

管理員指南

SunTM ONE Directory Proxy Server

圖 5.2

2003 年 6 月
816-4657-10

版權所有 © 2003 Sun Microsystems, Inc.。有些之前存在的部分，版權所有 © 2001 Netscape Communications Corporation。版權所有 © 1996-1998 Critical Angle Inc.。版權所有 © 1998-2001 Innosoft International, Inc.。保留所有權利。

Sun、Sun Microsystems 和 Sun 標誌是 Sun Microsystems, Inc. 在美國和其他國家 (地區) 的商標或註冊商標。Netscape 和 Netscape N 標誌是 Netscape Communications Corporation 在美國和其他國家 (地區) 的註冊商標。其他 Netscape 標誌、產品名稱和服務名稱也是 Netscape Communications Corporation 的商標，可能已在其他國家 (地區) 註冊。

Directory Proxy Server 產品的某些部分是源自版權屬於 University of Michigan、University of California at Berkeley 和 Harvard University 的軟體。未經書面明確同意之前，不得使用這些以大學名義推薦或促銷由此處所述產品，或說明文件所衍生之產品。

Directory Proxy Server 說明文件的某些部分版權屬於 The Internet Society (1997)。保留所有權利。

聯邦採購法：商業軟體和政府使用者係受標準授權合約條款和條件限制。

本文件中所描述產品的散佈，係受限制其使用、複製、散佈和反編譯的授權限制。在未獲得 Sun-Netscape Alliance 及其授權者 (如果有的話) 的書面授權之前，皆不得用任何方法將產品或本文件的任何部分重製成任何形式。

此文件係按「現況」提供，不為任何明示或默示條款、陳述及保證擔保，包括任何適售性、符合特定使用目的及不侵權之默示擔保，除非本免責聲明的內容已無法律效力。

目錄

關於本指南	3
應閱讀本指南的讀者	3
本指南的內容	4
本指南採用的慣例	4
相關資訊	5
協同工具功能	6
主控台協同工具功能	6
容易了解的名稱與描述	6
可自訂的字型	6
動態 GUI 佈局	6
鍵盤游標控制元件	6
非 UI 元素的對等 UI	6
對等的指令行介面	6
靜態元件協同工具功能	7
非 UI 元素的對等 UI	7
可以非協同性技術轉譯的表格	7
第 1 部分 Sun ONE Directory Proxy Server 簡介	9
第 1 章 Sun ONE Directory Proxy Server 概論	11
簡介	11
Directory Proxy Server 功能組	13
高可用性	13
負載平衡	13
容錯移轉	14
安全	14

主從架構相容性	15
第 2 章 Sun ONE Directory Proxy Server 部署方式	17
分散式目錄基礎架構	17
分散式 LDAP 目錄基礎架構	18
客戶安裝	18
客戶部署	19
LDAP 要求流程	19
集中式 LDAP 目錄基礎架構	20
客戶安裝	20
客戶部署	21
LDAP 要求流程	22
部署在單一防火牆的 Directory Proxy Server	23
部署在多個防火牆的 Directory Proxy Server	25
第 2 部分 主控台基本管理	27
第 3 章 Directory Proxy Server 主控台簡介	29
Sun ONE Console 入門	29
[伺服器回應程式] 標籤	30
[使用者群組] 標籤	31
Sun ONE Administration Server	32
啟動 Administration Server	32
停止 Administration Server	33
存取 Directory Proxy Server 主控台	33
步驟 1. 登入 Sun ONE Console	34
步驟 2. 開啓適當的 Directory Proxy Server 主控台	36
開啓 Directory Proxy Server 伺服器主控台	37
開啓 Directory Proxy Server 組態編輯器主控台	39
第 4 章 啟動、重新啟動及停止 Directory Proxy Server	43
啟動及停止 Directory Proxy Server	43
從 Sun ONE Console 啟動及停止 Directory Proxy Server	44
從命令列啟動及停止 Directory Proxy Server	45
從 Windows NT [服務] 面板啟動及停止 Directory Proxy Server	46
重新啟動 Directory Proxy Server	47
從命令列重新啟動 Directory Proxy Server	47
在 UNIX 平台上從 Sun ONE Console 重新載入 Directory Proxy Server	47
檢查 Directory Proxy Server 系統狀態	49
從 Sun ONE Console 檢查 Directory Proxy Server 狀態	49

從命令列檢查 Directory Proxy Server 狀態	50
從命令列啟動及停止 Directory Proxy Server	51
支援的標幟	51
重新啟動 Directory Proxy Server	52
第 5 章 建立系統組態實例	53
建立系統組態實例	53
儲存組態	59
第 6 章 建立多管理群組	61
群組概論	61
建立群組	66
修改群組	88
刪除群組	89
第 7 章 定義多管理物件	91
屬性重新命名物件	92
建立屬性重新命名物件	93
禁止的項目物件	95
建立禁止的項目物件	96
LDAP 伺服器物件	99
建立 LDAP 伺服器物件	99
負載平衡物件	104
建立負載平衡物件	106
搜尋大小限制物件	108
建立搜尋大小限制物件	108
修改物件	110
刪除物件	111
第 8 章 建立多管理事件物件	113
事件概論	113
建立事件物件	114
建立 OnBindSuccess 事件物件	114
建立 OnSSLEstablished 事件物件	117
修改事件物件	118
刪除事件物件	119
第 9 章 建立多管理動作物件	121
動作概論	121
建立動作物件	122
修改動作物件	124

刪除動作物件	125
--------------	-----

第 10 章 設定記錄

記錄概論	127
系統記錄	127
稽核記錄	130
設定記錄	130
步驟 1. 定義記錄設定值	130
步驟 2. 指定要使用的記錄代碼	134
從 Directory Proxy Server 伺服器主控台監視記錄	135

第 11 章 設定安全

準備設定 SSL 及 TLS	138
使用代碼的全裝置設定 SSL 或 TLS	138
使用代碼的全裝置設定 SSL 或 TLS	139
使用代碼及代碼的全裝置設定 SSL	139
設定 SSL 通訊	139
步驟 1. 安裝 Directory Proxy Server 的「伺服器憑證」	139
SSL 憑證	140
步驟 A. 產生伺服器憑證要求	140
步驟 B. 傳送伺服器憑證要求	141
步驟 C. 安裝憑證	142
步驟 D. 安裝憑證授權單位憑證或伺服器憑證鏈結	143
步驟 E. 備份及還原您的憑證資料庫	144
步驟 2. 設定 Directory Proxy Server 及用戶端之間的 SSL 連線	144
步驟 A. 將 Directory Proxy Server 憑證授權單位憑證添加到用戶端的信任資料庫	145
步驟 B. 變更 Directory Proxy Server 系統組態	145
步驟 C. 變更 Directory Proxy Server 的網域名稱	146
步驟 3. 設定 Directory Proxy Server 及 LDAP 伺服器之間的 SSL 連線	147
步驟 A. 安裝憑證授權單位憑證或伺服器憑證鏈結	147
步驟 B. 將 Directory Proxy Server 憑證授權單位憑證添加到 LDAP 伺服器的信任資料庫	148
步驟 C. 變更 LDAP 伺服器代碼	148

第 3 部分 附錄

附錄 A Directory Proxy Server 決策引擎

連線時建立群組	153
連結時變更群組	153
設定連結時變更群組	155
建立 TLS 時變更群組	155

高可用性安裝	156
跟隨導引	157
附錄 B Directory Proxy Server 常見問答集、功能及疑難排解	159
Directory Proxy Server 常見問答集	159
Directory Proxy Server 功能	160
疑難排解	162
附錄 C Directory Proxy Server 啟動組態檔	165
組態檔概論	165
啟動組態檔的關鍵字	166
configuration_url	166
configuration_bind_dn	167
configuration_bind_pw	168
configuration_username	168
sasl_bind_mechanism	168
附錄 D 指令導引	169
dpsconfig2ldif	169
dpsldif2config	169
先決條件:	170
後續條件:	171
索引	173

圖 2-1	內部高可用性組態	18
圖 2-2	分散式 LDAP 目錄基礎架構	19
圖 2-3	集中式 LDAP 目錄基礎架構	21
圖 2-4	Directory Proxy Server 有一個防火牆的設定	24
圖 2-5	Directory Proxy Server 有兩個防火牆的設定	25
圖 3-1	Sun ONE Console : [伺服器及應用程式] 標籤	30
圖 3-2	Sun ONE Console : [使用者及群組] 標籤	32
圖 3-3	Directory Proxy Server 伺服器主控台 : [工作] 標籤	37
圖 3-4	Directory Proxy Server 伺服器主控台 : [組態] 標籤 [設定] 標籤	38
圖 3-5	Directory Proxy Server 伺服器主控台 : [組態] 標籤 [加密] 標籤	39
圖 3-6	Directory Proxy Server 組態編輯器主控台	40
圖 6-1	Directory Proxy Server 組態編輯器主控台 [網路群組] 視窗	64
圖 6-2	決定群組成員資格的 Directory Proxy Server 決策樹	65
圖 6-3	Directory Proxy Server 網路群組定義	67
圖 7-1	利用屬性重新命名內容對應結構	94
圖 7-2	在一組 LDAP 目錄伺服器副本上負載平衡	106
圖 11-1	Directory Proxy Server 中二種不同的通訊連結	141
圖 11-2	用戶端以憑證為準的驗證作業	142
圖 11-3	連結時變更群組	158
圖 11-4	建立 TLS 時變更群組	160

「*管理員指南*」提供 Sun™ Open Net Environment (Sun ONE) Directory Proxy Server 的各種部署方式，並說明如何設定與維護。

本前言包含下列各節：

- 應閱讀本指南的讀者 (第 3 頁)
- 本指南的內容 (第 4 頁)
- 本指南採用的慣例 (第 4 頁)
- 相關資訊 (第 5 頁)
- 協助工具功能 (第 6 頁)

應閱讀本指南的讀者

「Directory Proxy Server 管理員指南」是為設定及操作一個以上伺服器的系統管理員所寫。本指南假設您已經有以下的背景：

- 對網際網路及 LDAP 有一般瞭解。
- 對 Sun ONE Directory Server 5.x 以及管理方式有一般瞭解。您應該能讀取並修改目錄資料。

本指南的用途

本指南分成以下三部分：

- 第 1 部分 「Sun ONE Directory Proxy Server 簡介」
- 第 2 部分 「主控台基本管理」
- 第 3 部分 「附錄」

本指南採用的慣例

本節說明本書採用的慣例。

Monospaced 字型 - 這種字體用於任何出現在電腦螢幕上的文字，或是您應該輸入的文字，此外，也用於檔案名稱、函數與範例上。

注意： 「注意」與「小心」標示重要的資訊。在繼續進行工作之前，請務必仔細閱讀這類資訊。

大於符號 (>) 用於分隔連續的功能表選項。例如，[物件]>[新增]>[使用者] 表示您應該先拉下 [物件] 功能表，將滑鼠向下拖曳使 [新增] 變成反白顯示，再將滑鼠向旁邊移到 [新增] 子功能表上，選取其中的 [使用者]。

您會在本書各處看到以下格式的路徑參考：

```
<server-root>/dps-<hostname>/...
```

<server-root> 是指預設的安裝目錄，<hostname> 代表安裝 Directory Proxy Server 的主機名稱。例如，如果安裝目錄是 /usr/sunone/servers，而主機名稱是 testmachine，實際的路徑就會是：

```
/usr/sunone/servers/dps-testmachine/. . .
```

本手冊所指定的所有路徑都依照 UNIX 格式。如果您使用的是 Windows NT 架構的目錄伺服器，就應該在本指南出現 UNIX 檔案路徑的時候，改成對等的 NT 檔案路徑。

相關資訊

除了本指南以外，Directory Proxy Server 說明文件集還包括：

- **Sun ONE Directory Proxy Server 版本資訊。** 這些版本資訊包含關於 Directory Proxy Server 版本的重要資訊。另外還包含了關於新功能、增強、已知問題的資訊以及其他最新的消息。在開始使用 Directory Proxy Server 之前請先閱讀本文件。
- **Sun ONE Directory Proxy Server 安裝指南。** 本指南包含安裝 Directory Proxy Server 的程序，附帶需求以及調整資訊。

您可以在下列網際網路位置找到其他有用的 Sun ONE 資訊：

- 線上產品說明文件 - <http://docs.sun.com>
- 產品支援與狀態 - <http://www.sun.com/service/support/software/>
- Sun Enterprise Services for Solaris 修補檔案和支援 - <http://www.sun.com/service/>
- 開發者資訊 - <http://www.sun.com/developers/>
- 支援與訓練 - <http://www.sun.com/supporttraining>
- 產品基本資料 - <http://www.sun.com/software/>

協助工具功能

以 Java™ Foundation Classes (JFC) 為基礎的 Sun ONE Directory Proxy Server 主控台支援協助性軟體與技術，讓殘障人士更容易使用本軟體。本附錄描述 Sun ONE Directory Proxy Server 主控台的協助工具功能，以及為了使文件更容易使用，而針對文件集所做的改進。

主控台協助工具功能

在以下所述的協助工具功能中，大部分功能只要透過使用 JFC/Swing! 元件就會自動提供。

容易了解的名稱與描述

所有物件都採用容易了解的名稱 (簡單明瞭地說明物件的用途)。協助性技術可以利用這些名稱將物件呈現給使用者。容易了解的描述是比較詳細的說明，視需要而提供有關物件的其他資訊。

可自訂的字型

文字窗格、功能表、標籤和資訊訊息中的字型樣式和大小都可以由使用者自行訂制。雖然本軟體使用色彩編碼的方式傳達訊息，但這並不是唯一的方式。

動態 GUI 佈局

動態佈局讓使用者能夠指定 Directory Server 視窗的大小和位置，或指定由使用者的設定來決定。

鍵盤游標控制元件

這個協助工具功能是專為無法使用滑鼠的使用者所提供的。只要點按 Tab 鍵，就可以在元件之間移動輸入焦點，按 Shift-Tab 則以反方向移動焦點。方向鍵讓使用者不用滑鼠也能夠在樹狀目錄上移動。

透過程式設計的方式將焦點暴露出來，使協助性軟體可以追蹤焦點及焦點的變更。

非文字元素的對等文字

以影像呈現程式元素時，這些以影像表達的資訊也有對等的文字。

對等的指令行介面

主控台大部分的功能都可以用指令行叫出。本指令行介面有完整的說明文件。

說明文件協助工具功能

Sun ONE Directory Proxy Server 5.2 文件集提供 PDF 和 HTML 兩種格式。本節描述 HTML 版本說明文件中的協助工具功能。

非文字元素的對等文字

連結或圖形都配有指定的替代文字標籤。凡是以圖形提供詳細描述的地方，也會提供這些描述的文字版本，可能在周圍的文字內，也可能在單獨的檔案內。

可以用協助性技術轉譯的表格

現在所有表格都包含描述性標題。周圍的文字也會提供表格內容的簡要描述。

Sun ONE Directory Proxy Server 简介

第 1 章 「Sun ONE Directory Proxy Server 概論」

第 2 章 「Sun ONE Directory Proxy Server 部署方式」

Sun ONE Directory Proxy Server

概論

本章為您介紹 Sun ONE Directory Proxy Server。本章包含下列各節：

- 簡介 (第 11 頁)
- Directory Proxy Server 功能組 (第 13 頁)

簡介

Sun ONE Directory Proxy Server 是電子商務解決方案之所有關鍵任務目錄服務的重要元件。Directory Proxy Server 是一個 LDAP 應用程式層通訊協定閘道，利用應用程式層負載平衡及容錯移轉的功能，提供強化的目錄存取控制、結構相容性及高可用性。

以功能來說，Directory Proxy Server 是在 LDAP 用戶端及 LDAP 目錄伺服器之間的「LDAP 存取路由器」。系統會根據 Directory Proxy Server 組態中定義的規則，將 LDAP 用戶端的要求篩選並導向至 LDAP 伺服器。也會根據 Directory Proxy Server 組態中定義的規則，篩選目錄伺服器傳來的結果，然後回傳給用戶端。此程式對 LDAP 用戶端而言完全透明，他們連線到 Directory Proxy Server 的方式與連線到任何 LDAP 目錄伺服器一樣。

Directory Proxy Server 是獨一無二的產品，為 Extranet 與 Intranet 目錄基礎架構提供高可用性、安全性以及用戶端相容性功能，包括：

- 自動負載平衡
- 透明的伺服器容錯移轉及容錯回復
- 自動跟隨轉介
- Extranet/Intranet 存取控制群組

- 安全的用戶端及伺服器驗證
- 動態查詢及回應篩選
- 動態結構對應
- 目錄或檔案類型的組態
- 可設定的記錄

Directory Proxy Server 可以和新的與現有的 LDAP 目錄基礎架構共存，並可互補所長，而且能與已部署在企業 Extranet 與 Intranet 的啓用目錄應用程式完全整合。您可部署本產品，以利用在客戶目錄基礎架構中現有的投資。Directory Proxy Server 能與支援 LDAP 的目錄伺服器互通。Directory Proxy Server 能與啓用及支援 LDAP 的目錄合用，不管是原生 LDAP 目錄、啓用 LDAP 的 X.500 目錄、或啓用 LDAP 的關聯資料庫。

Directory Proxy Server 實作 LDAPv3 網際網路規格，也支援較舊及功能較少的 LDAPv2 規格，以便與使用 LDAPv2、且已部署的啓用目錄用戶端應用程式相容。Directory Proxy Server 在 UNIX 及 Windows NT 平臺上會以獨立系統伺服器程式的形式執行。本伺服器具有多個執行緒，故可處理上千個 LDAP 用戶端要求，並同時將存取控制規則及通訊協定篩選規則套用到每個要求上。

Directory Proxy Server 可協助組織保護自己私密的目錄資訊，未經授權就無法存取，同時讓這些組織在公佈自己的公司資訊時亦能維護其安全性。Directory Proxy Server 可用來在 LDAP 目錄上設定複雜的存取控制原則，例如控制誰可以在目錄資訊樹狀目錄 (DIT) 的不同部分上，執行不同類型的作業。您也可以設定允許 Directory Proxy Server 禁止執行特定類型作業 (下載大量網頁的人及自動尋檢程式收集資訊時，所常執行的作業)。

Directory Proxy Server 與網頁代理伺服器不同，是以反向代理伺服器的模式操作。它不會將連線從防火牆後的用戶端轉送到網際網路上任意的伺服器；也不會快取搜尋結果。這主要是因為對資料套用存取控制規則的問題。目前只有在維護存取控制措施的 LDAP 目錄伺服器中才會這樣做。Directory Proxy Server 並不包含目錄伺服器存取控制的概念。

Directory Proxy Server 功能組

Directory Proxy Server 功能組提供特別的功能：高可用性、負載平衡、容錯移轉、類似防火牆的安全性以及主從架構相容性。

高可用性

Directory Proxy Server 在一組複製的 LDAP 目錄伺服器之間，提供自動負載平衡及容錯移轉與容錯回復功能，用來支援高可用性目錄部署作業。對於 Extranet 與 Intranet 環境來說，常常需要確定關鍵任務的啓用目錄用戶端及應用程式能全天候存取目錄資料。Directory Proxy Server 會維護所知範圍內所有目錄伺服器的連線狀態資訊，也能在一組已設定的目錄伺服器上，以動態方式執行 LDAP 操作的比例負載平衡。如果一個以上的目錄伺服器故障，負載就會按比例重新分配到剩下的伺服器。目錄伺服器重新上線時，負載就會以動態方式按比例重新配置。

例如，假設將目錄伺服器 A 設定成接收 40 百分比的 LDAP 用戶端負載、伺服器 B 是 20 百分比、伺服器 C 是 20 百分比、伺服器 D 是 20 百分比。如果目錄伺服器 B 失敗，Directory Proxy Server 會辨識出伺服器 A 的負載設定成伺服器 C 及 D 的二倍，然後會從伺服器 B 重新分配 20 百分比的負載，使伺服器 A 現在接收 50 百分比、伺服器 C 是 25 百分比、伺服器 D 是 25 百分比。伺服器 B 恢復時，Directory Proxy Server 會自動偵測出來，然後回復到四個伺服器原始設定的負載百分比。

網路層 IP 負載平衡裝置無法存取 LDAP 通訊協定層。然而，Directory Proxy Server 會將負載平衡與存取控制、查詢篩選以及查詢導向功能整合，並可自行決定應用程式層存取控制及 LDAP 導向。

負載平衡

您必須利用第 7 章「定義及管理內容物件」中所述的負載平衡內容，在 Directory Proxy Server 中設定負載平衡。Directory Proxy Server 能通訊的每個後端目錄伺服器，都設定成接收某個百分比的總用戶端負載。然後 Directory Proxy Server 會自動將用戶端查詢分配給不同的後端伺服器，以符合組態中定義的負載標準。如果某個伺服器故障，Directory Proxy Server 就會在可用的伺服器之間，根據各個負載百分比，按照比例分配各個伺服器的負載百分比。如果所有的後端 LDAP 伺服器都故障，Directory Proxy Server 就會開始拒絕用戶端的查詢。

Directory Proxy Server 是根據工作階段處理負載平衡。這表示選擇將用戶端查詢導向到特定伺服器的決策功能，會對每個用戶端工作階段套用一次，尤其是在用戶端工作階段開始時。所有該工作階段後續的用戶端查詢，都會導向到工作階段開始時所選擇的伺服器。

Directory Proxy Server 可負載平衡的後端 LDAP 伺服器數量，需視幾個因素而定，例如執行 Directory Proxy Server 的主機大小、可用的網路頻寬、Directory Proxy Server 接收到的各個查詢、用戶端工作階段的長度以及 Directory Proxy Server 的組態。一般來說，如果大部分的工作階段存活時間都很短，而且查詢都需要大量運算，則 Directory Proxy Server 能支援的伺服器就會比較少。需要大量運算的查詢必須檢查整個訊息，例如使用「屬性重新命名內容」(第 92 頁)中所說明的屬性重新命名功能時。

Directory Proxy Server 使用監視程式來檢查後端伺服器的健康狀況，包括只能以 SSL 通訊的伺服器。如果使用負載平衡，本功能就會自動啟用。Directory Proxy Server 每 10 秒就會對其後端目錄伺服器執行匿名搜尋作業，搜尋 Root DSE。如果其中一個故障或未回應，Directory Proxy Server 就會將其從可以使用的負載平衡伺服器組中移除。伺服器又可以使用時，就會將其再加入這個組裡面。

容錯移轉

Directory Proxy Server 會在連線嘗試收到連線拒絕的錯誤或逾時時，偵測到伺服器何時故障。由於這二個情形都是在工作階段的初始階段發生，而且當時沒有為該工作階段處理任何作業，所以如果有可以透明使用的伺服器，Directory Proxy Server 就會容錯移轉至另一個伺服器。如果是連線嘗試逾時，用戶端取得回應的時間就可能延遲過久。如果突然失去 Directory Proxy Server 及後端伺服器之間的連線，Directory Proxy Server 就會對所有待執行的作業將 LDAP_BUSY 錯誤傳回給受到影響的用戶端。然後 Directory Proxy Server 會將該用戶端連線容錯移轉至另一個目錄伺服器。

為了避免 Directory Proxy Server 變成目錄部署的單一失效點，我們建議您至少使用二個 Directory Proxy Server，並在前面新增 IP 設備。

安全

Directory Proxy Server 提供彈性的外部目錄存取控制機制，強化目錄伺服器提供的基本存取控制措施。存取控制機制允許不同的使用者及使用者群體，與特定的存取群組產生關聯，並對此存取群組套用系統管理員定義的安全限制及查詢篩選條件。系統管理員可根據 LDAP 驗證資訊、IP 位址、網功能變數名稱、及其他標準，控制存取項目的作業。

Directory Proxy Server 提供的重要安全功能，是保護 LDAP 用戶端與 LDAP 目錄伺服器之間建立的連結數量。您可以設定讓 Directory Proxy Server 監視許多特定測量項目，以使 LDAP 目錄伺服器不會受到連線攻擊；同時用戶端操作數量、用戶端在每個連線中能要求的操作數量以及特定用戶端群組的連線數量。也能讓無法使用的用戶端逾時。

您可設定讓 Directory Proxy Server 的指定測量項目不能超過特定臨限制。Directory Proxy Server 會監視這些測量項目，並確定不能超過臨限值。Directory Proxy Server 會保留幾個測量項目，例如特定主機開啓的連線數量、在特定工作階段上執行的操作數量等等，以限制可能發生的大量下載目錄及阻絕服務的攻擊。「建立系統組態實例」(第 53 頁)將詳細描述這些參數組態。

您也可以禁止特定類型的一般篩選條件，例如 (cn=A*) 或 (cn>A)，以便允許 Directory Proxy Server 限制大量下載的行為。第 6 章「建立及管理群組」中有更多如何設定篩選條件進行篩選的詳細資料。

Directory Proxy Server 允許已驗證的用戶端變更目錄服務的存取控制措施。如此一來，就算已驗證的用戶端在安全網路之外，也允許他們存取更多的目錄資訊。

Directory Proxy Server 支援 Secure Socket Layer (SSL) 傳輸通訊協定，提供資料防護功能。例如，您可設定 Directory Proxy Server，讓從受到保護網路外部存取您目錄服務的所有用戶端，都必須建立 SSL 工作階段。在 Directory Proxy Server 中設定 SSL 的詳細資料，請參閱「設定安全」(第 137 頁)。

這些功能可協助防範「阻絕服務」的攻擊與「流量攻擊」，這些攻擊方式目前在業界中極為常見。如果 Directory Proxy Server 偵測到已到達臨限值，就會開始拒絕對目錄伺服器的連線，並防範目錄伺服器受到攻擊且失效。

主從架構相容性

Directory Proxy Server 根據 LDAP 辨別名稱 (DN) 及群組存取權限，決定查詢導向的方式，包括根據驗證憑證識別行動使用者。Directory Proxy Server 會自動跟隨 LDAP 轉介 (可能由目錄伺服器傳回)，以支援極為分散且可擴充的目錄服務。自動跟隨轉介是大規模目錄部署形式的重要優點，讓您在必須以實體方式在一組目錄伺服器之間分散目錄資訊時，分散的目錄在使用者看來卻像是一個邏輯目錄。Directory Proxy Server 提供一個功能，可以用邏輯的方式聯合分散的目錄，以支援這類部署方式，進而支援可擴充的分散目錄服務。

Directory Proxy Server 支援任何符合 LDAPv2 或 LDAPv3 的用戶端應用程式。並支援結構重寫的功能，以使不一定符合目錄伺服器結構、且本身結構固定的用戶端應用程式能配合。例如，Microsoft Outlook™ 電子郵件用戶端有固定的結構，規定目錄伺服器要實作 Microsoft 定義的屬性，可能不符合企業本身較寬鬆的結構要求。

結構重寫的能力允許目錄系統管理員實作寬鬆目的的企業結構，然後將該結構的特定元素，以動態方式對應到功能較少的用戶端應用程式所要求的屬性類型組。Directory Proxy Server 則不預設結構，接受龐大標準所定義的任何屬性類型及物件類別，以及業界臨時制定的結構定義，包括 RFC1274、X.520、X.521、LIPS、PKIX、inetOrgPerson 及 DEN。

Sun ONE Directory Proxy Server

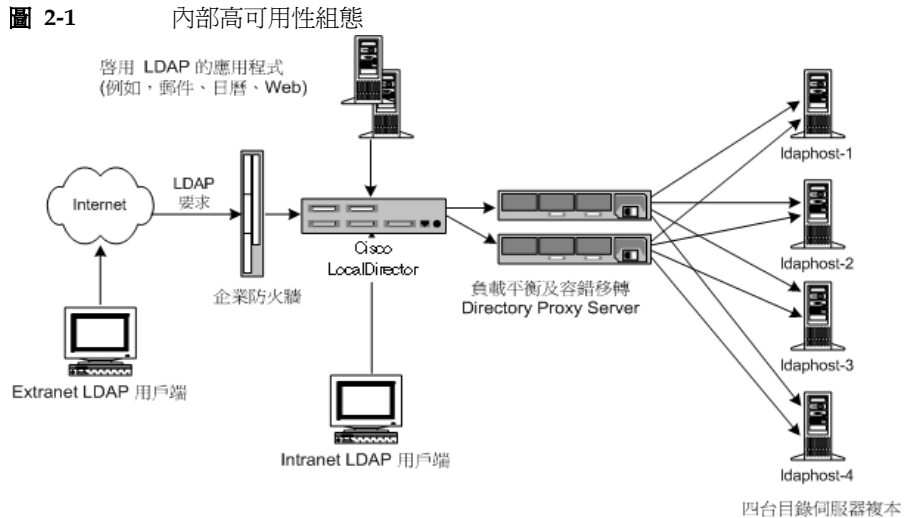
部署方式

根據您的運算環境，部署 Sun ONE Directory Proxy Server 的方法可能有幾種。本章描述並說明一般的部署方式，包括：

- 內部高可用性組態 (第 17 頁)
- 分散式 LDAP 目錄基礎架構 (第 18 頁)
- 集中式 LDAP 目錄基礎架構 (第 20 頁)
- 部署有單一防火牆的 Directory Proxy Server (第 23 頁)
- 部署有兩個防火牆的 Directory Proxy Server (第 25 頁)

高可用性組態

圖 2-1 所示的組態中，客戶已部署一個 LDAP 基礎架構僅供內部企業使用。外部網路沒有存取任何企業 LDAP 服務的需求。客戶已經部署了企業防火牆，會拒絕從防火牆外、向內部 LDAP 服務發出的任何存取要求。從內部發出的所有用戶端 LDAP 要求，都必須利用 Cisco LocalDirector 經由 Directory Proxy Server (才能有高可用性功能)，此處僅為範例，說明 IP 封包切換能確保用戶端能至少存取一個 Directory Proxy Server。客戶禁止任何人 (除了執行 Sun ONE Directory Proxy Server 的主機之外) 直接存取目錄伺服器，您可以使用防火牆來保護執行目錄伺服器及 Directory Proxy Server 的主機，以達成此目的。



分散式 LDAP 目錄基礎架構

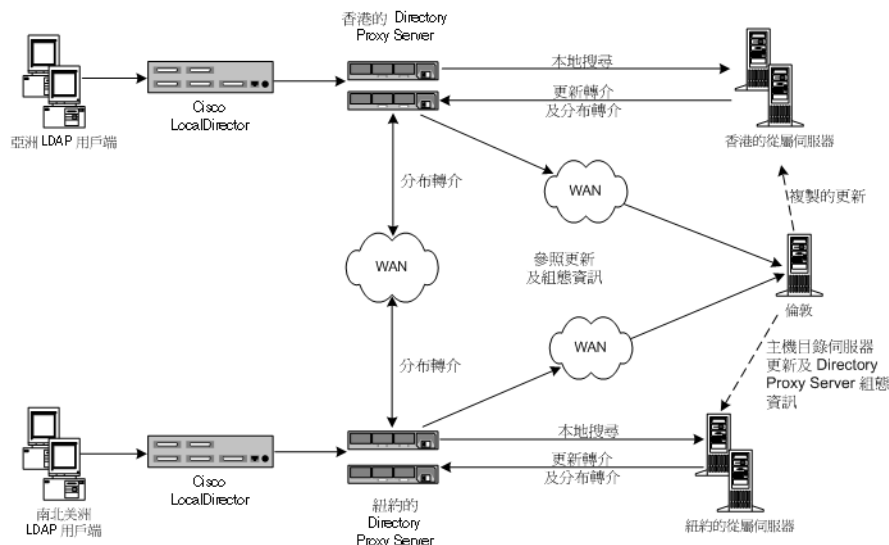
以下各節說明 Directory Proxy Server 在分散式 LDAP 目錄基礎架構中的角色：

- 客戶案例
- 客戶部署
- LDAP 要求流程

客戶案例

圖 2-2 所示的組態中，某大型金融機構的總部在倫敦，資料中心則在倫敦、紐約及香港。目前員工可使用的資料大部分都集中在倫敦的舊型 RDBMS 儲存庫。金融機構用戶端群體對這些資料發出的所有存取要求，都是透過廣域網路 (WAN)。該金融機構的這種集中模式碰到了擴充及效能問題，並決定改成分散式資料模式。該金融機構也決定要同時部署 LDAP 目錄基礎架構。此處所討論的資料已視為「關鍵任務」，因此應以高可用性、容錯的基礎架構來部署。分析用戶端應用程式設定檔後，發現各地區用戶端群體所存取的資料，有 95% 是各區群體所特有，因為該資料是以客戶為基礎。亞洲的用戶端鮮少存取北美洲的客戶資料，但是偶爾還是會有。用戶端群體也需要偶爾更新客戶資訊。

圖 2-2 分散式 LDAP 目錄基礎架構



客戶部署

由於結果顯示 95% 是本地資料存取，所以金融機構決定將 LDAP 目錄基礎架構依地理區域分散。該機構在各個地理位置部署多個目錄取用者伺服器（這些地理位置例如香港、紐約、倫敦；圖表中並未顯示倫敦取用者伺服器）。每個取用者伺服器設定成只存放該地區的客户資料。歐洲及中東的客户資料存放在倫敦的取用者伺服器中，南、北美洲的客户資料存放在紐約的取用者伺服器中，亞太地區的客户資料存放在香港的取用者伺服器中。這種部署方式將本地用戶端群體過於龐大的資料需求放在各群體中。此舉可大幅改善集中模式的效能，因為用戶端要求是在當地處理，所以降低了網路的額外負荷；當地的目錄伺服器以有效率的方式分割目錄基礎架構，所以增加目錄伺服器的效能及擴充性。每一組取用者目錄伺服器，都設定成如果用戶端提交更新要求或其他地方資料的搜尋要求，就會傳回轉介。

LDAP 要求流程

系統透過 Cisco LocalDirector，將用戶端 LDAP 要求傳送給 Sun ONE Directory Proxy Server。此處的 LocalDirector 產品僅為範例，說明 IP 封包切換能確保用戶端一定至少能存取一個 Directory Proxy Server。在本地部署的 Directory Proxy Server 一開始會將所有要求導向存放本地客户資料的本地目錄伺服器陣列。

Directory Proxy Server 實例設定成讓目錄伺服器陣列負載平衡，所以提供自動容錯移轉及容錯回復功能。本地目錄及透過 Directory Proxy Server 傳回用戶端的適當回應，滿足了用戶端對本地客戶資訊的搜尋要求。本地目錄伺服器將轉介傳回 Directory Proxy Server，初步滿足用戶端對「外地」客戶資訊的搜尋要求。

此轉介包含 LDAP URL，指向依地區分散的適當 Directory Proxy Server 實例。本地的 Directory Proxy Server 代表本地用戶端處理此轉介，並將搜尋要求傳送給適當的分散 Directory Proxy Server 實例。分散的 Directory Proxy Server 會將搜尋要求轉送給分散的目錄伺服器，並接收適當的回應。然後透過分散的本地 Directory Proxy Server 實例，將此回應傳回到本地用戶端。

本地目錄伺服器傳回的轉介，也初步滿足了本地 Directory Proxy Server 接收的更新要求。Directory Proxy Server 也是代表本地用戶端跟隨此轉介，可是這次是將更新要求轉送給倫敦的供應者目錄伺服器。供應者目錄伺服器將更新套用到供應者資料庫，並透過本地的 Directory Proxy Server 將回應傳送回本地用戶端。然後供應者的目錄伺服器會將更新向下傳送給適當的取用者伺服器。

所有的 Sun ONE Directory Proxy Server 都設定成啓動並在供應者目錄伺服器中尋找自己的組態。此舉允許您依地理位置分散多個 Directory Proxy Server 實例，但是能集中管理組態。

集中式 LDAP 目錄基礎架構

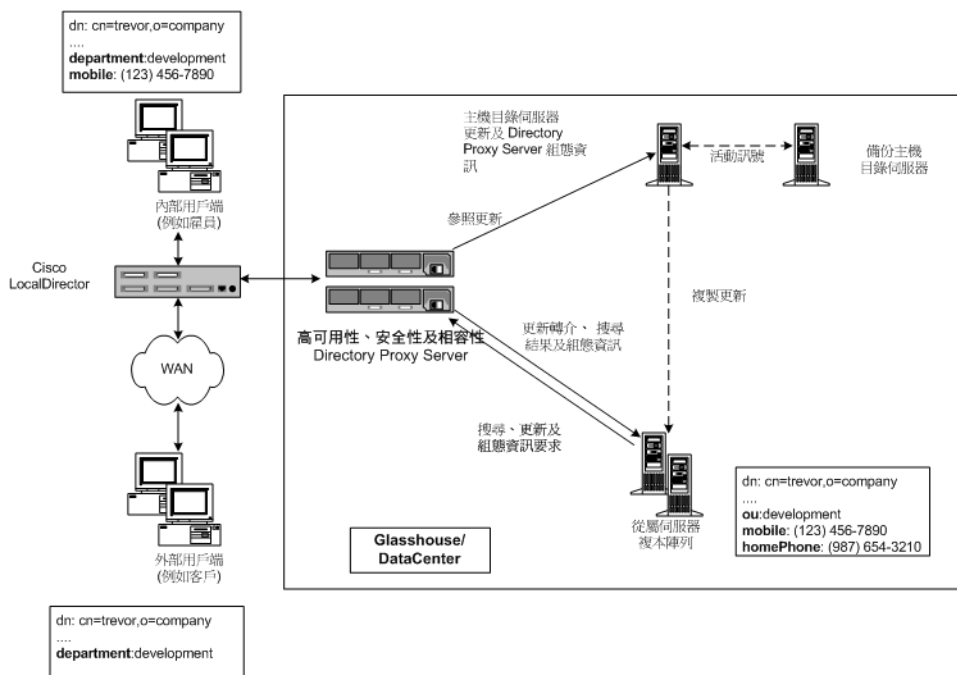
以下各節說明 Directory Proxy Server 在集中式 LDAP 目錄基礎架構中的角色：

- 客戶案例
- 客戶部署
- LDAP 要求流程

客戶案例

圖 2-3 描述的是客戶與員工遍佈全球的大型國際企業，該企業想要部署全企業的电子電話簿，以降低印刷紙本電話簿的成本、提升企業資訊的正確性、並節省自然環境資源。電子電話簿資訊必須讓客戶及員工都能使用，並且有適當的存取控制措施。而且要全天候都能使用，又因為客戶與員工散佈全球各時區，所以將這個特色視為關鍵任務。

圖 2-3 集中式 LDAP 目錄基礎架構



客戶部署

該國際企業決定部署集中式 LDAP 目錄基礎架構，以部署電子電話簿。在本實例中選擇集中式部署，是因為電子電話簿僅供企業員工參考。此並非客戶資料庫，雖然目的是讓客戶存取某些資訊。目前認為預估的目錄資料庫大小（大約 200,000 個項目）不足以要求更複雜的分散式部署模式，因為擴充性及效能都不會是問題。

由於有高可用性的要求，該企業決定部署多個取用者目錄伺服器副本，由單一供應者目錄伺服器提供。為了消除單一供應者目錄伺服器所衍生的單一失效點問題，此企業部署了備份供應者目錄伺服器。

部署 Sun ONE Directory Proxy Server 有三個理由。首先要在所有 LDAP 用戶端及目錄伺服器副本陣列之間，提供負載平衡及自動容錯移轉及容錯回復功能。其次要能分辨外部及內部的用戶端，並依此設定適當的存取控制措施。第三要讓使用電子電話簿的 LDAP 用戶端之間，以及目錄伺服器之間相容。除了利用自訂建立的電子電話簿應用程式以外，LDAP 用戶端也利用許多現成的啓用 LDAP 應用程式，內附

固定結構需求。這些結構需求不一定符合此企業設計的目錄結構，所以需要基本的結構屬性對應作業。此外，用戶端使用的啓用 LDAP 應用程式，並非全都能正確處理目錄伺服器傳送的轉介。Sun ONE Directory Proxy Server 設定成代表用戶端跟隨這些轉介。

LDAP 要求流程

系統會透過 Cisco LocalDirector，將所有的用戶端要求（不管是從內部或外部用戶端發出，也不管是搜尋要求或更新要求）傳送給 Directory Proxy Server 實例。此處的 LocalDirector 產品僅為範例，說明 IP 封包切換能確保用戶端一定至少能存取一個 Directory Proxy Server。部署多個 Directory Proxy Server 實例是為了確保沒有單一失效點問題。Directory Proxy Server 實例會在陣列中所有取用者目錄伺服器之間，負載平衡用戶端傳送的所有要求。Directory Proxy Server 也會偵測任何取用者伺服器的失效情形，並容錯移轉至陣列中可使用的取用者伺服器。

由於取用者伺服器是唯讀的副本，所以設定成在從用戶端接收更新要求時，會傳回 LDAP 轉介。此轉介包含 LDAP URL，指向供應者目錄伺服器。目錄伺服器傳回轉介時，Directory Proxy Server 會辨識出來，並代表用戶端跟隨此轉介。此舉會連結至供應者目錄伺服器，並將更新要求傳送至此。供應者目錄伺服器將更新套用到供應者資料庫，並透過 Directory Proxy Server 將回應傳送回用戶端。然後供應者的目錄伺服器會將更新向下傳送給適當的取用者伺服器。

