Novell Identity Manager Driver for LDAP

1.9.2

www.novell.com

實作指南

2006 年 5 月 25 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。

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 商標之相關資訊，請參閱 Novell 商標與服務清單 (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爲其個別擁有廠商的財產。

目錄

關於本指南

本指南將說明如何安裝及設定 Identity Manager Driver for LDAP。

使用對象

本指南是針對使用 Identity Manager Driver for LDAP 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) 上「Identity Manager 驅動程式」一節中的 *Identity Manager Driver for LDAP*。

其他文件

如需 Identiy 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)。

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 LDAP 簡介

1

1.1 新功能

表格 ***1-1*** 已發行功能之摘要說明

功能	LDAP 驅動程式版本	描述
支援 PasswordModify 延伸操作	1.9	Identity Manager Driver for LDAP 支援 RFC 3062 中定義的「PasswordModify 延伸操作」。 若您正在使用支援 PasswordModify 延伸操作的 LDAP 目錄 (例如 OpenLDAP)，則在設定或修改「訂閱者」通道上的密碼時，Driver for LDAP 會使用延伸操作。 如果 LDAP 目錄不支援 PasswordModify 延伸操作，Driver for LDAP 會依之前驅動程式版本的相同方式，在 UserPassword 屬性上設定一個值。這個值經過雜湊，且會安全儲存 此功能不需要您做任何設定。該驅動程式可以偵測出 LDAP 伺服器是否支援操作。
控制是否將二進位選項 (;Binary) 加入屬性名稱	1.9.2	「訂閱者」通道參數控制是否在爲值編碼時將二進位選項 (;binary) 加入屬性名稱。請參閱「LDAP 訂閱者設定」，第 26 頁。
控制是否將啓始搜尋結果同步化	1.9.2	「LDAP 搜尋」發行方法的參數控制是否將啓始搜尋結果同步化，或只將後續的變更同步化。請參閱「LDAP 發行者設定 僅限 LDAP 搜尋方法」，第 30 頁。

1.2 規劃的更新

未來的更新計劃將加入下列增強功能：

- 支援「發行者」通道「移動」事件
- 當 LDAP 伺服器是 Sun* 目錄時，支援「發行者」通道密碼同步化。

  更新驅動程式及安裝 Sun 目錄外掛程式後，即可獲得此項支援。您可以在 Sun 目錄中安裝及設定外掛程式組態。

1.3 術語的變更

以下是與舊版不同的詞彙：

表格 *1-2* 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)

1.4 驅動程式概觀

Identity Manager Driver for LDAP 會將 Identity Vault 與 LDAP 相容的目錄之間的資料同步化。此驅動程式可以在所有執行 Identity Vault 的平台上執行，包括 Windows*、NetWare® 、Linux*、Solaris* 和 AIX*，也可以在正在執行 Metadirectory 伺服器或 Identity Manager 遠端載入器的任何地方執行。

驅動程式使用輕量目錄存取協定 (Lightweight Directory Access Protocol，LDAP)，以雙向的方式爲 Identity Vault 和連接的 LDAP 相容目錄之間的變更進行同步化。

有了這個彈性的通訊模式，驅動程式就可以和在非 Identity Vault 所支援的平台 (例如 HP-UX*、OS/400 和 OS/390) 上執行之 LDAP 相容的目錄同步化。

驅動程式可以使用下列兩種發行方法之一來辨識資料變更，並透過 Identity Manager 將資料變更傳遞到 Identity Vault。

- changelog 方法

  有變更記錄時，便可使用此方法。變更記錄可在下列位置中找到：

  - Netscape* Directory Server
  - iPlanet* Directory Server
  - IBM* SecureWay Directory
  - Critical Path* InJoin* Directory
  - Oracle* Internet Directory

  請參閱 「LDAP 發行者設定 Changelog 和 LDAP 搜尋方法」，第 27 頁和「LDAP 發行者設定 僅限 Changelog 方法」，第 28 頁。

- LDAP 搜尋方法

  有些伺服器不使用 changelog 機制。LDAP 搜尋方法可讓 LDAP 驅動程式將 LDAP 伺服器相關資料發行到 Identity Vault。

  不需要其他軟體和對 LDAP 相容目錄進行變更。

  請參閱 「LDAP 發行者設定 僅限 LDAP 搜尋方法」，第 30 頁

如需 Identiy 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 的新功能」。

1.5 預設的驅動程式組態

本節討論此驅動程式特有的實作、新增或例外。如需 Identity Manager 基礎的詳細資訊，請參閱 《*Novell Identity Manager 3.0* 管理指南》。

1.5.1 資料流程

本節提供有關控制資料流程的通道、過濾器和規則的相關資訊。

發行者和訂閱者通道

驅動程式支援「發行者」和「訂閱者」通道：

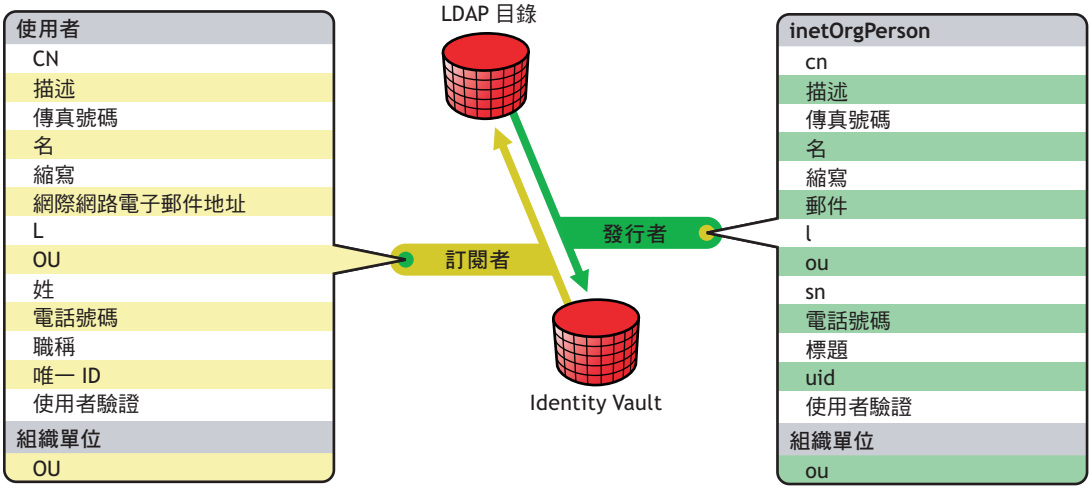
- 「發行者」通道會從 LDAP 目錄變更記錄或 LDAP 搜尋中讀取資訊，並將該資訊透過 Metadirectory 引擎提交到 Identity Vault。

  在預設狀態下，「發行者」通道每 20 秒就會檢查記錄，一次最多可處理 1000 筆，從第一筆未處理的開始算起。
- 「訂閱者」通道會監視 Identity Vault 物件的新增和修改，並發出對 LDAP 目錄做變更的 LDAP 指令。

過濾器

Identity Manager 使用過濾器來控制要共享哪些物件和屬性。預設的 LDAP 驅動程式過濾器組態允許共享物件和屬性，如下圖所示：

特性 ***1-1*** *LDAP* 驅動程式過濾器



規則

規則可用來控制驅動程式與 Identity Vault 之間的資料同步化。LDAP 驅動程式包含兩個可設定規則的預設組態選項。

- 「平面」選項可爲使用者在兩個目錄中實作平面結構。

有了這個組態時，若是在一個目錄中建立使用者物件，這些物件會被放置於您在爲另一個目錄安裝驅動程式期間，所指定之容器的根部。(在 Identity Vault 和 LDAP 目錄中，容器名稱不需要相同。) 更新現有的物件時，其網路位置會被保留。

- 「鏡像複製」選項會使各目錄中的階層式結構都相符。

  有了這個組態時，若是在一個目錄中建立新的使用者物件，這些物件會被放置於另一個目錄中符合鏡像複製容器之階層中。更新現有的物件時，其網路位置會被保留。

除了「佈置」規則以及「平面」組態不與「組織單位」物件同步化的情況以外，爲這些選項設定的規則都是相同的。

下表提供預設規則的相關資訊。這些規則 (Policy) 以及其所包含的個別規則 (Rule)，都可以按照第 4 章 「自定 LDAP 驅動程式。」, 第 25 頁所說明的，透過 Novell iManager 來自定。

表格 ***1-3*** 預設規則

規則	描述
映射	將 Identity Vault「使用者」物件和選取的內容映射到 LDAP inetOrgPerson。 將 Identity Vault Organizational Unit 映射到 LDAP organizationalUnit。 在預設狀態下，有不少的標準內容會被映射。
建立發行者	表示爲了在 Identity Vault 內建立「使用者」，必須定義 cn、sn 和 mail 屬性。爲了建立「組織單位」，必須定義 ou 屬性。
發行者佈置	使用「簡易」佈置選項，在 LDAP 目錄中建立的「使用者」物件會放置於您在輸入驅動程式組態時指定的 Identity Vault 容器中。以 cn 值爲「使用者」物件命名。 使用「鏡像複製」佈置選項，在 LDAP 目錄中建立的「使用者」物件會放置於鏡像複製物件的 LDAP 容器之 Identity Vault 容器中。
相符	表示當電子郵件屬性相符時，Identity Vault 中的使用者物件和 LDAP 目錄中的 inetOrgPerson 相同。
建立訂閱者	表示爲了在 LDAP 目錄中建立使用者，必須定義 CN、Surname 和 Internet Email Address 屬性。爲了建立「組織單位」，必須定義 OU 屬性。
訂閱者佈置	如果您在輸入驅動程式組態期間選擇「平面」佈置選項，在 Identity Vault 中建立的「使用者」物件會以輸入時指定的值爲依據。 如果您在輸入驅動程式組態期間選擇「鏡像複製」佈置選項，在 Identity Vault 中建立的「使用者」物件會放置於鏡像複製物件的 Identity Vault 容器之 LDAP 目錄容器中。

升級

2

2.1 升級驅動程式 Shim

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。新的驅動程式 Shim 可以執行 DirXML® 1.*x* 組態，而無需任何變更。

