Novell Identity Manager

3.5.1

www.novell.com

安裝指南

2007 年 9 月 28 日

Novell®

法律聲明

Novell, Inc. 對本文件的內容與使用不做任何陳述或保證，對本產品在任何特定用途的適銷性與適用性上，亦不做任何明示或默示的保證。此外，Novell, Inc. 保留隨時修改本出版品及其內容的權利，進行此類修正或更動時，亦毋需另行通知任何人士或公司組織。

此外，Novell, Inc. 對軟體不做任何陳述或保證，對本產品在任何特定用途的適銷性與適用性上，亦不做任何明示或默示的保證。此外，Novell, Inc. 保留隨時修改任何或全部 Novell 軟體的權利，進行此類更動時，亦毋需通知任何人士或公司。

此合約下提到的任何產品或技術資訊可能受美國出口管制法與其他國家 / 地區的貿易法的限制。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之實體，或是任何美國出口法所指定之禁運或恐怖主義國家。您同意不將交付產品用在禁止的核武、飛彈或生化武器等用途上。如需輸出 Novell 軟體的相關資訊，請參閱國際貿易服務 (http://www.novell.com/company/policies/trade_services)。Novell 無需承擔您無法取得任何必要的出口核准之責任。

本文件所述產品所使用技術的智慧財產權屬於 Novell, Inc. 所有。特別是 (但不限於) 這些智慧財產權可能包含 Novell 法律專利網頁 (http://www.novell.com/company/legal/patents/) 中所列的一或多項美國專利，以及在美國與其他國家 / 地區的一或多項其他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 產品最新的線上文件，請參閱 Novell 文件網頁 (http://www.novell.com/documentation)。

Novell 商標

若要查看 Novell 商標，請參閱 Novell 商標和服務標誌清單 (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各別擁有廠商的財產。

目錄

關於本指南

Novell® Identity Manager (先前稱爲 DirXML®) 是一種資料共享及同步服務，可讓應用程式、目錄和資料庫共享資訊。它會連結散佈的資訊，並讓您建立規則，用於在身分發生變更時管理對指定系統的自動更新。Identity Manager 提供了下列項目的基礎：帳戶提供、安全性、單次登入、使用者自助服務、驗證、授權、自動工作流程和 Web 服務。它可讓您整合、管理和控制您的分散式身分資訊，以便安全地將正確的資源傳送給正確的人員。

本指南提供 Identity Manager 技術的綜覽，同時說明 Identity Manager 的安裝、管理以及組態設定等功能。

使用對象

本指南的適用對象是計劃在網路環境中實作 Identity Manager 的管理員、顧問和網路工程師。

文件更新

如需本文件的最新版本，請參閱 Identity Manager 文件網站 (http://www.novell.com/documentation/idm35/index.html)。

其他文件

如需其他 Identity Manager 驅動程式的相關文件，請參閱 Identity Manager 驅動程式網站 (http://www.novell.com/documentation/idm35drivers/index.html)。

文件慣例

在 Novell 文件中，大於符號 (>) 是用來分隔步驟中的動作，以及交互參照路徑中的項目。

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

雖然在寫入單一路徑名稱時，有些平台採用反斜線，其他平台採用正斜線，但在本文中，路徑名稱一律使用反斜線。平台使用者如須使用正斜線 (如 Linux* 或 Unix*)，即應遵循軟體要求使用正斜線。

綜覽

1

1.1 Identity Manager 簡介

Novell® Identity Manager 是一項屢獲殊榮的資料共享和同步化解決方案，它會徹底改變您的資料管理方式。此服務可運用您的 Identity Vault (一種集中式資料儲存)，在應用程式、資料庫和目錄之間同步化、轉換和散佈資訊。

但 Identity Manager 並不僅止於此。以下列出 Identity Manager 的幾個功能：

- 密碼同步化
- 密碼自助服務
- 登入和稽核服務
- 透過使用者應用程式進行使用者的管理
- 工作流程提供
- 電子郵件通知
- 透過 Designer 公用程式設計驅動程式和規則

若想知道這些元件在此版本之 Identity Manager 中有哪些新功能，請參閱第 1.3 節 「Identity Manager 3.5.1 的新功能」 (第 14 頁)。若想進一步瞭解 Identity Manager 的各種組成元件和服務，請參閱第 1.4 節 「Identity Manager 安裝程式和服務」 (第 18 頁)。

Identity Manager 可讓已連接系統 (例如 SAP*、PeopleSoft*、Lotus* Notes*、Microsoft* Exchange、Active Directory* 和其他系統) 進行下列幾項操作：

- 與 Identity Vault 共享資料。
- 當與 Identity Vault 共享的資料在已連接系統中修改時，對其進行同步化和轉換。
- 當與已連接系統共享的資料在 Identity Vault 中修改時，對其進行同步化和轉換。

Identity Manager 進行此操作的方法是提供雙向架構，以允許管理員指定從 Identity Vault 流向應用程式以及從應用程式流向 Identity Vault 的資料。該架構使用 XML 來提供資料和事件轉譯功能，將 Identity Vault 資料和事件轉換爲指定的特定應用程式格式。同時還能將特定應用程式格式轉換爲 Identity Vault 所瞭解的格式。所有與應用程式的互動都會使用應用程式的原始應用程式介面 (API) 來進行。

Identity Manager 可讓您僅選取對應相關已連接系統特定記錄和欄位的屬性和類別。例如，目錄資料儲存可以選擇與 「人力資源部門」資料儲存共享 「使用者」物件，但不共享諸如

「伺服器」、「印表機」和「磁碟區」等網路資源物件。然後，「人力資源部門」資料儲存可以和其他人員共享使用者的名字、姓氏、姓名縮寫、電話號碼和工作地點，而不會共享使用者較爲個人的資訊 (例如家庭資訊和就業記錄)。

如果 Identity Vault 沒有您想要與其他應用程式共享之資料的類別或屬性，您可以延伸 eDirectory 綱要來包含它們。在此情況下，您的 Identity Vault 會成爲資訊的儲存機制，雖然它不需要這些資訊，但其他應用程式可以使用。應用程式特定的資料儲存可維護只有應用程式才需要的資訊儲存機制。

Identity Manager 會完成下列任務：

- 使用事件在 Identity Vault 中擷取變更。
- 做爲中樞器提取所有資料，以集中或散佈資料管理。
- 以 XML 格式公開目錄資料，讓 XML 應用程式或透過 Identity Manager 整合的應用程式可以使用和共享這些資料。
- 請仔細維護 Identity Vault 物件與所有其他整合式系統內物件之間的關聯，從而確保在所有已連接系統間適當地反映資料變更。

規則是對資料進行同步化時的關鍵。規則可以：

- 使用可管理在系統中定義之資料元素的特定過濾器來控制資料流程。
- 使用許可和過濾器來強制執行授權資料來源。
- 套用規則至 XML 格式的資料儲存資料。當變更流經 Identity Manager 時，這些規則會管理資料的解譯和轉換。
- 幾乎可將資料從 XML 轉換爲任何資料格式。如此可讓 Identity Manager 與各種應用程式共享資料。

使用 Identity Manager，貴公司可以簡化 HR 程序、降低資料管理成本、透過高度自訂的服務建立客戶關係，並可去除所有會影響成功的溝通障礙。以下是 Identity Manager 可以完成的活動範例：

表格 1-1 *Identity Manager 可以執行的操作*

活動	Identity Manager 解決方案
管理使用者帳戶	使用單一操作： Identity Manager 立即授予或移除對員工資源的存取。 Identity Manager 會提供自動員工提供功能，讓新員工取得對網路、電子郵件、應用程式、資源等存取權限。透過工作流程提供，您便可設定此程序來起始核准程序。 Identity Manager 還可以在終止或離開時限制或停用存取權限。
追蹤和整合資產庫存	Identity Manager 可以將所有資產庫存項目 (電腦、監視器、電話、文件庫資源、椅子、辦公桌等) 的設定檔新增至 Identity Vault，並將它們與個人、部門或組織等使用者設定檔整合。
自動化白頁 / 黃頁目錄	Identity Manager 可以建立統一的目錄，且具有不同層級的資訊，以供內部和外部使用。外部目錄可能僅包含電子郵件地址；而內部目錄可能包含地點、電話、傳真、行動電話、自宅地址等。

活動	Identity Manager 解決方案
增強使用者設定檔	Identity Manager 藉由新增或同步化電子郵件地址、電話號碼、自宅地址、優先設定、上下級關係、硬體資產、電話、金鑰、庫存和其他資訊，來增強使用者設定檔。
統一通訊存取	Identity Manager 會針對每一個別使用者或群組將目錄同步化爲通用管理介面，以簡化其網路、電話、呼叫器、Web 或無線存取。
加強夥伴關係	Identity Manager 可藉由在防火牆外的夥伴系統中建立設定檔 (員工、客戶等)，讓夥伴立即提供所需的服務，以加強夥伴關係。
改善供應鏈	Identity Manager 可辨識並彙總每個客戶多個帳戶的例項來改善客戶服務。
建立客戶忠誠度	Identity Manager 因爲發現客戶的需求而提供了新服務，讓客戶可以在同一個位置檢視所有資料，而不需前往個別的應用程式或區域。
自訂服務	Identity Manager 可對使用者 (員工、客戶、夥伴等) 提供包括關係、狀態和服務記錄在內之完整同步化資訊的設定檔。 這些設定檔可用於提供不同層級的服務和資訊存取權限，並根據客戶身分提供即時的自訂服務。
密碼管理	透過使用者應用程式，管理員可設定詰問 / 答覆問題，並允許使用者設定自己的密碼。 Client Login Extension for Novell Identity Manager 3.5.1 可將連結新增到 Novell 和 Microsoft GINA 登入用戶端，來協助密碼自助服務。用戶端允許存取 Identity Manager 的「使用者應用程式密碼自助服務」功能。 如果 Identity Manager 驅動程式支援密碼同步化，則可同步化多個連線系統的密碼。

1.2 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)

1.3 Identity Manager 3.5.1 的新功能

1.3.1 Identity Manager

支援 Open Enterprise Server 2

Open Enterprise Server 2 包含許多必要的軟體元件，包括 SUSE® Linux Enterprise Server 10 Support Pack 1、NetWare® 6.5 Support Pack 7、eDirectory 8.8 Support Pack 2、iManager 2.7 和 Security Services 2.0.5。Linux 和 NetWare Open Enterprise Server 2 平台均支援 Identity Manager。

iManager 外掛程式

Identity Manager 這個版本的 iManager 外掛程式與 Identity Manager 3.0 相容。除了回溯相容外，Identity Manager 3.5.1 也包含可報告驅動程式快取檔案資訊的外掛程式。

支援額外的作業系統平台

Identity Manager 支援舊版 Identity Manager 所支援的所有作業系統平台。此外，Identity Manager 某些元件可在 Microsoft Windows Vista*、AIX* 5.3、Red Hat* 5 AS/ES 64 位元組，和 Open Enterprise Server 2 (包含 SUSE Linux Enterprise Server 10 SP1 和 NetWare 6.5 SP7) 上執行。

支援額外的應用程式

Identity Manager 支援舊版 identity manager 所支援的所有應用程式。此外，Identity Manager 也支援安裝 eDirectory 8.8 SP2 和 iManager 2.7 的平台上的這些應用程式。

Non-root 安裝

Identity Manager 3.5.1 包括資訊和指令碼，可將 Identity Manager Metadirectory 引擎安裝至 eDirectory 的 Non-root 安裝。如需執行 Identity Manager 的 Non-root 安裝的步驟，請參閱第 4.9 節 「Identity Manager 的 Non-root 安裝」 (第 88 頁)。

Bundled 元件

Identity Manager 包含 Client Login Extension for Novell Identity Manager 3.5.1 和 Designer 2.1。

Client login extension for Novell Identity manager 3.5.1 是 Identity Manager 的新元件，它可將連結新增到 novell 和 microsoft gina 登入用戶端，來協助密碼自助服務。使用者在其登入用戶端中按一下「*忘記密碼*」連結時，Client Login Extension 會啓動限制的瀏覽器以存取 Identity Manager 的「使用者應用程式密碼自助服務」功能。此功能有助於減少因忘記密碼而致電到服務台求助的電話。

如需 Client Login Extension for Novell Identity Manager 3.5.1 的詳細資訊，請參閱「Novell Identity Manager 3.5.1 Administration Guide」中的 *Client Login Extension for Novell Identity Manager 3.5.1* 。如需有關 Designer 2.1 的詳細資訊，請參閱第 1.3.2 節「Designer for Identity Manager」(第 15 頁)。

1.3.2 Designer for Identity Manager

本節說明 Designer for Identity Manager 的增強功能。如需 Designer 2.1 所有增強和變更部分的詳細清單，請參閱新功能 (http://www.novell.com/documentation/designer21/index.html)。

地區設定支援

Designer for Identity Manager 的「提供」檢視現在可讓您定義：

- 使用者應用程式的預設地區設定。(這個地區設定用於在找不到使用者符合的地區設定時顯示內容。)
- 使用者應用程式驅動程式支援的地區設定。

此外，Designer 現在可以匯入和匯出電子郵件範本的本土化資料。

提供團隊編輯器

Designer for Identity Manager 現在包括「提供團隊編輯器」外掛程式。這個新的編輯器可讓您定義一組使用者，做爲「使用者應用程式」其「*要求與核准*」標籤中的團隊。可決定哪些人可以管理與此小組相關的提供申請和核准任務。

「提供團隊編輯器」提供另一種 iManager 外掛程式的團隊管理方法。

「提供」檢視適用性增強

「提供」檢視已增強，現在您能夠：

- 組織類別中的提供要求定義。您可以使用目錄抽象層編輯器來定義類別。
- 一次爲多個提供要求定義指派多個屬性 (例如託管者指派)。

電子郵件活動

電子郵件活動提供方法可將電子郵件傳送到核准活動外有興趣的一方。

核准活動

核准活動現在可從 「核准」活動屬性頁面上建立新表單。

「核准」活動也能夠將電子郵件通知中的 「回覆」地址設爲與 「寄件者」地址不同的地址。

記錄活動

「記錄」活動現在允許自訂要新增到工作流程其 「備註歷程」的訊息。

表單增強

表單現在支援 onload 事件。

ECMA 增強

目前支援以下欄位方法：

- getName()
- 驗證 ()
- 隱藏 ()
- 顯示 ()
- 焦點 ()
- 選擇 ()
- 啓用 ()
- 設定必要 ()

增強提供要求定義顯示名稱

提供要求定義的顯示名稱現在可定義爲靜態字串或可本土化的 ECMA 運算式。透過定義運算式，您可以自訂核准的工作顯示名稱。在使用者應用程式的工作清單中，這允許相同工作流程的不同例項顯示唯一的項目。

1.3.3 使用者應用程式

- 「使用者介面增強」(第 16 頁)
- 「跨平台變更」(第 17 頁)
- 「互通性變更」(第 17 頁)
- 「SOAP 端點增強」(第 17 頁)
- 「其他功能增強」(第 18 頁)

使用者介面增強

「團隊工作」顯示已經增強，讓介面更有彈性，並能最佳化使用者經驗。「團隊工作」頁面以兩個新的呈現檢視顯示動態內容，分別是 「範本」檢視和 「展示」檢視。這兩種格式使

用表格向使用者顯示資料。在這兩個格式中，使用者可以選擇要顯示的欄、指定欄顯示的順序，並按照欄中的值排序工作。

顯示格式的選項由管理員控制。管理員可視呈現的優先設定，或因須利用以下區分功能，選擇將檢視疊在另一檢視上：

- 「範本」檢視 (預設) 提供支援盲胞的協助工具。此外，它也包括可自訂的分頁功能。
- 「展示」檢視支援過濾，並提供資料匯出工具。

跨平台變更

這個版本爲以下應用程式伺服器平台新增執行時期支援：

- JBoss* 4.2.0 on SUSE Linux Enterprise Server 10.1、SUSE Linux Enterprise Server 9 SP2 和 Windows 2003 Server SP1
- WebSphere* 6.1 on Solaris* 10 和 Windows 2003 SP1

  使用者應用程式的安裝程式會爲您安裝 WAR。但是，您必須手動將 WAR 部署爲 WebSphere。

  WebSphere 的資料庫支援包括 Oracle* 10g、MS SQL* 2005 SP1 和 DB2。

  如需支援平台的完整清單，請參閱 「Identity Manager 的系統要求」(第 27 頁)。

本版本也新增以下瀏覽器環境的支援：

- Windows 2000 Professional SP4、Windows XP SP2 和 Windows Vista Enterprise Version 6 的 Internet Explorer 7
- Red Hat Enterprise Linux WS 4.0、Novell Linux Desktop 9、SUSE Linux 10.1 和 SUSE Linux Enterprise Desktop 10 的 Firefox*

互通性變更

這個版本已經進行以下互通性變更：

- 管理員現在可以使用組態設定來指定使用者應用程式是否應在「忘記密碼」畫面中顯示指示。
- 管理員現在可以使用組態設定來啓用或停用「登入」對話方塊中的密碼自動完成功能。這會控制瀏覽器是否讓使用者儲存其認證。
- 登入程序現在支援透過「存取管理員」驗證 Proxy 智慧卡。爲了讓此可行，使用者應用程式會接收插入在 HTTP 標頭的 SAML 主張，並使用這些主張讓 SASL 連線到目錄。

SOAP 端點增強

本版本的 SOAP 端點已進行以下增強：

- 已新增新的 VDX 服務，以提供可對目錄抽象層上執行查詢的 SOAP 端點。
- 已新增新的通知服務，以提供用於傳送電子郵件通知的 SOAP 端點。
- 已將名爲「取得程序陣列 ()」的新方法新增至「提供」服務，其中包括一個引數，可讓您限制傳回的程序數。
- 已將名爲「啓動關聯 ID()」的新方法新增至「提供」服務，可讓您啓動一組相關的工作流程，並使用關聯 ID 追蹤。

SOAP 端點讓開發人員能夠建置自己的應用程式。他們不會曝露在使用者應用程式的原始使用者介面上。

其他功能增強

使用者應用程式現在可讓您指定 URL 參數，這些參數可直接移至提供要求表單。

1.4 Identity Manager 安裝程式和服務

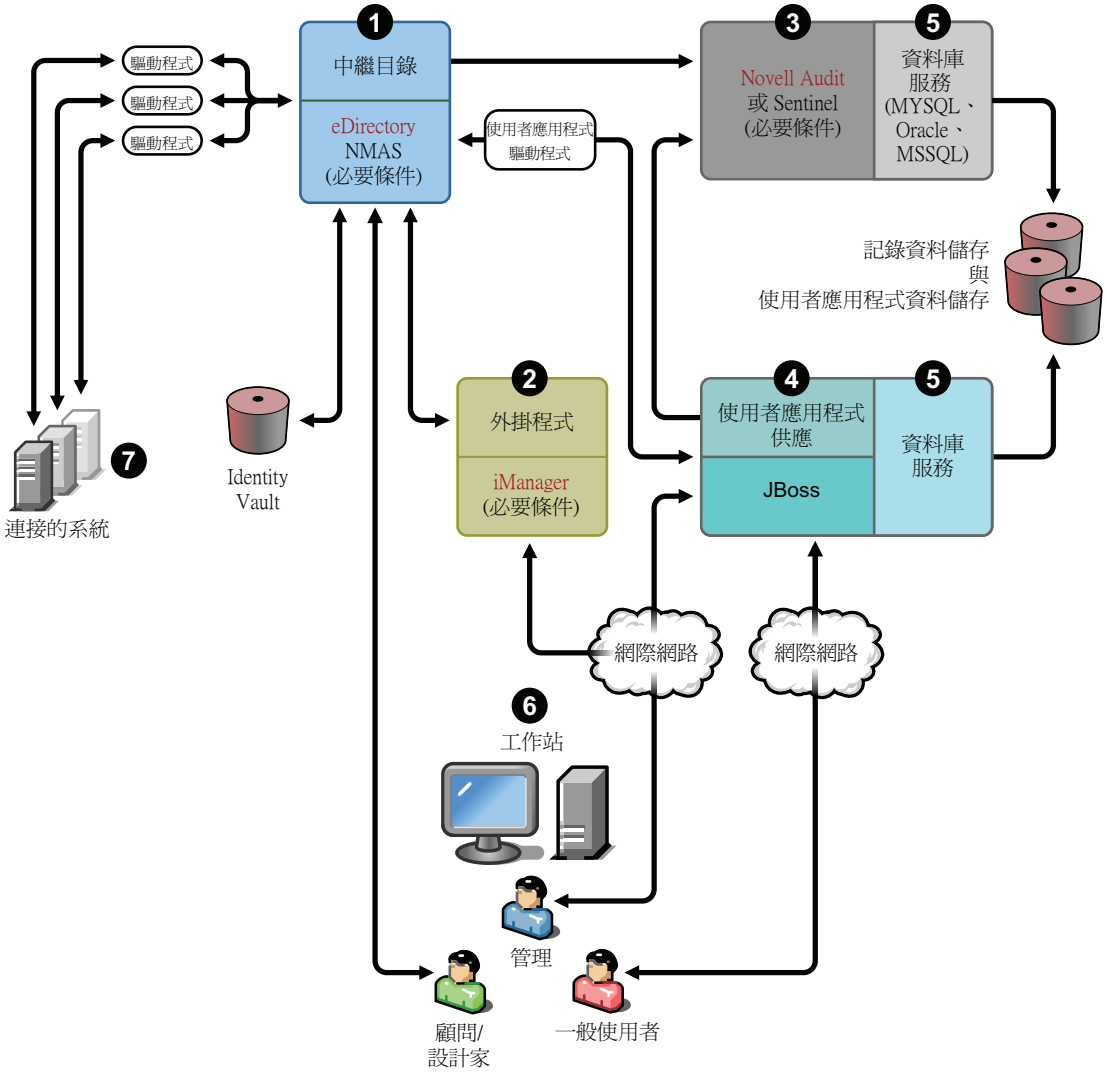
下列各節說明 Identity Manager 的安裝程式和服務。本節描述各種可讓 Identity Manager 功能完整的元件。

- 第 1.4.1 節 「安裝程式」 (第 18 頁)
- 第 1.4.2 節 「服務」 (第 20 頁)

1.4.1 安裝程式

Identity Manager 具有三個不同的安裝程式，以及七種需要安裝和設定組態的服務。下列圖形一覽了所有可讓 Identity Manager 功能完整的元件。

圖 1-1 Identity Manager 七種服務的圖形綜覽



以下是安裝程式和每個安裝所執行之操作的清單：

- 「Identity Manager Metadirectory 系統安裝」(第 20 頁)
- 「使用者應用程式和提供模組安裝」(第 20 頁)
- 「Designer 安裝」(第 20 頁)

附註：在安裝 Identity Manager 元件之前，您必須先安裝必要的軟體，包括 eDirectory 8.7.3.6 或更新版本 (用於上圖的 1 號和 3 號服務)、Security Services 2.0.4 及 NMAS 3.1.3 (1 號和 3 號)、iManager 2.6 或更新版本 (2 號)，以及 Novell Audit 2.0.2 Starter Pack 或 Sentinel 5.1.3 (3 號)。您可以從 Novell 下載網站 (http://download.novell.com) 取得必要軟體。如需必要軟體和安裝需求的詳細資訊，請參閱第 1.5 節 「Identity Manager 的系統要求」(第 27 頁)。

Identity Manager Metadirectory 系統安裝

該安裝程序會執行下列功能：

- 延伸整個 Identity Manager 產品的 eDirectory 綱要。
- 安裝 Metadirectory 引擎和系統服務。
- 安裝 iManager 的 Identity Manager 外掛程式。
- 安裝 Metadirectory 系統「遠端載入器」(如果已選取)。
- 安裝已連接系統的驅動程式。(驅動程式已安裝，但在啓用之前處於休眠狀態)。
- 安裝 Identity Manager 報告，以及任何 Metadirectory 系統公用程式和工具。

使用者應用程式和提供模組安裝

下列服務安裝在 Linux* 和 Windows 上：

- JBoss* 和 MySQL* (如果已選取)。
- 執行使用者應用程式所需的 WAR 檔案。

Designer 安裝

針對 Linux 和 Windows 各有一個安裝程式：它們會執行以下工作：

- 安裝 Eclipse* 架構。
- 安裝基本外掛程式。
- 安裝 Metadirectory 外掛程式
- 安裝目錄抽象層外掛程式。
- 安裝工作流程編輯器外掛程式。

1.4.2 服務

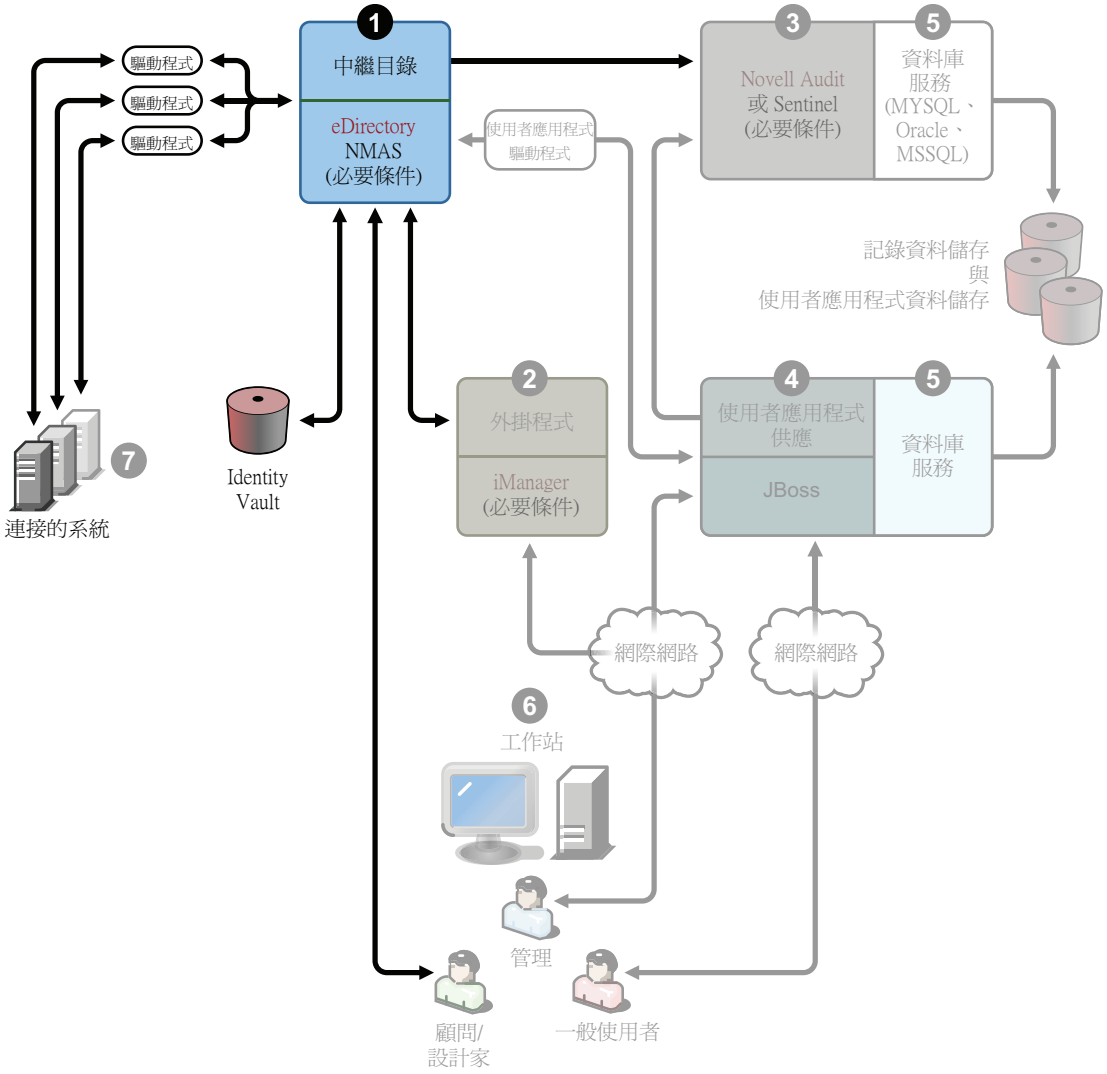
Identity Manager 提供了七種可以安裝和設定組態的服務。雖然在生產環境中不建議這樣做，但是您可以在單一電腦上安裝並設定所有七種服務。或者，您也可以在每個電腦上部署一種服務，或採用其他任何部署方式。第 1.5 節「Identity Manager 的系統要求」(第 27 頁) 對每種服務適用且受支援的必要硬體和軟體提出說明。

- 「Metadirectory 系統服務」(第 20 頁)
- 「Web 型態的管理服務」(第 22 頁)
- 「安全記錄服務」(第 23 頁)
- 「使用者應用程式和提供模組」(第 24 頁)
- 「資料庫服務」(第 24 頁)
- 「工作站」(第 26 頁)
- 「已連接系統」(第 26 頁)

Metadirectory 系統服務

此系統會用做 Identity Vault，且您在生產環境中僅需要一個 Metadirectory 引擎例項。

圖 1-2 *Metadirectory 系統服務*

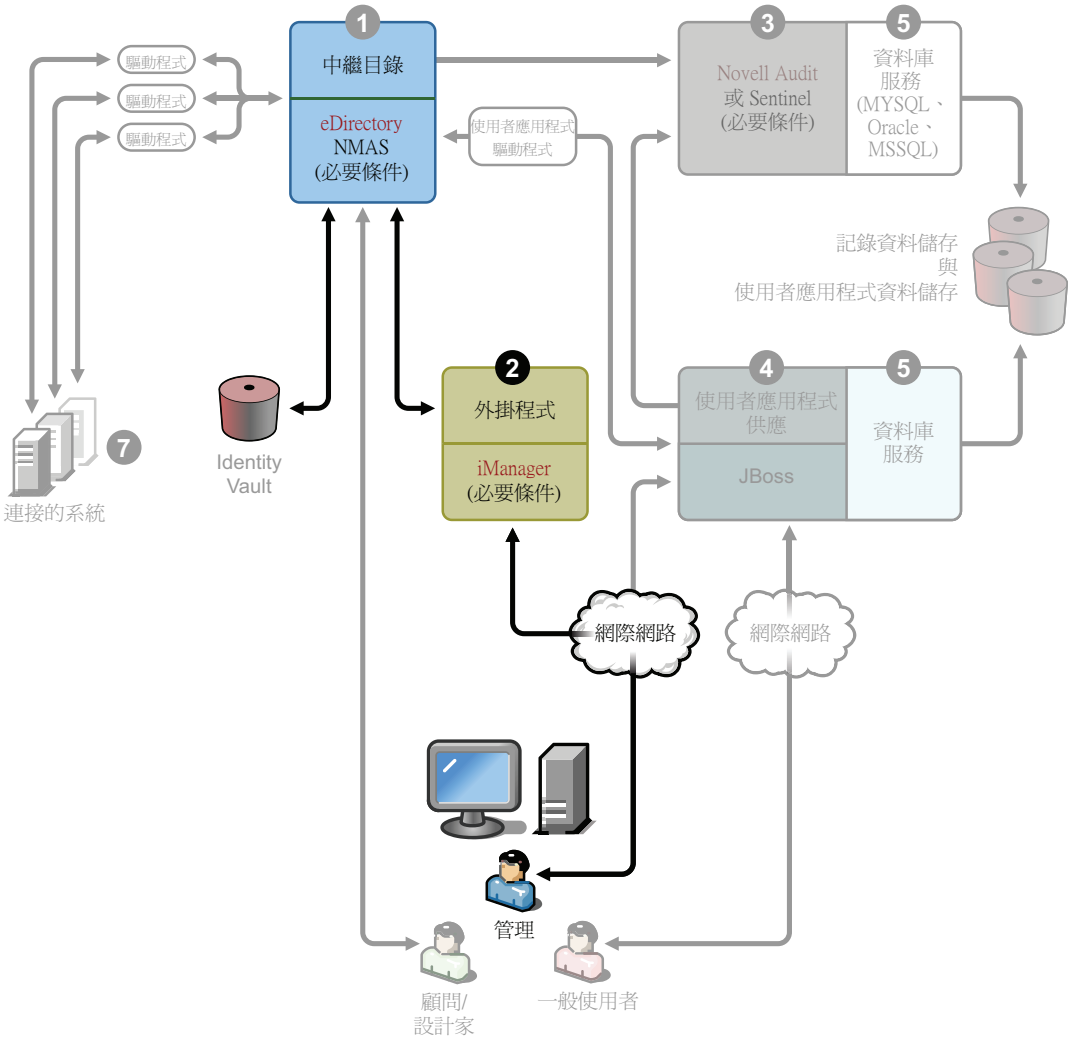


當一個系統的資料變更時，Identity Manager 中包含的 Metadirectory 引擎會根據您定義的業務規則，偵測並傳達這些變更至其他已連接系統。此解決方案可讓您針對任何特定資料強制執行授權資料來源 (例如，HR 應用程式擁有使用者的 ID，而郵件系統可能擁有使用者的電子郵件帳戶資訊)。

若要安裝 Identity Manager 和此服務，請參閱第 4 章 「安裝 Identity Manager」 (第 63 頁)。若要在安裝 Identity Manager 之前瞭解先決條件爲何，請參閱「Metadirectory 系統」 (第 28 頁) 所列的系統需求。

Web 型態的管理服務

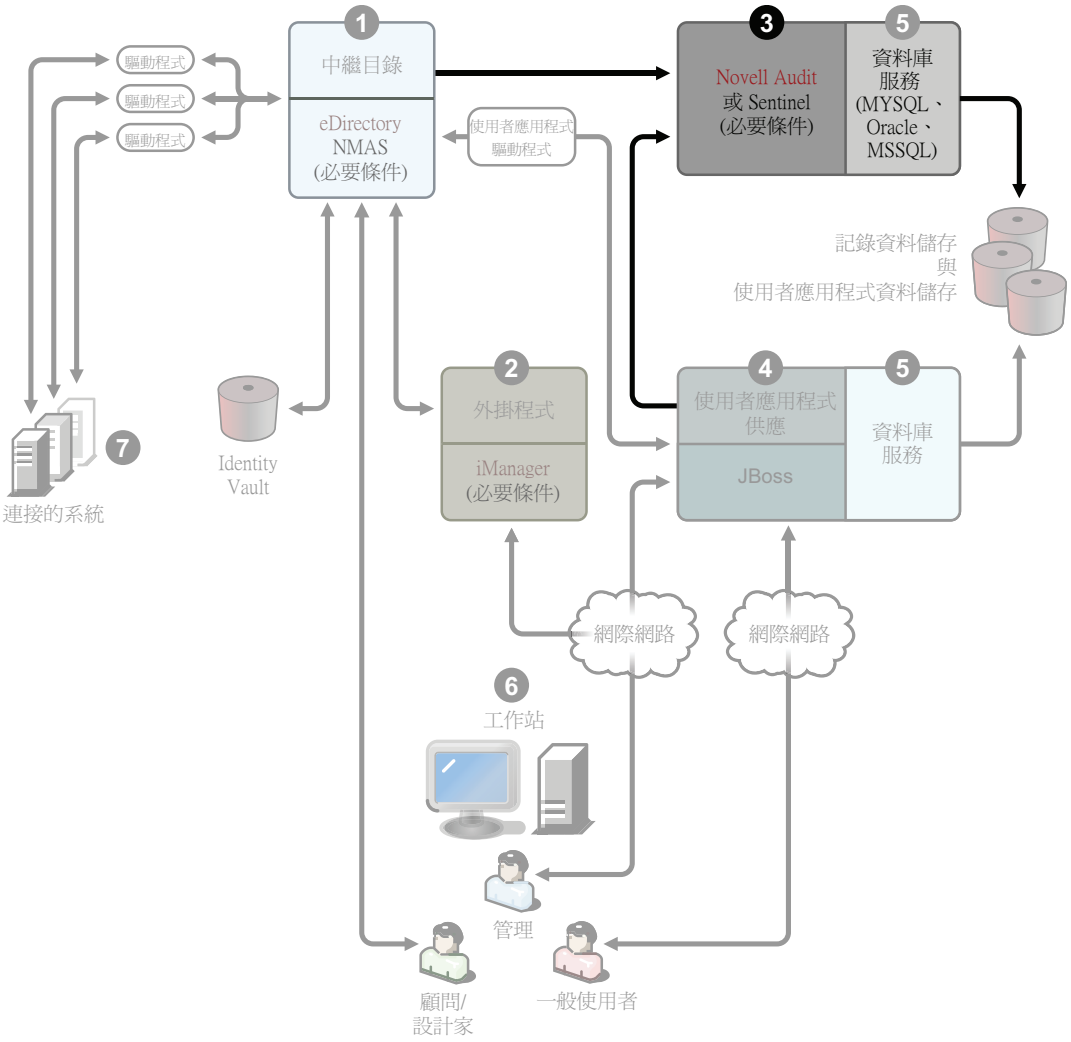
圖 1-3 Web 型態的管理服務



利用此服務可以管理 eDirectory 和 Metadirectory 系統 (使用已安裝 Identity Manager 和「使用者應用程式」外掛程式的 iManager 2.5 和更新版本)。您可以在安裝 Identity Manager 之伺服器上將 Identity Manager 外掛程式安裝至 iManager。若要安裝 Identity Manager 外掛程式和此服務，請參閱第 4 章 「安裝 Identity Manager」 (第 63 頁)。

安全記錄服務

圖 1-4 安全記錄服務

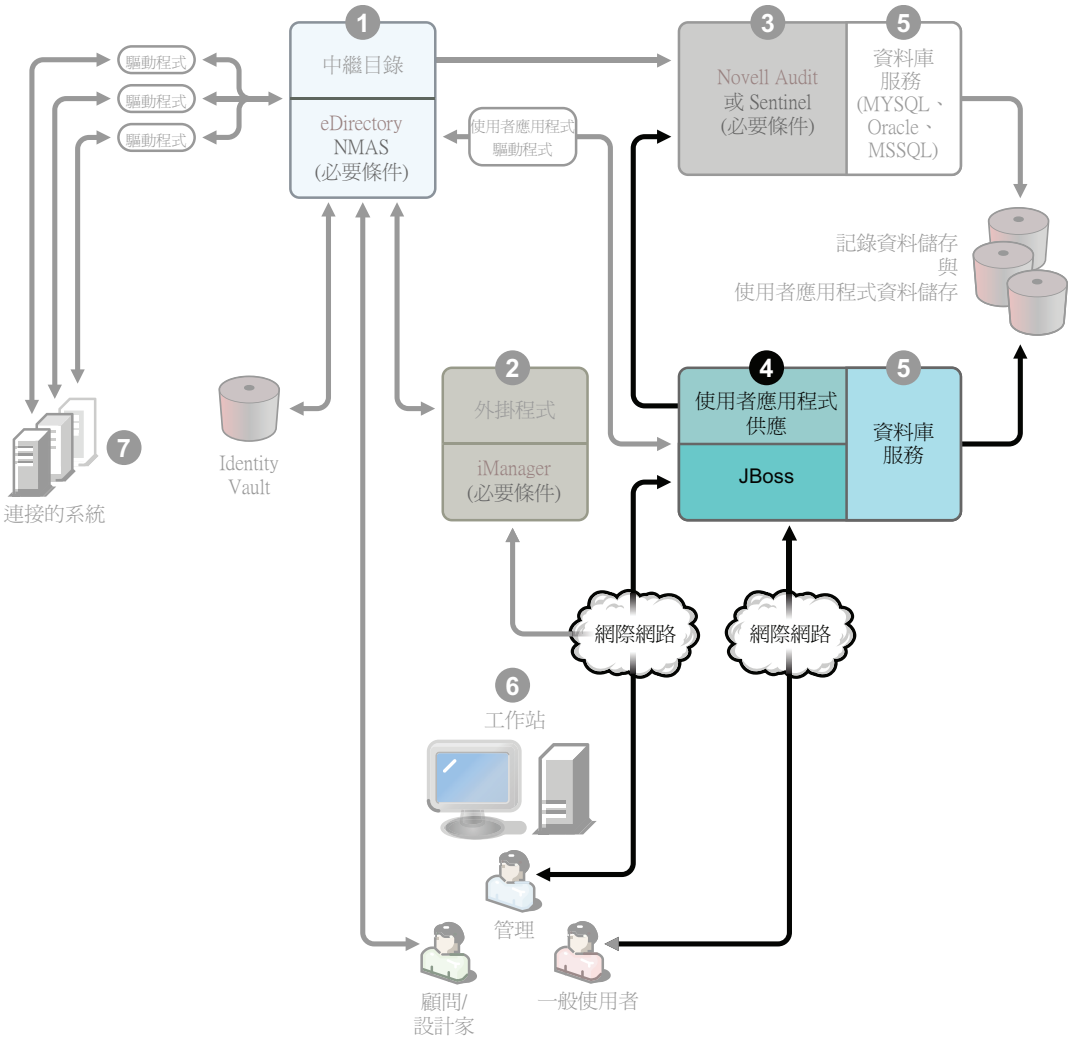


登入事件的儲存機制 (Identity Manager 軟體未安裝在此伺服器上，但安全記錄服務是必要的)。這是一種集中式服務，由 Identity Manager 和一般使用者應用程式以及工作流程系統服務所使用，並可從 Novell 下載網站 (http://download.novell.com) 個別下載。

<Check Alignment of PHs> 在「下載網站」上的「產品」或「技術」下拉功能表中，選取「 *Audit* 」，並按一下「*搜尋*」。按一下「 *Audit 2.0.2 Starter Pack* 」。請依隨附於 Starter Pack 的安裝指示操作。

使用者應用程式和提供模組

圖 1-5 使用者應用程式和提供模組

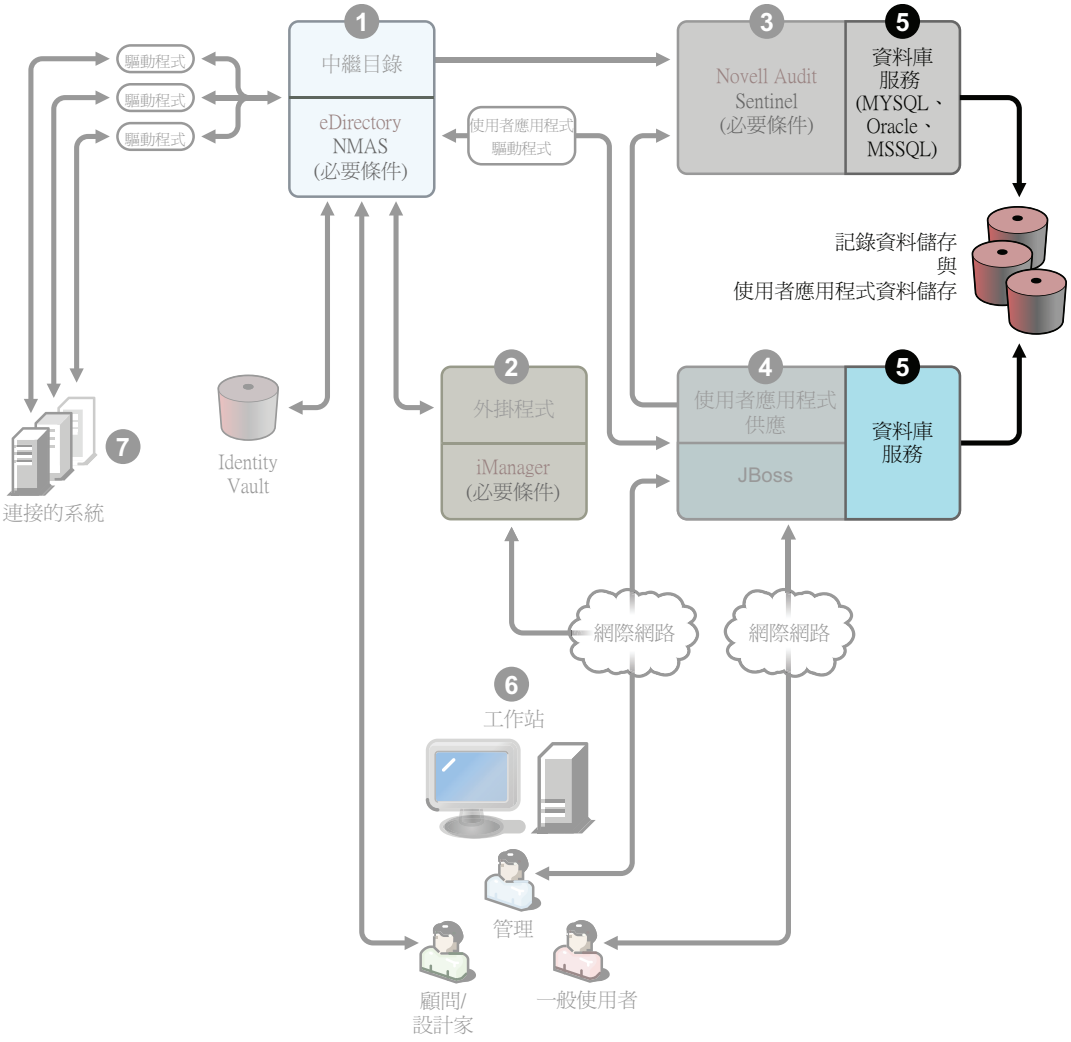


若要安裝此服務，請參閱第 5 章 「安裝「使用者應用程式」」(第 93 頁)。第 5.1 節 「安裝的先決條件」(第 93 頁) 說明了可受支援的硬體，以及每種服務的軟體準備需求。

資料庫服務

安全記錄服務和使用者應用程式 / 工作流程系統都需要資料庫。您可以設定一個資料庫用於兩個應用程式，或針對每個應用程式設定獨立的資料庫。

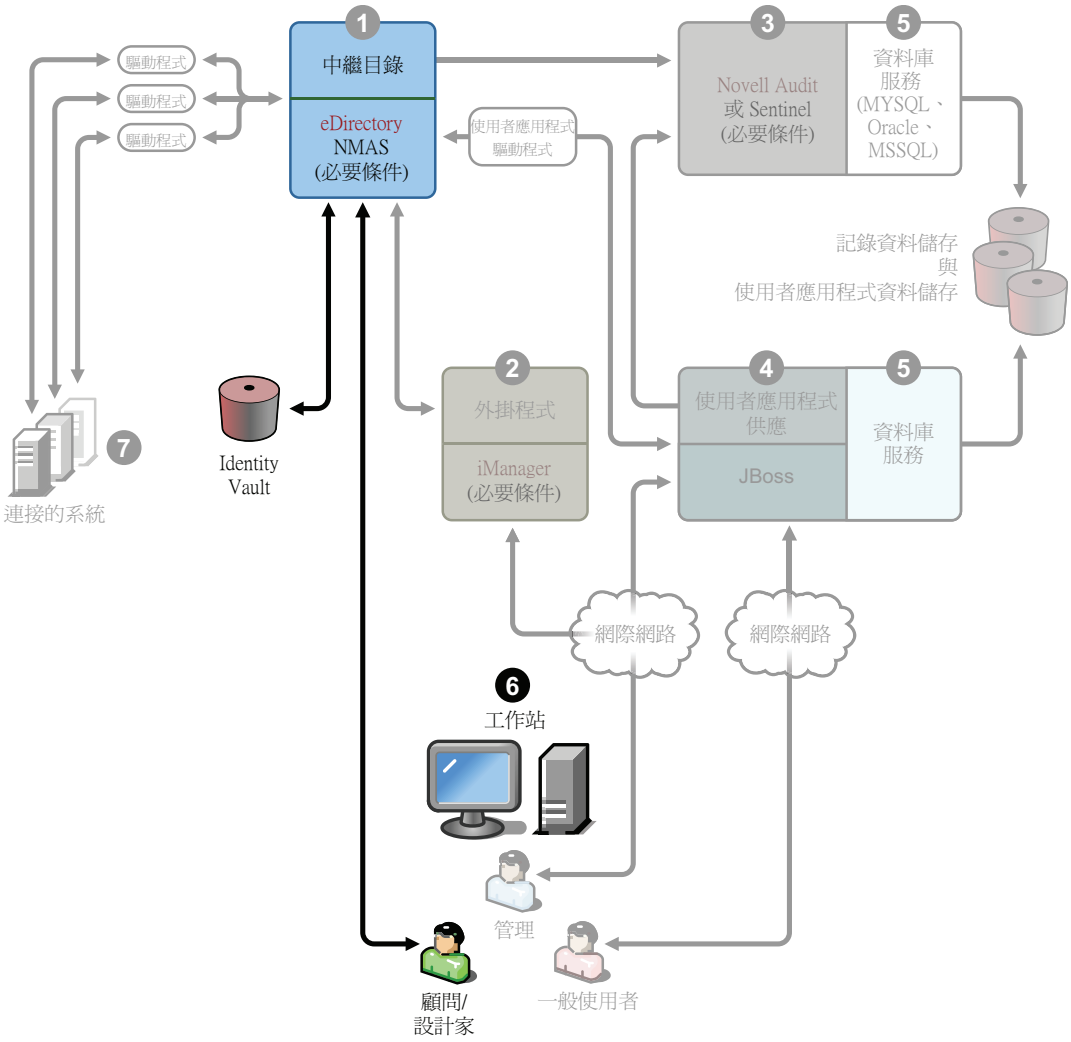
圖 1-6 資料庫服務



安全記錄服務不包括特定的資料庫。然而，您可以使用「使用者應用程式」和「提供」隨附的 MySQL 資料庫。使用者應用程式隨附 JBoss Application Server 4.2.0 版，且需要 JRE* 1.5.0_10。若要安裝此服務，請參閱第 5.2 節「安裝和組態」(第 99 頁)。

工作站

圖 1-7 Designer 的工作站服務

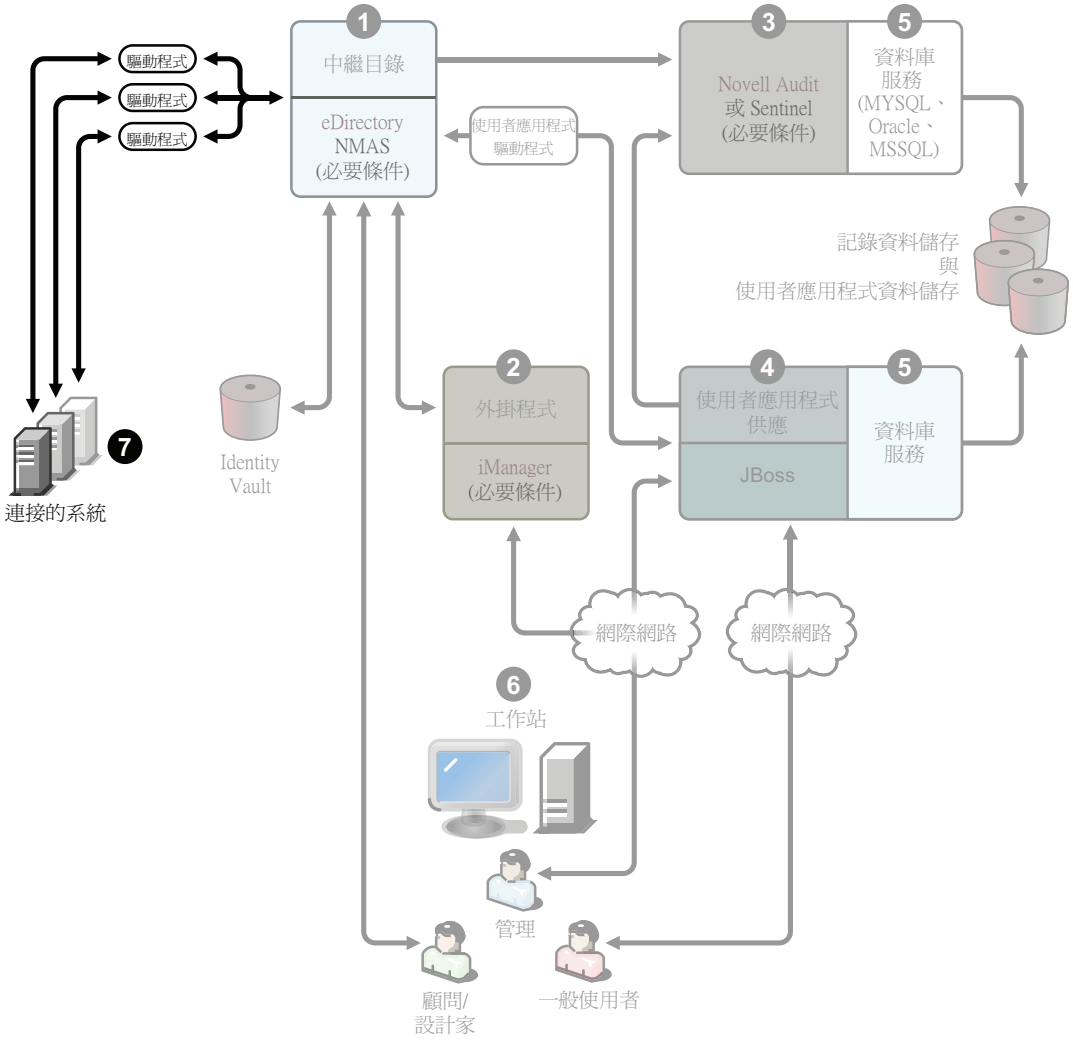


可讓 Designer 用來設計、部署和記錄 Identity Manager 系統，並用於產品隨附的公用程式、報告和工具。若要在工作站上安裝 Designer，請參閱「Designer 2.1 for Identity Manager 3.5.1」指南內的「*安裝*」。