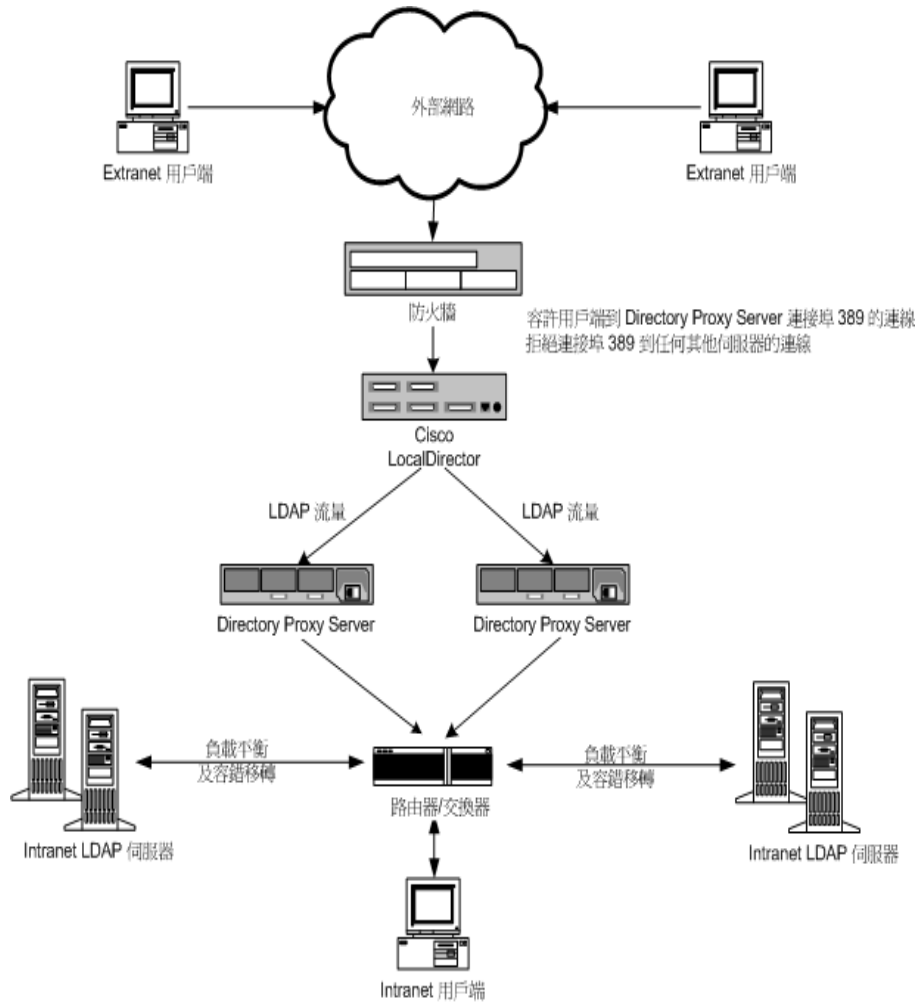
用戶端傳送的搜尋要求會透過 Directory Proxy Server，導向至取用者目錄伺服器副本陣列。您可設定讓 Sun ONE Directory Proxy Server 先「檢查」這些搜尋要求，再傳送給目錄伺服器，並篩選掉哪些要求不符合特定用戶端群組組態的存取控制措施及安全規則，並執行必要的對應作業。您也可設定讓 Directory Proxy Server「檢查」目錄伺服器傳回的搜尋結果，再執行適當的篩選及對應作業。在圖 2-3 所示的範例中，內部及外部的用戶端已要求搜尋屬於 Trevor 的項目。Directory Proxy Server 將這些傳入的要求都用相同方式處理，不管用戶端類型。目錄伺服器順利執行要求，並將 Trevor 項目傳回給 Directory Proxy Server。Directory Proxy Server 已經設定好，會根據原始要求是從內部或是外部用戶端發出，而用不同的方式操作搜尋結果。如果是外部用戶端，就會篩選掉項目中的行動電話號碼及家用電話號碼欄位，因為這些資料不適合讓客戶知道。還要注意 ou: development 屬性 / 值已經對應到 department: development。這是必要的，因為用戶端用來存取目錄的應用程式之一（例如 Outlook、Outlook Express）有固定的結構元素，它們並不符合部署在企業目錄伺服器中的結構元素。如果是內部用戶端，就會判斷行動電話號碼是很重要的資料元素，要公佈給員工，家用電話號碼就不是。如果是內部用戶端，Directory Proxy Server 的設定，就只會篩選掉家用電話號碼，讓用戶端看到行動電話號碼。請注意，系統也會執行將 ou 屬性對應到 department（部門）屬性的功能。

所有的 Sun ONE Directory Proxy Server 都設定成啓動並在供應者目錄伺服器中尋找自己的組態。此舉允許從一個目錄集中管理多個 Directory Proxy Server 組態。

部署指南- 防火牆的 Directory Proxy Server

您的組織的防火牆必須依圖 2-4 所示來設定，僅允許 LDAP 用戶端存取執行 Directory Proxy Server 的機器及連接埠。通常 LDAP 用戶端會連線到 TCP 連接埠 389 上。這個動作會保護執行 Directory Proxy Server 的主機，使其不會受到用戶端未經授權即嘗試存取。此外，利用路由器切換將執行代理伺服器的主機放在自己的區域網路上，可保護您的內部網路不會受到阻絕服務攻擊，譬如以不必要的網路流量對網路進行流量攻擊。防火牆也應禁止 LDAP 存取「隱藏」LDAP Directory Server 的機器及連接埠，藉以保護 LDAP 目錄資料庫。

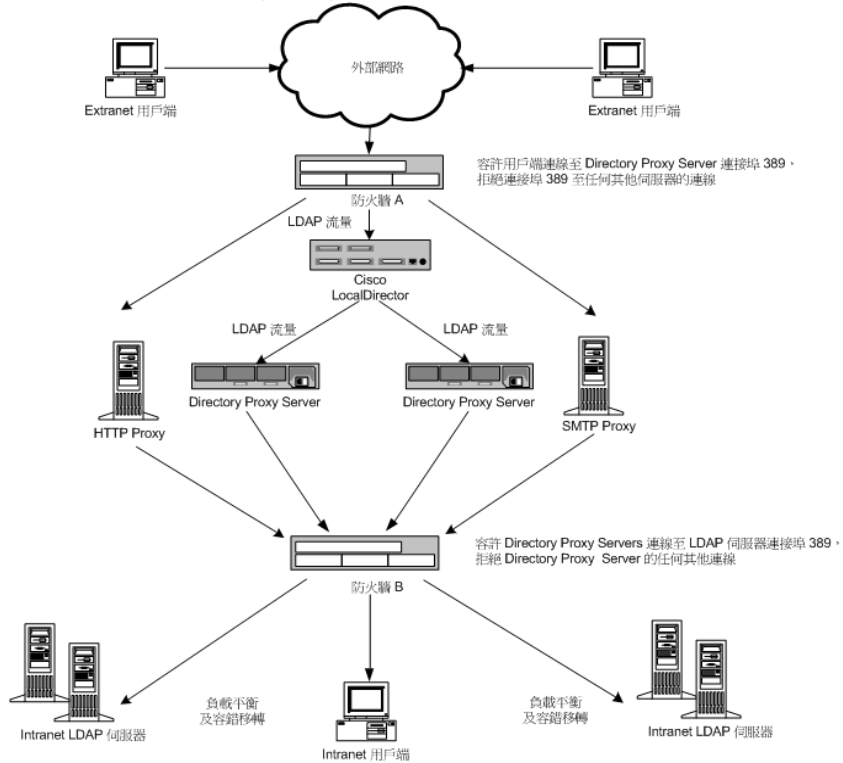
圖 2-4 Directory Proxy Server 有一個防火牆的設定



部署多個防火牆的 Directory Proxy Server

圖 2-5 所示的組態有圖 2-4 所示組態的所有優點，還有其他的安全性。安裝兩個防火牆可以在「代理伺服器」周圍建立控制區，允許網站管理員評估從外部網路發出的網路流量限制。此舉也確保如果「代理」伺服器之一受到入侵，不會被用來直接攻擊內部網路中的其他機器。防火牆 A 會設定成僅允許傳入封包通過（如果目標 IP 位址是處理 TCP 或 UDP 通訊協定的代理伺服器）。防火牆 B 會設定成僅允許從代理伺服器發出的封包通過（此機器需適合代理伺服器必須存取的伺服器）。

圖 2-5 Directory Proxy Server 有兩個防火牆的設定



主控台基本管理

第 3 章 「Directory Proxy Server 主控台簡介」

第 4 章 「啓動、重新啓動及停止 Directory Proxy Server」

第 5 章 「建立系統組態實例」

第 6 章 「建立及管理群組」

第 7 章 「定義及管理內容物件」

第 8 章 「建立及管理事件物件」

第 9 章 「建立及管理動作物件」

第 10 章 「設定及監視記錄」

第 11 章 「設定安全」

Directory Proxy Server 主控台簡介

安裝 Sun ONE Directory Proxy Server 後，您先要設定，才能與目錄部署合用，然後密切監視其活動。管理 Directory Proxy Server 時，您可以執行伺服器的特定工作，例如啓動、停止、及重新啓動伺服器；建立群組；設定伺服器以識別特定事件並執行適當動作；變更組態；執行任何例行伺服器維護工作；及監視記錄。

爲了讓您迅速簡便完成這些伺服器的特定工作，Directory Proxy Server 提供有 GUI 的系統管理工具：Directory Proxy Server [伺服器主控台] 及 Directory Proxy Server [組態編輯器主控台]，二者皆可從 [主控台] 存取。本章提供 Sun ONE 及 Directory Proxy Server 主控台的概論。

本章包含下列各節：

- Sun ONE Console 入門 (第 29 頁)
- 存取 Directory Proxy Server 主控台 (第 33 頁)

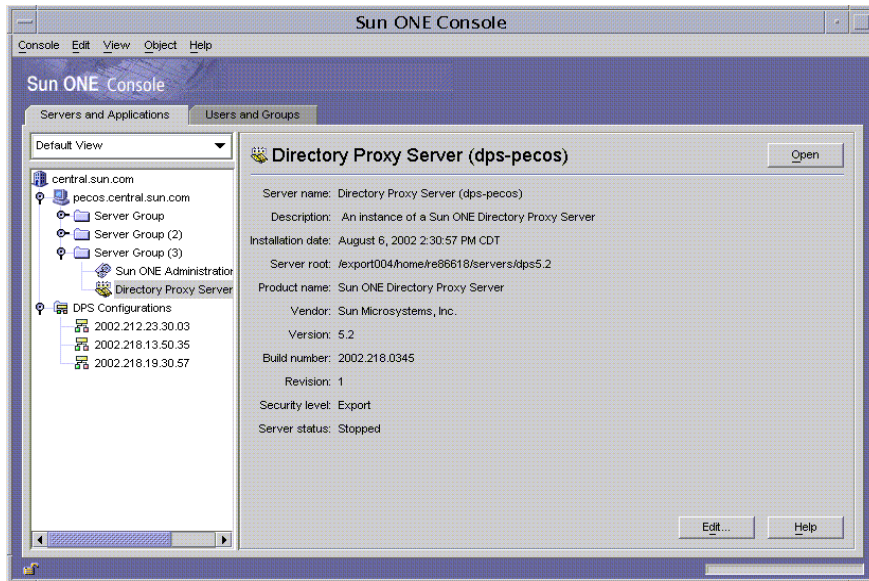
注意： 您可使用 Sun ONE Console 來管理不同的網路資源。然而，本章的焦點僅在使用 Sun ONE Console 對 Directory Proxy Server 進行系統管理。如需 Sun ONE Console 的完整資訊，請參閱「用 Sun ONE Console 管理伺服器」，包括在 Directory Proxy Server 說明文件內。您也可以從此網站取得此書的副本：<http://docs.sun.com/>

Sun ONE Console 介紹

Sun ONE Console 是獨立的 Java 應用程式，提供在組織組態目錄中註冊的所有網路資源 GUI 前端。此聯合管理介面，提供在網路上安裝的所有 Sun ONE 版本 5.x 伺服器實例存取點，以簡化網路管理作業。同樣地，也對使用者目錄提供了聯合管理介面，以簡化基本使用者及群組管理作業。

圖 3-1 顯示 Sun ONE Console 的 [伺服器及應用程式] 標籤，已選定某 Directory Proxy Server 實例。

圖 3-1 Sun ONE Console : [伺服器及應用程式] 標籤



[伺服器及應用程式] 標籤

針對任何指定的 Sun ONE Console 實例，組態資訊儲存在相同組態目錄中的資源組會定義該主控台能管理的網路限制，也就是，由受 Sun ONE Console 監視的最多主機與伺服器組。超級系統管理員 (管理組態目錄的人) 可在組態目錄中註冊的所有網路資源上設定存取權限。因此對於使用 Sun ONE Console 的指定系統管理員來說，實際可見的主機及伺服器可能更少，須視超級系統管理員設定的存取權限而定。

[伺服器及應用程式] 標籤顯示特定組態目錄中註冊的所有伺服器，讓您綜覽所控制的所有伺服器軟體及資源。您控制的項目會根據超級系統管理員為您設定的存取權限而定。

您可從此檢視方式，以單一操作動作在任意群組或伺服器叢集上執行工作。換句話說，您可在一部電腦上，利用 [伺服器及應用程式] 標籤管理在不同連接埠上安裝的一或多個伺服器。此外，您可連接兩下對應伺服器實例項目 (SIE) 的圖示，以存取個別伺服器的主控台 (或系統管理介面)。

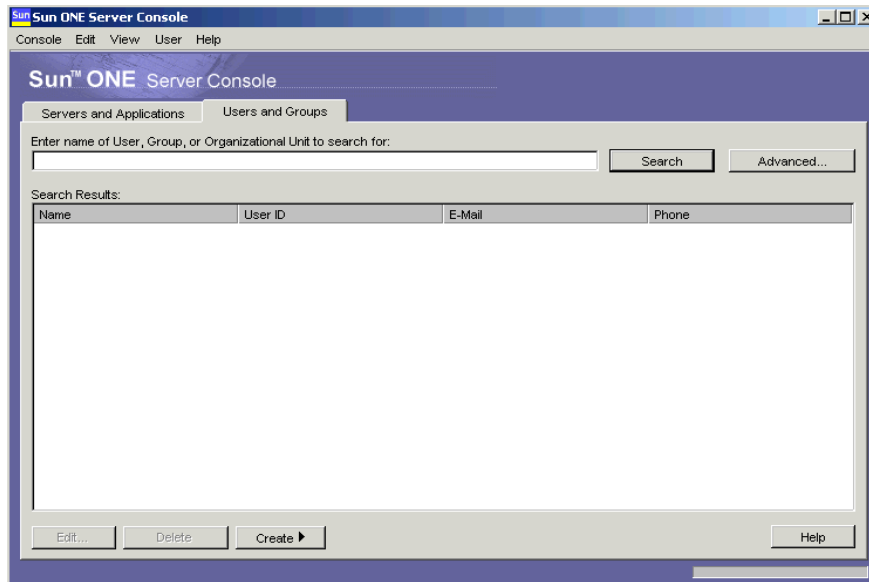
您可從 [伺服器及應用程式] 標籤完成 Directory Proxy Server 的不同工作。

- 啓動 Directory Proxy Server 伺服器主控台。
- 啓動 Directory Proxy Server 組態編輯器主控台 (您才能設定一組 Directory Proxy Server)。
- 設定 Directory Proxy Server 的存取權限。
- 啓動 Administration Server Console (您才能設定管理 Directory Proxy Server 的 Administration Server 實例)。

[使用者及群組] 標籤

[使用者及群組] 標籤 (如圖 3-2 所示) 管理個別使用者及群組的使用者帳號、群組清單及存取控制資訊。Sun ONE Console 架構內註冊的所有應用程式，在使用者目錄 (通常是全企業使用者資料的通用目錄) 中都會共用核心使用者及群組資訊。

圖 3-2 Sun ONE Console : [使用者及群組] 標籤



您可從此標籤完成不同的使用者與群組特定工作，例如這些：

- 新增、修改及刪除使用者目錄中的使用者及群組資訊。
- 在使用者目錄中搜尋特定的使用者及群組項目。

Sun ONE Administration Server

Sun ONE Administration Server 是啓用網頁 (HTTP) 的伺服器，讓您透過 Sun ONE Console 設定所有的 Sun ONE 伺服器，包括 Directory Proxy Server Administration Server (及組態目錄) 必須在您設定這些伺服器前執行。所有 Sun ONE 伺服器都包含 Administration Server，當您在伺服器群組中安裝第一個伺服器時，就會安裝 Administration Server。伺服器群組代表安裝在伺服器根目錄中的伺服器，由單一 Administration Server 實例管理。

您必須在 Sun ONE Console 登入畫面中輸入其 URL，才能存取 Administration Server；請參閱「步驟 1. 登入 Sun ONE Console」(第 34 頁)。本 URL 的依據，是您安裝 Directory Proxy Server 時所選擇的電腦主機名稱及連接埠號碼。URL 的格式如下：`http://<machine_name>.<your_domain>.<domain>:<port>`

您試圖存取 Administration Server 時，系統會提示您輸入使用者 ID 及密碼，以通過組態目錄的驗證。這些是您在電腦上安裝 Directory Proxy Server (或伺服器群組中的第一個伺服器) 及 Administration Server 時，所指定的系統管理員使用者名稱及密碼。一旦 Administration Server 執行，您就可使用 Sun ONE Console 管理群組中的所有伺服器，包括 Directory Proxy Server。

如需有關 Administration Server 的完整詳細資訊，請參閱用 *Sun ONE Console 管理伺服器*。若要在您的 Directory Proxy Server 安裝中找到本書的線上版本，請開啓此檔案：`<server-root>/manual/en/admin/ag/contents.htm`

您也可以從此網站取得此書的最新版：

<http://docs.Sun ONE.com/docs/manuals/console.html>

啓動 Administration Server

Directory Proxy Server 安裝程式會自動啓動您安裝時識別的 Administration Server 實例，以監視 Directory Proxy Server。如果您在安裝 Directory Proxy Server 後停止 Administration Server，就必須在能從 Directory Proxy Server 主控台管理 Directory Proxy Server 之前啓動此伺服器。

您可以從指令行或 Windows NT [服務] 面板啓動 Administration Server。

- 若要從指令行啓動 Administration Server：
在提示下輸入下列指令：`<server-root>/start-admin`
- Administration Server 在 Windows NT 系統中以服務的形式執行。您可使用 Windows NT [服務] 面板直接啓動服務。

上述所有方法，可在您安裝時指定的連接埠號碼上啓動 Administration Server。一旦伺服器在執行，您就可利用 Sun ONE Console 存取 Directory Proxy Server。

停止 Administration Server

未使用 Administration Server 時加以關閉是良好的安全實務作法。此舉可減少其他人變更您組態的機會。您可以從 Sun ONE Console、指令行或 Windows NT [服務] 面板關閉伺服器。

- 從 Sun ONE Console 關閉 Administration Server：
 - a. 登入 Sun ONE Console (請參閱「步驟 1. 登入 Sun ONE Console」(第 34 頁))。

- b. 在 [伺服器及應用程式] 標籤中，找到您要關閉的 Administration Server 實例，然後連接兩下對應的項目。

出現 Administration Server Console。

- c. 在 [工作] 標籤中按一下 [停止伺服器]。
- 從指令行關閉 Administration Server：
在提示下輸入下列指令：`<server-root>/stop-admin`
 - Administration Server 在 Windows NT 系統中以服務的形式執行；您可使用 Windows NT [服務] 面板直接停止服務。

存取 Directory Proxy Server 主控台

為從 Directory Proxy Server 主控台執行任何 Directory Proxy Server 系統管理工作，您必須先將其開啓。

- 步驟 1. 登入 Sun ONE Console
- 步驟 2. 開啓適當的 Directory Proxy Server 主控台

步驟 1. 登入 Sun ONE Console

您只有當對應的組態目錄及 Administration Server 執行時，才可啓動並使用 Sun ONE Console。如果伺服器尚未執行，請到指令行並啓動伺服器。如需關於從指令行啓動 Administration Server 的資訊，請參閱「啓動 Administration Server」(第 32 頁)。如需關於啓動組態目錄的資訊，請檢查 Sun ONE Directory Server 說明文件。

當您啓動 Sun ONE Console 時，會顯示登入視窗。您必須輸入系統管理員 ID、密碼、及 Administration Server (代表您有存取權限的伺服器群組) 的 URL (包括連接埠號碼)。您如果沒有網路上至少一個伺服器群組的存取權限，就不可使用 Sun ONE Console。

1. 利用適當的選項開啓 Sun ONE Console 應用程式：

- 若要在 UNIX 機器上取得本機存取權限，請在指令行提示下輸入下列指令：
`<server-root>/start-console`
- 若要在 Windows NT 機器上取得本機存取權限，請連按兩下桌面上 Sun ONE Console 圖示；您安裝第一個 Sun ONE 伺服器時，就會建立此圖示。

出現 [Sun ONE 主控台登入] 視窗。

2. 通過組態目錄的驗證。

使用者 ID。輸入您在機器上安裝 Administration Server 時，所指定的 *系統管理員 ID*。當您安裝第一個 Sun ONE 伺服器時就會安裝 Administration Server，或在安裝 Directory Proxy Server 時附帶安裝 Administration Server。

密碼。輸入您在 Directory Proxy Server 安裝階段在電腦上安裝 Administration Server 時，所指定的 *系統管理員密碼*。

Administration URL。本欄位應該顯示 Administration Server 的 URL。如果沒有您要的 Administration Server URL，請在本欄位中輸入 URL。本 URL 的依據，是您安裝 Directory Proxy Server 時所選擇的電腦主機名稱及 Administration Server 連接埠號碼。使用此格式：

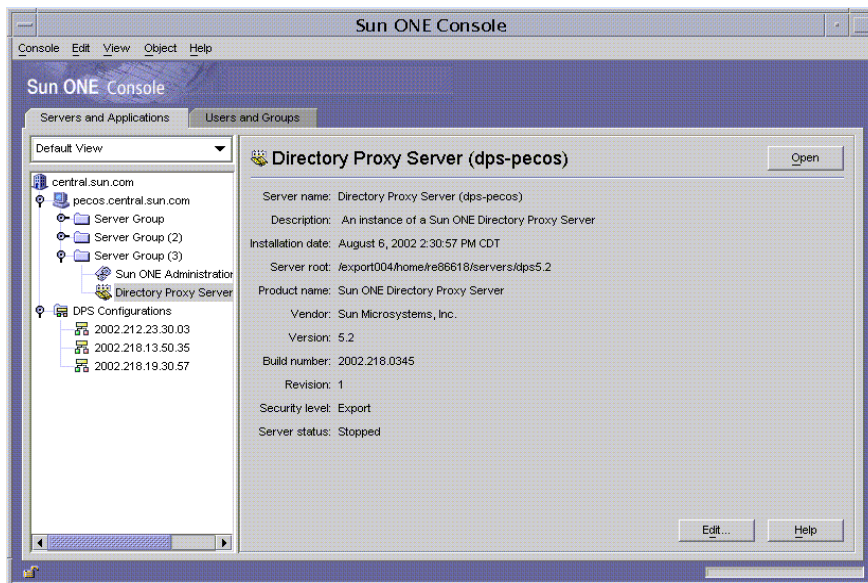
```
http://<machine_name>.<your_domain>.<domain>:<port_number>
```

例如，如果您的網域名稱是 sun，而您在主機上安裝的 Administration Server 稱爲 myHost，而且指定的連接埠號碼 12345，URL 的格式如下：

```
http://myHost.sun.com:12345
```

3. 按一下 [確定]。

Sun ONE Console 顯示您所控制的所有伺服器及資源清單。



步驟 2. 開啟適當的 Directory Proxy Server 主控台

在 Sun ONE Console 中，您會注意到 Directory Proxy Server 有二個項目，一個是 Directory Proxy Server 實例節點，另一個是 Directory Proxy Server 組態節點。Directory Proxy Server 實例節點對應 Directory Proxy Server 伺服器實例，Directory Proxy Server 組態節點對應多個 Directory Proxy Server 實例共用的組態。

每個節點都與有 GUI 的管理介面有關聯。

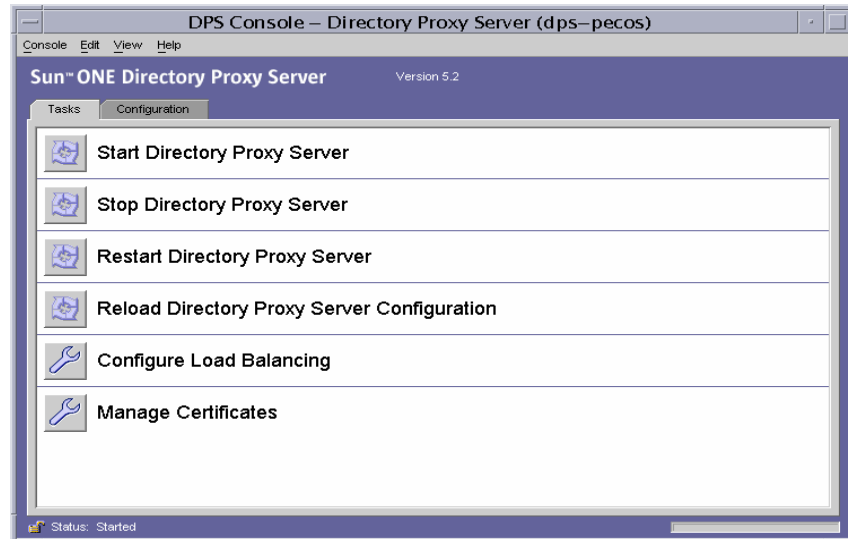
- Directory Proxy Server 主控台 - 本管理介面讓您建立、設定及管理 Directory Proxy Server 實例，例如啟動、停止、指定組態、監視記錄等等。您可利用 Directory Proxy Server 伺服器主控台從本機或遠端來存取伺服器。以 Directory Proxy Server 伺服器主控台建立及設定的 Directory Proxy Server，影響使用該組態的所有 Directory Proxy Server 實例。

- Directory Proxy Server 組態編輯器主控台 -- 多個 Directory Proxy Server 實例可共用邏輯及系統組態。Directory Proxy Server 實例共用組態資訊的能力，可簡化 Directory Proxy Server 叢集的管理作業。Directory Proxy Server 組態編輯器主控台是管理介面，讓您設定並管理 Directory Proxy Server 叢集。透過本介面編輯的項目，會影響使用已編輯組態的所有 Directory Proxy Server 實例。

開啓 Directory Proxy Server 伺服器主控台

一旦您登入 Sun ONE Console，就可開啓 Directory Proxy Server 伺服器主控台：在 Sun ONE Console 的瀏覽樹狀目錄中，展開包含 Directory Proxy Server 實例所屬伺服器群組的主機名稱、選取對應您要處理的 Directory Proxy Server 實例項目，然後按一下 [開啓]。Directory Proxy Server 主控台開啓 (圖 3-3)。

圖 3-3 Directory Proxy Server 伺服器主控台：[工作] 標籤

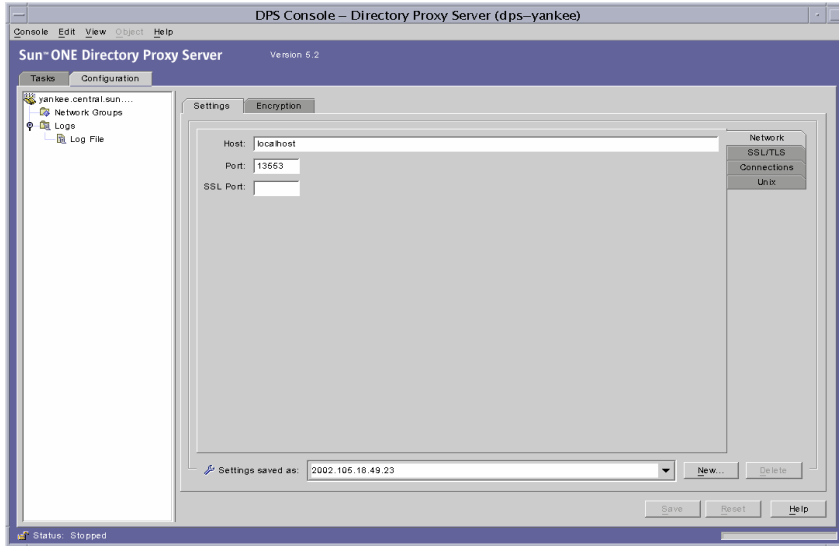


Directory Proxy Server 主控台有二個標籤 - [工作] 及 [組態]，每個都處理特定的系統管理領域。

[工作] 標籤讓您執行一般的工作，例如啟動、停止、重新啟動、及重新載入伺服器、重新分配或負載平衡不同的 LDAP 目錄及管理憑證。如需有關啟動、停止、及重新啟動 Directory Proxy Server 的詳細資訊，請參閱第 4 章「啟動、重新啟動及停止 Directory Proxy Server」。如需有關負載平衡的詳細資訊，請參閱第 7 章「定義及管理內容物件」。如需有關管理憑證的詳細資訊，請參閱第 11 章「設定安全」。

[組態] 標籤 (圖 3-4) 讓您檢視並修改特定實例的組態。

圖 3-4 Directory Proxy Server 伺服器主控台：[組態] 標籤 [設定] 標籤



[設定] 及 [加密] 標籤與設定此特定 Directory Proxy Server 實例之方式有關。

[設定] 標籤 (圖 3-4) 允許您設定以下參數：

網路。顯示 Directory Proxy Server 實體的 [主機名稱]、[連接埠] 及 [SSL 連接埠]。

SSL/TLS。顯示目前選取的組態，Directory Proxy Server 將其作為傳送及要求伺服器及用戶端之 SSL 憑證的位置。它也可為用戶端識別 Directory Proxy Server 的 SSL/TLS 版本，以及為 Directory Proxy Server 識別後端通訊的 SSL/TLS 版本。

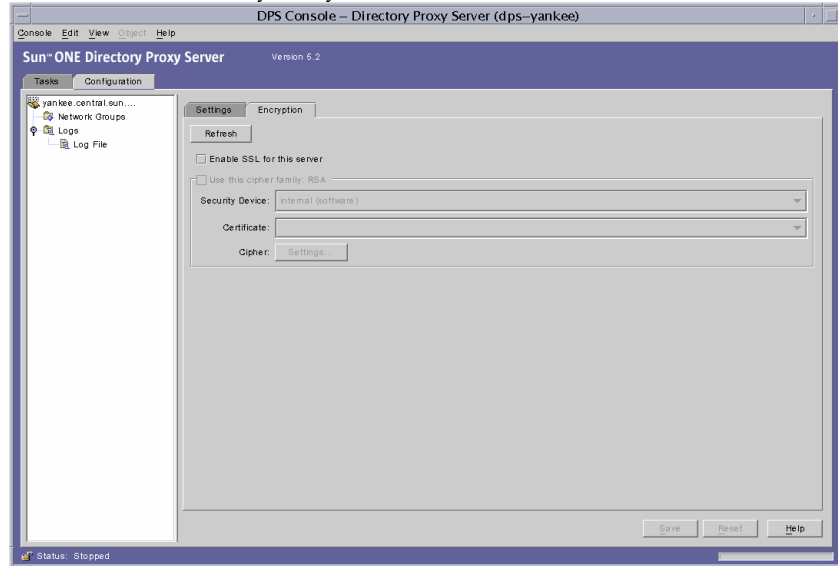
連線。顯示 Directory Proxy Server 連線積存值，允許您指定連線數量上限，以及設定連線集區逾時值。

Unix。顯示 Directory Proxy Server 實例的 UNIX 使用者 ID 及工作目錄。

設定值儲存為。允許您為下拉式方塊目前顯示的編輯工作階段指定 Directory Proxy Server 名稱值。您也可以建立新的 Directory Proxy Server 組態，或刪除舊 Directory Proxy Server 組態。

[組態] 標籤 [加密] 標籤 (圖 3-5) 讓您檢視並修改加密設定。

圖 3-5 Directory Proxy Server 伺服器主控台：[組態] 標籤 [加密] 標籤



[加密] 標籤允許您設定下列參數：

重新整理。允許您重新整理目前的畫面值，查看新增的憑證。

啓用此伺服器的 SSL。啓用這個 Directory Proxy Server 實例的 SSL 加密。

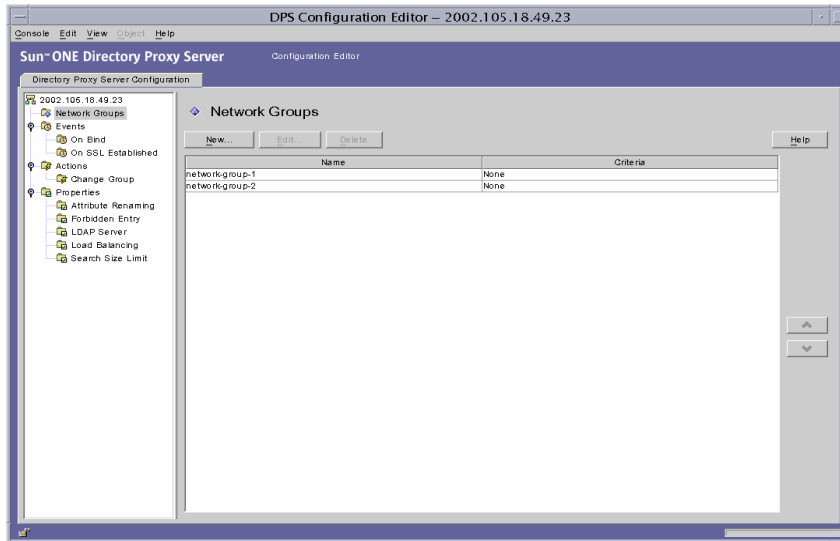
使用此加密系列 RSA。讓您設定此 Directory Proxy Server 實例的 [安全裝置]、[憑證] 及 [密碼設定]。

如需關於設定系統加密的資訊，請參閱「建立系統組態實例」(第 53 頁)。

開啓 Directory Proxy Server 組態編輯器主控台

一旦您登入主控台，就可開啓 Directory Proxy Server 組態編輯器主控台。在主控台的瀏覽樹狀目錄中，展開 Directory Proxy Server 組態節點，選取項目，然後按一下 [開啓]。Directory Proxy Server 組態編輯器主控台開啓 (圖 3-6)。

圖 3-6 Directory Proxy Server 組態編輯器主控台



左側的瀏覽樹狀目錄包含每個 Directory Proxy Server 之基本組態物件的節點。展開主要節點之一，可顯示每個物件子類型的樹狀目錄節點。按一下樹狀目錄節點，右側就會顯示表格，其中包含選取的樹狀目錄節點所指示之類型的所有現行物件。其順序很重要的物件表格（例如網路群組）有一組向上及向下按鈕，允許提高或降低個別物件的優先性。

表 3-1 列出瀏覽樹狀目錄中所示的組態物件。

表 3-1 Directory Proxy Server 組態編輯器主控台中的組態物件

組態物件類型	描述
網路群組	每個網路群組物件都可識別特殊用戶端群體，並指定要強制實施於符合該群組之用戶端的限制。 詳細資訊請參閱第 6 章「建立及管理群組」。
事件	事件物件是用來指定在預先判定的狀態時發生的條件。條件可附加到特定事件，而在滿足該條件時，Directory Proxy Server 就會採取某些動作。 詳細資訊請參閱第 8 章「建立及管理事件物件」。
動作	動作是用來指定發生事件時要採取的動作。詳細資訊請參閱第 9 章「建立及管理動作物件」。

表 3-1 Directory Proxy Server 組態編輯器主控台中的組態物件 (續)

組態物件類型	描述
內容	內容的功能是說明用戶端的更多特殊化限制。每個群組物件都可能包括由內容物件所定義的一組內容。 詳細資訊請參閱第 7 章「定義及管理內容物件」。

啓動、重新啓動及停止 Directory Proxy Server

本章描述如何啓動、停止及重新啓動 Sun ONE Directory Proxy Server 及如何檢查目前狀態。

本章包含下列各節：

- 啓動及停止 Directory Proxy Server (第 43 頁)
- 重新啓動 Directory Proxy Server (第 47 頁)
- 檢查 Directory Proxy Server 系統狀態 (第 49 頁)

注意： 只有當適當的 Directory Server (組態目錄中指出) 及 Administration Server 在執行時，才能利用 Directory Proxy Server 主控台。請務必在您安裝 Directory Proxy Server 時指定的連接埠上啓動 Administration Server。爲了將安全性風險降到最低，請在 Sun ONE Console 使用完畢後，將 Administration Server 關機。有關啓動及關閉 Administration Server 的說明，請參閱「Sun ONE Administration Server」(第 32 頁)。

啓動及停止 Directory Proxy Server

一旦安裝了 Directory Proxy Server，就會經常執行、監聽並接受要求；本伺服器會以 UNIX 常駐程式程序或 Windows NT 服務的形式執行，一般都在系統開機時啓動。

您可以用幾種方式啓動及停止 Directory Proxy Server。

- 從 Sun ONE Console (從本機及遠端)

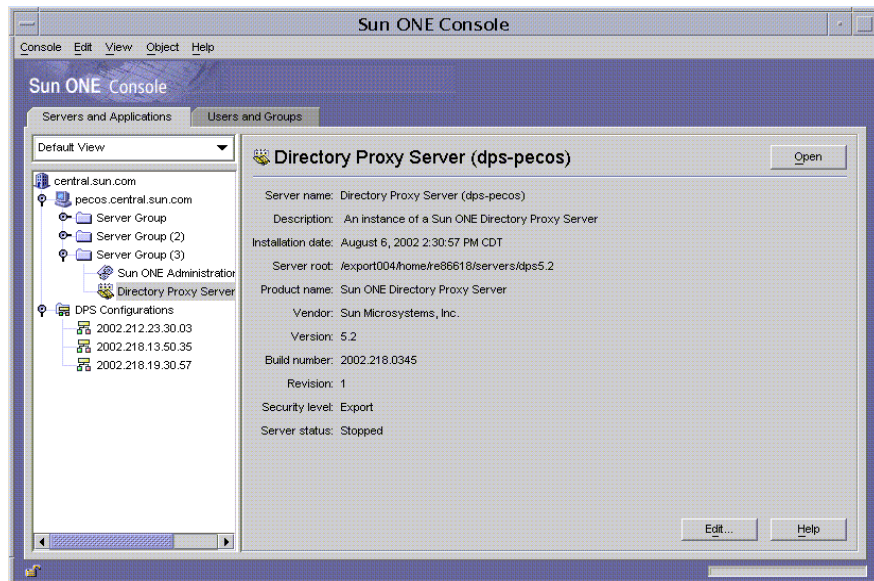
- 從命令列 (僅限本機)
- 在 Windows NT 系統上, 從 Windows NT [服務] 面板

請注意, 若停止 Directory Proxy Server, 就會完全關閉所有的元件、中斷服務, 直到再啟動此伺服器為止。如果主機當機或離線, 伺服器便會停止, 且正在處理的所有要求都會遺失。您必須再次啟動此伺服器才能還原服務。

從 Sun ONE Console 啟動及停止 Directory Proxy Server

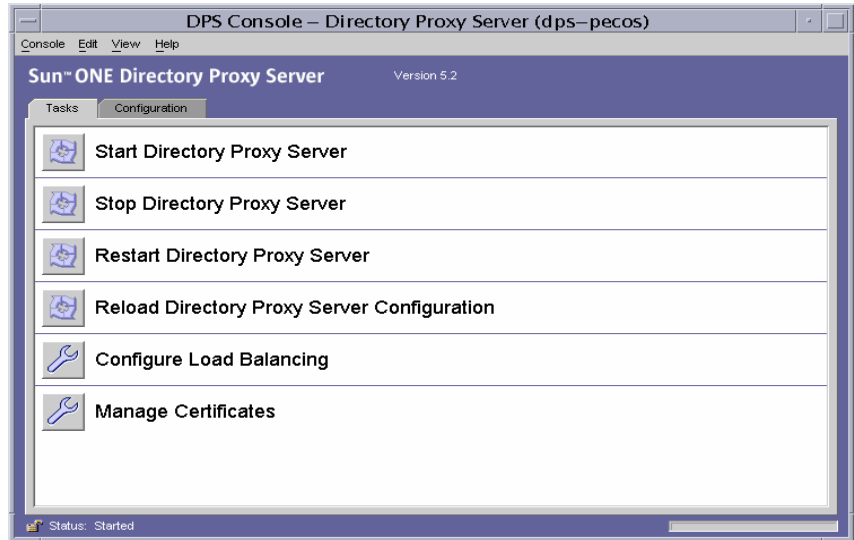
您可以利用 Sun ONE Console 來啟動及停止安裝在本機或遠端主機上的 Directory Proxy Server。若要啟動或停止 Directory Proxy Server：

1. 登入 Sun ONE Console (請參閱「步驟 1. 登入 Sun ONE Console」(第 34 頁))。
2. 在 [伺服器及應用程式] 標籤中展開主機名稱, 然後展開包含您要啟動的 Directory Proxy Server 實例的 [伺服器群組]。
3. 在瀏覽樹狀目錄中, 找到您要啟動或停止的 Directory Proxy Server 實例, 選取對應的項目, 然後按一下 [開啓]。



開啓 Directory Proxy Server [伺服器主控台]。

4. 在 [工作] 標籤中按一下 [啓動 Directory Access Router] 來啓動伺服器，或按一下 [停止 Directory Access Router] 來停止伺服器。



從命令列啓動及停止 Directory Proxy Server

若要從命令列啓動或停止 Directory Proxy Server：

1. 開啓連到伺服器的終端機視窗。
2. 在 UNIX 系統中，如果伺服器在小於 1024 的連接埠上執行，就以 root 登入；否則就以 root 或伺服器的使用者帳號登入。(依預設，如果 Directory Proxy Server 是以 root 執行，就會將自己的使用者 ID 變更成 nobody。)
3. 在命令列提示下輸入下列指令：

若要啓動 Directory Proxy Server：

```
<server-root>/dps-<hostname>/start-dps [.exe]
```

若要停止 Directory Proxy Server：

```
<server-root>/dps-<hostname>/stop-dps [.exe]
```

<server-root> 是保留 Directory Proxy Server 二進位檔案的目錄。您在安裝過程中會先指定這個目錄。

<hostname> 是安裝此 Directory Proxy Server 實例的主機名稱。

.exe 會指定副檔名；只有在 Windows NT 系統上執行此公用程式時才需要。

注意： 如果已經在執行 Directory Proxy Server，啟動指令就會失敗。先使用 stop-dps 指令，然後使用 start-dps 指令停止伺服器。

從 Windows NT [服務] 面板啟動及停止 Directory Proxy Server

如果您已經在 Windows NT 系統上安裝 Directory Proxy Server，便可從 Windows NT [服務] 面板啟動並停止伺服器（以服務方式）。Directory Proxy Server 服務有下列名稱：Sun ONE Directory Proxy Server。

若要從 Windows NT [服務] 面板啟動或停止 Directory Proxy Server：

1. 在您的桌面上選取 [開始] > [設定] > [控制台]。
2. 在出現的 [控制台] 視窗中連按兩下 [服務]。
3. 捲動服務清單，並找出對應到 Directory Proxy Server 實例的服務。
4. 若要啟動服務，請選取 Directory Proxy Server 實例，然後按一下 [啟動]。若要停止服務，請選取 Directory Proxy Server 實例，然後按一下 [停止]。

重新啟動 Directory Proxy Server

當您變更 Directory Proxy Server 的組態時，必須儲存變更才能將其儲存在組態目錄中。所有組態變更需要在您儲存變更後重新啟動 Directory Proxy Server 才行。如果必須重新啟動，主控台會提示您。