若要升級驅動程式 Shim，請執行下列動作：

1 請確定已使用目前所執行之驅動程式版本的所有修補程式來更新驅動程式。

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。檢視目前所用驅動程式版本的所有 TID 及產品更新。

爲了有助於將升級時的問題減至最少，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。

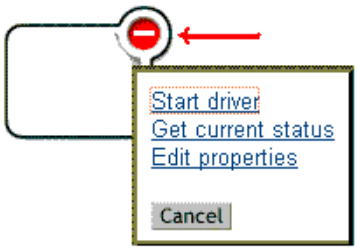
您可以在安裝 Metadirectory 引擎的同時執行此步驟，也可以在安裝該引擎之後再執行。請參閱第 3 章 「安裝 LDAP 驅動程式」, 第 11 頁。

3 安裝 Shim 之後，請重新啓動驅動程式。

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 選取要重新啓動的驅動程式，按一下狀態圖示，然後選取「啓動驅動程式」。



4 使用 Identity Manager 啓用身分證明來啓用驅動程式 Shim。

如需啓用的相關資訊，請參閱《*Identity Manager 3.0* 安裝指南》中的「啓用 Novell Identity Manager 產品」。

安裝驅動程式 Shim 之後，升級驅動程式組態。請參閱「升級驅動程式組態」，第 9 頁。

2.2 升級驅動程式組態

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驅動程式 Shim 一起運作，無需任何變更。

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，或是將現有的組態轉換爲 Identity Manager 格式，並爲其新增規則。

- 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。
- 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」。

安裝 LDAP 驅動程式

3

3.1 規劃考量

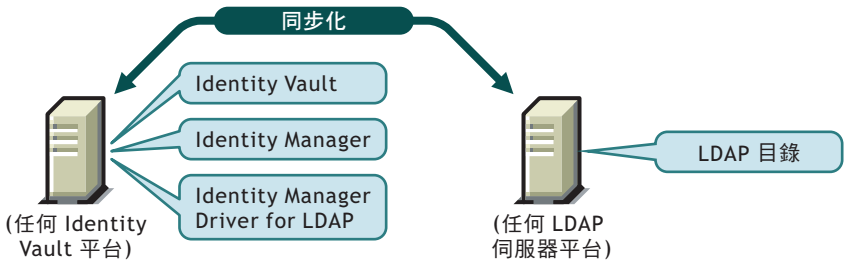
Identity Manager Driver for LDAP 可與大部份 LDAP v3 相容的 LDAP 伺服器一起運作。驅動程式會被寫入用於 LDAP 的 RFC 2251 規格中。如需相容性議題的相關資訊，請參閱「LDAP v3 相容性」，第 39 頁。

3.1.1 LDAP 驅動程式的安裝位置

Identity Manager 驅動程式可安裝在 Identity Vault 和 Metadirectory 引擎所安裝的同一部電腦上。此安裝程序被稱爲本地組態。

如下圖所示，在本地組態中，您會將 LDAP 驅動程式安裝在已安裝 Identity Vault 和 Metadirectory 引擎的同一部電腦上。

特性 ***3-1*** 本地組態



若因爲平台或規則的限制使本地組態無法施行，請在裝載目標應用程式的電腦上安裝 Identity Manager 驅動程式。此安裝程序被稱爲遠端組態。

雖然以遠端組態安裝 LDAP 驅動程式是可行的，但其所提供的額外彈性不大，原因如下：

- 驅動程式可以在任何 Identity Vault 平台上執行。
- 透過 LDAP 協定，驅動程式可以在任何平台上透過網路線與 LDAP 伺服器進行通訊。

3.1.2 升級至 Identity Manager 3

在 Identity Manager 安裝期間，您可以在安裝 Metadirectory 引擎的同時，安裝 Driver for LDAP (與其他 Identity Manager 驅動程式一起)。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。

3.1.3 蒐集資訊

在安裝及設定過程中，系統會提示您提供下列資訊：

- 是否使用「平面」或「鏡像複製」選項，爲階層式結構進行同步化處理。請參閱「規則」，第 7 頁。
- 用來保留同步化物件的 Identity Vault 和 LDAP 目錄容器。
- 要指定爲驅動程式安全性等值的 Identity Vault 使用者物件，以及要從同步化作業排除的物件。
- 用來提供驅動程式存取 LDAP 目錄時所需要的 LDAP 物件和密碼。

請參閱「輸入驅動程式組態範例檔案」，第 21 頁中的表格。

3.1.4 LDAP 資料來源的假設

如果您正利用「發行者」通道將有關 LDAP 目錄中之變更的資料傳送到 Identity Vault，必須要瞭解驅動程式用來發行資料的兩種方法：

- changelog 方法

  變更記錄是 LDAP 目錄中的一種機制。變更記錄可提供該驅動程式相關的 LDAP 事件資訊。有變更記錄時，便可使用此方法。

- LDAP 搜尋方法

  使用此方法可讓 LDAP 驅動程式將不使用變更記錄的 LDAP 伺服器相關資料發行到 Identity Vault。

3.2 系統先決條件

- ❑ Novell® Identity Manager
- ❑ Identity Manager 或更新版本的系統要求
- ❑ 如果您正在使用 changelog 方法，下列其中一個 LDAP 目錄：
  - Netscape Directory Server 4.*x* 或 6
  - iPlanet Directory Server 5.0 或以上版本
  - IBM SecureWay Directory 3.2、4.1.1 或 5.1
  - Critical Path InJoin Directory 3.1
  - Oracle Internet Directory 2.1.1 或以上版本
  - Sun ONE* 5.2
  - LDAP 第 3 版相容目錄

3.3 安裝

3.3.1 安裝 LDAP 驅動程式

您可以在安裝 Metadirectory 引擎之後，另行安裝驅動程式。

在 Windows 上安裝

在 Windows NT* 2003 伺服器或已安裝 Service Pack 2 的 Windows NT 2000 上，安裝 Identity Manager Driver for LDAP。

1. 從 Identity Manager 2.0 CD 或下載的影像檔執行安裝程式。

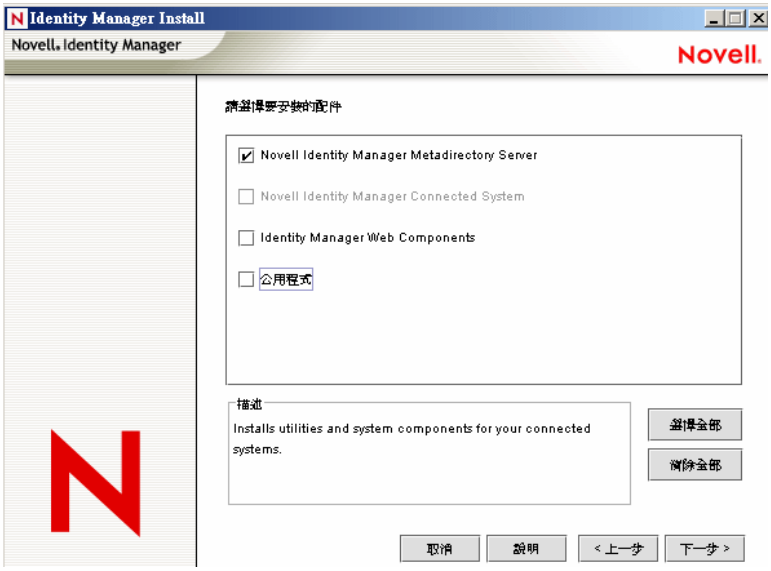
   下載檔案位於 Novell 下載 (http://download.novell.com/index.jsp)。

   如果安裝程式未自動啓動，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」。

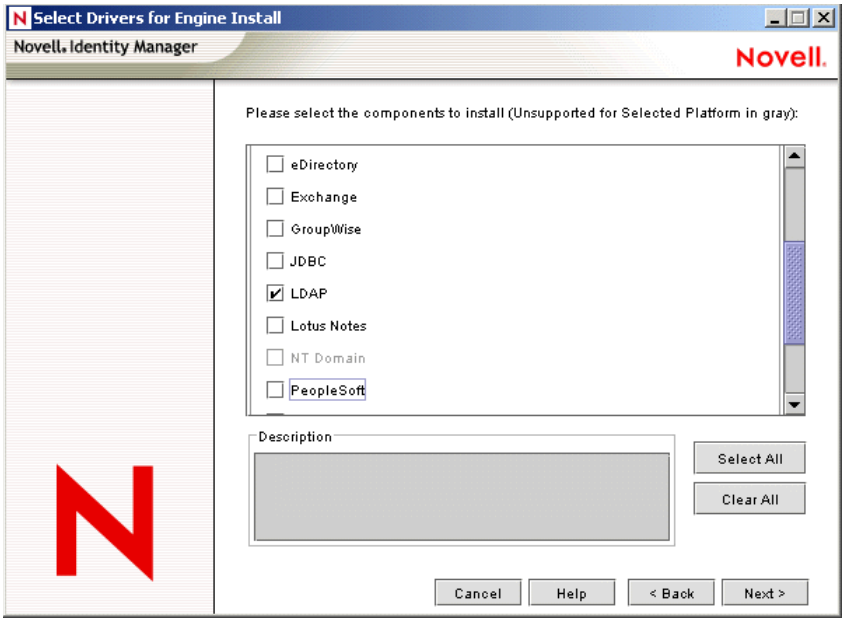
   對話方塊會提供下列資訊：
   - Metadirectory 伺服器
   - 連接伺服器系統的 Identity Manager
4. 在第二個「Identity Manager 概觀」對話方塊中，檢視資訊，然後按「下一步」。

   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「*LDAP*」，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「綱要延伸」對話方塊中，輸入使用者名稱和密碼，然後按「下一步」。

