Sun Java™ System

Identity Synchronization for Windows 1
安裝與配置指南

2004Q3

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

文件編號：817-7849

目錄

圖表清單

表格清單

前言

Sun Java™ System Identity Synchronization for Windows 1 2004Q3 (先前的 Sun™ ONE Identity Synchronization for Windows) 允許密碼和其他指定的使用者屬性在 Sun Java™ System Directory Server 和其他系統之間流動。

本指南說明如何安裝和配置 Sun Java System Identity Synchronization for Windows 以便在生產環境中使用。

有關此版本 Identity Synchronization for Windows 新特點和增強功能的最新資訊，請參閱線上版本說明：

http://docs.sun.com/db/doc

附註 本文件中提及的使用者介面會隨著產品未來的版本更替而有所變更。

本前言包含下列資訊：

本書的適用者

這本 *《安裝與配置指南》*適用於管理員、系統工程師，以及專業服務工程師安裝和配置 Identity Synchronization for Windows，以便在 Sun Java™ System Directory Server 與 Windows Active Directory/NT 電腦間建立雙向密碼和使用者屬性同步化。

您應該已熟悉

- 配置及操作 Directory Server 和 Windows Active Directory/NT
- 輕量級目錄存取協定 (LDAP)
- Java 技術
- 可延伸標記語言 (XML)
- 公開金鑰加密與「安全通訊端階層 (SSL)」協定的基本概念
- 內部網路、外部網路和網際網路安全，以及企業內數位憑證角色的基本概念

閱讀本書前

*《Sun Java System Identity Synchronization for Windows 1 2004Q3 版本說明》*包含與產品有關的最新資訊 — 包括可能取代本書中所提供指示的資訊。在嘗試本書中所說明的任何程序之前，請務必閱讀這些版本說明。

由於 Sun Java System Directory Server 在 Identity Synchronization for Windows 部署中被用作資料儲存庫，因此您應該熟悉隨該產品一起提供的文件。您可從 http://docs.sun.com/coll/DirectoryServer_04q2 線上存取 Directory Server 文件。

本書架構

*《Sun Java System Identity Synchronization for Windows 1 2004Q3 安裝與配置指南》*分成以下幾章：

- 第 1 章，「瞭解產品」：說明與 Identity Synchronization for Windows 相關的一些基本概念；如產品功能、系統元件、指令行公用程式、系統元件分佈，以及部署範例。
- 第 2 章，「準備安裝」：說明安裝及配置程序，並提供準備安裝產品時可能會有幫助的資訊。
- 第 3 章，「安裝核心程式」：說明如何使用 Identity Synchronization for Windows 安裝程式及如何安裝 Identity Synchronization for Windows 核心元件。
- 第 4 章，「配置核心資源」：說明如何使用主控台來新增及配置核心元件資源。
- 第 5 章，「安裝連接器與 Directory Server 外掛程式」：說明 Identity Synchronization for Windows 連接器與 Directory Server 外掛程式的安裝方法。
- 第 6 章，「現有使用者同步化」：說明如何針對新安裝的 Identity Synchronization for Windows 連結和重新同步化現有的使用者。
- 第 7 章，「遷移至 Identity Synchronization for Windows 1 2004Q3」：說明如何將系統從 Sun Java System Identity Synchronization for Windows 1.0 版遷移至 1 2004Q3 版。
- 第 8 章，「移除軟體」：說明如何移除 Identity Synchronization for Windows，包括如何準備解除安裝作業及如何手動解除安裝主控台。
- 第 9 章，「疑難排解」：爲您提供有關資訊，用於疑難排解 Identity Synchronization for Windows 安裝作業的問題。
- 第 10 章，「認識稽核與錯誤檔案」：提供稽核和錯誤記錄的相關資訊，包括如何設定記錄層級、檢視及瞭解您的日誌檔案和目錄來源狀態。
- 第 11 章，「配置安全性」：說明如何配置安全系統。提供的資訊包括強化安全性、保護複製配置的安全、啓用 SSL，以及將 Active Directory CA 憑證加入憑證資料庫。
- 附錄 A，「使用 Identity Synchronization for Windows 指令行公用程式」：說明如何使用 Identity Synchronization for Windows 指令行公用程式來執行不同工作。
- 附錄 B，「LinkUsers XML 文件範例」：提供可用於自訂環境的 Linkusers XML 文件範例 (`linkusers-simple.cfg`)。

- 附錄 C，「以非超級使用者身份在 Solaris 系統上執行服務」：說明如何以非超級使用者身份執行 Identity Synchronization for Windows 服務。
- 附錄 D，「定義和配置同步化使用者清單」：提供「同步化使用者清單」定義及多網域配置的相關資訊。
- 附錄 E，「複製環境的安裝註解」：概述配置和保護多主伺服器複製 (MMR) 部署安全所需的步驟。

本書中使用的慣例

本節的表格說明本書中所使用的慣例。內容歸納如下：

- 第 19 頁上的「印刷排版慣例」
- 第 19 頁上的「符號」
- 第 20 頁上的「快捷鍵」
- 第 20 頁上的「預設路徑及檔案名稱」

印刷排版慣例

下表說明本書中所使用的印刷排版慣例。

表格 1 印刷排版慣例

字體	涵義	範例
AaBbCc123 (固定間距)	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、範例程式碼。	編輯您的 .login 檔案。 使用 ls -a 來列出所有檔案。 % 您有郵件。
AaBbCc123 (固定間距粗體)	您鍵入的內容 (對照電腦螢幕輸出)。	**% su** 密碼：
AaBbCc123 (斜體)	書籍標題、新術語、強調的字。 指令或路徑名稱中要更換成實際名稱或值的萬用字元。	請閱讀*使用者手冊*的第 6 章。 這些稱爲*類別*選項。 *請勿*儲存檔案。 此檔案位於 *install-dir*/bin 目錄中。

符號

下表說明本書中所使用的符號慣例。

表格 2 符號慣例

符號	說明	範例	涵義
[ ]	包含選用的指令選項。	ls [-l]	-l 選項不是必要的。
{ | }	包含必要指令選項的一組選項。	-d {y|n}	-d 選項要求您使用 y 引數或 n 引數。
-	同時聯結多個按鍵。	Control-A	按下 Control 鍵的同時再按 A 鍵。
+	連續聯結多個按鍵。	Ctrl+A+N	按住 Control 鍵，放開它，再按後續按鍵。
>	在圖形化使用者介面中指示功能表項目選項。	「檔案」 > 「新增」 > 「範本」	從 「檔案」功能表中，選擇 「新增」。從「新增」子功能表中，選擇 「範本」。

快捷鍵

Identity Synchronization for Windows 在整個使用者介面中使用了*快捷鍵* (底線字母)，爲您提供更快的選項來執行某些工作。您只要鍵入底線字母就能執行工作。快捷鍵不區分大小寫。若要存取它們，請同時按 Alt 鍵。

預設路徑及檔案名稱

下表說明本書中所使用的預設路徑及檔案名稱。

表格 3 預設路徑及檔案名稱

專有名詞	說明
<*serverroot*>	代表 Identity Synchronization for Windows 安裝位置的父系目錄。
isw-<*hostname*>	代表 Identity Synchronization for Windows 實例目錄
<*current-working-directory*>/cert8.db	代表用戶端的憑證資料庫之預設路徑及檔案名稱
<*installation_root*>/isw-<*machine_name*>/logs/central/	代表 Identity Synchronization for Windows 中央日誌的預設路徑
<*installation_root*>/isw-<*machine_name*>/logs/	代表 Identity Synchronization for Windows 本機日誌的預設路徑 (適用於系統管理員、每個連接器，以及中央記錄程式)
/usr/sfw/bin	在 Solaris 系統中，certutil 預設安裝在此目錄位置中

相關文件

http://docs.sun.com網站可讓您在線上存取 Sun 技術文件。您可以瀏覽歸檔的檔案，或搜尋特定的書籍標題或主題。

本文件集中的書籍

下表歸納出 Identity Synchronization for Windows 文件集中所包含的書籍。

表格 4 本文件集中的書籍

書籍標題	說明
Sun Java System Identity Synchronization for Windows 1 2004Q3 安裝與配置指南 (http://docs.sun.com/doc/817-6199)	說明如何安裝和配置 Identity Synchronization for Windows 以便在生產環境中使用。
Sun Java System Identity Synchronization for Windows 1 2004Q3 Deployment Planning Guide (http://docs.sun.com/doc/817-6200)	提供用於規劃和部署 Identity Synchronization for Windows 的一般指導方針及最佳實務。
Sun Java System Identity Synchronization for Windows 1 2004Q3 版本說明 (http://docs.sun.com/doc/817-6202)	可在產品發行後取得。包含最新資訊，包括這一最新版本中的新功能說明、已知的問題和限制、安裝注意事項，以及如何報告軟體或文件問題。

其他文件

由於您將使用 Directory Server 和 Sun Java™ System Message Queue，所以您可能需要參考其產品文件。您可以從下列位置存取文件：

- Sun Java System Directory Server 文件
  http://docs.sun.com/coll/DirectoryServer_04q2
- Sun Java System Message Queue 文件
  http://docs.sun.com/db/prod/2296#hic

如需公開金鑰加密、安全資料傳輸層 (SSL) 協定、內部網路、外部網路及網際網路安全性，以及企業內部數位憑證的角色之基本概念資訊，請閱讀 《*Managing Servers with iPlanet Console 5.0*》手冊中與安全性相關的附錄。

有關 Windows 2003 Server 及 Windows 密碼策略的相關資訊，請閱讀下列 Microsoft 出版品：

- *Using Secedit.exe to Force Group Policy to Be Applied Again - Windows 2000 Servers Microsoft KB #227448*
- *A Description of the Group Policy Update Utility - Windows 2003 Servers Microsoft KB #298444*
- *Microsoft Knowledge Base 文章 232690*

線上存取 Sun 資源

如需產品下載作業、專業服務、修補程式及支援以及其他開發人員資訊，請前往下列網頁：

- 開發人員資訊
  http://developers.sun.com/prodtech/index.html
- 下載中心
  http://wwws.sun.com/software/download/
- 產品資料表
  http://www.sun.com/software/
- 線上產品文件
  http://docs.sun.com
- 產品支援與狀態
  http://www.sun.com/service/support/software/
- 專業服務
  http://www.sun.com/service/sunps/sunone/index.html
- Sun 企業服務、Solaris 修補程式與支援
  http://sunsolve.sun.com
- 支援與訓練
  http://www.sun.com/supportraining/

洽詢 Sun 技術支援

如果您有本產品的相關技術問題，且在產品文件中未解答這些問題，請造訪：

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

相關協力廠商網站參照

以下是本出版品所參照的協力廠商網站：

- 有關 Windows 2003 密碼策略的相關資訊，請造訪：

  http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dsscc_aut_xbby.asp

- 有關套用或修改 Windows 2003 中的密碼及群組策略的相關資訊，請造訪：

  http://www.microsoft.com/resources/documentation/windowsserv/2003/standard/proddocs/en-us/password_grouppolicy.asp

- 有關 Microsoft Certificate Services Enterprise Root 憑證授權單位的相關資訊，請造訪：

  http://support.microsoft.com/default.aspx?scid=kb;en-us;q247078

- 有關配置 LDAP over SSL 的相關資訊，請造訪：

  http://support.microsoft.com/default.aspx?scid=kb;en-us;321051

Sun 不負責本文件中提及之協力廠商網站的可用性。Sun 對在 (或透過) 此類網站或資源取得的任何內容、廣告、產品或其他材料不做保證且不負有法律責任。Sun 對因使用或相信在 (或透過) 此類網站或資源取得的任何內容、商品或服務而導致的損害或損失，或與之相關的實際或可能的損害或損失不負有法律責任。

Sun 歡迎您提出意見

Sun 致力於提昇其文件品質，並且歡迎您提供意見與建議。

若要提出意見，請前往 http://docs.sun.com 並按一下「傳送意見」。在線上表格中，請提供文件標題和文件號碼。文件號碼是七位數或九位數的號碼，您可以在書籍標題頁或文件的頂端找到此號碼。

例如，本書的標題是 *Sun Java System Identity Synchronization for Windows 1 2004Q3 安裝與配置指南*，文件號碼則是 817-7849。

安裝與配置

第 1 章

瞭解產品

Identity Synchronization for Windows 提供 Sun Java™ System Directory Server 5 2004Q2 與下列項目之間的雙向密碼和使用者屬性同步化：

- Windows 2000 或 Windows 2003 Server Active Directory
- Windows NT SAM Registry

Identity Synchronization for Windows 處理同步化事件時具有以下特點

- **安全**：Identity Synchronization for Windows 絕不「以明文」傳送密碼，而且只允許管理員存取系統。
- **穩定**：Identity Synchronization for Windows 保持目錄同步化，即使是當個別元件暫時無法使用時也是如此。
- **高效**：Identity Synchronization for Windows 同步化方式讓您的目錄伺服器幾乎沒有什麼負荷。

在您安裝 (或遷移到) Sun Java System Identity Synchronization for Windows 1 2004Q3 版前，您應該先熟悉本章中描述的概念，本章由以下幾節組成：

產品功能

Identity Synchronization for Windows 提供下列特色和功能：

- **雙向密碼同步化**：讓您可在 Sun Java System 目錄來源和 Windows Active Directory 及 Windows NT 目錄來源間進行使用者密碼同步化。

  同步化密碼可讓使用者存取使用這些目錄來源進行登入驗證的應用程式，因此他們只需要記憶一個密碼。此外，當使用者必須套用週期性密碼更新時，他們只需要在一個環境中更新密碼。

- **雙向使用者屬性同步化**：可讓您在一個目錄環境中建立、修改和刪除選取的屬性，並自動將值傳播到其他目錄環境。

- **雙向使用者帳號建立同步化**：可讓您在一個目錄環境中建立或刪除使用者帳號，並自動將新帳戶傳播到其他目錄環境。

- **雙向物件刪除、啓動及關閉**：可讓您控制物件刪除、啓動和關閉動作在 Directory Server 與 Active Directory 目錄來源 (Windows NT 沒有) 之間的傳遞方向。

- **多網域同步化**：可讓您與多個 Active Directory 和 Windows NT 網域，以及多個 Active Directory 群進行同步化。

- **集中式系統稽核**：可讓您從單一集中的位置監控安裝與配置狀態、日常系統作業，以及與部署相關的任何出錯情況。

不需修改 Windows 目錄中的項目，也不需變更使用目錄的應用程式。

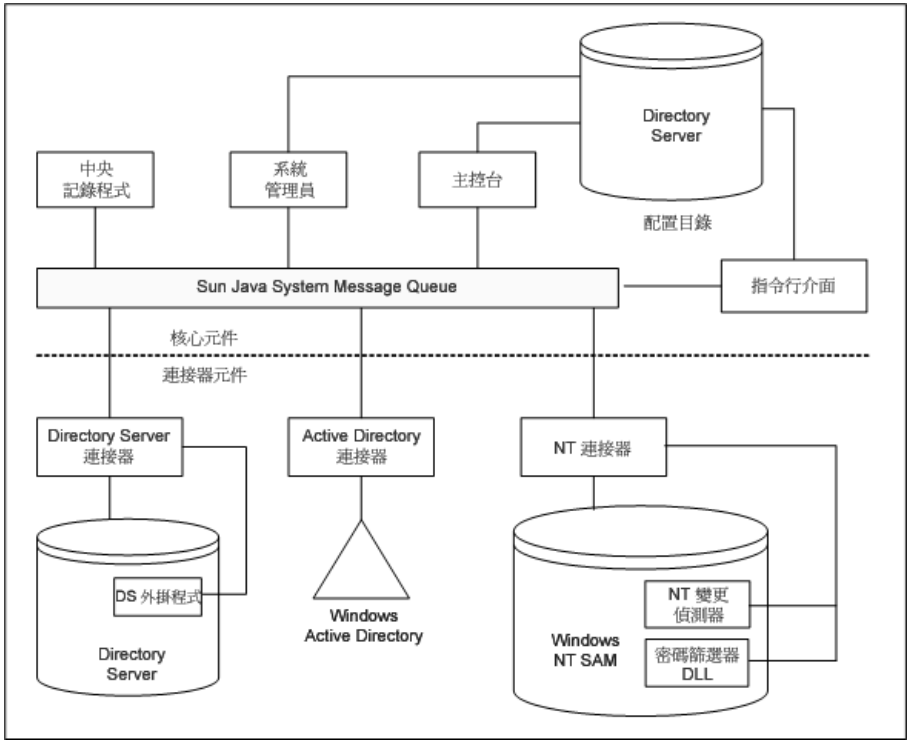
如果您使用 Identity Synchronization for Windows 在 Directory Server 和 Active Directory 之間進行同步化，則不需要在 Windows 作業環境中安裝任何元件。

如果您是在 Directory Server 和 Windows NT 之間進行同步化，您必須在 Windows NT 環境中安裝產品的 NT 元件。

系統元件

Identity Synchronization for Windows 包含一組核心元件和任意數量的個別*連接器*及*連接器子元件*，透過它們可實現 Sun Java System Directory Server 和 Windows 目錄之間的密碼和使用者屬性更新的同步化 (請參閱圖 1-1)。

圖 1-1 系統元件



本節定義並描述 Identity Synchronization for Windows 的每個元件，主題分述如下：

- 第 30 頁上的「監視程式程序」
- 第 30 頁上的「核心程式」
- 第 34 頁上的「連接器」
- 第 34 頁上的「連接器子元件」

監視程式程序

監視程式是一種 Identity Synchronization for Windows java 處理程序，負責啓動、重新啓動和停止各個後台 java 處理程序。「監視程式」可啓動及監控中央記錄程式、系統管理員和連接器 (但不監控子元件、Message Queue 或 Identity Synchronization for Windows 主控台)。

監視程式安裝在核心元件的安裝位置，可作爲 Solaris 常駐程式或 Windows 服務啓動。(有關啓動與停止服務的資訊，請參閱第 185 頁上的「啓動與停止服務」。)

核心程式

當您安裝 Identity Synchronization for Windows 時，首先安裝*核心*元件，然後對其進行配置，使其適用於您的環境。

核心程式由下列元件所構成，它們都是單獨的 java 程序。各項元件的描述從下列參考頁碼開始：

- 第 31 頁上的「配置目錄」
- 第 31 頁上的「主控台」
- 第 32 頁上的「指令行公用程式」
- 第 32 頁上的「系統管理員」
- 第 33 頁上的「中央記錄程式」

附註 監視程式安裝在核心程式的安裝位置，負責啓動與監控中央記錄程式和系統管理員。

有關詳細資訊，請參閱第 30 頁上的「監視程式程序」。

配置目錄

Identity Synchronization for Windows 將其配置資料*儲存*在 Directory Server 配置目錄下 (本程式不安裝配置目錄)。

主控台、系統管理員、指令行公用程式和安裝程式都會從配置目錄讀取產品配置資料或向其中寫入產品配置資料，包括：

- 有關各元件狀況的安裝資訊
- 每個目錄、網域、連接器和 Directory Server 外掛程式的配置資訊
- 連接器狀態
- 同步化設定，描述使用者建立、使用者刪除和屬性修改的方向
- 要同步化的屬性及兩個目錄環境 (Active Directory 和 Directory Server 或 Windows NT 和 Directory Server) 間的屬性對映
- 每個目錄拓樸中的同步化使用者清單
- 日誌設定

主控台

Identity Synchronization for Windows 提供一個主控台，可集中產品的所有元件配置和管理工作。

您可以使用主控台：

- 配置要同步化的目錄來源
- 除定義密碼外，還定義要同步化的使用者項目屬性的對映
- 指定要同步化 (或不同步化) 目錄或網域拓樸內的哪些使用者和屬性
- 監控系統狀態
- 啓動和停止同步化

指令行公用程式

Identity Synchronization for Windows 還提供指令行公用程式，您可直接從指令行執行下列工作：

- 根據您的配置和 SSL 設定值顯示憑證資訊
- 變更 Identity Synchronization for Windows 配置密碼
- 將匯出的 Identity Synchronization for Windows 1.0 版 XML 配置文件匯入
- 備妥 Sun Java System Directory Server 來源供 Identity Synchronization for Windows 使用
- 顯示完成安裝 / 配置過程必須執行之步驟，檢視已安裝之連接器、系統管理員和 Message Queue 的狀態
- 將配置目錄中的連接器狀態重設爲*未安裝*
- 同步化及連結兩個目錄中的現有使用者，並在安裝過程中預先填寫目錄
- 啓動同步化
- 停止同步化

有關本產品指令行公用程式以及其使用方式的詳細資訊，請參閱附錄 A，「使用 Identity Synchronization for Windows 指令行公用程式」。

系統管理員

Identity Synchronization for Windows 系統管理員是一個單獨的 java 程序，其功能如下：

- 利用產品的後端網路功能動態傳遞配置更新給連接器
- 保持每個連接器和所有連接器子元件的狀態
- 協調一開始用來同步化兩個目錄的 `idsync resync` 作業

中央記錄程式

可能已安裝連接器以便將它們廣泛地分佈到各遠端地理位置；因此，將所有登入資訊集中具有重要的管理價值，因爲這樣可以使管理員從一個位置監控同步化活動、偵測錯誤及評估整體系統的狀況。

管理員可使用中央記錄程式：

- 驗證系統是否正常執行
- 偵測並解決個別元件和系統整體性問題
- 稽核個別和系統整體性同步化活動
- 追蹤目錄環境間的使用者密碼同步化

有兩種不同的日誌類型：

- **稽核日誌**提供關於系統日常活動的資訊，其中包含目錄間使用者密碼同步化這類重要事件。透過增加或減少日誌訊息的詳細程度，您可以控制在稽核日誌中記錄之資訊的層級。

  附註 Identity Synchronization for Windows 也會將所有錯誤日誌訊息寫入稽核日誌中，以便於輕鬆建立與其他事件之間的關聯性。

- **錯誤日誌**提供關於符合嚴重錯誤和警告條件狀況的資訊。所有錯誤日誌項目都值得注意，所以您不能阻止記錄錯誤。如果發生錯誤，將一律記錄於錯誤日誌中。

連接器

連接器是負責管理單一資料來源類型之同步化處理的一項 java 程序。連接器可偵測出資料來源中的使用者變更，然後將這些變更透過 Message Queue 發佈到遠端連接器上。

Identity Synchronization for Windows 提供下列目錄專有的連接器，其負責在目錄和網域之間雙向同步化使用者屬性和密碼更新：

- **Directory Server 連接器**：支援 Directory Server 中的單一根字尾 (如字尾 / 資料庫)
- **Active Directory 連接器**：支援 Windows 2000 或 Windows 2003 Server Active Directory 環境中的單一實例。您可以爲額外網域使用多個連接器
- **Windows NT 連接器**：支援 Windows NT 環境中的單一網域

附註 監視程式安裝在連接器的安裝位置，負責啓動、重新啓動與停止連接器。有關詳細資訊，請參閱第 30 頁上的 「監視程式程序」。

連接器子元件

子元件是單獨從連接器中執行的輕量級處理程序或程式庫。連接器使用子元件來存取無法從遠端存取的原生資源，例如擷取 Directory Server 或 Windows NT 內的密碼。

下列連接器子元件與要同步化的目錄一同安裝，並透過加密連接與對應的連接器通訊。

- 第 34 頁上的 「Directory Server 外掛程式」
- 第 35 頁上的 「Windows NT 連接器子元件」

附註 Active Directory 連接器不需要子元件。

Directory Server 外掛程式

Directory Server 外掛程式是 Directory Server 連接器的子元件。應在每個要同步化的 Directory Server 中安裝 Directory Server 外掛程式。

此外掛程式可以

- 將加密的密碼儲存在 Retro Changelog 中，進而加強 Directory Server 連接器的變更偵測功能

- 提供 Active Directory 和 Directory Server 間使用者屬性和密碼同步化的雙向支援 (請參閱第 43 頁上的 「使用隨需密碼同步化來取得明文密碼」)

附註 Directory Server 外掛程式可於四向、多主伺服器複製 (MMR) 環境中運作。(舊版的 Identity Synchronization for Windows 只支援雙向 MMR。)

Windows NT 連接器子元件

如果您的安裝需要與 Windows NT SAM Registries 同步化，Identity Synchronization for Windows 安裝程式將在主要網域控制器 (PDC) 中與 Windows NT 連接器一道安裝下列項目：

- **變更偵測器**：藉由監控安全性日誌偵測使用者項目和密碼變更事件，然後將變更傳送到連接器
- **密碼篩選器**：擷取在 NT 網域控制器上所作之密碼變更，然後安全地將這些變更傳送到 NT 連接器

Message Queue

Identity Synchronization for Windows 使用 Message Queue (具有發佈 / 訂閱模型的一種持續性的訊息佇列機制) 在目錄來源之間傳播屬性與密碼變更，並將管理與配置資訊分佈至負責管理這些目錄來源的同步化之連接器。

Message Queue 是一種實施 Java 訊息服務 (JMS) 開放式標準的企業傳訊系統。JMS 規格是指一組程式設計介面，這組介面可爲處於分散式環境中的 java 應用程式提供建立、傳送、接收和讀取訊息的一種共同方式。

Message Queue 是由訊息發佈方與訂閱方構成，雙方使用一種共同的訊息服務來交換訊息。此訊息服務是由一或多個專用的訊息代理程式組合而成，這些代理程式負責控制對訊息佇列的存取、維護有關現用發佈方與訂閱方的資訊，並確保訊息的傳達。

Message Queue 可謂最佳方式，因爲它

- 建立了連接器之間的互信制度
- 簡化了所有元件的安全性存取控制
- 加速了端對端的密碼加密
- 確保所有密碼更新訊息的傳達
- 降低連接器與連接器之間通訊的複雜度和安全性風險

- 讓中央管理單位可以分佈配置資訊
- 支持將所有連接器日誌集中在一個中央位置

系統元件分佈

在您開發有效部署前，必須瞭解 Identity Synchronization for Windows 元件的組織方式及產品運作方式。本節內容分述如下：

瞭解本節及部署方案範例 (第 48 頁) 中描述的基本概念後，您應該能夠推知爲更複雜精密的方案 (如混合的 Active Directory 與 Windows NT 環境或多伺服器的環境) 建立部署策略時所需要的資訊。

核心程式

您先要在任何受支援作業系統的目錄伺服器上安裝所有核心元件，且只需安裝一次。Administration Server 須位於核心程式所在的電腦上。安裝核心程式之前，您必須安裝 Message Queue 3.5 SP1 Enterprise Edition。

Directory Server 連接器與外掛程式

您可以在任何支援的作業系統上安裝 Directory Server 連接器 (請見第 54 頁上的「作業系統需求」)。您不需要在執行被同步化的 Directory Server 的電腦上安裝 Directory Server 連接器。不過，每個配置的 Directory Server 來源都必須安裝一個 Directory Server 連接器。

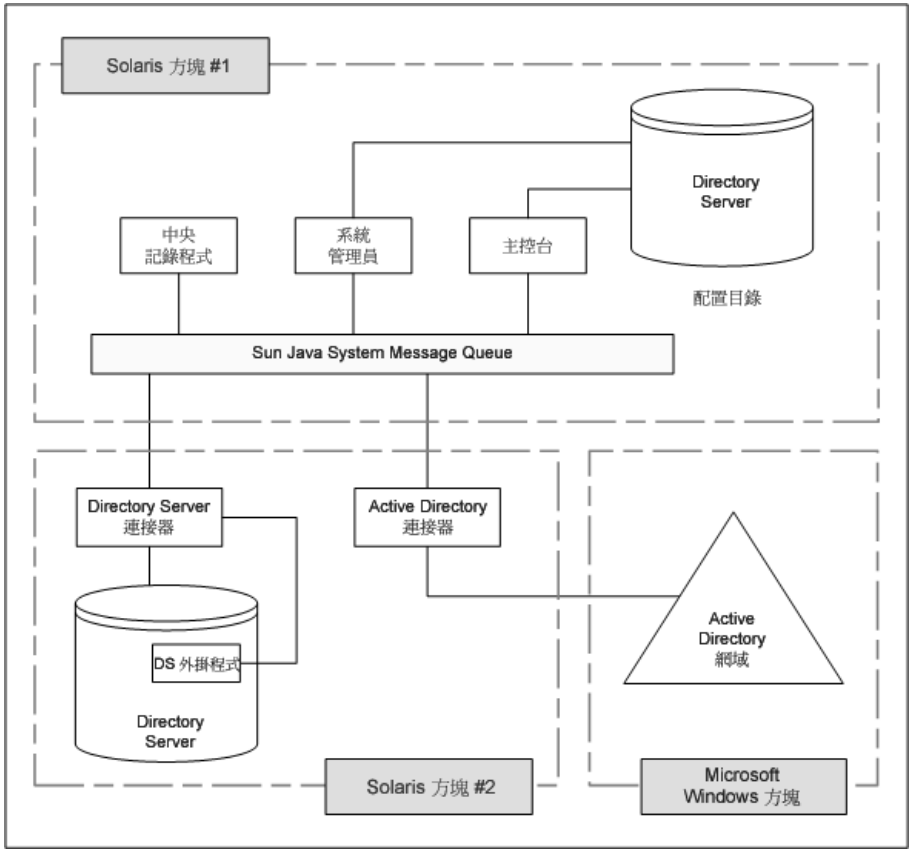
您必須在要同步化之 Directory Server 所在的每台主機上安裝 Directory Server 外掛程式。

附註 爲每個 Directory Server 來源安裝一個 Directory Server 連接器。不過，應爲每個要同步化的主伺服器、集線器和用戶複本安裝 Directory Server 外掛程式。

Active Directory 連接器

您可以在任何受支援的作業系統上安裝 Active Directory 連接器 (請參閱圖 1-2)。您不需要在 Windows 環境中安裝 Active Directory 連接器，不過每個 Active Directory 網域必須安裝一個 Active Directory 連接器。

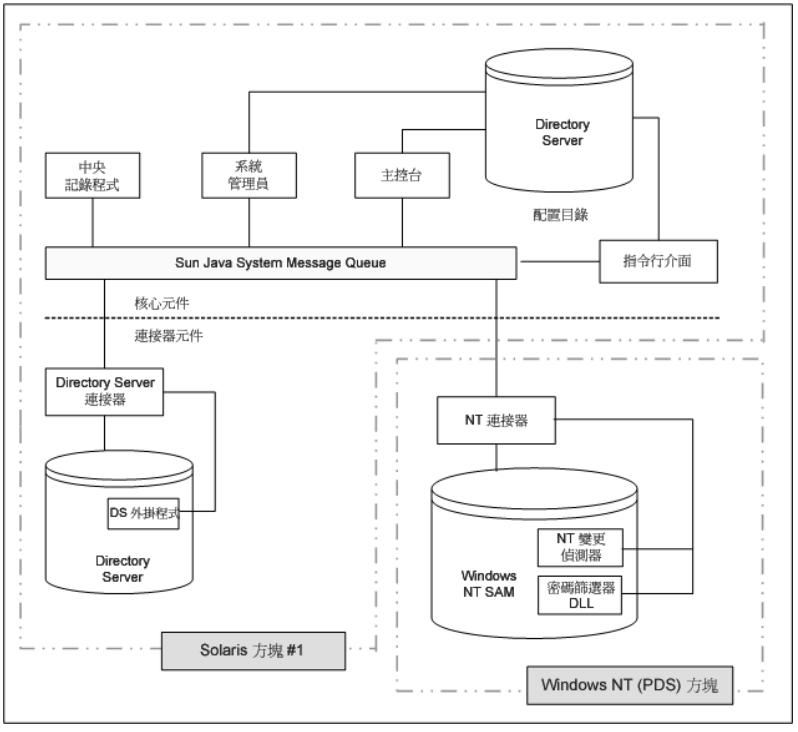
圖 1-2 Directory Server 和 Active Directory 元件分佈



Windows NT 連接器和子元件

若要與 Windows NT SAM Registry 同步化 (請參閱圖 1-3)，您必須在主要網域控制器 (PDC) 中安裝 Windows NT 連接器。此外，安裝程式會連同連接器在 NT 網域的 PDC 中安裝兩個 NT 連接器子元件 (變更偵測器和密碼篩選器 DLL)。一個 NT 連接器同步化一個 NT 網域的使用者和密碼。

圖 1-3 Directory Server 和 NT 元件分佈



Identity Synchronization for Windows 如何偵測目錄來源中的變更

本節說明 Sun Java System Directory Server (Directory Server)、Windows Active Directory 和 Windows NT 連接器如何偵測出使用者項目和密碼的變更。

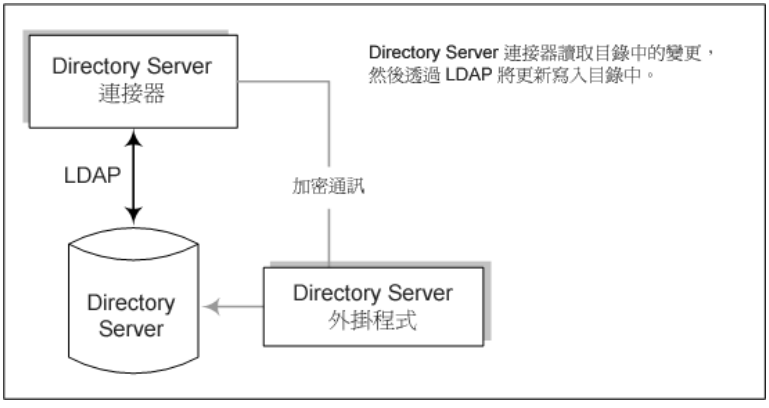
內容分述如下：

Directory Server 連接器如何偵測變更

Directory Server 連接器透過 LDAP 檢查 Directory Server Retro-Changelog，偵測出使用者項目和密碼變更事件。Directory Server 外掛程式可協助連接器進行下列操作：

- 加密明文密碼並使之可在 Retro Changelog 中使用，以擷取明文密碼。如果沒有此外掛程式，則只有雜湊的密碼會出現在 Retro Changelog 中，而雜湊的密碼是不能進行同步化的。
- 在 Active Directory 中執行隨需密碼同步化；這樣就無需在 Windows 環境中安裝任何 Identity Synchronization for Windows 元件 (請參閱第 43 頁上的「使用隨需密碼同步化來取得明文密碼」)。

圖 1-4 Directory Server 連接器如何偵測變更



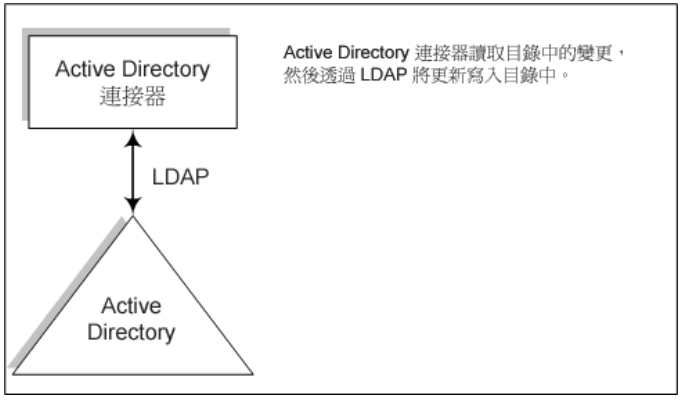
Active Directory 連接器如何偵測變更

Windows 2000/2003 Server Active Directory 連接器檢查 Active Directory 的 `USNChanged` 和 `PwdLastSet` 屬性值來偵測使用者項目和密碼的變更。

不同於 Directory Server 的 Retro Changelog，當您變更項目中的屬性時，Active Directory 並不會報告哪些屬性被變更。Active Directory 用來識別項目變更的方式是遞增 `USNchanged` 屬性。爲了偵測各個屬性的變更，Active Directory 和 Windows NT 連接器使用一個稱爲*物件快取*的同處理序資料庫。該物件快取可儲存各個 Active Directory 項目的一份雜湊複本，讓連接器得以藉此確實判斷有哪些項目屬性遭到修改。

您不需在 Windows 環境中安裝 Active Directory 連接器。它們可以在別處執行 (例如 Solaris 電腦上) 並透過 LDAP 從遠端偵測或進行變更。

圖 1-5 Active Directory 連接器如何偵測變更

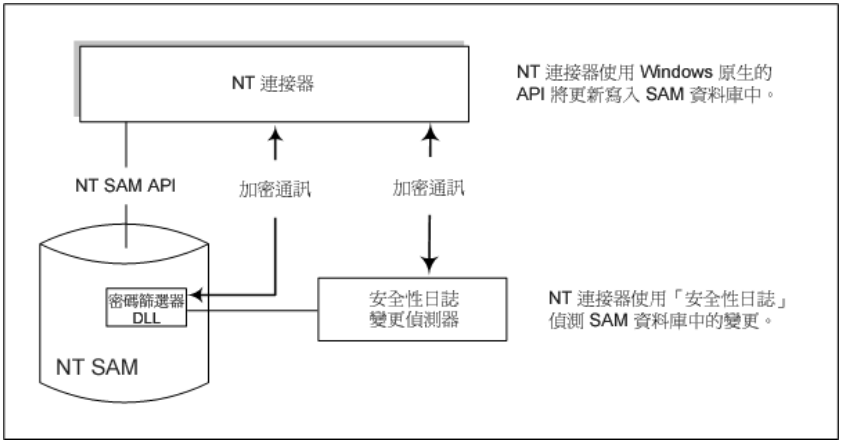


Windows NT 連接器如何偵測變更

Windows NT 連接器藉由檢查安全性日誌中有關使用者物件的稽核事件，來偵測使用者項目和密碼的變更。

若要與 Windows NT SAM Registry 同步化 (請參閱圖 1-3)，您必須在主要網域控制器 (PDC) 中安裝 Windows NT 連接器。此外，安裝程式會連同連接器在 NT 網域的 PDC 中安裝兩個 NT 連接器子元件 (變更偵測器和密碼篩選器 DLL)。一個 NT 連接器同步化一個 NT 網域的使用者和密碼。

圖 1-6 Windows NT 連接器如何偵測變更



附註 如果您的部署環境中有 Windows NT 電腦，則必須啓動稽核功能，否則 Identity Synchronization for Windows 無法記錄來自該台電腦的訊息。若要確定您的 Windows NT 電腦上的稽核記錄功能是否已啓動，請參閱第 278 頁上的「啓用 Windows NT 電腦上的稽核功能」。

如需變更偵測器與密碼篩選器 DLL 子元件的說明，請參閱第 35 頁上的「Windows NT 連接器子元件」。

傳播密碼變更

本節說明下列各種取得明文密碼的方式，有了明文密碼才能在 Windows 系統與 Directory Server 系統之間傳播密碼變更：

- 第 43 頁上的「使用密碼篩選器 DLL 來取得明文密碼」
- 第 43 頁上的「使用隨需密碼同步化來取得明文密碼」

使用密碼篩選器 DLL 來取得明文密碼

Windows NT 連接器必須取得明文密碼，才能將密碼變更傳播至 Sun Java System Directory Server。不過，您無法從 Windows 目錄擷取明文密碼，因爲密碼儲存至目錄之前已經先經過加密。

Windows NT 提供的密碼篩選器 DLL 介面，可讓元件在密碼永久性地儲存至目錄中之前，先擷取明文密碼。

使用隨需密碼同步化來取得明文密碼

雖然 Active Directory 支援與 Windows NT 相同的密碼篩選器，但您必須在每個網域控制器上安裝密碼篩選器 DLL，而不能只安裝在主要網域控制器 (PDC) 上。因爲這會造成很大的安裝負荷，所以 Identity Synchronization for Windows 使用一種不同的方式 (稱爲*隨需密碼同步化*) 來同步化從 Active Directory 傳播至 Directory Server 的密碼變更。

隨需密碼同步化使用的方式，是當使用者變更了其 Windows 2000 密碼之後嘗試登入時，在 Directory Server 取得新的密碼值。

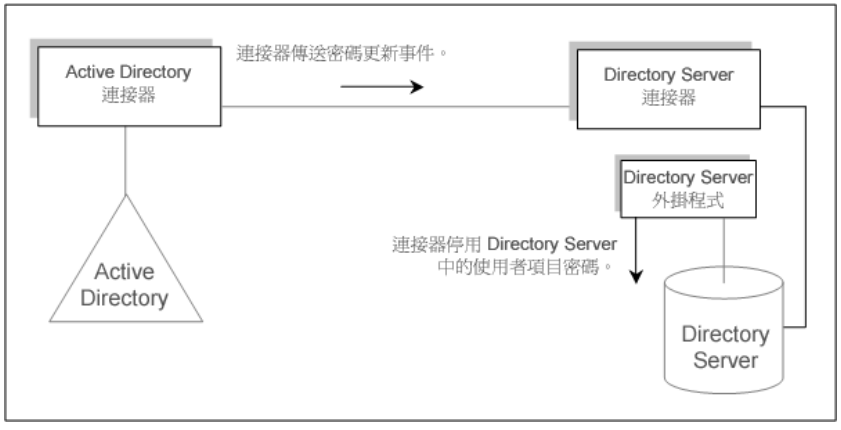
隨需密碼同步化亦可讓您使 Active Directory 上的密碼同步化，而不需使用密碼篩選器 DLL。

隨需密碼同步化的過程如下：

1. 使用者在 Windows 工作站上按 Ctrl-Alt-Del 並變更其密碼。新密碼儲存至 Active Directory。
2. Active Directory 連接器依照排定的時間間隔對系統進行輪詢。

   當連接器偵測到密碼變更 (根據 `USNchanged` (更新序號) 和 `PwdLastSet` 屬性所發生的變更) 時，連接器就會在 Message Queue 上發佈有關該密碼變更的訊息。該訊息會以 SSL 加密的通道傳輸。

圖 1-7 隨需密碼同步化 — 第 I 部分



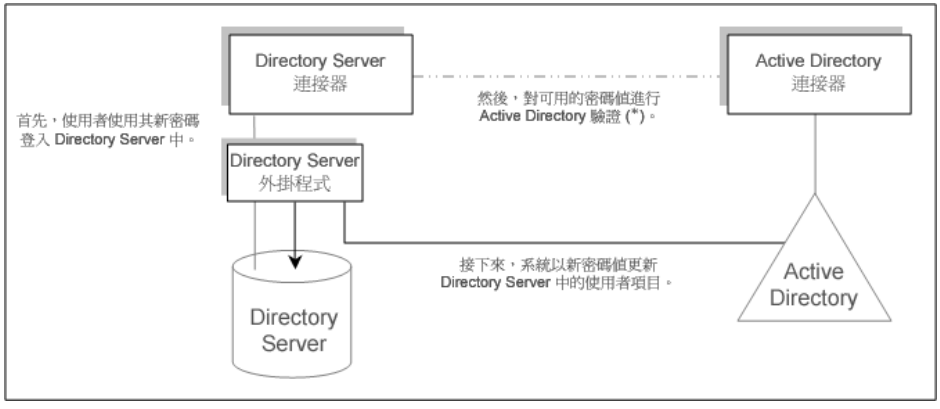
3. Directory Server 連接器收到從 Message Queue 傳來 (透過 SSL) 的密碼變更訊息。
4. Directory Server 連接器將使用者項目的 `dspswvalidate` 屬性設爲 `true`，使舊的密碼失效，並提醒 Directory Server 外掛程式密碼已經變更。
5. 當使用者使用 LDAP 應用程式 (例如 Portal Server) 嘗試登入 Directory Server 並接受身份驗證時，Sun Java System Directory Server 外掛程式會偵測出該 Directory Server 項目的密碼值是無效的。

6. Directory Server 外掛程式會在 Active Directory 中搜尋對應的使用者。當外掛程式找到該名使用者後，會嘗試使用該名使用者在登入 Directory Server 時輸入的密碼與 Active Directory 建立連結。

附註 隨需密碼同步化需要應用程式使用簡單的驗證機制來接受 Directory Server 的身份驗證，而非使用複雜的驗證機制，例如 SASL Digest-MD5。

7. 如果成功建立與 Active Directory 的連結，使用者就可以提供其新的 Active Directory 密碼，然後 Directory Server 外掛程式會設定該密碼並從 Directory Server 上該使用者項目中移除無效的密碼旗標。

圖 1-8 隨需密碼同步化 — 第 II 部分



附註 如果使用者驗證失敗，使用者項目密碼會保留在 Directory Server 中，而 Directory Server 和 Active Directory 上的密碼將不同步，直到使用者以有效密碼 (通過 Active Directory 身份驗證的密碼) 登入爲止。

穩定的同步化

Identity Synchronization for Windows 採取了許多預防措施，以確保您不會遺漏任何使用者變更事件，即使元件暫時無法使用時也是如此。Identity Synchronization for Windows 的穩定性與 TCP 網路通訊協定類似。TCP 可保證即使是透過有損的和間歇性連線的網路傳輸資料，最後還是能夠井然有序地傳輸完所有資料。當網路故障時，網路中斷期間所傳送的資料會在佇列中等候，並在連線恢復正常後重新傳送。即使下列任一元件暫時無法使用，Identity Synchronization for Windows 最後還是能夠偵測出並套用使用者變更事件：

- 連接器
- Directory Server
- Message Queue
- Active Directory 網域控制器
- Windows NT 主要網域控制器
- 系統管理員
- 配置目錄

如果這些元件中的任何一個無法使用，Identity Synchronization for Windows 會將同步化延遲到受影響的元件能夠使用爲止，並不會遺失任何變更 (即使是密碼的變更)。本 Identity Synchronization for Windows 版本不支援 Sun Cluster 或是其他標準、高可用性的解決方案。因爲 Identity Synchronization for Windows 是一種在幕後執行的應用程式，使用者並不會直接與其互動，所以通常不需具備高度可用性。如果發生災難性故障，可重新安裝 Identity Synchronization for Windows 元件，並使用 `idsync resync` 指令來重新同步化所有目錄來源。

在大多數的情況下，當元件無法使用時，本程式會讓同步化事件在佇列中等候，並一律等到該元件能夠使用之後才套用這些同步化事件。這種處理程序有兩個例外情況：

- 在多主伺服器複製的 (MMR) Directory Server 環境下，對 Windows 使用者所作之外部變更可與喜好的或輔助的 Directory Server 同步化。

  如果喜好的 Directory Server 無法使用，則 Directory Server 連接器會將變更套用至輔助伺服器。Identity Synchronization for Windows 不會偵測及傳播在任何主 Directory Server 上發生的外部變更，直到喜好的主伺服器能夠使用爲止。

- 雖然 Active Directory 連接器只能與單個 Active Directory 網域控制器通訊，Directory Server 外掛程式卻可能在執行隨需密碼同步化時，在所有 Active Directory 網域控制器之間發生故障。此時防故障備用功能就顯得格外重要 — 如果 Directory Server 外掛程式無法聯繫某個 Active Directory 網域控制器以確定使用者的新密碼，使用者就無法登入 Directory Server 中。

部署範例：雙電腦配置

本節中描述的部署方案是使用 Identity Synchronization for Windows 在 Sun 和 Windows 目錄間同步化使用者物件建立和雙向密碼修改作業。

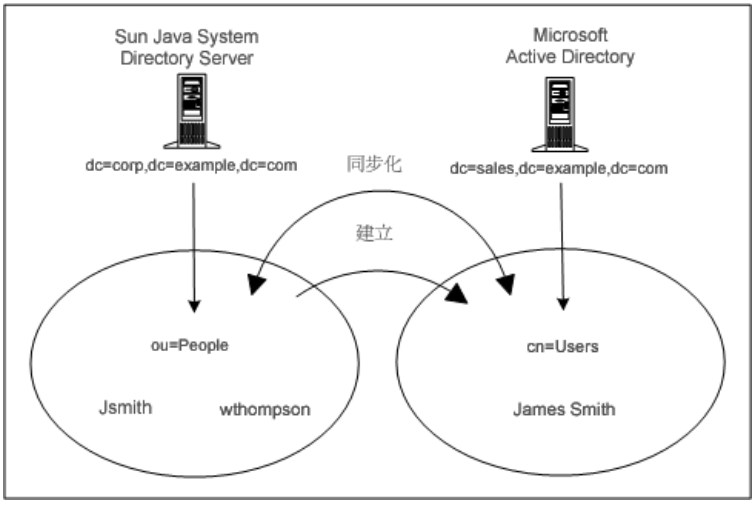
此部署方案包含兩個系統：

- 一個是執行 Sun Java System Directory Server (主機名稱：*corp.example.com*) 的系統
- 一個是在 Windows 2000 伺服器上執行 Active Directory (主機名稱：*sales.example.com*) 的系統

附註 雖然此方案中未使用 NT，但請注意 Identity Synchronization for Windows 也支援與 NT 網域的同步化，瞭解這一點很重要。

圖 1-9 說明此部署方案的同步化需求 (含相關屬性值的節點結構)。

圖 1-9 同步化需求



此方案有兩個目標：

- 在*使用者子樹* (Directory Server 中的 *ou=people* 和 Active Directory 中的 *cn=users*) 間雙向同步化使用者密碼。也就是說，只要任一目錄中發生了使用者密碼變更，密碼變更即會同步化至另一目錄中的相關使用者。

  例如，如果您變更 Directory Server 上 *ou=people* 容器中的 uid=Jsmith 的密碼，新密碼便會自動同步化至 Active Directory 伺服器上 *cn=users* 容器中的 cn=Joe Smith。

- 只將 Directory Server 使用者子樹中的使用者物件建立作業同步化至 Active Directory 使用者子樹。

  例如，如果您以指定的屬性集建立了新的使用者 (*ou=People* 容器中的 uid=WThompson)，則 Identity Synchronization for Windows 會接著以相同屬性集在 Active Directory 上爲 Wthompson 建立新的帳號 (*cn=Users* 容器中的 cn=William Thompson)。

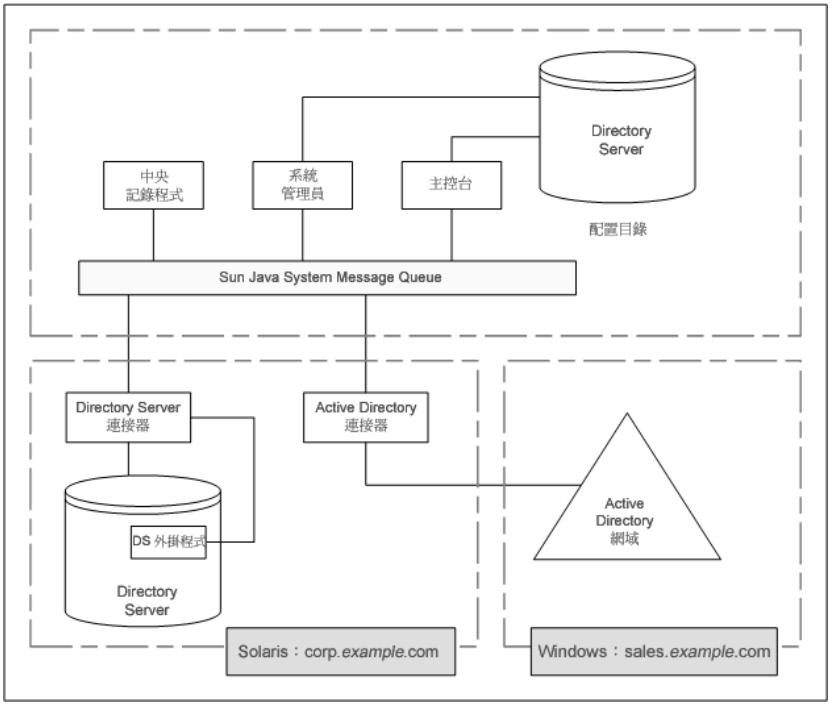
附註 Identity Synchronization for Windows 支援相同類型的多同步化來源 (例如，您可以在一個部署或多個 Active Directory 網域中有多個 Directory Server)。

建立、修改和刪除同步化設定對整個目錄集是整體性的，並且無法爲個別目錄來源專門指定。如果您將 Sun 中的使用者物件建立作業同步化到 Windows，則使用者物件建立作業將從安裝時配置的*所有* Sun Directory Server 傳播到*所有* Active Directory 網域和 Windows NT 網域。

實體部署

圖 1-10 說明了當 Active Directory 網域位於尚未安裝元件的另一 Active Directory 網域控制器中時，本產品的所有元件在一個 Solaris 方塊中的實體部署情況。

圖 1-10 Directory Server 和 Active Directory 方案



元件分佈

主機 *corp.example.com* 是安裝在 Solaris 作業系統中的 Directory Server。要同步化的 Directory Server 的根字尾是 *dc=corp,dc=example,dc=com*。

該電腦包含：

- Identity Synchronization for Windows 核心元件
- Identity Synchronization for Windows Directory Server 連接器
- Identity Synchronization for Windows Directory Server 外掛程式
- Identity Synchronization for Windows 配置目錄 (位於將不進行同步化的另一 Directory Server 實例中)

主機 *sales.example.com* 是要同步化的 Active Directory 網域。

第 2 章

準備安裝

在安裝 Identity Synchronization for Windows 1 2004Q3 或從 1.0 版遷移到 1 2004Q3 版之前，您應該熟悉安裝和配置程序。

本章描述以下程序說明並提供準備安裝產品時可能會有幫助的其他資訊。內容分作以下各節：

安裝需求

本節描述 Identity Synchronization for Windows 的安裝需求，其中包含作業系統版本、修補程式和用於各平台的公用程式。

作業系統需求

下表說明這個版本的 Identity Synchronization for Windows 對作業系統的需求：

表格 2-1 Solaris 需求

元件	Solaris 需求
核心元件	Solaris 8™ for UltraSPARC® (32 位元與 64 位元) Solaris 9™ SPARC® Platform Edition (32 位元與 64 位元) Solaris 9™ 作業系統 (Pentium II 或更高效能系統所用的 x86 平台版) IA-32
Sun Java™ System Directory Server 和 Windows Active Directory 所用的連接器	Solaris 8 for UltraSPARC (32 位元和 64 位元) SPARC 平台所用的 Solaris 9 (32 位元與 64 位元) Solaris 9 作業系統 (Pentium II 或更高效能系統所用的 x86 平台版) IA-32
Sun Java™ System Directory Server 的外掛程式	Solaris 8 for UltraSPARC (32 位元和 64 位元) SPARC 平台所用的 Solaris 9 (32 位元與 64 位元) Solaris 9 作業系統 (Pentium II 或更高效能系統所用的 x86 平台版) IA-32

表格 2-2 Windows 需求

元件	Windows 需求
核心元件	Windows 2000 Server SP4 Windows 2000 Advanced Server SP4
	Windows 2003 Server 標準版 (備有最新的安全性更新)
	Windows 2003 Server 企業版 (備有最新的安全性更新)
Sun Java™ System Directory Server 和 Windows Active Directory 所用的連接器	Windows 2000 Server SP4 Windows 2000 Advanced Server SP 4
	Windows 2003 Server 標準版 (備有最新的安全性更新)
	Windows 2003 Server 企業版 (備有最新的安全性更新)
Sun Java™ System Directory Server 的外掛程式	Windows 2000 Server SP4 Windows 2000 Advanced Server SP 4
	Windows 2003 Server 標準版 (備有最新的安全性更新)
	Windows 2003 Server 企業版 (備有最新的安全性更新)
NT 連接器與子元件	Windows Primary Domain Controller NT 4.0 Server SP 6A (僅適用於 x86)

硬體需求

您的硬體 (所有平台) 必須符合下列最低需求，才能執行 Identity Synchronization for Windows：

- Directory Server 上的最小安裝需要大約 400 MB 的 磁碟空間。
- 執行任何 Identity Synchronization for Windows 元件的伺服器至少需要 512 MB 的 RAM。(最好有更多的記憶體)

Sun Java System 軟體需求

在安裝 Identity Synchronization for Windows 之前，必須安裝下列 Sun Java System 軟體元件：

- Sun Java System Directory Server version 5 2004Q2 修補程式 117907-02 (或更高版本)

  修補程式的更正使 Identity Synchronization for Windows 1 2004Q2 的 Directory Server 5 2004Q2 可使用刪除功能。

  - **Solaris SPARC 套裝軟體格式**：修補程式編號 117907-02 或更高
  - **以 Solaris SPARC 壓縮的保存檔安裝**：修補程式 5077789
  - **Solaris x86 套裝軟體格式**：修補程式編號 117908-02 或更高
  - **以 Solaris x86 壓縮的保存檔安裝**：修補程式 5077789
  - **以 Windows 壓縮的保存檔安裝**：修補程式 5077789

  如需有關上述修補程式以及如何將它們套用到您的 Directory Server 環境的詳細資訊，請參閱位於 Identity Synchronization for Windows 下載目錄中的 `README.patch` 檔案，路徑如下：

  <download_root>`/patches/directory/README.patch`

  有關在 Solaris 系統上安裝 Directory Server 5 2004Q2 可能需要的修補程式之最新資訊，請參閱 *《Sun Java System Directory Server 5 2004Q2 Installation and Tuning Guide》*以及 *《Sun Java System Directory Server 5 2004Q2 版本說明》*，可於以下網站找到這些資訊：

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

- Sun Java System Message Queue (之前稱爲 Sun ONE Message Queue) version 3.5 SP1 Enterprise Edition。

附註	Identity Synchronization for Windows 1.0 版會附帶安裝 Message Queue，*但是版本 1 2004Q3 則不會*。 若要在*現有的* Sun Java System Message Queue 安裝中安裝 Identity Synchronization for Windows 核心元件，必須使用 Message Queue version 3.5 SP1 Enterprise Edition。如果嘗試在不正確的 Message Queue 版本上安裝核心元件，安裝將會失敗。

Identity Synchronization for Windows 下載服務包中包含 Message Queue。此軟體在各個平台的 /messagequeue 目錄下提供，如下所示：

- **Solaris SPARC**：/messagequeue/imq3_5-ent-solsparc.zip
- **Solaris x86**：/messagequeue/imq3_5-ent-soli386.zip
- **Windows**：/messagequeue/imq3_5-ent-win.exe

- Java Runtime Environment

  本產品並沒有隨附 Java Runtime Environment (JRE)。

  - 您必須安裝 J2SE (或 JRE) 1.4.2_04 (或更新) 才能在 Solaris 或 Windows 上執行 Identity Synchronization for Windows 安裝程式。
  - 您必須在 Windows NT 上安裝 JRE 1.4.1_03 (或更新版本)。

安裝憑證

若要安裝 Identity Synchronization for Windows，您必須提供下列憑證：

- 配置目錄
- 同步化的 Directory Server
- Active Directory (詳細資訊，請參閱 「安裝核心程式」。)

此外，您必須具有下列權限才能安裝 Identity Synchronization for Windows：

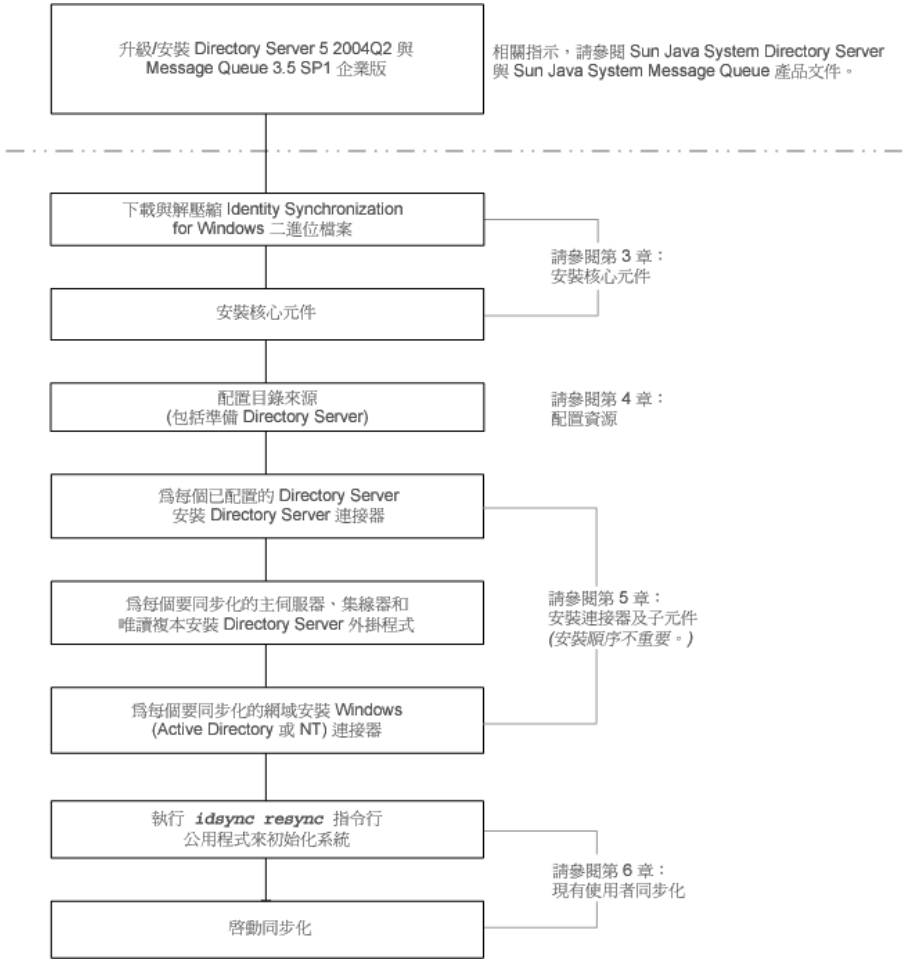
- **Solaris 系統**：您必須以*超級使用者身份*安裝。
- **Windows 系統**：您必須以*管理員身份*安裝。

附註 當您使用文字模式的安裝程式輸入密碼時，程式會自動遮罩密碼，使其不至於以明文顯示。只有 Solaris 系統才支援文字模式的安裝程式。

安裝概觀

圖 2-1 說明了針對單一主機部署安裝產品的程序。

圖 2-1 在單一主機部署中安裝



某些元件必須以特定順序安裝，請確定您已仔細閱讀所有的安裝說明。

Identity Synchronization for Windows 提供一份「待辦事項」清單，整個安裝與配置過程中都會顯示這份清單。此資訊畫面會列出爲了順利安裝及配置本產品您必須執行的所有步驟。

圖 2-2 Identity Synchronization for Windows 待辦事項清單

當您執行安裝及配置流程時，本程式會使清單上所有已完成的步驟呈現灰色 (正如您在圖 2-2 看到的一樣)。

本節的其他部分提供關於安裝和配置程序的概觀，主題分述如下：

- 第 60 頁上的「安裝核心元件」
- 第 60 頁上的「配置產品」
- 第 60 頁上的「備妥 Directory Server」
- 第 61 頁上的「安裝連接器和 Directory Server 外掛程式」
- 第 62 頁上的「現有使用者同步化」

附註 詳細的安裝及配置說明請見本手冊稍後的章節。

安裝核心元件

安裝核心元件時，您將會安裝下列元件：

- **主控台**：爲執行所有的產品元件配置和管理工作提供一個集中位置
- **中央記錄程式**：將所有稽核和錯誤記錄資訊匯集在一個中央位置
- **系統管理員**：向連接器動態傳送配置更新並維護每個連接器的狀態

附註 有關安裝核心元件的說明收錄在第 3 章，「安裝核心程式」。

配置產品

安裝核心元件後，便可以使用主控台來初始配置統一要從一個集中位置進行同步化的目錄來源 (和部署的其他特性)。

附註 有關配置目錄來源的說明收錄在第 4 章，「配置核心資源」。

備妥 Directory Server

Directory Server 連接器支援 Sun Java System Directory Server 5 2004Q2。

在您安裝 Directory Server 連接器之前，您必須爲每個即將同步化的已配置 Directory Server 主伺服器 (優先和輔助主伺服器兩者) 準備 Sun Java System Directory Server 來源。

您可以從主控台或從指令行使用 `idsync prepds` 子指令來執行此工作。

附註 有關準備目錄來源的說明收錄在第 113 頁上的「準備 Directory Server」。

安裝連接器和 Directory Server 外掛程式

可以安裝任意數量的連接器和 Directory Server 外掛程式，視您系統內已配置目錄的數量而定。

附註 主控台和安裝程式兩者都是使用目錄的*標籤*使連接器與要同步化的目錄聯結在一起。表格 2-3 說明 Identity Synchronization for Windows 的標籤命名慣例。

表格 2-3 標籤命名慣例

連接器類型	目錄來源標籤	子元件
Directory Server 連接器	根字尾或字尾 / 資料庫	Directory Server 外掛程式 爲要同步化的根字尾在每個 Directory Server (主伺服器或用戶) 中安裝一個外掛程式。
AD 連接器	網域名稱	無
NT 連接器	網域名稱	(隨 Window NT 連接器自動安裝) 變更偵測器與密碼篩選器 DLL 子元件會在同一次安裝中一起被安裝。 您必須使用圖形化使用者介面 (GUI) 安裝程式來安裝 Windows NT 連接器。

附註 有關安裝及配置連接器和 Directory Server 外掛程式的說明收錄在第 5 章，「安裝連接器與 Directory Server 外掛程式」中。

現有使用者同步化

在安裝連接器、外掛程式、子元件後，您必須執行 `idsync resync` 指令行公用程式以驅動現有使用者的部署。這項指令使用管理者指定的比對規則來

- 連結現有項目 (如需瞭解*連結*的定義，請參閱第 180 頁上的「連結使用者」。)
- 將遠端目錄的內容填入空的目錄中
- 批量同步化兩個現有使用者個體群之間的屬性值 (包括密碼)，其中 Windows 和 Directory Server 目錄兩者內的項目都互相唯一識別並連結。

