Sun Java™ System

# Directory Server 5.2

## 管理指南

2004Q2

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

文件號碼：817-7164

# 目錄

# 前言

《 Directory Server 管理指南》描述在 Directory Server 上配置和維護目錄服務時所需的所有程序。其中包括在適當時從主控台和指令行配置所有 Directory Server 功能的程序。

本前言包含下列各節：



執行本指南中描述的任何工作之前，請閱讀 Directory Server 版本資訊。

# 應閱讀本指南的人員

本指南針對目錄管理員而撰寫。

本指南的作者假設讀者已熟悉下列事項：

- LDAP 和相關通訊協定的規格
- 叢集模式 ( 如果結合使用 Sun Cluster 軟體和 Directory Server)
- 網際網路和全球資訊網技術

# 本指南架構

本指南分爲以下各章：

- Directory Server 管理概論

  提供關於 Directory Server 的概論資訊，以及您要使用主控台啓動管理目錄服務所需的最基本工作。

- 管理目錄項目

  討論如何使用 Directory Server Console 和 LDAP 指令行公用程式管理您的目錄內容。並且也描述如何使用選用的屬性加密功能儲存屬性，以及如何使用 DSML 存取您的目錄。

- 建立策略樹狀目錄

  描述尾碼、子尾碼和鏈接尾碼的樹狀目錄及其管理。本章也概述使用 Directory Server Console 和指令行工具建立和管理樹狀目錄元素。

- 備份與復原資料

  概述提供給大量匯入目錄資料、匯入和匯出整個尾碼、立刻備份所有尾碼和復原備份資料的工具。

- 管理身份和角色

  說明群組、角色和服務類別 (CoS.) 提供的進階項目管理功能

- 管理存取控制

  描述決定授與存取目錄的使用者何種權限的存取控制指令 (ACI)。

- 管理使用者帳戶和密碼

  概述使用者帳戶管理工作，包括配置密碼和帳戶鎖定策略、停用帳戶或使用者群組，以及限制使用者可用的系統資源。

- 管理複製

  描述執行用於設定各種複製案例的工作，包括配置複製的步驟、透過 WAN 和 SSL 複製、監視複製狀態和解決複製衝突。

- 延伸目錄結構

  討論預設目錄結構不足以滿足需求時，如何延伸結構。

- 編製目錄資料索引

  提供索引功能概論，描述如何管理各種索引。

- 管理驗證和加密

  提供 Directory Server 中可用的安全機制概論，並描述如何執行和配置這些方法。

- 執行通過驗證

  描述您如何使用通過驗證管理 Directory Server 的單獨實例上的使用者和組態目錄。

- 使用日誌檔監視 Directory Server

  描述如何藉由配置記錄策略，及分析伺服器所維護的狀態資訊，來監控 Directory Server 的方法。

- 使用 SNMP 監視目錄伺服器

  描述啓用由 ANMP 管理員應用程式監視的 Directory Server 次代理程式。

- 強制屬性值唯一性

  描述 UID 唯一性 Plug-in 能確保所指定的屬性值，在目錄或樹狀子目錄內的所有項目中是唯一的值。

- 疑難排解 Directory Server

  提供有關安裝 Directory Server 的基本疑難排解資訊。

- 使用 Sun Crypto 加速板

  提供有關結合使用 Directory Server 與 Sun Crypto 加速板，以增強連線效能的指令，此連線使用的是基於憑證之驗證的安全通訊端階層 (SSL) 協定。

- 感謝協力廠商授權

  提供所有協力廠商軟體元件的版權公告。

# 使用說明文件

Directory Server 手冊是可攜式文件格式 (PDF) 和超文字標記語言 (HTML) 格式的可線上使用檔案。這兩種格式都是使殘障人士更容易使用本軟體的協助性技術。接下來便可以從下列位置進入 Sun™ 說明文件網站：

```
http://docs.sun.com
```

接下來便可以從下列位置存取 Directory Server 說明文件集：

```
http://docs.sun.com/coll/DirectoryServer_04q2
```

表 1 簡短描述說明文件集中的每份文件。左邊欄提供每份文件的名稱和 Web 位置。右邊欄描述文件的一般內容。

**表 1** Directory Server 說明文件

| 文件 | 內容 |
|---|---|
| Directory Server 版本說明<br>`http://docs.sun.com/doc/817-5216` | 含有關於 Directory Server 的最新資訊，包括已知問題。 |
| Directory Server Technical Overview<br>`http://docs.sun.com/doc/817-5217` | 提供許多 Directory Server 主要功能的速覽。 |
| Directory Server Deployment Planning Guide<br>`http://docs.sun.com/doc/817-5218` | 解釋規劃目錄拓樸、資料結構、安全性與監控的方式，並討論範例佈署。 |
| Directory Server Installation and Migration Guide<br>`http://docs.sun.com/doc/817-5219` | 包括移至 Directory Server 最新版本的更新、升級和資料遷移程序。 |
| Directory Server Performance Tuning Guide<br>`http://docs.sun.com/doc/817-5220` | 提供可以用於最佳化 Directory Server 效能的提示與說明。 |
| Directory Server 管理指南<br>`http://docs.sun.com/doc/817-5221` | 提供使用主控台與指令行的程序，以管理目錄內容與配置 Directory Server 的每一個功能。 |
| Directory Server Administration Reference<br>`http://docs.sun.com/doc/817-5235` | 詳細說明 Directory Server 組態參數、指令、檔案、錯誤訊息和結構。 |
| Directory Server Plug-In Developer’ s Guide<br>`http://docs.sun.com/doc/817-5222` | 示範開發 Directory Server Plug-in 的方式。 |
| Directory Server Plug-In Developer’ s Reference<br>`http://docs.sun.com/doc/817-5223` | 詳細說明 Directory Server Plug-in API 的資料結構與功能 |

# 慣例

表 2 描述本指南中使用的字體慣例。

**表 2** 字體慣例

| 字體 | 意義 | 範例 |
|---|---|---|
| AaBbCc123<br>(Monospace) | API 和語言元素、HTML 標籤、網站 URL、指令名稱、檔案名稱、目錄路徑名稱、電腦-螢幕輸出、範例代碼。 | 編輯您的 `.login` 檔。<br>使用 `ls -a` 以列出所有檔案。<br>`% You have mail`。 |
| **AaBbCc123**<br>(Monospace bold) | 您輸入的內容，與電腦螢幕的輸出向比對 | `% su`<br>`password:` |
| *AaBbCc123*<br>( 斜體 ) | 書名。<br>新字或新專有名詞。<br>要強調的字。<br>以真實名稱或值取代的指令行變數。 | 參閱 《開發人員指南》的第 6 章。<br>這些稱爲*類別* 選項。<br>您*必須* 爲超級使用者才能進行。<br>檔案位於 *ServerRoot* 目錄中。 |

表 3 描述本指南中使用的預留位置慣例。

**表 3** 預留位置慣例

| 項目 | 意義 | 範例 |
|---|---|---|
| *install-dir* | 安裝後，在軟體二進位檔案碼所在之下的目錄字首預留位置。 | Solaris 系統上的預設 *install-dir* 字首是 `/`。<br>Red Hat 系統上的預設 *install-dir* 字首是 `/opt/sun`。 |
| *ServerRoot* | 伺服器實例和資料所在的目錄之預留位置。<br>您可以透過用戶端 Server Console，從遠端管理 *ServerRoot* 下的每一台伺服器。Server Console 使用伺服器端 Administration Server 執行必須直接在伺服器端系統上執行的工作。 | 預設的 *ServerRoot* 目錄是 `/var/opt/mps/serverroot°C` |
| `slapd-`*serverID* | 特定伺服器實例在 *ServerRoot* 之下，而且其相關資料依預設值所在的目錄之預留位置。 | 預設 *serverID* 是主機名稱。 |

表 4 描述本書中使用的符號慣例。

**表 4** 符號慣例

| 符號 | 意義 | 表示法 | 範例 |
|---|---|---|---|
| [ ] | 含有選用的指令選項。 | O[*n*] | -O4, -O |
| { } | 含有一組適用於所需指令選項的選擇。 | d{y\|n} | -dy |
| \| | 分隔指令選項選擇。 | | |
| + | 結合圖形使用者介面中使用的鍵盤捷徑中的同時按鍵輸入。 | | Ctrl+A |
| - | 結合圖形使用者介面中使用的鍵盤捷徑中的連續按鍵輸入。 | | Esc-S |
| > | 指出圖形使用者介面中的功能表選項。 | | [ 檔案 ] > [ 新增 ]<br>[ 檔案 ] > [ 新增 ] > [ 範本 ] |

表 5 描述本書中使用的 Shell 提示符號慣例。

**表 5** Shell 提示符號

| Shell | 提示符號 |
|---|---|
| C shell | *machine-name*% |
| C shell 超級使用者 | *machine-name*# |
| Bourne shell 和 Korn shell | $ |
| Bourne shell 和 Korn shell 超級使用者 | # |

通常使用 LDAP 資料交換格式 (LDIF) [RFC2849] 表示 Directory Server 指令的輸入和輸出。換行以便讀取。

# 網站上的資源與工具

下列位置含有關於 Java Enterprise System 及其諸如 Directory Server 元件產品的資訊：

```
http://wwws.sun.com/software/learnabout/enterprisesystem/index.html
```

有些支援的平台提供了存取 Directory Server 的原生工具。如需有關測試和維護 LDAP 目錄伺服器的更多有用工具，請下載 Sun Java System Directory Server Resource Kit (DSRK)。您可以在下列位置取得此軟體：

```
http://wwws.sun.com/software/download/
```

您可在 《Directory Server Resource Kit Tools Reference》中取得 DSRK 工具的安裝說明和參考說明文件。

若要開發目錄用戶端應用程式，您也可以從相同位置下載 Sun Java System Directory SDK for C 與 Sun Java System Directory SDK for Java。

此外，Java 命名及目錄介面 (JNDI) 技術可支援從 Java 應用程式中用 LDAP 與 DSML v2 存取 Directory Server。您可以從下列位置取得有關 JNDI 的資訊：

```
http://java.sun.com/products/jndi/
```

JNDI Tutorial 包含如何使用 JNDI 的詳細說明與範例。其取得位置在：

```
http://java.sun.com/products/jndi/tutorial/
```

本文件中有提供其他相關資訊的協力廠商 URL。

**備註** Sun 對本文件中提到的協力廠商網站的有效性不負任何責任。Sun 不認可或對任何內容、廣告、產品或其他透過網站或任何資源使用的資料負責。Sun 對任何因使用透過網站或任何資源的內容、商品或服務而造成的損害或損失不負任何責任或義務。

# 如何報告問題

如果 Directory Server 出現任何問題，請使用下列任一種機制聯絡 Sun 客戶支援：

- 請造訪 Sun 軟體支援服務網站

  ```
  http://www.sun.com/service/sunone/software
  ```

  此網站可連結至線上支援中心、ProductTracker，並維護程式和支援聯絡號碼。

- SunSolve 支援網站位址：

  ```
  http://sunsolve.sun.com
  ```

  此網站含有修補程式、支援文件、安全資訊和 Sun System 手冊。

- 電話分派號碼與您的維護合約有關。

爲了讓我們能夠最快的協助您解決問題，當您尋求支援時，請提供下列資訊：

- 對於問題的描述，包括問題發生時的狀況，以及問題對作業所造成的影響
- 機器類型、作業系統版本和產品版本，包括可能影響問題的任何修補程式和其他軟體
- 使用方法的詳細步驟以重建問題
- 任何錯誤記錄或核心傾印

# Sun 歡迎您的任何意見

Sun 致力於改善其文件內容，並歡迎您提供任何意見與建議。使用網頁格式提供回饋意見給 Sun：

```
http://www.sun.com/hwdocs/feedback/
```

請在適當欄位內提供完整文件標題和文件編號。文件編號是一個七位數或九位數數字，可以在本書的標題頁或文件上方找到。例如，此 《管理指南》的文件編號是 817-7164。

提供意見與建議時，您可能需要在表單中提供文件的英文標題及文件號碼。此文件的英文文件號碼及標題爲：817-5221，Sun Java ™ System Directory Server 5.2 2004Q2 Administration Guide。

第 1 章

# Directory Server 管理概論

Directory Server 產品包含了管理多重目錄的 Directory Server、Administration Server，以及透過圖形介面管理兩個伺服器的 Server Console。本章提供關於 Directory Server 的概論資訊，以及您要啓動管理目錄服務所需的最基本工作。

本章所介紹的兩種 Directory Server 5.2 新增功能是 Plug-in 簽名和 DSML-over-HTTP 通訊協定。驗證 Plug-in 簽名是額外的安全性功能，讓伺服器可偵測或防止未經授權的 Plug-in 載入。Directory Server Markup Language (DSML) 是一種以 XML 爲基礎的新格式，用於傳送要求給目錄伺服器。

本章包含下列章節：

**備註** 如果正在執行一個版本以上的 Directory Server，請注意本章中的所有範例都假設 Directory Server 5.2 是預設版本。如果不是這種情況，您必須執行一次下列指令，將 5.2 設定成預設版本：

```
# /usr/sbin/directoryserver -d 5.2
```

或在每次執行 `directoryserver` 指令以指定版本時加入 `-useversion` 選項，例如：

```
# /usr/sbin/directoryserver -useversion 5.2 start
```

# Director Server 管理概論

Directory Server 爲穩定、具延展性的伺服器，設計來管理企業內的使用者和資源目錄。它是以稱爲輕量型目錄存取通訊協定 (Lightweight Directory Access Protocol，LDAP) 的開放式系統伺服器通訊協定爲基礎。Directory Server 會以 `ns-slapd` 處理程序或服務在您的機器上執行。伺服器會管理目錄內容並回應用戶端的要求。

您可透過 Sun Java System 提供協助您管理 Directory Server ( 和數種其他 Sun Java System 伺服器 ) 的第二伺服器，即 Administration Server，以執行大部分的 Directory Server 管理工作。Server Console 是 Administration Server 的圖形化介面；*Directory Server Console* 是 Server Console 的一部分，專門設計來搭配 Directory Server 使用。

您可以透過 Directory Server Console 執行大部分的 Directory Server 管理工作。您也可以利用編輯組態檔，或使用指令行公用程式手動執行管理工作。如需關於 Server Console 的詳細資訊，請參閱 《Administration Server Administration Guide》。

**備註** 如果正在使用 Directory Server 資料服務的 Sun Cluster HA，在管理 Directory Server 和來自指令行時，您必須使用 `directoryserver`(1M) 指令及其子指令。

請勿直接使用單獨的程序檔和二進位檔案碼。

# 啓動和停止 Directory Server

如果不使用安全通訊端階層 (Secure Sockets Layer，SSL)，您可以利用列示於此處的方法啓動和停止 Directory Server。如果您使用 SSL，請參閱第 24 頁「啓動啓用 SSL 的伺服器」。

## 從指令行啓動和停止伺服器

從指令行啓動和停止伺服器。執行下列指令：

```
# /usr/sbin/directoryserver -useversion 5.2 start
```

或

```
# /usr/sbin/directoryserver -useversion 5.2 stop
```

只有 Directory Server 5.2 不是預設版本時，才需要 `useversion` 選項。關於 `directoryserver` 指令的完整語法，請參閱《Directory Server Administration Reference》的 Chapter 1 "Command-Line Tools Reference"。

這些指令必須作爲根執行，如果：

- 您將根指定爲 Directory Server 的 UID
- 您正在使用連接埠 < 1024 ( 需有存取權限 )

否則，兩個指令必須與 Directory Server 相同的 UID 和 GID 一起執行。例如，如果 Directory Server 以 `nobody` 執行，則必須以 `nobody` 執行 `start` 和 `stop` 公用程式。

關於 Directory Server 之前版本的使用者，請注意已無法在參照模式中啓動伺服器。您可以使用 Directory Server Console 設定全域參照。此程序在第 71 頁「設定預設參照」中有說明。

## 從主控台啓動和停止伺服器

Directory Server Console 正在執行時，您可以透過其圖形介面啓動、停止和重新啓動 Directory Server。如需執行主控台的說明，請參閱第 25 頁「啓動 Directory Server Console」。

1. 在 Directory Server Console 最上層的 [ 工作 ] 標籤上，按一下相應的 [ 啓動目錄伺服器 ]、[ 停止目錄伺服器 ] 或 [ 重新啓動目錄伺服器 ] 旁的按鈕。

當您成功地從 Directory Server Console 啓動或停止 Directory Server 時，主控台會

訊息對話，說明已經啓動伺服器或關閉伺服器。如發生錯誤，主控台將顯示有關該錯誤的所有訊息。

## 啓動啓用 SSL 的伺服器

啓用 SSL 之前，您必須在您的伺服器上安裝與配置憑證。如需管理憑證及啓用 SSL 的說明，請參閱第 11 章「管理驗證和加密」；如需關於憑證、憑證資料庫及取得伺服器憑證的資訊，請參閱《Administration Server Administration Guide》中的 Chapter 9 "Using SSL and TLS with Sun Java System Servers"。

若要啓動已啓用 SSL 的伺服器，您必須從指令行啓動伺服器，而且提供保護伺服器憑證的密碼。

或者，您可以建立密碼檔案以儲存您的憑證密碼。透過將您的憑證資料庫密碼放置在檔案中，可以從伺服器主控台啓動伺服器，並且允許伺服器在無人執行時，自動重新啓動。

| 小心 | 在密碼檔案中是以純文字儲存該密碼，因此其使用代表了重大的安全性風險。如果您的伺服器是在不安全的環境中執行，則請勿使用密碼檔案。 |
|---|---|

密碼檔案必須放置在下列位置中：

*serverRoot*`/alias/slapd-`*serverID*`-pin.txt`

其中 *serverID* 是您在安裝時爲伺服器指定的識別碼。

在檔案中包含安全 Token 的名稱及其密碼，如下：

*deviceName* `Token:`*password*

本範例顯示內部憑證資料庫的裝置名稱 ( 大小寫及空格必須完全依照如下顯示 )：

`Internal (Software) Token:`*password*

如果將憑證儲存在替代裝置上，請使用位在 [ 管理憑證 ] 對話方塊上方的下拉式功能表中的裝置名稱。若要建立憑證資料庫，您必須使用管理伺服器及 [ 憑證設定精靈 ]。如需關於 Directory Server 使用 SSL 的資訊，請參閱第 11 章「管理驗證和加密」。

# 使用 Directory Server Console

Directory Server Console 是您以 Server Console 的單獨視窗存取的介面。您可按照下列程序所述，從 Server Console 啓動 Directory Server Console。

## 啓動 Directory Server Console

1. 請檢查確認 Directory Server 常駐程式 `slapd-`*serverID* 正在執行中。若沒有，請以 root 或管理使用者身份輸入下列指令來啓動它：

   ```
   # /usr/sbin/directoryserver -useversion 5.2 start
   ```

2. 請檢查確認管理伺服器常駐程式 `ns-httpd` 正在執行中。若沒有，請以 root 或管理使用者身份輸入下列指令來啓動它：

   ```
   # /usr/sbin/directoryserver -useversion 5.2 start-admin
   ```

3. 輸入下列指令啓動 Server Console：

   ```
   # /usr/sbin/directoryserver -useversion 5.2 startconsole
   ```

   如果要在不是安裝 Administration Server 的電腦執行 Server Console，可能需要依《Administration Server Administration Guide》Chapter 6 的 "Network Settings" 所述配置 Administration Server 上的連線限制。

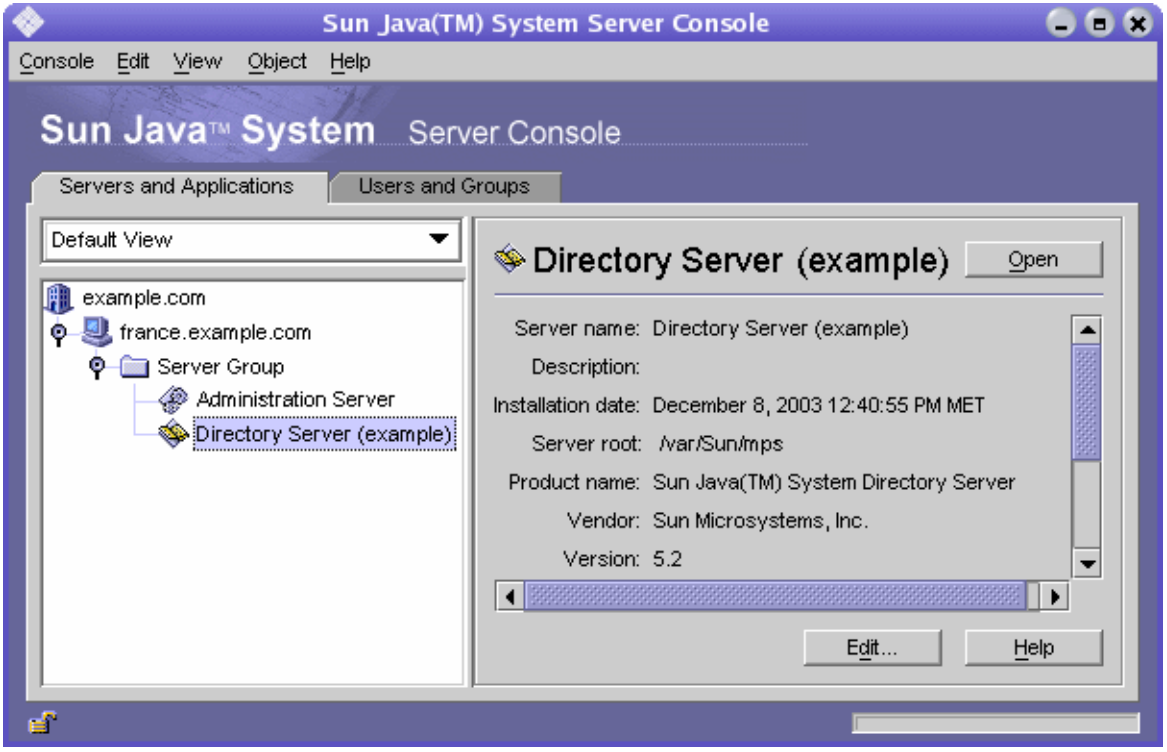
   顯示 [ 主控台 ] 登入視窗。或者，如果您的組態目錄 ( 包含 `o=NetscapeRoot` 尾碼的目錄 ) 儲存在單獨的 Directory Server 實例中，則會顯示視窗，要求該目錄伺服器的系統管理員使用者 DN、密碼及 Administration Server 的 URL。

4. 使用連結 DN 及使用者密碼登入，該使用者必須擁有充分的存取授權可執行您希望執行的作業。

   顯示 Server Console。

5. 在左面板的樹狀目錄中，瀏覽找尋您的 Directory Server 主機，然後按一下其名稱或圖示顯示其一般內容。

**圖 1-1** Sun Java System Server Console




若要編輯 Directory Server 名稱和描述，請按一下 [ 編輯 ] 按鈕。在文字方塊中輸入新的名稱和描述。按一下 [ 確定 ]，設定新名稱和描述。名稱會顯示在左邊的樹狀目錄中，如上圖所示。

6. 連按兩下樹狀目錄中的 Directory Server 名稱，或按一下 [ 開啓 ] 按鈕，顯示管理此目錄伺服器的 Directory Server Console。

## 瀏覽 Directory Server Console

Directory Server Console 提供介面，可在 Directory Server 實例上瀏覽及執行管理作業。此介面始終顯示四個標籤，可從其中存取所有 Directory Server 功能：

- [ 工作 ] 標籤 - 包含管理工作的按鈕，例如重新啓動伺服器。
- [ 組態 ] 標籤 - 提供管理伺服器之所有參數的存取。
- [ 目錄 ] 標籤 - 顯示與編輯目錄中所包含的資料項目。

- [ 狀態 ] 標籤 - 顯示伺服器的統計資料、日誌檔及複製狀態。

## [ 工作 ] 標籤

開啓 Directory Server Console 時，[ 工作 ] 標籤是第一個顯示的介面。它包含所有主要管理工作的按鈕，諸如下圖所示的啓動或停止 Directory Server。若要檢視所有工作及其按鈕，您或許需要捲動清單。

**圖 1-2** Directory Server Console 的 [ 工作 ] 標籤

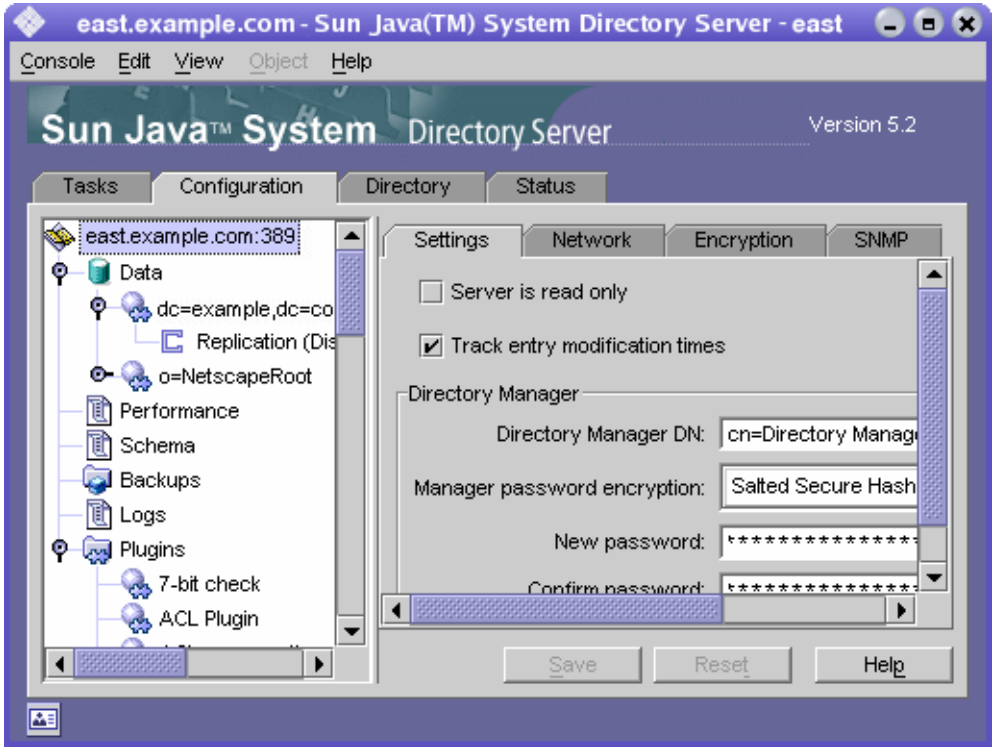

爲了執行這些工作，您必須以擁有系統管理員權限的使用者身份登入。權限不足的使用者無法看到 [ 工作 ] 按鈕。

## [ 組態 ] 標籤

Directory Server Console 的 [ 組態 ] 標籤提供介面和對話方塊，用來檢視及修改所有目錄設定值，如尾碼、複製、結構、記錄及 Plug-in 設定值。只有在您以擁有系統管理員權限的使用者身份登入時，這些對話方塊才能夠使用或生效。

此標籤的左邊含有所有組態功能的樹狀目錄，而右邊則顯示專門用來管理各功能的介面。這些介面通常包含其他標籤、對話方塊或快顯功能視窗。例如，下圖顯示整個目錄的一般設定值。

**圖 1-3** Directory Server Console 的 [ 組態 ] 標籤




當您選擇左樹狀目錄中的可設定項目時，該項目目前的設定值會顯示在右面板的一或多個標籤中。如需這些設定值的說明和行爲，請參閱本指南中描述各功能的章節。視設定的不同，某些變更在儲存時會立即生效，其他的則要等到重新啓動伺服器時才會生效。當伺服器必須重新啓動時，主控台將顯示對話方塊通知您。

標籤中未儲存的變更會在標籤名稱旁以紅色標記通知。即使您配置另一個項目或檢視其他主要標籤之一，標籤上還是會保持未儲存的變更。[ 儲存 ] 及 [ 重設 ] 按鈕可套用至指定可設定項目的所有標籤，但是不會影響其他項目的未儲存設定值。

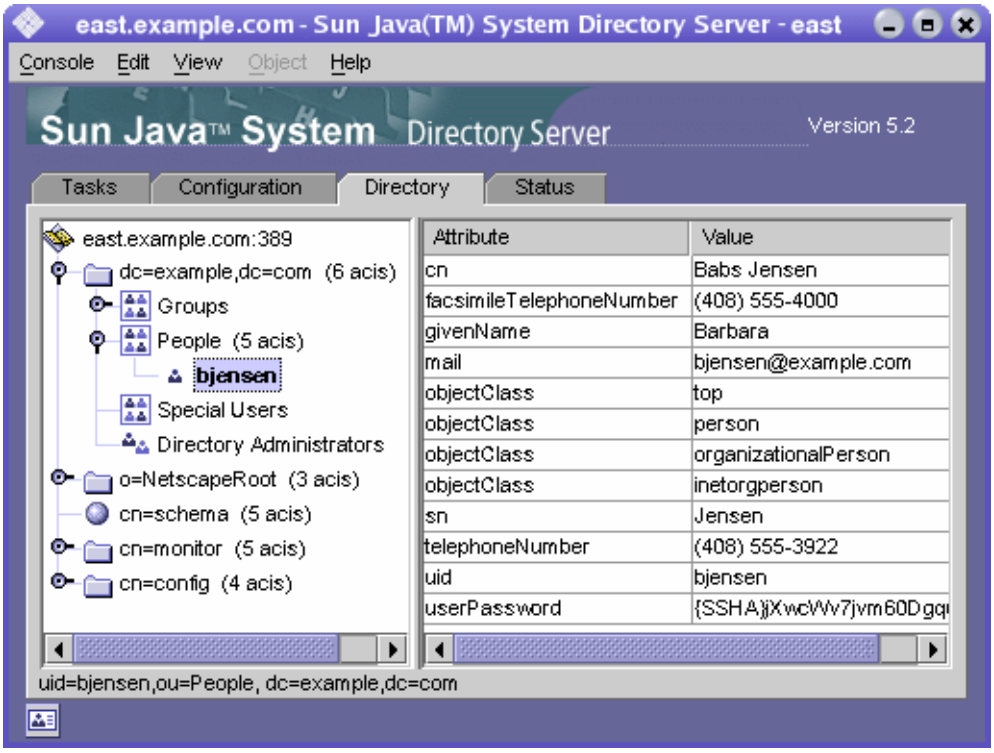
大多數文字欄位只允許您輸入具有該設定之正確語法的值。依據預設，在語法正確以前，設定標籤與您輸入的值會以紅色反白顯示。在所有設定值均爲有效語法前，[ 儲存 ] 按鈕會停用。您可以選擇用斜體字型代表反白顯示的錯誤值，如第 32 頁「視覺組態喜好設定」所述。

## [ 目錄 ] 標籤

主控台的 [ 目錄 ] 標籤爲了方便瀏覽，以樹狀目錄顯示目錄項目。在此標籤中，您可以瀏覽、顯示及編輯包含的所有項目和屬性。

**備註** 如果預計瀏覽數千個項目的清單，請建立瀏覽索引以便進行快速存取。如需指令，請參閱第 336 頁「主控台的瀏覽索引」。

**圖 1-4** Directory Server Console 的 [ 目錄 ] 標籤




如果登入時提供的連結 DN 具有充分的存取權限，則可以將組態項目視爲一般項目來檢視，並且可以直接修改。但是，您應該始終使用透過 [ 組態 ] 標籤可用的對話方塊來安全變更組態設定值。

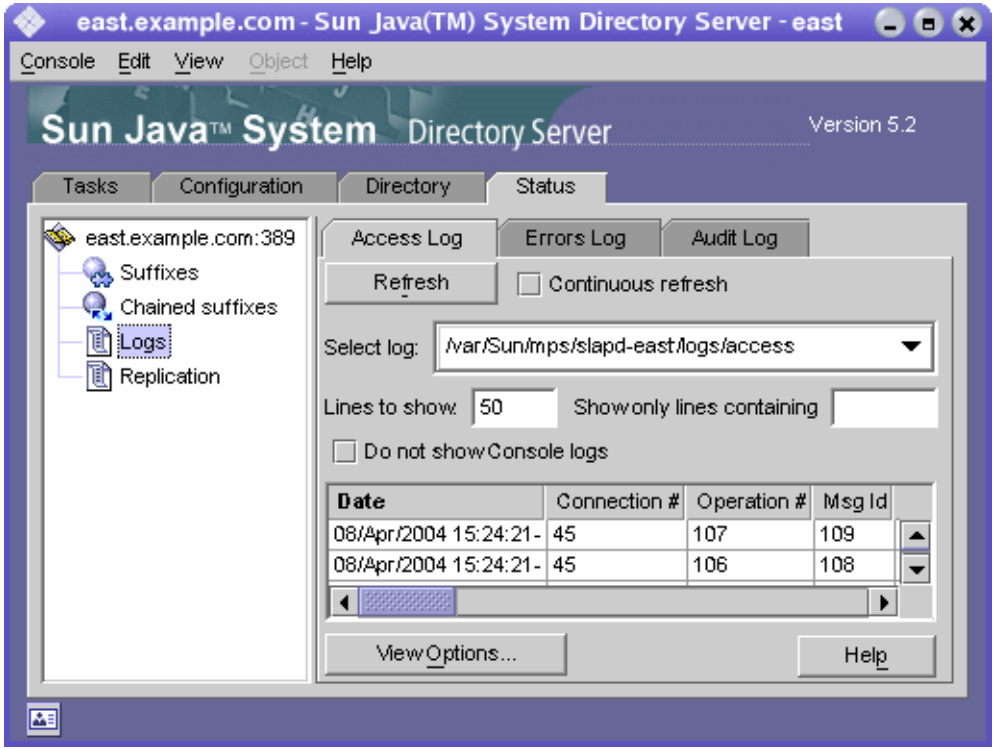
透過 [ 檢視 ] 功能表，有數個可用的選項可用來變更 [ 目錄 ] 標籤的佈局和內容。新佈局選項包括可檢視單一樹狀目錄中涵蓋葉項目在內的所有項目，而且也可以在右窗格中顯示屬性。預設是在右邊檢視葉項目，而非在左樹狀目錄中。

[ 檢視 ] > [ 顯示 ] 選項可啓用樹狀目錄中所有項目的 ACI 次數、角色次數及停用狀態圖示。在 圖 1-4 中，ACI 次數和葉項目顯示於左樹狀目錄中，而選擇項目的屬性值顯示於右窗格中。如需詳細資訊，請參閱第 33 頁「樹狀目錄檢視選項」。

### [ 狀態 ] 標籤

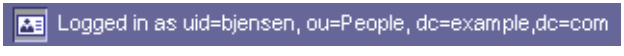
[ 狀態 ] 標籤顯示伺服器統計資料和日誌檔訊息。左樹狀目錄列出所有的狀態項目，在選擇時，各項目的內容會顯示在右窗格中。例如，下圖顯示日誌檔項目表。

**圖 1-5** Directory Server Console 的 [ 狀態 ] 標籤




## 從主控台檢視目前的連結 DN

您可以檢視用來登入 Directory Server Console 的 連結 DN，按一下位於顯示左下角的登入圖示即可。然後目前的連結 DN 會顯示於登入圖示旁，如此處所示：



## 變更您的登入身份

當您從 Directory Server Console 建立或管理項目時，以及當您首次存取 Server Console 時，系統讓您提供連結 DN 及密碼選項，以登入主控台。如此可識別正在存取樹狀目錄的使用者，以決定需要授與執行作業的存取授權。

首次啓動 Server Console 時，您可以目錄管理員 DN 登入。在任何時候，您都選擇以不同的使用者身份登入，而不必先停止再重新啓動主控台。

若要在 Server Console 中變更您的登入：

1. 在 Directory Server Console 上，請選擇 [ 工作 ] 標籤，然後按一下 [ 以新使用者登入目錄伺服器 ] 標籤旁的按鈕。或者，在另一個主控台標籤中時，請選擇 [ 主控台 ] > [ 登入爲新使用者 ] 功能表項目。

   顯示登入對話方塊。

2. 請輸入新 DN 和密碼，然後按一下 [ 確定 ]。

   請輸入您想要用來連結伺服器之項目的完整辨別名稱。例如，如果您想要以目錄管理員身份連結，則請在 [ 辨別名稱 ] 文字方塊中輸入下列 DN：

   ```
   cn=Directory Manager
   ```

以下章節，會進一步解說目錄管理員 DN 和密碼。

## 使用線上說明

線上說明爲 Directory Server Console 的大部分標籤和對話方塊提供上下文相關資訊。[ 說明 ] 按鈕通常位在這些介面的右下角。若要在任何螢幕上啓動上下文相關說明，其鍵盤快速鍵始終爲 Alt-P。

啓動線上說明會在主控台的內建瀏覽器中顯示 HTML 格式的頁面。您可以在這個頁面上按一下 [ 在瀏覽器中啓動 ] 按鈕，在外部瀏覽器 ( 如 Mozilla) 中顯示同一頁面。線上說明上有關詳細資訊的連結，也會開啓外部瀏覽器視窗。

每個線上說明頁會提供對應的標籤或對話方塊中所包含各欄位或按鈕的說明。當您透過主控台解釋、輸入或修改值時，這些資訊可以指引您。

Directory Server 的說明系統依存於 Administration Server。如果在 Administration Server 的遠端電腦上執行 Directory Server Console，您必須確認下列各項：

- 您可能必須設定 Administration Server 上強制執行的連線限制，以允許從您的電腦存取，如《Administration Server Administration Guide》 Chapter 6 的 "Network Settings" 所述。

- 如果要使用外部瀏覽器檢視線上說明頁，而且您的瀏覽器設爲使用代理，您必須執行下列動作：
  - 停用瀏覽器組態中的代理。在 Mozilla 中，選擇 [ 編輯 ] > [ 喜好設定 ] 功能表項目；再選擇 [ 進階 ] > [ 代理類別 ] 以存取代理組態。在 Internet Explorer 中，請選擇 [ 工具 ] 功能表中的 [ 網際網路選項 ]。
  - 配置 Administration Server 中的連線限制，以允許從代理伺服器存取。

| 小心 | 若配置 Administration Server 以允許從代理伺服器存取，會造成潛在的系統安全漏洞。 |
|---|---|

## 主控台剪貼簿

Directory Server Console 使用您的系統剪貼簿複製、剪下及貼上文字。若要減少輸入字元，當您在 [ 目錄 ] 標籤內瀏覽時，可以將項目的 DN 或 URL 複製到剪貼簿。

開啓必須在文字欄位中貼入 DN 或 URL 的對話方塊或另一個標籤之前：

1. 在 Directory Server Console 最上層的 [ 目錄 ] 標籤上，瀏覽整個樹狀目錄，選擇 ( 按一下滑鼠左鍵 ) 要複製其 DN 或 URL 的項目。
2. 然後選擇功能表中的 [ 編輯 ] > [ 複製 DN] 或 [ 編輯 ] > [ 複製 URL]。

## 主控台設定值

Directory Server Console 提供許多設定值，可自訂 [ 組態 ] 及 [ 目錄 ] 標籤中資訊的顯示方式。

### 視覺組態喜好設定

當您在最上層 [ 組態 ] 標籤上的欄位中修改組態參數與輸入值時，Directory Server Console 會使用彩色文字表示有效輸入。例如，如果啓用某項功能，該功能要求輸入進一步的組態值，則必要欄位的標籤會以紅色顯示，等您輸入有效值之後則會變成藍色。

依預設值，主控台使用紅色和藍色，但您可以依下列方式修改此行爲：

1. 在 Directory Server Console 的任意標籤上，選擇 [ 編輯 ] > [ 喜好設定 ] 功能表項目。在 [ 主控台喜好設定 ] 對話方塊中，選擇 [ 其他 ] 標籤。
2. 選擇您喜好的視覺組態標記的單選按鈕。您可以選擇彩色的字型或字型外觀，或同時選擇兩者。

3. 如需 [ 主控台喜好設定 ] 對話方塊的其他標籤上各項設定值的描述，請參閱《Administration Server Administration Guide》 Chapter 2 的 "Customizing Server Consol"。

   然後按一下 [ 確定 ] 以儲存變更。

4. 結束 Server Console 的所有視窗，再重新啓動。

## 樹狀目錄檢視選項

在 Directory Server Console 最上層的 [ 目錄 ] 標籤上，[ 檢視 ] 功能表的項目可讓您顯示樹狀目錄中的其他資訊，並可選擇右面板中顯示的內容。

下列 [ 檢視 ] 選項會影響 [ 目錄 ] 標籤的內容：

- 追蹤參照 - 若選擇此核取方塊，樹狀目錄將顯示參照目標的項目及所有子項，如同這些項目就在目錄中一樣。若清除此核取方塊，參照將顯示爲參照項目。如需詳細資訊，請參閱第 72 頁「建立智慧型參照」。
- 排序物件 - 若清除此核取方塊，則會依伺服器傳回項目的順序顯示項目。若選擇此核取方塊，則會根據下述的顯示屬性將樹狀目錄中同一層的項目排序。如需關於如何排序大型樹狀子目錄，而不影響伺服器效能的資訊，請參閱第 336 頁「主控台的瀏覽索引」。

  將依下列屬性所顯示的項目加以排序：`cn`、`givenname`、`o`、`ou`、`sn` 以及 `uid`。不會將依其他屬性顯示的項目加以排序。
- 顯示 >ACI 次數 - 如果項目的 `aci` 屬性中包含一或多個存取控制指令 (ACI)，樹狀目錄會在項目旁顯示個數。如需詳細資訊，請參閱第 6 章「管理存取控制」。
- 顯示 > 角色次數 - 如果項目是一或多個角色的成員，樹狀目錄會在項目旁顯示次數。如需詳細資訊，請參閱第 156 頁「指派角色」。
- 顯示 > 停用狀態 - 如果使用者或群組項目已停用，以防止連結到伺服器，則樹狀目錄會以項目的圖示顯示紅色方塊和線條。如需詳細資訊，請參閱第 257 頁「停用與啓用使用者與角色」。
- 佈局 > 檢視子項 - 當您選擇此佈局選項時，左面板中的樹狀目錄不會顯示目錄的葉項目，而選擇左面板中的父項節點會在右面板中顯示其所有子項，包括葉項目。您可以選擇任一面板的項目。
- 佈局 > 只檢視樹狀目錄 - 使用這個選項時，[ 目錄 ] 標籤只有一個面板，以顯示包含目錄中所有項目的樹狀目錄。
- 佈局 > 檢視屬性 - 在此佈局中，左面板顯示包含目錄中所有項目的樹狀目錄，而右面板顯示在樹狀目錄上選擇項目中儲存的屬性與值。

- 顯示屬性 - 按一下此功能表項目可查看 [ 顯示屬性 ] 對話方塊，並選擇 [ 目錄 ] 標籤顯示之項目的標籤。依預設值，標籤是項目第一個 RDN 屬性的值，例如 `People`。對於沒有 RDN 的基礎項目，標籤則是完整的 DN，例如 `dc=example,dc=com`。

  若要使用不同的屬性來顯示樹狀目錄中的項目，請選擇其他單選按鈕，並選擇屬性。沒有所選屬性的項目仍然會使用項目的第一個 RDN 屬性。依預設值，標籤中只使用屬性值。如果選擇 [ 顯示屬性名稱 ] 核取方塊，標籤會類似 `ou=People`。

- 重新整理 - 執行某些作業後，您必須重新整理樹狀目錄的顯示，才能檢視新的值。選擇此項目會從伺服器重新載入整個樹狀目錄。

# 配置 LDAP 參數

LDAP 參數是目錄伺服器中的基本設定值，例如目錄管理員的辨別名稱 (DN)、全域唯讀設定、連接埠組態及能否追蹤所有目錄修改時間等。

## 配置目錄管理員

*目錄管理員*是有權限的伺服器系統管理員，相當於 UNIX 的 root 使用者。存取控制不會套用至您定義爲目錄管理員的項目。您已在安裝過程中先定義了此項目。預設爲 `cn=Directory Manager`。

目錄管理員的 DN 儲存在 `nsslapd-rootDN` 屬性中，密碼儲存在 `cn=config` 分支的 `nsslapd-rootpw` 屬性中。

使用 Directory Server Console 變更目錄管理員 DN、密碼以及此密碼所使用的加密結構：

1. 以目錄管理員身份登入主控台。

   若您已經登入主控台，如需如何以不同使用者身份登入的說明，請參閱第 31 頁「變更您的登入身份」。

2. 在最上層的 [ 組態 ] 標籤上，選擇瀏覽樹狀目錄根部的伺服器節點，並在右面板中選擇 [ 設定值 ] 標籤。

3. 在 [ 目錄管理員 DN] 欄位中輸入新的辨別名稱。預設值是安裝期間所定義的值。

4. 從 [ 管理員密碼加密 ] 下拉式功能表中，選擇儲存結構，讓伺服器用來儲存目錄管理員的密碼。

5. 請使用所提供的文字欄位，輸入新密碼並做確認。

6. 按一下 [ 儲存 ]。

## 變更目錄伺服器連接埠號碼

您可利用 Directory Server Console 或變更 `cn=config` 項目下的 `nsslapd-port` 屬性值，修改使用者目錄伺服器的連接埠或安全連接埠號碼。

如果您想要修改包含 Sun Java System 組態資訊 (`o=NetscapeRoot` 樹狀子目錄 ) 的 Directory Server 連接埠或安全連接埠，可以透過 Directory Server Console 進行修改。

如果您變更組態目錄或使用者目錄連接埠或安全連接埠號碼，應該瞭解下列影響：

- 您必須變更 Administration Server 所配置的組態、使用者目錄連接埠或安全連接埠號碼。請參閱 《Administration Server Administration Guide》 Chapter 6 的 "Network Settings"。
- 如果您安裝了其他 Sun Java System Server，指向組態或使用者目錄，則您必須更新那些伺服器，以指向新的連接埠號碼。
- 如果設定非權限的連接埠號碼，而且 Directory Server 安裝在其他使用者可以存取的機器上，您可能冒著連接埠被另一個應用程式劫取的危險。也就是說，另一個應用程式可以連結相同的位址 / 連接埠對。此惡意應用程式可以處理要用於 Directory Server 的要求，而且可用於擷取驗證程序中使用的密碼、改變用戶端要求或伺服器回應或產生拒絕服務攻擊。若要避免此類安全性危險，請使用 `nsslapd-listenhost` 屬性指定 Directory Server 聆聽的介面 ( 位址 )。如需詳細資訊，請參閱 《Directory Server Administration Reference》 Chapter 2 "nsslapd-listenhost"。
- 透過主控台變更連接埠號碼不會對某些程序檔作必要的修改，而且需要以手動方式修改這些程序檔。如需更多資訊，請參閱 「Directory Server 版本說明」。

使用下列程序修改 Directory Server 在聆聽傳入 LDAP 要求時，所使用的連接埠或安全連接埠。若要修改 DSML 要求的連接埠，請參閱第 39 頁 「配置 DSML」。

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，選擇含有伺服器名稱的根節點，然後在右面板中選擇 [ 網路 ] 標籤。

   標籤顯示伺服器目前的 LDAP 通訊協定的連接埠設定值。

2. 在 [ 連接埠 ] 欄位中輸入您要伺服器用於進行非 SSL 通訊的連接埠號碼。預設值是 389。

3. 如果已依第 11 章 「管理驗證和加密」所述在此伺服器上啓用 SSL，您可以允許安全連接埠上的連線：

a. 選擇要使用安全連接埠和非安全連接埠的選項。

b. 在 [ 安全連接埠 ] 欄位中輸入您要伺服器用於進行 SSL 通訊的連接埠號碼。預設值是 636。

   您指定的加密連接埠號碼不可以與您用於一般 LDAP 通訊的連接埠號碼相同。

4. 按一下 [ 儲存 ]，然後再重新啓動伺服器。

如需資訊，請參閱第 23 頁 「啓動和停止 Directory Server」。

## 設定全域唯讀模式

在您的目錄中，每一個尾碼都可以放置獨立的唯讀模式，而且如果定義了特定參照也可以傳回此參照。Directory Server 也提供可套用至所有尾碼的全域唯讀模式，而且當定義了全域參照時，也可以傳回此參照。

全域唯讀模式是設計來讓系統管理員防止在執行如重新編製尾碼的索引時，同時修改了目錄的內容。基於這個原因，全域唯讀模式不會套用至下列組態分支：

- `cn=config`
- `cn=monitor`
- `cn=schema`

無論唯讀設定如何，「存取控制指令」(Access Control Instructions，ACI) 都應該保護這些分支，以防非管理使用者進行修改 ( 請參閱第 6 章「管理存取控制」)。全域唯讀模式可防止目錄中所有其他尾碼的更新作業，包括由目錄管理員啓動的更新作業。

如果啓用了唯讀模式，也會中斷尾碼上的複製。主機複本將不再變更任何複製，儘管它會持續複製在啓動唯讀模式前所作的所有變更。在停用唯讀模式前，用戶複本不會收到更新。多重主機複製藍本的主機不會變更任何複製，也無法收到其他主機的更新。

若要啓用或停用全域唯讀模式：

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，選擇組態樹狀目錄中的根節點，然後在右面板中選擇 [ 設定值 ] 標籤。
2. 選擇或取消選擇 [ 伺服器爲唯讀 ] 核取方塊。
3. 按一下 [ 儲存 ]。變更將立即生效。

如需關於將個別尾碼放置在唯讀模式的資訊，請參閱第 138 頁 「設定尾碼唯讀模式」。

## 追蹤目錄項目的修改

您可將伺服器配置成維護新近建立或修改項目的特殊屬性：

- `creatorsName` - 首先建立項目人員的辨別名稱。
- `createTimestamp` - 以 GMT ( 格林威治標準時間 ) 格式表示建立項目時間的時間戳記。
- `modifiersName` - 最後修改項目人員的辨別名稱。
- `modifyTimestamp`- 以 GMT 格式表示最後修改項目時間的時間戳記。

**備註** 當用戶端應用程式建立或修改鏈結尾碼中的項目時，`creatorsName` 和 `modifiersName` 屬性不會反映項目的真實建立者或修改者。這些屬性包含需要連結遠端伺服器的鏈結代理伺服器名稱。如需關於代理伺服器授權的資訊，請參閱第 111 頁「建立代理身份」。

追蹤複製尾碼的修改時間時，名稱和時間戳記屬性會被當成一般屬性而進行複製。如此一來，這些屬性會反映主機伺服器上項目原始修改的時間，而不是複製到用戶的時間。

若要啓用 Directory Server 追蹤此資訊：

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，選擇組態樹狀目錄中的根節點，然後在右面板中選擇 [ 設定值 ] 標籤。
2. 選擇 [ 追蹤項目修改次數 ] 核取方塊。

   伺服器會將 `creatorsName`、`createTimestamp`、`modifiersName` 和 `modifyTimestamp` 屬性加入至每一個新建或修改的項目。現有項目不會包含建立屬性。
3. 按一下 [ 儲存 ]，然後再重新啓動伺服器。

   如需更多資訊，請參閱第 23 頁「啓動和停止 Directory Server」。

# 驗證 Plug-in 簽名

驗證 Plug-in 簽名是 Directory Server 5.2 的新增功能。Directory Server 所提供的 Plug-in 各有一個數位簽名，可在啓動時由伺服器予以驗證。依預設值，伺服器將會驗證 Plug-in 簽名，但無論簽名是否存在或有效與否，它都會載入每一個 Plug-in。

驗證簽名有下列優點：

- 由 Directory Server 所提供的 Plug-in 的簽名代表它已經過嚴格測試，而且受到正式支援。
- 使用 Plug-in 二進位檔案碼本身的總和檢查碼，簽名驗證可偵測出 Plug-in 是否已遭到竄改。因此，簽名會保護在伺服器本身執行的敏感程式碼。
- 您可以配置伺服器只載入已經過簽署的 Plug-in，這有助於偵測未經過簽署及不支援的 Plug-in 的問題。

## 配置 Plug-in 簽名的驗證

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，選擇組態樹狀目錄中的 [Plug-in] 節點。目前的簽名驗證原則顯示在右面板中。
2. 選擇下列其中一個選項：
   - 不要驗證 Plug-in 的簽名 - 伺服器組態中定義的所有 Plug-in，不論簽名如何都予以載入。不會因爲 Plug-in 簽名而顯示任何警告或錯誤。
   - 標示含無效簽名的 Plug-in - 伺服器組態中定義的所有 Plug-in 都會載入，但伺服器將確認每個 Plug-in 的簽名。如果 Plug-in 二進位檔案碼已經遭到任何破壞，簽名將不再有效，而且伺服器將在啓動時在和錯誤日誌檔中顯示錯誤訊息。沒有簽名的 Plug-in 也會加上標幟。

     如果您有自訂、未經過簽署的 Plug-in，這是建議的選項。您的 Plug-in 將會載入，但您還是能夠檢視所有已簽署 Plug-in 的狀態。
   - 拒絕含無效簽名的 Plug-in - 伺服器將確認伺服器組態中定義的所有 Plug-in 的簽名，而且只載入含有效簽名的 Plug-in。伺服器將在啓動時在和錯誤記錄中顯示錯誤訊息，指出哪些 Plug-in 含無效簽名或無簽名。

     這是最安全的選項，但您將無法載入自訂、未經過簽署的 Plug-in。
3. 按一下 [ 儲存 ]，然後如第 23 頁「啓動和停止 Directory Server」中所述重新啓動 Directory Server。

## 檢視 Plug-in 的狀態

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，展開組態樹狀目錄中的 [Plug-in] 節點，並選擇要確認的 Plug-in。Plug-in 目前的組態顯示在右面板中。
2. [ 簽名狀態 ] 欄位顯示 Plug-in 的簽名驗證狀態，並包含下列值之一：

- 未知 - 將伺服器配置爲不驗證 Plug-in 簽名時，所有 Plug-in 都處於此簽名狀態。只有要驗證 Plug-in 簽名時，才會顯示下列狀態。
- 有效簽名 - Plug-in 組態提供簽名，而該簽名符合 Plug-in 二進位檔案碼的總和檢查碼；此 Plug-in 正式受到支援。只有要爲簽名加上標幟但不拒絕無效簽名時，才會顯示下列狀態。
- 無效簽名 - Plug-in 組態提供簽名，但該簽名不符合 Plug-in 二進位檔案碼的總和檢查碼；這個狀態表示 Plug-in 可能已經遭到竄改。
- 無簽名 - Plug-in 組態不提供簽名供伺服器驗證。

# 配置 DSML

除了在輕量型目錄存取通訊協定 (Lightweight Directory Access Protocol，LDAP) 中處理要求外，Directory Server 現在也回應使用目錄服務標記語言版本 2 (Directory Service Markup Language version 2，DSMLv2) 傳送的要求。DSML 爲用戶端編碼目錄作業的另外一種方式，但是伺服器會以所有相同的存取控制及安全性功能，將 DSML 視同任何其他要求來處理。事實上，DSML 處理程序允許很多其他類型的用戶端可以存取您的目錄內容。

Directory Server 支援透過超文字傳輸通訊協定 (Hypertext Transfer Protocol，HTTP/1.1) 使用 DSMLv2，以及使用簡單物件存取通訊協定 (Simple Object Access Protocol，SOAP) 版本 1.1 作爲程式設計通訊協定，以傳輸 DSML 內容。如需有關這些通訊協定和 DSML 要求範例的詳細資訊，請參閱第 91 頁「使用 DSMLv2 存取目錄」。

## 啓用 DSML 要求

由於 LDAP 爲存取目錄的標準通訊協定，依預設，安裝 Directory Server 後，不會啓用 DSML 要求。如果您想要自己的伺服器能夠回應透過 HTTP/SOAP 傳送的 DSML 要求，必須確實啓用這項功能。

若要透過主控台在您的伺服器上啓用 DSML 要求：

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，選擇組態樹狀目錄中的根節點，並選擇右面板中的 [ 網路 ] 標籤。
2. 選擇 [ 啓用 DSML] 核取方塊，並選擇下列其中一個安全選項：只有已啓用 SSL 時才可使用安全連接埠選項，如第 11 章「管理驗證和加密」所述。
   - 僅非安全連接埠 - 只接受非安全連接埠上透過未加密 HTTP 的 DSML 要求。

- 僅安全連接埠 - 只接受安全連接埠上透過 HTTPS 的 DSML 要求。
- 安全和非安全連接埠 - 兩個連接埠都作用中，用戶端可選擇任一個。

3. 然後編輯下列任何一個欄位：
   - 連接埠 - 用於接收 DSML 要求的 HTTP 連接埠。
   - 加密連接埠 - 使用 SSL 接收加密 DSML 要求的 HTTP 連接埠。
   - 相對 URL - 相對的 URL，在附加上主機和連接埠時，決定用戶端必須用來傳送 DSML 要求的完整 URL。

   依據預設，該伺服器會處理傳送至下列 URL 的要求：

   `http://`*host*`:80/dsml`

4. 按一下 [ 儲存 ]，將會提醒您必須重新啓動該伺服器，以開始回應 DSML 要求。

若要透過指令行啓用 DSML 要求：

1. 請執行下列 `ldapmodify` 指令，啓用 DSML 前端 Plug-in 並修改其設定值。修改 `ds-hdsml-port`、`ds-hdsml-secureport` 及 `ds-hdsml-rooturl` 屬性是選用的：

   ```
   % ldapmodify -h host -p LDAPport -D "cn=Directory Manager" -w passwd
   dn:cn=DSMLv2-SOAP-HTTP,cn=frontends,cn=plugins,cn=config
   changetype:modify
   replace:nsslapd-pluginEnabled
   nsslapd-pluginEnabled:on
   -
   replace:ds-hdsml-port
   ds-hdsml-port:DSMLport
   -
   add:ds-hdsml-secureport
   ds-hdsml-port:secureDSMLport
   -
   replace:ds-hdsml-rooturl
   ds-hdsml-root:relativeURL
   -
   ^D
   ```

   根據你所定義的參數及屬性值，DSML 用戶端可以使用下列 URL 將要求傳送至此伺服器：

   `http://`*host*`:`*DSMLport*`/`*relativeURL*

   `https://`*host*`:`*secureDSMLport*`/`*relativeURL*

2. 修改完成 DSML 前端 Plug-in 後，您必須重新啓動伺服器使變更生效。不過，在您重新啓動伺服器前，或許會想要配置 DSML 驗證的安全性和識別對映，如下列章節中所述。

## 配置 DSML 安全性

除了先前章節中所述的安全連接埠設定以外，您也可以配置接受 DSML 要求時所需要的安全層級。DSML 前端 Plug-in 的 `ds-hdsml-clientauthmethod` 屬性，決定用戶端所需要的驗證方法。此屬性可以擁有下列的值：

- `httpBasicOnly` - 伺服器使用 HTTP Authorization 標頭中的內容，尋找可以對映至目錄中項目的使用者名稱。此處理程序及其組態在第 42 頁「DSML 識別對映」中有進一步的描述。使用此設定時，傳到安全 HTTPS 連接埠的 DSML 要求透過 SSL 加密，但不使用用戶端憑證。
- `clientCertOnly` - 伺服器會使用用戶端憑證的認證識別用戶端。有了此值，所有 DSML 用戶端都必須使用安全 HTTPS 連接埠傳送 DSML 要求並提供憑證。該伺服器會檢查確認用戶端憑證符合目錄中的項目。如需更多資訊，請參閱第 11 章「管理驗證和加密」。
- `clientCertFirst` - 伺服器會嘗試先利用用戶端憑證 ( 如果有提供的話 ) 來驗證用戶端。否則，該伺服器會使用授權標頭的內容來驗證用戶端。

如果 HTTP 要求中既無憑證也沒有提供授權標頭，則伺服器會以匿名連結執行 DSML 要求。下列情況中也會使用匿名連結：

- 指定 `clientCertOnly` 時，用戶端提供了有效授權標頭，但是卻沒有憑證。
- 指定 `httpBasicOnly` 時，用戶端提供了有效憑證，但是卻沒有授權標頭。

不論 `ds-hdsml-clientauthmethod` 屬性值爲何，如果提供了憑證，但是此憑證卻無法對應至任何項目，或者如果已指定了 HTTP 授權標頭，但是無法對映至使用者項目，則將會拒絕 DSML 要求並出現錯誤訊息 403:「禁止」。

若要透過主控台設定 DSML 安全需求：

1. 在 Directory Server 主控台最上層的 [ 組態 ] 標籤上，選擇組態樹狀目錄中的根節點，並選擇右面板中的 [ 加密 ] 標籤。

   您必須已經依第 11 章「管理驗證和加密」所述配置及啓用 SSL。

2. 在 [DSML 用戶端驗證 ] 欄位中，從下拉式功能表選擇其中一個選項。
3. 按一下 [ 儲存 ]，接著重新啓動伺服器以強制執行新的安全設定。

若要透過指令行設定 DSML 安全需求：

1. 請執行下列 ldapmodify 指令，編輯 DSML 前端 Plug-in 的屬性：

```
% ldapmodify -h host -p LDAPport -D "cn=Directory Manager" -w passwd
dn:cn=DSMLv2-SOAP-HTTP,cn=frontends,cn=plugins,cn=config
changetype:modify
replace:ds-hdsml-clientauthmethod
ds-hdsml-clientauthmethod:httpBasicOnly or
 clientCertOnly or clientCertFirst
^D
```

2. 修改完成 DSML 前端 Plug-in 後，您必須重新啓動伺服器，強制執行此新的安全設定。

# DSML 識別對映

在執行沒有憑證的基本驗證時，Directory Server 會使用稱爲*識別對映*的機制來決定接受 DSML 要求時應使用的連結 DN。此機制會從 HTTP 要求的 Authorization 標頭中擷取資訊，決定要用於連結的識別。如需此機制的完整描述，請參閱第 358 頁「識別對映」。

伺服器組態中的下列項目，提供 DSML-over-HTTP 的預設識別對映：

```
dn:cn=default,cn=HTTP-BASIC, cn=identity mapping, cn=config
objectclass:top
objectclass:nsContainer
objectclass:dsIdentityMapping
cn:default
dssearchbasedn:ou=People,userRoot
dssearchfilter:(uid=${Authorization})
```

此對映會在 ou=People,*userRoot* 樹狀子目錄中搜尋其 uid 屬性符合 Authorization 標頭中指定的使用者名稱的項目。*userRoot* 是您在安裝目錄時定義的尾碼，例如 dc=example,dc=com。

在對映項目屬性內，您可以使用 ${*header*} 格式的預留位置，其中 *header* 是 HTTP 標頭的名稱。DSML 對映中最常使用的標頭爲：

- ${Authorization} - 此字串會由 HTTP 授權標頭中所包含的使用者名稱取代。授權標頭包含使用者名稱及其密碼，但是唯有使用者名稱會在預留位置中取代。
- ${From} - 此字串會由 HTTP 來源標頭中可能包含的電子郵件地址取代。
- ${host} - 此字串會以 DSML 要求的 URL 中的主機名稱和連接埠號碼取代，這些是伺服器本身的主機名稱和連接埠號碼。

若要使 DSML 要求執行不同的識別對映，請爲 HTTP 標頭定義新的識別對映：

1. 編輯預設的 DSML-over-HTTP 識別對映，或爲此通訊協定建立自訂的對映。如需識別對映項目中各屬性的定義，請參閱 第 358 頁「識別對映」。這些對映必須位於下列項目之下：
   `cn=HTTP-BASIC, cn=identity mapping, cn=config.`

您可以依照下列兩種方式之一建立新對映：

- 使用 Directory Server console 最上層的 [ 目錄 ] 標籤，用適當的物件類別建立新項目，如第 48 頁「使用主控台管理項目」所述。
- 使用 `ldapmodify` 工具，從指令行加入此項目，如第 64 頁「使用 ldapmodify 加入項目」中所述。

2. 新對映生效前須重新啓動 Directory Server。

系統會先評估自訂對映，而如果自訂對映都不成功，則再評估預設對映。如果所有對映在決定 DSML 要求的連結 DN 時都失敗了，則會禁止並拒絕 DSML 要求 ( 錯誤 403)。

第 2 章

# 管理目錄項目

本章討論如何使用 Directory Server Console 和 LDAP 指令行公用程式管理您的目錄內容。並且也描述如何使用選用的屬性加密功能儲存屬性，以及如何使用 DSML 存取您的目錄。在規劃您的目錄佈署時，應該描述自己的目錄所要包含的資料類型特徵。建立項目及修改預設結構前，請先閱讀《Directory Server Deployment Planning Guide》 Chapter 2 的 "Planning and Accessing Directory Data"。

本章假設您已瞭解了一些 LDAP 結構及其定義的物件類別和屬性知識。如需 Directory Server 所提供的結構及所有物件類別與屬性的定義簡介，請參閱《Directory Server Administration Reference》中的 "Object Class Reference" 和 "Attribute Reference" 各章。

您必須定義適當的存取控制指示 (ACI) 才能修改您的目錄。如需詳細資訊，請參閱第 6 章「管理存取控制」。

本章包含下列章節：

# 組態項目

Directory Server 將所有的組態資訊儲存在下列檔案內：

*ServerRoot*/slapd-*serverID*/config/dse.ldif

此檔案使用 LDAP 資料交換格式 (LDIF)。LDIF 是項目、屬性及其值的文字表示方式，而且是 RFC2849 (http://www.ietf.org/rfc/rfc2849) 中描述的標準格式。dse.ldif 檔案中的 Directory Server 組態的組成有：

- cn=config 項目的屬性和值。
- cn=config 下樹狀子目錄中的所有項目及其屬性和值。某項目或屬性的存在與否通常具有重大的意義。
- 根項目 ("") 與 cn=monitor 項目的物件類別與存取控制指令 (ACI)。這些項目的其他屬性由伺服器產生。

Directory Server 讓所有組態設定值都可透過 LDAP 進行讀寫。依預設值，目錄的 cn=config 分支只能由 Administration Server 中定義的目錄管理員 (directory administrator) 及目錄管理員 (directory manager) 存取。這些管理使用者可以檢視及修改組態項目，就如同其他任何目錄項目一樣。

您應該避免在 cn=config 項目下建立項目，因爲這樣的項目會儲存在 dse.ldif 檔案內，而這個檔案不像普通項目的資料庫一樣具有高度調整性。因此，如果有許多項目 ( 特別是可能需要經常更新的項目 ) 儲存在 cn=config 下，可能會降低效能。然而，將特定的使用者項目，例如 [ 複製管理員 ] ( 供應商連結 DN) 項目儲存在 cn=config 下很有用，因爲這樣可集中管理組態資訊。

## 使用主控台修改組態

建議您使用 Directory Server Console 最上層的 [ 組態 ] 標籤來修改組態。此標籤的面板與對話方塊提供以工作爲基礎的控制項，可幫助您快速、有效率地設定組態。此外，主控台介面會爲您管理組態的複雜性與相互依存性。

在本文件「使用主控台 ...」程序中會加以說明主控台的組態介面，這些程序說明如何使用 [ 組態 ] 標籤的面板與對話方塊完成特定的管理工作。介面本身會清楚指示儲存組態的方式以及重新啓動伺服器讓變更生效的時機。

## 從指令行修改組態

因爲 cn=config 樹狀子目錄可透過 LDAP 存取，所以可以用 ldapsearch、ldapmodify 和 ldapdelete 指令檢視及修改伺服器組態。cn=config 項目及其下所有項目都可利用第 61 頁「從指令行管理項目」中說明的程序與 LDIF 格式進行修改。

但是您必須了解這些項目的意義、其屬性的用途以及允許的值等。本文件的「從指令行 ...」程序中會解釋這些重要的考慮事項，該程序會舉例說明您可以設定的組態項目與屬性。如需所有組態項目與屬性的完整描述，包括允許值的範圍，請參閱《Directory Server Administration Reference》。

因此，從主控台修改組態會比從指令行修改更加容易。但是，有少數組態設定無法透過主控台進行，因此只提供指令行程序。您也可以撰寫使用指令行工具的指令檔，利用指令行程序將組態工作自動化。

## 修改 dse.ldif 檔案

dse.ldif 檔案包含伺服器啓動或重新啓動時將讀取及使用的組態。這個檔案的 LDIF 內容是 cn=config 項目及其樹狀子目錄。只有安裝期間所定義的系統使用者可讀寫此檔案。

直接編輯此檔案內容來修改組態比較容易出錯，因此不建議這種作法。您應該知道下列運作方式：

- 在啓動時只會讀取 dse.ldif 檔案一次。之後，伺服器組態就以組態項目在記憶體中的 LDAP 影像爲準。將刪除在執行伺服器時對檔案的修改。
- 使用主控台或從指令行修改組態會變更組態的 LDAP 影像。有些目錄功能會在啓動時讀取目前的組態，因此不必重新啓動伺服器。
- 每當組態的 LDAP 影像變更時，伺服器就會寫入 dse.ldif 檔案。有些目錄功能只在伺服器啓動時讀取其組態，而寫入檔案可確保變更會存在。

  現有的 dse.ldif 檔案會複製成爲 dse.ldif.bak，並覆寫現有的 dse.ldif.bak。因此，如果在伺服器重新啓動之前透過 LDAP 變更組態，對 dse.ldif 檔案所做的任何手動變更將會消失不見。
- 每次成功啓動目錄後，dse.ldif 檔案會複製成同一位置中的 dse.ldif.startOK。如果因爲組態變更錯誤導致無法啓動伺服器，您必須從這個檔案復原 dse.ldif。

# 使用主控台管理項目

您可以用 Directory Server Console 上的 [ 目錄 ] 標籤及項目編輯器對話方塊個別加入、修改或刪除項目。如果要同時操作幾個項目，請參閱第 60 頁「使用主控台執行大量作業」。

如需關於啓動 Directory Server Console 與瀏覽使用者介面的詳細資訊，請參閱第 25 頁「使用 Directory Server Console」。

## 建立目錄項目

Directory Server Console 提供數個可建立目錄項目的自訂範本。每個範本是特定類型之物件類別的自訂編輯器。表 2-1 顯示每個自訂編輯器所用的物件類別。

**表 2-1** 項目範本與對應的物件類別

| 範本 | 物件類別 |
|---|---|
| 使用者 | `inetOrgPerson` ( 用於建立與編輯 )<br>`organizationalPerson` ( 用於編輯 )<br>`person` ( 用於編輯 ) |
| 群組 | `groupOfUniqueNames` 及其他可能用於動態群組與憑證群組的物件類別 |
| 組織單位 | `organizationalUnit` |
| 角色 | `nsRoleDefinition` 及其他 ( 依選擇受管理、篩選或巢式角色而定 ) |
| 服務類別 | `cosSuperDefinition` 及其他 ( 依服務類別的類型而定 ) |
| 密碼策略 | `passwordPolicy` |
| 參照 | `referral` |

這些自訂編輯器所包含的欄位代表所有強制屬性，以及個別物件類別常用的部分選用屬性。若要用這些範本建立項目，請依照第 49 頁「使用自訂編輯器建立項目」中的說明進行。若要建立任何其他類型的項目，請參閱第 51 頁「建立其他類型的項目」。

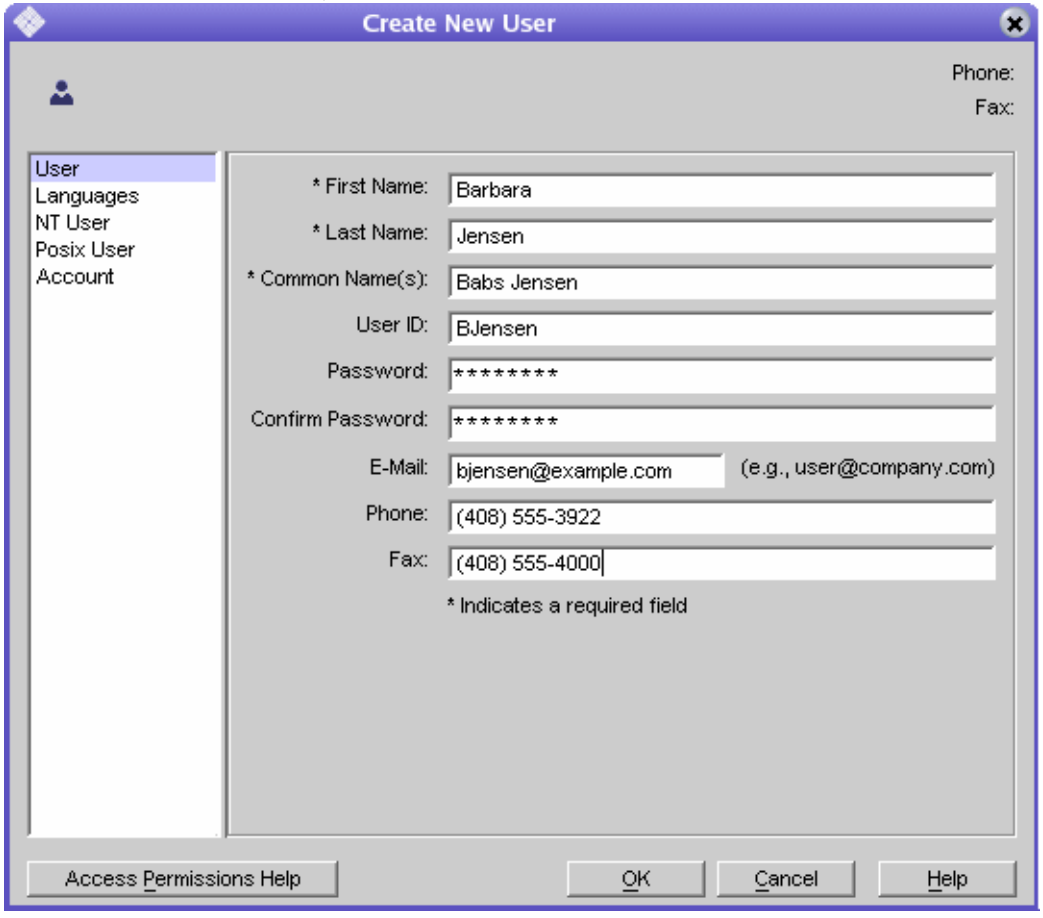
## 使用自訂編輯器建立項目

1. 在 Directory Server Console 最上層的 [ 目錄 ] 標籤上，展開樹狀目錄，以顯示要作爲新項目父項的項目。
2. 以滑鼠右鍵按一下父項，選擇 [ 新增 ] 功能表項目，再從子功能表中選擇項目類型：使用者、群組、組織單位、角色、服務類別、密碼策略或參照。或者，您可以在父項上按一下滑鼠左鍵以選擇父項，再從 [ 物件 ] > [ 新增 ] 功能表中選擇項目類型。出現您選擇之項目類型的自訂編輯器對話方塊。

   自訂編輯器的左欄有一連串的標籤，每個標籤的欄位則顯示在右邊。依預設值，所有自訂編輯器開啓時會選擇最上層的 [ 使用者 ] 或 [ 一般 ] 標籤，上面包含新項目的名稱和說明欄位。

   例如，下圖顯示使用者項目的自訂編輯器：

**圖 2-1** Directory Server Console - 使用者項目的自訂編輯器




3. 在自訂編輯器的欄位中爲您要提供的屬性輸入值。凡是欄位名稱旁有星號 (*) 的強制屬性都必須輸入值；其他欄位則可以保留空白。在允許多重值的欄位中，您可以按 Return 以分隔值。

   如需各項目類型的自訂編輯器中有關特定欄位進一步的協助，請按一下 [ 說明 ] 按鈕。如需 [ 使用者 ] 與 [ 組織單位 ] 編輯器上 [ 語言 ] 標籤的說明，請參閱第 53 頁「設定語言支援的屬性」。

   如需建立群組、角色及服務類別項目的進一步說明，請參閱第 5 章「管理身份和角色」。如需建立密碼策略的說明，請參閱第 7 章「管理使用者帳戶和密碼」。如需建立參照的說明，請參閱第 70 頁「設定參照」。

4. 按一下 [ 確定 ] 建立新的項目，並關閉自訂編輯器對話方塊，新項目出現在樹狀目錄中。

5. 自訂編輯器對話方塊並不會爲個別物件類別的所有選用屬性提供欄位。如果希望加入不顯示在自訂編輯器上的選用屬性，請依照第 54 頁「以標準編輯器修改項目」中的說明進行。

## 建立其他類型的項目

請依照以下步驟爲任何不在第 48 頁的表 2-1 中列出的物件類別建立項目。此程序也可用來建立目錄結構中已定義之任何自訂物件類別的項目：

1. 在 Directory Server Console 最上層的 [ 目錄 ] 標籤上，展開樹狀目錄，以顯示要作爲新項目父項的項目。

2. 以滑鼠右鍵按一下父項，再從子功能表中選擇 [ 新增 ] > [ 其他 ] 項目。或者，您可以在父項上按一下滑鼠左鍵以選擇父項，再選擇 [ 物件 ] > [ 新增 ] > [ 其他 ] 功能表項目。

   出現 [ 新增物件 ] 對話方塊。

3. 在 [ 新增物件 ] 對話方塊的物件類別清單中，選擇定義新項目的物件類別，再按一下 [ 確定 ]。

   如果選擇列在第 48 頁的表 2-1 中的物件類別，將顯示對應的自訂編輯器 ( 參閱第 49 頁「使用自訂編輯器建立項目」)。在其他情況中，則均顯示標準編輯器。

4. 建立新項目時，標準編輯器中會爲您選擇的物件類別中所有必要的屬性各提供一個欄位。所有必要屬性都必須輸入值。有些欄位有標準的預留位置值，例如 `New`，您應該用對您的項目有意義的值取代預留位置值。

5. 若要定義所選物件類別允許的其他屬性，您必須明確加入。若要爲選用屬性輸入值：

   a. 按一下 [ 加入屬性 ] 按鈕以顯示允許的屬性清單。

   b. 從 [ 加入屬性 ] 對話方塊中選擇一或多個屬性，再按一下 [ 確定 ]。

   c. 在標準編輯器中新屬性名稱旁輸入值。

   如需關於此對話方塊中其他控制項進一步的詳細資料，請參閱第 54 頁「以標準編輯器修改項目」。

6. 依照預設，會選擇其中一個必要屬性作爲命名屬性，該必要屬性會出現在標準編輯器中所顯示的項目 DN 中。若要變更命名屬性：

   a. 按一下 [ 變更 ] 按鈕以顯示 [ 變更命名屬性 ] 對話方塊。

   b. 在屬性表中，選擇要用在新項目 DN 中的一或多個屬性旁的核取方塊。

c. 在 [ 變更命名屬性 ] 對話方塊中按一下 [ 確定 ]。標準編輯器中的 DN 就會以選取的命名屬性顯示新的 DN。

7. 在標準編輯器中按一下 [ 確定 ]，以儲存新項目。

新項目在樹狀目錄中顯示爲父項的子項。

## 用自訂編輯器修改項目

對於列在第 48 頁的表 2-1 中的物件類別，您可以選擇使用對應的自訂編輯器或標準編輯器來編輯項目。使用自訂編輯器，可以很容易地存取最常用的欄位，而且介面會幫助您爲複雜的屬性 ( 例如角色或服務類別定義中的屬性 ) 定義值。

標準編輯器可讓您對項目執行比較進階的作業，例如加入物件類別、加入允許的屬性以及處理多重值屬性等。若要以標準編輯器編輯項目，請參閱第 54 頁「以標準編輯器修改項目」。

**備註** 自訂編輯器*只*可用來編輯列在第 48 頁的表 2-1 中的物件類別。至於包含其他*結構*物件類別的項目 ( 例如從 `inetorgperson` 繼承得來的自訂類別 )，則只能透過標準編輯器進行編輯。

若項目除了列示的物件類別之外還包含*輔助*物件類別，則該項目可以用自訂編輯器進行管理。但自訂編輯器中不顯示輔助類別所定義的任何屬性。如需輔助物件類別的定義，請參閱 《Directory Server Administration Reference》 Chapter 8 的 'Object Classes'。

## 啓動自訂編輯器

若要編輯第 48 頁的表 2-1 中所列物件類別的項目：

1. 在 Directory Server Console 最上層 [ 目錄 ] 標籤上，展開樹狀目錄，以顯示要編輯的項目。
2. 連按兩下項目。有幾個替代動作也可以啓動項目的自訂編輯器：
   - 以滑鼠右鍵按一下項目，再選擇 [ 以自訂編輯器編輯 ] 項目。
   - 以滑鼠左鍵按一下以選擇項目，再選擇 [ 物件 ] > [ 以自訂編輯器編輯 ] 功能表項目。
   - 以滑鼠左鍵按一下以選擇項目，再使用鍵盤快速鍵 Control-P。

   顯示項目的物件類別所使用的自訂編輯器。例如，第 50 頁的圖 2-1 中顯示 [ 使用者 ] 項目的自訂編輯器。
3. 依預設值，所有自訂編輯器開啓時會選擇最上層的 [ 使用者 ] 或 [ 一般 ] 標籤，上面包含新項目的名稱和說明欄位。針對您要修改的屬性，在自訂編輯器的欄位中編輯或移除值。欄位名稱旁以星號 (*) 標示的屬於強制屬性，您可以修改但無法移除這類屬性的值。其他欄位則可以保留空白。在允許多重值的欄位中，您可以按 Return 以分隔數值。

   選取左欄中的其他標籤，以修改對應面板上的值。如需各項目類型的自訂編輯器中有關特定欄位進一步的協助，請按一下 [ 說明 ] 按鈕。

   如需 [ 使用者 ] 與 [ 組織單位 ] 編輯器上 [ 語言 ] 標籤的說明，請參閱第 53 頁「設定語言支援的屬性」。在第 7 章「管理使用者帳戶和密碼」中說明了使用者與群組項目的 [ 帳戶 ] 標籤上的各欄位。爲「Directory Server 同步化服務」提供了 [NT 使用者 ] 與 [Posix 使用者 ] 標籤，如需詳細資料，請洽詢 Sun 代表。

   如需修改群組、角色與服務類別項目的進一步說明，請參閱第 5 章「管理身份和角色」」；如需修改密碼策略的說明，請參閱第 7 章「管理使用者帳戶和密碼」。如需修改參照的說明，請參閱第 70 頁「設定參照」。
4. 按一下 [ 確定 ] 儲存項目的變更，並關閉自訂編輯器對話方塊。如果修改了命名屬性 ( 例如使用者項目的一般名稱 )，樹狀目錄中將反映該變更。

## 設定語言支援的屬性

使用者與組織單位項目的自訂編輯器都提供國際化目錄的語言支援。

1. 依第 53 頁「啓動自訂編輯器」所述開啓您的項目的自訂編輯器。
2. 按一下左欄中的 [ 語言 ] 標籤。
3. 對於使用者項目，您可以用下拉式清單設定喜好的語言。

4. 對於使用者與組織單位項目，您可以在清單顯示的任何語言的指定欄位中輸入本地化的值。選擇語言，然後以該語言輸入一或多個值。定義本地化值之後，清單中的語言名稱會以粗體顯示。

   某些語言也有發音欄位，您可以在其中輸入本地化值的語音表示法。

5. 按一下 [ 確定 ] 儲存項目的變更，並關閉自訂編輯器對話方塊。

## 以標準編輯器修改項目

標準編輯器可根據登入主控台所用的連結 DN，允許您查看項目的所有可讀取屬性，並編輯可寫入屬性。它可讓您加入並移除屬性、設定多重值屬性以及管理項目的物件類別。加入屬性時，您可以定義二進位屬性與語言支援的子類別。

### 啓動標準編輯器

若要爲目錄中的任何項目啓動標準編輯器：

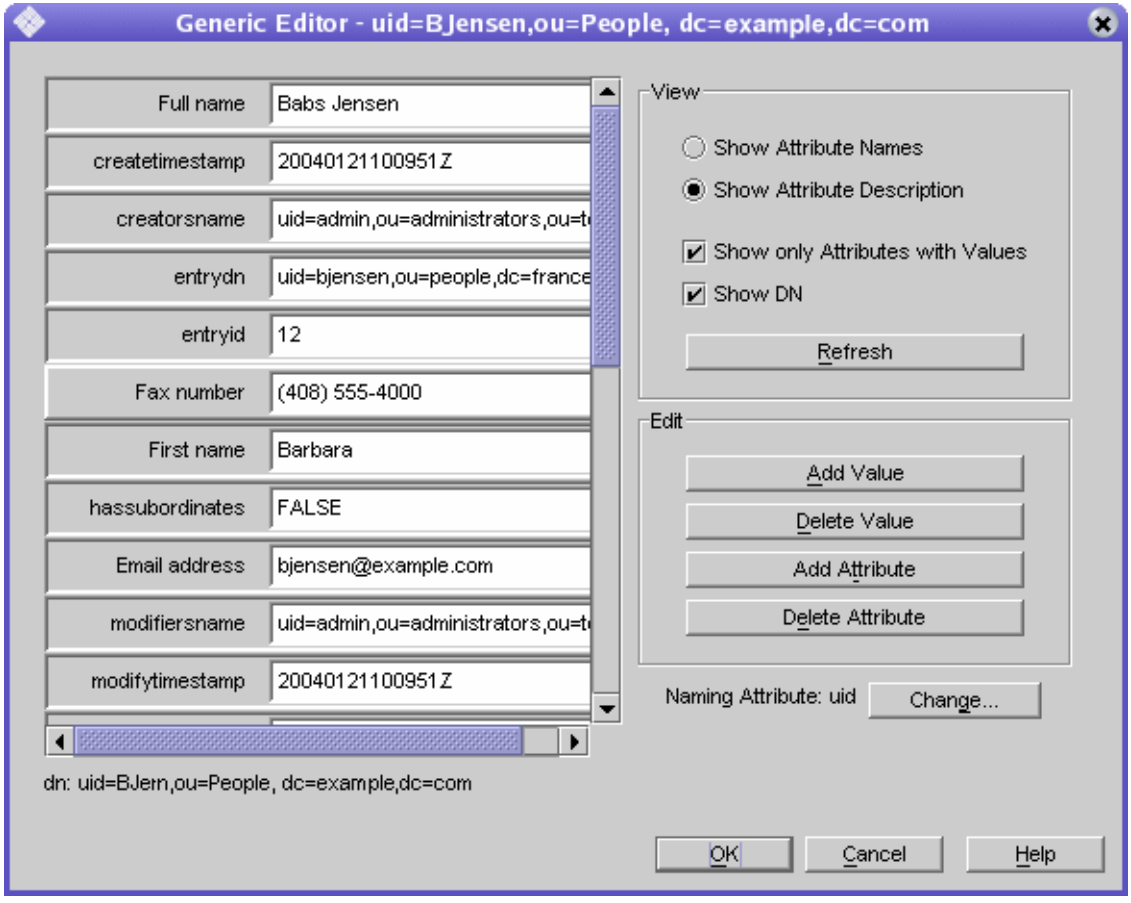
1. 在 Directory Server Console 最上層的 [ 目錄 ] 標籤上，展開樹狀目錄，以顯示要編輯的項目。

2. 以滑鼠右鍵按一下項目，再選擇 [ 以標準編輯器編輯 ] 項目。有幾個替代動作也可以啓動項目的自訂編輯器：

   - 以滑鼠左鍵按一下以選擇項目，再選擇 [ 物件 ] > [ 用標準編輯器編輯 ] 功能表項目。
   - 如果項目未列在第 48 頁的表 2-1 中，則連按兩下項目。依預設值，沒有自訂編輯器的物件類別會使用標準編輯器。

   顯示如下圖所示的標準編輯器。

**圖 2-2** Directory Server Console - 標準編輯器




在標準編輯器中，項目的屬性依字母順序排列，而且每個屬性值均各有一個文字方塊。所有屬性，包括唯讀與作業屬性都會顯示出來。右邊的控制項可讓您修改編輯器中的顯示，以及編輯屬性清單。

3. 或者，您可以用 [ 檢視 ] 方塊中的控制項修改標準編輯器的顯示：

   - 選擇 [ 顯示屬性名稱 ] 選項以檢視屬性最初在結構中定義的名稱。屬性清單將重新排列，以依名稱字母順序排列。
   - 選擇 [ 顯示屬性描述 ] 選項將屬性依替代名稱排列 (如果曾在結構中定義替代名稱 )。替代名稱通常可以更清楚地描述屬性。屬性清單將重新排列，以依照描述字母順序排列。

- 取消選取 [ 僅顯示含值的屬性 ] 核取方塊可列出項目的物件類別中由結構明確允許的所有屬性。如果項目包含 `extensibleObject` 物件類別，所有屬性都是隱含允許的，但不會列出來。預設狀況下只顯示有定義值的屬性。
- 選擇或取消選取 [ 顯示 DN] 核取方塊，以切換是否在屬性清單下顯示項目的辨別名稱。
- [ 重新整理 ] 按鈕將存取伺服器，以根據項目目前的內容更新所有屬性的值。

| 小心 | 按一下 [ 重新整理 ] 按鈕將立即移除您在標準編輯器中所做的任何修改，不會儲存它們。 |
|---|---|

下列各節描述設定屬性值、管理物件類別及變更項目命名屬性的控制方式。

## 修改屬性值

1. 依第 54 頁「啓動標準編輯器」所述開啓標準編輯器。
2. 捲動屬性清單，並按一下要修改的值。

   選取的屬性會反白顯示，而且在包含選取值的文字欄位內會出現編輯游標。
3. 使用滑鼠與鍵盤將文字編輯成所要的值。您可以用系統剪貼簿在此欄位中複製、剪下及貼上文字。

   如果無法編輯文字欄位的內容，表示屬性是唯讀的，或您沒有修改屬性的寫入權限。
4. 編輯其他任何值，或依需要對此項目執行其他修改，再按一下 [ 確定 ] 儲存變更，並關閉標準編輯器。

## 編輯多重值屬性

若屬性在目錄結構中定義爲多重值，則該屬性在標準編輯器中可以有多個欄位。如需更多資訊，請參閱第 9 章「延伸目錄結構」。

若要爲多重值屬性加入新值：

1. 依第 54 頁「啓動標準編輯器」所述開啓標準編輯器。
2. 捲動屬性清單，並按一下屬性或其中一個值。選取的屬性會反白顯示，並啓動 [ 加入值 ] 按鈕。如果未啓動此按鈕，表示選取的屬性不是定義爲多重值，或屬性是唯讀的，或是您沒有修改屬性的寫入權限。
3. 按一下 [ 加入值 ] 按鈕。清單中屬性名稱旁出現新的空白文字欄位。

4. 在新的文字欄位中輸入此屬性的新值。您可以用系統剪貼簿在此欄位中複製、剪下及貼上文字。
5. 編輯其他任何值，或依需要對此項目執行其他修改，再按一下 [ 確定 ] 儲存變更，並關閉標準編輯器。

若要移除多重值屬性的值：

1. 依第 54 頁「啓動標準編輯器」所述開啓標準編輯器。
2. 捲動屬性清單，並按一下要移除的特定值。選取的屬性會反白顯示，並啓動 [ 刪除值 ] 按鈕。如果未啓動此按鈕，表示選取的屬性是唯讀的，或您沒有修改屬性的寫入權限。
3. 按一下 [ 刪除值 ] 按鈕。就會移除包含選取值的文字欄位。
4. 編輯其他任何值，或依需要對此項目執行其他修改，再按一下 [ 確定 ] 儲存變更，並關閉標準編輯器。

## 加入屬性

在您可將屬性加入項目中之前，該項目必須已經包含需要或允許屬性的物件類別。如需詳細資訊，請參閱第 58 頁「管理物件類別」與第 9 章「延伸目錄結構」。

若要將屬性加入項目中：

1. 依第 54 頁「啓動標準編輯器」所述開啓標準編輯器。
2. 確定已核取 [ 僅顯示含值的屬性 ] 選項。
3. 按一下 [ 加入屬性 ] 按鈕以顯示包含屬性清單的對話方塊。此清單只包含針對項目所定義之物件類別允許的屬性。
4. 在 [ 加入屬性 ] 對話方塊中選擇要加入的一或多個屬性。
5. 或者，您可以從對話方塊上方的下拉式清單中選擇下列兩個子類型或其中之一：
   - [ 語言 ] 子類型 — 此子類型可用來指出屬性值所用的語言。您可以用不同語言將屬性加入許多次，以在目錄中儲存本地化資訊。

     或者，您可以在語言之外再選擇 [ 拼音 ] 子類型以表示此屬性的值包含指定語言中數值的對等發音。
   - 二進位子類型 — 指定二進位子類型至屬性，表示值應透過 LDAP 以二進位資料 ( 資料的不透明區塊 ) 傳輸，而不管其實際語法。應小心使用此選項。它的設計主要是針對沒有 LDAP 字串表示法的複雜語法，例如 `userCertificate`。請勿使用其值已作爲二進位的屬性之二進位子類型。
6. 選擇屬性及其選用子類型後按一下 [ 確定 ]。屬性會依字母順序加入標準編輯器的清單中。

7. 在新屬性名稱旁的空白文字欄位中輸入此屬性的新值。您可以用系統剪貼簿在此欄位中複製、剪下及貼上文字。
8. 編輯其他任何值，或依需要對此項目執行其他修改，再按一下 [ 確定 ] 儲存變更，並關閉標準編輯器。

## 移除屬性

若要從項目中移除屬性及其所有值：

1. 依第 54 頁 「啓動標準編輯器」所述開啓標準編輯器。
2. 捲動屬性清單，並按一下要移除的屬性名稱。選取的屬性會反白顯示，並啓動 [ 刪除屬性 ] 按鈕。如果未啓動此按鈕，表示選取的屬性是唯讀的，或您沒有修改屬性的寫入權限。

**備註** 標準編輯器允許您移除可爲此屬性定義之物件類別所需的屬性。如果嘗試儲存沒有必要屬性的項目，伺服器將回應物件類別違規。請確認您的項目包含它定義之所有物件類別的必要屬性。

3. 按一下 [ 刪除屬性 ] 按鈕。就會移除屬性及其所有文字欄位值。
4. 編輯其他任何值，或依需要對此項目執行其他修改，再按一下 [ 確定 ] 儲存變更，並關閉標準編輯器。

## 管理物件類別

項目的物件類別是由多重值的 `objectclass` 屬性所定義。修改此屬性時，標準編輯器會提供特殊的對話方塊，幫助您管理定義的物件類別。

若要爲項目加入物件類別：

1. 依第 54 頁 「啓動標準編輯器」所述開啓標準編輯器。
2. 捲動屬性清單，並選擇 `objectclass` 屬性。就會啓動 [ 加入值 ] 按鈕。如果未啓動此按鈕，表示您沒有權限，無法修改此項目的物件類別。
3. 按一下 [ 加入值 ] 按鈕。

   出現 [ 加入物件類別 ] 對話方塊。此視窗顯示您可加入項目中的物件類別清單。
4. 請選擇您想要加入此項目中的一或多個物件類別，再按一下 [ 確定 ]。您所選取的物件類別即顯示在 `objectclass` 屬性值清單中。
5. 如果新物件類別擁有還不存在項目中的必要屬性，標準編輯器將自動幫您加入。您必須爲所有必要屬性提供值。

6. 編輯其他任何值，或依需要對此項目執行其他修改，再按一下 [ 確定 ] 儲存變更，並關閉標準編輯器。

若要從項目中移除物件類別：

1. 依第 54 頁「啓動標準編輯器」所述開啓標準編輯器。
2. 捲動屬性清單，並按一下要移除之 `objectclass` 屬性的特定值。如果結構允許移除選取的物件類別，而且您有權限可修改此項目的物件類別，就會啓動 [ 刪除值 ] 按鈕。
3. 按一下 [ 刪除值 ] 按鈕。就會移除特定的物件類別。

   當您移除物件類別時，標準編輯器將自動移除其餘物件類別不允許或必要的任何屬性。如果移除命名屬性之一，將自動選擇另一個命名屬性，而且主控台將通知您確認此變更。
4. 編輯其他任何值，或依需要對此項目執行其他修改，再按一下 [ 確定 ] 儲存變更，並關閉標準編輯器。

## 重新命名項目

命名屬性是出現在項目辨別名稱 (DN) 中的屬性值配對。命名屬性是從項目現有的屬性中選擇而來。修改命名屬性即可重新命名項目：

1. 依第 54 頁「啓動標準編輯器」所述開啓標準編輯器。

   [ 變更 ] 按鈕旁的文字會顯示此項目目前的命名屬性。如果選擇 [ 顯示 DN] 核取方塊，您可以在屬性值清單下看到 DN 中的這些屬性。
2. 按一下 [ 變更 ] 按鈕。如果未啓動此按鈕，表示您沒有權限，無法重新命名此項目。

   出現 [ 變更命名屬性 ] 對話方塊。
3. 捲動屬性清單，選擇要放在此項目的 DN 中的屬性。選擇或取消選取屬性旁的核取方塊，以分別在命名屬性中加入或移除屬性。

   在同一父項下各項目的 DN 必須是唯一的。因此，您必須選擇其值或數值組合是唯一的命名屬性。如果 DN 不是唯一的，伺服器將拒絕儲存其項目。在慣例上，代表使用者的所有項目應使用相同的命名屬性。
4. 在 [ 變更命名屬性 ] 對話方塊中按一下 [ 確定 ]。標準對話方塊中的顯示會顯示此項目的新 DN。
5. 編輯其他任何值，或依需要對此項目執行其他修改，再按一下 [ 確定 ] 儲存變更，並關閉標準編輯器。

## 刪除目錄項目

若要使用 Directory Server Console 來刪除項目：

1. 在 Directory Server Console 最上層的 [ 目錄 ] 標籤上，展開樹狀目錄，以顯示要移除的項目。

   您也可以選擇樹狀子目錄的根節點，以刪除目錄的整個分支。

2. 以滑鼠右鍵按一下項目，再選擇 [ 刪除 ] 項目。數個替代動作也會刪除項目：

   - 以滑鼠左鍵按一下以選擇項目，再選擇 [ 編輯 ] > [ 刪除 ] 功能表項目。如果要將此項目貼到目錄的其他位置，您也可以使用 [ 編輯 ] > [ 剪下 ] 功能表項目。
   - 以滑鼠左鍵按一下以選擇項目，再使用鍵盤快速鍵 Control-D。

   當您選擇 [ 檢視 ] > [ 佈局 ] 選項以在 Directory Server Console 右面板中顯示子項後，您可以用 Control+ 按一下或 Shift+ 按一下的按鍵組合選擇多個要刪除的項目。

3. 確認您要刪除項目，或樹狀子目錄及其所有內容。

   伺服器可立即刪除一或多個項目。沒有復原。如果刪除多個項目，主控台將顯示資訊對話方塊，列出刪除項目數及發生的任何錯誤。

## 使用主控台執行大量作業

您可以用 LDIF 檔案加入多個項目、執行混合作業或匯入整個尾碼。若要使用 LDIF 檔案及 Directory Server Console 加入項目：

1. 用以上各節所顯示的語法在 LDIF 檔案中定義項目或作業。如果只要加入項目或初始化尾碼，就不需要 `changetype` 關鍵字，而且 LDIF 檔案可以只包含項目。如果要執行混合的作業，每個 DN 其後都應該跟著一個 `changetype`，而且視需要加上特定作業或屬性值。

2. 從 Directory Server 主控台匯入 LDIF 檔案。如需更多資訊，請參閱第 139 頁「匯入 LDIF 檔案」。

   如果要執行混合的作業，務必取消選取 [ 匯入 LDIF] 對話方塊上的 [ 僅加入 ]，讓伺服器會執行所有 LDIF 作業。

# 從指令行管理項目

ldapmodify 和 ldapdelete 指令行公用程式提供加入、編輯與刪除目錄項目的完整功能。您可以用它們管理伺服器的組態項目和使用者項目中的資料。這兩個公用程式也可用來撰寫指令檔，以執行一或多個目錄的大量管理工作。

ldapmodify 和 ldapdelete 指令用在本書各處的程序中。下列各節描述執行這些管理程序所需的所有基本作業。更進一步的功能、所有的指令行選項及這些指令的傳回值說明於《Directory Server Resource Kit Tools Reference》中的 Chapter 4 的 "ldapmodify" 和 Chapter 5 的 "ldapdelete"。

指令行公用程式的輸入始終採用 LDIF，您可以直接從指令行輸入，或透過輸入檔提供。下節提供有關 LDIF 輸入的資訊，隨後各節描述每種修改類型的 LDIF。

## 提供 LDIF 輸入

爲指令行公用程式提供 LDIF 輸入時，針對指令行輸入、特殊字元、結構檢查及項目的順序與大小等，有一些特殊考慮事項必須記住。所有目錄資料使用 Unicode 的 UTF-8 編碼儲存。因此您提供的任何 LDIF 輸入也必須以 UTF-8 編碼。LDIF 格式的詳細描述在《Directory Server Administration Reference》的 Chapter 7 "LDAP Data Interchange Format Reference" 中。

**備註** 請勿在 LDIF 屬性值字串的末尾不小心留下空格。Directory Server 讀取以空格作爲結束的屬性值時，它以 base64 對值進行編碼。

### 在指令行中止 LDIF 輸入

ldapmodify 和 ldapdelete 公用程式讀取您在指令後輸入的 LDIF 陳述式跟從檔案讀取是完全一樣的方式。當您完成提供輸入時，請輸入自己的 Shell 會辨識爲檔案結束 (end of file，EOF) 逸出順序的字元。

- 通常 EOF 逸出順序幾乎一定是 Control-D (^D)。

以下範例顯示如何中止 ldapmodify 指令的輸入：

```
prompt> ldapmodify -h host -p port -D bindDN -w password
dn:cn=Barry Nixon,ou=People,dc=example,dc=com
changetype:modify
delete:telephonenumber
^D
prompt>
```