您必須具備根部 (root) 的存取權，密碼才會有效。

9 在「摘要」對話方塊中，檢視所選取的選項，然後按一下「完成」。

10 在「安裝完成」對話方塊中，按一下「關閉」。

程式安裝完成後，必須依照「安裝驅動程式」，第 18 頁的說明設定驅動程式。

在 **NetWare** 上安裝

1 在 NetWare® 伺服器上，插入 Identity Manager 3 CD，然後裝上 CD 作爲卷冊。

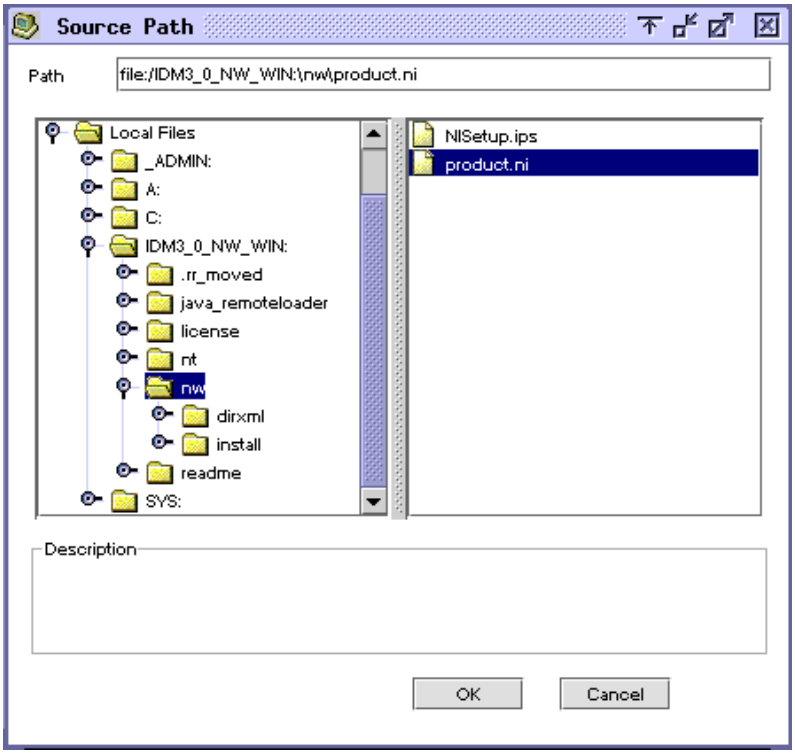
若要裝上 CD，請輸入 m cdrom。

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

5b 展開 nw 目錄，選取「product.ni」，然後按兩次「確定」。

6 在「歡迎」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 在「選取要安裝的引擎驅動程式」對話方塊中，只選取「分隔文字」。

取消選取下列選項：

- Metadirectory 引擎
- LDAP 之外的所有驅動程式

9 按「下一步」。

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 天內啓用驅動程式的授權。

11 在「綱要延伸」對話方塊中，輸入使用者名稱和密碼，然後按「下一步」。

12 在「摘要」頁面中，檢視所選取的選項，然後按一下「完成」。

13 按一下「關閉」。

程式安裝完成後，必須依照「安裝驅動程式」，第 18 頁的說明設定驅動程式。

在 **Linux**、**Solaris** 或 **AIX** 上安裝

根據預設，當您在安裝 Metadirectory 引擎時，Identity Manager Driver for LDAP 就已經安裝完成。若當時驅動程式未安裝完成，本節可以協助您進行安裝。

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，以根部身份登入。

2 插入 Identity Manager 3.0 CD，然後將其裝上。

一般而言，CD 會自動裝上。您可以手動方式裝上 CD。例如，若爲 SUSE® ，請輸入 mount /media/cdrom。

3 變更至設定目錄。

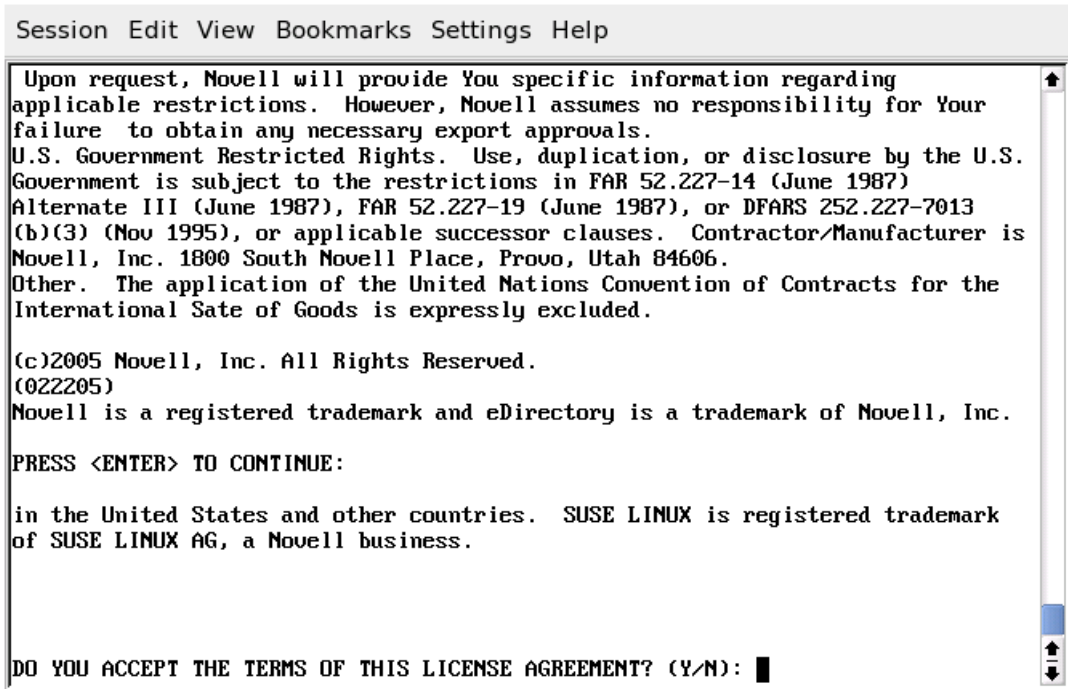
平台	路徑
Red Hat	/mnt/cdrom/linux/setup/
SUSE	/media/cdrom/linux/setup/
Solaris	/cdrom/solaris/_idm_2/setup/
AIX	/media/cdrom/aix/setup/

4 執行安裝程式。

例如，若爲 SUSE 請執行 ./dirxml_linux.bin。

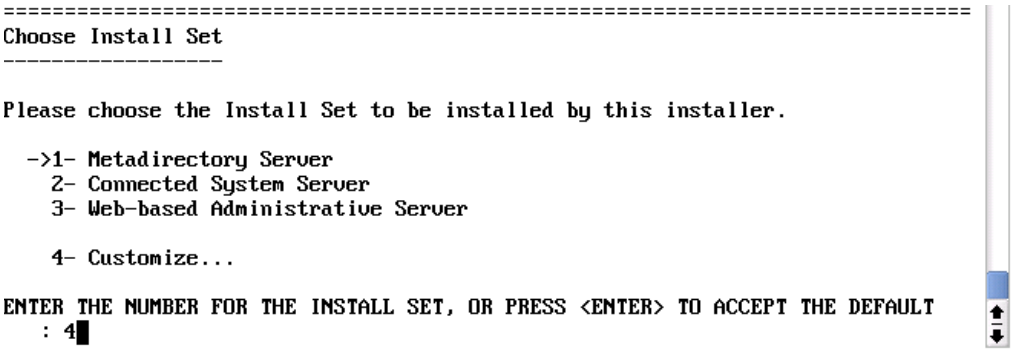
5 在「簡介」區段中，按 Enter。

6 按著 Enter，直到顯示「您是否接受授權合約條款」提示訊息後，輸入 y 以接受授權合約，然後按 Enter。



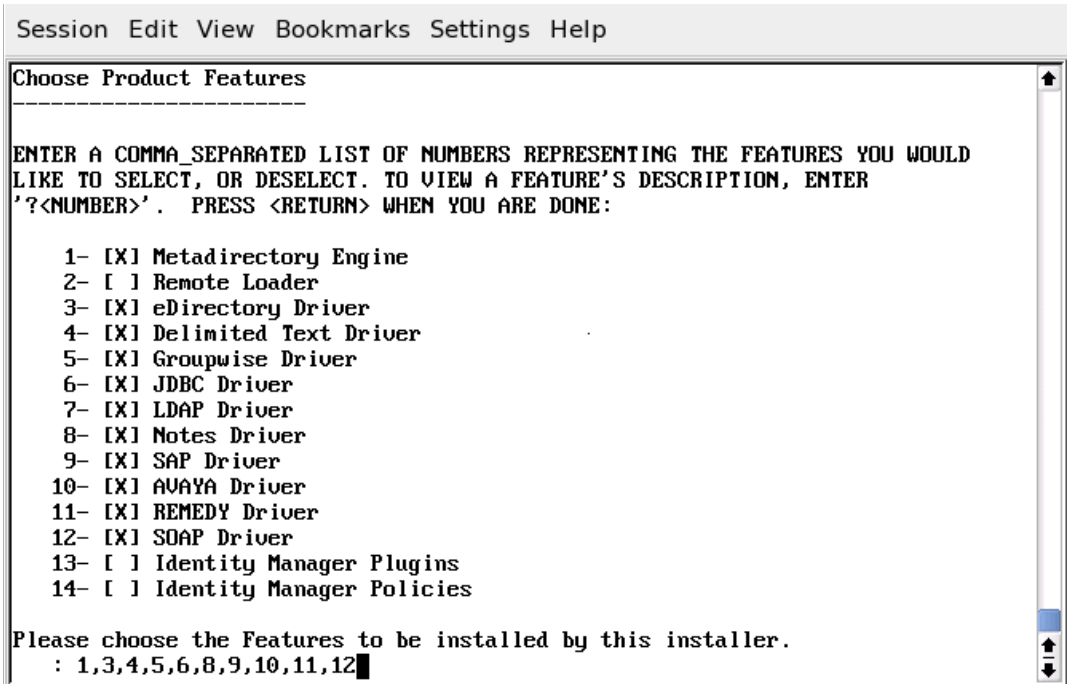
7 在「選擇安裝集」區段中，選取「自定」選項。

輸入 4，然後按 Enter。

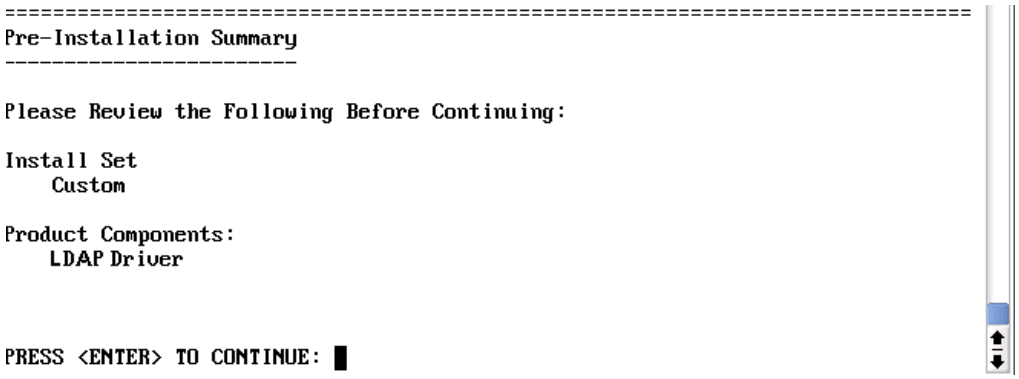


8 在「選擇產品功能」區段中，請取消選取除了 LDAP 以外的所有功能，然後按 Enter。

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。



9 在「預先安裝摘要」區段中，檢視選項。



若要返回上一個區段，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，必須依照「安裝驅動程式」，第 18 頁的說明設定驅動程式。