重新啟動期間 Directory Proxy Server 會重新讀取組態，並使用新組態進行以後的連線。已經建立的用戶端連線會繼續使用舊組態，直到用戶端中斷連線為止。只有 UNIX 平台上才有重新啟動的功能。在 Windows NT 上，重新啟動 Directory Proxy Server 就等於停止然後啟動 Directory Proxy Server。

您可以用兩種方式重新啟動 Directory Proxy Server：

- 從 Directory Proxy Server [伺服器主控台] (從本機及遠端)
- 從命令列 (僅限本機)

從命令列重新啟動 Directory Proxy Server

若要從命令列重新啟動 Directory Proxy Server：

1. 開啓連到伺服器的終端機視窗。
2. 在 UNIX 系統上，請以 root 或伺服器的使用者帳戶 (如果您原先以這種方式啟動伺服器) 登入。
3. 在命令列提示下輸入下列指令：

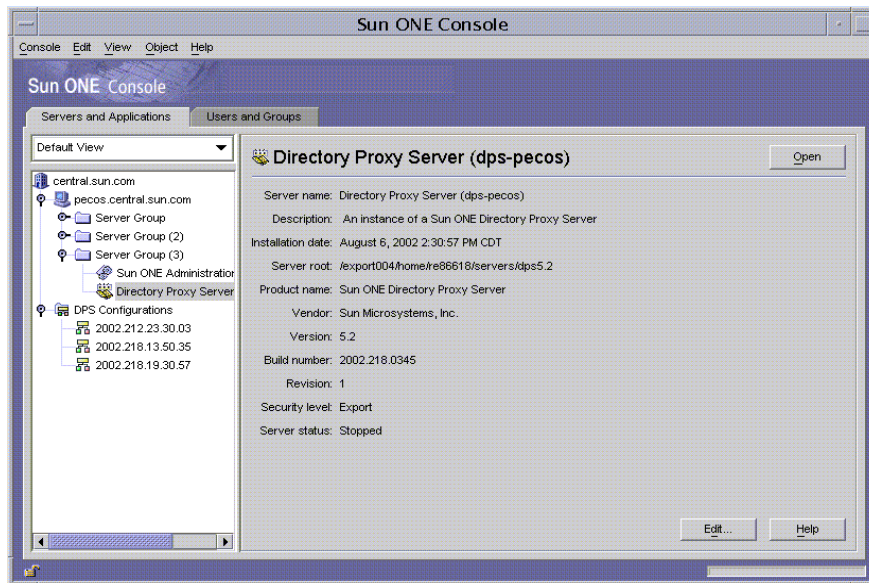
```
<server-root>/dps-<hostname>/restart-dps [.exe]
```

在 UNIX 平台從 Sun ONE Console 重新載入 Directory Proxy Server

您可以在 UNIX 平台上利用 Directory Proxy Server [伺服器主控台] 來重新載入安裝在本機或遠端主機上的 Directory Proxy Server。您在 UNIX 平台上變更 Directory Proxy Server 的組態時，重新載入 Directory Proxy Server 組態就會使變更生效。在 NT 平台上您必須重新啟動 Directory Proxy Server 組態。

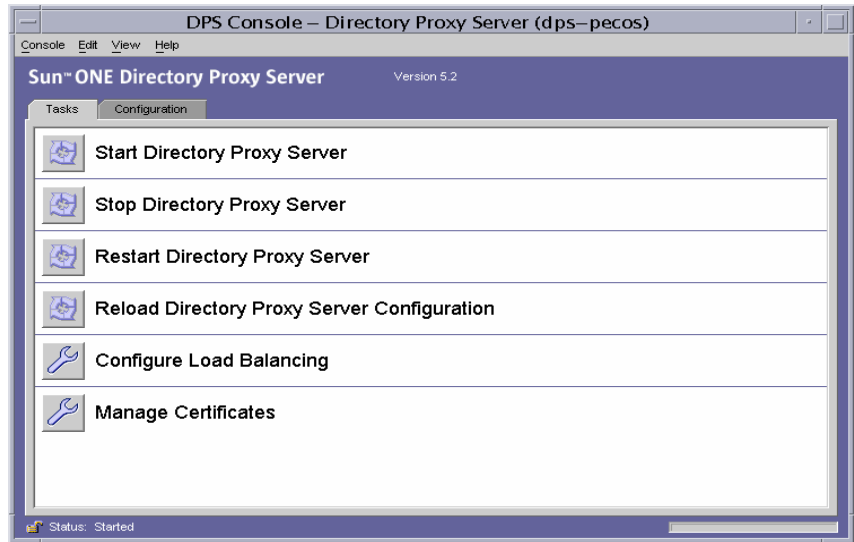
從 Directory Proxy Server [主控台] 重新載入 Directory Proxy Server：

1. 如果您還沒有檢視 Directory Proxy Server [伺服器主控台]，請登入 Sun ONE Console (請參閱 「 步驟 1. 登入 Sun ONE Console 」 (第 34 頁))。
2. 在 [伺服器及應用程式] 標籤中展開主機名稱，然後展開包含您要重新啟動的 Directory Proxy Server 實例的 [伺服器群組]。
3. 在瀏覽樹狀目錄中，找到您要啟動或停止的 Directory Proxy Server 實例，選取對應的項目，然後按一下 [開啓]。



開啓 Directory Proxy Server [伺服器主控台]。

4. 在 [工作] 標籤中按一下 [重新載入路由器組態] 來重新載入伺服器。



檢查 Directory Proxy Server 系統狀態

您可以用兩種方式檢查特定的 Directory Proxy Server 實例是啟動或是停止。

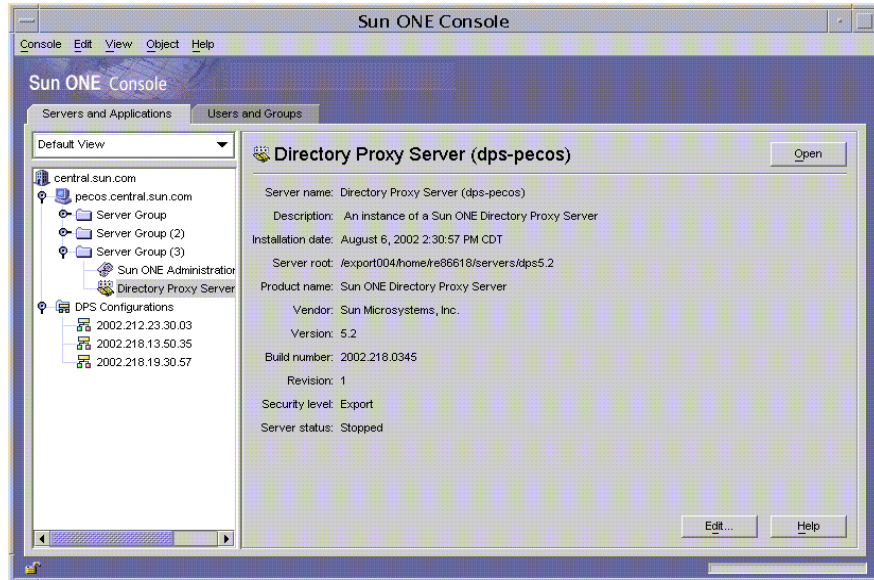
- 從 Sun ONE Console (從本機及遠端)
- 從命令列 (僅限本機)

從 Sun ONE Console 檢查 Directory Proxy Server 狀態

您可以利用 Sun ONE Console 得知特定的 Directory Proxy Server 實例是否在執行。

1. 登入 Sun ONE Console (請參閱「步驟 1. 登入 Sun ONE Console」(第 34 頁))。

2. 在 [伺服器及應用程式] 標籤中，選取對應到您要檢查的 Directory Proxy Server 實例的項目。



3. 在右邊窗格檢查 [伺服器狀態] 欄位。

如果選定的 Directory Proxy Server 實例正在執行，狀態就會是 [已啟動]。否則就會是 [警示]、[已停止] 或 [未知]。SIE 名稱成斜體字時，伺服器的狀態也會表示為 [已停止]。

從命令列檢查 Directory Proxy Server 狀態

若要從命令列得知特定的 Directory Proxy Server 實例是否正在執行：

1. 開啓連到伺服器的終端機視窗。
2. 在 UNIX 系統上，請以 root 或伺服器的使用者帳戶 (如果您原先以這種方式啟動伺服器) 登入。
3. 在命令列提示下輸入下列指令：

```
<server-root>/dps-<hostname>/status-dps [.exe]
```

從命令列啟動及停止 Directory Proxy Server

Directory Proxy Server 程式以 UNIX 常駐程式程序或 NT 服務的形式執行，一般都在系統開機時啟動。

在所有平台上，Directory Proxy Server 的啟動程式在下列位置：

```
<server-root>/dps-<hostname>/start-dps
```

啟動組態設定檔在下列位置：

```
<server-root>/dps-<hostname>/etc/tailor.txt
```

您可以下列位置中的指令檔啟動及停止 Directory Proxy Server：

```
<server-root>/dps-<hostname>
```

在 Windows NT 上應該使用 Windows NT [服務管理員] 來啟動及停止 Directory Proxy Server。在非 Windows NT 的平台上，Directory Proxy Server 只會產生一個核心影像以防當機 (如果其有效的使用者 ID 與真正的使用者 ID 相同)。因此，如果您要 Directory Proxy Server 產生核心，就必須將 `ids-proxy-sch-GlobalConfiguration` 物件類別中的 `ids-proxy-con-userid` 屬性，設定成與啟動 Directory Proxy Server 程序的使用者相同。依預設，如果 Directory Proxy Server 是以 `root` 執行，就會將自己的使用者 ID 變更成 `nobody`。

支援的標幟

表 4-1 描述啟動及停止指令檔支援的標幟。

表 4-1 啟動及停止指令檔支援的標幟

標幟	描述
-d	本標幟存在時，Directory Proxy Server 一次只會處理一個傳入連線，而且會把更詳細的內部追蹤資訊傳送給記錄檔。請不要在正常作業時使用本標幟，因為會讓 Directory Proxy Server 常駐程式無法脫離控制的終端機。
-D	本標幟告訴 Directory Proxy Server 要將更詳細的追蹤資訊傳送給記錄檔。Directory Proxy Server 仍將處理多個用戶端連線，並以常駐程式的形式執行。-d 及 -D 標幟應視為互相排斥。
-t < 啟動組態設定檔 >	本選項可用來指定其他的啟動組態設定檔。您必須指定組態設定檔的絕對路徑。

表 4-1 啟動及停止指令檔支援的標幟 (後續)

標幟	描述
-s	本選項告訴 Directory Proxy Server 要利用 LOG_DAEMON facility，將初始記錄訊息傳送給 syslogd。Windows NT 會忽略此標幟。如果沒有定義 dps_ROOT 環境變數，這個就是預設值。
-M	如果指定本標幟，Directory Proxy Server 就會產生另一個程序來自我監視。Directory Proxy Server 以不當的方式退出時，監視程序會在等候 30 秒後重新啟動 Directory Proxy Server。Windows NT 上沒有這個功能。
-r	本標幟的功能，是將值加入硬式編碼的登錄路徑後面。最後的登錄路徑會將 Directory Proxy Server 服務指向自己的組態資訊，譬如根目錄或實例根目錄名稱。在 Windows 系統上，您只能將一個 Directory Proxy Server 實例安裝在主機上。
-v	本標幟會列印 Directory Proxy Server 的版本資訊。本標幟在 Windows NT 上只能從命令列使用。

重新啟動 Directory Proxy Server

在 UNIX 平台上，您可以將 SIGHUP 通知傳送給 Directory Proxy Server，使其重新讀取自己的組態。如果順利重新讀取組態，Directory Proxy Server 會使用此新組態進行以後的連線。已經建立的用戶端連線會繼續使用舊組態，直到用戶端中斷連線為止。

若要通知 Directory Proxy Server 重新讀取自己的組態，請利用 `<server-root>/dps-<hostname>` 中的 `hup-dps` 指令。

某些屬性值不能用 HUP 通知 facility 變更。如果要變更下列組態參數，您必須關閉 Directory Proxy Server 然後再啟動。這些屬性包含：

```
ids-proxy-con-listen-port
ids-proxy-con-listen-host
ids-proxy-con-ldaps-port
ids-proxy-con-foreground
ids-proxy-con-listen-backlog
ids-proxy-con-ssl-cert
ids-proxy-con-ssl-key
```

此外，不能利用此 facility 變更 `ids-proxy-sch-LogProperty` 記錄內容。

在所有平台上，`restart-dps` 指令可在 `<server-root>/dps-<hostname>` 找到。重新啟動指令只會叫用前述目錄中的 `stop-dps` 及 `start-dps` 指令。

建立系統組態實例

系統參數會影響 Sun ONE Directory Proxy Server 的功能行爲。本章說明如何指定並儲存系統組態。

本章包含下列各節：

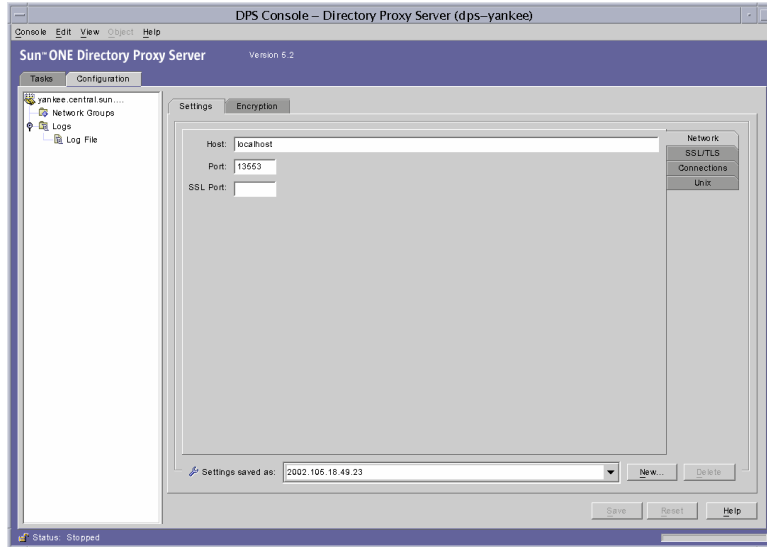
- 建立系統組態實例 (第 53 頁)
- 儲存組態 (第 59 頁)

建立系統組態實例

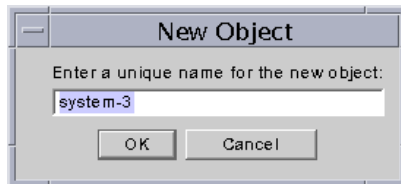
本節說明如何設定 Directory Proxy Server 實例的系統特定參數。若要建立系統組態的物件：

1. 存取 Directory Proxy Server 主控台；請參閱「存取 Directory Proxy Server 主控台」(第 33 頁)。

2. 在瀏覽樹狀目錄中，選取適當的 Directory Proxy Server 實例，再按 [開啓]。
在 Directory Proxy Server 主控台按 [組態] 標籤。



3. 按一下 [新增]。
出現 [新物件] 視窗。



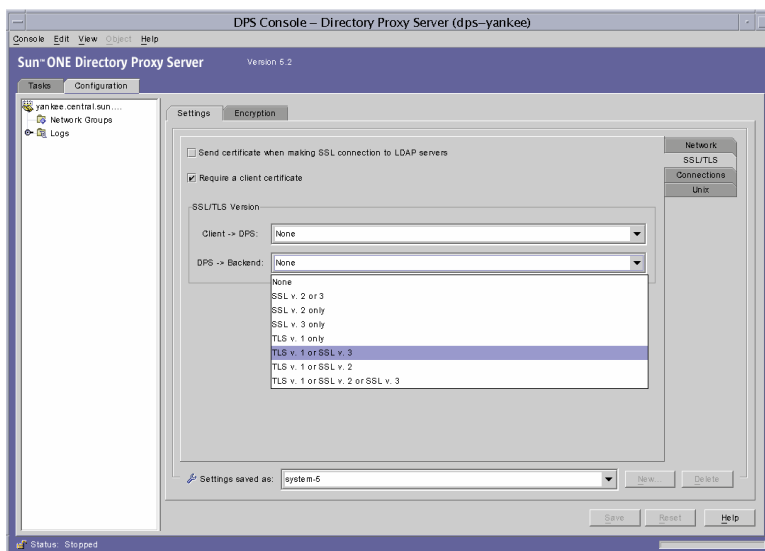
4. 在 [名稱] 欄位中，鍵入系統組態的名稱。名稱必須是獨一無二的英數字元字串。按 [確定]。
5. 在 [網路] 標籤中指定此系統組態的一般設定：

主機。輸入將監聽連線的 Directory Proxy Server 主機介面名稱。只有在執行 Directory Proxy Server 的主機上具備多個網路介面時，才需要此屬性。主機名稱預設為「localhost」，表示 Directory Proxy Server 將監聽所有可用的網路介面。指定「localhost」就會允許共用系統內容。

連接埠。輸入 Directory Proxy Server 將監聽傳入連線的連接埠號碼。此欄位的有效值為 1 到 65535。根據預設值，此值會設定為 389，作為 LDAP 的指定值。此連接埠號碼不能與在相同主機上執行的任何其他 LDAP 伺服器連接埠號碼相同。在 UNIX 平台上，必須以 root 身份啟動伺服器以監聽小於 1024 的連接埠號碼。

SSL 連接埠。輸入代表連接埠號碼的值，以監聽 LDAPS (LDAP over SSL) 連線。根據預設值，Directory Proxy Server 不會監聽來自 LDAPS 用戶端的連線。必須提供該值，以使用此非標準函數，來啓用用戶端發出的 LDAPS 連線 (如值為 636)。該值不能與主機的值相同。此選項也需要 TLS/SSL 組態，此組態位於 [加密] 標籤。

6. 按 [SSL/TLS] 標籤。



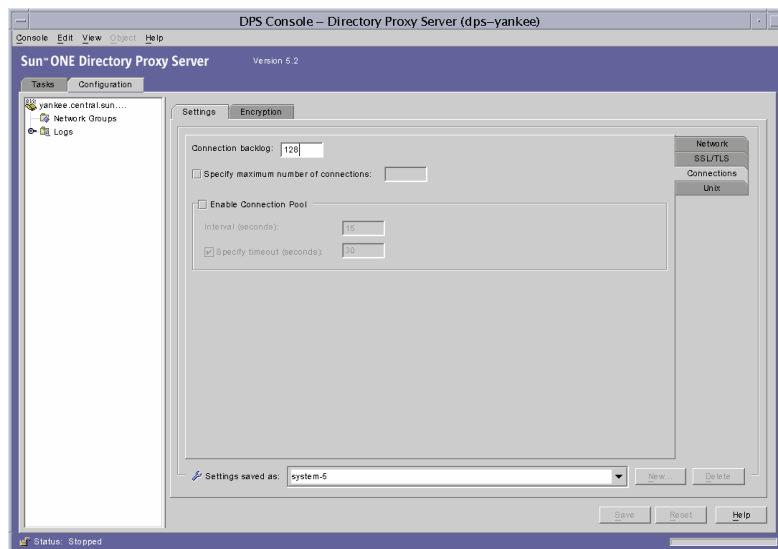
顯示預設組態，Directory Proxy Server 將其作為傳送及要求伺服器及用戶端之 SSL 憑證的位置。選取項目：

在進行連至 LDAP 伺服器的 SSL 連線時傳送憑證。如果您要讓 Directory Proxy Server 在進行 TLS 連線時，將其憑證傳送至後端 LDAP 目錄伺服器，請啓用此設定。根據預設值，此設定已停用。

需要用戶端憑證。啓用此設定以指定 Directory Proxy Server 將要求建立 SSL 工作階段的所有用戶端提交憑證鏈結。如果未提交憑證鏈結，則 Directory Proxy Server 將關閉連線。請注意，此選項不會影響 Directory Proxy Server 與後端伺服器之間的 SSL 工作階段。根據預設值，此設定已停用。

SSL/TLS 版本。 選取 [用戶端] > Directory Proxy Server 及 Directory Proxy Server > [後端] 旁的下拉式視窗，以選取各個情形適當的 SSL/TLS 版本。如果系統啓用 SSL，您就必須指定版本。

- 按 [連線] 標籤，並指定 Directory Proxy Server 維護其連線的方式。



顯示 Directory Proxy Server 連線積存值，允許您指定連線數量上限，以及設定連線集區逾時值。選取項目：

連線積存。 輸入大於零的值，以指定監聽通訊端佇列中，未完成之連線數量上限。預設為 128 個連線。最大值視基礎作業系統組態而定。

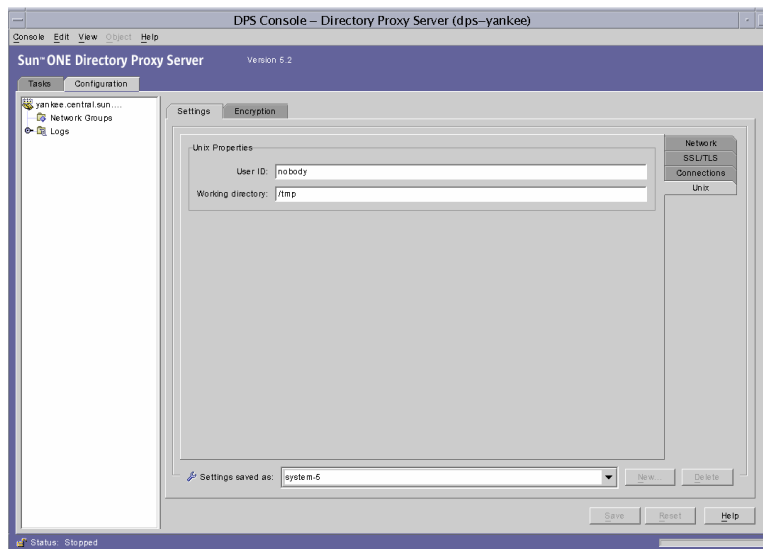
指定連線的最大數量。 選取此選項並輸入值 (大於零)，以指定 Directory Proxy Server 可接受的同時用戶端連線的數量上限。若要允許同時連線數量不受限制，請勿選取此選項。

啓用連線集區。 啓用 Directory Proxy Server 預先連線到目錄伺服器時，所使用的連線集區模組。設定值的預設為停用。如果啓用連線集區，則 Directory Proxy Server 會嘗試重新使用連至後端 LDAP 伺服器的現有連線。如果後端伺服器位於廣域網路 (WAN)，則切換此選項可使效能大幅增進。輸入下列值：

間隔。 輸入秒數 (不小於一)，可指定 Directory Proxy Server 採樣傳入要求以預測未來活動的間隔 (以秒計)。預設值是 15。

指定逾時。 選取此選項並輸入秒數 (不小於零)，可指定要等候多久 (以秒計) 才終止連至 LDAP 伺服器的閒置連線。如果未勾選此核取方塊，則不會套用逾時。預設值為 30。此值應小於後端 LDAP 伺服器的閒置連線逾時值。

8. 按 [UNIX] 標籤。

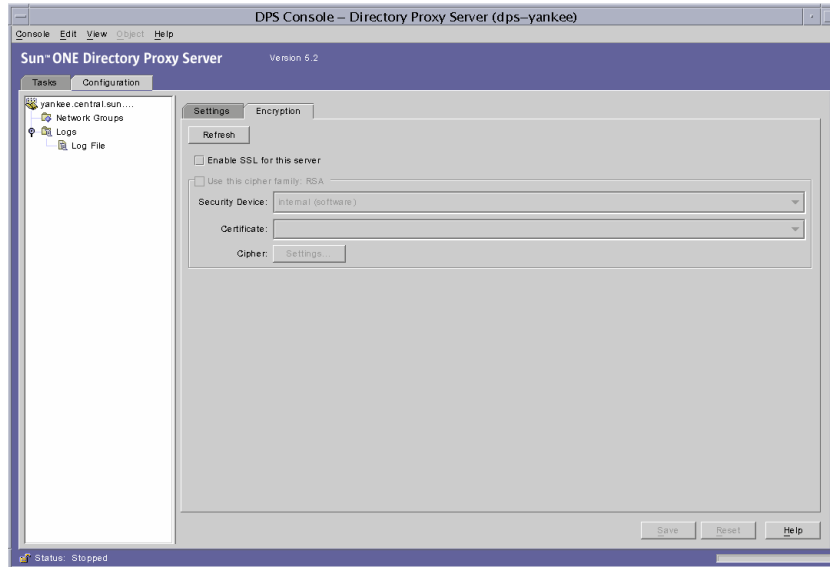


本面板包含關於 Directory Proxy Server 伺服器的屬性 (僅限 UNIX 環境) 。

使用者 ID。輸入將執行 Directory Proxy Server 的使用者 ID。如果將 Directory Proxy Server 執行為 *root*，則它會將其 *uid* 變更為此處指定的項目。預設是切換為 *nobody*。Windows NT 不適用此選項。

工作目錄。輸入應該執行 Directory Proxy Server 的目錄。Directory Proxy Server 會在啟動時，將其工作目錄變更為由此屬性指定的值的目錄。預設為 */tmp*。此屬性只在非 Windows NT 的平台上有效。

9. 選取 [加密] 標籤並設定啓用 SSL 通訊的 Directory Proxy Server。如需關於 SSL 通訊的伺服器設定資訊，請參閱設定安全。



[加密] 標籤允許您設定下列參數：

重新整理。 按一下可重新整理目前的畫面值。重新整理畫面可查看新建立的憑證。

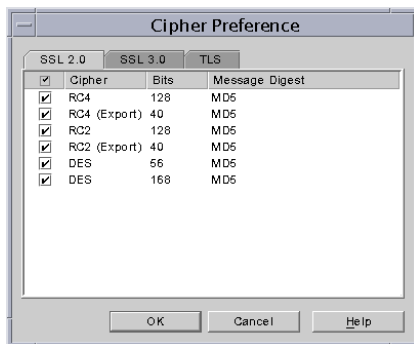
啓用此伺服器的 SSL。 選取此方塊，以啓用 Directory Proxy Server 透過安全連線進行監聽時，所需的 SSL/TLS 資訊。如果指定了 SSL 連接埠，則必須啓用此設定值，以儲存此組態。

使用此加密系列 RSA。 選取此方塊，以設定此 Directory Proxy Server 實例的 [安全裝置]、[憑證] 及 [密碼設定]

安全裝置。 按一下下拉式視窗選取可用的選項。預設為內部 (軟體)。

憑證。 按一下下拉式視窗選取可用的選項。

密碼。選取 [設定]，以設定 SSL 2.0、SSL 3.0 及 TLS 密碼偏好。按一下 [SSL 2.0]、[SSL 3.0] 及 [TLS] 標籤，並選取每個標籤想要的 [密碼] 旁的方塊。



10. 按一下 [儲存] 以儲存此物件。

Directory Proxy Server 組態已經修改，並提示您重新啓動依賴本組態的伺服器。現在還不要重新啓動伺服器。您可以將所有的組態都變更過後再進行重新啓動。

11. 重複步驟 3 至步驟 10，以建立其他物件。

12. 若要重新啓動伺服器，請參閱「重新啓動 Directory Proxy Server」(第 47 頁)。

注意： 如要在 [設定] 標籤中變更 [主機]、[連接埠] 及 [SSL 連接埠] 的欄位，則需要停止然後啓動 Directory Proxy Server。

有關停止然後啓動 Directory Proxy Server 的說明，請參閱「啓動及停止 Directory Proxy Server」(第 43 頁)。

儲存組態

dpsconfig2ldif 公用程式的功能是下載 Directory Proxy Server 組態，並將其儲存在 LDIF 檔案中。本公用程式可在下列位置找到：

```
<Install Root>/bin/dps_utilities/dpsconfig2ldif
```

本公用程式需要二個引數：

引數	意義
-t <i>filename</i>	<i>Filename</i> 是啓動組態檔的路徑。通常是 etc 目錄中的 tailor.txt 檔。

引數

`-o filename`

意義

輸出組態的檔案名稱。

建立及管理群組

當 LDAP 用戶端從 LDAP 目錄要求服務時，會連線到 Sun ONE Directory Proxy Server，從用戶端設定檔識別用戶端的存取權限、決定此用戶端是否能從目錄要求服務、執行所設定的限制，然後將要求轉送給適當的目錄。本章說明如何利用 Directory Proxy Server 組態編輯器主控台，來設定讓 Directory Proxy Server 識別用戶端並執行任何限制。

本章包含下列各節。

- 群組概論 (第 61 頁)
- 建立群組 (第 66 頁)
- 修改群組 (第 88 頁)
- 刪除群組 (第 89 頁)

群組概論

Directory Proxy Server 網路群組是了解 Directory Proxy Server 如何運作的關鍵 - 它們定義了 Directory Proxy Server 應如何識別 LDAP 用戶端，以及 Directory Proxy Server 應對符合該群組之用戶端強制實施哪些限制。確實了解 Directory Proxy Server 群組以利用其有效控制 LDAP 用戶端存取目錄的作業，是非常重要的。

您可以利用網路群組識別下列項目：

- 用戶端
- Directory Proxy Server 可從用戶端轉送要求到一組 LDAP 目錄。
- 用戶端在與其目錄組互動時，可執行的作業組。

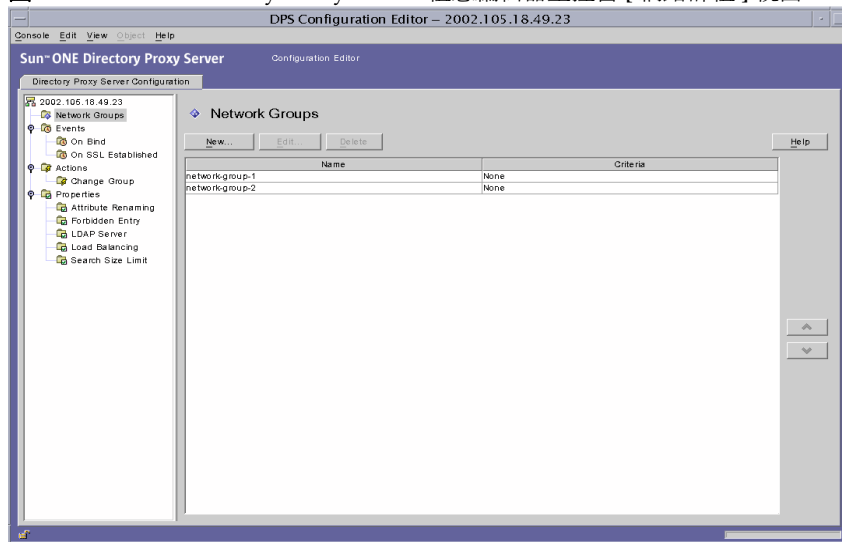
- 用戶端與其目錄組互動時，可存取資料。(因為 Directory Proxy Server 讓您隱藏目錄的特定項目並重新命名屬性，所以您可有效控制用戶端可看到目錄中包含的哪些資料。)

Directory Proxy Server 嘗試將連線的來源屬性與群組準則作比對，以決定用戶端的群組成員資格。伺服器以優先權的遞減排序 (從最高到最低的優先權) 檢查目前設定的群組。第一個符合網路群組準則的連線來源屬性可接收連線。因此，為一般及特定準則建立獨立的群組，並將最特殊到最一般的群組排定優先權，是非常重要的。

如果找不到與用戶端相符的群組，用戶端的要求會遭到拒絕，連線會關閉。所以 Directory Proxy Server 組態中一定至少會有一個群組項目。

群組的優先權排序，會根據其在 Directory Proxy Server 組態編輯器主控台 [網路群組] 視窗中的位置來指定 (請參閱圖 6-1)。在此視窗中，位於清單底端的群組，其優先權會較靠近頂端的群組來的低。未定義優先權相同群組的評估排序。

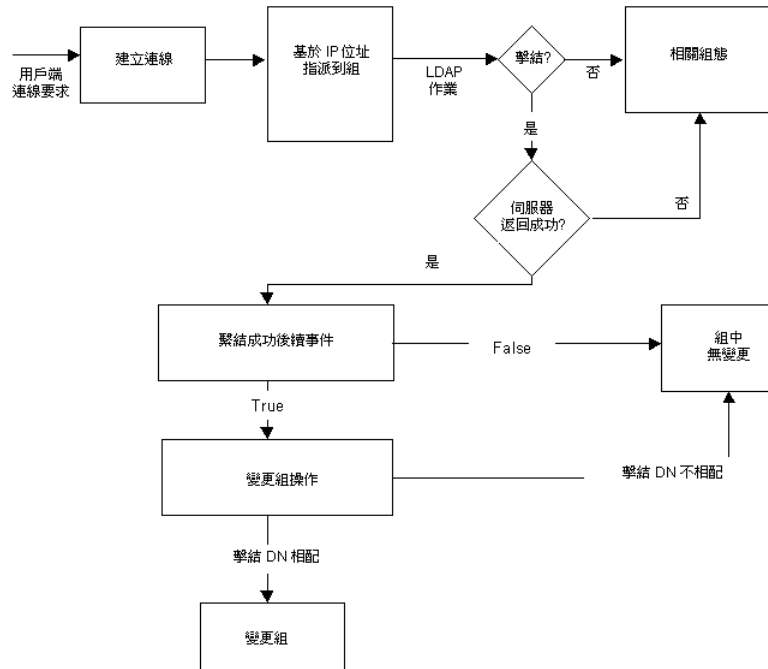
圖 6-1 Directory Proxy Server 組態編輯器主控台 [網路群組] 視窗



請注意，系統一開始會根據用戶端連線的網路位址，例如 IP 位址及 / 或網域名稱，將其分配到某個群組。他們會在連結成功之後變更其群組；如需詳細資訊，請參閱第 8 章「建立及管理事件物件」。一旦用戶端取得群組的成員資格，就表示群組的所有屬性都會套用到此用戶端。

圖 6-2 說明 Directory Proxy Server 如何評估群組，以回應用戶端的查詢。

圖 6-2 決定群組成員資格的 Directory Proxy Server 決策樹



群組的網路準則可依據下列項目：

- 主機的 IP 位址或網路遮罩
 - 單一 IP 位址 (例如, 129.153.129.14)
 - IP 四位元 / 符合位元 (例如, 129.153.129.0/24)
 - IP 四位元 / 符合四位元 (例如, 129.153.129.0/255,255,255,128)
- 主機的網域名稱
 - 完整名稱 (例如, box.eng.sun.com)
 - 尾碼名稱 (例如, .eng.sun.com)

請注意，如果用網域名稱尾碼規則來識別用戶端，請確定有設定 DNS，以將完全合格名稱傳回 DNS 查詢，如果傳回短名稱，本功能就沒有作用。

- 特殊
 - ALL (用於 catch-all 群組。)
 - 0.0.0.0 (用於初始成員資格不納入考慮的群組，例如，用戶端連結時才會用來切換的群組。)

爲了更瞭解 Directory Proxy Server 如何評估群組，請參閱表 6-1 列出的範例群組。此處顯示五個群組，按照特定到一般網路準則建立，並以優先權的遞減排序列出。

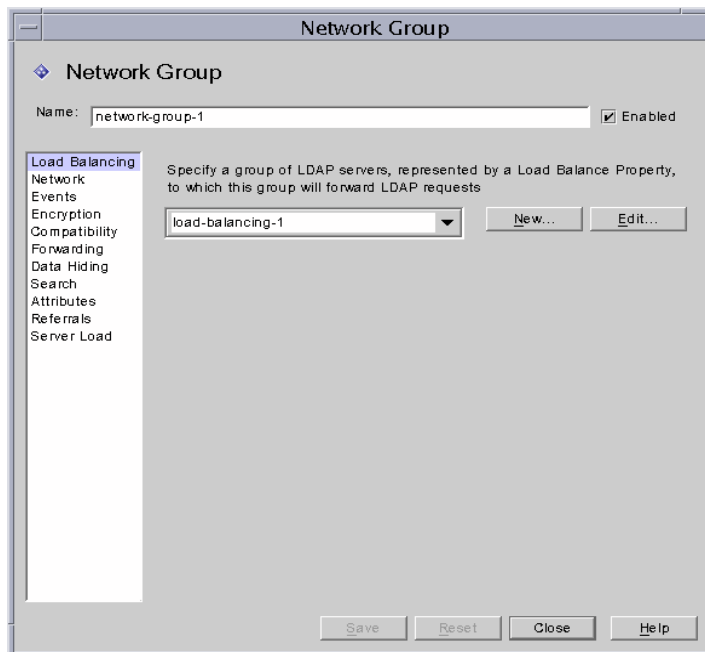
表 6-1 範例群組

優先權	群組名稱	網路準則
5	Admin-machine	129.153.129.72
4	IT-management-subnet	129.153.120.0/24
3	Operations	.ops.sun.com
2	Catch-all	ALL
1	Trusted	0.0.0.0

當 LDAP 用戶端從 LDAP 目錄要求服務時，Directory Proxy Server 會檢查要求是否來自 129.153.129.72 IP 位址。如果不是，Directory Proxy Server 會檢查要求是否符合 129.153.129.0/24。如果不是，Directory Proxy Server 會檢查要求是否從 .ops.sun.com 發出。如果不是，Directory Proxy Server 會將連線放在 catch-all 群組，然後移動到決策樹的下個步驟 (請參閱圖 6-2)。

圖 6-3 顯示您能建立群組的部分 Directory Proxy Server 組態編輯器主控台。

圖 6-3 Directory Proxy Server 網路群組定義



請注意，當建立網路群組時，您有機會指定準則的組合。表 6-2 概要說明。

表 6-2 網路群組可使用的準則清單

準則	描述
負載平衡	讓您指定由負載平衡內容所代表的 LDAP 伺服器群組，Directory Proxy Server 組將 LDAP 要求轉送到該伺服器群組。「負載平衡內容」(第 104 頁)。
網路	讓您指定用戶端的連線細節資料及其他網路準則，將他們的要求排序，或篩選到適當的群組。
事件	讓您指定哪些事件要與群組產生關聯，如此群組中的用戶端才能在順利連結到指定目錄時，有效變更群組。顯示事件的現有物件清單；如需詳細資訊，請參閱「建立群組」(第 66 頁)。
加密	讓您指定群組的加密準則(例如，指定用戶端是否能要求 SSL 工作階段)。

表 6-2 網路群組可使用的準則清單 (後續)

準則	描述
相容性	LDAP v2 規格 (RFC 1777) 不允許在同一工作階段中多次連結用戶端。然而，有些用戶端可預期使用此功能。您可以設定本選項與這些程式碼互通。
轉送	讓您指定將連結、比較、及其他 LDAP 要求傳送給伺服器的準則。
隱藏資料	讓您指定要對群組隱藏目錄中項目的哪些樹狀子目錄、項目、或屬性。顯示 [禁止的項目] 內容的現有物件清單；如需詳細資訊，請參閱「禁止的項目內容」(第 95 頁)。
搜尋	讓您指定群組的搜尋範圍及大小限制。顯示 [搜尋大小限制] 內容的現有物件清單；如需詳細資訊，請參閱「搜尋大小限制內容」(第 108 頁)。
屬性	讓您指定規則，防止特定搜尋種類及比較作業到達 LDAP 伺服器。顯示 [屬性重新命名] 內容的現有物件清單；如需詳細資訊，請參閱「屬性重新命名內容」(第 92 頁)。
轉介	讓您指定群組是要轉送、跟隨或放棄由伺服器傳回的轉介。請注意，不實作 LDAPv3 的用戶端將無法了解轉送的轉介。此設定適用於所有轉介 (除了搜尋接續轉介之外)。
伺服器載入	讓您指定細節資料，例如連至群組的連線總數、每一連線的同時操作數量及操作總數、每一 IP 位址的同時操作數量等等。

建立群組

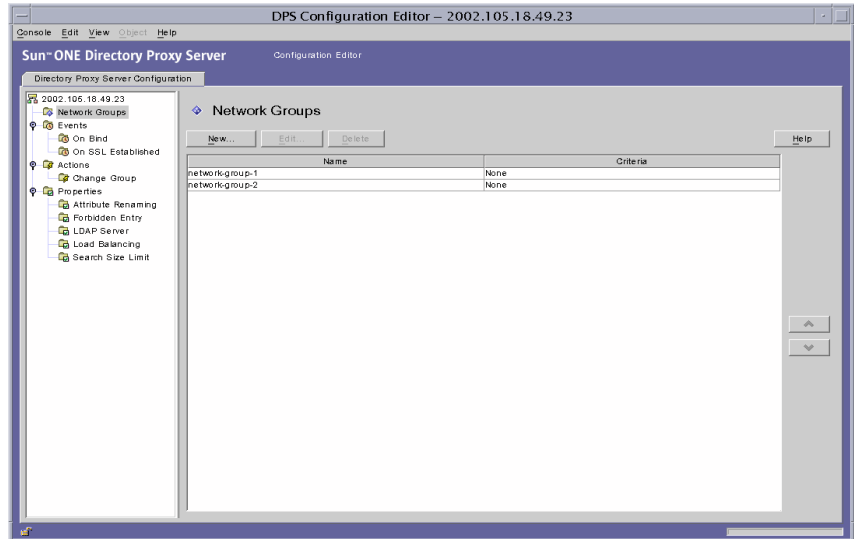
本節說明如何利用 Directory Proxy Server 組態編輯器主控台建立群組。開始建立群組之前，請務必閱讀「群組概論」(第 61 頁) 一節，並瞭解 Directory Proxy Server 群組的意義。建立必要的群組並排定優先權後，請務必測試組態，看看群組是否如預期篩選用戶端要求。

請注意，當建立網路群組時，您有機會指定許多準則。本節提供的說明，以這些準則出現在 UI 上的順序呈現，並依賴您的判斷，來設定群組的適當準則。

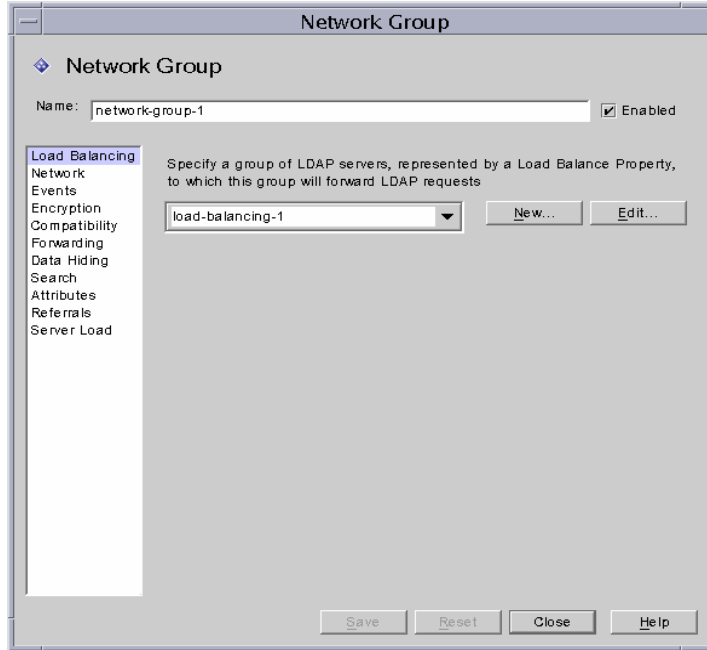
若要在 Directory Proxy Server 中建立網路群組，請依照這些步驟：

