，因此您必須指定對這些方法的評估順序。因此，若用戶端不支援列出的第一種認證方法，則會使用第二種方法。若用戶端不支援列出的所有認證方法，SOCKS 伺服器會結束連線而不接受請求。

▼ 編輯認證項目

1 **從 Server Manager 存取伺服器實例，然後按一下 [SOCKS] 標籤。**

2 **按一下 [Set SOCKS v5 Authentication] 連結。**

3 **選取您要編輯的認證項目，然後按一下 [Edit] 按鈕。**

4 **視需要進行變更。**

5 **按一下 [OK]。**

▼ 刪除認證項目

1 **從 Server Manager 存取伺服器實例，然後按一下 [SOCKS] 標籤。**

2 **按一下 [Set SOCKS v5 Authentication] 連結。**

3 **選取您要刪除的認證項目。**

4 **按一下 [Delete] 按鈕。**

▼ 移動認證項目

對項目的評估順序是依照它們在 `socks5.conf` 檔案中出現的順序。您可以移動這些項目以變更順序。

1 **從 Server Manager 存取伺服器實例，然後按一下 [SOCKS] 標籤。**

2 **按一下 [Set SOCKS v5 Authentication] 連結。**

3 **選取您要移動的認證項目，然後按一下 [Move] 按鈕。**

4 **在 [Move] 下拉式清單中，選取該項目在 `socks5.conf` 檔案中的位置。**

5 **按一下 [OK]。**

配置 SOCKS v5 連線項目

SOCKS 連線項目會指定 SOCKS 常駐程式應允許還是拒絕請求。

▼ 建立連線項目

1 **從 Server Manager 存取伺服器實例，然後按一下 [SOCKS] 標籤。**

2 **建立 [Set SOCKS v5 Connections] 連結。**

3 **按一下 [Add] 按鈕。**

4 **從 [Authentication Type] 下拉式清單中，選取此存取控制行所適用的認證方法。**

5 **從 [Connection Type] 下拉式清單中，選取該行所符合的指令類型。可能的指令類型為：**

- **Connect**
- **Bind**
- **UDP**
- **All**

6 **在 [Source Host Mask] 欄位中，鍵入連線控制項目所適用的主機 IP 位址或主機名稱。**

若您鍵入 IP 位址，請在後面加上正斜線，以及要套用至來源 IP 位址的遮罩。SOCKS 伺服器會將此遮罩套用至來源的 IP 位址，以確定是否爲有效主機。主機遮罩項目中請勿使用空格。若您未鍵入主機遮罩，則連線項目會套用至所有主機。

例如，您可以在主機遮罩欄位中鍵入 155.25.0.0/255.255.0.0。若主機的 IP 位址是 155.25.3.5，SOCKS 伺服器會將遮罩套用至該 IP 位址，並確定主機的 IP 位址符合連線控制項目所適用的 IP 位址 (155.25.0.0)。

7 **在 [Port Range] 欄位中，鍵入連線控制項目所適用之來源電腦的連接埠。**

連接埠範圍項目中請勿使用空格。若您不指定連接埠範圍，則連線項目會套用至所有連接埠。

您可以使用方括號 [ ] 以包含兩端的連接埠，或是使用括弧 ( ) 以排除兩端的連接埠。例如，[1000-1010] 表示這兩個數值之間的所有連接埠號，包括 1000 和 1010，而 (1000-1010) 則表示這兩個數值之間的所有連接埠號，但是不包括 1000 和 1010。您也可以混合使用方括號和括弧。例如，(1000-1010] 表示 1000 和 1010 之間的所有號碼，排除 1000，但包含 1010。

8. **在 [Destination Host Mask] 欄位中，鍵入連線項目所適用的 IP 位址或主機名稱。**

   若您鍵入 IP 位址，請在後面加上正斜線，以及要套用至內送 IP 位址的遮罩。SOCKS 伺服器會將此遮罩套用至目標電腦的 IP 位址，以確定該電腦是否爲有效的目標主機。主機遮罩項目中請勿使用空格。若您未鍵入目標主機遮罩，則連線項目會套用至所有主機。

   例如，您可以在目標主機遮罩欄位中鍵入 155.25.0.0/255.255.0.0。若目標主機的 IP 位址是 155.25.3.5，則 SOCKS 伺服器會將遮罩套用至該 IP 位址，並確定目標主機的 IP 位址符合代理伺服器項目所適用的 IP 位址 (155.25.0.0)。

9. **在 [Port Range] 欄位中，鍵入連線控制項目所適用之目標主機的連接埠。**

   連接埠範圍項目中請勿使用空格。若您不鍵入連接埠範圍，則連線項目會套用至所有連接埠。

   備註 – 大多數的 SOCKS 應用程式都請求用連接埠 0 來連結請求，表示沒有設定連接埠喜好設定。因此，連結的目標連接埠範圍應一律包含連接埠 0。

   您可以使用方括號 [ ] 以包含兩端的連接埠，或是使用括弧 ( ) 以排除兩端的連接埠。例如，[1000-1010] 表示這兩個數值之間的所有連接埠號，包括 1000 和 1010，而 (1000-1010) 則表示這兩個數值之間的所有連接埠號，但是不包括 1000 和 1010。您也可以混合使用方括號和括弧。例如，(1000-1010] 表示 1000 和 1010 之間的所有號碼，排除 1000，但包含 1010。

10. **在 [User Group] 欄位中，鍵入您要允許存取或拒絕存取的群組。**

    如未指定任何群組，則連線項目會套用至所有使用者。

11. **從 [Action] 下拉式清單中，針對您要建立的連線，選擇要允許或拒絕存取。**

12. **從 [Insert] 下拉式清單中，選取這個項目在 `socks5.conf` 檔案中的位置，然後按一下 [OK]。**

    因爲連線指令可以有多個，因此您必須指定對這些指令的評估順序。

▼ 編輯連線項目

1. **從 Server Manager 存取伺服器實例，然後按一下 [SOCKS] 標籤。**
2. **建立 [Set SOCKS v5 Connections] 連結。**
3. **選取您要編輯的連線項目，然後按一下 [Edit] 按鈕。**
4. **視需要進行變更。**

5 按一下 [OK]。

▼ 刪除連線項目

1 從 Server Manager 存取伺服器實例，然後按一下 [SOCKS] 標籤。

2 建立 [Set SOCKS v5 Connections] 連結。

3 選取您要刪除的連線項目。

4 按一下 [Delete] 按鈕。

▼ 移動連線項目

對項目的評估順序是依照它們在 `socks5.conf` 檔案中出現的順序。您可以移動這些項目以變更順序。

1 從 Server Manager 存取伺服器實例，然後按一下 [SOCKS] 標籤。

2 建立 [Set SOCKS v5 Connections] 連結。

3 選取您要移動的連線項目。

4 按一下 [Move] 按鈕。

5 在 [Move] 下拉式清單中，選取這個項目在 `socks5.conf` 檔案中的位置，然後按一下 [OK]。

配置 SOCKS v5 伺服器鏈接

將 SOCKS 伺服器鏈接在一起的方法與 Proxy Server 相同，這表示 SOCKS 伺服器可透過另一個 SOCKS 伺服器進行路由。

▼ 配置 SOCKS 伺服器鏈接

1 從 Server Manager 存取伺服器實例，然後按一下 [SOCKS] 標籤。

2 按一下 [Set SOCKS v5 Routing] 連結。

3 **若代理伺服器鏈中的下游代理伺服器在處理任何請求時需要認證，請在 [Server Chaining] 區段中，鍵入使用者名稱和密碼，供鏈接的 Proxy Server 進行認證。按一下 [OK]。**

配置路由項目

路由項目可用來對 Proxy Server 進行配置，以透過 SOCKS 伺服器路由請求。路由項目的兩種類型分別是 SOCKS v5 路由和 SOCKS v5 代理伺服器路由。

- SOCKS v5 路由會識別 SOCKS 常駐程式應針對特定 IP 位址使用哪個介面。
- SOCKS v5 代理伺服器路由會識別可經由另一部 SOCKS 伺服器存取的 IP 位址，以及該 SOCKS 伺服器是否直接連線至主機。經由 SOCKS 伺服器進行路由時，代理伺服器路由是很重要的。

▼ 建立路由項目

1 **從 Server Manager 存取伺服器實例，然後按一下 [SOCKS] 標籤。**

2 **按一下 [Set SOCKS v5 Routing] 連結。**

3 **在 [Routing] 區段中，按一下 [Add] 按鈕。**

4 **在 [Host Mask] 欄位中，鍵入內送和外寄連線必須通過指定介面的 IP 位址或主機名稱。**

若您鍵入 IP 位址，請在後面加上正斜線，以及要套用至內送 IP 位址的遮罩。SOCKS 伺服器會將此遮罩套用至 IP 位址，以確定是否爲有效主機。主機遮罩項目中請勿使用空格。若您不提供主機遮罩，則 SOCKS v5 項目會套用至所有主機。

例如，您可以在主機遮罩欄位中鍵入 155.25.0.0/255.255.0.0。若主機的 IP 位址是 155.25.3.5，SOCKS 伺服器會將遮罩套用至該 IP 位址，並確定主機的 IP 位址符合路由項目所適用的 IP 位址 (155.25.0.0)。

5 **在 [Host Mask] 欄位中，鍵入內送和外寄連線必須通過指定介面的 IP 位址或主機名稱。您的連接埠範圍不該有任何空格。**

若您不指定連接埠範圍，則 SOCKS v5 項目會套用至所有連接埠。

您可以使用方括號 [ ] 以包含兩端的連接埠，或是使用括弧 ( ) 以排除兩端的連接埠。例如，[1000-1010] 表示這兩個數值之間的所有連接埠號，包括 1000 和 1010，而 (1000-1010) 則表示這兩個數值之間的所有連接埠號，但是不包括 1000 和 1010。您也可以混合使用方括號和括弧。例如，(1000-1010] 表示 1000 和 1010 之間的所有號碼，排除 1000，但包含 1010。

6 **在 [Interface/Address] 欄位中，鍵入內送和外寄連線必須通過的 IP 位址或介面名稱。**

7 **從 [Insert] 下拉式清單中，選取這個項目在 `socks5.conf` 檔案中的位置，然後按一下 [OK]。**

因爲路由方法可以有多種，因此您必須指定對這些方法的評估順序。

備註 – 所指定的介面應同時用於內送和外寄連線，否則將因內送路由與配置介面不同而收到錯誤訊息。

▼ 建立代理伺服器路由項目

1 **從 Server Manager 存取伺服器實例，然後按一下 [SOCKS] 標籤。**

2 **按一下 [Set SOCKS v5 Routing] 連結。**

3 **在 [Proxy Routing] 區段中，按一下 [Add] 按鈕。**

4 **從 [代理伺服器類型] 下拉式清單中，選取您要經由其進行路由的 Proxy Server 類型。可供使用的項目如下**

- **SOCKS v5**
  - **SOCKS v4**
  - **Direct connection**

5 **在 [Destination Host Mask] 欄位中，鍵入連線項目所適用的 IP 位址或主機名稱。**

若您鍵入 IP 位址，請在後面加上正斜線，以及要套用至內送 IP 位址的遮罩。SOCKS 伺服器會將此遮罩套用至目標電腦的 IP 位址，以確定該電腦是否爲有效的目標主機。主機遮罩項目中請勿使用空格。若您未提供目標主機遮罩，則連線項目會套用至所有主機。