爲了簡化及可攜性，本文件中的範例不顯示提示或 EOF 順序。

### 使用特殊字元

在指令行輸入指令選項時，您可能必須忽略一些對指令行解譯器具有特殊意義的字元，如空格 ( )、星號 (*)、反斜線 (\) 等。例如，許多 DN 包含空格，要用在大部分 UNIX Shell 中，您必須將值置於雙引號 ("") 內：

```
-D "cn=Barbara Jensen,ou=Product Development,dc=example,dc=com"
```

依指令行解譯器而定，您應該使用單引號或雙引號做此用途。如需更多資訊，請參閱您的作業系統文件。

此外，如果您使用包含逗號的 DN，必須以反斜線 (\) 忽略逗號。例如：

```
-D "cn=Patricia Fuentes,ou=People,o=example.com Bolivia\,S.A."
```

請注意，`ldapmodify` 指令後的 LDIF 陳述式是由指令解譯，而非由 Shell 解譯，因此不需要特殊的考慮事項。

### 結構檢查

加入或修改項目時，所使用的屬性必須是項目中的物件類別必要或允許的屬性，而且您的屬性必須包含與定義語法相符的值。

修改項目時，Directory Server 會在整個項目上執行結構檢查，而不僅在被修改的屬性上進行檢查。因此，如果項目中的任何物件類別或屬性不符合結構，作業都可能會失敗。如需詳細資訊，請參閱第 311 頁「結構檢查」。

### 排列 LDIF 項目的順序

在加入項目的任何 LDIF 文字順序中，不論是在指令行或在檔案中，父項都必須列在子項前。如此一來，當伺服器處理 LDIF 文字時，就會先建立父項再建立子項。

例如，如果要在 People 樹狀子目錄中建立不存在目錄中的項目，必須先列出代表 People 容器的項目，再列出樹狀子目錄中的項目：

```
dn:dc=example,dc=com
dn:ou=People,dc=example,dc=com
...
People subtree entries
...
dn:ou=Group,dc=example,dc=com
...
Group subtree entries
...
```

您可以使用 ldapmodify 指令行公用程式建立目錄中的任何項目，但是尾碼或子尾碼的根部是特殊項目，必須與必要的組態項目產生關聯。若要加入新的根尾碼或子尾碼及其相關的組態項目，請參閱第 103 頁「從指令行建立尾碼」。

## 管理大型項目

加入或修改含有極大型屬性值的項目前，伺服器可能必須經過配置才能接受這類項目。爲保護伺服器以防負載過重，用戶端預設爲僅能傳送不超過 2 MB 的資料。

如果加入的項目大於此限制，或修改的屬性值大於此限制，伺服器將拒絕執行作業，並立即關閉連線。例如，在項目的一或多個屬性中如果有多媒體內容等二進位資料，就可能超過此限制。

而且，定義大型靜態群組的項目可能包含太多成員，以致於其表示法超過限制。但基於效能的原因，並不建議使用這樣的群組，您應該考慮重新設計目錄結構。如需更多資訊，請參閱第 154 頁「管理群組」。

若要修改伺服器對用戶端傳送的資料強制的大小限制：

1. 爲 cn=config 項目的 nsslapd-maxbersize 屬性設定新值。

- 若要使用主控台執行此動作，請以管理員或目錄管理員的身份登入，並根據第 54 頁「以標準編輯器修改項目」中的程序編輯 cn=config 項目。將 nsslapd-maxbersize 屬性設爲用戶端可一次傳送的最大位元數。
- 若要從指令行執行此動作，請使用下列指令：

  ```
  ldapmodify -h host -p port -D "cn=Directory Manager" -w password
  dn:cn=config
  changetype:modify
  replace:nsslapd-maxbersize
  nsslapd-maxbersize:sizeLimitInBytes
  ^D
  ```

  如需詳細資訊，請參閱 《Directory Server Administration Reference》 Chapter 2 的 "nsslapd-maxbersize"。

2. 依第 23 頁「啓動和停止 Directory Server」所述，重新啓動伺服器。

## 錯誤處理

指令行工具會循序處理 LDIF 輸入中的所有項目或修改。當第一個錯誤發生時，預設的運作方式是會停止處理。使用 -c 選項可不理會任何錯誤繼續處理所有輸入。您會在工具的輸出中看到錯誤狀況。

除了上述考慮事項之外，常見的錯誤包括：

- 沒有適當的作業存取權限。

- 用已存在目錄中 DN 加入項目。
- 於不存在的父項下加入項目。

如需關於錯誤狀況及迴避方式的詳細資訊，請參閱《Directory Server Resource Kit Tools Reference》中的 Chapter 4 "ldapmodify" 和 Chapter 5 "ldapdelete"。

## 使用 ldapmodify 加入項目

您可以用 `ldapmodify` 的 `-a` 選項在目錄中加入一或多個項目。下列範例建立一個結構項目以包含使用者，然後再建立使用者項目：

```
ldapmodify -a -h host -p port -D "cn=Directory Manager" -w password
dn:ou=People,dc=example,dc=com
objectclass:top
objectclass:organizationalUnit
ou:People
description:Container for user entries

dn:uid=bjensen,ou=People,dc=example,dc=com
objectclass:top
objectclass:person
objectclass:organizationalPerson
objectclass:inetorgPerson
uid:bjensen
givenName:Barbara
sn:Jensen
cn:Babs Jensen
telephoneNumber: (408) 555-3922
facsimileTelephoneNumber: (408) 555-4000
mail:bjensen@example.com
userPassword:clearPassword
```

`-D` 和 `-w` 選項分別指定有權建立這些項目之使用者的連結 DN 和密碼。`-a` 選項包含 LDIF 中即將加入的所有項目。然後以 DN 及屬性值指定每個項目，項目之間使用一個空白行。`ldapmodify` 公用程式會在輸入每個項目後建立，並報告任何錯誤。

在慣例上，項目的 LDIF 以下列順序列出屬性：

- 物件類別清單。
- 命名屬性或屬性。這是 DN 中所用的屬性，不一定是其中一項必要屬性。
- 所有物件類別的必要屬性清單。
- 任何希望包含的允許屬性。

輸入 userpassword 屬性的值時，請指定純文字版的密碼。伺服器會將這個值加密，並且只儲存加密的值。請務必要限制讀取權限，以保護 LDIF 檔案中的純文字密碼。

您也可以在指令行上使用不需要 -a 選項的 LDIF 替代格式。這種格式的優點是您可以將加入項目及修改項目的陳述式結合在一起，如下一節所示。

```
ldapmodify -h host -p port -D "cn=Directory Manager" -w password
dn:ou=People,dc=example,dc=com
changetype:add
objectclass:top
objectclass:organizationalUnit
ou:People
description:Container for user entries

dn:uid=bjensen,ou=People,dc=example,dc=com
changetype:add
objectclass:top
objectclass:person
objectclass:organizationalPerson
objectclass:inetorgPerson
uid:bjensen
givenName:Barbara
sn:Jensen
cn:Barbara Jensen
telephoneNumber: (408) 555-3922
facsimileTelephoneNumber: (408) 555-4000
mail:bjensen@example.com
userPassword:clearPassword
```

changetype:add 關鍵字指出應以後續的所有屬性建立指定 DN 的項目。所有其他選項和 LDIF 慣例都一樣。

在兩個範例中，您都可以用 -f *filename* 選項從檔案讀取 LDIF，而不從終端機輸入讀取。LDIF 檔案包含的格式必須跟使用 -a 選項時的終端機輸入格式相同。

## 使用 ldapmodify 修改項目

使用 changetype:modify 關鍵可加入、取代或移除現有項目中的屬性及其值。當您指定 changetype:modify 時，您也必須提供一或多個變更作業，以指出項目的修改方式。以下範例顯示三個可能的 LDIF 變更作業：

```
dn:entryDN
changetype:modify
add:attribute
attribute:value
...
-
replace:attribute
attribute:newValue
...
-
delete:attribute
[attribute:value]
...
```

在行中使用破折號 (-) 可分隔對同一項目的作業，空白行可分隔不同項目的作業群組。您也可以爲每個作業指定數個 *attribute*:*value* 配對，將它們同時加入、取代或刪除。

### 加入屬性值

以下範例顯示如何使用相同的 `add` LDIF 語法，爲現有的多重值屬性及尚不存在的屬性加入值：

```
ldapmodify -h host -p port -D "cn=Directory Manager" -w password
dn:uid=bjensen,ou=People,dc=example,dc=com
changetype:modify
add:cn
cn:Babs Jensen
-
add:mobile
mobile: (408) 555-7844
mobile: (408) 555-7845
```

若有下列狀況，此作業可能會失敗，而且伺服器將傳回錯誤：

- 屬性已存在指定的值。
- 值未依照屬性所定義的語法。
- 屬性類型不是項目的物件類別所需要或允許的。
- 屬性類型不是多重值，而且已經存在值。

## 使用二進位屬性子類型

*attribute*;binary 子類型表示屬性值應透過 LDAP 以二進位資料 ( 資料的不透明區塊 ) 傳輸，而不管它們的實際語法。此子類型的的設計主要是針對沒有 LDAP 字串表示法的複雜語法，例如 userCertificate。二進位子類型應僅用於此用途。

您可以在 ldapmodify 指令所用的任何 LDIF 陳述式中爲屬性名稱加入適當的子類型。

若要輸入二進位值，您可以直接在 LDIF 文字中輸入，或從另一個檔案中讀取。以下範例顯示從檔案讀取的 LDIF 語法：

```
ldapmodify -h host -p port -D "cn=Directory Manager" -w password
version: 1
dn:uid=bjensen,ou=People,dc=example,dc=com
changetype:modify
add: userCertificate;binary
userCertificate;binary:< file:///path/certFile
```

爲了使用 < 語法指定檔案名稱，LDIF 陳述式的開頭行必須是 version:1。當 ldapmodify 處理此陳述式時，它會將屬性設爲從指定檔案的完整內容讀取而來的值。

## 加入語言子類型的屬性

屬性的語言與拼音子類型用於指定本地化的值。當您爲屬性指定語言子類型時，該子類型會以下列方式加入屬性名稱：

*attribute*;lang-*CC*

其中 *attribute* 是現有的屬性類型，*CC* 是兩個字母的國碼，以指定語言。您可以選擇爲語言子類型加入拼音子類型，以指定本地化值的對等發音。在此況狀下，屬性名稱變成：

*attribute*;lang-*CC*;phonetic

若要在含子類型的屬性上執行作業，您必須明確配合其子類型。例如，如果要修改含 lang-fr 語言子類型的屬性值，您必須以下列方式在修改作業中包含 lang-fr：

```
ldapmodify -h -h host -p port -D "cn=Directory Manager" -w password
dn:uid=bjensen,ou=People,dc=example,dc=com
changetype:modify
replace:homePostalAddress;lang-fr
homePostalAddress;lang-fr:34\, avenue des Champs-Elysées
```

### 修改屬性值

以下範例顯示如何使用 LDIF 中的 `replace` 語法修改單值屬性和多重值屬性的所有值：

```
ldapmodify -h -h host -p port -D "cn=Directory Manager" -w password
dn:uid=bjensen,ou=People,dc=example,dc=com
changetype:modify
replace:sn
sn:Morris
-
replace:cn
cn:Barbara Morris
cn:Babs Morris
```

使用 `replace` 語法時，將移除指定屬性目前所有的值，並加入所有指定值。

### 刪除屬性值

以下範例顯示如何完全刪除屬性，以及只刪除多重值屬性中的一個值：

```
ldapmodify -h host -p port -D "cn=Directory Manager" -w password
dn:uid=bjensen,ou=People,dc=example,dc=com
changetype:modify
delete:facsimileTelephoneNumber
-
delete:cn
cn:Babs Morris
```

使用 `delete` 語法卻不指定 *attribute:value* 配對時，將移除屬性的所有值。如果指定 *attribute:value* 配對，則只會移除該值。

### 修改多重值屬性的一個值

爲了用 `ldapmodify` 指令修改多重值屬性的一個值，您必須依下列範例所示執行兩個作業：

```
ldapmodify -h host -p port -D "cn=Directory Manager" -w password
dn:uid=bjensen,ou=People,dc=example,dc=com
changetype:modify
delete:mobile
mobile: (408) 555-7845
-
add:mobile
mobile: (408) 555-5487
```

# 使用 ldapmodify 重新命名項目

重新命名項目，就是修改它的相對辨別名稱 (RDN)，這是項目 DN 中最左邊的 *attribute=value* 配對。此屬性稱爲命名屬性，而且在項目的各屬性之間它也必須以相同的值存在。

重新命名項目時，您無法變更 DN 的其他任何部分，而導致項目移到不同的樹狀子目錄。若要將項目完全移到不同的分支，您必須用舊項目的屬性在其他樹狀子目錄中建立新項目，再刪除舊項目。

而且，您無法重新命名有任何子項的項目，這是因爲父項的 RDN 用在其子項的 DN 中，而 DN 中的所有項目都必須存在所致。若要移動整個樹狀目錄，您必須在新位置重新建立該樹狀目錄。

使用 `changetype:modrdn` 關鍵字可用 LDIF 陳述式重新命名項目。以下範例將重新命名 Barbara Morris 的 `uid` 命名屬性：

```
ldapmodify -h host -p port -D "cn=Directory Manager" -w password
dn:uid=bjensen,ou=People,dc=example,dc=com
changetype:modrdn
newrdn:uid=bmorris
deleteoldrdn: 1
```

`newrdn` 行用 *attribute=value* 語法指定新的命名屬性。`deleteoldrdn` 行指示是否應同時將原本的命名屬性從項目中移除 (`1` 代表是，`0` 代表否 )。不論任一種狀況，新的命名屬性也都會加入項目。

# 使用 ldapdelete 刪除項目

使用 `ldapdelete` 指令行公用程式可從目錄中刪除項目。此公用程式會連結到目錄伺服器，並刪除 DN 所指定的一或多個項目。您必須提供有權刪除指定項目的連結 DN。

就如同父項不能重新命名一樣的道理，您也不能刪除有子項的項目。LDAP 通訊協定禁止子項不再有父項存在的狀況發生。例如，您無法刪除組織單位項目，除非先刪除屬於該組織單位的所有項目。

| | |
|---|---|
| 小心 | 請勿刪除尾碼 `o=NetscapeRoot`。Administration Server 使用此尾碼儲存已安裝 Sun Java System 伺服器的相關資訊。刪除此尾碼可能會迫使您重新安裝包括 Directory Server 在內的所有 Sun Java System 伺服器。 |

在下列範例中，組織單位中只有一個項目，所以我們刪除該項目，再刪除父項：

```
ldapdelete -h host -p port -D "cn=Directory Manager" -w password
uid=bjensen,ou=People,dc=example,dc=com
ou=People,dc=example,dc=com
```

## 使用 ldapmodify 刪除項目

您也可以使用 ldapmodify 公用程式的 `changetype:delete` 關鍵字刪除項目。凡是以上所述使用 `ldapdelete` 時的限制，在這裏同樣適用。使用 LDIF 語法刪除項目的優點是您可以在一個 LDIF 檔案中執行混合的作業。

以下範例將執行與先前範例相同的刪除作業：

```
ldapmodify -h host -p port -D "cn=Directory Manager" -w password
dn:uid=bjensen,ou=People,dc=example,dc=com
changetype:delete

dn:ou=People,dc=example,dc=com
changetype:delete
```

# 設定參照

您可以使用參照告訴用戶端應用程式在本機無法取得資訊時應聯絡哪部伺服器。參照是指到遠端尾碼或項目的指標，Directory Server 會將此指標傳回給用戶端，而不傳回結果。接下來，用戶端必須重新於參照中指定的遠端伺服器上執行作業。在三種狀況下會發生此重新導向作業：

- 當用戶端應用程式要求不存在本機伺服器的項目時，伺服器傳回預設參照。
- 當整個尾碼爲了進行維護，或基於安全性的原因而設爲離線狀態時，伺服器將傳回該尾碼定義的參照。尾碼層級的參照說明於第 107 頁「設定存取權限及參照」中。當用戶端要求寫入作業時，尾碼的唯讀複本也會向主機伺服器傳回參照。
- 您可以建立稱爲智慧型參照的項目。當用戶端明確存取智慧型參照時，伺服器將傳回它所定義的參照。Directory Server Console 會自動配置以追蹤智慧型參照，使它們就像是最上層 [ 目錄 ] 標籤上的本機項目一樣。

不論是哪一種狀況，一個參照就是一個 LDAP URL，其中包含另一部伺服器的主機名稱、連接埠號碼及選用的 DN。如需詳細資訊，請參閱 《Directory Server Administration Reference》中的 Chapter 6 "LDAP URL Reference"。如需關於如何在目錄佈署中使用參照的概論，請參閱 《Directory Server Deployment Planning Guide》中的 Chapter 5 "Distribution, Chaining, and Referrals"。

下列各節描述定義目錄的預設參照及定義智慧型參照的程序。

# 設定預設參照

當用戶端應用程式在 DN 上所提交的作業不包含在目錄所維護的任何尾碼內時，便會將預設參照傳回給該用戶端應用程式。預設參照有時候稱爲全域參照，因爲它們適用於目錄中的所有尾碼。伺服器將傳回定義的所有尾碼，但傳回的順序則未定義。

## 使用主控台設定預設參照

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，選擇位於組態樹狀目錄根部的伺服器節點，然後選擇右面板中的 [ 網路 ] 標籤。
2. 選擇 [ 傳回參照 ] 核取方塊，並在文字欄位中輸入 LDAP URL。或者，按一下 [ 建構 URL]，在指引下完成 LDAP URL 的定義。指到安全連接埠的 LDAP URL 範例如下：

   ```
   ldaps://east.example.com:636/dc=example,dc=com
   ```

   您可以用空格與引號分隔，輸入多個參照 URL，如下：

   ```
   "ldap://east.example.com:389" "ldap://backup.example.com:389"
   ```

3. 按一下 [ 儲存 ] 讓變更立即生效。

## 從指令行設定預設參照

使用 `ldapmodify` 指令行公用程式可在目錄組態檔的 `cn=config` 項目中加入或取代一或多個預設參照。例如：

```
ldapmodify -a -h host -p port -D "cn=Directory Manager" -w password
dn:cn=config
changetype:modify
replace:nsslapd-referral
nsslapd-referral:ldap://east.example.com:389
nsslapd-referral:ldap://backup.example.com:389
```

您不必重新啓動伺服器。

# 建立智慧型參照

智慧型參照可讓您將目錄項目或樹狀目錄對映到特定 LDAP URL。使用智慧型參照，您可以將用戶端應用程式指到特定伺服器，或特定伺服器上的特定項目。

通常，智慧型參照會指到另一部伺服器上有相同 DN 的實際項目。但是您可以定義智慧型參照，指到同一伺服器或不同伺服器上的任何項目。例如，您可以用下列 DN 定義項目：

```
uid=bjensen,ou=People,dc=example,dc=com
```

做爲智慧型參照，指到 `east.example.com` 伺服器上的另一個項目：

```
cn=Babs Jensen,ou=Sales,o=east,dc=example,dc=com
```

目錄使用智慧型參照的方式符合 RFC 2251 (`http://www.ietf.org/rfc/rfc2251.txt`) 的 4.1.11 節中指定的標準。

## 使用主控台建立智慧型參照

1. 在 Directory Server Console 最上層的 [ 目錄 ] 標籤上，展開樹狀目錄，以顯示要做爲智慧型參照父項的項目。
2. 以滑鼠右鍵按一下父項，選擇 [ 新增 ] > [ 參照 ] 功能表項目。或者，您可以在父項上按一下滑鼠左鍵以選擇父項，再選擇 [ 物件 ] > [ 新增 ] > [ 參照 ] 功能表項目。

   出現參照項目的自訂編輯器對話方塊。
3. 在編輯器的 [ 一般 ] 標籤上，輸入參照的名稱，並從下拉式清單中選擇其命名屬性。名稱將是您選擇的命名屬性的值。或者，您可以爲此參照輸入描述字串。
4. 在編輯器的 [URL] 標籤上，按一下 [ 建構 ] 按鈕以定義智慧型參照的 URL。在出現的對話方塊中輸入 LDAP URL 的元素。

   URL 的元素包括儲存參照項目之目錄伺服器的主機名稱和 LDAP 連接埠號碼，以及伺服器上目標項目的 DN。依預設值，目標 DN 與智慧型參照項目的 DN 相同。但是目標 DN 可以是任何尾碼、樹狀子目錄或分葉項目。
5. 在 LDAP URL 建構對話方塊中，按一下 [ 確定 ]。URL 就顯示在新參照文字方塊中。
6. 按一下新參照文字方塊旁的 [ 加入 ]，將參照加入清單。
7. 您可以定義多個 URL，做爲此項目傳回的參照。使用 [ 建構 ]、[ 加入 ]、[ 刪除 ] 與 [ 變更 ] 按鈕可建立與管理 [ 參照清單 ]。

8. 按一下 [ 參照驗證 ] 按鈕可顯示對話方塊，您可以在其中設定 Directory Server Console 在追蹤參照到遠端伺服器時將用來連結的憑證。您可以定義存取伺服器時將使用的連結 DN 與密碼。指向同一伺服器的所有參照都將使用相同的認證。

9. 使用 [ 加入 ]、[ 編輯 ] 與 [ 刪除 ] 按鈕可管理伺服器與對應認證清單。完成時按一下 [ 確定 ]。

10. 在參照的自訂編輯器中，按一下 [ 儲存 ] 儲存您的智慧型參照項目。

    在主控台的樹狀目錄中，您應該看到目標樹狀子目錄或項目取代智慧型參照項目。如果智慧型參照項目有黃色警告圖示，表示 URL 或認證無效。請連按兩下項目，等看到 [ 參照錯誤 ] 時按一下 [ 繼續 ]，並修改 [URL] 或 [ 參照驗證 ] 以修正錯誤。

## 從指令行建立智慧型參照

若要建立智慧型參照，請用 `referral` 與 `extensibleObject` 物件類別建立項目。referral 物件類別允許 `ref` 屬性，此屬性應該要包含 LDAP URL。`extensibleObject` 物件類別可讓您使用任何結構屬性做爲命名屬性，以便能夠對映到目標項目。

例如，定義下列項目傳回智慧型參照，而不傳回 `uid=bjensen` 項目：

```
ldapmodify -a -h host -p port -D "cn=Directory Manager" -w password
dn:uid=bjensen,ou=People,dc=example,dc=com
objectclass:top
objectclass:extensibleObject
objectclass:referral
uid:bjensen
ref:ldap://east.example.com/cn=Babs%20Jensen,ou=Sales,
 o=east,dc=example,dc=com
```

**備註** 伺服器會忽略 LDAP URL 中空格之後的任何資訊。因此在預計作爲參照的任何 LDAP URL 中，您必須改用 `%20`，而不是使用空格。必須忽略其他特殊字元。

定義智慧型參照後，對 `uid=bjensen` 項目的修改實際上會在其他伺服器的 `cn=Babs Jensen` 項目上執行。`ldapmodify` 指令將自動追蹤參照，例如：

```
ldapmodify -h host -p port -D "cn=Directory Manager" -w password
dn:uid=bjensen,ou=People,dc=example,dc=com
changetype:replace
replace:telephoneNumber
telephoneNumber: (408) 555-1234
```

爲了修改智慧型參照，您必須使用 ldapmodify 的 -M 選項，例如：

```
ldapmodify -M -h host -p port -D "cn=Directory Manager" -w password
dn:uid=bjensen,ou=People,dc=example,dc=com
changetype:replace
replace:ref
ref:ldap://east.example.com/cn=Babs%20Jensen,ou=Marketing,
 o=east,dc=example,dc=com
```

# 加密屬性值

屬性加密可以保護儲存在新目錄中的敏感性資料。屬性加密允許您指定以加密格式儲存之項目的特定屬性。這可防止資料於儲存在資料庫檔案、備份資料以及匯出的 LDIF 檔案時被讀取。

屬性值可利用此項功能，在將其儲存於 Directory Server 資料庫前，先行加密，以及在傳回到用戶端前再行解密回原始值。在用戶端和 Directory Server 之間傳送時，您必須使用存取控制項，防止用戶端存取沒有權限的屬性和 SSL 以加密屬性。如需一般資料安全性，特別是屬性加密的結構式概論，請參閱 《Directory Server Deployment Planning Guide》中的 Chapter 7 "Access Control, Authentication, and Encryption"。

只有在伺服器上配置並啓用 SSL 後，才會啓用屬性加密。不過，依據預設並不會加密任何屬性。系統會在尾碼層級中設定屬性加密。這是指將出現在每一個項目之尾碼的屬性加密。如果您想要將整個目錄中的某個屬性加密，必須啓用每一個尾碼中此屬性的加密。

---

**小心**　屬性加密會影響與尾碼相關的所有的資料及索引檔。如果修改現有尾碼的加密組態，您*必須*首先匯出其內容，變更組態，然後再重新匯入內容。主控台將幫助您執行這些步驟。

此外，在開啓加密時，您必須手動刪除可能仍舊包含未加密值的資料庫快取檔案。

您應該在新尾碼中載入或建立資料前，先啓用所有加密的屬性。

---

如果您選擇加密的屬性若會將某些項目當成命名屬性使用，則出現在 DN 中的值將不會加密，但儲存在項目中的值將會加密。

您可以選擇 userPassword 屬性進行加密，但這並沒有實際的安全性效益，除非密碼需以純文字儲存，如 DIGEST-MD5 SASL 驗證一樣。如果密碼策略中已爲密碼設定加密機制，則更進一步的加密所能增加的安全性有限，還會影響每一次連結作業的效能。

在儲存中，加密的屬性以表示使用加密演算法的加密標籤作爲開端。使用 DES 加密演算法的加密屬性會顯示如下：

```
{CKM_DES_CBC}3hakc&jla+=snda%
```

## 使用主控台配置屬性加密

1. 在 Directory Server Console 上選擇 [ 組態 ] 標籤，展開 [ 資料 ] 節點，並選擇您想要加密屬性值的尾碼。選擇右面板中的 [ 屬性加密 ] 標籤。

   此標籤包含一份表格，列出此尾碼目前所有加密屬性的名稱和加密結構。

2. 若要爲屬性啓用加密：

   a. 按一下 [ 加入屬性 ] 按鈕以顯示屬性清單。

   b. 從清單中選擇要加密的屬性，再按一下 [ 確定 ]。屬性會加入表格的 [ 屬性名稱 ] 欄。

   c. 從屬性名稱旁的下拉式清單中，選擇此屬性的 [ 加密結構 ]。

3. 若要使屬性不再加密，請從表格中選擇屬性名稱，再按一下 [ 刪除屬性 ] 按鈕。

4. 按一下 [ 儲存 ]。系統會提示您在變更組態前，先將尾碼內容匯出至 LDIF 檔案。

5. 按一下 [ 匯出尾碼 ] 開啓匯出對話方塊，或按一下 [ 繼續 ]，不需要匯出即可修改屬性加密組態。然後新的組態就會儲存起來。

   如果您尚未匯出尾碼，您必須立即執行此動作以儲存其內容。如果尾碼包含加密的屬性，而且您計劃在下個步驟中使用此 LDIF 檔案重新初始化尾碼，這些屬性在匯出的 LDIF 中可以保持加密狀態。

   現在將出現提示，要您從 LDIF 檔案初始化尾碼。

6. 現在按一下 [ 初始化尾碼 ] 開啓初始化對話方塊，然後再輸入 LDIF 檔案名稱載入目錄。

如果在上個步驟中匯出含加密屬性的尾碼，您現在必須用該檔案初始化，因爲一旦尾碼重新初始化後，加密值將無法回復。在載入及建立索引的同時，指定屬性的所有值都將會加密。

如果您不想在此時初始化尾碼，請按一下 [ 關閉 ]。您可於稍後再使用第 138 頁「匯入資料」中所描述的程序來匯入資料。

7. 如果組態已改爲會加密一或多個屬性，而且這些屬性在匯入作業之前曾經有值，資料庫快取中可能依舊看得到部分未加密的值。若要清除資料庫快取：

   a. 依第 23 頁「啓動和停止 Directory Server」所述停止 Directory Server。

   b. 以 root 或具有管理員權限的身份，將資料庫快取檔案從檔案系統中刪除：

   *ServerRoot*/slapd-*serverID*/db/__db.*

   c. 再次啓動 Directory Server。伺服器將自動建立新的資料庫快取檔案。

## 從指令行配置屬性加密

1. 如果要配置屬性加密的尾碼上有任何項目，您必須先將該尾碼的內容匯出到 LDIF 檔案。如需更多資訊，請參閱第 143 頁「匯出日期」。

   如果尾碼包含加密的屬性，而且您計劃在步驟 5 中使用此 LDIF 檔案重新初始化尾碼，這些屬性在匯出的 LDIF 中可以保持加密狀態。

2. 若要爲屬性啓用加密，請使用 `ldapmodify` 指令加入下列組態項目：

   ```
   ldapmodify -a -h host -p port -D cn=Directory Manager -p password
   dn:cn=attributeName, cn=encrypted attributes, cn=databaseName,
    cn=ldbm database, cn=plugins, cn=config
   objectclass:top
   objectclass:dsAttributeEncryption
   cn: attributeName
   dsEncryptionAlgorithm:cipherName
   ```

   其中 *attributeName* 是要加密的屬性類型名稱，*databaseName* 是對映到尾碼的資料庫符號名稱，而 *cipherName* 是下列其中之一：

   - `ckm_des_cbc` - DES 區塊加密
   - `ckm_des3_cbc` - 三重 DES 區塊加密
   - `ckm_rc2_cbc` - RC2 區塊加密
   - `ckm_rc4` - RC4 資料流加密

3. 若要使屬性不再加密，請使用 `ldapmodify` 指令修改下列組態項目：

```
ldapmodify -h host -p port -D cn=Directory Manager -p password
dn:cn=attributeName, cn=encrypted attributes, cn=databaseName,
 cn=ldbm database, cn=plugins, cn=config
changetype:modify
replace:dsEncryptionAlgorithm
dsEncryptionAlgorithm:clearText
```

其中 *attributeName* 是要加密的屬性類型名稱，而 *databaseName* 是對映到尾碼的資料庫符號名稱。

**備註** 請勿刪除屬性加密組態項目。下次初始化尾碼時會自動移除該項目。

4. 如果組態已改爲會加密一或多個屬性，而且這些屬性在匯入作業之前曾經有值，資料庫快取中可能依舊看得到部分未加密的值。若要清除資料庫快取：
   a. 依第 23 頁 「啓動和停止 Directory Server」所述停止 Directory Server。
   b. 以 root 或具有管理員權限的身份，將資料庫快取檔案從檔案系統中刪除：

      *ServerRoot*/slapd-*serverID*/db/__db.*
   c. 再次啓動 Directory Server。伺服器將自動建立新的資料庫快取檔案。在快取再次填滿之前，此尾碼中的作業效能可能會稍微受到影響。
5. 依第 138 頁 「匯入資料」所述用 LDIF 檔案初始化尾碼。

   在載入檔案及建立對應索引的同時，指定屬性的所有值都將會加密。

## 維護參考的完整性

*參考的完整性*是一種 Plug-in 機制，可確保維護相關項目之間的關係。許多屬性類型 ( 例如群組成員的屬性 ) 中包含另一個項目的 DN。參考的完整性可確保移除項目時，包含其 DN 的所有屬性也會一併移除。

例如，如果移除了目錄的使用者項目，而且已經啓用參考的完整性，則伺服器也會移除使用者爲成員之一之所有群組的使用者。如果沒有啓用參考的完整性，管理員必須手動從群組中移除使用者。如果您將 Directory Server 與其他需要用到使用者與群組管理的 Sun Java System 產品進行整合時，這會是一項重要功能。

# 參考的完整性操作方法

當啓用參考的完整性 Plug-in 時，其會在刪除或重新命名作業之後，立即執行特定屬性上的完整性更新。依據預設，參考的完整性 Plug-in 是停用的。

每當您刪除或重新命名目錄中的使用者或群組項目時，會將作業記錄在參考的完整性日誌檔中：

*ServerRoot*/slapd-*serverID*/logs/referint

經過特定時間 ( 即*更新間隔* ) 後，伺服器會在啓用參考的完整性之所有屬性上執行搜尋，並使搜尋出來的項目與出現在日誌檔中已刪除或已修改項目的 DN 互相符合。如果日誌檔顯示已經刪除項目，則對應的屬性也會刪除。如果日誌檔顯示已經變更項目，則對應的屬性值也會相對地修改。

若啓用參考完整性 Plug-in 的預設組態，每次執行刪除或重新命名作業後，它會立即在 member、uniquemember、owner、seeAlso 和 nsroledn 屬性上執行完整性更新。但是您可以依照您的需要配置參考完整性 Plug-in 的運作方式：

- 在不同檔案中記錄參考的完整性更新。
- 修改更新間隔。如果要減少參考的完整性更新對系統造成的影響，您最好增加更新之間的時間長度。
- 選擇要套用參考的完整性的屬性。如果使用或定義包含 DN 值的屬性，您可能想用參考的完整性 Plug-in 監控它們。

# 配置參考的完整性

使用下列程序可從 Directory Server Console 啓用或停用參考的完整性，以及配置 Plug-in：

## 從主控台上配置參考完整性

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，展開 [Plug-in] 節點，再選擇 [referential integrity postoperation] Plug-in。

   Plug-in 的設定顯示在右面板中。

2. 選擇 [ 啓用 Plug-in] 核取方塊以啓用 Plug-in，清除核取方塊以停用 Plug-in。
3. 設定 [ 引數 1] 的值，以修改更新的間隔秒數。常用的值爲：
   - 0 - 每次作業後立即更新這是預設值。請仔細考慮，每次刪除和修改作業後立即執行參考完整性檢查會對伺服器效能產生顯著的影響。

- 90 - 每 90 秒更新一次
- 3600 - 每 1 小時更新一次
- 10,800 - 每 3 小時更新一次
- 28,800 - 每 8 小時更新一次
- 86,400 - 每天更新一次
- 604,800 - 每周更新一次

依完整性和整體效能的折衷設定正值。

4. 設定 [ 引數 2] 的值，成爲參考完整性日誌檔的絕對路徑。

   [ 引數 3] 用不到，但必須存在。

5. 受參考完整性 Plug-in 監控的屬性由 [引數 4] 開始列起。按一下 [加入] 與 [刪除] 按鈕可管理此清單，及加入您自己的屬性。

| **備註** | 爲獲得最佳效能，由參考完整性 Plug-in 更新的屬性也應該編製索引。如需相關資訊，請參閱第 10 章「編製目錄資料索引」。 |
|---|---|

6. 按一下 [ 儲存 ] 以儲存您的變更。
7. 變更生效前，您必須重新啓動 Directory Server。

## 將參考的完整性用於複製

在複製環境中，存在某些使用參考完整性 Plug-in 的限制：

- 包含主機複本的所有伺服器上都必須啓用。
- 在每部主機上必須用相同的組態啓用。
- 在只包含集線器或用戶複本的伺服器上，啓用此功能並沒有幫助。

若要在複製拓樸中配置參考的完整性 Plug-in：

1. 確定已配置所有複本的組態，而且已定義所有複製協議。
2. 決定將爲其維護參考完整性的屬性組。並決定主機伺服器上所要使用的更新間隔。
3. 使用相同的屬性組及相同的更新間隔啓用所有主機伺服器上的參考完整性 Plug-in。此程序會在第 78 頁「配置參考的完整性」中描述。

4. 請確定所有用戶伺服器上參考的完整性 Plug-in 都是停用的。

### 將參考完整性用於繼承複製

從 4.x 主機向 5.x 使用者複製時，啓用參考完整性，您必須在 4.x 主機上重新配置參考完整性 Plug-in，將參考完整性變更寫入 4.x 變更記錄。此操作使參考完整性變更被複製。*如果沒有重新配置 Plug-in，參考完整性無法正常運作。*

在以下環境中重新配置參考完整性 Plug-in：

1. 停止 4.x 伺服器。
2. 開啓 *ServerRoot*/slapd-*ServerID*/config/ 中的 `slapd.ldbm.conf` 檔案。
3. 尋找以下面句子開始的行

   ```
   plugin postoperation on "referential integrity postoperation"
   ```

4. 透過將屬性清單前的引數由 **0** 變更爲 **1** 來修改此行。

   例如，將

   ```
   plugin postoperation on "referential integrity postoperation"
   "ServerRoot/lib/referint-plugin.dll" referint_postop_init 0
   "ServerRoot/slapd-serverID/logs/referint" 0 "member"
   "uniquemember" "owner" "seeAlso"
   ```

   變更爲

   ```
   plugin postoperation on "referential integrity postoperation"
   "ServerRoot/lib/referint-plugin.dll" referint_postop_init 0
   "ServerRoot/slapd-serverID/logs/referint" 1 "member"
   "uniquemember" "owner" "seeAlso"
   ```

5. 儲存 `slapd.ldbm.conf` 檔案。
6. 重新啓動伺服器。
7. 從 4.x 供應商重新初始化 5.x 使用者。

# 搜尋目錄

您可以使用任何 LDAP 用戶端找出目錄中的項目。大部份用戶端提供某種搜尋介面，讓您搜尋目錄和擷取項目資訊。

在您目錄中設定的存取控制會決定搜尋結果。一般使用者通常不會「看到」目錄的太多內容，而且目錄管理員擁有存取包括組態的所有資料之完整權限。

# 搜尋在 ldapsearch 的目錄

您可以使用 `ldapsearch` 指令行公用程式找出和擷取目錄項目。請注意，本節中描述的 `ldapsearch` 公用程式不是 Solaris 平台提供的公用程式，但是 Directory Server Resource Kit 的一部分。如需有關公用程式的詳細資訊，請參閱《Directory Server Resource Kit Tools Reference》。

此公用程式以指定使用者身份 ( 通常是辨別名稱 ) 和密碼開啓與伺服器的連線，並且根據搜尋篩選器找出項目。搜尋範圍可以包括單一項目、項目的直接子項目、或是整個樹狀目錄或樹狀子目錄。

搜尋以 LDIF 格式傳回的結果。

## ldapsearch 指令行格式

使用 `ldapsearch` 時，您必須使用下列格式輸入指令：

`ldapsearch` [*optional_options*] [*search_filter*] [*optional_list_of_attributes*]

其中

- *optional_options* 代表一系列的指令行選項。必須在搜尋篩選器之前指定這些選項 ( 如果有的話 )。
- *search_filter* 代表第 86 頁「LDAP 搜尋篩選器」中描述的 LDAP 搜尋篩選器。如果您未使用 `-f` 選項在檔案中提供搜尋篩選器，則必須指定搜尋篩選器。
- *optional_list_of_attributes* 代表以空格分隔的屬性清單。指定屬性清單會減少搜尋結果中傳回的屬性數目。此屬性清單必須出現在搜尋篩選器之後。如需範例，請參閱第 85 頁「顯示屬性的子集」。如果您沒有指定屬性清單，則搜尋會傳回目錄中設定的存取控制授與的所有屬性值 ( 操作屬性除外 )。

**備註** 如果想要傳回操作屬性作爲搜尋操作的結果，您必須在搜尋指令中明確地指定它們。若要擷取除了明確指定的操作屬性以外的規則屬性，在 ldapsearch 指令的屬性清單中使用星號 (*)。

## 使用特殊字元

使用 `ldapsearch` 指令行公用程式時，您可能必須指定一些對指令行解譯器具有特殊意義的字元，( 例如空格 [ ]、星號 [*]、反斜線 [\] 等 )。指定特殊字元時，將值置於引號 ( 「 」 ) 內。例如：

```
-D "cn=Charlene Daniels,ou=People,dc=example,dc=com"
```

依指令行解譯器而定，使用單引號或雙引號做此用途。如需詳細資訊，請參閱您的 Shell 說明文件。

## 常用的 ldapsearch 選項

以下列出了最常用的 ldapsearch 指令行選項。如果您指定含有空格 [ ] 的值，值應該置於雙引號之間，例如 -b "ou=groups, dc=example,dc=com"。

-b　指定搜尋的起點。這指定的值必須是目前存在於資料庫中的辨別名稱。如果 LDAP_BASEDN 環境變數已設定爲基礎 DN，則此選項爲可選項。

此選項中指定的值應該置於雙引號中。例如：

```
-b "cn=Charlene Daniels, ou=People, dc=example,dc=com"
```

-D　指定對伺服器進行驗證所使用的辨別名稱。如果您的伺服器支援匿名存取，則此選項爲可選項。如果已指定，則此值必須是 Directory Server 確認的 DN，而且也必須有搜尋項目的權限。例如：

```
-D "uid=cdaniels, dc=example,dc=com"
```

-h　在安裝 Directory Server 的機器上，指定主機名稱或 IP 位址。如果未指定主機，則 ldapsearch 使用 localhost。例如 -h myServer。

-l　指定等待完成搜尋請求的最大秒數。無論在這裏指定何值，ldapsearch 絕不會等候比伺服器 nsslapd-timelimit 屬性所允許的時間更長 ( 持續搜尋除外 )。如需有關持續搜尋的詳細資訊，請參閱《Directory Server Resource Kit Tools Reference》中的 Chapter 3 "ldapsearch"。

例如 -l 300。nsslapd-timelimit 屬性的預設值是 3,600 秒 (1 小時。)

-p　指定 Directory Server 使用的 TCP 連接埠號碼。例如 -p 5201。預設值爲 389，使用 SSL 選項時爲 636。

-s　指定搜尋的範圍。範圍可能是其中之一：

- base - 只搜尋在 -b 選項中指定，或由 LDAP_BASEDN 環境變數定義的項目。
- one - 只搜尋 -b 選項中指定的項目下一層子項。只搜尋子項目，未搜尋 -b 選項中指定的實際項目。
- sub - 搜尋在 -b 選項中指定的項目及其所有的子項。也就是說，在 -b 選項中識別的點開始執行樹狀子目錄搜尋。這是預設值，

-w　指定與在 -D 選項中指定的辨別名稱有關的密碼。如果您沒有指定此選項，則使用匿名存取。例如 -w diner892。

`-x` 指定在伺服器而不是用戶端上排序搜尋結果。如果您想要根據相符規則排序，例如使用國際搜尋等，這個選項很有用。一般而言，在伺服器端排序比在用戶端快，雖然伺服器端排序使用的是伺服器資源。

`-z` 指定回應搜尋要求時要傳回的項目數最大值。例如 `-z 1000`。

一般而言，無論這裏指定何值，`ldapsearch` 絕不會傳回比伺服器的 `nsslapd-sizelimit` 屬性所允許數量還要多的項目。但在使用此指令行引數時，您可以連結爲根 DN 以覆寫此限制。連結爲根 DN 時，此選項預設爲零 (0)。`nsslapd-sizelimit` 屬性的預設值是 2,000 個項目。

如需有關所有 `ldapsearch` 公用程式選項的詳細資訊，請參閱 《Directory Server Resource Kit Tools Reference》。

## ldapsearch 範例

在下一組範例中進行以下假設：

- 您想要在目錄中對所有項目執行搜尋。
- 伺服器位於主機名稱 **`myServer`** 上。
- 伺服器使用連接埠號碼 **`5201`**。
- 以 **`Directory Manager`** 身份鍵入密碼 **`password`** 連結目錄。
- 啓用供連接埠 **`636`** ( 預設 SSL 連接埠號碼 ) 上的伺服器使用的 SSL。
- 在其下儲存所有資料的尾碼是 **`dc=example,dc=com`**。

### 傳回所有項目

假定提供先前資訊，下列呼叫將在目錄中傳回所有項目：

```
ldapsearch -h myServer -p 5201 -D "cn=directory manager" -w password
 -b "dc=example,dc=com" -s sub "(objectclass=*)"
```

`"(objectclass=*)"` 是符合目錄中任何項目的搜尋篩選器。

### 指定指令行上的搜尋篩選器

您可以直接在指令行上指定搜尋篩選器。如果您這樣做，請確定將篩選器放在引號中 (「篩選器」)。同時，請勿指定 `-f` 選項。例如：

```
ldapsearch -h myServer -p 5201 -D "cn=directory manager" -w password
 -b "dc=example,dc=com" "(cn=Charlene Daniels)"
```

## 搜尋根 DSE 項目

根 DSE 是一個特殊項目，含有與目前伺服器實例有關的資訊，例如所支援尾碼、可用驗證機制等的清單。您可以透過提供「」搜尋基礎搜尋此項目。同時，必須指定 base 的搜尋範圍和 "(objectclass=*)" 的篩選器。例如：

```
ldapsearch -h myServer -p 5201 -D "cn=directory manager" -w password
 -b "" -s base "(objectclass=*)"
```

## 搜尋結構項目

Directory Server 將所有目錄伺服器結構儲存在特殊 cn=schema 項目中。此項目含有關於爲您的目錄伺服器定義的每個物件類別和屬性資訊。

您可以按如下方式檢查此項目內容：

```
ldapsearch -h myServer -p 5201 -D "cn=directory manager" -w password
 -b "cn=schema" -s base "(objectclass=*)"
```

**備註** 爲了達到高度的一致性，給定項目的結構次要項目位置由 subschemaSubentry 操作屬性指定。在這一版本的 Directory Server 中，此屬性值始終爲 cn=schema。

## 使用 LDAP_BASEDN

若要使搜尋更容易，您可以使用 LDAP_BASEDN 環境變數設定搜尋基礎。這樣做可讓您省略使用 -b 選項指定搜尋基礎 ( 如需有關設定環境變數的資訊，請參閱作業系統的說明文件 )。

通常會將 LDAP_BASEDN 設定成目錄的尾碼值。由於目錄尾碼和目錄中的根或最上層項目相等，這樣會使所有的搜尋從目錄的根項目開始。

例如，如果已將 LDAP_BASEDN 設定爲 dc=example,dc=com，您可以使用下列的指令行呼叫搜尋 (cn=Charlene Daniels)：

```
ldapsearch -h myServer -p 5201 -D "cn=directory manager" -w password
 "(cn=Charlene Daniels)"
```

在此範例中，使用 sub 的預設範圍，因爲 -s 選項不用於指定範圍。

## 顯示屬性的子集

ldapsearch 指令以 LDIF 格式傳回所有搜尋結果。依預設值，ldapsearch 傳回項目的辨別名稱，以及所有您可以讀取的屬性。您可以設定目錄存取控制，這樣就可以只讀取任何指定目錄項目上的屬性子集。只有操作屬性未傳回。如果想要傳回操作屬性作爲搜尋操作的結果，您必須在搜尋指令中明確地指定它們。如需有關操作屬性的詳細資訊，請參閱 《Directory Server Administration Reference》中的 Chapter 11 "Operational Attributes"。

假設您不想要看到搜尋結果傳回的所有屬性。您可以在搜尋篩選器之後立刻在指令行上指定想要的屬性，將傳回的屬性限制在某些特定的屬性範圍內。例如，若要顯示目錄中每個項目的 cn 和 sn 屬性，請使用以下指令：

```
ldapsearch -h myServer -p 5201 -D "cn=directory manager" -w password
 "(objectclass=*)" sn cn
```

此範例假設您以 LDAP_BASEDN 設定搜尋基礎。

## 搜尋所有多重值屬性

搜尋時，Directory Server 不一定依排序順序傳回多重值屬性。例如，假設您想要搜尋 cn=config 上的組態屬性，在變更生效之前需要重新啓動伺服器。

```
ldapsearch -h myServer -p 5201 -D "cn=directory manager" -w password
 -b cn=config "(objectclass=*)" nsslapd-requiresrestart
```

傳回下列結果：

```
dn:cn=config
nsslapd-requiresrestart:cn=config:nsslapd-port
nsslapd-requiresrestart:cn=config:nsslapd-secureport
nsslapd-requiresrestart:cn=config:nsslapd-plugin
nsslapd-requiresrestart:cn=config:nsslapd-changelogdir
nsslapd-requiresrestart:cn=config:nsslapd-changelogsuffix
nsslapd-requiresrestart:cn=config:nsslapd-changelogmaxentries
nsslapd-requiresrestart:cn=config:nsslapd-changelogmaxage
nsslapd-requiresrestart:cn=config:nsslapd-db-locks
nsslapd-requiresrestart:cn=config:nsslapd-return-exact-case
nsslapd-requiresrestart:cn=config,cn=ldbm database,cn=plugins,
  cn=config:nsslapd-allidsthreshold
nsslapd-requiresrestart:cn=config,cn=ldbm database,cn=plugins,
  cn=config:nsslapd-dbcachesize
nsslapd-requiresrestart:cn=config,cn=ldbm database,cn=plugins,
  cn=config:nsslapd-dbncache
nsslapd-requiresrestart:cn=config,cn=ldbm database,cn=plugins,
  cn=config:nsslapd-directory
nsslapd-requiresrestart:cn=encryption,cn=config:nssslsessiontimeout
nsslapd-requiresrestart:cn=encryption,cn=config:nssslclientauth
```

```
nsslapd-requiresrestart:cn=encryption,cn=config:nssslserverauth
nsslapd-requiresrestart:cn=encryption,cn=config:nsssl2
nsslapd-requiresrestart:cn=encryption,cn=config:nsssl3
...
```

如這裏所示，nsslapd-requiresrestart 屬性有多個值。這些值沒有依排序順序。如果您開發需要多值屬性 ( 按排序順序排列 ) 的應用程式，請確定您的應用程式會執行此排序。

### 搜尋時使用用戶端驗證

此範例顯示使用者 cdaniels 使用用戶端驗證搜尋目錄：

```
ldapsearch -h myServer -p 636 -b "dc=example,dc=com"
 -N  "cdanielsscertname" -Z -W certdbpassword
 -P /home/cdaniels/certdb/cert.db "(givenname=Richard)"
```

## LDAP 搜尋篩選器

搜尋篩選器爲搜尋操作選取要傳回的項目。它們是最常與 ldapsearch 指令行公用程式搭配使用的篩選器。使用 ldapsearch 時，您可以使用檔案分隔行上的每個篩選器，在檔案中放置多重搜尋篩選器，或者可以直接在指令行上指定搜尋篩選器。

例如，下列篩選器指定搜尋一般名稱 Lucie Du Bois：

```
(cn=Lucie Du Bois)
```

此搜尋篩選器傳回所有含一般名稱 Lucie Du Bois 的項目。一般名稱值的搜尋與大小寫無關。

一般名稱屬性有和語言標籤相關的值時，會傳回所有值。因此下列兩個屬性都符合此篩選器：

```
cn:Lucie Du Bois
```

```
cn;lang-fr:Lucie Du Bois
```

### 搜尋篩選器語法

搜尋篩選器的基本語法是：

(*attribute operator value*)

例如：

```
(buildingname>=alpha)
```

在此範例中，buildingname 是屬性，>= 是運算子，而 **alpha** 是值。您也可以定義使用不同屬性與布林運算子組合的篩選器。

下列各節對搜尋篩選器有詳細的描述：

- 使用搜尋篩選器中的屬性
- 使用搜尋篩選器中的運算子
- 使用複合搜尋篩選器
- 搜尋篩選器範例

## 使用搜尋篩選器中的屬性

搜尋項目時，您可以指定與該項目類型有關的屬性。例如，搜尋人員項目時，您可以使用 cn 屬性搜尋有特定一般名稱的人員。

人員項目的屬性範例可能包含：

- cn ( 人員的一般名稱 )
- sn ( 人員的姓氏 )
- telephoneNumber ( 人員的電話號碼 )
- buildingName ( 人員居住的大樓名稱 )
- l ( 人員所在的位置 )

如需列出與項目類型有關的屬性，請參閱 《Directory Server Administration Reference》。

## 使用搜尋篩選器中的運算子

在 表 2-2 中列出了可以在搜尋篩選器中使用的運算子：

**表 2-2** 搜尋篩選運算子

| 搜尋類型 | 運算子 | 描述 |
|---|---|---|
| 相等 | = | 傳回含有完全符合指定值的屬性之項目。例如 cn=Bob Johnson |
| 子字串 | =*string** *string* | 傳回含有指定子字串的屬性之項目。例如：<br>cn=Bob*<br>cn=*Johnson<br>cn=*John*<br>cn=B*John<br>( 星號 (*) 表示零 (0) 或更多字元。) |

**表 2-2** 搜尋篩選運算子 *( 續 )*

| 搜尋類型 | 運算子 | 描述 |
|---|---|---|
| 大於或等於 | >= | 傳回含有大於或等於指定值的屬性之項目。例如：<br>`buildingname >= alpha` |
| 小於或等於 | <= | 傳回含有小於或等於指定值的屬性之項目。例如：<br>`buildingname <= alpha` |
| 存在 | =* | 傳回含有指定屬性的一或多個值之項目。例如：<br>`cn`<br>`telephonenumber=*`<br>`manager=*` |
| 近似 | ~= | 傳回含有指定屬性的項目，該指定屬性擁有的值幾乎相當於搜尋篩選器中指定的值。例如：<br>`cn~=suret`<br>`l~=san fransico`<br>可能傳回<br>`cn=sarette`<br>`l=san francisco`<br>近似運算子是一個實驗性的運算子，而且只能和英語字串一起使用。它不能和非 ASCII 的字串使用，例如 Ja 或 Zn 等。 |

存在延伸搜尋至 dn 屬性 ( 例如 `cn:dn:=John`)，以及提供國際化搜尋支援的延伸運算子。

## 使用複合搜尋篩選器

如下所示，使用字首表示法中表示的布林運算子組合多種搜尋篩選器元件：

(*Boolean-operator* (*filter*) (*filter*) (*filter*) . . . }

其中 *Boolean-operator* 是列在表 2-3 中的任何一個布林運算子。

布林運算子可以組合和巢居在一起以形成複雜運算式，例如：

(*Boolean-operator* (*filter*) (*Boolean-operator* (*filter*) (*filter*) ) )

可以與搜尋篩選器一起使用的布林運算子包括：

**表 2-3** 搜尋篩選布林運算子

| 運算子 | 符號 | 描述 |
|---|---|---|
| AND | & | 要使陳述式爲真，則所有指定的篩選器必須爲真。<br>例如：<br>`(&(filter)(filter)(filter)...)` |
| OR | \| | 要使陳述式爲真，則至少有一個指定的篩選器必須爲真。<br>例如：<br>`(\|(filter)(filter)(filter)...)` |
| NOT | ! | 要使陳述式爲真，則指定的篩選器不能爲真。只有一個篩選器受到 NOT 運算子的影響。例如：<br>`(!(filter))` |

布林運算式的評估順序如下：

- 最內部到最外部的括弧運算式第一優先
- 所有運算式由左到右

## 使用檔案指定搜尋篩選器

您可以將搜尋篩選器輸入檔案，而不是輸入指令行中。這樣做時，在檔案中的分隔行上指定每個搜尋篩選器。`ldapsearch` 指其在檔案中出現的順序執行每一次搜尋。

例如，如果檔案包含：

```
(sn=Daniels)
(givenname=Charlene)
```

然後 `ldapsearch` 先找出所有包含姓氏 Daniels 的項目，然後再找出有指定名稱 Charlene 的所有項目。如果找到都符合這兩個搜尋準則的項目，則傳回項目兩次。

例如，假設您在名爲 `searchdb` 的檔案中指定之前的搜尋篩選器，而且使用 `LDAP_BASEDN` 設定搜尋基礎。下列傳回所有符合任一搜尋篩選器的項目：

```
ldapsearch -h myServer -p 5201 -D "cn=directory manager" -w password
 -f searchdb
```

您可以使用指定想要加入搜尋行末端的屬性名稱以限制傳回的屬性組。例如，下列的 `ldapsearch` 指令兩種搜尋都執行，但是只傳回 DN 和每個項目的 `givenname` 和 `sn` 屬性：

```
ldapsearch -h myServer -p 5201 -D "cn=directory manager" -w password
 -f searchdb sn givenname
```

### 在搜尋篩選器中指定含逗號的 DN

當搜尋篩選器內的 DN 含有作爲值其中一部分的逗點時，您必須以反斜線 (\) 忽略掉該逗號。例如，若要尋找在 example.com Bolivia, S.A. 樹狀子目錄中的每一個人，請使用下列指令：

```
ldapsearch -h myServer -p 5201 -D "cn=directory manager" -w password
-s base -b "o=example.com Bolivia\, S.A.,dc=example,dc=com"
"(objectclass=*)"
```

## 搜尋篩選器範例

下列搜尋項目的篩選器含有管理員屬性的一個或多個值。這也稱爲存在搜尋：

```
(manager=*)
```

下列搜尋項目的篩選器含有共用的名稱 Ray Kultgen。這也稱爲相等搜尋：

```
(cn=Ray Kultgen)
```

下列篩選器傳回所有項目，這些項目包括含有子字串 X.500 的描述屬性：

```
(description=*X.500*)
```

下列篩選器傳回所有組織單位是 Marketing，以及描述欄位不含子字串 X.500 的項目：

```
(&(ou=Marketing)(!(description=*X.500*)))
```

下列篩選器傳回所有組織單位是 Marketing，而且管理員是 Julie Fulmer 或 Cindy Zwaska 的所有項目

```
(&(ou=Marketing)(|(manager=cn=Julie Fulmer,ou=Marketing,
 dc=example,dc=com)(manager=cn=Cindy Zwaska,ou=Marketing,
 dc=example,dc=com)))
```

下列篩選器傳回不代表人員的所有項目：

```
(!(objectClass=person))
```

請注意，之前的篩選器有負面的效能影響，而且應該作爲複雜搜尋的一部分使用。下列篩選器傳回所有不代表人員和一般名稱類似 printer3b 的所有項目：

```
(&(cn~=printer3b)(!(objectClass=person)))
```

### 搜尋操作屬性

如果想要傳回操作屬性作爲搜尋操作的結果，您必須在搜尋指令中明確地指定它們。

```
ldapsearch -h myServer -p 5201 -D "cn=directory manager" -w password
 "(objectclass=*)" aci
```

若要擷取除了明確指定的操作屬性以外的規則屬性，請指定操作屬性除外的「*」。例如：

```
ldapsearch -h myServer -p 5201 -D "cn=directory manager" -w password
 "(objectclass=*)" aci *
```

# 使用 DSMLv2 存取目錄

下列範例指出如何使用 DSML 要求存取和搜尋目錄。如需有關 DSMLv2 標準的 DSML 相關屬性和資訊的完整清單，請參閱《Directory Server Administration Reference》的 Chapter 3 "Frontend Plugin Attributes"。

本節包含下列範例：

- 空匿名 DSML 「Ping」要求
- 作爲特定使用者發出 DSML 連結要求
- DSML 搜尋要求

請注意，這些範例中的 `content-length:` 標頭含有 DSMLv2 要求的精確長度。爲了使這些範例正常運作，請確定您使用的編輯器遵照這些內容長度，或是您可以適當地修改內容長度。

## 空匿名 DSML 「Ping」要求

依預設值停用 *DSML* 前端。如需有關如何啓用它的資訊，請參閱第 39 頁「啓用 DSML 要求」。若要檢查是否啓用 DSML 前端，如 代碼範例 2-1 所示傳送空 DSML 批次要求：

**代碼範例 2-1** 空匿名 DSML 要求

```
POST /dsml HTTP/1.1
content-length: 451
HOST:hostMachine
SOAPAction: ""
Content-Type:text/xml
Connection:close

<?xml version='1.0' encoding='UTF-8'?>
<soap-env:Envelope
   xmlns:xsd='http://www.w3.org/2001/XMLSchema'
   xmlns:xsi='http://www.w3.org/2001/XMLSchema-instance'
   xmlns:soap-env='http://schemas.xmlsoap.org/soap/envelope/'>

   <soap-env:Body>
      <batchRequest
          xmlns='urn:oasis:names:tc:DSML:2:0:core'
          requestID='Ping!'>
          <!-- empty batch request -->
      </batchRequest>
   </soap-env:Body>
</soap-env:Envelope>
```

此 DSML 要求的第一段含有連接很多 HTTP 標頭的 HTTP 方法行 (POST /dsml HTTP/1.1)。HTTP 方法行指定 HTTP 方法要求和 DSML 前端使用的 URL。`POST` 是 DSML 前端接受的唯一 HTTP 方法要求。`/dsml` URL 是 Directory Server 的預設 URL，但可以由任何其他有效的 URL 配置。接著的 HTTP 標頭指定 DSML 要求的剩餘詳細資訊。

- `content-length: 451`
  指定 SOAP/DSML 要求的精確長度
- `HOST: hostMachine`
  指定正在聯絡的主機 Directory Server 名稱。
- `SOAPAction:`
  是強制性的，而且通知目錄您想要在 HTTP/SOAP 堆疊上執行 DSML 要求。但也可能留空。
- `Content-Type: text/xml`
  必須有定義內容爲 XML 的 text/xml 值。
- `Connection: close`
  滿足要求後，指定關閉連線 ( 預設的 HTTP/1.1 運作方式是維持連線開啓。)

要求的其餘部分是 SOAP/DSML 區段。DSML 要求以 XML 前言標頭開始。

```
<?xml version='1.0' encoding='UTF-8'?>
```

這裏指定必須以 UTF-8 字元集編碼的要求。標頭後面接著含有強制加入 XML 結構、XML 結構執行個體和 SOAP 名稱空間的強制範圍和主體元素。

DSML 批次要求元素標記 DSML 批次要求的開始，而且後面隨即接著強制加入 DSMLv2 名稱空間：

```
xmlns='urn:oasis:names:tc:DSML:2:0:core'.
```

由以下的要求 ID 選擇性的識別要求

```
requestID='Ping!'>
```

空批次要求

```
<!-- empty batch request -->
```

以 XML 作註解，而且使用關閉批次要求、關閉 SOAP 主體和關閉 SOAP 範圍元素關閉 SOAP/DSML 批次要求。

如果啓用 DSML 前端，則傳回空的 DSML 回應：

```
HTTP/1.1 200 OK
Cache-control:no-cache
Connection:close
Date:Mon, 09 Sep 2002 13:56:49 GMT
Accept-Ranges:none
Server:Sun-ONE-Directory/5.2
Content-Type:text/xml; charset="utf-8"
Content-Length: 500

<?xml version='1.0' encoding='UTF-8' ?>
<soap-env:Envelope
   xmlns:xsd='http://www.w3.org/2001/XMLSchema'
   xmlns:xsi='http://www.w3.org/2001/XMLSchema-instance'
   xmlns:soap-env='http://schemas.xmlsoap.org/soap/envelope/'
   >
<soap-env:Body>
<batchResponse
   xmlns:xsd='http://www.w3.org/2001/XMLSchema'
   xmlns:xsi='http://www.w3.org/2001/XMLSchema-instance'
   xmlns='urn:oasis:names:tc:DSML:2:0:core'
   requestID='Ping!'
   >
</batchResponse>
</soap-env:Body>
</soap-env:Envelope>
```

如果沒有傳回任何項目，可以推斷前端已經停用。

最大數目限制同時連接至目錄和 DSML 要求的尺寸之用戶端數目。用戶端數目的限制由 `ds-dsml-poolsize` 和 `ds-dsml-poolmaxsize` 屬性指定，要求大小限制由 `ds-dsml-requestmaxsize` 屬性指定。如需有關 DSML 相關屬性的詳細資訊，請參閱《Directory Server Administration Reference》的 Chapter 2 "Frontend Plug-In Attributes"。

## 作爲特定使用者發出 DSML 連結要求

若要發出 DSML 要求，您可以以指定的使用者或匿名身份連結至目錄。若要以指定的使用者身份連結，要求必須包括 HTTP 授權標頭，該標頭含有 uid 和對映 dn 的密碼。

示範的 HTTP 授權要求如下：

```
POST /dsml HTTP/1.1
content-length: 578
Content-Type:text/xml; charset="utf-8"
HOST:hostMachine
Authorization:Basic ZWFzdGVyOmVnZw==
SOAPAction: ""
Connection:close

<?xml version='1.0' encoding='UTF-8'?>
<soap-env:Envelope
   xmlns:xsd='http://www.w3.org/2001/XMLSchema'
   xmlns:xsi='http://www.w3.org/2001/XMLSchema-instance'
   xmlns:soap-env='http://schemas.xmlsoap.org/soap/envelope/'>
   <soap-env:Body>
     <batchRequest
        xmlns='urn:oasis:names:tc:DSML:2:0:core'
        <extendedRequest>
          <requestName>1.3.6.1.4.1.4203.1.11.3</requestName>
        </extendedRequest>
     </batchRequest>
   </soap-env:Body>
</soap-env:Envelope>
```

在此範例中，HTTP 授權標頭傳送 uid 爲 easter 和密碼爲 egg，清晰地以 `easter:egg` 顯示，而且以 base64 編碼成爲 `Authorization:Basic ZWFzdGVyOmVnZw==`。

`<extendedRequest>` 標籤用於指定 LDAP 延伸作業。`<requestName>` 標籤用於指定延伸作業的 OID。在此範例中，OID `1.3.6.1.4.1.4203.1.11.3` 識別 `whoami` 延伸作業。如需有關 `whoami` 延伸作業的詳細資訊，請參閱 http://www.ietf.org/internet-drafts/draft-zeilenga-ldap-authzid-08.txt。

關於匿名存取，匿名存取常有嚴格的存取控制，而且可能有資料存取的限制，但不需要任何 HTTP 授權標頭。同樣地，您可以發出 DSML 要求以 LDAP 代理權執行 LDAP 作業。

因爲 DSML 要求的管理以批次爲基礎，如果您要發行 LDAP 代理權的要求，所需的 DSML 代理驗證要求必須是指定要求批次中的第一個。

# DSML 搜尋要求

代碼範例 2-2 顯示根 DSE 項目上的 DSML 基礎物件搜尋要求。

**代碼範例 2-2** DSML 搜尋要求

```
POST /dsml HTTP/1.1
HOST:hostMachine
Content-Length: 1081
Content-Type:text/xml
SOAPAction: ""
Connection:close

<?xml version='1.0' encoding='UTF-8'?>
<soap-env:Envelope
   xmlns:xsd='http://www.w3.org/2001/XMLSchema'
   xmlns:xsi='http://www.w3.org/2001/XMLSchema-instance'
   xmlns:soap-env='http://schemas.xmlsoap.org/soap/envelope/'
   >
   <soap-env:Body>
      <batchRequest
        xmlns='urn:oasis:names:tc:DSML:2:0:core'
        requestID='Batch of search requests'
        >
        <searchRequest
            dn=""
            requestID="search on Root DSE"
            scope="baseObject"
            derefAliases="neverDerefAliases"
            typesOnly="false"
            >
            <filter>
               <present name="objectClass"/>
            </filter>
            <attributes>
               <attribute name="namingContexts"/>
               <attribute name="supportedLDAPversion"/>
               <attribute name="vendorName"/>
               <attribute name="vendorVersion"/>
               <attribute name="supportedSASLMechanisms"/>
            </attributes>
        </searchRequest>
      </batchRequest>
   </soap-env:Body>
</soap-env:Envelope>
```

在此範例中：

- `dn=""`
  `requestID="search on Root DSE"`
  指定根 DSE 項目下的搜尋作業要求資料 ( 空 DN)，而且由選用的要求 ID 屬性識別。
- `scope="baseObject"`
  指定搜尋是基礎物件搜尋。
- `derefAliases="neverDerefAliases"`
  搜尋或找出搜尋的基礎物件時，指定不應解除參考的別名。這是 Directory Server 支援的唯一 `derefAliases` 值。
- `typesOnly="false"`
  指定要傳回的屬性名稱及其值。`typesOnly="true"` 只傳回屬性名稱。此屬性的預設值爲假。

關於符合篩選器的項目，依下列使用出現的 objectclass 篩選器：

```
<filter>
   <present name="objectClass"/>
</filter>
```

這等同於 LDAP 篩選器字串 (`objectclass=*`)。篩選器後面爲所需屬性清單：

```
<attributes>
   <attribute name="namingContexts"/>
   <attribute name="supportedLDAPversion"/>
   <attribute name="vendorName"/>
   <attribute name="vendorVersion"/>
   <attribute name="supportedSASLMechanisms"/>
</attributes>
```

第 3 章

# 建立和管理樹狀目錄

樹狀目錄包含伺服器的所有項目，並以其辨別名稱 (DN) 作爲識別。由於 DN 爲階層式的架構，架構中會建立分支與分葉，之後便可使用分支與分葉爲樹狀目錄中的資料建立結構。爲了管理樹狀目錄，樹狀目錄在管理上定義爲尾碼、子尾碼、鏈接尾碼。Directory Server Console 提供用於建立與管理所有這些元素的控制項，此外，您也可以使用指令行工具。

如需關於建立目錄資料建構及常用尾碼的概論，請參閱《Directory Server Deployment Planning Guide》的 Chapter 4 "The Directory Information Tree"。

本章包含下列章節：



## 建立尾碼

可以使用 Directory Server Console 或指令行建立根尾碼與子尾碼。

### 使用主控台建立新的根尾碼

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，以滑鼠右鍵按一下 [ 資料 ] 節點，然後在快顯功能表選取 [ 新增尾碼 ]。

   或者，可以選取 [ 資料 ] 節點，再選取 [ 物件 ] 功能表中的 [ 新增尾碼 ]。

顯示 [ 新增尾碼 ] 對話方塊。

2. 在 [ 尾碼 DN] 欄位中輸入唯一的尾碼名稱。名稱必須使用辨別名稱格式，包含以逗點分隔的一或多個屬性值配對。

   在慣例上，根尾碼使用網域 - 元件 (dc) 命名屬性。例如，您可以輸入 `dc=example,dc=org` 作爲新的尾碼 DN。

**備註** 尾碼名稱包含 DN 格式的屬性值配對，不過視爲單一字串。因此，所有的空格都有意義，而且均爲尾碼名稱的一部份。

3. 依預設值，伺服器會自動選擇此尾碼的資料庫檔案位置。此外，依照預設值，尾碼只會維護系統索引，不會對任何屬性加密，而且也不會配置複製。

   若要修改任何預設值，請按一下 [ 選項 ] 按鈕，顯示新的尾碼選項：

   a. 資料庫名稱也是包含資料庫檔案的目錄名稱。預設的資料庫名稱是尾碼 DN 中第一個命名屬性的值，爲了保持此值的唯一性，可能會附加一個數字。若要使用不同的名稱，請選取 [ 使用自訂值 ] 單選按鈕，並輸入新的唯一資料庫名稱。

      資料庫名稱只能包含 ASCII (7 位元 ) 英數字元、連字號 (-) 和底線符號 (_)。例如，可以將新的資料庫命名爲 `example_2`。

   b. 也可以選擇包含資料庫檔案的目錄位置。依預設值，此爲下列路徑的子目錄：

      *ServerRoot*/slapd-*serverID*/db

      請輸入新的路徑，或按一下 [ 瀏覽 ] 尋找資料庫目錄的新位置。新路徑在目錄伺服器主機必須是可存取的。

   c. 爲加速設定新尾碼的組態，可以選擇複製現有的尾碼。選取 [ 複製尾碼組態 ]，並選擇想要從下拉式功能表中複製的尾碼。接著，選取下列任一個要複製的組態：

      - 複製索引組態 - 新的尾碼會與複製尾碼相同的屬性上維護相同的索引。
      - 複製屬性加密組態 - 新的尾碼會啓用與複製尾碼中的屬性清單相同及加密結構相同的加密。
      - 複製複製組態 - 新的尾碼會與複製尾碼的複本類型相同，若爲供應商，則會複製所有的複製協議，而且將啓用複製。

   d. 當配置完所有新尾碼的選項後，請按一下 [ 確定 ]。新增尾碼對話方塊會顯示您選擇的所有選項。

4. 在 [ 新增尾碼 ] 對話方塊中按一下 [ 確定 ]，以建立新的根尾碼。

   根尾碼會自動出現在 [ 資料 ] 分支下。請參閱第 106 頁「管理尾碼」，以進一步配置新的尾碼。

   新的根尾碼不包含任何項目，連尾碼 DN 的項目都沒有。因此，在將它初始化並提供適當的存取權限之前，它在目錄中是無法存取的，而且在主控台 [ 目錄 ] 標籤中也看不見它。

   如果從 LDIF 檔案中初始化尾碼，則可略過其餘步驟。但是，請務必確認 LDIF 檔案中的根項目包含您的部署所需的存取控制指令 (ACI)。

5. 選取主控台最上層的 [ 目錄 ] 標籤。樹狀目錄內尚未顯示新的尾碼。

6. 只有目錄管理員擁有建立尾碼最上方項目的權限。如果不是以目錄管理員身份登入，則選取 [ 主控台 ] > [ 登入爲新使用者 ] 功能表項目。輸入目錄管理員的 DN 和密碼登入。依預設值，目錄管理員的 DN 爲 `cn=Directory Manager`。

7. 在樹狀目錄的根節點 ( 包含伺服器主機名稱與連接埠的節點 ) 上按一下滑鼠右鍵。選取快顯功能表中的 [ 新增根物件 ]，再選取新根尾碼的 DN。

   或者，選取樹狀目錄的根節點，再選擇 [ 物件 ] 功能表中的 [ 新增根物件 ] 項目。

8. 在顯示的 [ 新增物件 ] 對話方塊中，爲根物件選取一個物件類別。此物件類別將決定可加入根項目的其他屬性內容。

   按照慣例，包含 `dc` 命名屬性之尾碼 DN 的根物件屬於 `domain` 物件類別。通常，根物件是簡單物件，而且包含極少的資料。

9. 選好物件類別後，按一下 [ 新增物件 ] 對話方塊中的 [ 確定 ]。

   現在主控台會顯示新根物件的標準編輯器，並自動將預設的 ACI 組加入新物件。如需其他資訊，請參閱第 182 頁「預設 ACI」。加入及編輯拓樸必需的屬性值，包括 ACI 組的所有修改。

10. 項目編輯完成後，按一下 [ 標準編輯器 ] 中的 [ 確定 ]，以建立新尾碼的根物件。

    現在樹狀目錄內會顯示新尾碼，且可以根據 ACI 所授與的權限透過主控台管理新尾碼。

## 使用主控台建立新的子尾碼

下列程序描述如何在已存在的根尾碼或子尾碼下建立新的子尾碼：

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，展開 [ 資料 ] 節點與任何尾碼節點，以顯示父尾碼。
2. 在父尾碼節點上按一下滑鼠右鍵，再選取快顯功能表中的 [ 新增子尾碼 ]。

   或者，您可以選取父尾碼節點，再選擇 [ 物件 ] 功能表中的 [ 新增子尾碼 ]。

   顯示 [ 新增子尾碼 ] 對話方塊。
3. 在 [ 子尾碼 RDN] 欄位中輸入唯一的名稱。名稱必須採用相對辨別名稱格式，包含以逗點分隔的一或多個屬性值配對，例如 `ou=Contractors`。

   文字方塊下一行顯示此子尾碼的完整 DN ( 由 RDN 後附加父尾碼 DN 組成 )。

**備註** 子尾碼名稱包含 RDN 格式的屬性值配對，不過視爲單一字串。因此，所有的空格都有意義，而且均爲尾碼名稱的一部份。

4. 依預設值，伺服器會自動選擇此尾碼的資料庫檔案位置。此外，依照預設值，尾碼只會維護系統索引，不會對任何屬性加密，而且也不會配置複製。

   若要修改任何預設值，請按一下 [ 選項 ] 按鈕，顯示新的尾碼選項：

   a. 資料庫名稱也是包含資料庫檔案的目錄名稱。預設的資料庫名稱是 RDN 中第一個命名屬性的值，爲了保持此值的唯一性，可能會附加一個數字。若要使用不同的名稱，請選取 [ 使用自訂值 ] 單選按鈕，並輸入新的唯一資料庫名稱。

      資料庫名稱只能包含 ASCII (7 位元 ) 英數字元、連字號 (-) 和底線符號 (_)。例如，您可以將新的資料庫命名爲 `temps-US`。

   b. 也可以選擇包含資料庫檔案的目錄位置。依預設值，此爲下列路徑的子目錄：

      *ServerRoot*/`slapd-`*serverID*/`db`

      請輸入新的路徑，或按一下 [ 瀏覽 ] 尋找資料庫目錄的新位置。新路徑必須可被目錄伺服器應用程式存取。

   c. 爲加速設定新子尾碼的組態，可以選擇複製現有的尾碼，不論是其父尾碼或任何其他尾碼皆可。選取 [ 複製尾碼組態 ]，並選擇想要從下拉式功能表中複製的尾碼。接著，選取下列任一個要複製的組態：

      - 複製索引組態 - 新的尾碼會與複製尾碼相同的屬性上維護相同的索引。
      - 複製屬性加密組態 - 新的尾碼會啓用與複製尾碼中的屬性清單相同及加密結構相同的加密。

- 複製複製組態 - 新的尾碼會與複製尾碼的複本類型相同，若爲供應商，則會複製所有的複製協議，而且將啓用複製。

d. 當配置完所有新尾碼的選項後，請按一下 [ 確定 ]。[ 新增子尾碼 ] 對話方塊會顯示您選擇的所有選項。

5. 在 [ 新增子尾碼 ] 對話方塊中按一下 [ 確定 ]，以建立子尾碼。

   子尾碼會自動出現在 [ 組態 ] 標籤中它的父尾碼下。請參閱第 106 頁「管理尾碼」，以進一步配置新的尾碼。

   新的子尾碼不包含任何項目，連 RDN 的項目都沒有。因此，在將它初始化並提供適當的存取權限之前，它在目錄中是無法存取的，而且在主控台 [ 目錄 ] 標籤中也看不見它。

   如果從 LDIF 檔案中初始化尾碼，則可略過其餘步驟。但是，請務必確認 LDIF 檔案中的根項目包含您的部署所需的存取控制指令 (ACI)。

6. 在主控台最上層的 [ 目錄 ] 標籤上，展開樹狀目錄，顯示子尾碼的父層。此時還不會顯示新的子尾碼。

7. 只有目錄管理員擁有建立尾碼和次尾碼 (ACI.) 最上方項目的權限。如果不是以目錄管理員身份登入，則選取 [ 主控台 ] > [ 登入爲新使用者 ] 功能表項目。輸入目錄管理員的 DN 和密碼登入。依預設值，目錄管理員的 DN 爲 `cn=Directory Manager`。

8. 在子尾碼的父層上按一下滑鼠右鍵，再選取快顯功能表中的 [ 新增 ] 項目。在新物件清單中，選取與子尾碼 RDN 對應的物件類型。例如，如果建立 `ou=Contractors` 子尾碼，可選擇 OrganizationalUnit 項目。如果子尾碼的物件類別不在清單中，請選取 [ 其他 ]，並在顯示的 [ 新增物件 ] 對話方塊中選擇該物件類別。或者，選取子尾碼的父層，再選擇 [ 物件 ] 功能表中的 [ 新增 ] 項目。

9. 現在主控台會顯示新物件的自訂或標準編輯器。加入及編輯拓樸必需的屬性值，包括 ACI 組的所有修改。

10. 項目編輯完成後，按一下 [ 編輯器 ] 中的 [ 確定 ]，以建立新子尾碼的項目。

    現在樹狀目錄內會顯示新子尾碼，且可以根據 ACI 所授與的權限透過主控台管理新子尾碼。

## 從指令行建立尾碼

您也可以用 `ldapmodify` 指令行公用程式在您的目錄中建立尾碼。由於伺服器內部是以相同的方式管理根尾碼與子尾碼，因此從指令行建立這兩種尾碼的程序幾乎完全相同。

雖然在下列範例中使用「cn=Directory Manager」，但組態項目可以由任何管理使用者建立。但尾碼的最上方項目*必須*由目錄管理員建立。

1. 用下列指令在 cn=mapping tree,cn=config 下爲根尾碼建立尾碼組態項目：

   ```
   ldapmodify -a -h host -p port -D "cn=Directory Manager" -w password
   dn:cn="suffixDN",cn=mapping tree,cn=config
   objectclass:top
   objectclass:extensibleObject
   objectclass:nsMappingTree
   cn:suffixDN
   nsslapd-state:backend
   nsslapd-backend:databaseName
   ^D
   ```

   對於子尾碼，請用相同的指令，再加上下列屬性：
   `nsslapd-parent-suffix:"parentSuffixDN"`

   *suffixDN* 是新尾碼的完整 DN。對於根尾碼，慣例上是使用網域 - 元件 (dc) 命名屬性，例如 dc=example,dc=org。若是子尾碼，*suffixDN* 包含子尾碼的 RDN 與其父尾碼的 DN，例如 ou=Contractors,dc=example,dc=com。

   *databaseName* 是與此尾碼相關之內部管理資料庫的名稱。在所有尾碼的 *databaseNames* 中，名稱必須是唯一的，而且在慣例上，它是 *suffixDN* 的第一個命名元件值。*databaseName* 也是包含尾碼資料庫檔案的目錄名稱，因此應該只包含 ASCII (7 位元 ) 英數字元、連字號 (-) 與底線符號 (_)。

   若是子尾碼，*parentSuffixDN* 爲父尾碼真正的 DN。

2. 使用下列指令建立資料庫組態項目：

   ```
   ldapmodify -a -h host -p port -D "cn=Directory Manager" -w password
   dn:cn=databaseName,cn=ldbm database,cn=plugins,cn=config
   objectclass:top
   objectclass:extensibleObject
   objectclass:nsBackendInstance
   cn:databaseName
   nsslapd-suffix:suffixDN
   ^D
   ```

   其中 *databaseName* 和 *suffixDN* 必須擁有與先前步驟中所使用的值相同的值。

   將此項目加入目錄後，伺服器的資料庫模組將自動於下列目錄中建立資料庫檔案：

   *ServerRoot*/slapd-*serverID*/db/*databaseName*

   若要讓伺服器在其他位置建立資料庫檔案，請用下列屬性建立資料庫組態項目：

   nsslapd-directory:*path*/*databaseName*

伺服器將在指定的位置，自動建立名爲 *databaseName* 的目錄以儲存資料庫檔案。

3. 建立根尾碼或子尾碼的基礎項目。

   例如，使用下列指令可建立 `dc=example,dc=org` 根尾碼的基礎項目：

```
ldapmodify -a -h host -p port -D "cn=Directory Manager" -w password
dn:dc=example,dc=org
objectclass:top
objectclass:domain
dc:example
^D
```

   您必須包含 DN 的第一個命名屬性及其值，也必須包含基礎項目物件類別之結構所需的所有屬性。依照慣例，使用網域 - 元件 (`dc`) 的根尾碼 DN 擁有 `domain` 物件類別，它不需要其他任何屬性。

   您也應該在根尾碼中加入存取控制指令 (ACI) 屬性，以強制執行存取原則。下列是可加入的 `aci` 屬性值，以允許匿名讀取、安全的自我修改及完整的管理員存取權限：

```
aci:(targetattr != "userPassword") (version 3.0; acl
 "Anonymous access";
 allow (read, search, compare)userdn = "ldap:///anyone";)
aci:(targetattr != "nsroledn || aci || nsLookThroughLimit ||
 nsSizeLimit || nsTimeLimit || nsIdleTimeout ||
 passwordPolicySubentry || passwordExpirationTime ||
 passwordExpWarned || passwordRetryCount || retryCountResetTime
 || accountUnlockTime || passwordHistory ||
 passwordAllowChangeTime")(version 3.0; acl "Allow self entry
 modification except for nsroledn, aci, resource limit
 attributes, passwordPolicySubentry and password policy state
 attributes"; allow (write)userdn ="ldap:///self";)
aci:(targetattr ="*")(version 3.0;acl
 "Configuration Administrator";
 allow (all) userdn = "ldap:///uid=admin,ou=Administrators,
 ou=TopologyManagement, o=NetscapeRoot";)
aci:(targetattr ="*")(version 3.0;acl
 "Configuration Administrators Group";
 allow (all) (groupdn =
 "ldap:///cn=Configuration Administrators, ou=Groups,
 ou=TopologyManagement, o=NetscapeRoot");)
```

   以子尾碼爲例，使用下列指令可建立 `ou=Contractors,dc=example,dc=com` 的基礎項目：

```
ldapmodify -a -h host -p port -D "cn=Directory Manager" -w password
dn:ou=Contractors,dc=example,dc=com
objectclass:top
objectclass:organizationalUnit
description:base of separate subsuffix for contractor identities
^D
```

您必須包含 DN 的命名屬性及其值，也必須包含基礎項目物件類別之結構所需的所有屬性，而且可以加入其他允許的任何屬性。子尾碼擁有其父尾碼上的 ACI 所定義的存取控制，前提是這些 ACI 的範圍必須包含新的子尾碼。若要在子尾碼上定義不同的存取策略，請在建立基礎項目時指定您的 `aci` 屬性。

# 管理尾碼

建立尾碼可讓您同時管理該尾碼的所有內容。本節說明如何管理尾碼的存取，包括停用所有作業、將尾碼設爲唯讀以及建立尾碼層級的參照。

許多其他目錄管理工作是在尾碼層級配置，本書將於其他章節中介紹：

- 第 138 頁「匯入資料」
- 第 143 頁「匯出日期」
- 第 329 頁「管理索引」
- 第 74 頁「加密屬性值」
- 第 261 頁「管理複製」

## 停用或啓用尾碼

有時候，您可能必須將尾碼設爲無法使用以進行維護，或爲了安全性的原因而將其內容設爲無法使用。停用尾碼可讓伺服器無法爲回應嘗試存取該尾碼的任何用戶端作業，而讀取或寫入尾碼內容。如果已定義了預設參照，當用戶端嘗試存取停用的尾碼時，會傳回該參照。

### 使用主控台停用或啓用尾碼

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，展開 [ 資料 ] 節點，再選取要停用的尾碼。
2. 在右面板中，選取 [ 設定值 ] 標籤。依預設值，所有尾碼都會在建立時啓用。

如果已啓用此尾碼的複製功能，則會看到一個說明告訴您此標籤的內容可能自動更新。停用複製的尾碼也會中斷此尾碼的複製作業。只要複製中斷的時間不超過復原設定值，複製機制將在尾碼再度啓用後恢復更新此複本。複製復原設定值是用戶複本的清除延遲與其供應商的變更日誌檔的最大大小及時間 ( 請參閱第 267 頁「進階用戶組態」 )。

3. 取消選取 [ 啓用存取此尾碼 ] 核取方塊可停用尾碼，或選取此核取方塊可將其啓用。
4. 按一下 [ 儲存 ] 可套用變更，並可立即停用或啓用該尾碼。
5. 或者，可設定全域預設參照，此參照在停用的同時，也會針對此尾碼上的所有作業而傳回。此設定值位於最上層 [ 組態 ] 標籤的根節點 [ 網路 ] 標籤上。如需詳細資訊，請參閱第 71 頁「使用主控台設定預設參照」。

### 從指令行停用或啓用尾碼

1. 用下列指令編輯尾碼組態項目中的 `nsslapd-state` 屬性：

```
ldapmodify -h host -p port -D "cn=Directory Manager" -w password
dn:cn="suffixDN",cn=mapping tree,cn=config
changetype:modify
replace:nsslapd-state
nsslapd-state:disabled or backend
^D
```

其中 *suffixDN* 是定義尾碼 DN 時完整的字串，包括任何空格。將 `nsslapd-state` 屬性設定爲值 `disabled` 可停用尾碼，設定爲值 `backend` 可啓用完整存取。

當指令成功時，會立即停用尾碼。

2. 或者，可設定全域預設參照，此參照在停用的同時，也會針對此尾碼上的所有作業而傳回。如需詳細資訊，請參閱第 71 頁「從指令行設定預設參照」。

## 設定存取權限及參照

如果不要完全停用尾碼，只要限制其存取，您可以修改存取權限，以允許唯讀存取。此時，必須爲寫入作業的另一部伺服器定義參照。您也可以拒絕讀取和寫入存取，並爲尾碼上的所有作業定義參照。

參照也可用於將用戶端應用程式暫時指向不同的伺服器。例如，您可以在尾碼中加入參照，使得正在備份尾碼內容時，尾碼會指向不同的伺服器。

複製機制必須依靠寫入權限與參照，才能配置尾碼的複製功能。啓用複製、升級複本或降級複本都會修改參照設定值。

| 小心 | 如果已複製尾碼，修改參照可能會影響此尾碼的複製行爲。 |
|---|---|

## 使用主控台設定存取權限和參照

1. 在 Directory Server 主控台最上層的 [ 組態 ] 標籤上，展開 [ 資料 ] 節點，再選取要設定參照的尾碼。
2. 在右面板中，選取 [ 設定值 ] 標籤。如果啓用鏈接的尾碼，則只能設定權限和參照。如果已啓用此尾碼的複製功能，則會看到一個說明告訴您此標籤的內容可能自動更新。
3. 請選取下列其中一個單選按鈕，設定回覆給此尾碼項目上的任何寫入作業：
   - 處理寫入和讀取要求 - 預設狀態下會選取此單選按鈕，它代表尾碼的正常行爲。系統可能會定義參照，但是不會傳回參照。
   - 處理讀取要求，並傳回寫入要求的參照 - 如果希望將尾碼設爲唯讀，可選取此單選按鈕，並在清單中輸入一或多個 LDAP URL，作爲寫入要求傳回的參照。
   - 傳回讀取和寫入要求的參照 - 如果希望拒絕讀取與寫入存取，可選取此單選按鈕。此行爲與停用尾碼的存取相似，不同處是會特別針對此尾碼定義參照，而不是使用全域預設參照。
4. 使用 [ 加入 ] 與 [ 移除 ] 按鈕編輯參照清單。按一下 [ 加入 ] 按鈕會顯示建立新參照之 LDAP URL 的對話方塊。可對遠端伺服器中任何分支的 DN 建立參照。如需有關 LDAP URL 結構的詳細資訊，請參閱《Directory Server Administration Reference》的 Chapter 6 "LDAR URL Reference"。

   可輸入多個參照。目錄會傳回此清單的所有參照，回應來自用戶端應用程式的要求。
5. 按一下 [ 儲存 ] 可套用您的變更，並且立即開始強制執行新的權限和參照設定值。

## 從指令行設定存取權限和參照

參照是標示的 URL，也就是說 LDAP URL 之後可能接著空白字元和標籤。因爲空白字元很重要，參照的 URL 中的任何空白字元都必須使用 `%20` 加以忽略。

在下列指令中，*suffixDN* 是定義尾碼 DN 時完整的字串，包括任何空格。*LDAPURL* 爲有效的 URL，其中包含主機名稱、連接埠號碼及目標 DN，例如：

```
ldap://phonebook.example.com:389/ou=All%20People,dc=example,dc=com
```

1. 使用下列指令編輯尾碼的組態項目：

   ```
   ldapmodify -h host -p port -D "cn=Directory Manager" -w password
   dn:cn="suffixDN",cn=mapping tree,cn=config
   changetype:modify
   replace:nsslapd-state
   nsslapd-state:referral on update or referral
   -
   add:nsslapd-referral
   nsslapd-referral:LDAPURL
   ^D
   ```

   可重複最後的變更陳述式，將任何數量的 LDAP URL 加入 `nsslapd-referral` 屬性。

   當 nsslapd-state 值爲 `referral on update` 時，該尾碼爲唯讀，而且會傳回所有的 LDAP URL 作爲寫入作業的參照。當值爲 `referral` 時，會拒絕讀取與寫入兩項作業，而且會針對任何要求傳回參照。

2. 尾碼會變成唯讀或無法存取，當指令成功時，會立即準備好傳回參照。

# 刪除尾碼

刪除尾碼將會從目錄中移除它的整個分支。可刪除父尾碼，並在目錄中保留其子尾碼作爲新的根尾碼。

| 小心 | 當您刪除尾碼時，會將它永遠從目錄中完全移除，並移除尾碼的所有組態 ( 包括其複製組態 )。 |
|---|---|

## 使用主控台刪除尾碼

1. 在 Directory Server Console 的 [ 組態 ] 標籤上，展開資料節點。
2. 在想要移除的尾碼上按一下滑鼠右鍵，再選取快顯式功能表中的 [ 刪除 ]。

   或者，可以選取尾碼節點，再選擇 [ 物件 ] 功能表中的 [ 刪除 ]。
3. 顯示確認對話方塊，通知您將從目錄中移除所有尾碼項目。

   除了父尾碼以外，也可以選擇遞迴的刪除所有其子尾碼。如果要移除整個分支，請選取 [ 刪除此尾碼及其所有子尾碼 ]。相反的，如果只要移除特定的尾碼，並在目錄中保留其子尾碼，請選取 [ 僅刪除此尾碼 ]。
4. 按一下 [ 確定 ] 刪除該尾碼。

顯示進度對話方塊，告訴您主控台已經完成步驟。

## 從指令行刪除尾碼

若要從指令行刪除尾碼，請使用 ldapdelete 指令移除目錄中的組態項目。

如果想要刪除包含子尾碼的整個分支，必須尋找已刪除父項的子尾碼，並對每個子尾碼及其可能的子尾碼重複該程序。

1. 使用下列指令移除尾碼組態項目：

   ```
   ldapdelete -h host -p port -D "cn=Directory Manager" -w password
              -v 'cn="suffixDN",cn=mapping tree,cn=config'
   ```

   此指令從位於 *suffixDN* 的基礎項目開始，將尾碼從伺服器中移除。現在此尾碼將不再顯示，也無法在目錄中存取。-v 選項指定詳細輸出模式：顯示其他有關刪除操作的資訊。

2. 移除位於 cn=*databaseName*,cn=ldbm database,cn=plugins,cn=config 中對應的資料庫組態項目，及其下的所有項目。以下的指令使用 ilash 指令達成遞迴刪除。

   ```
   % ilash -call "http://host:port/" -user "cn=Directory Manager"
   [...]
   Enter password for "cn=Directory Manager":password
   [...]
   [example,com]% dcd cn=config
   [config]% ddelete -subtree \
   "cn=databaseName,cn=ldbm database,cn=plugins,cn=config"

   Removed cn=aci, cn=index, cn=databaseName, cn=ldbm database,
   cn=plugins, cn=config

   Removed cn=entrydn, cn=index, cn=databaseName, cn=ldbm database,
   cn=plugins, cn=config

   [...]

   Removed cn=encrypted attributes, cn=databaseName, cn=ldbm database,
   cn=plugins, cn=config

   Removed cn=index, cn=databaseName, cn=ldbm database, cn=plugins,
   cn=config

   Removed cn=monitor, cn=databaseName, cn=ldbm database, cn=plugins,
   cn=config

   Removed cn=databaseName,cn=ldbm database,cn=plugins,cn=config
   ```

此輸出會顯示與資料庫相關且必須移除的所有索引組態項目。完全刪除資料庫組態後，伺服器將移除與此尾碼相關的所有資料庫檔案及目錄。

# 建立鏈接尾碼

根尾碼與子尾碼都可以鏈接到其他伺服器，而且這兩個程序均可透過主控台或從指令行執行。

然而，在建立任何鏈接尾碼時，您應該在遠端伺服器上建立代理身份。本機伺服器在透過鏈接尾碼轉送作業時，會使用代理身份來連結遠端伺服器。

如果您使用完全一樣的參數配置許多鏈接尾碼，您也應該爲新的鏈接尾碼設定鏈接參數的預設值。在建立鏈接尾碼前或後的任何時間，也可以設定 LDAP 控制項與伺服器元件的鏈接策略，如第 122 頁「配置鏈接策略」中所述。

## 建立代理身份

代理身份是遠端伺服器上的一個使用者，本機伺服器將使用它來連結及轉送鏈接作業。基於安全性的原因，目錄管理員或管理使用者 (admin) 絕不應該作爲代理的身份。

而是應建立新的身份，此新身份專用於從指定伺服器執行鏈接作業。此身份應建立在即將鏈接的所有伺服器，以及在第 115 頁「使用主控台建立鏈接尾碼」或第 124 頁「使用主控台修改鏈接策略」中定義的所有容錯移轉伺服器上。代理身份必須有鏈接尾碼的完全存取權。

### 使用主控台建立代理身份

此程序適用於與作爲鏈接尾碼目標的遠端伺服器相連接的 Directory Server Console 上。

1. 在 Directory Server Console 最上層的 [ 目錄 ] 標籤上，展開樹狀目錄。
2. 在 cn=config 項目上按一下滑鼠右鍵，再選取快顯功能表中的 [ 新增 ] > [ 使用者 ] 。或者，選取 cn=config 項目，再選擇 [ 物件 ] 功能表中 [ 新增 ] > [ 使用者 ] 項目。
3. 在 [ 建立新使用者 ] 對話方塊的欄位中填入值，以描述代理身份，例如：

   | | |
   |---|---|
   | 名字： | `proxy` |
   | 姓氏： | *host1* |
   | 一般名稱： | *host1* `chaining proxy` |
   | 使用者 ID： | *host1*`_proxy` |
   | 密碼： | *password* |
   | 確認密碼： | *password* |

   其中 *host1* 是包含鏈接尾碼的伺服器名稱。每一部有尾碼鏈接至此伺服器的伺服器都應該使用不同的代理身份。

4. 按一下 [ 確定 ] 以儲存此新的代理身份。

### 從指令行建立代理身份

此程序使用 *host1* 與 *host2* 分別代表包含鏈接尾碼的本機伺服器及作爲鏈接尾碼目標的遠端伺服器。

1. 使用下列指令在 *host2* 上建立代理身份：

```
ldapmodify -a -h host2 -p port2 -D "cn=Directory Manager" -w password2
dn:uid=host1_proxy,cn=config
objectclass:top
objectclass:person
objectclass:organizationalPerson
objectclass:inetorgperson
uid:host1_proxy
cn:host1 chaining proxy
sn:host1
userpassword:password
description:proxy entry to be used for chaining from host1
^D
```

**小心** 您應該透過加密連接埠執行 `ldapmodify` 指令，以避免傳送純文字的密碼。

## 設定預設鏈接參數

鏈接參數會決定伺服器與鏈接伺服器的連線方式，以及伺服器在該鏈接尾碼上處理作業的方式。這些參數是在每個鏈接尾碼上配置。Directory Server 提供了每次建立鏈接尾碼時所用的預設值。您可以編輯這些預設值，以指定所有新鏈接尾碼上的鏈接參數。

每一個在修改預設參數後新建立的鏈接尾碼，都將使用您指定的值。然而，一旦建立尾碼之後，便只能依第 121 頁「管理鏈接尾碼」所述方式修改參數。

鏈接參數的屬性與預設值說明如下。如需允許值的描述，請參閱《Directory Server Administration Reference》的 Chapter 2 "Chained Suffix Plug-in Attributes"：

### 用戶端傳回參數

- `nsReferralOnScopedSearch` - 使用預設的開啓設定時，搜尋範圍完全在鏈接尾碼內的用戶端將收到遠端伺服器的參照。如此便可避免將搜尋結果傳送二次。當設爲關閉時，應該設定大小與時間限制參數，以避免在鏈接尾碼上執行冗長的搜尋。

- `nsslapd-sizelimit` - 此參數會決定在回應鏈接搜尋作業時將會傳回的項目數。預設大小限制爲 2000 個項目。如果想要限制涉及鏈接尾碼的廣泛搜尋，請將此參數設定爲低值。在任何情況下，遠端伺服器上所有的大小設定值均會限制該作業。

- `nsslapd-timelimit` - 此參數控制鏈接作業的時間長度。預設時間限制爲 3600 秒 (1 個小時 )。如果想要限制允許在鏈接尾碼上作業的時間，請將此參數設定爲低值。在任何情況下，遠端伺服器上所有的時間設定值均會限制該作業。

### 階層式鏈接參數

- `nsCheckLocalACI` - 在單一階層鏈接中，本機伺服器不會在鏈接尾碼上檢查連結使用者的存取權限，因爲那是遠端伺服器的責任。因此，預設值是 `off`。然而，階層式鏈接內的中介伺服器必須將此參數設成 `on`，才能夠檢查及限制轉送鏈接作業的伺服器所用之代理 DN 的存取權限。

- `nsHopLimit` - 迴圈偵測必須依靠此參數來定義允許的最大躍點數。系統不會轉送任何達到此躍點數的鏈接作業，而是在階層式拓樸中有意外迴圈的假設之下，將此作業放棄。

### 連線管理參數

- `nsOperationConnectionsLimit` - 鏈接尾碼可同時與遠端伺服器建立之 LDAP 作業連線數的最大值。預設值爲 10 個連線。

- `nsBindConnectionsLimit` - 鏈接尾碼可同時與遠端伺服器建立之連結連線數的最大值。預設值爲 3 個連線。

- `nsConcurrentBindLimit` - 每個 LDAP 連線同時連結作業數的最大值。預設值爲每個連線有 10 個未執行連結作業。

- `nsBindRetryLimit` - 與遠端伺服器連結失敗後，鏈接尾碼嘗試重新連結的次數。0 值代表鏈接的尾碼只會嘗試連結一次。預設值爲嘗試 3 次。

- `nsConcurrentOperationsLimit` - 每個 LDAP 連線同時作業數的最大值。預設值爲每個連線有 10 個作業。

- `nsBindTimeout` - 與鏈接尾碼的連結嘗試逾時之前的時間長度 ( 以秒爲單位 )。預設值爲 15 秒。

- nsAbandonedSearchCheckInterval - 伺服器檢查作業是否已被放棄之前的秒數。預設值爲 2 秒。
- nsConnectionLife - 鏈接尾碼與遠端伺服器之間的連線維持開啓，以便可以重複使用的時間長度。維持連線開啓會較爲快速，但會使用較多的資源。例如，如果您正使用撥接連線，您可能會想要限制連線的時間。預設值爲 0，表示連線沒有限制。

