Novell
Novell Identity Manager Roles Based Provisioning Module

3.6

www.novell.com

使用者應用程式：安裝指南

2008 年 1 月 18 日

Novell®

法律聲明

Novell, Inc. 不對本文件的內容或使用做任何陳述或保證，且特別聲明不對任何特定用途的適銷性或適用性提供任何明示或隱喻的保證。此外，Novell, Inc. 有權隨時修訂本說明文件或更改內容，而無義務向個人或團體告知這類修訂或變更。

此外，Novell, Inc. 對軟體不做任何表示或保證，對本產品在任何特定用途的商品可銷性與適用性方面，亦不做任何明示或默示保證。Novell, Inc. 亦保留在任何時候變更部份或全部 Novell 軟體的權利，而無義務向個人或團體告知這類變更。

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、轉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。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。

對於本文件中所述及之所有產品內附技術，Novell, Inc. 皆具有其智慧財產權。特別是 (但不限於) 這些智慧財產權可能包含 Novell 法律專利網頁 (http://www.novell.com/company/legal/patents/) 中所列的一或多項美國專利，以及在美國與其他國家 / 地區的一或多項其他專利或申請中的專利。

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

*線上文件：*如需存取 Novell 此產品與其他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

Novell® Identity Manager Roles Based Provisioning Module 3.6 包含支援角色提供的「Identity Manager 使用者應用程式」。本指南說明如何安裝 Novell Identity Manager Roles Based Provisioning Module 3.6。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 角色提供模組」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 角色提供模組」的其他文件，請造訪 Identity Manager 文件網站 (http://www.novell.com/documentation/lg/dirxmldrivers/index.html)。

文件慣例

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

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

雖然在寫入單一路徑名稱時，有些平台採用反斜線，其他平台採用正斜線，但在本文中，路徑名稱一律使用反斜線。使用者的平台如果要求使用正斜線 (例如 Linux* 或 UNIX*)，應依據軟體的要求使用正斜線。

綜覽

1

本章節將對安裝進行概述並說明系統要求。主題包括：

- 「安裝綜覽」(第 9 頁)
- 「關於安裝程式」(第 10 頁)
- 「系統需求」(第 10 頁)

1.1 安裝綜覽

Novell® Identity Manager Roles Based Provisioning Module 3.6 的安裝程序會安裝支援角色的「使用者應用程式」以及「角色提供模組」。安裝步驟如下所示：

1. 若要移轉至「Identity Manager 角色提供模組」，請參閱 *《Identity Manager 使用者應用程式：移轉指南》*(http://www.novell.com/documentation/idmrbpm36/pdfdoc/migration/migration.pdf)。
2. 請確認您符合系統需求。請參閱 「系統需求」(第 10 頁)。
3. 安裝 Identity Manager Metadirectory。如需說明，請參閱 *《Identity Manager 3.5.1 安裝指南》*(http://www.novell.com/documentation/idm35/pdfdoc/install/install.pdf)。必須先安裝 Identity Manager Metadirectory 伺服器，才能建立必需的驅動程式以及安裝「使用者應用程式」和「角色提供模組」。
4. 滿足安裝的必要條件。請參閱第 2 章 「安裝的先決條件」(第 17 頁)。
5. 尋找位於下載目錄中的 prerequisitefiles.zip 檔案，並將其解壓縮。手動安裝或套用已解除壓縮的檔案。
6. 如果您將使用 Designer 建立和設定驅動程式，請安裝 Designer 2.1.1。請參閱「安裝 Designer」(http://www.novell.com/documentation/designer21/admin_guide/index.html?page=/documentation/designer21/admin_guide/data/gsinstall.html)。
7. 在 iManager 或 Designer 2.1.1 中建立「使用者應用程式」驅動程式。「在 iManager 中建立使用者應用程式驅動程式」(第 29 頁) 中提供了有關在 iManager 中建立驅動程式的說明。

   在安裝「Novell Identity Manager 使用者應用程式」和「角色提供模組」之前，「使用者應用程式」驅動程式必須已經存在 (但不能開啓)。
8. 在 iManager 或 Designer 2.1.1 中建立「角色服務」驅動程式。「在 iManager 中建立角色服務驅動程式」(第 33 頁) 中提供了有關在 iManager 中建立驅動程式的說明。

   在安裝「Novell Identity Manager 使用者應用程式」和「角色提供模組」之前，「角色服務」驅動程式必須已經存在 (但不能開啓)。
9. 安裝並設定「Novell Identity Manager 使用者應用程式」和「角色提供模組」。請參閱：
   - 第 4 章 「在 JBoss 上使用 GUI 進行安裝」(第 35 頁)
   - 第 5 章 「透過主控台或使用單個指令進行安裝」(第 61 頁)
   - 第 6 章 「在 WebSphere 應用程式伺服器上進行安裝」(第 69 頁)

   附註：如果您使用的是 WebSphere*，就必須手動部署 WAR 檔案。

10 執行安裝後的任務。

1.2 關於安裝程式

「使用者應用程式」的安裝程式會：

- 指定現有的應用程式伺服器版本，以供使用。
- 指定要使用的現有資料庫版本，例如 MySQL*、Oracle*、DB2* 或 Microsoft* SQL Server*。資料庫可存放「使用者應用程式」資料和「使用者應用程式」組態資訊。
- 設定 JDK 的證書檔案組態，以便「使用者應用程式」(在應用程式伺服器上執行) 可以安全地與 Identity Vault 和「使用者應用程式」驅動程式通訊。
- 設定「Novell Identity Manager 使用者應用程式」的 Java* Web Application Archive (WAR) 檔案，並將其部署至「應用程式伺服器」。在 WebSphere 上，您必須手動部署 WAR。
- 依您的意願啓用 Novell Audit 記錄。
- 讓您輸入現有的萬能金鑰來還原特定的「角色提供模組」安裝，還可讓您支援叢集。

您可以使用下列三種模式來啓動安裝程式：

- 圖形使用者介面。請參閱第 4 章「在 JBoss 上使用 GUI 進行安裝」(第 35 頁) 或第 6 章「在 WebSphere 應用程式伺服器上進行安裝」(第 69 頁)。
- 主控台 (指令行) 介面。請參閱 「透過主控台安裝使用者應用程式」(第 61 頁)。
- 無訊息安裝。請參閱 「使用單一指令安裝使用者應用程式」(第 61 頁)。

1.3 系統需求

若要使用 Novell Identity Manager Roles Based Provisioning Module 3.6，必須擁有 表格 1-1 中列出的其中一個必需組件。

表格 1-1 系統需求

必需的系統組件	系統需求	註
Metadirectory 系統 (Identity Manager 3.5 或 3.5.1) ◆ Metadirectory 引擎 ◆ Novell Audit 代辦 ◆ 服務驅動程式 ◆ Identity Manager 驅動程式 ◆ 公用程式 (包含「應用程式工具」和「Novell Audit 設定」工具)	下列其中一個作業系統： ◆ Netware® 6.5 SP6 ◆ 含最新支援套件 1.0 的 Novell Open Enterprise Server (OES) ◆ Novell Open Enterprise Server (OES 2.0 ◆ 含最新支援套件 的 Windows* 2000 Server (32 位元) ◆ 含最新 Service Pack 的 Windows Server 2003 (32 位元) ◆ Linux Red Hat 3.0、4.0 或 5.0 ES 和 AS (可同時支援 32 位元和 64 位元) ◆ 含最新支援套件的 Suse Linux Enterprise Server 9 和 10 (可同時支援 32 位元和 64 位元) ◆ Solaris* 9 或 10 ◆ AIX* 5.2L、5.2 或 5.3 版 下列其中一個 eDirectory™ 版本： ◆ eDirectory 8.7.3.10 ◆ eDirectory 8.8.1 或 8.8.2 Security Services 2.0.5 (NMAS™ 3.1.3)	如果您使用的是 Metadirectory 系統平台，則支援在實作中使用 VMware*。 本版本中所有的 Identity Manager 軟體元件均爲 32 位元，即使它們在 64 位元處理器或 64 位元作業系統上執行。除非另有指定，否則 OES、NetWare、Windows 和 Linux 平台 (Red Hat* 和 SUSE®) 都支援下列所有 32 位元模式的處理器： ◆ Intel* x86-32 ◆ AMD* x86-32 ◆ Intel EM64T ◆ AMD Athlon64* 與 Opteron* Identity Manager 可支援下列的 eDirectory 8.8 功能： ◆ 相同伺服器上的多個 eDirectory 例項 ◆ 加密屬性 eDirectory 8.8 可支援 64 位元的 Red Hat Linux 4.0。 Windows Server 2003 的 64 位元版的「密碼同步化」可供使用。 請確定在安裝 eDirectory 8.8 之前已完整備份 eDirectory 資料庫。eDirectory 8.8 會升級資料庫結構部份，而且升級之後不允許再復原該資料庫結構。 現在，當 Xen Virtual Machine (VM) 做爲平行虛擬化模式中的訪客作業系統而在 SLES 10 中執行時，Xen 虛擬化可獲得 SUSE Linux Enterprise Server 10 的支援。需要適用於 SLES 10 的 Xen 修補程式 (請參閱 TID # 3915180 (http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3915180&sliceId=SAL_Public&dialogID=52670386&stateId=1%200%204926187))。

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

必需的系統組件	系統需求	註
安全記錄服務 ◆ 安全記錄伺服器 ◆ 平台代辦 (用戶端元件) ◆ Novell Audit 2.0.2 或 Sentinel™ 5.1.3	針對「安全記錄伺服器」，爲下列其中一個作業系統： ◆ 含最新支援套件的 Novell Open Enterprise Server (OES) 1.0 或 2.0 ◆ 含最新支援套件的 eDirectory 6.5 ◆ 含最新 Service Pack 的 Windows 2000 Server (32 位元) ◆ 含最新 Service Pack 的 Windows Server 2003 (32 位元) ◆ Linux Red Hat Linux 3.0、4.0 或 5.0 ES 或 AS (32 位元或 64 位元，但 Novell Audit 只能在 32 位元模式中執行) ◆ 含最新支援套件的 Solaris 10 10 ◆ 含最新支援套件的 SUSE Linux Enterprise Server 9 或 10 (32 位元和 64 位元，但 Novell Audit 只能在 32 位元模式中執行) ◆ Novell eDirectory 8.7.3.6 或 8.8，含最新支援套件 (必須在安全記錄伺服器上安裝) 針對「平台代辦」，爲下列其中一個作業系統： ◆ 含最新支援套件的 Novell Open Enterprise Server (OES) 1.1 SP1 ◆ 含最新支援套件的 eDirectory 6.5 ◆ Windows 2000 或 2000 Server、XP 或含最新 Service Pack 的 Windows Server 2003 (32 位元) ◆ Red Hat Linux 3 或 4 AS 或 ES (32 位元或 64 位元，但 Novell Audit 只能在 32 位元模式中執行) ◆ Solaris 8、9 或 10 ◆ SUSE Linux Enterprise Server 9 或 10 (32 位元和 64 位元，但 Novell Audit 只能在 32 位元模式中執行) iManager 2.6 或 2.7，含最新支援套件和外掛程式	OES、NetWare、Windows 和 Linux 平台 (Red Hat 和 SUSE) 支援下列所有 32 位元模式的處理器： ◆ Intel x86 ◆ AMD x86 ◆ Intel EM64T ◆ AMD Athlon64 和 Opteron 最低「安全伺服器」要求包括： ◆ 採用單一處理器的 Pentium II 400 MHz 伺服器等級 PC ◆ 至少 40 MB 磁碟空間 ◆ 512 MB RAM 允許記錄 eDirectory 事件的 eDirectory Instrumentation 支援下列 eDirectory 版本： ◆ eDirectory 8.7.3 (NetWare、Windows、Linux 和 Solaris) ◆ 含最新支援套件的 eDirectory 8.8 允許記錄 NetWare 事件的 NetWare Instrumentation 支援下列 NetWare 版本： ◆ 含最新支援套件的 eDirectory 5.1 ◆ 含最新支援套件的 eDirectory 6.0 ◆ NetWare 6.5 或含最新支援套件的 NetWare 6.5 ◆ 含最新支援套件的 Novell Open Enterprise Server (OES)

必需的系統組件	系統需求	註
使用者應用程式應用程式伺服器	「使用者應用程式」在 JBoss* 和 WebSphere 上執行，如下所述。 以下平台支援 JBoss 4.0.5 GA： ◆ Novell Open Enterprise Server (OES) 1.0 SP2 或最新支援套件 -- 僅適用於 Linux ◆ SUSE Linux Enterprise Server 9 SP2 (內含於 OES 1.0 SP2 中) 或 10.1.x (64 位元 JVM*) ◆ Windows 2000 Server (含 SP4)(32 位元) ◆ Windows 2003 Server (含 SP1)(32 位元) ◆ Solaris 10 支援套件，日期 6/06 以下平台支援 WebSphere 6.1： ◆ Solaris 10 (64 位元) ◆ Windows 2003 SP1 「使用者應用程式」需要 JRE* 1.5.0_14。	SUSE Linux Enterprise Server 的 32 位元模式可支援下列處理器： ◆ Intel x86 ◆ AMD x86 ◆ Intel EM64T ◆ AMD Athlon64 和 Opteron SUSE Linux Enterprise Server 將在下列處理器上以 64 位元模式執行： ◆ Intel EM64T ◆ AMD Athlon64 ◆ AMD Opteron ◆ Sun* SPARC* 現在，當 Xen Virtual Machine (VM) 做爲平行虛擬化模式中的訪客作業系統執行 SLES 10 時，Xen* 虛擬化可獲得 SUSE Linux Enterprise Server 10 的支援。需要適用於 SLES 10 的 Xen 修補程式 (請參閱 TID # (http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3915180&sliceId=SAL_Public&dialogID=52670386&stateId=1%200%204926187))。
使用者應用程式瀏覽器	使用者應用程式支援 Firefox 和 Internet Explorer，如下所示。 以下平台支援 Firefox 2： ◆ Windows 2000 Professional SP4 ◆ 含 SP2 的 Windows XP ◆ Red Hat Enterprise Linux 4.0 ◆ Novell Linux Desktop 9 ◆ SUSE Linux 10.1 ◆ SUSE Linux Enterprise Desktop 10 SP 以下平台支援 Internet Explorer 7： ◆ Windows 2000 Professional SP4 ◆ 含 SP2 的 Windows XP ◆ Windows Vista Enterprise 6 版 以下平台支援 Internet Explorer 6 SP1： ◆ Windows 2000 Professional SP4 ◆ 含 SP2 的 Windows XP	

必需的系統組件	系統需求	註
使用者應用程式的資料庫伺服器 ◆ MySQL ◆ Oracle ◆ MS SQL ◆ DB2	可使用 JBoss 支援以下資料庫： ◆ MySQL 5.0.27 版 ◆ Oracle 9i (9.2.0.1.4) ◆ Oracle 10g 2 版 (10.2.0.1.0) ◆ MS SQL 2005 SP1 可使用 WebSphere 支援以下資料庫： ◆ Oracle 10g 2 版 (10.2.0) ◆ MS SQL 2005 SP1 ◆ DB2 DV2 v9.1.0.0	「使用者應用程式」會使用資料庫執行各種任務，例如，儲存組態資料，以及爲任何進行中的工作流程活動儲存資料。 安全記錄服務和「使用者應用程式」與工作流程提供都需要資料庫。您可以設定一個資料庫用於兩個應用程式，或針對每個應用程式設定獨立的資料庫。安全記錄服務不包括特定的資料庫。 可同時使用精簡電腦驅動程式和 OCI 用戶端驅動程式支援 Oracle。
工作站 ◆ 適用於 Identity Manager 3.5.1 的 Designer 2.1.1 ◆ iManager Web 存取	已經在下列平台上測試 Designer： Windows： ◆ 含最新 Service Pack 的 Windows 2000 Professional ◆ Windows XP SP2 ◆ Microsoft Windows Vista Linux： ◆ SUSE Linux Enterprise Server 10 (僅適用於 Designer) ◆ SUSE Linux 10.1 ◆ SUSE Linux Enterprise Desktop 10 SP ◆ Red Hat Enterprise LinuxWS 4.0 (僅適用於 Designer)，Gnome* 預設值 ◆ Red Hat Fedora Core 5 (僅適用於 Designer)，Gnome 預設值 ◆ Novell Linux Desktop 9，KDE 預設值	Designer 使用 Eclipse 做爲其開發平台如需平台特定的資訊，請參閱 Eclipse 網站 (http://www.eclipse.org)。 Designer 的最低和建議硬體要求： ◆ 最低 1 GHz，建議 2 GHz 或更高速處理器 ◆ 最低 512MB 的 RAM，建議爲 1 GB 或更多記憶體 ◆ 最低解析度爲 1024 x 768，建議爲 1280 x 1024 先決條件軟體： ◆ Microsoft Internet Explorer 6.0 SP1 ◆ Microsoft Internet Explorer 7 ◆ 或 Mozilla* Firefox 2.0

必需的系統組件	系統需求	註
已連接的系統伺服器 (執行「遠端載入器」之個別伺服器上的主機) ◆ 遠端載入器 ◆ 「遠端載入器」組態工具 (僅限 Windows) ◆ Novell Audit 代辦 ◆ 密碼同步化代理程式 ◆ 已連接系統的驅動程式 Shim ◆ 已連接系統的工具	每個驅動程式都需要已連接的系統可以使用，並且已提供相關的應用程式介面 (API)。 如需每個系統特定的作業系統和已連接系統要求，請參閱 Identity Manager 驅動程式文件 (http://www.novell.com/documentation/idm35drivers)。	每個已連接的應用程式都需要個人具有應用程式特定的知識和職責。 遠端載入器系統： ◆ 含最新支援套件的 Windows NT* 4.0、Windows 2000 Server 或 Windows Server 2003 ◆ 含最新支援套件的 Windows Server* 2003 (64 位元) ◆ Windows Server 2003 (64 位元) 支援密碼同步化代理程式 ◆ Red Hat Linux 3.0、4.0 或 5.0 ES 或 AS ◆ SUSE Linux Enterprise Server 9 或 10 ◆ AIX 5.2L、5.2 或 5.3 版 Java 遠端載入器系統： ◆ HP-UX* 11i ◆ OS/400 ◆ xOS* ◆ 應該可以在具有 JVM 1.4.2 或以上版本的任何系統上使用
稽核	Novell Audit 2.0.2	
使用者應用程式 SSO 整合	需要 Novell Access Manager 3.0.1。	包含以 JDK*1.5 建構的 saslsaml.jar 版本。

安裝的先決條件

2

本節將說明安裝「Identity Manager 角色提供模組」的必要條件。主題包括：

2.1 Java Development Kit

JBoss、WebSphere 和 Identity Vault 對 Java Development Kit 的要求各不相同。

JBoss 應用程式伺服器：在 JBoss 應用程式伺服器上，使用 Java 2 Platform Standard Edition Development Kit 1.5.0_14 版。

使用此版本的 Sun JDK 按以下方法啓動「角色提供模組」安裝程式：

Linux/Solaris：

```
$ /opt/jdk1.5.0_10/bin/java -jar IdmUserApp.jar
```

Windows：

```
C:\Novell\InstallFiles\> "C:\Program
Files\Java\jdk1.5.0_10\bin\java.exe" -jar IdmUserApp.jar
```

安裝程序要求輸入 Java 的完整安裝路徑時，請提供 Sun JDK 的根路徑。例如，在 Linux 上，根路徑可能是

```
/opt/jdk1.5.0_10
```

附註：SLES 使用者：請勿使用 SLES 隨附的 IBM JDK。此版本在某些方面與該安裝程式不相容。

WebSphere 應用程式伺服器：在 WebSphere* 應用程式伺服器上，使用 WebSphere Application Server 6.1.0.9 隨附的 IBM JDK，並套用無限制規則檔。請對 6.1.0.9 套用 WAS JDK fixpack。

Identity Vault (Metadirectory) 安裝程式：Identity Vault (Metadirectory) 安裝程式會在 NetWare® 之外的所有平台上安裝它自己的 JVM。在 NetWare 上，Identity Vault 會使用系統上所安裝之任何版本的 Java。

2.2 安裝 Identity Manager Metadirectory

安裝 Identity Manager 3.5.1 Metadirectory。*《Novell Identity Manager 3.5.1 安裝指南》*(http://www.novell.com/documentation/idm35/pdfdoc/install/install.pdf) 中提供了說明。

將對 Identity Vault 的存取權授予 「Identity Manager 角色提供模組」管理員。若要實現此目的，請在蛆 Manager 嵣丹 V 管理員授予存取將儲存 「Identity Manager 角色提供模組」之網路位置的權限。

2.3 安裝 JBoss 應用程式伺服器

如果您計畫使用 JBoss* 應用程式伺服器，請執行以下任一操作：

- 根據製造廠商的說明下載並安裝 JBoss 4.2.0 應用程式伺服器
- 使用「角色提供模組」隨附的 JbossMysql 公用程式安裝 JBoss 應用程式伺服器 (可選安裝 MySQL)。如需說明，請參閱 「安裝 JBoss 應用程式伺服器和 MySQL 資料庫」(第 18 頁)。

