使用者應用程式：安裝指南

Novell® Identity Manager Roles Based Provisioning Module

4.0.1

2011 年 4 月 15 日

www.novell.com

法律聲明

Novell, Inc. 不對本文件的內容或使用做任何表示或保證，且特別聲明不對任何特定用途的適銷性或適用性提供任何明示或默示的保證。此外，Novell, Inc. 有權隨時修訂本出版品或更改其內容，而無義務向任何個人或實體告知這類修訂或變更。

此外，Novell, Inc. 不對軟體做任何表示或保證，且特別聲明不對任何特定用途的適銷性或適用性提供任何明示或默示的保證。此外，Novell, Inc. 有權隨時變更部分或全部 Novell 軟體，而無義務向任何個人或實體告知這類變更。

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規定，並同意取得出口、再出口或進口產品所需的一切授權或類別。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 / 地區。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。請參閱 Novell 國際貿易服務網頁 (http://www.novell.com/info/exports/)，以取得有關出口 Novell 軟體的詳細資訊。Novell 無需承擔您無法取得任何必要的出口核准之責任。

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

*線上文件：*若要存取本產品及其他 Novell 產品的最新線上文件，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

本指南說明如何安裝 Novell Identity Manager Roles Based Provisioning Module 4.0.1。各章節如下所示：

使用對象

本指南的適用對象爲規劃和實作 Identity Manager Roles Based Provisioning Module 的管理員和顧問。

意見反應

我們希望得到您對本手冊以及本產品隨附之其他文件的意見和建議。請使用線上文件中每頁底下的「使用者意見」功能，或造訪 www.novell.com/documentation/feedback.html，然後寫下您的意見。

其他文件

如需 Identity Manager 4.0.1 的其他相關文件，請參閱 Identity Manager 文件網站 (http://www.novell.com/documentation/idm401/index.html)。

Roles Based Provisioning Module 安裝綜覽

1

本章提供 Roles Based Provisioning Module 的安裝步驟綜覽。主題包括：

- 第 1.1 節 「安裝核對清單」 (第 9 頁)
- 第 1.2 節 「關於安裝程式」 (第 10 頁)
- 第 1.3 節 「系統要求」 (第 10 頁)

如果要從舊版的使用者應用程式或 Roles Based Provisioning Module 移轉，請參閱 *《使用者應用程式：移轉指南》*(http://www.novell.com/documentation/idm40/index.html)

1.1 安裝核對清單

若要安裝 Novell Identity Manager Roles Based Provisioning Module，必須執行下列任務：

- ❑ 驗證您的軟體符合系統要求。請參閱第 1.3 節 「系統要求」 (第 10 頁)。
- ❑ 下載 Identity Manager Roles Based Provisioning Module。請參閱第 2.2 節 「下載 Roles Based Provisioning Module」 (第 15 頁)。
- ❑ 安裝下列支援元件：
  - ❑ 確定您已安裝支援的 Identity Manager Metadirectory。請參閱第 2.1 節 「安裝 Identity Manager Metadirectory」 (第 15 頁)。
  - ❑ 安裝和設定應用程式伺服器。請參閱第 2.3 節「安裝應用程式伺服器」(第 16 頁)。
  - ❑ 安裝和設定資料庫。請參閱第 2.4 節 「安裝資料庫」 (第 22 頁)。
- ❑ 安裝 Roles Based Provisioning Module Metadirectory 元件。請參閱第 3 章 「安裝 Roles Based Provisioning Module」 (第 29 頁)。
- ❑ 在 Designer 4.0.1 for Identity Manager 中建立使用者應用程式驅動程式。
  - 請參閱第 4.1 節 「在 Designer 中建立驅動程式」 (第 43 頁)。
- ❑ 在 Designer 4.0.1 for Identity Manager 中建立角色與資源服務驅動程式。
  - 請參閱第 4.1 節 「在 Designer 中建立驅動程式」 (第 43 頁)
- ❑ 安裝並設定 Novell Identity Manager 使用者應用程式。(只有安裝了正確的 JDK，才能啓動安裝程式。請參閱第 2.5 節 「安裝 Java 開發套件」 (第 27 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。請參閱下列其中一節：
    - 第 5 章 「在 JBoss 上安裝使用者應用程式」 (第 53 頁)。
    - 第 6 章 「在 WebSphere 上安裝使用者應用程 式」 (第 75 頁)。
    - 第 7 章 「在 WebLogic 上安裝使用者應用程式」 (第 103 頁)。
  - 主控台 (指令行) 介面。請參閱第 8.1 節 「透過主控台安裝使用者應用程式」 (第 121 頁)。
  - 無訊息安裝。請參閱第 8.2 節 「使用單一指令安裝使用者應用程式」 (第 121 頁)。
- ❑ 執行第 9 章 「安裝後任務」 (第 133 頁) 中說明的安裝後任務。

重要：本指南未提供設定安全環境的相關指示。如需安全性的詳細資料，請參閱《使用者應用程式：管理指南》(http://www.novell.com/documentation/idm40/index.html)。

1.2 關於安裝程式

「使用者應用程式」的安裝程式會：

- 確定您的授權適用於 Identity Manager 4.0.1 Advanced Edition 還是適用於 Standard Edition，然後顯示相應的授權版本螢幕。
- 指定現有的應用程式伺服器版本，以供使用。
- 指定要使用的現有版本資料庫，例如 PostgreSQL、Oracle、DB2、Microsoft SQL Server 或 MySQL。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。
- 爲 Novell Identity Manager 使用者應用程式設定 Java Web 應用程式歸檔 (WAR) 檔案並將其部署至應用程式伺服器。在 WebSphere 和 WebLogic 上，必須手動部署 WAR。
- 啓用透過 Novell 或 OpenXDAS 稽核用戶端的記錄 (如果您希望這麼做)。
- 讓您能輸入現有的萬能金鑰來還原特定的 Roles Based Provisioning Module 安裝，並支援叢集。

1.3 系統要求

若要使用 Novell Identity Manager Roles Based Provisioning Module 4.0.1，必須安裝表格 1-1 中列出的其中一項必要元件。

表格 1-1 *系統要求*

必要的系統元件	系統要求
Metadirectory	eDirectory 8.8.6 搭配 Identity Manager 4.0.1 使用。 如需支援的作業系統清單，請參閱 Identity Manager 與 eDirectory 文件。

必要的系統元件	系統要求
應用程式伺服器	使用者應用程式可在 JBoss、WebSphere 和 WebLogic 上執行，如下所述。 使用者應用程式搭配 JBoss 5.1 使用時需要 Sun 的 JRE 1.6.0_20，可在下列平台上執行： ◆ Windows Server 2003 SP2 (僅 32 位元) ◆ Windows Server 2008 R2 (僅 64 位元) ◆ Windows Server 2008 SP1 (32 位元與 64 位元) ◆ Open Enterprise Server 2 SP3 (32 位元與 64 位元) ◆ SUSE Linux Enterprise Server 10 SP3 (32 位元與 64 位元) ◆ SUSE Linux Enterprise Server 11 SP1 (32 位元與 64 位元) ◆ Red Hat Enterprise Linux 5.4 (32 位元與 64 位元) WebSphere 7.0 上的使用者應用程式需要 IBM J9 VM (版次 2.4、J2RE 1.6.0) 與修復套件 7。它可以在以下平台上執行： ◆ Windows Server 2003 SP2 (僅 32 位元) ◆ Windows Server 2008 R2 (僅 64 位元) ◆ 安裝了最新支援套件的 Windows Server 2008 SP1 (32 位元與 64 位元) ◆ Open Enterprise Server 2 SP3 (32 位元與 64 位元) ◆ SUSE Linux Enterprise Server 10 SP3 (32 位元與 64 位元) ◆ SUSE Linux Enterprise Server 11 SP1 (32 位元與 64 位元) ◆ Red Hat Enterprise Linux 5.4 (32 位元與 64 位元) WebLogic 10.3 上的使用者應用程式需要 JRockit JVM 1.6.0_17，可在下列平台上執行。 ◆ Windows Server 2003 SP2 (僅 32 位元) ◆ Windows Server 2008 R2 (僅 64 位元) ◆ 安裝了最新支援套件的 Windows Server 2008 SP1 (32 位元與 64 位元) ◆ Open Enterprise Server 2 SP3 (32 位元與 64 位元) ◆ SUSE Linux Enterprise Server 10 SP3 (32 位元與 64 位元) ◆ SUSE Linux Enterprise Server 11 SP1 (32 位元與 64 位元) ◆ Red Hat Enterprise Linux 5.4 (32 位元與 64 位元) **附註：**只要訪客作業系統受到使用者應用程式的支援，使用者應用程式便可支援 Xen 與 VMW 虛擬化。

必要的系統元件	系統要求
瀏覽器	使用者應用程式支援 Firefox 和 Internet Explorer，如下所示。 FireFox 3.6 可在下列平台上執行： ◆ Windows XP SP3 ◆ Windows Vista ◆ Windows 7 ◆ SUSE Linux Enterprise Desktop 11 ◆ SUSE Linux Enterprise Server 11 ◆ Novell OpenSuSE 11.2 ◆ Apple Mac Internet Explorer 8 可以在以下平台上執行： ◆ Windows XP SP3 ◆ Windows Vista ◆ Windows 7 Internet Explorer 7 可在下列平台上執行： ◆ Windows XP SP3
資料庫伺服器	JBoss 5.1.0 支援以下資料庫： ◆ MS SQL 2008 ◆ MySQL 5.1 版 ◆ Oracle 11g ◆ PostgreSQL 8.4.3 WebSphere 7.0 支援以下資料庫： ◆ DB2 9.5 ◆ MS SQL 2008 ◆ Oracle 11g ◆ PostgreSQL 8.4.3 WebLogic 10.3 支援以下資料庫： ◆ MS SQL 2008 ◆ Oracle 11g ◆ PostgreSQL 8.4.3
Designer	Designer 4.0.1
OpenXDAS	OpenXDAS 0.8.345 版 SLES10 需要以下版本的 OpenXDAS ： ◆ openxdas-0.8.351-1.1.i586.rpm ◆ openxdas-0.8.351-1.1.x86_64.rpm
網域服務	Windows 適用的 OES 2 SP1 網域服務

必要的系統元件	系統要求
密碼管理處理安全回應	密碼管理處理安全回應功能需要使用版本 2770 版次 20080603 或更新版本的 NMAS 處理安全回應登入方法。

先決條件

2

本章說明在安裝 Identity Manager Roles Based Provisioning Module (RBPM) 之前，必須安裝或設定的軟體元件。主題包括：

2.1 安裝 Identity Manager Metadirectory

Roles Based Provisioning Module 4.0.1 必須與 Identity Manager 4.0.1 搭配使用。

如需安裝 Identity Manager 4.0.1 的指示，請參閱 Identity Manager 文件網站 (http://www.novell.com/documentation/idm40/index.html)。

2.2 下載 Roles Based Provisioning Module

若要獲得 Identity Manager Roles Based Provisioning Module 產品，請從 Novell 下載 (http://download.novell.com/index.jsp) 網站下載一個 .iso 影像檔。下載頁面會提供適用於 Identity Manager 4.0.1 Advanced Edition 與 Standard Edition 的相應 .iso 影像檔。選擇適用於您版本的正確 .iso 影像檔 (例如 Identity_Manager_4.0.1_User_Application_Advanced.iso 或 Identity_Manager_4.0.1_User_Application_Standard.iso)。

表格 2-1 介紹提供的使用者應用程式與 Roles Based Provisioning Module 的安裝檔案。您可以在 .iso 檔案內的產品 /RBPM 目錄中找到這些檔案。

表格 2-1 *提供的檔案與程序檔*

檔案	描述
IDMProv.war	Roles Based Provisioning Module WAR。包含支援身分自助服務功能與 Roles Based Provisioning Module 功能的 Identity Manager 使用者應用程式。
IDMUserApp.jar	使用者應用程式安裝程式。
silent.properties	這個檔案包含自動安裝所需的參數。這些參數與您在 GUI 或「主控台」安裝程序中設定的安裝參數相對應。您應該複製這個檔案，然後依照您的安裝環境來適當地修改內容。
JBossPostgreSQL.bin 或 JBossPostgreSQL.exe	方便安裝 JBoss Application Server 和 PostgreSQL 資料庫的公用程式。
nmassaml.zip	包含可支援 SAML 的 eDirectory 方法。只有在不是使用 Access Manager 時才需要。

檔案	描述
rbpm_driver_install.exe	Roles Based Provisioning Module 之 Metadirectory 元件 (角色與資源服務驅動程式、使用者應用程式驅動程式以及 eDirectory 綱要) 適用的 Windows 安裝程式。
rbpm_driver_install_linux.bin	Roles Based Provisioning Module 之 Metadirectory 元件 (角色與資源服務驅動程式、使用者應用程式驅動程式及 eDirectory 綱要) 適用的 Linux 安裝程式。
rbpm_driver_install_solaris.bin	Roles Based Provisioning Module 之 Metadirectory 元件 (角色與資源服務驅動程式、使用者應用程式驅動程式及 eDirectory 綱要) 適用的 Solaris 安裝程式。

安裝 Identity Manager Roles Based Provisioning Module 的系統上，必須至少有 320 MB 的可用儲存空間，以及供支援應用程式 (資料庫、應用程式伺服器等等) 使用的空間。隨著時間經過，系統會需要更多空間來容納其他變多的資料，例如資料庫或應用程式伺服器記錄。

預設安裝位置是：

- Linux 或 Solaris：/opt/novell/idm
- Windows：C:\Novell\IDM

安裝期間，您可以選取其他預設安裝目錄，但在開始安裝之前該目錄必須已經存在且可以寫入 (對於 Linux 或 Solaris，要求非根使用者可以寫入)。

2.3 安裝應用程式伺服器

- 第 2.3.1 節「安裝 JBoss 應用程式伺服器」(第 16 頁)
- 第 2.3.2 節「安裝 WebLogic 應用程式伺服器」(第 22 頁)
- 第 2.3.3 節「安裝 WebSphere 應用程式伺服器」(第 22 頁)

2.3.1 安裝 JBoss 應用程式伺服器

如果您打算使用「JBoss 應用程式伺服器」，您可以採取下列方法：

- 根據製造廠商的說明下載並安裝 JBoss 應用程式伺服器。關於支援的版本，請參閱第 1.3 節「系統要求」(第 10 頁)。
- 使用 Roles Based Provisioning Module 下載檔案提供的 JBossPostgreSQL 公用程式來安裝 JBoss Application Server (可另外選擇安裝 PostgreSQL)。如需說明，請參閱「安裝 JBoss Application Server 和 PostgreSQL 資料庫」(第 17 頁)。

請先安裝 Identity Manager Roles Based Provisioning Module 再啓動 JBoss 伺服器。啓動 JBoss 伺服器屬於安裝後任務。

表格 2-2 *JBoss 應用程式伺服器最小建議要求*

配件	建議
RAM	執行 Identity Manager Roles Based Provisioning Module 時，建議至少要有 512 MB 的 RAM 供 JBoss 應用程式伺服器使用。

配件	建議
連接埠	應用程式伺服器的預設連接埠爲 8180。請記錄應用程式伺服器所使用的連接埠。
SSL	如果您打算使用外部密碼管理，請啓用 SSL： ◆ 請在您部署 Identity Manager Roles Based Provisioning Module 和 IDMPwdMgt.war 檔案的 JBoss 伺服器上啓用 SSL。 ◆ 請確定您的防火牆已開放 SSL 連接埠。 如需啓用 SSL 的相關資訊，請參閱 JBoss 文件。 如需 IDMPwdMgt.war 檔案 的相關資訊，請參閱第 9.5 節 「設定外部忘記密碼管理」 (第 136 頁) 以及 *《使用者應用程式：管理指南》*(http://www.novell.com/documentation/idm40/index.html)。

安裝 JBoss Application Server 和 PostgreSQL 資料庫

JBossPostgreSQL 公用程式會在您的系統上安裝 JBoss Application Server 和 PostgreSQL。這個公用程式不支援主控台模式，需要圖形使用者介面環境。

附註：在 Windows 2008 上執行 RBPM JBossPostgreSQL 安裝程式之前，需要先諮詢您的 Windows 管理員，瞭解您的系統所使用的密碼規則。Windows 2008 伺服器密碼規則要求密碼遵循特定的一組規則。例如，密碼規則可能要求密碼包含非字母字元，及大小寫字元，或長度不少於 8 個字元。Windows 管理員可以修改或停用該規則。

以根使用者身分執行安裝程式。您需要以根使用者身分執行安裝程式。

若要執行 JBossPostgreSQL 公用程式：

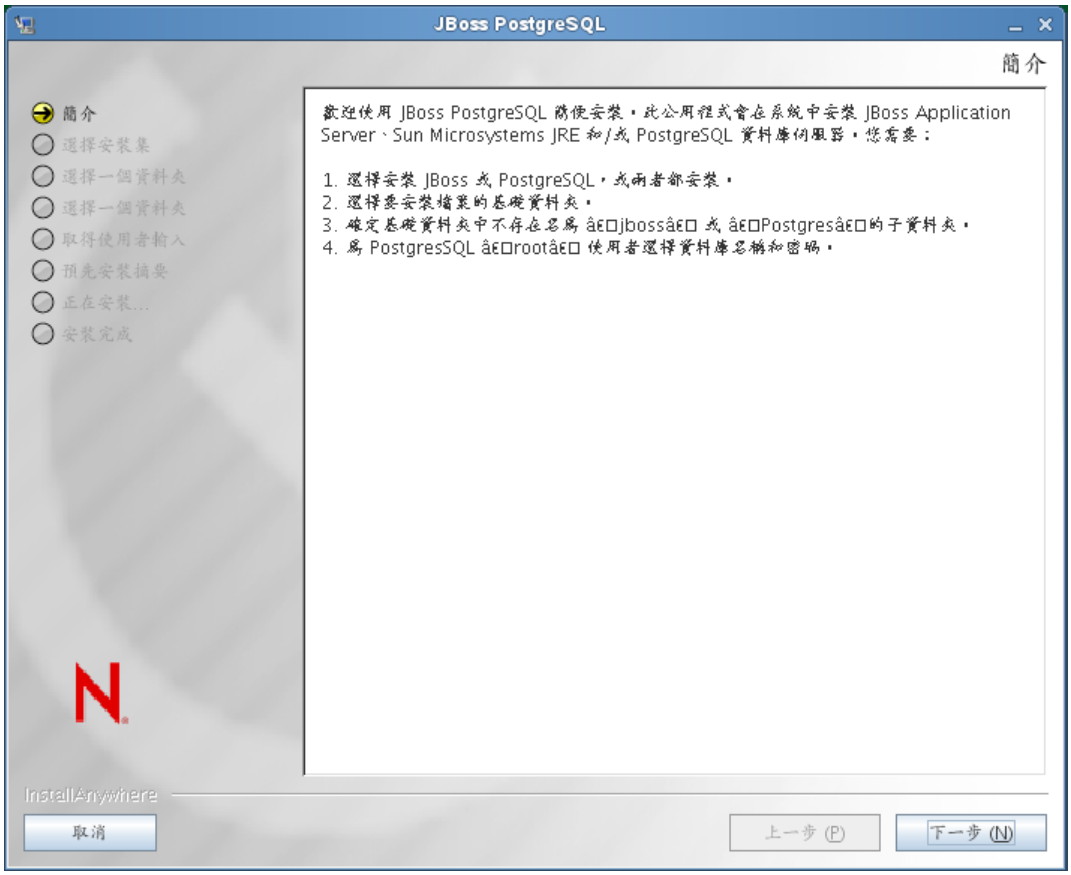
1 找到並執行 JBossPostgreSQL.bin 或 JBossPostgreSQL.exe。

/linux/jboss/JBossPostgreSQL.bin (若爲 Linux)
/nt/jboss/JBossPostgreSQL.exe (若爲 Windows)

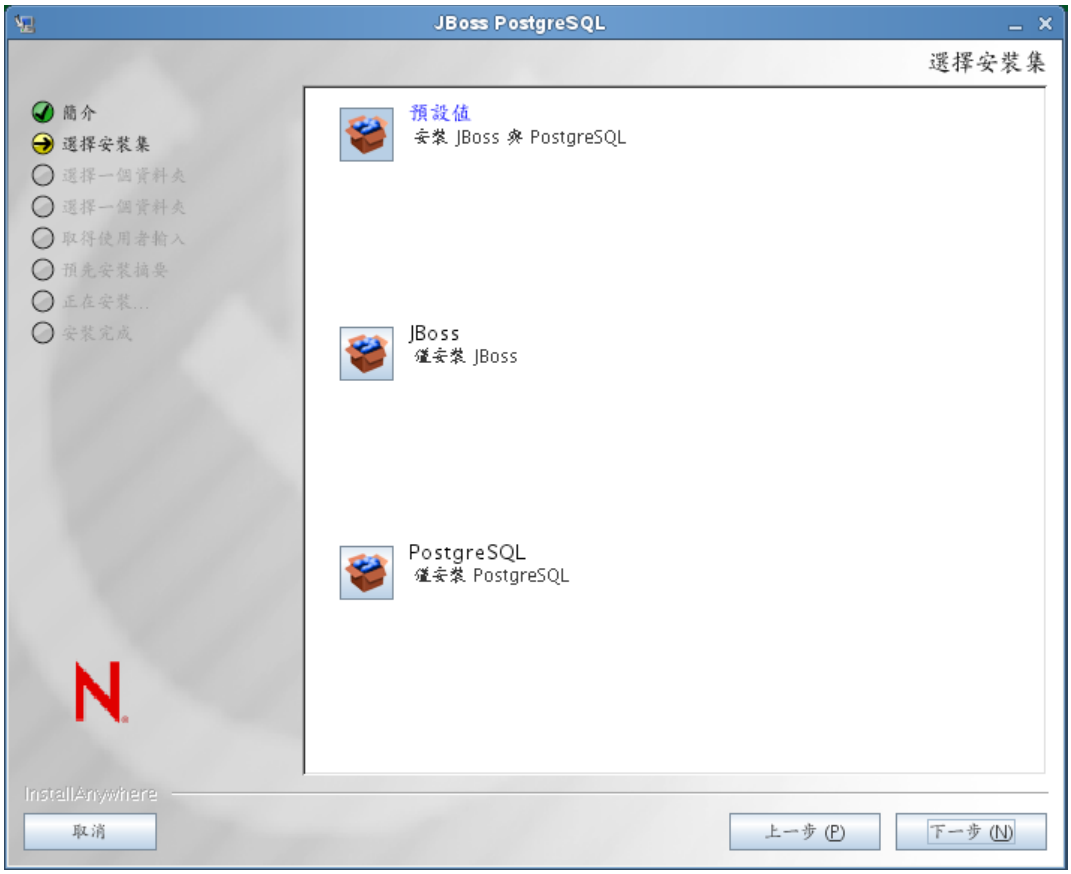
該公用程式不適用於 Solaris 系統。

JBossPostgreSQLJBossPostgreSQL 公用程式會顯示其開頭顯示畫面：

然後會顯示「簡介」螢幕：

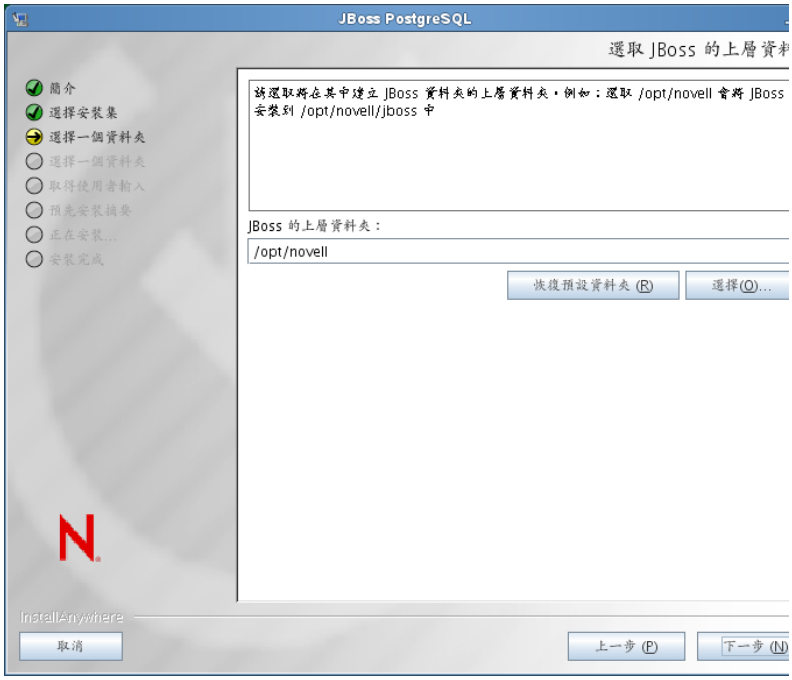
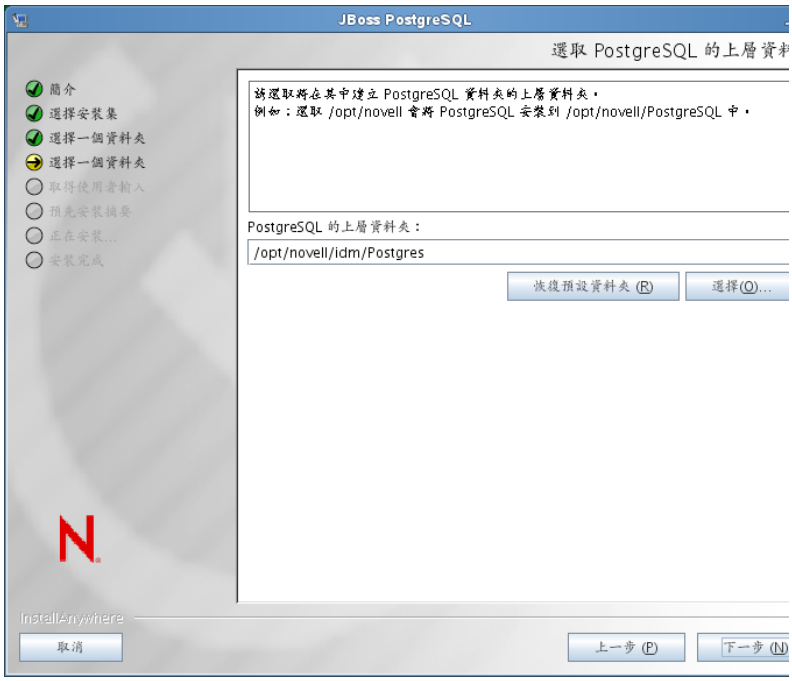


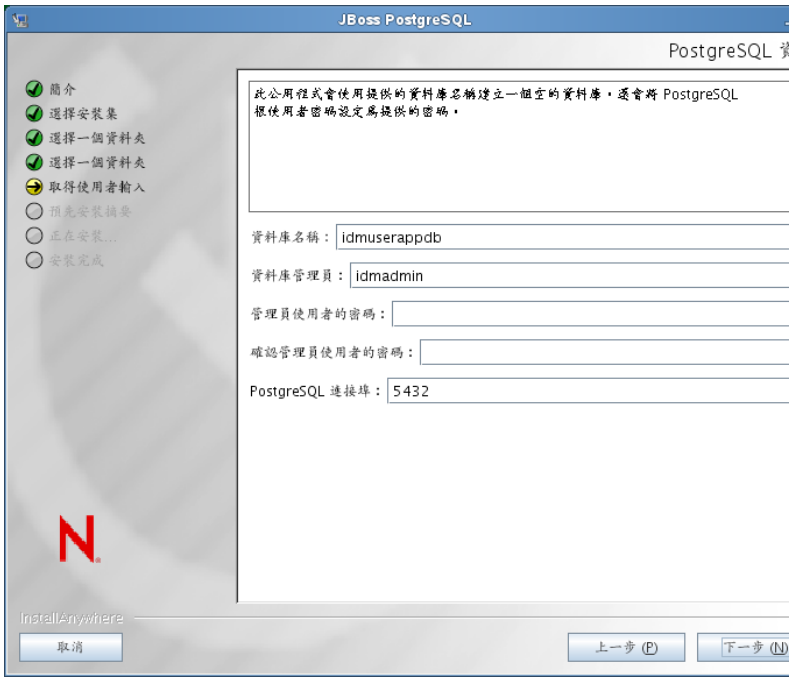
當您按「下一步」後，公用程式會顯示「*選擇安裝集*」螢幕：



2 依照螢幕上的指示來導覽公用程式。如需其他資訊，請參閱下表。

安裝畫面	描述
選擇安裝集	選擇要安裝的產品。 ◆ *預設*：在您指定的目錄中安裝 JBoss 和 PostgreSQL，以及用來啓動和停止 JBoss 和 PostgreSQL 的程序檔。 ◆ *JBoss*：在您指定的目錄中安裝 JBoss 應用程式伺服器以及用來啓動和停止的程序檔。 **附註：**此公用程式無法將「JBoss 應用程式伺服器」安裝爲 Windows 服務。如需說明，請參閱「將 JBoss 應用程式伺服器安裝爲服務或精靈」（第 21 頁）。 ◆ *PostgreSQL*：在您指定的目錄中安裝 PostgreSQL 並建立 PostgreSQL 資料庫，另外還會安裝用來啓動和停止 PostgreSQL 的程序檔。

安裝畫面	描述
選擇 JBoss 上層資料夾	按一下「*選擇*」來選取非預設的安裝資料夾。 
選擇 PostgreSQL 上層資料夾	按一下「*選擇*」以選取非預設的安裝資料夾。 

安裝畫面	描述
PostgreSQL 資訊	指定下列項目： ◆ *資料庫名稱*：指定要讓安裝程式建立的資料庫名稱。使用者應用程式安裝公用程式會提示您提供此名稱，所以請記下名稱和位置。預設資料庫爲 idmadmin。 ◆ *資料庫管理員*：該使用者將做爲資料庫的管理員。預設管理員爲 idmuserappdb。 ◆ *管理員使用者的密碼*：資料庫管理員的密碼。 ◆ *確認管理員使用者的密碼*：確認密碼。 ◆ *PostgreSQL 連接埠*：PostgreSQL 資料庫伺服器將監聽的連接埠。 
安裝前摘要	檢閱「摘要」頁面。如果指定正確，請按一下「*安裝*」。
安裝完成	公用程式會在您選取的產品安裝完成後顯示安裝完成的訊息： `The Installer has completed successfully.  Thank you for choosing Novell` **安裝程式會建立 novlua 使用者。**安裝程式會建立名爲 novlua 的新使用者。jboss_init 程序檔會以此使用者身分執行 JBoss，並且會將 JBoss 檔案中定義的許可權設定給此使用者。 **重要：**您需要注意，JBossPostgreSQL 公用程式無法保護 JMX 主控台或 JBoss Web 主控台的安全，致使 JBoss 環境處於完全開放狀態。因此，安裝完成後應立即鎖定環境，以消除安全風險。

將 JBoss 應用程式伺服器安裝爲服務或精靈

在 Linux 上，JBoss 預設以服務的形式啓動。一個名爲 /etc/init.d/jboss_init start/stop 的程序檔會安裝到設備中，以在系統重新開機時啓動 JBoss。

使用 JavaServiceWrapper。您可以使用 JavaServiceWrapper 來安裝、啓動和停止「JBoss 應用程式伺服器」以做爲 Windows 服務或 Linux 或 UNIX 精靈程序。請參閱 http://www.jboss.org/community/wiki/RunJBossAsAServiceOnWindows (http://www.jboss.org/community/wiki/RunJBossAsAServiceOnWindows) 上 JBoss 提供的指示。http://wrapper.tanukisoftware.org/doc/english/integrate-simple-win.html (http://wrapper.tanukisoftware.org/doc/english/integrate-simple-win.html) 上提供了一個類似包裝程式，它由 JMX 管理 (請參閱 http://wrapper.tanukisoftware.org/doc/english/jmx.html#jboss (http://wrapper.tanukisoftware.org/doc/english/jmx.html#jboss))。

重要：在舊版中，您可以使用協力廠商公用程式 (例如 JavaService) 將「JBoss 應用程式」安裝爲 Windows 服務並予以啓動和停止，但 JBoss 不再建議使用 JavaService。如需詳細資料，請參閱 http://www.jboss.org/wiki/JavaService (http://www.jboss.org/community/wiki/JavaService)。

2.3.2 安裝 WebLogic 應用程式伺服器

如果您打算使用 WebLogic 應用程式伺服器，請下載並安裝。如需支援的版本的相關資訊，請參閱第 1.3 節「系統要求」(第 10 頁)。

2.3.3 安裝 WebSphere 應用程式伺服器

如果您打算使用 WebSphere 應用程式伺服器，請下載並安裝。如需支援之版本的相關資訊，請參閱第 1.3 節「系統要求」(第 10 頁)。

如需 DB2 組態的相關說明，請參閱「設定 DB2 資料庫的說明」(第 25 頁)。

2.4 安裝資料庫

「使用者應用程式」會使用資料庫執行各種任務，例如，儲存組態資料，以及爲任何工作流程活動儲存資料。必須安裝和設定您平台所支援的其中一個資料庫，才能安裝 Roles Based Provisioning Module 和使用者應用程式。這包含：

- ❑ 安裝資料庫和資料庫驅動程式。
- ❑ 建立資料庫或資料庫例項。
- ❑ 記錄以下資料庫參數，以便在安裝使用者應用程式的過程中使用：
  - ◆ 主機和連接埠
  - ◆ 資料庫名稱、使用者名稱和使用者密碼
- ❑ 建立指向資料庫的資料來源檔案。

  安裝方法因應用程式伺服器而異。對於 JBoss，使用者應用程式安裝程式會建立指向資料庫的應用程式伺服器資料來源檔案，並依據 Identity Manager Roles Based Provisioning Module WAR 檔案的名稱命名該檔案。對於 WebSphere 和 WebLogic，應先手動設定資料來源，再進行安裝。
- ❑ 資料庫必須啓用 Unicode 編碼。

  使用者應用程式要求資料庫字元集使用 Unicode 編碼。例如，UTF-8 便是一種使用 Unicode 編碼的字元集，而 Latin1 則不是。安裝使用者應用程式之前，請驗證您的資料庫已設定有使用 Unicode 編碼的字元集。

附註：如果要移轉到新版的 Roles Based Provisioning Module，必須使用之前安裝 (也就是您要移轉的安裝來源) 所使用的使用者應用程式資料庫。

2.4.1 設定 MySQL 資料庫的說明

使用者應用程式需要對 MySQL 設定某些組態選項，如下所述：

- 「INNODB 存放引擎和表格類型」(第 23 頁)
- 「字元集」(第 23 頁)
- 「區分大小寫」(第 23 頁)
- 「Ansi 設定」(第 24 頁)
- 「使用者帳戶要求」(第 24 頁)

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。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。

除了設定 default-table-type=innodb 選項之外，您還可以將 ENGINE=InnoDB 選項附加至資料庫 SQL 程序檔中的建立表格陳述式。

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

在建立資料庫期間，還可以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了字元集，也必須在 IDM-ds.xml 檔案的 JDBC URL 中指定該字元集，如下所示：

```
<connection-url>jdbc:mysql://localhost:3306/
databasename?useUnicode=true&amp;characterEncoding=utf8&amp;connectionCollati
on=utf8_bin</connection-url>
```

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)。

Ansi 設定

您需要將 ansi 項目新增至 my.cnf (在 Linux 上) 或 my.ini 檔案 (在 Windows 上) 中。如果沒有新增此項目，RBPM 表格仍然會建立，但不會執行表格的初始資料載入，而且您可能還會看到「找不到訪客容器頁面定義」的錯誤訊息。

以下便是新增 ansi 項目後 my.cnf (或 my.ini) 檔案中包含的內容：

```
# These variables are required for IDM User Application
character_set_server=utf8
default-table-type=innodb

# Put the server in ANSI SQL mode.
#See http://www.mysql.com/doc/en/ANSI_mode.html
ansi
```

若要確認已變更爲使用 ansi 模式，可以在您的 MySQL 伺服器上執行以下 SQL 陳述式：

```
mysql> select @@global.sql_mode;
+-------------------------------------------------------------+
| @@global.sql_mode                                           |
+-------------------------------------------------------------+
| REAL_AS_FLOAT,PIPES_AS_CONCAT,ANSI_QUOTES,IGNORE_SPACE,ANSI |
+-------------------------------------------------------------+
1 row in set (0.00 sec)
```

使用者帳戶要求

安裝期間使用的使用者帳戶對使用者應用程式使用的資料庫必須具有完全存取權限 (擁有者)。此外，此帳戶還需要具備對系統中表格的存取權限。不同環境下，表格可能會有所不同。

建立使用者以登入 MySQL 伺服器，並將權限授予該使用者，例如：

GRANT ALL PRIVILEGES ON < 資料庫名稱 .>* TO < 使用者名稱 >@< 主機 > IDENTIFIED BY ' 密碼 '

最小權限組爲 CREATE、INDEX、INSERT、UPDATE、DELETE 與 LOCK TABLES。如需 GRANT 指令的文件，請參閱 http://www.mysql.org/doc/refman/5.0/en/grant.html (http://www.mysql.org/doc/refman/5.0/en/grant.html)。

重要：使用者帳戶還必須具有 mysql.user 表格的選取權限。以下是授予適當權限所使用的 SQL 語法：

```
USE mysql;
GRANT SELECT ON mysql.user TO <username>@<host>;
```