已連接系統

這是代管驅動程式的位置，而這些已連接系統可以是應用程式、資料庫、伺服器及其他服務。每個已連接的應用程式都需要個人具有應用程式特定的知識和職責。每個驅動程式都需要已連接系統可以使用，並且已提供相關的應用程式介面 (API)。

圖 1-8 已連接系統



安裝驅動程式是 Identity Manager 安裝程序的一部分。若要安裝 Identity Manager 和此服務，請參閱第 4 章 「安裝 Identity Manager」（第 63 頁）。若要瞭解設定驅動程式的詳細資訊，請參閱 Identity Manager 驅動程式文件網站 (http://www.novell.com/documentation/idmdrivers) 上的驅動程式特定文件。

1.5 Identity Manager 的系統要求

Novell Identity Manager 包含可以在多系統和平台上的環境內安裝的元件。根據系統組態，您可能需要多次執行 Identity Manager 安裝程式，以在適當的系統上安裝 Identity Manager 元件。

下表列出 Identity Manager 的安裝元件，以及每個元件的要求。

表格 1-3 *Identity Manager 系統元件和要求*

系統元件	系統需求	註
Metadirectory 系統 ◆ Metadirectory 引擎 ◆ Novell Audit 代辦 ◆ 服務驅動程式 ◆ Identity Manager 驅動程式 ◆ 公用程式 (包含「應用程式工具」和「Novell Audit 設定」工具)	下列其中一個作業系統： ◆ 含最新支援套件的 eDirectory 6.5 ◆ 含最新支援套件 1.0 的 Novell Open Enterprise Server (OES) ◆ Novell Open Enterprise Server (OES 2.0 ◆ 含最新 Service Pack 的 Windows 2000 Server (32 位元) ◆ 含最新 Service Pack 的 Windows Server 2003 (32 位元) ◆ Linux Red Hat 3.0、4.0 和 5.0 ES 和 AS (可同時支援 32 位元和 64 位元) ◆ 含最新支援套件的 Suse Linux Enterprise Server 9 和 10 (可同時支援 32 位元和 64 位元) ◆ Solaris 9 或 10 ◆ AIX 5.2L，5.2 和 5.3 版 下列其中一個 eDirectory 版本： ◆ 含最新支援套件的 eDirectory 8.7.3.6 ◆ 含最新支援套件的 eDirectory 8.8 Security Services 2.0.5 (NMAS 3.1.3)	如果您使用的是 Metadirectory 系統平台，則支援在實作中使用 VMWare*。 本版本中所有的 Identity Manager 軟體元件均爲 32 位元，即使它們在 64 位元處理器或 64 位元作業系統上執行。除非另有指定，否則 OES、NetWare、Windows 和 Linux 平台 (Red Hat 和 SUSE) 都支援下列所有 32 位元模式的處理器： ◆ Intel* x32-32 ◆ AMD* x86-32 ◆ Intel EM64T ◆ AMD Athlon64* 和 Opteron* Identity Manager 可支援下列的 eDirectory 8.8 功能： ◆ 相同伺服器上的多個 eDirectory 例項 ◆ 加密屬性 eDirectory 8.8 可支援 64 位元的 Red Hat Linux 4.0。 Windows Server 2003 的 64 位元版的「密碼同步化」可供使用。 請確定在安裝 eDirectory 8.8 之前已完整備份 eDirectory 資料庫。eDirectory 8.8 會升級資料庫結構部份，而且升級之後不允許再復原該資料庫結構。 現在，當 Xen Virtual Machine (VM) 做爲平行虛擬化模式中的訪客作業系統而在 SLES 10 中執行時，Xen 虛擬化可獲得 SUSE Linux Enterprise Server 10 的支援。需要適用於 SLES 10 的 Xen 修補程式 (請參閱 TID # 3915180 (http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3915180&sliceId=SAL_Public&dialogID=20406933&stateId=0%200%200414606))。

系統元件	系統需求	註

Web 型態的管理伺服器
• 密碼同步化
• iManager 2.6 和外掛程式
• iManager 2.7 和外掛程式
• 驅動程式組態
	下列其中一個作業系統：
	• NetWare 上含最新支援套件的 Novell Open Enterprise Server (OES) 1.0
	• Novell Open Enterprise Server (OES 2.0)
	• 含最新支援套件的 eDirectory 6.5
	• 含最新 Service Pack 的 Windows 2000 Server (32 位元)
	• 含最新 Service Pack 的 Windows Server 2003 (32 位元)
	• Microsoft Windows Vista
	• Linux Red Hat Linux 3.0、4.0、5.0 ES 和 AS (可同時支援 32 位元和 64 位元)
	• 含最新支援套件的 Solaris 9 或 10
	• 含最新支援套件的 Suse Linux Enterprise Server 9 和 10 (可同時支援 32 位元和 64 位元)
	透過「iManager 工作站」支援的作業系統：
	• 含最新 Service Pack 的 Windows 2000 Professional
	• 含 SP2 的 Windows XP
	• SUSE Linux Enterprise Desktop 10 SP
	• SUSE Linux 10.1
	下列軟體。
	• Novell iManager 2.6 和 2.7，含最新的支援套件和外掛程式
		本版本中所有的 Identity Manager 軟體元件均爲 32 位元，即使它們在 64 位元處理器或 64 位元作業系統上執行。除非另有說明，否則 OES、NetWare、Windows 和 Linux 平台 (Red Hat 和 SUSE) 都支援下列所有 32 位元模式的處理器：
		• Intel x86
		• AMD x86
		• Intel EM64T
		• AMD Athlon64 和 Opteron
		• 瀏覽器支援由 iManager 2.6 決定。此清單目前包括：
		  • Internet Explorer 6、SP1 和更新版本
		  • Internet Explorer 7
		  • Firefox* 2.0 和更新版本
		• 您必須完成「iManager 組態精靈」或 Designer 公用程式，以在 eDirectory 中安裝或部署入口網站內容。
		• (Windows) Novell Client™ 4.9 可從 Novell 軟體下載 (http://download.novell.com/index.jsp) 取得。
		• 當使用 iManager 登入其他網路樹，以管理遠端 Identity Manager 伺服器時，如果您使用遠端伺服器的伺服器名稱而不是 IP 位址，則可能會遇到錯誤。
		• 64 位元版的 Windows 2003 只支援「密碼同步化」代辦。

系統元件	系統需求	註
安全記錄服務 ◆ 安全記錄伺服器 ◆ 平台代辦 (用戶端元件) ◆ Novell Audit 2.0.2 或 Sentinel 5.1.3	針對「安全記錄伺服器」，爲下列其中一個作業系統： ◆ 含最新支援套件 2.0 的 Novell Open Enterprise Server (OES) 2.0 ◆ 含最新支援套件的 eDirectory 6.5 ◆ 含最新 Service Pack 的 Windows 2000 Server (32 位元) ◆ 含最新 Service Pack 的 Windows 2003 Server (32 位元) ◆ Red Hat Linux 4.0 或 5.0 AS 和 ES (32 位元和 64 位元)，但 Novell Audit 只能在 32 位元模式中執行) ◆ 含最新支援套件的 Solaris 9 或 10 ◆ SUSE Linux Enterprise Server 9 或 10 (32 位元和 64 位元，但 Novell Audit 只能在 32 位元模式中執行) ◆ Novell eDirectory 8.7.3.6 或 8.8，含最新支援套件 (必須在安全記錄伺服器上安裝) 針對「平台代辦」，爲下列其中一個作業系統： ◆ 含最新支援套件的 Novell Open Enterprise Server (OES) 1.1 SP1 ◆ 含最新支援套件的 eDirectory 6.5 ◆ Windows 2000 或 2000 Server、XP 或含最新 Service Pack 的 Windows Server 2003 (32 位元) ◆ Red Hat Linux 3 或 4 AS 和 ES (32 位元和 64 位元，但 Novell Audit 只能在 32 位元模式中執行) ◆ Solaris 8、9 或 10 ◆ SUSE Linux Enterprise Server 9 或 10 (32 位元和 64 位元，但 Novell Audit 只能在 32 位元模式中執行) iManager 2.6 和 2.7，含最新支援套件和外掛程式	OES、NetWare、Windows 和 Linux 平台 (Red Hat 和 SUSE) 支援下列所有 32 位元模式的處理器： ◆ Intel x86 ◆ AMD x86 ◆ Intel EM64T ◆ AMD Athlon64 和 Opteron 最低「安全伺服器」要求包括： ◆ 單一處理器、具有 Pentium* II 400 MHz 的伺服器等級 PC ◆ 至少 40 MB 磁碟空間 ◆ 512 MB RAM 允許記錄 eDirectory 事件的 eDirectory Instrumentation 支援下列 eDirectory 版本： ◆ eDirectory 8.7.3 (NetWare、Windows、Linux 和 Solaris) ◆ 含最新支援套件的 eDirectory 8.8 允許記錄 NetWare 事件的 NetWare Instrumentation 支援下列 NetWare 版本： ◆ 含最新支援套件的 eDirectory 5.1 ◆ 含最新支援套件的 eDirectory 6.0 ◆ NetWare 6.5 或含最新支援套件的 NetWare 6.5 ◆ 含最新支援套件的 Novell Open Enterprise Server (OES)

系統元件	系統需求	註
使用者應用程式	**應用程式伺服器** 使用者應用程式在 JBoss 和 WebSphere 上執行，如下所述。 以下平台支援 JBoss 4.2.0： ◆ 含最新支援套件的 Novell Open Enterprise Server (OES) 1.1 SP2 ◆ Novell Open Enterprise Server (OES) 2--SLES 10 SP1 和 NetWare 6.5 SP7 ◆ SUSE Linux Enterprise Server 9 SP2 (OES 1.0 SP2 內含) 和 10.1.x (6 位元 JVM*) ◆ Windows 2000 Server SP4 (含 32 位元) ◆ Windows 2003 Server SP1 (含 32 位元) ◆ Solaris 10 支援套件，日期 6/06 以下平台支援 WebSphere 6.1： ◆ Solaris 10 (64 位元模式) ◆ Windows 2003 SP1 以下平台支援 WebLogic 10： ◆ Solaris 10 (64 位元模式) ◆ Windows Server SP 11 使用者應用程式需要 JRE* 1.5.0_10 (請參閱第 5.1 節 「安裝的先決條件」 (第 93 頁)) **瀏覽器** 使用者應用程式支援 Firefox 和 Internet Explorer，如下所示。 以下平台支援 Firefox 2： ◆ Windows 2000 Professional SP4 ◆ 含 SP2 的 Windows XP ◆ Red Hat Enterprise Linux 4.0 ◆ Novell Linux Desktop 9 ◆ SUSE Linux 10.1 ◆ SUSE Linux Enterprise Desktop 10 SP 以下平台支援 Internet Explorer 7： ◆ Windows 2000 Professional SP4 ◆ 含 SP2 的 Windows XP ◆ Windows Vista Enterprise 6 版 以下平台支援 Internet Explorer 6： ◆ Windows 2000 Professional SP4 ◆ 含 SP2 的 Windows XP	SUSE Linux Enterprise Server 的 32 位元模式可支援下列處理器： ◆ Intel x86 ◆ AMD x86 ◆ Intel EM64T ◆ AMD Athlon64 和 Opteron SUSE Linux Enterprise Server 將在下列處理器上以 64 位元模式執行： ◆ Intel EM64T ◆ AMD Athlon64 ◆ AMD Opteron ◆ Sun SPARC* 現在，當 Xen Virtual Machine (VM) 做爲平行虛擬化模式中的訪客作業系統而在 SLES 10 中執行時，Xen 虛擬化可獲得 SUSE Linux Enterprise Server 10 的支援。需要適用於 SLES 10 的 Xen 修補程式 (請參閱 TID # 3915180 (http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3915180&sliceId=SAL_Public&dialogID=20406933&stateId=0%200%200414606))。

系統元件	系統需求	註
使用者應用程式的資料庫伺服器 ◆ MySQL ◆ Oracle ◆ MS SQL ◆ DB2	可使用 JBoss 支援以下資料庫： ◆ MySQL 5.0.27 版 ◆ Oracle 9i (9.2.0.1.0 和 9.2.0.5.0) ◆ Oracle 10g 2 版 (10.2.0.) ◆ MS SQL 2005 SP1 可使用 WebSphere 支援以下資料庫： ◆ Oracle 10g 2 版 (10.2.0.) ◆ MS SQL 2005 SP1 ◆ DB2 DV2 v9.1.0.0	使用者應用程式會使用資料庫執行各種任務，例如，儲存使用者應用程式的組態資料，以及爲任何進行中的工作流程活動儲存資料。 安全記錄服務和使用者應用程式與工作流程提供都需要資料庫。您可以設定一個資料庫用於兩個應用程式，或針對每個應用程式設定獨立的資料庫。安全記錄服務不包括特定的資料庫。 可同時使用精簡電腦驅動程式和 OCI 用戶端驅動程式支援 Oracle。
工作站 ◆ Designer ◆ iManager Web 存取	已經在下列平台上測試 Designer： Windows： ◆ 含最新 Service Pack 的 Windows 2000 Professional ◆ Windows XP SP2 ◆ 含最新 Service Pack 的 Windows Server 2003 (32 位元) ◆ Microsoft Windows Vista Linux： ◆ SUSE Linux Enterprise Server 10 (僅適用於 Designer) ◆ SUSE Linux 10.1 ◆ SUSE Linux Enterprise Desktop 10 SP ◆ Red Hat Linux 4.0 (僅適用於 Designer) ◆ Red Hat Fedora Core 5 (僅適用於 Designer) ◆ Novell Linux Desktop 9 ◆ GNOME、KDE、Red Hat Fedora	Designer 使用 Eclipse 做爲其開發平台如需平台特定的資訊，請參閱 Eclipse 網站 (http://www.eclipse.org/)。 Designer 的最低和建議硬體要求： ◆ 最低爲 1 GHz，建議爲 2 GHz 或更大。 ◆ 最低 RAM 爲 512 MB，建議 RAM 爲 1 GB 或更大。 ◆ 最低解析度爲 1024 x 768，建議解析度爲 1280 x 1024。 先決條件軟體： ◆ Microsoft Internet Explorer 6.0 SP1 ◆ Microsoft Internet Explorer 7 ◆ 或 Mozilla* Firefox 2.0

系統元件	系統需求	註
已連接的系統伺服器 (執行「遠端載入器」之個別伺服器上的主機) ◆ 遠端載入器 ◆ 「遠端載入器」組態工具 (僅限 Windows) ◆ Novell Audit 代辦 ◆ 密碼同步化代理程式 ◆ 已連接系統的驅動程式 Shim ◆ 已連接系統的工具	每個驅動程式都需要已連接的系統可以使用，並且已提供相關的應用程式介面 (API)。 如需每個系統特定的作業系統和已連接系統要求，請參閱 Identity Manager 驅動程式文件 (http://www.novell.com/documentation/idmdrivers)。	每個已連接的應用程式都需要個人具有應用程式特定的知識和職責。 遠端載入器系統： ◆ 含最新 Service Pack 的 Windows NT* 4.0、Windows 2000 Server 或 Windows Server 2003 ◆ 含最新 Service Pack 的 Windows Server 2003 (64 位元) ◆ Windows Server 2003 (64 位元) 支援密碼同步化代理程式 ◆ Red Hat Linux 3.0、4.0、5.0 ES 和 AS ◆ SUSE Linux Enterprise Server 9 或 10 ◆ Solaris 9 或 10 ◆ AIX 5.2L，5.2 和 5.3 版 Java 遠端載入器系統： ◆ HP-UX* 11i ◆ OS/400 ◆ zOS* ◆ 應該可以在具有 JVM 1.4.2 或以上版本的任何系統上使用

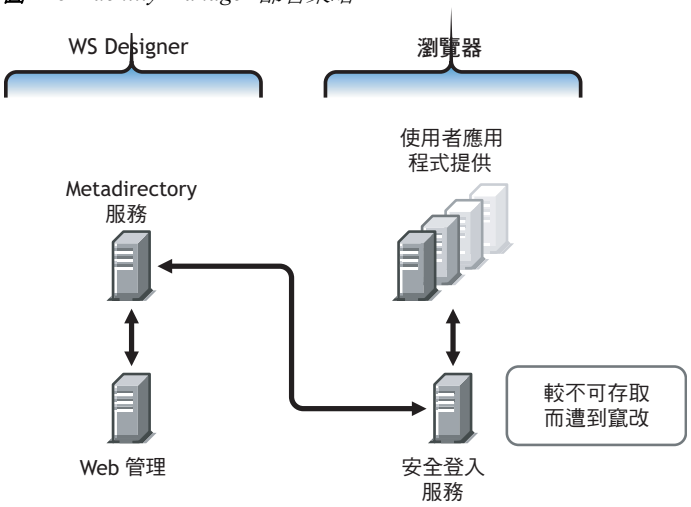
1.6 建議的部署策略

正如先前所指示，Identity Manager 隨附了您必須安裝並設定組態的七項服務。雖然不建議用於生產環境，但是您可以在單一伺服器上安裝並設定所有七項服務的組態。或者，您可以在每個伺服器上部署一項服務，或採用其他任何部署方式。

工作量是設計 Identity Manager 部署的主要因素。您可以分散的流量越多，應用程式所具有的潛在生產量就越好。

圖表 1-3 提供一種可行的部署策略，已針對 Metadirectory 服務、Web 型態的管理服務、安全記錄服務和使用者應用程式和工作流程模式的提供服務，分別建議了一個伺服器。

圖 1-9 Identity Manager 部署策略



Metadirectory 服務

部署 Identity Manager 服務的方式視服務工作量而定。例如，您可以在一個與已連接系統通訊的伺服器上安裝 Identity Manager 的 Metadirectory 服務。您只需要在一個執行 eDirectory 的伺服器上安裝 Metadirectory 引擎。

由於 iManager 的潛在生產量非常大，您可能不想將 Web 型態的管理服務與 Metadirectory 服務一起安裝。如果您確實要將 iManager 與 Identity Manager 安裝在相同的伺服器上，請先安裝 iManager，然後再安裝 Identity Manager 及其外掛程式。

Web 型態的管理服務

如果您已在伺服器上安裝 iManager 2.6，則僅需要執行 Identity Manager 的安裝程序，並安裝 iManager 的 Identity Manager 外掛程式。如果您在安裝使用者應用程式和工作流程系統服務，則還必須執行使用者應用程式安裝程序，並僅安裝 iManager 的使用者應用程式外掛程式。您需要針對使用者應用程式或附有提供安裝的使用者應用程式執行此動作 (它們是兩種不同的產品)。

使用者應用程式和安全記錄服務

如果您在執行大量提供，建議您將使用者應用程式安裝在其本身的伺服器上。您也可以視需要設定叢集。使用者應用程式中包括 MySQL 5.0.27，如果將其部署爲使用者應用程式安裝的一部分，或具有工作流程提供之使用者應用程式安裝的一部分，則無需設定其他資料庫服務。

不過，安全記錄服務不包括特定的資料庫，且安全記錄服務和使用者應用程式 / 工作流程提供服務都需要資料庫。您可以設定一個資料庫用於兩個應用程式，也可以針對每個服務設定獨立的資料庫。這取決於您執行的提供數量和記錄服務工作量。

附註：如果您要在個別的 (遠端) 伺服器上設定 Oracle 9i 或 10G，則需要安裝 Oracle，並設定「應用程式伺服器」的組態，以提供資料庫的遠端連接。

使用遠端載入器組態

如果您不想在已連接的系統伺服器上安裝 eDirectory 服務和 Metadirectory 引擎，則可以在 Identity Manager 安裝期間使用「*已連接系統*」選項。「遠端載入器」還會使用 SSL 技術，提供 Metadirectory 引擎與驅動程式之間的安全通訊路徑。在將系統連接至 Identity Manager 時，請記住這一點。

如需規劃 Identity Manager 系統的詳細資訊，請參閱第 2 章 「規劃」 (第 39 頁)。

1.7 取得 Identity Manager 及其服務的位置

若要下載 Identity Manager 及其服務：

1. 前往 Novell 下載網站 (http://download.novell.com)。
2. 在「*產品*」或「*技術*」功能表中，選取「*Novell Identity Manager*」，然後按一下「*搜尋*」。
3. 在「Novell Identity Manager 下載」頁面上，按一下您想要之檔案旁邊的「下載」按鈕。
4. 遵循畫面上的提示，將檔案下載到您電腦上的目錄中。
5. 重複執行步驟 2，直到您完全下載所需的檔案爲止。大多數安裝都需要多個 ISO 影像檔。

可以下載下列 Identity Manager 元件。

表格 1-4 *ISO 影像檔的運作方式*

Identity Manager 元件	平台	ISO
Identity Manager DVD 下列 Identity Manager 元件位於用於燒錄 DVD 的 ISO 影像檔上。這些元件也可以個別下載。 ◆ Identity Manager 和驅動程式 ◆ Designer for Identity Manager	Identity Manager: Linux、NetWare、Windows 和 UNIX* Designer： Linux 和 Windows	Identity_Manager_5_1_DVD.iso_1
Identity Manager 和驅動程式	NetWare 和 Windows	Identity_Manager_5_1_NW_Win.iso_1
Identity Manager 和驅動程式	Linux	Identity_Manager_5_1_Linux.iso_1
Identity Manager 和驅動程式	UNIX	Identity_Manager_5_1_Unix.iso_1
使用者應用程式 這是您購買之 Identity Manager 3 所隨附的使用者應用程式標準版本。	Linux 和 Windows	Identity_Manager_5_1_User_Application。_1 iso
Identity Manager 的使用者應用程式提供模組 這是使用者應用程式的「提供」版本，是 Identity Manager 的附加產品，需要單獨購買。	Linux 和 Windows	Identity_Manager_5_1_User_Application_ Provisioning.iso_1
Designer for Identity Manager	Windows	Identity_Manager_5_1_Designer_Win.iso_1
Designer for Identity Manager	Linux	Identity_Manager_5_1_Designer_Linux.iso_1

您購買的 Identity Manager 針對數種您可能擁有授權的常用客戶系統，而提供下列系統的整合模組：Novell eDirectory、Microsoft Active Directory、Microsoft Windows NT、LDAP v3 Directories、Novell GroupWise®、Microsoft Exchange 和 Lotus Notes。所有其他「Identity Manager 整合模組」必須單獨購買。

使用者應用程式元件隨附於兩個 ISO 影像檔上：使用者應用程式 ISO 影像檔爲標準版本，隨您的 Identity Manager 3 一起購入。Identity Manager 的使用者應用程式「提供模組」是一個整合了強大核准工作流程的附加產品。此「提供模組」位於不同的 ISO 影像檔上，要單獨購買。

您所購買的 Identity Manager 還包括 Designer for Identity Manager，它是一個強大而有彈性的管理工具，可大幅簡化組態設定和部署。

1.7.1 安裝 Identity Manager 3.5.1

- 若要在 Windows、Netware、UNIX 和 Linux 上安裝 Identity Manager 3.5.1，請參閱第 4 章 「安裝 Identity Manager」 (第 63 頁)
- 若要安裝使用者應用程式或附有 「提供」的使用者應程式，請參閱第 5 章 「安裝 「使用者應用程式」」 (第 93 頁)
- 若要安裝 Designer，請參閱 「Designer 2.1 for Identity Manager 3.5.1」指南內的 「*安裝*」。

附註：Linux & Unix (原本爲 NIS)、Mainframe 和 Midrange 驅動程式安裝程式位於 /platform/setup 目錄中。您必須從 Identity Manager 和使用者應用程式安裝程式分別執行這些安裝。

如需已知問題的清單，請參閱 Identity Manager 隨附的 Readme 檔案。

1.7.2 啓動 Identity Manager 3.5.1 產品

Identity Manager 產品需要啓用 (Designer 除外)。下列產品的試用期爲 90 天，之後您必須停止使用它們或者購買啓用。

- Identity Manager 3.5.1
- Identity Manager 的使用者應用程式提供模組
- 整合模組

重要：若要正確啓用使用者應用程式，您必須下載正確的 ISO 影像檔。例如，如果您購買 Identity Manager ，但是隨後下載了使用者應用程式提供模組而未單獨購買該 「提供模組」，則您的使用者應用程式實作會在 90 天之後停止運作。

如需啓用的其他資訊，請參閱第 6 章 「啓用 Novell Identity Manager 產品」 (第 171 頁)。

規劃 2

2.1 規劃 Identity Manager 實作的專案管理方面

本節概述實作 Identity Manager 的高層行政和專案管理方面 (如需技術方面的資訊，請參閱 第 2.3 節 「規劃 Identity Manager 實作的技術方面」 (第 52 頁))。

此規劃材料針對 Identity Manager 專案從開始到完整的產品部署爲止通常所執行之活動類型，提出了一份綜覽。實作身分管理策略需要您探查需求、瞭解環境中的共同工作人員、設計解決方案、取得共同工作人員的認同，以及測試和推行解決方案。本節旨在讓您充份瞭解程序，以便充分發揮 Identity Manager 的優勢。

我們強烈建議您任用 Identity Manager 專家，以在解決方案部署的每個階段中協助您。如需合作關係選項的相關資訊，請參閱 Novell 解決方案夥伴網站 (http://www.novell.com/partners/)。「Novell 教育訓練」也會提供說明 Identity Manager 實作的課程。

我們也強烈建議您設定一個測試 / 開發環境，可在其中測試、分析和開發您的各種解決方案。在一切都如您所需地進行時，便可將最終產品部署到您的生產環境中。

本節內容並非十分詳盡，不會說明所有可能的組態，在執行時也不很嚴格。每個環境都不相同，需要在所使用的活動類型中有些彈性。

2.1.1 Novell Identity Manager 部署

部署 Identity Manager 時，建議將下列數個活動做爲最佳作法：

探查

您可能要以可以執行下列動作的探查程序開始 Identity Manager 實作：

- 識別管理身分資訊的主要目標
- 定義或釐清所說明的業務問題
- 決定說明未解決之問題所需的事件
- 決定執行其中一或多個事件所要採取的動作

- 開發高層級策略或「解決方案藍圖」和已同意的執行路徑

探查可協助您一般性地瞭解所有共同工作人員的問題和解決方案。它是需要共同工作人員具有目錄、Novell eDirectory、Novell Identity Manager 和 XML 整合基本知識之分析階段的極好初級資料。

- 它可以建立所有共同工作人員之間的基本瞭解
- 它可以從共同工作人員處擷取關鍵的業務和系統資訊
- 它可讓您開發解決方案藍圖

探查還會識別緊接著的下一個步驟，可能包括下列內容：

- 規劃各種活動來依據各種要求條件進行準備，並準備進入設計階段
- 定義共同工作人員的其他教育訓練

關鍵交付項目

- 與關鍵業務和技術共同工作人員的結構化會晤
- 業務和技術問題的高層級摘要報告
- 下一步驟的建議
- 概述探查結果的執行簡報

要求和設計分析

此分析階段會擷取專案之技術和業務方面的詳細資訊，並產生資料模型和高層級 Identity Manager 結構設計。此活動是實作解決方案的關鍵性第一步。

設計的焦點應該是身分管理；不過，許多常與資源管理目錄相關聯的元素 (例如檔案和列印) 也可以處理。下列是您可能要評估的項目範例：

- 正在使用哪個版本的系統軟體？
- 目錄設計適當嗎？
- 目錄用來代管 Identity Vault 和 Identity Manager，還是用來延伸其他服務？
- 所有系統中的資料品質是否合適？ (如果資料的品質不堪使用，可能就無法如願進行業務規則的實作。)
- 您的系統需要資料管理嗎？

要求分析之後，您可以建立實作的範圍和專案規劃，並可以判定是否需要採取任何必要活動。爲了避免嚴重的錯誤，請儘量蒐集完整的資訊並記錄要求。

要求評估期間可能完成下列任務：

- 「定義業務要求」(第 40 頁)
- 「分析業務程序」(第 41 頁)
- 「設計企業資料模型」(第 42 頁)

定義業務要求

蒐集組織的業務程序和定義這些業務程序的業務要求。

例如，終止員工的業務要求可能是必須在終止員工的同一天移除員工的網路和電子郵件帳戶存取。

下列任務可以指引您定義業務要求：

- 建立程序流程、程序觸發和資料對應關係。

  例如，如果特定程序發生某些問題，則該任務將因此造成何種問題？會觸發何種其他程序？
- 對應應用程式之間的資料流程。
- 識別從一種格式變成另一種格式所要發生的資料轉換，例如從 2/25/2007 轉換爲 25 Feb 2007。
- 記錄存在的資料相依性。

  如果特定值變更，則瞭解該值是否存在相依性便十分重要。如果特定程序變更，則瞭解該程序是否存在依存性十分重要。

  例如，在人力資源部門系統中選取「暫時」員工狀態值，可能表示 IT 部門需要在 eDirectory 中建立在特定時間期間對網路的權限和存取受限的使用者物件。
- 列出優先程度。

  並非每一方的每個要求、希望或願望都可以立即實現。設計和部署提供系統的優先程度會協助您規劃藍圖。

  將部署分割成階段可能會很有好處，這樣就可以先實作一部分部署，以後再實作部署的其他部分。您也可以採取分階段部署的方式。這應該以組織內的人員群組爲基礎。
- 定義先決條件。

  實作特定部署階段所需的先決條件都應該記錄下來。這包括對您等待要與 Identity Manager 連接之已連接系統的存取。
- 識別授權資料來源。

  較早地瞭解管理員和管理者認爲他們所要擁有的系統資訊項目，可以協助您取得並始終保持各方的認同。

  例如，帳戶管理者可能要擁有授予員工特定檔案和目錄時所需的權限。可以藉由在帳戶系統中實作本地託管者指定來達成此目的。

分析業務程序

業務程序的分析通常從會晤最基本的個人 (如實際使用應用程式或系統的經理、管理員和員工) 開始。要說明的問題包括：

- 資料源自何處？
- 資料去向何處？
- 誰來負責資料？
- 哪些人員擁有資料所屬之業務功能的所有權？
- 要變更資料需要聯絡哪些人員？
- 正在變更的資料具有哪些隱含項目？
- 資料處理要執行哪些工作 (蒐集和 / 或編輯)？
- 會執行哪種類型的操作？
- 使用何種方法來確保資料品質和完整性？

- 系統位於何處 (在哪個伺服器上，哪個部門中)？
- 哪些程序不適合於自動處理？

例如，對「人力資源」部門中 PeopleSoft 系統管理員提出的問題可能包括

- 哪些資料儲存在 PeopleSoft 資料庫中？
- 哪些項目會出現在員工帳戶的各種面板中？
- 需要跨提供系統反映哪些動作 (例如新增、修改或刪除)？
- 其中哪些項目是必要的？ 哪些項目是選擇性的？
- 根據在 PeopleSoft 中執行的動作需要觸發哪些動作？
- 要忽略哪些操作 / 事件 / 動作？
- 如何轉換資料並將其對應至 Identity Manager？

會晤關鍵人員可以指向組織的其他區域，它們可提供整個程序的更清晰圖像。

設計企業資料模型

定義業務程序之後，您便可以開始設計反映目前業務程序的資料模型。

模型應該說明資料源自何處、會移至何處，以及其無法移至何處。還應說明重要事件如何影響資料流程。

您可能還要設計圖表，說明提出的業務流程和在該程序中實作自動提供的優點。

從回答下列問題

- 正在移動哪些類型的物件 (使用者、群組等)？
- 對哪些事件感興趣？
- 需要同步化哪些屬性？
- 需要針對正在管理的各種類型物件在整個業務期間儲存哪些資料？
- 同步化是單向還是雙向？
- 每個屬性的授權來源是哪個系統？

考量系統之間不同值的相互關係很重要。

例如，PeopleSoft 中的員工狀態欄位可能具有三個設定值：員工、約聘和實習生。不過，Active Directory 系統可能只有兩個值：永久和暫時。在此情況下，需要決定 PeopleSoft 中「約聘」狀態與 Active Directory 中「永久」和「暫時」值之間的關係。

此工作的焦點應該是瞭解每個目錄系統、各系統彼此之間的關係，以及需要跨系統同步化哪些物件和屬性。

關鍵交付項目

- 顯示 Identity Manager 內所有系統、授權資料來源、事件、資訊流程和資料格式標準、已連接系統與屬性之間對應關係的資料模型。
- 解決方案的適當 Identity Manager 結構
- 其他系統連線要求的詳細資料
- 資料驗證和記錄相符的策略
- 設計爲支援 Identity Manager 基礎結構的目錄

相依性

- 熟悉所有外部系統的員工 (例如 HR 資料庫管理員、網路和訊息傳送系統管理員)
- 系統綱要和範例資料的可用性
- 分析和設計階段的資料模型
- 基本資訊 (如組織圖、廣域網路 (Wide Area Network，WAN) 和伺服器基礎結構) 的可用性

概念檢驗

此活動的結果是產生實驗室環境中的範例實作，該實作會反映公司的業務規則和資料流程。它以在要求分析和設計期間開發之資料模型的設計爲基礎，且是生產試驗之前的最後一步。

附註：通常，此步驟有利於取得管理支援並爲最終的實作籌集資金。

關鍵交付項目

- 所有系統連線都可正常運作之正在運行的 Identity Manager 概念檢驗

相依性

- 硬體平台和設備
- 必要軟體
- 識別必要連線的分析和設計階段
- 用於測試目的之其他系統的可用性和存取
- 分析和設計階段的資料模型

資料驗證和準備

生產系統中資料的品質和一致性可能各不相同，因此，同步化系統時可能會出現不一致。此階段可在資源實作小組與「擁有」或管理系統中要整合之資料的業務單位或群組之間，呈現二者之間明顯的分歧點。有時，相關聯的風險和成本因素可能不屬於提供專案。

關鍵交付項目

- 適合於載入 Identity Vault 的生產資料集 (在分析和設計活動中識別)。這包括可能的載入方法 (大量載入或透過連接器載入)。還會識別已驗證或已格式化資料的要求。
- 還會根據所使用的設備和 Identity Manager 部署的整個分散式結構來識別和驗證效能因素。

相依性

- 分析和設計階段的資料模型 (提出的記錄相符和資料格式策略)
- 存取生產資料集

生產試驗

此活動的目的是要開始移轉到生產環境中。在此階段期間，可能會發生其他自訂。在此有限的啓動階段中，可以確認先前活動所想要的結果，並取得生產展示的合約。

附註：此階段可能會提供解決方案的接受準則，以及整個生產過程中必要的里程碑。

關鍵交付項目

- 提供資料模式和想要處理結果之即時概念檢驗和驗證的試驗解決方案。

相依性

- 所有先前的活動 (分析和設計、Identity Manager 技術平台)。

生產展示規劃

這是規劃生產部署的階段。該規劃應該：

- 確認伺服器平台、軟體修正和 Service Pack
- 確認一般環境
- 確認以混合共存的方式引入 Identity Vault
- 確認分割和複製策略
- 確認 Identity Manager 實作
- 規劃舊程序切換
- 規劃復原偶發事件策略

關鍵交付項目

- 生產展示規劃
- 舊程序切換規劃
- 復原偶發事件規劃

相依性

- 所有先前的活動

生產部署

這是將試驗解決方案延伸來影響生產環境中所有即時資料的階段。它通常遵循生產試驗符合所有技術和業務要求的合約。

關鍵交付項目

- 準備開始轉換的生產解決方案

相依性

- 所有先前的活動

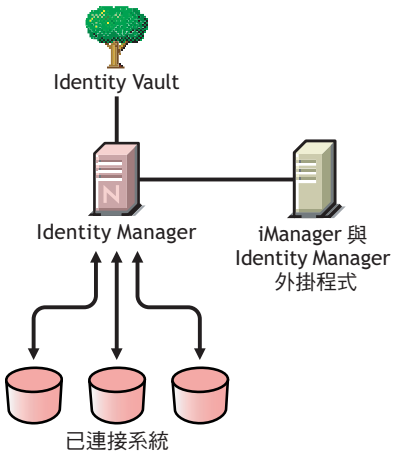
2.2 針對一般安裝案例進行規劃

下列案例是可能使用 Identity Manager 之環境的範例。針對每個案例都提供了一些指示，以協助您進行實作。

- 第 2.2.1 節「Identity Manager 的新安裝」(第 45 頁)
- 第 2.2.2 節「在相同環境中使用 Identity Manager 和 DirXML 1.1a」(第 47 頁)
- 第 2.2.3 節「從 Starter Pack 升級至 Identity Manager」(第 49 頁)
- 第 2.2.4 節「將「密碼同步化 1.0」升級至「Identity Manager 密碼同步化」」(第 50 頁)

2.2.1 Identity Manager 的新安裝

圖 2-1 新安裝



Identity Manager 是一套可讓您的 Identity Vault 自動完成在應用程式、資料庫和目錄之間同步化、轉換和散佈資訊的資料共享解決方案。

Identity Manager 解決方案包括下列元件：

- 「Identity Manager 與 Identity Vault」(第 45 頁)
- 「iManager Server 與 Identity Manager 外掛程式」(第 45 頁)
- 「已連接系統」(第 46 頁)
- 「一般 Identity Manager 任務」(第 46 頁)

Identity Manager 與 Identity Vault

Identity Vault 包含要與其他已連接系統共享或同步化的使用者或物件資料。建議您將 Identity Manager 安裝在其本身的 eDirectory™ 例項中，並將其做爲您的 Identity Vault。

iManager Server 與 Identity Manager 外掛程式

您可以使用 Novell® iManager 和 Identity Manager 外掛程式，管理您的 Identity Manager 解決方案。

已連接系統

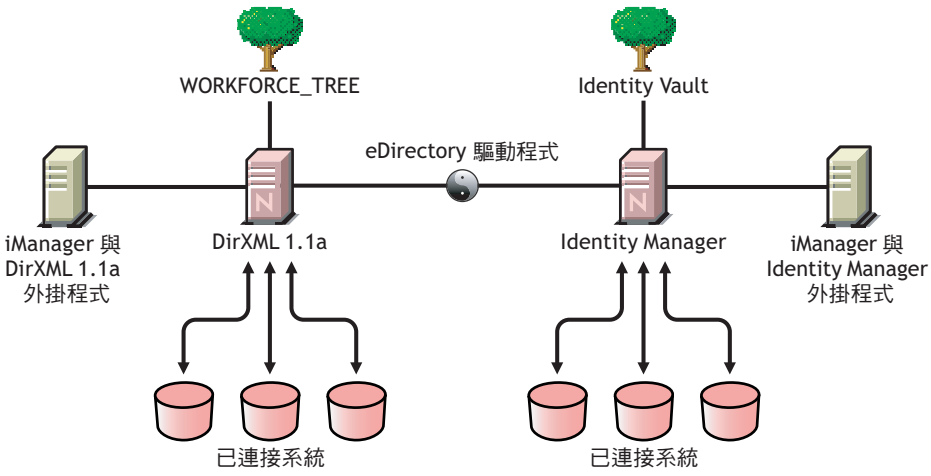
已連接系統可能包括要與 Identity Vault 共享或同步化資料的其他應用程式、目錄和資料庫。若要建立從 Identity Vault 到已連接系統的連線，請針對已連接系統安裝適當的驅動程式。如需特定指示，請參閱 (http://www.novell.com/documentation/idm35drivers/index.html) 驅動程式實作指南。

一般 Identity Manager 任務

- **安裝系統元件：**因爲 Identity Manager 解決方案可能會散佈在數個電腦、伺服器或平台之間，所以您應該在每個系統上執行安裝程式並安裝適當的元件。如需相關資訊，請參閱第 1.4 節 「Identity Manager 安裝程式和服務」(第 18 頁)。
- **設定已連接系統：**第 1.4 節「Identity Manager 安裝程式和服務」(第 18 頁) 如需特定指示，請參閱 (http://www.novell.com/documentation/idm35drivers/index.html) 驅動程式實作指南。
- **啓用解決方案：**Identity Manager 產品 (專業版、伺服器版本、「整合模組」和使用者應用程式) 需要在安裝後的 90 天內啓用。請參閱第 6 章 「啓用 Novell Identity Manager 產品」(第 171 頁)。
- **定義業務規則：**業務規則可讓您針對特定環境，自訂 Identity Vault 中資訊的流入和流出。規則還會建立新的物件、更新屬性值、進行網要轉換、定義相符準則、維護 Identity Manager 關聯和執行其他作業。「*iManager for Identity Manager 3.5.1 中的規則*」中有詳細的規則指南。
- **設定密碼管理的組態：**使用 「密碼規則」時，您可以藉由設定使用者該如何建立其密碼的規則，來增強安全性。您也可以提供自助選項，讓使用者在忘記密碼和重設密碼時能夠使用，進而降低 Help Desk 的成本。如需密碼管理的進一步資訊，請參閱 「使用密碼規則管理密碼 (http://www.novell.com/documentation/password_management31/index.html?page=/documentation/password_management31/pwm_administration/data/ampxjj0.html)」。
- **設定授權的組態：**授權定義可讓您將已連接系統上的權限授予 Identity Vault 中已定義的一組使用者。使用 「授權」規則，您可以對業務規則進行有效管理，並減少設定 Identity Manager 驅動程式之組態的必要。如需相關資訊，請參閱 《*Novell Identity Manager 3.5.1 管理指南*》內的 「建立並使用授權」。
- **使用 Novell Audit 記錄事件：**已將 Identity Manager 配備爲使用 Novell Audit 進行稽核和報告。Novell Audit 是一組技術，可提供監看、記錄、報告和通知功能。透過與 Novell Audit 整合，Identity Manager 可針對驅動程式和引擎活動的目前狀態和歷程狀態，提供詳細的資訊。此資訊由一組預先設定組態的報告、標準通知服務和使用者定義的記錄所提供。請參閱 《*Identity Manager 3.5.1 記錄和報告*》中的 「 使用狀態記錄 」。
- **工作流程核准和使用者應用程式：**Novell Identity Manager 使用者應用程式是一種強大的 Web 應用程式 (以及支援工具)，它的設計能夠在複雜的身分服務架構上提供豐富、直觀、可有效設定組態的 Web UI 體驗。Identity Manager 使用者應用程式與 「Identity Manager 提供模組」和 Novell Audit 一起使用時，可提供完整的端對端提供解決方案，該解決方案安全、可調整且易於管理。請參閱 《使用者應用程式文件 (http://www.novell.com/documentation/idm35)》。

2.2.2 在相同環境中使用 Identity Manager 和 DirXML 1.1a

圖 2-2 在與 DirXML 1.1a 相同的網路樹中安裝 Identity Manager



如果您在相同的環境中執行 Identity Manager 和 DirXML® 1.1a，請注意下列考量：

- 「建立 Identity Vault」(第 47 頁)
- 「管理工具」(第 47 頁)
- 「反向相容性」(第 47 頁)
- 「密碼管理」(第 48 頁)

建立 Identity Vault

建議您將 Identity Manager 安裝在單獨的 eDirectory 例項中，並將其做爲 Identity Vault。

管理工具

- ConsoleOne® 受 DirXML 1.1a 支援，但不受 Identity Manager 支援。
- 需要兩個 iManager 伺服器，一個用於 DirXML 1.1a 外掛程式，另一個用於 Identity Manager 外掛程式。這是因爲已增強外掛程式，且 Identity Manager 使用「DirXML 程序檔」。
- DirXML 1.1a 的 iManager 外掛程式無法讀取「DirXML 程序檔」，該程序檔用於大部份 Identity Manager 驅動程式的已定義驅動程式組態中。
- Designer 是一個可讓您設計、測試、更新和記錄 Identity Manager 驅動程式的工具。

反向相容性

- 您可以在 Identity Manager 伺服器上執行 DirXML 1.1a 驅動程式 Shim 和組態，且可以在驅動程式集的「Identity Manager 概觀」中檢視 iManager 中的驅動程式。但是 Identity Manager 外掛程式不會讓您檢視或編輯驅動程式組態，直到您將它們轉換爲 Identity Manager 格式爲止。

  在 Identity Manager 外掛程式中，如果您按一下 1.1a 格式的驅動程式，則會提示您完成轉換。這是使用精靈完成的簡單程序，不會變更驅動程式組態的功能。做爲程序的一部份，會儲存 DirXML 1.1a 版的備份副本。

- 當使用 Identity Manager 引擎執行 DirXML 1.1a 驅動程式時，則驅動程式的啓用仍然有效。不過，如果您將驅動程式 Shim 升級到 Identity Manager 版本，則需要取得新的啓用認證。如需詳細資訊，請參閱附錄 6 「啓用 Novell Identity Manager 產品」(第 171 頁)。
- 在大部分情況下，Identity Manager 驅動程式 Shim 可以使用 DirXML 1.1a 的組態執行。如需升級資訊，請參閱個別的驅動程式實作指南 (http://www.novell.com/documentation/idm35drivers/index.html)。

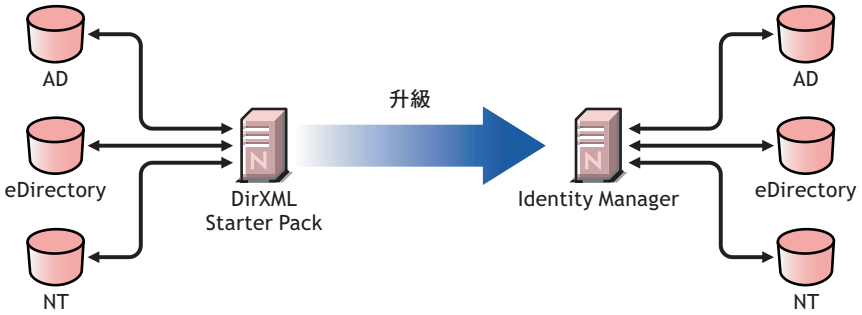
  明顯的例外是 「密碼同步化 1.0」，除非您在升級驅動程式 Shim 之後，新增部分其他驅動程式規則，否則它不會針對 Windows AD 和 Windows NT 正確地執行。如需指示，請參閱 Active Directory 和 NT Domain 之 「Identity Manager 驅動程式」的驅動程式實作指南 (http://www.novell.com/documentation/idm35drivers/index.html) 中有關 「密碼同步化」一節。
- 不支援使用 DirXML 1.1a 引擎執行 Identity Manager 驅動程式 Shim 和驅動程式組態。
- 不支援使用 DirXML 1.1a 驅動程式 Shim 執行 Identity Manager 驅動程式組態。
- 如果您在多個伺服器上執行相同的 Identity Manager 驅動程式組態，請確定伺服器執行的是相同版本的 Identity Manager 和相同版本的 eDirectory。

密碼管理

- 您可以建立會提供功能的 「密碼」規則，例如 「進階密碼規則」可要求安全性較高的密碼，以及使用者的 「忘記密碼自助服務」和 「重設密碼自助服務」。請參閱 《密碼管理 3.1 指南 (http://www.novell.com/documentation/password_management31/index.html)》中的 「管理密碼同步化」。
- 如果您開始與 NetWare® 6.5 的初始版本搭配使用 「通用密碼」，則在使用新密碼規則功能前，必須先執行某些升級步驟。請參閱 《密碼管理 3.1 指南 (http://www.novell.com/documentation/password_management31/index.html)》中的 「(僅 NetWare 6.5) 部署通用密碼」。如果您開始將 「通用密碼」與 NetWare 6.5 SP2 搭配使用，則無需執行該程序。
- 「Identity Manager 密碼同步化」會提供雙向密碼同步化，且所支援的平台比 「密碼同步化 1.0」更多。
- 如果您已將 「密碼同步化 1.0」與 Windows AD 或 Windows NT 搭配使用，請確定在安裝新的驅動程式 Shim 之前先檢視升級指示。請參閱第 2.2.4 節 「將 「密碼同步化 1.0」升級至 「Identity Manager 密碼同步化」」(第 50 頁)。
- 我們提供了驅動程式規則 「重疊」來協助您將雙向 「密碼同步化」功能新增至現有的驅動程式。請參閱 《*Novell Identity Manager 3.5.1 管理指南*》中的 「升級現有驅動程式組態以支援密碼同步化」。

2.2.3 從 Starter Pack 升級至 Identity Manager

圖 2-3 從 Starter Pack 升級至 Identity Manager



其他 Novell 產品中包含的 Identity Manager Starter Pack 解決方案可讓 NT Domain、Active Directory 和 eDirectory 中的資訊進行授權同步化。此外，數個其他系統的試用版驅動程式也隨附於此，這些包括 PeopleSoft、GroupWise® 和 Lotus Notes，可讓您瀏覽其他系統的資料同步化。

此解決方案還提供同步化使用者密碼的功能。使用 PasswordSync，使用者只需記住單一密碼，便可以登入以上任何一個系統。管理員可以在自己偏好的系統中管理密碼。無論何時其中一個環境中的密碼變更，所有環境中的密碼都會更新。

Identity Manager Starter Pack 隨附的 NetWare 6.5 和 Nterprise™ Linux Services 1.0 皆以 DirXML 1.1a 技術爲基礎。從 Starter Pack 升級至最新版的 Identity Manager 時，請記住下列考量：

- 「反向相容性」(第 49 頁)
- 「密碼管理」(第 50 頁)
- 「啓用」(第 50 頁)

反向相容性

- 您可以在 Identity Manager 伺服器上執行 DirXML 1.1a 驅動程式 Shim 和組態，且可以在驅動程式集的「Identity Manager 概觀」中檢視 iManager 中的驅動程式。但是 Identity Manager 外掛程式不會讓您檢視或編輯驅動程式組態，直到您將它們轉換爲 Identity Manager 格式爲止。

  在 Identity Manager 外掛程式中，如果您按一下 1.1a 格式的驅動程式，則會提示您完成轉換。這是使用精靈完成的簡單程序，不會變更驅動程式組態的功能。做爲程序的一部份，會儲存 DirXML 1.1a 版的備份副本。
- 當使用 Identity Manager 引擎執行 DirXML 1.1a 驅動程式時，則驅動程式的啓用仍然有效。不過，如果您將驅動程式 Shim 升級至 Identity Manager 版本，則需要新的啓用。
- 在大部分情況下，Identity Manager 驅動程式 Shim 可以使用 DirXML 1.1a 的組態執行。如需升級資訊，請參閱個別的驅動程式實作指南 (http://www.novell.com/documentation/idm35drivers/index.html)。

  明顯的例外是「密碼同步化 1.0」，除非您在升級驅動程式 shim 之後，新增部分其他驅動程式規則，否則它不會針對 Windows AD 和 Windows NT 正確地執行。如需指示，請參閱 Active Directory 和 NT Domain 之「Identity Manager 驅動程式」的驅動程式實作指南 (http://www.novell.com/documentation/idm35drivers/index.html) 中有關「密碼同步化」一節。

- 不支援使用 DirXML 1.1a 引擎執行 Identity Manager 驅動程式 Shim 和驅動程式組態。
- 不支援使用 DirXML 1.1a 驅動程式 Shim 執行 Identity Manager 驅動程式組態。
- 如果您在多個伺服器上執行相同的 Identity Manager 驅動程式組態，請確定伺服器執行的是相同版本的 Identity Manager 和相同版本的 eDirectory。

密碼管理

- 除非您在升級驅動程式 Shim 之後，新增部分其他驅動程式規則，否則 Starter Pack (DirXML 1.1a) 隨附的「密碼同步化 1.0」不會針對 AD 和 NT 正確地執行。如需指示，請參閱 Active Directory 和 NT Domain 之「Identity Manager 驅動程式」的驅動程式實作指南 (http://www.novell.com/documentation/idm35drivers/index.html) 中有關「密碼同步化」一節。
- 如需關於此升級程序的特定指示，請參閱第 2.2.4 節「將「密碼同步化 1.0」升級至「Identity Manager 密碼同步化」」(第 50 頁)。

