User Application：安装指南

Novell®
Identity Manager 基于角色的供应模块

3.6.1

2008 年 7 月 23 日

www.novell.com

法律声明

Novell, Inc. 对本文档的内容或使用不作任何声明或担保，特别是对用于任何特定目的的适销性或适用性不作任何明示或暗示的担保。另外， Novell, Inc. 保留随时修改本出版物及其内容的权利，并且没有义务将这些修改通知任何个人或实体。

另外， Novell, Inc. 对任何软件不作任何声明或保证，特别是对适销性或用于任何特定目的的适用性不作任何明示或暗示的保证。另外， Novell, Inc. 保留随时修改 Novell 软件全部或部分内容的权利，并且没有义务将这些修改通知任何个人或实体。

依据本协议提供的任何产品或技术信息都将受到美国出口控制和其他国家 / 地区的贸易法律的约束。您同意遵守所有出口控制法规，并同意在出口、再出口或进口可交付产品之前取得所有必要的许可证或分类证书。您同意不出口或再出口至当前美国出口排除列表上所列的实体，或者美国出口法律中规定的任何被禁运的国家 / 地区或支持恐怖主义的国家 / 地区。您同意不将可交付产品用于禁止的核武器、导弹或生物化学武器等终端用途。有关出口 Novell 软件的详细信息，请访问 Novell International Trade Services 万维网页面 (http://www.novell.com/info/exports/)。如果您未能获得任何必要的出口许可， Novell 对此不负任何责任。

Novell, Inc. 对本文档中介绍的产品中所包含的相关技术拥有知识产权。这些知识产权特别包括但不限于 Novell 法律专利万维网页 (http://www.novell.com/company/legal/patents/) 上列出的一项或多项美国专利，以及美国和其他国家 / 地区的一项或多项其他专利或者正在申请的专利。

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

*联机文档：*要访问本产品及其他 Novell 产品的最新联机文档，请参阅 Novell 文档万维网页 (http://www.novell.com/documentation)。

Novell 商标

有关 Novell 商标，请参阅 Novell 商标和服务标记列表 (http://www.novell.com/company/legal/trademarks/tmlist.html)。

第三方资料

所有第三方商标均属其各自所有者的财产。

目录

关于本指南

本指南说明如何安装 Novell® Identity Manager 基于角色的供应模块 3.6.1。包括以下几节：

适用对象

本指南适用于将计划和实施 Identity Manager 基于角色的供应模块的管理员和顾问。

反馈

我们期待听到您对本手册和本产品中包含的其他文档的意见和建议。使用联机文档中每页底部的 “ 用户意见 ” 功能，或访问 www.novell.com/documentation/feedback.html 并输入您的意见。

其他文档

有关 Identity Manager 基于角色的供应模块的更多文档，请参阅 Identity Manager 文档万维网站点 (http://www.novell.com/documentation/lg/dirxmldrivers/index.html)。

文档约定

在 Novell 文档中，大于号 (>) 用于分隔步骤内的操作和交叉参照路径中的项目。

商标符号 （®、™ 等）代表一个 Novell 商标。星号 (*) 表示第三方商标。

如果某个路径名的书写对某些平台需使用反斜线而对另一些平台需使用正斜线，则使用反斜线表示该路径名。如果平台要求使用正斜杠 （例如 Linux* 或 UNIX*），用户应根据软件的要求使用正斜杠。

基于角色的供应模块安装概述

1

本节提供了基于角色的供应模块安装步骤的概述。它还能够协助您对包含在元目录服务器安装中的 User Application 标准版进行安装和配置。包括以下主题：

如果从 User Application 或基于角色的供应模块的较早版本迁移，请参考 《*User Application：迁移指南* (http://www.novell.com/documentation/idmrbpm361/index.html)》

1.1 安装核对清单

要安装 Novell® Identity Manager 基于角色的供应模块或 User Application 标准版，必须执行以下任务：

- ❑ 校验软件是否满足系统要求。请参阅第 1.3 节 “ 系统要求 ”（第 10 页）。
- ❑ 下载 Identity Manager 3.6.1 基于角色的供应模块。请参阅第 2.2 节 “ 下载基于角色的供应模块 ”（第 15 页）。
- ❑ 设置以下支持组件：
  - ❑ 确保安装了受支持的 Identity Manager 元目录。请参阅第 2.1 节 “ 安装 Identity Manager 元目录 ”（第 15 页）。
  - ❑ 安装和配置应用程序服务器。请参阅第 2.3 节 “ 安装应用程序服务器 ”（第 16 页）。
  - ❑ 安装和配置数据库。请参阅第 2.4 节 “ 安装数据库 ”（第 19 页）。
  - ❑ 如果从 User Application 的较早版本迁移，并继续使用 Identity Manager 3.5.1 元目录，请执行以下任务：
    - ❑ 运行角色服务和 User Application 驱动程序安装实用程序来扩展身份库纲要并安装所需的角色服务和 User Application 驱动程序配置文件，然后根据需要复制任何附加文件。有关详细信息，请参阅第 2.6 节 “ 安装元目录 3.5.1 的其他文件 ”（第 20 页）。

      注释：Identity Manager 3.6 元目录以静默方式运行角色服务和 User Application 驱动程序安装实用程序。这确保您具有所有必需的文件。

    - ❑ 将 iManager_icons_for_roles.zip 中的内容复制到正确的 iManager 位置。请参阅第 2.6.3 节 “ 复制 iManager 图标 ”（第 22 页）。
    - ❑ 将 afadmin.jar 文件复制到正确的位置。请参阅复制 afadmin.jar （第 22 页）。
- ❑ 在 iManager 或 Designer for Identity Manager 3.0 中创建 User Application 驱动程序。
  - 对于 iManager：第 3.1 节 “ 在 iManager 中创建 User Application 驱动程序 ”（第 23 页）。
  - 对于 Designer：《User Application：设计指南 (http://www.novell.com/documentation/idmrbpm361/index.html)》。

- ❑ 在 iManager 或 Designer for Identity Manager 3.0 中创建角色服务驱动程序。
  - 对于 iManager：第 3.2 节 “ 在 iManager 中创建角色服务驱动程序 ”（第 25 页）。
  - 对于 Designer：《User Application：设计指南 (http://www.novell.com/documentation/idmrbpm361)》。
- ❑ 安装和配置 Novell Identity Manager User Application 或基于角色的供应模块。（您必须先安装了正确的 JDK*，然后才能启动安装程序。请参阅第 2.5 节 “ 安装 Java 开发工具包 ”（第 20 页）。）

  可以以下三种模式之一运行安装程序：
  - 图形用户界面。请参阅以下内容之一：
    - 第 4 章 “ 使用 GUI 安装程序在 JBoss 上进行安装 ”（第 27 页）。
    - 第 5 章 “ 使用 GUI 安装程序在 WebSphere Application Server 上进行安装 ”（第 33 页）。
    - 第 6 章“通过 GUI 安装程序在 WebLogic Application Server 上进行安装”（第 39 页）。
  - 控制台（命令行）界面。请参阅第 7.1 节 “ 从控制台安装 User Application”（第 47 页）。
  - 静默安装。请参阅第 7.2 节 “ 使用单个命令安装 User Application”（第 47 页）。
- ❑ 执行第 8 章 “ 安装后任务 ”（第 55 页）中说明的安装后任务。

1.2 关于安装程序

User Application 安装程序执行以下操作：

- 指定要使用的现有应用程序服务器版本。
- 指定要使用的数据库现有版本，例如：MySQL*、 Oracle*、 DB2* 或 Microsoft* SQL Server*。该数据库储存 User Application 数据和 User Application 配置信息。
- 配置 JRE 的证书文件，以便 User Application （运行于应用程序服务器上）能够安全地与身份库和 User Application 驱动程序通讯。
- 将用于 Novell Identity Manager User Application 的 Java* Web Application Archive (WAR) 文件配置并部署到应用程序服务器。在 WebSphere* 和 WebLogic* 上，必须手动部署 WAR。
- 根据需要启用 Novell Audit 日志记录或 OpenXDAS 日志记录。
- 允许导入现有主密钥，以恢复特定的基于角色的供应模块安装和支持群集。
- 将现有数据从 3.5.1 供应模块或 3.6 基于角色的供应模块迁移至 3.6.2 中所需的数据格式。

1.3 系统要求

要使用 Novell Identity Manager 基于角色的供应模块 3.6.1，必须具有表 1-1 中列出的必需组件之一。

表 1-1 *系统要求*

必需的系统组件	系统要求
Identity Manager 3.5.1 （元目录系统）	带最新支持包的 SUSE® Linux Enterprise Server (SLES) 10 （同时支持 32 位和 64 位） eDirectory™：8.8.2 Security Services 2.0.5 (NMAS™ 3.1.3)
Identity Manager 3.6 （元目录系统）	下列操作系统之一： ◆ Windows Server* 2003 SP2 （32 位） ◆ 带最新支持包的 Linux Red Hat 5.0 （32 位） ◆ 带最新支持包的 SLES* 10 SP2 （32 位） ◆ Solaris* 10 （32 位） ◆ AIX* 5L v5.3 （32 位） eDirectory：8.8.3
基于万维网的管理服务器 ◆ iManager 2.6 和插件（仅元目录 3.5.1） ◆ iManager 2.7 和插件	下列操作系统之一： ◆ 带最新支持包的 NetWare 平台上的 Novell Open Enterprise Server (OES) 1.0 ◆ Novell Open Enterprise Server 2.0 ◆ 带最新支持包的 NetWare 6.5 ◆ 带最新服务包的 Windows 2000 Server （32 位） ◆ 带最新服务包的 Windows Server 2003 （32 位） ◆ Microsoft Windows Vista* ◆ Red Hat Linux 3.0、 4.0 或 5.0 ES 或者 AS （同时支持 32 位和 64 位） ◆ 带最新支持包的 Solaris 9 或 10 ◆ 带最新支持包的 SUSE Linux Enterprise Server 9 或 10 （同时支持 32 位和 64 位） 通过 iManager 工作站支持的操作系统： ◆ 带最新服务包的 Windows 2000 Professional ◆ 带 SP2 的 Windows XP ◆ Windows Vista Ultimate 和 Business Edition （仅 iManager 2.7） ◆ SUSE Linux Enterprise Desktop 10 ◆ SUSE Linux 10.1 ◆ openSUSE® 10.3 （仅 iManager 2.7） 以下软件： ◆ 带最新支持包和插件的 Novell iManager 2.6 或 2.7

必需的系统组件	系统要求
安全日志记录服务 ◆ 安全日志记录服务器 ◆ 平台代理 （客户机组件） ◆ Novell Audit 2.0.2、Sentinel™ 5.1.3 或 Sentinel 6.1 （仅元目录 3.6）	对于安全日志记录服务器，需要下列操作系统之一： ◆ 带最新支持包的 Novell Open Enterprise Server 1.0 或 2.0 ◆ 带最新支持包的 NetWare 6.5 ◆ 带最新服务包的 Windows 2000 Server （32 位） ◆ 带最新服务包的 Windows Server 2003 （32 位） ◆ Linux Red Hat Linux 3.0、 4.0 或 5.0 ES 或者 AS （32 位或 64 位，尽管 Novell Audit 仅在 32 位模式上运行） ◆ 带最新支持包的 Solaris 9 或 10 ◆ 带最新支持包的 SUSE Linux Enterprise Server 9 或 10（32 位和 64 位，尽管 Novell Audit 仅在 32 位模式上运行） ◆ 带最新支持包的 Novell eDirectory 8.7.3.6 或 8.8 （必须安装在安全日志记录服务器上） 对于平台代理，需要下列操作系统之一： ◆ Novell Open Enterprise Server 1.0 SP1 或带最新支持包 ◆ 带最新支持包的 NetWare 6.5 ◆ Windows 2000 或 2000 Server、 XP 或带最新服务包的 Windows Server 2003 （32 位） ◆ Red Hat Linux 3 或 4 AS 或者 ES （32 位或 64 位，尽管 Novell Audit 仅在 32 位模式上运行） ◆ Solaris 8、 9 或 10 ◆ SUSE Linux Enterprise Server 9 或 10 （32 位和 64 位，尽管 Novell Audit 仅在 32 位模式上运行） 带最新支持包和插件的 iManager 2.6 或 2.7

必需的系统组件	系统要求
User Application 应用程序服务器	User Application 在 JBoss*、 WebSphere* 和 WebLogic* 上运行，如下所述。 带 JBoss 4.2.2 GA 的 User Application 需要 JRE* 1.5.0_15，在以下平台上受支持： ◆ Novell Open Enterprise Server (OES) 1.0 SP2 或带最新支持包 — 仅 Linux ◆ SUSE Linux Enterprise Server 9 SP2 （包含在 OES 1.0 SP2 中）或 10.1.x （64 位 JVM*） ◆ 带 SP1 的 Windows 2003 Server （64 位） ◆ Solaris 10 支持包 （日期为 6/06） ◆ Red Hat Linux 5 （32 位） WebSphere 6.1 上的 User Application 需要 IBM JDK。最低的修订包级别为 6.1.0.9，并应用了不受限的策略文件。它在以下平台上受支持： ◆ Solaris 10 （64 位） ◆ Windows 2003 SP1 (64 位) WebLogic 10 上的 User Application 需要 JRockit* 1.5.0_06，在以下平台上受支持。 ◆ Solaris 10 （32 位或 64 位) ◆ Windows 2003 SP1
User Application 浏览器	User Application 同时支持 Firefox* 和 Internet Explorer*，如下所述。 以下各操作系统支持 Firefox* 2： ◆ 带 SP2 的 Windows XP ◆ Windows Vista ◆ SUSE Linux 10.1 ◆ SUSE Linux Enterprise Desktop 10 ◆ openSUSE 10 以下各操作系统支持 Internet Explorer 7： ◆ 带 SP2 的 Windows XP ◆ Windows Vista Enterprise 以下各操作系统支持 Internet Explorer 6 SP1： ◆ 带 SP2 的 Windows XP

必需的系统组件	系统要求
User Application 的数据库服务器	JBoss 支持以下数据库： ◆ MySQL V5.0.51 ◆ Oracle 9i (9.2.0.1.4) ◆ Oracle 10g R2 (10.2.0.1.0) ◆ MS SQL 2005 SP1 WebSphere 支持以下数据库： ◆ Oracle 10g R2 (10.2.0) ◆ MS SQL 2005 SP1 ◆ DB2 DV2 v9.1.0.0 WebLogic 支持以下数据库： ◆ Oracle 10g R2 (10.2.0) ◆ MS SQL 2005 SP1 支持以下 JDBC 驱动程序： MS SQL Server V1.2.2828.100 Oracle 瘦驱动程序：Oracle JDBC Driver V10.2.0.1.0 Oracle OCI 驱动程序：Oracle JDBC Driver V10.2.0.2.0 MySQL Connector/J 5.0.8 DB2 Driver V1.4.2
工作站 ◆ Designer 3.0 for Identity Manager 3.6 ◆ iManager 万维网访问	已在下列平台上测试了 Designer： Windows： ◆ Windows XP SP2 ◆ Microsoft Windows Vista Linux： ◆ SUSE Linux Enterprise Server 10 （仅对于 Designer） ◆ SUSE Linux Enterprise Desktop 10 ◆ openSUSE 10
Audit	Novell Audit 2.0.2
OpenXDAS	OpenXDAS V0.5.257
User Application SSO 集成	需要 Novell Access Manager 3.0.1。