例如，您可以在目標主機遮罩欄位中鍵入 155.25.0.0/255.255.0.0。若目標主機的 IP 位址是 155.25.3.5，則 SOCKS 伺服器會將遮罩套用至該 IP 位址，並確定目標主機的 IP 位址符合代理伺服器項目所適用的 IP 位址 (155.25.0.0)。

6 **在 [Destination Port Range] 欄位中，鍵入代理伺服器項目所適用之目標主機的連接埠。**

連接埠範圍項目中請勿使用空格。若您不指定連接埠範圍，則代理伺服器項目會套用至所有連接埠。

您可以使用方括號 [ ] 以包含兩端的連接埠，或是使用括弧 ( ) 以排除兩端的連接埠。例如，[1000-1010] 表示這兩個數值之間的所有連接埠號，包括 1000 和 1010，而 (1000-1010) 則表示這兩個數值之間的所有連接埠號，但是不包括 1000 和 1010。您也可以混合使用方括號和括弧。例如，(1000-1010] 表示 1000 和 1010 之間的所有號碼，排除 1000，但包含 1010。

7 **在 [Destination Proxy Address] 欄位中，鍵入要使用的 Proxy Server 的主機名稱或 IP 位址。**

8 在 [Destination Proxy Port] 欄位中，鍵入 Proxy Server 要用來偵聽 SOCKS 請求的連接埠號。

9 從 [Insert] 下拉式清單中，選取這個項目在 `socks5.conf` 檔案中的位置，然後按一下 [OK]。

因爲路由方法可以有多種，因此您必須指定對這些方法的評估順序。

▼ 編輯路由項目

1 從 Server Manager 存取伺服器實例，然後按一下 [SOCKS] 標籤。

2 按一下 [Set SOCKS v5 Routing] 連結。

3 選取您要編輯的項目。

4 按一下 [Edit] 按鈕。

5 視需要進行變更。

6 按一下 [OK]。

▼ 刪除路由項目

1 從 Server Manager 存取伺服器實例，然後按一下 [SOCKS] 標籤。

2 按一下 [Set SOCKS v5 Routing] 連結。

3 選取您要刪除的項目。

4 按一下 [Delete] 按鈕。

▼ 移動路由項目

對項目的評估順序是依照它們在 `socks5.conf` 檔案中出現的順序。您可以移動這些項目以變更順序。

1 從 Server Manager 存取伺服器實例，然後按一下 [SOCKS] 標籤。

2 按一下 [Set SOCKS v5 Routing] 連結。

3 選取您要移動的項目。

4. 按一下 [Move] 按鈕。
5. 在 [Move] 下拉式清單中，選取這個項目在 `socks5.conf` 檔案中的位置，然後按一下 [OK]。

◆ ◆ ◆ 第 16 章

16 管理範本和資源

您可以使用範本將 URL 組合在一起，如此即可配置代理伺服器對 URL 的處理方法。您可以讓代理伺服器根據用戶端嘗試擷取的 URL，而有不同的運作方式。例如，您可能要求用戶端在從特定網域存取 URL 時，必須鍵入使用者名稱及密碼進行認證。或者拒絕存取指向影像檔的 URL。您可以根據檔案類型來配置不同的快取更新設定。

本章包含下列小節：

關於範本

範本是 URL (稱爲資源) 的集合。資源可能爲單一 URL、一組具有某些共同點的 URL 或整個協定。請先命名並建立範本，然後使用常規表示式來指定範本的 URL。以這種方式，您就可以配置代理伺服器以不同的方式來處理各種 URL 的請求。常規表示式可建立的任何 URL 式樣皆可放入範本中。下表列出預設的資源並提供關於其他範本的一些建議。

表 16–1 資源常規表示式萬用字元式樣

常規表示式式樣	配置的項目
`ftp://.*`	全部 FTP 請求
`http://.*`	全部 HTTP 請求
`https://.*`	全部安全的 HTTP 請求
`gopher://.*`	全部 Gopher 請求
`connect://.*:443`	傳送至 HTTPS 連接埠的所有 SSL (安全) 作業事件。

表 16–1 資源常規表示式萬用字元式樣 *(續)*

常規表示式式樣	配置的項目
`http://home\.example\.com.*`	`home.example.com` 網站上的所有文件。
`.*\.gif.*`	包含 `.gif` 字串的所有 URL
`.*\.edu.*`	包含 `.edu` 字串的所有 URL
`http://.*\.edu.*`	連線至 `.edu` 網域中某一台電腦的所有 URL

瞭解常規表示式

Proxy Server 可讓您使用常規表示式來識別資源。常規表示式用來指定字元串式樣。在代理伺服器中，常規表示式可用來尋找 URL 中相符的式樣。

下列範例說明常規表示式：

```
[a-z]*://[^:/]*\.abc\.com.*
```

此常規表示式會比對 `.abc.com` 網域中的所有文件。這些文件可能使用任何協定，也可能有任何副檔名。

下表列出常規表示式及其對應的涵義。

表 16–2 常規表示式及其涵義

表示式	涵義
。	比對除換行以外的任何單一字元。
x?	比對常規表示式 *x* 出現零次或一次的地方。
*x**	比對常規表示式 *x* 出現零次或多次的地方。
x+	比對常規表示式 *x* 出現一次或多次的地方。
x{n,m}	比對字元 *x*，其中 *x* 至少出現 *n* 次，但不超過 *m* 次。
x{n,}	比對字元 *x*，其中 *x* 至少出現 *n* 次。
x{n}	比對字元 *x*，其中 *x* 剛好出現 *n* 次。
[abc]	比對括號內的任何字元。
[^abc]	比對不在括號內的任何字元。
[a-z]	比對在括號範圍內的任何字元。
x	比對字元 *x*，其中 *x* 不是特殊字元。

表 16–2 常規表示式及其涵義 *(續)*

表示式	涵義
\x	移除特殊字元 *x* 的涵義。
"x"	移除特殊字元 *x* 的涵義。
xy	比對出現常規表示式 *x* 且後面跟著出現常規表示式 *y* 的地方。
x|y	比對常規表示式 *x* 或常規表示式 *y*。
^	比對字串的開頭。
$	比對字串的結尾。
(x)	組合常規表示式。

此範例說明如何使用第 312 頁的 「瞭解常規表示式」中的某些常規表示式。

```
[a-z]*://([^.:/]*[:/]|.*\.local\.com).*
```

- `[a-z]*` 會比對任何協定的文件。
- `://` 會比對一個 (:) 且後面跟著 (//)。
- `[^.:/]*[:/]` 比對不包含 (.)、(:)或 (/) 的任何字串，但後面跟著一個 (:) 或一個 (/)。因此，這個表示式會比對不完全合格的主機名稱以及含有連接埠號的主機。
- `|.*\.local\.com` 不會比對完全合格的網域名稱主機名稱，例如 `local.com`，但會比對 `.local.com` 網域中的文件。
- `.*` 會比對具有任何副檔名的文件。

根據第 312 頁的 「瞭解常規表示式」的說明，可以使用反斜線來替換或修改特殊字元的涵義。句點和問號等字元有特殊的涵義，因此在用來代表本身時必須替換。尤其，許多 URL 中經常會出現句點。若要在常規表示式中修改句點的特殊涵義，則句點前必須加上反斜線。

瞭解萬用字元式樣

您可以建立萬用字元式樣的清單，讓您指定從站點上可存取的 URL。根據用法而定，萬用字元的格式可以爲常規表示式或 shell 表示式。一般規則：

- 對於任何比對目標 URL 的式樣，請使用常規表示式。包括 <Object ppath=...>、URL 篩選以及 NameTrans、PathCheck 和 ObjectType 函數。
- 對於任何比對內送用戶端或使用者 ID 的式樣，請使用 shell 表示式，包括存取控制的使用者名稱和群組以及外來使用者的 IP 位址或 DNS 名稱，例如 <Client dns=...>。

您可以使用常規表示式萬用字元式樣來指定數個 URL。萬用字元可讓您在 URL 中指定一個字來篩選網域名稱或任何 URL。例如，您可能想要禁止存取包含「careers」字串的 URL。要具體實作，您可指定 `http://.*careers.*` 做爲範本的常規表示式。

使用範本

▼ 建立範本

您可以使用常規表示式萬用字元式樣來建立範本。接著可以配置僅影響此範本中指定之 URL 的設定。例如，您可以對 .GIF 影像採取某種快取配置，而對一般的 .html 檔案採取另一種配置。

1. **存取 Server Manager，然後按一下 [Templates] 標籤。**
   按一下 [Create Template] 連結。螢幕上會顯示 [Create Template] 頁面。
2. **在 [Template Name] 欄位中，鍵入您所建立的範本名稱，然後按一下 [OK]。**
   此名稱應當是容易記住的。Server Manager 會提示您儲存和套用變更。您可以在建立範本的常規表示式之後儲存變更，如餘下的步驟所述。

▼ 套用範本

1. **存取 Server Manager，然後按一下 [Templates] 標籤。**
2. **按一下 [Apply Template] 連結。**
   螢幕上會顯示 [Apply Template] 頁面。
3. **在 [URL Prefix Wildcard] 欄位中鍵入常規表示式萬用字元式樣，其中包含您要納入範本中的所有 URL。**
4. **從 [Template] 清單中，選取您剛才增加的新範本的名稱。**
5. **按一下 [OK]。**
6. **按一下 [Restart Required]。**
   此時會顯示 [Apply Changes] 頁面。
7. **按一下 [Restart Proxy Server] 按鈕以套用變更。**

▼ 移除範本

您可以移除現有範本。移除範本會刪除與範本相關聯的所有配置。例如，如果已在範本 TEST 中設定所有 URL 的存取控制，則移除 TEST 範本時也會移除此範本中所包含 URL 的存取控制。

1. **存取 Server Manager，然後按一下 [Templates] 標籤。**
2. **按一下 [Remove Template] 連結。**
   螢幕上會顯示 [Remove Template] 頁面。
3. **從 [Remove] 清單中選擇範本。**
4. **按一下 [OK]。**
5. **按一下 [Restart Required]。**
   此時會顯示 [Apply Changes] 頁面。
6. **按一下 [Restart Proxy Server] 按鈕以套用變更。**

▼ 編輯範本

您可以檢視及編輯在 Server Manager 中建立的範本。

1. **存取 Server Manager，然後按一下 [Templates] 標籤。**
2. **按一下 [View Template] 連結。**
   螢幕上會顯示 [View Template] 頁面。範本會顯示在表格中，此表格會列出範本的常規表示式及範本名稱。
3. **若要編輯現有範本，請按一下 [Edit Template Assignment] 連結。螢幕上會顯示 [Apply Template] 頁面。**

移除資源

您可以在 [Remove Resource] 頁面中刪除整個常規表示式物件及其對應的配置。例如，您可以移除 gopher 資源，如此就可以從代理伺服器的配置檔案中移除與此資源相關聯的所有設定。

▼ 移除資源

1. **存取 Server Manager，然後按一下 [Templates] 標籤。**
2. **按一下 [Remove Resource] 連結。**
   此時會顯示 [Remove Resource] 頁面。

3. **從 [Remove] 下拉式清單中選取您要移除的資源。**
4. **按一下 [OK]。**
5. **按一下 [Restart Required]。**
   此時會顯示 [Apply Changes] 頁面。
6. **按一下 [Restart Proxy Server] 按鈕以套用變更。**