2.4.2 設定 Oracle 資料庫的說明

建立 Oracle 資料庫時，請務必使用 AL32UTF8 來指定 Unicode 編碼的字元集。(請參閱 AL32UTF8 (http://download-east.oracle.com/docs/cd/B19306_01/server.102/b14225/glossary.htm#sthref2039)。)

建立 Oracle 資料庫的使用者時，需要使用 SQL Plus 公用程式發出以下陳述式。這些陳述式會建立使用者並設定使用者的權限。授予使用者 CONNECT 與 RESOURCE 權限，例如：

CREATE USER *IDM 使用者* IDENTIFIED BY *密碼*

GRANT CONNECT, RESOURCE to *IDM 使用者*

Oracle 11g 上的 UTF-8。在 Oracle 11g 上，可以發出以下指令，以確認您已啓用 UTF-8 ：

```
select * from nls_database_parameters;
```

如果未設定 UTF-8，會傳回以下資料：

```
NLS_CHARACTERSET
WE8MSWIN1252
```

如果已設定 UTF-8，則會傳回以下資料：

```
NLS_CHARACTERSET
AL32UTF8
```

2.4.3 設定 MS SQL Server 資料庫的說明

按以下步驟設定 MS SQL Server 資料庫：

1. 安裝 MS SQL 伺服器。
2. 連接到伺服器，並開啓用來建立資料庫與資料庫使用者的應用程式 (一般爲 SQL Server Management Studio 應用程式)。
3. 建立資料庫。SQL 伺服器不允許使用者選取資料庫使用的字元集。使用者應用程式在支援 UTF-8 的 NCHAR 欄類型中儲存 SQL Server 字元資料。
4. 建立登入。
5. 將登入新增爲資料庫的使用者。
6. 將這些權限授予登入：CREATE TABLE、CREATE INDEX、SELECT、INSERT、UPDATE 與 DELETE。

使用者應用程式需要 3.0.3.0.1119.0 版的 Microsoft SQL Server 2008 JDBC 驅動程式。請注意，正式對此 JDBC 驅動程式提供支援的只有 Sun Solaris、Red Hat Linux 以及 Windows 2000 或更新版本的作業系統。

2.4.4 設定 DB2 資料庫的說明

本節提供 DB2 組態設定的說明。

提供資料庫驅動程式 JAR

安裝期間，需要選取「*資料庫使用者名稱與密碼*」螢幕中的資料庫驅動程式 JAR 檔案。不過，「*資料庫驅動程式 JAR 檔案*」欄位的瀏覽按鈕僅允許您選取一個 (1) jar。但對於 DB2，必須提供兩 (2) 個 jar ：

- db2jcc.jar
- db2jcc_license_cu.jar

因此，如果在 WebSphere (DB2 唯一支援的應用程式伺服器) 上執行安裝程式，您可以選取其中一個 jar，但第二個 JAR 必須手動輸入，並使用執行安裝程式之作業系統所適用的正確檔案分隔符。您也可以手動輸入兩個項目。

例如，在 Windows 上：

```
c:\db2jars\db2jcc.jar;c:\db2jars\db2jcc_license_cu.jar
```

例如，在 Solaris 和 Linux 上：

```
/home/lab/db2jars/db2jcc.jar:/home/lab/db2jcc_license_cu.jar
```

調整 DB2 資料庫以防止鎖死和逾時

使用 DB2 時，如果遇到指示因鎖死或逾時已復原目前交易的錯誤，則問題可能是由於高階使用者與資料庫並行處理造成。

DB2 提供許多技術可解決鎖定衝突，包括微調成本最佳程式。《DB2 管理》文件中的*效能指南*是極佳的資訊來源，包含豐富的微調主題資訊。

沒有指示自從發生層級和資料大小變更後用於所有安裝的微調值。但是，在此有一些與您的安裝有關的 DB2 微調提示：

- reorgchk update statistics 命令將更新最佳化工具使用的統計資料。定期更新這些統計資料便足以減輕這個問題。
- 透過不鎖定已插入或更新列的下一個索引鍵來使用 DB2 登錄參數 DB2_RR_TO_RS，可改善發生狀況。
- 在資料庫中增加 MAXLOCKS 和 LOCKLIST 參數。
- 在資料庫連接集區中增加 currentLockTimeout 內容。
- 使用「資料庫組態顧問」，並最佳化以加快異動速度。
- 將所有的「使用者應用程式」表改變爲 VOLATILE，以讓最佳化程式了解，表格基數將明顯改變。例如，若要將 AFACTIVITY 表變成 VOLATILE 表，您可發出命令：
  ALTER TABLE AFACTIVITY VOLATILE

  在「使用者應用程式」已啓動且資料庫表已建立後，必須執行 ALTER TABLE 命令。如需此陳述式的詳細資訊，請參閱 ALTER TABLE 文件。以下是所有「使用者應用程式」表的 SQL 陳述式：

  ```
  ALTER TABLE AFACTIVITY VOLATILE
  ALTER TABLE AFACTIVITYTIMERTASKS VOLATILE
  ALTER TABLE AFBRANCH VOLATILE
  ALTER TABLE AFCOMMENT VOLATILE
  ALTER TABLE AFDOCUMENT VOLATILE
  ALTER TABLE AFENGINE VOLATILE
  ALTER TABLE AFENGINESTATE VOLATILE
  ALTER TABLE AFMODEL VOLATILE
  ALTER TABLE AFPROCESS VOLATILE
  ALTER TABLE AFPROVISIONINGSTATUS VOLATILE
  ALTER TABLE AFQUORUM VOLATILE
  ALTER TABLE AFRESOURCEREQUESTINFO VOLATILE
  ALTER TABLE AFWORKTASK VOLATILE
  ALTER TABLE AF_ROLE_REQUEST_STATUS VOLATILE
  ALTER TABLE ATTESTATION_ATTESTER VOLATILE
  ALTER TABLE ATTESTATION_ATTRIBUTE VOLATILE
  ALTER TABLE ATTESTATION_QUESTION VOLATILE
  ALTER TABLE ATTESTATION_REPORT VOLATILE
  ```

```
ALTER TABLE ATTESTATION_REQUEST VOLATILE
ALTER TABLE ATTESTATION_RESPONSE VOLATILE
ALTER TABLE ATTESTATION_SURVEY_QUESTION VOLATILE
ALTER TABLE ATTESTATION_TARGET VOLATILE
ALTER TABLE AUTHPROPS VOLATILE
ALTER TABLE DATABASECHANGELOG VOLATILE
ALTER TABLE DATABASECHANGELOGLOCK VOLATILE
ALTER TABLE DSS_APPLET_BROWSER_TYPES VOLATILE
ALTER TABLE DSS_APPLET_CFG VOLATILE
ALTER TABLE DSS_APPLET_CFG_MAP VOLATILE
ALTER TABLE DSS_BROWSER_TYPE VOLATILE
ALTER TABLE DSS_CONFIG VOLATILE
ALTER TABLE DSS_EXT_KEY_USAGE_RESTRICTION VOLATILE
ALTER TABLE DSS_USR_POLICY_SET VOLATILE
ALTER TABLE JBM_COUNTER VOLATILE
ALTER TABLE JBM_DUAL VOLATILE
ALTER TABLE JBM_ID_CACHE VOLATILE
ALTER TABLE JBM_MSG VOLATILE
ALTER TABLE JBM_MSG_REF VOLATILE
ALTER TABLE JBM_POSTOFFICE VOLATILE
ALTER TABLE JBM_ROLE VOLATILE
ALTER TABLE JBM_TX VOLATILE
ALTER TABLE JBM_USER VOLATILE
ALTER TABLE PORTALCATEGORY VOLATILE
ALTER TABLE PORTALPORTLETHANDLES VOLATILE
ALTER TABLE PORTALPORTLETSETTINGS VOLATILE
ALTER TABLE PORTALPRODUCERREGISTRY VOLATILE
ALTER TABLE PORTALPRODUCERS VOLATILE
ALTER TABLE PORTALREGISTRY VOLATILE
ALTER TABLE PROFILEGROUPPREFERENCES VOLATILE
ALTER TABLE PROFILEUSERPREFERENCES VOLATILE
ALTER TABLE PROVISIONING_CODE_MAP VOLATILE
ALTER TABLE PROVISIONING_CODE_MAP_LABEL VOLATILE
ALTER TABLE PROVISIONING_VIEW_VALUE VOLATILE
ALTER TABLE PROVISIONING_VIEW_VALUE_LABEL VOLATILE
ALTER TABLE SECURITYACCESSRIGHTS VOLATILE
ALTER TABLE SECURITYPERMISSIONMETA VOLATILE
ALTER TABLE SECURITYPERMISSIONS VOLATILE
ALTER TABLE SEC_DELPROXY_CFG VOLATILE
ALTER TABLE SEC_DELPROXY_SRV_CFG VOLATILE
ALTER TABLE SEC_SYNC_CLEANUP_QUEUE VOLATILE
```

2.5 安裝 Java 開發套件

使用者應用程式安裝程式要求您針對應用程式伺服器使用正確的 Java 環境版本，如下所述：

- 對於 JBoss 5.01，您需要使用 Sun 的 Java 2 Platform Standard Edition 開發套件 1.6 版 (JDK 或 JRE)。

  附註：方便起見，JBossPostgreSQL 公用程式會爲 JBoss 安裝正確的 JRE 版本。

- 對於 WebSphere 7.0，需要使用 IBM 的 1.6 JDK。
- 對於 WebLogic 10.3，需要使用 JRockit 的 1.6 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。

附註：SUSE Linux Enterprise Server (SLES) 使用者請勿使用 SLES 隨附的 IBM JDK。此版本與該安裝版本有多處不相容。

3 安裝 Roles Based Provisioning Module

本章說明如何使用 Roles Based Provisioning Module (RBPM) 安裝程式在 Identity Manager 中安裝 Roles Based Provisioning Module 的執行時期元件。主題包括：

重要：在此版本中，您將不再能透過 iManager 建立使用者應用程式驅動程式和角色與資源服務驅動程式。系統不再支援這種建立驅動程式的方式。現在，要建立這些驅動程式，您需要使用 Designer 中提供的新的套件管理功能，如第 4 章 「建立驅動程式」(第 43 頁) 中所述。

3.1 關於安裝 Roles Based Provisioning Module

Identity Manager 4.0.1 會自動爲您安裝 RBPM 的核心執行時期元件。不過，您也可以自行啓動 Roles Based Provisioning Module 的安裝程式。

您需要在安裝了 Identity Manager Metadirectory 環境的機器上執行 RBPM 安裝程式。如果 eDirectory 未安裝在預設位置或預設 dib 位置，該安裝將會失敗。

附註：如果 eDirectory 未在預設 LDAP 連接埠 389 與 636 上執行，RBPM 安裝程式也無法正常執行。如果未在預設 LDAP 連接埠上執行，您將一直收到綱要無效且您必須執行 NrfCaseUpdate 公用程式的提示。若要修復此問題，您需要手動延伸綱要，如第 3.4 節「手動延伸綱要」(第 40 頁) 中所述。

在 Identity Manager 中安裝這些項目之後，您需要遵照第 4 章 「建立驅動程式」(第 43 頁) 中所述的步驟，建立執行使用者應用程式所需的驅動程式。

重要：如果使用 3.6.1 或先前版本的 RBPM 建立的 eDirectory 網路樹中存在使用者應用程式驅動程式，則執行 Roles Based Provisioning Module 安裝程式之前需要先執行 NrfCaseUpdate 公用程式。如果不執行該公用程式，安裝將失敗。如果要執行 4.0.1 版的全新安裝或從 3.7 版升級，則無需執行此步驟。

3.2 執行 NrfCaseUpdate 公用程式

本節介紹 NrfCaseUpdate 公用程式的詳細資料。主題包括：

3.2.1 NrfCaseUpdate 綜覽

NrfCaseUpdate 程序對於角色與資源的混合大小寫搜尋能夠提供必要的支援。此程序透過修改使用者應用程式驅動程式使用的 nrfLocalizedDescrs 與 nrfLocalizedNames 屬性來更新綱要。如果 eDirectory 網路樹是使用 3.6.1 或先前版本的 RBPM 建立的，則在安裝 RBPM 4.0.1 以及移轉 Designer 4.0.1 中現有的驅動程式之前，必須執行此程序。如果要執行 4.0.1 版的全新安裝或從 3.7 版升級，則無需執行此步驟。

3.2.2 安裝綜覽

本節爲升級與移轉現有 RBPM 環境所需完成的步驟提供了綜覽。此綜覽強調在進行任何升級之前，必須使用 Designer 4.0.1 建立使用者應用程式驅動程式的備份。

1. 安裝 Designer 4.0.1。
2. 執行 Identity Vault 健康狀態檢查以確認綱要正確延伸。請使用 TID 3564075 完成健康狀態檢查。
3. 將現有的使用者應用程式驅動程式輸入至 Designer 4.0.1 中。
4. 將 Designer 專案歸檔。它代表驅動程式 RBPM 4.0.1 之前版本的狀態。
5. 執行 NrfCaseUpdate 程序。
6. 建立新的 Designer 4.0.1 專案並輸入使用者應用程式驅動程式，爲移轉做好準備。
7. 安裝 RBPM 4.0.1。
8. 使用 Designer 4.0.1 移轉驅動程式。
9. 部署移轉後的驅動程式。

3.2.3 NrfCaseUpdate 如何對綱要產生影響

NrfCaseUpdate 公用程式在更新 eDirectory 綱要中現有的屬性時，會刪除這些屬性中所有現有的例項。使用者應用程式驅動程式會使用這些屬性，因而將受到此綱要更新的影響，特別是角色與職務分離名稱及描述、自定證明申請以及報告。

NrfCaseUpdate 程序會在執行綱要更新前，提供用於將現有使用者應用程式驅動程式匯出至 LDIF 檔案的公用程式，以此來更新這些驅動程式。在綱要更新後匯入 LDIF 檔案會重新建立在綱要更新期間刪除的所有物件。

同樣，爲了起到預防作用，一定要備份所有現有的使用者應用程式驅動程式。請記住，綱要更新會影響所有 Identity Manager 分割區，因此很有必要使用 NrfCaseUpdate 輸出網路樹中的所有使用者應用程式驅動程式。

3.2.4 建立使用者應用程式驅動程式的備份

建議使用 Designer 建立使用者應用程式驅動程式的備份。執行 NrfCaseUpdate 程序前，應遵照以下程序備份現有的使用者應用程式驅動程式：

1. 安裝與 RBPM 4.0.1 一起提供的 Designer 4.0.1。
2. 建立 Identity Vault，並將其對應至包含使用者應用程式驅動程式的 Identity Manager 伺服器。
3. 使用 *「即時」* -> *「輸入」* 指令匯入驅動程式集與使用者應用程式驅動程式。
4. 儲存並歸檔此 Designer 專案。

3.2.5 使用 NrfCaseUpdate

NrfCaseUpdate 會提示您匯出每個驅動程式，然後再執行綱要更新。如果不確定是否存在使用者應用程式驅動程式，或是不確定其位置，請不要繼續，因爲綱要更新可能會使現有的使用者應用程式驅動程式失效。

Identity Manager 安裝目錄 (通常爲 /root/idm/jre) 下提供的 JRE 可以用於執行 NrfCaseUpdate。如果需要至 eDirectory 的 SSL 連線，應遵照第 3.2.7 節「讓 JRE 進行 SSL 連線」(第 33 頁) 的指示讓 JRE 進行 SSL 連線。

或者，您也可以從包含 eDirectory 證書的 JRE 所在的主機 (例如使用者應用程式伺服器主機) 遠端執行 NrfCaseUpdate 公用程式。這種情況下，需要在將所有驅動程式匯出至 LDIF 之後、綱要更新之前，使用 CTRL-C 結束 NrfCaseUpdate 公用程式。然後，可以使用 ndssch 指令手動更新 eDirectory 主機上的綱要，如下所示：

```
ndssch -h hostname adminDN update-nrf-case.sch
```

附註：NrfCaseUpdate 可以使用多種指令行引數。使用 -help 或 -? 可以查看詳細資訊。

遵循以下步驟執行 NrfCaseUpdate ：

1. 在執行 NrfCaseUpdate 公用程式之前，確定已經完成 Identity Vault 健康狀態檢查。請使用 TID 3564075 完成健康狀態檢查。
2. 啓動公用程式之前先識別現有使用者應用程式驅動程式的所有 DN。您需要有驗證身分證明才能將這些驅動程式匯出至 LDIF。
3. 執行 NrfCaseUpdate 公用程式。也可以選擇使用 -v 選項取得更詳細的輸出資訊：

   ```
   /root/idm/jre/bin/java -jar NrfCaseUpdate.jar -v
   ```
4. 系統會詢問您是否已有使用者應用程式驅動程式。如果有，請做肯定回答。否則做否定回答，並跳至步驟 15 (第 32 頁)。

   ```
   Do you currently have a User Application Driver configured [DEFAULT true] :
   ```
5. 接著，公用程式會詢問您是否有多個使用者應用程式驅動程式。如果有，請做肯定回答：

   ```
   Do you currently have more than one (1) User Application Driver configured
   [DEFAULT false] :
   ```
6. 指定擁有適當身分證明、可匯出使用者應用程式驅動程式之管理員的 DN ：

   ```
   Specify the DN of the Identity Vault administrator user.
   This user must have inherited supervisor rights to the user application
   driver specified above.
   (e.g. cn=admin,o=acme):
   ```

7 輸入此管理員的密碼：

```
Specify the Identity Vault administrator password:
```

8 輸入代管使用者應用程式驅動程式之 Identity Manager 伺服器的主機名稱或 IP 位址：

```
Specify the DNS address of the Identity Vault (e.g acme.com):
```

9 指定連線所使用的連接埠：

```
Specify the Identity Vault port [DEFAULT 389]:
```

10 下一個問題是詢問您是否使用 SSL 進行連線。如果要使用 SSL，JRE 要求托管儲存區中存在 eDirectory 證書。? 要堅持使用證書，請遵照第 3.2.7 節「讓 JRE 進行 SSL 連線」(第 33 頁) 的指示。

```
Use SSL to connect to Identity Vault: [DEFAULT false] :
```

11 指定要匯出之使用者應用程式驅動程式的完全合法的可辨識名稱：

```
Specify the fully qualified LDAP DN of the User Application driver located
in the Identity Vault
(e.g. cn=UserApplication,cn=driverset,o=acme):
```

如果 DN 包含空格，則必須將空格括在單引號中，如下所示：

```
'cn=UserApplication driver,cn=driverset,o=acme'
```

12 指定使用者應用程式要匯出至其中的 LDIF 檔案的名稱：

```
Specify the LDIF file name where the restore data will be written (enter
defaults to nrf-case-restore-data.ldif):
```

13 公用程式會張貼儲存到 LDIF 中之物件的相關資訊。

14 如果您指出自己擁有多個驅動程式，則會看到以下提示：

```
You indicated you have more than one (1) User Application Driver to
configure.
Do you have another driver to export? [DEFAULT false] :

If you have another driver to export then specify true. The utility will
repeat Steps 5 through 12 for each driver.

If you do not have another driver to export then specify false. Ensure that
you have exported all existing drivers before proceeding as the utility
will proceed with the schema update.
```

15 系統會提示您輸入 ndssch 公用程式的位置以及一般位置。ndssch 公用程式用於更新綱要。

```
Please enter the path to the schema utility:
For Unix/Linux typically /opt/novell/eDirectory/bin/ndssch
For Windows C:\Novell\NDS\schemaStart.bat:
```

16 公用程式會張貼綱要更新的狀態訊息：

```
Schema has successfully been updated for mixed case compliance!
```

附註：請務必給予 eDirectory 充分的時間來完成綱要變更同步。如果分配的時間太短，可能導致 LDIF 檔案輸入失敗。

---

17 在輸入 LDIF 檔案之前再執行一次 Identity Vault 健康狀態檢查，以確定綱要已正確延伸。請使用 TID 3564075 完成健康狀態檢查。

18 匯出所有驅動程式並成功套用綱要更新後，需要匯入每個 LDIF 檔案。您應指示允許傳送 ice 指令中的參考。建議使用以下指令行：

```
ice -l [mylogfile.log] -v -SLDIF -f [your_created_ldif] -c -DLDAP -s
[hostname] -p [389/636] -d [cn=myadmin,o=mycompany] -w [MYPASSWORD] -F -B
```

19 重新匯入所有驅動程式後，確認 NrfCaseUpdate 程序是否成功。如需相關資訊，請參閱第 3.2.6 節「NrfCaseUpdate 程序的確認」(第 33 頁)。

20 確認 NrfCaseUpdate 程序成功後，可以繼續安裝 RBPM 4.0.1。

3.2.6 NrfCaseUpdate 程序的確認

重新匯入所有驅動程式後，在使用者應用程式中檢閱以下項目，以確認還原是否成功：

- 角色名稱與描述
- 職務分離名稱與描述
- 證明申請，包括自定申請
- 報告

確認完成後，可以繼續進行安裝並升級到 RBPM 4.0.1。

3.2.7 讓 JRE 進行 SSL 連線

本節介紹如何將 JRE 設定爲使用 SSL 連線。

首先，從 Identity Vault 中的證書管理中心匯出自行簽署的證書：

1 在 iManager 的「*角色及任務*」檢視窗中，按一下「*目錄管理*」>「*修改物件*」。

2 選取 Identity Vault 的證書管理中心物件，然後按一下「*確定*」。通常可在安全性容器中找到該物件，其命名爲 *網路樹名稱* CA.Security。

3 按一下「*證書*」>「*自行簽署的證書*」。

4 按一下「*輸出*」。

5 當詢問您是否要匯出含證書的私密金鑰時，請按一下「*否*」，然後按一下「*下一步*」。

6 選取二進位 DER 格式。

7 按一下「*儲存匯出的證書*」連結。

8 瀏覽至電腦上要儲存檔案的位置，然後按一下「*儲存*」。

9 按一下「*關閉*」。

接著，將自行簽署的證書匯入到 JRE 的托管儲存區中。

1 使用 JRE 中包含的 keytool 公用程式。

2 在指令提示中輸入以下指令，將證書匯入到角色對應管理員的托管儲存區中：

```
keytool -import -file name_of_cert_file -trustcacerts -noprompt -keystore
filename -storepass password
```

例如：

```
keytool -import -file tree_ca_root.b64 -trustcacerts -noprompt -keystore
cacerts -storepass changeit
```

3.2.8 還原失效的使用者應用程式驅動程式

如果在使用 NrfCaseUpdate 處理現有的使用者應用程式驅動程式之前，綱要更新已經套用至該驅動程式，則驅動程式將失效，您需要使用備份還原該驅動程式。

重要： *千萬不要*刪除或重新命名失效的使用者應用程式驅動程式，否則會使所有驅動程式的關聯都失效。此外，如果您在角色與資源服務驅動程式執行期間刪除了使用者應用程式驅動程式，則角色與資源服務驅動程式會偵測到角色刪除事件，並移除指定使用者的角色。

此外，由於綱要變更無法以這種方式進行調整，因此僅將備份的驅動程式重新部署至 Identity Manager 並不夠。以下程序透過部署重新命名後的驅動程式副本以產生要還原的資料，藉以執行還原操作。

以下程序概述了使用 Designer 4.0.1 還原使用者應用程式驅動程式備份的程序：

1. 重新啓動 eDirectory 伺服器，以確保綱要修改已生效。
2. 開啓包含使用者應用程式驅動程式 UserAppDriver 之備份的 Designer 4.0.1 專案的副本。由於此程序會修改驅動程式的名稱，因此一定要使用專案的副本。
3. 選取使用者應用程式驅動程式與 Identity Vault 之間的連接器，然後按一下滑鼠右鍵並選擇「*內容*」。
4. 指定新名稱，例如 UserAppDriver_restore。選取「*套用*」，然後按一下「*確定*」。
5. 按一下「*儲存*」以儲存專案。
6. 選取 ID Vault 並選擇 *「即時」* -> *「綱要」* -> *「比較」*以同步化 ID Vault 綱要，然後選擇「*更新 Designer 以執行調整動作*」。
7. 儲存專案。
8. 選取驅動程式並選擇 *「驅動程式」* -> *「部署」*」，藉以部署重新命名後的驅動程式。
9. 執行 NrfCaseUpdate 並將新命名的驅動程式匯出至 LDIF 檔案。
10. 建立 LDIF 檔案的副本以進行編輯。
11. 編輯 LDIF 檔案並重新命名所有驅動程式參考，以反映您正在還原的使用者應用程式驅動程式。例如，如果您的原始使用者應用程式驅動程式爲 cn=UserAppDriver，則需要將 cn=UserAppDriver_restore 重新命名爲 cn=UserAppDriver。此步驟將有效建立一個反映實際使用者應用程式驅動程式的 LDIF 檔案。
12. 使用 ice 匯入修改後的 LDIF 檔案：

    ```
    ice -l[mylogfile.log] -v -SLDIF -f[your_created_ldif] -c -DLDAP -
    s[hostname] -p[389/636] -d[cn=myadmin,o=mycompany] -w[MYPASSWORD] -F -B
    ```

13. 注意使用 ice 匯入的狀態，以確保其成功。
14. 遵照第 3.2.6 節「NrfCaseUpdate 程序的確認」(第 33 頁) 中的指示確認驅動程式的還原情況。
15. 從驅動程式集中刪除重新命名後的驅動程式。

3.3 執行 RBPM 安裝程式

1. 啓動平台適用的安裝程式：

   Linux。

   ```
   rbpm_driver_install_linux.bin
   ```

Solaris。

`rbpm_driver_install_solaris.bin`

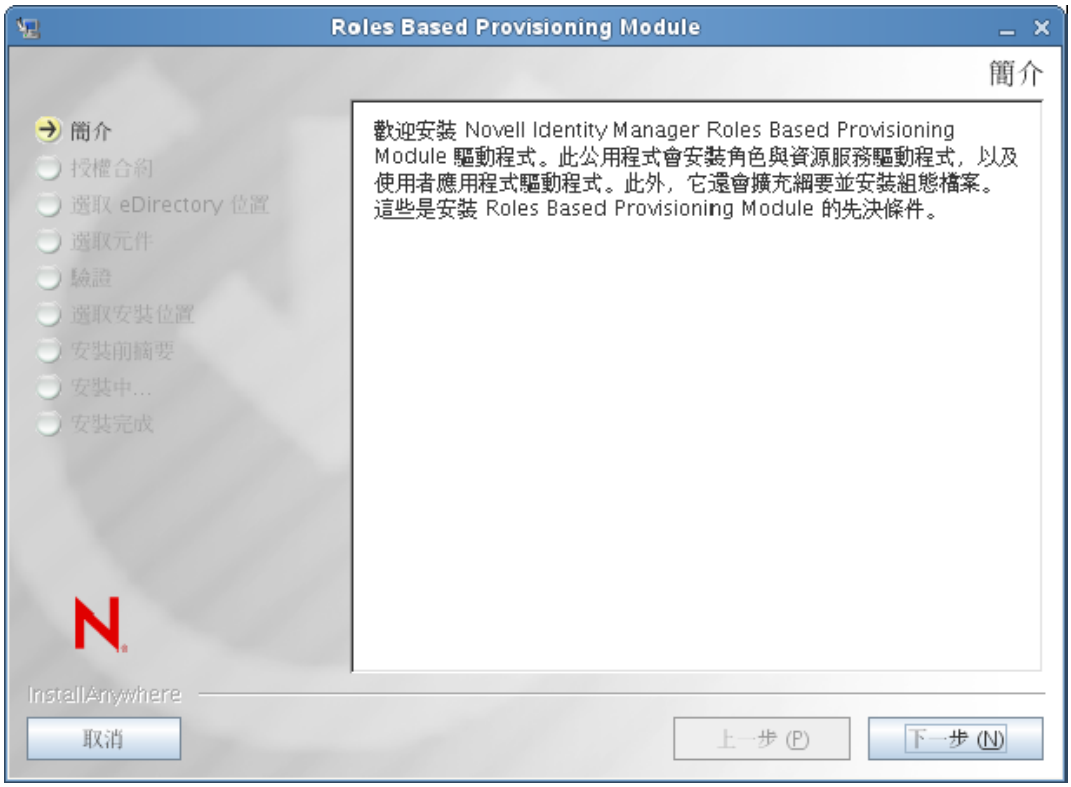
Windows。

`rbpm_driver_install.exe`

安裝程式啓動時會提示您選擇語言：

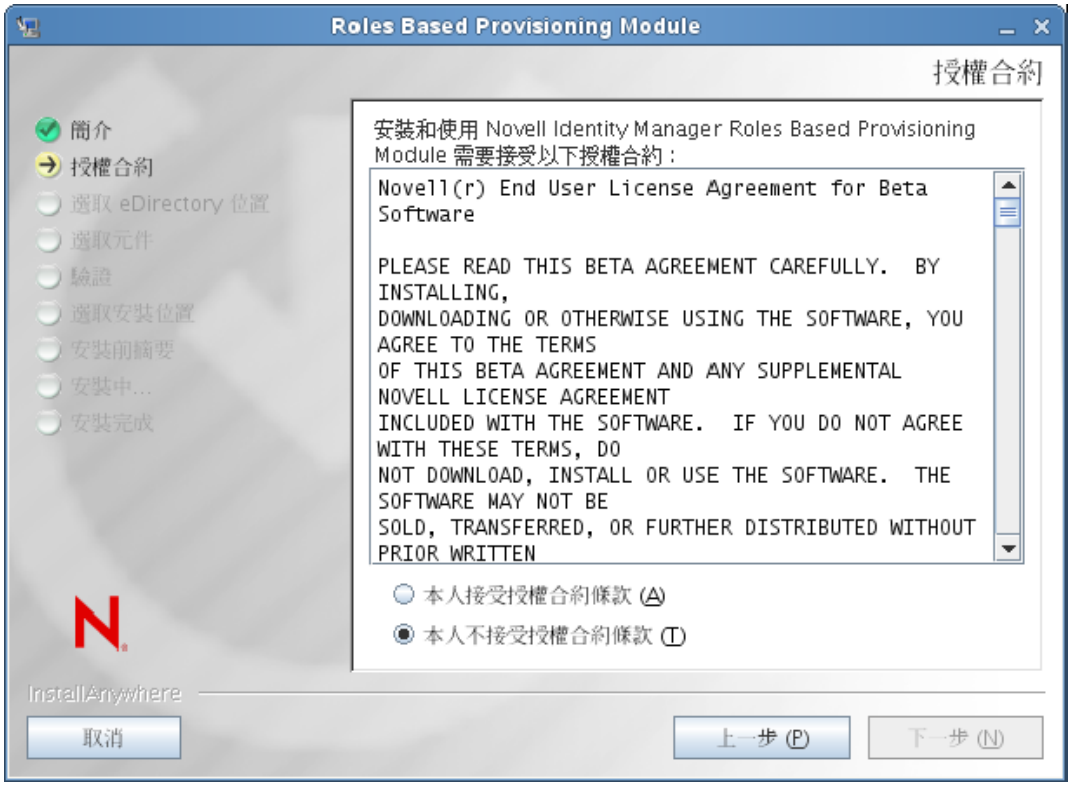
2 選擇安裝使用的語言，然後按一下「確定」。

安裝程式會顯示「簡介」螢幕。



3 按一下「*下一步*」。

安裝程式會顯示「授權合約」螢幕。



4 確認授權合約並按一下「*下一步*」。

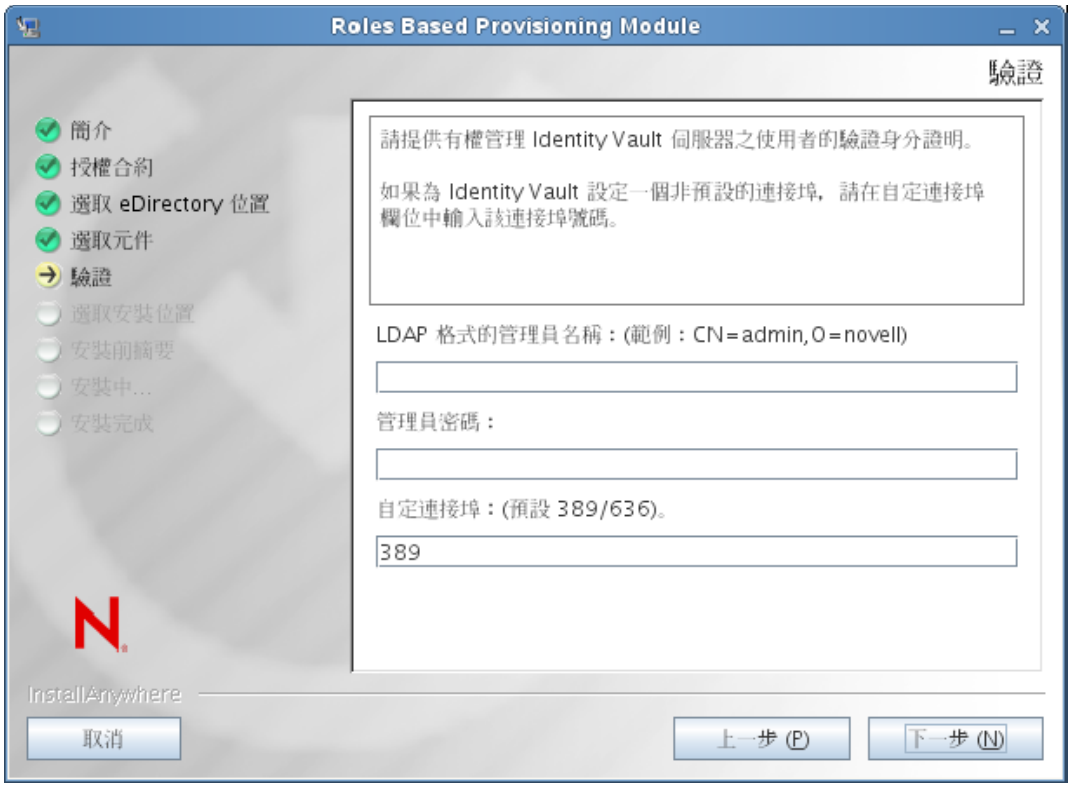
安裝程式會顯示「選取元件」螢幕，其中列出了執行 RBPM 使用者應用程式所需的 Metadirectory 元件：

元件說明如下：

元件	描述
Roles Based Provisioning Module	安裝使用者應用程式驅動程式以及角色與資源驅動程式。
綱要延伸	安裝 eDirectory 綱要延伸。
組態檔案	安裝驅動程式組態檔案。

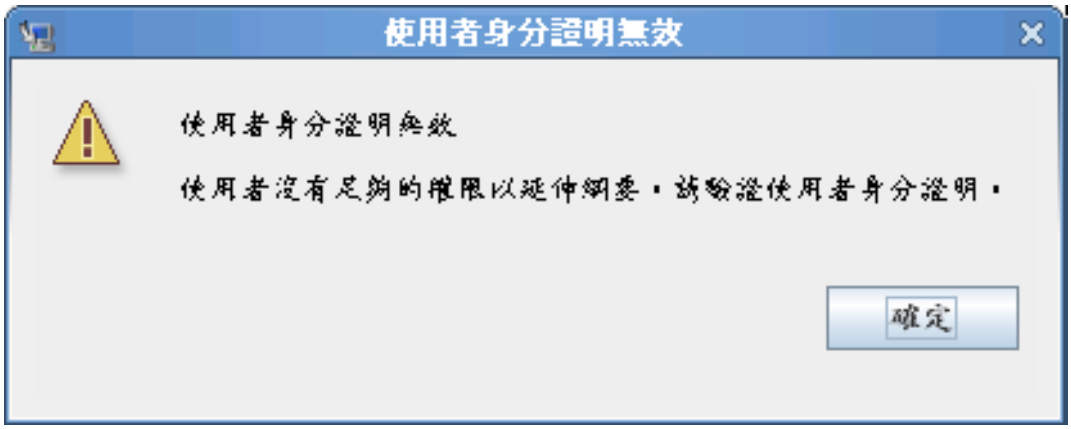
5 選取要安裝的元件，然後按一下「*下一步*」。一般情況下，可以安裝所有元件。

安裝程式會顯示「驗證」螢幕：

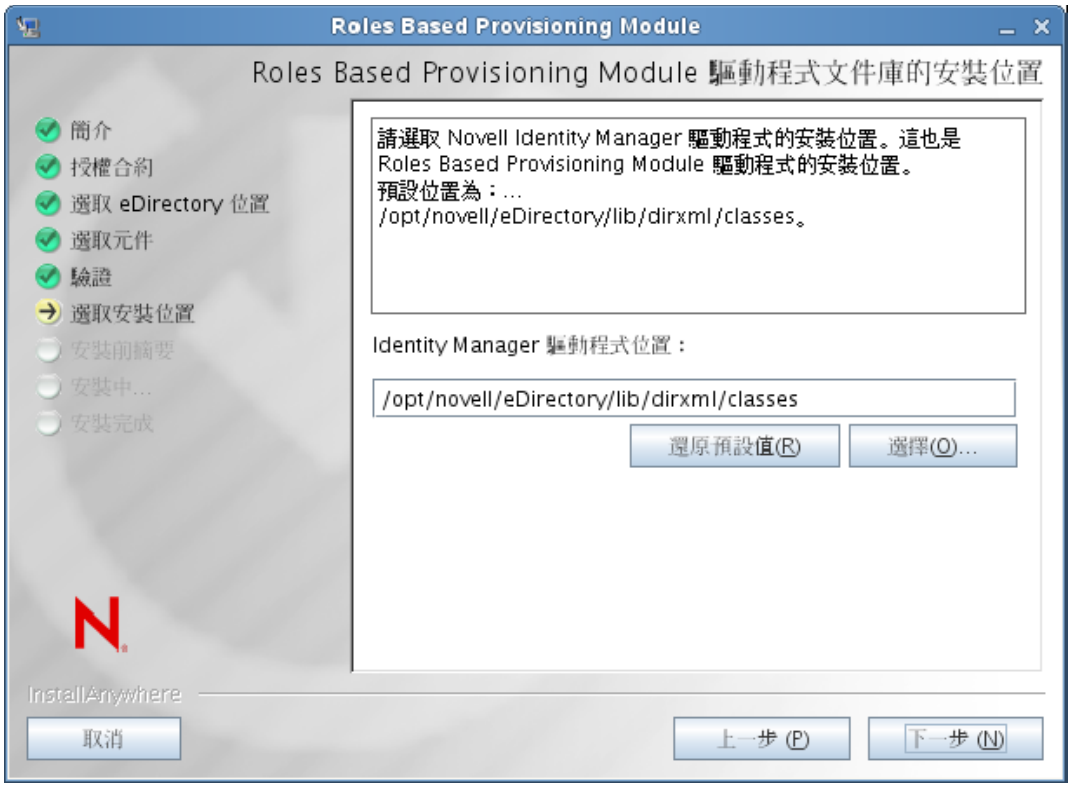


6 以 LDAP 格式提供管理員名稱並輸入密碼，另外還請指定 LDAP 伺服器的連接埠。

如果使用者身分證明無效，或者使用者不具備必要權限，則安裝程式會顯示出錯螢幕：



如果使用者身分證明有效，且使用者具備適當的權限，則安裝程式會顯示「Roles Based Provisioning Module 驅動程式文件庫的安裝位置」螢幕：