附註 有關同步化部署中現有使用者的說明收錄在第 6 章，「現有使用者同步化」。

配置概況

在安裝產品後，必須配置產品部署，其中包括：

- 配置要同步化的目錄和通用類別目錄
- 指定用於屬性修改和物件啓動 / 停止作用的同步化設定
- 爲已配置目錄之間的 (選用) 使用者項目建立和刪除指定同步化設定值

本節提供下列配置元素概念的概觀：

- 第 63 頁上的「目錄」
- 第 63 頁上的「配置目錄和通用類別目錄」
- 第 64 頁上的「同步化設定」
- 第 64 頁上的「物件類別」
- 第 65 頁上的「屬性和屬性對映」
- 第 67 頁上的「同步化使用者清單」

附註 詳細的配置說明請見本手冊稍後的章節。

目錄

目錄代表：

- 一個或多個 Sun Java System Directory Server 之中的單一根字尾 (字尾/資料庫)
- Windows 2000 或 Windows 2003 Active Directory 群中的單一 Active Directory 網域
- 單一 Windows NT 網域

對於每一目錄類型，可以配置任意數量的目錄。

配置目錄和通用類別目錄

Identity Synchronization for Windows 使用 Sun Java System Directory Server 配置目錄和 Active Directory 通用類別目錄作爲儲存庫，於其中擷取 Directory Server 或 Active Directory 目錄拓樸以及這些目錄的綱目資訊。

同步化設定

使用同步化設定可控制物件建立、物件刪除、密碼和其他屬性修改在 Sun 和 Windows 目錄之間傳播的方向。同步化流程選項如下：

- 從 Sun 到 Windows
- 從 Windows 到 Sun
- 雙向

附註 在包含 Active Directory 和 Windows NT 的配置中，對於 Windows NT 和 Sun 之間以及 Active Directory 和 Sun 之間的建立或修改操作，不可能儲存一項指定不同的同步化設定的配置。

物件類別

配置資源時，您將根據資源的*物件類別*來指定要同步化的項目。物件類別確定了哪些*屬性*可用於針對 Directory Server 和 Active Directory 二者進行同步化。

附註 物件類別不適用於 Windows NT。

Identity Synchronization for Windows 支援兩種物件類型：

- **結構性物件類別**：凡是依據所選的 Directory Server 建立或同步化的每一項目，都必須擁有至少一個結構性物件類別。請從下拉清單中選取結構性物件類別。(*在 Directory Server 上預設爲 inetorgperson*，在 Active Directory 上預設爲 *User*)
- **輔助物件類別**：
  - **Directory Server** 可讓您從「可用的輔助物件類別」清單窗格中選取一個或多個物件類別來擴大選取的結構性類別，這可爲同步化提供額外的屬性。
  - **Active Directory** 對輔助物件類別的限制較多。所選結構性物件類別之所有有效輔助物件類別中的屬性都可以用於同步化。

附註 有關配置物件類別與屬性的詳細資訊，請參閱第 4 章，「配置核心資源」。

屬性和屬性對映

屬性保有關於使用者項目的描述性資訊。每個屬性都有一個標籤和一個或多個值，並遵循標準語法，該語法適用於可儲存爲屬性值的資訊類型。

附註 可從主控台定義屬性。有關如何定義屬性的說明收錄在第 4 章。

屬性類型

Identity Synchronization for Windows 同步化*重要*和*建立*使用者屬性，如下所示：

- **重要屬性**：當屬性被修改時，根據指定的修改同步化設定在 Sun 和 Windows 目錄之間進行同步化。
- **建立屬性**：當建立新使用者時，根據指定的物件建立同步化設定在 Sun 和 Windows 目錄之間進行同步化。

  *必要建立屬性*是於目標目錄中成功完成建立作業所需的「必要」屬性。例如，Active Directory 預期 `cn` 和 `samaccountname` 在發生建立事件時都具備有效值。在 Sun 端，如果將 `inetorgperson` 配置爲 `user` 物件類別，Identity Synchronization for Windows 將認爲 `cn` 和 `sn` 是建立的必要屬性。

*僅*當從起始目錄傳播來的屬性中沒有值時，建立屬性預設才以預設值更新目標目錄建立屬性。(建立屬性的預設值可視其他屬性值而定。請參閱第 66 頁上的「參數化的屬性預設值」。)

附註 重要屬性會自動同步化爲建立屬性，反之則不行。建立屬性只在使用者建立期間同步化。

參數化的屬性預設值

Identity Synchronization for Windows 可讓您利用其他建立或重要屬性，爲建立屬性建立*參數化*的預設值。

若要建立參數化的預設屬性值，您必須在表示式字串中內嵌一個現有的建立或重要屬性名稱，並在其前後加上百分比符號 (%<*attribute_name*>%)。例如，`homedir=/home/%uid%` 或 `cn=%givenName%. %sn%`。

建立這些屬性預設值時：

- 您可以在建立表示式中使用多個屬性 (`cn=%givenName% %sn%`)，但 `%<`*attribute_name*`>%` 中的屬性必須只有單個值。
- 若 `A=%B%`，則 `B` 只能有一個預設值。
- 您可以使用反斜線符號 (\) 來表示引用 (例如，`diskUsage=0\%`)。
- 請勿使用具有循環代入條件的表示式 (例如，`sn=%uid%` 和 `uid= %sn%`)。

對映屬性

在您定義要同步化的屬性後，必須在 Sun 和 Windows 系統間對映屬性名稱。例如，必須對映 Sun `inetorgperson` 屬性到 Active Directory `user` 屬性。

附註 您對重要和建立屬性使用屬性對映，且必須爲每個目錄類型中的所有「必要建立屬性」配置屬性對映。

同步化使用者清單

建立同步化使用者清單 (SUL) 可定義 Sun 和 Windows 目錄兩者中要同步化的指定使用者。這些定義可使平型目錄資訊樹 (DIT) 同步化到階層式目錄樹。

以下概念用於定義同步化使用者清單：

- **基本 DN** (不適用於 Windows NT)：包含該 DN 中的所有使用者，除非另有更精確的 SUL 或是被篩選器排除。
- **篩選器**：使用使用者項目中的屬性將使用者排除於同步化之外，或是將具有相同基本 DN 的使用者分散爲多個 SUL。此篩選器使用的是 LDAP 篩選語法。
- **建立表示式** (不適用於 Windows NT)：在建立新使用者之處建構 DN，例如 `cn=%cn%,ou=sales,dc=example,dc=com`，其中 `%cn%` 將被更換爲現有使用者項目中的 `cn` 值。建立表示式必須以基本 DN 結尾。

SUL 包含兩個定義，其中每個定義都確定根據目錄類型的拓樸概念要同步化的使用者群組。

- 一個定義確定要同步化的 Directory Server 使用者 (例如：`ou=people, dc=example, dc=com`)
- 另一個定義確定要同步化的 Windows 使用者 (例如：`cn=users, dc=example, dc=com`)

當您準備建立 SUL 時，請詢問自己下列問題：

- 要同步化哪些使用者？
- 要排除哪些使用者於同步化之外？
- 新使用者應建立於何處？

附註 有關建立 SUL 的詳細資訊，請參閱附錄 D。

遷移到 1 2004Q3 版

從 Identity Synchronization for Windows 1.0 版 (或是版本 1.0 SP1) 進行遷移所使用的程序與第一次進行 1 2004Q3 安裝使用的程序相似，除了少數例外。

附註 遷移程序收錄在第 7 章中

在遷移到 Identity Synchronization for Windows 1 2004Q3 之前，應該注意以下事項：

- 安裝連接器之後，必須手動還原 Directory Server 連接器狀態檔案以及 Active Directory 和 NT 連接器物件快取檔案。請確定磁碟空間 (根據 `/isw-home/persist` 目錄和子目錄的大小來判定) 足以儲存各個 Active Directory 與 NT 連接器物件快取的複本。
- 您必須解除安裝所有的 1.0 和 1.0 SP1 版元件。

  如果 1 2004Q3 版安裝程式找到版本 1.0 系統殘留的元件，可能會導致安裝於 Directory Server 的 Identity Synchronization for Windows 網目和安裝在機器上的實際 Identity Synchronization for Windows 二進位碼檔案出現問題。

  附註 有關詳細資訊，請參閱第 209 頁上的「解除安裝 1.0 失敗時之處理」。

- 您必須將 Identity Synchronization for Windows 1 2004Q3 元件安裝在與先前使用 1.0 版時的相同平台及硬體架構中。

與 Active Directory 同步化密碼

Windows 2000 的預設密碼策略在 Windows 2003 已經變更，以預設強制執行嚴格的密碼。

Identity Synchronization for Windows 服務一定會偶爾建立不需要密碼的項目 (例如，在從 Directory Server 到 Active Directory 執行 `resync -c` 操作時)。因此，如果在 Active Directory (於 Windows 2000 或 2003 上) 或是 Directory Server 上啓用了密碼策略，可能會導致使用者建立錯誤。

雖然您不必停用 Active Directory 或 Directory Server 上的密碼策略，但應該瞭解在不同系統上強制執行密碼策略的相關問題。

如果您要與 Windows 2003 Server 標準版或企業版上的 Active Directory 同步化密碼，那麼下列安裝資訊就非常重要：

- 如果您要在 Windows 上安裝，則可將 Active Directory 連接器安裝在 Solaris 上。

  附註 Active Directory 連接器可與 Windows 2000 和 Windows 2003 Server 上的 Active Directory 配合使用。

- 在 Windows 2003 Server 上建立目錄來源、通用類別目錄與同步化使用者清單的程序與在 Windows 2000 上爲 Active Directory 建立目錄來源、通用類別目錄與同步化使用者清單使用的程序相同。
- 在 Windows 2003 Server 上，預設的密碼策略會強制執行嚴格的密碼設定方法，但 Windows 2000 上的預設密碼策略卻不是這樣。

此章節的剩餘部分將如下組織：

- 第 70 頁上的「強制執行密碼策略」：若您必須對 Windows 或 Directory Server 強制執行密碼策略，請閱讀此章節提供的資訊，以瞭解密碼策略會如何影響 Active Directory 與 Directory Server 之間的同步化結果。
- 第 75 頁上的「密碼策略範例」：本節提供了好幾種不同情況下使用的密碼策略範例。

強制執行密碼策略

本節說明 Windows 2003 Server、Windows 2000 和 Sun Java System Directory Server 5 2004Q2 中用於 Active Directory 的密碼策略會如何影響同步化結果。

內容歸納如下：

概況

如若您於 Active Directory (或 Directory Server) 上建立的使用者符合該系統需要的密碼策略，則會建立使用者且正確地同步化於兩個系統間。若您在兩個系統上皆啓用密碼策略，則密碼必須符合兩個系統的策略，否則將無法同步建立使用者。

- 若您於 Active Directory 上啓用了密碼策略功能，則應該在 Directory Server 上啓用相似配置或相符的密碼策略。
- 若您無法在 Active Directory 與 Directory Server 上建立一致的密碼策略，則您應該在您認爲是密碼與使用者建立的主導來源的一端啓用密碼策略。然而，仍然會因爲某些密碼策略配置，而出現幾種會讓使用者建立作業無法如預期執行的情形。

重要附註

以下小節提供了有關密碼策略的重要資訊：

Directory Server 密碼策略

如果您在 Active Directory 中以違反 Directory Server 密碼策略的密碼建立使用者，*將*在 Directory Server 中建立並同步化這些使用者，但建立的項目不會有密碼。直到新的使用者登入 Directory Server 中 (這將觸發隨需密碼同步化) 時才會設定密碼。此時，登入將會失敗，因爲該密碼違反了 Directory Server 密碼策略。

有數種方法可以從這個情況恢復正常：

- 在使用者下次登入 Active Directory 時強制他們變更密碼

- 變更 Active Directory 上的使用者密碼，並確保新密碼符合 Directory Server 密碼策略的要求

您可能想要查看 Active Directory 與 Directory Server 上設定的密碼策略是否相同 (或盡可能相似)。

Active Directory 密碼策略

若您在 Active Directory 上建立不符合 Active Directory 密碼策略的使用者，則這些使用者*將*建立於 Directory Server。

- 若密碼不符合密碼策略需求，則 Active Directory 實際上只是「暫時」建立使用者，之後會刪除相關項目。因此，Active Directory 連接器會看到此暫時的 `ADD` 並在 Directory Server 端建立使用者。使用者將不會擁有 Directory Server 的密碼，所以沒有人可以用使用者身份登入。另外，這些項目將不會連結至 Active Directory 中的有效項目。如果刪除操作是從 Active Directory 同步化到 Directory Server，則暫時建立的使用者會被自動刪除。
- 在 Directory Server 上建立使用者時不使用密碼。對於建立使用者，Directory Server 不會強制執行密碼策略，除非這些項目包含密碼。

有數種方法可以從這個情況恢復正常。最好是將刪除操作從 Active Directory 同步化到 Directory Server。或者是將使用者從 Directory Server 中移除，然後使用符合 Active Directory 密碼策略的有效密碼將其新增至 Active Directory。這個方法能確保將使用者建立於 Directory Server，並正確連結。Directory Server 上的使用者在第一次登入 Active Directory 時，密碼將無效，因而必須變更密碼。

- 若您不從 Directory Server 刪除使用者，且在之後嘗試使用新密碼再次新增 Active Directory 使用者，則 Directory Server 的 `ADD` 作業將失敗，因爲使用者已存在於 Directory Server 上。項目將不會連結在一起，且您將必須執行 `idsync resync` 指令來連結兩個獨立的帳號。
- 若您執行 `idsync resync` 指令，則必須爲連結至 Directory Server 項目的 Active Directory 帳號重設密碼。重設密碼會使 Directory Server 密碼無效，在下次當這些使用者用其新的 Active Directory 密碼進行 Directory Server 驗證時，將強制執行依要求同步化作業以更新 Directory Server 密碼。

建立無密碼的帳號

在某些情況下（例如重新同步化時），Identity Synchronization for Windows 必須建立無密碼的帳號。

Directory Server　當 Identity Synchronization for Windows 在 Directory Server 中建立無密碼的項目時，它會將 `userpassword` 屬性設爲 `{PSWSYNC}*INVALID*PASSWORD*`。該使用者將無法登入 Directory Server，直到您重設密碼爲止。這有一種例外情況，就是當您以 `-i NEW_USERS` 或 `NEW_LINKED_USERS` 選項執行 `resync` 時。在這種情況下，resync 會使新使用者的密碼失效，並在該使用者下次登入時觸發隨需密碼同步化。

Active Directory　當 Identity Synchronization for Windows 在 Active Directory 中建立沒有密碼的項目時，它會將使用者的密碼設爲隨機選取的強式密碼，此密碼符合 Active Directory 密碼策略的要求。在這種情況下，會記錄一則警告訊息，該使用者將無法登入 Active Directory，直到您重設密碼爲止。

下表說明當您使用 Identity Synchronization for Windows 時可能會遇到的一些不同情況：

- 表格 2-4 說明密碼策略如何影響同步化。
- 表格 2-5 說明密碼策略如何影響重新同步化。

可這些資訊作爲指南，以幫助確定密碼將保持同步化。(因爲系統配置的不同，這些表格不可能說明全部可能的配置情況。)

表格 2-4 密碼策略如何影響同步化行爲

情況			結果		
建立使用者的原始位置	**使用者符合的密碼策略**		**使用者建立於**		
	Directory Server	**Active Directory**	**Directory Server**	**Active Directory**	**註解**
Active Directory	是	是	是	是	
	是	否	**是 (請參閱註解)**	否	使用者將於 Directory Server 中建立。不過，如果刪除操作是從 Active Directory 同步化到 Directory Server，則會立即刪除此使用者。 請參閱第 71 頁上的「Active Directory 密碼策略」以瞭解詳細資訊。
	否	是	**是**	是	請參閱第 70 頁上的「重要附註」以瞭解詳細資訊。
	否	否	**是 (請參閱註解)**	否	使用者於 Directory Server 中建立。不過，如果刪除操作是從 Active Directory 同步化到 Directory Server，則會立即刪除此使用者。 請參閱第 71 頁上的「Active Directory 密碼策略」以瞭解詳細資訊。
Directory Server	是	是	是	是	
	是	否	是	否	
	否	是	否	否	
	否	否	否	否	

表格 2-5 密碼策略如何影響重新同步化行爲

	情況		
Resync 指令	**使用者符合的密碼策略**		**結果**
	Directory Server	**Active Directory**	
`resync -c -o Sun`	不適用	是	使用者將於 Active Directory 中建立，但該使用者無法登入。 請參閱第 72 頁上的「建立無密碼的帳號」以瞭解詳細資訊。
	不適用	否	使用者將於 Active Directory 中建立，但該使用者無法登入。 請參閱第 72 頁上的「建立無密碼的帳號」以瞭解詳細資訊。
`resync -c -i NEW_USERS | NEW_LINKED_USERS`	是	不適用	使用者將於 Directory Server 中建立，且在該使用者首次登入時將設定其密碼。 請參閱第 72 頁上的「建立無密碼的帳號」以瞭解詳細資訊。
	否	不適用	使用者將於 Directory Server 中建立，但他們無法登入，因爲其密碼違反 Directory Server 密碼策略。 請參閱第 70 頁上的「重要附註」與第 72 頁上的「建立無密碼的帳號」以取得詳細資訊。
`resync -c`	是	不適用	使用者將於 Directory Server 中建立，但他們無法登入，直到在 Active Directory 或 Directory Server 中設定了新的密碼值爲止。 請參閱第 72 頁上的「建立無密碼的帳號」以瞭解詳細資訊。
	否	不適用	使用者將於 Directory Server 中建立，但他們無法登入，直到在 Active Directory 或 Directory Server 中設定了新的密碼值爲止。 請參閱第 72 頁上的「建立無密碼的帳號」以瞭解詳細資訊。

密碼策略範例

本節說明使用以下規格的 Active Directory 與 Directory Server 密碼策略範例的不同情況：

- **Active Directory**：
  - 強制密碼歷程記錄：20 天
  - 最長密碼時間：30 天
  - 最短密碼時間：0 天
  - 密碼長度下限：7 個字元
  - 密碼必須符合複雜性要求：啓用
- **Directory Server**：
  - 使用者必須在重設之後變更密碼
  - 使用者可以變更密碼
  - 在歷程記錄中保留 20 個密碼
  - 密碼於 30 天後過期
  - 在密碼過期前 5 天傳送警告
  - 檢查密碼語法：密碼長度下限爲 7 個字元

錯誤訊息

核取「核心」系統的中央記錄程式 `audit.log` 檔案，以取得以下錯誤訊息：

在依要求同步化作業期間因爲密碼策略，無法更新 `DS` 的密碼：

```
WARNING 125 CNN100 hostname "DS Plugin (SUBC100):unable to update password
of entry 'cn=John Doe,ou=people,o=sun', reason:possible conflict with local
password policy"
```

附註 有關 Windows 2003 密碼策略的詳細資訊，請參閱 http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dssсc_aut_xbby.asp

有關 Directory Server 5 2004Q2 密碼策略的詳細資訊，請造訪

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

配置 Windows 以進行 SSL 作業

如果您計畫要將密碼變更從 Directory Server 傳播至 Windows Active Directory 伺服器，您必須配置每一個 Active Directory 伺服器使其使用 SSL，且您必須安裝高度加密的套件。

如果已透過自動從 Microsoft Certificate Services Enterprise Root 憑證授權單位取得證書而在 Active Directory 中啓用 LDAP over SSL，則 Identity Synchronization for Windows Active Directory 連接器安裝程式即可自動在 Active Directory 連接器中設定 SSL，有關憑證授權單位的描述，請造訪：

http://support.microsoft.com/default.aspx?scid=kb;en-us;q247078

不過，您可以利用更簡單的方式配置 LDAP over SSL，配置方式說明於以下 MSDN 技術注意事項中：

http://support.microsoft.com/default.aspx?scid=kb;en-us;321051

在這種情況下，如果您決定索取可靠的憑證來進行 SSL 通訊，則必須手動將憑證安裝在連接器的憑證資料庫中，請參照第 296 頁上的「在 Active Directory 連接器中啓用 SSL」中的說明。

安裝與配置決策

本章節提供有關安裝和配置的摘要資訊，並詳述您在佈署 Identity Synchronization for Windows 時所選擇的選項。請您在開始進行安裝程序前先備妥此資訊。本節包含下列內容：

核心元件安裝

在您安裝核心元件時必須提供下列資訊：

- **配置目錄主機和通訊埠**：指定 Directory Server 實例的配置目錄主機和通訊埠，Identity Synchronization for Windows 配置資訊將會儲存在此 Directory Server 實例上。

  您可指定一個 SSL 通訊埠作爲配置目錄通訊埠；如果您這麼做，就必須在安裝過程中將該通訊埠標示爲 SSL 通訊埠。

附註	Identity Synchronization for Windows 不支援以 `localhost` 形式安裝的配置目錄。

- **根字尾**：指定配置目錄的根字尾。所有的配置資訊都會儲存在此字尾下。
- **管理員的名稱與密碼**：指定配置 Directory Serve 的憑證。
- **配置密碼**：指定安全密碼以保護機密配置資訊的安全。
- **檔案系統目錄**：指定要安裝 Identity Synchronization for Windows 的位置。您必須將核心元件安裝在與 Directory Server Administration Server 相同的目錄中。
- **未使用的通訊埠號**：爲 Message Queue 實例指定可用的通訊埠號碼。

核心元件配置

在您配置核心元件時必須提供下列資訊：

- **Sun Java System Directory 網目伺服器**：指定您想從配置目錄下載的 Directory Server 資料。
- **使用者物件類別 (僅限 Directory Server)**：指定使用者物件類別，系統會使用此類別決定使用者類型。Identity Synchronization for Windows 會根據此物件類別衍生出一份屬性 (包括密碼屬性) 清單。這份清單的內容是從模式中移入的。
- **同步化屬性**：指定要在 Directory Server 和 Windows 環境中同步化的使用者項目屬性。
- **修改、建立和刪除流程**：指定想要在 Sun 和 Windows 系統間傳播修改、建立和刪除作業的方式。您可以選擇：
  - 從 Sun 到 Windows
  - 從 Windows 到 Sun
  - 雙向

  指定物件啓動和停止作用操作是否要在 Sun 與 Windows 系統間傳播，並且指定同步化這些物件的方法。
- **通用類別目錄**：指定通用類別目錄 (Active Directory 拓樸和網目資訊的儲存庫)。
- **Active Directory 網目控制器**：指定要從 Windows 通用類別目錄擷取之 Active Directory 模式來源的完全符合網域名稱 (FQDN)。
- **配置目錄**：指定用來儲存 Identity Synchronization for Windows 配置的 Directory Server。
- **Active Directory 來源**：指定用來同步化 Active Directory 網域的來源。
- **Windows NT 主要網域控制器**：指定要同步化的 Windows NT 網域以及每一個網域之「主要網域控制器」的名稱。
- **同步化使用者清單**：使用 LDAP DIT 和篩選條件資訊來指定要在 Directory Server、Active Directory 和 NT 上同步化的使用者。
- **Sun Java System Directory Server**：指定用來儲存要同步化之使用者的 Directory Server 實例。

連接器和 Directory Server 外掛程式安裝

在您安裝連接器和 Directory Server 外掛程式時必須提供下列資訊：

- **配置目錄主機和通訊埠**：指定 Directory Server 實例的配置目錄主機和通訊埠，Identity Synchronization for Windows 配置資訊將會儲存在此 Directory Server 實例上。
- **根字尾**：指定配置目錄的根字尾。使用安裝核心元件時指定的根字尾。
- **管理員的名稱與密碼**：指定配置 Directory Serve 的憑證。
- **配置密碼**：指定安全密碼以保護機密配置資訊的安全。
- **檔案系統目錄**：指定要安裝 Identity Synchronization for Windows 的位置。安裝在同一台電腦上的所有元件都必須具有相同的安裝路徑。
- **目錄來源**：指定想要爲其安裝連接器或外掛程式的目錄來源。

如果要安裝 Directory Server 和 Windows NT 連接器，就必須指定未使用的通訊埠。

如果要安裝 Directory Server 連接器和外掛程式，就必須指定對應於該連接器和外掛程式的 Directory Server 的主機、通訊埠和憑證。

使用指令行公用程式

Identity Synchronization for Windows 可讓您使用下列公用程式從指令行執行各式作業：

- 搭配使用 `idsync` 程序檔和下列子指令來執行 Identity Synchronization for Windows 指令行公用程式：
  - `certinfo`：根據您的配置和 SSL 設定值顯示憑證資訊
  - `changepw`：變更 Identity Synchronization for Windows 配置密碼
  - `prepds`：準備 Sun Java System Directory Server 來源供 Identity Synchronization for Windows 使用
  - `printstat`：列印安裝的連接器、系統管理員和 Message Queue 的狀態

    您也可以使用 `printstat` 指令來顯示完成安裝過程必須執行之剩餘安裝和配置步驟的清單。
  - `resetconn`：將配置目錄中的連接器狀態重設爲*未安裝*(僅限於發生硬體或解除安裝程式故障時)
  - `resync`：重新同步化和連結現有使用者並在安裝過程中預先填寫目錄
  - `startsync`：啓動同步化
  - `stopsync`：停止同步化

附註 有關這些公用程式的詳細資訊，請參閱附錄 A。

- 您可以使用下列公用程式從 Identity Synchronization for Windows 1.0 或 1.0 SP1 遷移到 Identity Synchronization for Windows 1 2004Q3：
  - `forcepwchg`：要求爲在 Identity Synchronization for Windows 1.0 版到 1 2004Q3 版遷移期間變更了其密碼的使用者變更密碼
  - `importcnf`：將匯出的 1.0 版 XML 配置文件匯入

附註 有關這些公用程式的詳細資訊，請參閱第 7 章。

安裝核對清單

這些核對清單的目的是協助您進行安裝。請將它們列印出來並在安裝 Identity Synchronization for Windows 前記錄下列資訊。

表格 2-6 核心元件安裝核對清單

必要資訊	項目
配置目錄主機和通訊埠	
配置目錄的根字尾。(如 dc=example、dc=com)	
要安裝 Identity Synchronization for Windows 的檔案系統目錄	
配置 Directory Server 的管理員名稱和密碼	
用來保護機密配置資訊的安全配置密碼	
Message Queue 實例的通訊埠號	

表格 2-7 核心元件配置核對清單

必要資訊	項目
Active Directory 通用類別目錄 (如果有)	
Directory Server 模式伺服器	
Directory Server 使用者結構和輔助物件類別。	
同步化屬性	
使用者項目的建立流程	
使用者項目的修改流程	
啓動和停止作用使用者項目的流程	
使用者項目的刪除流程	
Sun Java System Directory Server 目錄來源	
Active Directory 目錄來源	
同步化使用者清單	
Windows 來源篩選器建立表示式	
Sun Java System 來源篩選器建立表示式	

表格 2-8 連接器和 Directory Server 外掛程式安裝核對清單

必要資訊	項目
配置目錄主機和通訊埠	
配置目錄的根字尾。	
要安裝連接器的檔案系統目錄	
配置 Directory Server 的管理員名稱和密碼	
用來保護機密配置資訊的安全配置密碼	
目錄來源	
Directory Server 與 Windows NT 的未使用通訊埠	
對應於連接器和外掛程式的 Directory Server 的主機、通訊埠和憑證	

表格 2-9 連結使用者核對清單

必要資訊	項目
要連結的同步化使用者清單。	
用來比對等同使用者的屬性	
XML 配置檔案	

表格 2-10 重新同步化核對清單

必要資訊	項目
同步化使用者清單選項。	
同步化來源。	
如果在目標目錄來源沒有找到對應使用者，是否要自動建立一個使用者項目？	
是否要使 Directory Server 密碼無效？	
是否僅同步化符合指定 LDAP 篩選器且位於選定 SUL 中的使用者？	

第 3 章

安裝核心程式

本章說明如何使用 Identity Synchronization for Windows 安裝程式及如何安裝 Identity Synchronization for Windows 核心元件。

內容分作以下各節：

準備工作

啓動 Identity Synchronization for Windows 安裝程序之前：

- 請詳讀第 2 章，「準備安裝」。本章包含重要資訊，例如安裝工作的先決條件、檢查清單以及管理員權限需求。
- 本產品並沒有隨附 Java Runtime Environment (JRE)。
  如果需要，您可以從下列位置下載 Java Development Kit：

  `http://java.sun.com` 或 `http://www.java.com`

  您必須安裝 JRE 1.4.2_04 (或更新) 才能在 Solaris 或 Windows 2000/2003 系統上執行 Identity Synchronization for Windows 安裝程式。
- **只有 Windows 系統**：您必須先關閉任何開啓的「服務控制台」視窗才能啓動核心程式的安裝程式，否則安裝會失敗。
- 如果您的機器上還安裝有 Identity Synchronization for Windows 1.0 版 (或 1.0 SP1)，請詳讀第 7 章，「遷移至 Identity Synchronization for Windows 2004Q3」。

附註 如果 SUNWjss 套裝軟體未註冊供 Identity Synchronization for Windows 1.0 以外的其他應用程式使用，則 Identity Synchronization for Windows 1.0 解除安裝程式會移除該套裝軟體。這種情形特別容易發生在當您在 Solaris 電腦上安裝 Directory Server 5.2.2 的壓縮版本時，此時解除安裝程式會將 `jss3.jar` 檔案從 `/usr/share/lib/mps/secv1` 移除。

如果您在遷移至 Identity Synchronization for Windows 11 2004Q3 時遇到這種情形，安裝程式將會回報缺少一個必要檔案，並將該檔案的名稱記錄在安裝日誌中。發生這種情形時，您必須重新安裝必要的修補程式 (請參閱第 56 頁上的「Sun Java System 軟體需求」) 並重新啓動安裝程序。

- Identity Synchronization for Windows 1.0 版會附帶安裝 Message Queue，*但是版本 1 2004Q3 則不會*。您應該已經安裝 Message Queue 3.5 SP1 Enterprise Edition。

  Solaris 系統：請勿將 Message Queue 和 Identity Synchronization for Windows 安裝在相同的目錄中。

啓動安裝程式

本節說明如何下載、解壓縮 (或 unzip)，並在下列平台上執行 Identity Synchronization for Windows 安裝程式：

- 第 85 頁上的「Solaris SPARC 系統」
- 第 85 頁上的「Solaris x86 系統」
- 第 86 頁上的「Windows 系統」

Solaris SPARC 系統

使用下列步驟在 Solaris SPARC 作業系統上準備並執行 Identity Synchronization for Windows 安裝程式：

1. 以超級使用者身份登入。
2. 鍵入 **# mkdir isw12004Q3**，來建立新目錄，然後切換 (**cd**) 到該目錄。
3. 如果您尚未這麼做，請下載本產品的二進位碼檔案 (`isw-12004Q3.sparc-sun-solaris.tar.gz`) 到安裝目錄。
4. 使用下列指令解壓縮產品二進位碼檔案：

   ```
   # gunzip -dc isw-12004Q3.sparc-sun-solaris.tar.gz | tar -xvof -
   ```

5. 從 `isw12004Q3` 目錄切換到 `installer` 目錄，然後鍵入 **./runInstaller.sh** 執行安裝程式。

附註 若要以文字模式執行安裝程式，鍵入

```
./runInstaller.sh -nodisplay
```

當您執行 `runInstaller.sh` 程式時，Identity Synchronization for Windows 會自動遮罩密碼，使其不至於以明文顯示。

Solaris x86 系統

使用下列步驟在 Solaris x86 作業系統上準備並執行 Identity Synchronization for Windows 安裝程式：

1. 以超級使用者身份登入。
2. 鍵入 **# mkdir isw12004Q3**，來建立新目錄，然後切換 (**cd**) 到該目錄。
3. 如果您尚未這麼做，請下載本產品的二進位碼檔案 (`isw-12004Q3.x86-sun-solaris.tar.gz`) 到安裝目錄。
4. 使用下列指令解壓縮產品二進位碼檔案：

   ```
   # gunzip -dc isw-12004Q3.x86-sun-solaris.tar.gz | tar -xvof -
   ```

5. 從 isw12004Q3 目錄切換到 installer 目錄，然後鍵入 **./runInstaller.sh** 執行安裝程式。

附註 若要以文字模式執行安裝程式，鍵入

./runInstaller.sh -nodisplay

當您執行 runInstaller.sh 程式時，Identity Synchronization for Windows 會自動遮罩密碼，使其不至於以明文顯示。

Windows 系統

使用下列步驟在 Windows 作業系統準備並執行 Identity Synchronization for Windows 安裝程式：

1. 以管理員身份登入。
2. 鍵入 **# mkdir isw12004Q3** 來建立新目錄
3. 切換 (**cd**) 到 isw12004Q3 目錄。
4. 如果您尚未這麼做，請下載本產品的二進位碼檔案 (isw-12004Q3-windows.zip) 到安裝目錄。
5. 解壓縮 isw-12004Q3-windows.zip 檔案到空白目錄。
6. 從 isw12004Q3 目錄，透過 **cd** 指令切換到 installer 目錄，然後鍵入 **setup.exe** 執行安裝程式。

   Identity Synchronization for Windows 安裝精靈隨即出現。

附註 因爲您在 Administration Server 根目錄安裝核心程式，Identity Synchronization for Windows 精靈將偵測安裝需要的大部分資訊 (例如目錄路徑和名稱) 並自動填寫精靈畫面中的某些欄位。

如果資訊遺漏或不正確，您可手動輸入需要的資訊。

請繼續進入下一節，瞭解核心程式的安裝說明。

安裝核心程式

本節說明安裝 Identity Synchronization for Windows 核心程式到 Solaris 和 Windows 兩個作業系統上的程序。

在您安裝核心程式前，應該注意下列需求：

- **Solaris 系統**：您必須具有超級使用者權限才能安裝並執行 Solaris 服務。

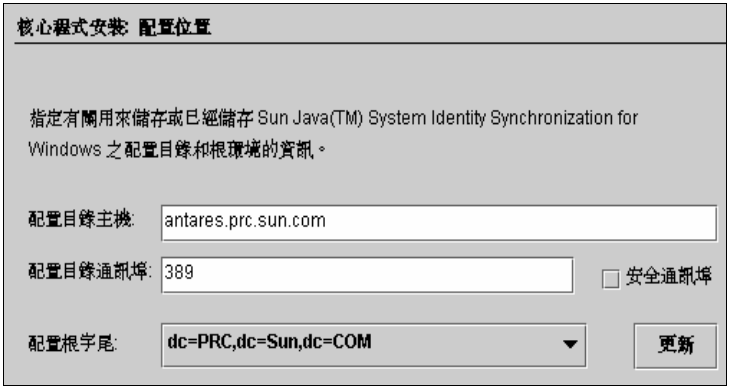
  附註 您必須以超級使用者身份來安裝本程式，但安裝好之後，即可配置軟體，使其以非超級使用者身份來執行 Solaris 服務。(請參閱附錄 C，「以非超級使用者身份在 Solaris 系統上執行服務」。)

- **Windows 2000/2003 系統**：您必須具有管理員權限才能安裝 Identity Synchronization for Windows。
- 您必須安裝核心程式到具有現存伺服器根目錄 (由管理伺服器所管理，伺服器版本 5 2004Q2 或更高) 的目錄中，否則安裝程式將失敗。(您可以使用 Directory Server 5 2004Q2 安裝程式安裝 Administration Server)

以下爲使用安裝精靈安裝 Identity Synchronization for Windows 核心元件的步驟：

1. 出現歡迎畫面時，閱讀其中的資訊並按「下一步」進入「軟體授權合約」畫面。
2. 閱讀授權合約內容後，選取：
   - **「是」(接受授權合約)** 表示接受授權條款並進入下一個畫面。
   - **「否」**表示停止安裝程序並結束安裝程式。
3. 將顯示「配置位置」畫面 (圖 3-1)，可讓您指定配置目錄位置。

圖 3-1 指定配置目錄位置



提供下列資訊：

- **配置目錄主機**：輸入將儲存 Identity Synchronization for Windows 配置資訊的 Sun Java System Directory Server 實例 (其與本機 Administration Server 相關) 之完全合格的網域名稱 (FQDN)。

  您可以指定在本機電腦上的實例或是執行在其他機器上的實例。

  附註 爲了避免出現無效憑證或主機名稱的警告，請確定指定的主機名稱對執行安裝程式的機器是可以透過 DNS 解析的。

- **配置目錄通訊埠**：指定要用來安裝配置目錄的通訊埠。(*預設通訊埠爲 389*。)

  若要啓用安全通訊，請啓用「安全通訊埠」選項並指定一個 SSL 通訊埠。(*預設 SSL 通訊埠爲 636*。)

  一旦程式確定配置目錄啓用了 SSL，所有 Identity Synchronization for Windows 元件將使用 SSL 來與配置目錄之間進行通訊。

附註 在將敏感配置資訊傳送到配置 Directory Server 之前，Identity Synchronization for Windows 會將其加密。

不過，如果您想要在主控台和配置目錄之間實現額外的傳輸加密，請務必對 Administration Server 和配置 Directory Server 兩者啓用 SSL。然後，配置與 Administration Server 間的安全連線，您將要向 Administration Server 驗證 Directory Server 主控台。(有關資訊，請參閱 *《Sun Java System Administration Server5 2004Q2 管理指南》*。)

- **配置根字尾**：從功能表選取要用來儲存 Identity Synchronization for Windows 配置的根字尾。

附註 如果程式偵測不到根字尾，需要手動輸入資訊 (或是變更預設值) 時，您必須按一下「更新」以重新產生根字尾清單。(您必須指定存在於配置 Directory Server 的根字尾。)

4. 按一下「下一步」開啓「配置目錄憑證」畫面。

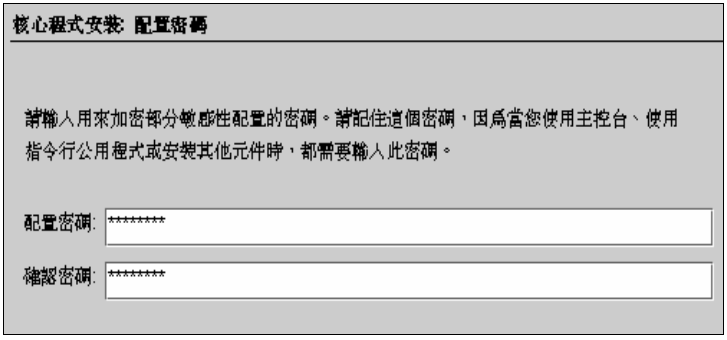
圖 3-2 指定管理員憑證

5. 輸入配置目錄管理員的使用者 ID 及密碼。
   - 若指定 `admin` 作爲使用者 ID，無需將使用者 ID 指定爲 DN。
   - 若使用任何其他的使用者 ID，則必須將 ID 指定爲完整的 DN。例如 *cn=Directory Manager*。

附註 如果您不使用 SSL 來與配置目錄進行通訊 (請參閱第 88 頁的步驟 3)，這些憑證將在不加密的情況下傳送。

6. 當您完成後，按一下「下一步」開啓「配置密碼」畫面。

圖 3-3 指定配置密碼



7. 您必須輸入並確認一個將用於加密敏感性配置資訊 (例如憑證) 的密碼。完成後按一下「下一步」。

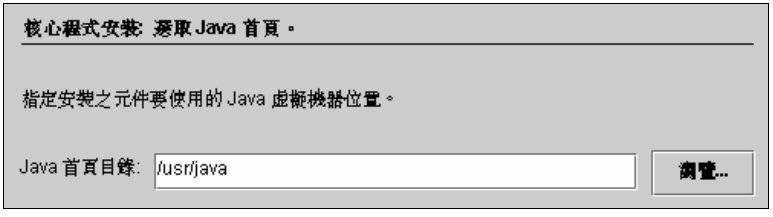
附註 務必記住此密碼，因爲在您要執行以下操作時，會需要它

- 進入 Identity Synchronization for Windows 主控台
- 建立或編輯配置
- 安裝元件
- 執行任何指令行公用程式

有關變更配置密碼的資訊，請參閱第 311 頁上的「使用 changepw」。

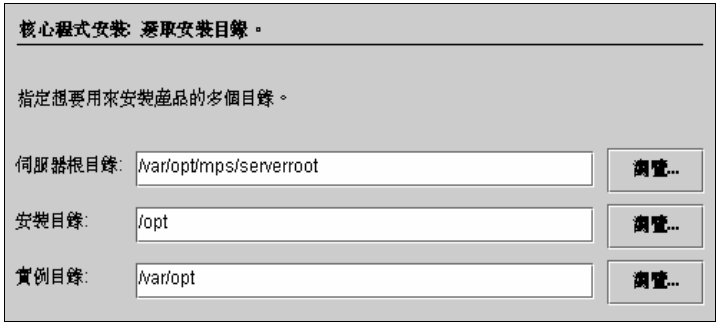
出現「選取 Java 首頁」畫面 (請參閱圖 3-4)。本程式會自動插入已安裝元件使用的 Java 虛擬機器目錄的位置。

圖 3-4 指定 Java 首頁目錄



8. 確認 Java 首頁目錄 (必須爲 JDK/JRE 1.4.2_04 或更新)：
   - 如果對位置感到滿意，請按一下「下一步」進入「選取安裝目錄」畫面 (第 92 頁上的圖 3-5)。
   - 如果位置不正確，請按一下「瀏覽」搜尋並選取 Java 的安裝目錄，例如：
     - **Solaris 系統**：`/var/java`
     - **Windows 系統**：`C:\Program Files\j2sdk1.4.2_04`

圖 3-5 指定安裝目錄



9. 在提供的文字欄位輸入下列資訊，或是按一下「瀏覽」搜尋並選取可用目錄：

- **伺服器根目錄**：指定 Directory Server 安裝伺服器根目錄的路徑和目錄名稱。主控台將安裝在此位置。

  附註 在 Windows 作業系統上只有一個伺服器根目錄有效，並且所有的產品都將安裝於該位置。

- **安裝目錄** (*只有在 Solaris 系統上安裝核心程式時才能使用*)：指定安裝目錄的路徑和目錄名稱。核心二進位碼檔案、程式庫和可執行檔將安裝在此位置。
- **實例目錄** (*只有在 Solaris 系統上安裝核心程式時才能使用*)：指定實例目錄的路徑和目錄名稱。變更的配置資訊 (例如日誌檔) 將儲存在此目錄。

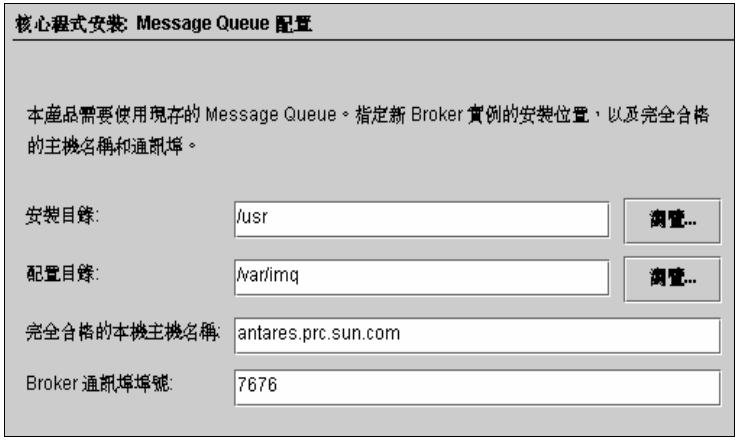
10. 按一下「下一步」進入「Message Queue 配置」畫面。

附註 在 Identity Synchronization for Windows 安裝開始之前，您應該安裝 Message Queue 3.5 SP1 Enterprise Edition。

Solaris 系統：請勿將 Message Queue 和 Identity Synchronization for Windows 安裝在相同的目錄中。

Windows 系統：您必須先關閉任何開啓的「服務控制台」視窗才能繼續進行，否則核心程式的安裝會失敗。

圖 3-6 配置 Message Queue



11. 在提供的文字欄位輸入下列資訊，或是按一下「瀏覽」搜尋並選取可用目錄：

- **安裝目錄**：指定 Message Queue 安裝目錄的路徑。
- **配置目錄**：指定 Message Queue 實例目錄的路徑和目錄名稱。
- **完全合格的本機主機名稱**：指定本機主機電腦的完全合格的網域名稱 (FQDN)。(每個主機只能執行一個 Message Queue 代理程式實例。)
- **Broker 通訊埠埠號**：指定未使用的通訊埠埠號，供 Message Queue 代理程式使用。(*預設通訊埠爲 7676*。)

12. 按一下「下一步」會出現「準備安裝」畫面。

    此畫面提供關於安裝的資訊，例如核心程式將安裝的目錄以及安裝核心程式需要的空間。

    - 如果對顯示的資訊滿意，按一下「立即安裝」安裝核心程式元件 (安裝程式會安裝二進位碼、檔案和套裝軟體)。
    - 如果資訊不正確，按一下「上一步」修改。

    系統會簡略地顯示「安裝中」訊息，然後「元件配置」畫面顯示，同時安裝程式將配置資料加入指定的配置 Directory Server 中。此作業包括：

    - 建立 Message Queue 代理程式實例
    - 將模式上傳至配置目錄
    - 將部署專用配置資訊上傳至配置目錄

    此作業將花費數分鐘並可能偶爾暫停，除非程序超過十分鐘，否則請不用擔心。(觀察進度列可監控安裝程式的狀態。)

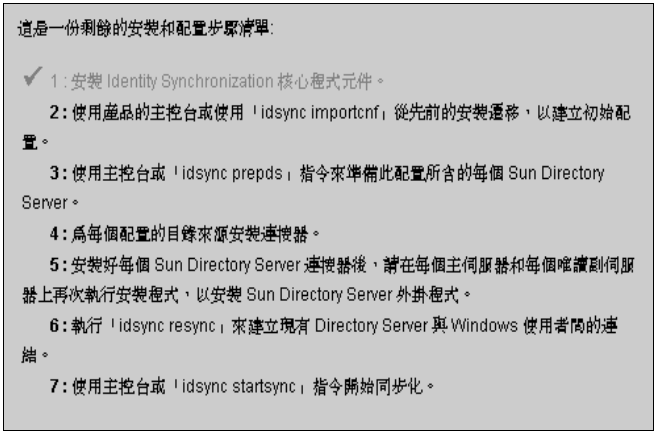
13. 當元件配置作業完成時，「安裝摘要」畫面會顯示，確認 Identity Synchronization for Windows 已成功安裝。

    您可按一下「詳細資訊」按鈕，查看已安裝的檔案之清單以及安裝之處。

14. 按一下「下一步」，程式將確定您必須執行哪些步驟才能成功地安裝及配置 Identity Synchronization for Windows。

出現「載入中 ...」訊息，接下來每個畫面都會簡略地顯示「剩餘的安裝步驟」，然後顯示下列畫面 (圖 3-7)。此畫面中的「待辦事項」清單內包含剩餘的安裝和配置步驟。(從主控台的「狀態」標籤也可以存取此畫面。)

圖 3-7 Identity Synchronization for Windows 待辦事項清單

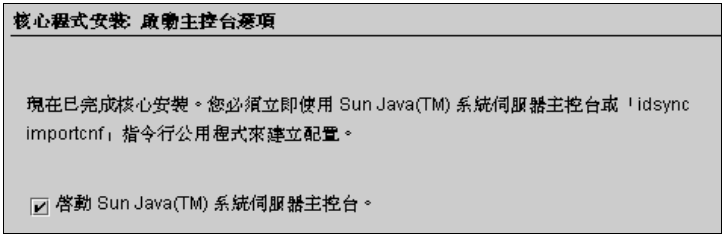


「待辦事項」畫面在安裝和配置過程中會不斷地重複出現。本程式會使清單中所有已完成的步驟呈灰色顯示。

直至目前爲止，「待辦事項」清單內包含的都是一般步驟。在您儲存配置之後，本程式會爲您的部署提供一份自訂的步驟清單 (例如，必須安裝哪些連接器)。

15. 詳讀完步驟清單後，按一下「下一步」，「啓動主控台選項」畫面即顯示，指出您已經完成核心程式的安裝。

圖 3-8 啓動主控台



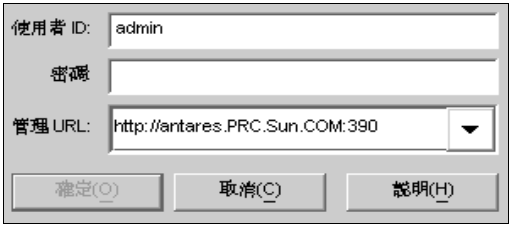
16. 接下來，您必須配置核心元件，您可從 Sun Java System 主控台進行配置 (依照預設，「啓動 Sun Java System 主控台」*選項是啓動的*)。

    如果您要從 Identity Synchronization for Windows 1.0 版或 SP1 遷移至 Identity Synchronization for Windows 1 2004Q3，則可使用 `idsync importcnf` 指令行公用程式將匯出的 1.0 或 SP1 版 XML 配置文件匯入。(有關說明，請參閱第 7 章，「遷移至 Identity Synchronization for Windows 1 2004Q3」。)

17. 按一下「完成」。

18. 如果您決定使用主控台，將顯示 Sun Java System 主控台登入對話方塊 (請參閱圖 3-9)。

圖 3-9 登入主控台



您必須輸入下列資訊才能登入主控台：

- **使用者 ID**：輸入您安裝 Administration Server 到電腦上時指定的管理員使用者 ID。
- **密碼**：輸入 Administration Server 安裝期間指定的管理員密碼。
- **管理 URL**：以下列格式輸入 Administration Server 目前的 URL 位置：

  http://<*hostname.your_domain.domain:port_number*>

  此處：

  - *hostname.your_domain.domain* 是您安裝 Administration Server 時選取的電腦主機名稱。
  - *port_number* 是您指定給 Administration Server 的通訊埠。

19. 在提供憑證後，按一下「確定」關閉對話方塊。
20. 您會被提示輸入配置密碼。輸入密碼後按一下「確定」。

當顯示 Sun Java System Server 主控台視窗時，您可以啓動配置核心。請接著看第 4 章，「配置核心資源」之說明。

第 4 章

配置核心資源

當您安裝了 Identity Synchronization for Windows 核心程式 (詳如第 3 章之說明) 後，必須先立即配置核心資源。

本章解釋如何使用「主控台」新增及配置各項資源，內容分作以下各節：

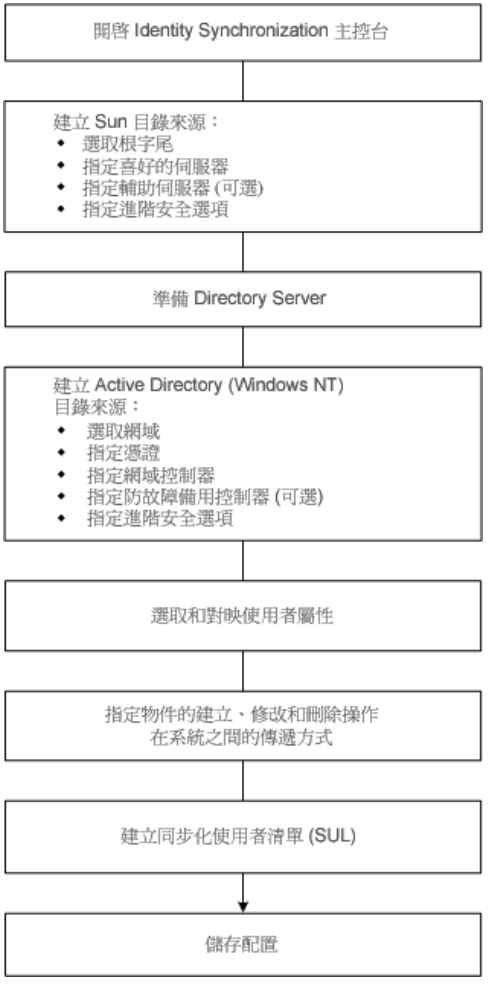
附註 爲能有效配置核心資源，您必須知道如何配置及操作 Directory Server 與 Active Directory。

配置這類資源時無需依照特定順序 (除非有文字特別指示)，不過在您熟悉產品前，仍請參照本章所示的順序進行配置，如此可節省時間並避免出錯。

配置概況

圖 4-1 說明了爲部署配置核心資源時所需使用的步驟。

圖 4-1 爲部署配置核心資源



開啓 Identity Synchronization for Windows 主控台

附註 如果您尚未登入 Sun Java System Server 主控台，請回到第 96 頁閱讀說明。

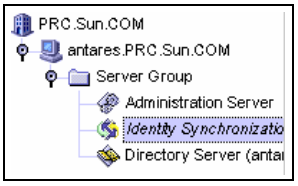
Sun Java System Server 主控台視窗 (圖 4-2) 列出了您控制下的所有伺服器，並提供了您的系統的相關資訊。

圖 4-2 Sun Java System 伺服器主控台

若要開啓 Identity Synchronization for Windows 主控台：

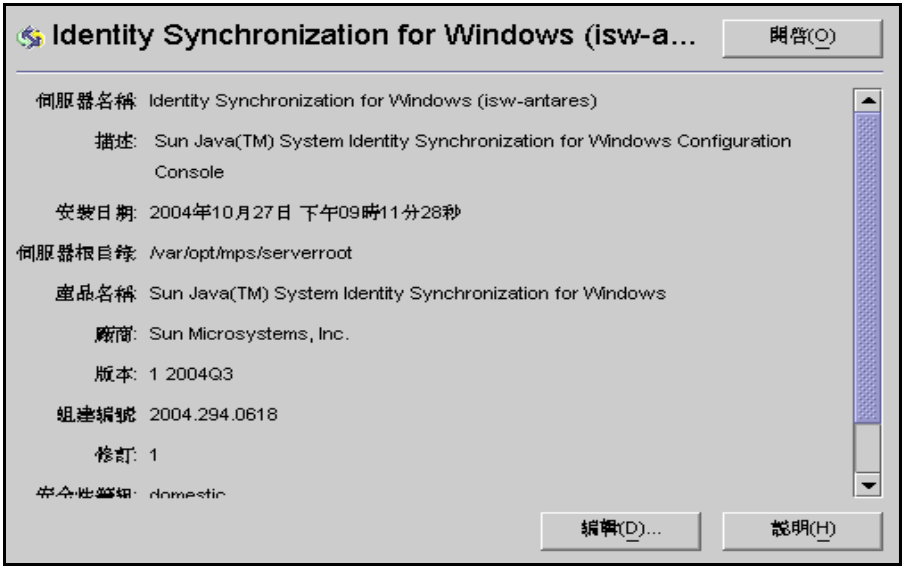
1. 在「伺服器與應用程式」標籤上，從導覽樹中選取包含 Identity Synchronization for Windows 實例所屬的「伺服器群組」的主機名稱節點。
2. 展開「伺服器群組」節點，選取其中的 Identity Synchronization for Windows 節點 (請參閱圖 4-3)。

圖 4-3 展開伺服器群組



資訊畫面改爲提供有關 Identity Synchronization for Windows 及您的系統的資訊 (示例請參閱圖 4-4)。

圖 4-4 Identity Synchronization for Windows 資訊畫面



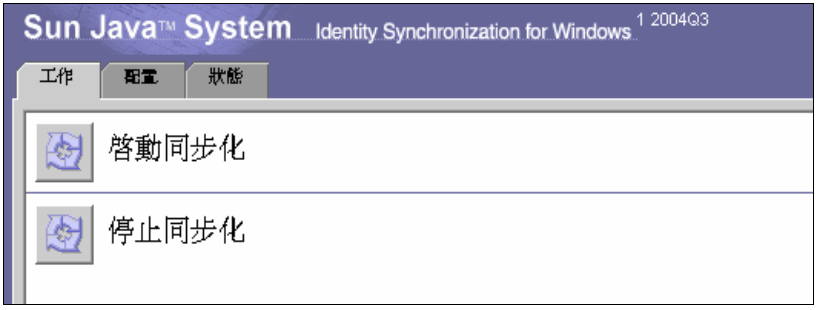
3. 按一下「開啓」按鈕 (位於畫面右上角)。

附註 (位於畫面底部的)「編輯」按鈕可用來編輯「伺服器名稱」及「描述」。

4. 系統會提示您輸入您在安裝核心時所指定的配置密碼 (請參閱第 90 頁)。輸入密碼後按一下 「確定」。

   Identity Synchronization for Windows 主控台隨即顯示，畫面如下：

圖 4-5 Identity Synchronization for Windows 主控台：「工作」標籤



此視窗含有三個標籤及一個狀態列：

- **工作** (*預設*)：使用此標籤來停止或啓動 Sun 與 Windows 系統間的同步操作。(有關啓動及停止服務的資訊收錄在第 6 章，「現有使用者同步化」。)

  附註 啓動及停止同步服務不等於啓動及停止 Windows 服務，請勿混淆。

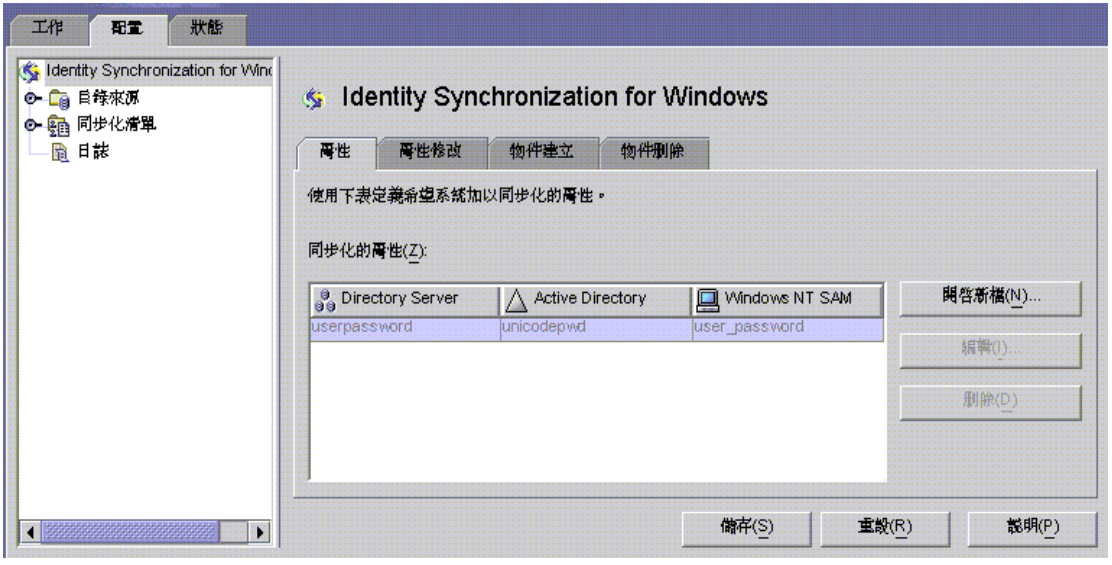
  若要啓動或停止 Windows 服務，必須透過 Windows 控制台進行，步驟是選取 「開始」 > 「控制台」 > 「系統管理工具」 > 「電腦管理」 > 「服務」。

- **配置**：透過此標籤來配置要同步化的系統。
- **狀態**：使用此標籤來執行下列動作：
  - 監視系統元件 (如連接器等) 的狀態。
  - 於配置及同步化過程中檢視 Identity Synchronization for Windows 所產生的稽核及錯誤日誌。
  - 更新與檢查 「待辦事項」清單的安裝和配置。
  - **狀態列**：由此處檢查系統的大致狀態。

  附註 有關 「狀態」標籤的詳細資訊，請參閱第 10 章。

5. 選取「配置」標籤 (請參閱圖 4-6)。

圖 4-6 Identity Synchronization for Windows 主控台：「配置」標籤



「配置」畫面包含以下標籤：

- **屬性**：使用此標籤來指定要在系統間同步的屬性。
- **屬性修改**：使用此標籤來指定密碼、屬性修改項目與物件停用項目在系統間傳播的方式。
- **物件建立**：使用此標籤來指定新建的密碼及屬性在系統間傳播的方式，以及指定同步化過程中由 Identity Synchronization for Windows 所產生的物件之初始值。
- **物件刪除**：使用此標籤來指定已刪除的密碼及屬性在系統間傳播的方式。

您必須配置至少一個 Sun Java System Directory Server 目錄來源，以及至少一個 Windows 伺服器目錄來源 (Active Directory 或 Windows NT 之一)。請前進至下一節，瞭解操作說明。

建立目錄來源

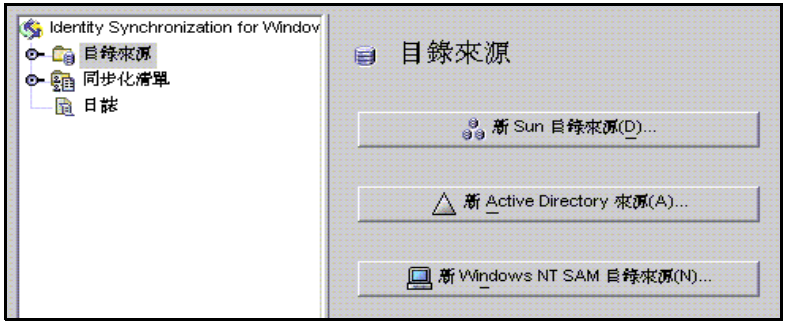
請務必依照下列順序建立目錄來源 (根據您要同步化的來源而定)：

1. 第 106 頁上的「建立 Sun Java System 目錄來源」
2. 第 113 頁上的「準備 Directory Server」
3. 第 117 頁上的「建立 Active Directory 來源」
4. 第 125 頁上的「建立 Windows NT SAM 目錄來源」

附註 最低限度，您必須配置至少一項 Sun Java System 目錄來源和至少一項 Windows 目錄來源 (Active Directory 和 / 或 NT SAM)。

在導覽樹中選取 「目錄來源」節點，即出現 「目錄來源」畫面 (請參閱圖 4-7)。

圖 4-7 進入「目錄來源」畫面



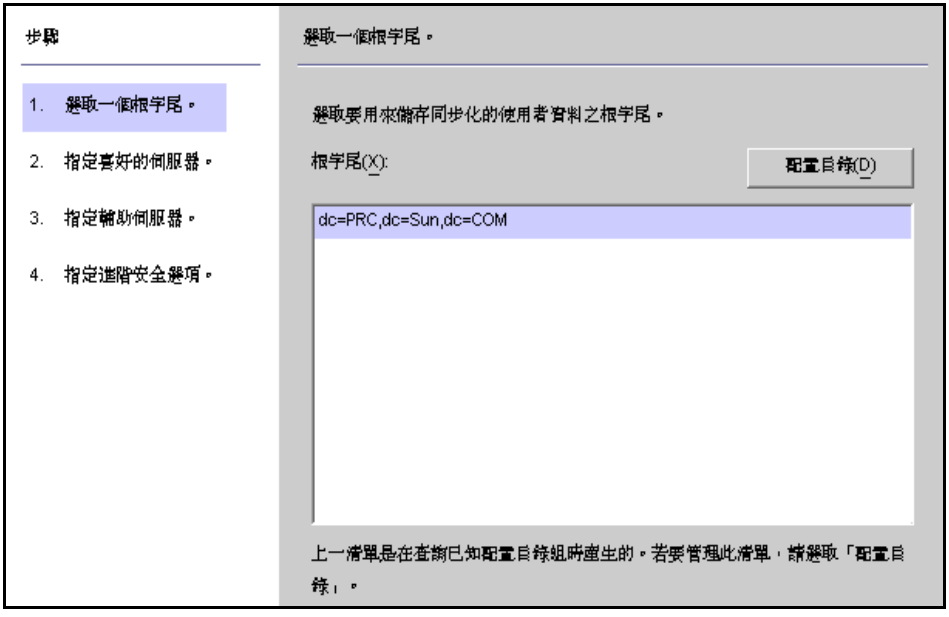
建立 Sun Java System 目錄來源

附註 每一項 Sun Java System 目錄來源均聯結至一個連接器和一組外掛程式，可在最多可有四台主伺服器的複製方案中部署這些外掛程式。任何 Directory Server 外掛程式都可從 Windows 目錄來源處理密碼有效性檢查，使用者可在任何主伺服器上變更密碼，不過，Directory Server 連接器最多只能對兩台（喜好的或輔助的）主伺服器同步化來自 Windows 目錄來源的變更。Directory Server 複製作業會將這兩台主伺服器的任一台伺服器所做的變更，複製到拓樸中的其他伺服器。

