

Novell Identity Manager Driver for eDirectory™

3.0

www.novell.com

實作指南

2006 年 5 月 8 日



Novell®

法律聲明

Novell, Inc. 不對本文件的內容或使用做任何陳述或保證，且特別聲明不對任何特定用途的適銷性或適用性提供任何明示或隱喻的保證。此外，Novell, Inc. 保留隨時修改本出版品及其內容的權利，且在進行此類修正或更動時，不需另行通知任何人士或公司。

此外，Novell, Inc. 不對任何軟體作任何陳述或保證，且特別聲明不對任何特定用途的適銷性或適用性提供任何明示或隱喻的保證。此外，Novell, Inc. 保留隨時修改任何或全部 Novell 軟體的權利，且在進行此類更動時，不需通知任何人士或公司。

這份授權書中所提及的任何產品或技術資訊皆受到美國出口管制法 (U.S. Export Control) 及其他國家的交易法約束。您同意遵守所有出口管制法規，並取得出口、再出口或進口交付物品所需之任何必要的授權或類別。您同意不出口或再出口至目前美國出口排除清單上所列公司，或者至美國出口法所指定之禁運或恐怖份子的國家。您同意不將交付產品用在禁止的核子武器、飛彈或化學生物武器等用途上。如需更詳細的 Novell 軟體出口資訊，請參閱 www.novell.com/info/exports/。Novell 無須承擔您無法取得任何必要的出口核准之責任。

版權 © 2000-2005 Novell, Inc. 版權所有。未經出版者的書面同意，本出版品的任何部份皆不可複製、影印、傳送，或是儲存在可擷取系統上。

Novell, Inc. 擁有在此份文件中所描述產品內含技術的智慧財產權。尤其 (但不限於) 這些智慧財產權可能包含一或多個列於 <http://www.novell.com/company/legal/patents/> 的美國專利，以及一或多個在美國和其他國家的額外專利或申請中的專利。

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

線上文件：若要存取本產品及其他 Novell 產品的線上文件，或取得更新，請參閱 www.novell.com/documentation。

Novell 商標

如需 Novell 商標之清單，請參閱商標 (<http://www.novell.com/company/legal/trademarks/tmlist.html>)。

協力廠商資料

所有的協力廠商商標均為其各別擁有廠商的財產。

目錄

關於本指南	3
1 綜覽	5
1.1 術語的變更	5
1.2 關鍵詞彙	5
2 安裝 Identity Manager Driver for eDirectory	7
2.1 驅動程式 Shim 的安裝位置	7
2.2 驅動程式先決條件	7
2.3 升級至 Identity Manager 3	7
2.4 安裝驅動程式 Shim	7
2.4.1 安裝至 Windows	8
2.4.2 安裝至 NetWare	10
2.4.3 安裝至 Linux、Solaris 或 AIX	12
2.5 啟用驅動程式	15
3 升級 Identity Manager Driver for eDirectory	17
3.1 準備升級	17
3.2 升級驅動程式 Shim	17
3.3 升級驅動程式組態	18
3.4 eDirectory 驅動程式的升級問題	18
4 驅動程式組態檔案範例	21
4.1 輸入驅動程式組態範例	21
4.1.1 使用 iManager 輸入	21
4.1.2 使用 Designer for Identity Manager 輸入	22
4.2 設定 Identity Manager 資料傳送的安全性	23
4.2.1 了解 eDirectory 驅動程式的安全性	23
4.2.2 設定 KMO	24
4.3 哪些屬性已同步化	25
4.4 密碼同步化	25
5 設定驅動程式	27
5.1 設定驅動程式物件內容	27
5.1.1 驗證參數	28
5.2 設定過濾器	29
5.3 設定發行者通道上的規則	30
5.4 使用驅動程式物件密碼	30
5.5 移轉或複製物件	31
A 文件更新	33
A.1 2006 年 5 月 8 日	33

關於本指南

本指南將說明如何安裝及設定 Identity Manager Driver for eDirectory 炕 C

- ◆ 第 1 章 「綜覽」, 第 5 頁
- ◆ 第 2 章 「安裝 Identity Manager Driver for eDirectory」, 第 7 頁
- ◆ 第 3 章 「升級 Identity Manager Driver for eDirectory」, 第 17 頁
- ◆ 第 4 章 「驅動程式組態檔案範例」, 第 21 頁
- ◆ 第 5 章 「設定驅動程式」, 第 27 頁

使用對象

本指南是針對使用 Identity Manager Driver for eDirectory 之 Novell® eDirectory 及 Identity Manager 管理員而撰寫的。

意見反應

我們想知道您對於本手冊與其他本產品隨附之文件的意見與建議。請使用線上文件中每頁底下的「使用者意見」功能，或請造訪 www.novell.com/documentation/feedback.html，然後寫下您的意見。

文件更新

如需本文件的最新版本，請參閱 [Novell 文件網站 \(http://www.novell.com/documentation\)](http://www.novell.com/documentation) 上「Identity Manager 驅動程式」章節內的 *Identity Manager Driver for eDirectory*。

其他文件

如需 Identity Manager 和其他 Identity Manager 驅動程式的相關資訊，請參閱 [Novell 文件網站 \(http://www.novell.com/documentation\)](http://www.novell.com/documentation)。

文件慣例

在本文件中，大於符號 (>) 是用以分隔步驟中的各個動作，以及前後參照路徑中的數個項目。

商標符號 (®、™ 等) 代表 Novell 的商標。星號 (*) 代表協力廠商的商標。

Identity Manager Driver for eDirectory™ 會同步化不同 eDirectory 網路樹之間的物件和屬性。

此驅動程式是所有其他 Identity Manager 驅動程式當中最獨特的驅動程式。因為您是在兩個 eDirectory 網路樹之間進行資料同步化，所以您需要分別在每個網路樹中各安裝一個驅動程式。一方網路樹的驅動程式就可以對另外一方網路樹的驅動程式進行通訊。

例如，TreeA 的「發行者」通道會與 TreeB 的「訂閱者」通道通訊。相反的，TreeB 的「發行者」會與 TreeA 的「訂閱者」通道通訊。因此，必須安裝和設定驅動程式兩次。一次為 TreeA 的 eDirectory 驅動程式，另外一次為 TreeB 的驅動程式。

如需 Identity Manager 新功能的相關資訊，請參閱《[Identity Manager 3.0 安裝指南](#)》中的「[Identity Manager 3 新功能](#)」。

1.1 術語的變更

以下是與舊版不同的詞彙：

表格 1-1 術語的變更

舊詞彙	新詞彙
DirXML®	Identity Manager
DirXML 伺服器	Metadirectory 伺服器
DirXML 引擎	Metadirectory 引擎
eDirectory	Identity Vault (指 eDirectory 屬性或類別時除外)

1.2 關鍵詞彙

驅動程式 Shim。Java 檔案 (NdsToNds.jar) 直接由 Identity Manager 載入。負責溝通 Identity Manager Driver for eDirectory 與 Identity Vault 之間的變更 (如：Identity Manager Driver for eDirectory 傳送到 Identity Vault 的事件變更，以及 Identity Vault 傳送到 Identity Manager Driver for eDirectory 的變更)；其功能即是做為連接 Identity Vault 與 Identity Vault 驅動程式物件之間的連結。