1. 存取 Directory Proxy Server 組態編輯器主控台；請參閱「存取 Directory Proxy Server 主控台」(第 33 頁)。

2. 在瀏覽樹狀目錄中，選取 [網路群組]。
右邊窗格會顯示現有的群組清單。



- 按一下 [新增]。
出現 [網路群組] 視窗。

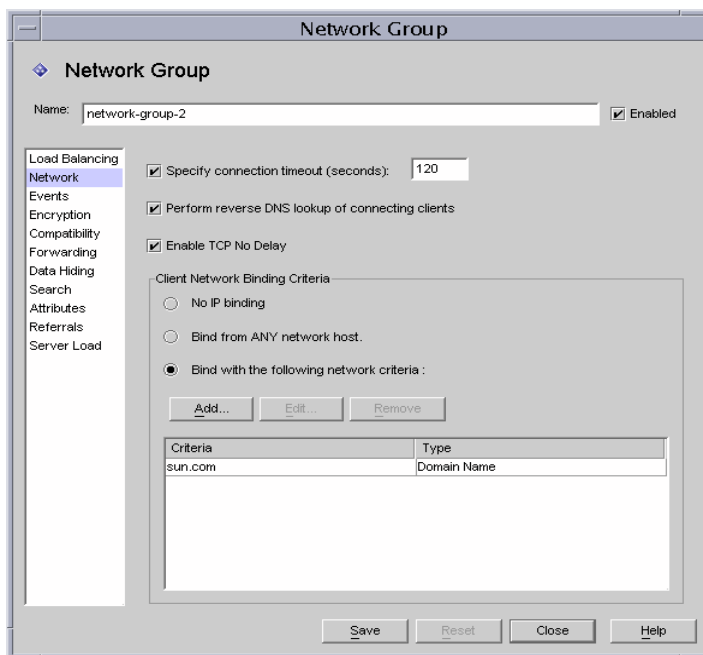


- 在 [名稱] 欄位中，鍵入群組的名稱。名稱必須是獨一無二的英數字元字串。
- 確定已選取 [已啓用] 選項，預設會選取它。若群組為 Directory Proxy Server 組態的一部份，則必須選取此選項。取消選取選項以停用組態中的群組。
- 視需要在下拉式功能表中指定負載平衡內容。此內容可識別 LDAP 伺服器群組，Directory Proxy Server 將 LDAP 要求轉送到該 LDAP 伺服器組，以使用 [負載平衡] 屬性來處理用戶端要求。相關聯的下拉式清單可顯示 [負載平衡] 屬性的現有物件，請參閱「負載平衡內容」(第 104 頁)。選取適當的物件。預設不會選取物件 (<NONE>)。如果沒有物件，則可按一下 [新增] 按鈕以立即建立物件。

新增。顯示對話方塊，以建立新的 [負載平衡] 屬性。

編輯。顯示對話方塊，以編輯現有的 [負載平衡] 屬性。

7. 若要指定群組的網路準則，以排序或篩選要求，請選取左邊框架的 [網路]。然後參考畫面上的元素描述，指定適當的網路值如下：
 - 指定連線逾時值。依預設不會有數值，也表示為不逾時連線。
 - 啟用連線用戶端的反向 DNS 查閱。
 - 選取 [啟用 TCP 未延遲]。
 - 定義 [用戶端網路連結準則]。



畫面上的元素描述如下：

指定連線逾時。如果您想輸入一個時間段，用戶端經過這段時間無活動的話，Directory Proxy Server 可關閉連至用戶端的連線，請選取此方塊。該值必須為秒數，通常不小於 120。依預設不會有數值，也表示為不逾時連線。請注意，如果未啟用 TCP 保持連線，則必須有此屬性，以防止遺失的用戶端連線阻礙 Directory Proxy Server。

執行連線用戶端的反向 DNS 查閱。預設會啟用此選項。如果停用 [反向 DNS 查閱]，則 Directory Proxy Server 將不會執行反向 DNS 查閱，以尋找連線用戶端的網域名稱。停用 [反向 DNS 查閱] 有時可大幅改善 Directory Proxy Server 效能。如果您將網域名稱或網域名稱尾碼作為 [用戶端網路連結準則] 的值，則不得停用 [反向 DNS 查閱]，否則 Directory Proxy Server 將無法正確運作。您必須設定讓 DNS 將完整的主機名稱傳回給查閱查詢。

啓用 TCP 未延遲。預設會啓用此選項。如果停用此選項，則 Directory Proxy Server 將會停用它本身與屬於該群組的用戶端間，用於連線的 Nagle 演算法。只有當 Directory Proxy Server 與用戶端之間的網路頻寬過小時，才可以停用 [TCP 未延遲]；然而，這樣可能會造成效能嚴重降低。

用戶端網路連結準則。使用此區段指定哪些用戶端可以連結此網路群組。

無 IP 連結。如果只有當用戶端連結到群組時才切換，請選取此選項。預設會選定此選項。如果用戶端只會在連結時使用群組來切換，則可取消選取此選項。

從任何網路主機連結。如果允許所有主機與此網路群組連結，請選取此選項。

以下列準則連結。選取此選項，指定符合網路群組的主機之網域名稱或 IP 位址；在這個情況下，群組必須指定將連結過來的主機之網域名稱或 IP 位址。

新增。顯示對話方塊，以新增網路準則。有四個選項：[網域名稱]、[IP 位址]、[IP 位址和位元]以及 [IP 位址和四位元]。

編輯。顯示對話方塊，以編輯網路準則。

移除。顯示對話方塊，以移除網路準則。

網域名稱對話方塊。指定可連結到網路群組之用戶端的網域名稱尾碼或完整名稱，例如 foo.sun.com。請注意，Directory Proxy Server 預設不假設任何網域名稱尾碼；因此，您必須提供完整的網域名稱。以句號開頭的網域名稱尾碼（例如 .sun.com）會導致網域名稱以該尾碼結尾的所有主機都相符。

同時注意到，如果用網域名稱尾碼規則來識別用戶端，請確定有設定 DNS，以將完全合格名稱傳回 DNS 查詢，如果傳回短名稱，本功能就沒有作用。

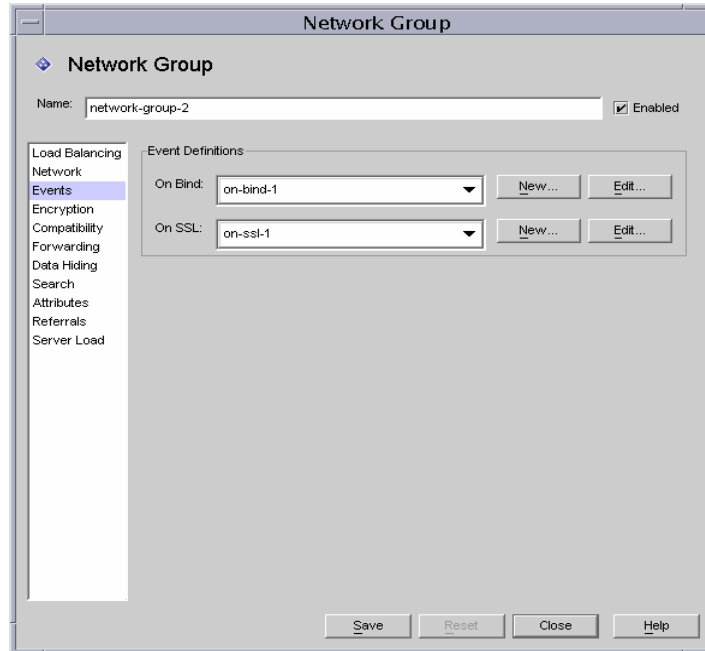
IP 位址。指定單一 IP 位址，其形式為帶有點的小數，例如 198.214.11.1。

IP 位址和位元。指定 IP 網路遮罩，其形式為 <網路編號>/<遮罩位元>，例如 198.241.11.0/24。前半部是網路編號，而後半部可指出比對所需的網路編號的位元數。

IP 位址和四位元。指定 IP 網路遮罩，其形式為一對帶有點的四個小數的組合，例如 198.241.11.0/255.255.255.128。前半部是網路編號，而後半部可指出比對所需的網路編號的位元。例如，198.214.11.0/255.255.255.128 會與 IP 位址為 198.214.11.63 的主機相符，而不會與 IP 位址為 198.214.11.191 的主機相符。

請注意，使用網域名稱或網域名稱尾碼都需要啓用 [執行連線用戶端的反向 DNS 查閱]。

8. 如果您要將事件導向動作與群組產生關聯 (例如，將用戶端從這個群組變更到另一個群組)，請選取左邊框架的 [事件]，然後在右邊框架指定適當的值。



畫面上的元素描述如下：

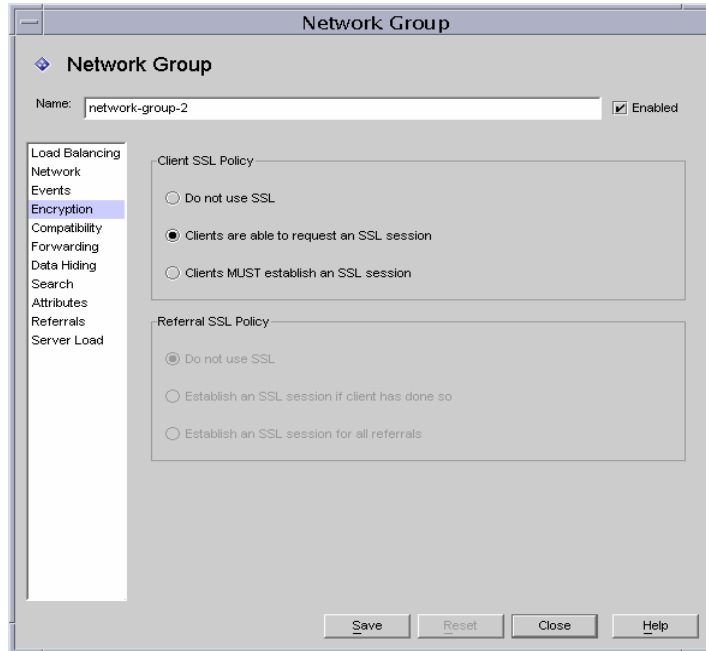
連結後續動作。 下拉式清單可顯示 OnBindSuccess 事件的現有物件，請參閱「建立 OnBindSuccess 事件物件」(第 114 頁)。選取用戶端順利完成連結作業時會執行的物件名稱。預設不會選取物件 (<NONE>)。如果沒有物件，則可按一下 [新增] 按鈕以立即建立物件。

SSL 後續動作。 下拉式清單可顯示 OnSSLEstablished 事件的現有物件，請參閱「建立 OnSSLEstablished 事件物件」(第 117 頁)。選取用戶端順利建立 SSL 工作階段時會執行的物件名稱。如果沒有物件，則可按一下 [新增] 按鈕以立即建立物件。

編輯。 顯示對話方塊，以編輯事件的行為。

新增。 顯示對話方塊，以建立新事件。

9. 如果您要指定群組的加密準則 (例如, 指定用戶端是否能要求 SSL 工作階段), 請選取左邊框架的 [加密], 然後在右邊框架指定適當的值。



畫面上的元素描述如下：

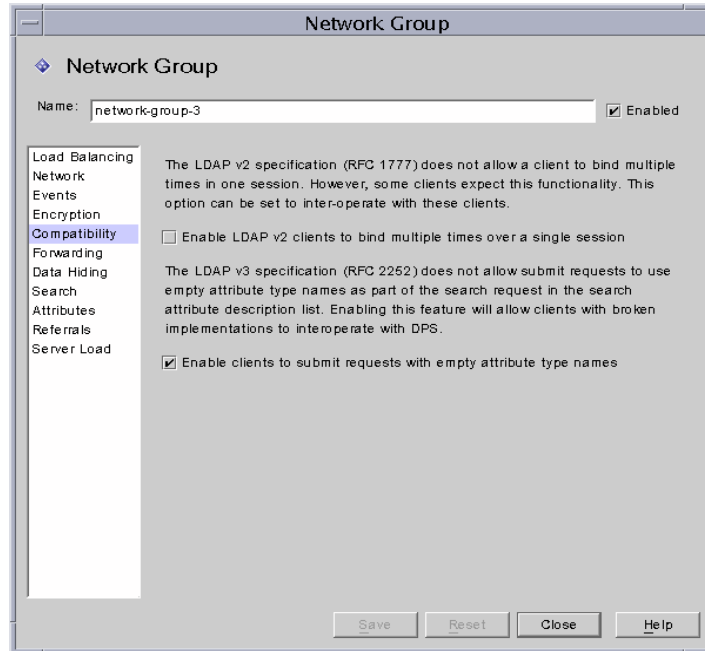
用戶端 SSL 原則。 設定用戶端 SSL 原則。

- **不要使用 SSL。** 如果不希望使用 SSL 加密, 請選取此選項。
- **用戶端可要求 SSL 工作階段。** 如果群組中的用戶端會建立要求 SSL 的 SSL 工作階段, 則可選取此選項。
- **用戶端必須建立 SSL 工作階段。** 如果群組中的用戶端在執行任何作業之前, 必須先建立 SSL 工作階段, 則可選取此選項。

轉介 SSL 原則。 跟隨轉介來設定 SSL 原則。

- **不要使用 SSL。** 如果不希望使用 SSL 加密, 請選取此選項。
- **建立 SSL 工作階段 (如果用戶端尚未建立它)。** 如果啓用此選項, 且用戶端已經具有利用 Directory Proxy Server 建立的 SSL 工作階段, 則 Directory Proxy Server 將只會為該群組中的用戶端啓動 SSL。
- **為所有轉介建立一個 SSL 工作階段。** 啓用此選項, 則發生轉介時, Directory Proxy Server 就會在轉送作業之前, 先啓動 SSL 工作階段。

10. 如果您要指定群組的相容性準則 (例如，允許用戶端在一個工作階段中連結多次)，請選取左邊框架的 [相容性]，然後在右邊框架指定適當的值。



畫面上的元素描述如下：

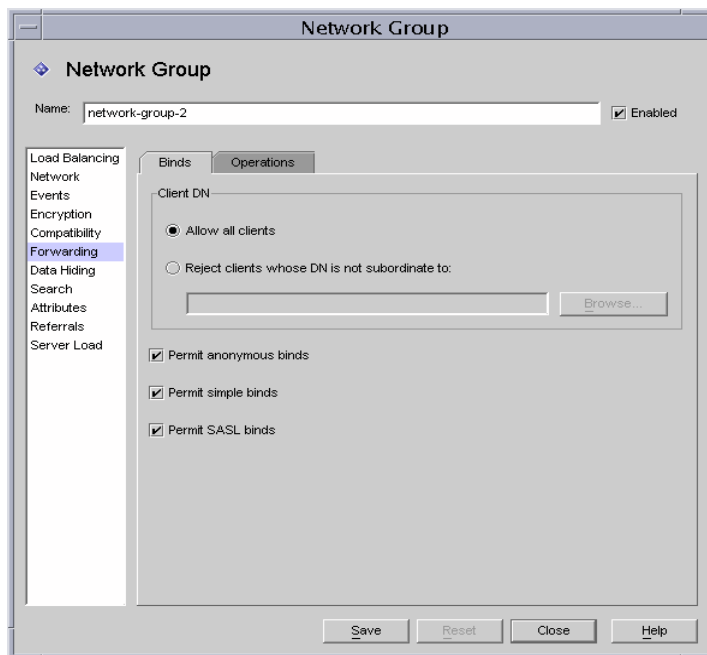
啓用 LDAP v2 用戶端以多次連結到單一工作階段。 LDAP v2 規格 (RFC 1777) 不允許在同一工作階段中多次連結用戶端。然而，有些用戶端可預期使用此功能。如果您要此群組讓用戶端提交搜尋要求，且此要求的屬性要求清單中一個以上的屬性是 NULL，則請選取此功能。此相容性功能讓 Directory Proxy Server 與某些不完整的啓用 JAVA 用戶端互通。請注意，屬性要求清單中的 NULL 屬性違反 LDAP 通訊協定。依預設，此選項設定成 TRUE。

讓用戶端可提交具有空屬性類型名稱的要求。 如果即使用戶端未識別他們的屬性類型名稱，您也要此群組允許他們提交要求，則請選取此功能。

11. 如果您要指定群組的轉送要求準則，請選取左邊框架的 [轉寄]，然後在右邊框架指定適當的值。

一旦 Directory Proxy Server 接受來自用戶端的連線並與一個群組相符時，其將等待用戶端傳送 LDAP 連結要求。Directory Proxy Server 會使用 [用戶端 DN]、[允許匿名連結]、[允許簡單連結] 及 [允許 SASL 連結]，來判定是否要將連結要求傳送到伺服器，或是拒絕連結要求並關閉用戶端連線。

如果用戶端的連結傳送已啓用的測試，則 Directory Proxy Server 就會將它轉送到伺服器。如果伺服器接受連結，連線就會建立。然而，如果伺服器傳回該連結要求的錯誤指示，Directory Proxy Server 會將錯誤指示轉送至用戶端，如果用戶端使用的是 LDAPv2，其也將關閉用戶端的連線。



[連結] 標籤中的元素描述如下：

允許所有用戶端。預設會啓用此選項，允許所有用戶端存取。

拒絕其 DN 非從屬的用戶端。如果您要此群組檢查辨別名稱 (DN)，請選取此選項。在非從屬於指定 DN 的連結中提供辨別名稱的任何用戶端都會遭到拒絕。使用 [瀏覽] 按鈕來瀏覽 LDAP 目錄以建構 DN。

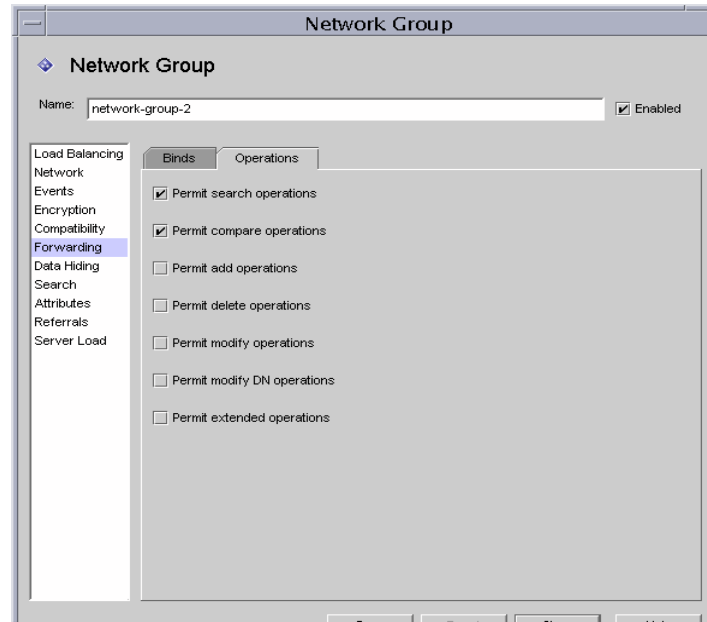
允許匿名連結。預設會啓用此選項，即使用戶端未提供密碼，也可允許連結。停用此選項以禁止匿名連結。

允許簡單連結。預設會啓用此選項，讓用戶端在安全狀態下提供密碼。停用此選項以禁止純文字密碼的已驗證連結要求。

允許 SASL 連結。預設會啓用此選項，指定允許 SASL 連結。停用此選項以禁止 SASL 驗證。

12. 選取 [操作] 標籤，並指定要轉送哪些操作。

依預設 Directory Proxy Server 會轉送搜尋及比較要求。Directory Proxy Server 也會辨識未連結的要求，並關閉連至 LDAP 伺服器的連線。



[操作] 標籤中的元素描述如下：

允許搜尋操作。預設會啟用此選項。停用此選項，以防範 Directory Proxy Server 將搜尋要求轉送到伺服器。

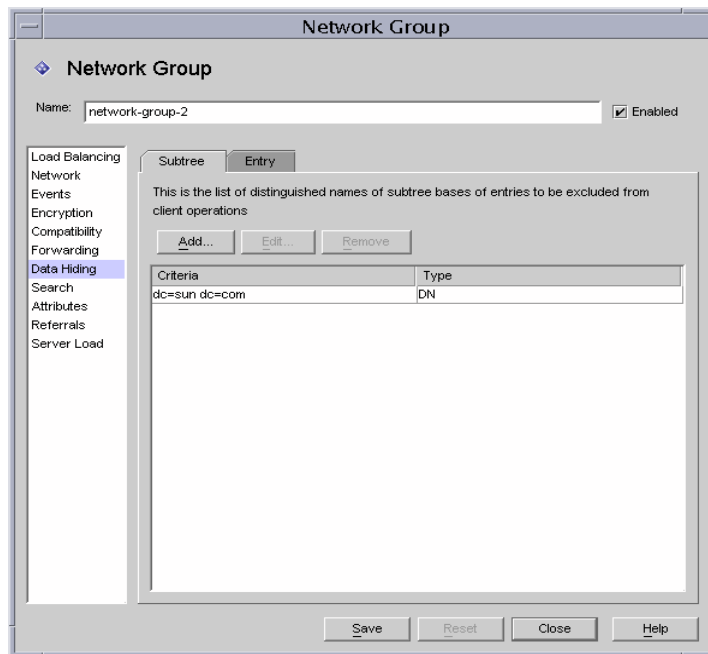
允許比較操作。預設會啟用此選項。停用此選項，以防範 Directory Proxy Server 將比較要求轉送到伺服器。

允許新增、刪除、修改、修改 DN 及延伸操作。依預設，Directory Proxy Server 不會轉送新增、修改、刪除、修改 DN 或延伸操作要求。若要允許轉送這些操作，請啓用以允許適當的操作。

請注意，您必須啓用 [允許延伸操作]，才能讓用戶端與 [啟動 TLS] 交涉。

- 如果您要指定群組的資料隱藏準則，請選取左邊框架的 [資料隱藏]，然後在右邊框架指定適當的值。

使用 [樹狀子目錄] 標籤指定要隱藏哪個部分的樹狀目錄，使用 [項目] 標籤指定要隱藏的項目或屬性。



[樹狀子目錄] 標籤中的元素描述如下：

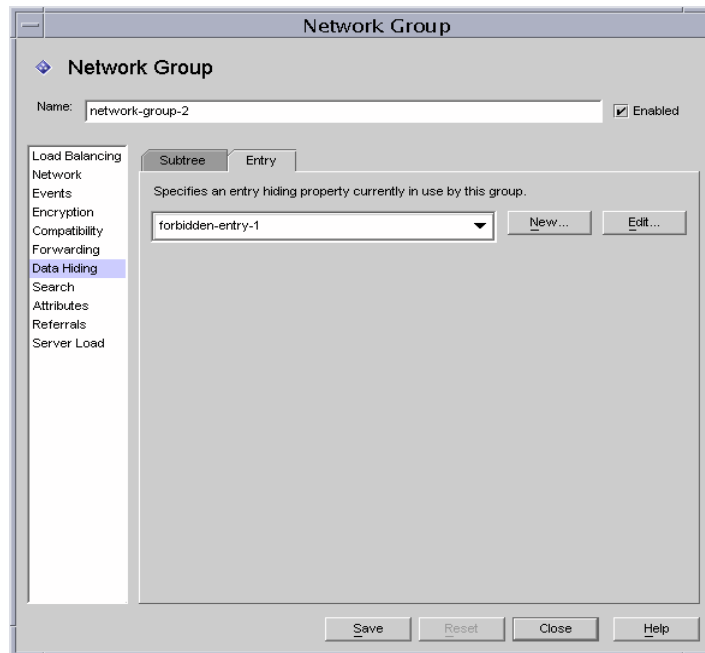
隱藏項目的樹狀子目錄。 要求項目位於禁止樹狀子目錄之上或之下的作業，會因為存取權限不足的錯誤而遭到拒絕。系統會捨棄與搜尋篩選相符且位於禁止樹狀子目錄內的項目。請注意，此作業不會從傳回作為結果之一部份的項目中，移除其值位於樹狀子目錄之下的 DN 語法屬性。

新增。 顯示對話方塊，以將辨別名稱加入至要排除項目之樹狀子目錄的基礎清單。如果網路群組中沒有辨別名稱，則預設為允許存取目錄中的所有項目。清單中的項目具有 dn 語法。

編輯。 顯示對話方塊，以編輯辨別名稱。

移除。 移除清單中的辨別名稱。

14. 選取 [項目] 標籤，並指定要隱藏的項目或屬性。



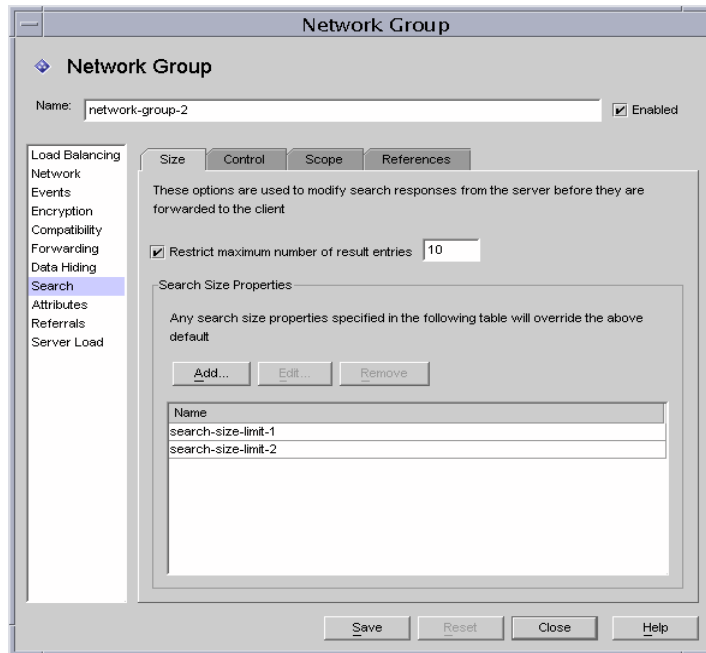
[項目] 標籤中的元素描述如下：

指定此群組目前所使用的 [項目隱藏內容]。下拉式清單可顯示 [禁止的項目] 屬性的現有物件，請參閱「禁止的項目內容」(第 95 頁)。選取物件名稱。預設不會選取物件 (<NONE>)。如果沒有物件，則可按一下 [新增] 按鈕以立即建立物件。

新增。顯示對話方塊，以建立新的 [禁止的項目] 內容。

編輯。顯示對話方塊，以編輯現有的 [禁止的項目] 內容。

15. 如果您要指定群組的搜尋屬性，請選取左邊框架的 [搜尋]，然後在右邊框架指定適當的值。



[大小] 標籤中的元素描述如下：

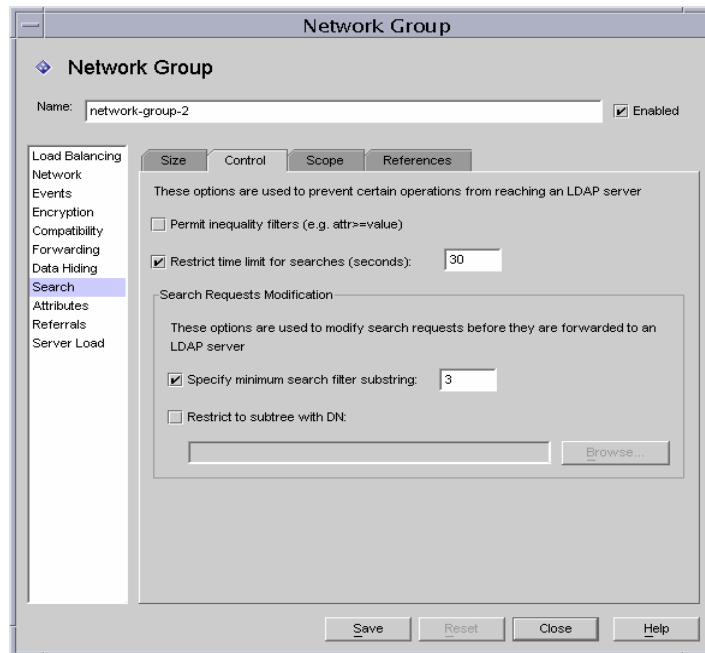
限制結果項目的最大數量。 啟用此選項，以指定單一搜尋作業一次可傳回用戶端的結果項目數量上限。值可為大於零的任何數字，且到達此值時會導致 `administrativeLimitExceeded` 錯誤，向用戶端指出將放棄後續項目。如果停用此內容，則預設為不放棄項目。

新增。 顯示對話方塊，以加入 [搜尋大小限制] 內容。如需詳細資訊，請參閱「搜尋大小限制內容」(第 108 頁)。

編輯。 顯示對話方塊，以編輯 [搜尋大小限制] 內容。

移除。 顯示對話方塊，以移除 [搜尋大小限制] 內容。(此動作將內容從群組移除，而不顯示對話方塊。)

16. 選取 [控制] 標籤，並指定控制搜尋篩選條件的準則。



[控制] 標籤中的元素描述如下：

允許非等式篩選。預設會啟用此選項。[允許非等式篩選] 可指定是否允許用戶端要求包含非等式篩選 ($attr>=value$) 及 ($attr<=value$) 的搜尋。如果網路群組不允許執行非等式搜尋，則停用此選項。

限制搜尋時間限制。啟用此選項並輸入值 (以秒計)，讓網路群組指定搜尋操作的時間限制上限 (以秒計)。如果用戶端指定的時間限制大於此選項指定的值，則此網路群組指定的值就會覆寫用戶端的要求。預設會停用此選項，且網路群組會允許用戶端設定任何時間限制，包括無限制。

指定最小搜尋篩選子字串。 啓用此選項並輸入值，以指定搜尋篩選條件之子字串的允許長度下限。值必須大於 1。如果停用此選項，則會預設為允許搜尋篩選任何大小的子字串。如果您想限制網頁自動尋檢程式可執行的搜尋種類，則應在網路群組中啓用此選項。例如，2 這個值會封鎖類似 (cn=A*) 的搜尋。

注意： 此屬性不影響 presence 篩選條件 (attrname=*)。若要禁止特定 presence 篩選條件，請使用禁止的比較組態。

限制為具有 DN 的樹狀子目錄。 啓用此選項，並為所有操作指定樹狀子目錄的基礎。此選項具有 dn 語法。如果停用此選項，則沒有基礎下限的限制。

其目標項目位於或低於基礎項目下限的操作，都不會受此選項影響。如果目標項目高於基礎項目下限，且操作是樹狀子目錄搜尋，則系統會在將查詢傳送到伺服器之前重新寫入查詢，以將目標項目變更為基礎下限。如果目標項目不低於基礎下限或高於它，則系統會拒絕要求，並報告無此物件的錯誤。

例如，如果 [限制具有 DN 的樹狀子目錄] 設為：

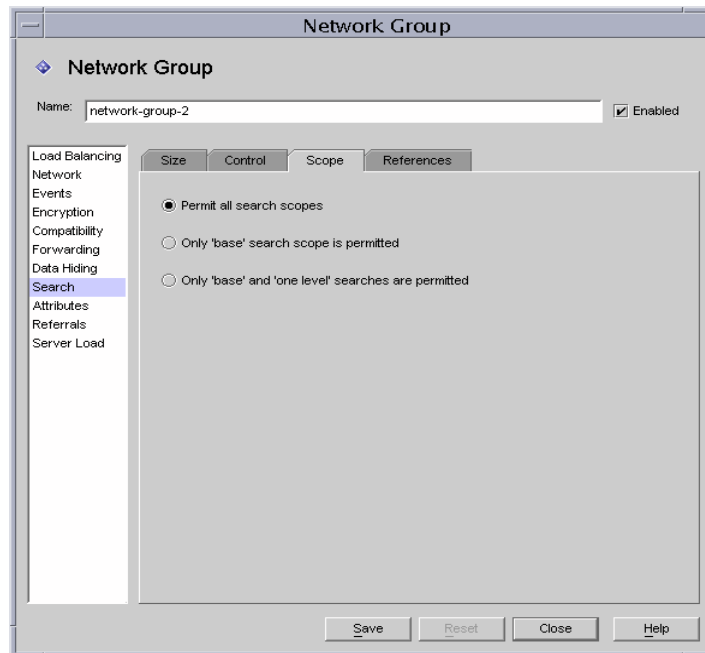
```
o=sun, st=California, c=US
```

且收到樹狀子目錄搜尋 st=California, c=US，則會重新寫入搜尋，讓伺服器執行下列樹狀子目錄搜尋

```
o=sun, st=California, c=US
```

瀏覽。 顯示對話方塊，以協助建構有效的 DN。

17. 選取 [範圍] 標籤，並指定用戶端可在搜尋要求中指定的搜尋範圍。



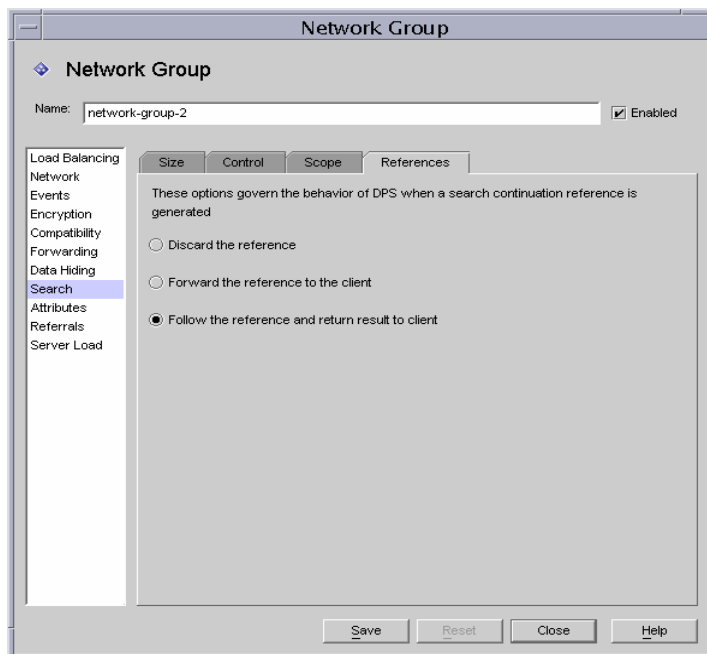
[範圍] 標籤中的元素描述如下：

允許所有搜尋範圍。預設會啟用此選項，允許用戶端的所有搜尋範圍。

只允許 [基礎] 搜尋範圍。啟用此選項，只允許基礎搜尋範圍。

只允許 [基礎] 及 [單層次] 搜尋。啟用此選項，只允許基礎搜尋及單層次搜尋。

18. 選取 [轉介] 標籤，並指定搜尋期間產生搜尋接續轉介時，要執行哪些動作。



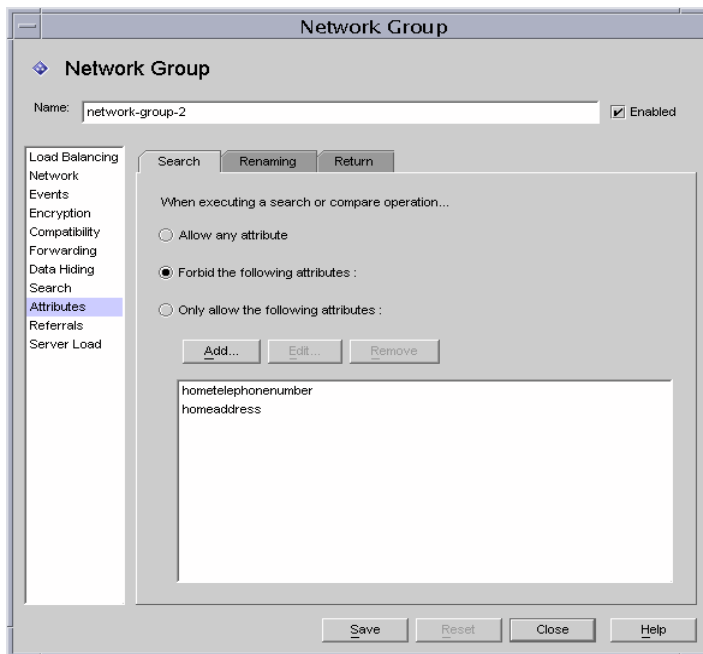
[轉介] 標籤中的元素描述如下：

放棄轉介。預設會啓用此選項，以放棄搜尋期間產生的轉介。

將轉介轉送到用戶端。只有在轉送搜尋接續轉介時，才啓用此選項。

跟隨轉介並將結果傳回用戶端。啓用此選項，以跟隨並傳回搜尋接續轉介結果。搜尋接續轉介是轉介的一種特殊案例，其中的部份查詢可由所查詢的原始目錄伺服器來滿足，但是該目錄伺服器轉介的是具有更多資料且可滿足查詢的另一目錄伺服器。此選項可用來隱藏其命名內容由另一 LDAP 伺服器主控的目錄資訊樹狀目錄的一部份。它也可防止用戶端尋找此伺服器執行位置的網路位址和連接埠。

19. 如果您要指定群組的屬性準則，請選取左邊框架的 [屬性]，然後在右邊框架指定適當的值。



[搜尋] 標籤中的元素描述如下：

此標籤是用來防止特定搜尋種類及比較作業到達 LDAP 伺服器。如果用戶端的要求受限於此限制，則 Directory Proxy Server 就會將存取權限不足的錯誤傳回用戶端。

允許任何屬性。預設會啟用此選項，以允許將所有屬性用於搜尋篩選條件和比較。

禁止下列屬性。啟用此選項，以指定用戶端無法用於搜尋篩選條件或比較要求的屬性名稱。

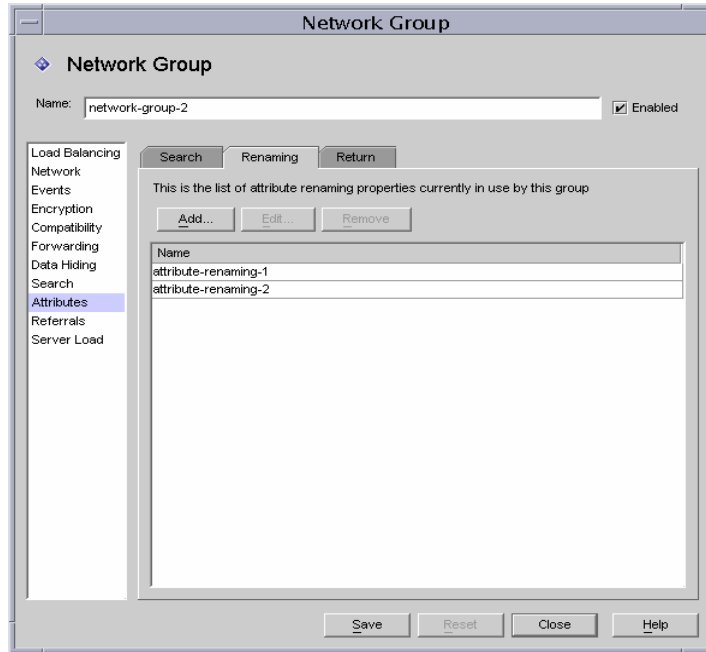
只允許下列屬性。啟用此選項，以指定可用於搜尋篩選條件或比較要求的屬性名稱。如果網路群組表格中有一或多個屬性值，且比較與任一項都不相符，則 Directory Proxy Server 就會拒絕要求。如果網路群組表格中沒有屬性，且屬性與任何屬性都不相符，則可由用戶端使用。例如，如果您只想讓用戶端搜尋 cn、dn 及 mail 屬性，則可將這些屬性加入表格。

新增。顯示對話方塊，以將屬性加入至表格中。您必須指定是否要禁止或允許這些屬性。

編輯。顯示對話方塊以編輯在表格中選取的屬性。

移除。 將屬性從表格中移除。

20. 選取 [重新命名] 標籤，並指定重新命名屬性的規則。



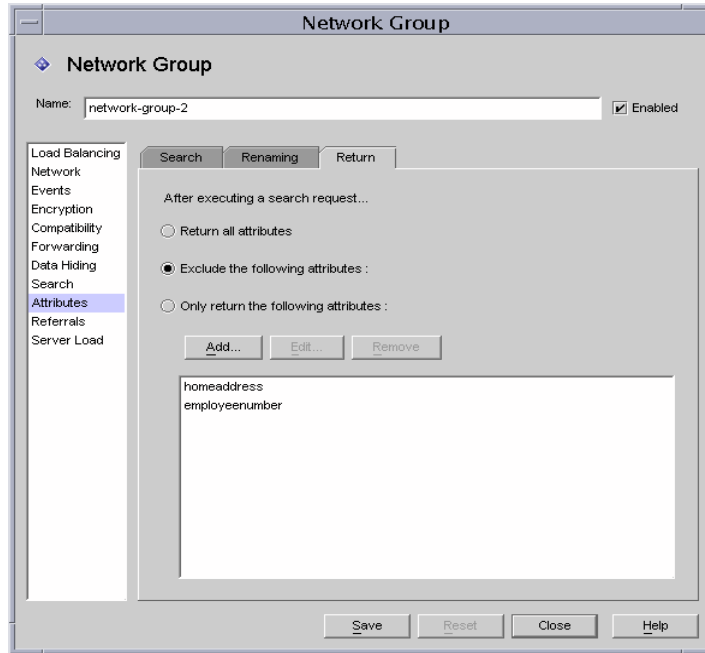
[重新命名] 標籤中的元素描述如下：

新增。 顯示對話方塊，以將一或多個現有屬性重新命名內容新增至此網路群組將使用的下列表格。(請參閱「屬性重新命名內容」(第 92 頁)。)