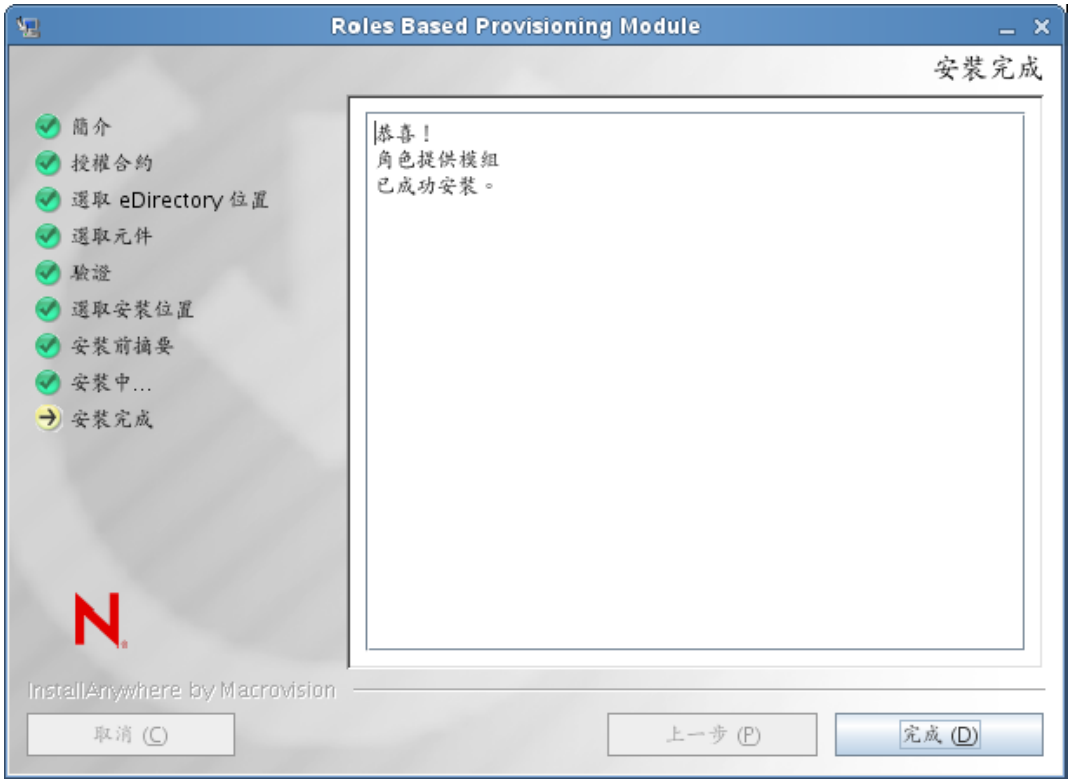


7 指定磁碟上用於儲存驅動程式文件庫的目標位置，然後按「*下一步*」。

安裝程式會顯示「安裝前摘要」螢幕：

8 如果摘要資訊正確，請按一下「*安裝*」，開始執行安裝程序。

當安裝程序完成時，安裝程式會顯示「安裝完成」螢幕：



附註：如果需要解除安裝與 RBPM 相關聯的執行時期元件，解除安裝程式會自動將伺服器機器重新開機，除非您正在以靜默模式在 Windows 上執行解除安裝程式。此種情況下，您需要手動將 Windows 機器重新開機。此外，如果想在整合式安裝程式之外解除安裝 Identity Manager，則需要先停止 NDS 服務，然後再啓動解除安裝程式。

3.4 手動延伸綱要

本節提供手動延伸綱要的指示。只有在解決 eDirectory 未安裝在預設位置或未在預設 LDAP 連接埠 389 與 636 上執行的情況下所發生的問題時，才需要執行這些步驟。

若要手動延伸綱要 (Windows)：

1 在安裝 Identity Manager 之後，停止 eDirectory。

2 執行以下指令，以延伸位於 eDirectory 安裝位置之 sch_nt.cfg 中列出的綱要。

```
<eDirLocation>\schemaStart.bat <eDirLocation> yes <admin name with tree>
<password> yes 6 " " " <schemafileName>"
"<serverName>" <dibPathLocation>
```

附註：*<dibPathLocation>* 必須包含 DIBFiles 資料夾。

以下爲一個指令範例：

```
C:\eDir\NDS\schemaStart.bat "C:\eDir\NDS" yes
".cn=admin.o=n.T=IDM-INSTALLISSUE." "n" yes 6 " "
"C:\eDir\NDS\ vrschema.sch" ".CN=WIN2008-64-NDS.O=n.T=IDMINSTALLISSUE."
"C:\DIB\NDS\DIBFiles"
```

附註：上面的指令並不會使用 sch_nt.cfg 來延伸所有綱要檔案，而是以手動方式延伸 sch_nt.cfg 中指定的每個綱要檔案。

3. 取消勾選「*選取元件*」視窗中的「*綱要延伸*」選項，然後安裝角色與資源驅動程式 (依照第 3.3 節「執行 RBPM 安裝程式」(第 34 頁) 中所述)。完成安裝。
4. 安裝角色與資源驅動程式之後，透過執行步驟 2 (第 40 頁) 中列出的指令，延伸角色綱要檔案 srvprv.sch 與 nrf-extensions.sch。

附註：此程序會使用 schemaStart.bat 延伸所需的綱要檔案。

5. 使用步驟 2 (第 40 頁) 中列出的指令，延伸 NrfCaseupdate 綱要 (update-nrf-case.sch)。
6. 啓動 eDirectory。

若要手動延伸綱要 (SUSE)：

1. 取消勾選「*選取元件*」視窗中的「*綱要延伸*」選項，然後安裝角色與資源驅動程式 (依照第 3.3 節「執行 RBPM 安裝程式」(第 34 頁) 中所述)。按「*下一步*」。
2. 爲驅動程式選擇適當的安裝位置，然後按「*下一步*」。
3. 爲驅動程式組態檔案選擇適當的安裝位置，然後按「*下一步*」。完成安裝。

   步驟 1 至 3 會複製 eDirectory 非預設位置中的驅動程式與驅動程式組態檔案。
4. 執行 ndssch 指令以延伸綱要 (即 srvprv.sch 與 nrf-extensions.sch)。

   ```
   ndssch [-h hostname[:port]] [-t tree_name] admin-FDN schemafile...
   ```

   例如：

   ```
   ndssch -h 172.16.1.137:524 -t TESTTREE -p 'PASSWORD'
   .cn=admin.o=novell.T=TESTTREE.
   /opt/novell/eDirectory/lib/nds-schema/srvprv.sch'
   ```
5. 重複步驟 4 以延伸 nrf-extensions.sch。

建立驅動程式

4

本章說明如何建立使用 Roles Based Provisioning Module (RBPM) 時所需的驅動程式。主題包括：

必須先建立使用者應用程式驅動程式，才能建立角色與資源服務驅動程式。因爲角色與資源服務驅動程式會參考使用者應用程式驅動程式中的角色 Vault 容器 (RoleConfig.AppConfig)，所以需要先建立使用者應用程式驅動程式。

驅動程式組態支援允許您執行下列工作：

- 將一個使用者應用程式驅動程式與一個角色與資源服務驅動程式相關聯。
- 將一個使用者應用程式與一個使用者應用程式驅動程式相關聯。

重要：在此版本中，您將不再能透過 iManager 建立使用者應用程式驅動程式和角色與資源服務驅動程式。系統不再支援這種建立驅動程式的方式。現在，要建立這些驅動程式，您需要使用 Designer 中提供的新的套件管理功能，如下所述。

4.1 在 Designer 中建立驅動程式

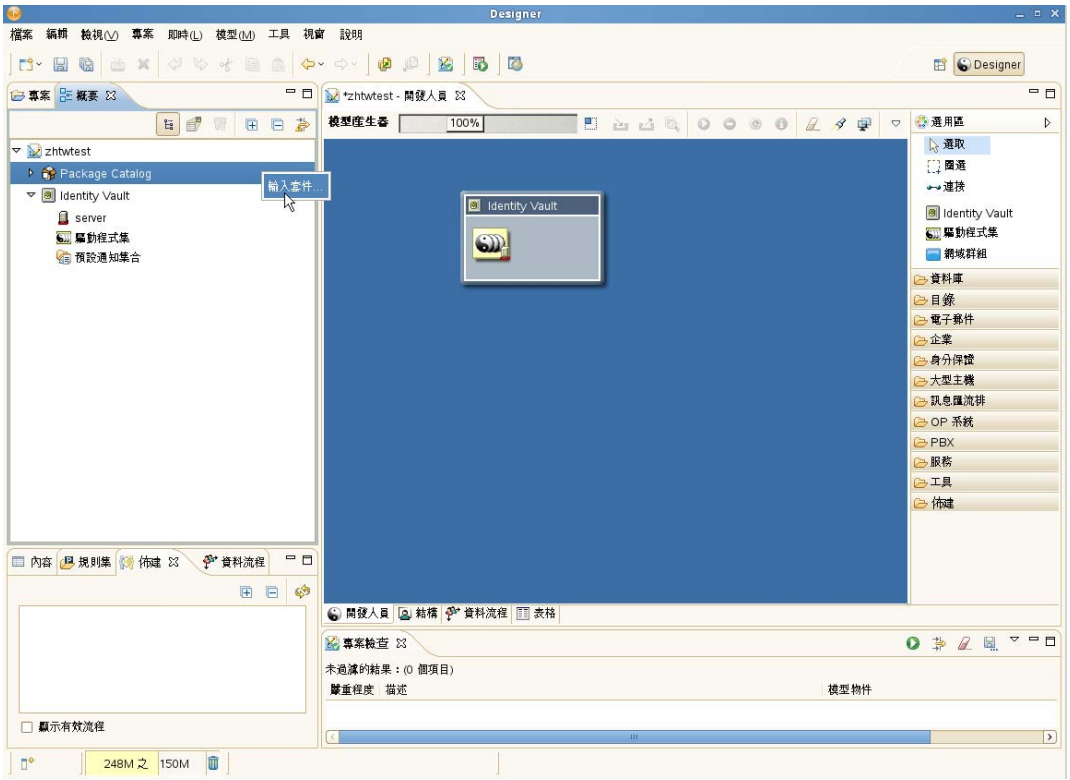
本節提供在 Designer 中建立驅動程式的指示。主題包括：

4.1.1 安裝套件

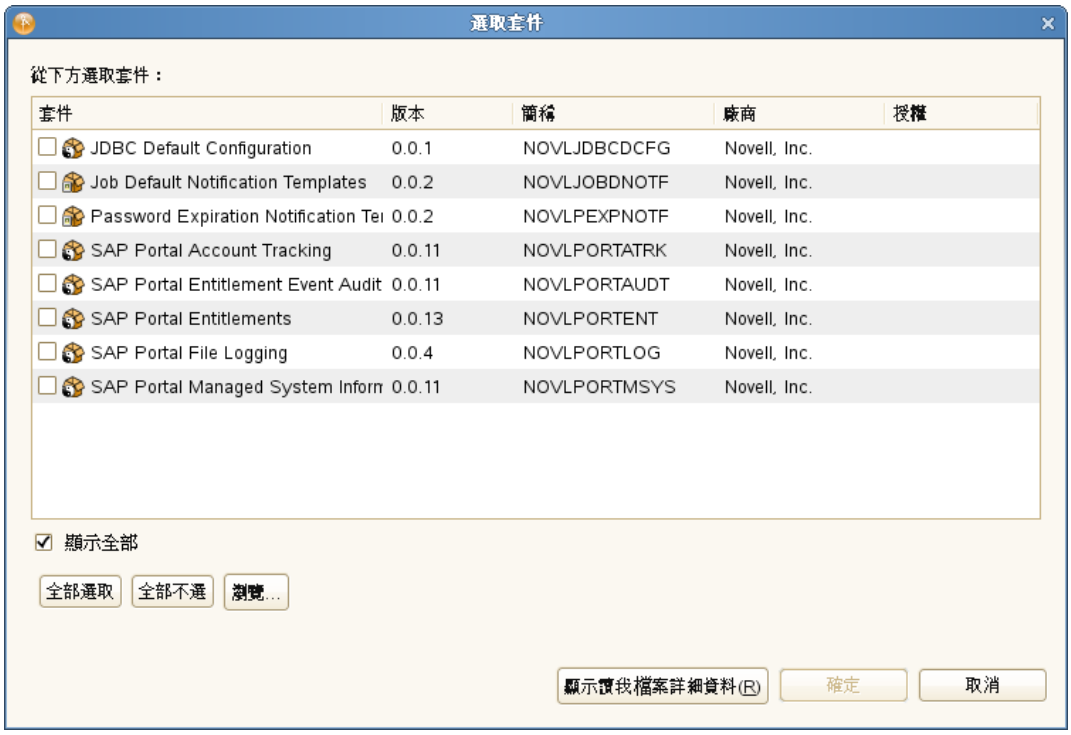
在嘗試設定驅動程式之前，您需要先確定套件目錄中存在所有必要的套件。在建立新的 Identity Manager 專案時，使用者介面會自動提示您將幾個套件輸入至新的專案中。若您在建立專案時選擇不輸入套件，則需要在以後予以安裝，如下所述。

若要在建立新的 Identity Manager 專案之後安裝套件：

1 在 Designer 中建立新的 Identity Manager 專案之後，選取「*套件目錄*」，然後按一下「*輸入套件*」。



Designer 會顯示「*選取套件*」對話方塊。



2 按一下「*全部選取*」，然後按一下「*確定*」。

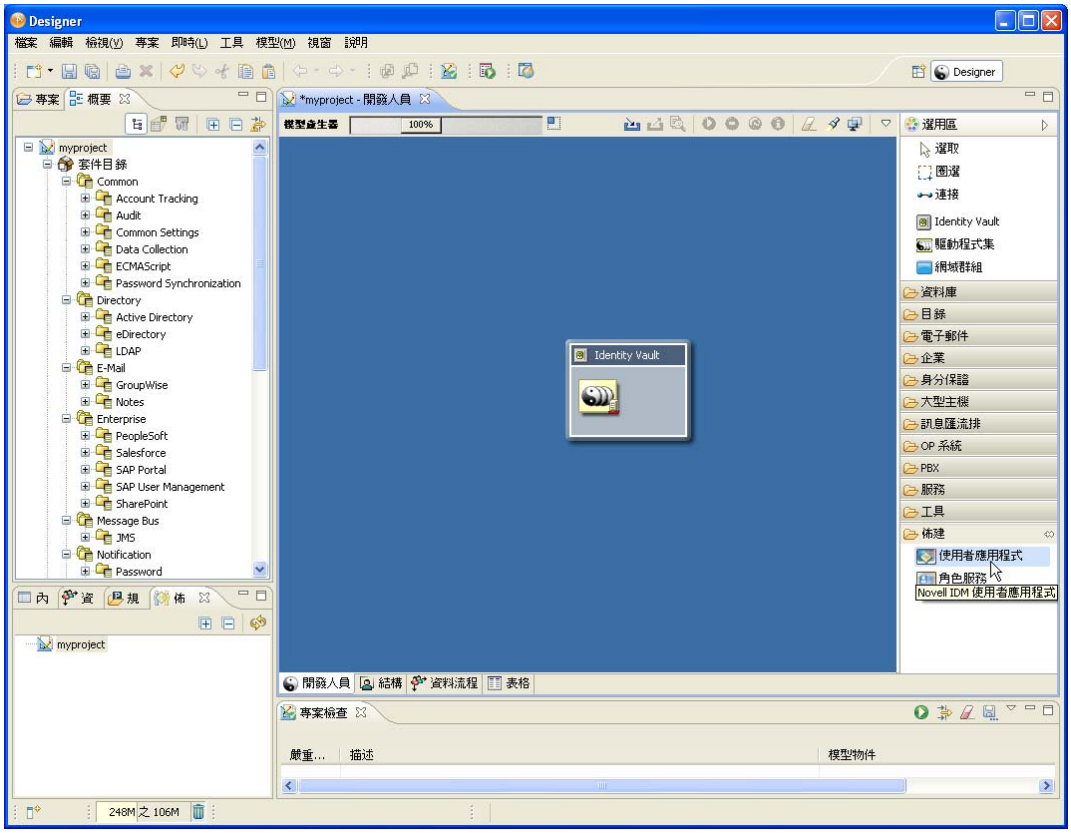
Designer 會在「*套件目錄*」下新增數個新的套件資料夾。這些套件資料夾與 Designer 中「*模型產生器*」檢視窗右側調色盤中的一些物件相對應。

3 按一下「*儲存*」以儲存專案。

4.1.2 在 Designer 中建立使用者應用程式驅動程式

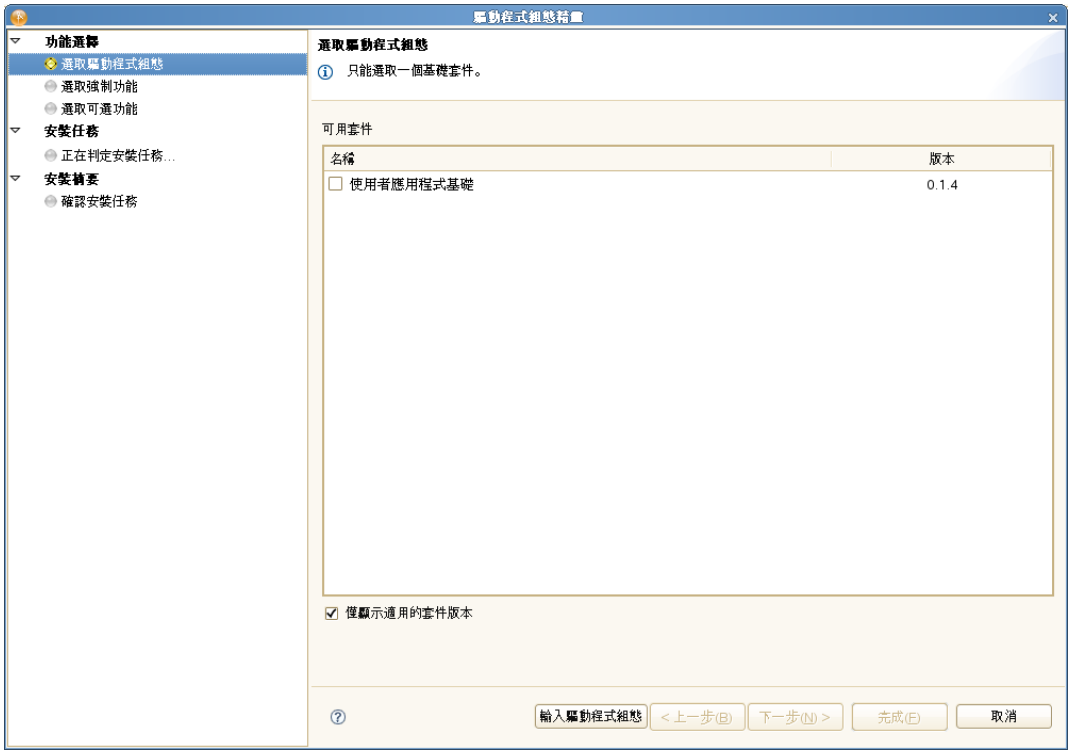
若要在 Designer 中建立使用者應用程式驅動程式：

1 在「*模型產生器*」檢視窗的調色盤中選取「*使用者應用程式*」。

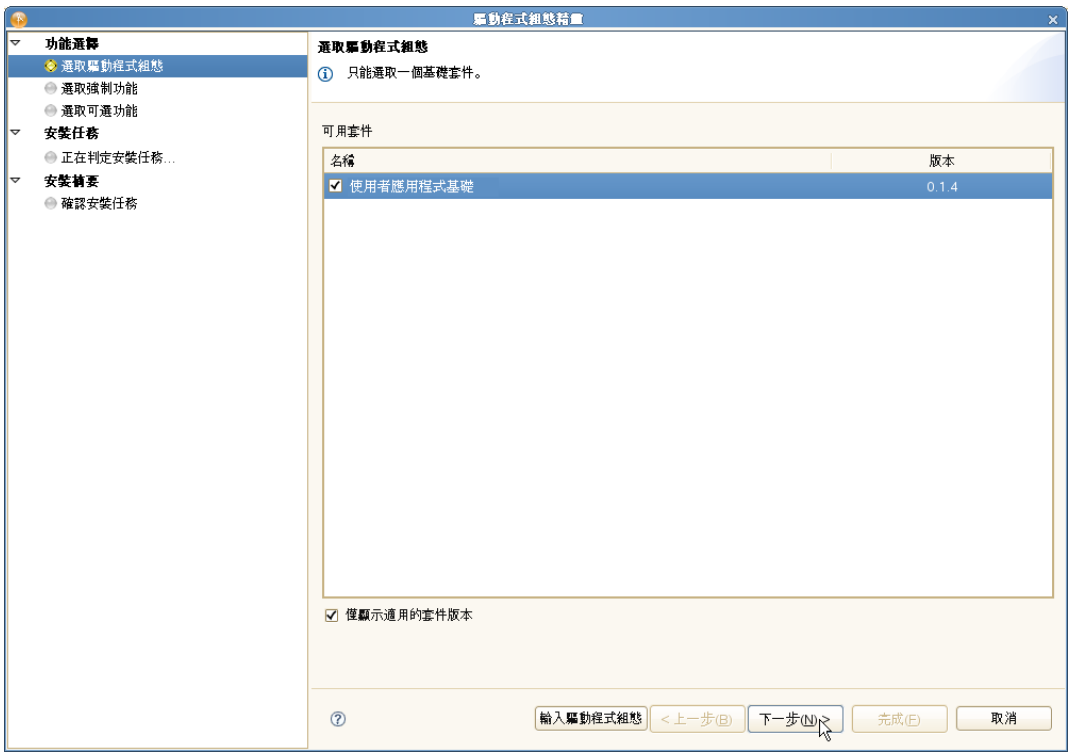


2 將「*使用者應用程式*」的圖示拖曳至「*模型產生器*」檢視窗中。

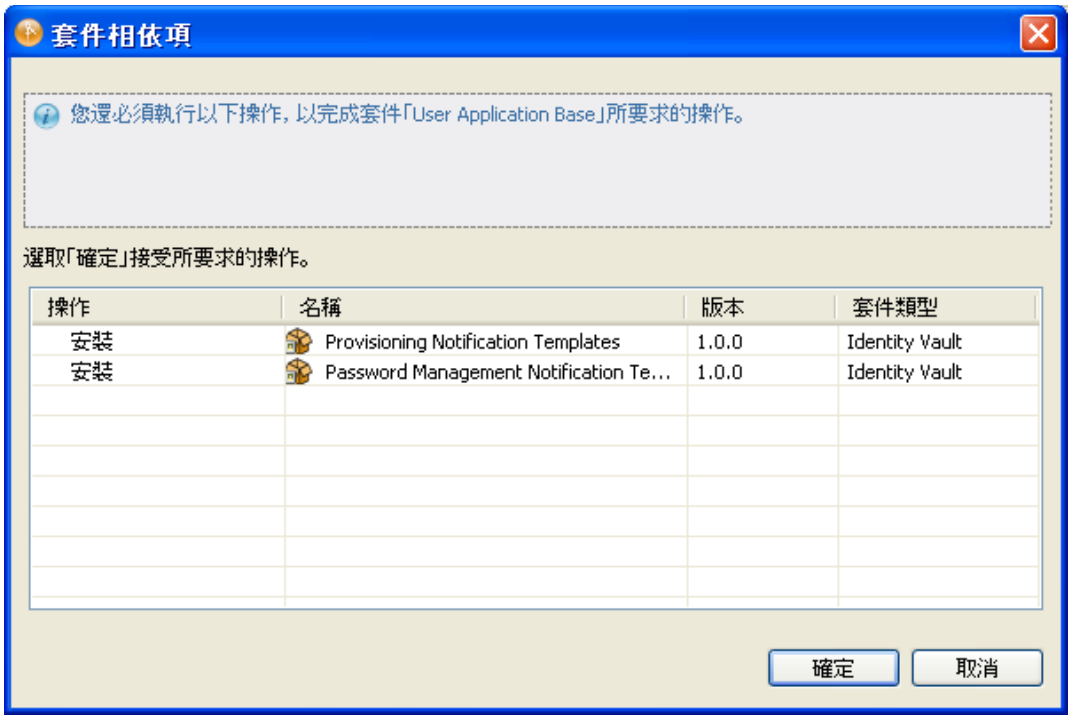
Designer 會顯示「*驅動程式組態精靈*」：



3 選取「*使用者應用程式基礎*」，然後按「*下一步*」：



介面會顯示一個對話方塊，通知您需要幾個額外的套件：



4 按一下「*確定*」安裝所需的套件。

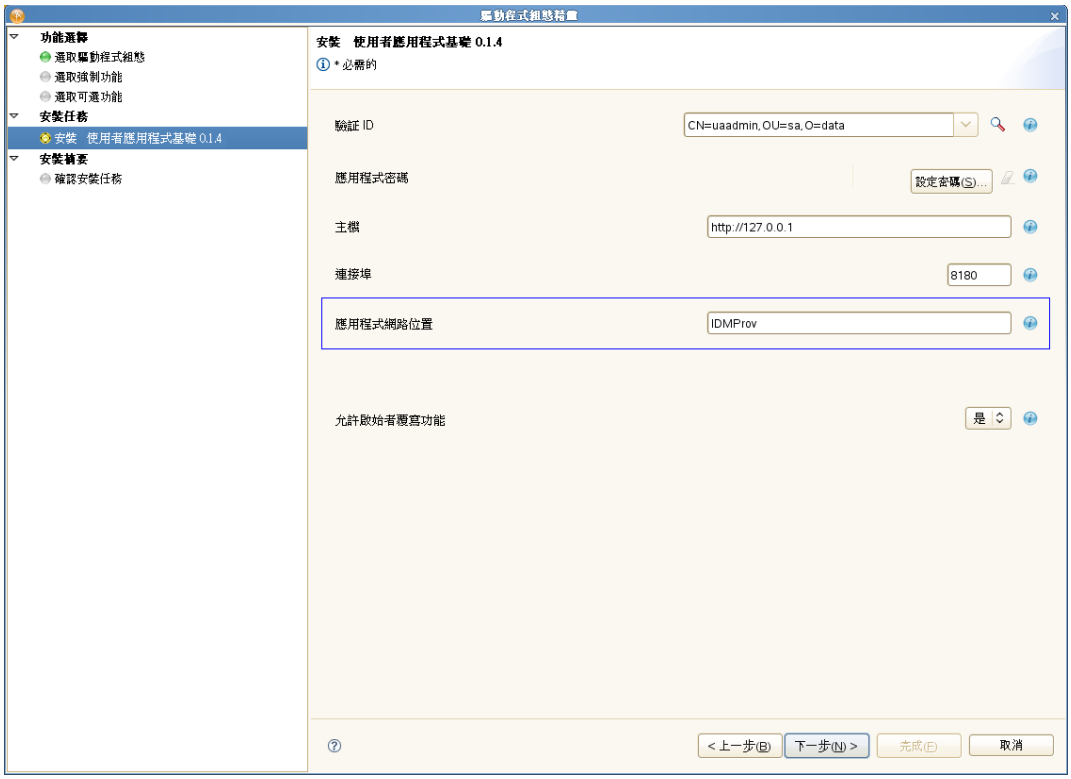
此時，精靈會顯示一個螢幕，讓您爲驅動程式命名。

5 您可以接受預設驅動程式名稱，也可以根據需要加以變更。

按「*下一步*」。

現在，精靈會顯示一個螢幕，讓您指定驅動程式的連接參數。

6 指定使用者應用程式管理員的 ID 與密碼，以及使用者應用程式伺服器的主機、連接埠與應用程式網路位置。若要允許佈建管理員以其他人 (佈建管理員指定爲該使用者的代理) 的名義啓動工作流程，請對「*允許啓始者覆寫功能*」選取「*是*」：



精靈會顯示「*確認安裝任務*」螢幕。

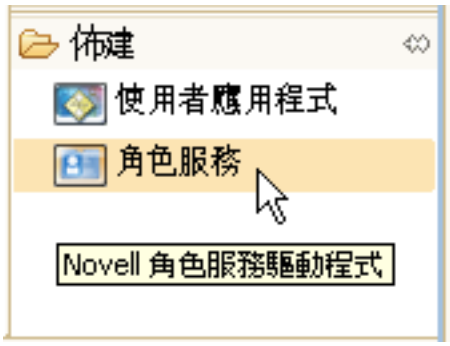
7 如果所有資訊都正確無誤，請按一下「*完成*」。

Designer 會將「*使用者應用程式*」驅動程式新增至「*模型產生器*」檢視窗：

4.1.3 在 Designer 中建立角色與資源服務驅動程式

若要在 Designer 中建立角色與資源服務驅動程式：

1 在「*模型產生器*」檢視窗的調色盤中選取「*角色服務*」：



2 將「*角色服務*」的圖示拖曳至「*模型產生器*」檢視窗中。

Designer 會顯示「*驅動程式組態精靈*」。

3 選取「*角色與資源服務基礎*」，然後按「*下一步*」。

精靈會顯示一個螢幕，讓您指定驅動程式的名稱。

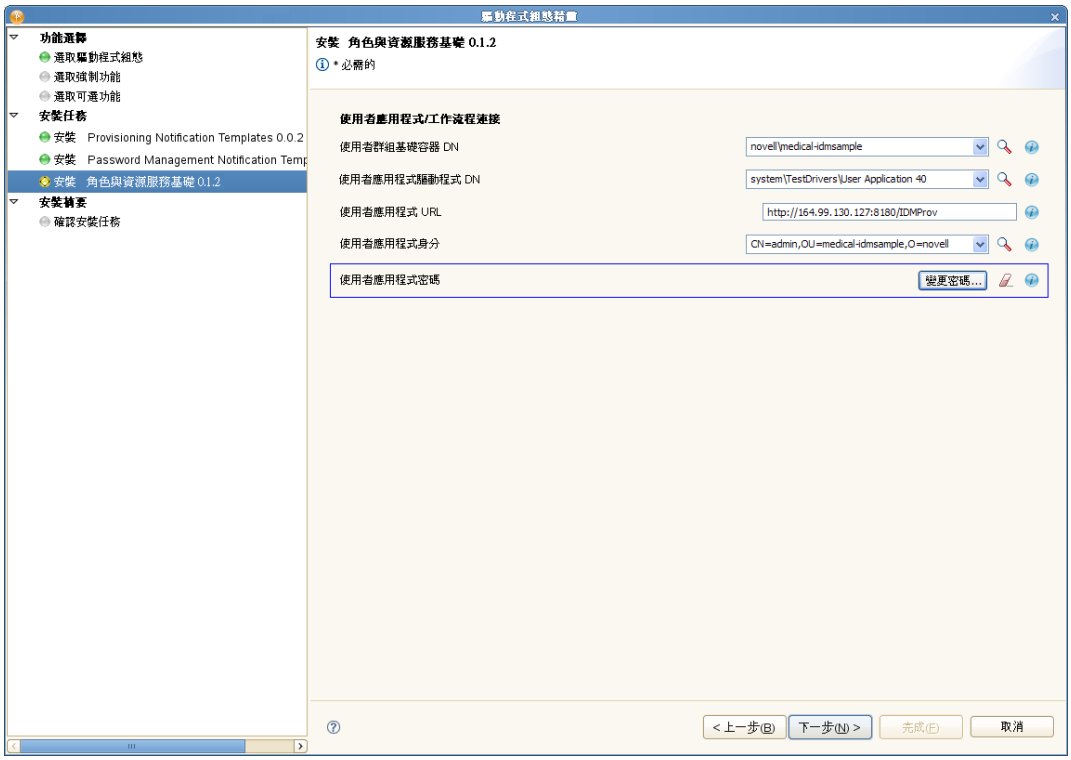
4 您可以接受預設驅動程式名稱，也可以根據需要加以變更。

按「*下一步*」。

現在，精靈會顯示一個螢幕，讓您指定驅動程式的連接參數。

5 指定基礎容器及您剛才建立之使用者應用程式驅動程式的 DN。由於該驅動程式尚未部署，瀏覽功能不會顯示剛才設定的使用者應用程式驅動程式，因此您可能需要鍵入驅動程式的 DN。

另外請提供使用者應用程式的 URL，以及使用者應用程式管理員的 ID 與密碼：



按「*下一步*」。

此時精靈會顯示「*確認安裝任務*」螢幕：

6 如果所有資訊都正確無誤，請按一下「*完成*」。

Designer 會將「*角色服務*」驅動程式新增至「*模型產生器*」檢視窗：

4.1.4 部署驅動程式

若要部署剛才設定的驅動程式：

1. 選取「驅動程式集」(在「*模型產生器*」或「*大綱*」檢視窗中)。
2. 選擇「*即時*」>「*部署*」。

   Designer 會開啓一個進度視窗，顯示正在部署的物件：

附註：複製 eDirectory 環境時，必須確保複製本包含 Identity Manager 的 NCP 伺服器物件。Identity Manager 只能做爲伺服器的本地複製本。因此，如果次要伺服器未包含該伺服器物件，則角色與資源服務驅動程式可能無法正常啓動。

在 JBoss 上安裝使用者應用程式

5

本章說明如何在 JBoss 應用程式伺服器上使用安裝程式的圖形使用者介面版本來安裝 Roles Based Provisioning Module 適用的使用者應用程式。本章包含下列主題：

如果您希望使用指令行進行安裝，請參閱第 8 章「使用主控台或單一指令來安裝」(第 121 頁)。

以根使用者身分執行安裝程式。您需要以根使用者身分執行安裝程式。

資料移轉。如需移轉的相關資訊，請參閱 *《使用者應用程式：移轉指南》*(http://www.novell.com/documentation/idm40/index.html)。

5.1 安裝和設定使用者應用程式 WAR

附註：對於 JBoss 5.1.0，安裝程式需要使用 Sun 的 Java 2 Platform Standard Edition Development Kit 1.6 版 (JRE 或 JDK)。如果使用其他版本，安裝程序將無法成功設定使用者應用程式 WAR 檔案。安裝會顯示成功，但是當您嘗試啓動「使用者應用程式」時會發生錯誤。

1 從指令行啓動您平台適用的安裝程式：

請務必使用正確的 Sun JRE 版本 (如第 1.3 節「系統要求」(第 10 頁) 中所述) 來啓動使用者應用程式安裝程式。若之前使用 Roles Based Provisioning Module 提供的 JBossPostgreSQL 公用程式安裝了 JRE，現在便可以使用以下指令來啓動安裝程式：

Linux/Solaris。

```
$ /opt/novell/jre/bin/java -jar IdmUserApp.jar
```

Windows。

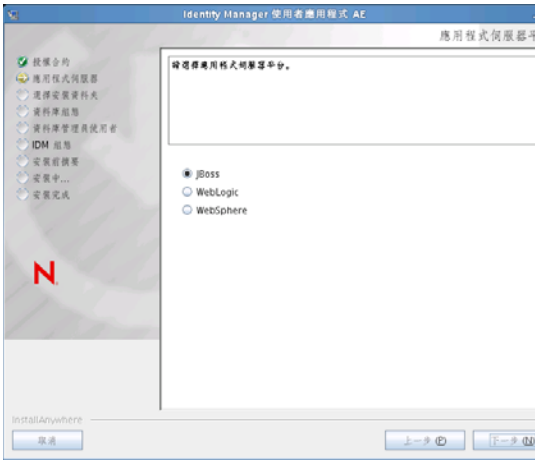
```
C:\Novell\InstallFiles\> "C:\Program Files\Java\jdk1.6.0_14\bin\java.exe"
-jar IdmUserApp.jar
```