請依下列步驟新建立一個 Sun Java System 目錄來源：

1. 按一下「新 Sun 目錄來源」按鈕呼叫執行「定義 Sun Java System 目錄來源」精靈。

圖 4-8 選取一個根字尾



程式會查詢已知的一組配置目錄來源，並將現有的根字尾 (在此亦稱作*命名上下文*) 顯示在清單窗格中。

預設情況下，程式知道您將產品安裝在哪個配置目錄，因此清單窗格會顯示出配置目錄已知的根字尾。

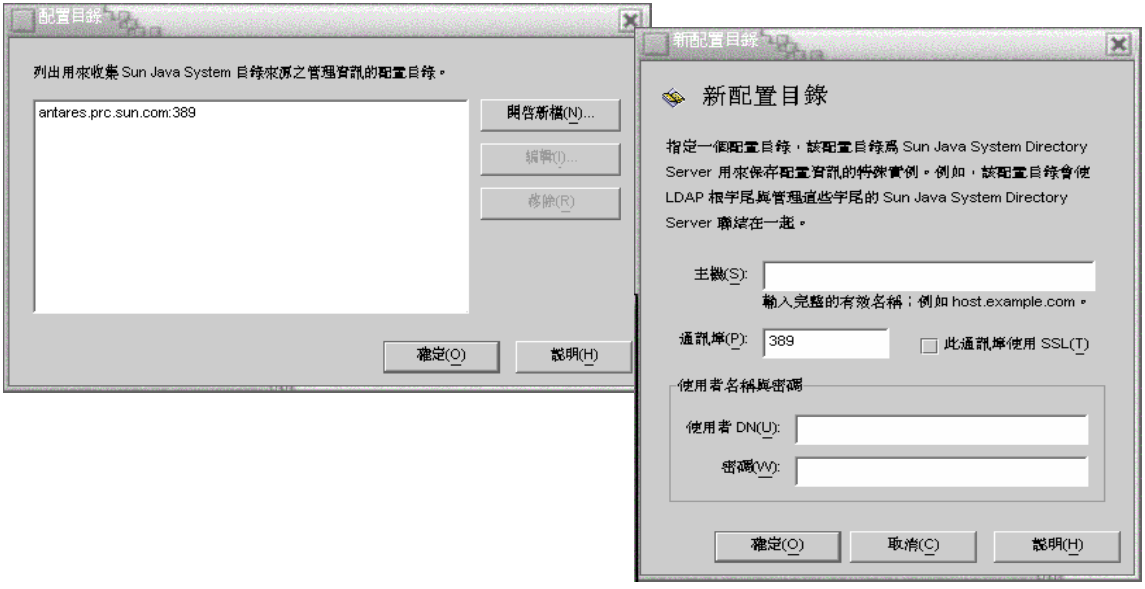
2. 從清單窗格中選取使用者所在的根字尾。(如果列出有數個根字尾，請選取您的使用者所在的根字尾。) 按一下「下一步」繼續進行步驟 3。

   如果您要同步化的根字尾與在 Identity Synchronization for Windows 中註冊的配置目錄不相關，則必須指定一個新的配置目錄，步驟如下：

   a. 按一下「配置目錄」按鈕來指定新的配置目錄。

   b. 出現「配置目錄」對話方塊 (圖 4-9) 後，按一下「開啓新檔」按鈕開啓「新配置目錄」對話方塊。

圖 4-9 選取新的配置目錄



c. 輸入下列資訊後，按一下「確定」儲存變更並關閉該對話方塊。

- **主機**：請輸入完整合格的主機名稱。

  例如：**machine1.example.com**

- **通訊埠**：輸入有效且未使用的 LDAP 通訊埠埠號。(*預設值爲 389*。)

  如果 Identity Synchronization for Windows 透過 SSL (安全資料傳輸層) 通訊埠與配置目錄進行通訊，請啓用「此通訊埠使用 SSL」方塊。

- **使用者 DN**：輸入您的管理員 (連結) 辨別名稱。

  例如：

  uid=admin,ou=Administrators,ou=TopologyManagement,o=NetscapeRoot

- **密碼**：輸入您的管理員密碼。

精靈會查詢您所指定的配置目錄，以確定受該目錄管理的所有目錄伺服器。

附註 Identity Synchronization for Windows 對於各個 Sun Java System Directory Server 來源僅支援一個根字尾。

附註

編輯與移除配置目錄

您亦可透過「配置目錄」對話方塊來管理您的配置目錄清單，步驟如下：

- 從清單窗格中選取配置目錄，然後按一下「編輯」按鈕。出現「編輯配置目錄」對話方塊後，可變更「主機」、「通訊埠」、「安全通訊埠」、「使用者名稱」及「密碼」參數。
- 從清單窗格中選取配置目錄，然後按一下「移除」即可將該目錄從清單中刪除。

---

d. 按一下「確定」關閉「配置目錄」對話方塊，則新選取的配置目錄之根字尾即顯示在清單窗格中。

預設情況下，Directory Server 會建立一個前綴與電腦的 DNS 網域項目元件相對應的根字尾。其使用的字尾如下：

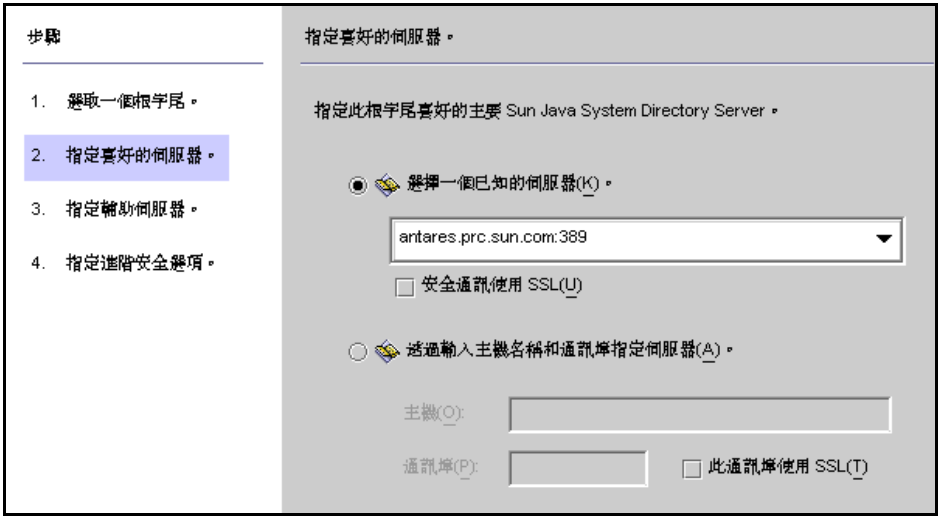
dc=< *您電腦的 _DNS_ 網域 _ 名稱* >

亦即，假設您的電腦網域爲 *example.com*，便應該將伺服器的字尾配置成 `dc=example, dc=com` 。依據選定字尾而命名的網域項目必須已存在於目錄中。

e. 選取根字尾，然後按一下「下一步」。

出現「指定喜好的伺服器」畫面 (請參閱圖 4-10)。

圖 4-10 指定喜好的伺服器



Identity Synchronization for Windows 使用喜好的 Directory Server 來偵測所有 Directory Server 主伺服器所做的變更。該喜好的伺服器同時也是將 Windows 系統上所做的變更套用到 Sun Java System 目錄系統之主要位置。

如果喜好的伺服器發生問題，輔助伺服器可暫時儲存這些變更，直到喜好的伺服器再度上線。

3. 使用下列一個方法來選取喜好的伺服器：

   - 啓用「選擇一個已知的伺服器」按鈕，接著從下拉清單中選取伺服器名稱。

     附註 Directory Server 必須正在執行，才會出現在清單內。假如伺服器暫時處於非作用中，請啓用「透過輸入主機名稱和通訊埠指定伺服器」按鈕，手動輸入伺服器資訊。

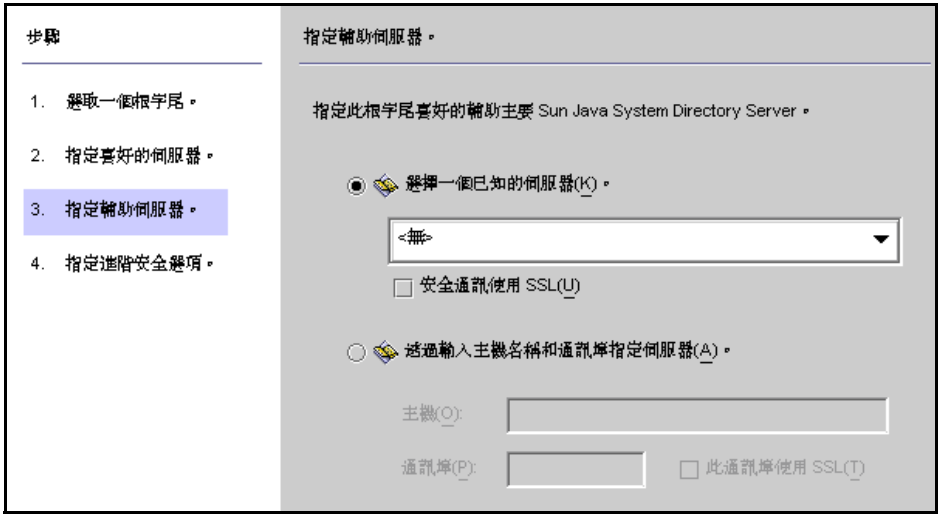
     如要讓 Directory Server 透過 SSL 進行通訊，請啓用「安全通訊使用 SSL」方塊。不過，當您啓用此功能時，必須在安裝後執行某些額外的設定步驟。有關詳細資訊，請參閱第 293 頁上的「在 Directory Server 中啓用 SSL」。

   - 啓用「透過輸入完整合格的主機名稱和通訊埠指定伺服器」按鈕，並於畫面上的伺服器「主機名稱」及「通訊埠」文字欄位中輸入資訊。

     如果您指定的通訊埠使用 SSL，請啓用「此通訊埠使用 SSL」方塊。

4. 按一下「下一步」會出現「指定輔助伺服器」畫面。

圖 4-11 指定輔助伺服器



- 若要指定輔助 Directory Server，請從下拉清單中選取伺服器名稱或手動輸入該資訊 (程序與先前指定喜好的伺服器時相同)，然後按一下「下一步」。

附註 Directory Server 必須正在執行，否則伺服器名稱*不會*出現在下拉清單中。假如伺服器暫時處於非作用中，請手動輸入伺服器資訊。

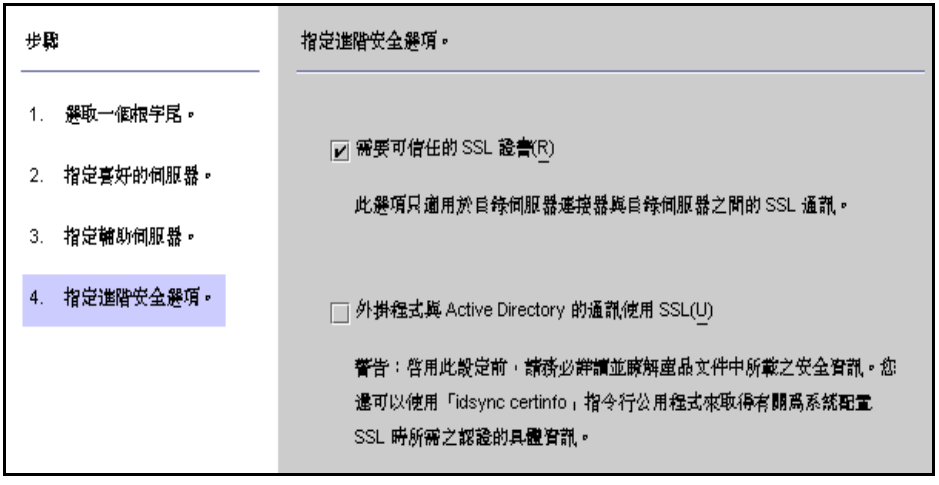
- 如果不想使用輔助伺服器，請直接按一下「下一步」。

附註

- 請勿在同一 Sun 目錄來源中將喜好的和輔助伺服器設爲相同的主機名稱及通訊埠。
- 當您啓用安全通訊埠功能時，必須在安裝後執行額外的設定步驟。有關詳細資訊，請參閱第 293 頁上的「在 Directory Server 中啓用 SSL」。

出現如下「指定進階安全選項」畫面：

圖 4-12 指定進階安全選項



在安裝過程中，您必須在使用者即將連結或要變更密碼的各 Directory Server (任何主伺服器、複本伺服器或集線器) 上安裝 Directory Server 外掛程式。

當 Directory Server 外掛程式要將密碼及屬性同步化至 Active Directory 時，必須連結到 Active Directory 以搜尋使用者及其密碼。此外，外掛程式會將日誌訊息寫入中央日誌及 Directory Server 的日誌。在預設下這些通訊作業不會透過 SSL 進行。

5. 如果想要使用安全的 SSL 通訊，*請詳讀所提供的警告說明*，然後再啓用下列一個或兩個選項：

   - 若只想加密通道通訊，或想加密通道通訊，並使用憑證來驗證 Directory Server 與 Directory Server 連接器間的參與者之身份，請啓用「需要憑證進行 SSL」方塊。

     如果您不想信任憑證，請清除核取方塊。

   - 若要在 Directory Server 外掛程式與 Active Directory 之間使用 SSL 安全通訊，請啓用「使用外掛程式的 SSL 與 Active Directory 進行通訊」方塊。

   附註

   - 如果啓用這些功能，需在安裝後進行額外的設定。請參閱第 11 章，「配置安全性」以瞭解詳細資訊。
   - 您可以使用 `idsync certinfo` 指令行公用程式來確定應將哪些憑證新增到各個 Directory Server 外掛程式及 / 或連接器憑證資料庫。請參閱第 310 頁上的「使用 certinfo」。
   - 如果您的主要及輔助 Directory Server 屬於多主伺服器複製 (MMR) 部署的一部分，請參閱附錄 E，「複製環境的安裝註解」中的詳細說明。

6. 完成「指定進階安全選項」畫面後，按一下「完成」。

   程式便會將所選的目錄來源加入「目錄來源」下的導覽樹中，並顯示「現在備妥 Directory Server？」對話方塊。

   您必須準備 Directory Server 以供 Identity Synchronization for Windows 使用。您可以選擇立即或稍後執行這項工作，但無論如何您必須在安裝連接器之前準備 Directory Server。(有關安裝連接器的說明收錄在第 5 章)。

   - 如要立即準備 Directory Server，請按一下「是」開啓精靈，然後進行下一節的操作，第 113 頁上的「準備 Directory Server」。
   - 如要稍後再執行這一過程，請按一下「否」並繼續進行第 117 頁上的「建立 Active Directory 來源」。

準備 Directory Server

本節說明如何準備 Sun Java System Directory Server 來源以供 Identity Synchronization for Windows 使用。

準備 Directory Server

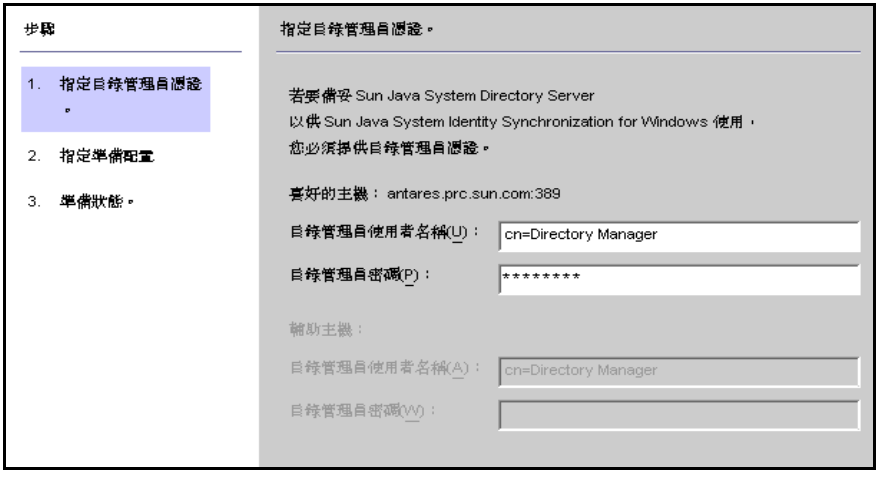
- 在喜好的主機上建立可用的 Retro-Changelog 資料庫及存取控制實例
- 在喜好的主機上建立可用的連接器使用者及使用者存取控制實例
- 在喜好的及輔助的主機上建立平等指數

附註

- 除了使用主控台以外，亦可使用 `idsync prepds` 指令行公用程式來準備 Directory Server。有關詳細資訊，請參閱第 313 頁上的「使用 prepds」。
- 若要使用 `idsync prepds` 指令行公用程式來準備 Directory Server，您必須知道所要使用的主機及其字尾，且必須具備目錄管理員的憑證。

您可以使用「備妥 Directory Server」精靈 (圖 4-13) 來準備 Directory Server。

圖 4-13 輸入您的目錄管理員憑證



若要存取此精靈，請使用下列一個方法：

- 當「現在備妥 Directory Server？」對話方塊顯示時，按一下「是」按鈕。
- 當「Sun 目錄來源」畫面顯示時 (在「配置」標籤上)，按一下「備妥 Directory Server」按鈕。

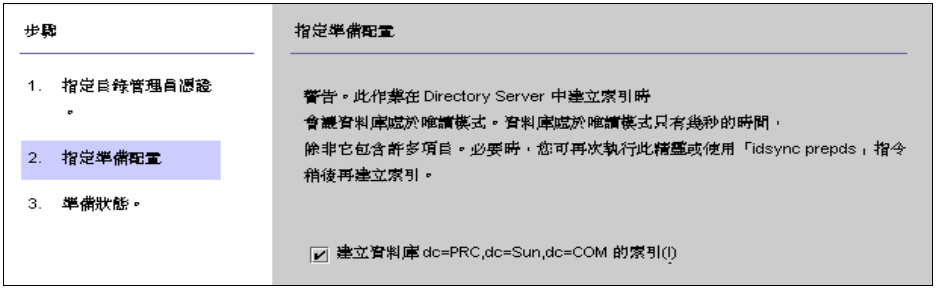
若要準備 Directory Server 來源：

1. 輸入目錄管理員帳戶的下列憑證：
   - **目錄管理員使用者名稱**
   - **目錄管理員密碼**

   如果您使用了輔助主機 (MMR 配置)，「輔助主機」的選項即可供使用，您也必須指定這些主機的憑證。

2. 完成後按一下「下一步」，「指定準備配置」畫面出現 (圖 4-14)。

圖 4-14 指定準備配置



閱讀警告訊息後，決定是否立即或稍後建立 Directory Server 索引。

附註

- 這項作業可能需要幾秒或幾分鐘的時間，視您的資料庫大小而定。
- 若資料庫處於唯讀模式，將無法執行任何資料庫資訊的更新動作。
- 先讓資料庫離線可顯著加快建立索引的速度。

- 如要立即建立索引，請啓用「建立資料庫索引」方塊，然後按一下「下一步」。
- 若要稍後建立索引 (無論是手動建立或再次執行此精靈來建立)，請取消「建立資料庫索引」方塊，然後按一下 「下一步」。

3. 出現 「準備狀態」畫面，提供有關 Directory Server 準備進度的資訊。
   - 當訊息窗格下方出現 「成功」訊息時，請按一下 「完成」。
   - 如果顯示錯誤訊息，則必須將報告的問題修正後才能繼續。請檢查錯誤日誌 (請參閱 「狀態」標籤) 以瞭解詳細資訊。

4. 回到「主控台」的「配置」標籤。選取導覽樹中的 Sun 目錄來源節點來檢視「Sun 目錄來源」畫面 (請參閱圖 4-15)。

圖 4-15 Sun 目錄來源畫面

透過此畫面可執行以下工作：

- **編輯伺服器**：按一下此按鈕再度開啓「定義 Sun Java System 目錄來源」畫面，您可從中變更任何一項伺服器配置參數。必要時，請檢閱「建立 Sun Java System 目錄來源」的說明。
- **備妥 Directory Server**：按一下此按鈕，依照針對第 113 頁上的「準備 Directory Server」的說明來準備 Directory Server。

  如果在初步準備 Directory Server 後發生任何變更 (例如，刪除索引或遺失 Retro-Changelog 資料庫)，您可以重新準備伺服器。

  附註 如果您爲喜好的 Sun 目錄來源重建 Retro-Changelog 資料庫，則預設的存取控制設定將不允許 Directory Server 連接器讀取資料庫內容。

  若要還原新的 Retro-Changelog 資料庫之存取控制設定，請執行 `idsync prepds`，或在「主控台」中選取適當的 Sun 目錄來源，然後按一下「備妥 Directory Server」按鈕。

- **重新同步化間隔**：指定您希望 Directory Server 連接器檢查有否變更的間隔長短。(*預設值爲 1000 毫秒*。)

5. 在您要同步化的 Sun Java System Directory Server 企業中，針對各個使用者個體群分別新增 Directory Server 目錄來源。

新增完畢後，您必須至少建立一個 Windows 目錄來源：

- 若要建立 Active Directory 目錄來源，請接著看下一節第 117 頁上的「建立 Active Directory 來源」。
- 若要建立 Windows NT 目錄來源，請接著看第 125 頁上的「建立 Windows NT SAM 目錄來源」。

建立 Active Directory 來源

您應爲網路中需要同步化的每個 Windows 網域新增一個 Active Directory 目錄來源。

每個 Active Directory 部署至少會有一個通用類別目錄知道全 Active Directory 網域內的所有通用資訊。

附註 每個 Active Directory 伺服器都有可能成爲通用類別目錄，且同一部署下可以包含多個通用類別目錄，但您只需要指定一個通用類別目錄。

您的網路中如有 Windows Active Directory 伺服器，請執行以下步驟：

1. 在導覽樹中選取「目錄來源」節點，然後按一下「目錄來源」畫面中的「新 Active Directory 來源」按鈕。

   出現「Windows 通用類別目錄」對話方塊 (圖 4-16)。

圖 4-16 Windows 通用類別目錄

2. 輸入以下資訊，然後按一下「確定」：

   - **主機**：輸入存有 Active Directory 群的通用類別目錄之電腦的完整合格的主機名稱。

     例如：**`machine2.example.com`**

   - **此通訊埠使用 SSL**：如果 Identity Synchronization for Windows 透過 SSL 通訊埠與通用類別目錄進行通訊，請啓用此選項。

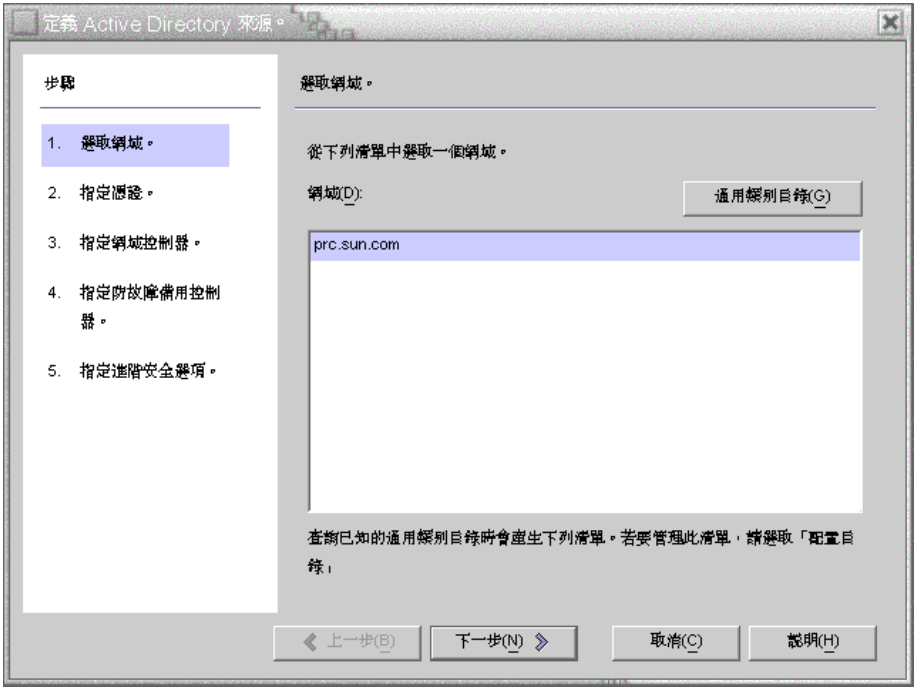
   - **使用者 DN**：輸入您的完整合格的管理員 (連結) 辨別名稱。(只要是能夠讓您瀏覽模式並確定系統上有哪些 Active Directory 網域可用的憑證便可。)

     例如：**`cn=Administrator,cn=Users,dc=example,dc=com`**

   - **密碼**：輸入指定使用者的密碼。

3. 即會顯示「定義 Active Directory 來源」精靈，如下所示：

圖 4-17 定義 Active Directory 來源精靈



此精靈會查詢 Active Directory 通用類別目錄以確定尚有哪些其他網域存在，並於「網域」清單窗格中顯示查詢到的網域。

4. 從清單窗格中選取名稱來指定 Active Directory 網域，按一下「確定」，然後進行 第 120 頁上的步驟 5。

   如果清單內未顯示您要使用的網域，您必須使用下列步驟，將知道該網域的通用類別目錄加入：

   a. 按一下「通用類別目錄」按鈕，即會顯示「通用類別目錄」精靈 (圖 4-18)。

圖 4-18 指定新的通用類別目錄

   b. 按一下「開啓新檔」按鈕。

   c. 出現「Windows 通用類別目錄」對話方塊後，輸入通用類別目錄的主機名稱及您的目錄來源憑證 (如第 118 頁所述)，然後按一下「確定」。

   d. 新的通用類別目錄和通訊埠即顯示在「通用類別目錄」清單窗格中。選取類別目錄名稱後，按一下「確定」。

   e. 如要在系統中新增更多通用類別目錄 (網域)，請重複上述步驟。

   f. 完成後按一下「選取網域」窗格內的「下一步」按鈕。

5. 出現「指定憑證」畫面後，複查「使用者 DN」欄位的值。

圖 4-19 指定此 Active Directory 來源的憑證

如果程式未在「使用者 DN」欄位中自動輸入管理員的辨別名稱 (或者您不想使用管理員的憑證)，請手動輸入使用者 DN 及密碼。

配置 Active Directory 來源時，您必須指定可供 Active Directory 連接器用來連接 Active Directory 的使用者名稱及密碼。

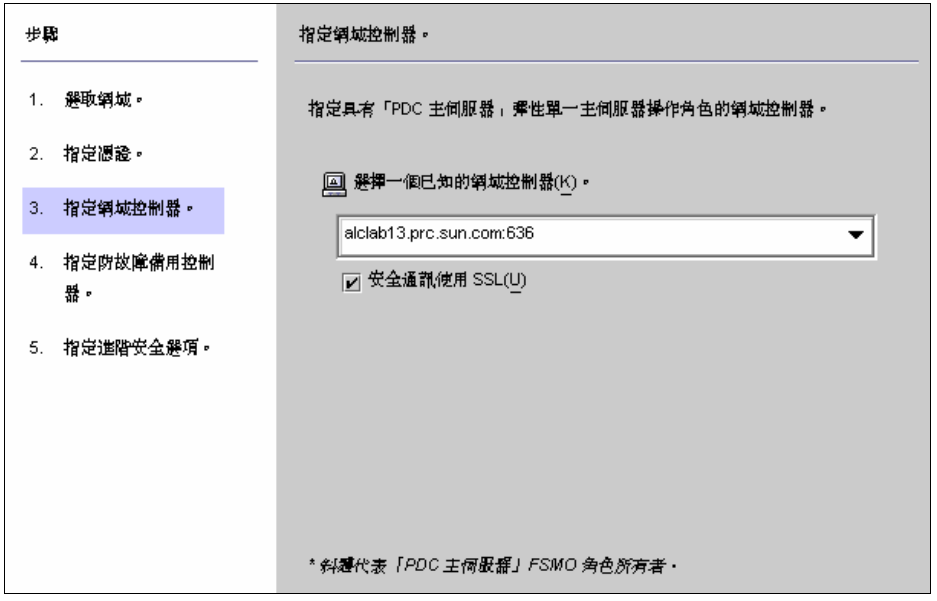
附註 連接器需要特定的存取權。最低權限視同步化的方向而定，即：

- 如果您僅配置從 Active Directory 傳遞至 Directory Server 的同步化，則 Active Directory 連接器的使用者不需要太多特殊的權限。一般使用者只要在所要同步化的網域內擁有「讀取所有屬性」的附加權限即可。
- 如果您配置從 Directory Server 傳遞至 Active Directory 的同步化，則連接器使用者必須具備更多權限，因爲同步化時會變更 Active Directory 中的使用者項目。在此種設定下，連接器使用者必須具備「完整控制」權限或者爲 Administrators 群組的成員。

---

6. 按一下「下一步」開啓「指定網域控制器」畫面。

圖 4-20 指定網域控制器



利用此畫面選取指定網域內所要同步化的控制器。(網域控制器在概念上類似於 Directory Server 的喜好的伺服器。)

如果所選的 Active Directory 網域含有多個網域控制器，請選取具有主要網域控制器 FSMO 角色之網域控制器進行同步化。

預設情況下，在所有網域控制器所做的密碼變更會立刻複製到主要網域控制器 FSMO 角色所有者，而如果您選取該網域控制器，Identity Synchronization for Windows 便會立即將密碼變更同步傳遞至 Directory Server。

在某些部署中，`AvoidPdcOnWan` 屬性可能會因爲網路與 PDC 的「距離」太遠而設在 Windows 登錄中，以避免同步化作業過度延遲。(請參閱 *Microsoft Knowledge Base 文章 232690*，瞭解詳細資訊。)

7. 從下拉清單中選取網域控制器。

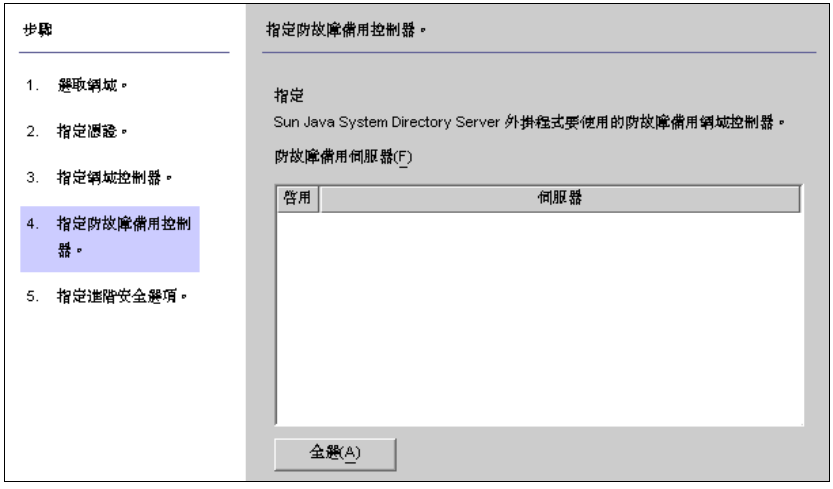
8. 如果希望 Identity Synchronization for Windows 連接器透過安全通訊埠與網域控制器進行通訊，請啓用「使用安全的通訊埠」方塊。

附註	如果您使用 Microsoft 憑證伺服器，程式會自動在 Active Directory 連接器中安裝 CA 憑證。反之，則您必須手動將 CA 憑證新增到 Active Directory 連接器中 (請參閱第 296 頁上的「在 Active Directory 連接器中啓用 SSL」)。此外，如果您在初步配置後變更同步化傳遞方向，上述程序亦同樣適用。

9. 完成後按一下「下一步」。

   出現「指定防故障備用控制器」畫面 (請參閱圖 4-21)。您可透過此畫面來指定任意數量的防故障備用網域控制器。

圖 4-21 指定防故障備用控制器



   Active Directory 連接器只會與一台 Active Directory 網域控制器進行通訊，且 Identity Synchronization for Windows 不支援該連接器所套用的防故障備用變更。不過，Directory Server 外掛程式在驗證對 Directory Server 的密碼變更時，能夠與任意數量的網域控制器進行通訊。

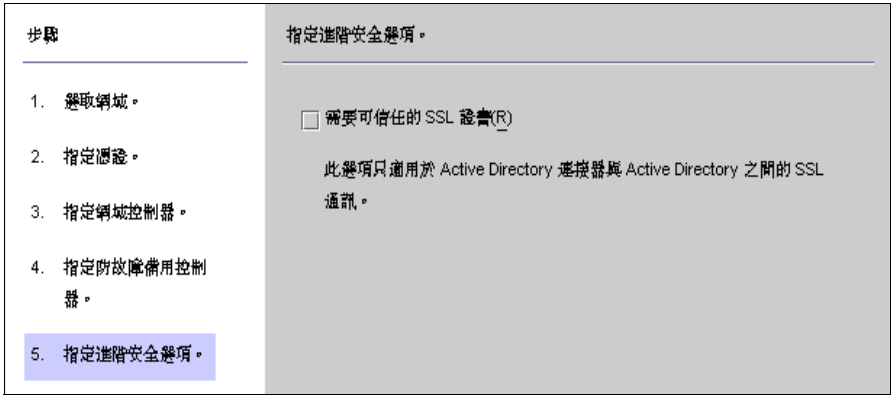
   如果當 Directory Server 嘗試連線至 Active Directory 網域控制器時該網域控制器無法使用，Directory Server 會重複嘗試連線至指定的防故障備用網域控制器。

10. 選取「防故障備用伺服器」清單窗格中所列的一個或多個伺服器名稱 (或者按一下「全選」按鈕指定清單中所有的伺服器)，然後按一下「下一步」。

11. 出現「指定進階安全選項」畫面 (圖 4-22)。

僅當您啓用「指定網域控制器」畫面的「安全通訊使用 SSL」方塊時，「需要可信任的 SSL 憑證」選項才處於活動狀態 (可供選取) (請參閱圖 4-20)。

圖 4-22 指定進階安全選項



- 若停用「需要可信任的 SSL 憑證」方塊 (*預設設定*)，則 Active Directory 連接器將透過 SSL 連線到 Active Directory，且不會驗證它是否信任 Active Directory 所傳遞的憑證。

  停用此選項可簡化設定程序，因爲您不必將 Active Directory 憑證放到 Active Directory 憑證資料庫中。

- 若啓用「需要可信任的 SSL 憑證」方塊，Active Directory 連接器將透過 SSL 連線到 Active Directory，而且必須驗證它是否信任 Active Directory 所傳遞的憑證。

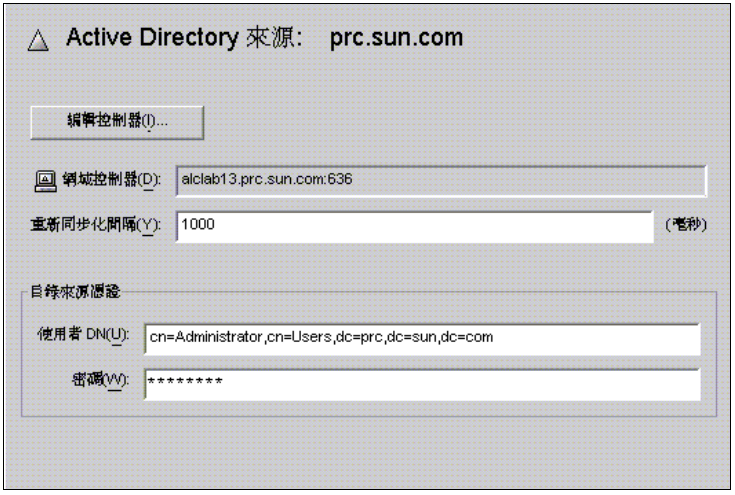
附註 您必須將 Active Directory 憑證加入 Active Directory 連接器的憑證資料庫中。有關說明，請參閱第 299 頁上的「將 Active Directory 憑證加入連接器的憑證資料庫中」。

12. 完成「進階安全選項」畫面後，按一下「完成」按鈕。

程式便會將新指定的 Active Directory 目錄來源新增到導覽樹的「目錄來源」下。

13. 選取 Active Directory 目錄來源節點來檢視「Active Directory 來源」畫面 (圖 4-23)。

圖 4-23 Active Directory 來源畫面



透過此畫面可執行以下工作：

- **編輯控制器**：按一下此按鈕可再度開啓「指定網域控制器」畫面，從中可變更任何網域控制器配置參數。必要時，請檢閱對「建立 Active Directory 來源」的說明。
- **重新同步化間隔**：指定您希望 Active Directory 連接器檢查有否變更的間隔長短。(*預設值爲 1000 毫秒*。)
- **目錄來源憑證**：變更指定的「使用者 DN」及 / 或密碼。

當 Active Directory 目錄來源建立完成後：

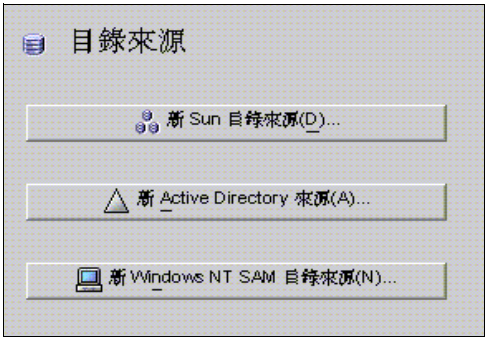
- 若要建立 Windows NT 目錄來源，請接著看下一節「建立 Windows NT SAM 目錄來源」。
- 若要建立並對映所要同步化的屬性，請接著看第 128 頁上的「選取與對映使用者屬性」。

建立 Windows NT SAM 目錄來源

若要在 Windows NT 平台上部署 Identity Synchronization for Windows，請依下列步驟指定 NT SAM 目錄來源：

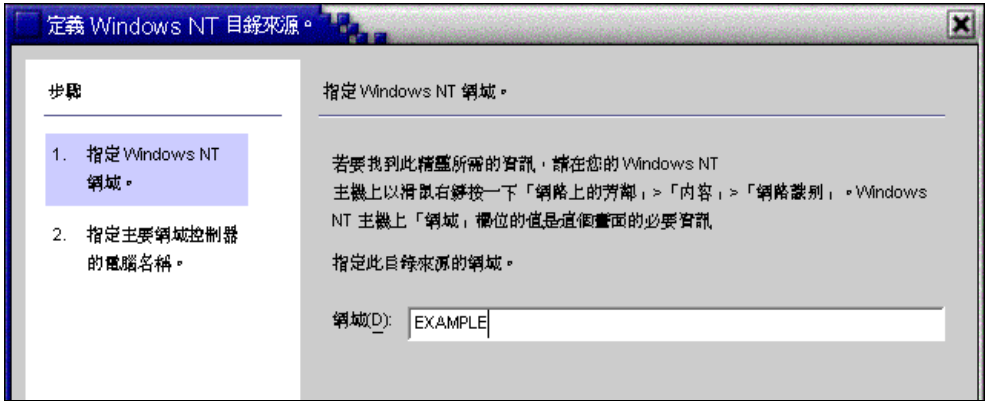
1. 在導覽樹中選取「目錄來源」節點，然後按一下「新 Windows NT SAM 目錄來源」按鈕。

圖 4-24 目錄來源畫面



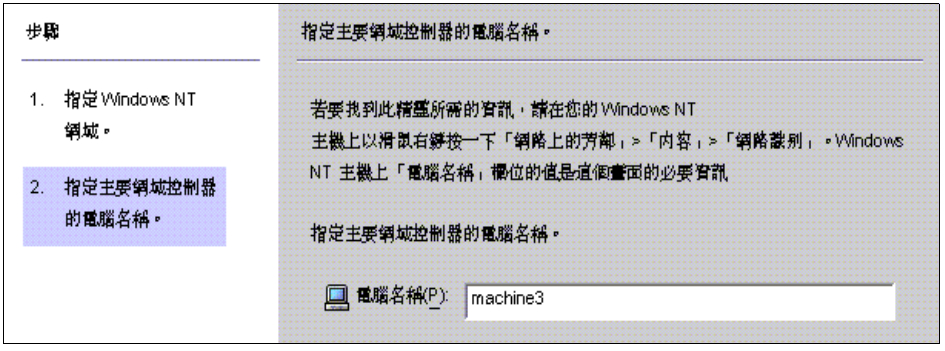
2. 出現「定義 Windows NT SAM 目錄來源」畫面 (請參閱圖 4-25) 後，請依照說明來尋找 Windows NT 網域名稱，並在「網域」欄位中輸入唯一的 NT 目錄來源網域名稱。完成後按一下「下一步」。

圖 4-25 指定 Windows NT SAM 網域名稱



3. 出現「指定主要網域控制器的電腦名稱」畫面 (請參閱圖 4-26) 後，請依照說明來尋找「主要網域控制器」的電腦名稱，並在「電腦名稱」欄位中輸入資訊。

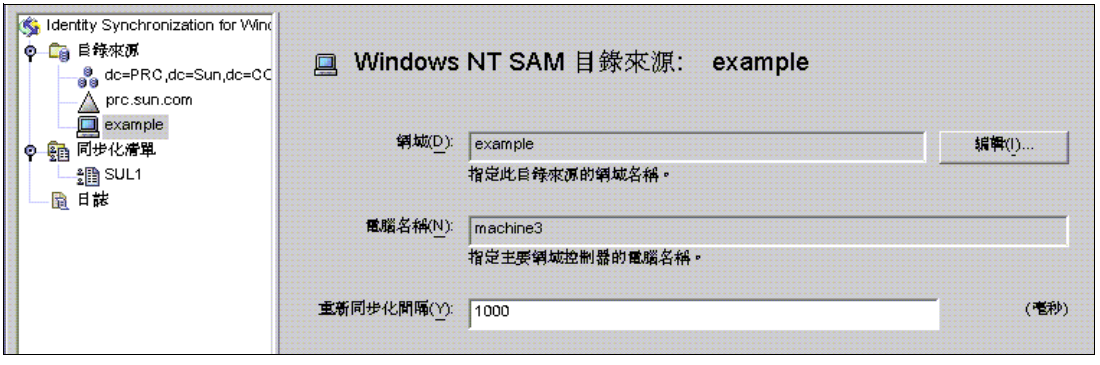
圖 4-26 指定主要網域控制器的名稱



4. 按一下「完成」。

程式便會將新指定的 Windows NT SAM 目錄來源新增到導覽樹的「目錄來源」下。選取新目錄來源節點，檢視「Windows NT SAM 來源」畫面 (請參閱圖 4-27)。

圖 4-27 Windows NT SAM 目錄來源畫面



透過此畫面可執行以下工作：

- **編輯**：按一下此按鈕可再度開啓「指定網域控制器」畫面，從中可變更任何網域控制器配置參數。必要時，請檢閱對「建立 Active Directory 來源」的說明。

- **重新同步化間隔**：指定您希望 Identity Synchronization for Windows 按怎樣的頻率檢查 Windows NT 變更。(*預設值爲 1000 毫秒*。)

5. 分別爲您的網路中的各台 Windows NT 電腦新增 Windows NT 目錄來源。

當 Windows NT SAM 目錄來源建立完成後，您即可著手建立及對映所要同步化的屬性，請接著看第 128 頁上的「選取與對映使用者屬性」。

刪除目錄來源

附註 如果您安裝有與目錄來源聯結的連接器，則在刪除目錄來源*之前*須先解除安裝該連接器。

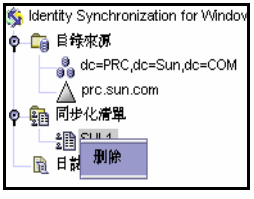
如果您必須刪除目錄來源，請參照以下步驟：

1. 您必須先刪除與該來源聯結的所有「同步化使用者清單 (SUL)」，才能刪除目錄來源。

   a. 在導覽樹的「同步化清單」下所列的受影響之「同步化使用者清單」節點上，按一下滑鼠右鍵。

   b. 出現快顯功能表時，選取「刪除」將 SUL 移除。

圖 4-28 刪除同步化使用者清單



2. 在導覽樹的「目錄來源」下所列的目錄來源節點上按一下滑鼠右鍵。
3. 出現快顯功能表時，選取「刪除」將該目錄來源移除。

選取與對映使用者屬性

當您建立及配置好 Directory Server 與 Windows 目錄來源後，必須決定您要同步化的使用者屬性，並將這些屬性進行系統間對映。

本節資訊的結構如下：

選取與對映屬性

這些屬性分作兩種：

- **重要屬性**：這類屬性會在您建立或修改使用者項目時於系統間同步化。
- **建立屬性**：這類屬性只在您建立使用者項目時才於系統間同步化。

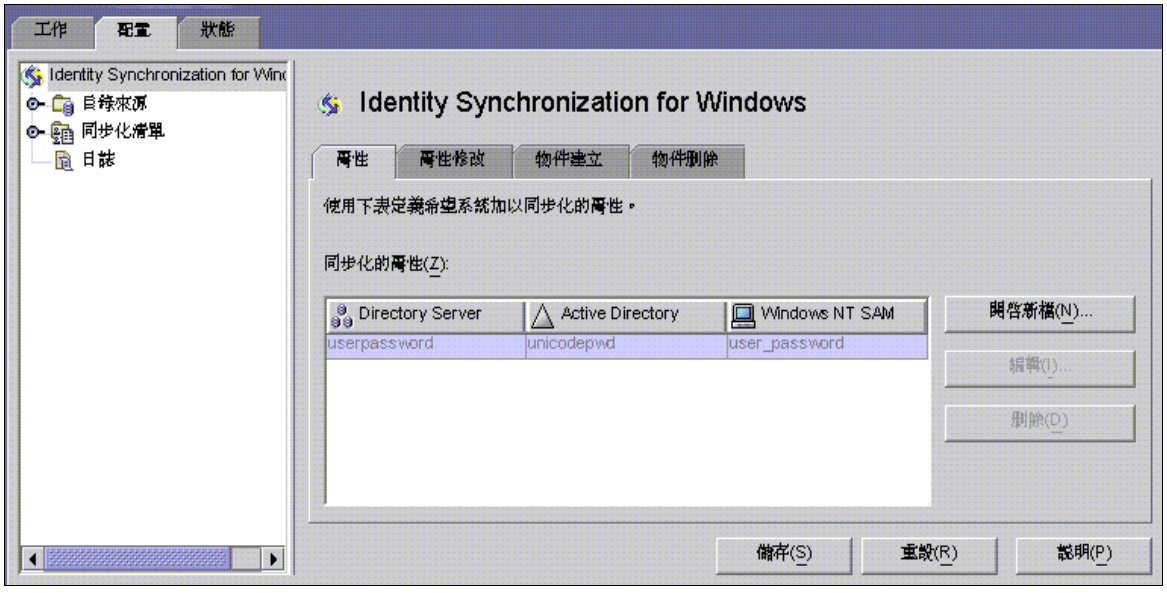
  某些建立屬性會根據各平台所使用的模式而具有*必要性*。這些屬性需要進行密碼同步化且必須對映至 Sun 屬性，才能在 Active Directory 伺服器上成功建立 `user` 物件類別項目。

本節說明如何選取需同步化的使用者屬性及這些屬性的對映方法 (一對一)，以便於在指定 Directory Server 的屬性時，能使對等屬性顯示在 Active Directory 及 / 或 Windows NT 環境中 (反之亦然)，並使附隨的 Windows 屬性值同步化。

若要選取及對映需同步化的屬性：

1. 選取導覽樹頂端的 Identity Synchronization for Windows 節點 (請參閱圖 4-29)。

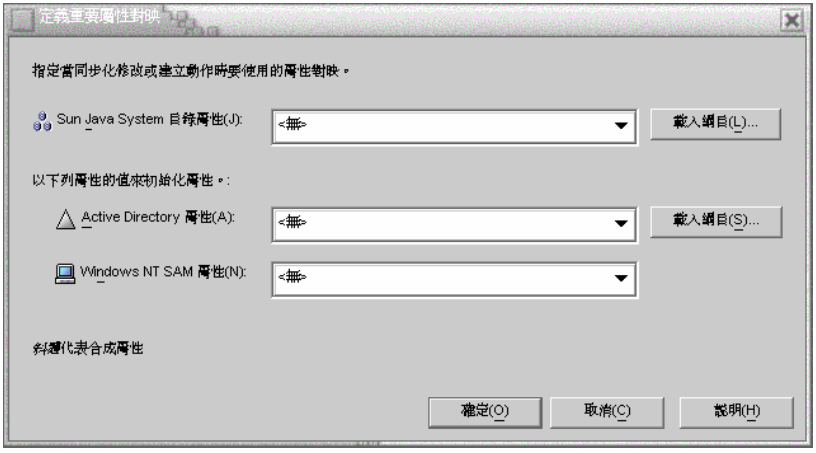
圖 4-29 屬性標籤



2. 選取「屬性」標籤並按一下「開啓新檔」按鈕。

   出現「定義重要屬性對映」對話方塊 (圖 4-30)。利用此對話方塊將屬性從 Directory Server 對映到您的 Windows 系統 (Active Directory 及 / 或 Windows NT)。

圖 4-30 定義重要屬性對映



附註 建立屬性中有哪些屬於 Directory Server (或 Active Directory) 的強制性屬性，視 Sun 端 (或 Active Directory 端) 使用者項目的 objectclass 配置而定。

3. 從 Sun Java System 屬性下拉清單中選取屬性 (例如 *cn*)，然後從 Active Directory 屬性及 / 或 Windows NT SAM 屬性下拉功能表中選取對等的屬性。
4. 完成後按一下「確定」。
5. 若要指定其他屬性，請重複步驟 2 至步驟 4。

完成後的同步化的屬性表大致如同以下範例所示，其中顯示 `userpassword`、`cn` 及 `telephonenumber` Directory Server 屬性對映至 `unicodepwd`、`cn` 及 `telephonenumber` Active Directory 屬性。

圖 4-31 完成後的同步化的屬性表

Directory Server	Active Directory	Windows NT S...
userpassword	unicodepwd	<無>
telephonenumber	telephonenumber	<無>
cn	cn	<無>

附註 程式會自動將 *inetOrgPerson* 當作 Sun Java System Directory Server 的預設物件類別，當您指定通用類別目錄時即已載入 Active Directory 模式。除非您要變更預設模式，否則請勿使用「載入模式」按鈕。

若要變更預設的模式來源，請參閱第 132 頁上的「變更綱目來源」的說明。

建立參數化的預設屬性值

Identity Synchronization for Windows 可讓您利用其他建立或重要屬性，建立*參數化*的預設屬性值。

若要建立參數化的預設屬性值，您必須在表示式字串中內嵌現有的建立或重要屬性名稱 - 前後皆加上百分比符號 (`%<`*attribute_name*`>%`)。例如，`homedir=/home/%uid%` 或 `cn=%givenName% %sn%`。

當您建立這些屬性值時：

- 您可以在建立表示式中使用多個屬性 (`cn=%givenName% %sn%`)。
- 若 `A=%B%`，則 `B` 只能有一個預設值。
- 您可以使用反斜線符號 (\) 來代表引號 (例如，`diskUsage=0\%`)。
- 請勿使用具備循環替代條件的表示式 (例如，如果您指定 `description=%uid%`，則無法使用 `uid=%description%`。)

變更綱目來源

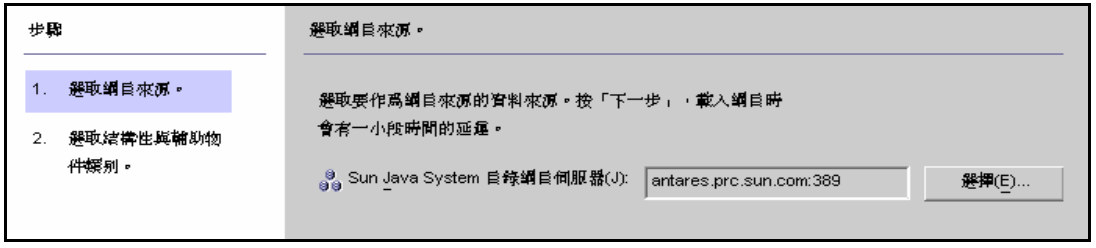
程式會自動提供預設的綱目來源，但您也能變更預設綱目。

請依下列程序變更預設的綱目來源：

1. 按一下 「定義重要屬性對映」對話方塊中的 「載入綱目」按鈕。

   出現 「選取綱目來源」畫面 (圖 4-32)。

圖 4-32 選取綱目來源



   利用此畫面來指定您要從哪一個 Sun Java System Directory Server 綱目伺服器讀取綱目。此綱目內含在您的系統上可用的物件類別及用來定義系統使用者可用的屬性之物件類別。

   預設情況下，程式會將您的配置目錄新增至 「Sun Java System 目錄綱目伺服器」欄位。

2. 若要選取不同的伺服器，按一下 「選擇」按鈕。

   出現 「選取 Sun 綱目主機」對話方塊。此對話方塊包含了配置目錄清單，這些目錄則收集了您的目錄來源之相關管理資訊。

   您可以從此對話方塊：

   - 建立新的配置目錄並加入清單。

     按一下 「新增」，並在出現的 「新配置目錄」對話方塊中，指定 「主機」、「通訊埠」、「使用者 DN」及 「密碼」。完成後按一下 「確定」。

   - 編輯現有目錄。

     按一下 「編輯」，接下來可在出現的 「編輯配置目錄」對話方塊中，變更 「主機」、「通訊埠」、「使用者 DN」及 / 或「密碼」。完成後按一下「確定」。

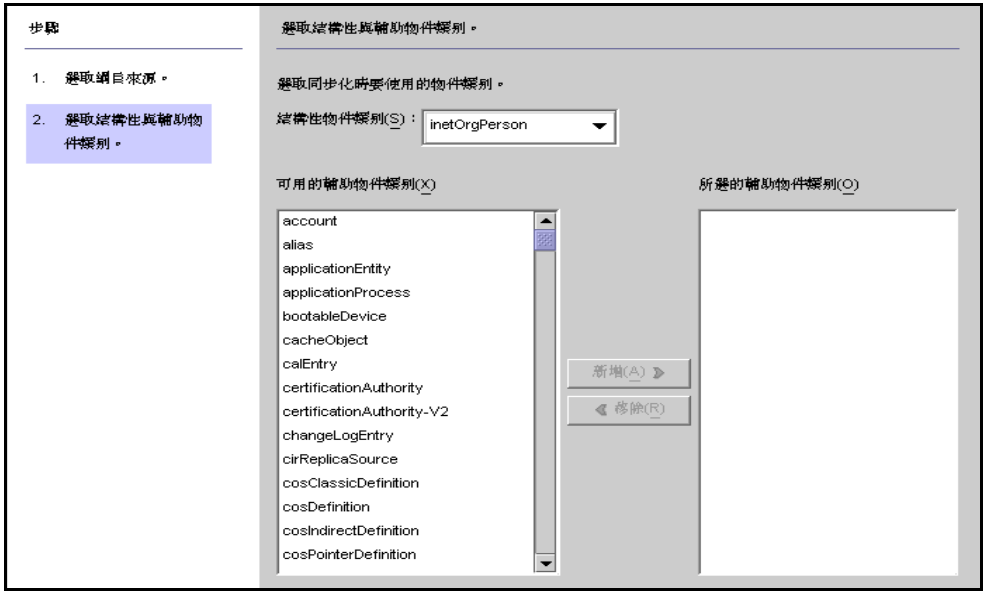
   - 從清單中移除目錄。

     從清單中選取目錄名稱，然後按一下 「移除」按鈕。

3. 從清單中選取伺服器，完成後按一下「確定」。(一般而言，您可以選擇其中一台 Sun 同步化主機作爲綱目來源。)

4. 按一下「下一步」按鈕，將出現「選取結構性與輔助物件類別」畫面 (圖 4-33)。

圖 4-33 選取結構性與輔助物件類別



利用此畫面指定要同步化的物件類別，步驟如下：

- **結構性物件類別**：凡是依據所選的 Directory Server 建立或同步化的每一項目，都必須擁有至少一個結構性物件類別。
- **輔助物件類別**：這類物件類別用於強化所選的結構性類別，並提供要同步化的其他屬性。

若要指定結構性與輔助物件類別：

a. 從下拉清單中選取結構性物件類別。(*預設值是 inetorgperson* 。)

b. 從「可用的輔助物件類別」清單窗格中選取一個或多個物件類別，然後按一下「新增」將選取的項目加入「所選的輔助物件類別」清單窗格。

所選的物件類別會確定哪些 Directory Server 來源屬性爲可供選用的重要屬性或建立屬性。物件類別也會確定強制性的建立屬性。

若要刪除「所選的輔助物件類別」清單中的選項，請按一下該物件類別名稱，然後按一下「移除」按鈕。

c. 完成後按一下「完成」，程式隨即載入模式及所選的物件類別。

於系統間傳播使用者屬性

建立並對映要同步化的使用者屬性後，您必須指示 Identity Synchronization for Windows 如何在 Sun 與 Windows 系統間傳播 (傳遞) 屬性的建立、修改及刪除。

預設情況下，Identity Synchronization for Windows

- 僅從 Windows 同步至 Sun Java System Directory Server
- 僅將密碼屬性同步化 (除非您在上一節中指定了重要屬性)
- 請勿同步化項目的建立或刪除

本節說明如何配置系統間的屬性同步化作業。內容歸納如下：

- 第 135 頁上的「指定物件建立的傳遞方向」
- 第 140 頁上的「指定物件修改項目的傳遞方向」
- 第 150 頁上的「指定刪除項目的傳遞方向」

指定物件建立的傳遞方向

請依照下列步驟指定物件建立於 Directory Server 與 Active Directory 系統間的傳遞方向：

1. 按一下「物件建立」標籤。

圖 4-34 選取與傳遞建立項目

2. 您可以依照以下方法啓用或停用建立項目的傳遞方向：
   - 啓用**物件建立從 Sun Java System Directory Server 傳遞至 Windows**，使建立項目從 Directory Server 環境傳播到您的 Windows 伺服器。
   - 啓用**物件建立從 Windows 傳遞至 Sun Java System Directory Server**，使建立項目從 Windows 環境傳播到您的 Directory Server。
   - 啓用兩個選項可進行雙向傳遞。
   - 停用兩個選項可避免使用者建立項目傳播到另一系統。(*預設值*)
3. 如要新增、編輯或刪除要於系統間同步化的建立屬性，請按一下位於所選項下方的「建立屬性」按鈕。

出現「建立屬性對映與數值」對話方塊 (請參閱圖 4-35 和圖 4-36)。

圖 4-35 建立屬性對映與數值：Directory Server 至 Windows

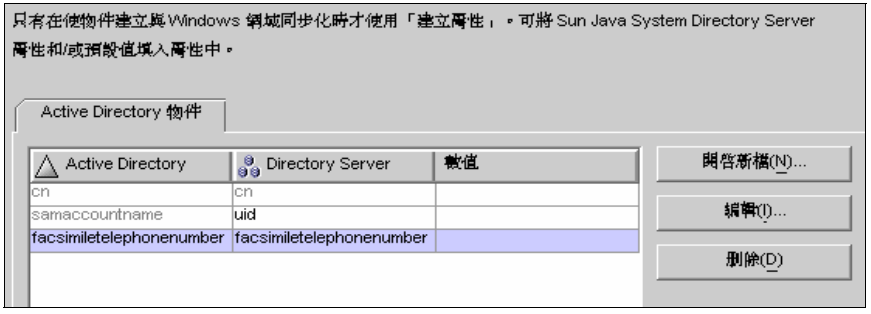
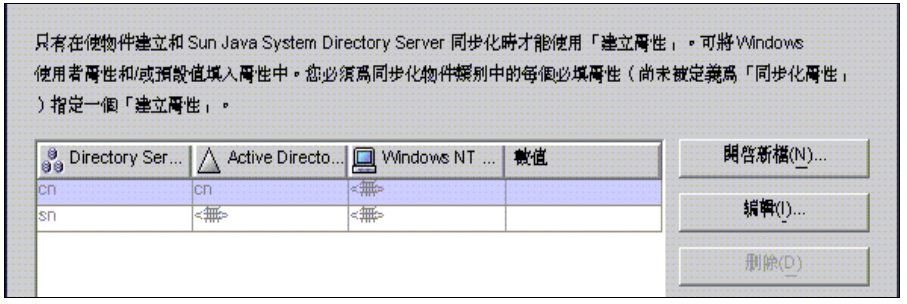


圖 4-36 建立屬性對映與數值：Windows 到 Directory Server



您可以透過任一對話方塊來執行下列動作：

- 指定新的建立屬性 (第 137 頁)

  附註 爲滿足有關使用者物件類別的必需屬性之模式限制，可能需要在使用者建立過程中指定於系統間傳遞的其他屬性。

  若將必要屬性指定爲*修改*屬性，則不需要其他屬性 (如第 128 頁上的「選取與對映使用者屬性」一節所述)。

- 編輯現有屬性 (請參閱第 137 頁)
- 移除現有屬性 (請參閱第 137 頁)

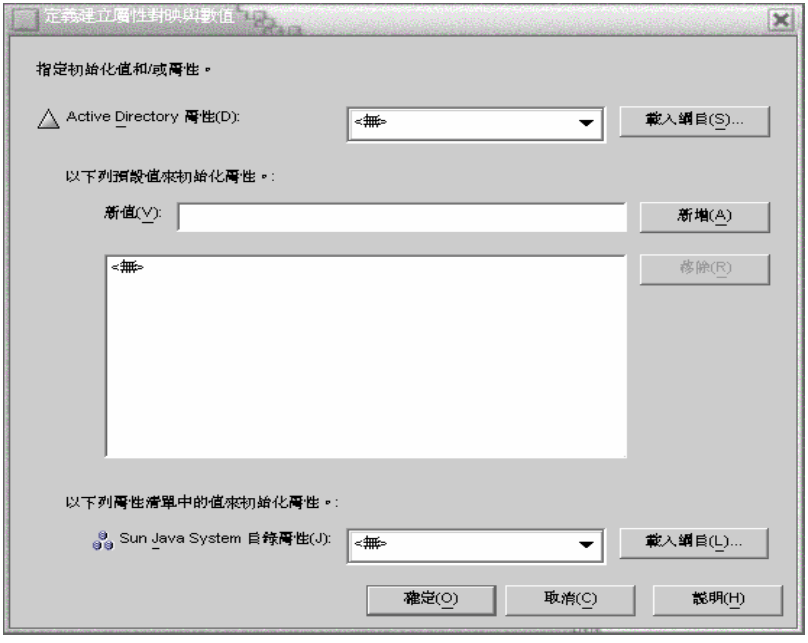
指定新的建立屬性

以下內容說明如何新增建立屬性並從 Active Directory 對映至 Directory Server。(新增建立屬性並進行從 Directory Server 至 Windows 的對映的過程與新增建立屬性並進行從 Windows 到 Directory Server 的過程類似。)

1. 按一下「建立屬性對映與數值」對話方塊中的「開啓新檔」按鈕。

   出現「定義建立屬性對映與數值」對話方塊 (圖 4-37)。

圖 4-37 定義建立屬性對映與數值



2. 從 Active Directory 屬性下拉清單中選取屬性值。

圖 4-38 選取新的 Active Directory 屬性

如果屬性本身接受多個值，則 Identity Synchronization for Windows 能讓您以多個值初始化屬性。

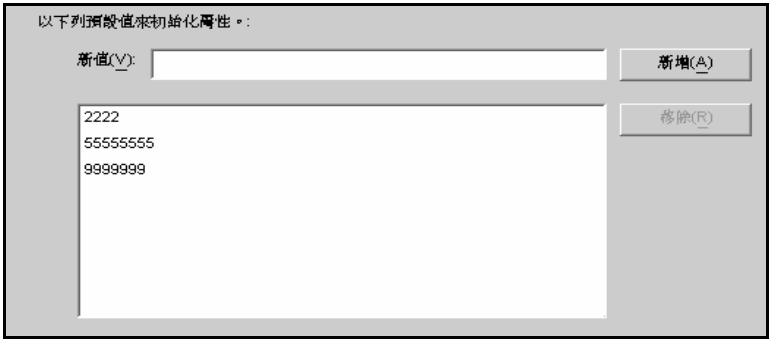
例如，假設貴公司有三個傳真機號碼，那麼您可以指定 `facsilimiletelephonenumber` 屬性同時用於 Sun Java System Directory Server 與 Active Directory，然後指定這三個號碼。

您必須知道哪些屬性接受多個值。若試著將多個值加入不接受多個值的屬性，則當程式嘗試建立物件時，會在執行階段發生錯誤。

3. 在「新值」欄位中輸入值並按一下「新增」。

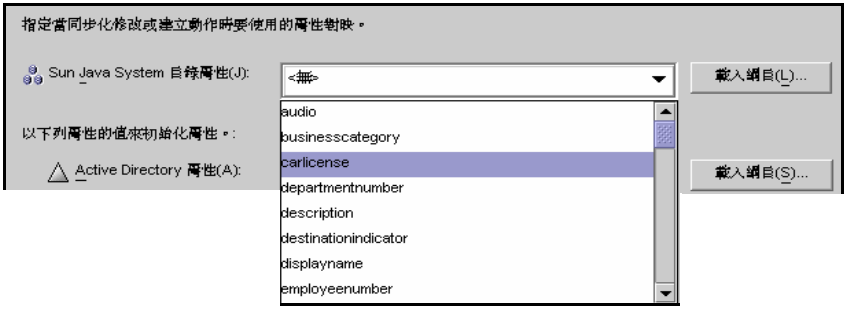
   本程式會將該屬性值加入清單窗格中。視您的需要重複此步驟多次來新增多個屬性值。

圖 4-39 爲建立屬性指定多個值



4. 若要將屬性對映至 Directory Server，請從「Directory Server 屬性」下拉清單中選取屬性名稱。

圖 4-40 對映 Directory Server 屬性



5. 完成後按一下「確定」。

   根據範例，完成的建立屬性與對映表大致如下圖所示：

圖 4-41 完成的建立屬性與對映表

Active Directory	Directory Server	數值
cn	cn	
samaccountname	uid	
facsimiletelephonenumber	facsimiletelephonenumber	