先决条件

2

本节说明在安装 Identity Manager 基于角色的供应模块或 User Application 标准版之前必须安装或配置的软件和组件。包括以下主题：

2.1 安装 Identity Manager 元目录

基于角色的供应模块 3.6.1 可用于 Identity Manager 3.5.1 或 3.6 元目录。

有关安装 Identity Manager 3.6 元目录的指导，请参阅 《*Novell Identity Manager 3.6 安装指南* (http://www.novell.com/documentation/idm36/)》。

如果具有 Identity Manager 3.5.1 元目录，必须先更新几个文件，基于角色的供应模块 3.6.1 才会运行。有关详细信息，请参阅第 2.6 节 “ 安装元目录 3.5.1 的其他文件 ”（第 20 页）。对于 Identity Manager 3.6 元目录则不必这样做，因为这些文件已作为 Identity Manager 3.6 元目录安装的一部分自动安装。

2.2 下载基于角色的供应模块

从 Novell Downloads (http://download.novell.com/index.jsp) 获取 Identity Manager 基于角色的供应模块 3.6.1 产品。下载产品的 .iso 映像文件，如表 2-1 所示。

表 2-1 *.iso 下载文件*

对于此产品	下载此 .iso
基于角色的供应模块	Identity_ Manager_3_6_1_User_Application_Provisioning.iso
User Application 标准版	Identity_Manager_3_6_1_User_Application_NON_Provisioning.iso

如果具有 Identity Manager 3.5.1 元目录，您还必须下载 Roles_Driver_Install_Utility.iso。如果您是 Identity Manager 3.6 元目录用户，则不必下载 Roles_Driver_Install_Utility.iso，因为此 .iso 中包含的文件已经是 Identity Manager 3.6 元目录安装的一部分。

表 2-2 说明了基于角色的供应模块或 User Application 标准版 .iso 文件中的安装文件。

表 2-2 iso 中交付的文件和脚本

文件	说明
IDMProv.war	基于角色的供应模块 WAR。它包括带身份自助服务功能和基于角色的供应模块的 Identity Manager 3.6.1 User Application。
IDM.war	User Application 标准版 WAR。它包含 Identity Manager 3.6.1 User Application （支持身份自助服务功能）。
IDMUserApp.jar	基于角色的供应模块和 User Application 安装程序。
silent.properties	包含静默安装所需参数的文件。这些参数与在 GUI 或控制台安装过程中设置的安装参数相对应。您应该复制此文件，然后修改文件的内容，以适应安装环境。
JBossMySQL.bin 或 JBossMySQL.exe	用于安装 JBoss Application Server 和 MySQL 数据库的一个方便的实用程序。
nmassaml.zip	包含一个 eDirectory 方法来支持 SAML。仅在不使用 Access Manager 时才需要。
afadmin.jar	仅对 Identity Manager 3.5.1 元目录是必需的。
prerequisitefiles.zip	仅对 Identity Manager 3.5.1 元目录是必需的。
	包含必须手动复制到正确位置的其他文件。

安装 Identity Manager 基于角色的供应模块或 User Application 标准版的系统必须至少具有 320 MB 可用于储存所支持应用程序 （数据库、应用程序服务器等）的额外空间。随着时间的推移，系统将需要更多的空间来容纳不断增多的其他数据，如数据库或应用程序服务器日志。

默认安装位置为：

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

安装时还可以选择其他默认安装目录，但该目录必须在开始安装前就存在并且是可写的（如果在 Linux 或 Solaris 中，必须是非根用户也可以写入）。

2.3 安装应用程序服务器

- 第 2.3.1 节 “ 安装 JBoss Application Server”（第 17 页）
- 第 2.3.2 节 “ 安装 WebLogic Application Server”（第 18 页）
- 第 2.3.3 节 “ 安装 WebSphere Application Server”（第 19 页）

2.3.1 安装 JBoss Application Server

如果计划使用 JBoss Application Server，您可以：

- 根据制造商的指导下载并安装 JBoss Application Server。请参阅第 1.3 节 “ 系统要求 ”（第 10 页）以了解受支持的版本。
- 使用基于角色的供应模块下载中提供的 JBossMySQL 实用程序安装 JBoss Application Server （可选安装 MySQL）。有关指导，请参阅安装 JBoss Application Server 和 MySQL 数据库 （第 17 页）。

在安装 Identity Manager 基于角色的供应模块之前，请不要启动 JBoss 服务器。启动 JBoss 服务器是安装后任务。

表 2-3 *JBoss Application Server 最低推荐要求*

组件	推荐
RAM	运行 Identity Manager 基于角色的供应模块时，建议 JBoss Application Server RAM 的最低要求是 512 MB。
端口	8080 是应用程序服务器的默认端口。记录下应用程序服务器所使用的端口。
SSL	如果计划使用外部口令管理，请启用 SSL： ◆ 在您部署 Identity Manager 基于角色的供应模块和 IDMPwdMgt.war 文件的 JBoss 服务器上启用 SSL。 ◆ 确保防火墙上打开了 SSL 端口。 有关启用 SSL 的信息，请参阅 JBoss 文档。 有关 IDMPwdMgt.war 文件的信息，请参阅第 8.5 节 “ 配置外部口令管理 ”（第 57 页）和《*User Application：管理指南* (http://www.novell.com/documentation/idmrbpm361/index.html)》。

安装 JBoss Application Server 和 MySQL 数据库

JBossMysql 实用程序在您的系统上安装 JBoss Application Server 和 MySQL。此实用程序不支持控制台方式，它需要图形用户界面环境。对 Linux/Unix 用户，建议您以非根用户身份安装它。

1 从 .iso 上查找并执行 JBossMySQL.bin 或 JBossMySQL.exe。

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

Solaris 不提供此实用程序。

2 遵照关于导航该实用程序的屏幕指导进行操作。参考下表获取其他信息。

安装屏幕	说明
选择安装集	选择要安装的产品。 ◆ *JBoss*：将 JBoss Application Server 安装到您指定的目录下，同时安装用于启动和停止它的脚本。 **注释：**此实用程序不将 JBoss Application Server 作为 Windows 服务安装。有关指导，请参阅安装 JBoss Application Server 作为一项服务或一个守护程序 （第 18 页）。 ◆ *MySQL*：在您指定的目录下安装 MySQL 并创建一个 MySQL 数据库，同时安装用于启动和停止它的脚本。
选择 JBoss 父文件夹	单击*选择*可选择不是默认文件夹的安装文件夹。
选择 MySQL 父文件夹	单击*选择*可选择不是默认文件夹的安装文件夹。
MySQL 信息	指定以下内容： ◆ *数据库名称*：指定安装程序要创建的数据库的名称。 User Application 安装实用程序会提示您输入此名称，因此，您应该记下该名称和位置。 ◆ *“根”用户口令*（并确认口令）：指定此数据库的根口令 （并确认口令）。
预安装摘要	查看“摘要”页面。如果规范正确，请单击*安装*。

安装选定产品之后，实用程序将显示一条成功完成的讯息。如果安装了 MySQL 数据库，请继续第 2.4.1 节“配置 MySQL 数据库”（第 19 页）。

安装 JBoss Application Server 作为一项服务或一个守护程序

要将 JBoss Application 作为守护程序启动，请参阅来自 JBoss (http://wiki.jboss.org/wiki/Wiki.jsp?page=StartJBossOnBootWithLinux) 的指导。

使用 JavaServiceWrapper 使用 JavaServiceWrapper，可以安装、启动和停止 JBoss Application Server，以作为 Windows 服务或 Linux 或 UNIX 守护程序进程。 JBoss 的说明请参阅 http://wiki.jboss.org/wiki/Wiki.jsp?page=RunJBossAsAServiceOnWindows (http://wiki.jboss.org/wiki/Wiki.jsp?page=RunJBossAsAServiceOnWindows)。以下展示一个这样的封装程序：http://wrapper.tanukisoftware.org/doc/english/integrate-simple-win.html (http://wrapper.tanukisoftware.org/doc/english/integrate-simple-win.html)：用 JMX 管理它 （参阅 http://wrapper.tanukisoftware.org/doc/english/jmx.html#jboss (http://wrapper.tanukisoftware.org/doc/english/jmx.html#jboss)）。

重要：对于先前版本，可以使用第三方实用程序 （如 JavaService）作为一项 Windows 服务安装、启动和停止 JBoss 应用程序服务器，但 JBoss 不再推荐使用 JavaService。有关详细信息，请参阅 http://wiki.jboss.org/wiki/Wiki.jsp?page=JavaService (http://wiki.jboss.org/wiki/Wiki.jsp?page=JavaService)。

2.3.2 安装 WebLogic Application Server

如果计划使用 WebLogic Application Server 10，请下载并安装。请参阅第 1.3 节“系统要求”（第 10 页）获取有关受支持版本的信息。

2.3.3 安装 WebSphere Application Server

如果计划使用 WebSphere Application Server 6.1，请下载并安装。请参阅第 1.3 节 “ 系统要求 ”（第 10 页）获取有关受支持版本的信息。

2.4 安装数据库

User Application 使用数据库来完成各项任务，如储存配置数据和任何工作流程活动的数据。安装基于角色的供应模块或 User Application 前，必须安装并配置了在您的平台上受支持的数据库之一。其中包括：

- ❑ 安装数据库和数据库驱动程序。
- ❑ 创建数据库或数据库实例。
- ❑ 记录以下数据库参数，以在 Identity Manager 基于角色的供应模块的安装过程中使用：
  - 主机和端口
  - 数据库名称、用户名和用户口令
- ❑ 创建指向该数据库的数据源文件。

  方法因应用程序服务器而异。对于 JBoss， Identity Manager 基于角色的供应模块安装程序创建指向数据库的应用程序服务器数据源文件，并根据 Identity Manager 基于角色的供应模块 WAR 文件名称命名文件。对于 WebSphere 和 WebLogic，请在安装前手动配置数据源。
- ❑ 数据库必须支持 UTF-8。

注释：如果正要迁移到基于角色的供应模块的新版本，则必须使用之前安装 （即要迁移的安装版本）所用的同一 User Application 数据库。

2.4.1 配置 MySQL 数据库

User Application 需要 MySQL 的某些配置选项。如果您自己安装 MySQL，请配置以下设置。如果通过使用 JbossMysql 实用程序安装 MySQL，则实用程序将为您设置正确的值，但需要知道为以下项目保留的值：

- INNODB 储存引擎和表类型 （第 19 页）
- 字符集 （第 20 页）
- 区分大小写 （第 20 页）

INNODB 储存引擎和表类型

User Application 使用了 INNODB 储存引擎，通过它可以选择为 MySQL 指定 INNODB 表类型。如果创建 MySQL 表时没有指定表类型，默认情况下，该表采用 MyISAM 表类型。如果选择在 Identity Manager 安装过程中安装 MySQL，则在此过程中安装的 MySQL 采用指定的 INNODB 表类型。为确保 MySQL 服务器使用 INNODB，请校验 my.cnf （Linux 或 Solaris）或 my.ini (Windows) 中包含以下选项：

default-table-type=innodb

它不应包含 skip-innodb 选项。

字符集

将整个服务器或仅仅某个数据库的字符集指定为 UTF-8。要在整个服务器范围内指定 UTF-8，可在 my.cnf （Linux 或 Solaris）或者 my.ini (Windows) 中包含以下选项：

character_set_server=utf8

也可以在创建数据库时使用以下命令指定数据库字符集：

create database databasename character set utf8 collate utf8_bin;

如果为数据库设置了字符集，还必须在 IDM-ds.xml 文件的 JDBC* URL 中指定该字符集，如以下示例所示：

```
<connection-url>jdbc:mysql://localhost:3306/
databasename?useUnicode=true&amp;characterEncoding=utf8&amp;connectionCollation=ut
f8_bin</connection-url>
```

区分大小写

如果计划跨服务器或平台备份或恢复数据，请确保所有服务器或平台上的大小写保持一致。要确保该一致性，请为所有 my.cnf （Linux 或 Solaris）或 my.ini (Windows) 文件中的 lower_case_table_names 指定相同的值 （0 或 1），而不是接受默认值 （Windows 默认为 0，而 Linux 默认为 1。）请在创建数据库保存 Identity Manager 表之前指定该值。例如，对于所有计划备份和恢复数据库的平台，可以指定

lower_case_table_names=1

（在 my.cnf 和 my.ini 文件中）。

2.5 安装 Java 开发工具包

基于角色的供应模块和 User Application 标准版安装程序最低需要使用 Java 2 开发平台标准版 (Java 2 Platform Standard Edition) 开发工具包版本 1.5。

将 JAVA_HOME 环境变量设置为指向 JDK*，以配合用户应用程序使用。或者，在 User Application 安装过程中手动指定路径，以覆盖 JAVA_HOME。

注释：对于 SUSE Linux Enterprise Server (SLES) 用户：请不要使用 SLES 随附的 IBM* JDK。此版本与部分安装过程不兼容。必须使用 Sun JDK。

2.6 安装元目录 3.5.1 的其他文件

如果使用 Identity Manager 元目录 3.5.1，则必须执行以下部分中所述的更多步骤：

- 第 2.6.1 节 “ 通过使用 GUI 安装角色服务驱动程序 ”（第 21 页）
- 第 2.6.2 节 “ 从控制台安装角色服务驱动程序 ”（第 22 页）
- 第 2.6.3 节 “ 复制 iManager 图标 ”（第 22 页）
- 第 2.6.4 节 “ 复制 afadmin.jar”（第 22 页）

对 Linux/Unix 用户，请以根用户身份安装它。

2.6.1 通过使用 GUI 安装角色服务驱动程序

仅在使用 Identity Manager 3.5.1 元目录时才需要此步骤。如果安装了 Identity Manager 3.6 元目录，则这些文件已经安装。

角色服务和 User Application 驱动程序实用程序提供了选项来执行以下操作：

- 扩展身份库纲要以支持 User Application 和基于角色的供应模块
- 将角色服务驱动程序和 User Application 驱动程序配置文件安装到元目录服务器。
- 将角色服务和 User Application 驱动程序配置文件安装到 iManager。

您将必须在元目录和 iManager 计算机上运行此安装程序。

注释：元目录必须安装在默认的位置才能使用此安装程序。

访问 Roles_Driver_Install_Utility.iso

1 为您的操作系统查找并执行此安装程序：

操作系统	角色服务驱动程序安装程序
AIX	roles_driver_install.aix.bin
Linux	roles_driver_install.linux.bin
Solaris	roles_driver_install.solaris.bin
Windows	roles_dirver_install.exe

2 使用以下信息完成安装：

安装屏幕	说明
许可协议	阅读许可协议，然后选择*我接受本许可协议的条款*。
选择组件	*驱动程序*：将角色服务驱动程序和 User Application 驱动程序安装到元目录服务器，然后更新支持库 JAR。 *纲要*：更新元目录纲要以包括基于角色的供应模块和 User Application 标准版所需的对象。它安装 nrf-extensions.sch 文件和 srvprv.sch 文件，然后对当前平台运行命令 （对于 Windows 为 NdsCons.exe，对于 UNIX/Linux 为 ndssch）。 *驱动程序配置文件*：安装角色服务驱动程序和 User Application 驱动程序配置文件。当您在 iManager 中创建新的驱动程序时将使用这些文件。您必须在托管 iManager 的计算机上运行此项。
鉴定	当选择*纲要扩展*时，必须指定用户名和口令。此用户必须具有该身份库的管理权限。例如， *cn=admin,o=novell*。
选择驱动程序的位置	如果选择安装角色服务和 User Application 驱动程序，系统将提示您输入在 eDirectory 服务器上的位置。它们通常安装在元目录的 /lib/dirxml/classes 目录下。
驱动程序配置文件的安装位置	指定安装程序应将驱动程序配置文件放置在 iManager 计算机上的位置。这些文件通常安装在 iManager 的 /nps/Dirxml.Drivers 目录下。

