Sun Java™ System

Web Proxy Server 4 .0.1
管理指南

2005Q4

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

文件號碼：819-3163

目錄

關於本指南

本指南描述如何配置與管理 Sun Java™ System Web Proxy Server 4 (原來稱爲 Sun™ ONE Web Proxy Server 和 iPlanet™ Web Proxy Server；以下稱爲 Sun Java System Web Proxy Server，或簡稱爲 Proxy Server)。

本前言包含以下各節：

本指南適用對象

本指南適用於生產環境中的資訊技術管理員。本指南假設使用者已熟悉下列內容：

- 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

本指南架構

本指南分爲多個部分，每個部分都有其專述的特定領域和作業。下表列出了本指南的各個部分及其內容。

表 1　　指南架構

部分	描述
第 1 部分 伺服器基本原理	簡介 Proxy Server 及其管理： • 第 1 章 「Sun Java System Web Proxy Server 簡介」 • 第 2 章 「管理 Sun Java System Web Proxy Server」
第 2 部分 使用 Administration Server	提供關於配置 Administration Server 喜好設定、管理使用者與群組、保證 Proxy Server 安全以及使用叢集在伺服器之間共用配置的詳細資訊： • 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 「使用憑證和密鑰」 • 第 6 章 「管理伺服器叢集」
第 3 部分 配置和監視 Proxy Server	提供關於配置伺服器喜好設定、設定存取控制以及監視伺服器活動的詳細資訊： • 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	提供關於 Proxy Server 如何處理請求的相關概念與作業的詳細資訊： • 第 11 章 「代理與路由 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」

表 1　　指南架構

部分	描述
第 5 部分 附錄	描述存取控制清單 (ACL) 檔案語法及伺服器效能調校： • 附錄 A「ACL 檔案語法」 • 附錄 B「調校伺服器效能」

文件慣例

下表列出了本指南中使用的文件慣例。

表 2　　文件慣例

元素	用法
檔案與目錄路徑	採用 UNIX® 格式，以正斜線分隔目錄名稱。
安裝根目錄	以 *server_root* 表示。預設的安裝目錄爲 `/proxyserver4`。
術語強調	新的字彙或術語、要強調的詞。
*斜體*文字	保留未譯的新的字彙或術語以及要強調的詞、路徑中的環境變數、預留位置。
固定間距文字	代碼範例、檔案名稱、路徑名稱、指令名稱、程式設計語言關鍵字、特性。
「AaBbCc123」	用於書名及章節名稱。

相關文件

可透過下列網址取得 HTML 和 PDF 格式的 Sun Java System Web Proxy Server 4 文件：

http://docs.sun.com/app/docs/prod/s1.webproxys#hic 與
http://docs.sun.com/app/docs/prod/s1.webproxys?l=zh_TW#hic

下表列出了各指南中描述的作業和概念。

表 3　　Proxy Server 文件

需要的相關資訊	請參閱
Proxy Server 版本： • 有關軟體和文件的最新資訊 • 新功能 • 支援的平台與環境 • 系統需求 • 已知問題與解決方法	「版本說明」
執行安裝和遷移作業： • 安裝 Sun Java System Web Proxy Server • 從版本 3.6 遷移至版本 4	「Installation and Migration Guide」
執行監督與管理作業： • 使用管理介面與指令行介面 • 配置伺服器喜好設定 • 管理使用者和群組 • 監視並記錄伺服器狀態 • 使用憑證與公開密鑰加密來保護伺服器的安全 • 控制伺服器存取 • 代理與路由 URL • 快取 • 篩選內容 • 使用反向代理伺服器 • 使用 SOCKS	「管理指南」 (以及產品隨附的線上說明)
建立自訂 Netscape Server 應用程式設計介面 (NSAPI) 外掛程式	「NSAPI Developerís Guide」
編輯配置檔案	「Configuration File Reference」

連絡 Sun 技術支援

如果您在本文件中找不到所需之本產品相關技術問題的解答，請至：

http://www.sun.com/service/contacting

意見

Sun 致力於改善文件品質並歡迎您的批評與指教。若要提出您的意見，請至 http://docs.sun.com，然後按一下用於傳送意見的連結。請務必在線上表單中提供文件標題以及文件號碼。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 819-3650，完整標題爲「Sun Java System Web Proxy Server 4.0.1 2005Q4 Administration Guide」。

協力廠商文件參照

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。

伺服器基本原理

第 1 章

Sun Java System Web Proxy Server 簡介

本章對 Sun Java™ System Web Proxy Server 進行概括介紹，其中簡單說明了本發行版本的新增功能，並簡要介紹用來主控、配置和管理 Proxy Server 的基於 Web 的使用者介面。

本章包含下列小節：

關於 Sun Java System Web Proxy Server

Sun Java System Web Proxy Server 是在高效能的網際網路和企業內部網路環境中實現 HTTP 快取和加速的基礎。Proxy Server 是功能強大的系統，可快取和篩選 Web 內容並可提高網路效能，具備與整個網路基礎架構緊密整合、跨平台支援以及集中管理能力。它相當於網路流量管理員，可以高效地分發和管理資訊，進而降低網路流量，縮短使用者的等待時間。Proxy Server 還能夠爲內容分發提供安全的閘道並做爲網路流量控制點，可確保使用者能安全有效地存取網路資源。

此版本的新功能

Sun Java System Web Proxy Server 4 包括以下增強功能：

- 新式的 HTTP 核心元件
- 支援 Linux 和 Solaris™ x86 平台
- 在所有平台上支援新式的 SSL (安全通訊端層)
- 在所有平台上實作多執行緒架構
- 改進了管理介面、圖形化使用者介面，更容易管理
- 新增了 NSAPI (Netscape Server 應用程式設計介面) 篩選器
- 提高了 LDAP (簡易目錄存取協定) 效能
- 提高了延展性和效能
- 增進了內容篩選
- 實作了 `server.xml` 配置檔案

Proxy Server「版本說明」中包含有關新功能和增強功能的更多資訊，網址爲：
http://docs.sun.com/app/docs/prod/s1.webproxys#hic 與
http://docs.sun.com/app/docs/prod/s1.webproxys?l=zh_TW#hic

入門

Sun Java System Web Proxy Server 使用 Administration Server 和 Server Manager 以 Web 爲基礎的使用者介面進行管理和配置，可透過瀏覽器存取這些介面。Administration Server 用於管理系統上安裝的所有 Proxy Server 實例的共用配置，而 Server Manager 用於配置個別的伺服器實例的設定。

本節包含以下主題：

- Administration Server 簡介
- Server Manager 簡介
- 配置檔案
- 常規表示式

備註 必須在瀏覽器中啓用 cookie，才能執行配置伺服器所必需的 CGI 程式。

Administration Server 簡介

Administration Server 是一種以 Web 爲基礎的使用者介面，用來管理系統上安裝的所有 Sun Java System Web Proxy Server 實例的共用配置。

在啓動 Administration Server 後 (請參閱第 31 頁的「啓動 Administration Server」)，可啓動瀏覽器並輸入 URL 來存取 Administration Server。URL 由安裝期間指定的主機名稱和連接埠號決定。例如：`http://myserver.mycorp.com:1234`。

可以爲一個以上管理員授予存取 Administration Server 的權限。如需有關分散式管理的更多資訊，請參閱第 40 頁的「允許多個管理員」。

存取 Administration Server

1. 啓動瀏覽器並輸入 URL，此 URL 反映在安裝期間爲 Administration Server 指定的主機名稱和連接埠號碼。例如：`http://myserver.mycorp.com:1234`。
2. 出現提示時，輸入在安裝時指定的使用者名稱和密碼。將顯示 Administration Server 的使用者介面。

Administration Server 設定以對應到特定作業的標籤加以分類。下表列出 Administration Server 的標籤，並簡短說明標籤的用途。

表 1-1 Administration Server 標籤

標籤	用途
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、配置分散式管理 (允許多位管理員)、自訂和檢視存取記錄與錯誤記錄。
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	增加與管理使用者、群組和組織單元
Security	建立新的可信任資料庫、請求及安裝 VeriSign 和其他憑證、變更密鑰對檔案密碼、檢視及管理已安裝的憑證、增加或替代 CRL (憑證撤銷清單) 和 CKL (洩漏密鑰清單)、管理 CRL 和 CKL、遷移 3.x 憑證

表 1-1 Administration Server 標籤

標籤	用途
Cluster	控制叢集中的遠端伺服器、增加和移除遠端伺服器、修改伺服器訊息

無論您處在哪個標籤或頁面，都會看到以下按鈕：

- **Version** — 顯示 Sun Java System Web Proxy Server 的版本資訊
- **Refresh** — 重新整理目前頁面
- **Help** — 顯示目前頁面的說明

如需有關使用 Administration Server 的更多資訊，請參閱第 31 頁的第 2 章 「管理 Sun Java System Web Proxy Server」。另請參閱 Administration Server 各標籤和頁面的線上說明。

Server Manager 簡介

Server Manager 是一種以 Web 爲基礎的使用者介面，用於啓動、停止與配置 Sun Java System Web Proxy Server 的個別實例。

存取 Server Manager

1. 存取 Administration Server，相關說明請參閱第 27 頁的 「Administration Server 簡介」。Administration Server 會顯示 [Servers] 標籤。
2. 在 [Manage Servers] 頁面上，按一下您要管理的伺服器實例的連結。將顯示 Server Manager 使用者介面。

Server Manager 設定以對應到特定作業的標籤加以分類。下表列出 Server Manager 的標籤，並簡短說明標籤的用途。

表 1-2 Server Manager 標籤

標籤	用途
Preferences	啓動並停止伺服器、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、增加與編輯偵聽通訊端、管理 MIME 類型、管理存取控制、配置 ACL 和 DNS 快取、配置 DNS 本端子網域、配置 HTTP 持續作用設定、設定密碼大小

表 1-2　Server Manager 標籤

標籤	用途
Routing	啓用與停用 proxying、設定路由喜好設定、轉寄用戶端憑證、啓用 Java IP 位址檢查、建立與編輯自動配置檔案、設定連結模式、更改預設 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	啓動與停止 SOCKS 伺服器、建立與管理 SOCKS 認證、連線和路由項目
URLs	檢視、建立和管理 URL 對映和重新導向
Caching	設定快取細節、增加與修改快取分割區、在現有分割區之間移動區段、設定快取容量、設定資源回收模式、調校快取、資源回收排程、調校資源回收設定、配置特定資源的快取功能、啓用本地主機的快取功能、變更檔案快取設定、設定快取批次更新、檢視有關記錄的快取 URL 的資訊、配置 ICP 鄰近區域中的代理伺服器、建立與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 檔中的資訊
Filters	建立篩選檔案、設定內容 URL 重寫、設定使用者代理程式限制和請求封鎖、隱藏外送標頭、設定 MIME 篩選器和 HTML 標記篩選器、依需要壓縮內容
Server Status	檢視記錄檔、記錄歸檔、設定記錄喜好設定、產生報告、監視目前作業、配置與控制 SNMP 子代理程式
Security	建立新的可信任資料庫、請求及安裝 VeriSign 和其他憑證、變更密鑰對檔案密碼、檢視及管理已安裝的憑證、增加或替代 CRL (憑證撤銷清單) 和 CKL (洩漏密鑰清單)、管理 CRL 和 CKL、遷移 3.x 憑證
Templates	建立、移除、套用和檢視範本，並移除資源

無論您處在哪個標籤或頁面，都會看到以下按鈕：

- **Version** — 顯示 Sun Java System Web Proxy Server 的版本資訊
- **Refresh** — 重新整理目前頁面
- **Help** — 顯示目前頁面的說明

您有時也會在 [Refresh] 按鈕下看到 [Restart Required] 連結。這表示已進行了變更，爲此需要重新啓動伺服器。若要套用變更，請按此連結，然後指定所需的動作。

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

配置檔案

Sun Java System Web Proxy Server 的配置和行爲由一組配置檔案決定。在管理介面中配置的設定會在配置檔案中反映出來。這些檔案可以手動編輯。

配置檔案位於 *instance_dir*/config 目錄中，其中 *instance_dir* 是伺服器實例。config 目錄中包含可用來控制不同程式元件的各種配置檔案。配置檔案的確切數目和名稱會視已啓用或載入程式元件的不同而異。此目錄中一定包含伺服器作業所必要的四個配置檔案。下表列出四個必要的配置檔案及其內容。

表 1-3　必要的配置檔案

檔案	內容
server.xml	大部分的伺服器配置 (此版本 Proxy Server 的新功能)
magnus.conf	全域伺服器初始化資訊
obj.conf	用於處理用戶端請求的指令
mime.types	用於決定所請求資源內容類型的資訊

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

常規表示式

常規表示式可用來識別資源與配置 Proxy Server，以便以不同的方式來處理不同 URL 的請求。當您使用 Administration Server 和 Server Manager 使用者介面來執行各種作業時，可指定常規表示式。如需有關常規表示式用法的詳細資訊，請參閱第 319 頁的第 16 章 「管理範本和資源」。

第 2 章

管理 Sun Java System Web Proxy Server

本章介紹使用 Administration Server 管理 Sun Java System Web Proxy Server 的基本方法。Administration Server 是一個網路型使用者介面，用於管理、增加、移除和遷移伺服器。

本章包含下列小節：

- 啓動 Administration Server
- 停止 Administration Server
- 執行多個 Proxy Server
- 移除伺服器實例
- 從 Proxy Server 3.6 遷移

如需有關配置 Administration Server 喜好設定的詳細資訊，請參閱第 37 頁的第 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 107 頁的第 6 章 「管理伺服器叢集」。

啓動 Administration Server

本節描述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

- 至指令行中的 *server_root*`/proxy-admserv`，然後鍵入 `./start` 以啓動 Administration Server (或 `./restart` 以重新啓動 Administration Server)。

在 Windows 上啓動 Administration Server

- 使用 [開始] > [程式集] > [Sun Microsystems] > [Sun Java System Web Proxy Server 版本] > [Start Admin]

  - 或 -

  使用 [控制台] > [系統管理工具] > [服務] > [Sun Java System Web Proxy Server 4.0] > [啓動]

  - 或 -

- 至指令提示符號中的 *server_root*\proxy-admserv，然後鍵入 startsvr.bat 以啓動 Administration Server (或 ./restart 以重新啓動 Administration Server)。

啓動 Administration Server 後，只要啓動瀏覽器並輸入反映在安裝期間爲 Administration Server 指定的主機名稱和連接埠號的 URL (例如 http://myserver.mycorp.com:1234)，就可以存取它。系統將會提示您輸入使用者名稱和密碼，此兩者也都是在安裝期間指定的。

可以爲一個以上管理員授予存取 Administration Server 的權限。如需關於分散式管理的更多資訊，請參閱第 40 頁的「允許多個管理員」。

停止 Administration Server

本節描述如何在不同的平台上停止 Administration Server。如需關於啓動 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

- 存取 Administration Server，按一下 [Preferences] 標籤，按一下 [Shutdown Server] 連結，然後按一下 [OK]。

  - 或 -

- 至指令行中的 *server_root*/proxy-admserv/，然後鍵入 ./stop。

在 Windows 上停止 Administration Server

- 使用 [服務] 視窗 ([控制台] > [系統管理工具] > [服務]) 中的 Sun Java System Proxy Server 4.0 Administration Server 服務

  - 或 -

- 至指令提示符號中的 *server_root*\proxy-admserv，然後鍵入 stopsvr.bat。

執行多個 Proxy Server

若要在系統上執行多個 Proxy Server，必須安裝與配置多個伺服器實例。下列程序描述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. 提供需要的資訊，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. 如果需要的話，請按一下 [Success] 頁面上的 [Configure Your New Server] 連結，成功地增加新的伺服器實例後將會顯示該頁面。將顯示 Server Manager 介面，可使用它來配置伺服器實例。

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，因此在執行下列程序前，請確定您希望移除伺服器實例。

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. 若要進行移除，請選取 [Confirming Server Removal] 核取方塊，然後按一下 [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。將保留 3.6 伺服器，並會建立具有相同設定的新的版本 4 伺服器。如需關於將伺服器從版本 3.6 遷移至版本 4 的更多資訊，請參閱「Proxy Server Installation and Migration Guide」。另請參閱關於 Proxy Server 使用者介面中與遷移有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 77 頁的「遷移憑證」。

第 2 部分

使用 Administration Server

第 3 章

設定管理喜好設定

本章描述如何使用 Administration Server 配置管理喜好設定。必須在瀏覽器中啓用 cookie，才能執行配置伺服器所必需的 CGI 程式。

本章包含下列小節：

建立與管理偵聽通訊端

必須先由偵聽通訊端接受請求並將其導向給正確的伺服器後，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` 及在安裝期間指定爲 Administration Server 連接埠號碼的連接埠號碼。

可以使用 Administration Server 的 [Edit Listen Sockets] 頁面來增加、編輯和刪除偵聽通訊端。必須至少有一個用來存取伺服器的偵聽通訊端。如果清單中只有一個偵聽通訊端，將無法刪除它。

本節包含以下主題：

增加偵聽通訊端

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

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. 按一下想要編輯的偵聽通訊端的連結，進行想要的變更，然後按一下 [OK]。

刪除偵聽通訊端

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. 選取想要刪除的偵聽通訊端旁邊的核取方塊，然後按一下 [OK]。系統會提示您確認刪除。必須至少有一個用來存取伺服器的偵聽通訊端。如果清單中只有一個偵聽通訊端，將無法刪除它。

變更超級使用者設定

可以爲 Administration Server 配置超級使用者存取。這些設定僅影響超級使用者帳號。如果 Administration Server 使用分散式管理，則必須爲允許的管理員配置額外的存取控制。

注意 如果 Sun Java™ System Directory Server 用於管理使用者與群組，則必須**先**更新目錄中的超級使用者項目，然後才能變更超級使用者名稱或密碼。如果不先更新目錄，將無法存取 Administration Server 中的 [Users and Groups] 介面。若要修正此問題，必須使用確實可以存取此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此目錄。

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。

超級使用者的名稱與密碼保留在名爲 `admpw` 的檔案中，此檔案位於 *server_root*`/proxy-admserv/config`。此檔案的格式爲 *username*`:`*password*。可以檢視此檔案以獲得使用者名稱，但密碼是加密的，無法讀取。如果忘記了密碼，可以編輯 `admpw` 檔案，將加密密碼刪除即可。接著可以執行下列動作：

1. 在提供使用者名稱但不提供密碼的情況下存取 Administration Server。
2. 按一下 [Preferences] 標籤。
3. 按一下 [Control Superuser Access] 連結。
4. 提供新密碼，然後按一下 [OK]。

注意 由於 `admpw` 檔案是可編輯的，因此將伺服器電腦放置在安全的地點並限制對其檔案系統的存取就顯得非常重要。

在 UNIX 和 Linux 系統上，請考慮變更檔案所有權，以便僅允許超級使用者或任何執行 Administration Server 常駐程式的系統使用者寫入此檔案。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

多個管理員可以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，然後才能啓用分散式管理。預設的目錄服務必須基於 LDAP。

分散式管理有兩個層級的使用者：超級使用者和管理員。

- 超級使用者是 *server_root*/proxy-admserv/config/admpw 中列示的使用者。這是在安裝時指定的使用者名稱和密碼。此使用者擁有對 Administration Server 中除 [Users and Groups] 表單外所有表單的完全存取權限，對 [Users and Groups] 表單是否擁有存取權限要視超級使用者在 LDAP 伺服器中是否擁有有效帳號而定。
- 管理員可直接轉至特定伺服器 (包括 Administration Server) 的 Server Manager 表單。他們看到的表單取決於爲其配置的存取控制規則 (通常由超級使用者進行配置)。管理員可以執行有限的管理作業，還可以進行會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 133 頁的第 8 章 「控制對伺服器的存取」。

啓用分散式管理

1. 確認已安裝目錄伺服器。
2. 存取 Administration Server。
3. 安裝目錄伺服器後，可能還需要建立管理群組 (如果尚未建立的話)。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 administrators 群組，並增加使用者 (要授予其權限來配置 Administration Server 或在其伺服器根下安裝的任何伺服器) 的名稱。如需有關特定欄位的更多資訊，請參閱線上說明。

      administrators 群組中的所有使用者都擁有對 Administration Server 的完全存取權限，但可以使用存取控制來限制允許他們配置的伺服器和表單。

      一旦建立了存取控制清單，便會將分散式管理群組增加至此清單中。如果 administrators 群組的名稱發生了變更，必須手動編輯存取控制清單以變更其參照的群組。
4. 按一下 [Preferences] 標籤。
5. 按一下 [Configure Distributed Administration] 連結。
6. 選取 [Yes] 以指定管理員群組，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關於伺服器存取的資訊。檢視這些記錄可以讓您監視伺服器活動和排解問題。Administration Server 記錄中記錄的資料類型與格式是透過 [Log Preferences] 頁面中的許多選項指定的。可以選擇 [Common Logfile Format] (提供固定數量的關於伺服器的資訊)，也可以建立可更好地滿足需求的自訂記錄檔格式。

若要存取 Administration Server 的 [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 163 頁的第 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。可以透過 Proxy Server 管理主控台或是使用文字編輯器來檢視錯誤與存取記錄。

存取記錄檔

存取記錄檔記錄關於傳送給伺服器的請求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 163 頁的第 9 章 「使用記錄檔」。

錯誤記錄檔

錯誤記錄列示了自建立記錄檔以來伺服器遇到的所有錯誤。它還包含關於伺服器的資訊訊息，如啓動伺服器的時間及嘗試登入伺服器卻遭到失敗的使用者。

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 163 頁的第 9 章 「使用記錄檔」。

使用目錄服務

可以使用 LDAP 在單一目錄伺服器中儲存與管理使用者名稱和密碼等資訊。也可以將伺服器配置爲允許使用者從多個可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 43 頁的第 4 章 「管理使用者和群組」。

限定伺服器存取

當 Proxy Server 評估內送請求時，會根據名爲存取控制項目 (ACE) 的階層結構規則來確定是否允許存取，然後會使用相符的項目來確定是應該允許還是應該拒絕此請求。每個 ACE 都會指定伺服器是否應該繼續檢查階層結構中的下一個 ACE。ACE 的集合稱爲存取控制清單 (ACL)。

可以針對是存取 Administration Server 還是伺服器實例中的特定資源 (如檔案、目錄及檔案類型) 來配置存取控制。在 Administration Server 的 [Global Settings] 標籤中配置對 Administration Server 的存取控制。在 Server Manager 的 [Preferences] 標籤中配置對伺服器實例中資源的存取控制。如需有關設定存取控制的更多資訊，請參閱第 133 頁的第 8 章 「控制對伺服器的存取」。

備註 必須先啓用分散式管理，才能限定伺服器存取。如需更多資訊，請參閱第 40 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。透過使用子代理程式和主代理程式，在網路管理工作站與伺服器之間傳送此資訊。

使用 Administration Server 中的 [Global Settings] 標籤配置 SNMP 主代理程式設定。主代理程式隨附 Administration Server 一同安裝。如需有關 SNMP 和代理程式設定的詳細資訊，請參閱第 187 頁的第 10 章 「監視伺服器」。另請參閱關於 Administration Server 的 [Global Settings] 標籤中主代理程式頁面以及 Server Manager 的 [Server Status] 標籤中子代理程式頁面的線上說明。

第 4 章

管理使用者和群組

本章描述如何增加、刪除、修改與管理能夠存取 Proxy Server 的使用者與群組。

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特定資訊和群組特定資訊的應用程式資料。

使用者和群組資訊儲存在文字格式的平面檔案中，或者儲存在支援 LDAP (簡易目錄存取協定) 的目錄伺服器 (如 Sun Java™ System Directory Server) 中。LDAP 是一個在 TCP/IP (傳輸控制協定 / 網際網路協定) 上執行的開放式目錄存取協定，可將其擴充到全域大小，包含上百萬個項目。

關於目錄服務

目錄服務使得所有使用者資訊都能夠透過單一來源進行管理。使用 Proxy Server 可以配置三種不同類型的目錄服務：LDAP、密鑰檔和摘要檔。

如果未配置任何其他目錄服務，則不管新建的第一個目錄服務類型爲何，均會將其值設定爲 `[default]`。建立目錄服務時，會以目錄服務詳細資訊更新 *server_root*`/userdb/dbswitch.conf` 檔案。

本節包含以下主題：

LDAP 目錄服務

使用 LDAP 目錄服務時，使用者與群組資訊儲存在基於 LDAP 的目錄伺服器中。

如果 LDAP 服務爲預設服務，則會如以下範例所示更新 `dbswitch.conf` 檔案：

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

如果 LDAP 服務爲非預設服務，則會如以下範例所示更新 `dbswitch.conf` 檔案：

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

密鑰檔目錄服務

密鑰檔是一個文字檔，包含雜湊格式的使用者密碼以及使用者所屬群組的清單。密鑰檔格式僅當意在使用 HTTP 基本認證時才可使用。如需關於認證方法的更多資訊，請參閱第 148 頁的「指定使用者和群組」。

建立基於密鑰檔的資料庫時，會如以下範例所示更新 dbswitch.conf 檔案：

```
directory keyfile file
keyfile:syntax keyfile
keyfile:keyfile D:\test22\keyfile\keyfiledb
```