◆ ◆ ◆ 第 17 章

17 使用用戶端自動配置檔案

若您有支援多個用戶端的多個代理伺服器，可以使用用戶端自動配置檔案來配置所有瀏覽器用戶端。自動配置檔案包含 JavaScript 函數，可決定瀏覽器應該使用哪個代理伺服器 (如果存在) 來存取各種 URL。

瀏覽器在啓動時會載入自動配置檔案。每次使用者按一下連結或鍵入 URL 時，瀏覽器會使用配置檔案來判斷是否應該使用代理伺服器；如果答案爲是，又要使用哪個代理伺服器。您可以利用這個功能，輕鬆地配置組織中的所有瀏覽器實例。爲用戶端提供自動配置檔案的方式有許多種。

- 您可以使用 Proxy Server 做爲傳回自動配置檔案的 Web 伺服器。將瀏覽器指向代理伺服器的 URL。把代理伺服器當成 Web 伺服器使用可讓您將自動配置檔案保存在一個地點，因此當您需要更新時，只需要變更一個檔案。
- 您可以將檔案儲存在瀏覽器可存取的 Web 伺服器、FTP 伺服器或任何網路目錄中。將瀏覽器配置成透過提供檔案的 URL 來尋找該檔案，故一般 URL 皆可接受。若需要執行複雜的計算；例如若您的組織中有大型代理伺服器鏈，則可撰寫 Web 伺服器 CGI 程式，以便根據檔案的存取者身分輸出不同的檔案。
- 您可以在本機中將自動配置檔案與瀏覽器的每個副本一起儲存。但是，若需要更新檔案，則您必須將該檔案的副本發行到每個用戶端。

您可以使用下列兩種方式的其中一種來建立自動配置檔案：使用 Server Manager 中的頁面，或手動建立檔案。本章稍後將有建立檔案的說明。

本章包含下列小節：

瞭解自動配置檔案

身爲 Proxy Server 管理員，您也必須負責建立與發行用戶端自動配置檔案。

自動配置檔案的用途

自動配置檔案以 JavaScript 撰寫，這是一種精簡的物件型程序檔語言，用於開發用戶端及伺服器網際網路應用程式。瀏覽器會解譯該 JavaScript 檔案。

瀏覽器首次載入時會下載該自動配置檔案。您可以將該檔案放在瀏覽器可使用 URL 來存取的任何位置。例如，您可以將該檔案放在 Web 伺服器上。您甚至可以將該檔案放在瀏覽器可使用 file:// URL 來存取的網路檔案系統中。

代理伺服器配置檔案是以 JavaScript 撰寫。該 JavaScript 檔案定義了單個函數 (稱爲 *FindProxyForURL*)，用於確定瀏覽器應對每個 URL 使用哪個 Proxy Server (如果存在)。瀏覽器會傳送兩個參數給 JavaScript 函數：瀏覽器執行所在之系統的主機名稱，以及瀏覽器嘗試取得的 URL。JavaScript 函數會傳回一個值給瀏覽器，告知瀏覽器如何繼續。

使用自動配置檔案就可以爲各種類型的 URL、各種伺服器或甚至一天的不同時段，指定不同的代理伺服器 (或完全不指定代理伺服器)。換句話說，您可以設定多部特殊用途的代理伺服器，例如一部代理伺服器處理 .com 網域、另一部處理 .edu 網域，再一部處理剩下類型的網域。透過這種方式可以分散負載，並更有效率地使用代理伺服器的磁碟，因爲這樣只會在快取記憶體中儲存所有檔案的一份副本，而不是多部代理伺服器都儲存相同的文件。

自動配置檔案也支援代理伺服器容錯移轉，因此若某部代理伺服器無法使用，瀏覽器會直接切換到另一部代理伺服器。

將代理伺服器當做 Web 伺服器存取

您可以在代理伺服器上儲存一或多個自動配置檔案，並將該代理伺服器當成 Web 伺服器使用 (其唯一的文件是自動配置檔案)。此舉可以讓身爲代理伺服器管理員的您，維護組織中用戶端所需的代理伺服器自動配置檔案。同時也可以透過這種方式將該檔案保存在集中位置，因此更新檔案時，只需要執行一次更新動作，所有的瀏覽器用戶端都就可以自動取得更新。

您可以將代理伺服器自動配置檔案放在 *server- root*/proxy-server*id*/pac/ 目錄中。在瀏覽器中，輸入代理伺服器自動配置檔案的 URL，方式是在 [Proxies] 標籤中鍵入該檔案的 URL。代理伺服器 URL 的格式如下：

http://*proxy.domain:port/URI*

例如，URL 可能爲 http://proxy.example.com。如果您確實使用了 URI，亦即緊隨在 host:port 組合之後的 URL 部分，則您可以使用範本來控制對各種自動配置檔案的存

取。例如，若建立了名爲 /test 的 URI，且其包含名爲 /proxy.pac 的自動配置檔案，便可以建立具有資源式樣 http://proxy.mysite.com:8080/test/.* 的範本。接著，您可以使用該範本來設定該目錄專屬的存取控制。

您可以建立多個自動配置檔案，並透過不同的 URL 來存取這些檔案。下表列出一些範例 URI，以及用戶端用來存取這些 URI 的 URL。

表 17–1 範例 URI 與對應的 URL

URI (路徑)	代理伺服器的 URL
/	http://proxy.mysite.com
/employees	http://proxy.mysite.com/employees
/group1	http://proxy.mysite.com/group1
/managers	http://proxy.mysite.com/managers

搭配反向代理伺服器使用 PAC 檔案

由於反向代理伺服器的運作方式之故，所以將 .pac 檔案用在代理伺服器與伺服器上會非常困難。當代理伺服器收到檔案請求時，必須判斷該請求是要存取本地 .pac 檔案或遠端文件。

若要將代理伺服器當做反向代理伺服器 (除了維護與提供 .pac 檔案功能之外)，請編輯 obj.conf 檔案，以確定 NameTrans 函數的順序是正確的。

建立標準對映，將代理伺服器當做反向代理伺服器。此動作通常會告訴代理伺服器將所有請求路由至遠端內容伺服器。您可以增加代理伺服器自動配置檔案，並將它對映到特定目錄，例如 /pac。在此情況下，想要取得 .pac 檔案的任何用戶端都必須使用如下 URL：

```
http://proxy.mysite.com/pac
```

注意 – 建立此對映時，請務必確定遠端內容伺服器沒有類似的目錄。

編輯 obj.conf 檔案，以確保代理伺服器自動配置檔案的指令與函數出現在其他對映之前。此指令與函數必須在最前面，因爲代理伺服器通常會先執行所有 NameTrans 函數，才處理請求。然而，透過自動配置檔案，代理伺服器會立即識別路徑並傳回 .pac 檔案。

下列範例是來自使用反向代理伺服器並維護自動配置檔案的 obj.conf 檔案。

```
<Object name="default">
NameTrans from="file:" fn="map" to="ftp:"
NameTrans from="/pac" fn="pac-map" name="file"
```

```
    to="/ns-home/proxy/pac/proxy.pac"
NameTrans fn="redirect" from="http://foo.*" url="http://www.acme.com"
NameTrans from="/ns-icons" fn="pfx2dir" dir="/ns-home/ns-icons" name="file"
NameTrans fn="reverse-map" from="http://web.acme.com"
    to="http://proxy.acme.com:8080"
NameTrans fn="map" from="http://proxy.acme.com:8080"
    to="http://web.acme.com"
NameTrans fn="map" from="/" to="http://web.acme.com"
PathCheck fn="url-check"
Service fn="deny-service"
AddLog fn="flex-log" name="access"
AddLog fn="urldb-record"
</Object>
```

使用 Server Manager 頁面來建立自動配置檔案

▼ 使用 Server Manager 建立自動配置檔案

1. **存取 Server Manager，並選取 [Routing] 標籤。**

2. **按一下 [Create/Edit Autoconfiguration File] 連結。**

   顯示的頁面中會列出代理伺服器系統上的所有自動配置檔案。您可以按一下自動配置檔案以進行編輯。剩下的步驟會告訴您如何建立新檔案。

3. **鍵入用戶端從代理伺服器取得自動配置檔案時，將使用的可選用 URI (URL 的路徑部分)。**

   例如，鍵入 / 可讓用戶端將該檔案當做代理伺服器的主文件 (類似 Web 伺服器的 `index.html` 檔案) 存取；往後用戶端存取代理伺服器以取得自動配置檔案時，將只需使用網域名稱。您可以使用多個 URI，並分別爲每個 URI 建立自動配置檔案。

4. **為自動配置檔案鍵入副檔名為 `.pac` 的名稱。**

   若您只有一個檔案，則只要命名爲 `proxy.pac` 即可。pac 爲 proxy autoconfiguration (代理伺服器自動配置) 的縮寫。所有自動配置檔案都是具有單一 JavaScript 函數的 ASCII 文字檔。

5. **按一下 [OK]。此時會顯示另一個頁面。**

   用戶端依順序完成頁面上的項目。該頁面上的項目是依用戶端排列。該頁面上的項目如下：

   - **Never Go Direct To Remote Server** 要求瀏覽器永遠使用您的代理伺服器。您可以指定代理伺服器未執行時，要使用的第二部代理伺服器。

- **Go Direct To Remote Server When** 決定何時略過代理伺服器。瀏覽器會以選項列在該頁面上的順序來判斷這些情況：
- **Connecting To Non-fully Qualified Host Names** 會在使用者只有指定電腦名稱時，就讓瀏覽器直接存取伺服器。例如，若內部 Web 伺服器的名稱是 `winternal.mysite.com`，則使用者只需鍵入 `http://winternal`，而非完全合格的網域名稱。在此情況下，瀏覽器會直接存取 Web 伺服器，而非代理伺服器。
- **Connecting To A Host In Domain** 會在用戶端可以解譯主機時，就讓瀏覽器直接存取伺服器。指定網域時，以點字元開頭。例如，您可以鍵入 `.example.com`。
- **Connecting To A Resolvable Host** 會在用戶端可以解析主機時，將瀏覽器直接傳送到伺服器。將 DNS 設定成僅解析本地 (內部) 主機時，通常會使用此選項。連線至區域網路外部的伺服器時，用戶端可能會使用代理伺服器。

注意 – 使用此選項時，用戶端會發現效能受到負面影響，因爲用戶端每次發出請求時都必須經過 DNS 查找。

- **Connecting To A Host In Subnet** 會在用戶端存取特定子網路內的伺服器時，就讓瀏覽器直接存取伺服器。當組織在某地理區域有許多子網路時，此選項就會非常有用。例如，某些公司可能有一個適用於全球子網路的網域名稱，但每個子網路皆有其特定的區域。

注意 – 使用此選項時，用戶端會發現效能受到負面影響，因爲用戶端每次發出請求時都必須經過 DNS 查找。

- **Except When Connecting To Hosts** 可讓您指定直接存取伺服器規則的例外。例如，若鍵入 `.example.com` 做爲要直接存取的網域，您可以把存取 `home.example.com` 當作例外。以後當瀏覽器存取 `home.example.com` 時會使用您的代理伺服器，但會直接存取 `example.com` 網域內的其他伺服器。
- **Secondary Failover Proxy** 指定代理伺服器未執行時要使用的第二部代理伺服器。
- **Failover Direct** 會在您的代理伺服器未執行時，讓瀏覽器直接存取伺服器。若指定了次要容錯移轉代理伺服器，Navigator 在直接存取伺服器之前，會先嘗試使用第二個代理伺服器。