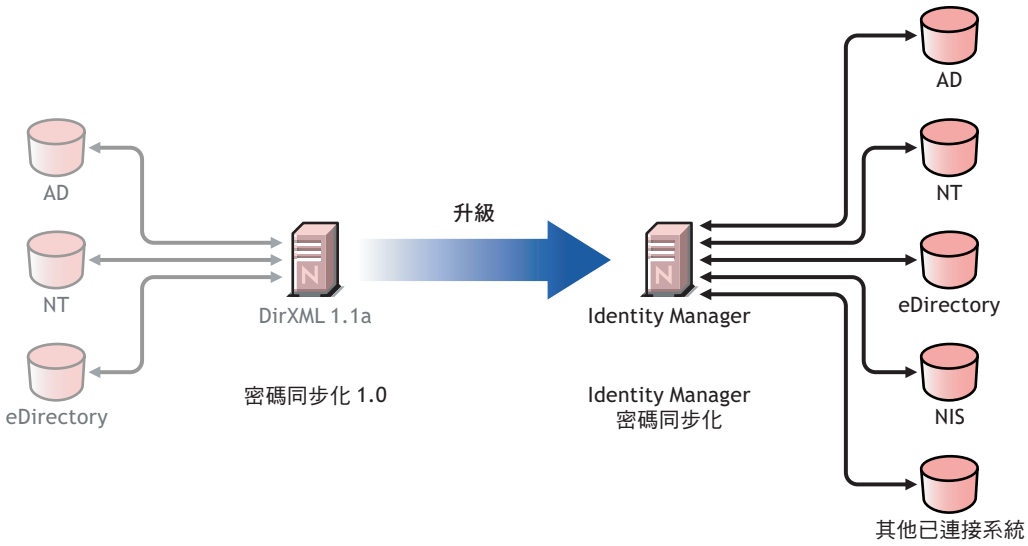
啓用

- 必須在 90 天之內啓用所有的 Identity Manager 產品。購買其他 Novell 軟體時，DirXML Starter Pack 包括 DirXML 1.1a 引擎以及 NT、AD 和 eDirectory 驅動程式的啓用。從 Identity Manager Starter Pack 升級時，您可能需要重新套用這些驅動程式的啓動認證。

  有關 dirxml 的詳細資訊，請參閱附錄 6「啓用 Novell Identity Manager 產品」(第 171 頁)。

2.2.4 將「密碼同步化 1.0」升級至「Identity Manager 密碼同步化」

圖 2-4 將「密碼同步化 1.0」升級至「Identity Manager 密碼同步化」



「Identity Manager 密碼同步化」提供許多功能，包括雙向密碼同步化、其他平台，以及在密碼同步化失敗時進行電子郵件通知。

如果您將 「密碼同步化 1.0」用於 Active Directory 或 NT Domain，則在安裝新的驅動程式 Shim 之前，檢視升級指示會很重要。

如果您將 Identity Manager 2.x 與 「密碼同步化 2.0」搭配執行，則無需執行這些步驟。

如需 「Identity Manager 密碼同步化」的一般資訊，請參閱 《*Novell Identity Manager 3.5.1 管理指南*》內的 「已連接系統中的密碼同步化」。該節包含一些概念資訊，包括新舊功能的比較、先決條件、每個已連接系統支援的功能清單、新增支援至現有的驅動程式，以及顯示如何使用新功能的數個案例。

本節內容：

使用 Active Directory 或 Windows NT 的密碼同步化

新的 「密碼同步化」功能由驅動程式規則來執行，而不是由個別的代辦執行。這表示如果您安裝新的驅動程式 Shim，但是未同時升級驅動程式，則 「密碼同步化 1.0」會繼續只針對現有的使用者執行。新的、已移動或已重新命名的使用者不會參與 「密碼同步化」，直至您完成驅動程式組態升級爲止。

使用下列一般步驟進行升級：

1. 升級環境，使其支援 「通用密碼」，包括升級 Novell Client™ (如果您正在使用它)。
2. 安裝 Identity Manager 3.5.1 驅動程式 Shim，以取代 Active Directory 或 Windows NT 的 DirXML 1.1a 驅動程式 Shim。
3. 隨即建立與 「密碼同步化 1.0」的反向相容性，方法是將規則新增至驅動程式組態。

   此步驟可讓 「密碼同步化 1.0」繼續正確運行，直到您切換到 「Identity Manager 密碼同步化」爲止。
4. 使用驅動程式規則來支援新的 「Identity Manager 密碼同步化」。
5. 安裝新的 「密碼同步化」過濾器並設定其組態。
6. 必要時，設定 SSL。
7. 必要時，使用密碼規則來啓用 「通用密碼」。
8. 設定要使用的 「Identity Manager 密碼同步化」案例。

   請參閱 《*Novell Identity Manager 3.5.1 管理指南*》中的 「實作密碼同步化」。
9. 移除 「密碼同步化 1.0」。

如需詳細資訊，請參閱適用 Active Directory 和 NT 網域之 Identity Manager 驅動程式的驅動程式實作指南 (http://www.novell.com/documentation/idm35drivers/index.html)。

升級 eDirectory 的密碼同步化

升級 eDirectory 相當簡單，假設您的驅動程式 Shim 和組態具有最新的修補程式，則驅動程式 Shim 會與現有的 DirXML 1.1a 驅動程式組態搭配運作，不需任何變更。如需指示，請參閱 《*Identity Manager 3.5.1 Driver for eDirctory：實作指南*》。

升級其他已連接系統驅動程式

「Identity Manager 密碼同步化」支援的已連接系統比「密碼同步化 1.0」更多。

如需其他系統支援的功能清單，請參閱《*Novell Identity Manager 3.5.1 管理指南*》內的「密碼同步化的已連接系統支援」。

已提供驅動程式規則「重疊」，可協助您將雙向「密碼同步化」功能新增至先前不支援之已連接系統的現有驅動程式。請參閱《*Novell Identity Manager 3.5.1 管理指南*》中的「升級現有驅動程式組態以支援密碼同步化」。

處理機密資訊

「通用密碼」在 eDirectory 內由四層加密保護，因此在該環境中非常安全。如果您選擇使用雙向密碼同步化，且同步化「通用密碼」與「配送密碼」，請記住您會擷取 eDirectory 密碼，並將其傳送至其他已連接系統。您需要確保密碼傳輸以及其同步化所到之已連接系統的安全。

除了密碼之外，您還可以使用 Novell SecretStore® 和 Novell SecureLogin 來對認證進行同步化。這可讓您在需要肯定認證功能的環境中提供 SecureLogin 通關密語的問題與回答。請參閱《*Novell Identity Manager 3.5.1 管理指南*》內的「安全性：最佳作法」。

2.3 規劃 Identity Manager 實作的技術方面

2.3.1 使用 Designer

Identity Manager 包含稱爲 Designer 的工具。Designer 可讓您設計、測試並記錄 Identity Manager 驅動程式。Designer 可讓您查看密碼同步以及資料流程。如需相關資訊，請參閱《*Designer 2.0 for Identity Manager 3.5.1 管理指南*》。

2.3.2 複製 Identity Manager 在伺服器上需要的物件

如果 Identity Manager 環境呼叫多個伺服器，以執行多個 Identity Manager 驅動程式，則做爲規劃的一部分，您務必將特定 eDirectory 物件複製到要執行這些 Identity Manager 驅動程式的伺服器上。

只要過濾後的複製本中包含驅動程式需要讀取或同步化的所有物件和屬性，便可以使用過濾後的複製本。

請記住您必須針對「Identity Manager 驅動程式」物件提供其所要同步化之任何物件的足夠 eDirectory 權限，可以藉由明確授予權限，或者讓「驅動程式」物件安全性等值於具有所需權限的物件來提供。

執行 Identity Manager 驅動程式的 (或者如果使用「遠端載入器」，該驅動程式參考的) eDirectory 伺服器必須保留下列物件的主複製本或讀 / 寫複製本：

- 該伺服器的「驅動程式集」物件。

每個執行 Identity Manager 的伺服器都應該具有一個「驅動程式集」物件。除非您有特定需要，否則請勿將多個伺服器與相同的「驅動程式集」物件相關聯。

附註：建立「驅動程式集」物件時，預設設定是建立個別的分割區。Novell 建議在「驅動程式集」物件上建立個別的分割區。若要讓 Identity Manager 運行，伺服器必須保留「驅動程式集」物件的完整複製本。如果伺服器具有「驅動程式集」物件安裝位置的完整複製本，則不需要分割區。

- 該伺服器的「伺服器」物件。

  「伺服器」物件是必要的，因爲它可讓驅動程式產生物件的金鑰配對。它對於遠端載入器認證資訊也很重要。

- 您想要與此驅動程式例項同步化的物件。

  除非物件的複製本與驅動程式在同一個伺服器上，否則驅動程式無法同步化那些物件。實際上，除非您建立規則指定其他方式 (「範圍過濾」的規則)，否則 Identity Manager 驅動程式會同步化伺服器上複製之*所有*容器中的物件。

  如果您想要驅動程式同步化所有使用者物件，一個最簡單的方法是在保留所有使用者之主複製本或讀 / 寫複製本的伺服器上，使用驅動程式的例項。

  不過，許多環境並沒有包含所有使用者複製本的單一伺服器，而是全部使用者會分散在多個伺服器上。在這種情況下，您有兩種選擇：

  - **將使用者聚集至單一伺服器上。**您可以將複製本新增至現有的伺服器上，來建立保留所有使用者的單一伺服器。如果需要，可以使用過濾後的複製本來減少 eDirectory 資料庫的大小，只要過濾後複製本中包含必要的使用者物件和屬性。
  - **使用範圍過濾，在多個伺服器上使用多個驅動程式例項。**如果您不想將使用者聚集至單一伺服器，則需要判定保留所有使用者的伺服器組，並在其中每個伺服器上設定一個 Identity Manager 驅動程式例項。

    若要防止驅動程式的各個例項嘗試同步化相同的使用者，您需要使用「範圍過濾」，以定義每個驅動程式例項應該同步化的使用者。範圍過濾是指，將規則新增至每個驅動程式，以將驅動程式的管理範圍限制在特定的容器。請參閱「使用範圍過濾來管理不同伺服器上的使用者」(第 54 頁)。
  - **在多個伺服器上使用多個驅動程式例項，不使用範圍過濾。**如果您想讓驅動程式的多個例項在不同的伺服器上執行，但不使用過濾後的複製本，則需要在不同驅動程式例項上定義規則，讓驅動程式可以在同一 Identity Vault 中處理不同的物件組。

- 您想要驅動程式在建立使用者時使用的「範本」物件 (如果您選擇使用範本)。

  Identity Manager 驅動程式不需要您指定 eDirectory「範本」物件來建立使用者。但是，如果您指定驅動程式在 eDirectory 中建立使用者時應該使用範本，則必須在執行驅動程式的伺服器上複製「範本」物件。

- 您想要 Identity Manager 驅動程式用於管理使用者的任何容器。

  例如，如果您已建立名爲「未啓用使用者」的容器來保留已停用的使用者帳戶，則必須在執行驅程式的伺服器上擁有該容器的主複製本或讀 / 寫複製本 (最好是主要複製本)。

- 驅動程式需要參考的任何其他物件 (例如，Avaya*PBX 驅動程式的工作順序物件)。

  如果驅動程式只是讀取，而不變更其他物件，則那些物件在伺服器上的複製本可以是唯讀複製本。

2.3.3 使用範圍過濾來管理不同伺服器上的使用者

範圍過濾是指，將規則新增至每個驅動程式規則，以將驅動程式的動作範圍限制在特定的容器。下面是您需要使用範圍過濾的兩種情況：

- 您想要驅動程式僅同步化特定容器中的使用者。

  Identity Manager 驅動程式預設會對所執行之伺服器上複製之所有容器中的物件，進行同步化。若要縮小該範圍，則您必須建立範圍過濾規則。

- 您想要 Identity Manager 驅動程式同步化所有使用者，但不想將所有使用者複製到相同的伺服器上。

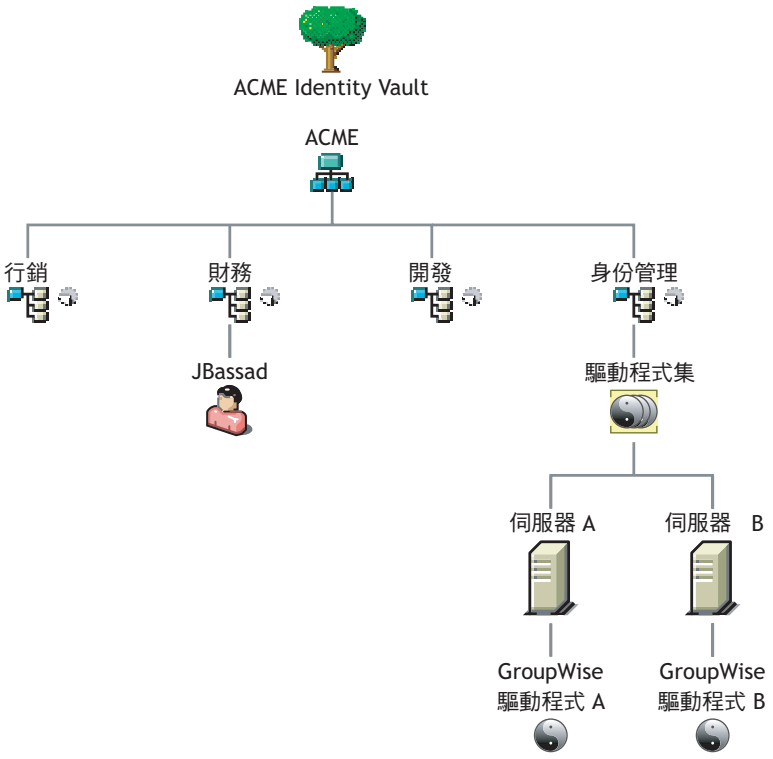
  若要同步化所有使用者，但不將他們複製到單一伺服器上，您需要判斷何者爲保留所有使用者的伺服器組，然後在其中每個伺服器上建立 Identity Manager 驅動程式例項。若要防止驅動程式的兩個例項嘗試同步化相同的使用者，您需要使用「範圍過濾」，以定義每個驅動程式例項應該同步化的使用者。

  附註：即使您的伺服器複製本目前沒有重疊，您也應該使用範圍過濾。以後，可以將複製本新增至伺服器，並可以無意地建立重疊。如果您將範圍過濾放置在適當位置，則 Identity Manager 驅動程式不會嘗試同步化相同的使用者，即使以後會將複製本新增至伺服器。

以下範例說明如何使用範圍過濾：

以下圖例顯示的 Identity Vault 具有三個存有使用者的容器：行銷部門、財務部門和開發部門。此外還顯示存有驅程式集的 Identity Manager 容器。其中每個容器中都是一個個別分割區。

圖 2-5 範圍過濾的網路樹範例



在此範例中，Identity Manager 管理員擁有兩個 Identity Vault 伺服器，「伺服器 A」和「伺服器 B」，如圖 2-6 (第 55 頁) 顯示。這兩個伺服器都不包含所有使用者的副本。每個伺服器包含三個分割區中的兩個，因此伺服器所保留內容的範圍重疊。

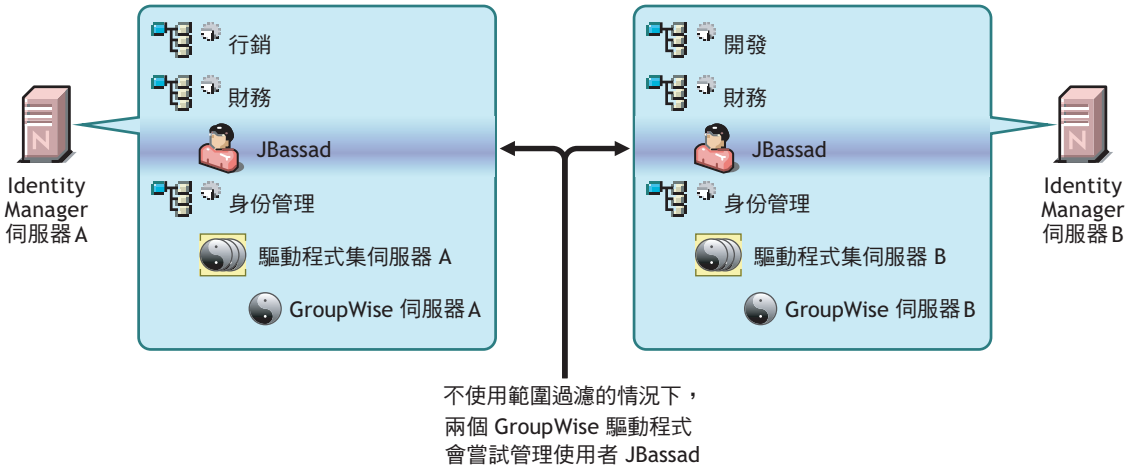
管理員想要網路樹中所有使用者由 groupwise® 驅動程式同步化，但不想將使用者複製本聚集至單一伺服器上。他選擇使用兩個 GroupWise 驅動程式例項，每個伺服器上各一個。他會安裝 Identity Manager，並在每個 Identity Manager 伺服器上設定 GroupWise 驅動程式。

「伺服器 A」會保存「行銷部門」和「財務部門」容器的複製本。該伺服器上還有 Identity Management 容器的複製本，該容器會保留「伺服器 A」的「驅動程式集」和「伺服器 A」的「GroupWise 驅動程式」物件。

「伺服器 B」會保留「開發部門」和「財務部門」容器的複製本，Identity Management 容器保留「伺服器 B」的「驅動程式集」和「伺服器 B」的「GroupWise 驅動程式」物件。

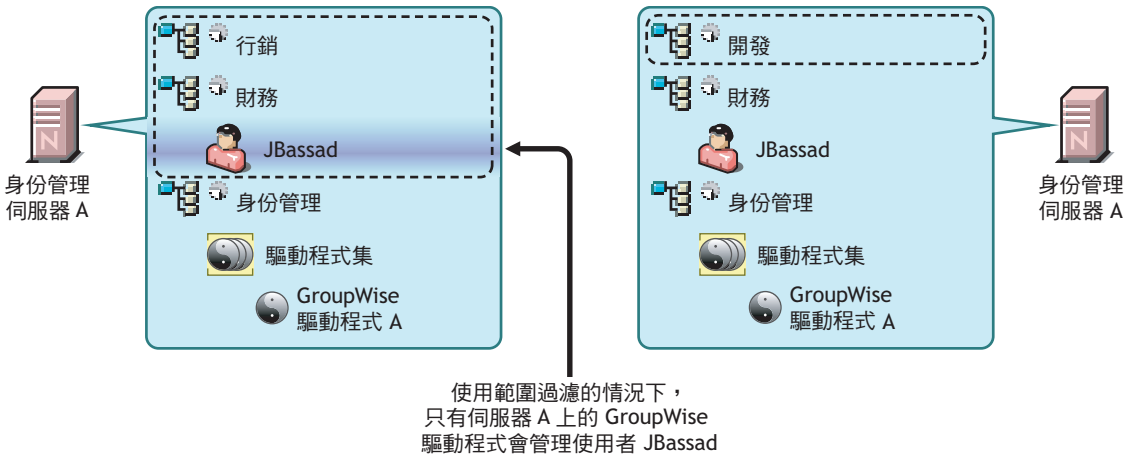
因爲「伺服器 A」和「伺服器 B」都會保存「財務部門」容器的複製本，所以這兩個伺服器都會保存「財務部門」容器中的使用者 JBassad。不使用範圍過濾的情況下，「GroupWise 驅動程式 A」與「GroupWise 驅動程式 B」都會同步化 JBassad。

圖 2-6 *具有重疊複製本，沒有範圍過濾的兩個伺服器*



下一個圖例顯示範圍過濾會防止驅動程式的兩個例項管理相同的使用者，因爲它會定義同步化每個容器的驅動程式。

圖 2-7 範圍過濾定義同步化每個容器的驅動程式



Identity Manager 3.5.1 具有預先定義的規則。有兩個規則可協助進行範圍過濾。「事件轉換 - 範圍過濾 - 包括子網路樹」和「事件轉換 - 範圍過濾 - 排除子網路樹」，「*瞭解 Identity Manager 的規則 3.5.1*」中有相關說明。

在此範例中，您會針對「伺服器 A」和「伺服器 B」使用「包括子網路樹」預先定義規則。您會分別定義每個驅動程式的範圍，以便它們僅同步化特定容器中的使用者。「伺服器 A」會同步化「行銷部門」和「財務部門」。「伺服器 B」會同步化「開發部門」。

升級

3

Identity Manager 具有多個不同部分。若要升級 Identity Manager，您需要確定已經考量產品的所有層面，才能成功升級。

部份升級案例在第 2.2 節「針對一般安裝案例進行規劃」(第 45 頁) 中說明。

3.1 升級路徑

表格包含不同版本 Identity Manager 支援的升級案例。每個案例都列示爲受支援或不受支援。

表格 3-1 *升級路徑案例*

已安裝版本	目前版本	支援升級？
DirXML® 1.1a	Identity Manager 3.5.1	是
Identity Manager 2.x	Identity Manager 3.5.1	是
Identity Manager 3.0x	Identity Manager 3.5.1	是

3.2 規則結構變更

Identity Manager 3.5 和 3.5.1 包含新的規則結構，此結構會影響驅動程式參考規則的方式。雖然 3.5.1 驅動程式結構在 Identity Manager 3.5.1 環境中提供新增的功能，但 3.0.x Metadirectory 引擎無法執行 3.5.1 驅動程式組態。

但是，Identity Manager 3.5 和 3.5.1 可執行 3.0x 驅動程式組態。如果您的 3.0.x 驅動程式組態同時與 3.0.x 和 3.5 Metadirectory 引擎產生關聯，則無法升級 3.0.x 驅動程式。3.0.x 驅動程式組態在 3.5.1 環境中作業，但它們沒有 Identity Manager 3.5 和以上版本可負擔的新增功能。如果 3.0.x 驅動程式只與 3.5.1 或較新 Metadirectory 引擎產生關聯，則您應將 3.0.x 驅動程式組態升級爲 3.5.1。

如需規則結構與升級驅動程式至 3.5.1 的詳細資訊，請參閱《*瞭解 Identity Manager 3.5.1 的規則*》中的「升級 Identity Manager 規則」。

3.3 升級程序

若要成功升級至 Identity Manager 3.5.1，需要完成下列步驟。

3.3.1 輸出驅動程式

升級之前最重要的步驟是，備份目前驅動程式及其組態資訊。若要備份驅動程式，您必須將其輸出。

從 ConsoleOne 輸出

1. 在 ConsoleOne® 中，在「驅動程式集」物件上按一下滑鼠右鍵，然後選取「*內容* > *DirXML* > *驅動程式*」。
2. 選取您要建立輸出的驅動程式，然後按一下「*輸出*」。
3. 指定檔名。保留預設副檔名 .xml，然後按一下「*儲存*」。
4. 按一下「*輸出組態*」。

在 iManager 中，您可以輸出驅動程式或整個驅動程式集。如果您輸出驅動程式集，則會建立單一組態檔案。如果您輸出每個驅動程式，則會針對每個驅動程式建立組態檔案。

從 iManager 輸出

1. 在 iManager 中，選取「*DirXML 公用程式* > *輸出驅動程式*」。
2. 瀏覽並選取您要輸出的驅動程式或驅動程式集，然後按一下「*下一步*」。
3. 保留提示欄位空白，以建立完全相同的驅動程式副本，然後按「*下一步*」。
4. 如果您選取「驅動程式集」物件，便會針對每個驅動程式收到的提示頁面。保留欄位空白，以建立每個驅動程式之完全相同的副本。
5. 按一下「*另存新檔*」。
6. 在「檔案下載」視窗中，按一下「*儲存*」。
7. 瀏覽並指定輸出的檔案位置和名稱，然後按一下「*儲存*」。

重要：儲存該檔案時，其副檔名應爲 .xml。

取得驅動程式的輸出之後，請在實驗室環境中測試該輸出。輸入驅動程式輸出，並測試驅動程式，以確定所有參數都正確，且所有功能都正常。

從 Designer 輸出

1. 在 Designer 中，在模型產生器檢視窗中用滑鼠右鍵按一下「驅動程式」或「驅動程式集」物件，然後按一下「*輸出至組態檔案*」。
2. 在「輸出驅動程式組態」視窗中，瀏覽並指定輸出的檔案位置和名稱，然後按一下「*儲存*」。

3.3.2 驗證最低要求

若要升級至 Identity Manager 3.5.1，執行 Identity Manager 服務的伺服器需要符合最低要求。如需每個平台的最低要求清單，請參閱表格 1-3 (第 28 頁)。

如果支援元件需要升級，請以下列順序執行升級：

1. 將 OS 升級至支援的版本。例如，從 NetWare® 6.0 升級至 NetWare 6.5。
2. 使用最新的支援套件將 eDirectory™ 升級至 eDirectory 8.7.3.6 或 eDirectory 8.8。
3. 您的 Security Services 2.0.5 必須擁有 NMAS™ 3.1.3，以取得 SSL 支援。
4. 以最新的支援套件將 iManager 升級至 iManager 2.6 or 2. (包括升級至 Apache 2.0.52 或以上版本，和 Tomcat 4.1.18 或最新版本)。
5. 您也必須在網路上安裝 Novell Audit 2.0.2 Starter Pack 或 Sentinel™ 5.1.3。
6. 如需「Identity Manager 使用者應用程式」和工作流程提供，請參閱第 5.1 節 「安裝的先決條件」(第 93 頁)。
7. 升級 Identity Manager。
8. 啓用 Metadirectory 引擎和任何已升級的驅動程式。

3.3.3 升級引擎

已升級支援元件之後，會升級 DirXML 或 Identity Manager 引擎。

1. 在升級前，請先確定您具有有效的驅動程式輸出。請參閱第 3.3.1 節 「輸出驅動程式」(第 58 頁)。
2. 停止驅動程式。
   - **2a** 在 iManager 中，選取「*Identity Manager* > *Identity Manager 概觀*」。
   - **2b** 瀏覽並選取「驅動程式集」物件，然後按一下「*搜尋*」。
   - **2c** 按一下驅動程式圖示的右上角，然後選取「*停止驅動程式*」。
3. 將驅動程式設爲手動啓動。
   - **3a** 在 iManager 中，選取「*Identity Manager* > *Identity Manager 概觀*」。
   - **3b** 瀏覽並選取「驅動程式集」物件，然後按一下「*搜尋*」。
   - **3c** 按一下驅動程式圖示的右上角，然後按一下「*編輯內容*」。
   - **3d** 在「驅動程式組態」頁面上的「*啓動選項*」下，選取「*手動*」。
4. Install Identity Manager 3.5.1。

   升級至 Identity Manager 3.5.1 的步驟與安裝 Identity Manager 3.5 的步驟相同。如需如何安裝 Identity Manager 的指示，請參閱第 4 章 「安裝 Identity Manager」(第 63 頁)。

   Identity Manager 3.5.1 會覆蓋之前版本的 Identity Manager，並更新二進位碼。iManager 和 Designer 都會升級驅動程式來使用新功能。

4a 在 iManager 中按一下驅動程式，開始驅動程式升級精靈。

Designer 會在偵測到舊版驅動程式時自動開始驅動程式升級精靈。

5 設定驅動程式啓動選項。

5a 在 iManager 中，選取「*Identity Manager* > *Identity Manager 概觀*」。

5b 瀏覽並選取「驅動程式集」物件，然後按一下「*搜尋*」。

5c 按一下驅動程式圖示的右上角，然後按一下「*編輯內容*」。

5d 在「驅動程式組態」頁面上的「啓動選項」下，選取「*自動啓動*」，或選取您偏好的驅動程式啓動方法。

6 查看驅動程式參數和規則，以確定每項都按照您想要的方式設定。

7 啓動驅動程式

7a 在 iManager 中，選取「*Identity Manager* > *Identity Manager 概觀*」。

7b 瀏覽並選取「驅動程式集」物件，然後按一下「*搜尋*」。

7c 按一下驅動程式圖示的右上角，然後選取「*啓動驅動程式*」。

3.3.4 升級遠端載入器

如果您正在執行「遠端載入器」，則還需要升級遠端載入器檔案。

1 建立「遠端載入器」組態檔案的備份。檔案的預設位置如下：

- Windows C:\Novell\RemoteLoader*remoteloadername*-config.txt
- Linux：在 rdxml 路徑中建立您自己的組態檔案。

2 停止「遠端載入器」服務或精靈。

3 執行遠端載入器的安裝程式。

這會將檔案和二進位碼升級至目前版本。<Check Alignment of PHs> 請參駝「Novell Identity Manager 3.5.1 管理指南」》內的「*安裝遠端載入器*」。

3.3.5 升級 UNIX/Linux 環境

在 UNIX 或 Linux 環境中從 Identity Manager 3.0.1 升級至 Identity Manager 3.5.1 會建立兩個解除安裝位置，但不會完全移除套件。例如，如果您從 UNIX 平台開始 (例如 SLES 9) 然後安裝 Identity Manager 3.0.1，則解除安裝的 Identity Manager 將位於 /root/dirXML 目錄中。輸入 rpm -qa | grep -i dxml 可顯示 dXML 套件的安裝時間。

如果您想將此部署升級至 Identity Manager 3.5.1，則會在 /root/idm 目錄中建立新的解除安裝位置，因爲命名已發生變更。輸入 rpm -qa 可顯示更新套件的安裝時間。

因爲目錄已發生變更，所以當管理員解除安裝 Identity Manager 3.5.1 時，解除安裝程式將不會移除所有套件，即使它指出所有項目都已成功移除。若要移除剩下的套件，請使用 DirXML 解除安裝程式。

3.4 升級密碼同步化

如果是從 DirXML 1.1a 升級至 Identity Manager 3.5.1，則需要升級「密碼同步化」。請參閱《*Novell Identity Manager 3.5.1 管理指南*》內的「升級密碼同步化 1.0」。

如果是從 Identity Manager 2.x 升級，則「密碼同步化」相同，不會升級。

3.5 從 RNS 升級至 Novell Audit

如果您目前正在使用報告和通知服務 (Reporting and Notification Service，RNS)，引擎仍會繼續處理報告和通知服務 (RNS) 功能，但不建議使用。因爲 Novell Audit 會擴充報告和通知服務 (RNS) 提供的功能，並且在 Identity Manager 以後的版本中可能不再支援 RNS，所以您應該計劃採用 Novell Audit。

如需詳細資訊，請參閱《*Identity Manager 3.5.1 記錄和報告*》中的「查詢和報告」。

3.6 升級 DirXML 1.1a 驅動程式組態

從 DirXML 1.1a 升級至 Identity Manager 3.5.1 時，驅動程式組態可能會進行升級。升級驅動程式組態有兩個方面：

- 將 DirXML 規則 (rule) 轉換爲 Identity Manager 規則 (policy)。此動作由轉換工具執行，並不會增強驅動程式的功能。舊驅動程式執行時不會進行此轉換，但執行轉換可讓您檢視 Identity Manager iManager 外掛程式中的現有驅動程式組態。

  您必須詳細進行測試，確保此步驟能正常運作。我們也強烈建議您設定一個測試 / 開發環境，可在其中測試、分析和開發您的各種解決方案。在一切都如您所需地進行時，便可將最終產品部署到您的生產環境中。
- 升級驅動程式規則，以新增功能。例如，Identity Manager 現在可以使用 DirXML 程序檔來處理之前位於樣式表中的功能。此層級的功能最好由 Identity Manager 專家處理。

請參閱《*Novell Identity Manager 3.5.1 管理指南*》內的「將驅動程式組態從 DirXML 3.5.1a 升級至 Identity Manager 1.1 格式」和「在 Identity Manager 環境中管理 DirXML 3.5.1a 驅動程式」。

另一個方法是從 Identity Manager 驅動程式組態開始，自訂該組態以執行與 DirXML 1.1a 組態相同的動作。

3.7 啓用 Identity Manager

完成升級之後，您有 90 天的時間可以啓用 Metadirectory 引擎，以及所有已升級的驅動程式。如果沒有啓用引擎和驅動程式，就會在 90 天之後停止運作。如需如何啓用 Identity Manager 的指示，請參閱第 6 章 「啓用 Novell Identity Manager 產品」 (第 171 頁)。

安裝 Identity Manager

4

本節包含安裝 Identity Manager 和 Identity Manager 驅動程式的要求和指示。

4.1 安裝之前

安裝 Identity Manager 之前，請參閱第 2 章 「規劃」(第 39 頁)。

4.2 Identity Manager 元件和系統要求

Novell® Identity Manager 包含可以在多系統和平台上的環境內安裝的元件。根據系統組態，您可能需要多次執行 Identity Manager 安裝程式，以在適當的系統上安裝 Identity Manager 元件。

表格 1-3, 「Identity Manager 系統元件和要求」(第 28 頁) 列出 Identity Manager 的安裝元件，以及每個系統的要求。

4.3 在 NetWare 上安裝 Identity Manager

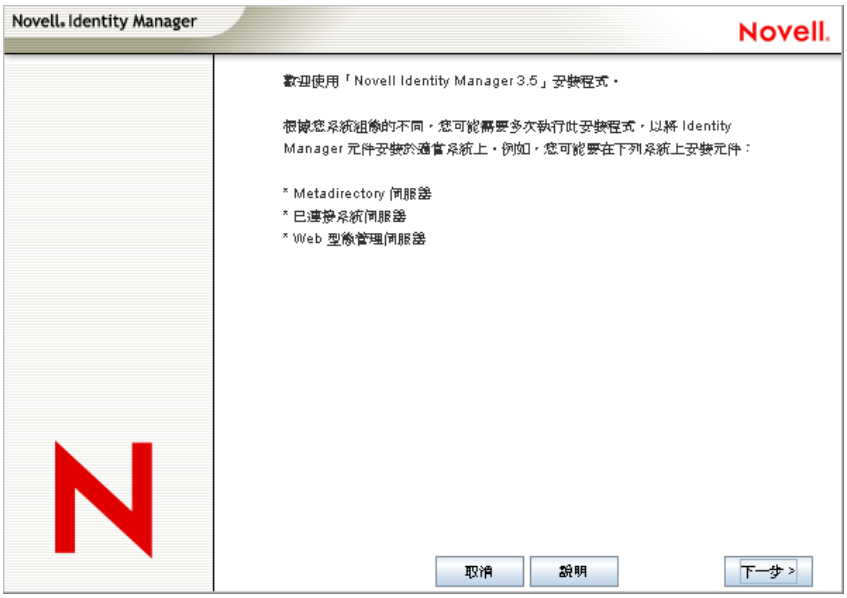
此程序涵蓋 NetWare® 之 「Metadirectory 伺服器」、「Web 元件」和 「公用程式」的安裝。在您開始之前，請確定系統符合第 4.2 節「Identity Manager 元件和系統要求」(第 63 頁) 中列出的要求。

1. 下載 Identity Manager。所需的 iso 影像檔。您可以下載 Identity Manager。iso 影像檔，來自 Novell 下載網站 (http://download.novell.com)。

   Identity Manager 的 NetWare 安裝位於 Identity_Manager_3_5_1_NW_Win.iso 或 Identity_Manager_3_5_1_DVD.iso 中。
2. 在您擷取檔案並將影像檔案放在光碟上，請將光碟放進伺服器的光碟機中，並允許將它掛載爲磁碟區。
3. 啓動 NetWare® GUI (在伺服器主控台提示下輸入 STARTX) 並選取 「*Novell* > *安裝*」。

4 在「已安裝的產品」視窗中選取「*新增*」，然後指定 Identity Manager product.ini 位於 NW 目錄中的檔案路徑。按一下「*確定*」後再按一下「*確定*，開始載入 Identity Manager 安裝程式。

5 已完成複製這些檔案之後，即會出現「Identity Manager 產品安裝」頁面。按一下「*下一步*」開始安裝。



6 選取授權合約的檢視語言，或使用預設的英文。

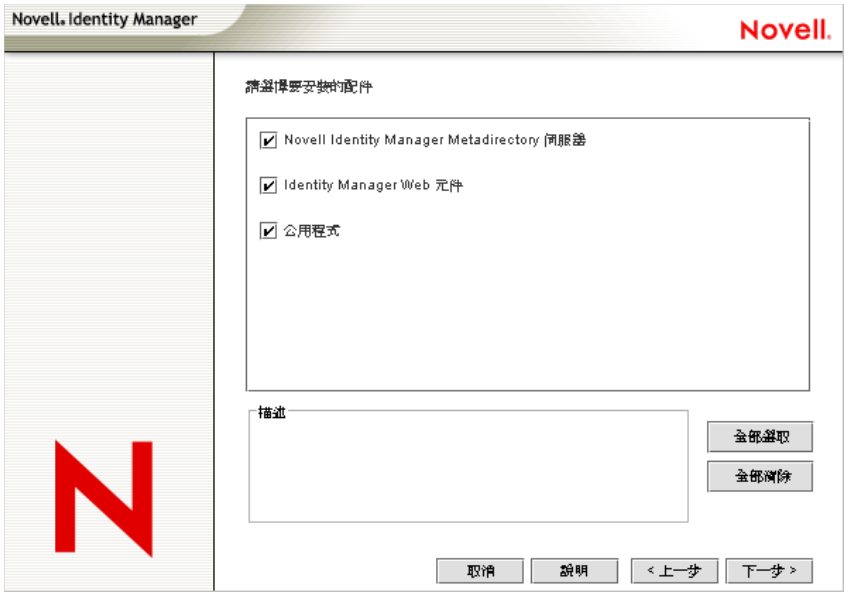
Identity Manager 安裝程式會自動視安裝的所在電腦，使用該電腦的語言進行安裝。如果安裝程式未翻譯成您電腦使用的語言，則預設使用英文。

7 閱讀授權合約，然後按一下「*我接受*」。

8 檢視說明系統類型的「綜覽」頁面，包括「Metadirectory 伺服器」、「web 元件」和「公用程式」，再按一下「*下一步*」繼續。

表格 1-3 (第 28 頁) 中亦包含此資訊。

9 在「Identity Manager 安裝」頁面上，選取您要安裝的元件。請參閱表格 1-3 (第 28 頁)。



可用選項如下。對於大多數安裝，您將選取所有元件。

- **Metadirectory 伺服器：**安裝 Metadirectory 引擎和服務驅動程式。在 NetWare 平台上，這包括下列項目的 Identity Manager 驅動程式：Avaya*、分隔文字、eDirectory™、、GroupWise®、JDBC*、JMS*、LDAP*、Linux/UNIX 設定、RACF*、SOAP、SIF*、Top Secret 以及工作順序。選取此選項也會擴充 eDirectory 綱要。

  重要：您必須先安裝 Novell eDirectory 8.7.3.6 和具有最新修補程式的 Security Services 2.0.5 (NMAS™ 3.1.3)，才能安裝此選項。將「Metadirectory 伺服器」元件安裝在您要執行 Identity Manager 之 Metadirectory 引擎的位置。如果沒有正確版本的 NMAS，您就會收到警告訊息，並且會失去 Identity Manager 的功能。

- **已連接系統：**安裝「遠端載入器」，其可讓您建立已連接系統與執行 Metadirectory 引擎的伺服器之間的連結。

  如果是 Identity Manager 的 Netware 安裝，則無法使用此選項，您在「安裝」螢幕上將看不到此選項。

- **Identity Manager Web 元件：**此選項會安裝 Identity Manager 外掛程式和驅動程式組態。

  必須先安裝 Novell iManager，才能安裝此選項。

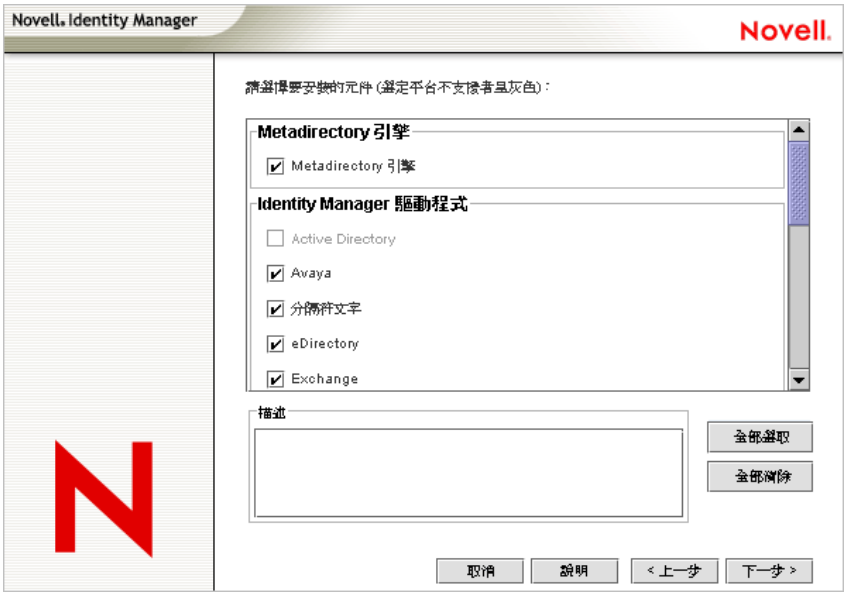
- **公用程式：**安裝 JDBC 驅動程式的其他程序檔以及其他驅動程式的公用程式。大多數驅動程式沒有與之連接的公用程式。驅動程式公用程式可能包括：
  - JDBC 驅動程式的 SQL 程序檔
  - JMS 元件
  - PeopleSoft 元件
  - 授權稽核工具
  - Active Directory 探查工具
  - Lotus Notes 探查工具

- SAP 公用程式

其他公用程式可讓您註冊 Identity Manager 的 Novell Audit 系統元件 (在安裝此驅動程式之前，必須先安裝有效的 eDirectory 版本和 Novell Audit 記錄伺服器)。

10 按一下「*下一步*」。

11 選取您要安裝的驅動程式，然後按一下「*下一步*」。



「選取引擎安裝的驅動程式」頁面可顯示哪些驅動程式能夠安裝在相對應的平台上。例如，在 NetWare 伺服器上，您無法安裝 Windows Active Directory 驅動程式。

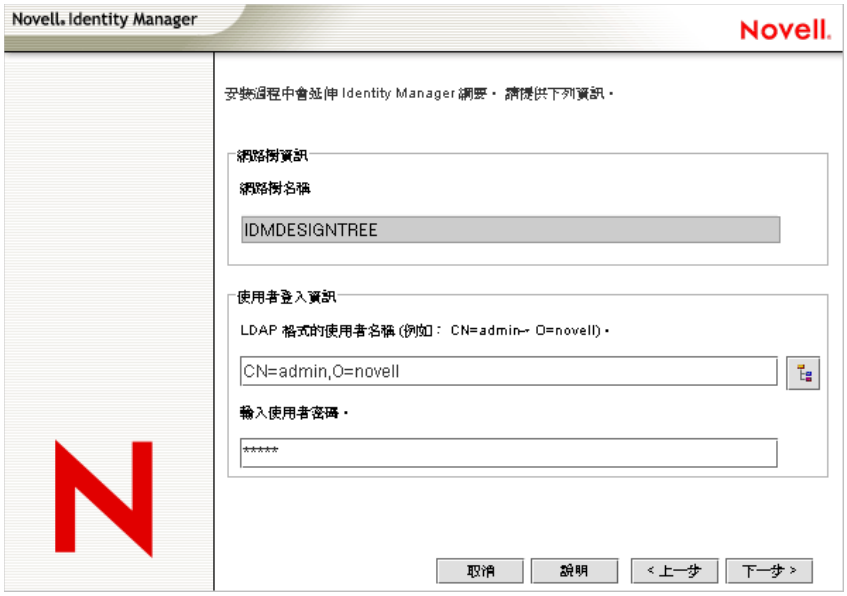
在預設狀態下，會選取此選項的所有可用驅動程式。建議安裝所有選取的驅動程式檔案，這樣當您稍後想要使用其他驅動程式時就無需執行安裝程式。在已透過 iManager 或 Designer 設定驅動程式組態，並部署驅動程式之後，才會使用驅動程式檔案。

如果您不要安裝所有的驅動程式，您可以按一下「*全部清除*」，再選擇您所需的驅動程式，或按一下您不要安裝的驅動程式，以取消選擇。如果日後您需要其他驅動程式，您必須返回這個安裝程式，以安裝任何您未選擇的驅動程式。您也可以使用 Designer 來建立、修改和部署驅動程式檔案。

12 當您看見提醒您啓用產品的資訊訊息時，請按一下「*確定*」。

驅動程式需要在安裝後的 90 天之內啓用；否則，將會關閉。

13 在「綱要延伸」頁面上，指定下列內容：



- **使用者名稱：** 指定具有延伸綱要之權限的使用者名稱 (爲輕量目錄存取協定 (LDAP) 格式，例如 CN=admin,O=novell)。在此頁面上，選取擁有足夠權限來延伸 eDirectory 綱要的使用者 (此人擁有網路樹根部的「監督者」權限，例如管理員)。
- **使用者密碼：**指定使用者的密碼。

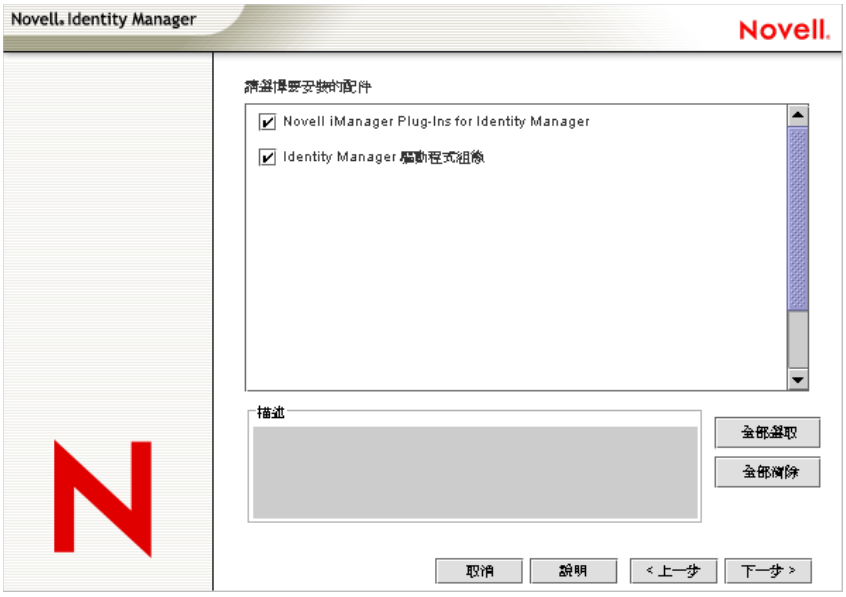
14 按一下「*下一步*」。

驗證使用者資訊時，您會看見第一個「元件」頁面 (共三個)：

*在第二個「元件」頁面上，如果您的伺服器已安裝「Novell Audit 系統」，則會選取 Identity Manager 的「Novell Audit 系統元件」。*否則，不會選取它。「*應用程式元件*」選項會安裝應用程式系統 (如 JDBC 和 PeopleSoft) 的元件。

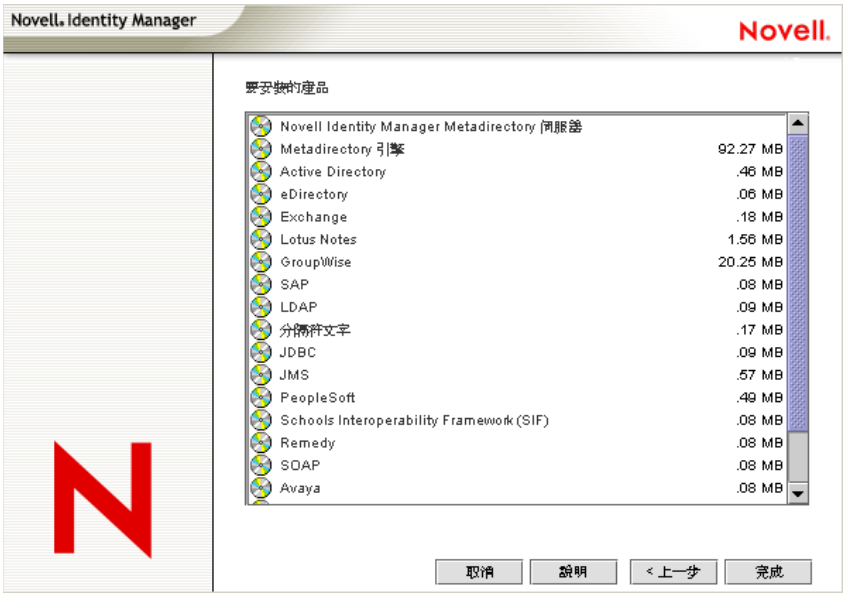
如果驅動程式偵測到現有的驅動程式組態檔案，就會將它們移到備份路徑。

15 按一下「*下一步*」。



16 第三個「元件」頁面會安裝公用程式。如果平台特定的公用程式供您所安裝之平台外的平台使用，則這些公用程式會變爲灰色。對於 NetWare，唯一可用的選項爲 JDBC 驅動程式的 SQL 程序檔案 JMS 元件。選擇您需要的元件，再按一下「*下一步*」。

17 在「摘要」頁面上讀取並驗證您的選項，然後按一下「*完成*」。



Novell Identity Manager 安裝程序會關閉 eDirectory 以延伸綱要。安裝程序開始安裝選取的產品和元件。

18 安裝完成並顯示「安裝完成」對話方塊之後，按一下「*關閉*」。

19 爲了讓 iManager 能辨識您安裝的外掛程式，請立即重新啓動您的 Web 服務，並重新啓動 Tomcat。

如果您已經安裝 Identity Manager 驅動程式，請使用 iManager 2.6 或更新版本的 Identity Manager 組態精靈，或者，您也可以使用 Designer 來設定驅動程式。

4.4 在 Windows 上安裝 Identity Manager

此程序涵蓋 Windows 之「Metadirectory 伺服器」、「Web 元件」和「公用程式」的安裝。

在您開始之前，請確定系統符合表格 1-3 (第 28 頁)中列出的要求。

1 下載 Identity Manager。所需的 iso 影像檔。您可以下載 Identity Manager。iso 影像檔，來自 Novell 下載網站 (http://download.novell.com)。

Identity Manager 的 Windows 安裝位於 Identity_Manager_3_5_1_NW_Win.iso 或 Identity_Manager_3_5_1_DVD.iso 中。

2 在擷取檔案之後，請連按兩下 \NT 目錄中的 install.exe 檔案。

已完成複製這些檔案之後，即會出現「Identity Manager 產品安裝」頁面。

3 按一下「*下一步*」開始安裝。

4 選取授權合約的檢視語言，或使用預設的英文。

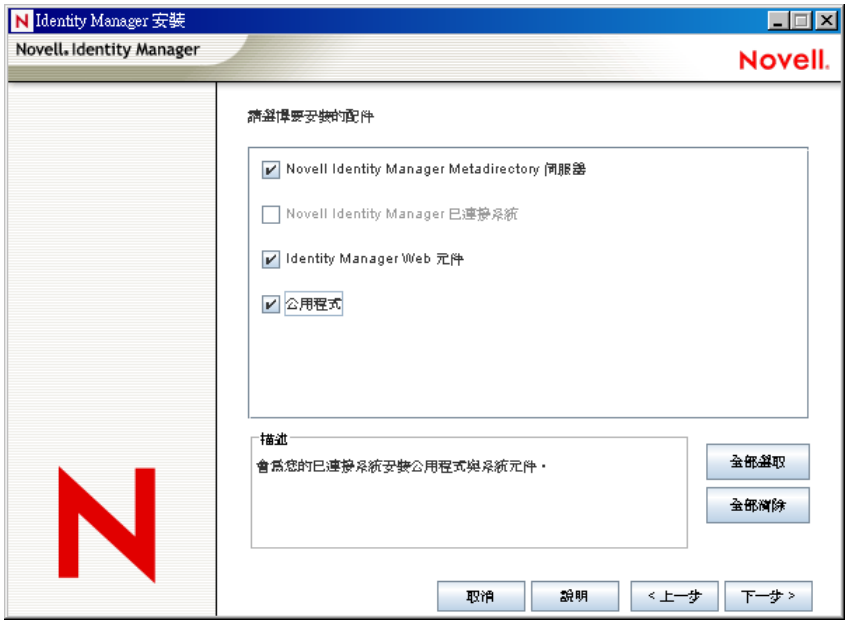
Identity Manager 安裝程式會自動視安裝的所在電腦，使用該電腦的語言進行安裝。如果安裝程式未翻譯成您電腦使用的語言，則預設使用英文。