附註：SLES 使用者：請勿使用 SLES 隨附的 IBM* JDK。此版本與該安裝有多處不相容，可能會導致萬能金鑰損毀的錯誤。

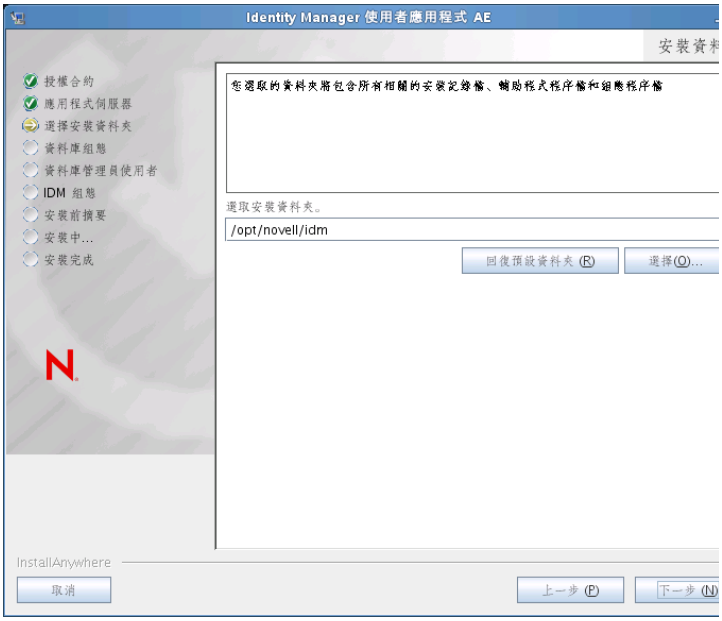
安裝程式啓動時會提示您選擇語言：

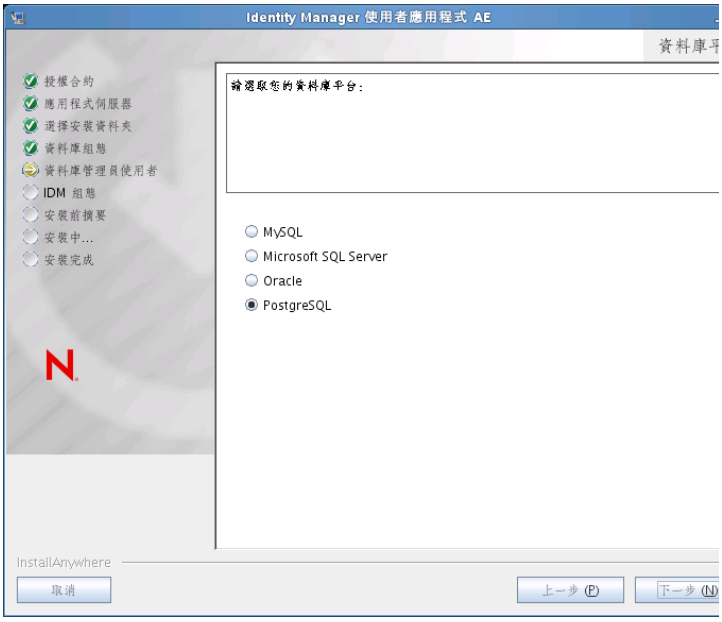
2 根據下列資訊選擇語言、確認授權合約並選取應用程式伺服器平台：

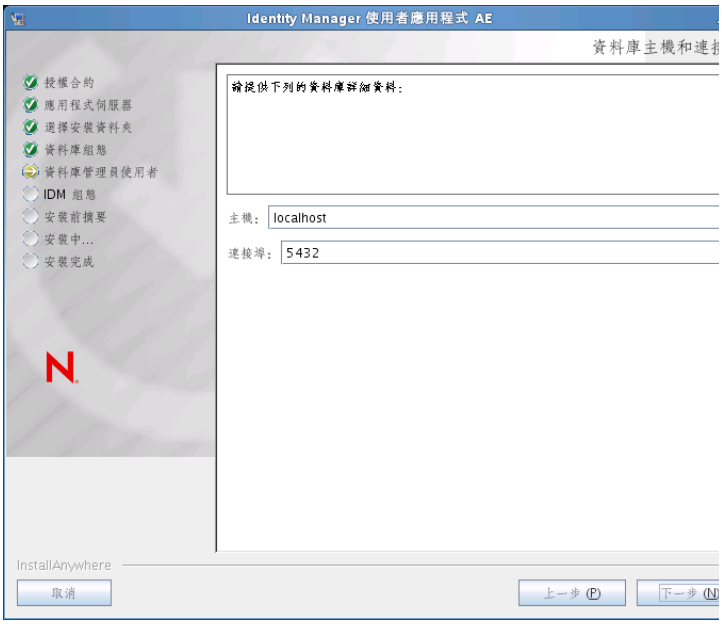
安裝畫面	描述
使用者應用程式安裝	選取安裝程式的語言。預設值爲英語。
授權合約	閱讀授權合約，然後選取「*我接受授權合約中的條款*」。

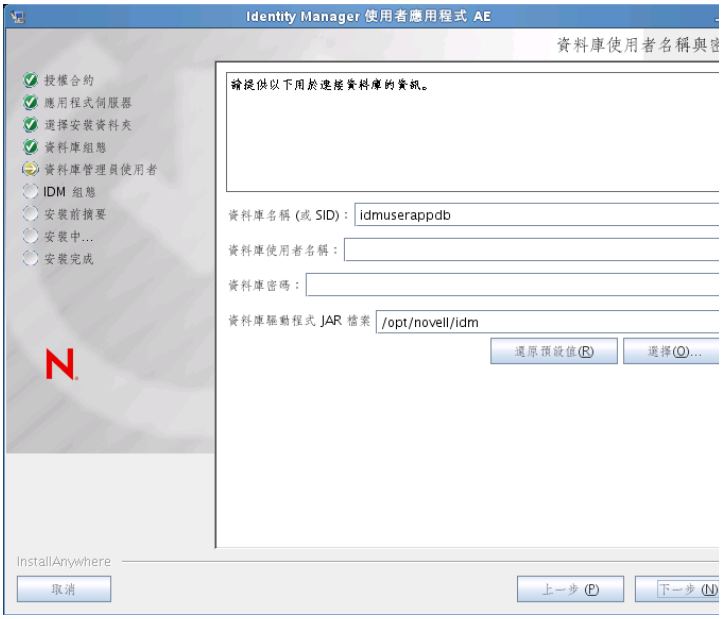
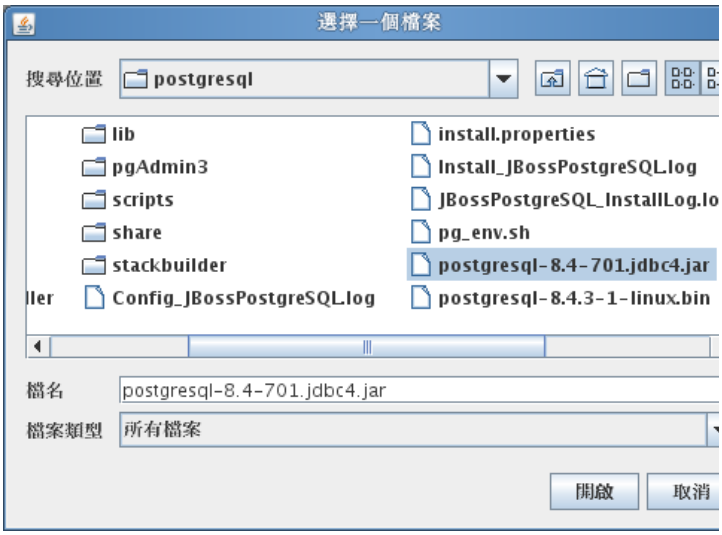
安裝畫面	描述
應用程式伺服器平台	選取 *JBoss*。  如果在 JBoss 上安裝，您需要使用 Sun 的 Java 環境啓動安裝程式。如果選取 JBoss 作爲您的應用程式伺服器，而且不使用 Sun 的 Java 來啓動安裝，則系統會顯示快顯錯誤訊息，並終止安裝： 

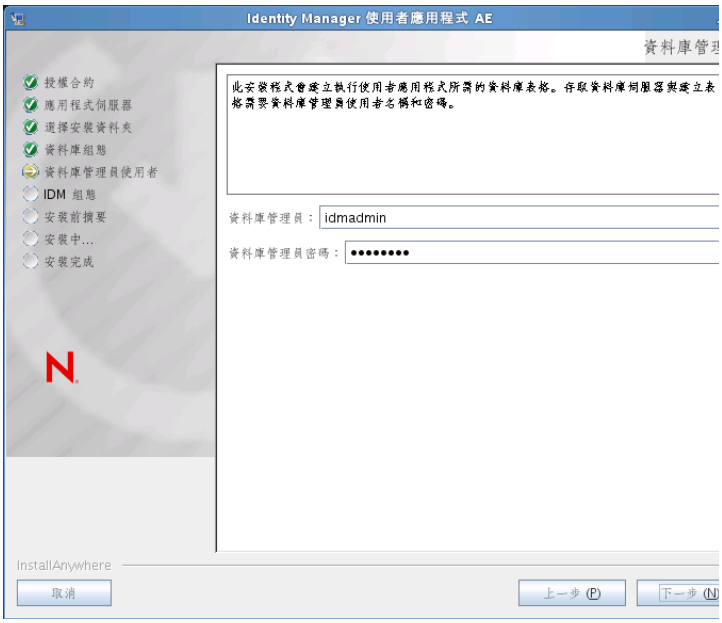
3 根據下列資訊選擇安裝資料夾並設定資料庫：

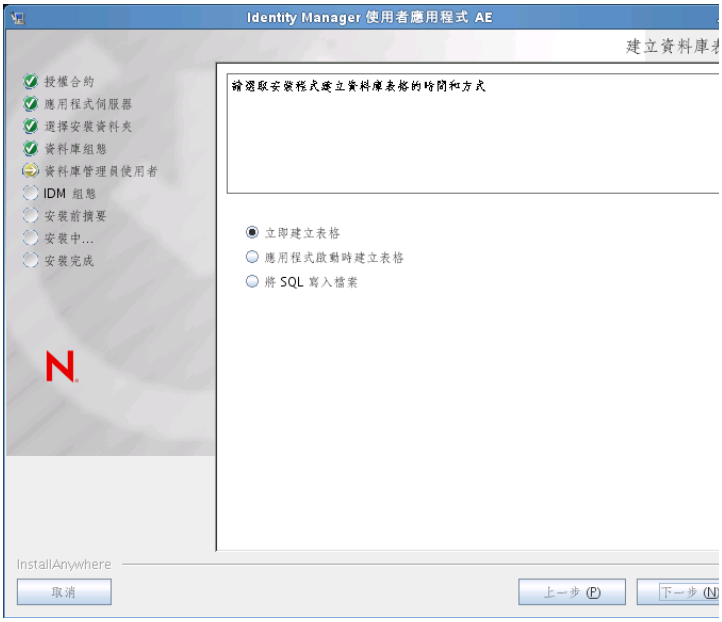
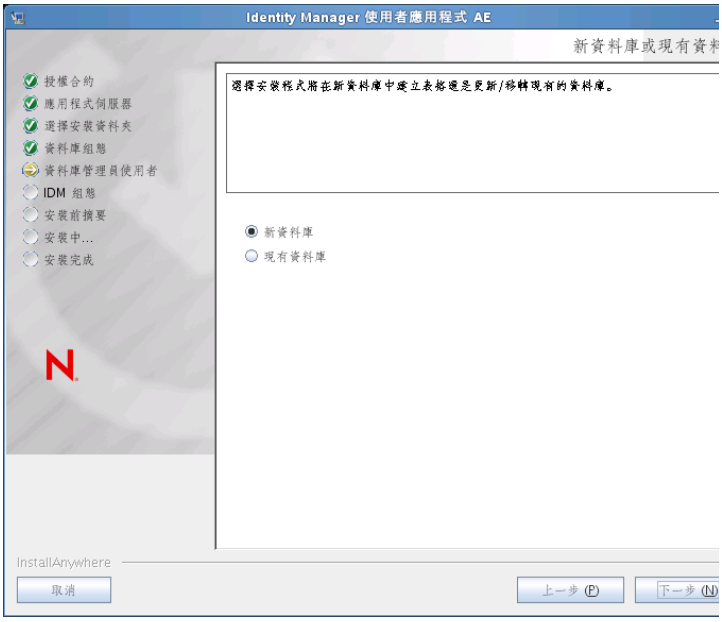
安裝畫面	描述
選擇安裝資料夾	指定安裝程式應該將檔案放在何處。 

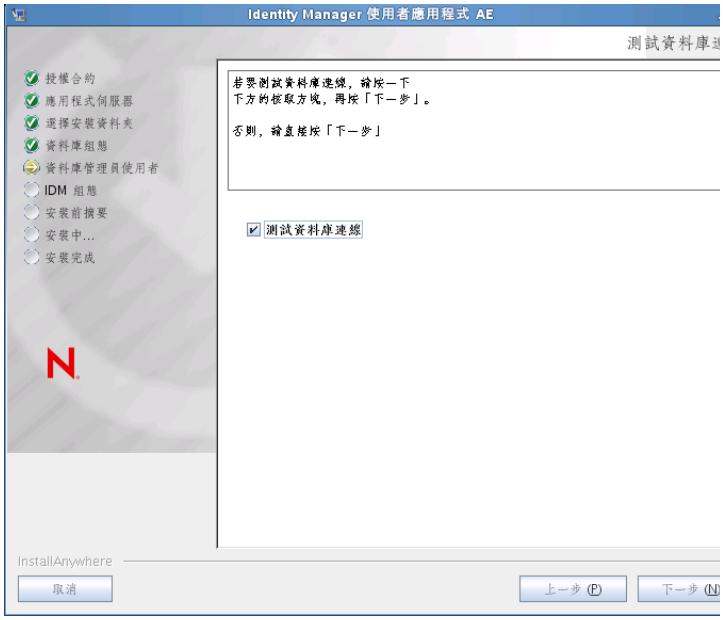
安裝畫面	描述
資料庫平台	選取資料庫平台：  資料庫與 JDBC 驅動程式必須已經安裝。對於 JBoss，選項包含下列各項： ◆ MySQL ◆ Microsoft SQL Server ◆ Oracle ◆ PostgreSQL

安裝畫面	描述
資料庫主機和連接埠	*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。 

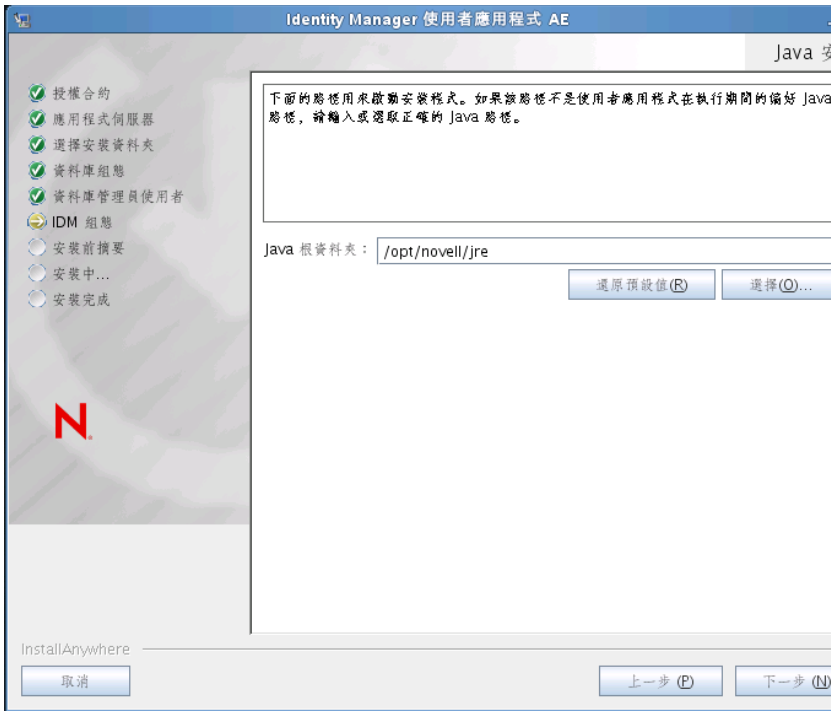
安裝畫面	描述
資料庫使用者名稱與密碼	*資料庫名稱* (或 SID)：對於 PostgreSQL、MySQL 或 MS SQL Server，請提供資料庫的名稱。對於 Oracle，請提供您先前建立的 Oracle 系統識別碼 (SID)。對於叢集，請爲叢集的每一個成員指定相同的資料庫名稱或 SID。預設資料庫名稱爲 idmuserappdb。 *資料庫使用者*名稱：指定資料庫使用者。若是叢集，請爲叢集的每一個成員指定相同的資料庫使用者。 *資料庫密碼*：指定資料庫密碼。若是叢集，請爲叢集的每一個成員指定相同的資料庫密碼。 *資料庫驅動程式 JAR 檔案*：爲資料庫伺服器提供簡易用戶端 JAR。此爲必填欄位。  對於 PostgreSQL，請選擇 postgresql-8.4-701.jdbc4.jar 檔案： 

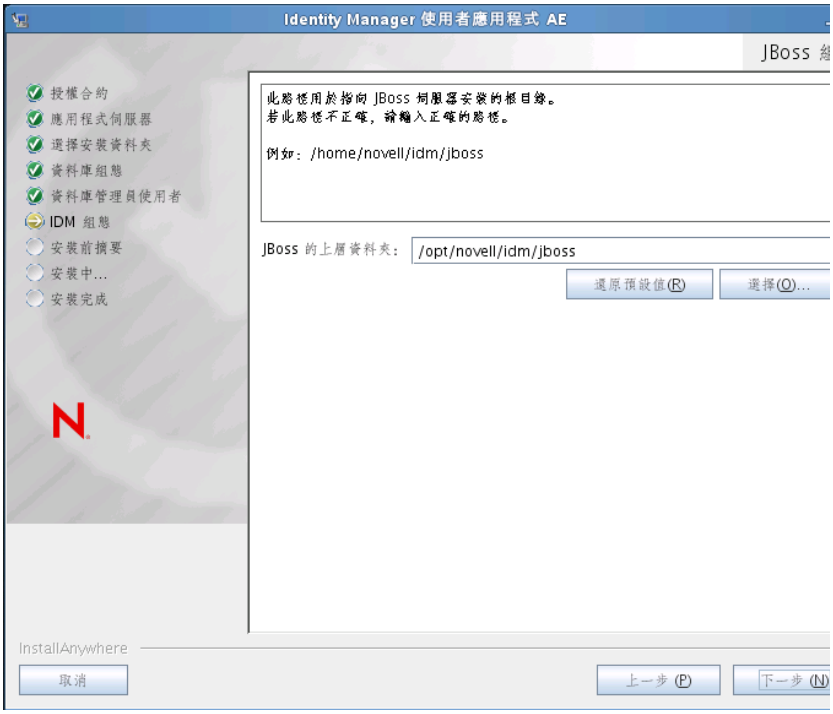
安裝畫面	描述
資料庫管理員	此螢幕已預先填入「資料庫使用者名稱與密碼」頁面上顯示的使用者名稱與密碼。如果之前指定的資料庫使用者不具備足夠許可，因而無法在資料庫伺服器中建立表格，則需要輸入具備必要權限的其他使用者 ID。 

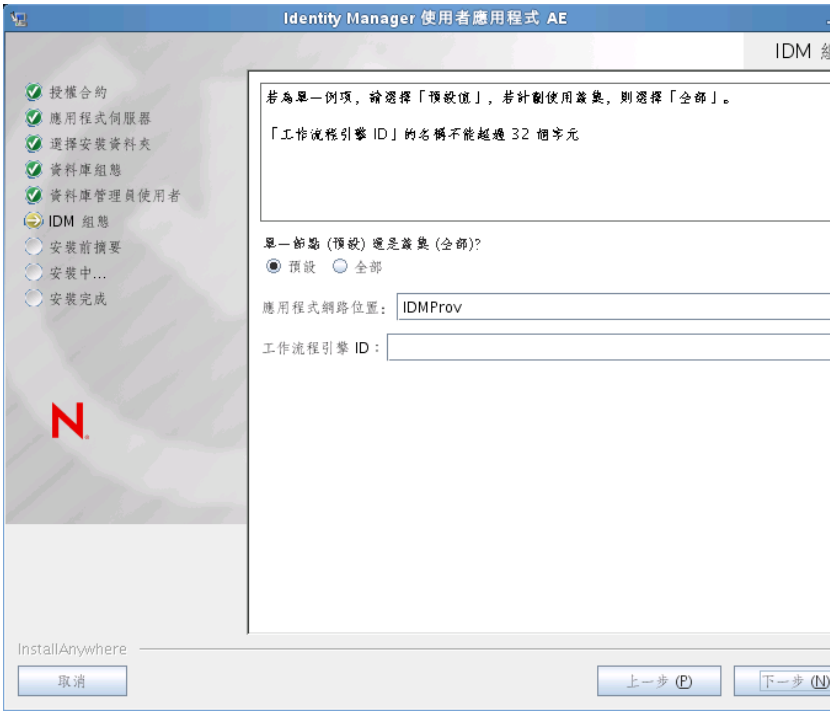
安裝畫面	描述
建立資料庫表格	指定應在何時建立資料庫表格：  「建立資料庫表格」螢幕可讓您選擇是要在安裝時還是在應用程式啓動時建立表格。此外，您也可以在安裝時建立綱要檔案，資料庫管理員以後會使用該檔案來建立表格。 如果您要產生綱要檔案，請選取「*將 SQL 寫入檔案*」核取方塊，並在「*綱要輸出檔案*」欄位中提供檔案名稱。
新資料庫或現有資料庫	如果要使用的是新資料庫或空資料庫，請選取「*新資料庫*」按鈕。如果要使用先前的安裝留下的現有資料庫，請選取「*現有資料庫*」按鈕。 

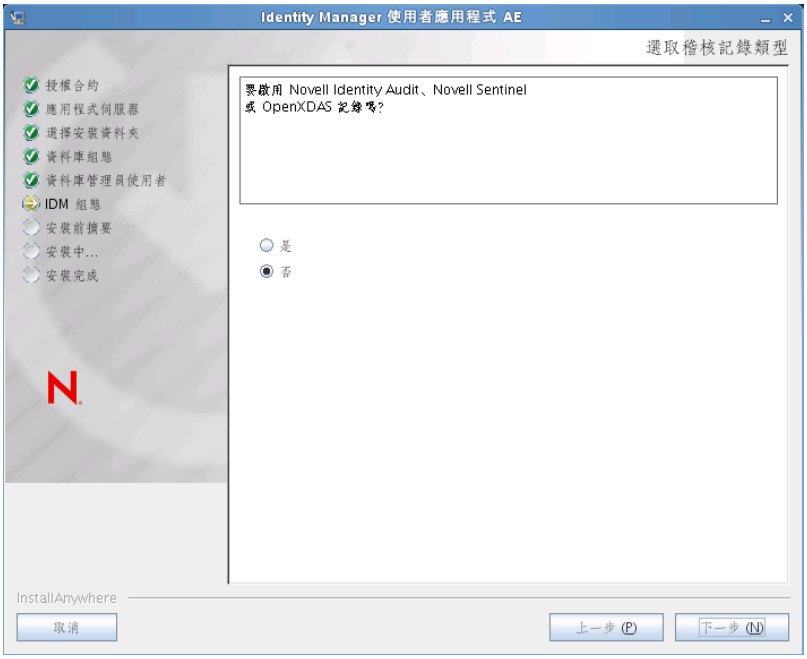
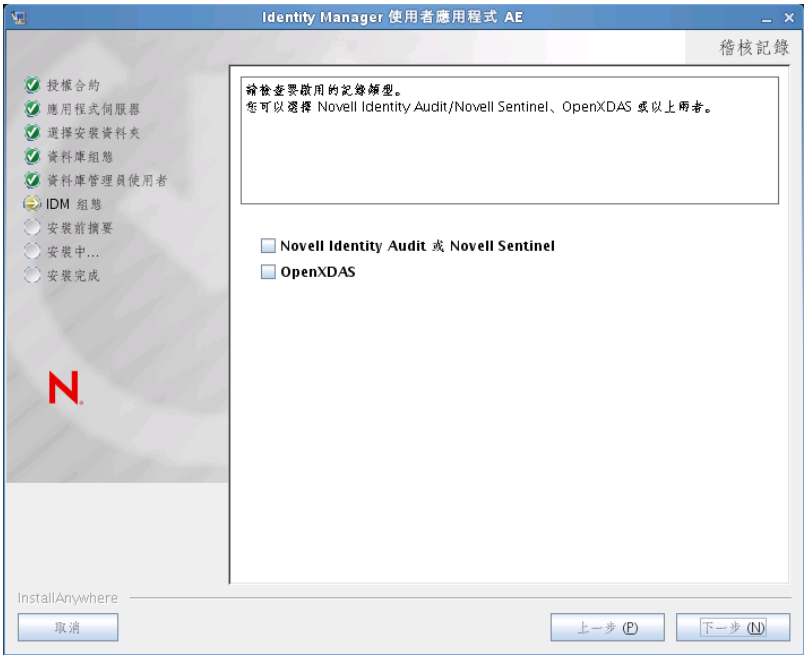
安裝畫面	描述
測試資料庫連接	若要確認之前螢幕中提供的資訊是否正確，可以選取「*測試資料庫連接*」核取方塊來測試資料庫連接：  安裝程式在直接建立表格以及建立 .SQL 檔案時都需要連接至資料庫。若測試資料庫連接而連接失敗，您還是可以繼續安裝。此種情況下，您將需要在安裝之後建立表格，如 *《User Application: Administration Guide》(使用者應用程式：管理指南)* (http://www.novell.com/documentation/idmrbpm40/agpro/?page=/documentation/idmrbpm40/agpro/data/bncf7rj.html) 中所述。

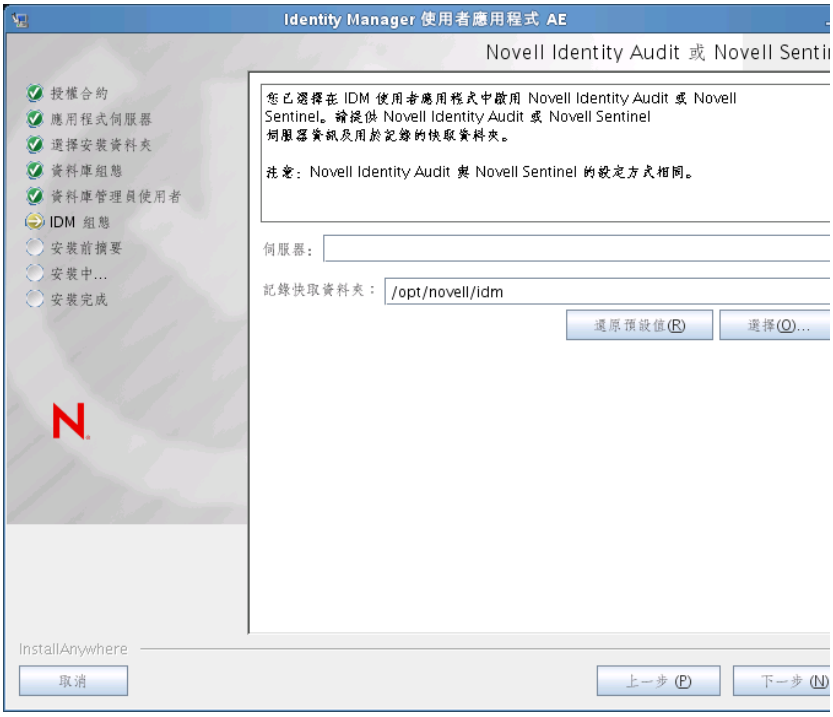
4 根據下列資訊設定 Java、JBoss 安裝、Identity Manager 以及稽核設定與安全性。

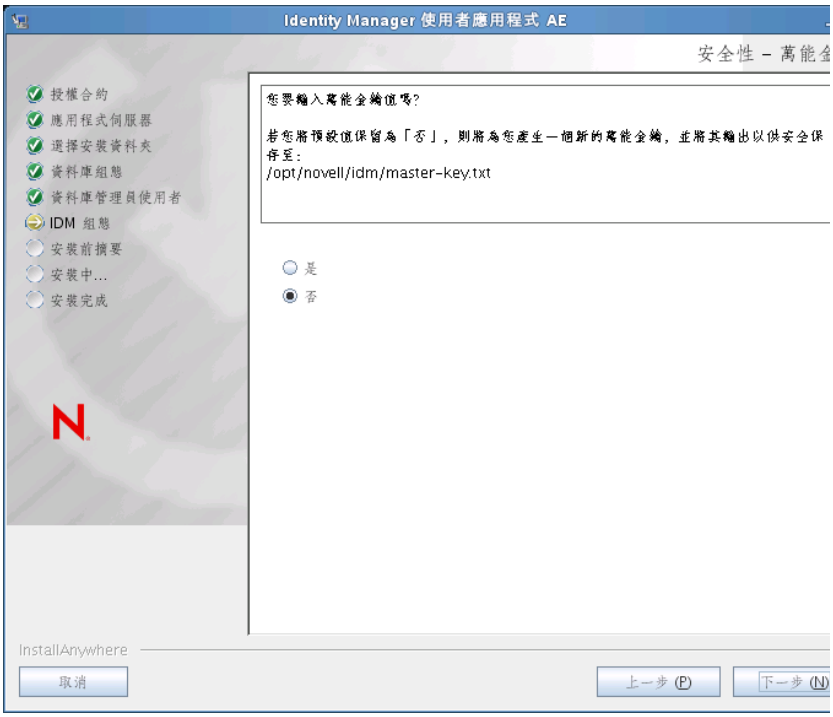
安裝畫面	描述
Java 安裝	指定 Java 安裝根資料夾。Java 安裝透過 JAVA_HOME 環境變數來提供 Java 路徑，並提供修正路徑的選項：  此時，安裝程式還會驗證選取的 Java 是否適用於所選的應用程式伺服器。另外，也會驗證其是否可以寫入指定 JRE 中的 cacerts。 然後，系統會提示您輸入 JBoss Application Server 的安裝位置。

安裝畫面	描述
JBoss 組態	告知「使用者應用程式」到何處尋找「JBoss 應用程式伺服器」。 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」的說明，請參閱「安裝 JBoss Application Server 和 PostgreSQL 資料庫」(第 17 頁)。 *JBoss 的上層資料夾*：指定 JBoss Application Server 的位置。 

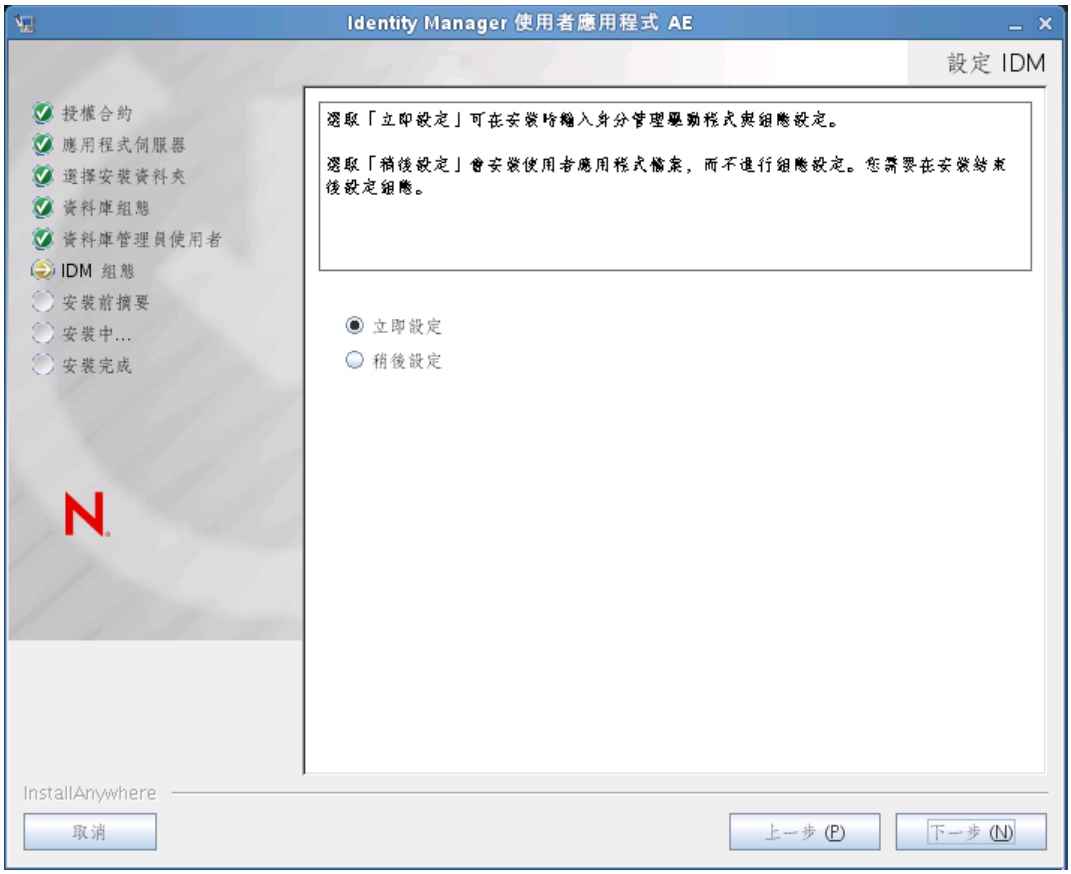
安裝畫面	描述
IDM 組態	選取應用程式伺服器組態的類型： ◆ 如果進行此安裝的節點不屬於叢集，請選取「*預設*」。 如果您選取「*預設值*」，後來又決定需要叢集，那就必須重新安裝「使用者應用程式」。 ◆ 如果安裝爲叢集的一部分，請選取「*全部*」 *應用程式網路位置*：應用程式伺服器組態的名稱、應用程式 WAR 檔案的名稱，以及 URL 網路位置的名稱。安裝程序檔會建立一個伺服器組態，並會依預設根據「*應用程式名稱*」來命名組態。請將應用程式名稱記錄下來，當您從瀏覽器啓動「使用者應用程式」時，請在 URL 中輸入這個名稱。 *工作流程引擎 ID*：叢集的每一個伺服器必須有唯一的「工作流程引擎 ID」。工作流程引擎 ID 只對叢集安裝有效，並且僅適用於您要安裝佈建 WAR 的情況。引擎 ID 名稱不能超過 32 個字元。*《使用者應用程式：管理指南》*的「設定叢集的工作流程」一節中，有對工作流程引擎 ID 的相關說明。 

安裝畫面	描述
選取稽核記錄類型	若要啓用記錄，請按一下「*是*」。若要停用記錄，請按一下「*否*」。  下一個面板會提示您指定記錄類型。請從下列選項中選擇： ◆ *Novell Identity Audit 或 Novell Sentinel*：啓用透過 Novell 用戶端對使用者應用程式的記錄。 ◆ *OpenXDAS*：將事件記錄至您的 OpenXDAS 記錄伺服器。 如需設定記錄的詳細資訊，請參閱 *《使用者應用程式：管理指南》*。 

安裝畫面	描述
Novell Identity Audit 或 Novell Sentinel	*伺服器*：如果啓用記錄，請指定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。 

安裝畫面	描述
安全性 - 萬能金鑰	*是*：可讓您「匯入」現有的萬能金鑰。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。 *否*：建立新的萬能金鑰。完成安裝之後，您必須手動記錄第 9.1 節「記錄萬能金鑰」(第 133 頁) 中所述的萬能金鑰。  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。 匯入現有的萬能金鑰有下列理由： ◆ 您想將安裝從臨時系統移到生產系統，並想保留臨時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。

5 若現在要設定 RBPM，請選取「*立即設定*」，然後按「*下一步*」。



(如果沒有顯示這些資訊，可能是您未完成第 2.5 節「安裝 Java 開發套件」(第 27 頁)中所述的步驟。)