安装屏幕	说明
安装前摘要	阅读“安装前摘要”页面，校验所选的安装参数，然后完成安装。

2.6.2 从控制台安装角色服务驱动程序

要以控制台（字符）模式运行安装程序，请发出以下命令：

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

遵循第 2.6.1 节“通过使用 GUI 安装角色服务驱动程序”（第 21 页）下对图形用户界面所述的相同步骤，阅读提示，然后在命令行处输入应答。

2.6.3 复制 iManager 图标

注释：如果安装了 iManager 2.7 及最新插件，则此过程不是必需的。

1. 如果下载了 .iso 映像，请查找 prerequisites.zip 文件。
2. 解压缩该文件，然后查找 iManager_icons_for_roles.zip 文件。

   这包含 eDirectory 中角色对象的 iManager 图标。
3. 解压缩该文件，然后将解压缩出的图标复制到 nps/portal/modules/dev/images/dir 目录。
4. 重启动 iManager 以便使用新图标。

2.6.4 复制 afadmin.jar

注释：如果安装了 iManager 2.7 及最新插件，则此过程不是必需的。

1. 如果下载了 .iso 映像，请查找 prerequisites.zip。

   您可以在 /36MetaDirSupport 目录中找到该文件。
2. 解压缩该文件，然后查找 afadmin.jar 文件。
3. 将 afadmin.jar 文件复制到 /iManager/nps/WEB-INF/lib 目录下。

创建驱动程序

3

本节说明如何创建使用基于角色的供应模块所需的驱动程序。包括以下主题：

重要：在创建角色服务驱动程序前，需要创建 User Application 驱动程序。需要先创建 User Application 驱动程序，因为角色服务驱动程序参照 User Application 驱动程序中的角色库容器 (RoleConfig.AppConfig)。

该驱动程序配置支持允许您执行以下操作：

- 将一个 User Application 驱动程序与一个角色服务驱动程序相关联。
- 将一个 User Application 与一个 User Application 驱动程序相关联。

3.1 在 iManager 中创建 User Application 驱动程序

基于角色的供应模块在 User Application 驱动程序中储存特定于应用程序的数据，以控制和配置应用程序环境。这包括应用程序服务器群集信息和工作流程引擎配置。

除了群集中基于角色的供应模块外，必须为每个 Identity Manager 基于角色的供应模块创建一个 User Application 驱动程序。同一群集中的基于角色的供应模块必须共享一个 User Application 驱动程序。有关在群集中运行基于角色的供应模块的信息，请参阅 《*User Application：管理指南* (http://www.novell.com/documentation/idmrbpm361/index.html)》。

重要：配置一组非群集基于角色的供应模块来共享一个驱动程序会使基于角色的供应模块中运行的一个或多个组件引起混淆。所导致的问题的根源难以检测。

要创建 User Application 驱动程序并将其与驱动程序集关联，请执行下列操作：

1. 在万维网浏览器中打开 iManager。

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

2. 请转到*角色和任务* > *Identity Manager 实用程序*并选择*新驱动程序*或*导入配置*（取决于您使用的插件版本）。

   对于 Identity Manager 3.5.1，请使用*新建驱动程序*链接。

   对于 Identity Manager 3.6，请使用*导入配置*链接。

3. 要在现有驱动程序集中创建驱动程序，选中*在现有驱动程序中*，单击对象选择器图表，选择驱动程序集对象，单击*下一步*，然后继续 步骤 4。

   或

如果需要新建驱动程序集 （比如，如果要将 User Application 驱动程序放置到不同于其他驱动程序的服务器上），选择*在新驱动程序集中*，单击*下一步*，然后定义新驱动程序集的属性。

3a 指定新驱动程序集的名称、环境和服务器。环境是服务器对象所在的 eDirectory™ 环境。

3b 单击*下一步*。

4 单击*从服务器导入驱动程序配置 （.XML 文件）*。

5 从下拉列表中选择 User Application 驱动程序配置文件。文件名为：

UserApplication_3_6_1-IDM3_5_1-V1.xml

如果此文件不在列表中，则角色服务驱动程序可能未正确安装。请参考第 2.6.1 节 “ 通过使用 GUI 安装角色服务驱动程序 ”（第 21 页）。

6 单击*下一步*。

7 将提示您提供驱动程序的参数。（通过滚动查看全部内容。）将参数记录下来，在安装基于角色的供应模块时将用到它们。

字段	说明
驱动程序名	创建的驱动程序的名称。
鉴定 ID	User Application 管理员的判别名。这是将赋予其管理用户应用程序入口权限的用户应用程序管理员。使用 eDirectory™ 格式，例如 admin.orgunit.novell，或通过浏览查找用户。这是一个必需的字段。
口令	鉴定 ID 中所指定 User Application 管理员的口令。
应用程序环境	User Application 环境。此为 User Application WAR 文件的 URL 的环境部分。默认为 *IDM*。
主机	部署 Identity Manager User Application 的应用程序服务器的主机名或 IP 地址。 如果 User Application 在群集中运行，请键入发送程序的主机名或 IP 地址。
端口	以上所列主机的端口。
允许覆盖启动程序:	通过选择 *是*，允许供应管理员以被指定为代理的用户的名义启动工作流程。

8 单击*下一步*。

9 单击*定义安全性等效*以打开 “ 安全性等效 ” 窗口 。浏览并选择管理员或其他主管对象，然后单击*添加*。

此步骤可为驱动程序指定所需的安全性许可权限。可以在 Identity Manager 文档中找到有关此步骤的重要性的细节。

10 （可选，但不推荐）单击*排除管理角色*。

11 单击*添加*，选择要在驱动程序操作 （如管理角色）中排除的用户，单击*确定*两次，然后单击*下一步*。

12 单击*确定*关闭 “ 安全性等效 ” 窗口，然后单击*下一步*显示摘要页面。

13 如果信息准确无误，则单击*完成*或*浏览完毕*。

重要：默认情况下，驱动程序为关闭状态。使驱动程序处于关闭状态，直到基于角色的供应模块安装完成为止。

3.2 在 iManager 中创建角色服务驱动程序

注释：如果使用 User Application 标准版，则不需要执行本部分的这些步骤。

在 iManager 中创建和配置角色服务驱动程序：

1. 在万维网浏览器中打开 iManager。

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

2. 在 *Identity Manager* > *Identity Manager 概述*下，选择要安装角色服务驱动程序的驱动程序集。

   先安装 User Application 驱动程序，再安装角色服务驱动程序。将 User Application 驱动程序版本 3.6.1 (UserApplication_3_6_1-IDM3_5_1-V1.xml) 与角色服务驱动程序一起使用。如果使用其他版本的 User Application 驱动程序，则角色编目将不可用。

3. 单击*添加驱动程序*。

4. 在该向导中，保留*现有驱动程序集*中的默认值。单击“下一步”。

5. 从下拉列表中选择 *RoleService_3_6_1-IDM3_5_1-V1.xml*。这是支持基于角色的供应模块的角色服务驱动程序配置文件。

   如果它不在此下拉列表中，则您还未将此文件复制到正确的位置。请参考第 2.6.1 节“通过使用 GUI 安装角色服务驱动程序”（第 21 页）。

   单击*下一步*。

   尝试创建驱动程序时，可能会看到以下错误：

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

   如果出现此情况，则 iManager 应用程序可能尚未获得新的角色纲要。新的纲要对于角色服务驱动程序是必需的。尝试重启动 iManager 和 eDirectory，以确保正确选择了所有新的纲要更改。

6. 在“导入请求信息”页面，填写请求的信息。下表说明了请求的信息。

选项	说明
驱动程序名	指定驱动程序名称或保留角色服务驱动程序的默认名称角色服务。如果用与现有驱动程序相同的名称安装新的驱动程序，则新驱动程序将重写现有驱动程序的配置。 使用*浏览*按钮查看所选驱动程序集上现有的驱动程序。这是一个必需的字段。
用户 - 组基本容器 DN	驱动程序仅对此基本容器中的用户、容器和组起作用。如果存在组角色指派，角色驱动程序仅对该容器域中的成员授予 / 撤消角色。

选项	说明
User Application 驱动程序 DN	主管角色系统的 User Application 驱动程序对象的判别名。使用 eDirectory 格式，如 UserApplication.driverset.org，或通过浏览找到驱动程序对象。这是一个必需的字段。
User Application URL	用于连接到 User Application 以启动批准工作流程的 URL。示例中给出的 URL 是 *http://host:port/IDM*。这是一个必需的字段。
User Application 身份	用于鉴定到 User Application 以启动批准工作流程的对象的判别名。这可以是将赋予其管理 User Application 门户权限的 User Application 管理员。使用 eDirectory 格式，如 admin.department.org，或通过浏览找到用户。这是一个必需的字段。
User Application 口令	鉴定 ID 中所指定 User Application 管理员的口令。口令用于鉴定到 User Application 以启动批准工作流程。这是一个必需的字段。
重输门户令	重输入 User Application 管理员口令。

7 填充信息后，单击*下一步*。

8 单击*定义安全性等效*以打开 “ 安全性等效 ” 窗口 。浏览并选择管理员或其他主管对象，然后单击*添加*。

此步骤可为驱动程序指定所需的安全性许可权限。可以在 Identity Manager 文档中找到有关此步骤的重要性的细节。

9 （可选，但不推荐）单击*排除管理角色*。

10 单击*添加*，选择要在驱动程序操作 （如管理角色）中排除的用户，单击*确定*两次，然后单击*下一步*。

11 单击*确定*关闭 “ 安全性等效 ” 窗口，然后单击*下一步*显示摘要页面。

12 如果信息正确，请单击*完成*。

4 使用 GUI 安装程序在 JBoss 上进行安装

本节说明如何在 JBoss Application Server 上通过使用安装程序的图形用户界面版本来安装 Identity Manager 基于角色的供应模块。它包含以下主题：

- 第 4.1 节 “ 安装和配置 User Application WAR”（第 27 页）
- 第 4.2 节 “ 测试安装 ”（第 32 页）

如果要使用命令行进行安装，请参阅第 7 章 “ 从控制台或使用单条命令进行安装 ”（第 47 页）。

以非根用户身份运行安装程序。

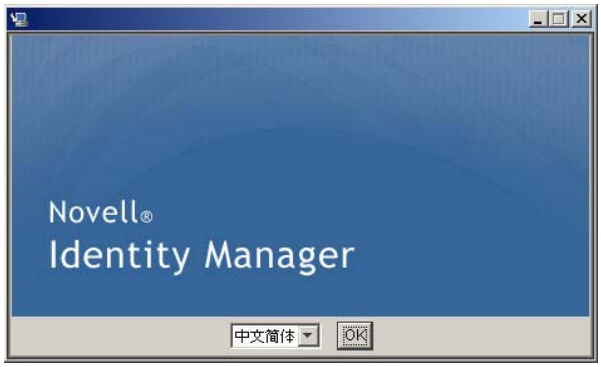
4.1 安装和配置 User Application WAR

注释 : 安装程序至少需要 Java 2 开发平台标准版开发工具包版本 1.5。如果使用更早的版本，安装过程将不会成功配置 User Application WAR 文件。安装看似成功，但尝试启动 User Application 时遇到错误。

1 从命令行起动平台的安装程序：

java -jar IdmUserApp.jar

当安装程序起动时，系统将提示您选择语言。



2 使用以下每个安装面板上的指导随附的信息完成安装：

安装屏幕	说明
Novell Identity Manager	选择安装程序的语言。默认为英语。
许可协议	阅读许可协议，然后选择 *我接受本许可协议的条款*。
应用程序服务器平台	选择 *JBoss*。

安装屏幕	说明
标准或供应	*标准*：如果安装 User Application 标准版，请选择此选项。 *基于角色的供应*：如果安装基于角色的供应模块，请选择此选项。
数据迁移	接受默认值 （校验未选择*是*）。 **警告：**不能选择*是*，如果选择 “ 是 ”，您将在启动 User Application 时遇到问题。 有关迁移的信息，请参阅 《*User Application：迁移指南* (http://www.novell.com/documentation/idmrbpm361/index.html)》。
WAR 在哪里？	如果 Identity Manager User Application WAR 文件所在的目录不同于安装程序，安装程序将提示提供 WAR 的路径。
选择安装文件夹	指定安装程序放置这些文件的位置。
数据库平台	选择数据库平台。必须已安装数据库和 JDBC 驱动程序。选项包括： ◆ MySQL ◆ Oracle （系统提示您提供 Oracle 版本） ◆ MS SQL Server
数据库主机和端口	*主机*：指定数据库服务器的主机名或 IP 地址。对于群集，对其中每个成员指定相同的主机名或 IP 地址。 *端口*：指定数据库监听程序的端口号。对于群集，对其中每个成员指定相同的端口。
数据库名称和特权用户	*数据库名称*（或 SID）：对于 MySQL 或 MS SQL Server，请提供预配置数据库的名称。对于 Oracle，请提供以前创建的 Oracle 系统标识符 (SID)。对于群集，对其中每个成员指定相同的数据库名称或 SID。 *数据库用户*：指定数据库用户。对于群集，对其中每个成员指定相同的数据库用户。 *数据库口令 / 确认口令*：指定数据库口令。对于群集，对其中每个成员指定相同的数据库口令。
Java 安装	指定 Java 安装根文件夹。

系统将提示您有关安装 JBoss Application Server 的位置的信息。

3 使用以下信息完成此面板，然后继续进行安装。

安装屏幕	说明
JBoss 配置	告知 User Application JBoss Application Server 所在的位置。 此安装过程不安装 JBoss Application Server。有关安装 JBoss Application Server 的指导，请参阅安装 JBoss Application Server 和 MySQL 数据库（第 17 页）。 *基本文件夹*：指定应用程序服务器的位置。 *主机*：指定应用程序服务器的主机名或 IP 地址。 *端口*：指定应用程序服务器的监听程序端口号。 JBoss 默认端口为 8080。
IDM 配置	选择应用程序服务器配置的类型： ◆ 如果此安装是群集中的一部分，选择 *全部* ◆ 如果此安装是单独节点，而不是群集的一部分，选择 *默认* 如果选择 *默认值*，并决定稍后需要群集，则必须重新安装 User Application。 *应用程序名称*：应用程序服务器配置的名称、应用程序 WAR 文件的名称和 URL 环境的名称。安装脚本创建服务器配置，并默认根据 *应用程序名称* 对配置命名。将应用程序名称记录下来，当从浏览器启动 User Application 时，将其添加到 URL 中。 *工作流程引擎 ID*：群集中的每个服务器都必须具有唯一的工作流程引擎 ID。工作流程引擎 ID 在 《*User Application：管理指南*》的第 3.5.4 节 “ 为群集配置工作流程 ” 中说明。
Audit 日志记录	要启用日志记录，请单击 *是*。下一面板将提示您指定日志记录的类型。从以下选项中选择： ◆ *Novell Audit*：启用 User Application 的 Novell® Audit 日志记录。 ◆ *OpenXDAS*：事件将记录到 OpenXDAS 日志记录服务器中。 有关设置 Novell Audit 或 OpenXDAS 日志记录的更多信息，请参阅 《*User Application：管理指南*》。