5 閱讀授權合約，然後按一下「*我接受*」。

6 檢視說明系統類型的「綜覽」頁面，包括「Metadirectory 伺服器」、「Web 元件」和「公用程式」，再按一下「*下一步*」繼續。

表格 1-3 (第 28 頁) 中亦包含此資訊。

7 在「Identity Manager 安裝」頁面上，選取您要安裝的元件。



下列選項可供使用：

- **Metadirectory 伺服器**：安裝 Metadirectory 引擎和服務驅動程式。這包括下列項目的 Identity Manager 驅動程式：Active Directory、Avaya、分隔文字、eDirectory、Exchange、GroupWise、JDBC、JMS、LDAP、Linux/UNIX 設定、Lotus Notes、PeopleSoft、RACF、Remedy、SOAP、SAP、SIF、Top Secret 以及工作順序。選取此選項也會延伸 eDirectory 綱要。

  重要：您必須先安裝 Novell eDirectory 8.8 和具有最新修補程式的 Security Services 2.0.5 (NMAS 3.1.3)，才能安裝此選項。將「Metadirectory 伺服器」元件安裝在您要執行 Identity Manager 之 Metadirectory 引擎的位置。如果沒有正確版本的 NMAS，您就會收到警告訊息，並且會失去 Identity Manager 的功能。

- **已連接系統**：安裝「遠端載入器」，其可讓您建立已連接系統與執行 Metadirectory 引擎的伺服器之間的連結。對於 Windows，此選項會安裝下列驅動程式：Active Directory、Avaya、分隔文字、eDirectory、Exchange、GroupWise、JDBC、JMS、LDAP、Linux/UNIX 設定、Lotus Notes、PeopleSoft、RACF、Remedy、SOAP、SAP、SIF、Top Secret 以及工作順序。

  安裝「已連接系統」，讓應用程序從應用程式伺服器連接到執行 Metadirectory 引擎的 eDirectory 型態伺服器。此程序包含在第 4.5 節「在 Windows 上安裝已連接系統選項」(第 75 頁)下。

- **Web 元件** 此選項會安裝驅動程式組態、iManager 外掛程式和應用程式程序檔與公用程式。

  必須先安裝 Novell iManager，才能安裝此選項。

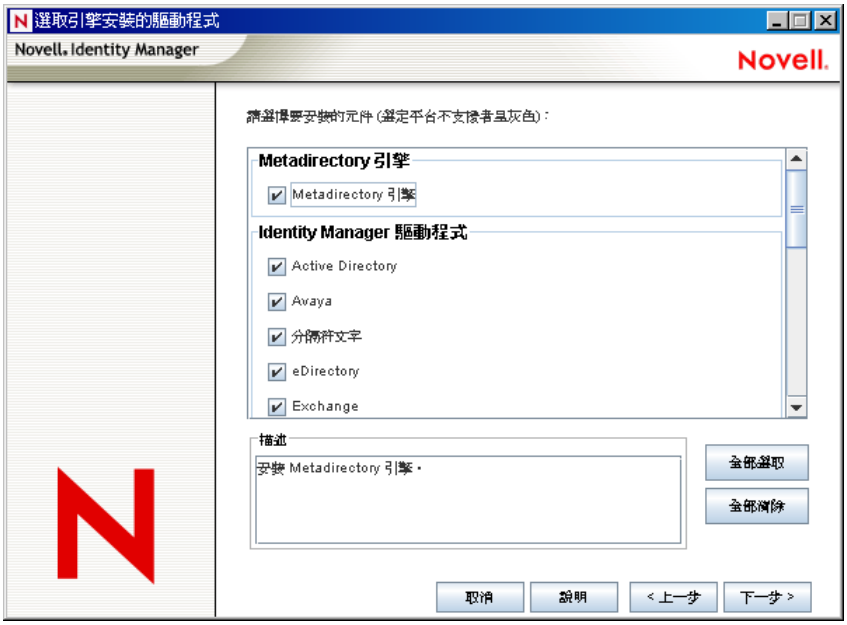
- **公用程式**：安裝 JDBC 驅動程式的其他程序檔以及其他驅動程式的公用程式。大多數驅動程式沒有與之連接的公用程式。驅動程式公用程式可能包括：
  - JDBC 驅動程式的 SQL 程序檔
  - JMS 元件

- PeopleSoft 元件
- 授權稽核工具
- Active Directory 探查工具
- Lotus Notes 探查工具
- SAP 公用程式
- Scripting Driver 安裝程式與組態工具

其他公用程式可讓您註冊 Identity Manager 的 Novell Audit 系統元件 (在安裝此驅動程式之前，必須先安裝有效的 eDirectory 版本和 Novell Audit 記錄伺服器)。

8 按一下「*下一步*」。

9 選取您要安裝的驅動程式，然後按一下「*下一步*」。



「選取引擎安裝的驅動程式」頁面可顯示哪些驅動程式能夠安裝在相對應的平台上。在預設狀態下，會選取所有可用的驅動程式。

建議安裝所有驅動程式檔案，這樣當您稍後想要使用其他驅動程式時就無需執行安裝程式。在已透過 iManager 或 Designer 設定驅動程式組態，並部署驅動程式之後，才會使用驅動程式檔案。

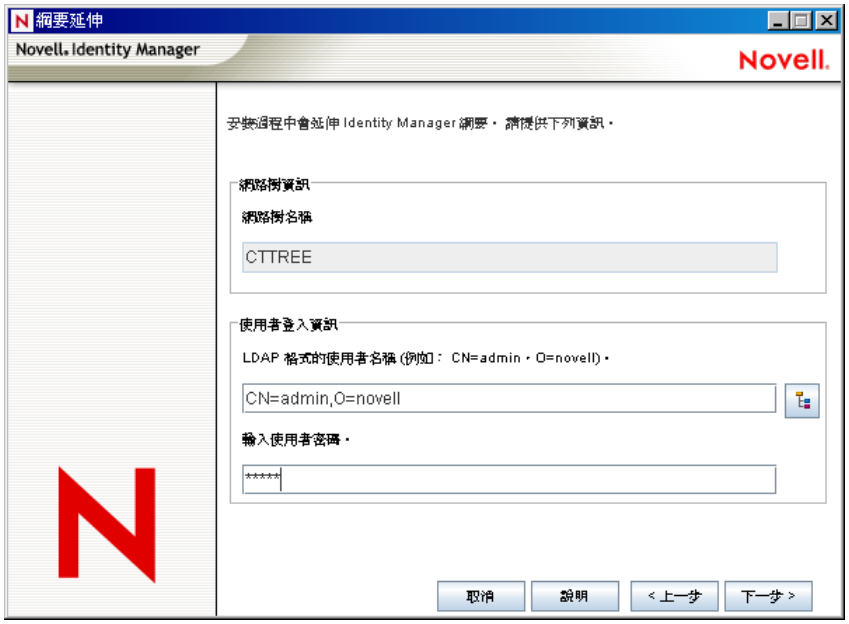
10 當您看見提醒您啓用產品的資訊訊息時，請按一下「*確定*」。

驅動程式需要在安裝後的 90 天之內啓用；否則，將會關閉。

11 但您看見「密碼同步化升級警告！」訊息時，請按一下「*確定*」。

此訊息是針對執行「密碼同步化 1.0」的 Windows 伺服器顯示。如果您想與 1.0 反向相容，則必須將其他規則新增至驅動程式組態檔案。如果沒有這些規則，則 Password Synchronization 1.0 僅可用於現有的帳戶，而不可用於新的或重新命名的帳戶。

12 在「綱要延伸」頁面上，指定下列內容：



- **使用者名稱：**針對擁有權限來延伸 eDirectory 綱要的使用者，指定使用者名稱 (使用 LDAP 格式，例如 CN=admin,O=novell)；此人擁有網路樹根部的「監督者」權限，例如管理員。
- **使用者密碼：**指定使用者的密碼。

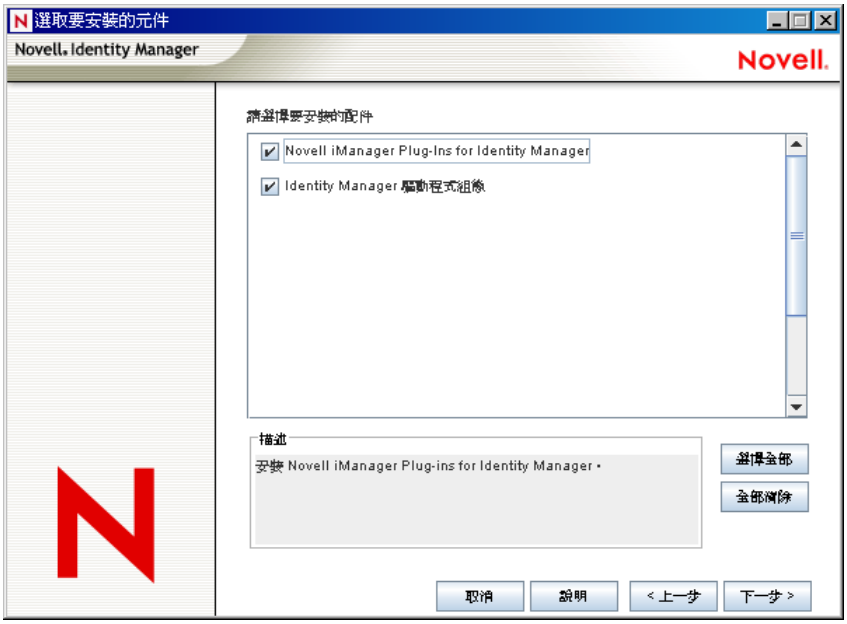
13 按一下「*下一步*」。驗證使用者資訊時，您會看見第一個 (共三個) 「元件」頁面：

在「選擇要安裝的元件」頁面上，如果您的 eDirectory 爲有效版本，且 Novell Audit 記錄伺服器已安裝在樹狀結構中，則「*註冊 Identity Manager 的 Novell Audit 系統元件*」已選擇。否則，不會選取它。「*應用程式元件*」選項會安裝應用程式系統 (如 JDBC 和 PeopleSoft) 的元件。

如果驅動程式偵測到現有的驅動程式組態檔案，就會將它們移到備份路徑。

「*Client Login Extension for Novell Identity Manager*」選項會將 Client Login Extension 的安裝程式複製到您的檔案系統中。如需 Client Login Extension for Novell Identity Manager 3.5.1 的詳細資訊，請參閱「 Novell Identity Manager 3.5.1 Administration Guide」中的 *Client Login Extension for Novell Identity Manager*。

14 選取您要安裝的產品，然後按一下「*下一步*」。



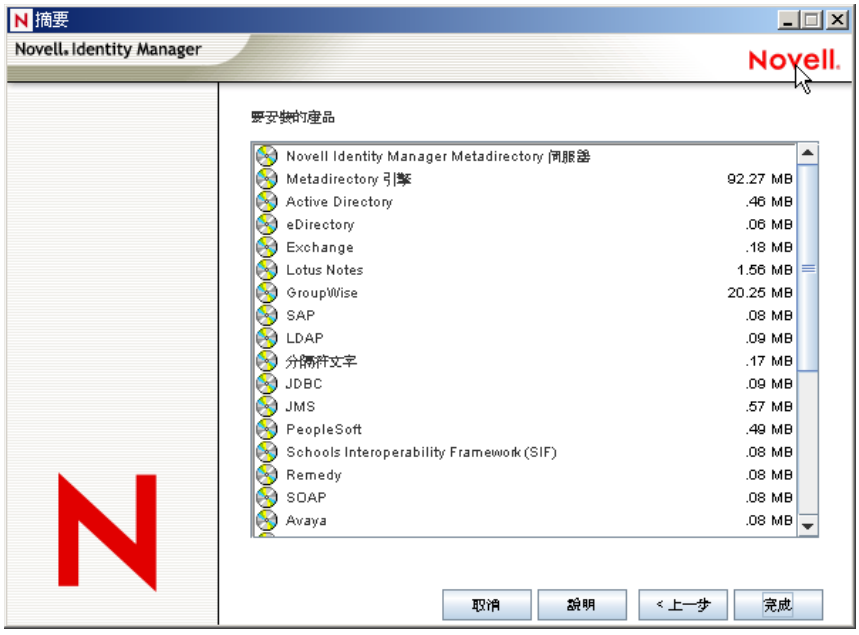
15 隨即顯示額外的頁面來使用 SSL 埠 443 安裝 iManager 的 Identity Manager 外掛程式。按一下「下一步」。

16 第三個「元件」頁面會安裝公用程式。Windows 安裝會顯示額外的畫面，顯示放置「應用程式元件」的目錄。預設爲 C:\Novell\NDS\DirXMLUtilities。按一下「下一步」。

17 在「選取要安裝的元件」頁面上，如果平台特定的公用程式供您所安裝之平台之外的平台使用，則這些公用程式會變爲灰色。在 Windows 上，所有元件都可用，包括 JDBC 驅動程式的的 SQL 程序檔、JMS 元件、Peoplesoft 元件、授權核准工具、Active Directory 探查工具、Lotus Notes 探查工具和 SAP 公用程式。選取您需要的元件，再按一下「*下一步*」。

18 如果您已選擇將 Client Login Extension for Novell Identity Manager 的安裝程式複製到您的檔案系統中，請選擇安裝路徑，或使用 C:\Novell\NDS\DirXMLUtilities\cle 的預設路徑。按一下「下一步」。

19 在「摘要」頁面上讀取並驗證您的選項，然後按一下「*完成*」。



Novell Identity Manager 安裝程序會關閉 eDirectory 以延伸綱要。安裝程序開始安裝選取的產品和元件。

20 安裝完成並顯示「安裝完成」對話方塊之後，按一下「*關閉*」。

21 爲了讓 iManager 能辨識您安裝的外掛程式，請立即重新啓動您的 Web 服務，並重新啓動 Tomcat。

如果您已經安裝 Identity Manager 驅動程式，請使用 iManager 2.6 或更新版本的 Identity Manager 組態精靈，或者，您也可以使用 Designer 來設定驅動程式。

4.5 在 Windows 上安裝已連接系統選項

第 4.4 節「在 Windows 上安裝 Identity Manager」(第 69 頁) 涵蓋 Windows 版之「Metadirectory 伺服器」、「Web 元件」和「公用程式」的安裝。此外，Windows 伺服器可以使用「已連接系統」選項。

當您不想讓應用程式伺服器代管 eDirectory 服務和 Metadirectory 引擎時，請使用「已連接系統」選項。「遠端載入器」會透過 Identity Manager 提供所需的同步化，而無需載入可在其他位置存取的應用程式。

在您開始之前，請確定系統符合表格 1-3 (第 28 頁) 中列出的要求。

1 下載 Identity Manager。所需的 iso 影像檔。您可以下載 Identity Manager。iso 影像檔，來自 Novell 下載網站 (http://download.novell.com)。

Identity Manager 的 Windows 安裝位於 Identity_Manager_3_5_1_NW_Win.iso 或 Identity_Manager_3_5_1_DVD.iso 中。

2 從 \NT 目錄執行 install.exe。

3 閱讀「歡迎」資訊，然後按一下「*下一步*」。

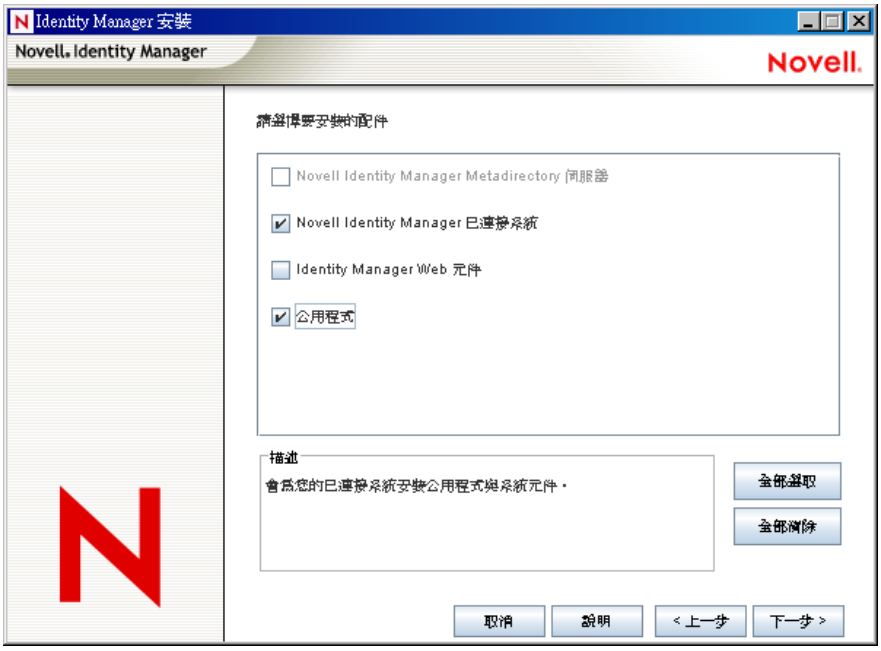
4 選取授權合約的檢視語言，或使用預設的英文。

Identity Manager 安裝程式會自動視安裝的所在電腦，使用該電腦的語言進行安裝。如果安裝程式未翻譯成您電腦使用的語言，則預設使用英文。

5 閱讀授權合約，然後按一下「*我接受*」。

6 檢視各種系統和元件的「綜覽」頁面，然後按「*下一步*」開始安裝。

7 若要選取「已連接系統」選項，請先按一下「*全部清除*」，然後選取「*已連接系統*」和「*公用程式*」。如果您的伺服器上安裝了 iManager 公用程式，而且想新增 Identity Manager 的 Identity Manager 外掛程式和驅動程式，則也應選取「*Web 元件*」。

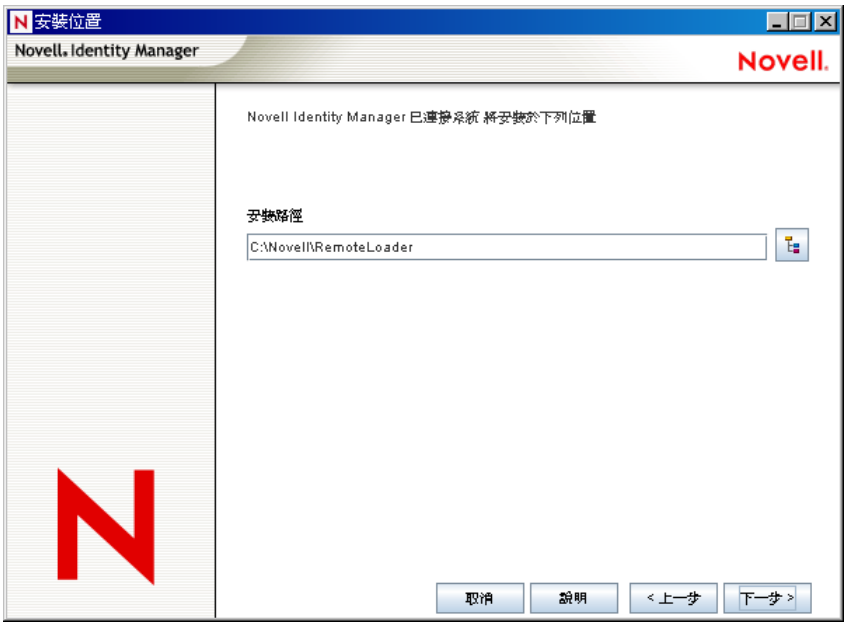


- **已連接系統**：安裝「遠端載入器」，其可讓您建立已連接系統與執行 Metadirectory 引擎的伺服器之間的連結。對於 Windows，此選項會安裝下列驅動程式：Active Directory、Avaya、分隔文字、eDirectory、Exchange、GroupWise、JDBC、JMS、LDAP、Linux/UNIX 設定、Lotus Notes、PeopleSoft、RACF、Remedy、SOAP、SAP、SIF、Top Secret 以及工作順序。
- **公用程式**：安裝 JDBC 驅動程式的其他程序檔以及其他驅動程式的公用程式。大多數驅動程式沒有與之連接的公用程式。驅動程式公用程式可能包括：
  - JDBC 驅動程式的 SQL 程序檔
  - JMS 元件
  - PeopleSoft 元件
  - 授權稽核工具
  - Active Directory 探查工具
  - Lotus Notes 探查工具
  - SAP 公用程式
  - Scripting Driver 安裝程式與組態工具

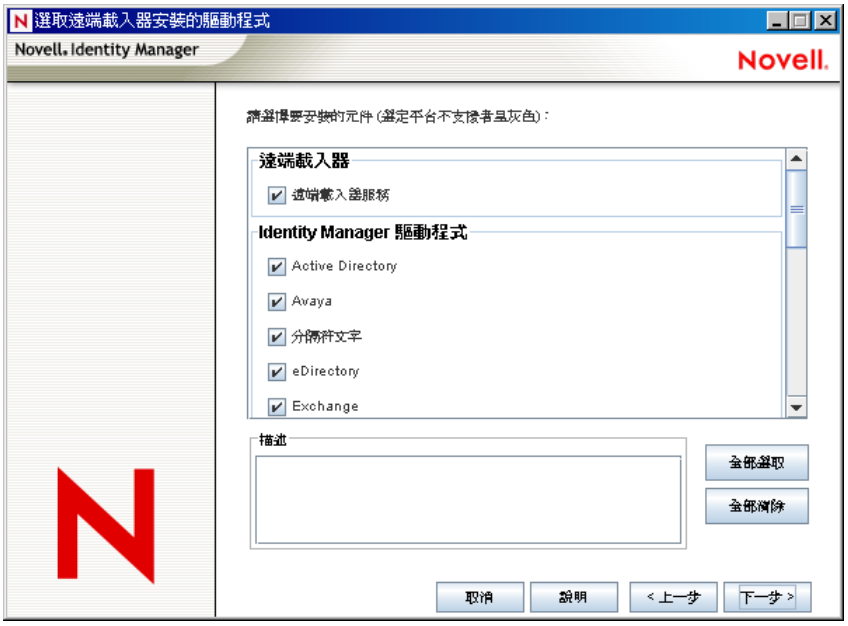
  其他公用程式可讓您註冊 Identity Manager 的 Novell Audit 系統元件 (在安裝此驅動程式之前，必須先安裝有效的 eDirectory 版本和 Novell Audit 記錄伺服器)。

8 按一下「下一步」。

9 在「安裝位置」頁面上，按一下「*下一步*」接受預設的目錄路徑，即 C:\Novell\RemoteLoader。



10 在「選取遠端載入器安裝的驅動程式」頁面上，請選取您要載入的 Identity Manager 驅動程式，然後按一下「*下一步*」。



驅動程式的選項包括：Acitve Directory、AVAYA、分隔文字、eDirectory、Exchange、GroupWise、JDBC、JMS、LDAP、Linux/UNIX 設定、Lotus Notes、PeopleSoft、RACF、Remedy、SOAP、SAP、SIF、Top Secret 以及工作順序。

如果您不要安裝所有的驅動程式，您可以按一下「*全部清除*」，再選擇您所需的驅動程式，或按一下您不要安裝的驅動程式，以取消選擇。如果日後您需要其他驅動程式，您

必須返回這個安裝程式，以安裝任何您未選擇的驅動程式。您也可以使用 Designer 來建立、修改和部署驅動程式檔案。

11 當您看見提醒您啓用產品的資訊訊息時，請按一下「*確定*」。

驅動程式需要在安裝後的 90 天之內啓用；否則，將會關閉。

12 但您看見「密碼同步化升級警告！」訊息時，請按一下「*確定*」。

此訊息是針對執行「密碼同步化 1.0」的 Windows 伺服器顯示。如果您想與 1.0 反向相容，則必須將其他規則新增至驅動程式組態檔案。如果沒有這些規則，則 Password Synchronization 1.0 僅可用於現有的帳戶，而不可用於新的或重新命名的帳戶。

13 按一下「*是*」在桌面上建立 Remote Loader Console 的捷徑。如果您不要捷徑，請按一下「*否*」。

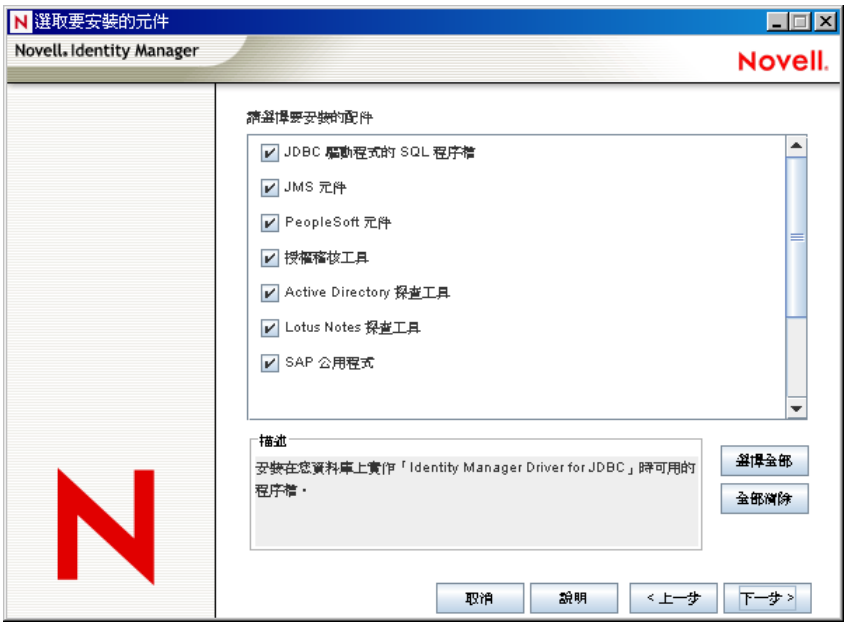
在「選擇要安裝的元件」頁面上，如果您的 eDirectory 爲有效版本，且 Novell Audit 記錄伺服器已安裝在樹狀結構中，則「*註冊 Identity Manager 的 Novell Audit 系統元件*」已選擇。否則，不會選取它。「*應用程式元件*」選項會安裝應用程式系統 (如 JDBC 和 PeopleSoft) 的元件。

「*Client Login Extension for Novell Identity Manager*」選項會將 Client Login Extension 的安裝程式複製到您的檔案系統中。如需 Client Login Extension for Novell Identity Manager 3.5.1 的詳細資訊，請參閱「 Novell Identity Manager 3.5.1 Administration Guide」中的 *Client Login Extension for Novell Identity Manager*。

14 選取您要安裝的產品，然後按一下「*下一步*」。

15 按一下「*下一步*」接受 Identity Manager 公用程式的預設安裝路徑 (C:\Novell\NDS\DirXMLUtilities)。

16 選取想安裝的驅動程式元件和公用程式，然後按一下「*下一步*」。



17 如果您已選擇將 Client Login Extension for Novell Identity Manager 的安裝程式複製到您的檔案系統中，請選擇安裝路徑，或使用 C:\Novell\NDS\DirXMLUtilities\cle 的預設路徑。按一下「下一步」。

18 檢視「摘要」頁面中列出的項目。如果您核准，請按一下「*完成*」以安裝元件。

19 按一下「*關閉*」離開安裝程式。

4.6 透過 GUI 介面在 UNIX/Linux 平台上安裝 Identity Manager

在您開始之前，請確定系統符合第 4.2 節「Identity Manager 元件和系統要求」(第 63 頁)中列出的要求。

1 下載 Identity Manager。所需的 iso 影像檔。您可以下載 Identity Manager。iso 影像檔，來自 Novell 下載網站 (http://download.novell.com)。

例如，Linux 位於 Identity_Manager_5_1_ 或 Identity_Manager_3_5_DVD.iso，而 AIX 和 Solaris 位於 Identity_Manager_1_3_Unix.iso 或 Identity_Manager_5_1_DVD.iso。_1_3_5_1

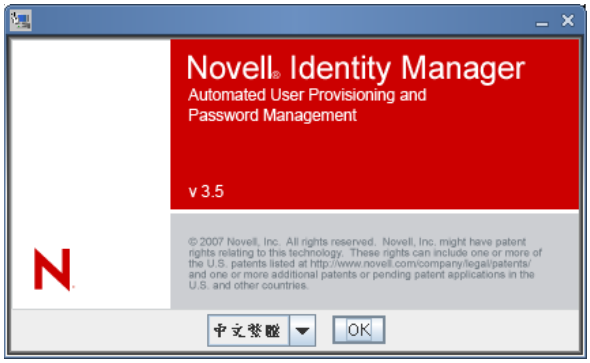
2 在主機電腦上，以根部身分登入。

3 若要在 Linux 上執行 GUI 安裝，請按一下根目錄中的 install.bin 檔案。系統將詢問您要以終端機模式或顯示模式來安裝檔案。選取「*終端機*」。install.bin 檔案會檢查 Xwindows 是否存在，如果存在則會啓動 Identity Manager 適用於 Linux 的 GUI 安裝程式。

附註：如果按一下 install.bin 無法啓動 GUI 安裝程式，則請開啓終端機視窗並手動 install.bin。如果您的 Solaris 伺服器可執行 eDirectory 8.8.x，則請不要使用 GUI 來執行 Identity Manager 安裝程式。請參閱第 4.7 節「使用主控台在 UNIX/Linux 平台上安裝 Identity Manager」(第 83 頁)。

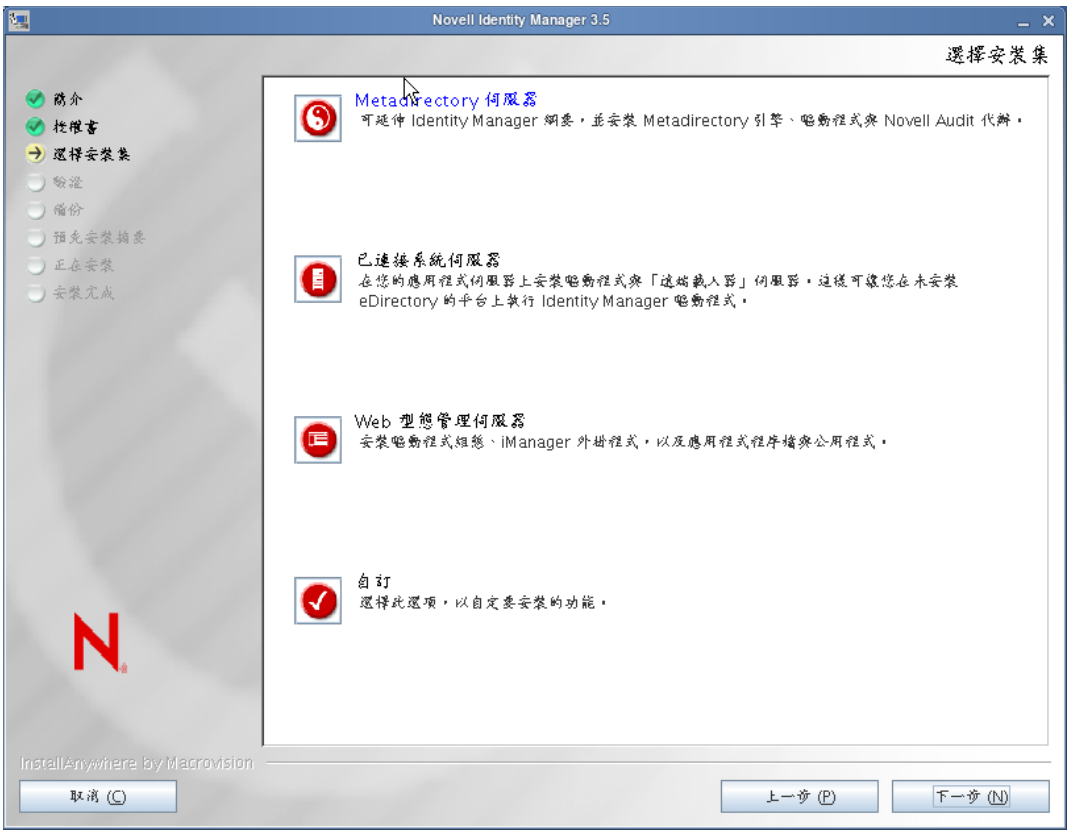
---

4 選取安裝程式的執行語言，或使用預設的英文。按一下「確定」。



5 檢閱「歡迎」資訊，然後按一下「*下一步*」繼續安裝。

6 閱讀授權合約，選取「*我接受授權合約中的條款*」，然後按一下「*下一步*」。



7 指定您想安裝的安裝集。安裝集包含下列元件：

- **Metadirectory 伺服器：**安裝 Metadirectory 引擎和服務驅動程式、Identity Manager 驅動程式、Novell Audit 代辦，並延伸 eDirectory 綱要。

  您必須先安裝 Novell eDirectory 8.7.3.6 或以上版本和具有最新支援套件的 Security Services 2.0.5 (NMAS 3.1.3)，才能安裝此選項。如果沒有安裝這些項目，Identity Manager 安裝程序就會停止。

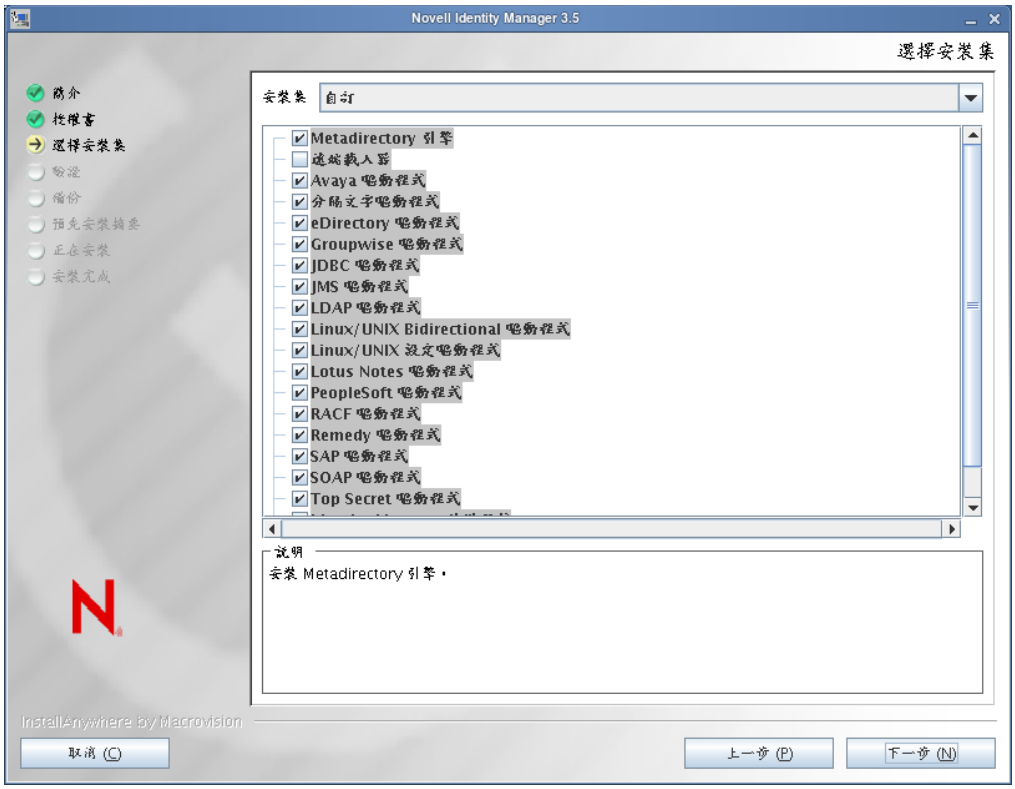
- **已連接系統伺服器：**安裝「遠端載入器」以及這些驅動程式：Avaya、分隔文字、GroupWise、JDBC、JMS、LDAP、Linux/UNIX 設定、Linux/UNIX Bidirectional、Lotus Notes、PeopleSoft、RACF、Remedy、SAP、SIF、Top Secret 以及工作順序。當您不想讓應用程式伺服器代管 eDirectory 服務和 Metadirectory 引擎時，請選擇「已連接系統伺服器」選項。

- **Web 型態的管理伺服器：**安裝 Identity Manager 外掛程式和 Identity Manager 驅動程式規則。

  必須先安裝 Novell iManager，才能安裝此選項。

  依預設，Identity Manager 驅動程式公用程式不會安裝在 Linux/UNIX 的安裝上。您必須從 Identity Manager 安裝光碟手動複製公用程式到 Identity Manager 伺服器。您可以在*平台的*\setup\utilities 目錄下找到所有公用程式。

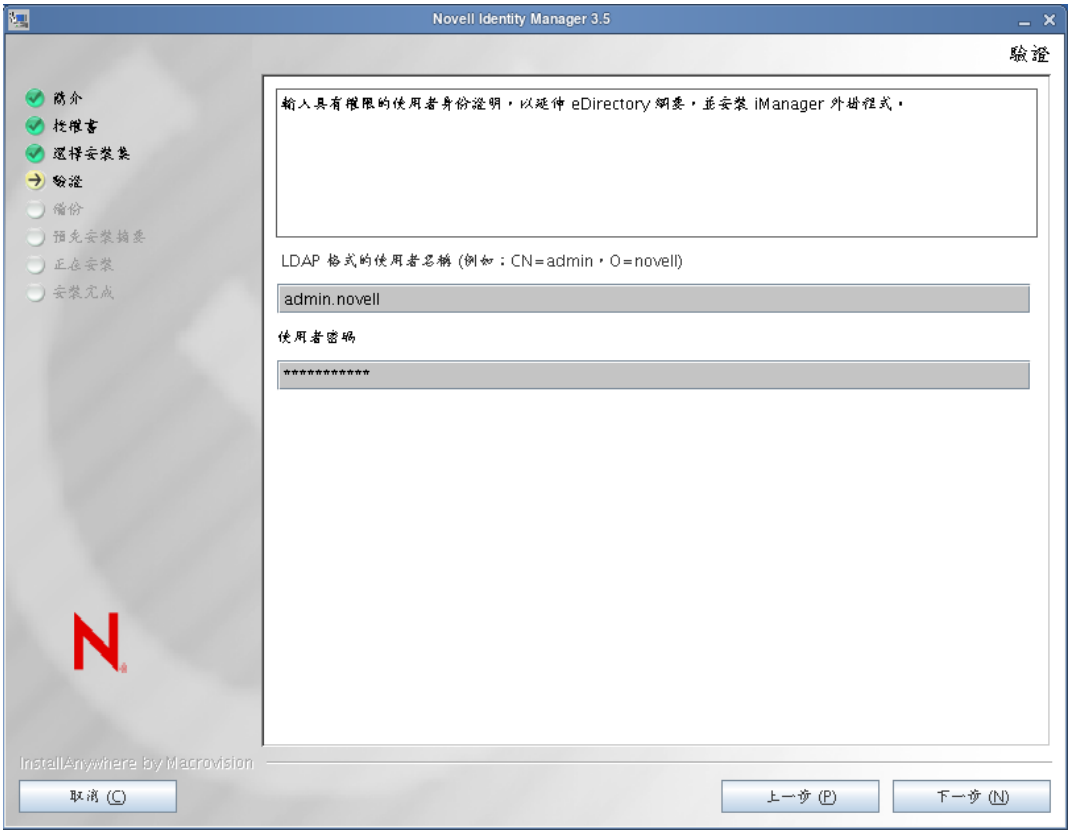
- **自訂：**安裝您從所有元件的清單中選取的特定元件。



您可以選取「*上一步*」返回先前的選單並修改您的安裝選項。

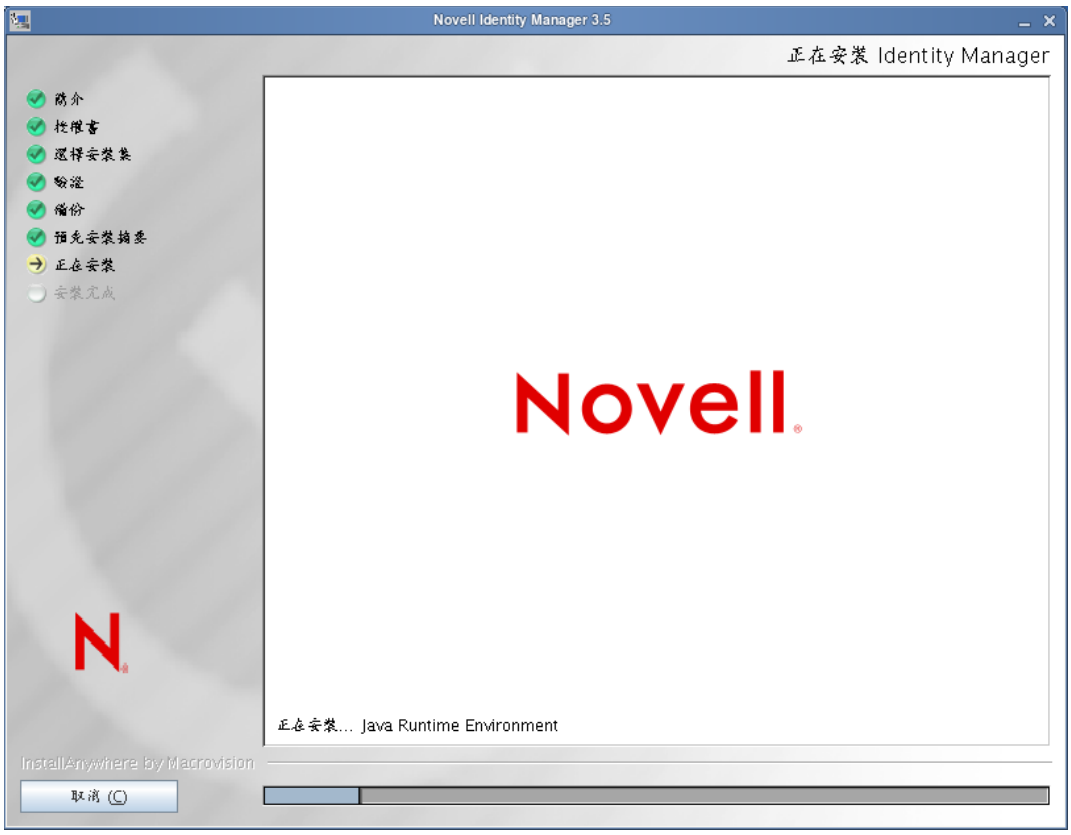
8 (選擇性) 是您選取的選項 (例如 Metadirectory 伺服器) 以及是否可執行 eDirectory v8.8 而定，系統會提示您設定 LD_LIBRARY_PATH 環境變數。若要執行此動作，請輸入 . /opt/novell/eDirectory/bin/ndspath 來執行 /opt/novell/eDirectory/bin/ndspath 程序檔，然後重新執行安裝。

9 如果您選取安裝 「Metadirectory 伺服器」，則會提示您輸入輕量目錄存取協定 (LDAP) 使用者名稱 (CN=admin,O=novell) 和密碼。選取擁有足夠權限來延伸 eDirectory 綱要的使用者 (此人擁有網路樹根部的 「監督者」權限，例如管理員)。



重要： (僅適用於 Solaris 安裝) 如果您在 eDirectory 存在的相同伺服器上安裝 Web 型態的管理伺服器，則當系統提示您輸入 Web 伺服器安全連接埠時，請將預設值變更爲某個可用的連接埠，例如 8443。

10 驗證 「預先安裝摘要」頁面中的資料是否正確，然後按一下 「*安裝*」開始安裝套件。



安裝 「Metadirectory 引擎」和綱要檔案時，eDirectory 會暫時關閉。依預設，會安裝所有可用的驅動程式，因此稍後當您需要另一個驅動程式時便不必執行安裝程式。在已透過 iManager 或 Designer 設定驅動程式組態，並部署驅動程式之後，才會使用驅動程式檔案。

11 當您看到 「*安裝完成*」頁面時，按一下完成來關閉安裝程式。

4.7 使用主控台在 UNIX/Linux 平台上安裝 Identity Manager

在您開始之前，請確定系統符合表格 1-3 (第 28 頁) 中列出的要求。

1 下載 Identity Manager。所需的 iso 影像檔。您可以下載 Identity Manager。iso 影像檔，來自 Novell 下載網站 (http://download.novell.com)。

例如，Linux 位於 Identity_Manager_5_1_ 或 Identity_Manager_3_5_DVD.iso，而 AIX 和 Solaris 位於 Identity_Manager_1_3_Unix.iso 或 Identity_Manager_5_1_DVD.iso。_1_3_5_1

2 在主機電腦上，以根部身分登入。

3 執行 . 設計目錄中的 bin 檔案。

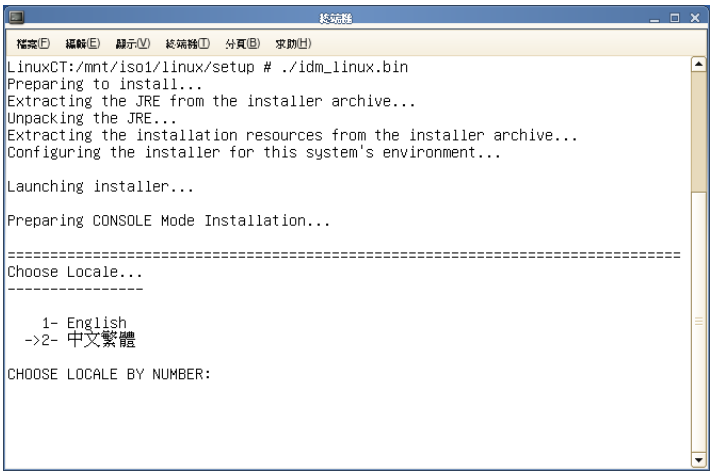
將目前的工作目錄變更爲安裝目錄，即安裝所在的位置。然後，輸入下列其中一個指令，以執行安裝。

平台	範例路徑	安裝檔案
Linux	linux/setup/	idm_linux.bin
Solaris	solaris/setup/	idm_solaris.bin
AIX	aix/setup/	idm_aix.bin

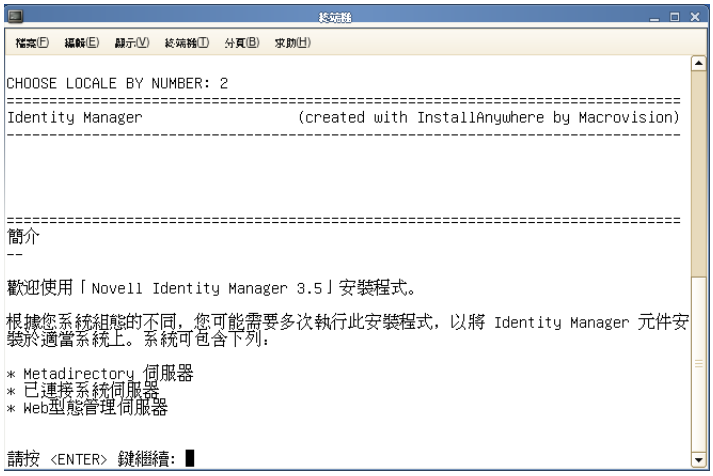
這些路徑是相對於安裝影像檔的根目錄，可以是您擴充該影像檔或掛載光碟的任何位置。這也視您下載的 ISO 影像檔而定。例如，Linux 位於 Identity_Manager_5_1_ 或 Identity_Manager_3_5_DVD.iso，而 AIX 和 Solaris 位於 Identity_Manager_1_3_Unix.iso 或 Identity_Manager_5_1_DVD.iso。_1_3_5_1

除非目前的工作目錄是安裝程式的所在目錄，否則安裝程式會找不到要安裝的套件。

4 選取安裝程式的執行語言，或使用預設的英文。輸入一個數字，按下 Enter。



5 檢視「歡迎」資訊，然後按 Enter 繼續安裝。



6 按 Enter 進入授權合約畫面，如果您同意使用條款，請輸入 Y。如果不同意，輸入 N 即可離開安裝程式。

```
===============================================================================
選擇安裝集
-----

請選取將由本安裝程式安裝的「安裝集」。

  ->1- Metadirectory 伺服器
    2- 已連接系統伺服器
    3- Web 型態管理伺服器

    4- 自訂...

針對所選「安裝集」輸入相應的號碼，或按一下 <ENTER> 接受預設值
      : 1
```

7 指定您要安裝之安裝集的適當號碼 (1-4)。安裝集包含下列元件：

- **1- Metadirectory 伺服器：**安裝 Metadirectory 引擎和服務驅動程式、Identity Manager 驅動程式、Novell Audit 代辦，並延伸 eDirectory 綱要。

  您必須先安裝 Novell eDirectory 8.8 和具有最新支援套件的 Security Services 2.0.5 (NMAS 3.1.3)，才能安裝此選項。如果沒有安裝這些項目，Identity Manager 安裝程序就會停止。

- **2- 已連接系統伺服器：**安裝 「遠端載入器」和這些驅動程式：Avaya、分隔文字、GroupWise、JDBC、JMS、LDAP、Linux/UNIX 設定、Linux/UNIX Bidirectional、Lotus Notes、PeopleSoft、RACF、Remedy、SAP、SIF、Top Secret 以及工作順序。*當您不想讓應用程式伺服器代管 eDirectory 服務和 Metadirectory 引擎時，可以選擇「已連接系統伺服器」選項。*

- **3- Web 型態的管理伺服器：**安裝 Identity Manager 外掛程式和 Identity Manager 驅動程式規則。

  必須先安裝 Novell iManager，才能安裝此選項。

  依預設，Identity Manager 驅動程式公用程式不會安裝在 Linux/UNIX 的安裝上。您必須從 Identity Manager 安裝光碟手動複製公用程式到 Identity Manager 伺服器。您可以在*平台的*\setup\utilities 目錄下找到所有公用程式。

- **4- 自訂：**安裝您從所有元件的清單中選取的特定元件。

您可以輸入 prev 返回先前的選單並修改您的安裝選項。

8 (選擇性) 是您選取的選項 (例如 Metadirectory 伺服器) 以及是否可執行 eDirectory v8.8 而定，系統會提示您設定 LD_LIBRARY_PATH 環境變數。若要執行此項操作，請執行

/opt/novell/eDirectory/bin/ndspath 程序檔，方法是輸入 ./opt/novell/eDirectory/bin/dspath，然後重新執行安裝。

9 如果您選取安裝「Metadirectory 伺服器」，則會提示您輸入輕量目錄存取協定 (LDAP) 使用者名稱 (CN=admin,O=novell) 和密碼。選取擁有足夠權限來延伸 eDirectory 綱要的使用者 (此人擁有網路樹根部的「監督者」權限，例如管理員)。

重要：(僅適用於 Solaris 安裝) 如果您在 eDirectory 存在的相同伺服器上安裝 Web 型態的管理伺服器，則當系統提示您輸入 Web 伺服器安全連接埠時，請將預設值變更爲某個可用的連接埠，例如 8443。

---

10 驗證摘要中所包含的資訊是否正確，然後按 Enter 開始安裝套件。

安裝「Metadirectory 引擎」和綱要檔案時，eDirectory 會暫時關閉。依預設，會安裝所有可用的驅動程式，因此稍後當您需要另一個驅動程式時便不必執行安裝程式。在已透過 iManager 或 Designer 設定驅動程式組態，並部署驅動程式之後，才會使用驅動程式檔案。

11 當您看到「安裝完成」頁面時，按 Enter 來關閉安裝程式。

4.8 使用主控台在 UNIX/Linux 上安裝已連結系統選項

第 4.7 節「使用主控台在 UNIX/Linux 平台上安裝 Identity Manager」(第 83 頁) 涵蓋 UNIX 平台上「Metadirectory 伺服器」、「Web 元件」和「公用程式」的安裝。此外，UNIX 或 Linux 伺服器可以使用「已連接系統」選項。

當您不想讓應用程式伺服器代管 eDirectory 服務和 Metadirectory 引擎時，請使用「已連接系統」選項。「遠端載入器」會透過 Identity Manager 提供所需的同步化，而無需載入可在其他位置存取的應用程式。

在您開始之前，請確定系統符合表格 1-3 (第 28 頁) 中列出的要求。

1 下載 Identity Manager。所需的 iso 影像檔。您可以下載 Identity Manager。iso 影像檔，來自 Novell 下載網站 (http://download.novell.com)。

例如，Linux 位於 Identity_Manager_5_1_ 或 Identity_Manager_3_5_DVD.iso，而 AIX 和 Solaris 位於 Identity_Manager_1_3_Unix.iso 或 Identity_Manager_5_1_DVD.iso。
_1_3_5_1