驅動程式。一組扮演 Identity Vault 和驅動程式 Shim 之間的連接器角色的規則、過濾器 and 物件。

此軟體能讓應用程式將事件從應用程式發行至目錄，讓應用程式從目錄訂閱事件，以及同步化目錄與應用程式之間的資料。

若要建立 Metadirectory 引擎和 Identity Vault 之間的連接，您可以指定驅動程式的組態和連接參數、規則及過濾器的值。

驅動程式物件。連接應用程式與執行 Identity Manager 之 Identity Vault 的通道、規則、規範和過濾器的集合。

每個驅動程式皆執行不同的任務。規則、規範和過濾器會告知驅動程式如何處理資料以執行這些任務。

「驅動程式」物件顯示驅動程式組態、規則和過濾器的相關資訊。此物件可讓您管理驅動程式，並提供驅動程式 Shim 參數的 eDirectory 管理。

Identity Vault。資料中心；應用程式和目錄會將變更發行到此處。然後 Identity Vault 會傳送變更到已經訂閱變更的應用程式和目錄。如此會產生兩個主要的資料流：「發行者」通道和「訂閱者」通道。

安裝 Identity Manager Driver for eDirectory

2

- 「驅動程式 Shim 的安裝位置」，第 7 頁
- 「驅動程式先決條件」，第 7 頁
- 「升級至 Identity Manager 3」，第 7 頁
- 「安裝驅動程式 Shim」，第 7 頁
- 「啓用驅動程式」，第 15 頁

2.1 驅動程式 Shim 的安裝位置

在 Novell® eDirectory 伺服器和您要同步化的網路樹中安裝 Identity Manager 和 eDirectory™ 驅動程式 Shim。此驅動程式不使用「遠端載入器」(Remote Loader) 技術，因為一個網路樹內的驅動程式會直接與其他網路樹內的驅動程式進行通訊。

驅動程式會使用 Novel Certificate Server™ 及「證書權限 (CA)」來確認資料的安全性。網路樹間的所有異動都會受 SSL 技術保護。如需資料安全性的相關資訊，請參閱「設定 Identity Manager 資料傳送的安全性」，第 23 頁。

2.2 驅動程式先決條件

- Identity Manager 的要求。請參閱《*Identity Manager 3.0 安裝指南*》。
- Novell Certificate Server 會在每部裝載 eDirectory 驅動程式的伺服器上執行。
- 有了「證書權限 (CA)」，SSL 加密才有作用。

2.3 升級至 Identity Manager 3

在安裝 Identity Manager 期間，您可以在 Metadirectory 引擎安裝完成後，同時安裝 Driver for eDirectory (和其他 Identity Manager 驅動程式一併安裝)。請參閱《*Identity Manager 3.0 安裝指南*》。您可以從 DirXML 1.1a 或 Identity Manager 2 升級至 Identity Manager 3。

2.4 安裝驅動程式 Shim

在安裝 Metadirectory 引擎的同時，可以安裝 Identity Manager Driver for eDirectory Shim (與其他的 Identity Manager 驅動程式一併安裝)。

您也可以先在 Metadirectory 引擎安裝完成後，另行安裝驅動程式。本章節假設您已在伺服器上安裝 Metadirectory 引擎 (可能還有其他驅動程式)，並且只需要安裝 eDirectory 驅動程式。

若沒有 CD，請下載您的平台所需的檔案 (例如，Identity_Manager_3_Linux_NW_Win.iso)，並儲存成一片 CD。下載檔案位於 [Novell 下載 \(http://download.novell.com/index.jsp\)](http://download.novell.com/index.jsp)。

重要：因為要在兩個不同的 Identity Vault (eDirectory) 伺服器上安裝驅動程式，所以您必須按部就班一個個地完成每個伺服器的安裝程序。

安裝期間，請將 NdsToNds.jar 複製到適當的目錄。下表顯示每個平台的相關位置：

作業系統	目錄
Linux*、Solaris* 或 AIX*	/usr/lib/dirxml/classes (若是 eDirectory 8.8，目錄則為：opt/novell/eDirectory/lib/dirxml/classes)
NetWare®	sys:system\lib
Windows* NT*/2000	預設值為 novell\nds，但您可以指定任何目錄。

程式安裝完成後，請依「[設定 Identity Manager 資料傳送的安全性](#)」，第 23 頁」的說明設定安全性。

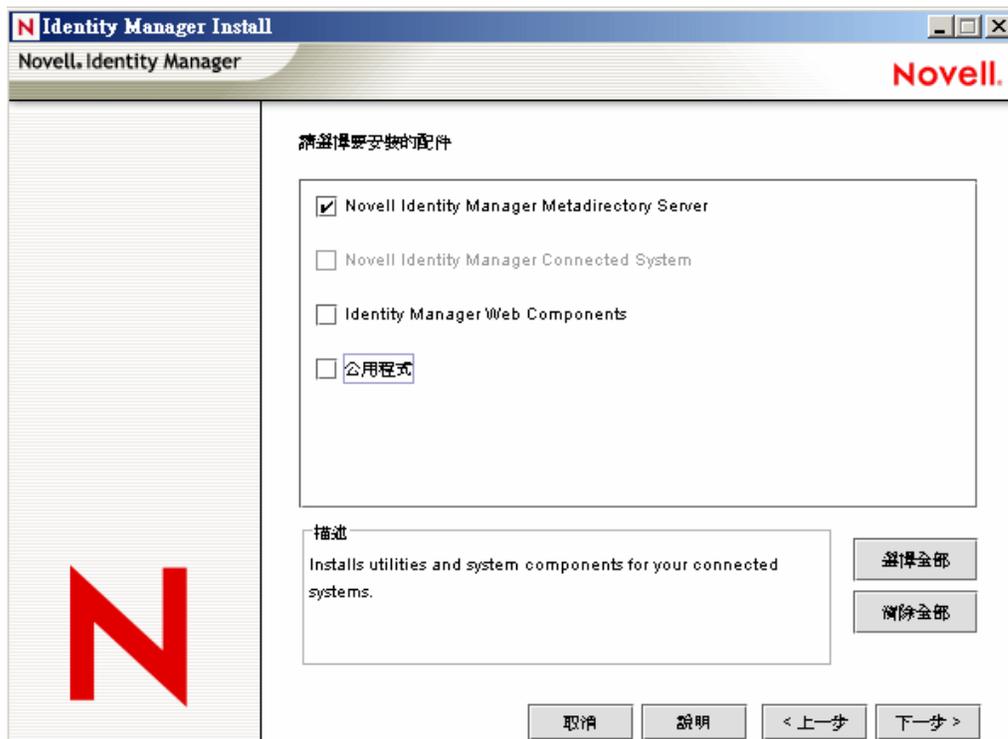
2.4.1 安裝至 Windows

- 1 請執行 Identity Manager 3.0 CD 的安裝程式。

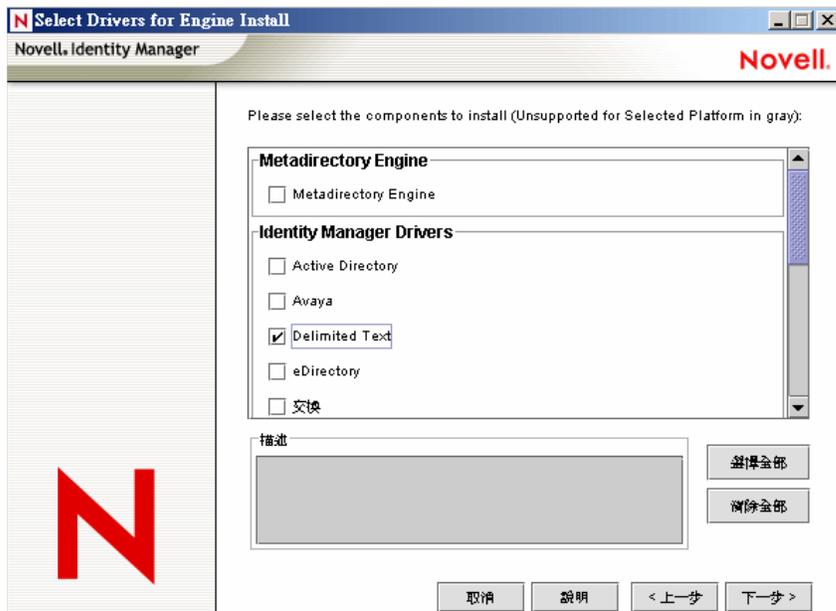
若安裝程式未自動執行，您可以執行 \nt\install.exe。

- 2 在「歡迎」對話方塊中，按「下一步」，然後接受授權合約。
- 3 在第一個「Identity Manager 概觀」對話方塊中，檢視資訊，然後按「下一步」。
對話方塊會提供下列資訊：
 - ◆ Metadirectory 伺服器
 - ◆ 連接的伺服器系統
- 4 在第二個「Identity Manager 概觀」對話方塊中，檢視資訊，然後按「下一步」。
對話方塊會提供下列資訊：
 - ◆ Web 型態的管理伺服器
 - ◆ Identity Manager 公用程式

