User Application：安装指南

Novell®

Identity Manager 基于角色的供应模块

3.7

2009 年 9 月 18 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保证。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。

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的最终用途。有关出口 Novell 软件的详细讯息，请访问 Novell International Trade Services 网页 (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：*要访问该 Novell 产品及其他 Novell 产品的最新联机文档，请参见 Novell 文档网页 (http://www.novell.com/documentation)。

Novell 商标

有关 Novell 商标，请参见 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 3.7.0。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

我们希望听到您对本手册和本产品中包含的其它文档的意见和建议。请使用联机文档每页底部的 “ 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。包括以下主题：

- 第 1.1 节 “ 安装核对清单 ”（第 9 页）
- 第 1.2 节 “ 关于安装程序 ”（第 10 页）
- 第 1.3 节 “ 系统要求 ”（第 10 页）

如果要从 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/idmrbpm37/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，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 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 17 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 17 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 18 页）。
  - ❑ 安装和配置数据库。请参阅第 2.4 节 “ 安装数据库 ”（第 22 页）。
- ❑ 安装基于角色的供应模块元目录组件。请参见第 3 章 “ 在元目录上安装基于角色的供应模块 ”（第 29 页）。
- ❑ 在 iManager 或 Designer 3.5 for Identity Manager 中创建 User Application 驱动程序。
  - 对于 iManager：第 4.1 节 “ 在 iManager 中创建 User Application 驱动程序 ”（第 41 页）。
  - 对于 Designer：《User Application：设计指南 (http://www.novell.com/documentation/idmrbpm37/index.html)》。
- ❑ 在 iManager 或 Designer 3.5 for Identity Manager 中创建角色和资源服务驱动程序。
  - 对于 iManager：第 4.2 节 “ 在 iManager 中创建角色和资源服务驱动程序 ”（第 42 页）。
  - 对于 Designer：《User Application：设计指南 (http://www.novell.com/documentation/idmrbpm37)》。
- ❑ 安装和配置 Novell Identity Manager User Application。（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 27 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 5 章 “ 在 JBoss 上安装 User Application”（第 45 页）。
    - 第 6 章 “ 在 WebSphere 上安装 User Application”（第 59 页）。
    - 第 7 章 “ 在 WebLogic 上安装 User Application”（第 75 页）。

- 控制台（命令行）界面。请参阅第 8.1 节 “ 从控制台安装 User Application”（第 89 页）。
- 静默安装。请参阅第 8.2 节 “ 使用单个命令安装 User Application”（第 89 页）。

❑ 执行第 9 章 “ 安装后任务 ”（第 97 页）中说明的安装后任务。

重要：本书不提供有关设置安全环境的指导。有关安全性的细节，请参见 《User Application：管理指南 (http://www.novell.com/documentation/idmrbpm37/index.html)》。

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。
- 指定要使用的现有数据库版本，例如 MySQL*、 Oracle*、 DB2*、 Microsoft* SQL Server* 或 PostgreSQL*。该数据库储存 User Application 数据和 User Application 配置信息。
- 配置 JDK 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。
- 配置 Novell Identity Manager User Application 的 Java* Web Application Archive (WAR) 文件，并将其部署到应用程序服务器中。在 WebSphere* 和 WebLogic* 上，必须手动部署 WAR。
- 通过 Novell 或 OpenXDAS 审计客户端启用日志记录 （如果您选择这样做的话）。
- 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。

1.3 系统要求

要使用 Novell Identity Manager 基于角色的供应模块 3.7.0，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 3.6 和 eDirectory	有关受支持操作系统的列表，请参见 Identity Manager 和 eDirectory 文档。
Identity Manager 3.6.1 和 eDirectory	有关受支持操作系统的列表，请参见 Identity Manager 和 eDirectory 文档。
基于 Web 的管理服务器 • iManager 2.7 SP2 和插件	有关受支持操作系统的列表，请参见 iManager 文档。 需要以下插件： • 适用于 iManager 2.7 的 Identity Manager 3.6.1b 插件 • 适用于 iManager 2.7 的 Password Management 3.6.1b 插件

必需的系统组件	系统要求
审计服务 ◆ Sentinel™ 6.1 ◆ Novell Identity Audit 1.0	有关受支持操作系统的列表，请参见 Sentinel 或 Novell Identity Audit 文档。

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。 与 JBoss 5.0.1 搭配使用的 User Application 需要 Sun 提供的 JRE* 1.6.0-14 并且在以下平台上受支持： ◆ Windows 2003 Server （32 位和 64 位） ◆ Windows 2008 Server （32 位和 64 位） ◆ Novell Open Enterprise Server (OES) SP1 （32 位和 64 位） ◆ SUSE Linux Enterprise Server 10 （32 位和 64 位） ◆ SUSE Linux Enterprise Server 11 （32 位和 64 位） ◆ Red Hat Linux 5 （32 位和 64 位） ◆ Solaris 10 （32 位和 64 位） 在 WebSphere 6.1 上运行的 User Application 需要 IBM J9 VM（版本 2.3，J2RE 1.5.0）。它在以下平台上受支持： ◆ Windows 2003 Server （32 位和 64 位） ◆ Windows 2008 Server （32 位和 64 位） ◆ SUSE Linux Enterprise Server 10 （32 位和 64 位） ◆ SUSE Linux Enterprise Server 11 （32 位和 64 位） ◆ Red Hat Linux 5 （32 位和 64 位） ◆ AIX 5.3 （64 位）（仅当使用 Oracle 10g 作为数据库时受支持） ◆ Solaris 10 （32 位和 64 位） 在 WebSphere 7.0 上运行的 User Application 需要 IBM J9 VM（版本 2.4，J2RE 1.6.0）。它在以下平台上受支持： ◆ Windows 2003 Server （32 位和 64 位） ◆ Windows 2008 Server （32 位和 64 位） ◆ SUSE Linux Enterprise Server 10 （32 位和 64 位） ◆ SUSE Linux Enterprise Server 11 （32 位和 64 位） ◆ Red Hat Linux 5 （32 位和 64 位） ◆ Solaris 10 （32 位和 64 位） 在 WebLogic 10.3 上运行的 User Application 需要 JRockit* JVM 1.6.0_05 并且在以下平台上受支持。 ◆ Windows 2003 Server （32 位和 64 位） ◆ Windows 2008 Server （32 位和 64 位） ◆ SUSE Linux Enterprise Server 10 （32 位和 64 位） ◆ SUSE Linux Enterprise Server 11 （32 位和 64 位） ◆ Red Hat Linux 5 （32 位和 64 位） ◆ Solaris 10 （32 位或 64 位) **注释：**只要虚拟机是 User Application 支持的操作系统之一， User Application 即支持 Xen 和 VMWare 虚拟化。