6. 若要指定其他屬性，請重複上述步驟。

編輯現有屬性

若要編輯任何建立屬性對映或數值，

1. 選取「物件建立」標籤，然後按一下所選建立選項下方之「建立屬性」按鈕。
2. 出現「建立對映與數值」對話方塊後，從表中選取屬性並按一下「編輯」按鈕。

   出現「定義建立對映與數值」對話方塊。
3. 利用下拉功能表變更 Directory Server 與 Active Directory (或 Windows NT) 之間的現有對映。

   例如，假設有一個 Sun Java System Directory Server 的 homephone 屬性對映至 Active Directory 的 othertelephone 屬性。您可以透過 Active Directory 屬性下拉清單，將對映變更爲 homephone。
4. 您也可以新增或移除屬性值：
   - 若要新增值，請在「新數值」欄位中輸入資訊，然後按一下「新增」。
   - 若要移除值，請從清單窗格中選取值，再按一下「移除」。
5. 完成後按一下「確定」以套用變更，並關閉「定義建立對映與數值」對話方塊。
6. 再按一次「確定」，關閉「建立對映與屬性」對話方塊。

移除屬性

若要移除建立屬性對映或數值：

1. 選取「物件建立」標籤，然後按一下所選的建立選項下方之「建立屬性」按鈕。
2. 出現「建立對映與數值」對話方塊後，從表中選取屬性並按一下「刪除」按鈕。

   該屬性隨即從表中移除。
3. 完成後按一下「確定」，關閉「建立對映與屬性」對話方塊。

指定物件修改項目的傳遞方向

利用「屬性修改」標籤 (圖 4-42) 可控制對使用者屬性及密碼所做的修改在 Sun 與 Windows 系統間傳播 (傳遞) 的方向。

圖 4-42 屬性修改標籤

您可使用此標籤來配置下列各項：

- 指定修改項目在 Directory Server 與 Windows 目錄來源之間的傳遞方向。
- 控制是否要同步化 Directory Server 與 Active Directory 目錄來源之間的物件啓動及停止作用 (Active Directory 上的*啓用*和*停用*)，並指定使用者帳號的啓動和停止作用方式。

附註 您無法與 Windows NT 目錄來源同步化帳號狀態。

指定方向

選取以下一個按鈕，控制如何在 Directory Server 和 Windows 系統之間傳遞在各自環境中所做的變更。

- **屬性修改從 Sun Java System Directory Server 傳遞至 Windows**：將在 Directory Server 環境中所做的變更傳播至 Windows 伺服器。
- **屬性修改從 Windows 傳遞至 Sun Java System Directory Server** (*預設值*)：將在 Windows 環境中所做的變更傳播至 Directory Servers。
- **屬性修改雙向傳遞**：雙向傳播變更 (從一個環境傳遞至另一環境)。

配置與同步化物件的啓動及停止作用

如果您啓用「將物件啓動 / 停止作用與 Active Directory 同步化」方塊 (請參閱圖 4-43)，則可同步化 Directory Server 與 Active Directory 目錄來源之間的物件的啓動和停止作用 (稱爲 Active Directory 上的*啓用*和*停用*)。

附註 您無法使啓動與停止作用和 Windows NT 目錄來源同步化。

圖 4-43 同步化物件的啓動與停止作用

若要同步化物件的啓動 / 停止作用：

1. 啓用「同步化 Directory Server 與 Active Directory 之間的物件停止作用」方塊。
2. 啓用下列一個按鈕，指定 Identity Synchronization for Windows 如何偵測和同步化物件的啓動和停止作用：
   - **與 Directory Server 工具互通** (請參閱第 142 頁)
   - **直接修改 Directory Server 的 nsAcountlock 屬性** (請參閱第 143 頁)
   - **使用 Directory Server 的自訂方式** (請參閱第 144 頁)

附註 這些選項是彼此互斥的。

- 如啓用「與 Directory Server 工具互通」選項，則 Identity Synchronization for Windows 就無法直接設定或移除 `nsAccountLock` 屬性。此外，程式無法偵測到使用其他角色 (如 `cn=nsdisabledrole, <database suffix>`) 或嵌套於其他角色內部的角色 (如 `cn=nsdisabledrole°B<database suffix>` 或 `cn=nsmanageddisabledrole, <database suffix>`) 停止作用的物件。
- 如啓用「修改 Directory Server 的 `nsAccountLock` 屬性」選項，則 Identity Synchronization for Windows 將無法偵測出使用 Directory Server 主控台或指令行公用程式啓動 / 停止作用的物件。
- 啓用「使用 Directory Server 的自訂方式」選項時，除非目錄的存取是由外部應用程式 (如 Sun Java™ System Access Manager (先前稱爲 Sun JES Identity Server)) 所控制，否則 Identity Synchronization for Windows 就無法鎖定該目錄外的物件。

與 Directory Server 工具互通

如果您使用 Directory Server 主控台或指令行工具來啓動 / 停止作用物件，則請選取此選項。

- 若要啓動物件，Identity Synchronization for Windows 將移除 `nsroledn` 屬性的 `cn=nsmanageddisabledrole,<database suffix>` 值。
- 若要停止作用物件，Identity Synchronization for Windows 會將 `cn=nsmanageddisabledrole,<database suffix>` 值加入 `nsroledn` 屬性。

附註 如啓用「與 Directory Server 工具互通」選項，則 Identity Synchronization for Windows 無法直接設定或移除 nsAccountLock 屬性。此外，Identity Synchronization for Windows 也無法偵測出使用其他角色停止作用的物件。

例如，cn=nsdisabledrole, <*database suffix*>，或嵌套於其他角色內部的角色 (如 cn=nsdisabledrole, <*database suffix*> 或 cn=nsmanageddisabledrole, <*database suffix*>)。

表格 4-1 說明了當您啓用「與 Directory Server 工具互通」選項時，Identity Synchronization for Windows 如何偵測和同步化物件的啓動 / 停止作用：

表格 4-1 與 Directory Server 工具互通

啓動	停止作用
只有在移除物件中的 cn=nsmanageddisabledrole,<*database suffix*> 角色後，Identity Synchronization for Windows 才能偵測到啓動動作。	只有在項目的 nsroledn 屬性包含 cn=nsmanageddisabledrole,<*database suffix*> 角色時，Identity Synchronization for Windows 才能偵測到停止作用。
當您從 Active Directory 同步化物件的啓動動作時，Identity Synchronization for Windows 就會藉由移除物件的 cn=nsmanageddisabledrole,<*database suffix*> 角色來啓動物件。	當您從 Active Directory 同步化物件的停止作用時，Identity Synchronization for Windows 就會藉由將 cn=nsmanageddisabledrole,<*database suffix*> 角色加入物件來停止作用該物件。

直接修改 Directory Server 的 NsAccountLock 屬性

當 Directory Server 啓動與停止作用均依照 Directory Server 的操作屬性 nsAccountLock 時，請使用此方式。此屬性按如下所述控制物件狀態：

- 當 nsAccountLock=true 時，物件會被停止作用，使用者無法登入。
- 當 nsAccountLock=false (或沒有值) 時，物件會啓動。

表格 4-2 說明了當您啓用「直接修改 Directory Server 的 nsAccountLock 屬性」選項時，Identity Synchronization for Windows 如何偵測以及同步化物件的啓動 / 停止作用：

表格 4-2 直接修改 Directory Server 的 nsAccountLock 屬性

啓動	停止作用
只有在 nsAccountLock 屬性設成 **true** 時，Identity Synchronization for Windows 才能偵測到停止作用的物件。	只有在缺少 nsAccountLock 屬性或將該屬性設爲 **false** 時，Identity Synchronization for Windows 才能偵測出啓動的物件。
從 Active Directory 同步化物件的停止作用時，Identity Synchronization for Windows 將移除 nsAccountLock 屬性。	當同步化 Active Directory 中的物件啓動動作時，Identity Synchronization for Windows 會將 nsAccountLock 屬性設爲 **true**。

使用 Directory Server 的自訂方式

當 Directory Server 的啓動和停止作用是由外部應用程式 (如 Sun Java™ System Access Manager (先前稱爲 Sun JES Identity Server)) 所專門控制時，請使用此方法。

配置 Directory Server 的自訂方式時，必須指定

- Identity Synchronization for Windows 如何偵測外部應用程式是啓動或還是停止作用了 Directory Server 中的物件
- 當從 Active Directory 向 Directory Server 進行同步化時，Identity Synchronization for Windows 如何啓動或停止作用物件

附註 如啓用「使用 Directory Server 的自訂方式」選項，則 Identity Synchronization for Windows 無法鎖定目錄外的物件，除非該目錄的存取權是由一個外部應用程式所控制，例如 Access Manager。

若要配置自訂的啓動和停止作用方式，請按一下「配置」按鈕，畫面接下來將顯示「配置 Directory Server 的自訂方式」對話方塊 (請參閱圖 4-44)。

圖 4-44 配置自訂的啓動及停止作用方式

此對話方塊包含下列功能：

- **啓動狀態屬性下拉清單**：使用此清單可指定 Identity Synchronization for Windows 用來同步化 Directory Server 與 Active Directory 之間啓動與停止作用的屬性。

  該清單包含目前所選的 Directory Server 結構性及輔助物件類別的模式中之所有屬性。

- **數值與狀態表**：使用此表可指定何時要啓動或停止作用與所選屬性相關的數值。
  - **「數值」欄**：使用此欄 (與「新增」和「移除」按鈕結合使用) 可指定用來表示使用中或非作用中狀態的屬性值。

本程式會自動在此欄中提供兩個值：

- **沒有值**：此時「啓動」狀態屬性沒有任何值。
- **所有其他值**：此時「啓動」狀態屬性有一個值，但此值不是在該「值和狀態」表中指定的。

○ **「狀態」欄**：使用此欄可指定「數值」項目 (在同一列中) 是否對應於啓動或停止作用的物件。

表格 4-3 指定啓動與停止作用狀態

數值	狀態	結果
沒有值	啓用	如果缺少屬性或此屬性沒有值，Identity Synchronization for Windows 會偵測該物件爲已啓用。
	已停用	如果缺少屬性或此屬性沒有值，Identity Synchronization for Windows 會偵測該物件爲已停用。
< *使用者定義* > 值	啓用	如果屬性具有 < *使用者定義* > 屬性，則 Identity Synchronization for Windows 會偵測該物件爲已啓用。
	已停用	如果屬性具有使用者定義屬性，則 Identity Synchronization for Windows 會偵測該物件爲已停用。
所有其他值	啓用	如果屬性有一個值，但在表格中未指定此值，則 Identity Synchronization for Windows 會偵測該物件爲已啓用。
	已停用	如果屬性有一個值，但在表格中未指定此值，則 Identity Synchronization for Windows 會偵測該物件爲已停用。

- **「新增」按鈕**：按一下此按鈕可在「數值」欄中新增項目。
- **「移除」按鈕**：在「數值」欄中選取一個項目，然後按一下此按鈕可將該項目移除。
- **「啓動的值」與「非作用中的值」下拉清單**：使用這兩個清單可指定 Identity Synchronization for Windows 用來*設定*物件狀態的數值。

同步化啟動與停用　使用下列程序可配置 Identity Synchronization for Windows，使其偵測以及同步化 Directory Server 與 Active Directory 之間的物件狀態：

1. 從「啓動」狀態屬性下拉清單中選取一個屬性。
2. 按一下「新增」按鈕可將屬性值加入表格的「數值」欄中。
3. 按一下每個「數值」項目旁的「狀態」欄，當顯示下拉清單時，選取「已啓用」或「已停用」。

圖 4-45　選取狀態

例如，如果您使用的是 Access Manager：

1. 從「啓動」狀態屬性下拉清單中選取 **`inetuserstatus`** 屬性。
2. 按一下「新增」按鈕，並在表格的「數值」欄中輸入**使用中**、**非作用中**和**刪除**屬性值。
3. 按一下「狀態」欄並按如下所示針對各個值選取「已啓用」或「已停用」：
   - **沒有值**：已啓用
   - **使用中**：已啓用
   - **非作用中**：已停用
   - **刪除**：已停用
   - **所有其他值**：已停用

根據此範例，表格 4-4 說明了 Identity Synchronization for Windows 如何在您啓用「使用 Directory Server 的自訂方式」選項時偵測和同步化啓動 / 停止作用 (使用 `inetuserstatus` 範例)。

表格 4-4 使用 inetuserstatus 值的範例結果

數值	狀態	結果
沒有值	啓動	如果缺少 `inetuserstatus` 屬性或此屬性沒有值，Identity Synchronization for Windows 會偵測該物件爲已啓動。
使用中	啓動	如果屬性值爲**使用中**，則 Identity Synchronization for Windows 會偵測該物件爲已啓動。
非作用中	停止作用	如果屬性值爲**非作用中**，則 Identity Synchronization for Windows 會偵測該物件爲已停止作用。
刪除	停止作用	若屬性值爲**刪除**，Identity Synchronization for Windows 會將物件視爲已停止作用。
所有其他值	停止作用	如果屬性有一個值，但在表格中未指定此值，則 Identity Synchronization for Windows 會偵測該物件爲已停止作用。

設定啓動與停止作用　當您在「數值」與「狀態」表格中填入項目時，Identity Synchronization for Windows 會按照如下所示自動填充**「啓動的值」**與**「非作用中的值」**下拉清單：

- 「啓動的值」清單包含具有「啓動」狀態的所有值 (例如**沒有值**和**使用中**)。
- 「非作用中的值」清單包含具有「停止作用」狀態的所有值 (例如**非作用中**和**刪除**)。
- 上述清單皆不包含「所有其他數值」值。

從「啓動的值」和 / 或「非作用中的值」下拉清單中選取一個值，指定在從 Active Directory 進行同步化時，Identity Synchronization for Windows 如何啓動和 / 或停止作用物件。

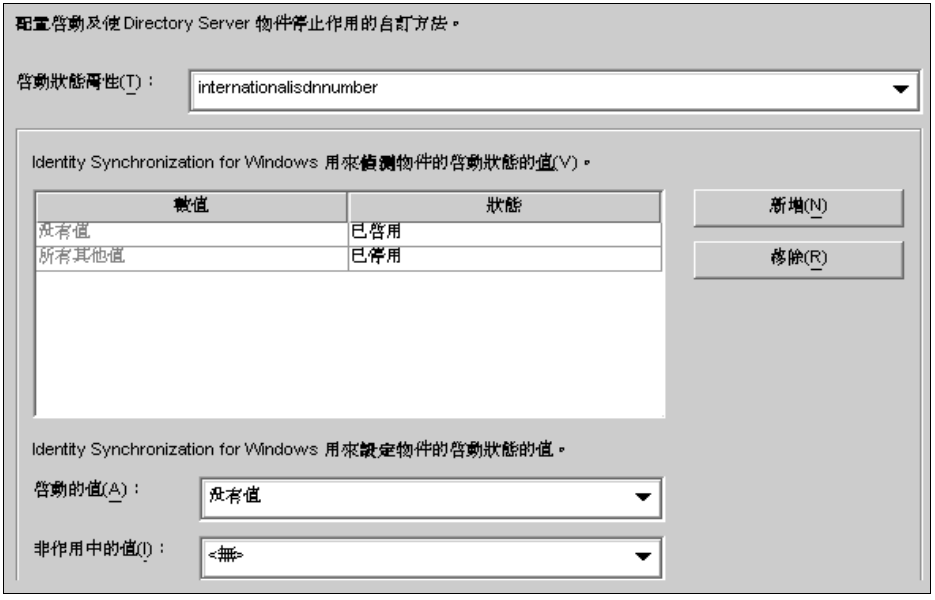
- **「啓動的值」**：控制物件的使用中狀態。
  - **沒有值**：如果物件包含使用中的值，Identity Synchronization for Windows 會將 Directory Server 中的狀態設爲「啓動」。
  - **使用中**：如果物件包含使用中的值，Identity Synchronization for Windows 會將 Directory Server 中的狀態設爲「啓動」。

- **「非作用中的值」**：控制物件的使用中狀態。
  - **非作用中**或**刪除**：Identity Synchronization for Windows 會將 Directory Server 中物件的狀態設爲「非作用中」。
  - **<*無*>**：非有效設定。您必須選取一個值。

附註 您必須指定一個「非作用中的值」，否則您的配置將會無效。

圖 4-46 說明了完整的「配置 Directory Server 的自訂方式」對話方塊。

圖 4-46 範例：完整的對話方塊



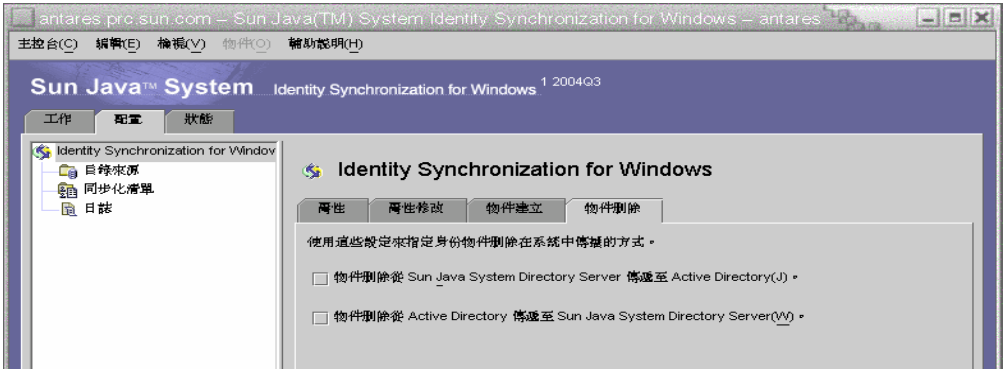
指定刪除項目的傳遞方向

利用「物件刪除」標籤來指定已刪除的使用者項目於 Directory Server 與 Active Directory 系統間的傳遞方向

附註 您無法指定 Windows NT 的物件刪除項目傳遞方向。

1. 選取導覽窗格頂端的 Identity Synchronization for Windows 節點，然後按一下「物件刪除」標籤。

圖 4-47 傳播使用者項目刪除



2. 啓用或停用刪除項目傳遞方向的步驟如下：
   - 啓動**物件刪除從 Sun Java System Directory Server 傳遞至 Active Directory**，使刪除項目從 Directory Server 環境傳播到您的 Active Directory 伺服器。
   - 啓動**物件刪除從 Active Directory 傳遞至 Sun Java System Directory Server**，使刪除項目從 Active Directory 環境傳播到您的 Directory Server。
   - 啓用兩個選項可進行雙向傳遞。
   - 停用兩個選項可避免使用者刪除傳播到另一系統。(*預設設定*)

建立同步化使用者清單

同步化使用者清單 (SUL) 用於指定兩個目錄來源中所要同步化的使用者。SUL 中的每個項目均要通過連接器，並依據您對該 SUL 配置的限制對它們進行評估。

每個 SUL 均包含兩個元素，一個用來識別要同步化的 Directory Server 使用者，一個用來識別要同步化的 Windows 使用者。

附註 若要將 Directory Server 的使用者與多個 Active Directory 網域同步，您必須針對各 Active Directory 網域逐一定義 SUL。

有關定義與配置 SUL 的詳細資訊 (包括定義的元件、定義多個 SUL 的方法、對多個 SUL 的處理過程以及配置多重 Windows 網域支援的方法)，請參閱第 331 頁上的附錄 D，「定義和配置同步化使用者清單」。

兩種 SUL 元素均包含三項定義，用以識別要同步化的使用者：

- **基本 DN**：要同步化的使用者之位置 (不適用於 NT)
- **命名屬性**：用於新建的使用者之屬性 (建立表示式) (不適用於 NT)
- **篩選器**：同步化時排除指定的使用者

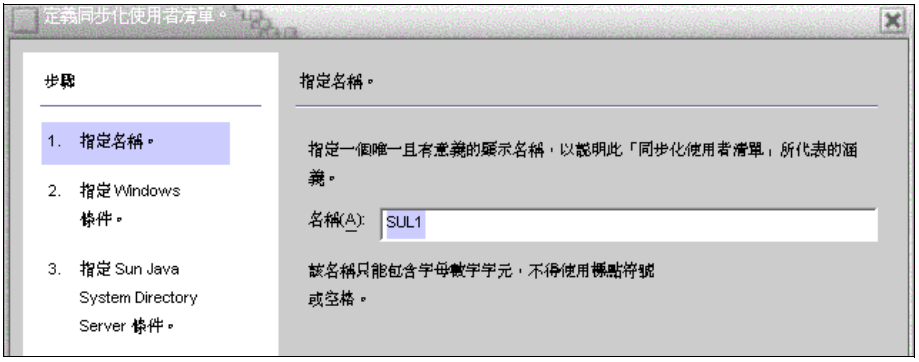
若要識別及連結伺服器間的使用者類型：

1. 在導覽樹中選取 「同步化使用者清單」節點，然後按一下 「新同步化使用者清單」按鈕。

圖 4-48 建立新的同步化使用者清單

出現「定義同步化使用者清單」精靈，如下所示：

圖 4-49 指定 SUL 名稱



您的第一份「同步化使用者清單」的程式預設值爲 *SUL1*。

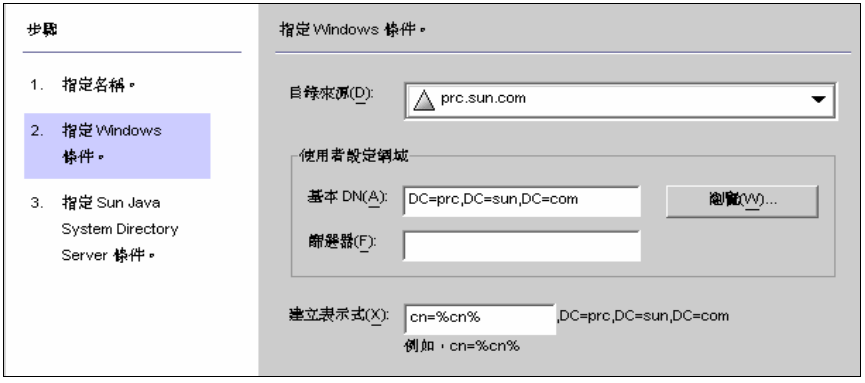
- 如果您接受預設名稱，請按一下「下一步」。
- 若要使用其他名稱，請在「名稱」欄位中鍵入要使用的名稱，再按一下「下一步」。

附註

- 請勿在 SUL 名稱中使用空格或任何標點符號。
- 您指定的名稱在系統中必須是唯一的。

出現「Windows 條件」畫面，如圖 4-50 所示。

圖 4-50 指定 Windows 條件



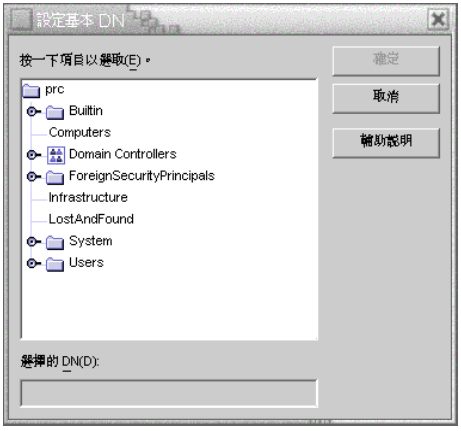
2. 從下拉清單中選取 Windows 目錄來源。

附註 建立 SUL *後*，就無法編輯此目錄來源。

3. *使用者設定網域* 用來設定要同步化的所有使用者。請按照下列任一方法，輸入「使用者設定網域」的「基本 DN」：

   - 將名稱輸入文字欄位 (例如 **DC=example,DC=com**)。
   - 按一下「瀏覽」按鈕開啓「設定基本 DN」對話方塊，以尋找並選取基本 DN。

圖 4-51 選取基本 DN



除非您使用篩選明確排除，否則所指定的基本 DN 下的所有使用者都將納入此 SUL。

附註 基本 DN 及建立表示式不適用於 Windows NT 伺服器。

4. 您可以輸入平等指數、存在指數或子字串篩選器，以指定此基本 DN 中要同步化的使用者。例如，假設您將同一個基本 DN 用於多個同步化使用者清單，即可利用篩選加以區別。

   平等篩選器語法類似於 LDAP 查詢語法，但平等子字串只允許 *****、**&**、**|**、**=**、**!** 字元。例如，您可以使用下列篩選器，將管理員從 SUL 中排除：

   ```
   (!(cn=Administrator))
   ```

   程式會自動在「建立表示式」欄位填入值。

附註 建立表示式用於定義新項目從 Active Directory 傳播至 Directory Server 時，所使用的父項 DN 及命名屬性。

除非您配置讓使用者屬性建立從 Active Directory 傳遞至 Directory Server，否則建立表示式不適用於 Sun 目錄 (請參閱 第 135 頁上的「指定物件建立的傳遞方向」)。

5. 如果建立表示式遺失或者您想要變更現有項目，可以對所有 Windows Active Directory 同步化使用者清單輸入建立表示式，例如：

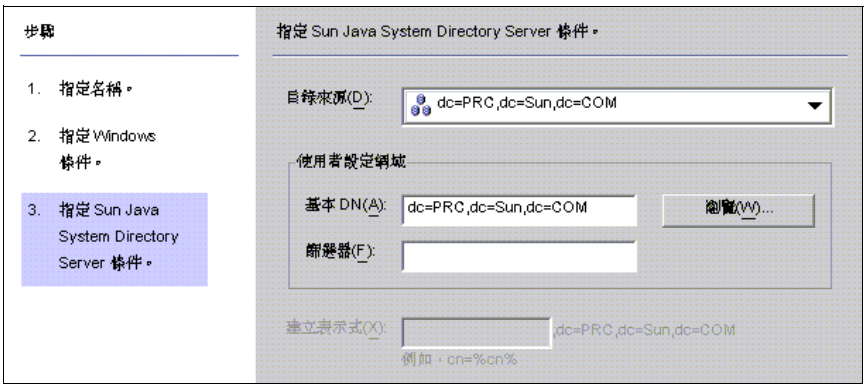
   cn=%*cn*%,cl=*users*,dc=example,dc=com

   如要變更建立表示式，必須選取要同步化的屬性。必要時，回到「物件建立」標籤，使用「建立屬性」按鈕新增及對映該屬性。

6. 按一下「下一步」指定 Sun Java System Directory Server 條件。

7. 出現「指定 Sun Java System Directory Server 條件」畫面後，重複步驟 2 至步驟 5 進行 Directory Server 條件設定。

圖 4-52 指定 Directory Server 條件

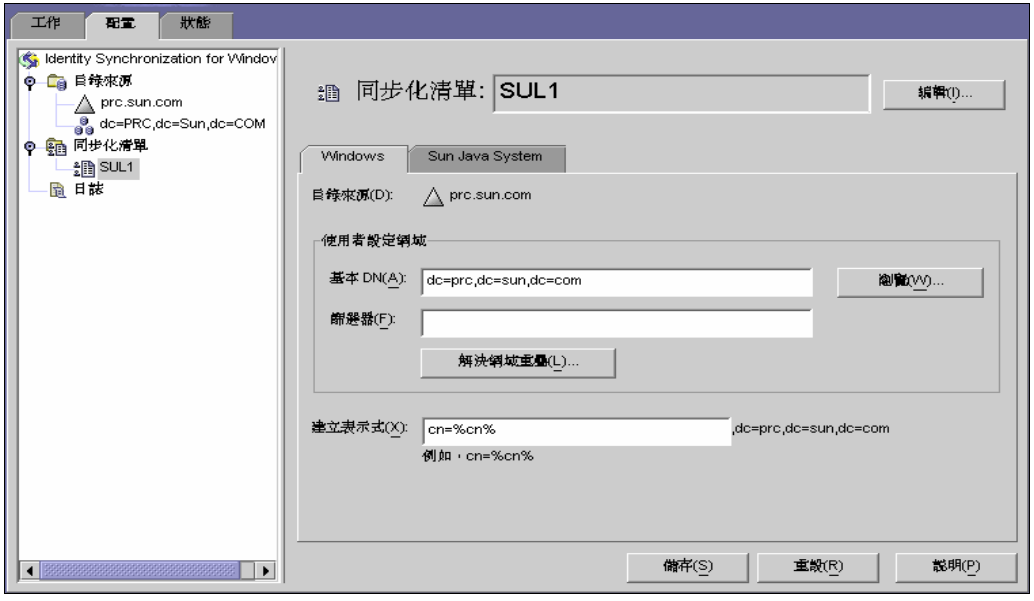


附註 按一下「完成」按鈕來建立 SUL 之後，就無法編輯此 SUL 所包含的 Active Directory 或 Directory Server 目錄來源。

8. 完成後按一下「完成」。

9. 此程式可將新的 SUL 節點新增到導覽樹中，「配置」標籤也會顯示出「同步化使用者清單」畫面。

圖 4-53 同步化清單畫面



10. 如遇同一使用者符合多個清單的情形，請按一下「解決網域重疊」按鈕來定義同步化使用者清單的喜好設定。(有關詳細資訊，請參閱第 331 頁上的「認識同步化使用者清單定義」。)

11. 建立一個同步化使用者清單，其中包含網路中除了 Directory Server 以外的所有目錄來源。

儲存配置

若要透過任何主控台畫面儲存您目前的配置：

1. 按一下「儲存」，儲存截至目前爲止的設定。
2. 當程式在評估您的配置設定時，會顯示「配置有效狀態」視窗。

圖 4-54 配置有效狀態視窗

儲存配置可能需花數分鐘，因爲程式會將資訊重寫至配置目錄並通知系統管理員。系統管理員 (或核心元件) 負責將您的配置設定分送給需要這些資訊的元件。

附註 配置驗證錯誤是紅色的，警告則是黃色的。

- 配置如有錯誤即無法儲存。
- 可以儲存有警告的配置，但是最好先嘗試解除警告。

3. 如果您的配置有效，請按一下「繼續」儲存配置。

   此時會顯示「連接器安裝說明」對話方塊 (類似於圖 4-55 中的清單)，提供有關安裝 Identity Synchronization for Windows 連接器與子元件方法的說明。

   該清單現在已更新爲針對您的部署所自訂的「待辦事項」清單。(截至目前爲止，這些步驟是通用的。) 請注意，您也可以從 Identity Synchronization for Windows 主控台的「狀態」標籤上存取及更新「待辦事項」清單。

圖 4-55 安裝連接器之說明

4. 詳閱其中的訊息後，按一下「確定」。

完成初步的核心配置後，即可開始安裝 Identity Synchronization for Windows 連接器及子元件。請接著看第 5 章，「安裝連接器與 Directory Server 外掛程式」之說明。

第 5 章

安裝連接器與 Directory Server 外掛程式

本章說明 Identity Synchronization for Windows 連接器與 Directory Server 外掛程式的安裝方法。內容歸納如下：

Identity Synchronization for Windows 是利用連接器來同步化目錄來源間的使用者密碼，並使用子元件增強連接器的變更 - 偵測與雙向同步化支援。

準備工作

開始進行連接器 /Directory Server 外掛程式安裝程序之前，應注意下列幾點：

- 開始安裝程序前，請先關閉主控台。如果主控台在安裝連接器或外掛程式期間開啓，則當元件在將配置資料新增至伺服器時，程式會發生衝突並產生錯誤訊息。
- 您必須在部署中存有需同步化的使用者之每台 Directory Server 機器上逐一安裝 Directory Server 外掛程式，這些機器包括主要伺服器、複本伺服器和集線器。
- Active Directory 連接器不具有子元件。
- Windows NT 連接器與子元件同步安裝。

- 您可以在安裝了核心元件的電腦上安裝 Directory Server 或 Active Directory 連接器，亦可在別台電腦上安裝連接器。(Windows NT 連接器必須安裝在需同步化的網域中之主要網域控制器 (PDC) 上)。
  - 如果您將連接器安裝在裝有核心元件的電腦上，程式會自動將連接器安裝在與核心元件相同的目錄中。
  - 如果您將連接器安裝在別台電腦上，程式會提示您指定以下資訊
    - 在核心元件安裝過程中提供的配置目錄資訊
    - 安裝目錄
- 每次安裝連接器或 Directory Server 外掛程式時，都必須執行安裝程式。

  例如，假設您要安裝 Directory Server 連接器、單一 Directory Server 外掛程式及 Active Directory 連接器，則您需要在安裝核心元件後分三次執行安裝程式。

執行安裝程式

請依下列程序重新啓動並執行安裝程式。每次安裝連接器或 Directory Server 外掛程式時，都必須執行這些步驟：

1. 在您要安裝連接器的電腦上重新執行安裝程式，步驟如下：
   - **Solaris 系統**：轉到 `installer` 目錄並鍵入 **`./runInstaller.sh`** 來執行安裝程式。

附註	若要以文字模式執行安裝程式，鍵入 **`./runInstaller.sh -nodisplay`** 當您執行 `runInstaller.sh` 程式時，Identity Synchronization for Windows 會自動遮罩密碼，使其不至於以明文顯示。

   - **Windows 系統**：轉到 `installer` 目錄並鍵入 **`setup.exe`** 來執行安裝程式。
2. 出現歡迎畫面時，閱讀其中的資訊並按一下「下一步」進入「軟體授權合約」畫面。
3. 閱讀授權合約內容後，選取：
   - **「是」(接受授權合約)** 表示接受授權條款並進入下一個畫面。
   - **「否」**表示停止安裝程序並結束安裝程式。

4. 出現 Sun Java System Directory Server 畫面。如下指定配置目錄位置：

   - **配置目錄主機**：輸入存有 Identity Synchronization for Windows 配置資訊的 Sun Java System Directory Server 實例 (其與 Administration Server 相關) 之完全合格的網域名稱。在此指定的實例必須與您在核心元件安裝時所指定者相同。
   - **配置目錄通訊埠** (*預設通訊埠爲 389*)：指定供配置目錄使用的通訊埠。您可以直接使用預設的通訊埠或者改設爲其他可用的通訊埠。

     若要啓用核心元件與配置目錄間的 SSL (安全資料傳輸層)，請啓用「安全通訊埠」選項並指定 SSL 通訊埠 (*預設 SSL 通訊埠爲 636*)。啓用此選項可防止敏感資訊在網路上以明文傳遞。
   - **配置根字尾**：從功能表選取您在核心元件安裝過程中所指定的根字尾。Identity Synchronization for Windows 配置將儲存在此根字尾中。

     附註 如果程式偵測不到根字尾，而需手動輸入伺服器資訊時，則您必須按一下「更新」以重新填入根字尾清單。

5. 按一下「下一步」開啓「配置目錄憑證」畫面。
6. 輸入配置目錄管理員的使用者 ID 及密碼。

   - 若指定 `admin` 作爲使用者 ID，無需將使用者 ID 指定爲 DN。
   - 若使用任何其他的使用者 ID，則必須將 ID 指定爲完整的 DN。例如 *cn=Directory Manager*。

   附註 除非您在步驟 4 中啓用了 SSL，否則這些憑證將以未加密的方式傳送。

7. 按一下「下一步」開啓「配置密碼」畫面，您必須在該畫面中輸入安裝核心元件時所指定的配置密碼。

   此外，若尚未在這台機器上安裝核心元件，系統會提示您提供 Java 主目錄的位置 (請參閱第 91 頁)。

8. 完成後按一下「下一步」。

附註 此時，安裝程序即爲您正在安裝的 Directory Server 外掛程式或者連接器類型之特定程序。

- 若要安裝連接器，請前進至第 162 頁上的「安裝連接器」。
- 若要安裝 Directory Server 外掛程式，請前進至第 173 頁上的「安裝 Directory Server 外掛程式」。

安裝連接器

本節說明如何安裝三種 Identity Synchronization for Windows 連接器，內容如下：

- 第 163 頁上的「安裝 Directory Server 連接器」
- 第 168 頁上的「安裝 Active Directory 連接器」
- 第 172 頁上的「安裝 Windows NT 連接器」

附註 安裝連接器時無需依照特定順序，但請不要嘗試同時安裝所有連接器。

安裝 Directory Server 連接器

完成第 160 頁上的「執行安裝程式」中所述的步驟後，會出現「連接器配置」畫面。

圖 5-1 選取 Directory Server 連接器

「選取要安裝的元件」清單內僅含有尚未安裝的連接器元件。例如，當您安裝 Directory Server 連接器 (在圖 5-1 爲 dc=example,dc=com) 後，程式便會將該項目從清單窗格中移除。

下表舉出部分範例目錄來源項目：

表格 5-1 目錄來源範例

目錄來源	範例項目
Sun Java System Directory Server	`dc=example,dc=com`
Windows Active Directory	`example.com`
Windows NT SAM	範例

若要安裝 Directory Server 連接器：

1. 啓用「Directory Server 連接器」元件旁的按鈕，然後按一下「下一步」。

   出現「Directory Server 連接器憑證」畫面 (圖 5-2)。

圖 5-2 輸入 Directory Server 連接器憑證

附註 程式會自動以您完全合格的「目錄管理員」辨別名稱來完成「使用者 DN」欄位，但您可在必要時變更此資訊。

請輸入以下資訊：

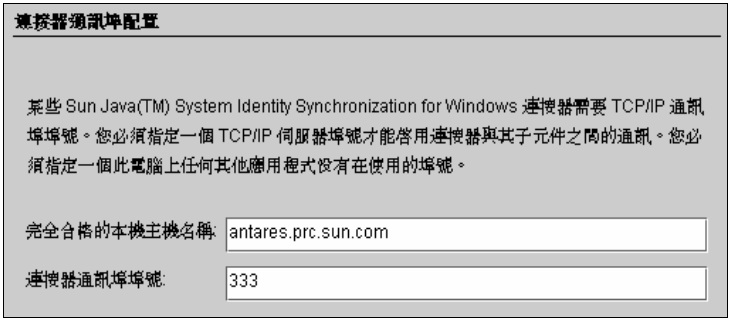
- **主要 Directory Server 使用者 DN**：必要時，請輸入完全合格的「目錄管理員」辨別名稱來變更預設的使用者 DN。
- **主要 Directory Server 密碼**：輸入您的目錄管理員密碼。

如有使用輔助主伺服器，則「輔助 Directory Server 使用者名稱」及「密碼」欄位即可供使用。程式會以針對「主要 Directory Server 使用者 DN」及「密碼」欄位所提供的相同項目來自動完成「目錄管理員 DN」欄位。您可在必要時變更此資訊。

程式會驗證 Directory Server 是否備妥並準備好進行資料同步化。當 Directory Server 備妥 (第 113 頁) 時，程式會建立一個帳號，供連接器用來連接 Directory Server (例如 uid=`PSWConnector`,*suffix*)。

2. 按一下「下一步」進入「連接器通訊埠配置」窗格。

圖 5-3 指定連接器本機主機與通訊埠

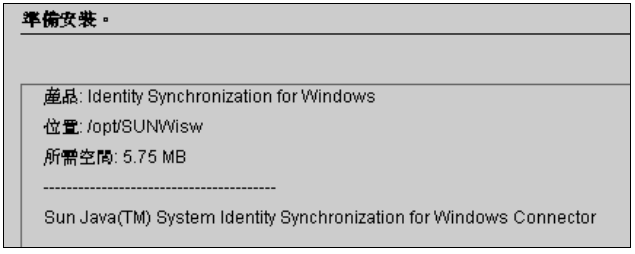


3. 輸入包含網域的「完全合格的本機主機名稱」，以及連接器偵聽的可用通訊埠埠號。(若指定正在使用中的通訊埠會發生錯誤訊息。)

   Directory Server 外掛程式需存取您在主控台中儲存的配置資訊。爲取得該資訊，外掛程式會透過此通訊埠的伺服器通訊端與 Directory Server 連接器進行通訊。此外，外掛程式會透過此通道記錄訊息，使訊息傳至中央日誌。

4. 按一下「下一步」出現「準備安裝」窗格，提供有關連接器安裝位置及安裝所需的磁碟空間的資訊。一切準備就緒後，按一下「立即安裝」按鈕。

圖 5-4 準備安裝窗格



附註 如果您在本機電腦上安裝核心元件，「準備安裝」窗格會指示您不需要任何空間來安裝連接器。這是因爲核心元件安裝作業已安裝了連接器二進位檔。由於沒有要安裝的其他二進位檔，所以不需額外的空間。

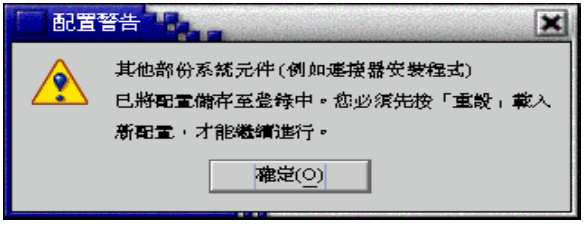
如果您安裝連接器所在的電腦不是安裝核心元件的電腦，「準備安裝」畫面就會指出需要多少空間才能在本機電腦中完成連接器的安裝作業。

連接器安裝經過以下兩個步驟即告完成：

- 在程式安裝二進位檔時，顯示 「正在安裝」窗格及進度列。
- 接著顯示 「元件配置」窗格。此步驟需花數分鐘的時間完成，因此會出現進度列顯示進度。

附註 如果您在開始安裝前未關閉主控台，會出現以下警告 (圖 5-5)。請在主控台中按一下「重設」，重新載入連接器的配置設定。

圖 5-5 配置警告對話方塊



上述步驟均完成後，會出現 「安裝摘要」窗格。

5. 若要檢視安裝日誌，按一下「詳細資訊」按鈕。

   - **Solaris 系統**：安裝日誌係寫入 `/var/sadm/install/logs/`
   - **Windows 系統**：安裝日誌係寫入 `%TEMP%` 目錄，其通常是子目錄，位於以下路徑的 `Local Settings` 資料夾下：
     `C:\Documents and Settings\Administrator`

附註 在某些 Windows 系統上 (如 Windows 2000 Advanced Server)，`Local Settings` 資料夾爲隱藏資料夾。

若要檢視該資料夾以及 `Temp` 子目錄，請開啓 Windows 檔案總管後，從功能表列中選取「工具」>「資料夾選項」。「資料夾選項」對話方塊開啓後，選取「檢視」標籤並啓用「顯示隱藏檔案」選項。

---

6. 按一下「下一步」，螢幕會出現「待辦事項清單」畫面 (圖 5-6)，指出您已順利完成及有待完成的步驟。

圖 5-6 待辦事項清單

7. 完成畫面後，按一下「完成」。

安裝 Directory Server 連接器後，可以再安裝您在配置資源時 (第 4 章) 所配置的其他連接器及 / 或 Directory Server 外掛程式：

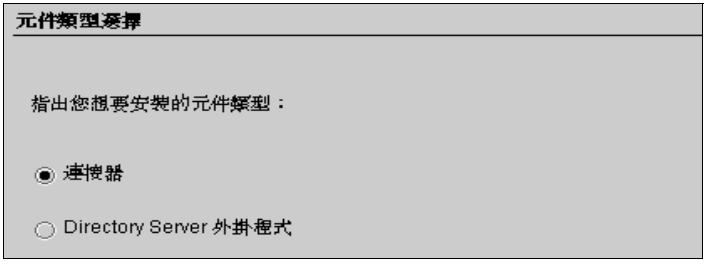
- 安裝其他 Directory Server 連接器：重新啓動安裝程式 (參照第 160 頁上的「執行安裝程式」中的說明)，然後重複步驟 1 至步驟 7。
- 安裝 Active Directory 連接器：轉至第 168 頁上的「安裝 Active Directory 連接器」。
- 安裝 Windows NT 連接器：轉至第 172 頁上的「安裝 Windows NT 連接器」。
- 安裝 Directory Server 外掛程式：轉至第 173 頁上的「安裝 Directory Server 外掛程式」。

安裝 Active Directory 連接器

完成第 160 頁上的「執行安裝程式」中所述的步驟後，會出現「元件類型選擇」畫面。

附註 安裝完 Directory Server 連接器後如尚有其他配置的連接器需要安裝，安裝程式會在顯示「連接器配置」窗格 (圖 5-7) 前，提供安裝連接器或 Directory Server 外掛程式的選項。

圖 5-7 選取連接器



元件清單僅含有那些尚未安裝的連接器元件。例如，假設您已安裝了 Directory Server 連接器 (在此假設 dc=example,dc=com)，它將不會出現在清單中。

若要安裝 Active Directory 連接器：

1. 啓用「連接器」按鈕，並按一下「下一步」。

   出現「連接器配置」畫面 (請參閱圖 5-8)。

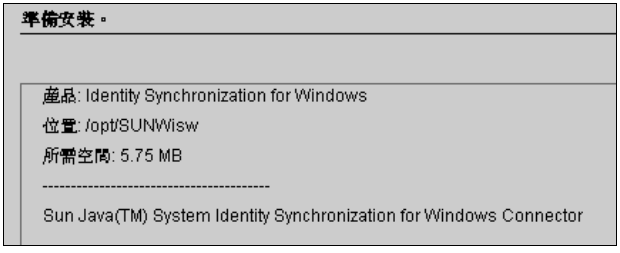
圖 5-8 選取 Active Directory 連接器

「選取要安裝的元件」清單內僅含有尚未安裝的連接器元件。例如，當您安裝 Directory Server 連接器 (在此假設 dc=example,dc=com) 後，程式便會將該項目從此清單窗格中移除。

2. 啓用 Active Directory 元件旁的按鈕，然後按一下「下一步」。

   出現「準備安裝」窗格 (圖 5-9)，提供有關連接器安裝位置及安裝所需的磁碟空間的資訊。

圖 5-9 準備安裝窗格



附註 如果您在本機電腦上安裝核心元件，「準備安裝」窗格會指示您不需要任何空間來安裝連接器。這是因爲核心元件安裝作業已安裝了連接器二進位檔。由於沒有要安裝的其他二進位檔，所以不需額外的空間。

如果您安裝連接器所在的電腦不是安裝核心元件的電腦，「準備安裝」畫面就會指出需要多少空間才能在本機電腦中完成連接器的安裝作業。

3. 一切準備就緒後，按一下「立即安裝」按鈕。

   當程式安裝二進位檔時，螢幕將顯示「正在安裝」窗格及進度列，接下來會顯示一個「安裝摘要」窗格以確認安裝已完成。

4. 若要檢視安裝日誌，按一下「詳細資訊」按鈕。

   - **Solaris 系統**：安裝日誌係寫入 `/var/sadm/install/logs/`
   - **Windows 系統**：安裝日誌係寫入 `%TEMP%` 目錄，它是一個子目錄，位於以下路徑的 `Local Settings` 資料夾下：
     `C:\Documents and Settings\Administrator`

附註 在某些 Windows 系統上 (如 Windows 2000 Advanced Server)，`Local Settings` 資料夾爲隱藏資料夾。

若要檢視該資料夾以及 `Temp` 子目錄，請開啓 Windows 檔案總管後，從功能表列中選取「工具」>「資料夾選項」。「資料夾選項」對話方塊開啓後，選取「檢視」標籤並啓用「顯示隱藏檔案」選項。

5. 按一下「下一步」，螢幕會出現「待辦事項清單」畫面 (圖 5-10)，指出您已順利完成及有待完成的步驟。

圖 5-10 待辦事項清單

6. 完成畫面後，按一下「完成」結束安裝程式。

安裝 Active Directory 連接器後，可以再安裝您在配置資源時 (第 4 章) 所配置的其他連接器及 / 或 Directory Server 外掛程式：

- 安裝其他 Active Directory 連接器：重新啓動安裝程式 (請參閱第 160 頁上的「執行安裝程式」)，然後重複步驟 1 至步驟 6。
- 安裝 Windows NT 連接器：轉至第 172 頁上的「安裝 Windows NT 連接器」。
- 安裝其他 Directory Server 連接器：重新啓動安裝程式 (參照第 160 頁上的「執行安裝程式」中的說明)，然後重複步驟 1 至步驟 7。
- 安裝 Directory Server 外掛程式：轉至第 173 頁上的「安裝 Directory Server 外掛程式」。

安裝 Windows NT 連接器

附註 您必須在所配置網域的「主要網域控制器 (PDC)」上安裝 Windows NT 連接器。

完成第 160 頁上的「執行安裝程式」中所述的步驟後，會出現「連接器配置」畫面。

若要安裝 Windows NT 連接器及 NT 子元件：

1. 啓用「Windows NT 連接器」按鈕並按一下「下一步」。
2. 出現「連接器通訊埠配置」窗格時，輸入包含網域的「完全合格的本機主機名稱」，以及連接器將要偵聽的可用通訊埠埠號。(若指定正在使用中的通訊埠會發生錯誤訊息。)

   Directory Server 外掛程式需存取您在主控台中儲存的配置資訊。爲取得該資訊，外掛程式會透過此通訊埠的伺服器通訊端與 Windows NT 連接器進行通訊。此外，外掛程式會透過此通道記錄訊息，使訊息傳至中央日誌。
3. 完成後按一下「下一步」。

   出現「準備安裝」窗格，提供有關連接器安裝位置及所需磁碟空間的資訊。
4. 一切準備就緒後，按一下「立即安裝」按鈕。

   連接器安裝經過以下兩個步驟即告完成：

   - 在程式安裝二進位檔時，顯示「正在安裝」窗格及進度列。
   - 接著顯示「元件配置」窗格。此步驟需花數分鐘的時間完成，因此會出現進度列顯示進度。

   附註 如果您在開始安裝前未關閉主控台，會出現以下警告 (請參閱圖 5-5)。請在主控台中按一下「重設」，重新載入連接器的配置設定。

   上述步驟均完成後，會出現「安裝摘要」窗格。
5. 若要檢視安裝日誌，按一下「詳細資訊」按鈕。

   安裝日誌係會被寫入 `%TEMP%` 目錄，在大多數 Windows NT 系統中爲 C:\TEMP。
6. 按一下「關閉」結束安裝程式。

安裝完 Windows NT 連接器後，可以再安裝您在配置資源時 (第 4 章) 所配置的其他連接器及 / 或 Directory Server 外掛程式：

- 安裝其他 Windows NT 連接器：重新啓動安裝程式 (請參閱第 160 頁上的「執行安裝程式」)，然後重複步驟 1 至步驟 6。
- 安裝 Directory Server 連接器：轉至第 163 頁上的「安裝 Directory Server 連接器」。
- 安裝 Active Directory 連接器：轉至第 168 頁上的「安裝 Active Directory 連接器」。
- 安裝 Directory Server 外掛程式：轉至第 173 頁上的「安裝 Directory Server 外掛程式」。

安裝 Directory Server 外掛程式

本節說明如何安裝 Identity Synchronization for Windows Directory Server 外掛程式。

附註	您必須在裝有 Directory Server 的電腦上安裝 Directory Server 外掛程式。 如果將外掛程式安裝在裝有核心元件或任何連接器的同一系統上，則當核心元件或連接器已安裝於系統上時，安裝程式會偵測到。所有其他元件都將安裝在安裝目錄中。

1. 完成第 160 頁上的「執行安裝程式」中所述的步驟。

圖 5-11 選取 Directory Server 外掛程式

2. 出現「連接器配置」畫面時，請啓用「Directory Server 外掛程式」(dc=example,dc=com) 按鈕，並按一下「下一步」。
3. 出現另一個「Directory Server 外掛程式安裝」窗格 (圖 5-12)。

圖 5-12 指定 Directory Server URL 與憑證

4. 從下拉清單中選取適當的主機類型。
   - **喜好的**：如要將外掛程式安裝在喜好的伺服器上，請選取此選項。
   - **輔助**：如要將外掛程式安裝在輔助伺服器上，請選取此選項。
   - **其他**：如要將外掛程式安裝在喜好的伺服器或輔助伺服器以外的其他電腦上，請選取此選項。
5. 如果您的 Directory Server 不是喜好的主機或輔助主機，請輸入它所在的 URL。
6. 輸入 Directory Server 管理員的名稱及密碼，然後按一下「下一步」。

   出現「準備安裝」窗格，提供有關外掛程式安裝位置及安裝所需的磁碟空間的資訊。
7. 一切準備就緒後，按一下「立即安裝」按鈕。

   外掛程式安裝經過以下兩個步驟即告完成：
   - 在程式安裝二進位檔時，顯示「正在安裝」窗格及進度列。
   - 接著顯示「元件配置」窗格。此步驟需花數分鐘的時間完成，因此會出現進度列顯示進度。
8. 完成這兩個步驟後，會出現下列提示。閱讀資訊後，請按一下「確定」關閉對話方塊。

圖 5-13 重新啓動 Directory Server 提示

9. 若要檢視安裝日誌，按一下「詳細資訊」按鈕。

   - **Solaris 系統**：安裝日誌係寫入 `/var/sadm/install/logs/`
   - **Windows 系統**：安裝日誌係寫入 `%TEMP%` 目錄，它是一個子目錄，位於以下路徑的 `Local Settings` 資料夾下：
     `C:\Documents and Settings\Administrator`

   附註 在某些 Windows 系統上 (如 Windows 2000 Advanced Server)，`Local Settings` 資料夾爲隱藏資料夾。

   若要檢視該資料夾以及 `Temp` 子目錄，請開啓 Windows 檔案總管後，從功能表列中選取「工具」>「資料夾選項」。「資料夾選項」對話方塊開啓後，選取「檢視」標籤並啓用「顯示隱藏檔案」選項。

10. 按一下「關閉」結束安裝程式。

    安裝 Directory Server 外掛程式後，可以再安裝您在配置資源時 (第 4 章) 所配置的其他連接器及 / 或 Directory Server 外掛程式：

    - 安裝其他 Directory Server 外掛程式：重新啓動安裝程式 (請參閱第 160 頁上的「執行安裝程式」)，然後重複步驟 2 至步驟 9。

      由於 Identity Synchronization for Windows 要求您在部署中的每台 Directory Server 上安裝外掛程式，因此可無限制的繼續執行外掛程式安裝程式。

    - 安裝 Directory Server 連接器：轉至第 163 頁上的「安裝 Directory Server 連接器」。
    - 安裝 Active Directory 連接器：轉至第 168 頁上的「安裝 Active Directory 連接器」。
    - 安裝 Windows NT 連接器：轉至第 172 頁上的「安裝 Windows NT 連接器」。

11. 重新啓動 Directory Server。

第 6 章

現有使用者同步化

Identity Synchronization for Windows 指令行公用程式提供了 `idsync resync` 子指令來驅動現有使用者的部署。這個指令可使用管理員指定的配對規則來連結現有的項目、將遠端目錄的內容填入空目錄中，或批量同步化兩個現有使用者個體群之間的屬性值 (包含密碼)。

本章說明如何使用 `idsync resync` 子指令來連結並同步化現有的使用者，以執行新的 Identity Synchronization for Windows 安裝作業。此外，本章也提供了啓動和停止同步化及服務的說明。內容歸納如下：

附註 在嘗試連結並同步化現有使用者前，請務必先安裝核心元件及連接器。

有關 `idsync resync` 子指令的詳細資訊，請參閱附錄 A，「使用 Identity Synchronization for Windows 指令行公用程式」。

表格 6-1 依據現有使用者個體群歸納出要執行的安裝後步驟：

表格 6-1 基於現有使用者個體群的安裝後步驟

使用者所屬系統		安裝後步驟	
Windows	**Directory Server**	**同步化現有使用者**	**不同步化現有使用者**
否	否	無	無
否	是	執行 `idsync resync -o Sun -c`，在 Windows 中建立現有的 Directory Server 使用者。	無
是	否	執行 `idsync resync -c`，在 Directory Server 中建立現有的 Windows 使用者。	執行 `idsync resync -u` 以填入連接器所獲的使用者項目之本機快取。
是	是	使用以下一種方法： • 執行 `idsync resync -f` <*filename*> 來連結並同步化 Active Directory 與 Directory Server 中的使用者。 • 執行 `idsync resync -f` <*filename*> `-k`，僅連結使用者。 • 執行 `idsync resync -f` <*filename*> `-k` 僅連結使用者，然後再執行 `idsync resync -o Sun` 以同步化 Directory Server 中的現有使用者。	執行 `idsync resync -u` 以填入連接器所獲的使用者項目之本機快取。

使用 idsync resync

本節說明連結及同步化程序，描述了使用 idsync resync 子指令的適當語法，並且解釋了如何驗證程序是否順利完成。內容歸納如下：

重新同步化使用者

附註 開始進行部署的同步化之前，請確定伺服器間所有的現有使用者均已同步化。

您可以使用 `idsync resync` 指令來連結現有的項目、建立使用者，以及同步化兩個目錄來源中的使用者屬性。特別是您能使用 `idsync resync` 指令來

- 將現有 Active Directory 或 Windows NT SAM 網域使用者填入空 Directory Server
- 連結所有使用者，然後同步化兩個現有目錄來源中的所有使用者項目屬性值 (密碼除外)

附註 如果有存在於 Directory Server 和 Windows 中的使用者，您必須執行 `idsync resync -f <`*filename*`>` 指令來連結和同步化這些使用者。

如果不希望讓現有使用者與 Directory Server 同步化，請在執行 `idsync resync` 時加上 `-u` 引數，如此便只會更新物件快取，不會將 Windows 的項目同步化到 Directory Server。

如有現有的 Windows 使用者但未執行 `idsync resync`，則是否會傳播對這些使用者所做的變更將視傳遞方向設定而定，甚至有可能在 Directory Server 中自動建立這些使用者。您必須再次執行 `idsync resync`，即使您已執行了該指令。

- 當兩個目錄來源變成不同步時，請同步化使用者項目
- 「填寫」 Active Directory 與 Windows NT SAM 連接器物件快取資料庫，該資料庫可維護 Active Directory 或 Windows NT SAM 使用者項目的陰影副本。

您無法使用 `idsync resync` 指令來同步化密碼 (但可使 Directory Server 密碼失效，以強制在 Active Directory 環境中進行隨需密碼同步化)。

連結使用者

在將使用者填入 Active Directory 和 Directory Server 並安裝 Active Directory 和 Directory Server 連接器之後 (開始同步化之前)，您必須使用 `idsync resync` 指令來確保兩個目錄來源中的全部現有使用者均已*連結*。

什麼是*連結*？ Identity Synchronization for Windows 藉由儲存下列不會改變的唯一識別碼，使 Directory Server 與 Windows 中的相同使用者相互關聯：

- 每個 Directory Server 使用者項目的 `dspswuserlink` 屬性
- 每個 Active Directory 使用者的 `objectguid` 屬性
- 每位 Windows NT SAM 使用者的網域名稱及 `RID` 組合

儲存此不變的識別碼可使 Identity Synchronization for Windows 同步化其他重要的識別碼，如 `uid` 和 `cn`。執行下列動作時，會填入 `dspswuserlink` 屬性：

- Identity Synchronization for Windows 在 Directory Server 中建立新使用者 (從 Windows 同步化新使用者之後或透過執行 `idsync resync -c`)
- Identity Synchronization for Windows 在 Windows 上建立新使用者 (從 Directory Server 同步化新使用者之後或透過執行 `idsync resync -c -o Sun`)
- 您可以依照本章的說明，執行 `idsync resync -c -f` 來連結 Directory Server 及 Windows 中已存在的項目。

若要連結現有的使用者，您必須提供用於比對兩個目錄之間的使用者的規則。例如，若要連結兩個目錄中的某一使用者項目，兩個目錄項目中的姓氏與名字必須相符。

連結使用者項目及解決資料衝突不僅是一項技術，更是一門藝術。`idsync resync` 子指令在連結相對目錄來源中的兩個使用者時可能失敗的原因有許多項，並且主要是由連結目錄中資料的一致性決定。

使用 `idsync resync` 的一種策略便是使用 `-n` 引數，這樣可在「*安全模式*」下執行作業，因此您就能在不進行實際變更的情況下預覽作業的結果。在安全模式下執行可使您逐步修正連結條件，直到您找到一組理想的使用者符合條件爲止。

不過，您應該注意到，需要在連結準確性與連結範圍之間取得平衡。

例如，假設兩個目錄來源中包含一個雇員 ID 或社保卡號，您可能要從僅包括此號碼的連結條件著手。或許您會覺得還應該將姓氏屬性納入條件中，以提高連結準確性。不過，您可能會遺失連結，因爲本應只有 ID 符合的那些項目由於資料中姓氏值的不一致而未實現配對。此時您必須執行資料清除程序來清除無法連結的項目。

idsync resync 引數

idsync resync 指令接受以下引數：

表格 6-2 idsync resync 用法

引數	涵義
-f <*filename*>	使用 Identity Synchronization for Windows 提供的其中一個指定 XML 配置檔案，在未連結的使用者項目之間建立連結 (請參閱附錄 B，「LinkUsers XML 文件範例」)
-k	僅在未連結的使用者之間建立連結 (不建立使用者或修改現有的使用者)。您必須將此引數與 -f 引數搭配使用。
-a <*ldap-filter*>	指定 LDAP 篩選器來限制要同步化的項目 篩選器將套用到重新同步化作業的來源。 例如，如果您指定 idsync resync -o Sun -a "usid=*"，則具有 uid 屬性的所有 Directory Server 使用者都將同步化到 Active Directory。
-l <*sul-to-sync*>	指定要重新同步化的個別「同步化使用者清單 (SUL)」 **附註**：您可以指定多個 SUL ID 來重新同步化多個 SUL，或是如果您沒有指定任何 SUL ID，程式將重新同步化您全部的 SUL。
-o (Sun | Windows)	指定重新同步化作業的來源 • **Sun**：將 Windows 項目的屬性值設定爲 Sun Java System Directory Server 目錄來源項目中的對應屬性值。 • **Windows**：將 Sun Java System Directory Server 項目的屬性值設定爲 Windows 目錄來源項目中的對應屬性值。 (*預設爲 Windows*。)
-c	如果在目標位置找不到對應的使用者，則自動建立一個使用者項目 • 爲在 Active Directory 或 Windows NT 中建立的使用者隨機產生一個加密的安全密碼 • 爲在 Directory Server 中建立的使用者自動建立一個特殊的密碼值 ((PSWSYNC)***INVALID PASSWORD***) (除非指定 -i 選項) **附註**：Identity Synchronization for Windows 將嘗試建立使用者，即使您尚未在該方向配置建立項目。例如，如果您尚未配置 Identity Synchronization for Windows，以便從 Windows 同步化到 Sun (反之亦然)，但卻指定 -c 引數，Identity Synchronization for Windows 就會嘗試建立未找到的使用者。
-i (ALL_USERS | NEW_USERS | NEW_LINKED_USERS)	重設在 Sun 目錄來源中同步化的使用者項目的密碼，當下一次需要使用者密碼時，在目前的網域內強制對這些使用者進行密碼同步化。 • **ALL_USERS**：對所有同步化的使用者強制進行隨需密碼同步化 • **NEW_USERS**：僅對新建的使用者強制進行隨需密碼同步化 • **NEW_LINKED_USERS**：對所有新建或連結的使用者強制進行隨需密碼同步化 有關這些選項對密碼驗證所造成的影響的相關資訊，請參閱表格 6-3。

表格 6-2 idsync resync 用法 *(續上頁)*

引數	涵義
-u	更新物件快取。 此引數僅更新 Windows 目錄來源的使用者項目之本機快取，防止在 Directory Server 中建立已存在的 Windows 使用者。如果使用此引數，Windows 使用者項目便不會與 Directory Server 使用者項目實現同步。此引數只有在 resync 來源爲 Windows 時有效。
-x	刪除不符合來源項目的所有目標使用者項目。
-n	在安全模式下執行，如此您可在不進行實際變更的情況下預覽作業結果。

表格 6-3 idsync resync 是否會使得 Directory Server 上的使用者密碼失效？

	使用者在連結的 Active Directory 及 Directory Server 上有一個項目。	使用者在未連結的 Active Directory 及 Directory Server 上有一個項目。	使用者在 Active Directory 上有一個項目，但在 Directory Server 上沒有項目。
-i ALL_USERS	是	是	是
-i NEW_LINKED_USERS	否	是	是
-i NEW_USERS	否	否	是
無 -i 值	否	否	否

表格 6-4 提供了範例來說明組合不同引數的執行結果 (-h、-p、-D、-w、- 和 -s 引數爲預設值，並且爲了方便說明，在此將其省略)。

表格 6-4 idsync resync 用法範例

引數	結果
idsync resync	顯示 resync 用法說明。
idsync resync -i ALL_USERS	使所有使用者密碼失效，強制進行隨需密碼同步化 (僅適用於 Active Directory 環境)。 在混合環境 (具有 Active Directory 和 NT 網域) 中，必須明確列出 Active Directory SUL。
idsync resync -c -i NEW_USERS	建立未在 Directory Server 中找到的使用者，並使其密碼無效以強制執行隨需密碼同步化。使用此指令可將現有的 Windows 使用者填入空的 Directory Server 實例。

表格 6-4 idsync resync 用法範例 *(續上頁)*

引數	結果
`idsync resync`	顯示 `resync` 用法說明。
`idsync resync -c -l SUL_sales -l SUL_finance`	僅針對 SUL_sales 和 SUL_finance SUL 在 Directory Server 中建立全部現有的 Active Directory 使用者 (但不強制進行隨需密碼同步化)。
`idsync resync -n`	在安全模式下執行，如此您可在不進行任何實際變更的情況下預覽 `resync` 作業的結果。
`idsync resync -o Sun -a "(sn=Smith)"`	同步化 Windows 中所有姓氏爲 (sn) Smith 的 Directory Server 使用者。
`idsync resync -u`	僅更新 Windows 連接器的物件快取，以避免在 Directory Server 中建立現有使用者。實際上未同步化任何使用者。
`idsync resync -f link.cfg -k -i NEW_LINKED_USERS`	根據 `link.cfg` 檔案中所指定的連結條件來連結尚未連結的使用者。Identity Synchronization for Windows 不會建立或修改使用者，但是新連結使用者的 Directory Server 密碼會被設爲 Active Directory 使用者的密碼。