「Roles Based Provisioning Module 組態」面板的預設檢視窗會顯示下列欄位：

安裝程式會採用「根容器 DN」中的值，並將其套用至下列值：

- 使用者容器 DN
- 群組容器 DN

安裝程式會採用「使用者應用程式管理員」欄位中的值，並將其套用至下列值：

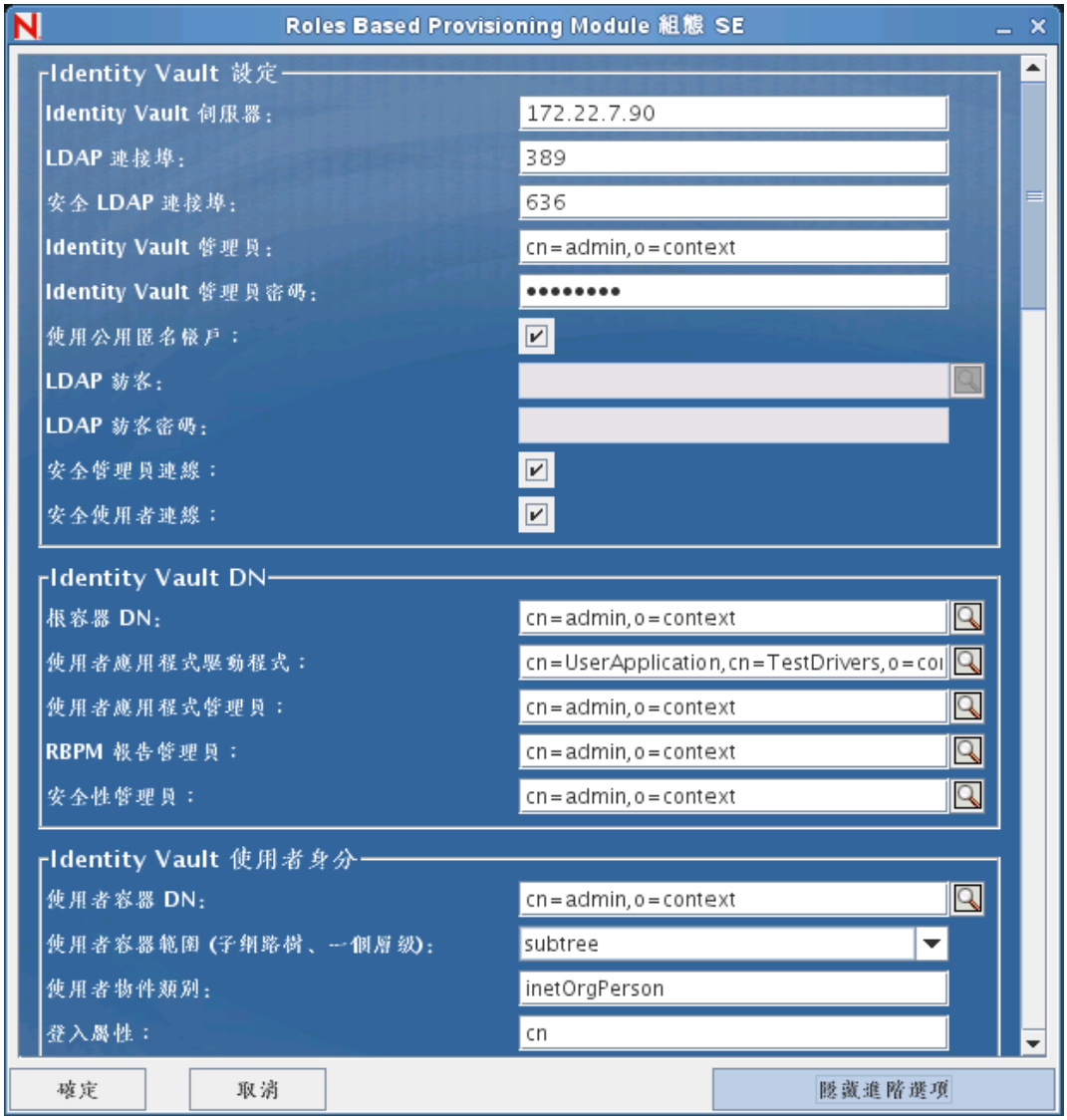
- 佈建管理員
- 法規遵循管理員
- 角色管理員
- 安全性管理員
- 資源管理員
- RBPM 組態管理員

如果希望能夠明確指定這些值，可以按一下「*顯示進階選項*」按鈕並進行變更。

「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。

如需每一個選項的說明，請參閱附錄 A「使用者應用程式組態參考」(第 141 頁)。

Standard Edition 的預設檢視窗會顯示部分安全性欄位，如下所示：



在 Identity Manager 4.0.1 Standard Edition 中，只需要指定以下管理員：

- 使用者應用程式管理員
- RBPM 報告管理員
- 安全性管理員

附註：出於測試目的，Novell 不會在 Standard Edition 中鎖定安全性模型。因此，安全性管理員可以指定所有網域管理員、委託管理員及其他安全性管理員。不過，線上環境中不支援使用這些進階功能。在線上環境中，所有管理員指定均受授權限制。Novell 會在稽核資料庫中收集監控資料，以確保線上環境遵循法規。此外，Novell 還建議只對一位使用者授予安全性管理員許可權。

6 根據以下資訊完成此安裝。

安裝畫面	描述
安裝前摘要	閱讀「安裝前摘要」頁面，確認您選擇的安裝參數。 *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。對安裝和組態參數感到滿意之後，請返回「安裝前摘要」頁面並按一下「*安裝*」。
安裝完成	表示已完成安裝。

安裝程式會建立 novlua 使用者。安裝程式會建立名爲 novlua 的新使用者。jboss_init 程序檔會以此使用者身分執行 JBoss，並且會將 JBoss 檔案中定義的許可權設定給此使用者。

5.1.1 檢視安裝和記錄檔案

如果安裝完成並且未發生任何錯誤，請繼續測試安裝。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。

5.2 測試安裝

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)：

/etc/init.d/jboss_init start (Linux 與 Solaris)

start-jboss.bat (Windows)

如果您執行的不是 X11 Window System，則需要在伺服器啓動程序檔中包含 -Djava.awt.headless=true 旗標。這是執行報告所必需的。例如，可在程序檔中包含以下行：

JAVA_OPTS="-Djava.awt.headless=true -Dfile.encoding=UTF-8 -Dsun.jnu.encoding=UTF-8 -server -Xms1024m -Xmx1024m -XX:MaxPermSize=512m

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 依照使用者應用程式驅動程式上方顯示的步驟啓動角色與資源服務驅動程式。

5 若要啓動並登入使用者應用程式，請使用您的網頁瀏覽器存取以下 URL ：

http:// *主機名稱* : *連接埠* / *應用程式名稱*

在此 URL 中，*主機名稱* : *連接埠*是應用程式伺服器的主機名稱 (例如，myserver.domain.com)，連接埠是應用程式伺服器的連接埠 (例如，JBoss 上預設爲 8180)。*應用程式名稱*預設爲 *IDMProv*。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。

出現「Novell Identity Manager 使用者應用程式」抵達頁面。

6 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 9.9 節 「疑難排解」 (第 137 頁)。

在 WebSphere 上安裝使用者應用程式

6

本章說明如何使用圖形使用者介面版本的安裝程式在 WebSphere 應用程式伺服器上安裝 Roles Based Provisioning Module 適用的使用者應用程式。

- 第 6.1 節「安裝和設定使用者應用程式 WAR」(第 75 頁)
- 第 6.2 節「設定 WebSphere 環境」(第 87 頁)
- 第 6.3 節「部署 WAR 檔案」(第 101 頁)
- 第 6.4 節「啓動和存取使用者應用程式」(第 101 頁)

以非根使用者的身分執行安裝程式。

資料移轉。如需移轉的相關資訊，請參閱 *《使用者應用程式：移轉指南》*(http://www.novell.com/documentation/idm40/index.html)。

6.1 安裝和設定使用者應用程式 WAR

附註：若是 WebSphere 7.0，安裝程序需要 IBM 的 1.6 版 JDK。如果使用其他版本，安裝程序將無法成功設定使用者應用程式 WAR 檔案。安裝會顯示成功，但是當您嘗試啓動「使用者應用程式」時會發生錯誤。

1. 瀏覽至含有安裝檔案的目錄。
2. 必須將無限制的規則檔案套用至 IBM JDK。您可以參閱 WebSphere 文件，獲取 IBM 提供的這些檔案的連結以及套用檔案的相關指示。請在進行安裝前先將這些檔案套用至 IBM JDK 環境。無限制規則檔案的 JAR 檔案必須放置於 JAVA_HOME\jre\lib\security 下。

   如果不使用這些無限制規則檔案，則會出現「金鑰大小不正確」的錯誤。出現此問題的根本原因是缺少無限制規則檔案，因此請務必使用正確的 IBM JDK。
3. 使用 IBM Java 環境啓動安裝程式，如下所示：

   Linux 或 Solaris。

   ```
   $ /opt/WS/IBM/WebSphere/AppServer/java/bin/java -jar IdmUserApp.jar
   ```

   Windows。

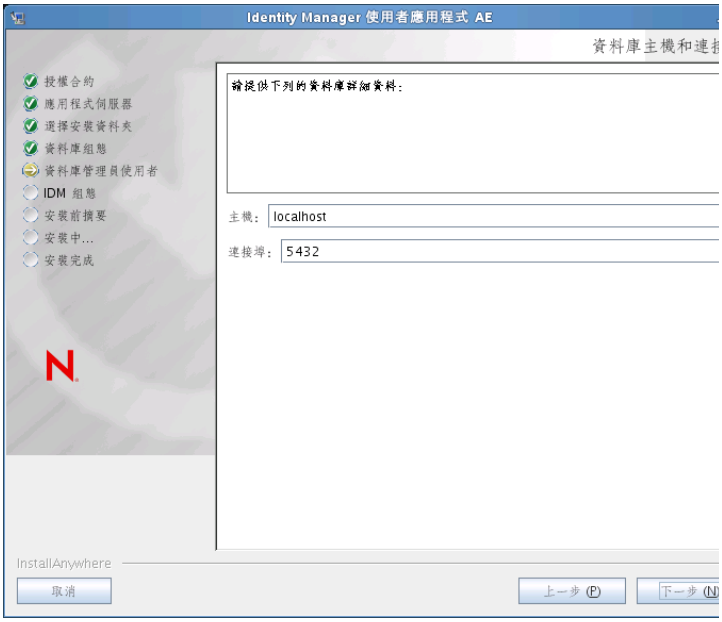
   ```
   C:\WS\IBM\WebSphere\AppServer\java\bin\java -jar IdmUserApp.jar
   ```

   安裝程式啓動時會提示您選擇語言：

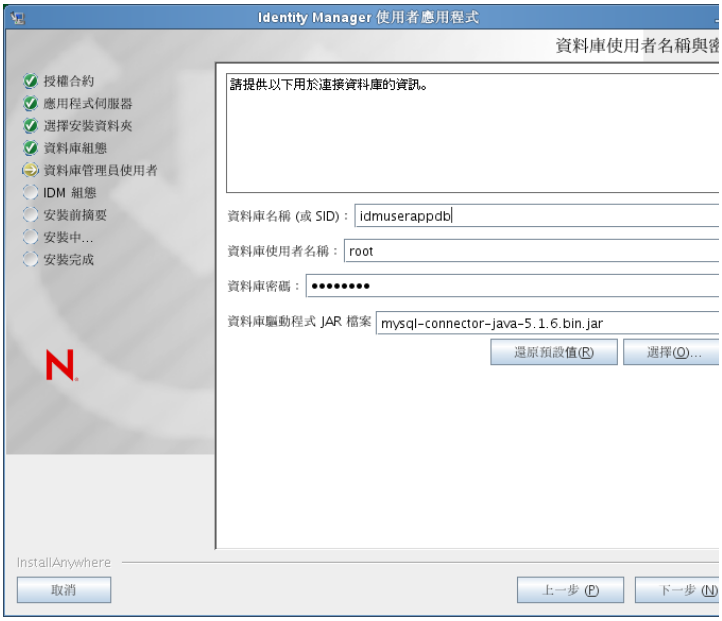
4 根據下列資訊選取語言、確認授權合約並選取應用程式伺服器平台：

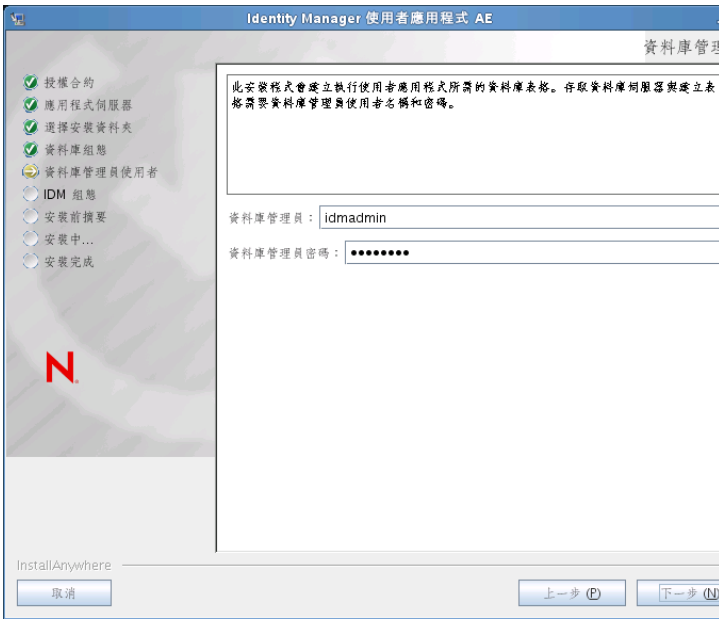
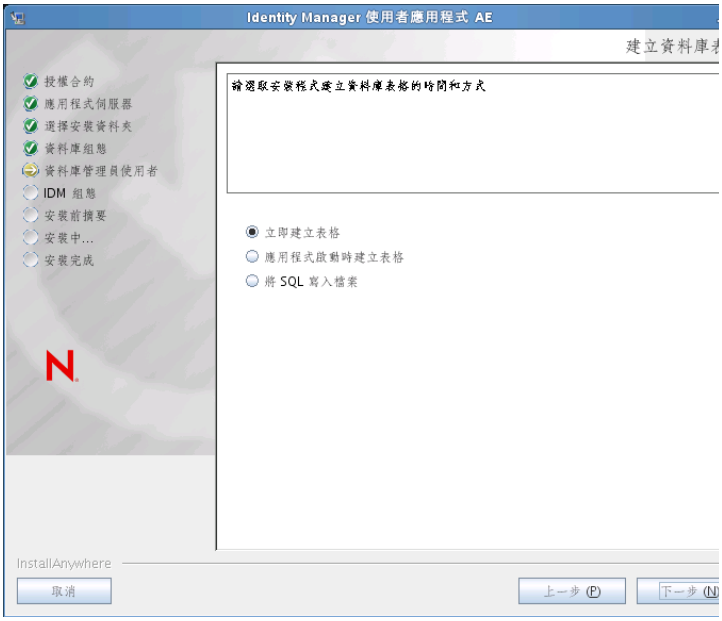
安裝畫面	描述
使用者應用程式安裝	選取安裝程式的語言。預設值爲英文。
授權合約	閱讀授權合約，然後選取「*我接受授權合約中的條款*」。
應用程式伺服器平台	選取 *WebSphere*。 如果「 使用者應用程式」的 WAR 檔案所在的目錄與安裝程式的不同，安裝程式就會提示您輸入 WAR 的路徑。 如果 WAR 儲存於預設位置，請按一下「*還原預設資料夾*」。若要指定 WAR 檔案的位置，按一下「*選擇*」並選取位置。 如果在 WebSphere 上安裝，您需要使用 IBM 的 Java 環境啓動安裝程式。如果選取 WebSphere 作爲您的應用程式伺服器，而不使用 IBM 的 Java 來啓動安裝，則系統會顯示快顯錯誤訊息，並終止安裝： 

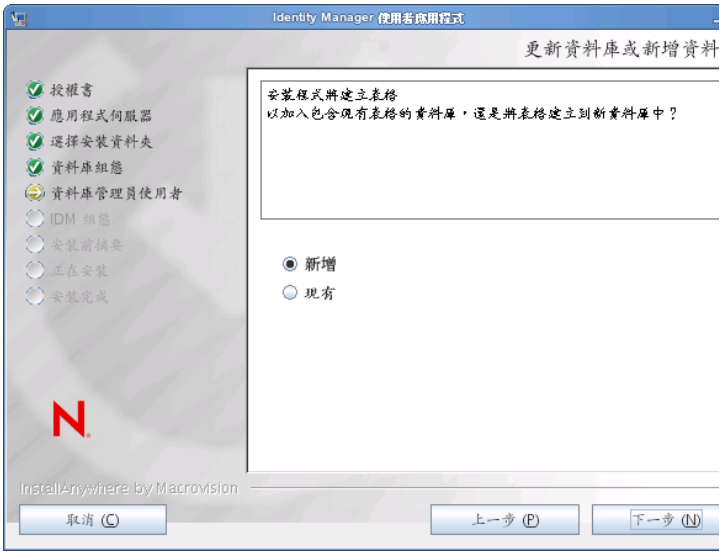
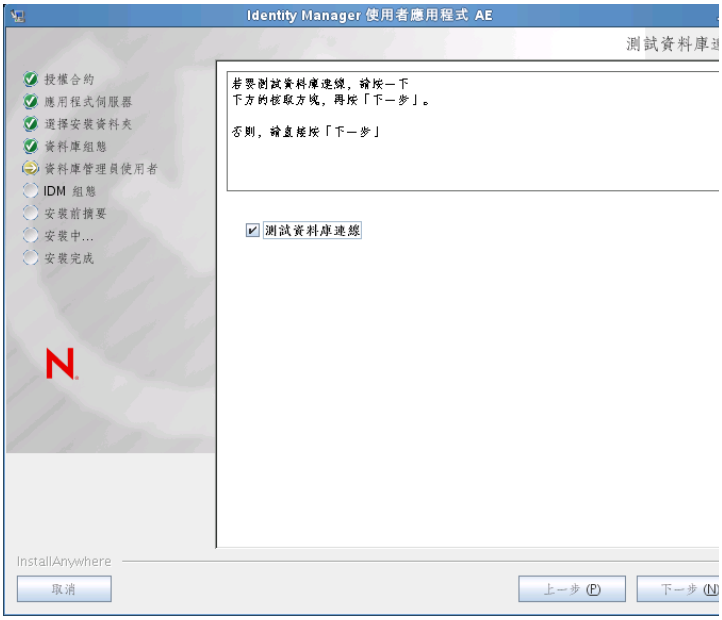
5 根據下列資訊選擇安裝資料夾並設定資料庫：

安裝畫面	描述
選擇安裝資料夾	指定安裝程式應該將檔案放在何處。
資料庫平台	選取資料庫平台。必須已安裝資料庫和 JDBC 驅動程式。對於 WebSphere，選項包含下列各項： ◆ Oracle ◆ Microsoft SQL Server ◆ IBM DB2 ◆ PostgreSQL
資料庫主機和連接埠	*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。 

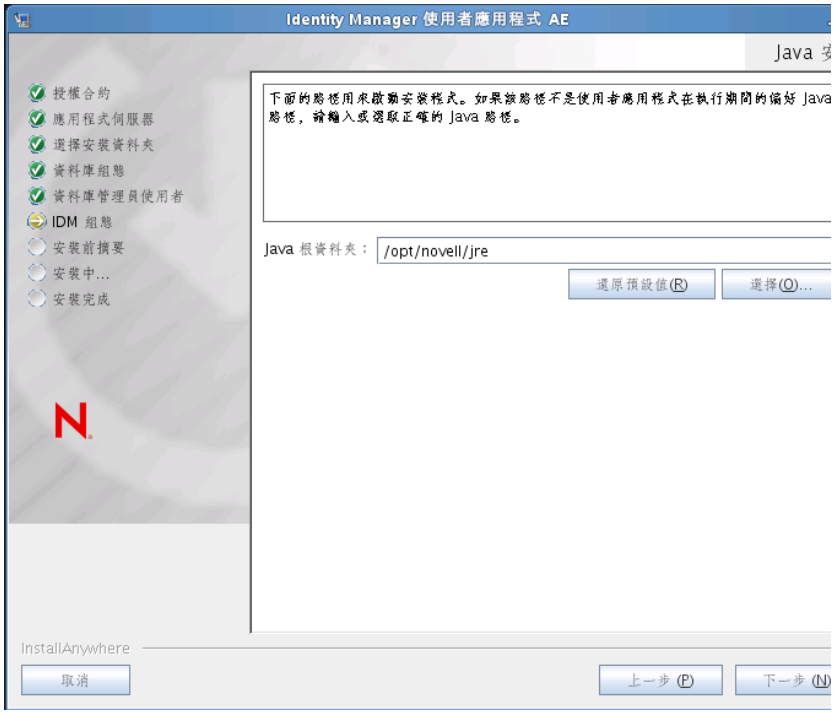
安裝畫面	描述

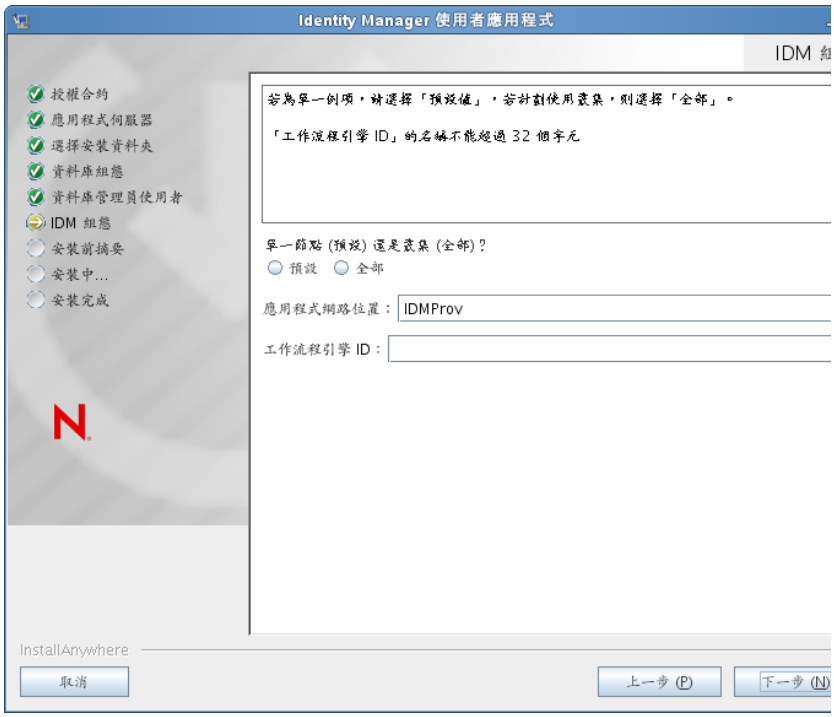
資料庫使用者名稱與密碼	*資料庫名稱* (或 SID)：對於 DB2、MS SQL Server 或 PostgreSQL，請提供您預先設定的資料庫名稱。對於 Oracle，請提供您之前建立的 Oracle 系統識別碼 (SID)。對於叢集，請爲叢集的每一個成員指定相同的資料庫名稱和 SID。
	
	*資料庫使用者*名稱：指定資料庫使用者。若是叢集，請爲叢集的每一個成員指定相同的資料庫使用者。
	
	資料庫密碼：指定資料庫密碼。若是叢集，請爲叢集的每一個成員指定相同的資料庫密碼。
	
	資料庫驅動程式 JAR 檔案：爲資料庫伺服器提供簡易用戶端 JAR。此爲必填欄位。
	
	重要：使用「*資料庫驅動程式 JAR 檔案*」欄位的瀏覽按鈕只能選取一 (1) 個 jar。但對於 DB2，必須提供兩 (2) 個 jar：
	◆ db2jcc.jar
	◆ db2jcc_license_cu.jar
	
	因此，您可以選取一個 JAR，但第二個 JAR 必須手動輸入，並使用執行安裝程式之作業系統所適用的正確檔案分隔符。您也可以手動輸入兩個項目。
	
	例如，在 Windows 上：
	
	`c:\db2jars\db2jcc.jar;c:\db2jars\db2jcc_license_cu.jar`
	
	例如，在 Solaris 和 Linux 上：
	
	`/home/lab/db2jars/db2jcc.jar:/home/lab/db2jcc_license_cu.jar`
	
	 

安裝畫面	描述
資料庫管理員	此螢幕已預先填入「資料庫使用者名稱與密碼」頁面上顯示的使用者名稱與密碼。如果之前指定的資料庫使用者不具備足夠許可，因而無法在資料庫伺服器中建立表格，則需要輸入具備必要權限的其他使用者 ID。 
建立資料庫表格	指定應在何時建立資料庫表格： 

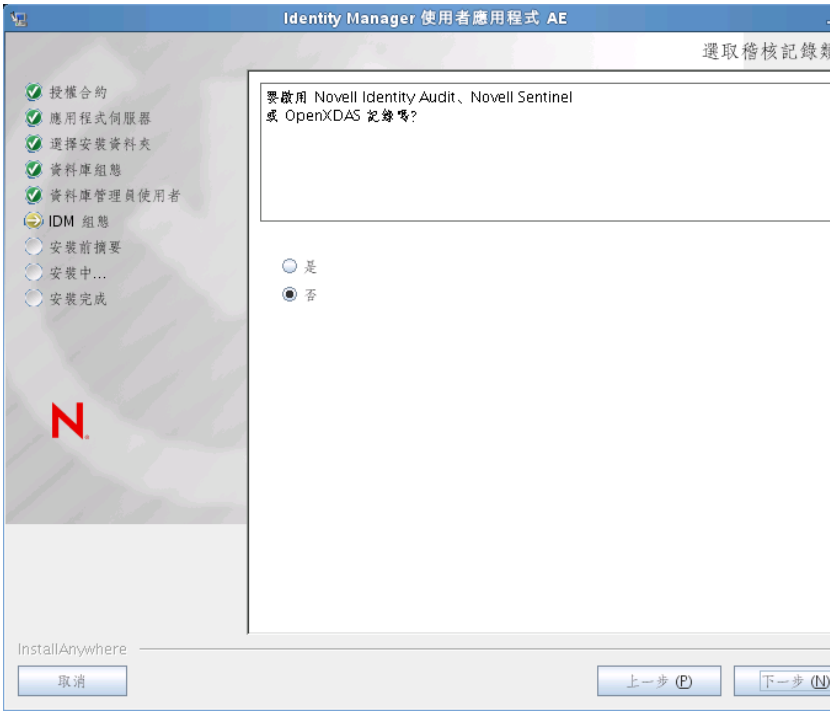
安裝畫面	描述
新資料庫或現有資料庫	如果要使用的是新資料庫或空資料庫，請選取「*新資料庫*」按鈕。如果要使用先前的安裝留下的現有資料庫，請選取「*現有資料庫*」按鈕。 
測試資料庫連接	若要確認之前螢幕中提供的資訊是否正確，可以選取「*測試資料庫連接*」核取方塊來測試資料庫連接：  安裝程式在直接建立表格以及建立 .SQL 檔案時都需要連接至資料庫。若測試資料庫連接而連接失敗，您還是可以繼續安裝。此種情況下，您將需要在安裝之後建立表格，如 *《User Application: Administration Guide》(使用者應用程式：管理指南)* (http://www.novell.com/documentation/idm40/agpro/?page=/documentation/idm40/agpro/data/bncf7rj.html) 中所述。

6 根據下列資訊設定 Java、Identity Manager 以及稽核設定與安全性。

安裝畫面	描述
Java 安裝	指定 Java 安裝根資料夾。Java 安裝透過 JAVA_HOME 環境變數來提供 Java 路徑，並提供修正路徑的選項：  此時，安裝程式還會驗證選取的 Java 是否適用於所選的應用程式伺服器。另外，也會驗證其是否可以寫入指定 JRE 中的 cacerts。

安裝畫面	描述
IDM 組態	*應用程式網路位置*：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「使用者應用程式」時，請在 URL 中輸入這個名稱。 

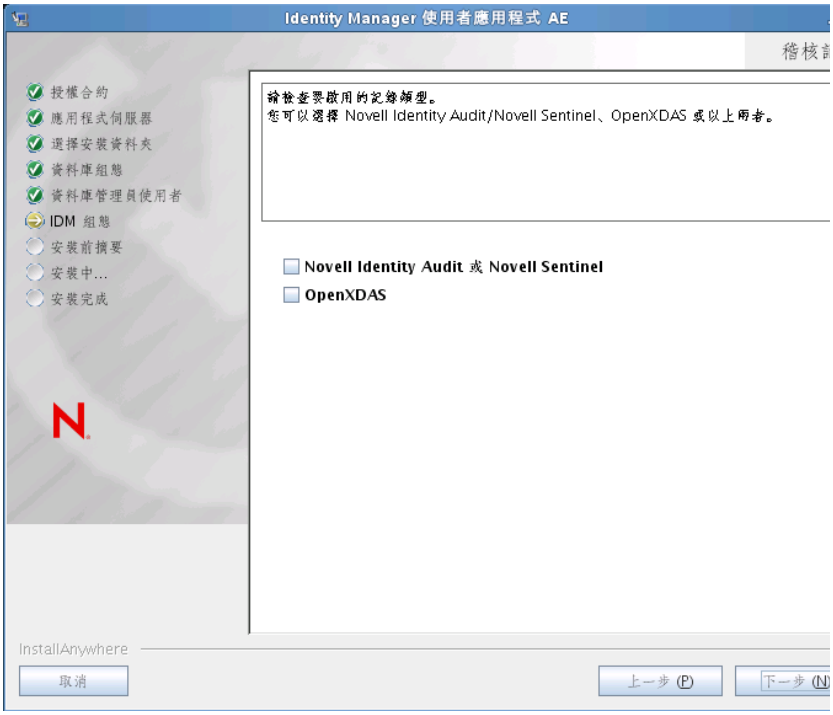
安裝畫面	描述
選取稽核記錄類型	若要啓用記錄，請按一下「*是*」。若要停用記錄，請按一下「*否*」。



下一個面板會提示您指定記錄類型。請從下列選項中選擇：

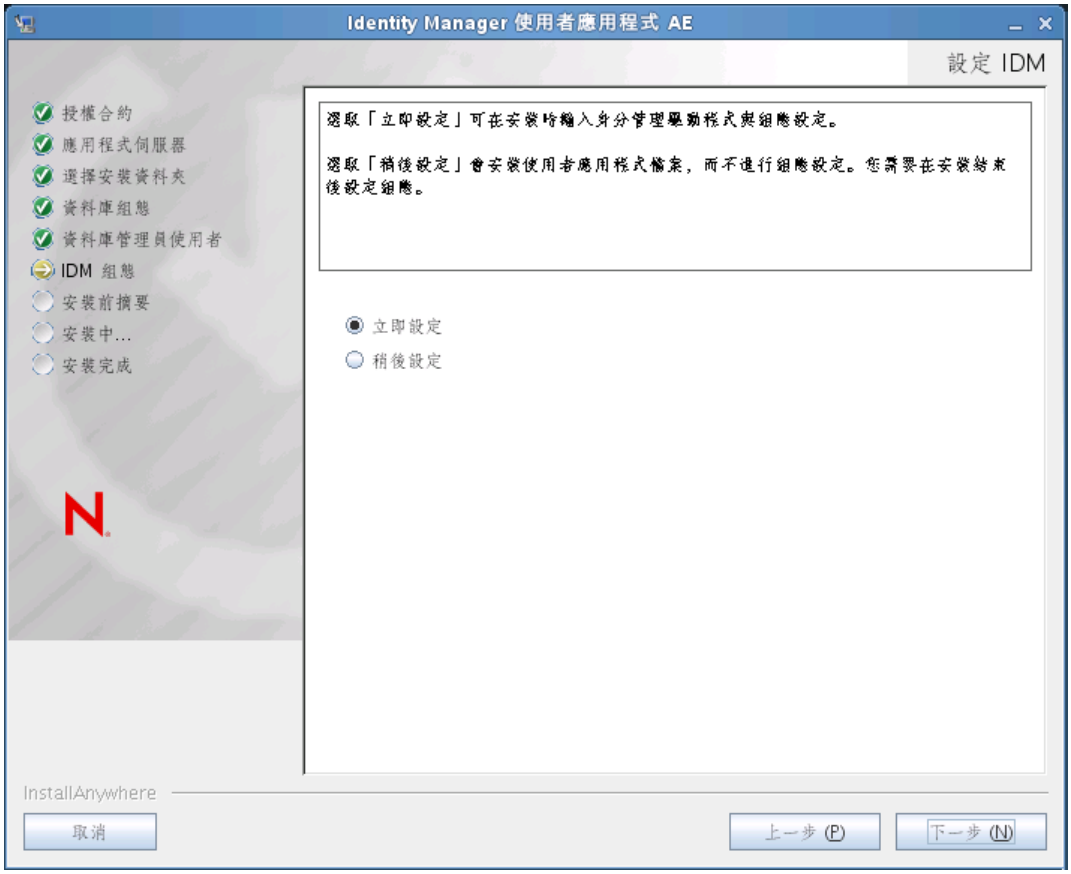
- *Novell Identity Audit 或 Novell Sentinel*：對使用者應用程式啓用透過 Novell 用戶端記錄的功能。
- *OpenXDAS*：將事件記錄至您的 OpenXDAS 記錄伺服器。

如需設定記錄的詳細資訊，請參閱 *《使用者應用程式：管理指南》*。



安裝畫面	描述
Novell Identity Audit 或 Novell Sentinel	*伺服器*：如果啓用記錄，請指定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。
安全性 - 萬能金鑰	*是*：可讓您「匯入」現有的萬能金鑰。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。 *否*：建立新的萬能金鑰。完成安裝之後，您必須手動記錄第 9.1 節「記錄萬能金鑰」(第 133 頁) 中所述的萬能金鑰。 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。 匯入現有的萬能金鑰有下列理由： ◆ 您想將安裝從臨時系統移到生產系統，並想保留臨時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。

7 若現在要設定 RBPM，請選取「*立即設定*」，然後按「*下一步*」。



(如果沒有顯示這些資訊，可能是您未完成第 2.5 節 「安裝 Java 開發套件」 (第 27 頁) 中所述的步驟。)

「Roles Based Provisioning Module 組態」面板的預設檢視窗會顯示下列六個欄位：

安裝程式會採用 「根容器 DN」中的值，並將其套用至下列值：

- 使用者容器 DN
- 群組容器 DN

安裝程式會採用 「使用者應用程式管理員」欄位中的值，並將其套用至下列值：

- 佈建管理員
- 法規遵循管理員
- 角色管理員
- 安全性管理員
- 資源管理員
- RBPM 組態管理員

如果要明確指定這些值，可以按一下 「*顯示進階選項*」按鈕並進行變更。

「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。

如需每一個選項的說明，請參閱附錄 A 「使用者應用程式組態參考」 (第 141 頁)。

8 根據以下資訊完成此安裝。

安裝畫面	描述
安裝前摘要	閱讀 「安裝前摘要」頁面，確認您選擇的安裝參數。 *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。對安裝和組態參數感到滿意之後，請返回 「安裝前摘要」頁面並按一下 「*安裝*」。
安裝完成	表示已完成安裝。

6.1.1 檢視安裝記錄檔

如果安裝完成時未發生任何錯誤，請移至第 6.2.2 節 「新增使用者應用程式組態檔和 JVM 系統內容」 (第 95 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。

6.2 設定 WebSphere 環境

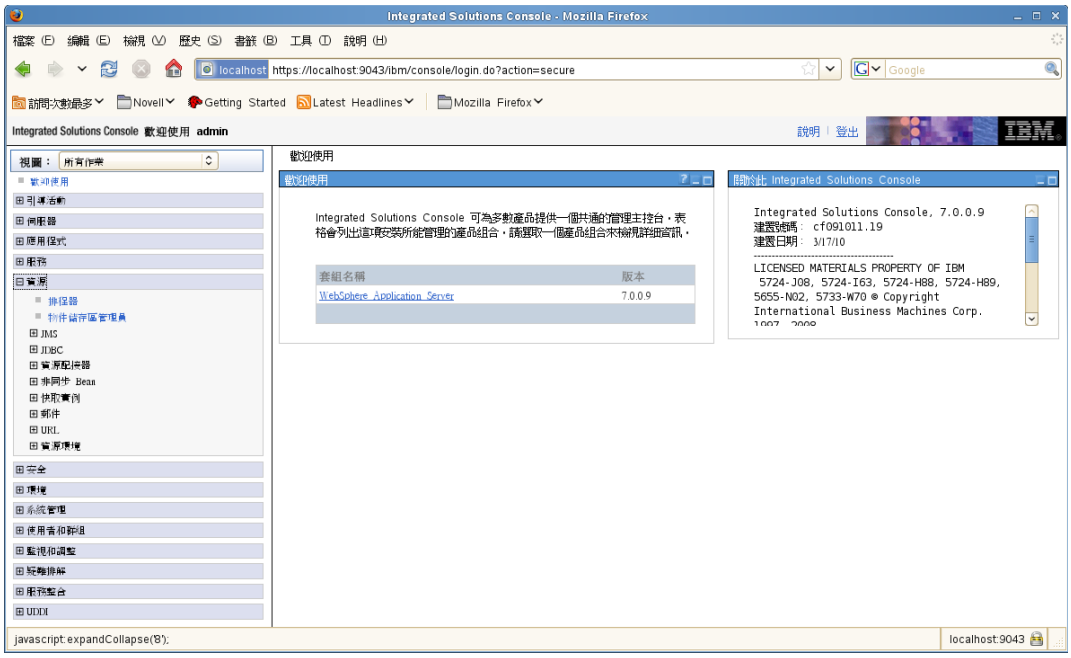
- 第 6.2.1 節 「設定連接池」 (第 87 頁)
- 第 6.2.2 節 「新增使用者應用程式組態檔和 JVM 系統內容」 (第 95 頁)
- 第 6.2.3 節 「將 eDirectory 託管根部輸入至 WebSphere Keystore」 (第 100 頁)
- 第 6.2.4 節 「將 preferIPv4Stack 內容傳送至 JVM」 (第 101 頁)