安装屏幕	说明
Novell Audit	*服务器*：如果启用了 Novell Audit 日志记录，请指定 Novell Audit 服务器的主机名或 IP 地址。如果禁用日志记录，将忽略此值。 *日志超速缓存文件夹*：指定日志记录超速缓存的目录。
安全 — 主密钥	*是*：允许您导入现有的主密钥。如果选择导入现有经加密的主密钥，请将密钥剪切并粘贴到安装过程窗口。 *否*：创建新的主密钥。完成安装后，必须手动记录主密钥，如第 8.1 节 “ 记录主密钥 ”（第 55 页）中所述。 安装过程中会将经加密的主密钥写到安装目录中的 master-key.txt 文件中。 导入现有主密钥的原因包括： ◆ 将安装从分级系统移到生产系统，并想保留访问过去分级系统中使用的数据库。 ◆ 已将 User Application 安装在 JBoss 群集中的第一个成员上，现在在群集中的后续成员上执行安装。 ◆ 由于磁盘故障，需要恢复 User Application。必须重新安装 User Application，并指定以前安装过程中所使用的同一个经过加密的主密钥。这样可以获得以前储存的加密数据的访问权。

4 系统会提示您提供安装程序用于配置 User Application WAR 文件的信息。（如果未提示您提供此信息，则您可能未完成第 2.5 节 “ 安装 Java 开发工具包 ”（第 20 页）中所述的步骤。

5 使用以下信息填写该面板，并继续进行安装。

安装屏幕	说明
User Application 配置	在 User Application 安装过程中，可以设置 User Application 配置参数。其中大部分参数都还可以于安装在 configupdate.sh 或 configupdate.bat 中进行配置，有关例外的项，参阅参数说明中的注释。 对于群集，对其中每个成员指定相同的 User Application 配置参数。 请参阅附录 A“IDM User Application 配置参照 ”（第 61 页）获取每个选项的说明。
安装前摘要	阅读 “ 安装前摘要 ” 页面，校验所选的安装参数。 如有必要，使用*上一步*返回到前面的安装页，对安装参数作出更改。 User Application 配置页的值没有保存下来，因此，在重新指定安装中的以前页面之后，必须重新输入 User Application 配置值。当安装和配置参数令人满意之后，返回 “ 安装前摘要 ” 页，然后单击*安装*。
安装完成	指示安装完成。

4.1.1 查看安装和日志文件

如果安装成功完成，没有错误，请继续测试安装。如果安装提示出现错误或警告，请检查日志文件以确定问题：

- Identity_Manager_User_Application_Installlog.log 保存基本安装任务的结果。
- Novell-Custom-Install.log 记录了有关安装过程中所执行的 User Application 配置。

4.2 测试安装

1 启动数据库。有关指导，请参阅数据库文档。

2 启动 User Application 服务器 (JBoss) 在命令行上，将安装目录更改为工作目录，然后执行以下底稿 （由 User Application 安装所提供）：

start-jboss.sh （Linux 和 Solaris）

start-jboss.bat (Windows)

要停止应用程序服务器，请使用 stop-jboss.sh 或 stop-jboss.bat，或者关闭正在运行 start-jboss.sh 或 start-jboss.bat 的窗口。

如果不是在 X11 Window 系统上运行，则需要在服务器启动脚本中包括 -Djava.awt.headless=true 标志。要运行报告，必须执行此操作。例如，您可以将以下行包括到脚本中：

JAVA_OPTS="-Djava.awt.headless=true -server -Xms256M -Xmx256M-XX:MaxPermSize=256m"

3 启动 User Application 驱动程序。这将启动到 User Application 驱动程序的通讯。

3a 登录 iManager。

3b 在左侧浏览帧中显示的 “ 角色和任务 ” 中，选中 *Identity Manager* 下面的 *Identity Manager 概述*。

3c 在显示的内容视图中，指定包含 User Application 驱动程序的驱动程序集，然后单击*搜索*。将出现一个图形，其中显示该驱动程序集及其关联的驱动程序。

3d 单击驱动程序上的红白色图标。

3e 选择*启动驱动程序*。驱动程序状态更改为阴阳符号，指示驱动程序先已启动。

在启动时，驱动程序将尝试与 User Application 进行 “ 握手 ” 通讯。如果应用程序服务器没有运行，或者如果 WAR 未成功部署，则驱动程序将返回错误。

4 要启动并登录到 User Application，请使用万维网浏览器并访问以下 URL：

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

在此 URL 中， *hostname*: *port* 是应用程序服务器主机名 （例如 myserver.domain.com），而 port 为应用程序服务器的端口 （例如 JBoss 上默认为 8080）。默认情况下，*ApplicationName* 为 *IDM*。在安装过程中提供应用程序服务器配置信息时指定应用程序名称。

会显示 Novell Identity Manager User Application 登录页。

5 在该页的右上角，单击*登录*可登录 User Application。

完成这些步骤之后，如果浏览器中还没有显示 Identity Manager User Application 页，请检查终端控制台上是否有错误讯息，并参阅第 8.7 节 “ 查错 ” （第 59 页）。

使用 GUI 安装程序在 WebSphere Application Server 上进行安装

5

本节说明如何在 WebSphere Application Server 上通过安装程序的图形用户界面版本安装 Identity Manager User Application。

以非根用户身份运行安装程序。

5.1 安装和配置 User Application WAR

注释 : 安装程序至少需要 Java 2 开发平台标准版开发工具包版本 1.5。如果使用更早的版本，安装过程将不会成功配置 User Application WAR 文件。安装看似成功，但尝试启动 User Application 时遇到错误。

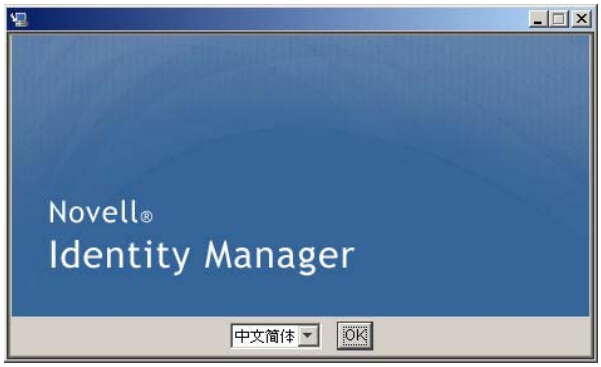
1 浏览找到包含安装文件的目录。

2 起动安装程序：

java -jar IdmUserApp.jar

对于 WebSphere，必须使用应用了无限制策略文件的 IBM JDK。

当安装程序起动时，系统将提示您选择语言。



3 使用以下每个安装面板上的指导随附的信息完成安装：

安装屏幕	说明
Novell Identity Manager	选择安装程序的语言。默认为英语。
许可协议	阅读许可协议，然后选择 *我接受本许可协议的条款*。

安装屏幕	说明
应用程序服务器平台	选择 *WebSphere*。 如果 User Application WAR 文件所在的目录不同于安装程序，安装程序将提示提供 WAR 的路径。 如果 WAR 在默认位置，可以单击*恢复默认文件夹*。或者，要指定 WAR 文件的位置，单击*选择*并选择某个位置。
标准或供应	*标准*：如果安装 User Application 标准版，请选择此选项。 *基于角色的供应*：如果安装基于角色的供应模块，请选择此选项。
数据迁移	接受默认值 （校验未选择*是*）。 **警告：**不能选择*是*，如果选择 “ 是 ”，您将在启动 User Application 时遇到问题。 有关迁移的信息，请参阅 《*User Application：迁移指南* (http://www.novell.com/documentation/idmrbpm361/index.html)》。
WAR 在哪里？	如果 Identity Manager User Application WAR 文件所在的目录不同于安装程序，安装程序将提示提供 WAR 的路径。
选择安装文件夹	指定安装程序放置这些文件的位置。
数据库平台	选择数据库平台。必须已安装数据库和 JDBC 驱动程序。选项包括： ◆ Oracle （系统提示您提供 Oracle 版本） ◆ MS SQL Server ◆ DB2
Java 安装	指定 Java 安装根文件夹。 **注释：**对于 WebSphere，必须使用应用了无限制策略文件的 IBM JDK。
IDM 配置	指定应用程序环境
Audit 日志记录	要启用日志记录，请单击*是*。下一面板将提示您指定日志记录的类型。从以下选项中选择： ◆ *Novell Audit*：启用 User Application 的 Novell Audit 日志记录。有关设置 Novell Audit 日志记录的更多信息，请参阅《*Identity Manager User Application：管理指南*》。 ◆ *OpenXDAS*：事件将记录到 OpenXDAS 日志记录服务器中。 有关设置 Novell Audit 或 OpenXDAS 日志记录的更多信息，请参阅 《*User Application：管理指南*》。
Novell Audit	*服务器*：如果启用了 Novell Audit 日志记录，请指定 Novell Audit 服务器的主机名或 IP 地址。如果禁用日志记录，将忽略此值。 *日志超速缓存文件夹*：指定日志记录超速缓存的目录。

安装屏幕	说明
安全 — 主密钥	*是*：允许您导入现有的主密钥。如果选择导入现有经加密的主密钥，请将密钥剪切并粘贴到安装过程窗口。 *否*：创建新的主密钥。完成安装后，必须手动记录主密钥。 安装过程中会将经加密的主密钥写到安装目录中的 master-key.txt 文件中。 导入现有主密钥的情况例如： ◆ 将安装从分级系统移到生产系统，并想保留访问过去分级系统中使用的数据库。 ◆ 已将 User Application 安装在群集中的第一个成员上，现在在群集中的后续成员上执行安装 （它们需要同一主密钥）。 ◆ 由于磁盘故障，需要恢复 User Application。必须重新安装 User Application，并指定以前安装过程中所使用的同一个经过加密的主密钥。这样可以获得以前储存的加密数据的访问权。

4 系统会提示您提供安装程序用于配置 User Application WAR 文件的信息。（如果未提示您提供此信息，则您可能未完成第 2.5 节“ 安装 Java 开发工具包 ”（第 20 页）中所述的步骤。

5 使用以下信息填写该面板，并继续进行安装。

安装屏幕	说明
User Application 配置	在 User Application 安装过程中，可以设置 User Application 配置参数。其中大部分参数都还可以于安装在 configupdate.sh 或 configupdate.bat 中进行配置，有关例外的项，参阅参数说明中的注释。 有关详细信息，请参阅附录 A“IDM User Application 配置参照 ”（第 61 页）。
安装前摘要	阅读 “ 安装前摘要 ” 页，校验所选的安装参数。 如有必要，使用*上一步*返回到前面的安装页，对安装参数作出更改。 User Application 配置页的值没有保存下来，因此，在重新指定安装中的以前页面之后，必须重新输入 User Application 配置值。当安装和配置参数令人满意之后，返回 “ 安装前摘要 ” 页，然后单击*安装*。
安装完成	指示安装已完成。

5.1.1 查看安装日志文件

如果安装成功完成，没有错误，请继续第 5.2.1 节 “ 添加 User Application 配置文件和 JVM 系统属性 ”（第 36 页）。

如果安装提示出现错误或警告，请检查日志文件以确定问题：

- Identity_Manager_User_Application_Installlog.log 保存基本安装任务的结果。
- Novell-Custom-Install.log 记录了有关安装过程中所执行的 User Application 配置。

5.2 配置 WebSphere 环境

- 第 5.2.1 节 “ 添加 User Application 配置文件和 JVM 系统属性 ”（第 36 页）
- 第 5.2.2 节 “ 将 eDirectory 可信根导入 WebSphere 密钥储存区 ”（第 37 页）

5.2.1 添加 User Application 配置文件和 JVM 系统属性

要成功安装 WebSphere，必须执行以下步骤：

1. 将 sys-configuration-xmldata.xml 文件从 User Application 安装目录复制到主管 WebSphere 服务器的计算机上的某个目录，例如， /UserAppConfigFiles。

   User Application 安装目录是安装有 User Application 的目录。
2. 在 JVM 系统属性中设置 sys-configuration-xmldata.xml 文件的路径。作为管理员用户登录到 WebSphere 管理控制台执行此操作。
3. 从左面板中，转到*服务器* > *应用程序服务器*
4. 单击服务器列表中的服务器名称，例如 server1。
5. 在右边的设置列表中，转到*服务器基础结构*下的 *Java 和进程管理*。
6. 展开链接，并选择*进程定义*。

7 在*其他属性*列表下，选择 *Java 虚拟机*。

8 选择 JVM 页标题*其他属性*下的 *自定义属性*。

9 单击*新建*可添加新 JVM 系统属性。

9a 对于*名称*，指定 extend.local.config.dir。

9b 对于*值*，指定安装时指定的安装文件夹 （目录）名称。

安装程序已将 sys-configuration-xmldata.xml 文件写入该文件夹。

9c 对于*说明*，指定属性的说明，例如 sys-configuration-xmldata.xml 的路径。

9d 单击*确定*以保存属性。

10 单击*新建*可添加其他新 JVM 系统属性。

10a 对于*名称*，指定 idmuserapp.logging.config.dir

10b 对于*值*，指定安装时指定的安装文件夹 （目录）名称。

10c 对于*说明*，指定属性的说明，例如 idmuserapp_logging.xml 的路径。

10d 单击*确定*以保存属性。

idmuserapp-logging.xml 文件仅在您通过 *User Application > 管理 > 应用程序配置 > 日志记录*沿用更改后才存在。

5.2.2 将 eDirectory 可信根导入 WebSphere 密钥储存区

1 将 eDirectory™ 可信根证书复制到托管 WebSphere 服务器的计算机上。

User Application 安装过程将这些证书导出到安装 User Application 的目录中。

2 将证书导入到 WebSphere 密钥储存区中。可以使用 WebSphere 管理员控制台 (通过 WebSphere 管理员控制台导入证书 （第 37 页）) 或通过命令行 (通过命令行导入证书 （第 37 页）) 执行此操作。

3 导入证书后，继续执行第 5.3 节 “ 部署 WAR 文件 ” （第 38 页）。

通过 WebSphere 管理员控制台导入证书

1 作为管理员用户登录到 WebSphere 管理控制台。

2 从左面板中，转到*安全性 > SSL 证书和密钥管理*。

3 在右侧的设置列表中，转到*其他属性*下的*密钥储存区和证书*。

4 选择 *节点默认信任储存区* （或正在使用的信任储存区）。

5 在右侧的*其他属性*下，选择*签名者证书*。

6 单击 “ 添加 ”。

7 键入证书文件的别名和完整路径。

8 在下拉列表中将数据类型更改为*二进制 DER 数据*。

9 单击 “ *确定* ”。现在，应该在签名者证书列表中看到证书。

通过命令行导入证书

在主管 WebSphere 服务器的计算机上，通过命令行运行密钥工具，将证书导入到 WebSphere 密钥储存区中。

注释：需要使用 WebSphere 密钥工具，否则此操作不起作用。此外，应确保储存区类型为 PKCS12。

WebSphere 密钥工具位于 /IBM/WebSphere/AppServer/java/bin。

以下是样本密钥工具命令：

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

如果系统中有多个 trust.p12 文件，则可能需要指定该文件的完整路径。

5.3 部署 WAR 文件

使用 WebSphere 部署工具部署 WAR 文件。

5.4 启动并访问 User Application

启动 User Application：

1. 作为管理员用户登录到 WebSphere 管理员控制台。
2. 从左侧导航面板转到*应用程序* > *企业应用程序*。
3. 选中要启动的应用程序旁的复选框，然后单击*启动*。