安裝 「Identity Manager 角色提供模組」之後，啓動 JBoss 伺服器。啓動 JBoss 伺服器屬於安裝後任務。

RAM:「Identity Manager 角色提供模組」在執行中時，JBoss 應用程式伺服器的建議最低 RAM 爲 512 MB。

埠：記下應用程式伺服器使用的連接埠；「角色提供模組」安裝程式會要求輸入此連接埠。(應用程式伺服器的預設爲 8080)。

SSL: 如果您計畫使用外部的密碼管理，則請在您部署 「Identity Manager 角色提供模組」和 IDMPwdMgt.war 檔案的 JBoss 伺服器上啓用 SSL。如需有關啓用 SSL 的說明，請參閱 JBoss 文件。此外，也請確定 SSL 連接埠在您的防火牆上開啓。如需有關 IDMPwdMgt.war 檔案的資訊，請參閱 「存取外部密碼 WAR」(第 96 頁) 以及 *《IDM 使用者應用程式：管理指南》*(http://www.novell.com/documentation/idmrbpm36/index.html)。

2.3.1 安裝 JBoss 應用程式伺服器和 MySQL 資料庫

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

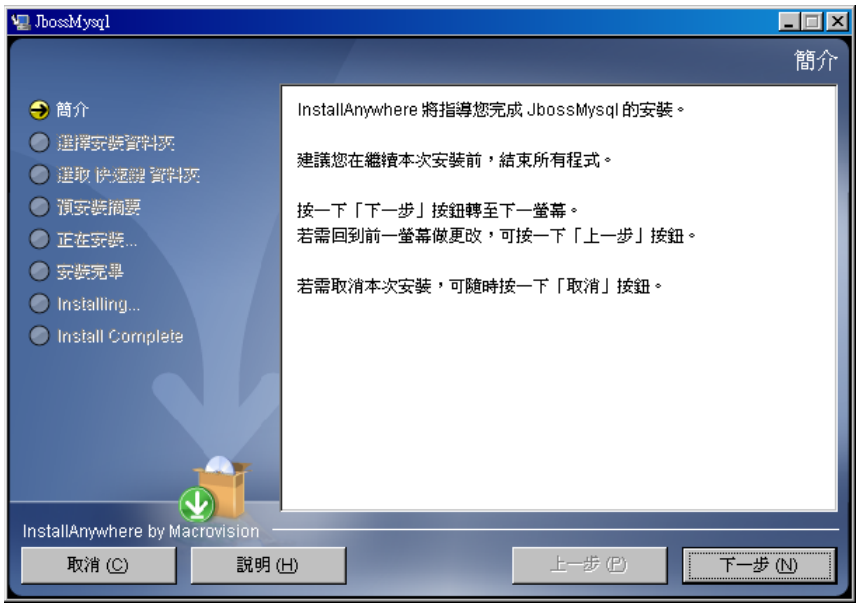
附註：此公用程式無法將 「JBoss 應用程式伺服器」安裝爲 Windows 服務。若要將 「JBoss 應用程式伺服器」安裝爲 Windows 系統上的服務，請參閱 「將 「JBoss 應用程式伺服器」安裝爲服務」(第 21 頁)。

---

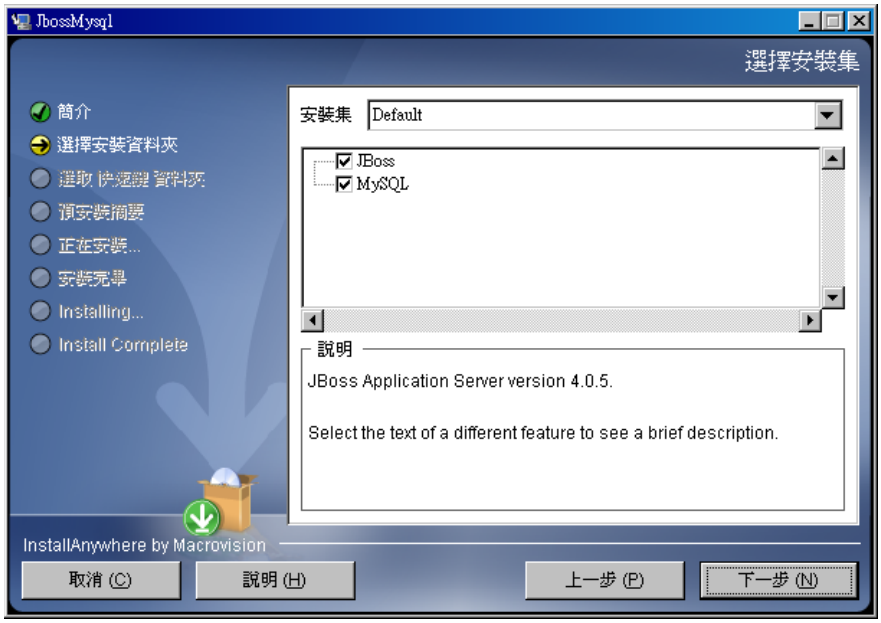
1. 找出並執行 JbossMysql.bin 或 JbossMysql.exe。您可以找到這個與 「使用者應用程式」安裝程式繫結的公用程式，該安裝程式位於

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

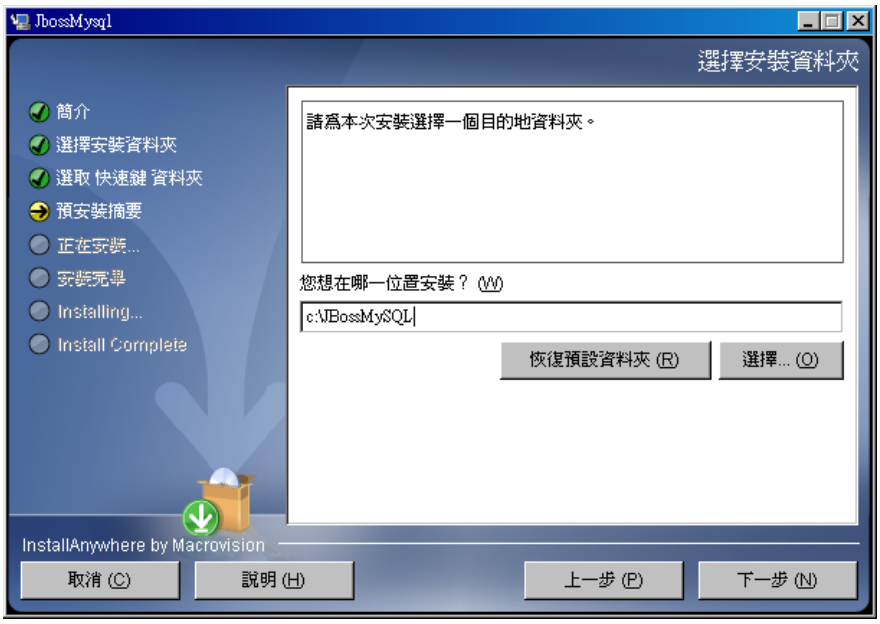
   未提供 Solaris 的公用程式。
2. 選取您的地區設定。
3. 請閱讀簡介頁面，然後按一下 「*下一步*」。



4 選取您要安裝的產品，然後按一下「*下一步*」。

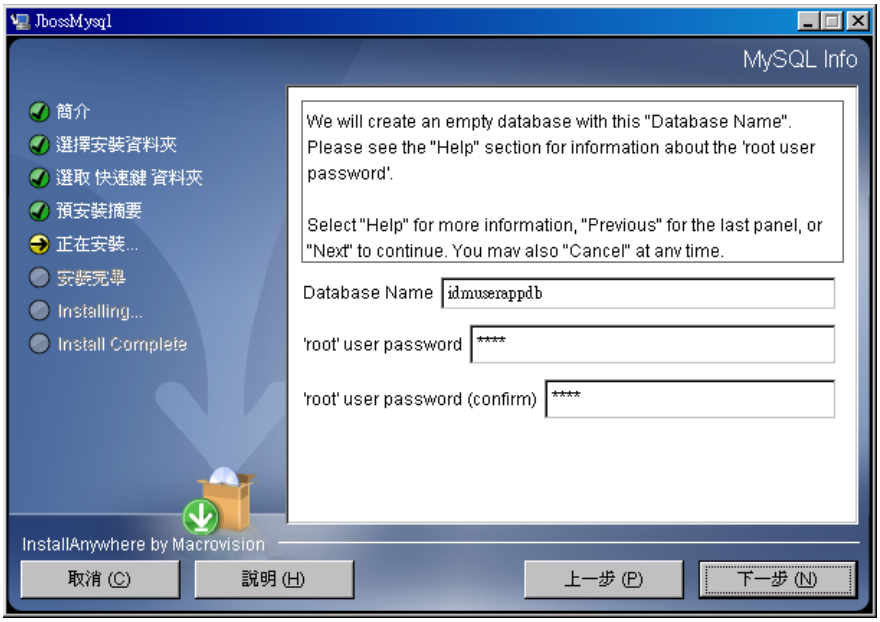


5 按一下「*選擇*」來選取基礎資料夾，選取的產品將安裝在該資料夾內，然後按一下「*下一步*」。



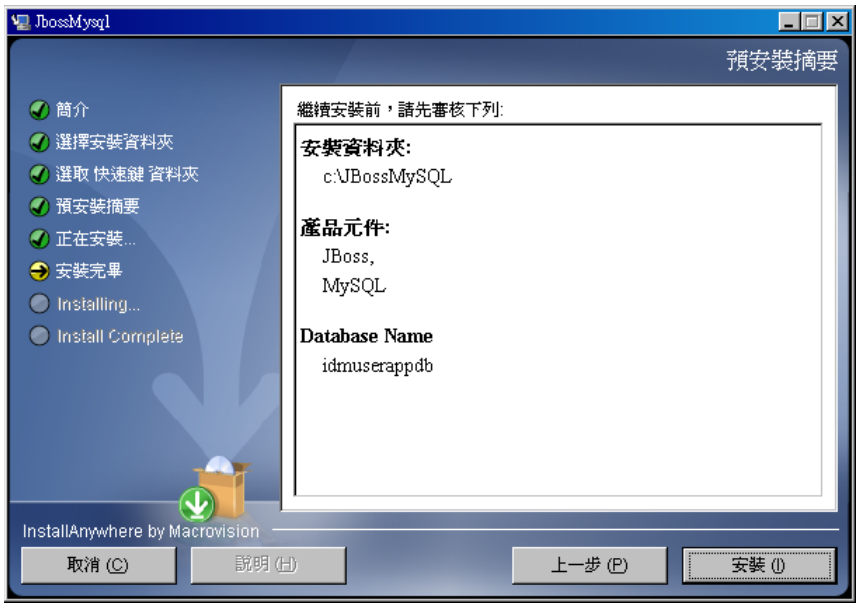
6 指定您資料庫的名稱。「使用者應用程式」安裝需要這個名稱。

7 指定資料庫根部使用者的密碼。



8 按一下「下一步」。

9 在「預先安裝摘要」中檢閱您的指定項目，然後按一下「*安裝*」。



在安裝完您選取的產品之後，公用程式會顯示安裝成功的訊息。如果您有安裝 MySQL 資料庫，請繼續前往 「設定您的 MySQL 資料庫」(第 23 頁)。

2.3.2 將「JBoss 應用程式伺服器」安裝爲服務

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

本節包含下列主題：

- 「使用 Java Service Wrapper」(第 21 頁)
- 「使用協力廠商的公用程式」(第 22 頁)

使用 Java Service Wrapper

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

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

wrapper.conf :

```
wrapper.java.command=%JAVA_HOME%/bin/java
wrapper.java.mainclass=org.tanukisoftware.wrapper.WrapperSimpleApp
wrapper.java.classpath.1=%JBOSS_HOME%/server/default/lib/wrapper.jar
wrapper.java.classpath.2=%JAVA_HOME%/lib/tools.jar wrapper.java.classpath.3=./run.jar
```

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

---

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

---

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

使用協力廠商的公用程式

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

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

2.4 安裝 WebSphere 應用程式伺服器

如果您計畫使用 WebSphere 應用程式伺服器，請下載並安裝 WebSphere 6.1.0.9 應用程式伺服器。請對 6.1.0.9 套用 WAS JDK fixpack。

2.5 資料庫

安裝資料庫和資料庫驅動程式，並建立資料庫或資料庫例項。記下以下資料庫參數，以在「Identity Manager 角色提供模組」的安裝程序中使用：

- 主機和連接埠
- 資料庫名稱、使用者名稱和使用者密碼

資料來源檔案必須指向資料庫。安裝方法因應用程式伺服器而異。對於 JBoss，「Identity Manager 角色提供模組」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 角色提供模組」 WAR 檔案的名稱命名該檔案。對於 WebSphere，先手動設定資料來源，再進行安裝。

必須爲 UTF-8 啓用資料庫。

- 「安裝 MySQL」(第 22 頁)
- 「設定您的 MySQL 資料庫」(第 23 頁)

2.5.1 安裝 MySQL

不論您是透過「IDM 使用者應用程式」公用程式還是靠自己來安裝 MySQL*，均可參閱「設定您的 MySQL 資料庫」(第 23 頁)。

附註：如果您計畫移轉某個資料庫，請先啓動該資料庫，然後才在安裝程式中選取移轉選項。如果您不想移轉資料庫，就無須在安裝「Identity Manager 角色提供模組」期間執行資料庫。只要在啓動應用程式伺服器之前啓動資料庫即可。

2.5.2 設定您的 MySQL 資料庫

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

- 「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)

INNODB 存放引擎和表格類型

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

default-table-type=innodb

不應該包含 skip-innodb 選項。

字元集

指定 UTF8 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 UTF8：

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資源集，還必須在 IDM-ds.xml 檔案的 JDBC* URL 中設定字元集，如下所示：

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

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)。

2.6 安全性必要條件

透過開啓 Novell Access Manager™ 或 iChain® 中的「Cookie 轉遞」選項，可以啓用「Identity Manager 角色提供模組」中的「同時登出」功能。如需說明，請參閱 《*Novell Access Manager 3.0 SP1 管理指南*》中的「插入到 Cookie 標頭」(http://www.novell.com/documentation/novellaccessmanager/adminguide/index.html?page=/documentation/novellaccessmanager/adminguide/data/b5pqck8.html)。

2.7 下載產品

從 Novell 下載 (http://download.novell.com/index.jsp) 處取得 Identity Manager Roles Based Provisioning Module 3.6 這一產品。

依您的系統下載正確的「使用者應用程式」 .iso 影像檔：
Identity_Manager_3_6_0_User_Application_Provisioning.iso

此 .iso 檔案包含以下傳送目錄：

/linux/user_application (適用於 Linux)
/nt/user_application (適用於 Windows)
/solaris/user_application (適用於 Solaris)
/36MetaDirSupport (包含更新 IDM 3.5.1 Metadirectory 以支援 IDM 3.6 使用者應用程式所需的檔案)

表格 2-1 列出了安裝 Identity Manager Roles Based Provisioning Module 3.6 所需的檔案和程序檔。

表格 2-1 *安裝 Identity Manager 3.6 使用者應用程式時所需的檔案和程序檔*

檔案	描述
IDMProv.war	這是「角色提供模組」 WAR 檔。它包含支援「身份自助服務」功能和「角色提供模組」的「Identity Manager 3.6 使用者應用程式」。
IDMUserApp.jar	這是「角色提供模組」安裝程式。
silent.properties	此檔案包含進行無訊息安裝所需的安裝參數。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。
prerequisitefiles.zip	此 ZIP 檔包含其他需要手動安裝的檔案。
UserApplication_3_6_0-IDM3_5_1-V1.xml	這是「使用者應用程式」驅動程式的組態檔案。
iManager_icons_for_roles.zip	此檔案包含 eDirectory 中角色物件的 iManager 圖示。

提示：可在目錄 /36MetaDirSupport 中找到 iManager_icons_for_roles.zip 和 prerequisites.zip。其他檔案位於 < *作業系統* > /user_application 目錄中。

安裝「Identity Manager 角色提供模組」的系統至少必須有 320 MB 的可用儲存空間。

預設安裝位置是：

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

在安裝期間，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，非根使用者可以寫入該目錄)。

2.8 安裝 prerequisitefiles.zip 檔的內容

在所下載的 .iso 影像中，找到 prerequisitefiles.zip 檔並將其解除壓縮。該 Zip 檔包含必須手動安裝的各檔案，如表格 2-2 所示：

表格 2-2 *需要手動安裝的檔案*

檔名	描述	說明
nrf-extensions.sch	eDirectory™ 綱要檔案	「擴充 Roles Based Provisioning Module 3.6 版的 eDirectory 綱要」(第 25 頁)
nrfdriver.jar	「角色服務」驅動程式 JAR	「複製角色服務驅動程式的 JAR 檔案」(第 26 頁)
RoleService-IDM3_5_1-V1.xml	「角色服務」驅動程式組態檔案	「複製角色服務驅動程式組態檔案」(第 27 頁)
UserApplicationn_3_6_0-IDM3_5_1-V1.xml	支援「角色提供模組」的「使用者應用程式」驅動程式組態檔案	「複製使用者應用程式驅動程式組態檔案」(第 27 頁)
dirxml.lsc	記錄應用程式記錄綱要檔案	「複製 dirxml.lsc 檔案」(第 27 頁)

- 「擴充 Roles Based Provisioning Module 3.6 版的 eDirectory 綱要」(第 25 頁)
- 「複製角色服務驅動程式的 JAR 檔案」(第 26 頁)
- 「複製角色服務驅動程式組態檔案」(第 27 頁)
- 「複製使用者應用程式驅動程式組態檔案」(第 27 頁)
- 「複製 dirxml.lsc 檔案」(第 27 頁)

2.8.1 擴充 Roles Based Provisioning Module 3.6 版的 eDirectory 綱要

擴充「角色提供模組」的 eDirectory 綱要，如下列各節所述：

- 「在 Windows 上擴充綱要」(第 26 頁)
- 「在 UNIX/Linux 上擴充綱要」(第 26 頁)
- 「在 NetWare 上擴充綱要」(第 26 頁)

在 Windows 上擴充綱要

在 Windows 伺服器上使用 NDSCons.exe 括充綱要。依預設，eDirectory 隨附的綱要檔案 (*.sch) 安裝於 C:\Novell\NDS 目錄中。

1. 按一下 *「開始」>「設定」>「控制台」>「Novell eDirectory 服務」*。
2. 按一下 *install.dlm*，然後按一下 *「啓動」*。
3. 按一下 *「安裝其他綱要檔案」*，然後按一下 *「下一步」*。
4. 以具有管理權限的使用者身份登入，然後按一下 *「確定」*。
5. 指定綱要檔案路徑和名稱 (例如，c:\Novell\NDS\nrf-extensions.sch)。
6. 按一下 *「完成」*。

在 UNIX/Linux 上擴充綱要

若要在 UNIX/Linux 平台上擴充 「角色提供模組」的 eDirectory 綱要，請執行以下步驟：

1. 新增 「角色提供模組」綱要檔案 nrf-extensions.sch。若要實現此目的，請在指令行處使用 ndssch 指令：

   ndssch [-h *主機名稱* [: *連接埠*]] [-t *網路樹名稱*] admin-FDN *綱要檔案名稱 .sch*

在 NetWare 上擴充綱要

在 NetWare 伺服器上使用 NWConfig.nlm 擴充綱要。eDirectory 隨附的綱要檔案 (*.sch) 安裝於 sys:\system\schema 目錄中。

1. 在伺服器主控台上輸入 nwconfig。
2. 選取 *「目錄選項」>「擴充綱要」*。
3. 以具有管理權限的使用者身份登入。
4. 按 F3 指定另一路徑，然後鍵入 sys:\system\schema (或 *.sch 檔案的路徑) 和 nrf-extensions.sch 綱要檔案。
5. 按下 Enter。

2.8.2 複製角色服務驅動程式的 JAR 檔案

在 Metadirectory 伺服器上手動安裝 「角色服務」驅動程式。若要這樣做，請依您的系統從已解除壓縮的 prerequisitefiles.zip 歸檔中將「角色服務」JAR 可執行檔 nrfdriver.jar 複製到正確目錄：

表格 2-3 *角色服務驅動程式 JAR 檔案的位置*

作業系統	目錄
UNIX (eDirectory 8.7.x)	/usr/lib/dirxml/classes
UNIX (eDirector 8.8.x)	/opt/novell/eDirectory/lib/dirxml/classes
Windows	<drive>:\novell\nds\lib
NetWare	SYS:SYSTEM\LIB

2.8.3 複製角色服務驅動程式組態檔案

依您的系統將「角色服務」驅動程式組態檔案 RoleService_IDM3_5_1-V1.xml 手動安裝到正確目錄：

表格 2-4 *角色服務驅動程式組態檔案的位置*

作業系統	目錄
Linux (eDirectory 8.7.x)	/usr/lib/dirxml/classes
Linux (eDirectory 8.8)	/var/opt/novell/iManager/nps/DirXML.Drivers
Windows	C:\Program Files\Novell\tomcat\webapps\nps\Dirxml.Drivers
NetWare	SYS:\tomcat\4\webapps\nps\Dirxml.Drivers