6 **按一下 [OK] 建立自動配置檔案。**

該檔案會儲存在 *server-root*`/proxy-server` *id*`/pac` 目錄中。

此時會顯示確認訊息，通知您已正確建立檔案。重複上述步驟建立所需數量的自動配置檔案。

建立自動配置檔案之後，請務必要求代理伺服器的所有使用者指向正確的自動配置檔案，或自行配置所有瀏覽器。

手動建立自動配置檔案

本小節說明如何手動建立自動配置檔案。

代理伺服器自動配置檔案是以用戶端 JavaScript 所撰寫。每個檔案都包含一個名爲 `FindProxyForURL()` 的 JavaScript 函數，決定瀏覽器針對各個 URL 使用哪個代理伺服器 (如果存在)。瀏覽器會傳送兩個參數給 JavaScript 函數：目標原始伺服器的主機名稱，以及它嘗試取得的 URL。JavaScript 函數會傳回一個值給 Navigator，告知 Navigator 如何繼續。下節說明函數語法與可能的傳回值。

`FindProxyForURL()` 函數

`FindProxyFor()` URL 函數的語法是：

```
function FindProxyForURL(url, host){   ...}
```

對於瀏覽器所存取的每個 URL，它會傳送 *url* 與 *host* 參數，並以下列方式呼叫函數：

```
ret = FindProxyForURL(url, host);
```

url 是要透過瀏覽器存取的完整 URL。

host 是從要存取之 URL 擷取的主機名稱。這只是爲了方便；它其實與 **://** 與第一個 **:**或其後 **/** 之間的字串相同。此參數不包含連接埠號。如果有需要，可以從 URL 擷取。

ret (傳回值) 是說明配置的字串。

函數傳回值

自動配置檔案包含函數 `FindProxyForURL()`。此函數使用用戶端主機名稱與要存取的 URL 做爲參數。此函數會傳回單一字串，告知瀏覽器如何繼續。若該字串爲空，則表示不使用任何代理伺服器。該字串可包含下表顯示任何數量的基本元素，每個基本元素以分號分隔。

表 17–2 `FindProxyForURL()` 傳回值

傳回值	導致的瀏覽器動作
`DIRECT`	直接與伺服器連線，而不透過任何代理伺服器。
`PROXY` *host*:*port*	使用指定的代理伺服器與連接埠號。若使用分號分隔多個值，則會使用第一個代理伺服器。若該代理伺服器故障，則會使用下一個代理伺服器，以此類推。

表 17–2 FindProxyForURL() 傳回值 (續)

傳回值	導致的瀏覽器動作
SOCKS *host:port*	使用指定的 SOCKS 伺服器。若使用分號分隔多個值，則會使用第一個代理伺服器。若該代理伺服器故障，則會使用下一個代理伺服器，以此類推。

若瀏覽器遇到無法使用的代理伺服器，瀏覽器會在 30 分鐘後自動重試先前無回應的代理伺服器，然後 1 小時後再重試，以此類推 (重試間隔爲 30 分鐘)。因此，若您暫時關閉某個代理伺服器，在該代理伺服器重新啓動後，您的用戶端會在 30 分鐘內繼續使用該代理伺服器。

若所有代理伺服器皆已當機，且未指定 DIRECT 傳回值，瀏覽器將會要求使用者決定是否要讓瀏覽器暫時忽略代理伺服器，而嘗試直接連線。瀏覽器將會詢問是否要在 20 分鐘之後重試代理伺服器，然後 20 分鐘之後再詢問一次，以此類推 (詢問間隔爲 20 分鐘)。

在以下範例中，傳回值將要求瀏覽器使用連接埠 8080 上名爲 `w3proxy.example.com` 的代理伺服器。若該代理伺服器無法使用，瀏覽器會使用連接埠爲 8080 上名爲 `proxy1.example.com` 的代理伺服器。

```
PROXY w3proxy.example.com:8080; PROXY proxy1.example.com:8080
```

在下一個範例中，主代理伺服器是 `w3proxy.example.com:8080` 。若該代理伺服器無法使用，瀏覽器會使用 `proxy1.example.com:8080`。若兩個代理伺服器都無法使用，則瀏覽器會直接存取伺服器。在 20 分鐘過後，瀏覽器會詢問使用者是否要重試第一個代理伺服器。

```
PROXY w3proxy.example.com:8080; PROXY proxy1.example.com:8080; DIRECT
```

JavaScript 函數與環境

JavaScript 語言具有數個預先定義的函數與環境條件，在使用代理伺服器時非常有用。這些函數都會檢查是否與某特定條件相符，並傳回 true 或 false 值。相關公用程式函數則爲例外，因爲它們會傳回 DNS 主機名稱或 IP 位址。您可以在主 `FindProxyForURL ()` 函數中使用這些函數，以決定要傳送給瀏覽器的傳回值。本章稍後的範例將提供使用這些函數的方式。

本小節會說明每個函數或環境條件。瀏覽器與代理伺服器整合時適用的函數和環境條件爲：

- 主機名稱函數爲：
  - `dnsDomainIs()()`
  - `isInNet()()`
  - `isPlainhost name()()`

    - `isResolvable()()`
    - `localHostOrDomainIs()()`
- 公用程式函數爲：
    - dnsDomainLevels()
    - dnsResolve()
    - myIpAddress()
- 以 URL/主機名稱爲基礎的條件爲：
    - shExpMatch()
- 以時間爲基礎的條件爲：
    - dateRange()
    - timeRange()
    - weekdayRange()

以主機名稱為基礎的函數

以主機名稱爲基礎的函數可讓您使用主機名稱或 IP 位址，來決定要使用的代理伺服器 (如果存在)。

`dnsDomainIs()`(host, domain)

`dnsDomainIs()()` 函數可偵測 URL 主機名稱是否屬於指定 DNS 網域。當您將瀏覽器配置成針對本機網域不使用代理伺服器時，此函數非常有用，如第 332 頁的「範例 1：除本地主機之外所有伺服器都使用代理伺服器」與第 332 頁的「範例 2：爲防火牆外的本地伺服器使用代理伺服器」中所述。

在根據 URL 所屬的 DNS 網域，從代理伺服器群組中選取要用來接收請求之代理伺服器時，若您使用多個代理伺服器來達成負載平衡，此函數也非常有用。例如，若您的負載平衡配置是將包含 `.edu` 的 URL 導向到一個代理伺服器，並將包含 `.com` 的 URL 導向到另一個代理伺服器，則可以使用 `dnsDomainIs()()` 來檢查 URL 主機名稱。

參數

host 是來自 URL 的主機名稱。

domain 是測試主機名稱時所依據的網域名稱。

傳回值

true 或 false

範例

下列敘述爲 true：

```
dnsDomainIs("www.example.com", ".example.com")
```

下列敘述爲 false：

```
dnsDomainIs("www", ".example.com") dnsDomainIs("www.mcom.com",
    ".example.com")
```

isInNet()(host, pattern, mask)

isInNet()() 函數可讓您將 URL 主機名稱解析爲 IP 位址，並測試它是否屬於遮罩所指定的子網路。這與 SOCKS 使用的 IP 位址式樣屬於相同類型。請參閱第 333 頁的「範例 4：直接連線到子網路」。

參數：

host 爲 DNS 主機名稱或 IP 位址。若傳送的是主機名稱，此函數會將它解析爲 IP 位址。

pattern 是以點分隔的 IP 位址式樣

mask 是 IP 位址式樣遮罩，決定應該比對 IP 位址的哪個部分。值 0 表示忽略；255 表示相符。若主機的 IP 位址符合指定的 IP 位址式樣，則此函數會傳回 true。

傳回值

true 或 false

範例

只有當主機的 IP 位址與 198.95.249.79 完全相符時，此敘述才爲 true：

```
isInNet(host, "198.95.249.79", "255.255.255.255")
```

只有當主機的 IP 位址與 198.95.* .* 完全相符時，此敘述才爲 true： isInNet(host, "198.95.0.0", "255.255.0.0")

isPlainhost name()(host)

isPlainhost name()() 函數會偵測所請求 URL 中的主機名稱，是一般主機名稱還是完全合格的網域名稱。當您想要讓瀏覽器直接連線到本地伺服器時，此函數非常有用，如第 332 頁的「範例 1：除本地主機之外所有伺服器都使用代理伺服器」與第 332 頁的「範例 2：爲防火牆外的本地伺服器使用代理伺服器」中所述。

參數

host 是來自 URL 的主機名稱，僅在主機名稱沒有網域名稱 (沒有以點分隔的區段) 時排除連接埠號。

傳回值

host 爲本機時傳回 true；*host* 爲遠端時傳回 false

範例

```
isPlainhost name("host")
```

若 *host* 是 www 之類的字串，則此函數會傳回 true。若 host 是 www. example.com 之類的字串，則此函數會傳回 false。

isResolvable()(host)

若防火牆內的 DNS 只能識別內部主機，您可以使用 isResolvable()() 函數來測試主機名稱屬於內部網路還是外部網路。透過使用此函數，您可以配置瀏覽器針對內部伺服器使用直接連線，而只針對外部伺服器使用代理伺服器。在防火牆內的內部主機可以解譯其他內部主機的 DNS 網域名稱，但無法解析所有外部主機的站點中，此函數非常有用。isResolvable()() 函數會查閱 DNS，嘗試將主機名稱解析爲 IP 位址。請參閱第 332 頁的 「範例 3：只會爲無法解譯的主機使用代理伺服器」

參數

host() 是來自 URL 的主機名稱。

傳回值

若此函數可以解析主機名稱，會傳回 true；否則會傳回 false

範例

```
isResolvable("host")
```

若 host() 是 www 之類的字串，且可透過 DNS 解析，則此函數會傳回 true。

localHostOrDomainIs()(host, hostdom)

localHostOrDomainIs()() 函數指定可能會由完全合格的網域名稱或一般主機名稱存取的本地主機。請參閱第 332 頁的 「範例 2：爲防火牆外的本地伺服器使用代理伺服器」。

若主機名稱與指定的主機名稱完全相符，或與不合格主機名稱相符的主機名稱中沒有網域名稱部分，則 localHostOrDomainIs()() 函數會傳回 true。

參數

host 是來自 URL 的主機名稱。

hostdom 是要比對之完全合格的主機名稱。

傳回值

true 或 false

範例

以下敘述爲 true (完全相符)：

```
localHostOrDomainIs("www.example.com", "www.example.com")
```

以下敘述爲 true (主機名稱符合，未指定網域名稱)：

```
localHostOrDomainIs("www", "www.example.com")
```

以下敘述爲 false (網域名稱不相符)：

```
localHostOrDomainIs("www.mcom.com", "www.example.com")
```

以下敘述爲 false (主機名稱不相符)：

```
localHostOrDomainIs("home.example.com", "www.example.com")
```

公用程式函數

您可以使用公用程式函數找出網域層級、執行瀏覽器的主機，或主機的 IP 位址。

`dnsDomainLevels()`**(host)**

`dnsDomainLevels()()` 函數可找出 URL 主機名稱中的 DNS 層級數目 (點的數目)。

參數

host 是來自 URL 的主機名稱。

傳回值

DNS 網域層級的數目 (整數)。

範例

`dnsDomainLevels("www")` 傳回 0。

`dnsDomainLevels("www.example.com")` 傳回 2。

dnsResolve()(host)

dnsResolve()() 函數會解析指定主機 (通常是來自 URL) 的 IP 位址。若 JavaScript 函數必須執行的式樣比對程序，比現有函數的功能更進階，則此函數就非常有用。