### 錯誤偵測參數

- nsmaxresponsedelay - 遠端伺服器爲回應鏈接作業的 LDAP 要求初始化可花費時間的最大值。此期間會以秒爲單位。在此延遲之後，本機伺服器會測試連線。預設延遲期間爲 60 秒。
- nsmaxtestresponsedelay - 檢查遠端伺服器是否有回應的測試持續時間。測試內容只是簡單地要求搜尋一個不存在的項目。此期間會以秒爲單位。如果在測試延遲期間內收不到回應，鏈接尾碼會假設遠端伺服器已關閉。預設的測試回應延遲期間爲 15 秒。

  如果您只爲此鏈接尾碼定義一部遠端伺服器，遠端伺服器的所有鏈接作業都將封鎖 30 秒，以防止負載過重。如果已定義容錯移轉伺服器，則鏈接作業將開始使用下一個定義的替代伺服器。

### 使用主控台設定預設鏈接參數

1. 在 Directory Server 主控台最上層的 [ 目錄 ] 標籤上，展開樹狀目錄，並選取下列項目：`cn=default instance config,cn=chaining database,cn=plugins,cn=config`。
2. 連按兩下此項目，或選取 [ 物件 ] > [ 以標準編輯器編輯 ] 功能表項目。修改上述清單中需要的屬性值。
3. 按一下 [ 標準編輯器 ] 對話方塊中的 [ 儲存 ]，變更將會立即生效。

### 從指令行設定預設鏈接參數

1. 使用 `ldapmodify` 指令編輯 `cn=default instance config,cn=chaining database,cn=plugins,cn=config` 項目。此項目的所有屬性成爲新鏈接尾碼中參數的預設值。

   例如，下列指令會將新鏈接尾碼中的預設大小限制提高到 5000 個項目，並將預設時間限制降低爲 10 分鐘：

   ```
   ldapmodify -h host -p port -D "cn=Directory Manager" -w password
   dn:cn=default instance config,cn=chaining database,
    cn=plugins,cn=config
   changetype:modify
   ```

```
replace:nsslapd-sizelimit
nsslapd-sizelimit: 5000
-
replace:nsslapd-timelimit
nsslapd-timelimit: 600
^D
```

對此項目的修改將立即生效。

## 使用主控台建立鏈接尾碼

下列程序幾乎與建立鏈接根尾碼和鏈接子尾碼的方式完全一樣：

1. 選擇 Directory Server Console 的 [ 組態 ] 標籤。
   - 若是鏈接根尾碼，在 [ 資料 ] 節點上按一下滑鼠右鍵，再選取快顯功能表中的 [ 新增鏈接的尾碼 ]。或者，可以選取 [ 資料 ] 節點，再選擇 [ 物件 ] 功能表中的 [ 新增鏈接的尾碼 ]。
   - 若是鏈接子尾碼，展開 [ 資料 ] 節點與任何尾碼節點，以顯示父尾碼。在父尾碼節點上按一下滑鼠右鍵，再選取快顯功能表中的 [ 新增鏈接的子尾碼 ]。或者，可以選取父尾碼節點，再選擇 [ 物件 ] 功能表中的 [ 新增鏈接的子尾碼 ]。

     顯示 [ 新增鏈接的 ( 子 ) 尾碼 ] 對話方塊。
2. 輸入要鏈接的遠端伺服器上項目的 DN。遠端項目不一定要是遠端尾碼的基礎項目：
   - 若是根尾碼，在 [ 尾碼 DN] 欄位中輸入遠端項目的完整 DN。可以輸入遠端樹狀目錄中項目的任何 DN。該項目將是鏈接根尾碼的基礎，而且該項目底下的任何項目均可透過鏈接尾碼取得。
   - 若是子尾碼，輸入即將鏈接之項目的子尾碼 RDN。該項目是鏈接子尾碼的基礎。顯示在文字欄位下的完整子尾碼名稱必須是存在於遠端伺服器上的項目。
3. 輸入包含尾碼資料的遠端伺服器主機名稱 ( 必要時包含網域 )。
4. 輸入存取遠端伺服器的連接埠號碼，如果這是安全連接埠，也請選取該核取方塊。使用安全連接埠時，鏈接作業會透過 SSL 加密。如需詳細資訊，請參閱第 121 頁「使用 SSL 進行鏈接」。

   對話方塊下方的文字會顯示遠端伺服器的完整 URL。

5. 輸入遠端伺服器上代理身份的連結 DN 與密碼。在遠端伺服器上存取尾碼內容時，本機伺服器會使用此 DN 作爲代理。例如，使用第 111 頁「建立代理身份」中定義的 `uid=`*host1*`_proxy,cn=config` DN。

   您無法使用遠端伺服器上目錄管理員的 DN。透過鏈接尾碼執行的作業將在 `creatorsName` 與 `modifiersName` 屬性中使用此代理身份。可以不使用代理 DN，如此一來，本機伺服器在存取遠端伺服器時將以匿名方式連結。

6. 按一下 [ 確定 ] 以建立鏈接尾碼。新尾碼會出現在組態樹狀目錄中，並包含鏈接的圖示。

7. 按一下新的鏈接尾碼以選取之，並選取右面板中的 [ 遠端伺服器 ] 標籤。

8. 可以選擇性地爲此鏈接尾碼定義一或多部容錯移轉伺服器。如果伺服器無法聯絡遠端伺服器，它會依定義的順序逐一嘗試容錯移轉伺服器，直到其中一部伺服器回應爲止。容錯移轉伺服器必須包含與被鏈接尾碼相同的尾碼，而且允許相同的連結 DN 作爲代理。

   若要定義容錯移轉伺服器，請在 [ 遠端伺服器 URL] 欄位中輸入更多配對的主機名稱與連接埠號碼，並以空格分隔。此欄位的格式如下：

   ```
   ldap[s]://hostname[:port][ hostname[:port]].../
   ```

9. 在 [ 遠端伺服器 ] 標籤底端，文字方塊會顯示允許透過鏈接執行代理作業所需的 ACI。必須將此 ACI 加入遠端伺服器上包含 *suffixDN* 的項目。如果您曾經定義任何容錯移轉伺服器，便應該將此 ACI 加入所有容錯移轉伺服器。使用 [ 複製 ACI] 按鈕可將 ACI 文字複製到您用來貼上的系統剪貼簿。

   將此 ACI 加入遠端伺服器上的基礎項目後，鏈接尾碼便會顯示在本機伺服器的樹狀目錄中。

---

小心　　您可能需要在同一個項目上定義其他 ACI，以限制存取目前透過鏈接公開的遠端伺服器。請參閱第 120 頁「透過鏈接尾碼的存取控制」。

---

10. 如果已經配置伺服器元件的鏈接策略，則必須也加入允許這些元件存取遠端伺服器的 ACI。例如，如果允許鏈接參考完整性 Plug-in ，則必須將下列 ACI 加入步驟 2中所指定之 DN 的基礎項目：

    ```
    aci:(targetattr "*")
     (target="ldap:///suffixDN")
     (version 3.0; acl "RefInt Access for chaining"; allow
     (read,write,search,compare) userdn = "ldap:///cn=referential
     integrity postoperation,cn=plugins,cn=config";)
    ```

# 從指令行建立鏈接尾碼

也可以用 ldapmodify 指令行公用程式在您的目錄中建立鏈接尾碼。由於伺服器內部是以相同的方式管理鏈接根尾碼與鏈接子尾碼，因此從指令行建立這兩種尾碼的程序幾乎完全相同。

1. 對於鏈接根尾碼，使用下列指令在 cn=mapping tree,cn=config 下建立鏈接尾碼項目：

   ```
   ldapmodify -a -h host -p port -D "cn=Directory Manager" -w password
   dn:cn=suffixDN,cn=mapping tree,cn=config
   objectclass:top
   objectclass:extensibleObject
   objectclass:nsMappingTree
   cn:suffixDN
   nsslapd-state:backend
   nsslapd-backend:databaseName
   ^D
   ```

   對於鏈接子尾碼，請使用相同的指令，再加上下列屬性：
   `nsslapd-parent-suffix:`*parentSuffixDN*

   若是鏈接子尾碼，*suffixDN* 是子尾碼的 RDN，及其父尾碼的 DN，例如 l=Europe,dc=example,dc=com。*suffixDN* 必須是可透過遠端伺服器取得之項目的 DN，但不一定要是遠端尾碼的基礎項目。

   尾碼名稱爲 DN 格式，不過視爲單一字串。因此，所有的空格都有意義，而且均爲尾碼名稱的一部份。爲了讓伺服器能夠存取遠端項目，*suffixDN* 字串必須遵照遠端尾碼中所使用相同的空格用法。

   *databaseName* 由鏈接 Plug-in 元件用以識別此鏈接尾碼。在所有尾碼的 *databaseNames* 中，名稱必須是唯一的，而且在慣例上，它是 *suffixDN* 的第一個命名元件值。鏈接尾碼與本機尾碼不同，鏈接尾碼在本機伺服器上沒有任何資料庫檔案。

   若是子尾碼，*parentSuffixDN* 爲父尾碼真正的 DN。父尾碼可以是本機尾碼或鏈接尾碼。

2. 使用下列指令建立鏈接組態項目：

   ```
   ldapmodify -a -h host -p port -D "cn=Directory Manager" -w password
   dn:cn=databaseName,cn=chaining database,cn=plugins,cn=config
   objectclass:top
   objectclass:extensibleObject
   objectclass:nsBackendInstance
   cn:databaseName
   nsslapd-suffix:suffixDN
   ```

```
nsfarmserverurl:LDAPURL
nsmultiplexorbinddn:proxyDN
nsmultiplexorcredentials:ProxyPassword
^D
```

其中 *databaseName* 和 *suffixDN* 必須擁有與先前步驟中所使用的值相同的值。*LDAPURL* 是遠端伺服器的 URL，但不包括任何尾碼資訊。URL 可以包含以下列格式列示的容錯移轉伺服器：

```
ldap[s]://hostname[:port][ hostname[:port]].../
```

LDAP URL 中所列的所有遠端伺服器都必須包含 *suffixDN*。如需關於指定安全連接埠的資訊，請參閱第 121 頁「使用 SSL 進行鏈接」。

*proxyDN* 是遠端伺服器上代理身份的 DN。在遠端伺服器上存取尾碼內容時，本機伺服器會使用此 DN 作爲代理。透過鏈接尾碼執行的作業將在 `creatorsName` 與 `modifiersName` 屬性中使用此代理身份。如果沒有指定代理 DN，當存取遠端伺服器時，本機伺服器會匿名連結。

*ProxyPassword* 是代理 DN 密碼的非加密值。當密碼儲存在組態檔時，系統會將密碼加密。例如：

```
nsmultiplexorbinddn:uid=host1_proxy,cn=config
nsmultiplexorcredentials:secret
```

**小心** 您應該透過加密連接埠執行 `ldapmodify` 指令，以避免傳送純文字的密碼。

新項目會自動包含所有鏈接參數，與在 `cn=default instance config,cn=chaining database,cn=plugins,cn=config` 中定義的預設值。您可以在建立鏈接組態項目時使用不同的值設定參數，以覆寫任何預設值。如需可定義值的屬性清單，請參閱第 112 頁「設定預設鏈接參數」。

3. 使用下列指令在遠端項目上建立 ACI。必須有此 ACI 才能透過鏈接執行代理作業。如需關於 ACI 的詳細資訊，請參閱 「第 6 章「管理存取控制」」。

```
ldapmodify -h host2 -p port2 -D "cn=Directory Manager" -w password2
dn:suffixDN
changetype:modify
add:aci
aci:(targetattr=*)(target = "ldap:///suffixDN")(version 3.0;acl
 "Allows use of admin for chaining"; allow (proxy)
 (userdn="ldap:///proxyDN");)
^D
```

**小心** 您可能需要在同一個項目上定義其他 ACI，以限制存取目前透過此伺服器公開的遠端伺服器。請參閱第 120 頁「透過鏈接尾碼的存取控制」。

4. 如果已經配置伺服器元件的鏈接策略，則必須也加入允許這些元件存取遠端伺服器的 ACI。例如，如果允許鏈接參考完整性 Plug-in，則必須將下列 ACI 加入包含 *suffixDN* 的基礎項目：

```
aci:(targetattr "*")
 (target="ldap:///suffixDN")
 (version 3.0; acl "RefInt Access for chaining"; allow
 (read,write,search,compare) userdn = "ldap:///cn=referential
 integrity postoperation,cn=plugins,cn=config";)
```

下列指令爲建立鏈接子尾碼的範例。請注意，只有當 DN 的命名屬性中出現逗點時，suffixDN 中的逗點才必須用反斜線 (\) 忽略掉。

```
ldapmodify -a -h host1 -p port1 -D "cn=Directory Manager" -w password1
dn:cn=l=Europe\,dc=example\,dc=com,cn=mapping tree,cn=config
objectclass:top
objectclass:extensibleObject
objectclass:nsMappingTree
cn:l=Europe,dc=example,dc=com
nsslapd-state:backend
nsslapd-backend:Europe
nsslapd-parent-suffix:dc=example,dc=com

dn:cn=Europe,cn=chaining database,cn=plugins,cn=config
objectclass:top
objectclass:extensibleObject
objectclass:nsBackendInstance
cn:Europe
nsslapd-suffix:l=Europe,dc=example,dc=com
nsfarmserverurl:ldap://host2:port2/
nsmultiplexorbinddn:uid=host1_proxy,cn=config
nsmultiplexorcredentials:proxyPassword
^D

ldapmodify -h host2 -p port2 -D "cn=Directory Manager" -w password2
dn:l=Europe,dc=example,dc=com
changetype:modify
changetype:modify
aci:(targetattr=*)(target =
```

```
 "ldap:///l=Europe,dc=example,dc=com")(version 3.0;acl
 "Allows use of admin for chaining"; allow (proxy)
 (userdn="ldap:///uid=host1_proxy,cn=config");)
^D
```

## 透過鏈接尾碼的存取控制

當驗證使用者存取鏈接尾碼時，伺服器會傳送使用者的身份給遠端伺服器。存取控制總是在遠端伺服器上評估。在遠端伺服器上評估的每一個 LDAP 作業都使用用戶端應用程式原始身份，此身份是透過代理驗證控制項所傳送。只有當使用者對遠端伺服器上包含的樹狀子目錄擁有正確的存取控制時，在遠端伺服器上的作業才會成功。這表示，您必須將一般的存取控制加入到遠端伺服器上，並加上一些限制：

- 您無法使用所有類型的存取控制。

  例如，以角色或篩選器爲基礎的 ACI 需要存取使用者項目。由於您是經由鏈接尾碼存取資料，因此只能驗證代理控制中的資料。所以在設計目錄時，應考慮到要確保使用者項目與使用者的資料位應在同一個尾碼中。

- 所有以用戶端的 IP 位址或 DNS 網域爲基礎的存取控制可能沒有作用，因爲用戶端的原始網域會在鏈接過程中遺失。

  遠端伺服器視用戶端應用程式所使用的 IP 位址與鏈接尾碼相同，且視用戶端應用程式是在相同的 DNS 網域中。

下列限制適用於爲了使用鏈接尾碼而建立的 ACI：

- ACI 必須與其使用的群組位在同一部伺服器上。如果是動態群組，群組中的所有使用者都必須位在 ACI 與群組內；如果是靜態群組，則可以參考遠端使用者。

- ACI 必須與其使用的任何 role 定義位在同一伺服器上，並與計劃擁有這些角色的任何使用者在一起。

- 如果使用者在遠端，參考使用者項目值的 ACI ( 例如 `userattr` 對象規則 ) 會有作用。

雖然存取控制總是在遠端伺服器上評估，但您也可以選擇讓它們在包含鏈接尾碼的伺服器與遠端伺服器上都進行評估。這會有幾項限制：

- 在存取控制評估期間，使用者項目的內容未必可供使用 ( 例如，如果在包含鏈接尾碼的伺服器上評估存取控制，而項目位在遠端伺服器上 )。

  基於效能的原因，用戶端無法執行遠端查詢及評估存取控制。

- 鏈接尾碼未必有權可存取被用戶端應用程式修改的項目。

在執行修改作業時，鏈接尾碼無法存取儲存在遠端伺服器上的完整項目。如果要執行刪除作業，鏈接尾碼只會知道項目的 DN。如果存取控制指定特定屬性，則透過鏈接尾碼進行的刪除作業將會失敗。

依預設值，不會評估在包含鏈接尾碼的伺服器上設定的存取控制。若要覆寫此預設值，請使用 `cn=`*databaseName*`,cn=chaining database,cn=plugins,cn=config` 項目中的 `nsCheckLocalACI` 屬性。除非使用階層式鏈接，否則並不建議在包含鏈接尾碼的伺服器上評估存取控制。如需詳細資訊，請參閱第 133 頁「配置串級鏈接」。

## 使用 SSL 進行鏈接

您可以配置伺服器在鏈接尾碼上執行作業時，會使用 SSL 與遠端伺服器進行通訊。在鏈接中使用 SSL 需要下列步驟：

1. 在遠端伺服器上啓用 SSL。
2. 在包含鏈接尾碼的伺服器上啓用 SSL。

   如需關於啓用 SSL 的詳細資訊，請參閱第 11 章「管理驗證和加密」。
3. 在建立或修改鏈接尾碼的程序中，指定遠端伺服器的 SSL 與安全連接埠。

   使用主控台時，在鏈接尾碼建立或組態程序中選取安全連接埠的核取方塊。請參閱第 115 頁「使用主控台建立鏈接尾碼」或第 124 頁「使用主控台修改鏈接策略」。

   使用指令行程序時，指定遠端伺服器的 LDAPS URL 與安全連接埠，例如：`ldaps://example.com:636/`。請參閱第 117 頁「從指令行建立鏈接尾碼」或第 125 頁「從指令行修改鏈接策略」。

當您配置鏈接尾碼與遠端伺服器使用 SSL 進行通訊時，並不表示執行該作業要求的用戶端應用程式也必須使用 SSL 進行通訊。用戶端可能使用 LDAP 或 DSML 通訊協定的連接埠。

# 管理鏈接尾碼

本節說明更新與刪除現有鏈接尾碼的方式，以及控制鏈接機制的方式。

# 配置鏈接策略

伺服器的鏈接策略會決定哪些 LDAP 控制項將會傳給鏈接伺服器，允許哪些伺服器元件存取鏈接尾碼。您應該知道這些設定值及其對涉及鏈接尾碼的作業有何影響。鏈接策略適用於伺服器上的所有鏈接尾碼。

預設的設定值是要讓正常作業能夠透明地完成。然而，如果您的作業涉及 LDAP 控制項，或您使用如參考完整性 Plug-in 這一類的伺服器元件時，您應該確定鏈接策略是依據您的需要所配置的。

鏈接策略的配置最好是在建立任何鏈接尾碼之前進行，則在一啓用鏈接尾碼時，便會立即套用該策略。但之後您也可以隨時修改策略。

## LDAP 控制項的鏈接策略

用戶端會將 LDAP 控制項當成要求的一部分來傳送，以便能使用某種方式修改作業或其結果。伺服器鏈接策略可決定伺服器會連同作業一併轉送給鏈接尾碼的控制項。依預設值，會轉送下列控制項給鏈接尾碼的遠端伺服器：

**表 3-1** 預設允許鏈接的 LDAP 控制項

| 控制項 OID | 控制項的名稱和描述 |
|---|---|
| 1.2.840.113556.1.4.473 | 伺服器端排序 - 與搜尋相關聯，會依據項目的屬性值將產生的項目排序。[1] |
| 1.3.6.1.4.1.1466.29539.12 | 鏈接迴圈偵測 - 追蹤伺服器與另一部伺服器鏈接的次數。當計數到到達配置的數字時，便會放棄作業，並通知用戶端應用程式。如需詳細資訊，請參閱第 135 頁「傳送階層式的 LDAP 控制項」。 |
| 2.16.840.1.113730.3.4.2 | 智慧型參照的受管理 DSA - 將智慧型參照當成項目傳回，而不追蹤參照。這讓您能夠變更或刪除智慧型參照本身。 |
| 2.16.840.1.113730.3.4.9 | 虛擬清單檢視 (VLV) - 提供搜尋的部分結果，而不一次傳回所有產生的項目。[1] |

1. 只有當搜尋範圍是單一尾碼時，才支援透過鏈接來使用伺服器端排序與 VLV 控制項。當用戶端應用程式對多個尾碼提出要求時，鏈接尾碼無法支援 VLV 控制項。

下表列出可以藉由配置鏈接策略而允許鏈接的其他 LDAP 控制項：

**表 3-2** 可鏈接的 LDAP 控制項

| 控制項 OID | 控制項的名稱和描述 |
|---|---|
| 1.3.6.1.4.1.42.2.27.9.5.2 | 取得有效權利要求 - 要求伺服器傳回與結果中的項目及屬性相關的存取權限與 ACI 資訊。 |

**表 3-2** 可鏈接的 LDAP 控制項 ( *續* )

| 控制項 OID | 控制項的名稱和描述 |
|---|---|
| 2.16.840.1.113730.3.4.12 | 受代理的驗證 ( 舊規格 ) - 允許用戶端在要求持續期間內承擔另一個身份。[1] |
| 2.16.840.1.113730.3.4.14 | 搜尋特定資料庫 - 用於搜尋作業，以指定必須在控制項所指名的資料庫上完成搜尋。 |
| 2.16.840.1.113730.3.4.16 | 驗證要求 - 提供一個連結要求，以要求伺服器在連結回應中提供憑證。 |
| 2.16.840.1.113730.3.4.17 | 僅限於真實屬性的要求 - 表示伺服器只應傳回真正包含於傳回項目內且不必解析虛擬屬性的屬性。 |
| 2.16.840.1.113730.3.4.18 | 受代理的驗證 ( 新規格 ) - 允許用戶端在要求持續期間內承擔另一個身份。[1] |
| 2.16.840.1.113730.3.4.19 | 僅限於虛擬屬性的要求 - 表示伺服器只應傳回由角色或服務類別功能所產生的屬性。 |

1. 應用程式可對受代理的驗證使用任一種控制項。這些 OID 應該採用相同的鏈接策略。如需詳細資訊，請參閱第 135 頁「傳送階層式的 LDAP 控制項」。

## 伺服器元件的鏈接策略

元件是指使用內部作業的任何伺服器功能或功能單位。例如，Plug-in 被視爲元件。爲執行元件的工作，大部分元件必須存取目錄內容 ( 如組態資料或儲存在目錄中的使用者資料 )。

依預設值，任何伺服器元件都不允許鏈接。如果要元件存取鏈接尾碼，您必須明確允許鏈接。可存取鏈接資料的元件依其 DN 列示於下。

如第 115 頁「使用主控台建立鏈接尾碼」中所述，必須在遠端伺服器上的 ACI 中授與某些權限，以允許鏈接。當鏈接伺服器元件時，必須在此 ACI 中允許搜尋、讀取與比較，使伺服器元件可以執行這些作業。不僅如此，某些元件還需要遠端伺服器的寫入權限，如清單中的說明：

- `cn=ACL Plugin,cn=plugins,cn=config` - ACI Plug-in 實行存取控制功能。用來擷取與更新 ACI 屬性的作業不會鏈接，因爲將本機與遠端 ACI 屬性混在一起非常不安全。但是，用來存取使用者項目的要求可以鏈接。如需關於與 ACI 及鏈接之限制相關的進一步資訊，請參閱第 182 頁「ACI 限制」。
- `cn=old plugin,cn=plugins,cn=config` - 此 Plug-in 代表所有 Directory Server 4.x Plug-in ，以及是否允許它們鏈接。4.x Plug-in 共用同一個鏈接策略。依 4.x Plug-in 所執行作業的不同，您可能必須在遠端伺服器上設定 ACI。

- `cn=resource limits,cn=components,cn=config` - 此元件根據使用者的連結 DN 設定資源使用限制。當允許鏈接此元件時，可以對其身份儲存在鏈接尾碼中的使用者強制執行資源限制。
- `cn=certificate-based authentication,cn=components,cn=config` - 此元件用於使用 SASL 外部連結方法時，它會從遠端伺服器擷取使用者憑證。

**小心** 若允許從鏈接尾碼進行以憑證爲基礎的驗證，可能會造成安全上的漏洞。如果其他尾碼鏈接到不受信任的遠端伺服器，便可以使用不受信任之伺服器上的憑證進行驗證。

- `cn=referential integrity postoperation,cn=plugins,cn=config` - 此 Plug-in 確保項目的移除會傳給其他可能參考其 DN 的項目，例如群組成員清單。當群組成員位在鏈接尾碼時，將此 Plug-in 用於鏈接上有助於簡化靜態群組的管理。當此 Plug-in 存取鏈接尾碼時，它需要有遠端伺服器的寫入權限。
- `cn=uid uniqueness,cn=plugins,cn=config` - UID 唯一性 Plug-in 會確保指定屬性的所有新值在伺服器上是唯一的。允許鏈接此 Plug-in 將確保整個樹狀目錄的唯一性。

**備註** 下列元件不得鏈接：

- 角色 Plug-in
- 密碼策略元件
- 複製 Plug-in

## 使用主控台修改鏈接策略

1. 在 Directory Server Console 的 [ 組態 ] 標籤上，選取 [ 資料 ] 節點，並在右面板中選取 [ 鏈接 ] 標籤。
2. 從右邊的清單中選取一或多個 LDAP 控制項，再按一下 [ 加入 ] 以允許鏈接。使用 [ 加入 ] 與 [ 刪除 ] 按鈕，建立允許鏈接的控制項清單。

   LDAP 控制項依其 OID 列示。如需每個控制項的名稱與描述，請參閱第 122 頁「LDAP 控制項的鏈接策略」。
3. 允許鏈接的伺服器元件會列在同一標籤下方。請從右邊的清單中選取一或多個元件名稱，再按一下 [ 加入 ] 以允許鏈接。使用 [ 加入 ] 與 [ 刪除 ] 按鈕，建立允許鏈接的元件清單。

   如需每個元件的描述，請參閱第 123 頁 「伺服器元件的鏈接策略」。

4. 按一下 [ 儲存 ] 以儲存鏈接策略。
5. 重新啓動伺服器，使變更生效。

### 從指令行修改鏈接策略

`cn=config,cn=chaining database,cn=plugins,cn=config` 項目包含鏈接策略組態的屬性。使用 `ldapmodify` 指令可編輯此項目：

1. 修改多重值的 `nsTransmittedControls` 屬性，使它包含允許鏈接之所有 LDAP 控制項的 OID。如需可鏈接的所有控制項 OID，請參閱第 122 頁「LDAP 控制項的鏈接策略」。

   例如，下列指令在鏈接控制項清單中加入有效權限控制項：

   ```
   ldapmodify -h host -p port -D "cn=Directory Manager" -w password
   dn:cn=config,cn=chaining database,cn=plugins,cn=config
   changetype:modify
   add:nsTransmittedControls
   nsTransmittedControls: 1.3.6.1.4.1.42.2.27.9.5.2
   ^D
   ```

   如果用戶端應用程式使用自訂控制項，而且您希望允許它們鏈接，您也可以將其 OID 加入 `nsTransmittedControls` 屬性。

2. 修改多重值的 `nsActiveChainingComponents` 屬性，使它包含允許鏈接之所有伺服器元件的 DN。如需每個元件的描述，請參閱第 123 頁「伺服器元件的鏈接策略」。

   例如，下列指令在鏈接元件清單中加入參考完整性元件：

   ```
   ldapmodify -h host -p port -D "cn=Directory Manager" -w password
   dn:cn=config,cn=chaining database,cn=plugins,cn=config
   changetype:modify
   add:nsActiveChainingComponents
   nsActiveChainingComponents:cn=referential integrity
    postoperation,cn=components,cn=config
   ^D
   ```

3. 修改鏈接策略組態項目後，必須重新啓動伺服器使變更生效。

## 停用或啓用鏈接尾碼

有時候爲了進行維護，或基於安全性的原因，可能必須將尾碼設爲無法使用。停用尾碼可阻止伺服器爲回應嘗試存取該尾碼的任何用戶端作業，而聯絡遠端伺服器。如果已定義了預設參照，當用戶端嘗試存取停用的尾碼時，會傳回該參照。

### 使用主控台停用或啓用鏈接尾碼

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，展開 [ 資料 ] 節點，再選取要停用的鏈接尾碼。
2. 在右面板中，選取 [ 設定值 ] 標籤。依預設值，所有鏈接尾碼都會在建立時啓用。
3. 取消選取 [ 啓用存取此尾碼 ] 核取方塊可停用尾碼，或選取此核取方塊可將其啓用。
4. 按一下 [ 儲存 ] 可套用變更，並可立即停用或啓用該尾碼。
5. 或者，可設定全域預設參照，此參照在停用的同時，也會針對此尾碼上的所有作業而傳回。此設定值位於最上層 [ 組態 ] 標籤的根節點 [ 網路 ] 標籤上。如需詳細資訊，請參閱第 71 頁「使用主控台設定預設參照」。

### 從指令行停用或啓用尾碼

1. 用下列指令編輯鏈接尾碼項目中的 `nsslapd-state` 屬性：

   ```
   ldapmodify -h host -p port -D "cn=Directory Manager" -w password
   dn:cn=suffixDN,cn=mapping tree,cn=config
   changetype:modify
   replace:nsslapd-state
   nsslapd-state:disabled or backend
   ^D
   ```

   其中 *suffixDN* 是定義尾碼 DN 時完整的字串，包括任何空格或反斜線 (\) 以忽略掉值中的逗點。將 `nsslapd-state` 屬性設定爲值 `disabled` 可停用尾碼，設定爲值 `backend` 可啓用完整存取。

   當指令成功時，會立即停用尾碼。

2. 或者，可設定全域預設參照，此參照在停用的同時，也會針對此尾碼上的所有作業而傳回。如需詳細資訊，請參閱第 71 頁「從指令行設定預設參照」。

## 設定存取權限及參照

如果不要完全停用鏈接尾碼，只要限制其存取，您可以修改存取權限，以允許唯讀存取。此時，必須爲寫入作業的另一部伺服器定義參照。您也可以拒絕讀取和寫入存取，並爲尾碼上的所有作業定義參照。

如需更多關於參照的一般性資訊，請參閱 《Directory Server Deployment Planning Guide》的 Chapter 5 "Distribution, Chaining, and Referrals"。

### 使用主控台設定存取權限和參照

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，展開 [ 資料 ] 節點，再選取要設定參照的鏈接尾碼。
2. 在右面板中，選取 [ 設定值 ] 標籤。如果啓用鏈接的尾碼，則只能設定權限和參照。
3. 請選取下列其中一個單選按鈕，設定回覆給此尾碼項目上的任何寫入作業：
   - 處理寫入和讀取要求 - 預設狀態下會選取此單選按鈕，它代表正常的行爲。系統會將讀取與寫入作業轉送給遠端伺服器，而將結果傳回用戶端。系統可能會定義參照，但是不會傳回參照至用戶端。
   - 處理讀取要求，並傳回寫入要求的參照 - 伺服器將只轉送讀取要求，並將結果傳回給用戶端。請在清單中輸入一個或多個 LDAP URL，作爲寫入要求傳回的參照。
   - 傳回讀取和寫入要求的參照 - 在清單中輸入一個或多個 LDAP URL，作爲所有作業傳回的參照。此行爲與停用尾碼的存取相似，不同處是會特別針對此尾碼定義參照，而不是使用全域預設參照。
4. 使用 [ 加入 ] 與 [ 移除 ] 按鈕編輯參照清單。按一下 [ 加入 ] 按鈕會顯示建立新參照之 LDAP URL 的對話方塊。可對遠端伺服器中任何分支的 DN 建立參照。如需有關 LDAP URL 結構的詳細資訊，請參閱 《Directory Server Administration Reference》的 Chapter 6 "LDAR URL Reference "。

   可輸入多個參照。目錄會傳回此清單的所有參照，回應來自用戶端應用程式的要求。
5. 按一下 [ 儲存 ] 可套用您的變更，並且立即開始強制執行新的權限和參照設定值。

### 使用主控台設定存取權限和參照

在下列指令中，*suffixDN* 是定義鏈接尾碼時完整的字串，包括任何空格。*LDAPURL* 爲有效的 URL，其中包含主機名稱、連接埠號碼及目標 DN，例如：

```
ldap://alternate.example.com:389/ou=People,dc=example,dc=com
```

1. 使用下列指令編輯鏈接尾碼項目：

```
ldapmodify -h host -p port -D "cn=Directory Manager" -w password
dn:cn=suffixDN,cn=mapping tree,cn=config
changetype:modify
replace:nsslapd-state
nsslapd-state:referral on update 或 referral
```

```
-
add:nsslapd-referral
nsslapd-referral:LDAPURL
^D
```

可重複最後的變更陳述式，將任何數量的 LDAP URL 加入 `nsslapd-referral` 屬性。

當 nsslapd-state 值爲 `referral on update` 時，該尾碼爲唯讀，而且會傳回所有的 LDAP URL 作爲寫入作業的參照。當值爲 `referral` 時，會拒絕讀取與寫入兩項作業，而且會針對任何要求傳回參照。

2. 尾碼會變成唯讀或無法存取，當指令成功時，會立即準備好傳回參照。

# 修改鏈接參數

定義鏈接尾碼後，您可以修改控制鏈接的參數。可以指定如何存取遠端伺服器、變更代理所用的 DN 或甚至變更遠端伺服器。您也可以修改效能參數，以控制伺服器建立與維護鏈接伺服器連線的方式。

## 使用主控台修改鏈接參數

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，展開 [ 資料 ] 節點，再選取要修改的鏈接尾碼。
2. 在右面板中，選取 [ 遠端伺服器 ] 標籤。
3. 若要變更遠端伺服器的名稱或連接埠，請修改 [ 遠端伺服器 URL] 欄位。URL 包含一或多個遠端伺服器的主機名稱與選用連接埠號碼，並採用下列格式：

   `ldap[s]://`*hostname*`[:`*port*`][ `*hostname*`[:`*port*`]].../`

   URL 不包含任何尾碼資訊。如需關於指定安全連接埠的資訊，請參閱第 121 頁「使用 SSL 進行鏈接」。當第一部伺服器無法回應鏈接尾碼時，會依照列示的順序來聯絡 URL 中的伺服器。LDAP URL 中所列示的所有遠端伺服器都必須包含 *suffixDN*，其爲鏈接尾碼的基礎項目。

4. 若要變更代理使用者的 DN，請在 [ 連結 DN] 欄位中輸入新值。在密碼欄位中輸入與確認此 DN 對應的密碼。

   *proxyDN* 是遠端伺服器上使用者的 DN。在遠端伺服器上存取尾碼內容時，本機伺服器會使用此 DN 作爲代理。透過鏈接尾碼執行的作業將在 `creatorsName` 與 `modifiersName` 屬性中使用此代理身份。如果沒有指定代理 DN，當存取遠端伺服器時，本機伺服器會匿名連結。

5. 標籤底端的文字方塊顯示允許此尾碼鏈接所需的 ACI。如果變更過遠端伺服器的 URL，您必須在新的遠端伺服器 ( 一台或多台 ) 上包含 *suffixDN* 的項目中加入此 ACI。如果修改過代理 DN，您應該更新所有鏈接伺服器上的 ACI。使用 [ 複製 ACI] 按鈕可將 ACI 文字複製到您用來貼上的系統剪貼簿。

6. 選取 [ 限制與控制項 ] 標籤，以配置鏈接要求的參數。階層式鏈接參數會於第 133 頁「配置串級鏈接」中說明。

7. 設定 [ 控制用戶端傳回 ] 參數以限制鏈接作業的大小與時間：

   - 領域搜尋傳回參照 - 範圍完全在鏈接尾碼內的搜尋是沒有效率的，因爲會傳送結果兩次。依預設值，伺服器將改爲傳回鏈接伺服器的參照，強迫用戶端直接在鏈接伺服器上執行搜尋。如果取消選取此選項，您應該設定下列參數，以限制即將鏈接的結果大小。
   - 大小限制或無大小限制 - 此參數會決定在回應鏈接搜尋作業時會傳回的項目數。預設大小限制爲 2000 個項目。如果想要限制涉及鏈接尾碼的廣泛搜尋，請將此參數設定爲低值。在任何情況下，遠端伺服器上所有的大小設定值均會限制該作業。
   - 時間限制或無時間限制 - 此參數控制鏈接作業的時間長度。預設時間限制爲 3600 秒 (1 個小時 )。如果想要限制允許在鏈接尾碼上作業的時間，請將此參數設定爲低值。在任何情況下，遠端伺服器上所有的時間設定值均會限制該作業。

8. 設定 [ 連線管理 ] 參數以控制伺服器如何管理網路連線，以及與遠端伺服器的連結：

   - 最大 LDAP 連線數。鏈接尾碼可同時與遠端伺服器建立之 LDAP 作業連線數的最大值。預設值是連線 10 次。
   - 最大連結連線數。鏈接尾碼可同時與遠端伺服器建立之連結連線數的最大值。預設值是連線 3 次。
   - 每次連線最大連結數。每個 LDAP 連線同時連結作業數的最大值。預設值爲每個連線有 10 個未執行連結作業。
   - 最大連結重試數。與遠端伺服器連結失敗後，鏈接尾碼將嘗試重新連結的次數。0 值代表鏈接的尾碼只會嘗試連結一次。預設值是嘗試 3 次。
   - 每次連線最大作業數。每個 LDAP 連線同時作業數的最大值。預設值爲每個連線有 10 個作業。
   - 連結逾時或無連結逾時。與鏈接尾碼的連結嘗試逾時之前的時間長度 ( 以秒爲單位 )。預設值爲 15 秒。
   - 放棄前逾時或無逾時。伺服器檢查作業是否已被放棄之前的秒數。預設值爲 2 秒。

- 連線存留時間或無限制。鏈接尾碼與遠端伺服器之間的連線維持開啓，以便可以重複使用的時間長度。維持連線開啓會較爲快速，但會使用較多的資源。例如，如果您正使用撥接連線，您可能會想要限制連線的時間。預設值爲連線沒有限制。

透過主控台無法設定錯誤偵測參數。請參閱第 130 頁 「從指令行修改鏈接參數」。

9. 完成設定鏈接參數後按一下 [ 儲存 ]。

## 從指令行修改鏈接參數

從指令行，您不僅可以設定使用主控台時所設定的參數，還可以配置第 114 頁 「錯誤偵測參數」中所述的其他參數：

1. 使用下列指令編輯要修改之尾碼對應的鏈接組態項目：

```
ldapmodify -h host -p port -D "cn=Directory Manager" -w password
dn:cn=databaseName,cn=chaining database,cn=plugins,cn=config
changetype:modify
replace:attributeName
attributeName:attributeValue
-
replace:attributeName2
attributeName2:attributeValue2
...
^D
```

可能的屬性名稱與值將於下列步驟中說明。可以在指令中包含數個變更陳述式，以便能夠一次變更任何數目的參數。

2. 修改 `nsfarmserverURL` 屬性可變更遠端伺服器的名稱或連接埠。其值是 URL，其中包含一或多個遠端伺服器的主機名稱與選用連接埠，並採用下列格式：

```
ldap[s]://hostname[:port][ hostname[:port]]...
```

URL 不包含任何尾碼資訊。如需關於指定安全連接埠的資訊，請參閱第 121 頁 「使用 SSL 進行鏈接」。當第一部伺服器無法回應鏈接尾碼時，會依照列示的順序來聯絡 URL 中的伺服器。LDAP URL 中所列示的所有遠端伺服器都必須包含 *suffixDN*，其爲鏈接尾碼的基礎項目。

3. 修改 `nsmultiplexorBindDN` 與 `nsmultiplexorCredentials` 屬性可變更代理存取遠端伺服器時所用的 DN。

在遠端伺服器上存取尾碼內容時，本機伺服器會使用此 DN 作爲代理。透過鏈接尾碼執行的作業將在 `creatorsName` 與 `modifiersName` 屬性中使用此代理身份。如果沒有指定代理 DN，當存取遠端伺服器時，本機伺服器會匿名連結。

4. 如果修改代理 DN 或其憑證，則必須在遠端伺服器上建立對應的 ACI。系統必須有此 ACI 才能透過鏈接執行代理作業：

```
ldapmodify -h host2 -p port2 -D "cn=Directory Manager" -w password2
dn:suffixDN
changetype:modify
add:aci
aci:(targetattr=*)(target = "ldap:///suffixDN")(version 3.0;acl
 "Allows use of admin for chaining"; allow (proxy)
 (userdn="ldap:///proxyDN");)
^D
```

5. 設定第 112 頁「設定預設鏈接參數」中所述的任何屬性，以控制遠端伺服器上連線與作業的處理方式。階層式參數將進一步於第 133 頁「配置串級鏈接」中說明。

# 最佳化執行緒用法

也可以設定伺服器全域使用的執行緒數目，以考慮鏈接所用的執行緒資源。由於鏈接作業必須轉送到遠端伺服器，因此作業所需的時間可能長很多，但是當遠端伺服器正在處理作業時其執行緒會保持閒置。如果您的鏈接伺服器有相當長的延遲，您應該提高執行緒數目，以便能夠同時處理更多的本機作業。

依預設值，伺服器所用的執行緒數目是 30，但是在使用鏈接尾碼時，您可以提高處理作業可用的執行緒數目，以改善效能。您需要的執行緒數目須視鏈接尾碼數、在鏈接尾碼上的作業數目與類型，以及於遠端伺服器上處理作業所需的平均時間而定。

一般而言，每一個鏈接尾碼應增加 5 到 10 個執行緒，這是假設在鏈接尾碼上執行的作業數與本機尾碼一樣。

## 使用主控台設定執行緒資源

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，按一下 [ 效能 ] 節點，並在右面板中選取 [ 其他 ] 標籤。
2. 爲 [ 執行緒的最大數量 ] 欄位輸入新值。
3. 按一下 [ 確定 ] 以儲存變更，並確認您必須重新啓動伺服器後變更才會生效的訊息。
4. 重新啓動目錄伺服器以使用執行緒的新號碼。

### 從指令行設定執行緒資源

1. 使用下列指令編輯全域組態項目，以修改執行緒數目：

```
ldapmodify -h host -p port -D "cn=Directory Manager" -w password
dn:cn=config
changetype:modify
replace:nsslapd-threadnumber
nsslapd-threadnumber:newThreadNumber
^D
```

2. 重新啓動目錄伺服器以使用執行緒的新號碼。

## 刪除鏈接尾碼

刪除鏈接尾碼後，會使得該鏈接尾碼無法透過本機樹狀目錄存取，但不會刪除鏈接伺服器上的項目或尾碼。可刪除父尾碼，並在目錄中保留其子尾碼作爲新的根尾碼。

### 使用主控台刪除鏈接尾碼

1. 在 Directory Server Console 的 [ 組態 ] 標籤上，展開 [ 資料 ] 節點。
2. 在想要移除的尾碼上按一下滑鼠右鍵，再選取快顯式功能表中的 [ 刪除 ]。

   或者，可以選取尾碼節點，再選擇 [ 物件 ] 功能表中的 [ 刪除 ]。
3. 顯示確認對話方塊，通知您可透過此鏈接尾碼存取的項目*不會*從遠端目錄中移除。

   除了父尾碼以外，也可以選擇遞迴的刪除所有其子尾碼。如果要移除整個分支，請選取 [ 刪除此尾碼及其所有子尾碼 ]。相反的，如果只要移除特定的尾碼，並在目錄中保留其子尾碼，請選取 [ 僅刪除此尾碼 ]。
4. 按一下 [ 確定 ] 刪除該尾碼。

   顯示進度對話方塊，告訴您主控台已經完成步驟。

### 從指令行刪除尾碼

若要從指令行刪除尾碼，請使用 `ldapdelete` 指令移除目錄中的組態項目。

如果想要刪除包含子尾碼的整個分支，必須尋找已刪除父項的子尾碼，並對每個子尾碼及其可能的子尾碼重複該程序。

1. 使用下列指令移除尾碼組態項目：

   ```
   ldapdelete -h host -p port -D "cn=Directory Manager" -w password
   cn=suffixDN,cn=mapping tree,cn=config
   ```

   此指令會使鏈接尾碼及其遠端項目不再顯示在目錄中。

2. 移除位在 `cn=databaseName,cn=chaining database,cn=plugins,cn=config` 中對應的資料庫組態項目，及其下的監控項目：

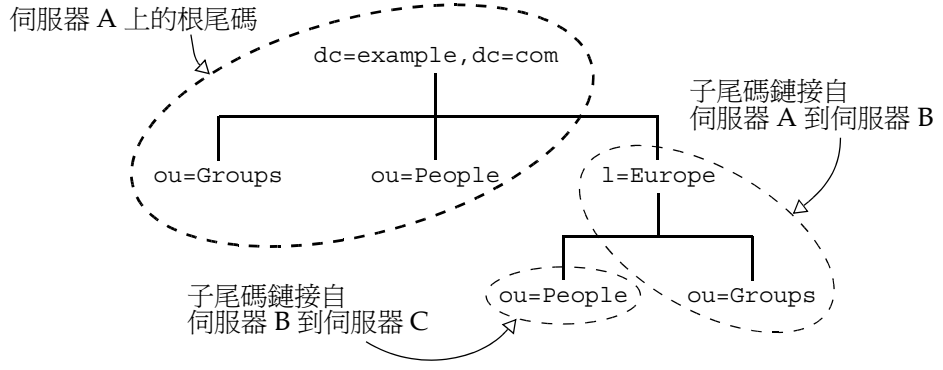
   ```
   ldapdelete -h 主機 -p 連接埠 -D "cn=Directory Manager" -w 密碼
   cn=monitor,cn=dbName,cn=chaining database,cn=plugins,cn=config
   cn=dbName,cn=chaining database,cn=plugins,cn=config
   ```

# 配置串級鏈接

在階層式鏈接中，與一部伺服器鏈接的樹狀子目錄本身可以是鏈接尾碼或包含鏈接子尾碼。當作業涉及一部伺服器中的鏈接尾碼時，系統會將此作業轉送到中介伺服器，該伺服器會聯絡第三部伺服器，依此類推。在存取樹狀目錄中的所有資料時，若需要經過伺服器之間一次以上的躍點，便會發生階層式鏈接。

例如，下圖顯示存取 `ou=People,l=Europe,dc=example,dc=com` 項目時是如何從伺服器 A 鏈接到伺服器 B，最後再到伺服器 C。伺服器 A 包含根尾碼 `dc=example,dc=com`，以及連到伺服器 B 上 `l=Europe,dc=example,dc=com` 分支的鏈接子尾碼。伺服器 B 包含 `l=Europe,dc=example,dc=com` 項目，但 `ou=People,l=Europe,dc=example,dc=com` 分支是連到伺服器 C 的鏈接子尾碼。伺服器 C 則實際包含 `ou=People,l=Europe,dc=example,dc=com` 項目

**圖 3-1** 有三部伺服器的階層式鏈接



# 設定階層式參數

有兩個鏈接參數可配置階層式作業：

- 所有伺服器都應配置迴圈偵測，以便能夠偵測到鏈接拓樸中任何意外的迴圈。如果未啓用迴圈偵測，迴圈中的伺服器將一再循環轉送作業，直到超過負載爲止。
- 所有中介鏈接尾碼都應設配置爲會評估本機 ACI，通常這不是在第一層的鏈接尾碼上執行的。

## 使用主控台設定階層式參數

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，展開 [ 資料 ] 節點，再選取要修改的鏈接尾碼。
2. 在右面板中，選取 [ 限制與控制項 ] 標籤，此處可修改 [ 階層式鏈接 ] 參數。
3. 在階層式鏈接的所有中介伺服器上，選取該核取方塊以檢查本機 ACI。

   在單一階層鏈接期間，不會選取此核取方塊，因爲使用者的存取權限不會在第一部伺服器上評估，而是在透過代理的第二部伺服器上進行。但是，在階層式鏈接的中介伺服器上，您必須啓用 ACI 檢查，以允許執行存取控制，之後再將作業轉送。
4. 在階層式鏈接的所有伺服器上，設定您的拓樸中所有鏈接作業允許的最大躍點數。同一個作業每轉送到另一個鏈接尾碼就算一次躍點，如果到達限制，鏈接尾碼將不再轉送該作業。

   您所設定的數目應該大於階層式鏈接最長的躍點數。任何達到限制的作業都會中止，因爲伺服器會假設這是拓樸中意外的迴圈。

   也必須設定鏈接組態以允許迴圈偵測控制，如第 135 頁「傳送階層式的 LDAP 控制項」中所述。
5. 完成設定階層式參數後，按一下 [ 儲存 ]。

### 從指令行設定階層式參數

1. 在所有中介伺服器上，使用下列指令編輯鏈接尾碼的鏈接組態項目：

   ```
   ldapmodify -h host -p port -D "cn=Directory Manager" -w password
   dn:cn=databaseName,cn=chaining database,cn=plugins,cn=config
   changetype:modify
   replace:nsCheckLocalACI
   nsCheckLocalACI:on
   -
   changetype:modify
   replace:nsHopLimit
   nsHopLimit:maximumHops
   ^D
   ```

   您應該將 *maximumHops* 設爲大於階層式鏈接中最長的躍點數。任何達到限制的作業都會中止，因爲伺服器會假設這是拓樸中意外的迴圈。也必須設定鏈接組態以允許迴圈偵測控制，如第 135 頁「傳送階層式的 LDAP 控制項」中所述。

2. 在階層式鏈接的所有其他伺服器上，使用下列指令編輯階層式尾碼的鏈接組態項目：

   ```
   ldapmodify -h host -p port -D "cn=Directory Manager" -w password
   dn:cn=databaseName,cn=chaining database,cn=plugins,cn=config
   replace:nsHopLimit
   nsHopLimit:maximumHops
   ^D
   ```

   其中 *maximumHops* 與上一步驟的定義相同。

## 傳送階層式的 LDAP 控制項

依預設值，鏈接尾碼不會傳送代理驗證控制項。但是當一個鏈接尾碼聯絡另一個鏈接尾碼時，需要此控制項才能傳送遠端伺服器上存取控制所需的使用者識別資訊。中介鏈接尾碼必須允許鏈接此控制項。

最近已定義第二個用於代理驗證控制項的通訊協定。因爲不同伺服器版本可能使用任一種控制項，您應將所有階層式伺服器設爲允許鏈接新、舊兩種代理驗證控制項。

此外，也必須設定迴圈偵測控制項，以防止階層式鏈接過程中發生迴圈。此控制項預設爲允許與鏈接作業一起轉送，但應該驗證此組態。如果伺服器不允許鏈接此控制項，將無法偵測涉及該伺服器的任何迴圈。

依照第 122 頁「配置鏈接策略」中的步驟執行，以確保允許鏈接下列三個控制項：

- 2.16.840.1.113730.3.4.12 - 代理驗證控制項 ( 舊規格 )

- 2.16.840.1.113730.3.4.18 - 代理驗證控制項 ( 新規格 )
- 1.3.6.1.4.1.1466.29539.12 - 迴圈偵測控制項

# 第 4 章

# 備份與復原資料

目錄伺服器所管理的資料通常都是大量匯入的，Directory Server 提供可匯入和匯出整個尾碼的工具。此外，還提供可一次備份所有尾碼的工具，以及從備份復原所有資料的工具。

您可以使用 LDAP 資料交換格式 (LDIF) 備份和復原資訊。

本章描述下列用於備份和復原目錄資料的程序：

- 設定尾碼唯讀模式
- 匯入資料
- 匯出日期
- 備份資料
- 從備份復原資料

**備註** 如果正在執行一個版本以上的 Directory Server，請注意本章中的所有範例都假設 Directory Server 5.2 是預設版本。如果不是這種情況，您必須執行一次下列指令，將 5.2 設定成預設版本：

```
# /usr/sbin/directoryserver -d 5.2
```

或在每次執行 `directoryserver` 指令以指定版本時加入 `-useversion` 選項，例如：

```
# /usr/sbin/directoryserver -useversion 5.2 ldif2db ...
```

## 設定尾碼唯讀模式

在 Directory Server 伺服器上執行特定匯出或備份作業前，您可以在任何指定的尾碼上啓用唯讀模式，以確定在指定時間您擁有尾碼內容狀態的真正影像。同時，在執行匯入或復原作業之前，您必須確定受該作業影響的尾碼*不是*唯讀模式。

在匯出或備份作業之前，Directory Server Console 和指令行公用程式並不會自動將目錄設定成唯讀模式，因爲這會讓您的目錄無法進行更新。但是，如果您有多重主機組態，您可以將一台伺服器的唯讀模式啓用，而您的資料在其他主機上仍維持可寫入的狀態。

若要使尾碼唯讀，請遵循在第 107 頁「設定存取權限及參照」中所描述的程序。或者，您可以將整個目錄伺服器設定爲無法寫入，如第 36 頁「設定全域唯讀模式」中所述。

## 匯入資料

Directory Server 提供兩種匯入資料的方法：

- 匯入 LDIF 檔可讓您爲目錄內的任何尾碼大量加入、修改和刪除項目。
- 從 LDIF 檔初始化尾碼會刪除尾碼中現有的資料，並以 LDIF 檔的內容取代這些資料。

您可以透過 Directory Server Console 和使用指令行公用程式來使用這兩種方法。

**備註** 所有匯入的 LDIF 檔都必須使用 UTF-8 字元集編碼。

匯入 LDIF 時，父項目必須存在目錄之中，或是從檔案中第一個加入。初始化尾碼時，LDIF 檔案必須包含有對應尾碼的根項目和所有樹狀目錄的節點。

下表顯示匯入和初始化之間的差異：

**表 4-1** 匯入資料與初始化尾碼的比較

| 比較的網域 | 匯入資料 | 初始化尾碼 |
|---|---|---|
| 覆寫內容 | 否 | 是 |
| LDAP 作業 | 加入，修改，刪除 | 僅加入 |
| 效能 | 較慢 | 快 |

**表 4-1** 匯入資料與初始化尾碼的比較

| 比較的網域 | 匯入資料 | 初始化尾碼 |
|---|---|---|
| 回應伺服器故障 | 最佳效果 ( 保留故障點之前所做的所有變更 ) | 不可部分完成 ( 故障後遺失所有的變更 ) |
| LDIF 檔案位置 | 在用戶端電腦上 | 本機對用戶端或本機對伺服器 |
| 匯入組態資訊 (cn=config) | 是 | 否 |

# 匯入 LDIF 檔案

執行匯入作業時，Directory Server Console 會執行 `ldapmodify` 作業將新的項目加入目錄中。項目是在 LDIF 檔中指定，此檔案也包含修改或刪除現有項目的更新陳述式，這是匯入作業的一部分。

匯入項目的目標是 Directory Server 所管理的任何尾碼，以及任何在組態中定義的鏈接尾碼或鏈接子尾碼。伺服器與其他任何加入項目的作業結合使用時，會在所有新項目匯入時編製新項目的索引。

## 使用主控台匯入 LDIF

您必須以目錄管理員或系統管理員的身份登入才能執行匯入：

1. 在 Directory Server Console 最上層的 [ 工作 ] 標籤，捲動至標籤的底部，按一下 [ 從 LDIF 匯入 ] 旁的按鈕。

   顯示 [ 匯入 LDIF] 對話方塊。

2. 在 [ 匯入 LDIF] 對話方塊的 [LDIF 檔案 ] 欄位中，輸入要匯入之 LDIF 檔的完整路徑，或按一下 [ 瀏覽 ] 選取本機檔案系統中的檔案。

   如果所存取的是遠端電腦上的目錄，則欄位名稱會顯示成 [LDIF 檔案 ( 在主控台電腦上 )]。這個標籤是提醒您正在瀏覽的是本機檔案系統，而不是遠端的目錄伺服器電腦。

3. 視需要設定下列選項：

   a. [ 僅加入 ] - LDIF 檔案中除了預設的加入指令外，可能還包含修改和刪除指令。如果您希望主控台只執行加入指令，並忽略 LDIF 檔案中所有其他指令，請選取這個核取方塊。

b. [ 錯誤時繼續 ] - 如果您希望主控台在發生錯誤時仍繼續匯入，請選取這個核取方塊。例如，如果您要匯入一個 LDIF 檔案，此檔案包含一些已存在於尾碼中的項目，則可以使用這個選項。主控台會記錄在執行匯入作業所發生的錯誤，例如在拒絕檔案中的現有項目。

   未選取此核取方塊時，匯入作業會在遇到第一個錯誤時停止。LDIF 檔案內所有停止作業之前的項目都會成功匯入，並且保留在目錄中。

4. 在 [ 拒絕的檔案 ] 欄位中，輸入記錄主控台所有無法匯入項目之檔案的完整路徑，或者是按一下 [ 瀏覽 ] 選取本機檔案系統中的檔案。

   例如，伺服器無法匯入目錄內現有的項目，或是沒有父項物件的項目。主控台會將伺服器傳送的錯誤訊息寫入拒絕檔案中。

   如果您將這個欄位空白，伺服器將不會記錄被拒絕的檔案。

5. 按一下 [ 確定 ] 開始匯入作業。

   Directory Server Console 會顯示一個對話方塊，其中含有作業的狀態，以及所發生任何錯誤的文字。如果 [ 拒絕的檔案 ] 欄位不是空白，則系統也會將所有錯誤訊息寫入指定的檔案中。

### 從指令行匯入 LDIF

`directoryserver ldif2ldap` 指令可透過 LDAP 匯入 LDIF 檔案，並執行其中的所有操作。使用此指令可以同時將資料匯入到所有目錄尾碼中。伺服器必須在執行中才能使用 `ldif2ldap` 匯入。

指令的完整路徑：

```
# /usr/sbin/directoryserver -s serverID ldif2ldap
```

下列範例使用 `ldif2ldap` 指令執行匯入。您無需根權限來執行此指令，但必須以具有根權限的使用者，諸如目錄管理員身份進行驗證，最後的參數指定要匯入的 LDIF 檔名。

```
# /usr/sbin/directoryserver -s example ldif2ldap \
  -D "cn=Directory Manager" -w password \
  -f /var/opt/mps/serverroot/slapd-example/ldif/demo.ldif
```

如需關於使用此指令的詳細資訊，請參閱 《Directory Server Administration Reference》 Chapter 1 的 "`ldif2ldap`"。

## 初始化尾碼

初始化尾碼會以 LDIF 檔案中只含額外項目的內容，覆寫尾碼中現有的資料。

| 小心 | 如果您正在管理的伺服器是組態 Directory Server，在初始化來自 LDIF 檔的尾碼時，除非正在復原資料，否則請小心不要覆寫 `o=NetscapeRoot` 尾碼。. 否則，您會刪除需要所有重新安裝之 Sun Java System 伺服器的資訊。 |
|---|---|

您必須以目錄管理員或系統管理員的身份登入驗證才能初始化尾碼。爲安全起見，只有目錄管理員和系統管理員擁有尾碼根項目的存取權，例如 `dc=example,dc=com`。因此，只有這些身份可以匯入包含有根項目的 LDIF 檔案。

## 從主控台初始化尾碼

| 小心 | 此程序可覆寫尾碼中的資料。 |
|---|---|

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，展開 [ 資料 ] 節點，顯示您要初始化的尾碼。
2. 在尾碼節點上按一下滑鼠右鍵，然後選取快顯功能表中的 [ 初始化 ]。或者，您可以選取尾碼節點，再選取 [ 物件 ] 功能表中的 [ 初始化 ]。顯示 [ 初始化尾碼 ] 對話方塊。
3. 在 [LDIF 檔案 ] 欄位中，輸入您想要用來初始化的 LDIF 檔案完整路徑，或是按一下 [ 瀏覽 ] 找到電腦上的這個檔案。
4. 如果您是從匯入檔案所在的本端電腦操作主控台，請跳到步驟 6。如果您是從含有 LDIF 檔案之伺服器的遠端電腦操作主控台，請選取下列其中一個選項：

   **於主控台上**。指出 LDIF 檔位於您正在執行主控台的機器上。在此情況下，您可以瀏覽該檔案。

   **於伺服器上**。表示 LDIF 檔案位在遠端伺服器上。在此情況下，「瀏覽」按鈕是停用的。依預設值，主控台會在下列目錄中尋找檔案：

   *ServerRoot*`/slapd-`*serverID*`/ldif`
5. 按一下「確定」。
6. 請確認您要覆寫尾碼中的資料。尾碼初始化將繼續進行，任何錯誤將報告於對話方塊中。

## 使用 ldif2db 指令初始化尾碼

`directoryserver ldif2db` 指令會初始化尾碼，覆寫現有的資料。此指令在繼續匯入之前會要求您關閉伺服器。

依預設值，指令會先進行儲存，然後再將現有的任何 o=NetscapeRoot 組態資訊與匯入檔案中的 o=NetscapeRoot 組態資訊合併。

| 小心 | 此指令可覆寫尾碼中的資料。 |
|---|---|

若要在伺服器停止時匯入 LDIF：

1. 由於爲指令行的 root，請使用下列指令停止伺服器：

   ```
   # /usr/sbin/directoryserver -s serverID stop
   ```

2. 執行匯入指令：

   ```
   # /usr/sbin/directoryserver -s serverID ldif2db ...
   ```

3. 如下所示啓動伺服器：

   ```
   # /usr/sbin/directoryserver -s serverID start
   ```

下列範例使用 ldif2db 指令將兩個 LDIF 檔案匯入至單一尾碼中。

```
/usr/sbin/directoryserver -s example ldif2db -n Database1 \
 -i /var/opt/mps/serverroot/slapd-example/ldif/demo.ldif \
 -i /var/opt/mps/serverroot/slapd-example/ldif/demo2.ldif
```

**表 4-2** 範例中所用 ldif2db 選項的描述

| 選項 | 描述 |
|---|---|
| -n | 指定要匯入資料之資料庫的名稱。<br>警告：如果您指定資料庫，而此資料庫並未對應包含在 LDIF 檔案中的尾碼，那麼資料庫中所包含的全部資訊都會被刪除，並且匯入失敗。請確定您沒有將資料庫的名稱拼錯。 |
| -i | 指定要匯入之 LDIF 檔的完整路徑名稱。此爲必要選項。您可使用多個 -i 引數，一次匯入一個以上的 LDIF 檔。匯入多個檔案時，伺服器會依照在指令行指定的順序將 LDIF 檔匯入。 |

如需關於使用此指令的詳細資訊，請參閱 《Directory Server Administration Reference》 Chapter 1 的 "ldif2db"。

## 使用 ldif2db 初始化尾碼

與 ldif2db 指令相同，directoryserver ldif2db-task 指令會覆寫指定尾碼中的資料。此指令檔要求伺服器需執行才能執行匯入。

此指令檔的指令是：

```
# /usr/sbin/directoryserver -s serverID ldif2db-task ...
```

下列範例使用 ldif2db-task 匯入 LDIF 檔。您無需根權限來執行此指令，但必須以具有根權限的使用者，諸如目錄管理員身份進行驗證，

```
/usr/sbin/directoryserver -s example ldif2db-task \
  -D "cn=Directory Manager" -w password -n Database1 \
  -i /var/opt/mps/serverroot/slapd-example/ldif/demo.ldif
```

下表描述此範例中所使用的 ldif2db-task 選項：

**表 4-3** 範例中所用 ldif2db-task 選項的描述

| 選項 | 描述 |
|---|---|
| -D | 指定根權限的使用者 DN，例如目錄管理員等。 |
| -w | 請指定使用者密碼。 |
| -n | 指定要匯入資料之資料庫的名稱。<br>警告：如果您指定資料庫，而此資料庫並未對應包含在 LDIF 檔案中的尾碼，那麼資料庫中所包含的全部資訊都會被刪除，並且匯入失敗。請確定您沒有將資料庫的名稱拼錯。 |
| -i | 指定要匯入之 LDIF 檔的完整路徑名稱。此爲必要選項。您可使用多個 -i 引數，一次匯入一個以上的 LDIF 檔。匯入多個檔案時，伺服器會依照在指令行指定的順序將 LDIF 檔匯入。 |

如需關於使用此指令的詳細資訊，請參閱 《Directory Server Administration Reference》 Chapter 1 的 "ldif2ldap-task"。

# 匯出日期

您可以使用 LDIF 匯出目錄的內容。下列情況適合匯出資料：

- 備份伺服器中的資料。
- 將資料複製到另一台目錄伺服器。
- 將資料匯出到另一個應用程式。
- 在變更目錄拓樸後重新擴展尾碼

匯出作業並不會匯出組態資訊 (cn=config)。

小心　在進行匯出作業時請勿停止伺服器。

## 使用主控台將整個目錄匯出到 LDIF

您可以根據最後一個匯出檔案的位置，來決定將部分或所有的目錄資料匯出到 LDIF 中。當 LDIF 檔案在伺服器上時，您可以只匯出伺服器上本機尾碼中鍵結的資料。如果 LDIF 檔案在伺服器遠端，您便可以匯出所有尾碼和鍵結的尾碼。

若要在伺服器執行時從 Directory Server Console 將目錄資料匯出到 LDIF：

1. 在 Directory Server Console 最上層的 [ 工作 ] 標籤，捲動至標籤的底部，按一下 [ 匯出到 LDIF] 旁的按鈕。

   顯示 [ 匯出 ] 對話方塊。

2. 如果您是在伺服器遠端的電腦上執行主控台，則 LDIF 檔案欄位下會顯示兩個單選按鈕。選取 [ 在主控台電腦 ] 表示您要匯出至執行主控台的機器中的 LDIF 檔案。選取 [ 在伺服器電腦 ] 表示您要匯出至位在伺服器電腦上的 LDIF 檔案。

3. 在 [LDIF 檔案 ] 欄位中輸入 LDIF 檔案的完整路徑和檔案名稱，或者按一下 [ 瀏覽 ] 找到此檔案。

   如果您已選取 [ 在伺服器電腦 ]，則停用 「瀏覽」按鈕。[ 瀏覽 ] 按鈕未啓用時，檔案會依預設值儲存在下列目錄中：

   *ServerRoot*/slapd-*serverID*/ldif

4. 如果您要匯出整個目錄，請選取 [ 所有的尾碼 ] 單選按鈕。

   如果您只要匯出目錄的樹狀子目錄，請選取 [ 樹狀子目錄 ] 單選按鈕，然後在文字方塊中輸入樹狀子目錄基礎的 DN。

   您也可以按一下 [ 瀏覽 ] 選取樹狀子目錄。

5. 按一下 [ 確定 ] 匯出目錄內容至檔案。

## 使用主控台將單一尾碼匯出到 LDIF

若要在伺服器執行時從 Directory Server Console 將一個尾碼匯出到 LDIF：

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，展開 [ 資料 ] 節點，顯示您要匯出的尾碼。
2. 在尾碼節點上按一下滑鼠右鍵，然後選取快顯功能表中的 [ 匯出 ]。或者，您可以選取尾碼節點，再選取 [ 物件 ] 功能表中的 [ 匯出 ]。

   顯示 [ 匯出尾碼 ] 對話方塊。
3. 在 [LDIF 檔案 ] 欄位中，輸入至 LDIF 檔案的完整路徑，或是按一下 [ 瀏覽 ] 找到電腦上的這個檔案。

   [ 瀏覽 ] 按鈕未啓用時，依預設值檔案會儲存在下列目錄中：

   *ServerRoot*/slapd-*serverID*/ldif
4. 如果尾碼已複製，您可以選取核取方塊以 [ 匯出複製資訊 ]。此功能僅在您匯出 LDIF 以初始化此尾碼的其他複本時需要。
5. 如果此尾碼的屬性加密已啓用，您可以選取核取方塊以 [ 解密 ] 屬性。爲此，您必須提供保護伺服器憑證資料庫的密碼。選取選項以輸入密碼或輸入包含密碼的檔案名稱。如果您無法提供解密屬性值的密碼，加密的值將顯示於 LDIF 輸出中。
6. 按一下 [ 確定 ] 匯出尾碼的內容至檔案。

## 從指令行匯出至 LDIF

您可以使用 `directoryserver db2ldif` 指令，匯出任何尾碼或目錄的樹狀子目錄至 LDIF。這個指令檔會將您所有的尾碼內容或部分內容匯出至 LDIF 檔案，不論伺服器正在執行或已經停止。

若要將資料庫的內容匯出至 LDIF 檔案，請使用下列指令：

```
# /usr/sbin/directoryserver -s serverID db2ldif ...
```

下列範例將兩個尾碼匯出至單一 LDIF 檔案：

```
/usr/sbin/directoryserver -s example db2ldif \
     -a /var/opt/mps/serverroot/slapd-example/output.ldif \
     -s "dc=example,dc=com" -s "o=NetscapeRoot"
```

下表描述此範例中所使用的 `db2ldif` 選項：

**表 4-4** 範例中所用 db2ldif 選項的描述

| 選項 | 描述 |
|---|---|
| `-a` | 定義伺服器儲存匯出 LDIF 之輸出檔案的名稱。這個檔案會依預設值儲存在 *ServerRoot*`/slapd-`*serverID* 目錄中。 |
| `-s` | 指定匯出時要包含的尾碼或樹狀子目錄。您可以使用多個 `-s` 引數來指定多個尾碼或樹狀子目錄。 |

`db2ldif` 指令也可以與 `-r` 選項結合使用，將複製的尾碼匯出到 LDIF 檔案中。所產生的 LDIF 將會含有複製機制所使用的屬性子類型。接下來，便可以將此 LDIF 檔案匯入到用戶的伺服器上以初始化用戶複本，如第 278 頁「初始化複本」中所述。

當 `db2ldif` 指令與 `-r` 選項結合使用時，伺服器必須不在執行狀態中。您必須先停止伺服器然後再啓動，或使用 `db2ldif.pl` 指令檔與 `-r` 選項，後者不需停止伺服器。

如需關於使用此指令檔的詳細資訊，請參閱《Directory Server Administration Reference》 Chapter 1 的 "db2ldif" 。

# 備份資料

備份資料時系統會儲存目錄內容的快照，以防日後資料庫檔案損毀或刪除。您可以使用 Directory Server Console 或指令行指令檔來備份尾碼。

**小心** 在執行備份作業期間請勿停止伺服器。

依預設值，此處所描述的所有備份程序都會將伺服器檔案的複本儲存在同一台主機上。爲了安全起見，您應該複製備份，然後將它儲存在不同的電腦或檔案系統中。

**備註** 您不可以使用這些備份方法來備份遠端伺服器上的鏈接尾碼。不同的伺服器必須個別進行備份。

## 使用主控台備份您的伺服器

從 Directory Server Console 備份伺服器時，伺服器會將所有資料庫的內容與相關的索引檔案，複製到備份位置上。您可以在伺服器執行時執行備份。

若要從主控台備份伺服器：

1. 在 Directory Server Console 最上層的 [ 工作 ] 標籤中，按一下 [ 備份目錄伺服器 ] 旁的按鈕。

   顯示 [ 備份目錄伺服器 ] 對話方塊。

2. 在 [ 目錄 ] 文字方塊中，輸入您要儲存備份之目錄的完整路徑。如果您在與目錄相同的電腦上執行主控台，請按一下 [ 瀏覽 ] 尋找本機目錄。

   或者按一下 [ 使用預設 ] 將備份儲存到下列目錄中：

   *ServerRoot*/slapd-*serverID*/bak/*YYYY_MM_DD_hh_mm_ss*

   其中 *serverID* 是您目錄伺服器的名稱，而產生的目錄名稱中會包含備份建立的時間與日期。

3. 按一下 [ 確定 ] 建立備份。

## 從指令行備份您的伺服器

您可以使用 `directoryserver db2bak` 指令，從指令行備份您的伺服器。不論伺服器是否在執行都可以使用此指令。

您無法使用這個備份方法來備份組態資訊。如需關於備份組態資訊的資訊，請參閱第 148 頁「備份 dse.ldif 組態檔」。

若要備份目錄，請使用下列指令：

```
# /usr/sbin/directoryserver -s serverID db2bak backupDir
```

*backupDir* 參數指定應該儲存備份的目錄。系統使用目前的日期產生預設的備份目錄名稱：`YYYY_MM_DD_hh_mm_ss`. 如需關於使用此指令的詳細資訊，請參閱《Directory Server Administration Reference》 Chapter 1 的 "db2bak"。如需有關設計佈署的備份策略資訊，請參閱 《Directory Server Deployment Planning Guide 》 Chapter 9 的 "Planning a Backup Strategy"。

## 備份 dse.ldif 組態檔

Directory Server 會自動備份 `dse.ldif` 組態檔。當您啓動 Directory Server 時，它會自動建立 `dse.ldif` 檔案的備份，並儲存在下列目錄中名爲 `dse.ldif.startOK` 的檔案內：

*ServerRoot*/slapd-*serverID*/config

當您修改 `cn=config` 分支時，檔案會先備份至 `config` 目錄中名爲 `dse.ldif.bak` 的檔案中，然後伺服器才會將修改寫入 `dse.ldif` 檔案。如果您需要儲存組態，請製作這些檔案的複本。

# 從備份復原資料

下列程序描述如何使用 Directory Server Console 或指令行來復原目錄中的尾碼。您的伺服器必須已經使用第 146 頁「備份資料」中所描述的程序備份。在復原與複製協議有關的尾碼前，請先詳細閱讀 第 148 頁「復原複製的尾碼」。

| | |
|---|---|
| 小心 | 在執行備份或復原作業期間請勿停止伺服器。<br><br>復原伺服器時會複製所有現有的資料庫檔案，因此在備份之後所有修改的資料都會遺失。 |

## 復原複製的尾碼

在將供應商伺服器與用戶伺服器之間複製的尾碼復原之前，您必須做特殊的考量。如果可能的話，您應該透過複製機制來更新尾碼，而不是從備份復原尾碼。此節將解釋復原複本的時間和方式，以及如何確定該複本在作業後與其他複本同步化。如需使用備份和復原以初始化複本的詳細資訊，請參閱第 278 頁「初始化複本」。

### 復原單一主機環境中的供應商

做爲單一主機供應者的尾碼含有整個複製拓樸的系統授權資料。因此，復原這個尾碼等於重新初始化整個拓樸中的所有資料。除非您想要從復原的備份內容將所有資料重新初始化，否則請勿復原單一主機。

如果單一主機資料因爲錯誤而無法復原，您可以考慮使用其中一台用戶主機的資料，因爲該主機可能包含比備份新的更新資料。在這種情況下，您必須將資料從用戶複本匯出到 LDIF 檔案，然後從 LDIF 檔案重新初始化主機。

不論您是復原備份或匯入主機複本上的 LDIF 檔案，之後您都必須將所有向此複本接收更新資料的集線器和用戶複本重新初始化。系統將會在供應商伺服器的記錄檔中記錄一個訊息，提醒您需要重新初始化用戶。

## 復原多重主機環境中的供應商

在多重主機複製中，其他主機每個都包含複製資料的系統授權複本。您無法用目前的複本內容來復原可能已經過時的舊備份。如果可能的話，您應該允許複製機制使用其他主機的內容更新此主機。

如果不可能，您只能用下列其中一種方法來復原多重主機複本：

- 最簡單的方法就是不復原備份，而是從其中一台其他主機重新初始化預定的主機。這樣可確保最新的資料會傳送至預定的主機，並且那些資料也已經準備好用來複製。請參閱第 282 頁「使用主控台初始化複本」或第 283 頁「從指令行初始化複本」。
- 當複本有上百萬個項目時，較快的方法是使用新的二進位複製功能來復原取自其中一個其他主機的最新備份。請參閱第 285 頁「使用二進位複製初始化複本」。
- 如果您已將主機備份，而該備份不比其他*任何*主機中的變更記錄內容還舊，則應該使用此備份來復原這台主機。如需變更記錄天數的描述，請參閱第 272 頁「進階多重主機組態」。復原舊備份時，其他主機會使用變更記錄，以自儲存備份之後的所有修改來更新此主機。

不論您如何復原或重新初始化，初始化之後的主機複本都將維持唯讀模式。此行爲讓複本可以與其他主機同步化，同步化後便可允許寫入作業，如第 279 頁「多重主機初始化後的交集」中所述。

在允許於復原或初始化的主機上執行寫入作業之前，先允許所有複本聚集的優點是：沒有任何集線器或用戶伺服器需要重新初始化。

## 復原集線器

此節只適用於當複製機制無法自動更新集線器複本時，例如，資料庫檔案損毀或複製中斷太久。當發生這些情況時，您必須使用下列其中一種方法來復原或重新初始化集線器複本：

- 最簡單的方法就是不復原備份，而是從其中一台主機複本重新初始化集線器。這樣可確保最新的資料會傳送至集線器，以備複製。請參閱第 282 頁「使用主控台初始化複本」或第 283 頁「從指令行初始化複本」。
- 當複本有上百萬個項目時，較快的方法是使用新的二進位複製功能來復原取自另一個集線器複本的最新備份。請參閱第 285 頁「使用二進位複製初始化複本」。如果沒有其他集線器複本可以複製，您必須依照上一段的描述重新初始化集線器，或是下一段的描述將集線器復原 ( 如果可能的話 )。

- 如果您已將集線器備份，而該備份不比*任何*供應商的變更記錄內容還舊 ( 不管是集線器或主機複本 )，則應該使用該備份來復原此集線器。如需變更記錄天數的描述，請參閱第 272 頁「進階多重主機組態」。復原舊備份時，其供應商會使用變更記錄，以自儲存備份之後的修改將此集線器更新。

**備註** 不論您如何復原或重新初始化集線器複本，您都*必須*重新初始化此集線器的所有用戶，包括集線器的其他所有層級。

### 復原專屬用戶

此節只適用於當複製機制無法自動更新專屬用戶複本時，例如，資料庫檔案被損毀或複製中斷太久。當發生這些情況時，您將必須使用下列其中一種方法來復原或重新初始化用戶：

- 最簡單的方法就是不復原備份，而是從其中一位供應商重新初始化用戶，主機或集線器複本皆可。這樣可確保最新的資料傳送至用戶，以備複製。請參閱第 282 頁「使用主控台初始化複本」或第 283 頁「從指令行初始化複本」。
- 當複本有上百萬個項目時，較快的方法是使用新的二進位複製功能來復原取自其他用戶複本的最新備份。請參閱第 285 頁「使用二進位複製初始化複本」。如果沒有其他用戶可以複製，您必須依照上一段的描述重新初始化複本，或是下一段的描述將用戶復原 ( 如果可能的話 )。
- 如果您用戶的備份不比*任何*供應商的變更記錄內容還舊 ( 不管是集線器或主機複本 )，則應該使用該備份來復原此用戶。如需變更記錄天數的描述，請參閱第 272 頁「進階多重主機組態」。復原舊備份時，其供應商會使用變更記錄，以自儲存備份之後進行的所有修改更新此用戶。

## 使用主控台復原您的伺服器

您可以使用 Directory Server Console，從之前建立的備份中復原損毀的目錄資料。若要使用主控台復原資料，必須執行 Directory Server。但是在復原期間，無法使用對應的尾碼來處理作業。

若要從之前建立的備份復原伺服器：

1. 在 Directory Server Console 最上層的 [ 工作 ] 標籤中，按一下 [ 復原目錄伺服器 ] 旁的按鈕。

   顯示 [ 復原目錄 ] 對話方塊。

2. 從 [ 可用備份 ] 清單中選取備份，或在 [ 目錄 ] 文字方塊中輸入有效備份的完整路徑。

   [ 可用備份 ] 清單中會顯示位於預設目錄中的所有備份：

   *ServerRoot*/slapd-*serverID*/bak

3. 按一下 [ 確定 ] 復原您的伺服器。

## 從指令行復原您的伺服器

您可以使用下列指令檔從指令行復原伺服器：

- 使用 `directoryserver bak2db` 指令。此指令需要關閉伺服器才能使用。
- 使用 `directoryserver bak2db-task` 指令。此指令需要執行伺服器才能使用。

### 使用 bak2db 指令

若要在伺服器關閉期間從指令行復原目錄：

1. 由於爲指令行的 root，請使用下列指令停止伺服器：

   ```
   # /usr/sbin/directoryserver -s serverID stop
   ```

2. 使用 `bak2db` 指令與備份目錄的完整路徑：

   ```
   # /usr/sbin/directoryserver -s serverID bak2db backupDir
   ```

3. 如下所示啓動伺服器：

   ```
   # /usr/sbin/directoryserver -s serverID start
   ```

下列範例從預設的備份目錄復原備份：

```
/usr/sbin/directoryserver -s example bak2db \
        /var/opt/mps/serverroot/slapd-example/bak/2003_07_01_11_34_00
```

如需詳細資訊，請參閱 《Directory Server Administration Reference》 Chapter 1 的 "bak2db"。

### 使用 bak2db-task

若要在伺服器執行期間從指令行復原目錄，請使用下列指令：

```
# /usr/sbin/directoryserver -s serverID bak2db-task ...
```

下列範例使用 `bak2db-task` 指令復原備份。`-a` 選項會提供備份目錄的完整路徑。

```
/usr/sbin/directoryserver -s example bak2db-task\
  -D "cn=Directory Manager" -w password \
  -a /var/opt/mps/serverroot/slapd-example/bak/2003_07_01_11_34_00
```

如需詳細資訊，請參閱 《Directory Server Administration Reference》 Chapter 1 的 "bak2db-task"。

# 復原 dse.ldif 組態檔

此目錄會在下列目錄中建立 dse.ldif 檔案的兩個備份複本：

*ServerRoot*/slapd-*serverID*/config

dse.ldif.startOK 檔案會在伺服器啓動時記錄 dse.ldif 檔案的複本。dse.ldif.bak 檔案中包含對 dse.ldif 檔案最新變更的備份。將包含最新變更的檔案複製到您的目錄中。

若要復原 dse.ldif 組態檔：

1. 由於爲指令行的 root，請使用下列指令停止伺服器：

   ```
   # /usr/sbin/directoryserver -s serverID stop
   ```

2. 變更至包含組態檔的目錄，例如：

   ```
   # cd /var/mps/serverrot/slapd-serverID/config
   ```

3. 使用已知爲完整的備份組態檔覆寫 dse.ldif 檔案。例如，您可以輸入下列指令：

   ```
   cp dse.ldif.startOK dse.ldif
   ```

4. 以下列指令啓動伺服器：

   ```
   # /usr/sbin/directoryserver -s serverID start
   ```

# 第 5 章

# 管理群組和角色

除了在目錄中資料的階層式結構以外，管理代表使用者的項目通常需要建立群組並共用一般的屬性值。Directory Server 透過群組、角色和服務類別 (CoS) 來提供此進階項目管理功能。

群組是指將其他項目命名爲成員清單或成員篩選器的項目。角色能提供相同或更多的功能，它透過一種機制，能在角色中的每一位成員上產生 `nsrole` 屬性。CoS 也會產生一種虛擬的屬性，允許項目共用一般的屬性值，而不需將屬性值儲存在每個項目中。

Directory Server 提供了一種功能，可以根據角色值和 CoS 虛擬屬性執行搜尋。任何作業中所用的篩選器字串內可包含 `nsRole` 屬性，或任何由 CoS 定義所產生的屬性，篩選字串也會執行此屬性值的任何一個比較作業。但是，系統無法爲虛擬的 CoS 屬性編製索引，因此任何涉及 CoS 所產生屬性的搜尋都無法被索引。這樣會消耗大量的時間和記憶體資源。

爲完全利用角色和服務類別所提供的功能，您應該在目錄部署的規劃階段就決定好目錄拓樸。如需這些機制的描述，及其簡化拓樸的方式，請參閱 《Directory Server Deployment Planning Guide》中的 Chapter 4 "The Directory Information Tree"。

本章包含下列章節：

# 管理群組

群組可用於讓群組產生關聯以簡化管理作業，例如用於定義 ACI。群組定義是一種特殊項目，它可爲靜態清單內的群組成員命名，或指定篩選器來定義一組動態項目。

群組可能成員的範圍是整個目錄，不論群組定義項目位在什麼位置上。爲簡化管理，所有群組定義項目通常都儲存在單一位置中，通常是根尾碼下的 `ou=Groups`。

定義靜態群組的項目是繼承自 `groupOfNames` 或 `groupOfUniqueNames` 物件類別。群組成員會依照它們的 DN，列示成 `member` 或 `uniqueMember` 屬性的多個值。

定義動態群組的項目是繼承自 `groupOfURLs` 物件類別。群組成員關係是由多重值 `memberURL` 屬性中所指定的一或多個篩選器來定義。動態群組的成員是指每次進行評估時，符合任一篩選器的項目。

下一節描述如何使用主控台建立和修改靜態與動態群組。

## 加入新的靜態群組

1. 在 Directory Server Console 最上層的 [ 目錄 ] 標籤上，在樹狀目錄內您想要加入新群組的項目上，按一下滑鼠右鍵，並選取 [ 新增 ] > [ 群組 ] 項目。

   或者，選取項目並選取 [ 物件 ] 功能表中的 [ 新增 ] > [ 群組 ] 項目。

2. 在 [ 建立新群組 ] 對話方塊中，您必須在 [ 群組名稱 ] 欄位中輸入新群組名稱，您也可以在 [ 描述 ] 欄位中加入該群組的選用描述。群組名稱會成爲新群組項目的 `cn` ( 一般名稱 ) 屬性值並出現在其 DN 中。

3. 在對話方塊的左清單中按一下 [ 成員 ]。在右面板中，預設值會選取 [ 靜態群組 ] 標籤。

4. 按一下 [ 加入 ] 將新成員加入群組中。顯示一般的 [ 搜尋使用者和群組 ] 對話方塊。

5. 在 [ 搜尋 ] 下拉式清單中，選取 [ 使用者 ] 並輸入搜尋字串，然後按一下 [ 搜尋 ]。按一下 [ 進階 ] 按鈕，搜尋特定屬性或特定屬性值。

   請在結果中選取一或多個項目，並按一下 [ 確定 ]。重複此步驟加入所有您想加入此靜態群組的成員。

**備註** 靜態群組成員有可能因爲鏈接的原因而成爲遠端成員。您可以使用參考的完整性 Plug-in，來確定被刪除的成員會自動從靜態群組項目中刪除。如需關於參考的完整性與鏈接結合使用的詳細資訊，請參閱第 122 頁「配置鏈接策略」。

6. 按一下左清單中的 [ 語言 ]，以其他語言指定您的群組名稱和描述字串。當主控台使用對應地區時，會顯示這些選項。

7. 按一下 [ 確定 ] 建立您的新群組，它會顯示爲其建立所在項目內的其中一個子項。

## 加入新的動態群組

1. 在 Directory Server Console 最上層的 [ 目錄 ] 標籤上，在樹狀目錄內您想要加入新群組的項目上，按一下滑鼠右鍵，並選取 [ 新增 ] > [ 群組 ] 項目。

   或者，選取項目並選取 [ 物件 ] 功能表中的 [ 新增 ] > [ 群組 ] 項目。

2. 在 [ 建立新群組 ] 對話方塊中，在 [ 群組名稱 ] 欄位中輸入新群組的名稱。您可以在 [ 描述 ] 欄位中，加入該群組的選用描述。群組名稱會成爲新群組項目的 cn ( 一般名稱 ) 屬性值並出現在其 DN 中。

3. 在對話方塊的左清單中按一下 [ 成員 ]，並選取右面板內的 [ 動態群組 ] 標籤。

4. 按一下 [ 加入 ]，建立包含定義群組成員之篩選器字串的 LDAP URL。顯示一般的 [ 建構並測試 LDAP URL] 對話方塊。

5. 在文字欄位中輸入 LDAP URL 或選取 [ 建構 ]，在指引下完成含有群組篩選器的 LDAP URL 建構作業。按一下 [ 測試 ] 檢視由此篩選器傳回的項目清單。

   在完成 URL 的建構後按一下 [ 確定 ]。重複此步驟加入所有包含定義動態群組之篩選器的 URL。

6. 按一下左清單中的 [ 語言 ]，以其他語言指定您的群組名稱和描述字串。當主控台使用對應地區時，會顯示這些選項。

7. 按一下 [ 確定 ] 建立您的新群組，它會顯示爲其建立所在項目內的其中一個子項。

## 修改群組定義

1. 在 Directory Server Console 最上層的 [ 目錄 ] 標籤上，連按兩下代表您要修改的群組項目。

   或者，選取該項目，再選取 [ 物件 ] 功能表中的 [ 開啓 ]。

2. 在 [ 編輯項目 ] 對話方塊中，變更 [ 一般 ]、[ 成員 ] 或 [ 語言 ] 類別中的群組資訊。您可以加入或移除靜態群組的成員，或加入、編輯或移除含有動態群組篩選器的 URL。

3. 完成群組定義的修改後，按一下 [ 確定 ]。

   若要在主控台檢視您的變更，請選取 [ 檢視 ] 功能表中的 [ 重新整理 ]。

### 移除群組定義

無論要移除哪一種群組類型，只要刪除定義該群組的項目即可。

# 指派角色

角色是另一種分組機制，設計此機制的目的是讓應用程式更有效率也更容易使用。角色的定義和管理方式類似群組，但除此之外，成員項目也具有產生的屬性，此屬性可表示項目所參與的角色。例如，應用程式只需讀取項目的角色即可，而無需先選取群組然後再瀏覽成員清單。

依預設值，角色的範圍限制在定義角色所在的樹狀子目錄內。Directory Server 引進巢式角色延伸範圍的功能，讓巢式角色能夠巢居在其他樹狀子目錄中，並擁有目錄中任何位置的成員。如需延伸角色範圍的詳細資料，請參閱第 164 頁「巢式角色定義的範例」。

## 關於角色

每個角色都有擁有該角色的*成員*或項目。從目錄中擷取項目後，角色機制會自動在每一個項目中產生 `nsRole` 屬性，這些項目可以是任何角色的成員。這個多重值屬性包含所有角色定義的 DN，在這些定義中項目是成員。`nsRole` 屬性是一個計算屬性，它並不與項目本身儲存在一起，而是在作業結果中當作一般屬性傳回給用戶端應用程式。

Directory Server 支援三種角色類型：

- 管理的角色 - 系統管理員將 `nsRoleDN` 屬性加入至想要的成員項目中，藉以指派受管理角色。這個屬性的值是角色定義項目的 DN。受管理角色類似靜態群組，不同處是前者的成員關係是定義在每個項目中，而非在角色定義項目中。
- 篩選的角色 - 等同於動態群組：它們在其 `nsRoleFilter` 屬性中定義篩選字串。篩選角色的範圍爲它所在的樹狀子目錄內，根部位在其定義項目的父項內。當伺服器傳回符合其篩選器之篩選角色範圍中的項目時，該項目會包含所產生的 `nsRole` 屬性，此屬性能識別角色。
- 巢式角色 - 爲其他角色定義命名的角色，包括其他巢式角色。巢式角色的成員集合是它所包含之角色中所有成員的聯集。巢式角色也可以定義延伸範圍，以包含其他樹狀子目錄中角色的成員。

角色使用戶端應用程式能夠直接讀取其 nsRole 屬性，以決定項目的所有角色成員。這簡化了用戶端處理最佳化目錄的使用情形。角色可以搭配 CoS 機制一起使用，爲角色成員產生其他屬性 ( 參閱第 176 頁「建立以角色爲基礎的屬性」 )。角色可用來定義存取控制 ( 參閱第 199 頁「定義角色存取 - roledn 關鍵字」 )。角色也支援其他功能，例如同時啓用或停用所有成員 ( 參閱第 257 頁「停用與啓用使用者與角色」 )。

## 搜尋 nsRole 屬性

Directory Server 允許在任何搜尋篩選器中使用 nsRole 屬性。您可以使用任何比較運算子搜尋此屬性的特殊值。搜尋 nsRole 屬性時，請謹記下列考量：

- 進行與 nsRole 屬性相關的搜尋時，可能會花費相當長的時間，因爲系統必須先評估所有角色然後才篩選項目。
- Directory Server 已最佳化，可對管理的角色中的特定成員關係進行相等搜尋。例如，下列搜尋幾乎與搜尋實際屬性一樣快：

  ```
  (&(objectclass=person)
    (nsRole=cn=managersRole,ou=People,dc=example,dc=com)
  ```

- 依預設值，用於定義受管理角色成員關係的 nsRoleDN 屬性已編製爲所有尾碼的索引。如果此屬性的索引停用，則管理角色成員關係的搜尋作業不再是最佳化。
- 搜尋內含篩選角色的項目涉及使用角色篩選器的內部搜尋。在角色範圍的所有尾碼中，如果出現在角色篩選器的所有屬性都已編製索引，就能以最快的速度執行此內部作業。

## nsRole 屬性的權限

nsRole 屬性只能由角色機制來指派，任何目錄使用者均無法寫入或修改該屬性。但是，您應該謹記下列考量：

- 任何目錄使用者可能都可以讀取 nsRole 屬性，但您可以定義存取控制來保護它不被讀取。
- nsRoleDN 屬性定義管理角色成員關係，您應該決定使用者是否可以將他自己加入角色中，或從角色中移除。如需防止使用者修改自己角色的 ACI，請參閱第 162 頁「受管理角色定義的範例」。
- 篩選的角色透過篩選器來決定成員關係，此篩選器是根據使用者項目中屬性的存在與否或屬性值來篩選。小心定義這些屬性的使用者權限，以控制誰可以定義篩選角色中的成員關係。

如需關於如何在目錄中使用角色的詳細資訊，請參閱《Directory Server Deployment Planning Guide》中的 Chapter 4 "Managed, Filtered, and Nested Roles"。

# 使用主控台指派角色

本節描述透過 Directory Server Console 建立和修改角色的程序。

## 建立受管理角色

受管理角色擁有角色定義項目，並透過將 nsRoleDN 屬性加入每個成員項目的方式來指定成員。若要使用主控台建立受管理角色並加入成員：

1. 在 Directory Server Console 的最上層 [ 目錄 ] 標籤上，在您想要加入新角色定義的樹狀目錄內項目上，按一下滑鼠右鍵，並選取 [ 新增 ] > [ 角色 ] 項目。

   或者，請選取項目並選取 [ 物件 ] 功能表中 [ 新增 ] > [ 角色 ] 項目。

2. 在 [ 建立新角色 ] 對話方塊中，您必須在 [ 角色名稱 ] 欄位中輸入新角色的名稱，您也可以在 [ 描述 ] 欄位中加入該角色的選用描述。群組名稱會成爲新角色項目的 cn ( 一般名稱 ) 屬性值，並顯示其 DN。

3. 在對話方塊的左清單中按一下 [ 成員 ]。在右窗格中，預設值會選取 [ 管理的角色 ] 單選按鈕。

4. 按一下成員清單下的 [ 加入 ] 將新的成員加入角色中。顯示一般的 [ 搜尋使用者和群組 ] 對話方塊。

5. 在 [ 搜尋 ] 下拉式清單中，選取 [ 使用者 ] 並輸入搜尋字串，然後按一下 [ 搜尋 ]。按一下 [ 進階 ] 按鈕，搜尋特定屬性或特定屬性值。

   請在結果中選取一或多個項目，並按一下 [ 確定 ]。重複此步驟加入所有您想加入此管理角色的成員。

6. 當完成將項目加入角色後，按一下 [ 確定 ]。樹狀目錄中顯示的新角色會有受管理角色的圖示，所有成員項目都會具有屬性 nsRoleDN，其值爲這個新角色項目的 DN。

7. 一旦角色建立後，您也可以將此角色指派給任何項目，方法是將 nsRoleDN 屬性加入具有角色項目之 DN 值的項目。

## 建立篩選的角色

如果項目擁有角色定義中的 LDAP 篩選器所選取的屬性或屬性值，該項目便是篩選角色的成員。

**備註** 篩選角色的篩選字串可以用任何屬性爲基礎，但是由 CoS 機制所產生的虛擬屬性除外 ( 參閱第 165 頁 「關於 CoS」 )。

若要使用主控台建立篩選的角色並加入成員：

1. 在 Directory Server Console 的最上層 [ 目錄 ] 標籤上，在您想要加入新角色定義的樹狀目錄內項目上，按一下滑鼠右鍵，並選取 [ 新增 ] > [ 角色 ] 項目。

   或者，請選取項目並選取 [ 物件 ] 功能表中 [ 新增 ] > [ 角色 ] 項目。

2. 在 [ 建立新角色 ] 對話方塊中，您必須在 [ 角色名稱 ] 欄位中輸入新角色的名稱，您也可以在 [ 描述 ] 欄位中加入該角色的選用描述。角色名稱會成爲新角色項目的 `cn` ( 一般名稱 ) 屬性值並出現在其 DN 中。

3. 在對話方塊的左清單中按一下 [ 成員 ]，並選取右面板內的 [ 篩選的角色 ] 單選按鈕。

4. 在文字欄位中輸入 LDAP 篩選器以定義將決定角色成員的篩選器。或者，按一下 [ 建構 ]，在指引下完成 LDAP 篩選器的建構作業。

5. 如果按一下 [ 建構 ]，就會出現 [ 建構 LDAP 篩選器 ] 對話方塊。略過 [LDAP 伺服器主機 ]、[ 連接埠 ]、[Base DN] 和 [ 搜尋範圍 ] 欄位，因爲您無法在篩選角色定義中指定它們。

   a. 只搜尋篩選角色中的使用者。這將會把元件 (`objectclass=person`) 加入篩選器中。如果您不要這個元件，您必須在 [ 建立新角色 ] 對話方塊的文字欄位中編輯 LDAP 篩選器。

   b. 從 [ 位置 ] 下拉式清單中選取一個屬性，並設定對應條件以優化篩選器。若要加入其他篩選器，請按一下 [ 更多 ]。若要移除不必要的篩選器，請按一下 [ 更少 ]。

   c. 按一下 [ 確定 ] 以使用篩選角色定義中的篩選器。接下來，您可以在文字欄位中編輯篩選器以修改任何元件。

6. 按一下 [ 測試 ] 以試用您的篩選器。[ 篩選測試結果 ] 對話方塊中將會顯示目前符合您篩選器的項目。

7. 按一下 [ 確定 ] 建立新的角色項目。新的角色會出現在樹狀目錄中，並具有篩選角色的圖示。

## 建立巢式角色

巢式角色可讓您建立包含其他角色的角色，以及延伸現有角色的範圍。在建立巢式角色之前，另一個角色必須是存在的。當您建立巢式角色時，主控台會顯示可以爲巢式之角色的清單。巢式角色可包含其他巢式角色，最多可達 30 層巢式。超過這個固定限制後，伺服器在評估角色時將會記錄錯誤。

若要使用主控台建立巢式角色並加入成員：

1. 在 Directory Server Console 的最上層 [ 目錄 ] 標籤上，在您想要加入新角色定義的樹狀目錄內項目上，按一下滑鼠右鍵，並選取 [ 新增 ] > [ 角色 ] 項目。

   或者，請選取項目並選取 [ 物件 ] 功能表中 [ 新增 ] > [ 角色 ] 項目。

2. 在 [ 建立新角色 ] 對話方塊中，您必須在 [ 角色名稱 ] 欄位中輸入新角色的名稱，您也可以在 [ 描述 ] 欄位中加入該角色的選用描述。角色名稱會成爲新角色項目的 cn ( 一般名稱 ) 屬性值並出現在其 DN 中。

3. 在對話方塊的左清單中按一下 [ 成員 ]，並選取右面板內的 [ 巢式角色 ] 單選按鈕。

4. 按一下 [ 加入 ] 將現有的角色加入巢式角色清單中。在出現的 [ 角色選取器 ] 中，從可用的角色清單中選取一或多個角色，並按一下 [ 確定 ]。

5. 按一下 [ 確定 ] 建立巢式角色項目。新的角色會出現在目錄中，並具有巢式角色的圖示。

6. 若要修改巢式角色的範圍，請使用第 164 頁「巢式角色定義的範例」中所示的指令行程序。

## 檢視和編輯項目的角色

1. 在 Directory Server Console 最上層的 [ 目錄 ] 標籤上，瀏覽樹狀目錄，以顯示要檢視或編輯其角色的項目。

2. 以滑鼠右鍵按一下項目，並選取快顯功能表中的 [ 設定角色 ]。或者，以滑鼠左鍵按一下項目以選取項目，再選取 [ 物件 ] 功能表中的 [ 設定角色 ]。

   顯示 [ 設定角色 ] 對話方塊。

3. 選取 [ 管理的角色 ] 標籤，以顯示此項目所屬的受管理角色。您可以執行下列動作：

   - 若要加入新的受管理角色，請按一下 [ 加入 ]，並從 [ 角色選取器 ] 視窗中選取可用的角色。在 [ 角色選取器 ] 視窗中按一下 [ 確定 ]。
   - 若要移除受管理角色，請選取該角色並按一下 [ 移除 ]。
   - 若要編輯與項目相關的受管理角色，請在表格中選取角色，再按一下 [ 編輯 ]。角色顯示在 [ 角色 ] 的自訂編輯器中。對角色執行任何變更，再按一下 [ 確定 ] 以儲存新的角色定義。

4. 選取 [ 其他角色 ] 標籤，以檢視此項目所屬的篩選或巢式角色。若要變更篩選或巢式角色的角色成員關係，您必須編輯角色定義：

   - 選取角色，再按一下 [ 編輯 ]，以顯示 [ 角色 ] 的自訂編輯器。對角色執行變更，再按一下 [ 確定 ] 以儲存新的角色定義。

5. 完成修改角色後，按一下 [ 確定 ] 以儲存變更。

## 修改角色項目

1. 在 Directory Server Console 上，選取 [ 目錄 ] 標籤。
2. 在瀏覽樹狀目錄內瀏覽以找到現有角色的定義項目，角色是其建立所在項目的子項。連按兩下角色。