摘要檔目錄服務

摘要檔基於加密的使用者名稱和密碼儲存使用者和群組資訊。

摘要檔格式的目的是支援 HTTP 摘要認證的使用，但它同時也支援基本認證，因此可在這兩種認證方法中使用。如需關於這些方法的更多資訊，請參閱第 148 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 file
digest:syntax digest
digest:digestfile D:\test22\digest\digestdb
```

備註 若要配置分散式管理，預設的目錄服務必須是基於 LDAP 的目錄服務。

配置目錄服務

目錄服務是在 Administration Server 的 [Global Settings] 標籤中建立與配置的。而使用者、群組和組織單元則是在 Administration Server 的 [Users and Groups] 標籤中建立與管理。

本節包含以下主題：

- 建立目錄服務
- 編輯目錄服務

建立目錄服務

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] 下拉式清單選取要建立的目錄服務的類型，然後按一下 [New]。將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 如果未配置任何其他目錄服務，則不管新建的第一個目錄服務類型爲何，均會將其值設定爲 `[default]`。

編輯目錄服務

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. 按一下想要編輯的目錄服務的連結，進行想要的變更，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] 標籤用於建立或修改使用者、群組和組織單元。使用者是 LDAP 資料庫中的個人，例如公司的員工。群組是共用某個共用屬性的兩個或更多個使用者。組織單元是組織內的分部，它使用 `organizationalUnit` 物件類別。本章後面對使用者、群組和組織單元有更詳盡的描述。

企業內的每個使用者和群組均由一個辨別名稱 (DN) 屬性表示。DN 屬性是一個包含所關聯使用者、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，就需要使用 DN。例如，每當建立或修改目錄項目、配置存取控制以及爲應用程式 (例如郵件或出版) 配置使用者帳號時，都必須提供 DN 資訊。Proxy Server 的 [Users and Groups] 介面用來建立或修改 DN。

以下範例表示 Sun Microsystems 公司某位員工的典型 DN：

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

此範例中的縮寫代表下列意義：

- `uid` 代表使用者 ID
- `e` 代表電子郵件地址

- cn 代表使用者的一般名稱
- o 代表組織
- c 代表國家

DN 可以包括各種名稱-值對，它們用於識別支援 LDAP 的目錄中的憑證主體和項目。

使用 LDIF

如果目前沒有目錄，或要在現有目錄中增加新的子樹，則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，並且會嘗試使用 LDIF 項目建立目錄或新的子樹。還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的目錄的 LDIF 格式檔案。可以使用 `ldapmodify` 指令行公用程式 (如果可用) 及相應的 LDIF 更新敘述來增加或編輯條目。

若要使用 LDIF 將項目增加至資料庫，請先在 LDIF 檔案中定義項目，然後從目錄伺服器匯入 LDIF 檔案。

建立使用者

Administration Server 中的 [Users and Groups] 標籤用於建立和修改使用者項目。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 請確保使用者不會在未經授權的情況下存取資源，從而保證伺服器的安全。Proxy Server 使用基於 ACL 的授權與認證模型。如需有關基於 ACL 的安全性的更多資訊，請參閱第 133 頁的第 8 章 「控制對伺服器的存取」。如需附加的安全性資訊，另請參閱第 69 頁的第 5 章 「使用憑證和密鑰」。

本節包含以下主題：

- 在基於 LDAP 的認證資料庫中建立使用者
- 在密鑰檔認證資料庫中建立使用者
- 在摘要檔認證資料庫中建立使用者

在基於 LDAP 的認證資料庫中建立使用者

將使用者項目增加至基於 LDAP 的目錄服務時，會使用基於 LDAP 的基礎目錄伺服器的服務來認證和授權使用者。本節列出了在使用基於 LDAP 的認證資料庫時應該考量的指導原則，並描述了如何透過 Proxy Server Administration Server 增加使用者。

建立基於 LDAP 的使用者項目的指導原則

使用 Proxy Server 管理主控台在基於 LDAP 的目錄服務中建立新使用者項目時，請考量下列指導原則：

- 輸入名字和姓氏時將自動填入使用者的全名和使用者 ID。使用者 ID 由使用者名字的第一個首字母及其後跟隨的使用者姓氏構成。例如，如果使用者名稱爲 Billie Holiday，則使用者 ID 自動設定爲 `bholiday`。如果您願意，可以用自己選擇的 ID 取代此使用者 ID。
- 使用者 ID 必須是唯一的。Administration Server 確定使用者 ID 是否唯一的方法是，從搜尋基底 (基底 dn) 向下搜尋整個目錄，以確定此使用者 ID 是否處於使用中。但請注意，如果使用目錄伺服器的 `ldapmodify` 指令行公用程式 (如果可用) 建立使用者，則不能確保使用者 ID 的唯一性。如果目錄中存在重複的使用者 ID，受影響的使用者將不能認證到目錄。
- 基底 dn 指定的辨別名稱是依預設執行目錄查找的位置，也是目錄樹中放置所有 Proxy Server Administration Server 項目的位置。DN 是表示目錄伺服器中項目名稱的字串。
- 建立新的使用者項目時，必須至少指定下列使用者資訊：
  - 姓氏
  - 全名
  - 使用者 ID
- 如果爲目錄定義了任何組織單元，則可以在 Administration Server 中使用 [Create User] 頁面上的 [Add New User To] 清單指定要放置新使用者的位置。預設的位置爲目錄的基底 dn (或稱根點)。

建立基於 LDAP 的使用者項目

若要建立使用者項目，請閱讀以下一節中概述的指導原則：第 48 頁的 「建立基於 LDAP 的使用者項目的指導原則」，然後執行下列程序。

在基於 LDAP 的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. 從下拉式清單選取 LDAP 目錄服務，然後按一下 [Select]。
4. 在顯示的頁面上輸入資訊。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 49 頁的「Directory Server 使用者項目」。
5. 按一下 [Create] 以建立使用者項目，或是按 [Create and Edit] 建立使用者項目並進入剛才建立項目的編輯頁面。

Directory Server 使用者項目

關於目錄伺服器使用者項目的備註：

- 使用者項目使用 `inetOrgPerson`、`organizationalPerson` 和 `person` 物件類別。
- 依預設，使用者辨別名稱的格式如下：

  `cn=`*full name*`,ou=`*organization*`, . . . ,o=`*base organization*`,c=`*country*

  例如，如果 Billie Holiday 的使用者項目建立於組織單元 Marketing 內，而且目錄的基底 dn 爲 `o=Ace Industry, c=US`，則使用者的 DN 爲：

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

  但要注意的是，此格式可以變更爲基於使用者 ID (uid) 的辨別名稱。
- 使用者表單欄位上的值會以 LDAP 屬性的形式儲存。

  下表列出了在 Proxy Server 介面中建立新使用者時顯示的欄位與對應的 LDAP 屬性。

表 4-1 LDAP 屬性 — 建立使用者項目

使用者欄位	LDAP 屬性
[Given Name]	`givenName`
[Surname]	`sn`
[Full Name]	`cn`
[User ID]	`uid`
[Password]	`userPassword`
[E-mail Address]	`mail`

下表列出了編輯使用者項目時還會顯示的欄位與對應的 LDAP 屬性。

表 4-2 LDAP 屬性 — 編輯使用者項目

使用者欄位	LDAP 屬性
[Title]	`title`
[Phone Number]	`telephoneNumber`

在密鑰檔認證資料庫中建立使用者

密鑰檔是一個文字檔，包含雜湊格式的使用者密碼以及使用者所屬群組的清單。

在密鑰檔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. 從下拉式清單選取基於密鑰檔的目錄服務，然後按一下 [Select]。
4. 在顯示的頁面中輸入資訊，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。

在摘要檔認證資料庫中建立使用者

摘要檔認證資料庫以加密形式儲存使用者與群組資訊。

在摘要檔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. 從下拉式清單選取基於摘要檔的目錄服務，然後按一下 [Select]。
4. 在顯示的頁面中輸入資訊，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 144 頁的「設定存取控制」。

管理使用者

使用者屬性透過 Administration Server 的 [Users and Groups] 標籤上的 [Manage Users] 頁面進行編輯。可以在此頁面中查找、變更、重新命名及刪除使用者項目。

本節包含以下主題：

尋找使用者資訊

編輯使用者項目之前，必須先依下列程序所述找出並顯示項目。

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. 從下拉式清單選取目錄服務，然後按一下 [Select]。如果是密鑰檔或摘要檔目錄服務，會顯示使用者清單。如果是基於 LDAP 的目錄服務，會顯示搜尋欄位。
4. 查找使用者資訊：

   如果是密鑰檔或摘要檔目錄服務，請按一下使用者的連結以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。

   如果是基於 LDAP 的目錄服務，請執行以下步驟：

   a. 在 [Find User] 欄位中，爲要編輯的項目輸入描述值。可以輸入任何下列內容：

      - 名稱。輸入完整或部分名稱。將傳回所有完全符合搜尋字串的項目。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。如果僅輸入部分使用者 ID，則將傳回包含此字串的所有項目。
      - 電話號碼。如果僅輸入部分號碼，則將傳回包含以搜尋號碼結尾的電話號碼的所有項目。

- 電子郵件地址。任何包含 @ 符號的搜尋字串均被假設爲電子郵件地址。如果找不到完全相符項，將執行搜尋來傳回以搜尋字串開始的所有電子郵件地址。
- 使用星號 (*) 可以傳回目前目錄中的所有項目。將欄位保留爲空白也有同樣的作用。
- 任意 LDAP 搜尋篩選器。任何包含等號 (=) 的字串均被視爲搜尋篩選器。

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的範圍。如需更多資訊，請參閱第 52 頁的「建立自訂搜尋查詢」。

b. 在 [Look Within] 欄位中，選取要在其下搜尋項目的組織單元。預設爲目錄的根點 (最上面的項目)。

c. 在 [Format] 欄位中，指定是將輸出設定爲適於在螢幕上顯示的格式還是適於印表機列印的格式。

d. 在此程序的任何階段中按一下 [Find] 按鈕，將顯示符合搜尋條件的所有使用者。

e. 按一下想要顯示的項目的連結。

建立自訂搜尋查詢

對於 LDAP 服務，[Find All Users Whose] 區段讓您可以建立自訂搜尋篩選器。使用這些欄位可以縮小 [Find User] 搜尋傳回的搜尋結果的範圍。

左側的下拉式清單可指定搜尋所基於的屬性。下表列出了可用的搜尋屬性選項。

表 4-3 搜尋屬性選項

選項	搜尋符合項
[Full name]	每個項目的全名
[Last name]	每個項目的姓氏
[User 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

中間的下拉式清單可指定要執行的搜尋類型。下表列出了可用的搜尋類型選項。

表 4-4 搜尋類型選項

選項	描述
[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，如果知道使用者名稱可能包含「Dylan」一詞，請將此選項與搜尋字串「Dylan」一同使用來尋找使用者項目。
[Is]	導致執行完全相符搜尋 (指定等同搜尋)。如果知道使用者屬性的準確值，請使用此選項。例如，知道使用者名稱的確切拼寫。
[Isn't]	傳回屬性值不完全符合搜尋字串的所有項目。使用此選項尋找目錄中名稱不是「John Smith」的所有使用者。請注意，使用此選項可能導致傳回極多項目。
[Sounds like]	導致執行近似或音似搜尋。如果知道屬性值但不清楚其拼寫方式，請使用此選項。例如，不清楚使用者的名稱拼寫是「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始的所有項目。例如，知道使用者名稱以「Miles」開頭，但不知道名稱的其餘部分。
[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，知道使用者名稱以「Dimaggio」結尾，但不知道名稱的其餘部分。

右側的文字欄位用來輸入搜尋字串。若要顯示在 [Look Within] 欄位中指定之目錄中包含的所有使用者項目，請輸入星號 (*) 或保留此欄位爲空白。

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. 如以下一節中所述顯示使用者項目：第 51 頁的「尋找使用者資訊」。
4. 依需要進行變更。如需有關特定欄位的更多資訊，請參閱線上說明。

備註 可能想要變更編輯使用者頁面未顯示的屬性值。在此情形下，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 54 頁的「重新命名使用者」。

管理使用者的密碼

下列程序描述如何變更或建立使用者密碼。

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. 如以下一節中所述顯示使用者項目：第 51 頁的「尋找使用者資訊」。
4. 依需要進行變更。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，還可以在用於編輯使用者密碼資訊的頁面 (可從 [Manage Users] 頁面存取) 上按一下 [Disable Password] 按鈕來停用使用者的密碼。這樣做可防止使用者登入伺服器，而又不必刪除其目錄項目。輸入新密碼即可再次授予使用者存取權限。

重新命名使用者

對於 LDAP 資料庫，重新命名功能僅會變更使用者 ID，所有其他欄位均保持不變。無法使用重新命名功能將某個組織單元內的項目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. 如以下一節中所述顯示使用者項目：第 51 頁的「尋找使用者資訊」。
4. 按一下 [edit user] 頁面上的 [Rename User] 按鈕，在顯示的頁面上輸入使用者 ID，然後按一下 [Save Changes]。

備註 可以指定透過將 `keepOldValueWhenRenaming` 參數設定爲 `false` (預設值) 來重新命名項目後 Administration Server 不再保留舊有的值。此參數可以在下列檔案中找到：

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. 如以下一節中所述顯示使用者項目：第 51 頁的「尋找使用者資訊」。
4. 按一下 [Delete User] (LDAP) 或 [Remove User] (密鑰檔與摘要檔)。

建立群組

群組是描述 LDAP 資料庫中物件集的物件。Sun Java System 伺服器群組由共用某個一般屬性的使用者組成。例如，物件集可能是在公司行銷部門工作的一些員工。這些員工可能屬於稱爲 Marketing 的群組。

對於 LDAP 服務，定義群組成員身份的方式有兩種：靜態和動態。靜態群組明確列舉其成員物件。靜態群組是一個一般名稱 (CN)，它包含 `uniqueMembers` 和 / 或 `memberURLs` 和 / 或 `memberCertDescriptions`。靜態群組的成員並不共用某個一般屬性，但 `cn=`*groupname* 屬性除外。

動態群組可讓您使用 LDAP URL 來定義僅與群組成員比對的規則集。動態群組的成員共用在 `memberURL` 篩選器中定義的某個一般屬性或屬性集。例如，如果需要一個包含 Sales 部門所有員工的群組，而這些員工已經存在於 LDAP 資料庫中 `ou=Sales,o=Airius.com` 底下，則需要定義擁有下列成員 URL 的動態群組：

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

結果是此群組將包含在樹中 `ou=Sales,o=sun` 點之下具有 `uid` 屬性的所有物件，即所有 Sales 部門成員。

對於靜態和動態群組，如果使用 `memberCertDescription`，則其成員可以從憑證共用一般屬性。請注意，只有在 ACL 使用 SSL 方法時才適用。

建立新群組後即可在其中增加使用者 (成員)。

本節包含以下主題：

- 關於靜態群組
- 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。除非將使用者增加至群組或刪除群組中的使用者，否則靜態群組不會變更。

建立靜態群組的指導原則

使用 Administration Server 介面建立新靜態群組時，請考量下列指導原則：

- 靜態群組可以包含其他靜態或動態群組。
- 如果爲目錄定義了組織單元，則可以在 Administration Server 介面中使用 [Create Group] 頁面上的 [Add New Group To] 清單指定要放置新群組的位置。預設位置爲目錄的根點 (最上面的項目)。
- 如需有關編輯群組的更多資訊，請參閱第 61 頁的 「編輯群組項目」。

建立靜態群組

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] 下拉式清單選取 [New Group]，然後按一下 [Go]。
4. 輸入有關 [Create Group] 頁面的資訊。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，或是按 [Create and Edit] 建立群組並進入剛才建立群組的編輯頁面。

關於動態群組

對於 LDAP 服務，如果想要自動基於任意屬性將使用者分組，或者想要將 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，可以建立一個群組，此群組自動包括含有 `department=marketing` 屬性的所有 DN。如果套用 `department=marketing` 搜尋篩選器，搜尋將傳回一個群組，其中包括含有 `department=marketing` 屬性的所有 DN。接著可以使用基於此篩選器所得到的搜尋結果定義動態群組。進而可以爲結果動態群組定義 ACL。

如何實作動態群組

Proxy Server 在 LDAP 伺服器模式中以 `objectclass=groupOfURLs` 方式實作動態群組。`groupOfURLs` 類別可以有零個或更多個 `memberURL` 屬性，每個屬性都是一個 LDAP URL，用來描述目錄中的一個物件集。群組成員將是這些物件集的併集。例如，以下群組僅包含一個成員 URL：

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

此範例描述由 `o=mcom.com` 下部門爲 `marketing` 的所有物件組成的集合。LDAP URL 可包含搜尋基底 DN、範圍和篩選器，但不能包含主機名稱和連接埠。這意味著僅能參考同一 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 58 頁的 「建立動態群組的指導原則」。

將自動包括 DN，而無須向群組中逐個增加。群組會動態變更，這是因爲每次 ACL 驗證需要群組查找時，Proxy Server 均會執行 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 到 LDAP 資料庫的對映在 `dbswitch.conf` 檔案 (它將 ACL 資料庫名稱與實際的 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，如果想要讓名爲 `staff` 群組中的成員身份具有基準存取權限，ACL 代碼會查找物件類別爲 `groupOf`*anything* 且 CN 的設定爲 `staff` 的物件。物件定義群組成員的方式有兩種：明確列舉成員 DN (對靜態群組的 `groupOfUniqueNames` 做法即如此)，或者指定 LDAP URL (例如，`groupOfURLs`)。

備註	群組可以同時爲靜態與動態。群組物件可以同時擁有 `objectclass=groupOfUniqueMembers` 和 `objectclass=groupOfURLs`。因此，`uniqueMember` 和 `memberURL` 屬性均有效。群組的成員身份是其靜態成員和動態成員的併集。

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。如果正在測試群組成員身份，而 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 確定每個 `memberURL` 是否符合的方法是將其基底 DN 和範圍與使用者 DN 做比對，然後使用使用者 DN 作爲基底 DN 並以 `memberURL` 爲篩選器來執行基底搜尋。此程序會包括大量的個別搜尋。

建立動態群組的指導原則

使用 Administration Server 介面建立新的動態群組時，請考量下列指導原則：

- 動態群組不能包含其他群組。
- 使用以下格式 (不含主機和連接埠資訊，因爲這些參數會被忽略) 輸入群組的 LDAP URL：

  `ldap:///`*`base_dn`*`?`*`attributes`*`?`*`scope`*`?(`*`filter`*`)`

  下表列出了 LDAP URL 所需要的參數。

表 4-5 LDAP URL 需要的參數

參數名稱	描述
`base_dn`	搜尋基底的 DN 或 LDAP 目錄中所有搜尋的起始點。此參數經常被設定爲目錄的字尾或根，例如 `o=mcom.com`。
`attributes`	搜尋傳回的屬性清單。若要指定一個以上的屬性，請使用逗號分隔這些屬性 (例如 `cn,mail,telephoneNumber`)。如果未指定任何屬性，則傳回所有屬性。動態群組成員身份檢查將忽略此參數。
`scope`	此參數是必需的。 搜尋的範圍，可以是下列值之一： • `base` 僅擷取關於在 URL 中指定的辨別名稱 (`base_dn`) 的資訊。 • `one` 僅擷取關於在 URL 中指定的辨別名稱 (`base_dn`) 下一級項目的資訊。此範圍不包括基準項目。 • `sub` 僅擷取關於在 URL 中指定的辨別名稱 (`base_dn`) 下所有層級項目的資訊。此範圍包括基準項目。
`(filter)`	此參數是必需的。 套用至搜尋指定範圍內項目的搜尋篩選器。如果使用的是 Administration Server 介面，則必須指定此屬性。必須帶有括號。

`attributes`、`scope` 和 (`filter`) 參數是依據它們在 URL 中的位置進行識別的。即使不想指定任何屬性，仍必須加入問號 (?) 來分隔此欄位。

繼續介紹建立動態群組的指導原則：

- 如果爲目錄定義了組織單元，則可以在 Administration Server 介面中使用 [Create Group] 頁面上的 [Add New Group To] 清單指定要放置新群組的位置。預設位置爲目錄的根點 (最上面的項目)。
- 如需有關編輯群組的更多資訊，請參閱第 61 頁的 「編輯群組項目」。

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] 下拉式清單選取 [Dynamic Group]，然後按一下 [Go]。
4. 輸入有關 [Create Group] 頁面的資訊。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，或是按 [Create and Edit] 建立群組並進入剛才建立群組的編輯頁面。

管理群組

對於 LDAP 服務，Administration Server 可使您藉由 Administration Server 的 [Users and Groups] 標籤上的 [Manage Groups] 頁面編輯群組和管理群組成員身份。

本節包含以下主題：

尋找群組項目

編輯群組項目之前，必須先依下列程序所述找出並顯示項目。

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] 欄位中輸入要尋找的群組的名稱。可以輸入任何下列內容：
   - 名稱。輸入完整或部分名稱。將傳回所有完全符合搜尋字串的項目。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 (*) 可以傳回目前目錄中的所有群組。將欄位保留爲空白也有同樣的作用。
   - 任意 LDAP 搜尋篩選器。任何包含等號 (=) 的字串均被視爲搜尋篩選器。

   也可以使用 [Find All Groups Whose] 區段建立自訂搜尋篩選器，縮小搜尋結果的範圍。如需更多資訊，請參閱第 60 頁的 「[Find All Groups Whose] 區段」。
4. 在 [Look Within] 欄位中，選取要在其下搜尋項目的組織單元。預設爲目錄的根點 (最上面的項目)。
5. 在 [Format] 欄位中，指定是將輸出設定爲適於在螢幕上顯示的格式還是適於印表機列印的格式。
6. 在此程序的任何階段中按一下 [Find] 按鈕，將顯示符合搜尋條件的所有群組。
7. 按一下想要顯示的項目的連結。

[Find All Groups Whose] 區段

對於 LDAP 服務，[Find All Groups Whose] 區段可讓您建立自訂搜尋篩選器。使用本區段中的欄位可以縮小由 [Find Group] 傳回的搜尋結果的範圍。

左側的下拉式清單可指定搜尋所基於的屬性。下列選項可供選用：

- **Name**。搜尋每個項目的完整名稱以確定符合項。
- **Description**。搜尋每個群組項目的描述以確定符合項。

中間的下拉式清單可指定要執行的搜尋類型。下列選項可供選用：

- **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，如果知道群組名稱可能包含 「Administrator」一詞，請將此選項與搜尋字串 「Administrator」一同使用來尋找群組項目。

- **Is。**導致執行完全相符搜尋。知道群組屬性的準確值時，請使用此選項。例如，知道群組名稱的確切拼寫。
- **Isn't。**傳回屬性值不完全符合搜尋字串的所有項目。如果要在目錄中尋找名稱不包含「administrator」的所有群組，請使用此選項。但請注意，使用此選項可能導致傳回極多項目。
- **Sounds like。**導致執行近似或音似搜尋。如果知道屬性值但不確定其拼寫，請使用此選項。例如，不知道群組名稱的拼法是「Sarret's list」、「Sarette's list」或是「Sarett's list」。
- **Starts with。**導致執行子字串搜尋。傳回屬性值以指定搜尋字串開始的所有項目。例如，知道群組名稱以「Product」開頭，但不知道名稱的其餘部分。
- **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，知道群組名稱以「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

本程序僅適用於 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. 如以下一節中所述找到要編輯的群組：第 60 頁的「尋找群組項目」。
4. 依需要進行變更。如需有關特定欄位和按鈕的更多資訊，請參閱線上說明。

備註	可能想要變更群組編輯頁面未顯示的屬性值。在此情形下，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

向群組增加成員

本程序僅適用於 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. 如以下一節中所述找到並顯示要管理的群組：第 60 頁的「尋找群組項目」，然後按一下 [Group Members] 旁邊的 [Edit] 按鈕。任何現有群組成員都將列在顯示的頁面中。還會顯示搜尋欄位。
   - 若要向成員清單中增加使用者項目，必須在 [Find] 下拉式清單中選取使用者。
   - 若要將群組項目增加至群組，必須選取 [Groups]。
4. 在 [Matching] 文字欄位中輸入搜尋字串。輸入下列任何一個選項：
   - 名稱。輸入完整或部分名稱。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。如果僅輸入部分使用者 ID，則將傳回包含此字串的所有項目。
   - 電話號碼。如果僅輸入部分號碼，則將傳回包含以搜尋號碼結尾的電話號碼的所有項目。
   - 電子郵件地址。任何包含 @ 符號的搜尋字串均被假設爲電子郵件地址。如果找不到完全相符項，將執行搜尋來傳回以搜尋字串開始的所有電子郵件地址。
   - 在此欄位中輸入星號 (*) 或者保留此欄位爲空，可以傳回目前位於目錄中的所有項目或群組。
   - 任意 LDAP 搜尋篩選器。任何包含等號 (=) 的字串均被視爲搜尋篩選器。
5. 按一下 [Add] 以尋找 LDAP 資料庫中的所有符合項目，然後將它們增加至群組。如果搜尋傳回任何不想增加至群組的項目，請按一下 [Remove From List] 欄中對應的核取方塊。(請注意，也可以建構一個搜尋篩選器以尋找要從群組中移除之項目，然後按一下 [Remove]。如需更多資訊，請參閱第 63 頁的「從群組成員清單中移除項目」。)
6. 完成群組成員清單後，按一下 [Save Changes]。項目會新增至群組成員清單。

將群組增加至群組成員清單

對於 LDAP 服務，可將群組 (而不是個別成員) 增加至群組的成員清單。這樣做會使屬於所包括群組的所有使用者都成爲接收群組的成員。例如，如果 Neil Armstrong 是「Engineering Managers」群組的成員，並使「Engineering Managers」群組成爲「Engineering Personnel」群組的成員，則 Neil Armstrong 也將成爲「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 62 頁的「增加群組成員」。

從群組成員清單中移除項目

本程序僅適用於 LDAP 服務。

若要移除群組成員清單中的項目

1. 存取 Administration Server，然後按一下 [Users and Groups] 標籤。
2. 按一下 [Manage Groups] 連結。
3. 如以下一節中所述找到要管理的群組：第 60 頁的「尋找群組項目」，然後按一下 [Group Members] 旁邊的 [Edit] 按鈕。
4. 爲要從清單中移除的每個成員按一下 [Remove From List] 欄中的相應核取方塊。也可以建構一個搜尋篩選器以尋找要從群組中移除之項目，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 62 頁的「增加群組成員」。
5. 按一下 [Save Changes]。項目即會從群組成員清單中刪除。

管理所有者

對於 LDAP 服務，管理群組所有者清單的方式與管理群組成員清單的方式相同。

下表列出了本指南中可提供更多資訊的主題。

表 4-6 管理所有者

若要	請參閱
將所有者增加至群組	第 62 頁的「增加群組成員」
將群組增加至所有者清單	第 63 頁的「將群組增加至群組成員清單」

表 4-6 管理所有者

若要	請參閱
從所有者清單移除項目	第 63 頁的「從群組成員清單中移除項目」

管理「另請參閱」

「另請參閱」是對可能與目前群組相關的其他目錄項目的參照。它們可讓使用者容易地找到與目前群組相關的使用者或其他群組的項目。可以像管理群組成員清單那樣管理「另請參閱」。

下表列出了本指南中可提供更多資訊的主題。

表 4-7 管理「另請參閱」

若要	請參閱
將使用者增加至「另請參閱」	第 62 頁的「增加群組成員」
將群組增加至「另請參閱」	第 63 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 63 頁的「從群組成員清單中移除項目」

重新命名群組

本程序僅適用於 LDAP 服務。重新命名群組項目時，只有群組名稱會變更。無法使用 [Rename Group] 功能將某個組織單元內的項目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，可以將群組從 Online Sales 重新命名爲 Internet Investments，但不能如此重新命名：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，如以下一節中所述找到要管理的群組：第 60 頁的「尋找群組項目」。

3. 按一下 [Rename Group] 按鈕，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

本程序僅適用於 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. 如第 60 頁的「尋找群組項目」中所述找到想要管理的群組，然後按一下 [Delete Group]。

備註	不會移除群組的個別成員，而只會移除群組項目。

建立組織單元

對於 LDAP 服務，組織單元可以包括許多群組，它通常代表分部、部門或其他獨立的實體。DN 可以存在於一個以上組織單元中。

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。

關於組織單元的備註：

- 使用 `organizationalUnit` 物件類別建立新的組織單元。
- 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*

例如，如果在 West Coast 組織單元中建立了一個稱爲 Accounting 的新組織，而基底 dn 爲 `o=Ace Industry,c=US`，則新組織單元的 DN 將爲：

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

管理組織單元

對於 LDAP 服務，組織單元透過 Administration Server 的 [Users and Groups] 標籤的 [Manage Organizational Units] 頁面進行編輯與管理。

本節包含以下主題：

尋找組織單元

本程序僅適用於 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] 欄位中輸入要尋找單元的名稱。可以輸入任何下列內容：
   - 名稱。輸入完整或部分名稱。將傳回所有完全符合搜尋字串的項目。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 (*) 可以傳回目前目錄中的所有群組。將欄位保留爲空白也有同樣的作用。
   - 任意 LDAP 搜尋篩選器。任何包含等號 (=) 的字串均被視爲搜尋篩選器。

   也可以使用 [Find All Units Whose] 區段的下拉式功能表來縮小搜尋結果的範圍。如需更多資訊，請參閱第 67 頁的「[Find All Units Whose] 區段」。
4. 在 [Look Within] 欄位中，選取要在其下搜尋項目的組織單元。預設值爲目錄的根點 (最上面的項目)。
5. 在 [Format] 欄位中，指定是將輸出設定爲適於在螢幕上顯示的格式還是適於印表機列印的格式。
6. 在此程序的任何階段中按一下 [Find] 按鈕，將顯示符合搜尋條件的所有組織單元。

7. 按一下想要顯示的項目的連結。

[Find All Units Whose] 區段

對於 LDAP 服務，[Find All Units Whose] 區段可讓您建立自訂搜尋篩選器。使用本區段中的欄位可以縮小由 [Find Organizational Unit] 傳回的搜尋結果的範圍。

左側的下拉式清單可指定搜尋所基於的屬性。下列選項可供選用：

- **Unit name。**搜尋每個項目的完整名稱以確定符合項。
- **Description。**搜尋每個組織部門項目的描述，以確定是否有符合項。

中間的下拉式清單可指定要執行的搜尋類型。下列選項可供選用：

- **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，如果知道組織部門的名稱可能包含「Administrator」一詞，請將此選項與搜尋字串「Administrator」一起使用來尋找組織部門項目。
- **Is。**導致執行完全相符搜尋。知道組織單元屬性的準確值時，請使用此選項。例如，知道組織單元名稱的確切拼寫。
- **Isn't。**傳回屬性值不完全符合搜尋字串的所有項目。也就是說，如果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。但請注意，使用此選項可能導致傳回極多項目。
- **Sounds like。**導致執行近似或音似搜尋。如果知道屬性值但不確定其拼寫，請使用此選項。例如，不知道組織單元名稱的拼法是「Sarret's list」、「Sarette's list」或是「Sarett's list」。
- **Starts with。**導致執行子字串搜尋。傳回屬性值以指定搜尋字串開始的所有項目。例如，知道組織單元名稱以「Product」開頭，但不知道名稱的其餘部分。
- **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，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

本程序僅適用於 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. 如以下一節中所述找到要編輯的組織單元：第 66 頁的「尋找組織單元」。
4. 依需要進行變更。如需有關特定欄位的更多資訊，請參閱線上說明。

備註 可能想要變更組織單元編輯頁面未顯示的屬性值。在此情形下，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

本程序僅適用於 LDAP 服務。重新命名組織單元項目時，只會變更組織單元的名稱。無法使用重新命名功能將某個組織單元內的項目移至另一個組織單元。

重新命名組織單元項目

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. 如以下一節中所述找到要編輯的組織單元：第 66 頁的「尋找組織單元」。
4. 按一下 [Rename] 按鈕，在顯示的頁面上輸入新的組織單元名稱，然後按一下 [Save Changes]。

移除組織單元

本程序僅適用於 LDAP 服務。

刪除組織單元項目

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. 如以下一節中所述找到要刪除的組織單元：第 66 頁的「尋找組織單元」。
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

使用憑證和密鑰

本章描述了如何使用憑證和密鑰認證來保護 Sun Java System Web Proxy Server 的安全。Proxy Server 結合了所有 Sun Java System 伺服器的安全架構，並建立在業界標準和公共協定的基礎之上，具有最大的互通性和一致性。

本章假設您已熟知公開密鑰加密的基本概念，包括加密與解密、公開密鑰與私密密鑰、數位憑證和加密協定。如需更多資訊，請參閱「Introduction to SSL」。此文件位於 http://docs.sun.com/source/816-6156-10/index.htm

本章包含下列小節：

基於憑證的認證

認證是確認身份的程序。在網路互動環境中，認證是一方對另一方的信任識別。憑證是支援認證的一種方式。

憑證中包含指定個人、公司或其他實體名稱的數位資料，並證明憑證中包含的公開密鑰屬於此實體。

用戶端和伺服器都可以擁有憑證。伺服器認證指用戶端對伺服器的信任識別 (即對假設負責特定網路位址上之伺服器的組織進行識別)。用戶端認證指伺服器對用戶端的信任識別 (即對假設使用用戶端軟體的使用者進行識別)。用戶端可以擁有多個憑證，就如同人可以有數個不同的身份一樣。

憑證由憑證授權單位 (CA) 核發並進行數位簽名。CA 可以是出售憑證的公司，也可以是負責爲公司的企業內部網路或企業間網路核發憑證的部門。您可以決定將哪些充分信任的 CA 做爲驗證其他使用者身份的機構。

除了公開密鑰和憑證所識別的實體名稱外，憑證還包括過期日期、核發憑證的 CA 之名稱及其數位簽名。

如需有關憑證內容和格式的更多資訊，請參閱「Introduction to SSL」。

如需有關支援的憑證擴充欄位的更多資訊，請參閱「All About Certificate Extensions」。此文件位於 http://www.mozilla.org/projects/security/pki/nss/tech-notes/tn3.html

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

申請伺服器憑證之前，必須建立一個可信任的資料庫。在 Proxy Server 中，Administration Server 和每個伺服器實例都可以擁有自己的可信任資料庫。可信任的資料庫只能在本機電腦上建立。

建立可信任的資料庫時，需要指定用於密鑰對檔案的密碼。亦需要此密碼來啓動使用加密通訊的伺服器。如需有關選擇密碼的注意事項清單，請參閱第 104 頁的「選擇增強的密碼」。

在可信任的資料庫中，可以建立和儲存公開密鑰和私密密鑰 (稱爲密鑰對檔案)。密鑰對檔案用於 SSL 加密。申請和安裝伺服器憑證時將會用到密鑰對檔案。安裝憑證之後，它會儲存在可信任的資料庫中。

密鑰對檔案以加密的形式儲存在以下目錄中：

server_root/alias/proxy-*serverid*-key3.db

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

建立可信任的資料庫

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. 輸入可信任資料庫的密碼。
4. 再次輸入密碼，然後按一下 [OK]。

使用 password.conf

依預設，Proxy Server 會在啓動前提示管理員提供密鑰資料庫密碼。若要重新啓動無人看管狀態的 Proxy Server，必須將密碼儲存在 password.conf 檔案中。只有在系統受到充份保護時才能這樣做，以免洩漏此檔案和密鑰資料庫。

通常，不能以 /etc/rc.local 或 /etc/inittab 檔案啓動已啓用 SSL 的 UNIX 伺服器，因爲伺服器在啓動之前會要求輸入密碼。儘管可以將密碼以純文字格式儲存在某個檔案中來自動啓動已啓用 SSL 的伺服器，但建議不要用這種方法。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，只有擁有者才具有此檔案的讀取和寫入權。

在 UNIX 上，將啓用了 SSL 的伺服器的密碼保留在 password.conf 檔案中會帶來很大的安全性風險。可以存取此檔案的任何使用者均可存取已啓用 SSL 的伺服器之密碼。將啓用了 SSL 的伺服器的密碼保留在 password.conf 檔案中之前，請考量可能帶來的安全性風險。

在 Windows 上，如果採用 NTFS 檔案系統，則應該對包含 password.conf 檔案的目錄之存取權限加以限定 (即使不使用此檔案)，來保護此目錄。Administration Server 使用者和 Proxy Server 使用者應該具有此目錄的讀取和寫入權限。保護此目錄可以防止其他使用者建立假的 password.conf 檔案。在 FAT 檔案系統上，無法以限定存取的方法來保護目錄或檔案。

自動啓動已啓用 SSL 的伺服器

自動啓動已啓用 SSL 的伺服器

1. 確定已啓用 SSL。
2. 在 Proxy Server 實例的 `config` 子目錄中建立新的 `password.conf` 檔案。
   - 如果使用的是 Proxy Server 隨附的內部 PKCS #11 軟體加密模組，請輸入以下資訊：
     `internal:`*your_ password*
   - 如果使用的是其他 PKCS #11 模組 (用於硬體加密或硬體加速器)，請在密碼之前指定 PKCS #11 模組的名稱。例如：
     `nFast:`*your_ password*

即使建立了 `password.conf` 檔案，在啓動 Proxy Server 時系統也總會提示您提供密碼。

申請和安裝 VeriSign 憑證

VeriSign 是 Proxy Server 的首選憑證授權單位。公司的技術簡化了憑證申請程序。VeriSign 的優勢在於能夠直接將憑證傳回伺服器。

爲伺服器建立可信任的憑證資料庫後，可以申請一個憑證並將其提交給 CA (憑證授權單位)。如果公司有自己的內部 CA，可以向此部門申請憑證。如果計劃從商業 CA 處購買憑證，請選擇一個 CA 並詢問其所需資訊的格式。

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。

本節包含以下主題：

申請 VeriSign 憑證

申請 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. 查閱本頁所列之步驟，然後按一下 [OK]。[VeriSign Enrollment Wizard] 隨即顯示，引導您完成登記程序。

安裝 VeriSign 憑證

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. 除非您想要使用外部加密模組，否則請從 [Cryptographic Module] 下拉式清單選取 [Internal]。
4. 輸入密鑰對檔案密碼或 PIN。
5. 從下拉式清單選取要擷取的作業事件 ID，然後按一下 [OK]。

申請和安裝其他伺服器憑證

除了 VeriSign，您亦可從其他憑證授權單位申請和安裝憑證。貴公司或組織可能會提供自己的內部憑證。本節描述如何申請和安裝其他類型的伺服器憑證。

本節包含以下主題：

CA 所需的資訊

開始申請程序前，務必確知您的 CA 要求哪些資訊。各 CA 所要求的資訊格式均有所不同，但大致而言 CA 可能要求您提供下列資訊。請注意，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**。憑證請求者的名稱。
- **Telephone number**。請求者的電話號碼。
- **Common name**。DNS 查找中使用的完整合格的主機名稱 (例如 `www.example.com`)。

- **Email address。**您與 CA 之間通信時使用的業務電子郵件位址。
- **Organization。**您公司、教育機構或組織等的正式法定名稱。多數 CA 會要求提供法律文件 (例如商業牌照的複本) 來證明此資訊。
- **Organizational unit。**公司內部組織單元的描述。
- **Locality。**組織所在城市、公國或國家 / 地區的說明。
- **State or Province。**企業所在的州或省。
- **Country。**國家 / 地區名稱的雙字元縮寫 (以 ISO 格式)。例如，美國的國家 / 地區代碼爲 US。

所有資訊結合爲一系列稱爲辨別名稱 (DN) 的屬性值對，可辨識憑證主體。

如果從商業 CA 處購買憑證，則必須在 CA 核發憑證之前與之連絡，以瞭解他們所需的其他資訊。多數 CA 都要求您提供身份證明。例如，CA 需要驗證您的公司名稱和公司授權負責管理伺服器的使用者，並且可能會詢問您是否具有使用所提供資訊的合法權限。

在某些商業 CA，組織或個人提供的身份證明越充分，所提供的憑證就越詳細、越準確。例如，您可以購買一張憑證，聲明 CA 不僅驗證了您是 `www.example.com` 電腦的合法管理員，而且驗證了您的公司已從事三年的商業活動且無重大客戶訴訟案件。

申請其他伺服器憑證

申請其他伺服器憑證

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. 指定是申請新憑證還是憑證更新。許多憑證在一段時間 (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. 指定提交憑證申請的方式：
   - 若要以電子郵件提交申請，請選取 [CA Email Address]，然後輸入用於此類申請的合適電子郵件位址。
   - 若要利用 CA 的網站提交申請，請選取 [CA URL]，然後輸入用於此類申請的 URL。
5. 從 [Cryptographic Module] 下拉式清單中，選取申請憑證時密鑰對檔案要使用的加密模組。

6. 輸入密鑰對檔案的密碼。除非您選取了內部模組以外的加密模組，否則此密碼即爲您在建立可信任的資料庫時所指定的密碼。伺服器將使用此密碼取得私密密鑰並對傳送給 CA 的訊息進行加密。然後，伺服器將您的公開密鑰及加密的訊息傳送給 CA。CA 會使用公開密鑰來解密您的訊息。
7. 輸入您的識別資訊，如姓名及電話號碼。此資訊的格式因 CA 而異。請注意，這些資訊中的大部分在憑證更新時通常都是不需要的。
8. 仔細檢查這些內容以確定其準確性，然後按一下 [OK]。資訊越準確，批準憑證的速度可能就越快。如果將申請送至憑證伺服器，系統會在提交申請之前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。申請包含以私密密鑰建立的數位簽名。CA 使用數位簽名來驗證申請在從伺服器電腦向 CA 路由的過程中未遭到竄改。只有在極少數情況下申請才會遭到竄改，這時，CA 通常會以電話形式與您連絡。

如果選擇以電子郵件傳送申請，伺服器將編寫內含申請的電子郵件訊息並將其傳送給 CA。通常，憑證會透過電子郵件傳回。如果您指定了憑證伺服器的 URL，您的伺服器會使用此 URL 向憑證伺服器提交申請。視 CA 而定，您可能會收到電子郵件或其他方式的回覆。

如果 CA 同意向您核發憑證，便會通知您。多數情況下，CA 會使用電子郵件向您傳送憑證。如果您的組織正在使用憑證伺服器，則也許可以使用憑證伺服器的表單搜尋憑證。

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 在核發憑證之前都要求您提供身份證明。而且，要獲得批准可能要花費一天到幾週的時間。您有責任及時向 CA 提供所有必要的資訊。

收到憑證後即可進行安裝。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

當您收到 CA 核發的憑證時，它是以您的公開密鑰加密過的，這樣只有您才能予以解密。若要解密和安裝憑證，必須輸入正確的可信任資料庫密碼。

憑證有三種類型：

- 提供給用戶端的您自己的伺服器憑證
- 用於憑證鏈中的 CA 自己的憑證
- 可信任 CA 的憑證

憑證鏈是由各個憑證授權單位依次簽署的一系列階層式憑證。CA 憑證具有憑證授權單位 (CA) 的標識，用於簽署此授權單位核發的憑證。父 CA 的 CA 憑證進而又可簽署 CA 憑證，如此類推，直到根 CA。

備註	如果 CA 不自動將其憑證傳送給您，您應發出此請求。許多 CA 會在電子郵件中同時附加他們的憑證和您的憑證，您的伺服器將同時安裝這兩個憑證。

當您收到 CA 核發的憑證時，它是以您的公開密鑰加密過的，這樣只有您才能予以解密。安裝憑證時，Proxy Server 會使用您指定的密鑰對檔案密碼將其解密。如下所述，您可以將電子郵件儲存在伺服器可以存取的位置，或者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：
   - [This Server]
   - [Server Certificate Chain]
   - [Certification Authority]

   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. 輸入密鑰對檔案密碼。
6. 輸入憑證名稱 (僅限在步驟 3 中選取了 [Server Certificate Chain] 或 [Certification Authority] 的情況下)。
7. 執行以下一項作業來提供憑證資訊：
   - 選取 [Message Is In This File]，然後輸入包含 CA 憑證之檔案的完整路徑名稱。
   - 選取 [Message Text (with headers)]，然後複製及貼上 CA 憑證內容。務必包含 [Begin Certificate] 和 [End Certificate] 標頭，包括開始和結束的連字符。
8. 按一下 [OK]。

9. 選取以下任一選項：
   - [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

遷移憑證

將憑證從 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，將自動更新檔案 (包括可信任的憑證資料庫)。

確認 Proxy Server 4 Administration Server 對舊有的 3.x 資料庫檔案有讀取權。這些檔案是位於 *3.x_server_root*/alias 目錄中的 *alias*-cert.db 和 *alias*-key.db。

只有在伺服器啓用了安全性時，才能遷移密鑰對檔案和憑證。您亦可使用 Administration Server 和 Server Manager 中 [Security] 標籤下的 [Migrate 3.x Certificates] 選項來讓密鑰及憑證自行遷移。如需有關特定設定的更多資訊，請參閱線上說明。

在先前版本中，參照憑證和密鑰對檔案時應採用可由多個伺服器實例使用的別名。Administration Server 管理著全部的別名及其委託憑證。而在 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密鑰對檔案，稱爲可信任的資料庫，而非別名。

對於 Administration Server 本身，可信任的資料庫及其委託憑證由 Administration Server 管理，而對於伺服器實例則由 Server Manager 管理。現在，憑證和密鑰對資料庫檔案依據使用它們的伺服器實例命名。在先前版本中，如果多個伺服器實例共用同一個別名，遷移時會爲新伺服器實例重新命名憑證和密鑰對檔案。

將遷移與伺服器實例關聯的整個可信任的資料庫。先前資料庫中列出的所有 CA 都將被遷移至 Proxy Server 4 資料庫。如果出現重複的 CA，則使用以前的 CA，直到它過期。請勿嘗試刪除重複的 CA。

Proxy Server 3.x 憑證會被遷移爲支援的 Network Security Services (NSS) 格式。憑證的命名係根據存取此憑證時所用的 Proxy Server 頁面 (也就是 [Administration Server Security] 標籤或 [Server Manager Security] 標籤)。

遷移憑證

1. 從本機電腦存取 Administration Server 或 Server Manager，然後按一下 [Security] 標籤。
2. 按一下 [Migrate 3.x Certificates] 連結。
3. 指定 3.6 伺服器安裝目錄的根目錄。
4. 指定此電腦的別名。
5. 輸入管理員密碼，然後按一下 [OK]。

使用內建根憑證模組

Proxy Server 隨附的可動態載入之根憑證模組包括許多 CA (其中包括 VeriSign) 的根憑證。使用根憑證模組可以更容易地將根憑證升級到更高的版本。以前，您需要逐個刪除舊的根憑證，然後再逐個安裝新的根憑證。現在若要安裝常用的 CA 憑證，只需將根憑證模組檔案更新到更高的版本，使它能在以後版本的 Proxy Server 中使用。

因爲根憑證是做爲 PKCS #11 加密模組實作的，所以絕不能刪除模組包含的根憑證，在管理這些憑證時也不會提供刪除憑證的選項。若要從伺服器實例中移除根憑證，可以透過刪除伺服器 `alias` 檔案中的以下內容來停用根憑證模組：

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

如果日後要復原根憑證模組，可以從 *server_root*`/bin/proxy/lib` (UNIX) 或 *server_root*`\bin\proxy\bin` (Windows) 將此擴展部分複製回 `alias` 子目錄。

可以修改根憑證的信任資訊。信任資訊將寫入所編輯的伺服器實例的憑證資料庫中，而並不返回至根憑證模組本身。

管理憑證

您可以檢視、刪除或編輯安裝在伺服器上的各種憑證的信任設定。其中包括您自己的憑證和來自 CA 的憑證。

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。
   - 如果使用內部加密模組管理預設配置的憑證，所有已安裝憑證的清單 (及其類型和過期日期) 將顯示出來。所有憑證都儲存在 *server_root*`/alias` 目錄中。
   - 如果使用外部加密模組 (例如硬體加速器)，必須先輸入每個特定模組的密碼，然後按一下 [OK]。憑證清單將會更新，模組中的憑證將加入其中。
3. 按一下要管理的憑證名稱。隨即將顯示一個頁面，其中包含針對此憑證類型的管理選項。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. 指定要進行的動作。下列選項可供選用：
   - [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

憑證資訊中包括擁有者和核發者。信任設定允許您設定用戶端信任或取消設定伺服器信任。對於 LDAP 伺服器憑證，伺服器必須是可信任的。

安裝和管理 CRL 和 CKL

憑證撤銷清單 (CRL) 和洩漏密鑰清單 (CKL) 能夠清楚地列出用戶端或伺服器使用者不應再信任的所有憑證和密鑰。如果憑證中的資料發生變更 (例如，某位使用者在憑證過期之前變更了辦公室或離開了組織)，則憑證將被撤銷，其資料將顯示在 CRL 中。如果密鑰被竄改或被洩漏，則此密鑰及其資料將顯示在 CKL 中。CRL 和 CKL 都由 CA 產生並定期更新。與您的特定 CA 連絡可取得這些清單。

本節包含以下主題：

安裝 CRL 或 CKL

安裝 CRL 或 CKL

1. 從 CA 取得 CRL 或 CKL，然後將之下載至本機目錄。
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. 輸入關聯檔案的完整路徑名稱，然後按一下 [OK]。將顯示 [Add Certificate Revocation List] 或 [Add Compromised Key List] 頁面，其中列出 CRL 或 CKL 資訊。如果資料庫中已存在 CRL 或 CKL，則將顯示 [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

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。將顯示 [Manage Certificate Revocation Lists /Compromised Key Lists] 頁面，其中列出所有已安裝的 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] 刪除 CRL 或 CKL，或是選取 [Quit] 返回至管理頁面。

設定安全性喜好設定

取得憑證後，便可以開始保護伺服器的安全。本節將描述 Sun Java System Web Proxy Server 所提供的許多安全性元素。

加密是變換資訊的過程，經過這一過程資訊變爲只有預定收件者才能理解的內容。解密也是變換加密資訊的過程，經過這一過程資訊重新變得可以理解。Proxy Server 支援安全通訊端層 (SSL) 和傳輸層安全性 (TLS) 加密協定。

密碼是一種用於加密或解密的加密演算法 (一種數學函數)。SSL 和 TLS 協定包含大量密碼組。某些密碼會比其他密碼更強大、更安全。一般而言，密碼使用的位元越多，資料解密便越難。

在任何雙向加密過程中，雙方都必須使用相同的密碼。由於可供使用的密碼眾多，必須讓伺服器使用最常用的密碼。

在安全連線過程中，用戶端和伺服器商定雙方都可用來通訊的最強密碼。您可以從 SSL 2.0、SSL 3.0 和 TLS 協定選擇密碼。

備註 SSL 2.0 後的版本已在安全性及效能上進行了改善。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。

單靠加密程序並不足以保護伺服器機密資訊的安全。必須將密鑰與加密密碼配合使用，才能產生真正的加密效果，或解密先前加密的資訊。加密程序使用以下兩種密鑰來取得此結果：公開密鑰和私密密鑰。使用公開密鑰加密的資訊只能使用關聯的私密密鑰進行解密。公開密鑰隨憑證發佈。只有關聯的私密密鑰受到保護。

如需有關各種密碼組的說明以及密鑰和憑證的更多資訊，請參閱「Introduction to SSL」。

若要指定伺服器可使用的密碼，請從 Proxy Server 使用者介面中的清單進行選取。除非您有不使用特定密碼的充分理由，否則您應全部選取 (雖然您可能不希望啓用加密效果並非最佳的密碼)。

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，伺服器會依預設使用此設定而不進行加密。

本節包含以下主題：

SSL 和 TLS 協定

Proxy Server 支援用於加密通訊的 SSL 與 TLS 協定。SSL 和 TLS 獨立於應用程式，可以在其上透明地分層排列更高階的協定。

SSL 和 TLS 協定支援各種用於伺服器和用戶端相互認證、傳輸憑證和建立階段作業密鑰的密碼。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制。在其他函數中，SSL 和 TLS 交換協定將決定伺服器和用戶端如何商定用來進行通訊的密碼組。

使用 SSL 與 LDAP 通訊

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

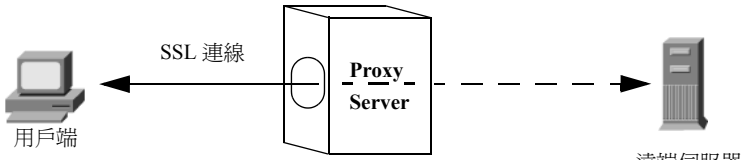
在 Administration Server 上啓用 SSL

1. 存取 Administration Server，然後按一下 [Global Settings] 標籤。
2. 按一下 [Configure Directory Service] 連結。
3. 在顯示的表格中按一下目錄服務的連結。將顯示 [Configure Directory Service] 頁面。若尚未建立基於 LDAP 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] 來配置目錄服務。如需更多有關針對基於 LDAP 之目錄服務所顯示的特定欄位的資訊，請參閱線上說明。
4. 選取 [Yes] 以使用 SSL 進行連線，然後按一下 [Save Changes]。

經過 Proxy Server 建立 SSL 通道

當您以正方向執行 Proxy Server (代理伺服器) 且用戶端請求經過代理伺服器與安全伺服器進行 SSL 連線時，代理伺服器將開啓一連向安全伺服器的連線，然後複製雙向的資料，而不干擾安全作業事件。此程序稱爲建立 SSL 通道，請見下圖的說明。

圖 5-1 使用 SSL 連線時，Proxy Server 無法檢視自己傳輸的資料。



Proxy Server 爲 SSL 作業事件建立通道。

若要將 SSL 通道與 HTTPS URL 配合使用，用戶端必須支援 SSL 與 HTTPS。HTTPS 是透過將一般 HTTP 與 SSL 配合使用實作而成的。不支援 HTTPS 的用戶端仍可使用 Proxy Server 的 HTTPS 代理功能存取 HTTPS 文件。

SSL 通道是一種不會影響應用程式層級 (HTTPS) 的低階作業。SSL 通道的安全性相當於無代理的 SSL。存在於其間的代理伺服器不會以任何方式犧牲安全性或降低 SSL 的功能性。

有了 SSL，資料流將被加密，使代理伺服器無法存取實際的作業事件。因此，存取記錄便不會列出從遠端伺服器接收的狀態碼或標頭長度。如此亦可避免代理伺服器或任何其他第三方竊聽作業事件。

因爲代理伺服器絕對無法檢視資料，因此即無法驗證用戶端與遠端伺服器之間所交流的協定是 SSL。這意味著代理伺服器亦無法防止其他協定通過。您應限定 SSL 連線只通往由 Internet Assigned Numbers Authority (IANA) 所指定的著名 SSL 連接埠，亦即連接埠 443 (HTTPS) 及連接埠 563 (SNEWS)。若有站點在其他連接埠上執行安全伺服器，您可明確設定例外情況，以允許連線到某些主機上的其他連接埠。上述作業是使用 connect://.* 資源完成的。

實際上，SSL 通道功能是一種一般的、類似 SOCKS 的功能，與協定無關，因此您亦可對其他服務使用此功能。Proxy Server 可爲支援 SSL 的任何應用程式處理 SSL 通道，不僅限於 HTTPS 與 SNEWS 協定。

配置 SSL 通道

下列程序描述如何配置 Proxy Server 來使用 SSL 通道。

配置 SSL 通道

1. 存取某伺服器實例的 Server Manager，然後按一下 [Routing] 標籤。
2. 按一下 [Enable/Disable Proxying] 連結。
3. 從下拉式清單選取 `connect://.*.443` 資源。`connect://` 方法是一種內部代理伺服器表示法，不存在於代理伺服器外。如需有關 connect 的更多資訊，請參閱第 84 頁的「SSL 通道的詳細技術性資料」中的下列描述。若要允許連線到其他連接埠，您可使用範本中類似的 URL 式樣。如需有關範本的更多資訊，請參閱第 319 頁的第 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 若代理伺服器配置錯誤，則可能會濫用 SSL 代理伺服器來完成 telnet 跳躍。其他人可使用代理伺服器使 telnet 連線顯示爲來自代理伺服器主機，而非實際的連線主機。這也正是您不能允許使用過多非必要的連接埠，且必須在代理伺服器上使用存取控制 (限定用戶端主機) 的原因。

SSL 通道的詳細技術性資料

就本質而言，SSL 通道使用 `CONNECT` 方法，以目標主機名稱及連接埠號碼做爲參數，後接空白行：

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

接著就是來自 Proxy Server 的成功回覆，後接一空白行：

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

用戶端與遠端伺服器間的連線隨即建立，資料可雙向傳輸，直至任一方關閉連線爲止。

實際上，爲了從以 URL 式樣爲基礎的標準配置機制中受益，主機名稱和連接埠號碼 (`energy.example.com:443`) 被自動對映至一 URL，如：

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

connect:// 僅是 Proxy Server 使用的一種內部表示法，用以使配置更簡易，且與其他 URL 式樣一致。在 Proxy Server 外，connect URL 並不存在，若 Proxy Server 從網路接收到這樣的 URL，會將之視爲無效，且拒絕對此請求提供服務。

爲偵聽通訊端啓用安全性

您可以透過以下方式來保護伺服器偵聽通訊端的安全：

- 開啓安全性
- 爲偵聽通訊端選取伺服器憑證
- 選取密碼

開啓安全性

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

若要在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 Sockets] 連結。
3. 輸入需要的資訊。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]。請注意，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。

備註	在建立偵聽通訊端後，請使用 [Edit Listen Sockets] 連結配置安全性設定。

若要在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. 按一下您要編輯的偵聽通訊端的連結。
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]。請注意，如果尚未安裝伺服器憑證，則只能選擇 [Disabled]。

爲偵聽通訊端選取伺服器憑證

您可以在 Administration Server 或 Server Manager 中將偵聽通訊端配置爲使用您已申請並安裝的伺服器憑證。

備註 必須至少安裝一個憑證。

若要爲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. 按一下您要編輯的偵聽通訊端的連結。
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]。請注意，如果尚未安裝伺服器憑證，則只能選擇 [Disabled]。
5. 選取 [Enabled] 並按一下 [OK] 後，請從偵聽通訊端的 [Server Certificate Name] 下拉式清單中選取伺服器憑證，然後再按一下 [OK]。

選取密碼

若要保護 Proxy Server 的安全，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。可以對 Administration Server 的偵聽通訊端啓用 SSL 和 TLS 協定。對 Server Manager 的偵聽通訊端啓用 SSL 與 TLS 相當於爲特定伺服器實例設定了安全性喜好設定。必須至少安裝一個憑證。

備註 對偵聽通訊端啓用 SSL 僅適用於反向代理伺服器分析藍本。亦即，僅當 Proxy Server 被配置爲執行反向代理時，才能對偵聽通訊端啓用 SSL。

預設設定允許使用最常用的密碼。除非您有不使用特定密碼組的充分理由，否則您應選取全部。如需有關特定密碼的更多資訊，請參閱「Introduction to SSL」。

[TLS Rollback] 的預設及建議設定爲 [Enabled]。這將伺服器配置爲偵測截取式版本回復攻擊的嘗試。爲了與某些未正確實作 TLS 規格的用戶端實現互通性，可能需要將此值設定爲 [Disabled]。

請注意，停用 TLS 回復將導致連線易遭受版本回復攻擊。版本回復攻擊是一種機制，第三方可以透過這種機制強制用戶端和伺服器使用安全性較低的早期協定 (例如 SSL 2.0) 進行通訊。由於 SSL 2.0 協定中存在眾所週知的缺陷，因此無法偵測到版本回復攻擊，這將使第三方更容易截取和解密加密的連線。

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，然後再按一下要編輯的偵聽通訊端的連結。安全偵聽通訊端可使用的密碼設定將顯示出來。

備註 如果未對偵聽通訊端啓用安全性，則不會列出任何 SSL 和 TLS 資訊。若要使用密碼，請務必對選取的偵聽通訊端啓用安全性。如需更多資訊，請參閱第 85 頁的「爲偵聽通訊端啓用安全性」。

3. 核取所需加密設定對應的核取方塊，然後按一下 [OK]。

備註 對於 Netscape Navigator 6.0，請同時選取 [TLS] 和 [SSL 3.0]。對於 TLS 回復，也要選取 TLS，並確定已停用 SSL 3.0 和 SSL 2.0。

在伺服器上啓用 SSL 後，其 URL 將使用 `https`，而非 `http`。指向已啓用 SSL 的伺服器上文件的 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)，則無須在 URL 中輸入連接埠號碼。

全域配置安全性

安裝已啓用 SSL 的伺服器時，會在 `magnus.conf` 檔案 (伺服器的主配置檔案) 中爲全域安全性參數建立指令項目。

設定 SSL 配置檔案指令的值

1. 針對某伺服器實例存取 Server Manager。
2. 務必爲要配置的偵聽通訊端啓用安全性。如需更多資訊，請參閱第 85 頁的「爲偵聽通訊端啓用安全性」。
3. 手動編輯 `magnus.conf` 檔案，然後針對下列設定輸入值：
   - `SSLSessionTimeout`
   - `SSLCacheEntries`
   - `SSL3SessionTimeout`

這些 SSL 配置檔案指令如下所述：如需有關 magnus.conf 的更多資訊，請參閱「Proxy Server Configuration File Reference」。

SSLSessionTimeout

SSLSessionTimeout 指令用於控制 SSL 2.0 階段作業的快取。

語法

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 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 階段作業的快取。

語法

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 之間。

使用外部加密模組

Proxy Server 支援以下使用外部加密模組 (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。

本節包含以下主題：

安裝 PKCS #11 模組

Proxy Server 支援公開密鑰加密標準 (PKCS) #11，此標準定義了在 SSL 和 PKCS#11 模組之間通訊所使用的介面。PKCS #11 模組用於實現與 SSL 硬體加速器的基於標準的連結。外部硬體加速器的匯入憑證和密鑰儲存在 secmod.db 檔案中，此檔案是在安裝 PKCS #11 模組時產生的。檔案位於 *server_root*/alias 目錄中。

使用 modutil 安裝 PKCS #11 模組

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 安裝 PKCS #11 模組

1. 確定已停止所有伺服器 (包括 Administration Server)。
2. 進入包含資料庫的 *server_root*/alias 目錄。
3. 將 *server_root*/bin/proxy/admin/bin 增加至 PATH 中。
4. 在 *server_root*/bin/proxy/admin/bin 中找到 modutil。
5. 設定環境。例如：
   - 在 UNIX 上：setenv

     LD_LIBRARY_PATH *server_root*/bin/proxy/lib:${LD_LIBRARY_PATH}
   - 在 Windows 上，將以下內容增加至 PATH

     LD_LIBRARY_PATH *server_root*/bin/proxy/bin

     您可以在以下目錄中找到您電腦的 PATH：
     server_root/proxy-admserv/start。
6. 輸入指令：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 PCKS #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

使用 pk12util 可以從內部資料庫中匯出憑證和密鑰，並將其匯入內部或外部 PKCS #11 模組。您始終可以將憑證和密鑰匯出至內部資料庫，但多數外部記號不會允許您匯出憑證和密鑰。依預設，pk12util 使用名爲 cert8.db 和 key3.db 的憑證和密鑰資料庫。

透過 pk12util 匯出

從內部資料庫匯出憑證和密鑰

1. 進入包含資料庫的 *server_root*/alias 目錄。
2. 將 *server_root*/bin/proxy/admin/bin 增加至 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，將以下內容增加至 PATH

     LD_LIBRARY_PATH *server_root*/bin/proxy/bin

     您可以在以下目錄中找到您電腦的 PATH：
     server_root/proxy-admserv/start。
5. 輸入指令：pk12util。將列出各種選項。
6. 執行所需的動作。

   例如，在 UNIX 中，請輸入：

   ```
   pk12util -o certpk12 -n Server-Cert [-d /server/alias] [-P https-test-host]
   ```
7. 輸入資料庫密碼。
8. 輸入 pkcs12 密碼。

透過 pk12util 匯入

將憑證和密鑰匯入內部或外部 PKCS #11 模組

1. 進入包含資料庫的 *server_root*/alias 目錄。
2. 將 *server_root*/bin/proxy/admin/bin 增加至 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，將以下內容增加至 PATH

  LD_LIBRARY_PATH *server_root*/bin/proxy/bin

  您可以在以下目錄中找到您電腦的 PATH：*server_root*/proxy-admserv/start。

5. 輸入指令：pk12util。將列出各種選項。
6. 執行所需的動作。

   例如，在 UNIX 中，請輸入：

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

   -P 必須跟在 -h 之後，並且必須是最後一個引數。

   輸入正確的記號名稱，包括大寫字母和引號之間的空格。
7. 輸入資料庫密碼。
8. 輸入 pkcs12 密碼。

以外部憑證啓動伺服器

如果伺服器的憑證安裝在外部 PKCS #11 模組 (例如，硬體加速器) 中，伺服器將無法使用此憑證啓動，除非您對 server.xml 檔案進行編輯，或依如下所述來指定憑證名稱。

伺服器始終嘗試使用名爲 「Server-Cert」的憑證啓動。但外部 PKCS #11 模組中的憑證會在其識別碼中包含模組的一個記號名稱。例如，安裝在名爲 smartcard0 的外部智慧卡讀取器上的伺服器憑證應命名爲 smartcard0:Server-Cert。

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

爲偵聽通訊端選取憑證名稱

爲偵聽通訊端選取憑證名稱

如果未對偵聽通訊端啓用安全性，則不會列出憑證的資訊。若要爲偵聽通訊端選取憑證名稱，首先務必對偵聽通訊端啓用安全性。如需更多資訊，請參閱第 85 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. 按一下要與憑證關聯的偵聽通訊端的連結。

4. 從 [Server Certificate Name] 下拉式清單中爲偵聽通訊端選取伺服器憑證，然後按一下 [OK]。清單中包含所有已安裝的內部和外部憑證。

您也可以手動編輯 `server.xml` 檔案，讓伺服器以此伺服器憑證啓動。將 `SSLPARAMS` 中的 `servercertnickname` 屬性變更爲：

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

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

備註 如果未曾建立可信任的資料庫，則在爲外部 PKCS# 11 模組申請或安裝憑證時將爲您建立一個可信任的資料庫。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。如果已經建立的預設資料庫沒有密碼，請使用 [Security] 標籤上的 [Create Database] 頁面來設定密碼。

FIPS-140 標準

您可以利用 PKCS #11 API 與執行加密作業的軟體或硬體模組通訊。在 Proxy Server 上安裝 PKCS #11 後，即可將伺服器配置爲與 FIPS-140 相容，FIPS 表示 Federal Information Processing Standards (聯邦資訊處理標準)。只有 SSL 3.0 中包含這些程式庫。

啓用 FIPS-140

1. 依據 FIPS-140 說明安裝此外掛程式。
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。[Edit Listen Socket] 頁面中顯示安全偵聽通訊端可用的安全性設定。

備註 若要使用 FIPS-140，請務必對選取的偵聽通訊端啓用安全性。如需更多資訊，請參閱第 85 頁的「爲偵聽通訊端啓用安全性」。

4. 從 [SSL Version 3] 下拉式清單選取 [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

執行可保護伺服器安全性的所有步驟後，可以爲用戶端設定其他安全性需求。

對於 SSL 連線來說，用戶端認證並非必要的程序，但是其的確可以進一步確保加密資訊傳送至正確的當事方。您可在反向代理伺服器中使用用戶端認證，以確保內容伺服器不會與未獲授權的代理伺服器或用戶端共用資訊。

本節包含以下主題：

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，以要求進行用戶端認證。如果啓用用戶端認證，必須提供用戶端認證，伺服器才能將回應傳送給查詢。

Proxy Server 支援透過比對用戶端憑證中的 CA 與用於簽署用戶端憑證的可信任 CA 來認證用戶端憑證。您可以在 [Security] 標籤上的 [Manage Certificates] 頁面檢視用於簽署用戶端憑證的可信任 CA 之清單。

您可以將 Proxy Server 配置爲拒絕不具有可信任 CA 核發之用戶端憑證的任何用戶端。若要接受或拒絕可信任的 CA，必須爲 CA 設定用戶端信任。如需更多資訊，請參閱第 79 頁的「管理憑證」。

如果憑證已過期，Proxy Server 將記錄錯誤、拒絕憑證並向用戶端傳回一則訊息。也可以在 [Manage Certificates] 頁面中檢視哪些憑證已經過期。

您可以將伺服器配置爲從用戶端憑證收集資訊並將其與 LDAP 目錄中的使用者項目比對。這樣可以確定用戶端擁有有效的憑證和 LDAP 目錄中的項目。而且還可以確定用戶端憑證與 LDAP 目錄中的憑證相符。若要瞭解如何進行此作業，請參閱第 96 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) 相符。如需更多資訊，請參閱第 141 頁的「使用存取控制檔案」。

要求用戶端認證

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. 按一下想要求用戶端認證的偵聽通訊端的連結。
4. 使用 [Client Authentication] 下拉式清單來要求偵聽通訊端的用戶端認證，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，可依下列分析藍本來配置用戶端認證：

- **Proxy-Authenticates-Client。**在此分析藍本下，您可允許存取所有具可接受憑證的用戶端，或是僅存取那些具可接受憑證且在 Proxy Server 的存取控制清單中被視爲認可使用者的用戶端。
- **Content-Server-Authenticates-Proxy。**在此分析藍本下，您可確保內容伺服器真正與您的 Proxy Server (而非其他的伺服器) 連線。
- **Proxy-Authenticates-Client and Content-Server-Authenticates-Proxy。**此分析藍本爲您的反向代理伺服器提供最大程度的安全性與認證。

如需有關如何配置上述分析藍本的資訊，請參閱第 94 頁的「設定反向代理伺服器中的用戶端認證」。

設定反向代理伺服器中的用戶端認證

安全反向代理伺服器中的用戶端認證可進一步確保您的連線安全無虞。以下說明內容將解釋如何依據您選擇的分析藍本配置用戶端認證。

備註	每一個分析藍本都假設您具有安全的 Client-to-Proxy 連線及 Proxy-to-Content-Server 連線。

Proxy-Authenticates-Client

配置 Proxy-Authenticates-Client 分析藍本

1. 遵照第 289 頁的第 14 章 「使用反向代理伺服器」的「設定反向代理伺服器」中的指示，配置安全的 Client-to-Proxy 與 Proxy-to-Content Server 分析藍本。
2. 存取某伺服器實例的 [Server Manager]，然後按一下 [Preferences] 標籤。
3. 按一下 [Edit Listen Sockets] 連結，然後再在顯示的表格中按一下您想要的偵聽通訊端的連結。(使用 [Add Listen Socket] 連結配置並增加偵聽通訊端。)
4. 指定用戶端認證需求：

   允許存取具有效憑證的所有使用者：

   - 在 [Security] 區段，使用 [Client Authentication] 設定要求此偵聽通訊端上的用戶端認證。請注意，如果尚未安裝伺服器憑證，此設定將不會顯示。

   僅允許存取那些具有效憑證且已指定爲存取控制中之可接受使用者的使用者：

   a. 在 [Security] 區段中，將 [Client Authentication] 設定保持爲關閉狀態。請注意，如果尚未安裝伺服器憑證，此設定將不會顯示。
   b. 在此伺服器實例的 [Server Manager Preferences] 標籤中，按一下 [Administer Access Control] 連結。
   c. 選取 ACL，然後按一下 [Edit] 按鈕。將顯示 [Access Control Rules For] 頁面 (若系統給予認證提示，請先行認證)。
   d. 開啓存取控制 (若尚未核取 [Access control Is On] 核取方塊，請核取它)。
   e. 將 Proxy Server 設定爲做爲反向代理伺服器認證。如需更多資訊，請參閱第 295 頁的「設定反向代理伺服器」。
   f. 按一下所需存取控制規則的 [Rights] 連結，在下方框架中指定存取權限，然後按一下 [Update] 以更新此項目。
   g. 按一下 [Users/Groups] 連結。在下方框架中，指定使用者與群組，選取 SSL 做爲認證方法，然後按一下 [Update] 以更新此項目。
   h. 按一下上方框架中的 [Submit] 以儲存您的項目。

   如需有關設定存取控制的更多資訊，請參閱第 133 頁的第 8 章 「控制對伺服器的存取」。

Content-Server-Authenticates-Proxy

配置 Content Server-Authenticates-Proxy 分析藍本

1. 請遵照第 295 頁的「設定反向代理伺服器」中的指示，配置安全的 Client-to-Proxy 與 Proxy-to-Content-Server 分析藍本。
2. 在內容伺服器上開啓用戶端認證。

備註	您可修改此分析藍本爲與 Proxy Server 進行非安全用戶端連線、與內容伺服器進行安全連線並讓內容伺服器認證 Proxy Server。若要這麼做，您必須關閉加密功能，並讓代理伺服器嚴格依據下列所述程序初始化憑證。

Proxy-Authenticates-Client and Content-Server-Authenticates-Proxy

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

1. 遵照相關說明配置 Proxy-Authenticates-Client 分析藍本，這些說明位於第 95 頁的「Proxy-Authenticates-Client」。
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

本節描述 Proxy Server 將用戶端憑證對映到 LDAP 目錄中項目的程序。

伺服器收到用戶端的請求時，會在處理請求之前詢問用戶端的憑證。有些用戶端會將用戶端憑證與請求一同傳送給伺服器。

備註	將用戶端憑證對映到 LDAP 之前，還必須配置所需的 ACL。如需更多資訊，請參閱第 133 頁的第 8 章「控制對伺服器的存取」。

伺服器將嘗試將 CA 與 Administration Server 中的可信任 CA 清單比對。若無相符的 CA，Proxy Server 會結束連線。如果能夠找到相符的 CA，伺服器將繼續處理請求。

驗證憑證是來自可信任的 CA 之後，伺服器會透過以下方式將憑證對映到 LDAP 項目：

- 將來自用戶端憑證的核發者和主體 DN 對映到 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。

伺服器使用名爲 certmap.conf 的憑證對映檔案來決定如何執行 LDAP 搜尋。對映檔案將告訴伺服器要從用戶端憑證中獲取哪些值 (如一般使用者的名稱、電子郵件位址等)。伺服器將使用這些值在 LDAP 目錄中搜尋使用者項目，但伺服器首先需要確定從 LDAP 目錄中的哪個位置開始搜尋。憑證對映檔案也會告訴伺服器開始搜尋的位置。

伺服器知道該從何處開始搜尋及搜尋何種項目 (上述第一點) 後，便會在 LDAP 目錄中執行搜尋 (第二點)。如果未找到相符項目或找到多個相符項目，並且**未**設置對映來驗證憑證，搜尋將失敗。

下表列出預期的搜尋結果運作方式。請注意，您可在 ACL 中指定預期的運作方式。例如，可指定當憑證比對失敗時，Proxy Server 只能接受您。如需有關如何設定 ACL 喜好設定的更多資訊，請參閱第 141 頁的「使用存取控制檔案」。

表 5-1 LDAP 搜尋結果

LDAP 搜尋結果	開啓憑證驗證	關閉憑證驗證
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後，就可以使用這些資訊來處理作業事件。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

憑證對映可確定伺服器如何在 LDAP 目錄中查找使用者項目。您可以使用 certmap.conf 配置憑證 (依名稱指定) 對映到 LDAP 項目的方式。您可以編輯此檔案，增加項目，來比對 LDAP 目錄的結構並列出您希望使用者擁有的憑證。使用者可以基於使用者 ID、電子郵件位址或 subjectDN 中使用的任何其他值進行認證。具體來說，對映檔案可定義以下資訊：

- 伺服器應從 LDAP 樹狀結構中的哪個開始搜尋
- 在 LDAP 目錄中搜尋時，伺服器應使用哪些憑證屬性做爲搜尋條件
- 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

此檔案包含一個或多個命名的對映，每個對映都適用於不同的 CA。對映的語法如下：

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

第一行用於指定項目的名稱以及形成 CA 憑證中辨別名稱的屬性。*name* 是任意的，您可隨意定義。但是，*issuerDN* 必須與核發用戶端憑證的 CA 之核發者 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=US
certmap sun2 ou=Sun Certificate Authority, o=Sun, c=US
```

提示 如果正在使用 Sun Java System Directory Server 並在比對核發者 DN 時遇到問題，請在 Directory Server 錯誤記錄中查找有用的資訊。

已命名對映中的第二行和隨後的行可以使屬性與值相符。certmap.conf 檔案中包含六個預設特性 (可以使用憑證 API 自訂特性)：

- DNComps 是一系列用逗號分隔的屬性，用於確定伺服器從 LDAP 目錄的哪個位置開始搜尋符合使用者 (即用戶端憑證的擁有者) 資訊的項目。伺服器從用戶端憑證收集這些屬性的值，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，如果將 DNComps 設定爲使用 DN 的 o 與 c 屬性，則伺服器會從 LDAP 目錄中的 o=*org*, c= *country* 項目開始搜尋，其中 *org* 與 *country* 用憑證中 DN 的值所替代。

  請注意以下情形：

  - 如果對映中不存在 DNComps 項目，伺服器將使用 CmapLdapAttr 設定或用戶端憑證中的整個主體 DN (即一般使用者資訊)。
  - 如果 DNComps 項目存在但沒有對應的值，伺服器將在整個 LDAP 樹中搜尋符合篩選器的項目。

- FilterComps 是一系列用逗號分隔的屬性，用於透過收集用戶端憑證中的使用者 DN 資訊來建立篩選器。伺服器將使用這些屬性的值，來形成用於比對 LDAP 目錄中各項目的搜尋條件。如果伺服器在 LDAP 目錄中找到了一個或多個與從憑證中收集到的使用者資訊相符合的項目，則表示搜尋成功並且伺服器可以選擇執行某個驗證。

  例如，如果 FilterComps 設定爲使用電子郵件位址和使用者 ID 屬性 (FilterComps=e,uid)，伺服器會在目錄中搜尋某項目，此項目的電子郵件及使用者 ID 值與從用戶端憑證所取得的一般使用者資訊相符合。電子郵件位址和使用者 ID 是非常好的篩選器，因爲它們在目錄中通常是唯一的。篩選器需要具體到足以與 LDAP 資料庫中的一個 (且只有一個) 項目相符。

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，使用者電子郵件位址在某些憑證中對應於 e 屬性，而 LDAP 將之稱爲 mail。

下表列出 x509v3 憑證的屬性。

表 5-2 x509v3 憑證的屬性

屬性	描述
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
email	電子郵件位址

- 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。它使用兩個值：[on] 和 [off]。只有當 LDAP 目錄中包含憑證時，才能使用此特性。此功能有助於確定一般使用者使用的憑證有效且未被撤銷。
- CmapLdapAttr 是 LDAP 目錄中包含使用者全部憑證之主體 DN 的屬性名稱。此特性的預設值爲 certSubjectDN。此屬性不是標準的 LDAP 屬性，因此要使用此特性，必須延伸 LDAP 模式。如需更多資訊，請參閱「Introduction to SSL」。

  如果 certmap.conf 檔案中存在此特性，伺服器將在整個 LDAP 目錄中搜尋屬性 (以此特性命名) 與完整的主體 DN (從憑證中取得) 相符合的項目。如果未找到任何項目，伺服器將使用 DNComps 和 FilterComps 對映重新嘗試搜尋。

  如果很難使用 DNComps 和 FilterComps 進行項目比對，則這種對比憑證與 LDAP 項目的方法非常有用。
- Library 特性的值爲共用程式庫或 DLL 的路徑名稱。只有當使用憑證 API 建立自己的特性時才需要使用此特性。
- InitFn 特性的值爲自訂程式庫中 init 函數的名稱。只有當使用憑證 API 建立自己的特性時才需要使用此特性。

如需有關這些特性的更多資訊，請參閱以下小節中的範例：第 100 頁的「對映範例」。

建立自訂特性

可使用用戶端憑證 API 來建立自己的特性。建立自訂對映後，就可按如下格式參照對映：

name:library *path_to_shared_library*
name: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。以下範例說明 certmap.conf 的不同使用方式。

範例 #1

本範例代表只有一個預設對映的 certmap.conf 檔案：

```
certmap default default
default:DNComps ou, o, c
default:FilterComps e, uid
default:verifycert on
```

使用本範例時，伺服器會在包含 ou=*orgunit*, o=*org*, c=*country* 項目的 LDAP 分支點開始搜尋，其中斜體文字將被用戶端憑證中主體 DN 的值所替代。

然後，伺服器使用憑證中的電子郵件位址與使用者 ID 值來在 LDAP 目錄中搜尋相符的項目。找到相符的項目時，伺服器將用戶端傳送的憑證與目錄中儲存的憑證相比對，以驗證憑證。

範例 #2

以下範例檔案中包括兩個對映：一個用於預設，另一個用於 US Postal Service：

```
certmap default default
default:DNComps
default:FilterComps e, uid
```

```
certmap usps ou=United States Postal Service, o=usps, c=US
usps:DNComps ou,o,c
usps:FilterComps e
usps:verifycert on
```

若伺服器收到的憑證不是來自 US Postal Service，它會使用預設對映 (從 LDAP 樹狀結構頂端開始搜尋符合用戶端電子郵件與使用者 ID 的項目)。若憑證來自 US Postal Service，則伺服器會從包含組織單元的 LDAP 分支開始搜尋相符的電子郵件位址。另請注意，若憑證來自 US Postal Service，則伺服器會驗證此憑證。而不會驗證其他憑證。

注意 憑證中的核發者 DN (即 CA 的資訊) 必須與對映的第一行中所列的核發者 DN 一致。在上例中，來自核發者 DN 的憑證 (`o=United States Postal Service,c=US`) 就不相符，因爲 `o` 和 `c` 屬性之間沒有空格。

範例 #3

下例使用 `CmapLdapAttr` 特性在 LDAP 資料庫中搜尋名爲 `certSubjectDN` 的屬性，其值應與用戶端憑證中的整個主體 DN 完全相符。

