使用者應用程式：安裝指南

Novell®
Identity Manager 角色提供模組

3.6.1

2008 年 7 月 23 日

www.novell.com

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

本指南說明如何安裝 Novell® Identity Manager 角色提供模組 3.6.1。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 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。

角色提供模組安裝綜覽

1

本節提供「角色提供模組」的安裝步驟綜覽。也可以協助您另外安裝和設定 Metadirectory 伺服器安裝所包含的「使用者應用程式標準版」。主題包括：

- 「安裝核對清單」(第 9 頁)
- 「關於安裝程式」(第 10 頁)
- 「系統需求」(第 10 頁)

如果是從舊版的「使用者應用程式」或「角色提供模組」移轉，請參閱《*使用者應用程式：移轉指南* (http://www.novell.com/documentation/idmrbpm361/index.html)》。

1.1 安裝核對清單

若要安裝 Novell® Identity Manager 角色提供模組或「使用者應用程式標準版」，您必須執行下列任務：

- ❑ 驗證您的軟體符合系統要求。請參閱「系統需求」(第 10 頁)。
- ❑ 下載 Identity Manager 3.6.1 角色提供模組。請參閱「下載角色提供模組」(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「安裝 Identity Manager Metadirectory」(第 15 頁)。
  - ❑ 安裝和設定應用程式伺服器。請參閱「安裝應用程式伺服器」(第 16 頁)。
  - ❑ 安裝和設定資料庫。請參閱「安裝資料庫」(第 19 頁)。
  - ❑ 如果您要從舊版的「使用者應用程式」移轉，並繼續使用 Identity Manager 3.5.1 Metadirectory，請執行下列任務：
    - ❑ 執行「角色服務驅動程式」和「使用者應用程式驅動程式」安裝公用程式來擴充 Identity Vault 綱要，並安裝必要的「角色服務」和「使用者應用程式」驅動程式組態檔案，然後依需要複製其他任何檔案。如需詳細資訊，請參閱「安裝 Metadirectory 3.5.1 的其他檔案」(第 20 頁)。

      附註：Identity Manager 3.6 Metadirectory 會自動執行「角色服務」和「使用者應用程式」驅動程式的安裝公用程式。這樣可以確保您有所有必要的檔案。

    - ❑ 將 iManager_icons_for_roles.zip 的內容複製到正確的 iManager 位置。請參閱「複製 iManager 圖示」(第 22 頁)。
    - ❑ 將 afadmin.jar 檔案複製到正確位置。請參閱「複製 afadmin.jar」(第 22 頁)。
- ❑ 在 Identity Manager 3.0 適用的 iManager 或 Designer 中建立「使用者應用程式」驅動程式。
  - iManager：「在 iManager 中建立使用者應用程式驅動程式」(第 23 頁)。
  - Designer：《使用者應用程式：設計指南 (http://www.novell.com/documentation/idmrbpm361/index.html)》。

- ❑ 在 Identity Manager 3.0 適用的 iManager 或 Designer 中建立「角色服務」驅動程式。
  - iManager：「在 iManager 中建立角色服務驅動程式」(第 25 頁)。
  - Designer：《使用者應用程式：設計指南 (http://www.novell.com/documentation/idmrbpm361)》。
- ❑ 安裝並設定「Novell Identity Manager 使用者應用程式」或「角色提供模組」(您必須先安裝正確的 JDK*，才能啓動安裝程式。請參閱 「安裝 Java 開發套件」(第 20 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 4 章 「使用 GUI 安裝程式在 JBoss 上安裝」(第 27 頁)。
    - 第 5 章 「使用 GUI 安裝程式在 WebSphere 應用程式伺服器上安裝」(第 35 頁)。
    - 第 6 章 「使用 GUI 安裝程式在 WebLogic 應用程式伺服器上安裝」(第 43 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 51 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 51 頁)。
- ❑ 執行第 8 章 「安裝後任務」(第 59 頁) 中說明的安裝後任務。

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* 和 WebLogic* 上，您必須手動部署 WAR。
- 啓用 Novell Audit 記錄或 OpenXDAS 記錄 (如果您選擇這樣做)。
- 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。
- 將「3.5.1 提供模組」或「3.6 角色提供模組」中的現有資料移轉成 3.6.2 所需的資料格式。

1.3 系統需求

若要使用 Novell Identity Manager 角色提供模組 3.6.1，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*

必要的系統組件	系統需求
Identity Manager 3.5.1 (Metadirectory 系統)	含最新支援套件的 SUSE® Linux Enterprise Server (SLES) 10 (可同時支援 32 位元和 64 位元) eDirectory™：8.8.2 Security Services 2.0.5 (NMAS™ 3.1.3)
Identity Manager 3.6 (Metadirectory 系統)	下列作業系統之一： ◆ Windows Server* 2003 SP2 (32 位元) ◆ Windows Server* 2008 ◆ 含最新支援套件的 Linux Red Hat 5.0 (32 位元) ◆ 含最新支援套件的 SLES* 10 SP2 (32 位元) ◆ Solaris* 10 (32 位元) ◆ AIX* 5L v5.3 (32 位元) eDirectory：8.8.3
Web 型管理伺服器 ◆ iManager 2.6 和外掛程式 (僅含 Metadirectory 3.5.1) ◆ iManager 2.7 和外掛程式	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 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* ◆ 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 ◆ Windows XP (包含 SP2) ◆ Windows Vista Ultimate 和 Business Edition (僅限 iManager 2.7) ◆ SUSE Linux Enterprise Desktop 10 SP ◆ SUSE Linux 10.1 ◆ openSUSE® 10.3 (僅限 iManager 2.7) 下列軟體： ◆ 含最新支援套件和外掛程式的 Novell iManager 2.6 或 2.7

必要的系統組件	系統需求
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、Sentinel™ 5.1.3 或 Sentinel 6.1 (僅限 Metadirectory 3.6)	針對「安全記錄伺服器」，必須爲下列其中一個作業系統： ◆ 含最新支援套件的 Novell Open Enterprise Server 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」，必須爲下列其中一個作業系統： ◆ Novell Open Enterprise Server 1.0 SP1 或最新支援套件 ◆ 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

必要的系統組件	系統需求
使用者應用程式應用程式伺服器	「使用者應用程式」在 JBoss*、WebSphere* 和 WebLogic* 上執行，如下所述。 「使用者應用程式」搭配 JBoss 4.2.2 GA 時需要 JRE™ 1.5.0_15，且在以下平台上支援： ◆ 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 2003 Server 包含 SP1 (64 位元) ◆ Solaris 10 支援套件，日期 6/06 ◆ Red Hat Linux 5 (32 位元) ◆ Windows 2008 Server 在 WebSphere 6.1 上執行「使用者應用程式」需要 IBM JDK。最低修正套件層級是 6.1.0.9，且套用無限制的規則檔案。在以下平台上支援： ◆ Solaris 10 (64 位元) ◆ Windows 2003 SP1 (64 位元) 在 WebLogic 10 上的「使用者應用程式」需要 JRockit* 1.5.0_06，並在這些平台上支援。 ◆ Solaris 10 (32 位元或 64 位元) ◆ Windows 2003 SP1
使用者應用程式瀏覽器	「使用者應用程式」同時支援 Firefox* 和 Internet Explorer*，如下所示。 以下平台支援 Firefox* 2： ◆ Windows XP (包含 SP2) ◆ Windows Vista ◆ SUSE Linux 10.1 ◆ SUSE Linux Enterprise Desktop 10 SP ◆ openSUSE 10 以下平台支援 Internet Explorer 7： ◆ Windows XP (包含 SP2) ◆ Windows Vista Enterprise 以下平台支援 Internet Explorer 6 SP1： ◆ Windows XP (包含 SP2)