   顯示 [ 編輯項目 ] 對話方塊。
3. 按一下左窗格中的 [ 一般 ] 以變更角色名稱和描述。
4. 按一下左窗格中的 [ 成員 ] 可變更管理和巢式角色的成員，或變更篩選角色的篩選器。
5. 按一下 [ 確定 ] 儲存您的變更。

## 刪除角色

刪除角色只會刪除角色定義的項目，而不會刪除其成員。

若要刪除角色：

1. 在 Directory Server Console 上，選取 [ 目錄 ] 標籤。
2. 在瀏覽樹狀目錄內瀏覽以找到角色的定義項目，角色是其建立所在項目的子項。
3. 以滑鼠右鍵按一下角色並選取 [ 刪除 ]。

   顯示對話方塊要求您確認刪除。按一下 [ 是 ]。
4. 顯示 [ 刪除的項目 ] 對話方塊，通知您角色已成功刪除。按一下 「確定」。

**備註** 刪除角色只會刪除角色項目，但不會刪除各角色成員的 `nsRoleDN` 屬性。若要如此執行，請啓用 「參考完整性 Plug-in」並進行配置以管理 `nsRoleDN` 屬性。如需詳細資訊，請參閱第 77 頁「維護參考的完整性」。

# 從指令行管理角色

角色是定義在目錄管理員可以透過指令行公用程式存取的項目中。一旦建立好角色，便要指派該角色的成員，方法如下：

- 受管理角色的成員其項目內擁有 nsRoleDN 屬性。
- 篩選角色的成員是符合 nsRoleFilter 屬性中所指定篩選器的項目。
- 巢式角色的成員是巢式角色定義項目之 nsRoleDN 屬性中所指定角色的成員。

所有角色定義都繼承自 LDAPsubentry 和 nsRoleDefinition 物件類別。下表列出其他的物件類別，以及各角色類型特有的相關屬性。

**表 5-1** 用於定義角色的物件類別與屬性

| 角色類型 | 物件類別 | 屬性 |
|---|---|---|
| 管理的角色 | nsSimpleRoleDefinition<br>nsManagedRoleDefinition | Description(選用) |
| 篩選的角色 | nsComplexRoleDefinition<br>nsFilteredRoleDefinition | nsRoleFilter<br>Description(選用) |
| 巢式角色 | nsComplexRoleDefinition<br>nsNestedRoleDefinition | nsRoleDN<br>Description(選用) |

## 受管理角色定義的範例

若要建立將指派給所有行銷人員的角色，請執行下列 ldapmodify 指令：

```
ldapmodify -a -h host -p port -D "cn=Directory Manager" -w password
dn:cn=Marketing,ou=marketing,ou=People,dc=example,dc=com
objectclass:top
objectclass:LDAPsubentry
objectclass:nsRoleDefinition
objectclass:nsSimpleRoleDefinition
objectclass:nsManagedRoleDefinition
cn:Marketing
description:managed role for marketing staff
```

請注意，nsManagedRoleDefinition 物件類別繼承自 LDAPsubentry、nsRoleDefinition 和 nsSimpleRoleDefinition 物件類別。

利用下列 ldapmodify 指令更新名爲 Bob 之行銷人員成員的項目，將角色指派給他：

```
ldapmodify -h host -p port -D "cn=Directory Manager" -w secret
dn:cn=Bob Arnold,ou=marketing,ou=People,dc=example,dc=com
changetype:modify
add:nsRoleDN
nsRoleDN:cn=Marketing,ou=marketing,ou=People,dc=example,dc=com
```

項目中出現 nsRoleDN 屬性，表示該項目是由其角色定義的 DN 所識別之受管理角色的成員。若要允許使用者修改他們自己的 nsRoleDN 屬性，但要防止使用者加入或移除 nsManagedDisabledRole，請加入下列存取控制指令 (ACI)：

```
aci:(targetattr="nsRoleDN")(targattrfilters="add=nsRoleDN:
 (!(nsRoleDN=cn=AdministratorRole,dc=example,dc=com)),
 del=nsRoleDN:(!(nsRoleDN=cn=nsManagedDisabledRole,dc=example,
 dc=com)")(version3.0;aci "allow mod of nsRoleDN by self except
 for critical values"; allow(write) userdn="ldap:///self";)
```

### 篩選角色定義的範例

若要爲業務經理設定篩選的角色，假設他們都有 isManager 屬性，請執行下列 ldapmodify 指令：

```
ldapmodify -a -h host -p port -D "cn=Directory Manager" -w password
dn:cn=ManagerFilter,ou=sales,ou=People,dc=example,dc=com
objectclass:top
objectclass:LDAPsubentry
objectclass:nsRoleDefinition
objectclass:nsComplexRoleDefinition
objectclass:nsFilteredRoleDefinition
cn:ManagerFilter
nsRoleFilter:(isManager=True)
Description:filtered role for sales managers
```

請注意，nsFilteredRoleDefinition 物件類別繼承自 LDAPsubentry、nsRoleDefinition 和 nsComplexRoleDefinition 物件類別。nsRoleFilter 屬性指定一個篩選器，可找出 ou=sales 組織中所有有下屬的員工，例如：

```
ldapsearch -h host -p port -D "cn=Directory Manager" -w password \
-b "ou=People,dc=example,dc=com" -s sub "(cn=*Fuentes)"
dn:cn=Carla Fuentes,ou=sales,ou=People,dc=example,dc=com
cn:Carla Fuentes
isManager:TRUE
...
nsRole:cn=ManagerFilter,ou=sales,ou=People,dc=example,dc=com
```

**備註** 篩選角色的篩選字串可以用任何屬性爲基礎，但是由 CoS 機制所產生的虛擬屬性除外 ( 參閱第 165 頁「關於 CoS」 )。

當篩選角色成員爲使用者項目時，您可以用存取控制指令 (ACI) 來保護篩選屬性，以限制篩選角色將他自己加入角色或從角色中移除的能力。

### 巢式角色定義的範例

使用 `nsRoleDN` 屬性來指定巢居於巢式角色內的角色。若要建立一個角色，此角色同時包含在上述幾個範例中所建立的行銷人員和業務經理角色的成員，請使用下列指令：

```
ldapmodify -a -h host -p port -D "cn=Directory Manager" -w password
dn:cn=MarketingSales,ou=marketing,ou=People,dc=example,dc=com
objectclass:top
objectclass:LDAPsubentry
objectclass:nsRoleDefinition
objectclass:nsComplexRoleDefinition
objectclass:nsNestedRoleDefinition
cn:MarketingSales
nsRoleDN:cn=ManagerFilter,ou=sales,ou=People,dc=example,dc=com
nsRoleDN:cn=Marketing,ou=marketing,ou=People,dc=example,dc=com
nsRoleScopeDN:ou=sales,ou=People,dc=example,dc=com
```

請注意，`nsNestedRoleDefinition` 物件類別繼承自 `LDAPsubentry`、`nsRoleDefinition` 和 `nsComplexRoleDefinition` 物件類別。`nsRoleDN` 屬性包含行銷的受管理角色和業務經理之篩選角色的 DN。上述幾個範例中的兩個使用者 Bob 和 Carla 成爲這個新巢式角色的成員。

此篩選器的範圍包括預設的範圍 ( 即篩選器所在的樹狀子目錄 )，以及在任何 `nsRoleScopeDN` 屬性值之下的樹狀子目錄。在此範例中，`ManagerFilter` 位於 `ou=sales,ou=People,dc=example,dc=com` 樹狀子目錄中，而且此樹狀子目錄必須加入範圍內。

## 定義服務類別 (CoS)

服務類別 (CoS) 機制會在爲用戶端應用程式擷取項目時，產生虛擬屬性。CoS 簡化了項目管理作業並減少儲存體的需求。

在使用群組和角色時，CoS 會依賴目錄中的說明項目，此外也可以透過主控台或指令行來設定 CoS。下一節描述 CoS，並說明以這兩種方法管理 CoS 的程序。

**備註** 任何搜尋作業均可測試 CoS 所產生的屬性是否存在或比較其值。虛擬屬性的名稱可以用在任何篩選字串中，不論是用於用戶端搜尋作業或用於篩選角色的內部篩選器中。Directory Server 也支援 VLV ( 虛擬清單檢視 ) 作業和伺服器端排序控制中的虛擬屬性，如同任何真實屬性一般。

# 關於 CoS

CoS 可爲 CoS 範圍內的任何項目定義虛擬屬性及其值，稱爲*目標項目*。每個 CoS 都包含下列目錄中的項目：

- CoS 定義項目 - 識別目前使用的 CoS 類型，以及所產生的 CoS 屬性名稱。如同角色定義項目，此項目是繼承自 `LDAPsubentry` 物件類別，CoS 的範圍是 CoS 定義項目父項之下的整個樹狀子目錄。同一個 CoS 屬性可能會有多個定義，因此可能會有多重值。
- 範本項目 - 含有一或多個虛擬屬性值，在 CoS 範圍內的所有項目都將使用此處所定義的值。在所產生的值可能是多重值時，也可能會有多個範本項目。

CoS 有三種類型，每一種類型會分別與 CoS 定義和範本項目之間不同的互動方式對應：

- 指標 CoS - CoS 定義項目會直接使用其 DN 來識別範本項目。所有目標項目均擁有與範本中所指定相同的 CoS 屬性值。
- 間接 CoS - CoS 定義會識別稱爲間接規範的屬性，間接規範在目標項目中的值必須包含範本的 DN。使用間接 CoS 時，每個目標項目可能會使用不同的範本，因此會有不同的 CoS 屬性值。
- 典型 CoS - CoS 定義會識別範本和規範的 Base DN，其中規範是屬性在目標項目中的名稱。規範屬性必須包含 RDN ( 相對網域名稱 )，當 RDN 與範本 Base DN 結合時，可決定範本是否包含 CoS 值。

CoS 定義項目是 `cosSuperDefinition` 物件類別的實例，並且也繼承自下列其中一個物件類別以指定 CoS 類型：

- `cosPointerDefinition`
- `cosIndirectDefinition`
- `cosClassicDefinition`

CoS 定義項目包含每個 CoS 類型特有的屬性，可視需要用於爲目標項目內的虛擬 CoS 屬性、範本 DN 和規範屬性命名。依預設值，CoS 機制不會使用與 CoS 屬性相同的名稱覆寫現有屬性的值。但是，CoS definition entry 的語法可讓您控制此行爲。

CoS 範本項目是 `cosTemplate` 物件類別的實例。CoS 範本項目包含 CoS 機制所產生屬性的值，所指定 CoS 的範本項目儲存在與 CoS 定義同一層的樹狀目錄中。

如果可能的話，定義和範本項目應該位於相同的位置以便於管理。同時，您應該使用能表示其功能的名稱爲它們命名。例如，定義項目 DN，如 `cn=ClCosGenerateEmployeeType,ou=People,dc=example,dc=com` 就比 `cn=ClassicCos1,ou=People,dc=example,dc=com` 更具描述性。

《Directory Server Deployment Planning Guide》Chapter 4 "Managing Attributes with Class of Service" 更詳細描述每個 CoS 類型，並提供範例和部署考量。如需關於物件類別和與各 CoS 類型相關屬性的詳細資訊，請參閱第 170 頁「從指令行管理 CoS」。

# CoS 限制

CoS 定義和範例項目的建立與管理，需符合下列限制：有關部署 CoS 虛擬屬性進一步限制的說明，請參閱 《Directory Server Deployment Planning Guide》 Chapter 4 "CoS Limitations"。

**無法爲與 CoS 所產生屬性有關的搜尋編製索引。**任何搜尋篩選器可能會測試虛擬屬性是否存在或比較它的值。*但是*，系統無法爲虛擬屬性編製索引，且任何與 CoS 所產生屬性相關的篩選器元件均會導致無法索引的搜尋，這對效能有很大的影響。請注意，Directory Server 5.2 引進雜湊表，以超過十種典型的 CoS 範本項目，加速在結構上的搜尋。預設爲啓用此 facility。如需有關如何停用此 facility 的資訊，請參閱 《Directory Server Administration Reference》 Chapter 2 "Class of Service Plug-in"。

**受限制的樹狀子目錄。**您無法在 cn=config 或 cn=schema 樹狀子目錄中建立 CoS 定義。因此，這些項目不會包含虛擬屬性。

**受限制的屬性類型。**您不可以用 CoS 機制產生下列屬性類型，因爲它們不會擁有與相同名稱之真實屬性一樣的行爲：

- `userPassword` - CoS 產生的密碼值無法用來連結目錄伺服器。
- `aci` - 目錄伺服器無法根據 CoS 所定義之虛擬 ACI 值的內容，套用任何存取控制。

- `objectclass` - 目錄伺服器將不會對 CoS 所定義的虛擬物件類別的值執行結構檢查。
- `nsRoleDN` - 伺服器不會使用 CoS 所產生的 `nsRoleDN` 值來產生角色。

**不支援屬性子類型。**CoS 機制不會產生含子類型 ( 如語言或 ;binary) 的屬性。

**真實和虛擬的屬性值。**CoS 機制永遠不會產生多重值屬性，此屬性同時含有項目中所定義的「真實」屬性值，以及 CoS 範本所定義的「虛擬」屬性值。屬性值可以是儲存在項目中的值，或是 CoS 機制所產生的值，如 「覆寫真實屬性值」和第 172 頁「多重值 CoS 屬性」中所描述。

**所有範本都必須在本機上。** 範本項目的 DN，不論是在 CoS 定義或目標項目的規範中，都必須參照目錄伺服器中的本機項目。它們所包含的範本和值，無法透過目錄鏈接或參照來擷取。

# 使用主控台管理 CoS

本節描述如何透過 Directory Server Console 建立和編輯 CoS 定義。

此外，如果您的 CoS 值需要安全性，您應該爲 CoS 定義、範本項目、與目標項目中的規範屬性定義存取控制指令 (ACI)。如需 CoS 安全性考量的資訊，請參閱《Directory Server Deployment Planning Guide》 Chapter 7 "Using CoS Securely"。如需使用主控台建立 ACI 的程序，請參閱第 6 章「管理存取控制」。

## 建立新的 CoS

使用指標 CoS 和典型 CoS 時，在定義項目之前您必須先建立範本項目：

1. 在 Directory Server Console 最上層的 [ 目錄 ] 標籤上，在樹狀目錄內您想要加入新範本項目的項目上，按一下滑鼠右鍵，並選取 [ 新增 ] > [ 其他 ] 項目。

   或者，選取父項，再從 [ 物件 ] 選單中選取 [ 新增 ] > [ 其他 ] 項目。

2. 在 [ 新物件 ] 對話方塊中，選取物件類別清單中的 `costemplate`。開啓 [ 標準編輯器 ] 對話方塊，顯示新範本中特定屬性的預設值。

3. 依照下列方式編輯新範本物件：

   a. 將 `LDAPsubentry` 和 `extensibleobject` 值加入 `objectclass` 屬性。

   b. 加入 `cn` 屬性，並指定可識別範本的值，例如 `cosTemplateForHeadquartersFax`。

c. 將命名屬性變更爲新的 cn 屬性。

   您可以加入其他任何屬性，並改用它作爲命名屬性，但一般都使用 cn。

d. 修改 cosPriority 屬性：將它設定成整數值，或移除優先權屬性 ( 如果不再需要的話 )。如需詳細資訊，請參閱第 173 頁「Cos 屬性優先權」。

e. 加入您希望用 CoS 機制在目標項目上產生的屬性及其屬性值。

4. 在 [ 標準編輯器 ] 對話方塊中按一下 [ 確定 ] 以建立範本項目。

5. 如您正在定義此範本的指標 CoS，請選取樹狀目錄中的新範本項目，然後選取功能表中的 [ 編輯 ] > [ 複製 DN]。

CoS 所有類型建立定義項目的程序均相同：

1. 在 Directory Server 主控台最上層的 [ 目錄 ] 標籤上，在樹狀目錄內您想要加入新 CoS 定義的項目上，按一下滑鼠右鍵，並選取快顯功能表上的 [ 新增 ] > [ 服務類別 ] 項目。

   或者，選取父項，再從 [ 物件 ] 選單中選取 [ 新增 ] > [ 服務類別 ] 項目。

   顯示 [ 服務類別 ] 項目的自訂編輯器。

2. 爲新的服務類別輸入名稱和選用描述。該名稱將顯示在 CoS 定義項目的 cn 命名屬性中。

3. 按一下左清單中的 [ 屬性 ] 標籤，對話方塊會顯示將由 CoS 機制在目標項目上產生的屬性清單。

   按一下 [ 加入 ] 瀏覽可能屬性的清單，並將它們加入清單中。

4. 一旦您將屬性加入清單後，[ 服務類別行爲 ] 欄中會有一個下拉式清單。按一下這個儲存格以選取覆寫行爲：

   - **不要覆寫目標項目屬性** - 只有當目標項目的相同屬性中已經沒有儲存對應的屬性值時，才會產生 CoS 屬性值。
   - **覆寫目標項目屬性** - 由 CoS 所產生的屬性值將複製目標項目中屬性的任何值。
   - **覆寫目標項目屬性，而且可操作** - 屬性會複製任何目標值且操作正常，因此除非明確地要求，否則此屬性對用戶端應用程式而言是隱藏的。

**備註** 如果在結構中也將屬性定義爲操作性，您就只能讓屬性成爲操作性。

5. 合併欄含有合併結構的核取方塊。選擇此核取方塊，允許此 CoS 屬性與相同屬性的其他 CoS 值合併。但是，CoS 屬性永遠都不會與現有值合併，它不是取代現有值，就是根據前一欄的定義而不產生。

6. 按一下左清單中的 [ 範本 ] 標籤，選取識別範本項目的方式，然後填寫對應的欄位。這將決定您希望定義的 CoS 類型。

   - **依 DN** - 此選項將定義指標 CoS：在 [ 範本 DN] 欄位中輸入範本項目的 DN。按一下 [ 瀏覽 ] 從目錄中選取範本 DN，或按 Ctrl-V 貼上您在建立範本項目後所複製的 DN。
   - **使用其中一個目標項目屬性的值** - 此選項將定義間接的 CoS：在 [ 屬性名稱 ] 欄位中輸入規範屬性的名稱，一定要選取含 DN 值的屬性。按一下 [ 變更 ] 選取清單中的屬性。
   - **使用其中一個目標項目屬性的 DN 和值** - 此選項將定義典型的 CoS：輸入範本的 Base DN 和屬性名稱。按一下 [ 瀏覽 ] 選取可能目標項目的父項目，並按一下 [ 變更 ] 選取清單中的屬性。

7. 按一下 [ 確定 ] 建立 CoS 定義項目。

## 編輯現有的 CoS

1. 在 Directory Server Console 最上層的 [ 目錄 ] 標籤上，連按兩下 CoS 定義項目，或在 CoS 定義項目上按一下滑鼠右鍵，再從快顯功能表中選取 [ 用自訂編輯器編輯 ]。

   顯示 [ 服務類別 ] 項目的自訂編輯器。

2. 依需要編輯名稱和描述欄位。

3. 按一下左清單中的 [ 屬性 ] 標籤，以新增或移除由 CoS 機制產生的虛擬屬性。

4. 按一下左清單中的 [ 範本 ] 標籤，重新定義範本規範屬性的名稱或範本項目 DN。這個對話方塊也可以用來重新定義 CoS 定義的類型。

5. 按一下 [ 確定 ] 儲存您的變更。

## 刪除 CoS

1. 在 Directory Server Console 最上層的 [ 目錄 ] 標籤上，瀏覽樹狀目錄，以顯示 CoS 定義項目。

2. 在 CoS 項目上按一下滑鼠右鍵，並從快顯功能表中選取 [ 刪除 ]。顯示對話方塊要求您確認刪除。按一下 [ 是 ]。

# 從指令行管理 CoS

由於所有組態資訊和範本資料都儲存成目錄中的項目，因此您可以使用 LDAP 指令行工具來配置及管理您的 CoS 定義。本節將示範如何從指令行建立 CoS 定義和範本項目。

此外，如果您的 CoS 值需要安全性，您應該爲 CoS 定義、範本項目、與目標項目中的規範屬性定義存取控制指令 (ACI)。如需 CoS 安全性考量的資訊，請參閱《Directory Server Deployment Planning Guide》第 7 章「安全地使用 CoS」。如需從指令行建立 ACI 的程序，請參閱 「第 6 章「管理存取控制」。

## 從指令行建立 CoS 定義項目

所有 CoS 定義項目都有 `LDAPsubentry` 物件類別，而且繼承自 `cosSuperDefinition` 物件類別。此外，每一個 CoS 類型均繼承自特定的物件類別，且包含對應的屬性。下表列出與每一類 CoS 定義項目相關的物件類別和屬性：

**表 5-2** CoS 定義項目中的物件類別與屬性

| CoS 類型 | CoS 定義項目 |
|---|---|
| 指標 CoS | `objectclass:top`<br>`objectclass:LDAPsubentry`<br>`objectclass:cosSuperDefinition`<br>`objectclass:cosPointerDefinition`<br>`cosTemplateDN:`*DN*<br>`cosAttribute:`*attributeName override merge* |
| 間接 CoS | `objectclass:top`<br>`objectclass:LDAPsubentry`<br>`objectclass:cosSuperDefinition`<br>`objectclass:cosIndirectDefinition`<br>`cosIndirectSpecifier:` *attributeName*<br>`cosAttribute:`*attributeName override merge* |
| 典型 CoS | `objectclass:top`<br>`objectclass:LDAPsubentry`<br>`objectclass:cosSuperDefinition`<br>`objectclass:cosClassicDefinition`<br>`cosTemplateDN:`*DN*<br>`cosSpecifier:` *attributeName*<br>`cosAttribute:`*attributeName override merge* |

在所有情況中，`cosAttribute` 都是多重值，每個值各定義一個即將由 CoS 機制產生的屬性。

您可以使用下列 CoS 定義項目中的屬性 ( 如需關於這些屬性的詳細資訊，請參閱《Directory Server Administration Reference》Chapter 10 "Attribute Reference")：

**表 5-3** CoS 定義項目屬性

| 屬性 | CoS 定義項目的目的 |
| --- | --- |
| `cosAttribute:` *attributeName override merge* | 定義您要產生屬性值之虛擬屬性的名稱。這個屬性有多重值，每個值分別代表其屬性值是由範本產生之屬性的名稱。*override* 和 *merge* 辨識符號指定在下表所述的特殊案例中計算 CoS 屬性值的方式。<br><br>*attributeName* 不可包含任何子類型。有子類型的屬性名稱會被忽略，但仍會處理 `cosAttribute` 的其他值。 |
| `cosIndirectSpecifier:` *attributeName* | 定義目標項目中屬性的名稱，間接 CoS 會使用此屬性值來識別範本項目。命名的屬性稱爲規範，且必須在每個目標項目中包含完整的 DN 字串。此屬性爲單值，但是規範屬性可以是多值以指定多個範本。 |
| `cosSpecifier:` *attributeName* | 定義目標項目中屬性的名稱，典型 CoS 會使用此屬性值來識別範本項目。命名的屬性稱爲規範，且必須包含可以在 RDN 範本項目中找到的字串。此屬性爲單值，但是規範屬性可以是多值以指定多個範本。 |
| `cosTemplateDN:` *DN* | 請在指標 CoS 定義中輸入範本項目的完整 DN，或在典型 CoS 定義中輸入範本項目的 Base DN。 |

`cosAttribute` 屬性允許在 CoS 屬性的名稱後加上兩個辨識符號。*override* 辨識符號具有下列其中一個值：

- `default` (也就是沒有辨識符號) - 表示當真實屬性值的類型與虛擬屬性值的類型相同時，伺服器不會覆寫儲存在項目中的真實屬性值。
- `override` - 表示伺服器一定會傳回 CoS 所產生的值，即使有值儲存於該項目內仍會傳回。
- `operational` - 表示只有當搜尋中有明確要求時，才會傳回屬性。操作性屬性並不需要通過結構檢查就可以傳回。同時此屬性的行爲也與 `override` 辨識符號相同。

  如果在結構中也將屬性定義爲操作性，您就只能讓屬性成爲操作性。例如，如果您的 CoS 產生 `description` 屬性的值，但因爲此屬性在結構中沒有標示操作性，所以您無法使用 `operational` 辨識符號。

下列的值可以包含或不包含 *merge* 辨識符號：

- `merge-schemes` - 允許虛擬 CoS 屬性成爲多重值屬性，您可以從多個範本或多個 CoS 定義來指定。如需詳細資訊，請參閱第 172 頁「多重值 CoS 屬性」。

### 覆寫「真實」屬性值

您可以建立含有 override 辨識符號的 CoS 定義項目，方法如下：

```
dn:cn=pointerCoS,dc=example,dc=com
objectclass:top
objectclass:LDAPsubentry
objectclass:cosSuperDefinition
objectclass:cosPointerDefinition
cosTemplateDn:cn=exampleUS,cn=data
cosAttribute:postalCode override
```

此指標 CoS 定義項目表示該項目與產生 postalCode 屬性值的範本項目 cn=exampleUS,cn=data 有關聯。覆寫辨識符號表示此值的優先權高於 postalCode 屬性的值 ( 如果目標項目中有此屬性值的話 )。

**備註** 如果 CoS 屬性是用操作性或覆寫辨識符號來定義的，則您將無法在 CoS 範圍內任何項目中，對該屬性的「真實」值執行寫入作業。

### 多重值 CoS 屬性

當您指定 merge-schemes 辨識符號時，所產生的 CoS 屬性可能是多重值屬性。CoS 屬性成爲多重值的方式有兩種：

- 使用間接或典型 CoS 時，目標項目中的規範屬性是多重值。此時，每個值會決定一個範本，每個範本的值是所產生值的一部份。
- 任何一種類型的多個 CoS 定義項目在它們的 cosAttribute 中，可以有相同的屬性名稱。此時，如果所有定義都含有 merge-schemes 辨識符號，則產生的屬性將包含所有每個定義所計算出來的值。

這兩種情況可能同時發生，並且甚至定義更多的值。但是在所有的情況中，產生屬性中的重複值將只會傳回一次。

當沒有 merge-schemes 辨識符號時，系統會使用範本項目的 cosPriority 屬性來決定產生屬性之所有範本中的單值，如下一節所描述。

merge-schemes 辨識符號時絕不會將目標中所定義的「真實」屬性值，與範本所產生的屬性值合併。*merge* 辨識符號與 *override* 辨識符號無關，所有組合都有可能，並且允許每種組合所默許的行爲。同時，您可以在屬性名稱後以任何順序指定辨識符號。

**備註** 當同一屬性有多個 CoS 定義時，這些定義必須均擁有相同的 *override* 與 *merge* 辨識符號。當 CoS 定義中出現不同的辨識符號組時，系統會在所有定義中隨意選取其中一個組合。

## Cos 屬性優先權

如果有多個 CoS 定義或多重值規範，但沒有 `merge-schemes` 辨識符號，則 Directory Server 會使用優先權屬性選取定義虛擬屬性單值的單一範本。

`cosPriority` 屬性代表在所有考慮範本中特定範本的全域優先權。優先權爲零代表最高優先權。沒有 `cosPriority` 屬性的範本則視爲最低優先權。當有兩個或以上的範本提供屬性值但卻擁有相同 ( 或沒有 ) 優先權時，系統會任意選取一個值。

當使用 `merge-schemes` 辨識符號時，並不會考慮範本的優先權。當合併時，不論範本定義的優先權爲何，所有考慮的範本皆會定義一個值。`cosPriority` 屬性是在 CoS 範本項目中定義，如下一節所描述。

**備註** `cosPriority` 屬性值必定不爲負值。而且，由間接 CoS 所產生的屬性不支援優先權。請勿在間接 CoS 定義的範本項目中使用 `cosPriority`。

## 從指令行建立 CoS 範本項目

使用指標 CoS 或典型 CoS 時，範本項目會包含 `LDAPsubentry` 和 `cosTemplate` 物件類別。必須特別爲 CoS 定義建立這個項目。將 CoS 範本項目設定成 `LDAPsubentry` 物件類別的實例，可允許執行一般的搜尋，而不受組態項目的阻止。

間接 CoS 機制的範本是目錄中現有的任意項目。目標不須預先識別，也不須指定 `LDAPsubentry` 物件類別，但它必須擁有輔助的 `cosTemplate` 物件類別。只有在評估 CoS 以產生虛擬屬性及屬性值時，才存取間接 CoS 範本。

不論在什麼情況下，CoS 範本項目都必須含有 CoS 在目標項目中所產生的屬性與屬性值。其屬性名稱是在 CoS 定義項目的 `cosAttribute` 屬性中指定。

下列範例顯示會產生 `postalCode` 屬性的指標 CoS 最高優先權的範本項目：

```
dn:cn=ZipTemplate,ou=People,dc=example,dc=com
objectclass:top
objectclass:LDAPsubentry
objectclass:extensibleobject
objectclass:cosTemplate
postalCode: 95054
cosPriority: 0
```

下一節提供範本項目的範例，以及每一種 CoS 定義項目類型的範例。

## 指標 CoS 的範例

下列指令會建立含有 `cosPointerDefinition` 物件類別的指標 CoS 定義項目。此定義項目使用以上指定的 CoS 範本項目，以便與 `ou=People,dc=example,dc=com` 樹狀目錄中的所有項目共用一般郵遞區號。

```
ldapmodify -a -h host -p port -D "cn=Directory Manager" -w password
dn:cn=pointerCoS,ou=People,dc=example,dc=com
objectclass:top
objectclass:LDAPsubentry
objectclass:cosSuperDefinition
objectclass:cosPointerDefinition
cosTemplateDn:cn=ZipTemplate,ou=People,dc=example,dc=com
cosAttribute:postalCode
```

CoS 範本項目 (`cn=ZipTemplate,ou=People,dc=example,dc=com`) 將儲存在它的 `postalCode` 屬性中的值提供給 `ou=People,dc=example,dc=com` 尾碼下的所有項目。如果在同一樹狀子目錄中搜尋任何沒有郵遞區號的項目，您就會看到產生的屬性值：

```
ldapsearch -h host -p port -D "cn=Directory Manager" -w password \
-b "ou=People,dc=example,dc=com" -s sub "(cn=*Jensen)"
dn:cn=Babs Jensen,ou=People,dc=example,dc=com
cn:Babs Jensen
...
postalCode: 95054
```

## 間接 CoS 的範例

間接 CoS 爲 `cosIndirectSpecifier` 屬性中的值命名，以找出每個目標特定的範本。這個間接 CoS 使用目標項目的 `manager` 屬性來識別 CoS 範本項目。範本項目是管理員的使用者項目，而且它必須包含要產生的屬性值。

下列指令建立包含 `cosIndirectDefinition` 物件類別的間接 CoS 定義項目：

```
ldapmodify -a -h host -p port -D "cn=Directory Manager" -w password
dn:cn=generateDeptNum,ou=People,dc=example,dc=com
objectclass:top
objectclass:LDAPsubentry
objectclass:cosSuperDefinition
objectclass:cosIndirectDefinition
cosIndirectSpecifier:manager
cosAttribute:departmentNumber
```

接下來，將 `cosTemplate` 物件類別加入範本項目，並確定它們定義了即將產生的屬性。在此範例中，所有管理員項目都將是範本：

```
ldapmodify -h host -p port -D "cn=Directory Manager" -w password
dn:cn=Carla Fuentes,ou=People,dc=example,dc=com
changetype:modify
add:objectclass
objectclass:cosTemplate
-
add:departmentNumber
departmentNumber: 318842
```

使用此 CoS 時，包含 `manager` 屬性的目標項目 (`ou=People,dc=example,dc=com` 下的項目 ) 會自動具有其管理員的部門編號。`departmentNumber` 屬性在目標屬性上是虛擬的，因爲它不存在於伺服器中，但它會作爲目錄項目的一部分傳回。例如，如果 Babs Jensen 的管理員定義爲 Carla Fuentes，則他的部門編號將是：

```
ldapsearch -h host -p port -D "cn=Directory Manager" -w password \
-b "ou=People,dc=example,dc=com" -s sub "(cn=*Jensen)"
dn:cn=Babs Jensen,ou=People,dc=example,dc=com
cn:Babs Jensen
...
manager:cn=Carla Fuentes,ou=People,dc=example,dc=com
departmentNumber: 318842
```

### 典型 CoS 的範例

此範例顯示如何用典型 CoS 產生郵遞區號。產生的值由範本項目指定，該項目是結合 CoS 定義中的 `cosTemplateDN` 和目標項目中 `cosSpecifier` 屬性的值。下列指令使用 `cosClassicDefinition` 物件類別建立定義項目：

```
ldapmodify -a -h host -p port -D "cn=Directory Manager" -w password
dn:cn=classicCoS,dc=example,dc=com
objectclass:top
objectclass:LDAPsubentry
objectclass:cosSuperDefinition
```

```
objectclass:cosClassicDefinition
cosTemplateDn:ou=People,dc=example,dc=com
cosSpecifier:building
cosAttribute:postalAddress
```

繼續使用同一個指令，建立範本項目，來爲每棟建築指定郵遞區號：

```
dn:cn=B07,ou=People,dc=example,dc=com
objectclass:top
objectclass:LDAPsubentry
objectclass:extensibleobject
objectclass:cosTemplate
postalAddres:7 Old Oak Street$Anytown, CA 95054
```

使用此 CoS 時，包含 `building` 屬性的目標項目 (`ou=People,dc=example,dc=com` 下的項目 ) 會自動具有對應的郵遞區號。CoS 機制會搜尋其 RDN 中具有規範屬性值的範本項目。在此範例中，如果 Babs Jensen 被指派到 B07 大樓，則他的郵寄地址會產生如下：

```
ldapsearch -h host -p port -D "cn=Directory Manager" -w password \
-b "ou=People,dc=example,dc=com" -s sub "(cn=*Jensen)"
dn:cn=Babs Jensen,ou=People,dc=example,dc=com
cn:Babs Jensen
...
building:B07
postalAddress:7 Old Oak Street$Anytown, CA 95054
```

## 建立以角色爲基礎的屬性

您可以根據項目所擁有的角色，建立會產生項目屬性值的典型 CoS 結構。例如，您可以使用以角色爲基礎的屬性，逐項目設定伺服器的透視限制。

若要建立以角色爲基礎的屬性，請使用 `nsRole` 屬性作爲典型 CoS 之 CoS 定義項目中的 `cosSpecifier`。因爲 `nsRole` 屬性可以有多重值，所以您可以定義擁有一個以上可能範本項目的 CoS 結構。爲解決範本項目使用時模稜兩可的情況，您可以在 CoS 範本項目中加入 `cosPriority` 屬性。

例如，您可以建立允許管理員角色成員的 CoS，以超出標準郵件信箱的額度限制。管理員角色如下所示：

```
dn:cn=ManagerRole,ou=People,dc=example,dc=com
objectclass:top
objectclass:LDAPsubentry
objectclass:nsRoleDefinition
objectclass:nsComplexRoleDefinition
```

```
objectclass:nsFilteredRoleDefinition
cn:ManagerRole
nsRoleFilter:(isManager=True)
Description:filtered role for managers
```

典型 CoS 定義項目將以下列方式建立：

```
dn:cn=generateManagerQuota,ou=People,dc=example,dc=com
objectclass:top
objectclass:LDAPsubentry
objectclass:cosSuperDefinition
objectclass:cosClassicDefinition
cosTemplateDn:cn=managerCOS,dc=example,dc=com
cosSpecifier:nsRole
cosAttribute:mailboxquota override
```

CoS 範本名稱必須結合 `cosTemplateDn` 和 `nsRole` ( 這是角色的 DN) 的值。例如：

```
dn:cn="cn=ManagerRole,ou=People,dc=example,dc=com",ou=People,
 dc=example,dc=com
objectclass:top
objectclass:LDAPsubentry
objectclass:extensibleobject
objectclass:cosTemplate
mailboxquota: 1000000
```

CoS 範本項目提供 `mailboxquota` 屬性值。其他的 `override` 辨識符號會告訴 CoS 覆寫目標項目中任何現有的 `mailboxquota` 屬性。目標項目若是角色的成員，將擁有由角色以及由 CoS 產生的虛擬屬性，例如：

```
ldapsearch -h host -p port -D "cn=Directory Manager" -w password \
-b "ou=People,dc=example,dc=com" -s sub "(cn=*Fuentes)"
dn:cn=Carla Fuentes,ou=People,dc=example,dc=com
cn:Carla Fuentes
isManager:TRUE
...
nsRole:cn=ManagerRole,ou=People,dc=example,dc=com
mailboxquota: 1000000
```

**備註** 角色項目和 CoS 定義項目應該位在樹狀目錄中的同一位置上，如此它們在其範圍內才會有相同的目標項目。CoS 目標項目也應該位在相同的位置，以方便尋找和維護。

# 監視 CoS Plug-in

Directory Server 5.2 可讓您監視 CoS Plug-in 的特定方面。CoS 監視屬性保留在 `cn=monitor,cn=Class of Service,cn=plugins,cn=config` 項目之下。如需有關這些屬性以及他們所提供資訊的詳細資料，請參閱 《Directory Server Administration Reference》Chapter 2 "cn=monitor,cn=Class of Service,cn=plugins, cn=config"。

第 6 章

# 管理存取控制

控制存取您的目錄內容是建立安全目錄不可或缺的一部份。本章說明存取控制指令 (ACI)，它可決定授與存取目錄的使用者哪一種權限。Directory Server 包含新的功能，可檢視指定使用者對指定項目擁有的有效權利。此功能可將管理複雜且功能強大之存取控制機制的作業簡化。

在目錄部署的計畫階段時，應該定義符合整體安全政策的存取控制策略。如需關於規劃存取控制策略的提示，請參閱 《Directory Server Deployment Planning Guide》 Chapter 7 "Designing Access Control"。

本章包含下列主題：

# 存取控制策略

定義存取權的機制稱爲*存取控制*。當伺服器收到要求時，它會使用使用者在連結作業中所提供的驗證資訊，以及伺服器中定義的存取控制指令 (ACI)，來允許或拒絕存取目錄資訊。伺服器可允許或拒絕權限，例如讀取、寫入、搜尋或比較。授與使用者的權限層級可能因所提供的驗證資訊不同而有所差異。

使用存取控制，您便可以控制存取整個目錄、目錄的樹狀子目錄、目錄中的特定項目 ( 包括定義組態工作的項目 )、特定的項目屬性組或特定的項目屬性值。可以設定特定使用者的權限、屬於特定群組或角色的所有使用者權限、或目錄中所有使用者的權限。最後，可以定義以 IP 位址或 DNS 名稱識別的特定用戶端的存取權。

## ACI 結構

控制存取指令以項目屬性的方式儲存在目錄中。`aci` 屬性是操作屬性；它可供目錄中的每個項目使用，不論項目的物件類別是否已定義此屬性。目錄伺服器在收到來自用戶端的 LDAP 要求時，Directory Server 會使用此屬性來評估要授與或拒絕的權利。如果有特別的要求，`ldapsearch` 作業中會傳回 `aci` 屬性。

ACI 陳述式分爲三個主要部分：

- 目標 - 決定將套用權限的項目或屬性。
- 權限 - 定義允許或拒絕的作業。
- 連結規則 - 決定誰會因爲其連結 DN 而被 ACI 限制。

ACI 的權限與連結規則部分的設定是採用配對方式，這些配對也稱爲存取控制規則 (ACR)。系統會根據伴隨指定權限的規則是否被評估爲正確，來決定授與或拒絕存取目標的指定權限。如需詳細資訊，請參閱第 183 頁「ACI 語法」。

## ACI 位置

如果包含 ACI 的項目中沒有任何子項目，則 ACI 僅套用在該項目；如果項目中有子項目，則 ACI 會套用在項目本身及其下所有的項目。因此，當伺服器評估任何指定項目的存取權限時，它會確認要求的項目與其根尾碼的基礎之間每個項目的 ACI。

`aci` 屬性是多重值屬性，這表示您可以爲同一個項目或樹狀子目錄定義多個 ACI。

您在項目上建立的 ACI 不會直接套用在該項目上，而是套用該項目之下的樹狀子目錄中的部份或全部項目。這樣做的優點在於，您可以在樹狀目錄高層訂定一般性的 ACI，讓 ACI 可以有效地套用於位在樹狀目錄下層的項目。例如，可以在 `organizationalUnit` 項目或 `locality` 項目的層級建立 ACI，此 ACI 的目標是包含 `inetorgperson` 物件類別的項目。

可以利用此功能在高層的分支點上訂定一般性規則，使目錄中的 ACI 數目減到最低。若要限制更特殊規則的範圍，您應該儘可能地將規則放在離葉項目最近的位置。

**備註** 放在根 DSE 項目 ( 含 DN "") 的 ACI 只套用在該項目。

# ACI 評估

爲了評估特定項目的存取權利，伺服器會編譯一份 ACI 清單，這些 ACI 存在於項目本身上，以及存在於可向項目根尾碼的基礎回溯的父項目上。評估期間，伺服器會依此順序處理 ACI；ACI 的評估會在項目及其根尾碼基礎間的所有尾碼和子尾碼中進行，而不在其他伺服器的鏈接尾碼之間進行。

**備註** 目錄管理員是唯一沒有套用存取控制，但具有權限的使用者。當用戶端以目錄管理員身份與目錄連結後，伺服器在執行作業之前不會評估任何 ACI。

因此，以目錄管理員執行 LDAP 作業的效能是無法與其他使用者的預期效能相提並論的。您應該要以一般使用者身份測試目錄效能。

依預設值，項目若沒有 ACI 可套用，則除了目錄管理員外，將拒絕所有使用者存取。必須由 ACI 明確授與存取權限，使用者才能存取伺服器中的任何項目。預設 ACI 定義匿名讀取存取，並允許使用者修改他們自己的項目，但維護安全性所需的屬性除外。如需詳細資訊，請參閱第 182 頁「預設 ACI」。

雖然伺服器優先執行最接近目標項目的 ACI，但套用至項目的所有 ACI 的影響是累積的。除非有任何一個 ACI 拒絕由 ACI 授與的存取權限，否則系統會允許該存取權限。拒絕存取的 ACI ( 不論出現在清單何處 )，其優先順序均高於允許存取同一資源的 ACI。

例如，如果您拒絕在目錄根層級中的寫入權限，則無論您是否授與任何特定的權限，任何使用者都無法寫入目錄。若要將目錄的寫入權限授與特定使用者，必須限制寫入權限的原始拒絕範圍，使它不包含該使用者。

## ACI 限制

爲目錄服務建立存取控制策略時，您必須知道下列限制：

- 如果使用鏈接功能將樹狀目錄分散在幾部伺服器上，則存取控制陳述式中所使用的關鍵字會有一些限制：
  - 依靠群組項目的 ACI (`groupdn` 關鍵字 ) 必須與群組項目位在同一部伺服器上。如果是動態群組，群組的所有成員也都必須在伺服器上有一個項目。如果是靜態群組，則成員的項目可位在遠端伺服器上。
  - 依靠角色定義的 ACI (`roledn` 關鍵字 ) 必須與角色定義項目位在同一部伺服器上。每一個要擁有角色的項目也都必須位在同一部伺服器上。

  但是，可以將儲存在目錄項目中的值與儲存在連結使用者項目中的值進行數值對應 ( 例如，使用 `userattr` 關鍵字 )。即使連結使用者在儲存 ACI 的伺服器上沒有任何項目，存取還是會以正常方式評估。

  如需關於如何鏈接存取控制評估的詳細資訊，請參閱第 120 頁「透過鏈接尾碼的存取控制」。
- 由 CoS 所產生的屬性不能用於所有 ACI 關鍵字中。尤其不應該將 CoS 所產生的屬性用於 `userattr` 和 `userdnattr` 關鍵字，因爲這樣存取控制規則將無作用。如需詳細資訊，請參閱第 199 頁「使用 userattr 關鍵字」。如需關於 CoS 的詳細資訊，請參閱第 5 章「管理身份和角色」。
- 存取控制規則總是在本機伺服器上評估。您*不可以*在 ACI 關鍵字所用的 LDAP URL 中指定伺服器的主機名稱或連接埠號碼。即使您指定了，也一樣不會將 LDAP URL 列入考量。如需詳細資訊，請參閱 《Directory Server Administration Reference》中的 Chapter 6 "LDAP URL Reference"。
- 授與代理權利時，您不能以目錄管理員身份將代理權利授與使用者，也不能將代理權利授與目錄管理員。

## 預設 ACI

當安裝 Directory Server 時，系統會在您在組態期間所指定的根尾碼上定義下列預設 ACI：

- 所有使用者擁有匿名存取目錄的權限，可執行搜尋、比較與讀取作業 ( 除了 `userpassword` 屬性之外 )。
- 連結使用者可以修改目錄中他們自己的項目，但無法予以刪除。他們無法修改 `aci`、`nsroledn` 和 `passwordPolicySubentry` 屬性，也無法修改任何資源限制屬性、密碼策略狀態屬性或帳戶鎖定狀態屬性。

- 組態管理員 ( 預設爲 `uid=admin,ou=Administrators, ou=TopologyManagement,o=NetscapeRoot`) 擁有代理權利以外的所有權利。
- 組態管理員群組的所有成員擁有代理權利以外的所有權利。
- 目錄管理員群組的所有成員擁有代理權利以外的所有權利。
- SIE 群組的所有成員擁有代理權利以外的所有權利。SIE 群組代表 Administration Server 中此目錄的伺服器群組的管理員。

當在目錄中建立新的根尾碼時，它的基礎項目擁有上述預設 ACI，但自我修改 ACI 除外。爲加強安全性，應該依第 99 頁「使用主控台建立新的根尾碼」中所述加入此 ACI。

Administration Server 的 NetscapeRoot 樹狀子目錄有它自己的一組預設 ACI：

- 組態管理員群組的所有成員在 NetscapeRoot 樹狀子目錄上擁有代理權利以外的所有權利。這讓他們可以將新成員加入組態管理員群組。
- 所有使用者擁有匿名存取 NetscapeRoot 樹狀子目錄的權限，可執行搜尋與讀取作業。
- 群組擴充 ACI 允許管理群組的成員存取群組定義。

下列各節說明如何修改這些預設值，以符合組織的需要。

# ACI 語法

ACI 是具有許多種可能變化的複雜結構。無論使用主控台或從指令行建立和修改 ACI，您都應該了解 LDIF 格式的 ACI 語法。下列各節將詳細說明 ACI 的語法。

**提示** 因爲 ACI 語法太複雜，Directory Server Console 並不支援以視覺方式編輯所有 ACI。而且，爲大量目錄項目設定存取控制時，使用指令行是比較快速的方式。因此，若要建立具有有效存取控制的安全目錄，了解 ACI 語法是很重要的。

`aci` 屬性的語法如下：

```
aci:(target)(version 3.0;acl "name";permission  bindRules;)
```

其中：

- *target* 指定要控制其存取權限的項目、屬性或項目與屬性組。目標可爲辨別名稱、一個或多個屬性，或單一 LDAP 篩選器；目標是選用的。如果未指定目標，ACI 會套用在定義 ACI 處的整個項目及其所有子項上。
- `version 3.0` 是識別 ACI 版本的必要字串。
- *name* 是 ACI 的名稱。名稱可爲識別 ACI 的任何字串。ACI 名稱是必要的，應該能夠描述 ACI 的效果。

**提示** 雖然名稱沒有任何限制，但是使用 ACI 的唯一名稱是好習慣。如果使用唯一名稱，「取得有效權利」控制項可讓您決定哪一個 ACI 有效。

- *permission* 特別地陳述了要允許或拒絕的權利，例如讀取或搜尋權利。
- *bindRules* 指定使用者爲獲得存取權所必須提供的憑證與連結參數。連結規則也可以以使用者或群組成員關係爲基礎，或是以用戶端的連線屬性爲基礎。

可以擁有多個目標和權限 - 連結規則配對。這可讓您將作爲目標的項目和屬性優化，並有效地爲指定目標設定多重存取控制項。例如：

```
aci:(target)...(target)(version 3.0;acl "name"; permission bindRule;
 permission bindRule; ...; permission bindRule;)
```

下列爲完整 LDIF ACI 的範例：

```
aci:(target="ldap:///uid=bjensen,dc=example,dc=com"
 (targetattr="*")(version 3.0; acl "example"; allow (write)
 userdn="ldap:///self";)
```

在此範例中，ACI 指明使用者 `bjensen` 有權修改她自己目錄項目中的所有屬性。

下列各節詳細說明 ACI 中每一部分的語法。

# 定義目標

目標會識別何者會套用 ACI。當用戶端要求對項目中的屬性執行作業時，伺服器會評估目標，了解是否必須評估 ACI 以允許或拒絕作業。如果未指定目標，則 ACI 會套用到包含 `aci` 屬性的項目中的所有屬性，及其下所有項目。

目標的一般語法爲下列其中一項：

(*keyword* = "*expression*")

(*keyword* != "*expression*")

其中：

- *keyword* 表示目標的類型。第 185 頁的「表 6-1」中的關鍵字定義下列目標類型：
  - 目錄項目，或其樹狀子目錄。
  - 項目的屬性。
  - 符合 LDAP 篩選器的項目或屬性組。
  - 符合 LDAP 篩選器的屬性值或數值組合。
- 等於 (=) 表示目標是 *expression* 中指定的物件，而不等於 (!=) 表示目標是 *expression* 中未指定的任何物件。

**備註** `targattrfilters` 關鍵字不支援「不等於」運算子。

- *expression* 會因關鍵字而有不同，並識別目標。雖然目前實作上接受像 `targetattr=*` 的運算式，*expression* 在語法上還是需要引號 (`""`)。在將來的版本語法檢查可能變得更嚴格，所以應該每次都使用引號。

下表列出每個關鍵字及相關運算式：

**表 6-1** LDIF 目標關鍵字

| 關鍵字 | 有效的運算式 | 允許萬用字元嗎？ |
|---|---|---|
| `target` | ldap:///*distinguished_name* | 是 |
| `targetattr` | *attribute* | 是 |
| `targetfilter` | *LDAP_filter* | 是 |
| `targattrfilters` | *LDAP_operation:LDAP_filter* | 是 |

## 將目錄項目設爲目標

使用 target 關鍵字和 LDAP URL 內的 DN 可將特定目錄項目及其下任何項目設爲目標。目標的 DN 必須位在 ACI 定義位置的項目下的樹狀子目錄中。目標運算式的語法如下：

```
(target = "ldap:///distinguished_name")
(target != "ldap:///distinguished_name")
```

辨別名稱必須位在以 ACI 定義位置的項目爲根部的樹狀子目錄中。例如，以下目標可用於 ou=People,dc=example,dc=com 上的 ACI 中：

```
(target = "ldap:///uid=bjensen,ou=People,dc=example,dc=com")
```

**備註** 項目的 DN 必須是以字串表示 (RFC 2253) 的辨別名稱。因此字元在文法上對 dn 很重要，例如逗號必須以反斜線 (\) 忽略掉。例如：

```
(target="ldap:///uid=cfuentes,o=Example Bolivia\, S.A.")
```

也可以在 DN 中使用萬用字元，將任何符合 LDAP URL 的項目設爲目標，項目數量不限。下列是萬用字元正確用法的範例：

- `(target="ldap:///uid=*,dc=example,dc=com")`

  比對整個 example.com 樹狀目錄中項目的 RDN 中有 uid 屬性的每一個項目。此目標將比對樹狀目錄中任一層的項目，例如：

  ```
  uid=tmorris,ou=sales,dc=example,dc=com
  uid=yyorgens,ou=marketing,dc=example,dc=com
  uid=bjensen,ou=eng,ou=east,dc=example,dc=com
  ```

- `(target="ldap:///uid=*Anderson,ou=People,dc=example,dc=com")`

  比對 ou=People 分支中 uid 以 Anderson 結束的所有項目。

- `(target="ldap:///*Anderson,ou=People,dc=example,dc=com")`

  比對 ou=People 分支中 RDN 以 Anderson 結束的所有項目，而不論命名屬性爲何。

允許使用多個萬用字元，例如 uid=*,ou=*,dc=example,dc=com。此範例比對 example.com 樹狀目錄中其辨別名稱包含 uid 與 ou 屬性的每個項目。

**備註** 辨別名稱的尾碼部分不能使用萬用字元。也就是，如果您的目錄使用尾碼 c=US 與 c=GB，則*不能*使用下列目標來參考這兩個尾碼：

```
(target="ldap:///dc=example,c=*").
```

也不能使用像 uid=bjensen,o=*.com 這樣的目標。

### 目標屬性

除了以目錄項目爲目標之外，也可以將目標項目的一或多個屬性，或是一或多個屬性除外的所有屬性設爲目標。這對於拒絕或允許存取項目的部分資訊非常有用。例如，您可以允許只存取指定項目的一般名稱、姓氏與電話號碼屬性；或者，您可以拒絕存取敏感的資訊，例如個人資料。

如果沒有 targetattr 規則，依預設值無法存取任何屬性。若要存取所有屬性，規則必須是 targetattr="*"。

目標屬性不必存在目標項目或其樹狀子目錄中，但只要這些屬性存在，就會套用 ACI。您設爲目標的屬性不必在結構中定義。這種缺乏結構檢查的方式讓您在匯入資料及其結構前便可實行存取控制策略。

若要將屬性設爲目標，請用 targetattr 關鍵字並提供屬性名稱。targetattr 關鍵字使用下列語法：

```
(targetattr = "attribute")
(targetattr != "attribute")
```

可以使用下列語法利用 targetattr 關鍵字，將多個屬性設爲目標：

```
(targetattr = "attribute1 || attribute2 ... || attributen")
(targetattr != "attribute1 || attribute2 ... || attributen")
```

例如，要將項目的一般名稱、姓氏及 uid 屬性設爲目標，請使用：

```
(targetattr = "cn || sn || uid")
```

目標屬性包含命名屬性的所有子類型。例如，(targetattr = "locality") 也會以 locality;lang-fr 爲目標。也可以特別將子類型設爲目標，例如 (targetattr = "locality;lang-fr-ca")。

您可以在 targetattr 規則中使用萬用字元，但並不鼓勵使用，因爲沒有特別的用途，而且可能對效能有負面的影響。

### 將項目與屬性視爲目標

依預設值，包含 targetattr 關鍵字之 ACI 的目標項目是 ACI 所在位置的項目。也就是，如果將 ACI

```
aci:(targetattr = "uid")(accessControlRules;)
```

放在 ou=Marketing,dc=example,dc=com 項目上，則 ACI 會套用在整個 Marketing 樹狀子目錄。但您也可以用 target 關鍵字明確指定目標，用法如下：

```
aci:(target="ldap:///uid=*,ou=Marketing,dc=example,dc=com")
 (targetattr="uid") (accessControlRules;)
```

target 與 targetattr 關鍵字的指定順序不相關。

## 使用 LDAP 篩選器將項目或屬性設爲目標

可以使用 LDAP 篩選器將符合某些條件的項目組設爲目標。若要如此設定，請在 targetfilter 關鍵字中使用 LDAP 篩選器。該 ACI 將套用在內含 ACI 的項目下樹狀子目錄中符合篩選器的所有項目。

targetfilter 關鍵字的語法爲：

```
(targetfilter = "LDAPfilter")
```

其中 *LDAPfilter* 是標準的 LDAP 搜尋篩選器。如需關於篩選器語法的詳細資訊，請參閱第 86 頁「LDAP 搜尋篩選器」。

例如，假設代表員工的所有項目都有 salaried 或 contractor 狀態，還有一個代表工作時數的屬性，此屬性以全職工作的百分比形式表示。若要將代表 contractor 或兼職員工的所有項目設爲目標，您可以使用下列篩選器：

```
(targetfilter = "(|(status=contractor)(fulltime<=79))")
```

**備註** ACI 中不支援描述國際化值對應規則的篩選器語法。例如，下列目標篩選器無效：

```
(targetfilter = "(locality:fr:=<= Quebec)")
```

目標篩選器將全體項目選爲 ACI 的目標。可以將 targetfilter 與 targetattr 關鍵字產生關聯，讓建立的 ACI 會套用在目標項目中的屬性子集上。

下列 LDIF 範例讓 Engineering Admins 群組的成員能夠修改 Engineering 業務類別中所有項目的 departmentNumber 與 manager 屬性。此範例使用 LDAP 篩選方式選擇 businessCategory 屬性設爲 Engineering 的所有項目：

```
dn:dc=example,dc=com
objectClass:top
objectClass:organization
aci:(targetattr="departmentNumber || manager")
 (targetfilter="(businessCategory=Engineering)")
 (version 3.0; acl "eng-admins-write"; allow (write)
 groupdn ="ldap:///cn=Engineering Admins, dc=example,dc=com";)
```

**提示** 雖然當將散佈目錄各處的項目與屬性設爲目標時，使用 LDAP 篩選器會相當有用，但結果有時可能難以預測，因爲篩選器並不直接指定您要管理存取的物件名稱。篩選 ACI 的目標項目組可能會隨著屬性的加入或刪除而改變。因此，如果在 ACI 中使用 LDAP 篩選器，則應在 `ldapsearch` 作業中使用相同的篩選器，以確認目標是否爲正確的項目和屬性。

## 使用 LDAP 篩選器將屬性值設爲目標

可以使用存取控制將特定屬性值設爲目標。這表示您可以依據屬性值是否符合 ACI 中定義的條件，來授與或拒絕權限。依據屬性值授與或拒絕存取權的 ACI 稱爲以值爲基礎的 ACI。

例如，可以授與組織內所有使用者修改的權限，以修改他們自己項目中的 `nsRoleDN` 屬性。但是，您也希望確保他們不會爲自己賦與某些重要角色，如「Top Level Administrator」。LDAP 篩選器可用來檢查屬性值是否符合條件。

若要建立以值爲基礎的 ACI，必須以下列語法使用 `targattrfilters` 關鍵字：

```
(targattrfilters="add=attr1:F1 && attr2:F2...&& attrn:Fn,
                  del=attr1:F1 && attr2:F2 ...&& attrn:Fn")
```

其中：

- `add` 代表建立屬性的作業。
- `del` 代表刪除屬性的作業。
- *attrn* 代表目標屬性。
- *Fn* 代表只套用在關聯屬性的篩選器。

建立項目時，如果將篩選器套用到新項目中的屬性，則該屬性的每個實例都必須滿足該篩選器。刪除項目時，如果將篩選器套用在該項目中的屬性，則該屬性的每個實例也都必須滿足該篩選器。

修改項目時，如果作業加入屬性，則必須滿足套用在該屬性的加入篩選器；如果作業刪除屬性，則必須滿足套用在該屬性的刪除篩選器。如果已存在於項目中之屬性的個別值被取代了，則必須同時滿足加入與刪除篩選器。

例如，請考慮下列屬性篩選器：

```
(targattrfilters="add=nsroleDN:(!(nsRoleDN=cn=superAdmin)) &&
telephoneNumber:(telephoneNumber=123*)")
```

此篩選器可用來允許使用者將任何角色 (nsRoleDN 屬性 ) 加入到自己的項目中，但 superAdmin 角色除外。它也允許使用者加入字首爲 123 的電話號碼。

| 備註 | 無法從 Directory Server Console 建立以值爲基礎的 ACI。 |
|---|---|

### 將單一目錄項目設爲目標

沒有明確的方法可以將單一項目設爲目標。但還是可以做得到：

- 利用建立連結規則，將連結要求中的使用者輸入對應儲存在目標項目中的屬性值。如需更多詳細資料，請參閱第 199 頁「根據相符值定義存取」。
- 藉由使用 targetfilter 關鍵字。

藉由使用 targetfilter 關鍵字，您便可以指定只會在所需項目中出現的屬性值。例如，在 Directory Server 安裝期間會建立下列 ACI：

```
aci:(targetattr="*")(targetfilter=(o=NetscapeRoot))
 (version 3.0; acl "Default anonymous access";
 allow (read, search) userdn="ldap:///anyone";)
```

此 ACI 只能套用在 o=NetscapeRoot 項目，因爲只有這個項目的 o 屬性值是 NetscapeRoot。

使用這些方法隨之而來的風險是您的樹狀目錄未來可能會改變，屆時請務必記得要修改此 ACI。

### 使用巨集定義目標

您可以使用巨集在 ACI 的目標部分中代表 DN，因此最佳化目錄中使用的 ACI 數目。如需詳細資訊，請參閱第 240 頁「進階的存取控制：使用巨集 ACI」。

## 定義權限

權限可以指定允許或拒絕存取的類型。可以允許或拒絕在目錄中執行特定作業的權限。各種可供指定的作業稱爲*權利*。

設定權限分爲兩個部分：

- 允許或拒絕存取
- 指定權利

### 允許或拒絕存取

可以明確允許或拒絕存取樹狀目錄的權限。如需關於何時應允許與拒絕存取的詳細說明，請參閱「Directory Server Deployment Planning Guide」 Chapter 7 的 "Designing Access Control"。

### 指定權利

權利詳細列出使用者可對目錄資料執行的特定作業。可以允許或拒絕所有權利，也可以指定下列一或多項權利：

**讀取。**表示使用者是否能讀取目錄資料。此權限僅適用於搜尋作業。

**寫入。**表示使用者是否能加入、修改或刪除*屬性*以修改項目。此權限適用於修改與 modrdn 作業。

**加入。**表示使用者是否能建立*項目*。此權限僅適用於加入作業。

**刪除。**表示使用者是否能刪除*項目*。此權限僅適用於刪除作業。

**搜尋。**表示使用者是否能搜尋目錄資料。使用者必須擁有搜尋與讀取權利，才能將傳回的資料視爲搜尋結果的一部份。此權限僅適用於搜尋作業。

**比較。**表示使用者是否能將他們提供的資料與目錄中儲存的資料做比較。若擁有比較權利，目錄在回應查詢時會傳回成功或失敗訊息，但使用者看不到項目或屬性的值。此權限僅適用於比較作業。

**自寫。**表示使用者是否能在目標項目的屬性中加入或刪除他們自己的 DN。此屬性的語法必須是「辨別名稱」。此權利僅供群組管理之用。自寫要配合代理驗證一起使用：它會授與從群組項目中加入或刪除代理 DN 的權利 ( 不是連結使用者的 DN)。

**代理。**表示指定的 DN 是否能使用另一個項目的權利存取目標。您可以使用目錄中任何使用者的 DN ( 目錄管理員 DN 除外 ) 授與代理存取權。不僅如此，您無法將代理權利授與目錄管理員。第 230 頁「代理驗證 ACI 範例」中提供了一個範例。

**全部。**表示指定的 DN 對目標項目擁有所有權利 ( 讀取、寫入、搜尋、刪除、比較與自寫 )，但*不包括*代理權利。

權利的授與彼此獨立。這表示獲得加入權利的使用者可以建立項目，但如果該使用者不曾特別獲得刪除權利，則無法刪除項目。因此，規劃目錄的存取控制策略時，必須確定授與權利的方式對使用者有意義。例如，只授與寫入權限，卻不授與讀取與搜尋權限，便沒有意義。

## LDAP 作業所需的權利

本節說明根據您要授權使用者執行之 LDAP 作業的不同，您必須授與使用者不同的權利。

**加入項目：**

- 授與正加入項目的加入權限。
- 授與項目中每個屬性值寫入的權限。依據預設授與此權利，但是可使用 `targattrfilters` 關鍵字加以限制。

**刪除項目：**

- 授與欲刪除項目的刪除權限。
- 授與項目中每個屬性值寫入的權限。依據預設授與此權利，但是可使用 `targattrfilters` 關鍵字加以限制。

**修改項目的屬性：**

- 授與該屬性類型的寫入權限。
- 授與每種屬性類型值的寫入權限。依據預設授與此權利，但是可使用 `targattrfilters` 關鍵字加以限制。

**修改項目的 RDN：**

- 授與該項目的寫入權限。
- 授與新 RDN 中所用屬性類型的寫入權限。
- 授與舊 RDN 中所用屬性類型的寫入權限 ( 如果要授與刪除舊 RDN 的權利 )。
- 授與新 RDN 中所用屬性類型值的寫入權限。依據預設授與此權利，但是可使用 `targattrfilters` 關鍵字加以限制。

**比較屬性值：**

- 授與該屬性類型的比較權限。

**搜尋項目：**

- 授與搜尋篩選器中所用每種屬性類型的搜尋權限。
- 授與項目所用至少一種屬性類型的讀取權限，以確定已傳回項目。
- 授與每種屬性類型讀取權取以使用項目傳回。

參照下列範例，可以更容易了解要允許使用者搜尋目錄所必須設定的權限。請思考下列搜尋：

```
ldapsearch -h host -p port -D "uid=bjensen,dc=example,dc=com" \
    -w password -b "dc=example,dc=com" \
            "(objectclass=*)" mail
```

使用下列 ACI 決定 `bjensen` 使用者是否能獲得存取權：

```
aci:(targetattr = "mail")(version 3.0; acl "self access to
 mail"; allow (read, search) userdn = "ldap:///self";)
```

搜尋結果清單空白，因爲此 ACI 未允許 `bjensen` 在 `objectclass` 屬性上搜尋的權限。如果希望上述的搜尋作業能夠成功，必須修改 ACI 以便讀取，如下：

```
aci:(targetattr = "mail || objectclass")(version 3.0; acl "self
 access to mail"; allow (read, search) userdn = "ldap:///self";)
```

### 權限語法

在 ACI 陳述式中，權限的語法爲：

```
allow|deny (rights)
```

其中 *rights* 是括弧內 1 到 8 個以逗號分隔的關鍵字清單。有效關鍵字爲 **read**、**write**、**add**、**delete**、**search**、**compare**、**selfwrite**、**proxy** 或 **all**。

在下列範例中，如果連結規則的評估結果是正確，便允許讀取、搜尋與比較存取：

```
aci:(target="ldap:///dc=example,dc=com") (version 3.0;acl
 "example"; allow (read, search, compare) bindRule;)
```

## 連結規則

視爲目錄定義之 ACI 的不同，有些作業必須*連結*到目錄。*連結*表示提供連結 DN 與密碼 ( 如果使用 SSL，則提供憑證 ) 讓您自身登入目錄或通過目錄的驗證。連結作業中所提供的憑證，以及連結的狀況均可決定是否允許或拒絕存取目錄。

ACI 中的每個權限組都有一個對應的連結規則，此規則詳細列出必要的憑證與連結參數。

簡單的連結規則可能需要存取目錄的使用者必須屬於特定的群組。複雜連結規則可能指明使用者必須屬於特定群組，而且必須在上午 8 點到下午 5 點之間從特定 IP 位址的電腦登入。

連結規則規定可以存取目錄的人員、時間與地點。連結規則可以更具體地規定：

- 獲得存取權的使用者、群組與角色

- 實體必須連結的來源位置。來自使用者驗證的位置可能不是正確的，因此無法受到信任。請勿依這種資訊決定 ACI。
- 連結必須發生的時間或日期
- 連結期間必須使用的驗證類型

此外，可以使用布林運算子將這些條件加以組合，讓連結的結構更加複雜。如需更多資訊，請參閱第 207 頁 「使用布林連結規則」。

伺服器會根據類似評估 LDAP 篩選器時所使用的三值邏輯，來評估 ACI 中所用的邏輯運算式，如「RFC 2251 輕量型目錄存取通訊協定 (v3) 」中所述。總而言之，這表示如果運算式中任何的元件被評估成未定義 ( 例如，如果因爲資源限制使運算式評估中止 )，則伺服器會正確地處理這種情況：它不會因爲複雜的布林運算式中出現未定義的值，而錯誤地授與存取權。

# 連結規則語法

以 ACI 的連結規則是否評估爲正確，作爲是否要允許或拒絕存取的依據。連結規則使用下列兩種模式之一：

*keyword* = "*expression*";

*keyword* != "*expression*";

其中等於 (=) 表示 *keyword* 與 *expression* 必須符合，連結規則才會成爲正確；而不等於 (!=) 則表示 *keyword* 與 *expression* 必須不符合，連結規則才會成爲正確。

| **備註** | `timeofday` 關鍵字也支援不相等運算式 (<、<=、>、>=)。這是唯一支援這些運算式的關鍵字。 |
|---|---|

*expression* 周圍的引號 ("") 和分隔的冒號 (;) 是必要的。可用的運算式須視關聯的 *keyword* 而定。

下表列出每個關鍵字與關聯的運算式，並指出運算式中是否允許萬用字元。

**表 6-2** LDIF 連結規則關鍵字

| 關鍵字 | 有效的運算式 | 允許萬用字元嗎？ |
|---|---|---|
| `userdn` | ldap:///*distinguished_name*<br>ldap:///all<br>ldap:///anyone<br>ldap:///self<br>ldap:///parent<br>ldap:///*suffix*??sub?(*filter*) | 是，僅限於 DN 中 |
| `groupdn` | [ldap:///*DN*] | 否 |
| `roledn` | [ldap:///*DN*] | 否 |
| `userattr` | *attribute*#*bindType* 或<br>*attribute*#*value* | 否 |
| `ip` | *IP_address* | 是 |
| `dns` | *DNS_host_name* | 是 |
| `dayofweek` | sun<br>mon<br>tue<br>wed<br>thu<br>fri<br>sat | 否 |
| `timeofday` | 0 - 2359 | 否 |
| `authmethod` | none<br>simple<br>ssl<br>sasl *authentication_method* | 否 |

下列各節將進一步詳細說明每個關鍵字的連結規則語法。

## 定義使用者存取 - userdn 關鍵字

使用者存取是用 `userdn` 關鍵字來定義。`userdn` 關鍵字需採用下列格式的一或多個有效辨別名稱：

```
userdn = "ldap:///dn [|| ldap:///dn]..."
userdn != "ldap:///dn [|| ldap:///dn]..."
```

其中 *dn* 可以是 DN 或是 anyone、all、self 或 parent 等運算式之一。這些運算式會參照下列使用者：

- userdn = "ldap:///anyone" - 匿名與驗證使用者。
- userdn = "ldap:///all" - 僅限驗證使用者。
- userdn = "ldap:///self" - 僅限與 ACI 目標項目一樣的使用者。
- userdn = "ldap:///parent" - 僅限 ACI 目標的父項。

userdn 關鍵字也可以表示爲如下列格式的 LDAP 篩選器：

```
userdn = ldap:///suffix??sub?(filter)
```

**備註** 字元在文法上對 dn 很重要，例如逗號必須以反斜線 (\) 忽略掉。

### 匿名存取 (anyone 關鍵字)

授與匿名存取目錄的權限，表示不論連結狀況如何，任何人都不需提供連結 DN 或密碼即可存取該目錄。可以將匿名存取限制在特定類型的存取 ( 例如，讀取存取或搜尋存取 )，或是限制在特定樹狀子目錄，或目錄中的個別項目。使用 anyone 關鍵字的匿名存取也允許任何驗證使用者存取。

例如，如果要允許匿名讀取和搜尋存取整個 example.com 樹狀目錄，請在 dc=example,dc=com 節點上建立下列 ACI：

```
aci:(version 3.0; acl "anonymous-read-search";
 allow (read, search) userdn = "ldap:///anyone";)
```

### 一般存取 (all 關鍵字)

可以用連結規則表示權限適用於成功連結該目錄的任何人。因此，all 關鍵字允許所有驗證使用者存取。如此一來既可以允許一般存取，同時又能防止匿名存取。

例如，如果要將整個樹狀目錄的讀取存取授與所有驗證使用者，請在 dc=example,dc=com 節點上建立下列 ACI：

```
aci:(version 3.0; acl "all-read"; allow (read)
 userdn="ldap:///all";)
```

### 自身存取 (self 關鍵字)

指定授權或拒絕使用者存取他們自己的項目。在此情況下，如果連結 DN 符合目標項目的 DN，便授與或拒絕存取。

例如，如果要授權 example.com 樹狀目錄中的所有使用者均可寫入存取其 userPassword 屬性，請在 dc=example,dc=com 節點上建立下列 ACI。

```
aci:(targetattr = "userPassword") (version 3.0; acl
 "modify own password"; allow (write) userdn = "ldap:///self";)
```

### 父項目存取 (parent 關鍵字)

指定唯有連結 DN 是目標項目的父項目時，才授與或拒絕使用者存取該項目。請注意，必須在 Server Console 中手動編輯 ACI，才能使用 parent 關鍵字。

例如，如果要允許使用者可修改他們連結 DN 的任何子項目，請在 dc=example,dc=com 節點上建立下列 ACI：

```
aci:(version 3.0; acl "parent access";
 allow (write) userdn="ldap:///parent";)
```

### LDAP URL

可以在 ACI 中使用下列包含篩選器的 URL，動態地將使用者設爲目標：

```
userdn = "ldap:///<suffix>??sub?(filter)"
```

例如，根據下列 URL，動態地授權或拒絕 example.com 樹狀目錄中 accounting 與 engineering 分支內所有使用者存取目標資源的權限：

```
userdn = "ldap:///dc=example,dc=com??sub?(|(ou=eng)(ou=acct))"
```

| **備註** | 在 LDAP URL 中不要指定主機名稱或連接埠號碼。LDAP URL 永遠套用於本機伺服器。 |
|---|---|

如需詳細資訊，請參閱《Directory Server Administration Reference》中的 Chapter 6 "LDAP URL Reference"。

### 萬用字元

也可以使用萬用字元 (*) 指定一組使用者。例如，指定 uid=b*,dc=example,dc=com 的使用者 DN，可表示依據您設定的權限，只允許或拒絕連結 DN 是以 b 爲開頭之使用者的存取權限。

### LDAP URL 的邏輯 OR

指定數個 LDAP URL 或關鍵字運算式以建立使用者存取的複雜規則。例如：

```
userdn = "ldap:///uid=b*,c=example.com ||
 ldap:///cn=b*,dc=example,dc=com";
```

與任一 DN 模式連結的使用者之連結規則被評估爲真。

### 排除特定 LDAP URL

使用不等於 (!=) 運算字定義排除特定 URL 或 DN 的使用者存取。例如：

```
userdn != "ldap:///uid=*,ou=Accounting,dc=example,dc=com";
```

如果用戶端不是以 accounting 樹狀子目錄中以 UID 爲基礎的辨別名稱來連結，則連結規則會被評估爲正確。只有當目標項目不在樹狀目錄的 accounting 分支下時，此連結規則才有道理。

## 定義群組存取 - groupdn 關鍵字

特定群組的成員可存取目標資源；這稱爲*群組存取*。群組存取是用 `groupdn` 關鍵字定義，以指定使用者如果用屬於特定群組的 DN 連結，即授權或拒絕該使用者存取目標項目。

`groupdn` 關鍵字需要採用下列格式的一或多個群組：

```
groupdn="ldap:///groupDN [|| ldap:///groupDN]..."
```

如果連結 DN 屬於任何 *groupDNs*. 指定的群組，則連結規則會被評估爲正確。下節使用 `groupdn` 關鍵字提供範例。

| **備註** | 字元在文法上對 dn 很重要，例如逗號必須以反斜線 (\) 忽略掉。 |
|---|---|

### 單一 LDAP URL

```
groupdn = "ldap:///cn=Administrators,dc=example,dc=com";
```

如果連結 DN 屬於 Administrators 群組，則連結規則會被評估爲正確。如果要將整個樹狀目錄的寫入權限授與給 Administrators 群組，請在 `dc=example,dc=com` 節點上建立下列 ACI：

```
aci:(version 3.0; acl "Administrators-write"; allow (write)
 groupdn="ldap:///cn=Administrators,dc=example,dc=com";)
```

### LDAP URL 的邏輯 OR

```
groupdn = "ldap:///cn=Administrators,dc=example,dc=com ||
ldap:///cn=Mail Administrators,dc=example,dc=com";
```

如果連結 DN 屬於 Administrators 或 Mail Administrators 群組，則連結規則會被評估爲正確。

## 定義角色存取 - roledn 關鍵字

特定角色的成員可存取目標資源；這稱爲*角色存取*。角色存取是用 `roledn` 關鍵字定義，以指定使用者如果用屬於特定角色的 DN 連結，即授權或拒絕該使用者存取目標項目。

`roledn` 關鍵字需要採用下列格式的一或多個有效辨別名稱：

```
roledn = "ldap:///dn [|| ldap:///dn]...[|| ldap:///dn]"
```

如果連結 DN 屬於指定的角色，則連結規則會被評估爲正確。

| **備註** | 字元在文法上對 dn 很重要，例如逗號必須以反斜線 (\) 忽略掉。 |
|---|---|

`roledn` 關鍵字與 `groupdn` 關鍵字的語法與用法都一樣。

## 根據相符值定義存取

可以設定連結規則，以指定用來連結目錄的項目屬性值必須與目標項目的屬性值相符。

例如，可以指定連結 DN 必須與使用者項目中 `manager` 屬性的 DN 相符，才能套用 ACI。在此情況下，只有使用者的管理員可以存取該項目。

此範例是根據 DN 相符值。然而，可以將連結中所用項目的任何屬性與目標項目比對。例如，可以建立 ACI，允許 `favoriteDrink` 屬性爲「beer」的任何使用者讀取其 `favoriteDrink` 值相同之其他使用者的所有項目。

### 使用 userattr 關鍵字

`userattr` 關鍵字可用來指定連結項目與目標項目之間必須相符的屬性值。

可以指定：

- 使用者 DN
- 群組 DN
- 角色 DN
- 在 LDAP URL 中的 LDAP 篩選器
- 任何屬性類型

`userattr` 關鍵字的 LDIF 語法如下：

```
userattr = "attrName#bindType"
```

或者，如果目前使用的屬性類型需要的值爲使用者 DN、群組 DN、角色 DN 或 LDAP 篩選器以外的值：

```
userattr = "attrName#attrValue"
```

其中：

- *attrName* 是相符值所用的屬性名稱
- *bindType* 是 `USERDN`,`GROUPDN`,`ROLEDN`,`LDAPURL` 中的一個
- *attrValue* 是代表屬性值的任何字串

**備註** `userattr` 關鍵字中不得使用由服務類別 (CoS) 定義所產生的屬性。ACI 包含的連結規則若取決於由 CoS 所產生的屬性值，則該 ACI 將無作用。

下列各節提供 `userattr` 關鍵字使用各種不同連結類型的範例。

### *使用 USERDN 連結類型的範例*

下列爲與以使用者 DN 爲基礎之連結有關聯的 `userattr` 關鍵字範例：

```
userattr = "manager#USERDN"
```

如果連結 DN 與目標項目中 `manager` 屬性的值相符，則連結規則會被評估爲正確。可以使用這種方式允許使用者的管理員修改員工屬性。只有當目標項目中的 `manager` 屬性表示成完整 DN 時，此機制才有作用。

下列範例會授權管理員可完整存取其員工項目的權限：

```
aci:(target="ldap:///dc=example,dc=com")(targetattr="*")
 (version 3.0;acl "manager-write";
 allow (all) userattr = "manager#USERDN";)
```

### *使用 GROUPDN 連結類型的範例*

下列爲與以群組 DN 爲基礎之連結有關聯的 `userattr` 關鍵字範例：

```
userattr = "owner#GROUPDN"
```

如果連結 DN 是目標項目 `owner` 屬性中指定的群組成員，則連結規則會被評估爲正確。例如，可以使用此機制以允許群組管理員工的狀態資訊。可以使用 `owner` 以外的屬性，只要所使用的屬性中包含群組項目的 DN。

您所指向的群組可以是動態群組，而且群組的 DN 可以在目錄的任何尾碼下。然而，由伺服器評估這類 ACI 會非常耗費資源。

如果使用與目標項目在同一尾碼下的靜態群組，可以使用下列運算式：

```
userattr = "ldap:///dc=example,dc=com?owner#GROUPDN"
```

在此範例中，群組項目位在 `dc=example,dc=com` 尾碼下。伺服器處理此類型的語法的速度會比上一個範例快。

### *使用 ROLEDN 連結類型的範例*

下列爲與以角色 DN 爲基礎之連結有關聯的 `userattr` 關鍵字範例：

```
userattr = "exampleEmployeeReportsTo#ROLEDN"
```

如果連結 DN 屬於目標項目的 `exampleEmployeeReportsTo` 屬性中指定的角色，則連結規則會被評估爲正確。例如，如果爲公司中的所有管理員建立巢式角色，您可以使用此機制授權所有階層的管理員可存取有關階層較管理員低之員工的資訊。

角色的 DN 可在目錄的任何尾碼下。此外，如果您使用篩選的角色，評估這類 ACI 會耗用伺服器上大量的資源。

### *使用 LDAPURL 連結類型的範例*

下列爲與以 LDAP 篩選器爲基礎之連結有關聯的 `userattr` 關鍵字範例：

```
userattr = "myfilter#LDAPURL"
```

如果連結 DN 符合目標項目的 *myfilter* 屬性中指定的篩選器，則連結規則會被評估爲正確。*myfilter* 屬性可以由包含 LDAP 篩選器的任何屬性取代。

### *使用任何屬性值的範例*

下列爲與以任何屬性值爲基礎之連結有關聯的 `userattr` 關鍵字範例：

```
userattr = "favoriteDrink#Beer"
```

如果連結 DN 與目標 DN 包含有 **`Beer`** 值的 `favoriteDrink` 屬性，則連結規則會被評估爲正確。

### 在 userattr 關鍵字中使用繼承

當使用 `userattr` 關鍵字將連結所用項目與目標項目產生關聯時，ACI 只會套用在指定的目標，而不會套用在其下的項目。在某些狀況下，您可能希望將 ACI 的套用由目標項目向下延伸幾個層級。只要使用 parent 關鍵字，並指定目標之下應繼承 ACI 的層級數，就可以辦得到。

當使用與 `parent` 關鍵字有關聯的 `userattr` 關鍵字時，語法如下：

```
userattr = "parent[inheritance_level].attribute#bindType"
```

其中：

- *inheritance_level* 是以逗號分隔的清單，表示目標之下有多少層級要繼承 ACI。可以包含目標項目下的 5 個層級 `[0,1,2,3,4]`，零 (0) 是指目標項目。
- *attribute* 是 `userattr` 或 `groupattr` 關鍵字的目標屬性。
- *bindType* 可爲 `USERDN` 或 `GROUPDN` 其中之一。繼承不支援 `LDAPURL` 與 `ROLEDN` 連結類型。

例如：

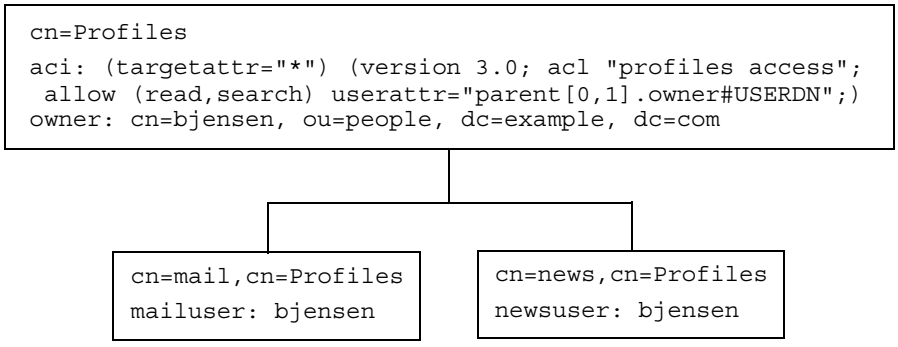
```
userattr = "parent[0,1].manager#USERDN"
```

如果連結 DN 與目標項目的 manager 屬性相符，則連結規則會被評估爲正確。當連結規則評估爲正確時，所授與的權限會套用在目標項目*以及*它下一層的所有項目。

#### *使用 userattr 繼承的範例*

下圖中的範例表示允許 `bjensen` 使用者讀取與搜尋 `cn=Profiles` 項目，以及包含 `cn=mail` 與 `cn=news` 的第一層子項目。

**圖 6-1** 在 userattr 關鍵字中使用繼承




在此範例中，如果不使用繼承，就必須執行下列任一項才能獲得同樣的結果：

- 明確地爲目錄中 cn=Profiles、cn=mail 與 cn=news 項目上的 bjensen 使用者設定讀取與搜尋存取。
- 將 owner 屬性和下列的 ACI 加入 cn=mail,cn=Profiles and cn=news,cn=Profiles 項目中：

```
aci:(targetattr="*") (version 3.0; acl "profiles access";
allow
 (read,search) userattr="owner#USERDN";)
```

## 使用 userattr 關鍵字授與對項目的權限

如果將 userattr 關鍵字搭配 all 或 add 權限一起使用，您可能發現伺服器的運作方式與預期狀況不相符。一般而言在目錄中建立新項目時，Directory Server 會對建立的項目而非父項目評估其存取權利。然而在使用 userattr 關鍵字的 ACI 中，此運作方式可能造成安全上的漏洞，因此要修改伺服器正常的運作方式以避免此情況發生。

請思考下列範例：

```
aci:(target="ldap:///dc=example,dc=com")(targetattr="*")
 (version 3.0; acl "manager-write"; allow (all)
 userattr = "manager#USERDN";)
```

此 ACI 將管理員直屬員工項目的全部權利授與管理員。但是，因爲存取權利是在建立的項目上評估，這類 ACI 也會允許任何員工建立項目，並將 manager 屬性設爲他們自己的 DN。例如，心懷不滿的員工 Joe (cn=Joe,ou=eng,dc=example,dc=com) 可能會在樹狀目錄的 Human Resources 分支中建立項目，以使用 ( 或濫用 ) 授與 Human Resources 員工的權限。

他可以利用建立下列項目來達成此目的：

```
dn:cn= Trojan Horse,ou=Human Resources,dc=example,dc=com
objectclass:top
...
cn:Trojan Horse
manager:cn=Joe,ou=eng,dc=example,dc=com
```

爲避免這類安全性威脅，ACI 評估處理程序不會在層級 0 ( 也就是項目本身 ) 授與加入權限，但您可以用 `parent` 關鍵字授與現有項目下的加入權利。您必須指定父項目下需要加入權利的層級數。例如，下列 ACI 允許爲 `dc=example,dc=com` 中的任何項目加入子項目，只要該項目有符合連結 DN 的 `manager` 屬性：

```
aci:(target="ldap:///dc=example,dc=com")(targetattr="*")
 (version 3.0; acl "parent-access"; allow (add)
 userattr = "parent[0,1].manager#USERDN";)
```

此 ACI 可確保加入權限只授與其連結 DN 與父項目的 manager 屬性相符的使用者。

## 定義來自特定 IP 位址的存取

使用連結規則，可以表示連結作業必須起源自特定 IP 位址。這通常用來強制讓所有目錄的更新均從指定的電腦或網路網域發生。

設定以 IP 位址爲基礎的連結規則的 LDIF 語法如下：

```
ip = "IPaddressList" 或 ip != "IPaddressList"
```

*IPaddressList* 是一張清單，以一或多個逗號將元素分隔，其中的元素可爲下列任一項：

- 特定的 IPv4 位址：`123.45.6.7`
- 使用萬用字元的 IPv4 位址，以指定子網路：`12.3.45.*`
- 使用子網路遮罩的 IPv4 位址或子網路：`123.45.6.*+255.255.255.115`
- 任何有效格式的 IPv6 位址，其格式定義於 RFC 2373 (`http://www.ietf.org/rfc/rfc2373.txt`)。下列位址相同：
  - `12AB:0000:0000:CD30:0000:0000:0000:0000`
  - `12AB::CD30:0:0:0:0`
  - `12AB:0:0:CD30::`
- IPv6 位址及其子網路字首長度：`12AB::CD30:0:0:0:0/60`

如果存取目錄的用戶端位在命名的 IP 位址中，則連結規則會被評估爲正確。這對於只允許從特定子網路或電腦進行某種目錄存取而言是非常有用。來自使用者驗證的 IP 位址可能不是正確的，因此無法受到信任。請勿依這種資訊決定 ACI。

從 Server Console 上，可以透過 [ 存取控制編輯器 ] 定義要套用 ACI 的特定電腦。如需詳細資訊，請參閱第 209 頁「使用主控台建立 ACI」。

## 定義來自特定網域的存取

連結規則可以指定連結作業必須起源自特定網域或主機電腦。這通常用來強制讓所有目錄的更新均從指定的電腦或網路網域發生。

設定以 DNS 主機名稱爲基礎的連結規則的 LDIF 語法如下：

```
dns = "DNS_Hostname" 或 dns != "DNS_Hostname"
```

| 小心 | dns 關鍵字要求您的電腦上必須使用 DNS 名稱服務。如果名稱服務不是 DNS，您應該改用 ip 關鍵字。 |
|---|---|

dns 關鍵字需要完全合格 DNS 網域名稱。若授與主機存取權，卻不指定網域，會造成潛在的安全性威脅。例如，下列運算式雖然可被允許，但並不建議您如此做：

```
dns = "legend.eng";
```

應該使用完全合格名稱，例如：

```
dns = "legend.eng.example.com";
```

dns 關鍵字允許萬用字元。例如：

```
dns = "*.example.com";
```

如果存取目錄的用戶端位在命名的網域，則連結規則會被評估爲正確。這對於只允許從特定網域進行存取非常有用。請注意，如果系統使用的名稱服務並非 DNS ，則萬用字元將無作用。在這種情況下，如果要限制存取特定網域，請使用 ip 關鍵字，如第 204 頁「定義來自特定 IP 位址的存取」中所述。

## 定義於特定時間或日期存取

可以用連結規則指定連結只能發生在一天中的某個時間，或一星期的某一天。例如，可以設定一條規則，只允許在星期一到星期五的上午 8 點到下午 5 點之間進行存取。用來評估存取權利的時間是目錄伺服器上的時間，而非用戶端上的時間。

設定以一天中某一時段爲基礎的連結規則的 LDIF 語法如下：

```
timeofday operator "time"
```

其中 *operator* 可爲下列符號之一：等於 (=)、不等於 !=}、大於 (>)、大於或等於 (>=)、小於 <} 或小於或等於 (<=)。以四位數表示 24 小時時間格式的時數與分鐘 (0 到 2359)。例如：

- 如果用戶端在系統時鐘顯示中午時的那一分鐘存取目錄，則 `timeofday = "1200";` 爲真。
- 在早上 1 點以外的時間存取，`timeofday != "0100";` 爲真。
- 從早上 8:01 到下午 11:59 之間存取，`timeofday > "0800";` 爲真。
- 從早上 8:00 到下午 11:59 之間存取，`timeofday > "0800";` 爲真。
- 從早上 12:00:00 到下午 5:59 之間存取，`timeofday < "1800";` 爲真。

**備註** 伺服器上的時間與日期用於評估 `timeofday` 和 `dayofweek` 連結規則，而不是用戶端上的時間。

設定以一星期中某天爲基礎的連結規則的 LDIF 語法如下：

```
dayofweek = "day1, day2 ..."
```

dayofweek 關鍵字可能的值爲一星期中各天的三個英文字母縮寫：`sun`、`mon`、`tue`、`wed`、`thu`、`fri`、`sat`。指定您想要授與存取權的所有日期，例如：

```
dayofweek = "Mon, Tue, Wed, Thu, Fri";
```

如果在列出的其中一個日期存取目錄，則連結規則爲真。

## 定義以驗證方法爲基礎的存取

可以設定連結規則，指明用戶端必須使用特定驗證方法連結到目錄。可用的驗證方法如下：

- **None** - 不需要驗證。這是預設值，代表匿名存取。
- **Simple** - 用戶端必須提供使用者名稱與密碼才能連結到目錄。
- **SSL** - 用戶端必須透過安全通訊端階層 (SSL) 或傳輸層安全性 (TLS) 連線才能連結到目錄。

若是 SSL，連線必須建立到 LDAPS 第二個連接埠；若是 TLS，連線必須透過 Start TLS 作業建立。這兩種狀況都必須提供憑證。如需設定 SSL 的資訊，請參閱第 11 章「管理驗證和加密」。

- **SASL** - 用戶端必須透過例如 DIGEST-MD5 或 GSSAPI 等簡易驗證及安全階層 (SASL) 機制才能連結到目錄。

您無法透過 [ 存取控制編輯器 ] 設定以驗證爲基礎的連結規則。

設定以驗證方法爲基礎的連結規則的 LDIF 語法如下：

```
authmethod = "authentication_method"
```

其中 *authentication_method* 是 `none`、`simple`、`ssl` 或 `sasl` *sasl_mechanism*。例如：

### 範例

下列是 `authmethod` 關鍵字的範例：

- `authmethod = "none";` 連結規則評估期間不會檢查驗證。
- `authmethod = "simple";` 如果用戶端使用使用者名稱與密碼存取目錄，則連結規則評估爲正確。
- `authmethod = "ssl";` 如果用戶端使用透過 LDAPS 的憑證存取目錄，則連結規則會被評估爲正確。如果用戶端使用透過 LDAPS 的簡單驗證 ( 連結 DN 與密碼 ) 進行驗證，將不會評估爲正確。
- `authmethod = "sasl DIGEST-MD5";` 如果用戶端使用 SASL DIGEST-MD5 機制存取目錄，則連結規則評估爲正確。其他支援的 SASL 機制爲 EXTERNAL ( 所有平台 ) 和 GSSAPI ( 僅限於 Solaris 系統 )。

## 使用布林連結規則

連結規則可以是使用布林運算式 `AND`、`OR` 與 `NOT` 的複雜運算式，以設定非常精確的存取規則。您無法使用 Server Console 建立布林連結規則，您必須建立 LDIF 陳述式。

布林連結規則的 LDIF 語法如下：

*bindRule* [*boolean*] [*bindRule*] [*boolean*] [*bindRule*] . . . ;)

例如，如果連結 DN 是系統管理員群組或郵件管理員群組的成員，而且用戶端是從 example.com 網域內部執行，則下列連結規則評估爲正確：

```
(groupdn = "ldap:///cn=administrators,dc=example,dc=com" or
groupdn = "ldap:///cn=mail administrators,dc=example,dc=com" and
dns = "*.example.com";)
```

位於結尾處的分號 (;) 是必要的分隔字元，必須出現在最後的連結規則後。

布林運算式的評估順序如下：

- 最內部到最外部的括弧運算式第一優先
- 所有運算式由左到右
- NOT 優先於 AND 或 OR 運算子

布林 OR 與布林 AND 運算子沒有優先順序。

請思考下列布林連結規則：

(*bindRule_A*) OR (*bindRule_B*)

(*bindRule_B*) OR (*bindRule_A*)

因爲布林運算式是由左到右評估，所以在第一個範例中，會先評估連結規則 A，再評估連結規則 B，而在第二個範例中，則先評估連結規則 B，再評估連結規則 A。

但是布林 NOT 會在布林 OR 與布林 AND *之前*評估。因此，在下列範例中：

(*bind_rule_A*) AND NOT (*bind_rule_B*)

會先評估連結規則 B，再評估連結規則 A，而不理會由左到右的規則。

# 從指令行建立 ACI

您可以使用 LDIF 陳述式手動建立存取控制指令，並用 `ldapmodify` 指令將它們加入到您的樹狀目錄中。因爲 ACI 值可能非常複雜，您最好檢視現有的值，然後複製起來幫您建立新的值。

## 檢視 aci 屬性值

系統儲存 ACI 作爲項目上 `aci` 屬性的一或多個值。`aci` 屬性是多重值操作屬性，目錄使用者可讀取與修改此屬性，而此屬性本身受到 ACI 保護。管理使用者通常對 `aci` 屬性擁有完整存取權，而且可使用下列其中一種方式檢視其內容。

可以在 [ 標準編輯器 ] 中檢視 aci 屬性值，就如同任何其他值一般。在 Directory Server Console 最上層的 [ 目錄 ] 標籤上，以滑鼠右鍵按一下有 ACI 的項目，並選擇 [ 以標準編輯器編輯 ] 功能表項目。但是，aci 值通常是長字串，不容易在此對話方塊中檢視與編輯。

因此，可以改爲在樹狀目錄的項目上按一下滑鼠右鍵，再選擇 [ 設定存取權限 ] 功能表項目以啓動 [ 存取控制編輯器 ]。選取 ACI 後按一下 [ 編輯 ]，再按一下 [ 手動編輯 ]，即可檢視對應的 aci 值。藉由在 ACI 的手動與視覺化編輯器之間切換，可比較 aci 值的語法與其組態。

如果您的作業系統允許，您可以從 [ 標準編輯器 ] 或 [ 手動存取控制編輯器 ] 中複製 aci 值，並將它貼入您的 LDIF 檔案。管理使用者也可以執行下列 ldapsearch 指令來檢視項目的 aci 屬性：

```
ldapsearch -h host -p port -D "cn=Directory Manager" -w password \
           -b entryDN -s base "(objectclass=*)" aci
```

產生的結果是您可以貼入新的 LDIF ACI 定義以進行編輯的 LDIF 文字。因爲 ACI 的值是長字串，所以 ldapsearch 操作上的輸出可能顯示在數行上，含有作爲連續標記的第一個空格。複製和貼上 LDIF 輸出時將此列入考慮。

**備註** 若要檢視 aci 值對授與或拒絕權限所產生的影響，請參閱第 231 頁「檢視有效權利」。

## 使用主控台建立 ACI

可以配置 Directory Server Console 以顯示目錄中哪些項目擁有 aci 屬性。選取或取消選取 [ 檢視 ] > [ 顯示 ] > [ACI 計數 ] 功能表選項，可切換此顯示。最上層 [ 目錄 ] 標籤內的清單項目便會附加上其 aci 屬性中已定義的 ACI 數目，接著您可以使用 Directory Server Console 檢視、建立、編輯與刪除目錄的存取控制指令。

如需 Directory Server 安全性政策中常用的存取控制規則集合，以及使用 Directory Server Console 建立這些規則的步驟式說明，請參閱第 214 頁「存取控制用法範例」。

[ 存取控制編輯器 ] 無法讓您在 [ 視覺化 ] 編輯模式中建構比較複雜的 ACI。尤其是，您無法從 [ 存取控制編輯器 ] 執行：

- 拒絕存取 ( 請參閱第 193 頁「權限語法」 )
- 建立以值爲基礎的 ACI ( 請參閱第 189 頁「使用 LDAP 篩選器將屬性值設爲目標」 )

- 定義父項目存取 ( 請參閱第 197 頁「父項目存取 (parent 關鍵字 )」 )
- 建立包含布林連結規則的 ACI ( 請參閱第 207 頁「使用布林連結規則」 )
- 大致上，建立使用下列關鍵字的 ACI：`roledn`, `userattr`, `authmethod`

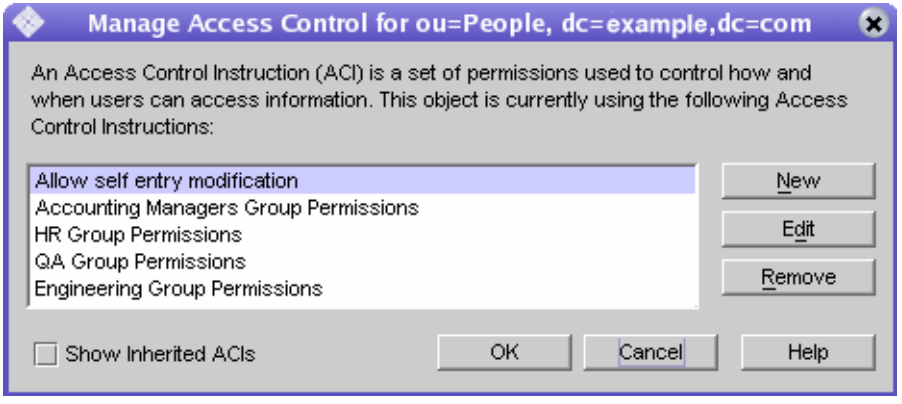
**提示** 在 [ 存取控制編輯器 ] 中，可以隨時按一下 [ 手動編輯 ] 按鈕，檢查透過圖形介面所執行之變更的 LDIF 表示法。

## 檢視項目的 ACI

1. 在 Directory Server Console 最上層的 [ 目錄 ] 標籤上，瀏覽樹狀目錄，以顯示要設定存取控制的項目。必須具有目錄系統管理員或目錄管理員權限才能編輯 ACI。
2. 以滑鼠右鍵按一下項目，並在快顯功能表中選取 [ 設定存取權限 ]。或者，以滑鼠左鍵按一下項目以選取項目，再選擇 [ 物件 ] 功能表中的 [ 設定存取權限 ]。