2.8.4 複製使用者應用程式驅動程式組態檔案

依您的系統將「使用者應用程式」驅動程式組態檔案 UserApplication_3_6_0-IDM3_5_1-V1.xml 手動安裝到正確目錄：

表格 2-5 *使用者應用程式驅動程式組態檔案的位置*

作業系統	目錄
Linux (eDir 8.7.x)	/usr/lib/dirxml/classes
Linux (eDir 8.8)	/var/opt/novell/iManager/nps/DirXML.Drivers
Windows	C:\Program Files\Novell\tomcat\webapps\nps\Dirxml.Drivers
NetWare	SYS:\tomcat\4\webapps\nps\Dirxml.Drivers

2.8.5 複製 dirxml.lsc 檔案

根據《Identity Manager 使用者應用程式：管理指南》(http://www.novell.com/documentation/idmrbpm36/pdfdoc/agpro/agpro.pdf) 中「設定記錄」一節中的說明，將 dirxml.lsc 檔案複製到 Audit 伺服器。

2.9 安裝角色的 iManager 圖示

在所下載的 .iso 影像中，找到 iManager_icons_for_roles.zip 檔並將其解除壓縮。將解除壓縮的圖示檔案複製到 nps/portal/modules/dev/images/dir 目錄。重新啓動 iManager 以使用新圖示。

建立驅動程式

3

本節說明如何建立使用 「角色提供模組」所需的驅動程式。主題包括：

- 「在 iManager 中建立使用者應用程式驅動程式」(第 29 頁)
- 「在 iManager 中建立角色服務驅動程式」(第 33 頁)

重要：必須先建立 「使用者應用程式」驅動程式，才能建立 「角色服務」驅動程式。因爲 「角色服務」驅動程式會參考 「使用者應用程式」驅動程式中的角色儲存區容器 (RoleConfig.AppConfig)，所以需要先建立 「使用者應用程式」驅動程式。

允許的驅動程式組態是：

- 可爲 iManager 中設定的每個驅動程式新增一個 「角色服務」驅動程式。
- 可將一個 「使用者應用程式」驅動程式與一個 「角色服務」驅動程式相關聯。
- 可將一個 「使用者應用程式」與一個 「使用者應用程式」驅動程式相關聯。

3.1 在 iManager 中建立使用者應用程式驅動程式

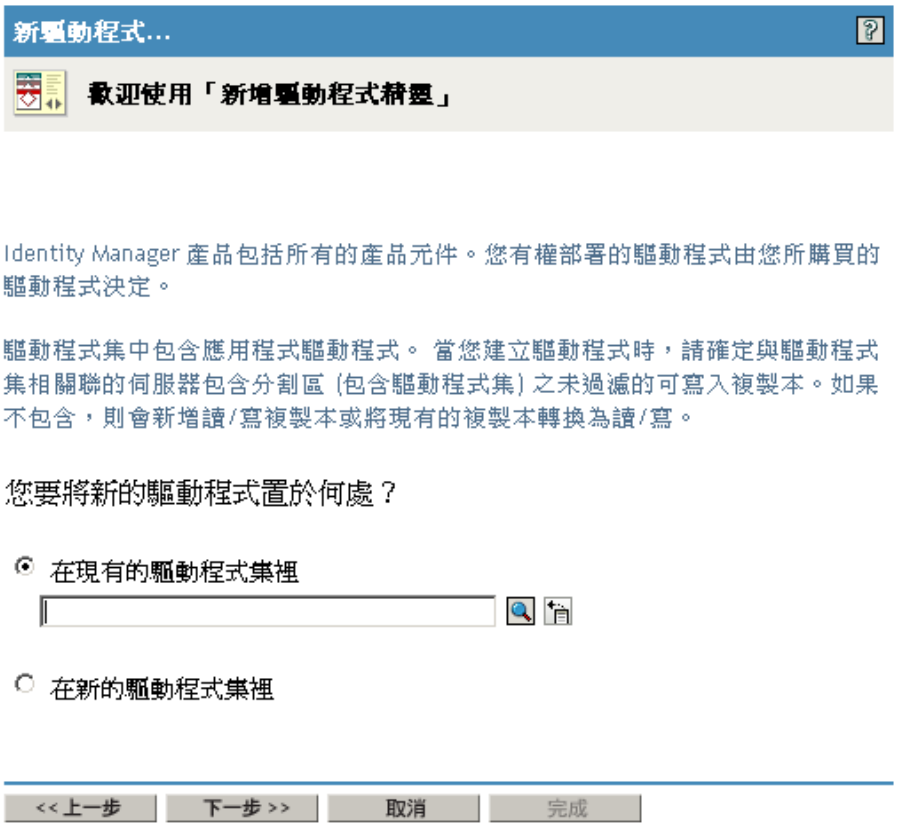
必須爲每個 「Identity Manager 角色提供模組」建立個別的 「使用者應用程式」驅動程式，屬於叢集成員的 「角色提供模組」除外。屬於同一個叢集的各個 「角色提供模組」必須共用同一個 「使用者應用程式」驅動程式。如需在叢集中執行 「角色提供模組」的相關資訊，請參閱 *《Identity Manager 使用者應用程式：管理指南》*(http://www.novell.com/documentation/idmrbpm36/index.html)。

「角色提供模組」將應用程式特定資料儲存在 「使用者應用程式」驅動程式中，以控制和設定應用程式環境。這包含 「 應用程式伺服器」資訊和工作流程引擎組態。

重要：將一組不屬於叢集的 「角色提供模組」設定爲共用一個驅動程式，會造成 「角色提供模組」中執行的一或多個元件之間的混淆。這些錯誤的來源很難偵測出來。

若要建立 「使用者應用程式」驅動程式，並將其與驅動程式集相關聯：

1. 在網頁瀏覽器中開啓 iManager 2.6 或更高版本。
2. 移至 「*角色和任務* > *Identity Manager 公用程式*」，並選取 「*新驅動程式*」來啓動 「建立驅動程式精靈」。

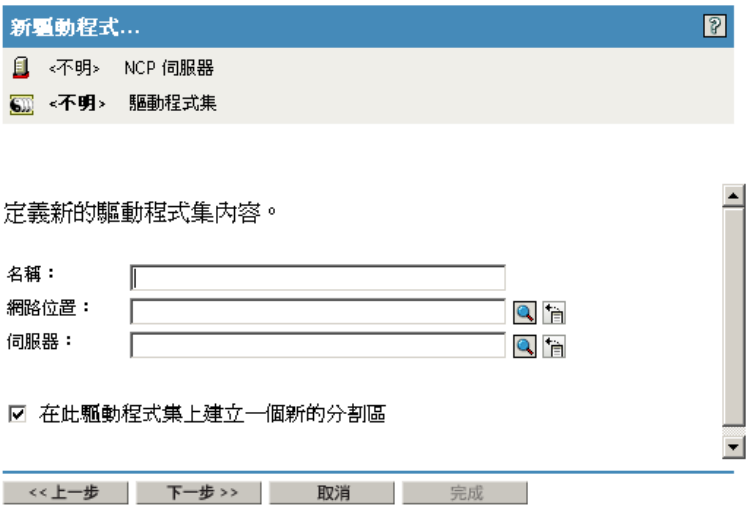


3 若要在現有的驅動程式集中建立驅動程式，選取「*在現有的驅動程式集裡*」，按一下物件選擇器圖示，選取驅動程式集物件，按一下「*下一步*」並繼續進行步驟 4。

或

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

3a 爲新的驅動程式集指定名稱、網路位置和伺服器。網路位置是伺服器物件所在的 eDirectory™ 網路位置。



3b 按一下「下一步」。

4 核取「*從伺服器 (.XML 檔案) 輸入驅動程式組態*」。

5 從下拉式清單中選取 *UserApplication_3_6_0-IDM3_5_1-V1.xml*。這是支援「角色提供模組」的「使用者應用程式」驅動程式組態檔案。

如果 *UserApplication_3_6_0-IDM3_5_1-V1.xml* 不在此下拉式清單中，則表明您沒有將此檔案複製到正確的位置。請參閱「複製使用者應用程式驅動程式組態檔案」(第 27 頁)。

6 按「*下一步*」。

7 系統會提示您輸入驅動程式的參數 (請捲動畫面檢視全部)。請記錄各個參數，您將在安裝「角色提供模組」時用到這些參數。

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

8 按「*下一步*」。

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

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

10 (選擇性，但建議使用) 按一下「*排除管理者角色*」。

11 按一下「*新增*」，選取要禁止其執行驅動程式動作的使用者 (如管理角色)，按兩次「*確定*」，再按「*下一步*」。

12 按一下「*確定*」，以關閉「安全性相等」視窗並顯示摘要頁面。

13 如果資訊正確，按一下「*完成*」或「*完成概觀*」。

重要：依預設，此驅動程式處於關閉狀態。在「角色提供模組」安裝完畢之前，將驅動程式保持爲關閉狀態。

3.2 在 iManager 中建立角色服務驅動程式

在 iManager 中建立和設定「角色服務」驅動程式。

1. 在網頁瀏覽器中開啓 iManager 2.6 或更高版本。
2. 在 *「Identity Manager」>「Identity Manager 綜覽」*中，選取要安裝之「角色服務」驅動程式所在的驅動程式集。

   在安裝「角色服務」驅動程式之前，先安裝「使用者應用程式」驅動程式。使用包含「角色服務」驅動程式的「使用者應用程式」驅動程式 3.6 版 (UserApplication_3_6_0-IDM3_5_1-V1.xml)。如果您使用其他版本的「使用者應用程式」驅動程式，「角色目錄」將不可用。

   每個驅動程式集只能有一個「角色服務」驅動程式。
3. 按一下「*新增驅動程式*」。
4. 在「新增驅動程式」精靈中，保留預設值「*在現有的驅動程式集中*」。按 *「下一步」*。
5. 從下拉式清單中選取 *RoleService-IDM3_5_1-V1.xml*。這是支援「角色提供模組」的「角色服務」驅動程式組態檔案。

   如果 *RoleService-IDM3_5_1-V1.xml* 不在此下拉式清單中，則表明您沒有將此檔案複製到正確的位置。請參閱「複製角色服務驅動程式組態檔案」(第 27 頁)。

   按 *「下一步」*。

   嘗試建立驅動程式時，可能會看到下列錯誤：

   ```
   The following 'Namespace Exception' occurred while trying to access
   the directory.  (CLASS_NOT_DEFINED)
   ```

如果是這樣，則表明 iManager 應用程式可能尚未套用新的「角色」綱要。新綱要是「角色服務」驅動程式所必需的。請嘗試重新啓動 iManager 會期 (關閉所有瀏覽器，然後再次登入 iManager)。或者，嘗試重新啓動伺服器。

6 在「輸入申請資訊」頁中填入申請資訊。下表描述了申請資訊。

選項	描述
驅動程式名稱	指定「角色服務」驅動程式的驅動程式名稱，或者保留預設名稱 Role Service。如果安裝的新驅動程式與現有驅動程式同名，新驅動程式會覆寫現有驅動程式的組態。 使用「*瀏覽*」按鈕檢視選定驅動程式集中的現有驅動程式。這是必要欄位。
使用者應用程式驅動程式 DN	代管角色系統之「使用者應用程式」驅動程式物件的可辨識名稱。使用 eDirectory 格式 (如 UserApplication.driverset.org)，或者瀏覽以尋找驅動程式物件。這是必要欄位。
使用者應用程式 URL	用於連接「使用者應用程式」以啓動核准工作流程的 URL。提供的範例 URL 爲 *http://host:port/IDM*。這是必要欄位。
使用者應用程式身份	用於驗證到「使用者應用程式」以啓動核准工作流程之物件的可辨識名稱。可以是您將賦予其管理「使用者應用程式」入口網站之權限的「使用者應用程式管理員」。使用 eDirectory 格式 (如 admin.department.org)，或者瀏覽以尋找使用者。這是必要欄位。
使用者應用程式密碼	「驗證 ID」中指定的「使用者應用程式管理員」密碼。此密碼用於驗證「使用者應用程式」以啓動核准工作流程。這是必要欄位。
重新輸入密碼	重新輸入「使用者應用程式管理員」的密碼。

7 填入資訊之後，按一下「*完成*」。

在 JBoss 上使用 GUI 進行安裝

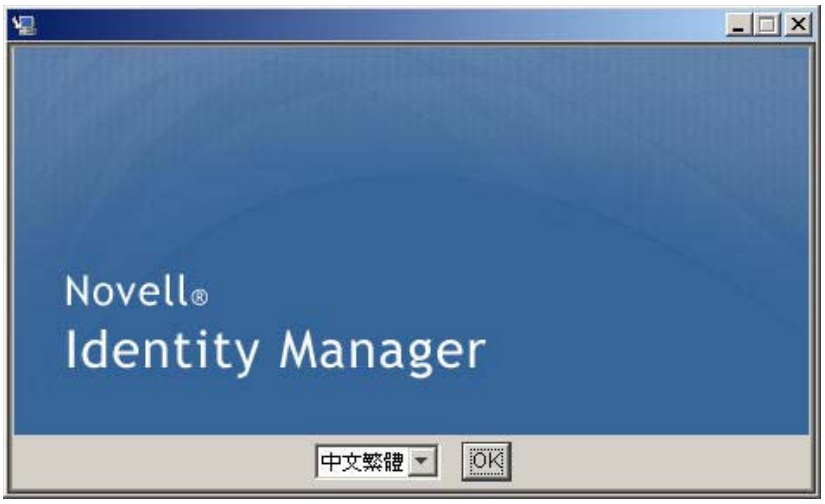
4

本節說明如何在 JBoss 應用程式伺服器上使用安裝程式的圖形使用者介面來安裝「Identity Manager 角色提供模組」。如果您希望透過主控台或使用單個指令在 JBoss 上進行安裝，請參閱第 5 章 「透過主控台或使用單個指令進行安裝」(第 61 頁)。

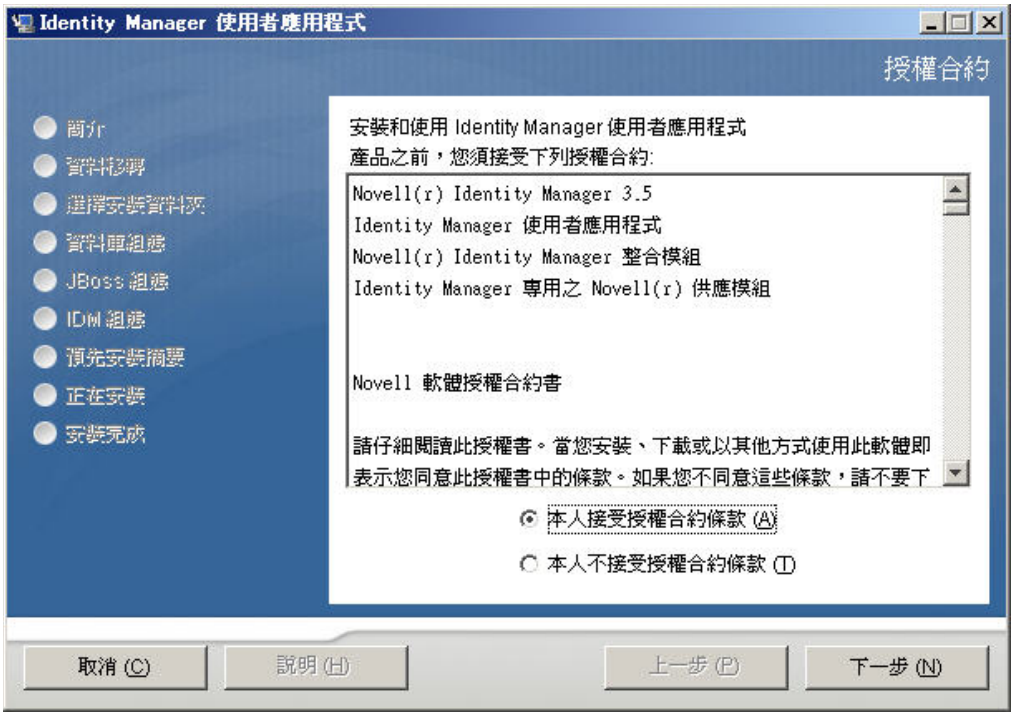
如果您希望使用指令行進行安裝，請參閱第 5 章 「透過主控台或使用單個指令進行安裝」(第 61 頁)。

4.1 啓動安裝程式 GUI

1. 瀏覽至含有安裝檔案的目錄，如表格 2-1 頁上 24 所述。
2. 從指令行啓動您平台的安裝程式：
   java -jar IdmUserApp.jar
3. 在下拉式選單中選取語言，然後按一下「*確定*」。



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



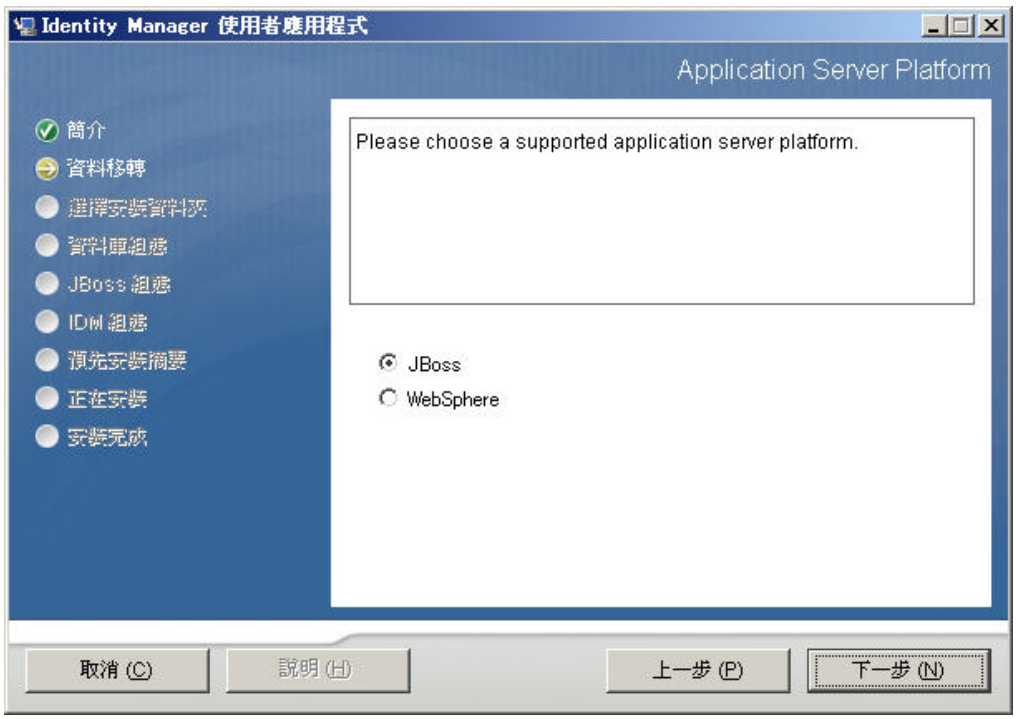
5 閱讀安裝精靈的「簡介」頁面，然後按一下「*下一步*」。

6 請繼續進行「選擇應用程式伺服器平台」(第 36 頁)。

4.2 選擇應用程式伺服器平台

完成「啓動安裝程式 GUI」(第 35 頁)中的程序，然後繼續執行下面的步驟：

1 選擇 JBoss 應用程式伺服器平台，然後按一下「*下一步*」。



4.3 移轉您的資料庫

1 如果您不要移轉資料庫，請按一下「*下一步*」並繼續進行 「指定 WAR 的位置」(第 39 頁)。

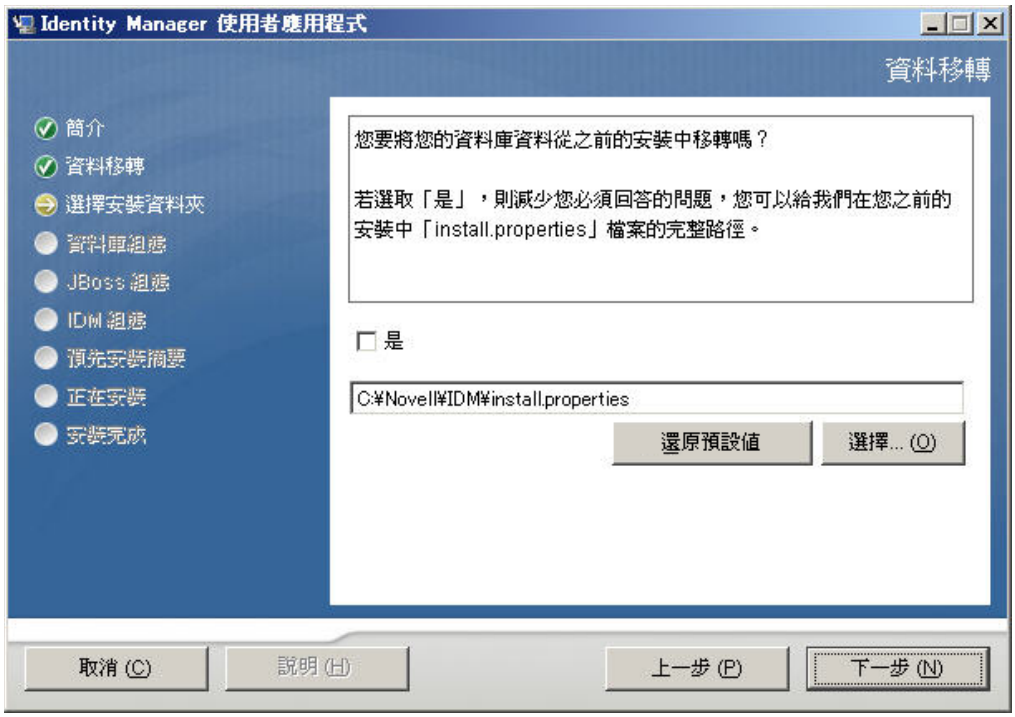
如果您想使用「使用者應用程式」 3.0 或 3.01 版的現有資料庫，則必須移轉該資料庫。繼續下一個步驟。