   启动后，*应用程序状态*列将显示一个绿色箭头。

访问 User Application

1. 使用在部署过程中指定的环境访问门户。

   在 WebSphere 上，万维网容器的默认端口是 9080，安全端口是 9443。URL 的格式为：http:// <*server*>:9080/IDMProv

通过 GUI 安装程序在 WebLogic Application Server 上进行安装

6

WebLogic 将基于您的输入配置 User Application WAR 文件。本节提供下列细节：

- 第 6.1 节 “WebLogic 安装核对清单 ”（第 39 页）
- 第 6.2 节 “ 安装和配置 User Application WAR”（第 39 页）
- 第 6.3 节 “ 准备 WebLogic 环境 ”（第 43 页）
- 第 6.4 节 “ 部署 User Application WAR”（第 45 页）
- 第 6.5 节 “ 访问 User Application”（第 45 页）

要了解使用非图形用户界面进行安装的信息，请参阅第 7 章 “ 从控制台或使用单条命令进行安装 ”（第 47 页）。

以非根用户身份运行安装程序。

6.1 WebLogic 安装核对清单

- ❑ 创建支持 WebLogic 的 WAR。

  使用 Identity Manager User Application 安装程序执行此任务。请参阅第 6.2 节 “ 安装和配置 User Application WAR”（第 39 页）。
- ❑ 通过将配置文件复制到相应的 WebLogic 位置，准备 WebLogic 环境以进行 WAR 部署。

  请参阅第 6.3 节 “ 准备 WebLogic 环境 ”（第 43 页）。
- ❑ 部署 WAR。

  请参阅第 6.4 节 “ 部署 User Application WAR”（第 45 页）。

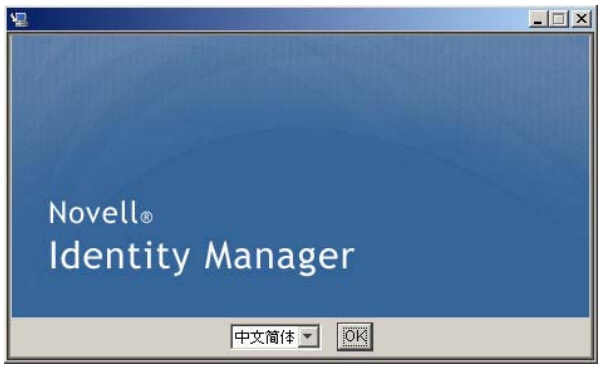
6.2 安装和配置 User Application WAR

注释 : 安装程序至少需要 Java 2 开发平台标准版开发工具包版本 1.5。如果使用更早的版本，安装过程将不会成功配置 User Application WAR 文件。安装看似成功，但尝试启动 User Application 时遇到错误。

1. 浏览找到包含安装文件的目录。
2. 从命令行起动针对您的平台的安装程序：

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

   当安装程序起动时，系统将提示您选择语言。



3 使用以下每个安装面板上的指导随附的信息完成安装：

安装屏幕	说明
Novell Identity Manager	选择安装程序的语言。默认为英语。
许可协议	阅读许可协议，然后选择*我接受本许可协议的条款*。
应用程序服务器平台	选择 *WebLogic* 用作应用程序服务器。
标准或供应	*标准*：如果安装 User Application 标准版，请选择此选项。 *基于角色的供应*：如果安装基于角色的供应模块，请选择此选项。
数据迁移	接受默认值 （校验未选择*是*）。 **警告：**不能选择*是*，如果选择 “ 是 ”，您将在启动 User Application 时遇到问题。 有关迁移的信息，请参阅 《*User Application：迁移指南* (http://www.novell.com/documentation/idmrbpm361/index.html)》。
WAR 在哪里？	如果 Identity Manager User Application WAR 文件所在的目录不同于安装程序，安装程序将提示提供 WAR 的路径。
选择安装文件夹	指定安装程序放置这些文件的位置。
数据库平台	选择数据库平台。必须已安装数据库和 JDBC 驱动程序。选项包括： ◆ Oracle （系统提示您提供版本） ◆ MS SQL Server
Java 安装	指定 Java 安装根文件夹。
IDM 配置	指定应用程序环境。从浏览器启动 User Application 时，这将是 URL 的一部分。
Audit 日志记录	要启用日志记录，请单击*是*。下一面板将提示您指定日志记录的类型。从以下选项中选择： ◆ *Novell Audit*：对 User Application 启用 Novell Audit 日志记录。 ◆ *OpenXDAS*：事件将记录到 OpenXDAS 日志记录服务器中。 有关设置 Novell Audit 或 OpenXDAS 日志记录的更多信息，请参阅《*User Application：管理指南*》。
Novell Audit	*服务器*：如果启用了 Novell Audit 日志记录，请指定 Novell Audit 服务器的主机名或 IP 地址。如果禁用日志记录，将忽略此值。 *日志超速缓存文件夹*：指定日志记录超速缓存的目录。

安装屏幕	说明
安全 — 主密钥	*是*：允许您导入现有的主密钥。如果选择导入现有经加密的主密钥，请将密钥剪切并粘贴到安装过程窗口。 *否*：创建新的主密钥。完成安装后，必须手动记录主密钥，如第 8.1 节“记录主密钥”（第 55 页）中所述。 安装过程中会将经加密的主密钥写到安装目录中的 master-key.txt 文件中。 导入现有主密钥的原因包括： ◆ 将安装从分级系统移到生产系统，并想保留访问过去分级系统中使用的数据库。 ◆ 已将 User Application 安装在 JBoss 群集中的第一个成员上，现在在群集中的后续成员上执行安装。 ◆ 由于磁盘故障，需要恢复 User Application。必须重新安装 User Application，并指定以前安装过程中所使用的同一个经过加密的主密钥。这样可以获得以前储存的加密数据的访问权。

4 系统会提示您提供安装程序用于配置 User Application WAR 文件的信息。（如果未提示您提供此信息，则您可能未完成第 2.5 节“安装 Java 开发工具包”（第 20 页）中所述的步骤。

安装屏幕	说明
User Application 配置	在 User Application 安装过程中，可以设置 User Application 配置参数。其中大部分参数都还可以于安装在 configupdate.sh 或 configupdate.bat 中进行配置，有关例外的项，参阅参数说明中的注释。 有关详细信息，请参阅附录 A“IDM User Application 配置参照 ”（第 61 页）
安装前摘要	阅读 “ 安装前摘要 ” 页面，校验所选的安装参数。 如有必要，使用*上一步*返回到前面的安装页，对安装参数作出更改。 User Application 配置页的值没有保存下来，因此，在重新指定安装中的以前页面之后，必须重新输入 User Application 配置值。当安装和配置参数令人满意之后，返回 “ 安装前摘要 ” 页，然后单击*安装*。
安装完成	指示安装已完成。

6.2.1 查看安装和日志文件

如果安装成功完成，没有错误，请继续准备 WebLogic 环境。如果安装提示出现错误或警告，请检查日志文件以确定问题：

- Identity_Manager_User_Application_Installlog.log 保存基本安装任务的结果。
- Novell-Custom-Install.log 记录了有关安装过程中所执行的 User Application 配置。

6.3 准备 WebLogic 环境

- 第 6.3.1 节 “ 配置连接池 ”（第 43 页）
- 第 6.3.2 节 “ 指定 User Application 配置文件的位置 ”（第 43 页）
- 第 6.3.3 节 “ 工作流程插件和 WebLogic 安装 ”（第 45 页）

6.3.1 配置连接池

- ❑ 将数据库驱动程序 JAR 文件复制到将用于部署 User Application 的域。
- ❑ 创建数据源

  遵循 WebLogic 文档中创建数据源的指导。

  数据源的 JNDI 名称必须与创建 User Application WAR 时指定的数据库名称相同，例如 jdbc/IDMUADataSource。
- ❑ 将 antlr-2.7.6.jar 从 User Application 安装目录复制到域 lib 文件夹。

6.3.2 指定 User Application 配置文件的位置

WebLogic 用户应用程序需要知道如何查找 sys-configuration-xmldata.xml 文件和 idmuserapp_logging.xml 文件。您可以通过将这些文件的位置添加到 setDomainEnv.cmd 文件来执行此操作。

要使其对应用程序服务器可用，请在 setDomainEnv.cmd 或 setDomainEnv.sh 文件中指定它的位置：

1. 打开 setDomainEnv.cmd 或 setDomainEnv.sh 文件。
2. 查找如下的行：

```
set JAVA_PROPERTIES

export JAVA_PROPERTIES
```

3. 在 JAVA_PROPERTIES 项下，添加以下项：
   - -Dextend.local.config.dir：指定包含 sys-configuration.xml 文件的文件夹 （而不是该文件本身）。
   - -Didmuserapp.logging.config.dir：指定包含 idmuserapp_logging.xml 文件的文件夹（而不是该文件本身）。

   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. 将环境变量 EXT_PRE_CLASSPATH 设置为指向 antlr.jar。

   4a 查找此行：

```
ADD EXTENSIONS TO CLASSPATH
```

   4b 在下面添加 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. 保存并退出该文件。

configupdate 实用程序同时使用 XML 文件，因此，您需要编辑 configupdate.bat 或 configupdate.sh 文件，如下所示：

1. 打开 configupdate.bat 或 configupdate.sh。
2. 查找以下行：

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

3. 在下面添加以下项：

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

4. 保存并关闭文件。
5. 运行 configupdate 实用程序以将证书安装到 BEA_HOME 下 JDK 的密钥储存区。

   当运行 configupdate 时，系统将提示您在正在使用的 JDK 下查找 cacerts 文件。如果您未在使用安装过程中指定的同一 JDK，则必须运行 WAR 上的 configupdate。请注意指定的 JDK，因为此项必须指向 WebLogic 所使用的 JDK。完成此操作以将连接的证书文件导入身份库。此操作的目的是将连接的证书导入 eDirectory。

6.3.3 工作流程插件和 WebLogic 安装

如果 enforce-valid-basic-auth-credentials 标志设置为 true， iManager 的工作流程管理插件将无法连接到 WebLogic 上运行的 User Application 驱动程序。要使该连接成功，必须禁用该标志。

要禁用 enforce-valid-basic-auth-credentials 标志，请按以下指示操作：

1. 打开 <*WLHome*>/user_projects/domains/base_domain/config/ 文件夹中的 Config.xml 文件。
2. 在 <security-configuration> 部分添加以下行：

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

3. 保存该文件并重启动服务器。

完成此更改后，应能登录到工作流程管理插件。

6.4 部署 User Application WAR

- 将 jsf-ri-1.1.1.war 作为库进行部署。
- 将更新的 User Application WAR 文件从安装目录 （通常为 Novell\IDM）复制到应用程序域。例如：

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

- 使用标准 WebLogic 部署过程部署 User Application WAR。

6.5 访问 User Application

- 导航至 User Application URL：

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

  例如：

  ```
  http://localhost:8080/IDMProv
  ```

从控制台或使用单条命令进行安装 7

本部分说明了可用来代替第 4 章 “ 使用 GUI 安装程序在 JBoss 上进行安装 ”（第 27 页）中描述的使用图形用户界面进行安装的方法。包括以下主题：

- 第 7.1 节 “ 从控制台安装 User Application”（第 47 页）
- 第 7.2 节 “ 使用单个命令安装 User Application”（第 47 页）

7.1 从控制台安装 User Application

本过程说明如何通过使用安装程序的控制台 （命令行）版本来安装 Identity Manager User Application。

注释 : 安装程序至少需要 Java 2 开发平台标准版开发工具包版本 1.5。如果使用更早的版本，安装过程将不会成功配置 User Application WAR 文件。安装看似成功，但尝试启动 User Application 时遇到错误。

---

1. 获得表 2-2 在第 16 页中所述的恰当的安装文件后，登录并打开终端会话。
2. 按如下所述，为使用 Java 的平台起动安装程序：

   java -jar IdmUserApp.jar -i console
3. 在导入步骤或创建主密钥步骤中，按照第 4 章 “ 使用 GUI 安装程序在 JBoss 上进行安装 ”（第 27 页）中针对图形用户界面说明的相同步骤，阅读命令行上的提示符并在命令行上输入相应的回复。
4. 要设置 User Application 配置参数，请手动起动 configupdate 实用程序。在命令行上，输入 Configupdate.sh（Linux 或 solaris）或 Configupdate.bat (windows)，然后输入如第 A.1 节 “User Application 配置：基本参数 ”（第 61 页）中所述的值。
5. 如果使用的是外部口令管理 WAR，请手动将其复制到安装目录和运行外部口令 WAR 功能的远程 JBoss 服务器部署目录。
6. 继续第 8 章 “ 安装后任务 ”（第 55 页）。

7.2 使用单个命令安装 User Application

本过程说明如何执行静默安装。对于静默安装，在安装过程中无需交互操作，从而可以节省您的时间，尤其在多个系统上执行安装时。 Linux 和 Solaris 上的程序安装支持静默方式。

1. 获取表 2-2 在第 16 页中列出的相应安装文件。
2. 登录并打开终端会话。
3. 找到安装文件中附带的 Identity Manager 属性文件 silent.properties。如果使用 CD，请将此文件复制到本地。
4. 编辑 silent.properties 以提供安装参数和 User Application 配置参数。

   有关每个安装参数的示例，请参阅 silent.properties 文件。安装参数与在 GUI 或控制台安装过程中设置的安装参数对应。

有关每个 User Application 配置参数的说明，请参阅表 7-1。User Application 配置参数和在 GUI 或控制台安装步骤或使用 configupdate 实用程序所设置的参数一致。