   出現如下圖所示的 [ 存取控制管理 ] 對話方塊。圖中列出在選取的項目上定義之所有 ACI 的描述，並可讓您進行編輯，或移除後再建立新的描述。

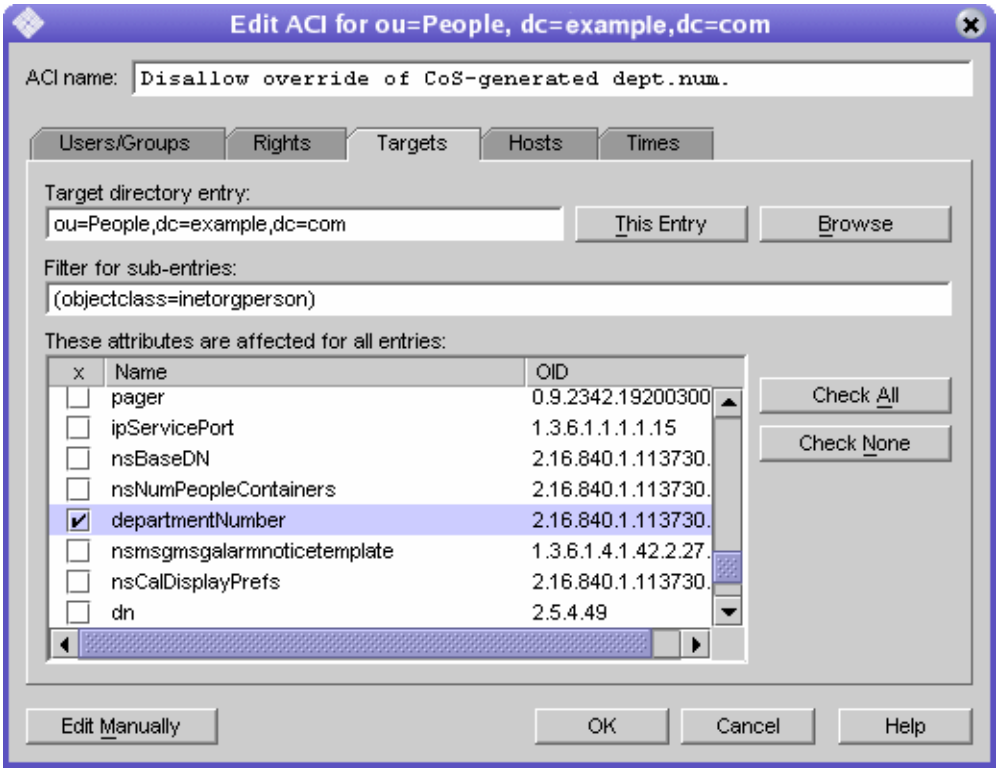
**圖 6-2** [ 存取控制管理 ] 對話方塊




   選取 [ 顯示繼承的 ACI] 核取方塊列出被選取項目之父項目所定義的所有 ACI，以及套用到項目的 ACI。繼承的 ACI 無法被編輯或移除，您必須在定義該 ACI 的項目上進行管理。

3. 按一下 [ 新增 ] 在選取的物件及其整個樹狀子目錄上定義新的存取權限。出現如圖 6-3 所示的 [ACI 編輯器 ]。

**圖 6-3** [ACI 編輯器 ] 對話方塊




對話方塊上方的 ACI 名稱是出現在 [ 存取控制管理 ] 對話方塊中的 ACI 描述。因爲描述性的 ACI 名稱會使整個目錄的 ACI 比較容易管理，尤其在檢視葉項目上繼承的 ACI 時。

[ 存取控制編輯器 ] 的各個標籤可讓您指定被授與或拒絕存取的使用者、存取中或遭限制的目標，以及進階參數，例如允許的主機名稱與作業時段等。如需關於 [ 存取控制 ] 標籤中個別欄位的詳細資料，請參閱線上說明。

[ACI 編輯器 ] 的各個標籤爲 ACI 值的內容提供圖形顯示。按一下 [ 手動編輯 ] 按鈕可查看 ACI 值並用文字方式進行編輯。在文字編輯器中，可以定義無法透過標籤定義的進階 ACI。但是一旦編輯 ACI 值之後，*即使*不使用進階功能，都一樣可能再也無法以視覺方式編輯 ACI。

# 建立新的 ACI

1. 顯示 [ 存取控制編輯器 ]。

   此工作在第 210 頁 「檢視項目的 ACI」中有說明。

   如果顯示的檢視與 第 211 頁的 「圖 6-3」不同，請按一下 [ 視覺化編輯 ] 按鈕。

2. 在 [ACI 名稱 ] 文字方塊中輸入名稱，爲 ACI 命名。

   名稱可以是任何字串，以用於唯一識別此 ACI。如果不輸入名稱，伺服器會使用 **`unnamed ACI`**。

3. 在 [ 使用者 / 群組 ] 標籤中，藉由反白顯示 [ 全部使用者 ]，或按一下 [ 加入 ] 按鈕在目錄中搜尋要加入的使用者，以選取要授與存取權的使用者。

   在 [ 加入使用者和群組 ] 視窗中：

   a. 從下拉式清單中選取一個搜尋區域，在 [ 搜尋 ] 欄位中輸入搜尋字串，再按一下 [ 搜尋 ] 按鈕。

      搜尋結果會顯示在下方的清單中。

   b. 反白顯示搜尋結果清單中您要的項目，再按一下 [ 加入 ] 按鈕將項目加入擁有存取權限的項目清單中。

   c. 按一下 [ 確定 ] 退出 [ 加入使用者和群組 ] 視窗。

      您選取的項目現在會列在 ACI 編輯器的 [ 使用者 / 群組 ] 標籤上。

4. 在 [ 存取控制編輯器 ] 中，按一下 [ 權利 ] 標籤，再使用核取方塊選取要授與的權利。

5. 按一下 [ 目標 ] 標籤，再按一下 [ 此項目 ] 以顯示作爲 ACI 目標的節點。

   可以變更目標 DN 的值，但新的 DN 必須是選取項目的直接或間接子項。

   如果不要將此節點下樹狀子目錄中的每一個項目都作爲 ACI 的目標，您必須在 [ 子項目的篩選器 ] 欄位中輸入篩選器。

   此外，可以在屬性清單中選取要作爲目標的屬性，將 ACI 的範圍限制在某些屬性。

6. 按一下 [ 主機 ] 標籤，再按一下 [ 加入 ] 以顯示 [ 加入主機篩選器 ] 對話方塊。

   可以指定主機名稱或 IP 位址。如果指定 IP 位址，則可以使用萬用字元 (*)。

7. 按一下 [ 時間 ] 標籤以顯示表格，列出允許存取的時段。

   依預設值，隨時都允許存取。可以在表格上按一下並拖曳游標，以變更存取時段；您無法選擇不連續的時段。

8. 當您完成編輯 ACI 後，請按一下 [ 確定 ]。

   退出 ACI 編輯器，新的 ACI 會列在 [ACI 管理員 ] 視窗中。

| 備註 | 在建立 ACI 期間，可以隨時按一下 [ 手動編輯 ] 以顯示與您的輸入對應的 LDIF 陳述式。可以修改此陳述式，但所做的變更未必會顯示在圖形介面上。 |
|---|---|

## 編輯 ACI

若要編輯 ACI：

1. 於 [ 目錄 ] 標籤上，在樹狀子目錄的項端項目上按一下滑鼠右鍵，再由快顯功能表中選擇 [ 設定存取權限 ]。

   顯示 [ 存取控制管理員 ] 視窗。該視窗包含屬於項目的 ACI 清單。

2. 在 [ 存取控制管理員 ] 視窗中，反白顯示要編輯的 ACI，再按一下 [ 編輯 ]。

   顯示 [ 存取控制編輯器 ]。如需關於可用此對話方塊編輯資訊的詳細資料，請參閱線上說明。

3. 在 [ 存取控制編輯器 ] 的各個標籤中進行您要的變更。

4. 當您完成編輯 ACI 後，請按一下 [ 確定 ]。

   退出 ACI 編輯器，被修改的 ACI 會列在 [ACI 管理員 ] 中。

## 刪除 ACI

若要刪除 ACI：

1. 於 [ 目錄 ] 標籤上，在樹狀子目錄的項端項目上按一下滑鼠右鍵，再由快顯功能表中選擇 [ 設定存取權限 ]。

   顯示 [ 存取控制管理員 ] 視窗。該視窗包含屬於項目的 ACI 清單。

2. 在 [ 存取控制管理員 ] 視窗中，選取要刪除的 ACI。

3. 按一下 [ 移除 ]。

   [ 存取控制管理員 ] 中不再列示該 ACI。

# 存取控制範例

本節中的範例將說明一家想像的 ISP 公司 example.com 如何執行其存取控制策略。所有範例都會解釋如何從主控台及使用 LDIF 檔案執行指定的工作。

example.com 的業務內容是提供網站代管服務及網際網路存取。example.com 網站代管有部份的服務是儲存用戶端公司的目錄。實際上，example.com 儲存 Company333 與 Company999 這兩家中型公司的目錄，並負責部分管理工作。除此之外，它也爲許多個人訂戶提供網際網路存取。

以下是 example.com 希望執行的存取控制規則：

- 將整個 example.com 樹狀目錄的讀取、搜尋與比較的匿名存取權限授與給 example.com 員工 ( 請參閱第 215 頁「授與匿名存取」 )。
- 將寫入存取權限授與給 example.com 員工，以取得 `homeTelephoneNumber`、`homeAddress` 這類個人資訊 ( 請參閱第 217 頁「授權可寫入存取個人項目」 )。
- 授權 example.com 員工可在其項目中加入任何角色，但某些重要角色除外 ( 請參閱第 219 頁「限制存取重要角色」 )。
- 將 People 分支中項目的所有權利授與給 example.com Human Resources 群組 ( 請參閱第 221 頁「授與尾碼的群組完整存取」 )。
- 授權所有 example.com 員工可在目錄的 Social Committee 分支下建立群組項目，以及可刪除其擁有的群組項目 ( 請參閱第 222 頁「授與加入與刪除群組項目的權利」 )。
- 授權所有 example.com 員工可將他們自己加入目錄的 Social Committee 分支下 ( 請參閱第 228 頁「允許使用者在群組中加入或移除他們自己」 )。
- 授權 Company333 與 Company999 的目錄管理員 (角色) 可分別存取樹狀目錄中各自的分支，但附帶某些條件，例如 SSL 驗證、時間與日期限制及指定位置等 ( 請參閱第 224 頁「將條件式存取授與群組或角色」 )。
- 授權個別訂戶可存取他們自己的項目 ( 請參閱第 217 頁「授權可寫入存取個人項目」 )。
- 拒絕個別訂戶存取他們自己項目中的帳單資訊 ( 請參閱第 226 頁「拒絕存取」 )。
- 授權給全世界可匿名存取個別訂戶樹狀子目錄，但已特別要求不列名的訂戶除外。( 目錄的這個部分可以是位於防火牆外且每天更新一次的從屬伺服器。) 請參閱第 215 頁「授與匿名存取」與 第 228 頁「使用篩選器設定目標」。

## 授與匿名存取

大部分目錄的運作方式是您至少可以匿名存取一個尾碼，進行讀取、搜尋或比較。例如，如果執行一個可供員工搜尋的公司人事目錄 ( 例如電話簿 )，您就可能希望設定這些權限。example.com 內部就是這樣的情況，這會在 ACI "Anonymous example.com" 範例中說明。

作爲一個 ISP，example.com 也要建立可供全世界存取的公開電話簿，以公告所有訂戶的聯絡資訊。這會在 ACI "Anonymous World" 範例中解說。

### *ACI "Anonymous example.com"*

在 LDIF 中，若要將整個 example.com 樹狀目錄的讀取、搜尋與比較權限授與 example.com 員工，請撰寫下列陳述式：

```
aci:(targetattr !="userPassword")(version 3.0; acl "Anonymous
 example"; allow (read, search, compare)
 userdn= "ldap:///anyone" and dns="*.example.com";)
```

此範例假設將 `aci` 加入至 `dc=example,dc=com` 項目。請注意，`userPassword` 屬性不在 ACI 的範圍內。

可執行下列作業，從主控台設定此權限：

1. 於 [ 目錄 ] 標籤上，在左瀏覽樹狀目錄的 example.com 節點上按一下滑鼠右鍵，再選擇快顯式功能表的 [ 設定存取權限 ] 以顯示 [ 存取控制管理員 ]。
2. 按一下 [ 新增 ] 顯示 [ 存取控制編輯器 ]。
3. 在 [ 使用者 / 群組 ] 標籤上的 [ACI 名稱 ] 欄位中，輸入 [Anonymous example.com]。請檢查 [ 全部使用者 ] 已經顯示在授與存取權限的使用者清單中。
4. 在 [ 權利 ] 標籤上，勾選讀取、比較與搜尋權利的核取方塊。請確認已經清除其他的核取方塊。
5. 在 [ 目標 ] 標籤上，按一下 [ 此項目 ]，讓 `dc=example,dc=com` 尾碼在目標目錄項目欄位中顯示。在屬性表中找到 `userPassword` 屬性，並清除對應的核取方塊。

   應該勾選所有其他的核取方塊。如果按一下 [ 名稱 ] 標頭，將屬性清單依字母順序排列，則這項工作會比較容易進行。
6. 在 [ 主機 ] 標籤上按一下 [ 加入 ]，並在 DNS 主機篩選器欄位中輸入 `*.example.com`。按一下 [ 確定 ] 退出對話方塊。
7. 在 [ 存取控制編輯器 ] 視窗中按一下 [ 確定 ]。

   將新的 ACI 加入到 [ 存取控制管理員 ] 視窗中所列示的 ACI 中。

### *ACI "Anonymous World"*

在 LDIF 中，若要將個別訂戶樹狀子目錄的讀取與搜尋存取授與全世界，同時拒絕存取不列名訂戶的資訊，您可以撰寫下列陳述式：

```
aci:(targetfilter= "(!(unlistedSubscriber=yes))")
 (targetattr="homePostalAddress || homePhone || mail")
 (version 3.0; acl "Anonymous World"; allow (read, search)
 userdn="ldap:///anyone";)
```

此範例假設將 ACI 加入至 `ou=subscribers,dc=example, dc=com` 項目。並假設每個訂戶項目都有 `unlistedSubscriber` 屬性，而且設爲 yes 或 no。目標定義會根據此屬性值篩選掉不列名的訂戶。如需關於篩選器定義的詳細資料，請參閱第 228 頁「使用篩選器設定目標」。

可執行下列作業，從主控台設定此權限：

1. 於 [ 目錄 ] 標籤上，在左瀏覽樹狀目錄的 example.com 節點下的 [ 簽署者 ] 項目上按一下滑鼠右鍵，再選擇快顯功能表中的 [ 設定存取權限 ] 以顯示 [ 存取控制管理員 ]。
2. 按一下 [ 新增 ] 顯示 [ 存取控制編輯器 ]。
3. 在 [ 使用者 / 群組 ] 標籤上的 [ACI 名稱 ] 欄位中，輸入 [Anonymous World]。請檢查 [ 全部使用者 ] 已經顯示在授與存取權限的使用者清單中。
4. 在 [ 權利 ] 標籤上，勾選讀取與搜尋權利的核取方塊。請確認已經清除其他的核取方塊。
5. 在 [ 目標 ] 標籤上，按一下 [ 此項目 ]，讓 `dc=subscribers, dc=example,dc=com` 尾碼在目標目錄項目欄位中顯示。
   a. 在次要項目欄位的篩選器中，輸入下列條件：

      (!(unlistedSubscriber=yes))

   b. 在屬性表中，勾選 `homePhone`、`homePostalAddress` 及 `mail` 屬性的核取方塊。

      應該清除所有其他的核取方塊。若要讓工作更加容易，請按一下 [ 全部不選 ] 按鈕，便會清除表格中所有屬性的核取方塊，然後按一下 [ 名稱 ] 標頭依字母順序加以組織，再選取相關的屬性。
6. 按一下「確定」。

   將新的 ACI 加入到 [ 存取控制管理員 ] 視窗中所列示的 ACI 中。

## 授權寫入存取個人項目

許多目錄管理員希望允許內部使用者變更他自己部分的屬性，但不是全部屬性。example.com 的目錄管理員希望允許使用者變更他們自己的密碼、住家電話號碼及住家地址，除此之外均不允許。這會在 ACI "Write example.com" 範例中解說。

example.com 的政策也允許訂戶更新 example.com 樹狀目錄中他們自己的個人資訊，前提是必須與目錄建立 SSL 連線。這會在 ACI "Write Subscribers" 範例中解說。

### *ACI "Write example.com"*

| **備註** | 藉由設定此權限，您也可以授與使用者刪除屬性值的權利。 |
|---|---|

在 LDIF 中，若要授權 example.com 員工可更新其密碼、住家電話號碼及住家地址，請撰寫下列陳述式：

```
aci:(targetattr="userPassword || homePhone ||
 homePostalAddress")(version 3.0; acl "Write example.com";
 allow (write) userdn="ldap:///self" and dns="*.example.com";)
```

此範例假設將 ACI 加入 `ou=People,dc=example,dc=com` 項目。

可執行下列作業，從主控台設定此權限：

1. 於 [ 目錄 ] 標籤上，在左瀏覽樹狀目錄的 `ou=People,dc=example,dc=com` 項目上按一下滑鼠右鍵，再選擇快顯式功能表的 [ 設定存取權限 ] 以顯示 [ 存取控制管理員 ]。
2. 按一下 [ 新增 ] 顯示 [ 存取控制編輯器 ]。
3. 在 [ 使用者 / 群組 ] 標籤上的 [ACI 名稱 ] 欄位中，輸入 [Write example.com]。請在授與存取權限的使用者清單中，執行下列作業：
   a. 選取並移除 [ 全部使用者 ]，然後按一下 [ 加入 ]。

      顯示 [ 加入使用者和群組 ] 對話方塊。
   b. 將 [ 搜尋 ] 區域設定爲 [ 特權 ]，並選取 [ 搜尋 ] 結果清單中的 [ 自身 ]。
   c. 按一下 [ 加入 ] 按鈕，在授與存取權限的使用者清單中列示 [ 自身 ]。
   d. 按一下 [ 確定 ] 退出 [ 加入使用者和群組 ] 對話方塊。
4. 在 [ 權利 ] 標籤上，勾選寫入權利的核取方塊。請確認已經清除其他的核取方塊。

5. 在 [ 目標 ] 標籤上，按一下 [ 此項目 ]，在目標目錄項目欄位中輸入 `ou=People,dc=example,dc=com`。在屬性表中，勾選 `homePhone`、`homePostalAddress` 與 `userPassword` 屬性的核取方塊。

   應該清除所有其他的核取方塊。若要讓工作更加容易，請按一下 [ 全部不選 ] 按鈕，便會清除表格中所有屬性的核取方塊，然後按一下 [ 名稱 ] 標頭依字母順序加以組織，再選取相關的屬性。

6. 在 [ 主機 ] 標籤上，按一下 [ 加入 ] 顯示 [ 加入主機篩選器 ] 對話方塊。在 DNS 主機篩選器欄位中，輸入 `*.example.com`。按一下 [ 確定 ] 退出對話方塊。

7. 在 [ 存取控制編輯器 ] 視窗中按一下 [ 確定 ]。

   將新的 ACI 加入到 [ 存取控制管理員 ] 視窗中所列示的 ACI 中。

### *ACI "Write Subscribers"*

**備註** 藉由設定此權限，您也可以授與使用者刪除屬性值的權利。

在 LDIF 中，若要授權 example.com 訂戶可更新其密碼與住家電話號碼，請撰寫下列陳述式：

```
aci:(targetattr="userPassword || homePhone")
 (version 3.0; acl "Write Subscribers"; allow (write)
 userdn= "ldap://self" and authmethod="ssl";)
```

此範例假設將 `aci` 加入至 `ou=subscribers,dc=example, dc=com` 項目。

請注意，example.com 訂戶對其住家地址沒有寫入存取，因爲他們可能會刪除此屬性，而 example.com 需要這項資訊才能處理帳單。因此，住家地址是關鍵業務資訊。

可執行下列作業，從主控台設定此權限：

1. 於 [ 目錄 ] 標籤上，在左瀏覽樹狀目錄的 example.com 節點下的 [ 簽署者 ] 項目上按一下滑鼠右鍵，再選擇快顯功能表中的 [ 設定存取權限 ] 以顯示 [ 存取控制管理員 ]。

2. 按一下 [ 新增 ] 顯示 [ 存取控制編輯器 ]。

3. 在 [ 使用者 / 群組 ] 標籤上的 [ACI 名稱 ] 欄位中，輸入 [Write Subscribers]。請在授與存取權限的使用者清單中，執行下列作業：

   a. 選取並移除 [ 全部使用者 ]，然後按一下 [ 加入 ]。

      顯示 [ 加入使用者和群組 ] 對話方塊。

   b. 將 [ 搜尋 ] 區域設定爲 [ 特權 ]，並選取 [ 搜尋 ] 結果清單中的 [ 自身 ]。

c. 按一下 [ 加入 ] 按鈕，在授與存取權限的使用者清單中列示 [ 自身 ]。

d. 按一下 [ 確定 ] 退出 [ 加入使用者和群組 ] 對話方塊。

4. 在 [ 權利 ] 標籤上，勾選要寫入的核取方塊。請確認已經清除其他的核取方塊。

5. 在 [ 目標 ] 標籤上，按一下 [ 此項目 ]，讓 `dc=subscribers, dc=example,dc=com` 尾碼在目標目錄項目欄位中顯示。

   a. 在次要項目欄位的篩選器中，輸入下列條件：

      (!(unlistedSubscriber=yes))

   b. 在屬性表中，勾選 `homePhone`、`homePostalAddress` 及 `mail` 屬性的核取方塊。

      應該清除所有其他的核取方塊。若要讓工作更加容易，請按一下 [ 全部不選 ] 按鈕，便會清除表格中所有屬性的核取方塊，然後按一下 [ 名稱 ] 標頭依字母順序加以組織，再選取相關的屬性。

6. 如果希望使用者使用 SSL 進行驗證，請按一下 [ 手動編輯 ] 按鈕以切換到手動編輯模式，並將 `authmethod=ssl` 加入 LDIF 陳述式，使其如下：

```
(targetattr="homePostalAddress || homePhone || mail")
 (version 3.0; acl "Write Subscribers"; allow (write)
 (userdn= "ldap:///self") and authmethod="ssl";)
```

   請注意這是一個分割以便於讀取的連續行。

7. 按一下「確定」。

   將新的 ACI 加入到 [ 存取控制管理員 ] 視窗中所列示的 ACI 中。

## 限制存取重要角色

可以在目錄中使用角色定義，以識別對業務、網路與目錄管理或其他用途具有關鍵影響的功能。

例如，您可以建立一個 `superAdmin` 角色，來識別公司全球各地的網站中，於特定日期時間可提供服務的系統管理員子集。或者，可以建立一個 `First Aid` 角色，包含特定網站上已完成急救訓練的所有工作人員。如需關於建立角色定義的資訊，請參閱第 156 頁「指派角色」。

當角色會對重要的公司或業務功能賦與任何特殊的使用者權限時，應該考慮限制存取該角色。例如，在 example.com 中，員工可以在他們自己的項目中加入任何角色，但 `superAdmin` 角色除外。這會在 ACI "Roles" 範例中解說。

### *ACI "Roles"*

在 LDIF 中，若要授權 example.com 員工可在他們自己的項目中加入 `superAdmin` 角色以外的任何角色，請撰寫下列陳述式：

```
aci:(targetattr="*") (targattrfilters="add=nsRoleDN:
 (nsRoleDN !="cn=superAdmin, dc=example, dc=com")")
 (version 3.0; acl "Roles"; allow (write)
 userdn= "ldap:///self" and dns="*.example.com";)
```

此範例假設將 ACI 加入 `ou=People,dc=example, dc=com` 項目。

可執行下列作業，從主控台設定此權限：

1. 於 [ 目錄 ] 標籤上，在左瀏覽樹狀目錄的 example.com 節點上按一下滑鼠右鍵，再選擇快顯式功能表的 [ 設定存取權限 ] 以顯示 [ 存取控制管理員 ]。
2. 按一下 [ 新增 ] 顯示 [ 存取控制編輯器 ]。
3. 在 [ 使用者 / 群組 ] 標籤上的 [ACI 名稱 ] 欄位中，輸入 [Roles]。請在授與存取權限的使用者清單中，執行下列作業：
   a. 選取並移除 [ 全部使用者 ]，然後按一下 [ 加入 ]。

      顯示 [ 加入使用者和群組 ] 對話方塊。

   b. 將 [ 加入使用者和群組 ] 對話方塊中的 [ 搜尋 ] 區域設定爲 [ 特權 ]，並選取 [ 搜尋 ] 結果清單中的 [ 自身 ]。
   c. 按一下 [ 加入 ] 按鈕，在授與存取權限的使用者清單中列示 [ 自身 ]。
   d. 按一下 [ 確定 ] 退出 [ 加入使用者和群組 ] 對話方塊。
4. 在 [ 權利 ] 標籤上，勾選要寫入的核取方塊。請確認已經清除其他的核取方塊。
5. 在 [ 主機 ] 標籤上，按一下 [ 加入 ] 顯示 [ 加入主機篩選器 ] 對話方塊。在 DNS 主機篩選器欄位中，輸入 `*.example.com`。按一下 [ 確定 ] 退出對話方塊。
6. 若要爲角色建立以值爲基礎的篩選器，請按一下 [ 手動編輯 ] 按鈕以切換到手動編輯模式。將下列加入 LDIF 陳述式的開頭：

   ```
   (targattrfilters="add=nsRoleDN:
    (nsRoleDN != "cn=superAdmin, dc=example,dc=com")")
   ```

   LDIF 陳述式應該如下：

   ```
   (targetattr="*") (targattrfilters="add=nsRoleDN:
    (nsRoleDN != "cn=superAdmin, dc=example,dc=com")")
    (target = "ldap:///dc=example,dc=com")
    (version 3.0; acl "Roles"; allow (write)
    (userdn = "ldap:///self") and (dns="*.example.com");)
   ```

7. 按一下「確定」。

   將新的 ACI 加入到 [ 存取控制管理員 ] 視窗中所列示的 ACI 中。

## 授與對於特定群組的完整存取

大部分目錄會有一個群組用來識別某些公司功能。這些群組可獲得目錄全部或部分的完整存取權。藉由在群組上套用存取權利，您可以避免爲每個成員個別設定存取權利；只要將使用者加入群組，即可簡單地將這些存取權利授與使用者。

例如，使用 [ 一般安裝 ] 處理序安裝 Directory Server 時，便會預設建立一個對目錄擁有完整存取的 Administrators 群組。

在 example.com 中，Human Resources 群組可完整存取目錄的 `ou=People` 分支，使他們能夠更新員工目錄。這會在 ACI "HR" 範例中解說。

### *ACI "HR"*

在 LDIF 中，若要將目錄中 employee 分支的全部權利授與 HR 群組，請使用下列陳述式：

```
aci:(targetattr="*") (version 3.0; acl "HR"; allow (all)
 userdn= "ldap:///cn=HRgroup,ou=People,dc=example,dc=com";)
```

此範例假設將 ACI 加入 `ou=People,dc=example,dc=com` 項目。

可執行下列作業，從主控台設定此權限：

1. 於 [ 目錄 ] 標籤上，在左瀏覽樹狀目錄中 example.com 節點下的 example.com-people 項目上按一下滑鼠右鍵，再選擇快顯功能表中的 [ 設定存取權限 ] 以顯示 [ 存取控制管理員 ]。
2. 按一下 [ 新增 ] 顯示 [ 存取控制編輯器 ]。
3. 在 [ 使用者 / 群組 ] 標籤上的 [ACI 名稱 ] 欄位中，輸入 [HR]。請在授與存取權限的使用者清單中，執行下列作業：
   a. 選取並移除 [ 全部使用者 ]，然後按一下 [ 加入 ]。

      顯示 [ 加入使用者和群組 ] 對話方塊。

   b. 將 [ 搜尋 ] 區域設爲 [ 使用者與群組 ]，並在 [ 搜尋 ] 欄位中輸入 [Hrgroup]。

      此範例假設您已建立 HR 群組或角色。如需關於群組與角色的詳細資訊，請參閱第 5 章「管理身份和角色」。

   c. 按一下 [ 加入 ] 按鈕，將 HR 群組列在被授與存取權限的使用者清單中。

   d. 按一下 [ 確定 ] 退出 [ 加入使用者和群組 ] 對話方塊。

4. 在 [ 權利 ] 標籤上，按一下 [ 全選 ] 按鈕。

   除了代理權利外，應該勾選所有核取方塊。

5. 按一下「確定」。

   將新的 ACI 加入到 [ 存取控制管理員 ] 視窗中所列示的 ACI 中。

## 授與對加入與刪除群組項目的權利

如果可提高工作效率，或增進公司動力，有些組織會希望允許員工在樹狀目錄中建立項目。

以 example.com 爲例，公司有一個活躍的社交委員會，此委員會組織成幾個社團：網球社、游泳社、滑雪社、演藝社等。任何 example.com 員工都可以建立代表新社團的群組項目。這會在 ACI "Create Group" 範例中解說。任何 example.com 員工都可以成爲這些群組的成員。這會在第 228 頁「允許使用者在群組中加入或移除他們自己」下的 ACI "Group Members" 範例中解說。只有群組擁有者可修改或刪除群組項目。這會在 ACI "Delete Group" 範例中解說。

### *ACI "Create Group"*

在 LDIF 中，若要授權 example.com 員工可在 `ou=Social Committee` 分支下建立群組項目，請撰寫下列陳述式：

```
aci:(target="ldap:///ou=social committee,dc=example,dc=com")
 (targetattr="*")(targattrfilters="add=objectClass:
 (|(objectClass=groupOfNames)(objectClass=top))")
 (version 3.0; acl "Create Group"; allow (read,search,add)
 userdn= "ldap:///uid=*,ou=People,dc=example,dc=com")
 and dns="*.example.com";)
```

**備註**

- 此 ACI 不授與寫入權限，也就是項目建立者無法修改項目。
- 因爲伺服器祕密地加入值「top」，您必須在 `targattrfilters` 關鍵字中指定 `objectclass=top`。

此範例假設將 ACI 加入至 `ou=social committee, dc=example,dc=com` 項目。

可執行下列作業，從主控台設定此權限：

1. 於 [ 目錄 ] 標籤上，在左瀏覽樹狀目錄中 example.com 節點下的 Social Committee 項目上按一下滑鼠右鍵，再選擇快顯功能表中的 [ 設定存取權限 ] 以顯示 [ 存取控制管理員 ]。
2. 按一下 [ 新增 ] 顯示 [ 存取控制編輯器 ]。

3. 在 [ 使用者 / 群組 ] 標籤上的 [ACI 名稱 ] 欄位中，輸入 [Create Group]。請在授與存取權限的使用者清單中，執行下列作業：

   a. 選取並移除 [ 全部使用者 ]，然後按一下 [ 加入 ]。

      顯示 [ 加入使用者和群組 ] 對話方塊。

   b. 將 [ 搜尋 ] 區域設定爲 [ 特權 ]，並選取 [ 搜尋 ] 結果清單中的 [ 所有已驗證的使用者 ]。

   c. 按一下 [ 加入 ] 按鈕，讓 [ 所有已驗證的使用者 ] 在授與存取權限的使用者清單中列出。

   d. 按一下 [ 確定 ] 退出 [ 加入使用者和群組 ] 對話方塊。

4. 在 [ 權利 ] 標籤上，勾選讀取、搜尋與加入的核取方塊。請確認已經清除其他的核取方塊。

5. 在 [ 目標 ] 標籤上，按一下 [ 此項目 ]，讓 `ou=social committee, dc=example,dc=com` 尾碼在目標目錄項目欄位中顯示。

6. 在 [ 主機 ] 標籤上，按一下 [ 加入 ] 顯示 [ 加入主機篩選器 ] 對話方塊。在 DNS 主機篩選器欄位中，輸入 `*.example.com`。按一下 [ 確定 ] 退出對話方塊。

7. 若要建立以值爲基礎的篩選器，讓員工只能在此樹狀子目錄中加入群組項目，請按一下 [ 手動編輯 ] 按鈕以切換到手動編輯模式。將下列加入 LDIF 陳述式的開頭：

   ```
   (targattrfilters="add=objectClass:(objectClass=groupOfNames)
    |(objectClass=top)")
   ```

   LDIF 陳述式應該如下：

   ```
   (targetattr = "*")
   (targattrfilters="add=objectClass:(objectClass=groupOfNames)
    |(objectClass=top)") (target="ldap:///ou=social
    committee,dc=example,dc=com) (version 3.0; acl "Create
   Group";
    allow (read,search,add) (userdn= "ldap:///all") and
    (dns="*.example.com"); )
   ```

8. 按一下「確定」。

   將新的 ACI 加入到 [ 存取控制管理員 ] 視窗中所列示的 ACI 中。

### *ACI "Delete Group"*

在 LDIF 中，若要授權 example.com 員工可修改或刪除 `ou=Social Committee` 分支下他們所擁有的群組項目，請撰寫下列陳述式：

```
aci:(target="ou=social committee,dc=example,dc=com)
 (targetattr = "*")
 (targattrfilters="del=objectClass:(objectClass=groupOfNames)")
 (version 3.0; acl "Delete Group"; allow (write,delete)
 userattr="owner#GROUPDN";)
```

此範例假設將 aci 加入至 ou=social committee, dc=example,dc=com 項目。

建立此 ACI 時，使用主控台並不是有效方法，因爲您將必須使用手動編輯模式建立目標篩選器，並檢查群組擁有權。

## 將條件式存取授與群組或角色

在許多情況中，當您將目錄的存取權限授與群組或角色時，您希望確認這些權限受到保護，不會讓侵入者冒用被授權的使用者。因此，在許多情況中，將重要存取權授與給群組或角色的存取控制規則往往附帶許多條件。

舉例來說，example.com 已爲它代管的 Company333 與 Company999 兩家公司各建立一個目錄管理員角色。它希望這些公司能夠管理它們自己的資料，並執行它們自己的存取控制規則，同時又能確保不受侵入者干擾。基於這個原因，Company333 與 Company999 對樹狀目錄中各自的分支擁有完整權利，但必須符合下列條件：

- 使用透過 SSL 的憑證通過驗證的連線
- 要求在星期一到星期四上午 8 點到下午 6 點之間存取，且
- 要求從每家公司指定的 IP 位址存取。

這些條件列在每家公司的單一 ACI 中，分別是 ACI "Company333" 與 ACI "Company999"。因爲這兩個 ACI 的內容相同，下列範例僅解說 "Company333" ACI。

### *ACI "Company333"*

在 LDIF 中，若要授權 Company333 可在上述條件下完整存取目錄中它們自己的分支，請撰寫下列陳述式：

```
aci:(target="ou=Company333,ou=corporate-clients,dc=example,dc=com")
 (targetattr = "*") (version 3.0; acl "Company333"; allow (all)
  (roledn="ldap:///cn=DirectoryAdmin,ou=Company333,
  ou=corporate-clients,dc=example,dc=com") and (authmethod="ssl")
  and (dayofweek="Mon,Tues,Wed,Thu") and (timeofday >= "0800" and
  timeofday <= "1800") and (ip="255.255.123.234"); )
```

此範例假設將 ACI 加入至 ou=Company333, ou=corporate-clients,dc=example,dc=com 項目。

可執行下列作業，從主控台設定此權限：

1. 於 [ 目錄 ] 標籤上，在左瀏覽樹狀目錄中 example.com 節點下的 Company333 項目上按一下滑鼠右鍵，再選擇快顯功能表中的 [ 設定存取權限 ] 以顯示 [ 存取控制管理員 ]。
2. 按一下 [ 新增 ] 顯示 [ 存取控制編輯器 ]。
3. 在 [ 使用者 / 群組 ] 標籤上的 [ACI 名稱 ] 欄位中，輸入 [Company333]。請在授與存取權限的使用者清單中，執行下列作業：
   a. 選取並移除 [ 全部使用者 ]，然後按一下 [ 加入 ]。

      顯示 [ 加入使用者和群組 ] 對話方塊。
   b. 將 [ 搜尋 ] 區域設爲 [ 使用者與群組 ]，並在 [ 搜尋 ] 欄位中輸入 [DirectoryAdmin]。

      此範例假設您已用 `DirectoryAdmin` 的 `cn` 建立一個系統管理員角色。
   c. 按一下 [ 加入 ] 按鈕，將系統管理員角色列在被授與存取權限的使用者清單中。
   d. 按一下 [ 確定 ] 退出 [ 加入使用者和群組 ] 對話方塊。
4. 在 [ 權利 ] 標籤上，按一下 [ 全選 ] 按鈕。
5. 在 [ 目標 ] 標籤上，按一下 [ 此項目 ]，讓 `ou=Company333,ou=corporate-clients,dc=example,dc=com` 尾碼在目標目錄項目欄位中顯示。
6. 在 [ 主機 ] 標籤上，按一下 [ 加入 ] 顯示 [ 加入主機篩選器 ] 對話方塊。在 [IP 位址主機篩選器 ] 欄位中輸入 `255.255.123.234`。按一下 [ 確定 ] 退出對話方塊。

   IP 位址必須是主機電腦上有效的 IP 位址，Company333 系統管理員使用此位址連線到 example.com 目錄。
7. 在 [ 時間 ] 標籤上，選擇對應到星期一到星期四以及上午 8 點到下午 6 點的時段。

   表格下方會出現訊息，指定您已選取的時段。

8. 若要對來自 Company333 系統管理員的連線強制執行 SSL 驗證，請按一下 [ 手動編輯 ] 按鈕以切換到手動編輯模式。將下列加入 LDIF 陳述式的尾碼：

   and (authmethod="ssl")

   LDIF 陳述式應類似：

```
aci:(targetattr = "*")(target="ou=Company333,
 ou=corporate-clients,dc=example,dc=com") (version 3.0; acl
 "Company333"; allow (all)
(roledn="ldap:///cn=DirectoryAdmin,
 ou=Company333,ou=corporate-clients, dc=example,dc=com") and
 (dayofweek="Mon,Tues,Wed,Thu") and (timeofday >= "0800" and
 timeofday <= "1800") and (ip="255.255.123.234") and
 (authmethod="ssl"); )
```

9. 按一下「確定」。

   將新的 ACI 加入到 [ 存取控制管理員 ] 視窗中所列示的 ACI 中。

## 拒絕存取

如果目錄儲存關鍵業務資訊，您可能希望特別地拒絕其存取。

例如，example.com 希望所有訂戶能夠查看其項目下的帳單資訊 ( 如連線時間或帳戶餘額 )，但明確拒絕寫入存取該資訊。這會分別在 ACI "Billing Info Read" 與 ACI "Billing Info Deny" 中解說。

### *ACI "Billing Info Read"*

在 LDIF 中，若要授權訂戶可讀取他們自己項目中的帳單資訊，請撰寫下列陳述式：

```
aci:(targetattr="connectionTime || accountBalance")
 (version 3.0; acl "Billing Info Read"; allow (search,read)
 userdn="ldap:///self";)
```

此範例假設已經在結構中建立相關的屬性，而且將 ACI 加入至 `ou=subscribers,dc=example,dc=com` 項目。

可執行下列作業，從主控台設定此權限：

1. 於 [ 目錄 ] 標籤上，在左瀏覽樹狀目錄的 example.com 節點下簽署者項目上按一下滑鼠右鍵，再選擇快顯功能表中的 [ 設定存取權限 ] 以顯示 [ 存取控制管理員 ]。
2. 按一下 [ 新增 ] 顯示 [ 存取控制編輯器 ]。
3. 在 [ 使用者 / 群組 ] 標籤上的 [ACI 名稱 ] 欄位中，輸入 [Billing Info Read]。請在授與存取權限的使用者清單中，執行下列作業：

a. 選取並移除 [ 全部使用者 ]，然後按一下 [ 加入 ]。

   顯示 [ 加入使用者和群組 ] 對話方塊。

b. 將 [ 加入使用者和群組 ] 對話方塊中的 [ 搜尋 ] 區域設定爲 [ 特權 ]，並選取 [ 搜尋 ] 結果清單中的 [ 自身 ]。

c. 按一下 [ 加入 ] 按鈕，在授與存取權限的使用者清單中列示 [ 自身 ]。

d. 按一下 [ 確定 ] 退出 [ 加入使用者和群組 ] 對話方塊。

4. 在 [ 權利 ] 標籤上，勾選搜尋與讀取權利的核取方塊。請確認已經清除其他的核取方塊。

5. 在 [ 目標 ] 標籤上，按一下 [ 此項目 ]，讓 `ou=subscribers, dc=example,dc=com` 尾碼在目標目錄項目欄位中顯示 。在屬性表中，勾選 `connectionTime` 和 `accountBalance` 屬性的核取方塊。

   應該清除所有其他的核取方塊。若要讓工作更加容易，請按一下 [ 全部不選 ] 按鈕，便會清除表格中所有屬性的核取方塊，然後按一下 [ 名稱 ] 標頭依字母順序加以組織，再選取相關的屬性。

   此範例假設您已經將 `connectionTime` 和 `accountBalance` 屬性加入至結構。

6. 按一下「確定」。

   將新的 ACI 加入到 [ 存取控制管理員 ] 視窗中所列示的 ACI 中。

### *ACI "Billing Info Deny"*

在 LDIF 中，若要拒絕訂戶可修改他們自己項目中帳單資訊的權限，請撰寫下列陳述式：

```
aci:(targetattr="connectionTime || accountBalance")
 (version 3.0; acl "Billing Info Deny";
 deny (write) userdn="ldap:///self";)
```

此範例假設已經在結構中建立相關的屬性，而且將 ACI 加入至 `ou=subscribers,dc=example,dc=com` 項目。

可執行下列作業，從主控台設定此權限：

1. 於 [ 目錄 ] 標籤上，在左瀏覽樹狀目錄的 example.com 節點下簽署者項目上按一下滑鼠右鍵，再選擇快顯功能表中的 [ 設定存取權限 ] 以顯示 [ 存取控制管理員 ]。

2. 按一下 [ 新增 ] 顯示 [ 存取控制編輯器 ]。

3. 在 [ 使用者 / 群組 ] 標籤上的 [ACI 名稱 ] 欄位中，輸入 [Billing Info Deny]。請在授與存取權限的使用者清單中，執行下列作業：

a. 選取並移除 [ 全部使用者 ]，然後按一下 [ 加入 ]。

顯示 [ 加入使用者和群組 ] 對話方塊。

b. 將 [ 加入使用者和群組 ] 對話方塊中的 [ 搜尋 ] 區域設定爲 [ 特權 ]，並選取 [ 搜尋 ] 結果清單中的 [ 自身 ]。

c. 按一下 [ 加入 ] 按鈕，在授與存取權限的使用者清單中列示 [ 自身 ]。

d. 按一下 [ 確定 ] 退出 [ 加入使用者和群組 ] 對話方塊。

4. 在 [ 權利 ] 標籤上，勾選要寫入的核取方塊。請確認已經清除其他的核取方塊。

5. 按一下 [ 手動編輯 ] 按鈕，並在顯示的 LDIF 陳述式中，將 **allow** 變更爲 **deny**。

6. 在 [ 目標 ] 標籤上，按一下 [ 此項目 ]，讓 `ou=subscribers, dc=example,dc=com` 尾碼在目標目錄項目欄位中顯示 。在屬性表中，勾選 `connectionTime` 和 `accountBalance` 屬性的核取方塊。

應該清除所有其他的核取方塊。若要讓工作更加容易，請按一下 [ 全部不選 ] 按鈕，便會清除表格中所有屬性的核取方塊，然後按一下 [ 名稱 ] 標頭依字母順序加以組織，再選取相關的屬性。

此範例假設您已經將 `connectionTime` 和 `accountBalance` 屬性加入至結構。

7. 按一下「確定」。

將新的 ACI 加入到 [ 存取控制管理員 ] 視窗中所列示的 ACI 中。

## 使用篩選器設定目標

如果要設定存取控制，以允許存取散佈目錄各處的許多項目，您可能希望使用篩選器來設定目標。請記住，因爲搜尋篩選器不直接指定您要管理存取的物件名稱，所以很容易不小心允許或拒絕存取錯誤的物件，尤其當目錄變得越複雜時越危險。此外，篩選器可能讓您不容易疑難排解目錄內發生的存取控制問題。

## 允許使用者在群組中加入或移除他們自己

許多目錄會設定 ACI，以允許使用者在群組中加入或移除他們自己。舉例來說，這對於允許使用者在郵件清單中加入及移除他們自己而言是非常有用。

在 example.com 中，員工可以將他們自己加入到 `ou=social committee` 樹狀子目錄下的任何群組項目中。這會在 ACI "Group Members" 範例中解說。

### *ACI "Group Members"*

在 LDIF 中，若要授權 example.com 員工可在群組中加入或刪除他們自己，請撰寫下列陳述式：

```
aci:(targettattr="member")(version 3.0; acl "Group Members";
 allow (selfwrite)
 (userdn= "ldap:///uid=*,ou=People,dc=example,dc=com") ;)
```

此範例假設將 ACI 加入至 `ou=social committee, dc=example,dc=com` 項目。

可執行下列作業，從主控台設定此權限：

1. 於 [ 目錄 ] 標籤上，在左瀏覽樹狀目錄中 `example.com` 節點下的 `People` 項目上按一下滑鼠右鍵，再選擇快顯功能表中的 [ 設定存取權限 ] 以顯示 [ 存取控制管理員 ]。
2. 按一下 [ 新增 ] 顯示 [ 存取控制編輯器 ]。
3. 在 [ 使用者 / 群組 ] 標籤上的 [ACI 名稱 ] 欄位中，輸入 [Group Members]。請在授與存取權限的使用者清單中，執行下列作業：
   a. 選取並移除 [ 全部使用者 ]，然後按一下 [ 加入 ]。

      顯示 [ 加入使用者和群組 ] 對話方塊。

   b. 將 [ 加入使用者和群組 ] 對話方塊中的 [ 搜尋 ] 區域設定爲 [ 特權 ]，並選取 [ 搜尋 ] 結果清單中的 [ 所有已驗證的使用者 ]。
   c. 按一下 [ 加入 ] 按鈕，讓 [ 所有已驗證的使用者 ] 在授與存取權限的使用者清單中列出。
   d. 按一下 [ 確定 ] 退出 [ 加入使用者和群組 ] 對話方塊。
4. 在 [ 權利 ] 標籤上，勾選自寫的核取方塊。請確認已經清除其他的核取方塊。
5. 在 [ 目標 ] 標籤上，在目標目錄項目欄位中輸入 `dc=example,dc=com` 尾碼。在屬性表中，勾選 `member` 屬性的核取方塊。

   應該清除所有其他的核取方塊。若要讓工作更加容易，請按一下 [ 全部不選 ] 按鈕，便會清除表格中所有屬性的核取方塊，然後按一下 [ 名稱 ] 標頭依字母順序加以組織，再選取相關的屬性。
6. 按一下「確定」。

   將新的 ACI 加入到 [ 存取控制管理員 ] 視窗中所列示的 ACI 中。

## 定義含有逗號之 DN 的權限

包含逗號的 DN 在您的 LDIF ACI 陳述式中需要特別處理。在 ACI 陳述式的目標與連結規則部分中，逗號必須以一個反斜線 (\) 忽略掉。下列範例解說此語法：

```
dn:o=example.com Bolivia\, S.A.
objectClass:top
objectClass:organization
aci:(target="ldap:///o=example.com Bolivia\,S.A.")
 (targetattr="*") (version 3.0; acl "aci 2"; allow (all)
 groupdn = "ldap:///cn=Directory Administrators,
 o=example.com Bolivia\, S.A.";)
```

## 代理驗證 ACI 範例

代理驗證方法是一種特殊形式的驗證：使用自己的身份連結到目錄的使用者會透過代理驗證獲得其他使用者的權利。

此範例假設：

- 用戶端應用程式的連結 DN 是 `uid=MoneyWizAcctSoftware, ou=Applications,dc=example,dc=com`。
- 用戶端應用程式要求存取的目標樹狀子目錄是 `ou=Accounting,dc=example,dc=com`。
- 擁有存取權限的 Accounting 管理員已經存在於目錄內的 `ou=Accounting,dc=example,dc=com` 樹狀子目錄中。

爲了讓用戶端應用程式能夠存取 Accounting 樹狀子目錄 ( 使用與 Accounting 管理員相同的存取權限 )：

- Accounting 管理員必須對 `ou=Accounting,dc=example,dc=com` 樹狀子目錄擁有存取權限。例如，下列 ACI 會將所有權利授與 Accounting 管理員項目：

  ```
  aci:(target="ldap:///ou=Accounting,dc=example,dc=com")
   (targetattr="*") (version 3.0; acl "allowAll-AcctAdmin"; allow
   (all) userdn="ldap:///dn:uid=AcctAdministrator,ou=Administrators,
   dc=example,dc=com";)
  ```

- 目錄內必須有下列將代理權利授與用戶端應用程式的 ACI：

  ```
  aci:(target="ldap:///ou=Accounting,dc=example,dc=com")
   (targetattr="*") (version 3.0; acl "allowproxy-
   accountingsoftware"; allow (proxy) userdn=
   "ldap:///dn:uid=MoneyWizAcctSoftware,ou=Applications,
   dc=example,dc=com";)
  ```

設定此 ACI 後，MoneyWizAcctSoftware 用戶端應用程式可連結到目錄，並傳送 `ldapsearch` 或 `ldapmodify` 這一類需要代理 DN 之存取權利的 LDAP 指令。

在以上範例中，如果用戶端希望執行 ldapsearch 指令，該指令會包含下列控制項：

```
ldapsearch \
-D "uid=MoneyWizAcctSoftware,ou=Applications,dc=example,dc=com" \
-w password\
-y "uid=AcctAdministrator,ou=Administrators,dc=example,dc=com"\ ...
```

請注意，用戶端以本身連結，但獲得代理項目的權限。用戶端不需要代理項目的密碼。

**備註** 您不能使用目錄管理員的 DN 做爲代理 DN，也不能將代理權利授與目錄管理員。不僅如此，如果 Directory Server 在同一個連結作業中收到多個代理驗證控制項，便會傳回錯誤給用戶端應用程式，而且連結嘗試不會成功。

## 檢視有效權利

維護目錄項目的存取策略時，若知道您定義的 ACI 對安全性有何影響是有用的。Directory Server 可讓您評估現有 ACI，並回報在指定項目上授與指定使用者的有效權利。

Directory Server 回應可能包含在搜尋作業中 [ 取得有效權利 ] 控制項。此控制項的回應是在搜尋結果中傳回有關項目與屬性的有效權利資訊。這個額外的資訊包括每個項目和每個項目中每個屬性的寫入權限。系統管理員可要求搜尋所用連結 DN 或任意 DN 的權限，讓系統管理員能夠測試目錄使用者的權限。

**小心** 檢視有效權利本身是目錄作業，應該受到保護並做適當的限制。請爲 aclRights 與 aclRightsInfo 屬性建立進一步的 ACI，以限制目錄使用者對這項資訊的存取。

有效權利功能需要依靠 LDAP 控制項。若要檢視鏈接尾碼的有效權利，您必須在鏈接策略中啓用此控制項，如第 122 頁「配置鏈接策略」中所述。您也必須確保用來連結遠端伺服器的代理身份也允許存取有效權利屬性。

# 使用取得有效權利控制項

使用 ldapsearch 指令與 -J "1.3.6.1.4.1.42.2.27.9.5.2" 選項以指定 [ 取得有效權利 ] 控制項。依預設值，控制項將在搜尋結果中傳回項目與屬性上連結 DN 項目的有效權利。請使用下列選項變更預設的行爲：

- -c "dn:*DN*" - 搜尋結果會顯示用指定 *DN* 連結之使用者的有效權利。此選項允許管理員檢查另一個使用者的有效權利。選項 -c "dn:" 將顯示匿名驗證的有效權利。
- -X "*attributeName ...*" - 搜尋結果也會包含具名屬性的有效權利。請使用此選項指定不出現在搜尋結果中的屬性。例如，使用此選項決定使用者是否有權限加入目前不存在項目中的屬性。

若使用 -c 與 -X 屬性中任一項，或同時使用兩者時，則暗示 [ 取得有效權利 ] 控制項的 OID 具有 -J 選項，因此不需要指定。如果您指定有效權利控制項的 NULL 值，則擷取目前使用者的權限和以目前 ldapsearch 操作傳回的屬性與項目的權限。

接著您必須選擇要檢視的資訊類型，可能是簡單權利，或是解釋如何授與或拒絕這些權利的詳細記錄資訊。資訊的類型分別由加入 aclRights 或 aclRightsInfo 來決定，作爲搜尋結果中傳回的屬性。可以要求兩個屬性都收到全部有效權利資訊，雖然簡單權利的資訊會在詳細記錄資訊中重複顯示。

---

**備註** aclRights 與 aclRightsInfo 屬性擁有虛擬作業屬性的行爲。它們不存在目錄中，而且除非明確要求，否則也不會傳回。這些屬性是 Directory Server 在回應 [ 取得有效權利 ] 控制項時所產生的。

基於這個原因，這兩個屬性都不能用於篩選器或任何種類的搜尋作業。

---

有效權利功能繼承其他參數，而這些參數會影響來自啓動搜尋作業的使用者之存取控制 ( 例如驗證方法、機器位址和名稱 )。

下列範例示範使用者如何檢視他在目錄中的權利。在結果中，1 表示授與權限，0 表示拒絕權限：

```
ldapsearch -J "1.3.6.1.4.1.42.2.27.9.5.2" \
           -h rousseau.example.com -p 389 \
           -D "uid=cfuente,ou=People,dc=example,dc=com" \
           -w password -b "dc=example,dc=com" \
           "(objectclass=*)" aclRights
```

```
dn:dc=example,dc=com
aclRights;entryLevel:add:0,delete:0,read:1,write:0,proxy:0

dn:ou=Groups, dc=example,dc=com
aclRights;entryLevel:add:0,delete:0,read:1,write:0,proxy:0

dn:ou=People, dc=example,dc=com
aclRights;entryLevel:add:0,delete:0,read:1,write:0,proxy:0

dn:cn=Accounting Managers,ou=groups,dc=example,dc=com
aclRights;entryLevel:add:0,delete:0,read:1,write:0,proxy:0

dn:cn=HR Managers,ou=groups,dc=example,dc=com
aclRights;entryLevel:add:0,delete:0,read:1,write:0,proxy:0

dn:uid=bjensen,ou=People, dc=example,dc=com
aclRights;entryLevel:add:0,delete:0,read:1,write:0,proxy:0

dn:uid=cfuente, ou=People, dc=example,dc=com
aclRights;entryLevel:add:0,delete:0,read:1,write:1,proxy:0
```

此結果告訴 Carla Fuente，她在目錄中至少擁有讀取存取的項目，以及她可以修改她自己的項目。有效權利控制項不會跳過正常的存取權限，所以使用者絕不會看到他沒有讀取權限的項目。在下列範例中，目錄管理員可以看到 Carla Fuente 沒有讀取權限的項目：

```
ldapsearch -h rousseau.example.com -p 389 \
           -D "cn=Directory Manager" -w password\
           -c "dn:uid=cfuente,ou=People,dc=example,dc=com" \
           -b "dc=example,dc=com" \
           "(objectclass=*)" aclRights

dn:dc=example,dc=com
aclRights;entryLevel:add:0,delete:0,read:1,write:0,proxy:0

dn:ou=Groups, dc=example,dc=com
aclRights;entryLevel:add:0,delete:0,read:1,write:0,proxy:0

dn:cn=Directory Administrators, dc=example,dc=com
aclRights;entryLevel:add:0,delete:0,read:0,write:0,proxy:0

dn:ou=Special Users,dc=example,dc=com
aclRights;entryLevel:add:0,delete:0,read:0,write:0,proxy:0

dn:ou=People, dc=example,dc=com
aclRights;entryLevel:add:0,delete:0,read:1,write:0,proxy:0

dn:cn=Accounting Managers,ou=groups,dc=example,dc=com
aclRights;entryLevel:add:0,delete:0,read:1,write:0,proxy:0

dn:cn=HR Managers,ou=groups,dc=example,dc=com
aclRights;entryLevel:add:0,delete:0,read:1,write:0,proxy:0
```

```
dn:uid=bjensen,ou=People, dc=example,dc=com
aclRights;entryLevel:add:0,delete:0,read:1,write:0,proxy:0

dn:uid=cfuente, ou=People, dc=example,dc=com
aclRights;entryLevel:add:0,delete:0,read:1,write:1,proxy:0
```

在以上輸出中，目錄管理員可以看到 Carla Fuente 既無法檢視特殊的使用者，也無法檢視樹狀目錄的目錄管理員分支。在以下範例中，目錄管理員可以看到 Carla Fuente 無法修改她自己項目中的 `mail` 與 `manager` 屬性：

```
ldapsearch -h rousseau.example.com -p 389 \
           -D "cn=Directory Manager" -w password\
           -c "dn:uid=cfuente,ou=People,dc=example,dc=com" \
           -b "dc=example,dc=com" \
           "(uid=cfuente)" aclRights "*"

version: 1
dn:uid=cfuente, ou=People, dc=example,dc=com

aclRights;attributeLevel;mail:search:1,read:1,compare:1,
 write:0,selfwrite_add:0,selfwrite_delete:0,proxy:0
mail:cfuente@example.com

aclRights;attributeLevel;uid:search:1,read:1,compare:1,
 write:1,selfwrite_add:1,selfwrite_delete:1,proxy:0
uid:cfuente

aclRights;attributeLevel;givenName:search:1,read:1,compare:1,
 write:1,selfwrite_add:1,selfwrite_delete:1,proxy:0
givenName:Carla

aclRights;attributeLevel;sn:search:1,read:1,compare:1,
 write:1,selfwrite_add:1,selfwrite_delete:1,proxy:0
sn:Fuente

aclRights;attributeLevel;cn:search:1,read:1,compare:1,
 write:1,selfwrite_add:1,selfwrite_delete:1,proxy:0
cn:Carla Fuente

aclRights;attributeLevel;userPassword:search:0,read:0,
 compare:0,write:1,selfwrite_add:1,selfwrite_delete:1,proxy:0
userPassword: {SSHA}wnbWHIq2HPiY/5ECwe6MWBGx2KMiZ8JmjF80Ow==

aclRights;attributeLevel;manager:search:1,read:1,compare:1,
 write:0,selfwrite_add:0,selfwrite_delete:0,proxy:0
manager:uid=bjensen,ou=People,dc=example,dc=com

aclRights;attributeLevel;telephoneNumber:search:1,read:1,compare:1,
 write:1,selfwrite_add:1,selfwrite_delete:1,proxy:0
telephoneNumber: (234) 555-7898
```

```
aclRights;attributeLevel;objectClass:search:1,read:1,compare:1,
 write:1,selfwrite_add:1,selfwrite_delete:1,proxy:0
objectClass:top
objectClass:person
objectClass:organizationalPerson
objectClass:inetorgperson

aclRights;entryLevel:add:0,delete:0,read:1,write:0,proxy:0
```

# 了解有效權利結果

有效權利要求依指定的選項傳回下列資訊：

- 權利資訊
- Write、Selfwrite_add 和 Selfwrite_delete 權限
- 記錄資訊

### *權利資訊*

依下列的子類型提供有效權限資訊：

| | |
|---|---|
| `aclRights;entrylevel` | 提供項目層級權限資訊 |
| `aclRights;attributelevel` | 提供屬性層級權限資訊 |
| `aclRightsInfo;entrylevel` | 提供項目層級記錄資訊 |
| `aclRightsInfo;attributelevel` | 提供屬性層級記錄資訊 |

`aclRights` 字串的格式是：*permission:value(permission:value)**

可能的項目層級權限是 `add`、`delete`、`read`、`write` 和 `proxy`。可能的屬性層級權限是 `read`、`search`、`compare`、`write`、`selfwrite_add`、`selfwrite_delete` 和 `proxy`。

這些權限的值可能是下列其中一個：

- `0` - 已授權
- `1` - 未授權
- `?` - 所授權限取決於您加入、刪除或取代的屬性值。如果看到 `?`，請參閱記錄資訊以建立授與或不授與權限的原因。
- `--` 表示問題中的屬性是虛擬屬性，因此無法更新。修改虛擬屬性的唯一辦法就是修改產生該屬性的機制。

### *Write、Selfwrite_add 和 Selfwrite_delete 權限*

在 Directory Server 5.2 中只有寫屬性層級權限有「`?`」值。對於加入和刪除權限，您可以加入及刪除的項目視項目中的屬性值而定。在項目上傳回權限 (`0` 或 `1`)，因爲它們是以 `ldapsearch` 作業傳回，而不是傳回「`?`」。

如果 write 權限的值是 1，則授與加入和刪除所有值 ( 授權 dn 值除外 ) 的 ldapmodify 作業之權限。寫入權限的值是 0，表示未授與加入或刪除任何值 ( 授權 dn 值除外 ) 的 ldapmodify 作業之權限。在其中一個 selfwrite 權限中，明確地傳回授權 dn 值的有效權限，也就是 selfwrite_add 或 selfwrite_delete。

雖然 selfwrite-add 和 selfwrite-delete 屬性層級不存在 ACI 環境中，一組 ACI 可以授與使用者修改操作的*只*加入或*只*刪除部份的 selfwrite 權限。就 selfwrite 權限而言，正在修改中的屬性值是授權 dn。write 沒有同樣的差異，因爲尚未定義爲了寫入權限所修改的屬性值。

有效權限取決於 targattrfilters ACI 時，「?」值表示如需有關權限的詳細資料，請參閱記錄資訊。根據 write、selfwrite_add 和 selfwrite_delete 權限之間的相對複雜*互*依性，表 6-3 說明這三個可能權限的組合所表示的意義。

**表 6-3** 有效權利權限*互*依性

| 寫入 | selfwrite_add | selfwrite_delete | 有效權利說明 |
|---|---|---|---|
| 0 | 0 | 0 | 無法加入或刪除此屬性的任何值。 |
| 0 | 0 | 1 | 只能刪除授權 dn 的值。 |
| 0 | 1 | 0 | 只能加入授權 dn 的值。 |
| 0 | 1 | 1 | 只能加入或刪除授權 dn 的值。 |
| 1 | 0 | 0 | 可以加入或刪除除了授權 dn 之外的所有值。 |
| 1 | 0 | 1 | 可以刪除所有*包含*授權 dn 的值，而且可以加入所有*排除*授權 dn 的值。 |
| 1 | 1 | 0 | 可以加入所有*包含*授權 dn 的值，而且可以刪除所有*排除*授權 dn 的值。 |
| 1 | 1 | 1 | 可以加入或刪除此屬性的所有值。 |
| ? | 0 | 0 | 不可以刪除加入或刪除入授權 dn 的值，但可能可以加入或刪除其他值有關寫入權限的詳細資料，請參閱記錄資訊。 |
| ? | 0 | 1 | 可以刪除，但不能加入授權 dn 的值，而且可能可以加入或刪除其他值。有關寫入權限的詳細資料，請參閱記錄資訊。 |
| ? | 1 | 0 | 可以加入，但不能刪除授權 dn 的值，而且可能可以加入或刪除其他值。有關寫入權限的詳細資料，請參閱記錄資訊。 |
| ? | 1 | 1 | 可以加入和刪除授權 dn 的值，而且可能可以修改加入或修改刪除其他值。有關寫入權限的詳細資料，請參閱記錄資訊。 |

*記錄資訊*

有效權利記錄資訊可讓您了解和偵錯存取控制的困難。記錄資訊包含稱爲 `acl_summary` 的存取控制摘要聲明，指示已允許或拒絕存取控制的原因。存取控制摘要聲明包含下列資訊：

- 是否允許或拒絕存取
- 所授與的權限
- 權限的目標項目
- 目標屬性的名稱
- 所要求的權利主體
- 是否由代理權進行要求，如果是則爲代理驗證 DN。
- 允許或拒絕存取的原因 ( 對偵錯用途很重要 )。可能原因列在 表 6-4 中：

**表 6-4** 有效權利記錄資訊原因與說明

| 記錄資訊原因 | 說明 |
|---|---|
| `no reason available` | 沒有可用於說明爲何允許或拒絕存取的原因。 |
| `no allow acis` | 不允許造成拒絕存取的 ACI 存在。 |
| `result cached deny` | 用於判斷存取允拒絕決定的快取資訊。 |
| `result cached allow` | 用於判斷存取允許決定的快取資訊。 |
| `evaluated allow` | 評估以判斷存取允許決定的 ACI。aci 的名稱包含在記錄資訊中。 |
| `evaluated deny` | 評估以判斷存取拒絕決定的 ACI。aci 的名稱包含在記錄資訊中。 |
| `no acis matched the resource` | 無 ACI 符合造成拒絕存取的資源或目標。 |
| `no acis matched the subject` | 無 ACI 符合造成拒絕存取的要求存取控制之主體。 |
| `allow anyone aci matched anon user` | 有 userdn = `"ldap:///anyone"` 主體的 ACI 允許存取匿名使用者。 |
| `no matching anyone aci for anon user` | 找不到有 userdn = `"ldap:///anyone"` 主體的 ACI，因此拒絕存取匿名使用者。 |
| root 使用者 | 使用者是 root DN 且可以存取。 |

**備註** 未提供虛擬屬性的寫入權限，也沒有提供任何有關的記錄評估資訊，因爲虛擬屬性無法更新。

如需精確的日誌檔格式，請參閱 《Directory Server Administration Reference》。

# 進階的存取控制：使用巨集 ACI

在使用重複樹狀目錄結構的組織中，使用巨集可以最佳化目錄中所用的 ACI 數目。減少樹狀目錄中的 ACI 數目，可讓您更容易管理您的存取控制策略，並改善 ACI 的記憶體使用效率。

巨集是在 ACI 中用來代表 DN 或部分 DN 的預留位置。您可以使用巨集在 ACI 的目標部分或連結規則部分 ( 或兩者 ) 中代表 DN。事實上，當 Directory Server 收到傳入的 LDAP 作業時，便會比對 ACI 巨集與 LDAP 作業的目標資源，以決定對應子字串 ( 若有 )。如果比對結果相符，就使用對應的子字串展開連結規則端的巨集，並評估展開的連結規則，來決定資源的存取權限。

## 巨集 ACI 範例

巨集 ACI 的優點及其運作方式可以用範例做最清楚的說明。第 241 頁的 「圖 6-4」顯示一個樹狀目錄，在此樹狀目錄中有效的使用巨集 ACI 減少整體 ACI 數目。

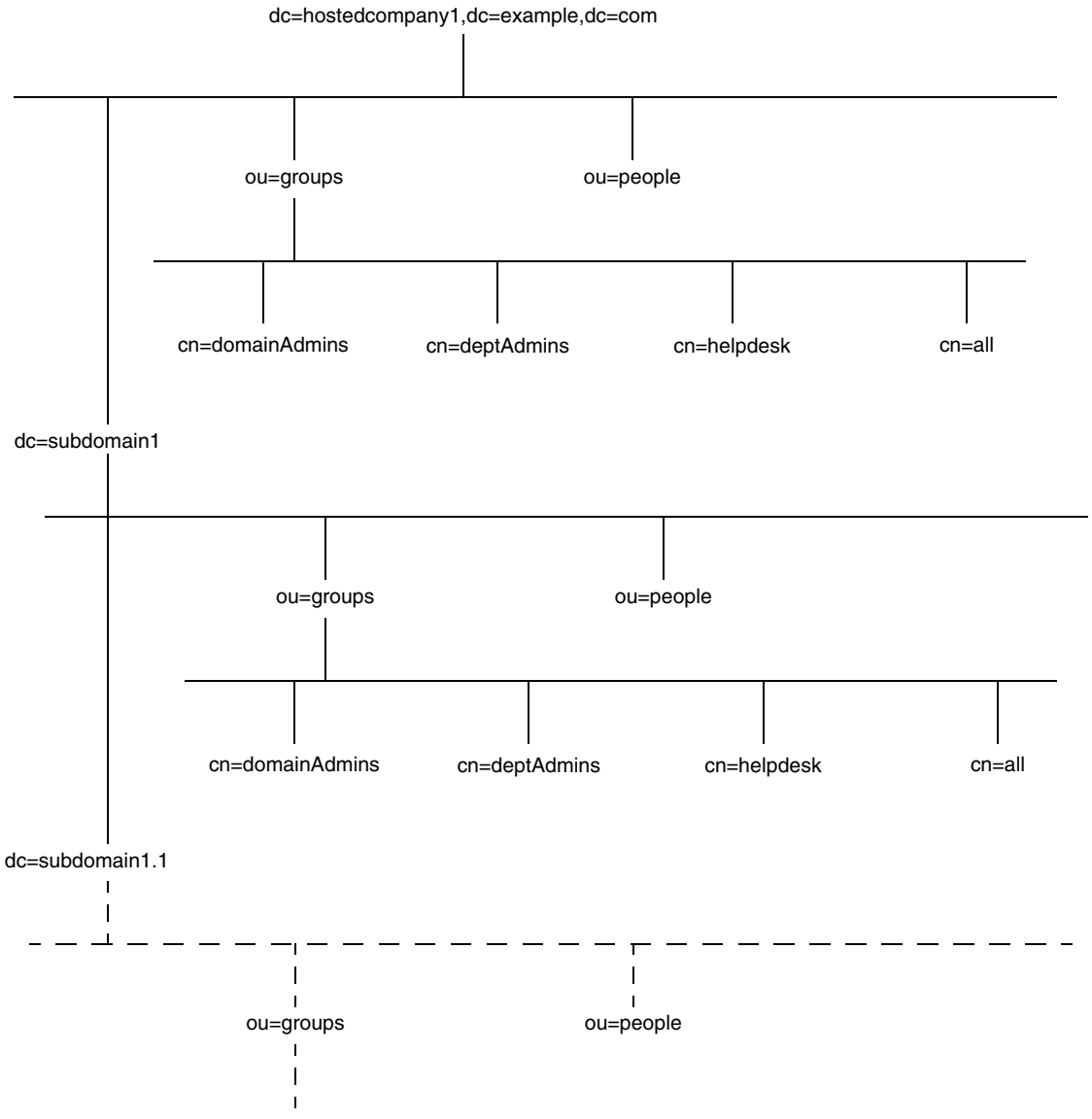
請注意圖中相同樹狀目錄結構 (`ou=groups,ou=people`) 的子網域一再呈現重複的模式。此模式也在整個樹狀目錄中一再重複，因爲 example.com 樹狀目錄儲存下列尾碼：`dc=hostedCompany2,dc=example,dc=com` 和 `dc=hostedCompany3,dc=example,dc=com`。

套用在樹狀目錄的 ACI 也有重複的模式。例如，下列 ACI 位於 `dc=hostedCompany1,dc=example,dc=com` 節點上：

```
aci:(targetattr="*")
 (targetfilter=(objectClass=nsManagedDomain))(version 3.0;
 acl "Domain access"; allow (read,search) groupdn=
 "ldap:///cn=DomainAdmins,ou=Groups,dc=hostedCompany1,
 dc=example,dc=com";)
```

此 ACI 將 DomainAdmins 群組的讀取與搜尋權利授與 `dc=hostedCompany1,dc=example,dc=com` 樹狀目錄中的任何項目。

**圖 6-4** 巨集 ACI 的樹狀目錄範例




下列 ACI 位於 `dc=hostedCompany1,dc=example,dc=com` 節點上：

```
aci:(targetattr="*")
 (targetfilter=(objectClass=nsManagedDomain))
 (version 3.0; acl "Domain access"; allow (read,search)
 groupdn="ldap:///cn=DomainAdmins,ou=Groups,dc=hostedCompany1
,
 dc=example,dc=com";)
```

下列 ACI 位於 dc=subdomain1,dc=hostedCompany1, dc=example,dc=com 節點上：

```
aci:(targetattr="*")
 (targetfilter=(objectClass=nsManagedDomain))
 (version 3.0; acl "Domain access"; allow (read,search)
 groupdn="ldap:///cn=DomainAdmins,ou=Groups,dc=subdomain1,
 dc=hostedCompany1,dc=example,dc=com";)
```

下列 ACI 位於 dc=hostedCompany2,dc=example,dc=com 節點上：

```
aci:(targetattr="*")
 (targetfilter=(objectClass=nsManagedDomain))
 (version 3.0; acl "Domain access"; allow (read,search)
 groupdn="ldap:///cn=DomainAdmins,ou=Groups,dc=hostedCompany2
,
 dc=example,dc=com";)
```

下列 ACI 位於 dc=subdomain1,dc=hostedCompany2, dc=example,dc=com 節點上：

```
aci:(targetattr="*")
 (targetfilter=(objectClass=nsManagedDomain))
 (version 3.0; acl "Domain access"; allow (read,search)
 groupdn="ldap:///cn=DomainAdmins,ou=Groups, dc=subdomain1,
 dc=hostedCompany2,dc=example,dc=com";)
```

在以上顯示的四個 ACI 中，唯一的差別是 groupdn 關鍵字中指定的 DN。藉由使用巨集代替 DN，便可以在 dc=example,dc=com 節點上，用樹狀目錄根部的一個 ACI 取代這些 ACI。此 ACI 顯示如下：

```
aci:(target="ldap:///ou=Groups,($dn),dc=example,dc=com")
 (targetattr="*")(targetfilter=(objectClass=nsManagedDomain))
 (version 3.0; acl "Domain access"; allow (read,search) groupdn=
 "ldap:///cn=DomainAdmins,ou=Groups,[$dn],dc=example,dc=com"
;)
```

請注意，此處必須引進先前未使用過的 target 關鍵字。

在以上範例中，ACI 的數目從四個減少到一個，但實際的優點取決於整個樹狀目錄中重複模式的多寡。

# 巨集 ACI 語法

爲簡化本節中的討論，用來提供連結憑證的 ACI 關鍵字 ( 如 userdn、roledn、groupdn 與 userattr) 合起來稱爲 ACI 的*主體*。主體決定 ACI 的套用對象。

巨集 ACI 包含下列運算式類型，以取代 DN 或部分 DN：

- (\$dn) - 用於對應目標，並直接替代成主體。
- [\$dn] - 用於替代主體的樹狀子目錄中適用的多重 RDN。
- (\$attr.*attributeName*) - 用於將 *attributeName* 屬性的值從目標項目替代成主體。

表 6-5 顯示 ACI 中可使用 DN 巨集的部分：

**表 6-5** ACI 關鍵字中的巨集

| 巨集 | ACI 關鍵字 |
|---|---|
| (\$dn) | target、targetfilter、userdn、roledn、groupdn、userattr |
| [\$dn] | targetfilter、userdn、roledn、groupdn、userattr |
| (\$attr.*attrName*) | userdn、roledn、groupdn、userattr |

適用下列限制：

- 在主體中使用 (\$dn) 與 [\$dn] 巨集時，*必須*定義包含 (\$dn) 巨集的目標。
- 在主體中，(\$dn) 巨集 ( 不是 [\$dn]) 可以跟 (\$attr.*attrName*) 巨集結合。

## 目標中 (\$dn) 的對應

ACI 目標中的 (\$dn) 巨集利用比較 LDAP 要求的目標項目來決定替代值。例如，有一個 LDAP 要求的目標爲 cn=all,ou=groups,dc=subdomain1, dc=hostedCompany1,dc=example,dc=com 項目，而定義目標的 ACI 如下：

```
(target="ldap:///ou=Groups,($dn),dc=example,dc=com")
```

(\$dn) 巨集會對應到 "dc=subdomain1, dc=hostedCompany1"。然後使用這個子字串替代 ACI 的主體。

## 替代主體中的 (\$dn)

在 ACI 的主體中，(\$dn) 巨集會被目標中相符的完整子字串取代。例如：

```
groupdn="ldap:///cn=DomainAdmins,ou=Groups,($dn),
 dc=example,dc=com"
```

變爲：

```
groupdn="ldap:///cn=DomainAdmins,ou=Groups,dc=subdomain1,
 dc=hostedCompany1,dc=example,dc=com"
```

一旦展開巨集後，Directory Server 會依照正常程序評估 ACI，判斷是否授與存取權。

**備註** 使用巨集替代的 ACI 與標準 ACI 不同，前者不一定會爲目標項目的子項授與存取權限。這是因爲，當子項的 DN 是目標時，替代的結果可能不會在主體字串中建立有效的 DN。

## 替代主體中的 [$dn]

[$dn] 的替代機制與 ($dn) 稍有不同。目標資源的 DN 會檢驗數次，每次會丟棄最左邊的 RDN 元件，直到找到相符項爲止。

例如，有一個 LDAP 要求的目標是 cn=all,ou=groups, dc=subdomain1,dc=hostedCompany1,dc=example,dc=com 樹狀子目錄，還有下列 ACI：

```
aci:(targetattr="*")
 (target="ldap:///ou=Groups,($dn),dc=example,dc=com")
 (version 3.0; acl "Domain access"; allow (read,search)
 groupdn="ldap:///cn=DomainAdmins,ou=Groups,[$dn],
 dc=example,dc=com";)
```

伺服器依下列方式處理，以展開此 ACI：

1. 目標中的 ($dn) 符合 dc=subdomain1,dc=hostedCompany1。
2. 將主體中的 [$dn] 以 dc=subdomain1,dc=hostedCompany1 取代。

   產生的主體是 groupdn="ldap:///cn=DomainAdmins,ou=Groups, dc=subdomain1,dc=hostedCompany1,dc=example,dc=com"。如果因爲連結 DN 是該群組的成員而獲得權限，巨集展開就會停止，進行評估 ACI。如果不是成員，處理將會繼續。

3. 將主體中的 [$dn] 以 dc=hostedCompany1 取代。

   產生的主體是 groupdn="ldap:///cn=DomainAdmins,ou=Groups, dc=hostedCompany1,dc=example,dc=com"。同樣地，測試連結 DN 是否爲此群組的成員，如果是，就完整評估 ACI。如果不是成員，巨集展開在最後一個相符值的 RDN 處停止，並且此 ACI 的 ACI 評估至此完成。

[$dn] 巨集的優點在於它以彈性的方式授權網域層級的系統管理員可存取樹狀目錄中的*全部*子網域。因此，在表示網域之間的階層關係時相當有用。

例如，請考慮下列 ACI：

```
aci:(target="ldap:///ou=*,($dn),dc=example,dc=com")
 (targetattr="*")(targetfilter=(objectClass=nsManagedDomain))
 (version 3.0; acl "Domain access"; allow (read,search) groupdn=
 "ldap:///cn=DomainAdmins,ou=Groups,[$dn],dc=example,dc=com";)
```

它授與 cn=DomainAdmins,ou=Groups, dc=hostedCompany1,dc=example,dc=com 的成員對 dc=hostedCompany1 下的所有子網域的存取權限，使得屬於該群組的系統管理員能夠存取 ou=people,dc=subdomain1.1,dc=subdomain1 樹狀子目錄。

但同時，cn=DomainAdmins,ou=Groups, dc=subdomain1.1 的成員會遭到拒絕存取 ou=people,dc=subdomain1, dc=hostedCompany1 和 ou=people,dc=hostedCompany1 節點。

### ($attr.*attrName*) 的巨集對應

($attr.*attrname*) 巨集總是用在 DN 的主體部分。例如，可以定義下列 roledn：

```
roledn = "ldap:///cn=DomainAdmins,($attr.ou),dc=HostedCompany1,
 dc=example,dc=com"
```

假設現在伺服器收到以下列項目爲目標的 LDAP 作業：

```
dn: cn=Babs Jensen,ou=People,dc=HostedCompany1,dc=example,dc=com
cn:Babs Jensen
sn:Jensen
ou:Sales
...
```

爲了評估 ACI 的 roledn 部分，伺服器讀取儲存在目標項目中的 ou 屬性值，並將在主體中的此值替代以展開巨集。在範例中，roledn 展開如下：

```
roledn = "ldap:///cn=DomainAdmins,ou=Sales,dc=HostedCompany1,
 dc=example,dc=com"
```

接下來，Directory Server 會根據正常的 ACI 評估演算法評估 ACI。

當巨集中指定的屬性是多重值屬性時，則會依序使用每個值來展開巨集，並使用第一個對應成功的值。

## 存取控制與複製

ACI 儲存爲項目的屬性，因此，如果包含 ACI 的項目是複製尾碼的一部分，則 ACI 會與其他任何屬性一樣被複製。

ACI 總是在服務傳入 LDAP 要求的目錄伺服器上評估。這表示當取用者伺服器收到更新要求時，它會傳回主機伺服器的參照，然後再評估能否在主機上服務該要求。

## 存取控制和鏈接

如果使用鏈接將樹狀目錄分散在幾部伺服器上，則存取控制陳述式中所使用的關鍵字會有一些限制：如需詳細資訊，請參閱第 182 頁「ACI 限制」。

當驗證使用者存取鏈接尾碼時，伺服器會傳送使用者的身份給遠端伺服器。存取控制總是在遠端伺服器上評估。在遠端伺服器上評估的每一個 LDAP 作業都使用用戶端應用程式原始身份，此身份是透過代理驗證控制項所傳送。只有當使用者對遠端伺服器上包含的樹狀子目錄擁有正確的存取控制時，在遠端伺服器上的作業才會成功。這表示，您必須將一般的存取控制加入到遠端伺服器上，並加上一些限制：如需詳細資訊，請參閱第 120 頁「透過鏈接尾碼的存取控制」。

# 記錄存取控制資訊

若要取得錯誤日誌檔中有關存取控制的資訊，必須設定適當的記錄層級。

若要從主控台設定錯誤日誌檔層級：

1. 在 Directory Server Console 最上層的 [ 目錄 ] 標籤上，以滑鼠右鍵按一下 `cn=config` 節點，並在快顯功能表中選擇 [ 以標準編輯器編輯 ]。

   這會在 [ 標準編輯器 ] 上顯示出 `cn=config` 項目的內容。

2. 將屬性值配對清單向下捲動，以找到 `nsslapd-errorlog-level` 屬性。

3. 將 `nsslapd-errorlog-level` 欄位中已顯示的值再加上 128。

   例如，如果已顯示的值爲 8192 ( 複製除錯 )，您應該將值變更爲 8320。如需關於錯誤日誌檔層級的完整資訊，請參閱 《Directory Server Administration Reference》。

4. 按一下 [ 確定 ] 儲存變更，並退出標準編輯器。

# 舊版的相容性

有些舊版 Directory Server 所用的 ACI 關鍵字在 Directory Server 5.2 中已不再使用。但爲了能與舊版相容性，所以仍然支援這些關鍵字。這些關鍵字是：

- `userdnattr`
- `groupdnattr`

因此，如果您原先在舊供應商伺服器與取用者 Directory Server 5.2 之間已設定複製協議，應該不會在 ACI 的複製中遇到任何問題。

但建議您最好用 `userattr` 關鍵字的功能取代這些關鍵字，如第 199 頁「根據相符值定義存取」中所述。

第 7 章

# 管理使用者帳戶和密碼

使用者連線至 Directory Server 時，系統會驗證該使用者，目錄會根據驗證期間所建立的身份，授與使用者存取權利和資源限制。

本章描述使用者帳戶管理的工作，包括配置目錄的密碼和帳戶鎖定策略，停用帳戶或使用者群組使其無法存取目錄，以及根據使用者的連結 DN 限制使用者可用的系統資源。

Directory Server 支援個別密碼策略。可以定義不同的密碼策略，策略數量不限，並將其中任一個策略套用在指定使用者或使用者群組。這樣可以更容易控制不同類型的使用者存取目錄的方式。

本章包含下列章節：

- 密碼策略概論
- 配置全域密碼策略
- 管理個別密碼策略
- 重設使用者密碼
- 停用與啓用使用者與角色
- 設定個別資源限制

## 密碼策略概論

安全的密碼策略能透過強制執行下列各項，讓與容易被猜測的密碼關聯的風險降至最低：

- 使用者必須根據排程變更他們的密碼。
- 使用者必須提供非一般的密碼。

- 當使用錯誤密碼連結超過指定次數後，帳戶可能會被鎖定。

Directory Server 支援個別和全域密碼策略。個別密碼策略由樹狀目錄中的次要項目定義，該次要項目再供具有該策略的使用者項目參考。如果使用者項目不參考個別策略，就將 `cn=PasswordPolicy,cn=config` 中的全域密碼策略套用至該使用者項目上。

密碼策略僅套用於 `userPassword` 屬性 ( 如果存在於使用者項目中 )，並根據此屬性進行驗證時強制實施。他們無法套用在例如 SASL GSSAPI 或 SSL 驗證等其他驗證。

下一節說明如何執行密碼策略，以及如何將這些策略指派給使用者和群組。如需詳細資訊，請參閱 《Directory Server Deployment Planning Guide》 Chapter 7 的 "Designing Password Policies"。

# 配置全域密碼策略

全域密碼策略適用於目錄中未定義個別策略的所有使用者。但是全域密碼不適用於目錄管理員。

## 使用主控台配置密碼策略

若要設定或修改 Directory Server 的全域密碼策略：

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，選取 [ 資料 ] 節點，然後選取右面板上的 [ 密碼 ] 標籤。
2. 在 [ 密碼 ] 標籤上，設定策略的下列部份：

- 選取 [ 重設後使用者必須變更密碼 ] 核取方塊，指定使用者必須在第一次登入後變更他們的密碼。

  如果選取這個核取方塊，則只授權目錄管理員可以重設使用者的密碼。一般具管理權限的使用者無法強迫使用者更新他們的密碼。

- 若要允許使用者變更自己的密碼，請選取 [ 使用者可以變更密碼 ] 核取方塊。
- 若要限制使用者變更密碼的頻率，請在 [ 允許在 X 天內變更 ] 文字方塊中輸入天數。若要允許使用者視需要任意變更自己的密碼，請選取 [ 無限制 ] 核取方塊。
- 若要防止使用者一再重複使用同一個密碼，請選取 [ 保留密碼記錄 ] 核取方塊，並指定伺服器爲 [ 記位 X 密碼 ] 文字方塊中的每個使用者保留的密碼數量。只要密碼仍存在清單中，使用者就無法設定該密碼。爲有效起見，您也應該限制使用者變更密碼的頻率。

- 如果不希望使用者密碼過期，請選取 [ 密碼永久有效 ] 單選按鈕。
- 否則，請選取 [ 密碼在 X 日後到期 ] 單選按鈕，強迫使用者定期變更密碼，然後輸入使用者密碼保持有效的天數。
- 如果選擇讓密碼會到期，則可以在 [ 在密碼到期前 X 天傳送警告 ] 欄位中，指定在密碼到期前多久須傳送警告給使用者。

  使用者收到警告時，密碼將在原日期到期。取消選取 [ 無論是否傳送警告，允許到期 ] 核取方塊，可延長到期時間，讓傳送警告後能有一段完整的警告期間。警告和延期將只會各發生一次。如果使用者在密碼到期後連結，則不寬限登入。
- 如果您希望伺服器檢查使用者密碼的語法，以確定該密碼符合密碼策略所設定的最小需求，請選取 [ 檢查密碼語法 ] 核取方塊。然後，在 [ 密碼最小長度 ] 文字方塊中指定密碼可接受的最短長度。
- 依預設值，目錄管理員無法重設違反密碼策略的密碼，例如重複使用記錄中的密碼。選取 [ 允許目錄管理員略過密碼策略 ] 核取方塊則可允許此作法。
- 從 [ 密碼加密 ] 下拉式功能表中，指定您希望伺服器儲存密碼時所使用的加密方法。

3. 按一下 [ 帳戶鎖定 ] 標籤，並選取 [ 帳戶必須鎖定 ] 核取方塊以定義帳戶鎖定策略：

- 輸入登入失敗次數和登入失敗期間，失敗必須在這段期間發生該次數後才會觸動鎖定。
- 選取 [ 永遠鎖定 ] 單選按鈕，讓鎖定成爲永久性，直到目錄管理員重設使用者密碼爲止。
- 否則，選取 [ 鎖定持續期間 ] 單選按鈕，並輸入使用者帳戶將暫時鎖定的分鐘數。

4. 完成密碼策略的變更後，請按一下 [ 儲存 ]。將立即強制執行新的全域密碼策略。

## 從指令行設定密碼策略

全域密碼策略由 `cn=Password Policy,cn=config` 項目的屬性定義。請使用 `ldapmodify` 公用程式變更此項目中的全域策略。

有關密碼策略中所有可能屬性的定義，請參閱 《Directory Server Administration Reference》 Chapter 2 的 "cn=Password Policy"。

例如，預設狀況下會關閉密碼語法和長度檢查，並停用帳戶鎖定。使用下列指令可開啓語法檢查，將最短長度設成 8，並啓用 5 分鐘的暫時性鎖定，在連續 5 次錯誤的密碼嘗試後將帳戶鎖定：

```
ldapmodify -h host -p port -D "cn=Directory Manager" -w password
dn:cn=Password Policy,cn=config
changetype:modify
replace:passwordCheckSyntax
passwordCheckSyntax:on
-
replace:passwordMinLength
passwordMinLength: 8
-
replace:passwordLockout
passwordLockout:on
-
replace:passwordMaxFailure
passwordMaxFailure: 5
-
replace:passwordLockoutDuration
passwordLockoutDuration: 300
-
replace:passwordUnlock
passwordUnlock:on
```

# 管理個別密碼策略

個別密碼策略定義於含 passwordPolicy 物件類別的次要項目中。策略可定義在樹狀目錄的任何位置，但是其 DN 的格式必須是 cn=*policy name*,*subtree*。使用 Directory Server Console 或指令行公用程式定義密碼策略後，在所要的使用者項目中設定 passwordPolicySubentry 屬性即可指派密碼策略。

在這一節中，我們舉例說明爲樹狀子目錄根部位在 dc=example,dc=com 的 Example.com 執行臨時員工的密碼策略。

## 使用主控台定義策略

1. 在 Directory Server Console 最上層的 [ 目錄 ] 標籤上，顯示要定義個別密碼策略次要項目的項目。
2. 以滑鼠右鍵按一下項目，並選取 [ 新增 ] > [ 密碼策略 ]。或者，以滑鼠左鍵按一下項目以選取該項目，再從 [ 物件 ] 功能表中選擇 [ 新增 ] > [ 密碼策略 ]。

   顯示 [ 密碼策略 ] 項目的自訂編輯器。

3. 在 [ 一般 ] 欄位中，輸入此策略的名稱和選用描述。這個名稱將成爲定義策略的次要項目的 cn 命名屬性值。

4. 按一下 [ 密碼 ] 標籤以設定策略的下列部分：

- 選取 [ 重設後使用者必須變更密碼 ] 核取方塊，指定使用者必須在第一次登入後變更他們的密碼。如果選取這個核取方塊，則只授權目錄管理員可以重設使用者的密碼。一般具管理權限的使用者無法強迫使用者更新他們的密碼。
- 若要允許使用者變更自己的密碼，請選取 [ 使用者可以變更密碼 ] 核取方塊。
- 若要限制使用者變更密碼的頻率，請在 [ 允許在 X 天內變更 ] 文字方塊中輸入天數。若要允許使用者視喜好任意變更自己的密碼，請選取 [ 無限制 ] 核取方塊。
- 若要防止使用者一再重複使用同一個密碼，請選取 [ 保留密碼記錄 ] 核取方塊，並指定伺服器爲每個使用者保留的密碼數量。只要密碼仍存在清單中，使用者就無法設定該密碼。爲有效起見，您也應該限制使用者變更密碼的頻率。
- 如果不希望使用者密碼過期，請選取 [ 密碼永久有效 ] 單選按鈕。
- 否則，請選取 [ 密碼在 X 日後到期 ] 單選按鈕，強迫使用者定期變更密碼，然後輸入使用者密碼保持有效的天數。
- 如果選擇讓密碼會到期，則可以指定應在密碼到期前多久須傳送警告給使用者。請在 [ 在密碼到期前 X 天傳送警告 ] 文字中，輸入要在密碼到期前應傳送警告的天數。

  使用者收到警告時，密碼將在原日期到期。取消選取 [ 無論是否傳送警告，允許到期 ] 核取方塊，可延長到期時間，讓傳送警告後能有一段完整的警告期間。警告和延期將只會各發生一次。如果使用者在密碼到期後連結，則不寬限登入。
- 如果您希望伺服器檢查使用者密碼的語法，以確定該密碼符合密碼策略所設定的最小需求，請選取 [ 檢查密碼語法 ] 核取方塊。然後，在 [ 密碼最小長度 ] 文字方塊中指定密碼可接受的最短長度。
- 依預設值，目錄管理員無法重設違反密碼策略的密碼，例如重複使用記錄中的密碼。選取 [ 允許目錄管理員略過密碼策略 ] 核取方塊則可允許此作法。
- 從 [ 密碼加密 ] 下拉式功能表中，指定您希望伺服器儲存密碼時所使用的加密方法。

5. 按一下 [ 鎖定 ] 標籤，並選取 [ 帳戶必須鎖定 ] 核取方塊以定義帳戶鎖定策略：

- 輸入登入失敗次數和登入失敗期間，失敗必須在這段期間發生該次數後才會觸動鎖定。
- 選取 [ 永遠鎖定 ] 單選按鈕，讓鎖定成爲永久性，直到目錄管理員重設使用者密碼爲止。

- 否則，選取 [ 鎖定持續期間 ] 單選按鈕，並輸入使用者帳戶將暫時鎖定的分鐘數。

6. 在自訂編輯器中按一下 [ 確定 ] 以儲存策略，並建立其次要項目。

## 從指令行定義策略

對於此密碼策略，想像您希望臨時員工的密碼在 100 天 (8,640,000 秒 ) 後到期，而且從密碼到期前 3 天 (259,200 秒 ) 起，會在使用者連結時傳回到期警告。開啓語法檢查以強制對密碼安全性進行最基本的檢查，並強制鎖定以防止入侵者企圖透過字典式攻擊破解密碼。至於策略的其他部份，則套用預設值。

在 `dc=example,dc=com` 下加入下列次要項目，藉以在 example.com 樹狀子目錄中定義此密碼策略：

```
ldapmodify -a -h host -p port -D "cn=Directory Manager" -w password
dn:cn=TempPolicy,dc=example,dc=com
objectClass:top
objectClass:passwordPolicy
objectClass:LDAPsubentry
cn:TempPolicy
passwordStorageScheme:SSHA
passwordChange:on
passwordMustChange:on
passwordCheckSyntax:on
passwordExp:on
passwordMinLength: 6
passwordMaxAge: 8640000
passwordMinAge: 0
passwordWarning: 259200
passwordInHistory: 6
passwordLockout:on
passwordMaxFailure: 3
passwordUnlock:on
passwordLockoutDuration: 3600
passwordResetFailureCount: 600
```

有關密碼策略中所有可能屬性的定義，請參閱 《Directory Server Administration Reference》 Chapter 2 的 "cn=Password Policy"。

# 指定密碼策略

指派個別密碼策略包括指向適當的策略次要項目。可以將策略加入單一項目中作爲 passwordPolicySubentry 的值，或者可用 CoS 和角色來管理策略。您也必須設定存取控制，以防止使用者修改套用在使用者上的密碼策略。

## 使用主控台

Directory Server 主控台提供了介面，可用於管理指派給使用者或群組的密碼策略：

1. 在 Directory Server Console 最上層的 [ 目錄 ] 標籤上，顯示要指派或修改個別密碼策略的使用者項目或群組項目。
2. 以滑鼠右鍵按一下項目，並選取快顯功能表中的 [ 設定密碼策略 ]。或者，在項目上按一下滑鼠左鍵以選取項目，然後選擇 [ 物件 ] 功能表中的 [ 設定密碼策略 ]。
3. [ 密碼策略 ] 對話方塊告訴您此項目適用哪個密碼策略：

- 如果適用全域策略，請按一下 [ 指派 ] 選擇樹狀目錄中任何位置的密碼策略次要項目。
- 如果已定義個別策略，則可取代、移除或編輯該策略。按一下 [ 編輯策略 ] 將啓動指名的策略次要項目的自訂編輯器。

  指派或取代密碼策略將啓動目錄瀏覽器對話方塊，在此處可以找到顯示小鑰匙圖示的密碼策略次要項目。

4. 如果已變更策略，請在 [ 密碼策略 ] 對話方塊中按一下 [ 確定 ]。新策略將立即生效。

## 從指令行

若要將密碼策略指派給使用者項目或群組項目，請將密碼策略的 DN 加入成爲 passwordPolicySubentry 屬性的值。例如，下列指令將指派 cn=TempPolicy,dc=example,dc=com 給 Barbara Jensen：

```
ldapmodify -h host -p port -D "cn=Directory Manager" -w password
dn:uid=bjensen,ou=People,dc=example,dc=com
changetype:modify
add:passwordPolicySubentry
passwordPolicySubentry:cn=TempPolicy,dc=example,dc=com
```

## 使用角色和 CoS

將使用者依角色分組時，可以使用 CoS 以指向適當的策略次要項目。如需使用角色和 CoS 的詳細資訊，請參閱第 5 章「管理身份和角色」。

舉例來說，下列指令會爲 Example.com 的臨時員工建立篩選的角色，並指派 cn=TempPolicy,dc=example,dc=com 給擁有該角色的員工：

```
ldapmodify -a -h host -p port -D "cn=Directory Manager" -w password
dn:cn=TempFilter,ou=people,dc=example,dc=com
objectclass:top
objectclass:LDAPsubentry
objectclass:nsRoleDefinition
objectclass:nsComplexRoleDefinition
objectclass:nsFilteredRoleDefinition
cn:TempFilter
nsRoleFilter:(&(objectclass=person)(status=contractor))
description:filtered role for temporary employees

dn:cn=PolTempl,dc=example,dc=com
objectclass:top
objectclass:nsContainer

dn:cn="cn=TempFilter,ou=people,dc=example,dc=com",
 cn=PolTempl,dc=example,dc=com
objectclass:top
objectclass:extensibleObject
objectclass:LDAPsubentry
objectclass:costemplate
cosPriority: 1
passwordPolicySubentry:cn=TempPolicy,dc=example,dc=com

dn:cn=PolCoS,dc=example,dc=com
objectclass:top
objectclass:LDAPsubentry
objectclass:cosSuperDefinition
objectclass:cosClassicDefinition
cosTemplateDN:cn=PolTempl,dc=example,dc=com
cosSpecifier:nsRole
cosAttribute:passwordPolicySubentry operational
```

具有 contractor 狀態的使用者現在變成須遵守 cn=TempPolicy,dc=example,dc=com 密碼策略。

## 保護個別密碼策略

若要防止使用者修改所套用的密碼策略，您也必須在根項目加入類似以下的 ACI：

```
ldapmodify -h host -p port -D "cn=Directory Manager" -w password
dn:dc=example,dc=com
changetype:modify
add:aci
aci:(targetattr != "passwordPolicySubentry")(version 3.0; acl
 "Allow self modification except for passwordPolicySubentry";
 allow (write) (userdn ="ldap:///self");)
```

## 重設使用者密碼

目錄將密碼值儲存在使用者項目的 `userPassword` 屬性中。根據伺服器的帳戶控制設定值，使用者可以依照您指定的密碼策略，使用標準工具來設定 `userPassword`，例如 `ldapmodify`。

如果發生永久的帳戶鎖定 ( 在密碼策略中，使用者操作屬性 `accountUnlockTime` 爲 `0`，且 `passwordUnlock` 爲 `off`)，則可將密碼重設爲目錄管理員以解除使用者帳戶的鎖定。例如，假設 Example.com 目錄的使用者 Barbara Jensen 因爲忘記又一再猜錯密碼，而被永久鎖定：

```
ldapmodify -h host -p port -D "cn=Directory Manager" -w password
dn:uid=bjensen,ou=People,dc=example,dc=com
changetype:modify
replace:userPassword
userPassword:ChAnGeMe
```

如果密碼策略中的 `passwordMustChange` 爲 on，Barbara 在下一次連結後必須變更密碼。記得告訴她，您已經將密碼改成 `ChAnGeMe` ( 最好是透過安全的管道 )。

## 停用使用者和角色

可以暫時地停用單一使用者帳戶或一組帳戶。一旦停用後，該使用者便無法連結至目錄。驗證作業將會失敗。

本節中的程序可用來以相同方式停用使用者和角色。然而當您停用角色時，停用的是角色的成員，而不是角色項目本身。如需關於角色的一般資訊，以及角色如何與存取控制互動的特殊資訊，請參閱第 5 章「管理身份和角色」。

## 使用主控台設定使用者與角色啟用

1. 在 Directory Server Console 最上層的 [ 目錄 ] 標籤上，瀏覽樹狀目錄，以顯示要停用或重新啟用的使用者項目或角色項目。
2. 連按兩下項目以顯示自訂編輯器，再按一下左欄中的 [ 帳戶 ] 標籤。

   右面板中顯示項目的啟用狀態。
3. 按一下按鈕以停用或啟用與此項目對應的使用者或角色。編輯器中使用者或角色圖示上會顯示一個紅色方塊，並有一長條穿過，表示項目即將停用。
4. 按一下 [ 確定 ] 關閉對話方塊，儲存項目新的啟用狀態。

   開啟自訂編輯器有一個捷徑，只要選取項目，再從 [ 物件 ] 功能表中選擇 [ 啟用 ] 或 [ 停用 ] 即可。

可以從 [ 主控台 ] 的 [ 檢視 ] > [ 顯示 ] 功能表中選取 [ 停用狀態 ]，即可檢視任何目錄物件的啟用狀態。然後，所有停用項目的圖示就會顯示有紅色長條穿過。不論使用者項目是直接停用，或是透過角色成員關係停用，都會顯示使用者項目正確的啟用狀態。

## 從指令行設定使用者與角色啟用

若要停用使用者帳戶或角色的成員，請使用 `directoryserver account-inactivate` 指令。若要啟動或停止使用者或角色，請使用 `directoryserver account-activate` 指令：

```
# /usr/sbin/directoryserver account-inactivate
# /usr/sbin/directoryserver account-activate
```

下列指令顯示如何使用這些指令停用再重新啟用 Barbara Jensen 的使用者帳戶：

```
/usr/sbin/directoryserver account-inactivate -h host -p port -D
"cn=Directory\
        Manager" -w password -I "uid=bjensen,ou=People,dc=example,dc=com"

/usr/sbin/directoryserver account-activate -h host -p port -D "cn=Directory\
        Manager" -w password -I "uid=bjensen,ou=People,dc=example,dc=com"
```