- 5 在「請選擇要安裝的元件」對話方塊中，只選取「Metadirectory 伺服器」，然後按「下一步」。



- 6 在「選取要安裝的引擎驅動程式」對話方塊中，只選取「eDirectory」，然後按「下一步」。



- 7 在「Identity Manager 升級警告」對話方塊中，按一下「確定」。
- 8 在「摘要」對話方塊中，檢視所選取的選項，然後按一下「完成」。

9 在「安裝完成」對話方塊中，按一下「關閉」。

程式安裝完成後，請依照「[設定驅動程式](#)」，[第 27 頁](#)的說明設定驅動程式。

2.4.2 安裝至 NetWare

1 在 NetWare 伺服器上，插入 Identity Manager CD，然後裝上 CD 作為卷冊。

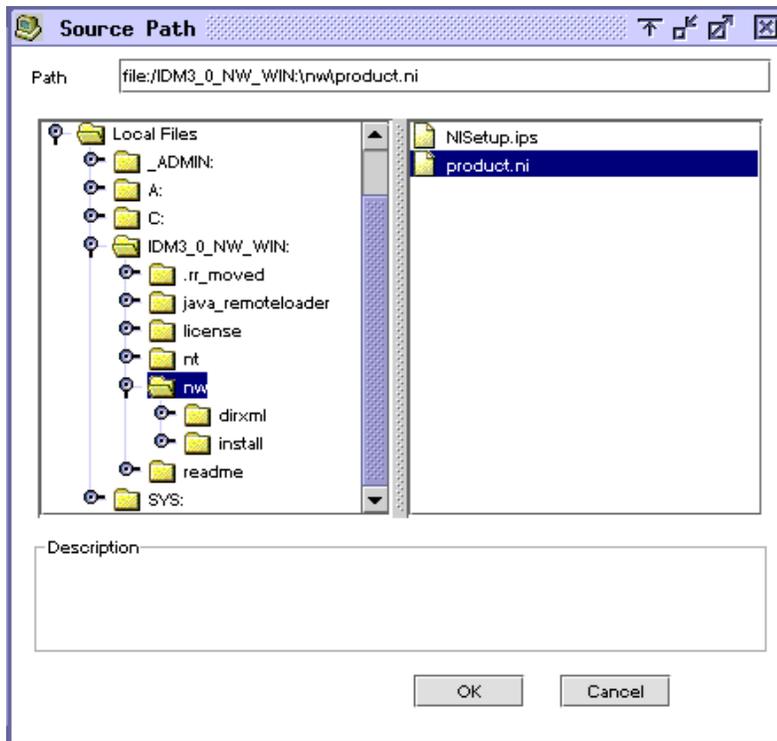
若要裝上 CD，請輸入 `m cdrom`。

2 (視情況) 若無法載入圖形化公用程式，請輸入 `startx` 來載入。

3 在圖形化公用程式中，按一下「Novell」圖示，然後按一下「安裝」。

4 在「已安裝的產品」對話方塊中，按一下「新增」。

5 在「來源路徑」對話方塊中，瀏覽並選取「`product.ni`」檔案。

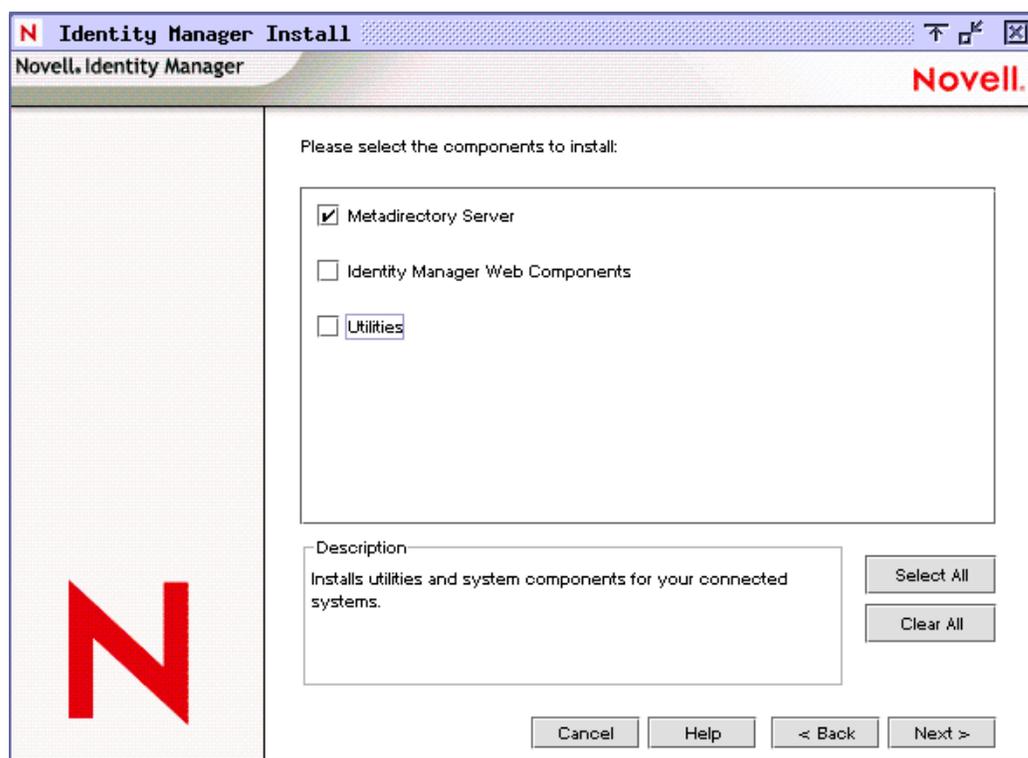


5a 瀏覽並且展開先前已裝上的 CD 卷冊 (Identity_Manager_3_Linux_NW_WIN)。

5b 展開「`nw`」目錄，選取「`product.ni`」，然後按兩次「確定」。

6 在「歡迎使用 Novell Identity Manager 3.0 安裝程式」對話方塊中，按「下一步」，然後接受授權合約。

7 在「安裝 Identity Manager」對話方塊中，只選取「Metadirectory 伺服器」。

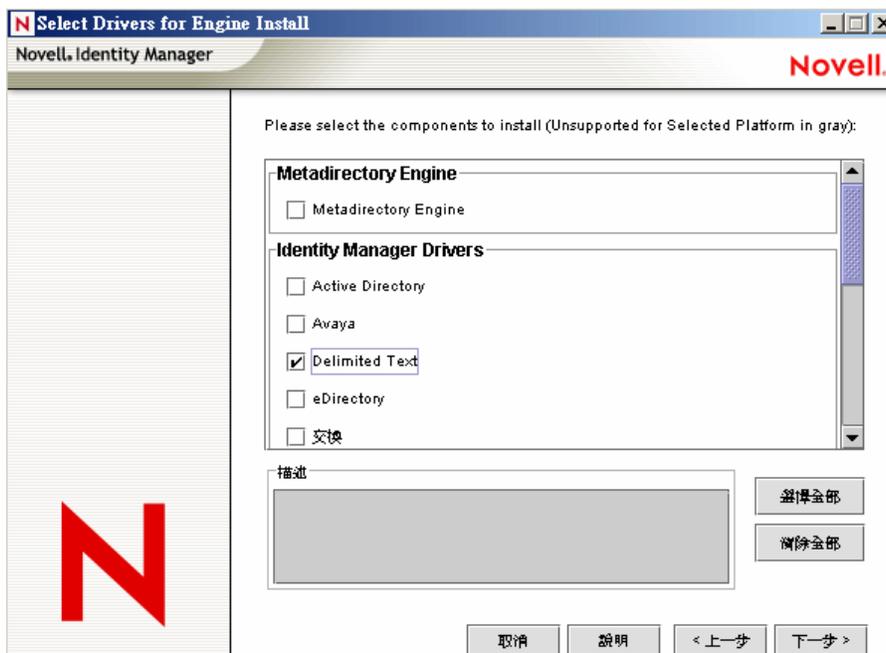


取消選取下列選項：

- ◆ Identity Manager Web 元件
- ◆ 公用程式

8 按「下一步」。

- 9 在「選取要安裝的引擎驅動程式」對話方塊中，只選取「eDirectory」。



取消選取下列選項：

- ◆ Metadirectory 引擎
- ◆ eDirectory 之外的所有驅動程式

- 10 在「Identity Manager 升級警告」對話方塊中，按一下「確定」。
對話方塊建議您在 90 天內啟用驅動程式的授權。
- 11 在「摘要」頁面中，檢視所選取的選項，然後按一下「完成」。
- 12 按一下「關閉」。

程式安裝完成後，請依照「設定驅動程式」，第 27 頁的說明設定驅動程式。

2.4.3 安裝至 Linux、Solaris 或 AIX

根據預設，當您在安裝 Metadirectory 引擎時，Identity Manager Driver for eDirectory 就已經安裝完成。若當時驅動程式未安裝完成，本章節將協助您進行安裝。

執行安裝程式的過程中，輸入「previous」即可回到上一個步驟（畫面）。

- 1 在終端機會期中，以 root 登入。
- 2 插入 Identity Manager CD，然後將其裝上。

一般而言，CD 會自動裝上。下表列出手動裝上 CD 的範例。而真正要輸入何指令，取決於系統的設定方式以及作業系統：

平台	輸入的內容
AIX* 或 Red Hat*	mount /mnt/cdrom，然後按 Enter

平台	輸入的內容
Solaris	mount /cdrom，然後按 Enter
SUSE®	mount /media/cdrom，然後按 Enter，或 mount /media/dvd，然後按 Enter

3 變更至設定目錄。

例如，變更至 *mount point/platform/setup*

- ◆ *mount point* 為 CD/DVD 裝上的位置。
- ◆ *platform* 為平台的名稱 (solaris、linux 或 aix)。

4 執行安裝程式。

例如，對於 Linux 請輸入「./dirxml_linux.bin」。

5 在「簡介」區段中，按 Enter。

6 接受授權合約。

按著 Enter，直到顯示「您是否接受授權合約條款」後，輸入 y，然後按 Enter。

```

File Edit Settings Help
obtain a copy from your local Novell office.
U.S. Government Restricted Rights. Use, duplication, or disclosure by the U.S.
Government is subject to the restrictions in FAR 52.227-14 (June 1987)
Alternate III (June 1987), FAR 52.227-19 (June 1987), or DFARS 252.227-7013
(b)(3) (Nov 1995), or applicable successor clauses. Contractor/ Manufacturer is
Novell, Inc., 1800 South Novell Place, Provo, Utah 84606.

PRESS <ENTER> TO CONTINUE:

Other. The application of the United Nations Convention of Contracts for the
International Sale of Goods is expressly excluded.

(c)1993, 2000-2003 Novell, Inc. All Rights Reserved.

Novell is a registered trademark and eDirectory and Nsure are trademarks of