3.3.2 安裝驅動程式

若您正在升級現有的驅動程式，則不需要安裝。

若這是第一次使用 LDAP 驅動程式，請在以下章節完成這些安裝工作：

- 「準備 LDAP 伺服器」，第 19 頁
- 「輸入驅動程式組態範例檔案」，第 21 頁
- 「啓動驅動程式」，第 23 頁
- 「移轉並重新同步化資料」，第 23 頁
- 「啓動驅動程式」，第 23 頁

準備 **LDAP** 伺服器

如果驅動程式只是用來同步化從 Identity Vault 到 LDAP 伺服器 (在「訂閱者」通道上) 的資料，大部份的 LDAP 伺服器和應用程式不需要任何其他組態就可以運作。

您需要經常建立具有必要權限之「使用者」物件，讓驅動程式可以向 LDAP 伺服器驗證。

然而，如果您需要將 LDAP 伺服器上的資料項變更同步寫回 Identity Vault (在「發行者」通道上)，並且打算使用 changelog 方法，則在執行驅動程式之前，您至少要在 LDAP 伺服器上執行另一個組態任務。驗證 LDAP 伺服器的變更記錄機制已啓用。

重要：如果 LDAP 伺服器沒有 changelog 機制，請使用 LDAP 搜尋方法。否則，驅動程式將無法爲該伺服器發行事件。

建立具驗證權限的 LDAP 使用者物件

當您使用 changelog 發行方法時，驅動程式會嘗試阻止迴路情況的發生。迴路情況是指「訂閱者」通道上發生的事件被傳回到「發行者」通道上的 Metadirectory 引擎。然而，LDAP 搜尋方法需要依賴 Metadirectory 引擎來阻止迴路。

使用 changelog 方法時，驅動程式阻止迴路情況發生的方法是查詢變更記錄，查看是哪一位使用者做了變更。如果進行變更的使用者和驅動程式用來驗證的使用者是同一位，「發行者」會假設是驅動程式的「訂閱者」通道做了變更。

附註：如果您使用的是 Critical Path InJoin Server，在該伺服器上的實作變更記錄會是受限的，因爲沒有提供啓始變更的物件 DN。因此，建立者 / 修改者 DN 無法用來判斷變更是否來自 Identity Vault。

在該情況下，所有在變更記錄中找到的變更會由「發行者」傳送到 Metadirectory 引擎，而最佳化 / 修改功能則會丟棄不需要的或重複的變更。

若要防止「發行者」通道丟棄正確的變更，請確定驅動程式用來驗證的「使用者」物件未用在其他用途上。

例如，假設您使用 Netscape Directory Server，並設定驅動程式以使用管理員帳戶 CN=Directory Manager。如果要以手動方式在 Netscape Directory Server 進行變更，並將該變更同步化，則您不能以 CN=Directory Manager 登入並進行變更。您必須使用另一個帳戶才行。

若要避開這個問題，請執行下列動作：

1. 建立一個供驅動程式專用的使用者帳戶。
2. 爲使用者帳戶指定權限，使其可以查看變更記錄，並進行您希望驅動程式能夠做的變更。

例如，在 VMP 公司處爲驅動程式建立使用者帳戶，名稱爲 uid=ldriver,ou=Directory Administrators,o=lansing.vmp.com。然後指定適用的權限給使用者帳戶，方法是以 LDAPModify 工具或 Novell 的 Import Conversion Export 公用程式，將下列 LDIF 套用到伺服器。

```
# give the new user rights to read and search the changelog


dn: cn=changelog


changetype: modify


add: aci


aci: (targetattr = "*")(version 3.0; acl "LDAP DirXML Driver";
allow (compare,read,search) userdn = "ldap:///
uid=ldriver,ou=Directory Administrators,o=lansing.vmp.com"; )


-


# give the new user rights to change anything in the
o=lansing.vmp.com container


dn: o=lansing.vmp.com


changetype: modify


add: aci


aci: (targetattr = "*")(version 3.0; acl "LDAP DirXML Driver";
allow (all) userdn = "ldap:///uid=ldriver,ou=Directory
Administrators,o=lansing.vmp.com"; )


-
```

啓用變更記錄

變更記錄是 LDAP 伺服器的一部份，讓驅動程式可以辨識需要從 LDAP 目錄發行到 Identity Vault 的變更。此驅動程式所支援的 LDAP 目錄支援 changelog 機制。

根據預設，Critical Path InJoin 和 Oracle Internet Directory 都有啓用變更記錄。除非變更記錄已經關閉，否則不需要執行任何其他步驟來啓動它。

在 IBM SecureWay、Netscape Directory Server 和 iPlanet Directory Server 安裝完成後，您必須啓用變更記錄。如需啓用變更記錄的相關資訊，請參閱支援 LDAP 目錄的說明文件。

提示：iPlanet 變更記錄需要啓用 Retro Changelog 外掛程式。

輸入驅動程式組態範例檔案

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

使用 iManager 輸入

請依照《*Novell Identity Manager 3.0* 管理指南》中「建立並設定驅動程式」章節內關於輸入驅動程式的指示，輸入 LDAP 驅動程式組態。

在輸入過程中，請提供下列有關驅動程式組態的相關資訊。

表格 ***3-1*** *LDAP* 驅動程式的設定值

欄位	描述
驅動程式名稱	要指定給此驅動程式的 Identity Vault 物件名稱，或是要更新組態的現有驅動程式。
佈置類型	使用「簡易」佈置選項，在 LDAP 目錄中建立的「使用者」物件會放置於您在輸入驅動程式組態時指定的 Identity Vault 容器中。以 cn 值爲「使用者」物件命名。 使用「鏡像複製」佈置選項，將 LDAP 目錄中建立的「使用者」物件放置於鏡像複製物件的 LDAP 容器之 Identity Vault 容器中。
eDirectory 容器	Identity Vault 中的容器，這是建立新使用者的地方。 如果這個容器不存在，您必須在啓動驅動程式之前建立該容器。 對於 LDAPMirrorSample.xml 組態，此目錄是驅動程式之「佈置」規則的起點。附屬容器的名稱應該要和 LDAP 鏡像複製容器中的附屬容器名稱相同。 對於「平面」組態，此容器包容所有的「使用者」物件。
LDAP 容器	LDAP 目錄中的容器，這是建立新使用者的地方。 如果這個容器不存在，您必須在啓動驅動程式之前建立該容器。 對於「平面」組態，此目錄是驅動程式之「佈置」規則的起始點。 對於 LDAPSimplePlacementSample.xml 組態，此容器包容所有的「使用者」物件。
LDAP 伺服器	LDAP 伺服器的主機名稱或 IP 位址及連接埠。
LDAP 驗證 DN	指定爲 LDAP 驅動程式建立之管理員帳戶的 LDAP DN。

欄位	描述
LDAP 驗證密碼	LDAP 驅動程式管理員帳戶的密碼。在下一個欄位重新輸入密碼，以進行確認。 這是已驗證之使用者的必要密碼。 如果 LDAP 驅動程式以獨佔方式使用 Directory Manager，預設的已驗證使用者之運作一切正常。然而，如果該使用者用在其他用途上，您可能需要在執行驅動程式之後變更預設值。請參閱 「建立具驗證權限的 LDAP 使用者物件」，第 19 頁。
SSL	爲 LDAP 協定通訊加密。
設定資料流程	◆ 雙向 (Bidirectional) 的意思是，LDAP 和 Identity Vault 都是彼此之間資料同步化的授權來源。 ◆ LDAP 到 eDirectory 的意思是，LDAP 是授權來源。 ◆ eDirectory 到 LDAP 的意思是，Identity Vault 是授權來源。
將驅動程式安裝爲遠端 / 本地	選取「遠端」以設定與「遠端載入器」服務一起使用的驅動程式，或選取「本地」以設定供本地使用的驅動程式。
遠端主機名稱和連接埠	指定安裝有「遠端載入器」服務並執行此驅動程式之主機名稱或 IP 位址和連接埠號碼。預設的連接埠爲 8090。
驅動程式密碼	「遠端載入器」使用驅動程式物件密碼來向 Metadirectory 伺服器進行自我驗證。驅動程式物件密碼必須與指定爲「Identity Manager 遠端載入器」上之驅動程式物件密碼相同。
遠端密碼	此密碼僅使用於遠端載入器組態。它允許「遠端載入器」向 Metadirectory 引擎驗證。 「遠端載入器」密碼是用來控制對「遠端載入器」例項的存取。「遠端載入器」密碼必須與指定爲「Identity Manager 遠端載入器」上之「遠端載入器」密碼相同。
密碼錯誤通知使用者	密碼失敗時，傳送電子郵件通知給指定的使用者。
啓用授權	選擇「是」或「否」。由於這是設計上的決策，因此在選擇使用之前，您應充分瞭解授權。 如需授權的相關資訊，請參閱《*Novell Identity Manager 3.0 管理指南*》中的「建立並使用授權」。

使用 Designer for Identity Manager 輸入

您可以使用 Designer for Identity Manager 來輸入 LDAP 驅動程式的基本驅動程式組態檔案。此基本檔案會建立驅動程式正常運作所需的物件和規則並設定其組態。

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. 在模擬器中，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「*LDAP.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。

請指定您環境的特定資訊。如需設定值相關資訊，請參閱 「使用 iManager 輸入」，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」。