在這兩組指令中，`-I` 選項指定要設定啟用狀態的使用者或角色的 DN。

如需詳細資訊，請參閱 《Directory Server Administration Reference》 Chapter 1 "`account-activate`" 和 "'`account-inactivate`"。

# 設定個別資源限制

可以使用與目錄連結之用戶端應用程式上的特殊操作屬性值，控制搜尋作業的伺服器限制。可以設定下列搜尋作業限制：

- 詳盡尋找限制用於指定將爲搜尋作業檢查的最大項目數。
- 大小限制用於指定伺服器在回應搜尋作業時，傳回用戶端應用程式的最大項目數。
- 時間限制用於指定伺服器處理搜尋作業所耗費時間的最大值。
- 閒置逾時用於指定伺服器在中斷連線之前，用戶端與伺服器的連線可以閒置的時間。

**備註** 目錄管理員可以預設使用無限制的資源。

您對特定使用者設定的資源限制，其優先順序高於您在全域伺服器組態中所設定的預設資源限制。您應該確認儲存個別資源限制的屬性受到保護，不會被包含使用者項目的尾碼上的下列 ACI 自我修改：

```
(targetattr != "nsroledn || aci || nsLookThroughLimit || nsSizeLimit ||
nsTimeLimit || nsIdleTimeout || passwordPolicySubentry ||
passwordExpirationTime || passwordExpWarned || passwordRetryCount ||
retryCountResetTime || accountUnlockTime || passwordHistory ||
passwordAllowChangeTime")(version 3.0; acl "Allow self entry
modification except for nsroledn, aci, resource limit attributes,
passwordPolicySubentry and password policy state attributes"; allow
(write)userdn ="ldap:///self";)
```

## 使用主控台設定資源限制

1. 在 Directory Server Console 最上層的 [ 目錄 ] 標籤上，瀏覽樹狀目錄，以顯示要設定資源限制的使用者。
2. 連按兩下項目以顯示自訂編輯器，並在左欄中按一下 [ 帳戶 ] 標籤。右面板中顯示目前在項目上設定的限制。
3. 在四個文字欄位中爲上述的資源限制輸入值。輸入值 -1 表示該資源沒有限制。
4. 完成時按一下 [ 確定 ]，以儲存新限制。

# 從指令行設定資源限制

使用 ldapmodify 指令可以在使用者項目上設定下列屬性，以限制該使用者的資源使用情形：

| 屬性 | 描述 |
|---|---|
| nsLookThroughLimit | 指定搜尋作業檢查的項目數。指定爲項目數目。指定此屬性 -1 值代表沒有限制。 |
| nsSizeLimit | 指定伺服器在回應搜尋作業時，傳回用戶端應用程式的最大項目數。指定此屬性 -1 值代表沒有限制。 |
| nsTimeLimit | 指定伺服器處理搜尋作業所耗費時間的最大值。將這個屬性值設定爲 -1 代表沒有時間限制。 |
| nsIdleTimeout | 指定在中斷連線之前，伺服器連線能夠閒置的時間。此值以秒爲單位。指定此屬性 -1 值代表沒有限制。 |

例如，可以依下列方式執行 ldapmodify 以設定項目的大小限制：

```
ldapmodify -h host -p port -D "cn=Directory Manager" -w password
dn:uid=bjensen,ou=People,dc=example,dc=com
changetype:modify
add:nsSizeLimit
nsSizeLimit: 500
```

ldapmodify 陳述式將 nsSizeLimit 屬性加入 Barbara Jensen 的項目中，並將其搜尋傳回的大小限制爲 500 個項目。

第 8 章

# 管理複製

複製是自動將目錄內容從一個 Directory Server 複製到另一個或多個 Directory Server 的機制。任一種寫入作業 - 加入、修改或甚至刪除項目 - 都會自動對映到其他 Directory Server。如需關於複製概念、複製案例以及目錄佈署中複製規劃方式等完整說明，請參閱《Directory Server Deployment Planning Guide》 Chapter 6 "Understanding Replication"。

Directory Server 5.2 包括以下新的複製功能：

- 透過廣域網路 (WAN) 的多重主機複製 (MMR) 可讓您在地理位置相距甚遠的主機之間建立複製協議，更有效地分散您的資料。
- MMR 現在支援 4 個能同時完全連接的主機，以提供額外的容錯移轉保護。
- 二進位複製使大型複本的初始化更快速。
- 部份複製可讓您指定要複製的屬性組，以便更有效率地分散您的資料。
- 新的指令行工具幫您監控複製括動。

本章描述爲了設定各種複製案例所要執行的工作，而且包含以下主題：

# 簡介

複製組態的配置工作相當複雜。開始之前，您應該充分瞭解組織即將佈署複製的方式，例如，要使用單一主機、多重主機還是有集線器的階層式複製。複製的單位是尾碼或子尾碼：屬於該尾碼的所有項目將會一起複製。在您計劃的部署中，您必須根據尾碼所包含的資料來識別主機、集線器或專屬用戶。

伺服器上複製的尾碼稱爲*複本*。主機是指接受來自用戶端的讀寫作業的複本。集線器與專屬用戶是只透過複製機制接收更新的唯讀複本；集線器會從主機或另一個集線器接收更新，然後轉送給另一個集線器或專屬用戶。專屬用戶則只接收來自用戶或集線器的更新。

下列三個圖表顯示一般複製案例中，複本之間的關係。

**圖 8-1** 單一主機複製

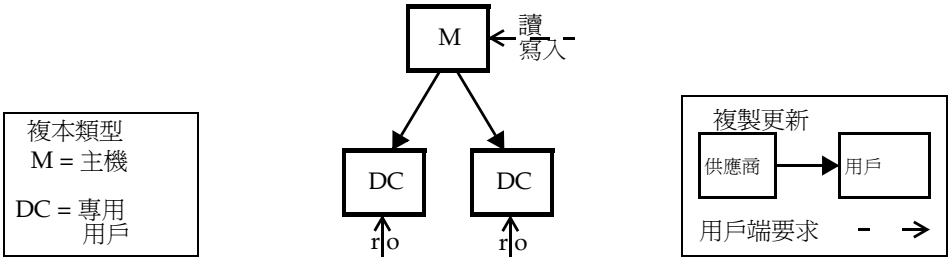



**圖 8-2** 有集線器的階層式複製

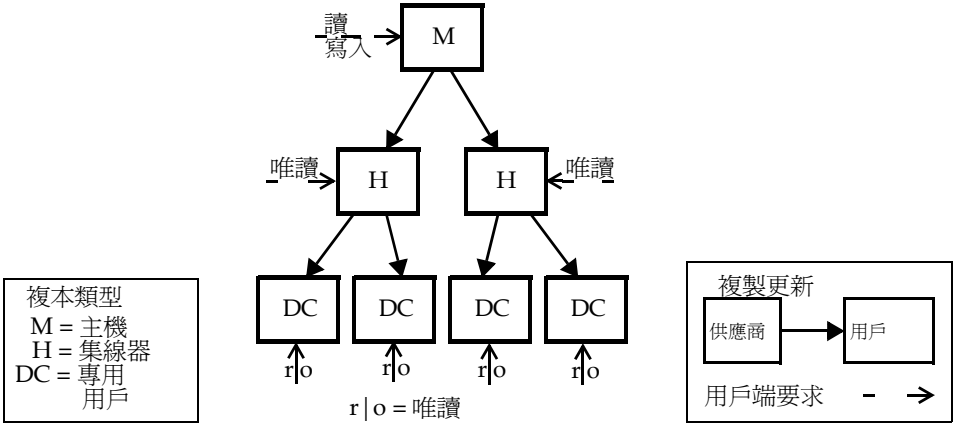
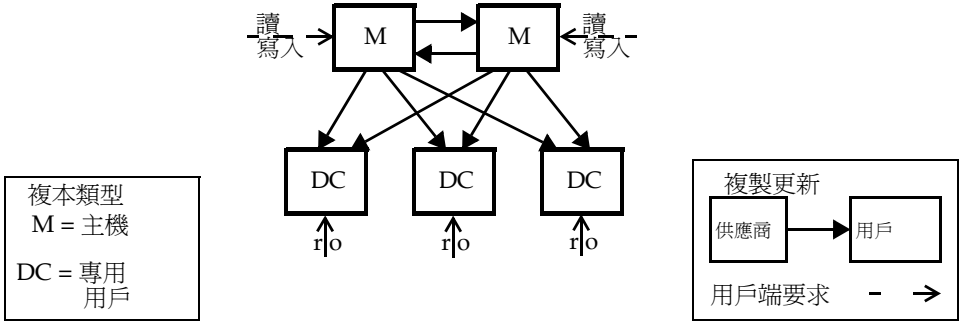



**圖 8-3** 多重主機複製




本文件也使用*供應商*與*用戶*等用語表示複製協議中兩個參與伺服器的角色。供應商

是傳送複製更新的伺服器，用戶則是接收複製更新的伺服器。上圖所顯示的關係如下：

- 單一主機是供應商，不是用戶。
- 多重主機複製中的主機既是供應商，*也是*其他主機的用戶。
- 集線器永遠是供應商兼用戶。
- 專屬用戶只是用戶。

許多複製設定值適用於協議中供應商或用戶角色的複本，不論其類型爲何。

# 配置複製的步驟摘要

下列步驟假設您要複製單一尾碼。如果您要複製多個尾碼，請在每部伺服器上同時進行相同的配置。換句話說，您可以重複每個步驟在多重尾碼上配置複製。

若要配置任何複製拓樸，依照下列順序進行：

1. 定義除單一主機外的所有伺服器上的複製管理員項目 ( 或使用所有伺服器上的預設複製管理員。)
2. 在所有包含專屬用戶複本的伺服器上，執行下列步驟：
   a. 爲用戶複本建立空白尾碼。
   b. 透過複製精靈啓用尾碼上的用戶複本。
   c. 選擇性地配置進階複本設定值。
3. 在所有包含集線器複本的伺服器上，執行下列步驟：
   a. 爲集線器複本建立空白尾碼。
   b. 透過複製精靈在尾碼上啓用集線器複本。
   c. 選擇性地配置進階複本設定值。
4. 在所有包含主機複本的伺服器上，執行下列步驟：
   a. 在要做爲主機複本的其中一個主機上選擇或建立尾碼。
   b. 透過複製精靈在尾碼上啓用主機複本。
   c. 選擇性地配置進階複本設定值。
5. 依照下列順序，在所有供應商複本上配置複製協議：
   a. 介於多重主機集合中的主機之間。

b. 介於主機與其專屬用戶之間。

c. 介於主機與集線器複本之間。

或者，您可以在此階段配置部份複製。

6. 配置介於集線器複本及其用戶之間的複製協議，

7. 若是在多重主機複製的情況下，請從包含原始資料的同一個主機複本初始化所有主機。初始化集線器和客戶複本。

**備註** 嘗試建立複製協議之前，啓用所有複製很重要。這樣可讓您在建立複製協議之後，立即初始化用戶複本。用戶初始化永遠是設定複製的最後一個階段。

# 選擇複製管理員

設定複製時其中一項重要的工作便是：選擇供應商在傳送複製更新時用來與用戶伺服器連結的項目，此項目稱爲*複製管理員*。所有含有接收更新的尾碼之伺服器，必須至少擁有一個複製管理員項目。

Directory Server 有預設複製管理員項目，此項目可用於每一台伺服器；它的 DN 是 `cn=Replication Manager,cn=replication,cn=config`。

對於簡單的複製案例，建議您使用預設的複製管理員。複製精靈會自動用此項目配置用戶複本，因而簡化複本的部署工作。

如果未定義密碼，複製精靈會提示您爲預設複製管理員設定密碼。日後若要變更密碼：

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，選擇 [ 資料 ] 節點，然後選擇右面板上的 [ 複製 ] 標籤。

2. 在 [ 複製管理員 ] 標題下的兩個文字欄位內輸入新的密碼。

3. 確認密碼之後，按一下 [ 儲存 ]。如果密碼與確認密碼不相符，便無法使用 [ 儲存 ] 按鈕。

如果不使用預設複製管理員，您可以建立任何新項目作爲複製管理員。例如，您可能想讓每個複製管理員項目，對每個複製的尾碼各有不同的密碼。另一個自行建立複製管理員的原因，是爲了支援不同的複製驗證模式，例如透過 SSL 使用憑證。

複製管理員項目必須包含您在定義複製協議時，所選擇的驗證方法需要的屬性。例如，預設複製管理員是一個 person 物件類別，可讓 userPassword 屬性進行簡單驗證。如需關於使用憑證連結複製管理員的詳細資料，請參閱第 288 頁「透過 SSL 複製」。

此複製管理員項目不應該位於用戶伺服器的複製尾碼中。適合定義複製管理員的位置在 cn=replication,cn=config 中。

如果您從指令行手動建立新的複製管理員，您必須透過修改複製組態項目的 nsDS5ReplicaBindDN 屬性指定客戶的連結 DN。

如果您正在使用原來的複製，複製管理員項目上會有其他限制。如需詳細資訊，請參閱第 300 頁「將 Directory Server 5.2 設定爲 Directory Server 4.x 的用戶」。

| | |
|---|---|
| 小心 | 您不能使用複製管理員項目的 DN 和密碼，在伺服器上連結或執行作業。複製管理員只能用於複製機制和其他可能需要重新初始化複本時使用。<br><br>您必須從未將目錄管理員當作複製管理員使用。 |

爲每個用戶選好複製管理員後，執行下列步驟：

1. 寫下或記住您所選擇或建立的複製管理員 DN。稍後在此用戶的供應商上建立供應商與此用戶的複製協議時，會需要此 DN 及其密碼。
2. 如果您定義密碼到期策略，您必須記住排除複製管理員，否則當密碼到期時，將無法複製。若要讓複製管理員項目的密碼不會到期，請建立密碼不會到期的密碼策略，再將它指定給複製管理員項目。如需詳細資訊，請參閱第 252 頁「管理個別密碼策略」。

## 配置專屬用戶

專屬用戶是複製尾碼的唯讀複本。它會接收來自連結爲複製管理員之伺服器的更新，以進行變更。配置用戶伺服器的工作包括準備空白尾碼以儲存複本，並使用複製精靈啓用該尾碼上的複製。可選用的進階組態包括選擇不同的複製管理員、設定參照或設定清除延遲。

下列各節提供在伺服器上配置一個專屬用戶複本的步驟。請在包含指定尾碼之專屬用戶複本的每部伺服器上重複所有程序。

## 爲用戶複本建立尾碼

如果用戶上還沒有空白尾碼，請使用與預訂主機複本相同的 DN 建立一個空白尾碼。如需說明，請參閱第 99 頁「建立尾碼」。

如果尾碼存在而且不是空白，則其內容會在從主機初始化複本時遺失。

## 啓用用戶複本

複製精靈簡化了啓用專屬用戶複本的工作：

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，展開 [ 資料 ] 節點與要設爲用戶複本的尾碼節點，然後選擇尾碼下方的 [ 複製 ] 節點。

   在右面板中顯示複製狀態資訊。

2. 按一下 [ 啓用複製 ] 按鈕開始複製精靈。

3. 預設狀態下會選擇 [ 用戶複本 ] 單選按鈕。按一下 [ 下一步 ] 繼續。

4. 如果尚未如此做，則會提示您輸入並確認預設複製管理員的密碼。在每一個欄位中輸入相同的密碼，再按一下 [ 下一步 ] 繼續。

   如果預設複製管理員已經定義密碼，精靈會略過此步驟。

5. 複製精靈於更新複製組態的同時，顯示狀態訊息。完成時，請按一下 [ 關閉 ]。

複製狀態現在顯示複製已經準備好接收更新，而且在左窗格中的圖示會變更以反映這項變化。

## 進階用戶組態

依預設值，複製精靈會將複本設爲使用預設的複製管理員。如果您想要使用不同的複製管理員項目，則必須設定進階組態。您也可以使用此對話方塊，設定修改和清除延遲的參照。

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，展開 [ 資料 ] 節點和您想要配置尾碼的節點，然後選擇尾碼下方的 [ 複製 ] 節點。

2. 在右面板中，按一下 [ 進階 ] 按鈕，顯示 [ 進階複本設定值 ] 對話方塊。

3. 在 [ 連結 DN] 標籤上，使用 [ 加入 ] 和 [ 刪除 ] 按鈕，建立有效複製管理員的 DN 清單。接著供應商可以於與此複本之間的協議內來使用任何一個 DN。您可利用輸入新 DN 的名稱或瀏覽目錄來加入新的 DN。

   若要透過 SSL 使用憑證來配置複製，請輸入憑證項目的 DN 作爲其中一個複製管理員。

4. 當您完成或選取更進階組態的 [ 選用 ] 標籤時，請按一下 [ 確定 ]。

5. 在 [ 進階複本設定值 ] 對話方塊的 [ 選用 ] 標籤上，LDAP URL 清單會指定傳送給此用戶之修改要求的額外參照。使用 [ 加入 ] 或 [ 刪除 ] 按鈕，建立 LDAP URL 清單。

   複製機制會自動配置用戶傳回複製拓樸中所有已知主機的參照。這些預設參照假設用戶端會在一般連線上使用簡單驗証。如果想要利用安全連線的 SSL 將與主機連結的選項提供給用戶端，請加入使用安全 *port* 號碼之格式 `ldaps://`*servername*`:`*port* 的參照。( 如果主機只是爲了安全連線而配置，URL 將依預設值指向安全的連接埠。)

   如果您已經加入一或多個 LDAP URL 作爲參照，則選擇清單下方的核取方塊時，會強迫用戶爲這些 LDAP URL 獨佔地傳送參照，而非爲主機複本。例如，如果您要用戶端永遠被參照到主機伺服器上的安全連接埠而不是預設連接埠，請建立這些安全連接埠的 LDAP URL 清單，並選取此核取方塊。如果您想要指定特定的主機，或指定應該處理所有更新的 Directory Server 代理，則您也可以使用獨占參照。

6. 此外，在 [ 選用 ] 標籤上，您也可以變更清除延遲。

   用戶伺服器儲存有關複本內容更新的內部資訊，而清除延遲參數則指定其保留此資訊的時間，這與其供應商伺服器上變更記錄的 `MaxAge` 參數有關。在兩個參數中，較短的參數可決定兩部伺服器間的複製在停用或當機後仍能回復正常的最長時間。預設值是 7 天，這已足夠大部份情況使用。

7. 按一下 [ 確定 ] 儲存此複本的進階複製組態。

# 配置集線器

集線器複本同時作爲用戶與主機，將複製資料進一步分散給更多用戶。集線器複本接收來自供應商的複製更新，並將複製更新傳給其用戶。集線器複本不接受修改，而是將參照傳回給主機。

配置集線器伺服器的工作包括準備空白的尾碼以儲存複本，並使用複製精靈啓用該尾碼上的複製。可選用的進階組態包括選擇不同的複製管理員、設定參照、設定清除延遲及設定變更記錄參數。

下列各節提供設定一個集線器伺服器的步驟。請在包含指定尾碼之集線器複本的每部伺服器上重複所有程序。

## 爲集線器複本建立尾碼

如果集線器伺服器上還沒有空白尾碼，請用與預訂主機複本相同的 DN 建立一個空白尾碼。如需說明，請參閱第 99 頁「建立尾碼」。

如果尾碼存在而且不是空白，則其內容會在從主機初始化複本時遺失。

## 啓用集線器複本

複製精靈簡化了啓用集線器複本的工作：

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，展開 [ 資料 ] 節點與要設爲集線器複本的尾碼節點，然後選擇尾碼下方的 [ 複製 ] 節點。

   在右面板中顯示複製狀態資訊。

2. 按一下 [ 啓用複製 ] 按鈕開始複製精靈。

3. 選擇 [ 集線器複本 ] 單選按鈕，再按一下 [ 下一步 ] 繼續。

4. 如果尚未如此做，則會提示您選擇變更日誌檔。預設變更日誌檔在文字欄位中顯示。如果不想要使用預設，請輸入變更記錄的檔名，或按一下 [ 瀏覽 ] 顯示檔案選擇器。

   如果已經啓用變更記錄，精靈會略過此步驟。

5. 按一下 [ 下一步 ]。如果尚未如此做，則會提示您輸入並確認預設複製管理員的密碼。在每一個欄位中輸入相同的密碼，再按一下 [ 下一步 ] 繼續。

   如果預設複製管理員已經定義密碼，精靈會略過此步驟。

6. 複製精靈於更新複製組態同時，也會顯示狀態訊息。完成時，請按一下 [ 關閉 ]。

複製狀態現在顯示複製已經準備好接收更新，而且在左窗格中的圖示會變更以反映這項變化。

## 進階集線器組態

集線器伺服器作爲供應商時需要變更記錄，而精靈會將集線器複本設爲使用預設的變更記錄設定值。若要修改這些設定值，請執行下列步驟：

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，選擇 [ 資料 ] 節點，然後選擇右面板上的 [ 複製 ] 標籤。
2. 您可能需要選取 [ 啓用變更記錄 ] 核取方塊並按一下 [ 重設 ] 按鈕，重新整理此標籤的內容。接著，應該會看到您在複製精靈中選擇的變更日誌檔。
3. 您可以對變更日誌檔的名稱變更，並更新變更記錄參數：
   a. 變更記錄最大筆數 - 對於爲了傳送更新給用戶而儲存的修改而言，變更記錄最大筆數可決定該修改的總數。依據預設，這是無限制的。如果您的複本收到許多大型的修改，您或許想要限制記錄的數目以節省磁碟空間。
   b. 變更記錄最長期限 - 可決定集線器儲存必須傳送給用戶更新的時間。依據預設，這是無限制的。建議使用變更記錄最長期限參數限制變更記錄大小。

複製精靈也使用預設的複製管理員。如果已經建立想要使用的不同複製管理員項目，則需要設定進階組態。您也可以使用此對話方塊，設定修改和清除延遲的參照。

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，展開 [ 資料 ] 節點和您想要配置尾碼的節點，然後選擇尾碼下方的 [ 複製 ] 節點。
2. 在右面板中，按一下 [ 進階 ] 按鈕，顯示 [ 進階複本設定值 ] 對話方塊。
3. 在 [ 連結 DN] 標籤上，使用 [ 加入 ] 和 [ 刪除 ] 按鈕，建立有效複製管理員的 DN 清單。接著供應商可以於與此複本之間的協議內來使用任何一個 DN。您可利用輸入新 DN 的名稱或瀏覽目錄來加入新的 DN。

   若要透過 SSL 使用憑證來配置複製，請輸入憑證項目的 DN 作爲其中一個複製管理員。
4. 當您完成或選取更進階組態的 [ 選用 ] 標籤時，請按一下 [ 確定 ]。
5. 在 [ 進階複本設定值 ] 對話方塊的 [ 選用 ] 標籤上，LDAP URL 清單會指定傳送給此集線器之修改要求的額外參照。使用 [ 加入 ] 或 [ 刪除 ] 按鈕，建立 LDAP URL 清單。

   複製機制可自動配置集線器，以傳回複製拓樸中所有已知主機的參照。這些預設參照假設用戶端會在一般連線上使用簡單驗証。如果想要利用安全連線的 SSL 將與主機連結的選項提供給用戶端，請加入使用安全 *port* 號碼之格式 `ldaps://`*servername*`:`*port* 的參照。

   如果您已經加入一或多個 LDAP URL 作爲參照，則選擇清單下方的核取方塊時，會限制伺服器只爲這些 LDAP URL 傳送參照，而非爲主機複本。例如，如果您要用戶端永遠被參照到主機伺服器上的安全連接埠而不是預設連接埠，請建立這些安全連接埠的 LDAP URL 清單，並選取此核取方塊。如果您想要指定特定的主機，或指定應該處理所有更新的 Directory Server 代理，則您也可以使用獨占參照。

6. 此外，在 [ 選用 ] 標籤上，您也可以變更清除延遲。

   集線器伺服器儲存有關複本內容更新的內部資訊，而清除延遲參數則指定其保留這些資訊的時間，這與供應更新之伺服器上的變更記錄 ( *不是*它自己的變更記錄 ) 的 MaxAge 參數有關。在兩個參數中，較短的參數可決定兩部伺服器間的複製在停用或當機後仍能回復正常的最長時間。預設值是 7 天，這已足夠大部份情況使用。

7. 按一下 [ 確定 ] 儲存此複本的進階複製組態。

# 配置主機複本

主機複本包含資料的主要複本，並先將所有修改集中之後，再將更新傳給其他所有複本。主機會記錄所有變更，檢查用戶狀態，並在需要時將更新傳給用戶。在多重主機複製中，主機複本也會收到來自其他主機的更新。

配置主機伺服器的工作包括定義包含主機複本的尾碼、用複製精靈啓用主機複本以及視需要配置進階複製。

下列各節提供配置一個主機伺服器的步驟。請在包含指定尾碼之主機複本的每部伺服器上重複所有程序。

## 爲主機複本定義尾碼

在包含要複製之項目的主機伺服器上選擇或建立尾碼。如需說明，請參閱第 99 頁「建立尾碼」。

建立複製協議之前，尾碼應包含所有的初始資料。如此一來，您才能夠立即根據這些資料初始化用戶複本。爲確保正確的多重主機組態與初始化，應該只有其中一個主機包含所有初始資料，而其他主機上的尾碼應該空白。

## 啓用主機複本

複製精靈簡化了啓用主機複本的工作：

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，展開 [ 資料 ] 節點與要設爲主複本的尾碼節點，然後選擇尾碼下方的 [ 複製 ] 節點。

   在右面板中顯示複製狀態資訊。

2. 按一下 [ 啓用複製 ] 按鈕開始複製精靈。

3. 選擇 [ 主機複本 ] 單選按鈕，再按一下 [ 下一步 ] 繼續。

4. 輸入複本 ID：選擇 1 到 65534 ( 含 1 與 65534) 之間的唯一整數。

   複本 ID 在指定尾碼的所有主機複本之中應該是唯一的。同一伺服器上不同尾碼的主機複本可以使用相同的複本 ID，前提是它在每個複本的其他主機之中是唯一的。

5. 按一下 [ 下一步 ]。如果尚未如此做，則會提示您選擇變更日誌檔。預設變更日誌檔在文字欄位中顯示。如果不想要使用預設，請輸入變更記錄的檔名，或按一下 [ 瀏覽 ] 顯示檔案選擇器。

   如果已經啓用變更記錄，精靈會略過此步驟。

6. 按一下 [ 下一步 ]。如果尚未如此做，則會提示您輸入並確認預設複製管理員的密碼。在單一主機複本的情況下不使用複製管理員，但您還是必須輸入密碼，才能繼續。在每一個欄位中輸入相同的密碼，再按一下 [ 下一步 ] 繼續。

   如果預設複製管理員已經定義密碼，精靈會略過此步驟。

7. 複製精靈於更新複製組態同時，也會顯示狀態訊息。完成時，請按一下 [ 關閉 ]。

現在複製狀態會顯示此主機的複本 ID，而且左窗格中的圖示會變更以顯示此尾碼已啓用複製。

## 進階多重主機組態

依預設值，精靈會將主機複本設爲使用預設的變更記錄設定值。若要修改變更記錄設定值，請執行以下步驟：

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，選擇 [ 資料 ] 節點，然後選擇右面板上的 [ 複製 ] 標籤。

2. 您可能需要選取 [ 啓用變更記錄 ] 核取方塊並按一下 [ 重設 ] 按鈕，重新整理此標籤的內容。接著，應該會看到您在複製精靈中選擇的變更日誌檔。

3. 您可以將變更日誌檔的名稱變更，並更新變更記錄參數：

   a. 變更記錄最大筆數 - 對於爲了傳送更新給用戶而儲存的修改而言，變更記錄最大筆數可決定該修改的總數。依據預設，這是無限制的。如果您的複本收到許多大型的修改，您或許想要限制記錄的數目以節省磁碟空間。

   b. 變更記錄最長期限 - 可決定主機儲存必須傳送給用戶更新的時間。依據預設，這是無限制的。建議使用變更記錄最長期限參數限制變更記錄大小。

複製精靈也使用預設的複製管理員。如果已經建立想要使用的不同複製管理員項目，則需要設定進階組態。您也可以使用此對話方塊，設定修改和清除延遲的參照。如果要配置單一主機，您可以略過此程序。

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，展開 [ 資料 ] 節點和您想要配置尾碼的節點，然後選擇尾碼下方的 [ 複製 ] 節點。
2. 在右面板中，按一下 [ 進階 ] 按鈕，顯示 [ 進階複本設定值 ] 對話方塊。
3. 在 [ 連結 DN] 標籤上，使用 [ 加入 ] 和 [ 刪除 ] 按鈕，建立有效複製管理員的 DN 清單。接著供應商可以於與此複本之間的協議內來使用任何一個 DN。您可利用輸入新 DN 的名稱或瀏覽目錄來加入新的 DN。

   若要透過 SSL 使用憑證來配置複製，請輸入憑證項目的 DN 作爲其中一個複製管理員。
4. 當您完成或選取更進階組態的 [ 選用 ] 標籤時，請按一下 [ 確定 ]。
5. 在 [ 進階複本設定值 ] 對話方塊的 [ 選用 ] 標籤上，LDAP URL 清單會指定傳送給此主機之修改要求的額外參照。初始化後，主機會立即自動傳送參照，如第 279 頁「多重主機初始化後的交集」所述。使用 [ 加入 ] 或 [ 刪除 ] 按鈕，建立 LDAP URL 清單。

   複製機制可自動配置集線器，以傳回複製拓樸中所有已知主機的參照。這些預設參照假設用戶端會在一般連線上使用簡單驗証。如果想要利用安全連線的 SSL 將與主機連結的選項提供給用戶端，請加入使用安全 *port* 號碼之格式 `ldaps://`*servername*`:`*port* 的參照。

   如果您已經加入一或多個 LDAP URL 作爲參照，則選擇清單下方的核取方塊時，會限制伺服器只爲這些 LDAP URL 傳送參照，而非爲主機複本。例如，如果您要用戶端永遠被參照到主機伺服器上的安全連接埠而不是預設連接埠，請建立這些安全連接埠的 LDAP URL 清單，並選取此核取方塊。
6. 此外，在 [ 選用 ] 標籤上，您也可以變更清除延遲。

   主機伺服器必須儲存有關複本內容更新的內部資訊，而清除延遲參數則指定其保留這些資訊的時間，這與供應更新之主機伺服器上的變更記錄 ( *不是*它自己的變更記錄 ) 的 MaxAge 參數有關。在兩個參數中，較短的參數可決定兩部伺服器間的複製在停用或當機後仍能回復正常的最長時間。預設值是 7 天，這已足夠大部份情況使用。
7. 按一下 [ 確定 ] 儲存此複本的進階複製組態。

## 建立複製協議

複製協議是在供應商上的一組參數，用以配置及控制更新傳送到指定用戶的方式。複製協議必須建立在傳送更新給其用戶的供應商複本上。您必須爲每一個要更新的用戶建立複製協議。

依照下列順序建立複製協議：

1. 介於多重主機集合中的主機之間，從包含要複製之尾碼原始複本的主機開始。
2. 介於主機與不透過集線器複製的專屬用戶之間。
3. 介於主機與集線器複本之間。
4. 介於集線器複本與其用戶之間。

例如，在有 2 台主機及 3 台專屬用戶的多重主機複製拓樸中 ( 如第 263 頁的「圖 8-3」所示 )，您應該依照下列順序建立 8 個複製協議：

- 介於一個主機與其他主機之間。
- 介於其他主機與第一個主機之間。
- 介於一個主機與三個專屬用戶中的每個專屬用戶之間。
- 介於其他主機與三個專屬用戶中的每個專屬用戶之間。

若要建立複製協議：

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，展開 [ 資料 ] 節點與供應商尾碼節點，然後選擇尾碼下方的 [ 複製 ] 節點。

   在右面板中顯示複製狀態資訊。

2. 按一下已定義複製協議清單旁的 [ 新增 ] 按鈕。
3. 在 [ 複製協議 ] 對話方塊中，選擇功能表中包含用戶複本的現有伺服器，或按一下 [ 其他 ] 按鈕以定義伺服器。

   當您按 [ 其他 ] 按鈕時，請輸入用戶伺服器的完全合格名稱，以及其 LDAP 連接埠號碼。如果在此連接埠上使用 SSL，請核取安全連接埠的方塊，爲複製更新啓用安全連線。

4. 在用戶伺服器上輸入複製管理員項目的 DN 與密碼。依預設值，這是預設複製管理員的 DN。

   如果您選擇具有安全連接埠的用戶，您可以按一下 [ 選項 ] 按鈕決定 DN 欄位的意義。如果您用密碼連線，供應商將使用簡單驗證，並透過加密的 SSL 連線進行通訊。如果您利用憑證進行連線，DN 欄位就是包含憑證的項目 DN，而且不需要密碼。

5. 選擇性地輸入此協議的描述字串。用戶伺服器名稱與連接埠號碼及描述字串將出現在此主機複本的複製協議清單中。
6. 完成時，按一下 [ 確定 ]。便會顯示確認對話方塊，詢問您是否要測試剛輸入的連線參數。

7. 如果要用指定的複製管理員與密碼來測試能否連線到指定的伺服器及連接埠號碼，請按一下 [ 是 ]。如果連線失敗，您還是能夠選擇使用此協議，例如，可能是參數正確，但伺服器是處於離線狀態。

   當您完成時，協議會出現在此主機複本的複製協議清單中。

稍後您可以編輯複製協議，以變更用戶伺服器上複製管理員的 DN 與密碼：

1. 從清單中選擇複製協議，再按一下 [ 編輯 ] 按鈕。
2. 在 [ 複製協議 ] 對話方塊中，請選擇 [ 連線 ] 標籤。
3. 編輯用戶伺服器的複製管理員 DN 或密碼。
4. 選擇性地編輯協議的描述字串。
5. 按一下 [ 確定 ] 儲存新設定值，並在將更新傳給此用戶時立即開始使用新設定值。

   在第 277 頁「啓用部份複製」與第 288 頁「透過 WAN 複製」中會說明其他標籤中的組態參數。

6. 在建立每個複製協議後，您可以選擇爲此尾碼配置部份複製，然後立即初始化複本，如第 278 頁「初始化複本」所述。

# 配置部份複製

依預設值，複製會將複製尾碼中的所有項目全部複製到用戶複本。若使用部份複製功能，您可以指定複製過程中所複製或排除的屬性子集。部份複製是在複製協議中配置，讓您可以爲主機的每個用戶複本定義屬性組。如此一來，您可以控制分散的資料內容，並且更有效率地使用複製頻寬及用戶資源。

例如，如果您要減少複製頻寬，可以選擇不複製通常爲大值的屬性，例如 `photo`、`jpegPhoto` 與 `audio`。因此，在用戶上無法使用這些屬性。又例如，您可以選擇只複製 `uid` 與 `userpassword` 屬性到專門用來執行驗證的用戶伺服器。

## 部份複製的考慮事項

凡是啓用或修改片斷的屬性組，都必須重新初始化用戶複本。因此，您應該在部署之前先決定部份複製的需要，並在第一次初始化複本之前定義您的屬性組。

複製小型屬性組時應小心，因爲已知某些屬性的 ACI、角色與 CoS 等複雜的功能之間存在有依存性。不僅如此，若不複製 ACI、角色或 CoS 機制的規範或搜尋條件中提及的其他屬性，可能破壞資料安全性，或造成搜尋中傳回不同的屬性組。管理要排除的屬性清單會比管理要包含的屬性清單安全，也比較不容易發生人爲錯誤。

如果複製的屬性組不允許所有複製的項目要符合該結構，您應該關閉用戶伺服器中的結構檢查。複製不符合結構的項目並不會產生錯誤，因爲複製機制會略過用戶上的結構檢查。但這樣一來，用戶將會包含不符合結構的項目，所以應該關閉結構檢查，以將連貫的狀態公開給其用戶端。

部份複製是在有集線器與專屬用戶之主機複本的複製協議中配置。多重主機複製環境中，不支援兩個主機複本之間的部份複製組態。而且，如果數個主機與同一個複本間有複製協議，則這些協議都必須複製同一個屬性組。

Directory Server 5.2 所提供的部份複製功能與舊版本的 Directory Server *不*向後相容。配置部份複製協議時，主機與用戶複本都必須在 Directory Server 實例版本 5.2 上。

## 定義屬性組

屬性組是一張屬性清單，清單上的屬性是當複本上啓用部份複製時所複製的屬性 ( 其他所有屬性均排除 )。您可以在主機伺服器上定義任何數目的屬性組，然後使其中一個屬性組與複製協議產生關聯。

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，選擇 [ 資料 ] 節點，然後選擇右面板上的 [ 複製 ] 標籤。
2. 按一下 [ 複製 ] 標籤下方的 [ 管理複製屬性組 ] 按鈕。您可能必須向下捲動才會看到此按鈕。

3. 按一下 [ 加入 ] 以定義新的屬性組，或從清單中選擇現有屬性組再按一下 [ 編輯 ] 進行修改。在顯示的 [ 屬性組 ] 對話方塊中選擇或取消選擇 [ 複製 ] 欄中的核取方塊，使對應的屬性可包含在屬性組中，或排除在組外。屬性名稱旁有核取方塊表示將會複製該屬性。

   預設狀態下會選擇所有屬性，建議您只將特別不希望複製的屬性取消選擇。如果要重新開始選擇，[ 全選 ] 按鈕會再次選擇所有屬性。當您取消選擇一些屬性後，目錄伺服器將複製*所有屬性，只排除*已取消選擇的屬性。如果稍後在結構中定義新的屬性，並用於複製項目中，這些新的屬性都將被複製，除非您編輯屬性組取消選擇該屬性。

   按一下 [ 全部不選 ] 按鈕將取消選擇所有屬性，然後您可以選擇要包含在屬性組中的屬性。當您按下 [ 全部不選 ]，然後定義正確的屬性組後，*只有選取的屬性*會被複製。如果稍後在結構中定義新的屬性，並用於複製項目中，這些新的屬性都不會被複製，除非您編輯屬性組選擇該屬性。

**備註**

`objectClass`、`nsUniqueId` 與 `nsDS50ruv` 屬性，以及 RDN 命名屬性*一定*會複製，不論您是否在屬性組中排除這些屬性。這是因爲 LDAP 修改需要 `objectClass` 與命名屬性，而複製則需要 `nsUniqueId` 與 `nsDS50ruv` 屬性才能正常運作。

排除 ACI 屬性將對用戶複本中的存取控制產生影響。排除 `userPassword` 屬性將導致沒有任何使用者能夠通過用戶複本的驗證。

4. 選擇性地輸入或修改此屬性組的描述字串。此文字將出現在定義的屬性組清單中，並在編輯即將使用此屬性組的複製協議時出現。如果未提供描述，伺服器將根據排除或包含的屬性產生描述。

5. 完成時，按一下 [ 儲存 ]。

# 啓用部份複製

只有現有的複製協議上可以啓用部份複製：

1. 依第 273 頁 「建立複製協議」所述建立複製協議，或選擇先前定義的協議進行修改。

2. 依第 293 頁 「停用複製協議」所述停用複製協議。*必須*停用協議後才能修改部份複製組態。

3. 選擇已停用的協議，再按一下 [ 編輯 ]。在出現的 [ 複製協議 ] 對話方塊中選擇 [ 複製屬性 ] 標籤。

4. 選擇 [ 只複製一組屬性 ] 核取方塊。
5. 從下拉式清單中選擇現有屬性組，或按一下 [ 新增 ] 定義新的屬性組，如第 276 頁「定義屬性組」所述。您也可以按一下 [ 管理複製屬性組 ] 以檢視及修改現有的屬性組定義。

   部份複製只允許一個屬性組與複製協議產生關聯。該屬性組應包含要複製的正確屬性清單。
6. 選擇屬性組後，按一下 [ 確定 ]。出現資訊訊息提醒您已配置部份複製，且您必須重新初始化用戶複本。按一下 [ 確定 ] 退出訊息。
7. 按一下 [ 啓用 ] 以重新啓用複製協議。
8. 您可以視複製屬性的不同，考慮停用用戶伺服器上的結構檢查。
9. 如果其他主機也與此複本之間有複製協議，您必須重複此程序，在所有其他主機上用相同的屬性組啓用部份複製。
10. 您必須立即初始化用戶複本，或重新初始化已複製的複本。請參閱下列「初始化複本」。

## 初始化複本

建立複製協議後，您必須先重新初始化用戶複本，然後複製才會真正開始。初始化期間，您會實際將資料從供應商複本複製到用戶複本。

某些錯誤狀況或組態變更會要求您必須重新初始化複本。重新初始化時，會刪除用戶上複製尾碼的內容，並以主機上尾碼的內容取代。這樣可確保複本之間保持同步，並且可以繼續複製更新。而且，此處所述的所有初始化方法都會自動重新建立用戶複本的索引，所以用戶已準備好以最佳狀態回應用戶端的讀取要求。

## 初始化時機

複本初始化必須在兩個複本都已完成配置之後，以及發生任何複製之前進行。一旦將尾碼中的資料完全複製到用戶之後，供應商便可以開始在用戶上重新執行更新作業。

在正常作業下，絕不應該重新初始化用戶。但如果因爲任何原因而從備份中復原單一主機複本，就應該重新初始化它更新的所有複本。若是多重主機複製，則已經由其他主機更新的用戶不必重新初始化。

您可以使用主控台在線上初始化複本，或使用指令行手動初始化複本。對於初始化小量用戶的作業而言，使用主控台在線上進行初始化相當方便。您可以直接從複製協議在線上初始化複本，但是因爲每個複本要依序初始化，所以此方法不適合大量複本的初始化。若要從單一 LDIF 檔案同時初始化大量用戶，用指令行手動初始化是比較有效的方法。

最後，經驗豐富的管理員可以使用二進位複製功能複製主機或客戶複本。這項功能有一些限制，因此只有對極大型資料庫檔案的複本 ( 例如包含幾百萬個項目的複本 ) 才有實用、省時的功效。

### 在多重主機複製中初始化複本

在多重主機複製的情況下，您應該依照下列順序初始化複本：

1. 確定已經有一台主機擁有要複製的完整資料。使用此主機，在每個其他主機上將複本初始化。
2. 從主機初始化其用戶複本 ( 請參閱第 282 頁「執行線上複本初始化」 )，或從任一台主機的 LDIF 檔案初始化用戶複本 ( 請參閱第 283 頁「匯出複本到 LDIF」。 )

### 在階層式複製中初始化複本

在階層式複製的情況下，請記住一定要依照下列順序初始化複本：

1. 如果您也有多重主機複製，請確定其中一個主機已經有要複製的完整資料集。使用此主機，在每個其他主機上將複本初始化。
2. 從主機複本初始化第一層集線器複本上的複本。
3. 如果有多層集線器，請從上一層初始化的集線器依序初始化每一層。
4. 從最後一層集線器複本，初始化專屬用戶上的複本。

## 多重主機初始化後的交集

在多重主機複製的情況下，當某一主機正在進行初始化時，其他主機仍可以處理變更作業。因此，當初始化完成時，新的主機也必須接收不包含在初始化資料中的新更新。由於初始化可能需時甚久，因此擱置的更新數也可能相當多。

爲了讓這些擱置更新能夠交集，新初始化的主機會自動將初始化後的用戶端作業設成唯讀模式。( 這只有透過來自指令行的 LDIF 檔案，或使用備份執行二進位複製時才爲真。) 此行爲是 Directory Server 5.2 中的新增功能。

因此在初始化後，多重主機組態中的主機將會處理複製更新，並允許讀取作業，但對於來自用戶端的寫入作業則會傳回參照。您可以如第 272 頁「進階多重主機組態」所述定義參照。在符合下列條件後，主機將會回復讀寫模式：

- 將 `ds5BeginReplicaAcceptUpdates` 組態屬性設爲 `start`，以明確允許更新作業。啓用更新之前，您應該確認新主機複製已經與其他主機交集。這可以用 Directory Serve 主控台上的複製組態面板，或透過指令行來完成 ( 請參閱下列程序 )。

  若要在初始化的主機上啓用更新，建議您採用手動操作的方式，因爲它可讓您在允許更新之前確認新主機是否與其他主機完全同步。

- 如果您先前已設定 `ds5referralDelayAfterInit` 屬性，主機複本將在指定延遲後自動切換回正常的讀寫模式。伺服器上每個主機複本的此屬性可以獨立設定。

  如果您選擇設定此屬性，您所選用的延遲應該永遠足以讓主機複本在初始化後與其他主機交集。此延遲會視預期初始化的大小與長度，以及其他主機上同時發生變更速率的不同而所有差異。主機若在初始化後仍在複製變更的同時接受更新作業，可能會產生無法解釋的錯誤。如果您碰到複製錯誤，請參閱《Directory Server Administration Reference》的 Chapter 4 "Error Log Message Reference"。

**備註** 當主機複本因爲這個新的行爲而傳送參照時，等候執行寫入作業的用戶端可能會因此而到達配置的躍點限制。您可能必須提高用戶端的躍點限制組態，讓它們可以連線到可用的主機。如果所有主機複本都已初始化或重新初始化，則所有寫入作業將因爲沒有複本接受用戶端更新而失敗。

不論何種情況，您應該緊密監控初始化的主機，並適當設定參照屬性，讓伺服器的回應達到最高限度。

## 透過主控台開始接受更新

在多重主機複本初始化後，執行這些步驟以明確允許更新作業：

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，展開 [ 資料 ] 節點與複製尾碼的節點，然後選擇尾碼下方的 [ 複製 ] 節點。

   在右面板中，主控台會顯示訊息表示複本已初始化，而且目前會爲更新作業傳回參照。如果此訊息表示已啓用自動參照延遲，您還是可以依照此程序覆寫該延遲。

2. 使用 insync 工具以確保複本已經與所有其他的主機交集。如果所有伺服器上修改之間的延遲是零，或如果複本從來沒有任何變更需要複製 ( 延遲爲 -1)，則複本之間爲同步。如需詳細資訊，請參閱 《Directory Server Administration Reference》 Chapter 1 的 "insync"。

3. 按一下訊息右邊的按鈕，立即開始接受更新作業。

### 透過指令行開始接受更新

下列指令可用於自動處理多重主機複本初始化的指令檔內，以檢查交集並明確允許更新作業：

1. 使用 insync 工具以確保複本已經與所有其他的主機交集。如果所有伺服器上修改之間的延遲是零，或如果複本從來沒有任何變更需要複製 ( 延遲爲 -1)，則複本之間爲同步。如需詳細資訊，請參閱 《Directory Server Administration Reference》 Chapter 1 的 "insync"。

2. 用下列指令修改 ds5BeginReplicaAcceptUpdates 組態屬性：

```
ldapmodify -h host -p port -D "cn=Directory Manager" -w password
dn:cn=replica, cn=suffixName, cn=mapping tree, cn=config
changetype:modify
add:ds5BeginReplicaAcceptUpdates
ds5BeginReplicaAcceptUpdates:start
^D
```

初始化複本時，會自動刪除 ds5BeginReplicaAcceptUpdates，使得初始化後會再次拒絕更新作業。

### 設定自動參照延遲

ds5ReferralDelayAfterInit 組態屬性會決定任何初始化後複本傳回參照的秒數。在此延遲後，複本將自動開始處理來自用戶端的更新作業。此屬性是每個複本特有的，而且應該根據第 279 頁「多重主機初始化後的交集」中所述的條件來設定屬性的值。

如果對應的複本最近已初始化，而且仍未接受更新，則變更此屬性值將動態影響對應的複本。您可以修改此數值以延長或縮短進行中的延遲；如果已超過延遲，而且複本正在接受更新，則設定此屬性將不會有任何影響。

此屬性的預設值是 -1，表示複本將無限期拒絕更新作業。在此情況下，您可以定義延遲，在超過延遲 ( 自初始化起算 ) 時自動允許更新。設定已超過的延遲將使複本立即開始接受更新。

1. 使用下列指令設定 ds5ReferralDelayAfterInit 屬性：

```
ldapmodify -h host -p port -D "cn=Directory Manager" -w password
dn:cn=replica, cn=suffixName, cn=mapping tree, cn=config
changetype:modify
replace:ds5ReferralDelayAfterInit
ds5ReferralDelayAfterInit:seconds
^D
```

## 使用主控台初始化複本

使用主控台在線上初始化複本是初始化或重新初始化用戶最簡單的方法。但是，如果您要初始化大量項目 ( 超過 1-2 百萬 )，此處理可能非常耗時，您或許覺得使用指令行進行手動用戶初始化更具效率 ( 如需詳細資訊，請參閱第 283 頁「從指令行初始化複本」 )。

使用主控台初始化用戶複本時，尾碼上的所有作業 ( 包括搜尋 ) 會參照到主機伺服器，直到初始化處理完成爲止。

在使用 Directory Server Console 時，使用已配置部份複製初始化複本的作業是透明的。初始化過程中，只會將選取的屬性傳送給用戶。

### 執行線上複本初始化

若要使用主控台初始化或重新初始化複本：

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，展開 [ 資料 ] 節點與主機複本的尾碼節點，然後選擇尾碼下方的 [ 複製 ] 節點。

   在右面板中顯示複製狀態資訊。

2. 在已定義的協議清單中，選擇與您要初始化的用戶對應的複製協議，再按一下 [ 動作 ]>[ 初始化遠端複本 ]。

   出現確認訊息，警告您原先已儲存在用戶上複本中的任何資訊都將遺失。

3. 在確認方塊中按一下 [ 是 ]。

   線上用戶初始化立即開始。複製協議的圖示顯示紅色齒輪，表示初始化處理的狀態。

4. 按一下 [ 重新整理 ]>[ 立即重新整理 ]，或選擇 [ 重新整理 ]>[ 繼續重新整理 ]，以追蹤用戶初始化的狀態。

   在清單下方的文字方塊中，會出現被反白顯示之協議的任何訊息。

如需關於監控複製與初始化狀態的詳細資訊，請參閱第 305 頁「監控複製狀態」。

# 從指令行初始化複本

對於複製大量項目的佈署而言，使用指令行手動初始化複本是用戶初始化的最快方法。凡是因爲效能限制而不適合採用線上程序時，均可使用手動處理。但是，手動用戶初始化處理比線上用戶初始化處理複雜許多。

若要手動初始化或重新初始化複本，先將尾碼資料的原始複本匯出到 LDIF 檔案。如果要初始化片斷複本，您應該篩選檔案，只保留複製的屬性。然後將該檔案傳輸到所有用戶伺服器，再進行匯入。在多重主機複製部署中，您可以用從原始主機匯出的 LDIF 檔案來初始化其他主機與任何用戶。在階層式複製環境中，您可以用同一個檔案初始化集線器複本與其用戶。

不論任何狀況，您都必須從配置的主機複本匯出的 LDIF 檔案開始。您無法使用任意的 LDIF 來初始化所有複本，因爲任意檔案中不包含複製資料。您必須先將您的 LDIF 檔案匯入主機複本，再用下列程序將它匯出。

## 匯出複本到 LDIF

您可以用 `db2ldif -r` 或 `db2ldif-task -r` 指令將複本內容儲存在 LDIF 檔案中。如需詳細資訊，請參閱第 145 頁「從指令行匯出至 LDIF」。您*必須*使用這些指令的 `-r` 選項來匯出複本。

下列範例會將整個 `dc=example,dc=com` 複本匯出到名爲 `example_master.ldif` 的檔案：

```
# /usr/sbin/directoryserver -s example stop
# /usr/sbin/directoryserver db2ldif -r -s "dc=example,dc=com" \
  -a /var/ds5/slapd-serverID/ldif/example_master.ldif
# /usr/sbin/directoryserver -s example start
```

然後您可以視需要篩選 LDIF 檔案，並將它傳輸到用戶主機，以初始化用戶複本。

## 篩選部份複製的 LDIF 檔案

如果您已配置部份複製，您應該先將任何不用的屬性篩選掉，再將匯出的 LDIF 檔案複製到用戶伺服器。針對這個用途，Directory Server 提供了 `fildif` 工具。此工具會篩選指定的 LDIF 檔案，只保留複製協議中定義的屬性組所允許的屬性。

此工具會讀取伺服器的組態，以決定屬性組定義。爲了讀取組態檔，`fildif` 工具必須作爲根執行，或作爲擁有程序和檔案的使用者執行 ( 由 `nsslapd-localuser` 屬性指定 )。例如，下列指令會篩選從上述範例的 `dc=example,dc=com` 尾碼中匯出的檔案：

```
# CAMUS=/var/opt/mps/serverroot/slapd-camus
# /var/opt/mps/serverroot/shared/bin/fildif \
-i $CAMUS/ldif/example_master.ldif \
-o $CAMUS/ldif/filtered.ldif -c $CAMUS/config/dse.ldif \
-b "cn=rousseau.example.com:389, cn=replica, \
cn=\"dc=example,dc=com\", cn=mapping tree, cn=config"
```

`-i` 與 `-o` 選項分別代表輸入檔與輸出檔。`-c` 選項是包含複製協議及屬性組定義的組態檔。`dse.ldif` 檔案是儲存 `cn=config` 項目內容 ( 包括複製協議與屬性組 ) 的伺服器所在位置。

`-b` 選項是定義部份複製之複製協議的 DN。在 Directory Server Console 中以目錄管理員的身份瀏覽 `cn=config` 尾碼，即可找到此項目。請選擇尾碼下方的 `cn=replica` 項目，並使用 [ 編輯 ]>[ 複製 DN] 功能表項目將此 DN 複製到剪貼簿，以便在輸入指令時使用。

如需 `fildif` 工具的完整指令行語法，請參閱 《Directory Server Administration Reference》的 Chapter 1 "fildif"。

接著您可以使用 `fildif` 所產生的 `filtered.ldif` 檔案，將此複製協議中的用戶初始化。將檔案傳輸到用戶伺服器，再依下一節的說明匯入檔案。

## 匯入 LDIF 檔案到用戶複本

您可以使用 Directory Server Console 中的匯入功能，或使用 `directoryserver ldif2db` 或 `directoryserver ldif2db-task` 指令，將含有主機複製內容的 LDIF 檔案匯入用戶複本中。就如所有匯入作業一樣，這些指令需要目錄管理員的連結 DN 與密碼才能執行匯入。在第 140 頁「從指令行匯入 LDIF」中會說明匯入的方法。

下列範例顯示如何匯入 LDIF 檔案，以初始化 `dc=example,dc=com` 用戶複本：

```
# /usr/sbin/directoryserver -s example stop
# /usr/sbin/directoryserver ldif2db -s "dc=example,dc=com" \
  -i example_master.ldif
# /usr/sbin/directoryserver -s example start
```

使用 `ldif2db-task` 不必先停止伺服器。如需詳細資訊，請參閱 《Directory Server Administration Reference》 Chapter 1 的 "ldif2db-task"。

# 使用二進位複製初始化複本

二進位複製功能會複製整個伺服器，方法是使用來自某個伺服器的二進位備份檔案來復原另一個伺服器上相同的目錄內容。此進階功能會與目錄伺服器的資料庫檔案互動，而且僅適合經驗豐富的管理員使用。

## 二進位複製的限制

因爲二進位複製功能會將資料庫檔案從一台電腦搬移到另一台電腦，所以這項機制有下列嚴格的限制：

- 兩台電腦必須使用相同的硬體及相同的作業系統，包括任何 Service Pack 或修補程式。
- 兩台電腦必須已安裝相同版本的 Directory Server，包括二進位檔案碼格式 (32 位元或 64 位元 )、Service Pack 或修補程式階層。
- 兩台電腦必須擁有分割成相同尾碼的相同樹狀目錄。*所有*尾碼的資料庫檔案*必須*一起複製，無法複製個別尾碼。
- 每個尾碼在兩部伺服器上必須配置相同的索引，包括 VLV (virtual list view，虛擬清單檢視 ) 索引。尾碼的資料庫必須擁有相同名稱。
- 即將複製的 Directory Server 不能包含 `o=NetscapeRoot` 尾碼，因爲這表示它無法作爲 Administration Server 的組態目錄。
- 每部伺服器必須將相同的尾碼設成複本，而且複本在兩部伺服器上必須具備相同的角色 ( 主機、集線器或用戶 )。如果已配置部份複製，所有伺服器上的配置必須完全一致。
- 任一部伺服器上都不能使用屬性加密。
- 若已啓用屬性值唯一性 Plug-in，此 Plug-in 在兩部伺服器上必須擁有相同的組態，而且必須在新的複本上重新配置 ( 如下列程序所述 )。

在上述條件下，您可以從一部主機伺服器的二進位複本初始化或重新初始化另一部主機伺服器，或從一部用戶伺服器的二進位複本初始化或重新初始化另一部用戶伺服器。下列兩個程序說明執行二進位複製的替代方法，一個方法不需要停止伺服器，另一個方法使用最小的磁碟空間。

## 不停止伺服器的二進位複製

執行二進位複製時，建議您使用以下程序，因爲它使用正常的備份功能來建立伺服器資料庫檔案的複本。執行正常備份可確保所有資料庫檔案都保持連貫的狀態，不需要停止伺服器。

但是此程序有某些限制，您應該列入考量。備份與復原作業會在同一台電腦上建立資料庫檔案的複本，因此每台電腦上由這些檔案佔用的磁碟空間會變成兩倍。此外，如果您的目錄包含數個 GB 的資料，這些檔案實際的複製作業可能耗費可觀的時間。如果您的磁碟空間有限，或您的資料庫檔案極大，請參閱第 286 頁「使用最小磁碟空間的二進位複製」。

1. 在新複本的目標機器上安裝 Directory Server，視需要建立伺服器的新實例，然後再根據第 285 頁「二進位複製的限制」來配置。
2. 在您涉及此複本的複製拓樸中建立所有的複製協議。這會包括從供應商到此複本的協議，如果不是專屬用戶，則爲從此複本到其用戶的協議。
3. 選擇完整配置和初始化的複本 ( 與要初始化主機、集線器或用戶所用的複本相同 )，並根據第 147 頁「使用主控台備份您的伺服器」中的程序在此尾碼上執行正常備份。
4. 將檔案從備份目錄複製或傳輸到目標電腦上的目錄，例如使用 `ftp` 指令。
5. 根據第 148 頁「從備份復原資料」中的程序將檔案載入目標伺服器。
6. 如果您已初始化多重主機複製案例中的新主機，請依照第 279 頁「多重主機初始化後的交集」中的程序進行，以確保新的複本將開始接受來自用戶端的更新作業。

## 使用最小磁碟空間的二進位複製

下列程序使用較少的磁碟空間及較短的時間，因爲它不必爲資料庫檔案製作備份。但是它會要求您停止被複製的伺服器，以確保資料庫檔案處於連貫的狀態。

---

小心　此程序*不可*用於重新初始化已參與多重主機複製案例的主機。它只可用於重新初始化用戶伺服器，或初始化新的主機伺服器。若要重新初始化現有的主機複本，請使用線上初始化、匯入 LDIF 檔案或依照第 285 頁「不停止伺服器的二進位複製」程序執行。

---

1. 在新複本的目標機器上安裝 Directory Server，視需要建立伺服器的新實例，然後再根據第 285 頁「二進位複製的限制」來配置。
2. 在您涉及此複本的複製拓樸中建立所有的複製協議。這會包括從供應商到此複本的協議，如果不是專屬用戶，則爲從此複本到其用戶的協議。
3. 停止即將初始化或重新初始化的目標伺服器，如第 23 頁「啓動和停止 Directory Server」所述。

4. 選擇一個與要初始化的複本相同類型 ( 可能爲主機、集線器或用戶 )、而且已完全配置並初始化的複本，並停止此伺服器。如果要複製多重主機組態中的主機複本，在停止主機之前您應該確定該主機已經完全更新爲來自其他主機的最新變更。
5. 移除所有來自目標伺服器的資料庫檔案，包括交易日誌檔、變更日誌檔和區域檔 (__db.xxx 檔 )。除非檔案的位置被更改，否則資料庫檔案與交易記錄應位於 *ServerRoot*/slapd-*serverID*/db 目錄。
6. 將所有資料庫檔案 ( 包括交易記錄 ) 從來源複本電腦複製或傳輸到目標電腦，例如使用 ftp 指令。除非檔案的位置被更改，否則資料庫檔案與交易記錄應位於 *ServerRoot*/slapd-*serverID*/db 目錄。

   如果要初始化主機或集線器複本，您必須複製變更記錄內所有的檔案，這些檔案預設位於 *ServerRoot*/slapd-*serverID*/changelog 目錄。
7. 重新啓動來源與目標伺服器。

## 啓用參考完整性 Plug-in

如果您要使用參考完整性 Plug-in ，您必須在所有主機伺服器上啓用此 Plug-in，但不必在集線器或用戶伺服器上啓用此 Plug-in。請參閱第 79 頁「將參考的完整性用於複製」。

# 透過 SSL 複製

您可以配置涉及複製的 Directory Server，讓所有複製作業都透過 SSL 連線上進行。若要做此設定，請完成下列步驟：

1. 將供應商與用戶伺服器都配置爲使用 SSL。

   如需詳細資訊，請參閱第 11 章「管理驗證和加密」。

**備註**

- 如果供應商伺服器憑證是在 SSL 信號交換期間無法作爲用戶端的 SSL 僅限於伺服器憑證，則透過 SSL 複製將會失敗。
- 自我簽署的憑證目前不支援透過 SSL 複製。

2. 如果用戶伺服器上的尾碼未配置複製，請依照第 267 頁「啓用用戶複本」所述啓用複製。
3. 依照第 267 頁「進階用戶組態」中的程序將用戶上憑證項目的 DN 定義爲另一個複製管理員。
4. 如果供應商伺服器上的尾碼未配置複製，請依照第 269 頁「啓用集線器複本」或第 271 頁「啓用主機複本」所述啓用複製。
5. 在供應商伺服器上，建立新的複製協議，使更新透過安全 SSL 連接埠傳送給用戶。如需詳細說明，請依照第 273 頁「建立複製協議」中的程序進行。指定用戶伺服器上的安全連接埠，並選擇使用密碼或憑證的 SSL 選項。輸入您所選之 SSL 選項 ( 複製管理員或憑證 ) 的 DN。

完成配置複製協議後，供應商會透過 SSL 將所有複製更新訊息傳送給用戶，並且使用憑證 ( 如果您選擇該選項 )。如果客戶初始化是透過主控台使用配置 SSL 的協議來執行，則客戶初始化也會使用安全連線。

# 透過 WAN 複製

Directory Server 5.2 引進了執行所有複製形式的功能，包括透過廣域網路 (WAN) 連接的電腦之間的多重主機複製 (MMR)。複製機制經過內部改良後，能讓供應商伺服器透過更高延遲及更低頻寬的網路，在合理的延遲內初始化及更新用戶。

**備註** 複製資料傳輸速率一定低於可用實體媒體允許的頻寬速率。如果複製之間的更新容量在實際上無法符合可用頻寬，使用調整將不會在更新負載過重的情況下導致複製不一致。複製延遲與更新效能須視許多因素而定，包括 ( 但不限於 )：修改率、項目大小、伺服器硬體、平均延遲及平均頻寬。如果您對工作環境中的複製有疑問，請聯絡您的 Sun 專業服務代表。

複製機制的內部參數依預設值便能在 WAN 環境中有最佳效能，但如果您因爲上述因素而有複製緩慢的問題，您或許想要試著調整視窗大小和群組大小參數。您也可以排定複製的時程，以避開網路尖峰時間，因而改進整體的網路使用情形。最後，Directory Server 支援複製資料的壓縮以最佳化頻寬使用。

## 配置網路參數

下列兩個參數會決定複製機制如何將項目集合成群組，以更有效率地透過網路傳送，這兩個參數會影響供應商與用戶交換複製更新訊息及認可的方式。

- 視窗大小 ( 預設值是 10) ñ 表示在無用戶立即認可的情況下所能傳送之更新訊息數的最大值。

  快速連續地傳送大量訊息，比傳送每個訊息後等待認可效率更高。使用適當的視窗大小，您可以減少等待複製更新或認可到達所花費的時間。

  如果您的用戶複製落後於供應商，將視窗大小增加到高於預設的值，例如 100，然後在進一步調整之前再檢查一次複製效能。當複製更新率爲高，而更新之間的時間因此而縮短時，即使以 LAN 連接的複製都能從較大的視窗大小上受益。

- 群組大小 ( 預設值是 1) ñ 表示可捆綁成單一更新訊息之資料修改數的最大值。

  如果網路連線成爲複製的瓶頸，請將群組大小增加成比預設值還高的值，例如 10，然後再次檢查複製效能。增加群組大小時，請確定：

  - 視窗大小的設定遠大於群組大小
  - 視窗大小 / 群組大小遠大於用戶上 `cn=config` 之下適用於 `nsslapd-maxThreadsPerConn` 的值 ( 通常是兩倍大 )。

  群組大小設定比 1 高時，在傳送更新到供應商之前，供應商不用等到填滿群組。如果要傳送的更新清單大於群組大小，供應商會盡量聚集，針對傳送用戶可同時處理的獨立修改群組。

對您所作的任何修改的結果進行監視，並進行相應的調整。如需指令，請參閱第 305 頁「監控複製狀態」。

這兩個網路參數在每個複製協議中均可設定，讓您可以根據每個用戶特有的網路條件自訂複製效能。

您不必中斷複製即可修改視窗及群組大小參數：

1. 選擇 Directory Server Console 主控台上的 [ 組態 ] 標籤，展開 [ 資料 ] 節點與複製尾碼的節點。
2. 請選擇尾碼下方的 [ 複製 ] 節點，並在右窗格中選擇您想要配置的複製協議，再按一下 [ 編輯 ]。
3. 選擇 [ 複製協議 ] 對話方塊的 [ 網路 ] 標籤，輸入新的視窗大小值 ( 範圍介於 1 到 1000 之間 )，與群組大小值 ( 範圍介於 1 到 100 之間 )。群組大小必須小於或等於視窗大小。
4. 按一下 [ 確定 ]，儲存新值並關閉 [ 複製協議 ] 對話方塊。

   新的參數值在下一次將複製更新傳送到對應的用戶時，會立即生效。

# 排程複製活動

如果複本之間的立即同步化不是那麼急迫，則透過 WAN 複製資料的其中一種方式便是將更新排程在網路使用較不頻繁時進行。當網路可用率較高時，更新的執行速度也會顯著加快，而且複製訊息不會更進一步地阻塞已經高度使用的網路。

您可以透過複製協議個別爲每個用戶排程於每天或每週執行更新：

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，展開 [ 資料 ] 節點與複製尾碼的節點。
2. 請選擇尾碼下方的 [ 複製 ] 節點，並在右窗格中選擇您想要配置的複製協議，再按一下 [ 編輯 ]。
3. 選擇 [ 複製協議 ] 對話方塊的 [ 排程 ] 標籤，選擇每週排程旁的單選按鈕。
4. 定義排程：
   a. 對於每週的更新，請選擇一週中要進行複製的一或多日的核取方塊。如果要進一步限制於這幾日內的複製條件，您可以選擇性地輸入時間範圍 ( 使用 24 小時制表示法 )。
   b. 對於每日的更新，請按一下 [ 全部 ] 以每天進行複製，並輸入時間範圍 ( 使用 24 小時制表示法 ) 指定執行複製的時間。

      請注意，時間範圍不能跨越午夜。

5. 按一下 [ 確定 ]，儲存新值並關閉 [ 複製協議 ] 對話方塊。

   新的排程將立即生效，導致對應用戶的下一次複製更新會延遲到排程允許的第一個時間才執行。

## 資料壓縮

如要降低複製所使用的頻寬，您可以設定複製在更新用戶時，壓縮傳送的資料。複製機制使用 Zlib 壓縮程式庫。供應商和用戶都必須使用 Solaris 或 Linux 平台才能啓用壓縮。

只有在主機伺服器的複製協議上，設定 `ds5ReplicaTransportCompressionLevel` 屬性，才能組態複製壓縮。此屬性可使用下列值中的一個：

- `0` - 不執行壓縮。這就是 `ds5ReplicaTransportCompressionLevel` 屬性未定義時的預設行爲。
- `1` - 使用 Zlib 程式庫預設的壓縮層級。
- `2` - 使用 Zlib 程式庫最佳大小的壓縮層級。
- `3` - 使用 Zlib 程式庫最佳速度的壓縮層級。

您應該依據經驗測試並選擇壓縮層級，爲您預期的複製使用率，在 WAN 環境下帶來最佳的結果。您不能在網路延遲不明顯的 LAN ( 區域網路 ) 中設定此參數，因爲壓縮和解壓縮的運算將使複製變慢。

例如，若要在 `east.example.com` 上使用最快速壓縮傳送複製更新至用戶，請使用下列 `ldapmodify` 指令：

```
ldapmodify -h host -p port -D "cn=Directory Manager" -w password
dn:cn=east.example.com:389,cn=replica,cn="suffixDN",
 cn=mapping tree,cn=config
changetype:modify
add:ds5ReplicaTransportCompressionLevel
ds5ReplicaTransportCompressionLevel: 3
^D
```

有關設定壓縮層級的詳細資訊，請參閱 《Directory Server Administration Reference》的 Chapter 2 "ds5ReplicaTransportCompressionLevel"。

# 修改複製拓樸

本節包含幾個用於管理現有複製拓樸的程序，例如編輯或移除複製協議、升級、降級或停用複本、強迫更新用戶以及管理變更記錄。

## 管理複製協議

您可以從主機尾碼的複製面板中管理複製協議，以變更協議中的驗證資訊、中斷傳給特定用戶的複製或將用戶從拓樸中移除。

### 變更複製管理員

您可以編輯複製協議，以變更用來連結用戶伺服器的複製管理員身份。爲避免中斷複製，您應該先在用戶上定義新的複製管理員項目或憑證項目，然後再修改複製協議。但如果複製因連結失敗而中斷，當您改正錯誤後，複製機制將會在複製復原設定值的限制內，自動傳送所有必要的更新 ( 請參閱第 267 頁「進階用戶組態」 )。

若要變更用戶用以通過驗證的複製管理員：

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，展開 [ 資料 ] 節點和複製尾碼節點，並選擇尾碼下方的 [ 複製 ] 節點。
2. 在右面板中，選擇要修改的複製協議，再按一下 [ 編輯 ]。
3. 在 [ 複製協議 ] 對話方塊中，請選擇 [ 連線 ] 標籤。

   狀態行會指示用戶伺服器的主機名稱與連接埠號碼。
4. 修改 DN 與密碼欄位，以包含另一個複製管理員項目的 DN 或密碼，或用戶伺服器上憑證項目的 DN。
5. 如果此複製協議使用透過安全連接埠的 SSL，您也可以按一下 [ 選項 ] 按鈕選擇安全驗證的類型。如果您用密碼進行連線，供應商將透過加密的 SSL 連線所指定的 DN 來使用簡單驗證。如果您用憑證進行連線，DN 欄位就是憑證項目的 DN，不需要密碼。

   您無法將現有的複製協議從非安全驗證切換成安全驗證，反之亦然。若要用不同的安全性設定啓用複製，您必須建立另一個複製協議。
6. 按一下 [ 確定 ] 儲存您的變更。

### 複製複製協議

複製複製協議是一種很簡單的方法，能夠爲大型複製拓樸中的供應商複本設定許多用戶：

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，展開 [ 資料 ] 節點和複製尾碼節點，並選擇尾碼下方的 [ 複製 ] 節點。
2. 從複製協議清單中，選擇要複製的協議。如果要用新的協議與用戶建立安全連線，您必須選擇也使用安全連接埠的現有協議。如果要建立新的非安全協議，您必須選擇非安全協議。

   按一下 [ 編輯 ] 並瀏覽 [ 複製協議 ] 對話方塊的各個標籤，以確認此協議的組態。這些標籤上的組態將於下列各節說明：

   - 在第 292 頁「變更複製管理員」中說明 [ 連線 ] 標籤。
   - 在第 288 頁「透過 WAN 複製」中說明 [ 排程 ] 與 [ 網路 ] 標籤。
   - 在第 275 頁「配置部份複製」中說明 [ 複製屬性 ] 標籤。
3. 在仍選擇同一個複製協議的情況下，按一下 [ 複製 ] 按鈕。
4. 從清單中選擇新用戶的主機名稱與連接埠號碼，或按一下 [ 加入主機 ] 按鈕以使用不同的主機與連接埠。清單和 [ 加入主機 ] 對話方塊將只允許您選擇與複製的用戶協議相同安全性類型的用戶。
5. 確定已選擇清單中的主機名稱，再按一下 [ 確定 ]，爲該用戶伺服器建立新的複製協議。
6. 新的協議會複製現有伺服器的所有組態資訊。這表示這兩部伺服器必須擁有完全相同的複製管理員項目，使用相同的密碼。如果要修改新協議的組態 ( 例如，變更複製管理員 DN)，請從清單中選擇該協議，再按一下 [ 編輯 ]。

## 停用複製協議

停用複製協議後，主機會停止傳送更新到指定的用戶。雖然到該伺服器的複製會停止，但仍會保留協議中所有的設定值。日後只要重新啓用該協議，即可繼續複製。如需有關中斷後繼續複製機制的資訊，請參閱下面的「啓用複製協議」。

若要停用複製協議：

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，展開 [ 資料 ] 節點和複製尾碼節點，並選擇尾碼下方的 [ 複製 ] 節點。
2. 在右面板中，選擇要停用的複製協議。
3. 在協議清單下方的方塊中選擇 [ 動作 ]>[ 停用協議 ]。
4. 按一下 [ 是 ] 以確認要停用該複製協議。

清單中協議的圖示便會改變，以顯示其已停用。

### 啓用複製協議

啓用複製協議將恢復與指定用戶的複製。但如果複製的中斷時間已超過複製復原設定值所允許的時間，而且其他供應商未更新該用戶，則您必須重新初始化該用戶。複製復原設定值是此供應商變更記錄與用戶的清除延遲這兩項設定的大小及天數之最大值 ( 請參閱第 267 頁「進階用戶組態」 )。

當中斷時間相當短，而且可以復原複製時，只要重新啓用協議，主機便會自動更新用戶。

若要啓用複製協議：

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，展開 [ 資料 ] 節點和複製尾碼節點，並選擇尾碼下方的 [ 複製 ] 節點。
2. 在右面板中，選擇要啓用的複製協議。
3. 在協議清單下方的方塊中按一下 [ 啓用 ] 按鈕。
4. 視需要重新初始化用戶複本。

### 刪除複製協議

刪除複製協議將停止對應用戶的複製，而且會移除有關該協議的所有組態資訊。日後若想恢復複製，請改爲停用協議，如第 293 頁「停用複製協議」所述。

若要刪除複製協議：

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，展開 [ 資料 ] 節點和複製尾碼節點，並選擇尾碼下方的 [ 複製 ] 節點。
2. 在右面板中，選擇要刪除的複製協議。
3. 按一下協議清單右邊的 [ 刪除 ] 按鈕。
4. 按一下 [ 是 ] 以確認要刪除該複製協議。

## 升級或降級複本

升級或降級複本會改變複本在複製拓樸中的角色。專屬用戶可以升級成集線器，集線器可以升級成主機；主機可以降級成集線器，而集線器也可以降級成專屬用戶。但是主機不可以直接降級成用戶，同樣地，用戶也不可以直接升級成主機。

多重主機複製機制中的升級與降級功能讓拓樸非常具有彈性。原先由用戶複本服務的網站可能會因爲成長，而需要具有幾個複本的集線器才能夠處理其負載。如果負載包含許多複本內容的修改，集線器便可以變成主機，以加快本機變更的速度，之後再將變更複製到其他網站上的其他主機。

若要升級或降級複本：

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，展開 [ 資料 ] 節點和複製尾碼節點，並選擇尾碼下方的 [ 複製 ] 節點。
2. 在右面板中，選擇 [ 變更 ]>[ 升級 - 降級複本 ] 功能表項目。
3. 複製精靈將只讓您選擇允許的新角色，然後逐步指導您進行新複本角色的組態設定程序。您應該要知道下列的結果：
   - 將主機降級成集線器時，複本將變成唯讀，並設爲會傳送參照給其餘主機。新的集線器將保留其所有用戶，不論是集線器或專屬用戶。
   - 將單一主機降級成集線器將會建立沒有主機複本的拓樸。精靈是假設您即將定義新的主機，才允許您執行此降級動作。但是您最好是先加入新的主機成爲多重主機，並讓它初始化後，再降級其他主機。
   - 將集線器降級成用戶時，將會刪除所有複製協議。如果集線器的用戶未由其他集線器或主機更新，該用戶將不再獲得更新。您應該在其他集線器或主機上建立新的協議，以更新這些用戶。
   - 將用戶升級成集線器時，便會啓用其變更記錄，而且您可以定義它與用戶的新協議。
   - 將集線器升級成主機時，複本將會接受修改要求，而且您可以定義它與其他主機、集線器或專用主機的新協議。

## 停用複本

停用複本會將它從複製拓樸中移除。它將不再獲得更新或傳送更新 ( 依其角色是主機、集線器或用戶而定 )。停用供應商將刪除所有複製協議，而且如果重新啓用複本的話，所有複製協議都必須重新建立。

若要停用複本：

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，展開 [ 資料 ] 節點和複製尾碼節點，並選擇尾碼下方的 [ 複製 ] 節點。
2. 在右面板中，選擇 [ 變更 ]>[ 停用複製 ] 功能表項目。
3. 在確認對話方塊中按一下 [ 是 ]。
4. 或者，重設此尾碼的寫入權限及參照。停用複本後，這些設定值仍然會依原狀保留，例如停用的用戶仍然會傳送修改要求給它原先的主機複本。

   若要修改寫入權限與參照，請在 [ 組態 ] 標籤上選擇此尾碼的節點，並在右面板的 [ 設定值 ] 標籤中進行修改。如需詳細資訊，請參閱第 126 頁「設定存取權限及參照」。

## 移動變更記錄

變更記錄是指定供應商複本上所有修改的內部記錄，伺服器利用它在其他複本上重新執行修改。變更記錄的內容是由伺服器自動管理，而且將透過多重主機更新進行更新 ( 即使是在伺服器重新啓動之後 )。

在舊版 Directory Server 中，變更記錄可透過 LDAP 存取，但現在則僅供伺服器內部使用。如果您有必須讀取變更記錄的應用程式，請使用 [Retro Changelog Plugin]，以達到回溯相容性。如需詳細資訊，請參閱第 302 頁「使用追溯變更記錄 Plug-in」。

只有當系統管理員必須將檔案移到其他位置時 ( 例如當檔案所在的磁碟已滿時 )，才應該修改變更記錄。

| 小心 | 當您停用變更記錄，或將變更記錄移到新位置時，變更記錄會重新初始化。不論任一種狀況，您都必須重新初始化此伺服器上複本的所有用戶。 |
|---|---|

您必須用 Directory Server Console 移動變更記錄，絕不能使用作業系統的 `rename` 或 `mv` 指令：

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，選擇 [ 資料 ] 節點，再選擇右面板中的 [ 複製 ] 標籤。
2. 在文字欄位中輸入新的位置。這是從現在起要儲存變更記錄的新路徑與目錄名稱。例如，將變更記錄從預設位置 *ServerRoot*`/slapd-`*serverID*`/changelogdb` 移到 *ServerRoot*`/slapd-`*serverID*`/newchangelog`。

   現有的變更記錄會從舊的位置刪除，新的變更記錄則保持在新的位置。
3. 在 [ 複製 ] 標籤中按一下 [ 儲存 ]。
4. 重新啓動 Directory Server。
5. 依第 278 頁「初始化複本」所述，重新初始化您的用戶。

## 保持複本同步

爲了進行定期維護，在停止 Directory Server 進行複製作業後，如果它重新上線時，必須確定它會立即透過複製獲得更新。對於多重主機環境中的主機，目錄資訊必須由多重主機集合中的另一部主機進行更新。若是其他狀況，在將集線器複本或專屬用戶設爲離線狀態以進行維護後，當它們重新上線時，必須由主機複本進行更新。

本節說明複製重試演算法，以及如何不等候下一次重試便強迫發生複製更新。

**備註** 只有已設定複製，*並且*已初始化用戶時，才可使用本節所描述的程序。

## 複製重試演算法

當供應商嘗試複製到用戶失敗時，它會以遞增的時間間隔定期重試。重試模式如下：20、40、80、160，然後 300 秒。之後，供應商會每隔 300 秒 (5 分鐘 ) 重試一次。

請注意，即使您已將複製協議設成供應商複本與用戶複本永遠保持同步，也不足以將已離線超過 5 分鐘的複本立即回復到最新狀態。

爲確保當伺服器恢復上線時目錄資訊會立即同步，您可以利用 Directory Server Console 或自訂的指令檔。

## 從主控台強迫複製更新

爲確保當用戶 ( 或多重主機複製組態中的主機 ) 在經過一段時間之後回復上線時，會立即傳送複製更新，您可以在儲存最新版目錄資料的供應商上執行這些步驟：

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，展開 [ 資料 ] 節點與主機複本的尾碼節點，並選擇尾碼下方的 [ 複製 ] 節點。

   在右面板中顯示複製狀態資訊。

2. 從要更新的用戶對應清單中選擇複製協議，再按一下 [ 動作 ]>[ 立即傳送更新 ]。

   這樣會對儲存須更新之資訊的複本啓動複製。

## 用指令行強迫複製更新

從需要更新的用戶上，下列指令檔提示其供應商立即傳送複製更新。您可以複製此範例，並爲它指定有意義的名稱，例如 `replicate_now.sh`。您必須爲此範例中所列的變數提供實際的值。

**備註** 系統管理員必須執行此指令檔，因爲只要離線的伺服器重新上線，便無法將它設定爲自動執行。

```
#!/bin/sh
SUP_HOST=supplier_hostname
SUP_PORT=supplier_portnumber
SUP_MGRDN=supplier_directoryManagerDN
SUP_MGRPW=supplier_directoryManagerPassword
MY_HOST=consumer_hostname
MY_PORT=consumer_portnumber

ldapsearch -1 -h ${SUP_HOST} -p ${SUP_PORT} -D "${SUP_MGRDN}" \
           -w ${SUP_MGRPW} -b "cn=mapping tree, cn=config" \
           "(&(objectclass=nsds5replicationagreement) \
              (nsDS5ReplicaHost=${MY_HOST}) \
              (nsDS5ReplicaPort=${MY_PORT}))" \
           dn nsds5ReplicaUpdateSchedule > /tmp/$$

cat /tmp/$$ |
awk '
BEGIN { s = 0 }
/^dn:/ { print $0;
  print "changetype:modify";
  print "replace:nsds5ReplicaUpdateSchedule";
  print "nsds5ReplicaUpdateSchedule: 0000-2359 0123456";
  print "-";
  print "";
  print $0;
  print "changetype:modify";
  print "replace:nsds5ReplicaUpdateSchedule";
  }
/^nsds5ReplicaUpdateSchedule:/ { s = 1; print $0; }
/^$/ {
  if ( $s == 1 )
    { print "-" ; print ""; }
  else
    { print "nsds5ReplicaUpdateSchedule: 0000-2359 0123456";
      print "-" ; print ""; };
  s = 0; }
' > /tmp/ldif.$$

echo "Ldif is in /tmp/ldif.$$"
echo

ldapmodify -c -h ${SUP_HOST} -p ${SUP_PORT} -D "${SUP_MGRDN}" \
           -w ${SUP_MGRPW} -f /tmp/ldif.$$
```

如果希望更新作業透過 SSL 連線進行，您必須用適當的參數與值修改指令檔中的 `ldapmodify` 指令。如需詳細資訊，請參閱第 360 頁「將 LDAP 用戶端配置爲使用安全性」。

## 與舊版進行複製

本節提供關於如何設定與舊版 Directory Server 進行複製的資訊。

就任何複製組態而言，Directory Server 5.1 與 5.2 完全相容，但下列情況例外：

- 無法使用部份複製，因此在 Directory Server 5.2 主機與 5.1 用戶複本之間不能設定部份複製。
- 在 5.2 供應商和 5.1 用戶間設定協議前，您必須在 `cn=config` 中設定 `nsslapd-schema-repl-useronly` 爲 `on`。否則，5.2 中的結構在複製至 5.1 版時，會建立衝突。加上這個設定，只有使用者定義的結構元素 ( 儲存在 `99user.ldif` 檔案中 ) 會被複製。請參閱第 323 頁「複製結構定義」。
- 在 Directory Server 5.2 中，結構檔案 11rfc2307.ldif 已改變，且遵循 RFC 2307 規則。您必須在 5.1 版的伺服器上更新相應的檔案，如第 301 頁「更新 Directory Server 5.1 Schema」所述。
- 在 5.1 用戶的參照清單中仍會顯示已降級成集線器的 5.2 主機。但由於降級的內部機制所致，已降級複本的連接埠號碼將是零。此參照 URL 將無法使用，而且當用戶端無法依照此參照時，大部分用戶端將會自動嘗試其他主機的參照。但是，您可能必須在存取這些 5.1 複本的用戶端上提高參照的躍點限制。5.2 用戶複本既不顯示也不將無法使用的參照 URL 傳回到效能降低的主機。

Directory Server 在下列條件下，5.2 可涉及含 4.x 版 Directory Server 的複製案例：

- Directory Server 5.2 設定爲主機，但只作爲 Directory Server 4.x 供應商的複製用戶。
- 用戶複本不能同時爲舊的 4.x 供應商與 5.2 供應商的用戶。但 5.2 伺服器可以有不同的複本，其中一個由舊的 Directory Server 提供，另一個由 5.2 Directory Server 提供。
- Directory Server 5.2 複本若已設定爲舊的 4.x 供應商的用戶，便不能作爲拓樸中此尾碼的集線器複本。

能夠使用 Directory Server 5.2 作爲舊 Directory Server 用戶的主要優點是，能方便遷移複製環境。如需關於遷移複製環境之步驟的詳細資訊，請參閱「Directory Server Installation and Migration Guide」中的 Chapter 4 "Replicated Server Upgrade"。

# 將 Directory Server 5.2 設定爲 Directory Server 4.x 的用戶

如果您計劃使用 Directory Server 5.2 作爲 4.x 版 Directory Server 的用戶，您必須依下列方式設定：

1. 依第 271 頁「啓用主機複本」所述，將複本啓用爲*主機*複本。即使複本是 4.x 供應商的用戶，都必須設定爲主機複本。
2. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，展開 [ 資料 ] 節點和複製尾碼節點，並選擇尾碼下方的 [ 複製 ] 節點。
3. 在右面板中，爲此複本選擇 [ 變更 ]>[ 啓用 4.x 相容性 ]；或者，選擇 [ 物件 ] 功能表中的 [ 啓用 4.x 相容性 ]。
4. 在 [ 啓用 4.x 相容性 ] 視窗中，指定舊供應商伺服器用於連結的連結 DN 與密碼。您在這裏指定的連結 DN 和密碼*只能*用於原來的複製。因此不能使用現有的 DN，或 5.x 複製中使用的預設複製管理員。

   如果使用「複製精靈」設定原來的複製，您指定的連結 DN 和密碼會正確地儲存在原來的複製組態項目中。如果從指令行手動設定原來的複製，必須使用 `nsslapd-legacy-updatedn` 和 `nsslapd-legacy-updatepw` 屬性，指定原來的複製組態項目中的連結 DN 和密碼。

   原來的複製只能與簡單驗證，而不能與使用憑證的安全驗證一起使用。
5. 按一下「確定」。現在此用戶複本即已準備好接收來自舊供應商的更新。
6. 請確定 5.2 複本伺服器上的結構定義了將從 4.x 版主機複製的內容中的所有屬性和物件類別。
7. 匯入 4.x 版主機上建立的 LDIF 複本檔案，以初始化 5.2 複本。在此檔案中的第一個項目包含有 4.x 複製機制所需的 `copiedfrom` 屬性。

在伺服器上啓用 4.x 相容性會設定預設安裝的舊複製 Plug-in。此 Plug-in 會處理來自舊供應商的更新，並對複製尾碼的內容執行更新。

**備註** 只要 4.x 相容性爲啓用狀態，此複本會爲來自用戶端的任何修改要求傳回參照。即使 Directory Server 5.2 設定爲主機複本，它都不會在此尾碼上執行修改要求，而是會傳回 4.x 供應商伺服器的參照。

爲完成舊複製設定，您必須立即將舊供應商設爲複製到 5.2 Directory Server。如需關於在 4.x Directory Server 上設定複製協議的說明，請參閱舊的 Directory Server 所提供的說明文件。

# 更新 Directory Server 5.1 Schema

在 Directory Server 5.2 中，結構檔案 `11rfc2307.ldif` 已改變，且遵循 RFC 2307 規則 (`http://www.ietf.org/rfc/rfc2307.txt`)。在設定或啓用 5.2 版和 5.1 版伺服器間的複製前，您必須更新 5.1 伺服器上的結構。在這兩個版本的伺服器上，結構檔案位於 *ServerRoot*`/slapd-`*serverID*`/config/schema/`。

1. 從 5.2 伺服器上複製檔案 `11rfc2307.ldif` 至 5.1 版伺服器。
   - 如果您有 5.1 版伺服器的 Solaris 套件軟體安裝程式，您必須刪除過時的 `10rfc2307.ldif` 檔案。
   - 如果你有 5.1 版伺服器其他平台的壓縮檔安裝程式，您將覆寫現有的 `11rfc2307.ldif` 檔案。
2. 下列結構檔案在此次變更中受到影響，必須從 5.2 版伺服器上複製，覆寫至 5.1 版伺服器上現有的檔案：
   - `20subscriber.ldif`
   - `30ns-common.ldif`
   - `50ns-admin.ldif`
   - `50ns-certificate.ldif`
   - `50ns-directory.ldif`
   - `50ns-legacy.ldif`
   - `50ns-mail.ldif`
   - `50ns-mlm.ldif`
   - `50ns-msg.ldif`
   - `50ns-netshare.ldif`
3. 重新啓動 5.1 版伺服器，然後繼續進行複製組態和複本初始化。由於同步化其他結構元素，有些結構屬性可能在伺服器間複製，這是複製機制的正常行爲。
4. 您可能必須更新依賴舊版本結構的任何應用程式。新的 `11rfc2307.ldif` 檔案做了下列修改：
   - `automount` 和 `automountInformation` 屬性已被移除。
   - `ipHost` 物件類別允許屬性的清單不再包含有 `o $ ou $ owner $ seeAlso $ serialNumber`。
   - `ieee802Device` 物件類別強制屬性的清單不再包含有 `cn`。

- ieee802Device 物件類別允許屬性的清單不再包含有 description $ l $ o $ ou $ owner $ seeAlso $ serialNumber。
- bootableDevice 物件類別強制屬性的清單不再包含有 cn。
- bootableDevice 物件類別允許屬性的清單不再包含有 description $ l $ o $ ou $ owner $ seeAlso $ serialNumber。
- nisMap 物件類別的 OID 現在是 1.3.6.1.1.1.2.9。

# 使用 追溯變更記錄 Plug-in

當您要用 Directory Server 5.2 主機複本維護 4.x 樣式的變更記錄時，便可以使用 追溯變更記錄 Plug-in。對於依附於 Directory Server 4.x 變更記錄格式的 Meta Directory 等應用程式而言，有時候這是必要的，因爲它們會從變更記錄讀取資訊。

追溯變更記錄 Plug-in *不*允許 Directory Server 5.2 成爲舊 4.x 用戶複本的供應商；只支援 Directory Server 5.2 作爲 4.x 供應商的用戶，如第 299 頁「與舊版進行複製」所述。追溯變更記錄 Plug-in 的運作與複製通訊協定無關，而且對複製拓樸也沒有影響。在單一主機部署案例的任何伺服器上，都可以啓用追溯變更記錄 Plug-in。一般而言，如果佈署中任何應用程式的需求包括追溯變更記錄，則不應該在此佈署中使用多重主機複製拓蹼。

除了伺服器的 5.2 變更記錄外，還保存追溯變更記錄。追溯變更記錄儲存在 cn=changelog 這個特殊尾碼下另一個資料庫中。追溯變更記錄由單一階層的項目組成。變更記錄中的每個項目都有物件類別 changeLogEntry，而且可以包含下表所列的各項屬性。

**表 8-1** 追溯變更記錄項目的屬性

| 屬性 | 定義 |
|---|---|
| changeNumber | 這個單值屬性永遠存在。它包含可唯一識別每一次變更的整數。此數字與變更發生的順序有關，數字越高，變更時間越近。 |
| targetDN | 此屬性包含受 LDAP 作業影響之項目的 DN。若是 modrdn 作業，targetDN 屬性包含項目修改或移動前的 DN。 |
| changeTime | 此屬性指定變更作業發生的時間。 |
| changeType | 指定 LDAP 作業的類型。此屬性可爲下列值中的一個：add、delete、modify 或 modrdn。 |
| changes | 對於加入及修改作業，此屬性包含對項目所做的變更 ( 格式爲 LDIF)。 |

**表 8-1** 追溯變更記錄項目的屬性 *( 續 )*

| 屬性 | 定義 |
|---|---|
| newRDN | 若是 modrdn 作業，此屬性指定項目新的 RDN。 |
| deleteOldRdn | 若是 modrdn 作業，此屬性指定是否刪除舊的 RDN。 |
| newSuperior | 若是 modrdn 作業，此屬性指定項目的 newSuperior 屬性。 |

# 啓用追溯變更記錄 Plug-in

追溯變更記錄 Plug-in 的組態資訊儲存在 dse.ldif 的 cn=Retro Changelog Plugin,cn=plugins,cn=config 項目中。

若要從 Directory Server Console 啓用追溯變更記錄 Plug-in ：

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，展開 [Plug-in] 節點，並向下捲動以選擇 [Retro Changelog Plugin]。
2. 在右面板中核取 [ 啓用 Plug-in] 核取方塊，再按一下 [ 儲存 ]。若要停用 Plug-in，請清除此核取方塊。
3. 啓用或停用 Plug-in 後，您必須重新啓動 Directory Server。

若要從指令行啓用追溯變更記錄 Plug-in：

1. 使用下列指令修改追溯變更記錄 Plug-in 組態項目：

```
ldapmodify -h host -p port -D "cn=Directory Manager" -w password
dn:cn=Retro Changelog Plugin,cn=plugins,cn=config
changetype:modify
replace:nsslapd-pluginenabled
nsslapd-pluginenabled:on
^D
```

2. 重新啓動伺服器。如需關於重新啓動伺服器的資訊，請參閱第 23 頁「啓動和停止 Directory Server」。

# 調整追溯變更記錄

變更記錄中的項目可在指定的時間後自動移除。若要設定在一段時間後自動將項目從變更記錄中刪除，您必須在 cn=Retro Changelog Plugin°B cn=plugins°B cn=config 項目中設定 nsslapd-changelogmaxage 組態屬性。此屬性只能從指令行設定，例如：

```
ldapmodify -h host -p port -D "cn=Directory Manager" -p password
dn:cn=Retro Changelog Plugin,cn=plugins,cn=config
changetype:modify
replace:nsslapd-changelogmaxage
nsslapd-changelogmaxage:IntegerTimeunit
^D
```

其中 *Integer* 代表一個數字，而 *Timeunit* 可爲下列其中一個值：`s` 代表秒、`m` 代表分鐘、`h` 代表小時、`d` 代表日或 `w` 代表星期。*Integer* 與 *Timeunit* 變數之間沒有空格，例如：

```
nsslapd-changelogmaxage:2d
```

在變更記錄的下一步作業中，會調整追溯變更記錄。

## 存取 追溯變更 記錄

變更記錄支援搜尋作業。它已針對包含下列格式之篩選器的搜尋最佳化：

```
(&(changeNumber>=X)(changeNumber<=Y))
```

一般而言，您不應該對追溯變更記錄執行加入或修改作業，但您可以刪除項目以調整變更記錄的大小；唯一需要對追溯變更記錄執行修改作業的機會是修改預設存取控制策略。

建立追溯變更記錄時，會預設套用下列存取控制策略：

- 讀取、搜尋與比較權限會授與追溯變更記錄最上層項目 `cn=changelog` 的所有驗證使用者 (`userdn=anyone`，在 `userdn=all` 處使用匿名存取不會遭到拒絕 )。
- 除了隱含地授與目錄管理員權限外，不授與寫入與刪除存取。

您不應該將讀取存取授與匿名使用者，因爲變更記錄項目內可能包含對敏感資料 ( 例如密碼 ) 的修改。如果連驗證使用者都不被允許檢視記錄內容，您可能希望進一步限制存取追溯變更記錄的內容。

若要修改套用在追溯變更記錄的預設存取控制策略，您應該修改 `cn=changelog` 項目的 `aci` 屬性。如需關於設定 `aci` 屬性的詳細資訊，請參閱第 6 章「管理存取控制」。

# 監控複製狀態

您可以使用新的指令行工具及 Directory Server 主控台監視複製狀態。

## 指令行工具

有三個新的指令行工具可用於監控您的複製部署：

- `repldisc` - 「尋找」及建構複製部署中所有已知伺服器的表格。
- `insync` - 指出供應商與一或多個用戶複本之間的同步狀態。
- `entrycmp` - 比較兩個或多個複本內相同的項目。

這些工具位在下列目錄內：

*ServerRoot*`/shared/bin`

如需這些工具的完整指令行語法和用法範例，請參閱 《Directory Server Administration Reference》 Chapter 1 的 "Tools Reference"。

## 複製狀態標籤

若要在 Directory Server Console 中檢視複製狀態摘要：

1. 在 Directory Server Console 上層的 [ 狀態 ] 標籤上，選擇 [ 複製 ] 節點。

   右面板會顯示表格，表格中包含爲此伺服器設定之每個複製協議的相關資訊。

2. 如果要監控複製狀態，請選擇 [ 繼續重新整理 ] 核取方塊。例如，您會看到複本何時完成初始化。

3. 如果您要判斷主機上尚未複製到用戶的最後一次修改，請按一下 [ 擱置變更數 ] 按鈕。系統會警告您此作業可能會耗費相當長的時間，並請您確認。判斷擱置變更數需要下載更新的用戶記錄，並將它與主機的變更記錄比較。如果記錄非常多，此作業可能會耗費很多時間與伺服器資源。

4. 您可以按一下欄標頭並調整其大小，來修改表格佈局。您也可以按一下 [ 檢視選項 ] 按鈕，並且只選擇要查看的項目，來修改表格內容。下列的 表 8-2 說明您可選擇表格中要爲此伺服器上的每個協議顯示的複製參數。

**表 8-2** Directory Server Console [ 狀態 ] 標籤上的複製參數

| 表格標頭 | 描述 |
|---|---|
| 尾碼 | 舉出正在複製的尾碼與子尾碼。 |
| 遠端複本 | 包含用戶伺服器的主機名稱與連接埠。 |
| 描述 | 包含在此複製協議中提供的描述字串。 |
| 狀態 | 表示協議是否已停用、正初始化用戶，或透過增量更新進行正常複製。 |
| 摘要 | 包含最近事件 ( 初始化或更新的開始或結束 ) 以及所接收的最新訊息。 |
| 傳送更新 | 自啓用複製或重新啓動伺服器起，傳送到用戶的個別更新累積總數。 |
| 最後更新開始 | 表示最近一次複製更新的開始時間。 |
| 最後更新結束 | 指示最近一次複製更新的結束時間。 |
| 最後更新訊息 | 提供最近一次複製更新的狀態。 |
| 最後初始化訊息 | 提供用戶最後一次的初始化狀態。 |
| 最後初始化開始 | 指示用戶複本最近一次初始化的開始時間。 |
| 最後初始化結束 | 指出用戶複本最近一次初始化的結束時間。 |

# 解決一般複製衝突

多重主機複製使用不嚴格的一致性複製模式。這表示可以同時在不同伺服器上修改相同的項目。因此在兩部伺服器之間傳送更新時，便需要解決衝突的變更。解決衝突多半會自動執行，並以每部伺服器上變更相關的時間戳記爲準。以最近的變更優先。

然而，有些情況必須透過手動操作，才能解決衝突的變更。若項目由無法由複製處理自動解決的變更衝突，則該項目會包含 `nsds5ReplConflict` 作業屬性作爲衝突標示。

請定期搜尋包含此屬性的項目，以找出發生衝突的項目。例如，您可以使用下列 `ldapsearch` 指令：

```
% ldapsearch -h host -p port -D "cn=Directory Manager" -w   password \
-b "dc=example,dc=com" "(nsds5ReplConflict=*)"
```

請注意，預設狀況下 `nsds5ReplConflict` 屬性會編製索引。

# 解決命名衝突

如果在伺服器互相複製變更之前建立有相同 DN 的項目，則可能在不同的主機上建立該項目。複製時，衝突解決機制將自動重新命名所建立的第二個項目。

在項目的 DN 中，加入操作屬性 nsuniqueid 指定的唯一識別符，重新命名有 DN 命名衝突的項目。例如，如果同時在兩個主機上建立項目 uid=bjensen,ou=People,dc=example,dc=com，複製後兩個主機上會有下列兩個項目：

- uid=bjensen,ou=People,dc=example,dc=com
- nsuniqueid=66446001-1dd211b2+uid=bjensen,dc=example,dc=com

第二個項目必須重新命名，使它擁有有用的 DN。您可以刪除衝突的項目，然後再以不相衝突的名稱加入。然而，保持項目最安全的作法是在建立時就重新命名它。重新命名程序須視命名屬性是單值或多重值屬性而定。每個程序分別說明如下。

