# Sun Java System Portal Server Secure Remote Access 7.2 管理指南

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

文件號碼：820–4824
2008 年 5 月

080618@20490

# 目錄

**前言** ..... 17

**第 1 部分 Secure Remote Access 伺服器元件** ..... 23

**1 Portal Server Secure Remote Access 伺服器簡介** ..... 25
Secure Remote Access 簡介 ..... 25
開放模式 ..... 26
安全模式 ..... 26
Secure Remote Access 服務 ..... 27
配置 Secure Remote Access 屬性 ..... 28
設定衝突解決 ..... 29
▼ 設定衝突解決層級 ..... 29
支援的應用程式 ..... 29
在您開始前 ..... 30

**2 使用閘道** ..... 31
閘道簡介 ..... 31
建立閘道設定檔 ..... 32
建立多個閘道實例 ..... 32
重新啓動閘道 ..... 33
配置閘道監視程式 ..... 33
指定虛擬主機 ..... 33
指定代理伺服器以連絡 Access Manager ..... 33
了解 platform.conf 檔案 ..... 34
使用 Web 代理伺服器 ..... 39
Web 代理伺服器配置 ..... 39
使用自動代理伺服器配置 ..... 45

使用範例 PAC 檔案 ..... 46
指定 PAC 檔案位置 ..... 47
在個別階段作業中新增服務 ..... 47
使用 Netlet 代理伺服器 ..... 47
啓用 Netlet 代理伺服器 ..... 50
重新啓動 Netlet 代理伺服器 ..... 50
使用 Rewriter 代理伺服器 ..... 50
建立 Rewriter 代理伺服器的實例 ..... 51
啓用 Rewriter 代理伺服器 ..... 51
重新啓動 Rewriter 代理伺服器 ..... 51
使用含有閘道的反向代理伺服器 ..... 51
取得用戶端資訊 ..... 52
使用認證鏈接 ..... 53
使用萬有字元憑證 ..... 54
停用瀏覽器快取 ..... 54
自訂閘道服務使用者介面 ..... 54
修改 srapGateway.properties 檔案 ..... 54
共用 LDAP 目錄 ..... 55

**3 使用 Proxylet** ..... 57
使用 Proxylet ..... 57
Proxylet 摘要 ..... 57
HTTPS 支援 ..... 58
使用 Proxylet 的優點 ..... 58
配置 Proxylet ..... 58

**4 使用 Rewriter** ..... 61
Rewriter 簡介 ..... 61
字元集編碼 ..... 62
Rewriter 使用方案 ..... 62
撰寫規則集 ..... 63
定義以語言爲基礎的規則 ..... 68
HTML 內容的規則 ..... 68
JavaScript 內容的規則 ..... 74
XML 內容的規則 ..... 87

Cascading Style Sheet (串接樣式表) 的規則 ..... 90
WML 的規則 ..... 90
使用遞迴功能 ..... 90
使用除錯記錄檔排除故障 ..... 90
設定 Rewriter 除錯層級 ..... 91
除錯檔案名稱 ..... 91
工作範例 ..... 93
HTML 內容範例 ..... 95
JavaScript 內容範例 ..... 102
XML 屬性範例 ..... 118
案例研究 ..... 119
假設狀況 ..... 119
6.x 與 3.0 規則集對映 ..... 123

**5 使用 NetFile** ..... 125
NetFile 簡介 ..... 125
支援檔案存取協定 ..... 125
▼ 建立 NetFile 策略 ..... 127

**6 使用 Netlet** ..... 129
Netlet 簡介 ..... 129
Netlet 元件 ..... 130
Netlet 使用方案 ..... 131
使用 Netlet ..... 131
從遠端主機下載 Applet ..... 132
定義 Netlet 規則 ..... 132
規則類型 ..... 135
Netlet 規則範例 ..... 138
Netlet 規則範例 ..... 143
Netlet 記錄資訊 ..... 146
在 Sun Ray 環境中執行 Netlet ..... 146
新的 HTML 檔 ..... 146
停用的 HTML 檔 ..... 148

**第 2 部分　配置 Secure Remote Access 伺服器** ..... 149

**7　配置 Secure Remote Access 伺服器存取控制** ..... 151
配置存取控制 ..... 151
▼配置存取控制 ..... 152

**8　配置 Secure Remote Access 閘道** ..... 153
配置設定檔核心選項 ..... 153
配置啓動模式 ..... 153
配置核心元件 ..... 155
配置基本選項 ..... 155
配置部署選項 ..... 158
配置代理伺服器設定 ..... 158
配置 Rewriter 代理伺服器與 Netlet 代理伺服器 ..... 159
配置安全性選項 ..... 161
配置 PDC 與非認證 URL ..... 161
配置 TLS 與 SSL 選項 ..... 162
配置效能選項 ..... 163
配置逾時與重試 ..... 163
配置 HTTP 選項 ..... 164
監視 Secure Remote Access 效能 ..... 165
配置 Rewriter 選項 ..... 165
配置基本選項 ..... 165
配置 URI 與規則集的對映 ..... 166
配置剖析器與 MIME 類型的對映 ..... 167
配置個人數位憑證認證 ..... 168
▼配置 PDC 與編碼裝置 ..... 169
▼在閘道機器上匯入根 CA 憑證 ..... 171
使用指令行選項配置閘道屬性 ..... 172
▼管理外部伺服器 Cookie 儲存 ..... 172
▼啓用將 Cookie 標示爲安全 ..... 173
▼建立不可使用之代理伺服器的 URL 清單 ..... 173
▼管理 URI 對映的規則集 ..... 174
▼指定預設網域 ..... 175
▼管理 MIME 推測 ..... 176

▼建立要剖析的 URI 對映清單 ..... 176
▼管理遮罩 ..... 177
▼指定遮罩種子字串 ..... 178
▼建立不要遮罩的 URI 清單 ..... 178
▼讓閘道通協定與原始 URI 通訊協定相同 ..... 179

**9 在閘道服務中配置 Rewriter** ..... 181
建立 URI 與規則集對映清單 ..... 181
在語法中使用萬用字元 ..... 182
在閘道服務中配置 Rewriter ..... 182
▼啓用閘道以重寫所有 URI ..... 182
▼指定不要重寫的 URI ..... 183
▼將 URI 對應至規則集 ..... 183
▼指定 MIME 對映 ..... 184
▼指定預設網域 ..... 185

**10 使用憑證** ..... 187
SSL 憑證簡介 ..... 187
憑證檔案 ..... 188
憑證信任屬性 ..... 189
CA 信任屬性 ..... 189
certadmin 程序檔 ..... 193
產生自簽憑證 ..... 193
產生憑證簽署請求 (CSR) ..... 194
新增根 CA 憑證 ..... 196
安裝來自憑證授權單位的 SSL 憑證 ..... 196
刪除憑證 ..... 198
修改憑證的信任屬性 ..... 199
列示根 CA 憑證 ..... 200
列示所有憑證 ..... 200
列印憑證 ..... 201

**11 配置 Netlet** ..... 203
配置 Netlet 屬性 ..... 203

▼配置基本屬性 ..... 203
▼配置進階屬性 ..... 204
▼建立、修改或刪除 Netlet 規則 ..... 205
Netlet 代理伺服器配置 ..... 207

**12 配置 Netlet 使用私有網域憑證** ..... 209
爲 PDC 配置 Netlet ..... 209
▼爲 PDC 配置 Netlet ..... 209

**13 配置 Proxylet** ..... 211
配置 Proxylet 屬性 ..... 211
▼配置 Proxylet 屬性 ..... 211
配置應用程式至入口網站桌面 ..... 213
▼配置應用程式至入口網站桌面 ..... 213
在 Java Web Start 或 Applet 模式中啓動 Proxylet ..... 214
▼在 Java Web Start 或 Applet 模式中啓動 Proxylet ..... 214

**14 配置 NetFile** ..... 215
NetFile 配置作業 ..... 215
▼配置基本選項 ..... 215
▼配置存取權限 ..... 217
▼配置主機喜好設定 ..... 217
▼配置作業喜好設定 ..... 218
▼配置作業權限 ..... 219

**15 配置安全套接層加速器** ..... 221
加速器簡介 ..... 221
Sun Crypto Accelerator 1000 ..... 221
啓用 Crypto Accelerator 1000 ..... 222
Sun Crypto Accelerator 4000 ..... 224
啓用 Crypto Accelerator 4000 ..... 225
外部 SSL 裝置與代理伺服器加速器 ..... 227
▼啓用外部 SSL 裝置加速器 ..... 227
▼配置外部 SSL 裝置加速器 ..... 228

**第 3 部分　管理 Secure Remote Access 伺服器** ..... 229

**16　管理閘道** ..... 231
管理閘道的工作 ..... 231
▼建立閘道設定檔 ..... 231
▼使用相同的 LDAP 建立閘道實例 ..... 232
▼啓動閘道實例 ..... 233
▼停止閘道 ..... 233
▼使用管理主控台啓動與停止閘道 ..... 234
▼使用不同的設定檔重新啓動閘道 ..... 234
▼重新啓動閘道 ..... 234
▼指定虛擬主機 ..... 235
▼指定代理伺服器 ..... 235
▼建立 Netlet 代理伺服器實例 ..... 235
▼重新啓動 Netlet 代理伺服器 ..... 236
▼建立 Rewriter 代理伺服器實例 ..... 236
▼重新啓動 Rewriter 代理伺服器 ..... 237
▼啓用反向代理伺服器 ..... 237
▼新增認證模組到現有 PDC 實例 ..... 238
▼停用瀏覽器快取 ..... 239
▼共用 LDAP 目錄 ..... 239

**17　聯合管理方案** ..... 241
使用聯合管理 ..... 241
聯合管理方案 ..... 241
配置聯合管理資源 ..... 242
▼配置聯合管理資源 ..... 242
配置 1 ..... 242
配置 2 ..... 244
配置 3 ..... 245

**A　配置屬性** ..... 249
存取控制服務 ..... 249
閘道服務 ..... 250

核心 ..... 250
代理伺服器 ..... 252
安全性 ..... 252
Rewriter ..... 254
NetFile 服務 ..... 256
主機 ..... 256
權限 ..... 257
檢視 ..... 258
作業 ..... 258
一般 ..... 259
Netlet 服務 ..... 260
Proxylet 服務 ..... 261

**B 記錄檔** ..... 263
關於記錄檔 ..... 263

**C 國家代碼** ..... 265
國家代碼清單 ..... 265

**索引** ..... 275

# 圖清單


圖 1–1 開放模式下含 Secure Remote Access 的 Portal Server ..... 26
圖 1–2 安全模式下含 Secure Remote Access 的 Portal Server ..... 27
圖 2–1 Netlet 代理伺服器的實作 ..... 49
圖 6–1 Netlet 元件 ..... 130

# 表清單


表 2–1 檔案特性 ..... 35
表 2–2 在 [網域與子網域的代理伺服器] 清單中的對映項目 ..... 42
表 2–3 HTTP 標頭中的訊息 ..... 52
表 4–1 * 萬用字元的使用範例 ..... 74
表 4–2 Rewriter 除錯檔案 ..... 91
表 4–3 範例規則集與案例研究之間的對映 ..... 121
表 4–4 SP3 規則對映 ..... 123
表 5–1 檔案系統和支援的協定 ..... 126
表 6–1 Netlet 規則中的欄位 ..... 133
表 6–2 支援的密碼清單 ..... 137
表 6–3 Netlet 規則範例 ..... 143
表 10–1 憑證檔案 ..... 188
表 10–2 憑證信任屬性 ..... 189
表 10–3 公開憑證授權單位 ..... 189
表 15–1 Crypto Accelerator 1000 安裝檢核清單 ..... 222
表 15–2 Crypto Accelerator 4000 安裝檢核清單 ..... 225
表 A–1 存取控制服務屬性 ..... 249
表 A–2 閘道服務核心屬性 ..... 250
表 A–3 閘道服務代理伺服器屬性 ..... 252
表 A–4 閘道服務安全性屬性 ..... 253
表 A–5 閘道服務 Rewriter 屬性 - 基本 ..... 254
表 A–6 閘道服務 Rewriter 屬性 - 進階 ..... 255
表 A–7 NetFile 服務主機配置屬性 ..... 256
表 A–8 NetFile 服務主機存取屬性 ..... 257
表 A–9 NetFile 服務權限屬性 ..... 257
表 A–10 NetFle 服務檢視屬性 ..... 258
表 A–11 NetFile 服務作業 - 流量屬性 ..... 259
表 A–12 NetFile 服務作業 - 搜尋屬性 ..... 259

表 A–13 NetFile 服務作業 - 壓縮屬性 ..... 259
表 A–14 NetFile 服務 - 一般屬性 ..... 260
表 A–15 Netlet 服務屬性 ..... 260
表 A–16 Proxylet 服務屬性 ..... 262
表 B–1 資訊和除錯檔案 ..... 263
表 C–1 二字母國家代碼 ..... 265

# 範例清單

範例 4–1 重新寫入 URL ..... 61

# 前言

本指南說明如何管理 Sun Java™ System Portal Server Secure Remote Access 7.2 伺服器。

Sun Java System Portal Server Secure Remote Access (SRA) 伺服器可讓遠端使用者透過網際網路安全地存取其組織的網路及其服務。此外，SRA 還能爲您的組織提供安全的內部入口網站，並讓所有目標族群 (例如員工、事業夥伴或一般大眾) 都能夠存取其內容、應用程式及資料。

本前言包含下列各節：


- 第 17 頁的 「本書適用對象」
- 第 17 頁的 「閱讀本書之前」
- 第 18 頁的 「本書架構」
- 第 19 頁的 「相關書籍」
- 第 19 頁的 「其他伺服器文件」
- 第 20 頁的 「相關協力廠商網站參考」
- 第 21 頁的 「指令範例中的 Shell 提示符號」


## 本書適用對象

「Sun Java System Portal Server Secure Remote Access 7.2 管理指南」適用於配置與管理 Secure Remote Access 伺服器的使用者。

「Sun Java System Portal Server Secure Remote Access 7.2 管理指南」 假設您是在管理 UNIX 系統與 TCP/IP 網路方面具有豐富經驗的網路或系統管理員。即使不是超級使用者，您也可以存取需要的機器，以安裝 Secure Remote Access 伺服器的各種元件。您確實需要必要的管理權限才能執行其他作業，例如配置使用者與服務。

## 閱讀本書之前

Portal Secure Remote Access 伺服器管理員應瞭解下列技術：

- Sun Java System Portal Server
- Sun Java System Directory Server
- Sun Java System Access Manager

- 您的 Web 容器，例如：
  - Sun Java System Application Server 8.2
  - Sun Java System Web Server 7.0
- 您的作業系統
- 基本的 UNIX® 管理程序
- 簡易目錄存取協定 (Lightweight Directory Access Protocol, LDAP)
- 遠端 Portlet 的 Web 服務 (Web Services for Remote Portlets, WSRP)

您還需要達到下列要求才能撰寫 Rewriter 規則：

- 瞭解超文字標記語言 (Hypertext Markup Language, HTML) 與 HTML 標記
- 精通 JavaScript™
- 基本瞭解可延伸標記語言 (Extensible Markup Language, XML)

# 本書架構

本書架構如下：

- 第 1 部分
  - 第 1 章說明 Sun Java System Portal Server 與 Portal Server Secure Remote Access 的關係。
  - 第 2 章說明與閘道相關的概念以及管理閘道的工作。
  - 第 3 章說明可讓使用者不用剖析網頁就可透過閘道存取企業內部網路網頁的 Proxylet。
  - 第 4 章說明如何使用 Proxylet 與 Rewriter 來透過閘道存取企業內部網路網頁。
  - 第 5 章說明如何使用 NetFile 來存取與操作遠端檔案系統與目錄。
  - 第 6 章說明如何使用 Netlet 在不安全的網路 (例如網際網路) 上安全地執行一般 TCP/IP 服務。
- 第 2 部分
  - 第 7 章說明如何管理對 Portal Server 管理主控台的存取。
  - 第 8 章說明如何從 Portal Server 管理主控台配置閘道屬性。
  - 第 9 章說明如何使用 [Rewriter] 標籤下的閘道服務來執行不同的作業。
  - 第 10 章說明管理憑證與安裝來自憑證授權單位的自簽憑證。
  - 第 11 章說明從 Portal Server 管理主控台配置 Netlet 屬性。
  - 第 12 章說明配置用戶端瀏覽器的 Java 外掛程式以搭配 PDC 使用 Netlet。
  - 第 13 章說明從 Portal Server 管理主控台配置 Proxylet。
  - 第 14 章說明使用 Portal Server 管理主控台設定 NetFile 選項、權限與喜好設定。
  - 第 15 章說明配置 Portal Server Secure Remote Access 伺服器的各種加速器。
- 第 3 部分

- 第 16 章說明建立閘道設定檔與閘道實例的方法。
- 第 17 章說明維持網路身份的多種方案。

- 附錄 A 說明您可透過 Portal Server 管理主控台爲每個 Portal Server Secure Remote Access 元件配置的 Sun Java System Portal Server Secure Remote Access 屬性。
- 附錄 B 包含除錯與其他類型的資訊。
- 附錄 C 列出您需要在憑證管理期間指定的雙字母國家/地區代碼。

# 相關書籍

- 「Sun Java System Portal Server 7.2 Deployment Planning Guide」
- 「Sun Java System Portal Server 7.2 Technical Overview」
- 「Sun Java System Portal Server 7.2 管理指南」
- 「Sun Java System Portal Server 7.2 Command-Line Reference」
- 「Sun Java System Portal Server 7.2 版本說明」
- 「Sun Java System Portal Server 7.1 Community Sample Guide」
- 「Sun Java System Portal Server 7.2 Technical Reference」
- 「Sun Java System Portal Server 7.2 Developer's Guide」

有關 Portal Server 概念和元件的介紹，請參閱「Sun Java System Portal Server 7.2 Technical Overview」。

## 其他伺服器文件

如需其他伺服器文件，則請造訪：

- Directory Server 文件，網址爲 `http://docs.sun.com/coll/1224.1` 及 `http://docs.sun.com/coll/1632.1`
- Access Manager 文件，網址爲 `http://docs.sun.com/coll/1292.2` 及 `http://docs.sun.com/coll/1414.2`
- Web Server 文件，網址爲 `http://docs.sun.com/coll/1308.3` 及 `http://docs.sun.com/coll/1425.2`
- Application Server 文件，網址爲 `http://docs.sun.com/coll/1310.3` 及 `http://docs.sun.com/coll/1416.2`
- Web Proxy Server 文件，網址爲 `http://docs.sun.com/coll/1311.4` 及 `http://docs.sun.com/coll/1580.2`

# 相關協力廠商網站參考

本文件參照了協力廠商的 URL，以提供附加的相關資訊。

**備註 –** Sun 對於本文件中所提及之協力廠商網站的可用性不承擔任何責任。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。對於因使用或依賴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。

# 文件、支援和培訓

Sun 網站提供有關下列額外資源的資訊：

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

# 印刷排版慣例

下表說明本書使用的印刷排版慣例。

**表 P–1** 印刷排版慣例

| 字體 | 意義 | 範例 |
|---|---|---|
| `AaBbCc123` | 指令、檔案及目錄的名稱；螢幕畫面輸出。 | 請編輯您的 `.login` 檔案。<br>請使用 `ls -a` 列出所有檔案。<br>**電腦名稱**`% you have mail.` |
| **`AaBbCc123`** | 您所鍵入的內容 (與螢幕畫面輸出相區別)。 | **電腦名稱**`% su`<br>`Password:` |
| **術語強調變數** | 新的字彙或要強調的詞。將用實際的名稱或數值取代的指令行變數。 | **快取**是儲存在本機的副本。<br>不**要**儲存檔案。<br>**注意**：有些強調的項目在線上以粗體顯示。 |
| *AaBbCc123* | 保留未譯的新的字彙或要強調的詞。 | 移除檔案的指令是 **`rm`** *filename*。 |

表 P–1 印刷排版慣例 (續)

| 字體 | 意義 | 範例 |
| --- | --- | --- |
| 「AaBbCc123」 | 用於書名及章節名稱。 | 請閱讀「使用者指南」的第 6 章。 |

# 指令範例中的 Shell 提示符號

下表顯示了 C shell、Bourne shell 和 Korn shell 的預設 UNIX 系統提示符號以及超級使用者提示符號。

表 P–2 Shell 提示符號

| Shell | 提示符號 |
| --- | --- |
| C shell | **電腦名稱**% |
| C shell 超級使用者 | **電腦名稱**# |
| Bourne shell 與 Korn shell | $ |
| Bourne shell 與 Korn shell 超級使用者 | # |

第 1 部分

# Secure Remote Access 伺服器元件


- 第 1 章
- 第 2 章
- 第 3 章
- 第 4 章
- 第 5 章
- 第 6 章

◆ ◆ ◆ 第 1 章

# 1 Portal Server Secure Remote Access 伺服器簡介

本章說明 Sun Java™ System Portal Server Secure Remote Access 以及 Sun Java System Portal Server 與 Sun Java System Portal Server Secure Remote Access 元件間的關係。

本章涵蓋下列主題：


- 第 25 頁的 「Secure Remote Access 簡介」
- 第 27 頁的 「Secure Remote Access 服務」
- 第 29 頁的 「支援的應用程式」


## Secure Remote Access 簡介

Secure Remote Access 可讓遠端使用者透過網際網路安全地存取其組織的網路及其服務。此外，還能爲您的組織提供安全的網際網路入口網站，從而讓任何目標族群 (例如員工、事業夥伴或一般大眾) 都可存取內容、應用程式及資料。

Secure Remote Access 提供以瀏覽器爲基礎的安全遠端存取，以從任何遠端裝置存取入口網站內容與服務。Secure Remote Access 是一個安全的存取解決方案，使用者無需用戶端軟體就可從任何裝有啓用 Java™ 技術的瀏覽器的裝置對其進行存取。與 Portal Server 的整合能確保使用者可安全加密地存取他們有權存取的內容與服務。

Secure Remote Access 軟體適用於部署高度安全遠端存取入口網站的企業。這些入口網站重視企業內部網路資源的安全性、保護與隱私權。Secure Remote Access 架構非常適用於這些入口網站類型。Secure Remote Access 軟體能讓使用者安全地經由網際網路存取企業內部網路資源，而無需在網際網路上顯露這些資源。

Portal Server 可在兩種模式下操作：「開放模式」與「安全模式」，如下列小節所述。

# 開放模式

在開放模式中，Portal Server 安裝時未安裝 Secure Remote Access。雖然這個模式下可以使用 HTTPS 通訊，但卻不可以使用安全遠端存取。因此使用者無法存取安全遠端檔案系統與應用程式。

開放入口網站與安全入口網站的主要不同爲，由開放入口網站提供的服務通常會位於非軍事區 (DMZ) 而不會位於安全企業內部網路中。DMZ 是一個位於公用網際網路與私有企業內部網路之間的小型受保護網路，通常由兩端的防火牆劃分界線。

若入口網站沒有包含關於部署公用資訊與允許存取免費應用程式的敏感資訊，則對於大量使用者存取請求的回應將會快於使用安全模式。

在「開放模式」中，Portal Server 安裝於防火牆後的單一伺服器上。多個用戶端透過網際網路經由單一防火牆存取 Portal Server。

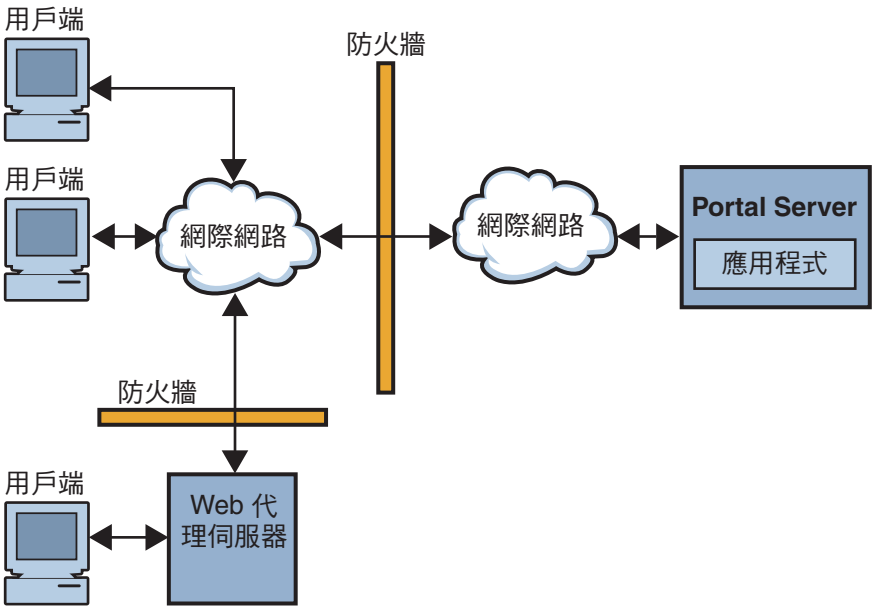



圖 1–1 開放模式下含 Secure Remote Access 的 Portal Server

# 安全模式

安全模式可讓使用者安全遠端存取需要的企業內部網路檔案系統與應用程式。

閘道位於非軍事區域 (DMZ)。閘道提供至所有企業內部網路 URL 與應用程式的單一安全存取點，如此會減少將在防火牆中被開放的連接埠數。所有其他 Portal Server 服務

(例如階段作業、認證與標準入口網站桌面) 皆位於 DMZ 之後的安全的企業內部網路中。用戶端瀏覽器至閘道的通訊將使用 HTTPS 透過安全套接層 (Secure Sockets Layer, SSL) 加密。閘道至伺服器與企業內部網路資源的通訊可使用 HTTP 或 HTTPS 加密。

在「安全模式」中，會使用 SSL 加密用戶端與閘道間的網際網路連線。SSL 也可以用於加密閘道與伺服器之間的連線。企業內部網路與網際網路之間的閘道將延伸用戶端與 Portal Server 之間的安全路徑。

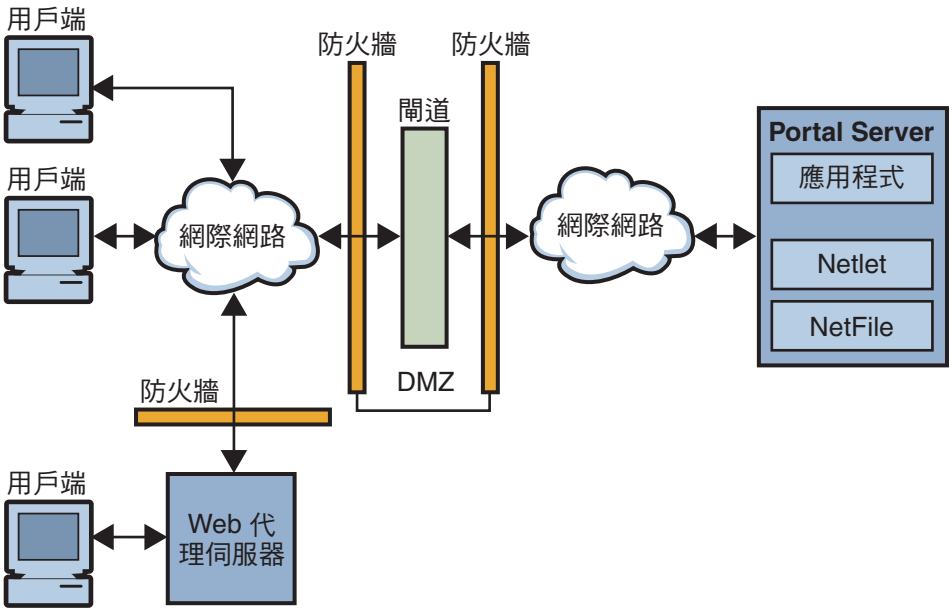



圖 1–2 安全模式下含 Secure Remote Access 的 Portal Server

可以新增其他伺服器與閘道以擴大網站。Secure Remote Access 軟體可以基於業務需求用不同方式配置。如需如何滿足業務需求的詳細資訊，請參閱「Sun Java System Portal Server 7.2 Deployment Planning Guid」。

# Secure Remote Access 服務

Secure Remote Access 軟體具有五個主要元件：

- **閘道**

  SRA 閘道在源自網際網路的遠端使用者階段作業與您的企業內部網路之間提供了介面與安全的屏障。閘道可透過單一介面，將來自內部 Web 伺服器和應用程式伺服器的內容安全地顯示給遠端使用者。

Web 伺服器使用以 Web 爲基礎的資源 (例如 HTML、JavaScript 與 XML) 以在用戶端與閘道之間進行通訊。Rewriter 是用於使 Web 內容可用的閘道元件。

應用程式伺服器會使用二進制通訊協定例如 telnet 與 FTP 以在用戶端與閘道之間進行通訊。位於閘道的 Netlet 就是基於這個目的而使用。請參閱第 2 章以取得詳細資訊。

- **Rewriter**

  Rewriter 會讓一般使用者可以瀏覽企業內部網路並使得那些頁面的連結與其他 URL 參照正確作業。Rewriter 會在 Web 瀏覽器位置欄位中前置閘道 URL，藉此經由閘道重新導向內容請求。請參閱第 4 章以取得詳細資訊。

- **Netfile**

  NetFile 是一個檔案管理應用程式，可遠端存取與操作檔案系統和目錄。NetFile 包括以 Java 爲基礎的使用者介面。請參閱第 5 章以取得詳細資訊。

- **Netlet**

  Netlet 能更方便地以安全方式在遠端桌面執行熱門應用程式與公司特定應用程式。在網站實施 Netlet 之後，使用者可以安全執行共用的 TCP/IP 服務，例如 Telnet 與 SMTP，和以 HTTP 爲基礎的應用程式例如 pcANYWHERE 或 Lotus Notes。請參閱第 6 章以取得詳細資訊。

- **Proxylet**

  Proxylet 是一個在用戶端機器上執行的動態代理伺服器。Proxylet 讀取並修改用戶端機器上瀏覽器的代理伺服器設定使其指向本地代理伺服器或 Proxylet，從而將 URL 重新導向至閘道。

# 配置 Secure Remote Access 屬性

您可在 Portal Server 管理主控台中使用下列服務配置 Secure Remote Access 屬性：

- 存取控制

  這個服務可讓您允許或拒絕存取特定的 URL 並管理單次登入功能。如需詳細資訊，請參閱第 7 章。

- 閘道

  設定檔 (閘道實例)。此服務可讓您配置所有與閘道相關的屬性，例如啓用元件、Cookie 管理、代理伺服器管理、安全性設定、效能調校、Rewriter 對映管理等。如需詳細資訊，請參閱第 8 章。

- NetFile

  這個服務可讓您配置所有與 NetFile 相關的屬性，例如共用主機、MIME 類型並存取不同類型的主機。如需詳細資訊，請參閱第 14 章。

- Netlet

  這個服務可讓您配置所有與 Netlet 相關的屬性，例如 Netlet 規則、存取需要的規則、組織與主機以及預設演算法。如需詳細資訊，請參閱第 11 章。

- Rewriter

  此服務可讓您下載、上傳與刪除所有 Rewriter 規則集。

- Proxylet

  此服務能夠讓您配置 Proxylet 相關的屬性，例如 Proxylet Applet 連結 IP 位址與連接埠號。如需詳細資訊，請參閱第 13 章。

**注意 –** 閘道在執行時不會接收屬性變更的通知。重新啓動閘道，以讓更新的設定檔屬性 (屬於閘道或其他任何服務) 生效。如需詳細資訊，請參閱第 172 頁的「使用指令行選項配置閘道屬性」。

# 設定衝突解決

## ▼ 設定衝突解決層級

1. **登入 Portal Server 管理主控台。**
2. **選取 [Secure Remote Access] 標籤，並按一下必要的服務標籤：Netlet、Netfile 或 Proxylet。**
3. **從 [選取 DN] 下拉式功能表選取 [組織] 或 [角色]。**
4. **從 [COS 優先順序] 下拉式方塊中，選取必要的 [衝突解決層級]。**
5. **按一下 [儲存] 完成作業。**

# 支援的應用程式

SRA 支援下列應用程式：

- Sun Java System Calendar Server Release 5.1.1 及更新版
- Sun Java System Messenger Express 6 2005Q1 - Sun Java System Messaging Server 5.2 及更新版
- Sun Java System Communications Express 6 2005Q1

## 在您開始前

### ▼ 啓用入口網站的 SRA

1. 使用 `PortalServer_base/psadmin switch-sra-status -u amadmin -f <passwordfile> on` 指令切換 SRA 狀態。

2. 使用 `PortalServer_base/psadmin provision-sra -u amadmin -f <passwordfile> -p <portal-id> --gateway-profile <profile-name> --enable` 指令佈建 SRA 狀態。

◆ ◆ ◆ 第 2 章

# 使用閘道

本章說明與閘道相關的概念。如需管理閘道的資訊，請參閱第 16 章。如需配置閘道的資訊，請參閱第 8 章。

本章涵蓋下列主題：


- 第 31 頁的 「閘道簡介」
- 第 34 頁的 「了解 platform.conf 檔案」
- 第 39 頁的 「使用 Web 代理伺服器」
- 第 45 頁的 「使用自動代理伺服器配置」
- 第 47 頁的 「使用 Netlet 代理伺服器」
- 第 50 頁的 「使用 Rewriter 代理伺服器」
- 第 51 頁的 「使用含有閘道的反向代理伺服器」
- 第 52 頁的 「取得用戶端資訊」
- 第 53 頁的 「使用認證鏈接」
- 第 54 頁的 「使用萬有字元憑證」
- 第 54 頁的 「停用瀏覽器快取」
- 第 54 頁的 「自訂閘道服務使用者介面」


## 閘道簡介

閘道在源自網際網路的遠端使用者階段作業與您的企業內部網路之間提供了介面與安全的屏障。透過單一介面至遠端使用者，閘道可經由內部 Web 伺服器和應用程式伺服器安全地顯示內容。

針對每個閘道實例，您必須完成下列工作：

- 第 32 頁的 「建立閘道設定檔」
- 第 32 頁的 「建立多個閘道實例」
- 第 8 章

其他與閘道相關的主題包含：

- 第 33 頁的 「重新啓動閘道」
- 第 33 頁的 「配置閘道監視程式」
- 第 33 頁的 「指定虛擬主機」
- 第 33 頁的 「指定代理伺服器以連絡 Access Manager」


# 建立閘道設定檔

閘道設定檔包含與閘道配置相關的所有資訊，如閘道偵聽的連接埠、SSL 選項及代理伺服器選項。安裝閘道時，如果選擇預設值，則會建立稱爲「default」的預設閘道。與預設設定檔對應的配置檔會出現在：`/etc/opt/SUNWportal/platform.conf.default`。

其中 `/etc/opt/SUNWportal` 是所有 `platform.conf.*` 檔案的預設位置。如需 `platform.conf` 檔案的詳細資訊，請參閱第 34 頁的 「了解 platform.conf 檔案」。

使用設定檔時，您可執行下列作業：

- 建立多個設定檔，定義每個設定檔的屬性，並視需要指定這些設定檔給不同的閘道。
- 在不同的機器上指定單一設定檔給閘道安裝。
- 指定不同的設定檔給在相同機器上執行的單一閘道實例。

**注意 –** 不要指定相同的設定檔給在相同機器上執行的閘道不同實例。該設定將會造成衝突，因爲連接埠號碼相同。

不要在不同的設定檔 (建立給相同的閘道) 中指定相同的連接埠號碼。以同樣的連接埠執行相同閘道的多重實例會造成衝突。

# 建立多個閘道實例

要建立閘道的多個實例，請參閱「Sun Java System Portal Server 7.2 Installation and Configuration Guide」中的第 4 章「Installing and Configuring a Gateway With Portal Server」。

## 建立多址閘道實例

多重介面閘道實例是一個 Portal Server 上的多重閘道。要建立這些實例，請將 `platform.conf` 檔案修改如下：

```
gatewaybindipaddress = 0.0.0.0
```

## 使用相同的 LDAP 建立閘道實例

如果您建立的是使用相同 LDAP 的多重閘道實例，在所有隨後的閘道上建立第一個閘道之後：

在 /etc/opt/SUNWam/config/ 中，修改 AMConfig-*instance-name*.properties 的下列區域，使其與第一個安裝的閘道實例一致。

請參閱第 232 頁的 「使用相同的 LDAP 建立閘道實例」

# 重新啓動閘道

一般而言，您不需要重新啓動閘道。只有發生下列事件時，才需要重新啓動閘道：

- 您已經建立新的設定檔並且需要指定此新的設定檔給閘道。
- 您已經在現有的設定檔中修改一些屬性，並且需要變更以使其生效。
- 閘道由於出現錯誤 (如記憶體不足) 而當機。
- 閘道停止回應，且不服務任何請求。

# 配置閘道監視程式

您可以配置監視程式監視閘道狀態的時間間隔。要啓動或停止監視程式，請執行 ./psadmin sra-watchdog -u amadmin -f <password-file> -t <type> on|off 指令。時間間隔預設爲 60 秒。要變更此值，可在 crontab 公用程式中編輯下列行：

```
0-59 * * * * gateway-install-root/SUNWportal/bin/
/var/opt/SUNWportal/.gw. 5 > /dev/null 2>&1
```

請參閱 crontab 的線上手冊以配置 crontab 項目。

# 指定虛擬主機

虛擬主機是指向相同機器 IP 和主機名稱的額外主機名稱。例如，如果一個主機名稱 abc 指向主機 IP 位址 192.155.205.133，您可新增另一個主機名稱 cde 指向相同的 IP 位址。

# 指定代理伺服器以連絡 Access Manager

您可以指定閘道用以連絡部署在 Portal Server 上的 SRA 核心支援 (RemoteConfigServlet) 的代理伺服器主機。閘道使用此代理伺服器連絡 Portal Server 與 Access Manager。請參閱第 235 頁的 「指定代理伺服器」。

# 了解 platform.conf 檔案

預設情況下，platform.conf 檔案位於：/etc/opt/SUNWportal。

platform.conf 檔案包含閘道所需的詳細資訊。本節提供一個範例 platform.conf 檔案，並說明所有的項目。

在配置檔中包含所有機器特定詳細資訊的優點，就是共用的設定檔可以被在多個機器上執行的閘道共享。

以下是 platform.conf 檔案的範例。

```
Tue May 30 11:51:23 IST 2006
debug.com.sun.portal.rewriter.original.level=INFO
gateway.favicon=
gateway.bindipaddress=10.12.154.236
debug.com.sun.portal.sra.rproxy.toFromServer.handler.java.util.logging.FileHandler.pattern=
/var/opt/SUNWportal/logs/sra/default/Gateway.toFromServer.%u.%g.log
gateway.port=443
rewriterproxy.jvm.flags=-ms64m -mx128m
portal.server.instance=default
debug.com.sun.portal.handler.java.util.logging.FileHandler.filter=
gateway.jdk.dir=/usr/jdk/entsys-j2se
gateway.ignoreURIList=/MSOffice/cltreq.asp,/_vti_bin/owssvr.dll
debug.com.sun.portal.rewriter.rest.level=INFO
gateway.trust_all_server_certs=true
debug.com.sun.portal.handler.java.util.logging.FileHandler.append=true
gateway.cdm.cacheCleanupTime=300000
gateway.httpurl=
debug.com.sun.portal.handler.java.util.logging.FileHandler.count=1
gateway.jvm.classpath=
debug.com.sun.portal.setserverlogs=false
gateway.protocol=https
debug.com.sun.portal.sra.rproxy.toFromServer=java.util.logging.FileHandler
rewriterproxy.jvm.classpath=
gateway.enable.customurl=false
debug.com.sun.portal.sra.rproxy.toFromBrowser=java.util.logging.FileHandler
debug.com.sun.portal.handler.java.util.logging.FileHandler.formatter=com.sun.portal.
log.common.PortalLogFormatter
debug.com.sun.portal.sra.rproxy.toFromBrowser.handler.java.util.logging.FileHandler.pattern=
/var/opt/SUNWportal/logs/sra/default/Gateway.toFromBrowser.%u.%g.log
debug.com.sun.portal.level=INFO
debug.com.sun.portal.rewriter.unaffected.separatefile=true
gateway.enable.accelerator=false
debug.com.sun.portal.rewriter.original.separatefile=true
gateway.virtualhost=nicp236.india.sun.com 10.12.154.236
debug.com.sun.portal.stacktrace=true
gateway.host=nicp236.india.sun.com
```

```
debug.com.sun.portal.handler.java.util.logging.FileHandler.pattern=
/var/opt/SUNWportal/logs/sra/default/%logger.%sraComponentType.%u.%g.log
gateway.certdir=/etc/opt/SUNWportal/cert/default
gateway.sockretries=3
gateway.allow.client.caching=true
debug.com.sun.portal.rewriter.unaffected.level=INFO
debug.com.sun.portal.rewriter.uriinfo.separatefile=true
log.config.check.period=2000
debug.com.sun.portal.rewriter.rewritten.level=INFO
gateway.userProfile.cacheSize=1024
debug.com.sun.portal.rewriter.rulesetinfo.level=INFO
netletproxy.jvm.classpath=
gateway.userProfile.cacheSleepTime=60000
debug.com.sun.portal.rewriter.uriinfo.level=INFO
debug.com.sun.portal.rewriter.rest.separatefile=true
gateway.notification.url=notification
debug.com.sun.portal.rewriter.rulesetinfo.separatefile=true
gateway.logdelimiter=&&
gateway.ignoreServerList=false
gateway.jvm.flags=-ms64m -mx128m
debug.com.sun.portal.handler.java.util.logging.FileHandler.limit=5000000
gateway.dsame.agent=http\://sunone216.india.sun.com\:8080/portal/RemoteConfigServlet
gateway.httpsurl=
gateway.retries=6
gateway.userProfile.cacheCleanupTime=300000
gateway.logging.password=X03MO1qnZdYdgyfeuILPmQ\=\= UX9x0jIua3hx1YOVRG/TLg\=\=
netletproxy.jvm.flags=-ms64m -mx128m
debug.com.sun.portal.rewriter.rewritten.separatefile=true
gateway.user=noaccess
gateway.external.ip=10.12.154.236
debug.com.sun.portal.handler=java.util.logging.FileHandler
gateway.cdm.cacheSleepTime=60000
rewriterproxy.accept.from.g
ateways=
rewriterproxy.checkacl=false
```

下列表格列出並說明 `platform.conf` 檔案中所有的欄位。

**表 2–1** 檔案特性

| 項目 | 預設值 | 描述 |
|---|---|---|
| `gateway.user` | noaccess | 閘道以此使用者執行。<br>閘道必須做爲超級使用者啓動，並且在初始化後，它會失去超級使用者權限而成爲此使用者。 |
| `gateway.jdk.dir` | | 這是閘道所使用之 JDK 目錄的位置。 |

表 2–1 檔案特性 (續)

| 項目 | 預設值 | 描述 |
|---|---|---|
| gateway.dsame.agent | | 當閘道啓動要取得其設定檔時，這是閘道會連絡 Access Manager 的 URL。 |
| portal.server.protocol<br>portal.server.host<br>portal.server.port | | 這是預設 Portal Server 安裝使用的通訊協定、主機和連接埠。 |
| gateway.protocolgateway.hostgateway.port | | 這是閘道的通訊協定、主機和連接埠。這些值與您在安裝時所指定的模式和連接埠相同。這些值用於建立通知 URL。 |
| gateway.trust_all_server_certs | true | 這表示閘道必須相信所有的伺服器憑證，或僅相信在閘道憑證資料庫中的伺服器憑證。 |
| gateway.trust_all_server_cert_domains | false | 當閘道和伺服器之間有 SSL 通訊時，會提供伺服器憑證給閘道。在預設情況下，閘道會檢查伺服器主機名稱是否與伺服器憑證 CN 相同。<br>如果屬性值設定爲 true，則閘道會停用它收到之伺服器憑證的網域名稱檢查。 |
| gateway.virtualhost | | 如果閘道機器有配置多個主機名稱，您可以在此欄位指定不同的名稱和識別提供者位址。 |
| gateway.virtualhost.defaultOrg=org | | 這會指定預設的 Org 給登入的使用者。<br>例如，假設虛擬主機欄位項目如下所示：<br>gateway.virtualhost=test.com employee.test.com<br>Managers.test.com<br>含有預設的 org 項目爲：<br>test.com.defaultOrg = o=root,dc=test,dc=com<br>employee.test.com.defaultOrg = o=employee,dc=test,dc=com<br>Manager.test.com.defaultOrg = o=Manager,dc=test,dc=com<br>使用者可以使用 https://manager.test.com 而非 https://test.com/o=Manager,dc=test,dc=com 以登入管理員的 org。<br>**備註** – virtualhost 和 defaultOrg 在 platform.conf 檔案中區分大小寫，但用於 URL 時則沒有區分。 |

表 2–1 檔案特性 (續)

| 項目 | 預設值 | 描述 |
|---|---|---|
| gateway.notification.url | | 閘道主機、通訊協定和連接埠的組合，用於建立通知 URL。用於從 Access Manager 接收階段作業通知。<br>請確定通知 URL 和任何組織的名稱不相同。如果通知 URL 和組織名稱相同，則使用者在嘗試連結到該組織時會看到空白頁面而非登入的頁面。 |
| gateway.retries | | 此數字是在啓動時，閘道嘗試連絡 Portal Server 的次數。 |
| gateway.debug | error | 設定閘道的除錯層級。除錯記錄檔位於 *debug-directory*/files。除錯檔案的位置在 gateway.debug.dir 項目中指定。<br>除錯層級爲：<br>■ error - 只會在除錯檔案中記錄幾個錯誤。在此種錯誤發生時，閘道通常會停止運作。<br>■ warning - 記錄警告訊息。<br>■ message - 記錄所有的除錯訊息。<br>■ on - 在主控台顯示所有的除錯訊息。<br>除錯檔案爲：<br>srapGateway.*gateway-profile-name* - 包含閘道的除錯訊息。<br>Gateway_to_from_server.*gateway-profile-name* - 在訊息模式下，此檔案包含閘道和內部伺服器之間所有的需求和回應標頭。<br>要產生此檔案，請變更 /var/opt/SUNWps/debug 目錄的寫入權限。<br>Gateway_to_from_browser.*gateway-profile-name* - 在訊息模式下，此檔案包含閘道和用戶端瀏覽器之間所有的需求和回應標頭。<br>要產生此檔案，請變更 /var/opt/SUNWps/debug 目錄的寫入權限。 |
| gateway.debug.dir | | 這是所有除錯檔案產生的目錄。<br>此目錄必須有足夠的權限以將 gateway.user 中提到的使用者寫入檔案。 |
| gateway.logdelimiter | | 目前沒有使用。 |
| gateway.external.ip | | 如果是在多址閘道機器上 (使用多重 IP 位址的機器)，您需要在此指定外部 IP 位址。此 IP 用於執行 FTP 的 Netlet。 |
| gateway.certdir | | 它指定憑證資料庫的位置。 |

表 2–1 檔案特性 (續)

| 項目 | 預設值 | 描述 |
|---|---|---|
| gateway.allow.client.caching | true | 允許或拒絕用戶端快取。<br>如果允許，用戶端瀏覽器可以快取靜態頁面和影像以取得較佳的效能 (藉由減低網路流量)。<br>如果拒絕，因爲沒有任何快取，安全性會更高，但是會因爲有較高的網路負載而導致效能落差。 |
| gateway.userProfile.cacheSize | | 這是在閘道上使用者設定檔項目被快取的數目。如果項目數量超過這個值，常用的項目會清除快取。 |
| gateway.userProfile.cacheSleepTime | | 以秒爲單位設定休息時間，以清除快取。 |
| gateway.userProfile.cacheCleanupTime | | 超過以秒爲單位的最大數字的時間後，會移除設定檔項目。 |
| gateway.bindipaddress | | 在多址機器上，這是閘道連結其 serversocket 的 IP 位址。要配置閘道偵聽所有介面，請置換 IP 位址以使 gateway.bindipaddress=0.0.0.0。 |
| gateway.sockretries | 3 | 目前沒有使用。 |
| gateway.enable.accelerator | false | 如果設定爲 true，則允許支援外部加速器。 |
| gateway.enable.customurl | false | 如果設定爲 true，則允許管理員指定一個自訂的 URL 讓閘道重新寫入頁面。 |
| gateway.httpurl | | 自訂 URL 的 HTTP reverse proxy URL 讓閘道重新寫入頁面。啓用 Proxylet 時請使用此項目。 |
| gateway.httpsurl | | 自訂 URL 的 HTTPS reverse proxy URL 讓閘道重新寫入頁面。如果啓用 Proxylet，請勿使用此項目。 |
| gateway.favicon | | 閘道將 favicon.icon 檔請求重新導向到的 URL。<br>此項目用於 Internet Explorer、Netscape 7.0 和更高版本中的「favorite icon」。<br>如果此項目保持空白，閘道會傳送一個「404 頁面找不到」的訊息給瀏覽器。 |
| gateway.logging.password | | 使用者 amService-srapGateway 的 LDAP 密碼，閘道會使用它來建立其應用程式階段作業。<br>密碼可以是加密文字或一般文字。 |
| http.proxyHost | | 代理伺服器主機會用於連絡 Portal Server。 |
| http.proxyPort | | 主機連接埠會用於連絡 Portal Server。 |

表 2–1 檔案特性 (續)

| 項目 | 預設值 | 描述 |
|---|---|---|
| http.proxySet | | 若需要代理伺服器，則屬性會設定爲 true。若特性設定爲 false，則會忽略 http.proxyHost 與 http.proxyPort。 |
| portal.server.*instance* | | 此特性值對應於 /etc/opt/SUNWam/config/AMConfig *-instance-name*.properties 檔案。如果值是預設值，則會指向 AMConfig.properties。 |
| gateway.cdm.cacheSleepTime | 60000 | 快取「用戶端偵測模組」回應的逾時值從 Access Manager 傳送到閘道。 |
| gateway.cdm.cacheCleanupTime | 300000 | 快取「用戶端偵測模組」回應的逾時值從 Access Manager 傳送到閘道。 |
| netletproxy.port | 10555 | Netlet 代理伺服器預設程式會偵聽此連接埠上的請求。 |
| rewriterproxy.port | 10555 | Rewriter 代理伺服器預設程式會偵聽此連接埠上的請求。 |
| gateway.ignoreServerList | false | 如果設定爲 true，會使用 AMConfig.properties 檔案中指定的值來建立 Access Manager 伺服器 URL。當 Access Manager 伺服器位於負載平衡器之後時，請將此屬性設定爲 true。 |
| rewriterproxy.accept.from.gateways | | 這是 IP 位址的清單，可將 Rewriter 代理伺服器設定爲接受來自該清單的請求。此屬性對 HTTP 與 HTTPS 模式均適用。它可加強安全性，僅接受來自此集合的請求，而不會處理所有其他的請求。IP 位址可使用逗點分隔。預設值是空的，被視爲舊有模式，亦即會尊重到 Rewriter 代理程式的所有請求。 |
| rewriterproxy.checkacl= | false | 啓用此特性可讓 Rewriter 代理伺服器檢查 ACL 值，就像閘道一樣。舊有模式值是「false」。當將此值設定爲 true 時，Rewriter 代理伺服器會在指定 DN 根據在閘道存取服務中指定的值檢查 URL，且會依據此處設定之清單集合來允許/拒絕請求。此值在 HTTP 與 HTTPS 模式中都有用。 |

# 使用 Web 代理伺服器

您可以使用協力廠商 Web 代理伺服器配置閘道以連絡 HTTP 資源。Web 代理伺服器位於客戶端與網際網路之間。

## Web 代理伺服器配置

不同的代理伺服器可能用於不同的網域和子網域。這些項目告訴閘道在特定的網域中，應該使用哪個代理伺服器以連絡特定的子網域。指定在閘道中的代理伺服器配置運作方式如下：

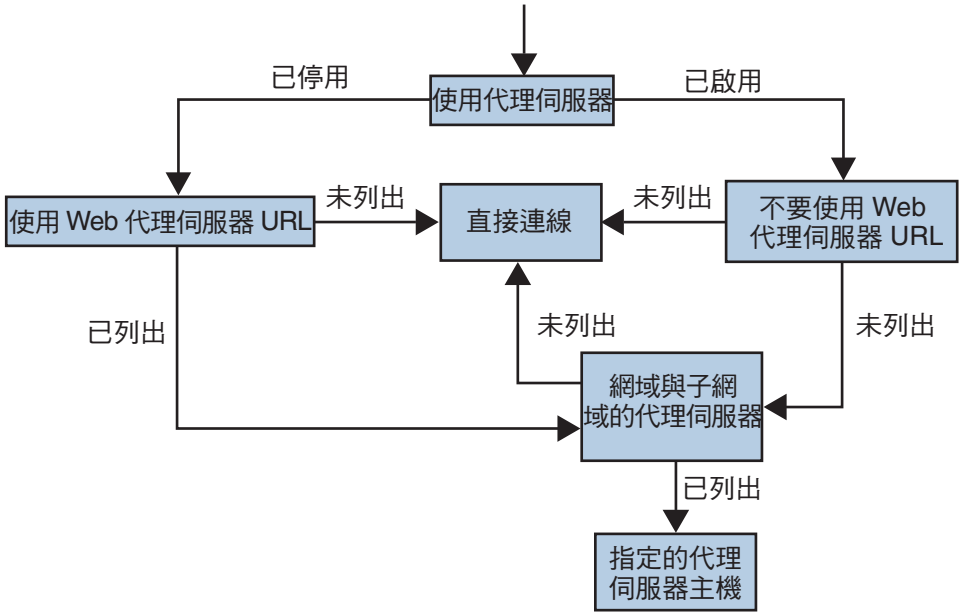
- 在閘道服務中，建立一個清單，其中包含網域和子網域，以及 [網域與子網域的代理伺服器] 欄位中必要的代理伺服器。

- 當 [使用代理伺服器] 選項啓用時：
  - 在 [網域與子網域的代理伺服器] 欄位所指定的代理伺服器會用於指定的主機。
  - 要在網域和子網域 (在 [網域與子網域的代理伺服器] 清單中指定的) 中啓用某些 URL 的直接連線，請在 [請勿使用 Web 代理伺服器 URL] 欄位中指定這些 URL。

  當 [使用代理伺服器] 選項停用時：
  - 要確認在網域和子網域 (在 [網域與子網域的代理伺服器] 欄位中指定的) 中某些 URL 使用代理伺服器，請在 [使用網路代理伺服器的 URL] 清單中指定這些 URL。

    雖然停用 [使用代理伺服器] 功能但仍可使用代理伺服器連接到列於 [使用 Web 代理伺服器] 清單下的 URL。這些 URL 的代理伺服器是從 [網域與子網域的代理伺服器] 清單中取得。

    下列圖例顯示如何以閘道服務中的代理伺服器配置爲基礎來解決 Web 代理伺服器的訊息。




在第 39 頁的 「Web 代理伺服器配置」中，如果啓用了 [使用代理伺服器]，且所需的 URL 列於 [請勿使用 Web 代理伺服器 URL] 清單中，則閘道會直接連到目標主機。