2 請確認您已經啓動想移轉的資料庫。

3 在安裝程式的「資料移轉」頁面中按一下「*是*」。

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

從前面的安裝過程指定 install.properties 檔案的位置，可減少您在後續頁面中必須選取的項目數目。



5 系統會要求您確認資料庫類型、主機名稱和連接埠。提供這些資訊，然後按「*下一步*」。

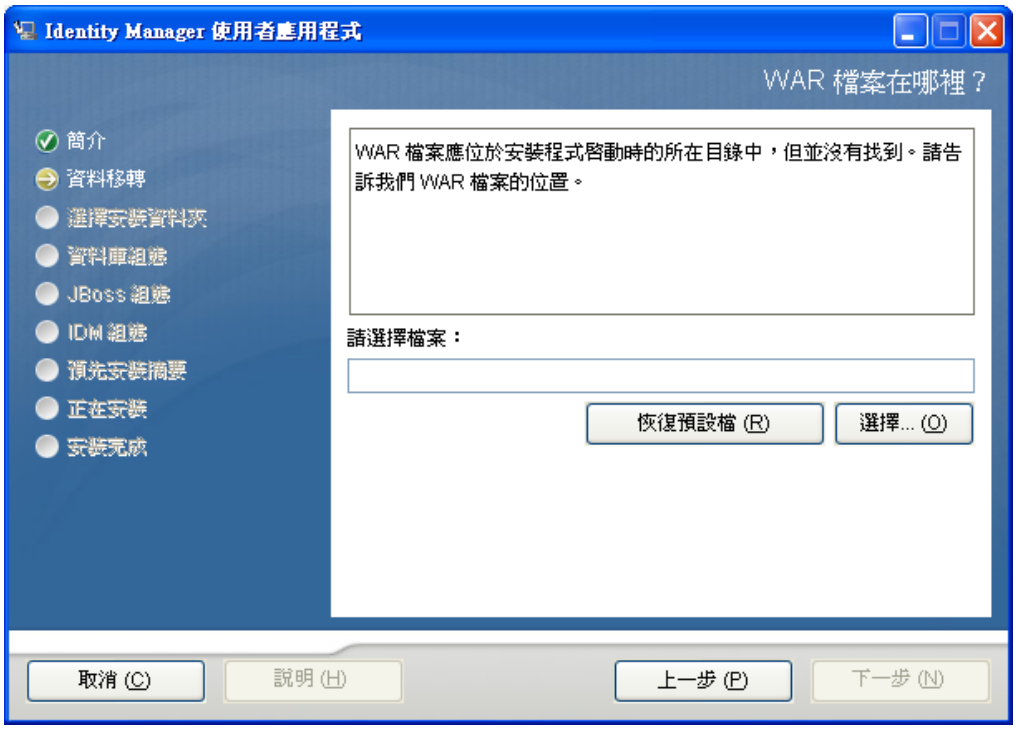
6 按一下「*下一步*」，繼續進行「指定 WAR 的位置」（第 39 頁）。「選擇安裝資料夾」（第 39 頁）

「使用者應用程式」安裝程式會升級您的「使用者安裝程式」，並移轉 3.0 或 3.0.1 版資料庫的資料到 3.5.1 版所使用的資料庫。如需移轉資料庫的詳細資訊和其他步驟，請參閱 *《Identity Manager 使用者應用程式：移轉指南》*(http://www.novell.com/documentation/idmrbpm36/index.html)。

4.4 指定 WAR 的位置

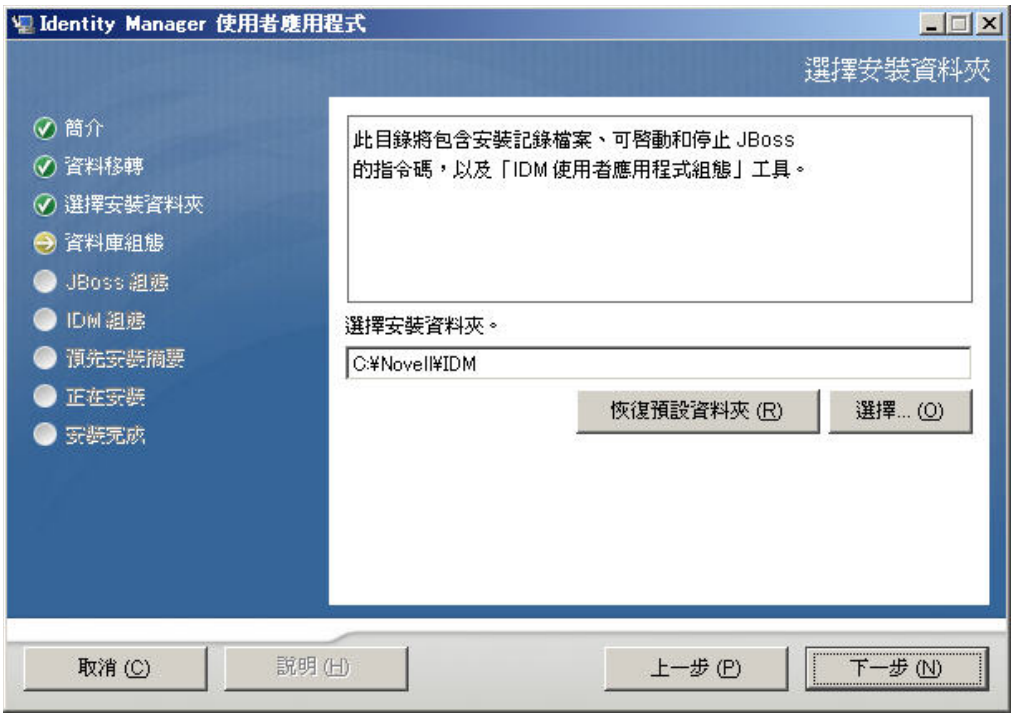
如果「Identity Manager 使用者應用程式」的 WAR 檔案所在的目錄與安裝程式的不同，安裝程式就會提示您輸入 WAR 的路徑。

1. 如果 WAR 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。
2. 按「*下一步*」，然後繼續「選擇安裝資料夾」(第 39 頁)。



4.5 選擇安裝資料夾

1. 在「選擇安裝資料夾」頁面上，選取「使用者應用程式」的安裝位置。如果您需要記住並使用預設的位置，請按一下「*還原預設資料夾*」，或者，如果您想選擇安裝檔案的其他位置，請按一下「*選擇*」來瀏覽一個位置。
2. 按「*下一步*」，然後繼續「選擇資料庫平台」(第 40 頁)。

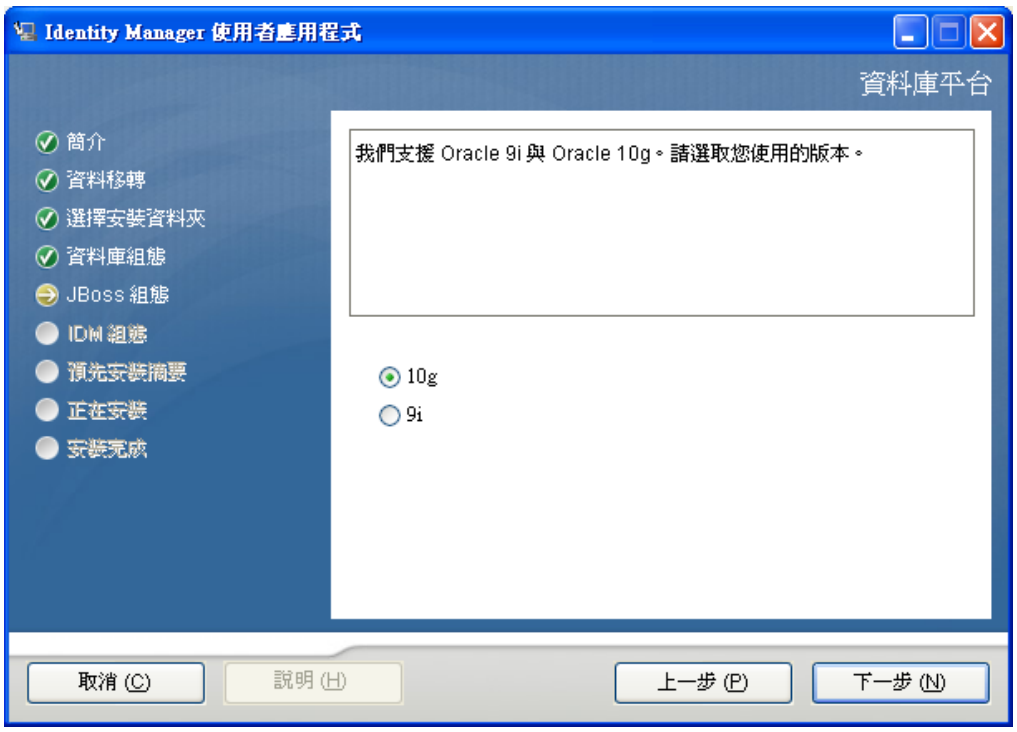


4.6 選擇資料庫平台

1 選取要使用的資料庫平台。

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

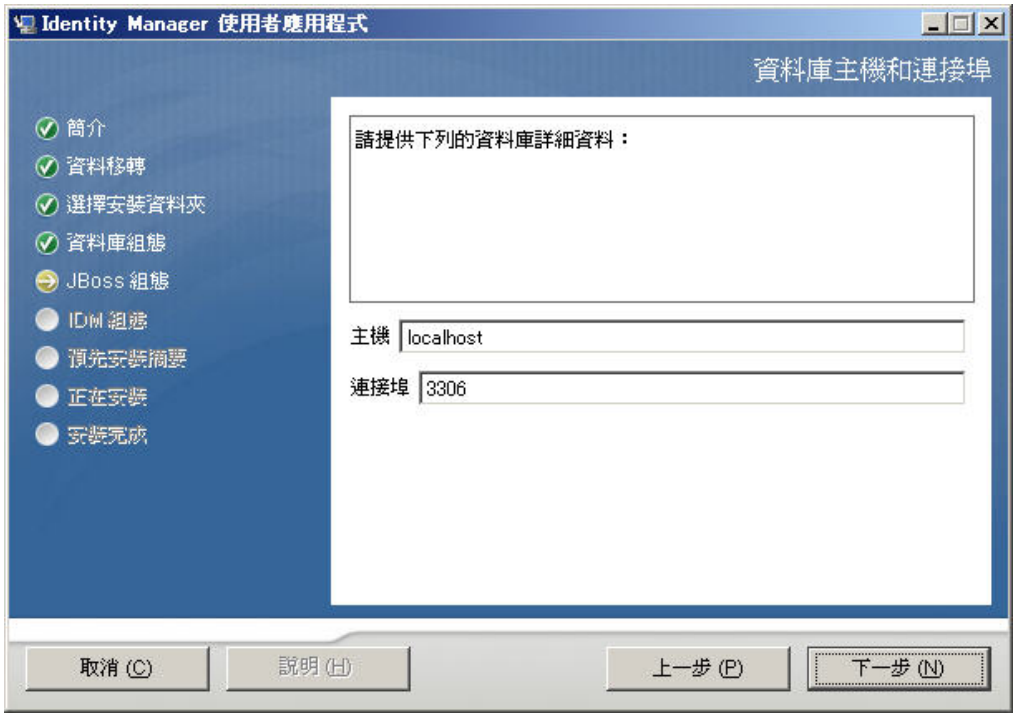
3 如果您使用 Oracle 資料庫，安裝程式就會詢問您所使用的版本。選擇您的版本。



4 按「*下一步*」，然後繼續「指定資料庫主機和連接埠」(第 41 頁)。

4.7 指定資料庫主機和連接埠

1 填寫下列欄位：

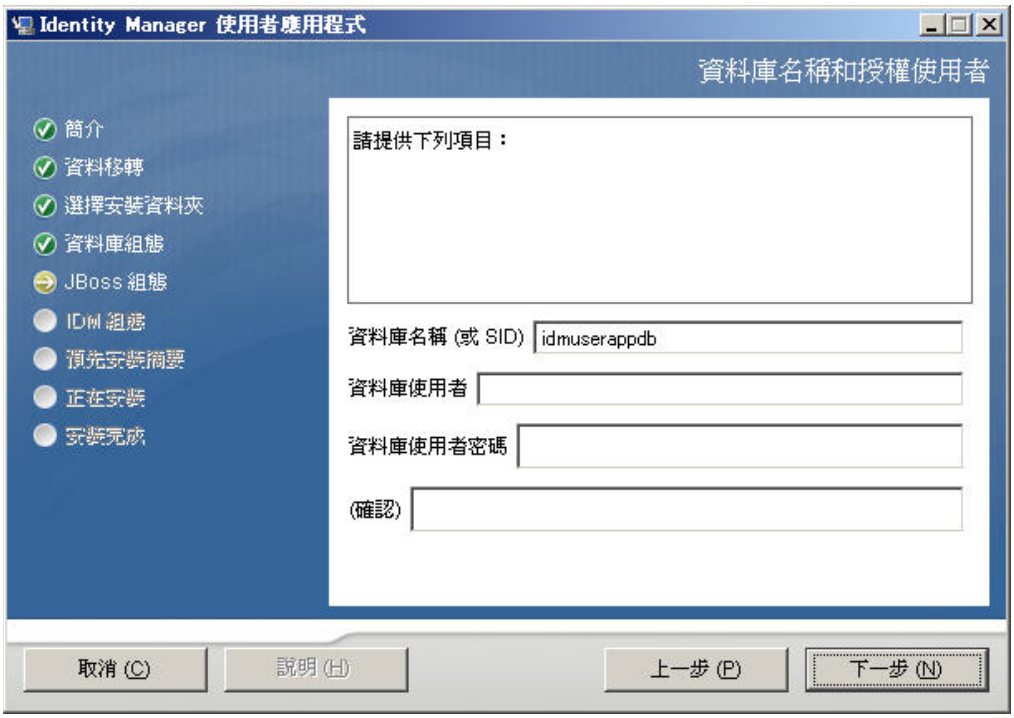


欄位	描述
主機	指定資料庫伺服器的主機名稱或 IP 位址。 對於叢集，請爲叢集的每一個成員指定相同的主機名稱和 IP 位址。
連接埠	指定資料庫的監聽程式連接埠號碼。 對於叢集，請爲叢集的每一個成員指定相同的連接埠。

2 按「*下一步*」，然後繼續「指定資料庫名稱和特權使用者」(第 42 頁)。

4.8 指定資料庫名稱和特權使用者

1 填寫下列欄位：



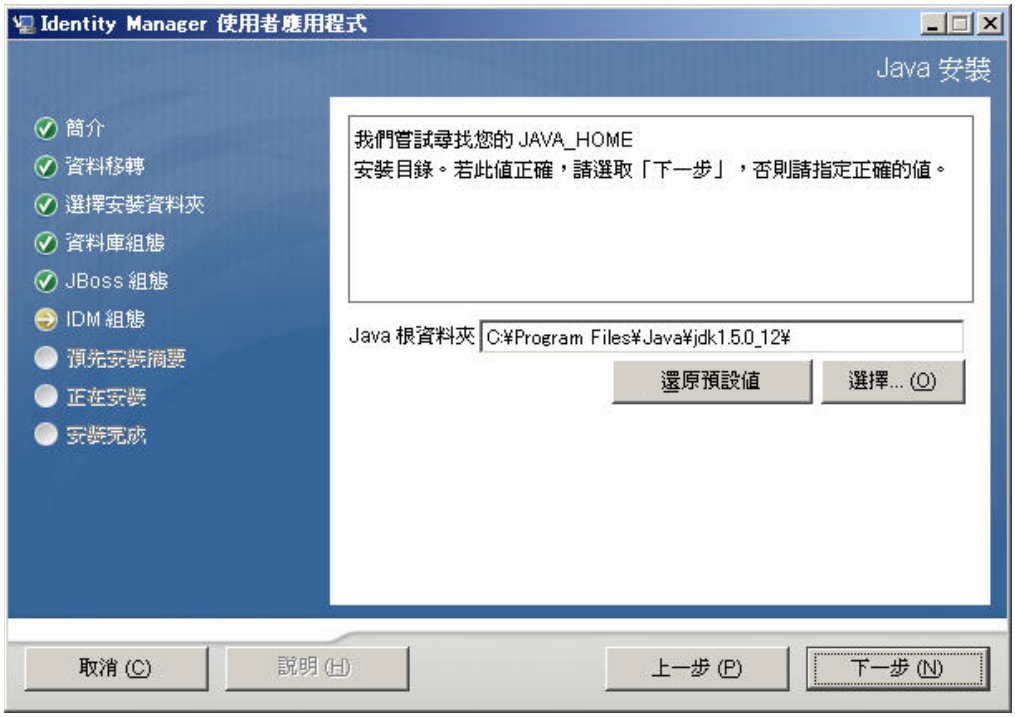
欄位	描述
資料庫名稱 (或 sid)	對於 MySQL 或 MS SQL Server，請提供您預先設定之資料庫的名稱。對於 Oracle，請提供您之前建立的 Oracle 系統識別碼 (SID)。 對於叢集，請爲叢集的每一個成員指定相同的資料庫名稱和 SID。
資料庫使用者	指定資料庫使用者。 對於叢集，請爲叢集的每一個成員指定相同的資料庫使用者。

欄位	描述
資料庫密碼 / 確認密碼	指定資料庫密碼。 對於叢集，請爲叢集的每一個成員指定相同的資料庫密碼。

2 按一下「*下一步*」，然後繼續「指定 Java 根目錄」(第 43 頁)。

4.9 指定 Java 根目錄

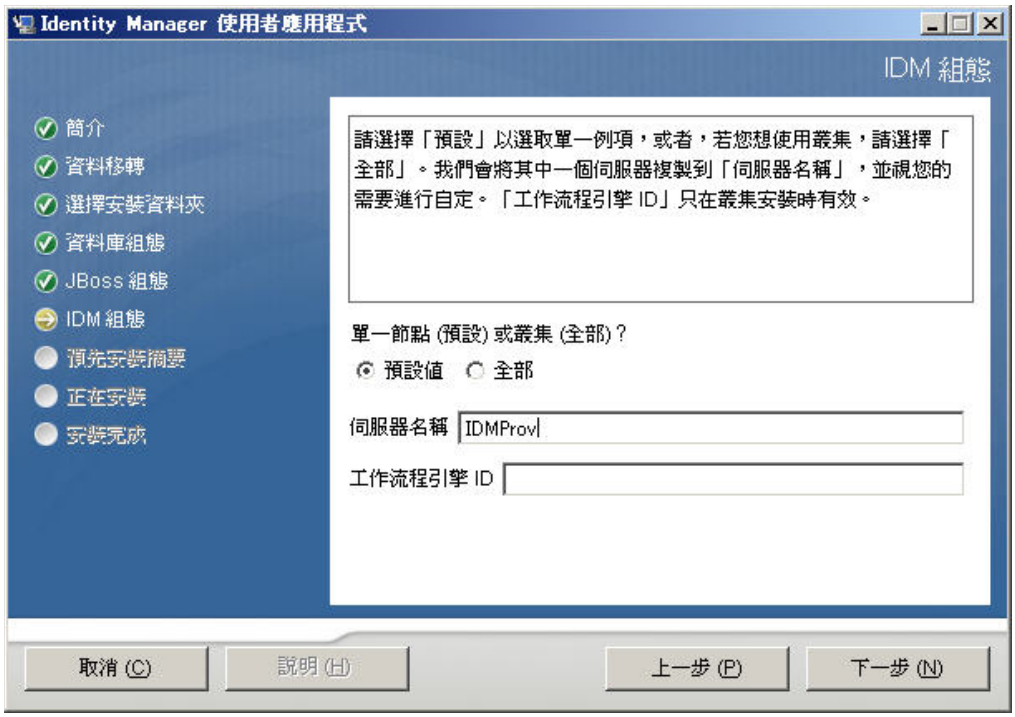
1 按一下「*選擇*」瀏覽您的 Java 根資料夾。若要使用預設位置，按一下「*還原預設值*」。