參數

host 是要解析的主機名稱。將指定的 DNS 主機名稱解析爲 IP 位址，並以字串傳回 (以點分隔的格式)。

傳回值

字串值 (由以點分隔的四組數字所組成的 IP 位址)

範例

以下範例將傳回字串 198.95.249.79。

```
dnsResolve("home.example.com")
```

myIpAddress()()

當 JavaScript 函數必須根據執行瀏覽器的主機而有不同的運作方式時，myIpAddress()() 函數就非常有用。此函數會傳回執行瀏覽器之電腦的 IP 位址。

傳回值

字串值 (由以點分隔的四組數字所組成的 IP 位址)

範例：

若您是在 home.example.com 電腦上執行 Navigator，以下範例會傳回字串 198.95.249.79。

```
myIpAddress()
```

以 URL/主機名稱為基礎的條件

您可比對主機名稱或 URL 以達到負載平衡和路由的目的。

shExpMatch()(str, shexp)

shExpMatch()() 函數會比對 URL 主機名稱或 URL 本身。此函數的主要用途是負載平衡，以及使用智慧型方式將 URL 路由至不同的代理伺服器。

參數

str 是要比較的任何字串 (例如，URL 或主機名稱)。

shexp 是比較時所依據的 shell 表示式。

若字串與指定的 shell 表示式相符，則此表示式會傳回 true。請參閱第 334 頁的 「範例 6：使用 shExpMatch()() 平衡代理伺服器的負載」。

傳回值

true 或 false

範例

第一個範例會傳回 true。第二個範例會傳回 false。

```
shExpMatch("http://home.example.com/people/index.html",
           ".*/people/.*")
shExpMatch("http://home.example.com/people/yourpage/index.html",
           ".*/mypage/.*")
```

以時間為根據的條件

您可以讓 **FindProxyForURL** 函數根據日期、時間或一週中的日期，有不同的運作方式。

dateRange() (day, month, year...)

dateRange()() 函數會偵測特定日期或日期範圍，例如 1996 年 4 月 19 日到 1996 年 5 月 3 日。若要讓 FindProxyForURL() 函數根據星期幾而有不同的運作方式 (例如，需要針對其中一個代理伺服器定期排程停機維護時間)，此函數就非常有用。

您可以使用數種方式指定日期範圍：

```
dateRange(day)dateRange(day1, day2)dateRange(mon)dateRange(month1,
month2)dateRange(year)dateRange(year1, year2)dateRange(day1, month1, day2,
month2)dateRange(month1, year1, month2, year2)dateRange(day1, month1, year1,
day2, month2, year2)dateRange(day1, month1, year1, day2, month2, year2, gmt)
```

參數

day 是 1 到 31 之間的整數，代表每月中的第幾天。

month 必須是下列其中一個月份字串：JAN FEB MAR APR MAY JUN JUL AUG SEP OCT NOV DEC

year 是四位整數的年份 (例如，1996)。

gmt 可以使用「GMT」字串表示，代表應以格林威治標準時間來比較時間，也可以留白表示使用本地時區。GMT 參數也可以指定於任何呼叫設定檔中，它始終做爲最後一個參數。若在每個種類 (日、月、年) 中僅指定單一值，則此函數只在與指定值相符的日期傳回 true 值。若指定兩個值，則從第一個指定時間到第二個指定時間之間都會傳回 true 結果值。

範例

此敘述在每月第一天 (本地時區) 會傳回 true：`dateRange(1)`

此敘述在每月第一天 (格林威治標準時間) 會傳回 true：`dateRange(1, "GMT")`

此敘述在每月的上半月都會傳回 true：`dateRange(1, 15)`

此敘述在每年 12 月 24 日會傳回 true：`dateRange(24, "DEC")`

此敘述在 1995 年 12 月 24 日會傳回 true：`dateRange(24, "DEC", 1995)`

此敘述在每年第一季都會傳回 true：`dateRange("JAN", "MAR")`

此敘述在每年 6 月 1 日到 8 月 15 日都會傳回 true： `dateRange(1, "JUN", 15, "AUG")`

此敘述在 1995 年 6 月 1 日到 1995 年 8 月 15 日都會傳回 true：`dateRange(1, "JUN", 15, 1995, "AUG", 1995)`

此敘述在 1995 年 10 月到 1996 年 3 月都會傳回 true：`dateRange("OCT", 1995, "MAR", 1996)`

此敘述在 1995 年整年都會傳回 true：`dateRange(1995)`

此敘述在 1995 年初到 1997 年末都會傳回 true：`dateRange(1995, 1997)`

timeRange (hour, minute, second...)

`timeRange()` 函數會偵測一天中的特定時間或時間範圍，例如下午 9 點到上午 12 點。若要讓 `FindProxyForURL()` 函數根據不同時間而有不同的運作方式，此函數非常有用。

```
timeRange(hour)timeRange(hour1, hour2)timeRange(hour1, min1, hour2,
min2)timeRange(hour1, min1, sec1, hour2, min2, sec2)
```

參數：

hour 是小時，介於 0 到 23 之間。0 是午夜，23 是下午 11:00 點。

min 是分鐘，介於 0 到 59 之間。

sec 是秒鐘，介於 0 到 59 之間。

gmt 可以是 GMT 字串 (表示 GMT 時區) 或未指定 (表示本地時區)。此參數可搭配每個參數設定檔使用，而且永遠是最後一個參數。

傳回值

true 或 false

範例：

此敘述在中午到下午 1:00 之間都會傳回 true：`timerange(12, 13)`

此敘述在中午到下午 12:59 (GMT) 之間都會傳回 true：`timerange(12, "GMT")`

此敘述在上午 9:00 到下午 5:00 之間都會傳回 true：`timerange(9, 17)`

此敘述在午夜與午夜過後三十秒之間都會傳回 true：`timerange(0, 0, 0, 0, 0, 30)`

weekdayRange()**(wd1, wd2, gmt)**

weekdayRange() 函數會偵測一週內的特定日期或一週內的日期範圍，例如星期一到星期五。若要讓 *FindProxyForURL* 函數根據星期幾而有不同的運作方式，此函數非常有用。

參數

wd1 和 *wd2* 皆爲下列其中一個星期幾字串：`SUN MON TUE WED THU FRI SAT`

gmt 可以是 GMT (表示格林威治標準時間) 或未指定 (表示本地時間)。

只有第一個參數 *wd1* 是必要參數。您可以忽略 *wd2* 或 *gmt*，或同時忽略兩者。

若只指定一個參數，此函數在參數所代表的星期幾當天會傳回 true。若將字串 GMT 指定爲第二個參數，就會以 GMT 表示時間。否則，會以您的本地時區表示時間。

若 *wd1* 和 *wd2* 皆已定義，而當天介於一週內指定的這兩天之間時，此條件爲 true。當作界線的這兩天也算在內。參數的順序非常重要；“MON,” “WED” 是指星期一到星期三，但 “WED,” “MON 是指星期三到下個星期一。

範例

此敘述在星期一到星期五 (本地時區) 之間會傳回 true。`weekdayRange("MON", "FRI")`

此敘述在星期一到星期五 (格林威治標準時間) 之間會傳回 true。 `weekdayRange("MON", "FRI", "GMT")`

此敘述在星期六 (本地時間) 會傳回 true。`weekdayRange("SAT")`

此敘述在星期六 (格林威治標準時間) 會傳回 true。`weekdayRange("SAT", "GMT")`

此敘述在星期五到星期一之間會傳回 true (順序非常重要) `weekdayRange("FRI", "MON")`

函數範例

本小節提供 JavaScript 函數的詳細範例。

範例 1：除本地主機之外所有伺服器都使用代理伺服器

在此範例中，瀏覽器會直接連線到未完全合格的所有主機，以及本機網域中的所有主機。存取其他主機時，則會透過名爲 `w3proxy.example .com:8080` 的代理伺服器。

備註 – 若該代理伺服器當機，則會自動進行直接連線。

```
function FindProxyForURL(url, host)
{
    if (isPlainhost name(host) ||
        dnsDomainIs(host, ".example.com") ||
        dnsDomainIs(host, ".mcom.com"))
        return "DIRECT";
    else
        return "PROXY w3proxy.example.com:8080; DIRECT";
}
```

範例 2：為防火牆外的本地伺服器使用代理伺服器

此範例類似第 332 頁的 「範例 1：除本地主機之外所有伺服器都使用代理伺服器」，但它會針對防火牆外部的本地伺服器使用代理伺服器。若主機 (例如，主 Web 伺服器) 屬於本機網域但位於防火牆外部，而且只能夠透過代理伺服器存取，則可以使用 `localHostOrDomainIs()()` 函數來處理那些異常：

```
function FindProxyForURL(url, host)
{
    if ((isPlainhost name(host) ||
    dnsDomainIs(host, ".example.com")) &&
    !localHostOrDomainIs(host, "www.example.com") &&
    !localHostOrDoaminIs(host, "merchant.example.com"))
        return "DIRECT";
    else
        return "PROXY w3proxy.example.com:8080; DIRECT";
}
```

此範例會針對所有主機使用代理伺服器，但 `example.com` 網域中的本地主機除外。主機 `www.example.com` 和 `merchant.example.com` 也會透過代理伺服器存取伺服器。

妥善指定異常的順序可增加效率：`localHostOrDomainIs()()` 函數只會針對位於本機網域中的 URL 執行，而不會針對每個 URL 執行。請特別注意 *and* 表示式之前、*or* 表示式周圍的括弧。

範例 3：只會為無法解譯的主機使用代理伺服器

此範例適用於內部 DNS 只能解析內部主機名稱的環境。其目的是只爲無法解析的主機使用代理伺服器。

```
function FindProxyForURL(url, host)
{
    if (isResolvable(host))
            return "DIRECT";
        else
            return "PROXY proxy.mydomain.com:8080";
}
```

使用此範例中的配置時，每次都需要經過 DNS 查找。因此，您可能需要搭配其他規則使用此範例，以便僅在其他規則沒有結果時才使用 DNS 查找。

```
function FindProxyForURL(url, host)
{
    if (isPlainhost name(host) ||
        dnsDomainIs(host, ".mydomain.com") ||
        isResolvable(host))
        return "DIRECT";
    else
        return "PROXY proxy.mydomain.com:8080";
}
```

範例 4：直接連線到子網路

在此範例中，會直接連線到指定子網路中的所有主機。其他主機則會經過代理伺服器。

```
function FindProxyForURL(url, host)
{
    if (isInNet(host, "198.95.0.0", "255.255.0.0"))
        return "DIRECT";
    else
        return "PROXY proxy.mydomain.com:8080";
}
```

在此範例中，您可以在開頭增加備援規則，以降低使用 DNS 的頻率：

```
function FindProxyForURL(url, host)
{
    if (isPlainhost name(host) ||
        dnsDomainIs(host, ".mydomain.com") ||
        isInNet(host, "198.95.0.0", "255.255.0.0"))
        return "DIRECT";
    else
        return "PROXY proxy.mydomain.com:8080";
}
```