如果 [使用代理伺服器] 是啓用的，且要求的 URL 未列於 [請勿使用 Web 代理伺服器 URL] 清單中，則閘道會透過指定的代理伺服器連到目標主機。此代理伺服器 (如果有指定) 可以從 [網域與子網域的代理伺服器] 清單中查看。

如果 [使用代理伺服器] 停用，且請求的 URL 有列於 [使用 Web 代理伺服器] 清單中，則閘道會使用列在 [網域與子網域的代理伺服器] 清單中的代理伺服器資訊連接目標主機。

如果 [使用代理伺服器] 是停用的，且要求的 URL 未列於 [請勿使用 Web 代理伺服器 URL] 清單中，則閘道會直接連線到目標主機。

如果您的情況不符合上述任何一項，且無法使用直接連線，閘道會顯示一個錯誤，說明連線無法使用。

---

**備註 –** 如果您正透過標準入口網站桌面的 [書籤通道] 存取該 URL，且您的情況不符合上述任何一項，閘道會傳送重新導向給瀏覽器。瀏覽器會使用自己的代理伺服器設定來存取該 URL。

---

## 語法

```
domainname [web_proxy1:port1]|subdomain1 [web_proxy2:port2]|
```

## 範例

```
sesta.com wp1:8080|red wp2:8080|yellow|* wp3:8080
```

* 是與任何結果都相符的萬用字元

其中，

`sesta.com` 是網域名稱而 `wp1` 是在 8080 連接埠上用於連絡的代理伺服器。

`red` 是子網域而 `wp2` 是在 8080 連接埠上用於連絡的代理伺服器。

`yellow` 是子網域。由於沒有指定代理伺服器，因此會使用指定給網域的代理伺服器，即爲在 8080 連接埠上的 `wp1`。

* 表示所有其他子網域必須在 8080 連接埠上使用 `wp3`。

---

**備註 –** 如果您沒有指定連接埠，預設是使用連接埠 8080。

---

## 處理網路代理伺服器資訊

當用戶端嘗試存取特定 URL 時，URL 中的主機名稱會與 [網域與子網域的代理伺服器] 清單中的項目進行比較。符合請求主機名稱之最長字尾的項目會被考慮。例如，假設請求的主機名稱是 `host1.sesta.com`。會依序進行下列搜尋，直到找到符合的結果。

- 會掃描 host1.sesta.com 的網域和子網域的代理伺服器。如果找到符合的項目，指定給此項目的代理伺服器會用來連接此主機。
- 否則，會掃描清單中的 *.sesta.com。如果找到符合的項目，會使用對應的代理伺服器。
- 否則，會尋找清單中的 sesta.com。如果找到符合的項目，會使用對應的代理伺服器。
- 否則，會尋找清單中的 *.com。如果找到符合的項目，會使用對應的代理伺服器。
- 否則，會尋找清單中的 com。如果找到符合的項目，會使用對應的代理伺服器。
- 否則，會尋找清單中的 *。如果找到符合的項目，會使用對應的代理伺服器。
- 如果找不到符合的項目，就會嘗試直接連線。

考慮 [網域與子網域的代理伺服器] 清單中的下列項目：

```
com p1| host1 p2 | host2 | * p3
sesta.com p4 | host5 p5 | * p6
florizon.com | host6
abc.sesta.com p8 | host7 p7 | host8 p8 | * p9
host6.florizon.com p10
host9.sesta.com p11
siroe.com | host12 p12 | host13 p13 | host14 | * p14
siroe.com | host15 p15 | host16 | * p16
* p17
```

閘道會將這些項目內部對應至如下列表格中顯示的表格。

**表 2–2** 在 [網域與子網域的代理伺服器] 清單中的對映項目

| 編號 | [網域與子網域的代理伺服器] 清單中的項目 | 代理伺服器 | 描述 |
|---|---|---|---|
| 1 | com | p1 | 指定於清單中。 |
| 2 | host1.com | p2 | 指定於清單中。 |
| 3 | host2.com | p1 | 由於沒有爲 host2 指定代理伺服器，會使用網域的代理伺服器。 |
| 4 | *.com | p3 | 指定於清單中。 |
| 5 | sesta.com | p4 | 指定於清單中。 |
| 6 | host5.sesta.com | p5 | 指定於清單中。 |
| 7 | *.sesta.com | p6 | 指定於清單中。 |
| 8 | florizon.com | 直接 | 如需詳細資訊，請參閱第 14 項的描述。 |
| 9 | host6.florizon.com | – | 如需詳細資訊，請參閱第 14 項的描述。 |

表 2–2 在 [網域與子網域的代理伺服器] 清單中的對映項目 *(續)*

| 編號 | [網域與子網域的代理伺服器] 清單中的項目 | 代理伺服器 | 描述 |
|---|---|---|---|
| 10 | abc.sesta.com | p8 | 指定於清單中。 |
| 11 | host7.abc.sesta.com | p7 | 指定於清單中。 |
| 12 | host8.abc.sesta.com | p8 | 指定於清單中。 |
| 13 | *.abc.sesta.com | p9 | 指定於清單中。在 `abc.sesta.com` 網域下，所有主機 (`host7` 和 `host8` 除外) 都會使用 `p9` 作爲代理伺服器。 |
| 14 | host6.florizon.com | p10 | 與第 9 個項目相同。第 9 個項目表示直接連線，而此項目表示應該使用代理伺服器 10。若遇到像這樣有兩個項目的情況，含有代理伺服器資訊的項目會視爲有效的項目。請忽略另一個項目。 |
| 15 | host9.sesta.com | p11 | 指定於清單中。 |
| 16 | siroe.com | 直接 | 由於沒有指定 `siroe.com` 的代理伺服器，因此會嘗試直接連線。 |
| 17 | host12.siroe.com | p12 | 指定於清單中。 |
| 18 | host13.siroe.com | p13 | 指定於清單中。 |
| 19 | host14.siroe.com | 直接 | 由於沒有指定 `host14` 的代理伺服器，因此會嘗試直接連線。 |
| 20 | *.siroe.com | p14 | 請參閱第 23 項描述。 |
| 21 | host15.siroe.com | p15 | 指定於清單中。 |
| 22 | host16.siroe.com | 直接 | 由於沒有指定 host16 或 `siroe.com` 的代理伺服器，因此會嘗試直接連線。 |
| 23 | *.siroe.com | p16 | 與第 20 個項目類似，但是指定的代理伺服器不同。這種情形下，無法知道閘道的實際運作方式。可能會使用兩個代理伺服器中的任意一個。 |
| 24 | * | p17 | 如果沒有其他的項目符合請求的 URL，就會使用 `p17` 作爲代理伺服器。 |

**提示 –** 與其在 [網域與子網域的代理伺服器] 清單中以 | 分隔代理項目，不如將個別的項目放置在清單的不同行中。例如取代如下的項目：

```
sesta.com p1 | red p2 | * p3
```

您指將此資訊指定爲：

```
sesta.com p1
red.sesta.com p2
*.sesta.com p3
```

此清單格式更容易追蹤重複項目或任何其他含糊的情況。

## 以 [網域與子網域的代理伺服器] 清單為基礎重新寫入

[網域與子網域的代理伺服器] 清單中的項目也會被 Rewriter 使用。網域符合列在 [網域與子網域的代理伺服器] 清單中網域的所有 URL，Rewriter 會重新寫入。

**注意 –** 在 [網域與子網域的代理伺服器] 清單中的 * 項目不會考慮重新寫入。例如，不會考慮項目 24。

如需 Rewriter 的資訊，請參閱第 4 章。

## 預設網域與子網域

當在 URL 中的目標主機不是完整限定的主機名稱，會使用預設的網域和子網域以使其有完整合格的名稱。

假設管理主控台中 [預設網域] 欄位內的項目是：

```
red.sesta.com
```

**備註 –** 在 [網域與子網域的代理伺服器] 清單中您必須要有對應的項目。

在上面的範例中，`sesta.com` 是預設的網域而 `red` 是預設的子網域。

如果要求的 URL 是 `host1`，則會使用預設的網域和子網域將此項目解析爲 `host1.red.sesta.com`。然後會在 [網域與子網域的代理伺服器] 清單中查詢 `host1.red.sesta.com`。

# 使用自動代理伺服器配置

要忽略 [網域與子網域的代理伺服器] 清單中的資訊，請啓用 [自動代理伺服器配置] 功能。

使用自動代理伺服器配置 (Proxy Auto Configuration, PAC) 檔案時：

- Portal Server、閘道、Netlet 與 Proxylet 使用 *Rhino* 軟體來剖析 PAC 檔案。您可以從 Java Enterprise System Accessory CD 安裝 `SUNWrhino` 套裝軟體。

  此套裝軟體包含 `js.jar` 檔案，其必須位於 `/usr/share/lib` 目錄。將此目錄新增到閘道和 Portal Server 機器上的 `webserver/appserver` 類別路徑，否則 Portal Server、閘道、Netlet 以及 Proxylet 無法剖析 PAC 檔案。
- `js.jar` 必須位於閘道機器上的 `$JRE_HOME/lib/ext` 目錄中，否則閘道無法剖析 PAC 檔案。
- 啓動時，閘道從閘道設定檔的「自動代理伺服器配置檔案」位置欄位中指定的位置取得 PAC 檔案。
- 閘道使用 URLConnection API 到達此位置。如果需要配置代理伺服器以到達閘道，必須以下列方式配置代理伺服器：

  1. 從指令行中，編輯下列檔案：

     `/etc/opt/SUNWportal/platform.conf.`*gateway-profile-name*
  2. 新增下列項目：

     `http.proxyHost=` *web-proxy-hostname*

     `http.proxyPort=` *web-proxy-port*

     `http.proxySet=true`
  3. 重新啓動閘道以使用指定的代理伺服器：

     `./psadmin start-sra-instance –u amadmin – f <`*password file*`> –N <`*profile name*`>– t <`*gateway*`>`
- 如果 PAC 檔案初始化失敗，閘道會使用 [網域與子網域的代理伺服器] 清單中的資訊。
- 如果從 PAC 檔案傳回「」空字串或「null」，閘道會假設該主機不屬於此企業內部網路。這與不在 [網域與子網域的代理伺服器] 清單中之主機的情況類似。

  如果您想要閘道使用直接連線連到主機，請返回到「DIRECT」。請參閱第 46 頁的「含有傳回 DIRECT 或 NULL 的範例」。
- 當指定多個代理伺服器時，閘道僅使用第一個返回的代理伺服器。閘道不會在指定給主機的多個代理伺服器之間嘗試修復錯誤或負載平衡。
- 閘道忽略 SOCKS 代理伺服器並嘗試直接連線，同時假設該主機是企業內部網路的一部分。

- 要指定代理伺服器，讓其通往任何不屬於內部企業網路的主機，請使用代理伺服器類型 STARPROXY。此代理伺服器類型是 PAC 檔案格式的延伸，與在閘道設定檔的 [網域與子網域的代理伺服器] 部分中的 `* proxyHost:port` 項目相似。請參閱第 46 頁的「含有傳回 STARPROXY 的範例」。

# 使用範例 PAC 檔案

下列範例顯示列在 [網域與子網域的代理伺服器] 清單中的 URL 和對應的 PAC 檔案。

## 含有傳回 DIRECT 或 NULL 的範例

如果將這些代理伺服器用於網域與子網域：

```
*intranet1.com proxy.intranet.com:8080

intranet2.com proxy.intranet1.com:8080
```

相對應的 PAC 檔案是：

```
// Start of the PAC File
function FindProxyForURL(url, host) {
         if (dnsDomainIs(host, ".intranet1.com")) {
             return "DIRECT";
         }
          if (dnsDomainIs(host, ".intranet2.com")) {
              return "PROXY proxy.intranet1.com:8080";
          }
          return "NULL";
}
//End of the PAC File
```

## 含有傳回 STARPROXY 的範例

如果將這些代理伺服器用於網域與子網域：

```
intranet1.com

intranet2.com.proxy.intranet1.com:8080

internetproxy.intranet1.com:80
```

相對應的 PAC 檔案是：

```
// Start of the PAC File
function FindProxyForURL(url, host) {
          if (dnsDomainIs(host, ".intranet1.com")) {
              return "DIRECT";
```

```
        }
        if (dnsDomainIs(host, ".intranet2.com")) {
            return "PROXY proxy.intranet1.com:8080;" +
                "PROXY proxy1.intranet1.com:8080";
        }
        return "STARPROXY internetproxy.intranet1.com:80";
}
//End of the PAC File
```

在這個情況下，如果請求的主機位於 .intranet2.com 網域，則閘道會連絡 proxy.intranet1.com:8080。如果 proxy.intranet1.com:8080 無法使用，請求會失敗。閘道不會進行容錯移轉與連絡 proxy1.intranet1.com:8080。

## 指定 PAC 檔案位置

用來指定 PAC 檔案位置的格式需視下列位置而定：

- 如果 PAC 檔案位於 Web 伺服器上，則 PAC URL 爲：

  http://hostname/*pacfile_name* .pac
- 如果 PAC 檔案是本機檔案 (例如，c:\\pacfile\\sample.pac)，則在 java 1.4.1_x 中，PAC URL 的輸入格式爲：

  file://c:/pacfile/sample.pac
- 如果 PAC 檔案是本機檔案 (例如，c:\\pacfile\\sample.pac)，則在 java 1.4.2_x 中，PAC URL 的輸入格式爲：

  file:///c:/pacfile/sample.pac

# 在個別階段作業中新增服務

當在個別階段作業中新增 Portal Server 服務時：

- 在 Portal Server 管理主控台中的 [閘道] > [核心] 下列出 Portal Server。
- 在 [閘道] > [安全性] 下的 [非認證 URL] 中列出 Portal Server URL。

# 使用 Netlet 代理伺服器

Netlet 封包在閘道是解密的，並會傳送到目標伺服器。然而，閘道需要透過非軍事區 (DMZ) 和企業內部網路之間的防火牆，存取所有的 Netlet 目的地主機。此設定需要在防火牆中開啓大量的連接埠。Netlet 代理伺服器可用於最小化在防火牆中開啓的連接埠數目。

藉由延伸用戶端的安全通道，透過閘道到存在於企業內部網路的 Netlet 代理伺服器，Netlet 強化閘道和企業內部網路之間的安全性。使用代理伺服器，Netlet 封包會由代理伺服器解密，之後會傳送至目的地。

使用 Netlet 代理伺服器的優點：

- 新增額外的安全性層級。
- 在大規模的部署環境中，最大程度減少閘道透過內部防火牆使用額外 IP 位址和連接埠的情況。
- 限制閘道和入口伺服器之間開啓的連接埠數目爲 1。此連接埠號碼可在安裝期間配置。
- 延伸客戶端和閘道之間的安全通道，最多可延伸到 Portal Server，如第 47 頁的 「使用 Netlet 代理伺服器」中的 [包含配置的 Netlet 代理伺服器] 部分所示。透過資料加密，Netlet 代理伺服器提供強化的安全益處，但可能會增加系統資源的使用。如需安裝 Netlet 代理伺服器的資訊，請參閱「Sun Java System 安裝指南」。

您可執行下列作業：

- 在 Portal Server 節點上或個別節點上安裝 Netle 代理伺服器。
- 使用管理主控台安裝多個 Netlet 代理伺服器並配置給單一閘道。這對負載平衡很有用。
- 在單一機器上配置多個 Netlet 代理伺服器實例。
- 將閘道的多重實例指向 Netlet 代理伺服器的單一安裝。
- 通道 Netlet 會透過 Web 代理伺服器。

顯示在有和沒有安裝 Netlet 代理伺服器的情況下，閘道和 Portal Server 的三個範例實作。元件包含一個用戶端、兩個防火牆、位於兩個防火牆之間的閘道、Portal Server 和 Netlet 目標伺服器。

第一個方案顯示沒有安裝 Netlet 代理伺服器的閘道和 Portal Server。資料加密僅從用戶端延伸到閘道。在第二防火牆中開啓一個連接埠給每個 Netlet 連線請求。

第二個方案顯示在 Portal Server 上安裝 Netlet 代理伺服器的閘道和 Portal Server。資料加密從用戶端一直延伸到 Portal Server。既然所有 Netlet 連線都是通過 Netlet 代理伺服器傳送的，在 Netlet 請求中的第二防火牆只需要開啓一個連接埠。

第三個方案顯示有在個別節點上安裝 Netlet 代理伺服器的閘道和 Portal Server。在個別節點上安裝 Netlet 代理伺服器會減少 Portal Server 節點上的負載。同樣的，在第二個防火牆中僅需要開啓兩個連接埠。其中一個連接埠提供給 Portal Server 使用，另一個連接埠傳送 Netlet 請求到 Netlet 代理伺服器伺服器。

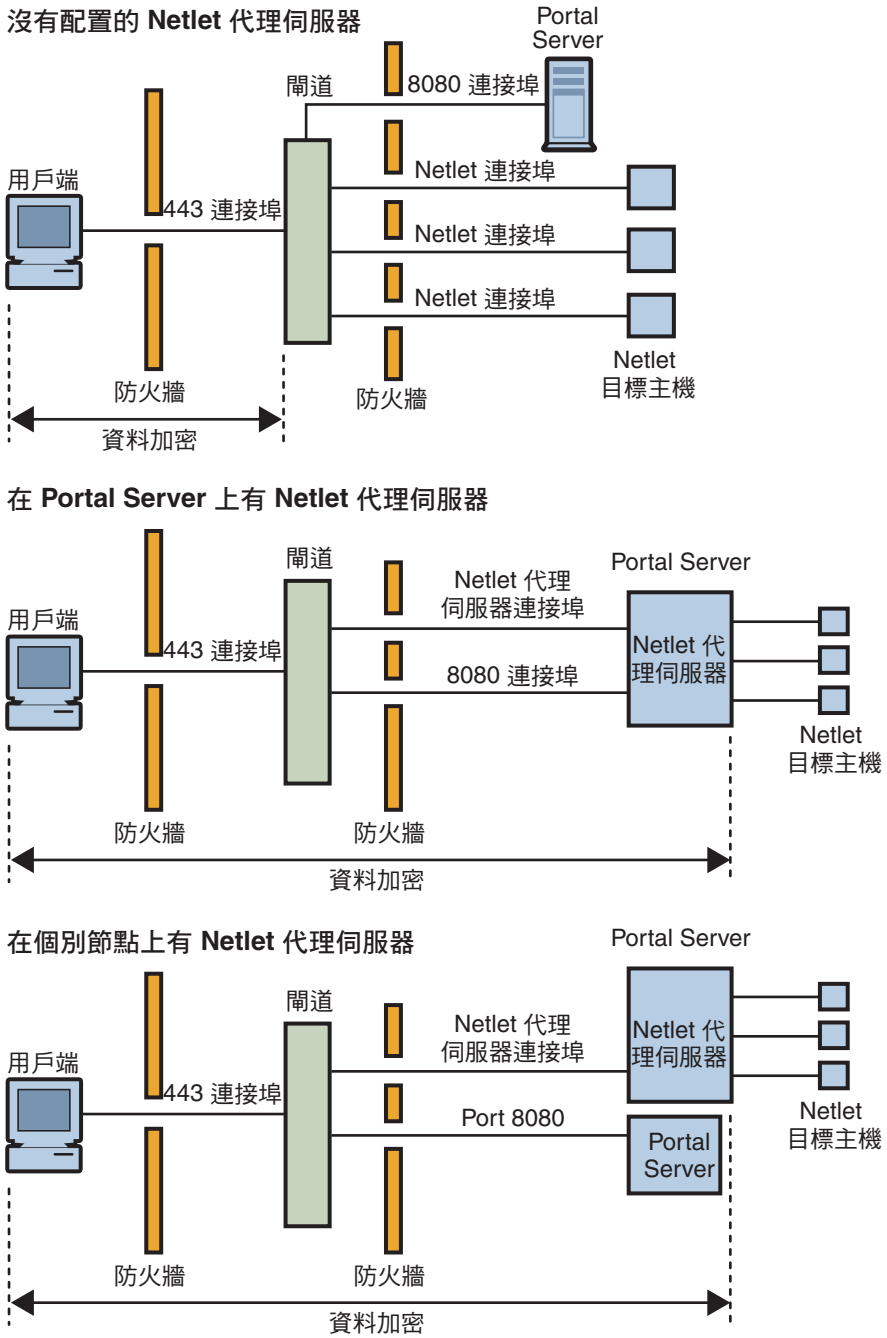



圖 2–1 Netlet 代理伺服器的實作

## 啓用 Netlet 代理伺服器

您可使用 Portal Server 管理主控台透過閘道服務啓用 Netlet 代理伺服器。

## 重新啓動 Netlet 代理伺服器

每次代理伺服器意外結束時，您可以配置 Netlet 代理伺服器以重新啓動。您可排程監視程式程序，以監視 Netlet 代理伺服器，並且在它當機時重新啓動。

您也可以手動重新啓動 Netlet 代理伺服器。請參閱第 236 頁的 「重新啓動 Netlet 代理伺服器」以取得步驟。

### 配置 Netlet 代理伺服器監視程式

您可以配置監視程式監視 Netlet 代理伺服器狀態的時間間隔。時間間隔預設爲 60 秒。要變更此時間間隔，請將下列行新增至 `crontab` 檔案：

0-59 * * * * *netlet-install-dir*`/bin/checkgw /var/opt/SUNWportal/.gw 5 > /dev/null 2>&1`

---

**備註 –** 要啓動或停止監視程式，請執行 `./psadmin sra-watchdog -u amadmin -f <password-file> -t <type> on|off` 指令。

---

# 使用 Rewriter 代理伺服器

Rewriter 代理伺服器安裝於企業內部網路中。閘道不會直接嘗試擷取內容，而是將所有請求轉寄給 Rewriter 代理伺服器，由代理伺服器獲取並傳回內容給閘道。

使用 Rewriter 代理伺服器的優點有：

- 如果在閘道和伺服器之間有防火牆，防火牆必須開啓兩個連接埠 - 一個在閘道和 Rewriter 代理伺服器之間，另一個在閘道與 Portal Server 之間。
- 在閘道和企業內部網路間的 HTTP 流量很安全，即使目標伺服器僅支援 HTTP 通訊協定 (不支援 HTTPS)。

如果您沒有指定 Rewriter 代理伺服器，當使用者嘗試存取企業內部網路的其中一台電腦，閘道元件會直接連線至企業內部網路的電腦。

如果您使用 Rewriter 代理伺服器作爲負載平衡器，請確定 Rewriter 的 `platform.conf.instance_name` 指向負載平衡器 URL。在 Portal Server 清單中指定負載平衡器主機。

如果每個閘道實例 (不一定要在入口節點上) 都有 Rewriter 代理伺服器的多個實例，請在 `platform.conf` 檔案中以 *host-name:port* 格式來提供每個 Rewriter 代理伺服器的詳細資訊，而非 Rewriter 代理伺服器的單一連接埠項目。

## 建立 Rewriter 代理伺服器的實例

使用 `rwpmultiinstance` 程序檔，在 Portal Server 節點上建立 Rewriter 代理伺服器的新實例。請在建立閘道設定檔之後執行此程序檔。

請參閱第 236 頁的 「建立 Rewriter 代理伺服器實例」 。

## 啓用 Rewriter 代理伺服器

在 Access Manager 管理主控台中，在「SRA 配置」下透過閘道服務啓用 Rewriter 代理伺服器。

## 重新啓動 Rewriter 代理伺服器

每次代理伺服器意外結束時，您可以配置重新啓動 Rewriter 代理伺服器。您可排程監視程式程序以監視，並在發生這種情況時重新啓動。

您也可以手動重新啓動 Rewriter 代理伺服器。

請參閱第 237 頁的 「重新啓動 Rewriter 代理伺服器」 。

### 配置 Rewriter 代理伺服器監視程式

您可以配置監視程式監視 Rewriter 代理伺服器狀態的時間間隔。時間間隔預設爲 60 秒。要變更時間間隔，請將下列行新增至 `crontab` 檔案：

0-59 * * * * *rewriter-proxy-install-root* `/bin/checkgw /var/opt/SUNWportal/.gw 5 > /dev/null 2>&1`

---

**備註 –** 要啓動或停止監視程式，請執行 `./psadmin sra-watchdog -u amadmin -f <password-file> -t <type> on|off` 指令。

---

# 使用含有閘道的反向代理伺服器

代理伺服器會傳送網際網路內容至企業內部網路，而反向代理伺服器則傳送企業內部網路內容至網際網路。您可配置反向代理伺服器的部署，以實現負載平衡與快取。

若在閘道前面部署具有協力廠商反向代理伺服器，則回應必須以反向代理伺服器的 URL ( 非閘道的 URL) 重新寫入。因此需要下列配置。

請參閱第 237 頁的 「啓用反向代理伺服器」 。

# 取得用戶端資訊

當閘道轉寄用戶端請求至任何內部伺服器時，會新增 HTTP 標頭至 HTTP 請求。您可以使用這些標頭以取得額外的用戶端資訊並偵測閘道的出現狀態。

要檢視 HTTP 請求標頭，請將 `platform.conf` 檔案中的項目設定爲 `gateway.error=message`。然後使用 servlet API 中的 `request.getHeader()`。以下表格列出 HTTP 標頭中的資訊。

**表 2–3** HTTP 標頭中的訊息

| 標頭 | 語法 | 描述 |
|---|---|---|
| PS-GW-PDC | `X-PS-GW- PDC: true/false` | 指出閘道上的 PDC 是否啓用。 |
| PS-Netlet | `X-PS-Netlet:enabled=true/false` | 指出閘道上的 Netlet 是否已經啓用或停用。<br>如果已經啓用 Netlet，則加密選項會寫入，指出閘道以 HTTPS (`encryption=ssl`) 或以 HTTP 模式 (`encryption=plain`) 執行。<br>例如：<br>■ `PS-Netlet: enabled=false`<br>Netlet 是停用的。<br>■ `PS-Netlet: enabled=true; encryption=ssl`<br>Netlet 使用在 SSL 模式中執行的閘道啓用。<br>未啓用 Netlet 時，不會寫入 `encryption=ssl` 或 `encryption=plain`。 |
| PS-GW-URL | `X-PS-GW-URL: http(s)://gatewayURL(:port)` | 指出用戶端要連接的 URL。<br>連接埠爲非標準連接埠時，例如，如果閘道爲 HTTP/HTTPS 模式且連接埠並非 80/443，那麼也會寫入 `:port`。 |

**表 2–3** HTTP 標頭中的訊息 (續)

| 標頭 | 語法 | 描述 |
|---|---|---|
| PS-GW-Rewriting-URL | `X-PS-GW-URL: http(s)://gatewayURL(:port) /[SessionInfo]` | 指出閘道重新寫入所有頁面的 URL。<br>1. 當瀏覽器支援 cookie 時，此標頭的值和 PS-GW-URL 標頭的值一樣。<br>2. 當瀏覽器不支援 cookie 時：<br>■ 並且如果目標主機在 [轉寄使用者階段作業 Cookie 到的使用者階段作業] 欄位中，則值是閘道重新寫入頁面的實際 URL (含有編碼 SessionID 資訊)。<br>■ 或者，如果目標主機不在 [轉寄使用者階段作業 Cookie 到的使用者階段作業] 欄位中，則 `SessionInfo` 字串是 `$SessionID`。<br>**備註 –** 在回應部分，如果使用者的 Access Manager sessionId 變更 (如來自認證頁面的回應)，則會以該值重新寫入這些頁面 (此值並非是先前在標頭中所指的值)。<br>例如：<br>■ 如果瀏覽器支援 cookie：<br>PS-GW-Rewriting-URL: https://siroe.india.sun.com:10443/<br>■ 如果瀏覽器不支援 cookie，且終端伺服器位於 [轉寄使用者階段作業 Cookie 到的使用者階段作業] 欄位中。<br>PS-GW-Rewriting-URL: https://siroe.india.sun.com:10443/SessIDValCustomEncodedValue/<br>■ 如果瀏覽器不支援 cookie，且終端伺服器不在 [轉寄使用者階段作業 Cookie 到的使用者階段作業] 欄位中。<br>PS-GW-Rewriting-URL: https://siroe.india.sun.com:10443/$SessionID |
| PS-GW-CLientIP | `X-PS-GW-CLientIP:` *IP* | 指示閘道從 `recievedSocket.getInetAddress().getHostAddress()` 所取得的 IP。<br>如果直接連到閘道，此值會提供用戶端的 IP。 |

# 使用認證鏈接

認證鏈接提供比一般機制更高層級的安全性。您可以讓使用者認證一個以上的認證機制。

此處的程序說明僅適用於在閘道同時啓用認證鏈接與「個人數位憑證」(Personal Digital Certificate, PDC) 認證。如需在閘道上沒有 PDC 認證的認證鏈接的資訊，請參閱「Access Manager 管理指南」。

例如，如果您取得 PDC 和 Radius 認證模組，使用者將必須認證這三個模組以存取標準入口網站桌面。

請參閱第 238 頁的 「新增認證模組到現有 PDC 實例」以取得步驟。

**備註 –** 如果啓用 PDC，它永遠都是第一個顯示在使用者面前的認證模組。

# 使用萬有字元憑證

萬用字元憑證接受含有萬用字元的單一憑證，該憑證必須位於擁有完全合格 DNS 名稱的主機中。

使用憑證可以在相同網域中維護多個主機的安全性。例如，`*.domain.com` 的憑證可以用於 `abc.domain.com` 和 `abc1.domain.com`。事實上，此憑證對於在 `domain.com` 網域中的任何主機都有效。

# 停用瀏覽器快取

由於可透過閘道元件僅使用 Web 瀏覽器從任何地方安全地存取後端公司資料，因此用戶端不應該在本機對資訊進行快取。

您可以修改指定閘道在 `platform.conf` 中檔案的屬性，以停用透過閘道快取重新導向的頁面。

停用此選項對閘道效能有影響。每次標準入口網站桌面更新時，閘道必須擷取頁面參照的每個東西，例如先前瀏覽器已經快取過的影像。然而，啓用這個功能後，遠端存取安全的內容將不會在用戶端網站留下快取過的痕跡。如果是從網咖或類似的遠端位置 (不在企業 IT 的控制下) 存取企業網路，此因素可能比效能問題更爲重要。

請參閱第 239 頁的 「停用瀏覽器快取」。

# 自訂閘道服務使用者介面

本節討論可以編輯的各種閘道特性檔案。

## 修改 srapGateway.properties 檔案

因下列用途您可以編輯此檔案：

- 自訂在閘道執行時可能會出現的錯誤訊息。
  - HTML-CharSets=ISO-8859-1 指定用於建立此檔案的字元集。

- 在大括號中的數字 (例如，{0}) 表示在執行期間顯示的值。您可以變更和此數字有關的標籤，或視需要重新整理標籤。請確定標籤和將顯示的訊息對應，因爲數字是和訊息相關聯的。

自訂記錄資訊。

在預設情況下，`srapGateway.properties` 檔案位於 *portal-server-install-root* `/SUNWportal/locale` 目錄中。所有出現在閘道機器上的訊息都在此檔案中，無論訊息的語言爲何。

要變更出現在用戶端標準入口網站桌面上之訊息的語言，請將此檔案複製到對應語言環境的目錄中，例如 *portal-server-install-root*`/SUNWportal/locale_en_US`。

### 修改 srapgwadminmsg.properties 檔案

因下列原因您可以編輯此檔案：

- 自訂出現在管理主控台上閘道服務之按鈕的標籤。
- 自訂當您配置閘道時，會出現的狀態訊息和錯誤訊息。

## 共用 LDAP 目錄

當 Portal Server 及 Access Manager 伺服器的兩個實例共用相同的 LDAP 目錄時，所有後續的 Portal Server、Access Manager 及閘道的實例都會共用相同的 LDAP 目錄。請參閱第 239 頁的「共用 LDAP 目錄」。

◆ ◆ ◆ 第 3 章

# 3 使用 Proxylet

本章說明可讓使用者透過閘道而非剖析網頁來存取企業內部網路網頁的 Proxylet。

# 使用 Proxylet

## Proxylet 摘要

Proxylet 是一個 Java applet，它將其本身設定爲用戶端機器上的代理伺服器。Proxylet 會讀取並修改用戶端機器上自動代理伺服器配置 (Proxy Auto Config, PAC) 檔案中的代理伺服器設定，將代理伺服器設定指向本地的代理伺服器 (Proxylet)。

Proxylet 從閘道繼承傳輸模式。如果已經將閘道配置爲在 SSL 上執行，Proxylet 會在用戶端機器與閘道或目標伺服器之間建立一個安全的通道。爲了加密目的，如果用戶端 JVM 爲 1.4 或更新版本，或者如果必要的 jar 檔是位於用戶端機器中，Proxylet 會使用 JSSE API。否則它會使用 KSSL API。解密會在用戶端機器上執行。

被導向至閘道的 URL 的網域和子網域已在閘道設定檔中指定。如果 URL 並不是閘道處理的部份網域，則請求會導向至網際網路。如果在閘道設定檔中有列出特定的 URL 網域，則 Proxylet 會將用戶端代理伺服器設定重設爲閘道點。

如果在閘道啓用個人數位憑證 (Personal Digital Certificate, PDC)，Proxylet 會支援用戶端認證。要檢查是否已啓用 PDC，請參閱第 52 頁的 「取得用戶端資訊」。

Proxylet 透過 Portal Server 管理主控台啓用，也可在管理主控台指定用戶端 IP 位址或代理伺服器主機名稱與連接埠。如果已啓用 Proxylet，它會針對用戶端機器檢查下列資訊：

- 適當的瀏覽器權限
- 瀏覽器是否爲 IE 6.0 sp2、IE 7 與 Firefox 2.0
- 機器或裝置是否可執行伺服器應用程式

如果滿足所有的要求，就會下載 applet 並在用戶端機器上啓動它。如果用戶端沒有安裝 JRE 1.4.2 或更新版本，當您具有網際網路連線及管理權限時，用戶端就會透過 Proxylet 自動下載 JRE。

使用 Proxylet 時，它會從自動代理程式配置 (Proxy Auto Configuration, PAC) 檔案或代理程式配置清單中擷取代理程式設定。

**備註 –** 確定使用者瞭解必須在使用 Proxylet applet 時，停用瀏覽器快顯式阻擋程式。

## HTTPS 支援

Proxylet 支援 HTTPS，可完成以下作業：

- 在用戶端伺服器完成解密。
- 可存取在 SSL 模式下執行的目標伺服器。
- 直接將用戶端憑證提供給目標伺服器。
- 閘道不支援基本驗證單次登入 (SSO)。(閘道無法將單次登入資訊插入 http 標頭)。
- 不支援基於 URL 的存取控制，僅支援基於主機的存取控制。
- 目前不支援在閘道前方設置外部加速器和外部反向代理伺服器。

**備註 –** 如果 Portal Server 使用 HTTPS，則不支援 Proxylet。

## 使用 Proxylet 的優點

不同於 Rewriter，Proxylet 安裝後很少需要或不需要變更。與協力廠商軟體 (例如 Microsoft Exchange Server) 的整合也非常容易。由於 Proxylet 不會接觸 Web 內容，閘道的效能也有所增加。因爲 Proxylet 不會修改內容或變更資料，使用者可以下載任何類型的內容，例如 `tar` 與 `gzip` 檔案。

## 配置 Proxylet

如需啓用與配置 Proxylet 的詳細資訊，請參閱第 13 章。

**備註 –** 如果使用者沒有用來執行 Proxylet 的適當 Java Virtual Machine (JVM)，請用瀏覽器連線至 Sun 網站下載 Java Runtime Environment。如果使用者的瀏覽器設定並未包含正確的值，或如果使用者在使用直接代理伺服器而未存取至網際網路，則無法下載 Proxylet。

◆ ◆ ◆ 第 4 章

# 4 使用 Rewriter

Secure Remote Access 的 Rewriter 元件可讓使用者透過剖析網頁，經由閘道來存取企業內部網路的網頁。

本章涵蓋下列主題：


- 第 62 頁的 「字元集編碼」
- 第 62 頁的 「Rewriter 使用方案」
- 第 63 頁的 「撰寫規則集」
- 第 63 頁的 「公開介面 (規則集 DTD)」
- 第 90 頁的 「使用除錯記錄檔排除故障」
- 第 63 頁的 「公開介面 (規則集 DTD)」
- 第 93 頁的 「工作範例」
- 第 119 頁的 「案例研究」
- 第 123 頁的 「6.x 與 3.0 規則集對映」


## Rewriter 簡介

Secure Remote Access 的 Rewriter 元件能讓一般使用者利用修改網頁上的統一資源識別碼 (Uniform Resource Identifier, URI) 參照，以指向閘道從而瀏覽企業內部網路。URI 可定義於任何已註冊名稱空間內封裝名稱的方法，並以該名稱空間爲其加標記。最常見的 URI 類別爲單一資源定址器 (Uniform Resource Locator, URL)。Rewriter 僅支援 HTTP 或 HTTPS。不論協定的大小寫爲何都支援。Rewriter 僅支援相對 URL 中包含反斜線符號。

**範例 4–1** 重新寫入 URL

`http://abc.sesta.com\\index.html` 會被重新寫入。

這些 URL 不會被重新寫入：`http:\\\\abc.sesta.com`。 *http:/abc.com*

# 字元集編碼

HTTP 標準需要 HTTP 標頭或 HTML 中繼標記爲網頁指定字元集。但是有時候此資訊沒有辦法使用。字元集必須爲已知，如此資料編碼的設定以及資料的顯示才會依照建立的想法進行。

要偵測字元集，請從 Java Enterprise System Accessory CD 安裝 SUNWjchdt 套裝軟體。如果已安裝此產品，Rewriter 將會偵測到它並在需要時使用。

---

**備註 –** 使用此產品將會影響效能，因此應該只在需要時才安裝此產品。如需安裝、配置與用法的詳細資訊，請參閱 jcharset_readme.txt。

---

# Rewriter 使用方案

使用者試圖經由閘道存取企業內部網路網頁時，即可使用 Rewriter 來順利存取網頁。URLScraper 與閘道會使用 Rewriter。

## URLScraper

URL Scraper 提供者會從配置的 URI 取得內容。將這些 URI 傳送至瀏覽器前，它會將所有相對 URI 展開爲絕對 URI。

例如，如果使用者嘗試用下列方式存取網站：

```
<a href="../mypage.html">
```

Rewriter 會將此轉譯爲：

```
<a href="http://yahoo.com/mypage.html">
```

其中 http://yahoo.com/test/ 是網頁的基準 URL。

如需 URLScraper 提供者的詳細資訊，請參閱「Sun Java System Portal Server 管理指南」。

## 閘道

閘道從網際網路入口網站獲取內容。將內容傳送至瀏覽器前，它會將閘道 URI 置於目前的 URI 之前，如此來自瀏覽器的後續 URI 請求都可到達閘道。

例如，如果使用者試圖用以下方式存取網際網路機器上的 HTML 網頁：

```
<a href="http://mymachine.intranet.com/mypage.html>"
```

Rewriter 會引用閘道置於這個 URL 之前，如下所示：

```
<a href="https://gateway.company.com/http://mymachine.intranet.com/ mypage.html>"
```

使用者點選與此控點相關的連結時，瀏覽器便會連絡閘道。閘道會從 `mymachine.intranet.com` 取得 `mypage.html` 的內容。

閘道使用多種規則來判定是否需重新寫入取得網頁中的元素。

# 撰寫規則集

如需定義規則集的詳細資訊，請參閱「Portal Server 管理指南」。在建立新規則集後，您必須定義必要的規則。

本節涵蓋下列主題：


- 第 63 頁的「公開介面 (規則集 DTD)」
- 第 65 頁的「XML DTD 範例」
- 第 66 頁的「撰寫規則的步驟」
- 第 66 頁的「規則集指導方針」
- 第 67 頁的「定義規則集根元素」
- 第 67 頁的「使用遞迴功能」
- 第 68 頁的「HTML 內容的規則」
- 第 74 頁的「JavaScript 內容的規則」
- 第 87 頁的「XML 內容的規則」
- 第 90 頁的「Cascading Style Sheet (串接樣式表) 的規則」
- 第 90 頁的「WML 的規則」


## 公開介面 (規則集 DTD)

規則集 DTD：

```
<?xml version="1.0" encoding="UTF-8"?>
<!--
The following constraints are not represented in DTD, but taken care of programmatically
    1. In a Rule, All Mandatory attributes cannot be "*".
    2. Only one instance of the below elements is allowed, but in any order.
    1)HTMLRules
    2)JSRules
    3)XMLRules
    3. ID should always be in lower case.
-->
<!ENTITY % eURL 'URL'>
<!ENTITY % eEXPRESSION 'EXPRESSION'>
<!ENTITY % eDHTML 'DHTML'>
<!ENTITY % eDJS 'DJS'>
<!ENTITY % eSYSTEM 'SYSTEM'>
```

```
<!ENTITY % ruleSetElements '(HTMLRules | JSRules | XMLRules)?'>
<!ENTITY % htmlElements '(Form | Applet | Attribute)*'>
<!ENTITY % jsElements '(Variable | Function)*'>
<!ENTITY % xmlElements '(Attribute | TagText)*'>

<!ELEMENT RuleSet (%ruleSetElements;,%ruleSetElements;,%ruleSetElements;)>
<!ATTLIST RuleSet
    id ID #REQUIRED
    extends CDATA "none"
>

<!-- Rules for identifying rules in HTML content -->
<!ELEMENT HTMLRules (%htmlElements;)>
<!ELEMENT Form EMPTY>
<!ATTLIST Form
    name CDATA #REQUIRED
    field CDATA #REQUIRED
    valuePatterns CDATA ""
    source CDATA "*"
>

<!ELEMENT Applet EMPTY>
<!ATTLIST Applet
    code CDATA #REQUIRED
    param CDATA "*"
    valuePatterns CDATA ""
    source CDATA "*"
>

<!-- Rules for identifying rules in JS content -->
<!ELEMENT JSRules (%jsElements;)>
<!ELEMENT Variable EMPTY>
<!ATTLIST Variable
    name CDATA #REQUIRED
    type (%eURL; | %eEXPRESSION; | %eDHTML; | %eDJS; | %eSYSTEM;) "EXPRESSION"
    source CDATA "*"
>

<!ELEMENT Function EMPTY>
<!ATTLIST Function
    name CDATA #REQUIRED
    paramPatterns CDATA #REQUIRED
    type (%eURL; | %eEXPRESSION; | %eDHTML; | %eDJS;) "EXPRESSION"
    source CDATA "*"
>

<!-- Rules for identifying rules in XML content -->
<!ELEMENT XMLRules (%xmlElements;)>
```

```
<!ELEMENT TagText EMPTY>
<!ATTLIST TagText
    tag CDATA #REQUIRED
    attributePatterns CDATA ""
    source CDATA "*"
>

<!ELEMENT Attribute EMPTY>
<!ATTLIST Attribute
    name CDATA #REQUIRED
    tag CDATA "*"
    valuePatterns CDATA ""
    type (%eURL; | %eDHTML; | %eDJS; ) "URL"
    source CDATA "*"
>
```

**備註 –** 除必要的屬性值不能只有 * 之外，您可使用 * 做爲規則值的一部分。會忽略這類規則，但是訊息會記錄在 RuleSetInfo 記錄檔中。如需此記錄檔的資訊，請參閱第 91 頁的「除錯檔案名稱」。

## XML DTD 範例

本節包含一範例規則集。我們使用第 140 頁的「案例研究」來說明 Rewriter 解譯這些規則的方式。

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!--
Rules for integrating a mail client with the gateway.
-->
<!DOCTYPE RuleSet SYSTEM "jar://rewriter.jar/resources/RuleSet.dtd">
<RuleSet type="GROUPED" id="owa">
<HTMLRules>
<Attribute name="action" />
<Attribute name="background" />
<Attribute name="codebase" />
<Attribute name="href" />
<Attribute name="src" />
<Attribute name="lowsrc" />
<Attribute name="imagePath" />
<Attribute name="viewClass" />
<Attribute name="emptyURL" />
<Attribute name="draftsURL" />
<Attribute name="folderURL" />
<Attribute name="prevMonthImage" />
<Attribute name="nextMonthImage" />
<Attribute name="style" />
<Attribute name="content" tag="meta" />
```

```
</HTMLRules>
<JSRules>
<!-- Rules for Rewriting JavaScript variables in URLs -->
<Variable name="URL"> _fr.location </Variable>
<Variable name="URL"> g_szUserBase </Variable>
<Variable name="URL"> g_szPublicFolderUrl </Variable>
<Variable name="URL"> g_szExWebDir </Variable>
<Variable name="URL"> g_szViewClassURL </Variable>
<Variable name="URL"> g_szVirtualRoot </Variable>
<Variable name="URL"> g_szBaseURL </Variable>
<Variable name="URL"> g_szURL </Variable>
<Function name="EXPRESSION" name="NavigateTo" paramPatterns="y"/>
</JSRules>
<XMLRules>
<Attribute name="xmlns"/>
<Attribute name="href" tag="a"/>
<TagText tag="baseroot" />
<TagText tag="prop2" />
<TagText tag="prop1" />
<TagText tag="img" />
<TagText tag="xsl:attribute"
attributePatterns="name=src" />
</XMLRules>
</RuleSet>
```

## 撰寫規則的步驟

撰寫規則的一般程序如下：

- 識別出含有需重新寫入內容之 HTML 網頁的目錄。
- 在這些目錄中，識別出需要重新寫入的網頁。
- 識別出各網頁上需重新寫入的 URL。識別出多數 URL 的簡易方法就是搜尋 "http" 與 "/"。
- 識別出 URL 的內容類型：HTML、JavaScript 或 XML。
- 在 Access Manager 管理主控台「Portal Server 配置」下的「Rewriter 服務」中編輯需要的規則集，以撰寫重新寫入各個 URL 所需的規則。
- 將所有規則合併到該網域的規則集中。

## 規則集指導方針

建立規則集時，請記住：

- 特定主機的優先順序是根據最長的 URI 符合。以下列的規則集爲例

```
mail1.central.abc.com|iplanet_mail_ruleset
*.sfbay.abc.com|sfbay_ruleset
*.abc.com|generic_ruleset
```

使用的會是 sfbay_ruleset，因爲它的符合內容最長。

- 規則集中的規則會依順序套用至網頁中的所有陳述式，直到有一個規則與特定陳述式相符。

  撰寫規則時，請牢記規則的順序。規則會以出現在規則集中的順序，套用至網頁中的陳述式。若您有特定規則，及包含 "*" 的一般規則，請先定義該特定規則，然後再定義一般規則。否則，在套用特定規則之前就會先套用一般規則至所有陳述式。
- 所有的規則都必須包含在 <RuleSet> </RuleSet> 標記內。
- 將所有需重新寫入 HTML 內容的規則納入規則集的 <HTMLRules> </HTMLRules> 區段。
- 將所有需重新寫入 JavaScript 內容的規則納入規則集的 <JSRules> </JSRules> 區段。
- 將所有需重新寫入 XML 內容的規則納入規則集的 <XMLRules> </XMLRules> 區段。
- 請在您的企業內部網路網頁中，識別出需重新寫入的 URL，然後將所需規則納入規則集的相應區段 (HTML、JSRules 或 XMLRules)。
- 將規則集指派至所需網域。
- 重新啓動閘道以使變更產生作用：

  *gateway-install-root*/SUNWportal/bin/gateway -n *gateway-profile-name* start

## 定義規則集根元素

規則集根元素具有兩種屬性：

- RuleSetName，例如，default_ruleset。會在 RuleSet 至 URI 的對映中參照此名稱。
- Extends。此屬性指的是規則集的繼承特性。值會指向您欲從中導出規則集的規則集。

  使用值 none 以表示此新的獨立規則集不依附於任何其他的規則集，或指定 *RuleSetName* 以表示您的規則集依附於其他規則集。

## 使用遞迴功能

Rewriter 使用遞迴功能在符合的字串式樣的結尾搜尋是否有相同的式樣。

例如，當 Rewriter 剖析下列字串時：

```
<a href="src=abc.jpg,src=bcd.jpg,src=xyz.jpg>
```

規則

```
<Attribute name="href" valuePatterns="*src=**"/>
```

僅會重寫第一個出現的式樣，其形式如下：

```
<a href="src=http://jane.sun.com/abc.jpg>
```

如果您使用遞迴選項

```
<Attribute name="href" valuePatterns="REC:*src=**"/>;
```

Rewriter 會搜尋相同的式樣，直至符合字串式樣的結尾，因此輸出將會是：

```
<a href="src=http://jane.sun.com/abc.jpg,src=http://jane.sun.com/bcd.jpg,
src=http://jane.sun.com/xyz.jpg>
```

# 定義以語言為基礎的規則

規則以下列語言爲基礎：

- HTML
- JavaScript
- XML

## HTML 內容的規則

可進一步將網頁上的 HTML 內容分類爲屬性、表單或 Applet。同樣地，HTML 內容的規則可分類爲：


- 第 68 頁的 「HTML 內容的屬性規則」
- 第 70 頁的 「用於 HTML 內容的表單規則」
- 第 71 頁的 「用於 HTML 內容的 Applet 規則」


### HTML 內容的屬性規則

此規則可識別需重新寫入值的標籤屬性。屬性值可爲簡單的 URL、JavaScript 或 DHTML 內容。例如：

- 「img」標籤中指向某個影像位置的 `src` 屬性 (簡單 URL)
- href 屬性中處理按一下連結時的動作的 `onClick` 屬性 (DJS)

此部分說明下列內容：


- 第 68 頁的 「屬性規則語法」
- 第 69 頁的 「屬性規則範例」
- 第 69 頁的 「DJS 屬性範例」


### 屬性規則語法

```
<Attribute name="attributeName" [tag="*" valuePatterns="" source="*" type="URL|DHTML|DJS"]/>
```

其中，

`attributeName` 爲屬性名稱 (必須的)

tag 是屬性所屬的標籤 (可選，預設爲 *，表示任何標籤)

valuePatterns 請參閱第 73 頁的 「在規則中與式樣相符」。

source 指定定義此屬性的頁面的 URI (可選，預設爲 *，表示在任何頁面中)

type 指定值的類型 (可選)。類型可能是：

URL - 簡單 URL (預設值)。

DHMTL - DHTML 內容。此類內容會以標準 HTML 內容的形式顯示，而且用於 Microsoft HTC 格式的檔案。

DJS - JavaScript 內容。所有 HTML 事件處理器，如 onClick 與 onMouseover，其 JavaScript 皆含有 HTML 屬性。

## 屬性規則範例

假設此網頁的基準 URL 是：

```
http://mymachine.intranet.com/mypage.html
```

網頁內容：

```
<a href="http://mymachine.intranet.com/mypage.html">
```

規則

```
<Attribute name="href"/>
或者
<Attribute name="href" tag="a"/>
```

輸出

```
<a href=gateway-URL/http://mymachine.intranet.com/myhome.html>
```

描述

因爲待重新寫入的 URL 已經是一個絕對 URL，因此只會將閘道 URL 前置於此 URL。

## DJS 屬性範例

假設此網頁的基準 URL 是：

```
http://abc.sesta.com/focus.html
```

網頁內容：

```
<Form>
```

```
<input TYPE=TEXT SIZE=20 value=focus
onClick="Check(\q/focus.html\q,\qfocus\q);return;">

</Form>
```

規則

```
<Attribute name="onClick" type="DJS"/>
<Function type="URL" name="Check" paramPatterns="y,"/>
```

輸出

```
<Form>

<INPUT TYPE=TEXT SIZE=20 value=focus onClick="Check(\q
gateway-URL
/http://abc.sesta.com/focus.html\q,\qfocus\q);return;">

</Form>
```

描述

重新寫入特定網頁內容需要兩個規則。第一個規則可識別 `onClick` JavaScript 記號。第二個規則可識別需重新寫入的 `check` 函數參數。在這種情況下，僅會重新寫入第一個參數，因爲 `paramPatterns` 用值 `y` 取代了第一個參數。

出現 JavaScript 記號的開道 URL 與網頁的基準 URL 會置於所需參數之前。

## 用於 HTML 內容的表單規則

使用者所瀏覽的 HTML 網頁可能包含表單。某些表單元素可能會將 URL 視爲值。

本節分爲下列部分：


- 第 70 頁的 「表單規則語法」
- 第 71 頁的 「表單規則範例」


### 表單規則語法

```
<Form name="form1" field="visit" [valuePatterns="" source="*"]/>
```

其中

`name` 爲表單名稱 (必須的)

`field` 是表單中的欄位，需要重新寫入它的值 (必須的)

`valuePatterns` 請參閱第 73 頁的 「在規則中與式樣相符」

`source` 是 html 網頁的 URL，即呈現此表單定義之處 (可選，預設爲 `*`，表示在任何網頁中)

### 表單規則範例

假設此網頁的基準 URL 是：

```
http://test.siroe.com/testcases/html/form.html
```

網頁內容

假設網頁的 URI 是 `form.html` 且位於伺服器的根目錄中。

```
<form name=form1  method=POST action=
"http://test.siroe.com/testcases/html/form.html">
<input type=hidden name=abc1 value="0|1234|/test.html">
</form>
```

要重新寫入出現在 `form1` 中名爲 `abc1` 的隱藏欄位值中的 `/text.html`，需要下列規則。

規則

```
<Form source="*/form.html" name="form1"
field="abc1" valuePatterns="0|1234|"/>
<Attribute name="action"/>
```

輸出

```
<FORM name="form1"
method="POST" action="gateway-URL/
http://test.siroe.com/testcases/html/form.html">
<input type=hidden name=abc1
value="0|1234|gateway-URL/
http://test.siroe.com/test.html">
</FORM>
```

描述

`action` 標記是使用某些已定義之 HTML 屬性規則所重新寫入的。

輸入標記屬性值的 `value` 的重新寫入方式如輸出中所示。已找出特定的 `valuePatterns`，然後即利用前置閘道 URL 及網頁的基準 URL 來重新寫入符合的 `valuePatterns` 後面的所有內容。請參閱第 73 頁的 「在規則中與式樣相符」。

## 用於 HTML 內容的 Applet 規則

單一網頁可以包含許多 Applet，而每個 Applet 則可以包含許多參數。Rewriter 會利用 Applet 的 HTML 定義與規則中指定的值相符，然後修改作爲 Applet 參數定義一部分呈現的 URL 值。此取代動作會在伺服器上進行，而非在使用者瀏覽特定網頁時進行。此規則可識別並重新寫入 HTML 內容中的 Applet 及物件標籤的參數。

本節分爲下列部分：

- 第 72 頁的 「Applet 規則語法」
- 第 72 頁的 「Applet 規則範例」


## Applet 規則語法

```
<Applet code="ApplicationClassName/ObjectID
" param="parametername" [valuePatterns="" source="*"] />
```

其中

`code` 是 Applet 或物件類別的名稱 (必須的)

`param` 是值需要重新寫入的參數的名稱 (必須的)

`valuePatterns` 請參閱第 73 頁的 「在規則中與式樣相符」。

`source` 是包含 Applet 定義的網頁的 URL (可選，預設爲 `*`，表示在任何網頁中)

## Applet 規則範例

假設此網頁的基準 URL 是：