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

如果用戶端憑證的主體爲：

```
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相符的項目，伺服器將繼續驗證各項目。如果未找到相符的項目，伺服器會使用 `DNComps` 和 `FilterComps` 搜尋相符的項目。在本範例中，伺服器會在 `o=LeavesOfGrass Inc, c=US` 下的所有項目中搜尋 `uid=Walt Whitman`。

備註 本範例假設 LDAP 目錄中包含帶有 `certSubjectDN` 屬性的項目。

設定增強的加密

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 位元大小的密鑰進行存取，或者不限定密鑰大小。您可以指定不符合限制條件時使用的檔案。如果未指定檔案，Proxy Server 將傳回 [Forbidden] 狀態。

如果所選取的存取密鑰大小與 [Security Preferences] 下目前的密碼設定不一致，Proxy Server 會顯示一個快顯對話方塊，警告您需要啓用密鑰大小更大的密碼。

密鑰大小限制的實作基於 `obj.conf` 中的 NSAPI `PathCheck` 指令，而不是 `Service fn=key-toosmall`。此指令爲：

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

其中，*nbits* 是密鑰中所需的最小位元數，*filename* 是不符合限制條件時所用檔案的名稱。

如果未啓用 SSL 或者未指定 `secret-keysize` 參數，`PathCheck` 將傳回 `REQ_NOACTION`。若目前階段作業的密鑰大小小於指定的 `secret-keysize`，則函數會傳回狀態爲 `PROTOCOL_FORBIDDEN` 的 `REQ_ABORTED` (若未指定 `bong-file`) 或 `REQ_PROCEED`，路徑變數被設定爲 `bong-file` *filename*。而且，如果不符合密鑰大小限制，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 交換。

備註 當在 [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。

設定增強的加密

1. 存取某伺服器實例的 [Server Manager]，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增強加密的資源，然後按一下 [Select]。您亦可指定常規表示式。如需更多資訊，請參閱第 319 頁的第 16 章 「管理範本和資源」。
4. 選取密鑰大小限制：
   - 168 位元或更大
   - 128 位元或更大
   - 56 位元或更大
   - 無限制

5. 指定要拒絕存取的訊息所在的檔案位置，然後按一下 [OK]。

如需有關密碼的更多資訊，請參閱「Introduction to SSL」。

其他安全性考量

除了某些人會嘗試破解您的密碼外，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。因此，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，將伺服器電腦放在一個安全的房間內，不允許任何不可信任的使用者將程式上傳至您的伺服器。本節描述了能夠使伺服器更安全的某些要點。

本節包含以下主題：

- 限制實體存取
- 限制管理存取
- 選擇增強的密碼
- 變更密碼或 PIN
- 限制伺服器上的其他應用程式
- 防止用戶端快取 SSL 檔案
- 限制連接埠
- 瞭解伺服器的限制

限制實體存取

這種簡單的安全方法經常會被遺忘。將伺服器電腦放在一個上鎖的房間中，只有經過授權的使用者才能進入房間。這樣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 (根) 密碼 (如果有的話)。

限制管理存取

如果使用遠端配置，請務必設定存取控制，只允許少數使用者和電腦進行管理。如果希望 Administration Server 爲一般使用者提供對 LDAP 伺服器或本機目錄資訊的存取權限，請考量維護兩個 Administration Server 和使用叢集管理。這樣啓用了 SSL 的 Administration Server 可做爲主伺服器，而另一個 Administration Server 則用於一般使用者的存取。如需有關叢集的更多資訊，請參閱第 107 頁的第 6 章 「管理伺服器叢集」。

您還應爲 Administration Server 開啓加密功能。如果不使用 SSL 連線進行管理，那麼透過非加密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。

選擇增強的密碼

您可以在伺服器中使用多個密碼：管理密碼、私密密鑰密碼、資料庫密碼等等。管理密碼是全部密碼中最重要的一個，因爲任何持有此密碼的使用者均可以在您的電腦上配置任何伺服器。私密密鑰密碼是次重要的密碼。如果某個使用者取得了您的私密密鑰和私密密鑰密碼，則可以建立假伺服器僞裝成您的伺服器，或者截取和變更進出您伺服器的通訊資料。

密碼最好是便於您自己記憶，他人又無法猜到。例如，*MCi12!mo* 可記爲 「My Child is 12 months old!」。而小孩子的姓名或生日等不適合做密碼。

建立難以破解的密碼

以下這些簡單的指導原則可幫助您建立增強的密碼。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。一些提示：

- 密碼長度應爲 6 至 14 個字元
- 不要使用非法字元：*、" 或空格
- 不要使用辭典單詞 (任何語言)
- 不要進行常用的字母取代，例如用 3 替代 E 或用 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

定期變更可信任資料庫 / 密鑰對檔案密碼或 PIN 是一個好習慣。如果在 Administration Server 中啓用了 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。

只應在本機電腦上變更此密碼。如需有關變更密碼的注意事項清單，請參閱第 104 頁的「建立難以破解的密碼」。

變更可信任資料庫 / 密鑰對檔案密碼

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] 下拉式清單中選取要在其中變更密碼的安全性記號。依預設，內部密鑰資料庫的安全性記號爲 [Internal]。若已安裝 PKCS #11 模組，則將列出所有安全性記號。
4. 輸入目前密碼。
5. 輸入新密碼。
6. 再次輸入密碼，然後按一下 [OK]。

確定您的密鑰對檔案受到保護。Administration Server 將密鑰對檔案儲存在 *server_root*`/alias` 目錄中。

瞭解檔案是否儲存在備份磁帶上及是否能被其他人截取也很重要。如果這樣，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

請謹慎考慮在伺服器電腦上執行的所有應用程式。利用伺服器上執行的其他程式中的漏洞可以避開伺服器的安全保護。請停用所有不必要的程式和服務。例如，UNIX `sendmail` 常駐程式難以安全地配置，而且可以透過程式設計來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。不要從伺服器電腦執行 `telnet` 或 `rlogin`。您亦不應在伺服器電腦上執行 `rdist`。如此可分發檔案，但亦可用於更新伺服器電腦上的檔案。

Windows

與其他電腦共用磁碟機和目錄時要格外小心。而且，要考量哪些使用者具有帳號或 Guest 權限。您需特別留意在伺服器安裝哪些程式或允許其他人在伺服器上安裝哪些程式。其他使用者的程式可能會存在安全漏洞。更糟糕的是，有人可能會上傳惡意程式，蓄意破壞伺服器的安全性。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可防止外面的使用者連線至絕對最小連接埠集以外的任何連接埠。這意味著取得電腦上 Shell 的唯一方法就是實際地使用伺服器電腦，它應該位在一個限定的區域內。

瞭解伺服器的限制

伺服器提供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，它也無法控制對伺服器電腦本身及其目錄和檔案的存取。

瞭解這些限制有助於您瞭解要避免哪些情形。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

本章描述叢集 Sun Java System Web Proxy Server 的概念，並且說明如何使用叢集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

叢集是可藉由單一 Administration Server 來管理的 Sun Java System Web Proxy Server 群組。每個叢集均必須包含一個指定做爲主 Administration Server 的伺服器。

透過將伺服器組織爲叢集，您可以：

- 建立一個中央位置來管理所有 Proxy Server
- 在伺服器之間共用一個或多個配置檔案
- 藉由一個主 Administration Server 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

使用叢集的指導原則

以下清單提供了將 Proxy Server 群組配置爲叢集的一些指導原則：

- 在建立任何叢集之前，必須安裝包括在特定叢集中的所有伺服器。
- 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。
- 叢集中的所有伺服器必須爲 Proxy Server 4 版本。只支援向業集中增加 Proxy Server 4 版本的伺服器。
- 所有 Administration Server 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 110 頁的「修改伺服器資訊」。
- 所有叢集專用 Administration Server 必須與主 Administration Server 有相同的使用者名稱與密碼。可採用分散式管理來在每個 Administration Server 上配置多個管理員。
- 必須將一個叢集專用 Administration Server 指定爲主 Administration Server (您選擇哪一個伺服器並沒有關係)。
- 主 Administration Server 必須對每個叢集專用 Administration Server 均具有存取權限。主 Administration Server 擷取關於所有已安裝 Sun Java System Web Proxy Server 的資訊。

設定叢集

以下是您設定 Proxy Server 叢集會採取的一般步驟：

設定 Proxy Server 叢集

1. 安裝叢集中要包括的 Proxy Server。請確定叢集的 Administration Server 具有主 Administration Server 可用來進行認證的使用者名稱與密碼。爲此，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。
2. 安裝將包含主 Administration Server 的 Proxy Server，確定使用者名稱與密碼與步驟 1 中設定的相符。
3. 將伺服器增加至叢集清單。如需更多資訊，請參閱第 109 頁的「將伺服器增加至叢集」。
4. 採用兩種方式之一來管理遠端伺服器：從 [Control Cluster] 頁面存取其 Server Manager 介面，或者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

當 Proxy Server 增加至某個叢集時，將會指定其 Administration Server 和連接埠號。如果此 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。您可以在稍後移除個別的伺服器。

備註 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。

增加遠端伺服器至叢集

1. 確定主 Administration Server 處於開啓狀態。
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 用於一般的 Administration Server
   - HTTPS 用於安全 Administration Server
5. 輸入遠端 Administration Server 的完全合格的主機名稱，與 `magnus.conf` 檔案中出現的名稱相同 (例如 `plaza.example.com`)。
6. 輸入遠端 Administration Server 的連接埠號。
7. 輸入遠端 Administration Server 的管理員使用者名稱與密碼，然後按一下 [OK]。主 Administration Server 將嘗試與遠端伺服器連絡。如果成功，系統會提示您確認將伺服器增加至叢集。

備註 當啓用叢集控制後，叢集的主伺服器會在 `proxy-`*serverid*`/config/cluster/`*server_name*`/proxy-`*serverid* 目錄中爲叢集中的每個從屬伺服器建立一些檔案。這些檔案均不可配置。

修改伺服器資訊

Administration Server 的 [Cluster] 標籤上的 [Modify Server] 選項只用於在從屬伺服器中的從屬管理連接埠資訊發生變更後對其進行更新。如果您變更叢集中某個遠端 Administration Server 的連接埠號碼，則還必須修改儲存在叢集中的有關此 Administration Server 的資訊。對從屬 Administration Server 進行任何其他變更都需要您先移除此伺服器，然後在變更之後再將其重新增加至叢集。

修改叢集中有關伺服器的資訊

1. 存取主 [Administration Server]，然後按一下 [Cluster] 標籤。
2. 按一下 [Modify Server] 連結。將依伺服器的唯一識別碼列示伺服器。
3. 選取要修改的伺服器，完成必要的變更，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]。您將無法再透過叢集存取已移除的伺服器。此伺服器只能透過其 Administration Server 存取。

控制伺服器叢集

Proxy Server 可讓您使用以下方式控制叢集中的遠端伺服器：

- 啓動與停止伺服器
- 檢視其存取記錄與錯誤記錄
- 傳輸配置檔案 (如果主 Administration Server 有一個以上的 Proxy Server 實例，將可以從任何伺服器將檔案傳送至增加到叢集中的從屬伺服器)。請注意，叢集必須爲同質叢集。叢集中所有伺服器的類型必須相同 (即爲 UNIX 或 Windows 伺服器)。從其他平台傳輸配置檔案可能導致伺服器掛機或當機。配置檔案有：
  - `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，然後進行想要的選擇。可在任何時間按一下 [Reset] 按鈕，將元素重設爲變更前它們所包含的值。
   - 從下拉式清單中選取 [Start]、[Stop] 或 [Restart]，然後按一下 [Go]。系統會提示您確認此動作。
   - 從下拉式清單中選取 [View Access] 或 [View Error]，然後輸入您要在記錄檔中檢視的最後行號。按一下 [Go] 以顯示資訊 (在顯示的 [Cluster Execution Report] 中按一下 [View] 按鈕)。

- 傳輸配置檔案：
  - 選取您要傳輸的配置檔案
  - 選取檔案所在的伺服器
  - 按一下 [Go] 傳輸資訊

第 3 部分

配置和監視 Proxy Server

第 7 章

配置伺服器喜好設定

本章描述了 Proxy Server 的系統設定及其配置方法。系統設定會影響整個 Proxy Server。這些設定包括代理伺服器使用的使用者帳號和所偵聽的連接埠等選項。

本章包含下列小節：

啓動 Proxy Server

本節描述如何在不同的平台上啓動 Proxy Server。一旦安裝了伺服器，它便會執行、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。將顯示 [Start/Stop Server] 頁面。
3. 按一下 [On] 按鈕。

伺服器的狀態將顯示在 [Start/Stop Server] 頁面上。

在 UNIX 或 Linux 上啓動 Proxy Server

- 從指令行中，進入 *server_root*/proxy-server*id* 並鍵入 ./start 啓動 Proxy Server。
- 使用 start。如果要將此程序檔與 init 搭配使用，則必須包括 start 指令 prxy:2:respawn:*server_root*/proxy-server*id*/start -start -i in /etc/inittab。

在 Windows 上啓動 Proxy Server

- 使用 [開始] > [程式集] > [Sun Microsystems] > [Sun Java System Web Proxy Server 版本] > [Start Proxy Server]
- 使用 [控制台] > [管理工具] > [服務] > [Sun Java System Web Proxy Server 4.0 (proxy-server*id*)] >[啓動]
- 從指令提示處，進入 *server_root*\proxy-server*id* 並鍵入 startsvr.bat 啓動 Proxy Server。

啓動已啓用 SSL 的伺服器

若要啓動已啓用 SSL 的伺服器，需要提供密碼。儘管可以透過將密碼以一般文字格式儲存在某個檔案中來自動啓動已啓用 SSL 的伺服器，但建議不要使用這種方法。

注意 若將已啓用 SSL 的伺服器密碼以一般文字格式儲存在伺服器的 start 程序檔中，會帶來很大的安全性風險。可以存取此檔案的任何使用者均可存取已啓用 SSL 的伺服器之密碼。在以一般文字格式儲存已啓用 SSL 的伺服器之密碼前，請考量安全性風險。

伺服器的 start 程序檔、密鑰對檔案以及密鑰密碼應該爲超級使用者所擁有 (或者，爲安裝了伺服器的非超級使用者的使用者帳號所擁有)，只有擁有者才擁有對它們的讀取和寫入權限。

在 UNIX 或 Linux 上自動啓動已啓用 SSL 的伺服器

1. 使用文字編輯器，開啓 `start` 檔案。
2. 在程序檔中找到 `-start` 行，並插入以下內容：

   `echo "`*password*`"|`

   其中，*password* 是您選擇的 SSL 密碼。

   例如，如果 SSL 密碼爲 `examples`，則編輯的行可能如下所示：

   ```
   -start)
     echo "examples"|./$PRODUCT_BIN -d $PRODUCT_SUBDIR/config $@
   ```

停止 Proxy Server

本節描述在不同平台上停止 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。將顯示 [Start/Stop Server] 頁面。
3. 按一下 [Off] 按鈕。

伺服器的狀態將顯示在 [Start/Stop Server] 頁面上。

在 UNIX 或 Linux 上停止 Proxy Server

- 從指令行中，進入 *server_root*`/proxy-server`*id* 並鍵入 `./stop`。

備註 如果使用 `etc/inittab` 檔案重新啓動伺服器，必須首先從 `/etc/inittab` 中移除啓動伺服器的行，並鍵入 `kill -1 1`，然後嘗試停止伺服器。否則，伺服器在停止後會自動重新啓動。

- 使用 `stop`，這樣可以完全關閉伺服器並中斷服務，直至伺服器重新啓動。如果將 `etc/inittab` 檔案設定爲自動重新啓動 (使用 `respawn`)，則必須在關閉伺服器之前移除 `etc/inittab` 中與代理伺服器相關的行，否則伺服器會自動重新啓動。

關閉伺服器後，伺服器可能需要幾秒鐘的時間來完成關閉程序並將狀態變更爲「Off」。

如果系統當機或離線，伺服器將會停止，其正在處理的任何請求均可能會遺失。

備註 如果您的伺服器安裝了安全性模組，將需要您輸入適當的密碼，然後再啓動或停止伺服器。

在 Windows 上停止 Proxy Server

- 使用 [開始] > [程式集] > [Sun Microsystems] > [Sun Java System Web Proxy Server 版本] > [Stop Proxy Server]
- 從指令提示處，進入 *server_root*\proxy-server*id* 並鍵入 `stopsvr.bat` 停止 Proxy Server。
- 使用 [服務] 視窗中的 [Sun Java System Proxy Server 4.0 (proxy-server*id*)]，進入視窗的方式：[控制台] > [管理工具] > [服務]

重新啓動 Proxy Server

本節描述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啓動伺服器：

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

  請注意，如果所用的 UNIX 或 Linux 版本不是源自 System V (如 SunOS 4.1.3)，則不能使用 `inittab` 檔案。
- 在系統重新啓動時，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，因而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. 若伺服器在編號小於 1024 的連接埠上執行，請以超級使用者身份登入；其他情況下，請以超級使用者身份或使用伺服器的使用者帳號登入。
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* 是伺服器的安裝目錄。

- 您可以在行結尾處使用選擇性參數 -i。-i 選項可以在 inittab 模式下執行伺服器，這樣一旦伺服器程序被終止或當機，inittab 將爲您重新啓動伺服器。此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 檔案的一個行中增加下列文字：

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

其中，*server_root* 爲伺服器的安裝目錄，proxy-server*id* 爲伺服器的目錄。

-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，您必須移除此行。

使用系統 RC 程序檔重新啓動伺服器

如果您使用 /etc/rc.local 或系統中的對等檔案，請將下列行放入 /etc/rc.local 中：

server_root/proxy-server*id*/start

以伺服器的安裝目錄替代 *server_root* 。

重新啓動伺服器 (Windows)

重新啓動伺服器的方式如下

- 使用服務控制台。

在 Windows 上重新啓動伺服器

1. 使用 [控制台] > [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] 變更爲 [自動]，這樣在每次電腦啓動或重新開機時系統都會啓動伺服器。

4. 按一下 [確定]。

設定終止逾時

當伺服器停止時，它會停止接受新連線。而是等待所有未完成的連線完成。伺服器在逾時前的等待時間可在 magnus.conf 檔案中配置。此值的預設設定爲 30 秒。若要變更此值，請將以下行增加至 magnus.conf 檔案：

TerminateTimeout *seconds*

其中，*seconds* 表示伺服器在逾時前將等待的秒數。

配置此值的優點是伺服器將等待更長的時間讓連線完成。不過，由於伺服器有從非回應用戶端開啓的連線，因此，延長終止逾時可能會使伺服器關機時所花費的時間延長。

檢視伺服器設定

在安裝期間，會爲 Proxy Server 配置一些設定。可以從 Server Manager 檢視這些及其他系統設定。[View Server Settings] 頁面列出 Proxy Server 的所有設定。若有未儲存和未套用的變更，此頁面也會告知於您，在這種情況下，您應儲存變更並重新啓動 Proxy Server，使其開始使用新的配置。

設定有兩種類型：技術設定和內容設定。伺服器的內容設定視伺服器的配置而定。一般而言，代理伺服器會列示所有範本、URL 對映和存取控制。對於各個範本，此頁面還會列示範本名稱、其常規表示式和範本設定 (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 子目錄下。

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。將顯示 [View Server Settings] 頁面。

檢視及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)。當目前的配置發生問題時，可利用此功能復原先前的配置。例如，如果您對代理伺服器的配置做了一些變更，而代理伺服器並未像預期的那樣執行 (例如，您拒絕存取 URL，但代理伺服器卻滿足了這樣的請求)，您可復原先前的配置，然後再重新變更配置。

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。將顯示 [Restore Configuration] 頁面。此頁面將按日期和時間順序列示所有先前的配置。
3. 按一下 [View] 連結可顯示某特定版本的技術設定與內容設定清單。

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。將顯示 [Restore Configuration] 頁面。此頁面將按日期和時間順序列示所有先前的配置。
3. 對要復原的版本按一下 [Restore] 連結。

   若要將所有檔案復原成特定時間的狀態，按一下表格最左側欄的 [Restore to *time*] 連結 (*time* 是要復原的日期和時間)。

也可以設定 [Restore Configuration] 頁面上顯示的備份數目。

設定顯示的備份數目

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

配置系統喜好設定

[Configure System Preferences] 頁面可用來設定或變更伺服器的基本狀況。可使用此頁面變更伺服器使用者、程序數目、偵聽佇列大小、代理逾時，以及 Proxy Server 中斷之後的逾時。它還可以讓您啓用 DNS、ICP、代理伺服器陣列和父陣列。

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。將顯示 [Configure System Preferences] 頁面。
3. 依需要變更選項，然後按一下 [OK]。
4. 按一下 [Restart Required]。將顯示 [Apply Changes] 頁面。
5. 按一下 [Restart Proxy Server] 按鈕以套用變更。

後面的小節將描述這些選項。

Server User

[Server User] 是代理伺服器使用的使用者帳號。您輸入的代理伺服器使用者名稱應已經做爲普通使用者帳號而存在。伺服器啓動時，它的執行方式就好像它是由此使用者身份啓動的一樣。

如果您不想建立新的使用者帳號，可選擇在同一主機上執行之另一台伺服器所用的帳號，或者如果在執行 UNIX 代理伺服器，可選擇使用者 nobody。不過在某些系統上，使用者 nobody 可以擁有檔案但不能執行程式，因此它不適合用作代理伺服器使用者名稱。

在 UNIX 系統上，所有由代理伺服器產生的程序都被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目。依預設，此值爲 1。除非另有要求，否則請勿修改此設定。

Listen Queue Size

[Listen Queue Size] 欄位指定偵聽通訊端上的最大擱置連線數目。

DNS

網域名稱服務 (DNS) 會將 IP 位址復原爲主機名稱。當 Web 瀏覽器連線到伺服器時，伺服器只取得用戶端的 IP 位址，例如 `198.18.251.30`。它不會取得主機名稱資訊，例如 `www.example.com.`。爲進行存取記錄和存取控制，伺服器可以將 IP 位址解析爲主機名稱。在 [Configure System Preferences] 頁面上，可以指示伺服器是否將 IP 位址解析爲主機名稱。

ICP

網際網路快取傳輸協定 (ICP) 是一種訊息傳送協定，可讓快取記憶體彼此進行通訊。快取記憶體可使用 ICP 來傳送有關快取 URL 是否存在，以及有關擷取這些 URL 的最佳位置的查詢和回覆。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 257 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，充當用於分散式快取的快取記憶體。如果啓用 [Configure System Preferences] 頁面上的代理伺服器陣列選項，就意味著您要配置的代理伺服器是代理伺服器陣列的一個成員，陣列中的所有其他成員都是它的同層級代理伺服器。如需有關使用代理伺服器陣列的更多資訊，請參閱第 266 頁的 「透過代理伺服器陣列進行路由」。

Parent Array

父陣列是代理伺服器或代理伺服器陣列的路由要經過的代理伺服器陣列。因此，如果代理伺服器在存取遠端伺服器之前要經過一個上游的代理伺服器陣列，則上游的代理伺服器陣列會被視爲父陣列。如需有關對代理伺服器使用父陣列的更多資訊，請參閱第 277 頁的 「透過父系代理伺服器陣列進行路由」。

Proxy Timeout

代理逾時是指在代理伺服器判定請求逾時之前，來自遠端伺服器的連續網路資料封包之間相隔的最長時間。代理逾時的預設值爲 5 分鐘。

備註	當遠端伺服器使用 server-push，且頁面之間的延遲長於代理逾時，則在傳輸完成前連線可能會終止。相反地，如果使用 client-pull，則可將多個請求傳送到代理伺服器。

調校 Proxy Server

使用 [Tune Proxy] 頁面可以變更預設參數，來調校代理伺服器的效能。

變更預設調校參數

1. 存取 Server Manager，然後按一下 [Preferences] 標籤。
2. 按一下 [Tune Proxy] 連結。將顯示 [Tune Proxy] 頁面。
3. 可以修改 FTP 清單的寬度，使其更符合您的需求。增加清單寬度可顯示更長的檔案名，從而減少對檔名的截斷。預設寬度爲 80 個字元。
4. 按一下 [OK]。
5. 按一下 [Restart Required]。將顯示 [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

在伺服器處理請求之前，必須經由偵聽通訊端接受請求，然後將其導向至正確的伺服器。安裝 Proxy Server 時，將自動建立一個偵聽通訊端 ls1。此偵聽通訊端使用 IP 位址 `0.0.0.0` 以及在安裝期間指定的代理伺服器連接埠號。不能刪除預設的偵聽通訊端。

可使用 Server Manager 的 [Add Listen Socket] 及 [Edit Listen Sockets] 頁面來增加、編輯和刪除偵聽通訊端。

本節包含以下主題：

- 刪除偵聽通訊端

增加偵聽通訊端

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。將顯示 [Add Listen Socket] 頁面。
3. 指定偵聽通訊端的內部名稱。您無法在建立偵聽通訊端之後變更此名稱。
4. 指定偵聽通訊端的 IP 位址。可用點對或 IPv6 表示法來表示。也可以是 `0.0.0.0`、`any`、`ANY` 或 `INADDR_ANY` (所有 IP 位址)。
5. 指定要建立偵聽通訊端的連接埠號。有效值爲 `1 - 65535`。在 UNIX 上，若要建立在連接埠 1 - 1024 上偵聽的通訊端時，必須擁有超級使用者權限。配置 SSL 偵聽通訊端可在連接埠 443 上偵聽。
6. 指定在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。這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。如果伺服器使用別名，則此名稱應爲伺服器別名。
7. 在下拉式清單中，指定要爲偵聽通訊端啓用還是停用安全性。
8. 按一下 [OK]。
9. 按一下 [Restart Required]。將顯示 [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

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。將顯示 [Edit Listen Sockets] 頁面。
3. 在 [Configured Sockets] 表中，按一下要編輯的偵聽通訊端的連結。將顯示 [Edit Listen Sockets] 頁面。

4. 依需要變更下列選項的設定：

- **General**
  - **Listen Socket ID。**偵聽通訊端的內部名稱。您無法在建立偵聽通訊端之後變更此名稱。
  - **IP Address。**偵聽通訊端的 IP 位址。這可用點對或 IPv6 表示法來表示。也可以是 `0.0.0.0`、any 或者 `ANY` 或 `INADDR_ANY` (所有 IP 位址)。
  - **Port。**要建立偵聽通訊端的連接埠號。有效值爲 1 - 65535。在 UNIX 上，若要建立在連接埠 1 - 1024 上偵聽的通訊端，必須擁有超級使用者權限。配置 SSL 偵聽通訊端可在連接埠 443 上偵聽。
  - **Server Name。**此偵聽通訊端的預設伺服器。
- **Security**

  如果已停用安全性，則僅顯示以下參數：
  - **Security。**啓用或停用選取的偵聽通訊端的安全性。

  如果啓用了安全性，則會顯示以下參數：
  - **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已安裝的憑證，以用於此偵聽通訊端。
  - **Client Authentication。**指定此偵聽通訊端上是否需要用戶端認證。依預設，此項爲 [Optional]。
  - **SSL Version 2。**啓用或停用 SSL 第 2 版。依預設會停用此項。
  - **SSL Version 2 Ciphers。**列示此密碼組內的所有密碼。透過核取或取消核取方塊可爲正在編輯的偵聽通訊端選取您希望啓用的密碼。將取消核取預設的版本。
  - **SSL Version 3。**啓用或停用 SSL 第 3 版。依預設會啓用此項。
  - **TLS。**啓用或停用 TLS (用於加密通訊的傳輸層安全協定)。依預設會啓用此項。
  - **TLS Rollback。**啓用或停用 TLS 回復。請注意，停用 TLS 回復將導致連線易遭受版本回復攻擊。依預設會啓用此項。
  - **SSL Version 3 and TLS Ciphers。**列示此密碼組內的所有密碼。透過核取或取消核取方塊可爲正在編輯的偵聽通訊端選取您希望啓用的密碼。將核取預設的版本。

- **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。預設爲 1，有效值爲 1 - 1024。

  Protocol Family。通訊端系列類型。有效值爲 `inet`、`inet6` 和 `nca`。對於 IPv6 偵聽通訊端，請使用值 `inet6`。指定 `nca` 可使用 Solaris™ 網路快取記憶體和加速器。

5. 按一下 [OK]。
6. 按一下 [Restart Required]。將顯示 [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

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. 選取要刪除之偵聽通訊端旁邊的核取方塊，然後按一下 [OK]。系統會提示您確認刪除。若偵聽通訊端不是唯一的偵聽通訊端，則可以刪除偵聽通訊端。
4. 按一下 [Restart Required]。將顯示 [Apply Changes] 頁面。
5. 按一下 [Restart Proxy Server] 按鈕以套用變更。

MIME 類型

多用途網際網路郵件延伸 (MIME) 類型是多媒體電子郵件和訊息傳送的標準。爲了您能夠依 MIME 類型篩選檔案，代理伺服器會提供一個頁面，讓您建立用於伺服器的新 MIME 類型。代理伺服器會將新類型增加到 `mime.types` 檔案中。如需有關依 MIME 類型封鎖檔案的更多資訊，請參閱第 285 頁的「依 MIME 類型篩選」。

本節包含以下主題：

建立新的 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。將出現 [Create/Edit MIME Types] 頁面，顯示代理伺服器的 `mime.types` 檔案中列出的所有 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`，其中 `type` 爲檔案或應用程式類型，`enc` 爲用於壓縮的編碼，`lang` 則爲語言編碼。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. 指定檔案字尾。「檔案字尾」是指與 MIME 類型對應的副檔名。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，不要將一個副檔名對映至兩個 MIME 類型。
6. 按一下 [New] 按鈕增加 MIME 類型。

編輯 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` 檔案中列出的所有 MIME 類型。
3. 可以按一下任意 MIME 類型的 [Edit] 連結，來編輯此 MIME 類型。
4. 依需要進行變更，然後按一下 [Change MIME Type] 按鈕。

移除 MIME 類型

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` 檔案中列出的所有 MIME 類型。
3. 您可以按一下任意 MIME 類型的 [Remove] 連結，來移除此 MIME 類型。

管理存取控制

[Administer Access Control] 頁面可讓您管理存取控制清單 (ACL)。ACL 用於控制哪些用戶端可以存取您的伺服器。ACL 可以篩選出特定的使用者、群組或主機，以允許或拒絕對部分伺服器的存取，並且可以設定認證，以只允許有效的使用者和群組存取部分伺服器。如需有關存取控制的更多資訊，請參閱第 133 頁的第 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。將顯示 [Administer Access Control] 頁面。
3. 挑選一個資源 (現有 ACL) 或是鍵入 ACL 名稱，然後按一下 [Edit] 按鈕。將顯示 [Access Control Rules for] 頁面。
4. 依需要進行變更，然後按一下 [Submit]。如需有關存取控制的更多資訊，請參閱 「設定伺服器實例的存取控制」，它位於第 133 頁的第 8 章 「控制對伺服器的存取」。

配置 ACL 快取記憶體

[Configure ACL Cache] 頁面可用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，以及設定項目到期時間。

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。將顯示 [Configure ACL Cache] 頁面。
3. 可以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數目。預設大小爲 200。
5. 從 [Proxy Auth Group Cache Size] 下拉式清單中選取可爲單個 UID/ 快取項目快取的群組 ID 數目。預設大小爲 4。

6. 選取快取項目到期之前經過的秒數。每次參照快取記憶體中的某個項目時，都將根據此值計算並檢查其存在時間。如果此項目的生命週期大於或等於 [Proxy Auth Cache Expiration] 的值，則不會使用此項目。如果將此值設定爲 0，則會關閉快取記憶體。

   如果將其設定爲一個較大的值，則對 LDAP 項目進行變更後需要重新啓動 Proxy Server。例如，如果將此值設定爲 120 秒，則在長達兩分鐘的時間內，Proxy Server 可能會與 LDAP 伺服器不同步。如果您的 LDAP 項目不太可能經常變更，則可使用較大的數值。預設到期時間值爲 2 分鐘。

7. 按一下 [OK]。
8. 按一下 [Restart Required]。將顯示 [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，以降低代理伺服器在將 DNS 主機名稱解析爲 IP 位址時執行 DNS 查找的次數。

配置 DNS 快取

[Configure DNS Cache] 頁面可用來啓用或停用 DNS 快取、設定 DNS 快取大小、設定 DNS 快取項目到期時間，以及啓用或停用負向 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。將顯示 [Configure DNS Cache] 頁面。
3. 可啓用或停用 DNS 快取。
4. 從 [DNS Cache Size] 下拉式清單中選取可儲存在 DNS 快取記憶體內的項目數。預設大小爲 1024。
5. 可以設定 DNS 快取到期時間。Proxy Server 會在達到預定的到期時間時，清除快取記憶體中的 DNS 快取項目。預設 DNS 到期時間爲 120 分鐘。
6. 可以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]。將顯示 [Apply Changes] 頁面。

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

配置 DNS 子網域

某些 URL 包含附帶許多子網域層級的主機名稱。如果第一個 DNS 伺服器無法解析主機名稱，Proxy Server 可能要花很長時間來進行 DNS 檢查。可以設定 Proxy Server 在將 [host not found] 訊息傳回用戶端之前要檢查的層級數。

例如，如果用戶端請求 `http://www.sj.ca.example.com/index.html`，代理伺服器可能需要花很長的時間將此主機解析成 IP 位址，因爲它必須經過四台 DNS 伺服器才能取得主機電腦的 IP 位址。因爲這些查找可能要花費很長的時間，所以您可以適當配置代理伺服器，使其在必須使用的 DNS 伺服器超過一定數量時放棄查找 IP 位址。

設定代理伺服器遍歷的子網域層級數

1. 存取 Server Manager，然後按一下 [Preferences] 標籤。
2. 按一下 [Configure DNS Subdomains] 連結。將顯示 [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目。
5. 按一下 [OK]。
6. 按一下 [Restart Required]。將顯示 [Apply Changes] 頁面。
7. 按一下 [Restart Proxy Server] 按鈕以套用變更。

配置 HTTP 持續作用功能

[Configure HTTP Client] 頁面可用來在 Proxy Server 上啓用持續作用功能。

代理伺服器支援 HTTP 持續作用資料封包。依預設，代理伺服器不會使用持續作用連線，但對某些系統而言，使用持續作用功能可提高代理伺服器的效能。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。

在 Web 上的一般主從式作業事件中，請求多份文件的用戶端可能會多次連線至伺服器。例如，如果用戶端請求含有幾個圖形影像的網頁，則用戶端需要針對每個圖形檔案分別發出請求。重新建立連線是很耗時的。

配置 HTTP 持續作用功能

1. 存取 Server Manager，然後按一下 [Preferences] 標籤。
2. 按一下 [Configure HTTP Client] 連結。將顯示 [Configure HTTP Client] 頁面。
3. 從下拉式清單中選取一個資源。選取 HTTP 或 HTTPS 資源以在 Proxy Server 上配置持續作用，或指定常規表示式。
4. 按一下對應的「持續作用」選項，以指定 HTTP 用戶端是否應使用永久性連線。
5. 在 [Keep Alive Timeout] 欄位中指定使永久性連線保持可用狀態的最大秒數。預設值爲 29。
6. 選取對應的 [Persistent Connection Reuse] 選項，以指定 HTTP 用戶端是否可對所有類型的請求重複使用現有的永久性連線。預設值爲 [off]，既不允許對非 GET 請求或帶有內文的請求重複使用永久性連線。
7. 在 [HTTP Version String] 欄位中指定 HTTP 通訊協定版本字串。除非遇到特定的通訊協定互通性問題，否則不應指定此參數。
8. 在 [Proxy Agent Header] 欄位中指定 Proxy Server 產品名稱和版本。
9. 在 [SSL Client Certificate Nickname] 欄位中指定要向遠端伺服器出示的用戶端憑證暱稱。
10. 選取對應的 [SSL Server Certificate Validation] 選項，以指定 Proxy Server 是否必須驗證由遠端伺服器出示的憑證。
11. 按一下 [OK]。
12. 按一下 [Restart Required]。將顯示 [Apply Changes] 頁面。
13. 按一下 [Restart Proxy Server] 按鈕以套用變更。

第 8 章

控制對伺服器的存取

本章描述如何控制對 Administration Server 的存取及對 Proxy Server 所提供資料的存取。可將存取限制爲伺服器所提供的所有資料，或是其提供的特定 URL。例如，可以指定只有特定人士才可以存取特定的 URL，或是這些特定人士以外的任何人都可以察看檔案。可以允許所有用戶端存取 HTTP 的 URL，但對於 FTP 則僅允許限定存取。也可以根據主機名稱或網域名稱限制 URL；例如，如果有一個服務於許多內部 Web 伺服器的 Proxy Server，但只希望特定人士存取儲存在其中一個伺服器中的機密研究專案。

在 Administration Server 上使用存取控制之前，必須啓用分散式管理並且在 LDAP 資料庫中配置管理群組。本章中的資訊是假設這些作業已經執行。

本章包含下列小節：

何爲存取控制？

存取控制可讓您決定能夠存取 Proxy Server 的使用者，以及他們可以存取的伺服器部分。可以控制對整個伺服器或只是部分伺服器 (例如，目錄、檔案、檔案類型等) 的存取。在評估內送請求時，會根據稱爲存取控制項目 (ACE) 的階層結構規則來決定存取。Proxy Server 會尋找相符的項目，以決定是應該授予還是應拒絕存取。每個 ACE 都會指定伺服器是否應該繼續檢查階層結構中的下一個項目。ACE 的集合稱爲存取控制清單 (ACL)。收到請求時，會檢查 `obj.conf` 檔案中是否有對 ACL 的參照，接著會使用此參照來決定存取。依預設，伺服器具有一個包含多個 ACL 的 ACL 檔案。

基於以下事項允許或拒絕存取：

- 誰在進行請求 (使用者 / 群組)
- 請求來自何方 (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)

本節包含以下主題：

使用者 / 群組的存取控制

可以僅允許特定的使用者或群組存取伺服器。使用者 / 群組存取控制需要使用者輸入使用者名稱和密碼，然後才能存取伺服器。伺服器會將用戶端憑證中的資訊或用戶端憑證本身與一個目錄伺服器項目進行比對。

Administration Server 僅使用基本認證。如果需要在 Administration Server 上進行用戶端認證，必須手動編輯 `obj.conf` 中的 ACL 檔案，將方法變更爲 SSL。

使用者 / 群組認證由爲伺服器配置的目錄服務執行。如需更多資訊，請參閱第 45 頁的「配置目錄服務」。

目錄服務實作存取控制用到的資訊可以透過任何以下一種來源獲得：

- 內部平面檔案類型資料庫
- 外部 LDAP 資料庫

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

- 預設
- 基本
- SSL
- 摘要
- 其他

當伺服器使用內部基於檔案的目錄服務時，支援伺服器實例的使用者 / 群組認證方法包括：

- 預設
- 基本
- 摘要

使用者 / 群組認證需要使用者在獲得存取權限前先自行認證。使用認證，使用者可以透過輸入使用者名稱和密碼、使用用戶端憑證或使用摘要認證外掛程式來確認其身份。使用用戶端憑證需要加密。

預設認證

預設認證是首選方法。[Default] 設定將使用 `obj.conf` 檔案中的預設方法；如果 `obj.conf` 檔案中沒有設定，將使用「基本」方法。如果選取 [Default]，則 ACL 規則將不會在 ACL 檔案中指定方法。選擇 [Default] 可讓您只需編輯 `obj.conf` 檔案中的一行文字即可很容易地變更所有 ACL 的方法。

基本認證

基本認證需要使用者輸入使用者名稱和密碼以存取伺服器。此爲預設設定。必須在 LDAP 資料庫 (如 Sun Java System Directory Server) 或檔案中建立並儲存使用者和群組清單。所使用的目錄伺服器不能與 Proxy Server 安裝在相同的伺服器根目錄下；也可以使用安裝在遠端電腦上的目錄伺服器。

當使用者嘗試存取已經有使用者 / 群組認證的資源時，系統會提示使用者輸入使用者名稱和密碼。伺服器將收到加密或未加密的資訊，這取決於是否爲伺服器開啓了加密 (SSL 已啓用)。

注意	如果使用不帶 SSL 加密的基本認證，將在網路中以未加密的文字形式傳送使用者名稱和密碼。網路封包可能會被截取，使用者名稱和密碼也可能會因此而被盜用。當基本認證與 SSL 加密和 / 或主機 /IP 認證結合使用時會獲得最佳效果。使用摘要認證可以避免此問題。

認證後使用者即會看見：

- 請求的資源 (如果已成功地進行了認證)
- 拒絕存取的訊息 (如果使用者名稱或密碼無效)

可以自訂未授權使用者會收到的訊息。如需更多資訊，請參閱第 153 頁的「拒絕存取時回應」。

SSL 認證

伺服器可以使用安全性憑證以兩種方式確認使用者的身份：

- 使用用戶端憑證中的資訊作爲身份的證明
- 確認 LDAP 目錄中發佈的用戶端憑證 (附加認證)

當將伺服器配置爲使用憑證資訊來認證用戶端時，伺服器將：

- 檢查以確定憑證是否來自一個可信任的 CA (憑證授權單位)。如果不是，認證將失敗，作業事件也將結束。若要瞭解如何啓用用戶端認證，請參閱第 81 頁的「設定安全性喜好設定」。
- 如果憑證來自可信任的 CA，請使用 `certmap.conf` 檔案將憑證對映到使用者的項目。若要瞭解如何配置憑證對映檔案，請參閱第 97 頁的「使用 certmap.conf 檔案」。
- 如果憑證正確進行了對映，請檢查爲此使用者指定的 ACL 規則。即使憑證正確進行了對映，ACL 規則也可能會拒絕此使用者的存取。

要求對特定資源的存取控制進行用戶端認證與要求對伺服器的所有連線進行用戶端認證不同。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 方法進行使用者與群組的認證，則必須符合下列情況：

- 用戶端必須提供由可信任的 CA 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

當要求對存取控制進行用戶端認證時，必須爲 Proxy Server 啓用 SSL 密碼。請參閱第 69 頁的第 5 章 「使用憑證和密鑰」，以瞭解有關啓用 SSL 的更多資訊。

爲了成功地存取經過 SSL 認證的資源，用戶端憑證必須來自 Proxy Server 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，`certmap.conf` 檔案也可以配置爲僅將憑證中的選取資訊與目錄伺服器項目進行比對。例如，可以將 `certmap.conf` 配置爲僅將瀏覽器憑證中的使用者 ID 和電子郵件位址與目錄伺服器項目進行比對。如需關於 `certmap.conf` 和憑證對映的更多資訊，請參閱第 69 頁的第 5 章 「使用憑證和密鑰」。另請參閱 「Proxy Server Configuration File Reference」。

摘要認證

可以將 Proxy Server 配置爲使用基於 LDAP 或基於檔案的目錄服務執行摘要認證。

摘要認證允許使用者基於使用者名稱與密碼進行認證，而無需將使用者名稱與密碼作爲清除文字傳送。瀏覽器使用使用者的密碼和 Proxy Server 提供的某些資訊，利用 MD5 演算法來建立摘要值。

當伺服器使用基於 LDAP 的目錄服務執行摘要認證時，在伺服器端上，也使用摘要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。如果這些摘要值相符，使用者將通過認證。要進行這種認證，目錄伺服器必須能夠存取清除文字形式的使用者密碼。Sun Java System Directory Server 具有一個可逆的密碼外掛程式，它使用對稱的加密演算法以加密形式儲存資料，這些資料可在稍後被解密成原來的形式。只有 Directory Server 保存了資料的密鑰。

對於基於 LDAP 的摘要認證，必須啓用 Proxy Server 隨附的可逆密碼外掛程式和摘要認證專用外掛程式。若要配置 Proxy Server 以處理摘要認證，請在 `dbswitch.conf` 檔案中設定資料庫定義的 `digestauth` 特性，可以在 *server_root*`/userdb/` 中找到此檔案。

伺服器將嘗試基於指定的 ACL 方法認證 LDAP 資料庫，如表 8-1 所示。如果未指定 ACL 方法，當要求進行認證時，伺服器將使用摘要認證或基本認證；當不要求進行認證時，伺服器將使用基本認證。

下表中將列出認證資料庫支援或不支援的摘要認證。

表 8-1 產生摘要認證挑戰

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

使用 `method=digest` 處理 ACL 時，伺服器將嘗試依以下步驟進行認證：

- 檢查 Authorization 請求標頭。如果未找到，將產生要求進行摘要認證的 401 回應，並且程序將停止。
- 檢查授權類型。如果認證類型爲摘要認證，伺服器將：
  - 檢查目前認證情況。如果不是此伺服器產生的有效、未過期的目前認證，將產生 401 回應，且程序將停止。如果目前認證已過期，將產生 401 回應 (其中 `stale=true`)，且程序將停止。

    可以透過變更 `magnus.conf` 檔案中 `DigestStaleTimeout` 參數的值來配置目前認證不過期的時間，此檔案位於 *server_root*`/proxy-server_name/config/` 中。若要設定此值，請將以下行增加至 `magnus.conf`：

    `DigestStaleTimeout` *seconds*

    其中 *seconds* 表示目前認證不過期的秒數。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。如果未找到相符項目，將產生 401 回應，且程序將停止。
  - 如果認證目錄是基於 LDAP 的，請檢查 LDAP 目錄中是否存在使用者；或者如果認證目錄是基於檔案的，請檢查檔案資料庫中是否存在使用者。如果未找到，將產生 401 回應，且程序將停止。
  - 從目錄伺服器或檔案資料庫取得 `request-digest` 值並檢查是否符合用戶端的 `request-digest`。如果未找到相符項目，將產生 401 回應，且程序將停止。
  - 建構 `Authorization-Info` 標頭並將其插入伺服器標頭中。

安裝摘要認證外掛程式

對於使用基於 LDAP 之目錄服務的摘要認證，必須安裝摘要認證外掛程式。此外掛程式在伺服器端計算摘要值，並將此值與用戶端提供的摘要值進行比對。如果這些摘要值相符，使用者將通過認證。

如果使用的是基於檔案的認證資料庫，則不需要安裝摘要認證外掛程式。

在 UNIX 上安裝摘要認證外掛程式

摘要認證外掛程式包含一個共用程式庫，此程式庫在下面兩個檔案中均可找到：

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

在 UNIX 上安裝摘要認證外掛程式

1. 確定此共用程式庫與 Sun Java System Directory Server 位於同一台伺服器電腦上。
2. 確定瞭解 Directory Manager 密碼。
3. 修改 `libdigest-plugin.ldif` 檔案，將對 `/path/to` 的所有參照變更爲安裝了摘要認證外掛程式共用程式庫的位置。
4. 若要安裝外掛程式，請輸入以下指令：

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

在 Windows 上安裝摘要認證外掛程式

必須將數個 `.dll` 檔案從 Proxy Server 安裝複製到 Sun Java System Directory Server 伺服器電腦中，以便讓 Directory Server 能夠正確地與摘要外掛程式一併啓動。

在 Windows 上安裝摘要認證外掛程式

1. 存取 Proxy Server 下列路徑中的共用程式庫：

   server_root`\bin\proxy\bin`

2. 複製以下檔案：
   - `nsldap32v50.dll`
   - `libspnr4.dll`
   - `libplds4.dll`

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 設定爲使用 DES 演算法

對儲存摘要密碼的屬性進行加密需要使用 DES 演算法。

將 Directory Server 設定爲使用 DES 演算法

1. 啓動 Sun Java System Directory Server 主控台。
2. 開啓 iDS 5.0 實例。
3. 選擇 [Configuration] 標籤。
4. 按一下外掛程式旁邊的 + 號。
5. 選取 DES 外掛程式。
6. 選擇 [Add] 以增加一個新屬性。
7. 輸入 `iplanetReversiblePassword`。
8. 按一下 [Save]。
9. 重新啓動 Sun Java System Directory Server 實例。

備註 若要在 `iplanetReversiblePassword` 屬性中爲使用者設定一個摘要認證密碼，輸入內容必須包含 `iplanetReversiblePasswordobject` 物件。

其他認證

可以使用存取控制 API 建立自訂認證方法。

主機 /IP 的存取控制

可以限制對 Administration Server 及其檔案和目錄的存取，方法爲僅限使用特定電腦的用戶端才能存取它們。可以指定要允許或拒絕其存取的電腦的主機名稱或 IP 位址。使用主機 /IP 認證來存取檔案或目錄對使用者來說是一個無縫的程序。使用者可以立即存取檔案和目錄而無需輸入使用者名稱或密碼。

由於可能有多個使用者使用某台電腦，因此主機 /IP 認證與使用者 / 群組認證結合使用時會更有效。如果同時使用這兩種認證方法，則存取時將要求提供使用者名稱和密碼。

主機 /IP 認證不要求在伺服器上配置 DNS (網域名稱服務)。如果選擇使用主機 /IP 認證，必須在網路中執行 DNS 並將伺服器配置爲使用此 DNS。若要啓用 DNS，請存取伺服器的 Server Manager，按一下 [Preferences] 標籤，然後按一下 [Configure System Preferences]。將會看見 DNS 設定。

啓用 DNS 會降低 Proxy Server 的效能，因爲伺服器將不得不執行 DNS 查詢。爲降低 DNS 查詢對伺服器效能的影響，請僅爲存取控制和 CGI 解析 IP 位址，而不要爲每個請求都解析 IP 位址。要執行此動作，請在 `obj.conf` 中指定以下項目：

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

使用存取控制檔案

對 Administration Server 或伺服器上的檔案或目錄使用存取控制時，這些設定將儲存在一個副檔名爲 `.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 和伺服器上配置的每個伺服器實例的 ACL 檔案都將位於 `/usr/Sun/Servers/httpacl/` 中。

主 ACL 檔案爲 `generated-proxy-`*serverid*`.acl`。臨時工作檔案則是 `genwork-proxy-`*serverid*`.acl`。如果使用 Administration Server 來配置存取，將擁有這兩個檔案。但是，如果要進行更複雜的限制，可以建立多個檔案並在 `server.xml` 檔案中參照這些檔案。還有數個功能只能透過編輯這些檔案才能取得，例如，基於一天中的某個時間或一週中的某一天來限定對伺服器的存取。

如需有關存取控制檔案及其語法的更多資訊，請參閱第 349 頁的附錄 A 「ACL 檔案語法」。如需有關 `server.xml` 的更多資訊，請參閱 「Proxy Server Configuration File Reference」。

配置 ACL 使用者快取

依預設，Proxy Server 將使用者和群組認證結果存放在 ACL 使用者快取中。可以使用 `magnus.conf` 檔案中的 `ACLCacheLifetime` 指令來控制 ACL 使用者快取的有效時間。每次參照快取中的某個項目時，都將計算其生命週期並檢查 `ACLCacheLifetime`。如果此項目的生命週期大於或等於 `ACLCacheLifetime`，則不會使用它。預設值爲 120

秒。將此值設定爲 0 (零) 將關閉快取。如果將其設定爲一個較大的值，則每次對 LDAP 項目進行變更時都需要重新啓動 Proxy Server。例如，如果將此值設定爲 120 秒，則在長達兩分鐘的時間內，Proxy Server 可能會與 LDAP 目錄不同步。僅當 LDAP 目錄經常變更的可能性不大時才需要設定一個較大的值。

透過 `ACLUserCacheSize` 的 `magnus.conf` 參數，可以配置快取中所能保留的最大項目數。此參數的預設值爲 200。新項目將增加至清單的開頭，當快取達到其最大大小時，將再循環此清單末尾的項目以建立新項目。

還可以使用 `magnus.conf` 的參數 `ACLGroupCacheSize` 來設定每個使用者項目所能快取的最大群組成員身份數。此參數的預設值爲 4。遺憾的是，群組中非成員身份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。

透過用戶端憑證控制存取

如果伺服器上已啓用 SSL，則可將用戶端憑證與存取控制結合使用。若要執行此動作，必須指定存取特定資源時需要用戶端憑證。伺服器上啓用此功能時，擁有憑證的使用者只需在初次嘗試存取限定資源時輸入其名稱與密碼。其身份一經建立，伺服器就會將他們的登入名稱與密碼對映至此特定憑證。從那時開始，使用者在存取需要用戶端認證的資源時，將不再需要輸入其登入名稱或密碼。當使用者嘗試存取限定資源時，他們的用戶端會將用戶端憑證傳送給伺服器，而伺服器會將此憑證與其對映清單進行比對。如果憑證屬於已授予其存取權限的使用者，則會提供資源。

備註	要求對特定資源的存取控制進行用戶端認證與要求對伺服器的所有連線進行用戶端認證不同。同時也請注意，需要所有 SSL 連線的用戶端憑證並不會自動將憑證對映至資料庫中的使用者。若要執行此動作，必須指定存取指定資源時需要用戶端憑證。

存取控制的工作方式

當伺服器收到頁面請求時，它會使用 ACL 檔案中的規則來確定是否應該授予存取權限。這些規則可以參照傳送此請求的電腦的主機名稱或 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 檔案的可能內容，並提供存取控制規則的範例。

```
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，如果某個使用者請求以下 URL：
`http://server_name/my_stuff/web/presentation.html`

Proxy Server 會先檢查整個伺服器的存取控制。如果整個伺服器的 ACL 設定爲 [Continue]，伺服器將檢查目錄 `my_stuff` 的 ACL。如果存在某個 ACL，伺服器將檢查此 ACL 中的 ACE，然後移至下一個目錄。此程序將繼續，直至找到的某個 ACL 拒絕存取，或者到達所請求 URL 的最後 ACL (在此情況下爲檔案 `presentation.html`)。

若要使用 Server Manager 爲本範例設定存取控制，可以僅爲此檔案建立一個 ACL，也可以爲指向此檔案的每個資源都建立一個 ACL。也就是說，一個用於整個伺服器，一個用於 `my_stuff` 目錄，一個用於 `my_stuff/web` 目錄，一個用於此檔案。

備註 如果有多個相符的 ACL，伺服器會使用最後一個相符的 ACL 敘述。

設定存取控制

本節描述限定存取的程序。可以爲所有伺服器設定全域存取控制規則，也可以爲特定伺服器做個別設定。例如，人力資源部門可以建立一些 ACL，允許所有通過認證的使用者檢視其自己的薪金資料，但只允許負責薪金的人力資源人員更新這些資料。

本節包含以下主題：

- 設定全域存取控制
- 設定伺服器實例的存取控制

備註 必須先配置並啓用分散式管理，然後才能設定全域存取控制。

設定全域存取控制

設定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. 從下拉式清單中選取管理伺服器 (`proxy-admserv`)，按一下 [Go] 以載入資料，然後按一下 [New ACL] (或 [Edit ACL])。
4. 提示時進行認證。將顯示 [Access Control Rules For] 頁面。Administration Server 具有兩行預設存取控制規則，它們是不可編輯的。
5. 選取 [Access Control Is On] (如果尚未選取)。
6. 若要將一個預設 ACL 規則增加至此表的最後一列，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] 頁面將顯示在下面的框架中。
8. 選取要允許其存取的使用者和群組，然後按一下 [Update]。如果按一下群組或使用者的 [List] 按鈕，將顯示供選擇的清單。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「指定使用者和群組」。
9. 按一下 [From Host] 欄中的 [Anyplace]。[From Host] 頁面將顯示在下面的框架中。
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 150 頁的「指定 [From Host]」。
11. 按一下 [Programs] 欄中的 [All]。[Programs] 頁面將顯示在下面的框架中。
12. 選取 [Program Groups]，或在 [Program Items] 欄位中輸入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 151 頁的「限定對程式的存取」。
13. (可選) 按一下 [Extra] 欄中的 X 符號以增加一個自訂的 ACL 表示式。[Customized Expressions] 頁面將顯示在下面的框架中。如需更多資訊，請參閱第 152 頁的「撰寫自訂表示式」。
14. 選取 [Continue] 欄中的核取方塊 (如果尚未選取的話)。伺服器將評估下一行，然後才確定是否允許此使用者進行存取。建立多行限制時，將依一般到特定的順序進行評估。
15. (可選) 按一下回收筒圖示以刪除存取控制規則中相應的行。

16. (可選) 按一下 [Response When Denied] 連結以便指定在拒絕存取時使用者會收到的回應。[Access Deny Response] 頁面將顯示在下面的框架中。選取想要的回應，指定適當的其他資訊，然後按一下 [Update]。如需有關設定的更多資訊，請參閱第 153 頁的「拒絕存取時回應」。
17. 按一下 [Submit] 以便在 ACL 檔案中儲存新的存取控制規則，或是按 [Revert] 將頁面中的元素重設爲變更前其所包含的值。

設定伺服器實例的存取控制

使用 Server Manager，可以建立、編輯或刪除特定伺服器實例的存取控制。刪除時請勿從 ACL 檔案中刪除所有 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。

設定伺服器實例的存取控制

1. 存取伺服器實例的 [Server Manager]，然後按一下 [Preferences] 標籤。
2. 按一下 [Administer Access Control] 連結。
3. 使用下列其中一種方法選取 ACL：
   - [Select A Resource] 可顯示使用 ACL 來限定存取的資源。從下拉式清單中選取一個資源，或是按一下 [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 319 頁的第 16 章「管理範本和資源」。
   - [Select An Existing ACL] 將列出已啓用的所有 ACL。尚未啓用的現有 ACL 將不會顯示在此清單中。請從下拉式清單中選擇。
   - [Type In The ACL Name] 可讓您建立具名 ACL。僅當瞭解 ACL 檔案後才可以使用此選項。如果要將具名 ACL 套用至資源，必須手動編輯 `obj.conf`。如需更多資訊，請參閱第 349 頁的附錄 A 「ACL 檔案語法」。
4. 按一下對應的 [Edit] 按鈕。將顯示 [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 規則增加至此表的最後一列，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] 頁面將顯示在下面的框架中。
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 148 頁的「設定動作」。

9. 按一下 [Users/Groups] 欄中的 [Anyone]。[User/Group] 頁面將顯示在下面的框架中。

10. 選取要允許其存取的使用者和群組，指定認證資訊，然後按一下 [Update]。如果按一下群組或使用者的 [List] 按鈕，將顯示供選擇的清單。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「指定使用者和群組」。

11. 按一下 [From Host] 欄中的 [Anyplace]。[From Host] 頁面將顯示在下面的框架中。

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 150 頁的「指定 [From Host]」。

13. 按一下 [Rights] 欄中的 [All]。[Access Rights] 頁面將顯示在下面的框架中。

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 151 頁的「限定對程式的存取」。

15. (可選) 按一下 [Extra] 欄下的 X 符號以增加一個自訂的 ACL 表示式。[Customized Expressions] 頁面將顯示在下面的框架中。如需更多資訊，請參閱第 152 頁的「撰寫自訂表示式」。

16. 選取 [Continue] 欄中的核取方塊 (如果尚未選取的話)。伺服器將評估下一行，然後才確定是否允許此使用者進行存取。建立多行限制時，將依一般到特定的順序進行評估。

17. (可選) 按一下回收筒圖示以刪除存取控制規則中相應的行。請勿從 ACL 檔案中刪除所有 ACL 規則。必須至少有一個 ACL 檔案，且其中至少包含一個 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，將收到語法錯誤訊息。

18. (可選) 按一下 [Response When Denied] 連結以便指定在拒絕存取時使用者會收到的回應。[Access Deny Response] 頁面將顯示在下面的框架中。選取想要的回應，指定適當的其他資訊，然後按一下 [Update]。如需有關設定的更多資訊，請參閱第 153 頁的「拒絕存取時回應」。

19. 按一下 [Submit] 以便在 ACL 檔案中儲存新的存取控制規則，或是按 [Revert] 將頁面中的元素重設爲變更前其所包含的值。

選取存取控制選項

以下主題描述在設定存取控制時可以選取的各種選項。對於 Administration Server，頭兩行爲預設設定，無法編輯。

本節包含以下主題：

設定動作

可以指定當請求符合存取控制規則時伺服器執行的動作。

- **Allow** 意味著使用者或系統可以存取請求的資源
- **Deny** 意味著使用者或系統不能存取此資源

伺服器將檢查整個存取控制項目 (ACE) 清單以確定存取許可權。例如，第一個 ACE 通常爲拒絕所有使用者。如果第一個 ACE 已設定爲 [Continue]，伺服器會檢查清單中的第二個 ACE。如果相符，則會使用下一個 ACE。如果未選取 [Continue]，將會拒絕所有使用者存取資源。伺服器將繼續向下檢查清單，直至找到某個不符合的 ACE，或者找到某個符合但未設定爲 [Continue] 的 ACE。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，將提示使用者輸入使用者名稱和密碼，然後才能存取在存取控制規則中指定的資源。

Proxy Server 將檢查儲存在 LDAP 伺服器 (如 Sun Java System Directory Server) 或內部基於檔案的認證資料庫中的使用者和群組的清單。

可以允許或拒絕資料庫中的每個使用者進行存取，也可以使用萬用字元式樣允許或拒絕特定使用者進行存取，還可以從使用者和群組的清單中選取允許或拒絕進行存取的使用者。

在使用者介面的 [Access Control Rules For] 頁面中，將爲 [Users/Groups] 顯示下列元素。

- **Anyone (No Authentication)** 是預設值，意味著任何使用者都可以存取此資源而不必輸入使用者名稱或密碼。但是，基於其他設定 (例如主機名稱或 IP 位址) 的不同，也可能會拒絕此使用者進行存取。對於 Administration Server，這意味著爲分散式管理指定的 administrators 群組中的任何使用者都可以存取各個頁面。
- **Authenticated People Only**
  - **All In The Authentication Database** 與在資料庫中具有項目的任何使用者相符。
  - **Only The following People** 指定要相符的使用者和群組。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的清單中選取。**Group** 與所指定群組中的所有使用者相符。**User** 與所指定的個別使用者相符。對於 Administration Server，使用者還必須位於爲分散式管理指定的 administrators 群組中。
- **Prompt For Authentication** 指定在認證對話方塊中顯示的訊息文字。可以使用此文字來描述使用者需要輸入的內容。基於不同的作業系統，使用者大約會看到此提示的前 40 個字元。大多數瀏覽器會快取使用者名稱和密碼，並將它們與提示文字相關聯。這意味著如果使用者存取伺服器中具有相同提示的區域 (檔案和目錄)，則不必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，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所使用的方法。Administration Server 僅提供了 「基本」認證方法。Server Manager 提供了以下方法：
  - **Default** 使用在 `obj.conf` 檔案中指定的預設方法；如果 `obj.conf` 檔案中沒有設定，則使用「基本」方法。如果選取 [Default]，則 ACL 規則將不會在 ACL 檔案中指定方法。選擇 [Default] 可讓您只需編輯 `obj.conf` 檔案中的一行文字即可很容易地變更所有 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後才會對使用者名稱和密碼進行加密 (SSL 已啓用)。否則，名稱與密碼會以清除文字形式傳送，如果被截取，則會爲他人獲悉。
  - **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。啓用加密後，將可以合併基本方法和 SSL 方法。

- **Digest** 使用一種認證機制，它使得瀏覽器能夠基於使用者名稱和密碼對使用者進行認證，而無需將使用者名稱與密碼作爲清除文字傳送。瀏覽器使用使用者的密碼和 Proxy Server 提供的某些資訊，利用 MD5 演算法來建立摘要值。伺服器端也會使用摘要認證外掛程式計算此摘要值，並會將它與用戶端提供的摘要值進行比對。
- **Other** 使用透過存取控制 API 建立的自訂方法。

- **Authentication Database** 指定伺服器用來認證使用者的資料庫。此選項僅能透過 Server Manager 使用。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。如果想要將個別 ACL 配置爲使用不同的資料庫，請選取 [Other]，然後指定資料庫。必須在 *server_root*`/userdb/dbswitch.conf` 中指定非預設資料庫及 LDAP 目錄。如果爲某個自訂資料庫使用存取控制 API，請選取 [Other] 並輸入資料庫名稱。

指定 [From Host]

可以基於請求來自的電腦限定對 Administration Server 的存取。

在使用者介面的 [Access Control Rules For] 頁面中，將爲 [From Host] 顯示下列元素。

- **Anyplace** 允許所有使用者和系統進行存取
- **Only From** 僅允許特定主機名稱或 IP 位址進行存取

如果選取了 [Only From] 選項，請在 [Host Names] 或 [IP Addresses] 欄位中輸入萬用字元式樣或以逗號分隔的清單。依主機名稱進行限定比依 IP 位址進行限定更靈活。如果使用者的 IP 位址有變更，不需要更新此清單。但是，依 IP 位址進行限定更可靠。如果對連線的用戶端進行 DNS 查詢失敗，則無法使用主機名稱限制。

只能在符合電腦的主機名稱或 IP 位址的萬用字元式樣中使用 * 萬用字元表示法。例如，若要允許或拒絕特定網域中的所有電腦，可以輸入符合此網域中所有主機的萬用字元式樣，如 `*.example.com`。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，* 必須取代名稱中的整個部分。也就是說，`*.example.com` 可以接受，但 `*users.example.com` 無法接受。當 * 出現在主機名稱中時，它必須是最左側的字元。例如，`*.example.com` 可以接受，但 `users.*.com` 無法接受。

對於 IP 位址，* 必須取代位址中的整個位元組。例如，`198.95.251.*` 可以接受，但 `198.95.251.3*` 無法接受。當 * 出現在 IP 位址中時，它必須是最右側的字元。例如，`198.*` 可以接受，但 `198.*.251.30` 無法接受。

限定對程式的存取

對程式的存取只能由 Administration Server 來限定。透過限定對程式的存取，可以僅允許指定的使用者檢視 Server Manager 頁面並確定這些使用者是否能夠配置此伺服器。例如，可以允許某些管理員配置 Administration Server 的 [Users and Groups] 區段，但拒絕他們存取 [Global Settings] 區段。

可以配置不同的使用者存取不同的功能領域。一旦爲某個使用者授予了對若干已選取功能領域的存取權限，當此使用者登入時，只有授權此使用者存取的那些功能領域的 Administration Server 頁面才可見。

在使用者介面的 [Access Control Rules For] 頁面中，將爲 [Programs] 顯示下列元素。

- **All Programs** 允許或拒絕對所有程式的存取。依預設，管理員可以存取某個伺服器的所有程式。
- **Only The Following** 讓您能夠指定使用者擁有存取權限的程式。
    - **Program Groups** 反映了 Administration Server 的各個標籤 (例如 [Preferences] 和 [Global Settings])，代表了對這些頁面的存取。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 位址來確定他們能檢視哪些頁面。
    - **Program Items** 讓您能夠在欄位中輸入頁面名稱來控制對程式中特定頁面的存取。

設定存取權限

伺服器實例的存取權限只能由 Server Manager 設定。存取權限可以限定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，還可以指定一個允許或拒絕部分存取權限的規則。例如，可以授予使用者對檔案的唯讀存取權限，這樣他們可以檢視資訊，但不能變更檔案。

在使用者介面的 [Access Control Rules For] 頁面中，將爲 [Rights] 顯示下列元素。

- **All Access Rights** 是預設值，它允許或拒絕所有權限。
- **Only The following Rights** 讓您能夠選取要允許或拒絕的權限組合：
    - **Read** 允許使用者檢視檔案，其中包括 HTTP 方法 GET、HEAD、POST 和 INDEX。
    - **Write** 允許使用者變更或刪除檔案，其中包括 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 和代理程式。
- **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` 檔案的目錄中檔案的清單。
- **Info** 允許使用者接收關於 URI 的資訊，例如 `http_head`。

撰寫自訂表示式

可以爲 ACL 輸入自訂表示式。只有當瞭解 ACL 檔案的語法和結構時，才能選取此選項。有若干功能只有透過編輯 ACL 檔案或建立自訂表示式才能實現。例如，可以基於一天中的某個時間和 / 或一週中的某一天來限定對伺服器的存取。

以下自訂表示式顯示了如何基於一天中的某個時間及一週中的某一天來限定存取。本範例假定 LDAP 目錄中有兩個群組。「Regular」群組可以在星期一到星期五的上午 8 點到下午 5 點進行存取。「Critical」群組可以隨時進行存取。

```
allow (read)
{
    (group=regular and dayofweek=Omon,tue,wed,thu,friO);
    (group=regular and (timeofday>=0800 and timeofday<=1700)) ;
    (group=critical)
}
```

如需有關有效語法和 ACL 檔案的更多資訊，請參閱第 349 頁的附錄 A 「ACL 檔案語法」。

關閉存取控制

取消選取 [Access Control Rules For] 頁面上標籤爲 [Acess Control Is On] 的選項時，會收到一個提示，詢問是否想要清除 ACL 中的記錄。按一下 [OK] 後，將從 ACL 檔案中刪除此資源的 ACL 項目。

如果要停用 ACL，請在檔案 `generated-proxy-`*`serverid`*`.acl` 中每行的開頭使用 # 符號，將 ACL 行變爲註釋。

在 Administration Server 中，可以爲特定伺服器實例建立和啓用存取控制，而爲其他伺服器停用存取控制 (依預設爲停用)。例如，可以透過 Administration Server 拒絕對 Server Manager 頁面的所有存取。對於依預設啓用了分散式管理且禁用了存取控制的任何其他伺服器，管理員仍可以存取和配置這些伺服器，但不能配置 Administration Server。

拒絕存取時回應

Proxy Server 提供在存取遭拒時的預設訊息，如有需要，也可以自訂回應。還可以爲每個存取控制物件建立不同的訊息。

依預設，Administration Server 的使用者會收到 *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 [Response When Denied] 連結。
2. 選取想要的回應，輸入適當的其他資訊 (請確定使用者可以存取將其重新導向至的回應)，然後按一下 [Update]。
3. 按一下 [Submit] 以儲存所作的變更，或是按一下 [Revert] 將此頁面中元素的值重設爲變更前所具有的值。

限制對伺服器中區域的存取

本節描述一些常用的對伺服器及其內容的限定。每個程序的步驟都詳述了必須執行的特定動作。但仍然必須完成以下部分中所述的步驟：第 146 頁的 「設定伺服器實例的存取控制」。

本節包含以下主題：

限定對整個伺服器的存取

可能希望爲某個群組中的使用者授予存取權限，以便他們可以從某個子網域中的電腦存取伺服器。例如，公司某部門可能有一個伺服器，您僅希望來自網路特定子網域中電腦的使用者能夠對其進行存取。

限定對整個伺服器的存取

使用針對伺服器實例存取控制設定的描述步驟 (請參閱第 146 頁的 「設定伺服器實例的存取控制」) 來執行下列動作：

1. 存取伺服器實例的 Server Manager。
2. 在 [Preferences] 標籤中，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]，然後按一下對應的 [Edit] 按鈕。將顯示 [Access Control Rules For] 頁面。
4. 增加一個新規則以拒絕所有使用者進行存取。
5. 增加另一個新規則以允許特定群組的存取。
6. 使用 [From Host] 指定想要限定的主機名稱與 IP 位址。
7. 按一下 [Submit] 以儲存所做的變更。

限定對目錄 (路徑) 的存取

可以允許某個群組中的使用者讀取或執行目錄及其子目錄中的應用程式和檔案 (這些內容由此群組的所有者控制)。例如，專案經理可以更新狀態資訊，供專案團隊複查。

限定對目錄的存取

使用針對伺服器實例存取控制設定的描述步驟 (請參閱第 146 頁的 「設定伺服器實例的存取控制」) 來執行下列動作：

1. 存取伺服器實例的 Server Manager。
2. 在 [Preferences] 標籤中，按一下 [Administer Access Control] 連結。
3. 從下拉式清單選取想要的資源，然後按一下 [Edit]。
4. 建立一個新規則並保留預設設定，以拒絕任何位置的任何使用者進行存取。
5. 建立另一個新規則，允許特定群組中的使用者僅具有讀取和執行權限。
6. 建立第三個新規則以允許特定使用者具有所有權限。
7. 取消選擇後兩個規則的 [Continue]。

8. 按一下 [Submit] 以儲存所做的變更。

限定對檔案類型的存取

可以限制對檔案類型的存取。例如，可能希望僅允許特定使用者建立在伺服器上執行的程式。任何使用者都將能夠執行程式，但僅有群組中的指定使用者才能夠建立或刪除程式。

限定對檔案類型的存取

使用針對伺服器實例存取控制設定的描述步驟 (請參閱第 146 頁的 「設定伺服器實例的存取控制」) 來執行下列動作：

1. 存取伺服器實例的 Server Manager。
2. 在 [Preferences] 標籤中，按一下 [Administer Access Control] 連結。
3. 按一下 [Select A Resource] 區段中的 [Regular Expression]，然後指定常規表示式。例如：`*.cgi`。
4. 按一下 [Edit]。
5. 建立一個新規則，允許所有使用者進行讀取。
6. 建立另一個規則，僅允許指定群組進行寫入和刪除。
7. 按一下 [Submit] 以儲存所做的變更。

對於檔案類型限制，應該保持兩個 [Continue] 方塊均被核取。當傳入對某個檔案的請求時，伺服器將首先檢查此檔案類型的 ACL。

`obj.conf` 中將建立一個 `Pathcheck` 函數，它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";`

基於一天中的某個時間限定存取

可以將對伺服器的寫入和刪除存取限定爲僅允許在指定的時間或指定的日期進行。

基於一天中的某個時間限定存取

使用針對伺服器實例存取控制設定的描述步驟 (請參閱第 146 頁的 「設定伺服器實例的存取控制」) 來執行下列動作：

1. 存取伺服器實例的 Server Manager。
2. 在 [Preferences] 標籤中，按一下 [Administer Access Control] 連結。