2 按一下「*下一步*」，然後繼續「指定 JBoss 應用程式伺服器設定」(第 44 頁)。

4.10 選擇應用程式伺服器組態類型

1 填寫下列欄位：



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

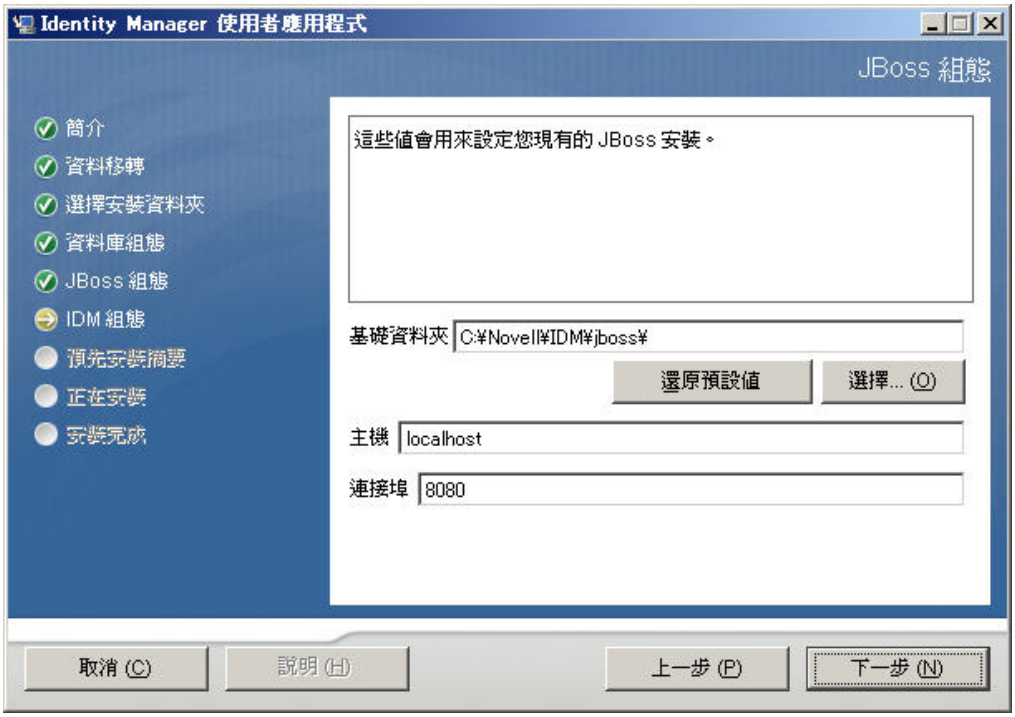
2 按「*下一步*」，然後繼續「啓用 Novell Audit 記錄」(第 45 頁)。

4.11 指定 JBoss 應用程式伺服器設定

在此頁面上讓「使用者應用程式」知道「JBoss 應用程式伺服器」的位置。

此安裝程序不會安裝「JBoss 應用程式伺服器」。如需安裝「JBoss 應用程式伺服器」的說明，請參閱「安裝 JBoss 應用程式伺服器和 MySQL 資料庫」(第 18 頁)。

1 提供基礎資料夾、主機和連接埠：



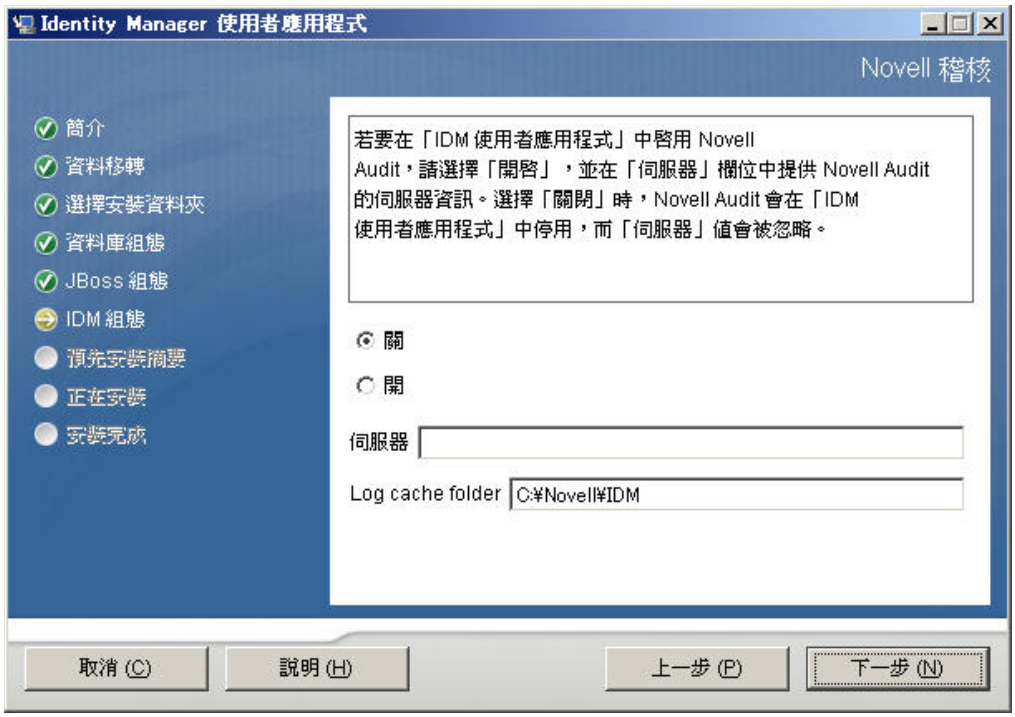
欄位	描述
基礎資料夾	指定應用程式伺服器的位置。
主機	指定應用程式伺服器的主機名稱或 IP 位址。
連接埠	指定應用程式伺服器的監聽程式連接埠號碼。預設的 JBoss 連接埠爲 8080。

2 按「*下一步*」，然後繼續「選擇應用程式伺服器組態類型」(第 43 頁)。

4.12 啓用 Novell Audit 記錄

(選擇性) 若要啓用「使用者應用程式」的 Novell Audit 記錄：

1 填寫下列欄位：



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

2 按「*下一步*」，然後繼續 「設定使用者應用程式組態」(第 48 頁)。

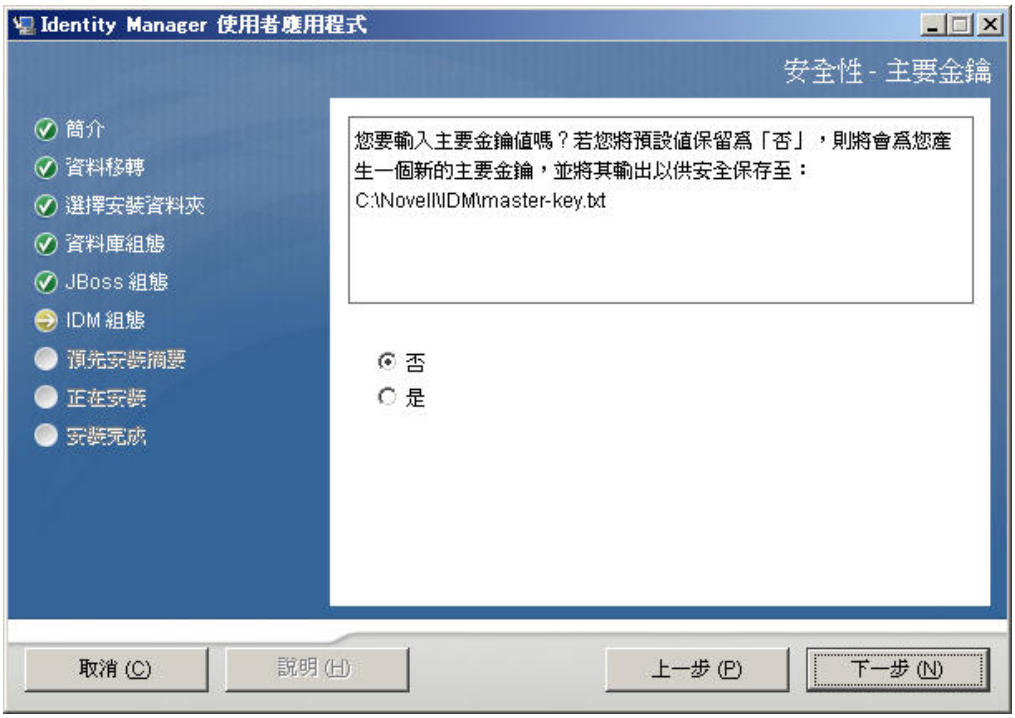
4.13 指定萬能金鑰

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

- 您想將安裝從預備系統移到生產系統，並想保留您在預備系統中使用的資料庫存取權限。
- 您之前將「使用者應用程式」安裝在 JBoss 叢集的第一個成員上，而現在要安裝在叢集的後續成員上 (它們需要同一個萬能金鑰)。

- 由於磁碟發生錯誤，您必須還原「使用者應用程式」。您必須重新安裝「使用者應用程式」，並指定先前安裝所使用的同一個加密萬能金鑰。這可讓您存取之前儲存的加密資料。

1 按一下「*是*」來使用現有的萬能金鑰，或按一下「*否*」來建立一個新的。



2 按一下「*下一步*」。

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

如果您選擇「*否*」，則請跳至「設定使用者應用程式組態」(第 48 頁)。完成安裝之後，您必須手動記錄「記錄萬能金鑰」(第 95 頁)中所述的萬能金鑰。

如果您選擇「*是*」，則請繼續進行步驟 3。

3 如果您選擇輸入現有的加密萬能金鑰，請剪下此金鑰並貼進安裝程序視窗。

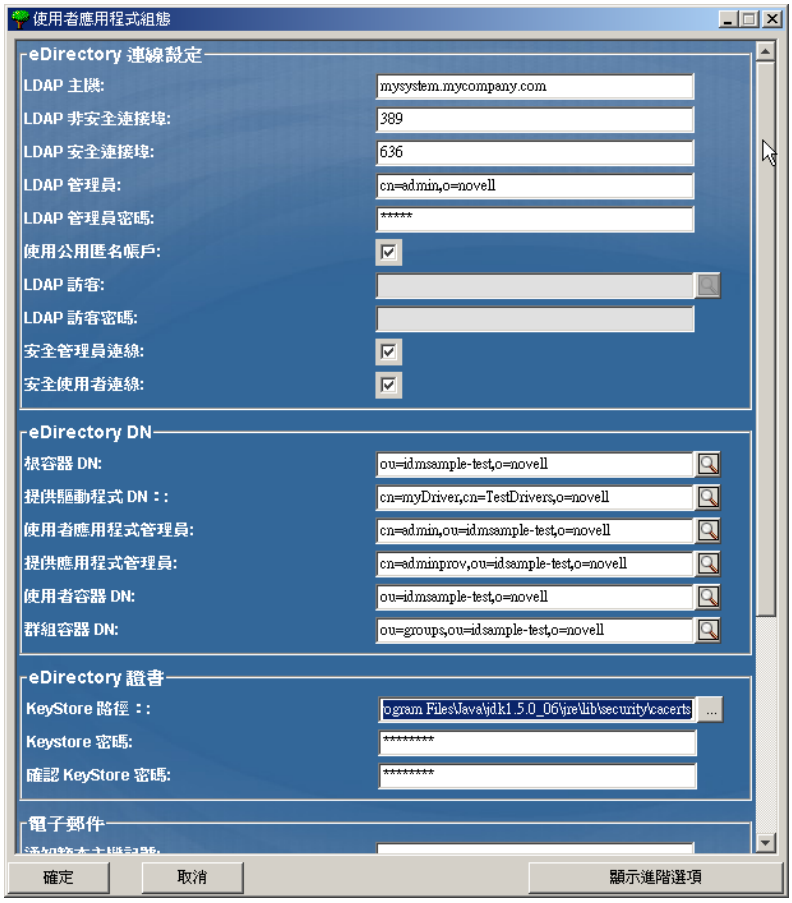
4 按 *「下一步」*。

4.14 設定使用者應用程式組態

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

對於叢集，請爲叢集的每一個成員指定同一個 「使用者應用程式」組態參數。

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


使用者應用程式組態
eDirectory 連線設定
LDAP 主機:
mysystem.mycompany.com
LDAP 非安全連接埠:
389
LDAP 安全連接埠:
636
LDAP 管理員:
cn=admin,o=novell
LDAP 管理員密碼:
*****
使用公用匿名帳戶:
LDAP 訪客:
LDAP 訪客密碼:
安全管理員連線:
安全使用者連線:
eDirectory DN
根容器 DN:
ou=idmsample-test,o=novell
提供驅動程式 DN ::
cn=myDriver,cn=TestDrivers,o=novell
使用者應用程式管理員:
cn=admin,ou=idmsample-test,o=novell
提供應用程式管理員:
cn=adminprov,ou=idsample-test,o=novell
使用者容器 DN:
ou=idmsample-test,o=novell
群組容器 DN:
ou=groups,ou=idsample-test,o=novell
eDirectory 證書
KeyStore 路徑 ::
ogram Files\Java\jdk1.5.0_06\jre\lib\security\cacerts
Keystore 密碼:
****
確認 KeyStore 密碼:
****
電子郵件
確定
取消
顯示進階選項

表格 4-1 使用者應用程式組態：基本參數

設定類型	欄位	描述
eDirectory 連線設定	*LDAP 主機*	必要。指定輕量目錄存取協定 (LDAP) 伺服器的主機名稱或 IP 位址。例如： `myLDAPhost`
	LDAP 非安全連接埠	指定 LDAP 伺服器的非安全連接埠。例如： 389。
	LDAP 安全連接埠	指定 LDAP 伺服器的安全連接埠。例如： 636。
	LDAP 管理員	必要。指定 LDAP 管理員的認證。此使用者必須已經存在。「使用者應用程式」會使用此帳戶，來建立 Identity Vault 的管理連線。這個值會根據萬能金鑰進行加密。
	LDAP 管理員密碼	必要。指定 LDAP 管理員密碼。這個密碼會根據萬能金鑰進行加密。
	使用公用匿名帳戶	允許未登入的使用者存取「LDAP 公用匿名帳戶」。
	LDAP 訪客	允許未登入的使用者存取允許的入口網站應用程式。這個使用者帳戶必須已存在於 Identity Vault。若要啓用「LDAP 訪客」，您必須取消選取「*使用公用匿名帳戶*」。若要停用「訪客使用者」，請選取「*使用公用匿名帳戶*」。
	LDAP 訪客密碼	指定 LDAP 訪客密碼。
	安全管理員連線	選取這個選項來要求，必須以安全插槽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	欄位	描述
eDirectory DN	*根容器 DN*	必要。指定根容器的輕量目錄存取協定 (LDAP) 可辨識名稱。當在目錄抽象層中沒有指定任何搜尋根部時，會將它用做預設實體定義搜尋根部。
	提供驅動程式 DN	必要。指定您先前在「在 iManager 中建立使用者應用程式驅動程式」(第 29 頁) 中建立之「使用者應用程式」驅動程式的可辨識名稱。例如，如果您的驅動程式爲 UserApplicationDriver、而驅動程式集稱爲 myDriverSet，並且該驅動程式集位於 o=myCompany 的網路位置，則輸入值： `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`
	使用者應用程式管理員	必要。Identity Vault 中擁有權限執行管理任務 (由「使用者應用程式」使用者容器指定) 的使用者。此使用者可以使用「使用者應用程式」的「*管理*」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*」索引標籤) 中公開的工作流程管理任務，您就必須給予此管理員適當的託管者權限，使其能夠存取「使用者應用程式」驅動程式中的物件例項。如需詳細資訊，請參閱 *《IDM 使用者應用程式：管理指南》*。 若想在部署「使用者應用程式」之後變更此指定，則必須使用「使用者應用程式」中的「*管理* > *安全性*」頁面。
	提供應用程式管理員	「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「提供應用程式管理員」。 若想在部署「使用者應用程式」之後變更此指定，則必須使用「使用者應用程式」中的「*管理* > *安全性*」頁面。
eDirectory DN (續)	*角色管理員*	此角色用於「Novell Identity Manager 角色提供模組」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。

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

設定類型	欄位	描述
	忘記密碼連結	此 URL 指向「忘記密碼」功能頁面。在外部或內部的密碼管理 WAR 中指定 ForgotPassword.jsf 檔案。如需詳細資料，請參閱「使用密碼 WAR」(第 58 頁)。
	忘記密碼回傳連結	如果您使用外部密碼管理 WAR，則請提供該外部「密碼管理 WAR」用來透過 Web 服務喚回「使用者應用程式」的路徑，例如 https://*idmhost:sslport*/idm。

2 如果您想設定「使用者應用程式」其他的組態參數，請按一下「*顯示進階選項*」(請捲動檢視整個面板)。表格 4-2 描述了「進階選項」參數。

如果您不想設定此步驟所述的其他參數，請跳至步驟 3。

表格 4-2 *使用者應用程式組態：所有參數*

設定類型	欄位	描述
eDirectory 連線設定	*LDAP 主機*	必要。指定 LDAP 伺服器的主機名稱或 IP 位址。例如： myLDAPhost
	LDAP 非安全連接埠	指定 LDAP 伺服器的非安全連接埠。例如： 389。
	LDAP 安全連接埠	指定 LDAP 伺服器的安全連接埠。例如： 636。
	LDAP 管理員	必要。指定 LDAP 管理員的認證。此使用者必須已經存在。「使用者應用程式」會使用此帳戶，來建立 Identity Vault 的管理連線。這個值會根據萬能金鑰進行加密。
	LDAP 管理員密碼	必要。指定 LDAP 管理員密碼。這個密碼會根據萬能金鑰進行加密。
	使用公用匿名帳戶	允許未登入的使用者存取「LDAP 公用匿名帳戶」。
	LDAP 訪客	允許未登入的使用者存取允許的入口網站應用程式。這個使用者帳戶必須已存在於 Identity Vault。若要啓用「LDAP 訪客」，您必須取消選取「*使用公用匿名帳戶*」。若要停用「訪客使用者」，請選取「*使用公用匿名帳戶*」。
	LDAP 訪客密碼	指定 LDAP 訪客密碼。
	安全管理員連線	選取這個選項來要求，必須以安全插槽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	欄位	描述
eDirectory DN	*根容器 DN*	必要。指定根容器的輕量目錄存取協定 (LDAP) 可辨識名稱。當在目錄抽象層中沒有指定任何搜尋根部時，會將它用做預設實體定義搜尋根部。
	提供驅動程式 DN	必要。指定您先前在「在 iManager 中建立使用者應用程式驅動程式」(第 29 頁)中建立之「使用者應用程式」驅動程式的可辨識名稱。例如，如果您的驅動程式爲 userapplicationdriver、而驅動程式集稱爲 mydriverset，並且該驅動程式集位於 o=myCompany 的網路位置，則輸入值： `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`
	使用者應用程式管理員	必要。Identity Vault 中擁有權限執行管理任務 (由「使用者應用程式」使用者容器指定) 的使用者。此使用者可以使用「使用者應用程式」的「*管理*」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*」索引標籤) 中公開的工作流程管理任務，您就必須給予此管理員適當的託管者權限，使其能夠存取「使用者應用程式」驅動程式中的物件例項。如需詳細資訊，請參閱 *《IDM 使用者應用程式：管理指南》*。 若想在部署「使用者應用程式」之後變更此指定，則必須使用「使用者應用程式」中的「*管理* > *安全性*」頁面。
	提供應用程式管理員	「提供應用程式管理員」會管理透過「使用者應用程式」的「*申請與核准*」索引標籤提供的提供工作流程功能。此使用者必須先存在於 Identity Vault，才能指定爲「提供應用程式管理員」。 若想在部署「使用者應用程式」之後變更此指定，則必須使用「使用者應用程式」中的「*管理* > *安全性*」頁面。

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

設定類型	欄位	描述
私密金鑰儲存區	*私密 KeyStore 路徑*	私密 KeyStore 含有「使用者應用程式」的私密金鑰和證書。保留。如果您想保留空白，此路徑則預設爲 /jre/lib/security/cacerts。
	私密 KeyStore 密碼	除非您另行指定，否則密碼爲 changeit。這個密碼會根據萬能金鑰進行加密。
	私密金鑰別名	除非您另行指定，否則密碼爲 novellIDMUserApp。
	私密金鑰密碼	除非您另行指定，否則密碼爲 nove1lIDM。這個密碼會根據萬能金鑰進行加密。
託管金鑰儲存區	*託管儲存區路徑*	「託管金鑰儲存區」包含所有託管簽名者的證書，用來驗證數位簽名。如果此路徑爲空，則「使用者應用程式」會從「系統」內容 javax.net.ssl.trustStore 取得路徑。如果路徑不在那裡，就假設爲 jre/lib/security/cacerts。
	託管儲存區密碼	如果此欄位爲空，則「使用者應用程式」會從「系統」內容 javax.net.ssl.trustStorePassword 取得密碼。如果值不在那裡，則使用 changeit。這個密碼會根據萬能金鑰進行加密。
Novell Audit 數位簽名和證書金鑰		包含 Novell Audit 的數位簽名金鑰和證書。
	Novell Audit 數位簽名證書	顯示數位簽名證書。
	Novell Audit 數位簽名私密金鑰	顯示數位簽名私密金鑰。這個金鑰會根據萬能金鑰進行加密。
Access Manager 和 iChain 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同時登出頁面。
	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「同時登出」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。以下兩個 URL 會視您的環境將同時登出功能導向至正確的頁面： Access Manager：https://yourAccessGatewayServer/AGLogout iChain：https://youriChainServer/cmd/ICSLogout