範例 5：使用 dnsDomainIs()() 平衡代理伺服器的負載

此範例比上述範例複雜。此範例使用四個代理伺服器，而其中一個是做爲其他伺服器的緊急備用伺服器。若任何三個代理伺服器當機，會由第四個代理伺服器接手。其他三個代理伺服器會根據 URL 式樣分擔負載，以使快取效果更好。對於任何文件，它在三個伺服器上只存在一份副本，而不是在其中的每個伺服器上都有一份副本。負載的分擔方式如下表所示。

表 17–3 平衡代理伺服器的負載

代理伺服器	目的
#1	.com 網域
#2	.edu 網域
#3	其他所有網域
#4	緊急備用

存取本機網域時皆應使用直接存取。所有代理伺服器都是在連接埠 8080 上執行。您可以使用 + 運算子來鏈結字串。

```
function FindProxyForURL(url, host)
{
    if (isPlainhost name(host) || dnsDomainIs(host, ".mydomain.com"))
        return "DIRECT";

    else if (dnsDomainIs(host, ".com"))
        return "PROXY proxy1.mydomain.com:8080; " +
               "PROXY proxy4.mydomain.com:8080";

    else if (dnsDomainIs(host, ".edu"))
        return "PROXY proxy2.mydomain.com:8080; " +
               "PROXY proxy4.mydomain.com:8080";

    else
        return "PROXY proxy3.mydomain.com:8080; " +
               "PROXY proxy4.mydomain.com:8080";
}
```

範例 6：使用 shExpMatch()() 平衡代理伺服器的負載

此範例基本上與第 334 頁的 「範例 5：使用 dnsDomainIs()() 平衡代理伺服器的負載」相同，但範例 5 使用 dnsDomainIs()()，而此範例使用 shExpMatch()()。

```
    function FindProxyForURL(url, host)
    {
    if (isPlainhost name(host) || dnsDomainIs(host, ".mydomain.com"))
```

```
    return "DIRECT";
else if (shExpMatch(host, "*.com"))
    return "PROXY proxy1.mydomain.com:8080; " +
           "PROXY proxy4.mydomain.com:8080";
else if (shExpMatch(host, "*.edu"))
    return "PROXY proxy2.mydomain.com:8080; " +
           "PROXY proxy4.mydomain.com:8080";
else
    return "PROXY proxy3.mydomain.com:8080; " +
           "PROXY proxy4.mydomain.com:8080";
}
```

範例 7：針對特定協定使用代理伺服器

您可以爲特定協定設定代理伺服器。您可以在 `FindProxyForURL()()` 函數中使用大部分標準 JavaScript 功能。例如，若要根據協定設定不同的代理伺服器，可以使用 `substring()()` 函數。

```
function FindProxyForURL(url, host)
{
    if (url.substring(0, 5) == "http:") {
        return "PROXY http-proxy.mydomain.com:8080";
    }
    else if (url.substring(0, 4) == "ftp:") {
        return "PROXY ftp-proxy.mydomain.com:8080";
    }
    else if (url.substring(0, 7) == "gopher:") {
        return "PROXY gopher-proxy.mydomain.com:8080";
    }
    else if         (url.substring(0, 6) == "https:" ||
            url.substring(0, 6) == "snews:") {
        return "PROXY security-proxy.mydomain.com:8080";
    }
    else {
        return "DIRECT";
    }
}
```

您也可以使用 `shExpMatch()()` 函數來完成此配置，例如：

```
...
if (shExpMatch(url, "http:*")) {
    return "PROXY http-proxy.mydomain.com:8080;
}
...
```

◆ ◆ ◆ 第 18 章

18 ACL 檔案語法

存取控制清單 (ACL) 檔案是一種文字檔，所包含的清單用來定義可存取的使用者。依預設，Proxy Server 使用一個包含用於存取伺服器的所有清單的 ACL 檔案。亦可建立多個 ACL 檔案，並在 `obj.conf` 檔案中進行參照。

Proxy Server 4 使用的 ACL 檔案語法與 Proxy Server 3.x 中使用的不同。本附錄說明各 ACL 檔案及其語法。如需有關控制對 Proxy Server 及其資源的存取之詳細資訊，請參閱第 8 章 「控制對伺服器的存取」。Proxy Server 4 版本支援資源範本，如第 16 章 「管理範本和資源」中所述。

本附錄包含下列小節：

關於 ACL 檔案及 ACL 檔案語法

所有 ACL 檔案均必須遵循特定的格式與語法。ACL 檔案是包含一個或多個 ACL 的文字檔。所有 ACL 檔案都必須以單一語法版本編號爲開頭。例如：

```
version 3.0;
```

版本行可出現於任意註釋行之後。Proxy Server 使用 3.0 版的語法。在註釋行開頭使用 # 符號，即可在檔案中包含註釋。

每個檔案中的 ACL 開頭都會包含一個定義其類型的敘述：路徑、資源或已命名。

- 路徑 ACL 指定絕對路徑給受其影響的資源。
- 資源 ACL 指定受其影響的範本，例如 `http://`、`https://`、`ftp://` 等。如需有關範本的更多資訊，請參閱第 16 章 「管理範本和資源」。

- 已命名 ACL 指定 `obj.conf` 檔案的資源中所參照的名稱。伺服器具有一個預設已命名資源，每一位使用者均可讀取該資源，而 LDAP 目錄中的使用者還可對其進行寫入。已命名 ACL 雖可從 Proxy Server 使用者介面建立，但是您還必須在 `obj.conf` 檔案的資源中手動參照已命名 ACL。

路徑及資源 ACL 可包括萬用字元。如需有關萬用字元的更多資訊，請參閱第 16 章 「管理範本和資源」。

類型行以字母 `acl` 開頭，其後接著以雙引號標示的類型資訊，最後接著一個分號。例如：

```
acl "default";acl "http://*.*";
```

所有 ACL 的每種類型資訊均必須爲唯一名稱，即使在不同的 ACL 檔案中亦如此。定義 ACL 的類型之後，可附加一個或多個認證敘述，以定義與 ACL 一起使用的方法。您也可以加入授權敘述，以定義允許或拒絕存取的人員和電腦。下列小節說明這些敘述的語法。

認證敘述

ACL 可選擇性地指定當伺服器處理 ACL 時必須使用的認證方法。一般常用的三種方法爲：

- 基本 (預設值)
- 摘要
- SSL

基本及摘要方法要求使用者於存取資源前，須提供使用者名稱及密碼。

SSL 方法要求使用者具備用戶端憑證。若要通過認證，Proxy Server 必須開啓加密，且使用者憑證的核發者必須在可信任的 CA 清單中。

依預設，伺服器會針對未指定方法的任意 ACL 使用基本方法。您的伺服器認證資料庫必須能夠支援使用者發送的摘要認證。

每一認證行都必須指定伺服器所認證的屬性：使用者、群組或使用者及群組兩者。以下出現於 ACL 類型行之後的認證敘述指定的是基本認證，其中的使用者與資料庫或目錄中的個別使用者相符：

```
authenticate(user) { method = "basic";};
```

以下範例使用 SSL 做爲使用者及群組的認證方法：

```
authenticate(user, group) { method = "ssl";};
```

以下範例指出允許使用者名稱以 `sales` 開頭的任意使用者：

```
allow (all) user = "sales*";
```

若最後一行變更爲 group = sales，則 ACL 將會失敗，因爲群組屬性並未接受認證。

授權敘述

每個 ACL 項目均可以包含一個或多個授權敘述。授權敘述指定允許\或拒絕哪些使用者存取伺服器資源。

寫入授權敘述

寫入授權敘述時，請使用以下語法：

```
allow|deny [absolute] (right[,right...]) attribute expression;
```

每行開頭必須爲 allow 或 deny。由於規則的階層關係，最好在第一條規則中拒絕所有使用者進行存取，然後在後續規則中明確允許使用者、群組或電腦進行存取。例如，如果您允許所有人存取稱爲 /my_files 的目錄，然後允許少數幾個使用者存取 /my_files/personal 子目錄，則子目錄的存取控制將不會有作用，因爲允許存取 /my_files 目錄的所有人也可以存取 /my_files/personal 目錄。爲防止上述情形發生，請爲子目錄建立一條規則，先拒絕所有使用者存取，然後允許需要存取的幾個使用者進行存取。

然而，在某些情況下，如果將預設 ACL 設定爲拒絕所有使用者存取，則其他 ACL 規則就不需要「deny all」規則。

下列行拒絕所有使用者存取：

```
deny (all) user = "anyone";
```

授權敘述的階層

ACL 中的階層取決於資源。當伺服器收到對於特定資源的請求時，會建置一個適用於該資源的 ACL 清單。伺服器首先增加其 obj.conf 檔案的 check-acl 敘述中所列出的已命名 ACL。然後再附加相符的路徑及資源 ACL。此清單將會以相同順序進行處理。除非有「absolute」ACL 敘述，否則將依順序評估所有敘述。如果「absolute allow」或「absolute deny」描述評估爲「true」，則伺服器將停止處理並接受此結果。

如果有多個匹配的 ACL 存在，則伺服器會使用匹配的最後一個描述。然而，如果您使用絕對描述，則伺服器會停止尋找其他匹配的 ACL，並使用包含絕對描述的 ACL。如果同一個資源具有兩個絕對敘述，則伺服器將會使用檔案中的第一個敘述，並停止尋找其他相符的資源。

```
version 3.0;acl "default";authenticate (user,group)
    { prompt="Sun Java System Web Proxy Server";};
    allow (read,execute,list,info) user = "anyone";
    allow (write,delete) user = "all";acl "http://*.*";
```

```
deny (all) user = "anyone";allow (all) user = "joe";
```

屬性表示式

屬性表示式以使用者名稱、群組名稱、主機名稱或 IP 位址爲基礎，定義被允許或被拒絕存取的使用者。下列幾行是如何對不同人員或電腦授予存取權的範例：

- `user = "anyone"`
- `user = "smith*"`
- `group = "sales"`
- `dns = "*.mycorp.com"`
- `dns = "*.mycorp.com,*.company.com"`
- `ip = "198.*"`
- `ciphers = "rc4"`
- `ssl = "on"`

您也可以使用 `timeofday` 屬性，根據伺服器上的本機時間，限定一天中可存取伺服器的時間。例如，使用 `timeofday` 屬性，限定特定使用者只能在特定時間內存取。

請以 24 小時制指定時間，例如以 0400 指定上午 4:00 或 2230 指定下午 10:30。以下範例限定使用者群組 `guests` 只能在上午 8:00 到下午 4:59 之間進行存取。

```
allow (read) (group="guests") and (timeofday<0800 or timeofday=1700);
```

也可以依星期幾來限定存取。請使用以下三個字母的縮寫來指定星期幾：Sun、Mon、Tue、Wed、Thu、Fri 和 Sat。

以下敘述允許 `premium` 群組中的使用者在任一天的任何時間進行存取。`discount` 群組中的使用者可於週末全天進行存取，以及非週休時間上午 8:00 到下午 4:59 以外的任何時間進行存取。

```
allow (read) (group="discount" and dayofweek="Sat,Sun") or (group="discount" and
(dayofweek="mon,tue,wed,thu,fri" and(timeofday<0800 or timeofday=1700)))or
(group="premium");
```

表示式的運算子

屬性表示式可使用多種運算子。圓括號表示運算子的優先順序。以下運算子可與 `user`、`group`、`dns` 及 `ip` 一起使用：

- and
- or
- not
- = (等於)
- != (不等於)