啓動驅動程式

若您在組態期間變更預設的資料位置，請在啓動驅動程式之前確定新的位置已存在。

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

2 在驅動程式集中尋找驅動程式。

3 在驅動程式圖示的右上角按一下驅動程式狀態指示器，然後按一下「啓動驅動程式」。

如果有變更記錄，驅動程式會處理變更記錄中的所有變更。如需強制啓始同步化的相關資訊，請參閱 「移轉並重新同步化資料」，第 23 頁。

移轉並重新同步化資料

Identity Manager 會在資料發生變更時，對其進行同步化。若要立即同步化所有資料，您可以選擇下列選項：

- 從 **eDirectory** 移轉資料： 可讓您選取要從 Identity Vault 移轉至 LDAP 伺服器的容器或物件。當您移轉物件時，Metadirectory 引擎會將所有的「相符」、「佈置」、「建立」規則以及「訂閱者」過濾器都套用至該物件。

附註：將資料從 Identity Vault 移轉到 LDAP 目錄時，可能需要變更 LDAP 伺服器設定，才能移轉更大量的物件。請參閱 「移轉使用者至 Identity Vault」，第 39 頁。

- 移轉資料至 **eDirectory**： 可讓您定義 Identity Manager 用來將物件從 LDAP 伺服器移轉至 Identity Vault 的準則。當您移轉物件時，Metadirectory 引擎會將所有的「相符」、「佈置」、「建立」規則以及「發行者」過濾器都套用至該物件。物件會根據您在「類別」清單中指定的順序移轉至 Identity Vault。
- 同步化： Identity Manager 會在「訂閱者」類別過濾器中尋找，以及處理這些類別的所有物件，並會合併相關聯的物件。會將未關聯的物件做爲「新增」事件處理。

若要使用其中一個選項，請執行下列動作：

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

2 尋找包含 Identity Manager Driver for LDAP 的驅動程式集，然後連按兩下驅動程式圖示。

3 按一下適當的移轉按鈕。

啓動驅動程式

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「啓用 Novell Identity Manager 產品」。

自定 LDAP 驅動程式。 4

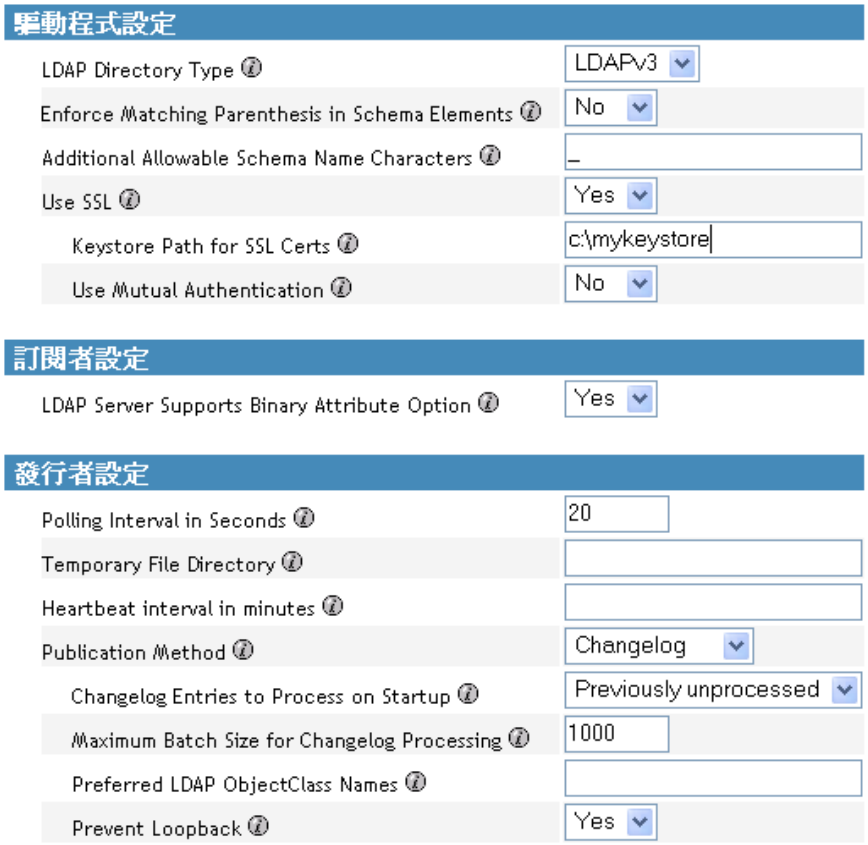
您可以使用 LDAP 驅動程式中隨附的範例組態做爲佈置的起點。然而，大部份 Identity Manager 佈置都需要您修改這些範例。

本節內容：

附註：當您在自定資料同步化時，必須針對所同步化的作業系統和帳戶，在受支援的標準和慣例內工作。若資料內含的字元在某個環境內有效，但在另一個環境內無效，便會產生錯誤。

4.1 控制 LDAP 目錄到 Identity Vault 的資料流程

特性 ***4-1*** 範例組態檔案中的設定

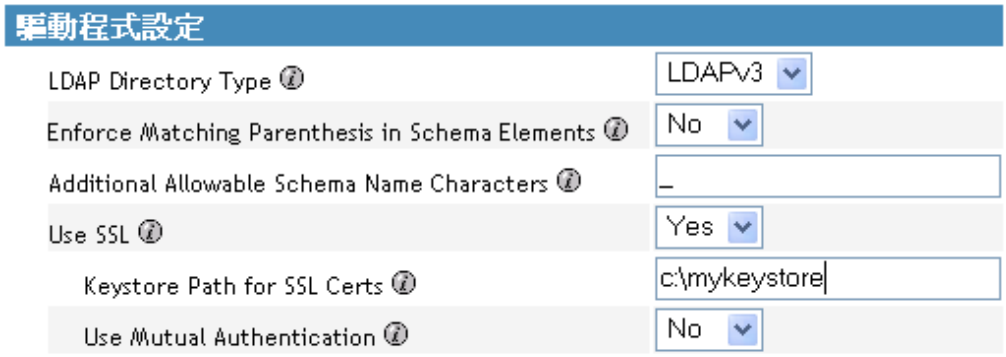


調整驅動程式的操作參數，可將驅動程式的行爲調整成與網路環境一致。例如，您發現預設的「發行者」通道輪詢間隔比同步化所需的時間短。設定較長的間隔可以改善網路效能，並保持適當的同步化。

如果 LDAP 伺服器有變更記錄，建議您使用 changelog 發行方法。如果沒有變更記錄，您可使用 LDAP 搜尋發行方法。偏好的方法是 changelog 方法。

4.1.1 LDAP 驅動程式設定

特性 ***4-2*** *LDAP* 驅動程式設定

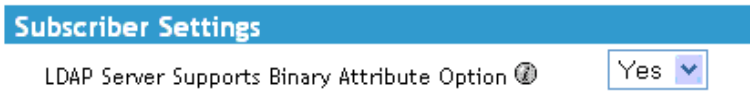


1. 在 iManager 中，選取「*Identity Manager*」>「*Identity Manager* 概觀」，然後搜尋驅動程式集。
2. 在驅動程式集中，按一下 LDAP 驅動程式圖示。
3. 在驅動程式檢視中，再按一下 LDAP 驅動程式圖示。
4. 捲動到「驅動程式參數」。
5. 在「驅動程式設定」區段中，選取所需的選項。

   如需設定的相關資訊，請按一下「資訊」圖示。

4.1.2 LDAP 訂閱者設定

特性 ***4-3*** *LDAP* 訂閱者設定



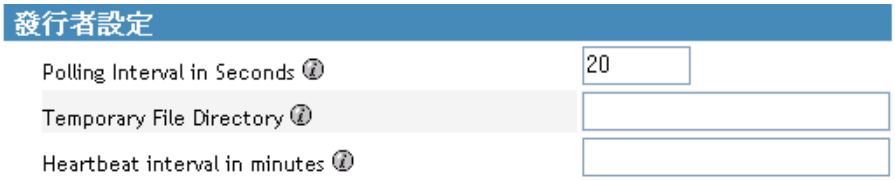
當輸入範例組態檔時，系統不會提示您提供此設定。然而，您可以在輸入檔案後再變更設定。在「訂閱者設定」區段中，選取所需的選項。

預設的設定值是「是」。大部份 LDAP 伺服器支援使用二進位屬性選項，如 RFC 2251 的第 4.1.5.1 節中所定義者。

若不知此驅動程式所連接的 LDAP 伺服器是否支援二進位屬性選項，請選取「是」。

4.1.3 LDAP 發行者設定 Changelog 和 LDAP 搜尋方法

特性 ***4-4*** *LDAP* 公用發行者設定



有些設定值可同時套用於 changelog 和 LDAP 搜尋發行方法。有些設定值只能套用於 changelog 發行方法。其他設定值則只能套用於 LDAP 搜尋發行方法。

輪詢間隔 **(** 以秒爲單位 **)**

驅動程式檢查 LDAP 伺服器的變更記錄或 LDAP 搜尋方法的時間間隔。當找到新的變更時，便將變更套用到 Identity Vault。

建議的輪詢間隔是 120 秒。

暫存檔目錄

將值設定到本地檔案系統 (即正在執行驅動程式的地方) 的目錄中，其中暫存狀態檔是可被寫入的。如果您未指定路徑，驅動程式會使用預設的驅動程式路徑。

表格 ***4-1*** 暫存檔目錄

平台或環境	預設目錄
eDirectory	DIB 檔案目錄
遠端載入器	遠端載入器根目錄

這些檔案可協助下列事項：

- 即使在驅動程式關閉時也可維護驅動程式一致性
- 防止因資料搜尋範圍擴大而產生記憶體不足現象

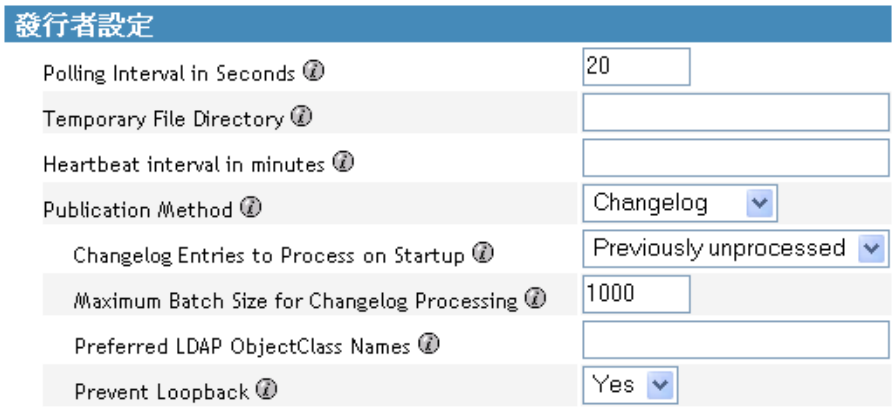
活動訊號間隔 **(** 以分鐘爲單位 **)**

若要開啓活動訊息，請輸入值。若要關閉活動訊號，則將此欄位保留空白。

如需驅動程式活動訊號的相關資訊，請參閱《*Novell Identity Manager 3.0* 管理指南》中的「新增驅動程式活動訊號」。

4.1.4 LDAP 發行者設定 僅限 Changelog 方法

特性 ***4-5*** *LDAP* 發行者通道上的 *Changelog* 設定。



啓動時處理的 **Changelog** 項目

此參數指定啓動時處理哪些項目。

- 全部：「發行者」嘗試處理在變更記錄中找到的所有變更。「發行者」會繼續處理，直到處理完所有變更爲止。它會根據輪詢率處理新變更。
- 無：當驅動程式開始執行時，「發行者」不會處理之前存在的項目。它會根據輪詢率處理新變更。
- 之前未處理：此設定爲預設值。如果這是第一次執行驅動程式，它的行爲會像 「全部」的情況，處理所有新的變更。