2 在主機電腦上，以根部身分登入。

3 執行設計目錄中的 bin 檔案。

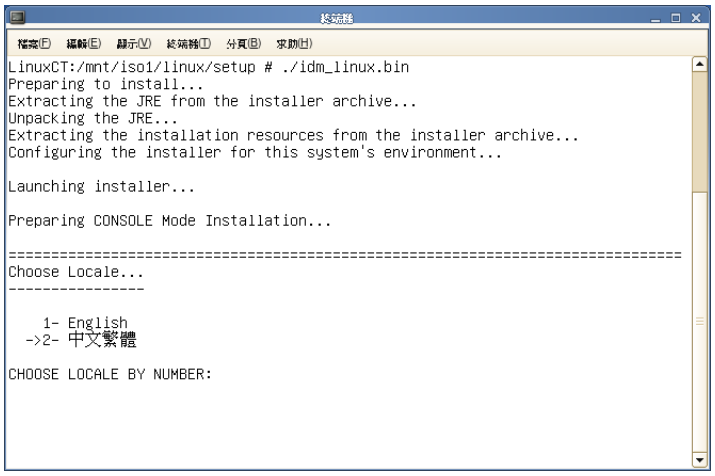
將目前的工作目錄變更爲安裝目錄，即安裝所在的位置。然後，輸入下列其中一個指令，以執行安裝：

平台	範例路徑	安裝檔案
Linux	linux/setup/	idm_linux.bin
Solaris	solaris/setup/	idm_solaris.bin
AIX	aix/setup/	idm_aix.bin

這些路徑是相對於安裝影像檔的根目錄，可以是您擴充該影像檔或裝上 CD 的任何位置。

除非目前的工作目錄是安裝程式的所在目錄，否則安裝程式會找不到要安裝的套件。

4 選取安裝程式的執行語言，或使用預設的英文。輸入一個數字，按下 Enter。



5 檢視 「歡迎」資訊，然後按 Enter 繼續安裝。

6 按 Enter 進入授權合約畫面，如果您同意使用條款，請輸入 Y。如果不同意，輸入 N 即可離開安裝程式。

7 指定號碼 2 以安裝 「已連接系統伺服器」。

安裝集包含「遠端載入器」和這些驅動程式：Avaya、分隔文字、GroupWise、JDBC、JMS、LDAP、Linux/Unix 設定、Linux/UNIX Bidirectional、Lotus Notes、PeopleSoft、RACF、Remedy、SAP、SIF、Top Secret 以及工作順序。

8 檢視「預先安裝摘要」畫面中列出的項目。按 Enter 安裝元件。

依預設，會安裝所有可用的驅動程式，因此稍後當您需要另一個驅動程式時便不必執行安裝程式。在已透過 iManager 或 Designer 設定驅動程式組態，並部署驅動程式之後，才會使用驅動程式檔案。

依預設，Identity Manager 驅動程式公用程式不會安裝在 Linux/UNIX 的安裝上。您必須從 Identity Manager 安裝光碟手動複製公用程式到 Identity Manager 伺服器。您可以在*平台的*\setup\utilities 目錄下找到所有公用程式。

9 當您看到「安裝完成」頁面時，按 Enter 來關閉安裝程式。

4.9 Identity Manager 的 Non-root 安裝

這個版本的 Identity Manager 可讓您將 Identity Manager Metadirectory 引擎安裝在 eDirectory 的 Non-root 安裝中。

您必須先安裝 Novell 和具有最新修補程式的 Security Services 3.1.3 (NMAS 8.8)，才能安裝此選項。如需以 non-root 使用者身分安裝 NICI 的詳細資訊，請參閱「*Novell eDirectory 8.8 安*

裝指南」一書中「*3.0 在 Linux 安裝或升級 Novell eDirectory*」標題下的「安裝 NICI (http://www.novell.com/documentation/edir88/index.html)」小節。

安裝 NICI 後，請按照 non-root eDirectory 8.8 的安裝指示進行，該指示位於 「*Novell eDirectory 8.8 安裝指南*」一書中「*3.0 在 Linux 安裝或升級 Novell eDirectory*」標題下的「Nonroot 使用者安裝 eDirectory 8.8 (http://www.novell.com/documentation/edir88/index.html)」小節。

1 下載 Identity Manager。所需的 iso 影像檔。您可以下載 Identity Manager。iso 檔，來自 Novell 下載網站 (http://download.novell.com)。

   例如，Linux 位於 Identity_Manager_5_1_ 或 Identity_Manager_3_5_DVD.iso，而 AIX 和 Solaris 位於 Identity_Manager_1_3_Unix.iso 或 Identity_Manager_5_1_DVD.iso。_1_3_5_1 non-root 安裝程式位於 . iso 影像。

2 在主機電腦上，以具有安裝在 Non-root eDirectory 中目錄其寫入權限的使用者身分登入。

3 執行 /setup/ 目錄中的 idm-nonroot-install 檔案。若要如此，請將目前工作目錄變更爲 setup 目錄，再輸入以下指令執行 Non-root 安裝：

   ./idm-nonroot-install

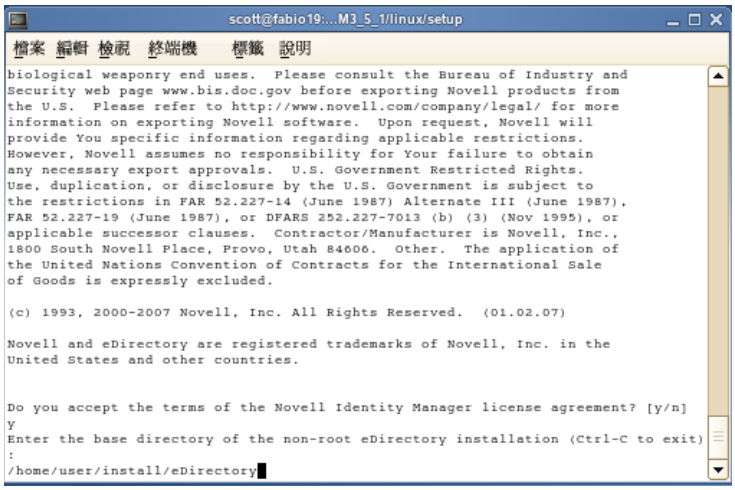
平台	範例路徑	安裝檔案
Linux	linux/setup/	idm-nonroot-install
Solaris	solaris/setup/	idm-nonroot-install
AIX	aix/setup/	idm-nonroot-install

   這些路徑與 iso 影像根部相關，且安裝程式找不到要安裝的套件，除非目前的工作目錄是安裝程式所在的目錄。

4 按下 Enter 會帶出一般使用者授權合約，再按下空白鍵可捲動整個合約。如果您同意使用條款，則輸入 Y。如果不同意，輸入 N 即可離開安裝程式。

5 輸入指向 Non-root eDirectory 目錄的路徑。例如：

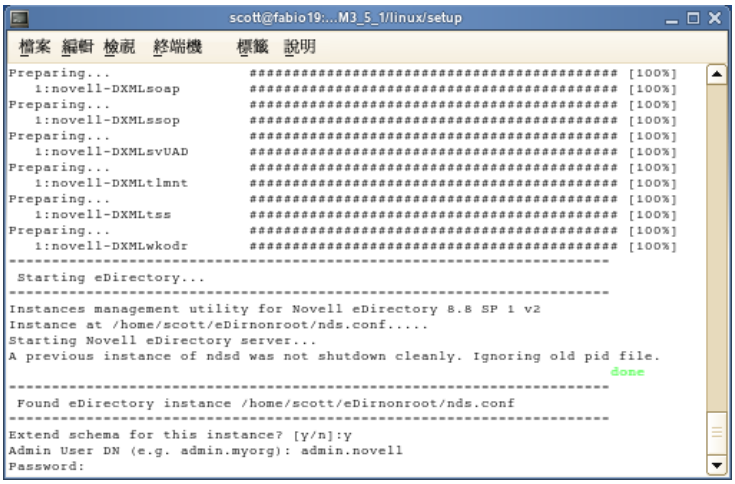
   /home/user/installed/eDirectory



安裝集包含「遠端載入器」和這些驅動程式：Avaya、分隔文字、GroupWise、JDBC、JMS、LDAP、Linux/Unix 設定、Linux/UNIX Bidirectional、Lotus Notes、PeopleSoft、RACF、Remedy、SAP、SIF、Top Secret 以及工作順序。

6 接下來會要求您展開登入使用者所擁有的每個 eDirectory 例項其綱要。對於每個例項，輸入 Y 可展開該例項的綱要，如果您不要展開該例項的綱要，則輸入 N。

7 如果您要選擇展開綱要，請輸入有權限展開綱要之使用者的可辨識名稱 (例如 admin.novell)。選取擁有足夠權限來延伸 eDirectory 綱要的使用者 (此人擁有網路樹根部的「監督者」權限，例如管理員)。



8 輸入密碼和按下 Enter。您必須爲每個您展開的 eDirectory 例項執行步驟 7 和 8。

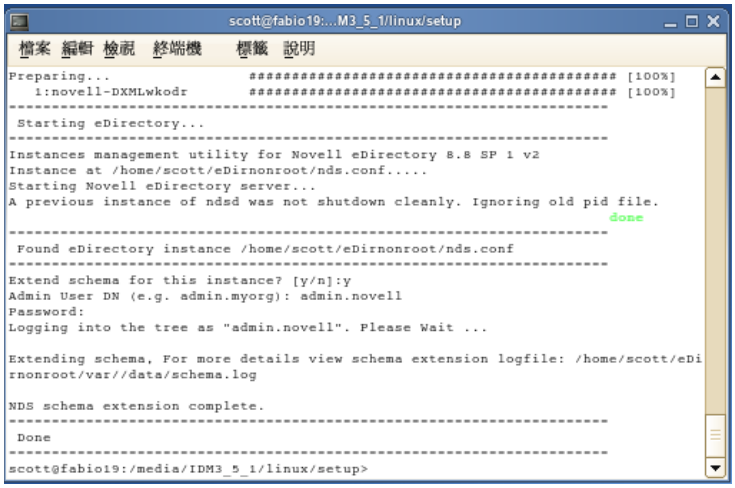
如果您日後要展開其他 eDirectory 例項的綱要，請執行 non-root eDirectory 其 opt/novell/eDirectory/bin 子目錄的 idm-nonroot-install 指令碼。以您要展開 eDirectory 例項的擁有者身分登入，再執行指令碼。

安裝指令碼會記錄在 eDirectory 樹狀目錄，並展開綱要。如果您要綱要展開程序的詳細資訊，請移至 /home/user/eDirnonroot/var/data/schema.log 檔案。

依預設，會安裝所有可用的驅動程式，因此稍後當您需要另一個驅動程式時便不必執行安裝程式。在已透過 iManager 或 Designer 設定驅動程式組態，並部署驅動程式之後，才會使用驅動程式檔案。

依預設，Identity Manager 驅動程式公用程式不會安裝在 Linux/UNIX 的安裝上。您必須從 Identity Manager 安裝光碟手動複製公用程式到 Identity Manager 伺服器。您可以在*平台的*\setup\utilities 目錄下找到所有公用程式。

9 完成網要展開時，便會安裝 Identity Manager。



4.10 安裝後任務

您不需手動載入或卸載 Identity Manager，因爲 Identity Manager 模組會在 Identity Manager 驅動程式啓動時載入。如果其中一個驅動程式的參數設定爲「自動啓動」，且該驅動程式和 eDirectory 正在執行中，則驅動程式會自動啓動 Identity Manager 模組。如果驅動程式的其中一個參數設定爲「手動」，則 Identity Manager 模組會在您啓動 Identity Manager 驅動程式時載入。

安裝 Identity Manager 後，您必須設定所安裝的驅動程式，來實作您定義爲業務程序的規則和需求。安裝後任務通常包含下列項目：

- 設定已連結系統。如需驅動程式特定的組態指示，請參閱「Identity Manager 驅動程式文件 (http://www.novell.com/documentation/dirxmldrivers)」。
- 建立和設定驅動程式。使用 iManager 或 Designer 公用程式來建立驅動程式或設定現有的驅動程式。請參閱《*Designer 2.1 for Identity Manager 3.5.1*》指南中的「匯入驅動程式組態檔案」。
- 定義規則。使用 iManager 或 Designer 公用程式來定義規則，讓驅動程式符合您的業務需求。請參閱《*Designer 2.1 的規則*》指南中的「建立規則」，或參閱《*瞭解 Identity Manager 3.5.1 的規則*》指南。
- 啓動、停止或重新啓動驅動程式。使用 iManager 或 Designer 公用程式來管理驅動程式的活動。請參閱《*Designer 2.1 for Identity Manager 3.5.1*》指南中的「匯入驅動程式組態檔案」。
- 啓用 Identity Manager。請參閱第 6 章 「啓用 Novell Identity Manager 產品」(第 171 頁)。

4.11 安裝自訂驅動程式

自訂驅動程式可能由下列項目組成：

- 一組 .jar 或原始 (. dll、. nlm 或 . so) 檔案
- 用於設定驅動程式組態的 XML 規則檔案
- 文件

如需建立自訂驅動程式或安裝驅動程式的相關資訊，請參閱 Novell 開發人員套件 (http://developer.novell.com/ndk/dirxml-index.htm)。亦請參閱 《*Novell Identity Manager 3.5.1 管理指南*》中的 「編輯驅動程式組態檔案」。

安裝「使用者應用程式」

5

本節說明如何安裝「Identity Manager 使用者應用程式」。主題包括：

5.1 安裝的先決條件

在安裝「Identity Manager 使用者應用程式」之前，請先驗證是否符合下列要求：

表格 5-1 *安裝必要條件*

環境要求	描述
Java* 開發套件	下載並安裝「Java 2 開發平台標準版套件 5.0」。使用 JRE 1.5.0_10 版。在 WebSphere 上，以套用未限制規則檔案的方式，使用 IBM* JDK*。 將 JAVA_HOME 環境變數設定爲指向 JDK* 來和「使用者應用程式」搭配使用。或者，在安裝「使用者應用程式」時手動指定來覆寫 JAVA_HOME。 ◆ 在 Linux 或 Solaris 指令提示下，輸入 echo $JAVA_HOME。若要建立或變更 JAVA_HOME，請建立或編輯 ~/.profile (位於 SUSE Linux)： # Java Home export JAVA_HOME=/usr/java/jdk1.5.0_10 #JRE HOME export JRE_HOME=$JAVA_HOME/jre ◆ 在 Windows，請檢視「*控制台* > *系統* > *進階* > *環境變數* > *系統變數*」。

環境要求	描述
JBoss 應用程式伺服器	如果您正在使用 JBoss，請下載並安裝 JBoss 4.2.0 Application Server。(請在安裝「使用者應用程式」後啓動此伺服器。請參閱第 5.9 節「安裝後任務」(第 164 頁))。 **RAM:** 執行「使用者應用程式」時，建議使用之應用程式伺服器的最低 RAM 是 512 MB。 **埠：**請記錄應用程式伺服器所使用的連接埠 (應用程式伺服器的預設爲 8080)。) **SSL:** 如果您計畫使用外部的密碼管理，則請在您部署「使用者應用程式」和 IDMPwdMgt.war 檔案的 JBoss 伺服器上啓用 SSL。如需相關指示，請參閱 JBoss 文件。此外，也請確定 SSL 連接埠在您的防火牆上開啓。如需有關 IDMPwdMgt.war 檔案的詳細資訊，請參閱第 5.9.4 節「存取外部密碼 WAR」(第 166 頁) 以及《*IDM 3.5.1 使用者應用程式：管理指南*》。(http://www.novell.com/documentation/idm35/index.html)
WebSphere 應用程式伺服器	如果您正在使用 WebSphere，請下載並安裝 WebSphere 6.1 Application Server。
啓用 iChain Logout	您可以啓用 iChain® 或 Novell Access Manager™ 中的「Cookie 轉遞」選項，來啓用「Identity Manager 使用者應用程式」中的 ICS Logout。
資料庫	安裝資料庫和資料庫驅動程式，並建立資料庫或資料庫例項。請將主機和連接埠記錄下來，您會在第 5.5.7 節「指定資料庫主機和連接埠」(第 115 頁) 中用到。將資料庫名稱、使用者名稱和使用者密碼記錄下來，您會在第 5.5.8 節「指定資料庫名稱和特權使用者」(第 116 頁) 中用到。 資料來源檔案必須指向資料庫。處理方式會視您的應用程式伺服器而不同。「使用者應用程式」安裝程式會建立一個應用程式伺服器資料來源檔案來指向此資料庫，並根據「使用者應用程式」的 WAR 檔案來命名該檔案。對於 WebSphere，先手動設定資料來源，再進行安裝。 必須爲 UTF-8 啓用資料庫。 不論您是透過「IDM 使用者應用程式」還是靠自己來安裝 MySQL，請都參閱第 5.1.3 節「設定您的 MySQL 資料庫」(第 98 頁)。 **附註：**如果您計畫移轉某個資料庫，請先啓動該資料庫，然後才在安裝程式中選取移轉選項。如果您不想移轉資料庫，資料庫就不需要在「使用者應用程式」安裝時執行。只要在啓動「 應用程式伺服器」之前啓動資料庫即可。
如果在 Linux 或 Solaris 上安裝「IDM 3.5.1 使用者應用程式」	預設的安裝位置爲 /opt/novell/idm 您可以在安裝程序中選取其他的預設安裝目錄。確定該目錄存在，並可由 non- root 使用者寫入。
如果在 Windows 上安裝「IDM 3.5.1 使用者應用程式」	**安裝目錄。**預設的安裝位置爲 C:\Novell\IDM。請確定此目錄存在，並且可寫入。您可以在安裝程序中選取其他的預設安裝目錄。
Identity Manager 3.5.1	您必須先安裝 Identity Manager 3.5.1 的 Metadirectory 伺服器，才能建立「使用者應用程式」驅動程式並安裝「使用者應用程式」。
「使用者應用程式」驅動程式	在您安裝「使用者應用程式」之前，「使用者應用程式」驅動程式必須先存在 (但是不能啓用)。

環境要求	描述
Identity Vault 存取	「使用者應用程式」需要使用者對將使用 「使用者應用程式」的網路位置，擁有管理員權限。
IDM 「使用者應用程式」儲存	安裝「使用者應用程式」的電腦必須至少擁有 320 MB 的可用儲存空間。

如果您已經驗證所有先決條件，請遵照下列各節的安裝指示執行：

- 第 5.1.1 節 「安裝 JBoss 應用程式伺服器和 MySQL 資料庫」 (第 95 頁)
- 第 5.1.2 節 「將 「JBoss 應用程式伺服器」安裝爲服務」 (第 97 頁)
- 第 5.1.3 節 「設定您的 MySQL 資料庫」 (第 98 頁)

5.1.1 安裝 JBoss 應用程式伺服器和 MySQL 資料庫

使用 JbossMysql 公用程式在您的系統上安裝 「JBoss 應用程式伺服器」和 MySQL。

此公用程式無法將 「JBoss 應用程式伺服器」安裝爲 Windows 服務。若要將 「JBoss 應用程式伺服器」安裝爲 Windows 系統上的服務，請參閱第 5.1.2 節 「將 「JBoss 應用程式伺服器」安裝爲服務」 (第 97 頁)。

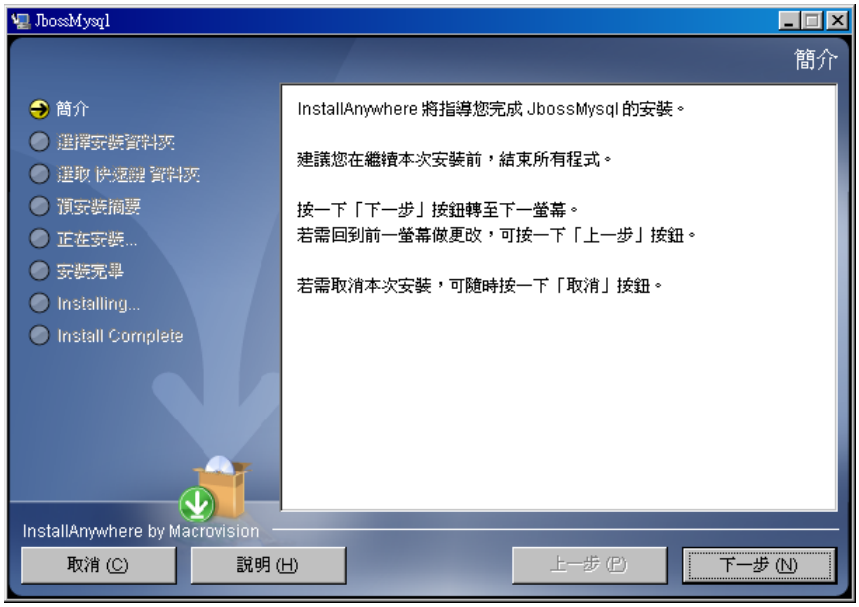
1 找出並執行 JbossMysql.bin 或 JbossMysql.exe。您可以找到這個與 「使用者應用程式」安裝程式繫結的公用程式，該安裝程式位於

/linux/user_application (Linux)
/nt/user_application (Windows)

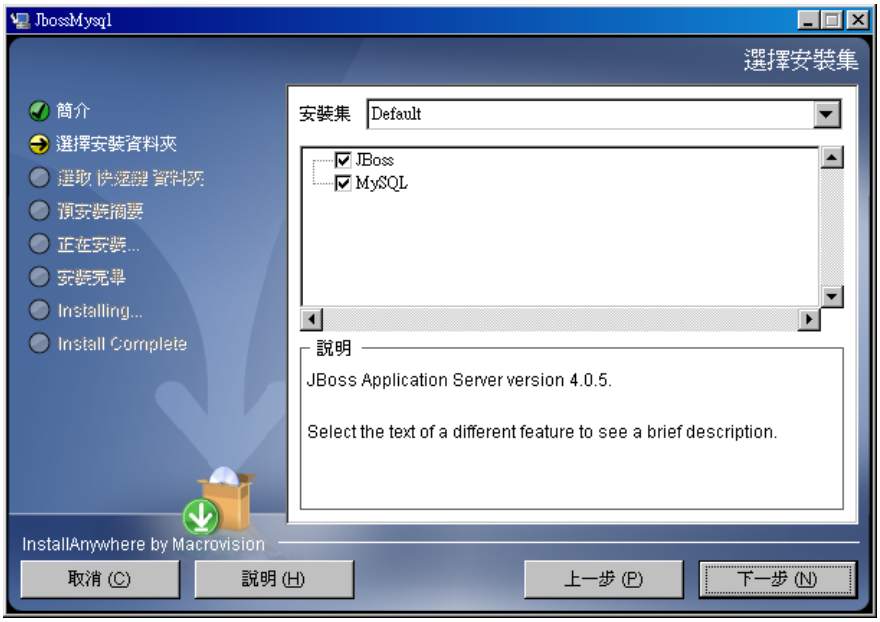
未提供 Solaris 的公用程式。

2 選取您的地區設定。

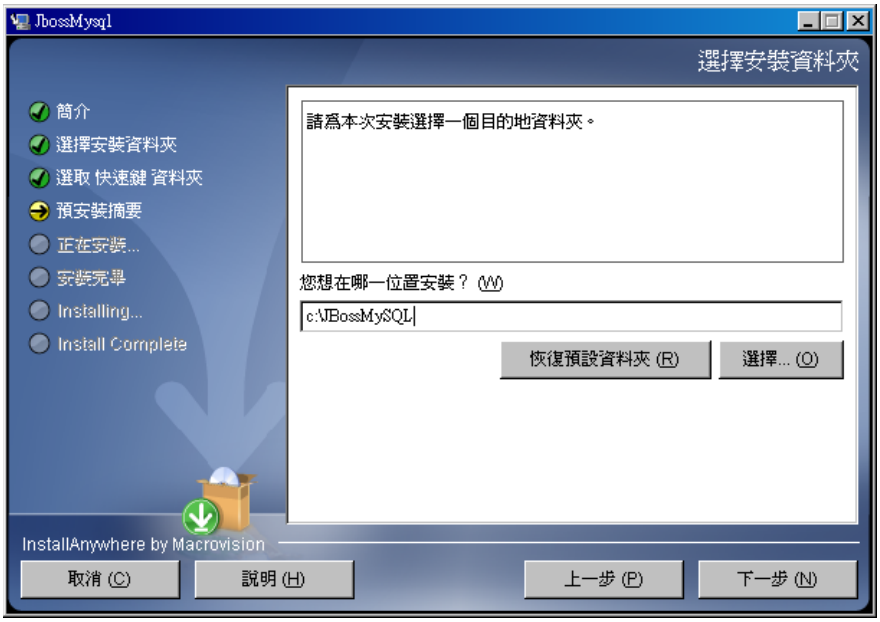
3 請閱讀簡介頁面，然後按一下 「 *下一步*」。



4 選取您要安裝的產品，然後按一下「*下一步*」。

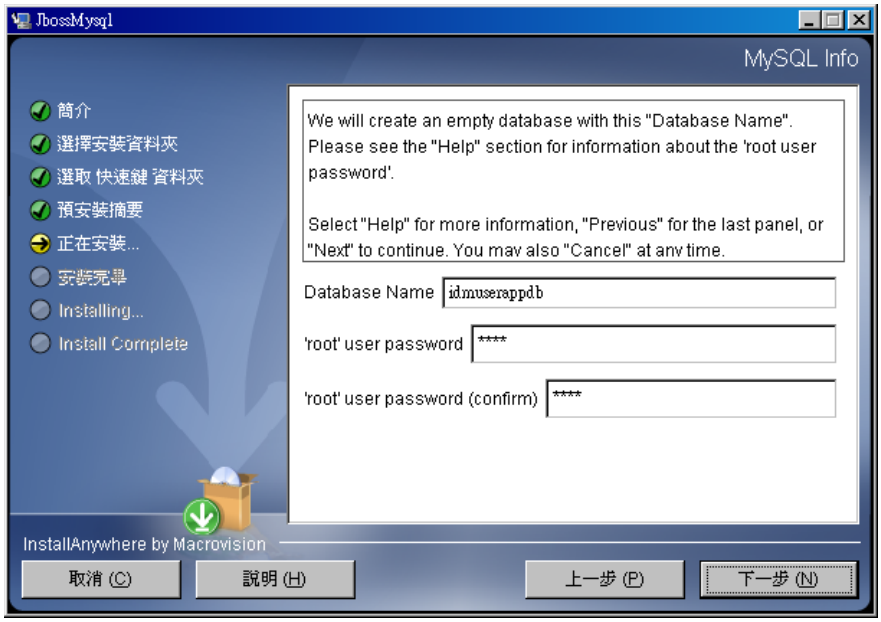


5 按一下「*選擇*」來選取基礎資料夾，選取的產品將安裝在該資料夾內，然後按一下「*下一步*」。



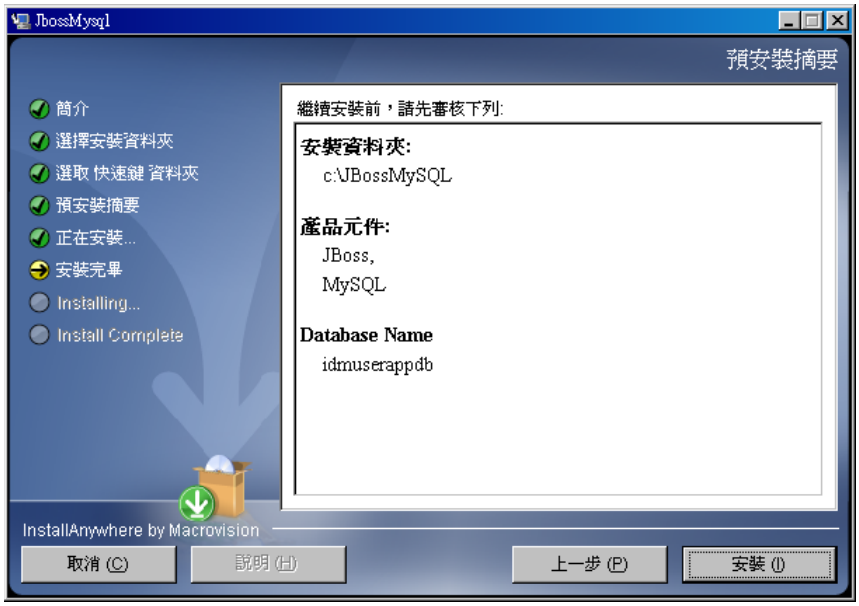
6 指定您資料庫的名稱。「使用者應用程式」安裝需要這個名稱。

7 指定資料庫根部使用者的密碼。



8 按一下「下一步」。

9 在「預先安裝摘要」中檢閱您的指定項目，然後按一下「*安裝*」。



在安裝完您選取的產品之後，公用程式會顯示安裝成功的訊息。如果您有安裝 MySQL 資料庫，請繼續前往第 5.1.3 節 「設定您的 MySQL 資料庫」 (第 98 頁)。

5.1.2 將「JBoss 應用程式伺服器」安裝爲服務

若要以服務的方式執行 JBoss Application Server，請使用 Java Service Wrapper 或協力廠商的公用程式。請至 http://wiki.jboss.org/wiki/Wiki.jsp?page=RunJBossAsAServiceOnWindows

(http://wiki.jboss.org/wiki/Wiki.jsp?page=RunJBossAsAServiceOnWindows)，參閱 JBoss 的指示。

- 「使用 Java Service Wrapper」(第 98 頁)
- 「使用協力廠商的公用程式」(第 98 頁)

使用 Java Service Wrapper

您可以使用 Java Service Wrapper 來安裝、啓動和停止 Windows 身分的「JBoss 應用程式伺服器」，或 Linux 或 UNIX 精靈程序。請檢查網際網路上是否有可用的公用程式和下載網站。

這類 wrapper 位於 http://wrapper.tanukisoftware.org/doc/english/integrate-simple-win.html (http://wrapper.tanukisoftware.org/doc/english/integrate-simple-win.html)，由 JMX 管理 (請參閱 http://wrapper.tanukisoftware.org/doc/english/jmx.html#jboss (http://wrapper.tanukisoftware.org/doc/english/jmx.html#jboss))。以下爲一些範例組態檔案：

wrapper.conf :

wrapper.java.command=%JAVA_HOME%/bin/java

wrapper.java.mainclass=org.tanukisoftware.wrapper.WrapperSimpleApp

wrapper.java.classpath.1=%JBOSS_HOME%/server/default/lib/wrapper.jar

wrapper.java.classpath.2=%JAVA_HOME%/lib/tools.jar wrapper.java.classpath.3=./run.jar

wrapper.java.library.path.1=%JBOSS_HOME%/server/default/lib wrapper.java.additional.1=-server wrapper.app.parameter.1=org.jboss.Main wrapper.logfile=%JBOSS_HOME%/server/default/log/wrapper.log wrapper.ntservice.name=JBoss wrapper.ntservice.displayname=JBoss Server

---

警告：您必須正確設定您的 JBOSS_HOME 環境變數。wrapper 不會自行設定這個變數。

---

java-service-wrapper-service.xml : <Xxml version="1.0" encoding="UTF-8"?><!DOCTYPE server><server> <mbean code="org.tanukisoftware.wrapper.jmx.WrapperManager" name="JavaServiceWrapper:service=WrapperManager"/> <mbean code="org.tanukisoftware.wrapper.jmx.WrapperManagerTesting" name="JavaServiceWrapper:service=WrapperManagerTesting"/></server

使用協力廠商的公用程式

對於舊版，您可以使用協力廠商的公用程式，例如 JavaService，以安裝、啓動和停止 JBoss Application Server 成爲 Windows 服務。

警告：JBoss 不再建議使用 JavaService。如需詳細資訊，請參閱 http://wiki.jboss.org/wiki/Wiki.jsp?page=JavaService (http://wiki.jboss.org/wiki/Wiki.jsp?page=JavaService)。

5.1.3 設定您的 MySQL 資料庫

您必須設定 MySQL 組態設定，使 MySQL 和 Identity Manager 3.5.1 搭配運作。如果您自行安裝 MySQL，就必須自行爲其進行設定。如果您使用 JbossMysql 公用程式來安裝 MySQL，則公用程式會爲您設定正確的值，但您必須知道那些值是什麼，才能維護下列項目：

- 「字元集」(第 99 頁)

- 「INNODB 存放引擎和表格類型」(第 99 頁)
- 「區分大小寫」(第 99 頁)

字元集

指定 UTF-8 做爲整個伺服器或只有資料庫的字元集。將下列選項納入 my.cnf (Linux 或 Solaris) 或 my.ini (Windows)，以涵蓋整個伺服器的基礎來指定 UTF-8：

character-set-server=utf8 或

在資料庫建立期間，使用下列指令來指定資料庫的字元集：

create database databasename character set utf8 collate utf8_bin;

如果您爲資料庫設定資源集，則也必須在 IDM-ds.xml 檔案的 JDBC URL 中設定字元集，如：

<connection-url>jdbc:mysql://localhost:3306/databasename?useUnicode=true&characterEncoding

INNODB 存放引擎和表格類型

「使用者應用程式」使用了 INNODB 存放引擎，可讓您爲 MySQL 選擇 INNODB 表格類型。如果您建立 MySQL 表格時沒有指定其表格類型，該表格就會預設使用 MyISAM 表格類型。如果您選擇從 Identity Manager 安裝程序安裝 MySQL，則該程序產生的 MySQL 會指定使用 INNODB 表格類型。若要確保您的 MySQL 伺服器使用 INNODB，請確認 my.cnf (Linux 或 Solaris) 或 my.ini (Windows) 包含下列選項：

default-table-type=innodb

不應該包含 skip-innodb 選項。

區分大小寫

如果您打算備份和還原伺服器或平台之間的資料，則請確定各伺服器和各平台之間都一致地區分大小寫。若要確保一致性，請在您所有的 my.cnf (Linux 或 Solaris) 或 my.ini (Windows) 檔案中爲 lower_case_table_names 指定相同的值 (0 或 1)，而不要接受預設值 (Windows 預設爲 0、Linux 預設爲 1)。請先指定這個值，再建立資料庫來存放 Identity Manager 表格。例如，您可以針對所有想在其上備份和還原資料庫的平台，指定

lower_case_table_names=1

(在 my.cnf 和 my.ini 檔案中)。

5.2 安裝和組態

1. 建立「使用者應用程式」並在結束時將其關閉。

   此步驟可在 Identity Vault 中建立新物件。某些物件將擁有預設的資料值 如需相關資訊，請參閱第 5.3 節 「建立「使用者應用程式」驅動程式」(第 100 頁)。

2. 執行「使用者應用程式」安裝程式。

   如需更多資訊，請參閱第 5.5 節 「從安裝 GUI 將「使用者應用程式」安裝在 JBoss 應用程式伺服器上」(第 107 頁) 或第 5.6 節 「將「使用者應用程式」安裝在 WebSphere 應用程式伺服器上」(第 133 頁)。

WebSphere 使用者必須手動部署 WAR 檔案。

重要：進行「Identity Manager 使用者應用程式」的安裝時，「使用者應用程式」驅動程式必須先存在，才能安裝應用程式。不過，請在安裝「Identity Manager 使用者應用程式」*之後*啓動驅動程式，否則「使用者應用程式」可能會傳回錯誤。

5.3 建立「使用者應用程式」驅動程式

除了叢集上的「使用者應用程式」不這麼做以外，您必須爲各個「使用者應用程式」建立個別的「使用者應用程式」驅動程式。屬於同一個 叢集的各個「使用者應用程式」必須共用同一個「使用者應用程式」驅動程式。如需執行叢集中的「使用者應用程式」的詳細資訊，請參閱《*Identity Manager 3.5.1 使用者應用程式管理指南*》。(http://www.novell.com/documentation/idm35/index.html)

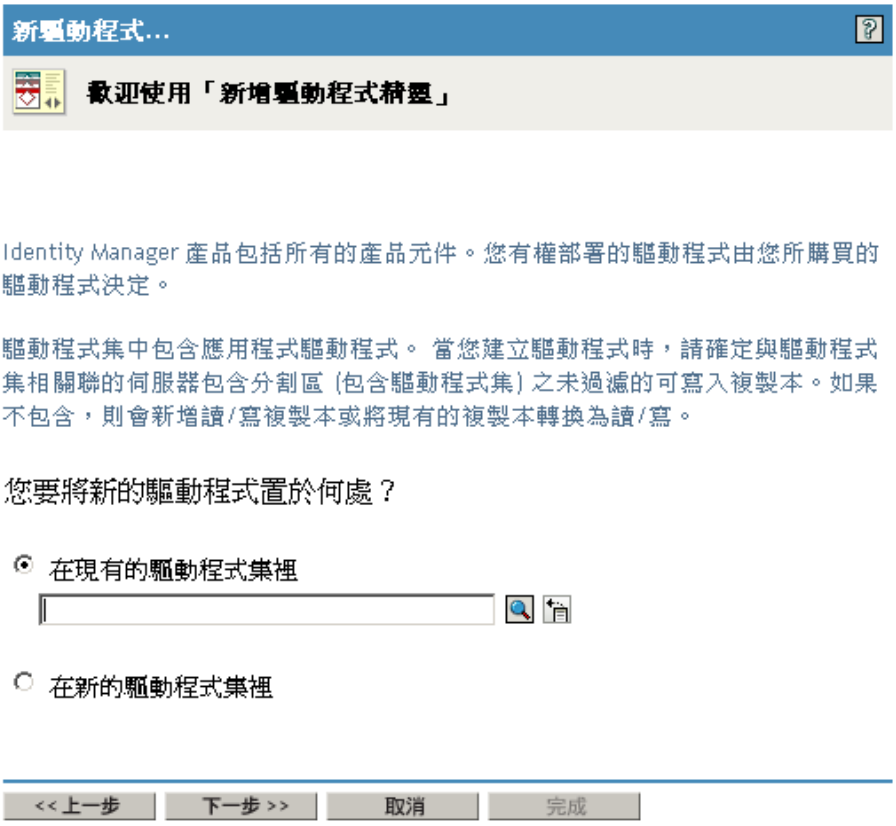
「使用者應用程式」會在驅動程式中存放應用程式的特定資料，來控制和設定應用程式環境。這包含「 應用程式伺服器」資訊和工作流程引擎組態。

重要：若設定一組非叢集的「使用者應用程式」來共用同一個驅動程式，這對在「使用者應用程式」中執行的一個或多個元件來說，可能會對它們造成混淆和設定錯誤。這些錯誤的來源很難偵測出來。

若要建立「使用者應用程式」驅動程式，並將其與驅動程式集相關聯：

1 使用 iManager 登入 Identity Vault (如果您尚未執行此操作的話)。

2 移至「*角色和任務* > *Identity Manager 公用程式*」，並選取「*新驅動程式*」來啓動「建立驅動程式精靈」。

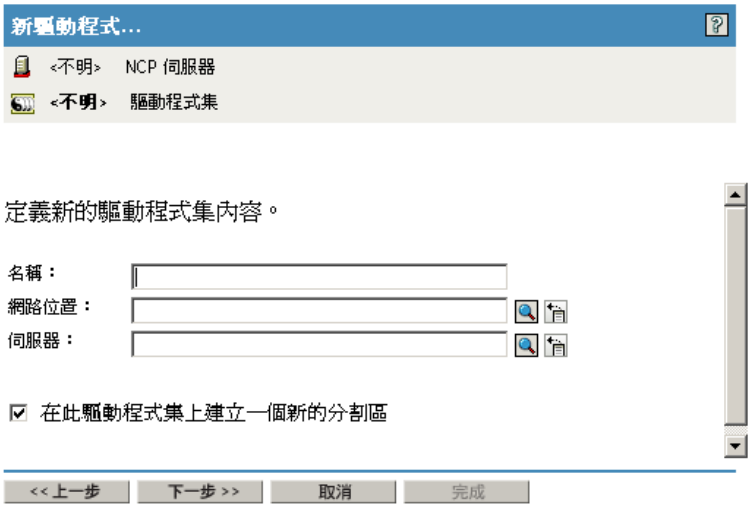


3 若要在現有的驅動程式集中建立驅動程式，選取「*在現有的驅動程式集裡*」，按一下物件選擇器圖示，選取驅動程式集物件，按一下「*下一步*」並繼續進行步驟 4。

或

如果您需要建立新的驅動程式集 (例如，如果您想將「使用者應用程式」驅動程式放在與其他驅動程式所在的不同伺服器上)，請選取「*在新的驅動程式集裡*」，按一下「*下一步*」，然後定義新驅動程式集的內容。

3a 請爲新的驅動程式集指定名稱、網路位置和伺服器。



3b 按一下「下一步」。

4 核取「*從伺服器 (.XML 檔案) 輸入驅動程式組態*」。

5 從下拉式清單選取 *UserApplication.xml*。

這是新驅動程式的組態檔案。

6 按一下「下一步」。

如果 *UserApplication.xml* 未列在此下拉式清單中，則您可能沒有執行 Identity Manager 3.5.1 安裝的「Web 型態的管理伺服器」部分。

7 系統會提示您輸入驅動程式的參數 (請捲動畫面檢視全部)。將各個參數記錄下來，您會在安裝「使用者應用程式」時用到。

欄位	描述
驅動程式名稱	您建立之驅動程式的名稱。
認證資訊 ID	「使用者應用程式管理員」的可辨識名稱。這是「使用者應用程式管理員」，您將對其賦予權限管理「使用者應用程式」入口網站。使用 eDirectory™ 格式 (例如 admin.orgunit.novell) 或瀏覽尋找使用者。這是必要欄位。
密碼	「認證資訊 ID」中指定的「使用者應用程式管理員」密碼。
應用程式網路位置	「使用者應用程式」網路位置。這是「使用者應用程式」WAR 檔案 URL 的網路位置部分。預設爲：IDM。
主機	部署「Identity Manager 使用者應用程式」之應用程式伺服器的主機名稱或 IP 位址。 如果執行叢集，請輸入發送器的主機名稱或 IP 位址。
連接埠	您在上方所列之主機的連接埠。
允許覆寫起始者： (值爲「是 / 否」)	*選取「是」可允許「提供管理員」以其所代理之人的名義，啓動工作流程。*

8 按「*下一步*」。

9 按一下「*定義安全性等值*」，以開啓「安全性相等」視窗。瀏覽並選取管理員或其他「監督者」物件，然後按一下「*新增*」。

此步驟提供給驅動程式所需的安全性權限。在 Identity Manager 文件中，可以找到關於此步驟重要性的詳細資訊。

10 (選擇性，但建議使用) 按一下「*排除管理者角色*」。

11 按一下「*新增*」，選取您想排除在驅動程式動作之外的使用者 (例如管理者角色)。

12 按兩次「*確定*」，然後按一下「*下一步*」。

13 按一下「*確定*」，以關閉「安全性相等」視窗並顯示摘要頁面。

14 如果資訊正確，按一下「*完成*」或「*完成概觀*」。

重要：此驅動程式預設爲關閉。讓驅動程式保持「關閉」，直到已安裝「使用者應用程式」爲止。

5.4 關於安裝程式

「使用者應用程式」的安裝程式會：

- 指定現有的應用程式伺服器版本，以供使用。
- 指定現有的資料庫版本，以供使用，例如 MySQL、Oracle 或 Microsoft SQL Server。資料庫可存放「使用者應用程式」資料和「使用者應用程式」組態資訊。
- 設定 JDK 的證書檔案組態，以便「使用者應用程式」(在應用程式伺服器上執行) 可以安全地與 Identity Vault 和「使用者應用程式」驅動程式通訊。
- 設定並部署「Novell Identity Manager 使用者應用程式」的 Java Web Application Archive (WAR) 檔案至「JBoss 應用程式伺服器」。
- 依您的意願啓用 Novell Audit 記錄。
- 讓您輸入現有的萬能金鑰來還原特定的「使用者應用程式」安裝，並支援叢集。

- 第 5.4.1 節「安裝程序檔和可執行檔」(第 106 頁)
- 第 5.4.2 節「安裝所需的值」(第 106 頁)

您可以使用下列三種模式來啓動安裝程式：

- 圖形使用者介面。請參閱第 5.5 節「從安裝 GUI 將「使用者應用程式」安裝在 JBoss 應用程式伺服器上」(第 107 頁)。
- 主控台 (指令行) 介面。請參閱第 5.7 節「從主控台介面安裝使用者應用程式」(第 159 頁)。
- 無訊息安裝。請參閱第 5.8 節「使用單一指令安裝使用者應用程式」(第 159 頁)。

5.4.1 安裝程序檔和可執行檔

透過下列其中一種方式來取得 Identity Manager 3.5.1 安裝檔案：

- 依您的系統下載正確的 「使用者應用程式」.iso 影像檔或 .zip 檔案：Identity_Manager_1_3_User_Application.iso 或 Identity_Manager_5_1_User_Application_Provisioning.iso。_5_1 下載檔案位於 Novell 下載 (http://download.novell.com/index.jsp)。
- 從 Novell, Inc. 下載產品 DVD：Identity_Manager_5_1_DVD.iso。_1

表格 5-2 列出您在安裝 「Identity Manager 3.5.1 使用者應用程式」時所需的檔案和程序檔。

表格 5-2 *安裝 Identity Manager 3.5.1 使用者應用程式時所需的檔案和程序檔*

檔案	描述
使用者應用程式 WAR	選擇一個： **IDM.war**。包含具有 「身分自助服務」功能的 「Identity Manager 3.5.1 使用者應用程式」。 **IDMProv.war**。包含 「Identity Manager 3.5.1 使用者應用程式」，以及 「身分自助服務」功能和 「提供模組」。

系統的 WAR 檔、IdmUserApp.jar 和 silent.properties 檔位於光碟內適用您系統的目錄中：

/linux/user_application (Linux)
/nt/user_application (Windows)
/solaris/user_application (Solaris)

5.4.2 安裝所需的值

表格 5-3 是一張工作表，用來記錄您想在安裝時使用的安裝參數。「使用者應用程式」組態參數也可以在安裝時設定，請參閱第 5.5.14 節 「設定使用者應用程式組態」 (第 122 頁)。

表格 5-3 *安裝參數工作表 針對 JBoss：*

參數	範例值	您的值
安裝資料夾	C:\IDM\IDMinstallIocation	
資料庫平台	MySQL	
資料庫主機	localhost	
資料庫連接埠	3306	
資料庫名稱或 SID	IDM	
資料庫使用者	根部 (除了 root directory，root partition 和 root object 外)	
資料庫使用者密碼		

參數	範例值	您的值
Java 根資料夾	C:\Java\jdk1.5.0_10\	
(JBoss) 基礎資料夾	C:\jboss	
JBoss 主機	localhost	
JBoss 連接埠	8080	
工作流程引擎 ID (用於叢集安裝。每個叢集成員擁有的都必須是唯一的。)		
應用程式名稱 (URL 網路位置)	IDM	
Novell Audit 伺服器	(名稱或 IP 位址)	
加密的萬能金鑰。請參閱第 5.5.13 節「指定萬能金鑰」(第 121 頁)。	_+FEJEefMAglH0A= =:3VRmp04lub21Y3GpdaXCY)LG qS1nBaL/	

5.5 從安裝 GUI 將「使用者應用程式」安裝在 JBoss 應用程式伺服器上

本節說明如何使用安裝程式的圖形使用者介面來安裝「Identity Manager 使用者應用程式」。

- 第 5.5.1 節「啓動安裝程式 GUI」(第 107 頁)
- 第 5.5.2 節「選擇應用程式伺服器平台」(第 109 頁)
- 第 5.5.3 節「移轉您的資料庫」(第 109 頁)
- 第 5.5.4 節「指定 WAR 的位置」(第 111 頁)
- 第 5.5.5 節「選擇安裝資料夾」(第 111 頁)
- 第 5.5.6 節「選擇資料庫平台」(第 113 頁)
- 第 5.5.7 節「指定資料庫主機和連接埠」(第 115 頁)
- 第 5.5.8 節「指定資料庫名稱和特權使用者」(第 116 頁)
- 第 5.5.9 節「指定 Java 根目錄」(第 117 頁)
- 第 5.5.10 節「指定 JBoss 應用程式伺服器設定」(第 117 頁)
- 第 5.5.11 節「選擇應用程式伺服器組態類型」(第 119 頁)
- 第 5.5.12 節「啓用 Novell Audit 記錄」(第 120 頁)
- 第 5.5.13 節「指定萬能金鑰」(第 121 頁)
- 第 5.5.14 節「設定使用者應用程式組態」(第 122 頁)
- 第 5.5.15 節「確認選擇並安裝」(第 133 頁)
- 第 5.5.16 節「檢視記錄檔案」(第 133 頁)