Novell, Inc. in the United States and other countries.

DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT? (Y/N): y

```

7 在「選擇安裝集」區段中，選取「自定」選項。

輸入 4，然後按 Enter。

```
File Edit Settings Help
=====
Choose Install Set
-----

Please choose the Install Set to be installed by this installer.

->1- DirXML Server
   2- DirXML Connected System Server
   3- Web-based Administrative Server

   4- Customize...

ENTER THE NUMBER FOR THE INSTALL SET, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
: 4
```

- 8 在「選擇產品功能」區段中，取消選取「eDirectory」以外的所有功能，然後按 Enter。若要取消選取某項功能，請輸入該功能之編號。在您取消選取的其他功能之間輸入逗號。

```
Session Edit View Bookmarks Settings Help
-----
Choose Product Features
-----

ENTER A COMMA SEPARATED LIST OF NUMBERS REPRESENTING THE FEATURES YOU WOULD
LIKE TO SELECT, OR DESELECT. TO VIEW A FEATURE'S DESCRIPTION, ENTER
'?<NUMBER>'. PRESS <RETURN> WHEN YOU ARE DONE:

   1-  Metadirectory Engine
   2-  Remote Loader
   3-  eDirectory Driver
   4-  Delimited Text Driver
   5-  Groupwise Driver
   6-  JDBC Driver
   7-  LDAP Driver
   8-  Notes Driver
   9-  SAP Driver
  10-  AVAYA Driver
  11-  REMEDY Driver
  12-  SOAP Driver
  13-  Identity Manager Plugins
  14-  Identity Manager Policies

Please choose the Features to be installed by this installer.
: 1,4,5,6,7,8,9,10,11,12
```

- 9 在「預先安裝摘要」區段中，檢視選項。

```
=====
Pre-Installation Summary
-----

Please Review the Following Before Continuing:

Install Set
  Custom

Product Components:
  eDirectory Driver

PRESS <ENTER> TO CONTINUE: █
```

若要返回上一個步驟，請輸入「previous」，然後按 Enter。

若要繼續，請按 Enter。

10 安裝完成後，按 Enter 結束安裝。

程式安裝完成後，請依照「[設定驅動程式](#)」，[第 27 頁](#)的說明設定驅動程式。

2.5 啓用驅動程式

在安裝後 90 天內啓用驅動程式。否則，驅動程式將停止執行。

如需啓用之相關資訊，請參閱《[Identity Manager 3.0 安裝指南](#)》中的「[啓動 Novell Identity Manager 產品](#)」。

升級 Identity Manager Driver for eDirectory

- 「準備升級」，第 17 頁
- 「升級驅動程式 Shim」，第 17 頁
- 「升級驅動程式組態」，第 18 頁
- 「eDirectory 驅動程式的升級問題」，第 18 頁

3.1 準備升級

請確定您已檢查過目前所用驅動程式所有的 TID 及產品更新。

如果您的驅動程式 Shim 及組態皆已安裝最新的修正程式，基本上新的驅動程式 Shim 就會配合您現有的驅動程式組態（不經任何變更）運作。

3.2 升級驅動程式 Shim

- 1 請確定您已使用所有的修補程式為目前正在執行的驅動程式進行更新。

為了有助於將升級時的問題降至最低，建議您先在所有驅動程式完成這個步驟。

- 2 安裝新的驅動程式 Shim。

您可以在安裝 Metadirectory 引擎的同時執行此步驟，或安裝完該引擎之後再執行。請參閱「[安裝驅動程式 Shim](#)」，第 7 頁。

升級時，新的驅動程式 Shim 會取代先前的驅動程式 Shim，但會保留先前驅動程式的組態。

- 3 安裝完 Shim 之後，請重新啟動驅動程式。

3a 在 iManager 中，選取「*Identity Manager*」>「*Identity Manager* 概觀」。

3b 瀏覽至存放驅動程式的驅動程式集。

3c 選取要重新啟動的驅動程式，按一下狀態圖示，然後選取「啟動驅動程式」。



- 4 (條件式) 利用您的 Identity Manager 啓用身分證明來啓用驅動程式 Shim。

您只要針對每組驅動程式集啓用一次，而無須針對每個驅動程式。您很可能已經啓用驅動程式集，所以可以略過此步驟。

如需啓用之相關資訊，請參閱《[Identity Manager 3.0 安裝指南](#)》中的「[啓用 Novell Identity Manager 產品](#)」。