注意 當使用 `idsync resync` 連結使用者時，請注意您應該在作業中使用索引化屬性。未索引化的屬性可能會影響效能。

假如 UserMatchingCriteria 組內具有多個屬性，且其中至少一項已經過索引化，則可能會有較佳的效能。然而，若是 `UserMatchingCriteria` 中的屬性均未經過索引化，則對於處理大型目錄，效能恐怕難令人接受。

檢查中央日誌中的結果

所有 `idsync resync` 作業的結果均會在名爲 `resync.log` 的特定中央日誌中報告。此日誌會列出所有正確連結及同步化的使用者、連結失敗者，以及先前連結的使用者。

附註 某些現存的特殊 Active Directory 使用者 (如 Administrator 和 Guest) 在此日誌中可能出現失敗的結果。

啓動與停止同步化

啓動與停止同步化*不會*啓動或停止個別的 java 程序、常駐程式或服務。一旦開始同步化，停止同步化就只會暫停作業。當您重新啓動同步化時，程式會從它停止的位置繼續進行同步化，且不會遺失任何變更。

若要啓動或停止同步化：

1. 在「Sun Java System 伺服器主控台」瀏覽窗格中，選取 Identity Synchronization for Windows 實例。
2. 出現 Identity Synchronization for Windows 窗格時，按一下右上角的「開啓」按鈕。
3. 出現提示時，請輸入配置密碼。
4. 選取「工作」標籤 (圖 6-1)：

圖 6-1 啓動與停止同步化

   - 若要啓動同步化，請按一下「啓動同步化」。
   - 若要停止同步化，請按一下「停止同步化」。

附註 您也可使用 `idsync startsync` 及 `idsync stopsync` 指令行公用程式來啓動和停止同步化。有關詳細說明，請參閱第 321 頁上的「使用 startsync」及第 322 頁上的「使用 stopsync」。

啓動與停止服務

Identity Synchronization for Windows 和 Message Queue 以*常駐程式*的形式安裝在 Solaris 中，以*服務*的形式安裝在 Windows 中。這些程序會在系統啓動時自動啓動，但您也可以手動的方式啓動和停止它們，如下所示：

- **Solaris 系統**：在指令行中，
  - 輸入 `/etc/init.d/isw start` 以啓動所有 Identity Synchronization for Windows 程序。
  - 輸入 `/etc/init.d/isw stop` 以停止所有 Identity Synchronization for Windows 程序。
  - 輸入 `/etc/init.d/imq start` 以啓動 Message Queue 代理程式。
  - 輸入 `/etc/init.d/imq stop` 以停止 Message Queue 代理程式。
- **Windows 系統**：
  - 從 Windows「開始」功能表中：
    I. 選取「開始」>「設定」>「控制台」>「系統管理服務」。
    II. 出現「系統管理服務」對話方塊時，按兩下「服務」圖示來開啓「服務」對話方塊。
    III. 選取 Identity Synchronization for Windows，然後從功能表列中選取「動作」>「啓動」(或「停止」)。對 iMQ Broker 重複此步驟。
  - 在指令行中，輸入 `net` 指令來控制服務。

附註 停止 Identity Synchronization for Windows 常駐程式 / 服務後並在重新啓動它之前，暫停 30 秒。連接器需要花費數秒時間才能完全關閉它們。

第 7 章

遷移至 Identity Synchronization for Windows 1 2004Q3

本章說明如何將系統從 Sun Java System Identity Synchronization for Windows 1.0 版遷移至 1 2004Q3 版。

附註 Identity Synchronization for Windows 1.0 版附帶安裝 Message Queue，*但 Identity Synchronization for Windows* 2004Q3 *不會執行這樣的安裝*。

安裝說明請參閱 Sun Java System Message Queue 產品文件。

內容分作以下各節：

概況

要從 Identity Synchronization for Windows 1.0 版 (或 1.0 SP1 版) 遷移到 1 2004Q3，需完成幾個主要階段：

1. 準備 Identity Synchronization for Windows 1.0 版 (或 1.0 SP1) 安裝，以進行遷移。
2. 解除安裝 Identity Synchronization for Windows 1.0 版 (或 1.0 SP1)。
3. 安裝或升級附屬產品。
4. 使用您備份的配置和連接器狀態來安裝 Identity Synchronization for Windows 1 2004Q3。

附註 在您安裝 Identity Synchronization for Windows 1.0 版 (或 1.0 SP1) 的同一個平台和架構上安裝 Identity Synchronization for Windows 1 2004Q3。

遷移準備工作

開始遷移過程之前：

- 請先熟悉 Sun Java System Identity Synchronization for Windows 1 版的新特色及功能 2004Q3。
- 閱讀第 2 章，「準備安裝」。中有助於規劃您的遷移程序的安裝及配置資訊。
- 記錄您的 1.0 版部署及配置。確實記下您在配置中所做的任何自訂化設定。
- 排程遷移。
  由於遷移程序至少需要四個小時，所以您可以排程在下班時間遷移。

當您將系統從 1.0 版遷移至 1 2004Q3 期間發生使用者輸入密碼或屬性變更情況，Identity Synchronization for Windows 將對這些變更進行以下處理：

- **Active Directory 系統**：凡於遷移過程中在 Active Directory 上所做的任何密碼變更，將於遷移程序完成後由 Directory Server 外掛程式進行隨需同步化。
- **Directory Server**：凡於遷移過程中在 Directory Server 上所做的任何密碼變更，一概不予同步化。不過，您可以在遷移程序完成後，從 Identity Synchronization for Windows 1 2004Q3 日誌中識別受影響的使用者。(請參閱第 233 頁上的「檢查日誌」。)
- **Windows NT**：凡於遷移過程中在 NT 上所做的任何密碼變更，一概不予同步化。

  不過，可以利用 `forcepwchg` 公用程式，識別受影響的使用者並強制其再次變更密碼。(請參閱第 198 頁上的「強制在 Windows NT 上變更密碼」與第 233 頁上的「檢查日誌」以取得詳細資訊。)
- 在遷移過程中發生的所有其他屬性變更 (在所有目錄來源),都將於遷移程序完成後予以同步化。

準備遷移

您將使用以下一或多個公用程式，從 1.0 版遷移至 1 2004Q3 版：

- **`export10cnf`**：此爲獨立式公用程式，可用來建立從 Identity Synchronization for Windows 1.0 配置匯出的配置檔案。(詳細資訊，請參閱第 190 頁上的「匯出 1.0 版配置」。)

  匯出後的 XML 文件內含目錄部署的拓樸，以及足以配置 Identity Synchronization for Windows 版 1 2004Q3 安裝的資訊。
- **`checktopics`**：此公用程式用來檢查 1.0 安裝版本中的 Message Queue 同步化主題，並確定佇列中是否留有任何尚未傳送的訊息。

  當您停止 1.0 同步化後，更新項目仍會保留在 Message Queue 中。進行遷移前，必須驗證 Message Queue 中是否無任何更新項目存在。(詳細資訊，請參閱第 196 頁上的「檢查未傳送的訊息」。)
- **`forcepwchg`**：此爲 Windows NT 工具，能讓您識別哪些使用者的密碼在遷移過程中發生變更，並於您的 1 2004Q3 版系統準備就緒時，強制該使用者再次變更密碼。(遷移期間於 Windows NT 上所做的密碼變更擷取不到。) (詳細資訊，請參閱第 198 頁上的「強制在 Windows NT 上變更密碼」。)

附註 上述公用程式便於讓 Identity Synchronization for Windows 1.0 版遷移至 1 2004Q3 版。遷移作業需在部署有 Identity Synchronization for Windows 1.0 的環境中執行。因此，上述公用程式僅在 Solaris/SPARC 及 Windows 套裝軟體中提供。

遷移公用程式位在 `migration` 安裝目錄中，無需執行額外的安裝步驟。

匯出 1.0 版配置

安裝連接器之前，您可以使用 `export10cnf` 公用程式，將現有的 1.0 版配置匯出成 XML 檔，然後使用 `idsync importcnf` 指令將該檔迅速無誤地匯入 1 2004Q3 系統。

提示 雖然可以透過 Identity Synchronization for Windows 主控台手動重新輸入 1.0 配置，但在此強烈建議您使用 `export10cnf` 公用程式。如果您決定不使用 `export10cnf`，則將無法保留連接器的配置狀態。

匯出 1.0 版配置的好處如下：

- 不必再透過管理主控台執行絕大多數的初步配置程序。
- 可確保 1 2004Q3 版中指定的連接器 ID 與 1.0 版所使用的連接器 ID 相符，如此能大幅簡化保留現有連接器狀態所需的工作，使它們可直接在 1 2004Q3 版部署中使用。

  (基本上，您需備份 `persist` 和 `etc` 目錄，之後只要將其還原即可，完全無需擔心基礎目錄結構問題)。

`export10cnf` 公用程式位在 `migration` 安裝目錄中，無需執行額外的安裝步驟。

使用 export10cnf 公用程式

若要將 Identity Synchronization for Windows 配置匯出到 XML 檔案，請按如下步驟從 `migration` 目錄執行 `export10cnf`：

- 開啓終端機視窗並鍵入：

```
java -jar export10cnf.jar -h <hostname> -p <port> -D <bind DN>
-w <bind password> -s <rootsuffix> -q <configuration password> -Z
-P <cert-db-path> -m <secmod-db-path> -f <filename>
```

例如，

```
java -jar export10cnf.jar -D "cn=dirmanager" -w - -q - -s
"dc=example,dc=com" -f exported-configuration
```

export10cnf 公用程式與 Identity Synchronization for Windows 指令行公用程式共用相同的共用引數 (請參閱第 306 頁上的「共用引數」)。唯一的 export10cnf 專用選項是 -f *<filename>*。如果作業成功，則此公用程式會將目前的配置匯出至引數 -f 所指定的檔案中。

插入明文密碼

基於安全性考慮，export10cnf 公用程式不會從 1.0 版配置匯出明文密碼。代之，該公用程式會在 cleartextPassword 欄位的適當地方插入空字串。例如，

```
<Credentials
        userName="cn=iswservice,cn=users,dc=example,dc=com"
        cleartextPassword=""/>
        <!-- INSERT PASSWORD BETWEEN THE DOUBLE QUOTES IN THE ABOVE FIELD
-->
```

您必須在匯出的配置檔案中，逐一將密碼手動輸入到每個 cleartextPassword 欄位的雙引號之間，*才能將該檔案匯入 Identity Synchronization for Windows 1 2004Q3*。(importcnf 驗證可避免將空密碼值匯入配置檔案中。)

例如，

```
<Credentials
        userName="cn=iswservice,cn=users,dc=example,dc=com"
        cleartextPassword="mySecretPassword"/>
        <!-- INSERT PASSWORD BETWEEN THE DOUBLE QUOTES IN THE ABOVE
FIELD -->
```

匯出配置檔案範例

第 192 頁上的代碼範例 7-1 舉出匯出後的配置檔案範例。

在此檔案中，

- ad-host.example.com 係指 Active Directory 網域控制器。
- ds-host.example.com 係指執行 Sun Java System Directory Server 的主機。

代碼範例 7-1 匯出配置檔案範例

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

<ActiveConfiguration>
  <SunDirectorySource
    parent.attr="DirectorySource"
    onDemandSSLOption="true"
    maxConnections="5"
    displayName="dc=example,dc=com"
    resyncInterval="1000">
    <SynchronizationHost
      hostOrderOfSignificance="1"
      hostname="ds-host.example.com"
      port="389"
      portSSLOption="true"
      securePort="636">
      <Credentials
        userName="uid=PSWConnector,dc=example,dc=com"/>
    </SynchronizationHost>
<SyncScopeDefinitionSet
      index="0"
      location="ou=people,dc=example,dc=com"
      filter=""
      creationExpression="cn=%cn%,ou=people,dc=example,dc=com"
      sulid="SUL"/>
  </SunDirectorySource>
<ActiveDirectorySource
parent.attr="DirectorySource"
    displayName="example.com"
    resyncInterval="1000">
```

```
<SyncScopeDefinitionSet
      index="0"
      location="cn=users,dc=example,dc=com"
      filter=""
      creationExpression="cn=%cn%,cn=users,dc=example,dc=com"
      sulid="SUL"/>
</ActiveDirectorySource>
<ActiveDirectoryGlobals
    flowInboundCreates="true"
    flowInboundModifies="true"
    flowOutboundCreates="true"
flowOutboundModifies="true">
    <AttributeDescription
      parent.attr="CreationAttribute"
name="samaccountname"
syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
<AttributeMap>
      <AttributeDescription
        parent.attr="WindowsAttribute"
        name="samaccountname"
        syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
      <AttributeDescription
        parent.attr="SunAttribute"
        name="uid"
        syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
    </AttributeMap>
<AttributeDescription
      parent.attr="SignificantAttribute"
      name="description"
      syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
<AttributeMap>
      <AttributeDescription
        parent.attr="SunAttribute"
        name="sn"
        syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
<AttributeDescription
        parent.attr="WindowsAttribute"
        name="sn"
        syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
    </AttributeMap>
```

```
<SynchronizationHost
      hostOrderOfSignificance="1"
      hostname="ad-host.example.com"
      port="389"
      portSSLOption="true"
      securePort="636">
      <Credentials
        userName="cn=iswservice,cn=users,dc=example,dc=com"
        cleartextPassword=""/>
        <!-- INSERT PASSWORD BETWEEN THE DOUBLE QUOTES IN THE ABOVE FIELD -->
    </SynchronizationHost>
<AttributeDescription
      parent.attr="CreationAttribute"
      name="cn"
      syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
    <TopologyHost
      parent.attr="SchemaLocation"
hostname="ad-host.example.com"
      port="3268"
      portSSLOption="true"
      securePort="3269">
      <Credentials
        parent.attr="Credentials"
        userName="cn=iswservice,cn=users,dc=example,dc=com"
        cleartextPassword=""/>
        <!-- INSERT PASSWORD BETWEEN THE DOUBLE QUOTES IN THE ABOVE FIELD -->
    </TopologyHost>
    <TopologyHost
      parent.attr="HostsTopologyConfiguration"
      hostname="ad-host.example.com"
      port="3268"
      portSSLOption="true"
      securePort="3269">
<Credentials
        parent.attr="Credentials"
        userName="cn=iswservice,cn=users,dc=example,dc=com"
        cleartextPassword=""/>
        <!-- INSERT PASSWORD BETWEEN THE DOUBLE QUOTES IN THE ABOVE FIELD -->
    </TopologyHost>
<AttributeMap>
      <AttributeDescription
        parent.attr="SunAttribute"
        name="cn"
        syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
```

```
 <AttributeDescription
        parent.attr="WindowsAttribute"
        name="cn"
        syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
    </AttributeMap>
<AttributeMap>
      <AttributeDescription
        parent.attr="SunAttribute"
        name="description"
        syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
<AttributeDescription
        parent.attr="WindowsAttribute"
name="description"
        syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
    </AttributeMap>
</ActiveDirectoryGlobals>
<SunDirectoryGlobals
    userObjectClass="inetorgperson"
    flowInboundCreates="true"
    flowInboundModifies="true"
    flowOutboundCreates="true"
    flowOutboundModifies="true">
<TopologyHost
      parent.attr="SchemaLocation"
      hostname="ds-host.example.com"
      port="389"
      portSSLOption="false"
      securePort="636">
      <Credentials
        parent.attr="Credentials"
        userName="cn=directory manager"
        cleartextPassword=""/>
        <!-- INSERT PASSWORD BETWEEN THE DOUBLE QUOTES IN THE ABOVE FIELD -->
    </TopologyHost>
   <TopologyHost
      parent.attr="HostsTopologyConfiguration"
      hostname="ds-host.example.com"
      port="389"
      portSSLOption="false"
      securePort="636"><Credentials
        parent.attr="Credentials"
        userName="cn=directory manager"
        cleartextPassword=""/>
        <!-- INSERT PASSWORD BETWEEN THE DOUBLE QUOTES IN THE ABOVE FIELD -->
    </TopologyHost>
```

```
<AttributeDescription
      parent.attr="SignificantAttribute"
      name="description"
      syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
<AttributeDescription
      parent.attr="CreationAttribute"
      name="sn"
      syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
    <AttributeDescription
      parent.attr="CreationAttribute"
      name="cn"
      syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
  </SunDirectoryGlobals>
</ActiveConfiguration>
```

配置匯出完成後，export10cnf 會報告這項作業的結果。假如作業失敗，則顯示適當錯誤訊息及錯誤識別碼。

檢查未傳送的訊息

Identity Synchronization for Windows 1.0 至 1 2004Q3 遷移程序藉由保留現有部署中的連接器狀態，將系統停機的可能降到最低。不過，這些狀態僅能夠反映出 Message Queue 最後一次收到並確認的變更，您無法確切得知訊息是否確實傳出並套用至目標連接器。

此情況下，只要 Message Queue 沒有變動即不會造成問題，然而 Message Queue 上的任何訊息會在遷移程序中 (您安裝 Message Queue 3.5 SP1 時) 遺失。

進行遷移前，請務必驗證現有 Message Queue 的同步化主題中不含任何未傳送的訊息。Identity Synchronization for Windows checktopics 公用程式可用來驗證所有的同步化主題是否均是空的 (且系統靜止無動作)。

使用 checktopics 公用程式

Solaris/SPARC 及 Windows Identity Synchronization for Windows 1 2004Q3 套裝軟體的 migration 目錄中提供 checktopics 公用程式。

附註 執行 checktopics 的唯一先決條件是使用適當的 Java 虛擬機器 (1.4.2_04 版或更新版本)。

執行 checktopics 公用程式時，它會連接配置目錄，其中包含有關「同步化使用者清單 (SUL)」和 Message Queue 目前使用的同步化主題名稱的資訊。此外，當您執行 checktopics 時，它會詢問 Message Queue 以得知各個作用中的同步化主題中尚留有多少未傳送的訊息，然後向您顯示查詢到的資訊。

若要執行 checktopics 指令行公用程式：

a. 開啓終端機視窗並使用 **cd** 指令進入 migration 目錄。

b. 從指令提示符號下，鍵入以下子指令：

```
java -jar checktopics.jar -h <hostname> -p <port> -D <bind_DN>
-w <bind_password> -s <root_suffix> -q <configuration_password> -Z
```

例如，

```
java -jar checktopics.jar -D "cn=directory manager" -w - -s
"dc=example,dc=com" -q -
```

附註

- 有關 checktopics 引數的詳細資訊，請參閱第 306 頁上的「共用引數」。
- 有關使用 checktopics 的詳細資訊，請參閱第 196 頁上的「檢查未傳送的訊息」。

執行 checktopics 後，檢查終端機是否留有訊息：

- 如果作業執行成功，終端機會顯示訊息表示日誌中已無未傳送的訊息。
- 假如作業失敗，則顯示適當錯誤訊息及錯誤識別碼。

清除訊息

如果作用中的同步化主題中仍有未傳送的訊息，可參照下列程序來清除訊息：

1. 重新啓動同步化。
2. 等候訊息套用至目標連接器。
3. 停止同步化。
4. 重新執行 `checktopics`。

強制在 Windows NT 上變更密碼

在 Windows NT 上進行遷移的過程中，系統不會監視密碼變更，也不會擷取新的密碼值。因此，當遷移完成後，無從判定新的密碼值。

與其在遷移至 1 2004Q3 之後要求所有的使用者變更密碼，較好的方法是使用 `forcepwchg` 指令行公用程式向所有在遷移過程中變更密碼的使用者發出密碼變更要求。

附註 `forcepwchg` 公用程式僅在 Windows 套裝軟體中提供。

`forcepwchg` 公用程式位在 Windows `migration` 目錄中。直接從該目錄執行 `forcepwchg` 即可，無需執行額外的安裝步驟。

您必須在安裝有 NT 元件 (連接器、變更偵測器 DLL 及密碼篩選器 DLL) 的主要網域控制器 (PDC) 主機上執行 `forcepwchg`，不能從遠端執行 `forcepwchg`。

`forcepwchg` 公用程式亦可輸出嘗試遷移的帳號名稱 (一列一個帳號名稱)。若遷移過程中發生錯誤，錯誤可能發生在遷移最後輸出的使用者帳號期間。

遷移系統

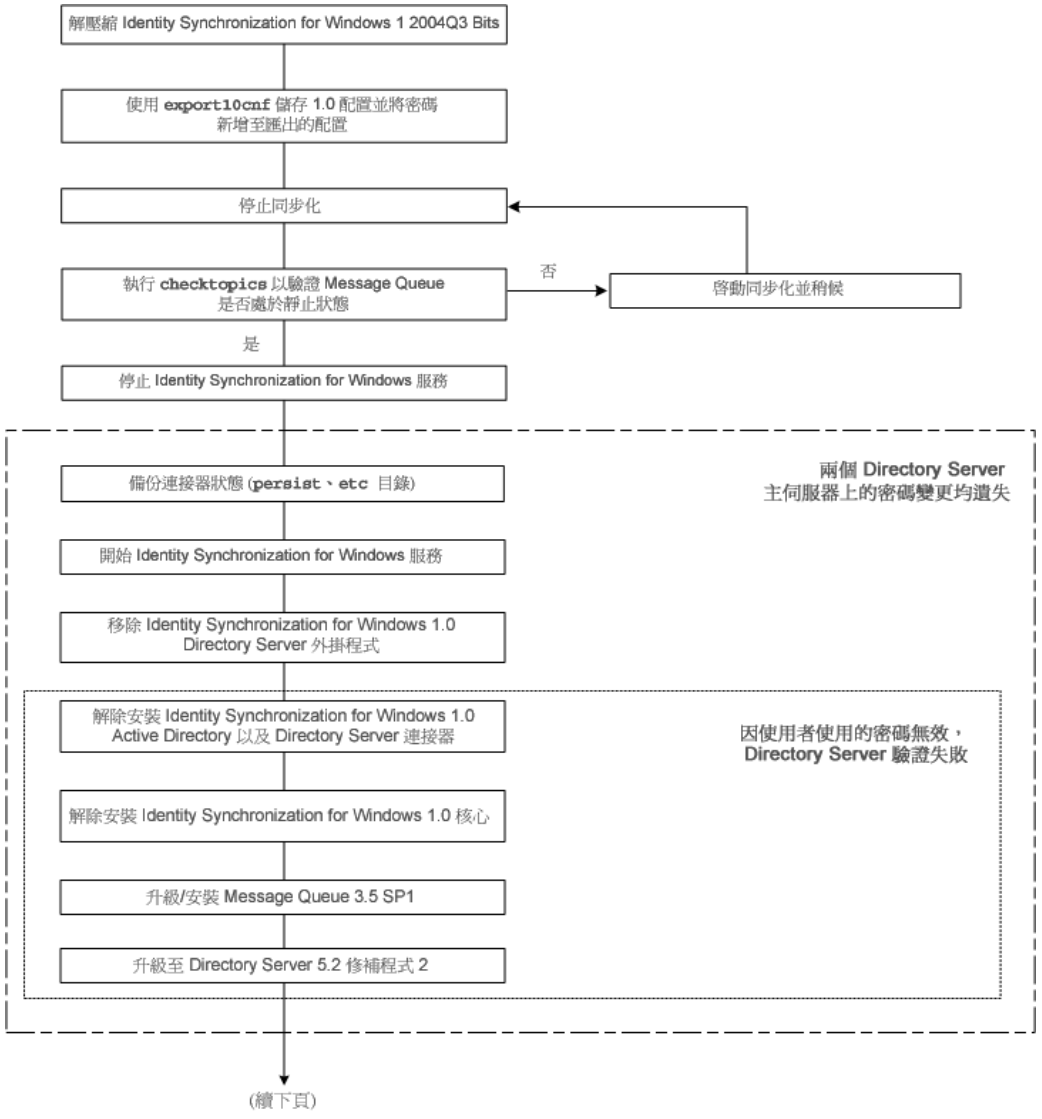
本節說明如何將單一主機部署遷移成 1 2004Q3 版。在單一主機部署中，所有的 Identity Synchronization for Windows 元件均安裝在一台主機上 (Windows 2000 Server、Solaris 8 或 9，或者 SPARC)，這些元件有：

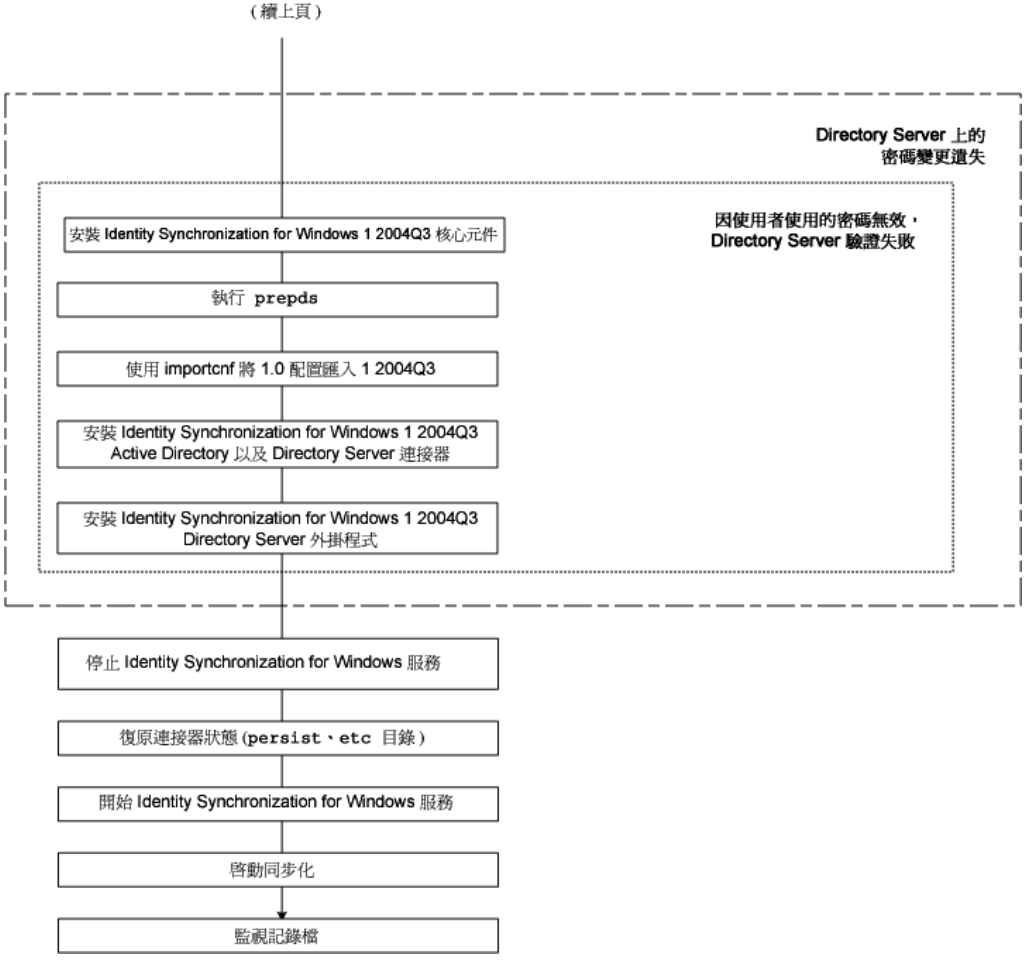
- Directory Server (單一實例)
- 核心 (Message Queue、中央記錄程式、系統管理員及主控台)
- Active Directory 連接器
- Directory Server 連接器
- Directory Server 外掛程式

附註 如果您使用 Solaris 作爲安裝主機，則需要有一台含 Active Directory 的 Windows 2000 電腦專門用來進行同步化。(Windows 2000 電腦上不需安裝任何元件。)

下圖繪示遷移程序，同時可將其視爲補充後述遷移說明的檢查清單。

圖 7-1 遷移單一主機部署




（續上頁）
Directory Server 上的
密碼變更遺失
因使用者使用的密碼無效，
Directory Server 驗證失敗
安裝 Identity Synchronization for Windows 1 2004Q3 核心元件
執行 prepds
使用 importcnf 將 1.0 配置匯入 1 2004Q3
安裝 Identity Synchronization for Windows 1 2004Q3
Active Directory 以及 Directory Server 連接器
安裝 Identity Synchronization for Windows 1 2004Q3
Directory Server 外掛程式
停止 Identity Synchronization for Windows 服務
復原連接器狀態 (persist、etc 目錄)
開始 Identity Synchronization for Windows 服務
啓動同步化
監視記錄檔

準備遷移

參照以下程序，準備將 Identity Synchronization for Windows 1.0 版遷移成 1 2004Q3 版：

1. 透過指令提示符號：
   - **Solaris 或 SPARC 系統：**鍵入 **`uncompress -c <`***filename***`> | tar xf -`**
   - **Windows 系統：**鍵入 **`%JAVA_HOME%\bin\jar -xf <`***filename***`>** (或使用任何 Windows 的 zip 歸檔程式，如 WinZip®)。

   解壓縮二進位碼檔案後，您會看到內含遷移所需工具的如下子目錄：
   - `installer/`
   - `lib/`
   - `migration/`

Solaris	Windows
export10cnf.jar	export10cnf.jar
—	forcepwchg.exe
checktopics.jar	checktopics.jar

2. 將 1.0 版配置設定匯出成 XML 檔。依照 第 190 頁上的「使用 export10cnf 公用程式」的說明，從 `migration` 目錄下執行 `export10cnf`。例如：

   ```
   java -jar export10cnf.jar -D "cn=directory manager" -w - -s
   "dc=example,dc=com" -q - -f export.cfg
   ```

3. 將密碼加入匯出後的 XML 檔。

   在匯出的配置檔案中，將密碼輸入各 `cleartextPassword` 欄位的雙引號之間 (請參閱第 191 頁上的「插入明文密碼」)。

4. 如第 184 頁上的「啓動與停止同步化」所述，停止同步化。

5. 確認您的系統是否在休眠狀態。依照 第 197 頁上的「使用 checktopics 公用程式」的說明，從 `migration` 目錄下執行 `checktopics`。

   例如：

   ```
   java -jar checktopics.jar -D "cn=directory manager" -w - -s
   "dc=example,dc=com" -q -
   ```

6. 如第 185 頁上的「啓動與停止服務」所述，停止 Identity Synchronization for Windows 服務 (常駐程式)。

   附註 請勿在此時停止 Sun ONE Message Queue 服務。

7. *僅限 Windows NT* - 停止 Sun One NT 變更偵測器服務。您可以鍵入下列指令，從指令行停止服務

   ```
   net stop "Sun One NT ChangeDetector Service"
   ```

8. *僅限 Windows NT* - 按如下步驟儲存 NT 變更偵測器服務計數器：

   a. 執行 `regedt32.exe` 來開啓「登錄編輯程式」。

   b. 選取 `HKEY_LOCAL_MACHINE` 視窗。

   c. 導覽到 `SOFTWARE\Sun Microsystems\PSW\1.0` 節點。

   d. 儲存以下登錄值：

      - `HighestChangeNumber`
      - `LastProcessedSecLogRecordNumber`
      - `LastProcessedSecLogTimeStamp`
      - `QueueSize`

9. 從現有的 1.0 安裝目錄樹備份 `persist` 和 `etc` 目錄，來儲存連接器狀態。

   - **Solaris 系統**：鍵入 **`cd <`*`serverroot`*`>/isw-<`*`hostname`*`>`**
     `tar cf /var/tmp/connector-state.tar persist etc`
   - **Windows 系統**：鍵入 **`cd <`*`serverroot`*`>\isw-<`*`hostname`*`>`**
     `zip -r C:\WINNT\Temp\connector-state.zip persist etc`
     `%JAVA_HOME%\bin\jar -cfM %TEMP%\connector-state.jar persist etc`
     (或使用任何 Windows 的 zip 歸檔程式，如 WinZip)

10. 啓動 Identity Synchronization for Windows 服務 (請參閱第 185 頁)。

    附註 您不必啓動 Sun ONE Message Queue 服務，因爲您從未停止它。

解除安裝 Identity Synchronization for Windows

附註 如果 SUNWjss 套裝軟體未註冊供 Identity Synchronization for Windows 1.0 以外的其他應用程式使用，則 Identity Synchronization for Windows 1.0 解除安裝程式會移除該套裝軟體。這種情形特別容易發生在當您在 Solaris 電腦上安裝 Directory Server 5.2.2 的壓縮版本時，此時解除安裝程式會將 `jss3.jar` 檔案從 `/usr/share/lib/mps/secv1` 移除。

如果您在遷移至 Identity Synchronization for Windows 11 2004Q3 時遇到這種情形，安裝程式將會回報缺少一個必要檔案，並將該檔案的名稱記錄在安裝日誌中。發生這種情形時，您必須重新安裝必要的修補程式 (請參閱第 56 頁上的「Sun Java System 軟體需求」) 並重新啓動安裝程序。

完成準備步驟後，您即可開始按如下步驟解除安裝 Identity Synchronization for Windows 1.0 版 (或 1.0 SP1)：

1. 手動解除安裝 Directory Server 外掛程式，並重新啓動所有安裝了外掛程式的 Directory Server。
2. 在安裝了外掛程式的每台 Directory Server 上執行下列步驟：
   a. 從 Directory Server 移除下列項目：

      ```
      cn=config,cn=pswsync,cn=plugins,cn=config
      cn=pswsync,cn=plugins,cn=config
      ```

      例如：

      ldapdelete -D "cn=directory manager" -w - -p <*port*> -c cn=config, cn=pswsync,cn=plugins,cn=config cn=pswsync,cn=plugins,cn=config

   b. 重新啓動 Directory Server。
      - **Solaris 系統**：鍵入 **<*serverroot*>/slapd-<*hostname*>/restart-slapd**
      - **Windows 系統**：鍵入 **<*serverroot*>\slapd-<*hostname*>\restart-slapd.bat**

   c. 從系統移除外掛程式二進位碼檔案。
      - **Solaris 系統**：鍵入 **rm <*serverroot*>/lib/psw-plugin.so**
        rm <*serverroot*>/lib/64/psw-plugin.so

- **Windows 系統**：鍵入 **del <*serverroot*>\lib\psw-plugin.dll**

3. 將目錄變更 (**cd**) 爲 **<*server_root*>\isw-<*hostname*>**，再使用 Identity Synchronization for Windows 1.0 解除安裝程式來解除安裝 1.0/1.0 SP1 版連接器及核心元件。

附註 您務必先解除安裝連接器，再解除安裝核心元件。

- **Solaris 或 SPARC 系統**：鍵入 **./runUninstaller.sh**
- **Windows 系統**：鍵入 **\runUninstaller.bat**

4. 使用下列步驟，從產品登錄檔案移除 Identity Synchronization for Windows 相關的項目：

   a. 備份檔案的副本，位置如下所示：

   - **Solaris 系統**：`/var/sadm/install/productregistry`
   - **Windows 系統**：`C:\WINNT\System32\productregistry`

   b. 若要從產品登錄檔案移除 Identity Synchronization for Windows 的相關項目，請遵循「從 Solaris 系統手動解除安裝 1.0 核心程式與實例」的步驟 6 說明操作

5. *僅限 Windows 系統* - 將核心程式解除安裝後重新開機。

附註 如果解除安裝因故失敗，可能需要手動解除安裝 Identity Synchronization for Windows 元件。此部分之說明請參閱第 209 頁上的「解除安裝 1.0 失敗時之處理」。

6. *僅限 Windows 系統* - 確認 Identity Synchronization for Windows 目前並未執行。必要時，您可以鍵入下列指令，從指令行停止服務

```
net stop "Sun ONE Identity Synchronization for Windows"
```

   若此服務在解除安裝完成後繼續執行，則會導致共用違規，使您無法刪除實例目錄。

7. 移除 Identity Synchronization for Windows 實例目錄 (`isw-<hostname>`)。

安裝或升級附屬產品

使用下列步驟來升級 Java Runtime Environment、安裝 Message Queue 及升級 Directory Server：

1. 在安裝了 Identity Synchronization for Windows 元件的每台主機 (Windows NT 除外) 上升級 Java 2 Runtime Environment (或 Java 2 SDK)。(版本不應低於 1.4.2_04。)

   - **Java 2 SDK**：http://java.sun.com/j2se/1.4.2/install.html
   - **Java 2 Runtime Environment**：http://java.sun.com/j2se/1.4.2/jre/install.html

2. 依照 *《Sun Java SystemMessage Queue 3.5 SP1 Installation Guide》*之說明，安裝 Message Queue 3.5 SP1。

3. 依照 *《Sun Java System Directory Server 5 2004Q2 Installation and Migration Guide》*之說明，將 Directory Server 升級至 5.2 SP2 版，該文件可於以下位置取得：

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

   Directory Server 升級會保留您目前的 Directory Server 配置與資料庫。

安裝 Identity Synchronization for Windows 1 2004Q3

依照下列步驟安裝 Identity Synchronization for Windows 1 2004Q3 元件：

1. 安裝 Identity Synchronization for Windows 1 2004Q3 核心程式。(請參閱第 87 頁上的「安裝核心程式」)
2. 針對 Directory Server 執行 `idsync prepds` 以更新模式，方法如下。
   - **Solaris 系統**：鍵入 **`cd /opt/SUNWisw/bin`**
     再鍵入：**`idsync prepds <`***arguments***`>`**
   - **Windows 系統**：鍵入 **`cd \<`***serverroot***`>\isw-<`***hostname***`>\bin`**
     再鍵入：**`idsync prepds <`***arguments***`>`**

   有關 `idsync prepds` 的詳細資訊，請參閱附錄 A，「使用 Identity Synchronization for Windows 指令行公用程式」。
3. 鍵入如下指令，匯入 1.0 版 XML 配置檔案

   `idsync importcnf <`*arguments***`>`**

   附註 當程式在您的輸入配置檔案中偵測到錯誤時，就會發生錯誤。Identity Synchronization for Windows 將中斷 `importcnf` 程序，並提供必要的資訊來更正錯誤。

   有關使用 `idsync importcnf` 的詳細資訊，請參閱附錄 A 中的「使用 importcnf」。
4. 安裝 Identity Synchronization for Windows 1 2004Q3 連接器 (請參閱第 162 頁上的「安裝連接器」)。
5. 安裝 Identity Synchronization for Windows 1 2004Q3 Directory Server 外掛程式 (第 173 頁上的「安裝 Directory Server 外掛程式」)。
6. 如第 185 頁上的「啓動與停止服務」所述，停止 Identity Synchronization for Windows 服務 (常駐程式)。
7. *僅限 Windows NT* - 停止 Sun Java™ System NT 變更偵測器服務。您可以鍵入下列指令，從指令行停止服務

   `net stop "Sun Java(TM) System NT Change Detector"`
8. *僅限 Windows NT* - 還原 NT 變更偵測器服務計數器：
   a. 執行 `regedt32.exe` 來開啓「登錄編輯程式」。

b. 選取 HKEY_LOCAL_MACHINE 視窗。

c. 導覽到 SOFTWARE\Sun Microsystems\Sun Java(TM) System Identity Synchronization for Windows\1.1 節點。

d. 按兩下以下每個項目來還原其值 (您在解除安裝 1.0 版之前所儲存的值)：

- HighestChangeNumber
- LastProcessedSecLogRecordNumber
- LastProcessedSecLogTimeStamp
- QueueSize

9. *僅限 Windows NT* - 啓動 Sun Java™ System NT 變更偵測器服務。您可以鍵入下列指令，從指令行啓動服務

```
net start "Sun Java(TM) System NT Change Detector"
```

10. 移除實例目錄中的 1 2004Q3 persist 和 etc 目錄 (及其所有內容)，並還原您在第 202 頁上的「準備遷移」中備份的 1.0 版 (或 1.0 SP1) 的 persist 和 etc 目錄。

- **Solaris 系統**：鍵入

```
cd /var/opt/SUNWisw
rm -rf etc persist
tar xf /var/tmp/connector-state.tar
```

- **Windows 系統**：鍵入

```
cd <serverroot>\isw-<hostname>
rd /s etc persist
%JAVA_HOME%\bin\jar -xf %TEMP%\connector-state.jar
```

(或使用任何 Windows 的 zip 歸檔程式，如 WinZip)

11. 啓動 Identity Synchronization for Windows 服務 (請參閱第 185 頁)。

12. 如第 184 頁上的「啓動與停止同步化」所述，啓動同步化。

13. 檢查中央稽核日誌，驗證是否無任何警告訊息。

附註 如果您曾自訂 1.0 版日誌設定，則必須將那些自訂化設定手動套用至 1 2004Q3 版安裝。請使用 Identity Synchronization for Windows 主控台配置 1 2004Q3 版日誌設定。

解除安裝 1.0 失敗時之處理

如果 1 2004Q3 版安裝程式發現 1.0 版系統元件殘留，1 2004Q3 安裝就會失敗。因此，開始安裝 1 2004Q3 版之前，應驗證系統上已徹底移除所有的 1.0 元件。

若解除安裝程式不解除安裝所有的 1.0/1.0 SP1 版元件，則您必須手動清除 Identity Synchronization for Windows 產品登錄及 Solaris 套裝軟體。

有關手動解除安裝 Identity Synchronization for Windows 1.0 版之詳細指示如以下三節所述：

- 第 210 頁上的「從 Solaris 系統手動解除安裝 1.0 核心程式與實例」
- 第 216 頁上的「從 Windows 2000 手動解除安裝 1.0 核心程式與實例」
- 第 222 頁上的「從 Windows NT 手動解除安裝 1.0 實例」

附註 本節中提供的說明僅適用於解除安裝 Identity Synchronization for Windows *1.0 版*。

除非 Identity Synchronization for Windows 解除安裝程式失敗，否則*請勿*使用下列各節提供的手動解除安裝程序。

從 Solaris 系統手動解除安裝 1.0 核心程式與實例

請參照本節之說明，手動解除安裝 Solaris 電腦上的核心程式。

附註 在本節中，Identity Synchronization for Windows 的位置描述如下：

<serverroot>/isw-*<hostname>*

其中，*<serverroot>* 表示 Identity Synchronization for Windows 安裝位置的父目錄。

例如，假設您將 Identity Synchronization for Windows 安裝在 /var/Sun/mps/isw-*<example>*，則 *<serverroot>* 應爲 /var/Sun/mps。

1. 在終端機視窗中鍵入 **/etc/init.d/isw stop** 以停止所有的 Identity Synchronization for Windows Java 程序。

   如果上述指令並未停止所有的 Java 程序，請鍵入：

   /usr/ucb/ps -gauxwww | grep java

   kill -s SIGTERM < ***由上述指令而得的程序 ID*****>**

2. 按如下方法停止 Message Queue：

   a. 在提示符號下，鍵入以下指令停止 Message Queue 代理程式：

      /etc/init.d/imq stop

   b. 若要停止任何剩餘的 imq 程序，鍵入：

      *** ps -ef | grep imqbroker**

      *** kill -s SIGTERM <** ***由上述指令而得的程序 ID*****>**

c. 使用下列方法之一來解除安裝代理程式套裝軟體及目錄：

- 使用 Message Queue 代理程式解除安裝程序檔 (位在您安裝核心程式的主機之 Identity Synchronization for Windows 實例目錄中) 來解除安裝代理程式。鍵入：

  /<*serverroot*>/isw-<*hostname*>/imq_uninstall

- 按如下方法手動解除安裝套裝軟體及目錄：

  使用 pkgrm：指令移除以下套裝軟體：

SUNWaclg	SUNWiqum	SUNWiqjx
SUNWiqlen	SUNWxsrt	SUNWiqu
SUNWjaf	SUNWiqfs	SUNWjhrt
SUNWiqdoc	SUNWiquc	SUNWiqsup
SUNWiqr	SUNWjmail	

  使用 rm -rf 指令移除以下目錄：

  ```
  rm -rf /etc/imq
  rm -rf /var/imq
  rm -rf /usr/bin/imq*
  ```

3. 若要移除 Identity Synchronization for Windows 1.0 Solaris 套裝軟體，請針對表格 7-1 中所列的各套裝軟體逐一執行 pkgrm <*packageName*>。(例如 **pkgrm SUNWidscm SUNWidscn SUNWidscr SUNWidsct SUNWidsoc**)

表格 7-1 需移除之 Solaris 套裝軟體

套裝軟體名稱	描述
SUNWidscm	Sun ONE Directory Server Identity Synchronization 之核心元件及連接器套裝軟體。
SUNWidscn	Sun ONE Directory Server Identity Synchronization 之主控台說明檔案套裝軟體。
SUNWidscr	Sun ONE Directory Server Identity Synchronization 之核心元件套裝軟體。
SUNWidsct	Sun ONE Directory Server Identity Synchronization 之連接器套裝軟體。
SUNWidsoc	Sun ONE Directory Server Identity Synchronization 之物件快取套裝軟體。

若要驗證所有的套裝軟體是否均已移除，請鍵入：

```
pkginfo | grep -i "Identity Synchronization"
```

附註 如果因元件間的相依關係而仍有既有的套裝軟體未移除，請再次執行 pkgrm <*packageName*> 指令。

4. 按如下方法移除 Director Server 外掛程式：
   a. 開啓 Directory Server 主控台並選取「配置」標籤。
   b. 在左窗格中，展開「外掛程式」節點並選取 pswsync 節點。
   c. 在右窗格中，取消核取「啓用外掛程式」核取方塊。
   d. 按一下「儲存」以儲存上述變更。
   e. 在 Directory Server 主控台中，尋找並移除配置目錄中的以下項目：

      cn=pswsync,cn=plugins,cn=config

   f. 停止 Directory Server。
   g. 若要移除外掛程式二進位碼檔案，請鍵入

      rm -f /<*serverroot*>/lib/psw-plugin.so

   h. 重新啓動 Directory Server。
5. 備份 (複製並重新命名) /var/sadm/install/productregistry 中目前的 productregistry 檔案。

6. 手動編輯 /var/sadm/install/ 中的 productregistry 檔案，移除下列項目 (*如果存在*)：

附註

- 爲得到最佳結果，請使用 XML 編輯器。或者亦可使用標準的文字編輯器。
- 檔案中未必含有下列所有的元件。
- 您必須刪除開頭標記 (<compid>)、結束標記 (<\compid>)，以及兩個標記之間所有的內容。下列清單中使用省略符號代表這些標記中所含的其他文字及 / 或標記。(請參閱第 214 頁的範例。)

- <compid>Identity Synchronization for Windows . . . </compid>
- <compid>Core . . . </compid>
- <compid>unistaller . . . </compid>
- <compid>wpsyncwatchdog . . . </compid>
- <compid>setenv . . . </compid>
- <compid>Create DIT . . . </compid>
- <compid>Extend Schema . . . </compid>
- <compid>resources . . . </compid>
- <compid>CoreComponents . . . </compid>
- <compid>Connector . . . </compid>
- <compid>DSConnector . . . </compid>
- <compid>Directory Server Plugin . . . </compid>
- <compid>DSSubcomponents . . . </compid>
- <compid>ObjectCache . . . </compid>
- <compid>ObjectCacheDLLs . . . </compid>
- <compid>SUNWidscr . . . </compid>
- <compid>SUNWidscm . . . </compid>
- <compid>SUNWidsct . . . </compid>
- <compid>SUNWidscn . . . </compid>

- <compid>SUNWidsoc . . . </compid>
- <compid>ADConnector . . . </compid>

<compid> 標記的範例如下。移除 <compid>、</compid> 以及標記之間所有的文字與標記。

```
<compid>Identity Synchronization for Windows
    <compversion>1.0
          <uniquename>Identity Synchronization for Windows</uniquename>
           <compinstance>1
                    <children>
                        <compref>ADConnector
                            <instance>1
                                <version>1.0</version>
                            </instance>
                        </compref>
                        <compref>DSSubcomponents
                        . . .

        </compinstance>
    </compversion>
</compid>
```

7. 移除下列 Identity Synchronization for Windows 目錄及檔案：

   a. 在安裝位置，鍵入

      rm -rf /<*serverroot*>/isw-<*hostname*>

   b. 移除啓動程式檔案，鍵入

      rm -rf /etc/init.d/isw

8. 如下清除配置目錄：

   a. 針對安裝有 Identity Synchronization for Windows 核心程式的配置目錄，執行以下 ldapsearch 指令以尋找 Identity Synchronization for Windows 主控台子目錄樹：

   ```
   ldapsearch -D "cn=directory manager" -w <my_password> -b
   o=netscaperoot "(nsnickname=isw)" dn
   ```

   附註 ldapsearch 位在 Directory Server 的 <*serverroot*>/shared/bin/ldapsearch 例如，var/Sun/mps/shared/bin/ldapsearch

   產生的結果項目大致如下 (請注意，項目的結尾一律爲 *o=NetscapeRoot*)：

   ```
   "cn=Sun ONE Identity Synchronization for Windows,cn=server
   group, cn=myhost.mydomain.com,ou=mydomain.com,o=NetscapeRoot"
   ```

   b. 使用 Directory Server 主控台移除 Identity Synchronization for Windows 主控台子目錄樹及其下的所有子目錄樹。

9. 如下清除 Identity Synchronization for Windows 配置登錄：

   a. 執行以下的 ldapsearch 指令，尋找 Directory Server 中的 Identity Synchronization for Windows 配置登錄：

   ```
   ldapsearch -D "cn=directory manager" -w <my_password> -b
   "dc=my,dc=domain"
   "(&(objectclass=iplanetservice)(ou=IdentitySynchronization))" dn
   ```

   產生的結果項目大致如下：

   ```
   "ou=IdentitySynchronization,ou=Services,dc=my,dc=domain"
   ```

   b. 使用 Directory Server 主控台移除 Identity Synchronization for Windows 配置登錄及其下的所有子目錄樹。

10. 如下清除其他所有的主控台相關檔案：

a. 移除所有的主控台 jar 檔案，鍵入：

`rm -rf <serverroot>/java/jars/isw*`
例如 `/var/Sun/mps/java/jars/isw*`

b. 移除所有的主控台 servlet jar 檔案，鍵入：

`rm -rf <serverroot>/bin/isw/`
例如 `/var/Sun/mps/bin/isw/`

從 Windows 2000 手動解除安裝 1.0 核心程式與實例

請參照本節之說明，手動解除安裝 Windows 2000 電腦上的核心程式。

附註 在本節中，Identity Synchronization for Windows 的位置描述如下：

<serverroot>`\isw-`*<hostname>*

其中，*<serverroot>* 表示 Identity Synchronization for Windows 安裝位置的父目錄。

例如，假設您將 Identity Synchronization for Windows 安裝在 `C:\Program Files\Sun\mps\isw-`*example*，則 *<serverroot>* 即爲 `C:\Program Files\Sun\mps`。

1. 透過以下方法之一，停止所有的 Identity Synchronization for Windows Java 程序：

- 選取「開始」>「設定」>「控制台」>「系統管理工具」>「服務」，開啓「服務」視窗。於右窗格中，在 Sun ONE Identity Synchronization for Windows 上按一下滑鼠右鍵並選取「停止」。
- 開啓「指令提示符號」視窗並鍵入以下指令：

`net stop "Sun ONE Identity Synchronization for Windows"`

- 如果上述方法無效，可使用以下步驟手動停止 Java 程序：

  I. 開啓「服務」視窗，在 Sun ONE Identity Synchronization for Windows 上按一下滑鼠右鍵並選取「內容」。

  II. 在「內容」視窗的「一般」標籤中，從「啓動類型」下拉清單選取「手動」。

  附註 您雖然可從「Windows 工作管理員」中檢視 Java 程序 (例如 `pswwatchdog.exe`)，但無法確定哪些程序與 Identity Synchronization for Windows 特別相關。基於這個理由，請勿透過「Windows 工作管理員」停止程序。

2. 透過以下方法之一停止 Message Queue (僅限於核心程序的解除安裝作業)：

   - 於「服務」視窗中，在右窗格的 iMQ Broker 上按一下滑鼠右鍵並選取「停止」。
   - 開啓「指令提示符號」視窗並鍵入以下指令：

     ```
     net stop "iMQ Broker"
     ```

   - 如果上述方法無效，可使用以下步驟手動停止 Message Queue：

     I. 開啓「服務」視窗，在 iMQ Broker 上按一下滑鼠右鍵並選取「內容」。

     II. 在「內容」視窗的「一般」標籤中，從「啓動類型」下拉清單選取「手動」。

3. 按如下步驟移除 Directory Server 外掛程式：

   a. 開啓 Directory Server 主控台並選取「配置」標籤。

   b. 在左窗格中，展開「外掛程式」節點並選取 pswsync 節點。

   c. 在右窗格中，取消核取「啓用外掛程式」核取方塊。

   d. 按一下「儲存」以儲存上述變更。

   e. 在主控台中，尋找並移除配置目錄中的以下項目：

      ```
      cn=pswsync,cn=plugins,cn=config
      ```

   f. 透過以下方法之一，停止 Directory Server：

      - 於「服務」視窗中，在右窗格的 Sun ONE Directory Server 5.2 上按一下滑鼠右鍵並選取「停止」。

- 開啓「指令提示符號」視窗並鍵入以下指令：

  net stop slapd-<*myhostname*>

g. 開啓「Windows 檔案總管」以尋找並移除外掛程式二進位碼檔案：

<*serverroot*>\lib\psw-plugin.so

h. 重新啓動 Directory Server。

4. 開啓「指令提示符號」視窗，鍵入 **regedit** 以開啓「登錄編輯程式」視窗。

重要事項 – 進行步驟 5 之前請備份您目前的登錄檔案。

a. 在「登錄編輯程式」中，選取左窗格中的頂端節點 (「我的電腦」)。

b. 從功能表列選取「登錄」>「匯出登錄檔案」。

c. 出現「匯出登錄檔案」對話方塊時，指定檔案名稱並選取備份登錄的儲存位置。

5. 在「登錄編輯程式」中，從功能表列選取「編輯」>「刪除」，將下列 Identity Synchronization for Windows 機碼從 Windows 登錄中移除：

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\ 下所有的項目 Identity Synchronization for Windows
- HKEY_LOCAL_MACHINE\SYSTEM* 下所有的 CurrentControlSet 及 ControlSet (如 ControlSet001 及 ControlSet002 等) 項目，其中包含下列項目 (如果存在)：
  - ...\Control\Session Manager\Environment\<*isw-installation directory*>
  - ...\Services\Eventlog\Application\Sun ONE Identity Synchronization for Windows
  - ...\Services\Sun ONE Identity Synchronization for Windows
  - ...\Services\iMQBroker

6. 備份 (複製並重新命名) C:\WINNT\system32 中目前的 productregistry 檔案。

7. 編輯 C:\WINNT\system32 \productregistry 檔案，移除下列標記：

附註

- 爲得到最佳結果，請使用 XML 編輯器。或者亦可使用標準的文字編輯器。
- 檔案中未必含有下列所有的元件。
- 您必須刪除開頭標記 (<compid>)、結束標記 (<\compid>)，以及兩個標記之間所有的內容。下列清單中使用省略符號代表這些標記中所含的其他文字及 / 或標記。(請參閱第 220 頁的範例。)

- <compid>Identity Synchronization for Windows . . . </compid>
- <compid>Core . . . </compid>
- <compid>unistaller . . . </compid>
- <compid>wpsyncwatchdog . . . </compid>
- <compid>setenv . . . </compid>
- <compid>Create DIT . . . </compid>
- <compid>Extend Schema . . . </compid>
- <compid>resources . . . </compid>
- <compid>CoreComponents . . . </compid>
- <compid>Connector . . . </compid>
- <compid>DSConnector . . . </compid>
- <compid>Directory Server Plugin . . . </compid>
- <compid>DSSubcomponents . . . </compid>
- <compid>ObjectCache . . . </compid>
- <compid>ObjectCacheDLLs . . . </compid>
- <compid>ADConnector . . . </compid>

<compid> 標記的範例如下。移除 <compid>、</compid> 以及標記之間所有的文字與標記。

```
<compid>Identity Synchronization for Windows
    <compversion>1.0
          <uniquename>Identity Synchronization for Windows</uniquename>
           <compinstance>1
                    <children>
                        <compref>ADConnector
                            <instance>1
                                <version>1.0</version>
                            </instance>
                        </compref>
                        <compref>DSSubcomponents
                        . . .

        </compinstance>
    </compversion>
</compid>
```

8. 移除 Identity Synchronization for Windows 安裝資料夾，其位在 <*serverroot*>\isw-<*hostname*>。

   例如 C:\Program Files\Sun\mps\isw-example

9. 如下清除配置目錄：

   a. 從「指令提示符號」視窗中，針對安裝有 Identity Synchronization for Windows 核心的配置目錄，執行 ldapsearch 指令以尋找 Identity Synchronization for Windows 主控台子目錄樹。

   附註 ldapsearch，位在 <*serverroot*>\shared\bin\ldapsearch。

   例如，C:\Program Files\Sun\mps\shared\bin\ldapsearch

   ```
   ldapsearch -D "cn=directory manager" -w <my_password> -b
   o=netscaperoot "(nsnickname=isw)" dn
   ```

   產生的結果項目大致如下 (請注意，項目的結尾一律爲 *o=NetscapeRoot*)：

   ```
   "cn=Sun ONE Identity Synchronization for Windows,cn=server
   group, cn=myhost.mydomain.com,ou=mydomain.com,o=NetscapeRoot"
   ```

b. 使用 Directory Server 主控台移除您找到的 Identity Synchronization for Windows 主控台子目錄樹及其下的所有子目錄樹。

10. 按如下步驟清除 Identity Synchronization for Windows 配置目錄 (*也稱爲配置登錄*)：

a. 從「指令提示符號」視窗中，執行以下的 `ldapsearch` 指令，尋找 Directory Server 中的 Identity Synchronization for Windows 配置目錄：

```
ldapsearch -D "cn=directory manager" -w <my_password> -b
"dc=my,dc=domain"
"(&(objectclass=iplanetservice)(ou=IdentitySynchronization))" dn
```

產生的結果項目大致如下：

```
"ou=IdentitySynchronization,ou=Services,dc=my,dc=domain"
```

b. 使用 Directory Server 主控台來移除您找到的配置目錄子樹，包括其下所有的子目錄樹。

11. 如下清除其他所有的主控台相關檔案：

a. 移除 <*serverroot*>\java\jars\isw* 中所有的主控台 jar 檔案例如 C:\Program Files\Sun\mps\java\jars\isw*

b. 移除 \<*directory_server_install_root*>\bin\isw\ 中所有的主控台 servlet jar 檔案例如 C:\SunOne\Servers\bin\isw\

12. 重新啓動機器使所有的變更生效。

從 Windows NT 手動解除安裝 1.0 實例

請參照本節指示，手動解除安裝 Windows NT 電腦上的實例。

附註 在本節中，Identity Synchronization for Windows 的位置描述如下：

<*serverroot*>\isw-<*hostname*>

其中，<*serverroot*> 表示 Identity Synchronization for Windows 安裝位置的父目錄。例如，如果您將 Identity Synchronization for Windows 安裝在 `C:\Program Files\Sun\mps\isw-`*example*，則 <*serverroot*> 應爲 `C:\Program Files\Sun\mps`。

1. 透過以下方法之一，停止所有的 Identity Synchronization for Windows Java 程序 (核心程式及實例安裝)：
   - 選取「開始」>「設定」>「控制台」>「系統管理工具」>「服務」，開啓「服務」視窗。於右窗格中，在 Sun ONE Identity Synchronization for Windows 上按一下滑鼠右鍵並選取「停止」。
   - 開啓「指令提示符號」視窗並鍵入以下指令：

     `net stop "Sun ONE Identity Synchronization for Windows"`

   - 如果上述方法無效，請使用以下步驟手動停止 Java 程序：
     I. 開啓「服務」視窗，在 Sun ONE Identity Synchronization for Windows 上按一下滑鼠右鍵並選取「內容」。
     II. 在「內容」視窗的「一般」標籤中，從「啓動類型」下拉清單選取「手動」。

     附註 您雖然可從「Windows 工作管理員」中檢視 Java 程序 (例如 `pswwatchdog.exe`)，但無法確定哪些程序與 Identity Synchronization for Windows 特別相關。基於這個理由，請勿透過「Windows 工作管理員」停止程序。

2. 透過以下方法之一，停止變更偵測器服務：
   - 於「服務」視窗中，在右窗格的「Sun ONE NT 變更偵測器服務」上按一下滑鼠右鍵並選取「停止」。

- 開啓「指令提示符號」視窗並鍵入以下指令：

  net stop "Sun ONE NT Change Detector Service"

- 如果上述方法無效，請使用以下步驟手動停止變更偵測器服務：

  I. 開啓「服務」視窗，在「變更偵測器服務」上按一下滑鼠右鍵並選取「內容」。

  II. 在「內容」視窗的「一般」標籤中，從「啓動類型」下拉清單選取「手動」。

3. 重新啓動 Windows NT 電腦。

4. 您必須移除 Identity Synchronization for Windows 登錄機碼。開啓「指令提示符號」視窗，鍵入 **regedt32** 以開啓「登錄編輯程式」視窗。

注意 *請勿*使用 `regedit`，因爲程式不允許您編輯多值字串。

繼續步驟 5 *之前*，請務必備份您目前的 Windows 登錄檔案。

---

a. 在「登錄編輯程式」中，選取左窗格中的頂端節點 (「我的電腦」)。

b. 從功能表列選取「登錄」>「匯出登錄檔案」。

c. 出現「匯出登錄檔案」對話方塊時，指定檔案名稱並選取備份登錄的儲存位置。

5. 在「登錄編輯程式」中，從功能表列選取「編輯」>「刪除」，將下列 Identity Synchronization for Windows 機碼從登錄中移除：
   - `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\` 下所有的項目 `Identity Synchronization for Windows`
   - `HKEY_LOCAL_MACHINE\SYSTEM\*` 下所有的 `CurrentControlSet` 及 `ControlSet` (如 `ControlSet001` 及 `ControlSet002` 等) 項目，其中包含下列項目 (如果存在)：
     - `...\Control\Session Manager\Environment\`*<isw-installation directory>*
     - `...\Services\Eventlog\Application\Sun ONE Identity Synchronization for Windows`
     - `...\Services\Sun ONE Identity Synchronization for Windows`
     - `...\Services\iMQBroker`
   - `HKEY_LOCAL_MACHINE\SOFTWARE\Sun Microsystems\PSW`
6. 使用 **`regedt32`** (*請勿使用* `regedit`) 來修改 (***請勿刪除***) 下列登錄機碼：
   a. 在左窗格中選取登錄機碼項目：

      `HKEY_LOCAL_MACHINE\SYSTEM\\CurrentControlSet\\CONTROL\\LSA`

      登錄值類型必須爲 `REG_MULTI_SZ`。

   b. 於右窗格中，在 Notification Packages 值上按一下滑鼠右鍵並選取「修改」。

   c. 將 `PASSFLT` 值變更爲 `FPNWCLNT`。
7. 備份 (複製並重新命名) `C:\WINNT\system32` 中目前的 `productregistry` 檔案。

8. 編輯 C:\WINNT\system32 productregistry 檔案，移除下列標記：

附註

- 爲得到最佳結果，請使用 XML 編輯器。或者亦可使用標準的文字編輯器。
- 檔案中未必含有下列所有的元件。
- 您必須刪除開頭標記 (<compid>)、結束標記 (<\compid>)，以及兩個標記之間所有的內容。下列清單中使用省略符號代表這些標記中所含的其他文字及 / 或標記。(請參閱第 220 頁的範例。)

- <compid>Identity Synchronization for Windows . . . </compid>
- <compid>Core . . . </compid>
- <compid>uninstaller . . . </compid>
- <compid>wpsyncwatchdog . . . </compid>
- <compid>setenv . . . </compid>
- <compid>Create DIT . . . </compid>
- <compid>Extend Schema . . . </compid>
- <compid>resources . . . </compid>
- <compid>CoreComponents . . . </compid>
- <compid>Connector . . . </compid>
- <compid>DSConnector . . . </compid>
- <compid>Directory Server Plugin . . . </compid>
- <compid>DSSubcomponents . . . </compid>
- <compid>ObjectCache . . . </compid>
- <compid>ObjectCacheDLLs . . . </compid>
- <compid>ADConnector . . . </compid>

<compid> 標記的範例如下。移除 <compid>、</compid> 以及標記之間所有的文字與標記。

```
<compid>Identity Synchronization for Windows
    <compversion>1.0
       <uniquename>Identity Synchronization for Windows</uniquename>
           <compinstance>1
                    <children>
                        <compref>ADConnector
                            <instance>1
                                <version>1.0</version>
                            </instance>
                        </compref>
                        <compref>DSSubcomponents
                        . . .