必要的系統組件	系統需求
使用者應用程式的資料庫伺服器	可使用 JBoss 支援以下資料庫： ◆ MySQL 5.0.51 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 WebLogic 支援以下資料庫： ◆ Oracle 10g 2 版 (10.2.0) ◆ MS SQL 2005 SP1 支援以下 JDBC 驅動程式： MS SQL Server 1.2.2828.100 版 Oracle 小型驅動程式：Oracle JDBC 驅動程式 10.2.0.1.0 版 Oracle OCI 驅動程式：Oracle JDBC 驅動程式 10.2.0.2.0 版 MySQL Connector/J 5.0.8 DB2 驅動程式 1.4.2 版
工作站 ◆ 適用於 Identity Manager 3.6 的 Designer 3.0 ◆ iManager Web 存取	已經在下列平台上測試 Designer： Windows： ◆ Windows XP SP2 ◆ Microsoft Windows Vista Linux： ◆ SUSE Linux Enterprise Server 10 (僅適用於 Designer) ◆ SUSE Linux Enterprise Desktop 10 SP ◆ openSUSE 10
稽核	Novell Audit 2.0.2
OpenXDAS	OpenXDAS 0.5.257 版
使用者應用程式 SSO 整合	需要 Novell Access Manager 3.0.1

先決條件

2

本節說明在安裝「Identity Manager 角色提供模組」或「使用者應用程式標準版」之前，您必須安裝或設定的軟體和元件。主題包括：

2.1 安裝 Identity Manager Metadirectory

「角色提供模組 3.6.1」可以搭配 Identity Manager 3.5.1 或 3.6 Metadirectory 一起使用。

如需 Identity Manager 3.6 Metadirectory 的安裝指示，請參閱 *《Novell Identity Manager 3.6 安裝指南》*(http://www.novell.com/documentation/idm36/)。

如果您有 Identity Manager 3.5.1 Metadirectory，您必須更新幾個檔案，「角色提供模組 3.6.1」才能運作。如需詳細資訊，請參閱 「安裝 Metadirectory 3.5.1 的其他檔案」(第 20 頁)。如果是 Identity Manager 3.6 Metadirectory，就沒有必要這樣做，因爲在安裝 Identity Manager 3.6 Metadirectory 時就會自動安裝那些檔案。

2.2 下載角色提供模組

從 Novell 下載區域 (http://download.novell.com/index.jsp) 取得 Identity Manager 角色提供模組 3.6.1 產品。根據您的產品，下載對應的 .iso 影像檔，如表格 2-1 所示。

表格 2-1 *.iso 下載檔案*

對於本產品	下載這個 .iso
角色提供模組 (Identity Manager 角色提供模組)	Identity_Manager_6_1_User_Application_ Provisioning.iso_1
使用者應用程式標準版	Identity_Manager_3_6_1_User_Application_NON_Provisioning.iso

如果您有 Identity Manager 3.5.1 Metadirectory，您也必須下載 Roles_Driver_Install_Utility.iso。如果您是 Identity Manager 3.6 Metadirectory 使用者，則不需要下載 Roles_Driver_Install_Utility.iso，因爲這個 iso 包含的檔案已經是 Identity Manager 3.6 Metadirectory 安裝的一部分。

表格 2-2 說明「角色提供模組」或「使用者應用程式標準版」.iso 檔案中所提供的安裝檔案。

表格 2-2 iso 中提供的檔案和程序檔

檔案	描述
IDMProv.war	角色提供模組 WAR。它包含支援「身分自助服務」功能和「角色提供模組」的「Identity Manager 3.6.1 使用者應用程式」。
IDM.war	使用者應用程式標準版 WAR。包含支援「身分自助服務」功能的「Identity Manager 3.6.1 使用者應用程式」。
IDMUserApp.jar	「角色提供模組」和「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。
JBossMySQL.bin 或 JBossMySQL.exe	方便安裝 JBoss 應用程式伺服器和 MySQL 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。
afadmin.jar	僅 Identity Manager 3.5.1 Metadirectory 才需要。
prerequisitefiles.zip	僅 Identity Manager 3.5.1 Metadirectory 才需要。 包含必須手動複製到正確位置的其他檔案。

您安裝「Identity Manager 角色提供模組」或「使用者應用程式標準版」的系統上，至少必須有 320 MB 的可用儲存空間，還要加上供支援應用程式使用的空間 (資料庫、應用程式伺服器等等)。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

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)。

2.3 安裝應用程式伺服器

- 「安裝 JBoss 應用程式伺服器」(第 17 頁)
- 「安裝 WebLogic 應用程式伺服器」(第 18 頁)
- 「安裝 WebSphere 應用程式伺服器」(第 19 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「系統需求」(第 10 頁)。
- 使用「角色提供模組」下載檔案隨附的 JBossMySQL 公用程式來安裝 JBoss 應用程式伺服器 (可另外選擇安裝 MySQL)。如需說明，請參閱「安裝 JBoss 應用程式伺服器和 MySQL 資料庫」(第 17 頁)。

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

表格 2-3 *JBoss 應用程式伺服器最小建議要求*

配件	建議
RAM	執行「Identity Manager 角色提供模組」時，建議至少要有 512 MB 的 RAM 供 JBoss 應用程式伺服器使用。
連接埠	應用程式伺服器的預設爲 8080。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 角色提供模組」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。 如需有關 IDMPwdMgt.war 檔案的資訊，請參閱「設定外部密碼管理」(第 61 頁)以及《*使用者應用程式：管理指南* (http://www.novell.com/documentation/idmrbpm361/index.html)》。

安裝 JBoss 應用程式伺服器和 MySQL 資料庫

JBossMySQL 公用程式會在您的系統上安裝 JBoss 應用程式伺服器和 MySQL。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。針對 Linux/Unix 使用者，建議您以非 root 使用者的身分來進行安裝。

1 請從 .iso 中找出並執行 JBossMySQL.bin 或 JBossMySQL.exe。

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

未提供 Solaris 的公用程式。

2 依照畫面上的指示來瀏覽公用程式。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。 • *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 18 頁)。 • *MySQL*：在您指定的目錄中安裝 MySQL 並建立 MySQL 資料庫，同時安裝用來啓動和停止的程序檔。
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 MySQL 上層資料夾	按一下「*選擇*」來選取非預設的安裝資料夾。
MySQL 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」安裝公用程式會詢問這個名稱，所以請記下名稱和位置。 • *root 使用者密碼* (和確認密碼)：指定這個資料庫的 root 密碼 (並確認)。
安裝前摘要	檢閱「摘要」頁面。如果指定正確，請按一下「*安裝*」。

公用程式在安裝您選取的產品之後，將會顯示成功完成的訊息。如果您有安裝 MySQL 資料庫，請繼續前往「設定 MySQL 資料庫」(第 19 頁)。

將 JBoss 應用程式伺服器安裝爲服務或精靈

若要以精靈方式啓動 JBoss 應用程式，請參閱 JBoss (http://wiki.jboss.org/wiki/Wiki.jsp?page=StartJBossOnBootWithLinux) 提供的指示。