6.2.1 設定連接池

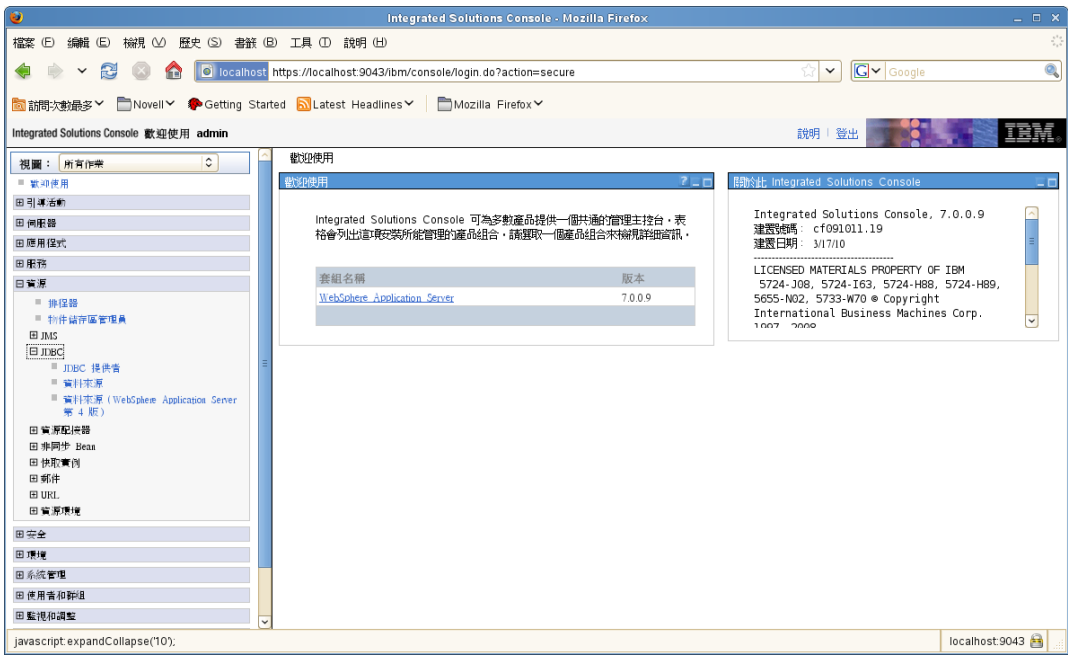
若要設定連接池以與 WebSphere 搭配使用，您需要建立 JDBC 提供者以及資料來源。本節提供有關建立提供者和資料來源的指示。

若要建立 JDBC 提供者：

1 展開 「整合式解決方案主控台」頁左側的 「*資源*」。



2 展開「*JDBC*」：



3 按一下「*JDBC 提供者*」：

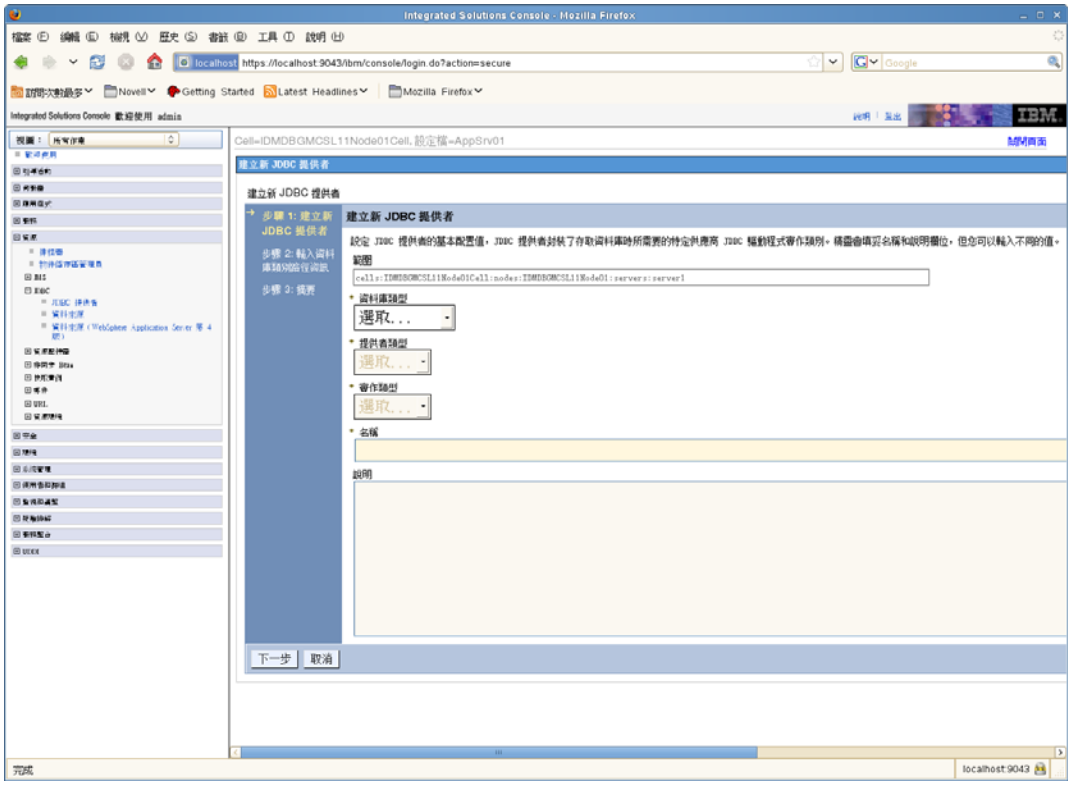
4 展開「*範圍*」：

5 選取「*節點 = 您伺服器的名稱 , 伺服器 =server1*」。

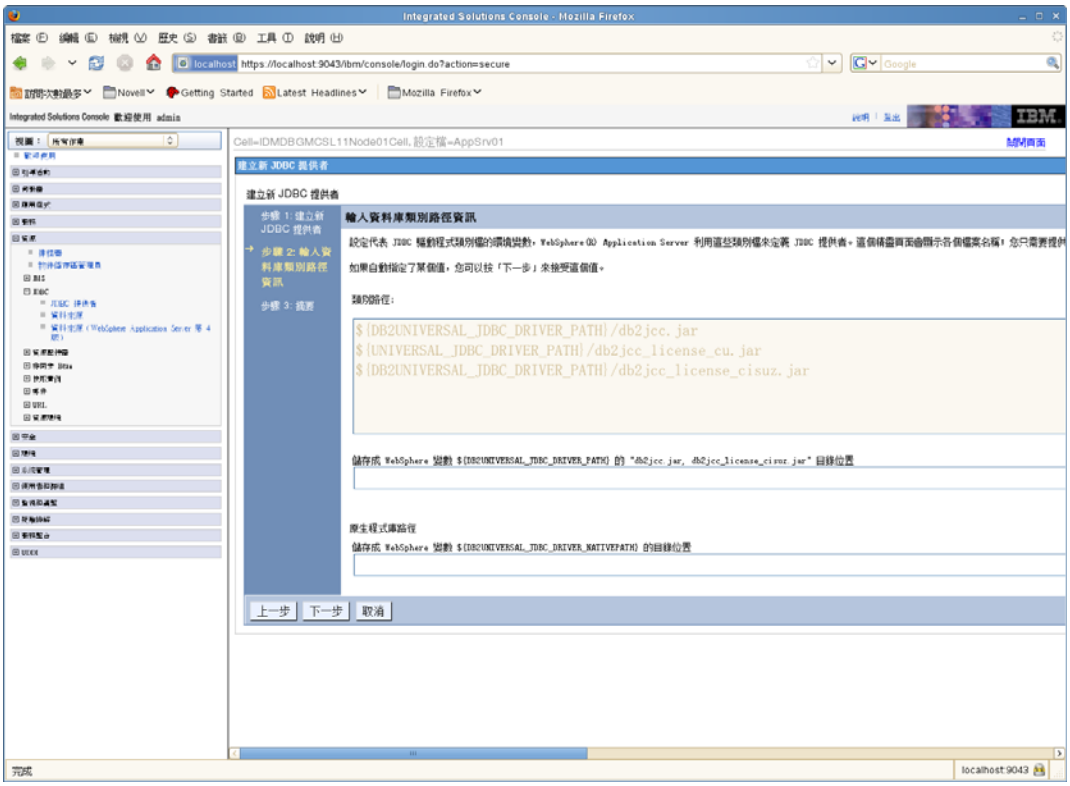
6 按一下「*新增*」按鈕。

7 選取「*資料庫類型*」(例如 DB2)。

8 按「*下一步*」。



9 輸入 JDBC 類別路徑資訊。



10 按一下 *「下一步」*。

11 按一下 *「完成」*。

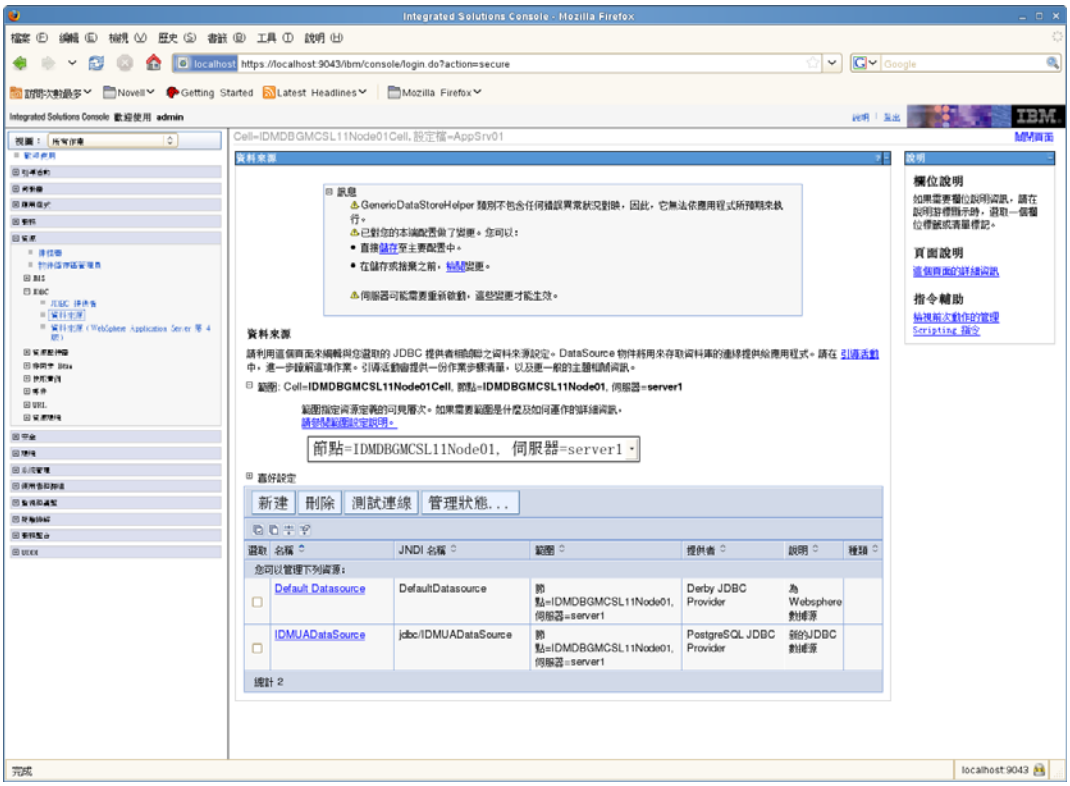
12 按一下「*儲存*」連結。

若要建立資料來源：

1 展開該頁左側的 *「資源」*。

2 展開 *「JDBC」*。

3 按一下 *「資料來源」*。



4 展開「*範圍*」。

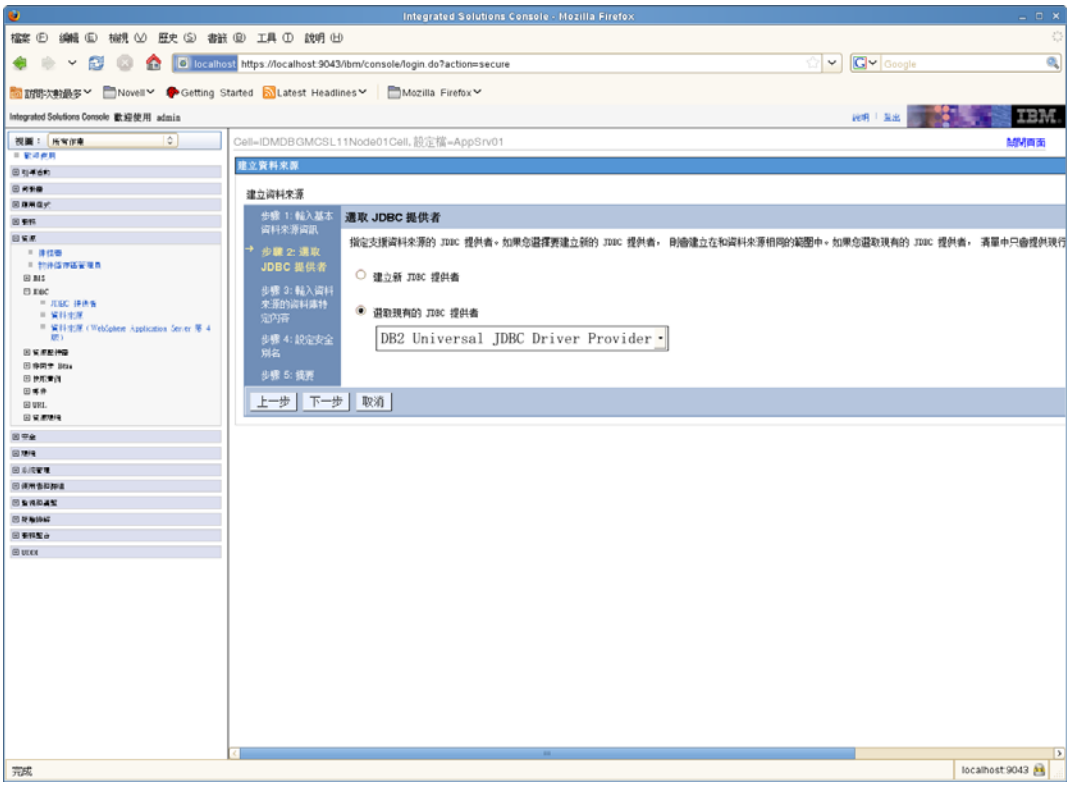
5 選取「*節點 = 您伺服器的名稱 , 伺服器 =server1*」。

6 按一下「*新增*」按鈕。

7 輸入資料來源名稱和 JNDI 名稱 (例如，對兩者均輸入 IDMUADataSource)。

8 按「*下一步*」。

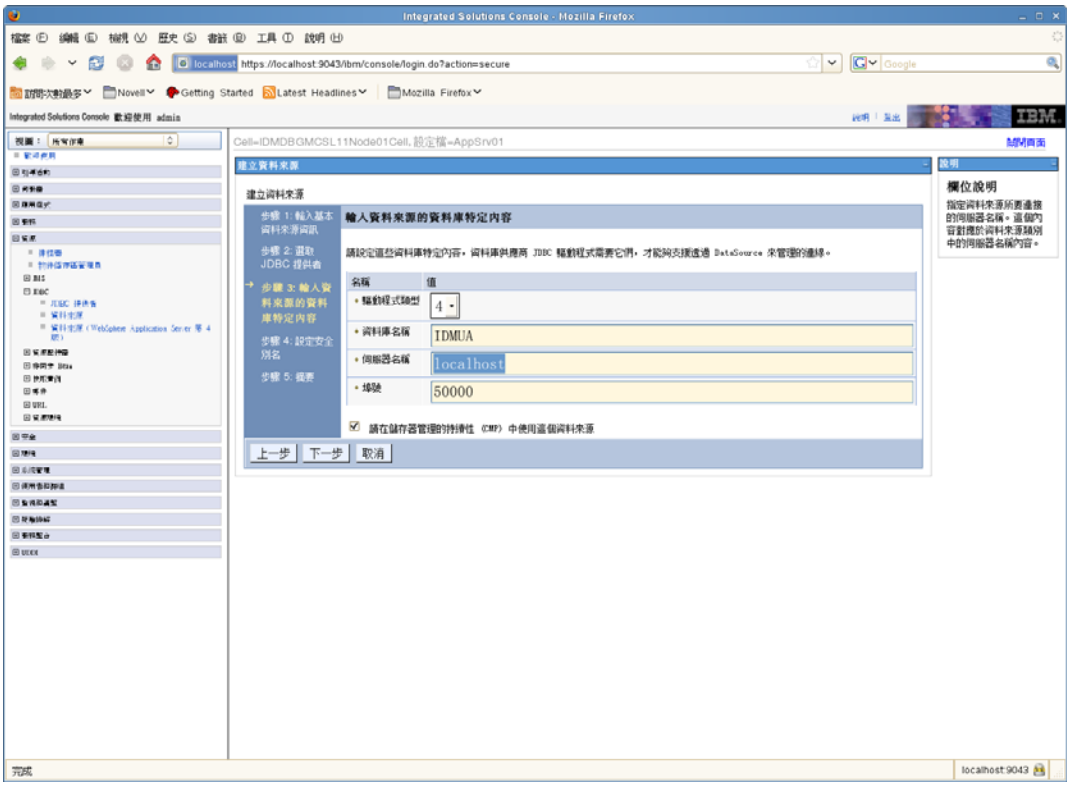
9 按一下「*選取一個現有的 JDBC 提供者*」。



10 選取您剛才建立的 JDBC 提供者。

11 按「*下一步*」。

12 輸入資料來源所需的資料庫資訊 (資料庫名稱、伺服器名稱、連接埠、使用者名稱及密碼)。



13 按「*下一步*」。

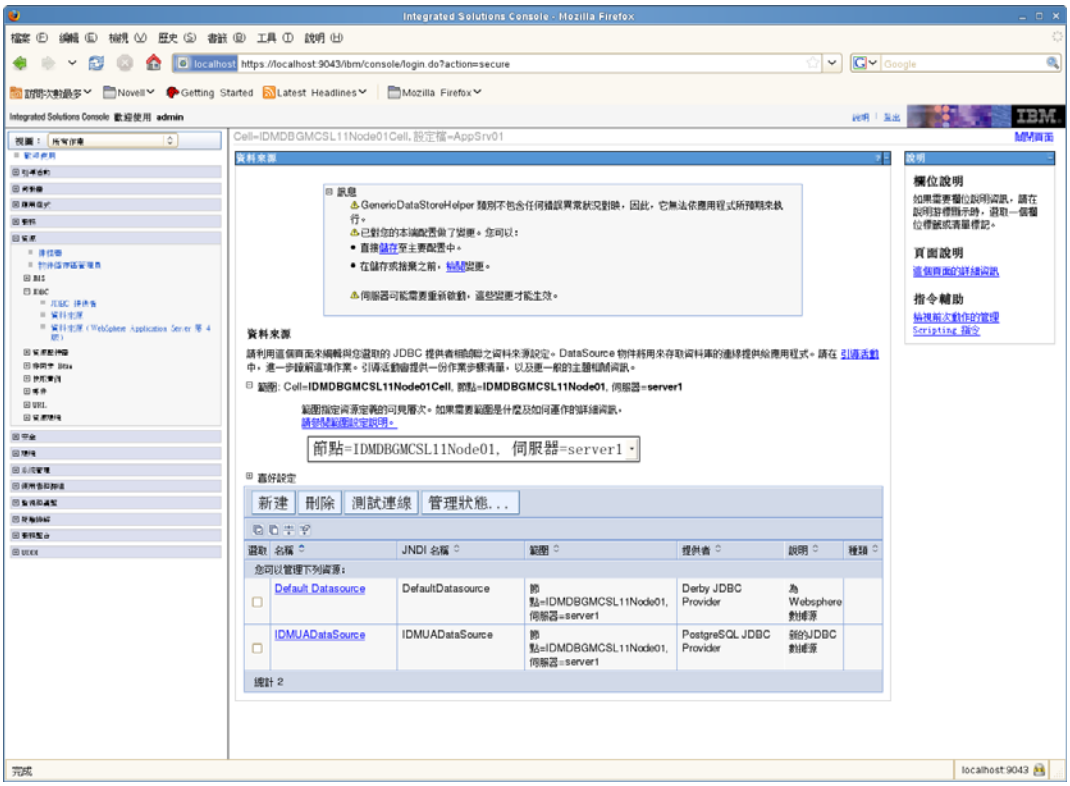
14 輸入安全性別名資訊或保留預設資訊。

15 按一下「*下一步*」。

16 按一下「*完成*」。

17 按一下「*儲存*」。

18 按一下名稱左側的核取方塊，選取這個新資料來源。



19 按一下「*測試連線*」按鈕，並確認其傳回「*成功*」。

6.2.2 新增使用者應用程式組態檔和 JVM 系統內容

要成功安裝 WebSphere 必須執行下列步驟：

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 伺服器之機器上的某個目錄，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 按一下伺服器清單中的某個伺服器名稱，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 將「*名稱*」指定爲 extend.local.config.dir。

9b 將「*值*」指定爲您在安裝期間指定的安裝資料夾 (目錄) 名稱。

安裝程式已將 sys-configuration-xmldata.xml 檔寫入此資料夾中。

9c 將「*描述*」指定爲該內容的描述，例如「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 將「*值*」指定爲您在安裝期間指定的安裝資料夾 (目錄) 名稱。

10c 將「*描述*」指定爲該內容的描述，例如「idmuserapp_logging.xml 的路徑」。

10d 按一下*確定*來儲存變更。

在您透過「*使用者應用程式*」>「*管理*」>「*應用程式組態*」>「*記錄*」保留這些變更之前，idmuserapp-logging.xml 檔並不存在。

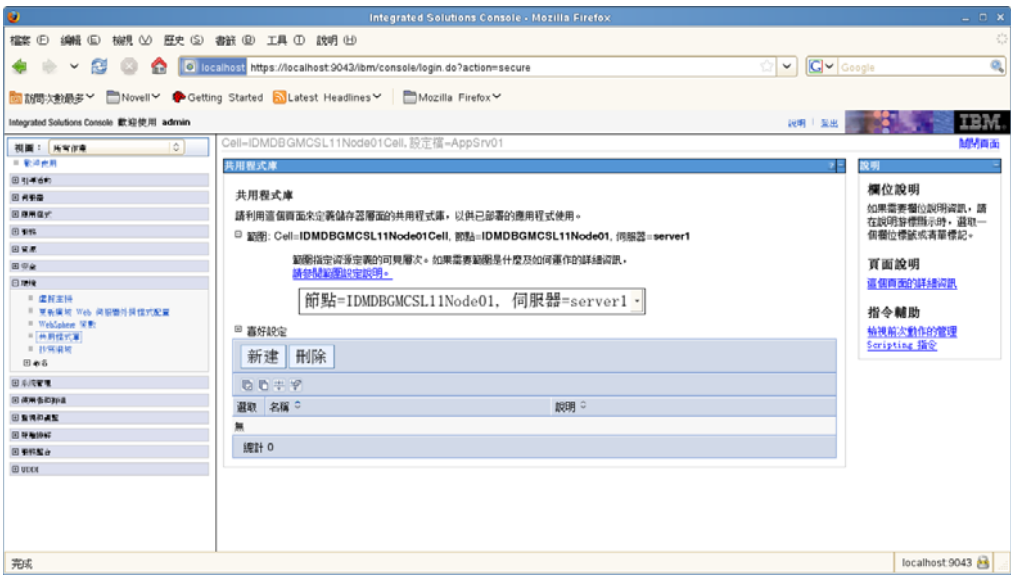
您還需要爲 WebSphere 上的使用者應用程式設定共享文件庫。共享文件庫定義爲確保應用程式正常執行所必需的類別載入行爲。

若要設定共享文件庫：

1 爲使用者應用程式建立共享文件庫：

1a 按一下左導覽目錄中的「*環境*」。

1b 按一下「*共享文件庫*」。



1c 按一下「*新增*」按鈕。

1d 輸入名稱 (例如 IDMUA 類別載入程式)。

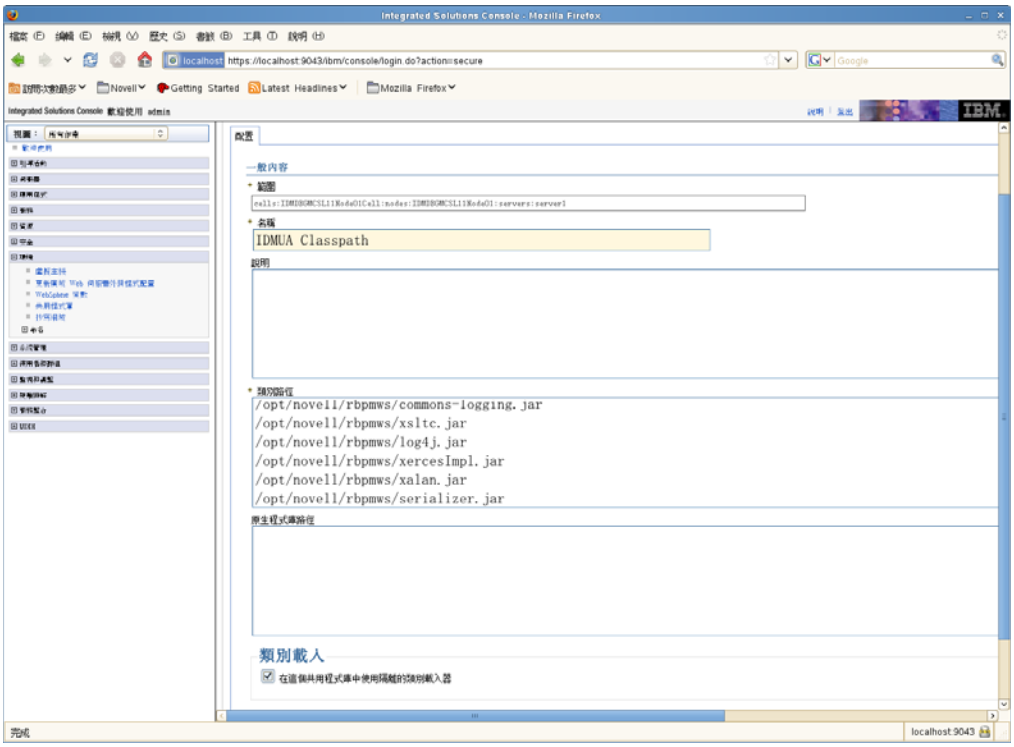
1e 在「類別路徑」欄位中輸入所需的 JAR 檔案清單：

- antlr.jar
- log4j.jar
- commons-logging.jar

  附註：您需要從 Apache 網站下載此 JAR 檔案。

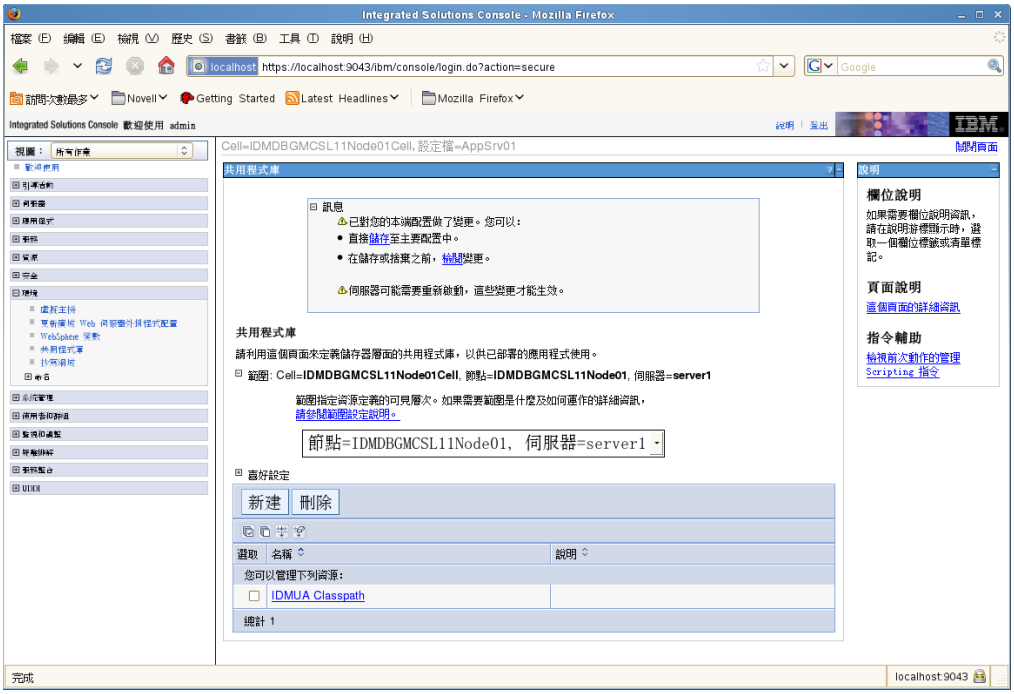
- xalan.jar

- xercesImpl.jar
- xsltc.jar
- serializer.jar
- jaxb-impl.jar
- IDMselector.jar



1f 按一下「*確定*」。

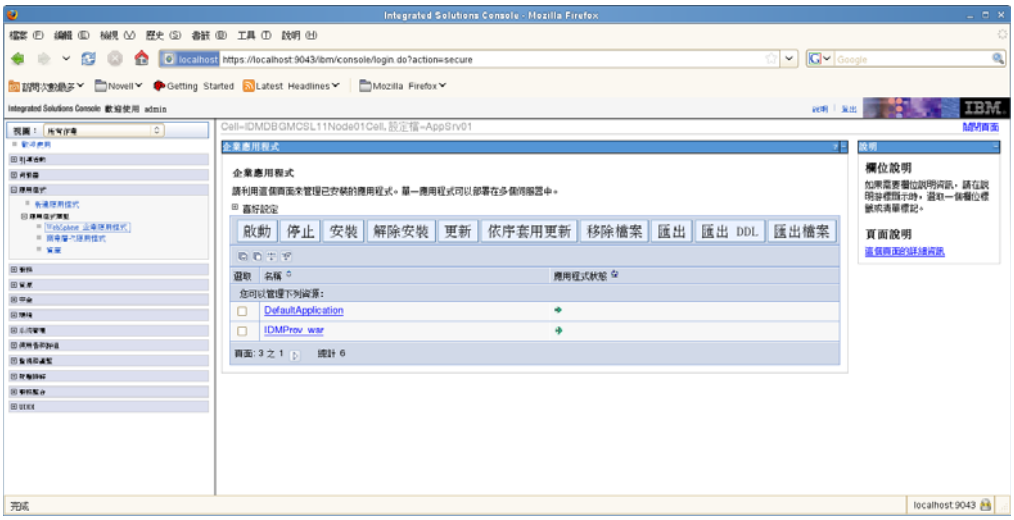
1g 按一下「*儲存*」連結。



2 將共享文件庫新增至 IDMProv ：

2a 按一下左側的「*應用程式*」。

2b 按一下「*WebSphere 企業應用程式*」。



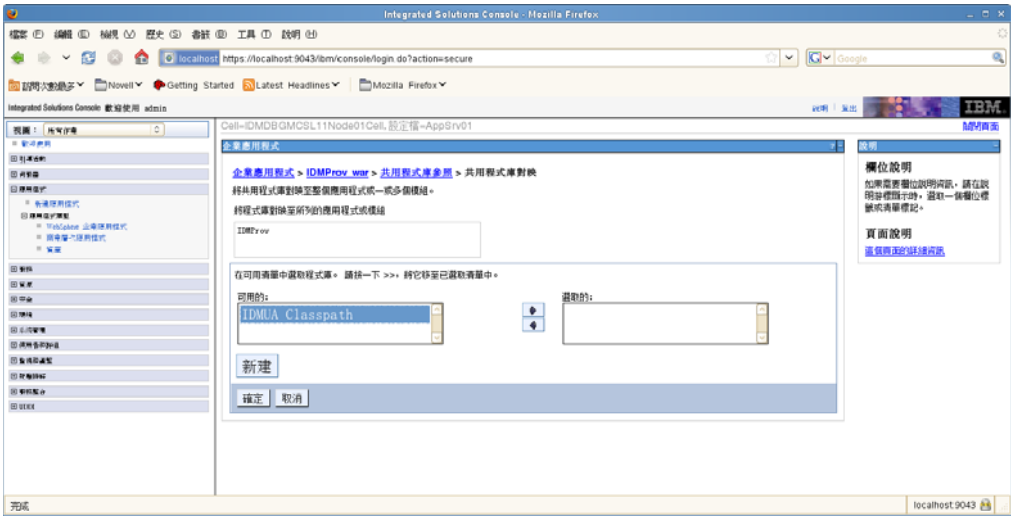
2c 按一下名稱「*IDMProv_war*」。

2d 在頁面底部「*參考*」下方，按一下「*共享文件庫參考*」。

2e 按一下「*IDMProv*」(而不是 IDMProv_war) 旁邊的核取方塊。

2f 按一下「*參考共享文件庫*」按鈕。

2g 按一下「*可用*」方塊中共享文件庫的名稱「*IDMUA 類別路徑*」。然後按一下向右箭頭，將文件庫移至「*已選定*」方塊中。



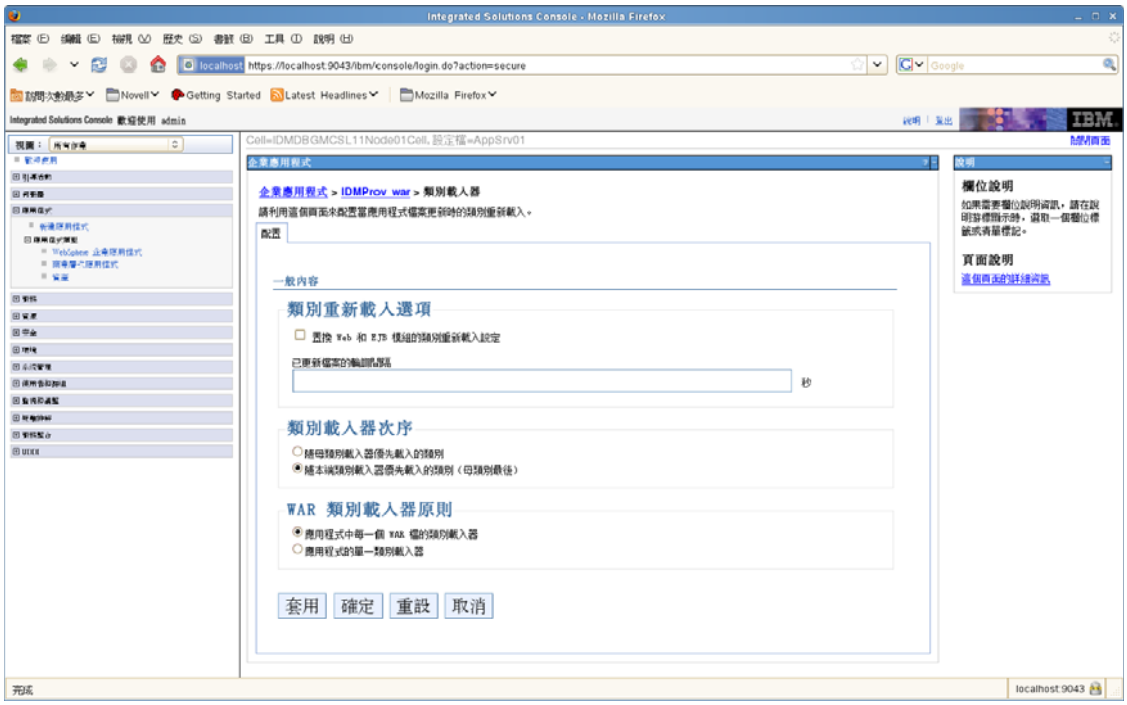
2h 按一下「*確定*」，返回到上一頁。

2i 再按一次「*確定*」。

2j 按一下「*儲存*」，儲存伺服器組態的變更。

2k 執行完所有其他組態步驟之後，重新啓動伺服器。

請注意，類別載入變更應在應用程式層級而非模組層級執行。WebSphere 會爲已部署的 WAR 建立一個 EAR，並將該 WAR 做爲 EAR 中的一個模組：



6.2.3 將 eDirectory 託管根部輸入至 WebSphere Keystore

1 將 eDirectory 託管根部證書複製到代管 WebSphere 伺服器的機器上。

「使用者應用程式」安裝程序會將證書匯出到您安裝 「使用者應用程式」所在的目錄。

2 將證書匯入至 WebSphere keystore。您可以使用 WebSphere 管理員主控台 (「使用 WebSphere 管理主控台匯入證書」(第 100 頁)) 或透過指令行 (「以指令行匯入證書。」(第 101 頁)) 來完成。

3 匯入證書後，繼續進行 第 6.3 節 「部署 WAR 檔案」(第 101 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 「*相關項目*」下的 「*Keystore 與證書*」。

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 鍵入證書檔案的別名和完整路徑。

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。

10 按一下螢幕頂端的 「*儲存*」連結。

以指令行匯入證書。

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。

以下是金鑰工具指令範例：

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。

6.2.4 將 preferIPv4Stack 內容傳送至 JVM

使用者應用程式使用 JGroups 來快取實作。在某些組態中，JGroups 需要將 preferIPv4Stack 內容設定爲 true，以確保 mcast_addr 繫結成功。不如此設定，可能會發生以下錯誤，並且快取作業將無法正常工作：

```
[10/1/09 16:11:22:147 EDT] 0000000d UDP           W org.jgroups.util.Util
createMulticastSocket could not bind to /228.8.8.8 (IPv4 address); make sure
your mcast_addr is of the same type as the IP stack (IPv4 or IPv6).
```

參數 java.net.preferIPv4Stack=true 是一個系統內容，可以使用與其他系統內容 (例如 extend.local.config.dir) 相同的方式進行設定。如需設定系統內容的指示，請參閱第 6.2.2 節「新增使用者應用程式組態檔和 JVM 系統內容」(第 95 頁)。