  如果以前就執行過驅動程式，此設定會使得 「發行者」只處理上次執行驅動程式後產生的新變更。之後，它會根據輪詢率處理新變更。

使用 changelog 方法時，驅動程式會尋找批次大小以及 「阻止迴路」設定。

Changelog 處理的最大批次大小

當 「發行者」通道處理 LDAP 變更記錄的新項目時，「發行者」會要求此批次大小的項目。如果項目數比這個變更記錄項目數還少，就會立即處理所有項目。如果比這個項目數還多，就會以這個批次大小接續處理。

偏好的 **LDAP ObjectClass** 名稱

「偏好的 *LDAP ObjectClass* 名稱」設定是選擇性的驅動程式參數，您可用它來指定 「發行者」通道上偏好的物件類別。

Identity Manager 要求以單一物件類別來識別物件。然而，有許多的 LDAP 伺服器和應用程式可以列出用於單一物件的多個物件類別。在預設狀態下，當 Identity Manager Driver for LDAP 在 LDAP 伺服器或被新增、刪除或修改的應用程式上找到物件時，會將事件傳送到 Metadirectory 引擎，並藉由使用具有綱要定義中最多的承襲層級的物件類別來識別該事件。

例如，以 inetorgperson、organizationalperson、person 和 top 物件類別來識別 LDAP 中的使用者物件。Inetorgperson 具有綱要中最多的承襲層級 (其承襲自 organizationalperson，而

organizationalperson 承襲自 person，person 則承襲自 top)。在預設狀態下，驅動程式會使用 inetorgperson 做爲向 Metadirectory 引擎報告的物件類別。

如果要變更驅動程式的預設行爲，您可以新增名爲 preferredObjectClasses 的選擇性驅動程式「發行者」參數。此參數值可以是一個 LDAP 物件類別，或是以空格分隔的 LDAP 物件類別清單。

當出現此參數時，Identity Manager Driver for LDAP 會檢查出現於「發行者」通道上的每一個物件，查看物件內是否包含清單中列出的其中一個物件類別。它會以其出現在 preferredObjectClasses 參數中的順序來尋找。如果發現其中一個列出的物件類別與 LDAP 物件上的其中一個 objectclass 屬性值相符，會使用該物件類別做爲向 Metadirectory 引擎報告的物件類別。如果沒有相符的物件類，則會爲了報告主要的物件類別而尋求其預設行爲。

阻止迴路

「阻止迴路」參數僅與 changelog 發行方法一起使用。LDAP 搜尋方法不會阻止迴路，除了置入 Metadirectory 引擎的阻止迴路功能以外。

「發行者」通道的預設行爲是要避免傳送「訂閱者」通道所做的變更。「發行者」通道會去查詢 creatorsName 或 modifiersName 屬性的 LDAP 變更記錄，藉以偵測「訂閱者」通道的變更，查看進行變更的已驗證項目是否和驅動程式用來向 LDAP 伺服器驗證的項目是同一個。如果是同一個項目，「發行者」通道會假設是驅動程式的「訂閱者」通道做了變更，所以不對變更進行同步化。

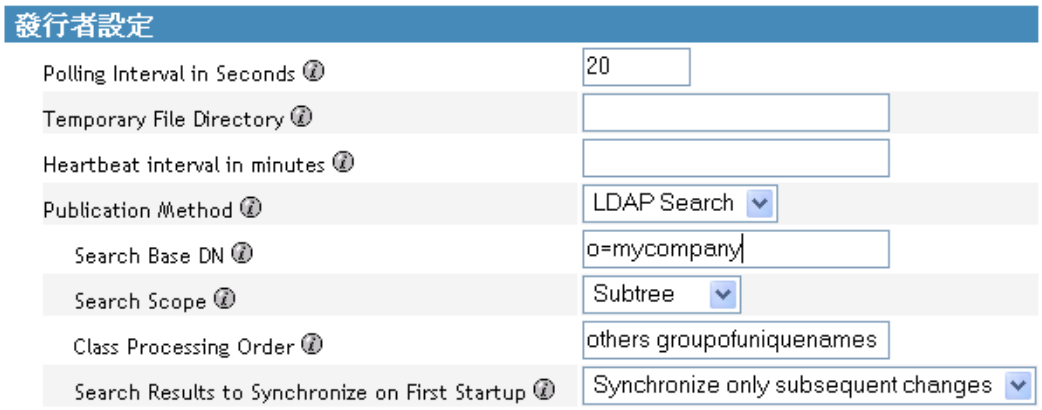
舉例來說，您可能沒有針對此驅動程式設定的「訂閱者」通道，卻想要使用和其他處理程序進行變更時所用的同一個 DN 和密碼。

如果您確定要讓這一類的迴路發生，請編輯驅動程式參數：

1. 在 iManager 中，選取「*Identity Manager*」>「*Identity Manager* 概觀」。
2. 在其驅動程式集中尋找驅動程式。
3. 按一下驅動程式以開啓「驅動程式概觀」頁面，然後再按一下驅動程式以開啓「修改物件」頁面。
4. 捲動到「發行者設定」區段，將「阻止迴路」設爲「否」。
5. 按一下「確定」，按一下「套用」，然後重新啓動驅動程式，讓此參數開始運作。

4.1.5 LDAP 發行者設定 僅限 LDAP 搜尋方法

特性 ***4-6*** *LDAP* 發行者通道上的 *LDAP* 搜尋設定。



以往 LDAP 驅動程式只能藉由讀取變更記錄來偵測 LDAP 伺服器中的變更。然而，有些伺服器不使用 changelog 機制，而事實上該機制不是 LDAP 標準的一部份。其中，變更記錄並不存在，而 LDAP 驅動程式先前並無法將這些 LDAP 伺服器的相關資料發行到 Identity Vault。

然而，LDAP 搜尋發行方法並不需要變更記錄。此方法會使用標準的 LDAP 搜尋方式，比對前一個搜尋間隔和下一個間隔的結果，藉以偵測變更。

您可以使用 LDAP 搜尋發行方法，做爲傳統 changelog 發行方法的替代方法。這些方法 Identity Manager Driver for LDAP 都支援。然而，changelog 方法在效能上較具優勢，當有變更記錄可用時便優先使用此方法。

如果沒有變更記錄，則需設定下列參數：

- 「搜尋基礎 DN」，第 30 頁
- 「搜尋範圍 (1-Subtree 子網路樹、2-One Level 一層、3-Base 基礎)」，第 30 頁
- 「類別處理順序」，第 31 頁
- 「第一次啓動時要同步化的搜尋結果」，第 31 頁

搜尋基礎 **DN**

如果因無變更記錄可用而使用 「發行者」通道時，必需的參數。將參數設爲容器的 LDAP 可辨識名稱 (DN)，該容器即爲輪詢搜尋應開始之處 (例如 ou=people,o=company)。

若要使用變更記錄，就讓此參數留空白。

搜尋範圍 **(1-Subtree** 子網路樹、**2-One Level** 一層、**3-Base** 基礎 **)**

指出輪詢搜尋的深度。此參數預設爲搜尋 「搜尋基礎 DN」指向的整個子網路樹。

沒有變更記錄可用時，設定此參數。

類別處理順序

當參照屬性需納入考量時，「發行者」通道用來調整某些事件之順序的選擇性參數。參數值是來自 LDAP 伺服器，並以空格分隔的類別名稱清單。例如，確定在新增至群組之前先建立新使用者，以及確定 interorgperson 優先於 groupofuniquenames。

Identity Manager Driver for LDAP 定義特定的類別名稱 "others"，表示除了明確列出類別以外的所有類別。

此參數的預設值是 "other groupofuniquenames"。

沒有變更記錄可用時，使用此參數。

第一次啓動時要同步化的搜尋結果

第一次啓動 LDAP 驅動程式時，該驅動程式會執行定義的 LDAP 搜尋。「第一次啓動時要同步化的搜尋結果」設定，定義是否將啓始搜尋結果同步化，或只將後續的變更同步化。

「發行方法」參數設爲「*LDAP* 搜尋」時，才會出現「第一次啓動時要同步化的搜尋結果」選項。當輸入組態檔時，系統不會提示您提供此設定。然而，您可以在輸入檔案後再變更設定。

1. 在 iManager 中，選取「*Identity Manager*」>「*Identity Manager* 概觀」，然後搜尋驅動程式集。
2. 在驅動程式集中，按一下 LDAP 驅動程式圖示。
3. 在驅動程式檢視中，再按一下 LDAP 驅動程式圖示。
4. 捲動到「驅動程式參數」。
5. 在「發行者設定」區段中，選取所需的選項。

   預設的設定是「僅同步化後續變更」。

4.2 設定資料同步化的組態

- 「決定哪些物件要同步化」，第 31 頁
- 「定義綱要映射」，第 32 頁
- 「在 Netscape 中定義物件佈置」，第 33 頁
- 「使用 eDirectory 群組和 Netscape」，第 34 頁