```
http://abc.siroe.com/casestudy/test/HTML/applet/rule1.html
```

網頁內容：

```
<applet codebase="appletcode" code="
RewriteURLinApplet.class" archive="/test.jar">
<param name=Test1 value="/index.html">
</applet>
```

規則

```
<Applet source="*/rule1.html" code=
"RewriteURLin*.class" param="Test*"/>
```

輸出

```
<APPLET codebase="gateway-URL
/http://abc.siroe.com/casestudy/test/HTML/
applet/appletcode" code="RewriteURLinApplet.class"
 archive="/test.jar"><param name="Test1" value="
gateway-URL/http:
//abc.siroe.com/index.html">
</APPLET>
```

描述

將重新寫入 `codebase` 屬性，因爲 `<Attribute name="codebase"/>` 是 `default_gateway_ruleset` 中已定義的規則。

所有以 Test 開頭的參數都會被重新寫入。顯示 Applet 碼的網頁基準 URL 及閘道 URL 都會置於 params 標籤的 value 屬性之前。

## 在規則中與式樣相符

您可以使用 valuePatterns 欄位來與式樣相符，並識別需重新寫入之陳述式的特定部分。

若您指定 valuePatterns 作爲規則的一部分，則會重新寫入所有位於符合之樣式後的內容。

請參考下列表單規則範例。

```
<Form source="*/source.html
" name="form1" field="visit
" [valuePatterns="0|1234|"]/>
```

其中

source 是顯示表單之 Html 網頁的 URL。

name 爲表單名稱。

field 是表單中的欄位，需要重新寫入它的值。

valuePatterns 指出需重新寫入的字串部分。會重新寫入所有出現在 valuePatterns 之後的內容 (可選，預設爲 ""，表示需重新寫入完整值)

## 以 valuePatterns 格式指定特殊化字元

您可以透過以反斜線退出特殊化字元的方式來指定它們。例如：

```
<Form source="*/source.html " name="form1" field=" visit" [valuePatterns="0|1234| \\
;original text|changed text"]/>
```

## 在 valuePatterns 中使用萬用字元

您可使用萬用字元星號 (*) 字元來完成用於重新寫入的式樣相符。

在 valuePatterns 欄位中，您不能僅指定一個 *。因爲 * 表示包含所有文字的符合結果，這樣 valuePattern 後沒有文字。因此，Rewriter 沒有可重新寫入的文字。您必須利用其他字串與 * 連用，如 *abc。在這種情況下，即會重新寫入所有位於 *abc 之後的內容。

**備註 –** 規則中的任何欄位皆可使用萬用字元星號 (*)。但是規則中所有的欄位不能都包含 *。若所有欄位皆包含 *，則會忽略此規則。不會顯示任何的錯誤訊息。

您可以利用 * 或 ** 與顯示在原始陳述式中的分隔字元 (分號或逗號) 連用，以分隔多個欄位。一個星號 (*) 會與所有不需重新寫入的欄位相符，而兩個星號 (**) 則會與所有需重新寫入的欄位相符。

第 73 頁的 「在 valuePatterns 中使用萬用字元」列出 * 萬用字元的某些用法範例。

**表 4–1** * 萬用字元的使用範例

| URL | valuePatterns | 描述 |
|---|---|---|
| `url1, url2, url3, url4` | `valuePatterns = "**, *, **, *"` | 會重新寫入 `url1` 與 `url3`，因爲 ** 會指出待重新寫入的部分 |
| `XYZABChttp://host1.sesta.com/dir1.html` | `valuePatterns = "*ABC"` | 僅會重新寫入 `http://host1.sesta.com/dir1.html` 部分。所有位於 `*ABC` 之後的項目皆需重新寫入。 |
| `"0\|dir1\|dir2\|dir3\|dir4\|test\|url1` | `valuePatterns = "*\|*\|**\|*\|**\|*\|"` | 會重新寫入 `dir2`、`dir4` 與 `url1`。需重新寫入的最後一個欄位不必以 ** 表示。 |

# JavaScript 內容的規則

JavaScript 可在多個位置包含 URL。Rewriter 無法直接剖析 JavaScript 與確定 URL 部分。必須撰寫特定規則集以協助 JavaScript 處理器識別及轉譯 URL。

具有 URL 類型的 JavaScript 元素分類如下：

- 第 74 頁的 「變數」
- 第 81 頁的 「函數引數」

## 變數

### 變數的一般語法是：

<Variable name="variableName" [type="URL|EXPRESSION|DHTML|DJS|SYSTEM" source="*"]>

視其所持有的值類型而定，JavaScript 變數可細分爲 5 種：

- 第 75 頁的 「URL 變數」
- 第 76 頁的 「EXPRESSION 變數」

- 第 77 頁的 「DHTML (動態 HTML) 變數」
- 第 79 頁的 「DJS (動態 JavaScript) 變數」
- 第 80 頁的 「SYSTEM 變數」


## URL 變數

變數值是一個可視爲 URL 的簡單字串。

本節分爲下列部分：


- 第 75 頁的 「URL 變數語法」
- 第 75 頁的 「URL 變數範例」


## URL 變數語法

```
<Variable name="variableName" type="URL" [source="*"]>
```

其中

`variableName` 爲變數名稱。將會重新寫入 `variableName` 的值 (必須的)

`type` 爲 URL 變數 (必須的，且值必須爲 URL)

`source` 是此 JavaScript 變數所在的網頁的 URI (可選，預設爲 `*`，表示在任何網頁中)

## URL 變數範例

假設基準 URL 是：

```
http://abc.siroe.com/tmp/page.html
```

網頁內容

```
<script LANGUAGE="Javascript">
<!--
//URL Variables
var imgsrc1="/tmp/tmp.jpg";
var imgsrc2="http://srap.sesta.com/tmp/tmp.jpg";
var imgsrc3=imgsrc2;
//-->
</SCRIPT>
```

規則

```
<Variable name="imgsrc*" type="URL"/>
```

輸出

```
<script LANGUAGE="Javascript">
<!--
//URL Variables
var imgsrc="gateway-URL/http://abc.siroe.com/tmp/tmp.jpg";
var imgsrc="gateway-URL/http://srap.sesta.com/tmp/tmp.jpg";
var imgsrc3=imgsrc2;
//-->
</SCRIPT>
```

描述

所有 URL 類型的變數及名稱以 `imgsrc` 開頭的變數皆會被重新寫入。在輸出的第一行，會前置顯示變數的閘道 URL 與網頁 URL。第二行已包含絕對路徑，因此僅會前置閘道 URL。第三行 var `imagsrc2` 將不會重新寫入，因爲其值並非字串，而是另一個 JavaScript 值。

## EXPRESSION 變數

EXPRESSION 變數的右側會有一個表示式。此表示式會產生一個 URL。Rewriter 會將 JavaScript 函數 (`psSRAPRewriter_convert_expression`) 附加至 HTML 網頁，因爲其無法在伺服器上計算這類表示式的值。此函數會將表示式視爲參數，並在用戶端瀏覽器中計算所需 URL 值。

若您不確定陳述式包含的是簡單 URL 或 EXPRESSION URL，請使用 EXPRESSION 規則，因爲其可處理兩種情況。

本節分爲下列部分：

- 第 76 頁的 「EXPRESSION 變數語法」
- 第 76 頁的 「EXPRESSION 變數範例」

## EXPRESSION 變數語法

```
<Variable name="variableName" [type="EXPRESSION" source="*"]/>
```

其中

`variableName` 是 JavaScript 變數的名稱，其值爲表示式 (必須的)

`type` 是 JavaScript 變數的類型 (可選，預設爲 EXPRESSION)

`source` 是網頁的 URI (可選，預設爲 `*`，表示任何來源)

## EXPRESSION 變數範例

假設此網頁的基準 URL 是：

```
http://abc.siroe.com/dir1/dir2/page.html
```

網頁內容

```
<script LANGUAGE="Javascript">
<!--
//Expression variables
var expvar= getURIPreFix() + "../../images/graphics"+".gif";
document.write("<A HREF="+expvar+">Link to XYZ content</A><P>")
var expvar="../../images/graphics"+".gif";
//-->
</SCRIPT>
```

規則

```
<Variable name="expvar" type="EXPRESSION"/>
```

**或者**

```
<Variable name="expvar"/>
```

輸出

```
var expvar=psSRAPRewriter_convert_expression(getURIPreFix()
 + "../../images/graphics"+".gif");document.write("<a href="+expvar+">>
Link to XYZ content</A><P>")var expvar="gateway-URL/http://abc.siroe.com/images/graphics"+".gif";
```

描述

`psSRAPRewriter_convert_expression` 函數會前置於第一行表示式變數 `expvar` 的右側之前。此函數可處理表示式，並於執行時間重新寫入內容。在第三行中，此值將被重新寫入爲簡單 URL。

## DHTML (動態 HTML) 變數

這些是含有 HTML 內容的 JavaScript 變數。

本節分爲下列部分：

- 第 77 頁的 「DHTML 語法」
- 第 78 頁的 「DHTML 範例」

## DHTML 語法

```
<Variable name="variableName" type="DHTML" [source="*"]/>
```

其中

`variableName` 是含有 DHTML 內容的 JavaScript 變數的名稱 (必須的)

`type` 是變數的類型 (必須的，此值必須爲 DHTML)

`source` 是網頁的 URL (可選，預設爲 `*`，表示在任何網頁中)

## DHTML 範例

假設此網頁的基準 URL 是：

```
http://abc.sesta.com/graphics/set1/
graphics/jsscript/JSVAR/page.html
```

網頁內容

```
<script LANGUAGE="Javascript">
<!--
//DHTML Var
var dhtmlVar="<a href=../../images/test.html>"
var dhtmlVar="<a href=/images/test.html>"
var dhtmlVar="<a href=images/test.html>"
//-->
</SCRIPT>
```

規則

```
<Variable name="dhtmlVar" type="DHTML"/>
<Attribute name="href"/>
```
**或者**
```
<Attribute name="href" tag="a"/>
```

輸出

```
<script LANGUAGE="Javascript">
<!--
//DHTML Var
var dhtmlVar="<a href=gateway-URL
/http://abc.sesta.com/graphics/
set1/graphics/images/test.html>"
var dhtmlVar="<a href=gateway-URL/
http
://abc.sesta.com/images/test.html>"
var dhtmlVar="<a href=gateway-URL/
http://abc.sesta.com/graphics/set1/
graphics/jscript/JSVAR/images/test.html>"
//--></SCRIPT>
```

描述

JavaScript 剖析器會讀取 `dhtmlVar` 的值作爲 HTML 內容，並經由 HTML 剖析器傳送內容。HTML 剖析器會套用符合 href 屬性規則的 HTML 規則，因此 URL 會被重新寫入。

## DJS (動態 JavaScript) 變數

這些是含有 JavaScript 內容的 JavaScript 變數。

本節分爲下列部分：


- 第 79 頁的 「DJS 語法」
- 第 79 頁的 「DJS 範例」


## DJS 語法

```
<Variable name="variableName" type="DJS" [source="*"]/>
```

其中

`variable` 是 JavaScript 變數，其值爲 javascript。

## DJS 範例

假設此網頁的基準 URL 是：

```
http://abc.sesta.com/dir1/dir2/dir3/jscript/dir4/page.html
```

網頁內容

```
//DJS Var
var dJSVar="var dJSimgsrc=\q/tmp/tmp.jpg\q;"
var dJSVar="var dJSimgsrc=\q../tmp/tmp.jpg\q;"
var dJSVar="var dJSimgsrc=
\qhttp://abc.sesta.com/tmp/tmp.jpg\q;"
```

規則

```
<Variable name="DJS">dJSVar/>
<Variable name="URL">dJSimgsrc/>
```

輸出

```
//DJS Var - need 2 rules
var dJSVar="var dJSimgsrc=\qgateway-URL
/http://abc.sesta.com/tmp/tmp.jpg\q;"var dJSVar="var dJSimgsrc=\q
gateway-URL/http
://abc.sesta.com/dir1/dir2/dir3/jscript/tmp/tmp.jpg\q;"
var dJSVar="var dJSimgsrc=\qgateway-URL/
http://abc.sesta.com/tmp/tmp.jpg\q;"
```

描述

此處必須使用兩個規則。第一個規則可找到動態 JavaScript 變數 `dJSVar`。此變數的值仍然是 `URL` 類型的 JavaScript。套用第二個規則來重新寫入此 JavaScript 變數的值。

## SYSTEM 變數

這些變數並非由使用者公佈且支援有限。這些變數可用作 JavaScript 標準的一部分。例如，window.location.pathname。

本節分爲下列部分：


- 第 80 頁的 「SYSTEM 變數語法」
- 第 80 頁的 「SYSTEM 變數範例」


## SYSTEM 變數語法

```
<Variable name="variableName" type="SYSTEM" [source="*"]/>
```

其中

variableName 是 JavaScript 系統變數 (必須的，其值可能是與下列式樣相符的值：document.URL、document.domain、location、doument.location、location.pathname、location.href、location.protocol、location.hostname、location.host 與 location.port。所有這些都會位於 generic_ruleset 中。請勿修改這些系統變數規則。)

type 指定系統類型值 (必須的，且值爲 DJS)

source 是此網頁的 URI (可選，預設爲 *，表示在任何網頁中)

## SYSTEM 變數範例

假設此網頁的基準 URL 是：

```
http://abc.siroe.com/dir1/page.html
```

網頁內容

```
<script LANGUAGE="Javascript">
<!--
//SYSTEM Var
alert(window.location.pathname);
//-->
</SCRIPT>
```

規則

```
<Variable name="window.location.pathname" type="SYSTEM"/>
```

輸出

```
</SCRIPT>
<SCRIPT LANGUAGE="Javascript">
<!--
```

```
//SYSTEM Var
alert(psSRAPRewriter_convert_pathname(window.location.pathname));
//-->
</SCRIPT>
```

描述

Rewriter 會找出與規則相符的系統變數，然後前置 psSRAPRewriter_convert_system 函數。此函數可在執行時間中處理系統變數，然後相應重新寫入結果 URL。

## 函數引數

需重新寫入其值的函數參數可分爲 4 類：

- 第 81 頁的 「URL 參數」
- 第 83 頁的 「EXPRESSION 參數」
- 第 84 頁的 「DHTML 參數」
- 第 86 頁的 「DJS 參數」

## 通用語法

```
<Function name="functionName " paramPatterns="y,y,"
[type="URL|EXPRESSION|DHTML|DJS" source="*"]/>
```

其中

name 是 JavaScript 函數的名稱 (必須的)

paramPatterns 指出需重新寫入的參數 (必須的)

y y 的位置會指出需重新寫入的參數。例如，在此語法中，需要重新寫入第一個參數，但第二個參數則不應重新寫入

type 指出此參數所需的值種類 (可選，預設爲 EXPRESSION 類型)

source 網頁源 URI (可選，預設爲 *，表示在任何網頁中)

## URL 參數

函數會將參數視爲字串，而此字串則可視爲 URL。

本節分爲下列部分：

- 第 82 頁的 「URL 參數語法」
- 第 82 頁的 「URL 參數範例」

## URL 參數語法

```
<Function name="functionName" paramPatterns="y,," type="URL" [source="*"]/>
```

其中

name 是含有 URL 類型參數的函數名稱 (必須的)

paramPatterns 指出需重新寫入的參數 (必須的)

y y 的位置會指出需重新寫入的參數。例如，在此語法中，需要重新寫入第一個參數，但第二個參數則不應重新寫入

type 是函數的類型 (必須的，此值必須爲 URL)

source 是具有此函數呼叫之網頁的 URL (可選，預設爲 *，表示在任何 URL 中)

## URL 參數範例

假設此網頁的基準 URL 是：

```
http://abc.sesta.com/test/rewriter/test1/jscript/test2/page.html
```

網頁內容

```
<script language="JavaScript">
<!--
function test(one,two,three){
alert(one + "##" + two + "##" +three);
}
test("/test.html","../test.html","123");
window.open("/index.html","gen",width=500,height=500);
//-->
</SCRIPT>
```

規則

```
<Function name="URL" name="test" paramPatterns="y,y,"/>
<Function name="URL" name="window.open" paramPatterns="y,,,"/>
```

輸出

```
<SCRIPT language="JavaScript">
<!--
function test(one,two,three) {
alert(one + "##" + two + "##" +three);
}
test("gateway-URL/http://abc.sesta.com/test.html","
gateway-URL/http://abc.sesta.com/test/rewriter/
```

```
test1/jscript/test.html","123");window.open("gateway-URL/
http://abc.sesta.com/index.html","gen",width=500,height=500);
//-->
</SCRIPT>
```

描述

第一個規則指出名稱爲 test 的函數中前兩個參數需要重新寫入。因此會重新寫入 test 函數的前兩個參數。第二個規則指出 window.open 函數的第一個參數需要重新寫入。window.open 函數中的 URL 會前置含有函數參數的網頁的閘道 URL 及基準 URL。

## EXPRESSION 參數

這些參數採用表示式值，即 URL 中的計算結果。

本節分爲下列部分：

- 第 83 頁的 「EXPRESSION 參數語法」
- 第 83 頁的 「EXPRESSION 參數範例」

## EXPRESSION 參數語法

```
<Function name="functionName" paramPatterns="y" [type="EXPRESSION" source="*"]/>
```

其中

name 爲函數名稱 (必須的)

paramPatterns 指出需重新寫入的參數 (必須的)

y y 的位置會指出需重新寫入的函數參數。上列語法中，僅會重新寫入第一個參數

type 指定 EXPRESSION 值 (可選)

source 是呼叫此函數的網頁的 URI

## EXPRESSION 參數範例

假設此網頁的基準 URL 是：

```
http://abc.sesta.com/dir1/dir2/page.html
```

網頁內容

```
<script language="JavaScript">
<!--
function jstest2(){
return ".html";
```

```
}
function jstest1(one){
return one;
}
var dir="/images/test"
var test1=jstest1(dir+"/test"+jstest2());
document.write("<a HREF="+test1+">TEST</a>");
alert(test1);
//-->
</SCRIPT>
```

規則

```
<Function type="EXPRESSION" name="jstest1" paramPatterns="y"/>
```

**或者**

```
<Function name="jstest1" paramPatterns="y"/>
```

輸出

```
<script language="JavaScript">
<!--
function jstest2(){
return ".html";
}
function jstest1(one){
return one;
}
var dir="/images/test"
var test1=jstest1(psSRAPRewriter_convert_expression(dir+"/test"+jstest2()));
document.write("<a HREF="+test1+">TEST</a>");
alert(test1);
//-->
</SCRIPT>
```

描述

規則將 `jstest1` 函數的第一個參數視爲 EXPRESSION 函數參數，從而指定此參數需要重新寫入。在網頁內容範例中，第一個參數是僅在執行時間中計算其值的表示式。Rewriter 會將 `psSRAPRewriter_convert_expression` 函數前置於此表示式之前。從而計算此表示式，並且 `psSRAPRewriter_convert_expression` 函數在執行階段重新寫入輸出。

---

**備註 –** 以上範例中，不需將 `test1` 變數作爲 JavaScript 變數規則的一部分。`jstest1` 的函數規則負責執行重新寫入。

---

## DHTML 參數

其值爲 HTML 的函數參數

本機 JavaScript 方法，如會以動態的方式產生 HTML 網頁的 document.write()，歸屬於此種類。

本節分爲下列部分：


- 第 85 頁的 「 DHTML 參數語法」
- 第 85 頁的 「DHTML 參數範例」


## DHTML 參數語法

```
<Function name="functionName" paramPatterns="y" type="DHTML" [source="*"]/>
```

其中

name 是函數名稱

paramPatterns 指出需重新寫入的參數 (必須的)

y y 的位置會指出需重新寫入的函數參數。上列語法中，僅會重新寫入第一個參數

## DHTML 參數範例

假設此網頁的基準 URL 是：

```
http://xyz.siroe.com/test/rewriter/test1/jscript/JSFUNC/page.html
```

網頁內容

```
<script>
<!--
document.write(\q<a href="/index.html">write</a><BR>\q)
document.writeln(\q<a href="index.html">writeln</a><BR>\q)
document.write("http://abc.sesta.com/index.html<BR>")
document.writeln("http://abc.sesta.com/index.html<BR>")
//-->
</SCRIPT>
```

規則

```
<Function name="DHTML" name="document.write" paramPatterns="y"/>
<Function name="DHTML" name="document.writeln" paramPatterns="y"/>
<Attribute name="href"/>
```

輸出

```
<SCRIPT>
<!--
document.write(\q<a href="gateway-URL/
```

```
http://xyz.siroe.com/index.html">write</a><BR>\q)
document.writeln(\q<a href="gateway-URL/
http://xyz.siroe.com/test/rewriter/test1/
jscript/JSFUNC/index.html">writeln</a><BR>\q)
document.write("http://abc.sesta.com/index.html<BR>")
document.writeln("http://abc.sesta.com/index.html<BR>")
//-->
</SCRIPT>
```

描述

第一個規則指出 `document.write` 函數中的第一個參數需要重新寫入。第二個規則指出 `document.writeln` 函數中的第一個參數需要重新寫入。第三個規則是一個簡單 HTML 規則，指出名稱爲 `href` 的所有屬性皆需重新寫入。在範例中，DHTML 參數規則會識別出函數中需重新寫入的參數。然後便套用 HTML 屬性規則，以實際重新寫入識別出的參數。

## DJS 參數

其值爲 JavaScript 的函數參數。

本節分爲下列部分：


- 第 86 頁的 「DJS 參數語法」
- 第 86 頁的 「DJS 參數範例」


## DJS 參數語法

```
<Function name="functionName" paramPatterns="y" type="DJS" [source="*"]/>
```

其中

`name` 是含有一個 DJS 參數的函數名稱 (必須的)

paramPatterns 指出上列函數中哪一個參數是 DJS (必須的)

y y 的位置會指出需重新寫入的函數參數。上列語法中，僅會重新寫入第一個參數

`type` 是 DJS (必須的)

`source` 是網頁的 URI (可選，預設爲 `*`，表示任何 URI)

## DJS 參數範例

假設此網頁的基準 URL 是：

```
http://abc.sesta.com/page.html
```

網頁內容

```
<script>
menu.addItem(new NavBarMenuItem("All Available Information","JavaScript:top.location=\qhttp://abc.sesta.com\q"));
</script>
```

規則

```
<Function name="DJS" name="NavBarMenuItem" paramPatterns=",y"/>
<Variable name="URL">top.location</Variable>
```

輸出

```
<script>
menu.addItem(new NavBarMenuItem("All Available Information",
"JavaScript:top.location=\qgateway-URL/
http://abc.sesta.com\q"));
</script>
```

描述

第一個規則指出 NavBarMenuItem 函數中的第二個包含 JavaScript 的參數需要重新寫入。在 JavaScript 中，top.location 變數亦需重新寫入。將使用第二個規則來重新寫入此變數。

# XML 內容的規則

網頁可能包含 XML 內容，其因此可包含 URL。需重新寫入的 XML 內容可分爲兩類：

- 第 87 頁的 「標記文字」 (與標記的 PCDATA 或 CDATA 相同)
- 第 88 頁的 「屬性」

## 標記文字

此規則是用於重新寫入標記元素的 PCDATA 或 CDATA。

本節分爲下列部分：

- 第 87 頁的 「標記文字語法」
- 第 88 頁的 「標記文字範例」

### 標記文字語法

```
<TagText tag="tagName"
[attributePatterns="attribute_patterns_for_ this_tag" source="*"]/>
```

其中

tagName 爲標記名稱

attributePatterns 是此標記的屬性及值式樣 (可選，表示此標記完全不具屬性)

source 是此 xml 檔案的 URI (可選，預設爲 *，表示任何 xml 網頁)

### 標記文字範例

假設此網頁的基準 URL 是：

```
http://abc.sesta.com/test/rewriter/test1/xml/page.html
```

網頁內容

```
<xml>
<Attribute name="src">test.html</attribute>
<attribute>abc.html</attribute>
</xml>
```

規則

```
<TagText tag="attribute" attributePatterns="name=src"/>
```

輸出

```
<xml>
<Attribute name="src">gateway-URL/
http://abc.sesta.com/test/rewriter/test1/
xml/test.html</attribute><attribute>abc.html</attribute>
</xml>
```

描述

網頁內容的第一行包含第 89 頁的 「屬性範例」。此網頁內容的第二行不包含具有屬性呼叫名稱且屬性名稱值爲 src 的屬性，因此不會執行任何重新寫入的動作。要進行重新寫入，我們亦需具有 <TagText tag="attribute"/>

## 屬性

XML 屬性的規則與 HTML 的屬性規則類似。其間的差異在於：XML 的屬性規則有大小寫之分，而 HTML 屬性規則則無。這是因爲 XML 中建立了區分大小寫的特性，而 HTML 中未建立。

Rewriter 會依據屬性名稱轉譯屬性值。

本節分爲下列部分：


- 第 89 頁的 「屬性語法」
- 第 89 頁的 「屬性範例」

## 屬性語法

```
<Attribute name="attributeName " [tag="*" type="URL" valuePatterns="*" source="*"
]/>
```

其中

`attributeName` 爲屬性名稱 (必須的)

`tag` 是包含此屬性的標記的名稱 (可選，預設爲 `*`，表示任何標記)

`valuePatterns` 請參閱第 73 頁的 「在規則中與式樣相符」。

`source` 是此 XML 網頁的 URI (可選，預設爲 `*`，表示在任何 XML 網頁中)

## 屬性範例

假設此網頁的基準 URL 是：

```
http://abc.sesta.com/test/rewriter/test1/xml/page.html
```

網頁內容

```
<xml>
<baseroot href="/root.html"/>
<img href="image.html"/>
<string href="1234|substring.html"/>
<check href="1234|string.html"/>
</xml>
```

規則

```
<Attribute name="href"tag="check" valuePatterns="1234|"/>
```

輸出

```
<xml>
<baseroot href="/root.html"/><img href="image.html"/>
<string href="1234|substring.html"/><check href="1234|
gateway-URL
/http://abc.sesta.com/test/rewriter/test1/xml/string.html"/></xml>
```

描述

上列範例中，僅重新寫入第四行，因爲其符合規則中所指定的所有條件。請參閱第 73 頁的 「在規則中與式樣相符」。

## Cascading Style Sheet (串接樣式表) 的規則

HTML 網頁中的 Cascading Style Sheet (包含 CCS2) 會被轉譯。沒有任何針對此轉譯而定義的規則，因爲 URL 僅出現在 CSS 的 `url()` 函數與匯入語法中。

## WML 的規則

WML 與 HTML 相似，因此會將 HTML 規則套用至 WML 內容。使用 WML 內容的一般規則集。請參閱第 68 頁的 「HTML 內容的規則」。

## 使用遞迴功能

Rewriter 使用遞迴功能在符合的字串式樣的結尾搜尋是否有相同的式樣。

例如，當 Rewriter 剖析下列字串時：

```
<a href="src=abc.jpg,src=bcd.jpg,src=xyz.jpg>
```

規則

```
<Attribute name="href" valuePatterns="*src=**"/>
```

僅會重寫第一個出現的式樣，看起來會像這個樣子：

```
<a href="src=http://jane.sun.com/abc.jpg>
```

但是如果您使用如下的遞迴選項，

```
<Attribute name="href" valuePatterns="REC:*src=**"/>;
```

Rewriter 在符合的字串式樣的結尾搜尋是否有相同的式樣，因此輸出將會是：

```
<a href="src=http://jane.sun.com/abc.jpg,src=
http://jane.sun.com/bcd.jpg,src=http://jane.sun.com/xyz.jpg>
```

# 使用除錯記錄檔排除故障

要排除 Rewriter 的故障，您需啓用除錯記錄檔。

除錯訊息分類如下：

- 錯誤 – 使得 Rewriter 無法復原的錯誤。
- 警告 – 不會對 Rewriter 的運作造成重大影響的警告。Rewriter 可從此類型的錯誤中復原，但可能會或不會造成不當行爲。有些出現在警告中的訊息僅是告知性的。例如「Not rewriting image content」(未重新寫入影像內容) 被記錄爲警告訊息。這個情況並不會造成重大影響，因爲 Rewriter 並不會用於重新寫入影像。

- 訊息 – 這是 Rewriter 所提供最高層級的資訊。

# 設定 Rewriter 除錯層級

## ▼ 設定 Rewriter 除錯層級

1 **以超級使用者身份登入閘道機器，然後編輯下列檔案：**

*gateway-install-root*/SUNWam/config/AMConfig-*instance-name*.properties

2 **設定除錯層級：**

com.iplanet.services.debug.level=

除錯層級爲：

error - 只會在除錯檔案中記錄嚴重錯誤。在此種錯誤發生時，Rewriter 通常會停止運作。

warning - 會記錄警告訊息。

message - 會記錄所有的除錯訊息。

off - 不會記錄任何除錯訊息。

3 **在 AMConfig-*instance-name* .properties 檔案的下列特性中，指定除錯檔案目錄：**

com.iplanet.services.debug.directory=/var/opt/SUNWam/debug

其中 /var/opt/SUNWam/debug 是預設的除錯目錄。

4 **從終端機視窗重新啓動閘道：**

./psadmin start-sra-instance –u amadmin – f <*password file*> –N <*profile name*>– t <*gateway*>

# 除錯檔案名稱

當將除錯層級設定爲 message 時，除錯會產生一組檔案。第 91 頁的 「除錯檔案名稱」會列出 Rewriter 檔案與其中包含的資訊。

**表 4–2** Rewriter 除錯檔案

| 檔案名稱 | 資訊 |
|---|---|
| RuleSetInfo | 包含已用於重新寫入的所有規則集，皆記錄在此檔案中。 |

表 4–2 Rewriter除錯檔案 *(續)*

| 檔案名稱 | 資訊 |
|---|---|
| Original Pages | 包含網頁 URI、resolveURI (若與網頁 URI 不同)、內容 MIME、套用至網頁的規則集、剖析器 MIME 與原始內容。<br>與剖析有關的特定錯誤/警告/訊息亦會出現在此檔案中。<br>在 message 模式中會記錄完整內容。在 warning 與 error 模式中只會記錄重新寫入期間發生的異常情況。 |
| Rewritten Pages | 包含網頁 URI、resolveURI (若與網頁 URI 不同)、內容 MIME、套用至網頁的規則集、剖析器 MIME 與已重新寫入的內容。<br>當除錯模式設爲 message 時，即會儲存這些資訊。 |
| Unaffected Pages | 包含未經修改的網頁清單。 |
| URIInfo Pages | 包含已找到及轉譯的 URL。所有其內容與原始資料相同的網頁詳細資訊將記錄至此檔案中。<br>記錄的詳細資訊包括：網頁 URI、MIME 與編碼資料、用於重新寫入的 rulesetID 以及剖析器 MIME。 |

除了上述檔案之外，Rewriter 會產生一個用於未留存於上述檔案中的其他除錯訊息的檔案。檔案名稱包括兩個部分：第一部分爲 `pwRewriter` 或 `psSRARewriter`，第二部分則爲使用 `portal` 或 *gateway-profile-name* 的副檔名。

除錯檔案會顯示在入口網站或閘道中。這些檔案是位於 `AMConfig-`*instance-name*`.properties` 檔案中指出的目錄。

Rewriter 元件會產生下列檔案組以協助除錯作業：

*prefix*_RuleSetInfo.*extension*

*prefix*_OrginalPages.*extension*

*prefix*_RewrittenPages.*extension*

*prefix*_UnaffectedPages.*extension*

*prefix*_URIInfo.*extension*

其中

*prefix* 爲用於 URLScraper 用途記錄檔的 `psRewriter` 或用於閘道用途記錄檔的 `psSRAPRewriter`。

*extension* 則爲用於 URLScraper 用途的 `portal` 或用於閘道用途的 `gateway-profile-name`。

例如，若利用閘道上的 Rewriter 來轉換網頁並使用預設的閘道設定檔，則除錯作業會產生下列檔案：

```
psSRAPRewriter_RuleSetInfo.default

psSRAPRewriter_OriginalPages.default

psSRAPRewriter_RewrittenPages.default

psSRAPRewriter_UnaffectedPages.default

psSRAPRewriter_URIInfo.default

psSRAPRewriter.default
```

# 工作範例

本節包括：

- 含需重新寫入之內容的簡單 HTML
- 重新寫入內容所需的規則
- 已重新寫入的相應 HTML 網頁

這些頁面範例位於 *portal-server-URL* `/rewriter` 目錄下。您可在套用規則前瀏覽整個頁面，然後經由您的閘道檢視含已重新寫入之輸出的檔案，以查看規則的套用結果。在某些範例中，規則已經是 `default_gateway_ruleset` 的一部分。在某些範例中，您必須將規則納入 `default_gateway_ruleset` 中。這一點會在適當之處提及。

---

**備註 –** 某些以粗體顯示的陳述式表示其已被重新寫入。

---

可用的範例如下：

HTML

- 第 95 頁的 「HTML 屬性範例」
- 第 99 頁的 「HTML 表單範例」
- 第 101 頁的 「HTML Applet 範例」

JavaScript

- 變數
  - 第 102 頁的 「JavaScript URL 變數的範例」
  - 第 102 頁的 「JavaScript 內容範例」
  - 第 106 頁的 「JavaScript DHTML 變數的範例」
  - 第 108 頁的 「JavaScript DJS 變數的範例」
  - 第 110 頁的 「JavaScript SYSTEM 變數的範例」

函數


- 第 112 頁的 「JavaScript URL 函數的範例」
- 第 113 頁的 「JavaScript EXPRESSION 函數的範例」
- 第 115 頁的 「JavaScript DHTML 函數的範例」
- 第 117 頁的 「JavaScript DJS 函數的範例」

XML

- XML 屬性範例

# HTML 內容範例

## HTML 屬性範例

### ▼ 使用 HTML 屬性範例

1 **您可自下列路徑存取此範例：**

*portal-server-URL* /rewriter/HTML/attrib/attribute.html

2 **請確定您已於閘道服務的 [網域與子網域的代理伺服器] 清單中定義** `abc.sesta.com` **與** `host1.siroe.com` **。**

若未定義，則會採用直接連接，且不前置閘道 URL。

您不需將此範例中指定的規則新增至 `default_gateway_ruleset` 中，因爲規則已完成定義。

#### 重新寫入前的 HTML

```
<html>
Rewriting starts
<head>
<title>TEST PAGE () </title>
</head>
ID-htmlattr.1
<br><br>
1.a href <a href="http://abc.sesta.com/images/logo.gif">http://..</a>
<br><br>
2. href <a href="https://host1.siroe.com">https://..</a>
<br><br>
3. href <a href="../images/logo.gif">../images/</a>
<br><br>
4. href <a href="images/logo.gif">images/..</a> <br><br>
5. href <a href="../../images/logo.gif">../../images/</a> <br><br>
Rewriting ends
</html>
```

#### 規則

```
<Attribute name="href"/>
```

## 重新寫入後的 HTML

```
<html>
Rewriting starts
<head>
<title>TEST PAGE () </title>
</head>
ID-htmlattr.1
<br><br>
1. a href <a href="gateway-URL/http://abc.sesta.com/images/logo.gif">http://..</a> <br>
```

// 重新寫入此 URL 是因爲 <Attrib name="href"/> 規則已於 default_gateway_ruleset 中加以定義。由於此 URL 是絕對 URL，因此僅會前置閘道 URL。請確定您已於閘道服務的 [網域與子網域的代理伺服器] 清單中定義 abc.sesta.com。否則，會認爲是直接連接，而不會前置閘道 URL。

```
2. href <a href="gateway-URL/https://host1.siroe.com">https://..</a>
```

// 同樣，host1.siroe.com 需於閘道服務的 [網域與子網域的代理伺服器] 清單中定義。否則，會認爲是直接連接，而不會前置閘道 URL。

```
<br><br>
3. href <a href="gateway-URL/portal-server-URL/rewriter/HTML/images/logo.gif">../images/</a>
```

// 由於指定的是相對路徑，因此會前置閘道 URL 與 portal-server-URL (附有所需子目錄)。此連結將無法作用，因爲在所提供之範例結構的 HTML 目錄下沒有名爲 images 的目錄。

```
<br><br>

4 href <a href="gateway-URL/portal-server-URL/rewriter/HTML/attrib/images/
logo.gif">images/..</a> <br><br>
```

// 由於指定的是相對路徑，因此會前置閘道 URL 與 Portal Server URL (附有所需子目錄)。

```
5. href <a href="gateway-URL/portal-server-URL/rewriter/images/logo.gif">
../../images/</a> <br><br>
```

// 由於指定的是相對路徑，因此會前置閘道 URL 與 Portal Server URL (附有所需子目錄)。此連結將無法作用，因爲在所提供之範例結構的 Rewriter 目錄下沒有名爲 images 的目錄。

```
Rewriting ends</html>
```

## HTML 動態 JavaScript 記號的範例

此部分討論使用 HTML JavaScript 記號範例

## ▼ 使用 HTML JavaScript 記號範例：

1. **您可自下列路徑存取此範例：**
   *portal-server-URL* /rewriter/HTML/jstokens/JStokens.html
2. **將此範例中指定的規則新增至 [重新寫入 JavaScript 來源的規則] 部分的** `default_gateway_ruleset` **中。**
3. **在 Portal Server 管理主控台的 Portal Server 配置下，編輯 Rewriter 服務中的** `default_gateway_ruleset`。
4. **從終端機視窗重新啓動閘道：**

```
./psadmin start-sra-instance –u amadmin – f  <password file> –N <profile name>– t  <gateway>
```

### 重新寫入前的 HTML

```
<html>
<head>
Rewriting starts
<script language="javascript">
function Check(test,ind){
if (ind == \qblur\q)
{alert("testing onBlur")}
if (ind == \qfocus\q)
{alert("testing onFocus")}
}
</SCRIPT>
</head>
<body>
<form>
<input TYPE=TEXT SIZE=20 value=blur onAbort="Check
(\q/indexblur.html\q,\qblur\q);return;">
<input TYPE=TEXT SIZE=20 value=blur onBlur="Check
(\q/indexblur.html\q,\qblur\q);return;">
<input TYPE=TEXT SIZE=20 value=focus onFocus="Check
(\q/focus.html\q,\qfocus\q);return;">
<input TYPE=TEXT SIZE=20 value=focus onChange="Check
(\q/focus.html\q,\qfocus\q);return;">
<input TYPE=TEXT SIZE=20 value=focus onClick="Check
(\q/focus.html\q,\qblur\q);return;">
<br><br>
</form>
</body>
```

```
Rewriting ends
</html>
```

## 規則

```
<Attribute name="onClick" type="DJS"/>
<Function type="URL" name="Check" paramPatterns="y"/>
```

**備註 –** `<Function name="URL" name="Check" paramPatterns="y"/>` 爲 JavaScript 函數規則，並於 JavaScript 函數範例中詳細說明。

## 重新寫入後的 HTML

```
<html>
<head>
Rewriting starts
<script language="javascript">
function Check(test,ind){
if (ind == \qblur\q)
{alert("testing onBlur")}
if (ind == \qfocus\q)
{alert("testing onFocus")}
}
</SCRIPT>
</head>
<body>
<form>
<input TYPE=TEXT SIZE=20 value=blur onAbort="Check
(\qgateway URL/portal-server-URL/indexblur.html\q,\qblur\q);return;">
<input TYPE=TEXT SIZE=20 value=blur onBlur="Check
(\qgateway URL/portal-server-URL/indexblur.html\q,\qblur\q);return;">
<input TYPE=TEXT SIZE=20 value=focus onFocus="Check
(\qgateway URL/portal-server-URL/focus.html\q,\qfocus\q);return;">
<input TYPE=TEXT SIZE=20 value=focus onChange="Check
(\qgateway URL/portal-server-URL/focus.html\q,\qfocus\q);return;">
<input TYPE=TEXT SIZE=20 value=focus onClick="Check
(\qgateway URL/portal-server-URL/focus.html\q,\qblur\q);return;">
```

// 所有敘述是依照此範例重寫。已在每種情況中前置閘道 URL 與 Portal Server URL。這是因爲 `onAbort`、`onBlur`、`onFocus`、`onChange` 與 `onClick` 的規則都已在 `default_gateway_ruleset` 檔案中定義。Rewriter 會偵測 JavaScript 記號，並將之傳送至 JavaScript 函數規則中以便進行進一步的處理。此範例中的第二個規則會告知 Rewriter 該重新寫入哪一個參數。

```
</body>
<br>
```

```
Rewriting ends

</html>
```

### HTML 表單範例

#### ▼ 使用表單範例

1. 您可自下列路徑存取表單範例：
   *portal-server-URL*/rewriter/HTML/forms/formrule.html
2. 請確定您已於閘道服務的 [網域與子網域的代理伺服器] 清單中定義 `abc.sesta.com`。
   若未定義，則會採用直接連接，且不前置閘道 URL。
3. 將此範例中指定的規則新增至 [重新寫入 HTML 屬性的規則] 部分的 `default_gateway_ruleset` 中。
4. 在 Portal Server 管理主控台的 Portal Server 配置下，編輯 Rewriter 服務中的 `default_gateway_ruleset`。
5. 從終端機視窗重新啓動閘道：

```
./psadmin start-sra-instance –u amadmin – f  <password file> –N <profile name>– t  <gateway>
```

### 重新寫入前的 HTML 網頁

```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
</head>
<body>
RW_START
<p>
<form name="form1" method="Post" action=
"http://abc.sesta.com/casestudy/html/form.html">
<input type="hidden" name="name1" value="0|1234|/test.html">
<input type="hidden" name="name3" value="../../html/test.html">
<form name="form2" method="Post" action="
http://abc.sesta.com/testcases/html/form.html"><br>
<input type="hidden" name="name1" value="0|1234|
../../html/test.html"></form>
RW_END </p>
</body>
</html>
```

## 規則

```
<Form source="*" name="form1" field="name1" valuePatterns="0|1234|"/>
```

## 重新寫入後的 HTML 網頁

```
<HTML>
<HEAD>
RW_START
</HEAD>
<BODY>
<P>
<FORM name=form1  method=POST action="gateway-URL/http://abc.sesta.com/casestudy/html/form.html">
```

// 重新寫入此 URL 是因爲已在 `default_gateway_ruleset` 中將 `<Attribute name="action"/>` 定義爲 HTML 規則的一部分。由於此 URL 應該是絕對 URL，因此僅需前置閘道 URL。請確定您已於閘道服務的 [網域與子網域的代理伺服器] 清單中定義 `abc.sesta.com`。否則，會認爲是直接連接，而不會前置閘道 URL。

```
<input type=hidden name=name1 value=
"0|1234|gateway URL/portal-server-URL/test.html">
```

// 此處的表單名稱爲 `form1`，而欄位名稱則爲 `name1`。上述名稱與規則中指定的表單名稱與欄位名稱相符。規則指出 `valuePatterns` 爲 `0|1234|`，其符合此陳述式中的 `value`。因此會重新寫入出現在 `valuePattern` 之後的 URL。將前置 Portal Server URL 與閘道 URL。請參閱第 73 頁的 「在規則中與式樣相符」以取得 `valuePatterns` 的詳細資訊。

```
<input type=hidden name=name3 value="../../html/test.html">
```

// 未重新寫入此 URL 是因爲此 `name` 不符合規則中所指定的 `field` 名稱。

```
</FORM>
<FORM name=form2 method=POST action=
"gateway-URL/http://abc.sesta.com/casestudy/html/form.html"><BR>
```

// 重新寫入此 URL 是因爲已在預設規則集中將 `<Attribute name="action"/>` 定義爲 HTML 規則的一部分。由於此 URL 應該是絕對 URL，因此僅需前置閘道 URL。

```
<input type=hidden name=name1 value="0|1234|../../html/test.html">
```

// 不重新寫入此 URL 是因爲此表單名稱不符合規則中所指定的名稱。

```
</FORM>
</BODY>
RW_END
</HTML>
```

## HTML Applet 範例

### ▼ 使用 Applet 範例

1. **請取得 Applet 類別檔案。**`RewriteURLinApplet.class` **檔案位於下列位置：**

   *portal-server-URL*/rewriter/HTML/applet/appletcode

   出現 Applet 代碼之網頁的基準 URL 爲：

   *portal-server-URL*/rewriter/HTML/applet/rule1.html

2. **將此範例中指定的規則新增至 [重新寫入 HTML 屬性的規則] 部分的** `default_gateway_ruleset` **中。**

3. **在 Portal Server 管理主控台的 Portal Server 配置下，編輯 Rewriter 服務中的** `default_gateway_ruleset`。

4. **重新啓動閘道：**

```
./psadmin start-sra-instance –u amadmin – f  <password file> –N <profile name>– t  <gateway>
```

#### 重新寫入前的 HTML

```
<html>
Rewriting starts
<br>
<applet codebase=appletcode code=RewriteURLinApplet.class archive=/test>
<param name=Test1 value="/index.html">
<param name=Test2 value="../index.html">
<param name=Test3 value="../../index.html">
</applet>
Rewriting ends
</html>
```

#### 規則

```
<Applet source="*/rule1.html" code="RewriteURLinApplet.class" param="Test*" />
```

#### 重新寫入後的 HTML

```
<HTML>
Rewriting starts
<BR>
<APPLET codebase=gateway-URL/portal-server-URL
/rewriter/HTML/applet/appletcode=RewriteURLinApplet.class archive=/test>
```

// 重新寫入此 URL 是因爲規則 <Attribute name="codebase"/> 已呈現爲 default_gateway_ruleset 檔案的一部份。會前置閘道與 Portal Server URL 以及至 appletcode 目錄的路徑。

```
<param name=Test1 value=
"gateway-URL/portal-server-URL/index.html">
```

// 重新寫入此 URL 是因爲此網頁的基準 URL 爲 rule1.html，且參數名稱符合規則中指定的參數 Test*。由於已將 index.html 指定放置於根層級，因此將直接前置閘道與 Portal Server URL。

```
<param name=Test2 value="gateway-URL
/portal-server-URL/rewriter/HTML/index.html">
```

// 重新寫入此 URL 是因爲此網頁的基準 URL 爲 rule1.html，且參數名稱符合規則中指定的參數 Test*。將依需要前置路徑。

```
<param name=Test3 value="gateway-URL
/portal-server-URL/rewriter/index.html">
```

// 重新寫入此 URL 是因爲此網頁的基準 URL 爲 rule1.html，且參數名稱符合規則中指定的參數 Test*。將依需要前置路徑。

```
</APPLET>
Rewriting ends
</HTML>
```

# JavaScript 內容範例

## JavaScript URL 變數的範例

### ▼ 使用 JavaScript URL 變數範例

1. **您可自下列路徑存取此範例：**
   *portal-server-URL* /rewriter/JavaScript/variables/url/js_urls.html
2. **請確定您已於閘道服務的 [網域與子網域的代理伺服器] 清單中定義** abc.sesta.com。
   若未定義，則會採用直接連接，且不前置閘道 URL。
3. **將此範例中指定的規則新增至 [重新寫入 JavaScript 來源的規則] 部分的** default_gateway_ruleset **中。**
4. **在 Portal Server 管理主控台的 Portal Server 配置下，編輯 Rewriter 服務中的** default_gateway_ruleset。

5 若您新增此規則，請重新啓動閘道：

```
./psadmin start-sra-instance –u amadmin – f  <password file> –N <profile name>– t  <gateway>
```

## 重新寫入前的 HTML 網頁

```
<html>
Rewriting starts
<head>
<title>JavaScript Variable test page</title>
</head>
<body>
<script LANGUAGE="Javascript">
<!--
//URL Variables
var imgsrc="/tmp/tmp.jpg";
var imgsrc="./tmp/tmp.jpg";
var imgsrc="../tmp/tmp.jpg";
var imgsrc="../../tmp/tmp.jpg";
var imgsrc="http://abc.sesta.com/tmp/tmp.jpg";
var imgsrc="../../../tmp/tmp.jpg";
var imgsrc="tmp/tmp.jpg";
//-->
</SCRIPT>
<br>
Testing JavaScript variables!
<br>
<img src="images/logo.gif">
<br>
Image
</body>
<br>
Rewriting ends
</html>
```

## 規則

```
<Variable name="imgsrc" type="URL"/>
```

## 重新寫入後的 HTML 網頁

```
<html>
Rewriting starts
<head>
<title>JavaScript Variable test page</title>
</head>
<body>
<script LANGUAGE="Javascript">
```

```
<!--
//URL Variables
var imgsrc="gateway-URL/portal-server-URL/tmp/tmp.jpg";
var imgsrc="gateway-URL/portal-server-URL
/rewriter/JavaScript/variables/url/tmp/tmp.jpg";
var imgsrc="gateway-URL/portal-server-URL
/rewriter/JavaScript/variables/tmp/tmp.jpg";
var imgsrc="gateway-URL/portal-server-URL
/rewriter/JavaScript/tmp/tmp.jpg";
var imgsrc="gateway-URL/http://abc.sesta.com/tmp/tmp.jpg";
var imgsrc="gateway-URL/portal-server-URL/rewriter/tmp/tmp.jpg";
var imgsrc="gateway-URL/portal-server-URL
/rewriter/JavaScript/variables/url/tmp/tmp.jpg";
```

// 上列所有 URL 皆爲規則中所指定的 URL 類型且名稱爲 `imgsrc` 的 JavaScript 變數。因此皆會前置閘道與 Portal Server URL。將依需前置位於 Portal Server URL 後的路徑。

```
//-->
</SCRIPT>
<br>
Testing JavaScript variables!
<br>
<img src="gateway URL/portal-server-URL/rewriter
/JavaScript/variables/url/images/logo.gif">
```

// 重新寫入此行是因爲已於 `default_gateway_ruleset` 中定義規則 `<Attribute name="src"/>`

```
<br>
Image
</body>
<br>
Rewriting ends
</html>
```

## JavaScript EXPRESSION 變數範例

### ▼ 使用 JavaScript EXPRESSION 變數範例

1. **您可自下列路徑存取此範例：**

   *portal-server-URL* /rewriter/JavaScript/variables/expr/expr.html

2. **將此範例中指定的規則新增 (若尚不存在) 至 [重新寫入 JavaScript 來源的規則] 部分的** `default_gateway_ruleset` **中。**

3. 在 Portal Server 管理主控台的 Portal Server 配置下，編輯 Rewriter 服務中的 `default_gateway_ruleset`。

4. 若您新增此規則，請重新啓動閘道：

```
./psadmin start-sra-instance –u amadmin – f  <password file> –N <profile name>– t  <gateway>
```

## 重新寫入前的 HTML 網頁

```
<html>
<head>
<title>JavaScript EXPRESSION Variables Test Page</title>
</head>
<body>
<script LANGUAGE="Javascript">
<!--
//Expression variables
var expvar1="images";
var expvar2="/logo.gif";
var expvar = expvar1 + expvar2;
document.write("<A HREF="+expvar+">EXPRESSION</A><P>")
var expvar="/images/logo"+".gif";
document.write("<A HREF="+expvar+">EXPRESSION</A><P>")
//-->
</SCRIPT>
Testing JavaScript EXPRESSION variables
</body>
</html>
```

## 規則

```
<Variable type="EXPRESSION" name="expvar"/>
```

## 重新寫入後的 HTML 網頁

```
<html>
<head>
<title>JavaScript EXPRESSION Variables Test Page</title>
</head>
<body>
<SCRIPT>
// Rewriter appends the wrapper function
psSRAPRewriter_convert_expression here
</SCRIPT>
<script LANGUAGE="Javascript">
<!--
//Expression variables
var expvar1="images";
```

```
var expvar2="/logo.gif";
var expvar =psSRAPRewriter_convert_expression( expvar1 + expvar2);
```

// Rewriter 會將此陳述式右側識別爲 JavaScript EXPRESSION 變數。Rewriter 無法在伺服器端計算出此表示式的值。因此，psSRAPRewriter_convert_expression 函數會被置於此表示式之前。此表示式將於用戶端計算，並視需要重新寫入。

```
document.write("<A HREF="+expvar+">EXPRESSION</A><P>")
```

// 將使用前一個陳述式之 expvar 的重新寫入值來計算此表示式的值。由於結果爲一有效的 URL (範例中此處出現一個圖形)，因此連結有效。

```
var expvar="gateway URL/portal-server-URL/images/logo"+".gif";
```

// Rewriter 會將 expvar 的右側識別爲字串表示式。此表示式可於伺服端計算，因此可直接重新寫入。

```
document.write("<A HREF="+expvar+">EXPRESSION</A><P>")
```

// 將使用前一個陳述式之 expvar 的重新寫入值來計算此表示式的值。由於結果不是有效的 URL (於結果位置中未出現圖形)，因此連結無效。

```
//-->
</SCRIPT>
Testing JavaScript EXPRESSION variables
</body>
</html>
```

## JavaScript DHTML 變數的範例

### ▼ 使用 JavaScript DHTML 變數範例

1. **您可自下列路徑存取此範例：**

   *portal-server-URL* /rewriter/JavaScript/variables/dhtml/dhtml.html

2. **請確定您已於閘道服務的 [網域與子網域的代理伺服器] 清單中定義** `abc.sesta.com`**。若未定義，則會採用直接連接，且不前置閘道 URL。**

3. **將此範例中指定的規則新增 (若尚不存在) 至 [重新寫入 JavaScript 來源的規則] 部分的** `default_gateway_ruleset` **中。在 Portal Server 管理主控台的 Portal Server 配置下，編輯 Rewriter 服務中的** `default_gateway_ruleset`**。**

4. **若您新增此規則，請重新啓動閘道：**

```
./psadmin start-sra-instance –u amadmin – f  <password file> –N <profile name>– t  <gateway>
```

## 重新寫入前的 HTML 網頁

```
<html>
<head>
<title>JavaScript DHTML Variable Test Page</title>
</head>
<body>
<script LANGUAGE="Javascript">
<!--
//DHTML Var
var dhtmlVar="<a href=../../images/test.html>"
var dhtmlVar="<a href=/../images/test.html>"
var dhtmlVar="<a href=/images/test.html>"
var dhtmlVar="<a href=images/test.html>"
var dhtmlVar="<a href=http://abc.sesta.com/images/test.html>"
var dhtmlVar="<img src=http://abc.sesta.com/images/test.html>"
//-->
</SCRIPT>
<br><br>
Testing DHTML Variables
<br><br>
<img src="images/logo.gif">IMAGE
</body>
</html>
```

## 規則

```
<Variable name="DHTML">dhtmlVar</Variable>
```

## 重新寫入後的 HTML 網頁

```
<html>
<head>
<title>JavaScript DHTML Variable Test Page</title>
</head>
<body>
<script LANGUAGE="Javascript">
<!--
//DHTML Var
var dhtmlVar="<a href=gateway-URL/portal-server-URL
/rewriter/JavaScript/images/test.html>"
```

// JavaScript DHTML 規則會將 `dhtmlVar` 的右側識別爲動態 HTML 內容。因此會套用 `default_gateway_ruleset` 檔案中的 HTML 規則。動態 HTML 包含 `href` 屬性。`default_gateway_ruleset` 定義規則 `<Attribute name="href"/>`。因此會重新寫入 `href` 屬性的值。但是 URL 並非絕對，因此網頁的基準 URL 與所需子目錄會取代相對 URL。最後會前置開道 URL 以導出最後的重新寫入輸出。