編輯。 顯示對話方塊，以編輯選定屬性重新命名的內容。

移除。 將屬性重新命名內容從表格中移除。

21. 選取 [傳回] 標籤，並指定將伺服器所傳回之搜尋結果轉送至用戶端之前，套用到搜尋結果的限制。



[傳回] 標籤中的元素描述如下：

傳回所有屬性。 預設會啟用此選項，並允許傳回所有屬性。

排除下列屬性。 啟用此選項，以指定要從搜尋結果項目中排除的屬性名稱。

只傳回下列屬性。 啟用此選項，以指定可從搜尋結果中傳回的屬性名稱 (如果有)。

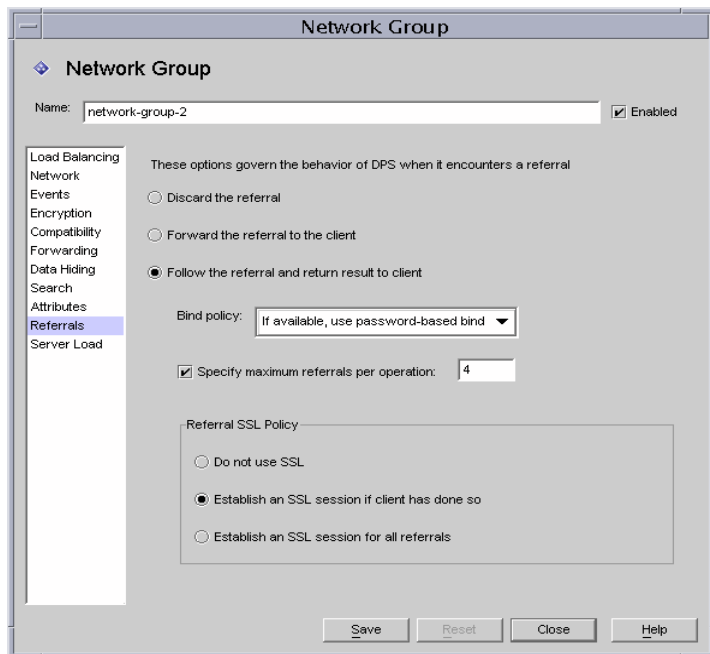
如果傳回作為搜尋之一部份的屬性不在「只傳回下列屬性」表格中，就不會傳回。如果表格是空的，而且這些屬性不在「排除下列屬性」表格中，就會傳回。

新增。 顯示對話方塊，以將屬性加入至表格中。您必須在上方指定是否要禁止或允許這些屬性。

編輯。 顯示對話方塊以編輯在表格中選取的屬性。

移除。 將屬性從表格中移除。

22. 如果您要指定群組的轉介 (例如，群組是否會轉送、跟隨或放棄由伺服器傳回的轉介)，請選取左邊框架的 [轉介]，然後在右邊框架指定適當的值。



畫面上的元素描述如下：

放棄轉介。 如果網路群組放棄由伺服器傳回的所有轉介，則可啓用此選項。

將轉介轉送到用戶端。 預設會啓用此選項，以轉送由伺服器傳回的轉介。

跟隨轉介並將結果傳回用戶端。 如果網路群組轉送由伺服器傳回的轉介，並將結果傳回用戶端，則可啓用此選項。

連結原則。 當完成操作轉介且該轉介被跟隨時，此選項控制連結原則。

請注意，Directory Proxy Server 無法為使用 SASL 機制連結的用戶端重新執行連結。因此，如果指定 [必需] 且用戶端使用 SASL 機制來連結，則會拒絕轉介操作。

永遠。 如果 Directory Proxy Server 在為連至此網路群組的用戶端跟隨轉介時應永遠匿名連結，請選取此選項。

任何。 如果網路群組在用戶端使用密碼型連結，或以匿名連結時應該使用簡單連結，則可選取此選項。此選項為預設值。

必需。 如果網路群組在用戶端沒有密碼型連結時應該拒絕轉介作業，則可選取此選項。

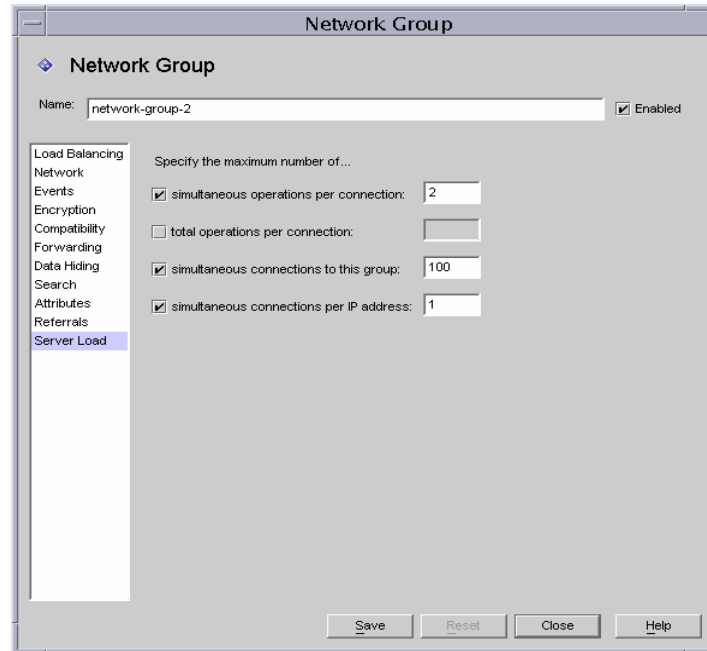
每一操作的轉介上限。輸入不小於零的整數值。這選項將會限制單一操作可跟隨的轉介上限數目。預設為 15。零值指出不會套用限制。

轉介 SSL 原則。爲了啓用 [轉介 SSL 原則面板]，必須在加密檢視上啓用 [SSL 可用] 選項。

如果用戶端已建立 SSL 工作階段。如果網路群組只會在用戶端已利用 Directory Proxy Server 建立 SSL 工作階段時啓動 SSL，則可啓用此選項。此選項爲預設值。

針對所有轉介。對於一個轉介，如果群組在轉送操作之前，先啓動 SSL 工作階段，則啓用 [針對所有轉介]。

23. 如果您要指定群組的 [伺服器載入] 準則，請選取左邊框架的 [伺服器載入]，然後在右邊框架指定適當的值。



畫面上的元素描述如下：

每一連線的同時操作數量。選取此選項，以限制 Directory Proxy Server 每次在該群組中進行連線時，將處理的同時操作數量。該值是一個大於零的整數。如果沒有此屬性，則不會實施限制。例如，如果您將此值設爲 1，則會強制該群組中的所有用戶端都執行同步 LDAP 操作。額外的同時要求 (除了放棄操作的要求之外) 將會失敗，並報告 [伺服器忙碌中] 的錯誤。

每一連線的操作總數。 選取此選項，以限制 Directory Proxy Server 每次在群組中進行連線時，將允許的操作總數。該值是一個大於零的整數。如果用戶端在一次連線中超過其群組所允許的操作數量上限，則該連線會由 Directory Proxy Server 關閉。如果沒有此屬性，則不會設定限制。

連至此群組的連線。 選取此選項，以限制連至此網路群組的同時連線數量，並指定數量。

每一 IP 位址的同時連線數量。 選取此選項，以限制用戶端可從單一 IP 位址進行的同時連線數量。預設會允許任何連線數量。

24. 按一下 [儲存] 以建立此群組。

Directory Proxy Server 組態已經修改，您必須重新啟動依賴本組態的伺服器。現在還不要重新啟動伺服器。您可以將所有的組態都變更過後再進行。

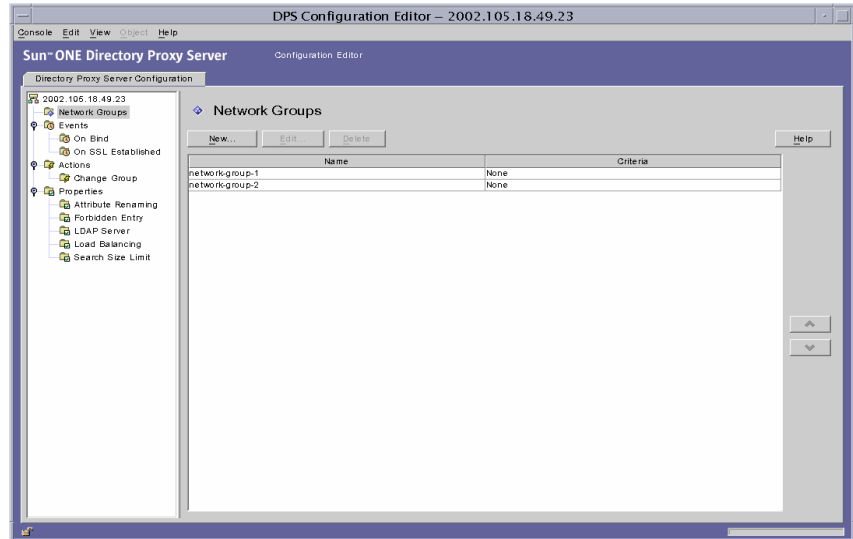
25. 重複步驟 3 至步驟 24，以建立其他群組。
26. 請到 [網路群組] 視窗 (請參閱步驟 2) 並適當排定群組的優先權。
27. 若要重新啟動伺服器，請參閱 「重新啟動 Directory Proxy Server」 (第 47 頁)。

修改群組

若要修改群組：

1. 存取 Directory Proxy Server 組態編輯器主控台；請參閱 「存取 Directory Proxy Server 主控台」 (第 33 頁)。

2. 在瀏覽樹狀目錄中，選取 [網路群組]。
右邊窗格會顯示現有的群組清單。



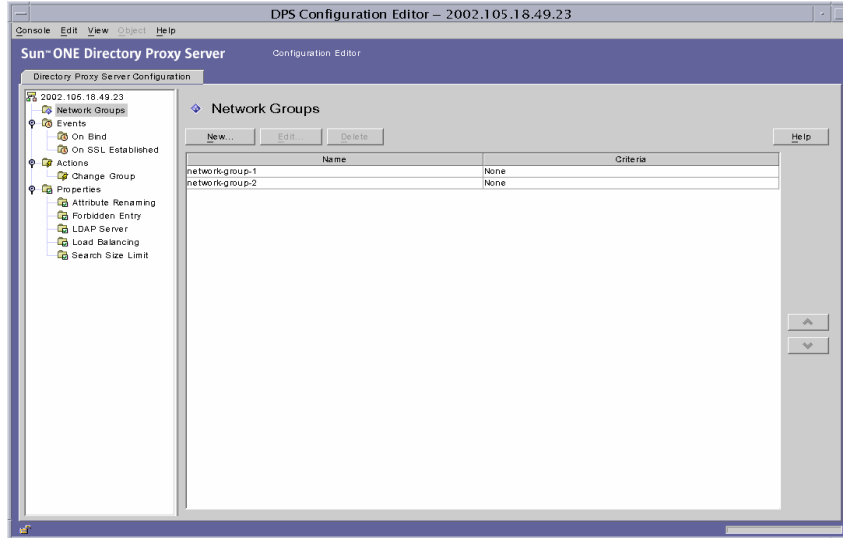
3. 在清單中選取您要修改的群組，然後按一下 [編輯]。
4. 進行必要的修改。
5. 按一下 [儲存] 以儲存您的變更。
Directory Proxy Server 組態已經修改，您必須重新啟動依賴本組態的伺服器。現在還不要重新啟動伺服器。您可以將所有的組態都變更過後再進行。
6. 重複步驟 3 至步驟 5，以修改其他群組。
7. 若要重新啟動伺服器，請參閱「重新啟動 Directory Proxy Server」(第 47 頁)。

刪除群組

您可以從 Directory Proxy Server 組態刪除任何不要的網路群組。若要刪除群組：

1. 存取 Directory Proxy Server 組態編輯器主控台；請參閱「存取 Directory Proxy Server 主控台」(第 33 頁)。

2. 在瀏覽樹狀目錄中，選取 [網路群組]。
右邊窗格會顯示現有的群組清單。



3. 在清單中選取您要刪除的群組，然後按一下 [刪除]。
4. 確認您的動作。
您刪除的群組名稱現在已經從清單上移除。Directory Proxy Server 組態已經修改，您必須重新啓動依賴本組態的伺服器。現在還不要重新啓動伺服器。您可以將所有的組態都變更過後再進行。
5. 重複步驟 3 及步驟 4，以刪除其他群組。
6. 若要重新啓動伺服器，請參閱「重新啓動 Directory Proxy Server」(第 47 頁)。

定義目錄內容物件

如同本書部署一章的說明，可將 Sun ONE Directory Proxy Server 當作 *LDAP 存取路由器*，協助您保護自己私密的目錄資訊，使其不會未經授權即遭存取，同時能讓這些組織公佈自己的公司資訊時保持安全。本伺服器可處理數千個 LDAP 用戶端要求，同時在轉送給目錄伺服器之前，針對每個要求套用複雜的存取控制規則及通訊協定篩選規則。

Directory Proxy Server 中的 [內容] 物件讓您指定 LDAP 用戶端必須遵循的特殊化限制。然後就可以將這些內容包括在必須套用限制的其他項目中。本章提供每個內容的概論，並說明如何利用 Directory Proxy Server 組態編輯器主控台建立內容物件。

本章包含下列各節：

- 屬性重新命名內容 (第 92 頁)
- 禁止的項目內容 (第 95 頁)
- LDAP 伺服器內容 (第 99 頁)
- 負載平衡內容 (第 104 頁)
- 搜尋大小限制內容 (第 108 頁)
- 修改內容物件 (第 110 頁)
- 刪除內容物件 (第 111 頁)

屬性重新命名內容

通常 LDAP 目錄包含實體的資訊，例如組織裡的人員及網路資源。每個實體在目錄中都有一個項目。目錄中的每個項目都以其辨別名稱 (DN) 識別，由一組屬性及其值代表。每個項目都有物件類別屬性，指定此項目描述的物件種類，並定義包含的其他屬性組。每個屬性描述項目的特色或特徵。例如某項目的物件類別可能是 `organizationalPerson`，表示此項目代表特定組織內的人。此物件類別允許 `givenname` 及 `telephoneNumber` 屬性。您指派給這些屬性的值，能提供代表此項目的人姓名及電話號碼。

在許多目錄部署中，LDAP 用戶端上定義的屬性未對應到伺服器上定義的屬性。為了讓這類設定中的用戶端及伺服器之間能通訊，Directory Proxy Server 支援屬性重新命名 - 也就是說，Directory Proxy Server 可以在查詢傳送給目錄伺服器之前，於用戶端查詢中將屬性重新命名成目錄伺服器了解的格式，並在伺服器回應傳送給用戶端之前，進行同樣的作業。

圖 7-1 說明 Directory Proxy Server 屬性重新命名功能如何對應結構。

圖 7-1 利用屬性重新命名內容對應結構



請注意，電子郵件用戶端規定人員的姓是 `surname` 屬性的值，但在 LDAP 伺服器中，姓是由 `sn` 屬性來指定。當 Directory Proxy Server 對應這二個屬性時，只有屬性名稱受影響；屬性值維持不變。

您可以利用 [屬性重新命名] 內容，來定義控制重新命名用戶端及伺服器屬性的規則。您可以指定必須對應到相對伺服器屬性 (反之亦然) 的用戶端屬性名稱。以這個方法，如果用戶端要求包含伺服器未知的屬性名稱，Directory Proxy Server 就能對應到此伺服器已知的名稱，並協助用戶端與此伺服器通訊。同樣地，當此伺服器回應時，Directory Proxy Server 會將用戶端未知的任何屬性轉換成已知格式。

下一節會說明如何從 Directory Proxy Server 組態編輯器主控台建立屬性重新命名內容的物件。

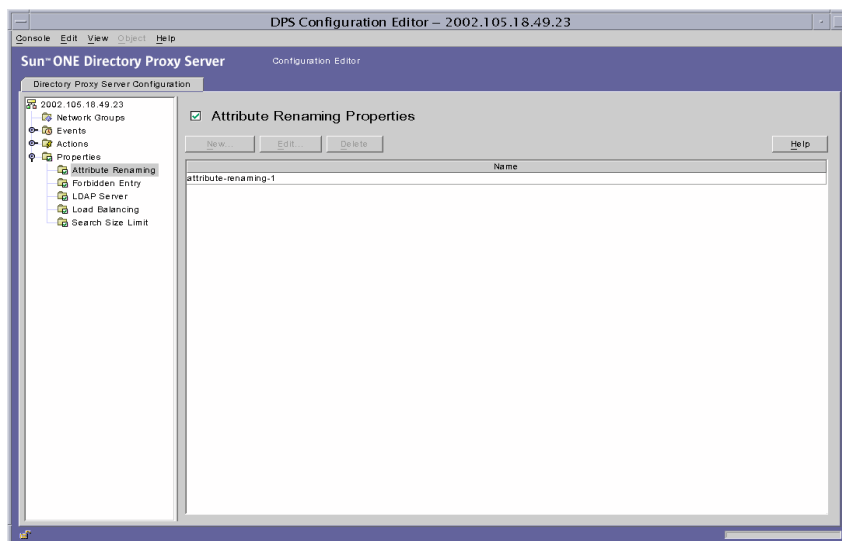
注意： 您為屬性重新命名內容建立的任何物件，必須有伺服器與用戶端兩種屬性。否則 Directory Proxy Server 會啟動失敗。

建立屬性重新命名內容物件

若要識別 Directory Proxy Server 應重新命名的用戶端及伺服器屬性：

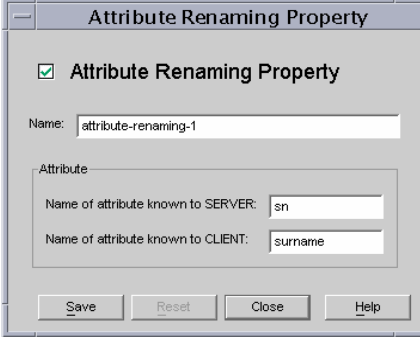
1. 存取 Directory Proxy Server 組態編輯器主控台；請參閱「存取 Directory Proxy Server 主控台」（第 33 頁）。
2. 在瀏覽樹狀目錄中展開 [內容] 節點，然後選取 [屬性重新命名]。

右邊窗格會顯示現有的屬性重新命名內容物件。



3. 按一下 [新增]。

出現 [屬性重新命名內容] 視窗。



4. 在 [名稱] 欄位中，鍵入內容物件的名稱。名稱必須是唯一的英數字元字串。

注意： 屬性名稱只能是 7 位元字元。

5. 在剩餘的欄位中識別對應的屬性：

屬性重新命名值可寫成其元件由句號分隔的十進位數字，例如 2.5.4.10。屬性重新命名值也可為屬性類型指定一或多個文字名稱。這些名稱必須以字母開頭，且只能包含 ASCII 字母、數字字元及連字號。值有區分大小寫。

伺服器已知的屬性名稱。輸入值，以指定伺服器已知的屬性名稱。

用戶端已知的屬性名稱。輸入值，以指定用戶端已知的屬性名稱。

如果用戶端要求包含由 [用戶端已知的屬性名稱] 所指定的屬性名稱，它就會轉換成 [伺服器已知的屬性名稱] 的值。同樣地，如果伺服器傳送的結果包含由 [伺服器已知的屬性名稱] 所指定的屬性名稱，它就會轉換成 [用戶端已知的屬性名稱] 的值。

6. 按一下 [儲存] 以建立此物件。

Directory Proxy Server 組態已經修改，您必須重新啓動依賴本組態的伺服器。現在還不要重新啓動伺服器。您可以將所有的組態都變更過後再進行。

7. 重複步驟 3 至步驟 6，以建立其他物件。

8. 若要重新啓動伺服器，請參閱「重新啓動 Directory Proxy Server」(第 47 頁)。

禁止的項目

因為各種不同的理由，LDAP 目錄中的特定項目 (或代表這些項目的屬性) 必須對 LDAP 用戶端隱藏。例如，如果您的目錄包含所有員工的項目，這些項目每個都包含員工資料的相關屬性，例如姓名、電子郵件位址、部門、辦公室位置、辦公室電話號碼、及家用電話號碼，您可以隱藏所有的員工家用電話號碼，不讓用戶端看到。

禁止的項目代表 LDAP 目錄中，需要對 LDAP 用戶端隱藏的項目。為了讓這類設定中的用戶端及伺服器之間能通訊，Directory Proxy Server 支援禁止的項目 - 也就是說，Directory Proxy Server 可以對 LDAP 用戶端隱藏這些項目的 LDAP 項目及屬性。

您可以利用 [禁止的項目] 內容，來定義控制隱藏目錄項目及其屬性的規則。此內容讓您指定必須用幾種方式隱藏的項目清單或項目的屬性。例如，您可以指定：

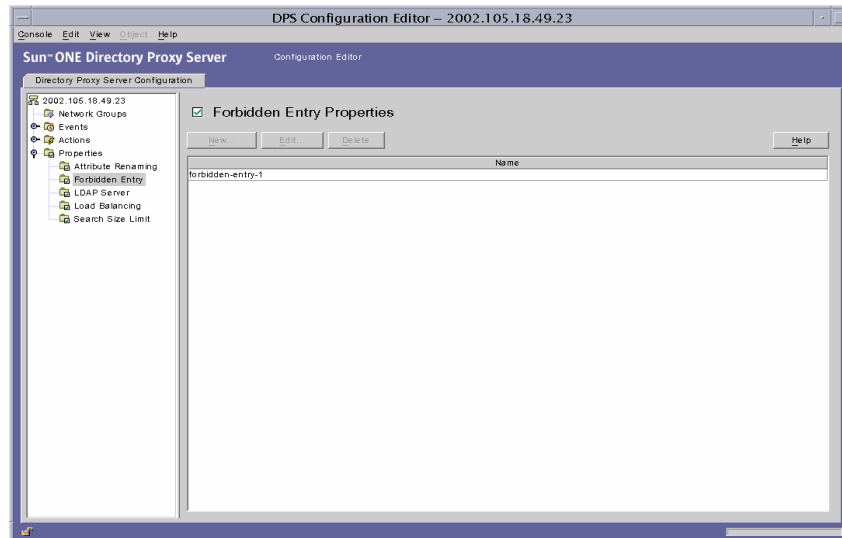
- 您要隱藏項目中的項目或屬性的 DN。
- 您要隱藏之項目中的項目或屬性的 DN 規則運算式 (例如，*. *OU=INTERNAL.*)。
- 項目的屬性名稱 / 值配對 (例如，secret:yes)。如果項目的屬性名稱 / 值配對與所指定的任一屬性名稱 / 值配對相符，就會隱藏該項目或其部份內容。

下一節會說明如何從 Directory Proxy Server 組態編輯器主控台建立禁止的項目內容的物件。

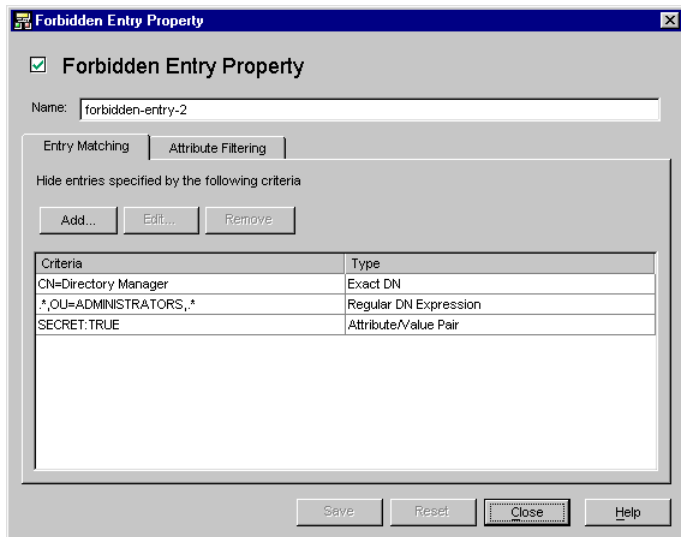
建立禁止的項目 ㄟ ㄟ 物件

若要識別 Directory Proxy Server 應對用戶端隱藏的任何項目之項目或屬性：

1. 存取 Directory Proxy Server 組態編輯器主控台；請參閱「存取 Directory Proxy Server 主控台」（第 33 頁）。
2. 在瀏覽樹狀目錄中展開 [內容] 節點，然後選取 [禁止的項目]。
右邊窗格會顯示現有的禁止的項目內容。



- 按一下 [新增]。
出現 [禁止的項目內容] 視窗。



- 在 [名稱] 欄位中，鍵入內容物件的名稱。名稱必須是唯一的英數字元字串。
- 在 [項目相符] 標籤中，指定適當的值；此標籤會顯示要隱藏的此內容名稱及 LDAP 項目之設定。

新增。顯示功能表，以新增隱藏 LDAP 項目的準則。準則可為下列類型：[精確 DN]、[規則 DN 運算式] 或 [屬性 / 值配對]。可以在項目中鍵入或瀏覽目錄資訊樹狀目錄，尋找現有的項目。

精確 DN。顯示對話方塊，以輸入要隱藏的項目 DN。

規則 DN 運算式。顯示對話方塊，以輸入要隱藏的項目的規則 DN 運算式。您應該以標準格式來指定 DN 的規則運算式，也就是說，RDN 元件與等號 (=) 之間應該沒有空格，且屬性名稱及值必須全為大寫字母。

例如，要將任何 DN 與 RDN 元件 `ou=internal` 進行比對，您必須指定如下：

```
.*OU=INTERNAL.*
```

如果 [屬性篩選] 標籤包含要併入的屬性名稱，而某個屬性與所列出的任一項都不相符，則不會傳回它。如果 LDAP 項目沒有屬性與 [屬性篩選標籤] 中要排除的任何屬性相符，就會傳回它。

您可以將以下的書籍做為規則運算式的參考「*Mastering Regular Expressions*」，Friedl 與 Oram 著，O'Reilly 發行，ISBN：1565922573。

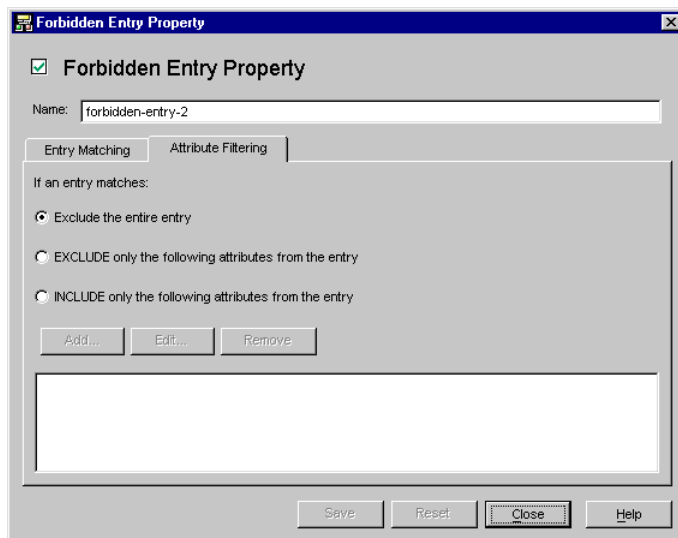
屬性 / 值配對。顯示對話方塊，以指定屬性名稱 / 值配對。如果項目的屬性名稱 / 值配對與所指定的任一屬性名稱 / 值配對相符，就會隱藏該項目或其部份內容。

例如，如果您要限制具有 `ou=internal` 屬性或 `secret=yes` 屬性的所有項目，則可指定下列項目屬性為 `ou`、值為 `internal`。

編輯。顯示編輯表格中目前所選項目的對話方塊。

移除。移除目前表格中選取的項目。

6. 選取 [屬性篩選] 標籤，並指定適當的值。



此標籤包含允許排除或特別併入的特定屬性的設定：

排除整個項目。選取此選項表示不執行屬性篩選並隱藏整個項目。

只從項目排除下列屬性。選取此選項表示表格包含要從項目 (已符合上述任一規格) 中排除之屬性名稱的清單。

只從項目包括下列屬性。選取此選項表示表格包含可傳回作為項目 (已符合上述任一規格) 一部份之屬性名稱的清單。

7. 按一下 [儲存] 以建立此物件。

Directory Proxy Server 組態已經修改，您必須重新啓動依賴本組態的伺服器。現在還不要重新啓動伺服器。您可以將所有的組態都變更過後再進行。

8. 重複步驟 3 至步驟 7，以建立其他物件。

- 若要重新啓動伺服器，請參閱「重新啓動 Directory Proxy Server」(第 47 頁)。

LDAP 伺服器物件

在目錄部署中，Directory Proxy Server 位於 LDAP 用戶端及 LDAP 目錄伺服器之間。在將 LDAP 用戶端傳送的要求轉送給 LDAP 目錄伺服器之前，先進行篩選，並於伺服器回應傳送給用戶端之前，進行同樣的作業。Directory Proxy Server 也在一組複製的目錄伺服器之間，支援自動負載平衡及自動容錯移轉及容錯回復功能。

您可以利用 [LDAP 伺服器] 內容，識別 Directory Proxy Server 應該用來當作後端伺服器的目錄伺服器。當定義此內容時，您可以指定 Directory Proxy Server 需要的所有詳細資料 - 例如，目錄伺服器的 IP 位址或完全合格主機名稱、目錄伺服器監聽用戶端連線的連接埠號碼、伺服器支援的 LDAP 版本、用於 Directory Proxy Server 及此伺服器之間通訊的版本，等等 - 以便與目錄伺服器通訊。

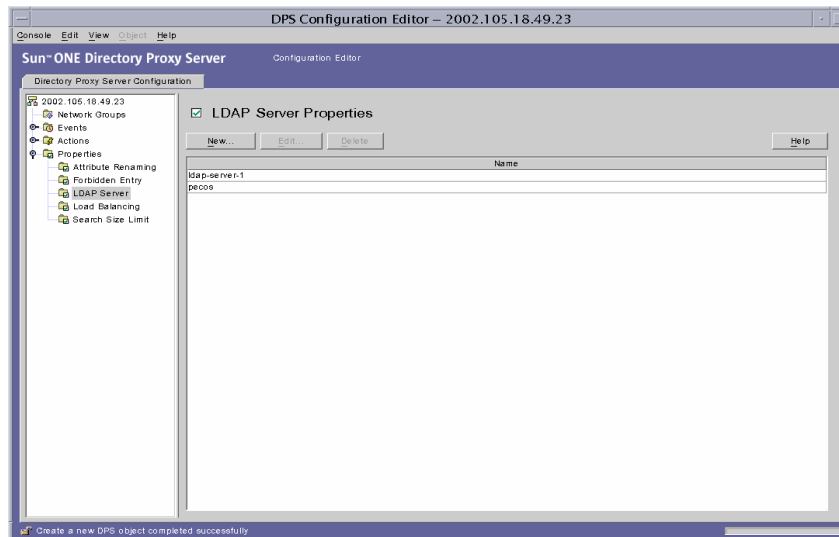
下一節會說明如何從 Directory Proxy Server 組態編輯器主控台建立 LDAP 伺服器內容的物件。

建立 LDAP 伺服器物件

若要識別 Directory Proxy Server 應與其通訊的目錄伺服器：

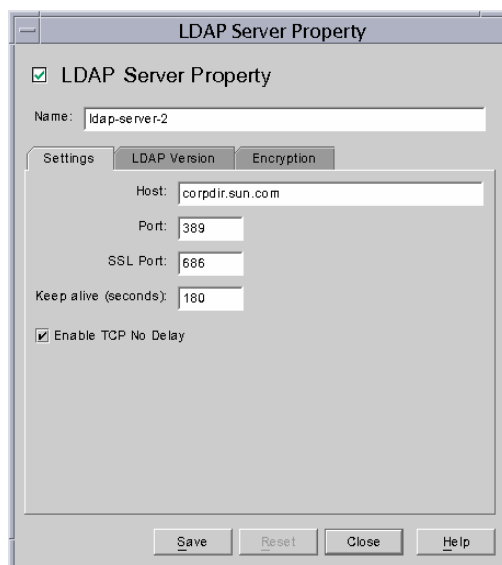
- 存取 Directory Proxy Server 組態編輯器主控台；請參閱「存取 Directory Proxy Server 主控台」(第 33 頁)。

2. 在瀏覽樹狀目錄中展開 [內容] 節點，然後選取 [LDAP 伺服器]。
右邊窗格會顯示現有的 [LDAP 伺服器] 內容物件。



3. 按一下 [新增]。
出現 [LDAP 伺服器內容] 視窗。

4. 在 [名稱] 欄位中，鍵入內容物件的名稱。名稱必須是唯一的英數字元字串。



5. 在 [設定] 標籤中指定此內容轉介的 LDAP 伺服器的基本設定。

主機。輸入一個值，以指定執行後端 LDAP 伺服器之主機的完整網域名稱或 IP 位址。此屬性是強制的。

連接埠。輸入可指定執行後端 LDAP 伺服器之連接埠的數字。如果沒有此屬性，則使用的預設連接埠為 389。

SSL 連接埠。輸入可指定後端 LDAP 伺服器監聽 LDAPS (LDAP over SSL) 連線之連接埠的數字。如果後端 LDAP 伺服器不支援 LDAPS，則請勿為此屬性設定任何值。

Keep Alive 間隔。輸入秒數，讓 Directory Proxy Server 等待此時間之後，才查詢未回應伺服器，以判斷連至 LDAP 目錄伺服器的網路連結是否已關閉，或是 LDAP 目錄伺服器已成為未回應伺服器。如果連線到 Directory Proxy Server 的用戶端具有擱置中的作業，且如果 Directory Proxy Server 在此處所指定的秒數內，均未收到連線 LDAP 的任何資料，則 Directory Proxy Server 將開啓連至它的另一個通訊通道，以測試 LDAP 伺服器的可用性。如果 Directory Proxy Server 無法進行此動作，它將會容錯移轉至另一個 LDAP 伺服器 (如果有)。此屬性的預設值為 180 秒。如果 LDAP 伺服器與 Directory Proxy Server 不是位於相同的區域網路，則建議您增加此值。

啓用 TCP 未延遲。 停用此選項，可導致 Directory Proxy Server 在連至此伺服器的連線上使用 Nagel 演算法。只有在 Directory Proxy Server 與此物件項目所定義的伺服器之間的網路頻寬非常有限時，才能停用此選項。預設會啓用此設定。

6. 選取 [LDAP 版本] 標籤，並指定適當的值。



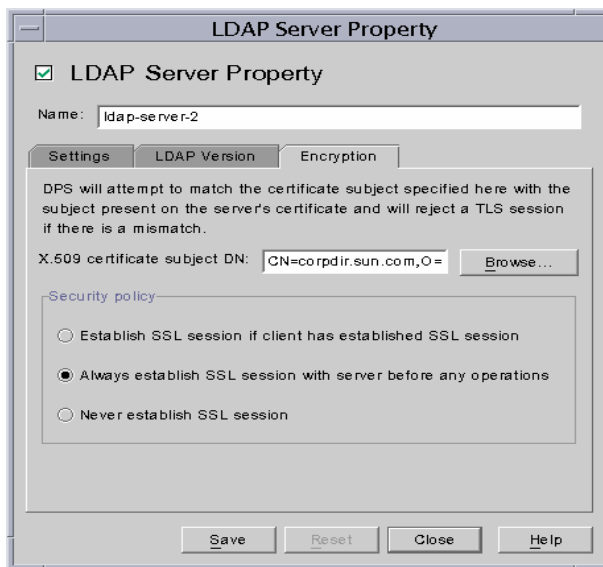
此標籤可顯示設定，指出此伺服器支援哪些 LDAP 版本，以及 Directory Proxy Server 與此伺服器之間的通訊應使用哪個版本。

支援的 LDAP 版本。 從現有的兩個選項中選取之一：LDAP 版本 2 和 3，或是僅 LDAP 版本 2。預設為 LDAP 版本 2 和 3。

要使用的 LDAP 版本。 從現有的三個選項中選取之一：「用戶端使用中的任何版本」、「僅 LDAP 版本 3」，或「僅 LDAP 版本 2」。與此項目所定義的後端伺服器對話時，此屬性告知 Directory Proxy Server 要使用的慣用 LDAP 通訊協定版本。預設會選取「用戶端使用中的任何版本」。

當您擁有 Directory Proxy Server 跟隨轉介所需的 LDAPv2 用戶端時，此選項就很有幫助。在這種情況下，Directory Proxy Server 本身需要作為 LDAPv3 用戶端連線到後端伺服器，才能讓後端伺服器將轉介傳回給它。如果參照此內容的網路群組允許多重 LDAP 版本 2 連結，則必須選取僅 LDAP 版本 3。

7. 選取 [加密] 標籤，並指定適當的值。



此標籤可顯示與 LDAP 伺服器 (此內容所參照) 的安全通訊相關的設定。

X.509 憑證主體 DN。指定 LDAP 伺服器的憑證主體名稱。如已指定，則 Directory Proxy Server 就會嘗試比對憑證主體與 LDAP 伺服器憑證上出現的主體，且會在出現不相符時拒絕 TLS 工作階段 (此屬性允許 Directory Proxy Server 驗證連線的 LDAP 伺服器。如果沒有設定此屬性，Directory Proxy Server 就會接受任何名稱)。

安全原則。選取選項之一以定義 Directory Proxy Server 與後端伺服器之間連線的安全性原則：[如果用戶端已建立 SSL 工作階段，則建立 SSL 工作階段]、[永遠在任何操作之前建立與伺服器的 SSL 工作階段]，或是 [永不建立 SSL 工作階段]。

8. 按一下 [儲存] 以建立此物件。
- Directory Proxy Server 組態已經修改，您必須重新啟動依賴本組態的伺服器。現在還不要重新啟動伺服器。您可以將所有的組態都變更過後再進行。
9. 重複步驟 3 至步驟 8，以建立其他物件。
 10. 若要重新啟動伺服器，請參閱「重新啟動 Directory Proxy Server」(第 47 頁)。

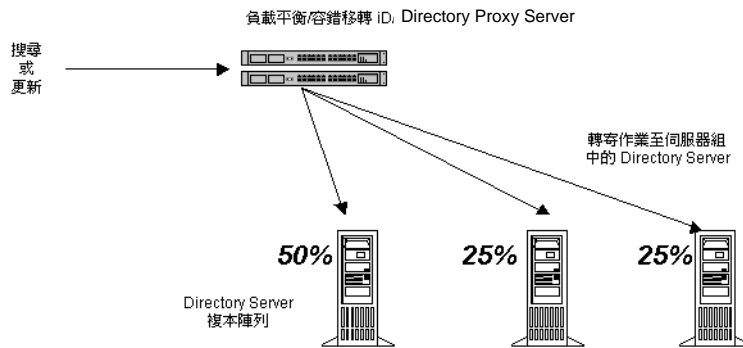
負載平衡

Directory Proxy Server 在一組複製的 LDAP 目錄伺服器之間，提供自動負載平衡及容錯移轉與容錯回復功能，啓用高可用性目錄部署作業。爲了讓 Directory Proxy Server 達成此目的，您必須識別應與 Directory Proxy Server 合用的目錄伺服器，並指定如何在這些伺服器之間分散用戶端負載。

您可利用 [負載平衡] 內容，設定讓 Directory Proxy Server 處理負載平衡。此內容讓您識別 Directory Proxy Server 應與其通訊的後端目錄伺服器，並指定每個目錄伺服器應接收的總用戶端負載百分比。一旦設定之後，Directory Proxy Server 會自動將用戶端查詢分配給不同的目錄伺服器，以符合組態中定義的負載準則。如果目錄伺服器故障，Directory Proxy Server 就會在可用的伺服器之間，根據各個負載百分比，按照比例分配各個伺服器的負載百分比。如果所有的後端 LDAP 伺服器都故障，Directory Proxy Server 就會開始拒絕用戶端的查詢。

圖 7-2 顯示在一組三個目錄伺服器副本之間，所分散的用戶端負載。

圖 7-2 在一組 LDAP 目錄伺服器副本上負載平衡



Directory Proxy Server 是根據工作階段處理負載平衡。這表示選擇將用戶端查詢導向到特定目錄伺服器的決策功能，會對每個用戶端工作階段套用一次；尤其是在用戶端工作階段開始時。所有該工作階段後續的用戶端查詢，都會導向到工作階段開始時所選擇的相同目錄伺服器。

Directory Proxy Server 可負載平衡的後端 LDAP 伺服器數量，需視幾個因素而定，其中幾個列於以下：

- 執行 Directory Proxy Server 的主機大小
- 可用的網路頻寬

- Directory Proxy Server 接收到的各個查詢
- 用戶端工作階段的長度
- Directory Proxy Server 的組態

一般來說，如果大部分的工作階段存活時間都很短，而且查詢需要大量運算，Directory Proxy Server 能支援的目錄伺服器就比較少。需要大量運算的查詢必須檢查整個訊息，譬如使用屬性重新命名 (請參閱「屬性重新命名內容」(第 92 頁)) 功能時。

Directory Proxy Server 會在連線嘗試收到連線拒絕的錯誤或逾時時，偵測到目錄伺服器何時故障。由於這二個情形都是在工作階段的初始階段發生，而且當時沒有為該工作階段處理任何作業，所以如果有可以透明使用的伺服器，Directory Proxy Server 就會容錯移轉至另一個伺服器。如果是連線嘗試逾時，用戶端取得回應的時間就可能延遲過久。如果突然失去 Directory Proxy Server 及後端伺服器之間的連線，Directory Proxy Server 就會對所有待執行的作業將 LDAP_BUSY 錯誤傳回給受到影響的用戶端。然後 Directory Proxy Server 會將該用戶端連線容錯移轉至另一個目錄伺服器。

為了避免 Directory Proxy Server 變成目錄部署的單一失效點，我們建議您至少使用二個 Directory Proxy Server，並在前面新增 IP 設備。第 2 章「Sun ONE Directory Proxy Server 部署方式」中將說明此點。不可能以此方式部署 Directory Proxy Server 時，建議您使用 -M 切換，讓 Directory Proxy Server 來自我監視。

Directory Proxy Server 使用監視程序來檢查後端伺服器的健康狀況。如果使用負載平衡，本功能就會自動啟用。Directory Proxy Server 每 10 秒就會對其後端目錄伺服器執行匿名搜尋作業，搜尋 Root DSE。如果其中一個故障或未回應，Directory Proxy Server 就會將其從可以使用的負載平衡伺服器組中移除。伺服器又可以使用時，就會將其再加入這個組裡面。為了讓監視功能運作有效率，您必須根據「Directory Proxy Server 安裝指南」的第 2 章「電腦系統需求」中描述的 `idsktune` 公用程式建議，設定 Directory Proxy Server 正在執行的主機。伺服器只啓用其安全連接埠時，Directory Proxy Server 會嘗試以安全的方式執行健康檢查。

下一節會說明如何從 Directory Proxy Server 組態編輯器主控台建立負載平衡內容的物件。

注意： 您為負載平衡內容建立的任何物件，必須至少有一個 [LDAP 伺服器] 內容，且百分比必須累計為 100%。否則 Directory Proxy Server 會啓動失敗。