4.2.1 決定哪些物件要同步化

Identity Manager 使用「發行者」及「訂閱者」通道上的過濾器，控制哪些物件要同步化，並且爲這些物件定義授權資料來源。

預設的過濾器如「過濾器」，第 7 頁中所示。使用下列程序，爲預設值做變更。

編輯發行者和訂閱者過濾器

1. 在 iManager 中，選取「*Identity Manager*」>「*Identity Manager* 概觀」。
2. 在其驅動程式集中找出驅動程式。
3. 按一下驅動程式，開啓「*Identity Manager* 驅動程式概觀」頁面。

4 按一下「發行者」或「訂閱者」過濾器圖示，進行適當的變更。

「發行者」過濾器必須包含 Identity Vault 強制屬性。「訂閱者」過濾器必須包含 LDAP 伺服器必需的屬性。

對於過濾器中選取的每一個物件和屬性，「映射」規則必須具有對應的項目，除非類別或屬性名稱與兩個目錄中的名稱相同。映射屬性之前，驗證對應的屬性確實存在於目標目錄中。

4.2.2 定義綱要映射

不同的 LDAP 伺服器具有不同的綱要。驅動程式第一次啓動時，會查詢特定綱要的伺服器。

您必須熟悉 eDirectory 屬性和 LDAP 伺服器屬性的特性。驅動程式會處理所有的 LDAP 屬性類型 (cis、ces、tel、dn、int、bin)。 也會處理 eDirectory Facsimile Telephone Number。

映射屬性時，請遵循以下指示：

- 驗證「發行者」及「訂閱者」規則中指定的每一個類別和屬性，都在「映射」規則中映射，除非類別或屬性名稱與兩個目錄中的名稱相同。
- 映射 eDirectory™ 屬性到 LDAP 伺服器屬性之前，驗證 LDAP 伺服器屬性確實存在。例如，爲 Identity Vault 上的「使用者」物件定義 Full Name 屬性，但是 fullname 卻不存在於 Netscape 上的 inetOrgPerson 物件中。
- 務必將屬性映射到相同類型的屬性。例如，將字串屬性映射到字串屬性、將八進位屬性映射到二進位屬性，或將電話號碼 (telenumber) 屬性映射到電話號碼屬性。
- 將多值屬性映射到多值屬性。

驅動程式不提供不同屬性類型之間的資料轉換，或是多值到單一值屬性的轉換。驅動程式也不了解結構化屬性，但是 Facsimile Telephone Number 和 Postal Address 除外。

Identity Manager 在語法上是靈活的，它接受從「發行者」傳入：

- 接受非結構化 / 非八進位語法 . Identity Manager 接受任何非結構化 / 非八進位語法 (任何其他的非結構化 / 非八進位語法)，只要實際的資料可以強制置入適用類型。也就是說，如果 Identity Vault 在尋找數值，實際資料就應該是數字。
- 將資料強制置入八進位值 . 當 Identity Manager 在期待八進位資料，卻得到另一個非八進位 / 非結構化類型的資料時，Identity Manager 會將字串值串列化爲 UTF-8，將資料強制置入八進位值。
- 將資料強制置入字串 . 當 Identity Manager 收到八進位資料，而實際上應收到另一個非結構化類型時，Identity Manager 會藉由解碼 Base64 資料將資料強制置入字串。接著，Identity Manager 會試著將結果解譯爲 UTF-8 編碼字串 (或平台的預設字元編碼，若爲非有效的 UTF-8 字串)，然後套用和「接受非結構化 / 非八進位語法」相同的規則。
- **FaxNumber** . 對於 faxNumber，如果傳進非結構化類型，「接受非結構化 / 非八進位語法」和「將資料強制置入字串」會套用到資料，以取得傳真號碼的電話號碼部份。其他欄位爲預設欄位。
- 狀態。狀態。對於狀態，False、No、F、N (大寫或小寫)、0 和 "" (空字串) 會被解譯爲 False，任何其他值被解譯爲 True。

若要設定「綱要映射」規則：

1 在 iManager 中，按一下「*Identity Manager*」>「*Identity Manager* 概觀」。

2 在其驅動程式集中找出驅動程式。

3 按一下驅動程式，開啓 「Identity Manager 驅動程式概觀」頁面。

4 按一下 「發行者」或 「訂閱者」通道上的綱要映射圖示。

5 依您安裝的需要編輯規則。

4.2.3 在 Netscape 中定義物件佈置

針對 Netscape Directory Server 中的物件，建議遵循下列 Netscape 命名規則。爲方便起見，這裡有命名規則的簡短說明。

目錄中包含代表人員的項目。這些人員項目必須有名字。也就是說，您必須判斷哪個相關的可辨識名稱 (RDN) 將用於每一個人員項目。DN 必須是唯一的、容易辨認的永久值。建議您使用 uid 屬性來指定與人員相關的唯一值。人員項目的範例 DN 爲：

uid=jsmith,o=novell

目錄中也包含代表人員以外的許多事情的項目 (例如群組、裝置、伺服器、網路資訊或其他資料)。建議您使用 RDN 中的 cn 屬性。因此，如果您在爲群組項目命名，請命名如下：

cn=administrators,ou=groups,o=novell

同時目錄也包含分支點或容器。您需要判斷要使用哪些屬性來識別分支點。由於屬性名稱是有意義的，因此請使用具其所代表之項目類型的屬性名稱。Netscape 建議的屬性定義如下：

表格 ***4-2*** *Netscape* 建議的屬性

屬性名稱	定義
c	國名
o	組織名稱
ou	組織單位
st	狀態
l	地域性
dc	領域元件

「訂閱者佈置」規則指定類別名稱的命名屬性。以下範例用於 「使用者」類別名稱。<placement> 陳述式指定將 uid 當成命名屬性使用。

```
<placement-rule> <match-class class-name="User"/> <match-path
prefix="\Novell-Tree\Novell\Users"/> <placement>uid=<copy-name/
>,ou=People,o=Netscape</ placement> </placement-rule>
```

下列 「訂閱者佈置」指定將 ou 當成 class-name Organizational Unit 的命名屬性使用。

```
<placement-rule> <match-class class-name="Organizational Unit"/>
<match-path prefix="\Novell-Tree\Novell\Users"/> <placement>ou=<copy-
name/>,ou=People,o=Netscape</placement> </placement-rule>
```

設定佈置規則

1. 在 iManager 中，按一下「*Identity Manager*」>「*Identity Manager* 概觀」。
2. 在其驅動程式集中找出驅動程式。
3. 按一下驅動程式，開啓「Identity Manager 驅動程式概觀」頁面。
4. 按一下「發行者」或「訂閱者佈置」規則圖示，進行適當的變更。

4.2.4 使用 eDirectory 群組和 Netscape

由於 Identity Vault 和 Netscape Directory Server 中的群組屬性是不同的，驅動程式需要某些特別處理。在「發行者」通道上，當驅動程式看到類別名稱爲 *groupofuniquenames* 的 *uniquemember* 屬性時，就會進行特別處理。

驅動程式也會設定 eDirectory Group 中的 Equivalent To Me 屬性。Equivalent To Me 屬性必須包含於「發行者」過濾器中。因爲已使用 eDirectory 屬性名稱，所以 Equivalent To Me 屬性並不需要在「綱要映射」規則中。Netscape Directory Server 中並沒有相等的屬性名稱。「訂閱者」通道上不需要特別處理。

4.3 設定 SSL 連接

驅動程式使用 LDAP 協定與 LDAP 伺服器進行通訊。大部份的 LDAP 伺服器允許非加密的 (純文字) 連接。此外，設定正確時，有些 LDAP 伺服器便會允許 SSL 加密的連接。SSL 連接使用公用 / 私密金鑰配對，爲 TCP/IP 插槽上的所有流量加密。實際的 LDAP 協定不會變更，但是通訊通道會執行加密。

每一個 LDAP 伺服器的 SSL 連接程序稍有不同。本文件內含涵蓋使用 Netscape Directory Server 4.12 時進行 SSL 連接的過程。

- 「步驟 1：產生伺服器證書」，第 34 頁
- 「步驟 2：傳送證書申請」，第 35 頁
- 「步驟 3：安裝證書」，第 35 頁
- 「步驟 4：在 Netscape Directory Server 4.12 中啓用 SSL」，第 36 頁
- 「步驟 5：從 eDirectory 網路樹內輸出託管根部。」，第 36 頁
- 「步驟 6：輸入託管根部證書」，第 36 頁
- 「步驟 7：調整驅動程式設定」，第 37 頁

如果您使用的是另一個 LDAP 伺服器，程序會很相似。

4.3.1 步驟 1：產生伺服器證書

首先您需要安裝伺服器證書。LDAP 伺服器本身能夠產生證書，但必須由伺服器託管的 CA 簽署證書。要簽署證書，可使用 Identity Vault 隨附的 CA。

若要產生證書申請：

1. 在 Netscape 主控台的導覽樹狀結構中，選取將與驅動程式通訊的伺服器。
2. 按一下「開啓伺服器」。
3. 按一下「任務」>「證書設定精靈」。

4 提供申請證書所需的資訊。

根據可能已安裝在主機系統上的證書或記號，您可能會看到一些或以下全部的欄位：

選取記號 **(Cryptographic** 裝置 **)**：選取「內部 *(* 軟體 *)*」。

已申請伺服器證書並準備好要安裝了嗎？ 選取「否」。

如果此主機沒有託管資料庫，它會爲您產生一個。

託管資料庫是安裝在本地主機上的金鑰配對及證書資料庫。當使用內部記號時，託管資料庫便是您安裝金鑰和證書的資料庫。

5 輸入及確認密碼。

密碼必須包含至少八個字元，其中至少一個必須是數字。此密碼有助於保障存取您建立的新金鑰資料庫的安全。

6 依系統指示，繼續提供資訊，然後按「下一步」。

7 建立託管資料庫之後，按「下一步」。

8 輸入所要的資訊，然後按「下一步」。

9 輸入先前選取之記號的密碼，然後按「下一步」。

「證書設定精靈」會爲您的伺服器產生證書申請。當您看到相關網頁，可將申請傳送到憑證授權單位。

4.3.2 步驟 2：傳送證書申請

1 將伺服器證書申請複製到另一個文字編輯器。

2 將檔案另存爲 csr.txt。

證書申請電子郵件顯示如下：

```
-----¹}©l²sÐ"Æ—•"¾------

          .

          .

          . -----µðßÙ²sÐ"Æ—•"¾------
```