```
var dhtmlVar="<a href=gateway-URL
/portal-server-URL/../images/test.html>"
```

// 雖然已附加此網頁的基準 URL，且已前置閘道 URL，但是最後的 URL 卻無效。這是因爲初始 URL `/../images/test.html` 不正確。

```
var dhtmlVar="<a href=gateway-URL
/portal-server-URL/images/test.html>"
```

// 同樣，JavaScript DHTML 規則會將右側識別爲動態 HTML 內容，並將之傳送至 HTML 規則。將套用 `default_gateway_ruleset` 中的 HTML 規則 `<Attribute name="href"/>`，且已如所示重新寫入陳述式。已前置閘道 URL 與 Portal Server URL。

```
var dhtmlVar="<a href=gateway URL/portal-server-URL/
rewriter/JavaScript/variables/dhtml/images/test.html>"
var dhtmlVar="<a href=gateway URL/http://abc.sesta.com/images/test.html>"
var dhtmlVar="<img src=gateway-URL/
http://abc.sesta.com/images/test.html>"
```

// JavaScript DHTML 規則會識別右側的動態 HTML 內容，並將陳述式傳送至 HTML 規則。將套用 `default_gateway_ruleset` 中的 `<Attribute name="src"/>` 規則。由於此 URL 是絕對 URL，因此僅需前置閘道 URL。請確定您已於 [網域與子網域的代理伺服器] 清單中定義 `abc.sesta.com` 以便重新寫入此 URL。

```
//-->
</SCRIPT>
<br><br>
Testing DHTML Variables
<br><br>
<img src="gateway-URL/portal-server-URL/
rewriter/JavaScript/variables/dhtml/images/logo.gif">
```

// 重新寫入此行是因爲已於 `default_gateway_ruleset` 中定義規則 `<Attribute name="src"/>`。

```
<br><br>
Image
</body>
</html>
```

## JavaScript DJS 變數的範例

### ▼ 使用 JavaScript DJS 變數範例

**1 您可自下列路徑存取此範例：**

*portal-server-URL* /rewriter/JavaScript/variables/djs/djs.html

2. 請確定您已於閘道服務的 [網域與子網域的代理伺服器] 清單中定義 `abc.sesta.com`。若未定義，則會採用直接連接，且不前置閘道 URL。

3. 將此範例中指定的兩個規則新增 (若尚不存在) 至 [重新寫入 JavaScript 來源的規則] 部分的 `default_gateway_ruleset` 中。在 Portal Server 管理主控台的 Portal Server 配置下，編輯 Rewriter 服務中的 `default_gateway_ruleset`。

4. 重新啓動閘道：

```
./psadmin start-sra-instance –u amadmin – f  <password file> –N <profile name>– t  <gateway>
```

## 重新寫入前的 HTML 網頁

```
<html>
<head>
<title>Dynamic JavaScript Variable Test Page</title>
</head>
<body>
<script LANGUAGE="Javascript">
<!--
var dJSVar="var dJSimgsrc=\q/tmp/tmp/jpg\q;"
var dJSVar="var dJSimgsrc=\q../../../tmp/tmp/jpg\q;"
var dJSVar="var dJSimgsrc=\qhttp://abc.sesta.com/tmp/tmp/jpg\q;"
//-->
</SCRIPT>
<br>
Testing Dynamic JavaScript Variables
<br>
<img src="images/logo.gif">
<br>
Image
</body>
</html>
```

## 規則

```
<Variable name="dJSVar" type="DJS"/>
<Variable name="dJSimgsrc" type="URL"/>
```

## 重新寫入後的 HTML 網頁

```
<html>
<head>
<title>Dynamic JavaScript Variable Test Page</title>
</head>
<body>
<script LANGUAGE="Javascript">
<!--
```

```
var dJSVar="var dJSimgsrc=\qgateway-URL
/portal-server-URL/tmp/tmp/jpg\q;"
var dJSVar="var dJSimgsrc=\qgateway-URL
/portal-server-URL/rewriter/tmp/tmp/jpg\q;"
var dJSVar="var dJSimgsrc=\qgateway-URL
/http://abc.sesta.com/tmp/tmp/jpg\q;"
```

// 所有上述陳述式皆會使用閘道及 Portal Server URL 重新寫入。將依需要前置適當的路徑。第一個規則會將 `dJSVar` 右側識別爲動態 JavaScript 變數。然後傳送至第二個規則；第二個規則會將 `dJSimgsrc` 右側識別爲 URL 類型的 JavaScript 變數。將相應進行重新寫入。

```
//-->
</SCRIPT>
<br>
Testing Dynamic JavaScript Variables
<br>
<img src="gateway-URL/portal-server-URL
/rewriter/JavaScript/variables/djs/images/logo.gif">
```

// 重新寫入此行是因爲已於 `default_gateway_ruleset` 中定義規則 `<Attribute name="src"/>`。

```
<br>
Image
</body>
</html>
```

## JavaScript SYSTEM 變數的範例

### ▼ 使用 JavaScript SYSTEM 變數範例

1. **您可自下列路徑存取此範例：**
   *portal-server-URL* /rewriter/JavaScript/variables/system/system.html
2. **將此範例中指定的規則新增 (若尚不存在) 至 [重新寫入 JavaScript 來源的規則] 部分的 `default_gateway_ruleset` 中。**
3. **在 Portal Server 管理主控台的 Portal Server 配置下，編輯 Rewriter 服務中的 `default_gateway_ruleset`。**
4. **重新啓動閘道：**

```
./psadmin start-sra-instance –u amadmin – f  <password file> –N <profile name>– t  <gateway>
```

## 重新寫入前的 HTML 網頁

```
<html>
<head>
<title>JavaScript SYSTEM Variables Test Page</title>
</head>
<body>
<script LANGUAGE="Javascript">
<!--
//SYSTEM Var
alert(window.location.pathname);
//document.write
("<A HREF="+window.location.pathname+">SYSTEM</A><P>")
//-->
</SCRIPT>
Testing JavaScript SYSTEM Variables
<br>
This page displays the path where
the current page is located when loaded.
</body>
</html>
```

## 規則

```
<Variable name="window.location.pathname" type="SYSTEM"/>
```

## 重新寫入後的 HTML

```
<html>
<head>
<title>JavaScript SYSTEM Variables Test Page</title>
</head>
<body>
<SCRIPT>
convertsystem function definition...
</SCRIPT>
<script LANGUAGE="Javascript">
<!--
//SYSTEM Var
alert(psSRAPRewriter_convert_system
(window.location, window.location.pathname, "window.location"));
```

// Rewriter 會將 `window.location.pathname` 識別爲 JavaScript SYSTEM 變數。此變數的值無法於伺服器端判定。因此 Rewriter 會在變數前前置 `psSRAPRewriter_convert_pathname` 函數。此包裝函數可於用戶端判定此變數的值，然後依需要重新寫入。

```
//-->
</SCRIPT>
Testing JavaScript SYSTEM Variables
<br>
This page displays the path where
the current page is located when loaded.
</body>
</html>
```

### JavaScript URL 函數的範例

## ▼ 使用 JavaScript URL 函數範例

1. 您可自下列路徑存取此範例：

   *portal-server-URL* /rewriter/JavaScript/functions/url/url.html

2. 將此範例中指定的規則新增 (若尚不存在) 至 [重新寫入 JavaScript 來源的規則] 部分的 `default_gateway_ruleset` 中。在 **Portal Server** 管理主控台的 **Portal Server** 配置下，編輯 **Rewriter** 服務中的 `default_gateway_ruleset`。

3. 重新啓動閘道：

```
./psadmin start-sra-instance –u amadmin – f  <password file> –N <profile name>– t  <gateway>
```

### 重新寫入前的 HTML 網頁

```
<html>
<body>
JavaScript URL Function Test Page
<br>
<script language="JavaScript">
<!--
function test(one,two,three)
{
alert(one + "##" + two + "##" +three);
}
test("/test.html","../test.html","123");
window.open("/index.html","gen",width=500,height=500);
//-->
</SCRIPT>
</body>
</html>
```

### 規則

```
<Function type="URL" name="test" paramPatterns="y,y"/>
<Function type="URL" name="window.open" paramPatterns="y"/>
```

### 重新寫入後的 HTML 網頁

```
<html>
<body>
JavaScript URL Function Test Page
<br>
<script language="JavaScript">
<!--
function test(one,two,three)
{
alert(one + "##" + two + "##" +three);
}
test("/test.html","../test.html","123");
window.open("gateway-URL/portal-server-URL
/index.html","gen",width=500,height=500);
//-->
</SCRIPT>
</body>
</html>
```

## JavaScript EXPRESSION 函數的範例

## ▼ 使用 JavaScript EXPRESSION 函數範例

1. 您可自下列路徑存取此範例：

   ```
   <portal-install-location>/SUNWportal/samples/rewriter
   ```

2. 將此範例中指定的規則新增 (若尚不存在) 至重新寫入 `JavaScript` 來源的規則部分的 `default_gateway_ruleset` 中。

3. 使用 **Portal Server** 管理主控台中的 **Rewriter** 服務來編輯 `default_gateway_ruleset`。

4. 重新啓動閘道：

```
./psadmin start-sra-instance –u amadmin – f  <password file> –N <profile name>– t  <gateway>
```

### 重新寫入前的 HTML 網頁

```
<html>
<body>
JavaScript EXPRESSION Function Test Page
<br><br><br>
<script language="JavaScript">
<!--
function jstest2()
{
```

```
return ".html";
}
function jstest1(one)
{
return one;
}
var dir="/images/test"
var test1=jstest1(dir+"/test"+jstest2());
document.write("<a HREF="+test1+">Test</a>");
alert(test1);
//-->
</SCRIPT>
</body>
</html>
```

## 規則

```
<Function type="EXPRESSION" name="jstest1" paramPatterns="y"/>
```

## 重新寫入後的 HTML 網頁

```
<html>
<body>
JavaScript EXPRESSION Function Test Page
<br><br><br>
<script>
<!--
// various functions including psSRAPRewriter_
convert_expression appear here.//-->
</SCRIPT>
<script language="JavaScript">
<!--
function jstest2()
{
return ".html";
}
function jstest1(one)
{
return one;
}
var dir="/images/test"
var test1=jstest1(psSRAPRewriter_convert_
expression(dir+"/test"+jstest2()));
```

// 此規則指出函數 `jstest1` 中類型爲 EXPRESSION 的第一個參數需要重新寫入。此表示式的值爲 `/test/images/test.html`。此值會被前置 Portal Server URL 與閘道 URL。

```
document.write("<a HREF="+test1+">Test</a>");
alert(test1);
//-->
</SCRIPT>
</body>
</html>
```

### JavaScript DHTML 函數的範例

## ▼ 使用 JavaScript DHTML 函數範例

1. 您可自下列路徑存取此範例：
   *portal-server-URL* /rewriter/JavaScript/functions/dhtml/dhtml.html
2. 將此範例中指定的規則新增 (若尚不存在) 至 [重新寫入 JavaScript 來源的規則] 部分的 `default_gateway_ruleset` 中。
3. 在 Portal Server 管理主控台的 Portal Server 配置下，編輯 Rewriter 服務中的 `default_gateway_ruleset`。
4. 重新啓動閘道：

```
./psadmin start-sra-instance –u amadmin – f  <password file> –N <profile name>– t  <gateway>
```

### 重新寫入前的 HTML 網頁

```
<html>
<head>
Testing JavaScript DHTML Functions
<br>
<br>
<script>
<!--
document.write(\q<a href="/index.html">write</a><BR>\q)
document.writeln(\q<a href="index.html">writeln</a><BR>\q)
document.write("http://abc.sesta.com/index.html<BR>")
document.writeln("http://abc.sesta.com/index.html<BR>")
//-->
</SCRIPT>
</head>
<body BGCOLOR=white>
<br><br>
Testing document.write and document.writeln
</body>
</html>
```

## 規則

```
<Function type="DHTML" name=" document.write" paramPatterns="y"/>
<Function type="DHTML" name=" document.writeln" paramPatterns="y"/>
```

## 重新寫入後的 HTML 網頁

```
<html>
<head>
Testing JavaScript DHTML Functions
<br>
<br>
<script>
<!--
document.write(\q<a href="gateway-URL
/portal-server-URL/index.html">write</a><BR>\q)
```

// 第一個規則指出 DHTML JavaScript 函數 `document.write` 的第一個參數需要重新寫入。Rewriter 會將第一個參數識別爲一個簡單的 HTML 陳述式。在 `default_gateway_ruleset` 中的 HTML 規則部分具有規則 `<Attribute name="href" />`，此規則指出此陳述式需重新寫入。

```
document.writeln(\q<a href="gateway-URL
/portal-server-URL/rewriter/JavaScript/functions/dhtml/index.html">writeln</a><BR>\q)
```

// 第二個規則指出 DHTML JavaScript 函數 `document.writeln` 的第一個參數需要重新寫入。Rewriter 會將第一個參數識別爲一個簡單的 HTML 陳述式。在 `default_gateway_ruleset` 中的 HTML 規則部分具有規則 `<Attribute name="href" />`，此規則指出此陳述式需重新寫入。

```
document.write("http://abc.sesta.com/index.html<BR>")
document.writeln("http://abc.sesta.com/index.html<BR>")
```

// 雖然 DHTML 規則識別出函數 `document.write` 與 `document.writeln`，但上述陳述式並未重新寫入。這是因爲這個情況下的第一個參數並非簡單 HTML。其可能是任何字串而 Rewriter 不知如何將之重新寫入。

```
//-->
</SCRIPT>
</head>
<body BGCOLOR=white>
<br><br>
Testing document.write and document.writeln
</body>
</html>
```

## JavaScript DJS 函數的範例

### ▼ 使用 JavaScript DJS 函數範例

1 您可自下列路徑存取此範例：

*portal-server-URL* /rewriter/JavaScript/functions/djs/djs.html

2 請確定您已於閘道服務的 [網域與子網域的代理伺服器] 清單中定義 `abc.sesta.com`。

若未定義，則會採用直接連接，且不前置閘道 URL。

3 將此範例中指定的規則新增 (若尚不存在) 至 [重新寫入 JavaScript 來源的規則] 部分的 `default_gateway_ruleset` 中。在 Portal Server 管理主控台的 Portal Server 配置下，編輯 Rewriter 服務中的 `default_gateway_ruleset`。

4 重新啓動閘道：

```
./psadmin start-sra-instance –u amadmin – f  <password file> –N <profile name>– t  <gateway>
```

#### 重新寫入前的 HTML 網頁

```
<html>
Test for JavaScript DJS Functions
<br>
<script>
menu.addItem(new NavBarMenuItem("All Available
Information","JavaScript:top.location=\qhttp://abc.sesta.com\q"));
//menu.addItem(new NavBarMenuItem("All Available Information","http://abc.sesta.com"));
</script>
</html>
```

#### 規則

```
<Function type="DJS" name="NavBarMenuItem" paramPatterns=",y"/>
<Variable type="URL" name="top.location"/>
```

#### 重新寫入後的 HTML 網頁

```
<html>
Testing JavaScript DJS Functions
<br>
<script>
menu.addItem(new NavBarMenuItem
("All Available Information","javaScript:top.location=
\qgateway-URL/http://abc.sesta.com\q"));
```

// abc.sesta.com 是閘道服務的 [網域與子網域的代理伺服器] 清單中的一項。因此 Rewriter 需要重新寫入此 URL。但因爲是絕對 URL，因此不需前置 Portal Server URL。DJS 規則指出 DJS 函數 NavBarMenuItem 的第二個參數需重新寫入。但是第二個參數又是 JavaScript 變數。重新寫入此變數的值需要第二個規則。第二個規則指出 JavaScript 變數 top.location 的值需重新寫入。由於符合所有條件，因此重新寫入 URL。

```
//menu.addItem(new NavBarMenuItem("All Available Information","http://abc.sesta.com"));
```

// 雖然 DJS 規則指出函數 NavBarMenuItem 的第二個參數需要重新寫入，但此陳述式中並未進行重新寫入。這是因爲 Rewriter 未將第二個參數識別爲簡單 HTML。

```
</script>
</html>
```

# XML 屬性範例

## ▼ 使用 XML 屬性範例

1. **您可自下列路徑存取此範例：**

   *portal-server-URL* /rewriter/XML/attrib.html

2. **將此範例中指定的規則新增 (若尚不存在) 至 [重新寫入 XML 來源的規則] 部分的 default_gateway_ruleset 中。**

3. **在 Portal Server 管理主控台的 Portal Server 配置下，編輯 Rewriter 服務中的 default_gateway_ruleset。**

4. **重新啓動閘道：**

```
./psadmin start-sra-instance –u amadmin – f  <password file> –N <profile name>– t  <gateway>
```

### 重新寫入前的 XML

```
<html>
RW_START
<body>
<xml>
<baseroot href="/root.html"/>
</xml>
<xml>
<img href="image.html"/>
</xml>
<xml>
<string href="1234|substring.html"/>
```

```
</xml>
<xml>
<check href="1234|string.html"/>
</xml>
</body>
RW_END
</html>
```

### 規則

```
<Attribute name="href" tag="check" valuePatterns="1234|"/>
```

### 重新寫入後的 HTML

```
<html>
Rewriting starts
<br>
<br>
<body>
<xml><baseroot href="/root.html"/></xml>
<xml><img href="image.html"/></xml>
<xml><string href="1234|substring.html"/></xml>
<xml><check href="1234|gateway-URL/portal-server-URL
/rewriter/XML/string.html"/></xml>
```

// 重新寫入此陳述式是因爲其符合規則中所指定的條件。`Attribute name` 是 `href`，`tag` 是 `check` 而 `valuePatterns` 是 `1234`。`valuePatterns` 之後所接的字串會被重新寫入。請參閱第 73 頁的「在規則中與式樣相符」以取得 `valuePatterns` 的詳細資訊。

```
</body>
Rewriting ends
</html>
```

# 案例研究

本節包括某範例郵件用戶端的來源 HTML 網頁。此案例研究並未囊括所有可能的情況與規則。這只是一個範例規則集，用以幫助您爲自己的企業內部網路網頁收集規則。

## 假設狀況

針對此案例研究訂出下列假設狀態：

- 郵件用戶端的基準 URL 假設爲 `abc.siroe.com`
- 閘道 URL 假設爲 `gateway.sesta.com`
- 位於閘道服務的 [網域與子網域的代理伺服器] 清單中的相關項目

## 範例網頁 1

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<!-- saved from url=(0053)http://abc.siroe.com/mailclient/destin/?Cmd=navbar -->
<HTML XMLNS:WM><HEAD>
<META http-equiv=Content-Type content="text/html; CHARSET=utf-8">
<META http-equiv=Pragma content=no-cache>
<META http-equiv=Expires content=0><!--Copyright (c) 2000 Microsoft Corporation.
All rights reserved.--><!--CURRENT FILE== "IE5" "WIN32" navbar -->
<STYLE>WM\\:DROPMENU {
BEHAVIOR: url(http://abc.siroe.com/mailweb/controls/dropmenu.htc)
}
</STYLE>
<LINK href="destin_files/navbar.css" type=text/css rel=stylesheet>
<SCRIPT language=javascript>
var g_szUserBase= "http://abc.siroe.com/mailclient/destin"+"/";
var g_szFolder= ".";
var g_szVirtualRoot= "http://abc.siroe.com/mailweb";
var g_szImagePath= g_szVirtualRoot + "/img/";
</SCRIPT>
<SCRIPT src="/destin_files/navbar.js"></SCRIPT>
<META content="MSHTML 6.00.2600.0" name=GENERATOR></HEAD>
<BODY oncontextmenu=return(event.ctrlKey); onselectstart=return(false);
id=outbar_mainbody style="BACKGROUND-COLOR: appworkspace" leftMargin=0
topMargin=0 scroll=no>
<TABLE class=nbTableMain id=nbTableMain style="HEIGHT: 100%" cellSpacing=0
cols=1 cellPadding=0 rows="2">
<TBODY>
<TR>
<TD class=treeBrand>
<DIV class=treeOFLOW><IMG
style="PADDING-RIGHT: 0px; PADDING-LEFT: 0px; PADDING-BOTTOM: 0px; PADDING-TOP: 0px"
src="/destin_files/logo-ie5.gif" border=0></DIV></TD></TR>
<TR height="100%">
<TD>
<TABLE class=nbTable cellSpacing=0 cols=1 cellPadding=0 rows="4">
<TBODY>
<TR>
<TD class=nbFlybar id=show_navbar onkeydown=flybar_keydown()
onclick=ToggleTab(this.id) tabIndex=0 noWrap>
<DIV class=treeOFLOW>Shortcuts</DIV></TD></TR>
<TR style="HEIGHT: 100%">
<TD id=idOutbarpane style="TEXT-ALIGN: center" vAlign=top><A
id=inbox
href="http://abc.siroe.com/mailclient/destin/Inbox/?Cmd=contents&amp;Page=1"
target=viewer alt="Go to inbox"><IMG class=nbImage alt="Go to inbox"
src="destin_files/navbar-inbox.gif"></A>
<DIV class=nbLabel>Inbox</DIV><BR><A id=calendar
href="http://abc.siroe.com/mailclient/destin/Calendar/?Cmd=contents"
```

```
target=viewer alt="Go to calendar"><IMG class=nbImage
alt="Go to calendar" src="destin_files/navbar-calendar.gif"></A>
<DIV class=nbLabel>Calendar</DIV><BR><A id=contacts
            href="http://abc.siroe.com/mailclient/destin/Contacts/?Cmd=contents"
target=viewer alt="Go to contacts"><IMG class=nbImage
alt="Go to contacts" src="destin_files/navbar-contacts.gif"></A>
<DIV class=nbLabel>Contacts</DIV><BR><A id=options
href="http://abc.siroe.com/mailclient/destin/?Cmd=options"
target=viewer alt="Go to options"><IMG class=nbImage
alt="Go to options" src="destin_files/navbar-options.gif"></A>
<DIV class=nbLabel>Options</DIV></TD></TR>
<TR style="HEIGHT: 1.5em">
<TD class=nbFlybar id=show_folders onkeydown=flybar_keydown()
onclick=ToggleTab(this.id) tabIndex=0 noWrap>
<DIV class=treeOFLOW>Folders</DIV></TD></TR>
<TR>
<TD class=nbTreeProgress id=treeProgress style="DISPLAY: none"
vAlign=top noWrap><SPAN id=idLoading
style="OVERFLOW: hidden">Loading...</SPAN>
</TD></TR></TBODY></TABLE></TD></TR></TBODY></TABLE>
</BODY></HTML>
```

## 描述

第 121 頁的「描述」顯示範例規則集與案例研究之間的對應關係。

**表 4–3** 範例規則集與案例研究之間的對映

| 網頁內容 | 套用的規則 | Rewriter 輸出 | 描述 |
|---|---|---|---|
| `var g_szVirtualRoot= "http://abc.siroe.com /mailweb";` | <Variable name="URL"> g_szVirtualRoot </Variable> | `var g_szVirtualRoot= "http://gateway.sesta.com /http://abc.siroe.com /mailweb";` | `g_szVirtualRoot` 是一個變數，其值爲簡單 URL。<br>此規則告知 Rewriter 搜尋 URL 類型的 `g_szVirtualRoot` 變數。若網頁中有這類變數，則 Rewriter 會將之轉換爲絕對 URL，然後前置閘道 URL。 |
| `src="/destin_files/ logo-ie5.gif"` | <Attribute name="src" /> | `src="http://gateway. sesta.com/ http://abc.siroe.com/ destin_files/logo-ie5.gif` | src 是屬性名稱，未附有任何標記或 valuePattern。<br>此規則告知 Rewriter 搜尋所有名稱爲 `src` 的屬性，然後重新寫入該屬性的值。 |

表 4–3 範例規則集與案例研究之間的對映 (續)

| 網頁內容 | 套用的規則 | Rewriter 輸出 | 描述 |
|---|---|---|---|
| href="http://abc.siro<br><br>e.com<br><br>/mailclient/destin/Inbox/<br>?Cmd=contents&Page=1" | <Attribute<br>name="href"/> | href="http://gateway.<br><br>sesta.com/<br>http://abc.siroe.com<br>/mailclient/destin/<br>Inbox/?Cmd=contents&<br><br>amp;Page=1" | href 是屬性名稱，未附有任何標記或 valuePattern。<br>此規則告知 Rewriter 搜尋所有名稱爲 href 的屬性，然後重新寫入該屬性的值。 |

**備註 –** 套用規則集的優先順序爲 hostname-subdomain-domain。

例如，假設您的以網域爲基礎規則集清單中包含下列項目：

```
sesta.com|ruleset1
eng.sesta.com|ruleset2
host1.eng.sesta.com|ruleset3
```

ruleset3 可套用於 host1 上的所有頁面。

ruleset2 可套用於 eng 子網域中的所有頁面，除了擷取於 host1 中的頁面。

ruleset1 可套用於 sesta.com 網域中的所有頁面，除了擷取於 eng 子網域與 host1 中的頁面。

1. 按一下 [儲存] 完成作業。
2. 從終端機視窗重新啓動閘道：

```
./psadmin start-sra-instance –u amadmin – f  <password file> –N <profile name>– t  <gateway>
```

### Outlook Web Access 的規則集

Secure Remote Access 伺服器支援 Sun Java System Web Server 和 IBM 應用程式伺服器上 Outlook Web Access (OWA) 的 MS Exchange 2000 SP3 以及 MS Exchange 2003 安裝。

## ▼ 配置 OWA 規則集

**1 以管理員身份登入 Portal Server 管理主控台。**

**2 選取 [Secure Remote Access] 標籤，並選取要設定屬性的閘道設定檔。**

3 **在 [對映 URI 至規則集] 欄位中，輸入安裝 Exchange 2000 的服務其名稱，隨後輸入 Exchange 2000 Service Pack 4 OWA 規則集。**

例如：

```
exchange.domain.com|exchange_2000sp3_owa_ruleset.
```

### 使用公用資料夾

在 Exchange 端，「公用資料夾」被配置爲使用 NTLM 授權。必須將它變更爲使用 HTTP Basic Authorization。

要執行此作業，請至 Exchange 伺服器，選取 [控制台] -->[系統管理工具]，然後開啓 [網際網路資訊服務]。

在 [預設網站] 下，有一個名爲 [公用] 的「公用資料夾」標籤。按一下滑鼠右鍵，然後選取 [內容]。按一下 [目錄安全性] 標籤。在 [匿名存取及認證] 控制台上，選取 [編輯...]。消取選取所有其他選項，僅勾選 [Basic Authentication]。

## 6.x 與 3.0 規則集對映

下表列出 Secure Remote Access 伺服器 Rewriter 規則與前版 Portal Server 產品的對映關係。

**表 4–4** SP3 規則對映

| Rewriter 6.0 DTD 元素 | Rewriter 3.0 清單方塊名稱 |
|---|---|
| **HTML 內容的規則** | |
| 屬性 - URL | 重新寫入 HTML 屬性 |
| 屬性 - DJS | 重新寫入包含 JavaScript 的 HTML 屬性 |
| 表單 | 重新寫入表單輸入標記清單 |
| Applet | 重新寫入 Applet/物件參數值清單 |
| **JavaScript 內容的規則** | |
| 變數 - URL | 重新寫入 URL 中的 JavaScript 變數 |
| 變數 - EXPRESSION | 重新寫入 JavaScript 變數函數 |
| 變數 - DHTML | 重新寫入 HTML 中的 JavaScript 變數 |
| 變數 - DJS | 重新寫入 JavaScript 中的 JavaScript 變數 |
| 變數 - SYSTEM | 重新寫入 JavaScript 系統變數 |

表 4–4 SP3 規則對映 (續)

| Rewriter 6.0 DTD 元素 | Rewriter 3.0 清單方塊名稱 |
|---|---|
| 函數 - URL | 重新寫入 JavaScript 函數參數 |
| 函數 - EXPRESSION | 重新寫入 JavaScript 函數參數函數 |
| 函數 - DHTML | 重新寫入 HTML 中 JavaScript 函數參數函數 |
| 函數 - DJS | 重新寫入 JavaScript 中的 JavaScript 函數參數 |
| **XML 內容的規則** | |
| 屬性 - URL | 重新寫入 XML 文件的屬性值 |
| 標記文字 | 重新寫入 XMl 文件的文字資料 |
| **CSS 內容的規則** | |
| 不需使用規則。依預設，所有 URL 皆會被轉譯。 | |
| **WML 內容的規則** | |
| 未定義任何規則。按 HTML 處理 WML，並會套用 HTML 規則。 | |
| **WMLScript 內容的規則** | |
| | |
| 不支援 WML 程序檔 | |

◆ ◆ ◆ 第 5 章

# 5 使用 NetFile

本章說明 NetFile 及其作業。要配置 NetFile，請參閱第 14 章。


- 第 125 頁的 「NetFile 簡介」
- 第 125 頁的 「支援檔案存取協定」


## NetFile 簡介

NetFile 是一個檔案管理應用程式，可以讓使用者存取並操作遠端檔案系統和目錄。

Secure Remote Access 的 NetFile 元件以 Java2 Applet 的形式提供。Java2 applet 有比較好的介面，同時新增了存取的便利性。

NetFile 提供了下列的主要功能：

- 便於新增或移除共享或資料夾
- 檔案上傳與下載
- 搜尋檔案和資料夾
- 使用 GZIP 和 ZIP 壓縮檔案
- 在 NetFile 環境中的郵件功能
- 儲存目前 NetFile 階段作業的資訊
- 檔案的「拖放」

## 支援檔案存取協定

NetFile 允許使用 FTP， NFS 與 jCIFS (Microsoft Windows) 協定存取遠端系統。其中包含下列檔案存取協定功能：

- 如果使用者指定 AUTODETECT 新增系統，NetFile 會使用下列順序以自動偵測要使用的協定：
  - 檢查在 21 連接埠上的 FTP 伺服器。如果 FTP 的回應包含 "NetWare" 字串，則被視爲是一個 NETWARE 主機。

- 在 2049 埠上檢查 NFS 伺服器的主機。
- 在 139 連接埠上檢查 Microsoft Windows 的主機。
- 如果上述操作都失敗，會顯示訊息告訴您無法確定主機類型。

  第一個偵測到的檔案系統類型將用於連接所請求的主機。可在 Portal Server 管理主控台 (PSConsole) 中變更主機偵測順序。

**備註 –** 如果伺服器在非標準的連接埠上執行，連線會失敗。

- NetFile 能讓使用者任意選擇檔案伺服器和協定。

  支援這些協定的平台列於下表。

**表 5–1** 檔案系統和支援的協定

| 檔案系統/協定 | 平台 |
|---|---|
| FTP | 在 Novell Netware 上的 Novell FTP 5.1 Server<br>在 Win NT 4.0 上的 MS FTP Server 4.0<br>在 Win NT 2000 上的 MS FTP Server 5.0<br>Solaris FTP Server<br>WU_FTP 2.6.1<br>ProFTPD 1.2.8<br>vsFTPd 1.2.0 |
| NFS | Solaris 2.6 和更高版本 |
| jCIFS | Windows 95/98/NT/2000/ME/XP |

**備註 –** 要使用 NetFile 將檔案上傳至 ProFTPD 伺服器，需要在執行 ProFTPD 伺服器的主機中的 `proftpd.conf` 檔案中，將「AllowStoreRestart」設定爲「on」。

對 Novell Netware 的支援，僅能透過 FTP 伺服器而非透過本機存取。

要存取 Microsoft Windows (SMB/CIFS) 檔案系統，必須將 jCIFS 安裝於 Portal Server。jCIFS 是實作 CIFS/SMB 網路協定的「開放原始碼」的用戶端程式庫。

## ▼ 建立 NetFile 策略

1 以管理員身份登入 Portal 管理主控台。

2 選取 [Secure Remote Access] 標籤並選取 [NetFile] 標籤。

3 從 [選取 DN] 下拉式方塊中選取 [組織]/[角色]/[使用者]。

4 將權限設定為存取/拒絕主機與服務。

5 按一下 [儲存]。

6 重新啓動閘道。

◆ ◆ ◆ 第 6 章

# 使用 Netlet

本章會介紹如何使用 Netlet 在使用者遠端桌面以及在您的企業內部網路中執行應用程式的伺服器之間，以安全的方式執行應用程式。要配置 Netlet，請參閱第 11 章。

本章包含下列章節：


- 第 129 頁的 「Netlet 簡介」
- 第 132 頁的 「從遠端主機下載 Applet」
- 第 132 頁的 「定義 Netlet 規則」
- 第 143 頁的 「Netlet 規則範例」
- 第 146 頁的 「Netlet 記錄資訊」
- 第 146 頁的 「在 Sun Ray 環境中執行 Netlet」


## Netlet 簡介

Sun Java System Portal Server 軟體使用者可能希望在他們的遠端桌面上，以安全的方式執行最常使用或特定於公司的應用程式。在您的平台上設定 Netlet 之後，您就可以安全存取這些應用程式。

Netlet 可讓使用者透過不安全的網路，例如網際網路，安全地執行 一般 TCP/IP 服務。您可執行 TCP/IP 應用程式 (如 Telnet 和 SMTP)、HTTP 應用程式以及任何使用固定連接埠的應用程式。

如果應用程式是以 TCP/IP 爲基礎或使用固定的連接埠，您可以在 Netlet 上執行應用程式。

---

**備註 –** 只有在使用 FTP 時才支援動態連接埠。要使用 Microsoft Exchange，請使用 OWA (Outlook Web Access)。

請確定通知您的使用者在使用 Netlet 時，停用他們瀏覽器中的快顯式阻擋程式選項。

---

# Netlet 元件

Netlet 所用的不同元件會顯示於第 130 頁的「Netlet 元件」。

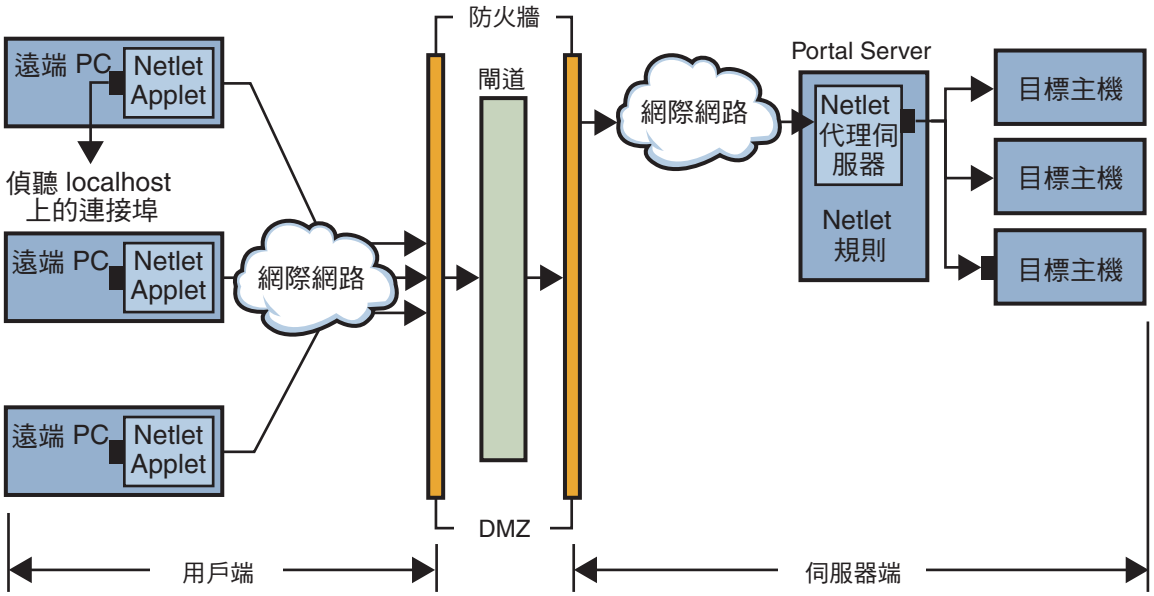



圖 6–1 Netlet 元件

## 位於 localhost 上的偵聽連接埠

此爲用戶端機器上 Netlet applet 偵聽的連接埠。用戶端機器爲 localhost。

## Netlet Applet

Netlet applet 負責在遠端用戶端機器和企業內部應用程式 (例如 Telnet、Graphon 或 Citrix) 之間設定加密的 TCP/IP 通道。Applet 會將封包加密並將它們傳送至閘道，並將來自閘道的回應封包解密，然後將它們傳送至本機的應用程式。

對於靜態規則，當使用者登入入口網站時，會自動下載 Netlet applet。對於動態規則，會在使用者在相對應的動態規則連結上按一下時，下載 applet。請參閱第 135 頁的「規則類型」以取得靜態與動態規則的詳細資訊。

要在 Sun Ray 環境中執行 Netlet，請參閱第 146 頁的「在 Sun Ray 環境中執行 Netlet」。

### Netlet 規則

Netlet 規則會將需要在用戶端機器上執行的應用程式映射至相應的目標主機。這表示 Netlet 只會在已傳送至連接埠 (於 Netlet 規則中定義) 的封包上運作。這可確保取得較大的安全性。

作爲管理員，您需要爲 Netlet 的功能運作配置一些規則。這些規則指定了各種詳細信息，例如要使用的加密、要呼叫的 URL、要下載的 applet、目標連接埠以及目標主機。當用戶端機器上的使用者透過 Netlet 提出請求時，這些規則會協助確定如何建立連線。請參閱第 132 頁的 「定義 Netlet 規則」以取得詳細資訊。

### Netlet 提供者

此爲 Netlet 的 UI 元件。提供者允許使用者透過 Portal Server 桌面配置必要的應用程式。會在提供者中建立連結，而使用者按一下連結以執行必要的應用程式。使用者也可以將桌面中動態規則的目標主機指定爲 Netlet 提供者。請參閱第 132 頁的 「定義 Netlet 規則」。

### Netlet 代理伺服器 (選擇性)

閘道可確保爲遠端用戶端機器以及閘道之間提供一條安全通道。Netlet 代理伺服器爲選用選項，您可以在安裝時選擇不安裝此代理伺服器。如需 Netlet 代理伺服器的資訊，請參閱第 47 頁的 「使用 Netlet 代理伺服器」。

## Netlet 使用方案

使用 Netlet 將會順序發生下列事件：

1. 遠端使用者登入至 Portal Server 桌面。
2. 如果已經爲使用者、角色或組織定義靜態 Netlet 規則，則將會自動下載 Netlet applet 至遠端用戶端。

   如果已經爲使用者、角色或組織定義動態規則，則使用者需要在 Netlet 提供者中配置必要的應用程式。當使用者按一下 Netlet 提供者中的應用程式連結時，將會下載 Netlet applet。請參閱第 132 頁的 「定義 Netlet 規則」以取得靜態與動態規則的詳細資訊。
3. Netlet 會偵聽在 Netlet 規則中定義的本機連接埠。
4. Netlet 會通過 Netlet 規則中指定的連接埠，設定遠端用戶端與主機之間的通道。

## 使用 Netlet

爲了使 Netlet 在運作時能夠符合不同組織中各種使用者的需要，您必須執行下列動作：

1. 依據使用者需求確定是否需要建立靜態或動態規則。請參閱第 135 頁的 「規則類型」。

2. 從 Portal Server 管理主控台配置 Netlet 服務的選項。如需配置 Netlet 的資訊，請參閱第 11 章。
3. 確定規則是否以組織、角色或使用者爲基礎，並視需要在每個層級中做出修改。如需組織、角色和使用者的詳細資訊，請參閱「Portal Server 管理指南」。

**備註 –** 請勿本地化在 `srapNetletServlet.properties` 檔案中的框架集參數的值。

# 從遠端主機下載 Applet

偶爾 URL 會傳回需要從遠端主機取得的內嵌 applet 之頁面。然而 Java 的安全性不允許 applet 與非其下載來源的主機進行通訊。要允許 applet 透過本機網路埠與閘道通訊，您必須核取 Access Manager 管理主控台上的 [下載 Applet] 欄位並指定以下語法：

*local-port:server-host:server-port*

其中

*local-port* 是 Netlet 偵聽來自 applet 流量的本機連接埠

*server-host* 是下載 applet 之處

*server-port* 是用來下載 applet 的連接埠

# 定義 Netlet 規則

Netlet 配置是 Netlet 規則所定義的，這些規則使用 [Secure Remote Access] 配置標籤下的 Portal Server 管理主控台配置。可爲組織、角色或使用者配置 Netlet 規則。如果 Netlet 規則用於角色或使用者，請在選取組織之後選取想要的角色或使用者。

**注意 –** Netlet 規則不支援多位元組輸入。請勿在 Netlet 規則中的任何欄位中指定多位元組字元。

Netlet 規則中不能包含任何高於 64000 的連接埠號。

第 132 頁的 「定義 Netlet 規則」會列出 Netlet 規則中的欄位。

**表 6–1** Netlet 規則中的欄位

| 參數 | 描述 | 值 |
|---|---|---|
| 規則名稱 | 指定此 Netlet 規則的名稱。您需要爲每個規則指定唯一的名稱。如此當您在定義使用者存取特定規則時將會非常有用。 | |
| 加密密碼 | 定義加密密碼，或是指定使用者可從中選擇的密碼清單。 | 您選取的密碼將會在 Netlet 提供者中以清單的形式出現。使用者可以從清單中選擇需要的密碼。<br>預設 - 會使用 Netlet 管理主控台中指定的 [預設 VM 原生密碼] 和 [預設 Java Plugin 密碼]。 |
| 遠端應用程式 URL | 指定當使用者按一下 Netlet 提供者中的相關連結時，瀏覽器所開啓的 URL。瀏覽器會開啓應用程式的視窗，並連接至稍後在規則中指定的本機連接埠號的 `localhost`。<br>您需要指定一個相對的 URL。 | Netlet 規則所呼叫之應用程式的 URL。例如，`telnet://localhost: 30000` 。<br>如果應用程式使用 applet 來呼叫應用程式，則指定一個 URL。<br>`null` – 如果應用程式不是由 URL 啓動或由桌面控制，請設定此值。對於不以網路爲基礎的應用程式而言，該項通常爲 true。 |
| 啓用下載 Applet | 指出是否需要爲此規則下載 applet。 | ■ *Client Port* 表示用戶端上的目標連接埠。此連接埠必須與預設的回送連接埠不同。爲每個規則指定唯一的**本機連接埠**。<br>■ *Server Host* 是會從該處下載 applet 的伺服器名稱。<br>■ *Server Port* 代表伺服器上用來下載 applet 的連接埠。<br>如果要下載 applet，而且未指定伺服器，則會從 Portal Server 主機下載 applet。 |
| 啓用延伸階段作業 | 此將控制 Netlet 爲使用中時 Portal Server 階段作業的閒置逾時。 | 僅在 Netlet 爲使用中且入口網站應用程式的其餘部分爲閒置時，選取此核取方塊以保持入口網站階段作業爲使用中。根據預設，不會選取此選項。 |

表 6–1 Netlet 規則中的欄位 *(續)*

| 參數 | 描述 | 值 |
| --- | --- | --- |
| 將本機連接埠對映至目標伺服器連接埠 | 本機連接埠 | Netlet 偵聽之用戶端上的連接埠。<br><br>*local-port* 的值必須唯一。您不能夠在一個以上的規則中指定某特定的連接埠號。<br><br>如果您要爲多個連線指定多個主機，請指定多個本機連接埠。請參閱第 139 頁的「包含多個主機連線的靜態規則」以取得語法。<br><br>對於 FTP 規則，本機連接埠值必須爲 30021。 |
| | 目標主機 | Netlet 偵聽之用戶端上的連接埠。<br><br>Netlet 連線的收件者。<br><br>*host* - 接收 Netlet 連線的主機名稱。此欄位用於靜態規則。使用簡單的主機名稱 (例如 `siroe`) 或完全合格的 DNS 式主機名稱 (例如 `siroe.mycompany.com`)。因下列原因指定多個主機：<br><br>*local-port* 的值必須唯一。您不能夠在一個以上的規則中指定某特定的連接埠號。<br><br>如果您要爲多個連線指定多個主機，請指定多個本機連接埠。請參閱第 139 頁的「包含多個主機連線的靜態規則」以取得語法。<br><br>對於 FTP 規則，本機連接埠值必須爲 30021。<br><br>與每個指定主機建立連線。您需要爲每個指定的主機指定相對應的用戶端以及目標連接埠。請參閱第 139 頁的「包含多個主機連線的靜態規則」以取得語法。<br><br>嘗試連接至指定主機清單中任何可用的主機。請參閱第 140 頁的「選擇多個主機的靜態規則」以取得語法。<br><br>`TARGET` - 在語法中指定 `TARGET` 的規則爲動態規則。`TARGET` 表示一般使用者能夠在桌面的 Netlet 提供者中指定一台或多台必要的目標主機。<br><br>在單個規則中，不可以同時有靜態主機和 TARGET。 |
| | | |

表 6–1 Netlet 規則中的欄位 *(續)*

| 參數 | 描述 | 值 |
|---|---|---|
| 目標連接埠 | 目標主機上的連接埠<br>除了主機與目標主機以外，您必須指定目標連接埠。<br>您可以在有多個目標主機的情況下，指定多個目標連接埠。以下列格式指定多個連接埠：`port1+port2+port3-port4+port5`。<br>連接埠號之間的加號 (+) 指出用於單一目標主機的替代連接埠。<br>連接埠號之間的減號 (-) 爲不同目標主機連接埠號的分隔符號。<br>Netlet 在此會嘗試依序使用 `port1`、`port2` 和 `port3` 連接至指定的第一台目標主機。如果此項操作失敗，Netlet 會嘗試以 `port4` 和 `port5` 依次連接至第二台主機。<br>您只可以爲靜態規則配置多個連接埠。 | |

閘道要從 Portal Server 取得階段作業通知時，新增下列指令行：

```
com.iplanet.am.jassproxy.trustAllServerCerts=true
```

至下列的特性檔中

Portal Server 上的 `/etc/opt/SUNWam/config/AMConfig.`*instance-name* `.properties`

# 規則類型

根據規則中指定目標主機的方式，Netlet 規則類型有兩種。

## 靜態規則

靜態規則會指定目標主機做爲規則的一部分。如果您建立一項靜態規則，使用者將無法指定需要的目標主機。在下列範例中，`sesta` 爲目標主機。

| 規則名稱 | 加密密碼 | URL | 啓用下載 Applet | 啓用延伸階段作業 | 將本機連接埠對映至目標伺服器連接埠 |
|---|---|---|---|---|---|
| ftpstatic | `SSL_RSA_WITH_RC 4_128_MD5` | 空 | false | true | ■ 本機連接埠：30021<br>■ 目標主機：sesta<br>■ 目標連接埠：21 |

您可以爲靜態規則配置多個目標主機和連接埠。請參閱第 139 頁的「包含多個主機連線的靜態規則」以取得範例。

## 動態規則

在動態規則中，不會將目標主機指定爲規則的一部分。使用者可以在 Netlet 提供者中指定必要的目標主機。在下列範例中，TARGET 爲目標主機的萬用字元。

| 規則名稱 | 加密密碼 | 遠端應用程式 URL | 啓用下載 Applet | 啓用延伸階段作業 | 將本機連接埠對映至目標伺服器連接埠 |
|---|---|---|---|---|---|
| ftpdynamic | SSL_RSA_WIT H_RC4_128_MD5 | 空 | 選取核取方塊 | 選取核取方塊 | ■ 本機連接埠：30021<br>■ 目標主機：TARGET<br>■ 目標連接埠：21 |

## 加密密碼

根據加密密碼，可進一步將 Netlet 規則依如下分類：

- **使用者可配置的密碼規則** - 在此規則中，您可指定使用者可從中選擇的密碼清單。這些選擇性密碼會在 Netlet 提供者中以清單的形式出現。使用者可以從清單中選擇必要的密碼。在下列範例中，使用者可以從多個密碼中作出選擇。

| 規則名稱 | 加密密碼 | 遠端應用程式 URL | 啓用下載 Applet | 啓用延伸階段作業 | 將本機連接埠對映至目標伺服器連接埠 |
|---|---|---|---|---|---|
| Telnet | SSL_RSA_WITH_RC4 _128_SHA | 空 | 選取核取方塊 | 選取核取方塊 | ■ 本機連接埠：30000<br>■ 目標主機：TARGET<br>■ 目標連接埠：23 |
| | SSL_RSA_WITH_RC4 _128_MD5 | | | | |

**備註 –** 雖然 Portal Server 主機可能已經啓用不同的密碼，但是使用者僅能從配置爲 Netlet 規則部分的清單中選擇。

請參閱第 137 頁的「支援的密碼」以取得 Netlet 所支援的密碼的清單。

- **管理員配置的密碼規則** - 在此規則中，會將密碼定義爲 Netlet 規則的一部份。使用者無法選擇必要的密碼。在下列的範例中，已經將密碼配置爲 SSL_RSA_WITH_RC4_128_MD5。

| 規則名稱 | 加密密碼 | 遠端應用程式 URL | 啓用下載 Applet | 啓用延伸階段作業 | 將本機連接埠對映至目標伺服器連接埠 |
|---|---|---|---|---|---|
| Telnet | SSL_RSA_WITH_RC4_128_MD5 | 空 | 選取核取方塊 | 選取核取方塊 | ■ 本機連接埠：30000<br>■ 目標主機：TARGET<br>■ 目標連接埠：23 |

請參閱第 137 頁的 「支援的密碼」以取得 Netlet 支援的密碼的清單。

## 支援的密碼

第 137 頁的 「支援的密碼」列出 Netlet 支援的密碼。

**表 6–2** 支援的密碼清單

| 密碼 |
|---|
| **原生 VM 密碼** |
| KSSL_SSL3_RSA_WITH_3DES_EDE_CBC_SHA |
| KSSL_SSL3_RSA_WITH_RC4_128_MD5 |
| KSSL_SSL3_RSA_WITH_RC4_128_SHA |
| KSSL_SSL3_RSA_EXPORT_WITH_RC4_40_MD5 |
| KSSL_SSL3_RSA_WITH_DES_CBC_SHA |
| **Java Plugin 密碼** |
| SSL_RSA_WITH_3DES_EDE_CBC_SHA |
| SSL_RSA_WITH_RC4 _128_MD5 |
| SSL_RSA_WITH_RC4 _128_SHA |
| SSL_RSA_EXPORT_WITH_RC4_40_MD5 |
| SSL_RSA_WITH_DES_CBC_SHA |
| SSL_RSA_WITH_NULL_MD5 |
| TLS_RSA_WITH_AES_128_CBC_SHA |
| TLS_RSA_WITH_AES_256_CBC_SHA |

## 向下相容性

先前的 Portal Server 版本並不支援將密碼作爲 Netlet 規則的一部分。爲了向下相容不含密碼的現有規則，規則會使用預設的密碼。不含密碼的現有規則如下：

| 規則名稱 | 加密密碼 | 遠端應用程式 URL | 啓用下載 Applet | 啓用延伸階段作業 | 將本機連接埠對映至目標伺服器連接埠 |
|---|---|---|---|---|---|
| Telnet | | `telnet://localhost:30000` | 請勿選取核取方塊 | 選取核取方塊 | ■ 本機連接埠：30000<br>■ 目標主機：TARGET<br>■ 目標連接埠：23 |

將被解譯爲：

| 規則名稱 | 加密密碼 | 遠端應用程式 URL | 啓用下載 Applet | 啓用延伸階段作業 | 將本機連接埠對映至目標伺服器連接埠 |
|---|---|---|---|---|---|
| Telnet | 預設密碼 | `telnet://localhost:30000` | 請勿選取核取方塊 | 選取核取方塊 | ■ 本機連接埠：30000<br>■ 目標主機：TARGET<br>■ 目標連接埠：23 |

這類似於 [加密密碼] 欄位已選擇爲 [預設] 的 [管理員配置的規則]。

**備註 –** Netlet 規則無法包含任何大於 64000 的連接埠號碼。

# Netlet 規則範例

本節包括一些 Netlet 規則的範例，以說明 Netlet 的語法。


- 第 138 頁的 「基本靜態規則」
- 第 139 頁的 「包含多個主機連線的靜態規則」
- 第 141 頁的 「呼叫 URL 的動態規則」
- 第 142 頁的 「下載 Applet 的動態規則」


## 基本靜態規則

本規則支援從用戶端至機器 `sesta` 的 Telnet 連線。

| 規則名稱 | 加密密碼 | 遠端應用程式 URL | 下載 Applet | 延伸式階段作業 | 將本機連接埠對映至目標伺服器連接埠 |
|---|---|---|---|---|---|
| myrule | `SSL_RSA_WITH_RC4_128_MD5` | 空 | 請勿選取核取方塊 | true | ■ 本機連接埠：1111<br>■ 目標主機：sesta<br>■ 目標連接埠：23 |

其中

`myrule` 爲規則的名稱。

SSL_RSA_WITH_RC4_128_MD5 表示要使用的密碼。

null 表示此應用程式不是由 URL 所呼叫或透過桌面執行。

false 表示用戶端並不會下載 applet 以執行此應用程式。

true 表示當 Netlet 連線在使用中的情況下 Portal Server 不應逾時。

1111 爲用戶端上的連接埠，Netlet 會在此偵聽來自目標主機的連線請求。

sesta 是 Telnet 連線上收件者主機的名稱。

23 是目標主機上用於連線的連接埠號，在本例中即爲已知的 Telnet 連接埠。

桌面 Netlet 提供者並不會顯示連結，但是 Netlet 會自動啓動與偵聽指定的連接埠 (1111)。指示使用者啓動用戶端軟體 - 此情形中爲連接至 localhost 的 Telnet 階段作業。

例如，如果要啓動 Telnet 階段作業，用戶端需要在終端機 UNIX 指令行中鍵入下列字元：

```
telnet localhost 1111
```

## 包含多個主機連線的靜態規則

本規則支援從用戶端至兩台機器，即 sesta 和 siroe 的 Telnet 連線。

| 規則名稱 | 加密密碼 | 遠端應用程式 URL | 啓用下載 Applet | 啓用延伸階段作業 | 將本機連接埠對映至目標伺服器連接埠 |
|---|---|---|---|---|---|
| myrule | SSL_RSA_WITH_RC4_128_MD5 | 空 | 請選取核取方塊 | 選取核取方塊 | ■ 本機連接埠：1111–1234<br>■ 目標主機：sesta-siroe<br>■ 目標連接埠：23 |

其中

23 是目標主機上用於連線的連接埠號碼 – Telnet 的保留連接埠。

1111 爲用戶端上的連接埠，Netlet 會在此偵聽來自第一個目標主機 sesta 的連線請求。

1234 爲用戶端上的連接埠，Netlet 會在此偵聽來自第二個目標主機 siroe 的連線請求。

此規則中的前六個欄位與第 138 頁的 「基本靜態規則」中的相同。差別在於有三個欄位用於識別第二個目標主機。

當您新增其他目標至規則時，必須爲每個新目標主機新增三個欄位：local port、destination host 與 destination port。

**備註 –** 您可以有多組此三個欄位，以描述與每個目標主機的連線。如果遠端用戶端是以 UNIX 爲基礎，則不可以使用低於 2048 的偵聽連接埠號，原因是數字較低的連接埠將會受到限制，並且您必須是超級使用者才能夠啓動偵聽程式。

此規則的作用與先前的規則相同。Netlet 提供者並不顯示任何連結，但是 Netlet 會自動在指定的兩個連接埠 (1111 和 1234) 上啓動與偵聽。使用者必須啓動用戶端軟體 (在此案例中是連線至連接埠 1111 上的 `localhost`，或連接埠 1234 上的 `localhost` 的 Telnet 階段作業) 以連線至第二個範例中的主機。