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://wiki.jboss.org/wiki/Wiki.jsp?page=RunJBossAsAServiceOnWindows (http://wiki.jboss.org/wiki/Wiki.jsp?page=RunJBossAsAServiceOnWindows) 上 JBoss 的相關指示。這類包裝程式之一在 http://wrapper.tanukisoftware.org/doc/english/integrate-simple-win.html (http://wrapper.tanukisoftware.org/doc/english/integrate-simple-win.html)：透過 JMX 加以管理 (請參閱 http://wrapper.tanukisoftware.org/doc/english/jmx.html#jboss (http://wrapper.tanukisoftware.org/doc/english/jmx.html#jboss))。

重要：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 應用程式」以做爲 Windows 服務，但 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)。

2.3.2 安裝 WebLogic 應用程式伺服器

如果您打算使用 WebLogic Application Server 10，請下載並安裝。如需支援的版本的相關資訊，請參閱「系統需求」(第 10 頁)。

2.3.3 安裝 WebSphere 應用程式伺服器

如果您打算使用 WebSphere Application Server 6.1，請下載並安裝。如需支援的版本的相關資訊，請參閱 「系統需求」(第 10 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。您必須已安裝和設定您的平台所支援的其中一個資料庫，才能安裝「角色提供模組」或「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
- ❑ 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，「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 和 WebLogic，先手動設定資料來源，再進行安裝。
- ❑ 必須爲 UTF-8 啓用資料庫。

附註：如果您要移轉到新版的「角色提供模組」，必須使用您用於較早之安裝 (也就是您要移轉的安裝來源) 的相同「使用者應用程式」資料庫。

2.4.1 設定 MySQL 資料庫

「使用者應用程式」需要 MySQL 的特定組態選項。如果您自行安裝 MySQL，請自行設定這些設定。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 19 頁)
- 「字元集」(第 20 頁)
- 「區分大小寫」(第 20 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 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，還必須在 IDM-ds.xml 檔案的 JDBC* URL 中指定字元集，如下所示：

```
<connection-url>jdbc:mysql://localhost:3306/
databasename?useUnicode=true&amp;characterEncoding=utf8&amp;connectionCollation=ut
f8_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)。

2.5 安裝 Java 開發套件

「角色提供模組」和「使用者應用程式標準版」安裝程式至少需要使用 Java 2 Platform Standard Edition 開發套件 1.5 版。

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」期間手動指定路徑來覆寫 JAVA_HOME。

附註：SUSE Linux Enterprise Server (SLES) 使用者：請勿使用 SLES 隨附的 IBM* JDK。此版本在某些方面與該安裝程式不相容。您必須使用 Sun JDK。

2.6 安裝 Metadirectory 3.5.1 的其他檔案

如果您使用 Identity Manager Metadirectory 3.5.1，您必須執行下列幾節所述的其他步驟：

- 「使用 GUI 來安裝角色服務驅動程式」(第 21 頁)
- 「從主控台安裝角色服務驅動程式」(第 22 頁)
- 「複製 iManager 圖示」(第 22 頁)
- 「複製 afadmin.jar」(第 22 頁)

針對 Linux/Unix 使用者，請以 root 使用者的身分來進行安裝。

2.6.1 使用 GUI 來安裝角色服務驅動程式

只有在使用 Identity Manager 3.5.1 Metadirectory 時才需要這樣做。如果您安裝 Identity Manager 3.6 Metadirectory，則已安裝這些檔案。

「角色服務」和「使用者應用程式驅動程式」安裝公用程式提供選項來執行下列動作：

- 擴充您的 Identity Vault 綱要來支援「使用者應用程式」和「角色提供模組」
- 將「角色服務」驅動程式和「使用者應用程式」驅動程式組態檔案安裝至 Metadirectory 伺服器。
- 將「角色服務」和「使用者應用程式」驅動程式組態檔案安裝至 iManager。

您在 Metadirectory 與 iManager 機器上都必須執行這個安裝程式。

附註：您的 Metadirectory 必須安裝在預設位置，才能使用這個安裝程式。

存取 Roles_Driver_Install_Utility.iso

1 根據您的作業系統，找出並執行適當的安裝程式：

作業系統	角色服務驅動程式安裝程式
AIX	roles_driver_install.aix.bin
Linux	roles_driver_install.linux.bin
Solaris	roles_driver_install.solaris.bin
Windows	roles_dirver_install.exe

2 請使用以下資訊完成此安裝：

安裝畫面	描述
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*」。
選取元件	*驅動程式*：將「角色服務」驅動程式和「使用者應用程式」驅動程式安裝至 Metadirectory 伺服器，並更新支援的程式庫 JAR。 *綱要*：更新 Metadirectory 綱要來包含「角色提供模組」和「使用者應用程式標準版」所需的物件。這會安裝 nrf-extensions.sch 檔案和 srvprv.sch 檔案，並對目前的平台執行指令 (Windows 爲 NdsCons.exe，UNIX/Linux 爲 ndssch)。 *驅動程式組態檔案*：安裝「角色服務」驅動程式和「使用者應用程式」驅動程式組態檔案。當您在 iManager 中建立新的驅動程式時會用到這些檔案。您必須在代管 iManager 的機器上執行這個動作。
驗證	當您選取*綱要延伸*時，您必須指定使用者名稱和密碼。這個使用者必須具有 Identity Vault 的管理權限。例如，*cn=admin,o=novell*。
選取驅動程式的位置	如果您選擇安裝「角色服務」和「使用者應用程式」驅動程式，則會要求您指定 eDirectory 伺服器上的位置。這些通常會安裝至 Metadirectory 的 /lib/dirxml/classes 目錄。

安裝畫面	描述
驅動程式組態檔案的安裝位置	指定安裝程式應該將驅動程式組態檔案放在 iManager 機器上的哪個位置。這些通常會安裝至 iManager 的 /nps/Dirxml.Drivers 目錄。
預先安裝摘要	閱讀「安裝前摘要」頁面，確認您選擇的安裝參數，然後完成安裝。

2.6.2 從主控台安裝角色服務驅動程式

若要在主控台 (字元) 模式下執行安裝程式，請發出下列指令：