驅動程式 Shim 安裝完成後，請升級驅動程式組態。請參閱「[升級驅動程式組態](#)」，第 18 頁。

3.3 升級驅動程式組態

重要：本章節的內容只適用於從 DirXML® 1.x 進行的升級。

因為您正在兩個不同的 Identity Vault 伺服器上升級驅動程式，所以必須先完成每個伺服器的升級程序。

安裝驅動程式 Shim 不會變更現有的組態。現有的組態會繼續與新的安裝驅動程式 Shim 一起運作。

然而，若要利用新功能，就必須升級驅動程式組態，您可以利用新的範例組態來取代驅動程式組態，或是將現有的組態為 Identity Manager 3 格式，並為其新增規則。

- ◆ 若要取代現有的組態，請輸入現有驅動程式物件的新範例組態。

範例組態包含所有新功能，例如「Identity Manager 密碼同步化」及「角色授權」功能。

- ◆ 若要轉換現有的驅動程式組態，以使用新的 Identity Manager 外掛程式加以編輯，請參閱《[Novell Identity Manager 3.0 管理指南](#)》中的「[將驅動程式組態從 DirXML 1.1a 升級至 Identity Manager 格式](#)」。
- ◆ 若要新增「Identity Manager 密碼同步化」功能至現有的驅動程式組態，請參閱《[Novell Identity Manager 3.0 管理指南](#)》中的「[升級現有的驅動程式組態以支援密碼同步化](#)」。

新的密碼同步化規則支援「通用密碼」和「配送密碼」。若您只想同步化「NDS® 密碼」，則不應該新增這些規則至驅動程式組態。可使用「公用金鑰」及「私密金鑰」屬性取代這些規則，同步化「NDS 密碼」。

3.4 eDirectory 驅動程式的升級問題

重要：本章節僅適用於從 DirXML 1.x 進行升級。

若您正在升級 Identity Manager 和 eDirectory 驅動程式，當證書過期時（或其中一種證書已過期），可能會遭遇資料同步化錯誤。

若在持有有效證書的伺服器上建立使用者，則該使用者將不會同步化至持有無效證書的伺服器。此外，您可能會在 DSTrace 中看見下列錯誤：

```
SSL handshake failed, X509_V_CERT_HAS_EXPIRED
```

```
SSL handshake failed, SSL_ERROR_ZERO_RETURN,
```

若在持有過期證書的伺服器上建立使用者，則該使用者仍會同步化至持有有效證書的伺服器。此外，您可能會在 DSTrace 中看見下列錯誤：

```
Error: 14094415: SSL Routines: SSL_READ_BYTES: sslv3 alert certificate
```

expired.

若要解決此問題，請建立新的證書。

驅動程式組態檔案範例

- ◆ 「輸入驅動程式組態範例」，第 21 頁
- ◆ 「設定 Identity Manager 資料傳送的安全性」，第 23 頁
- ◆ 「哪些屬性已同步化」，第 25 頁
- ◆ 「密碼同步化」，第 25 頁

4.1 輸入驅動程式組態範例

- ◆ 「使用 iManager 輸入」，第 21 頁
- ◆ 「使用 Designer for Identity Manager 輸入」，第 22 頁

4.1.1 使用 iManager 輸入

- 1 建立新的驅動程式，或輸入組態 eDirectory.xml 至現有的驅動程式。

在 Novell iManager 中，選取「Identity Manager 公用程式」，然後使用《*Novell Identity Manager 3.0 管理指南*》中，「管理 Identity Manager 驅動程式」所描述的其中一個任務。

- 2 遵循「設定 Identity Manager 資料傳送的安全性」，第 23 頁內的指示設定驅動程式組態。

精靈會提示您提供下列資訊：

項目	描述
遠端網路樹位址與連接埠	指定 DNS 主機名稱或 IP 位址，以及遠端網路樹中 Identity Manager 伺服器的連接埠。例如： 151.155.144.23:8196 hostname:8196
設定資料流程	雙向 ：兩個 eDirectory™ 網路樹為兩者之間資料同步化的授權來源。 授權的 ：本地網路樹為授權的來源。 從屬 ：本地網路樹不是授權的來源。

項目	描述
組態選項	<p>鏡像複製：階層式同步化本地與遠端網路樹之間的物件。</p> <p>若您選擇此選項，請使用相同的選項來設定正在同步化的兩個 eDirectory 網路樹。</p> <p>驅動程式組態中的這個選項會同步化「使用者」、「群組」、「組織」、「國家」以及「組織單位」物件。也會鏡像複製其他網路樹中子網路樹的結構。</p> <p>平面：同步化所有「使用者」及「群組」至特定的容器。</p> <p>此選項會同步化「使用者」及「群組」物件，並將所有使用者置於一個容器，而所有群組則置於另一個容器。</p> <p>此選項通常會與其他網路樹中的「部門」選項（或類似的組態）結合使用。</p> <p>此選項不會建立含有使用者和群組的容器。您必須手動建立這些容器。</p> <p>部門：依部門 (OU) 同步化使用者及群組。</p> <p>此選項會同步化「使用者」及「群組」物件，並且會根據管理主控台 of 「部門」欄位來放置容器中所有的使用者和群組。</p> <p>此組態通常會與其他網路樹中的「平面」選項（或類似的組態）結合使用。</p> <p>此選項不會建立每個部門的容器。您必須手動建立這些容器。這些容器必須與輸入期間所指定的容器相同。</p>
遠端基本容器	<p>僅適用於「鏡像複製」選項。</p> <p>指定遠端網路樹中同步化的基本容器，例如 Users.MyOrganization。</p>
基本容器	<p>僅適用於「鏡像複製」、「平面」及「部門」選項。</p> <p>指定本地網路樹中同步化的基本容器，例如 Users.MyOrganization。</p> <p>若與「鏡像複製」一同使用：利用上述的「遠端基本容器」進行鏡像複製的本地基本容器。</p> <p>若與「平面」一同使用：放入「使用者」的容器。</p> <p>若與「部門」一同使用：部門容器的父代。</p>
群組容器	<p>僅適用於「平面」。</p> <p>指定要放入「群組」的本地網路樹中同步化的基本容器，例如 Groups.MyOrganization。</p>

4.1.2 使用 Designer for Identity Manager 輸入

您可以使用 Designer for Identity Manager 來輸入 eDirectory 的基本驅動程式組態檔案。此基本檔案會建立和設定使驅動程式正確運作所需的物件及規則。

以下程序說明了其中一種輸入範例組態檔案的方式：

- 1 在 Designer 中開啓專案。

- 2 在模組器中，在「驅動程式集」物件上按一下滑鼠右鍵，然後選取「新增已連接的應用程式」。
- 3 從下拉式清單中選取「eDirectory.xml」，然後按一下「執行」。
- 4 在「執行提示驗證」視窗中按一下「是」。
- 5 填寫欄位，設定驅動程式組態。
指定您環境特定相關的資訊。如需設定值相關資訊，請參閱**步驟 2, 第 21 頁**中的表格。
- 6 指定參數後，按一下「確定」以輸入驅動程式。
- 7 自定及測試驅動程式。
- 8 部署驅動程式至 Identity Vault。
請參閱《*Designer for Identity Manager 3：管理指南*》中的「**部署專案至 Identity Vault**」。