## 選擇多個主機的靜態規則

使用此規則以指定多個替代主機。如果與規則中第一個主機的連線失敗，Netlet 會嘗試連接指定的第二個主機，以此類推。

| 規則名稱 | 加密密碼 | 遠端應用程式 URL | 啓用下載 Applet | 啓用延伸階段作業 | 將本機連接埠對映至目標伺服器連接埠 |
|---|---|---|---|---|---|
| gojoe | `SSL_RSA_WITH_RC4_128_MD5` | /gojoe.html | ■ 用戶端連接埠：8000<br>■ 伺服器主機：gojoe server<br>■ 伺服器連接埠：8080 | 選取核取方塊 | ■ 本機連接埠：10491<br>■ 目標主機：siroe+sesta<br>■ 目標連接埠：35+26+491-35+491 |

其中

`10491` 爲用戶端上的連接埠，Netlet 會在此偵聽來自目標主機的連線請求。

Netlet 會嘗試以相同順序連線至連接埠 `35`、`26` 和 `491` 上的 `siroe`，視何者可用而定。

如果無法建立與 `siroe` 的連線，Netlet 會嘗試以相同順序連線至連接埠 `35` 和 `491` 上的 `sesta`。

主機之間的加號 (+) 表示替代的主機。

連接埠號之間的加號 (+) 指出用於單一目標主機的替代連接埠。

連接埠號之間的減號 (-) 爲不同目標主機連接埠號的分隔符號。

**備註 –** 會按次序連線至鏈接中所提供的主機。例如，如果規則是 `siroe+ sesta`，則會先嘗試 `siroe`。如果連線失敗，則會嘗試連線至 `sesta`。如果規則中先列出的主機無法在使用中的網路實際使用，則連線至下一個可用主機的時間會隨著規則中的不可用主機數增加而增加。

## 呼叫 URL 的動態規則

此規則可以讓使用者配置必要的目標主機，讓使用者可以通過 Netlet 遠程登入不同主機。

| 規則名稱 | 加密密碼 | 遠端應用程式 URL | 啓用下載 Applet | 啓用延伸階段作業 | 將本機連接埠對映至目標伺服器連接埠 |
|---|---|---|---|---|---|
| myrule | `SSL_RSA_WITH_RC4_128_MD5` | telnet://localhost: 30000 | 請勿選取核取方塊 | 選取核取方塊 | ■ 本機連接埠：30000<br>■ 目標主機：TARGET<br>■ 目標連接埠：23 |

其中

`myrule` 爲規則的名稱。

SSL_RSA_WITH_RC4_128_MD5 表示要使用的密碼。

`telnet://localhost: 30000` 爲規則所呼叫的 URL。

`false` 表示將不會下載任何 applet。

`Extend Session(true)` 表示當 Netlet 連線在使用中的情況下 Portal Server 不應逾時。

`30000` 爲用戶端上的連接埠，Netlet 會在此偵聽此規則的連線需求。

`TARGET` 表示使用 Netlet 提供者的使用者需要配置的目標主機。

23 是 Netlet 開啓的目標主機上的連接埠，在本例中爲已知的 Telnet 連接埠。

## ▼ 在新增規則之後執行 Netlet

在新增規則之後，使用者必須完成某些步驟，使得 Netlet 能夠如預期般執行。使用者需要在用戶端執行下列動作：

1. **在標準 Portal Server 桌面的 Netlet 提供者區段中，按一下 [編輯]。**
   新的 Netlet 規則會列在 [新增新目標] 區段中的 [規則名稱] 底下。
2. **變更規則名稱，然後鍵入目標主機的名稱。**

3 **儲存變更**。
使用者會返回桌面，此時您可以在 Netlet 提供者區段中看見此新連結。

4 **按一下新連結**。
會啓動一個新的瀏覽器，並進至 Netlet 規則中所提供的 URL。

**備註 –** 透過重複上述步驟，您可以在相同的規則中新增一個以上的目標主機。只有最後選取的連結爲使用中。

## 下載 Applet 的動態規則

本規則定義從用戶端至動態配置的主機之間的連線。規則會從 applet 所在的伺服器上將 GO-Joe applet 下載至用戶端。

| 規則名稱 | 加密密碼 | 遠端應用程式 URL | 啓用下載 Applet | 延伸式階段作業 | 將本機連接埠對映至目標伺服器連接埠 |
|---|---|---|---|---|---|
| gojoe | SSL_RSA_WITH_RC4_128_MD5 | /gojoe.html | ■ 用戶端連接埠：8000<br>■ 伺服器主機：gojoe server<br>■ 伺服器連接埠：8080 | 選取核取方塊 | ■ 本機連接埠：3399<br>■ 目標主機：TARGET<br>■ 目標連接埠：58 |

其中

gojoe 是規則的名稱。

SSL_RSA_WITH_RC4_128_MD5 表示要使用的密碼。

例如 /gojoe.html 是包含 applet 的 HTML 頁面的路徑，路徑應與部署入口網站的 Web 容器文件根是相對的。

8000:server:8080 表示連接埠 8000 是用戶端上用來接收 applet 的目標連接埠，gojoeserve 是提供 applet 的伺服器名稱，而 8080 則是伺服器上的連接埠，applet 則從該處下載。

Extended Session(true) 表示當 Netlet 連線在使用中的情況下 Portal Server 不應逾時。

3399 爲用戶端上的連接埠，Netlet 會在此偵聽此類型的連線請求。

TARGET 表示使用 Netlet 提供者的使用者需要配置的目標主機。

58 爲 Netlet 所開啓的目標主機上的連接埠，在本例中爲 GoJoe 的連接埠。連接埠 58 爲目標主機偵聽其本身通訊的連接埠。Netlet 會將資訊從新的 applet 傳送至此連接埠。

# Netlet 規則範例

第 143 頁的 「Netlet 規則範例」列出某些共用應用程式的範例 Netlet 規則。

表格中有 7 欄，與 Netlet 規則的下列欄位相對應。規則名稱、URL、下載 Applet、本機連接埠、目標主機、目標連接埠。最後一欄包含規則的說明。

**備註 –** 第 143 頁的 「Netlet 規則範例」不會列出 Netlet 規則的 [密碼] 與 [延伸階段作業] 欄位。假設提供的範例中這兩個欄位是「SSL_RSA_WITH_RC4_128_MD5」和「true」。

**表 6–3** Netlet 規則範例

| 規則名稱 | 遠端應用程式 URL | 啓用下載 Applet | 將本機連接埠對映至目標伺服器連接埠 | 描述 |
|---|---|---|---|---|
| IMAP | 空 | 請勿選取核取方塊 | ■ 本機連接埠：10143<br>■ 目標主機：imapserver<br>■ 目標連接埠：143 | 用戶端中的 `Netlet local port` 不需要和伺服器端上的 `destination port` 相同。如果您使用任何標準 IMAP 和 SMTP 連接埠以外的連接埠，請確定已將用戶端配置爲可在不同於標準連接埠的連接埠上進行連接。<br>Solaris 用戶端使用者除非是以超級使用者的身份來執行，否則無法連接至低於 1024 的連接埠號。 |
| SMTP | 空 | 請勿選取核取方塊 | ■ 本機連接埠：10025<br>■ 目標主機：smtpserver<br>■ 目標連接埠：25 | |
| Lotus Web 用戶端 | 空 | 請勿選取核取方塊 | ■ 本機連接埠：80<br>■ 目標主機：lotus-server<br>■ 目標連接埠：80 | 本規則會告知 Netlet 偵聽連接埠 80 上的用戶端，並連接至 lotus 伺服器－連接埠 80 上的伺服器。Lotus Web Client 的一個需求是用戶端偵聽連接埠必須與伺服器連接埠相符。 |

表 6–3 Netlet 規則範例 *(續)*

| 規則名稱 | 遠端應用程式 URL | 啓用下載 Applet | 將本機連接埠對映至目標伺服器連接埠 | 描述 |
|---|---|---|---|---|
| Lotus Notes 非 Web 用戶端 | 空 | 請勿選取核取方塊 | ■ 本機連接埠：1352<br>■ 目標主機：lotus-domino<br>■ 目標連接埠：1352 | 利用此規則，Lotus Notes 用戶端可以透過 Netlet 連接至 Lotus Domino 伺服器。可確保當用戶端嘗試連接至伺服器時，它一定不會指向 `localhost` 作爲伺服器名稱。它必須指向 Lotus Domino 伺服器實際的伺服器名稱。伺服器名稱必須與伺服器的系統名稱相同。在使用 Netlet 時，用戶端必須將該名稱解析爲 `127.0.0.1`。實現這個動作的方法有兩種：<br>■ 將伺服器名稱設定爲指向用戶端主機表中的 `127.0.0.1`。<br>■ 將指向 `127.0.0.1` 的伺服器名稱的 DNS 項目匯出。<br>伺服器名稱必須和在設定期間用來配置 Domino 伺服器的伺服器名稱相同。 |

**表 6–3** Netlet 規則範例 *(續)*

| 規則名稱 | 遠端應用程式 URL | 啓用下載 Applet | 將本機連接埠對映至目標伺服器連接埠 | 描述 |
|---|---|---|---|---|
| Microsoft Outlook 與 Exchange Server<br><br>這個無法作用於 Windows NT、2000 與 XP。透過 Windows NT、2000 與 XP 的 Rewriter 使用 Outlook Web Access。 | 空 | 請勿選取核取方塊 | ■ 本機連接埠：135<br>■ 目標主機：exchange<br>■ 目標連接埠：135 | 此規則可告知 Netlet 偵聽用戶端上的連接埠 135，並連接至連接埠 135 上的伺服器 `exchange`。Outlook 用戶端會使用此連接埠與 Exchange 伺服器嘗試初始連絡，並決定與伺服器溝通所使用的後續連接埠。<br><br>在用戶端機器上：<br>■ 使用者必須將已經在 Outlook 用戶端中配置的 Exchange 伺服器的主機名稱變更爲 `localhost`。此選項的位置會因爲 Outlook 的版本而有所差異。<br>■ 使用者必須使用主機檔案將 Exchange 伺服器的主機名稱 (單一和完全合格) 映射至 IP 位址 `127.0.0.1`。<br>■ 在 Windows 95 或 98 中，檔案位於 `\\Windows\\Hosts`<br>■ 在 Windows NT4 中，檔案位於 `\\WinNT\\System32\\drivers\\etc\\Hosts`。<br>項目的外觀如下：<br>`127.0.0.1 exchange exchange.company.com`<br>Exchange 伺服器會將它自己的名稱傳回 Outlook 用戶端。此項映射可確保 Outlook 用戶端是使用 Netlet 用戶端連接回伺服器。 |
| FTP | 空 | 請勿選取核取方塊 | ■ 本機連接埠：30021<br>■ **目標主機**：*your-ftp_server.your-domain*<br>■ 目標連接埠：21 | 您可以使用受控制的一般使用者帳號提供 FTP 服務至單一的 FTP 伺服器。如此可確保遠端的 FTP 可從一般使用者系統安全傳輸至單一位置。如果沒有使用者名稱，FTP URL 會被解譯爲匿名的 FTP 連線。<br><br>您**必須**將連接埠 30021 定義爲您 Netlet FTP 規則的本機連接埠。<br><br>使用 Netlet 連線會支援動態 FTP。 |

表 6–3 Netlet 規則範例 *(續)*

| 規則名稱 | 遠端應用程式 URL | 啓用下載 Applet | 將本機連接埠對映至目標伺服器連接埠 | 描述 |
|---|---|---|---|---|
| Netscape 4.7 郵件用戶端 | 空 | 請勿選取核取方塊 | ■ 本機連接埠：30143、30025。<br>■ 目標主機：TARGET<br>■ 目標連接埠：10143 | 在 Netscape 用戶端中，使用者需要：<br>用於 IMAP 或內送郵件的 `localhost:30143`<br>用於 SMTP 或外送郵件的 `localhost:30025` |
| Graphon | third_party /xsession_start.html | 選取核取方塊 | ■ 本機連接埠：10491<br>■ 目標主機：TARGET<br>■ 目標連接埠：491 | 這是用於透過 Netlet 存取 Graphon 的規則。`xsession_start.html` 與 Graphon 連結。 |
| Citrix | third_party /citrix_start.html | 選取核取方塊 | ■ 本機連接埠：1494<br>■ 目標主機：TARGET<br>■ 目標連接埠：1494 | 這是用於透過 Netlet 存取 Citrix 的規則。`citrix_start.html` 與 Citrix 連結。 |
| RemoteControl | third_party /pca_start.html | 選取核取方塊 | ■ 本機連接埠：5631 5632<br>■ 目標主機：TARGET TARGET<br>■ 目標連接埠：5631 5632 | 這是用於透過 Netlet 存取「遠端控制」的規則。`pca_start.html` 與「遠端控制」連結。 |

# Netlet 記錄資訊

netlet applet 或 jws 的用戶端記錄會顯示於用戶端的 java 主控台上。

netlet 的伺服器記錄會顯示於 `/var/opt/SUNWportal/portals/<portal_ID>/logs/<INSTANCE_ID>` 目錄下的 `portal.0.0.log` 檔案中。

# 在 Sun Ray 環境中執行 Netlet

如果您希望執行的應用程式將 applet 下載至 Sun Ray 環境中的用戶端機器上，您需要變更 HTML 檔。以下是一個範例檔案，您可以透過該檔案瞭解必須執行的修改。

## 新的 HTML 檔

```
<!-- @(#)citrix_start.html 2.1
98/08/17 Copyright (c) 1998 i-Planet, Inc., All rights reserved.-->
<html>
```

```
<script language="JavaScript">
var KEY_VALUES;  // KEY_VALUES[\qkey\q] = \qvalue\q;
function retrieveKeyValues() {
      KEY_VALUES = new Object();
      var queryString  = \q\q + this.location;
      queryString = unescape(queryString);
      queryString = queryString.substring((queryString.indexOf(\q?\q)) + 1);
      if (queryString.length < 1) {
          return false; }
      var keypairs = new Object();
      var numKP = 0;
      while (queryString.indexOf(\q&\q) > -1) {
        keypairs[numKP] = queryString.substring(0,queryString.indexOf(\q&\q));
        queryString = queryString.substring((queryString.indexOf(\q&\q)) + 1);
        numKP++;
      }
      // Store what\qs left in the query string as the final keypairs[] data.
      keypairs[numKP++] = queryString;
      var keyName;
      var keyValue;
      for (var i=0; i < numKP; ++i) {
        keyName = keypairs[i].substring(0,keypairs[i].indexOf(\q=\q));
        keyValue = keypairs[i].substring((keypairs[i].indexOf(\q=\q)) + 1);
        while (keyValue.indexOf(\q+\q) > -1) {
          keyValue = keyValue.substring(0,keyValue.indexOf(\q+\q)) + \q \q
           + keyValue.substring(keyValue.indexOf(\q+\q) + 1);

        }
        keyValue = unescape(keyValue);
          // Unescape non-alphanumerics
        KEY_VALUES[keyName] = keyValue;
      }
}
function getClientPort(serverPort) {
    var keyName = "clientPort[\q" + serverPort +"\q]";
    return KEY_VALUES[keyName];
}
function generateContent() {
    retrieveKeyValues();
    var newContent =
        "<html>\\n"
          + "<head></head>\\n"
          + "<body>\\n"
          + "<applet code=\\"com.citrix.JICA.class\\" archive=\\
               "JICAEngN.jar\\" width=800 height=600>\\n"
          + "<param name=\\"cabbase\\" value=\\"JICAEngM.cab\\">\\n"
          + "<param name=\\"address\\" value=\\"localhost\\">\\n"
          + "<param name=ICAPortNumber value="
```

```
          + getClientPort(\q1494\q)
          + ">\\n"
          + "</applet>\\n"
          + "</body>\\n"
          + "</html>\\n";
    document.write(newContent);
}
</script>
<body onLoad="generateContent();">
</body>
</html>
```

# 停用的 HTML 檔

```
<html>
<body>
<applet code="com.citrix.JICA.class" archive=
   "JICAEngN.jar" width=800 height=600>
<param name="cabbase" value="JICAEngM.cab">
<param name="address" value="localhost">
<param name=ICAPortNumber value=1494>
</applet>
</body></html>
```

第 2 部分

# 配置 Secure Remote Access 伺服器

可使用 Portal Server 管理主控台 [Secure Remote Access] 標籤下可用的選項，來設定大部分屬性。任何新建立的組織或使用者會依預設繼承這些值。

您可以在組織層級、角色層級與使用者層級中，配置與 Secure Remote Access 相關的屬性，以下情況除外：

- 無法在使用者層級設定 [衝突解決層級]。請參閱第 29 頁的「設定衝突解決」。
- [MIME 類型配置檔案位置] 屬性只可以在組織層級中設定。

在組織層級設定的值，會由其下所有的角色與使用者繼承。在使用者層級設定的值會覆寫在組織或角色層級設定的值。

您可以在「服務配置」層級變更屬性值。這些新值僅會在新增新組織時有所體現。

本部分包含下列章節：


- 第 7 章
- 第 8 章
- 第 9 章
- 第 10 章
- 第 11 章
- 第 12 章
- 第 13 章
- 第 14 章
- 第 15 章

◆ ◆ ◆ 第 7 章

# 7 配置 Secure Remote Access 伺服器存取控制

本章說明如何透過 Sun Java System Portal Server 管理主控台允許或拒絕使用者存取。

## 配置存取控制

您可使用此欄位指定一般使用者無法透過閘道存取的 URL 清單。閘道會在檢查「允許的 URL」清單之前檢查「遭拒的 URL」清單。

您可以指定可由一般使用者透過閘道存取的所有 URL。依預設，此清單有萬用字元項目 (*)，表示可以存取所有 URL。若您希望允許存取所有 URL，而僅對特定 URL 限制存取，請將限制的 URL 新增至「遭拒的 URL」清單中。如果您希望僅允許存取特定 URL，請將「遭拒的 URL」清單保留空白，並在「允許的 URL」清單中指定需要的 URL，方法與上述相同。

SRA 軟體中的 [存取控制] 服務允許您控制多個主機的單次登入功能。爲使得單次登入功能可用，[啓用 HTTP 基本驗證] 選項必須於閘道服務中啓用。

使用 [存取控制] 服務，您可以停用某些主機的單次登入功能。這表示一般使用者每次連接至需要 HTTP 基本認證的主機時，都會需要認證，除非您啓用 [每個階段作業中的單次登入] 功能。

如果已停用了某個主機的單次登入功能，使用者則可以在單一 Portal Server 階段作業內重新連接至該主機。例如，假設您已停用對 `abc.sesta.com` 的單次登入。使用者第一次連接至該網站時，需要認證。使用者可以瀏覽其他網頁並在稍後返回此網頁，如果該網頁是處在相同的 Portal Server 階段作業中，則不需要認證。

## ▼ 配置存取控制

1. **以管理員身份登入 Portal Server 管理主控台。**
2. **選取 [Secure Remote Access] 標籤。**
3. **選取 [存取控制] 標籤。**
4. **修改下列屬性：**

| 屬性名稱 | 描述 |
| --- | --- |
| COS 優先順序 | 指定要用來決定屬性值繼承的值。如需有關此屬性的詳細資訊，請參閱「Sun Java System Directory Server 管理指南」。 |
| 每個階段作業中的單次登入 | 選取 [啓用] 核取方塊來啓用單次登入階段作業。 |
| 停用單次登入的主機 | 以 `abc.siroe.com` 的格式輸入主機名稱。 |
| 允許的認證層級 | 輸入允許的認證層級。使用星號以允許所有的層級。預設值是星號。 |
| 允許/拒絕存取 URL | 在 URL 欄位內輸入允許或拒絕透過閘道存取的 URL。輸入的 URL 格式爲：`http://abc.siroe.com`。請在 [動作] 下拉式清單中，按一下適當的 [允許] 或 [拒絕] 選項。<br>您也可以使用常規表示式，如 `http://*.siroe.com`。在這個情況下，會拒絕使用者存取 `siroe.com` 網域中的所有主機。<br>閘道會在檢查允許的 URL 清單之前先檢查拒絕存取的 URL。<br>**備註 –** [允許的 URL] 欄位預設中有 `*`，表示可以透過閘道存取所有的 URL。 |

**備註 –** 當您安裝 SRA 時，依預設並非所有使用者都可使用 [存取控制] 服務。僅有在安裝時依預設建立的 `amadmin` 使用者才可使用此服務。其他使用者在沒有此服務的情況下，無法透過閘道存取桌面。以 `amadmin` 的身份登入，並指定此服務給所有的使用者。

5. **按一下 [儲存] 完成作業。**

◆ ◆ ◆ 第 8 章

# 配置 Secure Remote Access 閘道

本章說明如何透過 Sun Java System Portal Server 管理主控台配置閘道屬性。

本章包含下列章節：


- 第 153 頁的「配置設定檔核心選項」
- 第 158 頁的「配置部署選項」
- 第 161 頁的「配置安全性選項」
- 第 163 頁的「配置效能選項」
- 第 165 頁的「配置 Rewriter 選項」
- 第 167 頁的「配置剖析器與 MIME 類型的對映」
- 第 166 頁的「配置 URI 與規則集的對映」
- 第 168 頁的「配置個人數位憑證認證」
- 第 172 頁的「使用指令行選項配置閘道屬性」


在您開始前

- 要建立閘道設定檔，請參閱第 32 頁的「建立閘道設定檔」

## 配置設定檔核心選項

本節說明下列作業：


- 第 153 頁的「配置啓動模式」
- 第 155 頁的「配置核心元件」


### 配置啓動模式

若您在安裝期間選擇以 HTTPS 模式執行閘道，則在安裝後閘道會以 HTTPS 模式執行。在 HTTPS 模式中，閘道會接受來自瀏覽器的 SSL 連線並拒絕非 SSL 連線。然而，您也可以配置以 HTTP 模式執行閘道。如此將可加速閘道的效能，因爲它與管理 SSL 階段作業、加密與解密 SSL 通訊流量的耗用時間並無關。

## ▼ 配置啓動模式

1. **以管理員身份登入 Portal Server 管理主控台。**
2. **選取 [Secure Remote Access] 標籤，並按一下設定檔名稱以修改其屬性。**
3. **選取 [核心] 標籤。**
4. **修改下列屬性：**

| | |
|---|---|
| HTTP 連線 | 選取 [HTTP 連線] 核取方塊，以允許閘道接受非 SSL 的連線。 |
| HTTP 連接埠 | 輸入 HTTP 連接埠號碼。預設值爲 80。 |
| HTTPS 連線 | 選取 [HTTPS 連線] 核取方塊，以允許閘道接受 SSL 連線。根據預設，會選取此選項。 |
| HTTPS 連接埠 | 輸入 HTTPS 連接埠號碼。預設值爲 443。 |

**備註 –** 可使用「Sun Java System Portal Server 7.2 Command-Line Reference」中的「psadmin set-attribute」 來修改下列屬性

*/space/PS/portal/bin/*`psadmin set-attribute -u amadmin -f` */space/PS/portal/bin/ps_password -p portal1* `-m gateway --gateway-profile` *profileID* `-a` *sunPortalGatewayDomainsAndRulesets -A $entry*

- sunPortalGatewayDefaultDomainAndSubdomains=Default Domains
- sunPortalGatewayLoggingEnabled=Enable Logging
- sunPortalGatewayEProxyPerSessionLogging=Enable per Session Logging
- sunPortalGatewayEProxyDetailedPerSessionLogging=Enable Detailed per Session Logging
- sunPortalGatewayNetletLoggingEnabled=Enable Netlet Logging
- sunPortalGatewayEnableMIMEGuessing=Enable MIME Guessing
- sunPortalGatewayParserToURIMap=Parser to URI Mappings
- sunPortalGatewayEnableObfuscation=Enable Masking
- sunPortalGatewayObfuscationSecretKey=Seed String for Masking
- sunPortalGatewayNotToObscureURIList=URIs not to Mask
- sunPortalGatewayUseConsistentProtocolForGateway=Make Gateway protocol Same as Original URI Protocol
- sunPortalGatewayEnableCookieManager=Store External Server Cookies
- sunPortalGatewayMarkCookiesSecure=Mark Cookies as secure

5 **從終端機視窗重新啓動閘道：**

```
./psadmin start-sra-instance -u amadmin -f passwordfile -N profilename -t gateway
```

# 配置核心元件

Netlet 會讓使用者在不安全的網路上 (如網際網路) 安全執行共用 TCP/IP 服務。您可執行 TCP/IP 應用程式 (如 Telnet 和 SMTP)、HTTP 應用程式以及任何使用固定連接埠的應用程式。若已啓用 Netlet，閘道需要確定外來的通訊是 Portal Server 通訊還是 Netlet 通訊。停用 Netlet 則會減少這種耗用時間，因爲閘道會假設所有外來的通訊是 HTTP 或 HTTPS 通訊。只有在確定不希望透過 Portal Server 使用任何應用程式時，才停用 Netlet。

## ▼ 配置元件

1 **以管理員身份登入 Portal Server 管理主控台。**

2 **選取 [Secure Remote Access] 標籤，並按一下設定檔名稱以修改其屬性。**

3 **選取 [核心] 標籤。**

4 **修改下列屬性：**

| 屬性名稱 | 描述 |
|---|---|
| Netlet | 選取 [啓用] 核取方塊以啓動 Netlet 服務。根據預設，會選取此選項。 |
| Proxylet | 選取 [啓用] 核取方塊以啓動 Proxylet 服務。根據預設，會選取此選項。 |

5 **使用下列指令選項，從終端機視窗重新啓動閘道：**

```
./psadmin start-sra-instance -u amadmin -f passwordfile -N profilename -t gateway
```

# 配置基本選項

## 關於 Cookie 管理屬性

許多網頁使用 Cookie 追蹤與管理使用者階段作業。閘道路由請求至在 HTTP 標題設定 Cookie 的網站時，閘道會以下列方法捨棄或傳遞那些 Cookie：

- 若未在閘道服務中選取 [啓用 Cookie 管理] 屬性，則不會重新寫入 Cookie。如此，瀏覽器中的 Cookie 可能不會到達企業內部網路主機，反之亦然。

- 若在閘道服務中選取 [啓用 Cookie 管理] 屬性，則會重新寫入 Cookie。閘道會確保瀏覽器的 Cookie 會到達想要的企業內部網路主機，反之亦然。

此設定不會套用至 Portal Server 用來追蹤 Portal Server 使用者階段作業的 Cookie。此設定由 [轉寄使用者階段作業 Cookie 到的使用者階段作業] 的 URL 選項配置所控制。

這個設定適用於所有允許使用者存取的網站 (也就是，您不可以選擇捨棄某些網站的 Cookie，而保留其他網站的 Cookie)。

---

**備註 –** 請勿將 URL 從 [Cookie 網域] 清單中移除，即使是在沒有 Cookie 的閘道中。有關 [Cookie 網域] 清單的資訊，請參閱「Access Manager 管理指南」。

---

## 關於 HTTP 基本認證屬性

HTTP 基本驗證可以設定於閘道服務中。

可以使用 HTTP 基本驗證保護網頁，造訪者需要在檢視網站前輸入使用者名稱與密碼 (HTTP 回應代碼爲 401 與 WWW-authenticate: BASIC)。Portal Server 可儲存使用者名稱及密碼，以便使用者在重新造訪受 BASIC 保護的網站時，不必重新輸入他們的憑證。這些憑證儲存於目錄伺服器的使用者設定檔中。

此設定不會確定使用者是否可造訪 BASIC 保護的網站，但只會確定是否將使用者輸入的憑證儲存於使用者設定檔。

這個設定適用於所有允許使用者存取的網站 (也就是，不可以某些網站啓用 HTTP 基本授權快取而其他網站停用)。

---

**備註 –** 如果 Microsoft Internet Information Server (IIS) 由 Windows NT 挑戰/回應 (HTTP 回應代碼 401，WWW-Authenticate: NTLM) 而非基本驗證進行保護，不支援瀏覽其提供的 URL。

---

您也可以使用管理主控台中的 [存取控制] 服務啓用單次登入。

## 關於 Portal Server 屬性

你可以爲閘道配置多個 Portal Server 以服務請求。安裝閘道時，您應該已經指定與閘道合作的 Portal Server。依預設，這個 Portal Server 會列示在 Portal Server 欄位中。您可以將更多 Portal Server 以 `http://`*portal- server-name:port number* 格式新增至清單中。閘道會以循環方式嘗試連絡每個列出的 Portal Server 以服務請求。

## 關於 [將使用者階段作業 Cookie 轉寄至的 URL] 屬性

Portal Server 利用 Cookie 追蹤使用者階段作業。當閘道發出 HTTP 請求至伺服器時 (例如，當呼叫桌面 servlet 以產生使用者桌面頁面時)，將轉寄此 cookie 至伺服器。伺服器上的應用程式會使用 cookie 以認證並識別使用者。

Portal Server 的 cookie 不會轉寄至發給伺服器之外其他機器的 HTTP 請求中，除非那些機器上的 URL 已指定於 [將使用者階段作業 Cookie 轉寄至的 URL ] 清單中。因此將 URL 新增至此清單，可使 servlet 與 CGI 能夠接收 Portal Server 的 cookie 並使用 API 識別此使用者。

使用隱式尾隨萬用字元可與 URL 相符。例如，清單中的預設輸入值：

```
http://server:8080
```

將導致 Cookie 轉寄至所有以 `http://server:8080` 開頭的 URL。

新增：

```
http://newmachine.eng.siroe.com/subdir
```

將導致 Cookie 轉寄至所有以該實際字串開始的 URL。

在此例中，Cookie 不會轉寄至任何以 "`http://newmachine.eng/subdir`" 開始的 URL，因爲這個字串不是以轉寄清單中的實際字串開頭。要使 Cookie 轉寄至以這個機器名稱變體開始的 URL，必須新增項目至轉寄清單。

同樣的，Cookie 也不會轉寄至以 "`https://newmachine.eng.siroe.com/subdir`" 開始的 URL，除非已將適當的項目新增至清單中。

### 關於 [從 URL 取得階段作業] 屬性

選取 [從 URL 取得階段作業] 選項時，階段作業資訊會編碼爲 URL 的部分，不論支援 Cookie 與否。這表示閘道會驗證在 URL 中找到的階段作業資訊，而非從用戶端瀏覽器傳送的階段作業 Cookie。

## ▼ 配置基本選項

1. **以管理員身份登入 Portal Server 管理主控台。**
2. **選取 [Secure Remote Access] 標籤，並按一下設定檔名稱以修改其屬性。**
3. **選取 [核心] 標籤。**
4. **修改下列屬性：**

| 屬性名稱 | 描述 |
| --- | --- |
| Cookie 管理 | 選取 [啓用] 核取方塊以啓用 Cookie 管理。<br>根據預設，會選取此選項。 |

| 屬性名稱 | 描述 |
| --- | --- |
| HTTP 基本認證 | 選取 [啓用 HTTP 基本驗證] 核取方塊以啓用 HTTP 基本驗證。 |
| Portal Server | 在欄位以 `http://portal-server-name:port-number` 格式輸入 Portal Server，並按一下 [新增]。<br>重複此步驟可新增更多 Portal Server 至 Portal Server 清單。 |
| 將使用者階段作業 Cookie 轉寄至的 URL | 輸入 [將使用者階段作業 Cookie 轉寄至的 URL] 並按一下 [新增]。<br>重複此步驟以新增更多 URL 至 [將使用者階段作業 Cookie 轉寄至的 URL] 清單。 |
| 閘道最低認證層級 | 輸入認證層級。<br>根據預設，會新增星號以允許各種層級的認證。 |
| 從 URL 取得階段作業 | 選取 [是] 可以從 URL 擷取有關階段作業的資訊。<br>根據預設，會選取 [否] 選項。 |

# 配置部署選項

## 配置代理伺服器設定

### ▼ 配置代理伺服器設定

1. **以管理員身份登入 Portal Server 管理主控台。**
2. **選取 [Secure Remote Access] 標籤，並按一下設定檔名稱以修改其屬性。**
3. **選取 [部署] 標籤。**
4. **修改下列屬性：**

| 屬性名稱 | 描述 |
| --- | --- |
| 使用代理伺服器 | 選取 [使用代理伺服器] 核取方塊來啓用 Web 代理伺服器。 |

| 屬性名稱 | 描述 | |
|---|---|---|
| Web 代理伺服器 URL | 在 [使用 Web 代理伺服器 URL] 編輯方塊中，以 `http://host name.subdomain.com` 格式輸入需要的 URL，然後按一下 [新增]。<br>URL 會新增至 [使用Web 代理伺服器 URL] 清單。 | 您可以指定閘道僅能透過列於 [網域與子網域的代理伺服器清單] 中的 Web 代理伺服器連絡特定 URL，即使已停用 [使用代理伺服器] 選項。您需要在 [使用網路代理伺服器 URL] 欄位中指定這些 URL。有關此值如何影響代理伺服器使用情形的詳細資訊，請參閱第 33 頁的「指定代理伺服器以連絡 Access Manager」。 |
| 網域與子網域的代理伺服器 | 此項目已新增至 [網域與子網域的代理伺服器] 清單方塊中。<br>輸入代理伺服器資訊的格式如下：<br>`domainname proxy1:port1\|subdomain1 proxy2:port2\|subdomain2 proxy3:port3\|* proxy4:port4`<br>* 表示 * 之後定義的代理伺服器會用於所有網域與子網域 (如果沒有特別說明)。<br>若您沒有指定代理伺服器連接埠，將依預設使用連接埠 8080。 | 有關如何將代理伺服器資訊套用至不同主機的詳細資訊，請參閱第 33 頁的「指定代理伺服器以連絡 Access Manager」。 |
| 代理伺服器密碼清單 | 在 [代理伺服器密碼清單] 欄位中，輸入每個代理伺服器的資訊，然後按一下 [新增]。<br>輸入代理伺服器資訊的格式如下：<br>`proxyserver\|username\|password`<br>`proxyserver` 對應至定義於 [網域與子網域代理伺服器清單] 的代理伺服器。 | 當代理伺服器需要認證以存取部分或所有網站時，您需要指定需要的使用者名稱及密碼，以便閘道驗證至指定的代理伺服器。 |
| 自動代理伺服器配置支援 | 選取 [啓用自動代理伺服器配置支援] 核取方塊以啓用 PAC 支援。 | 若您選取 [啓用自動代理伺服器配置支援] 選項，則會忽略在 [網域與子網域代理伺服器] 欄位中提供的資訊。閘道將「自動代理伺服器配置 (PAC)」檔案只用於企業內部網路配置。有關 PAC 檔案的資訊，請參閱第 45 頁的「使用自動代理伺服器配置」。 |
| 自動代理伺服器配置檔案位置 | 在 [位置] 欄位中，輸入 PAC 檔案的名稱與位置。 | |

# 配置 Rewriter 代理伺服器與 Netlet 代理伺服器

## 關於 NetLet 代理伺服器

藉由延伸用戶端透過閘道到存在於企業內部網路的 Netlet 代理伺服器的安全通道，Netlet 代理伺服器會強化閘道和企業內部網路之間 Netlet 通訊流量的安全性。若已啓用 Netlet 代理伺服器，則 Netlet 封包會由代理 Netlet 代理伺服器解密，之後會傳送至目標伺服器。這將減少需要在防火牆中開啓的連接埠數目。

### 關於 Rewriter 代理伺服器

Rewriter 代理伺服器可啓用閘道與企業內部網路之間的安全 HTTP 通訊。如果您沒有指定 Rewriter 代理伺服器，當使用者嘗試存取企業內部網路的機器，閘道元件會直接連線至企業內部網路。在安裝之後不會自動執行 Rewriter 代理伺服器。您必須依下列所述啓用 Rewriter 代理伺服器。

## ▼ 配置 Rewriter 代理伺服器與 Netlet 代理伺服器

1. **以管理員身份登入 Portal Server 管理主控台。**
2. **選取 [Secure Remote Access] 標籤，並按一下設定檔名稱以修改其屬性。**

   **備註 –** 請確定 Rewriter 代理伺服器與閘道使用相同的閘道設定檔。

3. **選取 [部署] 標籤。**
4. **修改下列屬性：**

| 屬性名稱 | 描述 |
| --- | --- |
| Rewriter 代理伺服器 | 選取 [Rewriter 代理伺服器] 核取方塊，以啓用 Rewriter 代理伺服器服務。 |
| Rewriter 代理伺服器清單 | a. 在 [Rewriter 代理伺服器] 編輯方塊中以 `hostname:port` 格式輸入主機與連接埠。<br>**提示 –** 要確定想要的連接埠是否可用或未使用，請在指令行中輸入：<br>**`netstat -a \| grep`** *port-number* **`\| wc -l`**<br>*port-number* 是想要使用的連接埠。<br>b. 按一下 [新增]。 |
| Netlet 代理伺服器 | 選取 [啓用 Netlet 代理伺服器] 核取方塊以啓用 Netlet 代理伺服器服務。 |

| 屬性名稱 | 描述 |
| --- | --- |
| Netlet 代理伺服器主機 | a. 在 [Netlet 代理伺服器主機] 欄位中以 `hostname:port` 格式輸入 Netlet 代理伺服器主機與連接埠。<br>**提示 –** 要確定想要的連接埠是否可用或未使用，請在指令行中輸入：<br>**`netstat -a \| grep`** *port-number* **`\| wc -l`**<br>*port-number* 是想要使用的連接埠。<br>b. 按一下 [新增]。 |
| 透過 Web 代理伺服器的 Netlet 通道 | 選取 [透過 Web 代理伺服器啓用 Netlet 通道] 核取方塊來啓用通道。 |

5 **在伺服器上執行** *portal-server-install-root*`/SUNWportal/bin/certadmin` **以建立 Rewriter 代理伺服器的認證。**

若您在安裝 Rewriter 代理伺服器時未選擇建立認證，則必須執行這個步驟。

6 **以超級使用者身份登入安裝 Rewriter 代理伺服器的機器並啓動 Rewriter 代理伺服器：**

*rewriter-proxy-install-root*`/SUNWportal/bin/rwproxyd -n` *gateway-profile-name* `start`

7 **以超級使用者身份登入安裝閘道的機器並重新啓動閘道：**

`./psadmin start-sra-instance -u amadmin -f` *passwordfile* `-N` *profilename* `-t gateway`

# 配置安全性選項

## 配置 PDC 與非認證 URL

### ▼ 配置 PDC 與非認證 URL

1 **以管理員身份登入 Portal Server 管理主控台。**

2 **選取 [Secure Remote Access] 標籤，並按一下設定檔名稱以修改其屬性。**

3 **選取 [安全性] 標籤。**

4 **修改下列屬性：**

| 屬性名稱 | 描述 |
| --- | --- |
| 啓用憑證的閘道主機 | a. 新增閘道名稱至啓用憑證的閘道主機清單。<br>以 `host1.sesta.com` 格式新增閘道。<br>b. 按一下 [新增]。 |
| 未認證的 URL | 您可以指定某些 URL 不需要認證。這些一般是包括影像的目錄。<br>在 [未驗證的 URL] 欄位中以 `folder/subfolder` 格式輸入想要的資料夾路徑。<br>鍵入的非完全合格的 URL (例如，/images) 會視爲入口網站 URL。<br>要新增非入口網站的 URL，請完全限定 URL，並按一下 [新增] 以將此項目新增至 [未驗證的 URL] 清單。 |
| 可信任的 SSL 網域 | 在 [可信任的 SSL 網域] 欄位中，輸入網域名稱並按一下 [新增]。 |

# 配置 TLS 與 SSL 選項

## ▼ 配置 TLS 與 SSL 選項

1. **以管理員身份登入 Portal Server 管理主控台。**
2. **選取 [Secure Remote Access] 標籤，並按一下設定檔名稱以修改其屬性。**
3. **選取 [安全性] 標籤。**
4. **修改下列屬性：**

| 屬性名稱 | 描述 |
| --- | --- |
| 40 位元加密 | 若想要允許 40 位元 (弱) 安全套接層 (SSL) 連線，則選取這個選項。如果您沒有選取這個選項，則只支援 128 位元的連線。<br>若您停用這個選項，則使用者必須確定瀏覽器的配置支援必要的連線類型。<br>**備註 –** 若爲 Netscape Navigator 4.7x 使用者必須執行下列作業：<br>a. 在 Communicator 功能表中 [工具] 之下選取 [安全資訊]。<br>b. 在左窗格中按一下 [助手] 連結。<br>c. 在 [進階安全性 (SSL) 配置] 之下按一下 [配置 SSL v2] 或 [配置 SSL v3]。<br>d. 啓用必要的密碼。 |
| 不加密 | 選取 [啓用空加密] 核取方塊以啓用空加密。 |

| 屬性名稱 | 描述 |
| --- | --- |
| SSL 加密選項 | Secure Remote Access 支援許多標準加密法。您可以選擇支援所有預先封裝的密碼，或單獨選擇想要的密碼。您可以爲每個閘道實例選擇特定的 SSL 密碼。若用戶端網站存在任何已選取的密碼，則會成功進入 SSL 訊號交換模式。 |
| SSL 2.0 版 | 選取 [啓用 SSL 2.0 版] 核取方塊，以啓用 2.0 版。預設會啓用此選項。<br>您可以啓用或停用 SSL 2.0 版。停用 SSL 2.0 表示只支援舊版 SSL 2.0 的瀏覽器將不能認證至 Secure Remote Access。這可確保較大的安全層級。 |
| SSL2 加密 | 選取 [啓用 SSL 加密選項] 核取方塊選項。<br>您可從 SSL 加密法清單，選取想要的加密法。 |
| SSL 3.0 版 | 您可以啓用或停用 SSL 3.0 版。停用 SSL 3.0 表示只支援 SSL 3.0 的瀏覽器將不能認證至 SRA 軟體。這可確保較大的安全層級。<br>選取 [啓用 SSL 3.0 版] 核取方塊以啓用 3.0 版。 |
| SSL3 加密 | 選取 [啓用 SSL 加密選項] 核取方塊選項。<br>您從 SSL3 加密法清單選取想要的加密法。 |
| TLS 加密 | 選取 [啓用 SSL 加密選項] 核取方塊選項。<br>您可從 TLS 加密法清單選取想要的加密法。 |

# 配置效能選項

## 配置逾時與重試

### ▼ 配置逾時與重試

1. **以管理員身份登入 Portal Server 管理主控台。**
2. **選取 [Secure Remote Access] 標籤，並按一下設定檔名稱以修改其屬性。**
3. **選取 [效能] 標籤。**
4. **修改下列屬性：**

| 屬性名稱 | 描述 |
| --- | --- |
| 伺服器重試間隔 (秒) | 指定若 Portal Server、Rewriter 代理伺服器或 Netlet 代理伺服器變得無法存取 (例如當機或關機) 時，嘗試啓動它們之請求的時間間隔 (單位爲秒)。 |
| 閘道逾時 (秒) | 指定閘道與瀏覽器的連線逾時時間，以秒爲單位。<br>在 [閘道逾時] 欄位中，以秒爲單位指定想要的間隔。 |
| 快取的通訊端逾時 (秒) | 指定閘道與入口網站伺服器的連線逾時時間，以秒爲單位。 |

# 配置 HTTP 選項

## ▼ 配置 HTTP 選項

1. **以管理員身份登入 Portal Server 管理主控台。**
2. **選取 [Secure Remote Access] 標籤，並按一下設定檔名稱以修改其屬性。**
3. **選取 [效能] 標籤。**
4. **修改下列屬性：**

| 屬性名稱 | 描述 |
| --- | --- |
| 最大執行緒儲存區大小 | 指定想要的執行緒數。<br>您可指定可於閘道執行緒池內預先建立的執行緒的最大數。 |
| 持續 HTTP 連線 | 選取 [啓用持續 HTTP 連線] 核取方塊以啓用 HTTP 連線。<br>您可以在閘道啓用 HTTP 永久性連線，以避免爲網頁中的每個物件 (例如影像與樣式表) 都開啓通訊端。 |
| 每一持續連線的最大請求數 | 輸入最大請求數。 |
| 持續通訊端連線的逾時 (秒) | 輸入想要的逾時時間，以秒爲單位。 |
| 帳號往返時間的寬限逾時 (秒) | 輸入想要的寬限逾時時間，以秒爲單位。<br>這是用戶端 (瀏覽器) 與閘道之間的網路通訊往返時間。<br>■ 請求自瀏覽器送出後，到達閘道所花費的時間<br>■ 從閘道傳送回應到瀏覽器實際收到回應之間的時間<br>這依賴於多個因素，例如網路情況和用戶端的連線速度。 |
| 最長連線佇列長度 | 指定閘道應接受的最大同步運作連線數。<br>指定想要的連線數。 |

## 監視 Secure Remote Access 效能

監視可讓管理員評估 Secure Remote Access 不同元件的效能。

### ▼ 監視 Secure Remote Access 效能

1. 登入 Portal Server 管理主控台。
2. 選取 [Secure Remote Access] 標籤，並按一下子功能表中的 [監視]。
3. 在 [監視] 頁面上，從下拉式功能表選取代理伺服器實例。
4. 選取 [MBeans] 表格中的屬性，以檢視效能值。

# 配置 Rewriter 選項

## 配置基本選項

### ▼ 配置基本選項

1. 以管理員身份登入 Portal Server 管理主控台。
2. 選取 [Secure Remote Access] 標籤，並按一下設定檔名稱以修改其屬性。
3. 選取 [Rewriter] 標籤。
4. 修改下列屬性：

| 屬性名稱 | 描述 |
| --- | --- |
| 重寫所有 URI | 選取 [啓用所有 URI 的重寫] 核取方塊，以使閘道重寫所有 URI。<br>若您啓用閘道服務中 [啓用所有 URI 的重寫] 選項，則 Rewriter 會重寫所有 URI 而不會將其於 [網域與子網域代理伺服器清單] 中的項目進行核對。忽略網域與子網域清單的代理伺服器項目。 |
| 不要重寫的 URI | 在編輯方塊中新增 URI。<br>**備註 –** 將 #* 新增至這份清單可允許重寫 URI，即使 href 規則是規則集的一部分也一樣。 |

# 配置 URI 與規則集的對映

規則集會建立於 Portal Server 管理主控台中 [Portal Server 配置] 之下的 Rewriter 服務中。請參閱「Portal Server 管理指南」以取得詳細資訊。

建立規則集之後，您可以使用 [對映 URI 至規則集] 欄位將網域與規則集進行關聯。下列兩個項目會依預設新增至 [對映 URI 至規則集] 欄位：

- *://*.Sun.COM/portal/*|default_gateway_ruleset

  其中 sun.com 是安裝入口網站的網域，而 /portal 是入口網站的安裝環境
- *|generic_ruleset

這表示對於預設網域的所有頁面，將套用預設閘道規則集。對於其他頁面，則套用常規規則集。預設閘道規則集與常規規則集爲預先封裝的規則集。

---

**備註 –** 對於所有顯示於桌面的內容，將使用預設網域的規則集，無論內容來自何處。

例如，假設桌面被配置爲從 URL `yahoo.com` 取得內容。Portal Server 位於 `sesta.com`。將套用 `sesta.com` 規則集至取得的內容。

---

---

**備註 –** 您爲其指定規則集的網域必須列於網域與子網域的代理伺服器清單中。

---

## ▼ 配置 URI 與規則集的對映

1. **以管理員身份登入 Portal Server 管理主控台。**
2. **選取 [Secure Remote Access] 標籤，並按一下設定檔名稱以修改其屬性。**
3. **選取 [Rewriter] 標籤。**
4. **修改下列屬性：**

| 屬性名稱 | 描述 |
| --- | --- |
| URI | 在 [對映 URI 至規則集] 欄位中輸入需要的網域或主機名稱以及規則集，然後按一下 [新增]。<br>此項目會新增至 [對映 URI 至規則集] 欄位中。<br>指定網域或主機名稱以及規則集的格式如下所示：<br>`domain-name\|ruleset-name`<br>例如：<br>`eng.sesta.com\|default`<br>**備註 – 套用規則集的優先順序為** `hostname-subdomain-domain`。<br>以網域爲基礎規則集清單中的項目範例如下：<br>`sesta.com\|ruleset1`<br>`eng.sesta.com\|ruleset2`<br>`host1.eng.sesta.com\|ruleset3`<br>■ `ruleset3` 可套用於 `host1` 上的所有頁面。<br>■ `ruleset2` 可套用於 `eng` 子網域中的所有頁面，除了擷取於 `host1` 中的頁面。<br>■ `ruleset1` 可套用於 `sesta.com` 網域中的所有頁面，除了擷取於 `eng` 子網域與 `host1` 中的頁面。 |

# 配置剖析器與 MIME 類型的對映

Rewriter 有四個不同的剖析器以根據內容類型 - HTML、JAVASCRIPT、XML 與 CSS - 剖析網頁。依預設共用 MIME 類型會與這些剖析器相關。您可以在閘道服務中的 [對映剖析器至 MIME 類型] 欄位中將新 MIME 類型與這些剖析器相關聯。此將 Rewriter 功能延伸至其他 MIME 類型。

分隔多個項目請使用分號或逗號 (";" 或 ",")。

例如：

HTML=text/html;text/htm;text/x-component;text/wml; text/vnl/wap.wml

意味任何含有這些 MIME 的內容會被傳送到 HTML Rewriter 而 HTML 規則將被套用以重新寫入 URL。

**提示 –** 移除 MIME 對映清單中不需要的剖析器可以提高作業速度。例如，若您確定某些內部網站的內容將不會有任何 JavaScript，可以將 JAVASCRIPT 項目從 MIME 對映清單中移除。

### ▼ 配置剖析器與 MIME 類型的對映

1. 以管理員身份登入 Portal Server 管理主控台。
2. 選取 [Secure Remote Access] 標籤，並按一下設定檔名稱以修改其屬性。
3. 選取 [Rewriter] 標籤。
4. 修改下列屬性：

| 屬性名稱 | 描述 |
| --- | --- |
| 剖析器 | a. 在 [對映剖析器至 MIME 類型] 欄位中，於編輯方塊中新增需要的 MIME 類型。使用分號或逗號以分隔多個項目。<br>以 `HTML=text/html;text/htm` 格式指定項目<br>b. 按一下 [新增] 以新增需要的項目至清單中。 |

# 配置個人數位憑證認證

PDC 會由「憑證授權單位 (CA)」核發且使用 CA 的私人金鑰簽署。CA 在核發憑證前，會先驗證請求主體的身份。因此 PDC 的出現是一個具有權威的認證機制。

PDC 包含所有者的公開金鑰、所有者名稱、過期日期、核發數位憑證的「憑證授權單位」名稱、序號與一些其他資訊。

使用者可以使用 PDC 與已編碼的裝置，例如 Portal Server 中用於認證的智慧卡、與 Java 卡。已編碼裝置包含一個與儲存於卡中的 PDC 等效的電子文件。如果使用者使用其中一個機制登入，則不會顯示登入畫面，也不會顯示認證畫面。

PDC 認證會處理相關的數個步驟：

1. 使用者從瀏覽器中輸入連線請求，例如 `https://my.sesta.com`。
   對這個請求的回應會視至 `my.sesta.com` 的閘道是否已配置爲接受憑證而定。

   **備註 –** 當閘道配置爲接受憑證時，將僅接受使用憑證的登入請求，不接受其他種類登入請求。

   閘道會檢查憑證是否由已知的「憑證授權單位」核發，是否已過期與是否被竄改。若憑證有效，則閘道會讓使用者繼續執行驗證程序的下一步驟。
2. 閘道會將此憑證傳遞到伺服器中 PDC 認證模組。

## ▼ 配置 PDC 與編碼裝置

1. 在 **Portal Server** 機器上的 `/etc/opt/SUNWam/config/AMConfig.properties` 檔案新增下列行：`com.iplanet.authentication.modules.cert.gwAuthEnable=yes` 。
2. 將必要的憑證匯入要啓用 PDC 的閘道的憑證資料庫。要配置憑證，請參閱第 171 頁的「在閘道機器上匯入根 CA 憑證」
3. 以管理員身份登入 **Access Manager** 管理主控台，並依照下列步驟執行：
   a. 選取 [身份識別管理] 標籤，然後選取 [組織]。
   b. 從 [檢視] 下拉式功能表，按一下組織的 [服務]。
   c. 按一下 [新增] 以註冊憑證。
4. 從 **Access Manager** 管理主控台中，依照下列步驟執行：
   a. 選取想要的組織並按一下 [憑證] 旁的箭頭。
   b. 在 [可信任的遠端主機] 清單方塊中，不反白顯示任意內容，然後按一下 [移除]。
   c. 在文字欄位中在文字方塊中輸入任意內容，然後按一下 [新增]。
   d. 按一下 [儲存]。
5. 從 **Access Manager** 管理主控台中，依照下列步驟執行：
   a. 選擇必要的組織，然後從 [檢視] 下拉式功能表選取 [服務]。
      會顯示服務清單。
   b. 按一下 [認證配置] 核心服務旁的箭頭，並按一下 [新增]。
      顯示 [新建服務實例] 頁面。
   c. 輸入服務實例名稱 `gatewaypdc`。
   d. 按一下 [提交]。
      顯示 [gatewaypdc 服務實例清單]。
   e. 按一下 **gatewaypdc** 以編輯服務。
      會顯示 gatewaypdc 顯示特性頁面。

f. 按一下 [認證模組] 旁的 [編輯] 連結，然後按一下 [新增]。
隨即顯示 [新增模組] 頁。

g. 在 [模組名稱] 欄位選擇 [憑證]，而在 [實施條件] 欄位中選擇 [必要的]，然後按一下 [確定]。

h. 按一下 [確定] 完成。

6 從 Access Manager 管理主控台中，依照下列步驟執行：

a. 按一下 [核心] 旁的箭頭。

b. 在 [組織認證] 模組清單方塊中，選取 gatewaypdc。

c. 在 [使用者配置檔] 下拉功能表中選擇 [動態]。

d. 按一下 [儲存] 完成作業。

7 以管理員身份登入 Portal Server 管理主控台，並依照下列步驟執行：

a. 選取 [Secure Remote Access] 標籤並選取適當的閘道設定檔。

b. 選取 [安全性] 標籤。

c. 在 [啓用憑證的閘道主機] 清單方塊中，新增閘道名稱。

d. 按一下 [儲存]。

8 從終端機視窗重新啓動閘道設定檔：

```
./psadmin start-sra-instance -u amadmin -f passwordfile -N profilename -t
gateway
```

9 將 CA 所發出的用戶端憑證安裝至必須存取已啓用 PDC 的閘道的瀏覽器。

10 安裝用戶端憑證至 JVM 金鑰庫。可如下所示，從 windows 機器的 [開始] > [設定] > [控制台] > [Java] 來存取 JVM 控制面板。
新增下列內容至 Applet 執行階段參數：