設定類型	欄位	描述
電子郵件	*通知範本 HOST 記號*	指定代管「Identity Manager 使用者應用程式」的應用程式伺服器。例如： `myapplication serverServer` 此值會取代電子郵件範本中的 $HOST$ 記號。建構的 URL 是提供申請任務和核准通知的連結。
	通知範本 PORT 記號	用於取代提供申請任務和核准通知中所使用之電子郵件範本中的 $PORT$ 記號。
	通知範本 SECURE PORT 記號	用於取代提供申請任務和核准通知中所使用之電子郵件範本中的 $SECURE_PORT$ 記號。
	通知範本 PROTOCOL 記號	指的是非安全通訊協定 HTTP。用於取代提供申請任務和核准通知中所使用之電子郵件範本中的 $PROTOCOL$ 記號。
	通知範本 SECURE PROTOCOL 記號	指的是安全通訊協定 HTTPS。用於取代提供申請任務和核准通知中所使用之電子郵件範本中的 $SECURE_PROTOCOL$ 記號。
	SMTP 電子郵件通知寄件者：	指定來自提供電子郵件中使用者的電子郵件。
	SMTP 電子郵件通知主機	指定提供電子郵件所使用的 SMTP 電子郵件主機。可以是 IP 位址或 DNS 名稱。
密碼管理		
	使用外部密碼 WAR	此功能可讓您指定一個「忘記密碼」頁面放在外部「忘記密碼 WAR」中，並指定一個 URL，讓外部「忘記密碼 WAR」用來透過 Web 服務喚回「使用者應用程式」。 如果您核取「*使用外部密碼 WAR*」，就必須提供「*忘記密碼連結*」和「*忘記密碼回傳連結*」的值。 如果您不勾選「*使用外部密碼 WAR*」，IDM 就會使用預設的內部「密碼管理」功能，./jsps/pwdmgt/ForgotPassword.jsf (開頭不使用 HTTP 通訊協定)。這會將使用者重新導向至「使用者應用程式」內建的「忘記密碼」功能，而不是外部 WAR。
	忘記密碼連結	此 URL 指向「忘記密碼」功能頁面。在外部或內部的密碼管理 WAR 中指定 ForgotPassword.jsf 檔案。如需詳細資料，請參閱 「使用密碼 WAR」(第 58 頁)。
	忘記密碼回傳連結	如果您使用外部密碼管理 WAR，則請提供該外部「密碼管理 WAR」用來透過 Web 服務喚回「使用者應用程式」的路徑，例如 https://*idmhost:sslport*/idm。

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

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

3 完成設定後，請按一下「*確定*」，然後繼續進行 「確認您的選擇後進行安裝」(第 59 頁)

4.15 使用密碼 WAR

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

- 「指定外部密碼管理 WAR」(第 58 頁)
- 「指定內部密碼 WAR」(第 59 頁)

4.15.1 指定外部密碼管理 WAR

1 使用安裝程序或 configupdate 公用程式。

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

3 如需「*忘記密碼連結*」組態參數，請指定外部密碼 WAR 的位置。

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

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

回傳連結必須使用 SSL 來確保和「使用者應用程式」之間的 Web 服務通訊安全無虞。並請參閱「設定 JBoss 伺服器之間的 SSL 通訊」(第 96 頁)。

5 請執行下列其中一個步驟：

- 如果您使用安裝程式，則請閱讀此步驟中的資訊，然後繼續前往步驟 6, 第 59 頁。
- 如果您使用 configupdate 公用程式來更新安裝根目錄中的外部密碼 WAR，則請閱讀此步驟，並手動將 WAR 重新命名爲您在「*忘記密碼連結*」中所指定的第一個目錄。然後繼續前往步驟 6, 第 59 頁。

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

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

4.15.2 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。

4.16 確認您的選擇後進行安裝

1 閱讀「預先安裝摘要」頁面，確認您選擇的安裝參數。

2 *如有必要，請使用「上一步」，返回先前的安裝頁面變更安裝參數。*

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

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

4.17 檢視記錄檔

1 如果安裝完成時未發生任何錯誤，請移至第 7 章 「安裝後任務」(第 95 頁)。

2 如果安裝發生錯誤或警告，請檢閱記錄檔案來找出問題。

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

如需解決問題的說明，請參閱「疑難排解」(第 98 頁)。

透過主控台或使用單個指令進行安裝

5

本節說明的安裝方法可用於取代第 4 章 「在 JBoss 上使用 GUI 進行安裝」(第 35 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：

- 「透過主控台安裝使用者應用程式」(第 61 頁)
- 「使用單一指令安裝使用者應用程式」(第 61 頁)

5.1 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」。

1. 取得表格 2-1 頁上 24 中所描述的適當安裝檔案。
2. 登入並開啓終端機會期。
3. 使用 Java 啓動平台的安裝程式，如下所示：

   java -jar IdmUserApp.jar -i console
4. 請依照第 4 章 「在 JBoss 上使用 GUI 進行安裝」(第 35 頁) 下所述的圖形使用者介面執行相同的步驟，閱讀指令行的提示並在指令行中輸入回應，然後繼續執行萬能金鑰的輸入或建立步驟。
5. 若要設定 「使用者應用程式」組態參數，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 「設定使用者應用程式組態」(第 48 頁) 中所述的值。
6. 如果您使用的是外部密碼管理 WAR，請手動將其複製到安裝目錄以及負責執行外部密碼 WAR 功能的遠端 JBoss 伺服器部署目錄中。
7. 請繼續進行第 7 章 「安裝後任務」(第 95 頁)。

5.2 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 頁上 24 中所列的適當安裝檔案。
2. 登入並開啓終端機會期。
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 5-1。「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 / *yourdirectorypath*/silent.properties

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

表格 5-1 *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。 必要。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。 必要。指定 LDAP 管理員的認證。此使用者必須已經存在。「使用者應用程式」會使用此帳戶，來建立 Identity Vault 的管理連線。這個值會根據萬能金鑰進行加密。
NOVL_CONFIG_LDAPADMINPASS=	eDirectory 連線設定：LDAP 管理員密碼。 必要。指定 LDAP 管理員密碼。這個密碼會根據萬能金鑰進行加密。
NOVL_CONFIG_ROOTCONTAINERNAME=	eDirectory DN：根容器 DN。 必要。指定根容器的輕量目錄存取協定 (LDAP) 可辨識名稱。當在目錄抽象層中沒有指定任何搜尋根部時，會將它用做預設實體定義搜尋根部。
NOVL_CONFIG_PROVISIONROOT=	eDirectory DN：提供驅動程式 DN。 必要。指定您先前在「在 iManager 中建立使用者應用程式驅動程式」(第 29 頁) 中建立之「使用者應用程式」驅動程式的可辨識名稱。例如，如果您的驅動程式爲 userapplicationdriver、而驅動程式集稱爲 mydriverset，並且該驅動程式集位於 o=myCompany 的網路位置，則輸入值： `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`
NOVL_CONFIG_LOCKSMITH=	eDirectory DN：使用者應用程式管理員。 必要。Identity Vault 中擁有權限執行管理任務 (由「使用者應用程式」使用者容器指定) 的使用者。此使用者可以使用「使用者應用程式」的「*管理*」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*」索引標籤) 中公開的工作流程管理任務，您就必須給予此管理員適當的託管者權限，使其能夠存取「使用者應用程式」驅動程式中的物件例項。如需詳細資訊，請參閱 *《IDM 使用者應用程式：管理指南》*。 若想在部署「使用者應用程式」之後變更此指定，則必須使用「使用者應用程式」中的「*管理* > *安全性*」頁面。

silent.properties 中的使用者應用程式參數名稱	使用者應用程式組態參數檔案中的同等參數
NOVL_CONFIG_PROVLOCKSMITH=	eDirectory DN：提供應用程式管理員。 此角色可用於 Identity Manager 的提供版本。「提供應用程式管理員」會使用「*管理*」索引標籤之下的「*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 「提供應用程式管理員」。 若想在部署 「使用者應用程式」之後變更此指定，則必須使用 「使用者應用程式」中的 「*管理* > *安全性*」頁面。
NOVL_CONFIG_ROLECONTAINERDN=	此角色用於 「Novell Identity Manager 角色提供模組」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_USERCONTAINERDN=	中繼目錄使用者身份：使用者容器 DN。 必要。指定使用者容器的 LDAP 可辨識名稱 (DN) 或完全合法的 LDAP 名稱。這會定義使用者和群組的搜尋範圍。此容器中 (和下方) 的使用者可以登入「使用者應用程式」。 **重要：**如果您想讓使用者可以執行工作流程，請確定 「使用者應用程式」驅動程式設定期間指定的「使用者應用程式管理員」存在於此容器中。
NOVL_CONFIG_GROUPCONTAINERDN=	中繼目錄使用者群組：群組容器 DN。 必要。指定群組容器的輕量目錄存取協定 (LDAP) 可辨識名稱 (DN) 或完全合法的 LDAP 名稱。由目錄抽象層內的實體定義使用。
NOVL_CONFIG_KEYSTOREPATH=	eDirectory 證書：KeyStore 路徑。必要。 針對應用程式伺服器用來執行之 JRE 的 KeyStore (cacerts) 檔案，輸入其完整路徑。「使用者應用程式」的安裝會修改 KeyStore 檔案。在 Linux 或 Solaris 上，使用者必須擁有權限寫入此檔案。
NOVL_CONFIG_KEYSTOREPASSWORD=	eDirectory 證書：KeyStore 密碼。 必要。指定 cacerts 密碼。預設值爲 「changeit」。

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_SECUREADMINCONNECTION=	eDirectory 連線設定：安全管理員連線。 指定 *True* 來要求，必須以安全插槽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。 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：會期逾時。 指定應用程式會期逾時間隔。
NOVL_CONFIG_LDAPPLAINPORT=	eDirectory 連線設定：LDAP 非安全連接埠。 指定 LDAP 伺服器的非安全連接埠，例如 389。
NOVL_CONFIG_LDAPSECUREPORT=	eDirectory 連線設定：LDAP 安全連接埠。 指定 LDAP 伺服器的安全連接埠，例如 636。
NOVL_CONFIG_ANONYMOUS=	eDirectory 連線設定：使用公用匿名帳戶。 指定 *True*，允許未登入的使用者存取「LDAP 公用匿名帳戶」。 指定 *False* 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 是提供申請任務和核准通知的連結。
NOVL_CONFIG_EMAILNOTIFYPORT=	電子郵件：通知範本 PORT 記號。 用於取代提供申請任務和核准通知中所使用之電子郵件範本中的 $PORT$ 記號。

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_EMAILNOTIFYSECUREPORT=	電子郵件：通知範本 SECURE PORT 記號。 用於取代提供申請任務和核准通知中所使用之電子郵件範本中的 $SECURE_PORT$ 記號。
NOVL_CONFIG_NOTFSMTPEMAILFROM=	電子郵件：SMTP 電子郵件通知寄件者。 指定來自提供電子郵件中使用者的電子郵件。
NOVL_CONFIG_NOTFSMTPEMAILHOST=	電子郵件：SMTP 電子郵件通知主機。 指定提供電子郵件所使用的 SMTP 電子郵件主機。可以是 IP 位址或 DNS 名稱。
NOVL_CONFIG_USEEXTPWDWAR=	密碼管理：使用外部密碼 WAR。 如果您使用的是外部密碼管理 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.jsf (開頭不使用 HTTP 通訊協定)。這會將使用者重新導向至「使用者應用程式」內建的「忘記密碼」功能，而不是外部 WAR。
NOVL_CONFIG_EXTPWDWARPATH=	密碼管理：忘記密碼連結。 在外部或內部的密碼管理 WAR 中指定「忘記密碼」功能頁面 ForgotPassword.jsf 的 URL。或者，接受預設的內部密碼管理 WAR。如需詳細資料，請參閱 「使用密碼 WAR」(第 58 頁)。
NOVL_CONFIG_EXTPWDWARRTNPATH=	密碼管理：忘記密碼回傳連結。 如果您使用外部密碼管理 WAR，則請提供該外部「密碼管理 WAR」用來透過 Web 服務喚回「使用者應用程式」的路徑，例如 https://*idmhost:sslport*/idm。
NOVL_CONFIG_USEROBJECTATTRIBUTE=	中繼目錄使用者身份：使用者物件類別。 LDAP 使用者物件類別 (通常爲 inetOrgPerson)。
NOVL_CONFIG_LOGINATTRIBUTE=	中繼目錄使用者身份：登入屬性。 代表使用者登入名稱的 LDAP 屬性 (例如 CN)。
NOVL_CONFIG_NAMINGATTRIBUTE=	中繼目錄使用者身份：命名屬性。 此 LDAP 可在查閱使用者或群組時做爲識別碼。這和登入屬性不一樣，後者只能用於登入，不可用於使用者 / 群組搜尋。
NOVL_CONFIG_USERMEMBERSHIPATTRIBUTE=	中繼目錄使用者身分：使用者成員資格屬性。選擇性。 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。

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_GROUPOBJECTATTRIBUTE=	中繼目錄使用者群組：群組物件類別。 LDAP 群組物件類別 (通常爲 groupofNames)。
NOVL_CONFIG_GROUPMEMBERSHIPATTRIBUTE=	中繼目錄使用者群組：群組成員資格屬性。 指定代表使用者群組成員資格的屬性。請勿在此名稱中使用空格。
NOVL_CONFIG_USEDYNAMICGROUPS=	中繼目錄使用者群組：使用動態群組。 指定 *True* 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。 指定 LDAP 動態群組物件類別 (通常爲 dynamicGroup)。
NOVL_CONFIG_PRIVATESTOREPATH=	私密金鑰儲存區：私密 KeyStore 路徑。 針對含有「使用者應用程式」的私密金鑰和證書的私密 KeyStore，指定其路徑。保留。如果您想保留空白，此路徑則預設爲 /jre/lib/security/cacerts。
NOVL_CONFIG_PRIVATESTOREPASSWORD=	私密金鑰儲存區：私密 KeyStore 密碼。
NOVL_CONFIG_PRIVATEKEYALIAS=	私密金鑰儲存區：私密金鑰別名。 除非您另行指定，否則密碼爲 novellIDMUserApp。
NOVL_CONFIG_PRIVATEKEYPASSWORD=	私密金鑰儲存區：私密金鑰密碼。
NOVL_CONFIG_TRUSTEDSTOREPATH=	託管金鑰儲存區：託管儲存區路徑。 「託管金鑰儲存區」包含所有託管簽名者的證書，用來驗證數位簽名。如果此路徑爲空，則「使用者應用程式」會從「系統」內容 javax.net.ssl.trustStore 取得路徑。如果路徑不在那裡，就假設爲 jre/lib/security/cacerts。
NOVL_CONFIG_TRUSTEDSTOREPASSWORD=	託管金鑰儲存區：託管儲存區密碼。
NOVL_CONFIG_AUDITCERT=	Novell Audit 數位簽名證書
NOVL_CONFIG_AUDITKEYFILEPATH=	Novell Audit 數位簽名私密金鑰檔案路徑
NOVL_CONFIG_ICSLOGOUTENABLED=	Access Manager 和 iChain 設定：同時登出已啓用。 指定 *True*，啓用「使用者應用程式」以及 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。

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_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。用於取代提供申請任務和核准通知中所使用之電子郵件範本中的 $PROTOCOL$ 記號。
NOVL_CONFIG_EMAILNOTIFYSECUREPROTOCOL=	電子郵件：通知範本 SECURE PORT 記號。
NOVL_CONFIG_OCSPURI=	其他：OCSP URI。 如果用戶端安裝使用線上證書狀態通訊協定 (On-Line Certificate Status Protocol，OCSP)，則請提供資源識別字串 (Uniform Resource Identifier，URI)。例如，格式爲 http://hstport/ocspLocal。OCSP URI 會在線上更新託管證書的狀態。
NOVL_CONFIG_AUTHCONFIGPATH=	其他：授權組態路徑。 授權組態檔案的完全合法名稱。

6 在 WebSphere 應用程式伺服器上進行安裝

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

6.1 啓動安裝程式 GUI

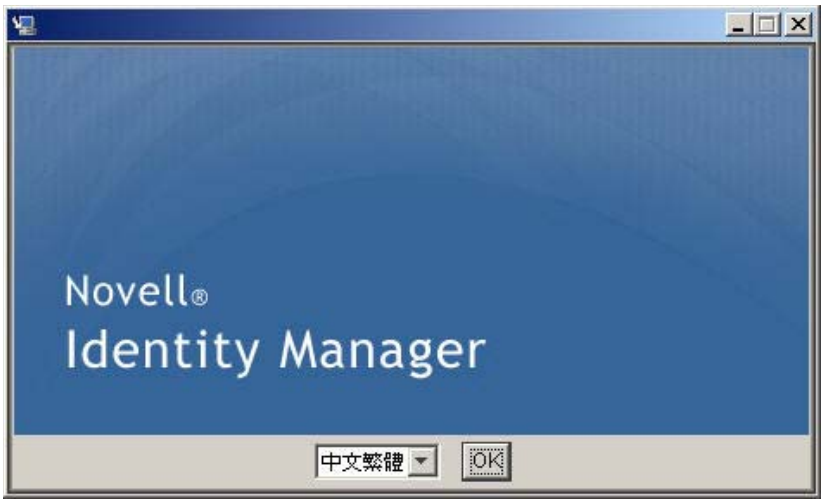
1 瀏覽至含有安裝檔案的目錄，如所述。

2 啓動安裝程式：

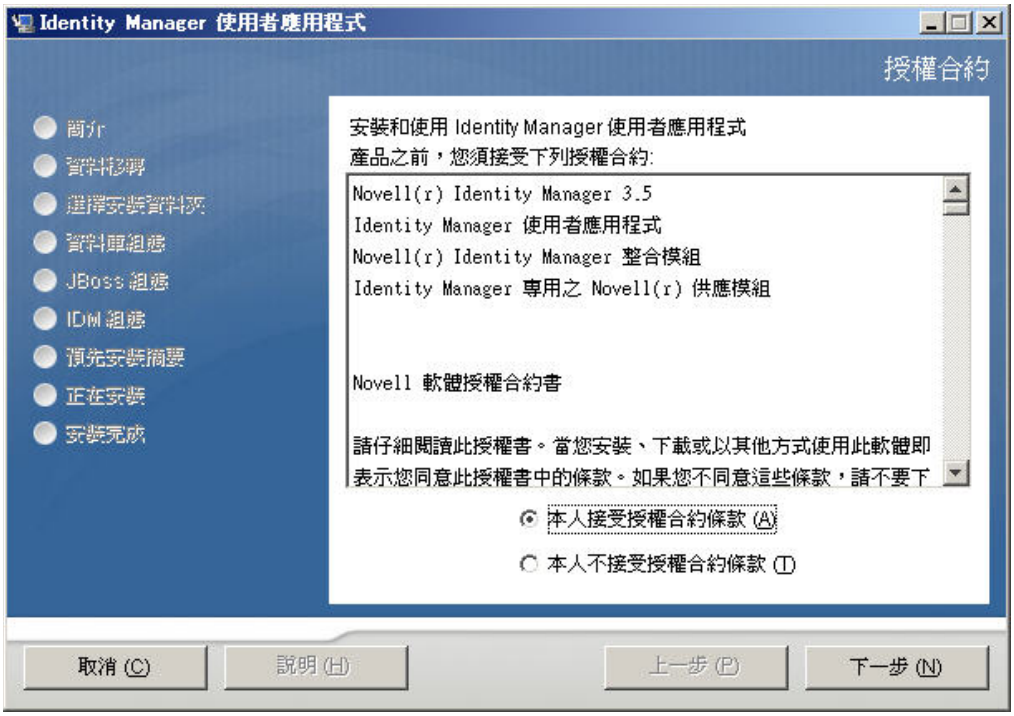
```
java -jar IdmUserApp.jar
```

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

3 在下拉式選單中選取語言，然後按一下「確定」。



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



5 閱讀安裝精靈的「簡介」頁面，然後按一下「*下一步*」。

6.2 選擇應用程式伺服器平台

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

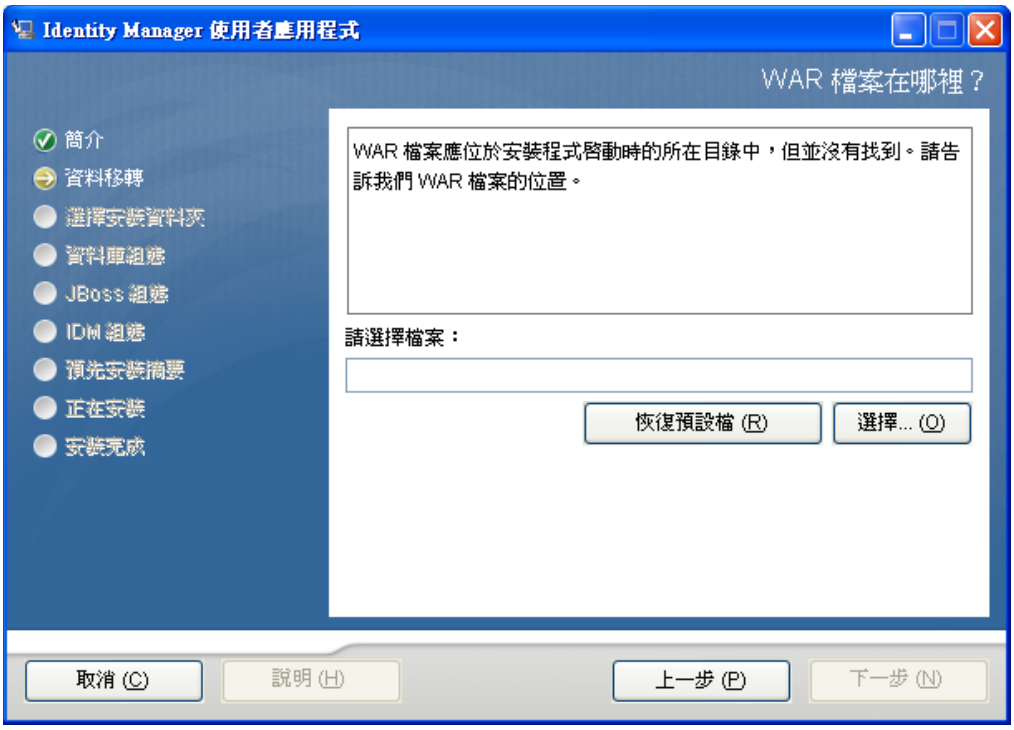
2 選取「*下一步*」。然後繼續執行 「指定 WAR 的位置」(第 71 頁).