4.2 設定 Identity Manager 資料傳送的安全性

所有 eDirectory 驅動程式通訊都受 SSL 保護。若要設定 eDirectory 系統組態來處理 Identity Manager 資料傳送的安全性，請執行 Novell iManager 中的 NDS2NDS 精靈。

- ◆ 「了解 eDirectory 驅動程式的安全性」，第 23 頁
- ◆ 「設定 KMO」，第 24 頁

4.2.1 了解 eDirectory 驅動程式的安全性

下列項目可協助您了解 eDirectory 驅動程式的安全性：

- ◆ 驅動程式會使用 SSL 插槽提供驗證及安全連接。SSL 使用數位證書讓使用者能連接至 SSL，以驗證其他使用者。Identity Manager 交互使用 Novell Certificate Server 證書，對機密資料進行安全管理。
- ◆ 若要使用驅動程式，您必須讓 Novell Certificate Server 在每個網路樹中執行。建議您使用來自其中一個含有驅動程式之網路樹的「證書權限」，發出用於 SSL 的證書。若網路樹沒有「證書權限」，您必須先建立一個。您可以使用外部「證書權限」。
- ◆ Novell 在實作驅動程式所使用的 SSL 時，是根據 eDirectory 的「Novell 保全驗證服務」(Novell Secure Authentication Services, SAS) 及 eDirectory 8.7.x 的 NTLS。這些必須在執行驅動程式的伺服器上安裝及設定。eDirectory 通常會自動執行這個動作。
- ◆ 若要設定驅動程式的安全性，必須建立和參考會利用驅動程式來連接 eDirectory 網路樹的證書。由於物件安全地包含兩個證書資料 (包括公用金鑰) 以及與證書相關的私密金鑰，所以 eDirectory 中的證書物件通稱為「金鑰材料物件」(Key Material Objects, KMO)。

您必須至少建立兩個 KMO (每個網路樹一個 KMO)，才能與 Identity Manager Driver for eDirectory 搭配使用。本章節說明使用每個網路樹的單一 KMO。

「NDS2NDS 驅動程式證書精靈」會設定 KMO。

- ◆ 如需詳細資訊：
 - ◆ 如需 Novell Certificate Server 的綜覽，請參閱 [Novell Certificate Server 線上文件 \(http://www.novell.com/documentation/crtsrv20/index.html\)](http://www.novell.com/documentation/crtsrv20/index.html)。

- ◆ 如需更詳細的 CA 資訊，以及網路樹內有關「證書權限」的設定資訊，請參閱設定 Novell PKI 服務 (<http://www.novell.com/documentation/lg/ndsse/ndsseenu/data/h6172k4q.html>)。

4.2.2 設定 KMO

設定 Identity Vault 系統以處理安全的 Identity Manager 資料傳送：

- 1 找出目的伺服器的網路樹名稱或 IP 位址。
- 2 啓動 iManager，並驗證您的第一個網路樹。
- 3 按一下「Identity Manager 公用程式」>「NDS2NDS 驅動程式證書」。
- 4 在「歡迎」頁面上，輸入第一個網路樹的必要資訊。

啓動 iManager 時，會使用所驗證之網路樹內的物件來提供預設值。您必須輸入或確認下列資訊：

- ◆ 驅動程式 DN：輸入 eDirectory 驅動程式的可辨識名稱 (例如，EDir-Workforce.Employee Provisioning.Services.YourOrgName)。
- ◆ 網路樹名稱：指定 Workforce 網路樹的 IP 位址。
- ◆ 具有 Admin 權限之帳戶的使用者名稱 (例如，Admin)。
- ◆ 使用者的密碼。
- ◆ 使用者的網路位置 (例如，Services.YourOrgName)。

- 5 按「下一步」。

精靈會使用所輸入的資訊來驗證第一個網路樹，驗證驅動程式 DN，以及驗證驅動程式是否與伺服器關聯。

- 6 指定第二個網路樹的必要資訊。

在「歡迎」頁面上，輸入第一個網路樹的必要資訊。

指定或確認下列資訊：

- ◆ 驅動程式 DN：輸入 eDirectory 驅動程式的可辨識名稱 (例如，EDir-Account.DriverSet.YourOrgName)。
- ◆ 網路樹名稱：輸入 Account 網路樹的網路樹名稱或 IP 位址。
- ◆ 具有 Admin 權限之帳戶的使用者名稱 (例如，Admin)。
- ◆ 使用者的密碼。
- ◆ 使用者的網路位置 (例如，London.YourOrgName)。

- 7 按「下一步」。

精靈會使用所輸入的資訊來驗證第二個網路樹，驗證驅動程式 DN，以及驗證驅動程式是否與伺服器關聯。

- 8 檢視「摘要」頁面上的資訊，然後按一下「完成」。

若這些網路樹已存在 KMO，則精靈會將它們刪除，並執行下列步驟：

- ◆ 在第一個網路樹內輸出 CA 的託管根部。
- ◆ 建立 KMO 物件。
- ◆ 提出證書登記申請。
- ◆ 將證書的金鑰配對名稱放置於驅動程式的「驗證 ID」中。

4.3 哪些屬性已同步化

範例驅動程式組態的過濾器會同步化下列屬性：

accessCardNumber	Initials	preferredDeliveryMethod
ACL	instantMessagingID	preferredName
assistant	internationalISDNNumber	私密金鑰
assistantPhone	網際網路電子郵件位址	公用金鑰
businessCategory	jackNumber	registeredAddress
city	jobCode	roomNumber
CN	L	S
co	語言	SA
公司	信箱 ID	安全性相等
costCenter	信箱位置	安全性旗標
costCenterDescription	mailstop	並請參閱
departmentNumber	管理員	siteLocation
描述	managerWorkforceID	姓
destinationIndicator	行動	電話號碼
directReports	NSCP:employeeNumber	teletexTerminalIdentifier
電子郵件地址	otherPhoneNumber	telexNumber
employeeStatus	O	Timezone
employeeType	OU	職稱
等值於我	呼叫器	tollFreePhoneNumber
傳真號碼	personalTitle	UID
全名	相片	uniqueID
親代識別字	實際交付貨品的辦公室名稱	vehicleInformation
名	郵寄地址	workforceID
群組成員	郵遞區號	x121Address
較高權限	郵政信箱	x500UniqueIdentifier

4.4 密碼同步化

本章節內含 Identity Manager Driver for eDirectory 特定所需的資訊，並假設您已熟悉《*Novell Identity Manager 3.0 管理指南*》內的「實作密碼同步化」。

- ◆ 驅動程式 Shim 仍舊如同在舊版程式中運作。在 Identity Manager 2.0 中，新的規則被加入範例驅動程式組態中，以支援 Identity Manager 密碼同步化，包括「通用密碼」的同步化。

- ◆ 若您決定要在多個網路樹中強制執行密碼規則，請確定密碼規則內的「進階密碼規則」與每個網路樹相容，如此才能夠成功的執行密碼同步化。

若在多個 eDirectory 網路樹內強制執行不相容的密碼規則，並選擇若未遵守則將密碼重設 (使用「如果密碼不一致，請將使用者的密碼重設為配送密碼，藉此在已連接系統上強制執行密碼規則」選項)，可能會發生每個 Identity Vault 伺服器皆嘗試變更不相容密碼的迴路情形。

如需密碼規則的相關資訊，請參閱《密碼管理指南 (http://www.novell.com/documentation/password_management/index.html)》中的「使用密碼規則管理密碼」。