```
roles_driver_install_<operatingsystemfile> -i console
```

依照「使用 GUI 來安裝角色服務驅動程式」(第 21 頁)中對於圖形使用者介面所說明的相同步驟，閱讀提示並在指令行輸入回應。

2.6.3 複製 iManager 圖示

附註：如果您已安裝 iManager 2.7 及最新的外掛程式，則不需要執行這個程序。

1. 在您下載的 .iso 影像中，找出 prerequisites.zip 檔案。
2. 將檔案解除壓縮，然後找出 iManager_icons_for_roles.zip 檔案。

   此檔案包含 eDirectory 中角色物件的 iManager 圖示。
3. 將檔案解除壓縮，然後將已解壓縮的圖示複製到 nps/portal/modules/dev/images/dir 目錄。
4. 重新啓動 iManager 以使用新圖示。

2.6.4 複製 afadmin.jar

附註：如果您已安裝 iManager 2.7 及最新的外掛程式，則不需要執行這個程序。

1. 在您下載的 .iso 影像中，找出 prerequisites.zip。

   您可以在 /36MetaDirSupport 目錄中找到這個檔案。
2. 將檔案解除壓縮，然後找出 afadmin.jar 檔案。
3. 將 afadmin.jar 檔案複製到 /iManager/nps/WEB-INF/lib 目錄。

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 23 頁)
- 「在 iManager 中建立角色服務驅動程式」(第 25 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。

驅動程式組態支援可讓您進行下列工作：

- 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。
- 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

「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。

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《*使用者應用程式：管理指南* (http://www.novell.com/documentation/idmrbpm361/index.html)》。

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。造成的問題很難找出原因。

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。

   使用 iManager 2.6 (若爲 Identity Manager 3.5.1) 或 iManager 2.7 (若爲 Identity Manager 3.6)。

2. 移至「*角色和任務* > *Identity Manager 公用程式*」，然後選取「*新驅動程式*」或「*輸入組態*」(根據您所使用的外掛程式版本而定)。

   針對 Identity Manager 3.5.1，請使用「*新增驅動程式*」連結。

   針對 Identity Manager 3.6，請使用「*輸入組態*」連結。

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「 *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 「 *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 「 *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 「使用者應用程式」驅動程式組態檔案。檔案名稱是：

UserApplication_3_6_1-IDM3_5_1-V1.xml

如果清單中沒有這個檔案，則表示 「角色服務」驅動程式可能安裝不正確。請參閱 「使用 GUI 來安裝角色服務驅動程式」 (第 21 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。預設值爲 *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：	*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*」來關閉 「安全性相等」視窗，然後按 「 *下一步*」來顯示摘要頁面。

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

附註：如果您使用「使用者應用程式標準版」，則不需要執行本節的步驟。

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。

   使用 2.6 (若爲 Identity Manager 3.5.1) 或 iManager 2.7 (若爲 Identity Manager 3.6)。

2. 在「*Identity Manager* > *Identity Manager 綜覽*」中，選取您要安裝「角色服務」驅動程式的驅動程式集。

   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 (UserApplication_3_6_1-IDM3_5_1-V1.xml) 的「使用者應用程式」驅動程式 3.6.1 版。如果您使用其他版本的「使用者應用程式」驅動程式，則沒有「角色目錄」可用。

3. 按一下「*新增驅動程式*」。

4. 在精靈中，保留預設值「*在現有的驅動程式集裡*」。按「*下一步*」。

5. 從下拉式清單中選取 *RoleService_3_6_1-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。

   如果不在此下拉式清單中，則表示您沒有將此檔案複製到正確的位置。請參閱「使用 GUI 來安裝角色服務驅動程式」(第 21 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。請試著重新啓動 iManager 和 eDirectory，以確保所有新的綱要變更都能確實生效。

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。
使用者群組基礎容器 DN	這個驅動程式只影響此基礎容器中的使用者、容器和群組。如果有群組角色指定，角色驅動程式只會對容器網域內的成員授予 / 廢止角色。

選項	描述
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。
使用者應用程式身分	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「*下一步*」。

8 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。

9 (選擇性，但建議使用) 按一下「*排除管理者角色*」。

10 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*」。

11 按一下「*確定*」來關閉「安全性相等」視窗，然後按「*下一步*」來顯示摘要頁面。

12 如果資訊正確，請按一下「*完成*」。

使用 GUI 安裝程式在 JBoss 上安裝 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」。本節包含下列主題：

- 「安裝和設定使用者應用程式 WAR」(第 27 頁)
- 「測試安裝」(第 32 頁)

如果您希望使用指令行進行安裝，請參閱第 7 章 「使用主控台或單一指令來安裝」(第 51 頁)。

以非 root 使用者的身分來執行安裝程式。

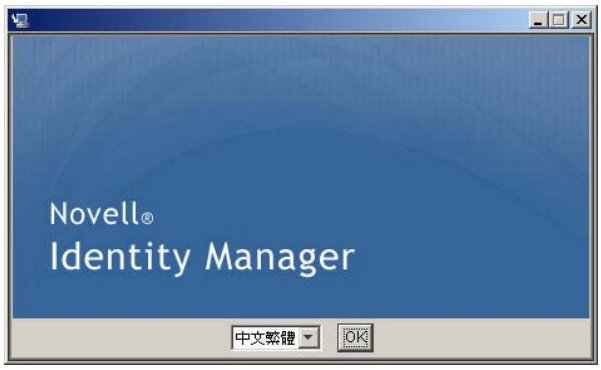
4.1 安裝和設定使用者應用程式 WAR

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 從指令行啓動您平台的安裝程式：

java -jar IdmUserApp.jar

安裝程式啓動時會提示您選擇語言。

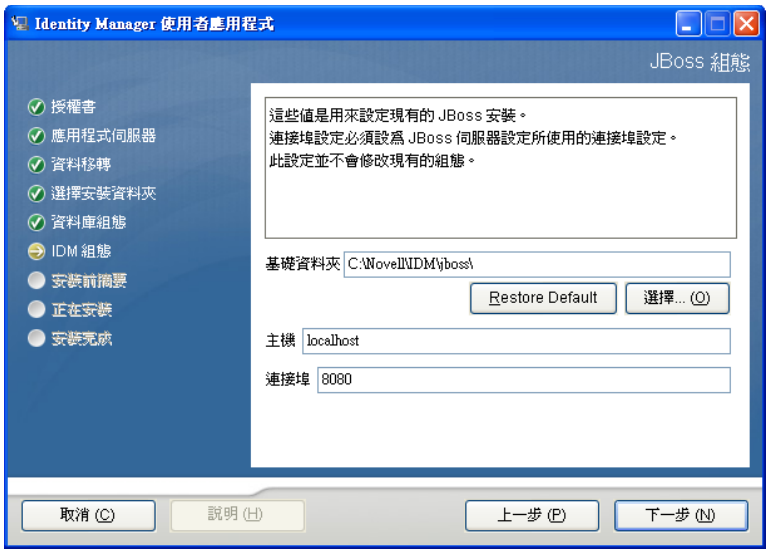


2 請依照下列資訊及每一個安裝面板的指示來完成安裝：

安裝畫面	描述
Novell Identity Manager	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 *JBoss*。
標準或提供	*標準*：如果是安裝「使用者應用程式標準版」，請選取這個選項。
	角色提供：如果是安裝「角色提供模組」，請選取這個選項。

安裝畫面	描述
資料移轉	接受預設值 (確認未選取「*是*」)。 **警告：**請勿選取「*是*」，如果選取「是」，您將會發生啓動「使用者應用程式」的問題。 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/idmrbpm361/index.html)》。