6.3 指定 WAR 的位置

完成 「啓動安裝程式 GUI」(第 69 頁) 中的程序，然後繼續執行下面的步驟：

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

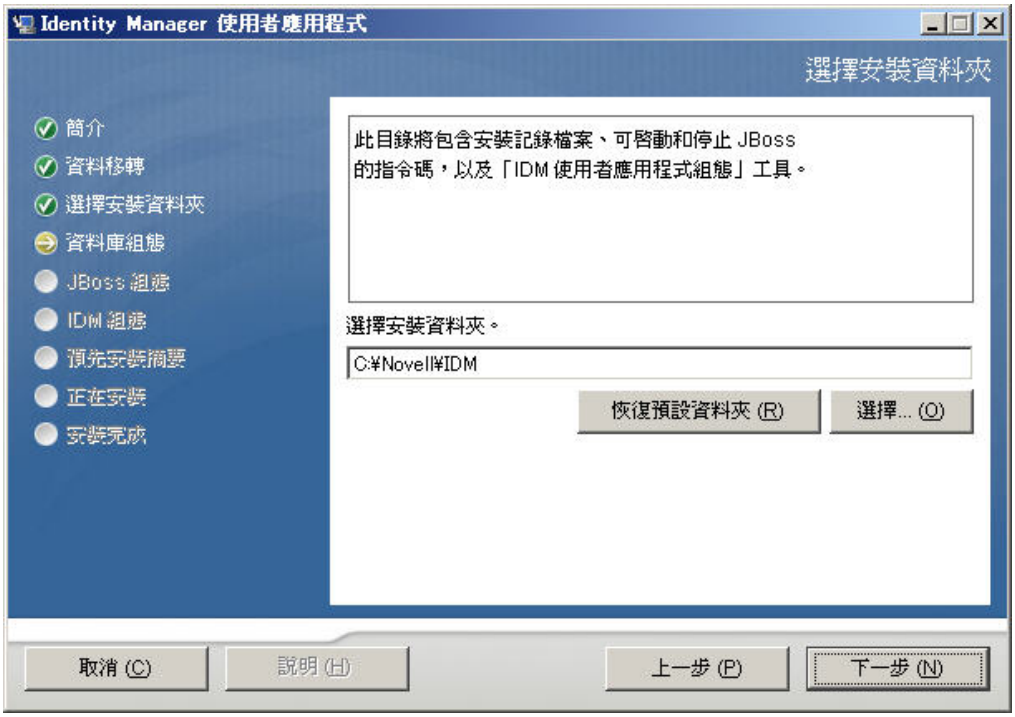
1 如果 WAR 儲存於預設位置，請按一下 「*還原預設資料夾*」。若要指定 WAR 檔案的位置，按一下 「*選擇*」並選取位置。



2 按「*下一步*」，然後繼續「選擇安裝資料夾」(第 72 頁)。

6.4 選擇安裝資料夾

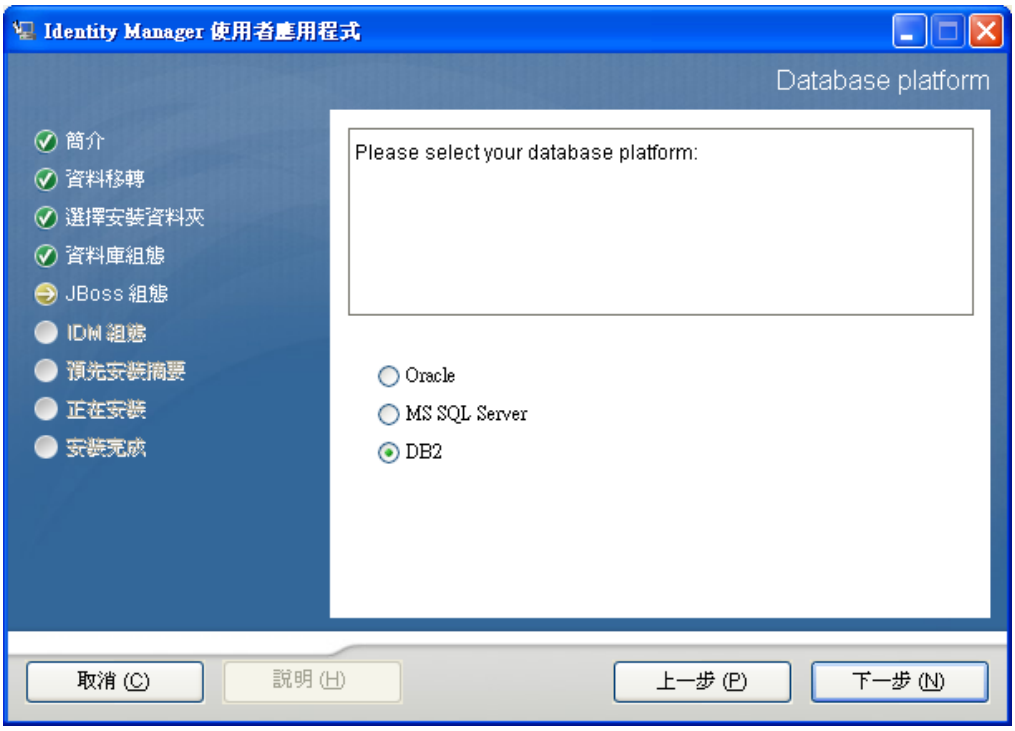
1 在「選擇安裝資料夾」頁面上，選取「使用者應用程式」的安裝位置。如果您要使用預設位置，請按一下「*還原預設資料夾*」，或者，如果想選擇其他位置來存放安裝檔案，請按一下「*選擇*」瀏覽到某個位置。



2 按「*下一步*」，然後繼續「選擇資料庫平台」(第 73 頁)。

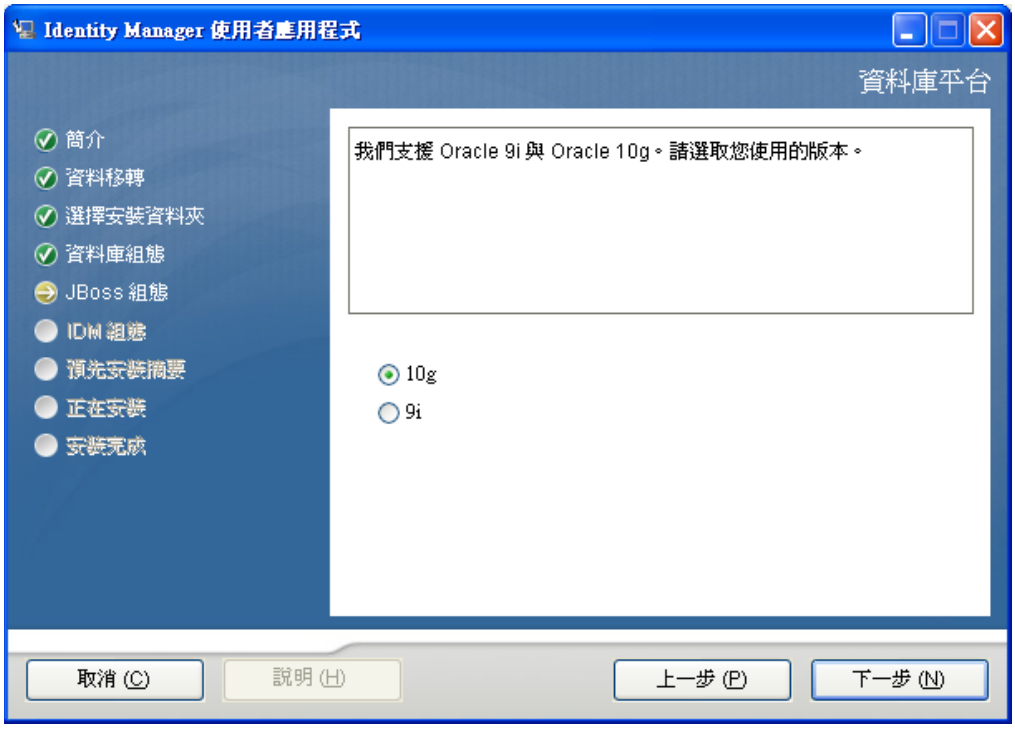
6.5 選擇資料庫平台

1 選取要使用的資料庫平台。



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

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

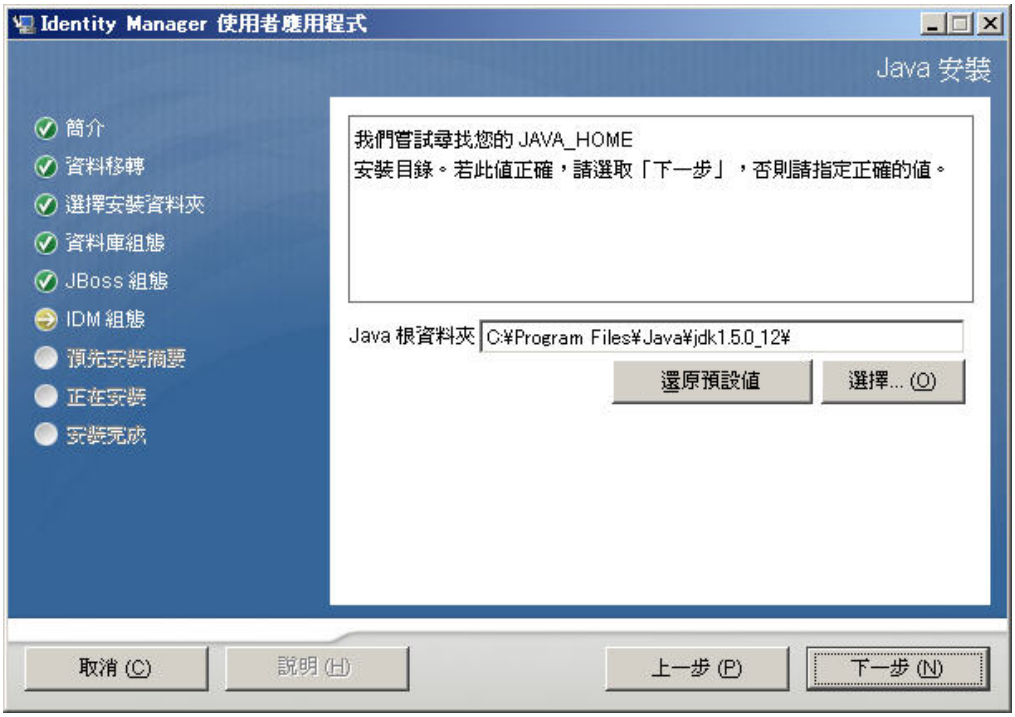


4 按「*下一步*」，然後繼續「指定 Java 根目錄」(第 74 頁)。

6.6 指定 Java 根目錄

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

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

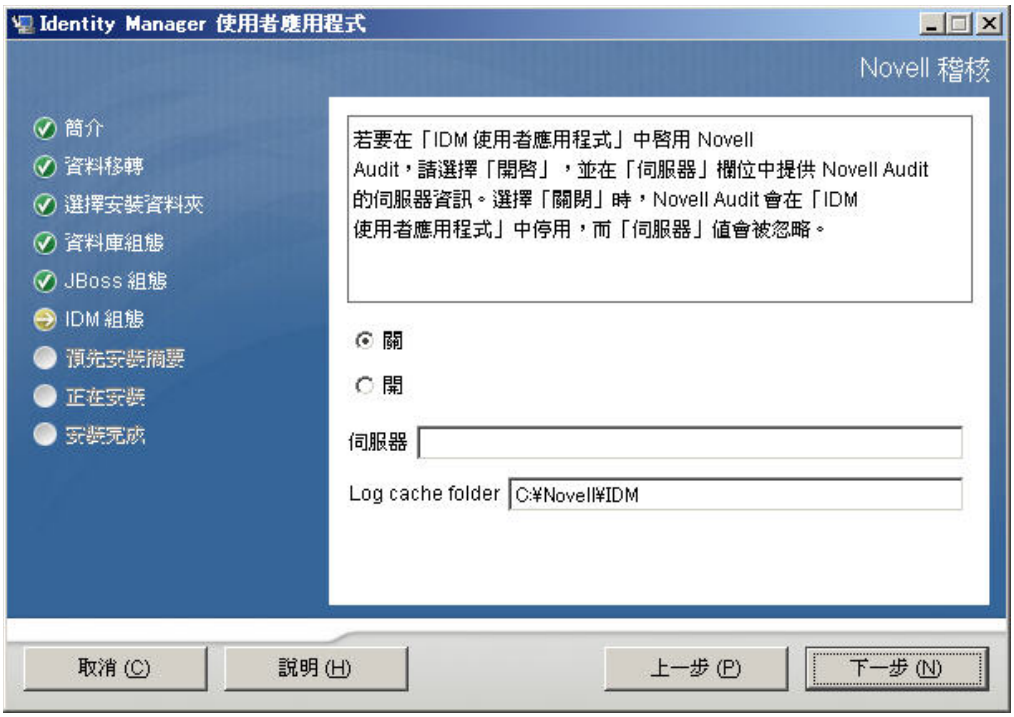


2 按「*下一步*」，然後繼續「啓用 Novell Audit 記錄」(第 75 頁)。

6.7 啓用 Novell Audit 記錄

若要啓用「使用者應用程式」的 Novell® Audit 記錄 (選擇性)：

1 填寫下列欄位：



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

2 按一下「*下一步*」，繼續進行「指定萬能金鑰」(第 76 頁)。

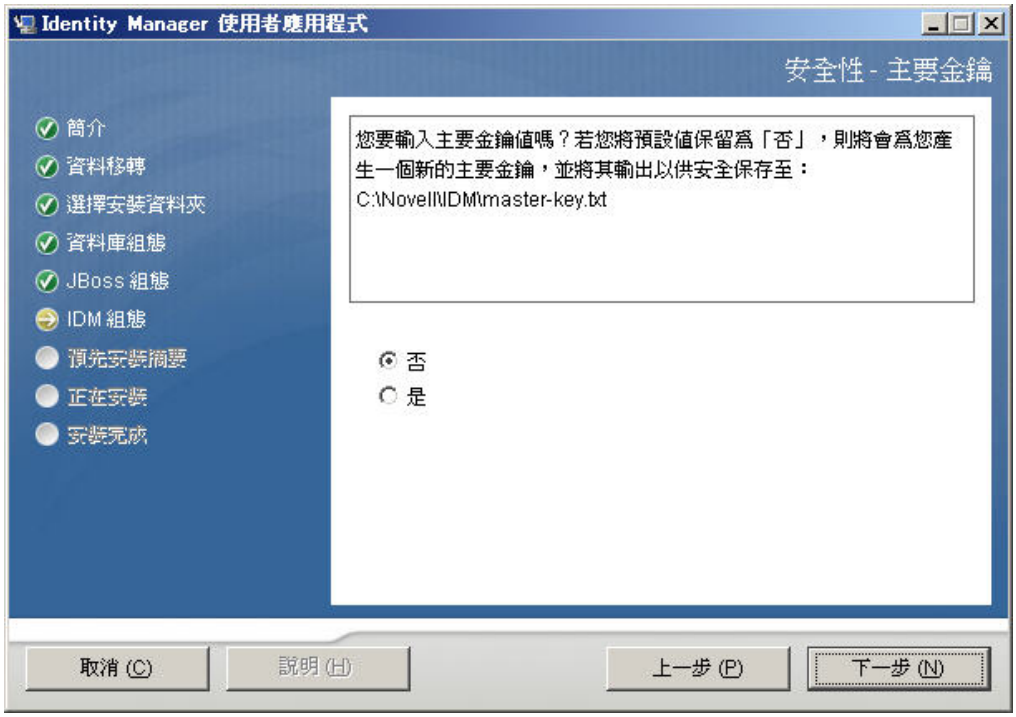
6.8 指定萬能金鑰

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

- 您想將安裝從預備系統移到生產系統，並想保留您在預備系統中使用的資料庫存取權限。

- 您之前將「使用者應用程式」安裝在 叢集的第一個成員上，而現在要安裝在叢集的後續成員上 (它們需要同一個萬能金鑰)。
- 由於磁碟發生錯誤，您必須還原「使用者應用程式」。您必須重新安裝「使用者應用程式」，並指定先前安裝所使用的同一個加密萬能金鑰。這可讓您存取之前儲存的加密資料。

1 按一下「是」來使用現有的萬能金鑰，或按一下「否」來建立一個新的



2 按一下「*下一步*」。

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

如果您選擇「*否*」，則請跳至「設定使用者應用程式組態」(第 78 頁)。在完成安裝後，您必須手動記錄萬能金鑰。如果您選擇「*是*」，請繼續 步驟 3, 第 77 頁。

3 如果您選擇輸入現有的加密萬能金鑰，請剪下此金鑰並貼進安裝程序視窗。

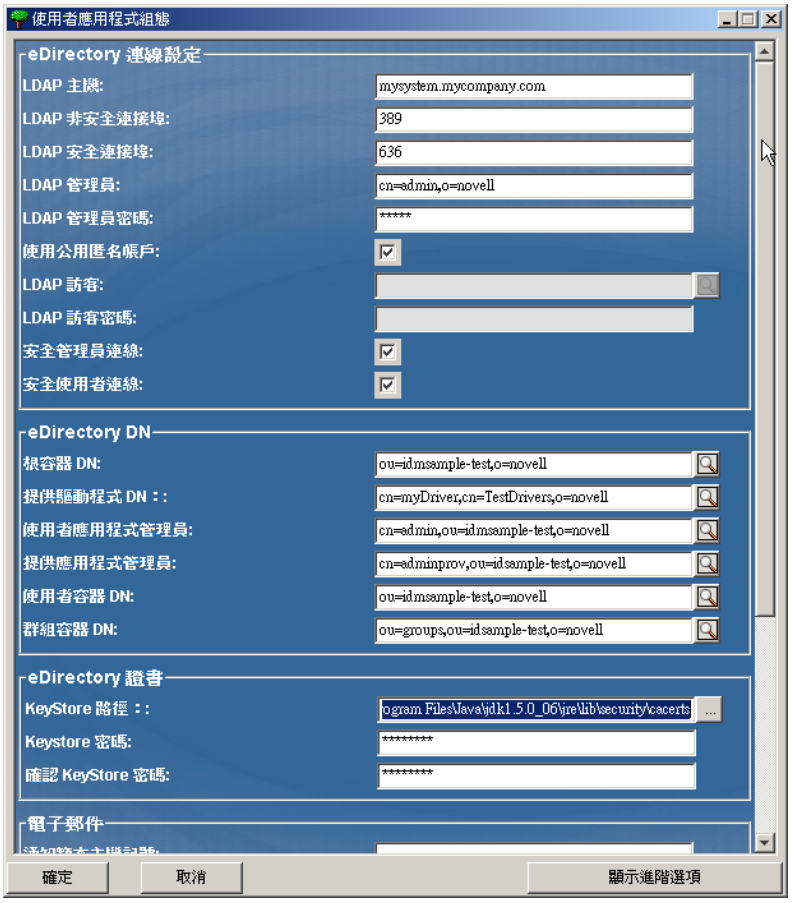
4 按一下「*下一步*」，繼續進行「設定使用者應用程式組態」(第 78 頁)。

6.9 設定使用者應用程式組態

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

1 在第一個「使用者應用程式組態」頁面上，按一下「*下一步*」。

2 設定表 表格 6-1 頁上 81 所述的「使用者應用程式」基本組態參數，然後繼續進行步驟 3。


使用者應用程式組態
eDirectory 連線設定
LDAP 主機:
mysystem.mycompany.com
LDAP 非安全連接埠:
389
LDAP 安全連接埠:
636
LDAP 管理員:
cn=admin,o=novell
LDAP 管理員密碼:
*****
使用公用匿名帳戶:
LDAP 訪客:
LDAP 訪客密碼:
安全管理員連線:
安全使用者連線:
eDirectory DN
根容器 DN:
ou=idmsample-test,o=novell
提供驅動程式 DN：:
cn=myDriver,cn=TestDrivers,o=novell
使用者應用程式管理員:
cn=admin,ou=idmsample-test,o=novell
提供應用程式管理員:
cn=adminprov,ou=idsample-test,o=novell
使用者容器 DN:
ou=idmsample-test,o=novell
群組容器 DN:
ou=groups,ou=idsample-test,o=novell
eDirectory 證書
KeyStore 路徑：:
ogram Files\Java\jdk1.5.0_06\jre\lib\security\cacerts
Keystore 密碼:
****
確認 KeyStore 密碼:
****
電子郵件
確定
取消
顯示進階選項