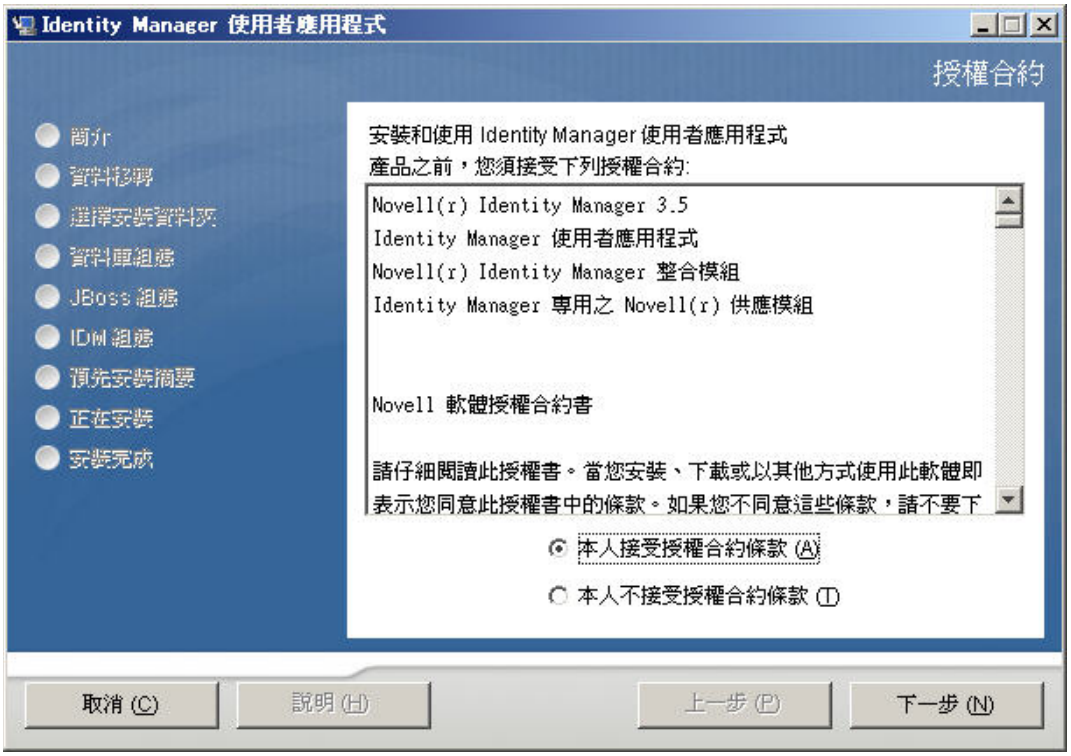
5.5.1 啓動安裝程式 GUI

1. 瀏覽至含有安裝檔案的目錄，如表格 5-2 (第 106 頁) 所述。
2. 從指令行啓動您平台的安裝程式：

java -jar IdmUserApp.jar

3 在下拉式選單中選取語言，然後按一下「*確定*」。

4 閱讀授權合約，按一下「*我接受授權合約中的條款*」，然後按一下「*下一步*」。

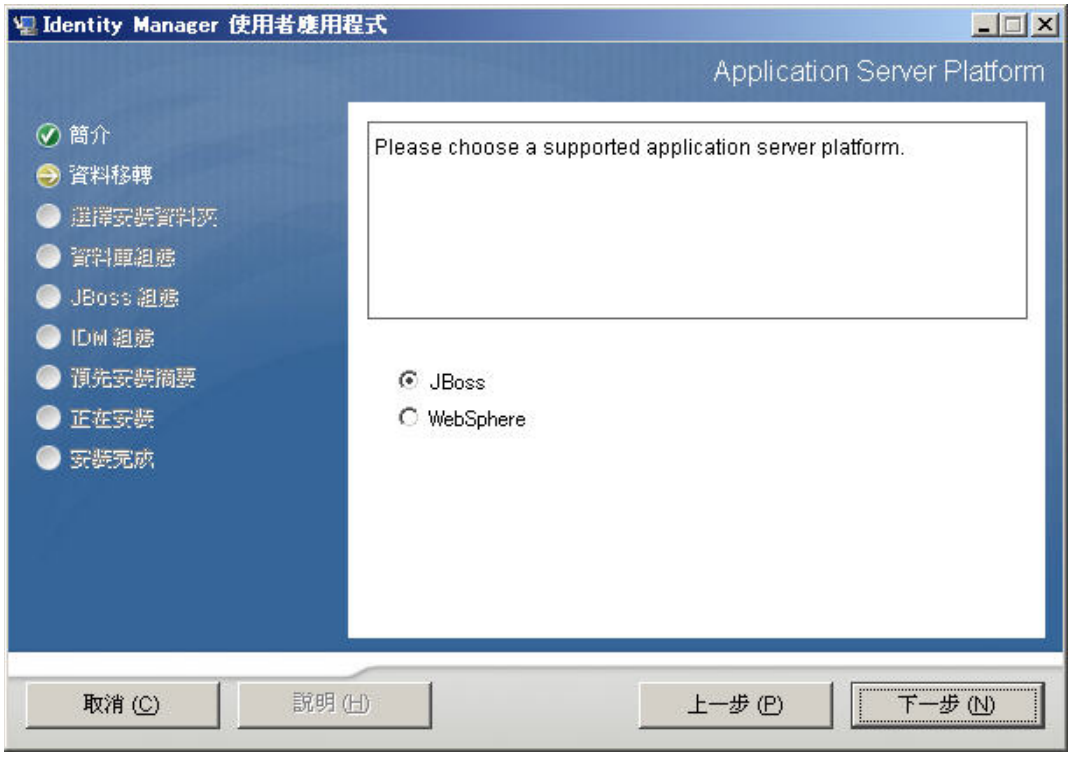


5 閱讀安裝精靈的「簡介」頁面，然後按一下「*下一步*」。

6 請繼續進行第 5.5.2 節 「選擇應用程式伺服器平台」 (第 109 頁)。

5.5.2 選擇應用程式伺服器平台

1 選擇 JBoss 應用程式伺服器平台，然後按一下「*下一步*」。



5.5.3 移轉您的資料庫

如果您不要移轉資料庫，請按一下「*下一步*」並繼續進行 第 5.5.4 節 「指定 WAR 的位置」 (第 111 頁)。

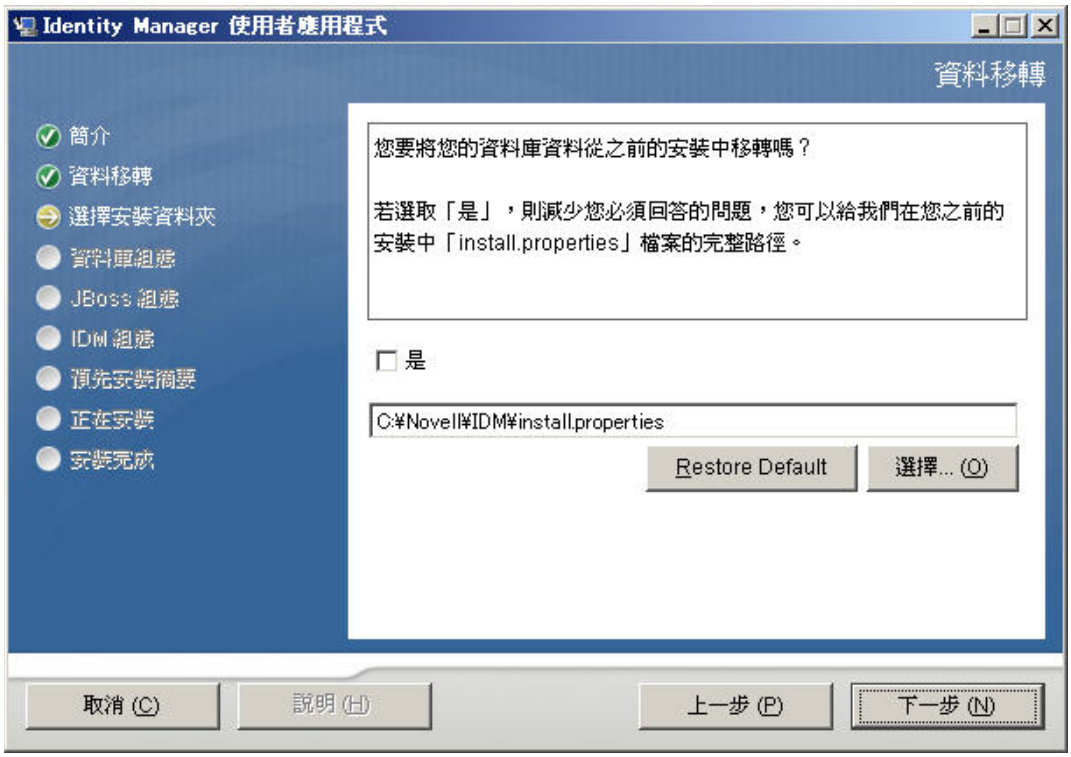
如果您想使用 「使用者應用程式」 3.0 或 3.01 版的現有資料庫，則必須移轉資料庫。

1 請確認您已經啓動想移轉的資料庫。

2 在安裝程式的 「資料移轉」頁面中按一下 「*是*」。

3 按一下 「*選擇*」在 Identity Manager 3.0 或 3.01 的 「使用者應用程式」安裝目錄中瀏覽 install.properties 檔案。

從之前的安裝指定 install.properties 檔案的位置，可減少您在之後頁面所選取的項目數目。



4 系統會要求您確認資料庫類型、主機名稱和連接埠。如此進行，再按一下「*下一步*」。

5 按一下「*下一步*」，繼續進行第 5.5.4 節「指定 WAR 的位置」(第 111 頁)。第 5.5.5 節「選擇安裝資料夾」(第 111 頁)

「使用者應用程式」安裝程式會升級您的「使用者安裝程式」，並移轉 3.0 或 3.0.1 版資料庫的資料到 3.5.1 版所使用的資料庫。如需移轉資料庫的詳細資訊和其他步驟，請參閱《*Identity Manager 使用者應用程式：移轉指南* (http://www.novell.com/documentation/idm35/index.html)》。

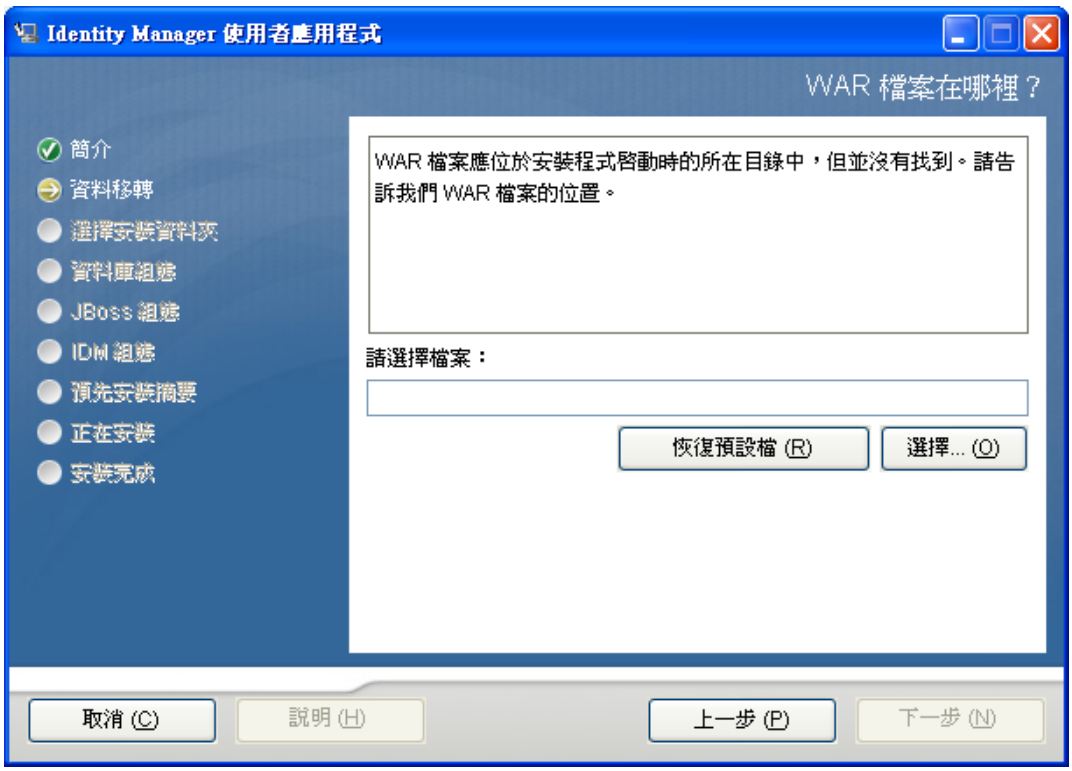
5.5.4 指定 WAR 的位置

如果「Identity Manager 使用者應用程式」的 WAR 檔案所在的目錄與安裝程式的不同，安裝程式就會提示您輸入 WAR 的路徑。

1 如果 WAR 在預設位置中，請按一下「*還原預設資料夾*」。

若要指定 WAR 檔案的位置，按一下「*選擇*」並選取位置。

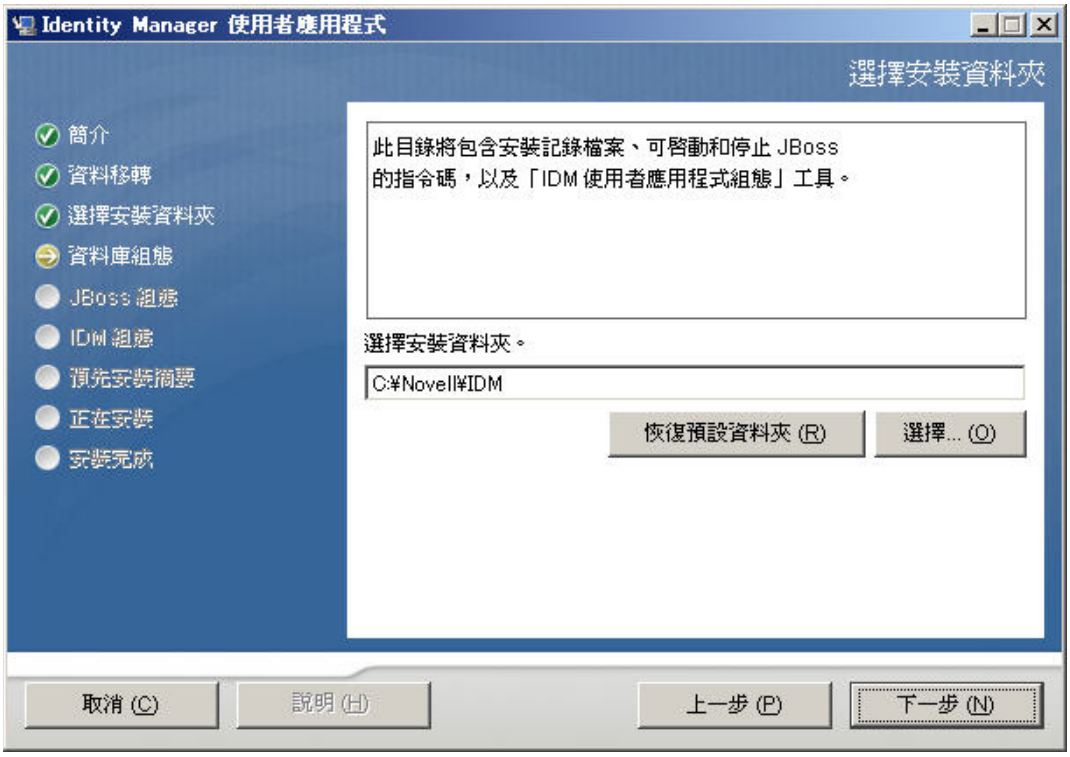
2 按「*下一步*」，然後繼續第 5.5.5 節「選擇安裝資料夾」(第 111 頁)。



5.5.5 選擇安裝資料夾

1 在「選擇安裝資料夾」頁面上，選取「使用者應用程式」的安裝位置。如果您需要記住並使用預設的位置，請按一下「*還原預設資料夾*」，或者，如果您想選擇安裝檔案的其他位置，請按一下「*選擇*」來瀏覽一個位置。

2 按「*下一步*」，然後繼續第 5.5.6 節 「選擇資料庫平台」 (第 113 頁)。

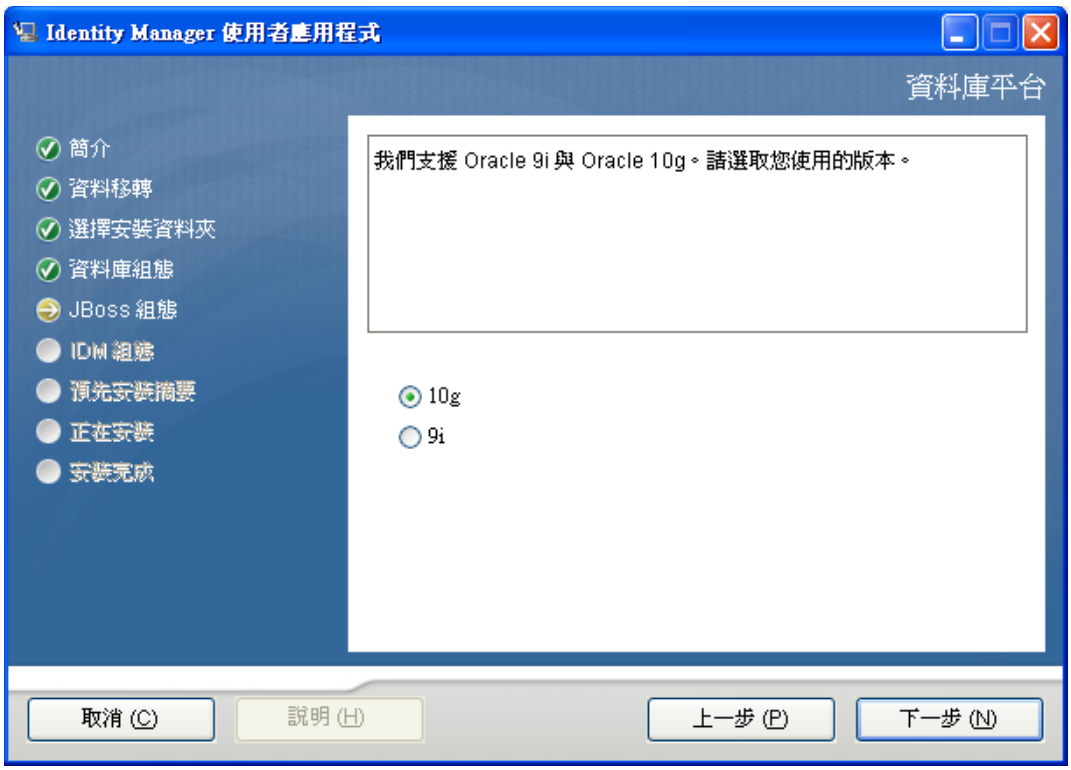


5.5.6 選擇資料庫平台

1 選取要使用的資料庫平台。

2 如果您使用 Oracle 資料庫，請繼續進行步驟 3。否則，請跳至步驟 4。

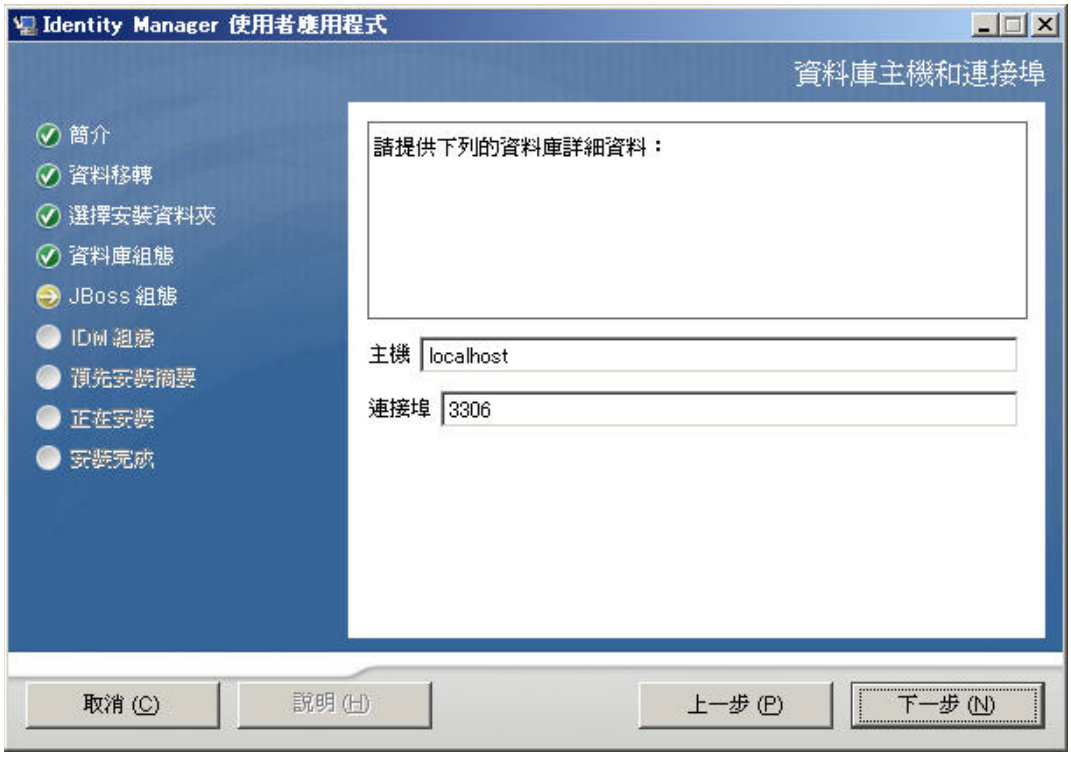
3 如果您使用 Oracle 資料庫，安裝程式就會詢問您所使用的版本。選擇您的版本。



4 按「*下一步*」，然後繼續第 5.5.7 節 「指定資料庫主機和連接埠」 (第 115 頁)。

5.5.7 指定資料庫主機和連接埠

1 填寫下列欄位：

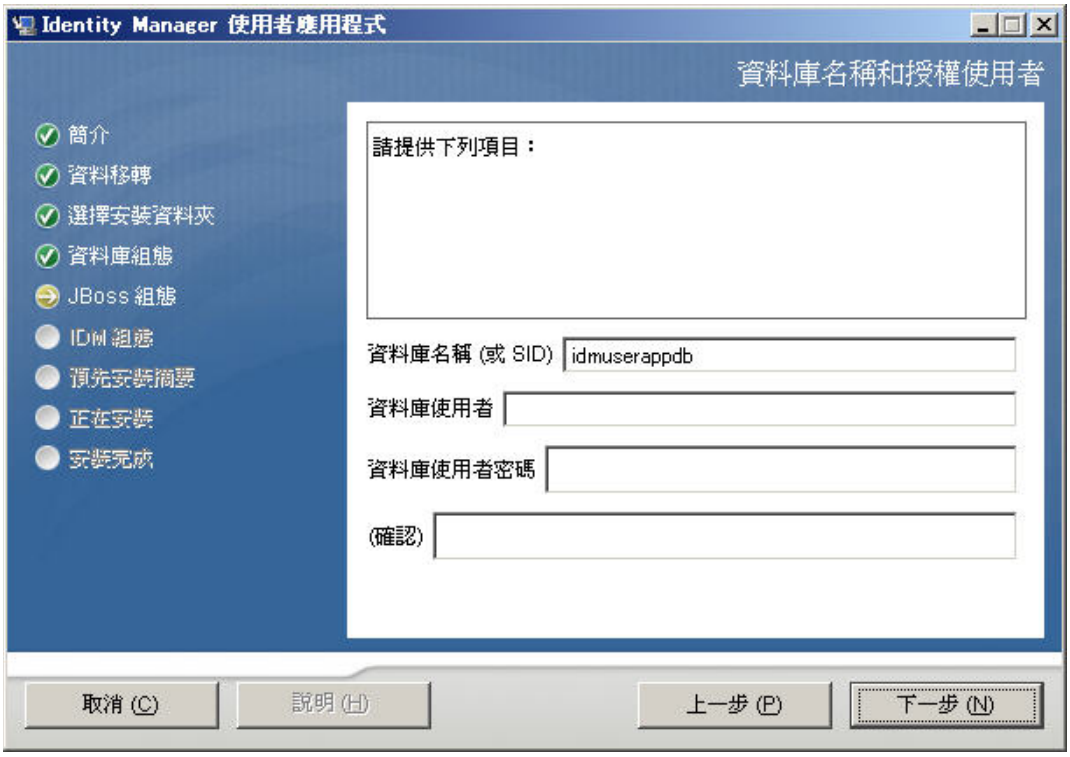


欄位	描述
主機	指定資料庫伺服器的主機名稱或 IP 位址。 對於叢集，請爲叢集的每一個成員指定相同的主機名稱和 IP 位址。
連接埠	指定資料庫的監聽程式連接埠號碼。 對於叢集，請爲叢集的每一個成員指定相同的連接埠。

2 按「*下一步*」，然後繼續第 5.5.8 節 「指定資料庫名稱和特權使用者」 (第 116 頁)。

5.5.8 指定資料庫名稱和特權使用者

1 填寫下列欄位：

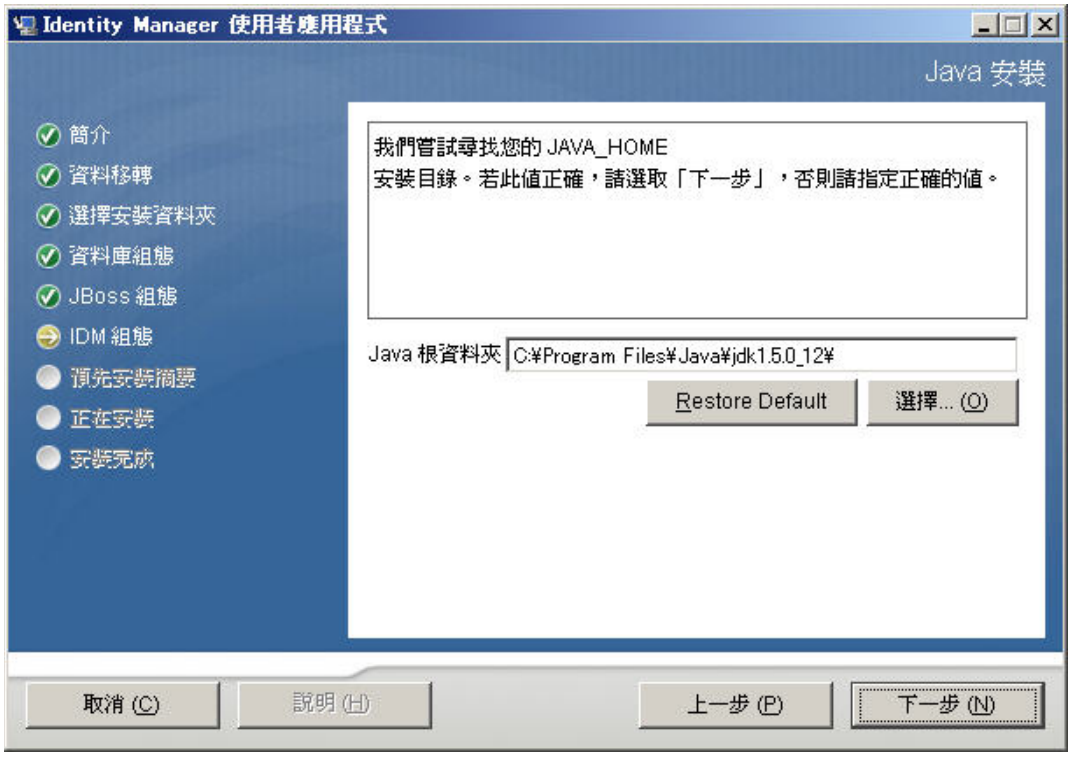


欄位	描述
資料庫名稱 (或 sid)	對於 MySQL 或 MS SQL Server，請提供您預先設定之資料庫的名稱。對於 Oracle，請提供您之前建立的 Oracle 系統識別碼 (SID)。 對於叢集，請爲叢集的每一個成員指定相同的資料庫名稱和 SID。
資料庫使用者	指定資料庫使用者。 對於叢集，請爲叢集的每一個成員指定相同的資料庫使用者。
資料庫密碼 / 確認密碼	指定資料庫密碼。 對於叢集，請爲叢集的每一個成員指定相同的資料庫密碼。

2 按一下「*下一步*」，然後繼續第 5.5.9 節「指定 Java 根目錄」(第 117 頁)。

5.5.9 指定 Java 根目錄

1 按一下「*選擇*」瀏覽您的 Java 根資料夾。若要使用預設位置，按一下「*還原預設值*」。



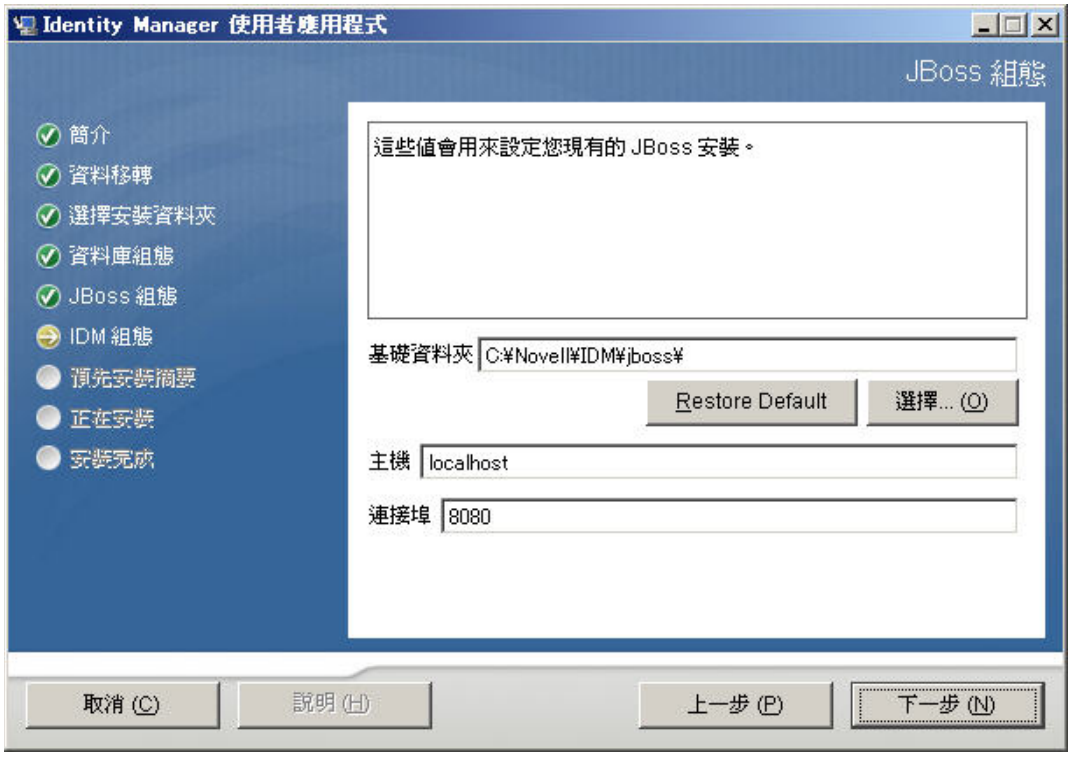
2 按一下「*下一步*」，然後繼續第 5.5.10 節 「指定 JBoss 應用程式伺服器設定」(第 117 頁)。

5.5.10 指定 JBoss 應用程式伺服器設定

在此頁面上讓「使用者應用程式」知道「JBoss 應用程式伺服器」的位置。

此安裝程序不會安裝「JBoss 應用程式伺服器」：如需安裝「JBoss 應用程式伺服器」的指示，請參閱第 5.1.1 節「安裝 JBoss 應用程式伺服器和 MySQL 資料庫」(第 95 頁)。

1 提供基礎資料夾、主機和連接埠：

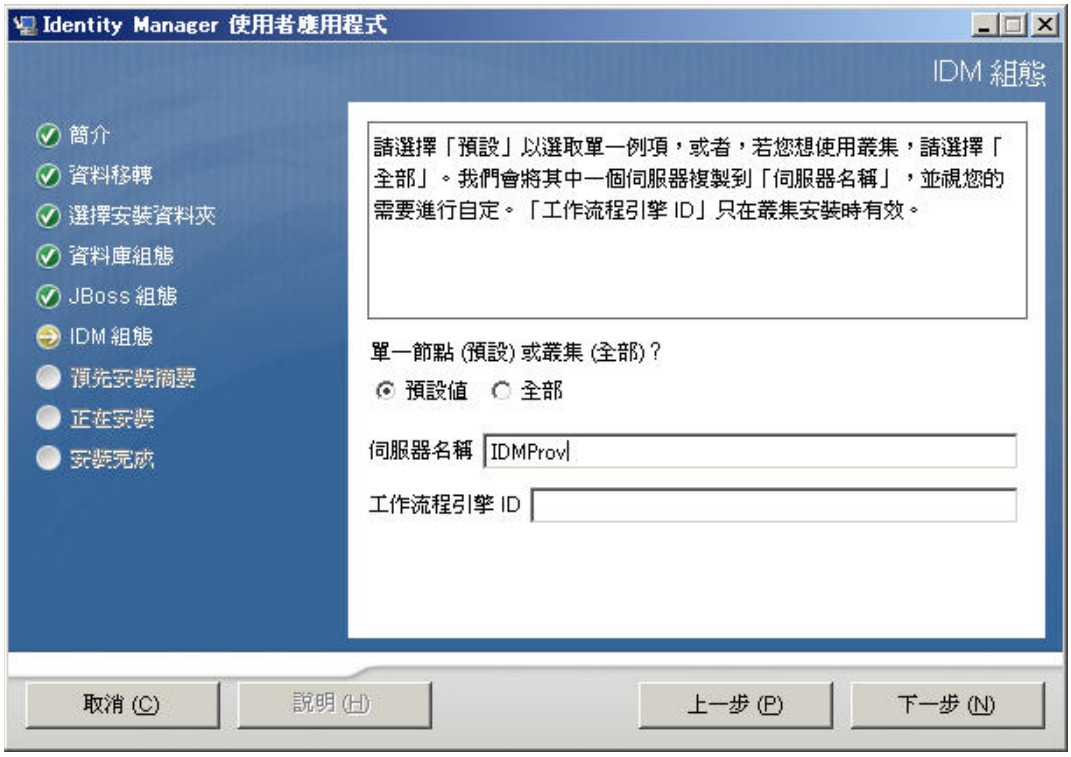


欄位	描述
基礎資料夾	指定應用程式伺服器的位置。
主機	指定應用程式伺服器的主機名稱或 IP 位址。
連接埠	指定應用程式伺服器的監聽程式連接埠號碼。預設的 JBoss 連接埠爲 8080。

2 按「*下一步*」，然後繼續第 5.5.11 節「選擇應用程式伺服器組態類型」(第 119 頁)。

5.5.11 選擇應用程式伺服器組態類型

1 填寫下列欄位：



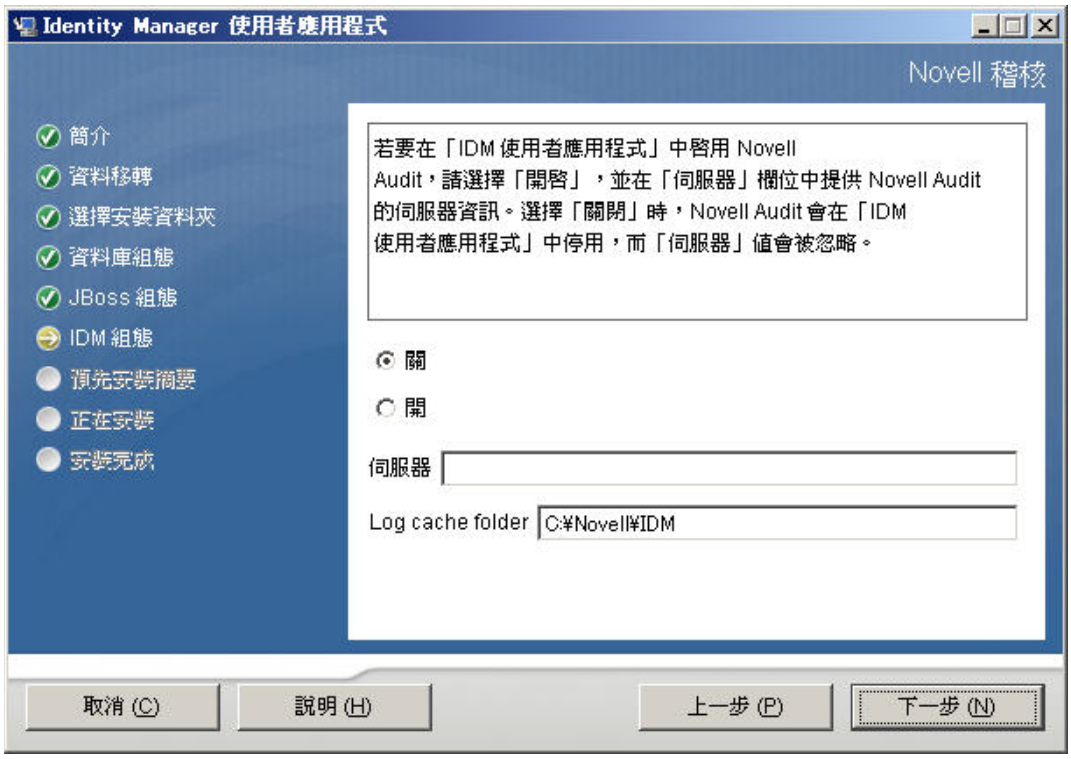
選項	描述
單一 (預設) 或叢集 (全部) >	選取應用程式伺服器組態的類型： ◆ 如果安裝爲叢集的一部分，請選取「*全部*」 ◆ 如果此安裝所在的單一節點不是叢集的一部分，請選取「*預設*」。
伺服器名稱	指定 伺服器名稱。 應用程式名稱指的是應用程式伺服器組態的名稱、應用程式 WAR 檔案的名稱以及 URL 網路位置的名稱。安裝程序檔會建立一個伺服器組態，並會依預設根據「*應用程式名稱*」來命名組態。 請將應用程式名稱記錄下來，當您從瀏覽器啓動「Identity Manager 使用者應用程式」時，可將其包含在 URL 中。
工作流程引擎 ID	叢集中的每一個 伺服器都有唯一的「工作流程引擎 ID」。在《*Identity Manager 使用者應用程式：管理指南*》的 3.5.4 節「設定叢集的工作流程」中，有「工作流程引擎 ID」的相關說明。

2 按「*下一步*」，然後繼續第 5.5.12 節「啓用 Novell Audit 記錄」(第 120 頁)。

5.5.12 啓用 Novell Audit 記錄

(選擇性) 若要啓用「使用者應用程式」的 Novell Audit 記錄：

1 填寫下列欄位：



選項	描述
之中	啓用「使用者應用程式」的 Novell Audit 記錄。 如需設定 Novell Audit 記錄的相關資訊，請參閱《*Identity Manager 使用者應用程式：管理指南*》。
關閉	停用「使用者應用程式」的 Novell Audit 記錄。您可以在稍後使用「使用者應用程式」的「*管理*」標籤來啓用它。 如需啓用 Novell Audit 記錄的相關資訊，請參閱《*Identity Manager 使用者應用程式：管理指南*》。
伺服器	如果您啓用 Novell Audit 記錄，請指定 Novell Audit 伺服器的主機名稱或 IP 位址。如果您關閉記錄，就會忽略這個值。

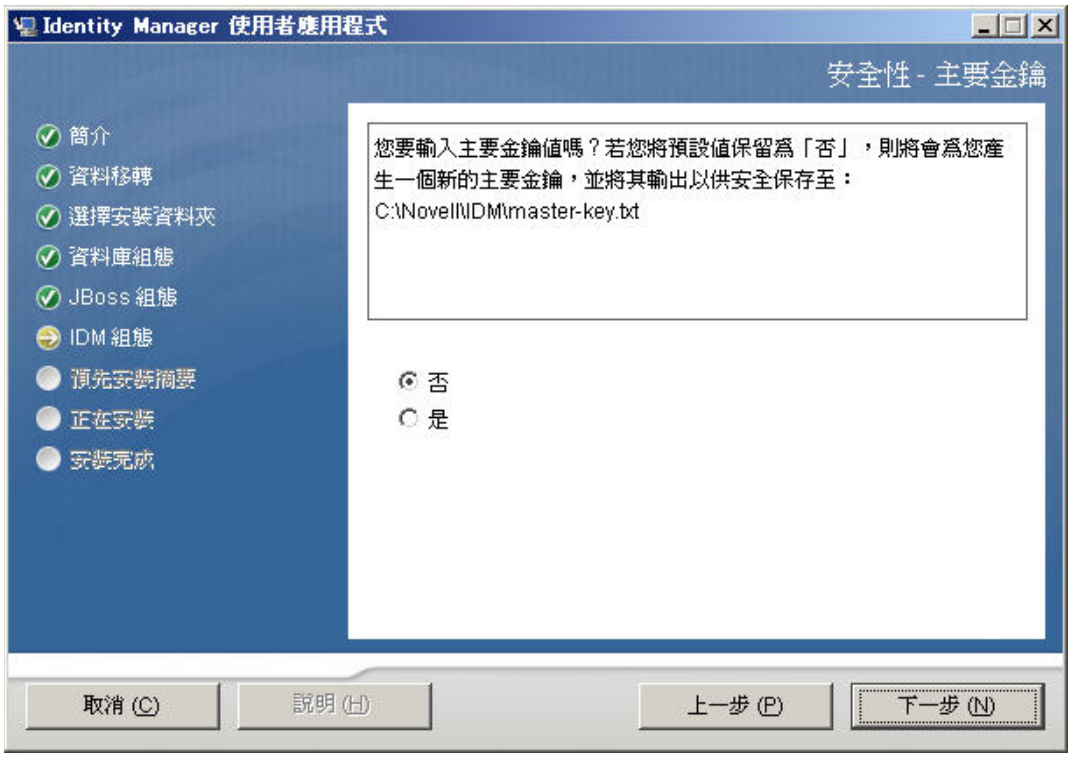
2 按「*下一步*」，然後繼續第 5.5.14 節「設定使用者應用程式組態」(第 122 頁)。

5.5.13 指定萬能金鑰

指定是否要輸入現有的萬能金鑰，或是要建立一個新的。需要輸入萬能金鑰的可能原因包括：

- 您想將安裝從預備系統移到生產系統，並想保留您在預備系統中使用的資料庫存取權限。
- 您之前將「使用者應用程式」安裝在 JBoss 叢集的第一個成員上，而現在要安裝在叢集的後續成員上 (它們需要同一個萬能金鑰)。
- 由於磁碟發生錯誤，您必須還原「使用者應用程式」。您必須重新安裝「使用者應用程式」，並指定先前安裝所使用的同一個加密萬能金鑰。這可讓您存取之前儲存的加密資料。

1 按一下「是」來使用現有的萬能金鑰，或按一下「否」來建立一個新的



2 按一下「*下一步*」。

安裝程序會將加密萬能金鑰寫入安裝目錄中的 master-key.txt 檔案。

如果您選擇「*否*」，則請跳至第 5.5.14 節「設定使用者應用程式組態」(第 122 頁)。完成安裝之後，您必須手動記錄第 5.9.1 節「記錄萬能金鑰」(第 165 頁) 中所述的萬能金鑰。

如果您選擇「*是*」，則請繼續進行步驟 3。

3 如果您選擇輸入現有的加密萬能金鑰，請剪下此金鑰並貼進安裝程序視窗。

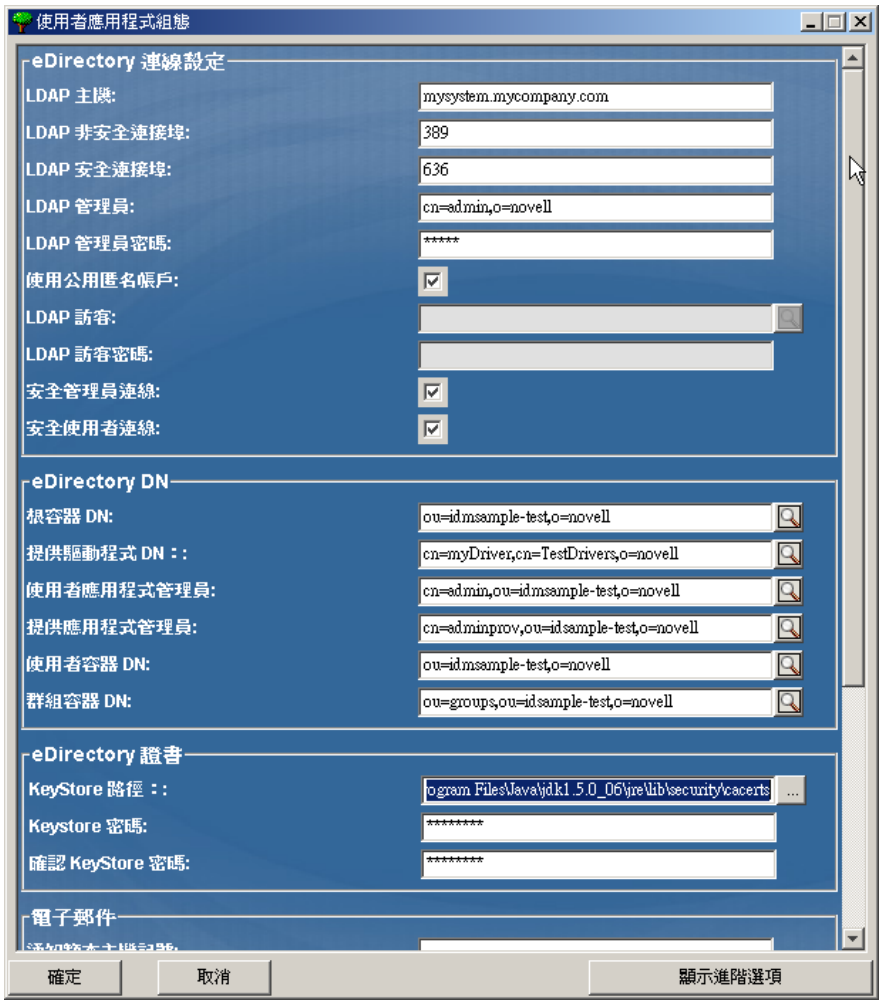
4 按一下「*下一步*」，繼續進行第 5.5.14 節 「設定使用者應用程式組態」(第 122 頁)。

5.5.14 設定使用者應用程式組態

「使用者應用程式」的安裝可讓您設定「使用者應用程式」組態參數。安裝之後，這些參數之中有大部分也可透過 configupdate.sh 或 configupdate.bat 進行編輯；如有例外，則於參數描述中說明。

對於叢集，請爲叢集的每一個成員指定同一個 「使用者應用程式」組態參數。

1 設定表格 5-4 所述的「使用者應用程式」基本組態參數，然後繼續進行步驟 2。



表格 5-4 使用者應用程式組態：基本參數

設定類型	欄位	描述
eDirectory 連線設定	*LDAP 主機*	必要。指定輕量目錄存取協定 (LDAP) 伺服器的主機名稱或 IP 位址。例如： `myLDAPhost`
	LDAP 非安全連接埠	指定 LDAP 伺服器的非安全連接埠。例如：389。
	LDAP 安全連接埠	指定 LDAP 伺服器的安全連接埠。例如： 636。
	LDAP 管理員	必要。指定 LDAP 管理員的認證。此使用者必須已經存在。「使用者應用程式」會使用此帳戶，來建立 Identity Vault 的管理連線。這個值會根據萬能金鑰進行加密。
	LDAP 管理員密碼	必要。指定 LDAP 管理員密碼。這個密碼會根據萬能金鑰進行加密。
	使用公用匿名帳戶	允許未登入的使用者存取「LDAP 公用匿名帳戶」。
	LDAP 訪客	允許未登入的使用者存取允許的入口網站應用程式。這個使用者帳戶必須已存在於 Identity Vault。若要啓用「LDAP 訪客」，您必須取消選取「*使用公用匿名帳戶*」。若要停用「訪客使用者」，請選取「*使用公用匿名帳戶*」。
	LDAP 訪客密碼	指定 LDAP 訪客密碼。
	安全管理員連線	選取這個選項來要求，必須以安全插槽完成使用管理員帳戶的所有通訊 (此選項可能有負面的效能影響)。
	安全使用者連線	選取這個選項來要求，必須以安全插槽完成使用登入使用者帳戶的所有通訊 (此選項可能有負面的效能影響)。

設定類型	欄位	描述
eDirectory DN	*根容器 DN*	必要。指定根容器的輕量目錄存取協定 (LDAP) 可辨識名稱。當在目錄抽象層中沒有指定任何搜尋根部時，會將它用做預設實體定義搜尋根部。
	提供驅動程式 DN	必要。指定您先前在第 5.3 節「建立「使用者應用程式」驅動程式」(第 100 頁) 中建立之「使用者應用程式」驅動程式的可辨識名稱。例如，如果您的驅動程式爲 UserApplicationDriver、而驅動程式集稱爲 myDriverSet，並且該驅動程式集位於 o=myCompany 的網路位置，則輸入值： `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`
	使用者應用程式管理員	必要。Identity Vault 中擁有權限執行管理任務 (由「使用者應用程式」使用者容器指定) 的使用者。此使用者可以使用「使用者應用程式」的「*管理*」標籤來管理入口網站。 *如果「使用者應用程式管理員」參與 iManager、Novell Designer for Identity Manager 或「使用者應用程式」(「申請與核准」標籤) 中公開的工作流程管理任務，您就必須給予此管理員適當的託管者權限，使其能夠存取「使用者應用程式」驅動程式中的物件例項。*如需詳細資訊，請參閱《*IDM 使用者應用程式：管理指南*》。 若想在部署「使用者應用程式」之後變更此指定，則必須使用「使用者應用程式」中的「*管理* > *安全性*」頁面。
	提供應用程式管理員	此角色可於 Identity Manager 3.5.1 的提供版本中取得。「提供應用程式管理員」會使用「*提供*」標籤 (在「*管理*」標籤之下) 來管理「提供工作流程」功能。這些功能可透過「使用者應用程式」的「*申請與核准*」標籤供使用者使用。此使用者必須先存在於 Identity Vault，才能指定爲「提供應用程式管理員」。 若想在部署「使用者應用程式」之後變更此指定，則必須使用「使用者應用程式」中的「*管理* > *安全性*」頁面。
eDirectory DN (續)	*使用者容器 DN*	必要。指定使用者容器的 LDAP 可辨識名稱 (DN) 或完全合法的 LDAP 名稱。這會定義使用者和群組的搜尋範圍。此容器中 (和下方) 的使用者可以登入「使用者應用程式」。 **重要：**如果您想讓使用者可以執行工作流程，請確定「使用者應用程式」驅動程式設定期間指定的「使用者應用程式管理員」存在於此容器中。

設定類型	欄位	描述
	群組容器 DN	必要。指定群組容器的輕量目錄存取協定 (LDAP) 可辨識名稱 (DN) 或完全合法的 LDAP 名稱。 由目錄抽象層內的實體定義使用。
eDirectory 證書	*KeyStore 路徑*	必要。針對應用程式伺服器用來執行之 JDK 的 KeyStore (cacerts) 檔案，輸入其完整路徑，或者，按一下瀏覽器小按鈕來瀏覽 cacerts 檔案。 在 Linux 或 Solaris 上，使用者必須擁有權限寫入此檔案。
	KeyStore 密碼 / 確認 KeyStore 密碼	必要。指定 cacerts 密碼。預設值爲「changeit」。
電子郵件	*通知範本 HOST 記號*	指定代管「Identity Manager 使用者應用程式」的應用程式伺服器。例如： `myapplication serverServer` 此值會取代電子郵件範本中的 $HOST$ 記號。建構的 URL 是提供申請任務和核准通知的連結。
	通知範本 PORT 記號	用於取代提供申請任務和核准通知中所使用之電子郵件範本中的 $PORT$ 記號。
	通知範本安全連接埠記號	用於取代提供申請任務和核准通知中所使用之電子郵件範本中的 $SECURE_PORT$ 記號。
	SMTP 電子郵件通知寄件者：	指定來自提供電子郵件中使用者的電子郵件。
	SMTP 電子郵件通知主機	指定提供電子郵件所使用的 SMTP 電子郵件主機。可以是 IP 位址或 DNS 名稱。
密碼管理	*使用外部密碼 WAR*	此功能可讓您指定一個「忘記密碼」頁面放在外部「忘記密碼 WAR」中，並指定一個 URL，讓外部「忘記密碼 WAR」用來透過 Web 服務喚回「使用者應用程式」。 如果您核取「*使用外部密碼 WAR*」，就必須提供「*忘記密碼連結*」和「*忘記密碼回傳連結*」的值。 如果您不核取「*使用外部密碼 WAR*」，IDM 就會使用預設的內部「密碼管理」功能。/jsps/pwdmgt/ForgotPassword.jsf (開頭不使用 HTTP 通訊協定)。這會將使用者重新導向至「使用者應用程式」內建的「忘記密碼」功能，而不是外部 WAR。
	忘記密碼連結	此 URL 指向「忘記密碼」功能頁面。在外部或內部的密碼管理 WAR 中指定 ForgotPassword.jsf 檔案。如需詳細資料，請參閱「使用密碼 WAR」(第 132 頁)。
	忘記密碼回傳連結	如果您使用外部密碼管理 WAR，則請提供該外部「密碼管理 WAR」用來透過 Web 服務喚回「使用者應用程式」的路徑，例如 https://*idmhost:sslport*/idm。

2 如果您想設定「使用者應用程式」其他的組態參數，請按一下「*顯示進階選項*」(請捲動檢視整個面板)。表格 5-5 描述了「進階選項」參數。

如果您不想設定此步驟所述的其他參數，請跳至步驟 3。

表格 5-5 *使用者應用程式組態：所有參數*

設定類型	欄位	描述
eDirectory 連線設定	*LDAP 主機*	必要。指定 LDAP 伺服器的主機名稱或 IP 位址。例如： myLDAPhost
	LDAP 非安全連接埠	指定 LDAP 伺服器的非安全連接埠。例如：389。
	LDAP 安全連接埠	指定 LDAP 伺服器的安全連接埠。例如： 636。
	LDAP 管理員	必要。指定 LDAP 管理員的認證。此使用者必須已經存在。「使用者應用程式」會使用此帳戶，來建立 Identity Vault 的管理連線。這個值會根據萬能金鑰進行加密。
	LDAP 管理員密碼	必要。指定 LDAP 管理員密碼。這個密碼會根據萬能金鑰進行加密。
	使用公用匿名帳戶	允許未登入的使用者存取「LDAP 公用匿名帳戶」。
	LDAP 訪客	允許未登入的使用者存取允許的入口網站應用程式。這個使用者帳戶必須已存在於 Identity Vault。若要啓用「LDAP 訪客」，您必須取消選取「*使用公用匿名帳戶*」。若要停用「訪客使用者」，請選取「*使用公用匿名帳戶*」。
	LDAP 訪客密碼	指定 LDAP 訪客密碼。
	安全管理員連線	選取這個選項來要求，必須以安全插槽完成使用管理員帳戶的所有通訊 (此選項可能有負面的效能影響)。
	安全使用者連線	選取這個選項來要求，必須以安全插槽完成登入使用者帳戶所完成的所有通訊 (此選項可能有負面的效能影響)。

設定類型	欄位	描述
eDirectory DN	*根容器 DN*	必要。指定根容器的輕量目錄存取協定 (LDAP) 可辨識名稱。當在目錄抽象層中沒有指定任何搜尋根部時，會將它用做預設實體定義搜尋根部。
	提供驅動程式 DN	必要。指定您先前在第 5.3 節「建立「使用者應用程式」驅動程式」(第 100 頁) 中建立之「使用者應用程式」驅動程式的可辨識名稱。例如，如果您的驅動程式爲 userapplicationdriver、而驅動程式集稱爲 mydriverset，並且該驅動程式集位於 o=myCompany 的網路位置，則輸入值： `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`
	使用者應用程式管理員	必要。Identity Vault 中擁有權限執行管理任務 (由「使用者應用程式」使用者容器指定) 的使用者。此使用者可以使用「使用者應用程式」的「*管理*」標籤來管理入口網站。 *如果「使用者應用程式管理員」參與 iManager、Novell Designer for Identity Manager 或「使用者應用程式」(「申請與核准」標籤) 中公開的工作流程管理任務，您就必須給予此管理員適當的託管者權限，使其能夠存取「使用者應用程式」驅動程式中的物件例項。*如需詳細資訊，請參閱《*IDM 使用者應用程式：管理指南*》。 若想在部署「使用者應用程式」之後變更此指定，則必須使用「使用者應用程式」中的「*管理* > *安全性*」頁面。
	提供應用程式管理員	此角色可於 Identity Manager 3.5.1 的提供版本中取得。「提供應用程式管理員」會使用「使用者應用程式」的「*申請與核准*」標籤來管理「提供工作流程」功能。此使用者必須先存在於 Identity Vault，才能指定爲「提供應用程式管理員」。 若想在部署「使用者應用程式」之後變更此指定，則必須使用「使用者應用程式」中的「*管理* > *安全性*」頁面。