- `Djavax.net.ssl.keyStore=Path to Keystore`
- `Djavax.net.ssl.keyStorePassword=password`
- `Djavax.net.ssl.keyStoreType=type`

11 存取您的閘道設定檔和機構：
https://gateway:instance-port/YourOrganization

您應該能夠登入而不會出現任何提示要求您輸入認證名稱的使用者名稱和密碼。

## ▼ 在閘道機器上匯入根 CA 憑證

1 **在閘道機器上匯入根 CA 憑證。**

   a. `<Gateway-Install-Dir>/SUNWportal/bin/certadmin -n <gw-profile-name>` 會列出 Certadmin 功能表。

   b. **選取選項 3。輸入憑證的路徑。**

   如需詳細資訊，請參閱第 10 章。

2 **產生「憑證簽署要求」以提交至 CA。**

   a. `<Gateway-Install-Dir>/SUNWportal/bin/certadmin -n <gw-profile-name>` 會列出 Certadmin 功能表。

   b. **選取選項 2。輸入適當資訊。**

   c. **儲存檔案。**

3 **提交「憑證簽署要求」至 CA，並取得核准。在 CA 簽署後，儲存憑證回應。**

4 **在取得 CA 核准後，匯入「伺服器憑證」。**

   a. `<Gateway-Install-Dir>/SUNWportal/bin/certadmin -n <gw-profile-name>` 會列出 Certadmin 功能表。

   b. **選取選項 4。**

   c. **指定包含「伺服器憑證」的檔案位置。**

5 **在 Portal Server 機器上匯入根 CA 憑證。**

# 使用指令行選項配置閘道屬性

此部分提供指令行選項，以從終端視窗配置下列作業的閘道屬性：


- 第 172 頁的「管理外部伺服器 Cookie 儲存」
- 第 173 頁的「啓用將 Cookie 標示爲安全」
- 第 173 頁的「建立不可使用之代理伺服器的 URL 清單」
- 第 174 頁的「管理 URI 對映的規則集」
- 第 175 頁的「指定預設網域」
- 第 176 頁的「管理 MIME 推測」
- 第 176 頁的「建立要剖析的 URI 對映清單」
- 第 177 頁的「管理遮罩」
- 第 178 頁的「指定遮罩種子字串」
- 第 178 頁的「建立不要遮罩的 URI 清單」
- 第 179 頁的「讓閘道通協定與原始 URI 通訊協定相同」


## ▼ 管理外部伺服器 Cookie 儲存

當啓用 [儲存外部伺服器 Cookie] 選項時，閘道會儲存與管理任何經由閘道存取的協力廠商應用程式或伺服器的 cookie。雖然應用程式或伺服器無法服務非 cookie 裝置或根據 cookie 進行狀態管理，閘道還是會透明遮罩應用程式或伺服器，使其無法了解閘道正在服務非 cookie 裝置。

有關非 Cookie 裝置與用戶端偵測的資訊，請參閱「*Access Manager* **自訂和** *API* **指南**。」

- **鍵入下列指令，並按下 Enter 鍵以管理外部伺服器 Cookie 的儲存。**

  - **啓用：**

    *PS_INSTALL_DIR*`/bin/psadmin set-attribute -u amadmin -f` *PASSWORD_FILE* `-m gateway --gateway-profile` *PROFILE_NAME* `-a CookieManagement true`

  - **停用：**

    *PS_INSTALL_DIR*`/bin/psadmin set-attribute -u amadmin -f` *PASSWORD_FILE* `-m gateway --gateway-profile` *PROFILE_NAME* `-a CookieManagement false`

  - **取得屬性值：**

    *PS_INSTALL_DIR* `/bin/psadmin get-attribute -u amadmin -f` *PASSWORD_FILE* `-m gateway --gateway-profile` *PROFILE_NAME* `-a CookieManagement`

**更多資訊** **亦請參閱**

「Sun Java System Portal Server 7.2 Command-Line Reference」中的「psadmin set-attribute」與「Sun Java System Portal Server 7.2 Command-Line Reference」中的「psadmin get-attribute」

## ▼ 啓用將 Cookie 標示為安全

當 cookie 標示爲安全時，瀏覽器會以更加的安全小心處理此 cookie。安全性的實施會根據瀏覽器而有所不同。必須啓用 [啓用 Cookie 管理] 屬性才可實現此功能。

- **鍵入下列指令，並按下 Enter 鍵將 Cookie 標示為安全。**

  - **啓用：**

    *PS_INSTALL_DIR*`/bin/psadmin set-attribute -u amadmin -f` *PASSWORD_FILE* `-m gateway --gateway-profile` *PROFILE_NAME* `-a MarkCookiesSecure true`

  - **停用：**

    *PS_INSTALL_DIR*`/bin/psadmin set-attribute -u amadmin -f` *PASSWORD_FILE* `-m gateway --gateway-profile` *PROFILE_NAME* `-a MarkCookiesSecure false`

  - **取得屬性值：**

    *PS_INSTALL_DIR* `/bin/psadmin get-attribute -u amadmin -f` *PASSWORD_FILE* `-m gateway --gateway-profile` *PROFILE_NAME* `-a MarkCookiesSecure`

更多資訊 **亦請參閱**

「Sun Java System Portal Server 7.2 Command-Line Reference」中的 「psadmin set-attribute」 與 「Sun Java System Portal Server 7.2 Command-Line Reference」中的 「psadmin get-attribute」

## ▼ 建立不可使用之代理伺服器的 URL 清單

閘道嘗試直接連接列於 [請勿使用網路代理伺服器 URL] 清單的 URL。Web 代理伺服器並不會用於連接這些 URL。

- **鍵入下列指令，並按下 Enter 鍵以管理不可使用之代理伺服器的 URL。**

---

**備註 –** 如果有一個以上的 URL，則以空格分開每個 URL。

---

  - **指定不使用的 URL：**

    *PS_INSTALL_DIR* `/bin/psadmin set-attribute -u amadmin -f` *PASSWORD_FILE* `-m gateway --gateway-profile` *PROFILE_NAME* `-a DontUseWebProxyURL -A` *"LIST_OF_URLS"*

- **新增至現有的 URL 清單：**

  *PS_INSTALL_DIR*/bin/psadmin set-attribute -u amadmin -f *PASSWORD_FILE* -m gateway --gateway-profile *PROFILE_NAME* -a DontUseWebProxyURL -A *"LIST_OF_URLS"*

- **從現有的 URL 清單移除：**

  *PS_INSTALL_DIR*/bin/psadmin set-attribute -u amadmin -f *PASSWORD_FILE* -m gateway --gateway-profile *PROFILE_NAME* -a DontUseWebProxyURL -E *"LIST_OF_URLS"*

- **取得現有的 URL 清單：**

  *PS_INSTALL_DIR* /bin/psadmin get-attribute -u amadmin -f *PASSWORD_FILE* -m gateway --gateway-profile *PROFILE_NAME* -a DontUseWebProxyURL

**更多資訊** **亦請參閱**

「Sun Java System Portal Server 7.2 Command-Line Reference」中的「psadmin set-attribute」與「Sun Java System Portal Server 7.2 Command-Line Reference」中的「psadmin get-attribute」

## ▼ 管理 URI 對映的規則集

Secure Remote Access 支援 Microsoft Exchange 2000 SP3 安裝以及 Outlook Web Access (OWA) 的 MS Exchange 2003。

1. **新增 URI 至現有的清單：**

   *PS_INSTALL_DIR*/bin/psadmin set-attribute -u amadmin -f *PASSWORD_FILE* -m gateway --gateway-profile default -a DomainsAndRulesets -A "*URI*|*RULE_SET_NAME URI*|*RULE_SET_NAME*"

2. **從現有的清單移除 URI：**

   *PS_INSTALL_DIR*/bin/psadmin set-attribute -u amadmin -f *PASSWORD_FILE* -m gateway --gateway-profile default -a DomainsAndRulesets -E "*URI*|*RULE_SET_NAME URI*|*RULE_SET_NAME*"

3. **取得現有的清單：**

   *PS_INSTALL_DIR* /bin/psadmin get-attribute -u amadmin -f *PASSWORD_FILE* -m gateway --gateway-profile *PROFILE_NAME* -a DomainsAndRulesets

4 **輸入下列指令，並按下 Enter 鍵以管理 Outlook Web Access 的規則集。**

- **新增規則集：**

  *PS_INSTALL_DIR*/bin/psadmin set-attribute -u amadmin -f *PASSWORD_FILE* -m gateway --gateway-profile default -a DomainsAndRulesets -A "*EXCHANGE2000_SERVER_NAME* exchange_2000sp3_owa_ruleset"

- **移除規則集：**

  *PS_INSTALL_DIR* /bin/psadmin set-attribute -u amadmin -f *PASSWORD_FILE* -m gateway --gateway-profile default -a DomainsAndRulesets -E "*EXCHANGE2000_SERVER_NAME* exchange_2000sp3_owa_ruleset"

- **設定 URI 至規則集的對映清單：**

  *PS_INSTALL_DIR*/bin/psadmin set-attribute -u amadmin -f *PASSWORD_FILE* -m gateway --gateway-profile *PROFILE_NAME* -a DomainsAndRulesets "*URI*|*RULE_SET_NAME URI*|*RULE_SET_NAME* "

**更多資訊** **亦請參閱**

「Sun Java System Portal Server 7.2 Command-Line Reference」中的「psadmin set-attribute」與「Sun Java System Portal Server 7.2 Command-Line Reference」中的「psadmin get-attribute」

## ▼ 指定預設網域

當 URL 僅包括主機名稱而沒有網域與子網域時，預設網域將特別有用。在此情況下，閘道假設主機名稱位於預設網域清單中，並繼續執行相應的操作。

例如，若 URL 中的主機名稱爲 `host1`，且預設網域與子網域被指定爲 `red.sesta.com`，則主機名稱會被解析爲 `host1.red.sesta.com`。

- **鍵入下列指令，並按下 Enter 鍵以指定預設網域。**

  - **設定預設網域：**

    *PS_INSTALL_DIR* /bin/psadmin set-attribute -u amadmin -f *PASSWORD_FILE* -m gateway --gateway-profile *PROFILE_NAME* -a DefaultDomainsAndSubdomains "*DOMAIN_NAME*"

  - **取得預設網域：**

    *PS_INSTALL_DIR* /bin/psadmin get-attribute -u amadmin -f *PASSWORD_FILE* -m gateway --gateway-profile *PROFILE_NAME* -a DefaultDomainsAndSubdomains

**更多資訊** **亦請參閱**

「Sun Java System Portal Server 7.2 Command-Line Reference」中的「psadmin set-attribute」與「Sun Java System Portal Server 7.2 Command-Line Reference」中的「psadmin get-attribute」

## ▼ 管理 MIME 推測

Rewriter 會根據網頁的 MIME 類型選擇剖析器。有些 Web 伺服器，如 WebLogic 和 Oracle，並不會傳送 MIME 類型。要解決這個問題，可以啓用 MIME 推測，方法是新增資料至 [剖析器至 URI 對映] 清單方塊。

- **鍵入下列指令，並按下 Enter 鍵以管理 MIME 推測。**

  - **啓用 MIME 猜測：**

    *PS_INSTALL_DIR* `/bin/psadmin set-attribute -u amadmin -f` *PASSWORD_FILE* `-m gateway --gateway-profile` *PROFILE_NAME* `-a EnableMIMEGuessing true`

  - **停用 MIME 推測：**

    *PS_INSTALL_DIR* `/bin/psadmin set-attribute -u amadmin -f` *PASSWORD_FILE* `-m gateway --gateway-profile` *PROFILE_NAME* `-a EnableMIMEGuessing false`

  - **取得值：**

    *PS_INSTALL_DIR*`/bin/psadmin get-attribute -u amadmin -f` *PASSWORD_FILE* `-m gateway --gateway-profile` *PROFILE_NAME* `-a EnableMIMEGuessing`

**更多資訊** **亦請參閱**

「Sun Java System Portal Server 7.2 Command-Line Reference」中的「psadmin set-attribute」與「Sun Java System Portal Server 7.2 Command-Line Reference」中的「psadmin get-attribute」

## ▼ 建立要剖析的 URI 對映清單

若已啓用 MIME 推測核取方塊，且伺服器沒有傳送 MIME 類型，可使用這個清單方塊以對映剖析器至 URI。

由分號分隔多個 URI。

例如 HTML=*.html; *.htm;*Servlet。這表示 HTML Rewriter 會用於重新寫入任何含有 html、htm，或 Servlet 副檔名的網頁內容。

- **鍵入下列指令，並按下 Enter 鍵以建立要剖析的 URI 對映清單。**

  - **設定要剖析的 URI 對映清單：**

    *PS_INSTALL_DIR*/bin/psadmin set-attribute -u amadmin -f *PASSWORD_FILE* -m gateway --gateway-profile *PROFILE_NAME* -a MIMEMap

  - **新增至現有的清單：**

    *PS_INSTALL_DIR* /bin/psadmin set-attribute -u amadmin -f *PASSWORD_FILE* -m gateway --gateway-profile *PROFILE_NAME* -a MIMEMap -A *LIST*

  - **從現有的清單移除：**

    *PS_INSTALL_DIR* /bin/psadmin set-attribute -u amadmin -f *PASSWORD_FILE* -m gateway --gateway-profile *PROFILE_NAME* -a MIMEMap -E *LIST*

  - **取得現有的清單：**

    *PS_INSTALL_DIR* /bin/psadmin get-attribute -u amadmin -f *PASSWORD_FILE* -m gateway --gateway-profile *PROFILE_NAME*-a MIMEMap

更多資訊 **亦請參閱**

「Sun Java System Portal Server 7.2 Command-Line Reference」中的 「psadmin set-attribute」

## ▼ 管理遮罩

遮罩允許 Rewriter 重新寫入 URI，如此便看不見頁面的企業內部網路 URL。

- **鍵入下列指令，並按下 Enter 鍵以管理遮罩。**

  - **啓用遮罩：**

    *PS_INSTALL_DIR*/bin/psadmin set-attribute -u amadmin -f *PASSWORD_FILE* -m gateway --gateway-profile *PROFILE_NAME* -a EnableObfuscation true

  - **停用遮罩：**

    *PS_INSTALL_DIR*/bin/psadmin set-attribute -u amadmin -f *PASSWORD_FILE* -m gateway --gateway-profile *PROFILE_NAME* -a EnableObfuscation false

  - **取得值：**

    *PS_INSTALL_DIR*/bin/psadmin get-attribute -u amadmin -f *PASSWORD_FILE* -m gateway --gateway-profile *PROFILE_NAME* -a EnableObfuscation

**更多資訊** **亦請參閱**

「Sun Java System Portal Server 7.2 Command-Line Reference」中的「psadmin set-attribute」與「Sun Java System Portal Server 7.2 Command-Line Reference」中的「psadmin get-attribute」

## ▼ 指定遮罩種子字串

種子字串會用於遮罩 URI。遮罩演算法會產生字串。

**備註 –** 若此種子字串已變更或閘道已重新啓動，則無法將已遮罩的 URI 新增書籤。

- **鍵入下列指令，並按下 Enter 鍵以指定遮罩種子字串。**
  - **設定遮罩種子字串：**

    *PS_INSTALL_DIR* `/bin/psadmin set-attribute -u amadmin -f` *PASSWORD_FILE* `-m gateway --gateway-profile` *PROFILE_NAME* `-a ObfuscationSecretKey` *SECRET_KEY*

  - **取得值：**

    *PS_INSTALL_DIR*`/bin/psadmin get-attribute -u amadmin -f` *PASSWORD_FILE* `-m gateway --gateway-profile` *PROFILE_NAME* `-a ObfuscationSecretKey`

**更多資訊** **亦請參閱**

「Sun Java System Portal Server 7.2 Command-Line Reference」中的「psadmin set-attribute」與「Sun Java System Portal Server 7.2 Command-Line Reference」中的「psadmin get-attribute」

## ▼ 建立不要遮罩的 URI 清單

某些應用程式 (例如 applet) 需要網際網路 URI 且無法被遮罩。要指定那些應用程式，請新增 URI 至清單方塊。

例如，如果您已新增 `*/Applet/Param*` 至清單方塊，當內容 URI `http://abc.com/Applet/Param1.html` 符合規則集的規則時，則不會將 URL 遮罩起來。

**備註 –** 如果有一個以上的 URI，則以空格分開每個 URI。

- **鍵入下列指令，並按下 Enter 鍵以建立不要遮罩的 URI 清單。**

  - **設定不要遮罩的 URI 清單：**

    *PS_INSTALL_DIR*`/bin/psadmin set-attribute -u amadmin -f` *PASSWORD_FILE* `-m gateway --gateway-profile` *PROFILE_NAME* `-a NotToObscureURIList` *LIST_OF_URI*

  - **新增至現有的清單：**

    *PS_INSTALL_DIR* `/bin/psadmin set-attribute -u amadmin -f` *PASSWORD_FILE* `-m gateway --gateway-profile` *PROFILE_NAME* `-a NotToObscureURIList -A` *LIST_OF_URI*

  - **從現有的清單移除：**

    *PS_INSTALL_DIR* `/bin/psadmin set-attribute -u amadmin -f` *PASSWORD_FILE* `-m gateway --gateway-profile` *PROFILE_NAME* `-a NotToObscureURIList -E` *LIST_OF_URI*

  - **取得現有的值：**

    *PS_INSTALL_DIR* `/bin/psadmin get-attribute -u amadmin -f` *PASSWORD_FILE* `-m gateway --gateway-profile` *PROFILE_NAME* `-a NotToObscureURIList`

**更多資訊** **亦請參閱**

「Sun Java System Portal Server 7.2 Command-Line Reference」中的「psadmin set-attribute」與「Sun Java System Portal Server 7.2 Command-Line Reference」中的「psadmin get-attribute」

## ▼ 讓閘道通協定與原始 URI 通訊協定相同

當閘道以 http 與 https 兩種模式執行時，可以啓用 Rewriter 以使用一致的通訊協定存取 HTML 內容的參照資源。

例如，若原始 URL 爲 `http://intranet.com/Public.html`，則會新增 http 閘道。若原始 URL 爲 `https://intranet.com/Public.html`，則會新增 https 閘道。

---

**備註 –** 這將僅套用至靜態 URI，而非產生於 Javascript 的動態 URI。

---

- **鍵入下列指令，並按下 Enter 鍵使閘道協定與原始的 URI 協定相同。**

  - **啓用：**

    *PS_INSTALL_DIR*`/bin/psadmin set-attribute -u amadmin -f` *PASSWORD_FILE* `-m gateway --gateway-profile` *PROFILE_NAME* `-a UseConsistentProtocolForGateway true`

- **停用：**

  *PS_INSTALL_DIR*`/bin/psadmin set-attribute -u amadmin -f` *PASSWORD_FILE* `-m gateway --gateway-profile` *PROFILE_NAME* `-a UseConsistentProtocolForGateway false`

- **取得值：**

  *PS_INSTALL_DIR*`/bin/psadmin get-attribute -u amadmin -f` *PASSWORD_FILE* `-m gateway --gateway-profile` *PROFILE_NAME* `-a UseConsistentProtocolForGateway`

**更多資訊** **亦請參閱**

「Sun Java System Portal Server 7.2 Command-Line Reference」中的「psadmin set-attribute」與「Sun Java System Portal Server 7.2 Command-Line Reference」中的「psadmin get-attribute」

◆ ◆ ◆ 第 9 章

# 9 在閘道服務中配置 Rewriter

在此反白內容。

本章包含下列各節：


- 第 181 頁的 「建立 URI 與規則集對映清單」
- 第 182 頁的 「在閘道服務中配置 Rewriter」


如需 rewriter 規則的詳細資訊，請參閱第 68 頁的 「定義以語言爲基礎的規則」

如需 Rewriter 問題的詳細資訊，請參閱第 90 頁的 「使用除錯記錄檔排除故障」。

如需 Rewriter 範例，請參閱第 93 頁的 「工作範例」。

## 建立 URI 與規則集對映清單

建立規則集之後，可以使用 [對映 URI 至規則集] 欄位將網域與規則集關聯在一起。下列兩個項目會依預設新增至 [對映 URI 至規則集] 欄位：

- `*://*.Sun.COM/portal/*|default_gateway_ruleset`

  其中 `sun.com` 是安裝入口網站的網域，而 /portal 是入口網站的安裝環境
- `*|generic_ruleset`

這表示，網域爲 `sun.com` 之入口網站目錄的所有網頁，將套用 `default_gateway_ruleset`。對於其他頁面，則套用常規規則集。`default_gateway_ruleset` 與 `generic_ruleset` 是預先封裝的規則集。

**備註 –** 對於所有顯示於標準入口網站桌面中的內容，將使用 `default_gateway_ruleset` 規則集，與取得內容處無關。

例如，假設配置標準入口網站桌面來從 URL `yahoo.com` 擷取內容。Portal Server 位於 `sesta.com`。將套用 `sesta.com` 規則集至取得的內容。

**備註 –** 您爲其指定規則集的網域必須列於網域與子網域的代理伺服器清單中。

## 在語法中使用萬用字元

您可對映一個完全合格的 URI 或在規則集中使用星號來對映部分 URI。

例如，您可以將 `java_index_page_ruleset` 套用至 `index.html` 網頁，如下所示：

```
www.sun.com/java/index.html/java_index_page_ruleset
```

或者，您可以將`java_directory_ruleset` 套用至 Java 目錄下的所有網頁，如下所示：

```
www.sun.com/java/* /java_directory_ruleset
```

# 在閘道服務中配置 Rewriter

藉由使用 [Rewriter] 標籤下的閘道服務，您可以執行下列兩種工作 - 基礎與進階：

基礎作業


- 第 182 頁的 「啓用閘道以重寫所有 URI」
- 第 183 頁的 「指定不要重寫的 URI」
- 第 183 頁的 「將 URI 對應至規則集」
- 第 184 頁的 「指定 MIME 對映」
- 第 185 頁的 「指定預設網域」


## ▼ 啓用閘道以重寫所有 URI

若您啓用閘道服務中 [啓用所有 URI 的重寫] 選項，則 Rewriter 會重寫所有 URI 而不會將其於 [網域與子網域代理伺服器清單] 中的項目進行核對。忽略網域與子網域清單的代理伺服器項目。

1. **以管理員身份登入 Portal Server 管理主控台。**
2. **選取 [Secure Remote Access] 標籤，並選取要修改其屬性的閘道設定檔。**

3. 選取 [Rewriter] 標籤。
4. 在 [基本選項] 下，選取 [啓用所有 URI 的重寫] 核取方塊，以使閘道重寫所有 URI。
5. 按一下 [儲存] 完成作業。
6. 從終端機視窗重新啓動閘道：

```
./psadmin start-sra-instance –u amadmin – f  <password file> –N <profile name>– t  <gateway>
```

## ▼ 指定不要重寫的 URI

1. 以管理員身份登入 Portal Server 管理主控台。
2. 選取 [Secure Remote Access] 標籤，並選取要設定屬性的閘道設定檔。
3. 選取 [Rewriter] 標籤。
4. 在 [基本選項] 下，於 [新增] 欄位內輸入 URI，並按一下 [新增]。
   URI 值會顯示於 [不要重寫的 URI] 方塊。

   **備註 –** 將 #* 新增至這份清單可允許重寫 URI，即使 href 規則是規則集的一部分也一樣。
5. 按一下 [儲存] 完成作業。
6. 從終端機視窗重新啓動閘道：

```
./psadmin start-sra-instance –u amadmin – f  <password file> –N <profile name>– t  <gateway>
```

## ▼ 將 URI 對應至規則集

1. 以管理員身份登入 Portal Server 管理主控台。
2. 選取 [Secure Remote Access] 標籤，並選取要設定屬性的閘道設定檔。
3. 選取 [Rewriter] 標籤。
4. 在 [Rewriter 選項] 下，按一下 [對映 URI 至規則集]，並按一下 [新增列]。

5 **在 URI 欄位內輸入必要的網域或主機名稱，並在 [規則集] 欄位中輸入適當的規則集。**

此項目會新增至 [對映 URI 至規則集] 清單中。指定網域或主機名稱以及規則集的格式如下所示：

```
domain name|ruleset name
```

例如：

```
eng.sesta.com|default
```

6 **按一下 [儲存] 完成作業。**

7 **從終端機視窗重新啓動閘道：**

```
./psadmin start-sra-instance –u amadmin – f  <password file> –N <profile name>– t  <gateway>
```

## ▼ 指定 MIME 對映

Rewriter 有四個不同的剖析器以根據內容類型：HTML、JAVASCRIPT、CSS 和 XML。依預設共用 MIME 類型會與這些剖析器相關。您可以在閘道服務中的 [對映剖析器至 MIME 類型] 欄位中將新 MIME 類型與這些剖析器相關聯。此將 Rewriter 功能延伸至其他 MIME 類型。

分隔多個項目請使用分號或逗號 (";" 或 ",")。例如：

```
HTML=text/html;text/htm;text/x-component;text/wml; text/vnl/wap.wml
```

意味任何含有這些 MIME 的內容會被傳送到 HTML Rewriter 而 HTML 規則將被套用以重寫 URL。

---

**提示 –** 移除 MIME 對映清單中不需要的剖析器可以提高作業速度。例如，若您確定某些內部網站的內容將不會有任何 JavaScript，可以將 JAVASCRIPT 項目從 MIME 對映清單中移除。

---

1 **以管理員身份登入 Portal Server 管理主控台。**

2 **選取 [Secure Remote Access] 標籤，並選取要設定屬性的閘道設定檔。**

3 **選取 [Rewriter] 標籤。**

4 **在 [Rewriter 選項] 下，按一下 [對映剖析器至 MIME 類型]。**

以 `HTML=text/html;text/htm` 格式指定項目

5 **按一下 [新增列] 將項目新增至清單。在 [MIME 類型] 欄位中輸入剖析器值以及其對映至的對應 MIME 值。**

6. **按一下 [儲存] 完成作業。**

7. **從終端機視窗重新啓動閘道：**

```
./psadmin start-sra-instance –u amadmin – f  <password file> –N <profile name>– t  <gateway>
```

## ▼ 指定預設網域

當 URL 僅包括主機名稱而沒有網域與子網域時，預設網域與子網域將特別有用。在此情況下，閘道將假設主機名稱位於預設網域與子網域中，並繼續執行相應的操作。

例如，若 URL 中的主機名稱爲 `host1`，且預設網域與子網域被指定爲 `red.sesta.com`，則主機名稱會被解析爲 `host1.red.sesta.com`。

1. **以管理員身份登入 Portal Server 管理主控台。**

2. **選取 [Secure Remote Access] 標籤，並選取要設定屬性的閘道設定檔。**

3. **選取 [部署] 標籤。**

4. **在 [網域與子網域的代理伺服器] 欄位中，輸入不包含代理伺服器的必要網域名稱。**

5. **按一下 [儲存] 完成作業。**

6. **從終端機視窗重新啓動閘道：**

```
./psadmin start-sra-instance –u amadmin – f  <password file> –N <profile name>– t  <gateway>
```

◆ ◆ ◆ 第 10 章

# 10 使用憑證

本章會介紹憑證管理並解釋如何安裝自簽的憑證與來自憑證授權單位 (CA) 的憑證。

本章說明下列主題：


- 第 187 頁的 「SSL 憑證簡介」
- 第 188 頁的 「憑證檔案」
- 第 189 頁的 「憑證信任屬性」
- 第 189 頁的 「CA 信任屬性」
- 第 193 頁的 「certadmin 程序檔」
- 第 193 頁的 「產生自簽憑證」
- 第 196 頁的 「安裝來自憑證授權單位的 SSL 憑證」
- 第 196 頁的 「新增根 CA 憑證」
- 第 199 頁的 「修改憑證的信任屬性」
- 第 200 頁的 「列示根 CA 憑證」
- 第 200 頁的 「列示所有憑證」
- 第 198 頁的 「刪除憑證」
- 第 201 頁的 「列印憑證」


## SSL 憑證簡介

Sun Java System Portal Server Secure Remote Access 軟體爲遠端使用者提供以憑證爲基礎的認證。SRA 使用安全套接層 (SSL) 以啓用安全通訊。此 SSL 通訊協定可實現兩部機器之間的安全通訊。

SSL 憑證使用公開金鑰與私人金鑰對提供加密與解密功能。

有兩種類型的憑證：

- 自簽憑證 (亦稱爲根 CA 憑證)
- 由憑證授權單位 (CA) 核發的憑證

依預設，當您安裝閘道時，系統會產生並安裝自簽憑證。

安裝之後，您可以隨時產生、獲得或取代憑證。

SRA 同時支援使用個人數位憑證 (PDC) 的用戶端認證。PDC 是透過 SSL 用戶端認證進行使用者認證的機制。有了 SSL 用戶端認證，SSL 訊號交換模式便會於閘道結束。閘道會擷取使用者的 PDC 並將它傳送到認證伺服器。而此伺服器會使用 PDC 認證使用者。要隨認證鏈接一起配置 PDC，請參閱第 53 頁的「使用認證鏈接」。

SRA 提供名爲 `certadmin` 的工具，可讓您用來管理 SSL 憑證。請參閱 第 193 頁的「certadmin 程序檔」。

**備註 –** 憑證快顯式視窗在 SSL 應用程式中很常見。建議使用者接受警告並繼續執行。

# 憑證檔案

與憑證相關的檔案位於 `/etc/opt/SUNWportal/cert/` *gateway-profile-name*。此目錄依預設包含 5 個檔案。

第 188 頁的「憑證檔案」列出這些檔案及其描述。

**表 10–1** 憑證檔案

| 檔案名稱 | 類型 | 描述 |
|---|---|---|
| `cert8.db`、`key3.db`、`secmod.db` | 二進位 | 包含憑證、金鑰和密碼編譯模組的資料。<br>可以使用 `certadmin` 程序檔進行操控。<br>如有必要，這些檔案可以在 Portal Server 主機和閘道元件或閘道之間共享使用。 |
| `.jsspass` | 隱藏文字檔 | 包含用於 SRA 金鑰資料庫的加密密碼。 |
| `.nickname` | 隱藏文字檔 | 以 *token-name:certificate-name* 格式儲存閘道需要使用的記號與憑證的名稱。<br>若您正在使用預設記號 (預設內部軟體加密模組的記號)，請省略記號名稱。在大部分的情形下，`.nickname` 檔案僅會儲存憑證名稱。<br>身爲管理員，您可以修改此檔案中的憑證名稱。閘道現在將使用您所指定的憑證。 |

# 憑證信任屬性

憑證的信任屬性表示以下資訊：

- 憑證 (就用戶端或伺服器憑證而言) 是否由信任的 CA 所核發。
- 是否可以信任憑證 (就根憑證而言) 作爲伺服器與用戶端憑證的核發者。

每種憑證有三種可能的信任種類，說明順序爲：「SSL、電子郵件、物件簽署」。只有第一種類別可用於閘道。在每個種類位置，可以使用零或其他信任屬性代碼。

種類的屬性代碼由逗號隔開，而整個屬性集則是由引號環繞。例如，閘道安裝期間產生並安裝的自簽憑證標記爲 "u,u,u"，表示此憑證爲伺服器憑證 (使用者憑證)，而不是根 CA 憑證。

第 189 頁的 「憑證信任屬性」列出可能的屬性值與每個值的意義。

**表 10–2** 憑證信任屬性

| 屬性 | 描述 |
|---|---|
| p | 有效點 |
| P | 可信任點 (暗含 p) |
| c | 有效 CA |
| T | 可信任的 CA 核發用戶端憑證 (暗含 c) |
| C | 可信任的 CA 核發伺服器憑證 (僅限 SSL) (暗含 c) |
| u | 憑證可以用於認證或簽署 |
| w | 傳送警告 (在該環境中使用憑證時，與其他屬性一起使用以便包含一個警告) |

# CA 信任屬性

憑證資料庫中包含眾所皆知的公開 CA。有關修改公開 CA 信任屬性的資訊，請參閱第 199 頁的 「修改憑證的信任屬性」。

第 189 頁的 「CA 信任屬性」列出最常用的憑證授權單位及其信任屬性。

**表 10–3** 公開憑證授權單位

| 憑證授權單位名稱 | 信任屬性 |
|---|---|
| Verisign/RSA Secure Server CA | CPp,CPp,CPp |
| VeriSign Class 4 Primary CA | CPp,CPp,CPp |

表 10–3 公開憑證授權單位 *(續)*

| | |
|---|---|
| GTE CyberTrust Root CA | CPp,CPp,CPp |
| GTE CyberTrust Global Root | CPp,CPp,CPp |
| GTE CyberTrust Root 5 | CPp,CPp,CPp |
| GTE CyberTrust Japan Root CA | CPp,CPp,CPp |
| GTE CyberTrust Japan Secure Server CA | CPp,CPp,CPp |
| Thawte Personal Basic CA | CPp,CPp,CPp |
| Thawte Personal Premium CA | CPp,CPp,CPp |
| Thawte Personal Freemail CA | CPp,CPp,CPp |
| Thawte Server CA | CPp,CPp,CPp |
| Thawte Premium Server CA | CPp,CPp,CPp |
| American Express CA | CPp,CPp,CPp |
| American Express Global CA | CPp,CPp,CPp |
| Equifax Premium CA | CPp,CPp,CPp |
| Equifax Secure CA | CPp,CPp,CPp |
| BelSign Object Publishing CA | CPp,CPp,CPp |
| BelSign Secure Server CA | CPp,CPp,CPp |
| TC TrustCenter, Germany, Class 0 CA | CPp,CPp,CPp |
| TC TrustCenter, Germany, Class 1 CA | CPp,CPp,CPp |
| TC TrustCenter, Germany, Class 2 CA | CPp,CPp,CPp |
| TC TrustCenter, Germany, Class 3 CA | CPp,CPp,CPp |
| TC TrustCenter, Germany, Class 4 CA | CPp,CPp,CPp |
| ABAecom (sub., Am. Bankers Assn.) Root CA | CPp,CPp,CPp |
| Digital Signature Trust Co. Global CA 1 | CPp,CPp,CPp |
| Digital Signature Trust Co. Global CA 3 | CPp,CPp,CPp |
| Digital Signature Trust Co. Global CA 2 | CPp,CPp,CPp |
| Digital Signature Trust Co. Global CA 4 | CPp,CPp,CPp |
| Deutsche Telekom AG Root CA | CPp,CPp,CPp |
| Verisign Class 1 Public Primary Certification Authority | CPp,CPp,CPp |
| Verisign Class 2 Public Primary Certification Authority | CPp,CPp,CPp |

表 10–3 公開憑證授權單位 (續)

| | |
|---|---|
| Verisign Class 3 Public Primary Certification Authority | CPp,CPp,CPp |
| Verisign Class 1 Public Primary Certification Authority - G2 | CPp,CPp,CPp |
| Verisign Class 2 Public Primary Certification Authority - G2 | CPp,CPp,CPp |
| Verisign Class 3 Public Primary Certification Authority - G2 | CPp,CPp,CPp |
| Verisign Class 4 Public Primary Certification Authority - G2 | CPp,CPp,CPp |
| GlobalSign Root CA | CPp,CPp,CPp |
| GlobalSign Partners CA | CPp,CPp,CPp |
| GlobalSign Primary Class 1 CA | CPp,CPp,CPp |
| GlobalSign Primary Class 2 CA | CPp,CPp,CPp |
| GlobalSign Primary Class 3 CA | CPp,CPp,CPp |
| ValiCert Class 1 VA | CPp,CPp,CPp |
| ValiCert Class 2 VA | CPp,CPp,CPp |
| ValiCert Class 3 VA | CPp,CPp,CPp |
| Thawte Universal CA Root | CPp,CPp,CPp |
| Verisign Class 1 Public Primary Certification Authority - G3 | CPp,CPp,CPp |
| Verisign Class 2 Public Primary Certification Authority - G3 | CPp,CPp,CPp |
| Verisign Class 3 Public Primary Certification Authority - G3 | CPp,CPp,CPp |
| Verisign Class 4 Public Primary Certification Authority - G3 | CPp,CPp,CPp |
| Entrust.net Secure Server CA | CPp,CPp,CPp |
| Entrust.net Secure Personal CA | CPp,CPp,CPp |
| Entrust.net Premium 2048 Secure Server CA | CPp,CPp,CPp |
| ValiCert OCSP Responder | CPp,CPp,CPp |
| Baltimore CyberTrust Code Signing Root | CPp,CPp,CPp |
| Baltimore CyberTrust Root | CPp,CPp,CPp |
| Baltimore CyberTrust Mobile Commerce Root | CPp,CPp,CPp |
| Equifax Secure Global eBusiness CA | CPp,CPp,CPp |
| Equifax Secure eBusiness CA 1 | CPp,CPp,CPp |
| Equifax Secure eBusiness CA 2 | CPp,CPp,CPp |
| Visa International Global Root 1 | CPp,CPp,CPp |

表 10–3 公開憑證授權單位 *(續)*

| | |
|---|---|
| Visa International Global Root 2 | CPp,CPp,CPp |
| Visa International Global Root 3 | CPp,CPp,CPp |
| Visa International Global Root 4 | CPp,CPp,CPp |
| Visa International Global Root 5 | CPp,CPp,CPp |
| beTRUSTed Root CA | CPp,CPp,CPp |
| Xcert Root CA | CPp,CPp,CPp |
| Xcert Root CA 1024 | CPp,CPp,CPp |
| Xcert Root CA v1 | CPp,CPp,CPp |
| Xcert Root CA v1 1024 | CPp,CPp,CPp |
| Xcert EZ | CPp,CPp,CPp |
| CertEngine CA | CPp,CPp,CPp |
| BankEngine CA | CPp,CPp,CPp |
| FortEngine CA | CPp,CPp,CPp |
| MailEngine CA | CPp,CPp,CPp |
| TraderEngine CA | CPp,CPp,CPp |
| USPS Root | CPp,CPp,CPp |
| USPS Production 1 | CPp,CPp,CPp |
| AddTrust Non-Validated Services Root | CPp,CPp,CPp |
| AddTrust External Root | CPp,CPp,CPp |
| AddTrust Public Services Root | CPp,CPp,CPp |
| AddTrust Qualified Certificates Root | CPp,CPp,CPp |
| Verisign Class 1 Public Primary OCSP Responder | CPp,CPp,CPp |
| Verisign Class 2 Public Primary OCSP Responder | CPp,CPp,CPp |
| Verisign Class 3 Public Primary OCSP Responder | CPp,CPp,CPp |
| Verisign Secure Server OCSP Responder | CPp,CPp,CPp |
| Verisign Time Stamping Authority CA | CPp,CPp,CPp |
| Thawte Time Stamping CA | CPp,CPp,CPp |
| E-Certify CA | CPp,CPp,CPp |
| E-Certify RA | CPp,CPp,CPp |

表 10–3 公開憑證授權單位 (續)

| | |
|---|---|
| Entrust.net Global Secure Server CA | CPp,CPp,CPp |
| Entrust.net Global Secure Personal CA | CPp,CPp,CPp |

# certadmin 程序檔

您可以使用 certadmin 程序檔執行下列憑證管理作業：


- 第 193 頁的 「產生自簽憑證」
- 第 194 頁的 「產生憑證簽署請求 (CSR)」
- 第 196 頁的 「新增根 CA 憑證」
- 第 197 頁的 「安裝來自 CA 的憑證」
- 第 198 頁的 「刪除憑證」
- 第 199 頁的 「修改憑證的信任屬性」
- 第 200 頁的 「列示根 CA 憑證」
- 第 200 頁的 「列示所有憑證」
- 第 201 頁的 「列印憑證」


## 產生自簽憑證

您需要爲每個伺服器和閘道之間的 SSL 通訊產生憑證。

### ▼ 安裝之後產生自簽憑證

1 **以超級使用者身份，在您想要產生憑證的閘道機器上執行 certadmin 程序檔：**

*portal-server-install-root*/SUNWportal/bin/certadmin -n *gateway-profile-name*

系統便會顯示憑證管理功能表。

```
1) Generate Self-Signed Certificate
2) Generate Certificate Signing Request (CSR)
3) Add Root CA Certificate
4) Install Certificate From Certificate Authority (CA)
5) Delete Certificate
6) Modify Trust Attributes of Certificate (e.g., for PDC)
7) List Root CA Certificates
8) List All Certificates
9) Print Certificate Content
10) Quit
choice: [10]
1
```

2. **在憑證管理功能表上選擇選項 1。**
   憑證管理程序檔會詢問您是否想要保留現有的資料庫檔案。

3. **請輸入組織特定的資訊、記號名稱和憑證名稱。**

---

**備註 –** 如需萬用字元憑證，請在主機的完全合格的 DNS 名稱中指定一個 * 號。例如，如果主機的完全合格 DNS 名稱爲 `abc.sesta.com`，請指定爲 `*.sesta.com`。產生的憑證現在對於 `sesta.com` 網域中的所有主機名稱都有效。

---

```
What is the fully-qualified DNS name of this host? [host_name.domain_name]
What is the name of your organization (ex: Company)? []
What is the name of your organizational unit (ex: division)? []
What is the name of your City or Locality? []
What is the name (no abbreviation please) of your State or Province? []
What is the two-letter country code for this unit? []
Token name is needed only if you are not using the default internal
(software) cryptographic module, for example, if you want to use a crypto card
(Token names could be listed using:
modutil -dbdir /etc/opt/SUNWportal/cert/gateway-profile-name -list);
Otherwise, just hit Return below.
Please enter the token name. []
Enter the name you like for this certificate?
Enter the validity period for the certificate (months) [6]
A self-signed certificate is generated and the prompt returns.
```

記號名稱 (預設空白) 和憑證名稱儲存於 `/etc/opt/SUNWportal/cert/`*gateway-profile-name* 之下的 `.nickname` 檔案中。

4. **重新啓動憑證以使閘道生效：**

```
./psadmin start-sra-instance -u amadmin -f passwordfile -N profilename -t gateway
```

# 產生憑證簽署請求 (CSR)

可以從 CA 訂製憑證之前，您需要產生包含 CA 所需要資訊的憑證簽署要求。

## ▼ 產生 CSR

1. **以超級使用者身份執行 `certadmin` 程序檔：**

```
portal-server-install-root/SUNWportal/bin/certadmin -n gateway-profile-name
```

系統便會顯示憑證管理功能表。

```
1) Generate Self-Signed Certificate
2) Generate Certificate Signing Request (CSR)
```

```
3) Add Root CA Certificate
4) Install Certificate From Certificate Authority (CA)
5) Delete Certificate
6) Modify Trust Attributes of Certificate (e.g., for PDC)
7) List Root CA Certificates
8) List All Certificates
9) Print Certificate Content
10) Quit
choice: [10]
2
```

**2 在憑證管理功能表上選擇選項 2。**

程序檔提示您輸入組織特定的資訊、記號名稱和網路管理員電子郵件及電話號碼。

請指定主機的完整合格 DNS 名稱。

```
What is the fully-qualified DNS name of this host? [snape.sesta.com]
What is the name of your organization (ex: Company)? []
What is the name of your organizational unit (ex: division)? []
What is the name of your City or Locality? []
What is the name (no abbreviation please) of your State or Province? []
What is the two-letter country code for this unit? []
Token name is needed only if you are not using the default internal
(software) cryptographic module,
for example, if you want to use a crypto card
(Token names could be listed using:
modutil -dbdir /etc/opt/SUNWportal/cert -list);
Otherwise, just hit Return below.
Please enter the token name []
Now input some contact information for
the webmaster of the machine that the certificate
is to be generated for.
What is the email address of the admin/webmaster for this server [] ?
What is the phone number of the admin/webmaster for this server [] ?
```

**3 輸入所有需要的資訊。**

---

**備註 –** 請務必填寫網路管理員電子郵件和電話號碼。爲了獲得有效的 CSR，必須填寫這兩項資訊。

---

CSR 會產生並儲存於 *portal-server-install-root* `/SUNWportal/bin/csr.hostname.datetimestamp` 檔案中。CSR 同時會列印於螢幕上。當您從 CA 訂製憑證時，可以直接複製並貼上 CSR。

# 新增根 CA 憑證

若用戶端網站提交的憑證由閘道憑證資料庫中不包含的 CA 所簽署，則 SSL 訊號交換模式將會失敗。

要避免這種情況，您需要新增根 CA 憑證到憑證資料庫。這項動作可以確保 CA 變成閘道所知的 CA。

瀏覽至 CA 的網站並獲得此 CA 的根憑證。當您使用 `certadmin` 程序檔時，請指定根 CA 憑證的檔案名稱和路徑。

## ▼ 新增根 CA 憑證

1 **以超級使用者身份執行 `certadmin` 程序檔。**

*portal-server-install-root*`/SUNWportal/bin/certadmin -n` *gateway-profile-name*

系統便會顯示憑證管理功能表。

```
1) Generate Self-Signed Certificate
2) Generate Certificate Signing Request (CSR)
3) Add Root CA Certificate
4) Install Certificate From Certificate Authority (CA)
5) Delete Certificate
6) Modify Trust Attributes of Certificate (e.g., for PDC)
7) List Root CA Certificates
8) List All Certificates
9) Print Certificate Content
10) Quit
choice: [10]
3
```

2 **在憑證管理功能表上選擇選項 3。**

3 **輸入包含根憑證的檔案名稱並輸入憑證名稱。**

根 CA 憑證將會新增至憑證資料庫。

# 安裝來自憑證授權單位的 SSL 憑證

閘道安裝期間，依預設系統會建立自簽憑證並安裝。在安裝之後的任何時間，您都可以安裝由供應商或由您公司的 CA 提供簽署的 SSL 憑證，其中這些供應商會提供正式的憑證授權單位 (CA) 服務。

這項工作包含的三個步驟爲：

- 第 194 頁的 「產生憑證簽署請求 (CSR)」

- 第 197 頁的 「從 CA 訂製憑證」
- 第 197 頁的 「安裝來自 CA 的憑證」


## 從 CA 訂製憑證

產生憑證簽署要求 (CSR) 之後，您需要使用 CSR 從 CA 訂製憑證。

### ▼ 從 CA 訂製憑證

1. **請至憑證授權單位的網站並訂製您的憑證。**

2. **提供 CA 所要求的 CSR。若 CA 要求請提供其他資訊。**

   您將會收到 CA 簽署的憑證。請將它儲存在檔案中。檔案中憑證內容前後請包含 "BEGIN CERTIFICATE" 和 "END CERTIFICATE" 兩行。

   下面的範例省略了實際的憑證資料。

```
-----BEGIN CERTIFICATE-----
The certificate contents...
----END CERTIFICATE-----
```

## 安裝來自 CA 的憑證

使用 `certadmin` 程序檔，將您從 CA 獲得的憑證安裝在本機資料庫檔案中，路徑是 `/etc/opt/SUNWportal/cert/` *gateway-profile-name*。

### ▼ 安裝來自 CA 的憑證

1. **以超級使用者身份執行 `certadmin` 程序檔。**

   *portal-server-install-root*`/SUNWportal/bin/certadmin -n` *gateway-profile-name*

   系統便會顯示憑證管理功能表。

```
1) Generate Self-Signed Certificate
2) Generate Certificate Signing Request (CSR)
3) Add Root CA Certificate
4) Install Certificate From Certificate Authority (CA)
5) Delete Certificate
6) Modify Trust Attributes of Certificate (e.g., for PDC)
7) List Root CA Certificates
8) List All Certificates
9) Print Certificate Content
10)Quit
choice: [10]
4
```

2. **在憑證管理功能表上選擇選項 4。**

   程序檔會讓您輸入憑證檔案名稱、憑證名稱和記號名稱。

   ```
   What is the name (including path) of file that contains the certificate?
   Please enter the token name you used when creating CSR for this certificate. []
   ```

3. **提供所有需要的資訊。**

   憑證安裝於 `/etc/opt/SUNWportal/cert/`*gateway-profile-name*，而且系統會傳回螢幕提示。

4. **重新啓動憑證以使閘道生效：**

   ```
   ./psadmin start-sra-instance -u amadmin -f passwordfile -N profilename -t gateway
   ```

# 刪除憑證

您可以使用憑證管理程序檔刪除憑證。

## ▼ 刪除憑證

1. **以超級使用者身份執行 `certadmin` 程序檔。**

   *portal-server-install-root*`/SUNWportal/bin/certadmin -n`

   其中 *gateway-profile-name* 是閘道實例的名稱。

   系統便會顯示憑證管理功能表。

   ```
   1) Generate Self-Signed Certificate
   2) Generate Certificate Signing Request (CSR)
   3) Add Root CA Certificate
   4) Install Certificate From Certificate Authority (CA)
   5) Delete Certificate
   6) Modify Trust Attributes of Certificate (e.g., for PDC)
   7) List Root CA Certificates
   8) List All Certificates
   9) Print Certificate Content
   10)Quit
   choice: [10]
   5
   ```

2. **在憑證管理功能表上選擇選項 5。**

3. **輸入要刪除的憑證名稱。**

# 修改憑證的信任屬性

若用戶端認證與閘道一起使用，憑證信任屬性則需要修改。其中一個用戶端認證範例爲 PDC (個人數位憑證)。核發 PDC 的 CA 必須受閘道所信任，其中 CA 憑證的 SSL 標記必須爲 "T"。

若閘道設爲與 HTTPS 網站通訊，HTTPS 網站伺服器憑證的 CA 必須受閘道所信任，而且 CA 憑證的 SSL 標記必須爲 "C"。

## ▼ 修改憑證的信任屬性

**1 以超級使用者身份執行 `certadmin` 程序檔。**

*gateway-install-root*`/SUNWportal/bin/certadmin -n` *gateway-profile-name*

其中 *gateway-profile-name* 是閘道實例的名稱。

系統便會顯示憑證管理功能表。

```
1) Generate Self-Signed Certificate
2) Generate Certificate Signing Request (CSR)
3) Add Root CA Certificate
4) Install Certificate From Certificate Authority (CA)
5) Delete Certificate
6) Modify Trust Attributes of Certificate (e.g., for PDC)
7) List Root CA Certificates
8) List All Certificates
9) Print Certificate Content
10)Quit
choice: [10]
6
```

**2 在憑證管理功能表上選擇選項 6。**

**3 輸入憑證名稱。例如：Thawte Personal Freemail CA。**

```
Please enter the name of the certificate?
Thawte Personal Freemail CA
```

**4 輸入憑證的信任屬性。**

```
Please enter the trust attribute you want the
certificate to have [CT,CT,CT]
```

系統將會變更憑證信任屬性。

# 列示根 CA 憑證

您可以使用憑證管理程序檔檢視所有根 CA 憑證。

## ▼ 檢視根 CA 清單

1 **以超級使用者身份執行 certadmin 程序檔。**

*portal-server-install-root*/SUNWportal/bin/certadmin -n *gateway-profile-name*

其中 *gateway-profile-name* 是閘道實例的名稱。

系統便會顯示憑證管理功能表。

```
1) Generate Self-Signed Certificate
2) Generate Certificate Signing Request (CSR)
3) Add Root CA Certificate
4) Install Certificate From Certificate Authority (CA)
5) Delete Certificate
6) Modify Trust Attributes of Certificate (e.g., for PDC)
7) List Root CA Certificates
8) List All Certificates
9) Print Certificate Content
10)Quit
choice: [10]
7
```

2 **在憑證管理功能表上選擇選項 7。**

系統會顯示所有根 CA 憑證。

# 列示所有憑證

您可以使用憑證管理程序檔檢視所有憑證及其對應的信任屬性。

## ▼ 列示所有憑證

1 **以超級使用者身份執行 certadmin 程序檔。**

*portal-server-install-root*
/SUNWportal/bin/certadmin -n
*gateway-profile-name*

其中 *gateway-profile-name* 是閘道實例的名稱。

系統便會顯示憑證管理功能表。

```
1) Generate Self-Signed Certificate
2) Generate Certificate Signing Request (CSR)
3) Add Root CA Certificate
4) Install Certificate From Certificate Authority (CA)
5) Delete Certificate
6) Modify Trust Attributes of Certificate (e.g., for PDC)
7) List Root CA Certificates
8) List All Certificates
9) Print Certificate Content
10)Quit
choice: [10]
8
```

**2 在憑證管理功能表上選擇選項 8。**

系統會顯示所有 CA 憑證。

# 列印憑證

您可以使用憑證管理程序檔列印憑證。

## ▼ 列印憑證

**1 以超級使用者身份執行 certadmin 程序檔。**

*portal-server-install-root*/SUNWportal/bin/certadmin -n *gateway-profile-name*

其中 *gateway-profile-name* 是閘道實例的名稱。

系統便會顯示憑證管理功能表。

```
1) Generate Self-Signed Certificate
2) Generate Certificate Signing Request (CSR)
3) Add Root CA Certificate
4) Install Certificate From Certificate Authority (CA)
5) Delete Certificate
6) Modify Trust Attributes of Certificate (e.g., for PDC)
7) List Root CA Certificates
8) List All Certificates
9) Print Certificate Content
10)Quit
choice: [10]
9
```

**2 在憑證管理功能表上選擇選項 9。**

3 輸入憑證名稱。

◆ ◆ ◆ 第 11 章

# 11 配置 Netlet

本章節說明如何透過 Sun Java System Portal Server 管理主控台配置 Netlet 屬性。可以在組織層級進行配置的所有屬性也可以在使用者層級進行配置。如需有關組織、角色與使用者層級屬性的詳細資訊，請參閱「Access Manager 管理指南」。

本章包含下列各節：


- 第 203 頁的「配置 Netlet 屬性」
- 第 207 頁的「Netlet 代理伺服器配置」


## 配置 Netlet 屬性

您可執行下列作業來配置 Netlet：


- 第 203 頁的「配置基本屬性」
- 第 204 頁的「配置進階屬性」
- 第 205 頁的「建立、修改或刪除 Netlet 規則」


### ▼ 配置基本屬性

1. **以管理員身份登入 Portal Server 管理主控台。**
2. **選取 [Secure Remote Access] 標籤並選取 [Netlet] 標籤。**
3. **從 [選取 DN] 清單選取使用者或組織的 DN，或新增 DN。**
4. **修改下列屬性：**

| 屬性名稱 | 描述 |
| --- | --- |
| COS 優先順序 | 指定要用來決定屬性值繼承的值。如需有關此屬性的詳細資訊，請參閱「Sun Java System Directory Server 管理指南」。 |
| 啓動使用 Netlet | 選取 Java Webstart 或 Applet 選項模式來啓動 Netlet 服務。 |
| 預設回送連接埠 | 指定經由 Netlet 下載 Applet 時，在本機上使用的連接埠。將使用預設值 58000，除非值在 Netlet 規則中被置換。<br>輸入需要的連接埠號。 |
| 保持使用中的間隔 (秒) | 如果用戶端透過 Web 代理伺服器連線到閘道，閒置的 Netlet 連線會因爲代理伺服器逾時而中斷。要防止發生這種情況，請輸入小於代理伺服器逾時的值。 |