3. 從 [Select A Resource] 區段中的下拉式清單選取整個伺服器，然後按一下 [Edit]。
4. 建立一個新規則，授予所有使用者讀取和執行權限。這意味著如果某個使用者要增加、更新或刪除檔案或目錄，將不會套用此規則，伺服器將搜尋另一個符合的規則。
5. 建立另一個新規則，拒絕所有使用者進行寫入和刪除。
6. 按一下 X 連結，建立一個自訂表示式。
7. 輸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" and
dayofweek = "sat,sun" or
(timeofday >= 1800 and
timeofday <= 600)
```

8. 按一下 [Submit] 以儲存所做的變更。自訂表示式中有任何錯誤都將產生一則錯誤訊息。請進行更正並再次提交。

基於安全性限定存取

可以爲同一伺服器實例配置 SSL 及非 SSL 偵聽通訊端。基於安全性限定存取允許您爲僅應透過安全通道傳輸的資源建立保護。

基於安全性限定存取

使用針對伺服器實例存取控制設定的描述步驟 (請參閱第 146 頁的 「設定伺服器實例的存取控制」) 來執行下列動作：

1. 存取伺服器實例的 Server Manager。
2. 在 [Preferences] 標籤中，按一下 [Administer Access Control] 連結。
3. 從 [Select A Resource] 區段中的下拉式清單選取整個伺服器，然後按一下 [Edit]。
4. 建立一個新規則，授予所有使用者讀取和執行權限。這意味著如果某個使用者要增加、更新或刪除檔案或目錄，將不會套用此規則，伺服器將搜尋另一個符合的規則。
5. 建立另一個新規則，拒絕所有使用者進行寫入和刪除。

6. 按一下 X 連結，建立一個自訂表示式。
7. 輸入 `ssl="on"`。例如：

```
user = "anyone" and ssl="on"
```

8. 按一下 [Submit] 以儲存所做的變更。自訂表示式中有任何錯誤都將產生一則錯誤訊息。進行更正並再次提交。

保證資源的存取安全

本節描述在啓用分散式管理之後，爲保證 Proxy Server 存取控制安全性而必須執行的其他作業。

本節包含以下主題。

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_root*`/httpacl/*.proxy-admserv.acl` 檔案以指定想要授與其存取控制權限的使用者。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 (gen*.proxy-admserv.acl) 中，請完成下面的步驟 1 和 2。

如果參照 ip 屬性的存取控制項目位於與某個伺服器實例相關的 ACL 檔案中，請僅爲此特定 ACL 完成下面的步驟 1。

啓用基於 IP 的存取控制

1. 編輯 *server_root*/httpacl/gen*.proxy-admserv.acl 檔案，除了 user 和 group 外，再將 ip 增加至認證清單，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";
   ```

爲基於檔案的認證建立 ACL

Proxy Server 支援使用基於檔案的認證資料庫，這些資料庫在平面檔案中以文字格式儲存使用者和群組資訊。ACL 架構被設計爲可以使用檔案認證資料庫。

備註 Proxy Server 不支援動態平面檔案。平面檔案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。

本節包含以下主題：

- 爲基於檔案認證的目錄服務建立 ACL
- 爲基於摘要認證的目錄服務建立 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 檔案包含定義檔案認證資料庫及其配置的項目。例如：

```
directory myfiledb file
myfiledb:syntax keyfile
myfiledb:keyfile /path/to/config/keyfile
```

下表列出了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	描述
syntax	(可選) 值爲 keyfile 或 digest。如果未指定，則預設爲 keyfile。
keyfile	(syntax=keyfile 時需要) 包含使用者資料的檔案路徑。
digestfile	(syntax=digest 時需要) 包含摘要認證使用者資料的檔案路徑。

注意 檔案認證資料庫檔案中一行的最大長度爲 255。如果有任何行超過此限制，伺服器將無法啓動，而且將會在記錄檔中記錄錯誤。

備註 確定在嘗試使用基於檔案的認證資料庫設定 ACL 前，已經配置了基於檔案的認證目錄服務。如需更多資訊，請參閱第 45 頁的「配置目錄服務」。

爲基於檔案認證的目錄服務建立 ACL

爲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] 標籤中，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，按一下要編輯的 ACL 項目的 [Users/Groups] 連結。[User/Group] 頁面將顯示在下面的框架中。
5. 在 [Authentication Database] 底下的下拉式清單中指定密鑰檔案資料庫。
6. 按一下 [Update]，然後按一下 [Submit] 以儲存所做的變更。

依據基於密鑰檔案的認證資料庫設定 ACL 時，將使用相應的 ACL 項目更新 `dbswitch.conf` 檔案，如下面給出的範例項目：

```
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";
```

爲基於摘要認證的目錄服務建立 ACL

檔案認證資料庫還支援一種檔案格式，此格式遵循 RFC 2617，適用於摘要認證。將儲存基於密碼和範圍的雜湊，且不維護清除文字密碼。

爲基於摘要認證的目錄服務建立 ACL

1. 存取伺服器實例的 Server Manager。
2. 在 [Preferences] 標籤中，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，按一下要編輯的 ACL 的 [Users/Groups] 連結。[User/Group] 頁面將顯示在下面的框架中。
5. 在 [Authentication Database] 底下的下拉式清單中指定摘要資料庫。

6. 按一下 [Update]，然後按一下 [Submit] 以儲存所做的變更。

當依據基於摘要認證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，如下面給出的範例項目：

```
version 3.0;
acl "default";
authenticate (user) {
     prompt = "filerealm";
     database = "mydigestfile";
     method = "digest";
};

deny (all) user = "anyone";
allow (all) user = "all";
```

第 9 章

使用記錄檔

您可以使用幾種不同的方法來監視伺服器的活動。本章介紹如何透過記錄和檢視記錄檔來監視伺服器。如需有關使用內建效能監視服務或 SNMP 的資訊，請參閱第 187 頁的第 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活動。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下的 proxy-server_name/logs/errors 中，列示了伺服器遇到的所有錯誤。存取記錄位於伺服器根目錄下的 proxy-server_name/logs/access 中，記錄了有關向伺服器發出的請求及伺服器提供的回應之資訊。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。您可以透過歸檔來備份伺服器的錯誤記錄檔和存取記錄檔。

備註 由於作業系統的限制，Proxy Server 在 Linux 上無法處理大於 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

本節論述記錄檔的建立方法。另外，本節還包括下列主題：

- 預設錯誤記錄
- 使用 syslog 進行記錄
- 使用 Windows eventlog 記錄

預設錯誤記錄

在 UNIX 和 Windows 平台上，管理伺服器的記錄集中儲存在管理 proxy-admserv/logs/ 目錄中。伺服器實例的記錄儲存在 proxy-server_name/logs/ 目錄中。

可以設定整個伺服器的預設記錄層級。您可以將 stdout 和 stderr 重新導向至伺服器的事件記錄，將記錄輸出重新導向至作業系統的系統記錄。此外，您也可將 stdout 和 stderr 內容導向至伺服器的事件記錄。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

syslog 適用於需要集中記錄的穩定作業環境。對於經常需要使用記錄輸出來進行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。

備註

- 如果將伺服器實例和管理伺服器的所有記錄資料集中在一個文件中，可能很難讀取和除錯。建議只將 syslog 主記錄檔用於已部署且正在順利執行的應用程式。
- 記錄的訊息與 Solaris 常駐應用程式的所有其他記錄混合在一起。

使用 syslog 記錄檔，並結合 syslogd 以及系統記錄常駐程式，您可以將 `syslog.conf` 檔案配置爲：

- 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一組使用者，或透過網路將其轉寄至另一台主機上的另一個 syslogd

記錄至 syslog 意味著來自 Proxy Server 和其他常駐應用程式的記錄都被收集在同一個檔案中，因此在記錄的訊息中增加了下列資訊，來識別來自特定伺服器實例的 Proxy Server 特有訊息：

- 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` 檔案中爲管理伺服器與伺服器實例配置 LOG 元素。

如需關於 UNIX 作業環境中使用的 syslog 記錄機制的更多資訊，請於終端提示處使用下列 man 指令：

```
man syslog

man syslogd

man syslog.conf
```

使用 Windows eventlog 記錄

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」。

記錄層級

下表按照嚴重性從低到高的次序，定義了 Proxy Server 中的記錄層級和訊息。

表 9-1 記錄層級

記錄層級	描述
finest	訊息指示除錯訊息的詳細程度。finest 最爲詳細。
finer	
fine	
info	訊息本質上是資訊性的，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。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

您可以將存取記錄檔和錯誤記錄檔設定爲自動歸檔。在某一時間，或者在指定間隔後，您的記錄將自動重建。Proxy Server 將儲存舊記錄檔，並用含有儲存日期及時間的名稱爲儲存的檔案加上戳記。

例如，您可以將存取記錄檔設定爲每隔一小時自動重建一次，Proxy Server 將儲存文件並命名爲 「access.200505160000」，其中記錄檔案的名稱、年、月、日與 24 小時制時間一起連成一個字元字串。依據您設定的記錄自動重建類型的不同，記錄歸檔檔案的確切格式也會不同。

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與基於 Cron 的記錄自動重建。

內部常駐程式記錄自動重建

這種記錄自動重建類型發生在 HTTP 常駐程式內，且只能在啓動時配置。內部常駐程式記錄自動重建可讓伺服器在無需重新啓動的情況下，於內部自動重建記錄。使用此方法自動重建的記錄將以下列格式儲存：

```
access.<YYYY><MM><DD><HHMM>
```

```
errors.<YYYY><MM><DD><HHMM>
```

您可以指定用於自動重建記錄檔案與啓動新記錄檔案的時間。例如，如果自動重建啓動時間爲凌晨 12:00，自動重建間隔爲 1440 分鐘 (一日)，當您儲存與套用變更時，不論當時時間爲何，都將立即建立新的記錄檔。記錄檔將在每天凌晨 12:00 自動重建，存取記錄將在凌晨 12:00 加戳記並儲存爲 `access.200505172400`。同樣，如果您將時間間隔設定爲 240 分鐘 (4 個小時)，4 個小時的時間間隔開始於凌晨 12:00，這樣存取記錄檔所包含資訊的收集時間段爲從凌晨 12:00 至上午 4:00、從上午 4:00 至上午 8:00、以此類推。

如果啓用了記錄自動重建，記錄檔自動重建將於伺服器啓動之時開始。要自動重建的第一個記錄檔在從目前時間到下一個自動重建時間這一時間段內收集資訊。以上述範例爲例，如果您將啓動時間設定爲凌晨 12:00，自動重建間隔爲 240 分鐘，且目前時間爲上午 6:00，則第一個自動重建的記錄檔包含從上午 6:00 至上午 8:00 收集的資訊，而下一個記錄檔包含從上午 8:00 至中午 12:00 收集的資訊。

基於排程程式的記錄自動重建

此類記錄自動重建基於 *server_root*/proxy-*server_name*/config/ 目錄下 `server.xml` 檔案中儲存的時間和日期。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儲存在 server_root/proxy-*server_name*/config/ 目錄的 `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`，它可能將變爲 `access.200505171630`。

伺服器啓動時，將初始化記錄自動重建。如果開啓自動重建功能，Proxy Server 會建立帶有時間戳記的存取記錄檔，並將在伺服器啓動時自動重建。

自動重建開始後，若出現需要記錄到存取記錄檔或錯誤記錄檔的請求或錯誤，並且它們發生在預先排程的「下一個自動重建時間」之後，則 Proxy Server 會建立帶時間戳記的新記錄檔。

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是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。

設定存取記錄喜好設定

在安裝期間，將爲伺服器建立名爲 access 的存取記錄檔。您可以透過指定是否記錄存取、使用什麼格式記錄、以及當用戶端存取資源時伺服器是否應花時間查找用戶端網域名稱，來自訂任何資源的存取記錄。

您可以使用 Server Manager 中的 [Set Access Log Preferences] 頁面來指定記錄喜好設定，或手動配置 obj.conf 檔案中的下列指令。在 obj.conf 中，伺服器將呼叫函數 flex-init 來初始化靈活記錄系統，並呼叫函數 flex-log 來以靈活記錄格式記錄請求所特有的資料。若要使用共用記錄檔格式記錄請求，伺服器將呼叫 init-clf 來初始化 obj.conf 中使用的「共用記錄」子系統，並呼叫 common-log 來以共用記錄格式 (爲大多數 HTTP 伺服器所採用) 記錄請求所特有的資料。

一旦建立了資源的存取記錄，您便無法變更其格式，除非將其歸檔或爲此資源建立新的存取記錄檔。

變更現有記錄檔的格式時，您應首先刪除 / 重新命名現有記錄檔或使用其他檔名。

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。將顯示 [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，輸入常規表示式並按一下 [OK]。
4. 指定是否記錄用戶端存取。這需要啓用網域名稱服務 (DNS)。
5. 指定存取記錄檔的絕對路徑。依預設，記錄檔儲存在伺服器根的 logs 目錄中。如果指定部分路徑，伺服器將假設此路徑與伺服器根中的 logs 目錄相關。

   如果編輯的是整個伺服器，則此欄位的預設值爲 $accesslog，它是配置檔案中表示伺服器之存取記錄檔的變數。
6. 選擇是否應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. 選擇存取記錄中使用的記錄檔格式類型。下列選項可供選用：
   - **Use Common LogFile Format。**包括用戶端的主機名稱、經認證的使用者名稱、請求日期與時間、HTTP 標頭、傳回至用戶端的狀態碼以及傳送給用戶端的文件的內容長度。
   - **Only Log。**可讓您選擇要記錄的資訊。您可以從以下靈活記錄格式項目中選擇：
     - **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。
     - **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"。**參考者用於指定一個頁面，用戶端從此頁面存取目前頁面。例如，如果使用者從文字搜尋查詢查看結果，則參考者將爲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、版本和執行的作業系統) 來自用戶端傳送給伺服器的 HTTP 標頭資訊中的 [User-agent] 欄位。
     - **Method。**使用的 HTTP 請求方式，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`，URI 爲 `special/docs`。
     - **Query String Of The URI。**URI 中問號之後的所有內容。例如，對於 `http://www.a.com:8080/special/docs?find_this`，URI 查詢字串爲 `find_this`。
     - **Protocol。**使用的傳輸協定和版本。
   - 若您選擇自訂格式，則請在 [Custom Format] 欄位中鍵入。
8. 按一下 [OK]。
9. 按一下 [Restart Required]。將顯示 [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

1. 存取 Server Manager，然後按一下 [Server Status] 標籤。
2. 按一下 [Set Access Log Preferences] 連結。將顯示 [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，輸入常規表示式，並按一下 [OK]。
4. 指定是否記錄用戶端存取。這需要啓用網域名稱服務 (DNS)。
5. 指定存取記錄檔的絕對路徑。依預設，記錄檔儲存在伺服器根的 logs 目錄中。如果指定部分路徑，伺服器將假設此路徑與伺服器根中的 logs 目錄相關。

   如果編輯的是整個伺服器，則此欄位的預設值爲 `$accesslog`，它是配置檔案中表示伺服器之存取記錄檔的變數。
6. 選擇是否應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. 選擇記錄檔的格式：共用、擴充、擴充 2、僅限指定的資訊 ([Only log] 單選按鈕)，或自訂。若您按一下 [Only log]，則可以使用以下靈活記錄格式項目：
8. 選擇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、擴充記錄檔格式、擴充 2 記錄檔格式、靈活記錄格式或您自己的可自訂格式。共用記錄檔格式爲一般支援的格式，可提供固定數量的伺服器資訊。靈活記錄格式可讓您選擇 (從 Proxy Server 中) 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、經認證的使用者名稱、請求日期與時間、HTTP 標頭、傳回至用戶端的狀態碼以及傳送給用戶端的文件的內容長度。
   - **Use Extended LogFile Format。**包括共用記錄檔格式的所有欄位，以及其他一些欄位，例如 [remote status]、[proxy to client content length]、[remote to proxy content length]、[proxy to remote content length]、[client to proxy header length]、[proxy to client header length]、[proxy to remote header length]、[remote to proxy header length] 與 [transfer time]。
   - **Use Extended2 LogFile Format。**包括擴充記錄檔格式的所有欄位，以及其他一些欄位，例如 [client status]、[server status]、[remote status]、[cache finish status] 和 [actual route]。

- **Only Log。**可讓您選擇要記錄的資訊。您可以從以下靈活記錄格式項目中選擇：
  - **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。
  - **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"。**參考者用於指定一個頁面，用戶端從此頁面存取目前頁面。例如，如果使用者從文字搜尋查詢查看結果，則參考者將爲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、版本和執行的作業系統) 來自用戶端傳送給伺服器的 HTTP 標頭資訊中的 [User-agent] 欄位。
  - **Method。**使用的 HTTP 請求方式，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`，URI 爲 `special/docs`。
  - **Query String Of The URI。**URI 中問號之後的所有內容。例如，對於 `http://www.a.com:8080/special/docs?find_this`，URI 查詢字串爲 `find_this`。
  - **Protocol。**使用的傳輸協定和版本。
  - **Cache Finish Statu。**此欄位指定是寫入、更新還是由更新檢查傳回快取檔案。
  - **Remote Server Finish Status。**此欄位指定向遠端伺服器發出的請求是成功地完成、在用戶端按一下 Netscape Navigator 中的 [停止] 按鈕後被中斷，還是因錯誤狀況而中止。
  - **Status Code From Server。**從伺服器傳回的狀態代碼。
  - **Route To Proxy (PROXY, SOCKS, DIRECT)。**用來擷取資源的路由。可直接、透過代理伺服器或透過 SOCKS 伺服器擷取文件。
  - **Transfer Time。**傳輸的時間長度 (以秒或毫秒爲單位)。

- **Header-length From Server Response**。伺服器回應的標頭長度。
- **Request Header Size From Proxy To Server**。代理向伺服器發出之請求標頭的大小。
- **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**。從用戶端收到的請求標頭的大小。
- **Content-length From Proxy To Server Request**。從代理傳送至伺服器的文件長度 (以位元組爲單位)。
- **Content-length Received From Client**。來自用戶端的文件的長度 (以位元組爲單位)。
- **Content-length From Server Response**。來自伺服器的文件的長度 (以位元組爲單位)。
- **Unverified User From Client**。在認證期間爲遠端伺服器指定的使用者名稱。

o 若您選擇自訂格式，則請在 [Custom Format] 欄位中鍵入。

9. 如果您不想記錄來自某些主機名稱或 IP 位址的用戶端存取，請將其鍵入 [host names] 和 [IP Addresses] 欄位中。對於伺服器不應記錄其存取動作的主機，可以萬用字元式樣輸入。例如，`*.example.com` 不會記錄 example.com 網域中人員的存取。您可以爲主機名稱和 IP 位址中的一個或兩者輸入萬用字元式樣。
10. 選擇是否要在記錄檔案內包含格式字串。如果使用 Proxy Server 的記錄分析器，則應包含格式字串。如果使用協力廠商的分析器，則可能不需要在記錄檔案內包含格式字串。
11. 按一下 [OK]。
12. 按一下 [Restart Required]。將顯示 [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 提供了一種使用 flexlog 功能記錄特定 cookie 的簡便方式。將「`Req->headers.cookie.cookie_name`」加入到配置檔案 `obj.conf` 中用於初始化 `flex-log` 子系統的行內。如果請求標頭中提供了 cookie 變數 `cookie_name`，將記錄此 cookie 變數的值；如果未提供，將記錄「-」。

設定錯誤記錄選項

Proxy Server 可讓您配置要記錄在伺服器錯誤記錄中的資訊。

設定錯誤記錄選項

1. 若要在 Administration Server 中設定錯誤記錄選項，請選擇 [Preferences] 標籤，然後按一下 [Set Error Log Preferences] 連結。

   若要在 Server Manager 中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. 在 [Log Level] 下拉式清單中，指定應記錄在錯誤記錄中的資訊量。下列選項可供選用：
4. 如果您要將 stdout 輸出重新導向至錯誤記錄，請選取 [Log Stdout] 核取方塊。
5. 如果您要將 stderr 輸出重新導向至錯誤記錄，請選取 [Log Stderr] 核取方塊。
6. 選取 [Log To Console] 核取方塊可將記錄訊息重新導向至主控台。
7. 如果您要使用 UNIX syslog 服務或 Windows 的事件記錄來產生和管理記錄，請選取 [Use System Logging] 核取方塊。
8. 按一下 [OK]。
9. 按一下 [Restart Required]。將顯示 [Apply Changes] 頁面。
10. 按一下 [Restart Proxy Server] 按鈕以套用變更。

配置 LOG 元素

下表描述了您可在 `server.xml` 檔案中配置的 LOG 元素的屬性：

表 9-2 LOG 屬性

屬性	預設值	描述
`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。允許的值如下 (依從最高到最低的次序) ： `finest`、`fine`、`fine`、`info`、`warning`、`failure`、`config`、`security` 與 `catastrophe`。

表 9-2 LOG 屬性

屬性	預設值	描述
logstdout	true	(可選) 如果爲 true，則將 stdout 輸出重新導向至錯誤記錄。合法值爲 on、off、yes、no、1、0、true、false。
logstderr	true	(可選) 如果爲 true，則將 stderr 輸出重新導向至錯誤記錄。合法值爲 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。
createconsole	false	(可選，僅限於 Windows) 如果爲 true，則爲 stderr 輸出建立 Windows 主控台。合法值爲 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。合法值爲 on、off、yes、no、1、0、true、false。

檢視存取記錄檔

您可以檢視伺服器的作用中存取記錄檔和已歸檔存取記錄檔。

若要從 Administration Server 檢視 Administration Server 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。

以下是共用記錄檔格式的存取記錄範例 (您可在 [Log Preferences] 視窗中指定此格式；如需更多資訊，請參閱第 168 頁的「設定存取記錄喜好設定」)：

```
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
```

表 9-3 說明此存取記錄範例的最後一行。

表 9-3 此存取記錄檔範例最後一行中的欄位

存取記錄欄位	範例
用戶端的主機名稱或 IP 位址	`198.18.17.222` (在此例中，因爲停用了代理伺服器的 DNS 查找設定，所以顯示用戶端的 IP 位址；如果啓用了 DNS 查找，則顯示用戶端的主機名稱。)
RFC 931 資訊	- (未實作 RFC 931 識別)
使用者名稱	abc (用戶端輸入的用於認證的使用者名稱)
請求的日期 / 時間	20/May/2005:14:16:09 +0530
請求	GET
協定	HTTP/1.1
狀態碼	504
傳輸的位元組	630

檢視錯誤記錄檔

錯誤記錄檔包含自建立記錄檔以來伺服器遇到的錯誤；也包含關於伺服器的資訊訊息，如啓動伺服器的時間。錯誤記錄中還記錄未成功的使用者認證。使用錯誤記錄可以尋找中斷的 URL 路徑或遺漏的檔案。

若要從 Administration Server 中檢視 Administration Server 的錯誤記錄檔，請選擇 [Preferences] 標籤，然後按一下 [View Error Log] 連結。

若要從 Server Manager 中檢視伺服器實例的錯誤記錄檔，請選擇 [Server Status] 標籤，然後按一下 [View Error Log] 連結。

以下是錯誤記錄中項目的三個範例。

```
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 文件介紹了此工具的參數。server-install/extras/flexanlg 目錄包含用於分析靈活記錄檔格式的指令行記錄分析器。但是，無論您選取了何種記錄檔格式，Server Manager 都預設使用靈活記錄檔報告工具。

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。您也可以從 Proxy Server 或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，應歸檔伺服器記錄。如需關於歸檔伺服器記錄的更多資訊，請參閱第 166 頁的 「歸檔記錄檔」。

您也可以首先轉到 server_root/proxy-server*id* 目錄，然後在指令提示處鍵入 **./start -shell**，而不用設定程式庫路徑。

若使用擴充或擴充 2 記錄格式，則除了您指定要報告的資訊之外，記錄分析器還會在輸出檔案中產生數個報告。後面幾個小節將描述這些報告。

傳輸時間分配報告

傳輸時間分配報告顯示代理伺服器傳輸請求花費的時間。此報告顯示的資訊依服務時間與完成百分比加以分類。以下是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%].........................................
```

狀態碼報告

狀態碼報告顯示代理伺服器從遠端伺服器接收的和向用戶端傳送的狀態碼與其數量。狀態碼報告還提供所有狀態碼的解釋。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
407		5 [1.0%]	Proxy authorization required
500		2 [0.4%]	Internal server error
504		6 [1.3%]	Gateway timeout

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的資料流量 (傳輸的位元組數目)。對於每種分析藍本，報告都將顯示以標頭與內容形式傳輸的資料量。資料流量報告還會顯示從快取記憶體到用戶端的資料流量。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

請求與連線報告

請求與連線報告顯示代理伺服器從用戶端接收的請求數目、代理伺服器與遠端伺服器建立的連線數目 (初始擷取、更新檢查與重新整理) 與代理伺服器藉由使用快取的文件來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的效能、代理伺服器快取的效能與直接連線的效能。

用戶端快取

備註 當用戶端對文件執行更新檢查時，如果遠端伺服器傳回 304 訊息，告知用戶端文件並未修改，則將發生用戶端快取命中。由用戶端發起的更新檢查將指示用戶端在快取記憶體中擁有自己的文件副本。

對於用戶端的快取，報告將顯示：

- **client and proxy cache hits：**一種用戶端快取符合情況，在這種符合情況中，代理伺服器與用戶端皆擁有請求文件的副本，首先透過查詢遠端伺服器針對代理伺服器的副本進行更新檢查，而之後針對代理伺服器的副本評估用戶端的請求。快取效能報告顯示代理伺服器服務的此類型請求的數目，與服務這些請求所用的平均時間量。
- **proxy shortcut no-check：**一種用戶端快取符合情況，在這種符合情況中，代理伺服器與用戶端皆擁有請求文件的副本，代理伺服器將告知用戶端 (無需與遠端伺服器確認) 用戶端快取記憶體中的文件是最新的。快取效能報告將顯示代理服務的此類型請求的數目，與服務這些請求所用的平均時間。
- **client cache hits only：**一種用戶端快取符合情況，在這種符合情況中，僅有用戶端擁有請求文件的副本。在此類型的請求中，代理伺服器直接爲用戶端的 If-modified-since GET 標頭建立通道。快取效能報告將顯示代理服務的此類型請求的數目，與服務這些請求所用的平均時間。
- **total client cache hits：**用戶端快取符合項目的總數目與服務這些請求所用的平均時間量。

代理伺服器快取

當用戶端從代理伺服器請求文件，如果代理伺服器的快取記憶體中已擁有此文件時，將發生代理快取符合情況。對於代理伺服器的快取符合項目，報告將顯示：

- **proxy cache hits with check：**一種代理伺服器快取符合情況，在這種符合情況中，代理伺服器查詢遠端伺服器來對文件進行更新檢查。快取效能報告將顯示代理服務的此類型請求的數目，與服務這些請求所用的平均時間。
- **proxy cache hits without check：**一種代理伺服器快取符合情況，在這種符合情況中，代理伺服器不查詢遠端伺服器來對文件進行更新檢查。快取效能報告將顯示代理服務的此類型請求的數目，與服務這些請求所用的平均時間。
- **pure proxy cache hits：**一種代理伺服器快取符合情況，在這種符合情況中，用戶端沒有請求文件的快取副本。快取效能報告將顯示代理服務的此類型請求的數目，與服務這些請求所用的平均時間。

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，報告將顯示：

- **total proxy cache hits：**代理伺服器快取符合項目的總數目與服務這些請求所用的平均時間量。

直接作業事件

直接作業事件是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。快取效能報告將顯示代理伺服器服務的此類型請求的數目、服務這些請求所用的平均時間與總作業事件的百分比。
- **other transactions**：使用非 200 或 304 狀態碼傳回的作業事件。快取效能報告顯示代理伺服器服務的此類型請求的數目與服務這些請求所用的平均時間。
- **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)。快取效能報告將顯示代理伺服器服務的此類型請求的數目、服務這些請求所用的平均時間與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。此報告顯示以下類別的值：

average transaction time：記錄的所有傳輸時間的平均值。

average transfer time without caching：不是從快取記憶體傳回的作業事件 (來自遠端伺服器的 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 與 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沒有錯誤情況下的平均傳輸時間。

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

對於分析的每個小時，每小時作業報告將顯示：

- 平均負載
- 不對遠端伺服器進行更新檢查的快取符合項目數目
- 對遠端伺服器進行更新檢查 (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
- 對遠端伺服器進行更新檢查 (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
- 對遠端伺服器進行更新檢查 (導致文件的部分被更新) 的代理伺服器快取符合項目數目
- 對遠端伺服器進行更新檢查 (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且無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。將顯示 [Generate Reports] 頁面。
3. 鍵入伺服器名稱，此名稱將顯示於產生的報告中。
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案。
6. 若您想要將結果儲存於檔案中，請在 [Output File] 欄位中鍵入輸出檔名。如果保留此欄位爲空白，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，因爲將輸出列印到螢幕上可能需要很長時間。

7. 選取是否爲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。**使用請求文件本地副本的次數，而非伺服器傳回頁面的次數。
   - **302 (Redirects) Status Codes。**伺服器因原始 URL 被移動而重新導向至新 URL 的次數。
   - **404 (Not Found) Status Codes。**伺服器找不到請求文件或由於用戶端不是授權的使用者而不提供文件的次數。
   - **500 (Server Error) Status Codes。**發生與伺服器相關的錯誤之次數。
   - **Total Unique URLs。**啓用存取記錄以來所存取的唯一 URL 的數目。
   - **Total Unique Hosts。**啓用存取記錄以來存取過伺服器的唯一主機的數目。
   - **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：
9. **Find Top *Number* Seconds Of Log。**基於最近幾秒鐘內的資訊產生統計資料。
10. **Find Top *Number* Minutes Of Log。**基於最近幾分鐘內的資訊產生統計資料。
11. **Find Top *Number* Hours Of Log。**基於最近幾小時內的資訊產生統計資料。
12. **Find *Number* Users (If Logged)。**基於使用者數目的資訊產生統計資料。
13. **Find Top *Number* Referers (If Logged)。**基於參考者數目的資訊產生統計資料。
14. **Find Top *Number* User Agents (If Logged)**。基於有關使用者代理程式的資訊 (例如瀏覽器類型、瀏覽器版本和作業系統) 產生統計資料。
15. **Find Top *Number* Miscellaneous Logged Items (If Logged)。**基於使用者數目的資訊產生統計資料。
16. 選擇是否產生清單。如果您選擇產生清單，請從以下清單中指定要產生清單的項目：
    - **URLs Accessed。**顯示存取過的 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數目的 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。**顯示存取伺服器的次數超過指定數目的主機。

17. 指定查看結果的順序。按照您希望各部分在報告中顯示的順序，爲以下項目賦予從 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。選項如下：
    - [Find Totals]
    - [General Statistics]
    - [Make Lists]
18. 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

若要透過指令行分析存取記錄檔，請執行工具 `flexanlg` (位於目錄 `server-install/extras/flexanlg` 中)。

若要執行 `flexanlg`，請於指令提示處鍵入下列指令與選項：

```
./flexanlg [-n name] [-x] [-r] [-p order] [-i file]* [ -m metafile ]* [-o file][-c opts] [-t opts] [-l opts]
```

標示 * 的選項可以重複。

以下是語法的描述。（鍵入 ./flexanlg -h. 可以在線上取得此資訊）：

```
-P：代理伺服器記錄格式                                          預設爲： no
-n servername：伺服器名稱
-x：以 HTML 輸出                                                預設爲： no
-r：將 IP 位址解析爲主機名稱                                    預設爲：no
-p [c,t,l]：輸出次序（計數、時間統計資料、清單）  預設爲： ctl
-i filename：輸入記錄檔                  預設爲： none
-o filename：輸出記錄檔                                         預設爲： stdout
-m filename：中介檔                  預設爲： none
-c [h,n,r,f,e,u,o,k,c,z]：對這些項目計數 -          預設爲： hnreuokc
    h：符合項目總數
    n：304 Not Modified 狀態碼（使用本機副本）
    r：302 Found 狀態碼（重新導向）
    f：404 Not Found 狀態碼（未找到文件）
    e：500 Server Error 狀態碼（配置不當）
    u：唯一 URL 總數
    o：唯一主機總數
    k：傳輸的千位元組總數
    c：快取記憶體儲存的千位元組總數
    z：不對任何項目計數。
-t [sx,mx,hx, xx,z]：尋找時間統計資料  預設爲： s5m5h10u10a10r10x10
    s(number)：尋找最近 (number) 秒的記錄
    m(number)：尋找最近 (number) 分鐘的記錄
    h(number)：尋找最近 (number) 小時的記錄
    u(number)：尋找記錄中最上面的 (number) 個使用者
    a(number)：尋找記錄中最上面的 (number) 個使用者代理程式
    r(number)：尋找記錄中上面的 (number) 個參考者
    x(number)：尋找最上面的 (number) 個雜項關鍵字
    z：不尋找任何時間統計資料。
-l [cx,hx]：產生清單 -                                          預設爲： c+3h5
    c(x,+x)：最常存取的 URL
             (x：僅列示 x 個項目）
              (+x：僅在存取次數多於 x 次時列示）
    h(x,+x)：最經常存取您的伺服器的主機（或 IP 位址）
              (x：僅列示 x 個項目）
              (+x：僅在存取次數多於 x 次時列示）
    z：不產生任何清單。
```

檢視事件 (Windows)

除了將錯誤記錄到伺服器錯誤記錄中，Proxy Server 還會將嚴重的系統錯誤記錄到事件檢視器內。事件檢視器可讓您監視系統上的事件。在開啓錯誤記錄之前，可使用事件檢視器查看基礎配置問題所導致的錯誤。

使用事件檢視器

1. 從 [開始] 功能表中，選取 [程式集]，然後選取 [管理工具]。在 [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 中的錯誤帶有 `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

監視伺服器

本章包含有關伺服器監視方法的資訊，包括內建監視工具及簡易網路管理協定 (SNMP)。

您可以將 SNMP、Sun Java System 管理資訊庫 (MIB) 以及網路管理軟體 (如 HP OpenView) 配合使用，以便像監視網路中的其他裝置那樣即時監視伺服器。

備註 在 Windows 上，在安裝 Proxy Server 4 之前，請確定您的系統已經安裝了 Windows SNMP 元件。

您可以使用統計資料功能或 SNMP 來即時檢視伺服器的狀況。如果您使用的是 UNIX 或 Linux，要想使用 SNMP，必須針對它配置您的 Proxy Server。本章提供了當您在 UNIX 或 Linux 上與配合使用 SNMP 和 Proxy Server 時所需的資訊。

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狀態。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此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 的系統經常性耗用。若啓用統計資料，伺服器會開始收集與儲存統計資料資訊。

一旦啓用了統計資料，您便可以檢視下列方面的統計資料：

- 連線
- DNS
- 持續作用
- 快取
- 伺服器請求

互動式伺服器監視器會報告各種伺服器統計資料的總數，如需有關各種伺服器統計資料的描述，請參閱線上說明中的 [Monitor Current Activity] 頁面。

處理 Proxy Server 統計資料

可使用稱爲 `stats-xml` 的內建函數收集 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` 函數產生報告。`stats-xml` 函數亦用於啓用設定檔，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設定檔，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"
```

它亦會建立 `NameTrans` 指令，使您能夠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，啓用統計資料會增加 `Service` 指令，以在選取 `NameTrans` 指令後處理 `stats-xml` 函數。

```
<Object name="stats-xml">

Service fn="stats-xml"
```

```
</Object>
```

備註 收集統計資料時會更新 obj.conf 中的 Init 函數。因此，您必須先停止然後再啓動您的伺服器以使這些變更生效。

您可使用下列 URL 擷取 stats-xml 輸出：

`http://`*computer_name*`:`*proxyport*`/stats-xml/proxystats.xml`

此請求將會傳回包含 Proxy Server 統計資料的 XML 頁面。有些瀏覽器允許您在瀏覽器視窗內檢視資料，有些則會要求您將資料儲存至外部檔案，然後再以外部檢視器檢視資料。若無法針對分析資料的不同檢視進行剖析，則此資訊的助益不會非常明顯。使用第三方工具對這一程序將有所幫助。若無剖析工具，則最好使用 Server Manager 或 perfdump SAF 來觀察 stats-xml 輸出。

限定存取 stats-xml 輸出

若您想要對可從瀏覽器檢視您伺服器的 stats-xml 統計資料之使用者進行限定，應針對 /stats-xml URI 建立 ACL。

還必須在 obj.conf 檔案中的 stats-xml 物件定義內參考 ACL 檔案。例如，若您已針對 /stats-xml URI 建立已命名的 ACL，則將需要依下列所示在物件定義中的 PathCheck 敘述內參考 ACL 檔案：

```
<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 上啓動統計資料才能監視效能。您可利用 Server Manager 或編輯 obj.conf 與 magnus.conf 檔案來執行上述作業。爲監視及調校建立自動工具或編寫自訂程式的使用者可能更喜歡直接處理 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。將顯示 [Monitor Current Activity] 頁面。
3. 針對 [Activate Statistics/Profiling?] 元素選取 [Yes] 選項以啓用統計資料。
4. 按一下 [OK]。
5. 按一下 [Restart Required]。將顯示 [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 中的預設物件下，增加下列行：

```
NameTrans fn="assign-name" name="stats-xml"
from="(/stats-xml|/stats-xml/.*)"
```

2. 在 `obj.conf` 中增加下列 Service 函數：

```
<Object name="stats-xml">

Service fn="stats-xml"

</Object>
```

3. 在 `magnus.conf` 中增加 `stats-init` SAF。

以下爲 `obj.conf` 中的 `stats-init` 的一個範例：

```
Init profiling="on" fn="stats-init" update-interval="5"
```

上述範例顯示您亦可指定下列項目：

- **update-interval。**以秒爲單位的統計資料更新期間。設定值越高 (頻率越低) 系統效能越好。最小值爲 1，預設值爲 5。
- **profiling。**啓動 NSAPI 效能設定檔。預設值爲 [no]，可稍微增進伺服器效能。不過，若您透過使用者介面啓動統計資料，依預設將開啓設定檔。

使用統計資料

一旦啓用了統計資料，您即可取得有關伺服器實例執行方式的各種資訊。統計資料被分爲多個功能區域。

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] 下拉式清單中選擇更新間隔。

   更新間隔是指兩次更新所顯示統計資料資訊間隔的秒數。
4. 從 [Select Statistics To Be Displayed] 下拉式清單中選擇您想要顯示的統計資料種類。如需有關統計資料類型的更多資訊，請參閱第 191 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啓用了 [Statistics/Profiling]，則您會看到一個顯示所選統計資料種類的頁面。此頁面每隔 5 到 15 秒更新一次，視您選擇的更新間隔而定。
6. 從下拉式清單中選取程序 ID。

   您可利用 Server Manager 檢視目前的作業，但這些種類對於調校您的伺服器並無完全的相關性。建議使用 Perfdump 統計資料調校您的伺服器。

在 Server Manager 中顯示統計資料

本節說明如何才能在 Server Manager 中檢視 `proxystats.xml` 資料。

您可檢視總數、最大值、尖峰數以及與 Proxy Server 連線、DNS 處理、持續作用值、快取及伺服器請求相關之資訊的條形圖。

下一節描述上述各項目可取得的資訊類型。

連線統計資料

您可從 Server Manager 取得下列連線統計資料：

- 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

DNS 統計資料

您可從 Server Manager 取得下列 DNS 統計資料：

- 最大 DNS 快取項目數
- 程序數
- DNS 快取符合項目數 (亦顯示爲條形圖)
- DNS 快取不符合項目數 (亦顯示爲條形圖)

持續作用統計資料

您可從 Server Manager 取得下列持續作用統計資料：

- 最大持續作用連線數
- 持續作用逾時
- 程序數
- 持續作用符合項目數 (亦顯示爲條形圖)
- 持續作用更新次數 (亦顯示爲條形圖)
- 持續作用拒絕次數 (亦顯示爲條形圖)
- 持續作用逾時次數 (亦顯示爲條形圖)

快取統計資料

您可從 Server Manager 取得下列快取統計資料：

- 最長快取存在時間 (以秒爲單位)
- 最大堆疊快取大小
- 最大記憶體快取對映大小
- 程序數
- 快取符合項目數 (亦顯示爲條形圖)
- 快取不符合項目數 (亦顯示爲條形圖)
- 資訊快取符合項目數 (亦顯示爲條形圖)
- 資訊快取不符合項目數 (亦顯示爲條形圖)
- 內容快取符合項目數 (亦顯示爲條形圖)

- 內容快取不符合項目數 (亦顯示爲條形圖)

伺服器請求統計資料

您可從 Server Manager 取得下列伺服器請求統計資料：

- 請求總數
- 接收位元組數
- 傳送位元組數
- 程序數
- 依 HTTP 伺服器代碼分解請求 (亦顯示爲條形圖) 例如，HTTP 伺服器代碼 200 表示完成的請求。

使用 perfdump 公用程式監視目前作業

Perfdump 公用程式是 Proxy Server 內建的一種伺服器應用程式函數 (SAF)，它會從 Proxy Server 內部統計資料收集效能資料片段，並將之以 ASCII 文字顯示。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。它不是只監視單一程序，而是將統計資料與程序數相乘，這樣可從整體上提供更精確的伺服器狀況。

啓用 perfdump 公用程式

啓用 `stats-xml` 函數後，您才能啓用 perfdump SAF，而且您僅能以直接編輯 `obj.conf` 檔案的方式予以啓用。

啓用 perfdump SAF：

1. 在 `obj.conf` 檔案的預設物件後增加下列物件：

   ```
   <Object name="perf">

   Service fn="service-dump"

   </Object>
   ```

2. 將下列項目增加至預設物件：

   ```
   NameTrans fn=assign-name from="/.perf" name="perf"
   ```

3. 重新啓動您的伺服器軟體。

4. 輸入此 URL 以存取 perfdump：

   `http://`*computer_name:proxyport*`/.perf`

   您可請求 perfdump 統計資料，並指定瀏覽器自動更新的頻率 (以秒爲單位)。下面的範例設爲每 5 秒更新一次：

   `http://`*computer_name:proxyport*`/.perf?refresh=5`

Perfdump 輸出範例

下列爲 Perfdump 輸出範例：

```
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

CacheInfo:
```

```
------------------
enabled             yes
CacheEntries        0/1024
Hit Ratio           0/0 (  0.00%)
Maximum Age         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」第 2 章的「Using Statistics to Tune Your Server」，其網址爲：

http://docs.sun.com/source/817-6249/index.html

限定存取 perfdump 輸出

若您想要對可從瀏覽器檢視您伺服器的 perfdum 統計資料的使用者進行限定，需要針對 /.perf URI 建立 ACL。

還必須在 obj.conf 檔案中的 perf 物件定義內參考 ACL 檔案。例如，若您已針對 /.perf URI 建立已命名的 ACL，則需要依下列所示在物件定義中的 PathCheck 敘述內參考 ACL 檔案：

```
<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。每次執行一種函數時，伺服器便會收集統計資料，並將之增加至儲存區。例如，send-cgi 和 NSServletService 函數分別用於爲 CGI 與 Java servlet 請求提供服務。您可定義兩個儲存區以維護 CGI 與 servlet 請求的單獨計數，或是建立一個儲存區以計算兩類動態內容的請求數。收集此資訊的成本極低，對於伺服器效能的影響通常微乎其微。您日後可使用 perfdump 公用程式存取此資訊。下列資訊儲存於儲存區中：

- **Name of the bucket。**此名稱用於將儲存區與某函數相關聯。
- **Description。**與儲存區關聯的函數的說明。
- **Number of requests for this function。**呼叫此函數的請求總數。
- **Number of times the function was invoked。**此數字與函數的請求數可能不一致，因爲針對一個請求，有些函數可能執行多次。
- **Function latency or the dispatch time。**伺服器呼叫此函數所耗費的時間。
- **Function time。**此函數本身所耗費的時間。

default-bucket 由伺服器預先定義。它會爲未與任何使用者定義儲存區相關聯的函數記錄統計資料。

配置

您必須在 magnus.conf 與 obj.conf 檔案中指定效能儲存區的所有配置資訊。系統僅會自動啓用預設儲存區。

首先，您必須依照第 193 頁的「使用 perfdump 公用程式監視目前作業」中所述啓用效能測量。

下列範例顯示如何在 magnus.conf 中定義新儲存區：

```
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"
```

上述範列會建立三個儲存區：acl-bucket、file-bucket 與 cgi-bucket。若要將這些儲存區與函數相關聯，請將 bucket=*bucket-name* 增加至您要進行效能測量的 obj.conf 函數。

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

您可使用 perfdump 公用程式存取儲存區中的伺服器統計資料。此效能儲存區資訊位於 perfdump 所傳回報告中最後的一部分。

報告包含以下資訊：

- Average、Total 與 Percent 欄提供每項請求的統計資料。
- Request Processing Time 是伺服器處理目前已接收之所有請求所需的總時間。
- Number of Requests 是此函數的總請求數。
- Number of Requests 是呼叫此函數的總次數。此數值與請求數不同，因爲處理一個請求時可能會多次呼叫某函數。此列的百分比欄參照所有儲存區的總呼叫數計算。

- Latency 是 Proxy Server 爲呼叫函數做準備所耗費的時間 (以秒爲單位)。
- Function Processing Time 是 Proxy Server 在函數內所耗費的時間 (以秒爲單位)。Function Processing Time 和 Total Response Time 百分比參照 Request Processing Time 總數計算。
- Total Response Time 是 Function Processing Time 與 Latency 的總和 (以秒爲單位)。

下列爲可透過 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 是適用於網路活動資料交換的協定。透過 SNMP，資料在受管理裝置與網路管理工作站 (NMS) 之間傳輸。受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 是用於遠端管理網路的系統。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 通常是指安裝了一個或多個網路管理應用程式的功能強大的工作站。諸如 HP OpenView 的網路管理應用程式以圖形的方式顯示有關受管理裝置 (如您的 Web 伺服器) 的資訊。例如，它可以顯示您企業中工作和停用的伺服器以及收到的錯誤訊數目與類型。當 SNMP 與代理伺服器配合使用時，會使用兩類代理程式 (子代理程式和主代理程式) 在 NMS 與伺服器之間傳輸上述資訊。

子代理程式會收集有關伺服器的資訊，並將這些資訊傳送至伺服器的主代理程式。除了 Administration Server，每個伺服器都具有子代理程式。

備註 變更任何 SNMP 配置之後，您必須按一下 [Apply Required] 按鈕，然後重新啓動 SNMP 子代理程式。

主代理程式會與 NMS 進行通訊。主代理程式隨附 Administration Server 一同安裝。

您可以在一台主機電腦上安裝多個子代理程式，但僅能安裝一個主代理程式。例如，如果您在同一台主機上安裝了 Directory Server、Proxy Server 以及 Messaging Server，則每個伺服器的子代理程式將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。主代理程式可存取的變數稱爲受管理物件。這些物件在稱爲管理資訊庫 (MIB) 的樹狀結構中進行定義。使用 MIB，可存取 Proxy Server 的網路配置、狀態以及統計資料。使用 SNMP，您可以從 NMS 檢視此資訊。MIB 樹的頂層表明網際網路物件識別碼具有以下四個子樹：directory (1)、mgmt (2)、experimental (3) 以及 private (4)。子樹 private (4) 包含節點 enterprises (1)。Enterprises (1) 節點中的每個子樹被指定給個別的企業，此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 位於節點 enterprises (1) 之下。Sun Java System 伺服器 MIB 位於節點 enterprises (1) 之下。每個 Sun Java System 伺服器子代理程式都會提供一個 MIB 以用於 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 也可以在伺服器的 MIB 中查詢資料，或者從遠端變更 MIB 中的變數。每個 Sun Java System 伺服器均具有自己的 MIB。所有 Sun Java System 伺服器 MIB 均位於：

```
server_root/plugins/snmp
```

Proxy Servers MIB 是名爲 proxyserv40.mib 的檔案。此 MIB 包含有關 Proxy Server 網路管理的各種變數的定義。您可使用 Proxy Server MIB 檢視 Proxy Server 的管理資訊，並即時監視伺服器。

設定 SNMP

通常，若要使用 SNMP，您的系統上必須安裝並執行一個主代理程式和至少一個子代理程式。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：

- 您的系統是否已經在執行 SNMP 代理程式 (您作業系統的本端代理程式)？
- 如果執行，您的本端 SNMP 代理程式是否支援 SMUX 通訊？ (如果您使用的是 AIX 平台，則系統支援 SMUX。)

請參閱您的系統文件，以取得有關如何確認此資訊的資訊。

備註 變更 Administration Server 中的 SNMP 設定，安裝新伺服器、或刪除現有伺服器之後，您必須執行下列步驟：

- (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 1 啓用 SNMP 主代理程式與子代理程式的簡介。

如果您的伺服器符合這些條件 ...	... 請遵循這些程序。在後面的小節中詳細地論述它們。
• 目前尚未執行任何本端代理程式	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。
• 目前正在執行本端代理程式 • 無 SMUX • 無需繼續使用本端代理程式	1. 當您爲 Administration Server 安裝了主代理程式之後，請停止本端代理程式。 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。
• 目前正在執行本端代理程式 • 無 SMUX • 需要繼續使用本端代理程式	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. 使用主代理程式連接埠號之外的連接埠號，重新啓動本端代理程式。 5. 爲系統上安裝的每個伺服器啓用子代理程式。
• 目前正在執行本端代理程式 • 支援 SMUX	1. 重新配置本端 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。

使用代理伺服器 SNMP 代理程式 (UNIX)

執行本端代理程式之後，如果要繼續將其與 Proxy Server 主代理程式配合使用，需要使用 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，您需要安裝然後啓動它。您還必須使用執行 Proxy Server 主代理程式的連接埠以外的連接埠號重新啓動本端 SNMP 主代理程式。

本節包括下列主題：

- 安裝代理伺服器 SNMP 代理程式
- 啓動 SNMP 代理程式
- 重新啓動本端 SNMP 常駐程式

安裝代理伺服器 SNMP 代理程式

如果您的系統已經在執行 SNMP 代理程式，並且您要繼續使用本端 SNMP 常駐程式，請遵循這些小節中的步驟：

1. 安裝 SNMP 主代理程式。請參閱第 203 頁的「安裝 SNMP 主代理程式」。
2. 安裝並啓動 SNMP 代理程式，然後重新啓動本端 SNMP 常駐程式。請參閱第 201 頁的「使用代理伺服器 SNMP 代理程式 (UNIX)」。
3. 啓動 SNMP 主代理程式。請參閱第 204 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 208 頁的「啓用子代理程式」。

若要安裝 SNMP 代理程式，請編輯 CONFIG 檔案 (您可以使用其他名稱命名此檔案)，使其包含 SNMP 常駐程式要偵聽的連接埠。此檔案位於伺服器根目錄下的 `plugins/snmp/sagt` 中。它還需要包含 SNMP 代理程式要轉寄的 MIB 樹和陷阱。

以下是 CONFIG 檔案的範例：

```
AGENT AT PORT 1161 WITH COMMUNITY public
SUBTREES       1.3.6.1.2.1.1,
                   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 SNMP 代理程式，請在指令提示下輸入以下內容：

```
# 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，您需要在 CONFIG 檔案中所指定的連接埠處重新啓動本端 SNMP 常駐程式。若要重新啓動本端 SNMP 常駐程式，請在指令提示下輸入以下內容：

```
# snmpd -P port_number
```

其中，*port_number* 爲在 CONFIG 檔案中指定的連接埠號。例如，在 Solaris 平台，使用上面提及的 CONFIG 檔案範例中的連接埠，您應該輸入：

```
# 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篩選其通訊。需要對其中一個名爲 snmpd.conf 的配置檔案進行變更，以便 SNMP 常駐程式接受來自於 SMUX 子代理程式的訊息。如需更多資訊，請參閱線上手冊中有關 snmpd.conf 的內容。您需要增加一行來定義各個子代理程式。

例如，您需要將此行增加至 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* 爲此主機的網路遮罩。

備註	請勿使用回送位址 127.0.0.1，要使用實際的 IP 位址。

安裝 SNMP 主代理程式

若要配置 SNMP 主代理程式，您必須做爲超級使用者安裝 Administration Server 實例。不過，透過將 SNMP 子代理程式配置爲與主代理程式配合使用，即使是非超級使用者也可以在 Web Server 實例上完成基本的 SNMP 工作 (如 MIB 瀏覽)。

安裝主 SNMP 代理程式

1. 以超級使用者身份登入。
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，請移往第 4 步。

   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，並瞭解其所支援的 MIB 樹。
3. 如果 SNMP 常駐程式正在執行，請終止其程序。
4. 在 Administration Server 中，從 [Global Settings] 標籤內選擇 [Set SNMP Master Agent Trap] 頁面。
5. 鍵入執行網路管理軟體的系統名稱。
6. 鍵入網路管理系統偵聽陷阱的連接埠號。(眾所周知的連接埠爲 162。) 如需有關陷阱的更多資訊，請參閱。
7. 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。
8. 按一下 [OK]。
9. 在 Administration Server 中，從 [Global Settings] 標籤內選擇 [Set SNMP Master Agent Community] 頁面。
10. 爲主代理程式鍵入社群字串。
11. 爲社群選擇一項作業。
12. 按一下 [New]。

啓用與啓動 SNMP 主代理程式

主代理程式作業是在一個名爲 CONFIG 的配置檔案中定義的。您可以使用「Server Manager」編輯 CONFIG 檔案或手動編輯此檔案。您必須先安裝 SNMP 主代理程式，然後才能啓用 SNMP 子代理程式。

在重新啓動主代理程式的時候，如果您收到一個類似於「System Error: Could not bind to port」的連結錯誤，請使用 `ps -ef | grep snmp` 檢查是否正在執行 `magt`。如果正在執行，請使用指令 `kill -9 pid` 結束程序。SNMP 的 CGI 將再次開始工作。

本節包括下列主題：

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。

在其他連接埠上手動啓動主代理程式

1. 編輯 */server_root*`/plugins/snmp/magt/CONFIG` 以指定所需的連接埠。
2. 依照下列步驟執行啓動程序檔：

   ```
   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。但是，使用者介面能夠偵測主代理程式是否正在執行。

手動配置 SNMP 主代理程式

手動配置 SNMP 主代理程式

1. 以超級使用者身份登入。
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，並瞭解其所支援的 MIB 樹。然後終止其程序。
3. 編輯 CONFIG 檔案，它位於伺服器根目錄下的 plugins/snmp/magt 中。
4. (可選) 在 CONFIG 檔案內定義變數 sysContact 與變數 sysLocation。

編輯主代理程式 CONFIG 檔案

手動配置 SNMP 主代理程式

1. 以超級使用者身份登入。
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，並瞭解其所支援的 MIB 樹。然後終止其程序。
3. 編輯 CONFIG 檔案，它位於伺服器根目錄下的 plugins/snmp/magt 中。
4. (可選) 在 CONFIG 檔案內定義變數 sysContact 與變數 sysLocation。

定義 sysContact 與 sysLocation 變數

您可以編輯 CONFIG 檔案來爲 sysContact 與 sysLocation 增加初始值，這些值用於指定變數 sysContact 與變數 sysLocation MIB-II。在本範例中，sysContact 與 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。

以下爲定義了變數 sysContract 與 sysLocation 的 CONFIG 檔案範例：

```
COMMUNITY          public
                   ALLOW ALL OPERATIONS

MANAGER            nms2
                   SEND ALL TRAPS TO PORT 162
                   WITH COMMUNITY public
```

```
INITIAL            sysLocation "Server room
987 East Cannon Road
Mountain 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 子代理程式以監視伺服器。

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。將顯示 [Configure SNMP Subagent] 頁面。
3. 在 [Master Host] 欄位中輸入伺服器的名稱與網域。
4. 在 [Description] 欄位中，輸入伺服器的描述，包含作業系統資訊。
5. 在 [Organization] 欄位中，輸入負責伺服器的組織。
6. 在 [Location] 欄位中輸入伺服器的絕對路徑。
7. 在 [Contact] 欄位中，輸入伺服器負責人的姓名以及此負責人的連絡資訊。
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]。將顯示 [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

一旦安裝了 SNMP 主代理程式，便可以手動啓動它，或透過使用 Administration Server 來啓動它。

手動啓動 SNMP 主代理程式

若要手動啓動主代理程式，請在指令提示下輸入下列內容：

```
# magt CONFIG INIT&
```

INIT 檔案是一個永久性檔案，它含有包括系統位置和連絡資訊的 MIB-II 系統群組資訊。如果 INIT 檔案不存在，則在首次啓動主代理程式的時候會建立此檔案。CONFIG 檔案中的無效管理程式名稱會導致主代理程式啓動失敗。

若要在非標準的連接埠上啓動主代理程式，請使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，在此對映上，主代理程式經由管理程式偵聽 SNMP 請求。傳輸對映允許主代理程式接受在標準連接埠與非標準連接埠處的連線。主代理程式也可以接受非標準連接埠的 SNMP 流量。目標系統對開啓的通訊端數目或每個程序中檔案描述元數目的限制會限定同步運作的 SNMP 的最大數目。以下爲傳輸對映項目的範例：

```
TRANSPORT          extraordinary   SNMP
                   OVER UDP SOCKET
                    AT PORT 11161
```

手動編輯 CONFIG 檔案之後，您應該在指令提示下鍵入以下內容來手動啓動主代理程式：