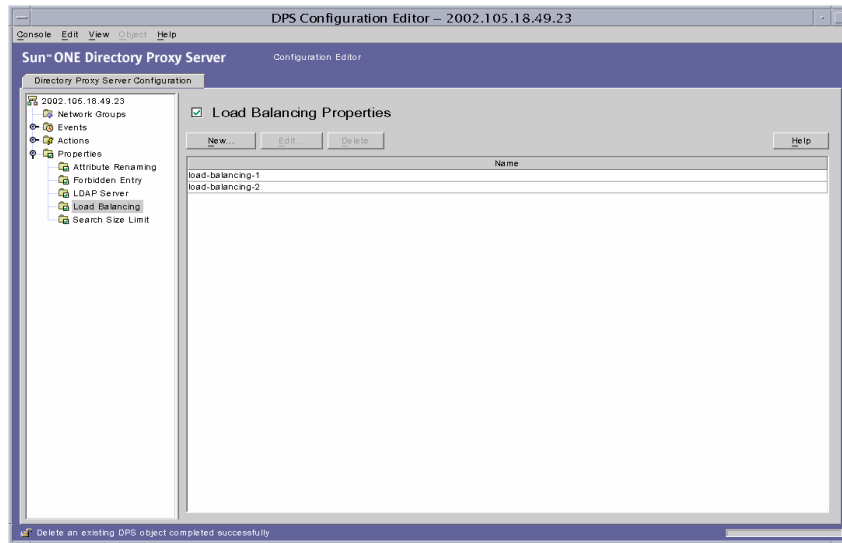
建立負載平衡內容物件

本節說明如何設定讓 Directory Proxy Server 處理負載平衡。在您為負載平衡內容建立物件之前，請務必識別 Directory Proxy Server 應該用來平衡用戶端負載的 LDAP 目錄伺服器。如需詳細資訊，請參閱「LDAP 伺服器內容」（第 99 頁）。

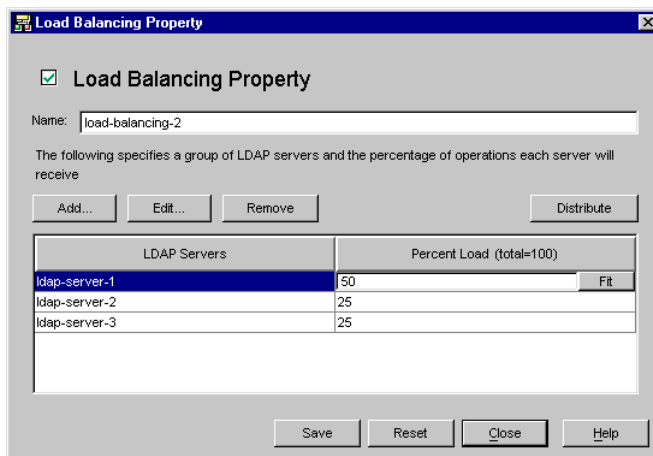
若要定義 Directory Proxy Server 應如何在一組目錄伺服器之間平衡負載：

1. 存取 Directory Proxy Server 組態編輯器主控台；請參閱「存取 Directory Proxy Server 主控台」（第 33 頁）。
2. 在瀏覽樹狀目錄中展開 [內容] 節點，然後選取 [負載平衡]。

右邊窗格會顯示現有的 [負載平衡] 內容物件清單。



- 按一下 [新增]。
出現 [負載平衡內容] 視窗。



- 在 [名稱] 欄位中，鍵入內容物件的名稱。名稱必須是唯一的英數字元字串。
- 利用剩餘的表單元素取得想要的結果。

若要編輯百分比，請按一下包含 LDAP 伺服器之列旁的 [百分比負載] 直欄，鍵入介於 0 與 100 的數字，然後按下 [調整] 按鈕。此動作會將百分比指派到嘗試加總所有百分比為 100 的目前列。目前的百分比總和會顯示在 [百分比負載] 欄名中。

新增。顯示對話方塊，以將轉介新增到 LDAP 伺服器內容。預設會為新增的第一台伺服器指派百分之百的負載，而後續新增的伺服器則為 0%。

編輯。顯示編輯表格中目前所選的項目的對話方塊。

移除。從跨伺服器執行負載平衡之伺服器的清單中，移除目前選取的 LDAP 伺服器。

分散。將百分比負載平均分散到表格中轉介的所有 LDAP 伺服器。

- 按一下 [儲存] 以建立此物件。
Directory Proxy Server 組態已經修改，您必須重新啟動依賴本組態的伺服器。現在還不要重新啟動伺服器。您可以將所有的組態都變更過後再進行。
- 重複步驟 3 至 步驟 6，以建立其他物件。
- 若要重新啟動伺服器，請參閱「重新啟動 Directory Proxy Server」(第 47 頁)。

搜尋大小限制內容

通常 LDAP 目錄可當作組織的中央儲存庫，讓跨組織部署的 LDAP 用戶端尋找資訊。LDAP 用戶端一般都會利用搜尋篩選條件搜尋特定資訊，以尋找資訊。搜尋項目時，用戶端一般都會指定與項目類型有關聯的屬性；例如當您搜尋人員項目時，可利用 CN 屬性搜尋特定人名的人。

Directory Proxy Server 可用來處理數千個 LDAP 用戶端要求，並可設定在 LDAP 目錄上套用複雜的存取控制原則，譬如控制誰可以在目錄資訊樹狀目錄 (DIT) 的不同部分上、執行不同類型的作業。您也可以設定讓 Directory Proxy Server 禁止特定類型作業，例如下載大量網頁的人及自動尋檢程式收集目錄內包含的資訊時，所執行的作業。

您可以利用 [搜尋大小限制] 內容，根據搜尋基準及搜尋範圍以套用大小限制。如果此內容物件項目所指定的搜尋基準或搜尋範圍都不符合特定搜尋，則大小限制就會預設為 [網路群組] 物件項目中指定的大小限制；請參閱第 6 章「建立及管理群組」。

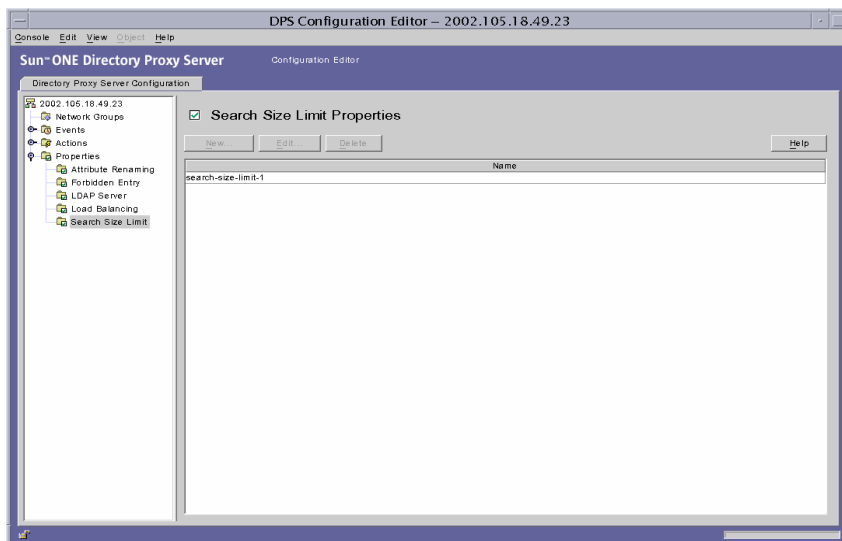
下一節會說明如何從 Directory Proxy Server 組態編輯器主控台建立搜尋大小限制內容的物件。

建立搜尋大小限制內容物件

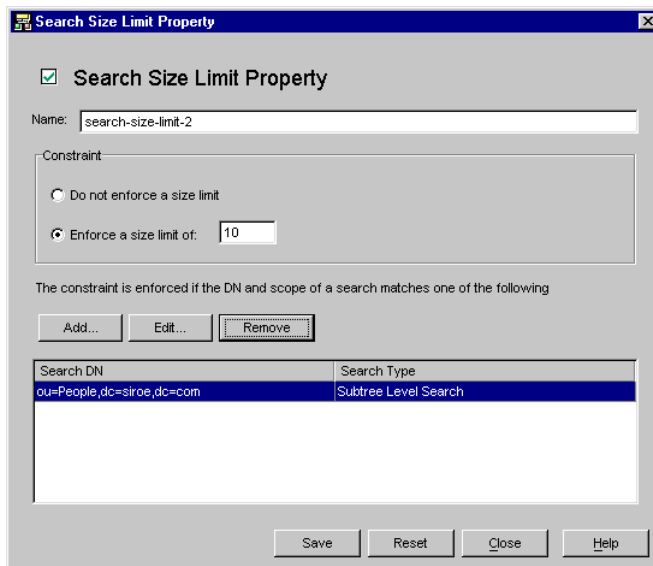
若要定義 Directory Proxy Server 應如何限制搜尋大小：

1. 存取 Directory Proxy Server 組態編輯器主控台；請參閱「存取 Directory Proxy Server 主控台」（第 33 頁）。

- 在瀏覽樹狀目錄中展開 [內容] 節點，然後選取 [搜尋大小限制]。



- 按一下 [新增]。
出現 [搜尋大小限制內容] 視窗。



- 在 [名稱] 欄位中，鍵入內容物件的名稱。名稱必須是唯一的英數字元字串。

5. 利用剩餘的表單元素取得想要的結果：
 - 限制。**指定是否強制實施大小限制。
 - 不強制大小限制。**選取此選項，以指定不強制實施大小限制。
 - 強制以下大小限制。**選取此選項並輸入整數值，以指定要強制實施的大小限制。
 - 新增。**顯示功能表，以新增大小限制。限制必須為兩個類型之一：單層次搜尋及樹狀子目錄層次搜尋。
 - 單層次搜尋。**顯示對話方塊，以輸入 DN 並將其新增至限制表格。如果單層次搜尋的搜尋基礎 DN，符合條件表格中單層次搜尋所指定的識別名稱之一，則系統會實施指定的大小限制，作為該搜尋的大小限制。
 - 樹狀子目錄層次搜尋。**顯示對話方塊，以輸入 DN。如果樹狀子目錄搜尋的搜尋基礎的 DN，符合條件表格中樹狀子目錄層次搜尋所指定的識別名稱之一，則系統會強制實施指定的大小限制，作為該搜尋的大小限制。
 - 編輯。**顯示編輯表格中目前所選項目的對話方塊。
 - 移除。**移除目前表格中選取的項目。
6. 按一下 [儲存] 以建立此物件。

Directory Proxy Server 組態已經修改，您必須重新啟動依賴本組態的伺服器。現在還不要重新啟動伺服器。您可以將所有的組態都變更過後再進行。
7. 重複 步驟 3 至 步驟 6，以建立其他物件。
8. 若要重新啟動伺服器，請參閱「重新啟動 Directory Proxy Server」(第 47 頁)。

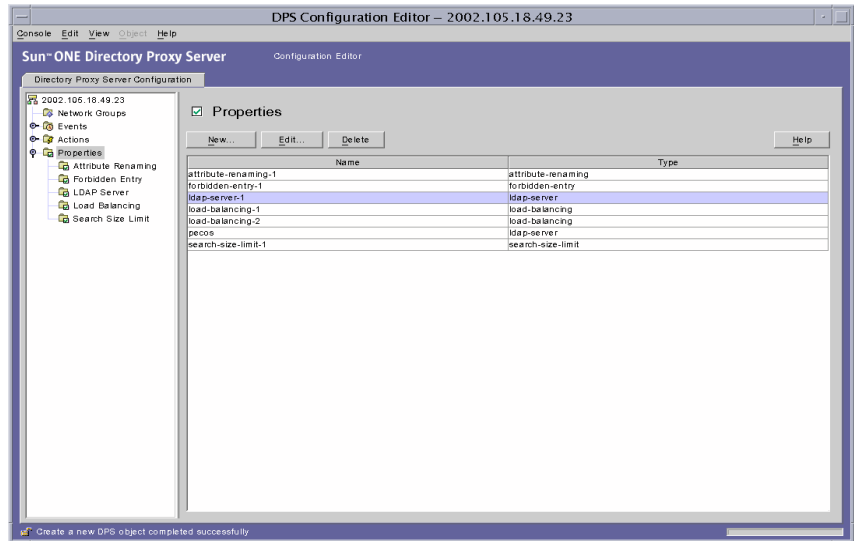
修改內容物件

若要修改內容物件：

1. 存取 Directory Proxy Server 組態編輯器主控台；請參閱「存取 Directory Proxy Server 主控台」(第 33 頁)。

2. 在瀏覽樹狀目錄中，選取 [內容] 節點。

右邊窗格會顯示現有的內容物件清單。若要檢視屬於特定內容的物件，請展開 [內容] 節點，然後選取您要的內容。



3. 在清單中選取您要修改的物件，然後按一下 [編輯]。
4. 進行必要的修改。
5. 按一下 [儲存] 以儲存您的變更。

Directory Proxy Server 組態已經修改，您必須重新啓動依賴本組態的伺服器。現在還不要重新啓動伺服器。您可以將所有的組態都變更過後再進行。

6. 重複步驟 3 至步驟 5，以修改其他物件。
7. 若要重新啓動伺服器，請參閱「重新啓動 Directory Proxy Server」(第 47 頁)。

刪除物件

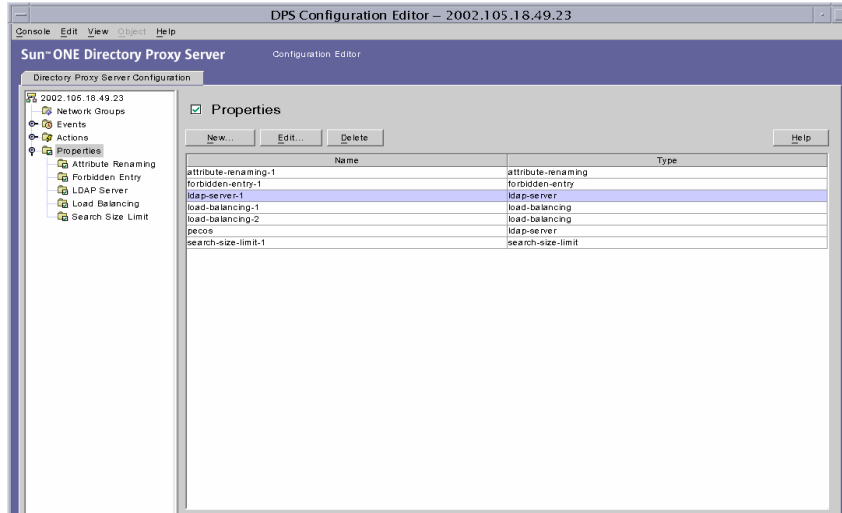
您可以從 Directory Proxy Server 組態刪除任何不要的內容物件。刪除物件之前，請確定任何其他的組態項目中都沒有使用這個物件。

若要刪除內容物件：

1. 存取 Directory Proxy Server 組態編輯器主控台；請參閱「存取 Directory Proxy Server 主控台」(第 33 頁)。

2. 在瀏覽樹狀目錄中，選取 [內容] 節點。

右邊窗格會顯示現有的內容物件清單。若要檢視屬於特定內容的物件，請展開 [內容] 節點，然後選取您要的內容。



3. 在清單中選取您要刪除的物件，然後按一下 [刪除]。
4. 確認您的動作。

Directory Proxy Server 組態已經修改，您必須重新啓動依賴本組態的伺服器。現在還不要重新啓動伺服器。您可以將所有的組態都變更過後再進行。

5. 重複步驟 3 及步驟 4，以刪除其他物件。
6. 若要重新啓動伺服器，請參閱「重新啓動 Directory Proxy Server」(第 47 頁)。

建立及管理事件物件

Sun ONE Directory Proxy Server 支援事件導向的動作，也就是可以設定讓 Directory Proxy Server 在發生特定事件時，執行所指定的動作。本章說明如何利用 Directory Proxy Server 組態編輯器主控台建立及管理事件物件。

本章包含下列各節：

- 事件概論 (第 113 頁)
- 建立事件物件 (第 114 頁)
- 修改事件物件 (第 118 頁)
- 刪除事件物件 (第 119 頁)

事件概論

*事件*就是 Directory Proxy Server 在執行時的某個特定點的特定狀態。您可以利用事件物件來指定在預先判定的狀態時，Directory Proxy Server 應評估的條件。您也必須指定 Directory Proxy Server 在達到條件時應採取的動作，以進行事件物件的部分定義作業。如需有關動作的詳細資訊，請參閱第 9 章「建立及管理動作物件」。

目前 Directory Proxy Server 可辨識或追蹤兩種事件：

- OnBindSuccess 事件 - 用戶端順利完成連結作業時就會評估本事件。
- OnSSLEstablished 事件 - 用戶端順利建立 SSL 工作階段時就會評估本事件。此事件沒有任何相關聯的條件，且永遠會執行其動作清單。

您只能根據這二個事件來定義事件物件。例如，您可以定義一個事件，用來偵測用戶端何時順利完成連結作業。本定義的部分可以用來在事件發生時採取某些動作，例如變更用戶端的存取群組。如需有關群組的詳細資訊，請參閱第 6 章「建立及管理群組」。

建立事件物件

本節說明如何根據 OnBindSuccess 及 OnSSLEstablished 事件來建立事件物件。如需有關這些事件的詳細資訊，請參閱「事件概論」(第 113 頁)。

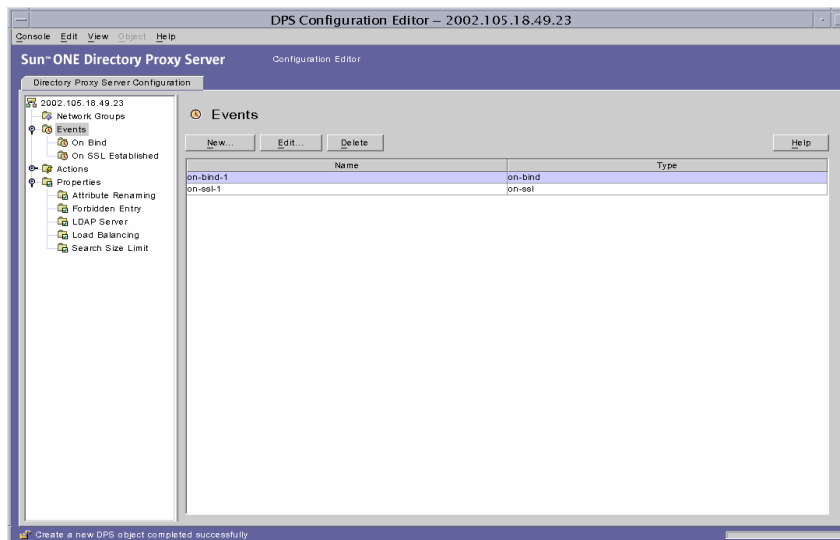
- 建立 OnBindSuccess 事件物件
- 建立 OnSSLEstablished 事件物件

建立 OnBindSuccess 事件物件

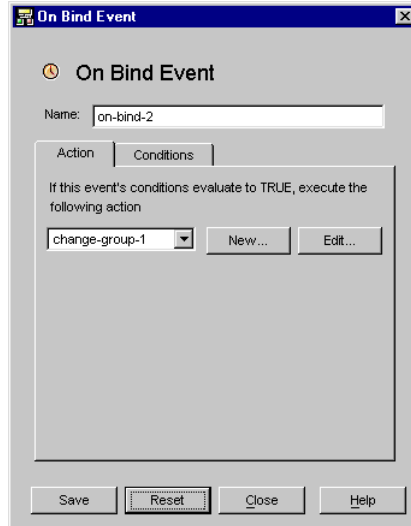
若要根據 OnBindSuccess 事件來建立事件物件：

1. 存取 Directory Proxy Server 組態編輯器主控台；請參閱「存取 Directory Proxy Server 主控台」(第 33 頁)。
2. 在瀏覽樹狀目錄中展開 [事件] 節點，然後選取 [連結後續動作]。

右邊窗格會顯示現有的事件物件中，以 OnBindSuccess 為基礎的事件清單。



- 按一下 [新增]。
出現 [連結後續事件] 視窗。



- 在 [名稱] 欄位中，鍵入事件物件的名稱。名稱必須是唯一的英數字元字串。
- 在 [動作] 標籤中，選取事件發生時要執行的動作 (也就是當事件評估為 **True** 時)。
新增。您也可以按一下 [新增] 按鈕，定義新的動作物件。
編輯。按一下 [編輯] 按鈕，修改屬於目前選取的動作物件參數。

6. 選取 [條件] 標籤，並指定條件。



只有在符合所指定的條件時，此事件才會評估為 **TRUE** - 也就是本標籤所指定的準則必須評估為 **TRUE**，[動作] 標籤中指定的動作才會執行。如果滿足用戶端 SSL 工作階段條件，且至少滿足三個用戶端連結條件之一，則條件一定為 **TRUE**。

需要用戶端 SSL 工作階段。 選取此選項，以指出只有在用戶端利用 Directory Proxy Server 建立 SSL 工作階段時，狀況才會評估為 **TRUE**。預設為 **FALSE**。

用戶端連結條件。 條件是下列選項之一：[匿名連結]、[密碼型連結] 及 [任何 SASL 型連結]。

匿名連結。 選取此選項表明只有在符合用戶端 SSL 工作階段需求，且用戶端已順利完成匿名連結時，才將條件評估為 **TRUE**。

密碼型連結。 選取此選項表明只有在符合用戶端 SSL 工作階段需求，且用戶端已順利完成密碼型連結時，才將條件評估為 **TRUE**。

任何 SASL 型連結。 選取此選項，表示只有在符合用戶端 SSL 工作階段需求，且用戶端已使用任何 SASL 機制順利完成連結時，才會將條件評估為 **TRUE**。

7. 按一下 [儲存] 以建立此事件物件。

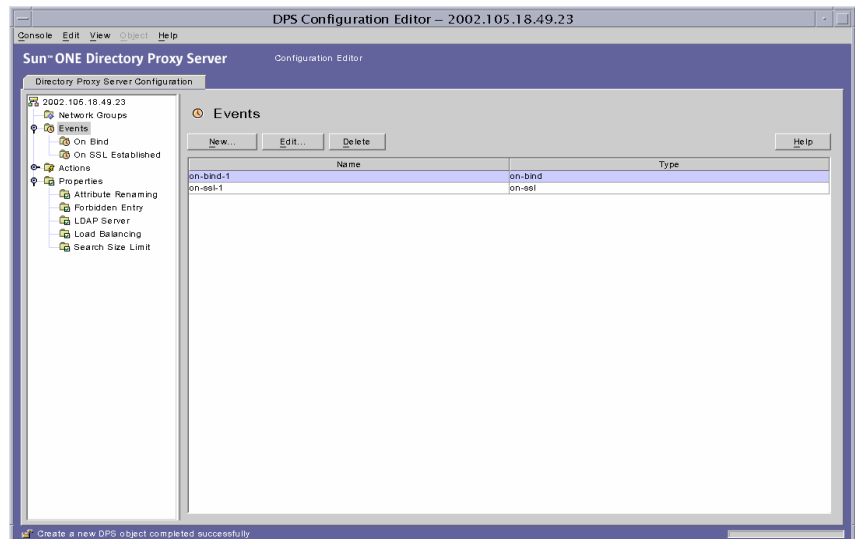
Directory Proxy Server 組態已經修改，您必須重新啟動依賴本組態的伺服器。現在還不要重新啟動伺服器。您可以將所有的組態都變更過後再進行。

8. 重複步驟 3 至步驟 7，以建立其他物件。
9. 若要重新啟動伺服器，請參閱「重新啟動 Directory Proxy Server」(第 47 頁)。

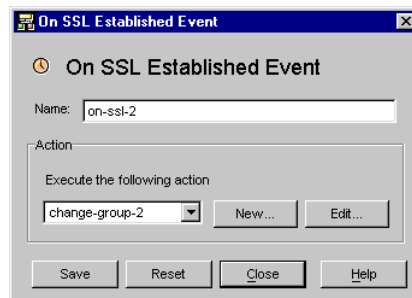
建立 OnSSLEstablished 事件物件

若要根據 OnSSLEstablished 事件來建立事件物件：

1. 存取 Directory Proxy Server 組態編輯器主控台；請參閱「存取 Directory Proxy Server 主控台」（第 33 頁）。
 2. 在瀏覽樹狀目錄中展開 [事件] 節點，然後選取 [建立的 SSL 後續動作]。
- 右邊窗格會顯示現有的事件物件中，以 OnSSLEstablished 為基礎的事件清單。



3. 按一下 [新增]。
- 出現 [建立的 SSL 後續事件] 視窗。



4. 在 [名稱] 欄位中，鍵入事件物件的名稱。名稱必須是唯一的英數字元字串。

5. 在 [動作] 區域中, 選取事件發生時要執行的動作 (也就是當事件評估為 TRUE 時)。

按一下 [編輯] 按鈕, 修改屬於目前選取的動作參數。您也可以按一下 [新增] 按鈕, 定義新的動作。

6. 按一下 [儲存] 以建立此事件物件。

Directory Proxy Server 組態已經修改, 您必須重新啟動依賴本組態的伺服器。現在還不要重新啟動伺服器。您可以將所有的組態都變更過後再進行。

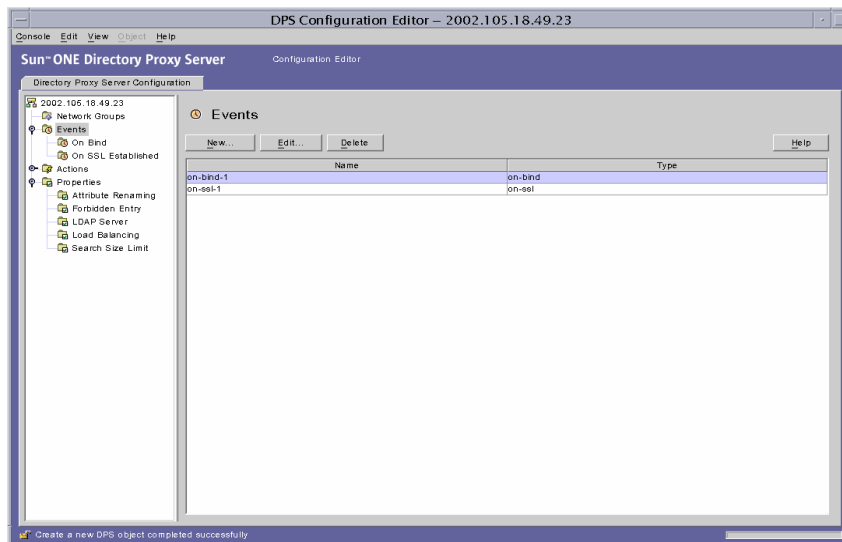
7. 重複步驟 3 至步驟 6, 以建立其他物件。
8. 若要重新啟動伺服器, 請參閱 「重新啟動 Directory Proxy Server」 (第 47 頁)。

修改事件物件

若要修改事件物件：

1. 存取 Directory Proxy Server 組態編輯器主控台；請參閱 「存取 Directory Proxy Server 主控台」 (第 33 頁)。
2. 在瀏覽樹狀目錄中, 選取 [事件]。

右邊窗格會顯示現有的事件物件清單。若要檢視屬於事件類型的物件, 請展開 [事件] 節點, 然後選取您要的事件類型。



3. 在清單中選取您要修改的事件物件，然後按一下 [編輯]。
4. 進行必要的修改。
5. 按一下 [儲存] 以儲存您的變更。

Directory Proxy Server 組態已經修改，您必須重新啟動依賴本組態的伺服器。現在還不要重新啟動伺服器。您可以將所有的組態都變更過後再進行。

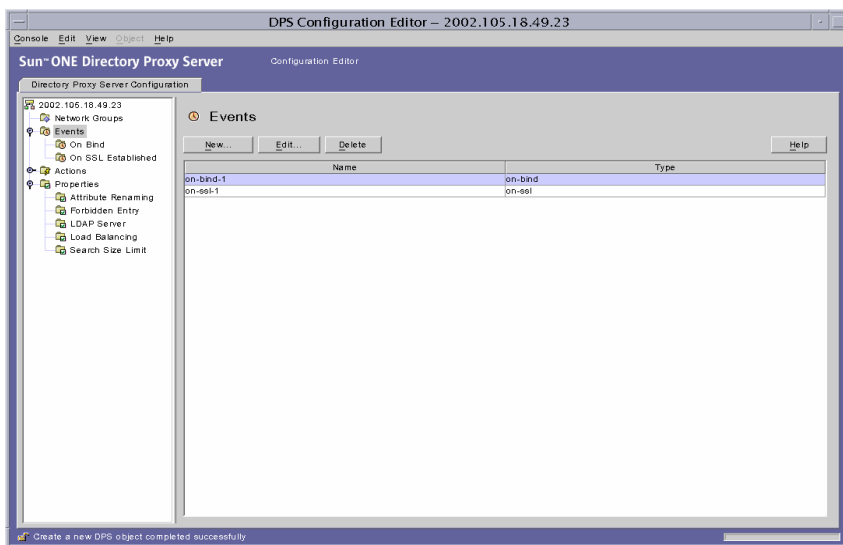
6. 重複步驟 3 至步驟 5，以修改其他物件。
7. 若要重新啟動伺服器，請參閱「重新啟動 Directory Proxy Server」(第 47 頁)。

刪除事件物件

您可以從 Directory Proxy Server 組態刪除任何不要的事件物件。若要刪除事件物件：

1. 存取 Directory Proxy Server 組態編輯器主控台；請參閱「存取 Directory Proxy Server 主控台」(第 33 頁)。
2. 在瀏覽樹狀目錄中，選取 [事件] 節點。

右邊窗格會顯示現有的事件物件清單。若要檢視屬於事件類型的物件，請展開 [事件] 節點，然後選取您要的事件類型。



3. 在清單中選取您要刪除的事件物件，然後按一下 [刪除]。

4. 出現提示時，確認您的動作。

您刪除的事件物件名稱現在已經從清單上移除。Directory Proxy Server 組態已經修改，您必須重新啓動依賴本組態的伺服器。現在還不要重新啓動伺服器。您可以將所有的組態都變更過後再進行。

5. 重複步驟 3 及步驟 4，以刪除其他物件。
6. 若要重新啓動伺服器，請參閱「重新啓動 Directory Proxy Server」(第 47 頁)。

建立及管理動作物件

Sun ONE Directory Proxy Server 支援事件導向的動作，也就是可以設定在發生特定事件時，讓 Directory Proxy Server 執行所指定的動作。本章說明如何利用 Directory Proxy Server 組態編輯器主控台建立及管理動作物件。

本章包含下列各節：

- 動作概論 (第 121 頁)
- 建立動作物件 (第 122 頁)
- 修改動作物件 (第 124 頁)
- 刪除動作物件 (第 125 頁)

動作概論

*動作*代表 Directory Proxy Server 可執行的工作。您可以利用動作物件，來指定當事件物件定義的規則或條件評估為 TRUE 時，Directory Proxy Server 應採取的動作。事件物件是用來指定在預先判定的狀態時，由 Directory Proxy Server 所評估的條件。如需有關事件的詳細資訊，請參閱第 8 章「建立及管理事件物件」。

目前 Directory Proxy Server 可執行一個名為 ChangeGroup 的動作。此動作可讓您設定 Directory Proxy Server，以便根據規則的評估，將某個用戶端從這個存取群組變更到另一個存取群組。如需有關群組的詳細資訊，請參閱第 6 章「建立及管理群組」。

如果您的 LDAP 目錄包含行動使用者 (例如從不同的 IP 位址或地點連線到目錄的使用者) 的資訊, change-group 功能就特別有用。您可用特殊的方式安裝 Directory Proxy Server, 讓行動使用者以動態 IP 位址連線到 Directory Proxy Server, 並歸為「預設」存取群組。「預設」存取群組的規則以 OnBindSuccess 事件為準, 只有在行動使用者通過驗證後才會評估為 TRUE。此規則也有 ChangeGroup 動作, 可以設定成在行動使用者以靜態 IP 位址存取 Directory Proxy Server 時, 將行動使用者從「預設」存取群組變更到一般會被指派到的存取群組。

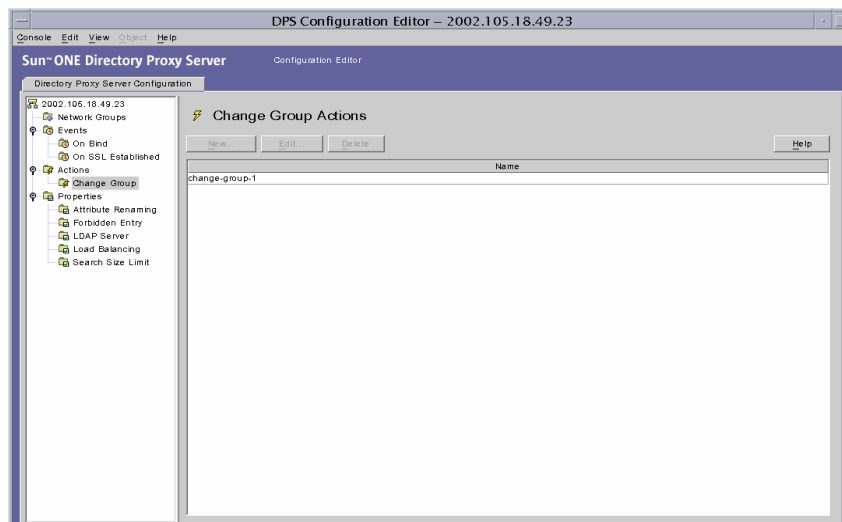
建立動作物件

您可建立某些事件發生時, 必須執行的動作物件。下列說明如何建立變更群組的動作物件。

若要建立將用戶端從一個群組變更到另一個群組的物件:

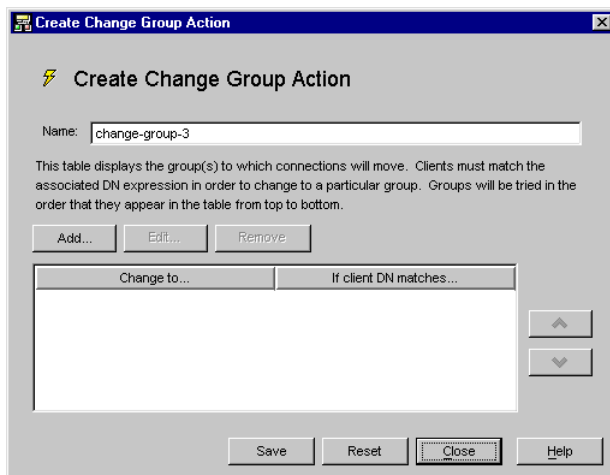
1. 存取 Directory Proxy Server 組態編輯器主控台; 請參閱「存取 Directory Proxy Server 主控台」(第 33 頁)。
2. 在瀏覽樹狀目錄中展開 [動作] 節點, 然後選取 [變更群組]。

右邊窗格會顯示現有的動作物件清單。



3. 按一下 [新增]。

出現 [建立變更群組動作] 視窗。



4. 在 [名稱] 欄位中，鍵入物件的名稱。名稱必須是唯一的英數字元字串。

5. 在 [動作] 標籤中，選取事件發生時要執行的動作（也就是當事件評估為 TRUE 時）。

變更到 ... 顯示用戶端可變更到的群組清單。若要進行變更，用戶端必須符合與每個群組都有關聯的 DN 運算式。若要編輯與特定群組或 [未變更] 項目相關的 DN 運算式，請按一下表格中的 [如果用戶端 DN 符合] 欄。系統會從上而下評估清單，直到與 DN 運算式相符為止。因此，將最常見的 DN 運算式放在清單底端，讓系統能夠評估所有運算式，是非常重要的。

您必須將規則運算式正常化（也就是說，RDN 元件與等號 (=) 之間不應有空格），以及所有屬性名稱及值必須大寫。

您可利用下列書籍做為規則運算式的參考：「*Mastering Regular Expressions*」，Friedl 與 Oram 著，O'Reilly 發行，ISBN：1565922573。

新增。 顯示添加群組的功能表，可以讓用戶端連線變更到這個群組。群組變更項目可為下列類型：[群組變更項目] 或 [未變更項目]。

群組變更項目。 顯示對話方塊，讓用戶端根據系統是否將相關聯的 DN 運算式評估為 TRUE，來變更網路群組。

未變更項目。 將列加入至表格，表示將相關聯的 DN 運算式評估為 TRUE 時，不應發生變更。這樣有助於提供變更群組清單之評估的「最少運算」。

編輯。 顯示編輯表格中目前所選項目的對話方塊。

移除。 移除目前表格中選取的項目。

6. 按一下 [儲存] 以建立動作物件。

Directory Proxy Server 組態已經修改，您必須重新啟動依賴本組態的伺服器。現在還不要重新啟動伺服器。您可以將所有的組態都變更過後再進行。

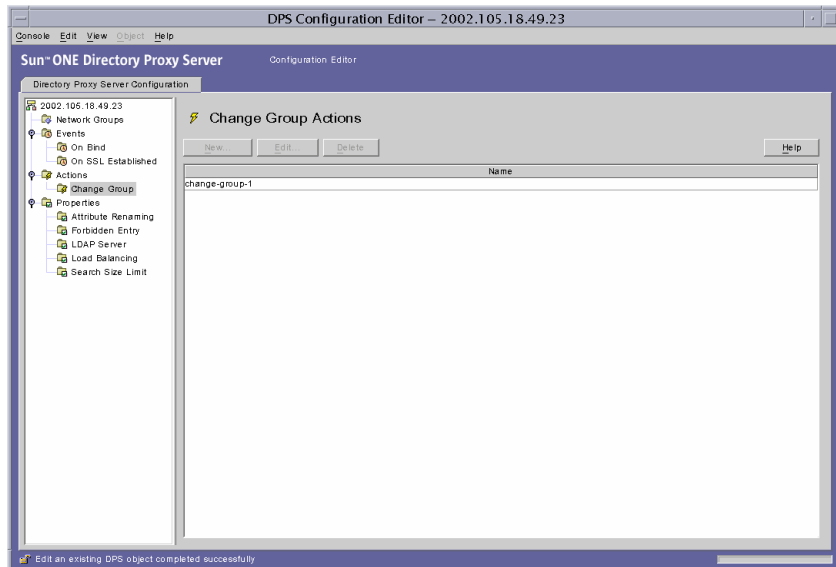
7. 重複步驟 3 至步驟 6，以建立其他物件。
8. 若要重新啟動伺服器，請參閱「重新啟動 Directory Proxy Server」(第 47 頁)。

修改動作物件

若要修改動作物件：

1. 存取 Directory Proxy Server 組態編輯器主控台；請參閱「存取 Directory Proxy Server 主控台」(第 33 頁)。
2. 在瀏覽樹狀目錄中，選取 [動作]。

右邊窗格會顯示現有的動作物件清單。



3. 在清單中選取您要修改的動作物件，然後按一下 [編輯]。
4. 進行必要的修改。

5. 按一下 [儲存] 以儲存您的變更。
Directory Proxy Server 組態已經修改，您必須重新啓動依賴本組態的伺服器。現在還不要重新啓動伺服器。您可以將所有的組態都變更過後再進行。
6. 重複步驟 3 至步驟 5，以修改其他物件。
7. 若要重新啓動伺服器，請參閱「重新啓動 Directory Proxy Server」(第 47 頁)。

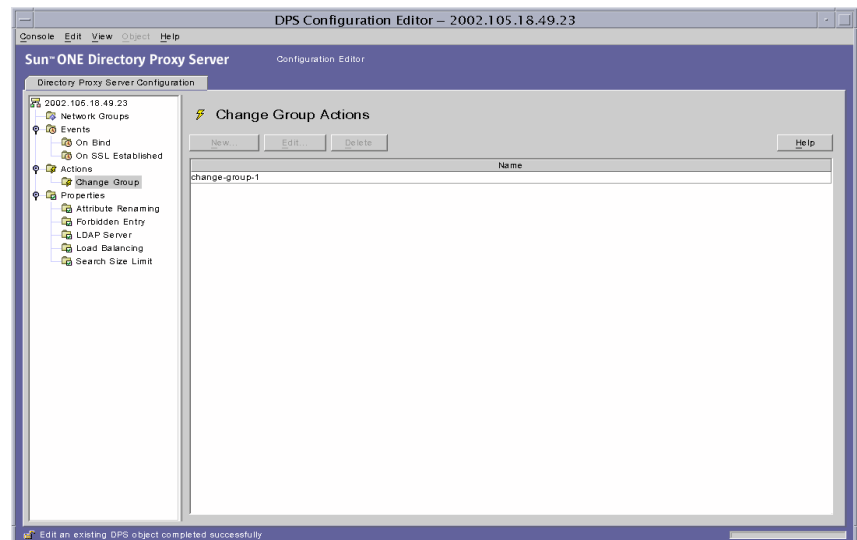
刪除動作物件

您可以從 Directory Proxy Server 組態刪除任何不要的動作物件。刪除動作物件之前，請確定任何事件物件的組態中都沒有使用這個動作物件。

若要刪除動作物件：

1. 存取 Directory Proxy Server 組態編輯器主控台；請參閱「存取 Directory Proxy Server 主控台」(第 33 頁)。
2. 在瀏覽樹狀目錄中，選取 [動作]。

右邊窗格會顯示現有的動作物件清單。



3. 在清單中選取您要刪除的動作，然後按一下 [刪除]。

4. 確認您的動作。

您刪除的物件名稱現在已經從清單上移除。Directory Proxy Server 組態已經修改，您必須重新啓動依賴本組態的伺服器。現在還不要重新啓動伺服器。您可以將所有的組態都變更過後再進行。

5. 重複步驟 3 及步驟 4，以刪除其他物件。

6. 若要重新啓動伺服器，請參閱「重新啓動 Directory Proxy Server」(第 47 頁)。

設定及監視記錄

本章說明如何設定讓 Sun ONE Directory Proxy Server 記錄項目或訊息，然後利用 Directory Proxy Server [伺服器主控台]，藉由記錄的項目監視其活動。

本章包含下列各節：

- 記錄概論 (第 127 頁)
- 設定記錄 (第 130 頁)
- 從 Directory Proxy Server 伺服器主控台監視記錄 (第 135 頁)