## 重新命名多重值命名屬性的項目

若要重新命名具有多重值命名屬性的衝突項目：

1. 保留舊的 RDN 值時，重新命名項目。例如：

   ```
   ldapmodify -h host -p port -D "cn=Directory Manager" -w password
   dn:nsuniqueid=66446001-1dd211b2+uid=bjensen,dc=example,dc=com
   changetype:modrdn
   newrdn:uid=NewValue
   deleteoldrdn: 0
   ^D
   ```

   您無法在此步驟中刪除舊的 RDN 值，因爲它同時含有無法刪除的 nsuniqueid 操作屬性。

2. 移除命名屬性的舊 RDN 值和衝突標示屬性。例如：

   ```
   ldapmodify -h host -p port -D "cn=Directory Manager" -w password
   dn:uid=NewValue,dc=example,dc=com
   changetype:modify
   delete:uid
   uid:bjensen
   -
   delete:nsds5ReplConflict
   ^D
   ```

### 重新命名單值命名屬性的項目

命名屬性爲單值時，例如 dc ( 網域元件 )，您不能只是重新命名項目爲相同屬性的其他值。而是必須爲它指定一個暫時名稱。

1. 用不同的命名屬性爲項目重新命名，並保留舊的 RDN。例如：

   ```
   ldapmodify -h host -p port -D "cn=Directory Manager" -w password
   dn:nsuniqueid=66446001-1dd211b2+dc=HR,dc=example,dc=com
   changetype:modrdn
   newrdn:o=TempName
   deleteoldrdn: 0
   ^D
   ```

   您無法在此步驟中刪除舊的 RDN 值，因爲它同時含有無法刪除的 nsuniqueid 操作屬性。

2. 將所需的命名屬性變更爲唯一值，然後移除衝突標示屬性。例如：

   ```
   ldapmodify -h host -p port -D "cn=Directory Manager" -w password
   dn:o=TempName,dc=example,dc=com
   changetype:modify
   replace:dc
   dc:uniqueValue
   -
   delete:nsds5ReplConflict
   ^D
   ```

3. 將項目重新命名爲預期的命名屬性。例如：

   ```
   ldapmodify -h host -p port -D "cn=Directory Manager" -w password
   dn:o=TempName,dc=example,dc=com
   changetype:modrdn
   newrdn:dc=uniqueValue
   deleteoldrdn: 1
   ^D
   ```

藉由將 deleteoldrdn 屬性的值設爲 1，可刪除暫時的屬性值配對 o=*TempName*。如果要保留此屬性，您可以將 deleteoldrdn 屬性值設爲 0。

## 解決遺留項目衝突

當複製刪除的作業時，若用戶伺服器發現被刪除的項目還有子項目，則衝突解決程序會建立*接合*項目，以避免目錄中有遺留的項目。

同樣地，當複製加入作業時，若用戶伺服器找不到父項目，則衝突解決程序會建立代表父項目的接合項目，使新項目不會成爲遺留項目。

接合項目是包含物件類別 glue 與 extensibleObject 的暫時項目。接合項目可以使用不同的方式建立：

- 如果衝突解決程序發現有相符唯一識別碼的已刪除項目，接合項目就是恢復使用該項目，並加上 glue 物件類別及 nsds5ReplConflict 屬性。

  在此情況下，您可以修改接合項目，以移除 glue 物件類別及 nsds5ReplConflict 屬性，將項目保留爲正常項目，或者您可以刪除接合項目及其子項目。

- 伺服器建立只含 glue 與 extensibleObject 物件類別的最小項目。

  在此情況下，您必須修改項目將它變成有意義的項目，或刪除它及其所有子項目。

## 解決潛在的交互操作性問題

爲了讓需要屬性唯一性的這類應用程式 ( 如郵件伺服器 ) 能夠具有交互操作性，您可能必須限制存取包含 nsds5ReplConflict 屬性的項目。如果不限制存取這些項目，只需要一個屬性的應用程式將同時挑選原始項目與包含 nsds5ReplConflict 的衝突解決項目，導致作業失敗。

若要限制存取，您必須使用下列指令修改授與匿名讀取存取的預設 ACI：

```
ldapmodify h host -p port -D "cn=Directory Manager" -w password
dn:dc=example,dc=com
changetype:modify
delete:aci
aci:(target ="ldap:///dc=example,dc=com")
 (targetattr !="userPassword"
 (version 3.0;acl "Anonymous read-search  access";
 allow (read, search, compare)(userdn = "ldap:///anyone");)
-
add:aci
aci:(target="ldap:///dc=example,dc=com")
 (targetattr!="userPassword")
 (targetfilter="(!(nsds5ReplConflict=*))")(version 3.0;acl
 "Anonymous read-search access";allow (read, search, compare)
 (userdn="ldap:///anyone");)
^D
```

新的 ACI 將會防止包含 nsds5ReplConflict 屬性的項目傳回到搜尋結果中。

第 9 章

# 延伸目錄結構

Directory Server 隨附標準結構，此結構包括上百種物件類別和屬性。雖然標準物件類別和屬性應該可以符合大部分的需求，但您仍可能需要建立新的物件類別和屬性以延伸您的結構。如需標準結構的概述，以及有關設計結構以符合您的佈署的指示，請參閱 《Directory Server Deployment Planning Guide》中的 Chapter 3 "Directory Server Schema"。

本章描述如何在下列章節中延伸您的結構：



## 結構檢查

當結構檢查處於開啓狀態時，Directory Server 會確保所有匯入、加入和修改作業都符合目前定義的目錄結構：

- 每個項目的物件類別與屬性符合結構。
- 項目包含其所有定義的物件類別的所有必要屬性。
- 項目只包含其物件類別允許的屬性。

| 備註 | 修改項目時，Directory Server 會在整個項目上執行結構檢查，而不僅在被修改的屬性上進行檢查。因此，如果項目中的任何物件類別或屬性不符合結構，作業都可能會失敗。結構檢查不會驗證與語法有關的屬性值有效性。 |
|---|---|

依預設值，結構檢查是開啓的，執行 Directory Server 時應始終開啓結構檢查。許多用戶端應用程式會假設如果結構檢查處於開啓狀態，就表示所有項目都符合結構。但是，開啓結構檢查將不會驗證目錄中現有的內容。唯一保證所有目錄內容都符合結構的方法是在加入任何項目或重新初始化所有項目前就開啓結構檢查。

通常您不會希望關閉結構檢查，唯一可能例外的狀況是要從已知符合結構的 LDIF 檔案匯入時，可以關閉結構檢查以加快匯入速度。但是這樣難免會有風險，萬一匯入不符合結構的項目，將無法偵測出來。

當項目不符合結構時，還是可以搜尋此項目，但對此項目執行的修改作業將會失敗。若要使項目符合結構，您必須執行下列操作：

1. 如果伺服器位於實際執行環境中，您最好先將整部伺服器設成唯讀狀態，以防結構檢查處於關閉狀態時發生任何修改。請參閱第 36 頁「設定全域唯讀模式」。
2. 依下述方式關閉結構檢查。
3. 擷取項目，並以人工方式跟目前定義的結構做比較，以判定不符合的原因。請參閱第 315 頁「檢視屬性」與 第 320 頁「檢視物件類別」。
4. 修改項目，使它符合結構。

   如果有許多不符合的項目，而這些項目呈現某種模式或是資料的新格式，您可以考慮改爲修改結構。但是您應該在部署之前預先規劃結構，將結構變更減到最少的程度。如需詳細資訊，請參閱「Directory Server Deployment Planning Guide」中的第 3 章「目錄伺服器結構」。
5. 依下述方式開啓結構檢查。
6. 如果已設定全域唯讀模式，請取消設定。

## 使用主控台設定結構檢查

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，選取組態樹狀目錄中的結構節點。

   右面板中包含結構的定義。

2. 面板上方的狀態訊息指示目前已啓用或已停用結構檢查。按一下右邊的按鈕即可開啓或關閉結構檢查：

   - 按鈕標示爲 [ 停用 ]，即可關閉結構檢查。
   - 當您可以開啓結構檢查時，按鈕將標示爲 [ 啓用 ]。

   新的結構檢查策略會立即生效。

## 從指令行設定結構檢查

您也可以設定 cn=config 項目的 nsslapd-schemacheck 屬性來開啓或關閉結構檢查：

```
ldapmodify -h host -p port -D "cn=Directory Manager" -w password
dn:cn=config
changetype:modify
replace:nsslapd-schemacheck
nsslapd-schemacheck:on or off
^D
```

伺服器將立刻強制執行新的結構檢查策略。

# 延伸結構概貌

將新屬性加入結構中時，您必須建立新的物件類別以包含這些屬性。雖然這樣看起來似乎很方便，只要將所需的屬性加入現有的物件類別中即可，而且此類別已經包含您所需要的大部分屬性，但是這樣做會危及與 LDAP 用戶端的交互操作性。

Directory Server 與現有 LDAP 用戶端的交互操作性依賴標準的 LDAP 結構。如果您變更標準結構，則在升級伺服器時也會遇到困難。基於相同的原因，您不能夠刪除標準結構元素。

如需關於物件類別、屬性、目錄結構與延伸結構規則的詳細資訊，請參閱《Directory Server Deployment Planning Guide》中的 Chapter 3 "Directory Server Schema"。如需關於標準屬性和物件類別的資訊，請參閱《Directory Server Administration Reference》中的 Chapter 9 "Object Class Reference" 和 Chapter 10 "Attribute Reference"。

Directory Server 結構儲存在 cn=schema 項目的屬性中。如同組態項目一樣，這是結構的 LDAP 檢視，而且是在伺服器啓動期間從檔案中讀取得來。結構檔案是 LDIF 檔案，位於：

*ServerRoot*/slapd-*serverID*/config/schema

此目錄包含 Directory Server 及其他依靠 Directory Server 的 Sun Java System 伺服器所用的標準結構檔案。這些檔案描述於《Directory Server Administration Reference》中的 Chapter 8 的 "Schema Supported by Directory Server 5.2" 中。標準結構本身描述於《Directory Server Administration Reference》中的 Chapter 9 “Object Class Reference“ 和 Chapter 10 “Attribute Reference“。

## 修改結構檔案

伺服器只在啓動時讀取一次結構檔案。檔案的 LDIF 內容會加入 cn=schema 中結構的記憶體 LDAP 檢視。因爲結構定義的順序至關重要，所以結構檔案名稱前會加上編號字首，並依文數字順序載入。只有安裝期間定義的系統使用者可寫入此目錄中的結構檔案。

若要修改檔案中的結構定義，您必須建立或修改所要的檔案，然後重新啓動伺服器。結構檔案中的定義語法描述於 RFC 2252 (http://www.ietf.org/rfc/rfc2252.txt) 中。

直接在 LDIF 檔案中定義結構時，X-ORIGIN 欄位的值不得使用 "user defined"。因爲這是保留值，專供透過 cn=schema 的 LDAP 檢視定義的結構描述元素，以及出現在檔案 99user.ldif 中的結構描述元素使用。

99user.ldif 檔案包含 cn=schema 項目以及從指令行或用主控台加入的所有結構定義的額外 ACI。加入新的結構定義時，將覆寫 99user.ldif 檔案。如果想修改此檔案，您必須立即重新啓動伺服器，以確保將成爲永久性變更。

您不應該修改在其他結構檔案中定義的標準結構。但是您可以加入新檔案，以定義新屬性和物件類別。例如，若要在許多伺服器上定義新的結構描述元素，您可以在 98mySchema.ldif 檔案內定義結構描述元素，再將此檔案複製到所有伺服器的結構目錄中。然後您必須重新啓動所有伺服器，以載入新的結構檔案。

## 從指令行修改結構

因爲結構由 cn=schema 中的 LDAP 檢視定義，所以您可以用 ldapsearch 和 ldapmodify 公用程式在線上檢視及修改結構。但是，您只能修改 X-ORIGIN 欄位的值是 "user defined" 的結構描述元素。伺服器將拒絕其他定義的任何修改。

使用 ldapmodify 可新增及刪除 attributeTypes 和 objectClasses 屬性的個別值。若要修改其中一個值，您必須刪除特定的值，再加入新值，因爲這些屬性是多重值屬性 ( 請參閱第 68 頁「修改多重值屬性的一個值」 )。所用的語法必須是 RFC 2252 (http://www.ietf.org/rfc/rfc2252.txt) 中所述用於定義結構描述元素的語法。

任何新的元素定義，以及您對使用者定義元素所做的變更，都將儲存在 99user.ldif 檔案中。

從指令行修改結構定義容易發生錯誤，因爲您必須輸入完全一致的冗長數值。但是您可以在必須更新目錄結構的指令檔中使用此功能。

## 使用主控台修改結構

若要自訂目錄結構，建議採用的方法是使用以下各節中所述的 Directory Server Console 介面。主控台可讓您檢視標準結構，並提供圖形介面用於定義新的屬性和物件類別，及編輯已定義的元素。

任何新的元素定義，以及您對使用者定義元素所做的變更，都將儲存在 99user.ldif 檔案中。

若要延伸目錄結構，您必須依下列順序進行：

1. 先依第 318 頁「建立屬性」所述，建立新的屬性。
2. 然後建立包含新屬性的物件類別，並將屬性加入物件類別。如需資訊，請參閱第 320 頁「建立物件類別」。

# 管理屬性定義

Directory Server Console 提供介面可檢視結構中的所有屬性，也可以建立、編輯與刪除您自己的屬性定義。

## 檢視屬性

若要檢視目前存在於目錄結構中所有屬性的相關資訊：

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，選取組態樹狀目錄中的 [ 結構 ] 節點，然後選取右面板中的 [ 屬性 ] 標籤。

   此標籤包含結構中所有標準 ( 唯讀 ) 與使用者定義屬性的表格。在表格中的線上按住滑鼠不放，可以顯示對應屬性的描述字串。

   下列表格描述屬性表的欄位。

**表 9-1** 屬性標籤中的表格欄位

| 欄標題 | 描述 |
|---|---|
| 名稱 | 屬性名稱 ( 有時候稱爲屬性類型 )。 |
| OID | 屬性的物件識別碼。OID 是字串，通常爲含有小數點的十進位數字，可唯一識別結構物件。<br>如需關於 OID 的詳細資料，或要爲您的企業要求字首，請傳送郵件至 `iana@iana.org` 給 IANA (Internet Assigned Number Authority，網際網路編號中心 )，或瀏覽 IANA 網站，網址是 `http://www.iana.org/`。 |
| 語法 | 語法描述此屬性所允許的數值格式，可能的語法列於第 316 頁的「表 9-2」中。 |
| Multivalued | 此欄的核取方塊指定屬性是否爲多重值。多重值屬性可以在一個項目中出現多次，但單值屬性則只能出現一次。 |

**表 9-2** 屬性語法定義

| 語法名稱 | 定義 |
|---|---|
| Binary ( 之前爲 `bin`) | 表示此屬性的值被視爲二進位資料。 |
| 布林值 | 表示此屬性只能是這兩個值中的一個：`True` 或 `False`。 |
| Country String | 表示此屬性的值僅限於 ISO 3166 所指定的兩個字母國碼，例如 `FR`。 |
| DN ( 之前爲 `dn`) | 表示此屬性的值爲 DN ( 辨別名稱 )。 |
| DirectoryString ( 之前爲 `cis`) | 表示此屬性的值可包含任何 UTF-8 編碼字元，並視爲不區分大小寫。 |
| GeneralizedTime | 表示此屬性的值被編碼爲可列印字串。必須指定時區。強烈建議使用 GMT。 |
| IA5String ( 之前爲 `ces`) | 表示此屬性的值只可包含 ASCII 字元的子集，而且視爲要區分大小寫。 |
| Integer ( 之前爲 `int`) | 表示此屬性的有效值是整數。 |
| OctetString | 與 Binary 行爲相同。 |

**表 9-2** 屬性語法定義 ( *後續* )

| 語法名稱 | 定義 |
| --- | --- |
| Postal Address | 表示此屬性的值被編碼爲<br>*dstring*`[$ dstring]*`<br>其中每個 *dstring* 元件均使用 DirectoryString 語法加以編碼成數值。在 *dstring* 中的反斜線和貨幣字元都必須加上括號，如此才不會與行分隔符號混淆。許多伺服器都將郵寄地址限制爲 6 行，每行不超過 30 個字元。例如：<br>`1234 Main St.$Anytown, CA 12345$USA` |
| TelephoneNumber ( 之前爲 `tel`) | 表示此屬性的值爲電話號碼格式。建議電話號碼使用國際格式。 |
| URI | 表示此屬性的值包含 URL ( 全球資源定位器 )，加上選用的字首，如 `http://`、`https://`、`ftp://`、`ldap://` 或 `ldaps://`。URI 值的行爲與 IA5String ( 參閱 RFC 2396, `http://www.ietf.org/rfc/rfc2396.txt`) 相同。 |

# 建立屬性

若要在結構中加入您自己的屬性定義。

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，選取組態樹狀目錄中的 [ 結構 ] 節點，然後選取右面板中的 [ 屬性 ] 標籤。
2. 按一下 [ 建立 ] 以顯示 [ 建立屬性 ] 對話方塊。
3. 在文字欄位中輸入資訊，以定義新的屬性。只有屬性名稱和語法是必要的：
   - 屬性名稱 - 輸入屬性的唯一名稱，也稱爲它的屬性類型。屬性名稱必須以字母開頭，而且只包含 ASCII 字母、數字和連字號。

**備註** 屬性名稱可包含大寫字母、但 LDAP 用戶端都不應該依賴這一點。根據 RFC 2251 (`http://www.ietf.org/rfc/rfc2251.txt`) 的 4.1.4 節，屬性名稱必須以不區分大小寫的方式處理。

   - 屬性 OID ( 選用 ) - 輸入屬性的物件識別碼。在第 316 頁的「表 9-1」中描述 OID。如果不指定 OID，Directory Server 會自動使用 *attributeName*`-oid`。請注意，爲嚴格遵守 LDAP v3，您必須提供有效的數字 OID。
   - 屬性別名 ( 選用 ) - 使用以逗號分隔的清單輸入屬性的替代名稱。
   - 屬性描述 ( 選用 ) - 輸入簡短的描述文字以解釋屬性的用途。
   - 語法 - 從描述屬性內含資料的下拉式清單中選取語法。在第 316 頁的「表 9-2」中描述可用的語法。
   - 多重值 - 依預設設值，屬性將爲多重值。如果每個項目中此屬性只能有一個值，請取消選取此核取方塊。
4. 在 [ 建立屬性 ] 對話方塊中，按一下 [ 確定 ]，以定義新的屬性。它將出現在使用者定義的屬性表中。

   在目錄項目中爲此屬性定義值之前，您必須先建立或編輯需要或允許此屬性的物件類別，如第 319 頁「管理物件類別定義」所述。

## 編輯屬性

使用主控台只可以編輯使用者定義的屬性。修改屬性的名稱、語法或多重值定義之前，您必須確定目錄中沒有任何項目目前正在使用此屬性，否則用戶端將無法存取該項目。

若要修改屬性的結構定義：

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，選取組態樹狀目錄中的 [ 結構 ] 節點，然後選取右面板中的 [ 屬性 ] 標籤。
2. 在 [ 使用者定義的屬性 ] 表中，選取要編輯屬性，並按一下 [ 編輯 ]。
3. 修改 [ 編輯屬性 ] 對話方塊中的欄位，以重新定義屬性。

   如果 OID 字串是以屬性名稱爲基礎，則每次變更名稱時就應該變更 OID。在第 316 頁的「表 9-1」中描述 OID。在第 316 頁的「表 9-2」中描述可用的語法。
4. 完成編輯屬性後，按一下 [ 確定 ] 以儲存變更。

## 刪除屬性

使用主控台只可以刪除使用者定義的屬性。刪除屬性定義之前，您必須確定目錄中沒有任何項目目前正在使用此屬性，否則用戶端將無法存取該項目。

若要刪除屬性的結構定義：

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，選取組態樹狀目錄中的 [ 結構 ] 節點，然後選取右面板中的 [ 屬性 ] 標籤。
2. 在 [ 使用者定義的屬性 ] 表中，選取屬性，並按一下 [ 刪除 ]。
3. 出現提示時，確認要刪除。

   伺服器將立即刪除屬性。您無法復原此動作。

# 管理物件類別定義

Directory Server Console 也提供介面可檢視結構中的所有物件類別，也可以建立、編輯與刪除您自己的物件類別定義。

## 檢視物件類別

若要檢視有關所有目前定義物件類別的資訊：

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，選取組態樹狀目錄中的 [ 結構 ] 節點，然後選取右面板中的 [ 物件類別 ] 標籤。

   這個標籤包含結構中所有標準 ( 唯讀 ) 和使用者定義屬性的清單。

2. 從任一個清單中選取要檢視的物件類別。

   標籤中的其他欄位顯示有關選取物件類別的下列資訊：

**表 9-3** 物件類別標籤的欄位

| 欄位 | 描述 |
|---|---|
| 必要的屬性 | 包含必須出現在使用此物件類別之項目中的屬性清單。此清單包括繼承的屬性。 |
| 允許的屬性 | 包含可能出現在使用此物件類別之項目中的屬性清單。此清單包括繼承的屬性。 |
| 父項 | 父項可識別物件類別繼承其屬性和結構的物件類別。物件類別自動繼承其父項物件類別的必要及允許的屬性。 |
| OID | 物件類別的物件識別碼。OID 是字串，通常爲含有小數點的十進位數字，可唯一識別結構物件。<br>如需關於 OID 的詳細資料，或要爲您的企業要求字首，請傳送郵件至 `iana@iana.org` 給 IANA (Internet Assigned Number Authority，網際網路編號中心 )，或瀏覽 IANA 網站，網址是 `http://www.iana.org/`。 |

## 建立物件類別

如果要建立繼承另一個物件類別的數個物件類別，您必須先建立父項物件類別。如果新的物件類別將使用自訂屬性，您也必須先定義這些屬性。

**備註** 主控台只允許您建立結構物件類別。這些物件類別必須繼承自父項。若要定義輔助及抽象物件類別，您必須使用指令行公用程式。

若要在結構中加入您自己的物件類別定義：

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，選取組態樹狀目錄中的 [ 結構 ] 節點，然後選取右面板中的 [ 物件類別 ] 標籤。
2. 按一下 [ 建立 ] 以顯示 [ 建立物件類別 ] 對話方塊。
3. 在文字欄位中輸入下列資訊以定義新的物件類別：
   - 名稱 - 輸入物件類別的唯一名稱。
   - 父項 - 選取要做爲父項的現有物件類別。預設狀況下會選取 `top`，而且如果您的物件類別不是繼承其他任何物件類別，就必須使用此父項。對應的清單中會顯示繼承自父項及其父項的必要和允許的屬性。

     一般而言，如果您想要爲使用者項目加入新屬性，其父項必須是 `inetOrgPerson` 物件類別。如果您想要爲合併的項目加入新屬性，其父項通常是 `organization` 或 `organizationalUnit`。如果您想要爲群組項目加入新屬性，其父項通常是 `groupOfNames` 或 `groupOfUniqueNames`。
   - OID ( 選用 ) - 輸入物件類別的物件識別碼。在第 320 頁的「表 9-3」中描述 OID。如果不指定 OID，Directory Server 會自動使用 *objectClassName*`-oid`。請注意，爲嚴格遵守 LDAP v3，您必須提供有效的數字 OID。
4. 定義使用您的新物件類別的項目將包含的屬性：
   - 若要定義*必須*出現的屬性，請在 [ 可用的屬性 ] 清單中選取一或多個屬性，然後按一下 [ 必要的屬性 ] 方塊左側的 [ 加入 ] 按鈕。
   - 若要定義*可*出現的屬性，請在 [ 可用的屬性 ] 清單中選取一或多個屬性，然後按一下 [ 允許的屬性 ] 方塊左側的 [ 加入 ] 按鈕。
   - 若要移除先前加入的屬性，請反白顯示任一個清單中的屬性，然後按一下對應的 [ 移除 ] 按鈕。您不可以移除繼承自父項物件類別的允許或必要的屬性。
5. 在 [ 建立物件類別 ] 對話方塊中，按一下 [ 確定 ]，以定義新的物件類別。它將出現在使用者定義的物件類別表中，而且現在您可以用此物件類別定義項目。

## 編輯物件類別

使用主控台只可以編輯使用者定義的物件類別。修改物件類別的定義之前，您必須確定目錄中沒有任何項目目前正在使用此物件類別，否則用戶端將無法存取該項目。

若要修改物件類別的結構定義：

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，選取組態樹狀目錄中的 [ 結構 ] 節點，然後選取右面板中的 [ 物件類別 ] 標籤。
2. 從 [ 使用者定義的物件類別 ] 清單中，選取要編輯的物件類別，並按一下 [ 編輯 ]。
3. 修改 [ 編輯物件類別 ] 對話方塊的欄位，以重新定義您的物件類別。

   您無法重新命名物件類別，也無法變更其 OID。若要修改這兩項，請刪除該物件類別，並建立新的物件類別。

   - 父項 - 選取要做爲父項的現有物件類別。對應的清單中會顯示繼承自父項及其父項的必要和允許的屬性。
   - 若要定義*必須*出現的屬性，請在 [ 可用的屬性 ] 清單中選取一或多個屬性，然後按一下 [ 必要的屬性 ] 方塊左側的 [ 加入 ] 按鈕。
   - 若要定義*可*出現的屬性，請在 [ 可用的屬性 ] 清單中選取一或多個屬性，然後按一下 [ 允許的屬性 ] 方塊左側的 [ 加入 ] 按鈕。
   - 若要移除先前加入的屬性，請反白顯示任一個清單中的屬性，然後按一下對應的 [ 移除 ] 按鈕。您不可以移除繼承自父項物件類別的允許或必要的屬性。
4. 完成編輯物件類別後，按一下 [ 確定 ] 以儲存變更。

## 刪除物件類別

使用主控台只可以刪除使用者定義的物件類別。刪除物件類別定義之前，您必須確定目錄中沒有任何項目目前正在使用此物件類別，否則用戶端將無法存取該項目。

若要刪除物件類別的結構定義：

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，選取組態樹狀目錄中的 [ 結構 ] 節點，然後選取右面板中的 [ 物件類別 ] 標籤。
2. 在使用者定義的物件類別清單中，選取物件類別名稱，並按一下 [ 刪除 ]。
3. 出現提示時，確認要刪除。

   伺服器將立即刪除物件類別定義。您無法復原此動作。

# 複製結構定義

當您設定在兩部伺服器之間複製一或多個尾碼時，也會自動複製結構。這可確保所有複本都有完整、完全一樣的結構，以定義可複製到用戶的所有物件類別與屬性。因此，主機伺服器也包含主機結構。

若要在所有複本上強制結構，您必須在所有主機上啓用結構檢查。因爲結構是在執行 LDAP 作業的主機上進行檢查，所以更新用戶時不需要檢查結構。爲改善效能，複製機制在用戶複本上會跳過結構檢查。

**備註** 集線器和專用用戶上不應該關閉結構檢查。結構檢查不會影響用戶的執行效能，所以應該保持開啓狀態，以表示複本內容符合其結構。

在用戶初始化期間，以及透過主控台或指令行工具修改結構時，主機伺服器會自動將結構複製給它的各個用戶。預設狀況下會複製整個結構，而且會建立還不存在用戶上的任何額外結構描述元素，並儲存在 `99user.ldif` 檔案中。

例如，假設主機伺服器在啓動時將結構定義放在 `98mySchema.ldif` 檔案中，然後您定義與其他伺服器 ( 可能是主機、集線器或專用用戶 ) 的複製協議。隨後，當您從這個主機初始化複本時，複製的結構將包含來自 `98mySchema.ldif` 的定義，但結構會儲存在複本伺服器上的 `99user.ldif` 中。

在用戶初始化期間複製過結構之後，只要在主機上的 `cn=schema` 中修改結構，則整個結構也將會複製到用戶。因此，透過指令行公用程式或主控台對主機結構所做的任何修改都會複製到用戶。這些修改將儲存在主機的 `99user.ldif` 中，而且藉由上述的相同機制，它們也會儲存在用戶的 `99user.ldif` 中。

## 修改複製結構檔案

複製機制無法偵測您直接對包含結構的 LDIF 檔案所做的任何變更。因此，如果依第 314 頁「修改結構檔案」所述更新結構，則即使重新啓動主機，變更還是不會複製到用戶。

Directory Server 5.2 提供以下指令檔，可將結構檔案中的變更「推送」給用戶：

```
# ServerRoot/slapd-serverID/schema_push.pl
```

以下程序可用來修改主機伺服器上的結構檔案：

1. 在結構目錄中，加入新的結構檔案，或修改現有的結構檔案：

   *ServerRoot*/slapd-*serverID*/config/schema

   只有安裝期間定義的系統使用者可寫入此目錄中的結構檔案。如需詳細資訊，請參閱第 314 頁「修改結構檔案」。

2. 如上所述，執行 schema_push.pl 指令檔。這個指令檔不會實際將結構「推送」給用戶，而是在結構檔案中寫入一個特殊的屬性，使得只要一載入結構檔案，就會立即複製結構。

3. 重新啓動伺服器。伺服器將載入所有結構檔案，而且複製機制將複製新的結構到其用戶。

# 限制結構複製

依預設值，每當複製機制複製結構時，它會將整個結構傳給其用戶。但有兩種情況，不需要這種作法：

- 使用主控台或從指令行修改 cn=schema 時，只能修改使用者定義的結構描述元素，所有標準結構不變。如果您經常修改結構，則每次都傳送大量未經變更的結構描述元素會影響執行效能。爲改善複製和伺服器效能，您可以只複製使用者定義的結構描述元素。
- 當 Directory Server 5.2 上的主機複製到 Directory Server 5.1 上的用戶時，這兩種版本的組態屬性結構並不相同，而且可能產生衝突。在這種情況下，您*必須*只複製使用者定義的結構描述元素，說明如下。

以下指令可用來限制結構複製，使得只複製使用者定義的結構：

```
ldapmodify -h host -p port -D "cn=Directory Manager" -w password
dn:cn=config
changetype:modify
replace:nsslapd-schema-repl-useronly
nsslapd-schema-repl-useronly:on
^D
```

預設值 off 會在必要時複製整個結構。

第 10 章

# 編製目錄資料索引

Directory Server 的索引就像書本的索引頁一樣，藉由把要搜尋的字串跟目錄內容的參考產生關聯，可以加快搜尋的速度。索引是屬性值的表格，儲存在單獨的資料庫檔案內。目錄中每個尾碼的索引建立與管理彼此獨立。一旦在尾碼組態中建立索引後，伺服器就會自動維護索引。

如需索引簡介、索引成本與效益、`nsslapd-allidsthreshold` 屬性說明以及提昇 Directory Server 效能的方法，請參閱《Directory Server Performance Tuning Guide》中的 Chapter 4 "Tuning Indexing"。

本章包含下列章節：



## 編製索引概論

每個尾碼的索引分別儲存在對應的資料庫目錄檔案內。每個索引檔案包含尾碼中爲指定屬性定義的所有索引。例如，爲一般名稱 (cn) 屬性維護的所有索引儲存在 *databaseName*`_cn.db3` 檔中。

當您初始化尾碼或使用本章所述的指令時，就會建立索引檔案。在用戶端搜尋作業與內部作業期間，伺服器會存取索引，以更快速地找到目錄中的項目。修改作業期間，目錄必須藉由更新索引檔案來更新目錄內容及維護索引。

Directory Server 支援下列索引類型：

- 存在索引 (`pres`) - 包含一個項目的清單，這些項目含有特殊的屬性，而不論其值爲何。

- 相等索引 (eq) - 可讓您更有效率地搜尋包含特定屬性值的項目。
- 近似索引 (approx) - 提供利用 ~= 篩選運算元的有效「發音近似」搜尋。例如，對於搜尋部份名稱或拼錯的名稱而言，近似索引是很有幫助的。Directory Server 使用各種 metaphone 語音演算法，在近似索引上執行搜尋。

**備註** Directory Server 的 metaphone 語音演算法只支援 US-ASCII 字母。因此，只能利用英文值使用近似編製索引。

- 子字串索引 (sub) - 提供如 cn=*john 或 cn=john* 之屬性值子字串的有效搜尋。由於每一個值有許多可能的子字串，因而這是成本高昂的索引維護方式。

  Directory Server 爲子字串編製索引，以便能夠在索引中找到要搜尋的最短*雙*字元子字串。因此使用索引，可以加快搜尋（sn=*ab）的速度，但是搜尋（sn=*a）卻不會加快速度。Directory Server 提供進一步的最佳化，允許對萬用字元*前*只有一個字元時進行起始的子字串搜尋。因此，在子字串索引可用時，也可以加速搜尋（sn=a*）的速度，但不能加速搜尋（sn=*a)) 的速度。如需有關子字串索引的詳細資訊，請參閱《Directory Server Performance Tuning Guide》中的 "Substring Indexes"。
- 對應規則索引 - 在本地化對應規則 ( 也稱爲定序排序 ) 的 OID 與要編製索引的屬性之間建立關聯，以加速在國際目錄中的搜尋。
- 瀏覽索引 - 改善以虛擬清單檢視 (VLV) 控制執行之搜尋回應時間。您可以在樹狀目錄中的任何分支點上建立瀏覽索引，以改善大幅擴展之樹狀子目錄的顯示效能，例如 ou=People,dc=example,dc=com。

## 系統索引

系統索引是不得刪除或修改的索引。Directory Server 需要有這些索引才能正確有效率地運作。下表列出每個尾碼中自動建立的系統索引：

**表 10-1** 每個尾碼中的系統索引

| 屬性 | 相等索引 | 存在索引 | 目的 |
|---|---|---|---|
| aci | | X | 讓目錄伺服器能夠快速取得目錄中維護的存取控制資訊。 |
| ancestorid | X | | 包含每個項目的原始節點清單。 |
| entrydn | X | | 加快根據 DN 搜尋的項目擷取速度。 |
| id2entry | X | | 包含目錄項目的實際資料庫。可以從此建立所有其他資料庫檔案。 |

**表 10-1** 每個尾碼中的系統索引 *( 後續 )*

| 屬性 | 相等索引 | 存在索引 | 目的 |
|---|---|---|---|
| nsUniqueId | X | | 用於搜尋特定項目。 |
| nscpEntryDN | X | | 供 Directory Server 內部的複製功能使用。 |
| nsds5ReplConflict | X | X | 用於協助找出複製衝突。 |
| numsubordinates | | X | 供 Directory Server Console 用於增強 [ 目錄 ] 標籤上的顯示效能。 |
| objectClass | X | | 用來協助在目錄中加速樹狀子目錄的搜尋。 |
| parentID | X | | 提高單層搜尋期間的目錄效能。 |

# 預設索引

當您在目錄中建立新尾碼時，伺服器會在對應的資料庫目錄中設定一組預設索引。您可以依編製索引的需要修改預設索引，但在取消設定索引之前，應該確定沒有任何伺服器 Plug-in 或您公司的其他伺服器會需要依靠該索引的屬性。

若要修改新尾碼建立時將使用的預設索引組，請參閱第 335 頁「修改預設索引組」。

下表列出 Directory Server 中預先設定的預設索引：

**表 10-2** 每個新尾碼的預設索引

| 屬性 | 相等索引 | 存在索引 | 子字串索引 | 目的 |
|---|---|---|---|---|
| cn | X | X | X | 改善最常使用類型的使用者目錄搜尋效能。 |
| givenName | X | X | X | 改善最常使用類型的使用者目錄搜尋效能。 |
| mail | X | X | X | 改善最常使用類型的使用者目錄搜尋效能。 |
| mailAlternateAddress | X | | | 由 Sun Java System Messaging Server 使用。 |
| mailHost | X | | | 由 Sun Java System Messaging Server 所使用。 |
| member | X | | | 改善 Sun Java System 伺服器效能。參考的完整性 Plug-in 也會使用此索引。如需詳細資訊，請參閱第 77 頁「維護參考的完整性」。 |
| nsCalXItemId | X | X | X | 由 Sun Java System Calendar Server 使用。 |

**表 10-2** 每個新尾碼的預設索引 *( 後續 )*

| 屬性 | 相等索引 | 存在索引 | 子字串索引 | 目的 |
|---|---|---|---|---|
| nsLIProfileName | X | | | 由 Sun Java System Messaging Server 的漫遊功能使用。 |
| nsRoleDN | X | | | 改善以角色爲基礎的作業效能。 |
| nswcalCALID | X | | | 由 Sun Java System Calendar Server 所使用。 |
| owner | X | | | 改善 Sun Java System 伺服器效能。參考的完整性 Plug-in 也會使用此索引。如需詳細資訊，請參閱第 77 頁「維護參考的完整性」。 |
| pipstatus | X | | | 由 Sun Java System Server 使用。 |
| pipuid | | X | | 由 Sun Java System Server 所使用。 |
| seeAlso | X | | | 改善 Sun Java System 伺服器效能。參考的完整性 Plug-in 也會使用此索引。如需詳細資訊，請參閱第 77 頁「維護參考的完整性」。 |
| sn | X | X | X | 改善最常使用類型的使用者目錄搜尋效能。 |
| telephoneNumber | X | X | X | 改善最常使用類型的使用者目錄搜尋效能。 |
| uid | X | | | 改善 Sun Java System 伺服器效能。 |
| uniquemember | X | | | 改善 Sun Java System 伺服器效能。參考的完整性 Plug-in 也會使用此索引。如需詳細資訊，請參閱第 77 頁「維護參考的完整性」。 |

# 屬性名稱快速參考表

下表列出所有具有主要或真實名稱以及別名的屬性。建立索引時，請確認使用主要名稱。

**表 10-3** 主要屬性名稱及其別名

| 主要屬性名稱 | 屬性別名 |
|---|---|
| authorCn | documentAuthorCommonName |
| authorSn | documentAuthorSurname |
| c | countryName |
| cn | commonName |
| co | friendlyCountryName |

**表 10-3** 主要屬性名稱及其別名

| 主要屬性名稱 | 屬性別名 |
|---|---|
| dc | domainComponent |
| dn | distinguishedName |
| drink | favoriteDrink |
| facsimileTelephoneNumber | fax |
| l | localityName |
| labeledUri | labeledUrl |
| mail | rfc822mailbox |
| mobile | mobileTelephoneNumber |
| o | organizationName |
| ou | organizationalUnitName |
| pager | pagerTelephoneNumber |
| sn | surname |
| st | stateOrProvinceName |
| street | streetAddress |
| ttl | timeToLive |
| uid | userId |

## 管理索引

本節描述如何使用 Directory Server Console 和指令行爲特定屬性建立及移除存在、相等、近似、子字串與國際索引。如需關於虛擬清單檢視 (VLV) 作業所需的獨立程序，請參閱第 336 頁「管理瀏覽索引」。

**備註** 因爲索引是每個尾碼特有的，您必須記得在*每一個*尾碼組態中建立您自己的新索引。

當您用主控台建立新尾碼時，您可以選擇複製現有尾碼的索引組態。

建立新索引前，請先衡量維護索引的成本與效益。請記住：

- 近似索引不適合使用在包含一般數值的屬性上，例如電話號碼，因爲這樣是沒有效率的。
- 若爲二進位屬性，則子字串索引無法運作。
- 相等索引不應該用於較大的數值，例如 `jpegPhoto` 這類計劃包含二進位資料的屬性。
- 維護索引需要更多資源，因此，只有一般搜尋的屬性才應該要編製索引。項目建立將會需要更多 CPU 時間，因爲伺服器必須檢查所有編製索引屬性，並且產生新項目中所包含之各索引屬性新項目。
- 各索引檔大小爲目錄內容的等比例。
- 視搜尋類型而定，雖然搜尋效能無法和編製索引的搜尋效能相提並論，但是搜尋要求中仍然可以指定沒有編製索引的屬性。

## 使用主控台管理索引

如果您計劃在許多屬性上修改或加入索引，您應該先將尾碼設爲唯讀，再將其內容匯出到 LDIF。接著利用從 LDIF 檔案重新初始化尾碼的方式，將會比尾碼重新編製索引的速度快。

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，展開 [ 資料 ] 節點，並選擇要編製索引的尾碼。然後選擇右面板上的 [ 索引 ] 標籤。

   「系統索引」表不得修改。請在「額外索引」表中的屬性上加入、修改或移除索引。

2. 若要在尚未編製索引的屬性上加入索引，請按一下 [ 加入屬性 ] 按鈕。在顯示的對話方塊中，選擇一或多個要編製索引的屬性，再按一下 [ 確定 ]。

   新屬性出現在「額外索引」表中。

3. 若要修改屬性的索引，請在「額外索引」表中選擇或取消選取要爲該屬性維護之每種索引類型旁的核取方塊。

4. 如果要爲包含非英文值的屬性建立索引，請在 [ 對應規則 ] 欄位中輸入要使用之定序排序的 OID。

   您可以用逗號分隔 ( 但不可以有空格 ) 列出多個 OID，來用多種語言爲屬性編製索引。如需支援的地區設定清單，及其關聯定序排序的 OID，請參閱《Directory Server Administration Reference》中的 Chapter 5 "Directory Internationalization Reference"。

5. 若要移除屬性的所有索引，請在表格中選擇它的列，再按一下 [ 刪除屬性 ] 按鈕。

6. 按一下 [ 儲存 ] 以儲存新的索引組態。

   如果移除屬性的所有索引，伺服器將移除該屬性的每個索引檔案，至此組態就已完成。如果您修改屬性的索引，或加入新索引，請繼續進行下一個步驟。

7. 出現警告對話方塊，通知您必須更新資料庫檔案，才能開始使用新索引。您可以重新編製尾碼索引，或將尾碼重新初始化。

   - 如果只加入或修改一或兩個索引，或是您的尾碼不得設爲無法使用，您應該重新編製尾碼索引。請按一下 [ 重新索引尾碼 ]，以顯示重新編製索引對話方塊。預設狀況下會選擇您對索引組態修改或加入的屬性。按一下 [ 確定 ] 以開啓重新編製這些屬性的索引。對於有幾百萬筆項目的目錄，若重新編製許多屬性的索引可能要花費幾個小時的時間才能完成，但在重新編製索引期間，尾碼將始終處於線上的狀態。

   - 如果在幾個屬性上加入或修改索引，而且您有一個從這個尾碼匯出的最新 LDIF 檔案，請按一下 [ 初始化尾碼 ] 按鈕。在 [ 初始化尾碼 ] 對話方塊中，輸入或瀏覽 LDIF 檔案的路徑與名稱，再按一下 [ 確定 ]。伺服器將從 LDIF 檔案重新初始化尾碼，並根據新組態建立所有索引。依目錄大小而定，重新初始化尾碼通常會比重新編製兩個或多個屬性的索引快，但在初始化過程中，尾碼將無法使用。

   - 如果不將尾碼重新編製索引或初始化，所有資料仍將可以使用，但不會建立新索引，也不會改善目錄存取效能。

   如果將尾碼重新編製索引或初始化，則對於您加入的任何新資料，或是目錄中任何現有的資料，新索引都會立即生效。您不需要重新啓動伺服器。

## 從指令行管理索引

從指令行建立或修改索引分爲兩個步驟：

- 使用 `ldapmodify` 指令行公用程式加入或修改索引組態項目。每個尾碼中的索引都是分別設定，索引組態項目與對應的資料庫組態儲存在一起。
- 執行 `directoryserver db2index-task` 指令以產生由伺服器進行維護的新索引組。

**小心** 不能刪除系統索引，因爲將其刪除可能會嚴重影響 Directory Server 效能。系統索引位於下列項目中：

```
cn=index,cn=databaseName,cn=ldbm database,cn=plugins,cn=config
```

```
cn=default indexes,cn=config,cn=ldbm database,
 cn=plugins,cn=config
```

刪除預設索引時要小心，因爲可能會影響到 Directory Server 的運作方式。

## 建立索引組態項目

若要爲尚未編製索引的屬性建立索引，您必須在對應資料庫的組態中爲該屬性建立新的項目。

索引組態項目擁有下列 DN：

```
cn=attributeName,cn=index,cn=databaseName,cn=ldbm database,
 cn=plugins,cn=config
```

其中 *databaseName* 是要建立索引之尾碼的對應資料庫名稱。例如，下列指令將爲法文的 sn ( 姓氏 ) 屬性值建立存在、相等、子字串和「發音類似」索引：

```
ldapmodify -a -h host -p port -D "cn=Directory Manager" -w password
dn:cn=sn,cn=index,cn=databaseName,cn=ldbm database,
 cn=plugins,cn=config
objectClass:top
objectClass:nsIndex
cn:sn
nsSystemIndex:false
nsIndexType:pres
nsIndexType:eq
nsIndexType:sub
nsIndexType:approx
nsMatchingRule: 1.3.6.1.4.1.42.2.27.9.4.76.1
^D
```

索引組態項目擁有 `nsIndex` 物件類別，而且 `nsSystemIndex` 屬性必須存在，它的值必須是 `false`。您無法建立新的系統索引。系統只維護由 Directory Server 內部定義的現有系統索引。

`nsIndexType` 屬性值列出將爲指定屬性維護的索引。請使用上述任何值定義對應的索引。

您也可以用單一值 none 明確停用屬性的索引，例如，暫時停用屬性的索引編製工作。如果索引組態項目中不包含 nsIndexType 屬性，將預設爲維護所有索引。

選用的 nsMatchingRule 屬性包含國際化索引的語言定序排序 OID。如需支援的地區設定清單，及其關聯定序排序的 OID，請參閱《 Directory Server Administration Reference》中的 Chapter 5 "Directory Internationalization Reference"。

如需關於索引組態屬性的詳細資料，請參閱《 Directory Server Administration Reference》 Chapter 2 的 "Default Index Attributes"。

**備註** 建立索引時，您應該永遠使用屬性的主要名稱 ( 不是屬性別名 )。屬性的主要名稱爲該結構中之屬性所列示的第一個名稱，例如 userid 屬性的 uid。如需所有主要與別名屬性名稱清單，請參閱第 328 頁的「表 10-3」。

## 修改索引組態項目

若要設定屬性上已定義的索引，請修改對應的索引項目。例如，以下在先前定義的 sn 索引組態上執行的指令將移除「發音類似」索引，並將語言改爲加拿大法文：

```
ldapmodify -h host -p port -D "cn=Directory Manager" -w password
dn:cn=sn,cn=index,cn=databaseName,cn=ldbm database,
 cn=plugins,cn=config
changetype:modify
delete:nsIndexType
nsIndexType:approx
-
replace:nsMatchingRule
nsMatchingRule: 1.3.6.1.4.1.42.2.27.9.4.78.1
^D
```

## 執行 db2index-task

建立索引項目後，若在現有索引項目上加入其他索引類型，或修改其定序排序，則執行 directoryserver db2index-task 指令以產生新的索引。此指令會根據其組態項目讀取尾碼內容，爲指定屬性編製索引。

在執行此指令時，使用者仍然可以透過伺服器取得尾碼內容，但在指令完成之前，將不進行索引搜尋。重新編製索引作業需要耗費大量資源，因此可能會影響伺服器上其他作業的效能。依目錄大小而定，重新初始化尾碼通常會比重新編製兩個或多個屬性的索引快，但在初始化過程中，尾碼將無法使用。如需詳細資訊，請參閱第 335 頁「重新初始化尾碼」。

下列範例會在 *databaseName* 對應的尾碼中重新產生 *sn* 索引。

```
# /usr/sbin/directoryserver db2index-task
  -D "cn=Directory Manager" -w password -n databaseName -t sn
```

如需詳細資訊，請參閱 《Directory Server Administration Reference》 Chapter 1 的 "db2index-task"。

### 刪除屬性的所有索引

如果要移除爲屬性設定的所有索引，您可以移除其組態項目和資料庫檔案。例如，下列指令將取消設定 *databaseName* 資料庫中 sn 屬性的所有索引。

```
ldapdelete -h host -p port -D "cn=Directory Manager" -w password \
"cn=sn,cn=index,cn=databaseName,cn=ldbm database,cn=plugins, \
 cn=config"
```

一旦刪除這個項目後，*databaseName* 資料庫對應的尾碼中將不再維護 sn 屬性的索引。若要節省磁碟空間，您也可以刪除對應的索引檔案，因爲伺服器將再也用不到該檔案。在此範例中，您可以刪除下列檔案：

*ServerRoot*/slapd-*serverID*/db/*databaseName*/*databaseName*_sn.db3

## 重新編製尾碼索引

如果您的索引檔案毀損，您必須重新編製尾碼索引，在對應的資料庫目錄中重新建立索引檔案。使用 Directory Server Console 重新編製尾碼索引的方式有二：重新編製索引或重新初始化。

### 重新編製尾碼索引

當您重新編製尾碼索引時，伺服器會檢查它包含的所有項目，並重新建立索引檔案。重新編製索引期間，尾碼的內容仍可供讀取與寫入作業使用。但伺服器必須掃描每個已重新編製索引的整個尾碼。依您設定的索引而定，可能花費數小時重新編製數百萬個項目的尾碼。而且，在重新編製索引期間，索引將無法使用，伺服器效能會受到影響。

若要使用主控台重新編製尾碼索引：

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，展開 [ 資料 ] 節點，顯示您要重新編製索引的尾碼。
2. 以滑鼠右鍵按一下尾碼組態節點，再選擇快顯功能表中的 [ 重新索引 ]。或者，在節點上按一下滑鼠左鍵以選擇節點，再從 [ 物件 ] 功能表中選擇 [ 重新索引 ]。

   出現 [ 重新索引尾碼 ] 對話方塊，列出所選尾碼上已編製索引的所有屬性清單。

3. 選擇要重新編製索引的每個屬性旁的核取方塊。使用 [ 全部檢查 ] 和 [ 不檢查 ] 按鈕可幫您選擇項目。因爲指定屬性的所有索引都儲存在同一個資料庫檔案中，您必須一起將它們全部重新編製索引。

4. 按一下「確定」。主控台顯示確認訊息，說明重新編製索引過程中可能發生非預期的搜尋結果，以及對效能的影響等。

5. 按一下 [ 是 ] 開始重新編製索引。

   主控台顯示對話方塊，內含有關重新編製索引的任何訊息。完成後請關閉對話方塊。

若要從指令行重新編製尾碼索引，請依照第 333 頁「執行 db2index-task」中的指示進行，並指定所有要重新建立索引檔案的屬性。

### 重新初始化尾碼

當您重新初始化尾碼時，其內容會被取代，並在匯入新內容時建立新的索引檔案。重新初始化尾碼通常會比重新編製多於一個屬性的索引快，因爲在載入項目的同時，只要一個階段即完成屬性的索引編製。但是在重新初始化期間，尾碼將無法使用。

以下所有步驟都可以使用 Directory Server Console 或從指令行執行：

1. 依第 107 頁「設定存取權限及參照」所述將尾碼設爲唯讀狀態。您必須先將尾碼設爲無法寫入，這樣在匯出內容後才不會發生任何修改。

2. 依第 145 頁「使用主控台將單一尾碼匯出到 LDIF」所述將整個尾碼匯出到 LDIF 檔案。

3. 依第 140 頁「初始化尾碼」所述匯入同一個 LDIF 檔案，以重新初始化尾碼。

   初始化期間，尾碼將無法使用。當初始化完成時，所有設定的索引將已準備好可供使用。

4. 依第 107 頁「設定存取權限及參照」所述重新將尾碼設爲可寫入。

## 修改預設索引組

建立新尾碼時所用的預設索引組是在下列項目下定義：

```
cn=default indexes,cn=config,cn=ldbm database,cn=plugins,cn=config
```

每當您使用主控台或從指令行建立尾碼時，就會依原狀複製預設索引定義，成爲對應資料庫的初始索引組態。

預設索引組只可用指令行公用程式進行設定。預設索引項目的語法與第 331 頁「從指令行管理索引」中所述的索引組態項目完全一樣。例如，使用下列 `ldapmodify` 指令即可加入預設索引組態項目：

```
ldapmodify -a -h host -p port -D "cn=Directory Manager" -w password
dn:cn=drink,cn=default indexes,cn=config,cn=ldbm database,
 cn=plugins,cn=config
objectClass:top
objectClass:nsIndex
cn:drink
nsSystemIndex:false
nsIndexType:eq
nsIndexType:sub
nsMatchingRule: 1.3.6.1.4.1.42.2.27.9.4.76.1
^D
```

加入此項目後，任何新尾碼都會將 `drink` 屬性的值編製索引，以進行法文的相等和子字串搜尋。

若要修改或刪除預設索引項目，請使用 `ldapmodify` 或 `ldapdelete` 指令編輯 `cn=default indexes,cn=config,cn=ldbm database,cn=plugins,cn=config` 中的索引組。

# 管理瀏覽索引

瀏覽索引是特殊的索引，只供要求伺服器端排序或虛擬清單檢視 (VLV) 結果的搜尋作業使用。對於要求將大量結果進行伺服器端排序的搜尋，使用瀏覽索引可以改善搜尋的效能。在未定義瀏覽索引時，伺服器可拒絕執行要求排序的搜尋要求 ( 依目錄組態而定 )；以防止大量的排序作業導致伺服器資源負載過重。

瀏覽索引套用在作爲搜尋基礎的項目，而且您必須爲排序要求中使用的每一個搜尋條件各建立一個索引。例如，如果用戶端應用程式經常要求所有使用者的排序清單，您可以針對用戶端所用的篩選字串在 `ou=People` 上建立瀏覽索引。

就如同其他索引一樣，爲維護瀏覽索引所需的更新作業過程中會有效能變慢的問題。您應該小心規劃並測試瀏覽索引的部署。

## 主控台的瀏覽索引

Directory Server Console 經常執行整個目錄的搜尋，以重新整理面板內容。如果您已依第 33 頁「樹狀目錄檢視選項」所述將主控台設成會排序樹狀目錄中的項目，您應該爲主控台建立瀏覽索引。

主控台的瀏覽索引是主控台所執行的搜尋特有的。它們也是使用主控台來建立。若要爲主控台建立瀏覽索引：

1. 在 Directory Server Console 最上層的 [ 目錄 ] 標籤上，瀏覽樹狀目錄，以顯示必須排序的大型樹狀子目錄的父項，例如包含數千筆使用者項目的 `ou=People,dc=example,dc=com`。
2. 以滑鼠右鍵按一下父項，再選擇快顯功能表中的 [ 建立瀏覽索引 ]。或者，以滑鼠左鍵按一下項目以選擇項目，再從 [ 物件 ] 功能表中選擇 [ 建立瀏覽索引 ]。

   [ 建立瀏覽索引 ] 對話方塊顯示索引建立的狀態。主控台會建立以下所示的瀏覽索引組態項目，然後產生索引檔案的內容。
3. 按一下 [ 關閉 ] 以關閉 [ 建立瀏覽索引 ] 對話方塊。

   對於任何主控台重新整理作業，新索引會立即生效，而且加入目錄的任何新資料都將受到維護。您不需要重新啓動伺服器。

主控台的瀏覽索引組態由下列項目組成。`vlvSearch` 項目定義即將編製索引之搜尋的基礎、範圍與篩選。`vlvIndex` 項目 `vlvSort` 屬性顯示支援以其排序的順序排序的屬性：

```
dn:cn=MCC entryDN,cn=databaseName,cn=ldbm database,
 cn=plugins,cn=config
objectClass:top
objectClass:vlvSearch
cn:MCC entryDN
vlvBase:"entryDN"
vlvScope: 1
vlvFilter:(|(objectclass=*)(objectclass=ldapsubentry))

dn:cn=by MCC entryDN, cn=MCC entryDN,cn=databaseName,
 cn=ldbm database,cn=plugins,cn=config
objectClass:top
objectClass:vlvIndex
cn:by MCC entryDN
vlvSort:cn givenname o ou sn uid
```

若要刪除 Directory Server Console 的瀏覽索引：

1. 在 Directory Server Console 最上層的 [ 目錄 ] 標籤上，瀏覽樹狀目錄，以顯示已建立瀏覽索引的項目。
2. 以滑鼠右鍵按一下項目，再選擇快顯功能表中的 [ 刪除瀏覽索引 ]。或者，以滑鼠左鍵按一下項目以選擇項目，再從 [ 物件 ] 功能表中選擇 [ 刪除瀏覽索引 ]。只有當所選項目擁有主控台的瀏覽索引時，這個功能表項目才會有作用。

3. 顯示 [ 刪除瀏覽索引 ] 對話方塊要求您確認要刪除索引。按一下 [ 是 ] 以刪除瀏覽索引。

## 用戶端搜尋的瀏覽索引

排序用戶端搜尋結果的自訂瀏覽索引必須手動定義。從指令行建立瀏覽索引或虛擬清單檢視 (virtual list view, VLV) 包括兩個步驟：

- 使用 `ldapmodify` 公用程式或 Directory Server Console 的 [目錄] 標籤加入新的瀏覽索引項目，或編輯現有的瀏覽索引項目。
- 執行 `directoryserver vlvindex` 指令以產生讓伺服器進行維護的新瀏覽索引組。

### 指定瀏覽索引項目

瀏覽索引是指定基礎項目及其樹狀子目錄上的指定搜尋特有的。瀏覽索引組態定義於包含項目的尾碼的資料庫組態中。

| **備註** | 您無法在鏈接尾碼上建立瀏覽索引，只能在本機尾碼和子尾碼上建立。 |
|---|---|

有兩個可用於設定瀏覽索引的項目。第一個使用 `vlvSearch` 物件類別，並指定將編製索引之搜尋作業的基礎、範圍與篩選。第二個項目是第一個項目的子項，並使用 `vlvIndex` 物件類別指定要排序的屬性，以及排序的順序。

以下範例使用 `ldapmodify` 公用程式建立瀏覽索引組態項目：

```
ldapmodify -a -h host -p port -D "cn=Directory Manager" -w password
dn:cn=Browsing ou=People, cn=databaseName,
 cn=ldbm database,cn=plugins,cn=config
objectClass:top
objectClass:vlvSearch
cn:Browsing ou=People
vlvbase:ou=People,dc=example,dc=com
vlvscope: 1
vlvfilter:(objectclass=inetOrgPerson)

dn:cn=Sort rev employeenumber, cn=Browsing ou=People,
 cn=databaseName,cn=ldbm database,cn=plugins,cn=config
objectClass:top
```

```
objectClass:vlvIndex
cn:Sort rev employeenumber
vlvSort:-employeenumber
^D
```

vlvscope 可能是 0 代表僅限基礎項目、1 代表基礎的下一層子項或 2 代表以基礎爲根部的整個樹狀子目錄。vlvfilter 是用戶端搜尋作業中即將使用的同一個 LDAP 篩選。因爲所有瀏覽索引項目位於同一位置，您應該使用描述性的 cn 值爲您的瀏覽索引命名。

每個 vlvSearch 項目必須至少擁有一個 vlvIndex 項目。vlvSort 屬性是定義排序屬性及排序順序的屬性名稱清單。屬性名稱前的虛線 (-) 指示反向排序。您可以定義數個 vlvIndex 項目，即可爲搜尋定義多個索引。延續上個範例，您可以加入下列項目：

```
ldapmodify -a -h host -p port -D "cn=Directory Manager" -w password
dn:cn=Sort sn givenname uid, cn=Browsing ou=People,
 cn=databaseName,cn=ldbm database,cn=plugins,cn=config
objectClass:top
objectClass:vlvIndex
cn:Sort sn givenname uid
vlvSort:sn givenname uid
^D
```

若要修改瀏覽索引組態，請編輯對應的 vlvSearch 或 vlvIndex 項目。若要移除瀏覽索引，讓伺服器不再維護此索引，請移除個別的 vlvIndex 項目，或如果只有一個這類項目，請同時移除 vlvSearch 項目和 vlvIndex 項目。當您移除 vlvIndex 項目時，您也可以移除對應的資料庫檔案，例如：

*ServerRoot*/slapd-*serverID*/db/*dbName*/*dbName*_vlv#Sortsngivennameuid.db3

## 執行 vlvindex 指令

建立瀏覽索引項目或修改瀏覽索引項目後，您必須執行 directoryserver vlvindex 指令以產生新的瀏覽索引組。這個指令將掃描目錄內容，並爲瀏覽索引建立資料庫檔案。

若要產生瀏覽索引，請使用下列指令：

```
# /usr/sbin/directoryserver vlvindex
```

以下範例會產生上一節定義的瀏覽索引：

```
  # /usr/sbin/directoryserver vlvindex -n databaseName -T "Browsing
ou=People"
```

**表 10-4** 範例中使用的 vlvindex 選項描述

| 選項 | 描述 |
|---|---|
| -n | 請指定含有需要索引項目的資料庫名稱。 |
| -T | 指定對應的瀏覽索引的 vlvSearch 項目的命名屬性值。將產生對應到指定 vlvSearch 項目的 vlvIndex 項目的所有索引。 |

如需詳細資訊，請參閱 《Directory Server Administration Reference》 Chapter 1 的 "vlvindex"。

# 第 11 章

# 管理驗證和安全性

Directory Server 支援數種機制以提供安全和受信任的網路通訊。LDAPS 是標準的 LDAP 通訊協定，此通訊協定在安全通訊端階層 (SSL) 上執行，用以加密資料並選用憑證。

Directory Server 也支援啓動傳輸層安全性 (Start TLS) 延伸作業，以便在原本未加密的 LDAP 連線上啓用 TLS。

Directory Server 現在也支援在簡單驗證及安全階層 (SASL) 上的 Generic Security Services API (GSSAPI)。這可讓您在 Solaris 作業系統中使用 Kerberos Version 5 安全通訊協定。再透過一個識別對映機制，使 Kerberos 策略與目錄中的識別產生關聯。

如需其他安全資訊，請參閱 NSS 網站：

`http://www.mozilla.org/projects/security/pki/nss/`

本章包含下列章節：

# Directory Server 中的 SSL 簡介

安全通訊端階層 (SSL) 在 Directory Server 與其用戶端之間提供加密通訊與選用的驗證。不論是 LDAP 或 DSML-over-HTTP 通訊協定都可以啓用 SSL，爲伺服器的任何連線提供安全性。此外，複製及鏈接尾碼機制也可以配置成使用 SSL，使伺服器之間能夠進行安全的通訊。

將 SSL 與簡單驗證 ( 連結 DN 與密碼 ) 一起使用時，所有進出伺服器的資料都會加密，以保證資料的機密性與完整性。用戶端可以選擇使用憑證通過 Directory Server 的驗證，或透過簡單驗證及安全階層 (SASL) 使用協力廠商的安全性機制通過驗證。以憑證爲基礎的驗證使用公開金鑰加密，以防有人僞造及冒充用戶端或伺服器的身份。

Directory Server 能夠在不同連接埠上同時處理 SSL 與非 SSL 通訊；您也可以限制所有通訊都必須通過安全連接埠，以維護系統安全性。用戶端驗證也是可設定的，您可以依據強制實施的安全層級，指定用戶端必須通過驗證，或是直接允許存取。

啓用 SSL 也會啓用 Start TLS 延伸作業，以提供一般 LDAP 連線上的安全性。用戶端可以連結到非 SSL 連接埠，再使用傳輸層安全性通訊協定啓動 SSL 連線。Start TLS 作業讓用戶端更有彈性，而且可能有助於簡化連接埠配置。

SSL 所提供的加密機制也用於屬性加密。啓用 SSL 將允許您在尾碼上配置屬性加密，使資料儲存在目錄期間能夠受到保護。如需詳細資訊，請參閱第 74 頁「加密屬性值」。

爲提供更多一層保護，您可以根據用戶端使用 SSL 或憑證，來配置目錄內容的存取控制。您可以定義要求特定驗證方法的存取控制指令 (ACI)，從而確保資料只能透過安全的通道傳送。如需詳細資訊，請參閱第 193 頁「連結規則」。

如需 SSL、網際網路安全性和憑證的完整描述，也包括如何在管理伺服器中配置 SSL，請參閱 《Administration Server Administration Guide》中的 Chapter 9 "Using SSL and TLS with Sun Java System Servers"。

## 啓動 SSL 的步驟概要

以下每個步驟都將於本章隨後各節中說明：

1. 取得 Directory Server 的憑證及安裝，並配置 Directory Server 以信任該憑證授權單位的憑證。此程序包括：
    a. 依需要建立憑證資料庫。

b. 從您的伺服器產生憑證要求，並傳送給即將爲您的伺服器提供憑證的憑證授權單位。

c. 在伺服器中安裝新的憑證。

d. 信任您的憑證授權單位及它發行的所有憑證。

2. 在您的目錄中啓動與配置 SSL，包括 LDAP 與 DSML 作業的安全連接埠。您也可以將 Directory Server Console 配置爲使用 SSL 來存取伺服器。

3. 或者，將伺服器配置爲使用下列一或多種用戶端驗證機制：

a. 以憑證爲基礎的預設驗證。

b. 透過 SASL 的 DIGEST_MD5 驗證機制。

c. 透過 SASL 的 GSSAPI 驗證，它可允許使用 Kerberos V5 安全機制。

4. 將您的用戶端配置爲在與 Directory Server 通訊時使用 SSL，包括您要用的任何選用驗證機制。

上述步驟中，有些可以用 `certutil` 工具執行，以透過指令行管理憑證。此工具於 `SUNWtlsu` 封裝中提供。

# 取得和安裝伺服器憑證

本節描述建立憑證資料庫、取得和安裝與 Directory Server 一起使用的憑證、以及將 Directory Server 配置成信任憑證授權單位 (CA) 憑證的程序。

## 建立憑證資料庫

初次在伺服器上配置 SSL 時，您必須爲安全裝置設定密碼。如果不使用外部的硬體安全裝置，則內部安全裝置是儲存在下列檔案中的憑證與金鑰資料庫：

*ServerRoot*`/alias/slapd-`*serverID*`-cert8.db`
*ServerRoot*`/alias/slapd-`*serverID*`-key3.db`

如果您的 *serverID* 包含大寫字母，您必須用以下指令行程序建立憑證資料庫。

### 使用主控台

使用主控台時，伺服器將在您第一次啓動 [ 憑證管理員 ] 對話方塊時自動建立憑證資料庫檔案：

1. 在 Directory Server Console 最上層的 [ 工作 ] 標籤上，按一下 [ 管理憑證 ] 按鈕；或者，在已顯示 [ 工作 ] 標籤時，從 [ 主控台 ] > [ 安全性 ] 功能表中選擇 [ 管理憑證 ] 項目。
2. 伺服器將自動建立憑證與金鑰資料庫，並要求您爲安全裝置設定密碼。這個密碼會保護憑證儲存在伺服器中的私密金鑰。請輸入兩次密碼以進行確認，再按一下 [ 確定 ]。

### 使用指令行

從指令行建立憑證資料庫檔案時，您必須使用以下程序中所示的路徑與檔案名稱字首，讓伺服器可以找得到它們。

1. 在伺服器主機電腦上，用下列指令建立憑證資料庫：

   `certutil -N -d` *`ServerRoot`*`/alias -P slapd-`*`LCserverID`*

   其中 *LCserverID* 是您的伺服器全部小寫的伺服器名稱。

   工具將提示您輸入密碼，以保護憑證的金鑰。

## 產生憑證要求

使用下列程序之一產生 PEM 格式的 PKCS #10 憑證要求。PEM 是 RFC 1421 到 1424 (`http://www.ietf.org/rfc/rfc1421.txt`) 所指定的 Privacy Enhanced Mail 格式，並用來代表 US-ASCII 字元的 base64 編碼憑證要求。要求的內容將類似下列範例：

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBrjCCARcCAQAwbjELMAkGA1UBhMCVXMxEzARBgNVBAgTCkNBElGT1JOSUExLD
AqBgVBAoTI25ldHNjYXBlIGNvb11bmljYXRpb25zIGNvcnBvcmF0aWuMRwwGgYDV
QQDExNtZWxsb24umV0c2NhcGUuY29tMIGfMA0GCSqGSIb3DQEBAUAA4GNADCBiQK
BgCwAbskGh6SKYOgHy+UCSLnm3ok3X3u83Us7u0EfgSLR0f+K41eNqqWRftGR83e
mqPLDOf0ZLTLjVGJaHJn4l1gG+JDf/n/zMyahxtV7+T8GOFFigFfuxJaxMjr2j7I
vELlxQ4IfZgwqCm4qQecv3G+N9YdbjveMVXW0v4XwIDAQABAAwDQYJKoZIhvcNAQ
EEBQADgYEAZyZAm8UmP9PQYwNy4Pmypk79t2nvzKbwKVb97G+MT/gw1pLRsuBoKi
nMfLgKp1Q38K5Py2VGW1E47/rhm3yVQrIiwV+Z8Lcc=
-----END NEW CERTIFICATE REQUEST-----
```

### 使用主控台

1. 在 Directory Server Console 最上層的 [ 工作 ] 標籤上，按一下 [ 管理憑證 ] 按鈕；或者，在已顯示 [ 工作 ] 標籤時，從 [ 主控台 ] > [ 安全性 ] 功能表中選擇 [ 管理憑證 ] 項目。

   顯示 [ 管理憑證 ] 對話方塊。

2. 選擇 [ 伺服器憑證 ] 標籤，並按一下 [ 要求 ] 按鈕。

   顯示 [ 憑證要求精靈 ]。

3. 如果您已安裝可讓伺服器直接與 CA 通訊的 Plug-in，現在可以選取該 Plug-in ；否則，您必須經由電子郵件或網站傳送產生的要求，以手動要求憑證。按一下 [ 下一步 ] 繼續。

4. 在空白文字欄位中輸入「要求者資訊」：

   **伺服器名稱。**輸入 Directory Server 的完全合格主機名稱，例如 `east.example.com`，此名稱與 DNS 查詢中所使用的名稱相同。

   **組織。**輸入您公司或機構的正式名稱。大部分的 CA 會要求您提供正式文件以驗證這項資訊，例如公司執照的複本。

   **組織單位。**( 選用 )。輸入您的部門或業務單位在公司內的描述性名稱。

   **位置。**( 選用 )。輸入您公司所在的城市名稱。

   **州或省。**輸入您公司所在州或省的完整名稱，不可用縮寫。

   **國家。**選擇代表您國家名稱的兩個字元縮寫 ( 採用 ISO 格式 )。美國的國碼爲 US。《Directory Server Administration Reference》中的 Chapter 5 "Directory Internationalization Reference" 中包含 ISO 國碼清單。

   按一下 [ 下一步 ] 繼續。

5. 輸入安全裝置的密碼，再按一下 [ 下一步 ]。此密碼於第 343 頁「建立憑證資料庫」中設定。

6. 選擇 [ 複製至剪貼簿 ] 或 [ 儲存至檔案 ]，以儲存您必須傳送到憑證授權單位的憑證要求資訊。

7. 按一下 [ 完成 ] 退出 [ 憑證要求精靈 ]。

## 使用指令行

1. 用下列指令建立伺服器的憑證要求：

   ```
   certutil -R \
   -s "cn=serverName,ou=division,o=company,l=city,st=state,c=country" \
   -a -d ServerRoot/alias -P slapd-serverID-
   ```

   `-s` 選項指定要求的伺服器憑證的 DN。憑證授權單位通常需要此範例中顯示的所有屬性，才能完整識別伺服器。如需每個屬性的描述，請參閱 步驟 4。

2. `certutil` 工具將提示您輸入伺服器金鑰資料庫的密碼。此密碼於第 343 頁「建立憑證資料庫」中設定。然後工具將產生 PEM 編碼文字格式的 PKCS #10 憑證要求。

# 安裝伺服器憑證

依憑證授權單位指定的程序，將上一節產生的要求傳給憑證授權單位。例如，您可能須以電子郵件傳送憑證要求，或者您可以透過 CA 的網站輸入要求。

一旦傳送要求後，您必須等待 CA 回應憑證，等待回應的時間長短不同。例如，如果您的 CA 在您公司內部，則回應您的要求只需一或兩天的時間。如果您選取的 CA 在公司外部，則可能需要花幾個星期的時間來回應您的要求。

當 CA 傳送回應後，請確定將資訊存成文字檔案，PEM 格式的 PKCS #11 憑證將類似下列範例。

```
-----BEGIN CERTIFICATE-----
MIICjCCAZugAwIBAgICCEEwDQYJKoZIhKqvcNAQFBQAwfDELMAkGA1UEBhMCVVMx
IzAhBgNVBAoGlBhbG9a2FWaWxsZGwSBXaWRnZXRzLCBJbmMuMR0wGwYDVQQLExRX
aWRnZXQgTW3FrZXJzICdSJyBVczEpMCcGAx1UEAxgVGVzdCBUXN0IFRlc3QgVGVz
dCBUZXN0IFlc3QgQ0EswHhcNOTgwMzEyMDIzMzUWhcNOTgwMzI2MDIzMpzU3WjBP
MQswCYDDVQQGEwJVUzEoMCYGA1UEChMfTmV0c2NhcGUgRGlyZN0b3J5VIFB1Ymxp
Y2F0aW9uczEWMB4QGA1UEAxMNZHVgh49dq2tLNvbjTBaMA0GCSqGSIb3DQEBAQUA
A0kAMEYkCQCksMR/aLGdfp4m0OiGgijG5KgOsyRNvwGYW7kfW+8mmijDtZaRjYNj
jcgpF3Vnlbxbc1X9LVjjNLC5737XZdAgEDozYwpNDARBglghkgBhvhCEAQEEBAMC
APAwHkwYDVR0jBBgwFAU67URjwCaGqZHUpSpdLxlzwJKiMwDQYJKoZIhQvcNAQEF
BQADgYEAJ+BfVem3vBOPBveNdLGfjlb9hucgmaMcQa9FA/db8qimKT/ue9UGOJqL
bwbMKBBopsDn56p2yV3PLIsBgrcuSoBCuFFnxBnqSiTS7YiYgCWqWaUA0ExJFmD6
6hBLseqkSWulk+hXHN7L/NrViO+7zNtKcaZLlFPf7d7j2MgX4Bo=
-----END CERTIFICATE-----
```

您也應該將憑證資料備份到安全的位置。萬一您的系統遺失了憑證資料，您便可以使用備份檔案重新安裝憑證。

一旦取得伺服器憑證後，您便可以準備將它安裝到伺服器的憑證資料庫中。

## 使用主控台

1. 在 Directory Server Console 最上層的 [ 工作 ] 標籤上，按一下 [ 管理憑證 ] 按鈕；或者，在已顯示 [ 工作 ] 標籤時，從 [ 主控台 ] > [ 安全性 ] 功能表中選擇 [ 管理憑證 ] 項目。

   顯示 [ 管理憑證 ] 視窗。

2. 選擇 [ 伺服器憑證 ] 標籤，並按一下 [ 安裝 ]。

   顯示 [ 憑證安裝精靈 ]。

3. 選擇以下選項之一，做爲憑證位置：

   **在這個檔案中。**在這個欄位中輸入憑證的絕對路徑。

**在下列編碼文字區塊內。**複製來自憑證授權單位或您所建立文字檔案中的文字，並將它貼到這個欄位中。例如：

按一下 [ 下一步 ] 繼續。

4. 確認顯示的憑證資訊是否正確，再按一下 [ 下一步 ]。
5. 指定憑證名稱，再按一下 [ 下一步 ]。此名稱將出現在憑證表中。
6. 輸入保護私密金鑰的密碼以確認憑證。此密碼與您在第 343 頁「建立憑證資料庫」的 步驟 2 中輸入的密碼相同。完成時按一下 [ 完成 ]。

新的憑證出現在 [ 伺服器憑證 ] 標籤的清單中。伺服器現在已經準備好啓用 SSL。

### 使用指令行

1. 用下列指令在您的憑證資料庫中安裝新的伺服器憑證：

```
certutil -A -n "certificateName" -t "u,," -a -i certFile \
         -d ServerRoot/alias -P slapd-serverID-
```

其中 *certificateName* 是您爲憑證指定的識別名稱，*certFile* 是文字檔，內含 PEM 格式的 PKCS #11 憑證。`-t "u,,"` 選項指示這是 SSL 通訊所用的伺服器憑證。

2. 或者，您也可以用下列 `certutil` 指令確認您安裝的憑證：

```
certutil -L -d ServerRoot/alias -P slapd-serverID-
```

列出的憑證中，包含 `u,,` 者爲伺服器憑證。

## 信任憑證授權單位

將 Directory Server 配置成信任憑證授權單位的作業包括取得憑證，以及將憑證安裝到伺服器的憑證資料庫中。此程序會因您使用的憑證授權單位不同而有差異。有些商業 CA 會提供網站讓您自動下載憑證，其他的則會依要求以電子郵件將憑證寄給您。

### 使用主控台

一旦取得 CA 憑證後，您便可以使用 [ 憑證安裝精靈 ] 配置 Directory Server，使其信任憑證授權單位。

1. 在 Directory Server Console 最上層的 [ 工作 ] 標籤上，按一下 [ 管理憑證 ] 按鈕；或者，在已顯示 [ 工作 ] 標籤時，從 [ 主控台 ] > [ 安全性 ] 功能表中選擇 [ 管理憑證 ] 項目。

顯示 [ 管理憑證 ] 視窗。

2. 選取 [CA 憑證 ] 標籤，並按一下 [ 安裝 ]。

   顯示 [ 憑證安裝精靈 ]。

3. 如果您將 CA 的憑證儲存到檔案中，請在提供的欄位中輸入檔案的路徑。如果您是透過電子郵件收到 CA 的憑證，請複製憑證 ( 包括標頭 ) 並將它貼到所提供的文字欄位中。按一下 [ 下一步 ]。

4. 確認顯示的憑證資訊對您的憑證授權單位而言是否正確，再按一下 [ 下一步 ]。

5. 指定憑證名稱，再按一下 [ 下一步 ]。

6. 選擇信任此 CA 的目的。您可以選擇其中之一，或兩者皆選：

   **接受來自用戶端的連線 ( 用戶端驗證 )。**如果您的 LDAP 用戶端會提出此 CA 所發行的憑證來執行以憑證爲基礎的用戶端驗證，選擇此核取方塊。

   **接受來自其他伺服器的連線 ( 伺服器驗證 )。**如果您的伺服器將與另一部伺服器透過 SSL 扮演複製供應商或鏈接多工器角色，而且該伺服器也擁有此 CA 所發行的憑證，選擇此核取方塊。

7. 按一下 [ 完成 ] 退出精靈。

## 使用指令行

1. 您也可以用下列指令安裝受信任的 CA 憑證：

   ```
   certutil -A -n "CAcertificateName" -t "trust,," -a -i certFile \
            -d ServerRoot/alias -P slapd-serverID-
   ```

   其中 *CAcertificateName* 是您爲受信任的 CA 指定的識別名稱，*certFile* 是文字檔，內含 PEM 編碼文字格式的 CA PKCS #11 憑證，而 *trust* 是下列代碼之一：

   - `T` — 信任此 CA 所發行的用戶端憑證。如果您的 LDAP 用戶端會提出此 CA 所發行的憑證來執行以憑證爲基礎的用戶端驗證，使用此代碼。
   - `C` — 信任此 CA 所發行的伺服器憑證。如果您的伺服器將與另一部伺服器透過 SSL 扮演複製供應商或鏈接多工器角色，而且該伺服器也擁有此 CA 所發行的憑證，使用此代碼。
   - `CT` — 信任此 CA 所發行的用戶端與伺服器憑證。如果上述兩種狀況都適用於此 CA，使用此代碼。

2. 或者，您也可以用下列 `certutil` 指令確認您安裝的憑證：

   ```
   certutil -L -d ServerRoot/alias -P slapd-serverID
   ```

   列出的憑證中，包含 `u,,` 者爲伺服器憑證，而包含 `CT,,` 者爲受信任的 CA 憑證。

# 啓用 SSL

一旦安裝好伺服器憑證並信任 CA 的憑證後，便可以準備啓用 SSL。大部分的時候，您希望在啓用 SSL 的情形下執行伺服器。如果您暫時停用了 SSL，在處理需要機密性、驗證或資料完整性的作業之前，請先確定已重新啓用 SSL。

必須先建立憑證資料庫、取得和安裝伺服器憑證，並信任 CA 的憑證之後，才能啓用 SSL，如第 343 頁「取得和安裝伺服器憑證」中所述。

接著，下列程序將啓動 SSL 通訊，並啓用目錄伺服器的加密機制：

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，選擇有伺服器名稱的根節點，然後選擇右面板中的 [ 加密 ] 標籤。

   標籤中會顯示目前伺服器的加密設定值。

2. 選擇 [ 啓用這台伺服器的 SSL] 核取方塊表示要啓用加密。

3. 核取 [ 使用此加密家族 ] 核取方塊

4. 從下拉式功能表中選擇您要使用的憑證。

5. 按一下 [ 加密設定值 ]，並在 [ 加密喜好設定 ] 對話方塊中選擇要使用的加密。如需關於特定加密的詳細資訊，請參閱第 350 頁「選擇 Encryption Cipher」。

6. 設定用戶端驗證的喜好設定：

   **不允許用戶端驗證。**使用這個選項時，伺服器將忽略用戶端憑證，而且將拒絕依此爲基礎的驗證。

   **允許用戶端驗證。**這是預設值。使用這個選項時，驗證是在用戶端要求時才執行。如需關於以憑證爲基礎之驗證的詳細資訊，請參閱第 352 頁「配置用戶端驗證」。

| **備註** | 如果您使用以憑證爲基礎並具有複製的驗證，則必須配置取用者端伺服器允許或要求用戶端驗證。 |
|---|---|

   **要求用戶端驗證。**使用這個選項時，如果用戶端不回應伺服器的驗證要求，用戶端連線將被拒絕。

| **備註** | 如果 Server Console 透過 SSL 連線到 Directory Server，則選擇 [ 要求用戶端驗證 ] 將停用通訊，因爲 Server Console 沒有用戶端驗證所需的憑證。若要從指令行修改此屬性，請參閱第 352 頁「允許用戶端驗證」。 |
|---|---|

7. 或者，如果希望主控台與 Directory Server 通訊時使用 SSL，請選擇 [ 在 Server Console 中使用 SSL]。
8. 完成時按一下 [ 儲存 ]。
9. 或者，設定伺服器在 LDAP 與 DSML-over-HTTP 通訊協定中進行 SSL 通訊時所要用的安全連接埠。如需資訊，請參閱第 35 頁「變更目錄伺服器連接埠號碼」。

   所有與安全連接埠的連線都必須使用 SSL。不論是否配置安全連接埠，一旦啓動 SSL，用戶端就可以使用 Start TLS 作業透過非安全連接埠執行 SSL 加密。
10. 重新啓動 Directory Server。

    如需更多資訊，請參閱第 24 頁「啓動啓用 SSL 的伺服器」。

# 選擇 Encryption Cipher

*加密 (cipher)* 是用來加密與解密資料的演算法。一般而言，加密過程中使用的位元越多，表示該加密*更強大*或更安全。SSL 的加密也由使用的訊息驗證類型識別。訊息驗證是另一個演算法，它會計算保證資料完整性的總和檢查碼。如需更多關於演算法及其強度的完整討論，請參閱 《Administration Server Administration Guide》 Appendix B 中的 "Ciphers Used With SSL"。

當用戶端啓動與伺服器的 SSL 連線時，用戶端與伺服器雙方必須同意用於加密資訊的加密方式。在任何雙向加密處理中，雙方必須使用相同的加密，通常是用雙方同時支援的最強加密方式。

Directory Server 爲 SSL 3.0 與 TLS 提供下列加密：

**表 11-1** 目錄伺服器提供的密碼

| 加密名稱 | 描述 |
|---|---|
| 無 | 未加密，只進行 MD5 訊息驗證 (rsa_null_md5)。 |
| RC4 (128 位元 ) | 具有 128 位元加密和 MD5 訊息驗證的 RC4 加密 (rsa_rc4_128_md5)。 |
| RC4 ( 匯出 ) | 具有 40 位元加密和 MD5 訊息驗證的 RC4 加密 (rsa_rc4_40_md5)。 |
| RC2 ( 匯出 ) | 具有 40 位元加密和 MD5 訊息驗證的 RC2 加密 (rsa_rc2_40_md5)。 |
| DES 或 DES ( 匯出 ) | 具有 56 位元加密和 SHA 訊息驗證的 DES (rsa_des_sha)。 |
| DES (FIPS) | 具有 56 位元加密和 SHA 訊息驗證的 FIPS DES。此加密符合 FIPS 140-1 美國政府密碼模組執行標準 (rsa_fips_des_sha)。 |

**表 11-1** 目錄伺服器提供的密碼 *( 續 )*

| 加密名稱 | 描述 |
|---|---|
| 三重 DES | 具有 168 位元加密和 SHA 訊息驗證的三重 DES (rsa_3des_sha)。 |
| 三重 DES (FIPS) | 具有 168 位元加密和 SHA 訊息驗證的 FIPS 三重 DES。此加密符合 FIPS 140-1 美國政府密碼模組執行標準 (rsa_fips_3des_sha)。 |
| Fortezza | 具有 80 位元加密和 SHA 訊息驗證的 Fortezza 加密。 |
| RC4 (Fortezza) | 具有 128 位元加密和 SHA 訊息驗證的 Fortezza RC4 加密 |
| 無 (Fortezza) | 未加密，只進行 Fortezza SHA 訊息驗證。 |

爲了繼續使用具有 SSL 的 Server Console，您必須至少選擇下列其中一個加密：

- 具有 40 位元加密和 MD5 訊息驗證的 RC4 加密。
- 未加密，只進行 MD5 訊息驗證 ( 不建議使用 )。
- 具有 56 位元加密和 SHA 訊息驗證的 DES。
- 具有 128 位元加密和 MD5 訊息驗證的 RC4 加密。
- 具有 168 位元加密和 SHA 訊息驗證的三重 DES。

使用以下程序可選擇伺服器要用的加密方式：

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，選擇有伺服器名稱的根節點，然後選擇右面板中的 [ 加密 ] 標籤。

   標籤中會顯示目前伺服器的加密設定值。務必確認伺服器的 SSL 已啓用，如第 349 頁「啓用 SSL」所述。

2. 按一下 [ 加密設定值 ]。

   顯示 [ 加密喜好設定 ] 對話方塊。

3. 在 [ 加密喜好設定 ] 對話方塊中，選擇或取消選取加密旁的核取方塊，以指定您希望伺服器使用的加密。

   除非您因安全性的理由而不使用特定加密，否則您應該選擇所有加密，除 `none,MD5` 之外。

**小心** 應避免選擇沒有加密或只有 MD5 的訊息驗證，因爲如果用戶端沒有其他加密可用，伺服器將使用此選項。在這種情況中，連線會因爲沒有使用加密而變得不安全。

4. 在[加密喜好設定]對話方塊中按一下[確定]，然後在[加密]標籤中按一下[儲存]。

## 允許用戶端驗證

如果 Directory Server 已設爲*需要*用戶端驗證和 Server Console 才能使用 SSL 進行連線，您將不再能夠使用 Server Console 管理任何 Sun Java System 伺服器。您必須改用適當的指令行公用程式。

但是如果希望變更目錄組態，讓您能夠使用 Server Console，您必須依照以下步驟執行，從*需要*改爲*允許*用戶端驗證：

1. 用下列指令修改 `cn=encryption,cn=config` 項目：

   ```
   ldapmodify -h host -p port -D "cn=Directory Manager" -w password
   dn:cn=encryption,cn=config
   changetype:modify
   replace:nsSSLClientAuth
   nsSSLClientAuth:allowed
   ^D
   ```

2. 依第 23 頁「從指令行啓動和停止伺服器」所述重新啓動 Directory Server。

   現在您可以啓動 Server Console。

# 配置用戶端驗證

用戶端驗證是讓伺服器確認用戶端身份的機制。用戶端驗證可以藉由用戶端提出的憑證，或透過以 SASL 爲基礎的機制 ( 如 DIGEST-MD5) 來進行 ( 提供 dn 和密碼 )。在 Solaris 作業系統上，Directory Server 現在支援透過 SASL 的 GSSAPI 機制，以允許用戶端透過 Kerberos V5 進行驗證。

以憑證爲基礎的驗證使用透過 SSL 通訊協定所取得的用戶端憑證，以找出使用者項目的識別資料。此機制也稱爲 `EXTERNAL`，因爲它依賴已在較低層建立的驗證機制。( 外部驗證在未來版本中可以配合 IP 安全通訊協定 (ipsec) 使用。)。

以憑證爲基礎的驗證詳細說明於《Administration Server Administration Guide》Chapter 9 的 "Using Client Authentication" 中。

下列各節描述在 Directory Server 上配置兩種 SASL 機制的方式。請參閱第 360 頁「將 LDAP 用戶端配置爲使用安全性」。

# 透過 DIGEST-MD5 的 SASL 驗證

DIGEST-MD5 機制會將用戶端所傳送的一個雜湊值比較使用者密碼的雜湊值來決定用戶端是否通過驗證。然而，因爲此機制必須讀取使用者密碼，所以凡是希望透過 DIGEST-MD5 通過驗證的使用者都必須擁有目錄中的 {CLEAR} 密碼。在目錄中儲存 {CLEAR} 密碼時，您必須確定已透過 ACI 適當限制存取密碼值，如第 6 章「管理存取控制」所述。您可能希望如第 74 頁「加密屬性值」所述在該尾碼中配置屬性加密，以進一步保護 {CLEAR} 密碼。

## 配置 DIGEST-MD5 機制

下列程序描述將 Directory Server 配置爲使用 DIGEST-MD5 所需的步驟：

1. 使用主控台或 `ldapsearch` 指令，確認 `DIGEST-MD5` 是根項目上 `supportedSASLMechanisms` 屬性的值。例如，下列指令將顯示已啓用的 SASL 機制：

   ```
   ldapsearch -h host -p port -D "cn=Directory Manager" -w password \
   -s base -b "" "(objectclass=*)" supportedSASLMechanisms

   dn:
   supportedSASLMechanisms:EXTERNAL
   supportedSASLMechanisms:DIGEST-MD5
   supportedSASLMechanisms:GSSAPI
   ^D
   ```

2. 如果未啓用 DIGEST-MD5，請使用下列 `ldapmodify` 指令將它啓用：

   ```
   ldapmodify -h host -p port -D "cn=Directory Manager" -w password
   dn:cn=SASL, cn=security, cn=config
   changetype:modify
   add:dsSaslPluginsEnable
   dsSaslPluginsEnable:DIGEST-MD5
   -
   replace:dsSaslPluginsPath
   dsSaslPluginsPath:ServerRoot/lib/sasl
   ^D
   ```

3. 使用 DIGEST-MD5 的預設識別對映，或依第 354 頁「DIGEST-MD5 識別對映」所述建立新的識別對映。

4. 確定已爲即將透過 SSL 使用 DIGEST-MD5 存取伺服器的所有使用者在 {CLEAR} 中儲存密碼。如需配置密碼儲存結構的說明，請參閱第 7 章「管理使用者帳戶和密碼」。

5. 如果修改了 SASL 組態項目或 DIGEST-MD5 識別對映項目之一，請重新啓動目錄伺服器。

## DIGEST-MD5 識別對映

SASL 機制的識別對映會嘗試將 SASL 識別的憑證對映目錄中的使用者項目。如需此機制的完整描述，請參閱第 358 頁「識別對映」。如果對映找不到與 SASL 識別相對的 DN，驗證將會失敗。

SASL 識別是稱爲 *Principal* 的字串，以每種機制特定的格式代表某使用者。在 DIGEST-MD5 中，用戶端所建立的 Principal 應該包含一個 `dn:` 字首及一個 LDAP DN，或是一個 `u:` 字首其後跟著由用戶端決定的任何文字。在對映期間，由用戶端傳送的 Principal 可在 `${Principal}` 預留位置中取得。

DIGEST-MD5 的預設識別對映是由伺服器組態中的下列項目提供：

```
dn:cn=default,cn=DIGEST-MD5,cn=identity mapping,cn=config
objectClass:top
objectClass:nsContainer
objectClass:dsIdentityMapping
objectClass:dsPatternMatching
cn:default
dsMatching-pattern:${Principal}
dsMatching-regexp:dn:(.*)
dsMappedDN: $1
```

此識別對映假設 Principal 的 `dn` 欄位包含目錄中現有使用者正確的 DN。

若要定義您自己的 DIGEST-MD5 識別對映：

1. 編輯預設識別對映，或在 `cn=DIGEST-MD5,cn=identity mapping,cn=config` 下建立新的識別對映。如需識別對映項目中各屬性的定義，請參閱第 358 頁「識別對映」。下列檔案中有一個 DIGEST-MD5 的對映範例：

   *ServerRoot*`/slapd-`*serverID*`/ldif/identityMapping_Examples.ldif`

   此範例假設 Principal 的不合格文字欄位包含所需識別的使用者名稱。下列指令顯示此對映的定義方式：

   ```
   ldapmodify -a -h host -p port -D "cn=Directory Manager" -w password
   dn:cn=unqualified-username,cn=DIGEST-MD5,cn=identity mapping,
    cn=config
   objectclass:dsIdentityMapping
   objectclass:dsPatternMatching
   objectclass:nsContainer
   objectclass:top
   cn:unqualified-username
   ```

```
dsMatching-pattern:${Principal}
dsMatching-regexp:u:(.*)@(.*)\.com
dsSearchBaseDN:dc=$2
dsSearchFilter:(uid=$1)
```

2. 新對映生效前須重新啓動 Directory Server。

# 透過 GSSAPI 的 SASL 驗證 (僅限於 Solaris)

透過 SASL 的 Generic Security Services API (GSSAPI) 可讓您使用如 Kerberos V5 一類協力廠商的安全性系統對用戶端進行驗證。只有 Solaris 平台提供 GSSAPI 程式庫。Sun 建議您在 Sun Enterprise Authentication Mechanism (SEAM) 1.0.1 伺服器上安裝 Kerberos V5 執行。

伺服器使用此 API 驗證使用者的身份。然後，SASL 機制會套用 GSSAPI 對映規則以取得 DN，做爲連線期間所有作業的連結 DN。

## 配置 Kerberos 系統

根據製造廠商的指示設定 Kerberos 軟體。如果使用 SEAM 1.0.1 伺服器，這包括下列步驟：

1. 設定 `/etc/krb5` 中的檔案。
2. 建立 Kerberos 資料庫以儲存使用者與服務，並在此資料庫中建立 LDAP 服務的 principal。LDAP 服務 principal 是：

   `ldap/`*`serverFQDN@REALM`*

   其中 *serverFQDN* 是您伺服器的完全合格網域名稱。
3. 建立金鑰標籤以儲存服務金鑰，包括 LDAP 服務的金鑰。
4. 啓動 Kerberos 常駐程式處理。

如需以上每一步驟的詳細指示，請參閱軟體說明文件。

## 設定 GSSAPI 機制

下列程序描述在 Solaris 平台上設定 Directory Server 以使用 GSSAPI 的所需步驟：

1. 使用主控台或 `ldapsearch` 指令，確認 `GSSAPI` 是根項目上 `supportedSASLMechanisms` 屬性的值。例如，下列指令將顯示已啓用的 SASL 機制：

   ```
   ldapsearch -h host -p port -D "cn=Directory Manager" -w password \
   -s base -b "" "(objectclass=*)" supportedSASLMechanisms
   ```

```
dn:
supportedSASLMechanisms:EXTERNAL
supportedSASLMechanisms:DIGEST-MD5
```

2. 預設狀況下不啓用 GSSAPI，您可以用下列 `ldapmodify` 指令將它啓用：

```
ldapmodify -h host -p port -D "cn=Directory Manager" -w password
dn:cn=SASL, cn=security, cn=config
changetype:modify
add:dsSaslPluginsEnable
dsSaslPluginsEnable:GSSAPI
-
replace:dsSaslPluginsPath
dsSaslPluginsPath:ServerRoot/lib/sasl
```

3. 依第 356 頁「GSSAPI 識別對映」所述建立 GSSAPI 的預設識別對映，以及任何自訂對映。

4. 在伺服器主機電腦上爲伺服器設定 Kerberos：

   a. 在 Kerberos 中建立下列包含工作階段金鑰的 LDAP 服務 principal：`ldap/`*`serverHostname@Realm`*，其中：

   - *serverHostname* 是伺服器主機電腦的完全合格網域名稱。此數值*必須*與 `cn=config` 中的 `nsslapd-localhost` 屬性值相同，只不過它*必須*爲全部小寫。
   - *Realm* 是您伺服器的 Kerberos 範圍。

   b. LDAP 服務必須對下列檔案中的金鑰資料庫擁有讀取存取權：`/etc/krbs/krb5.keytab`。

   c. 主機電腦上必須已設定 DNS。

5. 如果修改了 SASL 組態項目或 GSSAPI 識別對映項目之一，請重新啓動目錄伺服器。

## GSSAPI 識別對映

SASL 機制的識別對映會嘗試將 SASL 識別的憑證對應目錄中的使用者項目。如需此機制的完整描述，請參閱第 358 頁「識別對映」。如果對映找不到與 SASL 識別相對的 DN，驗證將會失敗。

SASL 識別是稱爲 *Principal* 的字串，以每種機制特定的格式代表某使用者。在使用 GSSAPI 的 Kerberos 中，Principal 識別的格式爲 *uid*`[/`*instance*`][@`*realm*`]`，其中 *uid* 可包含選用的 *instance* 識別碼，其後跟著選用的 *realm*，這通常是網域名稱。例如，以下爲有效的使用者 Principal：

```
bjensen
bjensen/Sales
bjensen@EXAMPLE.COM
bjensen/Sales@EXAMPLE.COM
```

一開始，目錄中不會定義任何 GSSAPI 對映。請依據您的用戶端定義所用 Principal 的方式，定義預設對映與任何需要的自訂對映。

若要定義 GSSAPI 的識別對映：

1. 在 `cn=GSSAPI,cn=identity mapping, cn=config` 下建立新的對映項目。如需識別對映項目中各屬性的定義，請參閱第 358 頁「識別對映」。

   GSSAPI 對映的範例位於下列檔案中：

   *ServerRoot*`/slapd-`*serverID*`/ldif/identityMapping_Examples.ldif`

   這個檔案中建議的預設 GSSAPI 對映假設 Principal 只包含使用者 ID，而這會將使用者限定在目錄的固定分支中：

   ```
   dn:cn=default,cn=GSSAPI,cn=identity mapping,cn=config
   objectclass:dsIdentityMapping
   objectclass:nsContainer
   objectclass:top
   cn:default
   dsMappedDN:uid=${Principal},ou=people,dc=example,dc=com
   ```

   這個檔案中的另一個範例顯示當使用者 ID 包含於內含已知範圍的 Principal 內時，要如何決定使用者 ID。

   ```
   dn:cn=same_realm,cn=GSSAPI,cn=identity mapping,cn=config
   objectclass:dsIdentityMapping
   objectclass:dsPatternMatching
   objectclass:nsContainer
   objectclass:top
   cn:same_realm
   dsMatching-pattern:${Principal}
   dsMatching-regexp:(.*)@example.com
   dsMappedDN:uid=$1,ou=people,dc=example,dc=com
   ```

2. 新對映生效前須重新啓動 Directory Server。

# 識別對映

Directory Server 中的數個驗證機制都需要將另一種通訊協定的憑證對映到目錄中的 DN。目前有這種狀況的包括 DSML-over-HTTP 通訊協定，以及 DIGEST-MD5 和 GSSAPI SASL 機制。這些機制都使用識別對映以根據用戶端所提供的通訊協定特定憑證決定連結 DN。

識別對映使用 `cn=identity mapping, cn=config` 組態分支中的項目。所有必須執行識別對映的通訊協定在此分支內各有一個容器：

- `cn=HTTP-BASIC, cn=identity mapping, cn=config` — 包含 DSML-over-HTTP 連線的對映。
- `cn=DIGEST-MD5, cn=identity mapping, cn=config` — 包含使用 DIGEST-MD5 SASL 機制的用戶端驗證的對映。
- `cn=GSSAPI, cn=identity mapping, cn=config` — 必須建立，包含使用 GSSAPI SASL 機制的用戶端驗證的對映。

對映項目定義從通訊協定特定的憑證中擷取元素的方法，以便用這些元素在目錄中搜尋。如果該搜尋傳回一個使用者項目，表示對映成功，連線將使用此項目做爲所有作業的連結 DN。如果搜尋傳回零個或多個項目，則對映失敗，將套用其他任何對映。

每個分支應包含該通訊協定的預設對映，以及任何數目的自訂對映。預設對映的 RDN 爲 `cn=default`，而自訂對映可擁有任何其他 RDN，只要使用 `cn` 做爲命名屬性。所有自訂對映都會依非決定性順序優先評估，直到成功爲止。如果所有自訂對映都失敗，最後才套用預設對映。如果預設對映也失敗，則用戶端的驗證失敗。

對映項目必須包含 `top`、`Container` 與 `dsIdentityMapping` 物件類別。然後項目可包含下列屬性：

- `dsMappedDN:`*DN* — 爲文字字串，定義目錄中的 DN。執行對映時，如果此 DN 存在，則會用於連結。萬一此 DN 不存在時，您也可以定義下列屬性執行搜尋。
- `dsSearchBaseDN:`*DN* — 搜尋的 Base DN。如果忽略了，則對映會在整個樹狀目錄中搜尋所有的根尾碼。
- `dsSearchScope:base|one|sub` — 搜尋範圍，也許是搜尋基礎本身、基礎下一層的子項、或基礎下的整個樹狀子目錄。忽略此屬性時，對映搜尋的預設範圍爲整個樹狀子目錄。
- `dsSearchFilter:`*filterString* — 篩選字串，用來執行對映搜尋。LDAP 搜尋篩選器定義於 RFC 2254 (`http://www.ietf.org/rfc/rfc2254.txt`) 中。

此外，對映項目也可包含 `dsPatternMatching` 物件類別，以允許使用以下屬性：

- `dsMatching-pattern:`*patternString* — 指定據以執行模式對映的字串。
- `dsMatching-regexp:`*regularExpression* — 指定對模式字串套用的規則運算式。

除了 `dsSearchScope` 之外，上述所有屬性都可包含 `${`*keyword*`}` 格式的保留位置，其中 *keyword* 是通訊協定特定憑證中元素的名稱。對映期間，保留位置將由用戶端所提供的實際元素值取代。

取代所有保留位置後，將會執行已定義的任何模式對應。模式對應將是與規則運算式進行比較。如果規則運算式不符合模式字串，則此對映失敗；如果符合，括弧中規則運算式項目的對應值將可供編號的保留位置使用，以用於其他屬性值中。例如，您可以爲 SASL 定義下列對映：