        </compinstance>
    </compversion>
</compid>
```

9. 移除 Identity Synchronization for Windows 安裝資料夾，其位在 <***serverroot***>\isw-<*hostname*>。

   例如 `C:\Program Files\Sun\mps\isw-example`

   附註 開始進行步驟 10 之前，必須編輯 Windows 登錄，詳如步驟 8 所述。

10. 移除密碼篩選器 DLL。

    在 `C:\winnt\system32` 資料夾中尋找 `passflt.dll` 檔案，將該檔案重新命名爲 **`passflt.dll.old`**。

11. 重新啓動機器使所有的變更生效。

其他遷移方案

由於尚有其他可行的部署拓樸，您實際的遷移程序有可能與上述單一主機部署的情形相異。

本節敘述兩種替代部署方案，並分別解釋各個案例的遷移方法。部署方案範例包括：

- 「多主伺服器複製部署」
- 第 230 頁上的「Windows NT 環境的多主機部署」

多主伺服器複製部署

在多主伺服器複製 (MMR) 部署中，兩個 Directory Server 實例安裝在不同主機上。各個主機可以在不同的作業系統上執行，不過在本方案中，兩台主機均在相同作業系統上執行。

表格 7-2 繪示 Identity Synchronization for Windows 元件分佈於兩台主機的情形。

表格 7-2 多主伺服器複製部署之元件分佈

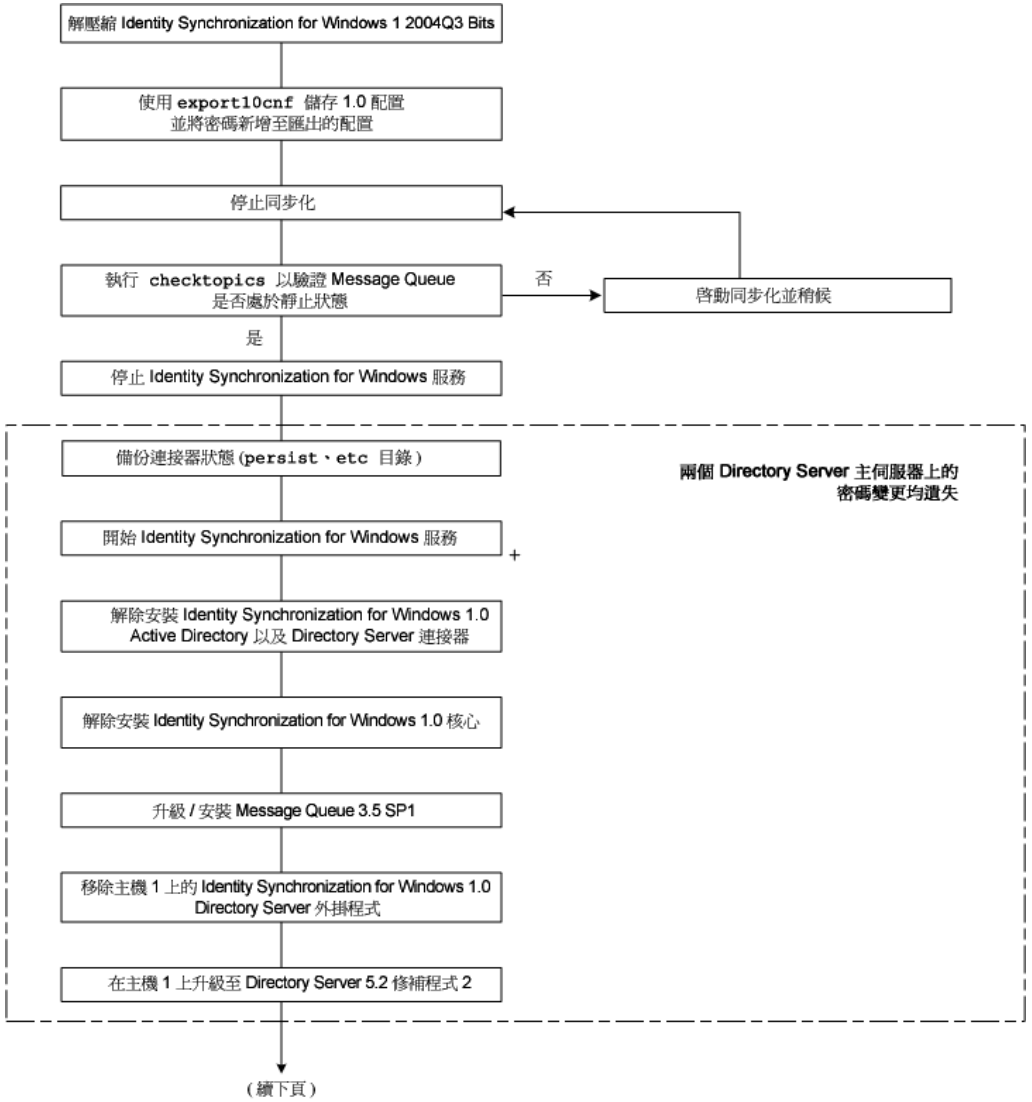
主機 1	主機 2
Directory Server (一實例) 爲同步化使用者的輔助伺服器	Directory Server (一實例) 爲同步化使用者的喜好伺服器
核心程式 (Message Queue、中央記錄程式、系統管理員及主控台)	Directory Server 外掛程式
Active Directory 連接器	
Directory Server 連接器	
Directory Server 外掛程式	

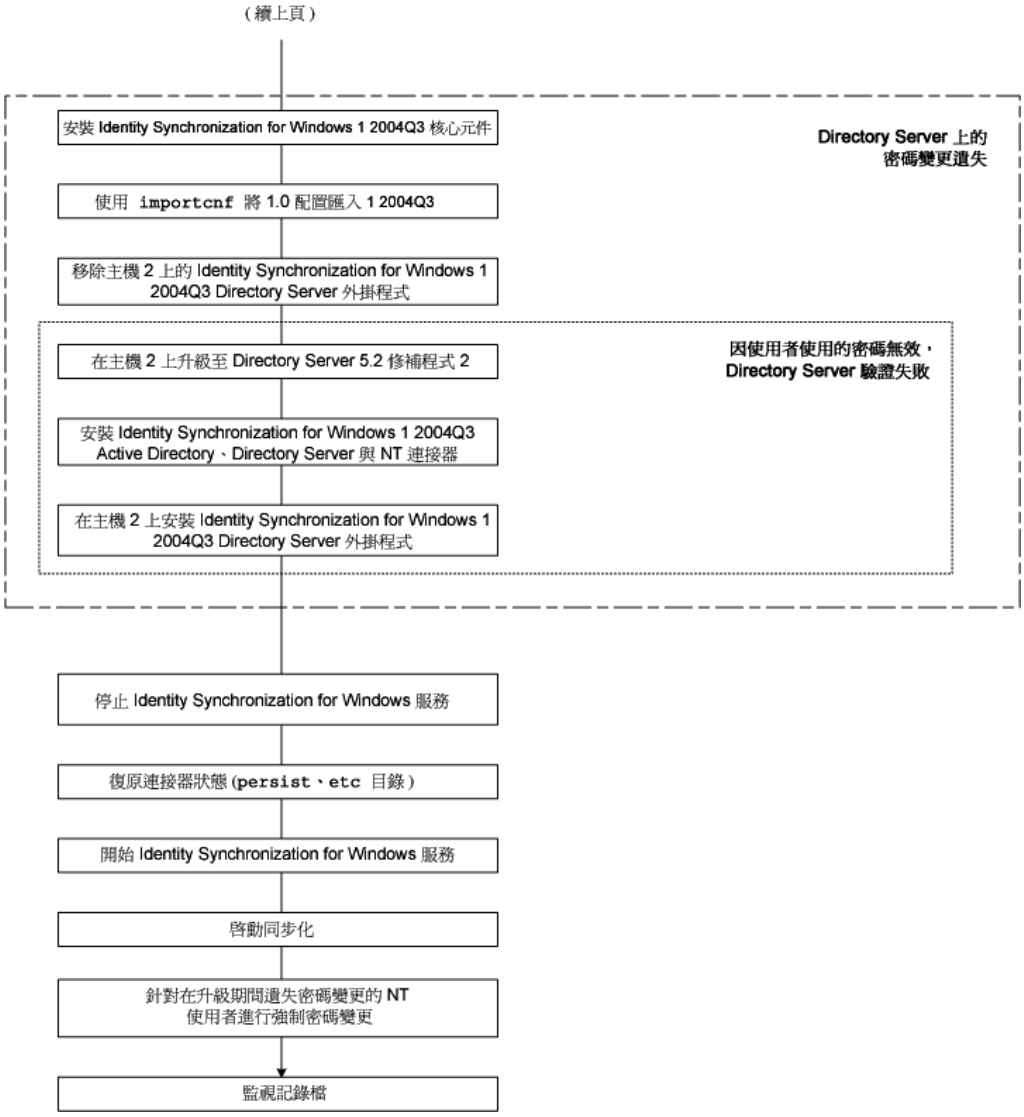
遷移程序會讓隨需密碼同步化持續於喜好伺服器或輔助伺服器上執行。

附註 如果兩個主機都在 Solaris 作業系統上執行，則需要第三個執行 Windows 2000 與 Active Directory 的主機專門用來進行同步化。(第三台主機不需安裝任何元件。)

下圖繪示在 MMR 部署中遷移 Identity Synchronization for Windows 之程序：

圖 7-2 遷移多主伺服器複製部署




（續上頁）
安裝 Identity Synchronization for Windows 1 2004Q3 核心元件
使用 importcnf 將 1.0 配置匯入 1 2004Q3
移除主機 2 上的 Identity Synchronization for Windows 1 2004Q3 Directory Server 外掛程式
在主機 2 上升級至 Directory Server 5.2 修補程式 2
安裝 Identity Synchronization for Windows 1 2004Q3 Active Directory、Directory Server 與 NT 連接器
在主機 2 上安裝 Identity Synchronization for Windows 1 2004Q3 Directory Server 外掛程式
Directory Server 上的密碼變更遺失
因使用者使用的密碼無效，Directory Server 驗證失敗
停止 Identity Synchronization for Windows 服務
復原連接器狀態 (persist、etc 目錄)
開始 Identity Synchronization for Windows 服務
啓動同步化
針對在升級期間遺失密碼變更的 NT 使用者進行強制密碼變更
監視記錄檔

Windows NT 環境的多主機部署

此部署方案中使用到以下三種主機：

- Windows NT 系統
- 包含已同步化使用者及 Directory Server 連接器之 Directory Server 主機
- 安裝所有其他元件之主機

表格 7-3 繪示 Identity Synchronization for Windows 元件分佈於三台主機的情形。

表格 7-3 多主機部署

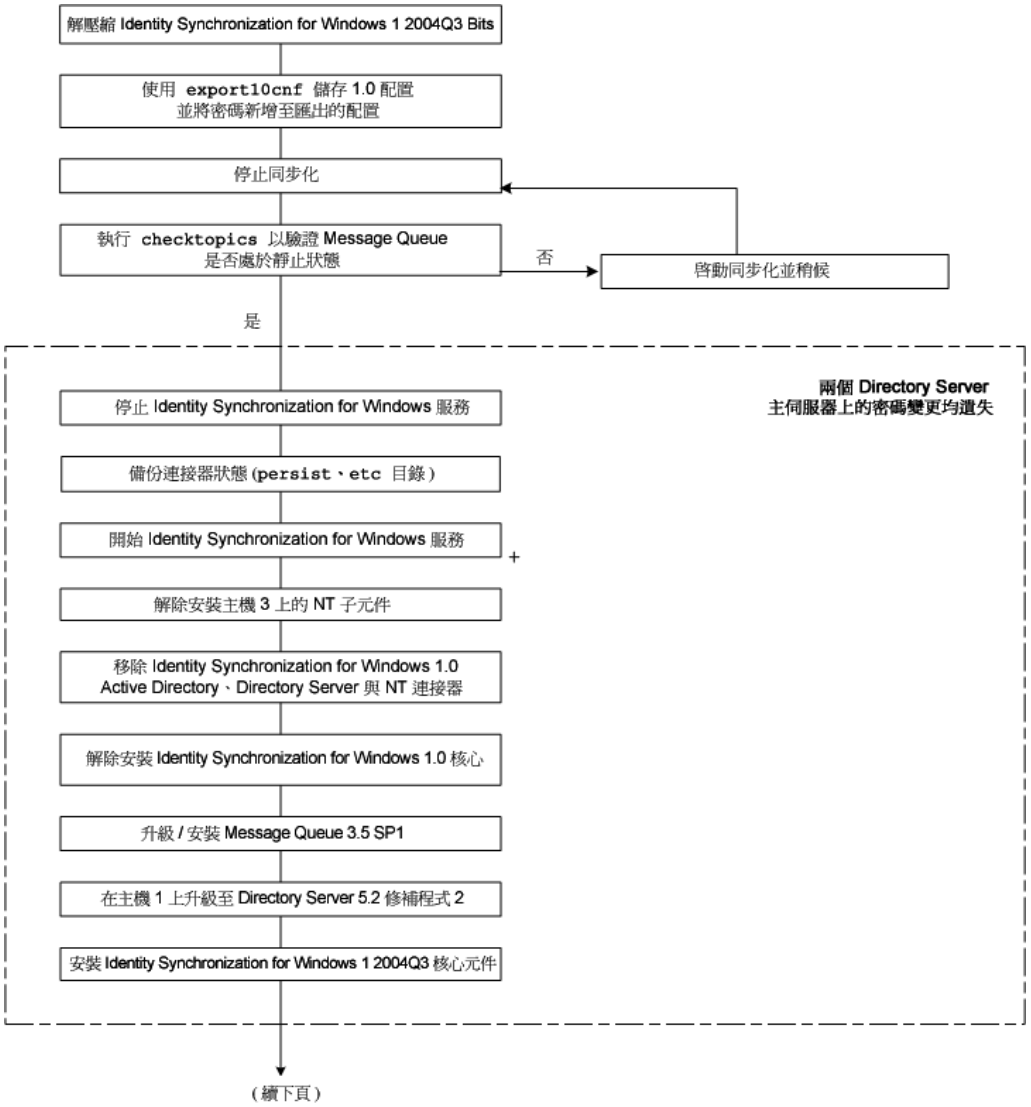
主機 1	主機 2	主機 3
Directory Server 帶配置儲存庫	已同步化使用者之 Directory Server	Windows NT 連接器
核心程式 (Message Queue、中央記錄程式、系統管理員及主控台)	Directory Server 連接器	Windows NT 子元件 (密碼篩選器 DLL 與變更偵測器服務)
Active Directory 連接器	Directory Server 外掛程式	

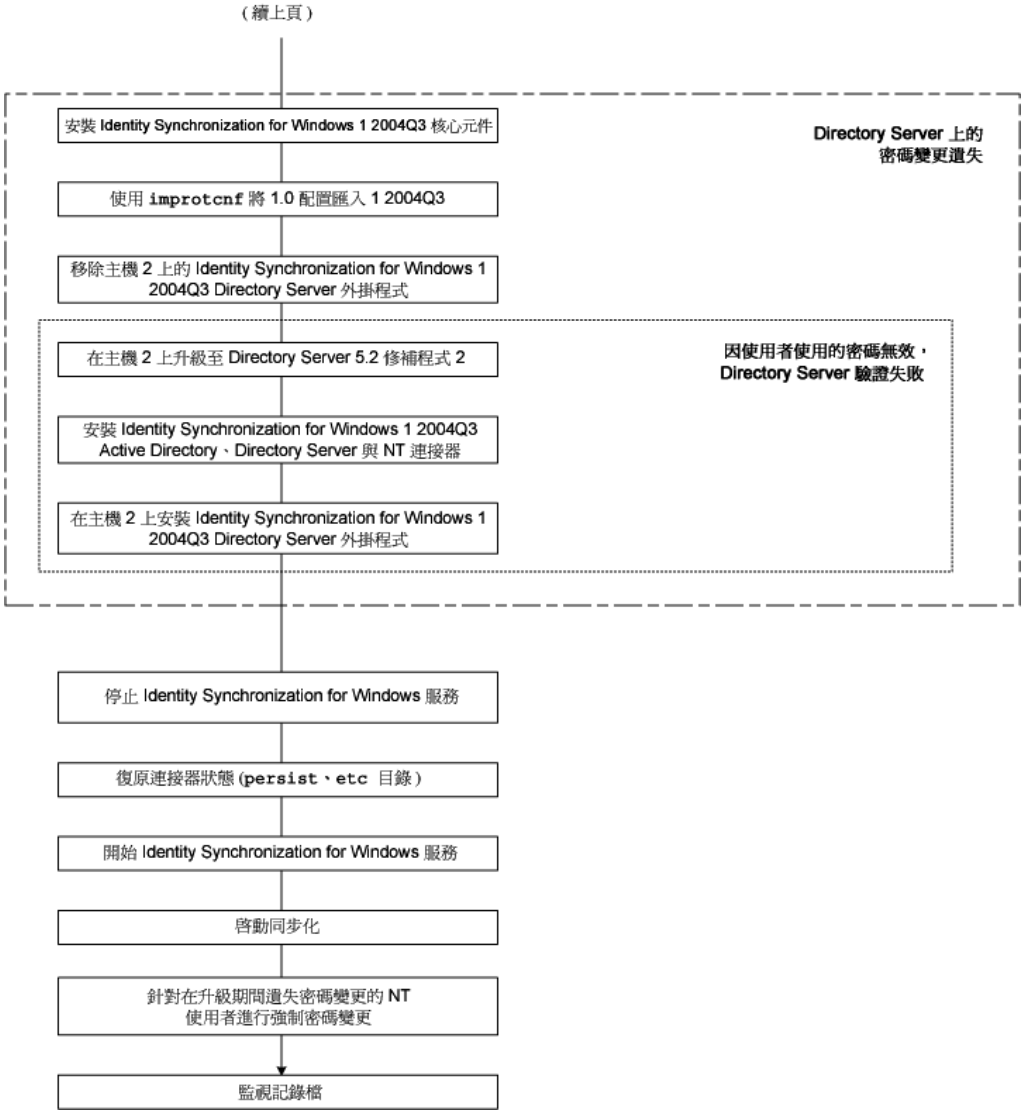
如同前述方案，主機 1 與主機 2 均在相同作業系統上執行。

附註 如果兩台主機都在 Solaris 作業系統上執行，則需要第四個執行 Windows 2000 與 Active Directory 的主機專門用來進行同步化。(第四台主機不需安裝任何元件。)

圖 7-3 繪示多主機部署中遷移 Identity Synchronization for Windows 之程序：

圖 7-3 遷移 Windows NT 環境的多主機部署




（續上頁）
安裝 Identity Synchronization for Windows 1 2004Q3 核心元件
使用 improtcnf 將 1.0 配置匯入 1 2004Q3
移除主機 2 上的 Identity Synchronization for Windows 1 2004Q3 Directory Server 外掛程式
在主機 2 上升級至 Directory Server 5.2 修補程式 2
安裝 Identity Synchronization for Windows 1 2004Q3 Active Directory、Directory Server 與 NT 連接器
在主機 2 上安裝 Identity Synchronization for Windows 1 2004Q3 Directory Server 外掛程式
Directory Server 上的密碼變更遺失
因使用者使用的密碼無效，Directory Server 驗證失敗
停止 Identity Synchronization for Windows 服務
復原連接器狀態 (persist、etc 目錄)
開始 Identity Synchronization for Windows 服務
啓動同步化
針對在升級期間遺失密碼變更的 NT 使用者進行強制密碼變更
監視記錄檔

檢查日誌

遷移至 1 2004Q3 版後，需檢查中央稽核日誌中是否有問題指示訊息，尤其遷移過程中 Directory Server 的使用者密碼變更可能會遺失，會出現如下的訊息：

```
[16/Apr/2004:14:23:41.029 -0500] WARNING    14  CNN101

ds-connector-host.example.com  "Unable to obtain password of user
cn=JohnSmith,ou=people,dc=example,dc=com, because the password was encoded
by a previous installation of Identity Synchronization for Windows
Directory Server Plugin.The password of this user cannot be synchronized at
this time.Update the password of this user again in the Directory Server."
```

此日誌訊息會一直存在，直到您在 Identity Synchronization for Windows 1 2004Q3 中開始進行同步化爲止，因此檢查日誌步驟需留待遷移程序的最後進行。

第 8 章

移除軟體

本章包含移除 Identity Synchronization for Windows 1 2004Q3 的程序，內容分成以下各節：

規劃解除安裝

開始移除軟體前，請牢記以下注意事項：

附註 必須*明確*依照指示解除安裝產品元件與子元件，並驗證已順利解除安裝所有的元件。

- 必須先解除安裝子元件與 Directory Server 外掛程式，才能解除安裝與其聯結的連接器，然後再解除安裝核心元件之前的所有聯結器。(Active Directory 連接器沒有任何需要解除安裝的子元件。)

  若未依適當順序解除安裝上述任一項元件，將無法選取並解除安裝其他元件。例如，假設您未先解除安裝連接器，則無法選取核心進行解除安裝。

- 請務必先解除安裝 Directory Server 外掛程式，再解除安裝核心元件。

  首先解除安裝核心元件會移除外掛程式位元，而不會從 Directory Server 上取消註冊這些位元，如此將造成 Directory Server 無法啓動，除非您手動移除 `cn=pswsync,cn=plugins,cn=config`。

- 在具有副本 (除主要及輔助伺服器以外) 的複製環境中，您必須先解除安裝 Directory Server 外掛程式，然後再重新啓動伺服器。
- 解除安裝連接器的順序不拘。
- 解除安裝 Sun Java System Directory Server 或 Windows NT 連接器後，您必須執行某些額外步驟，才能將連接器重新安裝在不同的電腦上或是使用不同的伺服器通訊埠。

  此時，您必須解除安裝然後再重新安裝所有對應的子元件，然後重新啓動安裝有核心的 Identity Synchronization for Windows 常駐程式 / 服務 (詳見第 185 頁上的「啓動與停止服務」)。

- 除非所有系統上的全部連接器與子元件均已解除安裝，否則請勿先解除安裝核心。
- 請務必在 Windows 2000 與 NT 平台上執行 `uninstall.cmd` 程序檔 (位於 `isw-`*<hostname>* 目錄中)。(您必須以管理員身份執行此批次檔。)
- 請務必在 Solaris 作業系統上執行 `runUninstall.sh` 程序檔 (預設情況下位於 `/opt/SUNWisw` 安裝目錄中)。(您必須以超級使用者身份執行此程序檔。)

解除安裝軟體

您的系統可能含有下列部分或所有 Identity Synchronization for Windows 元件：

- Active Directory 連接器
- Directory Server 連接器與外掛程式
- 核心元件

您的 Windows NT 系統可能含有 Windows NT 連接器和子元件。

請使用 `runUninstaller.sh` (Solaris) 或 `uninstall.cmd` (Windows) 移除所有的連接器及子元件，然後再移除核心 (如有安裝)。

本節分別說明以下主題：

解除安裝 Directory Server 外掛程式

附註

- 解除安裝程式僅會移除 Identity Synchronization for Windows Directory Server 外掛程式。您無法使用此解除安裝程式來移除其他任何 Directory Server 外掛程式。

  在本書中，*Directory Server 外掛程式*是指 Identity Synchronization for Windows Directory Server 外掛程式 (除非另有特別註明)。

- 若要以基於文字的模式執行解除安裝程式 (僅適用於 Solaris)，請鍵入

  `./runUninstaller.sh -nodisplay`

  當您執行此程式時，Identity Synchronization for Windows 會自動遮罩密碼，使其不至於以明文顯示。

請使用下列步驟來解除安裝 Identity Synchronization for Windows Directory Server 外掛程式。

1. 啓動解除安裝程式 (在 Solaris 系統中爲 `runUninstaller.sh`，在 Windows 系統中爲 `uninstall.cmd`)。

   這些解除安裝程式位於安裝目錄中 (預設爲 `/opt/SUNWisw` 目錄)。

2. 在「歡迎」畫面上按一下「下一步」。
3. 輸入配置目錄主機名稱及連接埠號。
   - 選取配置目錄的根字尾。(必要時，按一下「更新」可檢視字尾清單。)
   - 爲了在解除安裝程式與配置目錄伺服器之間進行安全通訊，點選「安全連接埠」方塊並指定 Directory Server 的 SSL 連接埠號。
4. 輸入針對該配置目錄所設的管理員名稱及密碼。
5. 選取「解除安裝 Directory Server 外掛程式」選項。
6. 輸入 Directory Server 主機名稱、通訊埠以及您的管理員憑證 (名稱及密碼)。
7. 按一下「下一步」執行進一步的解除安裝相關工作。
8. 在系統提示時，重新啓動安裝有外掛程式的 Directory Server。
9. 會顯示一個摘要視窗。請遵循該視窗所提供的指示。
   - **Solaris 系統**：解除安裝日誌係寫入 `/var/sadm/install/logs/`

- **Windows 系統**：解除安裝日誌係寫入 `%TEMP%` 目錄，其是子目錄，位於以下路徑的 `Local Settings` 資料夾下：

  `C:\Documents and Settings\Administrator`

  附註 在某些 Windows 系統上 (如 Windows 2000 Advanced Server)，`Local Settings` 資料夾爲隱藏資料夾。

  若要檢視該資料夾和 `Temp` 子目錄：

  開啓 Windows 檔案總管並從功能表列上選取「工具」> 「資料夾選項」。「資料夾選項」對話方塊開啓後，選取「檢視」標籤並啓用「顯示隱藏檔案」選項。

按一下「關閉」結束程式。

10. 如果 Directory Server 外掛程式是目標主機上安裝的*唯一* Identity Synchronization for Windows 元件，則可將 isw-*hostname* 資料夾刪除。
11. 重複步驟 1 至步驟 9 逐一解除網路中安裝在 Windows 2000 伺服器上的各個 Directory Server 外掛程式。

解除安裝連接器

若要解除安裝連接器，請依照以下步驟：

1. 啓動解除安裝程式 (在 Solaris 系統中爲 `runUninstaller.sh`，在 Windows 系統中爲 `uninstall.cmd`)。

   這些程式位於安裝目錄中 (預設爲 `/opt/SUNWisw` 目錄)。

2. 在「歡迎」畫面上按一下「下一步」。
3. 輸入配置目錄主機名稱及連接埠號。
   - 選取配置目錄的根字尾。(必要時，按一下「更新」可檢視字尾清單。)
   - 爲了在解除安裝程式與配置目錄伺服器之間進行安全通訊，點選「安全連接埠」方塊並指定 Directory Server 的 SSL 連接埠號。
4. 輸入針對該配置目錄所設的管理員名稱及密碼。
5. 選取所要解除安裝的連接器。

   附註 所選的連接器*必須*位於目標主機上。

6. 按一下「下一步」執行進一步的解除安裝相關工作。
7. 出現摘要視窗。請遵循該視窗所提供的指示。
   - **Solaris 系統**：解除安裝日誌係寫入 `/var/sadm/install/logs/`
   - **Windows 系統**：解除安裝日誌係寫入 `%TEMP%` 目錄，其是子目錄，位於以下路徑的 `Local Settings` 資料夾中：

     `C:\Documents and Settings\Administrator`

   附註 在某些 Windows 系統上 (如 Windows 2000 Advanced Server)，`Local Settings` 資料夾爲隱藏資料夾。
   若要檢視該資料夾和 `Temp` 子目錄：

   開啓 Windows 檔案總管並從功能表列上選取「工具」>「資料夾選項」。「資料夾選項」對話方塊開啓後，選取「檢視」標籤並啓用「顯示隱藏檔案」選項。

8. 按一下「關閉」結束程式。

9. 如目標主機上未安裝其他任何連接器，即可安全地將 `isw-<hostname>` 資料夾移除。
10. 針對安裝有連接器的所有主機，重複步驟 1 至步驟 7。

解除安裝核心

附註 請務必先解除安裝 Directory Server 外掛程式，再解除安裝核心元件。

在外掛程式之前解除安裝核心元件會移除外掛程式位元，而不會從 Directory Server 上取消註冊這些位元，這將造成 Directory Server 無法啓動，除非您手動移除 `cn=pswsync,cn=plugins,cn=config`。

請依照以下說明解除安裝核心：

1. 啓動解除安裝程式：
   - 在 **Windows** 電腦上：
     I. 按一下「開始」，然後選擇「設定」>「控制台」。
     II. 按兩下「新增 / 移除程式」。
     III. 在「新增 / 移除程式」視窗中，選取 `Identity Synchronization for Windows`，然後按一下「移除」。
   - 在 **Solaris 或 Windows** 電腦上，於 Solaris 中執行 `runUninstaller.sh`，或者在 Windows 上執行 `uninstall.cmd`。

     這些程式位於安裝目錄中 (預設爲 `/opt/SUNWisw` 目錄)。
2. 在「歡迎」畫面上按一下「下一步」。
3. 輸入配置目錄主機名稱及連接埠號。
   - 選取配置目錄的根字尾。(必要時，按一下「更新」可檢視字尾清單。)
   - 爲了在解除安裝程式與配置目錄伺服器之間進行安全通訊，點選「安全連接埠」方塊並指定 Directory Server 的 SSL 連接埠號。
4. 輸入針對該配置目錄所設的管理員名稱及密碼。
5. 選取所要解除安裝的核心元件後，按一下「下一步」。
6. 輸入配置目錄 URL，按一下「更新」，然後從下拉清單中選取相應的根字尾。
7. 按一下「下一步」執行進一步的解除安裝相關工作。

8. 出現摘要視窗。請遵循該視窗所提供的指示。

   - **Solaris 系統**：解除安裝日誌係寫入 `/var/sadm/install/logs/`
   - **Windows 系統**：解除安裝日誌係寫入 `%TEMP%` 目錄，其是子目錄，位於以下路徑的 `Local Settings` 資料夾下：

     ```
     C:\Documents and Settings\Administrator
     ```

   附註 在某些 Windows 系統上 (如 Windows 2000 Advanced Server)，`Local Settings` 資料夾爲隱藏資料夾。

   若要檢視該資料夾和 `Temp` 子目錄：

   開啓 Windows 檔案總管並從功能表列上選取「工具」>「資料夾選項」。「資料夾選項」對話方塊開啓後，選取「檢視」標籤並啓用「顯示隱藏檔案」選項。

9. 按一下「關閉」結束程式。

附註 如因故無法執行某特定連接器的連接器解除安裝程式 (例如因硬碟失敗而造成連接器檔案遺失) 時，請使用 idsync resetconn 子指令 (請參閱第 318 頁上的「使用 resetconn」)。

此指令會將配置目錄中的連接器狀態重設成 *uninstalled*，如此您即可將該連接器重新安裝至其他位置。resetconn 子指令類似於其他存取配置目錄的指令，其中包含兩個選項：

- **-e <*dir-source*>**：指定所要重設的目錄來源名稱。(在安裝程式中，連接器透過其目錄來源名稱進行識別。)
- **-n** (安全模式)：指出指令所指定的引數是否正確而不進行任何更動。

範例指令：

```
idsync resetconn -D "cn=Directory Manager" -w [-h CR-hostname]
[-p 389] [-s dc=example,dc=sun,dc=com] -q [-Z] [-P "cert8.db"]
[-m "secmod.db"] -e "dc=central,dc=example,dc=com" [-n]
```

resetconn 輸出：

```
NOTICE: This program will reset the installation state to
UNINSTALLED for the Connector associated with the specified
DirectorySource 'dc=central,dc=example,dc=com'.

Changing the Connector to an UNINSTALLED state is a last resort.
This is NOT meant to be used for uninstalling connectors.  It is
typically used if you lost a machine with the connector on it and can
not run the uninstaller.  Additionally, this program will rewrite
the existing configuration. This can be a lengthy process. Before
proceeding, you should stop the Console, any running installers, and
all other system processes. You may want to export the ou=Services
tree in the configuration directory to ldif as a backup.

Do you want to reset the installer settings for the connector (y/n)?
```

手動解除安裝主控台

當您移除其他所有的 Identity Synchronization for Windows 元件之後，必須手動解除安裝主控台。

從 Solaris 系統

若要從 Solaris 系統解除安裝主控台，請依照以下步驟：

1. 從配置目錄中刪除以下子樹狀目錄：

   cn=Sun Java (TM) System Identity Synchronization for Windows,cn=<*server_group*>,cn=<*hostname*>, ou=<*domain_name*>, o=netscaperoot

2. 對於所有的主控台安裝，從以下目錄中移除所有字首爲 *isw* 的 .jar 檔案：

   <*serverroot*></*server*>/java/jars

Windows 系統

若要從 Windows Active Directory 或 NT 系統解除安裝主控台，請依照以下步驟：

1. 從配置目錄中刪除以下子樹狀目錄：

   cn=Sun Java (TM) System Identity Synchronization for Windows,cn=<*server_group*>,cn=<*hostname*>, ou=<*domain_name*>, o=netscaperoot

2. 對於所有的主控台安裝，從以下目錄中移除所有字首爲 *isw* 的 .jar 檔案：

   <*serverroot*>/<*server*>/java/jars

第 9 章

疑難排解

本章所提供的資訊，可幫助您解決使用 Identity Synchronization for Windows 時可能遇到的疑難排解問題。內容歸納如下：

疑難排解核對清單

附註 管理員：在除錯問題時，請調整記錄層級 (如第 272 頁上的「配置日誌檔案」之說明)，如此才能確保日誌反映出可能造成問題的所有事件。

您必須調整記錄層級至「精細」或更高，否則某些事件 (例如，由於使用者未納入 SUL 中，所以程式無法將該使用者的變更同步化) 不會納入日誌檔中。在所有 `idsync resync` 作業期間，記錄層級都應保留在「資訊」層級。

在安裝和配置 Identity Synchronization for Windows 時，`idsync printstat` 指令可作爲一個有用的工具。當您執行 `printstat` 時 (請參閱第 317 頁上的「使用 printstat」)，它會顯示一份爲完成安裝及配置程序所必須執行的剩餘步驟的清單。

1. 中央日誌檔 error.log 中是否報告有任何問題？

   `isw-<`*hostname*`>/logs/central/error.log`

   幾乎所有錯誤都會在中央錯誤日誌檔案中加以報告。而且，通常可以在 `audit.log` 中取得有關任何錯誤的額外資訊。爲增進相關日誌項目的關聯性，`audit.log` 檔案亦在錯誤日誌中包含了所有日誌項目。

2. 版本說明文件中記載了許多已知的問題。其中是否解說到此問題？

3. 是否是於已完全解除安裝的電腦上執行的安裝？如果未徹底解除安裝先前的配置，則重新安裝此產品時可能會發生問題。有關如何清除先前安裝的詳細說明，請參閱第 8 章，「移除軟體」。

4. 是否正確安裝了核心元件？如果成功完成核心元件安裝，則日誌檔案會存放在 `isw-<`*hostname*`>/logs/central/` 目錄中。

5. Directory Server 在資源配置期間是否仍在執行？

6. 當前是否正在執行核心程式，包括 Message Queue 及系統管理員？在 Windows 系統上，請檢查有否適當的服務名稱。在 Solaris 系統上，請檢查有否適當的常駐程式名稱。使用 `idsync printstat` 指令驗證 Message Queue 和系統管理員是否在作用中。

7. 是否成功儲存了配置？如果 `idsync printstat` 指令列出連接器，則表示已成功儲存配置。

8. 是否已安裝所有連接器？每個要同步化的目錄來源都必須安裝一個連接器。

9. 是否已安裝所有子元件？ Directory Server 及 Windows NT 連接器要求在安裝連接器之後安裝子元件。每個 Directory Server 複本中都必須安裝有 Directory Server 外掛程式。
10. 是否執行了安裝後步驟？安裝 Directory Server 外掛程式後，必須重新啓動 Directory Server。安裝 Windows NT 子元件後，必須重新啓動 Windows NT 主要網域控制器。
11. 是否從主控台或指令行啓動同步化作業？
12. 所有連接器目前是否都在執行？
13. 透過主控台或 `idsync printstat` 來驗證是否所有連接器皆爲 SYNCING 狀態。
14. 要同步化的目錄來源目前是否正在執行？
15. 透過主控台來驗證修改及 / 或建立項目的同步化是否沿預期方向進行。
16. 如果同步化的使用者僅存在於一個目錄來源中，是否使用 `idsync resync` 指令在其他目錄來源中建立了這些使用者？

    附註 只要有現存的使用者，您就必須執行 `idsync resync`。如果不重新同步化現有使用者，則重新同步化行爲依舊爲非定義狀態。

17. 如果同步化的使用者存在於兩個目錄來源中，是否使用 `idsync resync` 指令連結了這些使用者？
18. 如果無法從 Active Directory 或 Windows NT 向 Sun Java System Directory Server 建立使用者，請驗證 Directory Server objectclass 中所有的強制性屬性是否已指定爲建立屬性，且對應屬性值是否出現在原始使用者項目中。
19. 如果建立從 Directory Server 至 Windows NT 的同步化，並且已成功建立使用者，但是卻無法使用帳戶，請驗證使用者名稱是否不合 Windows NT 的需求。

    例如，如果指定的名稱超過 Windows NT 的最大容許長度，此時雖然會在 NT 上建立使用者，但卻無法使用也無法編輯。在此情況下必須重新命名使用者 (「使用者」>「重新命名」)。
20. 您必須開啓 NT 稽核日誌，Windows NT SAM 變更偵測器子元件才會生效。請選取「開始」>「程式集」>「系統管理工具」>「使用者管理員」，然後選取「原則」>「稽核原則」。
    選取「稽核下列事件」，接著選取「使用者及群組管理」的「成功」和「失敗」方塊。

    選取「事件檢視器」中的「事件日誌設定值」>「事件日誌換行」，接著選取「視需要覆寫事件」。

21. 同步化使用者清單內的使用者是否無法同步化？例如，使用者是否符合「同步化使用者清單」的基本 DN 及篩選條件？在包含 Active Directory 的部署中，如果 Sun Java System Directory Server 項目未納入任何「同步化使用者清單」中，則會發生隨需密碼同步化失敗，且不會出現訊息。這經常是因爲同步化使用者清單篩選不正確而致。

22. 是否變更了同步化設定值？如果同步化設定由僅將使用者從 Active Directory 同步化至 Sun Java System Directory Server 變更爲將使用者從 Directory Server 同步化至 Active Directory，則必須將 Active Directory SSL CA 憑證加入連接器的憑證資料庫。`idsync certinfo` 指令依據目前 SSL 設定報告必須安裝的 SSL 憑證。

23. 是否正確指定了所有主機名稱，並且是以 DNS 可以解析的形式？在執行 Active Directory 連接器的電腦及執行 Sun Java System Directory Server 外掛程式的電腦上，Active Directory 網域控制器都應是 DNS 可以解析的形式。

24. 經過解析的 Active Directory 網域控制器 IP 位址之名稱是否與連接器與之連接所使用的名稱相同？

25. 來源連接器是否偵測到使用者變更？使用中央日誌 `audit.log` 來確定新增或修改使用者的目錄來源所使用的連接器是否偵測到修改項目。

26. 目標連接器是否處理此修改項目？

27. 是否配置了多個同步化使用者清單？如果是，是否存在衝突？使用主控台安排同步化使用者清單的順序，更具體的同步化使用者清單應排在較不具體的同步化使用者清單之前。

28. 如果設定爲雙向傳遞或從 Sun 傳遞至 Windows，並且部署中有 Active Directory 資料來源，請驗證連接器是否配置爲使用 SSL 通訊？

29. 如果懷疑 Solaris 環境中有記憶體問題，請檢查各程序。若要檢視以不同程序執行的元件，請輸入

    `/usr/ucb/ps -gauxwww | grep com.sun.directory.wps`

    輸出會提供完整的詳細資訊，包括連接器 ID、系統管理員和中央記錄程式。此功能適合用來檢視是否有耗用過量記憶體的程序。

30. 如果您正在建立或編輯 Sun Java System 目錄來源，並且 Directory Server 沒有顯示在「選擇一個已知的伺服器」下拉清單中，請檢查 Directory Server 是否在執行。Directory Server 必須正在執行，才會出現在可用主機下拉清單內。

    假如當事伺服器暫時處於非作用中，請在「透過輸入主機名稱和通訊埠指定伺服器」欄位中輸入主機及通訊埠。

附註	預設情況下，Identity Synchronization for Windows 使用短主機名稱；但是，預設主機名稱可能不適用於您的配置。每當要求您提供主機名稱時，建議輸入完整合格的名稱。

31. 執行解除安裝程式時有否收到下列錯誤？

```
./runInstaller.sh
IOException while making /tmp/SolarisNativeToolkit_5.5.1_1
executable:java.io.IOException:Not enough space
java.io.IOException:Not enough space
```

增加掛載於 `/tmp` 的交換檔案的大小。

連接器疑難排解

使用本節的資訊可疑難排解連接器的問題。內容歸納如下：

- 第 249 頁上的「如何確定管理目錄來源的連接器 ID」
- 第 250 頁上的「如何確定連接器的目前狀態」

如何確定管理目錄來源的連接器 ID

您可使用下列一種方法來確定連接器 ID：

- 「使用中央日誌」
- 「使用 idsync printstat」

使用中央日誌

藉由檢視中央 `audit.log`，確定要同步化的目錄來源的連接器 ID。啓動時，中央記錄程式會記錄每個連接器的 ID 及其管理的目錄來源。有關最新資訊，請檢視啓動標題的上一實例。

例如，下列日誌訊息中有兩個連接器：

- **CNN101** 是管理 `dc=airius,dc=com` 的 Sun Directory 連接器

- **CNN100** 是管理 `airius.com` 網域的 Active Directory 連接器

```
[2003/03/19 00:00:00.722 -0600] INFO    16     "System Component
Information:SysMgr_100 is the system manager (CORE);  console is the Product
Console User Interface;  CNN101 is the connector that manages
[dc=airius,dc=com (ldap://host1.airius.com:389)];  CNN100 is the connector
that manages [airius.com (ldaps://host2.airius.com:636)];"
```

使用 idsync printstat

也可以使用 `idsync printstat` 指令來取得連接器 ID 及狀態 (請參閱第 317 頁上的「使用 printstat」)。

這項指令的輸出範例如下：

```
Connector ID:CNN100
   Type:Active Directory
   Manages:airius.com (ldaps://host2.airius.com:636)
   State:READY

Connector ID:CNN101
   Type:Sun Java System Directory
   Manages:dc=airius,dc=com (ldap://host1.airius.com:389)
   State:READY

Sun Java System Message Queue Status:Started

Checking the System Manager status over the Sun Java System Message Queue.

System Manager Status:Started

SUCCESS
```

如何確定連接器的目前狀態

使用主控台中的「狀態」窗格、`idsync printstat` 指令 (如前所述)，或藉由檢視中央 `audit.log`，可確定同步化所牽涉的連接器之目前狀態。

搜尋 audit.log 中最近一條報告連接器狀態的訊息。
例如，在下面的日誌訊息中您會看到連接器 CNN101 的狀態爲 READY。

```
[2003/03/19 10:20:16.889 -0600] INFO    13  SysMgr_100 host1  "Connector
[CNN101] is now in state "READY"."
```

表格 9-1 說明了不同的連接器狀態。

表格 9-1 連接器狀態涵義

狀態	涵義
UNINSTALLED	連接器尚未安裝。
INSTALLED	已安裝連接器，但未收到其配置。
READY	已安裝連接器且已收到其配置，但尚未開始同步化。
SYNCING	已安裝連接器且已收到其配置，並已嘗試開始同步化。

連接器爲 UNINSTALLED 狀態時應採取什麼動作

安裝連接器。

如果無法安裝連接器，且無法重新安裝連接器，應採取什麼動作

如果無法安裝連接器，但 Identity Synchronization for Windows 安裝程式認爲已安裝了連接器，安裝程式將不允許重新安裝連接器。

執行 idsync resetconn (如第 318 頁上的「使用 resetconn」中所述)，重設連接器狀態爲 UNINSTALLED，接著重新安裝連接器。

連接器爲 INSTALLED 狀態時應採取什麼動作

如果連接器長時間維持在已安裝狀態，很可能是連接器未在執行中，或連接器無法與 Message Queue 進行通訊。

在已安裝連接器的電腦上，檢視連接器日誌 (audit.log 和 error.log) 中是否有潛在錯誤。如果連接器無法連接至 Message Queue，就會在日誌中報告該錯誤。如果遇到此狀況，請參閱第 258 頁上的「Message Queue 疑難排解」，瞭解可能的原因。

如果稽核日誌中的最新訊息已過時，則或許是連接器並未執行。請參閱第 253 頁上的「元件疑難排解」。

連接器爲 READY 狀態時應採取什麼動作

除非已啓動同步化並且已安裝連接器的所有子元件且子元件都已連接至該連接器，否則連接器會維持在 READY 狀態。如果尚未啓動同步化，請利用主控台或指令行公用程式來啓動同步化。

如果已啓動同步化，但連接器未進入 SYNCING 狀態，則可能是子元件有問題。請參閱第 256 頁上的「子元件疑難排解」。

連接器爲 SYNCING 狀態時應採取什麼動作

如果所有連接器皆爲 SYNCING 狀態，但修改項目尚未同步化，請驗證同步化設定值是否正確：

- 利用主控台來驗證修改及 / 或建立項目的同步化是否沿預期方向 (例如，從 Windows 至 Sun Java System Directory Server) 進行。
- 利用主控台來驗證所修改的屬性是否爲同步化屬性 (注意：密碼一律同步化)。如果建立的使用者項目未同步化，請驗證主控台中是否已啓用使用者建立傳遞方向。
- 來源連接器是否偵測到使用者變更？使用中央日誌 `audit.log` 來確定新增或修改使用者的目錄來源所使用的連接器是否偵測到修改項目。目標連接器是否處理此修改項目？

Active Directory 連接器無法透過 SSL 聯繫 Active Directory 時應採取什麼動作

如果 Active Directory 連接器無法透過 SSL 聯繫 Active Directory，並且顯示下列錯誤訊息，請重新啓動 AD 網域控制器。

```
Failed to open connection to ldaps://server.example.com:636,
error(91):Cannot connect to the LDAP server, reason:SSL_ForceHandshake
failed:(-5938) Encountered end of file.
```

元件疑難排解

使用本節的資訊可疑難排解元件問題。內容歸納如下：

Solaris 系統

執行 `/usr/ucb/ps -auxww | grep com.sun.directory.wps` 指令會列出所有執行中的 Identity Synchronization for Windows 程序。下面的表格列出了應在執行的程序。

表格 9-2 Identity Synchronization for Windows 程序

Java 程序類別名稱	元件	存在條件
`com.sun.directory.wps.watchdog.server.WatchDog`	系統監視程式	始終
`com.sun.directory.wps.centrallogger.CentralLoggerManager`	中央記錄程式	僅當安裝了核心程式時
`com.sun.directory.wps.manager.SystemManager`	系統管理員	僅當安裝了核心程式時
`com.sun.directory.wps.controller.AgentHarness`	連接器	每個安裝的連接器都有一個對應程序

如果執行中的程序數目不合預期，請發出下列命令來重新啓動所有 Identity Synchronization for Windows 程序。

```
# /etc/init.d/isw stop
# /etc/init.d/isw start
```

如果檢視程式程序正在執行，但執行中的 `java.exe` 程序數目不合預期，請參閱「檢查 WatchList.properties」一節來驗證是否正確安裝了所有元件。

如同其他系統元件，Sun Java System Directory Server 外掛程式會透過匯流排來傳送受中央記錄程式管理的日誌記錄，供一般使用者檢視。但是，外掛程式也會記錄某些可能不會透過匯流排顯現的訊息 (例如，當子元件無法聯繫連接器時)。在此情況下，日誌訊息僅會顯現在檔案系統的外掛程式 logs 目錄中，大致位置類似以下範例所示：

<serverroot>/isw-*<hostname>*/logs/SUBC*<id>*.

因爲外掛程式會與 Directory Server 程序一起執行，所以可能會發生外掛程式無法寫入其 logs 目錄的問題。如果目錄伺服器是以不同於 logs 目錄所有者的使用者身份執行，就會發生此問題。在此情況下，可能有必要使用原生作業系統指令來變更目錄權限或所有者，明確指定外掛程式權限。

Windows 系統

利用「服務」控制台來檢查是否已啓動「Sun Java System Identity Synchronization for Windows」服務。如果未啓動，則表示該電腦上未執行 Identity Synchronization for Windows，應將其啓動。如果已啓動服務，請利用工作管理員來驗證 pswwatchdog.exe (監視程式程序) 是否在執行，且執行中的 java.exe 程序是否合乎預期數目：

- 僅在安裝了核心程式時，才會有一個與 Message Queue 代理程式對應
- 僅在安裝了核心程式時，才會有一個與系統管理員對應
- 僅在安裝了核心程式時，才會有一個與中央記錄程式對應
- 電腦上安裝的每個連接器都有一個對應程序

附註 可能會有其他作用中的 java 程序，如 Directory Server 主控台。如果 pswwatchdog.exe 未在執行，請重新啓動「Sun Java System Identity Synchronization for Windows」服務。如果它正在執行，但執行中的 java.exe 程序數目不合預期，請參閱第 255 頁上的「檢查 WatchList.properties」來驗證是否正確安裝了所有元件。

檢查 WatchList.properties

在每台安裝了 Identity Synchronization for Windows 元件的電腦上，isw-< *電腦名稱* >/resources/WatchList.properties 檔案會列舉應在該電腦上執行的元件。process.name[n] 屬性命名應執行之元件。

在安裝了核心程式的電腦上，WatchList.properties 將包含中央記錄程式和系統管理員的項目：

```
process.name[1]=Central Logger
…
process.name[2]=System Manager
…
```

在安裝了連接器的電腦上，WatchList.properties 將包含每個連接器的一個對應項目。process.name 屬性是連接器 ID：

```
process.name[3]=CNN100
…
process.name[4]=CNN101
…
```

如果 WatchList.properties 中的項目與執行中的程序不符，請重新啓動 Identity Synchronization for Windows 常駐程式或服務。

如果 WatchList.properties 中的項目數與預期數目不符 (例如，雖然安裝了兩個連接器，卻僅有一個連接器項目)，請檢查安裝日誌中可能記錄的安裝失敗。

- **Solaris 系統**：安裝日誌係寫入 /var/sadm/install/logs/
- **Windows 系統**：安裝日誌係寫入 %TEMP% 目錄，它是一個子目錄，位於以下路徑的 Local Settings 資料夾下：

  C:\Documents and Settings\Administrator

附註 在某些 Windows 系統上 (如 Windows 2000 Advanced Server)，`Local Settings` 資料夾爲隱藏資料夾。

若要檢視該資料夾和 `Temp` 子目錄：

1. 開啓 Windows 檔案總管並從功能表列上選取「工具」>「資料夾選項」。
2. 「資料夾選項」對話方塊開啓後，選取「檢視」標籤並啓用「顯示隱藏檔案」選項。

子元件疑難排解

使用以下核對清單來疑難排解您部署中的子元件問題：

1. 是否安裝了所有子元件？

   子元件的安裝必須在安裝連接器後進行：

   - 對於 Active Directory 連接器，沒有要安裝的子元件。
   - 對於 Sun Java System Directory Server 連接器，必須在要同步化的 Sun Java System Directory Server 上安裝 Directory Server 外掛程式。
   - 對於 Windows NT 連接器，必須在每個要同步化的 Windows NT 網域的主要網域控制器上安裝 Windows 變更偵測器及密碼篩選器子元件。這兩個子元件在安裝 Windows NT 連接器後一併安裝。

附註 您必須開啓 NT 稽核日誌，Windows NT SAM 變更偵測器子元件才會生效。請選取「開始」>「程式集」>「系統管理工具」>「使用者管理員」，然後選取「原則」>「稽核原則」。選取「稽核下列事件」，接著選取「使用者及群組管理」的「成功」和「失敗」方塊。

選取「事件檢視器」中的「事件日誌設定值」>「事件日誌換行」，接著選取「視需要覆寫事件」。

2. 是否執行了字元件安裝後步驟？

   在 Sun Java System Directory Server 上安裝 Directory Server 外掛程式後，必須重新啓動伺服器。在主要網域控制器上安裝 NT 變更偵測器及密碼篩選器後，必須重新啓動伺服器。

3. 子元件是否正在執行？

   安裝有外掛程式的 Directory Server 是否正在執行？安裝了變更偵測器及密碼篩選器的主要網域控制器是否正在執行？

4. 子元件是否建立了與連接器的網路連線？

   於連接器正在執行的電腦上，執行 `netstat -n -a` 來驗證連接器是否正在偵聽子元件連線。下列範例展示了在三種不同案例下執行這個指令的結果。(連接器配置爲偵聽通訊埠 9999。)

   a. 連接器正在偵聽傳入的連線，且子元件已成功連接，這是預期的結果：

```
netstat -n -a | grep 9999
      *.9999               *.*    0   0 65536    0 LISTEN
12.13.1.2.44397 12.13.1.2.9999  73620 0 73620    0 ESTABLISHED
12.13.1.2.9999  12.13.1.2.44397 73620 0 73620    0 ESTABLISHED
```

   b. 連接器正在偵聽傳入的連線，但子元件尚未連接：

```
# netstat -n -a | grep 9999
     *.9999               *.*    0   0 65536    0 LISTEN
```

   驗證子元件正在執行後，檢查子元件的本機日誌，看是否有潛在問題。

   c. 連接器未在偵聽傳入的連線：

```
# netstat -n -a | grep 9999
<no output>
```

   驗證是否指定了正確的通訊埠埠號。驗證連接器正在執行且爲 READY 狀態。檢查連接器的本機日誌，看是否有潛在問題。

Message Queue 疑難排解

驗證 Sun Java System Message Queue 代理程式正在執行。向電腦發出 `telnet` 指令，正執行 Message Queue 代理程式的通訊埠便會傳回作用中的 Message Queue 服務的清單：

```
# telnet localhost 7676
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
101 psw-broker 3.0.1
cluster tcp CLUSTER 32914
admin tcp ADMIN 32912
portmapper tcp PORTMAPPER 7676
ssljms tls NORMAL 32913
jms tcp NORMAL 32911
.
Connection closed by foreign host.
```

- 如果輸出中未列出「`ssljms tcp NORMAL`」服務，請檢查 Message Queue 日誌，看是否有潛在問題。如果 Solaris 上安裝了核心程式，則 Message Queue 代理程式的日誌爲：

  `/var/imq/instances/psw-broker/log/log.txt`

- 如果 Windows 上安裝了核心程式，則代理程式的日誌爲：

  <*installation_root*>`\isw-`<*machine_name*>`\imq\var\instances\isw-broker\log\log.txt`

如果 `telnet` 指令失敗，則是因爲代理程式未在執行或指定了錯誤的通訊埠。請檢查代理程式日誌中的通訊埠埠號。使用下列指令行來指定代理程式通訊埠

```
[13/Mar/2003:18:17:09 CST] [B1004]: 浭tarting the portmapper service using
tcp [ 7676, 50 ] with min threads 1 and max threads of 1"
```

如果代理程式未在執行，在 Solaris 系統中執行 `/etc/init.d/imq start`，在 Windows 系統中啓動 `iMQ Broker` Windows 服務，就可啓動代理程式。

如果正在 Solaris 8 上安裝 Message Queue，並將要執行 `mquinstall` 來安裝所有套件，請在執行 `mqinstall` *前*務必設定 `IMQ_JAVAHOME`，確保軟體選用正確的 Java 版本。

如果您尚未安裝核心程式，就不需要設定 IMQ_JAVAHOME，因爲 Identity Synchronization for Windows 安裝程式會指示 Message Queue 代理程式應使用的 JVM。

代理程式配置目錄通訊疑難排解

Message Queue 代理程式依據儲存 Identity Synchronization for Windows 配置的 Directory Server 來驗證用戶端。如果代理程式無法連接至此 Directory Server，則任何用戶端都無法連接至 Message Queue，且代理程式日誌會記錄某些 javax.naming 例外，如 “javax.naming.CommunicationException” 或 “javax.naming.NameNotFoundException”.

若發生 javax.naming 例外，請執行下列動作

- 驗證 /var/imq/instances/isw-broker/props/config.properties 中的所有 imq.user_repository.ldap 屬性的值是否正確。如果有任何屬性值錯誤，請停止 Message Queue 代理程式，修正並儲存檔案，然後重新啓動代理程式。必須可以從代理程式的電腦解析目錄伺服器主機名稱。
- 驗證 /etc/imq/passfile 中的 imq.user_repository.ldap.password 屬性是否正確。
- 在某些情況下，如果根字尾有空白，代理程式便無法搜尋項目。

代理程式記憶體設定疑難排解

在正常作業期間，Message Queue 代理程式會耗用適量的記憶體。然而，在 idsync resync 作業期間，代理程式的記憶體需求會增加。如果代理程式到達其記憶體限制，未傳遞的訊息便會累積下來，idsync resync 作業會急遽減速或完全停止，並且 Identity Synchronization for Windows 之後可能會沒有回應。

代理程式進入低記憶體狀態時，其日誌中會出現下列訊息：

```
[03/Nov/2003:14:07:51 CST] [B1089]:In low memory condition, Broker is
attempting to free up resources

[03/Nov/2003:14:07:51 CST] [B1088]:Entering Memory State [B0024]:RED  from
previous state [B0023]:ORANGE - current memory is 1829876K, 90% of total
memory
```

若要避免發生此狀況：

- 依照 *《Sun Java System 1 2004Q3 Identity Synchronization for Windows 版本說明》*中所述，將代理程式的記憶體限制增至 1 或 2 GB。
- 在 idsync resync 作業期間，維持記錄層級的設定爲「資訊」。變更記錄層級爲「精細」或以上會增加代理程式負荷，這是因爲會有更多日誌訊息傳送至中央記錄程式。
- 一次針對單一「同步化使用者清單」執行 `idsync resync`。

如果代理程式確實發生記憶體不足，請採取下列復原步驟：

1. 檢查相應目錄中代理程式的永久性訊息存放區，驗證代理程式是否有積存的未傳遞訊息。
   - **Solaris 系統**：`/var/imq/instances/psw-broker/filestore/message/`
   - **Windows 系統**：<*installation_root*>`\isw-`<*machine_name*>`\imq\var\instances\isw-broker\filestore\message\`
2. 此目錄中的每個檔案都含有一個未傳遞的訊息。如果此目錄中有 10000 以上的檔案，則表明代理程式有訊息積存。[1] 否則，表明代理程式有其他問題。
3. 積存的訊息可能只是與 `idsync resync` 作業相關的日誌檔案，因此可將其安全移除。
4. 按照第 185 頁上的「啓動與停止服務」中的說明來停止 Message Queue 代理程式。
5. 移除永久性訊息存放區中的所有檔案。移除這些檔案的最簡單方法是遞迴移除 `message/` 目錄，然後再重建它。
6. 重新啓動 Message Queue 代理程式。

遵循本節的指示，以確保代理程式不會再次用盡記憶體。

1. 即使已傳遞了所有訊息，代理程式仍可能會保留最多 10000 個訊息檔案，以避免建立和刪除檔案而造成的效能損失。

SSL 問題疑難排解

診斷 SSL 問題時，另請參閱第 11 章，「配置安全性」中有關如何在 Identity Synchronization for Windows 中的元件間設定 SSL 的說明。本節包含下列內容：

- 核心程式元件間的 SSL
- 連接器與 Directory Server 或 Active Directory 間的 SSL
- Directory Server 外掛程式與 Active Directory 間的 SSL

核心程式元件間的 SSL

Identity Synchronization for Windows 安裝程式無法驗證核心程式安裝期間提供的 SSL 通訊埠是否正確。如果在核心元件安裝期間鍵入了錯誤的 SSL 通訊埠，核心元件便無法正常通訊。直至您首次嘗試儲存配置時，才會注意到存在問題。主控台將顯示以下警告訊息：

```
The configuration was successfully saved, however, the System Manager could
not be notified of the new configuration.
```

系統管理員日誌中會出現下列項目：

```
[10/Nov/2003:10:24:35.137 -0600] WARNING 14   example  "Failed to connect
to the configuration directory because "Unable to connect: (-5981)
Connection refused by peer.".Will retry shortly."
```

在此情況下，請解除安裝核心程式，並以正確的 SSL 通訊埠埠號再次安裝核心程式。

連接器與 Directory Server 或 Active Directory 間的 SSL

如果連接器無法透過 SSL 連接至 Directory Server 或 Active Directory，則中央錯誤日誌中會出現下列訊息：

```
[06/Oct/2003:14:02:48.911 -0600] WARNING 14  CNN100 host1  "failed to open
connection to ldaps://host2.airius.com:636."
```

開啓「主控台」並核取「指定進階安全選項」畫面 (請參閱第 123 頁)。

不可信的憑證

中央稽核日誌中提供有詳細資訊。例如，如果 LDAP 伺服器的 SSL 憑證不可信，則會記錄下列訊息：

```
[06/Oct/2003:14:02:480.951 -0600] INFO    14  CNN100 host1  "failed to open
connection to ldaps://host2.airius.com:636, error(91):Cannot connect to the
LDAP server, reason:SSL_ForceHandshake failed:(-8179) Peer's Certificate
issuer is not recognized."
```

在大多數情況下，不會將 CA 憑證新增至連接器的憑證資料庫。執行 Directory Server 隨附的 `certutil` 程式就可確認這一點。[1]

附註 `SUNWtlsu` 套件中提供了憑證管理公用程式，如 `certutil`，但 Directory Server 中未包捆有此類公用程式。(您可以從 Sun Microsystems 免費下載此套裝軟體。)

下載此套裝軟體後，您會在以下位置找到 `certutil`：

`/usr/sfw/bin/certutil`

1. 在 Solaris 系統上執行此命令前，必須新增 < *安裝根目錄* >`/lib` 目錄至 `LD_LIBRARY_PATH` 環境變數。

在此範例中，憑證資料庫中沒有憑證：[1]

```
# /usr/sunone/servers/shared/bin/certutil -L -d /usr/sunone/servers/
isw-host1/etc/CNN100
Certificate Name                                 Trust Attributes
p    Valid peer
P    Trusted peer (implies p)
c    Valid CA
T    Trusted CA to issue client certs (implies c)
C    Trusted CA to certs(only server certs for ssl) (implies c)
u    User cert
w    Send warning
```

在下列範例中，憑證資料庫僅包含 Active Directory CA 憑證：

```
# /usr/sunone/servers/shared/bin/certutil -L -d /usr/sunone/servers/
isw-host1/etc/CNN100
Certificate Name                                 Trust Attributes
airius.com CA                                    C,c,
p    Valid peer
P    Trusted peer (implies p)
c    Valid CA
T    Trusted CA to issue client certs (implies c)
C    Trusted CA to certs(only server certs for ssl) (implies c)
u    User cert
w    Send warning
```

如此處所示，CA 憑證的信任旗標必須是「C,,」。如果憑證存在並正確設定了信任旗標，但連接器仍然無法連接，請先驗證新增憑證後是否重新啓動了連接器，接著使用 Sun Java System 目錄隨附的 `ldapsearch` 指令來協助診斷問題。如果 `ldapsearch` 不接受憑證，連接器也不會接受。例如，`ldapsearch` 可拒絕不可信的憑證

1. Sun Java System Directory Server 和 Windows NT 連接器的預設憑證資料庫包含兩個憑證，即 `saint-cert100` 和 `saintRootCA`。此版本中不會使用這些憑證。

```
# /usr/sunone/servers/shared/bin/ldapsearch -Z -P /usr/sunone/
servers/isw-host1/etc/CNN100 -h host2 -b "" -s base "(objectclass=*)"
ldap_search: Can't contact LDAP server
    SSL error -8179 (Peer's Certificate issuer is not recognized.)
```

`-P` 選項指示 `ldapsearch` 使用連接器 CNN100 的憑證資料庫來驗證 SSL 憑證。將正確的憑證新增至連接器的憑證資料庫後，請驗證 `ldapsearch` 是否接受憑證，接著重新啓動連接器。

不符的主機名稱

當 Identity Synchronization for Windows 嘗試建立 SSL 連線時 (停用信任所有憑證設定)，Identity Synchronization for Windows 的連接器將驗證伺服器的主機名稱是否與伺服器在 SSL 交涉階段所提供憑證中的主機名稱相符。若主機名稱不符，連接器將拒絕建立連線。

Identity Synchronization for Windows 配置中的目錄來源主機名稱必須始終與該目錄來源所使用之憑證中內嵌的主機名稱相同。

您可以使用 `ldapsearch` 來驗證主機名稱是否相符，如下所示：

```
/var/mps/serverroot/shared/bin/ldapsearch.exe -Z -P
/var/opt/SUNWisw/etc/CNN100 -3
-h host2.example.com -p 636 -s base -b "" "(objectclass=*)"
```

若指令行中的主機名稱 (`host2.example.com`) 與憑證中內嵌的主機名稱不符，則會顯示下列錯誤訊息：

```
ldap_search: Can't contact LDAP server
SSL error -12276 (Unable to communicate securely with peer: requested do
main name does not match the server's certificate.)
```

若主機名稱相符，`ldapsearch` 指令成功執行，並顯示根 DSE 的內容。

過期的憑證

如果伺服器的憑證已過期，則會記錄下列訊息：

```
[06/Oct/2003:14:06:47.130 -0600] INFO    20  CNN100 host1  "failed to open
connection to ldaps://host2.airius.com:636, error(91):Cannot connect to the
LDAP server, reason:SSL_ForceHandshake failed:(-8181) Peer掇 Certificate has
expired."
```

在此情況下，必須向伺服器發出新憑證。

Directory Server 外掛程式與 Active Directory 間的 SSL

預設情況下，執行隨需密碼同步化時，Directory Server 不會透過 SSL 與 Active Directory 通訊。如果覆寫預設值來保護這一採用 SSL 的通訊，則必須按照第 11 章，「配置安全性」。中的說明將 Active Directory CA 憑證新增至每個主伺服器複本的 Directory Server 憑證資料庫。如果未新增此憑證，使用者將無法連結到 Directory Server，並發生錯誤「DSA 不願意執行。」，而外掛程式的日誌 (例如，`isw-<hostname>/logs/SUBC100/pluginwps_log_0.txt`) 將做以下報告：