設定類型	欄位	描述
中繼目錄使用者身分	*使用者容器 DN*	必要。指定使用者容器的 LDAP 可辨識名稱 (DN) 或完全合法的 LDAP 名稱。 這會定義使用者和群組的搜尋範圍。 此容器中 (和下方) 的使用者可以登入「使用者應用程式」。 **重要：**如果您想讓使用者可以執行工作流程，請確定「使用者應用程式」驅動程式設定期間指定的「使用者應用程式管理員」存在於此容器中。
	使用者物件類別	LDAP 使用者物件類別 (通常爲 inetOrgPerson)。
	登入屬性	代表使用者登入名稱的 LDAP 屬性 (例如 CN)。
	命名屬性	此 LDAP 可在查閱使用者或群組時做爲識別碼。這和登入屬性不一樣，後者只能用於登入，不可用於使用者 / 群組搜尋。
	使用者成員資格屬性	選用。代表使用者群組成員資格的 LDAP 屬性。請勿在此名稱中使用空格。
中繼目錄使用者群組	*群組容器 DN*	必要。指定群組容器的輕量目錄存取協定 (LDAP) 可辨識名稱 (DN) 或完全合法的 LDAP 名稱。由目錄抽象層內的實體定義使用。
	群組物件類別	LDAP 群組物件類別 (通常爲 groupofNames)。
	群組成員資格屬性	代表使用者群組成員資格的屬性。請勿在此名稱中使用空格。
	使用動態群組	如果您想要使用動態群組，請選取此選項。
	動態群組物件類別	LDAP 動態群組物件類別 (通常爲 dynamicGroup)。
eDirectory 證書	*KeyStore 路徑*	必要。針對應用程式伺服器用來執行之 JRE 的 keystore (cacerts) 檔案，輸入其完整路徑，或者，按一下瀏覽器小按鈕來瀏覽 cacerts 檔案。 「使用者應用程式」的安裝會修改 KeyStore 檔案。在 Linux 或 Solaris 上，使用者必須擁有權限寫入此檔案。
	KeyStore 密碼 *確認 KeyStore 密碼*	必要。指定 cacerts 密碼。預設值爲「changeit」。

設定類型	欄位	描述
私密金鑰儲存區	*私密 KeyStore 路徑*	私密 KeyStore 含有「使用者應用程式」的私密金鑰和證書。保留 . 如果您想保留空白，此路徑則預設爲 /jre/lib/security/cacerts。
	私密 KeyStore 密碼	除非您另行指定，否則密碼爲 changeit。這個密碼會根據萬能金鑰進行加密。
	私密金鑰別名	除非您另行指定，否則密碼爲 novellIDMUserApp。
	私密金鑰密碼	除非您另行指定，否則密碼爲 nove1lIDM。這個密碼會根據萬能金鑰進行加密。
託管金鑰儲存區	*託管儲存區路徑*	「託管金鑰儲存區」包含所有託管簽名者的證書，用來驗證數位簽名。如果此路徑爲空，則「使用者應用程式」會從「系統」內容 javax.net.ssl.trustStore 取得路徑。如果路徑不在那裡，就假設爲 jre/lib/security/cacerts。
	託管儲存區密碼	如果此欄位爲空，則「使用者應用程式」會從「系統」內容 javax.net.ssl.trustStorePassword 取得密碼。如果值不在那裡，則使用 changeit。這個密碼會根據萬能金鑰進行加密。
Novell Audit 數位簽名和證書金鑰		包含 Novell Audit 的數位簽名金鑰和證書。
	Novell Audit 數位簽名證書	顯示數位簽名證書。
	Novell Audit 數位簽名私密金鑰	顯示數位簽名私密金鑰。這個金鑰會根據萬能金鑰進行加密。
iChain 設定	*已啓用 ICS 登出*	若選取此選項，「使用者應用程式」就可支援同時登出「使用者應用程式」以及 iChain 或 Novell Access Manager。「使用者應用程式」會在登出時檢查是否有 iChain 或 Novell Access Manager 的 Cookie，如果有，就將使用者重新導向到 ICS 登出頁面。
	ICS 登出頁面	連結至 iChain 或 Novell Access Manager 登出頁面的 URL，其中的 URL 是 iChain 或 Novell Access Manager 需要的主機名稱。如果 ICS 登入已經啓用，且使用者登出了「使用者應用程式」，則該使用者會被重新導向至此頁面。

設定類型	欄位	描述
電子郵件	*通知範本 HOST 記號*	指定代管「Identity Manager 使用者應用程式」的應用程式伺服器。例如： `myapplication serverServer` 此值會取代電子郵件範本中的 $HOST$ 記號。建構的 URL 是提供申請任務和核准通知的連結。
	通知範本 PORT 記號	用於取代提供申請任務和核准通知中所使用之電子郵件範本中的 $PORT$ 記號。
	通知範本 SECURE PORT 記號	用於取代提供申請任務和核准通知中所使用之電子郵件範本中的 $SECURE_PORT$ 記號。
	通知範本 PROTOCOL 記號	指的是非安全通訊協定 HTTP。用於取代提供申請任務和核准通知中所使用之電子郵件範本中的 $PROTOCOL$ 記號。
	通知範本 SECURE PROTOCOL 記號	指的是安全通訊協定 HTTPS。用於取代提供申請任務和核准通知中所使用之電子郵件範本中的 $SECURE_PROTOCOL$ 記號。
	SMTP 電子郵件通知寄件者：	指定來自提供電子郵件中使用者的電子郵件。
	SMTP 電子郵件通知主機	指定提供電子郵件所使用的 SMTP 電子郵件主機。可以是 IP 位址或 DNS 名稱。
密碼管理		
	使用外部密碼 WAR	此功能可讓您指定一個「忘記密碼」頁面放在外部「忘記密碼 WAR」中，並指定一個 URL，讓外部「忘記密碼 WAR」用來透過 Web 服務喚回「使用者應用程式」。 如果您核取「*使用外部密碼 WAR*」，就必須提供「*忘記密碼連結*」和「*忘記密碼回傳連結*」的值。 如果您不核取「*使用外部密碼 WAR*」，IDM 就會使用預設的內部「密碼管理」功能。/jsps/pwdmgt/ForgotPassword.jsf (開頭不使用 HTTP 通訊協定)。這會將使用者重新導向至「使用者應用程式」內建的「忘記密碼」功能，而不是外部 WAR。
	忘記密碼連結	此 URL 指向「忘記密碼」功能頁面。在外部或內部的密碼管理 WAR 中指定 ForgotPassword.jsf 檔案。如需詳細資料，請參閱「使用密碼 WAR」(第 132 頁)。
	忘記密碼回傳連結	如果您使用外部密碼管理 WAR，則請提供該外部「密碼管理 WAR」用來透過 Web 服務喚回「使用者應用程式」的路徑，例如 https://*idmhost:ssl*/*port*/idm。

設定類型	欄位	描述
其他	*會期逾時*	應用程式會期逾時。
	OCSP URI	如果用戶端安裝使用線上證書狀態通訊協定 (On-Line Certificate Status Protocol，OCSP)，則請提供資源識別字串 (Uniform Resource Identifier，URI)。例如，格式爲 http://host:port/ocspLocal。OCSP URI 會在線上更新託管證書的狀態。
	授權組態路徑	授權組態檔案的完全合法名稱。
容器物件	*選取*	選取要使用的「容器物件類型」。
	容器物件類型	從下列的標準容器中進行選取：地區、國家、organizationalUnit 和領域。您也可以在 iManager 中定義自己的容器，然後將其新增至「*新增新容器物件*」之下。
	容器屬性名稱	列出與「容器物件類型」關聯的「屬性類型」名稱。
	新增新容器物件：容器物件類型	在 Identity Vault 中指定一個可做爲容器的 ObjectClass 之 LDAP 名稱。 如需有關容器的詳細資訊，請參閱《*Novell iManager 2.6 管理指南 (http://www.novell.com/documentation/imanager26/pdfdoc/imanager_admin_26/imanager_admin_26.pdf)*》
	新增新容器物件：容器屬性名稱	提供容器物件的屬性名稱。

附註：在安裝之後，您可以在此檔案中編輯大部分的設定。若要這麼做，請執行 configupdate.sh 程序檔或 Windows configupdate.bat 檔案 (位於您的安裝子目錄中)。請記住，在叢集中，對於叢集的所有成員，此檔案中的設定必須完全相同。

3 完成設定後，請按一下「*確定*」，然後繼續進行第 5.5.15 節「確認選擇並安裝」(第 133 頁)。

使用密碼 WAR

使用「*忘記密碼連結*」組態參數來爲一個具有「忘記密碼」功能的 WAR 指定位置。您指定的 WAR 可以在「使用者應用程式」的外部或內部。

指定外部密碼管理 WAR

1 使用安裝程序或 configupdate 公用程式。

2 在「使用者應用程式」組態參數中，核取「*使用外部密碼 WAR*」組態參數的核取方塊。

3 如需「*忘記密碼連結*」組態參數，請指定外部密碼 WAR 的位置。

納入主機名稱和連接埠，例如 http://localhost:8080/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsf。外部密碼 WAR 可以位於「使用者應用程式」的保護防火牆外面。

4 如需「*外部密碼回傳連結*」，則請提供該外部「密碼管理 WAR」用來透過 Web 服務喚回「使用者應用程式」的路徑，例如 https:// *idmhost:sslport*/idm 。

回傳連結必須使用 SSL 來確保和「使用者應用程式」之間的 Web 服務通訊安全無虞。並請參閱第 5.9.3 節「設定 JBoss 伺服器之間的 SSL 通訊」(第 165 頁)。

5 如果您使用安裝程式，則請閱讀此步驟中的資訊，然後繼續前往步驟 6。

如果您使用 configupdate 公用程式來更新安裝根目錄中的外部密碼 WAR，則請閱讀此步驟，並手動將 WAR 重新命名爲您在「*忘記密碼連結*」中所指定的第一個目錄。然後繼續前往步驟 6。

在安裝結束之前，安裝程式會將 IDMPwdMgt.war (隨附於安裝程式) 重新命名爲您指定的第一個目錄名稱。經過重新命名的 IDMPwdMgt.war 會變成您的外部密碼 WAR。例如，如果您指定 http://www.idmpwdmgthost.com/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsf，安裝程式就會將 IDMPwdMgt.war 重新命名爲 ExternalPwd.war。安裝程式會將重新命名的 WAR 移到安裝根目錄裡面。

6 手動複製 ExternalPwd.war 到負責執行外部密碼 WAR 功能的遠端 JBoss 伺服器部署目錄。

指定內部密碼管理 WAR

1 請勿核取「*使用外部密碼 WAR*」。

2 接受「*忘記密碼連結*」的預設位置，或提供其他密碼 WAR 的 URL。

3 接受「*忘記密碼回傳連結*」的預設值。

5.5.15 確認選擇並安裝

1 閱讀「預先安裝摘要」頁面，確認您選擇的安裝參數。

2 *如有必要，請使用「上一步」，返回先前的安裝頁面變更安裝參數。*

「使用者應用程式」組態頁面不會儲存這些值，因此在您重新指定先前的安裝頁面時，請務必重新輸入「使用者應用程式」的組態值。

3 對安裝和組態參數感到滿意之後，請返回「預先安裝摘要」頁面並按一下「*安裝*」。

5.5.16 檢視記錄檔案

1 如果安裝完成時未發生任何錯誤，請移至第 5.9 節「安裝後任務」(第 164 頁)。

2 如果安裝發生錯誤或警告，請檢閱記錄檔案來找出問題。

- Identity_Manager_User_Application_InstallLog.log 中保留基本安裝工作的結果
- Novell-Custom-Install.log 會存放「使用者應用程式」在安裝期間的組態資訊

如需解決問題的協助，請參閱第 5.11 節「疑難排解」(第 169 頁)。

5.6 將「使用者應用程式」安裝在 WebSphere 應用程式伺服器上

本節說明如何使用安裝程式的圖形使用者介面，在 WebSphere 應用程式伺服器上安裝「IDM 使用者應用程式」。

- 第 5.6.2 節 「選擇應用程式伺服器平台」 (第 135 頁)
- 第 5.6.3 節 「指定 WAR 的位置」 (第 136 頁)
- 第 5.6.4 節 「選擇安裝資料夾」 (第 138 頁)
- 第 5.6.5 節 「選擇資料庫平台」 (第 139 頁)
- 第 5.6.6 節 「指定 Java 根目錄」 (第 141 頁)
- 第 5.6.7 節 「啓用 Novell Audit 記錄」 (第 142 頁)
- 第 5.6.8 節 「指定萬能金鑰」 (第 143 頁)
- 第 5.6.9 節 「設定使用者應用程式組態」 (第 145 頁)
- 第 5.6.10 節 「確認選擇並安裝」 (第 155 頁)
- 第 5.6.11 節 「檢視記錄檔案」 (第 156 頁)
- 第 5.6.12 節 「新增使用者應用程式組態檔和 JVM 系統內容」 (第 156 頁)
- 第 5.6.13 節 「將 eDirectory 託管根部匯入至 WebSphere keystore」 (第 157 頁)
- 第 5.6.14 節 「部署 IDM WAR 檔」 (第 158 頁)
- 第 5.6.15 節 「啓動應用程式」 (第 158 頁)
- 第 5.6.16 節 「存取 「使用者應用程式入口網站」」 (第 159 頁)

5.6.1 啓動安裝程式 GUI

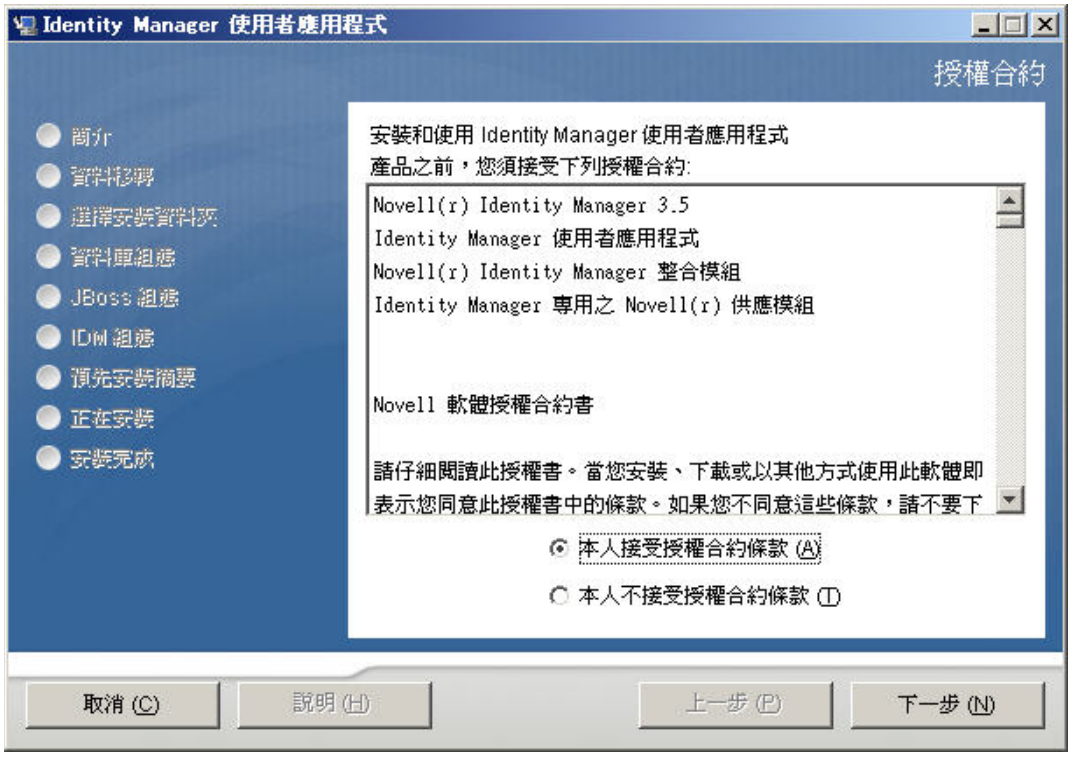
1 瀏覽至含有安裝檔案的目錄，如所述。

2 啓動安裝程式：

java -jar IdmUserApp.jar

3 在下拉式選單中選取語言，然後按一下 「確定」。

4 閱讀授權合約，按一下「*我接受授權合約中的條款*」，然後按一下「*下一步*」。



5 閱讀安裝精靈的「簡介」頁面，然後按一下「*下一步*」。

6 請繼續進行第 5.6.2 節 「選擇應用程式伺服器平台」 (第 135 頁)。

5.6.2 選擇應用程式伺服器平台

1 在「應用程式伺服器平台」視窗中，選取 WebSphere 應用程式伺服器平台。

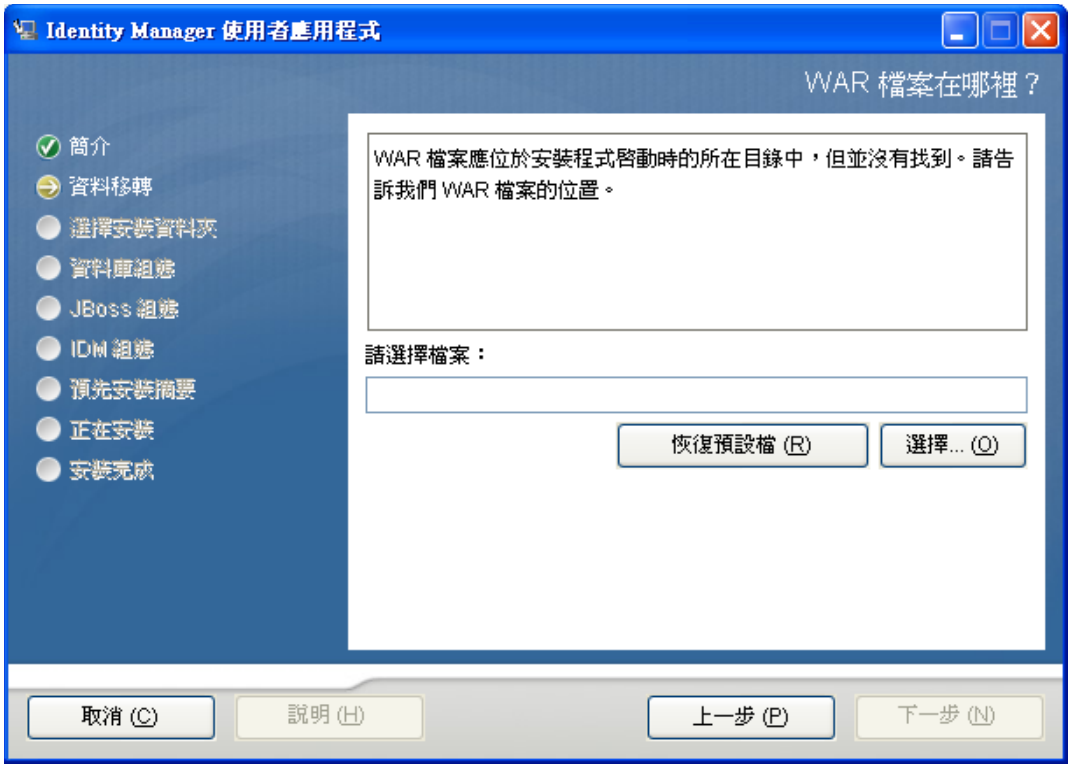
2 選取「*下一步*」。然後繼續執行第 5.6.3 節 「指定 WAR 的位置」 (第 136 頁)。

5.6.3 指定 WAR 的位置

如果「Identity Manager 使用者應用程式」的 WAR 檔案所在的目錄與安裝程式的不同，安裝程式就會提示您輸入 WAR 的路徑。

1 如果 WAR 在預設位置中，請按一下「*還原預設資料夾*」。

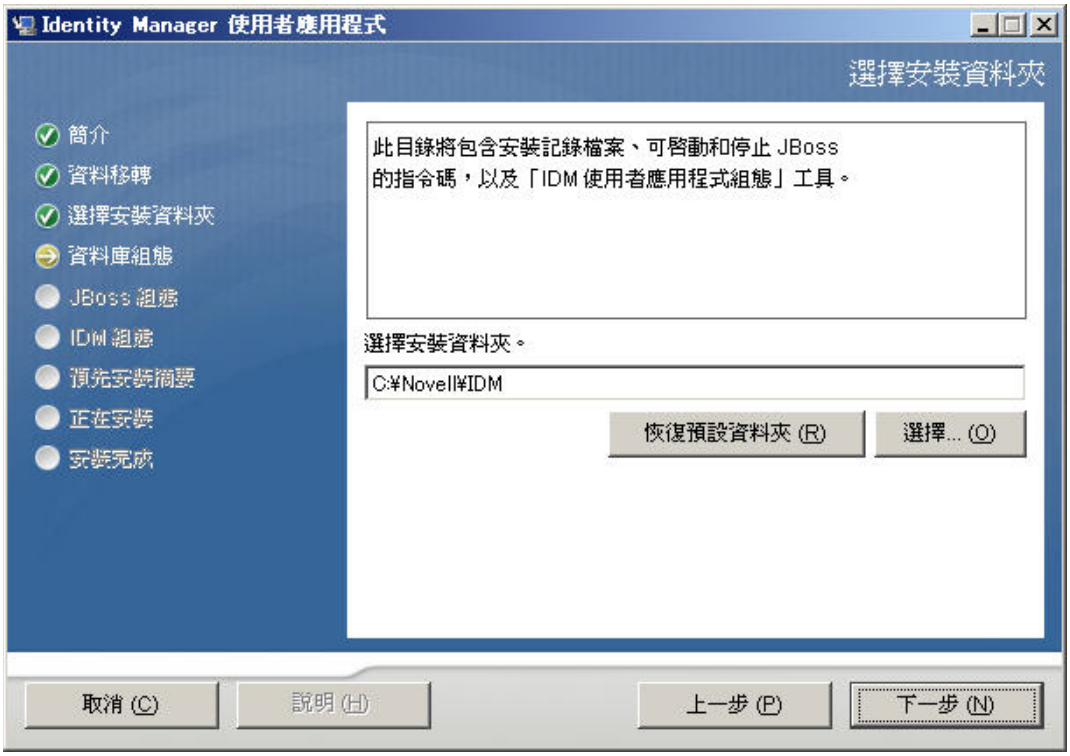
若要指定 WAR 檔案的位置，按一下「*選擇*」並選取位置。



2 按「*下一步*」，然後繼續第 5.6.4 節 「選擇安裝資料夾」 (第 138 頁)。

5.6.4 選擇安裝資料夾

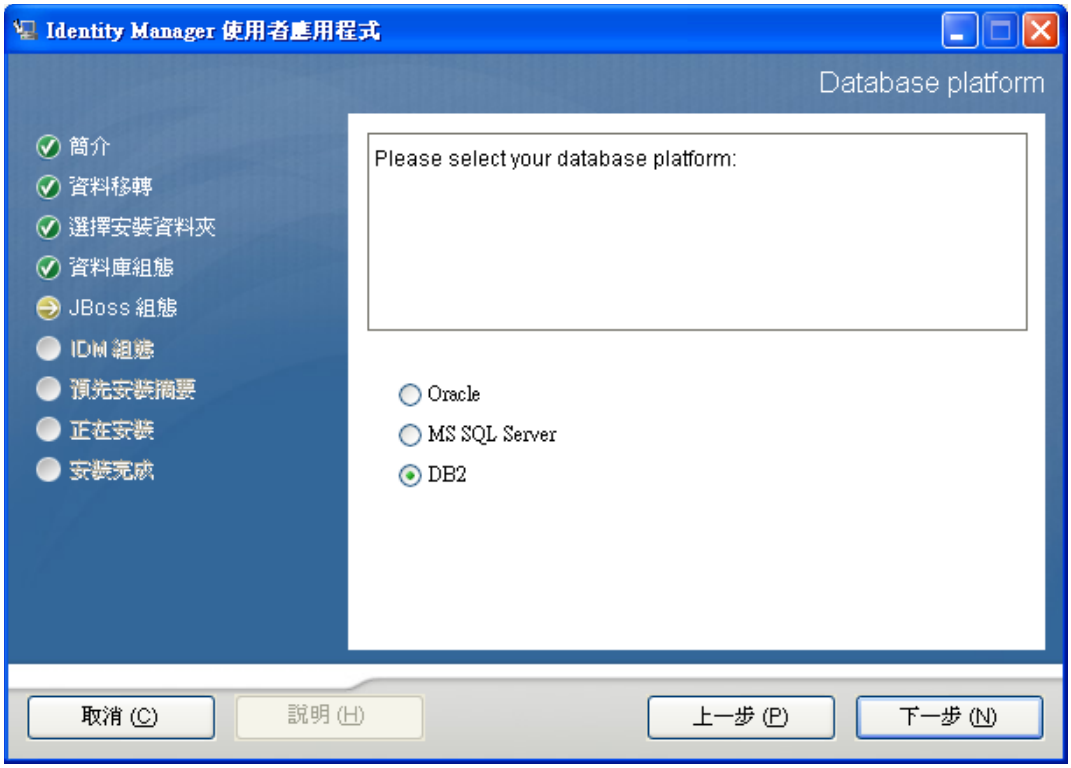
1 在「選擇安裝資料夾」頁面上，選取「使用者應用程式」的安裝位置。如果您需要記住並使用預設的位置，請按一下「*還原預設資料夾*」，或者，如果您想選擇安裝檔案的其他位置，請按一下「*選擇*」來瀏覽一個位置。



2 按「*下一步*」，然後繼續第 5.6.5 節 「選擇資料庫平台」 (第 139 頁)。

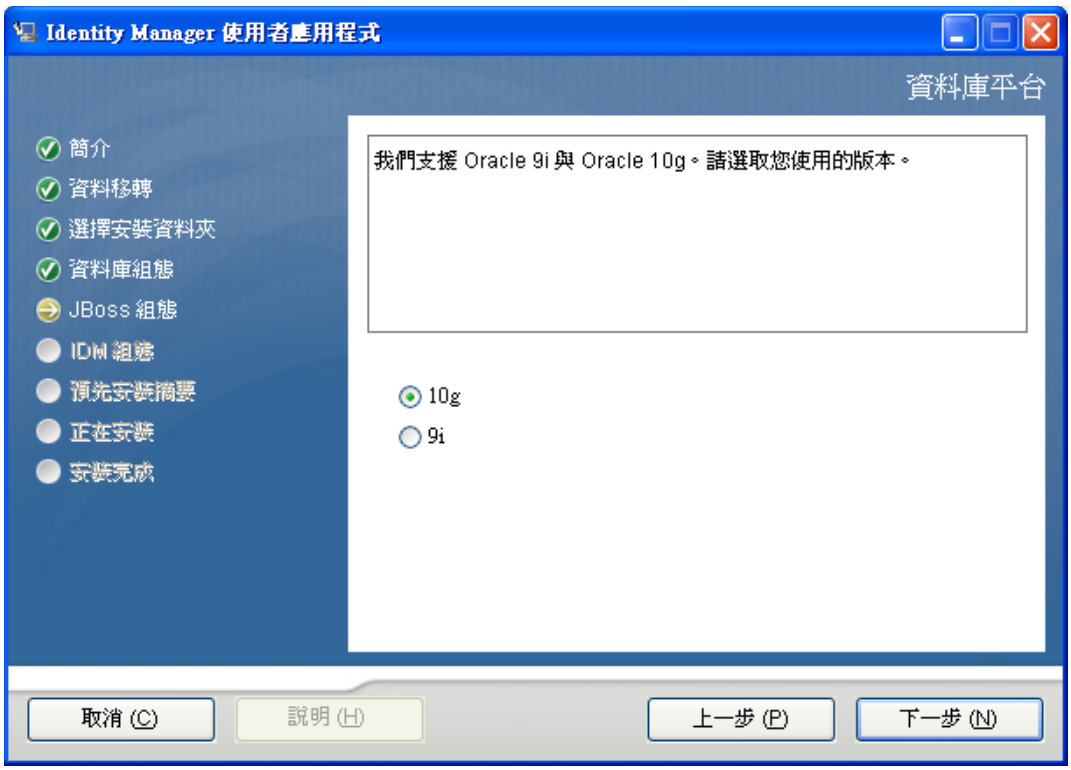
5.6.5 選擇資料庫平台

1 選取要使用的資料庫平台。



2 如果您使用 Oracle 資料庫，請繼續進行步驟 3。否則，請跳至步驟 4。

3 如果您使用 Oracle 資料庫，安裝程式就會詢問您所使用的版本。選擇您的版本。

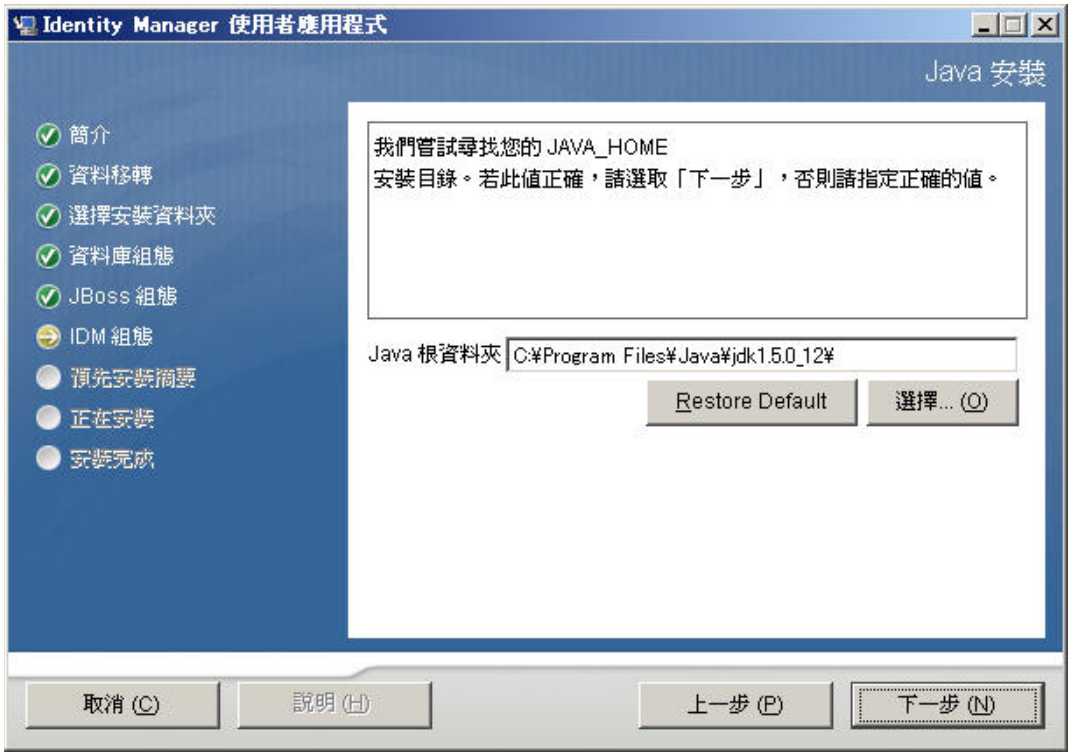


4 按「*下一步*」，然後繼續第 5.6.6 節 「指定 Java 根目錄」(第 141 頁)。

5.6.6 指定 Java 根目錄

附註：使用 WebSphere 時，您必須使用已套用未限制規則檔案的 IBM JDK。

1 按一下「*選擇*」瀏覽您的 Java 根資料夾。若要使用預設位置，按一下「*還原預設值*」。

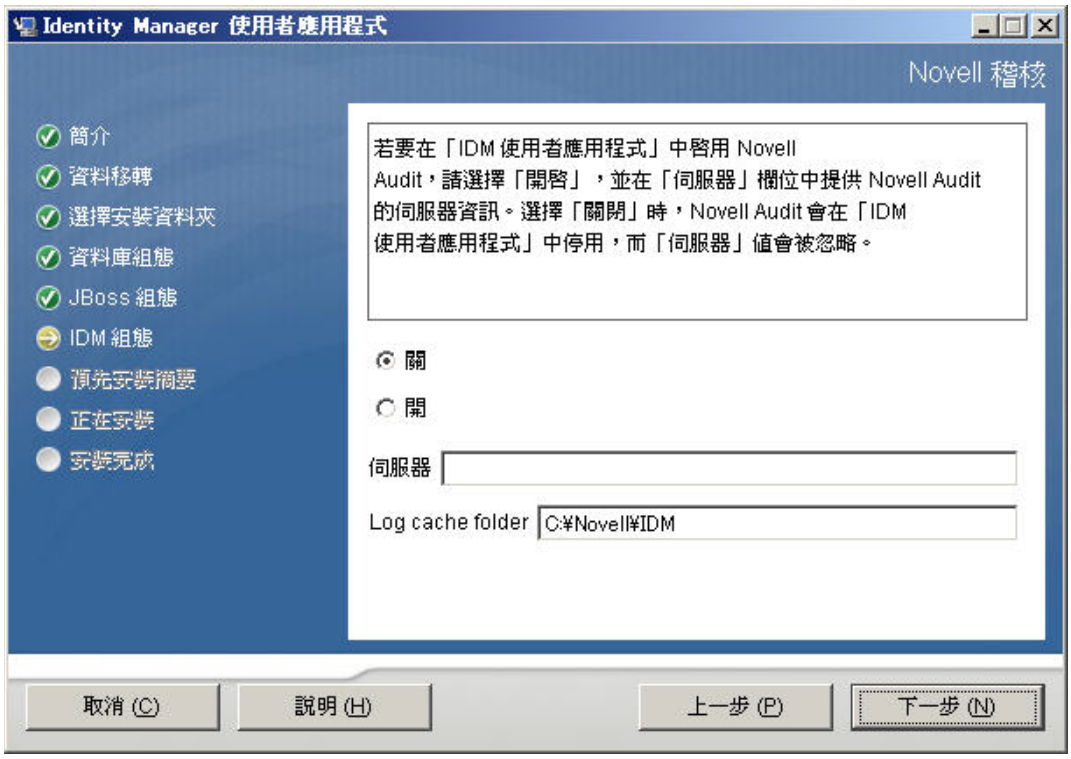


2 按「*下一步*」，然後繼續第 5.6.7 節 「啓用 Novell Audit 記錄」 (第 142 頁)。

5.6.7 啓用 Novell Audit 記錄

若要啓用「使用者應用程式」的 Novell Audit 記錄 (選擇性)：

1 填寫下列欄位：



選項	描述
關閉	停用「使用者應用程式」的 Novell Audit 記錄。您可以在稍後使用「使用者應用程式」的「*管理*」標籤來啓用它。 如需啓用 Novell Audit 記錄的相關資訊，請參閱《*Identity Manager 使用者應用程式：管理指南*》。
之中	啓用「使用者應用程式」的 Novell Audit 記錄。 如需設定 Novell Audit 記錄的相關資訊，請參閱《*Identity Manager 使用者應用程式：管理指南*》。
伺服器	如果您啓用 Novell Audit 記錄，請指定 Novell Audit 伺服器的主機名稱或 IP 位址。如果您關閉記錄，就會忽略這個值。
記錄快取資料夾	指定記錄快取的目錄。

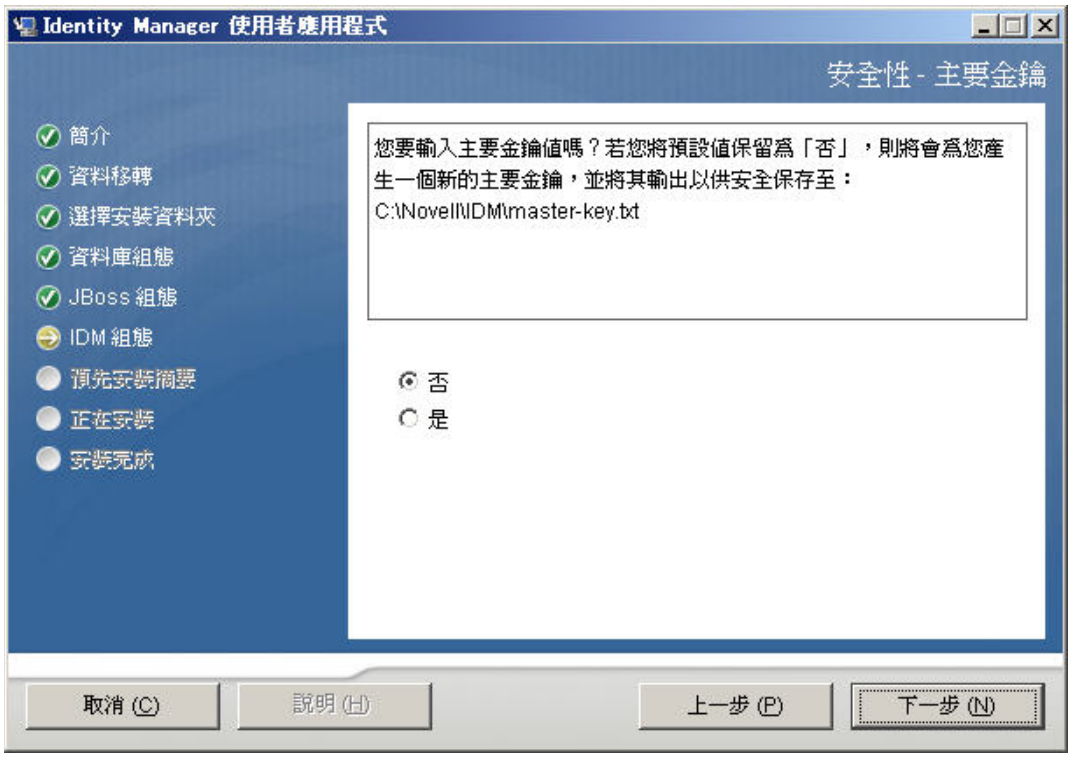
2 按一下「*下一步*」，繼續進行第 5.6.8 節 「指定萬能金鑰」 (第 143 頁)。

5.6.8 指定萬能金鑰

指定是否要輸入現有的萬能金鑰，或是要建立一個新的。需要輸入萬能金鑰的可能原因包括：

- 您想將安裝從預備系統移到生產系統，並想保留您在預備系統中使用的資料庫存取權限。
- 您之前將「使用者應用程式」安裝在 叢集的第一個成員上，而現在要安裝在叢集的後續成員上 (它們需要同一個萬能金鑰)。
- 由於磁碟發生錯誤，您必須還原「使用者應用程式」。您必須重新安裝「使用者應用程式」，並指定先前安裝所使用的同一個加密萬能金鑰。這可讓您存取之前儲存的加密資料。

1 按一下「是」來使用現有的萬能金鑰，或按一下「否」來建立一個新的



2 按一下「*下一步*」。

安裝程序會將加密萬能金鑰寫入安裝目錄中的 master-key.txt 檔案。

如果您選擇「*否*」，則請跳至第 5.6.9 節「設定使用者應用程式組態」(第 145 頁)。在完成安裝後，您必須手動記錄萬能金鑰。如果您選擇「*是*」，請繼續 步驟 3。

3 如果您選擇輸入現有的加密萬能金鑰，請剪下此金鑰並貼進安裝程序視窗。

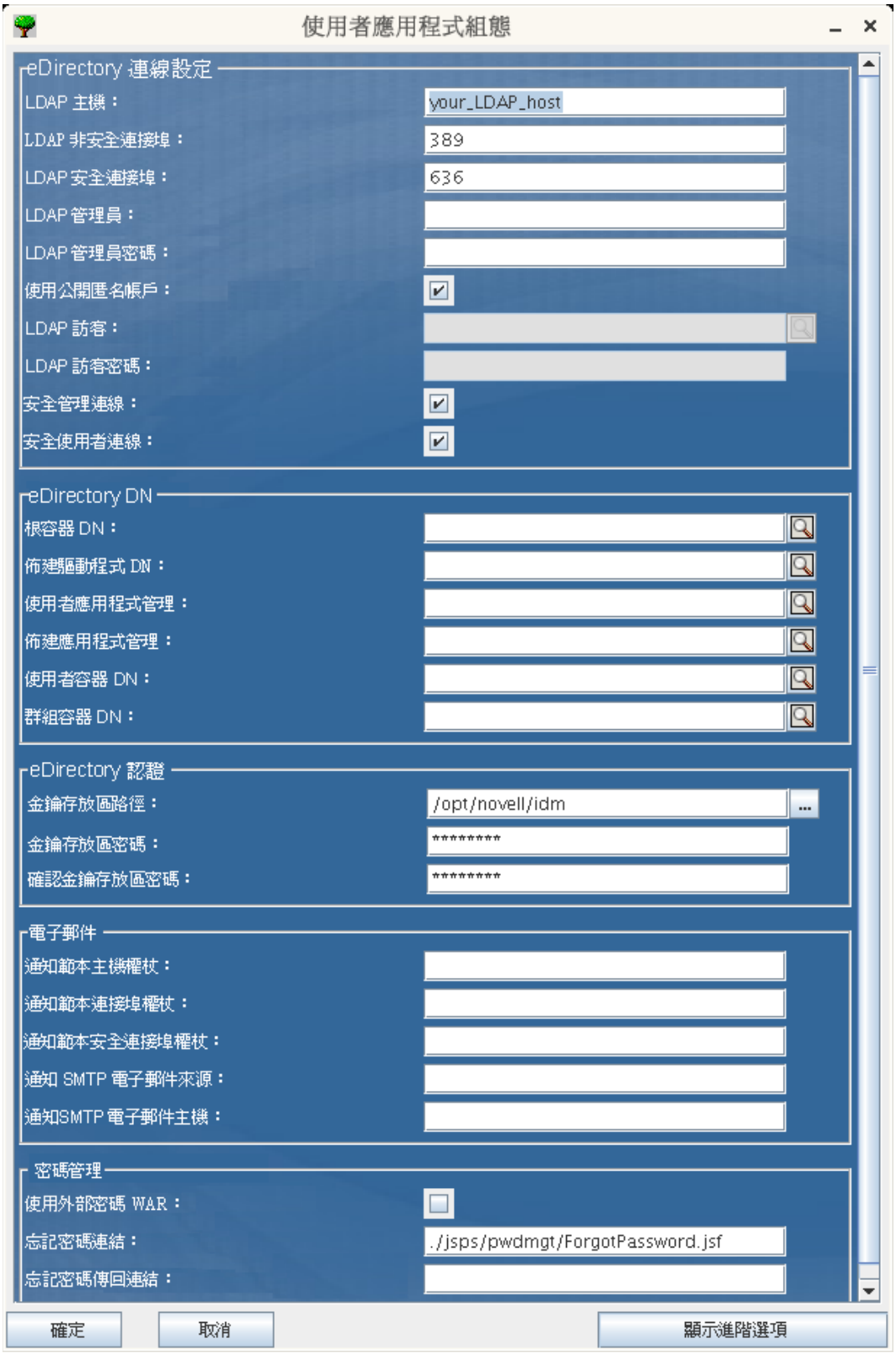
4 按一下「*下一步*」，繼續進行第 5.6.9 節 「設定使用者應用程式組態」 (第 145 頁)。

5.6.9 設定使用者應用程式組態

「使用者應用程式」的安裝可讓您設定 「使用者應用程式」組態參數。安裝之後，這些參數之中有大部分也可透過 configupdate.sh 或 configupdate.bat 進行編輯；如有例外，則於參數描述中說明。對於叢集，請爲叢集的每一個成員指定同一個 「使用者應用程式」組態參數。

1 在第一個 「使用者應用程式組態」頁面上，按一下「 *下一步*」。

2 設定表格 5-6 (第 147 頁) 所述的「使用者應用程式」基本組態參數，然後繼續進行步驟 3。



表格 5-6 *使用者應用程式組態：基本參數*

設定類型	欄位	描述
eDirectory 連線設定	*LDAP 主機*	必要。指定輕量目錄存取協定 (LDAP) 伺服器的主機名稱或 IP 位址。例如： `myLDAPhost`
	LDAP 非安全連接埠	指定 LDAP 伺服器的非安全連接埠。例如：389。
	LDAP 安全連接埠	指定 LDAP 伺服器的安全連接埠。例如： 636。
	LDAP 管理員	必要。指定 LDAP 管理員的認證。此使用者必須已經存在。「使用者應用程式」會使用此帳戶，來建立 Identity Vault 的管理連線。這個值會根據萬能金鑰進行加密。
	LDAP 管理員密碼	必要。指定 LDAP 管理員密碼。這個密碼會根據萬能金鑰進行加密。
	使用公用匿名帳戶	允許未登入的使用者存取「LDAP 公用匿名帳戶」。
	LDAP 訪客	允許未登入的使用者存取允許的入口網站應用程式。這個使用者帳戶必須已存在於 Identity Vault。若要啓用「LDAP 訪客」，您必須取消選取「*使用公用匿名帳戶*」。若要停用「訪客使用者」，請選取「*使用公用匿名帳戶*」。
	LDAP 訪客密碼	指定 LDAP 訪客密碼。
	安全管理員連線	選取這個選項來要求，必須以安全插槽完成使用管理員帳戶的所有通訊 (此選項可能有負面的效能影響)。
	安全使用者連線	選取這個選項來要求，必須以安全插槽完成使用登入使用者帳戶的所有通訊 (此選項可能有負面的效能影響)。

設定類型	欄位	描述
eDirectory DN	*根容器 DN*	必要。指定根容器的輕量目錄存取協定 (LDAP) 可辨識名稱。當在目錄抽象層中沒有指定任何搜尋根部時，會將它用做預設實體定義搜尋根部。
	提供驅動程式 DN	必要。「使用者應用程式管理員」的可辨識名稱。例如，如果您的驅動程式爲 UserApplicationDriver、而驅動程式集稱爲 myDriverSet，並且該驅動程式集位於 o=myCompany 的網路位置，則輸入值： `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`
	使用者應用程式管理員	必要。Identity Vault 中擁有權限執行管理任務 (由「使用者應用程式」使用者容器指定) 的使用者。此使用者可以使用「使用者應用程式」的「*管理*」標籤來管理入口網站。 如果「使用者應用程式管理員」參與 iManager、Novell Designer for Identity Manager 或「使用者應用程式」(「*申請與核准*」標籤) 中公開的工作流程管理任務，您就必須給予此管理員適當的託管者權限，使其能夠存取「使用者應用程式」驅動程式中的物件例項。如需詳細資訊，請參閱《*IDM 使用者應用程式：管理指南*》。 若想在部署「使用者應用程式」之後變更此指定，則必須使用「使用者應用程式」中的「*管理* > *安全性*」頁面。
	提供應用程式管理員	此角色可於 Identity Manager 3.5.1 的提供版本中取得。「提供應用程式管理員」會使用「*提供*」標籤 (在「*管理*」標籤之下) 來管理「提供工作流程」功能。這些功能可透過「使用者應用程式」的「*申請與核准*」標籤供使用者使用。此使用者必須先存在於 Identity Vault，才能指定爲「提供應用程式管理員」。 若想在部署「使用者應用程式」之後變更此指定，則必須使用「使用者應用程式」中的「*管理* > *安全性*」頁面。
eDirectory DN (續)	*使用者容器 DN*	必要。指定使用者容器的 LDAP 可辨識名稱 (DN) 或完全合法的 LDAP 名稱。這會定義使用者和群組的搜尋範圍。此容器中 (和下方) 的使用者可以登入「使用者應用程式」。 **重要：**如果您想讓使用者可以執行工作流程，請確定「使用者應用程式」驅動程式設定期間指定的「使用者應用程式管理員」存在於此容器中。

設定類型	欄位	描述
	群組容器 DN	必要。指定群組容器的輕量目錄存取協定 (LDAP) 可辨識名稱 (DN) 或完全合法的 LDAP 名稱。 由目錄抽象層內的實體定義使用。
eDirectory 證書	*KeyStore 路徑*	必要。針對應用程式伺服器用來執行之 JDK 的 KeyStore (cacerts) 檔案，輸入其完整路徑，或者，按一下瀏覽器小按鈕來瀏覽 cacerts 檔案。 在 Linux 或 Solaris 上，使用者必須擁有權限寫入此檔案。
	KeyStore 密碼 / 確認 KeyStore 密碼	必要。指定 cacerts 密碼。預設值爲「changeit」。
電子郵件	*通知範本 HOST 記號*	指定代管「Identity Manager 使用者應用程式」的應用程式伺服器。例如： `myapplication serverServer` 此值會取代電子郵件範本中的 $HOST$ 記號。建構的 URL 是提供申請任務和核准通知的連結。
	通知範本 PORT 記號	用於取代提供申請任務和核准通知中所使用之電子郵件範本中的 $PORT$ 記號。
	通知範本 SECURE PORT 記號	用於取代提供申請任務和核准通知中所使用之電子郵件範本中的 $SECURE_PORT$ 記號。
	SMTP 電子郵件通知寄件者：	指定來自提供電子郵件中使用者的電子郵件。
	SMTP 電子郵件通知主機	指定提供電子郵件所使用的 SMTP 電子郵件主機。可以是 IP 位址或 DNS 名稱。
密碼管理	*使用外部密碼 WAR*	此功能可讓您指定一個 「忘記密碼」頁面放在外部「忘記密碼 WAR」中，並指定一個 URL，讓外部「忘記密碼 WAR」用來透過 Web 服務喚回 「使用者應用程式」。 如果您核取「*使用外部密碼 WAR*」，就必須提供「*忘記密碼連結*」和「*忘記密碼回傳連結*」的值。 如果您不核取「*使用外部密碼 WAR*」，IDM 就會使用預設的內部「密碼管理」功能。/jsps/pwdmgt/ForgotPassword.jsf (開頭不使用 HTTP 通訊協定)。這會將使用者重新導向至「使用者應用程式」內建的「忘記密碼」功能，而不是外部 WAR。
	忘記密碼連結	此 URL 指向「忘記密碼」功能頁面。在外部或內部的密碼管理 WAR 中指定 ForgotPassword.jsf 檔案。
	忘記密碼回傳連結	如果您使用外部密碼管理 WAR，則請提供該外部「密碼管理 WAR」用來透過 Web 服務喚回「使用者應用程式」的路徑，例如 https://*idmhost:ssl*/*port*/idm。

3 如果您想設定「使用者應用程式」其他的組態參數，請按一下「*顯示進階選項*」(請捲動檢視整個面板)。表格 5-7 (第 150 頁) 描述了「進階選項」參數。如果您不想設定此步驟所述的其他參數，請跳至步驟 4。

表格 5-7 *使用者應用程式組態：所有參數*

設定類型	欄位	描述
eDirectory 連線設定	*LDAP 主機*	必要。指定 LDAP 伺服器的主機名稱或 IP 位址。例如： myLDAPhost
	LDAP 非安全連接埠	指定 LDAP 伺服器的非安全連接埠。例如：389。
	LDAP 安全連接埠	指定 LDAP 伺服器的安全連接埠。例如： 636。
	LDAP 管理員	必要。指定 LDAP 管理員的認證。此使用者必須已經存在。「使用者應用程式」會使用此帳戶，來建立 Identity Vault 的管理連線。這個值會根據萬能金鑰進行加密。
	LDAP 管理員密碼	必要。指定 LDAP 管理員密碼。這個密碼會根據萬能金鑰進行加密。
	使用公用匿名帳戶	允許未登入的使用者存取「LDAP 公用匿名帳戶」。
	LDAP 訪客	允許未登入的使用者存取允許的入口網站應用程式。這個使用者帳戶必須已存在於 Identity Vault。若要啓用「LDAP 訪客」，您必須取消選取「*使用公用匿名帳戶*」。若要停用「訪客使用者」，請選取「*使用公用匿名帳戶*」。
	LDAP 訪客密碼	指定 LDAP 訪客密碼。
	安全管理員連線	選取這個選項來要求，必須以安全插槽完成使用管理員帳戶的所有通訊 (此選項可能有負面的效能影響)。
	安全使用者連線	選取這個選項來要求，必須以安全插槽完成登入使用者帳戶所完成的所有通訊 (此選項可能有負面的效能影響)。