5 **按一下 [儲存] 完成作業。**

## ▼ 配置進階屬性

1 **以管理員身份登入 Portal Server 管理主控台。**

2 **選取 [Secure Remote Access] 標籤並選取 [Netlet] 標籤。**

3 **從 [選取 DN] 清單選取使用者或組織的 DN，或新增 DN。**

4 **修改下列屬性：**

| 屬性名稱 | 描述 |
| --- | --- |
| 在門戶網站登出時終止 Netlet | 選取 [是] 確保在使用者登出 Portal Server 時終止所有連線。這可確保取得較大的安全性。根據預設，會選取此選項。<br>選取 [否] 以確保即使在使用者登出 Portal Server 桌面之後，使用中的 Netlet 連線仍在作用中。<br>**備註 –** 當選取 [否] 選項時，不允許使用者在登出 Portal Server 後，建立新 Netlet 連線。僅會保留現有連線。 |
| 連線時重新認證 | 選取 [是] 指定經由 Netlet 下載 Applet 時，在本機上使用的連接埠。預設值是 58000，除非值在 Netlet 規則中被置換。根據預設，會選取 [否] 選項。 |
| 連線時顯示快顯式警告 | 選取 [是]，則當其他使用者正嘗試透過偵聽連接埠連線至 Netlet，並且使用者正在使用 Netlet 執行應用程式時，會在使用者桌面上顯示一個快顯式警告對話方塊。根據預設，會選取 [是] 選項。 |

| 屬性名稱 | 描述 |
| --- | --- |
| 在連接埠警告對話方塊中顯示核取方塊 | 選取 [是]，則當 Netlet 嘗試透過本機中可自由使用的連接埠連線至目標主機時 (如果它是在管理主控台中啓用)，會在使用者桌面中顯示快顯式警告對話方塊。根據預設，會選取 [是] 選項。 |
| Netlet 規則 | 在全域層級建立 Netlet 規則。您所建立的任何新組織都會繼承這些規則。如需建立、修改與刪除 Netlet 規則的詳細資訊，請參閱第 205 頁的 「建立、修改或刪除 Netlet 規則」 |
| 預設原生 VM 加密 | 從下拉式方塊選取 Netlet 規則的預設加密法。如果現有規則未將加密法包括成爲規則的一部分，當您在使用現有規則時，這個選項就非常有用。如需詳細資訊，請參閱第 137 頁的 「向下相容性」一節。 |
| 預設 Java 外掛程式加密 | 從下拉式方塊中選取預設 Java 外掛程式加密。請參閱第 137 頁的 「支援的密碼」以取得支援的加密法清單。 |
| 允許的/拒絕的主機 | 選取主機位址核取方塊，並選取主機以允許根據使用者或組織類型存取，並從下拉式方塊選取 [允許] 或 [拒絕] 選項。 新增新主機：<br>a. 按一下 [新增列]。<br>b. 輸入以指定完整合格主機位址，例如：要指定 `abc`，請輸入 `abc.sesta.com`。<br>**備註 –** 刪除現有的主機：從 [主機] 清單中，選取主機並按一下 [刪除]。<br>您可針對某些組織、角色或使用者定義存取或拒絕特定主機。例如，您可以設定含有五個主機的 [允許] 清單，使用者可遠端登入這五個主機。您可以拒絕對組織內特定主機的存取。爲每個規則指定唯一的**本機連接埠**。<br>**備註 –** 此欄位中的星號 (*) 表示此指定網域的所有主機皆爲可存取。例如，若您指定 `*.sesta.com`，則 `sesta.com` 網域中的所有 Netlet 目標將可由使用者執行。您也可以指定萬有字元的 IP 位址，例如 `xx.xxx.xxx.*`。 |
| 存取/拒絕 Netlet 規則 | 選取 Nelet 規則，並從下拉式方塊選取 [允許] 或 [拒絕] 選項。<br>您可以定義某些組織、角色或使用者對特定 Netlet 規則的存取。<br>您可以拒絕某些組織、角色或使用者對特定 Netlet 規則的存取。<br>**備註 –** 此欄位值如果爲星號 (*) 表示所有已定義的 Netlet 規則皆可用於已選的組織。 |

5 **按一下 [儲存] 完成作業。**

## ▼ 建立、修改或刪除 Netlet 規則

您也可以在組織、角色或使用者層級中建立新的規則或修改現有規則。您所建立的任何新組織都會繼承這些規則。

1 **以管理員身份登入 Portal Server 管理主控台。**

2. **選取 [Secure Remote Access] 標籤並選取 [Netlet] 標籤。**

3. **從 [選取 DN] 清單選取使用者或組織的 DN，或新增 DN。**

4. **在 [進階] > [Netlet 規則] 下，按一下 [新增規則]。**

   - **要刪除規則，請選取規則並按一下 [刪除]。**
   - **要修改規則，請按一下規則名稱。**
     在 Netlet 頁面中，按照下述步驟來修改參數。

5. **在 [規則名稱] 欄位中輸入規則名稱。**

6. **從可用加密法清單中選取 [其他]，並在 [加密密碼] 清單下，選取一或多個加密密碼或選取 [預設值] 來保留預設加密密碼。**
   如果現有規則未將加密法包括成爲規則的一部分，當您在使用現有規則時，這個選項就非常有用。如需資訊，請參閱「向下相容性」一節。如需加密法的詳細資訊，請參閱「指定預設加密密碼」。

7. **在 [遠端應用程式 URL] 欄位中輸入要呼叫的應用程式的 URL。**

8. **若需要下載 applet，則選取 [用戶端連接埠] 核取方塊。請在 [用戶端連接埠]、[伺服器主機] 與 [伺服器連接埠] 欄位中，輸入用戶端連接埠號碼、伺服器主機位址與伺服器連接埠號碼。為每個規則指定唯一的本機連接埠。**
   根據預設，會停用 [啓用下載 Applet] 方塊。只有在 applet 需要從 Portal Server 主機之外的主機下載時，才指定 applet 詳細資訊。如需詳細資訊，請參閱第 132 頁的 「從遠端主機下載 Applet」。

9. **選取 [啓用延伸階段作業] 核取方塊確保當與此規則相對應的 Netlet 階段作業在執行時，Portal Server 階段作業時間將會延長。**

10. **在 [將本機連接埠對映至目標伺服器連接埠] 下，依照下列步驟執行：**

    a. **在本機連接埠欄位中輸入 Netlet 偵聽的本機連接埠。**
       對於 FTP 規則，本機連接埠值必須爲 30021。

    b. **在 [目標主機] 欄位中輸入項目。**
       對於靜態規則，請輸入用於 Netlet 連線的目標機器之主機名稱。對於動態規則，請輸入 "TARGET"。

    c. **在 [目標連接埠] 欄位中輸入目標主機的連接埠。**

11 **按一下 [儲存] 完成作業。**

會在 Netlet 首頁上顯示規則名稱。

# Netlet 代理伺服器配置

在使用者層級還可以配置下列屬性：

- 瀏覽器代理伺服器類型
- 瀏覽器代理伺服器主機
- 瀏覽器代理伺服器連接埠
- 瀏覽器代理伺服器置換清單

如果您未在管理主控台中指定這些值，而且 Netlet 無法確定瀏覽器代理伺服器設定，當使用者透過 Netlet 初次建立連線時，系統將會詢問此資訊。使用者將會儲存此資訊並作爲未來連線之用。

Netlet 無法確定下列方案中的瀏覽器代理伺服器設定：

- 使用者擁有 Internet Explorer 4.x、5.x 或 6.x 以及 Java 外掛程式(1.4.0 之前的版本)，已經在 Java 外掛程式控制台的 [代理程式] 標籤中啓用 [使用瀏覽器設定] 選項，並且已經在 Internet Explorer 的 [本地區域網路設定] 對話方塊中的 [使用自動配置程序檔] 欄位中指定了附加產品或 INS 檔案。
- 使用者安裝了 Netscape 6.2 與 Java 外掛程式(1.3.1_01 或更新的版本) 並且已經在 Java 外掛程式控制台的 [代理程式] 標籤中啓用 [使用瀏覽器設定] 選項。

在上面兩種情況中，Netlet 無法確定瀏覽器設定，因此系統會要求使用者提供下列資訊：

- 瀏覽器代理伺服器類型

  此屬性值可以是 DIRECT 或 MANUAL。如果使用者從下拉清單中選擇 DIRECT，Netlet 將會直接與閘道主機連接。

- 瀏覽器代理伺服器主機

  指定需要的代理伺服器主機，Netlet 需要透過此主機進行連接。

- 瀏覽器代理伺服器連接埠

  指定代理伺服器主機上的連接埠，Netlet 需要透過此連接埠進行連接。

- 瀏覽器代理伺服器置換清單 (以逗號分隔)

  指定您不希望 Netlet 透過代理伺服器連接的主機。此清單可以包含多個以逗號分隔的主機名稱。

◆ ◆ ◆ 第 12 章

# 12 配置 Netlet 使用私有網域憑證

本章說明如何配置瀏覽器的 Java 外掛程式，以使 Netlet 能夠和 PDC 搭配使用。

**備註 –** 只有包含 JSSE 的 Virtual Machine (VM) 才能搭配使用 Netlet 與 PDC。

## 為 PDC 配置 Netlet

此處爲簡介文字。

### ▼ 為 PDC 配置 Netlet

1. **在 Portal Server 機器上 `/ect/opt/SUNWam/config/AMConfig.properties` 檔案中的任何位置新增 `com.iplanet.authentication.modules.cert.gwAuthEnable=yes`。**
2. **將必要的憑證匯入要啓用 PDC 的閘道的憑證資料庫。**
3. **在閘道機器上匯入根 CA 憑證。**
4. **新增 CA 憑證至您的閘道設定檔。**

   **提示 –** 建立您專屬的閘道設定檔，以測試 PDC。

   執行下列步驟以新增憑證至您的閘道設定檔。

   a. *Gateway Install Directory*`/SUNWportal/bin/certadmin -n gateway profile name`
      會列出 Certadmin 功能表。

   b. **選取選項 3。**

**c. 提供憑證路徑。**
會顯示已新增憑證的訊息。

**5 產生「憑證簽署要求」以提交至 CA。**
執行下列步驟以產生「憑證簽署要求」：

**a.** *Gateway Install Directory*`/SUNWportal/bin/certadmin -n gateway profile name`
會列出 Certadmin 功能表。

**b. 選取選項 2。**

**c. 提供問題的適當答案。**

**d. 將要求儲存成檔案。**

**6 提交「憑證簽署要求」至 CA，並取得核准。**

---

**提示 –** 在 CA 簽署後，儲存憑證簽署回應。

---

**7 匯入 CA 許可的「伺服器憑證」。**
執行下列步驟，以匯入「伺服器憑證」：

**a.** *Gateway Install Directory*`/SUNWportal/bin/certadmin -n gateway profile name`
會列出 Certadmin 功能表。

**b. 選取選項 4。**

**c. 提供包含「伺服器憑證」之檔案的位置。**

**8 將「根 CA」憑證匯入 Portal Server 機器。**

- **對於 Application Server，請使用下列指令以新增** `root-ca` **。**
  `./certutil -A -n rootca -t "TCu,TCu,TCuw" -d /var/opt/SUNWappserver/domains/domain1/config -a -i` *path to root-ca*

◆ ◆ ◆ 第 13 章

# 13 配置 Proxylet

本章說明如何透過 Sun Java System Portal Server 管理主控台配置 Proxylet。

本章包含下列章節：


- 第 211 頁的 「配置 Proxylet 屬性」
- 第 213 頁的 「配置應用程式至入口網站桌面」
- 第 214 頁的 「在 Java Web Start 或 Applet 模式中啓動 Proxylet」


## 配置 Proxylet 屬性

核取 [部署] 選項下的 [自動下載 Proxylet Applet] 核取方塊之後，就可以將 Proxylet 配置爲在使用者登入時自動啓動。當並未選取 [自動下載 Proxylet Applet] 核取方塊時，使用者可以按一下標準入口網站桌面的 Proxylet 通道中的 [啓動 Proxylet] 連結，以便在需要時取得 Proxylet。

### ▼ 配置 Proxylet 屬性

1. **以管理員身份登入 Portal Server 管理主控台。**
2. **選取 [Secure Remote Access] 標籤，然後選取 [Proxylet] 標籤。**
3. **從 [選取 DN] 清單方塊選取適當的 DN，或為特定使用者或組織新增現有的 DN。**
4. **在 Proxylet 網頁下，請依照下列步驟執行：**

| 屬性名稱 | 描述 |
| --- | --- |
| COS 優先順序 | 從選項清單中選取 Proxylet 通訊的服務類別。 |
| 自動下載 Proxylet Applet | 按一下 [是] 自動下載 Proxylet Applet 至用戶端機器。以下是下載 Proxylet Applet 的基本要求：<br>用戶端機器可執行伺服器應用程式<br>用戶端機器的 Java 版本是 1.4 或以上<br>瀏覽器是 IE 6.0 sp2 或 Firefox 2.0<br>正確的瀏覽器權限 |
| 透過 Proxylet 重新整理入口網站 | 如果您想在啓動 Proxylet 後，重新整理入口網站桌面，並讓流量經由 Proxylet，請按一下 [是]。如果同時啓用 [在 Proxylet 啓動後，重新整理入口網站] 與 [自動下載 Proxylet Applet]，[應用程式 Url] 就不會有作用。 |
| 啓動模式 | 選取 Java Web Start 或 Applet。 |
| 預設 Proxylet Applet 連結 IP | 鍵入 Proxylet 連結與偵聽瀏覽器請求的 IP 位址。 |
| 預設 Proxylet Applet 連接埠 | 鍵入 Proxylet 偵聽瀏覽器請求的連接埠號碼。 |
| 自動代理伺服器配置檔案位置 | 鍵入包含代理伺服器設定之配置文件的位置，此設定可來自自動代理伺服器配置 (Proxy Auto Configuration, PAC) 檔案或代理伺服器配置清單。 |

**5 在 [Proxylet 規則] 選項中，依照下列步驟執行：**

**a. 指定要透過 Proxylet 服務啓動的應用程式的規則。**

**b. 按一下 [新增]。**

**c. 在 [網域] 欄位中輸入網域名稱，例如 `www.google.com`。**

**d. 輸入 Proxylet 要處理的網域的主機與對應的連接埠號碼。這可確保 Proxylet 解析 HTTP 請求，並且該請求不透過閘道路由。**

**6 按一下 [儲存] 完成作業。**

# 配置應用程式至入口網站桌面

例如 HTTP、FTP 等請求，都會經由 Proxylet 服務。Proxylet 規則允許管理者指定基於協定、主機或連接埠的網域對映。使用 Proxylet 規則，您可指定自動代理伺服器配置 (Proxy Auto Configuration, PAC) 檔案中的網域和代理伺服器設定。例如，您可以建立規則，使所有 FTP 流量均透過 Netlet 路由，而所有 HTTP 流量則透過 Proxylet 路由。您可配置需要透過 Proxylet 服務提供的預先定義應用程式。可根據使用者或組織的喜好設定來完成。一旦新增應用程式以讓 Proxylet 處理，使用者桌面的管理就會更簡易，並提供更好的效能。

## ▼ 配置應用程式至入口網站桌面

**開始之前**

- 請確定已啓用 Proxylet 選項。如需啓用 Proxylet 的詳細資訊，請參閱「閘道設定檔」一章。

1. **以管理員身份登入 Portal Server 管理主控台。**
2. **選取 [入口網站] 標籤，然後選取要修改的入口網站實例。**
   會顯示 [桌面] 頁面。
3. **從 [選取 DN] 清單方塊選取適當的 DN，或為特定使用者或組織新增現有的 DN。**
4. **按一下 [管理容器與通道] 連結。**
   會顯示 [管理容器與通道] 頁面。
5. **從左窗格中選取 Proxylet。**
6. **從右窗格中選取 `Appurls` 連結。**
7. **在 [特性] 精靈中，輸入應用程式名稱與值。依需要修改應用程式特性。例如，輸入應用程式的適當名稱，以及 http://www.example.com。**
8. **按一下 [關閉] 完成。**
   現在，使用者或在組織層級都可檢視入口網站桌面上的應用程式連結。

# 在 Java Web Start 或 Applet 模式中啓動 Proxylet

您可從入口網站桌面上於 Java Web Start 或 Applet 模式中啓動 Proxylet。

## ▼ 在 Java Web Start 或 Applet 模式中啓動 Proxylet

1. **以 Proxylet 使用者身份登入入口網站桌面。**
2. **在首頁中，轉至 Proxylet 通道，並按一下 [編輯] 圖示。**
3. **從 [啓動模式] 清單方塊中，選取 [Java Web Start] 或 [Applet] 選項。**
4. **按一下 [已完成]。**

   要呼叫 Proxylet，請從 [Proxylet 通道] 選取應用程式。這會在 Java Web Start 或 Applet 模式中啓動應用程式。

   - 如果已選取 [自動下載]，按一下 Proxylet 通道下的應用程式。
   - 根據使用者喜好設定，會根據選擇 Java Web Start 或 Apple 模式，來顯示 Proxylet 主控台。接受所有憑證，並繼續使用應用程式。

◆ ◆ ◆ 第 14 章

# 配置 NetFile

本章說明如何透過 Sun Java System Portal Server 管理主控台配置 NetFile。

本章包含下列章節：


- 第 215 頁的 「NetFile 配置作業」


## NetFile 配置作業

本節包含下列作業：


- 第 215 頁的 「配置基本選項」
- 第 217 頁的 「配置存取權限」
- 第 217 頁的 「配置主機喜好設定」
- 第 218 頁的 「配置作業喜好設定」
- 第 218 頁的 「配置作業喜好設定」


### ▼ 配置基本選項

1. **以管理員身份登入 Portal Server 管理主控台。**
2. **選取 [ Secure Remote Access] 標籤並選取 [Netfile] 標籤。**
3. **從 [選取 DN] 清單選取使用者或組織的 DN，或新增 DN。**
4. **修改下列屬性：**

| 屬性名稱 | 描述 |
| --- | --- |
| COS 優先順序 | 指定要用來決定屬性值繼承的值。如需有關此屬性的詳細資訊，請參閱「Sun Java System Directory Server 管理指南」。 |
| 網域/主機喜好設定 | 輸入 NetFile 用於連絡允許主機所需要的預設網域。<br>僅在使用者當使用 NetFile 新增主機時未指定完全合格的主機名稱時，這個預設網域值才可用。<br>**備註 –** 請確定 [預設網域] 欄位不是空白，且包含有效的網域名稱。 |
| 預設 WINS/DNS 伺服器 | 輸入 Netfile 用來存取 Microsoft Windows 主機的 WINS/DNS 伺服器主機位址。<br>**備註 –** 使用者可以覆寫這個值，方法是在新增機器時，指定不同值。 |
| 主機偵測順序 | 使用 [上移] 和 [下移] 按鈕以指定主機偵測順序。 |
| 共用主機 | 輸入主機名稱或完整合格名稱，並按一下 [新增]。<br>若您提供的主機名稱與使用者配置的主機名稱相符，則兩個資訊集將會合併且使用者指定的值會覆寫您指定的值。<br>配置所有遠端 NetFile 使用者都可透過 NetFile 使用之主機的清單。 |

**備註 –** 例如，假設您已配置 4 個共用主機 - `sesta`、`siroe`、`florizon` 與 `abc`。使用者配置 3 個主機，其中 2 個是 `sesta` 與 `siroe`。在這類衝突狀況下，使用者指定的值會覆寫管理員指定的值。`florizon` 與 `abc` 也會列示於使用者的 NetFile 中，且使用者可以在那些主機上執行各種不同的作業。即使您在 [拒絕的主機] 清單中列示 `florizon`，`florizon` 也會列示於使用者的 NetFile 中，但不可以對 `florizon` 執行任何作業。

**主機類型** – 若使用者新增的主機已列示於 [共用主機] 清單中，則會優先使用使用者設定。若在此類型中有衝突，則不會爲該使用者新增管理員新增的共用。若使用者與管理員新增相同共用，則此共用將新增，但將優先使用由使用者設定的密碼。

**5 按一下 [儲存] 完成作業。**

## ▼ 配置存取權限

1. 以管理員身份登入 Portal Server 管理主控台。
2. 選取 [ Secure Remote Access] 標籤並選取 [Netfile] 標籤。
3. 從 [選取 DN] 清單選取使用者或組織的 DN，或新增 DN。
4. 按一下 [存取權限] 並修改下列屬性：

| 屬性名稱 | 描述 |
| --- | --- |
| 存取 Windows 主機 | 選取 [允許] 核取方塊，確定使用者擁有對 Windows 主機的存取權。<br>根據預設，會選取 [允許] 核取方塊。 |
| 存取 FTP 主機 | 選取 [允許] 核取方塊，確定使用者擁有對 FTP 主機的存取權。 |
| 存取 NFS 主機 | 選取 [允許] 核取方塊，確定使用者擁有對 NFS 主機的存取權。 |
| 存取 Netware 主機 | 選取 [允許] 核取方塊，確定使用者擁有對 Netware 主機的存取權。 |

5. 按一下 [儲存] 完成作業。

## ▼ 配置主機喜好設定

1. 以管理員身份登入 Portal Server 管理主控台。
2. 選取 [ Secure Remote Access] 標籤並選取 [Netfile] 標籤。
3. 從 [選取 DN] 清單選取使用者或組織的 DN，或新增 DN。
4. 依預設，因為 [允許/拒絕主機] 清單中有 * 項目，允許使用者透過 NetFile 存取所有主機。若您希望變更這種情況，請於清單中移除 * 項目，並僅指定使用者需要透過 NetFile 存取的主機。否則，您可以在此處保留 * 項目，並於 [拒絕的主機] 清單中指定您要拒絕存取的主機。在這個情況中，允許存取所有的主機，[遭拒的主機] 清單中指定的主機除外。

**備註 –** 若您拒絕存取某主機，並且使用者已在 NetFile 視窗中新增這個主機，已拒絕的主機將繼續顯示於使用者的 NetFile 視窗中。但使用者將無法在主機上執行任何作業。在 NetFile Java2 中，拒絕的主機，若顯示於應用程式中，會使用紅十字標識以表示其爲不可存取。若 [允許的主機] 與 [遭拒的主機] 兩個清單皆爲空白，則不允取存取任何主機。

5 **按一下 [儲存] 完成作業。**

## ▼ 配置作業喜好設定

1 **以管理員身份登入 Portal Server 管理主控台。**

2 **選取 [ Secure Remote Access] 標籤並選取 [Netfile] 標籤。**

3 **從 [選取 DN] 清單選取使用者或組織的 DN，或新增 DN。**

4 **修改下列屬性：**

| 屬性名稱 | 描述 |
| --- | --- |
| 預設壓縮類型 | 從下拉式方塊中選取 ZIP 或 GZ，做爲預設的檔案壓縮格式。 |
| 預設壓縮層級 | 從下拉式方塊中，選取預設壓縮層級。預設值是 6。 |
| 暫存目錄位置 | 輸入暫存檔案的位置。若伺服器中未存在指定的暫存目錄，則會建立。<br>某些作業必須要使用暫存目錄，例如郵寄檔案。預設的暫存目錄是 `/tmp`。暫存檔會在需要的作業已完成後刪除。<br>**備註 –** 確保執行 Web 伺服器的 ID (例如 `nobody` 或 `noaccess`) 擁有指定目錄的 `rwx` 權限。還要確保 ID 對於需要的暫時目錄的完整路徑擁有 `rx` 權限。<br>**提示 –** 您可以爲 NetFile 建立單獨的暫存目錄。如果您爲 Portal Server 所有模組指定了共用的暫存目錄，磁碟空間可能很快就會用完。如果暫存目錄已無空間，則 NetFile 中的某些作業 (例如郵寄檔案) 將無法運作。 |

| 屬性名稱 | 描述 |
| --- | --- |
| 檔案上傳限制 (MB) | 在此欄位輸入可上傳檔案大小之最大值。預設值是 5MB。<br>如果上傳的檔案大小超過此處指定的限制，將出現一個錯誤訊息，且無法上傳檔案。若您輸入一個無效的值，NetFile 會將此值重新設定爲預設值。您可以爲不同的使用者指定不同的檔案上傳大小限制。 |
| 搜尋目錄限制 | 輸入在單一搜尋作業中可以搜尋之目錄的最大數。如果有很多使用者同時登入，此項限制將有助於減少網路擁塞並加快存取速度。預設值爲 100。<br>假設使用者有一個名爲 *A* 的目錄。並假設 *A* 有 100 個子目錄。若您指定欲搜尋目錄的最大數目爲 100，此作業將會搜尋整個 A 目錄並停止。此搜尋作業無法繼續搜尋使用者機器中的其他目錄，因爲在 *A* 目錄中已經達到 100 的限制值。已到達累積搜尋限制的搜尋結果會顯示給使用者，並且顯示一個錯誤訊息說明已經超過其搜尋限制。要繼續搜尋，使用者必須手動在下一個目錄中重新啓動搜尋。以深度優先的方式執行搜尋作業。這表示搜尋作業會執行於使用者所選目錄中的所有子目錄，之後再移動至下一個目錄。 |

5 **按一下 [儲存] 完成作業。**

## ▼ 配置作業權限

您可以允許或拒絕使用者在遠端主機上執行下列作業。

1 **以管理員身份登入 Portal Server 管理主控台。**

2 **選取 [ Secure Remote Access] 標籤並選取 [Netfile] 標籤。**

3 **從 [選取 DN] 清單選取使用者或組織的 DN，或新增 DN。**

4 **修改下列屬性：**

| 屬性名稱 | 描述 |
| --- | --- |
| 檔案重新命名 | 選取 [允許] 核取方塊，以讓使用者重新命名檔案。預設會選取此選項。 |
| 檔案/資料夾刪除 | 選取 [允許] 核取方塊，以讓使用者刪除檔案與目錄。預設會選取此選項。 |

| 屬性名稱 | 描述 |
| --- | --- |
| 檔案上傳 | 選取 [允許] 核取方塊，以讓使用者上傳檔案。預設會選取此選項。 |
| 檔案/資料夾下載 | 選取 [允許] 核取方塊，以讓使用者下載檔案或目錄。預設會選取此選項。 |
| 檔案搜尋 | 選取 [允許] 核取方塊，以讓使用者執行檔案搜尋作業。預設會選取此選項。 |
| 檔案郵寄 | 選取 [允許] 核取方塊，以讓使用者存取郵件。預設會選取此選項。 |
| 檔案壓縮 | 選取 [允許] 核取方塊，以讓使用者選擇壓縮類型。預設會選取此選項。 |
| 變更使用者 ID | 選取 [允許] 核取方塊，以讓使用者變更他們的使用者 ID。使用者可使用不同的 ID 連線至使用 NetFile 的主機。<br>在大型組織中，使用者可能有多個使用者 ID。您可能會想限制使用者使用單一使用者 ID。在那種情況下，您可停用 [允許變更使用者 ID] 選項。如此可以避免特定組織中的所有使用者變更他們的使用者 ID，並限制他們必須使用以單一 ID (桌面登入 ID) 透過 NetFile 連接至主機。另一種情況是使用者可能在不同機器上會有不同的登入 ID，在此情況下，您可能希望允許使用者依需要變更 ID。 |
| 變更 Microsoft Windows 網域 | 選取 [允許] 核取方塊，以讓使用者變更預設 Microsoft Windows 網域主機。預設會選取此選項。<br>若使用者指定網域名稱，則需要指定網域的使用者名稱與密碼。若需要使用主機的使用者名稱與密碼，則使用者需要移除 [使用者網域] 名稱欄位中的網域。 |

**備註 –** 當未選取上述任何選項時，則僅會在使用者再次登入 Portal Server 桌面時，變更才會生效。

**5 按一下 [儲存] 完成作業。**

◆ ◆ ◆ 第 15 章

# 15 配置安全套接層加速器

本章說明如何配置 Sun Java System Portal Server Secure Remote Access 的各種加速器。

本章包含下列章節：


- 第 221 頁的 「加速器簡介」
- 第 221 頁的 「Sun Crypto Accelerator 1000」
- 第 224 頁的 「Sun Crypto Accelerator 4000」
- 第 227 頁的 「外部 SSL 裝置與代理伺服器加速器」


## 加速器簡介

外部加速器爲專用的輔助處理器，可完全卸載伺服器中央處理器的安全套接層 (Secure Socket Layer, SSL) 運算資源，從而釋出中央處理器以執行其他工作，並提高 SSL 事務處理的處理速度。

## Sun Crypto Accelerator 1000

Sun™ Crypto Accelerator 1000 (Sun CA1000) 板是小型的 PCI 板，作爲加密輔助處理器提高公開金鑰及對稱式加密的速度。本產品無外部介面。此 PCI 板會透過內部的 PCI 匯流排介面與主機進行通訊。此板的作用是加速電子商務應用程式中針對安全協定的多種計算密集加密演算過程。

許多重要的加密運算功能，如 RSA [7] 與 Triple-DES (3DES) [8] 可從應用程式完全卸載至 Sun CA1000，並以平行的方式執行。如此可釋出中央處理器以執行其他工作，提高 SSL 事務處理的處理速度。

有關詳細步驟，請參閱第 222 頁的 「配置 Crypto Accelerator 1000」。

# 啓用 Crypto Accelerator 1000

請確定已安裝 Portal Server Secure Remote Access 以及閘道伺服器憑證 (自簽或由任何 CA 所核發)。如需詳細資訊，請參閱第 10 章。

第 222 頁的「啓用 Crypto Accelerator 1000」 是一份檢核清單，可協助您在安裝 SSL Accelerator 前追蹤所需資訊，並列出了 Crypto Accelerator 1000 參數與值。

**表 15–1** Crypto Accelerator 1000 安裝檢核清單

| 參數 | 值 |
|---|---|
| SRA 安裝基底目錄 | /opt |
| SRA 憑證資料庫路徑 | /etc/opt/SUNWportal/cert/default |
| SRA 伺服器憑證暱稱 | server-cert |
| 範圍 | sra-keystore |
| 範圍使用者 | crypta |

## ▼ 配置 Crypto Accelerator 1000

1. **請遵照使用者指南中的指示安裝硬體。請參閱：**

   `http://www.sun.com/products-n-solutions/hardware/docs/pdf/816-2450-11.pdf`

2. **請從光碟安裝下列套件。**

   `SUNWcrypm`、`SUNWcrypu`、`SUNWcrysu`、`SUNWdcar`、`SUNWcrypr`、`SUNWcrysl`、`SUNWdcamn`、`SUNWdcav`

3. **安裝下列修補程式。(您可從 `http://sunsolve.sun.com` 取得這些修補程式)**

   110383-01、108528-05、112438-01

4. **請確定您有 `pk12util` 和 `modutil` 兩項工具。**

   這些工具會安裝於 `/usr/sfw/bin` 下。如果在 `/usr/sfw/bin` 目錄中無法找到工具，您需要手動在 Sun Java System 發行媒體中新增 SUNWtlsu 套裝軟體：

   `Solaris_[sparc/x86]/Product/shared_components/`

5. **建立插槽檔案：**

   `vi /etc/opt/SUNWconn/crypto/slots`

   並將 "crypta@sra" 置於檔案中的首位且爲唯一的行。

6 **建立並設定範圍。**

a. **以超級使用者的身份登入。**

b. **鍵入以下指令：**

```
cd /opt/SUNWconn/bin/secadm
```

```
secadm> create realm=sra
```

已成功建立範圍 sra。

7 **建立使用者：**

a. **鍵入並回應以下指令：**

secadm> `set realm=sra`

secadm{srap}> `su`

secadm{root@sra}> `create user=crypta`

Initial password:

Confirm password:

已成功建立使用者 crypta。

8 **以您建立的使用者登入。**

secadm{root@sra}> `login user=crypta`

Password:

secadm{crypta@sra}> `show key`

此使用者無可用的金鑰。

9 **載入 Sun Crypto 模組。**

環境變數 `LD_LIBRARY_PATH` 必須指向 `/usr/lib/mps/secv1/`

輸入：

```
modutil -dbdir /etc/opt/SUNWportal/cert/default -add "Sun Crypto Module"
-libfile /opt/SUNWconn/crypto/lib/libpkcs11.so
```

請利用下列指令確認是否已載入此模組：

```
modutil -list -dbdir /etc/opt/SUNWportal/cert /default
```

10 **將閘道憑證及金鑰匯出至「Sun Crypto 模組」。**

環境變數 `LD_LIBRARY_PATH` 必須指向 `/usr/lib/mps/secv1/`

輸入：

```
pk12util -o servercert.p12 -d /etc/opt/SUNWportal/cert/default -n server-cert
pk12util -i servercert.p12 -d /etc/opt/SUNWportal/cert/default -h "crypta@sra"
```

現在請執行顯示金鑰指令：

```
secadm{crypta@sra}> show key
```

您應可看到此使用者的兩個金鑰。

11 **變更 /etc/opt/SUNWportal/cert/default/.nickname 檔案中的暱稱。**

```
vi /etc/opt/SUNWportal/cert/default/.nickname
```

將 `server-cert` 替換爲 `crypta@sra:server-cert`

12 **啓用加速密碼。**

SUN CA1000 會加速 RSA 的功能，但僅支援 DES 與 3DES 密碼加速。

13 **修改 `/etc/opt/SUNWportal/platform.conf.`*gateway-profile-name* 以啓用加速器：**

```
gateway.enable.accelerator=true
```

14 **從終端機視窗重新啓動閘道：**

```
./psadmin start-sra-instance -u amadmin -f passwordfile -N profilename -t gateway
```

---

**備註 –** 閘道會於連接埠上與單線 ServerSocket (非 SSL) 連結，此連接埠爲閘道設定檔中所提及的 https 連接埠。

在外來用戶端通訊流量上不會進行任何 SSL 加密或解密。加速器會完成上述動作。

在此模式下 PDC 將無法運作。

---

# Sun Crypto Accelerator 4000

Sun™ Crypto Accelerator 4000 板是一個基於乙太網路的十億位元網路介面卡，支援 Sun 伺服器上的 IPsec 及 SSL (對稱與非對稱) 加密硬體加速。

除了作爲處理未加密網路通訊流量的標準十億位元乙太網路介面卡之外，其亦包含加密硬體以提高加密 IPsec 通訊流量的輸送量。

Crypto Accelerator 4000 板可加速硬體及軟體上的加密演算過程。其亦支援 DES 與 3DES 加密的整批資料加密。

有關詳細步驟，請參閱第 225 頁的 「配置 Crypto Accelerator 4000」。

# 啓用 Crypto Accelerator 4000

請確定已安裝 SRA 以及閘道伺服器憑證 (自簽或由任何 CA 所核發)。下列檢核清單可幫助您在安裝 SSL Accelerator 前跟蹤記錄所需資訊。

第 222 頁的「啓用 Crypto Accelerator 1000」 列出 Crypto Accelerator 4000 參數與值。

**表 15–2** Crypto Accelerator 4000 安裝檢核清單

| 參數 | 值 |
|---|---|
| Portal Server Secure Remote Access 安裝基底目錄 | /opt |
| SRA 實例 | default |
| SRA 憑證資料庫路徑 | /etc/opt/SUNWportal/cert/default |
| SRA 伺服器憑證暱稱 | server-cert |
| CA4000 金鑰庫 | srap |
| CA4000 金鑰庫使用者 | crypta |

## ▼ 配置 Crypto Accelerator 4000

1. **請遵照使用者指南中的指示安裝硬體與軟體套件。請參閱：**
   http://www.sun.com/products-n-solutions/hardware/docs/pdf/816-2450-11.pdf

2. **安裝下列修補程式。(您可從 http://sunsolve.sun.com 取得這些修補程式)：** `114795`

3. **請確定您有下列工具：** `certutil`、`pk12util` **與** `modutil`。
   這些工具會安裝在 `/usr/sfw/bin` 目錄下。
   如果在 `/usf/sfw/bin` 目錄中找不到工具，您需要
   從 Sun Java System 發行媒體中手動新增 SUNWtlsu 套裝軟體：
   `Solaris_[sparc/x86]/Product/shared_components/`

4. **初始化此板。**
   執行 `/opt/SUNWconn/bin/vcadm` 工具以初始化 crypto 板並設定下列值。
   初始安全官員姓名：`sec_officer`
   金鑰庫名稱：`sra-keystore`
   在 FIPS 140-2 模式下執行：`No`

5 **建立使用者**。

vcaadm{vca0@localhost, sec_officer}> `create user`

新使用者名稱：`crypta`

輸入新使用者密碼：

Confirm password:

已成功建立使用者 crypta。

6 **將記號對映至金鑰庫**。

```
vi /opt/SUNWconn/cryptov2/tokens
```

將 `sra-keystore` 附加至檔案。

7 **啓用整批資料加密**。

```
touch /opt/SUNWconn/cryptov2/sslreg
```

8 **載入 Sun Crypto 模組**。

環境變數 `LD_LIBRARY_PATH` 必須指向 `/usr/lib/mps/secv1/`

輸入：

```
modutil -dbdir /etc/opt/SUNWportal/cert/default -add "Sun Crypto Module"
-libfile /opt/SUNWconn/cryptov2/lib/libvpkcs11.so
```

您可利用下列指令確認是否已載入此模組：

```
modutil -list -dbdir /etc/opt/SUNWportal/cert/default
```

9 **將閘道憑證及金鑰匯出至「Sun Crypto 模組」**。

環境變數 `LD_LIBRARY_PATH` 必須指向 `/usr/lib/mps/secv1/`

```
pk12util -o servercert.p12 -d /etc/opt/SUNWportal/cert/default -n server-cert
```

```
pk12util -i servercert.p12 -d /etc/opt/SUNWportal/cert/default -h "sra-keystore"
```

您可利用下列指令確認是否已匯出此金鑰：

```
certutil -K -h "sra-keystore" -d /etc/opt/SUNWportal/cert/default
```

10 **變更 `/etc/opt/SUNWportal/cert/default/.nickname` 檔案中的暱稱**：

```
vi /etc/opt/SUNWportal/cert/default/.nickname
```

將 `server-cert` 替換爲 `sra-keystore:server-cert`

11 **啓用加速密碼**。

**12 從終端機視窗重新啓動閘道：**

```
./psadmin start-sra-instance -u amadmin -f passwordfile -N profilename -t gateway
```

閘道會提示您輸入金鑰庫密碼。

輸入密碼或 "sra-keystore":crypta:crytpa-password 的個人識別碼

---

**備註 –** 閘道會於連接埠上與單線 ServerSocket (非 SSL) 連結，此連接埠爲閘道設定檔中所提及的 https 連接埠。

在外來用戶端通訊流量上不會進行任何 SSL 加密或解密。加速器會完成上述動作。

在此模式下 PDC 將無法運作。

---

# 外部 SSL 裝置與代理伺服器加速器

在開放模式下，外部 SSL 裝置可在 Portal Server Secure Remote Access (SRA) 之前執行。其提供用戶端與 SRA 之間的 SSL 連結。

可執行下列作業：

- 第 227 頁的 「啓用外部 SSL 裝置加速器」
- 第 228 頁的 「配置外部 SSL 裝置加速器」

## ▼ 啓用外部 SSL 裝置加速器

**1 請確定已安裝 SRA，且已有閘道在開放模式 (HTTP 模式) 下執行。**

**2 啓用 HTTP 連線。**

下表列出外部 SSL 裝置與代理伺服器加速器的參數與值。

| 參數 | 值 |
|---|---|
| SRA 實例 | default |
| 閘道模式 | http |
| 閘道連接埠 | 880 |
| 外部裝置/代理伺服器連接埠 | 443 |

## ▼ 配置外部 SSL 裝置加速器

1. **請遵照使用者指南中的指示安裝硬體與軟體套件。**
2. **請安裝必需安裝的修補程式 (若有)。**
3. **配置閘道實例以使用 HTTP。**
4. **請在 `platform.conf` 檔案中輸入下列值：**

   ```
   gateway.enable.customurl=true

   gateway.enable.accelerator=true

   gateway.httpurl=https:// external-device-URL:port-number
   ```

5. **有兩種方式可配置閘道通知：**
   - 當 Access Manager 可於 880 連接埠聯繫閘道機器時 (階段作業通知將會使用 HTTP 方式)，請在 `platform.conf` 檔案中輸入值。

     ```
     vi /etc/opt/SUNWportal/platform.conf.default

     gateway.protocol=http

     gateway.port=880
     ```

     - 當 Access Manager 可於 443 連接埠聯繫外部裝置/代理伺服器時 (階段作業通知將會使用 HTTPS 方式)，請在 `platform.conf` 檔案中輸入值。

       ```
       vi /etc/opt/SUNWportal/platform.conf.default

       gateway.host=External Device/Proxy Host Name

       gateway.protocol=https

       gateway.port=443
       ```

6. **請確定已開啓並執行 SSL 裝置/代理伺服器，且已配置為將通訊流量導向閘道連接埠。**
7. **從終端機視窗重新啓動閘道：**

   ```
   ./psadmin start-sra-instance -u amadmin -f passwordfile -N profilename -t gateway
   ```

第 3 部分

# 管理 Secure Remote Access 伺服器

Secure Remote Access 伺服器有兩種管理介面：

- Portal Server 管理主控台
- 「Sun Java System Portal Server 7.2 Command-Line Reference」第 1 章「psadmin Utility」中介紹的指令行公用程式

大部分的管理作業，都是透過網路式 Portal Server 管理主控台執行，使用者可以透過 Web 瀏覽器從本機或遠端存取該主控台。如需詳細資訊，請參閱「Sun Java System Portal Server 7.2 管理指南」中的「使用 Portal Server 管理主控台」。

然而，例如修改檔案的作業必須經由 UNIX 指令行介面管理。


- 第 16 章
- 第 17 章

◆ ◆ ◆ 第 16 章

# 管理閘道

此處介紹重要內容

## 管理閘道的工作

本節包含下列管理入口網站伺服器閘道的作業：


- 第 231 頁的 「建立閘道設定檔」
- 第 232 頁的 「使用相同的 LDAP 建立閘道實例」


### ▼ 建立閘道設定檔

1. **以管理員身份登入 Portal Server 管理主控台。**

2. **按一下 [Secure Remote Access] 標籤並按一下 [新建設定檔]。**
   會顯示 [新建設定檔] 頁面。

3. **輸入新閘道設定檔名稱。**

4. **選取欲使用的設定檔，以在下拉式清單中建立新設定檔。**
   在預設情況下，您建立的任何新設定檔都是以預先封裝的預設設定檔爲基礎。如果您已經建立自訂的設定檔，則可以從下拉清單中選擇該設定檔。新的設定檔會繼承所選設定檔的所有屬性。

   爲新設定檔複製現有設定檔也會複製相同的連接埠。請變更新設定檔的連接埠，這樣才不會與現有設定檔的連接埠衝突。

5. **按一下 [確定]。**
   現在已建立新設定檔，並列於 [設定檔] 頁面。

**注意 –** 請確定變更了實例的連接埠，這樣就不會與使用中的現有連接埠相衝突。

6. **使用 Telnet 登入需要建立實例的電腦。預設閘道實例已啓動，並在此電腦上執行。**
7. **以立即配置模式安裝 AM-SDK。**
8. **以立即配置模式或選取稍後配置模式，使用 UI 安裝程式安裝閘道。**
9. **將 `/opt/SUNWportal/template/sra/GWConfig.properties.template` 檔案複製至暫存位置。例如，`/tmp`。**
10. **依需要修改值。**

**備註 –** 值應符合新設定檔閘道實例中的連接埠號碼。

11. **一旦完成，就執行下列指令：**

```
./psadmin create-sra-instance -u amadmin -f <passwordfile> -S <template file
location>.template -t gateway
```

12. **請使用新的閘道設定檔名稱重新啓動閘道，確保讓變更生效：**

`./psadmin start-sra-instance –u amadmin – f` *<password file>* `–N` *<profile name>*`– t` *<gateway>*

如需啓動與停止閘道的詳細資訊，請參閱第 233 頁的 「啓動閘道實例」。要配置閘道，請參閱第 8 章

## ▼ 使用相同的 LDAP 建立閘道實例

1. **使用第一個閘道採用的相同字串，替代用來加密與解密密碼的金鑰。**

```
am.encryption.pwd= string_key_specified_in gateway-install
```

2. **替代應用程式認證模組之共用密碼的金鑰：**

```
com.iplanet.am.service.secret= string_key_specified_in gateway-install
```

3. **在 `/etc/opt/SUNWam/config/ums` 中修改 `serverconfig.xml` 的下列區域，使其與 Portal Server 第一個安裝的實例一致：**

```
<DirDN> cn=puser,ou=DSAME Users,dc=sun,dc=net</DirDN>

<DirPassword> string_key_specified_in gateway-install</DirPassword>
```

```
<DirDN>cn=dsameuser,ou=DSAME Users,dc=sun,dc=net</DirDN>

<DirPassword>string_key_specified_in gateway-install </DirPassword>
```

4 **重新啓動 Access Manager 服務**。

## ▼ 啓動閘道實例

在預設情況下，閘道以使用者 noaccess 啓動。

1 **安裝閘道並建立需要的設定檔後，執行下面的指令以啓動閘道：**

`./psadmin start-sra-instance –u amadmin – f <password file> –N <profile name> – t <gateway>`

`default` — 是在安裝時建立的預設閘道設定檔。您可以稍後建立自己的設定檔，並且用新的設定檔重新啓動閘道。請參閱第 32 頁的 「建立閘道設定檔」。

---

**備註 –** 請以適當的設定檔名稱取代 <*profile name*> 以啓動閘道的其他實例。

重新啓動伺服器 (已配置閘道實例於其上的電腦) 會重新啓動閘道的所有實例。

請確定 `/etc/opt/SUNWportal` 目錄中沒有任何備份設定檔。

---

2 **執行下列指令來檢查閘道是否在指定的連接埠上執行：**

`netstat -an | grep` *port-number*

預設的閘道連接埠是 443。

## ▼ 停止閘道

1 **使用下面的指令以停止閘道：**

`./psadmin stop-sra-instance –u amadmin – f <password file> –N <profile name> – t <gateway>`

---

**備註 –** 請以適當的設定檔名稱取代 <*profile name*> 以啓動閘道的其他實例。

---

2 **執行下列指令以驗證是否還有任何閘道程序尚在執行中：**

```
/usr/bin/ps -ef | grep entsys
```

## ▼ 使用管理主控台啟動與停止閘道

1. **登入 Portal Server 管理主控台。**
2. **選取 [Secure Remote Access] 標籤。**
3. **按一下 [管理實例] 子功能表。**
4. **在 [SRA 代理伺服器實例] 下，選取實例。**
   - **按一下 [啓動] 以啓動實例。**
   - **按一下 [停止] 停止實例。**

## ▼ 使用不同的設定檔重新啓動閘道

- **重新啓動閘道：**

  `./psadmin start-sra-instance –u amadmin – f <`*password file*`> –N <`*profile name*`> – t <`*gateway*`>`

## ▼ 重新啓動閘道

- **在終端機視窗中，連線為超級使用者並執行下列動作之一：**
  - 啓動監視程式程序：

    ```
    ./psadmin sra-watchdog -u uid -f password-filename -t instance-type on
    ```

    | | |
    |---|---|
    | `[--adminuser \| -u] uid` | 指定管理者辨別名稱 (DN) 或使用者 ID。 |
    | `[-passwordfile \| -f] password-filename` | 在密碼檔中指定管理員的密碼。 |
    | `[--type \| -t] instance-type` | 指定 Secure Remote Access 實例類型。輸入：gateway、nlproxy 或 rwproxy。 |

    如需監視程式指令的資訊，請參閱「Sun Java System Portal Server Command Line Reference Guid」。

    這會在 crontab 公用程式中建立一個項目，而現在監視程式會啓動。監視程式會監視在特定機器上閘道所有正在執行的實例和閘道連接埠，且如果閘道效能降低會重新啓動閘道。

## ▼ 指定虛擬主機

1 **以超級使用者身份登入並編輯所需閘道實例的** `platform.conf` **檔：**

`/etc/opt/SUNWportal/platform.conf.`*gateway-profile-name*

2 **新增下列項目：**

`gateway.virtualhost=`*fully-qualified-gateway-host gateway-ip-address fully-qualified-reverse-proxyhost*

`gateway.enable.customurl=true` (此值依預設設定爲 false。)。

3 **重新啓動閘道：**

`./psadmin start-sra-instance –u amadmin – f` <*password file*> `–N` <*profile name*>`– t` <*gateway*>

如果不指定這些值，則閘道會預設成一般的運作方式。

## ▼ 指定代理伺服器

1 **從指令行中，編輯下列檔案：**

`/etc/opt/SUNWportal/platform.conf.`*gateway-profile-name*

2 **新增下列項目：**

`http.proxyHost=`*proxy-host*
`http.proxyPort=`*proxy-port*
`http.proxySet=true`

3 **重新啓動閘道，為針對伺服器所提出的請求使用指定的代理伺服器：**

`./psadmin start-sra-instance –u amadmin – f` <*password file*> `–N` <*profile name*>`– t` <*gateway*>

## ▼ 建立 Netlet 代理伺服器實例

1 **使用 Telnet 登入需要建立實例的電腦。預設閘道實例已啓動，並在此電腦上執行。**

2 **將** `/opt/SUNWportal/template/sra/NLPConfig.properties.template` **檔案複製至暫存位置。 例如，**`/tmp`。

3 **依需要在新設定檔的檔案中修改值。**

4. **一旦完成，就執行下列指令：**

   ```
   ./psadmin create-sra-instance -u amadmin -f <passwordfile> -S <template file location>.template -t nlproxy
   ```

5. **請使用要求的閘道設定檔名稱重新啓動 Netlet 伺服器的新實例，以確保變更生效：**

   ```
   ./psadmin start-sra-instance –u amadmin – f <password file> –N <profile name> – t nlproxy
   ```

## ▼ 重新啓動 Netlet 代理伺服器

- **在終端機視窗中，連線為超級使用者並執行下列動作之一：**

  - **啓動監視程式程序：**

    ```
    psadmin sra-watchdog -u uid -f password-filename -t instance-type on
    ```

    輸入 `nlproxy` 以取代 *instance-type*。如需此指令的詳細資訊，請參閱「Sun Java Portal Server Command Line Reference Guid」。

    這會在 crontab 公用程式中建立一個項目，而現在監視程式會啓動。監視程式會監視 Netlet 代理伺服器並在效能降低時啓用代理伺服器。

  - **手動啓動 Netlet 代理伺服器：**

    ```
    psadmin start-sra-instance -u uid -f password-filename -N sra-instance-name -t instance-type
    ```

    輸入 `nlproxy` 以取代 *instance-type*。此設定檔名稱是對應到所需 Netlet 代理伺服器實例。如需此指令的詳細資訊，請參閱「Sun Java Portal Server Command Line Reference Guid」。

## ▼ 建立 Rewriter 代理伺服器實例

1. **使用 Telnet 登入需要建立實例的電腦。預設閘道實例已啓動，並在此電腦上執行。**

2. **將 `/opt/SUNWportal/template/sra/GWConfig.properties.template` 檔案複製至暫存位置。例如，`/tmp`。**

3. **依需要在新設定檔的檔案中修改值。**

4. **一旦完成，就執行下列指令：**

   ```
   ./psadmin create-sra-instance -u amadmin -f <passwordfile> -S <template file location>.template -t rwproxy
   ```

5 **請使用要求的閘道設定檔名稱重新啓動 Rewirter 伺服器的新實例，以確保變更生效：**

`./psadmin start-sra-instance –u amadmin – f <password file> –N <profile name> – t rwproxy`

## ▼ 重新啓動 Rewriter 代理伺服器

- **在終端機視窗中，連線為超級使用者並執行下列動作之一：**
  - **啓動監視程式程序：**

    `psadmin sra-watchdog -u uid -f password-filename -t instance-type on`

    請輸入 `rwproxy` 取代 *instance-type*。如需此指令的詳細資訊，請參閱「Sun Java Portal Server Command Line Reference Guid」。

    這會在 crontab 公用程式中建立一個項目，而現在監視程式會啓動。監視程式會監視 Rewriter 代理伺服器連接埠並在當機時重新啓動。

  - **手動啓動 Rewriter 代理伺服器：**

    `start-sra-instance -u uid -f password-filename -N sra-instance-name -t instance-type`

    輸入 `rwproxy` 取代 *instance-type*。此設定檔是對應到所需 Rewriter 代理伺服器實例。如需此指令的詳細資訊，請參閱「Sun Java Portal Server Command Line Reference Guid」。

## ▼ 啓用反向代理伺服器

1 **以超級使用者身分登入並編輯所需閘道實例的 `platform.conf` 檔：**

`/etc/opt/SUNWportal/platform.conf.` *gateway-profile-name*

2 **新增下列項目：**

`gateway.virtualhost=` *fully-qualified-gateway-host gateway-ip-address fully-qualified-reverse-proxyhost*

`gateway.enable.customurl=true` (此值依預設設定爲 false。)。

`gateway.httpurl=` *http reverse-proxy-URL*

`gateway.httpsurl=`*https reverse-proxy-URL*

`gateway.httpurl` 將用於覆寫在連接埠接收的回應，其中連接埠在閘道設定檔會列示爲 HTTP 連接埠。

`gateway.httpsurl` 將用於覆寫在連接埠接收的回應，其中連接埠在閘道設定檔會列示爲 HTTPS 連接埠。

3 **重新啓動閘道：**

`./psadmin start-sra-instance –u amadmin – f <`*password file*`> –N <`*profile name*`> – t <`*gateway*`>`

如果不指定這些值，則閘道會預設成一般的運作方式。

## ▼ 新增認證模組到現有 PDC 實例

1 **以管理員的身份登入 Access Manager 管理主控台。**

2 **選取需要的組織。**

3 **從 [檢視] 下拉方塊中選取 [服務]。**
會顯示服務。

4 **按一下 [認證配置]。**
顯示 [服務實例清單]。

5 **按一下 [Gatewaypdc]。**
會顯示 Gatewaypdc 特性頁面。

6 **按一下 [編輯]。**
隨即顯示 [新增模組] 頁。

7 **選擇 [模組名稱] 並設定 [旗標] 為 [必要的]。**

8 **按一下 [確定]。**

9 **新增一個或多個模組後按一下 [儲存]。**

10 **在 `gatewaypdc` 特性頁面中按一下 [提交]。**

11 **重新啓動閘道以使變更生效：**

*gateway-install-location*`/SUNWportal/bin/psadmin start-sra-instance –u amadmin – f <`*password file*`> –N <`*profile name*`>– t <`*gateway*`>`

## ▼ 停用瀏覽器快取

1 **以超級使用者身分登入並編輯所需閘道實例的 `platform.conf` 檔：**

`/etc/opt/SUNWportal/platform.conf.`*gateway-profile-name*

2 **編輯下面的行：**

```
gateway.allow.client.caching=true
```

此值依預設設定爲 `true`。變更此值爲 `false` 以停止瀏覽器在用戶端快取。

3 **重新啓動閘道：**

`./psadmin start-sra-instance –u amadmin – f` <*password file*> `–N` <*profile name*> `– t` <*gateway*>