6.3 部署 WAR 檔案

使用 WebSphere 部署工具來部署 WAR 檔案。

6.3.1 WebSphere 7.0 的其他組態

若要將 WebSphere 7.0 與 RBPM 4.0.1 搭配使用，您需要注意，此 RBPM 版本中有幾個 JAR 檔案 (如 commons-digester.jar) 已升級至最新的可用版本。因此，如果未正確設定環境，則可能會發生與 WebSphere 隨附之 JAR 檔案的版本衝突問題。

若要確保使用的是正確的 JAR 檔案，您需要設定 WebSphere 伺服器，讓其先載入 IDMProv.war 中的類別。對於 IDMProv.war 檔案，需要對 IDMProv.war 選取「*本地類別載入器載入的類別優先 (父代最後)*」選項。

6.4 啓動和存取使用者應用程式

若要啓動「使用者應用程式」：

1. 以 admin 使用者登入 WebSphere 管理主控台。
2. 從左側導覽面板中，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。

存取「使用者應用程式」

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，安全連接埠則爲 9443。URL 的格式爲：http://< *伺服器* >:9080/IDMProv

在 WebLogic 上安裝使用者應用程式 7

WebLogic 安裝程式會根據您的輸入來設定「使用者應用程式」WAR 檔案。本章提供下列詳細資訊：

- 第 7.1 節「WebLogic 安裝核對清單」(第 103 頁)
- 第 7.2 節「安裝和設定使用者應用程式 WAR」(第 103 頁)
- 第 7.3 節「準備 WebLogic 環境」(第 117 頁)
- 第 7.4 節「部署使用者應用程式 WAR」(第 120 頁)
- 第 7.5 節「存取使用者應用程式」(第 120 頁)

若要瞭解如何使用非圖形使用者介面來安裝，請參閱第 8 章 「使用主控台或單一指令來安裝」(第 121 頁)。

以非根使用者的身分執行安裝程式。

資料移轉。如需移轉的相關資訊，請參閱 *《使用者應用程式：移轉指南》*(http://www.novell.com/documentation/idm40/index.html)。

7.1 WebLogic 安裝核對清單

- ❑ 安裝 WebLogic。

  按照 WebLogic 文件中的安裝指示執行。
- ❑ 建立啓用 WebLogic 的 WAR。

  使用「Identity Manager 使用者應用程式」安裝程式來執行這項任務。請參閱第 7.2 節「安裝和設定使用者應用程式 WAR」(第 103 頁)。
- ❑ 將組態檔案複製到適當的 WebLogic 位置，使 WebLogic 環境準備好來部署 WAR。

  請參閱第 7.3 節「準備 WebLogic 環境」(第 117 頁)。
- ❑ 部署 WAR。

  請參閱第 7.4 節「部署使用者應用程式 WAR」(第 120 頁)。

7.2 安裝和設定使用者應用程式 WAR

附註：若是 WebSphere 10.3，安裝程序需要 JRockit 的 Java 2 Platform Standard Edition 開發套件 1.6 版 (JDK)。如果使用其他版本，安裝程序將無法成功設定使用者應用程式 WAR 檔案。安裝會顯示成功，但是當您嘗試啓動「使用者應用程式」時會發生錯誤。

1. 瀏覽至含有安裝檔案的目錄。
2. 使用 JRockit Java 環境 (1.6_17 版) 從指令行啓動平台適用的安裝程式：

   Solaris。

   ```
   $ /opt/WL/bea/jrockit_160_17/bin/java -jar IdmUserApp.jar
   ```

   Windows。

```
C:\WL\bea\jrockit_160_17\bin\java -jar IdmUserApp.jar
```

安裝程式啓動時會提示您選擇語言。

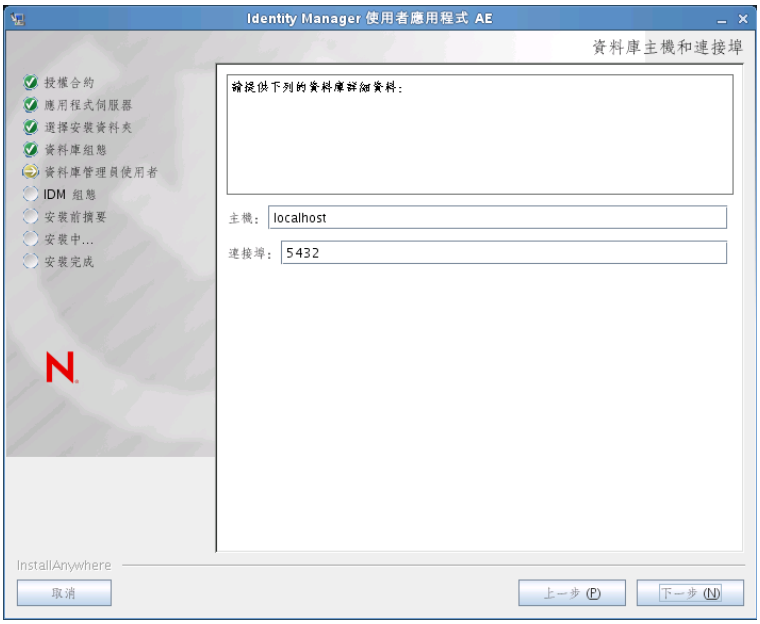
3 根據下列資訊選取語言、確認授權合約並選取應用程式伺服器平台：

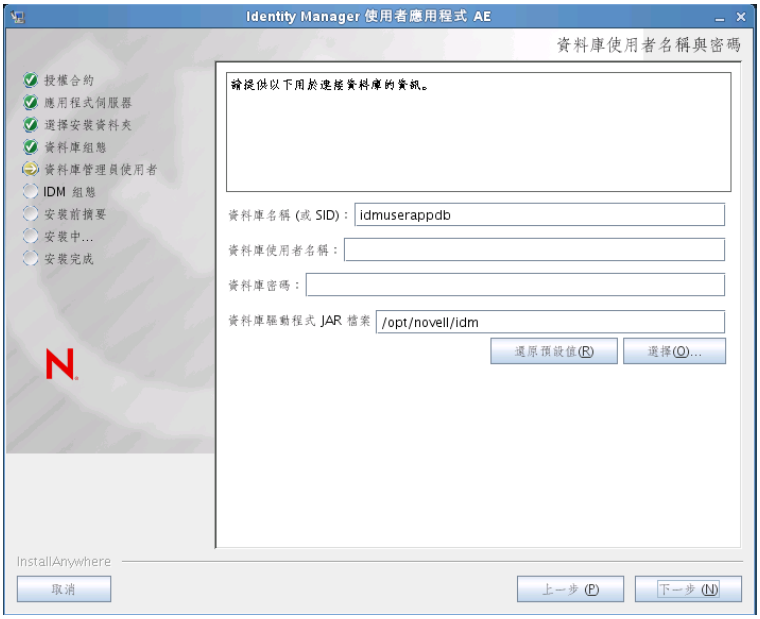
安裝畫面	描述
使用者應用程式安裝	選取安裝程式的語言。預設值爲英文。
授權合約	閱讀授權合約，然後選取「*我接受授權合約中的條款*」。

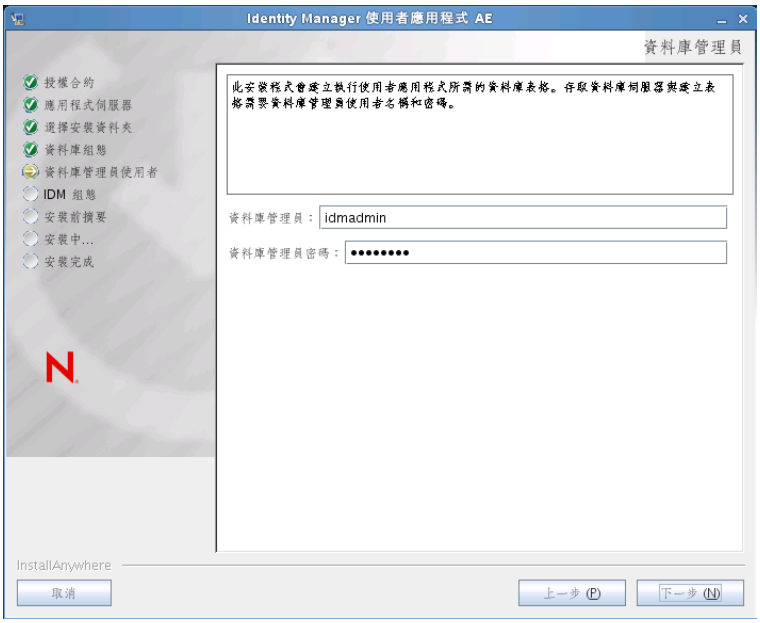
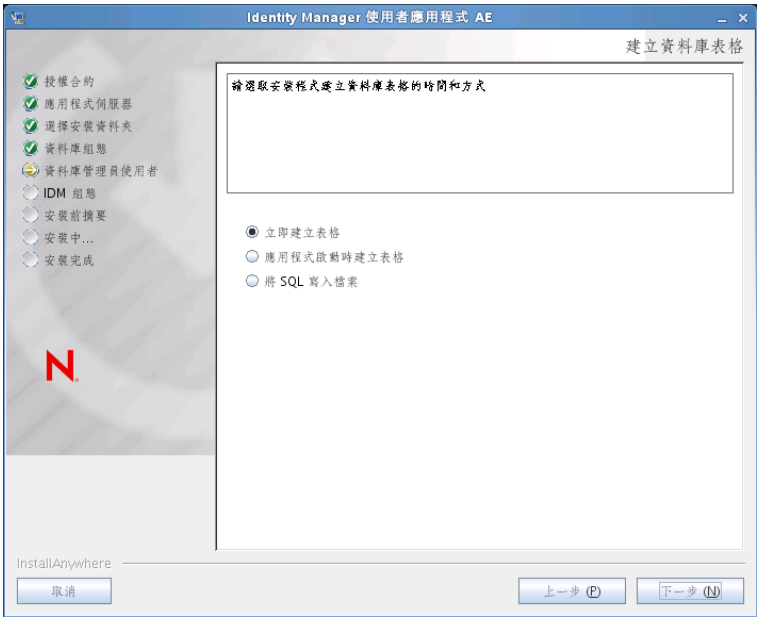
安裝畫面	描述
應用程式伺服器平台	選取「*WebLogic*」。 如果「 使用者應用程式」的 WAR 檔案所在的目錄與安裝程式的不同，安裝程式就會提示您輸入 WAR 的路徑。 如果 WAR 儲存於預設位置，請按一下「*還原預設資料夾*」。若要指定 WAR 檔案的位置，按一下「*選擇*」並選取位置。 如果在 WebLogic 上安裝，您需要使用 BEA 的 Java 環境 (jrockit) 啓動安裝程式。如果選取 WebLogic 作爲您的應用程式伺服器，而不使用 jrockit 來啓動安裝，則系統會顯示快顯錯誤訊息，並終止安裝： 

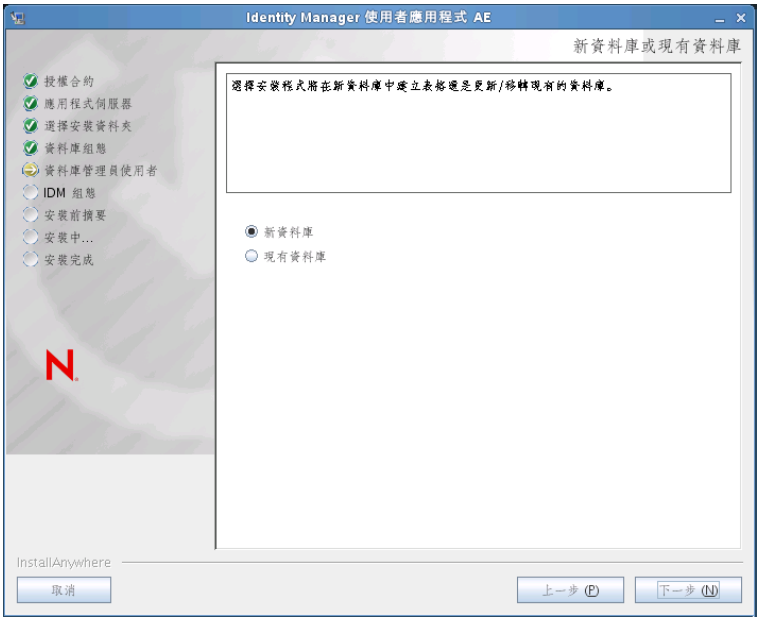
4 根據下列資訊選擇安裝資料夾並設定資料庫：

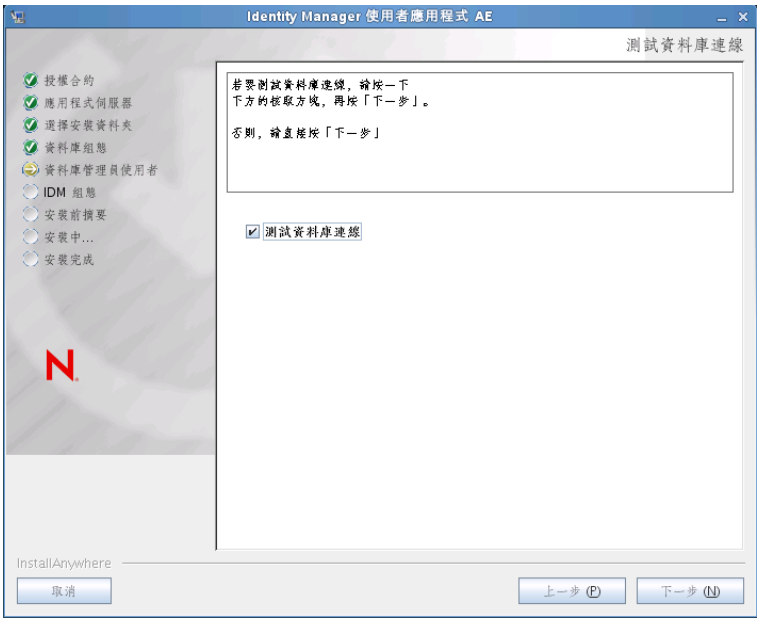
安裝畫面	描述
選擇安裝資料夾	指定安裝程式應該將檔案放在何處。
資料庫平台	選取資料庫平台。必須已安裝資料庫和 JDBC 驅動程式。對於 WebLogic，選項包含下列各項： ◆ Oracle ◆ Microsoft SQL Server ◆ PostgreSQL

安裝畫面	描述
資料庫主機和連接埠	*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。 

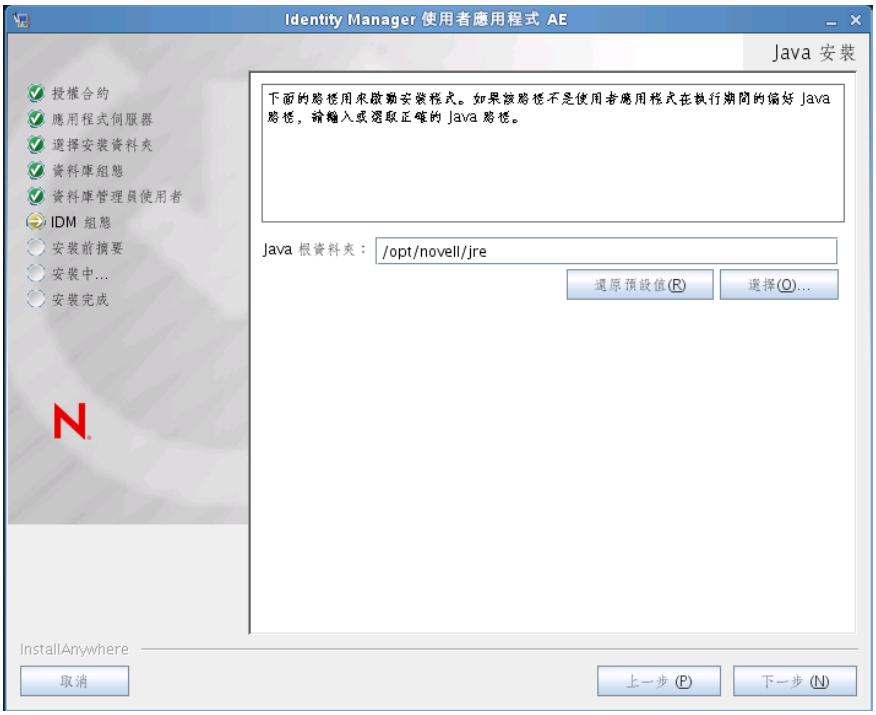
安裝畫面	描述
資料庫使用者名稱與密碼	*資料庫名稱* (或 SID)：對於 MS SQL Server 或 PostgreSQL，請提供您預先設定的資料庫名稱。對於 Oracle，請提供您之前建立的 Oracle 系統識別碼 (SID)。對於叢集，請爲叢集的每一個成員指定相同的資料庫名稱和 SID。 *資料庫使用者*名稱：指定資料庫使用者。若是叢集，請爲叢集的每一個成員指定相同的資料庫使用者。 *資料庫密碼*：指定資料庫密碼。若是叢集，請爲叢集的每一個成員指定相同的資料庫密碼。 *資料庫驅動程式 JAR 檔案*：爲資料庫伺服器提供簡易用戶端 JAR。此爲必填欄位。 

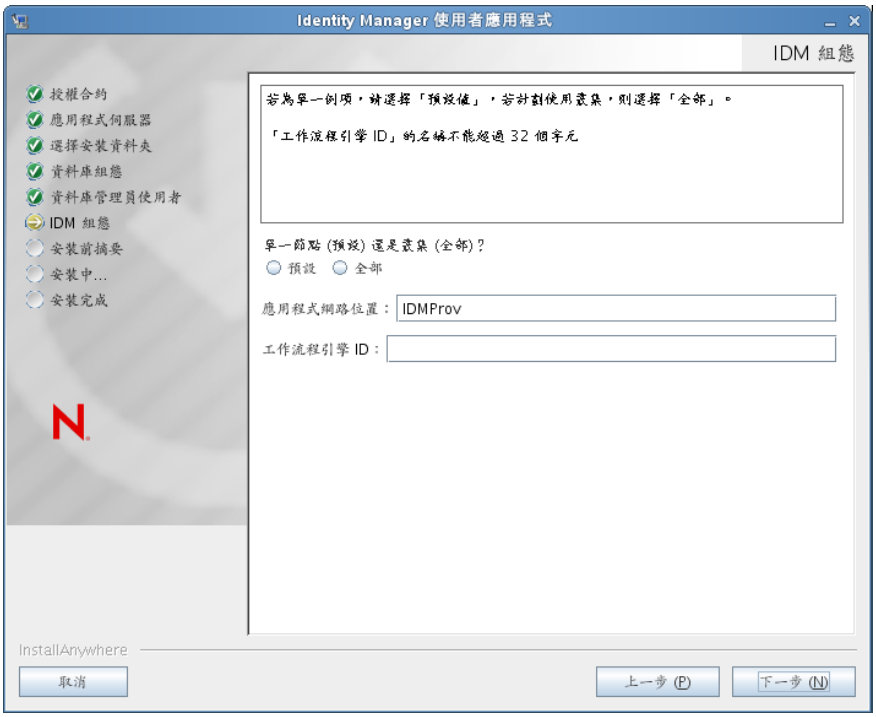
安裝畫面	描述
資料庫管理員	此螢幕已預先填入「資料庫使用者名稱與密碼」頁面上顯示的使用者名稱與密碼。如果之前指定的資料庫使用者不具備足夠許可，因而無法在資料庫伺服器中建立表格，則需要輸入具備必要權限的其他使用者 ID。 
建立資料庫表格	指定應在何時建立資料庫表格： 

安裝畫面	描述
新資料庫或現有資料庫	如果要使用的是新資料庫或空資料庫，請選取「*新資料庫*」按鈕。如果要使用先前的安裝留下的現有資料庫，請選取「*現有資料庫*」按鈕。 

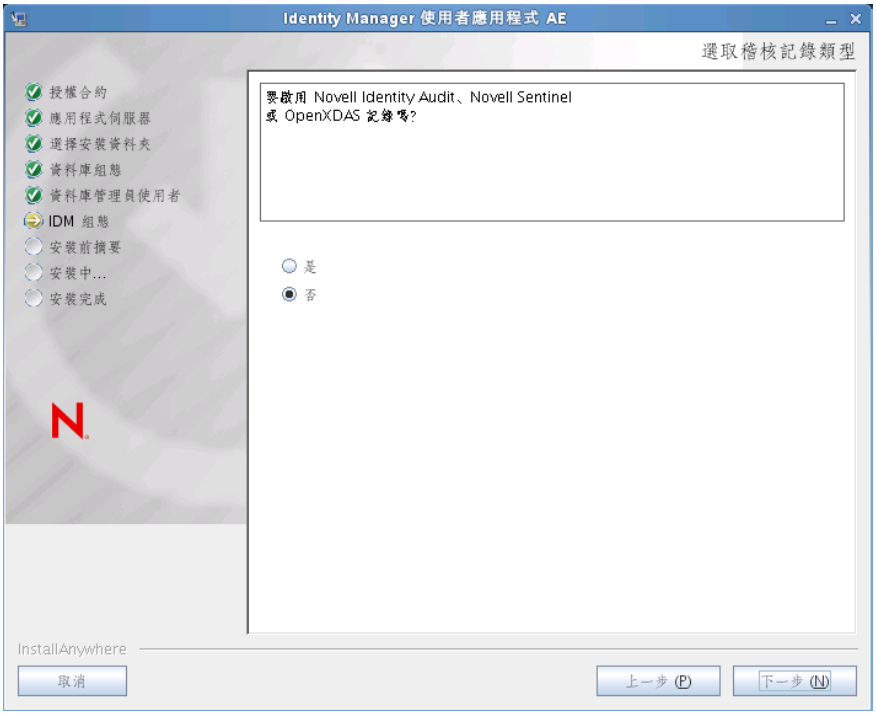
安裝畫面	描述
測試資料庫連接	若要確認之前螢幕中提供的資訊是否正確，可以選取「*測試資料庫連接*」核取方塊來測試資料庫連接：  安裝程式在直接建立表格以及建立 .SQL 檔案時都需要連接至資料庫。若測試資料庫連接而連接失敗，您還是可以繼續安裝。此種情況下，您將需要在安裝之後建立表格，如 *《User Application: Administration Guide》(使用者應用程式：管理指南)* (http://www.novell.com/documentation/idm40/agpro/?page=/documentation/idm40/agpro/data/bncf7rj.html) 中所述。

5 根據下列資訊設定 Java、Identity Manager 以及稽核設定與安全性。

安裝畫面	描述
Java 安裝	指定 Java 安裝根資料夾。Java 安裝透過 JAVA_HOME 環境變數來提供 Java 路徑，並提供修正路徑的選項：  此時，安裝程式還會驗證選取的 Java 是否適用於所選的應用程式伺服器。另外，也會驗證其是否可以寫入指定 JRE 中的 cacerts。

安裝畫面	描述
IDM 組態	*應用程式網路位置*：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「使用者應用程式」時，請在 URL 中輸入這個名稱。 

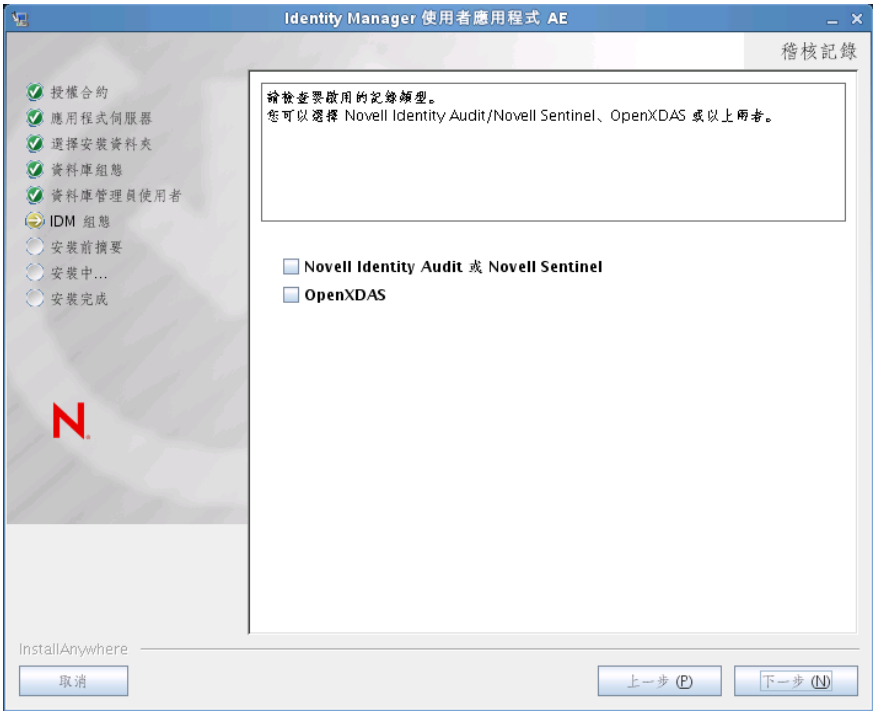
安裝畫面	描述
選取稽核記錄類型	若要啓用記錄，請按一下「*是*」。若要停用記錄，請按一下「*否*」。



下一個面板會提示您指定記錄類型。請從下列選項中選擇：

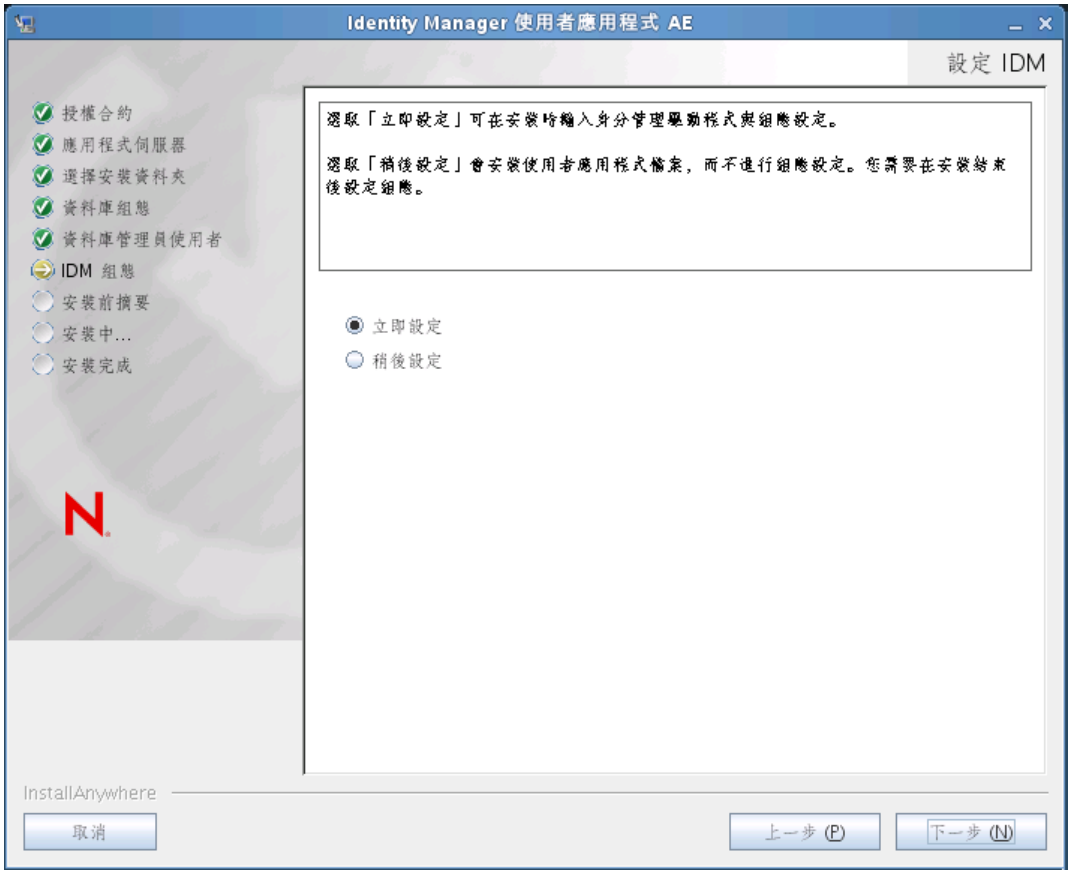
- *Novell Identity Audit 或 Novell Sentinel*：啓用透過 Novell 稽核用戶端對使用者應用程式的記錄。
- *OpenXDAS*：將事件記錄至您的 OpenXDAS 記錄伺服器。

如需設定記錄的詳細資訊，請參閱 *《使用者應用程式：管理指南》*。



安裝畫面	描述
Novell Identity Audit 或 Novell Sentinel	*伺服器*：如果啓用記錄，請指定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。
安全性 - 萬能金鑰	*是*：可讓您「匯入」現有的萬能金鑰。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。 *否*：建立新的萬能金鑰。完成安裝之後，您必須手動記錄第 9.1 節「記錄萬能金鑰」(第 133 頁) 中所述的萬能金鑰。 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。 匯入現有的萬能金鑰有下列理由： ◆ 您想將安裝從臨時系統移到生產系統，並想保留臨時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。

6 若現在要設定 RBPM，請選取「*立即設定*」，然後按「*下一步*」。



(如果沒有顯示這些資訊，可能是您未完成第 2.5 節「安裝 Java 開發套件」(第 27 頁)中所述的步驟。)

「Roles Based Provisioning Module 組態」面板的預設檢視窗會顯示下列六個欄位：

安裝程式會採用「根容器 DN」中的值，並將其套用至下列值：

- 使用者容器 DN
- 群組容器 DN

安裝程式會採用「使用者應用程式管理員」欄位中的值，並將其套用至下列值：

- 佈建管理員
- 法規遵循管理員
- 角色管理員
- 安全性管理員
- 資源管理員
- RBPM 組態管理員

如果要明確指定這些值，可以按一下「*顯示進階選項*」按鈕並進行變更。

「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。

如需每一個選項的說明，請參閱附錄 A 「使用者應用程式組態參考」 (第 141 頁)。

7 根據以下資訊完成此安裝。

安裝畫面	描述
安裝前摘要	閱讀 「安裝前摘要」頁面，確認您選擇的安裝參數。 *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。對安裝和組態參數感到滿意之後，請返回 「安裝前摘要」頁面並按一下 「*安裝*」。
安裝完成	表示已完成安裝。

7.2.1 檢視安裝和記錄檔案

如果安裝完成並且未發生任何錯誤，請繼續準備 WebLogic 環境。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。

7.3 準備 WebLogic 環境

7.3.1 設定連接池

- ❑ 將資料庫驅動程式 JAR 檔案複製到您要部署使用者應用程式的網域。
- ❑ 建立資料來源。

  依照 WebLogic 文件中的指示建立資料來源。

  請注意，無論您在建立使用者應用程式 WAR 時爲資料來源或資料庫指定了什麼名稱，資料來源的 JNDI 名稱都必須爲 jdbc/IDMUADataSource。

7.3.2 指定 RBPM 組態檔案位置

WebLogic 使用者應用程式需要知道如何尋找 sys-configuration-xmldata.xml 檔案、idmuserapp_logging.xml 檔案及 wl_idmuserapp_logging.xml 檔案。因此，您需要將這些檔案的位置新增至 setDomainEnv.cmd 檔案中。

爲了使應用程式伺服器可以找到這些檔案，請在 setDomainEnv.cmd 或 setDomainEnv.sh 檔案中指定其位置：

1 開啓 setDomainEnv.cmd 或 setDomainEnv.sh 檔案。

2 找出如下所示的那一行：

```
set JAVA_PROPERTIES
export JAVA_PROPERTIES
```

3 在 JAVA_PROPERTIES 項目下，新增下列項目：

- -Dextend.local.config.dir==< 目錄路徑 >：指定 sys-configuration.xml 檔案所在的資料夾 (不是檔案本身)。
- -Didmuserapp.logging.config.dir==< 目錄路徑 >：指定 idmuserapp_logging.xml 檔案所在的資料夾 (不是檔案本身)。
- -Dlog.init.file==< 檔案名稱 > ：指定用於 log4j 組態的 wl_idmuserapp_logging.xml 檔案。此檔案會在同一應用程式伺服器上安裝多個應用程式的情況下，處理使用者應用程式所需的 appender 和 logger 組態。

例如，在 Windows 上：

```
set JAVA_OPTIONS=-Dextend.local.config.dir=c:\novell\idm
set JAVA_OPTIONS=%JAVA_OPTIONS% -
Didmuserapp.logging.config.dir=c:\novell\idm
set JAVA_OPTIONS=%JAVA_OPTIONS%
-Dlog.init.file=wl_idmuserapp_logging.xml
```

4 將環境變數 EXT_PRE_CLASSPATH 設定爲指向以下 JAR 檔案：

- antlr-2.7.6.jar
- log4j.jar
- commons-logging.jar

  附註：您需要從 Apache 網站下載此 JAR 檔案。

- xalan.jar
- xercesImpl.jar
- xsltc.jar
- serializer.jar
- IDMselector.jar

附註：也可以將這些 JAR 檔案複製到 IDMProv.war 檔案內的 WEB-INF/lib 目錄中，如此便無需將這些檔案新增至 EXT_PRE_CLASSPATH 變數。

4a 找出這一行：

```
ADD EXTENSIONS TO CLASSPATH
```

4b 在這一行下面新增 EXT_PRE_CLASSPATH。例如，在 Windows 上：

```
set
EXT_PRE_CLASSPATH=C:\bea\user_projects\domains\base_domain\lib\antlr-
2.7.6.jar;C:\bea\user_projects\domain\base_domain\lib\log4j.jar;C:\be
a\user_projects\domains\base_domain\lib\commons-
logging.jar;C:\bea\user_projects\domains\base_domain\lib\xalan.jar;C:
\bea\user_projects\domains\base_domain\lib\xercesImpl.jar;C:\bea\user
_projects\domains\base_domain\lib\xsltc.jar;C:\bea\user_projects\doma
ins\base_domain\lib\serializer.jar
```

例如，在 Linux 上：

```
export EXT_PRE_CLASSPATH=/opt/bea/user_projects/domains/base_domain/
lib/antlr-2.7.6.jar:/opt/bea/user_projects/domain/base_domain/lib/
log4j.jar:/opt/bea/user_projects/domains/base_domain/lib/commons-
logging.jar:/opt/bea/user_projects/domains/base_domain/lib/
xalan.jar:/opt/bea/user_projects/domains/base_domain/lib/
xercesImpl.jar:/opt/bea/user_projects/domains/base_domain/lib/
xsltc.jar:/opt/bea/user_projects/domains/base_domain/lib/
serializer.jar
```

5 儲存並結束檔案。

設定的公用程式也會使用這些 XML 檔案，因此，您需要編輯 configupdate.bat 或 configupdate.sh 檔案，如下所示：

1 開啓 configupdate.bat 或 configupdate.sh。

2 找出下一行：

```
-Duser.language=en -Duser.region="
```

3 更新該行，在其中包含 sys-configuration.xml 檔案的路徑：

例如，在 Windows 上：

```
-Dextend.local.config.dir=c:\novell\idm
```

例如，在 Linux 上：

```
-Dextend.local.config.dir=/opt/novell/idm
```

4 儲存然後關閉該檔案。

5 執行 configupdate 公用程式，將證書安裝至 BEA_HOME 之下的 JDK KeyStore。

執行 configupdate 時會詢問您目前使用的 JDK 的 cacerts 檔案。如果您使用的 JDK 不是安裝期間所指定的 JDK，則必須在 WAR 上執行 configupdate。請注意指定的 JDK，因爲這個項目必須指向 WebLogic 所使用的 JDK。這是爲了匯入 Identity Vault 連線所需的證書檔案。這是爲了匯入 eDirectory 連線所需的證書。

configupdate 公用程式中的 Identity Vault 證書值必須指向下列位置：

```
c:\jrockit\jre\lib\security\cacerts
```

7.3.3 移除 OpenSAML JAR 檔案

WebLogic 使用的 OpenSAML JAR 檔案與使用者應用程式所需的檔案有衝突。因此，您需要從 WebLogic /WL103/modules 目錄中移除這些檔案，以確保使用者應用程式在 WebLogic 上正確部署。此要求適用於任何未啓用 SSO 的使用者應用程式。

請務必從 WebLogic /WL103/modules 目錄中移除以下 JAR 檔案：

```
com.bea.core.bea.opensaml_1.0.0.0_5-0-2-0.jar
com.bea.core.bea.opensaml2_1.0.0.0_5-0-2-0.jar
```

7.3.4 工作流程外掛程式和 WebLogic 安裝

如果 enforce-valid-basic-auth-credentials 旗標設爲 true，則到 iManager 的「工作流程管理」外掛程式會無法連線到 WebLogic 上執行的「使用者應用程式驅動程式」。爲讓連線可以成功，您必須將此旗標停用。

若要停用 enforce-valid-basic-auth-credentials 旗標，請依照這些指示：

1. 開啓 <*WLHome*>\user_projects\domains\idm\config\ 資料夾中的 config.xml 檔案。
2. 在 <security-configuration> 區段末尾的上方新增下行：

   ```
   <enforce-valid-basic-auth-credentials>false</enforce-valid-basic-auth-credentials>
   </security-configuration>
   ```

3. 儲存檔案並重新啓動伺服器。

進行這項變更之後，您應該會無法登入「工作流程管理」外掛程式。

7.4 部署使用者應用程式 WAR

此時，您可以使用標準的 WebLogic 部署程序部署使用者應用程式 WAR。

7.5 存取使用者應用程式

- 導覽至「使用者應用程式」URL：

  ```
  http://application-server-host:port/application-context
  ```