- ◆ 若驅動程式的過濾器在「公用金鑰」和「私密金鑰」屬性中設定為「同步化」，則 NDS® 的密碼會在網路樹之間進行同步化，而不管您已建立哪些其他設定值。
若您想要使用「通用密碼」來同步化密碼，請在希望同步化「通用密碼」的所有類別上，將 eDirectory 驅動程式上的過濾器設定成「忽略」、「公開金鑰」和「私密金鑰」屬性。
- ◆ 若要新增 Identity Manager 密碼同步化功能至現有的驅動程式組態，請參閱《*Novell Identity Manager 3.0 管理指南*》中的「升級現有的驅動程式組態以支援密碼同步化」。新的密碼同步化規則支援「通用密碼」和「配送密碼」。若您只想同步化「NDS 密碼」，則這些規則不應該新增至驅動程式組態。可使用公用金鑰及私密金鑰屬性取代這些規則，以同步化「NDS 密碼」。
- ◆ 若「密碼規則」已啟用「通用密碼」，並且未選取同步化「通用密碼」與「NDS 密碼」的設定時，則 iManager 內的「檢查密碼狀態」任務不會在已連接的系統上運作。「檢查密碼狀態」任務可讓您查看，在 Identity Manager 內使用者的密碼是否已與連接系統的密碼同步化。

若您正在使用 Identity Manager Driver for eDirectory，並且使用者密碼規則在「組態選項」索引標籤中的指定如下：「通用密碼」更新時「NDS 密碼」不應被更新，則該使用者的「檢查密碼狀態」任務永遠會顯示該密碼未經過同步化。即使在連接系統上，Identity Manager 的「配送密碼」與「通用密碼」實際上是相同的，密碼狀態還是會顯示為未同步化。

這是因為 Identity Vault 檢查密碼功能會在此時檢查「NDS 密碼」，而不是透過 NMAST™ 來參考「通用密碼」。

根據預設，「NDS 密碼」會在密碼規則內的「通用密碼」更新時被更新。若您選取此選項，則「檢查密碼狀態」應會是連接系統的正確狀態。

- ◆ 若要使用驅動程式，您必須讓 Novell® Certificate Server™ 在每個代管驅動程式的伺服器上執行。您必須也建立「證書權限 (CA)」，SSL 的加密才有作用。我們的建議是，由包含驅動程式的其中一個網路樹之「證書權限」發出用於 SSL 的證書。若您的網路樹沒有「證書權限」，請先建立一個。您可以使用外部「證書權限」。

如需建立 CA 和設定 Certificate Server 的詳細指示，請參閱「設定 Identity Manager 資料傳送的安全性」，第 23 頁。

設定驅動程式

- ◆ 「設定驅動程式物件內容」，第 27 頁
- ◆ 「設定過濾器」，第 29 頁
- ◆ 「設定發行者通道上的規則」，第 30 頁
- ◆ 「使用驅動程式物件密碼」，第 30 頁

如需密碼同步化的相關資訊，請參閱「密碼同步化」，第 25 頁。

5.1 設定驅動程式物件內容

一般而言，驅動程式的內容會在您輸入驅動程式組態檔並執行「證書精靈」時，自動設定。

若要手動設定內容：

- 1 在 iManager 中，按一下「*Identity Manager*」>「*Identity Manager* 概觀」。
- 2 找出包含 eDirectory™ 驅動程式的驅動程式集，然後按一下驅動程式的圖示。
- 3 從「*Identity Manager* 驅動程式概觀」頁面，按一下「eDirectory 驅動程式」物件，其中將顯示驅動程式的組態。
- 4 找出「驅動程式模組」區段，然後選取「Java」。

驅動程式模組

- Java
- 本地
- 連接至遠端載入器

名稱：

com.novell.nds.dirxml.driver.nds.DriverShimImpl

- 5 在「名稱」編輯方塊中，輸入下列 eDirectory 驅動程式的 Java 類別名稱：

com.novell.nds.dirxml.driver.nds.DriverShimImpl

- 6 設定參數。

5.1.1 驗證參數

驗證

us-linux-srv.novell

驗證 ID:	<input type="text" value="eDirectory Driver(us_linux_srv_kmo)"/>
驗證網路位置:	<input type="text" value="10.2.30.165:8196"/>
遠端載入器連接參數:	<input type="text" value="<不是遠端載入器>"/>
驅動程式快取限制 (千位元組):	<input type="text" value="0"/>
應用程式密碼:	設定密碼
遠端載入器密碼:	<不是遠端

應用程式密碼

輸入密碼:

重新輸入密碼:

啟動選項

us-linux-srv.novell

自動開始
 手動
 關閉

提供讓來源伺服器與目的伺服器通訊的資訊。

驗證 ID

若您希望來源伺服器和目的伺服器交換安全資訊 (例如密碼)，請執行「NDS2NDS eDirectory 證書精靈」。此精靈會建立「金鑰材料物件 (KMO)」，並將正確的 KMO 名稱放置在「驗證 ID」欄位中。

KMO 為保全插槽層 (SSL) 證書：



驗證網路位置

在「驗證網路位置」欄位中，輸入目的伺服器的主機名稱或 IP 位址，以及十進制的連接埠編號 (例如，187.168.1.1:8196)。

附註：若您看到「"java.net.ConnectException: Connection Refused," no port connection is available on the remote side」，此項錯誤可能由下列其中一項所造成：

- ◆ 遠端的驅動程式未執行。
- ◆ 驅動程式正在執行，但設定為使用不同的連接埠。

遠端載入器連接參數

Identity Manager Driver for eDirectory 不需要「遠端載入器」選項 (也未使用)。

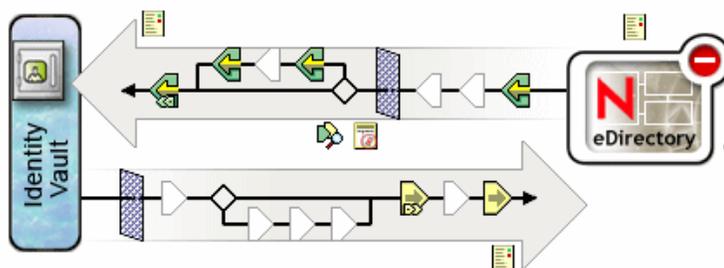
驅動程式快取限制

除非「Novell 支援中心」(Novell Support) 要求，否則請勿修改此欄位。

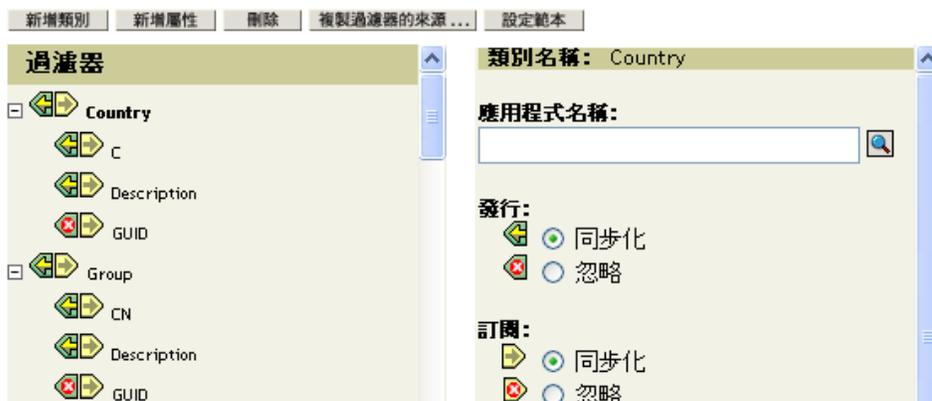
5.2 設定過濾器

一個過濾器可以控制「發行者」和「訂閱者」通道。您應該修改過濾器，使其包含要在 Identity Manager 處理過程中使用的物件類別和屬性。若要修改過濾器：

- 1 在 iManager 中，按一下「Identity Manager」>「Identity Manager 概觀」。
- 2 找出包含 eDirectory 驅動程式的驅動程式集，然後按一下驅動程式的圖示，以顯示「Identity Manager 驅動程式概觀」頁面。
- 3 按一下「發行者」通道上的過濾器。