```
# magt CONFIG INIT&
```

方法二：編輯 /etc/services 檔案以允許主代理程式接受在標準連接埠與非標準連接埠處的連線。

使用 Administration Server 啓動 SNMP 主代理程式

使用 Administration Server 啓動 SNMP 主代理程式

1. 登入 Administration Server。
2. 在 Administration Server 中，從 [Global Settings] 標籤中選擇 [Control SNMP Master Agent] 頁面。
3. 按一下 [Start]。

您也可以從 [Control SNMP Master Agent] 頁面，停止與重新啓動 SNMP 主代理程式。

配置 SNMP 主代理程式

啓用了主代理程式並在主機電腦上啓用子代理程式之後，您需要配置主機的 Administration Server。此作業需要指定社群字串與陷阱目標。

配置社群字串

社群字串爲 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工作站是否被授予取得資訊的權限。當社團字串在 SNMP 封包中傳送時，不會隱藏；字串以 ASCII 文字的形式傳送。

您可以從 Administration Server 中的 [Set SNMP Master Agent Community] 頁面配置 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。在 Administration Server 中，您還可以檢視、編輯和移除已經配置的社群。

配置陷阱目標

SNMP 陷阱爲 SNMP 代理程式傳送至網路管理工作站的訊息。例如，當介面的狀態由工作中變更爲停用，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，以便傳送陷阱。您可以從 Proxy Server 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。使用 Proxy Server 配置陷阱目標實際上也就是在編輯 `CONFIG` 檔案。

啓用子代理程式

安裝了隨附 Administration Server 的主代理程式之後，如果要嘗試啓動此主代理程式，您必須首先啓用伺服器實例的子代理程式。如需有關安裝主代理程式的更多資訊，請參閱第 203 頁的「安裝 SNMP 主代理程式」。您可以使用 Server Manager 啓用子代理程式。

若要在 UNIX 或 Linux 平台上停用 SNMP 功能，必須首先停止子代理程式，然後停止主代理程式。如果首先停止了主代理程式，便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 [Configure SNMP Subagent] 頁面啓動子代理程式。如需更多資訊，請參閱線上說明中的相應小節。

啓用了代理程式之後，您可以從 [Control SNMP Subagent] 頁面或 Windows 的服務控制台啓動、停止或重新啓動此代理程式。

備註 變更任何 SNMP 配置之後，您必須按一下 [Apply Required] 按鈕，然後重新啓動 SNMP 子代理程式。

瞭解 SNMP 訊息

GET 與 SET 是由 SNMP 定義的兩種訊息類型。GET 與 SET 訊息由網路管理工作站 (NMS) 傳送至主代理程式。您可以經由 Administration Server 同時使用二者，或使用其中一個。

SNMP 以協定資料單元 (PDU) 的形式交換網路資訊。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，也稱爲受管理物件，具有值和標題，必要時，可以將這些值和標題報告給 NMS。由伺服器傳送到 NMS 的協定資料單元稱爲「陷阱」。下面舉例說明 GET、SET 以及「陷阱」訊息的用法。

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 將一則訊息傳送至 Administration Server 主代理程式。此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. 子代理程式將資料或狀態報告給主代理程式，然後，主代理程式將訊息轉寄回 (一則 GET 訊息) NMS。
5. NMS 經由其網路管理應用程式，用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傳送一則訊息或一個「陷阱」至 NMS。例如：

1. 子代理程式通知主代理程式伺服器已經停止。
2. 主代理程式會傳送一則訊息或一個「陷阱」，將事件報告給 NMS。
3. NMS 經由其網路管理應用程式，用文字或圖形顯示資訊。

第 4 部分

管理 Proxy Server

第 11 章

代理與路由 URL

本章描述代理伺服器如何處理請求，並解釋如何爲特定資源啓用代理，以及如何配置代理伺服器來將 URL 路由至不同的 URL 或伺服器。

本章包含下列小節：

爲資源啓用 / 停用代理

可以爲資源開啓或關閉代理。資源可以是個別的 URL、具有共通點的許多 URL 組成的群組，或是整個協定。您可以控制是否對整個伺服器、各種資源或範本檔案內指定之資源開啓代理設定。這意味著只要關閉資源的代理設定，即可拒絕對一或多個 URL 的存取。這可做爲拒絕或允許所有對某個資源之存取的全局方式。您也可以利用 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 280 頁的 「篩選 URL」。

爲資源啓用代理

1. 存取 Server Manager，然後按一下 [Routing] 標籤。
2. 按一下 [Enable/Disable Proxyin] 連結。將顯示 [Enable/Disable Proxying] 頁面。
3. 從下拉式清單中選取資源，或按一下 [Regular Expression] 按鈕，輸入常規表示式並按一下 [OK]。
4. 可以爲指定的資源選擇預設設定。可以選擇不代理此資源 (停用代理)，也可以爲此資源啓用代理。下列選項可供選用：

- **Use Default Setting Derived From A More General Resource。**將爲此資源使用更一般性資源的設定 (包括此設定)。
- **Do Not Proxy This Resource。**不能透過代理到達此資源。
- **Enable Proxying Of This Resource。**代理伺服器可讓用戶端存取此資源 (如果它們通過其他安全與授權檢查)。爲資源啓用代理時，**將啓用所有方法**。讀取方法 (包括 GET、HEAD、INDEX、POST 和用於 SSL 通道的 CONNECT) 和寫入方法 (包括 PUT、MKDIR、RMDIR、MOVE 和 DELETE) 會全部對此資源啓用。如果排除所有其他的安全檢查，所有的用戶端都具備讀寫存取權。

5. 按一下 [OK]。
6. 按一下 [Restart Required]。將顯示 [Apply Changes] 頁面。
7. 按一下 [Restart Proxy Server] 按鈕以套用變更。

經過另一個代理伺服器路由

[Set Routing Preferences] 頁面可用來配置代理伺服器，使其使用得出的預設配置或直接連線來路由某些資源；或是經過代理伺服器陣列、ICP 鄰近區域、另一個代理伺服器或 SOCKS 伺服器進行路由。

爲資源配置路由

爲資源配置路由

1. 存取 Server Manager，然後按一下 [Routing] 標籤。
2. 按一下 [Set Routing Preferences] 連結。將出現 [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，輸入常規表示式並按一下 [OK]。
4. 選取與希望所配置資源使用之路由類型對應的單選按鈕。可選取以下一個選項。

- **Derived Default Configuration。**代理伺服器使用更一般性的範本 (也就是內含更簡短之相符常規表示式的範本) 來確定它應使用遠端伺服器還是另一個代理伺服器。例如，如果代理伺服器將所有 `http://.*` 請求路由到另一個代理伺服器，將所有 `http://www.*` 請求路由到遠端伺服器，則您可爲 `http://www.example.*` 請求建立一個得出的預設配置路由，然後這些請求會按照 `http://www.*` 範本中的設定直接送達遠端伺服器。
- **Direct Connections。**請求將一律直接送達遠端伺服器，而不經過代理伺服器。
- **Route Through A SOCKS Server。**指定資源的請求將經過一個 SOCKS 伺服器傳送。如果您選取此選項，就必須指定代理伺服器路由請求時將經過的 SOCKS 伺服器的名稱 (或 IP 位址) 和連接埠號碼。
- **Route Through。**讓您指定是否要經過代理伺服器陣列、ICP 鄰近區域、父陣列和 / 或代理伺服器進行路由。如果在此選取多個路由方法，代理伺服器將會遵循表單上所示的階層 (即，代理伺服器陣列、重新導向、ICP、父陣列、另一個代理伺服器)。如需有關經過代理伺服器路由的更多資訊，請參閱第 216 頁的「鏈接代理伺服器」。

  如需有關經過 SOCKS 伺服器路由的資訊，請參閱第 217 頁的「經過 SOCKS 伺服器路由」。如需有關經過代理伺服器陣列、父陣列或 ICP 鄰近區域路由的資訊，請參閱第 231 頁的第 12 章 「快取」。

備註 若要在非預設埠上 (443 以外的連接埠) 啓用連線請求的路由，需要將 `obj.conf` 檔案中的 `ppath` 參數變更爲 `connect://.*`。

5. 按一下 [OK]。
6. 按一下 [Restart Required]。將顯示 [Apply Changes] 頁面。
7. 按一下 [Restart Proxy Server] 按鈕以套用變更。

鏈接代理伺服器

您可以讓代理伺服器存取另一個代理伺服器來取得某些資源，而不是存取遠端伺服器。也就是說，您可以將代理伺服器鏈接在一起。鏈接是在防火牆後組織若干代理伺服器的好方法。利用鏈接也可以建立階層式的快取。

經過另一個代理伺服器路由

1. 存取 Server Manager，然後按一下 [Routing] 標籤。
2. 按一下 [Set Routing Preferences] 連結。將出現 [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，輸入常規表示式並按一下 [OK]。
4. 在頁面的 [Routing Through Another Proxy] 區段中選擇 [Route Through] 選項。
5. 選擇 [Another Proxy] 核取方塊。
6. 在 [Another Proxy] 欄位中，輸入路由時要經過的代理伺服器的名稱或 IP 位址。
7. 按一下 [OK]。
8. 按一下 [Restart Required]。將顯示 [Apply Changes] 頁面。
9. 按一下 [Restart Proxy Server] 按鈕以套用變更。

經過 SOCKS 伺服器路由

如果網路上已有遠端 SOCKS 伺服器在執行，可以將代理伺服器配置爲連線此遠端伺服器來取得特定資源。

經過 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。將出現 [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，輸入常規表示式並按一下 [OK]。
4. 在頁面的 [Routing Through Another Proxy] 區段中選擇 [Route Through] 選項。
5. 選擇 [Route Through SOCKS Server] 選項。
6. 指定代理伺服器路由請求時將經過的 SOCKS 伺服器的名稱 (或 IP 位址) 和連接埠號碼。
7. 按一下 [OK]。

備註	啓用經過 SOCKS 伺服器路由後，應使用 [SOCKS v5 Routing] 頁面來建立代理伺服器路由。代理伺服器路由決定著能夠透過代理伺服器路由所經過之 SOCKS 伺服器來存取的 IP 位址。它們也指定 SOCKS 伺服器是否直接連線至主機。

8. 按一下 [Restart Required]。將顯示 [Apply Changes] 頁面。
9. 按一下 [Restart Proxy Server] 按鈕以套用變更。

將用戶端 IP 位址轉寄給伺服器

[Forward Client Credentials] 頁面可用來配置代理伺服器，使其傳送用戶端憑證至遠端伺服器。

透過配置讓代理伺服器傳送用戶端 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。將顯示 [Forward Client Credentials] 頁面。
3. 從下拉式清單中選取資源，或按一下 [Regular Expression] 按鈕，輸入常規表示式並按一下 [OK]。

4. 依需要變更下列選項：

   - **Client IP Addressing Forwarding。**Proxy Server 在發出文件請求時不將用戶端的 IP 位址傳送至遠端伺服器，而是做爲用戶端，將自己的其 IP 位址傳送給遠端伺服器。不過在下列情況下，您可能也想要傳送用戶端的 IP 位址：

     - 當代理伺服器是內部代理伺服器鏈的一份子時。
     - 當伺服器必須知道用戶端的 IP 位址才允許用戶端存取時。您可以使用範本將用戶端的 IP 位址僅傳送給特定伺服器。

     選取下列一個選項來配置代理伺服器，使其傳送用戶端 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。**您可指定代理伺服器轉寄 IP 位址時所使用的 HTTP 標頭。預設的 HTTP 標頭稱爲 `Client-ip`，但您可使用您選擇的任何標頭來傳送 IP 位址。

   - **Client Proxy Authentication Forwarding。**選取下列一個選項來配置代理伺服器，使其傳送用戶端的詳細認證資訊：

     - **Default。**允許 Proxy Server 轉寄用戶端的詳細認證資訊。
     - **Blocked。**不允許代理伺服器轉寄用戶端的詳細認證資訊。
     - **Enabled Using HTTP Header。**您可指定代理伺服器轉寄詳細認證資訊時所使用的 HTTP 標頭。

   - **Client Cipher Forwarding**。選取下列一個選項來配置代理伺服器，使其傳送用戶端的 SSL/TLS 密碼組名稱至遠端伺服器：

     - **Default。**允許 Proxy Server 轉寄用戶端的 SSL/TLS 密碼組名稱至遠端伺服器。
     - **Blocked。**不允許代理伺服器轉寄用戶端的 SSL/TLS 密碼組名稱至遠端伺服器。
     - **Enabled Using HTTP Header。**您可指定代理伺服器轉寄用戶端的 SSL/TLS 密碼組名稱至遠端伺服器時使用的 HTTP 標頭。預設的 HTTP 標頭稱爲 `Proxy-cipher`，但您可使用您選擇的任何標頭來傳送用戶端的 SSL/TLS 密碼組名稱。

   - **Client Keysize Forwarding。**選取下列一個選項來配置代理伺服器，使其傳送用戶端的 SSL/TLS 密鑰大小至遠端伺服器：

     - **Default。**允許 Proxy Server 轉寄用戶端的 SSL/TLS 密鑰大小至遠端伺服器。

- **Blocked。**不允許代理伺服器轉寄用戶端的 SSL/TLS 密鑰大小至遠端伺服器。
- **Enabled Using HTTP Header。**您可指定代理伺服器轉寄用戶端的 SSL/TLS 密鑰大小至遠端伺服器時使用的 HTTP 標頭。預設的 HTTP 標頭稱爲 `Proxy-keysize`，但您可使用您選擇的任何標頭來傳送用戶端的 SSL/TLS 密鑰大小。

❍ **Client Secret Keysize Forwarding。**選取下列一個選項來配置代理伺服器，使其傳送用戶端的 SSL/TLS 密鑰大小至遠端伺服器：

- **Default。**允許 Proxy Server 轉寄用戶端的 SSL/TLS 密鑰大小至遠端伺服器。
- **Blocked。**不允許代理伺服器轉寄用戶端的 SSL/TLS 密鑰大小至遠端伺服器。
- **Enabled Using HTTP Header。**您可指定代理伺服器轉寄用戶端的 SSL/TLS 密鑰大小至遠端伺服器時使用的 HTTP 標頭。預設的 HTTP 標頭稱爲 `Proxy-secret-keysize`，但您可使用您選擇的任何標頭來傳送用戶端的 SSL/TLS 密鑰大小。

❍ **Client SSL Session ID Forwarding。**選取下列一個選項來配置代理伺服器，使其傳送用戶端的 SSL/TLS 階段作業 ID 至遠端伺服器：

- **Default。**允許 Proxy Server 轉寄用戶端的 SSL/TLS 階段作業 ID 至遠端伺服器。
- **Blocked。**不允許代理伺服器轉寄用戶端的 SSL/TLS 階段作業 ID 至遠端伺服器。
- **Enabled Using HTTP Header。**您可指定代理伺服器轉寄用戶端的 SSL/TLS 階段作業 ID 至遠端伺服器時使用的 HTTP 標頭。預設的 HTTP 標頭稱爲 `Proxy-ssl-id`，但您可使用您選擇的任何標頭來傳送用戶端的 SSL/TLS 階段作業 ID。

❍ **Client Issuer DN Forwarding。**選取下列一個選項來配置代理伺服器，使其傳送用戶端的 SSL/TLS 憑證核發者之辨別名稱至遠端伺服器：

- **Default。**允許 Proxy Server 轉寄用戶端的 SSL/TLS 憑證核發者之辨別名稱至遠端伺服器。
- **Blocked。**不允許代理伺服器轉寄用戶端的 SSL/TLS 憑證核發者之辨別名稱至遠端伺服器。
- **Enabled Using HTTP Header。**您可指定代理伺服器轉寄用戶端的 SSL/TLS 憑證核發者之辨別名稱至遠端伺服器時使用的 HTTP 標頭。預設的 HTTP 標頭稱爲 `Proxy-issuer-dn`，但您可使用您選擇的任何標頭來傳送用戶端的 SSL/TLS 憑證核發者之名稱。

- **Client User DN Forwarding。**選取下列一個選項來配置代理伺服器，使其傳送用戶端的 SSL/TLS 憑證主體之辨別名稱至遠端伺服器：
  - **Default。**允許 Proxy Server 轉寄用戶端的 SSL/TLS 憑證主體之辨別名稱至遠端伺服器。
  - **Blocked。**不允許代理伺服器轉寄用戶端的 SSL/TLS 憑證主體之辨別名稱至遠端伺服器。
  - **Enabled Using HTTP Header。**您可指定代理伺服器轉寄用戶端的 SSL/TLS 憑證主體之辨別名稱至遠端伺服器時使用的 HTTP 標頭。預設的 HTTP 標頭稱爲 `Proxy-user-dn`，但您可使用您選擇的任何標頭來傳送用戶端的 SSL/TLS 憑證主體之名稱。
- **Client SSL/TLS Certificate Forwarding。**選取下列一個選項來配置代理伺服器，使其傳送用戶端的 SSL/TLS 憑證至遠端伺服器：
  - **Default。**允許 Proxy Server 轉寄用戶端的 SSL/TLS 憑證至遠端伺服器。
  - **Blocked。**不允許代理伺服器轉寄用戶端的 SSL/TLS 憑證至遠端伺服器。
  - **Enabled Using HTTP Header。**您可指定代理伺服器轉寄用戶端的 SSL/TLS 憑證至遠端伺服器時使用的 HTTP 標頭。預設的 HTTP 標頭稱爲 `Proxy-auth-cert`，但您可使用您選擇的任何標頭來傳送用戶端的 SSL/TLS 憑證。
- **Client Cache Information Forwarding。**選取下列一個選項來配置代理伺服器，使其傳送有關本機快取符合項目的資訊至遠端伺服器：
  - **Default。**允許 Proxy Server 轉寄有關本機快取符合項目的資訊至遠端伺服器。
  - **Blocked。**不允許代理伺服器轉寄有關本機快取符合項目的資訊至遠端伺服器。
  - **Enabled Using HTTP Header。**您可指定 HTTP 標頭，代理伺服器在轉寄有關本機快取符合項目的資訊至遠端伺服器時會用到它。預設的 HTTP 標頭稱爲 `Cache-info`，但您可使用您選擇的任何標頭來傳送有關本機快取符合項目的資訊。
- **Set Basic Authentication Credentials。**選取下列一個選項來配置代理伺服器，使其傳送 HTTP 請求：
  - **User。**指定要認證的使用者。
  - **Password。**指定使用者密碼。
  - **Using HTTP Header。**您可指定代理伺服器傳遞憑證時所使用的 HTTP 標頭。

5. 按一下 [OK]。
6. 按一下 [Restart Required]。將顯示 [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，用戶端可能具備限定存取的功能，僅允許對某些 IP 位址進行存取。爲使用戶端可以使用此功能，代理伺服器應支援對 Java IP 位址進行檢查。此支援允許用戶端查詢代理伺服器，以找出用來擷取資源的 IP 位址。當此功能啓用時，用戶端可請求代理伺服器傳送原始伺服器的 IP 位址，代理伺服器將 IP 位址附加在標頭中。一旦用戶端知道原始伺服器的 IP 位址後，它可明確地指定對以後的連線使用此 IP 位址。

檢查 Java IP 位址

1. 存取 Server Manager，然後按一下 [Routing] 標籤。
2. 按一下 [Check Java IP Address] 連結。將顯示 [Check Java IP Address] 頁面。
3. 從下拉式清單中選取資源，或按一下 [Regular Expression] 按鈕，輸入常規表示式並按一下 [OK]。
4. 選取單選按鈕來啓用、停用 Java IP 位址檢查或使用其預設配置。

備註	預設選項使用從更一般性的範本 (也就是內含更簡短之相符常規表示式的範本) 所得出的預設配置來確定應啓用還是停用 Java IP 位址檢查。

5. 按一下 [OK]。
6. 按一下 [Restart Required]。將顯示 [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

如果代理伺服器支援多個用戶端，您可以使用用戶端自動配置檔來配置所有的瀏覽器用戶端。自動配置檔包含一個 JavaScript 函數，能決定 Navigator 存取不同的 URL 時所要使用的代理伺服器 (如果有的話)。如需有關此功能的更多資訊，請參閱第 325 頁的第 17 章 「使用用戶端自動配置檔案」。

設定網路連結模式

您可以從網路上連線或結束連線代理伺服器。利用此功能，可便捷地將代理伺服器安裝在可攜式電腦上，可用它來作簡報示範。

當代理伺服器從網路結束連線時，文件會直接從快取記憶體傳回。代理伺服器不能進行最新狀態檢查，因此文件會很快地被擷取 (文件可能不是最新的；如需有關快取的更多資訊，請參閱第 231 頁的第 12 章 「快取」)。

此外，如果您沒有跟網路連線，連線永遠不會掛斷，因爲代理伺服器知道沒有網路，就永遠不會嘗試連線遠端伺服器。當網路中斷但代理伺服器電腦仍在執行時，您可使用此無網路設定。

備註 請注意，執行從網路結束連線的代理伺服器意味著您終究將從快取記憶體存取舊的資料。另外，不透過網路執行就不需要代理伺服器安全功能。

Proxy Server 提供了四種網路連結模式：

- 預設模式源自最一般性的相符物件之配置。
- 一般模式是代理伺服器的一般作業模式。代理伺服器會從內容伺服器擷取快取記憶體中還沒有的文件。如果文件已存在於快取記憶體中，則會將這些文件與內容伺服器中的文件加以比對，確定這些文件是否爲最新。如果某個快取檔案已變更，則會被替代成目前的副本。
- Fast-demo 模式用於在網路可用時提供流暢的簡報示範。如果在快取記憶體中找到文件，則不會與內容伺服器連線，甚至不會去查證文件是否經過變更。此模式擺脫了因等候內容伺服器回應而造成的延遲。如果文件不在快取記憶體中，則會從內容伺服器中擷取並快取此文件。fast-demo 模式較一般模式更不易造成延遲，但有時可能會傳回舊的資料，因爲它在找到文件後不會對文件執行更新檢查。
- 無網路模式專門用於沒有網路連線的可攜式電腦。代理伺服器會傳回快取記憶體中的文件，如果快取記憶體中沒有文件，則會傳回錯誤。代理伺服器永遠不會嘗試與內容伺服器連線，這樣可避免代理伺服器在嘗試取得根本不存在的連線時掛斷和逾時。

變更代理伺服器的執行模式

1. 存取 Server Manager，然後按一下 [Routing] 標籤。
2. 按一下 [Set Connectivity Mode] 連結。將顯示 [Set Connectivity Mode] 頁面。
3. 從下拉式清單中選取資源，或按一下 [Regular Expression] 按鈕，輸入常規表示式並按一下 [OK]。
4. 選取您想要的模式。
5. 按一下 [OK]。
6. 按一下 [Restart Required]。將顯示 [Apply Changes] 頁面。
7. 按一下 [Restart Proxy Server] 按鈕以套用變更。

變更預設 FTP 傳輸模式

FTP 有兩種不同的方式來建立 FTP 伺服器和用戶端 (代理伺服器相當於用戶端) 之間的資料連線。這兩種模式分別稱爲 PASV 和 PORT 模式 FTP。

- **被動模式 (PASV)。**從代理伺服器啓動資料連線，然後 FTP 伺服器接受連線。這對於執行 Proxy Server 的站點而言比較安全，因爲它不需接受傳入的連線。
- **主動模式 (PORT)。**由遠端 FTP 伺服器啓動資料連線，然後代理伺服器接受內送的連線。如果代理伺服器位於防火牆內，防火牆會阻斷從 FTP 伺服器內送的 FTP 資料連線，這意味著 PORT 模式無法發揮作用。

某些 FTP 站點會執行防火牆，使代理伺服器的 PASV 模式無法發揮作用。因此，您可將代理伺服器配置爲使用 PORT 模式 FTP。您可開啓整個伺服器的 PORT 模式，或是只開啓特定 FTP 伺服器的 PORT 模式。

備註	如果遠端 FTP 伺服器不支援 PASV 模式，則即使開啓 PASV 模式，代理伺服器仍將使用 PORT 模式。

如果代理伺服器位於防火牆之後，使 PORT 模式 FTP 無法發揮作用，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更一般性資源的模式。如果沒有指定，則將使用 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。將顯示 [Set FTP Mode] 頁面。
3. 從下拉式清單中選取資源，或按一下 [Regular Expression] 按鈕，輸入常規表示式並按一下 [OK]。
4. 選擇 FTP 傳輸模式。
5. 按一下 [OK]。
6. 按一下 [Restart Required]。將顯示 [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

如果將代理伺服器配置爲讓傳出的連線經過 SOCKS 伺服器傳出，則您必須明確地指定用於 SOCKS 之名稱伺服器的 IP 位址。

如果您要用某個 DNS 伺服器而不是防火牆內的內部 DNS 服務來解析外部主機名稱，則應指定名稱伺服器 IP 位址。

指定 SOCKS 名稱伺服器 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。將顯示 [Set SOCKS Name Server] 頁面。
3. 在文字欄位中輸入 DNS 名稱伺服器的 IP 位址。
4. 按一下 [OK]。

備註 過去，這一允許指定 SOCKS 名稱伺服器 IP 位址的功能只能透過 SOCKS_NS 環境變數存取。如果您設定環境變數並使用 [SOCKS Name Server Setting] 表單來指定名稱伺服器 IP 位址，則代理伺服器將會使用表單上指定的 IP 位址，而不會使用環境變數。

5. 按一下 [Restart Required]。將顯示 [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] 頁面可用來在指定的原始伺服器之間分配負載。

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。將顯示 [Configure HTTP Request Load Balancing] 頁面。
3. 從下拉式清單中選取資源，或按一下 [Regular Expression] 按鈕，輸入常規表示式並按一下 [OK]。
4. 在 [Server] 欄位中指定原始伺服器的 URL。如果給定多個伺服器參數，Proxy Server 將在指定的原始伺服器之間分配負載。
5. 在 [Sticky Cookie] 欄位中指定 cookie 的名稱，它若出現在回應中，會使後續的請求居留在原始伺服器中。預設值爲 `JSESSIONID`。
6. 在 [Sticky Parameter] 欄位中指定 URI 參數的名稱以檢查路由資訊。當 URI 參數出現在請求 URI 中，且其值包含一個冒號，其後跟隨一個路由 ID，則請求將居留於以此路由 ID 標識的原始伺服器。預設值爲 `jsessionid`。
7. 在 [Route Header] 欄位中指定 HTTP 請求標頭的名稱，此標頭可用來將路由 ID 傳遞至原始伺服器。預設值爲 `proxy-jroute`。
8. 在 [Route Cookie] 欄位中指定 Proxy Server 在回應中發現居留式 cookie 時產生的 cookie 的名稱。預設值爲 `JROUTE`。
9. 按一下對應的 [Rewrite Host] 選項以指示是否重寫 Host HTTP 請求標頭，使其與伺服器參數所指定的主機相符合。
10. 按一下對應的 [Rewrite Location] 選項以指示是否應重寫與伺服器參數相符的 Location HTTP 回應標頭。
11. 按一下對應的 [Rewrite Content] 選項以指示是否應重寫與伺服器參數相符的 Content-Location HTTP 回應標頭。
12. 選取核取方塊以指示是否應重寫與伺服器參數相符的 *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]。將顯示 [Apply Changes] 頁面。
15. 按一下 [Restart Proxy Server] 按鈕以套用變更。

管理 URL 與 URL 對映

Server Manager 允許將 URL 對映至其他伺服器，有時稱作鏡像服器。當用戶端以鏡像 URL 存取代理伺服器時，代理伺服器會從鏡像伺服器 (而不是從 URL 中指定的伺服器) 中擷取所請求的文件。用戶端決不會察覺請求正傳送至不同的伺服器。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 傳回用戶端 (而不是文件)，所以用戶端之後可以請求新的文件。對映功能也允許將 URL 對映至檔案，像是 PAC 與 PAT 對映一樣。

本節包含以下主題：

建立 URL 對映

若要對映 URL，您要指定 URL 前綴與要對映的位置。以下小節描述了不同類型的 URL 對映。您可以建立四種類型的 URL 對映：

- 標準對映將 URL 前綴對映至另一個 URL 前綴。例如，可相應配置代理伺服器，使其一接到以 `http://www.example.com` 開始的請求即移至特定的 URL。
- 反向對映將重新導向的 URL 前綴對映至另一個 URL 前綴。當內部伺服器將重新導向的回應而非文件傳送至代理伺服器時，反向代理伺服器會使用這些對映。如需更多資訊，請參閱第 289 頁的第 14 章 「使用反向代理伺服器」。
- 常規表示式將所有符合表示式的 URL 對映至單個 URL。例如，您可以將所有符合 .*job.* 的 URL 對映至特定的 URL (這或許能解釋代理伺服器爲何不讓使用者前往特定 URL）。
- 用戶端自動配置將 URL 對映至儲存在代理伺服器上之特定 `.pac` 檔案。如需有關自動配置檔的更多資訊，請參閱第 325 頁的第 17 章 「使用用戶端自動配置檔案」。
- 代理伺服器陣列表 (PAT) 將 URL 對映至儲存在代理伺服器上之特定 `.pat` 檔案。只能從主代理伺服器建立此類型的對映。如需有關 PAT 檔案與代理伺服器陣列的更多資訊，請參閱第 266 頁的 「透過代理伺服器陣列進行路由」。

正存取某個 URL 的用戶端會被傳送至同一伺服器或不同伺服器上的不同位置。當資源已經移動或當您需要維護相對連結的完整性 (在無尾隨斜線的情況下存取目錄時)，這是很有用的。

例如，假設您的 Web 伺服器 (hi.load.com) 負荷量很重，您想要鏡像至稱爲 mirror.load.com 的另一個伺服器。您可以配置代理伺服器來對進入 hi.load.com 電腦的 URL 使用 mirror.load.com 電腦。

來源 URL 前綴必須是未退出的，但需位於目標 (鏡像) URL 中，只有在 HTTP 請求中不合法的字元才需要退出。

注意 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 [URLs] 標籤。
2. 按一下 [Create Mapping] 連結。將顯示 [Create Mapping] 頁面。
3. 選取要建立的對映類型。
   - **Regular Mappings**。將 URL 前綴對映至另一個 URL 前綴。例如，可相應配置代理伺服器，使其一接到以 `http://www.example.com` 開始的請求即移至特定的 URL。如果您選取此選項，頁面下方會顯示下列選項：
     - **Rewrite Host**。按一下對應的選項以指示是否重寫 Host HTTP 標頭，使其與 `to` 參數所指定的主機相符合。
   - **Reverse Mappings**。將重新導向的 URL 前綴對映至另一個 URL 前綴。當內部伺服器將重新導向的回應而非文件傳送至代理伺服器時，反向代理伺服器會使用這些對映。如需有關反向代理伺服器的更多資訊，請參閱第 289 頁的第 14 章 「使用反向代理伺服器」。如果您選取此選項，頁面下方會顯示下列選項：
     - **Rewrite Location**。按一下對應的選項以指示是否應重寫 Location HTTP 回應標頭。
     - **Rewrite Content Location**。按一下對應的選項以指示是否應重寫 Content-location HTTP 回應標頭。
     - **Rewrite Headername**。選取核取方塊以指示是否應重寫 *headername* HTTP 回應標頭，其中 *headername* 是使用者定義的標頭名稱。
   - **Regular Expressions**。將所有與表示式相符的 URL 對映至單個 URL。如需有關常規表示式的更多資訊，請參閱第 319 頁的第 16 章 「管理範本和資源」。
   - **Client Autoconfiguration**。將 URL 對映至儲存於 Proxy Server 上的特定 .pac 檔案。如需有關自動配置檔的更多資訊，請參閱第 325 頁的第 17 章 「使用用戶端自動配置檔案」。

- **Proxy Array Table (PAT)**。將 URL 對映至儲存於 Proxy Server 上的特定 .pat 檔案。只能從主代理伺服器建立此類型的對映。如需有關 PAT 檔案與代理伺服器陣列的更多資訊，請參閱第 231 頁的第 12 章 「快取」中的「透過代理伺服器陣列進行路由」

4. 鍵入對映來源前綴。對於標準對映和反向對映而言，這應是您要替代的 URL 中的一部分。

   對於常規表示式對映，URL 前綴應爲您希望所有 URL 均與其相符的常規表示式。如果您也爲對映選擇了範本，則常規表示式只適用於範本的常規表示式內的 URL。

   對於用戶端自動配置對映和代理伺服器陣列表對映，URL 前綴應爲用戶端存取的完整 URL。

5. 鍵入對映目標。

   對於除用戶端自動配置和代理伺服器陣列表以外的所有對映類型而言，它應是要向其對映的完整 URL。對於用戶端自動配置對映而言，此值應爲 .pac 檔案在代理伺服器硬碟上的絕對路徑。對於代理伺服器陣列表對映而言，此值應爲 .pat 檔案在主代理伺服器之本機磁碟上的絕對路徑。

6. 從下拉式清單中選取範本名稱，如果您不想套用範本，則保持 [NONE] 值不變。
7. 按一下 [OK] 建立對映。
8. 按一下 [Restart Required]。將顯示 [Apply Changes] 頁面。
9. 按一下 [Restart Proxy Server] 按鈕以套用變更。

檢視、編輯或移除現有 URL 對映

變更現有的對映

1. 存取 Server Manager，然後按一下 [URLs] 標籤。
2. 按一下 [View/Edit Mappings] 連結。將顯示 [View/Edit Mappings] 頁面。
3. 若要編輯對映，請按一下對映旁邊的 [Edit] 連結。您可以編輯對映所影響的前綴、對映的 URL 以及範本。按一下 [OK] 以確認變更。
4. 若要移除對映，請按一下您要編輯的對映，然後按一下對映旁邊的 [Remove] 連結。
5. 按一下 [Restart Required]。將顯示 [Apply Changes] 頁面。
6. 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，使其將重新導向的 URL 傳回用戶端，而並不取得並傳回文件。藉由重新導向功能，用戶端可得知原先請求的 URL 已被重新導向至不同的 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，使用者不需再度明確地請求文件。

URL 重新導向在您想要拒絕使用者對某區域的存取時是很有用的，因爲您可將使用者重新導向至說明存取遭拒之原因的 URL。

重新導向一個或多個 URL

1. 存取 Server Manager，然後按一下 [URLs] 標籤。
2. 按一下 [Redirect URLs] 連結。將顯示 [Redirect URLs] 頁面。
3. 輸入做爲 URL 前綴的來源 URL。
4. 輸入重新導向到的 URL。此 URL 可以爲 URL 前綴或固定的 URL。

   如果您選擇使用 URL 前綴做爲要重新導向的目標 URL，請選取 [URL prefix] 欄位旁的單選按鈕，然後輸入 URL 前綴。如果您選擇使用固定的 URL，請選取 [Fixed URL] 欄位旁的單選按鈕，然後輸入固定的 URL。
5. 按一下 [OK]。
6. 按一下 [Restart Required]。將顯示 [Apply Changes] 頁面。
7. 按一下 [Restart Proxy Server] 按鈕以套用變更。

第 12 章

快取

本章描述 Sun Java™ System Web Proxy Server 如何快取文件，同時描述如何使用線上頁面來配置快取。

本章包含下列小節：

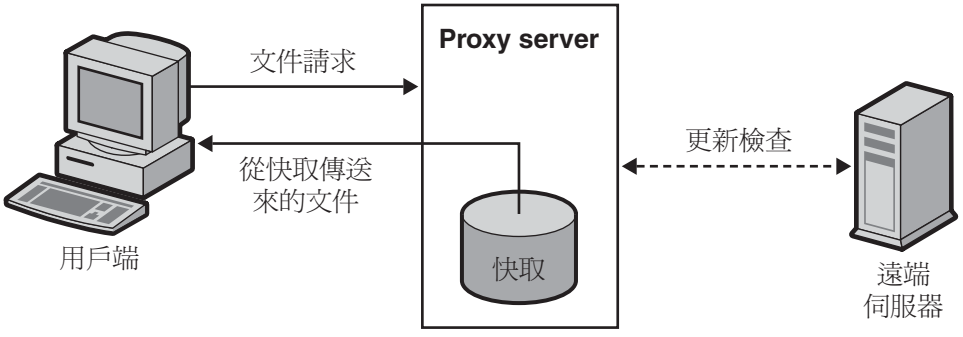
快取如何作業

快取能減少網路流量，並且爲使用代理伺服器而不是直接存取遠端伺服器的用戶端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（請參閱圖 12-1）。如果代理伺服器確定檔案並非最新，則會從遠端伺服器更新此文件，並在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



快取中的檔案將自動由 Sun Java™ System Web Proxy Server 資源回收公用程式 (CacheGC) 來維護。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。概念上而言，分割區是磁碟上留作快取用途的儲存區域。如果希望讓快取跨越幾個磁碟，必須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，其他分割區則不受影響。

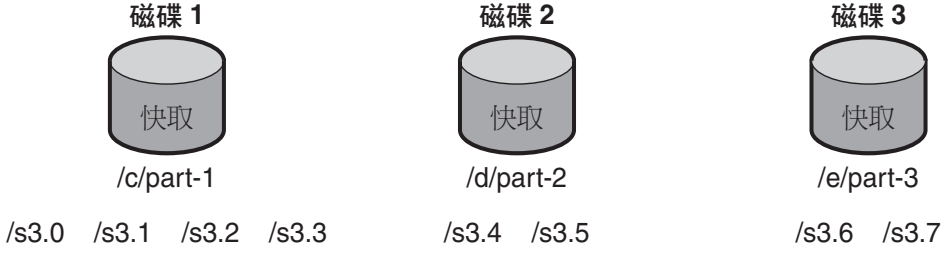
在單一位置儲存大量快取檔案會減低效能，所以在每個分割區中建立幾個目錄或區段是不錯的方法。在快取結構中，區段是分割區之下的一級。在跨所有分割區的快取中，最多可有 256 個區段。快取區段的數量必須是 2 的乘冪 (例如，1、2、4、8、16、...256)。

快取階層結構中的最低一級是子區段。子區段是區段中的目錄。每個區段有 64 個子區段。快取檔案儲存在快取中最低一級的子區段中。

圖 12-2 顯示了具有分割區與區段的範例快取結構。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，後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，其後爲區段編號。對於顯示爲 s3.4 的區段，3 表示代表快取區段數目的 2 的乘冪 ($2^3 = 8$)，而 4 表示此區段的編號 (對於標示爲 0 到 7 的 8 個區段)。因此，s3.4 表示 8 個區段的第 5 個。

圖 12-2 快取結構的範例



分散快取中的檔案

Proxy Server 使用特定的演算法來確定應將文件儲存到的目錄。此演算法能確保文件平均分散在各目錄中。平均分散的重要性在於，包含大量文件的目錄容易造成效能問題。

Proxy Server 使用 RSA MD5 演算法 (訊息摘要 5) 將 URL 簡化爲 16 個位元組的二進制資料，並使用此資料的 8 個位元組來計算 16 個字元的十六進制檔案名稱，將文件儲存在快取中時將使用此名稱。

設定快取細節

可藉由設定快取細節來啓用快取並控制 Proxy Server 將快取的協定類型。快取細節包括下列項目：

- 是啓用還是停用了快取
- 快取儲存其暫存檔案的工作目錄
- 將記錄快取 URL 的目錄的名稱
- 快取的大小
- 快取的容量
- 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將其回報給遠端伺服器

設定快取細節

1. 存取 Server Manager，然後按一下 [Caching] 標籤。
2. 按一下 [Set Cache Specifics] 連結。將顯示 [Set Cache Specifics] 頁面。
3. 可選取相應選項來啓用或停用快取。依預設，快取爲啓用狀態。如需更多資訊，請參閱第 236 頁的「啓用快取」。
4. 輸入工作目錄。依預設，工作目錄位於代理伺服器實例下。如果希望快取目錄位於其他位置，可進行變更。如需更多資訊，請參閱第 236 頁的「建立快取工作目錄」。

5. 按一下 [Partition Configuration] 連結。將顯示 [Add/Edit Cache Partitions] 頁面。可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大小上限。最大快取大小爲 32GB。如需更多資訊，請參閱第 236 頁的「設定快取大小」。

6. 按一下 [Cache Capacity Configuration] 連結。將顯示 [Set Cache Capacity] 頁面。可在 [Set Cache Capacity] 頁面中設定快取容量。如需更多資訊，請參閱第 236 頁的「編輯快取容量」。

7. 選取 [Cache HTTP] 核取方塊以啓用 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更新檢查，還是讓它每隔一段時間進行檢查。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 237 頁的「快取 HTTP 文件」。選項如下：

   - 選取 [Always Check That The Document Is Up To Date] 選項來確保 HTTP 文件一直爲最新。
   - 從 [Check Only If Last Check More Than] 下拉式清單中選取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決定更新檢查的執行方式：
     - **Use Last-modified Factor**。這是原始伺服器連同文件一起傳送的最後一次修改的標頭。
     - **Use Only Explicit Expiration Information**。代理伺服器使用 Expires 標頭確定快取項目爲最新還是已過期。
   - 選取 [Never Report Accesses To Remote Server] 選項來防止代理伺服器向遠端伺服器報告存取的次數。
   - 選取 [Report Cache Hits To Remote Server] 選項來追蹤文件的存取次數並將其回報給遠端伺服器。

8. 可設定快取 FTP 文件的重新整理間隔。選取 [Yes; Reload If Older Than] 核取方塊，同時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 239 頁的「快取 FTP 與 Gopher 文件」。

9. 可設定快取 Gopher 文件的重新整理間隔。選取 [Yes; Reload If Older Than] 核取方塊，同時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 239 頁的「快取 FTP 與 Gopher 文件」。

10. 按一下 [OK]。

11. 按一下 [Restart required]。將顯示 [Apply Changes] 頁面。

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

下列各節提供關於 [Set Cache Specifics] 頁面上所列元素的更多資訊，並將協助您確定最符合您需要的設定。

啓用快取

快取是一種可爲代理伺服器使用者降低網路流量的有效方式。快取無需從遠端伺服器擷取文件，進而還可縮短給用戶端的回應時間。每當啓用快取時，代理伺服器就可發揮最佳效用。

建立快取工作目錄

快取檔案位於快取分割區中。在 [Set Cache Specifics] 頁面中指定的工作目錄通常是快取的父系目錄。所有快取檔案會出現在快取目錄底下的有組織目錄結構中。如果變更快取目錄名稱或將其移到其他位置，則必須向代理伺服器告知新位置。

可將快取目錄結構延伸至多個檔案系統，如此可將一個大型快取結構分成好幾個小型磁碟，而不用將其全部存放在一個大型磁碟中。每個代理伺服器都必須有自己的快取目錄結構，也就是說，多個代理伺服器不能同時共用快取目錄。

設定快取大小

快取大小指示分割區大小。快取大小應一律小於快取容量，因爲快取容量是快取可擴充到的大小上限。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的影響甚鉅。如果快取太小，Cache GC 必須更頻繁地移除快取文件以挪出更多的磁碟空間，同時也必須更頻繁地從內容伺服器擷取文件，從而會使效能降低。

最好能設定較大的快取大小，因爲快取的文件越多，網路流量的負載就會越小，代理伺服器的回應時間也就越短。此外，GC 也會移除使用者已經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。

也可以將快取分割成多個磁碟分割區。

注意 變更快取結構會很耗時。

編輯快取容量

可從 [Set Cache Specifics] 頁面以及 [Set Cache Capacity] 頁面編輯快取容量。如需有關編輯快取容量的更多資訊，請參閱第 240 頁的 「設定快取容量」。

快取 HTTP 文件

就本質而言，快取 HTTP 文件與快取 FTP 和 Gopher 文件不同。HTTP 文件能提供其他協定的文件無法提供的快取功能。但是，藉由適當設定與配置快取，可確保 Proxy Server 能有效快取 HTTP、FTP 與 Gopher 文件。

所有 HTTP 文件都有描述性的標頭區段，Proxy Server 使用它來比較與計算代理伺服器快取中的文件與遠端伺服器上的文件。代理伺服器對 HTTP 文件進行更新檢查時，會傳送一個請求到伺服器，告知伺服器若發現快取中的版本過期則傳回文件。從上次請求至今此文件通常還未變更，所以不會進行傳輸。這種透過檢查來瞭解 HTTP 文件是否爲最新的方法能節省頻寬並減少延時。

爲減少與遠端伺服器的作業事件，Proxy Server 讓您可以爲 HTTP 文件設定 [Cache Expiration] 設定。[Cache Expiration] 設定會告知代理伺服器在傳送請求至伺服器之前預估 HTTP 文件是否需要更新檢查。代理伺服器會根據 HTTP 文件中標頭的 Last-Modified 日期來進行預估。

對於 HTTP 文件，還可以使用 [Cache Refresh] 設定。此選項指定代理伺服器是否一直進行更新檢查 (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才進行檢查。表 12-1 顯示如果過期設定與重新整理設定都已指定，代理伺服器會有怎樣的動作。使用重新整理設定會顯著減少延時和節省頻寬。

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
一直進行更新檢查	(不適用)	一直進行更新檢查
使用者指定的間隔	使用文件的「expires」標頭	間隔到期時進行更新檢查
	透過文件的 Last-Modified 標頭進行預估	預估值與 expires 標頭中的較小者 *

* 對於經常變更的文件，使用較小的值能防止從快取中取得過期的資料。

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更新檢查，還是讓它根據 [Cache Refresh] 設定 (更新檢查間隔) 來進行檢查。例如，HTTP 文件的合理重新整理間隔爲四到八個小時。重新整理間隔越長，代理伺服器連線至遠端伺服器的次數就越少。即使代理伺服器在重新整理間隔期間沒有進行更新檢查，使用者仍可按一下用戶端中的 [Reload] 按鈕來強制重新整理，這個動作會強制代理伺服器與遠端伺服器進行更新檢查。

可在 [Set Cache Specifics] 頁面或 [Set Caching Configuration] 頁面中設定 HTTP 文件的重新整理間隔。[Set Cache Specifics] 頁面讓您可以配置全域快取程序，而 [Set Caching Configuration] 頁面讓您可以控制特定 URL 與資源的快取程序。

設定 HTTP 快取過期策略

還可使用 last-modified 因素或僅使用明確的過期資訊以設定伺服器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，它指定此檔案將會過期的日期與時間。使用明確的 Expires 標頭的 HTTP 文件並不是很多，所以最好根據 Last-modified 標頭來進行預估。

如果決定基於 Last-modified 標頭對 HTTP 文件進行快取，則必須選取要在過期預估中使用的分數。這個分數，也就是 LM 因素，將與文件上次修改時間和上次對文件執行更新檢查的時間之間的間隔相乘，然後將產生的數目與上次更新檢查以來的時間加以比較。如果此數目小於時間間隔，則表示文件尚未過期。較小的分數會讓代理伺服器更頻繁地檢查文件。例如，假定有一個文件，上次變更它是在十天前。如果將 last-modified 因素設定爲 0.1，代理伺服器會將其解譯爲此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。

同樣以此做爲範例，如果 HTTP 文件的快取重新整理設定爲小於一天，代理伺服器一天中將進行一次以上的更新檢查。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])。

可在 [Set Cache Specifics] 頁面或 [Set Caching Configuration] 頁面中設定 HTTP 文件的過期設定。[Set Cache Specifics] 頁面讓您可以配置全域快取程序，而 [Set Caching Configuration] 頁面讓您可以控制特定 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 快取文件後至重新整理文件前，文件可能會被存取許多次。對於遠端伺服器，將一個副本傳送給將快取它的代理伺服器僅表示一次存取或一個 「符合項目」。Sun Java™ System Web Proxy Server 可以對在更新檢查之間從代理伺服器快取存取某份文件的次數進行計數，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。這樣一來，如果將遠端伺服器配置爲能夠識別此標頭類型，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 文件快取的唯一方法是設定 [Cache Refresh] 間隔。[Cache Refresh] 間隔是 Proxy Server 從遠端伺服器擷取文件最新版本之前等待的時間。如果不設定 [Cache Refresh] 間隔，即使快取中的版本爲最新，代理伺服器還是會擷取這些文件。

設定 FTP 與 Gopher 快取重新整理間隔

如果要爲 FTP 與 Gopher 設定快取重新整理間隔，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)。如果資料時常變更，您會希望至少每幾小時就擷取這些檔案。在重新整理期間，會有將過期檔案傳送給用戶端的風險。如果間隔足夠短 (幾小時)，就能消除大多數的此類風險，同時回應時間也得到顯著縮短。

可在 [Set Cache Specifics] 頁面或 [Set Caching Configuration] 頁面中設定 FTP 與 Gopher 文件的快取重新整理間隔。[Set Cache Specifics] 頁面讓您可以配置全域快取程序，而 [Set Caching Configuration] 頁面讓您可以控制特定 URL 與資源的快取程序。如需關於使用 [Set Cache Specifics] 頁面的更多資訊，請參閱第 234 頁的「設定快取細節」，如需關於使用 [Set Caching Configuration] 頁面的更多資訊，請參閱第 242 頁的「配置快取」。

備註	如果 FTP 與 Gopher 文件的情況差異甚鉅 (有些經常變更，有些則很少變更)，請使用 [Set Caching Configuration] 頁面來爲每種文件分別建立範本 (例如，建立包含資源 `ftp://.*.gif` 的範本)，然後爲此資源設定適當的重新整理間隔。

建立與修改快取

快取分割區是預留作爲快取用途的部分磁碟或記憶體。如果快取容量改變，可能想要使用 [Add/Edit Cache Partitions] 頁面來變更或增加分割區。利用此頁面可編輯分割區的位置、快捷名稱和大小限值。也可以檢視此分割區的快取區段表。

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。將顯示 [Add/Edit Cache Partitions] 頁面。
3. 按一下 [Add Cache Partition] 按鈕。將顯示 [Cache Partition Configuration] 頁面。

4. 爲新分割區輸入適當的值。
5. 按一下 [OK]。
6. 按一下 [Restart Required]。將顯示 [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。將顯示 [Add/Edit Cache Partitions] 頁面。
3. 在要變更的分割區名稱上按一下。
4. 編輯資訊。
5. 按一下 [OK]。
6. 按一下 [Restart Required]。將顯示 [Apply Changes] 頁面。
7. 按一下 [Restart Proxy Server] 按鈕以套用變更。

設定快取容量

快取容量值用於導出快取目錄結構。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結構有直接關係。容量越大，階層結構也就越大。快取容量應等於或大於快取大小。如果確定以後要增加快取大小 (如透過增加外部磁碟的方式)，則最好將容量設定爲大於快取大小。快取容量最大爲 32 GB，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。將顯示 [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]。將顯示 [Apply Changes] 頁面。
6. 按一下 [Restart Proxy Server] 按鈕以套用變更。

管理快取區段

代理伺服器快取可分隔成一或多個快取區段。最多可以分隔成 256 個區段。快取區段的數量必須是 2 的乘冪 (例如，1、2、4、8、16、...256)。最大容量爲 32GB (最佳值)，具有 256 個快取區段。

如果選擇使用 500MB 的快取容量，安裝程式會建立 4 個快取區段 (500 / 125 = 4)；如果選擇使用 2GB 的快取容量，安裝程式會建立 16 個區段 (2000 / 125 = 16)。選擇 125MB 作爲每個區段的最佳值以取得區段的數目。區段的數目越多，跨區段儲存與分散的 URL 的數目就越大。

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。將顯示 [Manage Sections] 頁面。
3. 變更表中的資訊。可在現有的各分割區間移動區段。
4. 按一下 [OK]。
5. 按一下 [Restart Required]。將顯示 [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

[Set Garbage Collection Preferences] 頁面可用來設定資源回收模式。

可使用快取資源回收器來刪除快取中的檔案。可以自動模式或明確模式來進行資源回收。明確模式由管理員使用 [Schedule Garbage Collection] 頁面在外部排定。選取一種模式，然後按一下 [OK]。按一下 [Restart Required]。將顯示 [Apply Changes] 頁面。按一下 [Restart Proxy Server] 按鈕以套用變更。

資源回收排程

[Schedule Garbage Collection] 頁面可讓您指定進行資源回收的日期和時間。

對資源回收排程：

1. 存取 Server Manager，然後按一下 [Caching] 標籤。
2. 按一下 [Schedule Garbage Collection] 連結。將顯示 [Schedule Garbage Collection]。
3. 從 [Schedule Garbage Collection At] 清單選取進行資源回收的時間。
4. 指定進行資源回收的一週中的某一天。
5. 按一下 [OK]。
6. 按一下 [Restart Required]。將顯示 [Apply Changes] 頁面。
7. 按一下 [Restart Proxy Server] 按鈕以套用變更。

配置快取

可使用 [Set Caching Configuration] 頁面來爲特定資源配置想要爲其配置的快取類型。可爲符合指定的常規表示式式樣的 URL 指定好幾個配置參數值。此功能可讓您根據快取的文件類型嚴密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
- 快取需要認證之頁面的方式
- 快取查詢的方式
- 快取檔案大小的上限與下限值
- 重新整理快取文件的時機
- 快取過期策略
- 用戶端中斷的快取運作方式
- 至原始伺服器的連線失敗時快取的運作方式

備註 如果將某個資源的快取預設值設定爲 [Derived Configuration] 或 [Don't Cache]，快取配置選項將不會出現在 [Set Caching Configuration] 頁面上。但是，如果爲資源選擇快取預設值 [Cache]，則可指定其他幾個配置項目。

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。將顯示 [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，輸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]。將顯示 [Apply Changes] 頁面。
7. 按一下 [Restart Proxy Server] 按鈕以套用變更。

快取配置元素

下列各節描述 [Set Caching Configuration] 頁面上所列的項目。這些節中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

代理伺服器可讓您指定特定資源的快取預設值。資源是符合指定的特定條件的檔案類型。例如，可能希望伺服器能自動從 company.com 網域快取所有文件。如果是這樣，請按一下 [Set Caching Configuration] 頁面頂端的 [Regular Expression] 按鈕，然後在出現的欄位中輸入

```
[a-z] *://[^/:]\.company\.com.*
```

。

依預設，將選取 [Cache] 選項。伺服器就會自動從此網域快取所有可快取的文件。如需關於常規表示式的更多資訊，請參閱 「瞭解常規表示式」。

備註	如果將某個資源的快取預設值設定爲 [Derived Configuration] 或 [Don't Cache]，就不需要爲此資源配置快取。但是，如果爲資源選擇快取預設值 [Cache]，則可指定其他幾個配置項目。如需這些項目的清單，請參閱第 242 頁的 「配置快取」。

還可在 [Set Cache Specifics] 頁面上設定 HTTP、FTP 和 Gopher 的快取預設值。

快取需要認證的頁面

可讓伺服器快取需要使用者認證的檔案。如果選擇讓 Proxy Server 快取這些檔案，Proxy Server 會爲快取中的檔案加上標籤，這樣一來，當使用者要求這些檔案時，Proxy Server 就會知道這些檔案需要來自遠端伺服器的認證。

因爲代理伺服器不知道遠端伺服器進行認證的方式，也不知道使用者的 ID 或密碼，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更新檢查。因此，使用者必須輸入 ID 和密碼才能獲得對此檔案的存取權。如果使用者已在 Navigator 階段作業的初期存取過此伺服器，Navigator 會自動傳送認證資訊，而不會要求使用者提供此認證資訊。

如果不啓用對需要認證的頁面的快取，代理伺服器會採用預設值，也就是不對它們進行快取。

快取查詢

快取查詢僅適用於 HTTP 文件。可以限制快取查詢的長度，也可以完全禁止快取查詢。查詢越長，就越不可能重複，快取的必要性也就越低。

下列爲查詢專用的快取限制：存取方法必須爲 GET，文件不得受到保護 (除非啓用對經認證頁面的快取功能)，回應必須至少包含一個 Last-modified 標頭。這需要查詢引擎指明可快取查詢結果文件。如果出現 Last-modified 標頭，則查詢引擎應支援條件式 GET 方法 (附帶 If-modified-since 標頭)，如此快取才會有效；否則它應傳回 Expires 標頭。

設定快取文件大小的上下限

可以爲 Proxy Server 快取的檔案設定下限與上限大小。如果網路連線速度快，可能需要設定下限大小。如果連線速度快，擷取小型檔案的速度會快至伺服器根本不需要快取這些檔案。在這種情況下，可能只想快取較大的檔案。可能想要設定檔案大小上限，以確定大型檔案不會佔用太多的代理伺服器磁碟空間。

設定更新檢查策略

可以使用此選項確保 HTTP 文件一直爲最新。也可以指定 Proxy Server 的重新整理間隔。

設定過期策略

可以使用 last-modified 因素或明確過期資訊來設定過期策略。

設定用戶端中斷的快取運作方式

如果文件只擷取了一部分用戶端就中斷了資料傳輸，則代理伺服器可以快取的方式完成整個文件的擷取。代理伺服器的預設值是在快取時完成文件的擷取，只要文件的擷取至少已完成 25%。否則，代理伺服器會終止遠端伺服器連線並移除已擷取了一部分的檔案。可以提高或降低用戶端中斷的百分比。

至伺服器的連線失敗時的運作方式

如果因爲無法與原始伺服器連線，致使對過期文件進行的更新檢查失敗，可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

如果從本地主機請求的 URL 缺少網域名稱，Proxy Server 將不會快取它，這是爲了避免重複快取。例如，如果使用者從本機伺服器請求 `http://machine/filename.html` 和 `http://machine.example.com/filename.html`，則這兩個 URL 可能都會出現在快取中。因爲這些檔案來自本地伺服器，可以極快速地擷取到，所以不需要以任何方式快取這些檔案。

但是，如果您的公司在許多遠端位置都有伺服器，可能想要從所有主機快取文件，以減少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。將顯示 [Cache Local Hosts] 頁面。
3. 從下拉式清單選取資源，或按一下 [Regular Expression] 按鈕，輸入常規表示式並按一下 [OK]。如需關於常規表示式的更多資訊，請參閱第 319 頁的第 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]。將顯示 [Apply Changes] 頁面。
7. 按一下 [Restart Proxy Server] 按鈕以套用變更。

配置檔案快取

依預設，檔案快取處於開啓狀態。檔案快取設定包含在 server.xml 檔案中。可以使用 Server Manager 變更檔案快取設定。

備註 [Configure File Cache] 頁面會顯示在使用者介面中，但此頁面在 Proxy Server 4 這個發行版本中沒有實作

配置檔案快取

1. 在 Server Manager 中，按一下 [Preferences] 標籤。
2. 按一下 [File Cache Configuration] 連結。將顯示 [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。

   如果啓用 [Transmit File]，伺服器會快取檔案快取中檔案的開啓檔案描述元，而非檔案內容，並使用 PR_TransmitFile 將檔案內容傳送至用戶端。啓用 [Transmit File] 時，就不會存在檔案快取通常會在小型、中型和大型檔案之間做出的區分，因爲只有開啓檔案描述元才會被快取。依預設，Windows 上的 [Transmit File] 爲啓用，在 UNIX 上則爲停用。在 UNIX 系統上，僅針對原本就對 PR_TransmitFile 提供作業系統支援的平台啓用 [Transmit File]，目前這樣的平台有 HP-UX 和 AIX。建議不要在其他 UNIX/Linux 平台上使用此選項。
5. 輸入雜湊表的大小。預設大小是檔案最大數目的兩倍加 1。例如，如果將檔案的最大數目設定爲 1024，則預設的雜湊表大小爲 2049。
6. 輸入有效快取項目的最長存在時間 (秒)。預設值爲 30。此設定控制快取檔案後可以繼續使用快取資訊的時間。超過 MaxAge 設定值的項目會被替代成同一檔案的新項目 (如果此檔案是透過快取參照的話)。根據是否依定期排程更新內容 (修改現有檔案) 來設定最長存在時間。例如，如果一天以固定時間間隔更新內容四次，可將最長存在時間設定爲 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. 輸入要快取的 [Maximum Number of Files]。預設值爲 1024。

8. 輸入中型與小型檔案大小限值 (位元組)。依預設，[Medium File Size Limit] 設定爲 537600，而 [Small File Size Limit] 設定爲 2048。

   快取會以不同方式處理小型、中型與大型檔案。透過將檔案對映到虛擬記憶體來快取中型檔案的內容 (目前僅限於 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。雖然會快取大型檔案的資訊，但不會快取大型檔案 (較中型檔案爲大) 的內容。在小型檔案與中型檔案間做出區分的好處在於，當小型檔案數量很多時能避免浪費虛擬記憶體眾多頁面的一部分。因此 [Small File Size Limit] 的值通常略微低於 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 (位元組)。依預設爲 10485760。小型檔案空間是用於快取的堆疊儲存區空間大小 (位元組)，其中包括用於快取小型檔案的堆疊儲存區空間。在 UNIX/Linux 上，預設值爲 1048576。

10. 按一下 [OK]。

11. 按一下 [Restart Required]。將顯示 [Apply Changes] 頁面。

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

檢視 URL 資料庫

可檢視所有記錄的快取 URL 的名稱與屬性。URL 資訊顯示成一份快取文件清單，按存取協定和網站名稱分組。在 [Search] 欄位中鍵入網域名稱可限制清單內顯示的 URL。透過存取此資訊，可執行各種快取管理功能，如將快取內的文件設定爲過期以及移除文件。

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。將顯示 [View URL Database] 頁面。

3. 按一下 [Regenerate] 按鈕以產生快取 URL 的最新清單。如果想要檢視特定 URL 的資訊，請在 [Search] 欄位中輸入 URL 或常規表示式，然後按一下 [Search] 按鈕。

4. 如果想要檢視按網域名稱和主機分組的快取資料庫資訊，請從清單中選取一個網域名稱。將出現此網域內的主機清單。按一下主機名稱，將出現 URL 清單。

5. 按一下 URL 的名稱。將出現有關此 URL 的詳細資訊。

將快取中的檔案設定爲過期以及移除檔案

可以從 [View URL Database] 頁面將快取中的文件設定爲過期以及移除文件。

將快取 URL 設定爲過期或將它們移除

1. 存取 Server Manager，然後按一下 [Caching] 標籤。
2. 按一下 [View URL Database] 連結。將顯示 [View URL Database] 頁面。
3. 按一下 [Regenerate] 按鈕。將會產生快取資料庫的快照。此快照構成了其餘步驟的基礎。
4. 如果知道想要設定爲過期或移除的特定 URL，請在 [Search] 欄位中輸入此 URL 或符合此 URL 的常規表示式，然後按一下 [Search] 按鈕。如果想要處理按網域名稱和主機分組的 URL，請從清單中選取一個網域名稱。將出現此網域內的主機清單。按一下主機名稱，將出現 URL 清單。
5. 若要將個別檔案設定爲過期，請選取那些檔案的 URL 旁邊的 [Ex] 選項，然後按一下 [Exp/Rem Marked] 按鈕。若要將清單中的所有檔案設定爲過期，請按一下表單底部的 [Exp All] 按鈕。若要從快取中移除個別檔案，請選取那些檔案的 URL 旁邊的 [Rm] 選項，然後按一下 [Exp/Rem Marked] 按鈕。若要移除清單中的所有檔案，請按一下 [Rem All] 按鈕。
6. 按一下 [Regenerate] 按鈕可重新產生快照。

備註 使用 [Ex] 或 [Rm] 選項時，會處理關聯的檔案，但所做變更不會反映在快照中。需重新產生快照才能顯示變更。

使用快取批次更新

[Cache Batch Update] 功能可讓您預先載入指定網站中的檔案，或每當代理伺服器不忙碌時對快取內已有的文件進行更新檢查。可透過 [Set Cache Batch Updates] 頁面建立、編輯和刪除 URL 批次以及啓用和停用批次更新功能。

建立批次更新

可透過指定要批次更新的檔案來主動地 (而不是按需要) 快取檔案。代理伺服器可讓您對快取內現有的若干個檔案執行更新檢查，或是預先載入某個網站中的多個檔案。

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。將顯示 [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] 和 [Create]。
4. 按一下 [OK]。將顯示 [Set Cache Batch Updates] 頁面。
5. 在 [Name] 區段中，輸入新的批次更新項目的名稱。
6. 在頁面的 [Source] 區段中，按一下要建立的批次更新類型的單選按鈕。如果要對快取內的所有文件執行更新檢查，請按一下第一個單選按鈕。如果要從給定來源 URL 開始以遞迴方式快取 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] 區段中指定想要排除在批次更新之外的所有檔案。
9. 在 [Resources] 區段中輸入最大同時連線數以及遍歷的最大文件數。
10. 在 [Timing] 區段中輸入批次更新產生的開始和結束時間。任一時刻只能有一個作用中的批次更新，所以最好不要與其他批次更新配置重疊。
11. 按一下 [OK]。

備註	建立、編輯和刪除批次更新配置時不需開啓批次更新。但是，如果希望批次更新根據在 [Set Cache Batch Updates] 頁面上設定的時間執行，則必須開啓批次更新。

12. 按一下 [Restart Required]。將顯示 [Apply Changes] 頁面。
13. 按一下 [Restart Proxy Server] 按鈕以套用變更。

編輯或刪除批次更新配置

使用 [Set Cache Batch Updates] 頁面可編輯或刪除批次更新。如果需要將某些檔案排除在批次更新之外，或想要更頻繁地更新批次，則可能想要編輯批次更新。也可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。將顯示 [Set Cache Batch Updates] 頁面。
3. 如果要編輯某批次，請從 [Create/Select a Batch Update Configuration] 旁的下拉式清單選取此批次的名稱與 「Edit」。如果要刪除某批次，請從下拉式清單選取此批次的名稱與 「Delete」。
4. 按一下 [OK]。將顯示 [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]。將顯示 [Apply Changes] 頁面。
8. 按一下 [Restart Proxy Server] 按鈕以套用變更。

使用快取指令行介面

代理伺服器隨附幾個指令行公用程式，可讓您配置、變更、產生以及修復快取目錄結構。這些公用程式大多數與 Server Manager 的頁面完全相同，但如果需要對維護 (例如，cron 工作) 進行排程，可能想要使用這些公用程式。所有這些公用程式都位於 `extras` 目錄中。

執行指令行公用程式

1. 至指令行提示符號的 *server_root*/`proxy-server`*id* 目錄。
2. 鍵入 **`./start -shell`**

   下列各節描述各種公用程式。

建立快取目錄結構

代理伺服器有一個稱爲 `cbuild` 的公用程式，它是一個離線快取資料庫管理程式。這個公用程式可讓您使用指令行介面建立新的快取結構或修改現有的快取結構。可以使用 Server Manager 頁面來讓代理伺服器能夠使用新建立的快取。這個公用程式不會更新 `server.xml` 檔案。`cbuild` 無法對有多個分割區的快取做大小調整。`server.xml` 檔案有一個稱爲 `CACHE` 的元素，其中包含 `cachecapacity` 參數。透過 `cbuild` 建立或修改快取時，應該在 `server.xml` 檔案中手動更新 `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">
```