```
[06/Nov/2003:15:56:16.310 -0600]  INFO    td=0x0376DD74 logCode=81
ADRepository.cpp:310    "unable to open connection to Active Directory
server at ldaps://host2.airius.com:636, reason: "
```

在此情況下，必須將 Active Directory CA 憑證新增至 Directory Server 的憑證資料庫，並重新啓動 Directory Server。

控制器問題疑難排解

從備份檔案復原 Active Directory 網域控制器時，無法重設某些計數器。

若要確保可正確重設所有計數器，請在還原 Active Directory 網域控制器後重新同步化所有使用者。

第 10 章

認識稽核與錯誤檔案

Identity Synchronization for Windows 提供有關安裝與配置狀態、日常系統作業，及任何部署出錯情況的資訊。

本章說明如何存取及瞭解下列各節中的資訊：

認識日誌

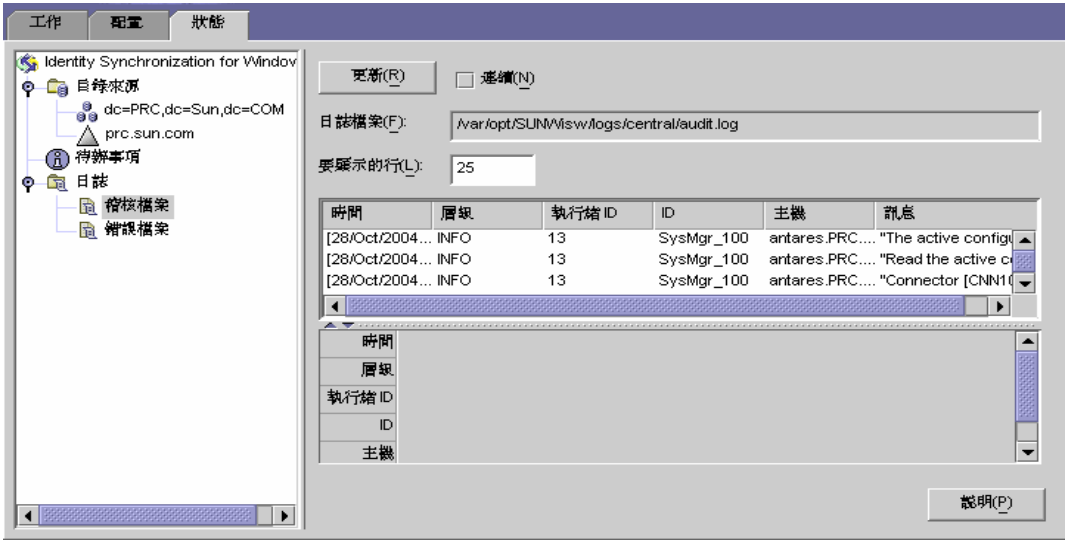
您可從 Identity Synchronization for Windows 主控台的「狀態」標籤中檢視各種類型的資訊。

如果您在導覽樹窗格 (左側) 中選取了下列任一節點，「狀態」標籤上顯示的內容就會改變，轉而顯示有關該項目的詳細資訊。

- **目錄來源**：選取一個目錄來源節點 (例如 dc=example,dc=com) 以檢視有關該目錄來源的狀態資訊。
- **待辦事項**：選取此節點可顯示一份步驟清單，清單上列出成功安裝及配置 Identity Synchronization for Windows 所必須完成的步驟 (本程式會使所有已完成的步驟呈灰色顯示)。
- **稽核檔案**：選取此節點可顯示有關日常系統作業的資訊 (包括出錯情況)。

- **錯誤檔案**：選取此節點可顯示有關您系統上錯誤情況的資訊。(錯誤日誌基本上相當於一個篩選器，專門篩選顯示錯誤項目。)

圖 10-1 「狀態」標籤



日誌類型

本節說明 Identity Synchronization for Windows 使用的各種不同日誌類型：

- 第 268 頁上的「中央日誌」
- 第 269 頁上的「本機元件日誌」
- 第 270 頁上的「Windows NT 本機子元件日誌」
- 第 270 頁上的「Directory Server 外掛程式日誌」

中央日誌

只要 Identity Synchronization for Windows 元件能夠存取 Message Queue，所有的稽核及錯誤訊息就都會記錄在 Identity Synchronization for Windows 中央記錄程式中。因此，這些中央日誌 (包括所有元件發出的訊息) 是監視的主要對象。

集中式日誌位於安裝有核心程式的電腦上的下列目錄之中：

- **Solaris 系統**：`/var/opt/SUNWisw/logs`

- **Windows 系統**：<*installation_root*>/isw-<*machine_name*>/logs/central/

具體的日誌詳見表格 10-1。

表格 10-1 Identity Synchronization for Windows 日誌類型

日誌名稱	描述
error.log	報告警告及嚴重訊息。
audit.log	即 error.log 的超集合，其中包含各個同步化事件的相關訊息。
resync.log	報告由 resync 指令所產生的訊息。

各中央日誌亦包含每個元件 ID 的相關資訊。例如：

```
[2003/03/14 14:48:23.296 -0600] INFO    13     "System Component
Information:SysMgr_100 is the system manager (CORE);  console is the Product
Console User Interface;  CNN100 is the connector that manages [airius.com
(ldaps:// server1.airius.com:636)];  CNN101 is the connector that manages
[dc=airius,dc=com (ldap:// server2.airius.com:389)];"
```

除了中央記錄程式之外，各個元件都有它們自己的本機日誌。如果連接器發生的問題無法記錄在中央記錄程式上，則您可使用這些本機日誌來診斷發生的問題。

本機元件日誌

每一連接器、系統管理員以及中央記錄程式均具有下列本機日誌：

表格 10-2 本機日誌

日誌名稱	描述
audit.log	即 error.log 的超集合，其中包含各個同步化事件的相關訊息。這類訊息亦會寫入中央 audit.log.。
error.log	報告警告及嚴重訊息。這類訊息亦會寫入中央 error.log。

上述本機日誌位於下列子目錄中：

- **Solaris 系統**：/var/opt/SUNWisw/logs
- **Windows 系統**：<*installation_root*>/isw-<*machine_name*>/logs/central/

sysmgr 與 clogger100 (中央記錄程式) 目錄位在安裝有核心程式的電腦上。

Identity Synchronization for Windows 會藉由將目前的日誌移至包含日期的日誌檔而進行這些本機元件日誌的每日輪替，例如：

```
audit_2004_08_06.log
```

附註 依照預設，Identity Synchronization for Windows 會在十天後刪除連接器日誌。您可編輯 Log.properties 檔案中的 com.sun.directory.wps.logging.maxmiumDaysToKeepOldLogs 值並重新啓動服務常駐程式來延長此期間。

Windows NT 本機子元件日誌

下列 Windows NT 子元件亦具有本機日誌：

- Windows NT 變更偵測器 DLL
- 密碼篩選器 DLL

這類子元件日誌位在以下目錄的 SUBC1XX (如 SUBC100) 子目錄中：

<installation_root>/isw-*<machine_name>*/logs/

Identity Synchronization for Windows 會限制這類日誌的大小不得超過 1 MB，並且只保留最新的 10 個日誌。

Directory Server 外掛程式日誌

Directory Server 外掛程式透過 Directory Server 連接器以及 Directory Server 記錄設備，將資訊記錄到中央日誌中。因此，Directory Server 本機外掛程式日誌訊息也將儲存在 Directory Server 錯誤日誌中。

Directory Server 將其他 Directory Server 外掛程式和元件的資訊儲存在錯誤日誌中。爲了識別 Identity Synchronization for Windows Directory Server 外掛程式的訊息，您可篩選出包含 isw 字串的文字行。

依照預設，錯誤日誌中只會顯示最精簡的外掛程式日誌訊息。例如：

```
[14/Jun/2004:17:08:36 -0500] - ERROR<38747> - isw - conn=-1 op=-1 msgId=-1
- Plugins unable to establish connection to DS Connector at attila:1388,
will retry later
```

您可按照如下方式，從 Directory Server 管理主控台變更 Directory Server 錯誤日誌的預設冗長度：

1. 開啓 Directory Server 主控台。
2. 選擇「配置」標籤。
3. 按一下導覽窗格中的「日誌」節點。
4. 選取「錯誤」標籤。
5. 按一下「日誌層級」按鈕。
6. 啓用「外掛程式」方塊。如果想要讓日誌內容更詳細，也可以啓用「精細模式」。
7. 按一下「確定」，然後按一下「儲存」。

有關 Directory Server 記錄功能的詳細資訊，請參閱 *《Sun Java System Directory 5 2004Q2 Server Administrator's Guide》* (http://docs.sun.com/db/coll/DirectoryServer_04q2)。

讀取日誌

每一條日誌訊息都包含以下資訊：

- **時間：**指明產生日誌項目的時間及日期。例如：

  ```
  [13/Aug/2004:06:14:36:753 -0500]
  ```

- **層級：**指明日誌訊息的嚴重性與冗長度。
  Identity Synchronization for Windows 使用下列日誌層級：

表格 10-3 日誌層級

日誌層級	描述
資訊	這些訊息提供有關各項動作的最精簡資訊，以便您確定系統執行是否正常。例如，您可看到偵測到變更的時間以及同步化發生的時間。這些訊息一律會記錄到稽核日誌。
精細	這類訊息包含動作在系統內傳遞期間之進一步資訊。
更精細	這類訊息包含動作在系統內傳遞期間之更詳細資訊。如將所有元件的記錄層級設定爲「更精細」，可能會影響效能。
最精細	這類訊息包含動作在系統內傳遞期間之最詳盡的資訊。如將所有元件的記錄層級設定爲「最精細」，可能會嚴重影響效能。

- **執行緒 ID**：顯示導致事件發生的功能之 Java 執行緒 ID。
- **ID**：識別導致事件發生的元件 (主控台、系統管理員等等)。
- **主機**：顯示導致事件發生的主機之名稱。
- **訊息**：顯示與事件相關的稽核或錯誤資訊。在此列舉如下範例：

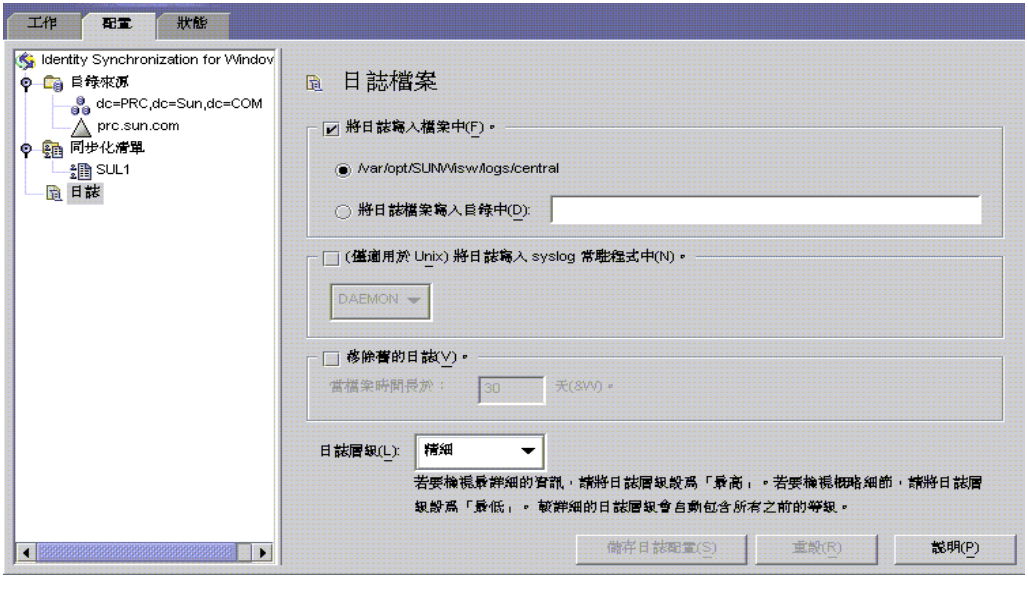
  "Resetting Central Logger configuration ..."
  "System manager is shutting down."
  "Processing request (ID=<*ID_number*> from the console to stop synchronization."

配置日誌檔案

您可使用 Identity Synchronization for Windows 主控台來配置您的部署的記錄功能，方法如下：

1. 開啓主控台，選取「配置」標籤。
2. 展開導覽樹窗格中的節點，直到看見「日誌」節點爲止。
3. 選取「日誌」節點，「日誌檔案」窗格即顯示在「配置」標籤上 (請參閱圖 10-2)。

圖 10-2 配置日誌檔案



4. 透過「日誌檔案」窗格來配置日誌檔案，步驟如下：

   - **將日誌寫入檔案中。**啓用此選項可將日誌寫入核心主機上的檔案。

     選取此選項後，即可：

     - 啓用預設日誌目錄和檔案 (例如，/var/opt/SUNWisw/logs/central)。
     - 啓用「將日誌檔案寫入目錄中」選項，並爲該日誌檔案指定路徑及檔名。

     附註 主控台不會驗證指定的日誌檔案位置是否確實存在。如果日誌目錄不存在，則中央記錄程式將嘗試建立該日誌目錄。因此，在您嘗試檢視日誌之前，不會有訊息指出所指定及儲存的日誌位置不存在。試著檢視日誌數次後，會出現訊息指出主控台在指定位置找不到日誌。

   - *僅限 Solaris* — **將日誌寫入 syslog 常駐程式中。**如果 Identity Synchronization for Windows 常駐在 Solaris 平台，請啓用此選項。使用下拉清單來選取寫入日誌的方式。(*預設值爲 DAEMON*。)

     附註 如果選取此選項，Identity Synchronization for Windows 會將一切事件記錄在 syslog 中，不過，syslog 的預設配置是只記錄「警告」與「嚴重」訊息。

     若要配置 syslog，使其記錄「資訊」訊息，請編輯 /etc/syslog.conf 並將下列文字行：

     ```
     *.err;kern.debug;daemon.notice;mail.crit
     /var/adm/messages
     ```

     變更爲

     ```
     *.err;kern.debug;daemon.notice;daemon.info;mail.crit
     /var/adm/messages
     ```

     作好此變更之後，必須以如下方式重新啓動 syslog 常駐程式：

     ```
     /etc/init.d/syslog stop ; /etc/init.d/syslog start
     ```

     若要啓用「精細」、「更精細」和「最精細」記錄功能，請將 daemon.debug 納入以分號分隔的清單中。

- **移除舊的日誌。**日誌檔案的數量將會持續無止盡地增加 (每天一個檔案)。爲了避免磁碟空間不足，請啓用此選項並指定程式可在何時從中央日誌檔案中刪除舊的日誌。

  例如，如果您指定 30 天，Identity Synchronization for Windows 會將達到 31 天的檔案全部移除。

- **日誌層級。**使用下拉清單選取您希望在系統日誌中看到的詳細資料層級。(請參閱第 271 頁上的「日誌層級」。)

5. 按一下「儲存日誌配置」按鈕可根據所選的選項來建立日誌檔案。

檢視目錄來源狀態

若要檢視您的目錄來源的狀態，請：

1. 從 Identity Synchronization for Windows 主控台中，選取「狀態」標籤。
2. 在導覽樹窗格中，展開「目錄來源」節點，然後選取目錄來源節點 (例如 dc=example,dc=com)。

   「狀態」標籤的內容改爲顯示有關所選目錄來源的資訊 (示例請參閱圖 10-3)。

圖 10-3 目錄來源狀態

附註 當您檢視目錄來源狀態時，實際上是在檢視與目錄來源聯結的連接器狀態。

「狀態」標籤中顯示下列資訊：

- **更新：**按一下「更新」可更新此標籤中的資訊。
- **狀態：**反映出目錄來源的目前狀態。有效的狀態包括：
  - **未安裝：**連接器尚未安裝。
  - **已安裝：**已安裝連接器，但是尚未準備好進行同步化，因爲還沒接收到運行時間配置。如果連接器維持此狀態超過一分鐘，表示可能發生某些錯誤。
  - **就緒：**連接器已準備好進行同步化，但目前尚未開始同步化任何物件。如果尚未啓動同步化，或雖然已啓動同步化，但並非所有子元件均已建立與連接器之間的連線，則連接器會維持「就緒」狀態。
  - **正在同步：**連接器正在同步化物件。可能仍有錯誤，所以如果您發現變更未同步化，請查看錯誤日誌。
- **使用中**：指出目錄來源正在使用中還是已經關閉。
- **上次通訊：**指出上次目錄來源的連接器回應的時間。

檢視安裝與配置狀態

若要查看還要進行哪些步驟才能完成 Identity Synchronization for Windows 的安裝與配置過程，請使用下列程序：

1. 從 Identity Synchronization for Windows 主控台中，選取 「狀態」標籤。
2. 展開導覽樹窗格中的 「待辦事項」節點。

   「狀態」標籤的內容改爲顯示安裝與配置步驟的核對清單 (示例請參閱圖 10-3)。

圖 10-4 檢視待辦事項清單

3. 按一下 「更新」按鈕 (右上方) 更新清單。

   完成的步驟將會顯示核取標記並呈現灰色。您必須完成剩下的步驟才能順利完成安裝與配置過程。

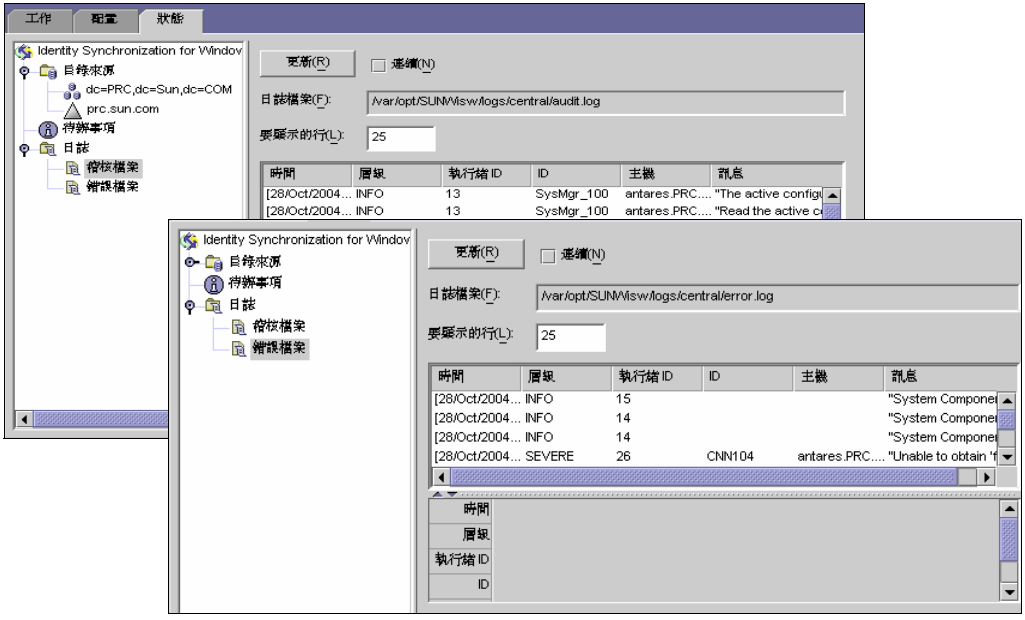
檢視稽核和錯誤日誌

若要檢視您的錯誤日誌，請：

1. 從 Identity Synchronization for Windows 主控台中，選取 「狀態」標籤。
2. 在導覽樹窗格中，展開 「稽核檔案」或 「錯誤檔案」節點。

「狀態」標籤內容改爲顯示目前的日誌 (圖 10-5)。

圖 10-5 檢視日誌



「狀態」標籤中顯示下列資訊：

- **更新**：載入最新的稽核或錯誤資訊。
- **連續**：不斷地更新及顯示最新的稽核或錯誤資訊。
- **日誌檔案**：顯示讀取的稽核或錯誤日誌之完整路徑名稱，例如：

  `C:\Program Files\Sun\MPS\isw-<`*hostname*`>\logs\central\audit.log`
- **要顯示行**：指定顯示多少稽核或錯誤項目。(*預設值爲 25* 。)

啓用 Windows NT 電腦上的稽核功能

如果您的部署環境中有 Windows NT 電腦，請確定已啓用稽核功能，否則 Identity Synchronization for Windows 無法記錄來自該台電腦的訊息。

使用下列程序可啓用 Windows NT 電腦上的稽核記錄功能：

1. 從 Windows NT 的「開始」功能表中，選取「程式集」>「系統管理工具」>「網域使用者管理員」。
2. 當「使用者管理員」對話方塊顯示時，從功能表列選取「原則」>「稽核」。

   出現「稽核原則」對話方塊。
3. 啓用「稽核下列事件」按鈕，然後啓用「成功」與「失敗」方塊。
4. 按一下「確定」關閉對話方塊。

這些設定會一直有效，直到您再次改變它們爲止。

第 11 章

配置安全性

本章介紹有關配置部署安全性的重要資訊。內容歸納如下：

附註 本章的內容是假設您已經熟悉公開金鑰加密法以及安全資料傳輸層 (SSL) 協定的基本概念，並瞭解內部網路、外部網路和網際網路安全，以及企業中數位憑證角色的概念。如果您不熟悉這些概念，請參閱手冊 *《Managing Servers with iPlanet Console 5.0》*中與安全性相關的附錄。

安全概觀

密碼爲敏感資訊；因此，Identity Synchronization for Windows 採取了安全預防措施，以確保用來存取同步化目錄的使用者和管理密碼憑證不會被洩漏。

本節涵蓋下列安全方法：

此安全方法目的是爲避免發生下列事件：

- 偷竊者透過網路攔截純文字密碼
- 攻擊者使用連接器變更使用者密碼爲其選擇的值，這相當於攔截使用者的純文字密碼
- 攻擊者取得 Identity Synchronization for Windows 的授權元件的存取權限
- 非授權使用者從磁碟上儲存的檔案中重新找回密碼
- 入侵者從原爲系統元件之一、但已移除的硬碟中找到密碼。這可能是一個同步化的密碼，或一個用來存取目錄的系統密碼。

指定配置密碼

在產品配置目錄中儲存敏感資訊以及在網路中進行傳輸的過程中，爲了保護這些資訊的安全，Identity Synchronization for Windows 使用*配置密碼*。您 (管理員) 在安裝核心元件時必須指定一個配置密碼，並且在開啓主控台或執行 Identity Synchronization for Windows 安裝程式時必須提供此密碼。

附註 系統管理員必須存取配置密碼後才能將其傳送給連接器，因此系統管理員會將此密碼儲存在其初始化檔案中。

檔案系統存取控制可防止未經授權的使用者存取系統管理員的初始化檔案。Identity Synchronization for Windows 安裝程式不會對此密碼強制使用密碼策略。

若要在選擇配置密碼時增加安全性，請參閱第 286 頁上的 「強化安全」。

使用 SSL

您可配置 Identity Synchronization for Windows，使其在元件使用 LDAP 的所有位置都使用 LDAP over SSL。對 Message Queue 的所有存取都受 SSL 保護。

在從 Directory Server 同步化到 Active Directory 時，必須在 Active Directory 連接器與 Active Directory 之間使用 SSL。

需要可靠的 SSL 憑證

依照預設，配置爲使用 SSL 的連接器將接受伺服器 (也就是 Directory Server 或 Active Directory) 傳回的任何 SSL 憑證，其中包括不可靠、已過期及無效的憑證。連接器與伺服器之間的所有網路通訊將會經過加密，但連接器不會偵測出僞裝成真正 Active Directory 或 Directory Server 的伺服器。

若要強制使連接器只接受可靠憑證，請使用主控台來啓用 「目錄來源配置精靈」中「指定進階安全選項」畫面上的「需要可信任的 SSL 憑證」選項 (請參閱第 123 頁)。啓用此選項之後，必須按照 `idsync certinfo` 的報告，將相應的 CA 憑證加入連接器的憑證資料庫中。

產生的 3DES 金鑰

由配置密碼產生的 3DES 金鑰可用來保護產品配置目錄中所有敏感資訊的安全。除了日誌訊息外，所有 Message Queue 的訊息均以按主題的 3DES 金鑰進行加密。連接器與子元件間傳送的訊息則以按作業階段的 3DES 金鑰加密。Directory Server 外掛程式以 3DES 金鑰加密所有使用者密碼變更。

SSL 與 3DES 金鑰保護摘要

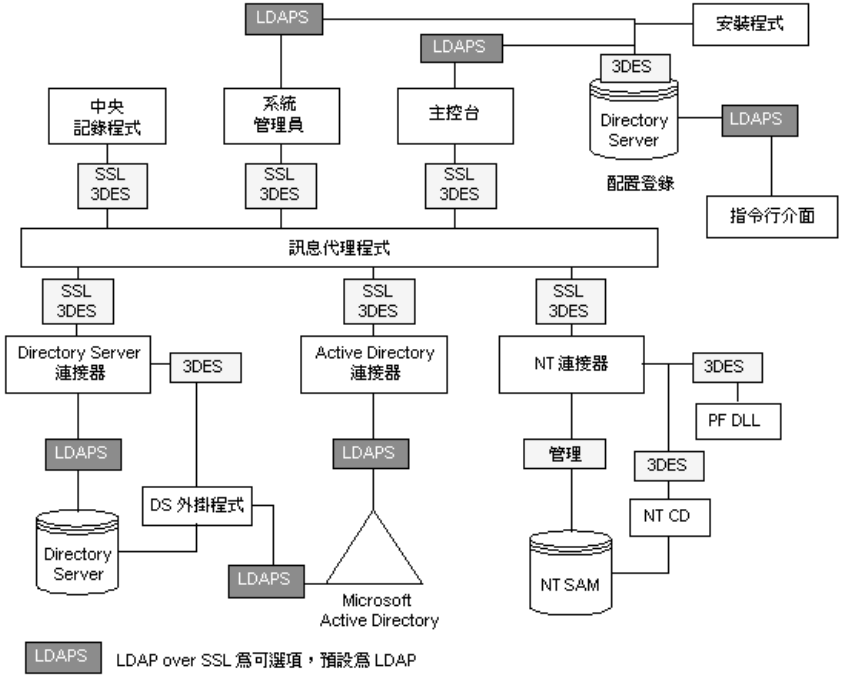
表格 11-1 摘要說明了 Identity Synchronization for Windows 如何保護透過網路傳送的敏感資訊的安全。

表格 11-1 使用網路安全性功能來保護敏感資訊

使用此保護方式	在下列資訊類型之間
LDAP over SSL (可選)	• Directory Server 連接器和 Directory Server，Active Directory 連接器和 Active Directory • Directory Server 外掛程式和 Active Directory • 指令行介面和產品的配置目錄 • 主控台和產品的配置目錄 • 主控台和 Active Directory 通用類別目錄 • 主控台和 Active Directory 網域或同步化的 Directory Server • Message Queue 代理程式和產品的配置目錄 • 連接器、系統管理員、中央記錄程式、指令行介面和主控台可透過 LDAPS 來驗證 Message Queue • 安裝程式和配置目錄伺服器 • 安裝程式和 Active Directory • 安裝程式和同步化的 Directory Server
以 3DES 金鑰加密 (預設)	• Directory Server 連接器和 Directory Server 外掛程式 (包括所有資料) • Windows NT 連接器、Windows NT 密碼篩選器 DLL 和 Windows NT 變更偵測器 (包括所有資料) • 產品配置目錄中的所有敏感資訊 • 在連接器和子元件間傳送的所有訊息 (以按作業階段的 3DES 金鑰加密) • 透過 Message Queue 傳送的所有 (非日誌) 訊息

圖 11-1 包含本節所討論的安全功能概觀。

圖 11-1 Identity Synchronization for Windows 安全概觀



Message Queue 存取控制

Identity Synchronization for Windows 使用 Message Queue 的存取控制以避免未授權存取訊息訂閱和發佈，使每個連接器可信任它所接收到的信任訊息。

只有 Message Queue 和連接器已知的專有使用者名稱與密碼，才可用來存取 Message Queue 代理程式。每條透過 Message Queue 傳送的訊息均以按主題的 3DES 金鑰加密，這可保護訊息內容並避免不瞭解主題金鑰的外界人士傳送有意義的訊息。這些方法可避免 (a) 攻擊者傳送偽裝的密碼同步化訊息到連接器，(b) 攻擊者偽裝成連接器並接收真正的密碼更新訊息。

附註 依預設，Message Queue 的用戶端，如連接器和系統管理員，將接受任何 Message Queue 代理程式傳回的 SSL 憑證。有關如何強化 Message Queue 憑證驗證與其他與 Message Queue 相關的安全議題的詳細資訊，請參閱第 286 頁上的「強化安全」。

目錄憑證

連接器需要授權的憑證以變更 Active Directory 以及同步化 Directory Server 中的密碼。這些授權的憑證在儲存於產品配置目錄前會先經過加密。

永久性儲存保護摘要

表格 11-2 摘要說明了 Identity Synchronization for Windows 如何保護儲存於磁碟上的敏感資訊的安全。

表格 11-2 永久性儲存保護

永久性儲存	機密資訊	保護
配置目錄伺服器中儲存的產品配置	存取目錄所需的憑證與按 Message Queue 主題的 3DES 金鑰儲存於產品配置目錄中。	所有儲存於產品配置目錄中的敏感資訊均以配置密碼所產生的 3DES 金鑰進行加密。有關進一步保護產品配置目錄的相關建議，請參閱「強化安全」。
Directory Server Retro Changelog	Directory Server 外掛程式擷取密碼變更並先將其加密，然後再將其寫入 Directory Server Retro Changelog 中。	Directory Server 外掛程式以每個部署專有的 3DES 金鑰來加密所有使用者密碼變更。
Message Queue 代理程式永久性儲存	Message Queue 代理程式儲存在所有連接器間傳送的同步化訊息。	除了日誌訊息外，所有持續訊息均以按主題的 3DES 金鑰加密。
Message Queue 代理程式目錄憑證	Message Queue 代理程式依據產品配置目錄驗證使用者。它使用核心安裝時提供的目錄管理使用者名稱與密碼連接到配置目錄。	目錄密碼儲存於 passfile 中，後者由檔案系統存取控制保護。
系統管理員啓動檔案	系統管理員啓動檔案包含存取配置的資訊。其中包括配置密碼與核心安裝時提供的目錄管理使用者名稱與密碼。	此檔案由檔案系統存取控制保護。
連接器和中央記錄程式啓動檔案	每個連接器以及中央記錄程式都有一個包含存取 Message Queue 所需憑證的初始配置檔案。	這些檔案由檔案系統存取控制保護。
目錄伺服器外掛程式啓動配置	外掛程式的配置 (儲存於 cn=config) 包含連接到連接器所需的憑證。	子樹狀目錄 cn=config 以 ACI 進行保護，而鏡像此樹狀結構的 `dse.ldif` 檔案則以檔案系統存取控制來保護。
NT 密碼篩選器 DLL 以及 NT 變更偵測器啓動配置	NT 子元件配置 (儲存於 Windows 登錄中) 包含連接到連接器所需的憑證。	如果 PDC 登錄存取不安全，可以用存取控制保護這些登錄金鑰。
Windows 連接器的物件快取	Windows 連接器將雜湊的使用者密碼儲存在連接器的物件快取中。	密碼不是以純文字格式儲存，但以 MD5 雜湊進行加密。這些資料庫檔案由檔案系統存取控制保護 (請參閱「強化安全」)。

強化安全

此節說明產品目前版本中存在的潛在安全問題，以及有關如何在產品預設配置外擴展並加強安全性的建議。內容包含下列幾項：

配置密碼

配置密碼用來保護敏感的配置資訊，但安裝程式並不對此密碼強制使用任何密碼策略；請確保此密碼遵循嚴格的指導原則，選擇一個複雜的密碼，該密碼不易被猜出，並遵循增強式密碼的標準策略指導原則。

例如，密碼應至少有八個字元，包含大小寫字母以及非字母數字字元。密碼不應包括您的姓名、縮寫或日期。

建立配置目錄憑證

若要存取產品配置目錄所在的 Directory Server，您的憑證必須位於配置管理員群組中。不過，如果您出於任何原因而需要建立除 *admin* 之外的憑證，請考慮下列事項：

安裝程式要求您爲儲存於主控台管理子樹狀結構中的使用者供應憑證。不過，核心安裝程式不會將除了 *admin* 以外的使用者展開爲 "`uid=admin,ou=Administrators, ou=TopologyManagement, o=NetscapeRoot`"。因此，您必須在進行核心安裝時指定整個 DN。

若要建立 *admin* 以外的新使用者：

1. 以下列方式建立使用者

   ```
   ou=Administrators, ou=TopologyManagement, o=NetscapeRoot
   ```

2. 將新憑證加入配置管理員群組中

3. 設定 ACI，使其只允許此使用者或配置管理員群組中的所有使用者存取儲存產品配置目錄處的 Directory Server
4. 在核心安裝期間指定整個 DN

   有關管理 Directory Server 中存取控制的詳細資訊，請參閱 *《Sun Java System Directory Server 5 2004Q2 Administrator's Guide》*第 6 章：〈Managing Access Control〉。

Message Queue 用戶端憑證驗證

依預設，Message Queue 的用戶端，如連接器和系統管理員，將接受任何 Message Queue 代理程式傳回的 SSL 憑證。

1. 若要取代此設定並強制 Message Queue 用戶端驗證 Message Queue 代理程式的憑證，請編輯：

   `<`*installation_root*`>/resources/WatchList.properties`

2. 將下列內容新增到 `Watchlist.properties` 中每一程序的 JVM 引數中：

   ```
   -Djavax.net.ssl.trustStore=<keystore_path>
   -DimqSSLIsHostTrusted=false
   ```

3. 重新啓動 Identity Synchronization for Windows 常駐程式或服務。

`javax.net.ssl.trustStore` 屬性應該指向信任代理程式憑證的 JSEE 金鑰庫，例如，`/etc/imq/keystore` 可用於安裝核心的電腦上，因爲這是由代理程式使用的金鑰庫。

Message Queue 自簽 SSL 憑證

依照預設，Message Queue 代理程式使用自簽 SSL 憑證。若要安裝不同的憑證，可使用 Java 隨附的 `keytool` 公用程式以修改代理程式的金鑰庫 (在 Solaris 系統中位於 `/var/imq/instances/isw-broker/etc/keystore`，在 Windows 2000 系統中位於 `<`*mq_installation_root*`>/var/instances/isw-broker/etc/keystore`)。憑證別名必須爲 `imq`。

存取 Message Queue 代理程式

依照預設，Message Queue 的所有服務都使用動態通訊埠，但它本身的通訊埠對映器除外。爲了透過防火牆存取代理程式或限制可以連接到代理程式的主機組，對於所有服務，代理程式應使用固定通訊埠。

這可透過設定 `imq.<`*服務名稱*`>.<`*通訊協定類型*`>.port` 代理程式配置屬性來完成。請參閱 *《Sun Java System Message Queue Administrator's Guide》*以獲得詳細資訊。

配置目錄憑證驗證

在透過 SSL 連接到產品配置目錄時，系統管理員接受任何憑證；在透過 SSL 連接到產品配置目錄時，Message Queue 代理程式接受任何憑證。目前無法使系統管理員或 Message Queue 代理程式驗證產品配置目錄 SSL 憑證。

限制存取配置目錄

安裝核心時，將資訊新增到儲存產品配置目錄的 Directory Server 的程序不包含新增任何存取控制資訊。要將存取限制爲配置管理員，可使用下列 ACI：

```
(targetattr = "*") (target =
"ldap:///ou=IdentitySynchronization,ou=Services,dc=example,dc=com")
(version 3.0;acl "Test";deny (all)(groupdn != "ldap:///cn=Configuration
Administrators, ou=Groups, ou=TopologyManagement, o=NetscapeRoot");)
```

有關管理 Directory Server 中存取控制的詳細資訊，請參閱 *《Sun Java System Directory Server 5 2004Q2 Administrator's Guide》*第 6 章：〈Managing Access Control〉。

保護複製配置的安全

使用複製連接到 Directory Server 的部署遵循安全概觀中所列的相同規則。此節提供一個範例複製配置，並說明如何於此配置中啓用 SSL。

附註 有關規劃、部署和保護複製配置的概觀，請參閱附錄 E，「複製環境的安裝註解」。

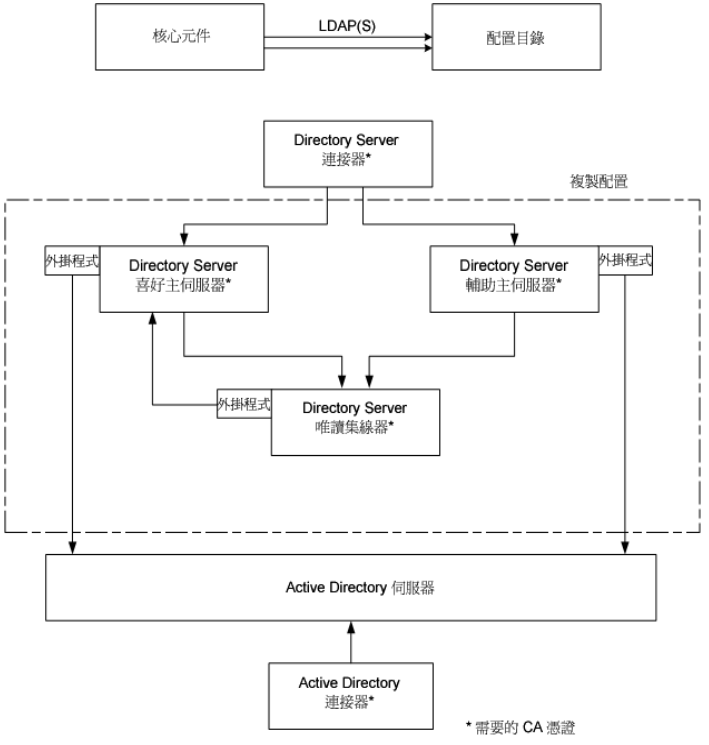
表格 11-3 列出需要 CA 憑證的配置元件，並指出在相應位置需要哪些憑證。

表格 11-3 需要 CA 憑證的 MMR 配置元件

元件	需要的 CA 憑證
優先的 Directory Server 複製主伺服器	Active Directory 系統
輔助 Directory Server 複製主伺服器	Active Directory 系統
唯讀的 Directory Server 集線器	優先的 Directory Server 複製主伺服器 輔助 Directory Server 複製主伺服器
Directory Server 連接器	優先的 Directory Server 複製主伺服器 輔助 Directory Server 複製主伺服器
Active Directory 連接器	Active Directory 系統

圖 11-2 顯示以 MMR 配置安裝的 Identity Synchronization for Windows，其中有兩個包含多個 Directory Server 唯讀集線器或用戶的重複 Directory Server 主伺服器。每個 Directory Server 都有一個外掛程式，但只有一個 Directory Server 連接器、一個 Active Directory 系統以及一個 Active Directory 連接器。

圖 11-2 複製配置



附註 如果爲 SSL 配置 Directory Server 來源，必須確保喜好和次要 Directory Server 憑證均獲得重複 Directory Server 的信任。對於以 Directory Server 集線器或唯讀副本安裝於系統上的每個其他類型的 Directory Server 外掛程式，情況亦如此。

Directory Server 外掛程式與其相關 Directory Server 可存取相同的 CA 憑證。

使用 idsync certinfo

基於目前的 Identity Synchronization for Windows SSL 設定，使用 `idsync certinfo` 公用程式確定所需要的憑證。執行 `idsync certinfo` 以擷取有關每個憑證資料庫中所需憑証的資訊。

附註 爲 SSL 配置 Directory Server 來源時，您必須確定喜好與輔助 Directory Server 憑證均獲得所有目錄子元件或外掛程式的重複 Directory Server 的信任。

如果 Identity Synchronization for Windows 嘗試建立 SSL 連線 (已啓用信任所有憑證的設定)，而伺服器的主機名稱與 SSL 交涉階段由伺服器提供之憑證中的主機名稱不相符，則 Identity Synchronization for Windows 連接器將拒絕建立連線。

Identity Synchronization for Windows 配置中的目錄來源主機名稱必須始終與該目錄來源所使用之憑證中內嵌的主機名稱相同。

引數

表格 11-4 說明可用於 `idsync certinfo` 子指令的引數：

表格 11-4 certinfo 引數

引數	說明
`-h` <*CR-hostname*>	指定配置目錄主機名稱。本引數預設爲安裝核心期間指定的值。
`-p` <*CR-port-no*>	指定配置目錄 LDAP 通訊埠埠號。(*預設值爲 389*。)
`-D` <*bind-DN*>	指定配置目錄連結辨別名稱 (DN)。本引數預設爲安裝核心期間指定的值。
`-w` <*bind-password* | `->`	指定配置目錄連結密碼。 - 值從標準輸入 (STDIN) 讀取密碼。
`-s` <*rootsuffix*>	指定配置目錄根字尾。其中根字尾是一個辨別名稱，例如 `dc=example,dc=com`。 本引數預設爲安裝核心期間指定的值。
`-q` <*configuration_password*>	指定配置密碼。- 值從標準輸入 (STDIN) 讀取密碼。

用法

以下範例使用 idsync certinfo 來搜尋獲派於 SSL 通訊下執行的系統元件。此範例的結果可以確定兩個連接器 (CNN101 以及 CNN100)，並提供有關從何處匯入相應 CA 憑證的說明。

```
:\Program Files\Sun\MPS\isw-hostname\bin> idsync certinfo -h CR-hostname
-p 389 -D "cn=Directory Manager" -w dirmanager -s dc=example,dc=com
-q <password>
Connector:CNN101
Certificate Database Location: C:\Program
Files\Sun\MPS\isw-hostname\etc\CNN101
Get 'Active Directory CA' certificate from Active Directory and import into
Active Directory Connector certificate db for server
ldaps::/hostname.example.com:636
Connector:CNN100
Certificate Database Location:   C:\Program
Files\Sun\MPS\isw-hostname\etc\CNN100
Export 'Directory Server CA' certificate from Directory Server certificate
db and import into Directory Server Connector certificate db
ldaps://hostname.example.com:636
Export 'Active Directory CA' certificate from Active Directory Server
hostname.example.sun.com:389 and import into Directory Server Server
certificate db for server ldaps://hostname.example.com:638
SUCCESS
```

在 Directory Server 中啓用 SSL

遵循這些步驟，使用自簽憑證以在 Directory Server 中啓用 SSL。

附註 這些簡化程序是爲了方便您使用。有關詳細資料，請參閱「*Directory Server 5 2004Q2 Administrator's Guide*」。

附註

- 在 Windows 中，請使用 Directory Server 5 2004Q2 版 (或更新版本) 隨附的 `certutil`。

  *不要*使用 5 2004Q2 之前 Directory Server 各版本隨附的 `certutil`。`certutil` 的早期版本與 Identity Synchronization for Windows 不相容。

- 在 Solaris 中，依照預設已將 `certutil` 安裝在 `/usr/sfw/bin` 中。

1. 爲 Directory Server 建立一個新的金鑰憑證資料庫，方法爲輸入下列內容：

```
C:\Program Files\Sun\MPS\shared\bin\certutil.exe -d . -P slapd-hostname-

In order to finish creating your database, you
must enter a password which will be used to
encrypt this key and any future keys.
The password must be at least 8 characters long,
and must contain at least one non-alphabetic character.
Enter new password:
Re-enter password:
```

附註 這些範例於伺服器根下第一層目錄 `alias` 中執行。否則，Directory Server 將無法找到憑證資料庫。

2. 產生自簽憑證，這將是 Directory Server 使用的伺服器憑證。確保根據 Directory Server 執行時所在伺服器的主機名稱選擇主題 DN。

附註 依照預設，自簽憑證有效期爲三個月。如果您要增加或減少此期間，請使用 -v <*months-valid*> 選項。例如，要將期間增加到 24 個月，輸入 **-v 21**，或要將此期間減少爲一個月，則輸入 **-v -2**。

```
C:\Program Files\Sun\MPS\shared\bin\certutil.exe -d . -P slapd-hostname-
-S -n server-cert -s "cn=hostname.example.com,c=us" -x -t CTu,,
A random seed must be generated that will be used in the
creation of your key.One of the easiest ways to create a
random seed is to use the timing of keystrokes on a keyboard.
To begin, type keys on the keyboard until this progress meter
is full.DO NOT USE THE AUTOREPEAT FUNCTION ON YOUR KEYBOARD!
Continue typing until the progress meter is full:
|************************************************************|
Finished.Press enter to continue:
Enter Password or Pin for "NSS Certificate DB":
Generating key.This may take a few moments...
```

3. 顯示憑證以供檢查之用。

```
C:\Program Files\Sun\MPS\shared\bin\certutil.exe -L -d . -P
slapd-hostname-
Certificate Name           Trust Attributes
server-cert                CTu,,
p    Valid peer
P    Trusted peer (implies p)
c    Valid CA
T    Trusted CA to issue client certs (implies c)
C    Trusted CA to certs(only server certs for ssl) (implies c)
u    User cert
w    Send warning
```

4. 建立一個個人識別碼檔案，這樣在每次重新啓動 Directory Server 時便不需要輸入憑證資料庫密碼。

```
C:\Program Files\Sun\MPS\alias > echo Internal (Software)
Token:<secret12> slapd-hostname-pin.txt
```

5. 以如下方式在 Directory Server 中啓用 SSL：
   a. 開啓主控台。
   b. 選擇「配置」標籤。
   c. 選擇「加密」標籤 (在右窗格中)。
   d. 爲此伺服器選擇「啓用 SSL」。
   e. 選擇使用此加密系列：RSA。
   f. 按一下「儲存」再按兩次「確定」。
   g. 選擇「網路」標籤。
   h. 更新「安全通訊埠」欄位。如果在與 Active Directory 相同的電腦上執行，通訊埠必須從 636 改爲一個未使用的通訊埠，否則 Directory Server 將無法啓動。
   i. 按一下「儲存」，再按「是」，然後按「確定」。
   j. 選擇「工作」標籤 (位於頂部)。
   k. 按一下「重新啓動 Directory Server」，然後按一下「是」。

從 Directory Server 憑證資料庫擷取 CA 憑證

確定您已經在 Directory Server 中啓用 SSL。爲了將 Directory Server 憑證匯出到臨時檔案，以便於您將其匯入到 Directory Server 連接器的憑證資料庫中，請發出下列指令：

```
C:\Program Files\Sun\MPS\shared\bin\certutil.exe -L -d . -P slapd-hostname-
-n server-cert -a > C:\s-cert.txt
```

這些範例於伺服器根下第一層目錄 `alias` 中執行。否則，Directory Server 將找不到憑證資料庫。

在 Active Directory 連接器中啓用 SSL

Identity Synchronization for Windows 會*自動*透過 SSL 擷取 Active Directory SSL 憑證，然後使用您爲連接器提供的憑證將這些 Active Directory SSL 憑證匯入該連接器的憑證資料庫中。

不過，如果發生錯誤 (例如，憑證無效或找不到 SSL 憑證)，您可擷取一個 Active Directory CA 憑證並將其加入連接器的憑證資料庫中。請參閱以下各節的說明：

- 第 296 頁上的「擷取 Active Directory 憑證」
- 第 299 頁上的「將 Active Directory 憑證加入連接器的憑證資料庫中」

擷取 Active Directory 憑證

如果發生錯誤，您可按照下列各節所述之方式，使用 `certutil` (Windows 2000/2003 隨附的一個程式) 或 LDAP 來擷取一個 Active Directory 憑證。

附註 本節所討論的 `certutil` 指令與 Directory Server 所隨附並在本手冊前面所述之 `certutil` 指令並*不*相同。

使用 Window 的 certutil

若要使用 `certutil` 程式擷取 Active Directory 憑證，請：

1. 從 Active Directory 電腦執行下列指令，以匯出憑證。

   ```
   C:\>certutil -ca.cert cacert.bin
   ```

2. 接著可以將檔案 `cacert.bin` 匯入到憑證資料庫中。

使用 LDAP

若要使用 LDAP 擷取 Active Directory 憑證，請：

1. 針對 Active Directory 執行下列搜尋：

   ```
   ldapsearch -h <CR-hostname> -D <administrator_DN> -w
   <administrator_password> -b
   "cn=configuration,dc=put,dc=your,dc=domain,dc=here"
   "cacertificate=*"
   ```

   其中 <*administrator_DN*> 可能類似於：

   ```
   cn=administrator,cn=users,dc=put,dc=your,dc=domain,dc=here
   ```

   在本範例中，網域名稱爲：<*put.your.domain.name.here*>。

   有數個項目會符合搜尋篩選條件。您可能需要其 DN 中使用 `cn=Certification Authorities, cn=Public Key Services` 的項目。

2. 開啓文字編輯器並剪下第一個 CA 憑證屬性的第一個值 (必須是 base64 編碼的文字區塊)。將該值 (文字區塊) 貼到文字編輯器中 (僅限於值)。編輯內容，使每一行都不以空格開頭。

3. 在第一行前加上 -----BEGIN CERTIFICATE-----，在最後一行後加上 -----END CERTIFICATE-----。請參閱以下範例：

```
-----BEGIN CERTIFICATE-----

MIIDvjCCA2igAwIBAgIQDgoyk+Tu14NGoQnxhmNHLjANBgkqhkiG9w0BAQUFA
DCBjjEeMBwGCSqGSIb3DQEJARYPYmVydG9sZEBzdW4uY29tMQswCQYDVQQGEwJVUzELMAkG
A1UECBMCVFgxDzANBgNVBAcTBkF1c3RpbjEZMBcGA1UEChMQU3VuIE1pY3Jvc3lzdGVtczE
QMA4GA1UECxMHaVBsYW5ldDEUMBIGA1UEAxMLUmVzdGF1cmFudHMwHhcNMDIwMTExMDA1ND
A5WhcNMTIwMTExMDA1OTQ2WjCBjjEeMBwGCSqGSIb3DQEJARYPYmVydG9sZEBzdW4uY29tM
QswCQYDVQQGEwJVUELMAkGA1UECBMCVFgxDzANBgNVBAcTBkF1c3RpbjEZMBcGA1UEChMQU
3VuIE1pY3Jvc3lzdGVtczEQMA4GA1UECxMHaVBsYW5ldDEUMBIGA1UEAxMLUmVzdGF1cmFu
dHMwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAyekZa8gwwhw3rLK3eV/12St1DVUsg31LOu3
CnB8cMHQZXlgiUgtQ0hm2kpZ4nEhwCAHhFLD3iIhIP4BGWQFjcwIDAQABo4IBnjCCAZowEw
YJKwYBBAGCNxQCBAYeBABDAEEwCwYDVR0PBAQDAgFGMA8GA1UdEwEB/wQFMAMBAf8wHQYDV
R0OBBYEFJ5Bgt6Oypq7T8Oykw4LH6ws2d/IMIIBMgYDVR0fBIIBKTCCASUwgdOggdCggc2G
gcpsZGFwOi8vL0NOPVJlc3RhdXJhbnRzLENOPWRvd2l0Y2hlcixDTj1DRFAsQ049UHVibGl
jJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049Q29uZmlndXJhdGlvbixEQz1yZX
N0YXVyYW50cyxEQz1jZW50cmFsLERDPXN1bixEQz1jb20/Y2VydGlmaWNhdGVSZXZvY2F0a
W9uTGlzdD9iYXNlP29iamVjdGNsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50ME2gS6BJhkdo
dHRwOi8vZG93aXRjaGVyLnJlc3RhdXJhbnRzLmNlbnRyYWwuc3VuLmNvbS9DZXJ0RW5yb2x
sL1Jlc3RhdXJhbnRzLmNybDAQBgkrBgEEAYI3FQEEAwIBADANBgkqhkiG9w0BAQUFAANBAL
5R9R+ONDdVHWu/5Sd9Tn9dpxN8oegjS88ztv1HD6XSTDzGTuaaVebSZV3I+ghSInsgQbH0g
W4fGRwaI BvePI4=

-----END CERTIFICATE-----
```

4. 將該憑證儲存至檔案中 (例如 ad-cert.txt)。

5. 接著可以將該檔案 (例如 ad-cert.txt) 匯入到憑證資料庫中。請接著進入下一節 「將 Active Directory 憑證加入連接器的憑證資料庫中」，瞭解操作說明。

將 Active Directory 憑證加入連接器的憑證資料庫中

只有在安裝連接器後針對 Active Directory 連接器啓用了 SSL，或在安裝時提供了無效憑證的情況下，才需要使用此程序。

1. 在安裝了 Active Directory 連接器的電腦中，停止 Identity Synchronization for Windows 服務 / 常駐程式。
2. 使用以下方法之一，擷取 Active Directory CA 憑證：
   - 第 296 頁上的「使用 Window 的 certutil」
   - 第 297 頁上的「使用 LDAP」
3. 假設 Active Directory 連接器具有連接器 ID CNN101 (請參閱 `logs/central/error.log` 以獲得從連接器 ID 到對它所管理的目錄來源的對映)，然後轉至安裝有該連接器之電腦中相應的憑證資料庫目錄，並匯入憑證檔案：
   - 如果是使用 `certutil` 擷取憑證，請輸入：

     ```
     C:\\Program Files\Sun\MPS\shared\bin\certutil.exe -A -d . -n
     ad-ca-cert -t C,, -i \cacert.bin
     ```

   - 如果是使用 LDAP 擷取憑證，請輸入：

     ```
     C:\\Program Files\Sun\MPS\shared\bin\certutil.exe -A -d . -n
     ad-ca-cert -t C,, -a -i \ad-cert.txt
     ```

4. 重新啓動 Identity Synchronization for Windows 服務 / 常駐程式。

附註 由於 Directory Server `certutil.exe` 是在您安裝 Directory Server 5 2004Q2 時自動安裝的，因此如果安裝連接器的電腦上沒有 Directory Server 時，您無法將 CA 憑證加入該連接器中。

至少，您必須在安裝 Active Directory 連接器的伺服器上，安裝來自 Directory Server 5 2004Q2 套裝軟體的 Sun Java System 伺服器基礎程式庫以及 Sun Java System 伺服器基礎系統程式庫。(您不需要安裝 Administration Server 或 Directory Server 元件。)

此外，務必從主控台選擇 JRE 子元件 (以確保您可以解除安裝)。

新增 Active Directory 憑證到 Directory Server

執行這些步驟，將 Active Directory CA 憑證新增到 Directory Server 憑證資料庫。

附註 確定您已經在 Directory Server 中啓用 SSL。

1. 使用以下方法之一，擷取 Active Directory CA 憑證：
   - 第 296 頁上的「使用 Window 的 certutil」
   - 第 297 頁上的「使用 LDAP」
2. 停止 Directory Server。
3. 在安裝有 Directory Server 的電腦上，按如下方法匯入 Active Directory CA 憑證：
   - 如果是使用 `certutil` 擷取憑證，請輸入：

     ```
     C:\\Program Files\Sun\MPS\shared\bin\certutil.exe -A -d . -P
     slapd-hostname- -n ad-ca-cert -t C,, -i \cacert.bin
     ```

   - 如果是使用 LDAP 擷取憑證，請輸入：

     ```
     C:\\Program Files\Sun\MPS\shared\bin\certutil.exe -A -d . -P
     slapd-hostname- -n ad-ca-cert -t C,, -a -i \ad-cert.txt
     ```

4. 啓動 Directory Server。

新增 Directory Server 憑證到 Directory Server 連接器

如果您在 Directory Server 外掛程式與 Active Directory 之間啓用 SSL 通訊功能，則必須將 Active Directory CA 憑證加入每個 Directory Server 主伺服器的憑證資料庫中。使用以下步驟：

1. 在安裝了 Directory Server 連接器的電腦中，停止 Identity Synchronization for Windows 服務 / 常駐程式。
2. 擷取 Directory Server CA 憑證。

3. 假設 Directory Server 連接器包含連接器 ID CNN100 (請參閱 `logs/example/error.log` 以獲得從連接器 ID 到對它所管理的目錄來源的對映)，然後轉至安裝有該連接器之電腦中相應的憑證資料庫目錄，並匯入 `cacert.bin` 檔案：

```
C:\Program Files\Sun\MPS\shared\bin\certutil.exe -A -d . -n ds-cert -t
C,, -i C:\s-cert.txt
```

附註 如果憑證是以 ASCII 格式取得的，請新增一個「`-a`」引數到 `certutil` 指令行，以表示它是 ASCII 格式而非二進位格式。

4. 重新啓動 Identity Synchronization for Windows 服務 / 常駐程式。

附錄

使用 Identity Synchronization for Windows 指令行公用程式

Identity Synchronization for Windows 可讓您從指令行執行各種工作。本附錄解釋如何透過 Identity Synchronization for Windows 指令行公用程式來執行不同工作。內容分作以下各節：

共用功能

Identity Synchronization for Windows 指令行公用程式共用下列功能：

共用引數

本節描述大部分指令行公用程式共用的引數 (選項)。內容分作以下各表：

- 表格 A-1 所有子指令共用的引數：介紹下列所有 `idsync` 子指令 (*除了 prepds*) 和遷移工具共用的引數。

```
-D <bind-DN> -w <bind-password | -> [-h <Configuration Directory-hostname>]
[-p <Configuration Directory-port-no>] [-s <rootsuffix>] [-Z] [-P <cert-db-path>]
[-m <secmod-db-path>]
```

附註

括號 [ ] 代表選擇性引數。

Identity Synchronization for Windows 安裝程式會根據您在安裝期間提供的資訊自動寫入預設值到 `-h`、`-p`、`-D` 和 `-s` 引數。不過，您可以在指令行指定不同的值覆寫預設值。

爲了支援多位元組字元，Identity Synchronization for Windows 在指令行介面 (CLI) 環境檔案中以 base64 來編碼 `-s <rootsuffix>` 和 `-D <bind-DN>` 的預設值。不應變更根字尾預設值。可在指令行上覆寫連結 DN 的預設值，或以 CLI 環境檔案中的相應 base64 編碼值來更新 DN 的預設值。

- 表格 A-2 所有子指令共用的 SSL 相關引數：介紹一些選擇性引數，用於提供關於使用安全套接層 (SSL) 安全存取 Configuration Directory Server 的資訊。這些引數也對所有的 `idsync` 子指令和遷移工具共用。

- 表格 A-3 配置目錄引數：介紹與配置目錄相關的引數。這些引數對兩個以上的 idsync 子指令和遷移工具共用。

附註 特定子指令的專有引數將會在相關的子指令章節中說明。

表格 A-1 所有子指令共用的引數

引數	描述
-h <*Configuration Directory-hostname*>	指定配置目錄主機名稱。本引數預設爲安裝核心期間指定的值。
-p <*Configuration Directory-port-no*>	指定配置目錄 LDAP 通訊埠埠號。
-D <*bind-DN*>	指定配置目錄連結辨別名稱 (DN)。本引數預設爲安裝核心期間指定的值。
-w <*bind-password* | ->	指定配置目錄連結密碼。- 值從標準輸入 (STDIN) 讀取密碼。
-s <*rootsuffix*>	指定配置目錄根字尾。其中根字尾是一個辨別名稱，例如 dc=example,dc=com。本引數預設爲安裝核心期間指定的值。
-q <*configuration_password* | ->	指定配置密碼。- 值代表將從標準輸入 (STDIN) 讀取密碼。 所有子指令的這個引數均爲*必要引數*，但 prepds 除外。

表格 A-2 所有子指令共用的 SSL 相關引數

引數	描述
-Z	指定用來提供安全通訊的 SSL。當連線至配置目錄存取指令行介面或喜好的 / 輔助的 Directory Server 時，提供基於憑證的用戶端驗證。
-P <*cert-db-path*>	指定用戶端的憑證資料庫路徑及檔案名稱。 此憑證資料庫必須包含用來簽署 Directory Server 憑證資料庫的 CA 憑證。 如果您指定 -Z 但未使用 -P，<*cert-db-path*> 預設爲 <*current-working-directory*>/cert8.db。 **附註**：如果 Identity Synchronization for Windows 沒有在指定目錄中找到憑證資料庫，程式會在該目錄中建立一個 *empty* 資料庫，其由三個檔案構成：cert8.db、key3.db 及 secmod.db。
-m <*secmod-db-path*>	指定安全模組資料庫的路徑。例如： /var/Sun/MPS/slapd-<*serverID*>/secmod.db 唯有當安全模組資料庫與憑證資料庫本身所在的目錄不同時，才需指定此引數。

表格 A-3 配置目錄引數

引數	描述
`-a` <*ldap_filter*> 與 `forcepwchg` 和 `resync` 子指令配合使用	指定在從來源 SUL 擷取使用者時要使用的 LDAP 篩選器，並讓作業在確定使用者是否歸於指定的 SUL 之前，從目錄來源擷取使用者焦點子集。
`-f` <*filename*> 與 `export10cnf`、`importcnf` 和 `resync` 子指令配合使用	指定 XML 配置文件的檔案名稱。
`-n` 與 `forcepwchg`、`importcnf` 和 `resetconn` 子指令配合使用	在安全模式下執行動作，以便預覽作業效果，而又不會造成實際的變更。

輸入密碼

在需要密碼引數之處 (例如 `-w` <*bind-password*> 或 `-q` <*configuration_password*>)，您可以使用「`-`」引數告訴密碼程式從 `STDIN` 讀取密碼。

如果您對多個密碼選項使用「`-`」值，`idsync` 將根據引數順序提示您輸入密碼。

在此情形下，程式先提示您輸入 <*bind-password*>，然後再提示輸入 <*configuration-password*>。

取得說明

您可以在指令主控台中使用下列指令之一顯示關於 `idsync` 或其任何子指令的用法資訊：

- **`-help`**
- **`--help`**
- **`-?`**

若要獲得用法資訊

- 對於 `idsync` (包含有效子指令的清單)，在指令提示符號處鍵入上述說明選項之一，並按一下 Return 鍵。
- 對於子指令，在指令提示符號處鍵入跟有說明選項的子指令，並按一下 Return 鍵。

使用 idsync 指令

使用 idsync 指令和子指令執行 Identity Synchronization for Windows 指令行公用程式。

附註 idsync 指令可在將引數傳送到 Directory Server 前，將所有的 DN 值引數 (例如連結 DN 或字尾名稱) 從指定給該視窗的字元集轉換爲 UTF-8。

在字尾名稱中不要使用反斜線作爲退出字元。

若要在 Solaris 上指定 UTF-8 字元，您的終端機視窗必須要有基於 UTF-8 的語言環境。請確定環境變數的 LC_CTYPE 和 LANG 的設定正確。

您可以使用下列方法之一執行帶子指令的 idsync 指令 (除非另有特別指示)：

- **從 Solaris：**
  a. 開啓終端機視窗並使用 **cd** 指令進入 /opt/SUNWisw/bin 目錄。
  b. 鍵入如下帶有一個子指令的 idsync 指令

     idsync <*subcommand*>

- **從 Windows：**
  a. 開啓指令視窗並使用 **cd** 指令進入 <*install_path*>\isw-<*hostname*>\bin 目錄。
  b. 鍵入如下帶有一個子指令的 idsync 指令

     idsync <*subcommand*>

表格 A-4 列出所有的 idsync 公用程式子指令及其用途：

表格 A-4 idsync 子指令快速參照

子指令	用途
certinfo	根據您的配置和 SSL 設定值顯示憑證資訊。(請參閱第 310 頁上的「使用 certinfo」)
changepw	變更 Identity Synchronization for Windows 配置密碼 (請參閱第 311 頁上的「使用 changepw」)
importcnf	將匯出的 Identity Synchronization for Windows 1.0 版 XML 配置文件匯入 (請參閱第 312 頁上的「使用 importcnf」)
prepds	準備 Sun Java System Directory Server 來源，以供 Identity Synchronization for Windows 使用 (請參閱第 313 頁上的「使用 prepds」)

表格 A-4 idsync 子指令快速參照

子指令	用途
printstat	顯示完成安裝 / 配置過程必須執行之步驟的清單。同時提供安裝的連接器、系統管理員和 Message Queue 的狀態 (請參閱 第 317 頁上的「使用 printstat」)
resetconn	將配置目錄中的連接器狀態重設爲*未安裝* (請參閱第 318 頁上的「使用 resetconn」)
resync	連結及重新同步化現有使用者並在安裝過程中預先填寫目錄 (請參閱第 319 頁上的「使用 resync」)
startsync	啓動同步化 (請參閱第 321 頁上的「使用 startsync」)
stopsync	停止同步化 (請參閱第 322 頁上的「使用 stopsync」)

使用 certinfo

您可以根據您的配置和 SSL 設定值使用 certinfo 子指令顯示憑證資訊。此類資訊可協助您決定針對每個連接器和 / 或 Directory Server 外掛程式必須將哪些憑證加入憑證資料庫。

若要顯示憑證資訊，開啓終端機視窗 (或指令視窗) 並鍵入如下 **idsync certinfo** 指令：

```
idsync certinfo [<bind-DN>] -w <bind-password | -> [-h <Configuration
Directory-hostname>] [-p <Configuration Directory-port-no>] [-s <rootsuffix>] -q
<configuration_password> [-Z] [-P <cert-db-path>] [-m <secmod-db-path>]
```

附註 因爲 certinfo 子指令無法存取連接器和 Directory Server 的憑證資料庫，所以它列出的某些必要步驟可能已經執行過。

例如：

```
idsync certinfo -w <admin-password> -q <configuration-password>
```

附註 關於 certinfo 引數的詳細資訊，請參閱第 306 頁上的「共用引數」。

使用 changepw

您可以使用 changepw 子指令變更 Identity Synchronization for Windows 配置密碼。

若要變更 Identity Synchronization for Windows 的配置密碼：

1. 停止所有 Identity Synchronization for Windows 程序 (例如，系統管理員、中央記錄程式、連接器、主控台、安裝程式 / 解除安裝程式)。
2. 停止所有程序後，將配置目錄匯出到 ldif 來備份 ou=Services 目錄樹。
3. 鍵入如下 **idsync changepw** 指令：

```
idsync changepw [-D <bind-DN>] -w <bind-password | -> [-h <Configuration
Directory-hostname>] [-p <Configuration Directory-port-no>] [-s <rootsuffix>]
-q <configuration_password> [-Z] [-P <cert-db-path>] [-m <secmod-db-path>]
-b <new password | - > [-y]
```

例如：

idsync changepw -w *<admin password>* -q *<old config password>* -b -q *<new config password>*

下列引數是 changepw 專用的：

表格 A-5 idsync changepw 引數

引數	描述
-b *<password>*	指定一個新的配置密碼。- 值從標準輸入 (STDIN) 讀取密碼。
[-y]	不提示使用者確認指令。

附註 關於其他 changepw 引數的詳細資訊，請參閱第 306 頁上的「共用引數」。

4. 回應在終端機視窗中顯示的訊息。例如，

```
Are you sure that want to change the configuration password (y/n)? yes
Before restarting the system - you must edit the
$PSWHOME/resources/SystemManagerBootParams.cfg file and change the
'deploymentPassword' to the new value.