5 使用以下命令起动静默安装：

java -jar IdmUserApp.jar -i silent -f / *您的目录路径* /silent.properties

如果文件所在目录不同于安装程序底稿中的目录，请键入 silent.properties 的完整路径。此底稿将必要文件释放到临时目录并启动静默安装。

表 7-1 *静默安装的 User Application 配置参数*

silent.properties 中的 User Application 参数名称	User Application 配置参数文件中的等价参数名
NOVL_CONFIG_LDAPHOST=	eDirectory™ 连接设置：LDAP 主机。 为 LDAP 服务器指定主机名或 IP 地址。
NOVL_CONFIG_LDAPADMIN=	eDirectory 连接设置：LDAP 管理员。 指定 LDAP 管理员的身份凭证。该用户必须已经存在。User Application 使用此帐户来建立与身份库的管理连接。此值已使用主密钥进行过加密。
NOVL_CONFIG_LDAPADMINPASS=	eDirectory 连接设置：LDAP 管理员口令。 指定 LDAP 管理员口令。此口令已使用主密钥进行过加密。
NOVL_CONFIG_ROOTCONTAINERNAME=	eDirectory DN：根容器 DN。 指定根容器的 LDAP 判别名。如果没有在目录抽象层中指定搜索根，则将该判别名用作默认的实体定义搜索根。
NOVL_CONFIG_PROVISIONROOT=	eDirectory DN：供应驱动程序 DN。 指定以前在第 3.1 节 “ 在 iManager 中创建 User Application 驱动程序 ”（第 23 页）中创建的 User Application 驱动程序的判别名。例如，如果驱动程序为 UserApplicationDriver，驱动程序集称为 myDriverSet，并且驱动程序集位于环境 o=myCompany 中，则可以输入以下值： `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`

silent.properties 中的 User Application 参数名称	User Application 配置参数文件中的等价参数名
NOVL_CONFIG_LOCKSMITH=	eDirectory DN：User Application Admin。 身份库中有权执行所指定 User Application 用户容器的管理任务的现有用户。该用户可以使用 User Application 的*管理*选项卡管理门户。 如果 User Application 管理员参与 iManager、Designer for Identity Manager 或 User Application（*请求和批准*选项卡）中显示的工作流程管理任务，则必须授予此管理员对 User Application 驱动程序中包含的对象实例的相应受托者权利。有关细节，请参考 《*User Application：管理指南*》。 要在部署 User Application 之后更改指派，必须使用 User Application 中的*管理* > *安全*页面。
NOVL_CONFIG_PROVLOCKSMITH=	eDirectory DN：供应应用程序 Admin。 Identity Manager 的供应版本中可以使用此角色。供应应用程序管理员使用*供应*选项卡 （*管理*选项卡下）来管理供应工作流程功能。用户可以通过 User Application 的*请求和批准*选项卡使用这些功能。在将用户指定为供应应用程序管理员之前，身份库中必须存在此用户。 要在部署 User Application 之后更改指派，必须使用 User Application 中的*管理* > *安全*页面。
NOVL_CONFIG_ROLECONTAINERDN=	此角色在 Novell Identity Manager 基于角色的供应模块中可用。此角色允许成员创建、去除或修改所有角色，授予或撤消指派给任何用户、组或容器的任何角色。它还允许其角色成员运行任何用户的任何报告。默认情况下，会对 User Application Admin 指派此角色。 要在部署 User Application 后更改此指派，请使用 User Application 中的*角色* > *角色指派*页面。
NOVL_CONFIG_COMPLIANCECONTAINERDN	合规性模块管理员是一个系统角色，它允许成员执行*合规性*选项卡上的所有功能。在将用户指定为合规性模块管理员之前，身份库中必须存在此用户。
NOVL_CONFIG_USERCONTAINERDN=	Meta-Directory 用户身份：用户容器 DN。 指定用户容器的 LDAP 判别名 (DN) 或完全限定的 LDAP 名称。这定义用户和组的搜索范围。允许该容器中 （及其下）的用户登录 User Application。 **重要：**如果要使该用户能够执行工作流程，请确保在 User Application 驱动程序设置过程中指定的 User Application 管理员在该容器中存在。
NOVL_CONFIG_GROUPCONTAINERDN=	Meta-Directory 用户组：组容器 DN。 指定组容器的 LDAP 判别名 (DN) 或完全限定的 LDAP 名称。由目录抽象层中的实体定义使用。

silent.properties 中的 User Application 参数名称	User Application 配置参数文件中的等价参数名
NOVL_CONFIG_KEYSTOREPATH=	eDirectory 证书：密钥储存区路径。必需。 指定应用程序服务器所使用的 JRE 的密钥储存区 (cacerts) 文件。User Application 安装过程中将修改密钥储存区文件。在 Linux 或 Solaris 上，用户必须具有写此文件的权限。
NOVL_CONFIG_KEYSTOREPASSWORD=	eDirectory 证书：密钥储存区口令。 指定 cacerts 口令。默认值为 changeit。
NOVL_CONFIG_SECUREADMINCONNECTION=	eDirectory 连接设置：安全 Admin 连接。 必需。通过指定为 *True*，可以要求所有使用 Admin 帐户的通讯都通过安全套接字进行 （此选项可能对性能不利）。此设置允许不需要 SSL 的其他操作在无 SSL 的情况下运行。 如果 Admin 帐户不使用安全套接字通讯，则指定为 *False*。
NOVL_CONFIG_SECUREUSERCONNECTION=	eDirectory 连接设置：安全用户连接。 必需。通过指定为 *True*，可以要求所有使用已登录用户帐户的通讯都通过安全套接字进行 （此选项可能对性能有严重不利影响）。此设置允许不需要 SSL 的其他操作在无 SSL 的情况下运行。 如果用户帐户不使用安全套接字通讯，则指定为 *False*。
NOVL_CONFIG_SESSIONTIMEOUT=	杂项：会话超时。 必需。指定应用程序会话超时时间间隔。
NOVL_CONFIG_LDAPPLAINPORT=	eDirectory 连接设置：LDAP 非安全端口。 必需。为 LDAP 服务器指定非安全端口，比如 389。
NOVL_CONFIG_LDAPSECUREPORT=	eDirectory 连接设置：LDAP 安全端口。 必需。为 LDAP 服务器指定安全端口，比如 636。
NOVL_CONFIG_ANONYMOUS=	eDirectory 连接设置：使用公开匿名帐户。 必需。指定为 *True* 可以允许未登录的用户访问 LDAP 公开匿名帐户。 指定为 *False* 则启用 NOVL_CONFIG_GUEST。
NOVL_CONFIG_GUEST=	eDirectory 连接设置：LDAP Guest。 允许没有登录的用户访问允许的门户小程序。同时必须取消选择 *使用公开匿名帐户*。身份库中必须已经存在 Guest 用户帐户。要禁用 Guest 用户，请选择 *使用公开匿名帐户*。
NOVL_CONFIG_GUESTPASS=	eDIRECTORY 连接设置：LDAP Guest 口令。

silent.properties 中的 User Application 参数名称	User Application 配置参数文件中的等价参数名
NOVL_CONFIG_EMAILNOTIFYHOST=	电子邮件：通知模板 HOST 令牌。 指定主管 Identity Manager User Application 的应用程序服务器。例如： `myapplication serverServer` 此值将替换电子邮件模板中的 $HOST$ 令牌。所建立的 URL 是指向供应请求任务和批准通知的链接。
NOVL_CONFIG_EMAILNOTIFYPORT=	电子邮件：通知模板 Port 令牌。 用于替换供应请求任务和批准通知所用的电子邮件模板中的 $PORT$ 令牌。
NOVL_CONFIG_EMAILNOTIFYSECUREPORT=	电子邮件：通知模板 Secure Port 令牌。 用于替换供应请求任务和批准通知所使用电子邮件模板中的 $SECURE_PORT$ 令牌。
NOVL_CONFIG_NOTFSMTPEMAILFROM=	电子邮件：通知 SMTP 电子邮件发件人。 必需。指定供应电子邮件中发送电子邮件的用户。
NOVL_CONFIG_NOTFSMTPEMAILHOST=	电子邮件：通知 SMTP 电子邮件主机。 必需。指定供应电子邮件所使用的 SMTP 电子邮件主机。这可以是 IP 地址或 DNS 名。
NOVL_CONFIG_USEEXTPWDWAR=	口令管理：使用外部口令 WAR。 如果使用外部口令管理 WAR，则指定为 *True*。如果指定为 *True*，则还必须提供 *NOVL_CONFIG_EXTPWDWARPTH* 和 *NOVL_CONFIG_EXTPWDWARRTNPATH* 的值。 指定为 *False* 可以使用默认的内部口令管理功能。 /jsps/pwdmgt/ForgotPassword.jsf （开头没有 http(s) 协议）。这将用户重定向到内置于 User Application 的 “ 忘记口令 ” 功能，而不是外部 WAR。
NOVL_CONFIG_EXTPWDWARPATH=	口令管理：忘记口令链接。 指定外部或内部口令管理 WAR 中的 “ 忘记口令 ” 功能页的 URL ForgotPassword.jsf。或者接受默认的内部口令管理 WAR。有关细节，请参阅配置外部口令管理 （第 57 页）。
NOVL_CONFIG_EXTPWDWARRTNPATH=	口令管理：忘记口令返回链接。 如果使用的是外部口令管理 WAR，需提供外部口令管理 WAR 用来通过万维网服务回调 User Application 的路径，例如 https:// *idmhost:sslport*/idm。
NOVL_CONFIG_USEROBJECTATTRIBUTE=	Meta-Directory 用户身份：用户对象类。 必需。 LDAP 用户对象类 （通常为 inetOrgPerson）。

silent.properties 中的 User Application 参数名称	User Application 配置参数文件中的等价参数名
NOVL_CONFIG_LOGINATTRIBUTE=	Meta-Directory 用户身份：登录属性。 必需。代表用户的登录名的 LDAP 属性 （比如 CN）。
NOVL_CONFIG_NAMINGATTRIBUTE=	Meta-Directory 用户身份：命名属性。 必需。用作查找用户或组时的标识符的 LDAP 属性。这不同于登录属性，登录属性仅在登录时使用，在用户 / 组搜索时不使用。
NOVL_CONFIG_USERMEMBERSHIPATTRIBUTE=	Metadirectory 用户身份：用户成员资格属性。可选。 必需。代表用户的组成员资格的 LDAP 属性。不要在该名称中使用空格。
NOVL_CONFIG_GROUPOBJECTATTRIBUTE=	Meta-Directory 用户组：组对象类。 必需。 LDAP 组对象类 （通常是 groupofNames）。
NOVL_CONFIG_GROUPMEMBERSHIPATTRIBUTE=	Meta-Directory 用户组：组成员资格属性。 必需。指定代表用户组成员资格的属性。不要在该名称中使用空格。
NOVL_CONFIG_USEDYNAMICGROUPS=	Meta-Directory 用户组：使用动态组。 必需。要使用动态组，请指定 *True*。否则，指定 *False*。
NOVL_CONFIG_DYNAMICGROUPOBJECTCLASS=	Meta-Directory 用户组：动态组对象类。 必需。指定 LDAP 动态组对象类 （一般为 dynamicGroup）。
NOVL_CONFIG_PRIVATESTOREPATH=	私用密钥储存区：私用密钥储存区路径。 指定包含 User Application 的私用密钥和证书的私用密钥储存区的路径。保留 . 如果保留为空的话，将采用默认路径 /jre/lib/security/cacerts。
NOVL_CONFIG_PRIVATESTOREPASSWORD=	私用密钥储存区：私用密钥储存区口令。
NOVL_CONFIG_PRIVATEKEYALIAS=	私用密钥储存区：私用密钥别名。 别名为 novellIDMUserApp，除非另行指定。
NOVL_CONFIG_PRIVATEKEYPASSWORD=	私用密钥储存区：私用密钥口令。
NOVL_CONFIG_TRUSTEDSTOREPATH=	可信密钥储存区：可信储存路径。 可信密钥储存区包含所有用于验证数字签名的可信签名者的证书。如果此路径为空的话， User Application 将从系统属性 javax.net.ssl.trustStore 中获取路径。如果那里没有路径，则假定为 jre/lib/security/cacerts。
NOVL_CONFIG_TRUSTEDSTOREPASSWORD=	可信密钥储存区：可信储存口令。
NOVL_CONFIG_AUDITCERT=	Novell Audit 数字签名证书

silent.properties 中的 User Application 参数名称	User Application 配置参数文件中的等价参数名
NOVL_CONFIG_AUDITKEYFILEPATH=	Novell Audit 数字签名私用密钥文件路径。
NOVL_CONFIG_ICSLOGOUTENABLED=	Access Manager 和 iChain 设置：已启用同时注销。 通过指定为 *True*，可以启用同时注销 User Application 和 Novell Access Manager 或 iChain®。注销时， User Application 检查是否存在 Novell Access Manager 或 iChain cookie，如果存在 cookie，则将用户重路由到 ICS 注销页。 要禁用同时注销，请指定为 *False*。
NOVL_CONFIG_ICSLOGOUTPAGE=	Access Manager 和 iChain 设置：同时注销页面。 指定 Novell Access Manager 或 iChain 注销页面的 URL，此 URL 是 Novell Access Manager 或 iChain 期望的主机名。如果启用了 ICS 日志记录并且用户要注销 User Application，则将用户重路由到此页面。
NOVL_CONFIG_EMAILNOTIFYPROTOCOL=	电子邮件：通知模板 PROTOCOL 令牌。 指非安全协议 HTTP。用于替换供应请求任务和批准通知所用的电子邮件模板中的 $PROTOCOL$ 令牌。
NOVL_CONFIG_EMAILNOTIFYSECUREPROTOCOL=	电子邮件：通知模板 Secure Port 令牌。
NOVL_CONFIG_OCSPURI=	杂项：OCSP URI。 如果客户安装使用在线证书状态协议 (OCSP)，请提供统一资源标识符 (URI)。比如，格式为 http://host:port/ocsplocal。OCSP URI 在线更新可信证书的状态。
NOVL_CONFIG_AUTHCONFIGPATH=	杂项：授权配置路径。 授权配置文件的完全限定名。
NOVL_CONFIG_CREATEDIRECTORYINDEX	杂项：创建 eDirectory 索引 如果希望静默安装程序在 NOVL_CONFIG_SERVERDN 中指定的 eDirectory 服务器上创建 manager、ismanager 和 srvprvUUID 属性的索引，请指定 True。如果此参数设置为 True，则不能将 NOVL_CONFIG_REMOVEEDIRECTORYINDEX 设置为 True。 为达到最佳性能，应完成索引的创建。索引应处于联机方式，才可使用 User Application。

silent.properties 中的 User Application 参数名称	User Application 配置参数文件中的等价参数名
NOVL_CONFIG_REMOVEDIRECTORYINDEX	杂项：去除 eDirectory 索引 如果希望静默安装程序去除 NOVL_CONFIG_SERVERDN 中指定的服务器上的索引，请指定 True。如果此参数设置为 True，则 NOVL_CONFIG_CREATEEDIRECTORYINDEX 不能为 True。
NOVL_CONFIG_SERVERDN	杂项：服务器 DN 指定应创建或去除索引的 eDirectory 服务器。

安装后任务

8

本部分说明安装后任务。包括以下主题：

8.1 记录主密钥

在安装后，立即复制加密的主密钥并将其记录在一个安全的位置。

1. 打开安装目录中的 master-key.txt 文件。
2. 将经过加密的主密钥复制到一个安全位置，保证系统故障时也能访问。

警告：要始终保留加密主密钥的复本。如果丢失了主密钥，比如由于设备发生故障，则需要使用经过加密的主密钥重获加密数据的访问权。

如果此安装位于群集的第一个成员上，当在群集中其他成员上安装 User Application 驱动时，需使用此经加密的主密钥。

8.2 配置 User Application

有关配置 Identity Manager User Application 和角色子系统的安装后指导，请参考以下内容：

- 在 《*Novell IDM 基于角色的供应模块 3.6.1 管理指南*》中，该部分的标题为 “ 配置 User Application 环境 ”。
- 《*Novell IDM 基于角色的供应模块 3.6.1 设计指南*》

8.2.1 设置 Novell Audit

根据 《User Application：管理指南 (http://www.novell.com/documentation/idmrbpm361/index.html)》中 “ 设置日志记录 ” 一节中的指示，将 dirxml.lsc 文件 （位于 prerequisites.zip 文件中）复制到审计服务器。

8.3 配置 eDirectory

8.3.1 在 eDirectory 中创建索引

要改进 User Application 的性能，eDirectory™ 管理员应为 manager、ismanager 和 srvprvUUID 属性创建索引。如果这些属性没有索引， User Application 用户可能会遇到不良性能，尤其在群集环境中。

如果选择 User Application 配置面板的*高级*选项卡上的*创建 eDirectory 索引*，这些索引可在安装过程中自动创建 （表 A-2 在第 66 页中所述），或者参考 《*Novell eDirectory 管理指南* (http://www.novell.com/documentation)》获取使用索引管理器创建索引的指导。

8.3.2 安装和配置 SAML 鉴定方法

仅在希望使用 SAML 鉴定方法且不同时使用访问管理器时，才需要此配置。如果使用访问管理器， eDirectory 树中将已包含此方法。此过程包括：

- ❑ 在 eDirectory 树中安装 SAML 方法。
- ❑ 使用 iManager 编辑 eDirectory 属性

在 eDirectory 树中安装 SAML 方法

1. 在 .iso 中找到并解压缩 nmassaml.zip 文件。
2. 将 SAML 方法安装到 eDirectory 树中。
   - **2a** 扩展在 authsaml.sch 中储存的纲要