記錄概論

Directory Proxy Server 可維護兩個類型的記錄：

- 系統記錄
- 稽核記錄

下列幾節會詳細說明這兩個類型。

系統記錄

Directory Proxy Server 可維護各種不同事件及系統錯誤的延伸記錄，讓您能監視及偵錯系統。所有記錄都可以文字檔來維護，並儲存在本機檔案系統，讓您便於迅速及便捷的檢索。根據預設值，Directory Proxy Server 會將記錄項目寫入該檔案：

```
<server-root>/dps-<hostname>/logs/fwd.log
```

記錄檔中的每個訊息都有時間戳記。還有 Directory Proxy Server 內部的程序號碼及訊息號碼。

Directory Proxy Server 記錄的事件會分成各個類別，以便識別及篩選。這些都列在表 10-1。每個類別都代表特性相同或類似的訊息，或屬於特定功能區。根據組態的設定，記錄檔可記錄屬於這些類別之一（或以上）的項目。

在 Directory Proxy Server 組態中，每個訊息類別都對應到特定的記錄層級。記錄層級指出伺服器執行的記錄層級 - 也就是說記錄的詳細程度。

- 較高的優先權層級表示詳細資料較少，因為只記錄優先權高的事件。
- 較低的優先權層級表示詳細資料較多，因為記錄檔中記錄較多種類的事件。

表 10-1 會以優先權的遞減排序列出訊息類別 - [關鍵] 的優先權層級最高，[詳細追蹤] 的優先權層級最低。

表 10-1 記錄層級

記錄層級或嚴重性	描述
強制	強制訊息是一定會寫入到記錄的訊息。這些訊息指出 Directory Proxy Server 讀取的組態、Directory Proxy Server 啟動時的版本號碼等等。 您不能設定屬於這個層級的訊息。
關鍵	這些訊息指出 Directory Proxy Server 遇到需要立即注意的某些問題。例如， <i>Directory Proxy Server process 1234 has exited, attempting restart in 10 seconds</i> 。
例外	這些訊息指出未預期的錯誤狀況，例如，Directory Proxy Server 已接收來自用戶端 / 伺服器的格式化錯誤的 LDAP 訊息。例如， <i>Could not decode search request</i> 。
警告	這些訊息可指定 Directory Proxy Server 可忽略的錯誤狀況，但系統管理員必須加以調查。例如， <i>Local host name lookup failed.System default group may not function correctly</i> 。
通知	這些是參考訊息。例如， <i>Received NULL continuation reference from server.Discarding..</i> 。
追蹤	這些是偵錯訊息。例如， <i>Result received from server lderr =32, matched=o=sun.com, errtxt=no such object</i> 。追蹤訊息包含通訊協定傾印。使用追蹤層級會迅速產生非常大的記錄檔。
詳細追蹤	這些訊息可提供較為詳細的偵錯資訊，例如可重新使用連線的要求匿名連結。這些訊息通常對於 Directory Proxy Server 工程 / 支援小組都是有意義的。

Directory Proxy Server 可讓您指定記錄的數量 - 您可利用記錄層級，根據事件的嚴重性篩選記錄項目。根據預設值，層級會設定為 [警告]。

注意： 記錄層級是累加的，也就是說，如果您選擇 [警告] 作為記錄層級，則會記錄 [警告]、[例外] 及 [關鍵] 層級訊息。記錄資料可能非常龐大，尤其是以較低 (較詳細) 的記錄層級執行時更是如此。請確定主機有足夠的磁碟空間以供所有記錄檔使用。

在 Windows NT 以外的平台上，您可選擇將 Directory Proxy Server 設定成將記錄訊息傳送給 `syslog` 常駐程式，而不是檔案；不可將記錄訊息同時傳送給檔案及 `syslog` 常駐程式。如果您選擇此組態，請確定 `syslogd` 設定正確。例如，如果要將所有的訊息都寫入到特定的 `/var/adm/messages` 檔，就必須將下列這一行加入 `/etc/syslog.conf` 檔：

```
daemon.crit;daemon.warning;daemon.info;daemon.debug
/var/adm/messages
```

請注意，Directory Proxy Server 使用 `daemon facility` 語法，優先權或記錄層級為關鍵、警告、資訊、及偵錯。表 10-1 顯示 `syslog` 事件及 Directory Proxy Server 事件的對應。

表 10-2 記錄層級的對應

Directory Proxy Server 事件	syslog 事件
強制	資訊
關鍵	關鍵
例外	錯誤
警告	警告
通知	資訊
追蹤	資訊
詳細追蹤	資訊

若要旋轉 Directory Proxy Server 記錄並控制其他的記錄功能，請使用下列物件類別：

```
ids-proxy-sch-LogProperty
```

有關本物件類別及其使用方式的詳細資訊，請參閱「dpsconfig2ldif」（第 169 頁）。

稽核記錄

除了記錄系統及錯誤訊息之外，Directory Proxy Server 也可維護所有事件及連線統計資料的稽核蹤跡 - 例如，可以記錄剛剛完成與 LDAP 目錄之連結 / 解除連結的用戶端 DN。

根據預設值，Directory Proxy Server 不會設定為記錄稽核訊息。您隨時可以啓用此功能。您也可以指定是否要將稽核訊息記錄到系統記錄項目寫入的同一個檔案，或是記錄到其他的檔案。除非已經設定成寫入到不同的檔案，否則系統會將稽核訊息（以及其他記錄訊息）記錄到系統記錄項目寫入的同一個檔案；詳細資訊請參閱「系統記錄」（第 127 頁）。

注意： 稽核記錄可讓您偵測任何未經授權的存取行為或活動。建議您啓用此功能。另外爲了安全起見，您應該定期檢查 Directory Proxy Server 稽核記錄，看看是否有不尋常的活動。

設定記錄

若要設定讓 Directory Proxy Server 記錄項目，請依照這些步驟：

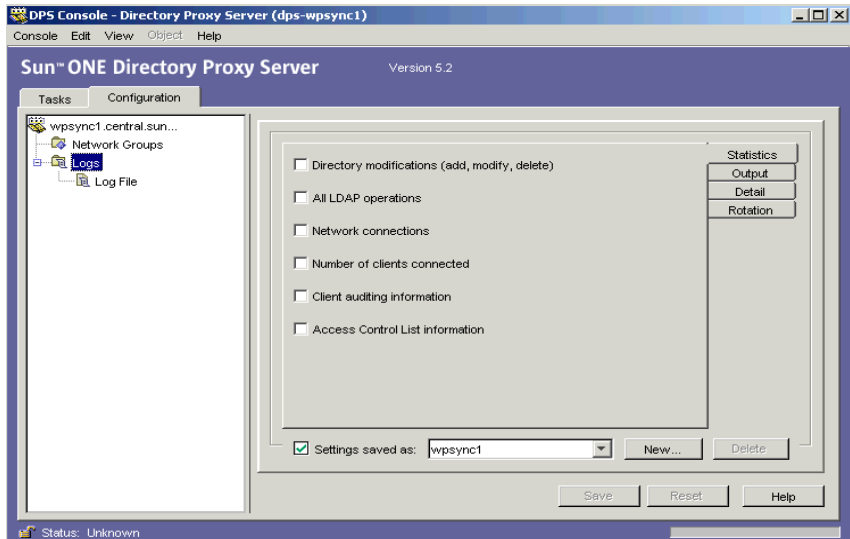
- 步驟 1. 定義記錄設定值
- 步驟 2. 指定要使用的記錄內容

步驟 1. 定義記錄設定值

只有在您要建立或定義 [記錄內容] 的物件時，才需要此步驟。如果您已經建立 [記錄內容] 物件，並且想使用其中之一，請跳到下個步驟。

1. 存取 Directory Proxy Server 主控台；請參閱「存取 Directory Proxy Server 主控台」（第 33 頁）。

2. 選取 [組態] 標籤，然後在瀏覽樹狀目錄中展開 [記錄]。
右邊窗格會在右邊顯示現有的記錄內容物件。



3. 按一下 [新增] 定義新物件。
現在可以使用 [記錄內容] 視窗的 [統計資料] 標籤。
4. 在 [名稱] 欄位中，鍵入物件的名稱。名稱必須是唯一的英數字元字串。
5. 在 [統計資料] 標籤中指定要記錄的資訊種類。

根據您要記錄的訊息類型，來核取方塊。預設不會選取任何選項。記錄訊息可分類為下列群組：目錄修改、所有 LDAP 操作、網路連線、連線的用戶端數量以及用戶端稽核資訊。

目錄修改。系統將記錄寫入至目錄的作業統計，例如添加、修改以及刪除。

所有 LDAP 操作。系統會記錄所有 LDAP 操作的統計資料。

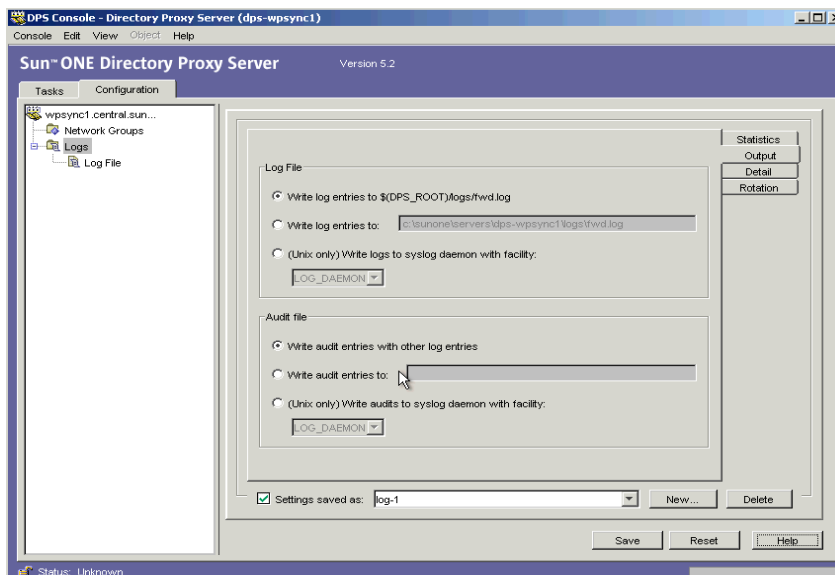
網路連線。系統將記錄關於網路連線的統計。

連線的用戶端數量。系統會記錄一般統計資料，例如有多少用戶端連線。

用戶端稽核資訊。會記錄稽核資訊，例如剛剛完成連結 / 解除連結之用戶端的 DN。

存取控制清單資訊。這包含對記錄資訊擁有存取權限之使用者的清單。

6. 選取 [輸出] 標籤，並指定要將記錄項目傳送到哪裡，以及是否要記錄稽核軌跡。



記錄檔。顯示控制 Directory Proxy Server 寫入其記錄項目位置的選項。

將記錄項目寫入至 `$(dps_ROOT)/logs/fwd.log`。這是 Directory Proxy Server 將其記錄項目寫入檔案 `$(dps_ROOT)/logs/fwd.log` 的預設設定值，其中 `$(dps_ROOT)` 是安裝 Directory Proxy Server 伺服器根目錄下目錄的位置，通常是 `/usr/sunone/servers/dps-<hostname>` 或 `\Program\Files\sunone\Servers\dps-<hostname>`。

將記錄項目寫入到。指定替代檔案，使 Directory Proxy Server 將其記錄項目導向至其中。無論是何種平台，檔案分隔符號都應該遵循 UNIX 慣例。

將記錄寫入利用 **facility** 語法的 **syslog** 常駐程式。(僅限 UNIX) 選擇 Directory Proxy Server 會用來記錄項目的 syslog facility 程式碼。只有安裝在 UNIX 機器上的 Directory Proxy Server 伺服器使用此記錄內容時，才應該選取此設定。為安裝在 Windows NT 系統上的 Directory Proxy Server 指定此選項，將使其無法操作。建議您如果要指定此屬性的值，可以為 Windows NT 和 UNIX 建立獨立的記錄內容。

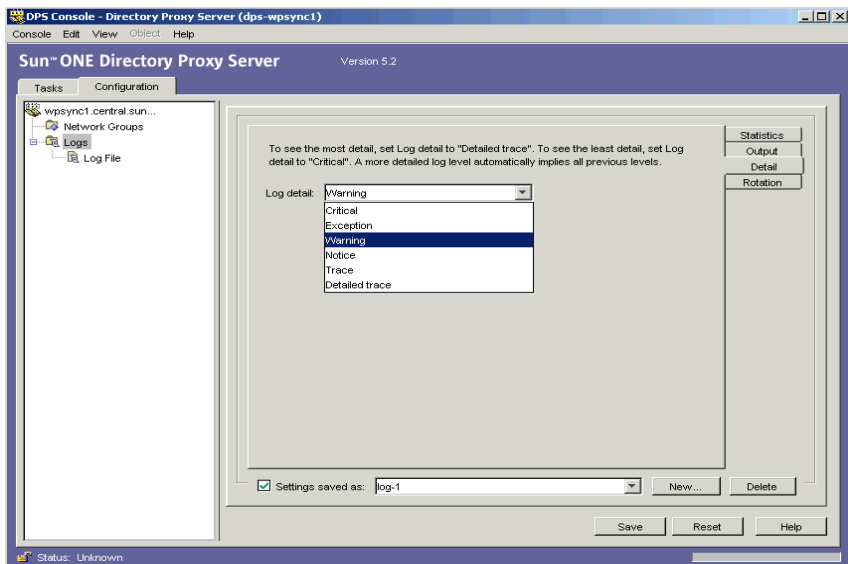
稽核檔案。顯示控制 Directory Proxy Server 寫入其稽核記錄項目位置的選項。若要讓此功能運作，則必須選取 [統計資料] 標籤的 [用戶端稽核資訊] 選項，以啟用稽核記錄。

透過其他記錄項目寫入稽核項目。這是預設的設定，其中的 Directory Proxy Server 會將其稽核記錄項目寫入至上方記錄檔設定值中所指定的相同輸出。

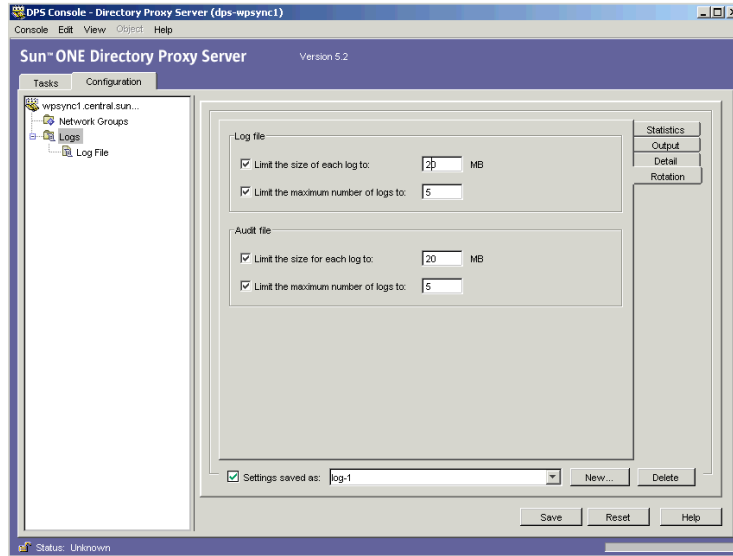
將記錄項目寫入到。指定替代檔案，使 Directory Proxy Server 將其稽核記錄項目導向至其中。無論是何種平台，檔案分隔符號都必須遵循 UNIX 慣例。

將稽核寫入利用 facility 語法的 syslog 常駐程式。(僅限 UNIX) 選擇 Directory Proxy Server 會用來記錄稽核項目的 syslog facility 程式碼。只有 Directory Proxy Server 伺服器主控的 UNIX 機器使用此記錄內容時，才應該選取此設定。指定此選項將導致 Windows NT 架構的 Directory Proxy Server 無法運作。建議您如果要指定此屬性的值，可以為 Windows NT 和 UNIX 建立獨立的記錄內容物件。

7. 選取 [詳細資料] 標籤，並指定記錄層級 - 記錄想要的詳細資料數量。
在下拉式功能表中選擇記錄層級。



8. 選取 [旋轉] 標籤來控制調整及旋轉記錄的方式。



記錄檔。顯示限制 Directory Proxy Server 記錄檔之大小與數量上限的選項。

將每個記錄的大小限制為。輸入每個記錄檔的大小上限 (以 MB 計)。

將記錄的最大數量限制為。輸入要建立及旋轉的記錄檔數量上限。

稽核檔案。顯示限制 Directory Proxy Server 稽核檔之大小與數量上限的選項。

將每個記錄的大小限制為。輸入每個記錄檔的大小上限 (以 MB 計)。

將記錄的最大數量限制為。輸入要建立及旋轉的記錄檔數量上限。

9. 按一下 [儲存] 以儲存您的變更。

現在清單中出現物件的名稱。已經修改 Directory Proxy Server 組態，並提示您重新啟動伺服器。

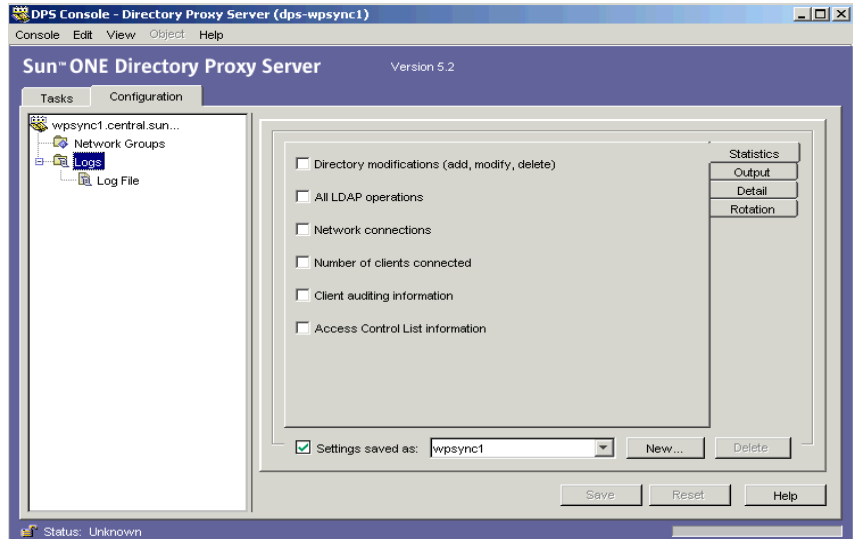
10. 若要重新啟動伺服器，請參閱「重新啟動 Directory Proxy Server」(第 47 頁)。

步驟 2. 指定要使用的記錄內容

在此步驟中，您要選取用來記錄訊息的現有記錄內容。

1. 存取 Directory Proxy Server [伺服器主控台]；請參閱「存取 Directory Proxy Server 主控台」(第 33 頁)。

2. 選取 [組態] 標籤，然後在瀏覽樹狀目錄中選取 [記錄]。
右邊窗格會顯示目前系統內容指定的記錄內容相關資訊。



3. 在「設定儲存為」下拉式清單中，選取您要使用的內容。
4. 按一下 [儲存] 以儲存您的變更。

Directory Proxy Server 現在已經設定成根據組態中的定義來記錄訊息。已經修改 Directory Proxy Server 組態，並提示您重新啓動伺服器。

5. 選取 [工作] 標籤，並重新啓動伺服器，請參閱「重新啓動 Directory Proxy Server」(第 47 頁)。

從 Directory Proxy Server 伺服器主控台監視記錄

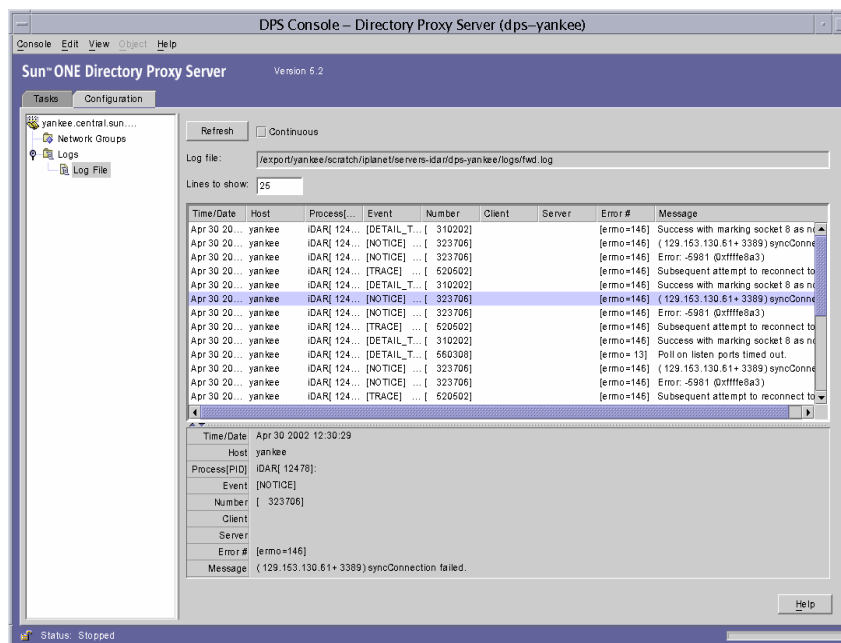
一旦您設定讓 Directory Proxy Server 記錄訊息 (請參閱「設定記錄」(第 130 頁))，您就可以檢視記錄訊息，以監視其活動。例如，當您碰到 Directory Proxy Server 的問題，需要疑難排解時，檢查伺服器記錄的錯誤或資訊訊息就可能有用。另外，檢查記錄檔就可以監視 Directory Proxy Server 作業的許多層面。

爲了達成此目的，Directory Proxy Server [伺服器主控台] 提供了簡單的機制，可以檢視記錄檔的內容。您選擇檢視的記錄檔內容會以表格的形式顯示。表格分割爲幾個部份：頂端窗格顯示表格式的記錄，而底端窗格顯示目前選取之記錄的明細。每個記錄包含記錄該訊息時的日期與時間、訊息的嚴重性及記錄的一般描述等資訊。

一旦您開啓記錄檔來檢視，就可以指定要顯示的記錄或項目數量，以讀取部分內容。以下說明如何檢視檔案中的記錄：

1. 存取 Directory Proxy Server [伺服器主控台]；請參閱「存取 Directory Proxy Server 主控台」（第 33 頁）。
2. 選取 [組態] 標籤，然後在瀏覽樹狀目錄中展開 [記錄]。
3. 選取記錄檔。

右邊窗格會顯示檔案中記錄項目的檢視選項。您可以選取目前記錄內容中指定的任何記錄檔；如果有設定，Directory Proxy Server 會有不同的記錄及稽核資訊檔案。



表單元素的描述如下：

重新整理。讀取記錄並在下表中顯示記錄。

持續。選取此設定讓此檢視以最新的記錄持續重新整理。

記錄檔。顯示目前檢視的檔案名稱。

顯示行數。指定要從記錄檔讀取的行數上限。

從 Directory Proxy Server 伺服器注冊監視記錄

Sun ONE Directory Proxy Server 支援 SSL/TLS，以便讓用戶端及後端目錄伺服器之間使用安全通訊，將於下列各節中說明：

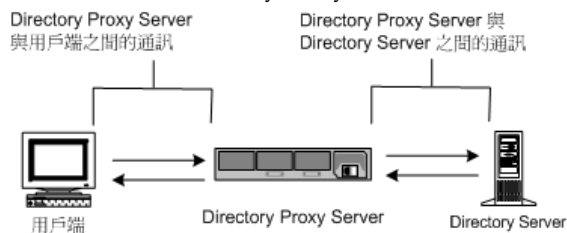
- 準備設定 SSL 及 TLS
- 設定 SSL 通訊

本節的某些資訊是假設您已經熟悉公鑰密碼學及 Secure Sockets Layer (SSL) 通訊協定的基本概念，並了解 Intranet、Extranet、網際網路安全的概念，以及數位憑證在企業中的角色。如果您是第一次接觸這些概念，建議您先閱讀本手冊中與安全有關的附錄：用 Sun ONE Console 管理伺服器。

如果您是從 iDAR 5.0x 升級，在「Directory Proxy Server 安裝指南」中有遷移 SSL 組態的詳細程序。

Directory Proxy Server 有二個可分開設定的通訊連結。每個通訊連結都可以是明碼，或使用 Transport Layer Security (TLS) 或 Secure Sockets Layer (SSL) 通訊協定加密。您可以用二種不同的通訊連結，因此可以在 LDAP 用戶端及 Directory Proxy Server 之間與 Directory Proxy Server 及 LDAP 目錄之間，設定啓用 TLS 或 SSL 通訊。圖 11-1 說明 Directory Proxy Server 的這個能力。

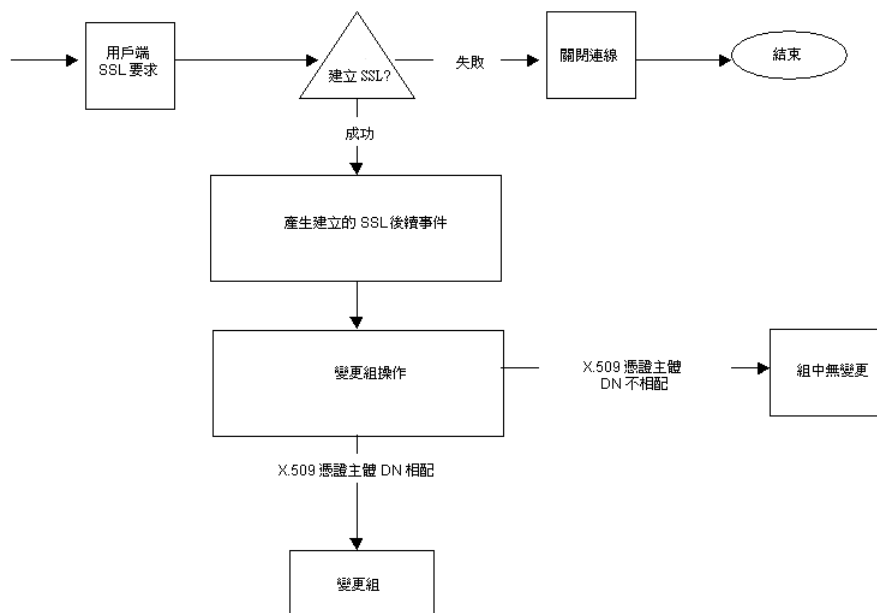
圖 11-1 Directory Proxy Server 中二種不同的通訊連結



若通過驗證的憑證其 CA 受信任根憑證已完成安裝而且可以供 Directory Proxy Server 使用，則 Directory Proxy Server 就能確認用戶端及伺服器的憑證。

圖 11-2 說明用戶端建立 SSL 工作階段後，Directory Proxy Server 如何確認用戶端傳送的憑證。

圖 11-2 用戶端以憑證為準的驗證作業



準備設定 SSL 及 TLS

您必須根據自己是使用內部安全裝置、外部硬體裝置、或兩者兼用的情形，個別設定 SSL 及 TLS。本節會告訴您如何進行。

使用內部安全裝置設定 SSL 或 TLS

若要使用內部安全裝置設定 SSL 或 TLS，您必須要求並安裝憑證。若要要求憑證，請執行 [憑證要求精靈]。若要安裝憑證，請執行 [憑證安裝精靈]。出現提示時，請指定您要將憑證安裝在內部安全裝置上。

使用外部安全裝置設定 SSL 或 TLS

若要使用外部安全裝置 (例如 FORTEZZA) 設定 SSL，首先要安裝外部設備製造商提供的 PKCS #11 模組。然後執行 [憑證要求精靈]，在出現提示時指定外部安全裝置。

使用內部及外部安全裝置設定 SSL

您的企業內某些伺服器及用戶端可能只使用內部安全裝置，其他的可能同時使用內部及外部安全裝置。如果您的伺服器必須與同時執行內部及外部安全裝置的產品進行通訊，請執行 [憑證要求精靈] 二次。在第一次使用期間出現提示時，請指定內部安全裝置。在第二次使用期間出現提示時，請指定外部安全裝置。

設定 SSL 通訊

一般來說，設定啓用 SSL 通訊的 Directory Proxy Server 包含這些步驟：

- 步驟 1. 安裝 Directory Proxy Server 的「伺服器憑證」
- 步驟 2. 設定 Directory Proxy Server 及用戶端之間的 SSL 連線
- 步驟 3. 設定 Directory Proxy Server 及 LDAP 伺服器之間的 SSL 連線

步驟 1. 安裝 Directory Proxy Server 的「伺服器憑證」

要求及安裝憑證時，您必須使用二個精靈。可使用 [憑證要求精靈] 來要求新的伺服器憑證，或更新您已經在使用的憑證。可使用 [憑證安裝精靈] 來安裝憑證授權單位 (CA) 傳送來的憑證。您第一次使用 [憑證要求精靈] 時，本程式還會為您建立並安裝金鑰及憑證資料庫。

若要安裝 Directory Proxy Server 的伺服器憑證，請依照這些步驟：

- 步驟 A. 產生伺服器憑證要求
- 步驟 B. 傳送伺服器憑證要求
- 步驟 C. 安裝憑證
- 步驟 D. 安裝憑證授權單位憑證或伺服器憑證鏈結

- 步驟 E. 備份及還原您的憑證資料庫

SSL 憑證

Sun ONE Directory Proxy Server 可安裝三種憑證：伺服器憑證、伺服器憑證鏈結、或受信任的憑證授權單位 (CA) 憑證。

*伺服器憑證*是只與您的伺服器有關聯的單一憑證。此憑證可讓用戶端識別您的伺服器。您必須向憑證授權單位 (CA) 要求這類憑證。若要取得並安裝伺服器憑證，請產生要求並傳送給憑證授權單位 (CA)。然後安裝憑證。

*伺服器憑證鏈結*是您公司內部憑證伺服器或已知的憑證授權單位為您自動產生的一組憑證。鏈結中的憑證可回溯到原始的憑證授權單位，提供身分證明。您每次取得或安裝新的伺服器憑證時，都需要此證明。

*受信任的憑證授權單位憑證*是您公司內部憑證伺服器或已知的憑證授權單位為您自動產生的單一憑證。受信任的憑證授權單位憑證的功能是驗證用戶端。

若要取得受信任的憑證授權單位 (CA) 憑證，請先連線到內部憑證伺服器或憑證授權單位網站。請複製必要的憑證資訊，然後存成檔案。然後使用 [憑證安裝精靈] 來安裝憑證。

您可以在伺服器上安裝任何數量的 SSL 憑證。設定目錄伺服器實例的 SSL 時，您至少必須安裝一個伺服器憑證及一個受信任的憑證授權單位憑證。

步驟 A. 產生伺服器憑證要求

您可利用 Sun ONE Directory Proxy Server 來產生憑證要求，然後傳送給憑證授權單位 (CA)。

1. 在 Sun ONE Directory Proxy Server 瀏覽樹狀目錄中，選取您要使用 SSL 加密的伺服器實例。
2. 在伺服器實例上連按兩下，或按一下 [開啓]，開啓伺服器實例的管理視窗。
3. 從 [主控台] 功能表選擇 [安全] > [管理憑證]。

您也可以按一下 [管理憑證] 工作。

如果安全裝置沒有密碼，系統就會提示您輸入新密碼。

4. 按一下 [要求]，開啓 [憑證要求精靈]。
5. 選擇 [手動要求憑證]，然後按一下 [下一步]。

6. 輸入所要求的資訊：

伺服器名稱。(選用) 為您要求憑證的電腦輸入完整合格主機名稱。

組織。(選用) 輸入您的組織名稱。

組織單位。(選用) 輸入您的事業部、部門、或其他組織單位。

城市 / 地區。(選用) 輸入您組織單位所在的城市或區。

州 / 省。(選用) 輸入您組織單位所在的州或省。

國家 / 地區。(選用) 在下拉式功能表中選取您組織單位所在的州或省。

您可利用下列按鈕切換要求表單的二個檢視方式。

顯示 DN。按一下以顯示辨別名稱 (DN) 格式的要求者資訊。只有當您在欄位中輸入資訊時，才看得見本按鈕。

顯示欄位。按一下以顯示欄位中的要求者資訊。只有當您在欄位中輸入 DN 格式的資訊時，才看得見本按鈕。

7. 按一下 [下一步]。

8. 輸入儲存此憑證的安全裝置密碼。

如果您正在使用內部 (軟體) 安全裝置，這個就是金鑰及憑證資料庫的密碼。如果您正在使用外部 (硬體) 模組，這個就是智慧卡或其他安全裝置的密碼。

9. 按一下 [下一步]。

10. 選取下列其中一項：

[**複製到剪貼簿**]。按一下可將您的憑證要求複製到剪貼簿。

[**儲存至檔案**]。按一下可將您的要求儲存成文字檔。系統會提示您選擇檔案的名稱與位置。

11. 按一下 [完成]，關閉 [憑證要求精靈]。

步驟 B. 傳送伺服器憑證要求

一旦您產生了伺服器憑證要求，就要傳送給憑證授權單位進行處理。許多憑證授權單位允許您透過他們的網站提交憑證。其他單位可能要求您將加入要求的電子郵件訊息傳送給他們。

1. 利用您的電子郵件程式建立新的電子郵件訊息。

2. 將您的憑證要求貼到訊息中。

如果您將憑證要求儲存到檔案中，請在文字編輯器中開啓。將要求複製並貼上到訊息本文。

如果您將憑證要求複製到剪貼簿，請貼到訊息的本文中。

3. 輸入您要求的主題及收件人。主題及收件人的類型會根據您使用的憑證授權單位而不同。如需詳細資訊，請參閱您的憑證授權單位網站。

4. 將電子郵件訊息傳送給憑證授權單位。

一旦提交要求後，就必須等憑證授權單位將您的憑證傳回來。往返時間極不固定，而且需視憑證授權單位而定。如果您公司有內部的憑證授權單位，可能只需要一、二天就可以收到您的憑證。如果您使用外部的憑證授權單位，憑證授權單位可能要花幾週才能回應您的要求。

步驟 C. 安裝憑證

依各憑證授權單位的做法，您可能會在電子郵件訊息中收到憑證，或可能必須從憑證授權單位的網站檢索。一旦您有了憑證，就可以備份並安裝。

1. 將您從憑證授權單位收到的憑證資料儲存在文字檔中。

如果您遺失憑證資料，就可以利用此備份檔重新安裝憑證。

2. 在 Sun ONE Directory Proxy Server 瀏覽樹狀目錄中，選取您要安裝憑證的伺服器實例。

3. 按一下 [開啓]，開啓伺服器實例的管理視窗。

4. 在 [工作] 標籤上按一下 [管理憑證] 工作按鈕。

您也可以開啓 [主控台] 功能表，然後選擇 [安全] > [管理憑證]。

5. 按一下 [伺服器憑證] 標籤。

6. 指定儲存此憑證的位置。

- 如果您要將此憑證儲存在內部安全裝置上，請從 [安全裝置] 下拉式清單中選取內部 (軟體)，然後按一下 [安裝]。

- 如果您要將此憑證儲存在外部硬體裝置上，請從 [安全裝置] 下拉式清單中選取裝置，然後按一下 [安裝]。

7. 輸入憑證的位置或文字。
在本機檔案中。如果憑證儲存在您系統上的文字檔中，請輸入該檔案的完整路徑。
在下列編碼的文字區塊中。如果您將憑證複製到剪貼簿，請從剪貼簿按一下 [貼上] 按鈕，將憑證文字貼到文字欄位中。
8. 按一下 [下一步]。
 如果您在上一步輸入的憑證資訊有效，就會看到包含憑證細節的頁面。
9. 請確認憑證資訊正確，然後按一下 [下一步]。
10. 輸入憑證名稱，然後按一下 [下一步]。
11. 輸入儲存此憑證的安全裝置的密碼。
 如果您將憑證安裝到內部 (軟體) 安全裝置上，請輸入金鑰及憑證資料庫的密碼。如果您將憑證安裝到外部 (硬體) 安全裝置上，請輸入該裝置的密碼。
12. 按一下 [完成]。

步驟 D. 安裝憑證授權單位憑證或伺服器憑證鏈結

1. 從您的憑證授權單位取得憑證授權單位憑證或伺服器憑證。
2. 在 Sun ONE Directory Proxy Server 瀏覽樹狀目錄中，選取您要安裝憑證授權單位憑證的伺服器實例。
3. 按一下 [開啓]，開啓伺服器實例的管理視窗。
4. 在 [工作] 標籤上按一下 [管理憑證] 工作按鈕。
 您也可以開啓 [主控台] 功能表，然後選擇 [安全] > [管理憑證]。
5. 選取 [憑證授權單位憑證] 標籤，然後按一下 [安裝]。
6. 輸入憑證的位置或文字：
在本機檔案中。如果憑證儲存在您系統上的文字檔中，請輸入該檔案的完整路徑。
在下列編碼的文字區塊中。如果要將憑證複製到剪貼簿，請從剪貼簿按一下 [貼上] 按鈕，將憑證文字貼到文字欄位中。
7. 按一下 [下一步]。
 如果在上一步輸入的憑證資訊有效，就會看到包含憑證細節的頁面。
8. 請確認憑證資訊正確，然後按一下 [下一步]。

9. 輸入憑證名稱，然後按一下 [下一步]。
10. 請選取此憑證的信任選項：
 - 從用戶端接收連線。**如果您要信任此憑證授權單位發出的用戶端憑證，請核取此方塊。
 - 連線到其他伺服器。**如果您要信任此憑證授權單位發出的伺服器憑證，請核取此方塊。
11. 按一下 [完成]。

步驟 E. 備份及還原您的憑證資料庫

每次安裝憑證時，您應該備份憑證資料庫。如果您的資料庫毀損，就可以從本備份還原憑證資訊。

備份您的憑證資料庫

1. 開啓您的伺服器根資料夾。
2. 將 `alias` 資料夾中的所有檔案複製到另一個位置（最好是在其他的磁碟上）。
本資料夾包含信任資料庫的憑證以及私密金鑰。

從備份還原您的憑證資料庫

- 將您的備份檔複製到伺服器根資料夾的 `alias` 子資料夾。

小心 如果從備份還原憑證資料庫，您會失去備份後所安裝的所有憑證。在還原您的憑證資料庫之前，請確定您有所有憑證的副本，以免需要重新安裝。

步驟 2. 設定 Directory Proxy Server 及用戶端之間的 SSL 連線

若要設定 Directory Proxy Server 及 LDAP 用戶端之間的 SSL 連線，請依照這些步驟：

- 步驟 A. 將 Directory Proxy Server 憑證授權單位憑證添加到用戶端的信任資料庫
- 步驟 B. 變更 Directory Proxy Server 系統組態
- 步驟 C. 變更 Directory Proxy Server 的網路群組

步驟 A. 將 Directory Proxy Server 憑證授權單位憑證添加到用戶端的信任資料庫

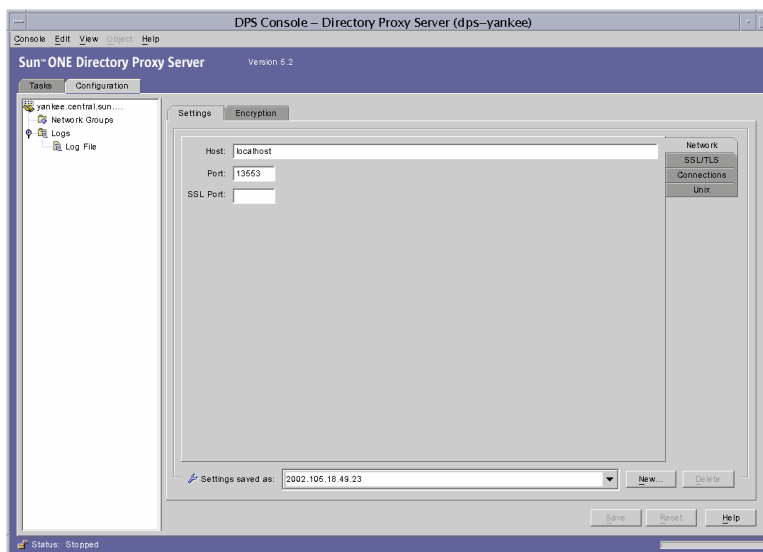
注意 只有在用戶端確認伺服器憑證時，才需要此步驟。所有的 Netscape 及 Sun 用戶端都會確認。然而，有的用戶端不會確認。在這個情況下就不需要設定信任關係。

當 Directory Proxy Server 提供自己的憑證給 LDAP 用戶端時，用戶端會嘗試確認此憑證是否有效。作為確認程序的一部分，用戶端要檢查送出憑證的憑證授權單位，是否受到用戶端信任。因此，送出 Directory Proxy Server 伺服器憑證的憑證授權單位之根憑證，必須安裝在用戶端的信任資料庫中。

安裝 Directory Proxy Server 伺服器憑證的最後一個步驟時，您要將 Directory Proxy Server 憑證授權單位憑證複製到文字檔。根據每個用戶端應用程式的說明文件，並將憑證授權單位憑證安裝到自己的信任資料庫中。

步驟 B. 變更 Directory Proxy Server 系統組態

Directory Proxy Server [主控台] 視窗中的 [設定] 及 [加密] 標籤，可以讓您為 Directory Proxy Server 定義啟用 SSL 通訊的標準。如需詳細資訊，請參閱「建立系統組態實例」（第 53 頁）。



變更適當系統組態實例的下列項目，並儲存您的變更。

- 在 [設定] 標籤中指定 [SSL 連接埠] 欄位的值。Directory Proxy Server 會監聽您指定連接埠號碼上的 LDAP (LDAP over SSL) 連線。根據預設值，Directory Proxy Server 不會監聽來自 LDAP 用戶端的連線。必須提供這個值，才能讓使用其他連接埠 636 方法建立 TLS/SSL 的用戶端啟用 LDAPS 連線。該值不能與 [連接埠] 欄位的值相同。(此選項也需要 TLS/SSL 組態，該組態位於 [加密] 標籤。)

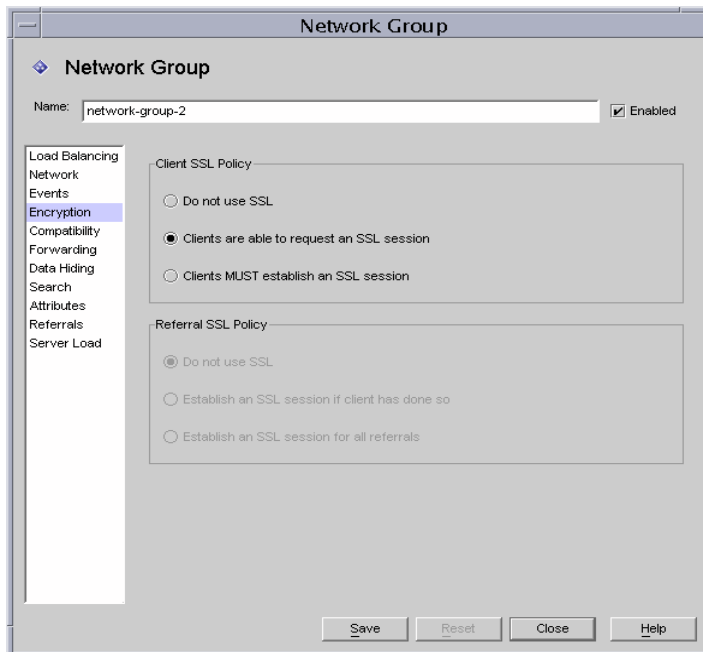
如果您需要參數的描述，請按一下 [說明] 按鈕。

- 在 [SSL/TLS 加密] 標籤中指定所有必要的資訊。

如果您需要參數的描述，請按一下 [說明] 按鈕。

步驟 C. 變更 Directory Proxy Server 的網路群組

Directory Proxy Server 利用網路群組來識別用戶端，並判定他們對 LDAP 目錄包含資訊的存取權限；如需詳細資訊，請參閱第 6 章「建立及管理群組」。