WAR 檔案在哪裡？	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。
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。選項包括： ◆ MySQL ◆ Oracle (會提示您選擇 Oracle 版本) ◆ MS SQL Server
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。
資料庫名稱和授權使用者	*資料庫名稱* (或 SID)：如果使用 MySQL 或 MS SQL Server，請提供您預先設定的資料庫的名稱。對於 Oracle，請提供您之前建立的 Oracle 系統識別碼 (SID)。對於叢集，請爲叢集的每一個成員指定相同的資料庫名稱和 SID。 *資料庫使用者*：指定資料庫使用者。對於叢集，請爲叢集的每一個成員指定相同的資料庫使用者。 *資料庫密碼* / *確認密碼*：指定資料庫密碼。對於叢集，請爲叢集的每一個成員指定相同的資料庫密碼。
Java 安裝	指定 Java 安裝根資料夾。

將會提示您輸入 JBoss 應用程式伺服器安裝在何處的相關資訊。

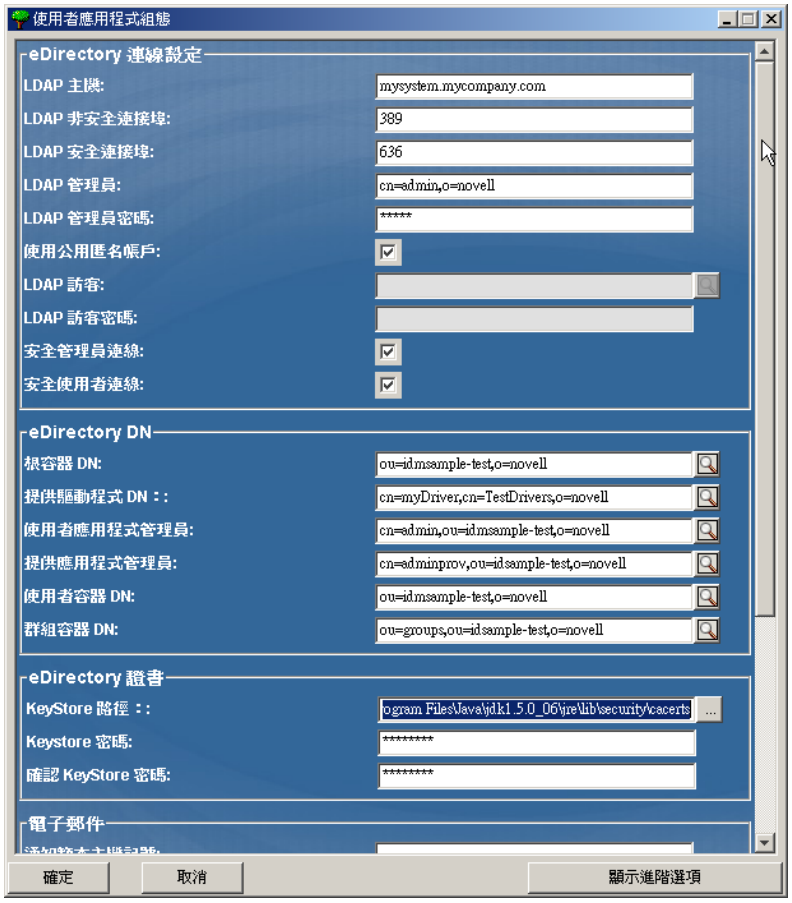


3 請使用下列資訊來完成這個面板，然後繼續安裝。

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 應用程式伺服器和 MySQL 資料庫」(第 17 頁)。 *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。
IDM 組態	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*」。 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」。 *應用程式名稱*：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 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」。在《*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。

安裝畫面	描述
稽核記錄	若要啓用記錄，請按一下「*是*」。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 Audit*：對「使用者應用程式」啓用「Novell® Audit 記錄」。 ◆ *OpenXDAS*：將事件記錄至您的 OpenXDAS 記錄伺服器。 如需設定 Novell Audit 或 OpenXDAS 記錄的相關資訊，請參閱 *《使用者應用程式：管理指南》*。
Novell Audit	*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。
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 「記錄萬能金鑰」（第 59 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。

4 將會提示您輸入資訊，供安裝程式用來設定「使用者應用程式」 WAR 檔案。（如果未提示您輸入這項資訊，表示您可能未完成 「安裝 Java 開發套件」（第 20 頁）中所述的步驟。）



5 請使用下列資訊來完成這個面板，然後繼續安裝。

安裝畫面	描述
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。 如需每一個選項的說明，請參閱附錄 A 「IDM 使用者應用程式組態參考」，第 65 頁 。
預先安裝摘要	閱讀 「預先安裝摘要」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 「預先安裝摘要」頁面並按一下 「*安裝*」。
安裝完成	表示已完成安裝。

4.1.1 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。

4.2 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)：

   start-jboss.sh (Linux 和 Solaris)

   start-jboss.bat (Windows)

   若要停止應用程式伺服器，請使用 stop-jboss.sh 或 stop-jboss.bat，或關閉正在執行 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。

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

5 使用 GUI 安裝程式在 WebSphere 應用程式伺服器上安裝

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」。

- 「安裝和設定使用者應用程式 WAR」(第 35 頁)
- 「設定 WebSphere 環境」(第 39 頁)
- 「部署 WAR 檔案」(第 40 頁)
- 「啓動和存取使用者應用程式」(第 40 頁)

以非 root 使用者的身分來執行安裝程式。

5.1 安裝和設定使用者應用程式 WAR

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。

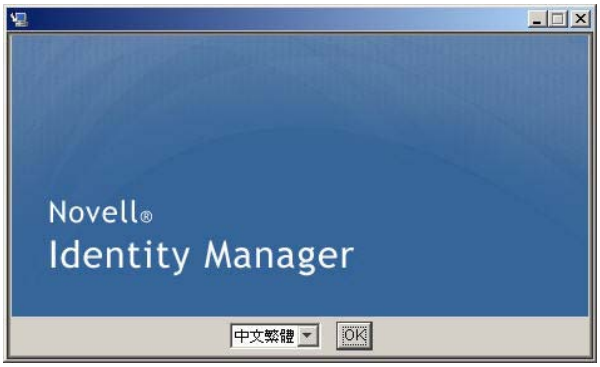
1 瀏覽至含有安裝檔案的目錄。

2 啓動安裝程式：

java -jar IdmUserApp.jar

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

安裝程式啓動時會提示您選擇語言。



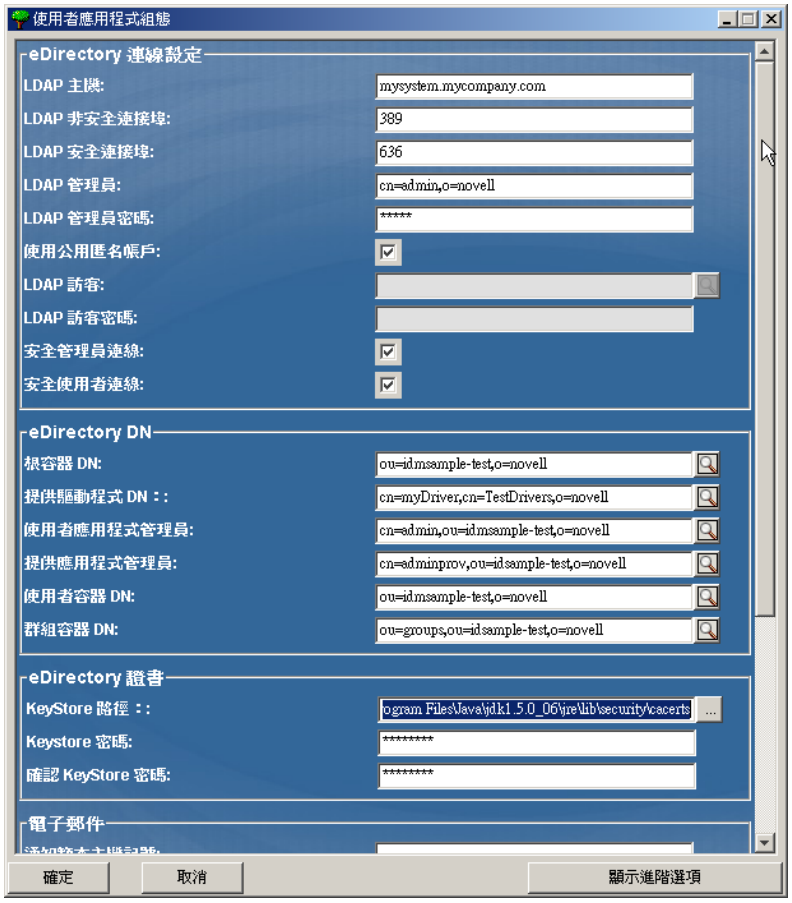
3 請依照下列資訊及每一個安裝面板的指示來完成安裝：

安裝畫面	描述
Novell Identity Manager	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 *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。
標準或提供	*標準*：如果是安裝 「使用者應用程式標準版」，請選取這個選項。 *角色提供*：如果是安裝 「角色提供模組」，請選取這個選項。
資料移轉	接受預設值 (確認未選取「*是*」)。 **警告：**請勿選取「*是*」，如果選取 「是」，您將會發生啓動「使用者應用程式」的問題。 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/idmrbpm361/index.html)》。
WAR 檔案在哪裡？	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。
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。選項包括： ◆ Oracle (會提示您選擇 Oracle 版本) ◆ MS SQL Server ◆ DB2
Java 安裝	指定 Java 安裝根資料夾。 **附註：**使用 WebSphere 時，您必須使用已套用未限制規則檔案的 IBM JDK。
IDM 組態	指定應用程式位置
稽核記錄	若要啓用記錄，請按一下 「*是*」。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 Audit*：對 「使用者應用程式」啓用 「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》*。 ◆ *OpenXDAS*：將事件記錄至您的 OpenXDAS 記錄伺服器。 如需設定 Novell Audit 或 OpenXDAS 記錄的相關資訊，請參閱*《使用者應用程式：管理指南》*。
Novell Audit	*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。

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。 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。

4 將會提示您輸入資訊，供安裝程式用來設定「使用者應用程式」 WAR 檔案。(如果未提示您輸入這項資訊，表示您可能未完成 「安裝 Java 開發套件」 (第 20 頁) 中所述的步驟。)



5 請使用下列資訊來完成這個面板，然後繼續安裝。

安裝畫面	描述
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。 如需詳細資訊，請參閱附錄 A 「IDM 使用者應用程式組態參考」，第 65 頁。