  例如：

  ```
  http://localhost:8180/IDMProv
  ```

使用主控台或單一指令來安裝

8

本章說明的安裝方法可用於取代第 5 章 「在 JBoss 上安裝使用者應用程式」 (第 53 頁) 中所述之使用圖形使用者介面進行安裝的方法。主題包括：

- 第 8.1 節 「透過主控台安裝使用者應用程式」 (第 121 頁)
- 第 8.2 節 「使用單一指令安裝使用者應用程式」 (第 121 頁)
- 第 8.3 節 「以靜默模式或主控台模式執行 JBossPostgreSQL 公用程式」 (第 129 頁)
- 第 8.4 節 「以靜默模式或主控台模式執行 RIS 安裝程式」 (第 131 頁)

8.1 透過主控台安裝使用者應用程式

本程序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」。

附註：安裝程式至少需要 Java 2 Platform Standard Edition 開發套件 1.5 版。如果您使用舊版本，則安裝程序無法成功地設定 「使用者應用程式」 WAR 檔案。安裝會顯示成功，但是當您嘗試啓動 「使用者應用程式」時會發生錯誤。

---

1. 一旦您獲得如 表格 2-1 (第 15 頁) 所述的適當安裝檔案後，請登入並開啓終端機工作階段。
2. 使用 Java 啓動平台的安裝程式，如下所示：

   java -jar IdmUserApp.jar -i console
3. 請依照第 5 章 「在 JBoss 上安裝使用者應用程式」 (第 53 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。
4. 若要設定 「使用者應用程式」組態參數，請手動啓動 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 A.1 節 「使用者應用程式組態：基本參數」 (第 141 頁) 中所述的值。
5. 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。
6. 請繼續進行第 9 章 「安裝後任務」 (第 133 頁)。

8.2 使用單一指令安裝使用者應用程式

本程序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 2-1 (第 15 頁) 中所列的適當安裝檔案。
2. 登入並開啓終端機工作階段。
3. 找到安裝檔案中隨附的 Identity Manager 內容檔案 silent.properties。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 8-1。「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 / *目錄路徑* /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 8-1 *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同等參數**
NOVL_CONFIG_LDAPHOST=	eDirectory 連線設定：LDAP 主機。 指定 LDAP 伺服器的主機名稱或 IP 位址。
NOVL_CONFIG_LDAPADMIN=	eDirectory 連線設定：LDAP 管理員。 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。 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。 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。 「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`

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同等參數
NOVL_CONFIG_LOCKSMITH=	eDirectory DN：使用者應用程式管理員。 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*」索引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，則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 *《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，必須使用「使用者應用程式」中的 *「管理」* > *「安全性」*頁面。
NOVL_CONFIG_PROVLOCKSMITH=	eDirectory DN：佈建應用程式管理員。 Identity Manager 的佈建版本中會提供此使用者。「提供應用程式管理員」會使用「*管理*」索引標籤下方的「*提供*」索引標籤來管理「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*」索引標籤供使用者使用。此使用者必須先存在於 Identity Vault，才能指定爲「佈建應用程式管理員」。 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_ROLECONTAINERDN=	此角色用於 Novell Identity Manager Roles Based Provisioning Module 中。此角色允許成員建立、移除或修改所有角色，授予或撤銷對任何使用者、群組或容器所做的任何角色指定。它還允許其角色成員爲任一使用者執行報告。依預設，「使用者應用程式」管理員會指定爲此角色。 若要在部署「使用者應用程式」之後更改此指定，請使用「使用者應用程式」中的 *「角色」* > *「角色指定」*頁面。
NOVL_CONFIG_COMPLIANCECONTAINERDN	法規遵循模組管理員是一個系統角色，允許成員執行「*法規遵循*」索引標籤上的所有功能。此使用者必須先存在於 Identity Vault 中，才能指定爲「法規遵循模組管理員」。

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同等參數
NOVL_CONFIG_USERCONTAINERDN=	中繼目錄使用者身份：使用者容器 DN。 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。 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。 指定應用程式伺服器使用的 JRE 之 keystore (cacerts) 檔案的完整路徑。「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。 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。 必要。指定 *True* 來要求，必須以安全插槽進行所有使用管理員帳戶的通訊 (此選項可能會對效能產生負面影響)。此設定允許不透過 SSL 來執行不需要 SSL 的其他操作。 如果管理員帳戶不使用安全插槽通訊，則指定 *False*。
NOVL_CONFIG_SECUREUSERCONNECTION=	eDIRECTORY 連線設定：安全使用者連線。 必要。指定 *True* 來要求，必須以安全插槽進行所有使用登入之使用者帳戶來執行的通訊 (此選項可能會對效能產生負面影響)。此設定允許不透過 SSL 來執行不需要 SSL 的其他操作。 如果使用者的帳戶不使用安全插槽通訊，則指定 *False*。
NOVL_CONFIG_SESSIONTIMEOUT=	其他：工作階段逾時。 必要。指定應用程式工作階段逾時間隔。
NOVL_CONFIG_LDAPPLAINPORT=	eDirectory 連線設定：LDAP 非安全連接埠。 必要。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同等參數
NOVL_CONFIG_LDAPSECUREPORT=	eDirectory 連線設定：LDAP 安全連接埠。 必要。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。 必要。指定 *True*，允許未登入的使用者存取「LDAP 公用匿名帳戶」。 指定 *False* 則改爲啓用 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 是佈建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。 用於取代佈建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。 用於取代佈建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。 必要。指定來自佈建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。 必要。指定佈建電子郵件所使用的 SMTP 電子郵件主機。可以是 IP 位址或 DNS 名稱。

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同等參數
NOVL_CONFIG_USEEXTPWDWAR=	密碼管理：使用外部密碼 WAR。 如果您使用的是外部密碼管理 WAR，請指定 *True*。如果您指定 *True*，還必須提供 *NOVL_CONFIG_EXTPWDWARPTH* 和 *NOVL_CONFIG_EXTPWDWARRTNPATH* 的值。 指定「*False*」即使用預設的內部密碼管理功能 *./jsps/pwdmgt/ForgotPassword.jsp* (開頭不加 http(s) 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。 在外部或內部密碼管理 WAR 中指定「忘記密碼」功能頁面 ForgotPassword.jsp 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「設定外部忘記密碼管理」(第 136 頁)。
NOVL_CONFIG_EXTPWDWARRTNPATH=	密碼管理：忘記密碼回傳連結。 指定「忘記密碼回傳連結」以便使用者在執行忘記密碼操作後使用。
NOVL_CONFIG_FORGOTWEBSERVICEURL=	密碼管理：忘記密碼 Web 服務 URL。 外部忘記密碼 WAR 將使用此 URL 回撥到使用者應用程式以執行重要的忘記密碼功能。此 URL 的格式爲： `https://<idmhost>:<sslport>/<idm>/pwdmgt/service`
NOVL_CONFIG_USEROBJECTATTRIBUTE=	中繼目錄使用者身份：使用者物件類別。 必要。LDAP 使用者物件類別 (通常爲 inetOrgPerson)。
NOVL_CONFIG_LOGINATTRIBUTE=	中繼目錄使用者身份：登入屬性。 必要。代表使用者登入名稱的 LDAP 屬性 (例如 CN)。
NOVL_CONFIG_NAMINGATTRIBUTE=	中繼目錄使用者身份：命名屬性。 必要。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。選擇性。 必要。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。 必要。LDAP 群組物件類別 (通常爲 groupofNames)。

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同等參數
NOVL_CONFIG_GROUPMEMBERSHIPATTRIBUTE=	中繼目錄使用者群組：群組成員資格屬性。 必要。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。 必要。指定 *True* 以使用動態群組。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。 必要。指定 LDAP 動態群組物件類別 (通常爲 dynamicGroup)。
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。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_ICSLOGOUTENABLED=	Access Manager 和 iChain 設定：同時登出已啓用。 指定 *True* 會啓用使用者應用程式與 Novell Access Manager 或 iChain 的同時登出功能。「使用者應用程式」會在登出時檢查是否有 Novell Access Manager 或 iChain 的 Cookie，如果有，就將使用者重新路由至 ICS 登出頁面。 指定 *False*，停用同時登出功能。
NOVL_CONFIG_ICSLOGOUTPAGE=	Access Manager 和 iChain 設定：同時登出頁面。 指定到 Novell Access Manager 或 iChain 登出頁面的 URL，其中 URL 是 Novell Access Manager 或 iChain 所需的主機名稱。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。用於取代佈建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。

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同等參數
NOVL_CONFIG_AUTHCONFIGPATH=	其他：授權組態路徑。 授權組態檔案的完全合法名稱。
NOVL_CONFIG_CREATEDIRECTORYINDEX	其他：建立 eDirectory 索引。 在 NOVL_CONFIG_SERVERDN 中所指定的 eDirectory 伺服器上，如果您希望自動安裝程式在 manager、ismanager 和 srvprvUUID 屬性上建立索引，請指定 true。如果這個參數設爲 true，NOVL_CONFIG_REMOVEEDIRECTORYINDEX 就不能設爲 true。 爲取得最佳效能結果，您應該完成索引的建立。您必須先將索引置於「線上」模式，之後才讓「使用者應用程式」可供使用。
NOVL_CONFIG_REMOVEDIRECTORYINDEX	其他：移除 eDirectory 索引。 如果您希望自動安裝程式移除 NOVL_CONFIG_SERVERDN 中所指定的伺服器上的索引，請指定 true。如果這個參數設爲 true，NOVL_CONFIG_CREATEEDIRECTORYINDEX 就不能是 true。
NOVL_CONFIG_SERVERDN	其他：伺服器 DN。 指定要建立或移除索引的 eDirectory 伺服器。
NOVL_CREATE_DB	指出建立資料庫的方式。選項包括： ◆ now ：立即建立資料庫。 ◆ file ：將 SQL 輸出寫入檔案 ◆ startup ：在應用程式啓動時建立資料庫
NOVL_DATABASE_NEW	指出資料庫是新增的還是現有的。如果是新增的資料庫，請指定「*True*」。如果是現有的資料庫，請指定 *False*。
NOVL_RBPM_SEC_ADMINDN	安全性管理員。 此角色會授予各成員安全性網域內的所有功能。 安全性管理員可以對安全性網域內的所有物件執行所有允許的動作。安全性網域允許安全性管理員爲 Roles Based Provisioning Module 內所有網域的所有物件設定存取許可。安全性管理員可以設定團隊，還可以指定網域管理員、委託管理員及其他安全性管理員。
NOVL_RBPM_RESOURCE_ADMINDN	資源管理員。 此角色會授予各成員資源網域內的所有功能。資源管理員可以對資源網域內的所有物件執行所有允許的動作。

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同等參數
NOVL_RBPM_CONFIG_ADMINDN	此角色會授予各成員組態網域內的所有功能。RBPM 組態管理員可以對組態網域內的所有物件執行所有允許的動作。他可以控制對 Roles Based Provisioning Module 內之導覽項目的存取權限。此外，RBPM 組態管理員還可以設定委託與代理服務、佈建用者介面及工作流程引擎。
RUN_LDAPCONFIG=	指定您要在何時設定 LDAP 設定：現在或以後。值包括： ◆ Now ：將提供的 LDAP 組態設定填入 WAR，立即執行 LDAP 設定 ◆ Later ：只是安裝使用者應用程式檔案，而不設定 LDAP 設定。

8.2.1 靜默安裝模式下在環境中設定密碼

如果不想在 silent.properties 檔案中指定密碼，可以改爲在環境中設定密碼。在這種情況下，靜默安裝程式將從環境中而不是從 silent.properties 檔案讀取密碼。如此可以提高安全性。

需要爲使用者應用程式安裝程式設定以下密碼：

- NOVL_DB_USER_PASSWORD
- NOVL_CONFIG_DBADMIN_PASSWORD
- NOVL_CONFIG_LDAPADMINPASS
- NOVL_CONFIG_KEYSTOREPASSWORD

若要在 Linux 上設定密碼，請使用 export 指令，如下例所示：

```
export NOVL_DB_USER_PASSWORD=myPassWord
```

若要在 Windows 上設定密碼，請使用 set 指令，如下例所示：

```
set NOVL_DB_USER_PASSWORD=myPassWord
```

8.3 以靜默模式或主控台模式執行 JBossPostgreSQL 公用程式

您可在主控台模式或靜默模式下執行 JBossPostgreSQL 公用程式。在以靜默模式執行 JBossPostgreSQL 公用程式之前，您需要編輯該公用程式的內容檔案。編輯好內容檔案之後，請使用以下指令將其啓動：

```
JBossPostgreSQL -i silent -f <path to the properties file>
```

例如：

```
JBossPostgreSQL -i silent -f /home/jdoe/idm-install-files/silent.properties
```

以下爲適用於 JBossPostgreSQL 靜默安裝的內容：

表格 8-2 JBossPostgreSQL 組態內容

內容	描述
USER_INSTALL_DIR	要安裝 JBoss 與 JRE 的路徑。 若正在安裝 JBoss，則必須填寫；否則，請留爲空白。
NOVL_DB_NAME	要使用之資料庫的名稱。預設資料庫名稱爲 idmuserappdb。 若正在安裝 PostgreSQL，則必須填寫。若不是在安裝 PostgreSQL，將會忽略此值。
NOVL_DB_PASSWORD	資料庫根密碼。 若正在安裝 PostgreSQL，則必須填寫。若不是在安裝 PostgreSQL，將會忽略此值。
NOVL_DB_PASSWORD_CONFIRM	確認資料庫根密碼。 若正在安裝 PostgreSQL，則必須填寫。若不是在安裝 PostgreSQL，將會忽略此值。

CHOSEN_INSTALL_FEATURE_LIST	要安裝的安裝集。
	
	必要。可以選擇 JBoss 與 PostgreSQL 這兩個產品，或只安裝其中之一。
	
	範例：
	
	`CHOSEN_INSTALL_FEATURE_LIST=JBoss, PostgreSQL`
	
	`CHOSEN_INSTALL_FEATURE_LIST=JBoss,""`

USER_MAGIC_FOLDER_1	PostgreSQL 安裝目錄的名稱。 若正在安裝 PostgreSQL，則必須填寫。若 CHOSEN_INSTALL_FEATURE_LIST 不包含 PostgreSQL，將會忽略此內容。
START_DB	指出安裝程式是否將在安裝期間啓動資料庫。若要讓安裝程式啓動資料庫，請指定值 Start；否則將此內容留爲空白。 選擇性。

8.3.1 靜默安裝模式下在環境中設定密碼

如果不想在 silent.properties 檔案中指定密碼，可以改爲在環境中設定密碼。在這種情況下，靜默安裝程式將從環境中而不是從 silent.properties 檔案讀取密碼。如此可以提高安全性。

需要爲使用者應用程式安裝程式設定以下密碼：

- NOVL_DB_PASSWORD
- NOVL_DB_USER_PASSWORD

若要在 Linux 上設定密碼，請使用 export 指令，如下例所示：

```
export NOVL_DB_USER_PASSWORD=myPassWord
```

若要在 Windows 上設定密碼，請使用 set 指令，如下例所示：

```
set NOVL_DB_USER_PASSWORD=myPassWord
```

8.4 以靜默模式或主控台模式執行 RIS 安裝程式

本版本隨附了單獨的安裝程式，可用來設定 Rest Information Services (RIS) 功能。此功能可對支援 REST 資源的 RIS.war 檔案進行設定。透過 RIS 公開的 REST 資源可以發出 SOAP 呼叫，以從各 RBPM 系統收集資訊。

您可在主控台模式或靜默模式下執行 RIS 安裝程式。在執行 RIS 安裝程式之前，您需要編輯該安裝程式的內容檔案。編輯好內容檔案之後，請使用以下指令將其啓動：

```
RisUpdateWar -i silent -f <path to the properties file>
```

例如：

```
RisUpdateWar -i silent -f /home/jdoe/idm-install-files/silent.properties
```

該安裝程式需要以下資訊：

- RIS.war 的位置
- 使用者應用程式執行時使用的連接埠
- 爲使用者應用程式定義的網路位置
- 將在其上部署 RIS.war 的主機名稱

以下爲適用於 RIS 安裝的內容：

表格 8-3 *RIS 組態內容*

內容	描述
NOVL_INSTALL_HOST	將在其上部署 RIS.war 的主機名稱。此名稱不能爲 localhost。 必要。
NOVL_USERAPP_PORT	RBPM 使用者應用程式執行時使用的連接埠。 必要。
NOVL_CONTEXT_NAME	使用者應用程式的網路位置名稱。 必要。
RIS_INSTALL_DIRECTORY	RIS.war 所在的目錄。 必要。
RIS_WAR_FILE	RIS.war 檔案的名稱。 請勿變更此值。

內容	描述
RIS_INSTALL_LOG	安裝程式的記錄檔案名稱。可以根據自己的喜好來命名該檔案。安裝程式會將該檔案寫入 RIS_INSTALL_DIR 內容中所指定的位置。 如果將此內容留爲空白，則預設記錄檔案爲 RIS-Install.log。 選擇性。

安裝後任務

9

本章說明安裝後的任務。主題包括：

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。

9.2 設定使用者應用程式

有關設定 「Identity Manager 使用者應用程式和角色子系統」的安裝後說明，請參閱下列各項：

- *《Novell IDM Roles Based Provisioning Module 管理指南》*中的 「設定使用者應用程式環境」一節。
- *《Novell IDM Roles Based Provisioning Module 設計指南》*

9.2.1 設定記錄

若要設定記錄，請按照 《使用者應用程式：管理指南》(http://www.novell.com/documentation/idm40/index.html) 之 「設定記錄」一節中的指示執行。

9.3 設定 eDirectory

9.3.1 在 eDirectory 中建立索引

爲了提高使用者應用程式的效能，eDirectory 管理員應該爲 manager、ismanager 和 srvprvUUID 屬性建立索引。如果沒有建立這些屬性的索引，使用者應用程式使用者將會感到其效能不佳，在叢集環境中更是如此。

如果在「使用者應用程式組態面板」的「*進階設定*」索引標籤上選取「*建立 eDirectory 索引*」(如表格 A-2 (第 143 頁) 中所述)，安裝期間可以自動建立這些索引。如需使用索引管理員建立索引的指示，請參閱 《*Novell eDirectory 管理指南*》(http://www.novell.com/documentation)。

9.3.2 安裝和設定 SAML 驗證方法

只有在您想要使用 SAML 驗證方法且不使用 Access Manager 時，才需要進行這項設定。如果您使用 Access Manager，則您的 eDirectory 樹狀結構已包含這個方法。程序包括：

- ❑ 在 eDirectory 樹狀結構中安裝「SAML 方法」。
- ❑ 使用 iManager 來編輯 eDirectory 屬性。

在 eDirectory 樹狀結構中安裝 SAML 方法

1. 找到 nmassaml.zip 檔案並解壓縮。
2. 將 SAML 方法安裝至 eDirectory 樹狀結構中。
   - **2a** 擴充 authsaml.sch 中儲存的綱要

     下列範例顯示如何在 Linux 上執行這項動作：

     ```
     ndssch -h <edir_ip> <edir_admin> authsaml.sch
     ```
   - **2b** 安裝 SAML 方法。

     下列範例顯示如何在 Linux 上執行這項動作：

     ```
     nmasinst   -addmethod <edir_admin> <tree> ./config.txt
     ```

編輯 eDirectory 屬性

1. 開啓 iManager，然後移至「*角色和任務*」>「*目錄管理*」>「*建立物件*」。
2. 選取「*顯示所有物件類別*」。
3. 建立 authsamlAffiliate 類別的新物件。
4. 選取 authsamlAffiliate，然後按一下「*確定*」。(您可以使用任何有效的名稱來命名這個物件。)
5. 若要指定「網路位置」，請在樹狀結構中選取 *SAML Assertion.Authorized Login Methods.Security* 容器物件，然後按一下「*確定*」。

6 您必須新增類別物件 authsamlAffiliate 的屬性。

6a 移至 iManager 的「*檢視物件*」>「*瀏覽*」索引標籤，在 SAML Assertion.Authorized Login Methods.Security 容器中找出您的新分支物件。

6b 選取新的分支物件，然後選取「*修改物件*」。

6c 將 *authsamlProviderID* 屬性新增至新的分支物件。這個屬性用來比對判斷提示與其分支。這個屬性的內容必須完全符合 SMAL 判斷提示所傳送的 Issuer 屬性。

6d 按一下「*確定*」。

6e 將 *authsamlValidBefore* 和 *authsamlValidAfter* 屬性新增至分支物件。當判斷提示有效時，這些屬性會定義判斷提示中接近 *IssueInstant* 的時間長短，以秒爲單位。一般預設值爲 180 秒。

6f 按一下「*確定*」。

7 選取 Security 容器，然後選取「*建立物件*」，在您的 Security 容器中建立「*託管根部容器*」。

8 在「託管根部容器」中建立「*託管根部*」物件。

8a 返回「*角色和任務*」>「*目錄管理*」，然後選取「*建立物件*」。

8b 再次選取「*顯示所有物件類別*」。

8c 爲您的分支用來簽署判斷提示的證書，建立「*託管根部*」物件。您必須有證書的 DER 編碼副本才能這樣做。

8d 爲簽署證書鏈至根 CA 證書中的每一個證書，建立新的託管根部物件。

8e 將網路位置設爲稍早所建立的「託管根部容器」，然後按一下「*確定*」。

9 返回「物件檢視器」。

10 將 *authsamlTrustedCertDN* 屬性新增到隸屬的物件，然後按一下「*確定*」。

這個屬性應該指向您在上一步建立的簽署證書的「託管根部物件」(分支的所有判斷提示必須由這個屬性所指的證書來簽署，否則會被拒絕)。

11 將 *authsamlCertContainerDN* 屬性新增到隸屬的物件，然後按一下「*確定*」。

這個屬性應該指向您先前建立的「託管根部容器」。(這個屬性用來驗證簽署證書的證書鏈。)

9.4 安裝後重新設定使用者應用程式 WAR 檔案

若要更新您的 WAR 檔案，您可以執行 configupdate 公用程式，如下所示：

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 公用程式參數的相關資訊，請參閱第 A.1 節「使用者應用程式組態：基本參數」(第 141 頁) 或表格 8-1 (第 122 頁)。

2 將新的 WAR 檔案部署到您的應用程式伺服器上。

若爲 WebLogic 和 WebSphere，將 WAR 檔案重新部署至應用程式伺服器。若爲 JBoss 單一伺服器，將變更套用至已部署的 WAR。如果您在 JBoss 叢集中執行，則需要在叢集的每一個 JBoss 伺服器中更新 WAR 檔案。

9.5 設定外部忘記密碼管理

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。

9.5.1 指定外部忘記密碼管理 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. 爲「*忘記密碼連結*」組態參數指定外部密碼 WAR 的位置。

   請將主機和連接埠包含於其中，例如 http://localhost:8180/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsp。外部密碼 WAR 可以位於保護「使用者應用程式」的防火牆之外。
4. 爲「*忘記密碼回傳連結*」指定在使用者執行完忘記密碼程序後顯示的連結。使用者按一下此連結會重新導向到指定的連結。
5. 爲「*忘記密碼 Web 服務 URL*」提供外部忘記密碼 WAR 用以回撥到使用者應用程式的 Web 服務 URL。URL 必須採用以下格式：https://<*idmhost*>:<*sslport*>/<*idm*>/pwdmgt/service。

   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 9.5.4 節「設定 JBoss 伺服器之間的 SSL 通訊」(第 137 頁)。
6. 手動將 ExternalPwd.war 複製到執行外部密碼 WAR 功能的遠端 JBoss 伺服器部署目錄。

9.5.2 指定內部密碼 WAR

1. 在「使用者應用程式」組態參數中，不選中「*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。

9.5.3 測試外部忘記密碼 WAR 組態

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，則可以在下列位置存取：

- 直接在瀏覽器中存取。前往外部密碼 WAR 中的「忘記密碼」頁面，例如 http://localhost:8180/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsp。
- 在「使用者應用程式」登入頁面中，按一下「*忘記密碼*」連結。

9.5.4 設定 JBoss 伺服器之間的 SSL 通訊

如果您在安裝期間選取了使用者應用程式組態檔案中的「*使用外部密碼 WAR*」，則必須在部署使用者應用程式 WAR 和外部忘記密碼管理 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。

9.6 更新忘記密碼設定

您可以在安裝完成後變更「*忘記密碼連結*」、「*忘記密碼回傳連結*」和「*忘記密碼 Web 服務 URL*」的值。使用 configupdate 公用程式或使用者應用程式。

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。

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*」。修改下列欄位：

- *忘記密碼連結* (例如：http://localhost:8180/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsp)
- *忘記密碼回傳連結* (例如：http://localhost/IDMProv)
- *忘記密碼 Web 服務 URL* (例如：https://<*idmhost*>:<*sslport*>/<*idm*>/pwdmgt/service)

9.7 安全性考量

安裝過程中，安裝程式會將記錄檔案寫入安裝目錄。這些檔案包含組態的相關資訊。一旦完成對環境的設定，便應刪除這些記錄檔案或將其儲存在安全的位置。

安裝過程中，您可以選擇將資料庫綱要寫入檔案。由於此檔案包含資料庫的描述資訊，因此在安裝完成後應將其移動到安全的位置。

9.8 增加 Identity Manager Java 堆積大小

在企業環境中，角色與資源服務驅動程式需要的最大 Java 堆積要比 Identity Manager 中定義的預設量多。建議將最大 Java 堆積大小設定爲 256MB，以免出現 OutOfMemoryError 情況。

可以在 iManager 之「驅動程式集」內容的「其他」區段下指定 Java 堆積大小，也可以透過設定 DHOST_JVM_INITIAL_HEAP 與 DHOST_JVM_MAX_HEAP 環境變數來指定。請參閱《Identity Manager Common Driver Administration Guide》(Identity Manager 常用驅動程式管理指南) (http://www.novell.com/documentation/idm40/idm_common_driver/index.html?page=/documentation/idm40/idm_common_driver/data/front.html)，以取得有關設定 Java VM 選項的詳細資訊。

9.9 疑難排解

您的 Novell 代表會和您一起解決任何安裝與組態方面的問題。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。

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 使用者身份、使用者群組
◆ Access Manager 或 iChain 設定
	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 8180 已在使用中」。	關閉任何可能已在執行的 Tomcat 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，以使用 8180 以外的連接埠，請記得編輯使用者應用程式驅動程式的 config 設定。
當應用程式伺服器啓動時，您看到一則訊息，指出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。
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)。

問題	建議的動作

電子郵件通知沒有傳送。	執行 configupdate 公用程式檢查您是否已提供下列「使用者應用程式」組態參數的值：E-Mail From 和 E-Mail Host。
	
	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 c:\opt\novell\idm) 執行下列指令：
	
	`configupdate.bat`

使用者應用程式組態參考

A

本章說明在「使用者應用程式」安裝或組態更新期間提供值的選項。

A.1 使用者應用程式組態：基本參數

圖 A-1 *使用者應用程式組態基本選項*

表格 A-1 *使用者應用程式組態的基本選項*

設定類型	選項	描述
Identity Vault 設定	*Identity Vault 伺服器*	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`
	Identity Vault 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。 只要您沒有在「使用者應用程式」的「管理」索引標籤中修改過這項設定，就可以使用 configupdate 公用程式來修改這項設定。
	Identity Vault 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。 只要您沒有在「使用者應用程式」的「管理」索引標籤中修改過這項設定，就可以使用 configupdate 公用程式來修改這項設定。
Identity Vault 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。
	使用者應用程式驅動程式 DN	必要。「使用者應用程式管理員」的可辨識名稱。例如，您的驅動程式爲 UserApplicationDriver，驅動程式集名爲 myDriverSet，並且該驅動程式集位於網路位置 o=myCompany，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*」索引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，則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 *《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，必須使用「使用者應用程式」中的 *「管理」* > *「安全性」*頁面。 如果您已啓動代管「使用者應用程式」的應用程式伺服器，則無法透過 configupdate 來變更這項設定。
	RBPM 網路位置名稱	顯示目前的網路位置名稱。
	RBPM 報告管理	指向報告管理員。安裝程式預設會將此值設定爲與其他安全性欄位中相同的使用者。

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。

A.2 使用者應用程式組態：所有參數

這個表格包含您按一下「*顯示進階設定選項*」時可用的組態參數。

表格 A-2 *使用者應用程式組態：所有選項*

設定類型	選項	描述
Identity Vault 設定	*Identity Vault 伺服器*	必要。指定 LDAP 伺服器的主機名稱或 IP 位址。例如： myLDAPhost
	LDAP 連接埠	指定 LDAP 伺服器的非安全連接埠。例如：389。
	安全 LDAP 連接埠	指定 LDAP 伺服器的安全連接埠。例如：636。
	Identity Vault 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。
	Identity Vault 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。
	安全管理員連接	選取這個選項來要求，必須以安全插槽進行所有使用管理員帳戶的通訊。(此選項可能會對效能產生負面影響)。此設定允許不透過 SSL 來執行不需要 SSL 的其他操作。
	安全使用者連線	選取這個選項來要求，必須以安全插槽進行所有使用登入之使用者帳戶來執行的通訊。(此選項可能會對效能產生負面影響)。此設定允許不透過 SSL 來執行不需要 SSL 的其他操作。

設定類型	選項	描述
Identity Vault 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。
	使用者應用程式驅動程式 DN	必要。「使用者應用程式管理員」的可辨識名稱。例如，您的驅動程式爲 UserApplicationDriver，驅動程式集名爲 myDriverSet，並且該驅動程式集位於網路位置 o=myCompany，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*」索引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，則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。如需詳細資料，請參閱 *《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，必須使用「使用者應用程式」中的 *「管理」* > *「安全性」*頁面。 如果您已啓動代管「使用者應用程式」的應用程式伺服器，則無法透過 configupdate 來變更這項設定。
	佈建管理員	佈建管理員可以管理使用者應用程式中提供的佈建工作流程功能。只有 Identity Vault 中存在的使用者才能指定爲佈建管理員。 若要在部署使用者應用程式之後變更此指定，請使用使用者應用程式中的 *「管理」* > *「管理員指定」*頁面。
	法規遵循管理員	法規遵循管理員是一個系統角色，允許成員執行「*法規遵循*」索引標籤上的所有功能。只有 Identity Vault 中存在的使用者才能指定爲法規遵循模組管理員。 在 configupdate 期間，只有在您還未指定有效的法規遵循管理員時，對這個值的變更才會生效。如果已存在有效的法規遵循管理員，則不會儲存所做的變更。 若要在部署使用者應用程式之後變更此指定，請使用使用者應用程式中的 *「管理」* > *「管理員指定」*頁面。
	角色管理員	此角色允許成員建立、移除或修改所有角色，授予或撤銷對任何使用者、群組或容器所做的任何角色指定。它還允許其角色成員爲任一使用者執行報告。依預設，「使用者應用程式」管理員會指定爲此角色。 若要在部署使用者應用程式之後變更此指定，請使用使用者應用程式中的 *「管理」* > *「管理員指定」*頁面。 在 configupdate 期間，只有在您還未指定有效的「角色管理員」時，對這個值的變更才會生效。如果有效的「角色管理員」已存在，則不會儲存您所做的變更。

設定類型	選項	描述
	安全性管理員	此角色會授予各成員安全性網域內的所有功能。 安全性管理員可以對安全性網域內的所有物件執行所有允許的動作。安全性網域允許安全性管理員爲 Roles Based Provisioning Module 內所有網域的所有物件設定存取許可。安全性管理員可以設定團隊，還可以指定網域管理員、委託管理員及其他安全性管理員。 若要在部署使用者應用程式之後變更此指定，請使用使用者應用程式中的 *「管理」* > *「管理員指定」*頁面。
	資源管理員	此角色會授予各成員資源網域內的所有功能。資源管理員可以對資源網域內的所有物件執行所有允許的動作。 若要在部署使用者應用程式之後變更此指定，請使用使用者應用程式中的 *「管理」* > *「管理員指定」*頁面。
	RBPM 組態管理員	此角色會授予各成員組態網域內的所有功能。RBPM 組態管理員可以對組態網域內的所有物件執行所有允許的動作。他可以控制對 Roles Based Provisioning Module 內之導覽項目的存取權限。此外，RBPM 組態管理員還可以設定委託與代理服務、佈建用者介面及工作流程引擎。 若要在部署使用者應用程式之後變更此指定，請使用使用者應用程式中的 *「管理」* > *「管理員指定」*頁面。
	RBPM 報告管理	指向報告管理員。安裝程式預設會將此值設定爲與其他安全性欄位中相同的使用者。
	重新啓始化 RBPM 安全性	允許您重設安全性的核取方塊。
	IDMReport URL	指向 Identity Reporting 模組使用者介面的 URL。
Identity Vault 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。 此容器中 (和下方) 的使用者可以登入「使用者應用程式」。 如果您已啓動代管「使用者應用程式」的應用程式伺服器，則無法透過 configupdate 來變更這項設定。 **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。
	使用者容器範圍	這會定義使用者的搜尋範圍。
	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。

設定類型	選項	描述
Identity Vault 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。 如果您已啓動代管「使用者應用程式」的應用程式伺服器，則無法透過 configupdate 來變更這項設定。
	群組容器範圍	這會定義群組的搜尋範圍。
	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)。
Identity Vault 證書	*KeyStore 路徑*	必要。指定應用程式伺服器用來執行的 JRE 之 keystore (cacerts) 檔案的完整路徑，或者，按一下瀏覽器小按鈕導覽至 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。 **WebSphere 注意事項。**Keystore 路徑欄位需要設定爲 RBPM 的安裝目錄，而不是 JBoss 安裝中 JDK cacerts 檔案的位置。預設值會設定爲正確的位置。
	KeyStore 密碼	必要。指定 cacerts 密碼。預設值爲「changeit」。
	確認 KeyStore 密碼	
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。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。
	Keystore 類型 JKS	指出您要使用之數位簽名的類型。如果核取此欄位，即表示託管儲存區路徑的類型爲 JKS。
	Keystore 類型 PKCS12	指出您要使用之數位簽名的類型。如果核取此欄位，即表示託管儲存區路徑的類型爲 PKCS12。
Novell Audit 數位簽名與證書金鑰		包含稽核服務的數位簽名金鑰與證書。
	Novell Audit 數位簽名證書	顯示稽核服務的數位簽名證書。
	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。

設定類型	選項	描述
Access Manager 設定	*啓用同時登出*	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 Novell Access Manager 或 iChain。「使用者應用程式」會在登出時檢查是否有 Novell Access Manager 或 iChain 的 Cookie，如果有，就將使用者重新路由至 ICS 登出頁面。
	同時登出頁面	到 Novell Access Manager 或 iChain 登出頁面的 URL，其中 URL 是 Novell Access Manager 或 iChain 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。
電子郵件伺服器組態	*通知樣板主機*	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 是佈建申請任務和核准通知的連結。
	通知樣板連接埠	用於取代佈建申請任務和核准通知中所使用之電子郵件樣板中的 $PORT$ 記號。
	通知樣板安全連接埠	用於取代佈建申請任務和核准通知中所使用之電子郵件樣板中的 $SECURE_PORT$ 記號。
	通知樣板通訊協定	指的是非安全通訊協定 HTTP。用於取代佈建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。
	通知樣板安全通訊協定	指的是安全通訊協定 HTTPS。用於取代佈建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	指定來自佈建電子郵件中使用者的電子郵件。
	SMTP 伺服器名稱	指定佈建電子郵件所使用的 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」。 如果選取「*使用外部密碼 WAR*」，則必須提供「*忘記密碼連結*」、「*忘記密碼回傳連結*」和「*忘記密碼 Web 服務 URL*」的值。 如果不選取「*使用外部密碼 WAR*」，Identity Manager 就會使用預設的內部「密碼管理」功能 ./jsps/pwdmgt/ForgotPassword.jsp (開頭不加 http(s) 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。在外部或內部密碼管理 WAR 中指定 ForgotPassword.jsp 檔案。
	忘記密碼回傳連結	指定「*忘記密碼回傳連結*」以便使用者在執行忘記密碼操作後使用。

設定類型	選項	描述
	忘記密碼 Web 服務 URL	外部忘記密碼 WAR 將使用此 URL 回撥到使用者應用程式以執行重要的忘記密碼功能。此 URL 的格式爲： `https://<idmhost>:<sslport>/<idm>/pwdmgt/service`
其他	*工作階段逾時*	應用程式工作階段逾時。
	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 Identity Vault 索引	如果您希望安裝公用程式在 manager、ismanager 和 srvprvUUID 屬性上建立索引，請選取這個核取方塊。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。在安裝「使用者應用程式」之後，您可以使用 iManager 來手動建立這些索引。請參閱第 9.3.1 節「在 eDirectory 中建立索引」(第 134 頁)。 爲取得最佳效能，您應該完成索引的建立。您必須先將索引置於「線上」模式，之後才讓「使用者應用程式」可供使用。
	移除 Identity Vault 索引	移除 manager、ismanager 和 srvprvUUID 屬性上的索引。
	伺服器 DN	選取要建立或移除索引的 eDirectory 伺服器。 **附註：**若要在多個 eDirectory 伺服器上設定索引，您必須執行許多次 configupdate 公用程式。您一次只能指定一個伺服器。
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 中指定可做爲容器的物件類別的 LDAP 名稱。
	新增新容器物件：容器屬性名稱	提供容器物件的屬性名稱。