## ▼ 共用 LDAP 目錄

1 **將 `AMConfig.properties` 中的下列區域修改為與最先安裝的 Portal Server 及 Access Manager 伺服器實例相一致：**

# 會使用金鑰來加密和解密密碼。
`am.encryption.pwd=t/vnY9Uqjf12NbFywKuAaaHibwlDFNLO <==` REPLACE THIS STRING WITH THE ONE FROM FIRST PORTAL INSTALL

/* The following key is the shared secret for application auth module */
`com.iplanet.am.service.secret=AQICxIPLNc0WWQRVlYZN0PnKgyvq3gTU8JA9 <==` REPLACE THIS STRING WITH THE ONE FROM FIRST PORTAL INSTALL

2 **在 `/etc/opt/SUNWam/config/ums` 中，將 `serverconfig.xml` 中的下列區域修改為與最先安裝的 Portal Server 及 Access Manager 伺服器實例不一致：**

```
<DirDN>
    cn=puser,ou=DSAME Users,dc=sun,dc=net
</DirDN>
    <DirPassword>
         AQICxIPLNc0WWQT22gQnGgnCp9rUf+FuaqpY
         <==  REPLACE THIS STRING WITH THE ONE FROM FIRST PORTAL INSTALL
  </DirPassword>

<DirDN>
   cn=dsameuser,ou=DSAME Users,dc=sun,dc=net
</DirDN>
     <DirPassword>
          AQICxIPLNc0WWQT22gQnGgnCp9rUf+FuaqpY
          <==  REPLACE THIS STRING WITH THE ONE FROM FIRST PORTAL INSTALL
     </DirPassword>
```

3 重新啓動 Access Manager 服務。

◆ ◆ ◆ 第 17 章

# 17 聯合管理方案

將討論下列主題：


- 第 241 頁的 「使用聯合管理」
- 第 241 頁的 「聯合管理方案」
- 第 242 頁的 「配置聯合管理資源」


## 使用聯合管理

聯合管理能讓使用者聚集他們的本機識別，以使他們有一個網路識別。聯合管理使用網路識別以允許使用者登入一個服務提供者的網站，並且不需要重新認證他們的識別即可存取其他服務提供者的網站。這稱爲單次登入。

在入口伺服器上開啓模式和安全模式配置聯合管理。「Portal Server 管理指南」描述了如何在開放模式中配置聯合管理。於安全模式中使用 Portal Server Secure Remote Access 伺服器配置聯合管理之前，請確保聯合管理可在開啓模式中運作。如果您的使用者要在開啓模式和安全模式中從相同的瀏覽器中使用聯合管理，他們必須清除 cookie 並從瀏覽器進行快取。

如需「聯合管理」的詳細資訊，請參閱「Access Manager 聯合管理指南」。

## 聯合管理方案

使用者認證到一個初始的服務提供者。服務使用者是商業用途或是提供以網路爲主之服務的非營利組織。此廣泛的種類可以包括網際網路入口網站、運輸提供者、金融機構、娛樂事業公司、圖書館、大學和政府行政機構。

服務提供者可以使用 cookie 以儲存使用者在用戶端瀏覽器的階段作業資訊。Cookie 也包含使用者的識別提供者。

識別提供者是在提供認證服務中指定的服務提供者。做爲認證的管理服務，它們同時也維持並管理身份識別資訊。識別提供者所完成的認證受到隸屬於它的所有伺服器提供者所認可。

當使用者程式存取不隸屬於該識別提供者的服務時，此識別提供者會將該 cookie 轉寄給獨立的服務提供者。此服務提供者之後便可存取在 cookie 中呼叫的識別提供者。

然而，無法在不同的 DNS 網域間讀取 cookie。因此使用「共用網域 Cookie 服務」以重新導向服務提供者到正確的識別提供者，因此使用者就可以啓用單次登入。

# 配置聯合管理資源

聯合資源、服務提供者、識別提供者和共同網域 Cookie 服務 (CDCS) 在其所存在的閘道中設定檔中配置。這部分說明如何配置三個方案：

## ▼ 配置聯合管理資源

1. **當所有資源位在企業內部網路時**
2. **當所有資源沒有位於企業內部網路，或識別提供者位於網際網路**
3. **當所有資源沒有位於企業網路，或當企業提供者受到閘道保護，且識別提供者是協力廠商並位於網際網路。**

### 配置 1

在此配置中，服務提供者、識別提供者和「共用網域 Cookie 服務」都部署在相同的企業內部網路中，而識別提供者並未發佈到網際網路網域名稱伺服器 Domain Name Server (DNS) 中。CDCS 爲選填項目。

在此配置中，閘道指向服務提供者，也就是 Portal Server。此配置對 Portal Server 的多重實例都有效。

#### ▼ 配置閘道為服務提供者 (Portal Server)

1. **以管理員身份登入 Portal Server 管理主控台。**
2. **選取 [Secure Remote Access] 標籤，並選取適當的閘道設定檔，以修改其屬性。**
   便會顯示 [編輯閘道設定檔] 頁面。
3. **選取 [核心] 標籤。**

4 選取 [啓用 Cookie 管理] 核取方塊以啓用 cookie 管理。

5 選取 [安全性] 標籤。

6 在 Portal Server 欄位中，輸入 Portal Server 名稱，以使用相對 URL，例如：列於 [未驗證的 URL] 清單中的 /amserver 或 /portal/dt。例如：

http:// *idp-host:port*/amserver/js

http:// *idp-host:port*/amserver/UI/Login

http://*idp-host:port* /amserver/css

http://*idp-host:port* /amserver/SingleSignOnService

http://*idp-host:port*/amserver/UI/blank

http://*idp-host:port* /amserver/postLogin

http:// *idp-host:port*/amserver/login_images

7 在 Portal Server 欄位中輸入 Portal Server 名稱。例如 /amserver。

8 按一下 [儲存]。

9 選取 [安全性] 標籤。

10 在 [未驗證的 URL] 清單中，新增聯合資源。例如：

/amserver/config/federation

/amserver/IntersiteTransferService

/amserver/AssertionConsumerservice

/amserver/fed_images

/amserver/preLogin

/portal/dt

11 按一下 [新增]。

12 按一下 [儲存]。

13 如果需要 Web 代理伺服器以連線至在 [未驗證的 URL] 清單中的 URL，請選取 [部署] 標籤。

14 在 [網域與子網域的代理伺服器] 欄位中，輸入所需的 Web 代理伺服器。

15 按一下 [新增]。

16 按一下 [儲存]。

17 從終端機視窗中，重新啓動閘道：

`./psadmin start-sra-instance –u amadmin – f <password file> –N <profile name>– t <gateway>`

# 配置 2

在此配置中識別提供者、識別提供者和共同網域 Cookie 提供者 (CDCP) 沒有部署於企業內部網路，或識別提供者是位於網際網路上的協力廠商。

在此配置中，閘道指向服務提供者，也就是 Portal Server。此配置對 Portal Server 的多重實例都有效。

## ▼ 配置閘道為服務提供者 (Portal Server)

1 以管理員身份登入 Portal Server 管理主控台。

2 選取 [Secure Remote Access] 標籤，並選取適當的閘道設定檔，以修改其屬性。

3 選取 [核心] 標籤。

4 選取 [啓用 Cookie 管理] 核取方塊以啓用 cookie 管理。

5 在 Portal Servers 欄位中，輸入服務提供者的入口網站伺服器名稱，以使用相對 URL，例如：列於 [未認證 URL] 清單中的 `/amserver` 或 `/portal/dt`。

`http://idp-host:port/amserver/js`

`http://idp-host:port /amserver/UI/Login`

`http://idp-host:port /amserver/css`

`http:// idp-host:port/amserver/SingleSignOnService`

`http://idp-host:port /amserver/UI/blank`

`http://idp-host:port /amserver/postLogin`

`http:// idp-host:port/amserver/login_images`

6 按一下 [儲存]。

7 按一下 [安全性] 標籤。

8 在 [未認證 URL] 清單中，新增聯合資源。例如：

`/amserver/config/federation`

```
/amserver/IntersiteTransferService

/amserver/AssertionConsumerservice

/amserver/fed_images

/amserver/preLogin

/portal/dt
```

9. **按一下 [新增]。**
10. **按一下 [儲存]。**
11. **如果需要 Web 代理伺服器以連線至在 [未驗證的 URL] 清單中的 URL，請選取 [部署] 標籤。**
12. **在 [網域與子網域代理伺服器] 欄位中，輸入 Web 代理伺服器的相關資訊。**
13. **按一下 [新增]。**
14. **按一下 [儲存]。**
15. **從終端機視窗中，重新啓動閘道：**

    `./psadmin start-sra-instance –u amadmin – f` *<password file>* `–N` *<profile name>*`– t` *<gateway>*

## 配置 3

在此配置中識別提供者、識別提供者和共同網域 Cookie 提供者 (CDCP) 沒有部署於企業內部網路，或服務提供者是位於網際網路上的協力廠商，且識別提供者受到閘道保護。

在此配置中，閘道指向識別提供者，也就是 Portal Server。

此配置對 Portal Server 的多重實例都有效。此配置在網路上是不太可能發生的，然而，一些企業網路在其企業內部網路可能會有這樣的配置，也就是說，識別提供者可能位於由防火牆保護的子網路中，而伺服器提供者可以在企業網路中直接存取。

### ▼ 配置閘道至識別提供者 (Portal Server)

1. **以管理員身份登入 Portal Server 管理主控台。**
2. **選取 [Secure Remote Access] 標籤，並選取適當的閘道設定檔，以修改其屬性。**
3. **選取 [核心] 標籤。**

4. 選取 [啓用 Cookie 管理] 核取方塊以啓用 cookie 管理。
5. 在 Portal Servers 欄位中，輸入識別提供者的入口網站伺服器名稱，以使用相對 URL，例如：列於 [未認證 URL] 清單中的 `/amserver` 或 `/portal/dt`。

   `http://`*idp-host:port*`/amserver/js`

   `http://`*idp-host:port* `/amserver/UI/Login`

   `http://`*idp-host:port* `/amserver/css`

   `http://` *idp-host:port*`/amserver/SingleSignOnService`

   `http://`*idp-host:port* `/amserver/UI/blank`

   `http://`*idp-host:port* `/amserver/postLogin`

   `http://` *idp-host:port*`/amserver/login_images`
6. 按一下 [儲存]。
7. 選取 [安全性] 標籤。
8. 在 [未認證 URL] 清單中，新增聯合資源。例如：

   `/amserver/config/federation`

   `/amserver/IntersiteTransferService`

   `/amserver/AssertionConsumerservice`

   `/amserver/fed_images`

   `/amserver/preLogin`

   `/portal/dt`
9. 按一下 [新增]。
10. 按一下 [儲存]。
11. 如果需要 Web 代理伺服器以連線至在 [未驗證的 URL] 清單中的 URL，請選取 [部署] 標籤。
12. 在 [網域與子網域代理伺服器] 欄位中，輸入 Web 代理伺服器的相關資訊。
13. 按一下 [新增]。
14. 按一下 [儲存]。

**15 從終端機視窗中，重新啓動閘道：**

`./psadmin start-sra-instance –u amadmin – f <password file> –N <profile name>– t <gateway>`

◆ ◆ ◆ 附錄 A

# 配置屬性

本附錄說明您可透過每個 Portal Server Secure Remote Access 元件的 Portal Server 管理主控台，爲每個 Sun Java System Portal Server Secure Remote Access 配置的屬性：


- 第 249 頁的 「存取控制服務」
- 第 250 頁的 「閘道服務」
- 第 256 頁的 「NetFile 服務」
- 第 260 頁的 「Netlet 服務」
- 第 261 頁的 「Proxylet 服務」


## 存取控制服務

第 249 頁的 「存取控制服務」會列出存取控制服務屬性。

表 A–1 存取控制服務屬性

| 屬性 | 預設值 | 描述 |
|---|---|---|
| 遭拒的 URL | | 一般使用者無法透過閘道存取的 URL 清單。 |
| 允許的 URL | * | 一般使用者可以透過閘道存取的 URL 清單。 |
| 停用單次登入的主機 | | 停用清單中主機的單次登入功能。 |
| 啓用每個階段作業中的單次登入 | | 啓用階段作業的單次登入功能。 |
| 允許的驗證等級 | * | 表示信任認證的程度。使用星號可允許所有認證等級。有關認證等級的資訊，請參閱「Access Manager 管理指南」。 |

# 閘道服務

當您按一下閘道服務時，右邊的窗格會顯示一個可用來建立新設定檔的按鈕，以及顯示已經建立之所有閘道設定檔的清單。

如果您按一下 [新增]，則下一個窗格將會提示您輸入新的閘道設定檔名稱。您可以選擇使用預設範本或是選擇先前建立的閘道設定檔作爲範本。

如果您在其中一個列出的閘道設定檔名稱上按一下，將會出現一個標籤清單。他們是：


- 第 250 頁的 「核心」
- 第 252 頁的 「代理伺服器」
- 第 252 頁的 「安全性」
- 第 254 頁的 「Rewriter」


## 核心

第 250 頁的 「核心」列出了閘道服務核心屬性。

**表 A–2** 閘道服務核心屬性

| 屬性 | 預設值 | 描述 |
|---|---|---|
| 啓用 HTTPS 連線 | | 啓用 HTTPS 連線。 |
| HTTPS 連接埠 | 443 | 指定 HTTPS 連接埠。 |
| 啓用 HTTP 連線 | * | 啓用 HTTP 連線。 |
| HTTP 連接埠 | 80 | 指定 HTTP 連接埠。 |
| 啓用 Rewriter 代理伺服器 | * | 在閘道和企業內部網路之間實現安全的 HTTP 通訊。Rewriter 代理伺服器及閘道使用相同的閘道設定檔。 |
| Rewriter 代理伺服器清單 | | Rewriter 代理伺服器的清單。對於 Rewriter 代理伺服器的多個實例，請以 *host-name:port* 的格式輸入每一個實例的詳細資訊。 |
| 啓用 Netlet | 已核取 | 確保 TCP/IP (如 Telnet 及 SMTP)、HTTP 應用程式及固定連接埠應用程式的安全性。 |
| 啓用 Proxylet | 已核取 | 啓用在用戶端機器上 Proxylet 的下載。 |

表 A–2 閘道服務核心屬性 *(續)*

| 屬性 | 預設值 | 描述 |
|---|---|---|
| 啓用 Netlet 代理伺服器 | | 藉由透過閘道將安全通道從用戶端延伸到位於企業內部網路的 Netlet 代理伺服器，以強化閘道和企業內部網路之間的 Netlet 通訊流量的安全性。如果您不想在 Portal Server 中使用應用程式，則請停用此選項。 |
| Netlet 代理伺服器主機 | | 列出 Netlet 代理伺服器主機，格式如下：hostname:port |
| 啓用 Cookie 管理 | | 爲允許使用者存取的所有網站追蹤與管理使用者階段作業。(請勿套用至 Portal Server 用來追蹤 Portal Server 使用者階段作業的 Cookie)。 |
| 啓用持續 HTTP 連線 | 已核取 | 在閘道啓用 HTTP 永久性連線，以避免爲網頁中的每個物件 (例如影像與樣式表) 都開啓通訊端。 |
| 每一持續連線的最大請求數 | 10 | 指定每一持續連線的要求數。 |
| 持續通訊端連線的逾時 | 50 | 指定在關閉插槽前需要經過的時間量。 |
| 帳號往返時間的寬限逾時 | 20 | 指定在瀏覽器傳送請求後，請求到閘道的寬限時間量，和閘道傳送回應以及瀏覽器實際收到之間的間隔時間。 |
| 將使用者階段作業 Cookie 轉寄至的 URL | | 讓 servlet 和 CGI 可以收到 Portal Server 的 cookie 並使用 API 來識別使用者。 |
| 最長連線佇列長度 | 50 | 指定閘道可以接受的最大並行運作連線。 |
| 閘道逾時 (秒) | 120 | 指定閘道與瀏覽器的連線逾時前的時間間隔 (單位：秒)。 |
| 最大執行緒儲存區大小 | 200 | 指定可於閘道執行緒池內預先建立的執行緒的最大數。 |
| 快取的通訊端逾時 | 200 | 指定閘道與 Portal Server 的連線逾時前的時間間隔 (單位：秒)。 |
| Portal Server | | 以下列格式指定 Portal Server：`http://` *portal server name:port -number*。閘道會以循環方式嘗試連絡每個列出的 Portal Server 以服務請求。 |
| 伺服器重試間隔 (秒) | 120 | 指定當 Portal Server、Rewriter 代理伺服器或 Netlet 代理伺服器變得無法存取 (例如當機或關機) 之後，嘗試啓動它們之請求之間的時間間隔。 |

表 A–2 閘道服務核心屬性 (續)

| 屬性 | 預設值 | 描述 |
| --- | --- | --- |
| 儲存外部伺服器 Cookie | | 允許閘道儲存與管理可透過閘道存取之任何協力廠商應用程式或是伺服器的 cookie。 |
| 從 URL 取得階段作業資訊 | | 將階段作業資訊編碼爲 URL 的一部分，不論是否支援 cookie。閘道會使用 URL 中找到的階段作業資訊進行驗證，而不是使用用戶端瀏覽器傳送的階段作業 cookie。 |

# 代理伺服器

第 252 頁的 「代理伺服器」列出了閘道服務代理伺服器屬性。

表 A–3 閘道服務代理伺服器屬性

| 屬性 | 預設值 | 描述 |
| --- | --- | --- |
| 使用代理伺服器 | | 使得可以使用 Web 代理伺服器。 |
| 使用網路代理伺服器 URL | | 列出閘道需要連絡的 URL，而連絡僅能透過 [網域和子網域的代理伺服器清單] 中列出的 Web 代理伺服器進行 (即使 [使用代理伺服器] 選項已經停用)。 |
| 請勿使用網路代理伺服器 URL | | 列出閘道可以直接連接的 URL。 |
| 網域與子網域的代理伺服器 | iportal.com<br>sun.com | 指定應該使用哪個代理伺服器以連絡特定網域中的特定子網域。 |
| 代理伺服器密碼清單 | | 指定當代理伺服器需要認證以存取部分或所有網站時，閘道向指定的代理伺服器認證所需的伺服器名稱、使用者名稱及密碼。 |
| 啓用自動代理伺服器配置支援 | | 指定將忽略在 [網域與子網域的代理伺服器] 欄位中提供的資訊。 |
| 自動代理伺服器配置檔案位置 | | 指定用於 PAC 支援的檔案位置。 |
| 透過 Web 代理伺服器啓用 Netlet 通道 | | 透過閘道將安全通道從用戶端延伸至存在於企業內部網路的 Web 代理伺服器。 |

# 安全性

第 252 頁的 「安全性」列出了閘道服務安全性屬性。

**表 A–4** 閘道服務安全性屬性

| 屬性 | 預設值 | 描述 |
|---|---|---|
| 啓用 HTTP 基本認證 | 已核取 | 儲存使用者名稱和密碼，如此當使用者重新造訪有 BASIC 保護的網站時，將不需要重新輸入其憑證。 |
| 未認證的 URL | /portal/desktop/images<br>/amserver/login_images<br>/portal/desktop/css<br>/amserver/jss<br>/amconsole/console/css<br>/portal/searchadmin/console/js<br>/amconsole/con sole/js<br>/amserver/css | 指定不需要任何認證的 URL，例如包含影像的目錄。 |
| 啓用憑證的閘道主機 | | 列出已啓用憑證的閘道主機。 |
| 允許 40 位元加密 | | 允許 40 位元 (弱) 安全套接層 (SSL) 連線。如果您沒有選取這個選項，則只支援 128 位元的連線。 |
| 啓用 SSL 2.0 版 | 已核取 | 啓用 SSL 2.0 版本。<br>停用 SSL 2.0 表示只支援舊版 SSL 2.0 的瀏覽器將不能認證至 SRA。這可確保較大的安全層級。 |
| 啓用 SSL 加密選項 | | 啓用 SSL 加密選項。您可以選擇支援所有預先封裝的密碼，或者您可以單獨選擇需要的密碼。您可以爲每個閘道實例選擇特定的 SSL 密碼。 |
| SSL2 加密 | | 列出您可以選擇的 SSL 版本 2 密碼。 |
| SSL3 加密 | | 列出您可以選擇的 SSL 版本 3 密碼。 |
| TLS 加密 | | 列出 TLS 密碼。 |
| 啓用 SSL 3.0 版 | 已核取 | 啓用 SSL 3.0 版。<br>停用 SSL 3.0 表示只支援 SSL 3.0 的瀏覽器將不能認證至 SRA 。這可確保較大的安全層級。 |
| 啓用空加密 | | 啓用空加密。 |
| 可信任的 SSL 網域 | | 列出信任的 SSL 網域。 |

表 A–4 閘道服務安全性屬性 (續)

| 屬性 | 預設值 | 描述 |
| --- | --- | --- |
| 將 Cookie 標示爲安全 | | 將 Cookie 標示爲安全。必須啓用 [啓用 Cookie 管理] 選項。 |

# Rewriter

Rewriter 標籤有兩個子區段：


- 第 254 頁的 「基本」
- 第 255 頁的 「進階」


## 基本

第 254 頁的 「基本」列出了閘道服務 Rewriter 基本屬性。

表 A–5 閘道服務 Rewriter 屬性 - 基本

| 屬性 | 預設值 | 描述 |
| --- | --- | --- |
| 啓用所有 URL 的重寫 | | 指定重寫所有 URI，但不核對 [網域與子網域的代理伺服器] 清單中的項目。 |
| 對映 URI 至規則集 | `*://*.iportal.com*/portal/* \|default_gateway_ruleset`<br>`*/portal/NetFileOpenFileServlet* \|null_ruleset`<br>`*\|generic_ruleset`<br>`REPLACE_WITH_IPLANET_MAIL_SERVER_NAME \|iplanet_mail_ruleset`<br>`REPLACE_WITH_EXCHANGE_SERVER_ NAMEexchange_2000sp3_owa_ruleset`<br>`*://*.iportal.com*/amconsole/* \|default_gateway_ruleset`<br>`REPLACE_WITH_INOTES_SERVER_NAME \|inotes_ruleset`<br>`http*://*/portal/NetFileController* \|null_ruleset` | 使用 [對映 URI 至規則集] 清單建立網域與規則集之間的關聯。規則集是在 Access Manager 管理主控台的 [Portal Server 配置] 下建立。 |

表 A–5 閘道服務 Rewriter 屬性 - 基本 *(續)*

| 屬性 | 預設值 | 描述 |
| --- | --- | --- |
| 對映剖析器至 MIME 類型 | `JAVASCRIPT=application/x-java`<br>`XML=text/xml`<br>`HTML=text/html;text/htm;text/x-component; text/wml;text/vnd.wap.wml`<br>`CSS=text/css` | 建立新的 MIME 類型與 HTML、JAVASCRIPT、CSS 或 XML 之間的關聯。以分號或逗號分隔多個項目。 |
| 不要重寫的 URI | | 列出不要重寫的 URI。注意：將 #* 新增至這份清單可允許重寫 URI，即使 href 規則是規則集的一部分也一樣。 |
| 預設網域 | | 將主機名稱解析爲預設網域與子網域。在安裝期間會指定這個選項 |

## 進階

第 255 頁的 「進階」 列出了閘道服務 Rewriter 進階屬性。

表 A–6 閘道服務 Rewriter 屬性 - 進階

| 屬性 | 預設值 | 描述 |
| --- | --- | --- |
| 啓用 MIME 推測 | | 當未傳送 MIME 時，啓用 MIME 推測。您必須將資料新增至 [對映剖析器至 URI] 清單方塊。 |
| 對映剖析器至 URI 對映 | | 將剖析器對映至 URI。由分號分隔多個 URI。<br>例如 HTML=*.html; *.htm;*Servlet<br>表示 Rewriter 會用於重新寫入任何含有 html、htm，或 Servlet 副檔名的網頁內容。 |
| 啓用遮罩 | | 允許 Rewriter 重新寫入 URI，如此即可隱藏網頁的企業內部網路 URL。 |
| 遮罩的種子字串 | | 指定可用於遮罩 URI 的種子字串。遮罩演算法會產生此隨機字串。 |

表 A–6 閘道服務 Rewriter 屬性 - 進階 *(續)*

| 屬性 | 預設值 | 描述 |
| --- | --- | --- |
| 不要遮罩的 URI | | 指定不要遮罩的網際網路 URI。當應用程式 (例如 applet) 需要網際網路 URI 時便可使用此選項。<br>例如您新增<br>*/Applet/Param*<br>至清單方塊，如果內容 URI http://abc.com/Applet/Param1.html 與規則集相符，就不會遮罩此 URL。 |
| 讓閘道通訊協定與原始 URI 通訊協定相同 | | 讓 Rewriter 使用一致的通訊協定存取 HTML 內容中參照的資源。<br>這將僅套用至靜態 URI，而非產生於 Javascript 的動態 URI。 |

# NetFile 服務

當您按一下 NetFile 服務，右邊的窗格將會顯示標籤。他們是：

- 第 256 頁的 「主機」
- 第 257 頁的 「權限」
- 第 258 頁的 「檢視」
- 第 258 頁的 「作業」
- 第 259 頁的 「一般」

## 主機

[主機] 標籤有兩個子區段：

- 第 256 頁的 「配置」
- 第 257 頁的 「存取」

### 配置

第 256 頁的 「配置」列出了 Netfile 主機配置屬性。

表 A–7 NetFile 服務主機配置屬性

| 屬性 | 預設值 | 描述 |
| --- | --- | --- |
| 作業系統字元集 | Unicode(UTF-8) | 指定在與主機通訊時用來作爲預設編碼的字元集。 |

表 A–7 NetFile 服務主機配置屬性 (續)

| | | |
|---|---|---|
| 主機偵測順序 | WIN、NETWARE、FTP、NFS | 指定主機偵測順序。 |
| 共用主機 | | 指定所有遠端 NetFile 使用者都可以透過 NetFile 使用的主機。 |
| 預設網域 | | 指定 NetFile 用於連絡允許主機所需要的預設網域。 |
| 預設 Microsoft Windows 網域/工作群組 | | 指定使用者爲存取 Microsoft Windows 主機而選擇的預設 Microsoft Windows 網域/工作群組。 |
| 預設 WINS/DNS 伺服器 | | 指定 NetFile 用於存取 Windows 主機的 WINS/DNS 伺服器。 |

## 存取

第 257 頁的 「存取」列出了 NetFile 服務主機存取屬性。

表 A–8 NetFile 服務主機存取屬性

| 屬性 | 預設值 | 描述 |
|---|---|---|
| 允許存取 Windows 主機 | 已核取 | 允許存取 Microsoft Windows 主機。 |
| 允許存取 FTP 主機 | 已核取 | 允許存取 FTP 主機。 |
| 允許存取 NFS 主機 | 已核取 | 允許存取 NFS 主機。 |
| 允許存取 Netware 主機 | 已核取 | 允許存取 Netware 主機。 |
| 允許的主機 | * | 指定使用者能夠透過 NetFile 存取的主機。 |
| 遭拒的主機 | | 指定使用者不能夠透過 NetFile 存取的主機。 |

# 權限

若您在使用者開始使用 NetFile 之後停用這些選項，則只有在使用者登出 NetFile 並重新登入後，此項變更才會生效。

第 257 頁的 「權限」列出了 Netfile 服務權限屬性。

表 A–9 NetFile 服務權限屬性

| 屬性 | 預設值 | 描述 |
|---|---|---|
| 允許檔案重新命名 | 已核取 | 允許使用者重新更名檔案。 |

表 A–9 NetFile 服務權限屬性 (續)

| 屬性 | 預設值 | 描述 |
|---|---|---|
| 允許檔案/資料夾刪除 | 已核取 | 允許使用者刪除檔案及資料夾。 |
| 允許檔案上傳 | 已核取 | 允許使用者上傳檔案。 |
| 允許檔案/資料夾下載 | 已核取 | 允許使用者下載檔案及資料夾。 |
| 允許檔案搜尋 | 已核取 | 允許使用者搜尋。 |
| 允許檔案郵寄 | 已核取 | 允許檔案郵寄。 |
| 允許檔案壓縮 | 已核取 | 允許壓縮檔案。 |
| 允許變更使用者 ID | 已核取 | 允許使用者使用不同的 ID。 |
| 允許變更 Windows 網域 | 已核取 | 允許使用者變更 Microsoft Windows 網域。 |

# 檢視

第 258 頁的 「檢視」列出了 Netfile 服務檢視屬性。

表 A–10 NetFle 服務檢視屬性

| 屬性 | 預設值 | 描述 |
|---|---|---|
| 視窗大小 | 700\|400 | 以像素爲單位指定 NetFile 視窗在使用者桌面上的大小。若您輸入的值無效，NetFile 會使用此預設值。 |
| 視窗位置 | 100\|50 | 指定 NetFile 視窗在使用者桌面上顯示的位置。若您輸入的值無效，NetFile 會使用此預設值。 |

# 作業

[作業] 標籤的子區段如下：

- 第 258 頁的 「流量」
- 第 259 頁的 「搜尋」
- 第 259 頁的 「壓縮」

## 流量

第 258 頁的 「流量」列出了 NetFile 服務作業流量屬性。

表 A–11 NetFile 服務作業 - 流量屬性

| 屬性 | 預設值 | 描述 |
| --- | --- | --- |
| 暫存目錄位置 | /tmp | 爲不同 NetFile 檔案作業指定暫存目錄。<br>確保執行 Web 伺服器的 ID (例如 nobody 或 noaccess) 擁有指定目錄的 rwx 權限。還要確保 ID 對於需要的暫時目錄的完整路徑擁有 rx 權限。<br>您可以爲 NetFile 建立單獨的暫存目錄。如果您爲 Portal Server 所有模組指定了共用的暫存目錄，磁碟空間可能很快就會用完。如果暫存目錄已無空間，則 NetFile 將無法運作。 |
| 檔案上傳限制 (MB) | 5 | 指定檔案可以上傳的最大大小。若您輸入一個無效的值，NetFile 會將此值重新設定爲預設值。請確定您鍵入了整數值。<br>您可以爲不同的使用者指定不同的檔案上傳大小限制。 |

## 搜尋

第 259 頁的 「搜尋」列出了 NetFile 服務作業搜尋屬性。

表 A–12 NetFile 服務作業 - 搜尋屬性

| 屬性 | 預設值 | 描述 |
| --- | --- | --- |
| 搜尋目錄限制 | 100 | 指定在單一搜尋作業中，可搜尋目錄的最大數目。 |

## 壓縮

第 259 頁的 「壓縮」列出了 NetFile 服務作業壓縮屬性。

表 A–13 NetFile 服務作業 - 壓縮屬性

| 屬性 | 預設值 | 描述 |
| --- | --- | --- |
| 預設壓縮類型 | Zip | 指定使用 Zip 或 Gzip 壓縮類型。 |
| 預設壓縮層級 | 6 | 指定壓縮層級，有效值從 1 到 9。 |

# 一般

第 259 頁的 「一般」列出了 Netfile 服務一般屬性。

表 A–14 NetFile 服務 - 一般屬性

| 屬性 | 預設值 | 描述 |
| --- | --- | --- |
| MIME 類型配置檔案位置 | /opt/S1PS62/SUNWportal/samples/config/netfile | 指定傳送至用戶端瀏覽器的回應內容類型。 |

# Netlet 服務

第 260 頁的 「Netlet 服務」列出 Netlet 服務屬性。

表 A–15 Netlet 服務屬性

| 屬性 | 預設值 | 描述 |
| --- | --- | --- |
| Netlet 規則 | | 選擇新增或刪除規則。 |
| 如果您新增一個規則，將會需要下列九個屬性： | | |
| --規則名稱 | | 爲規則指定唯一的名稱。 |
| --加密密碼 | | 指定需要的密碼。 |
| --URL | | 指定要啓動之應用程式的 URL。 |
| --下載 Applet | | 指定是否需要下載 Applet。如果已經使用 Applet，則相關編輯方塊中的語法爲：<br>local-port:server-host:server-port |
| --延伸階段作業 | | 確保當與此規則相對映的 Netlet 階段作業在執行時，Portal Server 階段作業時間將會延長。 |
| --對映本機連接埠至目標伺服器連接埠 | | 指定本機連接埠、目標主機以及目標連接埠。在輸入那些數值之後 (在此表中的下三行)，請按一下 [新增] 以便讓此規則出現在清單中。 |
| --本地連接埠 | | 指定 Netlet 偵聽的本機連接埠。對於 FTP 規則，本機連接埠值必須爲 30021。 |
| --目標主機 | | 靜態規則包含用於 Netlet 連線的目標機器之主機名稱。<br>動態規則包含 "TARGET" 這個字。 |
| --目標連接埠 | | 指定目標主機上的連接埠。 |
| 預設原生 VM 加密 | | 爲 Netlet 規則指定預設加密法。如果現有規則未將加密法包括成爲規則的一部分，當您在使用現有規則時，這個選項就非常有用。 |

表 A–15 Netlet 服務屬性 (續)

| 屬性 | 預設值 | 描述 |
|---|---|---|
| 預設 Java Plugin 加密 | | 爲 Netlet 規則指定預設加密法。如果現有規則未將加密法包括成爲規則的一部分，當您在使用現有規則時，這個選項就非常有用。 |
| 預設回送連接埠 | 58000 | 當透過 Netlet 下載 applet 時，指定用戶端上使用的連接埠。可以在 Netlet 規則中忽略此預設值。 |
| 重新認證連線 | | 確保使用者每次重新建立 Netlet 連線，都必須輸入 Netlet 密碼。 |
| 連線時顯示快顯式警告 | 已核取 | 當使用者在 Netlet 執行應用程式且當入侵者嘗試透過偵聽連接埠存取桌面時會顯示一則訊息。 |
| 在連接埠警告對話方塊中顯示核取方塊 | 已核取 | 當 Netlet 嘗試在使用者的標準入口網站桌面上連線到目標主機時，提供使用者抑制警告對話方塊快顯的選項。 |
| 保持現有的間隔 (分鐘) | 0 | 如果用戶端透過 Web 代理伺服器連線到閘道，開置的 Netlet 連線會因爲代理伺服器逾時而中斷。爲了避免這種情形，請爲此參數賦予一個小於代理伺服器逾時的值。 |
| 在門戶網站登出時終止 Netlet | 已核取 | 確保在使用者登出 Portal Server 時，所有連線都已終止。 |
| 存取 Netlet 規則 | * | 定義存取某些組織、角色或使用者的特定的 Netlet 規則。 |
| 拒絕 Netlet 規則 | | 拒絕存取某些組織、角色或使用者的特定的 Netlet 規則。 |
| 允許的主機 | * | 定義某個組織、角色或使用者對特定主機的存取。 |
| 遭拒的主機 | | 拒絕存取組織中特定的主機。 |

# Proxylet 服務

第 261 頁的 「Proxylet 服務」列出 Proxylet 服務屬性。

表 A–16 Proxylet 服務屬性

| 屬性 | 預設值 | 描述 |
| --- | --- | --- |
| 自動下載 Proxylet Applet | | 如果核取了該核取方塊，會在使用者登入時下載 Proxylet 到用戶端機器。 |
| 預設 Proxylet Applet 連結 IP | 127.0.0.1 | Proxylet Applet 常駐的 IP 位址。 |
| 預設 Proxylet Applet 連接埠 | 58081 | 此爲 Proxylet 偵聽的連接埠。 |

◆ ◆ ◆ 附錄 B

# 記錄檔

下列記錄檔位於預設的 /var/opt/SUNWportal/debug 目錄，且包含除錯與其他類型的資訊：

## 關於記錄檔

表 B–1 資訊和除錯檔案

| 檔案名稱 | 內容 |
| --- | --- |
| 下列記錄檔是由位於預設目錄 /etc/opt/SUNWam/debug/file 的 AMConfig-*instance-name*.properties 檔案中的除錯參數所控制：如需 Linux 路徑名稱，請參閱「Solaris 與 Linux 路徑名稱比較 」。 | |
| amconsole | Netfile、Netlet 和 Gateway Admin 檔案 |
| srapNetFile | NetFile 資訊檔 |
| srapNetlet | Netlet 資訊檔 |
| srapProxylet | Proxylet 資訊檔 |
| 下列記錄檔是由預設目錄 /etc/opt/SUNWportal 中 platform.conf.gateway-profile-name 檔案的除錯參數 gateway.debug 所控制。如需 Linux 路徑名稱，請參閱「Solaris 與 Linux 路徑名稱比較」。 | |
| srapGateway.gateway-profile -name | 閘道資訊 |

表 B–1 資訊和除錯檔案 *(續)*

| 檔案名稱 | 內容 |
| --- | --- |
| Gateway_to_from_server.gateway-profile-name | |
| Gateway_to_from_browser.gateway-profile-name | |
| srapNetletProxy.gateway-profile-name | |
| srapRewriterProxy.gateway-profile-name | |
| rwproxy.log.rewriter-proxy-instance-name | Rewriter 代理伺服器的開始與停止時間 |
| nlproxy.log.netlet-proxy-instance-name | Netlet 代理伺服器的開始與停止時間 |
| gateway.log.gateway.instance.name | 閘道的開始與停止時間 |
| 下列的 Rewriter 檔是由預設目錄 `/var/opt/SUNWam/config/` 檔案的 `AMConfig-`*`instance-name`*` .properties` **檔案** 中的除錯參數所控制。請參閱第 90 頁的 「使用除錯記錄檔排除故障」以取得詳細資訊。 | |
| RuleSetInfo | 所有已用於重新寫入的規則集皆記錄在此檔案中。 |
| Original Pages | 包含網頁 URI、解決的 URI (若解決的 URI 與網頁 URI 不同)、內容 MIME、套用至網頁的規則集、剖析器 MIME 與原始內容。<br>與剖析有關的特定錯誤/警告/訊息亦會出現在此檔案中。<br>在 message 模式中，會記錄完整內容；在 warning 及 error 模式下則僅會記錄重新寫入期間所發生的異常情況。 |
| Rewritten Pages | 包含網頁 URI、解決的 URI (若解決的 URI 與網頁 URI 不同)、內容 MIME、套用至網頁的規則集、剖析器 MIME 與重新寫入的內容。<br>當除錯模式設爲 message 時，即會儲存這些資訊。 |
| Unaffected Pages | 包含未經修改的網頁清單。 |
| URIInfo Pages | 此檔案包含已找到及轉譯的 URL。所有其內容與原始資料相同的網頁詳細資訊將記錄至此檔案中。<br>記錄的詳細資訊包括：網頁 URI、MIME 與編碼資料、用於重新寫入的 rulesetID 以及剖析器 MIME。 |

◆ ◆ ◆ 附錄 C

# 國家代碼

下列表格中列出了二字母國家代碼，在認證管理期間您需要指定這些國家代碼。

## 國家代碼清單

表 C–1 二字母國家代碼

| | |
|---|---|
| ad | 安道爾侯國 |
| ae | 阿拉伯聯合大公國 |
| af | 阿富汗伊斯蘭國 |
| ag | 安地卡及巴布達 |
| ai | 安圭拉 |
| al | 阿爾巴尼亞 |
| am | 亞美尼亞 |
| an | 荷屬安地列斯 |
| ao | 安哥拉 |
| aq | 南極大陸 |
| ar | 阿根廷 |
| arpa | 舊的美國官方網路 |
| as | 美屬薩摩亞 |
| at | 奧地利 |
| au | 澳大利亞 |

表 C–1 二字母國家代碼 *(續)*

| | |
|---|---|
| aw | 阿魯巴 |
| az | 亞塞拜然 |
| ba | 波士尼亞赫塞哥維納 |
| bb | 巴貝多 |
| bd | 孟加拉 |
| be | 比利時 |
| bf | 布基納法索 |
| bg | 保加利亞 |
| bh | 巴林 |
| bi | 蒲隆地 |
| bj | 貝南 |
| bm | 百慕達 |
| bn | 汶萊 |
| bo | 玻利維亞 |
| br | 巴西 |
| bs | 巴哈馬 |
| bt | 不丹 |
| bv | 布威島 |
| bw | 波札那 |
| by | 白俄羅斯 |
| bz | 貝里斯 |
| ca | 加拿大 |
| cc | 可可斯群島 |
| cf | 中非 |
| cd | 剛果民主共和國 |
| cg | 剛果 |
| ch | 瑞士 |
| ci | 象牙海岸 |
| ck | 柯克群島 |

表 C–1 二字母國家代碼 *(續)*

| | |
|---|---|
| cl | 智利 |
| cm | 喀麥隆 |
| cn | 中國 |
| co | 哥倫比亞 |
| com | 商業組織 |
| cr | 哥斯大黎加 |
| cs | 前捷克斯洛伐克 |
| cu | 古巴 |
| cv | 維德角 |
| cx | 聖誕島 |
| cy | 塞浦路斯 |
| cz | 捷克共和國 |
| de | 德國 |
| dj | 吉布地 |
| dk | 丹麥 |
| dm | 多米尼克 |
| do | 多明尼加 |
| dz | 阿爾及利亞 |
| ec | 厄瓜多爾 |
| edu | 教育組織 |
| ee | 愛沙尼亞 |
| eg | 埃及 |
| eh | 西撒哈拉 |
| er | 厄利垂亞 |
| es | 西班牙 |
| et | 衣索比亞 |
| fi | 芬蘭 |
| fj | 斐濟 |
| fk | 福克蘭群島 |

表 C–1 二字母國家代碼 *(續)*

| | |
|---|---|
| fm | 密克羅尼西亞 |
| fo | 法羅群島 |
| fr | 法國 |
| fx | 法國 (歐洲領土) |
| ga | 加彭 |
| gb | 英國 |
| gd | 格瑞那達 |
| ge | 喬治亞 |
| gf | 法屬圭亞那 |
| gh | 加納 |
| gi | 直布羅陀 |
| gl | 格陵蘭 |
| gm | 甘比亞 |
| gn | 幾內亞 |
| gov | 美國政府 |
| gp | 哥德普洛 (法屬) |
| gq | 赤道幾內亞 |
| gr | 希臘 |
| gs | 聖喬治與聖文森群島 |
| gt | 瓜地馬拉 |
| gu | 關島 (美屬) |
| gw | 幾內亞比索 |
| gy | 圭亞那 |
| hk | 香港 |
| hm | 赫德島及麥當勞群島 |
| hn | 宏都拉斯 |
| hr | 克羅埃西亞 |
| ht | 海地 |
| hu | 匈牙利 |

表 C–1 二字母國家代碼 *(續)*

| | |
|---|---|
| id | 印尼 |
| ie | 愛爾蘭 |
| il | 以色列 |
| in | 印度 |
| int | 國際組織 |
| io | 英屬印度洋領土 |
| iq | 伊拉克 |
| ir | 伊朗 |
| is | 冰島 |
| it | 義大利 |
| jm | 牙買加 |
| jo | 約旦 |
| jp | 日本 |
| ke | 肯亞 |
| kg | 吉爾吉斯共和國 (吉爾吉斯) |
| kh | 柬埔寨王國 |
| ki | 吉里巴斯 |
| km | 葛摩 |
| kn | 聖基茨-尼維斯-安圭拉 |
| kp | 北韓 |
| kr | 南韓 |
| kw | 科威特 |
| ky | 開曼群島 |
| kz | 哈薩克 |
| la | 寮國 |
| lb | 黎巴嫩 |
| lc | 聖露西亞 |
| li | 列支敦斯登 |
| lk | 斯里蘭卡 |

表 C–1 二字母國家代碼 (續)

| | |
|---|---|
| lr | 賴比瑞亞 |
| ls | 賴索托 |
| lt | 立陶宛 |
| lu | 盧森堡 |
| lv | 拉脫維亞 |
| ly | 利比亞 |
| ma | 摩洛哥 |
| mc | 摩納哥 |
| md | 摩達維亞 |
| mg | 馬達加斯加 |
| mh | 馬紹爾群島 |
| mil | 美國軍隊 |
| mk | 馬其頓 |
| ml | 馬利 |
| mm | 緬甸 |
| mn | 蒙古 |
| mo | 澳門 |
| mp | 北馬里安納群島 |
| mq | 馬丁尼克 (法屬) |
| mr | 茅利塔尼亞 |
| ms | 蒙特色拉特島 |
| mt | 馬爾他 |
| mu | 模里西斯 |
| mv | 馬爾地夫 |
| mw | 馬拉威 |
| mx | 墨西哥 |
| my | 馬來西亞 |
| mz | 莫三比克 |
| na | 納米比亞 |

表 C–1 二字母國家代碼 *(續)*

| | |
|---|---|
| nato | NATO (本組織已在 1996 解散 - 請參閱 hq.nato.int) |
| nc | 新喀里多尼亞群島 (法屬) |
| ne | 尼日 |
| net | 網路 |
| nf | 諾福克島 |
| ng | 奈及利亞 |
| ni | 尼加拉瓜 |
| nl | 荷蘭 |
| no | 挪威 |
| np | 尼泊爾 |
| nr | 諾魯 |
| nt | 中立區 |
| nu | 紐威島 |
| nz | 紐西蘭 |
| om | 阿曼 |
| org | 非營利組織 (sic) |
| pa | 巴拿馬 |
| pe | 秘魯 |
| pf | 玻里尼西亞 (法屬) |
| pg | 巴布亞紐幾內亞 |
| ph | 菲律賓 |
| pk | 巴基斯坦 |
| pl | 波蘭 |
| pm | 聖皮埃爾島及密克隆島 |
| pn | 皮特康群島 |
| pr | 波多黎各 |
| pt | 葡萄牙 |
| pw | 帛琉 |
| py | 巴拉圭 |

表 C–1 二字母國家代碼 *(續)*

| | |
|---|---|
| qa | 卡達 |
| re | 留尼旺 (法屬) |
| ro | 羅馬尼亞 |
| ru | 俄羅斯聯邦 |
| rw | 盧安達 |
| sa | 沙烏地阿拉伯 |
| sb | 索羅門群島 |
| sc | 塞席爾 |
| sd | 蘇丹 |
| se | 瑞典 |
| sg | 新加坡 |
| sh | 聖赫勒拿島 |
| si | 斯洛維尼亞 |
| sj | 冷岸及央棉群島 |
| sk | 斯洛伐克共和國 |
| sl | 獅子山 |
| sm | 聖馬利諾 |
| sn | 塞內加爾 |
| so | 索馬利亞 |
| sr | 蘇利南 |
| st | 聖多美普林西比 |
| su | 前蘇聯 |
| sv | 薩爾瓦多 |
| sy | 敘利亞 |
| sz | 史瓦濟蘭 |
| tc | 土克斯及開科斯群島 |
| td | 查德 |
| tf | 法屬南方領土 |
| tg | 多哥 |

表 C–1 二字母國家代碼 *(續)*

| | |
|---|---|
| th | 泰國 |
| tj | 塔吉克 |
| tk | 托克勞群島 |
| tm | 土庫曼 |
| tn | 突尼西亞 |
| 至 | 東加 |
| tp | 東帝汶 |
| tr | 土耳其 |
| tt | 千里達及托巴哥 |
| tv | 吐瓦魯 |
| tw | 台灣 |
| tz | 坦尚尼亞 |
| ua | 烏克蘭 |
| ug | 烏干達 |
| uk | 英國 |
| um | 美國邊遠島嶼 |
| us | 美國 |
| uy | 烏拉圭 |
| uz | 烏茲別克 |
| va | 教廷 (梵蒂岡) |
| vc | 聖文森及格瑞那丁 |
| ve | 委內瑞拉 |
| vg | 英屬維爾京群島 |
| vi | 美屬維爾京群島 |
| vn | 越南 |
| vu | 萬那杜 |
| wf | 瓦利斯及福杜納群島 |
| ws | 薩摩亞 |
| ye | 葉門 |

表 C–1 二字母國家代碼 (續)

| | |
|---|---|
| yt | 馬約特島 |
| yu | 南斯拉夫 |
| za | 南非 |
| zm | 尚比亞 |
| zr | 薩伊 |
| zw | 辛巴威 |

# 索引


**A**
AMConfig 特性檔案, 預設值，39
applet，130
　下載，142

**C**
certadmin 程序檔，193-202
Citrix, html 檔案，146-148
Communication Express，29

**D**
DMZ，26
DNS，144

**E**
Enterprise System Accessory CD
　jchdt 套裝軟體，62
　SUNWrhino 套裝軟體，45

**F**
FTP, NetFile 中支援的，125

**H**
HTML, Rewriter 中的規則，68-74
HTTP
　使用 web 代理伺服器的資源，39
　連絡資源，39
　標頭，52

**J**
Java™，45, 62
JavaScript, Rewriter 中的規則，74-87
Jchardet, 使用 PAC 檔案，45-47
jCIFS
　NetFile 中支援的，125
　供 Windows 存取，126

**M**
Messenger Express，29
Microsoft Exchange Server，145
MIME, 要剖析的類型，167-168
MIME 類型, 建立清單，167-168

**N**
Net 規則, 範例，143-146
NetFile，125
　支援的協定，125-127
　主機偵測順序，126
　使用 Novell Netware，126

NetFile *(續)*
使用 ProFTPD 伺服器，126
啓用存取，127
簡介，125
Netlet，130
applet，130
元件，130-131
在 Sun Ray 環境中，146-148
使用 PAC 檔案，45-47
使用方案，131
爲 PDC 配置，209-210
連接埠號碼，138
規則，131, 132-142
偵聽連接埠，130
從遠端主機下載 Applet，132
提供者，131
簡介，129-132
Netlet 代理伺服器
使用，47-50
重新啓動，50
啓用，50
優點，48
Netlet 代理程式，131
Netlet 規則
動態，136
靜態規則，135-136
Netlet 規則範例
FTP，145
IMAP，143
Lotus Notes 非 Web 用戶端，144
Lotus Web 用戶端，143
Microsoft Outlook 與 Exchange Server，145
Netscape 4.7 郵件用戶端，146
SMTP，143
NFS, NetFile 中支援的，125
Novell Netware, NetFile 的協定，126

**O**

Outlook Web Access，145
配置，122
規則集，122

**P**

PAC, 配置，45-47
PAC 檔案, 使用 Rhino 軟體，45
PDC
配置，209-210
認證，188
認證鏈接，53
platform.conf，34-39
特性，35-39
ProFTPD, 使用 NetFile，126
Proxylet
使用 PAC 檔案，45-47
優點，58

**R**

Rewriter
[網域與子網域的代理伺服器] 清單，44
6.x 與 3.0 規則集對映，123-124
HTML 規則，68-74
JavaScript 規則，74-87
URLScraper，62
XML 規則，87-89
工作範例，93-119
在規則中與式樣相符，73-74
建立 URI 與規則集的對映清單，166-167
建立不要重寫的 URI 清單，182
使用除錯記錄，90-93
使用萬用字元，182
案例研究，119-123
配置，182-185
規則集 DTD，63-65
撰寫規則，66
範例，93-119
Rewriter 代理伺服器
建立，51
重新啓動，51
啓用，51
優點，50
Rhino 軟體, 來剖析 PAC 檔案，45
ruleset, generic，181
rwpmultiinstance，51

**S**

SMB, 供 windows 存取，126
SRA
  服務，27-28
  連絡 SRA 核心，33
  軟體，25
SSL，187
SUNWjchdt 套裝軟體，62

**T**

TCP/IP，129

**U**

UNIX, 指令行，229
URL, 由動態 Netlet 規則呼叫，141-142
URLScraper，62

**W**

Web 代理伺服器，39-44
Windows, jCIFS 必要的，126
WML, Rewriter 中的規則，90

**X**

XML 規則, Rewriter 中，87-89
入口網站管理員, 知識，17-18
支援的密碼，137
元件, Netlet，130-131
反向代理伺服器，51
  啓用，237-238
加速器
  Sun Crypto 1000，221-224
  Sun Crypto 4000，224-227
  外部 SSL 裝置，227-228
  代理伺服器，227-228
主機代理伺服器, 建立，33
主機偵測順序, 用於 NetFile，126
代理伺服器
  Web，39-44
  反向，51
  加速器，227-228
  指定主機代理伺服器，33
代理程式, Netlet，131
行事曆，29
多址閘道，32
多重實例, 閘道，32
多個實例, Rewriter 代理伺服器，50
安全套接層，27
安全模式，26-27
自訂, 閘道使用者介面，54-55
自動代理伺服器配置，45-47
自動偵測, 在 Netfile 中，125
自簽憑證，193-194
串接樣式表, Rewriter 中，90
協定
  NetFile，125-127
  在 NetFile 中支援的，125
非軍事區，26
拒絕, URL，151
服務, SRA，27-28
建立
  Rewriter 代理伺服器，51
  URI 與規則集的對映清單，166-167
  不要重寫的 URI 清單，182
  主機代理伺服器，33
  閘道設定檔，32
使用者可配置的密碼，136
重新啓動
  Netlet Portal 代理伺服器，50
  Rewriter 代理伺服器，51
  閘道，33
除錯記錄, Rewriter，90-93
信任屬性，189
指定, 衝突解決，29
案例研究, Rewriter，119-123
記錄檔, 檔案名稱，263
通知，29
連接埠, Netlet，130
連接埠號碼, Netlet，138
配置
  Outlook Web Access，122

配置 *(續)*
Rewriter，182-185
遭拒的 URL，151
特性, platform.conf，35-39
動態規則
Netlet，136
下載 applet，142
呼叫，141-142
規則
Netlet，132-142
Rewriter，66
Rewriter 中的 HTML，68-74
Rewriter 中的 JavaScript，74-87
WML，90
串接樣式表，90
規則集對映, 建立 URI 清單，166-167
停止, 閘道，233
停用, 瀏覽器快取，54
國家代碼, 雙字母值，265
執行
應用程式，18, 129
產生, 自簽憑證，193-194
啓用
NetFile 存取，127
Netlet 代理伺服器，50
Rewriter 代理伺服器，51
反向代理伺服器，237-238
認證鏈接，53-54
密碼
支援的，137
使用者可配置的，136
管理員配置的，136
處理順序, 代理伺服器，41-44
登入, Rewriter，90-93
萬用字元
Web 代理伺服器中，41
於 Rewriter 中，182
萬用字元憑證，54
開放模式，26
閘道
多址，32
使用 PAC 檔案，45-47
重新啓動，33
停止，233
閘道 *(續)*
閘道設定檔，32
簡介，31
預設
閘道設定檔，32
網域，44
預設網域, 重寫，44
管理員配置的密碼，136
疑難排解，90-93
網域與子網域的代理伺服器，41
監視程式
Netlet 代理伺服器，50
Rewriter 代理伺服器，51
認證
PDC，53, 188
鏈接，53-54
模式
安全，26-27
開放，26
範例, Rewriter，93-119
標頭, HTTP，52
衝突解決，29
憑證
certadmin 程序檔，193-202
SSL，187-188
公開憑證，189-193
列示所有，200-201
列示根 CA 憑證，200
列印，201-202
自簽，193-194
刪除，198
信任屬性，189
訂製，197
根 CA 憑證，196
修改信任屬性，199
從 CA 安裝，196-198
萬用字元，54
憑證簽署請求，194-195
檔案，188
靜態規則，135-136
聯合管理，241
應用程式
支援的，29-30
執行，18, 129

瀏覽器快取, 停用, 54