預先安裝摘要	閱讀 「預先安裝摘要」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 「預先安裝摘要」頁面並按一下 「*安裝*」。
安裝完成	表示已完成安裝。

5.1.1 檢視安裝記錄檔

如果安裝完成時未發生任何錯誤，請移至 「新增使用者應用程式組態檔和 JVM 系統內容」(第 39 頁)。

如果安裝發生錯誤或警告，請檢閱記錄檔案來找出問題。

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

5.2 設定 WebSphere 環境

5.2.1 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。

5.2.2 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。

「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 40 頁)) 或透過指令行 (「以指令行匯入證書。」(第 40 頁)) 來完成。

3 匯入證書後，繼續進行「部署 WAR 檔案」(第 40 頁)。

使用 WebSphere 管理主控台匯入證書

1 以 admin 使用者身分登入 WebSphere 管理主控台。

2 從左面板中，移至「*安全性* > *SSL 證書和金鑰管理*」。

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

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

5 在右側的「*額外內容*」中，選取「*簽署者證書*」。

6 按一下「*新增*」。

7 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。

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。

5.3 部署 WAR 檔案

使用 WebSphere 部署工具來部署 WAR 檔案。

5.4 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

使用 GUI 安裝程式在 WebLogic 應用程式伺服器上安裝

6

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。本節提供下列詳細資訊：

若要瞭解如何使用非圖形使用者介面來安裝，請參閱第 7 章 「使用主控台或單一指令來安裝」(第 51 頁)。

以非 root 使用者的身分來執行安裝程式。

6.1 WebLogic 安裝核對清單

- ❑ 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 「安裝和設定使用者應用程式 WAR」(第 43 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 「準備 WebLogic 環境」(第 47 頁)。
- ❑ 部署 WAR。

  請參閱 「部署使用者應用程式 WAR」(第 49 頁)。

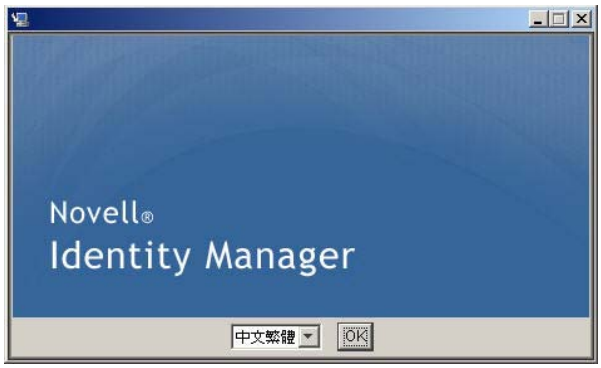
6.2 安裝和設定使用者應用程式 WAR

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. 瀏覽至含有安裝檔案的目錄。
2. 從指令行啓動您平台的安裝程式：

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

   安裝程式啓動時會提示您選擇語言。

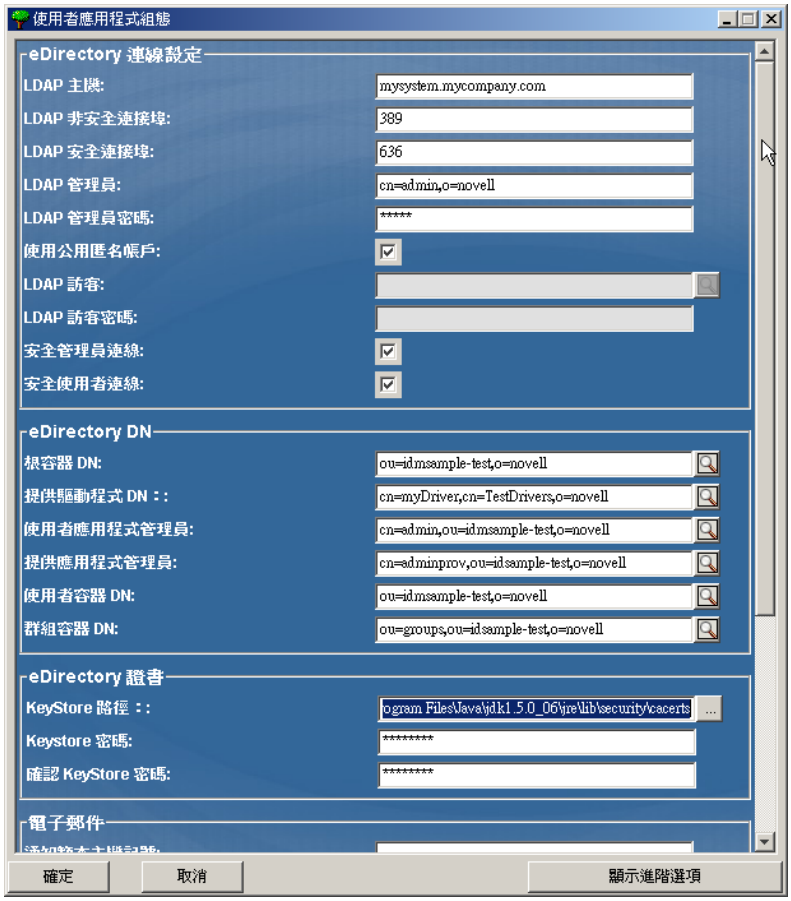


3 請依照下列資訊及每一個安裝面板的指示來完成安裝：

安裝畫面	描述
Novell Identity Manager	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 *WebLogic* 做爲應用程式伺服器。
標準或提供	*標準*：如果是安裝「使用者應用程式標準版」，請選取這個選項。 *角色提供*：如果是安裝「角色提供模組」，請選取這個選項。
資料移轉	接受預設值 (確認未選取「*是*」)。 **警告：**請勿選取「*是*」，如果選取「是」，您將會發生啓動「使用者應用程式」的問題。 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/idmrbpm361/index.html)》。
WAR 檔案在哪裡？	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。
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。選項包括： ◆ Oracle (會提示您選擇版本) ◆ MS SQL Server
Java 安裝	指定 Java 安裝根資料夾。
IDM 組態	指定應用程式位置。當您從瀏覽器啓動「使用者應用程式」時，這會變成 URL 的一部分。
稽核記錄	若要啓用記錄，請按一下「*是*」。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 Audit*：對「使用者應用程式」啓用「Novell Audit 記錄」。 ◆ *OpenXDAS*：將事件記錄至您的 OpenXDAS 記錄伺服器。 如需設定 Novell Audit 或 OpenXDAS 記錄的相關資訊，請參閱 *《使用者應用程式：管理指南》*。
Novell Audit	*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。

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「記錄萬能金鑰」(第 59 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。

4 將會提示您輸入資訊，供安裝程式用來設定「使用者應用程式」WAR 檔案。(如果未提示您輸入這項資訊，表示您可能未完成「安裝 Java 開發套件」(第 20 頁)中所述的步驟。)



安裝畫面	描述
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。 如需詳細資訊，請參閱附錄 A 「IDM 使用者應用程式組態參考」，第 65 頁
預先安裝摘要	閱讀「預先安裝摘要」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「預先安裝摘要」頁面並按一下「*安裝*」。
安裝完成	表示已完成安裝。

6.2.1 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。

6.3 準備 WebLogic 環境

- 「設定連接池」(第 47 頁)
- 「指定使用者應用程式組態檔案位置」(第 47 頁)
- 「工作流程外掛程式和 WebLogic 安裝」(第 49 頁)

6.3.1 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 文件的指示建立資料來源。

  資料來源的 JNDI 名稱必須與您建立「使用者應用程式」 WAR 時所指定的資料庫名稱相同，例如 jdbc/IDMUADataSource。
- ❑ 從「使用者應用程式」安裝目錄中，將 antlr-2.7.6.jar 複製到網域的 lib 資料夾。

6.3.2 指定使用者應用程式組態檔案位置

WebLogic 使用者應用程式需要知道如何尋找 sys-configuration-xmldata.xml 檔案和 idmuserapp_logging.xml 檔案。在作法上，您可以將檔案的位置新增至 setDomainEnv.cmd 檔案中。

爲了讓應用程式伺服器找到這些檔案，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：指定 sys-configuration.xml 檔案所在的資料夾 (不是檔案本身)。
   - -Didmuserapp.logging.config.dir：指定 idmuserapp_logging.xml 檔案所在的資料夾 (不是檔案本身)。

   例如，在 Windows 上：

   ```
   set JAVA_OPTIONS=-Dextend.local.config.dir=c:/bea/user_projects/domains/
   base_domain/idm.local.config.dir
   -Didmuserapp.logging.config.dir=c:/bea/user_projects/domains/base_domain/
   idm.local.config.dir
   ```

4. 設定環境變數 EXT_PRE_CLASSPATH 來指向 antlr.jar。

   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
   ```