設定類型	欄位	描述
eDirectory DN	*根容器 DN*	必要。指定根容器的輕量目錄存取協定 (LDAP) 可辨識名稱。當在目錄抽象層中沒有指定任何搜尋根部時，會將它用做預設實體定義搜尋根部。
	提供驅動程式 DN	必要。「使用者應用程式管理員」的可辨識名稱。例如，如果您的驅動程式爲 userapplicationdriver、而驅動程式集稱爲 mydriverset，並且該驅動程式集位於 o=myCompany 的網路位置，則輸入值： `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`
	使用者應用程式管理員	必要。Identity Vault 中擁有權限執行管理任務 (由「使用者應用程式」使用者容器指定) 的使用者。此使用者可以使用「使用者應用程式」的「*管理*」標籤來管理入口網站。 如果「使用者應用程式管理員」參與 iManager、Novell Designer for Identity Manager 或「使用者應用程式」(「*申請與核准*」標籤) 中公開的工作流程管理任務，您就必須給予此管理員適當的託管者權限，使其能夠存取「使用者應用程式」驅動程式中的物件例項。如需詳細資訊，請參閱《*IDM 使用者應用程式：管理指南*》。 若想在部署「使用者應用程式」之後變更此指定，則必須使用「使用者應用程式」中的「*管理* > *安全性*」頁面。
	提供應用程式管理員	此角色可於 Identity Manager 3.5.1 的提供版本中取得。「提供應用程式管理員」會使用「使用者應用程式」的「*申請與核准*」標籤來管理「提供工作流程」功能。此使用者必須先存在於 Identity Vault，才能指定爲「提供應用程式管理員」。 若想在部署「使用者應用程式」之後變更此指定，則必須使用「使用者應用程式」中的「*管理* > *安全性*」頁面。

設定類型	欄位	描述
中繼目錄使用者身分	*使用者容器 DN*	必要。指定使用者容器的 LDAP 可辨識名稱 (DN) 或完全合法的 LDAP 名稱。 這會定義使用者和群組的搜尋範圍。 此容器中 (和下方) 的使用者可以登入「使用者應用程式」。 **重要：**如果您想讓使用者可以執行工作流程，請確定「使用者應用程式」驅動程式設定期間指定的「使用者應用程式管理員」存在於此容器中。
	使用者物件類別	LDAP 使用者物件類別 (通常爲 inetOrgPerson)。
	登入屬性	代表使用者登入名稱的 LDAP 屬性 (例如 CN)。
	命名屬性	此 LDAP 可在查閱使用者或群組時做爲識別碼。這和登入屬性不一樣，後者只能用於登入，不可用於使用者 / 群組搜尋。
	使用者成員資格屬性	選用。代表使用者群組成員資格的 LDAP 屬性。請勿在此名稱中使用空格。
中繼目錄使用者群組	*群組容器 DN*	必要。指定群組容器的輕量目錄存取協定 (LDAP) 可辨識名稱 (DN) 或完全合法的 LDAP 名稱。由目錄抽象層內的實體定義使用。
	群組物件類別	LDAP 群組物件類別 (通常爲 groupofNames)。
	群組成員資格屬性	代表使用者群組成員資格的屬性。請勿在此名稱中使用空格。
	使用動態群組	如果您想要使用動態群組，請選取此選項。
	動態群組物件類別	LDAP 動態群組物件類別 (通常爲 dynamicGroup)。
eDirectory 證書	*KeyStore 路徑*	必要。針對應用程式伺服器用來執行之 JRE 的 keystore (cacerts) 檔案，輸入其完整路徑，或者，按一下瀏覽器小按鈕來瀏覽 cacerts 檔案。 「使用者應用程式」的安裝會修改 KeyStore 檔案。在 Linux 或 Solaris 上，使用者必須擁有權限寫入此檔案。
	KeyStore 密碼 *確認 KeyStore 密碼*	必要。指定 cacerts 密碼。預設值爲「changeit」。

設定類型	欄位	描述
私密金鑰儲存區	*私密 KeyStore 路徑*	私密 KeyStore 含有「使用者應用程式」的私密金鑰和證書。保留。如果您想保留空白，此路徑則預設爲 /jre/lib/security/cacerts。
	私密 KeyStore 密碼	除非您另行指定，否則密碼爲 changeit。這個密碼會根據萬能金鑰進行加密。
	私密金鑰別名	除非您另行指定，否則密碼爲 novellIDMUserApp。
	私密金鑰密碼	除非您另行指定，否則密碼爲 nove1IIDM。這個密碼會根據萬能金鑰進行加密。
託管金鑰儲存區	*託管儲存區路徑*	「託管金鑰儲存區」包含所有託管簽名者的證書，用來驗證數位簽名。如果此路徑爲空，則「使用者應用程式」會從「系統」內容 javax.net.ssl.trustStore 取得路徑。如果路徑不在那裡，就假設爲 jre/lib/security/cacerts。
	託管儲存區密碼	如果此欄位爲空，則「使用者應用程式」會從「系統」內容 javax.net.ssl.trustStorePassword 取得密碼。如果值不在那裡，則使用 changeit。這個密碼會根據萬能金鑰進行加密。
Novell Audit 數位簽名和證書金鑰		包含 Novell Audit 的數位簽名金鑰和證書。
	Novell Audit 數位簽名證書	顯示數位簽名證書。
	Novell Audit 數位簽名私密金鑰	顯示數位簽名私密金鑰。這個金鑰會根據萬能金鑰進行加密。
iChain 設定	*已啓用 ICS 登出*	若選取此選項，「使用者應用程式」就可支援同時登出「使用者應用程式」以及 iChain 或 Novell Access Manager。「使用者應用程式」會在登出時檢查是否有 iChain 或 Novell Access Manager 的 Cookie，如果有，就將使用者重新導向到 ICS 登出頁面。
	ICS 登出頁面	連結至 iChain 或 Novell Access Manager 登出頁面的 URL，其中的 URL 是 iChain 或 Novell Access Manager 需要的主機名稱。如果 ICS 登入已經啓用，且使用者登出了「使用者應用程式」，則該使用者會被重新導向至此頁面。

設定類型	欄位	描述
電子郵件	*通知範本 HOST 記號*	指定代管「Identity Manager 使用者應用程式」的應用程式伺服器。例如： `myapplication serverServer` 此值會取代電子郵件範本中的 $HOST$ 記號。建構的 URL 是提供申請任務和核准通知的連結。
	通知範本 PORT 記號	用於取代提供申請任務和核准通知中所使用之電子郵件範本中的 $PORT$ 記號。
	通知範本 SECURE PORT 記號	用於取代提供申請任務和核准通知中所使用之電子郵件範本中的 $SECURE_PORT$ 記號。
	通知範本 PROTOCOL 記號	指的是非安全通訊協定 HTTP。用於取代提供申請任務和核准通知中所使用之電子郵件範本中的 $PROTOCOL$ 記號。
	通知範本 SECURE PROTOCOL 記號	指的是安全通訊協定 HTTPS。用於取代提供申請任務和核准通知中所使用之電子郵件範本中的 $SECURE_PROTOCOL$ 記號。
	SMTP 電子郵件通知寄件者：	指定來自提供電子郵件中使用者的電子郵件。
	SMTP 電子郵件通知主機	指定提供電子郵件所使用的 SMTP 電子郵件主機。可以是 IP 位址或 DNS 名稱。
密碼管理		
	使用外部密碼 WAR	此功能可讓您指定一個「忘記密碼」頁面放在外部「忘記密碼 WAR」中，並指定一個 URL，讓外部「忘記密碼 WAR」用來透過 Web 服務喚回「使用者應用程式」。 如果您核取「*使用外部密碼 WAR*」，就必須提供「*忘記密碼連結*」和「*忘記密碼回傳連結*」的值。 如果您不核取「*使用外部密碼 WAR*」，IDM 就會使用預設的內部「密碼管理」功能。/jsps/pwdmgt/ForgotPassword.jsf (開頭不使用 HTTP 通訊協定)。這會將使用者重新導向至「使用者應用程式」內建的「忘記密碼」功能，而不是外部 WAR。
	忘記密碼連結	此 URL 指向「忘記密碼」功能頁面。在外部或內部的密碼管理 WAR 中指定 ForgotPassword.jsf 檔案。
	忘記密碼回傳連結	如果您使用外部密碼管理 WAR，則請提供該外部「密碼管理 WAR」用來透過 Web 服務喚回「使用者應用程式」的路徑，例如 https://*idmhost:sslport*/idm。

設定類型	欄位	描述
其他	*會期逾時*	應用程式會期逾時。
	OCSP URI	如果用戶端安裝使用線上證書狀態通訊協定 (On-Line Certificate Status Protocol，OCSP)，則請提供資源識別字串 (Uniform Resource Identifier，URI)。例如，格式爲 http://host:port/ocspLocal。OCSP URI 會在線上更新託管證書的狀態。
	授權組態路徑	授權組態檔案的完全合法名稱。
	建立 eDirectory 索引	
	伺服器 DN	
容器物件	*選取*	選取要使用的「容器物件類型」。
	容器物件類型	從下列的標準容器中進行選取：地區、國家、organizationalUnit 和領域。您也可以在 iManager 中定義自己的容器，然後將其新增至「*新增新容器物件*」之下。
	容器屬性名稱	列出與「容器物件類型」關聯的「屬性類型」名稱。
	新增新容器物件：容器物件類型	在 Identity Vault 中指定一個可做爲容器的 ObjectClass 之 LDAP 名稱。 如需有關容器的詳細資訊，請參閱《*Novell iManager 2.6 管理指南 (http://www.novell.com/documentation/imanager26/pdfdoc/imanager_admin_26/imanager_admin_26.pdf)*》
	新增新容器物件：容器屬性名稱	提供容器物件的屬性名稱。

4 完成設定後，請按一下「*確定*」，然後繼續進行第 5.6.10 節 「確認選擇並安裝」 (第 155 頁)

5.6.10 確認選擇並安裝

1 閱讀 「預先安裝摘要」頁面，確認您選擇的安裝參數。

2 *如有必要，請使用 「上一步」，返回先前的安裝頁面變更安裝參數。*

「使用者應用程式」組態頁面不會儲存這些值，因此在您重新指定先前的安裝頁面時，請務必重新輸入 「使用者應用程式」的組態值。

3 對安裝和組態參數感到滿意之後，請返回 「預先安裝摘要」頁面並按一下 「*安裝*」。請繼續進行第 5.6.11 節 「檢視記錄檔案」 (第 156 頁)。

5.6.11 檢視記錄檔案

如果安裝完成時未發生任何錯誤，請移至第 5.6.12 節 「新增使用者應用程式組態檔和 JVM 系統內容」(第 156 頁)。

如果安裝發生錯誤或警告，請檢閱記錄檔案來找出問題。

- Identity_Manager_User_Application_Installlog.log 中保留基本安裝工作的結果
- Novell-Custom-Install.log 會存放 「使用者應用程式」在安裝期間的組態資訊。

5.6.12 新增使用者應用程式組態檔和 JVM 系統內容

1. 將 「使用者應用程式」安裝目錄中的 sys-configuration-xmldata.xml 檔案，複製到代管 WebSphere 伺服器的機器上的目錄，例如 /UserAppConfigFiles。「使用者應用程式」安裝目錄是您安裝 「使用者應用程式」所在的目錄。
2. 將路徑設定到 JVM 系統內容中的 sys-configuration-xmldata.xml 檔案。以 admin 使用者身分登入 WebSphere 管理主控台。
3. 從左面板中，移至 「*伺服器* > *應用程式伺服器*」
4. 在伺服器清單中的伺服器名稱上按一下，例如 server1。
5. 在右面板的設定清單中，移至 「*伺服器基礎結構*」中的 「*Java 和程序管理*」。
6. 展開連結，選取 「*程序定義*」。
7. 在 「*額外內容*」清單下，選取 「*Java 虛擬機器*」。
8. 選取 JVM 頁面 「*額外內容*」標題下的 「*自訂內容*」。
9. 按一下 「*新增*」以新增新的 JVM 系統內容。

9a 爲「*名稱*」指定 extend.local.config.dir。

9b 爲「*值*」指定目錄，例如 /UserAppConfigFiles，您在此目錄中複製 sys-configuration-xmldata.xml 檔案。

9c 爲「*描述*」指定內容的描述，例如「到 sys-configuration-xmldata.xml 的路徑」。

9d 按一下*確定*來儲存變更。

10 按一下「*新增*」以新增另一個新 JVM 系統內容。

10a 爲「*名稱*」指定 idmuserapp.logging.config.dir。

10b 爲「*值*」指定目錄，例如 /UserAppConfigFiles，您在此目錄中複製 sys-configuration-xmldata.xml 檔案。

10c 爲「*描述*」指定內容的描述，例如「到 sys-configuration-xmldata.xml 的路徑」。

10d 按一下*確定*來儲存變更。

附註：idmuserapp-logging.xml 檔案不需要存在於這個目錄中。當記錄組態變更時，便會建立這個檔案。

---

11 請繼續執行下一小節第 5.6.13 節「將 eDirectory 託管根部匯入至 WebSphere keystore」(第 157 頁)。

5.6.13 將 eDirectory 託管根部匯入至 WebSphere keystore

1 「使用者應用程式」安裝程序將 eDirectory 託管根部證書匯出到您安裝「使用者應用程式」所在的目錄。將這些證書複製到代管 WebSphere 伺服器的機器上。

2 將證書匯入至 WebSphere keystore。您可以使用 WebSphere 管理主控台 (「使用 WebSphere 管理主控台匯入證書」(第 157 頁)) 或透過指令行 (「以指令行匯入證書。」(第 157 頁)) 來完成。

3 匯入證書後，繼續進行第 5.6.14 節「部署 IDM WAR 檔」(第 158 頁)。

使用 WebSphere 管理主控台匯入證書

1 以 admin 使用者身分登入 websphere 管理主控台。

2 從左面板中，移至「*安全性* > *SSL 證書和金鑰管理*」。

3 在右側的設定清單中，移至「*額外內容*」下的「*Keystore 和證書*」。

4 選取「*NodeDefaultTrustStore*」(或您目前使用託管區)。

5 在右側的「*額外內容*」中，選取「*簽署者證書*」。

6 按一下「*新增*」。

7 輸入別名和到證書檔案的完整路徑。

8 將下拉式清單中的「資料」類型變更爲「*二進位 DER 資料*」。

9 按一下「*確定*」。您現在應該會在簽署者證書清單中看到證書。

以指令行匯入證書。

1 從託管 WebSphere 伺服器的機器上的指令行，執行金鑰工具將證書匯入至 WebSphere keystore。

附註：您必須使用 WebSphere 金鑰工具，否則這功能無法作用。此外，請確定 store 類型爲 PKCS12。

WebSphere 金鑰工具位於 /IBM/WebSphere/AppServer/java/bin。

金鑰工具指令範例

keytool -import -trustcacerts -file servercert.der -alias myserveralias -keystore trust.p12 -storetype PKCS12

如果您的系統上有多個 trust.p12，您必須指定到檔案的完整路徑。

5.6.14 部署 IDM WAR 檔

1. 以 admin 使用者身分登入 websphere 管理主控台。
2. 在左面板中，移至「*應用程式* > *安裝新應用程式*」
3. 瀏覽至 IDM War 的檔案位置 (IDM WAR 檔案是在安裝「使用者應用程式」期間設定的，它位在您安裝「使用者應用程式」期間，所指定的「使用者應用程式」安裝目錄中)。
4. 輸入應用程式的內部根部，例如 IDMProv。這將會是 URL 路徑。
5. 確定「*只有在需要額外資料時提示我*」已選取，再按一下「*下一步*」移至「*選取安裝選項*」頁面。
6. 接受此頁面的預設值，並按一下「*下一步*」移至「*對應模組至伺服器*」畫面。
7. 將此頁面上的所有設定均保留爲預設值，並按一下「*下一步*」移至「*對應資源參考至資源*」頁面。
8. 對於驗證模式，請選取「*使用者預設方法*」核取方塊。接著，在「*驗證資料輸入*」下拉清單中，選取您先前建立的別名，例如 MyServerNode01/MyAlias。
9. 在驗證設定下方的表格中，找到您在部署的模組。在「目標資源 JNDI 名稱」欄下，按一下瀏覽按鈕來指定 JNDI 名稱。這會帶出資源清單。選取您先前建立的資料來源，並按一下「*套用*」按鈕回到「對應資源參考至資源」頁面，例如 MyDataSource。
10. 選取「*下一步*」移至「*對應 Web 模組的虛擬主機*」頁面。
11. 將這張頁面的所有設定保留爲預設值，並按一下「*下一步*」移至「*摘要*」頁面。
12. 按一下「*完成*」以完成指定。
13. 完成部署後，按一下「*儲存*」儲存變更。
14. 請繼續進行第 5.6.15 節「啓動應用程式」(第 158 頁)。

5.6.15 啓動應用程式

1. 以 admin 使用者登入 WebSphere 管理主控台。
2. 在左導覽面板中，移至「*應用程式* > *企業應用程式*」。
3. 選取您要啓動的應用程式旁的核取方塊，再按一下「*開始*」。

   啓動後，「*應用程式狀態*」欄會顯示綠色箭頭。

5.6.16 存取「使用者應用程式入口網站」

1 使用您在部署期間指定的內容來存取入口網站。

WebSphere 上 Web 容器的預設連接埠是 9080，或是 9443 安全連接埠。日期的格式爲：

http:// <*server*>:9080/IDMProv

5.7 從主控台介面安裝使用者應用程式

本節說明如何使用安裝程式的主控台 (指令行) 來安裝「Identity Manager 使用者應用程式」。

1 取得表格 5-2 (第 106 頁) 中所描述的適當安裝檔案。

2 登入並開啓終端機會期。

3 使用以下指令，爲含有 Javae 的平台啓動安裝程式：

java -jar IdmUserApp.jar -i console

4 請依照第 5.5 節「從安裝 GUI 將「使用者應用程式」安裝在 JBoss 應用程式伺服器上」(第 107 頁) 下所述的圖形使用者介面執行相同的步驟，閱讀指令行的提示並在指令行中輸入回應，然後繼續執行萬能金鑰的輸入或建立步驟。

5 若要設定「使用者應用程式」組態參數，您必須手動啓動 configupdate 公用程式。在指令行中輸入 configupdate.sh (Linux 或 Solaris) 或 configupdate.bat (Windows)，然後填入第 5.5.14 節「設定使用者應用程式組態」(第 122 頁) 中所述的值。

6 如果您使用外部密碼管理 WAR，則請手動將其複製到安裝目錄以及負責執行外部密碼 WAR 功能的遠端 JBoss 伺服器部署目錄中。

7 請繼續進行第 5.9 節「安裝後任務」(第 164 頁)。

5.8 使用單一指令安裝使用者應用程式

本節說明如何進行無訊息安裝。無訊息安裝期間不需要任何互動，可節省您的時間，當您必須在一個以上的系統上進行安裝時更是如此。Linux 和 Solaris 可支援無訊息安裝。

1 取得表格 5-2 (第 106 頁) 中所列的適當安裝檔案。

2 登入並開啓終端機會期。

3 找到 IDM 內容檔案 silent.properties 的位置，此檔案隨附於安裝檔案中。如果您從光碟進行，請製作此檔案的本機副本。

4 編輯 silent.properties 來提供您的安裝參數以及「使用者應用程式」組態參數。

請檢視 silent.properties 檔案中各個安裝參數的範例。安裝參數與您在 GUI 或「主控台」安裝程序中設定的安裝參數相對應。

如需「使用者應用程式」各個組態參數的描述，請參閱表格 5-8。「使用者應用程式」組態參數與您在 GUI 或「主控台」安裝程序中設定的參數相同，或與 configupdate 公用程式的相同。

5 啓動無訊息安裝，如下所示：

java -jar IdmUserApp.jar -i silent -f / *yourdirectorypath*/silent.properties

如果 silent.properties 的所在目錄與安裝程式程序檔的不同，則請輸入該檔案的完整路徑。程序檔會將必要的檔案解壓縮至暫存目錄，然後啓動無訊息安裝。

表格 5-8 無訊息安裝的使用者應用程式組態參數

silent.properties 中的使用者應用程式參數名稱	使用者應用程式組態參數檔案中的相等參數和描述
NOVL_CONFIG_LDAPHOST=	eDirectory 連線設定：LDAP 主機。必要。指定 LDAP 伺服器的主機名稱或 IP 位址。
NOVL_CONFIG_LDAPADMIN=	必要。指定 LDAP 管理員的認證。此使用者必須已經存在。「使用者應用程式」會使用此帳戶，來建立 Identity Vault 的管理連線。這個值會根據萬能金鑰進行加密。
NOVL_CONFIG_LDAPADMINPASS=	eDirectory 連線設定：LDAP 管理員密碼。必要。指定 LDAP 管理員密碼。這個密碼會根據萬能金鑰進行加密。
NOVL_CONFIG_ROOTCONTAINERNAME=	eDirectory DN：根容器 DN。必要。指定根容器的輕量目錄存取協定 (LDAP) 可辨識名稱。當在目錄抽象層中沒有指定任何搜尋根部時，會將它用做預設實體定義搜尋根部。
NOVL_CONFIG_PROVISIONROOT=	eDirectory DN：提供驅動程式 DN。必要。指定您先前在第 5.3 節「建立「使用者應用程式」驅動程式」(第 100 頁) 中建立之「使用者應用程式」驅動程式的可辨識名稱。例如，如果您的驅動程式爲 userapplicationdriver、而驅動程式集稱爲 mydriverset，並且該驅動程式集位於 o=myCompany 的網路位置，則輸入值： `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`
NOVL_CONFIG_LOCKSMITH=	eDirectory DN：使用者應用程式管理員。必要。Identity Vault 中擁有權限執行管理任務 (由「使用者應用程式」使用者容器指定) 的使用者。此使用者可以使用「使用者應用程式」的「*管理*」標籤來管理入口網站。 如果「使用者應用程式管理員」參與 iManager、Novell Designer for Identity Manager 或「使用者應用程式」(「*申請與核准*」標籤) 中公開的工作流程管理任務，您就必須給予此管理員適當的託管者權限，使其能夠存取「使用者應用程式」驅動程式中的物件例項。如需詳細資訊，請參閱《*IDM 使用者應用程式：管理指南*》。 若想在部署「使用者應用程式」之後變更此指定，則必須使用「使用者應用程式」中的「*管理* > *安全性*」頁面。

silent.properties 中的使用者應用程式參數名稱	使用者應用程式組態參數檔案中的相等參數和描述
NOVL_CONFIG_PROVLOCKSMITH=	eDirectory DNs：提供應用程式管理員。此角色可於 Identity Manager 3.5.1 的提供版本中取得。「提供應用程式管理員」會使用「*提供*」標籤 (在「*管理*」標籤之下) 來管理「提供工作流程」功能。這些功能可透過「使用者應用程式」的「*申請與核准*」標籤供使用者使用。此使用者必須先存在於 Identity Vault，才能指定爲「提供應用程式管理員」。 若想在部署「使用者應用程式」之後變更此指定，則必須使用「使用者應用程式」中的「*管理* > *安全性*」頁面。
NOVL_CONFIG_USERCONTAINERDN=	中繼目錄使用者身分：使用者容器 DN。必要。指定使用者容器的 LDAP 可辨識名稱 (DN) 或完全合法的 LDAP 名稱。這會定義使用者和群組的搜尋範圍。此容器中 (和下方) 的使用者可以登入「使用者應用程式」。 **重要：**如果您想讓使用者可以執行工作流程，請確定「使用者應用程式」驅動程式設定期間指定的「使用者應用程式管理員」存在於此容器中。
NOVL_CONFIG_GROUPCONTAINERDN=	中繼目錄使用者群組：群組容器 DN。必要。指定群組容器的輕量目錄存取協定 (LDAP) 可辨識名稱 (DN) 或完全合法的 LDAP 名稱。由目錄抽象層內的實體定義使用。
NOVL_CONFIG_KEYSTOREPATH=	eDirectory 證書：KeyStore 路徑。必要。針對應用程式伺服器用來執行之 JRE 的 KeyStore (cacerts) 檔案，輸入其完整路徑。「使用者應用程式」的安裝會修改 KeyStore 檔案。在 Linux 或 Solaris 上，使用者必須擁有權限寫入此檔案。
NOVL_CONFIG_KEYSTOREPASSWORD=	eDirectory 證書：KeyStore 密碼。必要。指定 cacerts 密碼。預設值爲「changeit」。
NOVL_CONFIG_SECUREADMINCONNECTION=	eDirectory 連線設定：安全管理員連線。 指定 True 來要求，必須以安全插槽完成使用管理員帳戶的所有通訊 (此選項可能有負面的效能影響)。 如果管理員帳戶沒有使用安全插槽通訊，則指定 False。
NOVL_CONFIG_SECUREUSERCONNECTION=	eDIRECTORY 連線設定：安全使用者連線。 指定 True 來要求，必須以安全插槽完成登入使用者帳戶所完成的所有通訊 (此選項可能有負面的效能影響)。 如果使用者的帳戶沒有使用安全插槽通訊，則指定 False。
NOVL_CONFIG_SESSIONTIMEOUT=	其他：會期逾時。指定應用程式會期逾時間隔。
NOVL_CONFIG_LDAPPLAINPORT=	eDirectory 連線設定：LDAP 非安全連接埠。指定 LDAP 伺服器的非安全連接埠，例如 389。

silent.properties 中的使用者應用程式參數名稱	使用者應用程式組態參數檔案中的相等參數和描述
NOVL_CONFIG_LDAPSECUREPORT=	eDirectory 連線設定：LDAP 安全連接埠。指定 LDAP 伺服器的安全連接埠，例如 636。
NOVL_CONFIG_ANONYMOUS=	eDirectory 連線設定：使用公用匿名帳戶。 指定 True，允許未登入的使用者存取「LDAP 公用匿名帳戶」。 指定 False，改爲啓用 NOVL_CONFIG_GUEST。
NOVL_CONFIG_GUEST=	eDirectory 連線設定：LDAP 訪客。允許未登入的使用者存取允許的入口網站應用程式。您必須取消選取「*使用公用匿名帳戶*」。這個訪客使用者帳戶必須已存在於 Identity Vault。若要停用訪客使用者，請選取「*使用公用匿名帳戶*」。
NOVL_CONFIG_GUESTPASS=	eDirectory 連線設定：LDAP 訪客密碼。
NOVL_CONFIG_EMAILNOTIFYHOST=	電子郵件：通知範本 HOST 記號。指定代管「Identity Manager 使用者應用程式」的應用程式伺服器。例如： `myapplication serverServer` 此值會取代電子郵件範本中的 $HOST$ 記號。建構的 URL 是提供申請任務和核准通知的連結。
NOVL_CONFIG_EMAILNOTIFYPORT=	電子郵件：通知範本 PORT 記號。用於取代提供申請任務和核准通知中所使用之電子郵件範本中的 $PORT$ 記號。
NOVL_CONFIG_EMAILNOTIFYSECUREPORT=	電子郵件：通知範本 SECURE PORT 記號。用於取代提供申請任務和核准通知中所使用之電子郵件範本中的 $SECURE_PORT$ 記號。
NOVL_CONFIG_NOTFSMTPEMAILFROM=	電子郵件：SMTP 電子郵件通知寄件者。指定來自提供電子郵件中使用者的電子郵件。
NOVL_CONFIG_NOTFSMTPEMAILHOST=	電子郵件：SMTP 電子郵件通知主機。指定提供電子郵件所使用的 SMTP 電子郵件主機。可以是 IP 位址或 DNS 名稱。
NOVL_CONFIG_USEEXTPWDWAR=	密碼管理：使用外部密碼 WAR。 如果您使用外部密碼管理 WAR，請指定 True。如果您指定 True，就必須同時提供 *NOVL_CONFIG_EXTPWDWARPTH* 和 *NOVL_CONFIG_EXTPWDWARRTNPATH* 的值。 指定 False，使用預設的內部「密碼管理」功能。/jsps/pwdmgt/ForgotPassword.jsf (開頭不使用 HTTP 通訊協定)。這會將使用者重新導向至「使用者應用程式」內建的「忘記密碼」功能，而不是外部 WAR。
NOVL_CONFIG_EXTPWDWARPATH=	密碼管理：忘記密碼連結。在外部或內部的密碼管理 WAR 中指定「忘記密碼」功能頁面 ForgotPassword.jsf 的 URL。或者，接受預設的內部密碼管理 WAR。如需詳細資料，請參閱「使用密碼 WAR」(第 132 頁)。

silent.properties 中的使用者應用程式參數名稱	使用者應用程式組態參數檔案中的相等參數和描述
NOVL_CONFIG_EXTPWDWARRTNPATH=	密碼管理：忘記密碼回傳連結。如果您使用外部密碼管理 WAR，則請提供該外部「密碼管理 WAR」用來透過 Web 服務喚回「使用者應用程式」的路徑，例如 https://*idmhost:sslport*/idm。
NOVL_CONFIG_USEROBJECTATTRIBUTE=	中繼目錄使用者身分：使用者物件類別。LDAP 使用者物件類別 (通常爲 inetOrgPerson)。
NOVL_CONFIG_LOGINATTRIBUTE=	中繼目錄使用者身分：登入屬性。代表使用者登入名稱的 LDAP 屬性 (例如 CN)。
NOVL_CONFIG_NAMINGATTRIBUTE=	中繼目錄使用者身分：命名屬性。此 LDAP 可在查閱使用者或群組時做爲識別碼。這和登入屬性不一樣，後者只能用於登入，不可用於使用者 / 群組搜尋。
NOVL_CONFIG_USERMEMBERSHIPATTRIBUTE=	中繼目錄使用者身分：使用者成員資格屬性。選用。代表使用者群組成員資格的 LDAP 屬性。請勿在此名稱中使用空格。
NOVL_CONFIG_GROUPOBJECTATTRIBUTE=	中繼目錄使用者群組：群組物件類別。LDAP 群組物件類別 (通常爲 groupofNames)。
NOVL_CONFIG_GROUPMEMBERSHIPATTRIBUTE=	中繼目錄使用者群組：群組成員資格屬性。指定代表使用者群組成員資格的屬性。請勿在此名稱中使用空格。
NOVL_CONFIG_USEDYNAMICGROUPS=	中繼目錄使用者群組：使用動態群組。指定 True，使用動態群組。否則，請指定 False。
NOVL_CONFIG_DYNAMICGROUPOBJECTCLASS=	中繼目錄使用者群組：動態群組物件類別。指定 LDAP 動態群組物件類別 (通常爲 dynamicGroup)。
NOVL_CONFIG_PRIVATESTOREPATH=	私密金鑰儲存區：私密 KeyStore 路徑。針對含有「使用者應用程式」的私密金鑰和證書的私密 KeyStore，指定其路徑。保留。如果您想保留空白，此路徑則預設爲 /jre/lib/security/cacerts。
NOVL_CONFIG_PRIVATESTOREPASSWORD=	私密金鑰儲存區：私密 KeyStore 密碼。
NOVL_CONFIG_PRIVATEKEYALIAS=	私密金鑰儲存區：私密金鑰別名。除非您另行指定，否則密碼爲 novellIDMUserApp。
NOVL_CONFIG_PRIVATEKEYPASSWORD=	私密金鑰儲存區：私密金鑰密碼。
NOVL_CONFIG_TRUSTEDSTOREPATH=	託管金鑰儲存區：託管儲存區路徑。「託管金鑰儲存區」包含所有託管簽名者的證書，用來驗證數位簽名。如果此路徑爲空，則「使用者應用程式」會從「系統」內容 javax.net.ssl.trustStore 取得路徑。如果路徑不在那裡，就假設爲 jre/lib/security/cacerts。
NOVL_CONFIG_TRUSTEDSTOREPASSWORD=	託管金鑰儲存區：託管儲存區密碼。
NOVL_CONFIG_AUDITCERT=	Novell Audit 數位簽名證書
NOVL_CONFIG_AUDITKEYFILEPATH=	Novell Audit 數位簽名私密金鑰檔案路徑

silent.properties 中的使用者應用程式參數名稱	使用者應用程式組態參數檔案中的相等參數和描述
NOVL_CONFIG_ICSLOGOUTENABLED=	iChain 設定：已啓用 ICS 登出。 指定 True，可同時登出「使用者應用程式」以及 iChain 或 Novell Access Manager。「使用者應用程式」會在登出時檢查是否有 iChain 或 Novell Access Manager 的 Cookie，如果有，就將使用者重新導向到 ICS 登出頁面。 指定 False，停用同步登出功能。
NOVL_CONFIG_ICSLOGOUTPAGE=	iChain 設定：ICS 登出頁面。指定 URL，連結至 iChain 或 Novell Access Manager 登出頁面，其中的 URL 是 iChain 或 Novell Access Manager 需要的主機名稱。如果 ICS 登入已經啓用，且使用者登出了「使用者應用程式」，則該使用者會被重新導向至此頁面。
NOVL_CONFIG_EMAILNOTIFYPROTOCOL=	電子郵件：通知範本 PROTOCOL 記號。指的是非安全通訊協定 HTTP。用於取代提供申請任務和核准通知中所使用之電子郵件範本中的 $PROTOCOL$ 記號。
NOVL_CONFIG_EMAILNOTIFYSECUREPROTOCOL=	電子郵件：通知範本 SECURE PORT 記號。
NOVL_CONFIG_OCSPURI=	其他：OCSP URI。如果用戶端安裝使用線上證書狀態通訊協定 (On-Line Certificate Status Protocol，OCSP)，則請提供資源識別字串 (Uniform Resource Identifier，URI)。例如，格式爲 http://hstport/ocspLocal。OCSP URI 會在線上更新託管證書的狀態。
NOVL_CONFIG_AUTHCONFIGPATH=	其他：授權組態路徑。授權組態檔案的完全合法名稱。

5.9 安裝後任務

安裝和設定「使用者應用程式」以後，請處理安裝後任務。

- 第 5.9.1 節「記錄萬能金鑰」(第 165 頁)
- 第 5.9.2 節「檢查您的叢集安裝」(第 165 頁)
- 第 5.9.3 節「設定 JBoss 伺服器之間的 SSL 通訊」(第 165 頁)
- 第 5.9.4 節「存取外部密碼 WAR」(第 166 頁)
- 第 5.9.5 節「更新忘記密碼設定」(第 166 頁)
- 第 5.9.6 節「設定電子郵件通知」(第 166 頁)
- 第 5.9.7 節「測試 JBoss 應用程式伺服器上的安裝」(第 167 頁)
- 第 5.9.8 節「設定提供小組及其要求」(第 168 頁)
- 第 5.9.9 節「在 eDirectory 中建立索引」(第 168 頁)

5.9.1 記錄萬能金鑰

安裝之後，請立即複製加密萬能金鑰，並將其記錄在安全的地方。

1. 在安裝目錄中開啓 master-key.txt 檔案。
2. 將加密萬能金鑰複製到安全的地方，供系統失敗時取用。

警告：請永遠保存一份加密萬能金鑰。如果萬能金鑰遺失 (例如，當設備失敗時)，您則需要加密萬能金鑰來重新取得加密的資料。

如果此安裝位於 叢集的第一個成員上，則當您在叢集的其他成員上安裝 「使用者應用程式」時，請使用此加密萬能金鑰。

如需有關萬能金鑰的詳細資料，請參閱 《*Identity Manager 使用者應用程式：管理指南* (http://www.novell.com/documentation/idm35/index.html)》中有關 「*使用者應用程式敏感資料的加密*」和 「*叢集 JBoss*」的章節。

5.9.2 檢查您的叢集安裝

檢查您的叢集安裝。確定 JBoss 叢集中的每個 JBoss 伺服器有以下：

- 一個唯一的分割區名稱 (分割區名稱)
- 一個唯一的分割區 UDP (partition.udpGroup)
- 一個唯一的 「工作流程引擎 ID」
- 相同的 (同一個) WAR 檔案。依預設，安裝程序會將 WAR 寫入 jboss\server\IDM\deploy 目錄。

請確定 WebSphere 叢集中的每一個伺服器都有唯一的工作流程引擎 ID。

如需詳細資訊，請參閱 《*Identity Manager 使用者應用程式：管理指南* (http://www.novell.com/documentation/idm35/index.html)》第 4 章中對叢集提出討論的小節。

5.9.3 設定 JBoss 伺服器之間的 SSL 通訊

如果您在安裝期間核取了 「使用者應用程式」中的 「*使用外部密碼 WAR*」，就必須在您部署 「使用者應用程式」的 WAR 和 IDMPwdMgt.war 檔案的 JBoss 伺服器之間，設定 SSL 通訊。如需指示，請參閱 JBoss 文件。

5.9.4 存取外部密碼 WAR

如果您擁有外部密碼 WAR 並且想藉由存取它來測試「忘記密碼」功能，則可以透過下列方式存取：

- 在瀏覽器中：前往外部密碼 WAR 中的「忘記密碼」頁面，例如 http://localhost:8080/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsf。
- 在「使用者應用程式」登入頁中，按一下「*忘記密碼*」連結。

5.9.5 更新忘記密碼設定

您可以在安裝之後變更「*忘記密碼連結*」和「*忘記密碼回傳連結*」的值。使用 configupdate 公用程式或「使用者應用程式」。

若要使用 configupdate 公用程式。在指令行中將目錄變更爲安裝目錄，並輸入 configupdate.sh (Linux 或 Solaris) 或 configupdate.bat (Windows)。如果您在建立或編輯外部密碼管理 WAR，則必須先手動重新命名 WAR，再將其複製到遠端 JBoss 伺服器。

若要使用「使用者應用程式」：以「使用者應用程式管理員」的身分登入，然後移至「*管理 > 應用程式組態 > 密碼模組設定 > 登入*」。修改以下：

- *忘記密碼連結* (例如：http://localhost:8080/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsf)
- *忘記密碼回傳連結* (例如：https://idmhost:sslport/idm)

5.9.6 設定電子郵件通知

若要實作「忘記密碼」和「工作流程」電子郵件通知功能：

1. 在 iManager 中的「角色和任務」之下，選取「工作流程管理」，再選取「*電子郵件伺服器選項*」。
2. 在「*主機名稱*」之下指定您的 SMTP 伺服器名稱。
3. 在「*寄件者*」旁邊指定電子郵件位址 (例如，*noreply@novell.com*)，然後按一下「*確定*」。

5.9.7 測試 JBoss 應用程式伺服器上的安裝

1 啓動資料庫。如需指示，請參閱資料庫文件。

2 啓動「使用者應用程式」伺服器 (JBoss)。在指令行中將安裝目錄做爲工作目錄，然後執行下列程序檔 (由「使用者應用程式」安裝所提供)：

start-jboss.sh (Linux 和 Solaris)

start-jboss.bat (Windows)

如果您需要停止應用程式伺服器，請使用 stop-jboss.sh 或 stop-jboss.bat，或請關閉正在執行 start-jboss.sh 或 start-jboss.bat 的視窗。

3 啓動「使用者應用程式」驅動程式。這可建立與「使用者應用程式」驅動程式之間的通訊。

3a 登入 iManager。

3b 在左導覽框架中的「角色和任務」顯示中，選取「*Identity Manager*」之下的「*Identity Manager 概觀*」。

3c 在出現的內容檢視窗中，指定包含「使用者應用程式」驅動程式的驅動程式集，然後按一下「*搜尋*」。即會出現一個圖形，顯示驅動程式集及其相關聯的驅動程式。

3d 按一下驅動程式上的紅色和白色圖示。

3e 選取「*啓動驅動程式*」。驅動程式狀態會變更爲陰陽符號，表示驅動程式已經啓動。

驅動程式在啓動時，會嘗試和「使用者應用程式」一同「交換信號」("handshake")。如果您的應用程式伺服器沒有在執行，或者 WAR 沒有成功部署，驅動程式就會傳回錯誤。

4 若要啓動並登入「使用者應用程式」，請使用您的網頁瀏覽器前往 以下 URL：

http://*hostname*:*port*/*ApplicationName*

其中的 *hostname*:*port* 是應用程式伺服器的主機名稱 (例如，myserver.domain.com)，而 port 是應用程式伺服器的連接埠 (例如，JBoss 上預設爲 8080)。*ApplicationName* 預設爲 IDM。在安裝期間，當您提供應用程式伺服器的組態資訊時，指定了應用程式名稱。

「Novell Identity Manager 使用者應用程式」的著陸頁面應當顯示。

5 在該頁的右上角，按一下「*登入*」，以登入「使用者應用程式」。

完成這些步驟時，如果「Identity Manager 使用者應用程式」頁面沒有在瀏覽器中出現，則請檢查終端機主控台是否有錯誤訊息，並請您參閱第 5.11 節「疑難排解」(第 169 頁)。

5.9.8 設定提供小組及其要求

設定您的「提供小組」和「提供小組要求」，以允許進行工作流程任務。如需指示，請參閱《*Identity Manager 3.5.1 使用者應用程式：管理指南* (http://www.novell.com/documentation/idm35/index.html)》。

5.9.9 在 eDirectory 中建立索引

爲了改善「IDM 使用者應用程式」的效能，「eDirectory 管理員」必須建立 manager、ismanager 和 srvprvUUID 屬性的索引。如果沒有建立這些屬性的索引，「使用者應用程式」的效能就可能受損，尤其在叢集環境中更是如此。*如需使用「索引管理員」來建立索引的指示，請參閱《Novell eDirectory 管理指南》*。(http://www.novell.com/documentation)

5.10 安裝後重新設定 IDM WAR 檔

1. 透過執行 configupdate.sh 或 configupdate.bat，在「使用者應用程式」安裝目錄中執行 ConfigUpdate 公用程式。這可讓您更新安裝目錄中的 WAR 檔。

   如需 ConfigUpdate 公用程式參數資訊，請參閱第 5.5.14 節「設定使用者應用程式組態」(第 122 頁) 或 第 5.6.9 節「設定使用者應用程式組態」(第 145 頁)。
2. 將新的 WAR 檔案部署到您的應用程式伺服器上。

5.11 疑難排解

您的 Novell 代表會解決您可的任何設定和組態問題。於此同時，我們在這裡提出一些方法，讓您在遇到問題時嘗試使用。

表格 5-9 *疑難排解使用者應用程式*

問題	建議的動作

您想要修改安裝期間所做的「使用者應用程式」組態設定。包括諸如下列項目的組態：
◆ Identity Vault 連接和證書
◆ 電子郵件設定
◆ Metadirectory 使用者身分、使用者群組
◆ iChain 設定
	您可以不依賴安裝程式來執行組態公用程式。
	在 Linux 和 Solaris 上，從安裝目錄 (預設爲 /opt/novell/idm) 執行下列指令：
	`configupdate.sh`
	在 Windows 上，從安裝目錄 (預設爲 c:\opt\novell\idm) 執行下列指令：
	`configupdate.bat`

當應用程式伺服器啓動時發生例外，記錄訊息爲「連接埠 8080 已在使用中」。	關閉可能已在執行之 Tomcat 的任何例項 (或其他伺服器軟體)。如果您決定重新設定應用程式伺服器來使用 8080 以外的連接埠，請記得編輯 iManager 中「使用者應用程式」驅動程式的組態設定。
當應用程式伺服器啓動時，您看到一個訊息表示找不到任何託管證書。	請確定您使用「使用者應用程式」安裝程序中指定的 JDK 來啓動應用程式伺服器。
您無法登入入口網站管理頁面。	請確定「使用者應用程式管理員」帳戶存在。請勿將此帳戶與您的 iManager 管理帳戶混淆。它們是不同的管理物件 (或者說，它們應該是不同的)。
您可以使用管理員身分登入，但無法建立新使用者。	「使用者應用程式管理員」必須是頂端容器的託管者，並需要具有「監督者」權限。您可以嘗試設定「使用者應用程式」的「管理員」權限與輕量目錄存取協定 (LDAP) 管理員的權限相等 (使用 iManager)，而這只是權宜之計。
應用程式伺服器啓動時，發生 MySQL 連線錯誤。	請勿以根部身分執行 (不過，如果您執行 IDM 隨附的 MySQL 版本，這個問題就不太可能發生)。 請確定 MySQL 正在執行 (並且執行的是正確的副本)。結束 MySQL 的任何其他例項。執行 /idm/mysql/start-mysql.sh，再執行 /idm/start-jboss.sh。 在文字編輯器中檢查 /idm/mysql/setup-mysql.sh，並更正任何存在疑問的值。然後，執行程序檔並執行 /idm/start-jboss.sh。

問題	建議的動作
您在啓動 應用程式伺服器時遇到 KeyStore 錯誤。	您的應用程式伺服器沒有使用 「使用者應用程式」安裝期間指定的 JDK。 使用 keytool 指令，來輸入證書檔案： `keytool -import -trustcacerts -alias aliasName -file certFile -keystore ..\lib\security\cacerts -storepass changeit` ◆ 以您爲此證書選擇的唯一名稱來取代 *aliasName*。 ◆ 以證書檔案的完整路徑和名稱來取代 *certFile*。 ◆ 預設 KeyStore 密碼爲 changeit (如果您有不同的密碼，請指定它)。

電子郵件通知沒有傳送。	執行 configupdate 公用程式，檢查您是否爲 「電子郵件來源」和 「電子郵件主機使用者應用程式」組態參數提供值。
	
	在 Linux 或 Solaris 上，從安裝目錄 (預設爲 /opt/novell/idm) 執行下列指令：
	`configupdate.sh`
	
	在 Windows 上，從安裝目錄 (預設爲 /opt/novell/idm) 執行下列指令：
	`configupdate.bat`

啓用 Novell Identity Manager 產品

6

下列資訊說明基於 Novell® Identity Manager 之產品的啓用方式。您必須在安裝後的 90 天內啓用 Identity Manager、「整合模組」和「提供模組」，否則它們會關閉。在 90 天內的任何時間或之後，您可以選擇啓用 Identity Manager 產品。

您可以藉由完成下列工作來啓用 Identity Manager：

- 購買 Identity Manager 產品授權
- 使用認證啓用 Identity Manager 產品
- 安裝產品啓用認證
- 檢視 Identity Manager 和驅動程式的產品啓用

6.1 購買 Identity Manager 產品授權

若要購買 Identity Manager 產品授權，請參閱如何購買 Novell Identity Manager 網頁 (http://www.novell.com/products/identitymanager//howtobuy.html)。

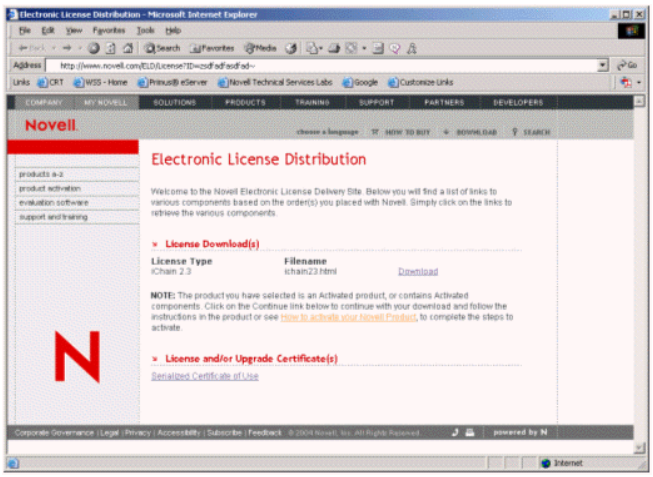
在您購買產品授權之後，Novell 會透過電子郵件傳送給您一個「客戶 ID」。這封電子郵件還包含您可以從中取得認證之 Novell 網站的 URL。如果您想不起或從來沒有收到「客戶 ID」，請聯絡「Novell 啓用中心」：1-800-418-8373 (美國)。其他地區，請撥 1-801-861-8373 (您必須支付撥打 801 區碼的費用)。

6.2 使用認證啓用 Identity Manager 產品

1 在您購買授權之後，Novell 會以電子郵件傳送「客戶 ID」給您。在這封電子郵件中的「訂單詳細資料」區段有一個網站連結，您可以從該網站取得認證。按一下連結，前往該網站。

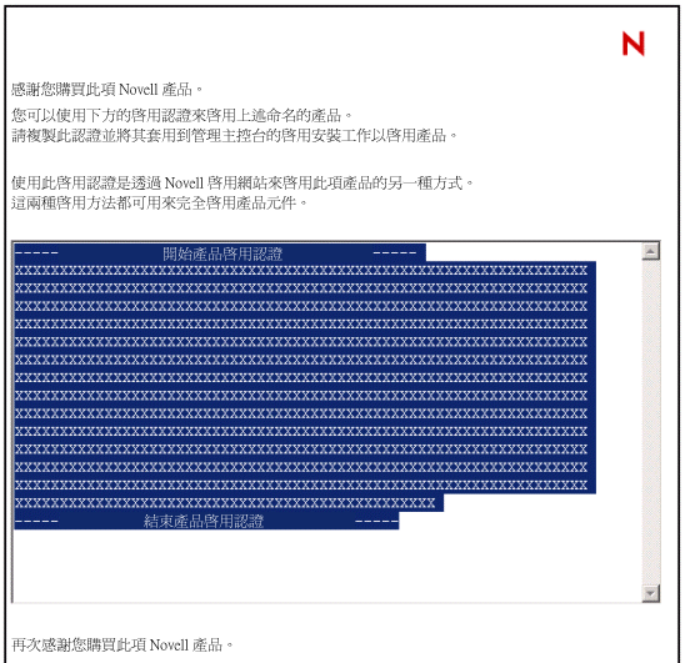
重要：啓用產品時不需此電子郵件。如果此電子郵件傳送給您所在國家內的其他人士，請聯絡「Novell 啓用中心」以取得詳細資訊。

按一下連結後，您將看到如下所示的頁面：



2 按一下授權下載連結，並儲存 (下載) 或開啓 .html 檔案。

開啓檔案之後，其內容應該與下列圖例中顯示的內容類似：



3 如需如何啓用 Identity Manager 元件的指示，請繼續前往第 6.3 節 「安裝產品啓用認證」(第 172 頁)。

6.3 安裝產品啓用認證

您應該透過 iManager 安裝 「產品啓用認證」。

1 開啓包含 「產品啓用認證」的 Novell 電子郵件。

2 請執行下列其中一個步驟：

- 儲存「產品啓用認證」檔案。

  或

- 開啓「產品啓用認證」檔案，然後複製「產品啓用認證」的內容到您的剪貼簿。請小心複製內容，並確定其中沒有額外的行列和空格。您應該從認證的第一個破折號 (-) 開始複製 (----BEGIN PRODUCT ACTIVATION CREDENTIAL)，一直複製到最後一個破折號 (-) (END PRODUCT ACTIVATION CREDENTIAL-----)。

3 開啓 iManager。

4 選擇「*Identity Manager* > *Identity Manager 概觀*」。

5 選取驅動程式集或瀏覽至驅動程式集，然後按「*下一步*」。

6 在「Identity Manager 概觀」頁面上尋找驅動程式集的位置，按一下紅色的「*啓用要求者*」連結，然後按一下「*安裝啓用*」。

7 選取您想在其中啓用 Identity Manager 元件的驅動程式集。

8 請執行下列其中一個步驟：

- 指定儲存「Identity Manager 啓用認證」的位置，然後按「*下一步*」。

  或

- 將「Identity Manager 啓用認證」的內容貼至文字區域，然後按「*下一步*」。

9 按一下*「完成」*。

附註：您需要啓用具有驅動程式的每一個驅動程式集。您可以使用認證來啓用任何網路樹。

6.4 檢視 Identity Manager 和驅動程式的產品啓用

對於每一個驅動程式集，您可以查看爲 Metadirectory 引擎和 Identity Manager 驅動程式安裝的「產品啓用認證」。若要檢視「產品啓用認證」，請執行下列動作：

1. 開啓 iManager。
2. 按一下「*Identity Manager*」>「*Identity Manager 概觀*」。
3. 在物件名稱欄位中輸入驅動程式集的名稱，或輸入您想用來檢視啓用資訊的驅動程式名稱。

   或

   瀏覽並選取您想要檢視其啓用資訊的驅動程式集或驅動程式。
4. 找到您想要檢視其啓用資訊的驅動程式集，然後按一下驅動程式集名稱。
5. 選取「*啓用*」索引標籤。

   您可以檢視啓用認證的文字，或者如果報告錯誤，則可以移除啓用認證。

附註：在安裝驅動程式集的有效「產品啓用認證」之後，您可能仍會在驅動程式名稱旁邊看到「需要啓用」。如果是這種情況，請重新啓動驅動程式，該訊息應該會消失。