```
dsMatching-pattern:${Principal}
dsMatching-regexp: (.*)@(.*)\.(.*)
dsMappedDN:uid=$1,ou=people,dc=$2,dc=$3
```

如果用戶端用 `bjensen@example.com` 的 Principal 進行驗證，此對映將定義連結 DN `uid=bjensen,ou=people,dc=example,dc=com`。如果此 DN 存在目錄中，則對映將成功，用戶端將通過驗證，而且在此連線期間執行的所有作業都將使用此連結 DN。

`dsMatching-pattern` 與 `dsMatching-regexp` 的比較是使用 Posix `regexec(3C)` 與 `regcomp(3C)` 函數呼叫。Directory Server 使用延伸規則運算式，而且所有比較會區分大小寫。如需詳細資訊，請參閱這些函數的 `man` 說明頁。

可包含保留位置的屬性值必須將不在保留位置內的任何 `$`、`{` 與 `}` 字元編碼，即使不使用保留位置。您必須以下列值編碼這些字元：`$` 爲 `\24`、`{` 爲 `\7B` 及 `}` 爲 `\7D`。

使用保留位置與替代的方式可讓您建立從通訊協定特定的憑證中擷取使用者名稱或任何其他值的對映，將此值用來定義對映的 DN 或在目錄中的任何位置搜尋對應 DN。您應該定義對映，擷取目錄用戶端提供的預期憑證，再將它們對映到您特定的目錄結構。

**小心** 建立定義不正確的對映將成爲安全上的漏洞。例如，對映中若不使用模式對映，而是對映到固定的 DN，則該對映一定會成功，因此即使非目錄使用者的用戶端一樣會通過驗證。

比較安全的作法是定義數個對映，分別處理不同的用戶端憑證格式，而不要單單建立一個過度通用而且寬鬆的對映。您永遠都要嘗試將用戶端連線根據用戶端的憑證對映到特定使用者。

# 將 LDAP 用戶端配置爲使用安全性

下列各節說明如何在希望與目錄伺服器建立安全連線的 LDAP 用戶端中設定及使用 SSL。在 SSL 連線中，伺服器傳送其憑證到用戶端。用戶端必須先信任伺服器的憑證，使伺服器通過驗證。然後用戶端可以選擇傳送它自己的憑證或兩種 SASL 機制 (DIGEST-MD5 或使用 Kerberos V5 的 GSSAPI) 之一的資訊，以啓動一種用戶端驗證機制。

下列各節使用 `ldapsearch` 工具做爲啓用 SSL 的 LDAP 用戶端的範例。目錄伺服器所提供的 `ldapmodify`、`ldapdelete` 與 `ldapcompare` 工具都以相同的方式設定。這些目錄存取工具是以 Directory SDK for C 爲基礎，詳細文件記錄在 《Directory Server Resource Kit Tools Reference》中。

若要在非 LDAP 用戶端上設定 SSL 連線，請參閱應用程式所提供的說明文件。

**備註** 有些用戶端應用程式執行 SSL，但不確認伺服器是否有受信任的憑證。它們使用 SSL 通訊協定來提供資料加密，但不保證機密性，也無法防止冒充。

## 在用戶端中配置伺服器驗證

當用戶端建立與伺服器的 SSL 連線時，它必須信任伺服器提出的憑證。爲執行此動作，用戶端必須：

- 擁有憑證資料庫。
- 信任發行伺服器憑證的憑證授權單位 (CA)。
- 指定 LDAP 用戶端的 SSL 選項。

Mozilla 就是使用 SSL 透過 HTTP 通訊協定與 Web 伺服器進行通訊的用戶端應用程式。您可以用 Mozilla 管理您的 LDAP 用戶端也將會使用的憑證。或者，您可以用 `certutil` 工具管理憑證資料庫。

### 透過 Mozilla 管理用戶端憑證

下列程序描述如何使用 Mozilla 管理用戶端電腦上的憑證資料庫。

1. Mozilla 一啓動就會確保憑證資料庫已存在，否則它將視需要建立憑證資料庫。憑證資料庫將與其他 Mozilla 喜好設定一起儲存在檔案中，例如 `.mozilla/`*username*`/`*string*`.slt/cert8.db`。

   如果您使用此程序，請找出 Mozilla 所建立的憑證資料庫並記住其路徑，以供您的用戶端應用程式使用。

2. 使用 Mozilla 瀏覽找出爲您要存取的目錄伺服器發行憑證的憑證授權單位網站。Mozilla 將自動擷取憑證授權單位的憑證，並詢問您是否應該信任該憑證。

   例如，如果使用內部部署的 Sun Java System 憑證伺服器，您將移到類似 `https://`*hostname*`:444` 格式的 URL。

3. 當 Mozilla 提示時，信任憑證授權單位的憑證。您應該信任伺服器驗證的 CA 憑證。

   依 CA 網站的不同，可能會無法執行此步驟。如果 Mozilla 不自動提示您信任 CA 憑證，請使用下列程序手動執行。

### 透過指令行管理用戶端憑證

使用 `certutil` 工具透過指令行管理憑證。此工具於 `SUNWtlsu` 封裝中提供。

1. 在用戶端主機電腦上，用下列指令建立憑證資料庫：

   `certutil -N -d` *path* `-P` *prefix*

   工具將提示使用者輸入密碼，以保護憑證。然後工具將建立下列檔案：*path*/*prefix*`cert8.db` and *path*/*prefix*`key3.db`.

   憑證資料庫應由 LDAP 用戶端應用程式的使用者個別建立在只能由該使用者存取的位置，例如使用者主目錄的受保護子目錄。

2. 聯絡爲您要存取的 Directory Server 發行憑證的憑證授權單位，並要求其 CA 憑證。您可以傳送電子郵件或存取網站，以取得 PKCS #11 憑證的 PEM 編碼文字版本。將此憑證儲存在檔案內。

   例如，如果使用內部部署的 Sun Java System 憑證伺服器，您將移到類似 `https://`*hostname*`:444` 格式的 URL。從最上層的 [ 擷取 ] 標籤，選擇 [ 匯入 CA 憑證鏈接 ]，並複製那裏的編碼憑證。

   或者，如果您從同一個 CA 取得您的用戶端與伺服器憑證，您可以重複使用透過第 347 頁「信任憑證授權單位」程序所取得的 CA 憑證。

3. 將 CA 憑證匯入爲受信任的 CA，可以發行 SSL 連線中所用的伺服器憑證。請使用下列指令：

   `certutil -A -n "`*certificateName*`" -t "C,," -a -i` *certFile* `-d` *path* `-P` *prefix*

其中 *certificateName* 是您爲此憑證指定的識別名稱，*certFile* 是文字檔，內含 PEM 編碼文字格式的 CA PKCS #11 憑證，而 *path* 和 *prefix* 與 步驟 1 中相同。

LDAP 用戶端應用程式的每個使用者都必須將 CA 憑證匯入他的憑證資料庫中。所有使用者都可以匯入位在 *certFile* 中的相同憑證。

### 指定伺服器驗證的 SSL 選項

若要用 `ldapsearch` 工具在 SSL 中執行伺服器驗證，使用者只需指定憑證資料庫的路徑。透過安全連接埠建立 SSL 連線時，伺服器將會傳送其憑證。然後 `ldapsearch` 工具將在使用者的憑證資料庫中尋找發行伺服器驗證那個 CA 的信任 CA 憑證。

以下指令顯示使用者如何指定由 Mozilla 建立的憑證資料庫：

```
ldapsearch -h host -p securePort \
           -D "uid=bjensen,dc=example,dc=com" -w bindPassword \
           -Z -P .mozilla/bjensen/string.slt/cert8.db \
           -b "dc=example,dc=com" "(givenname=Richard)"
```

## 在用戶端中配置以憑證爲基礎的驗證

用戶端驗證的預設機制使用憑證以安全地識別目錄伺服器的使用者。爲了執行以憑證爲基礎的用戶端驗證，您必須：

- 爲每個目錄使用者取得憑證，並安裝在用戶端應用程式可存取的位置。
- 用同一憑證的二進位複本配置使用者的目錄項目。驗證過程中，伺服器會將用戶端應用程式提出的憑證，對映此複本，以明確識別使用者。
- 依《Administration Server Administration Guide》 Chapter 9 的 "Using Client Authentication" 所述，爲伺服器配置以憑證爲基礎的驗證。
- 爲以憑證爲基礎的驗證指定 LDAP 用戶端的 SSL 選項。

這些程序需要 `certutil` 工具以透過指令行管理憑證。此工具於 `SUNWtlsu` 封裝中提供。

### 取得與安裝使用者憑證

每個想用以憑證爲基礎的驗證存取目錄的使用者都必須要求並安裝用戶端憑證。此程序假設使用者已依第 360 頁「在用戶端中配置伺服器驗證」所述配置憑證資料庫。

1. 用下列指令建立使用者憑證的要求：

   ```
   certutil -R \
   -s "cn=Babs Jensen,ou=Sales,o=example.com,l=city,st=state,c=country"\
   -a -d path -P prefix
   ```

   `-s` 選項指定要求憑證的 DN。憑證授權單位通常需要此範例中顯示的所有屬性，才能完整識別憑證的擁有者。透過步驟 9 中的憑證對映機制，憑證 DN 將對映到使用者的目錄 DN。

   *path* 與 *prefix* 指出使用者憑證與金鑰資料庫的位置。`certutil` 工具將提示使用者輸入金鑰資料庫的密碼。然後工具會以 PEM 編碼文字格式產生 PKCS #10 憑證要求。

2. 將編碼的憑證要求儲存在檔案內，再依憑證授權單位指定的程序傳送到您的憑證授權單位。例如，您可能須以電子郵件傳送憑證要求，或者您可以透過 CA 的網站輸入要求。

3. 一旦傳送要求後，您必須等待 CA 回應憑證，等待回應的時間長短不同。例如，如果您的 CA 在您公司內部，則回應您的要求只需一或兩天的時間。如果您選取的 CA 在公司外部，則可能需要花幾個星期的時間來回應您的要求。

4. 當 CA 傳送回應後，請將新憑證的 PEM 編碼文字下載或複製到文字檔內。

5. 用下列指令在憑證資料庫中安裝新的使用者憑證：

   ```
   certutil -A -n "certificateName" -t "u,," -a -i certFile -d path -P prefix
   ```

   其中 *certificateName* 是您爲憑證指定的識別名稱，*certFile* 是文字檔，內含 PEM 格式的 PKCS #11 憑證，而 *path* 和 *prefix* 與步驟 1 中相同。

   或者，如果您透過 Mozilla 管理憑證資料庫，您的 CA 網站上可能有連結可直接安裝憑證。請按一下此連結，並依照 Mozilla 提示的對話方塊按步驟進行。

6. 用下列指令建立憑證的二進位複本：

   ```
   certutil -L -n "certificateName" -d path -r > userCert.bin
   ```

   其中 *certificateName* 是您在安裝時爲憑證指定的名稱，*path* 是憑證資料庫的位置，而 *userCert.bin* 是即將包含二進位格式憑證的輸出檔名稱。

7. 在 Directory Server 上，將 `userCertificate` 屬性加入擁有用戶端憑證之使用者的目錄項目。

- 若要透過主控台加入憑證：

  a. 從 Directory Server Console 最上層的 [ 目錄 ] 標籤，找到樹狀目錄中的使用者項目，在其上按一下滑鼠右鍵，並從快顯功能表中選擇 [ 以標準編輯器編輯 ]。

  b. 在「標準編輯器」中，按一下 [ 加入屬性 ]。

c. 從快顯對話方塊中選擇 userCertificate 屬性，從子類型下拉式清單中選擇 binary。您必須指定 binary 子類型，否則憑證對映將會失敗。

d. 在 [ 標準編輯器 ] 中找到新的 userCertificate 欄位。按一下對映的 [ 設定值 ] 按鈕爲此屬性設定二進位值。

e. 在 [ 設定值 ] 對話方塊中輸入在步驟 6 中所建立的 *userCert.bin* 檔案名稱，或按一下 [ 瀏覽 ] 找到檔案。

f. 在 [設定值] 對話方塊中按一下 [確定]，然後在 [標準編輯器] 中按一下 [儲存]。

- 若要從指令行加入憑證，請依下述範例所示使用 ldapmodify 指令。此指令使用 SSL 透過安全連線傳送憑證：

```
ldapmodify -h host -p securePort \
           -D "uid=bjensen,dc=example,dc=com" -w bindPassword \
           -Z -P .mozilla/bjensen/string.slt/cert8.db
version: 1
dn:uid=bjensen,dc=example,dc=com
changetype:modify
add:userCertificate
userCertificate;binary:< file:///path/userCert.bin
```

  您必須將 binary 子類型包含在其中，否則憑證對映將會失敗。在 < 前後的空格是有意義的，必須完全依照顯示方式使用。爲了使用 < 語法指定檔案名稱，LDIF 陳述式的開頭行必須是 version:1。當 ldapmodify 處理此陳述式時，它會將屬性設爲從指定檔案的完整內容讀取而來的值。

8. 在 Directory Server 上，依需要安裝並信任爲您發行使用者憑證那個 CA 的憑證。要接受來自用戶端的連線就必須信任此 CA。請參閱第 347 頁「信任憑證授權單位」。

9. 依《Administration Server Administration Guide》 Chapter 9 的 "Using Client Authentication" 所述，爲 Directory Server 配置以憑證爲基礎的驗證。在此程序中，您將編輯 certmap.conf 檔案，讓伺服器將透過 LDAP 用戶端提出的使用者憑證對映到相對的使用者 DN。

   確定 certmap.conf 檔中的 verifyCert 參數已設定成 on。然後伺服器將確認使用者項目是否包含相同的憑證，因而明確識別使用者。

## 爲以憑證爲基礎的用戶端驗證指定 SSL 選項

若要用 ldapsearch 工具在 SSL 中執行以憑證爲基礎的用戶端驗證，使用者必須指定幾個指令行選項，以使用其憑證。透過安全連接埠建立 SSL 連線時，工具會驗證伺服器的憑證，再將使用者憑證傳給伺服器。

以下指令顯示使用者如何指定選項，以存取由 Mozilla 建立的憑證資料庫：

```
ldapsearch -h host -p securePort \
           -Z -P .mozilla/bjensen/string.slt/cert8.db \
           -N "certificateName" \
           -K .mozilla/bjensen/string.slt/key3.db -W keyPassword \
           -b "dc=example,dc=com" "(givenname=Richard)"
```

`-Z` 選項指示以憑證爲基礎的驗證，*certificateName* 指定要傳送的憑證，而 `-K` 與 `-W` 選項讓用戶端應用程式可以存取憑證以便能夠傳送憑證。若不指定 `-D` 和 `-w` 選項，連結 DN 將由憑證對映來決定。

# 在用戶端中使用 SASL DIGEST-MD5

在用戶端使用 DIGEST-MD5 機制時，您不必安裝使用者憑證。但是如果您希望使用加密的 SSL 連線，您還是必須依第 360 頁「在用戶端中配置伺服器驗證」所述信任伺服器憑證。

## 指定範圍

範圍用於定義可從中選擇驗證識別的名稱空間。在 DIGEST-MD5 驗證中，您必須通過特定範圍的驗證。

Directory Server 使用電腦的完全合格主機名稱做爲 DIGEST-MD5 的預設範圍。伺服器使用存在 `nsslapd-localhost` 組態屬性中的主機名稱的小寫字母值。

如果不指定範圍，將使用伺服器提供的預設範圍。

## 指定環境變數

在 UNIX 環境中，您必須設定 `SASL_PATH` 環境變數，讓 LDAP 工具能夠找到 DIGEST-MD5 程式庫。DIGEST-MD5 程式庫是由 SASL Plug-in 動態載入的共享程式庫，因此您應該依下列方式設定 SASL_PATH 變數 ( 以 Korn shell 爲例 )：

```
export SASL_PATH=ServerRoot/lib/sasl
```

此路徑假設 Directory Server 安裝在即將啓動 LDAP 工具的同一主機上。

## ldapsearch 指令的範例

執行 DIGEST-MD5 用戶端驗證可以不必使用 SSL。以下範例將使用預設 DIGEST-MD5 識別對映來決定連結 DN：

```
ldapsearch -h host -p nonSecurePort -D "" -w bindPassword \
           -o mech=DIGEST-MD5 [-o realm="hostFQDN"] \
           -o authid="dn:uid=bjensen,dc=example,dc=com" \
           -o authzid="dn:uid=bjensen,dc=example,dc=com" \
           -b "dc=example,dc=com" "(givenname=Richard)"
```

上述範例顯示如何使用 `-o`（小寫字母 o）選項指定 SASL 選項。範圍是選用的，但如果指定範圍，它必須是伺服器主機電腦的完全合格網域名稱。`authid` 與 `authzid` 都必須存在而且完全相同，但不使用預計用於代理作業的 `authzid`。

`authid` 的值是識別對映中所用的 Principal。建議您讓 `authid` 包含 `dn:` 字首其後跟著目錄中的有效使用者 DN，或是 `u:` 字首其後跟著用戶端所決定的任何字串。這可讓您使用第 354 頁「DIGEST-MD5 識別對映」中所顯示的對映。

通常您希望 SSL 連線透過安全連接埠提供加密，以及 DIGEST-MD5 提供用戶端驗證。以下範例將透過 SSL 執行同一作業：

```
ldapsearch -h host -p securePort \
           -Z -P .mozilla/bjensen/string.slt/cert8.db \
           -N "certificateName" -W keyPassword \
           -o mech=DIGEST-MD5 [-o realm="hostFQDN"] \
           -o authid="dn:uid=bjensen,dc=example,dc=com" \
           -o authzid="dn:uid=bjensen,dc=example,dc=com" \
           -b "dc=example,dc=com" "(givenname=Richard)"
```

在此範例中，`-N` 和 `-W` 選項是 `ldapsearch` 指令所需，但不用在用戶端驗證中。而是，伺服器將依 `authid` 值中 Principal 再次執行 DIGEST-MD5 識別對映。

# 在用戶端中使用 Kerberos SASL GSSAPI

在用戶端使用 GSSAPI 機制時，您不必安裝使用者憑證，但必須配置 Kerberos V5 安全性系統。而且，如果希望使用加密的 SSL 連線，您必須依第 360 頁「在用戶端中配置伺服器驗證」所述信任伺服器憑證。

## 在用戶端主機上配置 Kerberos V5

您必須在即將執行 LDAP 用戶端的主機電腦上配置 Kerberos V5：

1. 依照安裝指示安裝 Kerberos V5。Sun 建議要安裝 Sun Enterprise Authentication Mechanism (SEAM) 1.0.1 用戶端軟體。
2. 配置 Kerberos 軟體。若使用 SEAM，請配置 `/etc/krb5` 下的檔案，以便設定 `kdc` 伺服器，定義預設範圍，以及您的 Kerberos 系統所要求的其他任何組態工作。

3. 如有必要，修改 /etc/gss/mech 檔案，使列示的第一個值是 kerberos_v5。

### 指定 Kerberos 驗證的 SASL 選項

1. 使用啓用 GSSAPI 的用戶端應用程式之前，您必須用下列指令，以您的使用者 Principal 初始化 Kerberos 安全性系統：

   ```
   kinit userPrincipal
   ```

   *userPrincipal* 是您的 SASL 識別，例如 bjensen@example.com。

2. 以下 ldapsearch 工具的範例顯示如何使用 -o ( 小寫字母 o) 選項指定使用 Kerberos 的 SASL 選項：

   ```
   ldapsearch -h host -p securePort \
              -Z -P .mozilla/bjensen/string.slt/cert8.db \
              -N "certificateName" -W keyPassword \
              -o mech=GSSAPI [-o realm="example.com" \
              -o authid="bjensen@example.com" \
              -o authzid="bjensen@example.com"] \
              -b "dc=example,dc=com" "(givenname=Richard)"
   ```

3. 在此範例中，-N 與 -W 選項是 ldapsearch 指令所需，但不用在用戶端驗證中。realm、authid 與 authzid 可省略，因爲 kinit 指令所初始化的 Kerberos 快取中會提供這兩個選項。如果提供的話，authid 與 authzid 必須完全一樣，但不使用計劃供代理作業使用的 authzid。authid 的值是識別對映中所用的 Principal。如需詳細資訊，請參閱第 356 頁「GSSAPI 識別對映」。

第 12 章

# 執行通過驗證

通過驗證 (PTA) 是一種機制，目錄伺服器可藉此機制參閱另一個目錄伺服器以驗證連結要求。PTA Plug-in 提供此項功能；允許目錄伺服器接受不是儲存在其本機尾碼中之項目的簡單連結作業（以密碼爲基礎）。

Directory Server 使用 PTA 可允許您在 Directory Server 的不同實例上，管理自己的使用者和組態目錄。

**備註** 當您爲使用者目錄與組態目錄使用相同的伺服器時，PTA Plug-in 未列在 Directory Server Console 中，您可以建立它以使用通過驗證。

本章在下列章節中說明 PTA Plug-in：

- 目錄伺服器使用 PTA 的方法
- 配置 PTA Plug-in

## 目錄伺服器使用 PTA 的方法

如果您在 Directory Server 的單獨實例上安裝組態目錄和使用者目錄，安裝程式會自動設定 PTA 以允許「組態管理員」使用者（通常爲 `admin`）執行管理任務。

在這種情況下，PTA 是必要的，因爲 `admin` 使用者項目會儲存在組態目錄的 `o=NetscapeRoot` 之下。因此，嘗試要連結使用者目錄作爲 `admin` 通常會失敗。PTA 允許使用者目錄將憑證傳送給用來驗證使用者目錄的組態目錄。然後使用者目錄會允許 `admin` 使用者進行連結。

將此範例中的使用者目錄當作 PTA 伺服器使用，也就是將連結要求傳遞至另一個目錄伺服器的伺服器。將組態目錄會當作*驗證伺服器*使用，也就是包含項目並且驗證要求用戶端之連結憑證的伺服器。

您也會在本章中看到 *PTA 樹狀子目錄*字串的使用。通過驗證樹狀子目錄是*不存在於* PTA 伺服器中的樹狀子目錄。當使用者的連結 DN 包含此樹狀子目錄時，系統會將使用者的憑證傳送至驗證目錄。

此一系列的步驟將顯示通過驗證是如何運作的：

1. 您在主機 `configdir.example.com` 上，安裝組態目錄伺服器 ( 驗證目錄 )，其包含有通過驗證樹狀子目錄 `o=NetscapeRoot`。
2. 您在主機 `userdir.example.com` 上，安裝使用者目錄伺服器 (PTA 伺服器 )，其在 `dc=example,dc=com` 尾碼內包含有資料。
3. 在使用者目錄的安裝過程中，系統將提示您提供指向組態目錄的 LDAP URL，例如：

   ```
   ldap://configdir.example.com/o=NetscapeRoot
   ```

4. 安裝程式以您提供的 LDAP URL 配置並啓用使用者目錄內的 PTA Plug-in 。

   現在，使用者目錄已配置爲 PTA 目錄。它將傳送其 DN 含有 `o=NetscapeRoot` 的項目的所有連結要求至組態目錄 `configdir.example.com`。
5. 安裝完成時，`admin` 使用者即嘗試連結至使用者目錄以開始建立使用者資料。

   `admin` 項目在組態目錄中儲存爲 `uid=admin, ou=Administrators,ou=TopologyManagement,o=NetscapeRoot`。所以，使用者目錄通過如 PTA Plug-in 組態所定義之組態目錄的連結要求。
6. 組態目錄可驗證連結憑證，包括密碼，並傳回確認至使用者目錄。
7. 使用者目錄允許 `admin` 使用者進行連結。

# 配置 PTA Plug-in

PTA Plug-in 組態資訊在 PTA 伺服器中指定爲 `cn=Pass Through Authentication,cn=plugins,cn=config` 項目。

如果您在不同伺服器實例中安裝了使用者和組態目錄，系統會自動將 PTA Plug-in 項目加入使用者目錄組態。如果您在相同的實例上同時安裝了兩個目錄，而且您希望以其他目錄執行通過驗證，則必須先建立 Plug-in 組態項目。

## 建立 Plug-in 組態項目

1. 執行下列指令以建立 Plug-in 組態項目：

```
ldapmodify -a -h PTAhost -p port -D "cn=Directory Manager" -w password
dn:cn=Pass Through Authentication,cn=plugins,cn=config
objectClass:top
objectClass:nsSlapdPlugin
objectClass:extensibleObject
cn:Pass Through Authentication
nsslapd-pluginPath:ServerRoot/lib/passthru-plugin.so
nsslapd-pluginInitfunc:passthruauth_init
nsslapd-pluginType:preoperation
nsslapd-plugin-depends-on-type:database
nsslapd-pluginId:passthruauth
nsslapd-pluginVersion: 5.2
nsslapd-pluginVendor:Sun Microsystems, Inc.
nsslapd-pluginDescription:pass through authentication plugin
nsslapd-pluginEnabled:on or off
nsslapd-pluginarg0:ldap[s]://authenticatingHost[:port]/PTAsubtree options
```

   其中 *ServerRoot* 視您的安裝而定。

   Plug-in 引數指定了識別驗證目錄伺服器的主機名稱、選用的連接埠和 PTA 樹狀子目錄的 LDAP URL。如果沒有指定連接埠，LDAP 預設值爲 389、LDAPS 爲 636。您也可以設定選用的連線參數，如下列章節所述。如果 *PTAhost* 已有 *PTAsubtree* 存在，Plug-in 將*不會*通過連結要求至 *authenticatingHost*，連結將在本地端處理，而不會通過。

2. 依第 23 頁「啓動和停止 Directory Server」所述，重新啓動伺服器。

## 配置 PTA 以使用安全連線

因爲 PTA Plug-in 必須傳送包含密碼的連結憑證至驗證目錄，因此我們建議您使用安全連線。若要配置 PTA 目錄以透過 SSL 與驗證目錄進行通訊：

- 在 PTA 和驗證目錄中配置和啓用 SSL，如第 11 章「管理驗證和加密」所述。
- 建立或修改 PTA Plug-in 組態，以在 LDAP URL 中使用 LDAPS 和安全連接埠，例如：

  ```
  ldaps://configdir.example.com:636/o=NetscapeRoot
  ```

## 設定選用連線參數

PTA Plug-in 引數接受一組選用連線參數在 LDAP URL 之後：

```
ldap[s]://host[:port]/subtree [maxconns,maxops,timeout,ldapver,connlife]
```

參數必須依顯示的順序指定。雖然這些參數爲選用，但是如果您要指定其中一個，則您必須全部指定。如果您不希望自訂所有參數，請依下列指定其預設值。請確認*樹狀子目錄*參數和選用的參數間有空格。

您可配置下列每個 LDAP URL 的選用參數：

- *maxconns* - PTA 伺服器可同時開放給驗證伺服器的最大連線數目。此參數限制可通過至驗證伺服器的同時連結數量。預設值是 3。
- *maxops* - PTA 目錄伺服器可同時傳送至單一連線中之驗證目錄伺服器的最大連結要求數量。此參數進一步限制同時通過驗證的數量。預設值爲 5。
- *timeout* - 您要 PTA 伺服器等待驗證伺服器回應的最大延遲秒數。預設值爲 300 秒（五分鐘）。
- *ldapver* - 您想要 PTA 伺服器連線至驗證伺服器使用的 LDAP 協定版本。LDAPv2 的允許值是 2，LDAPv3 的允許值是 3。預設值是 3。
- *connlife* - 在時間限制的秒數內，PTA 伺服器將重新使用連線至驗證伺服器。如果該時間到期後，用戶端才要求 PTA 樹狀子目錄內的連結，伺服器會關閉 PTA 連線，再開啓新的連線。除非啓動連結要求而且伺服器判定已經超過逾時值，否則伺服器不會關閉連線。如果您不指定此選項，或者如果只有一個驗證伺服器列於 LDAP URL 中，則不會強制執行任何時間限制。如果列示了兩個或以上的主機，則預設爲 300 秒 ( 五分鐘 )。

下列 PTA Plug-in 引數的範例增加連線數量至 10，但是降低逾時時間爲一分鐘（60 秒鐘）。所有其他參數的預設值指定如下：

```
ldaps://configdir.example.com:636/o=NetscapeRoot 10,5,60,3,300
```

## 指定多重伺服器和樹狀子目錄

您可以使用多組引數配置 PTA Plug-in ，以指定多重驗證伺服器、多重 PTA 樹狀子目錄或兩者同時指定。每個引數包含一個 LDAP URL，並可能有其自己的連線選項組。

當相同的 PTA 伺服器有多重驗證伺服器時，他們可以做爲容錯移轉伺服器。每當 PTA 連線達到逾時限制，Plug-in 將依列出的順序建立連線至驗證伺服器。如果所有連線皆逾時，則驗證將失敗。

當已定義多重 PTA 樹狀子目錄，Plug-in 將依據連結 DN，通過驗證要求至對映的伺服器。下列範例顯示四個 Plug-in 引數，定義兩個 PTA 樹狀子目錄，每一個都有驗證的容錯轉移伺服器和伺服器特定的連線參數：

```
nsslapd-pluginarg0:ldaps://configdir.example.com/o=NetscapeRoot
 10,10,60,3,300
nsslapd-pluginarg1:ldaps://configbak.example.com/o=NetscapeRoot
 3,5,300,3,300
nsslapd-pluginarg2:ldaps://east.example.com/ou=East,ou=People,
 dc=example,dc=com 10.10,300,3,300
nsslapd-pluginarg3:ldaps://eastbak.example.com/ou=East,ou=People,
 dc=example,dc=com 3,5,300,3,300
```

如以下範例所示，也可以用空格分隔主機名稱以指定多重伺服器：

```
nsslapd-pluginarg0:ldaps://configdir.example.com:636
  configbak.example.com:636/o=NetscapeRoot 10,10,60,3,300
```

# 修改 PTA Plug-in 組態

您可以在任何時間重新配置 PTA Plug-in ，啓用或停用，或變更驗證主機或 PTA 樹狀子目錄。

1. 編輯 PTA Plug-in 組態項目 (`cn=Pass Through Authentication,cn=plugins,cn=config`) 以修改 `nsslapd-pluginenabled` 和 `nsslapd-pluginarg`*N* 屬性。您可以使用主控台或 `ldapmodify` 公用程式編輯組態。

   例如，下列指令將啓用 PTA Plug-in 和 SSL，以及上述顯示的連線參數。

   ```
   dn:cn=Pass Through Authentication,cn=plugins,cn=config
   changetype:modify
   replace:nsslapd-pluginenabled
   nsslapd-pluginenabled:on
   -
   replace:nsslapd-pluginarg0
   nsslapd-pluginarg0:ldaps://configdir.example.com:636/
    o=NetscapeRoot 10.100.60,3,300
   -
   replace:nsslapd-pluginarg1
   nsslapd-pluginarg1:ldaps://configbak.example.com:636/
    o=NetscapeRoot 3,5,300,3,300
   ^D
   ```

2. 依第 23 頁「啓動和停止 Directory Server」所述，重新啓動伺服器。

第 13 章

# 使用日誌檔監視 Directory Server

本章描述如何藉由配置記錄策略，及分析伺服器所維護的狀態資訊，來監視 Directory Server 的方法。

Directory Server 提供三種類型的日誌檔：

- 存取記錄 - 列出與伺服器連線的用戶端和要求的作業。
- 錯誤記錄 - 提供有關伺服器錯誤的資訊。
- 稽核記錄 - 提供有關修改尾碼及組態的詳細資料。

伺服器中的狀態資訊包含有關連線和快取活動的統計資訊。透過 Directory Server Console 可以取得此資訊，並且透過 LDAP 指令行工具可以取得監視項目的資訊。如需關於使用 SNMP 監視伺服器的資訊，請參閱第 14 章「使用 SNMP 監視目錄伺服器」。

本章包含下列章節：

# 定義日誌檔策略

下列各節描述如何定義日誌檔的建立和刪除策略。

## 定義日誌檔自動重建原則

如果您希望目錄定期封存目前記錄並啓動新記錄，您可以在 Directory Server Console 中定義日誌檔自動重建策略。您可配置下列參數：

- 您想要目錄保存的記錄總數。當目錄到達此記錄數目時，在建立新的記錄前，它會刪除資料夾中最舊的日誌檔。預設爲 10 個記錄。請勿將此值設定爲 1。如果您這樣設定的話，目錄將無法自動重建記錄，而且記錄將無限增長。
- 各日誌檔大小的最大值 (MB)。如果您不想設定記錄大小的最大值，請在此欄位中輸入 -1。預設爲 100 MB。當日誌檔到達此最大值 ( 或在下一個步驟中定義的最長時間 ) 時，目錄會封存檔案並啓動新的日誌檔。如果您將記錄數目的最大值設定爲 1，則目錄會忽略此屬性。
- 目錄封存目前的日誌檔並建立新日誌檔的頻率，是依據輸入的分鐘、小時、天、週或月的數目。預設爲每天。如果您將記錄數目的最大值設定爲 1，則目錄會忽略此屬性。

## 定義日誌檔刪除策略

如果您希望目錄自動刪除舊的封存記錄，您可以在 Directory Server Console 中定義日誌檔刪除策略。只有在您先前已經定義了日誌檔自動重建策略時，日誌檔刪除策略才會有意義。如果您只有一個日誌檔，則無法使用日誌檔刪除。

記錄自動重建時，伺服器會評估並套用日誌檔刪除策略。

您可配置下列參數：

- 合併封存日誌檔大小的最大值。到達最大值時，將自動刪除最舊的封存日誌檔。如果您不想設定記錄大小的最大值，請在欄位中輸入 -1。預設爲 500 MB。如果將日誌檔數目設定爲 1 時，會忽略此參數。
- 可用磁碟空間的最小數量。到達此可用磁碟空間的最小值時，將自動刪除最舊的封存日誌檔。預設爲 5 MB。如果將日誌檔數目設定爲 1 時，會忽略此參數。
- 日誌檔的最長天數。到達此日誌檔的最長天數時，將自動刪除此日誌檔。預設爲 1 個月。如果將日誌檔數目設定爲 1 時，會忽略此參數。

## 手動日誌檔自動重建

如果您尚未設定自動的日誌檔建立或刪除策略，您可手動自動重建日誌檔。依據預設，可以在下列目錄中找到存取、錯誤及稽核日誌檔：

*ServerRoot*/slapd-*serverID*/logs

若要手動自動重建日誌檔：

1. 請關閉伺服器。如需說明，請參閱第 23 頁「啓動和停止 Directory Server」。
2. 萬一您需要舊的日誌檔作爲以後的參考時，請移除或重新命名您自動重建的日誌檔。
3. 重新啓動伺服器。如需說明，請參閱第 23 頁「啓動和停止 Directory Server」。

   伺服器將根據每個記錄組態，自動建立新檔案。

## 存取日誌檔

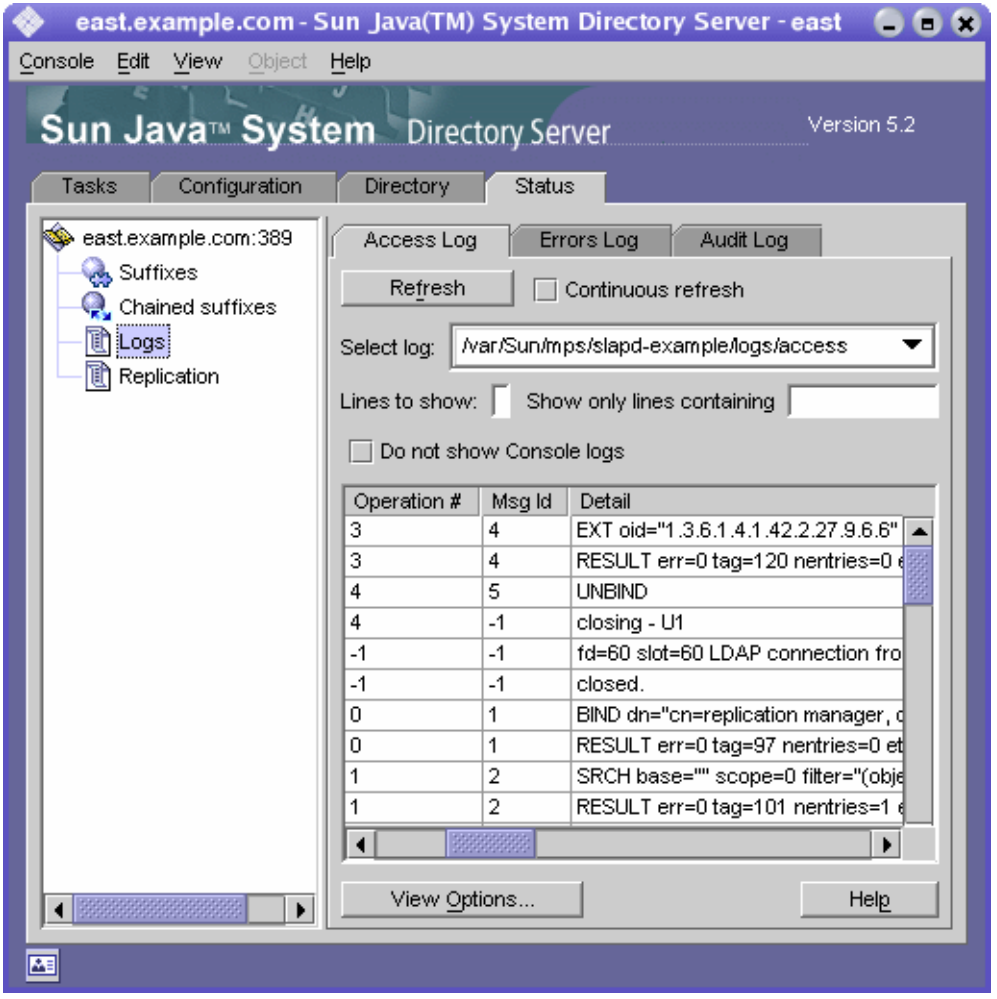
存取日誌檔包含有關用戶端與目錄連線的詳細資訊。Directory Server Resource Kit 提供日誌分析器工具 `logconv.pl`，可讓您分析 Directory Server 存取日誌檔。日誌分析器工具擷取使用統計資料，然後計算重大事件的發生次數。如需此工具的詳細資訊，請參閱《Directory Server Resource Kit Tools Reference》 Chapter 24 "The Log Analyzer Tool"。

### 檢視存取日誌檔

1. 在 Directory Server Console 最上層的 [ 狀態 ] 標籤上，選擇 [ 記錄 ] 圖示，並選擇右面板中的 [ 存取記錄 ] 標籤。

   I. 此標籤顯示一份表格，內含選擇的存取日誌檔內最新的項目，如下圖所示。如需關於存取訊息的說明，請參閱《Directory Server Administration Reference》中的 Chapter 3 "Access Log Content"。

**圖 13-1** 檢視記錄內容




2. 若要重新整理目前的顯示，請按一下 [ 重新整理 ]。如果想要每十秒自動重新整理顯示，請選擇 [ 繼續 ] 核取方塊。
3. 若要檢視不同的存取日誌檔，請從 [ 選取記錄 ] 下拉式功能表中選擇該日誌檔。
4. 若要顯示不同數目的訊息，在 [ 顯示行數 ] 的文字方塊中輸入您想要檢視的行數，然後按一下 [ 重新整理 ]。
5. 若要篩選記錄訊息，您可以在 [ 僅顯示包含的行數 ] 文字方塊中輸入字串，再按一下 [ 重新整理 ]。您也可以選擇 [ 不要顯示主控台記錄 ] 核取方塊，以篩選掉從主控台連線傳給伺服器的任何訊息。

6. 若要修改日誌檔項目表的欄位，請按一下 [ 檢視選項 ]。使用 [ 檢視選項 ] 對話方塊的控制項可變更欄位的順序、加入或移除欄位，以及選擇可將表格排序的欄。

## 配置存取日誌檔

您可配置若干個設定值以自訂存取日誌檔，包括目錄儲存存取日誌檔的位置，以及建立和刪除策略。

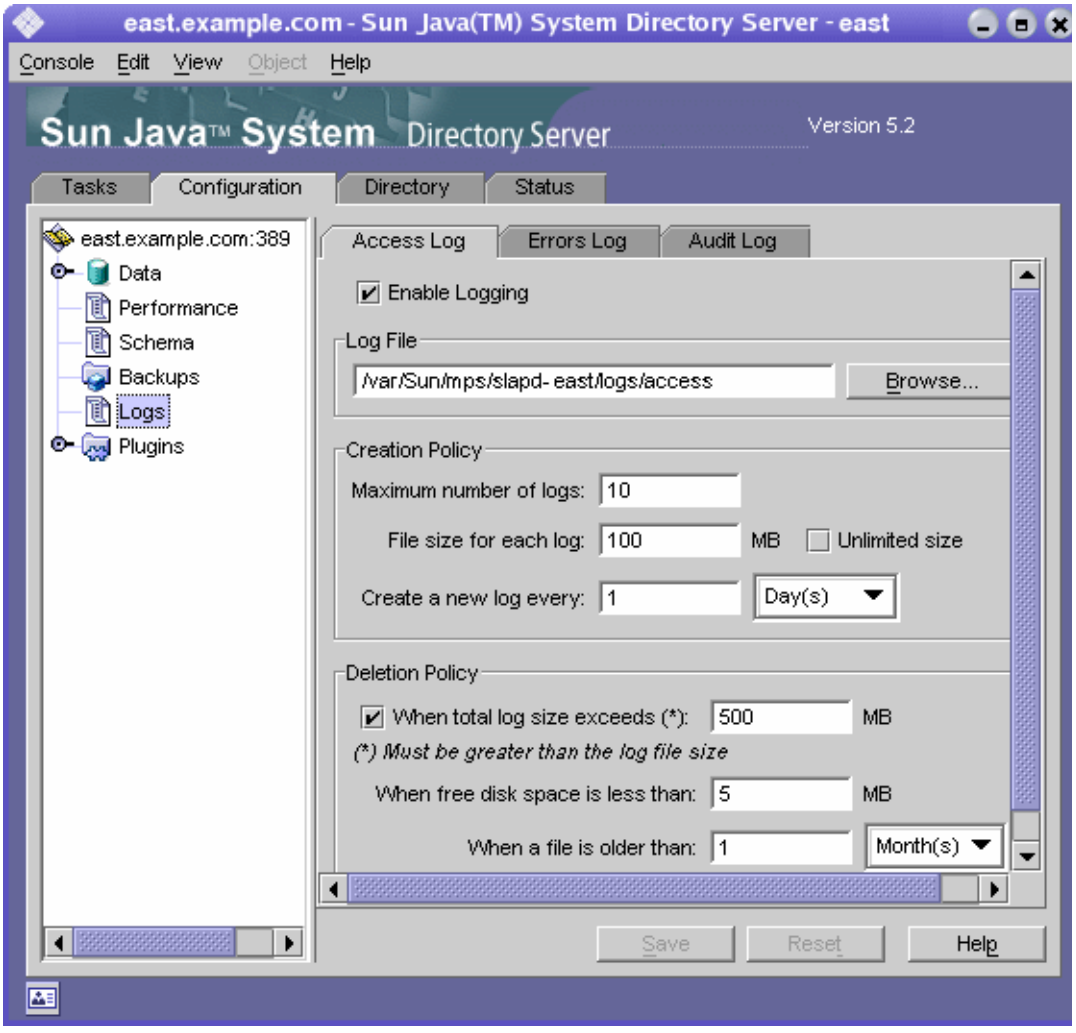
您也可停用目錄的存取日誌檔。您可以這樣處理，因爲存取日誌檔可能會快速增長 ( 每 2,000 次存取目錄，您的存取日誌檔大約會增加 1 MB )。不過，在您關閉存取日誌檔前，請考慮存取日誌檔所提供之有用的疑難排解資訊。

若要配置存取記錄：

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，選擇 [ 記錄 ] 圖示，並選擇右面板中的 [ 存取記錄 ] 標籤。

   此標籤包含存取記錄的組態設定，如 圖 13-2 所示：

**圖 13-2** 日誌檔自動重建與刪除的組態面板




2. 若要啓用存取記錄，請選擇 [ 啓用記錄 ] 核取方塊。

   如果不希望目錄維護存取日誌檔，請清除此核取方塊。

   存取日誌檔預設爲啓用狀態。

3. 在 [ 日誌檔 ] 欄位中，請輸入希望目錄用於存取日誌檔的完整路徑和檔名。預設檔爲：

   *ServerRoot*/slapd-*serverID*/logs/access

4. 設定記錄數目的最大值、記錄大小，以及封存週期。

   如需這些參數的相關資訊，請參閱第 376 頁「定義日誌檔自動重建原則」。

5. 設定合併封存日誌檔大小的最大值、可用磁碟空間的最小數量，以及日誌檔的最長天數。

   如需這些參數的相關資訊，請參閱第 376 頁「定義日誌檔刪除策略」。

6. 當您完成變更作業後，請按一下 [ 儲存 ]。

# 錯誤日誌檔

錯誤記錄中包含了在正常作業期間，目錄所遇到錯誤與事件的詳細訊息。

## 檢視錯誤日誌檔

1. 在 Directory Server Console 最上層的 [ 狀態 ] 標籤上，選擇 [ 記錄 ] 圖示，並選擇右面板中的 [ 錯誤記錄 ] 標籤。

   此標籤顯示一份表格，內含選擇的錯誤日誌檔內最新的項目，如第 378 頁上的「圖 13-1」中所示。如需錯誤訊息的說明，請參閱《Directory Server Administration Reference》中的 Chapter 4 "Error Log Message Reference"。

2. 若要重新整理目前的顯示，請按一下 [ 重新整理 ]。如果想要每十秒自動重新整理顯示，請選擇 [ 繼續 ] 核取方塊。

3. 若要檢視封存的錯誤日誌檔，請在 [ 選取記錄 ] 下拉式功能表中選擇。

4. 若要指定不同數目的訊息，在 [ 顯示行數 ] 的文字方塊中輸入您想要檢視的行數，然後按一下 [ 重新整理 ]。

5. 若要篩選日誌檔訊息，您可以在 [ 只顯示包含的行 ] 文字方塊中輸入字串，再按一下 [ 重新整理 ]。您也可以選擇 [ 不要顯示主控台記錄 ] 核取方塊，以篩選掉從主控台連線傳給伺服器的任何錯誤訊息。

6. 若要修改日誌檔項目表的欄位，請按一下 [ 檢視選項 ]。使用 [ 檢視選項 ] 對話方塊的控制項可變更欄位的順序、加入或移除欄位，以及選擇可將表格排序的欄。

## 配置錯誤日誌檔

您可以變更錯誤日誌檔的幾項設定，包括目錄儲存日誌檔的位置，以及希望在目錄的日誌檔中所要包含的資訊。

若要配置錯誤日誌檔：

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，選擇 [ 記錄 ] 圖示，並選擇右面板中的 [ 錯誤記錄 ] 標籤。

   此標籤包含錯誤日誌檔的組態設定，例如第 380 頁上的「圖 13-2」中顯示的各項。

2. 若要啓用錯誤日誌檔，請選擇 [ 啓用記錄 ] 核取方塊。

   如果不希望目錄維護錯誤日誌檔，請清除此核取方塊。錯誤日誌檔預設爲啓用狀態。

3. 若要設定錯誤記錄的詳細程度，請按一下 [ 記錄層級 ] 按鈕以顯示 [ 錯誤記錄層級 ] 對話方塊。選取一個以上您要詳細錯誤及除錯資訊的內部產品元件。或者，選取 [ 詳細資訊 ] 核取方塊以傳回最大量的執行階段輸出，包含瑣碎的訊息。

   變更預設值的這些值，可能會導致您的錯誤日誌檔迅速增長，所以必須預留足夠的磁碟空間。除非 Sun Java System Customer Support 要求您這麼做，否則建議您切勿變更記錄層級。

4. 在 [ 日誌檔 ] 欄位中，請輸入您希望用於存放錯誤日誌檔之目錄的完整路徑和檔名。預設檔案爲：

   *ServerRoot*/slapd-*serverID*/logs/error

5. 設定記錄數目的最大值、記錄大小，以及封存週期。

   如需這些參數的相關資訊，請參閱第 376 頁「定義日誌檔自動重建原則」。

6. 設定合併封存日誌檔大小的最大值、可用磁碟空間的最小數量，以及日誌檔的最長天數。

   如需這些參數的相關資訊，請參閱第 376 頁「定義日誌檔刪除策略」。

7. 當您完成變更作業後，請按一下 [ 儲存 ]。

# 稽核記錄

稽核記錄中包含有關每個尾碼及伺服器組態變更的詳細資訊。存取日誌檔和錯誤記錄會預設爲啓用狀態，稽核記錄則不然。檢視此日誌檔之前，您必須將它啓用。

## 配置稽核記錄

您可以使用 Directory Server Console 啓用和停用稽核記錄，並指定儲存稽核日誌檔的位置。

若要配置稽核記錄：

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，選取 [ 記錄 ] 圖示，並選取右面板中的 [ 稽核記錄 ] 標籤。

   此標籤包含稽核記錄的組態設定值，例如第 380 頁上的「圖 13-2」中顯示的各項。

2. 若要啓用稽核記錄，請選取 [ 啓用記錄 ] 核取方塊。

   若要停用稽核記錄，請清除該核取方塊。稽核記錄預設爲停用狀態。

3. 在 [ 日誌檔 ] 欄位中，請輸入用於存放稽核記錄之目錄的完整路徑和檔名。預設檔案爲：

   *ServerRoot*/slapd-*serverID*/logs/audit

4. 設定記錄數目的最大值、記錄大小，以及封存週期。

   如需這些參數的相關資訊，請參閱第 376 頁「定義日誌檔自動重建原則」。

5. 設定合併封存日誌檔大小的最大值、可用磁碟空間的最小數量，以及日誌檔的最長天數。

   如需這些參數的相關資訊，請參閱第 376 頁「定義日誌檔刪除策略」。

6. 當您完成變更作業後，請按一下 [ 儲存 ]。

## 檢視稽核記錄

1. 在 Directory Server Console 最上層的 [ 狀態 ] 標籤上，選取 [ 記錄 ] 圖示，並選取右面板中的 [ 稽核記錄 ] 標籤。

   此標籤顯示一份表格，內含選取的稽核記錄內最新的項目，如第 378 頁上的「圖 13-1」中所示。

2. 若要重新整理目前的顯示，請按一下 [ 重新整理 ]。如果想要每十秒自動重新整理顯示，請選取 [ 繼續 ] 核取方塊。

3. 若要檢視封存的稽核記錄，請在 [ 選取記錄 ] 下拉式功能表中選取。

4. 若要指定不同數目的訊息，在 [ 顯示行數 ] 的文字方塊中輸入您想要檢視的行數，然後按一下 [ 重新整理 ]。

5. 若要篩選日誌檔訊息，您可以在 [ 只顯示包含的行 ] 文字方塊中輸入字串，再按一下 [ 重新整理 ]。

# 監視伺服器活動

伺服器會一直維護有關其活動的計數器和統計資料，例如，連線和作業數，及所有尾碼的快取活動。這些資訊可幫助您疑難排解任何錯誤，及觀察伺服器的效能。您可以從 Directory Server Console 或指令行監視 Directory Server 的目前活動。

許多可以監視的參數可反映 Directory Server 效能，而且可能受到組態及調整的影響。如需關於組態屬性及其調整方法的詳細資訊，請參閱《Directory Server Performance Tuning Guide》。

## 使用主控台監視您的伺服器

1. 在 Directory Server Console 最上層的 [ 狀態 ] 標籤上，選擇狀態樹狀目錄根部的伺服器圖示。

   右面板中顯示關於伺服器活動的目前資訊。如果該伺服器目前未執行，則此標籤不會提供效能監視資訊。

2. 請按一下 [ 重新整理 ]，以重新整理目前的顯示。如果您想要伺服器持續更新顯示的資訊，請選取 [ 繼續 ] 核取方塊。

   這個伺服器狀態面板會顯示：

- 伺服器的啓動日期和時間。
- 伺服器目前的日期和時間。當複製爲啓用狀態時，您應該定期檢查，確定每部伺服器上的日期不會開始不一致。
- 資源摘要表。此表格分別爲下列資源列出啓動迄今的總數量，以及啓動迄今每分鐘的平均數量。

**表 13-1** 資源摘要表

| 資源 | 啓動迄今的總數與每分鐘平均數 |
|---|---|
| 連線 | 建立的用戶端連線數。 |
| 啓動作業 | 用戶端要求的作業數。 |
| 作業完成 | 未由用戶端中止的作業數，並將結果傳回給用戶端。 |
| 傳送到用戶端的項目 | 搜尋結果中傳回的項目數。 |
| 傳送到用戶端的位元組 | 所有用戶端要求之回應中的位元組數。 |

- 目前資源使用情形表。此表格顯示下列於最後一次重新整理面板時所使用資源。

**表 13-2** 目前資源使用情形

| 資源 | 最新的即時使用情形 |
|---|---|
| 作用中執行緒 | 用於處理要求的執行緒數量。伺服器的內部機制 ( 例如複製或鏈接 ) 可建立其他的執行緒。 |
| 開啓連線 | 目前開啓連線的數目。每一個連線可負責多個作業，因此就會有多個執行緒。 |
| 剩餘可用連線 | 伺服器可同時開啓的剩餘連線總數。此數目是根據目前開啓連線的數目，以及伺服器允許開啓同時連線的總數。大多數情況下，後面的值由作業系統決定，而且以工作中可用的檔案描述元數目來表示。 |
| 等候從用戶端讀取的執行緒 | 如果伺服器開始接收用戶端的要求，之後該要求的傳輸因某種原因而被切斷，則執行緒可能會一直等候讀取。一般而言，等候讀取的執行緒往往是網路或用戶端速度太慢的指標。 |
| 使用的資料庫 | 此伺服器上儲存的尾碼數量。此數字不包含鏈接尾碼。 |

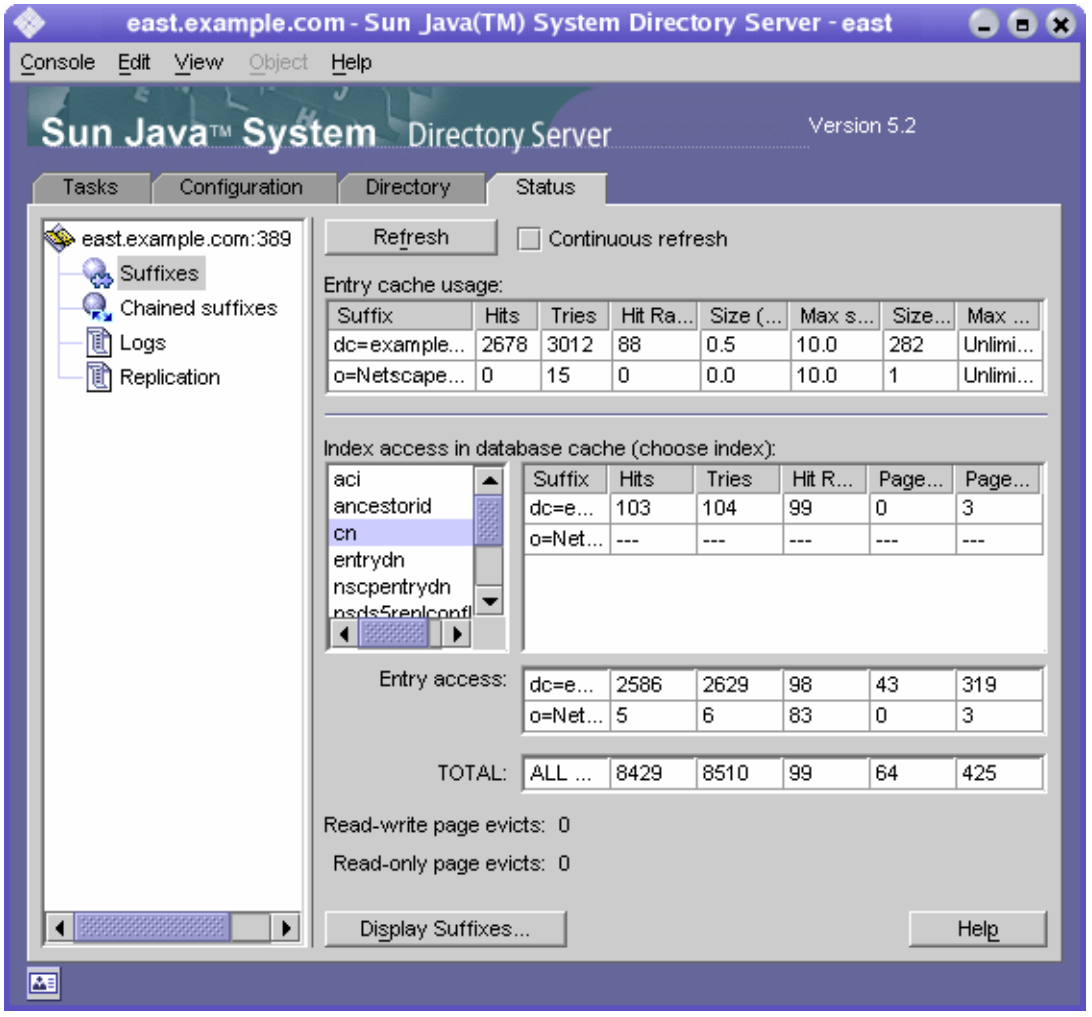
- 連線狀態表。本表顯示有關目前已開啓連線的下列資訊。

**表 13-3** 連線狀態表

| 欄標頭 | 描述 |
|---|---|
| 已開啓的時間 | 連線在伺服器上建立的時間。 |
| 已啓動 | 此連線期間要求的作業數。 |
| 已完成 | 於此連線期間，未被用戶端終止且由伺服器完成的作業數。 |
| 連結爲 | 指定用戶端用來與伺服器連結的辨別名稱。如果用戶端未通過伺服器的驗證，則此欄會顯示「未連結」。 |
| 狀態 | • 未中斷 - 表示伺服器爲閒置狀態，或正在透過連線傳送或接收資料。<br>• 已中斷 - 表示伺服器正在等候透過連線讀取或寫入資料。可能的原因是網路或用戶端速度太慢。 |
| 類型 | 表示是 LDAP 連線或 DSML-over-HTTP 連線。 |

3. 按一下左狀態樹狀目錄中的 [ 尾碼 ] 節點。此面板顯示有關於每個尾碼之資料庫快取內項目快取和索引使用情形的監視資訊，如下圖所示。

**圖 13-3** 尾碼監視面板




視需要設定重新整理模式。按一下面板底端的 [ 顯示尾碼 ]，以選取表格中要列出的尾碼。

- 第一個表格顯示下列與每個項目快取相關的資訊。

**表 13-4** 項目快取使用情形

| 欄標頭 | 描述 |
|---|---|
| 尾碼 | 尾碼的 Base DN。 |

**表 13-4** 項目快取使用情形 ( *後續* )

| 欄標頭 | 描述 |
|---|---|
| 點擊 | 從快取而非從磁碟讀取得來的項目數。 |
| 嘗試 | 從快取要求的項目數。 |
| 點擊率 (%) | 嘗試成功的比率，以百分比表示。 |
| 大小 (MB) | 來自指定尾碼之項目快取內容的目前大小。 |
| 大小上限 (MB) | 目前組態中快取大小之最大值。 |
| 大小 ( 項目 ) | 來自指定尾碼之快取內項目的目前數量。 |
| 大小上限 ( 項目 ) | 目前組態中快取項目數目的最大值。 |

下表顯示每個尾碼的資料庫快取的存取情形。

- 第一個表格顯示透過配置的索引存取資料庫快取的情形。請從屬性名稱清單中，選取要查看索引統計資料的屬性。表格將只顯示內含的選定屬性已被編製索引之尾碼的資料。
- 項目存取表顯示存取資料庫快取以擷取項目的情形。
- 最後一個表格中的 [ 總數 ] 顯示對所有資料庫快取的所有組合存取。

三個表格都具有下列欄位：

**表 13-5** 存取資料庫快取

| 欄標頭 | 描述 |
|---|---|
| 尾碼 | 尾碼的 Base DN。 |
| 點擊 | 透過索引讀取的項目數。 |
| 嘗試 | 透過索引要求的項目數。 |
| 點擊率 (%) | 嘗試成功的比率，以百分比表示。 |
| 讀取分頁 | 從磁碟讀入尾碼快取的分頁數。 |
| 分頁寫入至 | 從快取寫回磁碟的分頁數。每當讀寫的分頁經過修改，隨後又要從快取移除以留出空間給新分頁時，該尾碼分頁就會寫回磁碟。 |

- 在表格下方，下列分頁收回是所有資料庫快取的累計。從快取捨棄的分頁必須寫入磁碟中，這可能會影響伺服器效能。分頁收回數越低越好：

- 讀寫分頁收回 - 指定爲產生容納新分頁的空間，而從快取捨棄的讀寫分頁數。此值不同於 [ 分頁寫入至 ]，因爲這些是尚未修改過的捨棄讀取寫入分頁。
- 唯讀分頁收回 - 指定爲產生容納新分頁的空間，而從快取內捨棄的唯讀分頁數。

4. 根據情況按一下左狀態樹狀目錄中的 [ 鏈接尾碼 ] 節點。此面板中顯示有關在存取目錄中配置之鏈接尾碼的資訊。視需要設定重新整理模式。

   在清單中選取鏈接尾碼的 DN，以檢視其統計資料。右邊的表格列出在鏈接尾碼上執行的所有不同作業次數。

# 從指令行監視您的伺服器

您可以藉由對下列項目執行搜尋作業，從任意 LDAP 用戶端監視 Directory Server 目前的活動：

- `cn=monitor`
- `cn=monitor, cn=ldbm database, cn=plugins, cn=config`
- `cn=monitor,cn=`*`dbName`*`,cn=ldbm database,cn=plugins,cn=config`
- `cn=monitor,cn=`*`dbName`*`,cn=chaining database,cn=plugins,cn=config`

其中 *dbName* 是要監視之尾碼的資料庫名稱。請注意，依預設值，除了有關每次連線的資訊外，任何人 ( 包括匿名連結的用戶端 ) 都可讀取 `cn=monitor` 項目。

以下範例顯示如何檢視一般伺服器統計資料：

```
ldapsearch -h host -p port -D "cn=Directory Manager" -w password \
           -s base -b "cn=monitor" "(objectclass=*)"
```

如需有關這些項目中所有可用監視屬性的描述，請參閱 《Directory Server Administration Reference》 Chapter 2 中的 “Monitoring Attributes”、“Database Monitoring Attributes”、“Database Monitoring Attributes under cn=NetscapeRoot” 和 “Chained Suffix Monitoring Attributes” 。

第 14 章

# 使用 SNMP 監視目錄伺服器

簡易網路管理通訊協定 (SNMP) 是一個標準化的管理通訊協定，可用來即時監控與管理裝置及應用程式。Directory Server 提供一個次代理程式介面，讓它可以受到 SNMP 管理員應用程式監控。這讓網路應用程式能夠決定目錄伺服器的狀態，並取得有關其活動的資訊。

Directory Server SNMP 次代理程式包含唯讀值，所以 SNMP 管理應用程式無法在伺服器上執行動作。

一般而言，第 13 章「使用日誌檔監視 Directory Server」中所述的存取與錯誤日誌檔可以提供更詳盡的伺服器資訊，而 LDAP 是用來安全存取及修改伺服器組態的所選通訊協定。不過，SNMP 次代理程式確實允許 Directory Server 實例參與現有的網路管理系統。

本章包含下列主題：

- Sun Java System 伺服器中的 SNMP
- Directory Server MIB 概述
- 設定 SNMP
- 在 Directory Server 中配置 SNMP
- 啓動與停止 SNMP 次代理程式

# Sun Java System 伺服器中的 SNMP

SNMP 讓管理應用程式能夠對映用程式和執行代理程式或次代理程式的裝置進行查詢。SNMP 代理程式或次代理程式會收集來自應用程式或裝置的資訊，以回應來自 SNMP 管理員的查詢。在由代理程式的管理資訊庫 (MIB) 所定義的表格中，資訊是以變數的型式建構而成。

網路管理員會經常查詢次代理程式中的 SNMP 變數，次代理程式則傳回要求的值。SNMP 也定義一套機制，讓代理程式能夠傳送 *Trap* 訊息給所有網路管理員，以報告事件。如果在啓動 Directory Server 常駐程式之前正在執行次代理程式和主代理程式，則 Directory Server 次代理程式在 Directory Server 啓動或關閉時傳送 SMUX Trap 至主代理程式。主代理程式將此轉換成 SNMP Trap。

主機上可以安裝多個次代理程式。例如，如果將 Directory Server、應用程式伺服器和郵件伺服器 (Messaging Server) 全部安裝在同一台主機上，則每一個伺服器的次代理程式都會與同一個主代理程式進行通訊。主代理程式隨 Administration Server 一起安裝。

如需進一步的資訊，請參閱《 Administration Server Administration Guide》中的 Chapter 10 "Using SNMP to Monitor Servers"。

設定伺服器能夠透過 SNMP 接受監控的一般程序如下：

1. 編譯 Directory Server MIB，並將它整合進您的 SNMP 管理系統。請參閱系統說明文件。
2. 在機器上設定 SNMP，然後透過 Sun Java System Server Console 配置和啓動 SNMP 主代理程式。
3. 透過 Directory Server Console 配置 SNMP 次代理程式。
4. 透過 Directory Server Console 啓動 SNMP 次代理程式。
5. 存取由 MIB 定義的 SNMP 受管理物件，並透過代理程式將它公開。這個步驟完全依您的 SNMP 管理系統而定。

下列各節描述 Directory Server 組態特定的步驟。

# Directory Server MIB 概述

Directory Server 的 MIB 有下列物件識別碼：

```
iso.org.dod.internet.private.enterprises.netscape.nsldap
(nsldapd OBJECT IDENTIFIER ::= { 1.3.6.1.4.1.1450.7 })
```

它定義在下列檔案中：

*ServerRoot*/plugins/snmp/netscape-ldap.mib

MIB 定義了可透過 SNMP 監控的變數，以及變數內含的數值類型。目錄 MIB 分成四個不同的受管理物件表：

- 作業表 - 包含目錄中有關連結、作業、參照及錯誤的統計資料。這些變數值也存在目錄的 cn=snmp,cn=monitor 項目的屬性中。請參閱 《Directory Server Administration Reference》 Chapter 2 的 "Monitoring Attributes"。
- 項目表 - 包含目錄中的項目數和項目快取點擊。這些變數值也與目錄的 cn=snmp,cn=monitor 項目的屬性中的作業變數混在一起。請參閱 《Directory Server Administration Reference》 Chapter 2 的 "Monitoring Attributes"。
- 互動表 - 包含曾跟此目錄伺服器通訊的最近 5 個目錄伺服器的統計資料。請參閱 《Directory Server Administration Reference》 Chapter 2 的 "Interactions Table of Supported SNMP Managed Objects"。
- 實體表 - 包含描述這個 Directory Server 實例的變數，例如其伺服器 ID 和版本。請參閱 《Directory Server Administration Reference》 Chapter 2 的 "Entity Table of SNMP Supported Managed Objects"。

在可以使用目錄的 MIB 之前，必須將它與您可以在下列目錄中找到的 MIB 一起編譯：

*ServerRoot*/plugins/snmp/mibs

如需關於 MIB 編譯方式的資訊，請參閱 SNMP 產品說明文件。

# 設定 SNMP

如果您的系統已經執行支援 SMUX 通訊的 SNMP 代理程式，您不需要安裝主代理程式。但您必須變更原生代理程式的組態。如果您的系統不是正在執行原生 SNMP 代理程式，您必須使用 Server Console 配置和啓動主代理程式。

如果您使用預設的連接埠設定值 (SNMP 爲 161)，則必須以 root 使用者身份執行 Administration Server 和 Directory Server。如果重新配置主代理程式以使用高於 1000 的連接埠，則不必以 root 執行。

依預設值，主代理程式使用連接埠 161，但它與大部分平台上原生 SNMP 代理程式的預設連接埠相衝突。您必須在啓動主代理程式之前先停用原生的 SNMP 代理程式，或將主代理程式的配置改爲使用其他連接埠。若要停用原生的 SNMP 代理程式，請參閱平台的說明文件。若要配置並啓動主代理程式，請依照《Administration Server Administration Guide》 Chapter 10 的 "Configuring the Master Agent" 中的指示進行。

# 在 Directory Server 中配置 SNMP

在平台上設定 SNMP 代理程式或服務後，您必須配置 Directory Server 實例中的 SNMP 參數。若要從 Directory Server Console 配置 SNMP 組態：

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，選取組態樹狀目錄根部的伺服器節點，再選取右面板中的 [SNMP] 標籤。
2. 選取 [ 啓用統計資料收集 ] 核取方塊。爲改善資源使用情形，預設狀況下不會收集 SNMP 變數的統計資料。如果您不使用 SNMP，也不透過 LDAP 監控 `cn=snmp,cn=monitor` 項目的屬性，您應該讓這個核取方塊保持停用狀態。
3. 在對映的文字欄位中，輸入主代理程式的主機名稱和連接埠號碼。

   預設值分別是 `localhost` 和連接埠 `199`。
4. 在 [ 描述屬性 ] 方塊的文字欄位中輸入資訊。這些值將反映在此伺服器公開的 SNMP 實體表中：
   - 描述 - 輸入目錄伺服器的描述，類似 Server Console 的拓樸樹中此實例的描述欄位。
   - 組織 - 輸入目錄伺服器所屬的公司或內部組織的名稱。
   - 位置 - 輸入目錄伺服器主機的地理位置。
   - 聯絡人 - 輸入目錄伺服器管理員的電子郵件地址或聯絡資訊。

5. 按一下 [ 儲存 ] 以儲存變更。
6. 依以下章節所述，啓動或重新啓動 SNMP 次代理程式。

# 啓動與停止 SNMP 次代理程式

以下程序描述如何從上啓動、重新啓動或停止 Directory Server Console SNMP 次代理程式。如需從指令行啓動和停止次代理程式的資訊，請參閱《Directory Server Administration Reference》中的 "`directoryserver sagt`" 指令。

**備註** 如果在同一部主機上加入另一個伺服器實例，而且您希望該實例成爲 SNMP 網路的一部分，您必須重新啓動 SNMP 次代理程式。

啓動、停止和重新啓動 SNMP 次代理程式：

1. 在 Directory Server Console 最上層的 [ 組態 ] 標籤上，選取組態樹狀目錄根部的伺服器節點，再選取右面板中的 [SNMP] 標籤。
2. 使用 [ 描述屬性 ] 下的次代理程式控制按鈕以啓動、停止或重新啓動次代理程式。

   停止目錄並不會停止目錄次代理程式。如果要停止次代理程式，您必須從這個標籤執行停止作業。

第 15 章

# 強制屬性值唯一性

UID 唯一性 Plug-in 能確保所指定的屬性值，在目錄或樹狀子目錄內的所有項目中是唯一的。當有任何作業嘗試加入含有指定屬性現有值的項目，或有任何作業加入或修改屬性成爲目錄中的現有值時，Plug-in 會停止這些作業。

依預設值停用 UID 唯一性 Plug-in。啓用後，可依預設值確保 `uid` 屬性的唯一性。您可以建立新的 Plug-in 實例，以在其他屬性上強制執行唯一值。UID 唯一性 Plug-in 的限制是：它只能確保單一伺服器上屬性值的唯一性。

本章包含下列章節：



## 概論

UID 唯一性 Plug-in 是一個前置作業 Plug-in，它會在伺服器更新目錄之前，檢查所有的 LDAP 作業。Plug-in 會判斷該作業是否會導致兩個項目擁有相同的屬性值，當發生這種情況時，伺服器會中止作業並傳回錯誤 19 `LDAP_CONSTRAINT_VIOLATION` 至用戶端。

您可以配置 Plug-in 在目錄內一個或多個樹狀子目錄中，或是在特定物件類別的項目之間，強制執行唯一性。這個組態決定將強制執行唯一屬性值的項目組。只有當作業的目標是這個項目組中的項目時，且該屬性值在這組所有項目之間不是唯一值時，作業才會被中止。

如果您希望強制執行其他屬性的唯一性，您可以定義多個 UID 唯一性 Plug-in 的實例。定義您要其值爲唯一的每個屬性和項目組的一個 Plug-in 實例。您也可以讓同一個屬性擁有多個 Plug-in 實例，以在多個項目組中強制執行「不同」的唯一性。每一組中只允許一次指定屬性。

當您在現有目錄上啓用屬性唯一值時，伺服器並不會在現有項目間檢查唯一值。而只有在加入項目，或者是加入或修改屬性時，才會強制執行唯一性。

依預設值，UID 唯一性 Plug-in 是停用的，因爲它會影響多重主機複製的作業。您可以在使用複製時啓用 UID 唯一性 Plug-in，但您應該要注意第 400 頁「使用有複製的唯一性 Plug-in」中所描述的行爲。

# 強制執行 uid 屬性的唯一性

本節說明如何啓用和配置 `uid` 屬性的預設唯一性 Plug-in。若要強制執行其他屬性的唯一性，請參閱第 399 頁「強制執行其他屬性的唯一性」。

## 使用主控台配置 Plug-in

使用主控台時，您必須修改預設的 `uid` 唯一性 Plug-in，以強制執行其他屬性唯一性。如果不希望擁有 `uid` 唯一性 Plug-in，請將它維持在停用狀態，並爲其他屬性建立新的 Plug-in 實例，如第 399 頁「強制執行其他屬性的唯一性」所述。

1. 在 Directory Server Console 最上層 [ 組態 ] 標籤上，展開 Plug-in 節點，並選取 `uid uniqueness` Plug-in。
2. 在右窗格中，選取核取方塊以啓用 Plug-in。

   請勿修改初始化功能或 Plug-in 模組路徑的欄位。
3. 根據您指定已強制執行唯一性之樹狀子目錄的方式，修改 Plug-in 引數。
   - 若要指定單一樹狀子目錄的 Base DN，請編輯引數 2 的值。若要指定一個以上的樹狀子目錄，請按一下 [ 加入 ] 以加入更多引數，並在每個新文字欄位中輸入樹狀子目錄的 Base DN。
   - 若要依基礎項目的物件類別來指定樹狀子目錄，請將引數設定成下列的值：

引數 1：attribute=uid
引數 2：markerObjectClass=*baseObjectClass*

Plug-in 將在目錄內每個項目下的樹狀子目錄中強制執行 uid 唯一性，該目錄具有指定的 *baseObjectClass*。例如，如果您在許多分支中都有使用者項目，如 ou=Employees 和 ou=Contractors，則請指定 markerObjectClass=organizationalUnit。

因爲標示物件類別下的分支範圍可能相當大，您可能需要進一步限制屬性唯一性的執行，以根據項目的物件類別來確認項目。按一下 [ 加入 ] 加入第三個 Plug-in 引數，並將它設定爲下列的值：

引數 3：requiredObjectClass=*entryObjectClass*

在具有 *baseObjectClass* 之項目的樹狀子目錄中，只有當作業以具有 *entryObjectClass* 的項目爲目標時，Plug-in 才會強制執行唯一性。例如，如果您有傳統的使用者項目，請指定 requiredObjectClass=inetorgperson。

4. 當您編輯完 uid 唯一性 Plug-in 後，請按一下 [ 儲存 ]。系統會提醒您必須重新啓動伺服器才能使變更生效。
5. 重新啓動伺服器以開始強制執行 uid 屬性的唯一值。

# 從指令行配置 Plug-in

下列程式描述如何使用 ldapmodify 指令啓用和配置 uid 唯一性 Plug-in。Plug-in 組態項目的 DN 爲 cn=uid uniqueness,cn=plugins,cn=config。

1. 將 nsslapd-pluginEnabled 屬性設定爲 on 或 off，可分別啓用或停用 Plug-in。

```
ldapmodify -h host -p port -D "cn=Directory Manager" -w password
dn:cn=uid uniqueness,cn=plugins,cn=config
changetype:modify
replace:nsslapd-pluginEnabled
nsslapd-pluginEnabled:on or off
^D
```

2. 根據您指定已強制執行唯一性之樹狀子目錄的方式，修改 Plug-in 引數。

- 若要指定單一樹狀子目錄的 Base DN，請修改 nsslapd-pluginarg1 的值：

```
ldapmodify -h host -p port -D "cn=Directory Manager" -w password
dn:cn=uid uniqueness,cn=plugins,cn=config
changetype:modify
replace:nsslapd-pluginArg1
nsslapd-pluginArg1:subtreeBaseDN
^D
```

若要指定一個以上的樹狀子目錄，請加入更多引數，並以樹狀子目錄的完整 Base DN 作爲每個引數的值：

```
ldapmodify -h host -p port -D "cn=Directory Manager" -w password
dn:cn=uid uniqueness,cn=plugins,cn=config
changetype:modify
add:nsslapd-pluginArg2
nsslapd-pluginArg2:subtreeBaseDN
-
add:nsslapd-pluginArg3
nsslapd-pluginArg3:subtreeBaseDN
-
...
^D
```

- 若要根據樹狀子目錄的基礎項目中之類別物件來指定該樹狀子目錄，請將引數設定成下列的值：Plug-in 會在具有 *baseObjectClass* 的每個項目下的樹狀子目錄中，強制執行 `uid` 屬性的唯一性。或者，您可以在第三個引數中指定 *entryObjectClass*，如此只有在作業以具有此物件類別的項目爲目標時，Plug-in 才會強制執行唯一性。

  ```
  ldapmodify -h host -p port -D "cn=Directory Manager" -w password
  dn:cn=uid uniqueness,cn=plugins,cn=config
  changetype:modify
  replace:nsslapd-pluginArg0
  nsslapd-pluginArg0:attribute=uid
  -
  replace:nsslapd-pluginArg1
  nsslapd-pluginArg1:markerObjectClass=baseObjectClass
  -
  replace:nsslapd-pluginArg2
  nsslapd-pluginArg2:requiredObjectClass=entryObjectClass
  ^D
  ```

3. 重新啓動伺服器以使變更生效。

# 強制執行其他屬性的唯一性

UID 唯一性 Plug-in 可以用來強制執行任何屬性的唯一性。您必須在目錄中的 `cn=plugins,cn=config` 下建立新的項目，才能建立 Plug-in 的新實例。

1. 使用 `ldapmodify` 指令來加入新 Plug-in 實例的組態項目。指令的第一部分如下所示。指令的其他部分則顯示在下列步驟中。

   ```
   ldapmodify -a -h host -p port -D "cn=Directory Manager" -w password
   dn:cn=plug-in_name,cn=plugins,cn=config
   objectClass:top
   objectClass:nsSlapdPlugin
   objectClass:extensibleObject
   cn:plug-in_name
   nsslapd-pluginDescription:Enforce unique attribute values
   nsslapd-pluginType:preoperation
   nsslapd-plugin-depends-on-type:database
   nsslapd-pluginPath:ServerRoot/lib/uid-plugin.so
   nsslapd-pluginVersion: 5.2
   nsslapd-pluginVendor:Sun Microsystems, Inc.
   nsslapd-pluginId:NSUniqueAttr
   nsslapd-pluginInitfunc:NSUniqueAttr_Init
   nsslapd-pluginEnabled:on 或 off
   ...
   ^D
   ```

   在指令的第一個部分中，*plug-in_name* 應該是包含屬性名稱的簡短描述性名稱，例如 `cn=mail uniqueness`。當伺服器重新啓動後，將新實例的啓用狀態指定爲 `on` 或 `off`。

2. 指令的其他部分會指定 Plug-in 引數，這些引數視您決定要強制執行唯一性的樹狀子目錄之方式而定：

- 若要根據其 Base DN 來定義一或多個樹狀子目錄，則第一個引數必須是屬性的名稱，且應該具有唯一值，而後續的引數則是樹狀子目錄基礎項目的完整 DN：

  ```
  nsslapd-pluginarg0: attribute_name
  nsslapd-pluginarg1:subtreeBaseDN
  nsslapd-pluginarg2:subtreeBaseDN
  ...
  ^D
  ```

- 若要根據樹狀子目錄的基礎項目內物件類別來定義該樹狀子目錄，則第一個引數必須包含 `attribute=`*attribute_name*，以指定應該具有唯一值的屬性名稱。第二個引數必須是 *baseObjectClass*，此引數決定要強制執行唯一性之樹狀子目錄的基礎項目。或者，您可以在第三個引數中指定 *entryObjectClass*，如此只有當作業以具有此物件類別的項目爲目標時，Plug-in 才會強制執行唯一性。

```
nsslapd-pluginarg0:attribute=attribute_name
nsslapd-pluginarg1:markerObjectClass=baseObjectClass
nsslapd-pluginarg2:requiredObjectClass=entryObjectClass
^D
```

在所有的 Plug-in 引數中，等號 ( = ) 前後都不可以有空格。

3. 重新啓動伺服器，將這個唯一性 Plug-in 的新實例載入伺服器中。

# 使用 Plug-in 複製的唯一性 Plug-in

當更新作業是複製作業的一部分時，UID 唯一性 Plug-in 並不會對屬性值進行任何檢查。這不會影響單一主機的複製，但 Plug-in 無法自動對多重主機複製強制執行屬性唯一性。

## 單一主機複製案例

因爲用戶端應用程式所做的所有修改都是在主機複本上執行，所以主機伺服器上應該啓用 UID 唯一性 Plug-in。此外，應該配置 Plug-in 以強制執行複製尾碼中的唯一性。因爲主機會確定所需屬性的值是唯一的，所以不需要在用戶伺服器上啓用 Plug-in。

在單一主機的用戶上啓用 UID 唯一性 Plug-in，並不會干擾複製或正常的伺服器作業，但卻可能讓效能稍微降低。

## 多重主機複製案例

UID 唯一性 Plug-in 的設計，並不適用於多重主機複製案例。因爲多重主機複製對複製模型的一致性要求不嚴謹，所以同時在兩台伺服器上加入相同的屬性值並不會被刪除，即使這兩台伺服器都已經啓用 Plug-in。

但是，您可以在下列情況中使用 UID 唯一性 Plug-in：

- 您執行唯一性檢查的屬性是命名屬性。
- 所有主機上相同樹狀子目錄的相同屬性都已經啓用唯一性 Plug-in。

遇到這些情況時，系統會在複製期間將唯一性衝突報告爲命名衝突。命名衝突需要以手動方式解決。如需關於解決複製衝突的資訊，請參閱第 306 頁「解決一般複製衝突」。

使用 Windows 複製的唯一性 Plug-in

第 16 章

# 疑難排解 Directory Server

本章提供有關安裝 Directory Server 的基本疑難排解資訊。

## 疑難排解安裝

表 16-1 常見安裝問題及解決方案

| 問題 | 可能的解決方案 |
| --- | --- |
| 我收到有關遺漏程式庫的訊息。 | 執行 `idsktune`，至少修正所有 ERROR 狀況，以及安裝所有建議的修補程式。 |
| 安裝未起作用，而且我現在無法解除安裝。我該怎麼辦？ | 請移除產品登錄檔 ( *除非這樣一來將對其他產品造成負面影響* )：<br>• 以超級使用者身份在 Solaris 系統上安裝時，產品登錄檔位於 `/var/sadm/install/productregistry`<br>• `/var/tmp/sw/productregistry` 位於 AIX 和 HP-UX 系統上<br>• `/var/tmp/productregistry` 位於 Red Hat 系統上<br>• `%SYSTEM_DIR%\system32\productregistry` 位於 Windows 上<br>接下來，請在重新安裝之前，手動移除部份已安裝的檔案。 |
| 安裝失敗而且我不知道是何原因。是否擁有安裝日誌檔？ | 是。日誌檔位於下列位置：<br>• 在 Solaris 系統上，`/var/sadm/install/logs` ( 以超級使用者身份安裝 ) 或 `/var/tmp` ( 以一般使用者身份安裝 )<br>• 在其他 UNIX 系統上，`/var/tmp`<br>• 在 Windows 系統上，`%TEMP%` 資料夾 |

表 16-1 常見安裝問題及解決方案 (*續*)

| 問題 | 可能的解決方案 |
| --- | --- |
| 用戶端找不到伺服器。 | 嘗試使用如 `dirserv` 之類的主機名稱。<br>如果這樣無效，請確定伺服器是否列在您所用名稱服務 ( 如 DNS) 中，並嘗試使用完全合格網域名稱，如 `dirserv.example.com`。<br>如果這樣無效，請嘗試使用主機的 IP 位址，如 `192.168.0.30`。 |
| 連接埠使用中。 | 如果是進行升級，您可能在升級前未關閉 Directory Server。請關閉舊的伺服器，再手動啓動升級的伺服器。<br>否則，可能是有其他伺服器正在使用該連接埠。請用適當的工具 ( 例如，在 UNIX 系統上可用 `netstat`(1M) 公用程式加上 `-a` 選項 ) 檢查哪些連接埠爲使用中，以判斷哪些連接埠依然可供使用。 |
| 發生 LDAP 驗證錯誤，導致安裝失敗。 | 您在安裝期間提供的完全合格網域名稱可能不正確，例如提供的是 `dirserv.nisDomain.Example.COM`，而正確的應爲 `dirserv.example.com`。 |
| 我忘了目錄管理員 DN 與密碼。 | 目錄管理員 DN 是記錄在 *ServerRoot*`/slapd-`*serverID*`/config/dse.ldif` 中的 `nsslapd-rootdn` 值。<br>目錄管理員密碼是記錄在 `dse.ldif` 中的 `nsslapd-rootpw` 值。如果密碼未加密 - 強烈建議您應予以加密！ - 然後密碼會以純文字格式顯示在 `dse.ldif` 中，而不會加上如 {`SSHA`} 之類的加密結構識別碼字首。<br>如果密碼經過加密，您必須手動修正此問題。<br>1. 停止 Directory Server。<br>2. 請變更 `dse.ldif` 中的 `nsslapd-rootpw` 值，小心其後不要加上字首。<br>3. 儲存並關閉 `dse.ldif`。<br>4. 重新啓動伺服器。<br>5. 將您爲 `nsslapd-rootpw` 指定的值登入爲目錄管理員。<br>6. 依《Directory Server 管理指南》所述，爲目錄管理員設定加密結構，然後再變更一次密碼。 |

表 16-1 常見安裝問題及解決方案 (*續*)

| 問題 | 可能的解決方案 |
| --- | --- |
| 我誤裝 32 位元版本的 Directory Server。<br>要如何改爲執行 64 位元版本？ | 1. 依《Directory Server 管理指南》所述，將所有資料匯出到 LDIF。<br>2. 移除所有資料庫檔案。<br>資料庫檔案位於實例的 `cn=config,cn=ldbm database,cn=plugins,cn=config` 上的 `nsslapd-directory` 值所指示的路徑下。<br>3. 安裝 64 位元的元件 (如果尚未安裝)。<br>4. 將 *ServerRoot*`/bin/slapd/server/64/ns-slapd` 設爲可執行。<br>5. 如果作業系統以 32 位元模式執行，請以 64 位元模式重新開機。<br>6. 如有必要，變更快取大小設定以用於 32 位元模式。<br>7. 初始化匯出到 LDIF 的所有資料，依《Directory Server 管理指南》所述。<br>8. 重新啓動伺服器。 |
| 我誤裝 64 位元版本的 Directory Server。<br>要如何改爲執行 32 位元版本？ | 1. 依《Directory Server 管理指南》所述，將所有資料匯出到 LDIF。<br>2. 移除所有資料庫檔案。<br>資料庫檔案位於實例的 `cn=config,cn=ldbm database,cn=plugins,cn=config` 上的 `nsslapd-directory` 值所指示的路徑下。<br>3. 變更 *ServerRoot*`/bin/slapd/server/64/ns-slapd` 的模式，將其設定爲無法執行。<br>4. 初始化匯出到 LDIF 的所有資料，依《Directory Server 管理指南》所述。<br>5. 重新啓動伺服器。 |

表 16-1 常見安裝問題及解決方案 *(續)*

| 問題 | 可能的解決方案 |
| --- | --- |
| 我撰寫了一個指令檔來處理安裝。當我嘗試使用我的指令檔安裝時，安裝程式傳回 73，而不是 0。<br><br>此處發生了什麼問題？ | 安裝程式傳回的代碼如下：<br>0 - SUCCESS<br>1 - WARNING_REBOOT_REQUIRED<br>2 - WARNING_PLATFORM_SUPPORT_LIMITED<br>3 - WARNING_RESOURCE_NOT_FOUND<br>4 - WARNING_CANNOT_WRITE_LOG<br>5 - WARNING_LOCALE_NOT_SUPPORTED<br>50 - ERROR_FATAL<br>51 - ERROR_ACCESS<br>52 - ERROR_PLATFORM_NOT_SUPPORTED<br>53 - ERROR_NO_WINDOWING_SYSTEM_AVAILABLE<br>54 - ERROR_RESOURCE_NOT_FOUND<br>55 - ERROR_TASK_FAILURE<br>56 - ERROR_USER_EXIT<br>57 - ERROR_CANNOT_UPGRADE<br>58 - ERROR_NOTHING_TO_DO<br>59 - ERROR_IN_SERIALIZATION<br>60 - ERROR_ABNORMAL_EXIT<br>61 - ERROR_INCOMPATIBLE_STATEFILE<br>62 - ERROR_UNKNOWN_COMMANDLINE_OPTION<br>70 - ERROR_NOT_INSTALLED<br>71 - PARTIALLY_UNINSTALLED<br>72 - FULLY_UNINSTALLED<br>73 - INSTALLED<br>74 - ERROR_FAILED<br>75 - ERROR_STOPPED<br>76 - ERROR_STOPPED_ON_ERROR<br>77 - PARTIALLY_INSTALLED<br><br>換句話說，73 表示安裝成功。 |

# 附錄 A

# 使用 Sun Crypto 加速板

本附錄提供有關結合使用 Directory Server 與 Sun Crypto 加速板，以增強連線效能的指令，此連線使用的是基於憑證之驗證的安全通訊端階層 (SSL) 協定。

## 開始前

表 A-1 所涵蓋的項目，必須在嘗試使用 Sun Crypto 加速板以增強 SSL 連線效能之前完成。

**表 A-1** 使用介面卡的先決條件

| 先決條件 | 說明 |
| --- | --- |
| 介面卡安裝 | 當您在主機上安裝硬體、驅動程式、修補檔案和管理公用程式時，請參閱介面卡所提供的產品說明文件。 |
| Directory Server 安裝 | 如需指令，請參閱「Sun Java Enterprise System 2004Q2 安裝指南。 |
| 伺服器憑證 (PKCS#12 格式 ) | 取得 Directory Server 的伺服器憑證做爲 `.p12` 檔案 |
| CA 憑證 (PEM 格式 ) | 取得憑證授權單位 (CA) 的 CA 憑證做爲隱私權增強型郵件 (PEM) 格式檔案。 |

請參閱第 11 章「管理驗證和加密」中有關 SSL 協定本身和 SSL 憑證的討論，以及如何透過 Server 主控台結合使用協定與支援管理之 Sun Java System 伺服器的指令。

# 建立 Token

Directory Server 使用 Token 和密碼來存取加速板上的適當密碼金鑰資料。Token 採用 *user@realm* 的格式，其中 *user* 是使用加速板形式的使用者 ( 密碼金鑰資料的擁有者 )，而 *realm* 是使用加速板形式的範圍 ( 使用者及其金鑰資料的邏輯分割區 )。加速板 *user* 不需與系統上的使用者帳戶有任何關係。此變數只供介面卡使用。如需使用者和範圍的進一步說明，請參照加速板產品說明文件。

您可以使用系統所提供介面卡適用的 `secadm`(1M) 公用程式來建立 Token 的使用者和範圍。加速板也允許建立多個 *slots* 來管理多個應用程式的 Token。此處假設因爲效能的緣故，您將主機指定給 Directory Server 並因此只使用了一個插槽 ( 預設值 )。如需使用配備多個軟體應用程式之介面卡的詳細資訊，請參閱加速板產品說明文件。

請執行下列步驟建立 Token 的使用者與範圍以存取預設的插槽。

1. 啓動 `secadm` 公用程式。

   `$` *CryptoPath*`/bin/secadm`

   預設的 *CryptoPath* 爲 `/opt/SUNWconn/crypto`。

2. 建立 Token 的範圍。

   ```
   secadm> create realm=dsrealm
   System Administrator Login Required
   Login: super-user
   Password:
   Realm dsrealm created successfully.
   ```

3. 設定要建立使用者的範圍。

   ```
   secadm> set realm=dsrealm
   secadm{dsrealm}> su
   System Administrator Login Required
   Login: super-user
   Password:
   secadm{root@dsrealm}#
   ```

4. 建立使用者 `nobody` 爲使用預設的插槽，並在重新啓動已配置 SSL 的 Directory Server 時輸入密碼。

```
secadm{root@dsrealm}# create user=nobody
Initial password: password
Confirm password: password
User nobody created successfully.
secadm{root@dsrealm}# exit
```

此時您已經建立 Token nobody@dsrealm 的使用者和範圍，並提供重新啓動 Directory Server 時所要使用的密碼。

## 產生介面卡的連結

加速板連結必須使用您所產生的外部安全模組形式，這樣 Directory Server 才能與介面卡連結。請執行下列步驟，使外部安全模組與可支援多個 SSL 演算法之 Directory Server 憑證資料庫之間產生連結。

1. 使用 modutil 之前，請設定 LD_LIBRARY_PATH。

   ```
   $ set LD_LIBRARY_PATH=ServerRoot/lib ; export LD_LIBRARY_PATH
   ```

2. 建立安全模組資料庫 ( 如果沒有的話 )。

   ```
   $ cd ServerRoot/shared/bin
   $ ./modutil -create -dbdir ../../alias -dbprefix "slapd-serverID"
   ```

3. 將外部安全模組加入安全模組資料庫中。

   ```
   $ ./modutil -add "Crypto Mod" -dbdir ../../alias -nocertdb \
   -libfile CryptoPath/lib/libpkcs11.so \
   -mechanisms "RSA:DSA:RC4:DES" -dbprefix "slapd-serverID"
   ```

   預設的 *CryptoPath* 爲 /opt/SUNWconn/crypto。

4. 列出安全模組以確定加入成功。

   ```
   $ ./modutil -list -dbdir ../../alias -dbprefix "slapd-serverID"
   ```

   您應該會看到在步驟 3 中所加入之 Crypto Mod 的項目。

5. 將外部安全模組設定成 RSA、DSA、RC4 和 DES 的預設值。

   ```
   $ ./modutil -default "Crypto Mod" -dbdir ../../alias \
   -mechanisms "RSA:DSA:RC4:DES" -dbprefix "slapd-serverID"
   ```

   這應該會成功地變更預設的安全模組。

此時，您已經產生加速板的連結並且可以匯入憑證。

# 匯入憑證

在配置 SSL 之前，您必須匯入所取得的伺服器以及 CA 憑證，如 第 407 頁上的「表 A-1」中所述。執行下列步驟以匯入憑證。

1. 匯入伺服器憑證 `.p12` 檔。

   ```
   $ cd ServerRoot/shared/bin
   $ ./pk12util -i ServerCert.p12 -d ../../alias -P "slapd-serverID" \
   -h "nobody@dsrealm"
   Enter Password or Pin for "nobody@dsrealm": password
   Enter Password for PKCS12 file: password
   ```

2. 匯入 CA 憑證。

   ```
   $ ./certutil -A -n "Crypto CA Cert" -t CT -i CACert.txt \
   -d ../../alias -P "slapd-serverID" -h "nobody@dsrealm"
   ```

3. 列出與 Token 相關的憑證以確定匯入成功。

   ```
   $ ./certutil -L -d ../../alias -P "slapd-serverID" \
   -h "nobody@dsrealm"
   ```

   您應該會看到在步驟 1 和步驟 2 中所加入之憑證的項目。

此時您已經匯入憑證，並且可以配置 Directory Server 以聆聽 SSL 連線。

# 配置 SSL

利用您建立的 Token 和密碼、在外部安全模組和 Directory Server 憑證資料庫之間產生的連結、以及所匯入的憑證，便可以將 Directory Server 配置爲成在安全模式中啓動。執行這些步驟來配置 SSL 並在安全模式中重新啓動 Directory Server。

1. 建立修改的 `ssl.ldif` 檔，變更與 SSL 相關的 Directory Server 組態項目。

**程式碼範例 A-1** 修改爲使用介面卡來啓用 SSL (`ssl.ldif`)

```
dn:cn=RSA,cn=encryption,cn=config
changetype:add
objectclass:top
objectclass:nsEncryptionModule
cn:RSA
nsSSLToken:nobody@dsrealm
nsSSLPersonalitySSL:ServerCertNickname[1]
nsSSLActivation:on

dn:cn=encryption,cn=config
changetype:modify
replace:nsSSL3
nsSSL3:on
-
replace:nsSSLClientAuth
nsSSLClientAuth:allowed
-
replace:nsSSL3Ciphers
nsSSL3Ciphers:-rsa_null_md5,+rsa_rc4_128_md5,+rsa_rc4_40_md5,
 +rsa_rc2_40_md5,+rsa_des_sha,+rsa_fips_des_sha,+rsa_3des_sha,
 +rsa_fips_3des_sha,+fortezza,+fortezza_rc4_128_sha,
 +fortezza_null,+tls_rsa_export1024_with_rc4_56_sha,
 +tls_rsa_export1024_with_rc4_56_sha,
 +tls_rsa_export1024_with_des_cbc_sha
-
replace:nsCertfile
nsCertfile:alias/slapd-serverID-cert8.db
-
replace:nsKeyFile
nsKeyFile:alias/slapd-serverID-key3.db

dn:cn=config
changetype:modify
replace:nsslapd-secureport
nsslapd-secureport:port
-
replace:nsslapd-security
nsslapd-security:on
```

1. 此暱稱包含在 Directory Server 的憑證中。

此處的 *port* 是 `nsslapd-secureport` 的值，爲 Directory Server 在安全模式中啓動後聆聽 SSL 連線的連接埠。

2. 套用修改以變更 Directory Server 組態。

```
$ ldapmodify -p currPort -D "cn=directory manager" -w password -f ssl.ldif
```

其中 *currPort* 爲 Directory Server 目前聆聽用戶端要求的連接埠號碼。

3. 在安全模式中重新啓動 Directory Server。

```
$ ServerRoot/slapd-serverID/restart-slapd
Enter PIN for nobody@dsrealm: password
```

此處的 *password* 爲建立 Token `nobody@dsrealm` 時提供給 `nobody` 的使用者密碼。

此時，Directory Server 透過您指定的連接埠聆聽 SSL 流量。您可以配置 Sun Java System Administration Server 和用戶端應用程式以透過該連接埠存取有 SSL 機制的 Directory Server。如需詳細資訊，請參閱第 11 章「管理驗證和加密」。

# 感謝詞和特別授權

本產品包含下列版權公告所涵蓋之軟體。此處提及之所有商標與註冊商標爲其個別擁有者之財產。

INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

COPYRIGHT Copyright (c) 1997-2000 Messaging Direct Ltd. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY MESSAGING DIRECT LTD. "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL MESSAGING DIRECT LTD. OR ITS EMPLOYEES OR AGENTS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. END COPYRIGHT

COPYRIGHT Copyright (c) 2000 Fabian Knittel. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain any existing copyright notice, and this entire permission notice in its entirety, including the disclaimer of warranties.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Redistributions in binary form must reproduce all prior and current copyright notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR(S) BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. END COPYRIGHT

The source code to the Standard Version of Perl can be obtained from CPAN sites, including http://www.perl.com/.

This product incorporates compression code by the Info-ZIP group. There are no extra charges or costs due to the use of this code, and the original compression sources are freely available from ftp://ftp.cdrom.com/pub/infozip/ on the Internet.

# 詞彙

如需本說明文件集中使用的完整專有名詞清單，請參閱 Java Enterprise System 詞彙 (http://docs.sun.com/doc/816-6873)。

# 索引

## A



## B

# C



# D



# F



# G



# H

## I



## K



## L



## M



## N

## P



## R



## S



## T

## U



## V



## W



## X



## Z



## 一畫



## 三畫



## 下畫



## 丁畫

## 索引

## 七畫



## 八畫

## 十一畫



## 十畫

## 十一畫



## 十二畫

# 十三畫

## 十五畫



## 十六畫



## 十七畫

## 十一畫



## 十八畫



## 十九畫

## 二十一畫



## 二十二畫



## 二十三畫