   例如，在 Linux 上：

   ```
   export EXT_PRE_CLASSPATH=/opt/bea/user_projects/domains/base_domain/lib/
   antlr-2.7.6.jar
   ```

5. 儲存並結束檔案。

Configupdate 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. 在這一行下面新增下列項目：

   ```
   Add -Dextend.local.config.dir=<directory-path>\extend.local.config.dir
   ```

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，您必須在 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。

6.3.3 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/base_domain/config/ 資料夾中的 Config.xml。
2. 在 <security-configuration> 區段中新增下一行：

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

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。

6.4 部署使用者應用程式 WAR

- 將 jsf-ri-1.1.1.war 部署爲文件庫。
- 從安裝目錄中 (通常是 Novell\IDM)，將已更新的「使用者應用程式」WAR 檔案複製到應用程式網域。例如：

  ```
  bea\user_projects\domains\base_domain\servers\AdminServer\upload
  ```

- 採用標準的 WebLogic 部署程序來部署「使用者應用程式」 WAR。

6.5 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:8080/IDMProv
  ```

使用主控台或單一指令來安裝

7

本節說明的安裝方法可用於取代第 4 章 「使用 GUI 安裝程式在 JBoss 上安裝」(第 27 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 51 頁)
- 「使用單一指令安裝使用者應用程式」(第 51 頁)

7.1 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 2-2 頁上 16 所述的適當安裝檔案後，請登入並開啓終端機會期。
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 4 章 「使用 GUI 安裝程式在 JBoss 上安裝」(第 27 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 「使用者應用程式組態：基本參數」(第 65 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 8 章 「安裝後任務」(第 59 頁)。

7.2 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 2-2 頁上 16 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 7-1。「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 7-1 *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。 指定您先前在「在 iManager 中建立使用者應用程式驅動程式」(第 23 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`

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*」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 *《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。
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_COMPLIANCECONTAINERDN	「合規模組管理員」是一個系統角色，允許成員執行「*合規*」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 「合規模組管理員」。

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=	中繼目錄使用者身分：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。 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。 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：會期逾時。 必要。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。 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 是提供申請任務和核准通知的連結。
NOVL_CONFIG_EMAILNOTIFYPORT=	電子郵件：通知範本 PORT 記號。 用於取代提供申請任務和核准通知中所使用之電子郵件範本中的 $PORT$ 記號。
NOVL_CONFIG_EMAILNOTIFYSECUREPORT=	電子郵件：通知範本 SECURE PORT 記號。 用於取代提供申請任務和核准通知中所使用之電子郵件範本中的 $SECURE_PORT$ 記號。
NOVL_CONFIG_NOTFSMTPEMAILFROM=	電子郵件：SMTP 電子郵件通知寄件者。 必要。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。 必要。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。

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.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 「設定外部密碼管理」(第 61 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=	中繼目錄使用者身分：使用者物件類別。 必要。LDAP 使用者物件類別 (通常爲 inetOrgPerson)。
NOVL_CONFIG_LOGINATTRIBUTE=	中繼目錄使用者身分：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=	中繼目錄使用者身分：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)。
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。

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_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_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。
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。

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_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。
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。

安裝後任務

8

本節說明安裝後的任務。主題包括：

8.1 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。

8.2 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 角色提供模組 3.6.1 管理指南》中*「設定使用者應用程式環境」一節。
- *《Novell IDM 角色提供模組 3.6.1 設計指南》*

8.2.1 設定 Novell Audit

根據《使用者應用程式：管理指南 (http://www.novell.com/documentation/idmrbpm361/index.html)》的 「設定記錄」一節中的指示，將 dirxml.lsc 檔案 (位於 prerequisites.zip 檔案中) 複製到 Audit 伺服器。

8.3 設定 eDirectory

8.3.1 在 eDirectory 中建立索引

爲了增進「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」使用者會感受到效能不佳，尤其在叢集環境中更是如此。

如果您在安裝期間，於「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 頁上 70 中所述)，則可以自動建立這些索引，您也可以參閱 《*Novell eDirectory 管理指南*》(http://www.novell.com/documentation)，以取得使用「索引管理員」建立索引的相關指示。

8.3.2 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. 找到並解壓縮 .iso 中的 nmassaml.zip 檔案。
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。)

8.4 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 「使用者應用程式組態：基本參數」(第 65 頁) 或表格 7-1 頁上 52。

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。

8.5 設定外部密碼管理

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。

- 「指定外部密碼管理 WAR」(第 62 頁)
- 「指定內部密碼 WAR」(第 62 頁)
- 「測試外部密碼 WAR 組態」(第 62 頁)
- 「設定 JBoss 伺服器之間的 SSL 通訊」(第 62 頁)

8.5.1 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 62 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。