可以用兩種模式來呼叫 cbuild 公用程式。第一種模式爲：

```
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。它位於下列路徑 *server_root*/proxy-server*id*/config。
- *cache-dir* 是快取結構的目錄。
- *cache size* 是快取可擴充到的上限大小。此選項不能與 *cache-dim* 參數一起使用。上限大小爲 65135 MB。
- -r 可調整現有快取結構的大小 (假如它只有單一分割區)。對於建立新快取則不需要。

可以執行 cbuild 的第二種模式爲：

```
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。它位於下列路徑 *server_root*/proxy-server*id*/config。
- *cache-dir* 是快取結構的目錄。

- *cache-dim* 確定區段的數目。例如，在圖 12-1 中，區段顯示爲 s3.4，其中 3 代表大小。*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 (假如它只有單一分割區)。對於建立新快取則不需要。

管理快取 URL 清單

代理伺服器有一個稱爲 `urldb` 的公用程式，可管理快取中的 URL 清單。可使用此公用程式來列出已快取的 URL。也可以選擇性地將快取資料庫中的快取物件設定爲過期及移除它們。

`urldb` 指令可根據 -o 選項分成三個群組：

- 網域
- 網站
- URL

若要列出網域，請在指令行中輸入下列內容：

`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` 會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。它位於下列路徑 *server_root*`/proxy-server`*id*`/config`。

若要列出網域中所有符合的網站，請在指令行中輸入下列內容：

`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` 會列出網域中符合常規表示式的所有網站
- *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。它位於下列路徑 *server_root*`/proxy-server`*id*`/config`

若要列出所有符合的網站，請在指令行中輸入下列內容：

```
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` 會列出符合常規表示式的所有網站
- *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。它位於下列路徑 *server_root*`/proxy-server`*id*`/config`

若要列出網站中所有符合的 URL，請在指令行中輸入下列內容：

```
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` 會列出符合常規表示式的網站中的所有 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。它位於下列路徑 *server_root*`/proxy-server`*id*`/config`

若要將網站中符合的 URL 設定爲過期或將它們移除，請在指令行中輸入下列內容：

```
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 iserver_root/proxy-serverid/config
```

其中

- `matching_urls_from_site` 會列出符合常規表示式的網站中的所有 URL
- *reg_exp* 是所使用的常規表示式
- *site_name* 是網站的名稱
- `-x e` 是用於將快取資料庫中符合的 URL 設定爲過期的選項。 此選項不能與網域和網站模式一起使用
- `-x r` 是用於將快取資料庫中符合的 URL 移除的選項
- *conf-dir* 是代理伺服器實例的配置目錄。它位於下列路徑 *server_root*`/proxy-server`*id*`/config`

若要列出所有符合的 URL，請在指令行中輸入下列內容：

```
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` 會列出符合常規表示式的所有 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。它位於下列路徑 *server_root*`/proxy-server`*id*`/config`

若要將所有符合的 URL 設定爲過期或將它們移除，請在指令行中輸入下列內容：

```
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` 會列出符合常規表示式的所有 URL

- *reg_exp* 是所使用的常規表示式
- `-x e` 是用於將快取資料庫中符合的 URL 設定爲過期的選項
- `-x r` 是用於將快取資料庫中符合的 URL 移除的選項
- *conf-dir* 是代理伺服器實例的配置目錄。它位於下列路徑 *server_root*`/proxy-server`*id*`/config`

若要將 URL 清單設定爲過期或將其移除，請在指令行中輸入下列內容：

`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-server`*id*`/config`

其中

- `url-list` 是需要設定爲到期的 URL 清單。此選項可用於提供 URL 清單。
- `-x e` 是用於將快取資料庫中符合的 URL 設定爲過期的選項。
- `-x r` 是用於將快取資料庫中符合的 URL 移除的選項。
- *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。它位於下列路徑 *server_root*`/proxy-server`*id*`/config`。

管理快取資源回收

`cachegc` 公用程式可讓您基於快取大小限制來清除快取資料庫中可能已過期的物件，或太舊以致於無法在目錄中快取的物件。

備註 在使用 `cachegc` 公用程式時，請確定 CacheGC 並未在代理伺服器實例中執行。

可以下列方式來使用 `cachegc` 公用程式：

`cachegc -f` *leave-fs-full-percent* `-u` *gc-high-margin-percent* `-l` *gc-low-margin-percen*`t -e` *extra-margin-percen*`t -d` *conf-dir*

例如：

`cachegc -f 50 -u 80 -l 60 -e 5 -d` *server_root*`/proxy-server`*id*`/config`

其中

- *leave-fs-full-percent* 可確定快取分割區大小的百分比，低於此百分比時資源回收將不會執行。
- *gc-high-margin-percent* 可控制最大快取大小的百分比，達到此百分比時就會觸發資源回收。
- *gc-low-margin-percen*t 可控制做爲資源回收器目標的最大快取大小的百分比。
- *extra-margin-percen*t 是由資源回收器用來確定要移除的快取百分比。
- *conf-dir* 是代理伺服器實例的配置目錄。它位於下列路徑 *server_root*/proxy-server*id*/config。

管理批次更新

bu 公用程式可更新快取，它在兩種模式下工作。在第一種模式中，它會遍歷快取資料庫並藉由爲每個 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，它會從給定 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 RFC 相容的自動器。

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-server*id*/config

其中

- *hostname* 是執行代理伺服器的機器的主機名稱。預設值爲 localhost。
- *port* 是代理伺服器執行時所使用的連接埠。預設連接埠爲 8080。
- *time-lmt* 是公用程式執行時的時間限制。
- *contact-address* 確定將透過從 bu 傳送來的 HTTP 請求傳送的連絡地址。預設值爲 worm@proxy-name。
- *sleep-time* 是兩個連續請求之間的暫停時間。預設值爲 5 秒。
- *object* 是目前正在執行的 bu.conf 中指定的物件。
- -r n 選項確定是否遵循了 robot.txt 策略。預設值爲 y。
- *conf-dir* 是代理伺服器實例的配置目錄。它位於下列路徑 *server_root*/proxy-server*id*/config。

使用網際網路快取協定 (ICP)

關於 ICP

網際網路快取協定 (ICP) 是一種物件位置協定，它可讓快取彼此進行通訊。快取可使用 ICP 來傳送有關快取 URL 是否存在，以及有關擷取這些 URL 的最佳位置的查詢和回覆。在典型的 ICP 交換中，一個快取將傳送有關某個 URL 的 ICP 查詢到所有鄰近的快取。然後這些快取會傳回 ICP 回覆，指明它們是否包含此 URL。如果它們不包含此 URL，就會傳回「MISS」。如果包含此 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內的代理伺服器進行通訊。它可讓一個管理網域中的代理伺服器快取與另一管理網域中的代理伺服器快取進行通訊。對於好幾個代理伺服器想要進行通訊但無法全部從一個主代理伺服器進行配置 (因爲它們位於代理伺服器陣列中) 的情形而言，ICP 是有效的。圖 12-3 顯示不同管理網域中各代理伺服器之間的 ICP 交換。

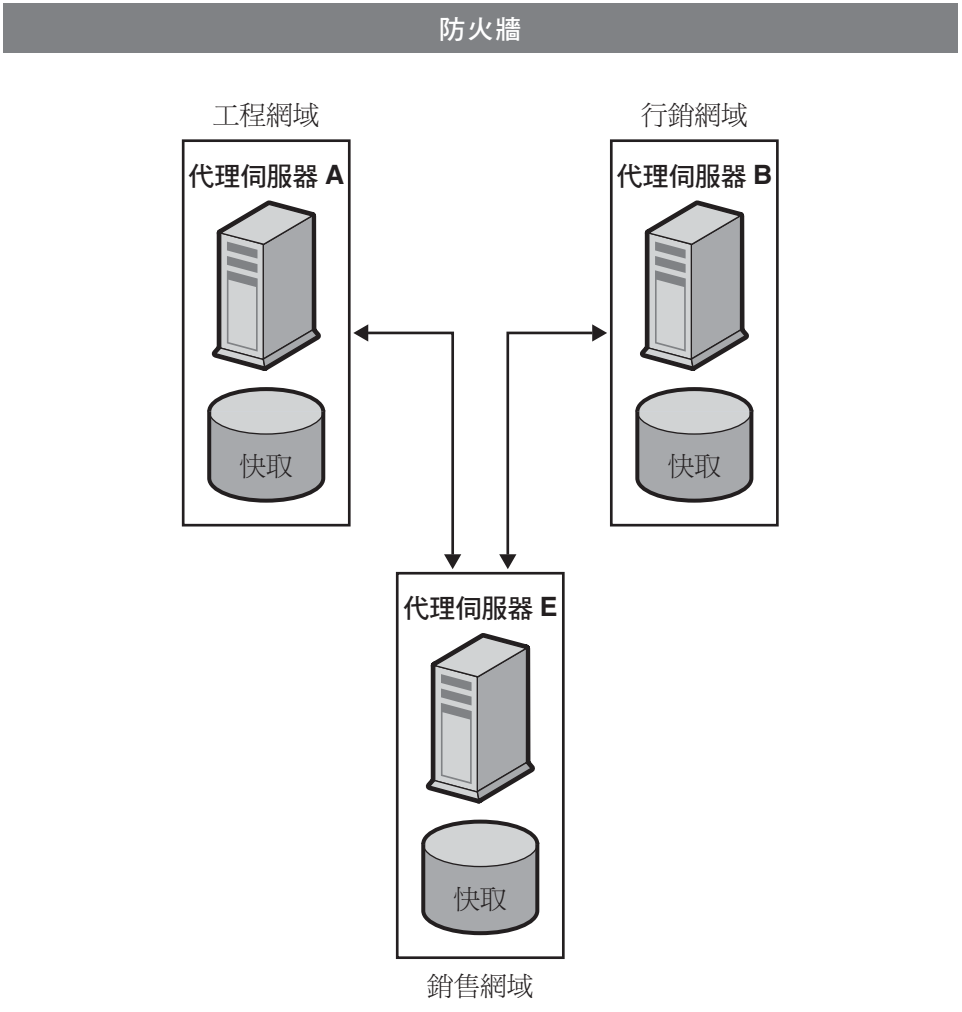
透過 ICP 相互通訊的代理伺服器稱爲**芳鄰**。一個 ICP 鄰近區域內的芳鄰不得超過 64 個。ICP 鄰近區域內的芳鄰有 2 種類型，**父系芳鄰**和**同層級芳鄰**。如果沒有其他芳鄰具備請求的 URL，則只有父系芳鄰可存取遠端伺服器。ICP 鄰近區域可以沒有父系芳鄰，也可以有一個以上父系芳鄰。ICP 鄰近區域內的任何芳鄰如果**不是**父系芳鄰，就會被視爲同層級芳鄰。同層級芳鄰無法擷取遠端伺服器中的文件，除非同層級芳鄰被標示爲 ICP 的預設路由，且 ICP 使用預設值。

可以使用**輪詢回合**來確定芳鄰接收查詢的順序。輪詢回合是 ICP 查詢循環。必須爲每個芳鄰指定一個輪詢回合。如果將所有芳鄰都配置在輪詢回合一，則會在一個循環中查詢所有芳鄰。換句話說，它們將同時接受查詢。如果將某些芳鄰配置在輪詢回合 2，則會先查詢輪詢回合一中的所有芳鄰，如果它們都沒有傳回「HIT」，則會查詢回合二中的所有代理伺服器。輪詢回合的最大數目爲二。

因爲 ICP 父系芳鄰可能會成爲網路瓶頸，可以使用輪詢回合來減輕其負載。常用設定方法是將所有同層級芳鄰配置在輪詢回合一中，而將所有父系芳鄰配置在輪詢回合二中。如此，當本機代理伺服器請求 URL 時，請求會先傳送到鄰近區域中的所有同層級芳鄰。如果同層級芳鄰都沒有請求的 URL，則將請求傳送給父系芳鄰。如果父系芳鄰沒有此 URL，就會從遠端伺服器擷取。

ICP 鄰近區域中的每個芳鄰都必須至少有一個執行中的 ICP 伺服器。如果芳鄰沒有執行中的 ICP 伺服器，就無法回覆來自其芳鄰的 ICP 請求。啓用代理伺服器上的 ICP 時會啓動 ICP 伺服器 (如果它尚未執行)。

圖 12-3 ICP 交換



設定 ICP

1. 向 ICP 鄰近區域增加父系芳鄰。(希望 ICP 鄰近區域中有父系芳鄰時才需要執行此步驟。) 如需關於向 ICP 鄰近區域增加父系芳鄰的更多資訊，請參閱第 259 頁的「向 ICP 鄰近區域增加父系芳鄰」。
2. 向 ICP 鄰近區域增加同層級芳鄰。如需關於向 ICP 鄰近區域增加同層級芳鄰的更多資訊，請參閱第 261 頁的「向 ICP 鄰近區域增加同層級芳鄰」。
3. 配置 ICP 鄰近區域中的每個芳鄰。如需關於配置 ICP 芳鄰的更多資訊，請參閱第 263 頁的「配置個別 ICP 芳鄰」。
4. 啓用 ICP。如需關於啓用 ICP 的資訊，請參閱第 264 頁的「啓用 ICP」。
5. 如果代理伺服器在其 ICP 鄰近區域中有同層級芳鄰或父系芳鄰，請啓用透過 ICP 鄰近區域進行路由。如需關於啓用透過 ICP 鄰近區域進行路由的更多資訊，請參閱第 265 頁的「啓用透過 ICP 鄰近區域進行路由」。

向 ICP 鄰近區域增加父系芳鄰

向 ICP 鄰近區域增加父系代理伺服器

1. 存取 Server Manager，然後按一下 [Caching] 標籤。
2. 按一下 [Configure ICP] 連結。將顯示 [Configure ICP] 頁面。
3. 在頁面的 [Parent List] 區段中按一下 [Add] 按鈕。將顯示 [ICP Parent] 頁面。
4. 在 [Machine Address] 欄位中輸入要向 ICP 鄰近區域增加的父系代理伺服器的 IP 位址或主機名稱。
5. 在 [ICP Port] 欄位中輸入父系代理伺服器用來偵聽 ICP 訊息的連接埠號。
6. 在 [Multicast Address] 欄位中，可輸入父系代理伺服器偵聽的多重播送位址。多重播送位址是可讓多台伺服器偵聽的 IP 位址。使用多重播送位址可讓代理伺服器傳送一個查詢至網路，偵聽此多重播送位址的所有芳鄰都能看到此查詢；如此一來，就不需要將查詢分別傳送至每個芳鄰。使用多重播送爲選擇性。

備註	不同輪詢回合中的芳鄰不應偵聽同一個多重播送位址。

7. 在 [TTL] 欄位中，輸入將多重播送訊息轉寄至的子網路數目。如果將 [TTL] 設定爲 1，多重播送訊息將只會轉寄至本機子網路。如果 [TTL] 爲 2，訊息將會轉寄至所有相差一個層級的子網路，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，如果想要防止不相關的芳鄰收到 ICP 鄰近區域內的代理伺服器所傳送的 ICP 訊息，應在 [TTL] 欄位中設定較低的 TTL 值。

8. 在 [Proxy Port] 欄位中，輸入父系代理伺服器的連接埠。
9. 從 [Polling Round] 下拉式清單中選擇希望父系代理伺服器位於的輪詢回合。預設輪詢回合爲 1。
10. 按一下 [OK]。
11. 按一下 [Restart Required]。將顯示 [Apply Changes] 頁面。
12. 按一下 [Restart Proxy Server] 按鈕以套用變更。

編輯 ICP 鄰近區域中的父系代理伺服器配置

編輯父系代理伺服器配置

1. 存取 Server Manager，然後按一下 [Caching] 標籤。
2. 選取 [Configure ICP] 連結。將顯示 [Configure ICP] 頁面。
3. 按一下要編輯的父系代理伺服器旁的單選按鈕。
4. 按一下 [Edit] 按鈕。
5. 修改相應的資訊。
6. 按一下 [OK]。
7. 按一下 [Restart Required]。將顯示 [Apply Changes] 頁面。
8. 按一下 [Restart Proxy Server] 按鈕以套用變更。

移除 ICP 鄰近區域中的父系代理伺服器

移除 ICP 鄰近區域中的父系代理伺服器

1. 存取 Server Manager，然後按一下 [Caching] 標籤。
2. 選取 [Configure ICP] 連結。將顯示 [Configure ICP] 頁面。
3. 按一下要移除的父系代理伺服器旁的單選按鈕。
4. 按一下 [Delete] 按鈕。
5. 按一下 [Restart Required]。將顯示 [Apply Changes] 頁面。
6. 按一下 [Restart Proxy Server] 按鈕以套用變更。

向 ICP 鄰近區域增加同層級芳鄰

向 ICP 鄰近區域增加同層級代理伺服器

1. 存取 Server Manager，然後按一下 [Caching] 標籤。
2. 選取 [Configure ICP] 連結。將顯示 [Configure ICP] 頁面。
3. 在頁面的 [Sibling List] 區段中按一下 [Add] 按鈕。將顯示 [ICP Sibling] 頁面。
4. 在 [Machine Address] 欄位中，輸入要向 ICP 鄰近區域增加的同層級代理伺服器的 IP 位址或主機名稱。
5. 在 [Port] 欄位中，輸入同層級代理伺服器用來偵聽 ICP 訊息的連接埠號。
6. 在 [Multicast Address] 欄位中，輸入同層級代理伺服器偵聽的多重播送位址。多重播送位址是可讓多台伺服器偵聽的 IP 位址。使用多重播送位址可讓代理伺服器傳送一個查詢至網路，偵聽此多重播送位址的所有芳鄰都能看到此查詢；如此一來，就不需要將查詢分別傳送至每個芳鄰。

備註 不同輪詢回合中的芳鄰不應偵聽同一個多重播送位址。

7. 在 [TTL] 欄位中，輸入將多重播送訊息轉寄至的子網路數目。如果將 [TTL] 設定爲 1，多重播送訊息將只會轉寄至本機子網路。如果 [TTL] 爲 2，訊息將會轉寄至所有相差一個層級的子網路。

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，如果想要防止不相關的芳鄰收到 ICP 鄰近區域內的代理伺服器所傳送的 ICP 訊息，應在 [TTL] 欄位中設定較低的 TTL 值。

8. 在 [Proxy Port] 欄位中，輸入同層級代理伺服器的連接埠。
9. 從 [Polling Round] 下拉式清單中選擇希望同層級代理伺服器位於的輪詢回合。預設輪詢回合爲 1。
10. 按一下 [OK]。
11. 按一下 [Restart Required]。將顯示 [Apply Changes] 頁面。
12. 按一下 [Restart Proxy Server] 按鈕以套用變更。

編輯 ICP 鄰近區域中的同層級代理伺服器配置

編輯同層級代理伺服器配置

1. 存取 Server Manager，然後按一下 [Caching] 標籤。
2. 選取 [Configure ICP] 連結。將顯示 [Configure ICP] 頁面。
3. 按一下要編輯的同層級代理伺服器旁的單選按鈕。
4. 按一下 [Edit] 按鈕。
5. 修改相應的資訊。
6. 按一下 [OK]。
7. 按一下 [Restart Required]。將顯示 [Apply Changes] 頁面。
8. 按一下 [Restart Proxy Server] 按鈕以套用變更。

移除 ICP 鄰近區域中的同層級芳鄰

移除 ICP 鄰近區域中的同層級代理伺服器

1. 存取 Server Manager，然後按一下 [Caching] 標籤。
2. 選取 [Configure ICP] 連結。將顯示 [Configure ICP] 頁面。
3. 按一下要移除的同層級代理伺服器旁的單選按鈕。
4. 按一下 [Delete] 按鈕。
5. 按一下 [Restart Required]。將顯示 [Apply Changes] 頁面。
6. 按一下 [Restart Proxy Server] 按鈕以套用變更。

配置個別 ICP 芳鄰

需要配置 ICP 鄰近區域內的每個芳鄰 (或稱本機代理伺服器)。

配置 ICP 鄰近區域內的本機代理伺服器

1. 存取 Server Manager，然後按一下 [Caching] 標籤。
2. 選取 [Configure ICP] 連結。將顯示 [Configure ICP] 頁面。
3. 在 [Binding Address] 欄位中，輸入芳鄰伺服器將連結至的 IP 位址。
4. 在 [Port] 欄位中，輸入芳鄰伺服器用來偵聽 ICP 的連接埠號。
5. 在 [Multicast Address] 欄位中，輸入芳鄰偵聽的多重播送位址。多重播送位址是可讓多台伺服器偵聽的 IP 位址。使用多重播送位址可讓代理伺服器傳送一個查詢至網路，偵聽此多重播送位址的所有芳鄰都能看到此查詢；如此一來，就不需要將查詢分別傳送至每個芳鄰。

   如果指定了芳鄰的多重播送位址和連結位址，芳鄰會使用連結位址來傳送回覆，使用多重播送位址來進行偵聽。如果連結位址或多重播送位址都沒有指定，作業系統會自行決定要用哪個位址來傳送資料。
6. 在 [Default Route] 欄位中，輸入當沒有鄰近代理伺服器回應以「符合項目」時，芳鄰應將請求路由至的代理伺服器的名稱或 IP 位址。如果在此欄位中輸入「origin」或將其留爲空白，預設路由將指向原始伺服器。

備註	如果從 [No Hit Behavior] 下拉式清單中選擇「first responding parent」，在 [Default Route] 欄位中輸入的路由將不起作用。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] 欄位中輸入在 [Default Route] 欄位中輸入的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級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。可以選擇：
   - **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，輸入將爲 ICP 請求提供服務的程序數。
10. 在 [Timeout] 欄位中，輸入芳鄰在每一回合中等待 ICP 回應的最長時間。
11. 按一下 [OK]。
12. 按一下 [Restart Required]。將顯示 [Apply Changes] 頁面。
13. 按一下 [Restart Proxy Server] 按鈕以套用變更。

啓用 ICP

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。將顯示 [Configure System Preferences] 頁面。
3. 選取 ICP 的 [Yes] 單選按鈕。
4. 按一下 [OK]。
5. 按一下 [Restart Required]。將顯示 [Apply Changes] 頁面。
6. 按一下 [Restart Proxy Server] 按鈕以套用變更。

啓用透過 ICP 鄰近區域進行路由

啓用透過 ICP 鄰近區域進行路由

1. 存取 Server Manager，然後按一下 [Routing] 標籤。
2. 按一下 [Set Routing Preferences] 連結。將出現 [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，輸入常規表示式並按一下 [OK]。
4. 選取文字 [Route Through] 旁的單選按鈕。
5. 選取 ICP 旁的核取方塊。
6. 如果要讓用戶端直接從具有此文件的 ICP 芳鄰擷取文件，而不用透過其他芳鄰取得，請選取文字 [redirect] 旁的核取方塊。
7. 按一下 [OK]。

注意 重新導向目前不受任何用戶端支援，所以現在請不要使用此功能。

備註 只有當代理伺服器在 ICP 鄰近區域內有其他同層級芳鄰或父系芳鄰時，才需要啓用透過 ICP 鄰近區域進行路由。如果代理伺服器是另一代理伺服器的父系，並且自身沒有任合同層級芳鄰或父系芳鄰，則需要只爲此代理伺服器啓用 ICP。不需要啓用透過 ICP 鄰近區域進行路由。

8. 按一下 [Restart Required]。將顯示 [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

關於代理伺服器陣列

分散式快取的代理伺服器陣列能讓多個代理伺服器像單一快取那樣發揮作用。換句話說，陣列中的每個代理伺服器將包含不同的快取 URL，這些 URL 可以由瀏覽器或下游代理伺服器擷取。代理伺服器陣列可防止有多個代理伺服器時經常出現的快取重複。代理伺服器陣列會透過雜湊型路由將請求路由到代理伺服器陣列中的正確快取。

代理伺服器陣列也允許遞增式延展性。換句話說，如果決定向代理伺服器陣列增加另一代理伺服器，每個成員的快取均不會失效。每個成員的快取中只有 $1/n$ 的 URL 會被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進行路由

對於每個透過代理伺服器陣列路由的請求，雜湊函數會爲陣列中的每個代理伺服器指定一個分數，這個分數以請求的 URL、代理伺服器的名稱以及代理伺服器的負載因素爲基礎。接著會將請求路由至具有最高分數的代理伺服器。

因爲 URL 請求可能來自用戶端與代理伺服器兩方，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，用戶端使用代理伺服器自動配置 (PAC) 機制來確定要透過哪個代理伺服器。但是，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 檔案來確定所請求 URL 的適當路由，圖 12-4 顯示了用戶端至代理伺服器路由。

在圖 12-4 中，代理伺服器陣列的每個成員均載入並輪詢主代理伺服器，以確定 PAT 檔案是否有更新。用戶端一旦擁有 PAC 檔案，就只有配置變更時才需要再次下載此檔案。一般而言，用戶端會在重新啓動時下載 PAC 檔案。

代理伺服器會從透過管理介面製作的代理伺服器陣列成員身份表 (PAT) 規格來自動產生特殊的 PAC 檔案。

在代理伺服器至代理伺服器路由中，代理伺服器使用某個 PAT (代理伺服器陣列表) 檔案來計算雜湊演算法，此檔案並非用戶端所使用的 PAC 檔案。此 PAT 檔案是一個包含代理伺服器陣列相關資訊的 ASCII 檔案，這些資訊包括代理伺服器的機器名稱、IP 位址、連接埠、負載因素、快取大小等。對於在伺服器處計算雜湊演算法，使用 PAT 檔案比使用 PAC 檔案 (必須在執行階段解譯的 JavaScript 檔案) 要高效得多。但是，大多數用戶端無法識別 PAT 檔案格式，所以必須使用 PAC 檔案。圖 12-5 顯示了代理伺服器至代理伺服器路由。

將在代理伺服器陣列的一個代理伺服器 — 主代理伺服器上建立 PAT 檔案。代理伺服器管理員必須確定哪個代理伺服器將做爲主代理伺服器。管理員可以從這個主代理伺服器變更 PAT 檔案，之後代理伺服器陣列的所有其他成員將可手動或自動輪詢主代理伺服器以取得這些變更。可以配置每個成員自動根據這些變更產生 PAC 檔案。

還可以將代理伺服器陣列鏈接在一起，以進行階層式路由。如果代理伺服器透過上游代理伺服器陣列路由內送請求，此上游代理伺服器陣列即爲父系代理伺服器陣列。父系代理伺服器陣列是代理伺服器經過的代理伺服器陣列。換句話說，如果用戶端向代理伺服器 X 請求文件，而代理伺服器 X 沒有此文件，就會將請求傳送給代理伺服器陣列 Y，而不會將其直接傳送給遠端伺服器。所以，代理伺服器陣列 Y 是父系代理伺服器陣列。在圖 12-5 中，代理伺服器陣列 1 是代理伺服器陣列 2 的父系代理伺服器陣列。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。通常輪詢的是父代理伺服器陣列中的主代理伺服器。所請求 URL 的雜湊演算法使用下載的 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 中具有最高分數的代理伺服器擷取請求的 URL。在圖 12-5 中，就用戶端所請求的 URL 而言，代理伺服器 B 具有最高分數。

圖 12-4 用戶端至代理伺服器路由

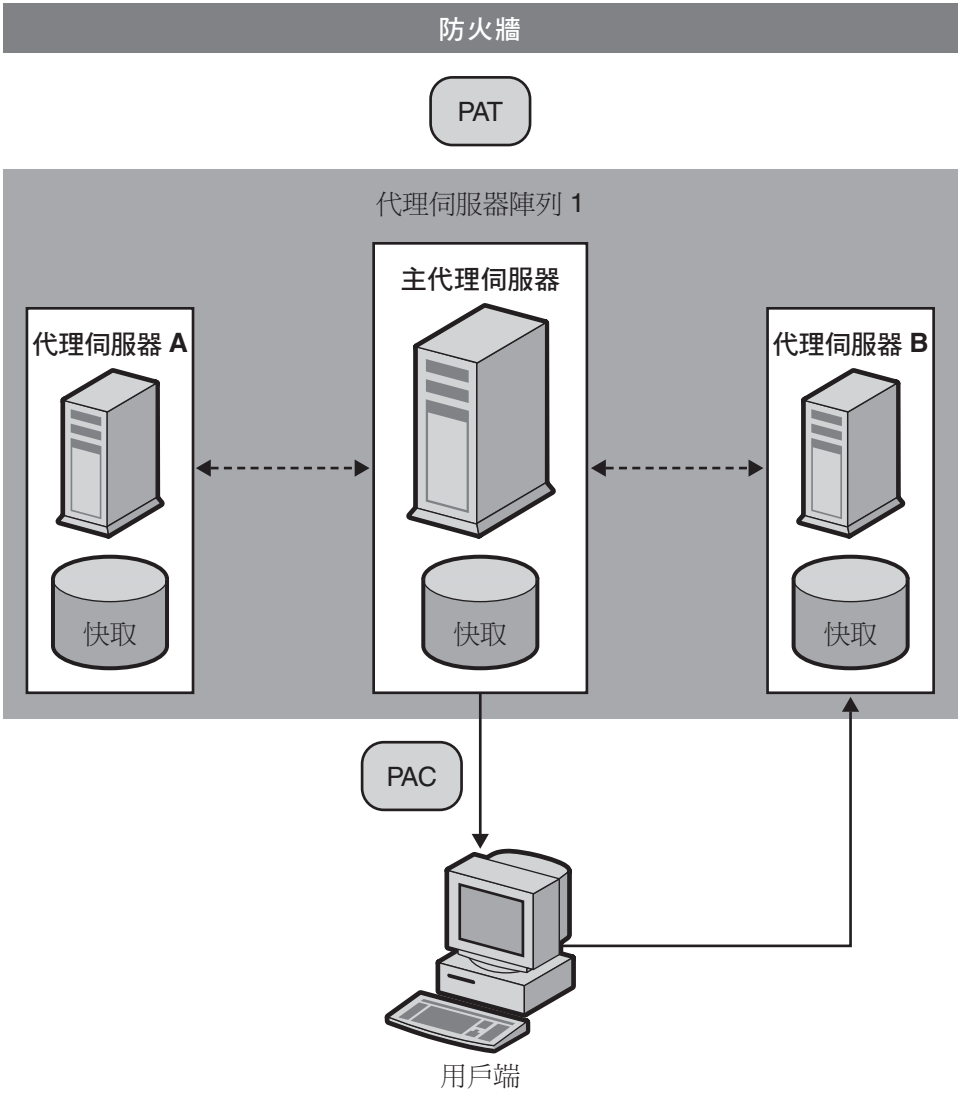
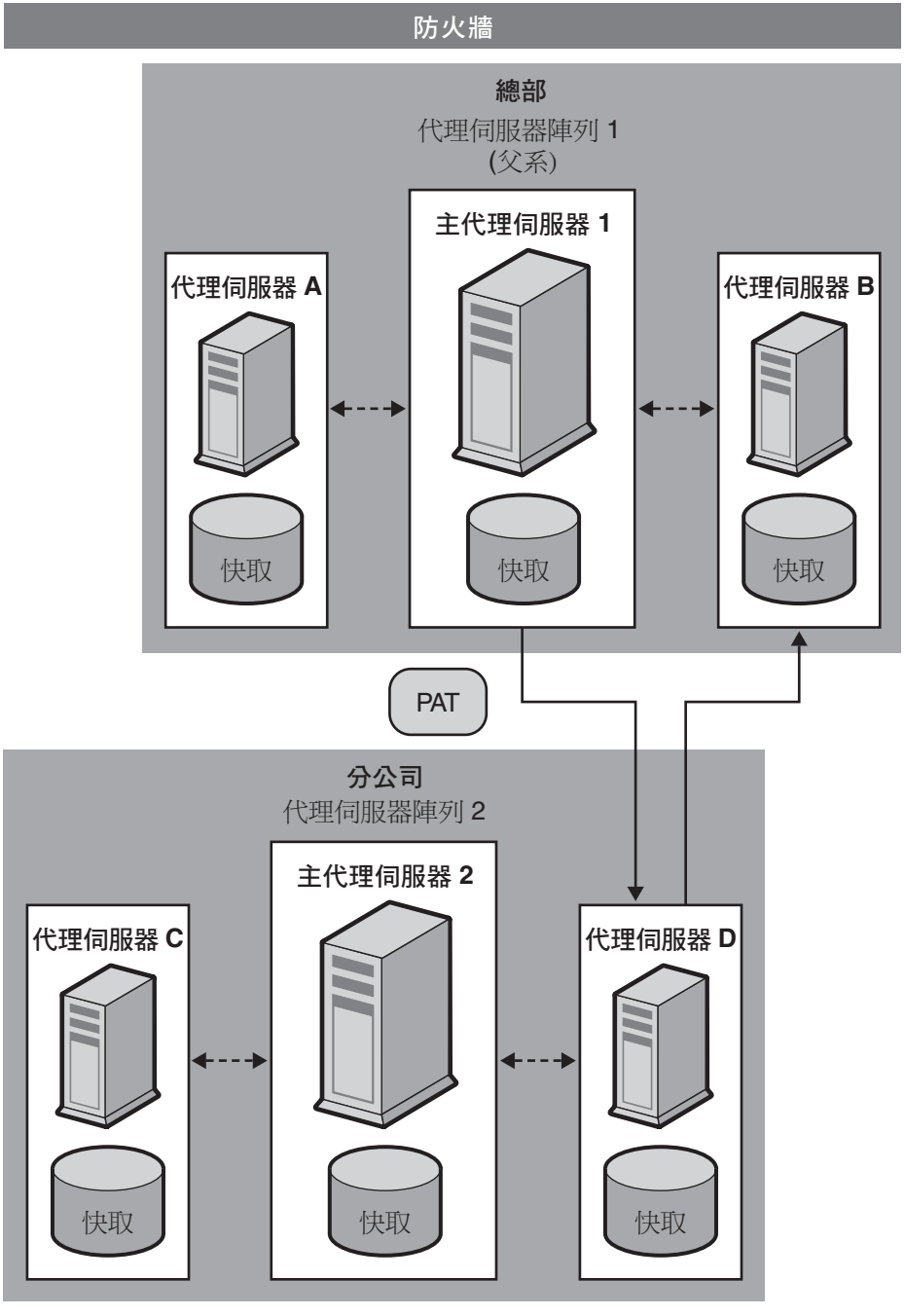


圖 12-5 代理伺服器至代理伺服器路由



設定代理伺服器陣列

1. 從主代理伺服器執行下列步驟：

   a. 建立代理伺服器陣列。如需關於建立成員清單的更多資訊，請參閱第 271 頁的「建立代理伺服器陣列成員清單」。

   b. 使用 PAT 檔案產生 PAC 檔案。如果使用用戶端至代理伺服器路由，則只需產生 PAC 檔案。如需關於使用 PAT 檔案產生 PAC 檔案的更多資訊，請參閱第 276 頁的「使用 PAT 檔案產生 PAC 檔案」。

   c. 配置陣列的主成員。如需關於配置主成員的更多資訊，請參閱第 273 頁的「配置代理伺服器陣列成員」。

   d. 啓用透過代理伺服器陣列進行路由。如需關於啓用透過代理伺服器陣列進行路由的更多資訊，請參閱第 274 頁的「啓用透過代理伺服器陣列進行路由」。

   e. 建立 PAT 對映以將 URL 「/pat」對映至 PAT 檔案。

   f. 啓用代理伺服器陣列。如需關於啓用代理伺服器陣列的更多資訊，請參閱第 275 頁的「啓用代理伺服器陣列」。

2. 從每個非主代理伺服器執行下列步驟：

   a. 配置陣列的非主成員。如需關於配置非主成員的更多資訊，請參閱第 273 頁的「配置代理伺服器陣列成員」。

   b. 啓用透過代理伺服器陣列進行路由。如需關於啓用透過代理伺服器陣列進行路由的更多資訊，請參閱第 274 頁的「啓用透過代理伺服器陣列進行路由」。

   c. 啓用代理伺服器陣列。如需關於啓用代理伺服器陣列的更多資訊，請參閱第 275 頁的「啓用代理伺服器陣列」。

備註 如果代理伺服器陣列將透過父系代理伺服器陣列路由，則還必須啓用父系代理伺服器陣列，並配置每個成員透過父系代理伺服器陣列進行路由來取得所需的 URL。如需關於父系代理伺服器陣列的更多資訊，請參閱第 277 頁的「透過父系代理伺服器陣列進行路由」。

建立代理伺服器陣列成員清單

只應從陣列的主代理伺服器處建立及更新代理伺服器陣列成員清單。只需建立代理伺服器陣列成員清單一次，但可隨時對其進行修改。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。

注意 如要對代理伺服器陣列成員清單進行增補或變更，只應透過陣列中的主代理伺服器進行。陣列中的所有其他成員都只能讀取成員清單。

1. 存取 Server Manager，然後按一下 [Caching] 標籤。
2. 按一下 [Configure Proxy Array] 連結。將顯示 [Configure Proxy Array] 頁面。
3. 在 [Array name] 欄位中，輸入陣列的名稱。
4. 在 [Reload Configuration Every] 欄位中，輸入每次針對 PAT 檔案的輪詢之間的分鐘數。
5. 按一下 [Array Enabled] 核取方塊。
6. 按一下 [Create] 按鈕。

備註 在開始增加成員至成員清單前，請務必按一下 [OK]。

備註 建立代理伺服器陣列後 [Create] 按鈕會變更爲 [OK] 按鈕。

7. 按一下 [Restart Required]。將顯示 [Apply Changes] 頁面。
8. 爲代理伺服器陣列中的每個成員輸入下列資訊，然後按一下 [OK]：
   - **Name。**要向成員清單增加的代理伺服器的名稱。
   - **IP Address。**要向成員清單增加的代理伺服器的 IP 位址。
   - **Port。**此爲成員輪詢 PAT 檔案時使用的連接埠。
   - **Load Factor。**一個整數，表示應通過此成員路由的相關負載。
   - **Status。**成員狀態。此值可爲 [on] 或 [off]。如果停用某個代理伺服器陣列成員，此成員的請求將透過另一個成員重新路由。

備註 在增加其他成員之前，應該先增加主成員。

備註 爲要增加的每個代理伺服器陣列成員輸入相關資訊之後，請務必按一下 [OK]。

9. 按一下 [Restart Required]。將顯示 [Apply Changes] 頁面。
10. 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

可隨時在代理伺服器陣列成員清單中變更成員的資訊。只能從主代理伺服器處編輯代理伺服器陣列成員清單。

注意 如要對代理伺服器陣列成員清單進行增補或變更，只應透過陣列中的主代理伺服器進行。如果從陣列中任何其他成員處修改此清單，所有變更都會遺失。

編輯代理伺服器陣列中任何成員的成員清單資訊

1. 存取 Server Manager，然後按一下 [Caching] 標籤。
2. 按一下 [Configure Proxy Array] 連結。將顯示 [Configure Proxy Array] 頁面。
3. 在 [Member List] 中，選取要編輯的成員旁的單選按鈕。
4. 按一下 [Edit] 按鈕。將顯示 [Configure Proxy Array Member] 頁面。
5. 編輯相應的資訊。
6. 按一下 [OK]。
7. 按一下 [Restart Required]。將顯示 [Apply Changes] 頁面。
8. 按一下 [Restart Proxy Server] 按鈕以套用變更。

備註 如果要讓變更生效，並將變更分發給代理伺服器陣列的成員，必須更新 [Configure Proxy Array] 頁面上的 [Configuration ID]，然後按一下 [OK]。若要更新配置 ID，只需將其增加 1。

刪除代理伺服器陣列成員

刪除代理伺服器陣列成員時會將它們從代理伺服器陣列中移除。只能從主代理伺服器處刪除代理伺服器陣列成員。

注意 如要對代理伺服器陣列成員清單進行增補或變更，只應透過陣列中的主代理伺服器進行。如果從陣列中任何其他成員處修改此清單，所有變更都會遺失。

刪除代理伺服器陣列的成員

1. 存取 Server Manager，然後按一下 [Caching] 標籤。
2. 按一下 [Configure Proxy Array] 連結。將顯示 [Configure Proxy Array] 頁面。
3. 在 [Member List] 中，選取要刪除的成員旁的單選按鈕。
4. 按一下 [Delete] 按鈕。

備註 如果要讓變更生效，並將變更分發給代理伺服器陣列的成員，必須更新 [Configure Proxy Array] 頁面上的 [Configuration ID]，然後按一下 [OK]。若要更新配置 ID，只需將其增加 1。

5. 按一下 [Restart Required]。將顯示 [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。無法從某個成員處配置陣列的其他成員。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。將顯示 [Configure Proxy Array Member] 頁面。
3. 在 [Proxy Array] 區段中，透過選取相應的單選按鈕來指定成員是否需要針對 PAT 檔案進行輪詢。選項包括：
   - **Non-Master Member。**如果配置的成員**不是**主代理伺服器，則應選取此選項。任何不是主代理伺服器的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處擷取它。

- **Master Member。**如果要配置主代理伺服器，則應選取此選項。如果要配置主代理伺服器，PAT 檔案將位於本機，不需進行輪詢。

4. 在 [Poll Host] 欄位中，輸入要針對 PAT 檔案進行輪詢的主代理伺服器的名稱。
5. 在 [Port] 欄位中，輸入主代理伺服器接受 HTTP 請求所使用的連接埠。
6. 在 [URL] 欄位中，輸入主代理伺服器上 PAT 檔案的 URL。如果已在主代理伺服器上建立了 PAT 對映，將 PAT 檔案與 URL `/pat` 對映，則應在 [URL] 欄位中輸入 **`/pat`**。
7. 在 [Headers File] 欄位中，輸入檔案的完整路徑名稱，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。
8. 按一下 [OK]。
9. 按一下 [Restart Required]。將顯示 [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進行路由

啓用透過代理伺服器陣列進行路由

1. 存取 Server Manager，然後按一下 [Routing] 標籤。
2. 按一下 [Set Routing Preferences] 連結。將出現 [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，輸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與 / 或父系代理伺服器陣列的核取方塊。
6. 如果選擇透過代理伺服器陣列路由，並希望將請求重新導向給其他 URL，請選取 [redirect] 核取方塊。重新導向表示如果代理伺服器陣列的某個成員收到它不應提供服務的請求，則會告知用戶端要連絡哪個代理伺服器來處理此請求。
7. 按一下 [OK]。

備註 只有在配置的代理伺服器是代理伺服器陣列的成員時，才可以啓用代理伺服器陣列路由。只有在父系代理伺服器陣列存在時，才可啓用父系代理伺服器陣列路由。這兩個路由選項相互獨立。

注意 重新導向目前不受任何用戶端支援，所以現在不應使用此功能。

8. 按一下 [Restart Required]。將顯示 [Apply Changes] 頁面。
9. 按一下 [Restart Proxy Server] 按鈕以套用變更。

啓用代理伺服器陣列

啓用代理伺服器陣列

1. 存取 Server Manager，然後按一下 [Preferences] 標籤。
2. 按一下 [Configure System Preferences] 連結。將顯示 [Configure System Preferences] 頁面。
3. 按一下要啓用的陣列類型 (一般代理伺服器陣列或父系代理伺服器陣列) 的 [Yes] 選項。
4. 按一下 [OK]。

備註 如果不是透過代理伺服器陣列進行路由，在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的 PAC 檔案進行正確路由。如果停用父系代理伺服器陣列選項，應已在 [Set Routing Preferences] 頁面中設定了有效的替代路由選項，例如明確的代理伺服器或直接連線。

5. 按一下 [Restart Required]。將顯示 [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

如果選擇透過代理伺服器陣列進行路由，則必須指定是否要將請求重新導向給其他 URL。重新導向表示如果代理伺服器陣列的某個成員收到它不應提供服務的請求，則會告知用戶端要連絡哪個代理伺服器來處理此請求。

注意 重新導向目前不受任何用戶端支援，所以現在不應使用此功能。

使用 PAT 檔案產生 PAC 檔案

因爲大多數用戶端無法識別 PAT 檔案格式，用戶端至代理伺服器路由方式的用戶端會使用代理伺服器自動配置 (PAC) 機制來接收關於要經過哪個代理伺服器的資訊。但是，用戶端不是使用標準的 PAC 檔案，而是使用一種源自 PAT 檔案的特殊 PAC 檔案。這個特殊 PAC 檔案會計算雜湊演算法來確定所請求 URL 的適當路由。

可以使用 PAT 檔案手動或自動產生 PAC 檔案。如果從代理伺服器陣列的特定成員處手動產生 PAC 檔案，此成員會根據 PAT 檔案中的現有資訊立即重新產生 PAC 檔案。如果將代理伺服器陣列成員配置爲自動產生 PAC 檔案，則每次成員偵測到 PAT 檔案有修改版本時，就會自動重新產生此檔案。

備註	如果沒有爲代理伺服器使用代理伺服器陣列功能，則應使用 [Create / Edit Autoconfiguration File] 頁面來產生 PAC 檔案。如需更多資訊，請參閱 第 325 頁的第 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

備註	PAC 檔案只能從主代理伺服器產生。

使用 PAT 檔案手動產生 PAC 檔案

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。將顯示 [Configure Proxy Array] 頁面。
3. 按一下 [Generate PAC] 按鈕。將顯示 [PAC Generation] 頁面。
4. 如果要在 PAC 檔案中使用自訂邏輯，請在 [Custom logic file] 欄位中輸入包含自訂邏輯的檔案名稱，此邏輯是您希望包含在所產生的 PAC 檔案中的邏輯。將把此邏輯插入到 `FindProxyForURL` 函數中的代理伺服器陣列選取邏輯之前。此函數通常用於不需通過代理伺服器陣列的本機請求。

   如果已經在 [Configure Proxy Array Member] 頁面上輸入自訂邏輯檔案，此資訊會自動寫入此欄位中。可視需要編輯自訂邏輯的檔案名稱，所做的變更也會傳輸至 [Configure Proxy Array Member] 頁面。
5. 在 [Default Route] 欄位中，輸入當陣列中的代理伺服器不存在時用戶端所要使用的路由。

   如果已經在 [Configure Proxy Array Member] 頁面上輸入預設路由，此資訊會自動寫入此欄位中。可視需要編輯預設路由，所做的變更也會傳輸至 [Configure Proxy Array Member] 頁面。
6. 按一下 [OK]。

7. 按一下 [Restart Required]。將顯示 [Apply Changes] 頁面。
8. 按一下 [Restart Proxy Server] 按鈕以套用變更。

使用 PAT 檔案自動產生 PAC 檔案

每次偵測到變更時使用 PAT 檔案自動產生 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。將顯示 [Configure Proxy Array Member] 頁面。
3. 選取 [Auto-generate PAC File] 核取方塊。
4. 如果要在 PAC 檔案中使用自訂邏輯，請在 [Custom Logic File] 欄位中輸入包含自訂邏輯的檔案名稱，此邏輯是您希望包含在所產生的 PAC 檔案中的邏輯。將把此邏輯插入到 `FindProxyFor URL` 函數中的代理伺服器陣列選取邏輯之前。

   如果已經在 [Configure Proxy Array] 頁面上輸入並儲存自訂邏輯檔案，此資訊會自動寫入此欄位中。可視需要編輯自訂邏輯檔案名稱，所做的變更也會傳輸至 [Configure Proxy Array] 頁面。
5. 在 [Default Route] 欄位中，輸入當陣列中的代理伺服器不存在時用戶端所要使用的路由。
6. 如果已經在 [Configure Proxy Array] 頁面上輸入並儲存預設路由，此資訊會自動寫入此欄位中。可視需要編輯預設路由，所做的變更也會傳輸至 [Configure Proxy Array] 頁面。
7. 按一下 [OK]。
8. 按一下 [Restart Required]。將顯示 [Apply Changes] 頁面。
9. 按一下 [Restart Proxy Server] 按鈕以套用變更。

透過父系代理伺服器陣列進行路由

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代理伺服器陣列路由，而不是直接存取遠端伺服器。

將代理伺服器或代理伺服器陣列成員配置爲透過父系代理伺服器陣列路由

1. 啓用父系代理伺服器陣列。如需關於啓用陣列的更多資訊，請參閱第 275 頁的「啓用代理伺服器陣列」。
2. 啓用透過父系代理伺服器陣列進行路由。如需關於啓用透過陣列進行路由的更多資訊，請參閱第 274 頁的「啓用透過代理伺服器陣列進行路由」。

3. 存取 Server Manager，然後按一下 [Caching] 標籤。
4. 按一下 [Configure Proxy Array Member] 連結。將顯示 [Configure Proxy Array Member] 頁面。
5. 在頁面的 [Parent Array] 區段的 [Poll Host] 欄位中輸入要針對 PAT 檔案進行輪詢的父系代理伺服器陣列中代理伺服器的主機名稱。此代理伺服器通常是父系代理伺服器陣列的主代理伺服器。
6. 在頁面的 [Parent Array] 區段的 [Port] 欄位中輸入要針對 PAT 檔案進行輪詢的父代理伺服器陣列中代理伺服器的連接埠號。
7. 在 [URL] 欄位中，輸入主代理伺服器上 PAT 檔案的 URL。如果已在主代理伺服器上建立 PAT 對映，則應將此對映輸入此 [URL] 欄位中。
8. 在表單的 [Parent Array] 區段的 [Headers File] 欄位中輸入檔案的完整路徑名稱，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]。將顯示 [Apply Changes] 頁面。
11. 按一下 [Restart Proxy Server] 按鈕以套用變更。

檢視父系代理伺服器陣列資訊

如果代理伺服器陣列透過父系代理伺服器陣列進行路由，則需要有關父系代理伺服器陣列成員的資訊。父系代理伺服器陣列會以 PAT 檔案的形式傳送此資訊。此 PAT 檔案內的資訊會顯示在 [View Parent Array Configuration] 頁面上。

檢視父系代理伺服器陣列資訊

1. 存取 Server Manager，然後按一下 [Caching] 標籤。
2. 按一下 [View Parent Array Configuration] 連結。將顯示 [View Parent Array Configuration] 頁面。
3. 檢視資訊。

第 13 章

透過代理伺服器篩選內容

本章描述如何篩選 URL，使您的代理伺服器或是禁止存取 URL，或是修改其傳回用戶端的 HTML 和 JavaScript 內容。本章還解釋如何根據用戶端正在使用的 Web 瀏覽器 (使用者代理程式) 透過代理伺服器來限定存取。

代理伺服器可讓您使用 URL 篩選檔案來確定伺服器支援哪些 URL。例如，您可以建立或購買包含要限定之 URL 的文字檔案，而無需手動鍵入要支援的 URL 萬用字元式樣。此功能可讓您建立一個 URL 檔案，您可在許多不同的代理伺服器上使用它。

您也可以根據 URL 的 MIME 類型來篩選 URL。例如，可以允許代理伺服器快取並傳送 HTML 和 GIF 檔案，但不讓它取得二進制或可執行檔，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

您可使用 URL 檔案來配置代理伺服器所擷取的內容。可以建立一份代理伺服器始終支援的 URL 之清單，以及一份代理伺服器始終都不支援的 URL 之清單。

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閱讀的內容，則可以建立一份准許兒童檢視的 URL 之清單。然後，可讓代理伺服器只擷取核准的 URL，如果用戶端嘗試前往不支援的 URL，則或是讓代理伺服器傳回預設的「Forbidden」訊息，或是建立自訂訊息，解釋爲何用戶端無法存取此 URL。

若要根據 URL 限定存取，您必須建立要允許或限定的 URL 之檔案。可透過 Server Manager 執行此作業。建立好檔案之後，即可設定限制條件。後面的小節將描述這些程序。

建立 URL 的篩選檔案

篩選檔案是包含 URL 清單的檔案。代理伺服器使用的篩選檔案是純文字檔，其 URL 行的式樣如下：

```
protocol://host:port/path/filename
```

可以在以下三個區段中分別使用常規表示式：`protocol`、`host:port` 與 `path/filename`。例如，如果您想要爲通往 netscape.com 網域的所有通訊協定建立一個 URL 式樣，應在檔案中增加以下一行：

```
.*://.*\.example\.com/.*
```

只有當您未指定連接埠號時，此行才起作用。如需有關常規表示式的更多資訊，請參閱第 319 頁的第 16 章 「管理範本和資源」中的「瞭解常規表示式」。

如果您要在不使用 Server Manager 的情況下建立自己的檔案，則應使用 [Server Manager] 頁面來建立一個空檔案，然後將您的文字內容增加至此檔案中，或是將此檔案替代成包含常規表示式的檔案。

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。將顯示 [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. 在下拉式清單右側的文字方塊中鍵入篩選檔案的名稱，然後按一下 [Create/Edit] 按鈕。將顯示 [Filter Editor] 頁面。

5. 使用 [Filter Content] 可捲動文字方塊輸入 URL 和 URL 的常規表示式。[Reset] 按鈕可清除此欄位中的所有文字。

   如需有關常規表示式的更多資訊，請參閱第 319 頁的第 16 章 「管理範本和資源」中的「瞭解常規表示式」。

6. 按一下 [OK]。

代理伺服器會建立檔案，並讓您返回 [Restrict URL Filter Access] 頁面。篩選檔案建立於 `proxy-server`*id*`/conf_bk` 目錄下。

設定篩選檔案的預設存取

一旦有了包含您想要使用的 URL 的篩選檔案，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。將顯示 [Restrict URL Filter Access] 頁面。
3. 選擇想要用於篩選器的範本。

   通常，您會想爲整個代理伺服器建立篩選檔案，但也可以爲 HTTP 建立一組篩選檔案，再爲 FTP 建立另一組篩選檔案。

4. 使用 [URL Filter To Allow] 清單來選擇篩選檔案，其中包含您希望代理伺服器支援的 URL。
5. 使用 [URL Filter To Deny] 清單來選擇篩選檔案，其中包含您希望代理伺服器拒絕存取的 URL。
6. 選擇您希望代理伺服器在用戶端請求拒絕的 URL 時傳回用戶端的文字內容。可以選擇下列兩個選項之一：
   - 可傳送代理伺服器產生的預設「Forbidden」回應。
   - 可傳送文字或內含自訂文字的 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]。將顯示 [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 4 可以檢查傳回用戶端的內容並以其他字串替代式樣 (如 URL)。可以配置的參數有兩個 — 來源字串和目標字串。Proxy Server 會尋找與來源字串相符的文字，並以目標字串中的文字加以替代。此功能僅可在反向代理模式下使用。

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。將顯示 [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 319 頁的第 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]。將顯示 [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。將顯示 [Set Content URL Rewriting] 頁面。
3. 按一下您要編輯之 URL 重寫式樣旁邊的 [Edit] 連結。
4. 按一下 [OK]。
5. 按一下 [Restart Required]。將顯示 [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。將顯示 [Set Content URL Rewriting] 頁面。
3. 按一下您要刪除之 URL 重寫式樣旁邊的 [Remove] 連結。按一下 [OK] 確認刪除。

4. 按一下 [Restart Required]。將顯示 [Apply Changes] 頁面。
5. 按一下 [Restart Proxy Server] 按鈕以套用變更。

限定特定 Web 瀏覽器的存取

可根據用戶端 Web 瀏覽器的類型和版本來限定對代理伺服器的存取。根據所有 Web 瀏覽器在發出請求時傳送至伺服器的 user-agent 標頭進行限制。

根據用戶端 Web 瀏覽器來限定對代理伺服器的存取

1. 存取 Server Manager，然後按一下 [Filters] 標籤。
2. 按一下 [Set User-Agent Restriction] 連結。將顯示 [Set User-Agent Restriction] 頁面。
3. 從下拉式清單中選取資源，或是鍵入與想要 Proxy Server 支援的瀏覽器的 user-agent 字串相符的常規表示式。如果您要指定一個以上的用戶端，請將常規表示式以括號括住，並使用 | 字元分隔多個項目。如需有關常規表示式的更多資訊，請參閱第 319 頁的第 16 章 「管理範本和資源」中的「瞭解常規表示式」。
4. 核取 [Allow Only User-Agents Matching] 選項。
5. 按一下 [OK]。
6. 按一下 [Restart Required]。將顯示 [Apply Changes] 頁面。
7. 按一下 [Restart Proxy Server] 按鈕以套用變更。

封鎖請求

您可能要根據上傳內容類型來封鎖檔案的上傳以及其他請求。

根據 MIME 類型封鎖請求

1. 存取 Server Manager，然後按一下 [Filters] 標籤。
2. 按一下 [Set Request Blocking] 連結。將顯示 [Set Request Blocking] 頁面。
3. 從下拉式清單中選取資源，或按一下 [Regular Expression] 按鈕，輸入常規表示式並按一下 [OK]。