     以下示例显示了在 Linux 上执行此操作的方式：

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

     以下示例显示了在 Linux 上执行此操作的方式：

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

编辑 eDirectory 属性

1. 打开 iManager，然后转至*角色和任务* > *目录管理* > *创建对象*。
2. 选择*显示所有对象类*。
3. 创建类 authsamlAffiliate 的一个新对象。
4. 选择 authsamlAffiliate，然后单击*确定*。（您可以为此对象指定任意有效的名称。）
5. 要指定环境，选择树中的 *SAML Assertion.Authorized Login Methods.Security* 容器对象，然后单击*确定*。
6. 必须将属性添加到类对象 authsamlAffiliate 中。
   - **6a** 转至 iManager *查看对象* > *浏览*选项卡，然后在 SAML Assertion.Authorized Login Methods.Security 容器中查找新的附属对象。
   - **6b** 选择新的附属对象，然后选择*修改对象*。
   - **6c** 将 *authsamlProviderID* 属性添加到新的附属对象。此属性用于与其附属匹配声明。此属性的内容必须与 SAML 声明发送的 Issuer 属性完全匹配。
   - **6d** 单击*确定*。

6e 将 *authsamlValidBefore* 和 *authsamlValidAfter* 属性添加到附属对象。当认为某声明有效时，这些属性围绕该声明中的 *IssueInstant* 定义以秒为单位的时间段。通常默认值为 180 秒。

6f 单击 “*确定*”。

7 选择安全性容器，然后选择*创建对象*，以在安全性容器中创建*可信根容器*。

8 在可信根容器中创建*可信根*对象。

8a 返回到*角色和任务* > *目录管理*，然后选择*创建对象*。

8b 再次选择*显示所有对象类*。

8c 为附属将用于对声明签名的证书创建*可信根*对象。必须具有证书的 DER 编码的副本才能执行此操作。

8d 在到根 CA 证书的签名证书链中为每个证书创建新的可信根对象。

8e 将 “ 环境 ” 设置为先前创建的 “ 可信根容器 ”，然后单击*确定*。

9 返回到对象查看器。

10 向您所属对象添加 *authsamlTrustedCertDN* 属性，然后单击*确定*。

此属性应指向先前步骤中所创建签名证书的 “ 可信根对象 ”。（该附属的所有声明必须通过此属性指向的证书进行签名，否则它们将被拒绝。）

11 向您所属对象添加 *authsamlCertContainerDN* 属性，然后单击*确定*。

此属性应指向您之前创建的 “ 可信根容器 ”。（此属性用于校验签名证书的证书链。）

8.4 安装后重配置 User Application WAR 文件

要更新 WAR 文件，可以运行 configupdate 实用程序，如下所示：

1 通过执行 configupdate.sh 或 configupdate.bat，运行 User Application 安装目录中的 ConfigUpdate 实用程序。这使您能够更新安装目录中的 WAR 文件。

有关 ConfigUpdate 实用程序参数的信息，请参阅第 A.1 节 “User Application 配置：基本参数 ”（第 61 页）和表 7-1 在第 48 页。

2 将新的 WAR 文件部署到应用程序服务器。

对于 WebLogic 和 WebSphere，重新将 WAR 文件部署到应用程序服务器。对于 JBoss 单服务器，这些更改将应用于所部署的 WAR。如果正在 JBoss 群集中运行，则群集中的每个 JBoss 服务器都需要更新 WAR 文件。

8.5 配置外部口令管理

通过*忘记口令链接*配置参数，可以指定包含 “ 忘记口令 ” 功能的 WAR 的位置。可以对 User Application 指定外部或内部 WAR。

- 第 8.5.1 节 “ 指定外部口令管理 WAR”（第 58 页）
- 第 8.5.2 节 “ 指定内部口令 WAR”（第 58 页）
- 第 8.5.3 节 “ 测试外部口令 WAR 配置 ”（第 58 页）
- 第 8.5.4 节 “ 在 JBoss 服务器间配置 SSL 通讯 ”（第 58 页）

8.5.1 指定外部口令管理 WAR

1 使用安装过程或 configupdate 实用程序。

2 在 User Application 配置参数中，选中*使用外部口令 WAR* 配置参数复选框。

3 对于*忘记口令链接*配置参数，指定外部口令 WAR 的位置。

包括主机和端口，比如 http://localhost:8080/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsf。外部口令 WAR 可以位于保护 User Application 的防火墙之外。

4 对于*忘记口令返回链接*，需提供外部口令管理 WAR 用于通过万维网服务回调 User Application 的路径，比如 https:// *idmhost:sslport*/idm。

返回链接必须使用 SSL，以确保与 User Application 进行安全万维网服务通讯。另请参阅第 8.5.4 节 “ 在 JBoss 服务器间配置 SSL 通讯 ”（第 58 页）。

5 执行以下操作之一：

- 如果使用了安装程序，请阅读此步骤中的信息，然后继续步骤 6。
- 如果使用 configupdate 实用程序更新安装根目录中的外部口令 WAR，请阅读此步骤并手动将 WAR 重命名为在*忘记口令链接*中指定的第一个目录。然后，继续步骤 6。

在安装结束之前，安装程序将 IDMPwdMgt.war （安装程序中附带）重命名为指定的第一个目录。经过重命名的 IDMPwdMgt.war 称为外部口令 WAR。例如，如果指定的是 http://www.idmpwdmgthost.com/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsf，安装程序会将 IDMPwdMgt.war 重命名为 ExternalPwd.war。安装程序将重命名过的 WAR 移至安装根目录。

6 手动将 ExternalPwd.war 复制到运行外部口令 WAR 功能的远程 JBoss 服务器部署目录。

8.5.2 指定内部口令 WAR

1 在 User Application 配置参数中，不选择*使用外部口令 WAR*。

2 接受*忘记口令链接*的默认位置，或者提供另一个口令 WAR 的 URL。

3 接受*忘记口令返回链接*的默认值。

8.5.3 测试外部口令 WAR 配置

如果使用的是外部口令 WAR 并且想通过访问测试 “ 忘记口令 ” 功能，则可以在以下位置访问它：

- 直接在浏览器中访问。转至外部口令 WAR 中的 “ 忘记口令 ” 页，比如 http://localhost:8080/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsf。
- 在 “User Application 登录 ” 页上，单击*忘记口令*链接。

8.5.4 在 JBoss 服务器间配置 SSL 通讯

如果安装过程中在 User Application 配置文件中选择了*使用外部口令 WAR*，则必须配置部署 User Application WAR 和 IDMPwdMgt.war 文件的 JBoss 服务器之间的 SSL 通讯。有关指导，请参阅 JBoss 文档。

8.6 升级忘记口令设置

可以在安装后更改*忘记口令链接*和*忘记口令返回链接*的值。或者使用 configupdate 实用程序，或者使用 User Application。

使用 configupdate 实用程序。在命令行上，将目录更改为安装目录，然后输入 configupdate.sh （linux 或 Solaris）或 configupdate.bat (Windows)。如果要创建或编辑外部口令管理 WAR，那么，在将 WAR 复制到远程 JBoss 服务器之前，必须手动重命名 WAR。

使用 User Application。以 User Application 管理员身份登录，然后转至*管理 > 应用程序配置 > 口令和模块设置 > 登录*。修改以下字段：

- *忘记口令链接*（例如：http://localhost:8080/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsf）
- *忘记口令返回链接*（例如：https://idmhost:sslport/idm）

8.7 查错

Novell® 代表将会帮您解决遇到的任何设置和配置问题。同时，这里提供了一些在您遇到某些问题时可以尝试的操作。

问题	建议的操作

想要修改在安装过程中设置的 User Application 配置。这包括类似于下列项目的配置：
• 身份库连接和证书
• 电子邮件设置
• Metadirectory 用户身份、用户组
• Access Manager 或 iChain® 设置
	在独立于安装程序的情况下运行配置实用程序。
	在 Linux 和 Solaris 上，从安装目录 （默认为 /opt/novell/idm）运行以下命令：
	`configupdate.sh`
	在 Windows 上，从安装目录 （默认为 c:\opt\novell\idm）运行以下命令：
	`configupdate.bat`

应用程序服务器启动时出现异常，显示日志讯息端口 8080 已被使用。	关闭 Tomcat （或其他服务器软件）的可能已在运行的任何实例。如果决定将应用程序服务器重新配置为使用 8080 以外的其他端口，请记住在 iManager 中编辑 User Application 驱动程序的配置设置。
当应用程序服务器启动时，显示讯息称找不到任何可信证书。	确保使用在 User Application 安装中指定的 JDK 启动应用程序服务器。
无法登录门户 Admin 页。	确保存在 User Application 管理员帐户。不要将此帐户与 iManager Admin 帐户相混淆。存在着 （或应该有）两个不同的 Admin 对象。
可以以 Admin 身份登录，但不能创建新用户。	User Application 管理员必须是顶层容器的受托者，并且需要有主管权限。作为权宜之计，可以尝试将 User Application 管理员的权限设置为等效于 LDAP 管理员的权限 （使用 iManager）。

问题	建议的操作
当启动应用程序服务器时，出现 MySQL 连接错误。	请不要以根用户身份运行。（如果您运行随 Identity Manager 提供的 MySQL 版本，几乎不会出现此问题。） 确保 MySQL 正在运行 （并且适当的拷贝正在运行）。停止 MySQL 的其他任何实例。运行 /idm/mysql/start-mysql.sh，然后运行 /idm/start-jboss.sh。 在文本编辑器中检查 /idm/mysql/setup-mysql.sh，并纠正任何可疑的值。然后运行底稿，再运行 /idm/start-jboss.sh。
启动 应用程序服务器时遇到密钥储存区错误 .	应用程序服务器没有运行在安装 User Application 时所指定的 JDK。 使用 keytool 命令导入证书文件： `keytool -import -trustcacerts -alias aliasName -file certFile -keystore ..\lib\security\cacerts -storepass changeit` ◆ 使用为该证书选择的唯一名称替换 *aliasName*。 ◆ 使用证书文件的完整路径和名称替换 *certFile*。 ◆ 默认的密钥储存区口令为 changeit （如果有其他口令，请指定）。

没有发送电子邮件通知。	通过运行 configupdate 实用程序检查是否指定了以下 User Application 配置参数的值：“ 电子邮件收件人 ”和“ 电子邮件主机 ”。
	
	在 Linux 或 Solaris 上，从安装目录 （默认为 /opt/novell/idm）运行以下命令：
	
	`configupdate.sh`
	
	在 Windows 上，从安装目录 （默认为 c:\opt\novell\idm）运行以下命令：
	
	`configupdate.bat`

IDM User Application 配置参照

A

本节说明 User Application 安装或配置更新过程中对其提供值的选项。

A.1 User Application 配置：基本参数

图 A-1 *User Application 配置基本选项*

表 A-1 User Application 配置：基本选项

设置类型	选项	说明
eDirectory® 连接设置	*LDAP 主机*	必需。指定 LDAP 服务器的主机名或 IP 地址，及其安全端口。例如： `myLDAPhost`
	LDAP 非安全端口	为 LDAP 服务器指定非安全端口。例如：389。
	LDAP 安全端口	为 LDAP 服务器指定安全端口。例如：636。
	LDAP 管理员	必需。指定 LDAP 管理员的身份凭证。该用户必须已经存在。User Application 使用此帐户来建立与身份库的管理连接。此值已使用主密钥进行过加密。 只要未使用 User Application 的 “ 管理 ” 选项卡修改此设置，就可使用 configupdate 实用程序进行修改。
	LDAP 管理员口令	必需。指定 LDAP 管理员口令。此口令已使用主密钥进行过加密。 只要未使用 User Application 的 “ 管理 ” 选项卡修改此设置，就可使用 configupdate 实用程序进行修改。
	使用公开匿名帐户	允许没有登录的用户访问 LDAP 公开匿名帐户。
	LDAP Guest	允许没有登录的用户访问允许的门户小程序。身份库中必须已经存在此用户帐户。要启用 LDAP Guest，必须取消选择*使用公开匿名帐户*。要禁用 Guest 用户，请选择*使用公开匿名帐户*。
	LDAP Guest 口令	指定 LDAP Guest 口令。
	安全 Admin 连接	通过选中此选项，可以要求所有使用 Admin 帐户的通讯都通过安全套接字进行。（此选项可能对性能不利）。此设置允许不需要 SSL 的其他操作在无 SSL 的情况下运行。
	安全用户连接	通过选中此选项，可以要求所有使用已登录用户帐户的通讯都通过安全套接字进行。（此选项可能对性能不利）。此设置允许不需要 SSL 的其他操作在无 SSL 的情况下运行。

设置类型	选项	说明
eDirectory DN	*根容器 DN*	必需。指定根容器的 LDAP 判别名。如果没有在目录抽象层中指定搜索根，则将该判别名用作默认的实体定义搜索根。
	供应驱动程序 DN	必需。指定 User Application 驱动程序的判别名（如第 3.1 节“在 iManager 中创建 User Application 驱动程序”（第 23 页）中所述）。例如，如果驱动程序为 UserApplicationDriver，驱动程序集称为 MyDriverSet，并且驱动程序集位于环境 o=myCompany 中，则可以输入以下值： `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`
	User Application Admin	必需。身份库中有权执行所指定 User Application 用户容器的管理任务的现有用户。该用户可以使用 User Application 的*管理*选项卡管理门户。 如果 User Application 管理员参与 iManager、 Designer for Identity Manager 或 User Application （*请求和批准*选项卡）中显示的工作流程管理任务，则必须授予此管理员对 User Application 驱动程序中包含的对象实例的相应受托者权利。有关细节，请参考 《*User Application：管理指南*》。 要在部署 User Application 之后更改指派，必须使用 User Application 中的*管理* > *安全*页面。 如果已启动托管 User Application 的应用程序服务器，则无法通过 configupdate 更改此设置。
	供应应用程序管理员	供应应用程序管理员使用*供应*选项卡 （*管理*选项卡下）管理供应工作流程功能。用户可以通过 User Application 的*请求和批准*选项卡使用这些功能。在将用户指定为供应应用程序管理员之前，身份库中必须存在此用户。 要在部署 User Application 之后更改指派，必须使用 User Application 中的*管理* > *安全*页面。
	合规性管理员	合规性模块管理员是一个系统角色，它允许成员执行*合规性*选项卡上的所有功能。在将用户指定为合规性模块管理员之前，身份库中必须存在此用户。 configupdate 执行过程中，仅在未指派有效的合规性模块管理员时，对此值的更改才会生效。如果存在有效的合规性模块管理员，则将不保存更改。 要在部署 User Application 后更改此指派，请使用 User Application 中的*角色* > *角色指派*页面。