表格 6-1 *使用者應用程式組態：基本參數*

設定類型	欄位	描述
eDirectory 連線設定	*LDAP 主機*	必要。指定輕量目錄存取協定 (LDAP) 伺服器的主機名稱或 IP 位址。例如： `myLDAPhost`
	LDAP 非安全連接埠	指定 LDAP 伺服器的非安全連接埠。例如： 389。
	LDAP 安全連接埠	指定 LDAP 伺服器的安全連接埠。例如： 636。
	LDAP 管理員	必要。指定 LDAP 管理員的認證。此使用者必須已經存在。「使用者應用程式」會使用此帳戶，來建立 Identity Vault 的管理連線。這個值會根據萬能金鑰進行加密。
	LDAP 管理員密碼	必要。指定 LDAP 管理員密碼。這個密碼會根據萬能金鑰進行加密。
	使用公用匿名帳戶	允許未登入的使用者存取「LDAP 公用匿名帳戶」。
	LDAP 訪客	允許未登入的使用者存取允許的入口網站應用程式。這個使用者帳戶必須已存在於 Identity Vault。若要啓用「LDAP 訪客」，您必須取消選取「*使用公用匿名帳戶*」。若要停用「訪客使用者」，請選取「*使用公用匿名帳戶*」。
	LDAP 訪客密碼	指定 LDAP 訪客密碼。
	安全管理員連線	選取這個選項來要求，必須以安全插槽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	欄位	描述
eDirectory DN	*根容器 DN*	必要。指定根容器的輕量目錄存取協定 (LDAP) 可辨識名稱。當在目錄抽象層中沒有指定任何搜尋根部時，會將它用做預設實體定義搜尋根部。
	提供驅動程式 DN	必要。「使用者應用程式管理員」的可辨識名稱。例如，如果您的驅動程式爲 UserApplicationDriver、而驅動程式集稱爲 myDriverSet，並且該驅動程式集位於 o=myCompany 的網路位置，則輸入值： `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`
	使用者應用程式管理員	必要。Identity Vault 中擁有權限執行管理任務 (由「使用者應用程式」使用者容器指定) 的使用者。此使用者可以使用「使用者應用程式」的「*管理*」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*」索引標籤) 中公開的工作流程管理任務，您就必須給予此管理員適當的託管者權限，使其能夠存取「使用者應用程式」驅動程式中的物件例項。如需詳細資訊，請參閱 *《IDM 使用者應用程式：管理指南》*。 若想在部署「使用者應用程式」之後變更此指定，則必須使用「使用者應用程式」中的「*管理* > *安全性*」頁面。
	提供應用程式管理員	「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「提供應用程式管理員」。 若想在部署「使用者應用程式」之後變更此指定，則必須使用「使用者應用程式」中的「*管理* > *安全性*」頁面。
eDirectory DN (續)	*角色管理員*	此角色用於「Novell Identity Manager 角色提供模組」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。

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

設定類型	欄位	描述
	忘記密碼連結	此 URL 指向「忘記密碼」功能頁面。在外部或內部的密碼管理 WAR 中指定 ForgotPassword.jsf 檔案。
	忘記密碼回傳連結	如果您使用外部密碼管理 WAR，則請提供該外部「密碼管理 WAR」用來透過 Web 服務喚回「使用者應用程式」的路徑，例如 https://*idmhost:sslport*/idm。

3 如果您想設定「使用者應用程式」其他的組態參數，請按一下「*顯示進階選項*」(請捲動檢視整個面板)。表格 6-2 頁上 84 描述了「進階選項」參數。如果您不想設定此步驟所述的其他參數，請跳至步驟 4。

表格 6-2 *使用者應用程式組態：所有參數*

設定類型	欄位	描述
eDirectory 連線設定	*LDAP 主機*	必要。指定 LDAP 伺服器的主機名稱或 IP 位址。例如： myLDAPhost
	LDAP 非安全連接埠	指定 LDAP 伺服器的非安全連接埠。例如： 389。
	LDAP 安全連接埠	指定 LDAP 伺服器的安全連接埠。例如： 636。
	LDAP 管理員	必要。指定 LDAP 管理員的認證。此使用者必須已經存在。「使用者應用程式」會使用此帳戶，來建立 Identity Vault 的管理連線。這個值會根據萬能金鑰進行加密。
	LDAP 管理員密碼	必要。指定 LDAP 管理員密碼。這個密碼會根據萬能金鑰進行加密。
	使用公用匿名帳戶	允許未登入的使用者存取「LDAP 公用匿名帳戶」。
	LDAP 訪客	允許未登入的使用者存取允許的入口網站應用程式。這個使用者帳戶必須已存在於 Identity Vault。若要啓用「LDAP 訪客」，您必須取消選取「*使用公用匿名帳戶*」。若要停用「訪客使用者」，請選取「*使用公用匿名帳戶*」。
	LDAP 訪客密碼	指定 LDAP 訪客密碼。
	安全管理員連線	選取這個選項來要求，必須以安全插槽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	欄位	描述
eDirectory DN	*根容器 DN*	必要。指定根容器的輕量目錄存取協定 (LDAP) 可辨識名稱。當在目錄抽象層中沒有指定任何搜尋根部時，會將它用做預設實體定義搜尋根部。
	提供驅動程式 DN	必要。「使用者應用程式管理員」的可辨識名稱。例如，如果您的驅動程式爲 userapplicationdriver、而驅動程式集稱爲 mydriverset，並且該驅動程式集位於 o=myCompany 的網路位置，則輸入值： `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`
	使用者應用程式管理員	必要。Identity Vault 中擁有權限執行管理任務 (由「使用者應用程式」使用者容器指定) 的使用者。此使用者可以使用「使用者應用程式」的「*管理*」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*」索引標籤) 中公開的工作流程管理任務，您就必須給予此管理員適當的託管者權限，使其能夠存取「使用者應用程式」驅動程式中的物件例項。如需詳細資訊，請參閱*《IDM 使用者應用程式：管理指南》*。 若想在部署「使用者應用程式」之後變更此指定，則必須使用「使用者應用程式」中的「*管理* > *安全性*」頁面。
	提供應用程式管理員	「提供應用程式管理員」會管理透過「使用者應用程式」的「*申請與核准*」索引標籤提供的提供工作流程功能。此使用者必須先存在於 Identity Vault，才能指定爲「提供應用程式管理員」。 若想在部署「使用者應用程式」之後變更此指定，則必須使用「使用者應用程式」中的「*管理* > *安全性*」頁面。

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

設定類型	欄位	描述
私密金鑰儲存區	*私密 KeyStore 路徑*	私密 KeyStore 含有「使用者應用程式」的私密金鑰和證書。保留。如果您想保留空白，此路徑則預設爲 /jre/lib/security/cacerts。
	私密 KeyStore 密碼	除非您另行指定，否則密碼爲 changeit。這個密碼會根據萬能金鑰進行加密。
	私密金鑰別名	除非您另行指定，否則密碼爲 novellIDMUserApp。
	私密金鑰密碼	除非您另行指定，否則密碼爲 nove1lIDM。這個密碼會根據萬能金鑰進行加密。
託管金鑰儲存區	*託管儲存區路徑*	「託管金鑰儲存區」包含所有託管簽名者的證書，用來驗證數位簽名。如果此路徑爲空，則「使用者應用程式」會從「系統」內容 javax.net.ssl.trustStore 取得路徑。如果路徑不在那裡，就假設爲 jre/lib/security/cacerts。
	託管儲存區密碼	如果此欄位爲空，則「使用者應用程式」會從「系統」內容 javax.net.ssl.trustStorePassword 取得密碼。如果值不在那裡，則使用 changeit。這個密碼會根據萬能金鑰進行加密。
Novell Audit 數位簽名和證書金鑰		包含 Novell Audit 的數位簽名金鑰和證書。
	Novell Audit 數位簽名證書	顯示數位簽名證書。
	Novell Audit 數位簽名私密金鑰	顯示數位簽名私密金鑰。這個金鑰會根據萬能金鑰進行加密。
Access Manager 和 iChain 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。

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

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

4 完成設定後，請按一下「*確定*」，然後繼續進行 「確認您的選擇後進行安裝」(第 89 頁)

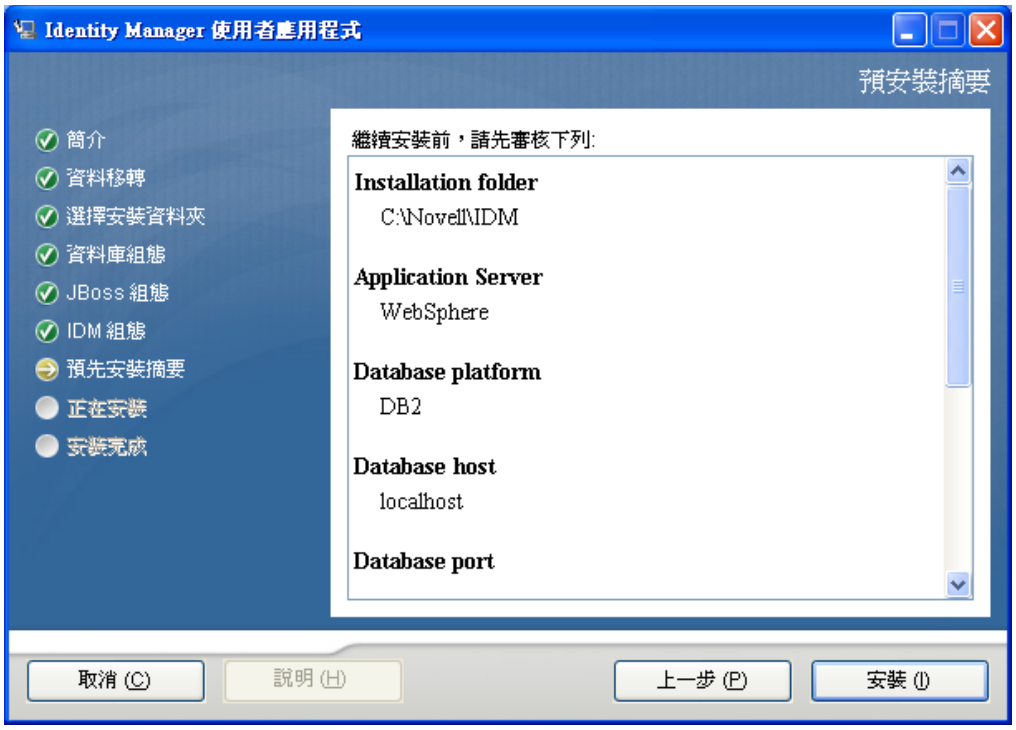
6.10 確認您的選擇後進行安裝

1 閱讀「預先安裝摘要」頁面，確認您選擇的安裝參數。

2 *如有必要，請使用「上一步」，返回先前的安裝頁面變更安裝參數。*

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

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



6.11 檢視記錄檔

如果安裝完成時未發生任何錯誤，請移至 「新增使用者應用程式組態檔和 JVM 系統內容」(第 90 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。

6.12 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。

附註：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。

6.13 將 eDirectory 託管根部輸入至 WebSphere Keystore

1 「使用者應用程式」安裝程序會將 eDirectory™ 託管根證書輸出至「使用者應用程式」的安裝目錄。將這些證書複製到代管 WebSphere 伺服器的機器上。

2 將證書匯入至 WebSphere keystore。您可以使用 WebSphere 管理員主控台 (「使用 WebSphere 管理主控台匯入證書」(第 91 頁)) 或透過指令行 (「以指令行匯入證書」(第 91 頁)) 來完成。

3 匯入證書後，繼續進行 「部署 IDM WAR 檔」(第 92 頁)。

6.13.1 使用 WebSphere 管理主控台匯入證書

1 以 admin 使用者身分登入 websphere 管理主控台。

2 從左面板中，移至「*安全性 > SSL 證書和金鑰管理*」。

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

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

5 在右側的「*額外內容*」中，選取「*簽署者證書*」。

6 按一下 *「新增」*。

7 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。

6.13.2 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 金鑰工具儲存於 /IBM/WebSphere/AppServer/java/bin 中。

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。

6.14 部署 IDM WAR 檔

1. 以 admin 使用者身分登入 websphere 管理主控台。
2. 在左側面板中，移至 *「應用程式」* > *「安裝新應用程式」*。
3. 瀏覽至 IDM War 的檔案位置。

   IDM WAR 檔案是在安裝「使用者應用程式」期間設定的。它位於您安裝「使用者應用程式」期間所指定的「使用者應用程式」安裝目錄中。
4. 鍵入應用程式的「網路位置」根部，例如 IDMProv。這是 URL 路徑。
5. 選中選項圓鈕「*僅當需要其他資訊時提示。*」，然後按「*下一步*」移至「選取安裝選項」頁面。
6. 接受此頁面的所有預設值，然後按「*下一步*」移至「對應模組至伺服器」頁面。
7. 接受此頁面的所有預設值，然後按「*下一步*」移至「對應資源參考至資源」頁面。
8. 爲驗證方法選取「*使用預設方法*」核取方塊。然後，在「*驗證資料項目*」下拉式清單中，選取您先前建立的別名，例如 MyServerNode01/MyAlias。
9. 在驗證設定下方的表格中，找到您在部署的模組。在「目標資源 JNDI 名稱」欄下，按一下瀏覽按鈕來指定 JNDI 名稱。這會帶出資源清單。選取您先前建立的資料來源，並按一下「*套用*」按鈕回到「對應資源參考至資源」頁面，例如 MyDataSource。
10. 選取「*下一步*」移至「*對應 Web 模組的虛擬主機*」。
11. 接受此頁面的所有預設值，然後選取「*下一步*」轉至「摘要」頁面。
12. 按一下「*完成*」以完成部署。
13. 完成部署後，按一下「*儲存*」儲存變更。
14. 請繼續進行「啓動應用程式」(第 92 頁)。

6.15 啓動應用程式

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。

6.16 存取「使用者應用程式入口網站」

1. 使用您在部署期間指定的內容來存取入口網站。

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

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

安裝後任務

7

本節說明安裝後的任務。主題包括：

7.1 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。

7.2 安裝後組態

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 3.6 管理指南》中*「設定使用者應用程式環境」一節。
- *《Novell IDM Roles Based Provisioning Module 3.6 設計指南》*

7.3 檢查您的叢集安裝

在 JBoss 叢集中，確保叢集中的每個應用程式伺服器都具有下列各項：

- 一個唯一的分割區名稱 (分割區名稱)

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

在 WebSphere 叢集中，確保叢集中的每個應用程式伺服器都有唯一的工作流程引擎 ID。

如需詳細資訊，請參閱《*Identity Manager 使用者應用程式：管理指南* (http://www.novell.com/documentation/idmrbpm36/index.html)》第 4 章中對叢集提出討論的小節。

7.4 設定 JBoss 伺服器之間的 SSL 通訊

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

7.5 存取外部密碼 WAR

如果您擁有外部密碼 WAR 並且想藉由存取它來測試「忘記密碼」功能，則可以在下列位置存取：

- 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:8080/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsf。
- 在「使用者應用程式」登入頁中，按一下「*忘記密碼*」連結。

7.6 更新忘記密碼設定

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

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

7.7 設定電子郵件通知

若要實作「忘記密碼」和「工作流程」電子郵件通知功能：

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

7.8 測試 JBoss 應用程式伺服器上的安裝

1 啓動資料庫。如需指示，請參閱資料庫文件。

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

start-jboss.sh (Linux 和 Solaris)

start-jboss.bat (Windows)

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

如果您執行的不是 X11 Window 系統，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 -server -Xms256M -Xmx256M-XX:MaxPermSize=256m"

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

3a 登入 iManager。

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

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

3d 按一下驅動程式上的紅色和白色圖示。

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

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

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

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

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)，而連接埠是應用程式伺服器的連接埠 (例如，JBoss 上預設爲 8080）。*ApplicationName* 預設爲 IDM。在安裝期間，當您提供應用程式伺服器的組態資訊時，指定了應用程式名稱。

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

5 在該頁的右上角，按一下「*登入*」，以登入「使用者應用程式」。

完成這些步驟時，如果「Identity Manager 使用者應用程式」頁面沒有在瀏覽器中出現，則請檢查終端機主控台是否有錯誤訊息，並請您參閱 「疑難排解」(第 98 頁)。

7.9 設定提供小組及其要求

設定您的「提供小組」和「提供小組要求」，以允許進行工作流程任務。如需指示，請參閱 *《Identity Manager 使用者應用程式：管理指南》*(http://www.novell.com/documentation/idmrbpm36/index.html)。

7.10 在 eDirectory 中建立索引

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

7.11 安裝後重新設定 IDM WAR 檔

若要更新 IDM WAR 檔案：

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 公用程式參數的資訊，請參閱表格 4-2 頁上 53、表格 5-1 頁上 62 或表格 6-2 頁上 84。
2. 將新的 WAR 檔案部署到您的應用程式伺服器上。

7.12 疑難排解

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

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 8080 已在使用中」。	關閉可能已在執行之 Tomcat 的任何例項 (或其他伺服器軟體)。如果您決定重新設定應用程式伺服器來使用 8080 以外的連接埠，請記得編輯 iManager 中「使用者應用程式」驅動程式的組態設定。
當應用程式伺服器啓動時，您看到一個訊息表示找不到任何託管證書。	請確定您使用「使用者應用程式」安裝程序中指定的 JDK 來啓動應用程式伺服器。
您無法登入入口網站管理頁面。	請確定「使用者應用程式管理員」帳戶存在。請勿將此帳戶與您的 iManager 管理帳戶混淆。它們是不同的管理物件 (或者說，它們應該是不同的)。
您可以使用管理員身分登入，但無法建立新使用者。	「使用者應用程式管理員」必須是頂端容器的託管者，並需要具有「監督者」權限。您可以嘗試設定「使用者應用程式」的「管理員」權限與輕量目錄存取協定 (LDAP) 管理員的權限相等 (使用 iManager)，而這只是權宜之計。

問題	建議的動作
應用程式伺服器啓動時，發生 MySQL 連線錯誤。	請勿以根部身分執行 (不過，如果您執行的是 Identity Manager 隨附的 MySQL 版本，這個問題就不太可能發生。) 請確定 MySQL 正在執行 (並且執行的是正確的副本)。結束 MySQL 的任何其他例項。執行 /idm/mysql/start-mysql.sh，再執行 /idm/start-jboss.sh。 在文字編輯器中檢查 /idm/mysql/setup-mysql.sh，並更正任何存在疑問的值。然後，執行程序檔並執行 /idm/start-jboss.sh。
您在啓動應用程式伺服器時遇到 KeyStore 錯誤。	您的應用程式伺服器沒有使用「使用者應用程式」安裝期間指定的 JDK。 使用 keytool 指令，來輸入證書檔案： `keytool -import -trustcacerts -alias aliasName -file certFile -keystore ..\lib\security\cacerts -storepass changeit` ◆ 以您爲此證書選擇的唯一名稱來取代 *aliasName*。 ◆ 以證書檔案的完整路徑和名稱來取代 *certFile*。 ◆ 預設 KeyStore 密碼爲 changeit (如果您有不同的密碼，請指定它)。

電子郵件通知沒有傳送。	執行 configupdate 公用程式檢查您是否已提供下列「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 /opt/novell/idm) 執行下列指令：
	`configupdate.bat`