4. 按一下所需請求封鎖類型對應的單選按鈕。選項如下：
   - [Disabled] — 停用請求封鎖功能
   - [Multipart MIME (File Upload)] — 封鎖所有檔案的上傳
   - [MIME Types Matching Regular Expression] — 封鎖符合所輸入之常規表示式的 MIME 類型請求。如需有關常規表示式的更多資訊，請參閱第 319 頁的第 16 章 「管理範本和資源」中的「瞭解常規表示式」。
5. 選擇是要封鎖所有用戶端的請求，還是封鎖符合您輸入之常規表示式的使用者代理程式請求。
6. 按一下想要封鎖其請求的方法對應的單選按鈕。選項包括：
   - [Any Method With Request Body] — 封鎖具有請求內文的所有請求，不論具體方法如何。
   - [only for:]
     [POST] — 封鎖使用 POST 方法的檔案上傳請求
     [PUT] — 封鎖使用 PUT 方法的檔案上傳請求
   - [Methods Matching Regular Expression] — 封鎖使用您輸入之方法的檔案上傳請求
7. 按一下 [OK]。
8. 按一下 [Restart Required]。將顯示 [Apply Changes] 頁面。
9. 按一下 [Restart Proxy Server] 按鈕以套用變更。

隱藏外送標頭

可透過配置代理伺服器，使其從請求移除外送標頭 (通常是基於安全性原因)。例如，您可能想要防止傳出 [From] 標頭，因爲它會透露使用者的電子郵件位址，或者您可能想要篩選掉 user-agent 標頭，讓外部伺服器無法判斷您的組織所使用的 Web 瀏覽器。在請求被轉寄至網際網路之前，您也可能想要移除只用於公司內部網路中的記錄或與用戶端相關的標頭。

此功能不會影響由代理伺服器本身特殊處理或產生的標頭，也不會影響讓通訊協定正常作業所必備的標頭 (例如 If-Modified-Since 和 Forwarded)。

雖然您無法阻止轉寄標頭自代理而產生，但這不屬於安全問題。遠端伺服器可根據連線偵測出正在進行連線的代理主機。在代理鏈接中，可由外部代理伺服器隱藏來自內部代理伺服器的轉寄標頭。當您不希望將內部代理伺服器或用戶端主機名稱透露給遠端伺服器時，建議您以這種方式設定您的伺服器。

隱藏外送標頭

1. 存取 Server Manager，然後按一下 [Filters] 標籤。
2. 按一下 [Suppress Outgoing Headers] 連結。將顯示 [Suppress Outgoing Headers] 頁面。
3. 在 [Suppress Headers] 文字方塊中輸入一份想要隱藏的請求標頭清單，各標頭以逗號分隔。例如，若要隱藏 [From] 和 [User-Agent] 標頭，請輸入 **`from,user-agent`**。您輸入的標頭是不區分大小寫的。如需有關常規表示式的更多資訊，請參閱第 319 頁的第 16 章 「管理範本和資源」中的 「瞭解常規表示式」。
4. 按一下 [Restart Required]。將顯示 [Apply Changes] 頁面。
5. 按一下 [Restart Proxy Server] 按鈕以套用變更。

依 MIME 類型篩選

您可將代理伺服器配置爲封鎖與 MIME 類型相符的特定檔案。例如，您可透過設定代理伺服器，使其封鎖任何可執行檔或二進位檔案，這樣使用您的代理伺服器的任何用戶端都不會下載可能存在的電腦病毒。

如果需要代理伺服器支援新的 MIME 類型，請在 [Server Manager] 中選擇 [Preferences] > [Create/Edit MIME Types]，然後增加類型。如需有關建立 MIME 類型的更多資訊，請參閱第 128 頁的 「建立新的 MIME 類型」。

您可將篩選 MIME 類型的方式與範本結合使用，這樣對於特定 URL 將只封鎖特定的 MIME 類型。例如，您可封鎖來自 `.edu` 網域內任何電腦的可執行檔。

依 MIME 類型篩選

1. 存取 Server Manager，然後按一下 [Filters] 標籤。
2. 按一下 [Set MIME Types] 連結。將顯示 [Set MIME Filters] 頁面。
3. 選擇您要用來篩選 MIME 類型的範本，或確定您正在編輯整個伺服器。
4. 在 [Current filter] 文字方塊中，您可輸入與要封鎖之 MIME 類型相符的常規表示式。

   例如，若要篩選掉所有應用程式，您可鍵入 **`application/.*`** 做爲常規表示式。這比針對每個應用程式類型來檢查每一 MIME 類型速度更快。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 319 頁的第 16 章 「管理範本和資源」中的 「瞭解常規表示式」。

5. 核取您要篩選的 MIME 類型。當用戶端嘗試存取被封鎖的檔案時，代理伺服器會傳回「403 Forbidden」訊息。
6. 按一下 [OK]。
7. 按一下 [Restart Required]。將顯示 [Apply Changes] 頁面。
8. 按一下 [Restart Proxy Server] 按鈕以套用變更。

依 HTML 標記篩選

代理伺服器可讓您指定要在將檔案傳至用戶端之前篩選掉的 HTML 標記。這樣可以篩選掉 HTML 檔案中內嵌的物件，例如 Java applets 和 JavaScript。若要篩選 HTML 標記，需指定開頭和結尾 HTML 標記。然後，代理伺服器會在將檔案傳送至用戶端之前，以空白替換那些標記中的所有文字和物件。

備註	如果將代理伺服器配置爲快取原始 (未經編輯的) 檔案，則代理伺服器會在快取記憶體內儲存此資源。

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。將顯示 [Set HTML Tag Filters] 頁面。
3. 選擇您要修改的範本。您可以選擇 HTTP，或是選擇僅指定特定 URL (例如來自於 .edu 網域內主機之 URL) 的範本。
4. 核取您要篩選的任何預設 HTML 標記對應的篩選器方塊。預設標記如下：
   - APPLET 通常包圍住 Java applet。
   - SCRIPT 表示 JavaScript 代碼的開頭。
   - IMG 指定內嵌的影像檔。
5. 您可輸入想要篩選的任何 HTML 標記。鍵入開頭和結尾的 HTML 標記。

   例如，若要篩選掉表單，可在 [Start Tag] 方塊中鍵入 **FORM** (HTML 標記不區分大小寫)，在 [End Tag] 方塊中鍵入 /**FORM**。如果您要篩選的標記沒有結尾標記 (例如 OBJECT 和 IMG)，則可讓 [End Tag] 方塊保留空白。
6. 按一下 [OK]。
7. 按一下 [Restart Required]。將顯示 [Apply Changes] 頁面。

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

爲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，還可以提高內容量，而不會增加硬體消耗。內容壓縮縮短了內容的下載時間，使需要撥號與高流量連線的使用者明顯受益。

透過內容壓縮，Proxy Server 可傳送經過壓縮的資料，並指導瀏覽器即時解壓縮資料，這樣便可減少資料傳送量，並加快頁面顯示速度。

將伺服器配置爲依需要壓縮內容

您可將 Proxy Server 配置爲即時地壓縮傳輸資料。動態產生的 HTML 頁面只有在使用者請求時才會出現。

將伺服器配置爲依需要壓縮內容

1. 存取 Server Manager，然後按一下 [Filters] 標籤。
2. 按一下 [Compress Content on Demand] 連結。將顯示 [Compress Content on Demand] 頁面。
3. 從下拉式清單中選取資源，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 319 頁的第 16 章 「管理範本和資源」中的「瞭解常規表示式」。
4. 指定以下資訊：
   - **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。選擇 yes 或 no。如果設定爲 yes，則當選取經過壓縮的檔案版本時，總是會插入 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，此值設定爲 yes。
   - **Fragment Size。**指定壓縮程式庫 (`zlib`) 用於控制每次壓縮內容量的記憶體分段大小 (以位元組爲單位)。預設值爲 8096。
   - **Compression Level。**指定壓縮的層級。選擇 1 至 9 之間的值。數值爲 1 時速度最快；數值爲 9 時壓縮效果最佳。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]。將顯示 [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

本章描述如何使用 Proxy Server 做爲反向代理伺服器。反向代理伺服器是代理伺服器針對特定替代用法時的名稱。它可以用於防火牆之外，充當外部用戶端的安全內容伺服器，以避免有人在未受監視的情況下從您公司之外直接存取伺服器的資料。它還可以用來進行複製；也就是說，可以在高用量伺服器之前附加多個代理伺服器，以實現負載平衡。本章描述 Proxy Server 在防火牆內外的替代用法。

本章包含下列小節：

反向代理的工作方式

反向代理有兩個模型。一個模型利用 Proxy Server 的安全功能來處理作業事件，而另一個模型則利用其快取功能在高用量伺服器上提供負載平衡。這兩種模型與常規的代理伺服器用法不同的是它們不會嚴格地在防火牆上作業。

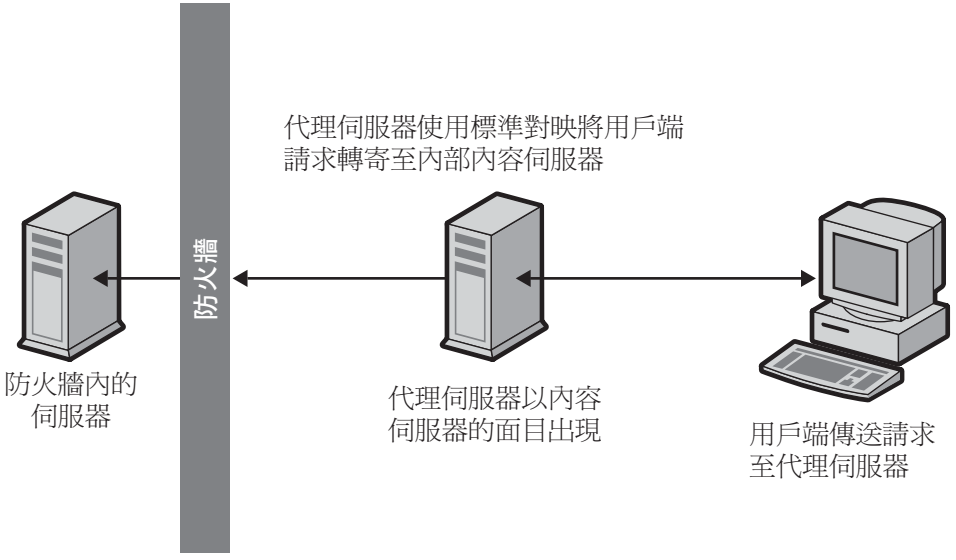
代理伺服器是伺服器的替身

若某台內容伺服器帶有必須確保安全的敏感資訊，例如信用卡號碼的資料庫，則可以在防火牆之外設定一台代理伺服器做爲內容伺服器的替身。當外部用戶端嘗試存取內容伺服器時，其會被傳送至代理伺服器。真正的內容安全地儲存在防火牆之內的內容伺服器中。代理伺服器位於防火牆之外，對於用戶端來說就好像內容伺服器一樣。

當用戶端向您的站點發出請求時，請求會進入代理伺服器中。之後，代理伺服器會透過防火牆的特定通道將用戶端的請求傳送給內容伺服器。內容伺服器再透過此通道將結果傳送回代理伺服器。代理伺服器將擷取的資訊傳送給用戶端，好像代理伺服器就是真正的內容伺服器一樣 (請參閱圖 14-1)。若內容伺服器傳回錯誤訊息，則代理伺服器可以截取訊息，並在將訊息傳送至用戶端之前變更列於標頭中的所有 URL。這樣可防止外部用戶端取得內部內容伺服器的重新導向 URL。

透過這種方法，代理伺服器在安全的資料庫與可能的惡意攻擊之間設立了一道額外的屏障。即使攻擊成功 (這幾乎不太可能)，攻擊者充其量僅能存取一個作業事件所涉及的資訊，而不能存取整個資料庫。未授權的使用者無法進入真正的內容伺服器，因爲防火牆通道僅允許代理伺服器存取。

圖 14-1 反向代理伺服器看起來好像真正的內容伺服器



可以透過配置防火牆路由器，來允許特定連接埠上的特定伺服器 (在此情況中，代理伺服器位於其指派的連接埠上) 經由防火牆進行存取，而禁止其他機器進出。

安全反向代理

當代理伺服器與另一台機器之間的一個或多個連線使用安全通訊端層 (SSL) 協定來加密資料時，會發生安全反向代理。

安全反向代理有許多用途：

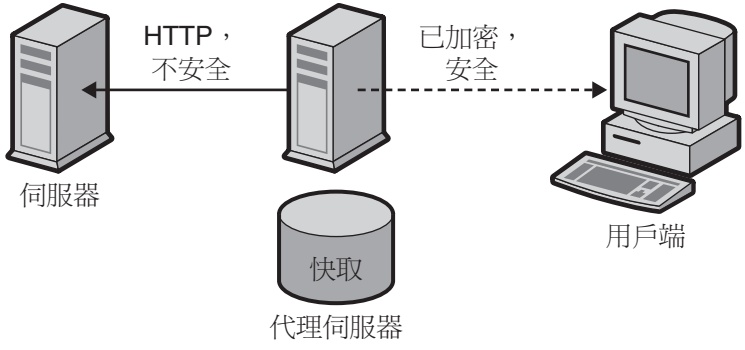
- 可以提供從防火牆外之代理伺服器至防火牆內之安全內容伺服器之間的一個加密連線。
- 可以允許用戶端安全連線至代理伺服器，協助資訊的安全傳輸 (例如信用卡號碼)。

由於加密資料會增加系統經常性耗用，所以安全反向代理會降低每個安全連線的速度。然而，因爲 SSL 提供了快取機制，兩連線方可以重複使用之前協商的安全性參數，從而大幅減少之後連線的經常性耗用。

配置安全反向代理伺服器的方法有三種：

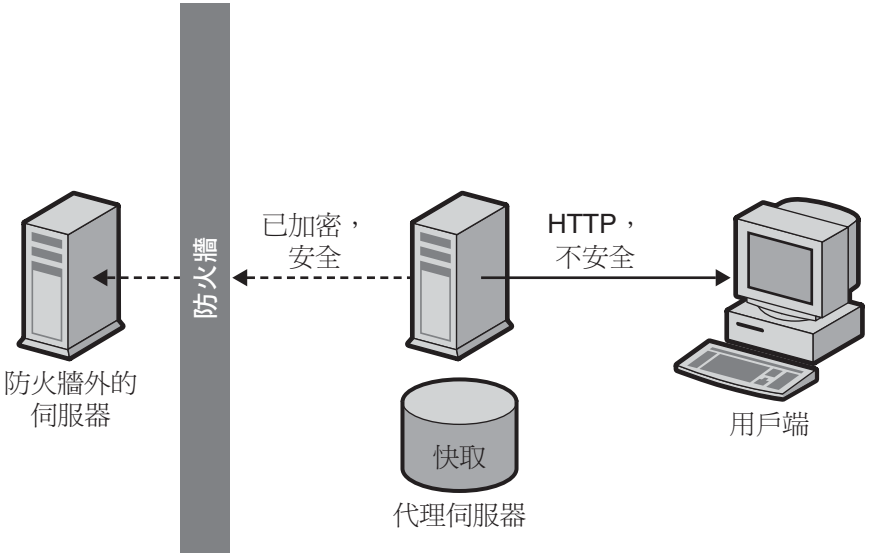
用戶端安全連線到代理伺服器。若未授權的使用者很少或幾乎沒有機會存取在代理伺服器與內容伺服器之間交換的資訊，則此分析藍本將是很有效的方式 (請參閱圖 14-2)。

圖 14-2 用戶端安全連線到代理伺服器



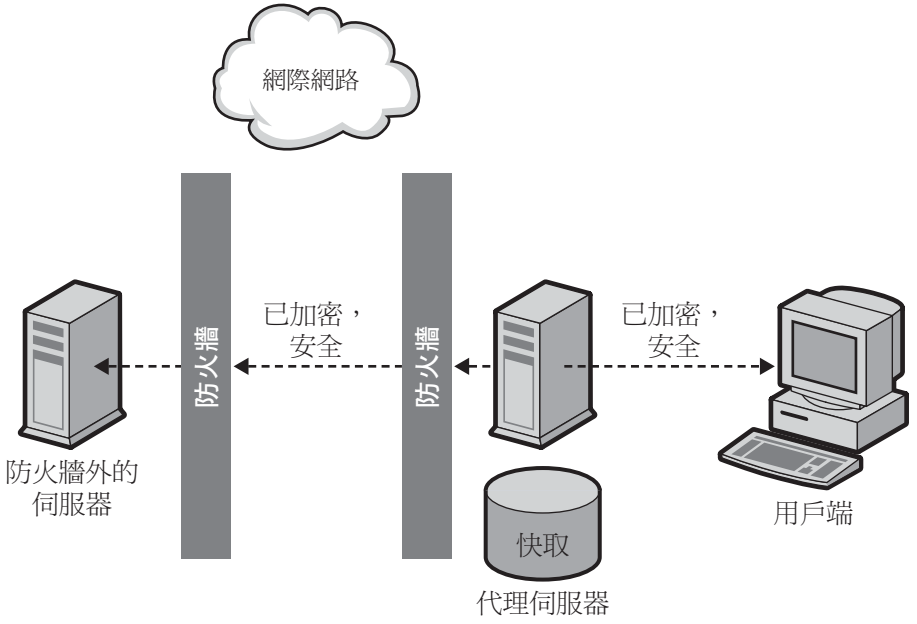
代理伺服器安全連線到內容伺服器。若用戶端位於防火牆之內而內容伺服器位於防火牆之外，則此分析藍本將是很有效的方式。在此分析藍本中，代理伺服器可以做爲站點之間的安全通道 (請參閱圖 14-3)。

圖 14-3 代理伺服器安全連線到內容伺服器



- **用戶端安全連線到代理伺服器且代理伺服器安全連線到內容伺服器**。若在伺服器、代理伺服器及用戶端之間交換的資訊必須是安全的，則此分析藍本將是很有效的方式。在此分析藍本中，代理伺服器做爲站點之間的安全通道，並透過用戶端認證進一步提高安全性 (請參閱圖 14-4)。

圖 14-4 用戶端安全連線到代理伺服器且代理伺服器安全連線到內容伺服器



如需有關如何設定每種配置的資訊，請參閱第 295 頁的「設定反向代理伺服器」。

除了 SSL 之外，代理伺服器還可以使用用戶端認證，這就要求向代理伺服器發出請求的電腦提供憑證 (或身份識別表) 來驗證其身份。

用於負載平衡的代理

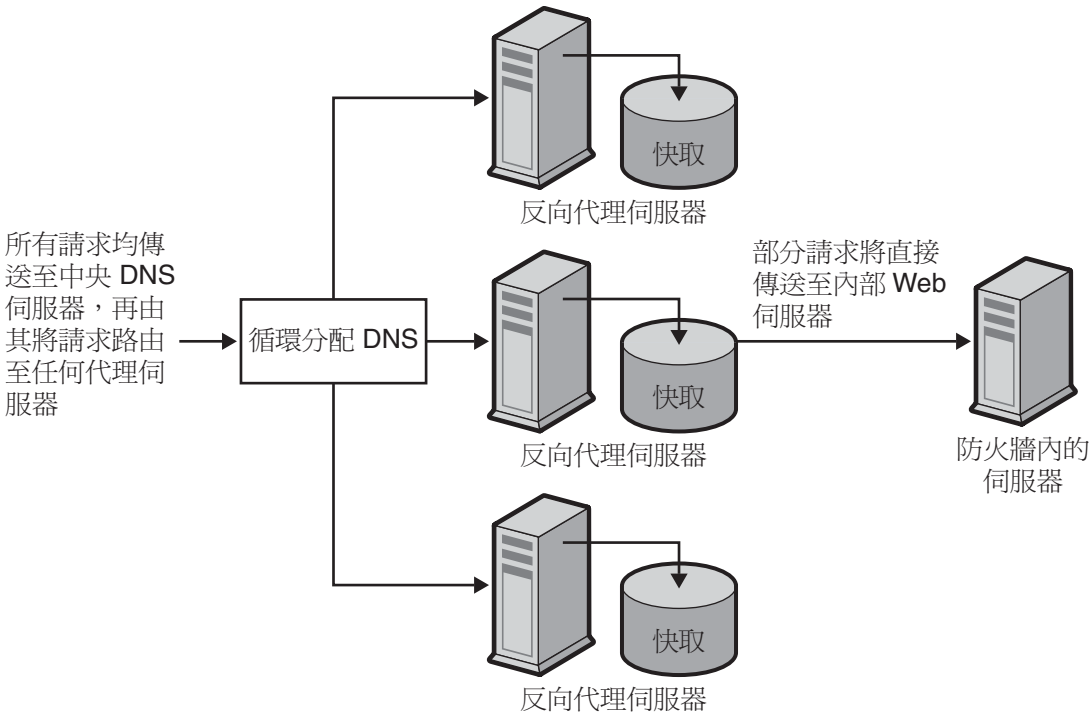
您可以在組織中使用多個代理伺服器以平衡 Web 伺服器之間的網路負載。此模型可讓您利用代理伺服器的快取功能建立伺服器池，來實現負載平衡。在此情況下，代理伺服器可以位於防火牆的任意一側。若 Web 伺服器每天接收大量的請求，則可以使用代理伺服器來承擔 Web 伺服器的負載，使網路存取更加有效率。

代理伺服器相當於用戶端請求與真實伺服器之間的媒介。代理伺服器會快取請求的文件。若代理伺服器有多個，DNS 可以採用「循環」選擇其 IP 位址的方式來隨機路由請求。用戶端每次會使用相同的 URL，但請求採用的路由每次可能會經過不同的代理伺服器。

使用多個代理伺服器來處理高用量內容伺服器的請求之優點在於：伺服器可以處理比單獨使用時更繁重的負載，而且會更有效率。在代理伺服器第一次從內容伺服器擷取文件的初始啓動期間之後，內容伺服器的請求數將會大幅減少。

僅有 CGI 請求與偶而發生的新請求必須以各種方式到達內容伺服器。其餘的請求可以由代理伺服器處理。這裡舉個例子。假設向伺服器發出的請求中有 90% 都不是 CGI 請求 (表示其可被快取)，內容伺服器每天會接收 2 百萬個符合項目。在此情況下，若連接三個反向代理伺服器，且每個伺服器每天可處理 2 百萬個符合項目，那麼每天總共可以處理 6 百萬個符合項目。有 10% 的請求到達內容伺服器，總共可達每天每個代理伺服器約處理 200,000 個符合項目，總共僅有 600,000 個，這大大提高了效率。符合項目的數目可以從 2 百萬個增至 6 百萬個，而內容伺服器的負載可以相應地從 2 百萬個減至六十萬個。實際的結果要視具體情況而定。

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，必須擁有兩個對映：標準對映與反向對映。

- 標準對映將請求重新導向至內容伺服器。當用戶端從代理伺服器請求文件時，代理伺服器需要標準對映來告知要到何處取得真實的文件。

注意 不應將提供自動配置檔案的代理伺服器與反向代理伺服器一起使用。這是因爲代理伺服器可能會傳回錯誤的結果。

- 反向對映可以爲來自內容伺服器的重定向產生代理伺服器陷阱。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，若用戶端請求的文件已移動或找不到，則內容伺服器將傳回訊息給用戶端，說明它無法在請求的 URL 處找到文件。在傳回的訊息中，內容伺服器會增加 HTTP 標頭，列出用於取得已移動的檔案的 URL。爲了維持內部內容伺服器的私密性，代理伺服器可以使用反向對映來重新導向 URL。

假設有一個名爲 `http://http.site.com/` 的 Web 伺服器，且要爲其設定反向代理伺服器。可以呼叫反向代理伺服器 `http://proxy.site.com/`。

應建立**標準**對映與**反向**對映，方法如下：

1. 存取 Server Manager，然後按一下 [URLs] 標籤。
2. 按一下 [Create Mapping] 連結。將顯示 [Create Mapping] 頁面。
3. 在出現的頁面中，輸入一個對映的資訊。例如：

   標準對映：

   來源前綴：`http://proxy.site.com`

   來源目標：`http://http.site.com/`

4. 按一下 [OK]。返回頁面並建立第二個對映：

   反向對映：

   來源前綴：`http://http.site.com/`

   來源目標：`http://proxy.site.com/`

5. 若要進行變更，請按一下 [OK]。

   按一下 [OK] 按鈕之後，代理伺服器將會增加一個或多個額外的對映。若要查看對映，請按一下名爲 [View/Edit Mappings] 的連結。額外的對映應爲以下格式：

   from: /

   to: `http://http.site.com/`

   這些額外的自動對映針對以一般伺服器形式連接至反向代理伺服器的使用者。第一個對映用於擷取以標準代理伺服器形式連線至反向代理伺服器的使用者。根據設定，通常只有第二個對映是必需的，但同時擁有這兩者並不會使代理伺服器出現問題。

備註 若 Web 伺服器有數個 DNS 別名，則每個別名應該有一個對應的標準對應。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 應用程式仍將在原始伺服器上執行，代理伺服器本身不執行 CGI 應用程式。然而，若 CGI 程序檔指示可以快取結果 (藉由發出 Last-modified 或 Expires 標頭來暗示存活時間不爲零)，則代理伺服器將快取結果。

注意 當爲 Web 伺服器創作內容時，請記住，反向代理伺服器也會爲這些內容提供服務，所以指向 Web 伺服器上檔案的所有連結都應是相對連結。HTML 檔案中一定**不可以**有主機名稱參照，也就是說，所有連結是針對頁面的：

```
/abc/def
```

而不應是完整合格的主機名稱，例如：

```
http://http.site.com/abc/def
```

設定安全反向代理伺服器

設定安全反向代理之前，應該熟悉數位憑證、憑證授權單位與認證。

設定安全反向代理伺服器的程序與設定不安全反向代理伺服器幾乎一樣。唯一的不同點在於您必須指定 HTTPS 做爲加密檔案所使用的協定。

以下說明內容將解釋如何根據您選擇的配置分析藍本設定安全反向代理伺服器。爲了示範如何設定對映，這些說明內容假設您擁有一個名爲 `http.site.com` 的 Web 伺服器，而且您希望設定一個名爲 `proxy.site.com` 的安全反向代理伺服器。執行這些步驟時，應使用 Web 伺服器與代理伺服器的名稱代替說明內容中使用的範例名稱。

用戶端安全連線到代理伺服器

1. 存取 Server Manager，然後按一下 [URLs] 標籤。
2. 按一下 [Create Mapping] 連結。將顯示 [Create Mapping] 頁面。
3. 在出現的頁面中，使用以下方法設定標準對映與反向對映：

   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。

   若要查看剛建立的對映，請按一下名爲 [View/Edit Mappings] 的連結。

備註 只有在代理伺服器以安全模式執行時，此配置才有效。換言之，必須啓用加密且必須在指令行中重新啓動代理伺服器。若要在指令行重新啓動代理伺服器，則請進入代理伺服器目錄並鍵入 **./start**。

代理伺服器安全連線到內容伺服器

1. 存取 Server Manager，然後按一下 [URLs] 標籤。
2. 按一下 [Create Mapping] 連結。將顯示 [Create Mapping] 頁面。
3. 在出現的頁面中，使用以下方法設定標準對映與反向對映：

   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。若要查看剛建立的對映，請按一下名爲 [View/Edit Mappings] 的連結。

備註 只有在內容伺服器以安全模式執行時，此配置才有效。

用戶端安全連線到代理伺服器且代理伺服器安全連線到內容伺服器

1. 存取 Server Manager，然後按一下 [URLs] 標籤。
2. 按一下 [Create Mapping] 連結。將顯示 [Create Mapping] 頁面。

3. 在出現的頁面中，設定如下的標準對映與反向對映：

   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。若要查看剛建立的對映，請按一下名爲 [View/Edit Mappings] 的連結。

備註 只有在代理伺服器和內容伺服器以安全模式執行時，此配置才有效。換言之，對於代理伺服器，必須啓用加密且必須在指令行中重新啓動代理伺服器。若要在指令行重新啓動代理伺服器，則請進入代理伺服器目錄並鍵入 **`./restart`**。

反向代理伺服器中的虛擬多方主控

虛擬多方主控功能使原始伺服器或這裡的反向代理伺服器能夠回應多個 DNS 別名，就像在這些位址中的每一位址上都安裝了一台不同的伺服器一樣。舉例來說，您可使用下列 DNS 主機名稱：

- `www`
- `specs`
- `phones`

可將其中的每一項對映至同一 IP 位址 (反向代理伺服器的 IP 位址)。然後您可讓反向代理伺服器根據存取它時所使用的 DNS 名稱發揮不同的功能。

虛擬多方主控功能還可讓您主控單台反向代理伺服器上多個不同的 *domains*。例如：

- `www.domain-1.com`
- `www.domain-2.com`
- `www.domain-3.com`

請注意，您可以將多個本機主機名稱與多個網域全都組合在一個代理伺服器中：

- www
- specs
- phones
- www.domain-1.com
- www.domain-2.com
- www.domain-3.com

本節包含以下主題：

- 虛擬多方主控功能的詳細資訊
- 虛擬多方主控的重要注意事項

虛擬多方主控功能的詳細資訊

爲使虛擬多方主控功能工作，首先要指定 DNS 主機與網域名稱 (或別名)，然後給出一個目標 URL 前綴，傳送給此主機名稱的請求將導向到此 URL。舉例來說，您可以有兩個對映：

- engr.domain.com -> http://int-engr.domain.com
- mktg.domain.com -> http://int-mktg.domain.com

對映並不一定要從根到根；您可以在目標 URL 中指定其他的 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，您可使用：

- www.domain-1.com -> http://int-engr.domain.com
- www.domain-2.com -> http://int-mktg.domain.com

系統將查看 HTTP "Host:" 標頭，並根據標頭選擇相符的虛擬多方主控對映。若沒有相符的多方主控對映，伺服器將按對映在配置檔中的出現順序繼續查看其他對映，或者若找不到任何符合的項目，伺服器將不執行對映。若沒有符合的項目，代理伺服器一般將以「Proxy denies fulfilling the request」回應。

配置虛擬多方主控

1. 存取 Server Manager，然後按一下 [URLs] 標籤。
2. 按一下 [Configure Virtual Multihosting] 連結。將顯示 [Configure Virtual Multihosting] 頁面。
3. 在 [Source Hostname (alias)] 欄位中，指定此對映所應適用的本機主機名稱 (或 DNS 別名)。
4. 在 [Source Domain Name] 欄位中，輸入此對映所應適用的本機網域名稱。一般而言，這是您自己網路的網域名稱，除非您想要多方主控多個不同的 DNS 網域。
5. 在 [Destination URL Prefix] 欄位中，輸入目標 URL 前綴，當主機和網域名稱符合上述規格時，請求將被導向到此 URL。
6. 若要使用範本，從 [Use This Template] 下拉式清單中選取範本名稱，若不想套用範本，則保持 [NONE] 值不變。
7. 按一下 [OK]。
8. 按一下 [Restart Required]。將顯示 [Apply Changes] 頁面。
9. 按一下 [Restart Proxy Server] 按鈕以套用變更。

   爲要建立的每個虛擬多方主控對映重複以上步驟。

所有虛擬多方主控對映都將出現在 [Configure Virtual Multihosting] 頁面的底部。請注意，[Source Hostname (alias)] 和 [Source Domain Name] 欄位會與代理伺服器的連接埠號一起合併成一個常規表示式，用於比對 [Host:] 標頭。

例如，如果使用主機名稱 www、網域名稱 example.com 以及連接埠號 8080，將顯示下列常規表示式：

```
www(|.example.com)(|:8080)
```

這將確保比對出使用者可能鍵入或用戶端可能傳送的下列所有可能的組合字串 (某些用戶端軟體可能會忽略連接埠號，即使連接埠號不是 80 形式時亦是如此，因爲伺服器顯然是知道自己所偵聽的連接埠號的)：

- `www`
- `www:8080`
- `www.example.com`
- `www.example.com:8080`

虛擬多方主控的重要注意事項

在配置反向代理伺服器對映之前，必須停用用戶端自動配置功能。這樣做將不會導致任何問題，因爲用戶端自動配置功能用於正向代理伺服器作業，而非反向代理伺服器。

[Virtual Multihosting] 功能將建立自動反向對映。換句話說，請不要爲使用 [Virtual Multihosting] 頁面輸入的對映建立反向對映。

應使用 `obj.conf` 中的 `virt-map` 函數指定虛擬對映。

將依照在 obj.conf 配置檔案中指定的順序比對虛擬對映。若在虛擬對映之前有標準對映、反向對映、常規表示式對映或用戶端自動配置對映，則將首先套用這些對映。同樣，若在虛擬對映中未找到符合的項目，會繼續轉換 `obj.conf` 中虛擬對映區段之後的下一個對映。

若代理伺服器的連接埠號發生變更，則需要重新建立虛擬多方主控對映，因爲他們現在的連接埠號碼是錯誤的。

第 15 章

使用 SOCKS

本章描述如何配置與使用 Sun Java System Web Proxy Server 附帶的 SOCKS 伺服器。Proxy Server 支援 SOCKS 版本 4 和 5。

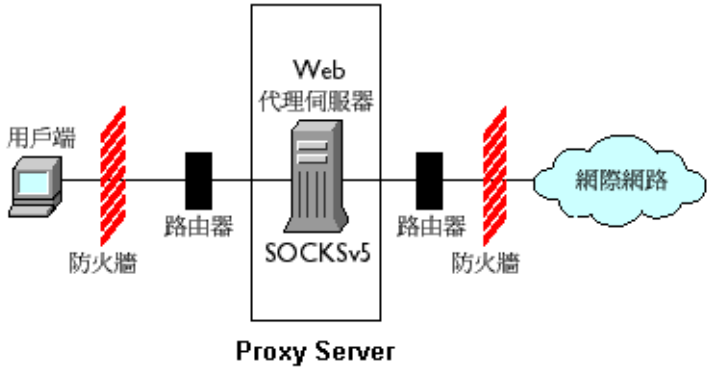
本章包含下列小節：

關於 SOCKS

SOCKS 是一種網路代理協定，可將來自 SOCKS 伺服器相對端主機的連線請求重新導向，並能讓某一端上的主機取得對另一端上主機的完全存取權限，而不需要其具有直接 IP 連線能力。SOCKS 通常用來作爲網路防火牆，讓 SOCKS 伺服器後面的主機具有對網際網路的完全存取權限，同時亦可防止網際網路中的未經授權者存取內部主機。

SOCKS 伺服器是一個常規防火牆常駐程式，它以點對點方式控制透過防火牆的存取。SOCKS 伺服器可對請求進行認證與授權、建立代理伺服器連線及中繼資料。SOCKS 伺服器是在網路層級而不是在應用程式層級運作，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，因此可以用來傳送 Proxy Server 不支援的那些協定 (例如 Telnet)。

圖 15-1 SOCKS 伺服器在網路中的位置



使用隨附的 SOCKS v5 Server

Sun Java System Web Proxy Server 附帶自己的 SOCKS 常駐程式，可識別其他 SOCKS 常駐程式所使用的標準 `socks5.conf` 檔案格式。Proxy Server 可使用此常駐程式路由請求，也可以脫離 Proxy Server 單獨執行來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 314 頁的「配置路由項目」。

Proxy Server 附帶的 SOCKS 常駐程式依預設爲停用狀態，可以從 Server Manager 介面的 [SOCKS] 標籤或是從指令行啓用此常駐程式。如需更多資訊，請參閱第 307 頁的「啓動與停止 SOCKS v5 Server」。

備註	在 Proxy Server 4 中，SOCKS 常駐程式的名稱已經從 `ns-sockd` 變更爲 `sockd`。

下列爲使用 Proxy Server 附帶的 SOCKS 伺服器時必須採取的高階步驟：

1. 配置 SOCKS 伺服器 (請參閱第 307 頁的「配置 SOCKS v5 Server」)。
2. 如果 SOCKS 伺服器將在具有多個介面的電腦中執行，請建立 SOCKS 路由項目 (請參閱第 314 頁的「配置路由項目」)。
3. 建立認證項目 (請參閱第 309 頁的「配置 SOCKS v5 認證項目」)。
4. 建立連線項目 (請參閱第 311 頁的「配置 SOCKS v5 連線項目」)。
5. 啓用 SOCKS 伺服器 (請參閱第 307 頁的「啓動與停止 SOCKS v5 Server」)。

關於 socks5.conf

Sun Java System Web Proxy Server 使用 `socks5.conf` 檔案控制對 SOCKS 伺服器及其服務的存取。其中的每一行定義 Proxy Server 接收到與此行相符的請求時將執行的動作。在 Server Manager 中做出的選擇會寫入 `socks5.conf` 中。也可以手動編輯此檔案。`socks5.conf` 檔案位於如下的安裝根目錄 (*server_root*)：

server_root/`proxy-`*serverid*/`config` 目錄

本節提供關於 `socks5.conf` 的一般資訊。如需有關檔案及其指令和語法的詳細資訊，請參閱「Proxy Server Configuration File Reference」。

認證

可以將 SOCKS 常駐程式配置爲需要認證才能使用其服務。認證的依據是連線用戶端的主機名稱和連接埠。如果選擇需要使用者名稱與密碼，則會根據 `socks5.conf` 檔案所參照的使用者名稱與密碼檔案來認證此資訊。如果提供的使用者名稱與密碼與密碼檔案中的項目不符，存取會遭到拒絕。密碼檔案中使用者名稱與密碼的格式爲 *username password*，其中使用者名稱和密碼以空格隔開。也可以禁止使用者。如果需要使用者名稱與密碼認證，必須將 `SOCKS5_PWDFILE` 指令增加至 `socks5.conf` 中。如需有關指令及其語法的更多資訊，請參閱 Proxy Server 的「 Configuration File Reference」中的 `socks5.conf` 區段。

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。對指令的處理順序是依照它們在配置檔案中出現的順序。對於不符合任何允許指令的請求，將拒絕其存取。

記錄

SOCKS 常駐程式會將錯誤與存取訊息都記錄在 SOCKS 記錄檔中。記錄檔的位置及記錄類型可以在 `socks5.conf` 中指定。

SOCKS 常駐程式每個小時會產生一個統計項目，提供常駐程式的統計資料。

調校

可以使用 `socks5.conf` 檔案來確定 SOCKS 伺服器所使用的工作者與接受執行緒的數目。這些數量會影響 SOCKS 伺服器的效能。

如需有關工作者與接受執行緒設定及其對效能影響的更多資訊，請參閱以下一節的相關段落：第 307 頁的「配置 SOCKS v5 Server」。

啓動與停止 SOCKS v5 Server

可以從 Server Manager 或是從指令行啓動與停止 SOCKS 伺服器。

從 Server Manager 啓動與停止 SOCKS 伺服器

1. 存取伺服器實例的 Server Manager，然後按一下 [SOCKS] 標籤。
2. 按一下 [Start/Stop SOCKS Server] 連結。
3. 啓動或停止 SOCKS 伺服器。

從指令行啓動與停止 SOCKS 伺服器

執行 *server_root*/proxy-*serverid* 目錄中的程序檔，其中 *server_root* 爲安裝根目錄：

- `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 Server

配置 SOCKS 伺服器

1. 存取伺服器實例的 Server Manager，然後按一下 [SOCKS] 標籤。
2. 按一下 [Configure SOCKS v5] 連結。
3. 在 [SOCKS Port] 欄位中，輸入 SOCKS 伺服器將會偵聽的連接埠號 (依預設爲 1080)。
4. 選取想要使用的 SOCKS 選項。下列選項可供選用：
   - **Disable Reverse DNS Lookup。**停用 SOCKS 伺服器的反向 DNS 查找功能。反向 DNS 會將 IP 位址轉換爲主機名稱。停用反向 DNS 查找功能可節省網路資源。此功能依預設爲停用狀態 (也就是說，依預設 [Disable Reverse DNS Lookup] 核取方塊爲選取狀態)。如果反向 DNS 查找功能爲停用狀態，而請求的是含主機名稱的 URL，則伺服器將不會把主機名稱對應至 IP 位址。如果反向 DNS 查找功能爲啓用狀態，伺服器將會執行對映，SOCKS 記錄檔中將會增加項目，列出 DNS 轉換。
   - **Use Client-specific Bind Port。**可讓用戶端在 BIND 請求中指定連接埠。如果停用此選項，SOCKS 會忽略用戶端的請求連接埠並指定隨機連接埠。依預設此參數爲停用狀態。

- **Allow Wildcard As Bind IP Address。**可讓用戶端在 BIND 請求中指定全部爲零 (0.0.0.0) 的 IP 位址，表示任何 IP 位址皆可連線。若停用此選項，用戶端必須指定將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。依預設此參數爲停用狀態。
- **Quench Updates。**每小時停用自動統計檔案寫入一次。如果停用此選項，會在每次請求時執行寫入 (請參閱第 306 頁的「記錄」)。

備註 [Quench Updates] 元素會顯示在使用者介面中，但在 Proxy Server 4 這個版本中沒有實作。

5. 在 [Log File] 欄位中，輸入 SOCKS 記錄檔的完整路徑名稱。預設路徑爲 *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 可讓 SOCKS 伺服器判定用戶端的使用者名稱。一般而言，只有在用戶端採用某種 UNIX 風格時此功能才有效。下列選項可供選用
   - **Don't Ask。**絕不使用 ident 判定用戶端的使用者名稱。此爲建議與預設設定。
   - **Ask But Don't Require。**詢問所有用戶端的使用者名稱，但並不需要此名稱。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 伺服器應使用的工作者與接受執行緒的數目 (這些數目會影響 SOCKS 伺服器的效能)，然後按一下 [OK]：
   - **Number Of Worker Threads。**預設值爲 40。如果 SOCKS 伺服器速度太慢，請增加工作者執行緒的數量。如果它不穩定，請減少數量。在變更此數量時，請從預設數量開始並視需要進行增減。工作者執行緒的一般數量介於 10 到 150 之間。最大絕對值爲 512，但數量超過 150 後容易造成浪費和不穩定。
   - **Number Of Posted Accepts。**預設值爲 1。如果 SOCKS 伺服器斷線，請增加接受執行緒的數量。如果它不穩定，請減少數量。在變更此數量時，請從預設數量開始並視需要進行增減。接受執行緒的一般數量介於 1 到 10 之間。最大絕對值爲 512，但數量超過 60 後容易造成浪費和不穩定。這是一項非常重要的設定。如果 SOCKS 伺服器欠載同時連線中斷，並因而使得請求失敗，請調準此設定。

配置 SOCKS v5 認證項目

SOCKS 認證項目確定 SOCKS 常駐程式應接受來自哪些主機的連線及應使用哪些類型的認證來認證這些主機。

本節包含以下主題：

建立認證項目

建立 SOCKS 認證項目

1. 存取伺服器實例的 Server Manager，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，輸入 SOCKS 伺服器將要認證之主機的 IP 位址或主機名稱。如果輸入 IP 位址，請在位址之後加上正斜線以及要套用於內送 IP 位址的遮罩。SOCKS 伺服器會將此遮罩套用於 IP 位址，以確定其是否爲有效主機。請勿在主機遮罩項目中包含空格。如果不輸入主機遮罩，認證項目將會套用於所有主機。

   例如，可在 [host mask] 欄位中輸入 155.25.0.0/255.255.0.0。如果主機的 IP 位址爲 155.25.3.5，SOCKS 伺服器會將遮罩套用於此 IP 位址，然後判定主機的 IP 位址符合認證記錄所適用的 IP 位址 (155.25.0.0)。
5. 在 [Port Range] 欄位中輸入 SOCKS 伺服器將會認證之主機的連接埠。請勿在連接埠範圍項目中包含空格。如果不輸入連接埠範圍，認證項目會套用於所有連接埠。

   可使用方括號 [ ] 來包括範圍兩端的連接埠，也可以使用括弧 ( ) 將它們排除在外。例如，[1000-1010] 表示 1000 和 1010 之間的所有連接埠號 (包括 1000 和 1010)，而 (1000-1010) 表示 1000 和 1010 之間的所有連接埠號 (但不包括 1000 和 1010)。也可以將方括號和括弧混用。例如，(1000-1010] 表示 1000 和 1010 之間的所有連接埠號，不包括 1000，但包括 1010。

6. 在 [Authentication Type] 下拉式清單中選取認證類型。下列選項可供選用
   - **Require user-password。**存取 SOCKS 伺服器需要有使用者名稱和密碼。
   - **User-password, if available。**如果使用者名稱和密碼可用，應使用它們來存取 SOCKS 伺服器 (它們並非存取所必需的)。
   - **Ban。**禁止存取 SOCKS 伺服器。
   - **None。**存取 SOCKS 伺服器時不需要認證。
7. 從 [Insert] 下拉式清單中選取此項目在 `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，所以必須指定對這些方法的評估順序。因此，如果用戶端不支援所列示的第一種認證方法，就會改用第二種方法。如果用戶端不支援列示的任何認證方法，SOCKS 伺服器將會結束連線，不接受請求。

編輯認證項目

編輯認證項目

1. 存取伺服器實例的 Server Manager，然後按一下 [SOCKS] 標籤。
2. 按一下 [Set SOCKS v5 Authentication] 連結。
3. 選取想要編輯的認證項目，然後按一下 [Edit] 按鈕。
4. 進行所需的變更，然後按一下 [OK]。

刪除認證項目

刪除認證項目

1. 存取伺服器實例的 Server Manager，然後按一下 [SOCKS] 標籤。
2. 按一下 [Set SOCKS v5 Authentication] 連結。
3. 選取想要刪除的認證項目，然後按一下 [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。可以透過移動的方式來變更項目的順序。

移動認證項目

1. 存取伺服器實例的 Server Manager，然後按一下 [SOCKS] 標籤。
2. 按一下 [Set SOCKS v5 Authentication] 連結。
3. 選取想要移動的認證項目，然後按一下 [Move] 按鈕。
4. 從 [Move] 下拉式清單中選取此項目在 `socks5.conf` 檔案中的位置，然後按一下 [OK]。

配置 SOCKS v5 連線項目

SOCKS 連線項目指定 SOCKS 常駐程式是應允許還是應拒絕請求。

本節包含以下主題：

建立連線項目

建立連線項目

1. 存取伺服器實例的 Server Manager，然後按一下 [SOCKS] 標籤。
2. 按一下 [Set SOCKS v5 Connections] 連結。
3. 按一下 [Add] 按鈕。
4. 在 [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. 在 [Connection Type] 下拉式清單中選取此行所符合的指令類型。可能的指令類型爲：
   - **Connect**
   - **Bind**
   - **UDP**
   - **All**

6. 在 [Source Host Mask] 欄位中輸入連線控制項目適用的主機的 IP 位址或主機名稱。如果輸入 IP 位址，請在位址之後加上正斜線以及要套用於來源的 IP 位址的遮罩。SOCKS 伺服器會將此遮罩套用於來源的 IP 位址，以確定其是否爲有效主機。請勿在主機遮罩項目中包含空格。如果不輸入主機遮罩，連線項目將會套用於所有主機。

   例如，可在 [host mask] 欄位中輸入 155.25.0.0/255.255.0.0。如果主機的 IP 位址爲 155.25.3.5，SOCKS 伺服器會將遮罩套用於此 IP 位址，然後判定主機的 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，輸入連線控制項目適用的來源電腦上的連接埠。請勿在連接埠範圍項目中包含空格。如果不指定連接埠範圍，連線項目會套用於所有連接埠。

   可使用方括號 [ ] 來包括範圍兩端的連接埠，也可以使用括弧 ( ) 將它們排除在外。例如，[1000-1010] 表示 1000 和 1010 之間的所有連接埠號 (包括 1000 和 1010)，而 (1000-1010) 表示 1000 和 1010 之間的所有連接埠號 (但不包括 1000 和 1010)。也可以將方括號和括弧混用。例如，(1000-1010] 表示 1000 和 1010 之間的所有連接埠號，不包括 1000，但包括 1010。

8. 在 [Destination Host Mask] 欄位中輸入連線項目適用的 IP 位址或主機名稱。如果輸入 IP 位址，請在位址之後加上正斜線以及要套用於內送 IP 位址的遮罩。SOCKS 伺服器會將此遮罩套用於目標電腦的 IP 位址，以確定其是否爲有效目標主機。請勿在主機遮罩項目中包含空格。如果不輸入目標主機遮罩，連線項目將會套用於所有主機。

   例如，可在 [destination host mask] 欄位中輸入 155.25.0.0/255.255.0.0。如果目標主機的 IP 位址爲 155.25.3.5，SOCKS 伺服器會將遮罩套用於此 IP 位址，然後判定目標主機的 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] 欄位中輸入連線控制項目適用的目標主機上的連接埠。請勿在連接埠範圍項目中包含空格。如果不輸入連接埠範圍，連線項目會套用於所有連接埠。

備註 大多數 SOCKS 應用程式會請求將連接埠 0 用於處理連結請求，這意味著它們沒有任何連接埠喜好設定。因此，連結的目標連接埠範圍應一律包含連接埠 0。

可使用方括號 [ ] 來包括範圍兩端的連接埠，也可以使用括弧 ( ) 將它們排除在外。例如，[1000-1010] 表示 1000 和 1010 之間的所有連接埠號 (包括 1000 和 1010)，而 (1000-1010) 表示 1000 和 1010 之間的所有連接埠號 (但不包括 1000 和 1010)。也可以將方括號和括弧混用。例如，(1000-1010] 表示 1000 和 1010 之間的所有連接埠號，不包括 1000，但包括 1010。

10. 在 [User Group] 欄位中輸入想要允許或拒絕其存取的群組。如果不指定群組，連線項目將套用於所有使用者。
11. 從 [Action] 下拉式清單中選擇針對所要建立的連線的允許或拒絕存取動作。
12. 從 [Insert] 下拉式清單中選取此項目在 `socks5.conf` 檔案中的位置，然後按一下 [OK]。因爲連線指令可以有多種，所以必須指定對這些指令的評估順序。

編輯連線項目

編輯連線項目

1. 存取伺服器實例的 Server Manager，然後按一下 [SOCKS] 標籤。
2. 按一下 [Set SOCKS v5 Connections] 連結。
3. 選取想要編輯的連線項目，然後按一下 [Edit] 按鈕。
4. 進行所需的變更，然後按一下 [OK]。

刪除連線項目

刪除連線項目

1. 存取伺服器實例的 Server Manager，然後按一下 [SOCKS] 標籤。
2. 按一下 [Set SOCKS v5 Connections] 連結。
3. 選取想要刪除的連線項目，然後按一下 [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。可以透過移動的方式來變更項目的順序。

移動連線項目

1. 存取伺服器實例的 Server Manager，然後按一下 [SOCKS] 標籤。
2. 按一下 [Set SOCKS v5 Connections] 連結。
3. 選取想要移動的連線項目，然後按一下 [Move] 按鈕。
4. 從 [Move] 下拉式清單中選取此項目在 `socks5.conf` 檔案中的位置，然後按一下 [OK]。

配置 SOCKS v5 Server 鏈接

可用與鏈接 Proxy Server 相同的方法將 SOCKS 伺服器鏈接在一起 (也就是說，一個 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. 存取伺服器實例的 Server Manager，然後按一下 [SOCKS] 標籤。
2. 按一下 [Set SOCKS v5 Routing] 連結。
3. 在 [Server Chaining] 區段中，輸入用於認證至鏈接的 Proxy Server 的使用者名稱與密碼 (如果代理伺服器鏈中的下游代理伺服器需要認證才能爲任何請求提供服務)，然後按一下 [OK]。

配置路由項目

路由項目可以用來將 Proxy Server 配置爲透過 SOCKS 伺服器路由請求。路由項目有兩種類型，SOCKS v5 路由和 SOCKS v5 代理伺服器路由：

- SOCKS v5 路由確定 SOCKS 常駐程式針對特定 IP 位址應該使用哪個介面。
- SOCKS v5 代理伺服器路由確定能夠透過其他 SOCKS 伺服器存取的 IP 位址，以及此 SOCKS 伺服器是否直接與主機連線。在透過 SOCKS 伺服器路由時，代理伺服器路由是重要的。

本節包含以下主題：

建立 SOCKS v5 路由項目

建立路由項目

1. 存取伺服器實例的 Server Manager，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] 欄位中輸入內送和外寄連線必須通過的指定介面所對應的 IP 位址或主機名稱。如果輸入 IP 位址，請在位址之後加上正斜線以及要套用於內送 IP 位址的遮罩。SOCKS 伺服器會將此遮罩套用於 IP 位址，以確定其是否爲有效主機。請勿在主機遮罩項目中包含空格。如果不輸入主機遮罩，SOCKS v5 項目將會套用於所有主機。

   例如，可在 [host mask] 欄位中輸入 155.25.0.0/255.255.0.0。如果主機的 IP 位址爲 155.25.3.5，SOCKS 伺服器會將遮罩套用於此 IP 位址，然後判定主機的 IP 位址符合路由項目所適用的 IP 位址 (155.25.0.0)。
5. 在 [Port Range] 欄位中輸入內送和外寄連線必須通過的指定介面所對應的連接埠。連接埠範圍不應包含任何空格。如果不指定連接埠範圍，SOCKS v5 項目將會套用於所有連接埠。

   可使用方括號 [ ] 來包括範圍兩端的連接埠，也可以使用括弧 ( ) 將它們排除在外。例如，[1000-1010] 表示 1000 和 1010 之間的所有連接埠號 (包括 1000 和 1010)，而 (1000-1010) 表示 1000 和 1010 之間的所有連接埠號 (但不包括 1000 和 1010)。也可以將方括號和括弧混用。例如，(1000-1010] 表示 1000 和 1010 之間的所有連接埠號，不包括 1000，但包括 1010。
6. 在 [Interface/Address] 欄位中輸入內送和外寄連線必須通過的介面的 IP 位址或名稱。
7. 從 [Insert] 下拉式清單中選取此項目在 `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，所以必須指定對這些方法的評估順序。

備註	指定的介面應該用於內送與外寄連線，否則將因內送路由與配置的介面不同而收到錯誤訊息。

建立 SOCKS v5 代理伺服器路由項目

建立代理伺服器路由項目

1. 存取伺服器實例的 Server Manager，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 [Proxy Type] 下拉式清單中選取透過其進行路由的 Proxy Server 的類型。下列選項可供選用
   - **SOCKS v5**
   - **SOCKS v4**
   - **Direct connection**
5. 在 [Destination Host Mask] 欄位中輸入連線項目適用的 IP 位址或主機名稱。如果輸入 IP 位址，請在位址之後加上正斜線以及要套用於內送 IP 位址的遮罩。SOCKS 伺服器會將此遮罩套用於目標電腦的 IP 位址，以確定其是否爲有效目標主機。請勿在主機遮罩項目中包含空格。如果不輸入目標主機遮罩，連線項目將會套用於所有主機。

   例如，可在 [destination host mask] 欄位中輸入 155.25.0.0/255.255.0.0。如果目標主機的 IP 位址爲 155.25.3.5，SOCKS 伺服器會將遮罩套用於此 IP 位址，然後判定目標主機的 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] 欄位中輸入代理伺服器項目所適用的目標主機上的連接埠。請勿在連接埠範圍項目中包含空格。如果不指定連接埠範圍，代理伺服器項目會套用於所有連接埠。

   可使用方括號 [ ] 來包括範圍兩端的連接埠，也可以使用括弧 ( ) 將它們排除在外。例如，[1000-1010] 表示 1000 和 1010 之間的所有連接埠號 (包括 1000 和 1010)，而 (1000-1010) 表示 1000 和 1010 之間的所有連接埠號 (但不包括 1000 和 1010)。也可以將方括號和括弧混用。例如，(1000-1010] 表示 1000 和 1010 之間的所有連接埠號，不包括 1000，但包括 1010。
7. 在 [Destination Proxy Address] 欄位中，輸入要使用的 Proxy Server 的主機名稱或 IP 位址。
8. 在 [Destination Proxy Port] 欄位中輸入連接埠號，Proxy Server 將會透過此連接埠偵聽是否有 SOCKS 請求。
9. 從 [Insert] 下拉式清單中選取此項目在 `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，所以必須指定對這些方法的評估順序。

編輯路由項目

編輯路由項目

1. 存取伺服器實例的 Server Manager，然後按一下 [SOCKS] 標籤。
2. 按一下 [Set SOCKS v5 Routing] 連結。
3. 選取想要編輯的項目，然後按一下 [Edit] 按鈕。
4. 進行所需的變更，然後按一下 [OK]。

刪除路由項目

刪除路由項目

1. 存取伺服器實例的 Server Manager，然後按一下 [SOCKS] 標籤。
2. 按一下 [Set SOCKS v5 Routing] 連結。
3. 選取想要刪除的項目，然後按一下 [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。可以透過移動的方式來變更項目的順序。

移動路由項目

1. 存取伺服器實例的 Server Manager，然後按一下 [SOCKS] 標籤。
2. 按一下 [Set SOCKS v5 Routing] 連結。
3. 選取想要移動的項目，然後按一下 [Move] 按鈕。
4. 從 [Move] 下拉式清單中選取此項目在 `socks5.conf` 檔案中的位置，然後按一下 [OK]。

第 16 章

管理範本和資源

利用範本您可將多個 URL 分組在一起，以便能夠配置代理伺服器對它們的處理方式。依據用戶端所嘗試擷取的不同 URL，可以讓代理伺服器有不同的運作方式。例如，可以需要用戶端在存取特定網域的 URL 時進行認證（ 鍵入使用者名稱和密碼 ）。或者，可以拒絕存取指向影像檔的 URL。可根據檔案類型配置不同的快取記憶體更新設定。

本章包含下列小節：

關於範本

範本是 URL 的集合，這些 URL 也稱爲資源。資源可以是一個 URL、一組有某些共同點的 URL、或是整個協定。首先命名並建立範本，然後使用常規表示式將 URL 指定給範本。這就意味著您可以將代理伺服器配置爲以不同的方式來處理不同 URL 的請求。範本中可以包含任何能使用常規表示式建立的 URL 式樣。表 16-1 列出預設的資源，並提供其他範本的一些概念。

表 16-1 資源常規表示式萬用字元式樣

常規表示式式樣	配置的內容
`ftp://.*`	所有 FTP 請求
`http://.*`	所有 HTTP 請求
`https://.*`	所有安全的 HTTP 請求
`gopher://.*`	所有 Gopher 請求
`connect://.*:443`	所有對 HTTPS 連接埠的 SSL (安全) 作業事件。
`http://home\.example\.com.*`	`home.example.com` 網站上的所有文件。
`.*\.gif.*`	包含 `.gif` 字串的任何 URL
`.*\.edu.*`	包含 `.edu` 字串的任何 URL
`http://.*\.edu.*`	任何前往 `.edu` 網域中電腦的 URL

瞭解常規表示式

Proxy Server 允許使用常規表示式來識別資源。常規表示式可指定字元字串的式樣。在代理伺服器中，常規表示式可用於尋找 URL 中的相符式樣。

以下是常規表示式的範例：

```
[a-z]*://[^:/]*\.abc\.com.*>
```

此常規表示式可比對到來自 `.abc.com` 網域的任何文件。文件可以是任何協定，可以帶有任何的副檔名。

表 16-2 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
.	比對除換行字元外的任何單一字元。
x?	比對常規表示式 *x* 出現零次或一次。
*x**	比對常規表示式 *x* 出現零次或多次。
x+	比對常規表示式 *x* 出現一次或多次。
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* 恰好出現 *n* 次。
[abc]	比對括號中的任何字元。
[^abc]	比對不在括號中的任何字元。
[a-z]	比對括號中指定範圍內的任何字元。
x	比對字元 *x*，其中 *x* 不是特殊字元。
\x	移除特殊字元 *x* 的涵義。
"x"	移除特殊字元 *x* 的涵義。
xy	比對常規表示式 *x* 及 *y*，其中 *y* 必須出現在 *x* 之後。
x|y	比對常規表示式 *x* 或常規表示式 *y*。
^	比對字串開頭。
$	比對字串結尾。
(x)	將常規表示式分組。