- 4 自定驅動程式。



在此例中，「國家」和「群組」是類別。若要新增類別，請按一下「新增類別」，然後選取類別。若要刪除類別，請選取該類別，然後按一下「刪除」。

在此例中，「CN」是「群組」類別的屬性。若要新增屬性，請選取該類別，按一下「新增屬性」，然後選取屬性。

若要修改類別或屬性，請選取該類別或屬性，然後選取右窗格中的選項。在此例中，「國家」屬性會在「發行者」和「訂閱者」通道上同步化。不過，GUID 屬性不會在「發行者」通道上同步化。

若要同步化 GUID 屬性，請選取該屬性，然後在「發行」區段中按一下「同步化」。對於「訂閱者」通道上設定為「同步化」的所有類別而言，GUID 屬性是必要屬性。

一般而言，除了 GUID 屬性之外，某一個網路樹內的「訂閱者」通道過濾器應符合其他網路樹內的「發行者」通道過濾器，反之亦然。

- 5 按一下「套用」，然後再按一下「確定」。

5.3 設定發行者通道上的規則

驅動程式上的規則通常應該只放置於「發行者」物件上，而不是在「訂閱者」物件上。「相符」和「佈置」規則無法正確地在「訂閱者」通道上運作，因為「訂閱者」通道主要扮演其他網路樹之「發行者」通道的事件來源的角色。

某些時候需要在「訂閱者」通道上放置「事件轉換」或「建立規則」，以防止在通道上傳送不必要的資料。請參閱《*Identity Manager 3.0 安裝指南*》內的「[使用範圍過濾管理不同伺服器上的使用者](#)」。

5.4 使用驅動程式物件密碼

除了使用 SSL 所需的強制證書之外，對於其他的安全性，您需要設定驅動程式，以使網路樹上的「訂閱者」通道能夠驗證遠端網路樹上的「發行者」通道。位於每個網路樹內的驅動程式物件密碼，必須設定為與其他網路樹中的應用程式密碼相符。

若要在網路樹中設定「Identity Manager 驅動程式」物件密碼：

- 1 在 iManager 中，按一下「*Identity Manager*」>「*Identity Manager* 概觀」。
 - 2 找出包含 eDirectory 驅動程式的驅動程式集，然後按一下驅動程式的圖示。
 - 3 從「Identity Manager 驅動程式概觀」頁面中，按一下 eDirectory 驅動程式物件。
 - 4 選取「驅動程式組態」。
- 視 iManager 的版本和您的環境而定，您可從下拉式清單或索引標籤中選取。
- 5 找出「驅動程式物件密碼」區段。

驅動程式物件密碼

驅動程式物件密碼: [設定密碼](#)

驗證

us-linux-srv.novell

驗證 ID:

驗證網路位置:

遠端載入器連接參數:

驅動程式快取限制 (千位元組):

驅動程式密碼

輸入密碼:

重新輸入密碼:

確定 取消

- 6 輸入驅動程式物件密碼。

重要：在設定了驅動程式物件密碼後，便無法移除該密碼。

7 在「驗證」區段中，輸入應用程式密碼。

驗證

us-linux-srv.novell

驗證 ID:	eDirectory Driver(us_linux_srv_kmo)
驗證網路位置:	10.2.30.165:8196
遠端載入器連接參數:	<不是遠端載入器>
驅動程式快取限制 (千位元組):	0
應用程式密碼:	設定密碼
遠端載入器密碼:	<不是遠端載入器>

啟動選項

us-linux-srv.novell

自動開始
 手動
 關閉

應用程式密碼

輸入密碼:

重新輸入密碼:

8 按一下「套用」，再按一下「確定」。

5.5 移轉或複製物件

雖然 iManager 沒有「複製」功能，但您可以使用「從 eDirectory 移轉」選項，將物件從某個 eDirectory 網路樹複製到另一個 eDirectory 網路樹。複製的範圍，視驅動程式的規則而定。例如，依據套用到驅動程式的規則，可以將所有的屬性從某個 eDirectory 網路樹複製（同步）到另一個 eDirectory 網路樹。此類的「複製」需要您跨越網路樹同步化所有的屬性，將物件放在同一個位置，在移轉期間不得變更任何資料。

時戳永遠會與重新同步化作業關聯。重新同步化操作會尋找已關聯（已被同步化），但在時戳後即已變更的物件。它也會試圖尋找可能在時戳後被建立的物件。按一下「重新同步化」讓新的使用者進行同步化。

若不使用「重新同步化」選項來複製物件，您可以使用「從 eDirectory 移轉」選項。此選項可讓您指定及同步化物件的清單。對於清單內的每個物件，iManager 會將資料寫入目錄中。Identity Manager 會記錄變更，並且為列出的物件啟動同步化程序。

1 請確定來源 eDirectory 網路樹內的伺服器，以及目的 eDirectory 網路樹內的伺服器上，已經安裝了 Identity Manager 3。

2 在來源網路樹內的伺服器上設定 Identity Manager Driver for eDirectory。

在 eDirectory 驅動程式的「驗證」窗格中，提供目的伺服器的名稱或 IP 位址及連接埠。請參閱「設定驅動程式物件內容」，第 27 頁。

選取移轉選項：「平面」、「鏡像複製」或「部門」。若要在將資料從來源網路樹移轉至目的網路樹時保留目錄結構（包括次容器及名稱），請選取「鏡像複製」。

3 在目的網路樹內的伺服器上設定 Identity Manager Driver for eDirectory。

在「驗證」窗格中，提供來源伺服器的名稱或 IP 位址及連接埠。

4 設定兩個網路樹之間的 SSL。

使用「NDS2NDS 精靈」，在兩個網路樹中建立 KMO。請參閱「設定 KMO」，第 24 頁。

若要啓動「NDS2NDS 精靈」，請於 iManager 中選取「Identity Manager 公用程式」>「NDS-to-NDS 驅動程式證書」。

5 在 iManager 中選取「Identity Manager」，按一下「Identity Manager 概觀」，然後按一下驅動程式。

6 選取「從 eDirectory 移轉」。



使用 eDirectory 對 eDirectory 的移轉，從來源網路樹移轉至目的網路樹。

「移轉至 eDirectory」選項不能與 Identity Manager Driver for eDirectory 搭配使用。

7 選取物件。

例如，選取「使用者」物件或「容器」物件。您可以搜尋或瀏覽物件。同時，也可以新增多個物件。

8 按兩次「確定」。

用戶端 (例如，iManager) 會在清單內的每個物件寫入值。此項變更事件會使 Identity Manager 將資料推送至您的目的網路樹。

文件更新

A

本章節包含 Identity Manager Driver for eDirectory 的全新或更新的資訊。

本文件在網路上提供兩種格式：HTML 和 PDF。HTML 和 PDF 文件內容皆保持在最新狀態，包含本章節所列出的文件變更。

若您需要得知所使用的 PDF 文件的副本是否為最新版本，請檢查該 PDF 檔的發行日期。日期位於「法律聲明」一節中，就在標題頁面之後。

A.1 2006 年 5 月 8 日

表格 A-1 變更日期：2006 年 5 月 8 日

位置	變更
「安裝驅動程式 Shim」，第 7 頁	下列兩點已經澄清： <ul style="list-style-type: none">◆ 本章節假設伺服器上已安裝 eDirectory。◆ 本章節將說明如何新增 eDirectory 驅動程式到伺服器中。