设置类型	选项	说明
eDirectory DN（续）	*角色管理员*	此角色在 Novell Identity Manager 基于角色的供应模块中可用。此角色允许成员创建、去除或修改所有角色，授予或撤消指派给任何用户、组或容器的任何角色。它还允许其角色成员运行任何用户的任何报告。默认情况下，会对 User Application Admin 指派此角色。 要在部署 User Application 后更改此指派，请使用 User Application 中的*角色* > *角色指派*页面。 configupdate 执行过程中，仅在未指派有效的角色管理员时，对此值的更改才会生效。如果存在有效的角色管理员，则将不保存更改。
	用户容器 DN	必需。指定用户容器的 LDAP 判别名 (DN) 或完全限定的 LDAP 名称。这定义用户和组的搜索范围。允许该容器中（及其下）的用户登录 User Application。 **重要：**如果要使该用户能够执行工作流程，请确保在 User Application 驱动程序设置过程中指定的 User Application 管理员在该容器中存在。 如果已启动托管 User Application 的应用程序服务器，则无法通过 configupdate 更改此设置。
	组容器 DN	必需。指定组容器的 LDAP 判别名 (DN) 或完全限定的 LDAP 名称。 由目录抽象层中的实体定义使用。 如果已启动托管 User Application 的应用程序服务器，则无法通过 configupdate 更改此设置。
eDirectory 证书	*密钥储存区路径*	必需。指定应用程序服务器用于运行的、 JDK 密钥储存区 (cacerts) 文件的完整路径，或单击小浏览器按钮，然后浏览找到 cacerts 文件。 在 Linux 或 Solaris 上，用户必须具有写此文件的权限。
	密钥储存区口令 / 确认密钥储存区口令	必需。指定 cacerts 口令。默认值为 changeit。

设置类型	选项	说明
电子邮件	*通知模板 Host 令牌*	指定主管 Identity Manager User Application 的应用程序服务器。例如： `myapplication serverServer` 此值将替换电子邮件模板中的 $HOST$ 令牌。所建立的 URL 是指向供应请求任务和批准通知的链接。
	通知模板 Port 令牌	用于替换供应请求任务和批准通知所用的电子邮件模板中的 $PORT$ 令牌。
	通知模板 Secure Port 令牌	用于替换供应请求任务和批准通知所用的电子邮件模板中的 $SECURE_PORT$ 令牌。
	通知 SMTP 电子邮件发件人：	指定供应电子邮件中发送邮件用户的电子邮件。
	通知 SMTP 电子邮件主机：	指定供应电子邮件所使用的 SMTP 电子邮件主机。这可以是 IP 地址或 DNS 名。
口令管理	*使用外部口令 WAR*	通过此功能，可以指定外部忘记口令 WAR 中的 “ 忘记口令 ” 页，或外部忘记口令 WAR 用于通过万维网服务回拨 User Application 的 URL。 如果选择 *使用外部口令 WAR*，则必须提供 *忘记口令链接* 和 *忘记口令返回链接* 的值。 如果没有选择 *使用外部口令 WAR*，则 IDM 将使用默认的内部口令管理功能。 /jsps/pwdmgt/ForgotPassword.jsf （开头没有 http(s) 协议）。这将用户重定向到内置于 User Application 的 “ 忘记口令 ” 功能，而不是外部 WAR。
	忘记口令链接	此 URL 指向 “ 忘记口令 ” 功能页。指定外部或内部口令管理 WAR 中的 ForgotPassword.jsf 文件。有关细节，请参阅配置外部口令管理 （第 57 页）。
	忘记口令返回链接	如果使用的是外部口令管理 WAR，需提供外部口令管理 WAR 用来通过万维网服务回调 User Application 的路径，例如 https:// *idmhost:sslport*/idm。

注释 : 安装后，可以编辑此文件中的大部分设置。要执行此操作，请运行安装子目录中的 configupdate.sh 底稿或 Windows configupdate.bat 文件。请记住，在群集中，此文件中的设置对于群集中的所有成员必须保持一致。

A.2 User Application 配置：所有参数

当单击 *显示高级选项* 时，该表包含可用的配置参数。

表 A-2 *User Application 配置：所有选项*

设置类型	选项	说明
eDirectory 连接设置	*LDAP 主机*	必需。为 LDAP 服务器指定主机名或 IP 地址。例如： myLDAPhost
	LDAP 非安全端口	为 LDAP 服务器指定非安全端口。例如：389。
	LDAP 安全端口	为 LDAP 服务器指定安全端口。例如：636。
	LDAP 管理员	必需。指定 LDAP 管理员的身份凭证。该用户必须已经存在。User Application 使用此帐户来建立与身份库的管理连接。此值已使用主密钥进行过加密。
	LDAP 管理员口令	必需。指定 LDAP 管理员口令。此口令已使用主密钥进行过加密。
	使用公开匿名帐户	允许没有登录的用户访问 LDAP 公开匿名帐户。
	LDAP Guest	允许没有登录的用户访问允许的门户小程序。身份库中必须已经存在此用户帐户。要启用 LDAP Guest，必须取消选择*使用公开匿名帐户*。要禁用 Guest 用户，请选择*使用公开匿名帐户*。
	LDAP Guest 口令	指定 LDAP Guest 口令。
	安全 Admin 连接	通过选中此选项，可以要求所有使用 Admin 帐户的通讯都通过安全套接字进行。（此选项可能对性能不利）。此设置允许不需要 SSL 的其他操作在无 SSL 的情况下运行。
	安全用户连接	通过选中此选项，可以要求所有使用已登录用户帐户的通讯都通过安全套接字进行。（此选项可能对性能有严重不利影响）。此设置允许不需要 SSL 的其他操作在无 SSL 的情况下运行。

设置类型	选项	说明
eDirectory DN	*根容器 DN*	必需。指定根容器的 LDAP 判别名。如果没有在目录抽象层中指定搜索根，则将该判别名用作默认的实体定义搜索根。
	供应驱动程序 DN	必需。指定 User Application 驱动程序的判别名 （如第 3.1 节 “在 iManager 中创建 User Application 驱动程序 ”（第 23 页）中所述）。例如，如果驱动程序为 UserApplicationDriver，驱动程序集称为 myDriverSet，并且驱动程序集位于环境 o=myCompany 中，则可以输入以下值： `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`
	User Application Admin	必需。身份库中有权执行所指定 User Application 用户容器的管理任务的现有用户。该用户可以使用 User Application 的*管理*选项卡管理门户。 如果 User Application 管理员参与 iManager、 Designer for Identity Manager 或 User Application （*请求和批准*选项卡）中显示的工作流程管理任务，则必须授予此管理员对 User Application 驱动程序中包含的对象实例的相应受托者权利。有关细节，请参阅 《 *User Application：管理指南*》。 要在部署 User Application 之后更改指派，必须使用 User Application 中的*管理* > *安全*页面。 如果已启动托管 User Application 的应用程序服务器，则无法通过 configupdate 更改此设置。
	供应应用程序管理员	供应应用程序管理员通过 User Application 的*请求和批准*选项卡管理可用的供应工作流程功能。在将用户指定为供应应用程序管理员之前，身份库中必须存在此用户。 要在部署 User Application 之后更改指派，必须使用 User Application 中的*管理* > *安全*页面。
	合规性管理员	合规性模块管理员是一个系统角色，它允许成员执行*合规性*选项卡上的所有功能。在将用户指定为合规性模块管理员之前，身份库中必须存在此用户。 configupdate 执行过程中，仅在未指派有效的合规性模块管理员时，对此值的更改才会生效。如果存在有效的合规性模块管理员，则将不保存更改。 要在部署 User Application 后更改此指派，请使用 User Application 中的*角色* > *角色指派*页面。
	角色管理员	此角色在 Novell Identity Manager 基于角色的供应模块中可用。此角色允许成员创建、去除或修改所有角色，授予或撤消指派给任何用户、组或容器的任何角色。它还允许其角色成员运行任何用户的任何报告。默认情况下，会对 User Application Admin 指派此角色。 要在部署 User Application 后更改此指派，请使用 User Application 中的*角色* > *角色指派*页面。 configupdate 执行过程中，仅在未指派有效的角色管理员时，对此值的更改才会生效。如果存在有效的角色管理员，则将不保存更改。

设置类型	选项	说明
Metadirectory 用户身份	*用户容器 DN*	必需。指定用户容器的 LDAP 判别名 (DN) 或完全限定的 LDAP 名称。 允许该容器中 （及其下）的用户登录 User Application。 如果已启动托管 User Application 的应用程序服务器，则无法通过 configupdate 更改此设置。 **重要：**如果要使该用户能够执行工作流程，请确保在 User Application 驱动程序设置过程中指定的 User Application 管理员在该容器中存在。
	用户容器范围	这定义了用户的搜索范围。
	用户对象类	LDAP 用户对象类 （通常为 inetOrgPerson）。
	登录属性	代表用户的登录名的 LDAP 属性 （比如 CN）。
	命名属性	用作查找用户或组时的标识符的 LDAP 属性。这不同于登录属性，登录属性仅在登录时使用，在用户 / 组搜索时不使用。
	用户成员资格属性	可选。代表用户的组成员资格的 LDAP 属性。不要在该名称中使用空格。
元目录用户组	*组容器 DN*	必需。指定组容器的 LDAP 判别名 (DN) 或完全限定的 LDAP 名称。由目录抽象层中的实体定义使用。 如果已启动托管 User Application 的应用程序服务器，则无法通过 configupdate 更改此设置。
	组容器范围	这定义了组的搜索范围。
	组对象类	LDAP 组对象类 （通常是 groupofNames）。
	组成员资格属性	代表用户组成员资格的属性。不要在该名称中使用空格。
	使用动态组	如果需要使用动态组，请选择该选项。
	动态组对象类	LDAP 动态组对象类 （一般 dynamicGroup）。
eDirectory 证书	*密钥储存区路径*	必需。指定应用程序服务器用于运行的、 JRE 的密钥储存区 (cacerts) 文件的完整路径，或单击小浏览器按钮，然后浏览找到 cacerts 文件。 User Application 安装过程中将修改密钥储存区文件。在 Linux 或 Solaris 上，用户必须具有写此文件的权限。
	密钥储存区口令	必需。指定 cacerts 口令。默认值为 changeit。
	确认密钥储存区口令	

设置类型	选项	说明
私用密钥储存区	*私用密钥储存区路径*	私用密钥储存区包含 User Application 的私用密钥和证书。保留 . 如果保留为空的话，将采用默认路径 /jre/lib/security/cacerts。
	私用密钥储存区口令	口令为 changeit，除非另行指定。此口令已使用主密钥进行过加密。
	私用密钥别名	别名为 novellIDMUserApp，除非另行指定。
	私用密钥口令	口令为 novellIDM，除非另行指定。此口令已使用主密钥进行过加密。
可信密钥储存区	*可信储存区路径*	可信密钥储存区包含所有用于验证数字签名的可信签名者的证书。如果此路径为空的话， User Application 将从系统属性 javax.net.ssl.trustStore 中获取路径。如果那里没有路径，则假定为 jre/lib/security/cacerts。
	可信储存口令	如果此字段为空的话， User Application 将从系统属性 javax.net.ssl.trustStorePassword 中获取口令。如果那里没有值，则使用 changeit。此口令已使用主密钥进行过加密。
Novell Audit 数字签名和证书密钥		包容 Novell Audit 数字签名密钥和证书。
	Novell Audit 数字签名证书	显示数字签名证书。
	Novell Audit 数字签名私用密钥	显示数字签名私用密钥。此密钥已使用主密钥进行过加密。
Access Manager 和 iChain 设置	*已启用同步注销*	如果选中了此选项，则 User Application 支持同时注销 User Application 和 Novell Access Manager 或 iChain。注销时，User Application 检查是否存在 Novell Access Manager 或 iChain cookie，如果存在 cookie，则将用户重路由到 ICS 注销页。
	同步注销页面	Novell Access Manager 或 iChain 注销页面的 URL，其中 URL 是 Novell Access Manager 或 iChain 期望的主机名。如果启用了 ICS 日志记录并且用户要注销 User Application，则将用户重路由到此页面。

设置类型	选项	说明
电子邮件	*通知模板 HOST 令牌*	指定主管 Identity Manager User Application 的应用程序服务器。例如： `myapplication serverServer` 此值将替换电子邮件模板中的 $HOST$ 令牌。所建立的 URL 是指向供应请求任务和批准通知的链接。
	通知模板 PORT 令牌	用于替换供应请求任务和批准通知所用的电子邮件模板中的 $PORT$ 令牌。
	通知模板 SECURE PORT 令牌	用于替换供应请求任务和批准通知所用的电子邮件模板中的 $SECURE_PORT$ 令牌。
	通知模板 PROTOCOL 令牌	指非安全协议 HTTP。用于替换供应请求任务和批准通知所用的电子邮件模板中的 $PROTOCOL$ 令牌。
	通知模板 SECURE PROTOCOL 令牌	指安全协议 HTTPS。用于替换供应请求任务和批准通知所使用电子邮件模板中的 $SECURE_PROTOCOL$ 令牌。
	通知 SMTP 电子邮件发件人：	指定供应电子邮件中发送电子邮件的用户。
	通知 SMTP 电子邮件主机：	指定供应电子邮件所使用的 SMTP 电子邮件主机。这可以是 IP 地址或 DNS 名。
口令管理		
	使用外部口令 WAR	通过此功能，可以指定外部忘记口令 WAR 中的 “ 忘记口令 ” 页，或外部忘记口令 WAR 用于通过万维网服务回拨 User Application 的 URL。 如果选择 *使用外部口令 WAR*，则必须提供 *忘记口令链接* 和 *忘记口令返回链接* 的值。 如果没有选择 *使用外部口令 WAR*，则 IDM 将使用默认的内部口令管理功能。 /jsps/pwdmgt/ForgotPassword.jsf （开头没有 http(s) 协议）。这将用户重定向到内置于 User Application 的 “ 忘记口令 ” 功能，而不是外部 WAR。
	忘记口令链接	此 URL 指向 “ 忘记口令 ” 功能页。指定外部或内部口令管理 WAR 中的 ForgotPassword.jsf 文件。
	忘记口令返回链接	如果使用的是外部口令管理 WAR，需提供外部口令管理 WAR 用来通过万维网服务回调 User Application 的路径，例如 https:// *idmhost:sslport*/idm。
杂项	*会话超时*	应用程序会话超时。
	OCSP URI	如果客户安装使用在线证书状态协议 (OCSP)，请提供统一资源标识符 (URI)。例如，格式为 http://host:port/ocspLocal。OCSP URI 在线更新可信证书的状态。
	授权配置路径	授权配置文件的完全限定名。

设置类型	选项	说明
	创建 eDirectory 索引	如果希望安装实用程序创建 manager、 ismanager 和 srvprvUUID 属性的索引，请选中此复选框。如果这些属性没有索引， User Application 用户可能会遇到不良性能，尤其在群集环境中。安装 User Application 后，可使用 iManager 手动创建这些索引。请参阅第 8.3.1 节 “ 在 eDirectory 中创建索引 ”（第 56 页）。 为达到最佳性能，应完成索引的创建。索引应处于联机方式，才可使用 User Application。
	去除 eDirectory 索引	去除 manager、 ismanager 和 srvprvUUID 属性的索引。
	服务器 DN	选择应创建或去除索引的 eDirectory 服务器。 **注释 :** 要在多个 eDirectory 服务器上配置索引，必须多次运行 configupdate 实用程序。一次只能指定一个服务器。
容器对象	*所选*	选择要使用的每个数字对象类型。
	容器对象类型	有以下标准容器可供选择：位置、国家 / 地区、组织单位、组织和域。也可以在 iManager 中自己定义容器，然后在*添加新容器对象*下面添加这些容器。
	容器属性名称	列出与容器对象类型相关的属性类型名称。
	添加新的容器对象：容器对象类型	指定可作为容器的身份库中对象类的 LDAP 名称。 有关容器的信息，请参阅 《*Novell iManager 2.6 管理指南 (http://www.novell.com/documentation/imanager26/pdfdoc/imanager_admin_26/imanager_admin_26.pdf)*》。
	添加新的容器对象：容器属性名称	提供容器对象的属性名称。