在您設定的每個群組中，要在 [加密] 標籤中設定適當的選項，以指出您是否要強迫用戶端在傳送任何 LDAP 操作前啟動 TLS 工作階段、讓用戶端自行決定、或禁止用戶端啟動 TLS 工作階段。例如，您可能想啟用 [SSL 可用] 及 [用戶端必須建立 SSL 工作階段] 選項。如需 [加密] 標籤中所顯示選項的詳細資訊，請參閱第 6 章「建立及管理群組」第 72 頁的步驟 9。

如果啟用跟隨轉介，您就應該檢查 [轉介 SSL 原則]。請在左邊視窗的清單中選取 [轉介]，以啟用跟隨轉介。

Directory Proxy Server 可跟隨由後端伺服器傳回的轉介。所傳回的 LDAP URL 必須依照 RFC 2255 格式。如果沒有指定主機連接埠，用戶端就必須了解要聯絡的適當 LDAP 伺服器。

Directory Proxy Server 會把沒有主機或連接埠號碼的 LDAP URL，轉譯成發出此轉介的相同主機之轉介。例如：

ldap:///dc=central,dc=sun,dc=com	相同主機、連接埠的轉介，但基底不同。
ldap://:10389/	相同主機的轉介，但連接埠不同。
ldap://host/	主機「主機」的轉介，在預設的連接埠 389 上。

步驟 3. 設定 Directory Proxy Server 與 LDAP 伺服器之間的 SSL 連線

若要設定 Directory Proxy Server 及 LDAP 伺服器之間的 SSL 連線，請依照這些步驟：

- 步驟 A. 安裝憑證授權單位憑證或伺服器憑證鏈結
- 步驟 B. 將 Directory Proxy Server 憑證授權單位憑證添加到 LDAP 伺服器的信任資料庫
- 步驟 C. 變更 LDAP 伺服器內容

步驟 A. 安裝憑證授權單位憑證或伺服器憑證鏈結

如果您要 Directory Proxy Server 確認 LDAP 伺服器傳送的憑證，則需要此步驟。如需詳細資訊，請參閱「步驟 D. 安裝憑證授權單位憑證或伺服器憑證鏈結」（第 143 頁）。

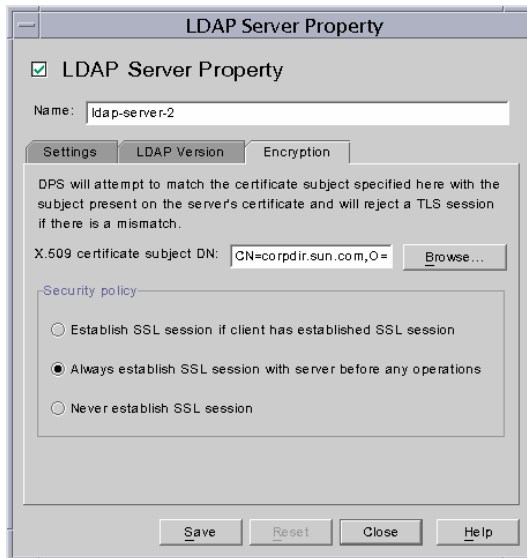
步驟 B. 將 Directory Proxy Server 憑證授權單位憑證添加到 LDAP 伺服器的信任資料庫

當 Directory Proxy Server 提供自己的憑證給 LDAP 伺服器時，伺服器會嘗試確認此憑證的有效性。作為確認程序的一部分，伺服器要檢查送出 Directory Proxy Server 憑證的憑證授權單位，是否受到伺服器信任。因此，送出 Directory Proxy Server 伺服器憑證的憑證授權單位之根憑證，必須安裝在 LDAP 伺服器的信任資料庫中。

安裝 Directory Proxy Server 伺服器憑證的最後一個步驟時，您要將 Directory Proxy Server 憑證授權單位憑證複製到文字檔。根據每個 LDAP 伺服器的說明文件，並將憑證授權單位憑證安裝到自己的信任資料庫中。如果您正在使用 Sun ONE Directory Server，可使用 [管理憑證精靈] (可從 Directory Server Console 的 [工作] 標籤啟動)，將憑證授權單位憑證新增到目錄伺服器的信任資料庫中。

步驟 C. 變更 LDAP 伺服器內容

[LDAP 伺服器內容] 視窗中的 [加密] 標籤，可以讓您為每個 LDAP 伺服器定義啓用 SSL 通訊的標準。如需詳細資訊，請參閱「建立 LDAP 伺服器內容物件」(第 99 頁)。



變更適當 LDAP 伺服器內容物件的下列項目，並儲存您的變更。

- 將 [安全原則] 選項設定成適當值，讓 Directory Proxy Server 永遠與後端伺服器建立 SSL/TLS，永不與後端伺服器建立 TLS/SSL，或只有在用戶端與 Directory Proxy Server 建立 SSL/TLS 時，才與後端伺服器建立 SSL/TLS。
- 將 [X.509 憑證主體 DN] 欄位設定成 LDAP 伺服器的憑證主體名稱 (X.509 憑證中的主體屬性)。如已指定，則 Directory Proxy Server 就會嘗試比對憑證主體與 LDAP 伺服器憑證上出現的主體，且會在出現不相符時拒絕 TLS 工作階段 (此屬性允許 Directory Proxy Server 驗證連線的 LDAP 伺服器。如果沒有設定此屬性，Directory Proxy Server 就會接受任何名稱)。

附錄

附錄 A 「Directory Proxy Server 決策功能」

附錄 B 「Directory Proxy Server 常見問答集、功能及疑難排解」

附錄 C 「Directory Proxy Server 啟動組態檔」

附錄 D 「指令轉介」

Directory Proxy Server 決策功能

本附錄說明 Directory Proxy Server 中，某些特定功能的控制流程。包括：

- 連線時建立群組 (第 153 頁)
- 繫結時變更群組 (第 153 頁)
- 建立 TLS 時變更群組 (第 155 頁)
- 高可用性安裝 (第 156 頁)
- 跟隨轉介 (第 157 頁)

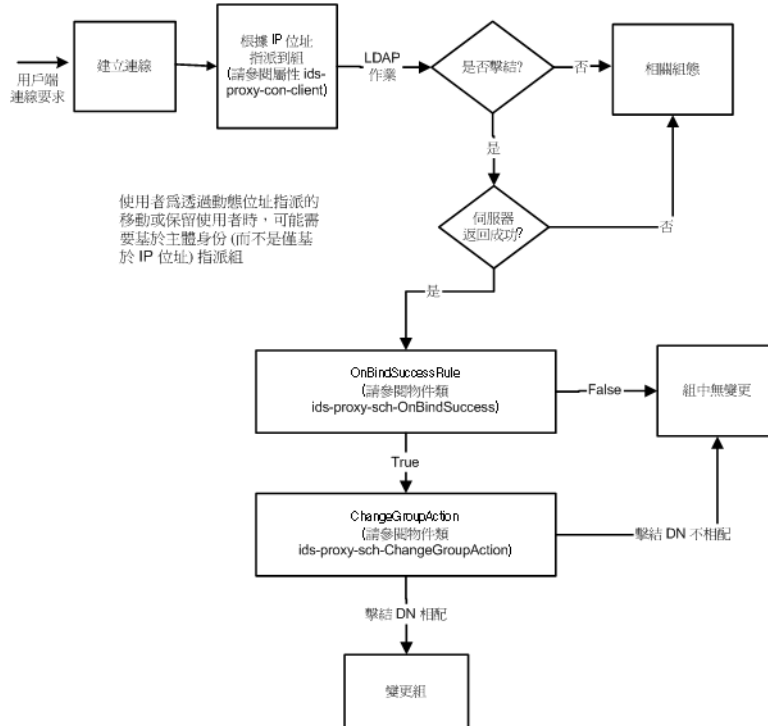
連線時建立群組

用戶端連線到 Directory Proxy Server 時，會檢查 `ids-proxy-sch-NetworkGroup` 物件項目中的 `ids-proxy-con-Client` 屬性，直到找到相符項目為止。系統會嘗試 `ids-proxy-con-priority` 屬性的定義中，`ids-proxy-sch-NetworkGroup` 物件最高到最低的優先權。Directory Proxy Server 會將用戶端放在 `ids-proxy-con-client` 屬性符合此用戶端 IP 位址的第一個群組。如果沒有符合的群組，就會關閉連線。

連結時變更群組

用戶端開始連線時，會根據其 IP 位址放在某個群組中。用戶端與目錄建立連結時，便可根據不同的存取控制措施，移動到不同的群組。為了達成這個目的，初始的群組物件必須包含規則物件，在順利完成連結作業時加以評估。如果規則評估為 `TRUE`，便會採取變更群組動作，將用戶端移動到其他群組。圖 11-3 能說明此功能。

圖 11-3 連結時變更群組



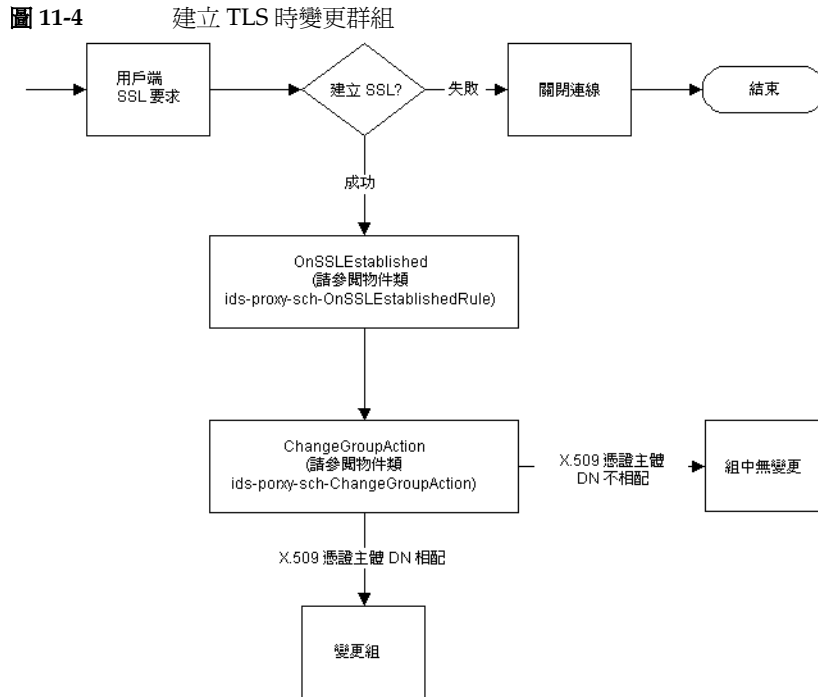
設定連結時變更群組

下列步驟說明如何設定 Directory Proxy Server，以便在使用簡單連結驗證機制時，在 cn=Directory Manager 連結成功後變更群組。

1. 建立新的 [網路群組]，讓連結成功後的 user cn=Directory Manager 移動過去。如需詳細資訊，請參閱「建立群組」(第 66 頁)。如果只能用手動變更的方式才能讓某個使用者成為此群組的一部份，請在 [網路群組] 面板的 [網路] 標籤中設定 [無 IP 連結]。也請確定此群組在允許某些 IP 連結的其他 [網路群組] 之後。
2. 建立新 [變更群組] 動作。如需詳細資訊，請參閱「建立動作物件」(第 122 頁)。將變更至設定成您在步驟 1 建立的群組名稱。將 if DN matches 設定成 cn=Directory Manager。您也可以將其他的所有項目設定成 NONE (不要變更群組)，也就是 *。
3. 建立連結後續事件。如需詳細資訊，請參閱「建立 OnBindSuccess 事件物件」(第 114 頁)。在 [動作] 標籤上設定成您在步驟 2 建立的 [變更群組] 動作。在 [條件] 標籤選取 [密碼型連結]。
4. 在步驟 1 建立的 [網路群組] 中之事件標籤上，選取您在步驟 3 建立的 [連結後續事件]。如需詳細資訊，請參閱「修改群組」(第 88 頁)。

建立 TLS 時變更群組

建立 TLS 時變更群組與建立連結機制時變更群組類似，用戶端可以在順利建立 TLS 工作階段時變更群組。用戶端建立 TLS 時，系統會評估 [已建立的 SSL] 規則，隨後就會有 [變更群組] 動作。圖 11-4 說明此功能。



高可用性部署

如果您已經設定一個以上的後端目錄伺服器，便可安裝 Directory Proxy Server 讓這些伺服器負載平衡，而且如果其中一個後端伺服器故障，就可以容錯移轉至另一個。為了達成這個目的，您必須建立 [負載平衡內容] (請參閱「負載平衡內容」(第 104 頁))，並將您要負載平衡的伺服器包含到群組物件中。您也必須建立 [LDAP 伺服器內容] (請參閱「LDAP 伺服器內容」(第 99 頁)) 對每個後端伺服器的說明，並包含到 [負載平衡內容] 中。您必須在 [負載平衡內容] 物件中，指定每個後端伺服器所佔的總負載百分比。有了這個設定，如果其中一個後端目錄伺服器故障，Directory Proxy Server 就會重新分配負載。系統會在伺服器故障時，將用戶端從第一個伺服器容錯移轉至另一個。Directory Proxy Server 也會在自己與 LDAP 伺服器之間的網路連線斷掉或 LDAP 伺服器未回應時進行容錯移轉。

注意： Directory Proxy Server 在利用 SASL 機制連結用戶端時，無法進行容錯移轉。

跟隨轉介

LDAPv2 用戶端無法自行跟隨轉介時，可以設定讓 Directory Proxy Server 代為跟隨轉介。您的後端 LDAP 目錄伺服器必須能傳送轉介，也就是說，必須支援 LDAP v3 標準。設定讓 Directory Proxy Server 與後端 LDAP 伺服器使用 LDAP v3，才能讓 Directory Proxy Server 從目錄伺服器接收轉介。然後設定您的群組轉介及接續轉介原則。

Directory Proxy Server 常見問答集、 功能及疑難排解

本附錄包含 Sun ONE Directory Proxy Server 的有用資訊。此文件包含常見問題的解答 (FAQ)、Directory Proxy Server 特定功能的說明以及疑難排解資訊。

本附錄包含下列各節：

- Directory Proxy Server 常見問答集 (第 159 頁)
- Directory Proxy Server 功能 (第 160 頁)
- 疑難排解 (第 162 頁)

Directory Proxy Server 常見問答集

Directory Proxy Server 是什麼？

Directory Proxy Server 是一個為 LDAP 用戶端及 LDAP 伺服器設計的 LDAP 代理伺服器。系統會根據 Directory Proxy Server 組態中定義的規則，將 LDAP 用戶端的要求轉送至 LDAP 伺服器。伺服器傳來的結果會回傳給用戶端，也是根據組態中定義的規則。此程序對用戶端而言完全透明，他們連線到 Directory Proxy Server 的方式與連線到 LDAP 伺服器一樣。

我為什麼需要 LDAP 代理伺服器？

許多企業想要讓外界能看到他們部分的目錄資訊，但是又要保持內部其他部分的私密性。有了 Directory Proxy Server，您就可以輕易達成這個目標，而且不用將目錄的密碼指派給外部的用戶端。Directory Proxy Server 也可以當做企業目錄服務的高可用性解決方案，並有負載平衡及容錯移轉功能。

另外也提供了額外的安全功能，譬如防護阻絕服務的攻擊與搜尋限制。

Directory Proxy Server 支援哪個版本的 LDAP 通訊協定？

Directory Proxy Server 支援使用 LDAPv2 或 LDAPv3 通訊協定的 LDAP 用戶端或鏈結 LDAP 伺服器。

Directory Proxy Server 支援安全驗證及加密嗎？

Directory Proxy Server 支援使用憑證以公鑰形式資料加密的 SSLv3 服務。LDAP 用戶端可用的安全驗證及加密機制，可以使用安全 LDAP 連接埠或 Internet Transport Layer Security (TLS) 模式，這種模式使用 Diffie-Hellman、Digital Signature Standard (DSA)、及 Triple-DES 加密演算法。

Directory Proxy Server 能與非 LDAP 功能的目錄伺服器合用嗎？

Directory Proxy Server 能與支援 LDAP 的目錄伺服器合用。某些目錄產品廠商在自己的行銷文宣中號稱能實作 LDAP，但其實並非如此。Directory Proxy Server 已與 Sun ONE Directory Server 通過最徹底的測試。

如果使用 Directory Proxy Server 5.0 的主控台，就支援用 Sun ONE Directory Server 5.0 當作組態的存放處。

您可以設定 Directory Proxy Server 的組態公用程式嗎？

Directory Proxy Server 5.0 包含一個 Java 架構的 GUI (主控台)，可用來設定 Directory Proxy Server。此主控台利用 Sun ONE Directory Server 來儲存自己產生的組態。

Directory Proxy Server 功能

Directory Proxy Server 能防範拒絕服務的攻擊嗎？

是的。您可以限制每個連線處理的同步作業、每個連線所允許的作業數量、同時連線的總數、每個群組 (網路、子網路或根據連結 DN) 的最大同時連線數、及單一 IP 位址的最大同時連線數。

Directory Proxy Server 支援「反向」代理嗎？

嚴格說來，Directory Proxy Server 就是一個反向代理伺服器，但是 LDAP 通訊協定並不支援反向代理的概念。

Directory Proxy Server 能防範 LDAP 目錄的「拖網」嗎？

是的。拖網指的是非常廣泛的查詢，用來將您的目錄的一大部分下載回去，許多網站都希望禁止這種行爲。Directory Proxy Server 有很多方式可以禁止或限制拖網行爲：

- 搜尋的範圍可以限制在一層的樹狀目錄，整個子目錄則可以隱藏，而且可以針對查詢傳回的項目設定數量限制。
- 您可以禁止非等式搜尋，進而根據長度禁止以排除及子字串搜尋方式、將許多結果傳回的搜尋行爲；例如，禁止搜尋以 A-Z 字母爲開頭的姓氏。
- 您也可以設定讓 Directory Proxy Server 拒絕無索引的搜尋。無索引的搜尋效率奇差，還可能對效能有不良影響。

Directory Proxy Server 會自動對查詢進行負載平衡嗎？

Directory Proxy Server 對一組後端 LDAP 伺服器支援自動伺服器負載平衡的功能。Directory Proxy Server 也支援在主 LDAP 伺服器故障時，自動容錯移轉至第二個 LDAP 伺服器。

一個 Directory Proxy Server 伺服器能對幾個 LDAP 伺服器進行負載平衡？

目錄伺服器的效能需求，以及 Directory Proxy Server 執行的工作複雜程度，決定了 Directory Proxy Server 能負載平衡的最佳目錄伺服器數量。例如，如果 Directory Proxy Server 負責的工作很複雜，譬如屬性重新命名，您設定讓 Directory Proxy Server 負責負載平衡的目錄伺服器數量就應該縮減。爲避免複雜的 Directory Proxy Server 組態對效能可能產生的影響，請考慮添置 Directory Proxy Server。

可以篩選搜尋要求嗎？

是的。您可以設定讓 Directory Proxy Server 拒絕搜尋特定屬性的搜尋動作。此外，您可以設定讓 Directory Proxy Server 修改傳入的搜尋要求，使其符合指定的最小搜尋基礎、搜尋範圍及時間限制。

可以篩選搜尋結果嗎？

是的。所傳回的搜尋結果項目數量，以及搜尋組包含的屬性，都可以加以篩選。搜尋結果項目也可以根據項目 DN 或內容加以篩選。

存取群組如何定義？

根據用戶端的網路位址，可提供用戶端不同的目錄存取層次。所以可以讓企業防火牆內、外、執行子網路的用戶端，甚至是各台電腦，都有不同的存取層次。此外，可以在用戶端順利完成 LDAP 連結作業或建立 SSL 工作階段時，變更存取層次。

Directory Proxy Server 支援防護密碼驗證嗎？

是的。利用 SASL 機制，便可實作許多防護密碼驗證方法。但是後端目錄伺服器必須支援這些機制。Directory Proxy Server 不支援 SASL 機制與連線防護及 SASL EXTERNAL 機制合用。

Directory Proxy Server 能自動跟隨轉介嗎？

根據存取群組，可設定下列轉介。您可以設定讓各種存取群組自動跟隨轉介、傳回轉介、或放棄轉介。

Directory Proxy Server 會快取搜尋結果資訊嗎？

Directory Proxy Server 版本 5.0 SP1 不支援搜尋結果快取功能。

Directory Proxy Server 有屬性重新命名的功能嗎？

Directory Proxy Server 可以用透明的方式重新命名用戶端與伺服器之間的屬性名稱。

疑難排解

我要如何分析連線嘗試的記錄？

您可設定讓 Directory Proxy Server 使用 syslog 或寫入到特定的記錄檔。您可以從 Stanford University 的 ftp (<ftp://ftp.stanford.edu/general/security-tools/swatch>) 下載一個叫 swatch 的常見 UNIX 公用程式。swatch 可以用來監視 Directory Proxy Server 產生的記錄檔，並在所定義的事件發生時通知系統管理員。

我已經設定讓 Directory Proxy Server 跟隨轉介。可是當我非 LDAPv2 用戶端執行搜尋時，就碰到 error 32 (無此物件) 或其他錯誤。

爲了讓 Directory Proxy Server 接收從後端伺服器傳來的轉介，必須讓其使用 LDAPv3。請確定您已經將每個 LDAP 伺服器內容選取爲「僅 LDAP 版本 3」。

我在記錄檔中注意到，就算我的後端伺服器全都正常運作，某些閒置的用戶端連線還是會一直容錯移轉。

您的後端目錄伺服器正在讓閒置連線逾時，然後加以關閉。Directory Proxy Server 會容錯移轉這些關閉的連線。您也必須設定 Directory Proxy Server 的閒置連線逾時。這樣會清除閒置和外洩的用戶端連線，也可以避免遭受阻絕服務的攻擊。

能夠限制包含 presence 篩選條件的搜尋要求嗎？

Directory Proxy Server 版本 5.0 SP1 沒有限制用戶端使用 presence 篩選條件的直接辦法。但是有二個間接方法可以解決這個問題。

您可以將 `ids-proxy-con-forbidden-compare` 設定成不要比較的屬性名稱。這個方法限制過嚴，因為會拒絕包含 `(mail=*)` 及 `(mail=Andy*)` 過濾條件的搜尋。

另外由於 presence 過濾條件 (`attrName=*`) 一定會產生相同的結果 (假設資料不變)，我們可以利用 `ids-proxy-con-size-limit` 屬性及

`ids-proxy-sch-SizeLimitProperty` 來限制破壞範圍。雖然 LDAP 不要求要以指定的順序傳回項目，但是在大部分 (所有) 的實作下，搜尋結果不是以排序的順序傳回，就是以未排序的順序傳回，而順序每次都一樣。因此如果設定 Directory Proxy Server 有大小限制 (利用 `size-limit` 屬性或 `SizeLimitProperty`)，則每次都只會傳回第一個 'n'。因為這些 'n' 項目只能有二組，所以大幅降低了目錄拖網的風險。

請注意，Directory Proxy Server 會儘可能在要求中設定這個大小限制，所以目錄伺服器不需要自己傳送所有的項目。

大小限制屬性讓您在必要時，套用大小限制的例外狀況。例如假設您有一個項目是 `o=A`，在其下有 400 個組織單位 (OU)。每個 OU (組織單位) 下都有人。如果您要用戶端看到所有的 OU (組織單位)，可是每次只能看到 5 個人，您可以設定 `SizeLimitProperty`，讓基準 `o=A` 及只有一個層次範圍的搜尋不套用任何限制。其他的搜尋就套用 5 的限制。

當我設法執行工作或執行某個主控台功能時，我碰到的錯誤訊息說我心須確認 Administration Server 執行正常，而且此主機在連線到 Administration Server 的權限。

登入到管理 Directory Proxy Server 的 Administration Server 時，Directory Proxy Server 的主控制台也產生了錯誤訊息。您可能必須在 Administration Server 的主機上啟動 Sun ONE Console。開啓管理 Directory Proxy Server (就是您嘗試呼叫工作失敗的那一個) 的 Administration Server 伺服器主控台。按一下 [組態] 標籤，然後按一下 [網路] 標籤。在 [連線限制] 下，確定管理 Directory Proxy Server 失敗的 Sun ONE Console 主機沒有被禁止存取 Administration Server。如需詳細資訊，請參閱「Sun ONE Console Server 管理指南」。

Directory Proxy Server 啓動組態檔

本附錄包含 Directory Proxy Server 組態檔的資訊。包括：

- 組態檔概論 (第 165 頁)
- 啓動組態的關鍵字 (第 166 頁)

組態檔概論

`tailor.txt` 檔包含 Directory Proxy Server 要找到主要組態時，所需的啓動載入資訊。此檔中的指示會規定 Directory Proxy Server 的主要組態是要利用其他檔案，還是 Directory Proxy Server 會從 LDAP 伺服器取得主要組態。依預設，Directory Proxy Server 會在安裝實例目錄的 `etc` 子目錄中，尋找啓動 `tailor.txt` 組態檔。注意：利用指令行參數 `-t`，就可以讓 Directory Proxy Server 使用其他的檔案當作啓動組態檔。

啓動組態檔的功能是協助支援高可用性組態，可列出幾個聯絡點，用來檢索主要組態。啓動組態檔中利用二個關鍵字來描述聯絡點。Begin 及 End。Directory Proxy Server 會根據指定的次序處理聯絡資訊。Directory Proxy Server 在各個聯絡點上的動作，要看指定的聯絡點類型而定 (LDAP URL 或檔案的絕對路徑名稱)。

Directory Proxy Server 會針對 LDAP URL 類型的聯絡點，嘗試聯絡指定的主機。如果主機不願或無法傳回組態，Directory Proxy Server 會嘗試下一個聯絡點 (如果有的話)。如果此主機傳回組態，Directory Proxy Server 就會編輯所傳回的內容，然後開始遵守主要組態的指示，如果組態被視為無效，就會中止執行。

Directory Proxy Server 會針對檔案類型的聯絡點，嘗試載入指定的檔案，當作自己的主要組態。如果遺漏所指定的組態或組態被視為無效，Directory Proxy Server 就會中止執行。Directory Proxy Server 如果碰到檔案類型的聯絡點，就不會嘗試移動到下一個聯絡點。

Directory Proxy Server 從 LDAP 主機檢索主要組態時，會在三個方式中選取之一來連結到主機：匿名、簡單、或使用 SASL。

若要完成匿名連結，需省略 `configuration_bind_pw` 及 `configuration_bind_dn` 指示。換句話說，您的啟動組態聯絡資訊只會指定 `configuration_url` 指令。

簡單連結要使用 `configuration_bind_pw` 及 `configuration_bind_dn` 兩個指示才能支援。

SASL 連結需要指定 `sasl_bind_mechanism`、`configuration_bind_pw` 以及下列其中一個（而且只能有一個）指示：`configuration_bind_dn` 或 `configuration_username`。

啟動組態的關鍵字

被列舉的每個聯絡點都使用 `Begin` 關鍵字來標示聯絡點項目的啓始。反過來說，每個聯絡點項目都是以 `End` 關鍵字來終止。啟動組態檔中規定的每個指示都以一行表示。啟動組態不會辨識也不支援連續行。組態的選項以選項來指定，後面跟著冒號及三個一組的值。

`configuration_url`

`configuration_url` 選項會指定 LDAP 目錄伺服器，以及儲存 Directory Proxy Server 組態的目錄中的項目辨別名稱，或指定 LDIF 格式的本機檔案。例如，如果 Directory Proxy Server 組態儲存在 `ldap.sun.com` 主機上的 LDAP 目錄中、且 LDAP 服務在連接埠 389 上執行、且 Directory Proxy Server 項目的辨別名稱是 `ids-proxy-con-Server-Name= Directory Proxy Server`，就應該把下列加入組態檔：

```
Begin
configuration_url:
ldap://ldap.sun.com:389/ids-proxy-con-Server-Name= Directory Proxy
Server
End
```

如果組態要保留在 LDAP 伺服器中，您也許需要在 `ids-proxy-con-Server-Name= Directory Proxy Server` 後面指定尾碼，才能繼續與主機目錄的命名內容相容。例如：


```

Begin
configuration_url:
ldap://ldap.sun.com:389/ids-proxy-con-Server-Name= Directory Proxy
Server,
ou=services, dc=sun, dc=com
End

```

組態檔中的每個啓動組態指示，都應該以連續的一行來指定。

注意： 請勿把 `configuration_url` 範例中的自動換行符號，轉譯成在組態檔中插入換行符號的指示。

組態儲存成 LDIF 格式的檔案時 (也就是說，`<server-root>/dps-<hostname>/etc/tailor.ldif`)，就應該把下列加入組態檔：

```

Begin
configuration_url:
file://<server-root>/dps-<hostname>/etc/tailor.ldif#ids-proxy-con-S
erver-Name= Directory Proxy Server
End

```

configuration_bind_dn

`configuration_bind_dn` 選項會指定 Directory Proxy Server 連結到 `configuration_url` 選項中指定的 LDAP 伺服器時，要使用的辨別名稱。Directory Proxy Server 會以此辨別名稱執行簡單連結，並把 `configuration_bind_pw` 的值當作密碼。例如：

```

Begin
configuration_url:
ldap://ldap.sun.com:389/ids-proxy-con-Server-Name= Directory Proxy
Server
configuration_bind_dn: cn=Directory Manager
configuration_bind_pw: secret
End

```

如果 `configuration_url` 是「檔案」形式，就不需要 `configuration_bind_dn` 選項，而且會加以忽略。注意：`configuration_bind_dn` 及 `configuration_username` 指示互相排斥。

configuration_bind_pw

`configuration_bind_pw` 選項的功能是指定連結到 LDAP 目錄時要使用的密碼。此指示的功能是指定簡易或 SASL 連結時要使用的密碼。爲了保持安全，必須保護組態檔不被他人未經授權讀取。如果 `configuration_url` 是「檔案」形式，就不需要 `configuration_bind_pw` 選項，而且會忽略。(請參閱 `configuration_bind_dn` 參考範例。)

configuration_username

`configuration_username` 選項會指定 Directory Proxy Server 連結到 `configuration_url` 選項中指定的 LDAP 伺服器時，要使用的使用者名稱。此選項只有在使用 SASL 連結機制時才會使用。注意：`configuration_bind_dn` 及 `configuration_username` 指示互相排斥。

```
Begin
configuration_url:
ldap://ldap.sun.com:389/ids-proxy-con-Server-Name= Directory Proxy
Server
configuration_username: administrator
configuration_bind_pw: secret
sasl_bind_mechanism: CRAM-MD5
End
```

sasl_bind_mechanism

您可以根據要讓 Directory Proxy Server 使用哪種 SASL 連結機制，把 `sasl_bind_mechanism` 選項設定成 CRAM-MD5 或 DIGEST-MD5。如果沒有此選項，Directory Proxy Server 就會執行簡易連結或匿名連結。DIGEST-MD5 提供的安全等級比 CRAM-MD5 高，但是 DIGEST-MD5 的普及率沒有 CRAM-MD5 高。

指令簡介

本附錄說明與 Sun ONE Directory Proxy Server 相關的有用指令行程式。

本附錄包含下列各節：

- dpsconfig2ldif(第 169 頁)
- dpsldif2config(第 169 頁)

dpsconfig2ldif

dpsconfig2ldif 公用程式的功能是下載 Directory Proxy Server 組態，並儲存在 LDIF 檔案中。本公用程式可在下列位置找到：

```
<Install Root>/bin/dps_utilities/dpsconfig2ldif
```

本公用程式需要二個引數：

引數	描述
-t <i>filename</i>	<i>Filename</i> 是啟動組態檔的路徑。通常是 etc 目錄中的 tailor.txt 檔。
-o <i>filename</i>	輸出組態的檔案名稱。

dpsldif2config

ImportConfigLdif 會匯入 dpsConfig2Ldif 產生的 LDIF 檔。本公用程式可在下列位置找到：

```
<Install Root>/bin/dps_utilities/dpsldif2config
```

本公用程式需要下列引數：

引數	描述
ldif	包含 Directory Proxy Server 物件選項的 ldif 檔名稱：
-C	要建立的組態名稱 (如果未指定就是 imported-configuration)
-h	目錄主機名稱 (如果未指定就是 localhostd)
-P	目錄連接埠號碼 (如果未指定就是 389)
-D	目錄使用者 dn (如果未指定就是匿名連結)
-w	目錄使用者密碼 (如果未指定就是匿名連結)
-v	詳細

ImportConfigLdif 會匯入三種物件：

- 共用組態 (即 [Directory Proxy Server 組態] 節點下，主要主控台拓樸樹狀目錄中的這些組態)
- 共用系統內容
- 共用記錄屬性。

「組態名稱」參數只適用剛才說明的共用組態物件。系統內容及記錄屬性會從 ldif 檔「原封不動」地加入。如果共用組態物件沒有上述的參數名稱，這個指令檔就會利用上述的參數名稱建立新的組態。如果「已經」有上述名稱的組態，就不會進行匯入。如果目錄中已經有系統內容及記錄屬性，也不會加入。

一旦匯入組態，就必須重新啟動主要主控台，才能在拓樸樹狀目錄中檢視組態。爲了開始使用組態，Directory Proxy Server 實例伺服器就必須將自己指派到每個組態：系統會透過 Directory Proxy Server [伺服器主控台] 中的 [網路群組] 節點指派共用組態；透過 Directory Proxy Server [伺服器主控台] 中的系統節點指派 [系統內容] ([設定儲存爲 ...])；且透過 Directory Proxy Server [伺服器主控台] 中的 [記錄] 節點指派 [記錄屬性] ([設定儲存爲 ...])。

先決條件：

- 已經從 5.0(sp 1) 進行遷移。

後續條件：

- 所匯入的 ldif 檔中刻意忽略 belongs-to 屬性。

dpsdif2config

A

Administration Server 32

停止 33

從 Sun ONE Console 33

從 Windows NT [服務] 面板 33

從指令行 33

啓動 32

從 Windows NT [服務] 面板 33

從指令行 32

與 Sun ONE Console 的關係 32

與伺服器根目錄的關係 32

alias

包含憑證資訊的目錄 144

C

ChangeGroup 動作

已定義 121

configuration_bind_dn 選項 167

configuration_bind_pw 選項 168

configuration_url 選項 166

configuration_username 選項 168

D

-D 標幟 51

-d 標幟 51

Directory Proxy Server 主控台

簡介 36

Directory Proxy Server 伺服器主控台

[工作] 標籤 37

[組態] 標籤 37

重新啓動 Directory Proxy Server 47

開啓 33

監視記錄 135

簡介 36

Directory Proxy Server 伺服器主控台的 [工作] 標籤 37

您可完成的工作 37

Directory Proxy Server 伺服器主控台的 [組態] 標籤 37, 39

Directory Proxy Server 伺服器憑證 139

Directory Proxy Server 的伺服器憑證 139

Directory Proxy Server 的憑證 139

Directory Proxy Server 組態編輯器主控台

您可完成的工作 40

開啓 33

簡介 37

I

IDAR_ROOT 變數 52

L

LDAP 伺服器內容 99

M

-M 標幟 52

O

OnBindSuccess 事件

已定義 113

為其建立物件 114

OnSSLEstablished 事件

已定義 113

為其建立物件 117

S

SASL 連結 166

sasl_bind_mechanism 選項 168

Secure Sockets Layer (SSL) 137

SSL

產生憑證要求 140–141

通訊協定概論 ??–139

傳送手動的憑證要求 141

準備設定 138

Sun ONE Console

[伺服器及應用程式] 標籤 30

[使用者及群組] 標籤 31

如何啟動 34

在 Unix 中 35

在 Windows NT 中 35

使用者 ID 35

停止 Administration Server 33

停止 Directory Proxy Server 44

密碼 35

啟動 Directory Proxy Server 44

登入 URL 32, 35

與 Administration Server 的關係 32

檢查 Directory Proxy Server 狀態 49

簡介 29

Sun ONEConsole

重新啟動 Directory Proxy Server 47

T

-t 標幟 51

taylor.txt 檔 165

Token，請參閱安全裝置

Transport Layer Security (TLS) 137

V

-v 標幟 52

三書

已定義的伺服器憑證鏈結 140

ㄉ書

內容 91

LDAP 伺服器 99

刪除 111

負載平衡 104

- 修改 110
- 搜尋大小限制 108
- 禁止的項目 95
- 屬性重新命名 92

七畫

- 加密設定 58
- 加密通訊連結 137
- 目錄代理伺服器伺服器主控台
 - [組態] 標籤 39

六畫

- 共用的組態 40
- 如何開啓 Directory Proxy Server 主控台 33
- 如何檢查 Directory Proxy Server 是否為開或關 49
- 安裝伺服器憑證 139

五畫

- 伺服器
 - 要求憑證 140–141
 - [伺服器及應用程式] 標籤 30
 - 伺服器的開 / 關狀態 49
 - 伺服器根目錄
 - 與 Administration Server 的關係 32
 - 伺服器群組 32
 - 伺服器憑證要求，產生 140–141
 - 刪除
 - 內容物件 111
 - 事件物件 119
 - 動作物件 125
 - 群組 89
 - 系統記錄 127
 - 寫入位置 127

- 系統管理員
 - 存取權限 30
 - 所提供的工具
 - Directory Proxy Server 伺服器主控台 36
 - Directory Proxy Server 組態編輯器主控台 37
 - Sun ONEConsole 29
 - 登入 Sun ONE Console 35

八畫

- 事件
 - 刪除物件 119
 - 建立物件 114
 - 修改物件 118
 - 概論 113
 - 類型 113
- 取得 Directory Proxy Server 的伺服器憑證 139
- 定義
 - LDAP 伺服器內容 99
 - 事件物件 114
 - 負載平衡內容 104
 - 記錄內容 130
 - 動作物件 122
 - 搜尋大小限制內容 108
 - 禁止的項目內容 95
 - 群組 66
 - 屬性重新命名內容 92
- 明碼通訊連結 137
- [使用者及群組] 標籤 31

九畫

- 建立
 - LDAP 伺服器內容物件 99
 - 系統組態物件 53
 - 事件物件 114
 - 負載平衡內容物件 106
 - 記錄內容物件 130
 - 動作物件 122

- 搜尋大小限制內容物件 108
- 禁止的項目內容項目物件 96
- 群組 66
- 屬性重新命名內容物件 93
- 負載平衡內容 104
- 重新啓動
 - Directory Proxy Server 47
 - 從 Directory Proxy Server 伺服器主控台 47
 - 從命令列 47
- 限制搜尋大小 108

十畫

- 修改
 - 內容物件 110
 - 系統組態物件 53
 - 事件物件 118
 - 動作物件 124
 - 群組 88
- 記錄
 - 到 syslog 常駐程式 129
 - 記錄層級 128
 - 選擇正確層級的重要性 129
 - 記錄類型 127
 - 系統 127
 - 稽核 130
 - 從 Directory Proxy Server 伺服器主控台監視 135
 - 設定 130
 - 概論 127
- 記錄內容 130

十一畫

- 停止
 - Administration Server 33
 - 從 Sun ONE Console 33
 - 從 Windows NT [服務] 面板 33
 - 從指令行 33
 - Directory Proxy Server 43
 - 從 Sun ONE Console 44

- 從 Windows NT [服務] 面板 46
- 從命令列 45
- 動作
 - 刪除物件 125
 - 建立物件 122
 - 修改物件 124
 - 概論 121
- 匿名連結 166
- 啓動
 - Administration Server 32
 - 從 Windows NT [服務] 面板 33
 - 從指令行 32
 - Directory Proxy Server 43
 - 從 Sun ONE Console 44
 - 從 Windows NT [服務] 面板 46
 - 從命令列 45
 - Directory Proxy Server 伺服器主控台 33
 - Directory Proxy Server 組態編輯器主控台 33
 - Sun ONE Console 34
 - 在 Unix 中 35
 - 在 Windows NT 中 35
- 啓動組態的關鍵字 166
- 移除
 - 內容物件 111
 - 事件物件 119
 - 動作物件 125
 - 群組 89
- 設定
 - LDAP 伺服器內容 99
 - 加密設定 58
 - 系統設定 53
 - 事件 114
 - 事件導向動作 122
 - 負載平衡內容 104
 - 記錄 130
 - 記錄內容 130
 - 搜尋大小限制內容 108
 - 禁止的項目內容 95
 - 群組 66
 - 屬性重新命名內容 92
- 通訊連結
 - 加密 137
 - 明碼 137

十三畫

搜尋大小限制內容 108

概論

事件 113

記錄 127

動作 121

群組 61

禁止的項目內容 95

群組

加密設定 72

伺服器載入 87

刪除 89

決定成員資格 62

事件導向動作 71

使用狀況 61

建立 66

相容性設定 73

修改 88

從一個變更到另一個 62

搜尋屬性 78

概論 61

資料隱藏 76

網路準則 69

優先權的意義 62

轉介 86

轉送要求 73

屬性 83

群組成員資格 62

群組的優先權 62

十四畫

監視記錄 135

十五畫

稽核記錄 130

寫入位置 130

編輯

內容 110

系統組態物件 53

事件物件 118

動作物件 124

群組 88

十六畫

憑證

安裝 142

伺服器憑證 140

憑證要求，以電子郵件的形式傳送 141

憑證授權單位

受信任的憑證授權單位憑證 140

憑證資料庫

從備份還原 144

備份 144

十七畫

檢查 Directory Proxy Server 狀態

從 Sun ONE Console 49

從命令列 50

十八畫

簡單連結 166

二十一畫

屬性

記錄 130

屬性重新命名內容 92

二十三 卷

變更

事件物件 118

動作物件 124

群組 62, 88