SUCCESS
```

5. 您必須在重新啓動系統前修改 SystemManagerBootParams.cfg 檔案。

   $PSWHOME\resources （其中 $PSWHOME 是 *<isw-installation directory>*）中的 SystemManagerBootParams.cfg 檔案包含系統管理員用於連接配置目錄的配置密碼。

   例如，如下變更密碼值：

   變更前：<*Parameter name="manager.configReg.deploymentPassword" value="***oldpassword**"/>

   變更後：<*Parameter name="manager.configReg.deploymentPassword" value="***newpassword**"/>

6. 如果程式報告有任何錯誤，請從步驟 2 使用 ldif 還原配置目錄，然後再試一次。最有可能的錯誤原因是在密碼變更期間主控配置目錄的 Directory Server 無法使用。

使用 importcnf

注意 *只有在從* Identity Synchronization for Windows 1.0 或 1.0 SP1 版遷移到 1 2004Q3 版時，才使用 idsync importcnf。

安裝核心元件之後 (第 3 章，「安裝核心程式」)，使用 idsync importcnf 子指令將匯出的 Identity Synchronization for Windows 1.0 版 (SP1) XML 配置檔案 (包含核心元件配置資訊) 匯入。

若要匯入 1.0 版的 XML 配置檔案，請開啓終端機視窗 (或指令視窗) 並鍵入如下 **idsync importcnf** 指令：

```
idsync importcnf [-D <bind-DN>] -w <bind-password | -> [-h <Configuration
Directory-hostname>] [-p <Configuration Directory-port-no>] [-s <rootsuffix>] -q
<configuration_password> [-Z] [-P <cert-db-path>] [-m <secmod-db-path>] -f <filename>
[-n]
```

例如：

```
idsync importcnf -w <admin_password> -q <configuration_password> -f "MyConfig.cfg"
```

下列引數是 importcnf 專用的：

表格 A-6 idsync importcnf 引數

引數	描述
-f <*filename*>	指定 XML 配置文件的名稱。
-n	在安全模式下執行動作，以便預覽作業效果，而又不會造成實際的變更。

附註 關於其他 importcnf 引數的詳細資訊，請參閱第 306 頁上的「共用引數」。

在匯入 1.0 版的 XML 配置檔案後，您必須對爲同步化配置的所有 Directory Server 來源執行 prepds，(請參閱第 313 頁上的「使用 prepds」) 然後才可安裝 Identity Synchronization for Windows 連接器和子元件。

使用 prepds

使用主控台或 prepds 子指令可準備 Sun Java System Directory Server 來源供 Identity Synchronization for Windows 使用。必須先執行 prepds 才能安裝 Directory Server 連接器。

執行 idsync prepds 子指令後，適用的 ACI 會套用到 cn=changelog 項目，其爲 Retro-Changelog 資料庫的根節點。

- 如果您準備*喜好的主要* Directory Server 供 Identity Synchronization for Windows 使用，則必須提供 *Directory Manager* 憑證。

目錄管理員使用者是 Directory Server 上的特殊使用者，其具有 Directory Server 實例中完整的權限。(ACI 不適用於目錄管理員使用者。)

例如，只有目錄管理員可以設定 Retro-Changelog 資料庫的存取控制，這是對於喜好的主要伺服器 Identity Synchronization for Windows 需要目錄管理員憑證的原因之一。

附註 如果您因爲任何原因而爲喜好的 Sun 目錄來源重建 Retro-Changelog 資料庫，則預設的存取控制設定將不允許 Directory Server 連接器讀取資料庫內容。

若要還原 Retro-Changelog 資料庫之存取控制設定，請執行 `idsync prepds`，或在「主控台」中選取適當的 Sun 目錄來源，然後按一下「備妥 Directory Server」按鈕。

附註 您可配置系統，使其在超過一段指定時間後自動移除 (或*調整*) Change-log 項目。從指令行中，修改 `cn=Retro Changelog Plugin, cn=plugins, cn=config` 內的 `nsslapd-changelogmaxage` 配置屬性：

`nsslapd-changelogmaxage:` *IntegerTimeunit*

此處：

- ***Integer*** 是一個數字
- ***Timeunit*** 是秒數 (顯示爲 s)、分鐘數 (顯示爲 m)、時數 (顯示爲 h)、天數 (顯示爲 d)、週數 (顯示爲 w)。(Integer 與 Timeunit 變數之間不得有空格。)

例如，`nsslapd-changelogmaxage: 2d`

有關詳細資訊，請參閱《Sun Java™ System Directory Server 5 2004Q2 管理指南》中的〈管理複製〉一章。

- 您可以使用*管理*憑證準備一個*輔助*伺服器。

附註 在執行 idsync prepds *之前*，務必規劃您的 Identity Synchronization for Windows 配置，因爲您必須知道將使用哪些主機和字尾。

對已安裝、配置並同步化 Directory Server 連接器和外掛程式的 Directory Server 字尾執行 idsync prepds 會產生一個訊息，要求您安裝 Directory Server 連接器。請忽略此訊息。

若要準備 Sun Java System Directory Server 來源，請開啓終端機視窗 (或指令視窗) 並鍵入如下 **idsync prepds** 指令：

```
idsync prepds [-D <bind-DN>] -w <bind-password | -> [-h <preferred host>]
[-p <preferred-port>] [-s <database-suffix>] [-Z] [-P <cert-db-path>]
[-m <secmod-db-path>] [-j <secondary_host>] [-r <secondary-port>] [-E <admin DN of
secondary host>] [-u <password for secondary host | ->] [-x]
```

例如：

```
idsync prepds -D "cn=Directory Manager" -w <preferred master password> -h
<preferred-host> -p 389 -s dc=example,dc=com -j "secondary host" -r 389 -E
"cn=Administrator" -u <secondary master password> -s dc=example,dc=com
```

附註 只重新定義 prepds 子指令的 -h、-p、-D、-w 和 -s 引數 (詳見下表)。此外，-q 引數不適用。

表格 A-7 介紹 idsync prepds 所專用的引數：

表格 A-7 prepds 引數

引數	描述
-h <*name*>	指定作爲喜好主機之 Directory Server 實例的 DNS 名稱。
-p <*port*>	指定作爲喜好主機之 Directory Server 實例的通訊埠埠號。(*預設值爲 389*。)
-j <*name*> (*可選*)	指定作爲輔助主機之 Directory Server 實例的 DNS 名稱 (適用於 Sun Java System Directory Server 5 2004Q2 多主伺服器複製 (MMR) 環境)。
-r <*port*> (*可選*)	指定作爲輔助主機的 Directory Server 所使用的通訊埠 (適用於 Sun Java System Directory Server 5 2004Q2 多主伺服器複製 (MMR) 環境)。(*預設值爲 389*。)

表格 A-7 prepds 引數 *(續上頁)*

引數	描述
-D <*dn*>	指定喜好主機之目錄管理員使用者的辨別名稱。
-w <*password*>	指定喜好主機之目錄管理員使用者的密碼。 - 值從標準輸入 (STDIN) 讀取密碼。
-E <*admin-DN*>	指定輔助主機之目錄管理員使用者的辨別名稱。
-u <*password*>	指定輔助主機之目錄管理員使用者的密碼。 - 值從標準輸入 (STDIN) 讀取密碼。
-s <*rootsuffix*>	指定根字尾供新增索引時使用 (將對根字尾同步化使用者)。 **附註**：喜好主機和輔助主機的資料庫名稱可能不同，但是子尾則相同。因此，程式可以找到每個主機的資料庫名稱並用來新增索引。
-x	不將 dspswuserlink 屬性的平等指數和存在指數加入資料庫中。

如果您在複製環境 (例如，您有喜好的主伺服器、輔助的主伺服器和兩個用戶伺服器) 中執行 idsync prepds，您只需要在喜好伺服器和輔助主伺服器執行 idsync prepds 一次。

若要執行 idsync prepds

1. 請確定 Directory Server 複製功能開啓並正在執行 (如果適用的話)。
2. 從主控台或指令行執行 idsync prepds 指令，例如：

```
idsync prepds -h M1.example.com -p 389 -j M2.example.com -r 389 . . .
```

執行 idsync prepds 指令完成下列作業：

- M1：
  - 啓用並延伸 RCL，以擷取更多屬性 (dspswuserlink 等等)

    RCL 只需要在 M1 上。
  - 延伸模式。
  - 用 ACI 新增 uid=pswconnector,<*suffix*> user。
  - 新增索引到 dspswuserlink 屬性，暫時使 Directory Server 處於唯讀模式直到索引完成。

    您可以稍後新增索引來避免停機，但是必須在安裝 Directory Server 連接器*之前*新增索引。

- 在 M2 上新增索引。

附註

- 複製動作可確保 Identity Synchronization for Windows 將模式資訊和 uid=pswconnector 從喜好主伺服器複製到輔助主伺服器和兩個用戶伺服器。
- 您必須安裝 Directory Server 連接器一次。您必須在*所有*目錄中安裝 Directory Server 外掛程式。
- 只需要在喜好和輔助主伺服器中建立索引。(複製不會將索引配置從喜好主伺服器推向輔助主伺服器。)

使用 printstat

您可以使用 printstat 子指令來：

- 顯示完成安裝和配置過程必須執行之剩餘步驟的清單
- 列印安裝的連接器、系統管理員和 Message Queue 的狀態

  可能的狀態設定包括：

  - **未安裝。**未安裝連接器。
  - **已安裝。**已安裝連接器，但是尚未準備好進行同步化，因爲還沒接收到運行時間配置。
  - **就緒。**連接器已準備好進行同步化，但尚未同步化任何物件。
  - **正在同步。**連接器正在同步化物件。

若要列印安裝的連接器、系統管理員和 Message Queue 的狀態，請開啓終端機視窗 (或指令視窗) 並輸入如下 **idsync printstat** 指令：

```
idsync printstat [-D <bind-DN>] -w <bind-password | -> [-h <Configuration
Directory-hostname>] [-p <Configuration Directory-port-no>] [-s <rootsuffix>]
-q <configuration_password> [-Z] [-P <cert-db-path>] [-m <secmod-db-path>]
```

例如：

```
idsync printstat -w <admin password> -q <configuration password>
```

附註 有關 printstat 引數的詳細資訊，請參閱第 306 頁上的「共用引數」。

使用 resetconn

您可以使用 resetconn 子指令將配置目錄中的連接器狀態重設爲*未安裝*。例如，如果硬體故障妨礙您解除安裝連接器，請使用 resetconn 將連接器的狀態變更爲未安裝，如此您即可重新安裝連接器。

注意 resetconn 子指令應只在硬體或解除安裝程式故障時使用。

若要從指令行重設連接器狀態，開啓終端機視窗 (或指令視窗) 並鍵入如下 **idsync resetconn** 指令：

```
idsync resetconn [-D <bind-DN>] -w <bind-password> | -> [-h <Configuration
Directory-hostname>] [-p <Configuration Directory-port-no>] [-s <rootsuffix>] -q
<configuration_password> [-Z] [-P <cert-db-path>] [-m <secmod-db-path>] -e
<directory-source-name> [-n]
```

例如：

```
idsync resetconn -w <admin password> -q <configuration_password> -e
"dc=example,dc=com"
```

表格 A-8 介紹 resetconn 所專用的引數：

表格 A-8 idsync resetconn 引數

引數	描述
-e <*dir-source*>	指定所要重設的目錄來源名稱。
-n	在安全模式下執行動作，以便預覽作業效果，而又不會造成實際的變更。

附註 `idsync printstat` 可用來尋找目錄來源名稱。

有關 `resetconn` 引數的詳細資訊，請參閱第 306 頁上的「共用引數」。

使用 resync

您可使用 `resync` 子指令來驅動現有使用者的部署。這項指令使用管理者指定的比對規則來

- 連結現有的項目
- 將遠端目錄的內容填入空的目錄中
- 批量同步化兩個現有使用者個體群之間的屬性值

附註 有關連結與同步化使用者的詳細資訊，請參閱第 177 頁上的「現有使用者同步化」。

若要重新同步化現有使用者並預先填寫目錄，請開啓終端機視窗 (或指令視窗) 並鍵入如下 **`idsync resync`** 指令：

```
idsync resync [-D <bind-DN>] -w <bind-password> | -> [-h <Configuration
Directory-hostname>] [-p <Configuration Directory-port-no>] [-s <rootsuffix>] -q
<configuration_password> [-Z] [-P <cert-db-path>] [-m <secmod-db-path>] [-n] [-f <xml
filename for linking>] [-k] [-a <ldap-filter>] [-l <sul-to-sync>] [-o Sun | Windows]
[-c] [-x] [-u] [-i ALL_USERS | NEW_USERS | NEW_LINKED_USERS]
```

例如：

```
idsync resync -w <admin password> -q <configuration_password>
```

表格 A-9 介紹 resync 所專用的引數：

表格 A-9 idsync resync 用法

引數	涵義
-f <*filename*>	使用 Identity Synchronization for Windows 提供的任一指定 XML 配置檔案，在未連結的使用者項目之間建立連結 (請參閱附錄 B，「LinkUsers XML 文件範例」。)
-k	僅在未連結的使用者之間建立連結 (不建立使用者或修改現有使用者)
-a <*ldap-filter*>	指定一個 LDAP 篩選器以限制要同步化的項目 該篩選器將套用於重新同步化作業的來源。 例如，如果指定 idsync resync -o Sun -a "uid=*"，則所有具備 uid 屬性的 Directory Server 使用者都將同步化到 Active Directory。
-l <*sul-to-sync*>	指定要重新同步化的個別同步化使用者清單 (SUL) **附註**：您可以指定多個 SUL ID 來重新同步化多個 SUL，或是如果您沒有指定任何 SUL ID，程式將重新同步化您全部的 SUL。
-o (Sun | Windows)	指定重新同步化作業的來源 • **Sun**：將 Windows 項目的屬性值設定爲 Sun Java System Directory Server 目錄來源項目中的對應屬性值。 • **Windows**：將 Sun Java System Directory Server 項目的屬性值設定爲 Windows 目錄來源項目中的對應屬性值。 (*預設值爲 Windows*。)
-c	如果在目標目錄來源沒有找到對應使用者，則自動建立一個使用者項目 • 爲在 Active Directory 或 Windows NT 中建立的使用者隨機產生一個密碼 • 除非指定了 -i 選項，否則自動爲 Directory Server 中建立的使用者建立一個特殊密碼值 ((PSWSYNC)***INVALID PASSWORD***)
-i (ALL_USERS | NEW_USERS | NEW_LINKED_USERS)	重設 Sun 目錄來源中同步化的使用者項目的密碼，當下一次需要使用者密碼時強制對目前網域中的這些使用者進行密碼同步化。 • **ALL_USERS**：強制對所有同步化的使用者執行隨需密碼同步化 • **NEW_USERS**：只強制對新建立的使用者執行隨需密碼同步化 • **NEW_LINKED_USERS**：強制對所有新建立和新連結的使用者執行隨需密碼同步化
-u	只更新物件快取。不修改任何項目。 此引數只會更新 Windows 目錄來源的使用者項目之本機快取，如此可避免在 Directory Server 中建立既存的 Windows 使用者。如果使用此引數，Windows 使用者項目便不會與 Directory Server 使用者項目實現同步。此引數只有在 resync 來源爲 Windows 時有效。
-x	刪除所有不符合來源項目的目標使用者項目。
-n	在安全模式下執行動作，以便預覽作業效果，而又不會造成實際的變更。

附註

- 執行不帶引數的 idsync resync 可檢視用法說明。
- 有關 resync 引數的詳細資訊，請參閱第 306 頁上的「共用引數」。
- 有關重新同步化現有使用者的詳細資訊，請參閱第 177 頁上的「現有使用者同步化」。

執行 resync 後，請檢查中央 ¾]Æ÷§È ª x 中的 resync.log 檔案。如果產生錯誤，請參閱第 9 章，「疑難排解」。

使用 startsync

您可以從指令行使用 startsync 子指令啓動同步化。

若要啓動同步化，開啓終端機視窗 (或指令視窗) 並鍵入如下 **idsync startsync** 指令：

```
idsync startsync [-D <bind-DN>] -w <bind-password | -> [-h <Configuration
Directory-hostname>] [-p <Configuration Directory-port-no>] [-s <rootsuffix>] -q
<configuration_password> [-Z] [-P <cert-db-path>] [-m <secmod-db-path>]
```

例如：

```
idsync startsync -w <admin password> -q <configuration_password>
```

表格 A-10 介紹 startsync 所專用的引數：

表格 A-10 idsync startsync 引數

引數	描述
[-y]	不提示使用者確認指令。

附註 有關其他 startsync 引數的詳細資訊，請參閱第 306 頁上的「共用引數」。

使用 stopsync

您可以從指令行使用 stopsync 子指令停止同步化。

若要停止同步化，開啓終端機視窗 (或指令視窗) 並鍵入如下 **idsync stopsync** 指令：

```
idsync stopsync [-D <bind-DN>] -w <bind-password | -> [-h <Configuration
Directory-hostname>] [-p <Configuration Directory-port-no>] [-s <rootsuffix>] -q
<configuration_password> [-Z] [-P <cert-db-path>] [-m <secmod-db-path>]
```

例如：

```
idsync stopsync -w <admin password> -q <configuration_password>
```

附註 有關 stopsync 引數的詳細資訊，請參閱第 306 頁上的「共用引數」。

使用 forcepwchg 遷移公用程式

在遷移時變更其密碼的使用者將在 Windows NT 和 Directory Server 中有不同的密碼。您可以使用 `forcepwchg` 公用程式向 Identity Synchronization for Windows 1.0 版到 1 2004Q3 版的遷移程序期間變更其密碼的使用者要求密碼變更。

附註 `forcepwchg` 公用程式只在 Windows 套裝軟體中提供。

在使用 `forcepwchg` 之前，必須確認以下各項：

- 確定您未將 Directory Server 中的 7 位元核對外掛程式配置爲強制 `userpassword` 屬性實施 7 位元值。使用 Directory Server 主控台可達到此目的。
- 確定用於驗證的用戶端正確地將您所用語言環境的值轉譯爲 UTF-8。(例如，隨附於 Directory Server 的 `ldapsearch` 的 `-i` 選項)。

若要執行 `forcepwchg` 指令行公用程式，

1. 開啓「指令提示符號」視窗並使用 cd 指令進入執行遷移之主機上的 Windows `migration` 目錄。(Identity Synchronization for Windows 1.0 NT 元件 (連接器、變更偵測器 DLL、密碼篩選器 DLL) 必須安裝在 PDC 主機上。)
2. 從 `migration` 目錄，鍵入

```
java -jar forcepwchg.jar [-n] [-a] [-t <time_specification>]
```

例如，

```
forcepwchg.jar -n -a
forcepwchg.jar -t 33m
```

表格 A-11 介紹 forcepwchg 所專用的引數：

表格 A-11 forcepwchg 引數

選項	描述
-n	指定*預覽模式*。 在預覽模式中，公用程式會列印出所有一般使用者的名稱，除了： • 內建帳號 (Administrator 和 Guest，如果指定 -a 引數)。 • 在使用 -t 引數指定的時間段變更了密碼的使用者。 在預覽模式中，任何使用者都可以執行 forcepwchg。 在非預覽模式中，只有管理員可以執行 forcepwchg。
-a	要求所有使用者 (除了 Administrator 和 Guest) 變更其密碼。 如果您使用 -t 引數則無法使用此引數。
-t <*time_specification*>	強制過去 <*time specification*> 內變更了密碼的使用者變更其密碼。其中 <*time specification*> 可以有下列格式： • **<***number***>**：秒數 (例如，-t 30) • **<***number***>m**：分鐘數 (例如，-t 25m) • **<***number***>h**：小時數 (例如，-t 6h) 例如，如果您指定 forcepwchg -t 6h，所有在前六小時內變更密碼的使用者將被要求重新變更其密碼。
-?	列印用法資訊。

附註 有關使用 forcepwchg 的詳細資訊，請參閱第 198 頁上的「強制在 Windows NT 上變更密碼」。

LinkUsers XML 文件範例

本附錄提供了兩個 XML 配置文件的範例，您可將其與 `idsync resync` 子指令配合使用，連結您的部署中現有的使用者。

下列兩個檔案均可從您安裝核心元件的 `samples1` 子目錄下取得：

- 第 326 頁上的「範例 1：linkusers-simple.cfg」(常見的簡易配置範例)
- 第 327 頁上的「範例 2：linkusers.cfg」(較複雜的配置範例，充分展示了指定連結條件的強大功能)

您可修改這些範例，使其適用於您的環境。這兩個檔案中包含的註解可以說明如何修改範例，來連結您的使用者 (包括如何連結多個 SUL 中的使用者)。

範例 1：linkusers-simple.cfg

```
<!--

    Copyright 2004 Sun Microsystems, Inc. All rights reserved

    Use is subject to license terms.

-->

<!--

    This xml file is used to link Windows and Sun Directory Server users from the command
    line.  It is passed to the 'idsync resync' script as the -f option.

    This is a simple file that links users in the SUL1 synchronization user list that have
    the same login name, that is the Directory Server uid attribute matches the Active
    Directory samaccountname attribute.

    For more complex matching rules, see the linkusers.cfg sample.

-->

<UserLinkingOperationList>

    <UserLinkingOperation parent.attr="UserLinkingOperation" sulid="SUL1">

        <UserMatchingCriteria parent.attr="UserMatchingCriteria">

            <AttributeMap parent.attr="AttributeMap">

                <AttributeDescription parent.attr="SunAttribute" name="uid"/>

                <AttributeDescription parent.attr="WindowsAttribute" name="samaccountname"/>

            </AttributeMap>

        </UserMatchingCriteria>

    </UserLinkingOperation>

</UserLinkingOperationList>
```

範例 2：linkusers.cfg

```
<?xml version =”1.0” encoding=”UTF-8”?>
<!--
    Copyright 2004 Sun Microsystems, Inc. All rights reserved
    Use is subject to license terms.

-->

<!--

    This xml file is used to link Windows and Sun Directory Server users from
    the command line.  It is passed to the 'idsync resync' script as the -f option.

-->

<!--

    The following parameters allowLinkingOutOfScope: if true, then Windows users can be
    linked to Sun Directory Server users that are outside of the users' Synchronization
    User List. Default is false.

-->
<UserLinkingOperationList allowLinkingOutOfScope="false">

<!--
    UserLinkingOperation encapsulates the configuration of a single SUL to link.
    It includes the SUL ID and a list of attributes to match.
    A separate UserLinkingOperation must be specified for each SUL being linked.

-->
<UserLinkingOperation parent.attr="UserLinkingOperation" sulid="SUL1">

<!--
    UserMatchingCriteria encapsulates a list of attributes that must match for a user
    to be linked. -->

<!--
    For two users to match using this UserMatchingCriteria, they must have the same
    givenName and the same sn. -->

<UserMatchingCriteria parent.attr="UserMatchingCriteria">
    <AttributeMap parent.attr="AttributeMap">
        <AttributeDescription parent.attr="SunAttribute" name="sn"/>
        <AttributeDescription parent.attr="WindowsAttribute" name="sn"/>
    </AttributeMap>
    <AttributeMap parent.attr="AttributeMap">
        <AttributeDescription parent.attr="SunAttribute" name="givenName"/>
        <AttributeDescription parent.attr="WindowsAttribute"
        name="givenName"/>
    </AttributeMap>
</UserMatchingCriteria>
```

```
<!--
    Multiple UserMatchingCriteria can be specified for a single SUL.They are treated as
    a logical OR.In this example, (the givenName's and sn's must match (see above)) OR
    (the employee(Number|ID) must match), for the user to be linked.Notice that attribute
    that is specified, employeeNumber, is the name of the DS attribute. -->

<!--
    This UserMatchingCriteria is commented out because employeeNumber is not an indexed
    attribute in DS.All attributes used in a UserMatchingCriteria should be indexed.

    <UserMatchingCriteria parent.attr="UserMatchingCriteria">
        <AttributeMap parent.attr="AttributeMap">
            <AttributeDescription parent.attr="SunAttribute" name="employeeNumber"/>
            <AttributeDescription parent.attr="WindowsAttribute" name="employeeID"/>
        </AttributeMap>
    </UserMatchingCriteria>

-->

</UserLinkingOperation>

<!--
    When multiple SULs are linked, a separate UserLinkingOperation is specified
    for each.As shown here, each UserLinkingOperation can use different
    UserMatchingCriteria:in this example, users in SUL2 are only linked if their
    sn and employeeNumber match.

    Note:this UserLinkingOperation is currently commented out because
    the example configuration only has a single SUL.

<UserLinkingOperation parent.attr="UserLinkingOperation" sulid="SUL2">
    <UserMatchingCriteria parent.attr="UserMatchingCriteria">
        <AttributeMap parent.attr="AttributeMap">
            <AttributeDescription parent.attr="SunAttribute" name="sn"/>
            <AttributeDescription parent.attr="WindowsAttribute" name="sn"/>
        </AttributeMap>
            <AttributeMap parent.attr="AttributeMap">
                <AttributeDescription parent.attr="SunAttribute" name="employeeNumber"/>
                <AttributeDescription parent.attr="WindowsAttribute" name="employeeID"/>
        </AttributeMap>
    </UserMatchingCriteria>
</UserLinkingOperation>
-->

</UserLinkingOperationList>
```

以非超級使用者身份在 Solaris 系統上執行服務

您必須具有超級使用者權限才能安裝並執行 Identity Synchronization for Windows 服務。不過，安裝本產品之後，您可配置軟體，使其以非超級使用者身份來執行程式服務。

附註 如果您要以非超級使用者身份來執行服務，則必須變更 Identity Synchronization for Windows 實例目錄之下所有目錄的權限。(*預設*目錄爲 `/var/opt/SUNWisw`。)

若要以非超級使用者身份在 Solaris 上執行服務，請執行下列步驟：

1. 使用 UNIX `useradd` 指令來建立 Identity Synchronization for Windows 的使用者帳號 (*可選步驟*)。

   您也可以使用 `nobody` 使用者身份執行服務。
   本程序中剩下的範例假設您建立了一個名爲 *`iswuser`* 的使用者。

2. 若要在 Solaris 上安裝 Sun Java System Directory Server 連接器，必須在安裝時爲連接器選擇一個未設定權限的通訊埠。
   (例如，可以使用大於 1024 的通訊埠。)

   附註 您必須以 `root` (超級使用者) 身份在剩下步驟中執行所有指令。

3. 安裝好所有元件之後，執行下列指令以停止 Identity Synchronization for Windows：

   `/etc/init.d/isw stop`

4. 您必須更新實例目錄的所有權。
   例如，如果您在 /var/opt/SUNWisw 下安裝本產品。

   ```
   chown -R iswuser /var/opt/SUNWisw
   chown -R iswuser /opt/SUNWisw
   ```

5. 在文字編輯器中，開啓 /etc/init.d/isw 檔案並將下列文字行：

   ```
   "$EXEC_START_WATCHDOG" "$JAVA_PATH" "$INSTALL_DIR" "CONFIG_DIR"
   ```

   更換成下列文字行：

   ```
   su iswuser -c "$EXEC_START_WATCHDOG '$JAVA_PATH' '$INSTALL_DIR'
   'CONFIG_DIR'"
   ```

6. 執行下列指令以重新啓動服務：

   ```
   /etc/init.d/isw start
   ```

7. 使用指定使用者的 userid 來執行下列指令，以確認元件正在執行：

   ```
   ps -ef | grep iswuser
   ```

定義和配置同步化使用者清單

本附錄提供關於同步化使用者清單 (SUL) 定義的補充資訊，並說明如何配置多個網域。內容歸納如下：

認識同步化使用者清單定義

每個同步化使用者清單 (SUL) 均包含兩個定義，一個用來確定要同步化的 Directory Server 使用者，另一個用來確定要同步化的 Windows 使用者。

每個定義均可確定目錄中要同步化的使用者、不要同步化的使用者以及建立新使用者之處。

附註 您使用 Identity Synchronization for Windows 主控台選取的物件類別也可確定要同步化的使用者。程式只會同步化具有選定物件類別的使用者，其中包括具有選定物件類別之子類別的所有使用者。

例如，如果選取 `organizationalPerson` 物件類別，則 Identity Synchronization for Windows 將會同步化具有 `inetorgperson` 物件類別的使用者，因爲它是 `organizationalPerson` 物件類別的子類別。

表格 D-1 介紹 SUL 定義的組成元件：

表格 D-1 SUL 定義組成元件

組成元件	定義	適用環境		
		Sun	**AD**	**NT**
基本 DN	定義要同步化的所有使用者之父項 LDAP 節點。 同步化使用者清單的基本 DN 包括該 DN 中所有的使用者，除非使用者被同步化使用者清單的篩選器排除，或是使用者的 DN 符合更精細的同步化使用者清單。例如，`ou=sales,dc=example,dc=com`。	是	是	否
篩選器	定義 LDAP 形式篩選器，用於從同步化使用者清單納入或排除使用者。篩選器可包含 `&`、`|`、`!`、`=` 與 `*` 運算符。不支援 `>=` 與 `<=` 運算符。所有的比較都是使用大小寫不須相符的字串比較完成的。 例如，`(& (employeeType=manager)(st=CA))` 將只包括在 California 的所有經理。	是	是	是
建立表示式	定義新建立使用者的父項 DN 和命名屬性 (只適用於啓用了建立的情況下)。 建立表示式必須包括同步化使用者清單的基本 DN。例如，`cn=%cn%,ou=sales,dc=example,dc=com`。(其中 `%cn%` 記號由即將建立的使用者項目的值替代。)	是	是	否

附註 若要將 Sun Java System Directory Server 中的使用者與多個 Active Directory 網域同步，您必須針對各 Active Directory 網域定義至少一個 SUL。

如果定義多個 SUL，Identity Synchronization for Windows 會重複配對每個 SUL 定義來確定 SUL 中的成員。程式會先以更具體的基本 DN 來檢查 SUL 定義。例如，程式先測試 `ou=sales,dc=example,dc=com` 的配對，然後再測試 `dc=example,dc=com` 的配對。

如果兩個 SUL 定義具有相同的基本 DN 和不同的篩選器，則 Identity Synchronization for Windows 無法自動決定應該先測試哪個篩選器，因此您必須使用「解決網域重疊」功能來排序兩個 SUL 定義。如果使用者符合某個 SUL 定義的基本 DN，但不符合該基本 DN 的任何篩選器，則程式會將該使用者從同步化中排除 (即使該使用者符合精細程度較低的基本 DN 之篩選器)。

配置多重 Windows 網域

爲支援將多重 Windows 網域同步化到相同的 Directory Server 容器 (例如 ou=people,dc=example,dc=com)，Identity Synchronization for Windows 使用包含網域資訊的「合成」 Windows 屬性。

- 就 Active Directory 網域而言，Identity Synchronization for Windows 先將 activedirectorydomainname 屬性設定爲 Active Directory 網域名稱 (例如 *east.example.com*)，然後再將項目同步化到 Directory Server。
- 就 Windows NT 網域而言，Identity Synchronization for Windows 先將 user_nt_domain_name 屬性設定爲 Windows NT 網域名稱 (例如 *NTEXAMPLE*)，然後再將項目同步化到 Directory Server。

儘管這些屬性並不實際出現在 Windows 使用者項目中，但可用於在 Identity Synchronization for Windows 主控台中同步化，並可對映到 Directory Server 使用者屬性。一旦 Identity Synchronization for Windows 對映網域屬性之後，同步化期間這些屬性會在 Directory Server 項目中設定並可用於同步化使用者清單 (SUL) 篩選器中。

下列範例說明 Identity Synchronization for Windows 如何使用這些屬性。本範例假設將三個 Windows 網域 (兩個 Active Directory 網域以及一個 Windows NT 網域) 與一個 Directory Server 實例同步化。

1. Active Directory 網域 east.example.com 中的使用者將以 ou=people,dc=example,dc=com 同步化到 Directory Server。
2. Active Directory 網域 west.example.com 中的使用者將以 ou=people,dc=example,dc=com 同步化到 Directory Server。
3. Windows NT 網域 NTEXAMPLE 中的使用者將以 ou=people,dc=example,dc=com 同步化到 Directory Server。

當您建立或修改 Directory Server 使用者時，程式會使用 SUL 篩選器來決定將在哪個 Windows 網域同步化使用者 (因爲每個 Directory Server SUL 都有相同的基本 DN，ou=people,dc=example,dc=com)。activedirectorydomainname 和 user_nt_domain_name 屬性使建構篩選器變得容易。

若要從主控台的「屬性」標籤中建構一個篩選器，請：

1. 將 Directory Server destinationindicator 屬性對映到 Active Directory activedirectorydomainname 屬性以及 Windows NT user_nt_domain_name 屬性。

2. 如下所示爲每個 Windows 網域配置一個 SUL：

```
EAST_SUL
  Sun Java System Directory Server definition
    Base DN:ou=people,dc=example,dc=com
    Filter:destinationindicator=east.example.com
    Creation Expression:cn=%cn%,ou=people,dc=example,dc=com
Active Directory definition (east.example.com)
    Base DN:cn=users,dc=east,dc=example,dc=com
    Filter:<none>
    Creation Expression:cn=%cn%,cn=users,dc=east,dc=example,dc=com
WEST_SUL
  Sun Java System Directory Server definition
    Base DN:ou=people,dc=example,dc=com
    Filter:destinationindicator=west.example.com
    Creation Expression:cn=%cn%,ou=people,dc=example,dc=com
Active Directory definition (west.example.com)
    Base DN:cn=users,dc=west,dc=example,dc=com
    Filter:<none>
    Creation Expression:cn=%cn%,cn=users,dc=west,dc=example,dc=com
NT_SUL
  Sun Java System Directory Server definition
    Base DN:ou=people,dc=example,dc=com
    Filter:destinationindicator=NTEXAMPLE
    Creation Expression:cn=%cn%,ou=people,dc=example,dc=com
Windows NT definition (NTEXAMPLE)
    Base DN:NA
    Filter:<none>
    Creation Expression:NA
```

注意，每個 Directory Server SUL 定義都有相同的基本 DN 以及建立表示式，但是篩選器指示對應 Windows 使用者項目的網域。

若要進一步說明這些設定值如何讓 Directory Server 使用者項目同步化到各 Windows 網域，請參考此測試實例：

1. 在 Active Directory east.example.com 網域中建立 `cn=Jane Test,cn=users,dc=east,dc=example,dc=com`。
2. Identity Synchronization for Windows 用 `destinationindicator=east.example.com` 在 Directory Server 中建立使用者項目 `cn=Jane Test,ou=people,dc=example,dc=com`。

3. 修改 Directory Server 中的 cn=Jane Test,ou=people,dc=example,dc=com 項目。
4. 因爲 Jane Test 的 destinationindicator 屬性爲 east.example.com，她的項目將符合 EAST_SUL 同步化使用者清單篩選器，並且修改將被同步化到 east.example.com Active Directory 網域。

本範例假設 Identity Synchronization for Windows 建立使用者時的傳遞方向是從 Windows 同步化到 Directory Server。如果不是這種情形，您可以執行 idsync resync 指令來設定 destinationindicator 屬性。

附註 當您在部署了多個 SUL 的環境中使用 idsync resync -f 時，可能必須將連結配置檔案中的 allowLinkingOutOfScope 選項設爲 true。請參閱附錄 B，「LinkUsers XML 文件範例」以瞭解詳細資訊。

本範例使用 inetorgperson 中現有的屬性 destinationIndicator，其還可用於其他用途。如果此屬性已經使用，或是選取了不同的物件類別，則您必須將使用者的 Directory Server 項目中的某些屬性對映到 user_nt_domain_name 以及 / 或是 activedirectorydomainname 屬性。您選擇用於容納此值的 Directory Server 屬性必須在用於屬性對映配置的其餘部分的物件類別中。

如果沒有尚未使用的屬性可保留此網域資訊，您必須建立新的物件類別來容納新網域屬性以及將用於 Identity Synchronization for Windows 的所有其他屬性。

複製環境的安裝註解

Identity Synchronization for Windows 1 2004Q3 支援同步化單一複製字尾中的使用者。

附註 本附錄歸納出配置與保全多主伺服器複製 (MMR) 部署的程序。這些資訊直接摘錄自 *《Sun Java System Directory Server 5 2004Q2 Administrator's Guide》*，並非 Identity Synchronization for Windows 專用的資訊。

MMR 部署的設計和實現是非常*複雜的*。請參閱 *《Sun Java System Directory Server 5 2004Q2 Deployment Guide》*來規劃部署，參閱 *《Sun Java System Directory Server 5 2004Q2 Administrator's Guide》*來實現部署。

本附錄內容分作以下各節：

配置複製

附註 在多主伺服器複製 (MMR) 環境中，Identity Synchronization for Windows 可讓您爲任何特定 Sun 目錄來源指定喜好的伺服器和輔助伺服器。

Directory Server version 5 2004Q2 現在支援四向 MMR (您可以在四個主伺服器中的任何一個變更複本資料庫)。當您在第三或第四主伺服器安裝外掛程式時，必須選取*其他*主機類型，並在外掛程式安裝期間手動輸入 Directory Server 實例的參數。

下列步驟假設您要複製單一字尾。如果您要複製多個字尾，可在各個伺服器上平行配置它們。換言之，您可重複各個步驟在多個字尾上配置複製。

若要配置任何複製拓樸，請依照下列順序執行：

1. 在所有伺服器 (單一主伺服器除外) 上定義複製管理員項目 (或在所有伺服器上使用預設複製管理員)。
2. 在所有包含專屬用戶複本的伺服器上：
   a. 爲用戶複本建立空白的字尾。
   b. 透過複製精靈對字尾啓用用戶複本。
   c. 配置進階複本設定值 (可選步驟)。
3. 在所有包含集線器複本的伺服器上 (如果適用)：
   a. 爲集線器複本建立空白的字尾。
   b. 透過複製精靈對字尾啓用集線器複本。
   c. 配置進階複本設定值 (可選步驟)。
4. 在所有包含主伺服器複本的伺服器上：
   a. 在將成爲主伺服器複本的一個主伺服器上選擇或建立一個字尾。
   b. 透過複製精靈對字尾啓用主伺服器複本。
   c. 配置進階複本設定值 (可選步驟)。
5. 以下列順序對所有供應者複本配置複製合約：
   a. 在多主伺服器集中的主伺服器之間。
   b. 在主伺服器和專屬用戶之間。

c. 在主伺服器和集線器複本之間。

您也可以在此階段配置部分複製 (可選步驟)。

6. 在集線器複本及其用戶之間配置複製合約。
7. 如果是多主伺服器複製的環境，請從包含原始資料複本的相同主伺服器複本初始化所有的主伺服器。初始化集線器和用戶複本。

配置透過 SSL 複製

附註 有關本程序的所有參考資料請參閱《*Sun Java System Directory Server 5 2004Q2 管理指南*》中的章節。

若要對複製中涉及的 Directory Server 進行配置，使所有複製作業透過 SSL 連線實現，請完成下列步驟：

1. 將供應者和用戶伺服器配置爲使用 SSL。

詳細內容請參閱 11 章「管理驗證與加密」。

附註
- 如果供應者伺服器憑證是僅限 SSL 伺服器使用的憑證 (無法在 SSL 訊號交換期間作爲用戶端使用)，則透過 SSL 複製將會失敗。
- 目前並不支援使用自簽憑證透過 SSL 進行複製。

2. 如果沒有爲用戶伺服器上的字尾配置複製，請按照第 8 章的〈啓用用戶複本〉中的說明將其啓用。
3. 依照第 8 章的〈進階用戶配置〉中的程序，將用戶的憑證項目之 DN 定義爲另一個複製管理員。
4. 如果沒有爲供應者伺服器上的字尾配置複製，請參照第 8 章的〈啓用集線器複本〉或〈啓用主伺服器複本〉中的描述將其啓用。
5. 在供應者伺服器上，建立新的複製合約來將更新傳送到安全 SSL 通訊埠上的用戶。有關詳細說明，請參閱第 8 章的〈建立複製合約〉中描述的程序。在用戶伺服器上指定一個安全通訊埠並在 SSL 選項中選擇使用密碼或是憑證。爲您選擇的 SSL 選項輸入 DN，可以是複製管理員或憑證。

在您配置完複製合約後，供應者將所有複製更新訊息透過 SSL 傳送給用戶，並且如果您選擇了該選項，還將使用憑證。如果透過主控台使用爲 SSL 配置的合約來進行用戶初始化，用戶初始化也將使用安全連線。

在 MMR 環境中配置 Identity Synchronization for Windows

下列程序歸納了在 MMR 環境下配置 Identity Synchronization for Windows 的步驟，詳細說明請見本指南中的其他部分。

1. 從 Identity Synchronization for Windows 主控台，爲您要同步化的字尾指定喜好的和輔助的 Directory Server 主伺服器。(請參閱第 106 頁上的「建立 Sun Java System 目錄來源」。)

   您不需提供有關您的拓樸中其他 Directory Server 的資訊。

2. 從主控台或使用 `idsync prepds` 指令行公用程式來準備喜好的和輔助的伺服器。(請參閱第 113 頁上的「準備 Directory Server」或第 313 頁上的「使用 prepds」。)

   如果您使用指令行公用程式，則應同時指定喜好的伺服器和輔助伺服器所使用的引數，這樣一來，只要呼叫一次就可同時啓動兩個伺服器。

3. 爲在這些目錄之間複製的字尾安裝 Directory Server 連接器。(請參閱第 163 頁上的「安裝 Directory Server 連接器」。)

4. 將 Directory Server 外掛程式安裝在喜好的主伺服器、輔助主伺服器，以及負責管理複製之字尾中的使用者的所有其他 Directory Server 實例上。(請參閱第 173 頁上的「安裝 Directory Server 外掛程式」。)

詞彙

以下專有名詞用於 Identity Synchronization for Windows 產品和此文件集中。

CA 請參閱憑證授權單位。

CLI 請參閱指令行介面。

DIT 請參閱目錄資訊樹。

DM 請參閱目錄管理員。

DNS 網域名稱系統。網路中的電腦用來將標準 IP 位址 (例如 198.93.93.10) 與主機名稱 (例如 www.example.com) 關聯的系統。電腦通常從 DNS 伺服器取得主機名稱的 IP 位址，或在其系統上維護的表格中查詢此地址。

FSMO 角色 彈性的單一主伺服器操作角色。Active Directory 用於防止多主伺服器部署中發生更新衝突的機制。即使部署作業爲多主伺服器，部分物件仍會在單一主伺服器模式下更新，這與 Windows NT 網域中傳統的「主要網域控制器 (PDC)」概念很相似。Active Directory 部署中有五個 FSMO 角色，但只有 PDC 模擬器角色會影響 Identity Synchronization for Windows。由於密碼更新立即會隨 PDC 模擬器角色只被複製到 Active Directory 網域控制，所以 Identity Synchronization for Windows 使用此網域控制器進行同步化。否則，與 Sun Java System Directory Server 的同步化可能會延遲幾分鐘。

Identity Synchronization for Windows 主控台 用於配置和監視 Identity Synchronization for Windows 的圖形化使用者介面。

IP 位址 網際網路通訊協定位址。一組由小數點分隔的數字，指定電腦在網際網路上的實際位置 (例如，192.168.2.1)。

ISO 國際標準組織。

Java 訊息服務　訊息傳送標準 API，可讓基於 Java 2 Platform Enterprise Edition (J2EE) 的應用程式元件建立、傳送、接收及讀取訊息。它允許進行鬆散結合、可靠及非同步的分散式通訊。

JMS　請參閱 Java 訊息服務。

LDAP　輕量級目錄存取協定。專用於在 TCP/IP 和多重平台間執行的目錄服務協定。Identity Synchronization for Windows 使用 LDAP 與 Active Directory 網域控制器和 Sun Java System Directory Server 進行通訊。

LDAP URL　提供使用 DNS 尋找目錄伺服器然後經由 LDAP 完成查詢的方法。LDAP URL 範例爲 `ldap://ldap.example.com`

LDAP 用戶端　用於請求和檢視來自 LDAP Directory Server 的 LDAP 項目的軟體。在連線到 LDAP 伺服器時，Identity Synchronization for Windows 連接器將作爲 LDAP 用戶端。

Message Queue　請參閱 Sun Java System Message Queue

MMR　請參閱多主伺服器複製。

MQ　請參閱 Sun Java System Message Queue。

RCL　請參閱 retro changelog。

retro changelog　一個 Directory Server 資料庫 (cn=changelog)，儲存對 Directory Server 所做所有變更的記錄。Identity Synchronization for Windows 使用 retro changelog 來偵測對 Directory Server 所做的變更。在 MMR 環境中，必須啓用喜好的 Directory Server 上的 retro changelog。

SSL　安全資料傳輸層。用於在雙方 (用戶端與伺服器) 之間建立安全連線的一個軟體資料庫。用於實現 HTTPS (HTTP 的安全版本) 及 LDAPS (LFAP 的安全版本)。

SUL　請參閱同步化使用者清單。

Sun Java System Message Queue　實現「Java 訊息服務 (JMS)」開放標準的企業訊息傳送系統。Message Queue 的基礎結構包含發佈方與訂閱方，它們藉由共同服務來交換訊息。Sun Java System Message Queue 由專用的訊息代理程式進行管理，它負責控制 Message Queue 的存取、維護使用中的出版社和訂閱者的相關資訊，並確保傳遞這些資訊。Identity Synchronization for Windows 使用 Message Queue 來安全地同步化使用者變更事件、發布配置資訊，以及監視遠端元件的狀況。

Sun Java System Message Queue 代理程式　一台獨立式 Java 伺服器，可使用戶端存取 Sun Java System Message Queue。在 Solaris 系統中，透過 `/etc/init.d/imq daemon` 程序檔控制代理程式；而在 Windows 系統中，則是透過「iMQ 代理程式」服務控制。Identity Synchronization for Windows 在安裝核心元件過程中配置並啓動代理程式。

uid　與 UNIX 系統上每個使用者相關聯的獨特號碼。

URL　單一資源定址器。伺服器和用戶端用於請求文件的定址系統。通常稱爲位置。URL 的格式爲 `[protocol]://[machine:port]/[document]`。只有在選定的伺服器上才需要通訊埠號，此號碼通常由伺服器分配，如此使用者就不必將其置於 URL 中。

子元件　與連接器分開執行的輕量級程序或程式庫。子元件在連接器所管理的目錄來源附近執行，並會啓用連接器中無法在遠端電腦或獨立程序中實現的功能。子元件可透過自訂的加密通道與連接器通訊，以接收配置資訊、報告變更事件並記錄到中央記錄程式。Identity Synchronization for Windows 包含三個子元件：Directory Server 外掛程式、Windows NT 密碼篩選器 DLL 及 Windows NT 變更偵測器。

中央記錄程式　一個管理所有中央日誌的核心元件，這些中央日誌是每個連接器的稽核和錯誤日誌的彙總。管理員可藉由監視這些日誌來監視整個 Identity Synchronization for Windows 的安裝狀況。您可直接檢視中央日誌，也可透過 Identity Synchronization for Windows 主控台檢視。在預設狀況下，中央日誌位於安裝有核心元件的電腦之 `<`*install-root*`>/logs/central/` 子目錄下。

主物件類別　請參閱結構性物件類別。

主控台　用於配置和監視伺服器應用程式的圖形化使用者介面。Sun Java System Directory Server 與 Identity Synchronization for Windows 有獨立的主控台。

主機名稱　以 machine.domain.com 爲形式的電腦名稱，會轉譯爲一個 IP 位址。例如，`www.example.com` 是在網域 *com* 子網域 *example* 中的電腦 *www*。

代理　一個連接器元件，可與 Message Queue 互動，並轉譯其 Directory Server 名稱與 Windows 名稱之間的屬性。在日誌訊息中，經常將代理程式作爲某個特定動作的參考。

代理程式　請參閱 Sun Java System Message Queue 代理程式。

外掛程式　一種附加程式，可將其載入並作爲整體系統的一部分來使用。

例如，Identity Synchronization for Windows 使用 Directory Server 外掛程式來加強 Directory Server 連接器變更偵測功能，並爲 Active Directory 和 Directory Server 之間的密碼同步化提供雙向支援。

用戶端　請參閱 LDAP 用戶端。

目錄來源　Sun Java System Directory Server、Windows Active Directory 網域或 Windows NT 網域。目錄來源包含要同步化的使用者。

目錄資訊樹　儲存在目錄中的資訊之邏輯表示，它鏡像了大多數檔案系統所使用的樹模型，其中樹目錄的根在階層頂部顯示。

目錄管理員　授權的目錄伺服器管理員，相較於 UNIX 中的超級使用者。Identity Synchronization for Windows 需要目錄管理員憑證才可以執行特定的配置作業，但連接器不需要目錄管理員憑證以進行同步化作業。

同步化主機　根據同步化使用者清單 (SUL) 中定義的規則儲存同步化資料的伺服器。

同步化使用者清單　在要同步化的 Sun 和 Windows 目錄中定義使用者。「同步化使用者清單」可根據 LDAP 基本 DN 或篩選器限制要同步化的使用者之範圍。

同步化的屬性　請參閱重要屬性。

地區設定　針對特定地區、文化和 / 或習慣的使用者，定義用來呈現這些使用者資料的比較順序、字元類型、貨幣格式、時間 / 日期格式。其中包括了有關如何解釋、儲存或比較指定語言的資料的資訊。地區設定也會指出應使用哪一代碼頁來表示指定語言。

多主伺服器複製　一個目錄伺服器複製模型，在此模型內，您可以在數個主伺服器複本中的任意一個上寫入及更新項目，而不必在執行寫入或更新之前與其他主伺服器複本進行通訊。在一台伺服器中所做的修改會自動複製到其他伺服器。您可在部署多個目錄伺服器主複本時安裝 Identity Synchronization for Windows。然而，當同步化對 Windows 的變更時，必須要有喜好的目錄伺服器；而當同步化來自 Windows 的變更時，必須要有喜好或輔助的目錄伺服器。

字元類型　將字母字元同數值 (或其他) 字元以及大寫到小寫字母的對應區別開來。

字尾　目錄樹頂部的項目名稱，資料儲存在其下方。在相同目錄內可以有多個字尾。每個資料庫只有一個字尾。

存取操作　一個連接器層，其透過協定 (如 LDAP) 直接與目錄來源通訊。Identity Synchronization for Windows 對 Directory Server、Active Directory 及 Windows NT 有不同的存取實施方式。在日誌訊息中，經常將存取操作作爲某個特定動作的參考。

安全資料傳輸層　請參閱 SSL。

伺服器主控台　基於 Java 的應用程式可讓您從 GUI 執行 Directory Server 的管理員管理。

伺服器根　伺服器電腦上專門用於保留伺服器程式配置、維護以及資訊檔案的目錄。

系統管理員　獨立式 Java 程序，由安裝了核心元件的「監視程式」常駐程式 / 服務所啓動。系統管理員會將配置資訊發布到連接器和中央核心元件，監視系統的狀況並協調 `idsync resync` 作業。

協定　描述網路中的裝置如何交換資訊的一組規則。

命名上下文　(也稱爲根字尾) 目錄資訊樹 (DIT) 的特定字尾，由其辨別名稱 (DN) 來識別，例如 dc=example,dc=com。在 Identity Synchronization for Windows 中，用於 Sun Java System Directory Server 的目錄來源由字尾所定義，該字尾中包含要同步化的資料。

拓樸　在實體伺服器之間分隔目錄樹以及這些伺服器彼此連結的方式。

服務　在 Windows 電腦上負責特定系統工作的後台程序。服務程序不需要人工操縱即可繼續運作。在 Windows 中，連接器、系統管理員和中央日誌程式作爲由 Identity Synchronization for Windows 監視程式服務所啓動和監視的程序執行。

物件快取　Windows 連接器用於偵測對使用者項目所做變更的處於程序中的資料庫。物件快取可儲存每一個使用者項目的雜湊摘要，這可讓 Windows 連接器確定使用者項目中已發生變更的特定屬性。

物件類別　用於指定項目所描述的物件種類以及項目中所包含的有效和強制屬性集的一個範本。例如，Directory Server 可指定一個 `inetorgperson` 物件類別，它具有 `cn` 和 `userpassword` 等屬性。隨需密碼同步化：一種機制，藉由此機制使 Directory Server 中的使用者密碼無法被更新，直到使用者嘗試進行 Directory Server 身份驗證時爲止。僅當提供的密碼符合 Active Directory 中儲存的密碼時，才會同步化使用者的密碼。這將簡化 Active Directory 環境中的密碼同步化。

建立屬性　只有在建立物件時才會同步化的屬性。當建立物件時會自動同步化所有重要屬性。對於在遠端目錄中可能沒有相應屬性值的建立屬性，您可以爲其配置預設值。

指令行介面　程式及其使用者之間的一種通訊方式，僅依賴於文字式輸入和輸出。指令可藉助鍵盤或類似的裝置輸入，並由程式來解譯和執行。Identity Synchronization for Windows 指令行介面稱爲 `idsync`，並且位於安裝了核心元件的 `bin/` 目錄中。

重要屬性　建立或修改項目時所同步化的屬性。

重新同步化間隔　連接器檢查目錄來源變更的頻率。此定期檢查很有效，而且只需要讀取自上次檢查以來已變更的使用者項目。主控台以微秒爲單位表示此值，並提供預設值 1000 (1 秒)。

核心元件　安裝的第一個 Identity Synchronization for Windows 元件。此核心元件包含在配置目錄、系統管理員、中央日誌程式、主控台及指令行介面中儲存的初始配置。

根　UNIX 機器上權限最大的使用者 (也稱爲超級使用者)。超級使用者對電腦上的所有檔案都具有完全存取權限。在 Solaris 系統中，必須將 Identity Synchronization for Windows 安裝爲根。

根字尾　一個或多個 LDAP 子字尾的父項。目錄樹可包含一個以上的根字尾。

配置目錄　Directory Server 的特殊安裝，此 Directory Server 用作配置和狀態資訊的儲存庫。Identity Synchronization for Windows 會將其所有配置儲存在安裝核心元件過程中所選擇的配置目錄實例內。

配置密碼　安裝核心元件的過程中所選擇的密碼，可保護配置目錄所儲存的所有敏感性 Identity Synchronization for Windows 資訊。使用安裝程式、主控台或指令行介面時必須提供配置密碼。

配置登錄　Identity Synchronization for Windows 用來代表配置目錄的另一個術語。

副檔名　位於句點或小數點 (.) 後的檔案名稱部分，通常用來定義檔案類型 (例如，.GIF 和 .HTML)。例如，在名爲 `index.html` 的檔案中，副檔名爲 *`html`*。

動作　單個同步化事件的封裝。Identity Synchronization for Windows 連接器使用動作來溝通使用者變更事件。每個動作都包含一個類型 (如 `CREATE`、`MODIFY` 或 `DELETE`) 及來自使用者項目的足夠屬性，以使目標連接器可同步化變更。所有動作皆以單元方式執行。

基本 DN　基本辨別名稱。對基本 DN、項目 DN 以及目錄樹中其下所有的項目執行一項搜尋作業。對於 Active Directory 和 Directory Server 而言，「同步化使用者清單」以特定的基本 DN 爲基礎。系統將同步化此基本 DN 下的所有使用者，除非篩選器明確排除其下的使用者。

基本辨別名稱　請參閱基本 DN。

密碼策略　管理如何在指定目錄中使用密碼的一組規則。

密碼檔案　UNIX 機器上的一種檔案，用於儲存 UNIX 使用者登入名稱、密碼和使用者 ID 號碼。因其所在的位置，也可稱爲 `/etc/passwd`。

常駐程式　在 UNIX 機器上負責特定系統工作的後台程序。常駐程式處理程序不需要人工操縱即可繼續運作。連接器、系統管理員和中央日誌程式作爲常駐程式程序執行，這些程序由 Identity Synchronization for Windows 監視程式啓動和監視。

控制器　可與代理程式和存取操作元件通訊的連接器元件。控制器可執行與金鑰同步化相關的工作，如確定使用者在「同步化使用者清單」中的成員資格、搜尋及連結對等使用者項目，以及透過比較現行的使用者項目與物件快取中所儲存的舊版本來偵測對使用者所做的變更。在日誌訊息中，經常將控制器作爲某個特定動作的參考。

通用類別目錄　Windows 儲存庫，它會儲存 Active Directory 目錄拓樸及 Active Directory 目錄的網目資訊。

連接器　管理 Identity Synchronization for Windows 與單一資料來源 (如 Directory Server、Active Directory 網域或 Windows NT 網域) 之間互動操作的一個 Java 程序。連接器負責偵測資料來源中的使用者變更，並透過 Message Queue 發佈這些變更到遠端連接器、訂閱使用者變更主題，以及將這些主題中的更新套用到資料來源。

連結 DN　執行作業時用於驗證 LDAP 目錄的辨別名稱 (例如 Active Directory 或 Directory Server)。

連結辨別名稱　請參閱連結 DN。

喜好的目錄伺服器　Identity Synchronization for Windows 用於偵測並套用對使用者項目所做變更的目錄伺服器主實例。當這台伺服器可用時，Identity Synchronization for Windows 不會與其他任何目錄伺服器主實例通訊。

結構性物件類別　項目的主要物件類別，用於定義 Identity Synchronization for Windows 所同步化的使用者項目中的有效和強制屬性集。例如，預設的 Active Directory 物件類別是 `user`；預設的 Directory Server 物件類別則是 `inetorgperson`。請參閱輔助物件類別。

超級使用者　請參閱根。

階層式複製　在階層式複製方案中，一台伺服器 (通常稱爲*集線器供應者*) 要同時作爲特定複本的用戶和供應者。這台伺服器持有一個唯讀複本並維護一個變更日誌。它從存有資料主要複本的供應者伺服器接收更新，並依次爲用戶提供以上更新。

傳入　在連接器內，從目錄來源朝向 Message Queue 傳遞的動作方向。連接器所偵測的變更會傳入系統中。動作的相關日誌訊息通常會參照在連接器的傳入端所發生的事件。

傳出　在連接器內，從 Message Queue 朝向目錄來源傳遞的動作方向。由連接器所套用的變更會傳出到同步化的目錄來源中。動作的相關日誌訊息通常會參照在連接器的傳出端所發生的事件。

監視程式　獨立式 Java 程序，在安裝有核心元件或連接器的每台電腦上安裝。監視程式會啓動所有 Identity Synchronization for Windows Java 程序，包含系統管理員、中央日誌程式及連接器。這些元件中若有任何元件失敗，監視程式會重新啓動它們。在 Solaris 系統中，透過 `/etc/init.d/isw` 常駐程式程序檔來控制代理程式；而在 Windows 系統中，則是透過「Sun Java™ System Identity Synchronization for Windows」服務來控制。

網域　(1) (n.) 完全合格的網域名稱的最後部份，用於識別具有網域名稱的公司或組織 (例如，example.com、host.example.com)。

(2) (n.) 由單一電腦系統所控制的資源。

網域控制器　Windows 伺服器，可儲存使用者帳號資訊、驗證使用者，以及對 Windows 網域強制執行安全性原則。Identity Synchronization for Windows 連接器可直接與網域控制器通訊，以偵測對使用者帳號的變更，並同步化 Directory Server 使用者項目中所做的變更。

輔助目錄伺服器　當喜好的目錄伺服器不可用時，可供 Identity Synchronization for Windows 使用的 MMR 環境中的目錄伺服器主實例。在無法使用喜好的目錄伺服器時，Identity Synchronization for Windows 可將 Active Directory 或 Windows NT 中所做的變更同步化到輔助目錄伺服器，但在喜好的目錄伺服器可用之前，將無法同步化在輔助伺服器或其他任何目錄伺服器主實例中所做的變更。

輔助物件類別　可擴大選定結構性類別的物件類別，它提供用於同步化的其他屬性。請參閱結構性物件類別。

輕量級目錄存取協定　請參閱 LDAP。

模式　描述可將何種類型資訊儲存爲目錄中之項目的定義。當資訊不符合儲存在目錄中的模式時，嘗試存取目錄的用戶端可能無法顯示正確的結果。

模式檢查　確保在目錄中新增或修改的項目符合定義的模式。模式檢查在預設情況下爲開啓，使用者在試圖儲存不符合模式的項目時將收到錯誤訊息。

確認　一則專用訊息，用來確認已接收到其他元件的訊息。Identity Synchronization for Windows 在連接器與 Message Queue 之間以及連接器元件 (代理程式、控制器與存取操作) 之間使用確認，以確保可靠地同步化所有變更。

稽核日誌　一個中央日誌檔案，其中包含針對於每日事件的項目，如正在同步化的使用者之密碼。管理員可使用 Identity Synchronization for Windows 主控台來控制此日誌中所顯示的項目數及詳細等級。

每個連接器都會產生一個關於該連接器所處理之使用者的稽核日誌，此外還有一個中央稽核日誌，包含了由部署作業中所有連接器所產生的稽核日誌的彙總。

憑證　將公開金鑰與網路身份相聯結的一個資料集合。利用此資訊可接收電子訊息，以檢驗訊息及訊息傳送者的驗證。當您配置 Identity Synchronization for Windows 連接器來使用 SSL 通訊時，必須先將憑證加入連接器的憑證資料庫，然後才可進行可靠的 SSL 通訊。另請參閱憑證授權單位。

憑證授權單位　銷售和發佈驗證憑證的公司或組織。您可以從信任的憑證授權單位 (也稱爲 *CA*) 購買驗證憑證。您可使用根憑證授權單位的憑證來簽署其他憑證。配置 Identity Synchronization for Windows 連接器來使用 SSL 時，必須將相應根憑證授權單位的憑證加入連接器的憑證資料庫中。

憑證資料庫　憑證的安全儲存庫，包含三個檔案：`cert8.db`、`key3.db` 及 `secmod.db`。在 Identity Synchronization for Windows 中，每個連接器都有它自己的資料庫目錄 (例如，`<`*install-root*`>/etc/CNN100`)。另請參閱憑證。

辨別名稱　LDAP 目錄中項目名稱和位置的字串陳述。

檔案類型　指定檔案的格式。例如，圖形檔案通常儲存爲 `GIF` 格式，而文字檔案通常儲存爲 `ASCII` 文字格式。檔案類型通常由副檔名定義 (例如，.GIF 或 .HTML)。

屬性　包含某一項目的有關描述資訊。屬性具有標籤和值。每個屬性同樣還依照針對某一資訊類型 (可儲存爲屬性值) 的標準語法。

屬性清單　針對指定項目類型或物件類別的必須或可選屬性清單。

權限　在存取控制的上下文中，權限規定是授予還是拒絕對目錄資訊的存取權，以及授予或拒絕的存取層級。

驗證　將用戶端使用者的身份提供給 Directory Server 的程序。使用者必須提供連結 DN 和相應密碼，以獲得目錄的存取權。根據目錄管理員給予使用者的權限，Directory Server 可允許該使用者執行功能或存取檔案和目錄。

驗證憑證　由協力廠商發佈的一個數位檔案，該檔案不可轉移或僞造。爲了核對並驗證第三方，將驗證憑證由伺服器傳送到用戶端 (或由用戶端傳送到伺服器)。

索引

數字

A

B

C

D

E

F

I

J

K

L

M

N

O

P

R

S

T

U

W

X

二畫

三畫

四畫

五畫

六畫

七畫

八畫

九畫

十畫

十一畫

十二畫

十三畫

十四畫

十五畫

十六畫

十七畫

十八畫

十九畫

二十畫

二十一畫

二十二畫

二十三畫