3 在 iManager 中，選取「*Novell Certificate Server*」>「發出證書」。

4 在「檔名」欄位中，瀏覽到 csr.txt，然後按「下一步」。

5 選取「組織證書權限」。

6 指定 SSL 爲金鑰類型，然後按「下一步」。

7 指定證書參數，按「下一步」，然後按一下「完成」。

8 以 Base64 格式將證書儲存爲 cert.b64，並儲存到本端磁碟或磁片中。

4.3.3 步驟 3：安裝證書

1 在 Netscape 主控台的導覽樹狀結構中，選取將與驅動程式連接的伺服器。

2 按一下「開啓」。

3 按一下「任務」>「證書設定精靈」。

4 啓動精靈，指出您準備安裝證書。

5 當出現提示時，請提供下列資訊：

選取記號 **(Cryptographic** 裝置 **)**： 選取「內部 *(* 軟體 *)*」。

已申請伺服器證書並準備好要安裝了嗎？ 選取「是」。

6 按「下一步」。

7 在「安裝證書」欄位中，選取「這個伺服器」。

8 在「密碼」欄位中，輸入您用來設定託管資料庫的密碼，然後按「下一步」。

9 在「證書位於此檔案」欄位中，輸入證書的絕對路徑 (例如 A: \CERT.B64)。

10 產生證書之後，按一下「新增」。

11 在成功安裝證書之後，按一下「完成」。

4.3.4 步驟 4：在 Netscape Directory Server 4.12 中啓用 SSL

安裝完證書之後，完成下列動作即可啓用 SSL：

1 在 Netscape 主控台的導覽樹狀結構中，選取要與 SSL 加密功能一併使用的伺服器。

2 按一下「開啓」>「組態」>「加密」。

3 輸入下列資訊：

啓用 **SSL**： 選取此選項。

加密系列： 選取「*RSA*」。

使用的記號： 選取「內部 *(* 軟體 *)*」。

使用的證書： 選取「伺服器證書」。

用戶端驗證： 由於驅動程式不支援用戶端驗證，請選取「允許用戶端驗證」。

4 按一下「儲存」。

5 按一下「任務」，然後重新啓動伺服器，如此變更才會生效。

4.3.5 步驟 5：從 eDirectory 網路樹內輸出託管根部。

1 在 iManager 中，選取「*eDirectory* 管理」>「修改物件」。

2 瀏覽到「證書權限」(CA) 物件，然後按一下「確定」。

3 從下拉式清單選取「證書」。

4 按一下「輸出」。

5 當提示訊息顯示「您要輸出私密金鑰及證書嗎？」，請按一下「否」。

6 按「下一步」。

7 在「檔名」欄位中，輸入檔名 (例如 PublicKeyCert)，然後選取「*Base64*」格式。

8 按一下「輸出」。

4.3.6 步驟 6：輸入託管根部證書

您需要將託管根部證書輸入到 LDAP 伺服器的託管資料庫和用戶端的證書儲存區。

輸入到 **LDAP** 伺服器的託管資料庫

您需要將託管根部證書輸入到 LDAP 伺服器的託管資料庫。由於伺服器證書是由 Identity Vault 的 CA 簽署的，因此需要將託管資料庫設定成託管 Identity Vault CA。

1. 在 Netscape 主控台中，按一下「任務」>「證書設定精靈」>「下一步」。
2. 在「選取記號」，接受內部 (「軟體」) 的預設值。
3. 在「已申請伺服器證書並準備好要安裝了嗎？」中，選取「是」。
4. 按兩次「下一步」。
5. 在「安裝證書」對話方塊中，選取「託管證書權限」。
6. 按「下一步」。
7. 選取「證書位於此檔案」，輸入包含託管根部證書的 .b64 檔案的完整路徑。
8. 按「下一步」。
9. 驗證畫面上的資訊，然後按一下「新增」。
10. 按一下「完成」。

輸入用戶端的證書儲存區

您需要將託管根部證書輸入到驅動程式可使用的證書儲存區 (也稱爲金鑰儲存區)。

1. 使用 rt.jar 中找到的 KeyTool 類別。

   例如，如果公用金鑰證書以 PublicKeyCert.b64 儲存於磁片，而您想要將它輸入到目前目錄中名爲 .keystore 的新證書儲存檔案中，請在指令行輸入下列指令：

   ```
   java sun.security.tools.KeyTool -import -alias TrustedRoot -file
   a:\PublicKeyCert.b64
   [XXX]
   -keystore .keystore -storepass keystorepass
   ```

2. 當您被要求託管此證書時，請選取「是」，然後按一下「*Enter*」。
3. 將 .keystore 檔複製到具有 Identity Vault 檔案的相同檔案系統上的任何目錄中。
4. 在 iManager 中，選取「*Identity Manager*」>「*Identity Manager* 概觀」。
5. 搜尋驅動程式。
6. 按一下 LDAP 驅動程式物件，然後在「*Identity Manager* 驅動程式概觀」頁面中再按它一下。
7. 在「*KeyStore* 路徑」參數中，輸入 .keystore 檔案的完整路徑。

4.3.7 步驟 7：調整驅動程式設定

下表列出了驅動程式設定值，以及其在範例組態中的預設值。

表格 ***4-3*** 驅動程式設定值和預設值

參數	範例組態值	描述
將 SSL 用在 LDAP 連接上	否	此參數值應該爲「是」或「否」，代表是否要在與 LDAP 伺服器的通訊中使用 SSL 連接。若要使用 SSL，您也必須要正確地設定 LDAP 伺服器組態。 如需相關資訊，請參閱 「設定 SSL 連接」，第 34 頁。
SSL 連接埠	636	除非「將 SSL 用在 LDAP 連接上」設爲「是」，否則此參數會被忽略。其指出 LDAP 伺服器用在安全連接上的連接埠。
KeyStore 路徑 (用於 SSL 證書)	[空白]	當「將 SSL 用在 LDAP 連接上」設爲「是」，此參數值應該是 KeyStore 檔案的完整路徑，而該檔案包含簽署伺服器證書之「證書權限」(CA) 的託管根部證書。 如需建立 KeyStore 檔案的相關資訊，請參閱 「輸入用戶端的證書儲存區」，第 37 頁 "。

疑難排解

5

5.1 移轉使用者至 Identity Vault

有些 LDAP 伺服器的設定會限制可由 LDAP 查詢傳回的項目數量。例如，iPlanet Directory Server 5.1 預設限制爲 2000 個物件。

從 LDAP 移轉使用者資料到 Identity Vault 時，驅動程式會向伺服器提出 LDAP 查詢，並傳回符合準則的物件 (例如 objectclass=User)。

限制 LDAP 查詢上可傳回的項目數量，可能會造成移轉在完成之前即停止動作，縱使 Identity Manager 驅動程式仍繼續正常執行。

要解決這個問題，請變更限定值。例如，在 iPlanet 中執行下列動作：

1. 移到 「組態」索引標籤處，然後選取 「資料庫」設定值。
2. 提高 LDBM 外掛程式索引標籤上的重新檢查限定值，從預設值 5000 調到適當的數量。

   這也是完成查詢的同時，查詢可以查看的記錄數。
3. 移到 「組態」索引標籤處，選取 「目錄伺服器設定」，選取 「效能」索引標籤，根據需要移轉的使用者帳戶數來提高大小限定值。

   這是查詢可以傳回的實際記錄數。

   調整過這些設定值之後，應該就可以正確地完成移轉動作了。

5.2 OutOfMemoryError

如果您使用 LDAP 搜尋方法，而驅動程式因 java.lang.OutOfMemoryError 問題而關閉：

1. 試著設定或增加 DHOST_JVM_INITIAL_HEAP 和 *DHOST_JVM_MAX_HEAP* 環境變數。
2. 重新啓動驅動程式。
3. 監看驅動程式，確定變數提供足夠的記憶體。

如需相關資訊，請參閱 TID 10062098 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10062098.htm)。

5.3 LDAP v3 相容性

Identity Manager Driver for LDAP 可與大部份 LDAP v3 相容的 LDAP 伺服器一起運作。驅動程式會被寫入用於 LDAP 的 RFC 2251 規格中。爲了增加與某些不完全符合 RFC 2251 要求之 LDAP 伺服器的相容性，我們已爲 LDAP 驅動程式加入一些調整元素。

有一個不能忽略也不能改變的相容性議題是 RFC 2251 要求，也就是伺服器允許 「訊息 ID」值最高到 2,147,483,647 (使用 4 位元組的整數值)。

Oracle Internet Directory 2.1.1.0.0 版 (屬於 Oracle 8i 的一部份) 只允許 「訊息 ID」值最高到 32,767 (使用 2 位元組的整數值)。因此，造成它與 Identity Manager Driver for LDAP 無法正常運作。

如果需要與 Oracle Internet Directory 相容，Novell 建議您升級到 9.2.0.1.0 (包含在 Oracle 9i 內) 或更新版本。

5.4 常見問題解答

問題：LDAP 搜尋方法每一次都會擷取所有資料，或只是擷取最後一次輪詢之後的更新部份？

回答： LDAP 搜尋方法會將這次輪詢和下次輪詢之間的更新同步化。

問題：如果可以選擇使用 LDAP 搜尋方法或 changelog 方法，我是否應該使用 LDAP 搜尋方法？

回答： changelog 方法具有效能優勢。請多加使用。偏好的方法是 changelog 方法。

文件更新

A

本節包含 Identity Manager Driver for LDAP 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 文件的副本是否爲最新版本，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。

全新或更新的文件在下列日期發行：

- 「2006 年 5 月 25 日」，第 41 頁

A.1 2006 年 5 月 25 日

表格 ***A-1*** 變更日期：*2006* 年 *5* 月 *8* 日

位置	變更
「新功能」，第 5 頁	此主題新增兩個項目。
「規劃的更新」，第 5 頁	新增這個主題。
「規劃考量」，第 11 頁	新增一段與 LDAP v3 相容性議題和 RFC 2251 規格相關的內容。
「控制 LDAP 目錄到 Identity Vault 的資料流程」，第 25 頁	重新組織這一區段，讓 changelog 和 LDAP 搜尋方法更容易實作。
「LDAP 訂閱者設定」，第 26 頁	增加新「訂閱者」參數的相關資訊。
「第一次啓動時要同步化的搜尋結果」，第 31 頁	增加新「發行者」參數的相關資訊。
「LDAP v3 相容性」，第 39 頁	新增這個區段。
「常見問題解答」，第 40 頁	新增這個區段。