此範例說明表 16-2 中一些常規表示式的用法。

```
[a-z]*://([^.:/]*[:/]|.*\.local\.com).*"
```

- `[a-z]*` 可比對到任何協定的文件。
- `://` 比對跟有 (//) 的 (:)。
- `[^.:/]*[:/]` 比對不包括 (.)、(:) 或 (/) 且其後跟有 (:) 或 (/) 的任何字元字串。因此，它將比對到非完整合格的主機名稱和帶有連接埠號的主機。
- `|.*\.local\.com` 不比對 local.com 這樣的完全合格網域名稱的主機名稱，但比對 .local.com 網域中的文件。

- .*" 比對帶任何副檔名的文件。

備註 如表 16-2 中所述，反斜線可用於退出或移除特殊字元的涵義。句號和問號等字元都有特殊的涵義，因此當這類字元用來表示它們自己時，必須退出。特別是句號，它會在許多 URL 中出現。因此，若要移除常規表示式中句號的特殊涵義，必須在句號前面加上反斜線。

瞭解萬用字元式樣

可以建立萬用字元式樣的清單，用來指定可從您的站點存取哪些 URL。萬用字元可以是常規表示式格式，也可以是 shell 表示式格式，視具體用法而定。通常的規則是：

- 對比對目標 URL 的任何式樣使用常規表示式。這包括 <Object ppath=...>、URL 篩選器、NameTrans、PathCheck 和 ObjectType 函數。
- 對比對外來用戶端或使用者 ID 的任何式樣使用 shell 表示式，其中包括用於存取控制的使用者名稱和群組及外來使用者的 IP 位址或 DNS 名稱 (例如，<Client dns=...>)。

可以使用常規表示式式樣指定多個 URL。可以利用萬用字元按網域名稱或按包含給定字樣的任何 URL 來篩選。例如，您可能要禁止存取含「careers.」字串的 URL。爲此，可以指定 `http://.*careers.*` 做爲範本的常規表示式。

建立新範本

可以使用常規表示式萬用字元式樣來建立範本。然後，可以配置只影響此範本中指定的 URL 之特性。例如，可以對 `.GIF` 影像使用一種類型的快取配置，而對一般 `.HTML` 檔案使用另一種。

建立範本

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

   按一下 [Create Template] 連結。將顯示 [Create Template] 頁面。

2. 在 [Template Name] 欄位中，鍵入要建立的範本名稱，並按一下 [OK]。

   名稱應容易記憶。Server Manager 會提示您儲存並套用變更。可以在建立範本的常規表示式後儲存變更，如其餘的步驟所述。

套用範本

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。將顯示 [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，包括所有要在範本中包含的 URL。
4. 在 [Template] 清單中，選取您剛剛增加的新範本名稱。
5. 按一下 [OK]。
6. 按一下 [Restart Required]。將顯示 [Apply Changes] 頁面。
7. 按一下 [Restart Proxy Server] 按鈕以套用變更。

移除範本

可以移除現有範本。移除範本時，範本的所有相關配置隨之刪除。例如，如果已爲範本 TEST 中的所有 URL 設定存取控制權，當移除 TEST 範本時，對範本中所含 URL 的存取控制權也隨之移除。

移除範本

1. 存取 Server Manager，然後按一下 [Templates] 標籤。
2. 按一下 [Remove Template] 連結。將顯示 [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]。將顯示 [Apply Changes] 頁面。
6. 按一下 [Restart Proxy Server] 按鈕以套用變更。

檢視範本

可以檢視並編輯在 Server Manager 中建立的範本。

編輯範本

1. 存取 Server Manager，然後按一下 [Templates] 標籤。
2. 按一下 [View Template] 連結。將顯示 [View Template] 頁面。範本將顯示在一個表格中，並列出範本的常規表示式和範本名稱。
3. 若要編輯現有範本，請按一下 [Edit Template Assignment] 連結，它會將您帶往 [Apply Template] 頁面。

移除資源

可以使用 [Remove Resource] 頁面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，使與之相關聯的所有設定也隨之從代理伺服器的配置檔案中移除。

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。將顯示 [Remove Resource] 頁面。
3. 從 [Remove] 下拉式清單中，選取想要移除的資源。
4. 按一下 [OK]。
5. 按一下 [Restart Required]。將顯示 [Apply Changes] 頁面。
6. 按一下 [Restart Proxy Server] 按鈕以套用變更。

第 17 章

使用用戶端自動配置檔案

如果您擁有支援許多用戶端的多個 Proxy Server，您可以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，可決定在存取不同的 URL 時，瀏覽器使用哪一個代理伺服器。

當瀏覽器啓動時會載入自動配置檔案。每當使用者按一下一個連結或鍵入一個 URL，瀏覽器會使用配置檔來決定它是否應該使用代理伺服器，以及如果決定使用，應該使用哪個代理伺服器。利用此功能可以輕鬆配置組織中所有的瀏覽器實例。有幾種方式可以讓您向用戶端提供自動配置檔案。

- 您可以使用代理伺服器做爲傳回自動配置檔案的 Web 伺服器。您將瀏覽器指向代理伺服器的 URL。若讓代理伺服器充當 Web 伺服器，可以將自動配置檔案保存在某個地方，當您需要更新時，您只需要變更一個檔案即可。
- 您可以在 Web 伺服器、FTP 伺服器或是瀏覽器能夠存取的任何網路目錄中儲存此檔案。配置瀏覽器時將檔案的 URL 提供給瀏覽器，使其能夠找到檔案，就像任何一般的 URL 那樣。如果您需要執行複雜的計算 (例如，如果您的組織中有大型的代理鏈接)，可以編寫一個 Web 伺服器 CGI 程式，視存取檔案的使用者而輸出不同的檔案。
- 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；但是如果您需要更新檔案，則必須將檔案的副本分發給每個用戶端。

您可以透過下列兩種方式建立自動配置檔案：可使用 Server Manager 中的頁面，或是手動建立檔案。建立檔案的指示在本章的稍後會加以說明。

本章包含下列小節：

瞭解自動配置檔案

本功能記載於此手冊中的原因是身爲 Proxy Server 管理人員的您也會建立與分發用戶端自動配置檔案。

自動配置檔案做些什麼

自動配置檔案是以 JavaScript 編寫的，它是一種簡潔的、基於物件的程式檔語言，用於開發用戶端與伺服器網際網路應用程式。瀏覽器可解譯 JavaScript 檔案。

瀏覽器會在初次載入時下載自動配置檔案。檔案可以保存在瀏覽器能夠使用 URL 到達的任何位置。例如，檔案可以保存在 Web 伺服器中。檔案甚至可以保存在網路檔案系統中，只要瀏覽器可以使用 file:// URL 存取到。

代理伺服器配置檔是以 JavaScript 編寫。JavaScript 檔案定義了一個函數 (稱爲 **FindProxyForURL**)，用以決定瀏覽器應對每個 URL 使用哪個代理伺服器 (如果有的話)。瀏覽器會爲 JavaScript 函數傳送兩個參數：執行瀏覽器的系統之主機名稱以及其嘗試取得的 URL。JavaScript 函數會傳回一個值給瀏覽器，告訴它如何繼續。

利用自動配置檔案可以爲不同類型的 URL、各種伺服器、甚至各種一天中的各個時間指定不同的代理伺服器 (或完全不指定代理伺服器)。換言之，您可以擁有多個專用化的代理伺服器，例如，可讓某個伺服器提供 .com 網域服務，另一個提供 .edu 網域服務，再另一個則提供所有其他服務。如此可以將負載分開並且提高代理伺服器磁碟的使用效率，原因是任何檔案在快取記憶體中都只有一個副本 (而不是多個代理伺服器皆儲存相同的文件)。

自動配置檔案也支援代理伺服器容錯移轉，因此如果有某個代理伺服器無法使用，瀏覽器將會不需設定地切換至另一個代理伺服器。

存取做爲 Web 伺服器的代理伺服器

您可以將一個或多個自動配置檔案儲存在代理伺服器，並且讓代理伺服器充當 Web 伺服器 (其僅有的文件是自動配置檔案)。這樣一來，身爲代理伺服器管理的您就會維護組織中的用戶端所需要的代理伺服器自動配置檔案。它同時也可以讓您將檔案保存在中央位置，這樣如果必須更新檔案，您只需要更新一次，接著所有瀏覽器用戶端就會自動進行更新。

將代理伺服器自動配置檔案保存在 *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，方法是在 [Proxies] 標籤中鍵入檔案的 URL。代理伺服器的 URL 格式如下：

`http://`*proxy.d omain:port/URI*

例如，URL 可以爲 `http://proxy.example.com`。您不需要指定 URI (跟在 host:port 組合後面的 URL 部分)；但是如果您有使用 URI，則可以使用範本來控制對不同自動配置檔案的存取。例如，如果您建立一個名爲 /test 的 URI，其中包含名爲 `/proxy.pac` 的自動配置檔案，則可以建立具有資源式樣 `http://proxy.mysite.com:8080/test/.*` 的範本。您接著可以使用此範本來特別設定針對此目錄的存取控制。

您可以建立多個自動配置檔案並且透過不同的 URL 存取這些檔案。表 17-1 列出了部分範例 URI 以及用戶端存取它們時使用的 URL。

表 17-1 範例 URI 和相應的 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

對反向代理伺服器使用 Pac 檔案

鑒於反向代理伺服器的運作方式，要讓代理伺服器既充當反向代理伺服器又服務於 `.pac` 檔案是非常困難的。這是由於代理伺服器取得檔案請求後，需要決定所請求的是本機 `.pac` 檔案還是遠端文件。

爲了讓代理伺服器既充當反向代理伺服器又維護與服務 `.pac` 檔案，您需要手動地編輯 `obj.conf` 檔案以確保 NameTrans 函數的順序正確。

建立標準對映可讓代理伺服器充當反向代理伺服器。這通常會告知代理伺服器將所有請求路由至遠端的內容伺服器。您可以增加代理伺服器自動配置檔案並對映至特定的目錄，例如 /pac。在此情況中，希望取得 `.pac` 檔案的任何用戶端都將使用如下的 URL：

`http://proxy.mysite.com/pac`

注意 但是使用此對映之後，您必須確定遠端內容伺服器並沒有類似的目錄。

編輯 obj.conf 檔案以確定代理伺服器自動配置檔案的指令與函數在任何其他對映之前出現。此類指令與函數必須最先出現，因爲代理伺服器在爲請求提供服務前通常會執行所有 NameTrans 函數。但是使用自動配置檔案之後，代理伺服器會立刻辨識路徑並傳回 .pac 檔案。

以下是 obj.conf 檔案的一個範例，它使用了反向代理伺服器並且維護一個自動配置檔案：

```
<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 頁面建立自動配置檔案

使用 Server Manager 頁面建立自動配置檔案

1. 存取 Server Manager，然後選取 [Routing] 標籤。
2. 按一下 [Create / Edit Autoconfiguration File] 連結。出現的頁面會列出代理伺服器系統中現有的任何自動配置檔案。您可按一下自動配置檔案對其進行編輯。其餘的步驟會告訴您如何建立新檔案。
3. 鍵入做爲 URL 路徑部分的可選 URI，用戶端從代理伺服器取得自動配置檔案時會使用它。例如，鍵入 / 讓用戶端將檔案做爲代理伺服器的主要文件 (類似 Web 伺服器的 index.html 檔案) 存取；這樣當用戶端存取代理伺服器的自動配置檔案時，將只使用網域名稱。您可使用多個 URI 並爲每個 URI 建立單獨的自動配置檔案。
4. 使用 .pac 副檔名鍵入自動配置檔案的名稱。如果您有一個檔案，可簡單地將其稱爲 proxy.pac (pac 是 proxy autoconfiguration (代理伺服器自動配置) 的縮寫)。所有自動配置檔案皆爲含有單一 JavaScript 函數的 ASCII 文字檔。

5. 按一下 [OK]。將出現另一個頁面。使用此頁面可建立自動配置檔案。用戶端依順序完成頁面上的項目。頁面上的項目如下：

- **Never Go Direct To Remote Server** 告訴 Navigator 始終使用代理伺服器。爲防止您的代理伺服器不執行，您可指定要使用的第二個代理伺服器。
- **Go Direct To Remote Server When** 讓您在特定場合下略過代理伺服器。Navigator 會按照選項在頁面上列示之順序來判斷這些情況：
  - **Connecting To Non-fully Qualified Host Names** 告訴 Navigator 在使用者只指定電腦名稱時直接移至伺服器。例如，如果內部 Web 伺服器名爲 `winternal.mysite.com`，使用者可能只鍵入 `http://winternal`，而不鍵入完全合格的網域名稱。在這種情況下，Navigator 會直接移至 Web 伺服器，而不會移至代理伺服器。
  - **Connecting To A Host In Domain** 可讓您指定最多三個 Navigator 可直接存取的網域名稱。指定網域時，請以點字元做爲開頭。例如，您可鍵入 `.example.com`。
  - **Connecting To A Resolvable Host** 讓 Navigator 在用戶端能夠解析主機時直接移至伺服器。通常在 DNS 設爲只解析本機 (內部) 主機時使用此選項。用戶端會在連接至本機網路外部的伺服器時，使用代理伺服器。

注意 上述選項會使用戶端針對每個請求查閱 DNS。也因爲如此，會使用戶端的效能降低。有鑒於它的負面影響，您應避免使用此選項。

  - **Connecting To A Host In Subnet** 讓 Navigator 在用戶端存取特定子網路中的伺服器時，直接移至伺服器。此選項適用於當某個組織在某個地區有許多子網路時。例如，某些公司可能將它的一個網域名稱用於全世界的子網路，而每個子網路均專屬於某個特定的區域。

注意 上述選項會使用戶端針對每個請求查閱 DNS。也因爲如此，會使用戶端的效能降低。有鑒於它的負面影響，您應避免使用此選項。

  - **Except When Connecting To Hosts** 可讓您指定直接移至伺服器這一規則的異常狀況。例如，如果您鍵入 `.example.com` 做爲要直接前往的網域，您可以將前往 `home.example.com` 做爲一個異常情況。指示 Navigator 在前往 `home.example.com` 時使用代理伺服器，但直接至 `example.com` 網域中的任何其他伺服器。
  - **Secondary Failover Proxy** 指定當您的代理伺服器不執行時所要使用的第二個代理伺服器。

- **Failover Direct** 指示 Navigator 在您的代理伺服器不執行時直接移至這些伺服器。如果指定了第二個容錯轉移代理伺服器，Navigator 會在直接移至伺服器之前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。檔案儲存於 *server-root*/proxy-server*id*/pac 目錄下。您將收到一則確認訊息，說明已正確建立檔案。重複上述步驟以視您的需要建立任意數量的自動配置檔案。

一旦建立自動配置檔案，請務必告知所有使用伺服器的人員指向正確的自動配置檔案，或是親自配置 Navigator 的各個副本。

手動建立自動配置檔案

本節描述如何手動建立自動配置檔案。

代理伺服器自動配置檔案是使用用戶端 JavaScript 編寫而成。每個檔案包含一個 JavaScript 函數 (稱爲 **FindProxyForURL**)，用以決定瀏覽器應對每個 URL 使用哪個代理伺服器 (如果有的話)。瀏覽器會爲 JavaScript 函數傳送兩個參數：目標原始伺服器的主機名稱以及其嘗試取得的 URL。JavaScript 函數會傳回一個值給 Navigator，告訴它如何繼續。下節將描述函數的語法以及可能傳回的值。

FindProxyForURL 函數

FindProxyFor URL 函數的語法如下：

```
function FindProxyForURL(url, host)
{
   ...
}
```

瀏覽器存取每個 URL 時，都會傳送 **url** 和 **host** 參數並且以下列方式呼叫函數：

```
ret = FindProxyForURL(url, host);
```

url 爲在瀏覽器中被存取的完整 URL。

host 爲從正被存取的 URL 所擷取的主機名稱。這樣僅是爲了方便起見；它與 **://** 和其後的第一個 **:** 或 **/** 之間的字串相同。此參數中不包括連接埠號。它可以依據需要從 URL 擷取。

ret (傳回值) 爲描述配置的字串。

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以及其存取的 URL 做爲參數。函數將傳回一個字串，告訴瀏覽器如何繼續進行。如果字串爲空值，則不能使用任何代理伺服器。字串可以包含如表 17-2 中所示任何數目的建構區段，以分號分隔。

表 17-2 FindProxyForURL 傳回值

傳回值	瀏覽器的結果動作
`DIRECT`	直接與伺服器建立連線而不經過任何代理伺服器。
`PROXY` *host:port*	使用指定的代理伺服器和連接埠號。如果有多個以分號分隔的值，則使用第一個代理伺服器。如果此代理伺服器失敗，則會使用下一個代理伺服器，依此類推。
`SOCKS` *host:port*	使用指定的 SOCKS 伺服器。如果有多個以分號分隔的值，則使用第一個代理伺服器。如果此代理伺服器失敗，則會使用下一個代理伺服器，依此類推。

如果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未回應的代理伺服器，接著在一小時後再試，以 30 分鐘爲間隔依此類推。這意味著如果您暫時關閉了代理伺服器，用戶端在啓動後的 30 分鐘以內將會繼續使用代理伺服器。

如果所有代理伺服器都已當機，而且未指定 DIRECT 傳回值，瀏覽器將會詢問使用者是否應該暫時忽略代理伺服器而嘗試採用直接連線。在 20 分鐘後，Navigator 將會詢問是否應該重試代理伺服器，接著在下一個 20 分鐘後重新詢問，以 20 分鐘爲間隔依此類推。

在下列範例中，傳回值會指示瀏覽器使用連接埠 8080 上名爲 `w3proxy.example.com` 的代理伺服器，但是如果此代理伺服器無法使用，瀏覽器會使用連接埠 8080 上名爲 `proxy1.example.com` 的代理伺服器：

```
PROXY w3proxy.example.com:8080; PROXY proxy1.example.com:8080
```

在下面的範例中，主要的代理伺服器爲 `w3proxy.example.com:8080`；如果此代理伺服器無法使用，瀏覽器會使用 `proxy1.example.com:8080`。如果兩個代理伺服器皆無法使用，則瀏覽器會直接前往伺服器 (在 20 分鐘之後，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 有數個預先定義的函數與環境條件，在您使用代理時非常有用。每個函數都會檢查是否有符合特定條件，然後會傳回 True 或 False 值。相關的公用程式函數是一個例外，原因是它們會傳回一個 DNS 主機名稱或 IP 位址。您可以在主要的 **FindProxyForURL** 函數中使用這些函數來決定傳送給瀏覽器的傳回值。有關這些函數的特定使用方法，請參閱本章稍後的範例。

每個函數或環境條件在本節中均會說明。適用於瀏覽器與代理伺服器整合的函數或環境條件爲：

基於主機名稱的函數

- dnsDomainIs()
- isInNet()
- isPlainhost name()
- isResolvable()
- localHostOrDomainIs()

相關公用程式函數：

- dnsDomainLevels()
- dnsResolve()
- myIpAddress()

基於 URL/ 主機名稱的條件：

- shExpMatch()

基於時間的條件：

- dateRange()
- timeRange()
- weekdayRange()

基於主機名稱的函數

基於主機名稱的函數可讓您使用主機名稱或 IP 位址來決定要使用哪個代理伺服器 (如果有的話)。

dnsDomainIs(host, domain)

dnsDomainIs() 函數偵測 URL 主機名稱是否屬於給定的 DNS 網域。如第 341 頁的「範例 1：代理除本地主機以外的所有伺服器」和第 341 頁的「範例 2 ： 代理防火牆外的本機伺服器」所示，當您將瀏覽器配置爲不對本機網域使用代理伺服器時，此函數非常有用。

如果根據 URL 所屬的 DNS 網域從代理伺服器群組選取接收請求的代理伺服器，則當您使用多個代理伺服器進行負載平衡時，則此函數也很有用。例如，如果將包含 .edu 的 URL 引至某個代理伺服器，而將包含 .com 的 URL 引至另一個代理伺服器，來平衡負載，則您可以使用 **dnsDomainIs()** 檢查 URL 主機名稱。

參數：
host 爲 URL 中的主機名稱。

domain 爲用以測試主機名稱的網域名稱。

傳回值：
true 或 false

範例：
下列敘述將爲 true：

```
dnsDomainIs("www.example.com", ".example.com")
```

下列敘述將爲 false：

```
dnsDomainIs("www", ".example.com")
dnsDomainIs("www.mcom.com", ".example.com")
```

isInNet(host, pattern, mask)

isInNet() 函數可用來將 URL 主機名稱解析爲 IP 位址，並測試其是否屬於遮罩指定的子網路。這與 SOCKS 使用的 IP 位址式樣比對屬於同一類型。請參閱第 342 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。如果傳送的是主機名稱，則此函數會將其解析爲 IP 位址。

pattern 爲以圓點分隔的 IP 位址式樣

mask 爲 IP 位址式樣遮罩，可決定應與 IP 位址的哪些部分進行比對。0 值代表忽略；255 代表比對。如果主機的 IP 位址與指定的 IP 位址式樣相符，則此函數爲 true。

傳回值：
true 或 false

範例：
只有在主機的 IP 位址與 198.95.249.79 完全符合時，此敘述才爲 true：

```
isInNet(host, "198.95.249.79", "255.255.255.255")
```

只有在主機的 IP 位址符合 198.95.*.* 時，此敘述才爲 true：

```
isInNet(host, "198.95.0.0", "255.255.0.0")
```

isPlainhost name(host)

isPlainhost name() 函數會偵測請求的 URL 中的主機名稱是一般的主機名稱還是完全合格的網域名稱。如果您希望 Netscape Navigator 直接與本機伺服器連線 (如第 341 頁的「範例 1：代理除本地主機以外的所有伺服器」和第 341 頁的「範例 2 ：代理防火牆外的本機伺服器」所示)，則此函數將非常有用。

參數：
host 爲 URL 中的主機名稱 (不包括連接埠號)，但條件是主機名稱中沒有網域名稱 (沒有點區段)。

傳回值：
如果 **host** 爲本機則爲 true；如果 **host** 爲遠端則爲 false

範例：

```
isPlainhost name("host")
```

如果 **host** 類似 www，則會傳回 true；如果主機類似 `www.example.com` 則會傳回 false。

isResolvable(host)

如果在防火牆內部的 DNS 只能識別內部主機，您可以使用 **isResolvable()** 函數來測試主機名稱是網路內部的還是外部的。使用此函數，您可以將瀏覽器配置爲對內部伺服器使用直接連線，而僅對外部伺服器使用代理伺服器。在一些站點，防火牆內的內部主機能夠解析其他內部主機的 DNS 網域名稱，但是無法解析所有外部主機，此時此函數非常有用。**isResolvable()** 函數會查閱 DNS，嘗試將主機名稱解析爲 IP 位址。請參閱第 342 頁的 「範例 3 ： 只代理未解析的主機」

參數：
host 爲 URL 中的主機名稱。這樣會嘗試解析主機名稱，如果成功則傳回 true。

傳回值：
如果可以解析主機名稱，則傳回 true；如果不能，則傳回 false

範例：

```
isResolvable("host")
```

如果 **host** 類似於 `www` 且可以透過 DNS 進行解析，則此函數會傳回 true。

localHostOrDomainIs(host, hostdom)

localHostOrDomainIs() 函數指定可用完全合格的網域名稱或一般的主機名稱存取的本地主機。請參閱第 341 頁的「範例 2 ： 代理防火牆外的本機伺服器」。

如果主機名稱與指定的主機名稱完全相符，或者如果在主機名稱中沒有與非合格主機名稱相符的網域名稱部分，則 **localHostOrDomainIs()** 函數會傳回 `true`。

參數：
host 爲 URL 中的主機名稱。

hostdom 爲要比對的完全合格的主機名稱。

傳回值：
true 或 false

範例：
下列敘述爲 true (完全相符)：

```
localHostOrDomainIs("www.example.com", "www.example.com")
```

下列敘述爲 true (主機名稱相符，未指定網域名稱)：

```
localHostOrDomainIs("www", "www.example.com")
```

下列敘述爲 false (網域名稱不相符)：

```
localHostOrDomainIs("www.mcom.com", "www.example.com")
```

下列敘述爲 false (主機名稱不相符)：

```
localHostOrDomainIs("home.example.com", "www.example.com")
```

相關公用程式函數

利用相關公用程式函數可找出網域層級、正在執行 Netscape Navigator 的主機或是主機的 IP 位址。

dnsDomainLevels(host)

dnsDomainLevels() 函數會在 URL 主機名稱中尋找 DNS 層級的數目 (點數)。

參數：
host 爲 URL 中的主機名稱。

傳回值：
DNS 網域層級的數目 (整數)。

範例：

```
dnsDomainLevels("www")
```

returns 0。

```
dnsDomainLevels("www.example.com")
```

returns 2。

dnsResolve(host)

dnsResolve() 函數解析給定主機的 IP 位址 (通常是從 URL)。如果 JavaScript 函數必須執行的式樣比對比使用現有函數所能完成的更進階，則此函數非常有用。

參數：
host 爲要解析的主機名稱。將給定的 DNS 主機名稱解析爲 IP 位址，然後將它以點分隔的字串形式傳回。

傳回值：
點四分形式的 IP 位址字串值

範例：
下列範例將會傳回字串 198.95.249.79。

```
dnsResolve("home.example.com")
```

myIpAddress()

當 JavaScript 函數必須視執行瀏覽器的主機而有不同的運作方式時，**myIpAddress()** 函數非常有用。此函數傳回執行瀏覽器的電腦之 IP 位址。

傳回值：
點四分形式的 IP 位址字串值

範例：
如果在電腦 `home.example.com` 上執行 Navigator，下列範例傳回字串 198.95.249.79。

```
myIpAddress()
```

基於 URL/ 主機名稱的條件

您可以比對主機或 URL 來取得負載平衡與路由

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在不同代理伺服器中取得負載平衡以及 URL 的智慧路由。

參數：
str 是要比較的任何字串 (例如 URL 或主機名稱)。

shexp 是用來進行比較的 shell 表示式。

如果字串與指定的 shell 表示式相符，則此表示式爲 true。請參閱第 344 頁的「範例 6 ： 以 shExpMatch() 平衡代理伺服器負載」。

傳回值：
true 或 false

範例：
第一個範例傳回 true，第二個範例傳回 false。

```
shExpMatch("http://home.example.com/people/index.html",
            ".*/people/.*")

shExpMatch("http://home.example.com/people/yourpage/index.html",
           ".*/mypage/.*")
```

基於時間的條件

可以使得 **FindProxyForURL** 函數視日期、時間或星期幾而有不同的運作方式。

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。如果您希望
FindProxyForURL 函數會視當天日期而有不同的運作方式，比方如果爲其中一個代理伺服器排定定期的維護關機時間，則此函數非常有用。

日期範圍可以透過數種方式指定：

```
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 爲在 1 和 31 之間的一個整數，代表一個月中的某天。

month 爲下列一個月字串：

```
JAN FEB MAR APR MAY JUN JUL AUG SEP OCT NOV DEC
```

year 是一個四位數字的整數，代表年度 (例如 1996 年)。

gmt 或者爲字串 GMT (以格林威治標準時間進行時間比較)，或者保留空白 (假設時間處於當地時區)。GMT 參數可以在任何呼叫設定檔中指定，始終做爲最後一個參數。如果只指定一個值 (從每個類別：day, month, year)，函數只有在與指定值相符的日期才會傳回 true 值。如果指定了兩個值，從第一個指定的時間到第二個指定的時間這一範圍內，結果皆爲 true。

範例：

此敘述在本地時區每月的第一天爲 true。

```
dateRange(1)
```

此敘述在格林威治標準時間每月的第一天爲 true。

```
dateRange(1, "GMT")
```

此敘述在每月的前半個月爲 true。

```
dateRange(1, 15)
```

此敘述在每年的 12 月 24 日爲 true。
```
dateRange(24, "DEC")
```

此敘述在 1995 年 12 月 24 日爲 true。
```
dateRange(24, "DEC", 1995)
```

此敘述在每年的第一季期間爲 true。
```
dateRange("JAN", "MAR")
```

此敘述在每年的 6 月 1 日到 8 月 15 日爲 true。
```
dateRange(1, "JUN", 15, "AUG")
```

此敘述從 1995 年 6 月 1 日到 1995 年 8 月 15 日爲 true。
```
dateRange(1, "JUN", 15, 1995, "AUG", 1995)
```

此敘述從 1995 年 10 月到 1996 年 3 月爲 true。
```
dateRange("OCT", 1995, "MAR", 1996)
```

此敘述在 1995 年的整年度爲 true。
```
dateRange(1995)
```

此敘述從 1995 年初到 1997 年末爲 true。
```
dateRange(1995, 1997)
```

timeRange (hour, minute, second...)

timeRange 函數偵測特定的時刻或時間範圍，例如晚 9 點到上午 12 點。如果您希望 **FindProxyForURL** 函數會視時間而有不同的運作方式，則此函數非常有用。

```
timeRange(hour)
timeRange(hour1, hour2)
timeRange(hour1, min1, hour2, min2)
timeRange(hour1, min1, sec1, hour2, min2, sec2)
```

參數：
hour 是 0 到 23 的小時數。(0 爲午夜，23 爲晚上 11 點)

min 是 0 到 59 的分鐘數。

sec 爲 0 到 59 的秒數。

gmt 或者爲字串 GMT (代表 GMT 時區)，或者不指定 (代表當地時區)。此參數可以對每個參數設定檔使用，而且始終爲最後一個參數。

傳回值：
true 或 false

範例：
此敘述從中午到下午 1:00 爲 true。
```
timerange(12, 13)
```

此敘述從 GMT 中午到下午 12:59 爲 true。
```
timerange(12, "GMT")
```

此敘述從上午 9:00 到下午 5:00 爲 true。
```
timerange(9, 17)
```

從中午到中午過後的 30 秒之間爲 true。
```
timerange(0, 0, 0, 0, 0, 30)
```

weekdayRange(wd1, wd2, gmt)

weekdayRange() 函數會偵測特定的星期或星期範圍，例如星期一到星期五。如果您希望 **FindProxyForURL** 函數視星期幾而有不同的運作方式，則此函數非常有用。

參數：
wd1 和 **wd2** 是下列任意一個星期字串：
```
SUN MON TUE WED THU FRI SAT
```

gmt 或者爲 GMT (代表格林威治標準時間) 或者保留空白 (代表當地時間)。

只有第一個參數 wd1 是必須要有的。wd2 或 gmt (或兩者) 可以留空。

如果只有一個參數出現，函數會在參數代表的星期幾傳回 true 值。如果字串 GMT 指定爲第二個參數，則會採用 GMT 的時間，否則會採用您當地時區的時間。

如果同時定義 wd1 和 wd2，則當目前的星期是在這兩個星期之間時，此條件爲 true。含頭尾兩日。參數的順序很重要；“MON,” “WED” 爲星期一到星期三，但是 “WED,” “MON” 則是從星期三到下週的星期一。

範例：
下列敘述在星期一到星期五 (當地時區) 爲 true。
```
weekdayRange("MON", "FRI")
```

下列敘述在星期一到星期五 (格林威治標準時間) 爲 true。
```
weekdayRange("MON", "FRI", "GMT")
```

下列敘述在當地時間的星期六爲 true。
```
weekdayRange("SAT")
```

下列敘述在格林威治標準時間星期六爲 true。
```
weekdayRange("SAT", "GMT")
```

下列敘述在星期五到星期一爲 true (順序很重要)
`weekdayRange("FRI", "MON")`

詳細範例

範例 1：代理除本地主機以外的所有伺服器

在此範例中，Netscape Navigator 會直接與非完全合格的所有主機以及在本機網域中的主機連線。所有其他情況則要經過名爲 `w3proxy.example.com:8080` 的代理伺服器。

備註 如果代理伺服器關閉，將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 ： 代理防火牆外的本機伺服器

此範例與前一個範例類似，但是它是對防火牆外的本機伺服器使用代理伺服器。如果有屬於本機網域但是卻在防火牆外的主機 (例如主要 Web 伺服器)，而且只能透過代理伺服器才能到達，則這些異常情況是使用 **localHostOrDomainIs()** 函數來處理：

```
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";
}
```

此範例對 `example.com` 網域中除本地主機以外的所有主機使用代理伺服器。主機 `www.example.com` 和 `merchant.example.com` 也會經過代理伺服器。

對異常情況的規定可以提高效率：**localHostOrDomainIs()** 函數只能對本地網域中的 URL 執行，並非對每個 URL 皆能執行。特別要注意 *and* 表示式之前在 *or* 表示式周圍的括號。

範例 3 ： 只代理未解析的主機

本範例適用於所設內部 DNS 只能解析內部主機名稱的環境中，而其目標是只對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";
}
```

本範例需要每次查閱 DNS，因此它應該與其他規則組合，以便只有在其他規則不能獲得結果時才查閱 DNS：

```
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，給定子網路中的所有主機都直接連線，而其他主機則要經過代理伺服器。

```
function FindProxyForURL(url, host)
{
    if (isInNet(host, "198.95.0.0", "255.255.0.0"))
        return "DIRECT";
    else

        return "PROXY proxy.mydomain.com:8080";
}
```

在開頭增加備援規則可以將此範例中對 DNS 的使用減至最少：

```
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：以 dnsDomainIs() 平衡代理伺服器負載

此範例較爲複雜。代理伺服器有四個，其中一個伺服器是做爲其他伺服器的備用，如果其餘三個伺服器中有任何一個當機，第四個伺服器將會接替其工作。其餘三個代理伺服器根據 URL 的式樣分擔負載，這樣它們的快取會更有效率 (在三個伺服器上只有一個文件的副本，而不是每個伺服器上都有一個副本)。負載分配的方式如表 17-3 中所示。

表 17-3 平衡代理伺服器負載

代理伺服器	用途
#1	.com 網域
#2	.edu 網域
#3	所有其他網域
#4	熱待機

所有本機存取應爲直接存取。所有代理伺服器都在連接埠 8080 上執行。您可以在 JavaScript 中使用 + 運算子連接字串。

```
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 ： 以 shExpMatch() 平衡代理伺服器負載

此範例在本質上與範例 5 相同，但是它使用的是 **shExpMatch()** 而非使用 **dnsDomainIs()**。

```
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：代理特定協定

您可以將某個代理伺服器設定爲針對某個特定的協定。多數標準的 JavaScript 功能都可用於 **FindProxyForURL()** 函數中。例如，若要根據協定設定不同的代理伺服器，您可以使用 **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()** 函數完成此動作，例如：

```
...
if (shExpMatch(url, "http:*")) {
    return "PROXY http-proxy.mydomain.com:8080;
}

...
```

第 5 部分

附錄

ACL 檔案語法

存取控制清單 (ACL) 檔案是文字檔案，其中的清單定義了誰可以存取 Proxy Server 資源。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。也可以建立多個 ACL 檔案，並在 `obj.conf` 檔案中參照這些檔案。

Proxy Server 4 使用的 ACL 檔案語法與 Proxy Server 3.x 不同。本附錄描述了 ACL 檔案及其語法。如需有關控制存取 Proxy Server 及其資源的詳細資訊，請參閱第 133 頁的第 8 章 「控制對伺服器的存取」。Proxy Server 4 版本支援資源範本，相關資訊參閱第 319 頁的第 16 章 「管理範本和資源」。

本附錄包含下列小節：

關於 ACL 檔案和 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 檔案均必須以語法版本號碼開始。例如：

```
version 3.0;
```

只能有一個版本行，此版本行可以出現於任何註釋行之後。Proxy Server 使用語法版本 3.0。在註釋行的開始處使用 # 符號可以將註釋加入檔案中。

檔案中的每個 ACL 均以定義其類型的敘述開始。ACL 可以是以下三種類型之一：

- 路徑 ACL 指定受其影響的資源之絕對路徑。
- 資源 ACL 指定受其影響的範本，例如 `http://`、`https://`、`ftp://` 等等。如需有關範本的更多資訊，請參閱第 319 頁的第 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。伺服器具有預設的已命名資源，每一位使用者均可讀取此資源，而 LDAP 目錄中的使用者還可對其進行寫入存取。儘管可以從 Proxy Server 使用者介面建立已命名 ACL，但您還是必須藉由 obj.conf 檔案中的資源手動參照已命名 ACL。

路徑 ACL 和資源 ACL 可以包括萬用字元。如需有關萬用字元的更多資訊，請參閱第 319 頁的第 16 章 「管理範本和資源」。

類型行以字母 acl 開始，然後是以雙引號標示的類型資訊，其後跟隨一個分號。例如：

```
acl "default";
acl "http://*.*";
```

所有 ACL 的每種類型資訊必須具有唯一的名稱，即使在不同的 ACL 檔案中亦如此。定義 ACL 的類型之後，可以用一個或多個敘述來定義 ACL 使用的方法 (認證敘述) 以及允許或拒絕哪些使用者與電腦存取 (授權敘述)。以下小節描述了這些敘述的語法。

本節包含以下主題：

- 認證敘述
- 授權敘述
- 預設 ACL 檔案

認證敘述

ACL 可以選擇性地指定伺服器處理 ACL 時必須使用的認證方法。有三種一般方法：

- 基本 (預設)
- 摘要
- SSL

「基本」和「摘要」方法需要使用者在存取資源之前輸入使用者名稱和密碼。

SSL 方法需要使用者具有用戶端憑證。若要進行認證，必須爲 Proxy Server 開啓加密功能，而且使用者的憑證核發者必須在可信任 CA 清單中。

依預設，伺服器針對未指定方法的任意 ACL 使用「基本」方法。伺服器的認證資料庫必須支援使用者傳送的「摘要」認證。

每個認證行均必須指定伺服器認證的屬性 (使用者、群組或者這兩者)。以下認證敘述出現於 ACL 類型行之後，它指定對與資料庫或目錄中的個別使用者相符的使用者進行「基本」認證。

```
authenticate (user) {
    method = "basic";
};
```

以下範例使用 SSL 做爲使用者和群組的認證方法：

```
authenticate (user, group) {
    method = "ssl";
};
```

以下範例允許使用者名稱以 sales 一詞開始的所有使用者進行存取：

```
allow (all) user = "sales*";
```

如果最後一行變更爲 group = sales，則 ACL 將失敗，因爲未認證群組屬性。

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。

撰寫授權敘述

撰寫授權敘述時請使用以下語法：

```
allow|deny [absolute] (right[,right...]) attribute expression;
```

每一行以 allow 或 deny 開始。一般來說，最好在第一條規則中拒絕所有使用者存取，然後在後續規則中具體指出允許哪些使用者、群組或電腦進行存取。這是由於規則具有階層結構。也就是說，如果您想要允許所有人存取名爲 /my_files 的目錄，但只允許少數人存取子目錄 /my_files/personal，則子目錄的存取控制將不起作用，原因是被允許存取 /my_files 目錄的任何人也都可以存取 /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，先拒絕所有人存取，然後再允許少數需要存取的使用者進行存取。

但在某些情況下，如果將預設 ACL 設定爲拒絕所有人存取，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 的階層取決於資源。當伺服器接收到對特定資源的請求時，會建立一份申請此資源的 ACL 清單。伺服器首先增加其 obj.conf 檔案的 check-acl 敘述中所列示的已命名 ACL。接著，伺服器會附加符合的路徑與資源 ACL。此清單的處理順序與此相同。除非有「absolute」 ACL 敘述，否則將依順序對所有敘述求值。如果求出「absolute allow」或「absolute deny」敘述的值爲「true」，伺服器將停止處理並接受此結果。

如果有多個相符的 ACL，伺服器會使用最後一個相符的敘述。然而，如果您使用絕對敘述，則伺服器會停止尋找其他相符項，並使用包含絕對敘述的 ACL。如果同一個資源有兩個絕對敘述，則伺服器將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

屬性表示式基於使用者名稱、群組名稱、主機名稱或 IP 位址來定義允許或拒絕哪些使用者存取。以下各行舉例說明了如何爲不同使用者或電腦授予存取權限：

- user = "anyone"
- user = "smith*"
- group = "sales"
- dns = "*.mycorp.com"
- dns = "*.mycorp.com,*.company.com"
- ip = "198.*"
- ciphers = "rc4"
- ssl = "on"

也可以使用 timeofday 屬性來對存取伺服器的時間 (基於伺服器上的本機時間) 進行限定。例如，使用 timeofday 屬性限定使用者在特定時間內進行存取。

應使用 24 小時制指定時間，例如 0400 表示上午 4:00，2230 表示晚上 10:30。以下範例限定名爲 guests 的使用者群組在上午 8:00 到下午 4:59 之間存取：

```
allow (read)
    (group="guests") and
    (timeofday<0800 or timeofday=1700);
```

也可以限定使用者在星期幾進行存取。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意一天的任意時間存取。discount 群組中的使用者在週末可以全天存取，在工作日可以在上午 8 點到下午 4:59 以外的任意時間存取。

```
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

在屬性表示式中可以使用多種運算子。圓括號表示運算子的優先順序。對於 user、group、dns 和 ip 可以使用下列運算子：

- and
- or
- not
- = (等於)
- != (不等於)

對於 timeofday 和 dayofweek 可以使用下列運算子：

- 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 檔案爲伺服器提供預設設定。在使用者介面中建立設定前，伺服器將一直使用工作檔案 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

對於其他字元，必須在字元前後加上雙引號。

一條敘述可以單獨放在一行，並以分號結束。多條敘述放於大括號內。項目清單必須使用逗號分隔，並在前後加上雙引號。

在 obj.conf 中參照 ACL 檔案

在 obj.conf 檔案中可以參照已命名 ACL 或單獨的 ACL 檔案。這是透過在 PathCheck 指令中使用 check-acl 函數來完成的。此行使用以下語法：

```
PathCheck fn="check-acl" acl="aclname"
```

其中 *aclname* 是 ACL 出現在任何 ACL 檔案中的唯一名稱。

例如，可以將以下行增加到 obj.conf 檔案中，以使用名爲 testacl 的 ACL 來限定對目錄的存取：

```
<Object ppath="https://"
PathCheck fn="check-acl" acl="testacl"
</Object
```

在上述範例中，第一行的物件聲明要進行存取限定的伺服器資源。第二行的 PathCheck 指令使用 check-acl 函數將已命名 ACL (testacl) 連結至出現此指令的物件。testacl ACL 可以出現於 server.xml 所參照的任何 ACL 檔案中。

調校伺服器效能

許多元素影響 Proxy Server 環境中的效能，包括代理伺服器用戶端、Proxy Server、原始伺服器及網路。本附錄描述可以進行的調整，它們可提昇 Proxy Server 的效能。

本附錄包含下列小節：

注意 本附錄「僅」供進階管理員使用。調校伺服器時要非常小心，在進行任何變更前，請務必先備份配置檔案。

一般效能注意事項

本節描述在分析 Proxy Server 效能時需要考慮的一般事項。

本節包含以下主題：

存取記錄

停用存取記錄能夠提昇 Proxy Server 的效能。但同時也要付出某種代價，因爲您將無法瞭解誰在存取 Proxy Server 以及他們在請求哪些頁面。

可以將 obj.conf 檔案中的下列指令變爲注釋來停用 Proxy Server 存取記錄：

```
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 快取調校

依預設，Proxy Server 將使用者和群組認證結果存放在 ACL 使用者快取中。可以使用 magnus.conf 檔案中的 ACLCacheLifetime 指令來控制 ACL 使用者快取的有效時間。每次參照快取中的某個項目時，都將計算其生命週期並檢查 ACLCacheLifetime。如果此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，這意味著 Proxy Server 在兩分鐘長的時間內可能不會與 LDAP 伺服器同步。將值設定爲 0 (零) 會使快取關閉，並且在每次使用者認證時都會強制 Proxy Server 查詢 LDAP 伺服器。在實作存取控制時，這會對 Proxy Server 的效能產生不良影響。但如果設定較大的 ACLCacheLifetime 值，則在每次變更 LDAP 項目後，可能都需要重新啓動 Proxy Server，因爲這樣做將強制 Proxy Server 查詢 LDAP 伺服器。僅當 LDAP 目錄經常變更的可能性不大時才需要設定一個較大的值。

ACLUserCacheSize 是 magnus.conf 的一個參數，它配置最多可以保留在快取中的項目數。預設值爲 200。新項目將增加至清單的開頭，當快取達到其最大大小時，將再循環此清單末尾的項目以允許建立新項目。

還可以使用 ACLGroupCacheSize 參數來設定每個使用者項目最多可以快取的群組成員身份數。預設值爲 4。遺憾的是，將不會快取群組中非成員身份的使用者，這將導致每個請求都要進行數個 LDAP 目錄存取。

緩衝區大小

可以指定傳送緩衝區的大小 (SndBufSize) 以及伺服器通訊端處的接收緩衝區 (RcvBufSize) 大小。可以在 magnus.conf 檔案中配置這些參數，建議的參數值會因爲 UNIX 和 Linux 作業系統的差異而有所不同。請參閱作業系統文件以便能夠正確地設定這些參數。

連線逾時

使用 magnus.conf 檔案中的 AcceptTimeout 指令可以指定伺服器等待來自用戶端的資料到達的秒數，此時間過後將關閉連線。如果逾時時間已到但資料仍未到達，將關閉連線。依預設，將此項設定爲 30 秒。在多數情況下，不需要變更此項設定。將此值設定爲少於預設值可以釋放執行緒，但也可能因此中斷與連線速度較慢之使用者的連線。

錯誤記錄層級

增大 server.xml 檔案的 LOG 標記中 loglevel 屬性的值會使伺服器在錯誤記錄中產生與儲存更多資訊。但是這樣的話，會在將項目寫入此檔案時對效能產生不良影響。只在對問題除錯時增大記錄，在不處於疑難排解模式時將記錄最小化。

安全性需求

啓用 SSL 可提昇 Proxy Server 的私密性與安全性，但同時會影響效能，因爲資料封包的加密與解密都會耗用效能。可能想要考慮將加密與解密的處理轉給硬體加速卡來完成。

Solaris 檔案系統快取

Proxy Server 快取並不儲存在隨機存取記憶體中。每次從快取中擷取文件時，檔案的存取都是針對檔案系統進行的。可能想要考慮使用 Solaris 的檔案系統快取將 Proxy Server 快取預先載入至記憶體中。接著將從記憶體而不是檔案系統擷取快取檔案。

逾時值

逾時對伺服器效能有明顯的影響。設定 Proxy Server 的最佳化逾時有助於節省網路資源。

有兩個實例專用 SAF (伺服器應用程式函數) 和一個全域參數，可以使用它們來配置 Proxy Server 內的逾時值。

本節包含以下主題：

init-proxy SAF (obj.conf)

`init-proxy` 函數用來初始化 Proxy Server 的內部設定。會在 Proxy Server 初始化期間呼叫此函數，但還應在 `obj.conf` 檔案中指定此函數以確保值已正確初始化。

此函數的語法如下：

```
Init fn=init-proxy
  timeout=seconds
  timeout-2=seconds
```

在上例中，可以將下列參數直接套用於 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等待多長時間後中止閒置連線。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。若設定較小的逾時值，則會中止長時間後才會產生結果 (如資料庫查詢閘道) 的 CGI 程序檔。

  若要確定伺服器的最佳代理伺服器逾時，請考慮以下問題：

  - Proxy Server 是否會處理許多資料庫查詢或 CGI 程序檔？
  - 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。建議的最大代理伺服器逾時值爲 1 小時。預設值爲 300 秒 (5 分鐘)。

  可以檢視或修改代理伺服器逾時值，方法是在 Server Manager 中存取 [Preferences] 標籤底下的 [Configure System Preferences] 頁面。將以 [Proxy Timeout] 來參照此參數。

- `timeout-2` (中斷之後的逾時) — 中斷之後的逾時值會告知 Proxy Server 在用戶端中止作業事件之後它必須繼續寫入快取檔案的時間長度。換言之，如果 Proxy Server 幾乎已經完成文件的快取，而這時用戶端中止了連線，則伺服器將可以繼續快取文件，直至達到中斷之後的逾時值。

  建議的最大中斷之後的逾時值爲 5 分鐘。預設值爲 15 秒。

http-client-config SAF (obj.conf)

`http-client-config` 函數用來配置 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"
```

設定的定義如下：

- `keep-alive` — (可選) 指出 HTTP 用戶端是否應該嘗試使用永久性連線的布林值。預設值爲 true。
- `keep-alive-timeout` — (可選) 保持永久性連線開啓的最大秒數。預設值爲 29。

- always-use-keep-alive — (可選) 指出 HTTP 用戶端是否可以對所有請求類型重複使用現有的永久性連線的布林值。預設值爲 false，意味著對於非 GET 請求或有內文的請求，將不會重複使用永久性連線。
- protocol — (可選) HTTP 通訊協定版本字串。依預設，HTTP 用戶端會使用 HTTP/1.0 或 HTTP/1.1 (視 HTTP 請求的內容而定)。一般而言，除非遇到特定協定互通的功能方面的問題，否則請不要使用此協定參數。
- proxy-agent — (可選) Proxy-agent HTTP 請求標頭的值。預設值爲包含 Proxy Server 產品名稱與版本的字串。

KeepAliveTimeout (magnus.conf)

此參數確定伺服器保持用戶端與伺服器之間 HTTP 持續作用連線或永久性連線開啓的最長時間 (秒)。其預設值爲 30 秒。如果閒置時間超過 30 秒，連線將會逾時。最大值爲 300 秒 (5 分鐘)。

備註 magnus.conf 檔案中的逾時設定將套用於用戶端與 Proxy Server 之間的連線。obj.conf 檔案的 http-client-config SAF 中的逾時設定將套用於 Proxy Server 和原始伺服器間的連線。

更新檢查

Proxy Server 提昇效能的方式是從本機快取中提供文件，而不是從原始伺服器取得文件。這個方法有一個缺點，就是可能會提供已經過期的文件。

Proxy Server 可以執行檢查來確定文件是否爲最新版本，如果確定文件爲舊版本，將會重新整理快取版本。只應在必要時執行此項更新檢查，因爲頻繁地檢查文件可能會降低 Proxy Server 的整體效能。

在 [Caching] 標籤的 [Set Cache Specifics] 頁面中配置更新檢查。預設設定爲每兩小時檢查是否有新版的文件。此資訊透過 max-uncheck 參數在 ObjectType 指令中進行配置。

若要在提昇伺服器效能的同時確保文件爲最新版本，請自訂更新檢查，方法是結合 last-modified 因素來確定合理的文件使用期限。

Last-Modified 因素

last-modified 因素用來微調文件更新處理。此因素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 因素是介於 .02 和 1.0 之間的分數。將以此數目乘以文件的實際上次修改時間與上次對文件執行更新檢查的時間之間的間隔，然後將產生的數目與上次更新檢查以來的時間加以比較。如果此數目小於時間間隔，則表示文件尚未過期。但如果它大於時間間隔，則表示文件已過期，而且會從原始伺服器取得新版文件。

last-modified 因素可使您確保對最近變更的文件的檢查頻率高於對舊版文件的檢查頻率。

應將 last-modified 因素設定在 0.1 和 0.2 之間。

DNS 設定

DNS 是用來將標準 IP 位址與主機名稱相關聯的系統。如果未合理配置此系統，它可能會佔用有價值的 Proxy Server 資源。若要使效能最佳化，請考慮執行下列動作：

- 啓用「DNS 快取」

  啓用「DNS 快取」的方法是，在 Server Manager 中選擇 [Preferences] 標籤底下的 [Configure DNS Cache] 連結。選取對應 DNS 快取的 [Enabled] 單選按鈕。

- 不記錄用戶端 DNS 名稱 — 只記錄用戶端 IP 位址

  停用用戶端 DNS 名稱記錄的方法是，在 Server Manager 中選擇 [Server Status] 標籤底下的 [Set Access Log Preferences] 連結。選取 [IP Addresses] 單選按鈕以記錄 IP 位址而非用戶端主機名稱。

- 停用反向 DNS

  「反向 DNS」會將 IP 位址轉換爲主機名稱。停用「反向 DNS」的方法是，在 Server Manager 中選擇 [Preferences] 標籤底下的 [Configure System Preferences] 連結。選取 [No] 單選按鈕以停用反向 DNS。

- 避免基於用戶端主機名稱的存取控制

  在存取控制敘述中使用用戶端的 IP 位址而非主機名稱 (如有可能)。

執行緒數目

magnus.conf 檔案中的 RqThrottle 參數用來指定 Proxy Server 能夠處理的同步作業事件的最大數目。預設值爲 128。可透過變更此數值來調整伺服器，將執行的作業事件的延時減至最低。

若要計算同步請求的數目，伺服器會對作用中請求的數目進行計數，有一個新的請求到達時將數目增加一，完成某個請求時將數目減去一。新請求到達時，伺服器會查看正在處理的請求數是否已達到最大數目。如果已經達到限制，它將推遲處理新請求，直至作用中請求的數目降到最大數目之下。

透過檢視 perfdump 產生的資料的 SessionCreationInfo 部分，或是檢視 proxystats.xml 資料，可以監視同步請求的數目。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。下列資訊來自 perfdump 輸出：

```
SessionCreationInfo:
------------------------
Active Sessions          1
Keep-Alive Sessions      0
Total Sessions Created   48/128
```

Active Sessions 顯示目前正在爲請求提供服務的階段作業 (請求處理執行緒) 數目。Keep-Alive Sessions 與 Active Sessions 類似，但它專用於指出用戶端是否正在請求持續作用連線。Total Sessions Created 顯示已建立的階段作業數及允許的最大階段作業數目。這些是 RqThrottle 值的最小與最大值。

備註 RqThrottleMin 是伺服器在啓動時初始化的執行緒的最小數目。預設值爲 48。此參數也可以在 magnus.conf 檔案中設定，但在預設狀態下不會顯示。

到達已配置執行緒的最大數目並不一定不好，如果看見此訊息，並不需要自動增加 RqThrottle 值。到達此限制表示伺服器在尖峰負載時需要這麼多的執行緒，但只要伺服器能夠及時爲請求提供服務，即表示對伺服器的調校是適當的。但在這種情況下，連線會在連線佇列中排隊，可能會使其溢位。如果定期檢查 perfdump 輸出並注意到建立的階段作業總數經常接近 RqThrottle 最大值，則請考慮增大執行緒限制。

適合的 RqThrottle 值範圍介於 100 到 500 之間，視負載情況而定。

傳入連線池

可以使用 KeepAlive* 及 magnus.conf 中的相關設定 (包括下列設定) 來調校傳入連線池：

- MaxKeepAliveConnections
- KeepAliveThreads
- KeepAliveTimeout
- KeepAliveQueryMaxSleepTime
- KeepAliveQueryMeanTime
- ConnQueueSize
- RqThrottle
- acceptorthreads

備註 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，其網址爲：

http://docs.sun.com/source/817-6249/index.html

傳出連線池設定無法在此 Proxy Server 版本中配置。

FTP 清單寬度

可能想要修改 FTP 清單的寬度，使其更符合您的需求。增加清單寬度可顯示更長的檔案名，從而減少對檔案名稱的截斷。預設寬度爲 80 個字元。

可以選擇 Server Manager 的 [Preferences] 標籤底下的 [Tune Proxy] 連結來修改 FTP 清單寬度。

快取架構

可以透過合理地設計快取架構來提昇伺服器的效能。設計快取架構時請記住以下建議：

- 分布負載
- 使用多個代理伺服器快取分割區
- 使用多個磁碟機
- 使用多個磁碟控制器

正確的快取設定對於 Proxy Server 的效能而言非常重要。在設計代理伺服器快取架構時，需要記住的最重要規則是分布負載。應將快取設定爲每個分割區大約 1 GB，而且應使其跨多個磁碟與多個磁碟控制器。這種編排提供了比使用單一的大容量快取更快的檔案建立與擷取速度。

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，或是對快取內已有的文件進行更新檢查。通常會在 Proxy Server 上的負載處於最低水平時啓動此功能。可以透過 [Cache Batch Updates] 表單來建立、編輯和刪除 URL 批次以及啓用和停用批次更新功能。

可以透過指定要批次更新的檔案來主動地 (而不是按需要) 快取內容。Proxy Server 可讓您對快取內現有的若干個檔案執行更新檢查，或是預先載入某個網站中的多個檔案。

在有伺服器與代理伺服器網路的大型網站中，管理員可能想要使用批次更新來預先載入 Web 的給定區域。批次程序將對文件中的所有連結執行遞迴下降，在本機快取內容。這個功能對於遠端伺服器而言可能是個負擔，因此在使用時請小心。可以採取一些措施來防止此程序無限期地執行遞迴，透過 `bu.conf` 配置檔案中的參數可以對此程序進行一定程度的控制。

使用 Proxy Server 存取記錄來確定最常使用哪些網站，並對這些網站執行批次更新來提昇效能。

資源回收

資源回收是檢查 Proxy Server 快取並移除舊 (過期) 檔案的程序。資源回收是一個需要耗費大量資源的程序，因此可能需要調校某些資源回收設定以提昇其效能。

下列參數提供了微調資源回收程序的功能。可以檢視或修改 [Tune Garbage Collection] 表單上的這些參數，選擇 Server Manager 的 [Caching] 標籤底下的 [Tune GC] 即可找到這些參數。

本節包含以下主題：

gc hi margin percent 變數

`gc hi margin percent` 變數用來控制最大快取大小的百分比，到達此百分比時將觸發資源回收。

此值必須高於 `gc lo margin percent` 的值。

`gc hi margin percent` 的有效範圍是 10% 到 100%。預設值爲 80% (到達快取容量的 80% 時將觸發資源回收)。

gc lo margin percent 變數

`gc lo margin percent` 變數用來控制資源回收器的目標最大快取大小百分比。

此值必須低於 `gc hi margin percent` 的值。

`gc lo margin percent` 的有效範圍是 5% 到 100%。預設值爲 70% (目標爲在資源回收後使快取的滿容率達到 70%)。

gc extra margin percent 變數

如果觸發資源回收的原因不是由於分割區的大小接近允許的最大大小 (gc hi margin percent)，資源回收器將會使用 gc extra margin percent 變數設定的百分比來確定要移除的快取百分比。

gc extra margin percent 的有效範圍是 0% 到 100%。預設值爲 30% (移除現有快取檔案的 30%)。

gc leave fs full percent 變數

gc leave fs full percent 值確定快取分割區大小的百分比，低於此百分比時將不會進行資源回收。此值可避免當某個其他應用程式獨佔磁碟空間時資源回收器移除快取中的所有檔案。

gc leave fs full percent 的有效範圍爲 0% (允許完全移除) 到 100% (不移除任何檔案)。預設值爲 60% (允許快取大小縮小爲目前大小的 60%)。

Solaris 效能調校

可以使用 Solaris 核心中的各種參數來微調 Proxy Server 效能。下表列出了其中的部分參數。

表 B-1 Solaris 效能調校參數

參數	範圍	預設值	調準值	註釋
rlim_fd_max	/etc/system	1024	8192	處理開啓檔案描述元限制。應將預期的負載 (用於相關的通訊端、檔案和管道，如果有的話) 計算在內。
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。將此參數設定爲 0 會使其具有無限大小，這樣效能的執行就不會因爲缺少緩衝區空間而受到影響。也請在用戶端設定此參數。
tcp_close_wait_interval	ndd/dev/tcp	240000	60000	也請在用戶端設定此參數。
tcp_conn_req_max_q	ndd/dev/tcp	128	1024	

表 B-1 Solaris 效能調校參數

參數	範圍	預設值	調準值	註釋
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	如果是流量較大的網站，請減少此值。
tcp_rexmit_interval_initial	ndd/dev/tcp	3000	3000	如果重新傳輸大於 30-40%，請增加此值。
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	也請在用戶端設定此參數。
tcp_slow_start_initial	ndd/dev/tcp	1	2	可略微加快少量資料的傳輸速度。
tcp_xmit_hiwat	ndd/dev/tcp	8129	32768	使用此參數可增大傳輸緩衝區。
tcp_recv_hiwat	ndd/dev/tcp	8129	32768	使用此參數可增大接收緩衝區。

如需有關這些參數的更多資訊，請參閱「Sun ONE Web Server 6.1 Performance Tuning, Sizing, and Scaling Guide」的第 5 章：

http://docs.sun.com/source/817-6249/index.html

索引

符號

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

一畫

二畫

三畫

四畫

五畫

六畫

七畫

八畫

九畫

十畫

十一畫

十二畫

十三畫

十四畫

十五畫

十六畫

十七畫

十八畫

十九畫

二十一畫

二十二畫

二十三畫

二十三畫