以下運算子可與 `timeofday` 及 `dayofweek` 一起使用：

- 大於
- < 小於
- = 大於或等於
- <= 小於或等於

預設 ACL 檔案

安裝後，*server_root*/httpacl/generated.proxy- *serverid*.acl 檔案會爲伺服器提供預設設定。您在使用者介面中建立設定以前，伺服器都會使用工作檔案 genwork.proxy-*serverid*.acl。編輯 ACL 檔案時，您可以在 genwork 檔案中進行變更，然後使用 Proxy Server 儲存和套用這些變更。

一般語法項目

輸入字串可以包含以下字元：

- 字母 a 到 z
- 數字 0 到 9
- 句點和底線

其他字元必須在前後加上雙引號。

單一敘述可以單獨放在一行，並以分號結尾。多個敘述放於花括號內。項目清單必須使用逗號分隔，並以雙引號標示。

參照 obj.conf 檔案中的 ACL 檔案

您可以在 obj.conf 檔案的 PathCheck 指令中，使用 check-acl 函數參照已命名 ACL 或個別 ACL 檔案。該行使用以下語法：

```
PathCheck fn="check-acl" acl="aclname "
```

其中 *aclname* 爲 ACL 出現於任意 ACL 檔案中的唯一名稱。

例如，如果您想要使用名稱爲 testacl 的 ACL 來限定對目錄的存取，則可以將以下各行增加至 obj.conf 檔案：

```
<Object ppath="https://"PathCheck fn="check-acl" acl="testacl"</Object>
```

在此範例中，第一行是一個物件，敘述您想要限定對哪些伺服器資源的存取。第二行是 PathCheck 指令，其使用 check-acl 函數將已命名的 ACL (testacl) 連結到指令所在的物件。testacl ACL 可出現於 server.xml 參照的任意 ACL 檔案中。

◆ ◆ ◆ 第 19 章

19 調校伺服器效能

有許多元素會影響到 Proxy Server 環境的效能，包括代理伺服器用戶端、Proxy Server、原始伺服器及網路。本附錄說明可能改善 Proxy Server 效能的一些調整工作。

本附錄僅供進階管理員使用。調校伺服器時請務必謹慎，在進行任何變更之前，務必做好配置檔案備份。

本附錄包含下列小節：

一般效能注意事項

本小節說明分析 Proxy Server 效能時，應注意的一般領域。

本小節包含以下主題：

- 第 345 頁的 「安全性需求」
- 第 345 頁的 「Solaris 檔案系統快取」

存取記錄

停用存取記錄可以提昇 Proxy Server 的效能。不過，如此便無法檢視存取 Proxy Server 之人以及他們請求的頁面。

若要停用 Proxy Server 存取記錄，請在 obj.conf 檔案中爲下列指令加入註釋：

```
Init fn=“flex-init” access=“$accesslog” format.access=“%Ses->client.ip% -
%Req->vars.auth-user% [%SYSDATE%] \\”%Req->reqpb.clf-request%\\ “
%Req->srvhdrs.clf-status% %Req->srvhdrs.content-length%” ...AddLog
fn=“flex-log” name=“access”
```

ACL 快取記憶體調校

依預設，Proxy Server 將會在 ACL 使用者快取記憶體中快取使用者及群組認證結果。您可以使用 magnus.conf 檔案中的 ACLCacheLifetime 指令，控制 ACL 使用者快取記憶體的有效期限。每次參照快取記憶體中的某個項目時，都將計算其生命週期並檢查 ACLCacheLifetime。如果該項目的生命週期大於或等於 ACLCacheLifetime，則不會使用它。

ACLCacheLifetime 的預設值爲 120 秒，這表示 Proxy Server 與 LDAP 伺服器處於不同步狀態的時間，最長可長達兩分鐘。將此值設爲 0 (零) 將關閉快取記憶體，並迫使 Proxy Server 於每次使用者請求認證時都必須查詢 LDAP 伺服器。若 Proxy Server 實作存取控制，則此種設定會對 Proxy Server 的效能造成負面影響。若將 ACLCacheLifetime 設爲較大的值，則每次對 LDAP 項目進行變更時，可能都必須重新啓動 Proxy Server，因爲此種設定會迫使 Proxy Server 查詢 LDAP 伺服器。請僅在 LDAP 目錄不經常變更時，才設定一個較大的值。

ACLUserCacheSize 是 `magnus.conf` 中的一個參數，用於配置快取記憶體中可以保留的最大項目數。此參數的預設值爲 200。新的項目會增加至清單開頭，而且當快取記憶體的大小達到最大值時，位於此清單尾端的項目會回收以建立新的項目。

您也可以使用 *ACLGroupCacheSize* 參數，設定每個使用者項目可以快取的最大群組成員數。群組中非成員身分的使用者不會被快取，這將導致每個請求都要進行數個 LDAP 目錄存取。

緩衝區大小

您可以指定伺服器通訊端的傳送緩衝區 (SndBufSize) 及接收緩衝區 (RcvBufSize) 的大小。這些參數都可於 `magnus.conf` 檔案中配置。建議值會因不同的 UNIX 及 Linux 作業系統而異。請參閱作業系統文件，以正確設定這些參數。

連線逾時

您可以使用 magnus.conf 檔案中的 *AcceptTimeout* 參數，指定伺服器在關閉連線前等候資料從用戶端到達的秒數。如果逾時時間已到但資料仍未到達，連線將會關閉。此參數預設爲 30 秒。在大多數情況下，您不需要變更此設定。若將此參數值設爲低於預設值，可以釋放出一些執行緒，但卻可能會使連線速度較慢的使用者中斷連線。

錯誤記錄層級

提高 server.xml () 檔案中的 LOG 標籤的記錄層級屬性，會導致伺服器在錯誤記錄中產生並儲存更多資訊。不過，將項目寫入至該檔案會影響效能。僅在進行問題除錯時才提高記錄層級，不使用疑難排解模式時則降低記錄層級。

安全性需求

啓用 SSL 可提高 Proxy Server 的私密性與安全性，但也會影響到效能，因爲將封包加密和解密會需要經常性耗用時間。您可以考慮將加密和解密處理工作移至硬體加速卡。

Solaris 檔案系統快取

Proxy Server 快取不儲存在隨機存取記憶體中。每當從快取擷取文件時，即會向檔案系統存取檔案。您可以考慮使用 Solaris 檔案系統快取，將 Proxy Server 快取預先載入記憶體。之後只要參照已快取的檔案，就會從記憶體中擷取，而非從檔案系統擷取。

逾時值

逾時對伺服器效能的影響巨大。爲 Proxy Server 設定最合適的逾時值，有助於節省網路資源。

若要配置 Proxy Server 內的逾時值，可使用兩個針對實例的 SAF (伺服器應用程式函數) 及一個全域參數：

- 第 345 頁的 「init-proxy() SAF (obj.conf 檔案)」
- 第 346 頁的 「http-client-config() SAF (obj.conf 檔案)」
- 第 347 頁的 「KeepAliveTimeout() SAF (magnus.conf 檔案)」

init-proxy() SAF (obj.conf 檔案)

init-proxy() 函數會初始化 Proxy Server 的內部設定。Proxy Server 初始化時會呼叫此函數，但您仍然應該在 obj.conf 檔案中指定此函數，才能正確初始化各個參數值。

此函數的語法如下：

```
Init fn=init-proxy timeout=seconds timeout-2=seconds
```

在上述範例中，下列參數會直接套用至 Proxy Server 的 init-proxy SAF 逾時設定：

- timeout (代理伺服器逾時) - 代理伺服器逾時參數會告知伺服器應等待多久才能退出閒置連線。若設定較大的代理伺服器逾時值，會將有價值的代理伺服器執行緒長時間由可能已當機的用戶端佔用。 若逾時值較低，則會退出需要很長時間才產生結果的 CGI 程序檔，如資料庫查詢閘道。

  若要決定伺服器的最佳代理伺服器逾時值，請考量下列事項：

  - Proxy Server 會處理許多資料庫查詢或 CGI 程序檔嗎？
  - Proxy Server 處理的請求數目是否少到在任何給定的時間都可以有閒置的程序？

    如果對上述問題中任何一個的答案爲是，就可以決定設定較大的代理伺服器逾時值。建議設定的最高代理伺服器 *timeout* 值爲 1 小時。預設值爲 300 秒 (5 分鐘)。

    您可以存取 Server Manager 中 [Preferences] 標籤下的 [Configure System Preferences] 頁面，以檢視或修改代理伺服器逾時值。將以 [Proxy Timeout] 來參照此參數。

  timeout-2 (中斷後逾時) - 中斷後逾時值告知 Proxy Server 在用戶端退出作業事件後，要繼續寫入快取檔案多長時間。換句話說，如果 Proxy Server 快要完成文件快取時用戶端突然退出連線，伺服器仍然可以繼續快取文件，直到 timeout after interrupt 值才停止。

  建議的最高 timeout after interrupt 值爲 5 分鐘。預設值爲 15 秒。

http-client-config() SAF (obj.conf 檔案)

http-client-config 函數可配置 Proxy Server 的 HTTP 用戶端。

此函數的語法如下：

```
Init fn=http-client-config
  keep-alive=(true|false)
  keep-alive-timeout=seconds
  always-use-keep-alive=(true|false)
  protocol=HTTP Protocol
  proxy-agent="Proxy-agent HTTP request header"
```

其設定爲：

- always-use-keep-alive - (可選) 布林值，指出 HTTP 用戶端是否應嘗試使用永久性連線。預設值爲 [true]。
- keep-alive-timeout - (可選) 使永久性連線保持開啓的最大秒數。預設值爲 29。
- always-use-keep-alive - (可選) 布林值，指出 HTTP 用戶端是否可對各種請求重複使用現有的永久性連線。預設值爲 [false]，表示對於非 GET 請求或含有內文的請求將不會重複使用永久性連線。

- protocol - (可選) HTTP 協定版本字串。依預設，HTTP 用戶端將使用 HTTP/1.0 或 HTTP/1.1，視 HTTP 請求的內容而定。僅在發生特定協定的互通功能問題時，才使用 protocol 參數。
- proxy-agent - (可選) Proxy-agent HTTP 請求標頭的值。預設值爲包含 Proxy Server 產品名稱和版本的字串。

`KeepAliveTimeout()` SAF (`magnus.conf` 檔案)

`KeepAliveTimeout()` 參數決定伺服器將用戶端與 Proxy Server 之間的 HTTP 持續作用連線或永久性連線保持開啓的最長時間 (以秒爲單位)。預設爲 30 秒。如果閒置超過 30 秒，連線即逾時。最長爲 300 秒 (5 分鐘)。

注意 – `magnus.conf` 檔案中的逾時設定會套用至用戶端和 Proxy Server 之間的連線。`obj.conf` 檔案中的 `http-client-config` SAF 逾時設定則會套用至 Proxy Server 與原始伺服器之間的連線。

最新狀態檢查

Proxy Server 提升效能的方法，是從本機快取提供文件，而非從原始伺服器獲得。此方法的缺點之一是可能會提供已過時的文件。

Proxy Server 可執行檢查，確定快取中是否爲最新文件，若文件已過時，則會重新整理快取的版本。只在必要時才執行最新狀態檢查，因爲經常檢查文件會降低 Proxy Server 的整體效能。