   - 如果您使用 configupdate 公用程式來更新安裝根目錄中的外部密碼 WAR，則請閱讀此步驟，並手動將 WAR 重新命名爲您在「*忘記密碼連結*」中所指定的第一個目錄。然後繼續前往步驟 6。

   在安裝結束之前，安裝程式會將 IDMPwdMgt.war (隨附於安裝程式) 重新命名爲您指定的第一個目錄名稱。經過重新命名的 IDMPwdMgt.war 會變成您的外部密碼 WAR。例如，如果您指定 http://www.idmpwdmgthost.com/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsf，安裝程式就會將 IDMPwdMgt.war 重新命名爲 ExternalPwd.war。安裝程式會將重新命名的 WAR 移到安裝根目錄裡面。
6. 手動複製 ExternalPwd.war 到負責執行外部密碼 WAR 功能的遠端 JBoss 伺服器部署目錄。

8.5.2 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。

8.5.3 測試外部密碼 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: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。

8.5.4 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。

8.6 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)

8.7 疑難排解

您的 Novell® 代表會和您一起解決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 使用者身分、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 (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 c:\opt\novell\idm) 執行下列指令：
	
	`configupdate.bat`

IDM 使用者應用程式組態參考

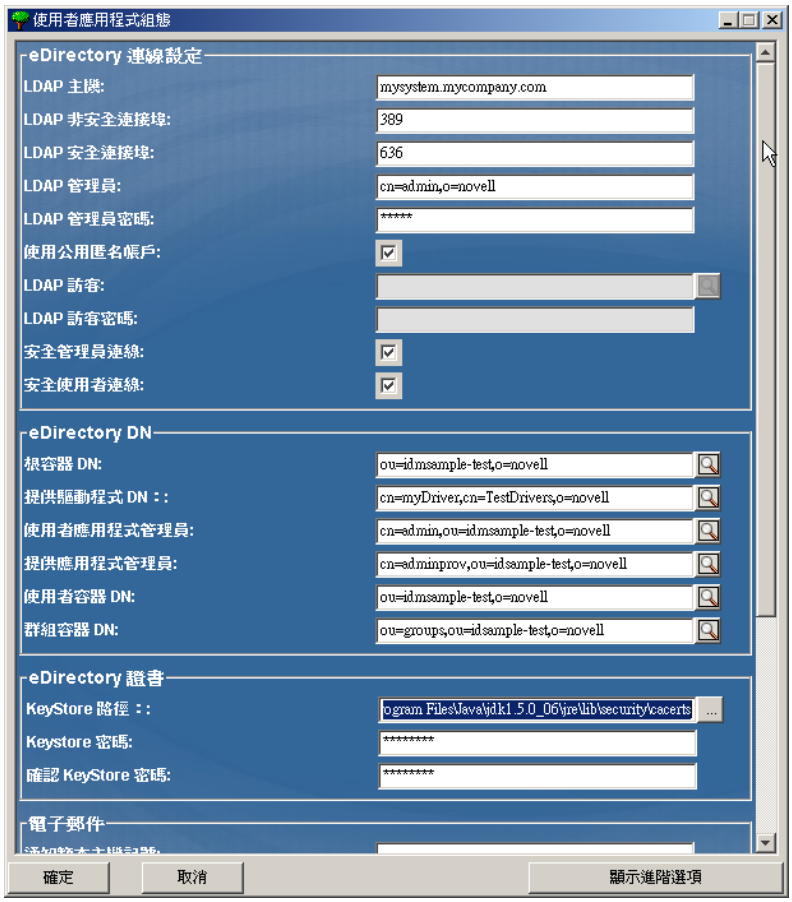
A

本節說明在「使用者應用程式」安裝或組態更新期間提供值的選項。

- 「使用者應用程式組態：基本參數」(第 65 頁)
- 「使用者應用程式組態：所有參數」(第 69 頁)

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：基本選項*

設定類型	選項	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。 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。
	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。 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。
	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	選項	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「使用者應用程式」驅動程式的可辨識名稱 (在「在 iManager 中建立使用者應用程式驅動程式」(第 23 頁) 中說明)。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 *《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。 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。
	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。
	合規管理員	「合規模組管理員」是一個系統角色，允許成員執行「*合規*」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「合規模組管理員」。 在 configupdate 期間，只有在您還未指定有效的「合規模組管理員」時，對這個值的變更才會生效。如果有效的「合規模組管理員」已存在，則不會儲存您所做的變更。 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「*角色* > *角色指定*」頁面。

設定類型	選項	描述
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。 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。
	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。 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 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。
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」。

設定類型	選項	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。
	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「設定外部密碼管理」(第 61 頁)。
	忘記密碼回傳連結	如果您使用外部密碼管理 WAR，則請提供該外部「密碼管理 WAR」用來透過 Web 服務喚回「使用者應用程式」的路徑，例如 https://*idmhost*:*ssl port*/idm。

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
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	選項	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「使用者應用程式」驅動程式的可辨識名稱 (在「在 iManager 中建立使用者應用程式驅動程式」(第 23 頁) 中說明)。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。請參閱《*使用者應用程式：管理指南*》以取得詳細資料。 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。 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。
	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。
	合規管理員	「合規模組管理員」是一個系統角色，允許成員執行「*合規*」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「合規模組管理員」。 在 configupdate 期間，只有在您還未指定有效的「合規模組管理員」時，對這個值的變更才會生效。如果有效的「合規模組管理員」已存在，則不會儲存您所做的變更。 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「*角色* > *角色指定*」頁面。

設定類型	選項	描述
	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。 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。
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。 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。
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。 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)。

設定類型	選項	描述
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	
私密金鑰儲存區	*私密 KeyStore 路徑*	私密 KeyStore 含有「使用者應用程式」的私密金鑰和證書。保留。如果您想保留空白，此路徑則預設爲 /jre/lib/security/cacerts。
	私密 KeyStore 密碼	除非您另行指定，否則密碼爲 changeit。這個密碼會根據萬能金鑰進行加密。
	私密金鑰別名	除非您另行指定，否則密碼爲 novellIDMUserApp。
	私密金鑰密碼	除非您另行指定，否則密碼爲 nove1IIDM。這個密碼會根據萬能金鑰進行加密。
託管金鑰儲存區	*託管儲存區路徑*	「託管金鑰儲存區」包含所有託管簽名者的證書，用來驗證數位簽名。如果此路徑爲空，則「使用者應用程式」會從「系統」內容 javax.net.ssl.trustStore 取得路徑。如果路徑不在那裡，就假設爲 jre/lib/security/cacerts。
	託管儲存區密碼	如果此欄位爲空，則「使用者應用程式」會從「系統」內容 javax.net.ssl.trustStorePassword 取得密碼。如果值不在那裡，則使用 changeit。這個密碼會根據萬能金鑰進行加密。
Novell Audit 數位簽名和證書金鑰		包含 Novell Audit 的數位簽名金鑰和證書。
	Novell Audit 數位簽名證書	顯示數位簽名證書。
	Novell Audit 數位簽名私密金鑰	顯示數位簽名私密金鑰。這個金鑰會根據萬能金鑰進行加密。
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	選項	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:ssl*/*port*/idm。
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。

設定類型	選項	描述
	建立 eDirectory 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「在 eDirectory 中建立索引」(第 60 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 eDirectory 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。 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。