最新狀態檢查是在 [Caching] 標籤的 [Set Cache Specifics] 頁面配置。預設值是每隔兩小時檢查是否有新文件。此資訊是在 ObjectType 指令中使用 max-uncheck 參數配置的。

若要在提昇伺服器效能的同時確保文件爲最新版本，請自訂最新狀態檢查，方法是結合 last-modified 因子來確定合理的文件使用期限。

Last-Modified 因子

Last-Modified 因子有助於根據已有記錄的先前變更來確定文件變更的可能性。

Last-Modified 因子是介於 .02 和 1.0 之間的分數。其值需乘以文件上次實際修改時間，和上次對文件執行最新狀態檢查時間兩者的間隔。將所得數字和自上次執行最新狀態檢查以來的時間做比較。如果此數字小於時間間隔，表示文件尚未過期。但是，如果此數字大於時間間隔，則表示文件已過期，並且需從原始伺服器取得新的文件版本。

Last-modified 因子可讓您確定最近變更過的文件的檢查頻率會高於舊文件的檢查頻率。

應將 Last-modified 因子設定在 0.1 和 0.2 之間。

DNS 設定

DNS 是用於在標準 IP 位址與主機名稱之間建立關聯的系統。此系統若配置不當，就會佔用有價值的 Proxy Server 資源。若要使效能最佳化，請考慮下列選項：

- 啓用 DNS 快取。

  請在 Server Manager 的 [Preferences] 標籤下選擇 [Configure DNS Cache] 連結，以啓用 DNS 快取。選取 DNS 快取的 [Enabled] 單選按鈕。
- 僅記錄用戶端 IP 位址，而非記錄用戶端 DNS 名稱。

  在 Server Manager 的 [Server Status] 標籤下選擇 [Set Access Log Preferences] 連結，可以停用用戶端 DNS 名稱記錄。選取 [IP addresses] 單選按鈕以記錄 IP 位址，而非記錄用戶端主機名稱。
- 停用反向 DNS。

  反向 DNS 會將 IP 位址轉譯爲主機名稱。在 Server Manager 的 [Preferences] 標籤下選擇 [Configure System Preferences] 連結，可以停用反向 DNS。選取 [No] 單選按鈕，以停用反向 DNS。
- 避免根據用戶端主機名稱進行存取控制

  在存取控制敘述中盡可能使用用戶端的 IP 位址，不要使用主機名稱。

執行緒數目

magnus.conf 檔案中的 RqThrottle 參數用於指定 Proxy Server 可以處理的最大同步作業事件數。預設值爲 128。變更此值即可調節伺服器，減少所執行作業事件的延遲狀況。

伺服器爲了計算同步請求數，會計算使用中的請求數目。新請求到達時伺服器會將該數字加上 1，完成請求時則會減掉 1。當新請求到達時，伺服器會檢查正在處理的請求是否到達了最大數目。如果已達到限制，則會等到使用中的請求數目低於數目上限時，才開始處理新的請求。

透過檢視 `perfdump` 所產生資料的 SessionCreationInfo 部分，或檢視 `proxystats.xml` 資料，您可以監視同步請求數目。可以透過此資訊確定與執行緒的總數 (限制) 相比，同步 (尖峰) 請求的最大數目。下列資訊取自 `perfdump` 輸出：

```
SessionCreationInfo:
------------------------
Active Sessions          1
Keep-Alive Sessions      0
Total Sessions Created   48/128
```

[Active Sessions] 顯示目前在處理請求的階段作業數目 (請求處理執行緒)。[Keep-Alive Sessions] 與 [Active Sessions] 相似，但僅限於持續作用的連線。[Total Sessions Created] 顯示已建立的階段作業數及允許的階段作業數上限。這些值分別爲 RqThrottle 值的最小值和最大值。

注意 – RqThrottleMin 是伺服器啓動時所啓動的最小執行緒數目。預設值爲 48。此參數也可以在 `magnus.conf` 檔案中設定，但依預設並不會顯示。

達到所配置的執行緒數目上限不一定是壞事。您不需要因此自動增加 RqThrottle 值。達到此限制意味著伺服器在尖峰負載期間需要這麼多數目的執行緒。只要伺服器可以及時處理請求，就表示伺服器的調校得當。不過，這個時候連線會在連線佇列等候，可能會因此造成佇列溢位。如果您的 `perfdump` 輸出經常顯示已建立的階段作業總數值常接近 RqThrottle 上限，可考慮提高執行緒限制。

合適的 RqThrottle 值應介於 100 到 500 之間，視負載而定。

傳入連線池

可以使用 magnus.conf 中的 KeepAlive* 設定及相關設定調校傳入連線池，包括下列項目：

- MaxKeepAliveConnections
- KeepAliveThreads
- KeepAliveTimeout
- KeepAliveQueryMaxSleepTime
- KeepAliveQueryMeanTime
- ConnQueueSize
- RqThrottle
- acceptorthreads

如需有關這些參數的更多資訊，請參閱「Sun ONE Web Server 6.1 SP6 *Performance Tuning, Sizing, and Scaling Guide*」的第 2 章，網址爲：

http://docs.sun.com/app/docs/doc/819-6516/

在此 Proxy Server 發行版本中無法配置傳出連線池設定。

FTP 清單寬度

提高 FTP 清單寬度可接受較長的檔案名稱，從而減少檔案名稱被截斷的情況。預設寬度爲 80 個字元。

要修改 FTP 清單寬度，請選擇 Server Manager [Preferences] 標籤下的 [Tune Proxy] 連結。

快取架構

妥善配置快取可以改善伺服器效能。架構快取時，應注意的建議事項：

- 分散負載。
- 使用多個代理伺服器快取分割區。
- 使用多台磁碟機。
- 使用多個磁碟控制器。

適當的快取設定對 Proxy Server 的效能極爲重要。在配置代理伺服器快取時需牢記的最重要的規則就是要分散負載。每個分割區可設定約 1 GB 快取記憶體，且應將其分散至多個磁碟及多個磁碟控制器。此種安排在建立及擷取檔案速度上，要比一個單獨的大型快取記憶體快許多。

快取批次更新

快取批次更新功能可讓您從指定的網站預先載入檔案，或對快取記憶體中已經存在的文件執行最新狀態檢查。通常在 Proxy Server 的負載達到最低時，才會啓動此作業。您可以在 [Cache Batch Updates] 頁面中建立、編輯及刪除 URL 批次，以及啓用與停用批次更新。

您可以指定要以批次方式更新的檔案，以便主動快取內容，而不只是在要求時才快取。Proxy Server 可讓您對快取記憶體中的多個檔案執行最新狀態檢查，或從某特定網站預先載入多個檔案。

在具有伺服器及代理伺服器網路的大型網站中，建議您以批次更新方式來預先載入 Web 的指定區域。批次處理會對文件中的連結執行遞迴下降，並將內容快取到本機上。此項功能可能會造成遠端伺服器的負擔，因此請謹慎使用。在 `bu.conf` 配置檔案中的參數可避免此程序無限期執行遞迴，並對此程序提供某種程度的控制。

請使用 Proxy Server 存取記錄來確定哪些網站最常更新，並對那些網站執行批次更新以提昇效能。

資源回收

資源回收是指檢視 Proxy Server 快取，然後移除陳舊檔案的程序。資源回收是一項密集使用資源的處理程序。因此，建議您調校一些資源回收設定，以提高其效能。

下列參數可微調資源回收程序。您可以在 Server Manager 的 [Caching] 標籤下選擇 [Tune GC]，以取得 [Tune Garbage Collection] 表單，並於此檢視或修改這些參數。 這些參數包括：

- *gc hi margin percent*
- *gc lo margin percent*
- *gc extra margin percent*
- *gc leave fs full percent*

gc hi margin percent 變數

gc hi margin percent 變數可控制快取記憶體大小百分比的上限，當達到此百分比時，就會觸發資源回收。

此值必須大於 gc lo margin percent 的值。

gc hi margin percent 的有效範圍介於 10% 到 100% 之間。預設值爲 80%，表示當快取記憶體的使用容量達到 80% 時，即會觸發資源回收。

gc lo margin percent 變數

gc lo margin percent 變數用於控制最大快取記憶體大小百分比，資源回收器以此百分比爲目標。

此值必須低於 gc hi margin percent 的值。

gc lo margin percent 的有效範圍爲 5% 到 100% 之間。預設值爲 70%。表示其目標爲資源回收後，快取記憶體使用量應該達到 70%。

gc extra margin percent 變數

如果觸發資源回收的原因不是因爲分割區的大小接近允許的大小上限 (gc hi margin percent)，則資源回收將使用 gc extra margin percent 變數設定的百分比，以決定應移除的快取部分。

gc extra margin percent 的有效範圍爲 0% 到 100% 之間。預設值爲 30%，表示會移除現有快取檔案的 30%。

gc leave fs full percent 變數

gc leave fs full percent 值決定快取分割區大小的百分比，若低於此值將不會進行資源回收。若其他應用程式獨佔了磁碟空間，此值可防止資源回收移除快取中的所有檔案。

gc leave fs full percent 的有效範圍爲 0% (允許全部移除) 到 100% (不允許移除)。預設值爲 60%，此值允許將快取大小縮減爲其現行大小的 60%。

Solaris 效能調校

Solaris 核心中有各種參數可用來微調 Proxy Server 效能。下表列出部分的參數。

表 19–1 Solaris 效能調校參數

參數	範圍	預設值	調校值	註釋
rlim_fd_max	/etc/system	1024	8192	程序開啓檔案描述元限制。應涵蓋相關通訊端、檔案及管道 (如果有的話) 的預期負載。
rlim_fd_cur	/etc/system	64	8192	
sq_max_size	/etc/system	2	0	控制串流驅動程式佇列大小。設定此參數爲 0 表示效能執行不會由於缺乏緩衝區空間而受到影響。用戶端也須設定此參數。
tcp_close_wait_interval	ndd/dev/tcp	240000	60000	用戶端也須設定此參數。
tcp_conn_req_max_q	ndd/dev/tcp	128	1024	
tcp_conn_req_max_q0	ndd/dev/tcp	1024	4096	
tcp_ip_abort_interval	ndd/dev/tcp	480000	60000	
tcp_keepalive_interval	ndd/dev/tcp	7200000	900000	對於高流量的網站，請降低此值。
tcp_rexmit_interval_initial	ndd/dev/tcp	3000	3000	如果重新傳輸作業的數量大於 30-40%，請提高此值。
tcp_rexmit_interval_max	ndd/dev/tcp	240000	10000	
tcp_rexmit_interval_min	ndd/dev/tcp	200	3000	
tcp_smallest_anon_port	ndd/dev/tcp	32768	1024	用戶端也須設定此參數。

表 19–1 Solaris 效能調校參數 *(續)*

參數	範圍	預設值	調校值	註釋
tcp_slow_start_initial	ndd/dev/tcp	1	2	少量資料的傳輸速度會稍微快一點。
tcp_xmit_hiwat	ndd/dev/tcp	8129	32768	使用此參數以提高傳輸緩衝區。
tcp_recv_hiwat	ndd/dev/tcp	8129	32768	使用此參數以提高接收緩衝區。

如需有關這些參數的更多資訊，請參閱「Sun ONE Web Server 6.1 SP6 *Performance Tuning, Sizing, and Scaling Guide*」的第 5 章，網址爲：

http://docs.sun.com/app/docs/doc/819-6516/

索引

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S