必需的系统组件	系统要求
User Application 浏览器	User Application 同时支持 Firefox* 和 Internet Explorer*，如下所述。 FireFox* 3 在以下平台上受支持： ◆ 带 SP3 的 Windows XP ◆ Windows Vista ◆ SUSE Linux Enterprise Desktop 11 ◆ Novell OpenSuSE 10 ◆ Novell OpenSuSE 11 ◆ Apple Mac Firefox* 2 （仅版本 2.0.0.20）在以下平台上受支持： ◆ Novell SUSE Linux Enterprise Desktop 10 ◆ Novell SUSE Linux Enterprise Server 10 ◆ Novell OpenSuSE 10 Internet Explorer 8 在以下平台上受支持： ◆ 带 SP3 的 Windows XP ◆ Windows Vista Internet Explorer 7 在以下平台上受支持： ◆ Windows XP SP3

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： ◆ MS SQL 2005 ◆ MySQL V5.1 ◆ Oracle 10g ◆ Oracle 11g ◆ PostgreSQL 8.8.3 WebSphere 6.1 支持以下数据库： ◆ DB2 9.5 ◆ MS SQL 2005 ◆ Oracle 10g ◆ Oracle 11g WebSphere 7.0 支持以下数据库： ◆ DB2 9.5 ◆ MS SQL 2005 ◆ Oracle 10g ◆ Oracle 11g WebLogic 10.3 支持以下数据库： ◆ MS SQL 2005 ◆ Oracle 10g ◆ Oracle 11g 支持以下 JDBC 驱动程序： MS SQL Server：sqljdbc_1.0 (sqljdbc.jar)、 sqljdbc_1.1 (sqljdbc.jar)、sqljdbc_1.2 (sqljdbc.jar)、 sqljdbc_2.0 （sqljdbc.jar 和 sqljdbc4.jar） 与 WebLogic 搭配使用的 Oracle10g 或 Oracle11g：ojdbc6.jar （内置在 WebLogic 中） 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：mysql-connector-java.jar v. 5.1.7 IBM DB2 9.5：DB2 JDBC Universal Driver Architecture 3.52.95 PostgreSQL：PostgreSQL8.1JBDC3
Designer	Designer 3.5
OpenXDAS	OpenXDAS V0.8.345 对于 SLES10，需要以下 OpenXDAS 版本： ◆ openxdas-0.8.351-1.1.i586.rpm ◆ openxdas-0.8.351-1.1.x86_64.rpm

必需的系统组件	系统要求
User Application SSO 集成	Novell Access Manager 3.1.1 或 3.1.1 IR1 Novell Secure Login 6.1
Domain Services	OES 2 SP1 Domain Services for Windows
口令管理询问应答	NMAS Challenge Response Login Method 版本：对于口令管理询问应答功能，需要 2770 版本：20080603 或更高版本。

先决条件

2

本节说明在安装 Identity Manager 基于角色的供应模块 (RBPM) 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 3.7 可用于 Identity Manager 3.6 或 3.6.1 元目录。

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

2.2 下载基于角色的供应模块

从 Novell Downloads (http://download.novell.com/index.jsp) （Novell 下载）中获取 Identity Manager 基于角色的供应模块 3.7 产品。为显示在表 2-1 中的产品下载 .iso 映像文件。

表 2-1 *.iso 下载文件*

对于此产品	下载此 .iso
User Application	Identity_Manager_RBPM_3_7_0_User_Application.iso
适用于元目录的基于角色的供应模块组件	Identity_Manager_RBPM_3_7_0_Driver_Install_Utility.iso

表 2-2 说明随 User Application 提供的安装文件以及基于角色的供应模块的 .iso 文件。

表 2-2 *随 ISO 提供的文件和脚本*

文件	描述
IDMProv.war	基于角色的供应模块 WAR。它包括带身份自助服务和基于角色的供应模块功能的 Identity Manager User Application。
IDMUserApp.jar	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。

文件	描述
JBossMySQL.bin 或 JBossMySQL.exe	用于安装 JBoss 应用程序服务器和 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。
rbpm_driver_install.exe	适用于基于角色的供应模块元目录组件的 Windows 安装程序（角色和资源服务驱动程序、 User Application 驱动程序和 eDirectory 纲要）。
rbpm_driver_install_aix.bin	适用于基于角色的供应模块元目录组件的 AIX 安装程序 （角色和资源服务驱动程序、 User Application 驱动程序和 eDirectory 纲要）。
rbpm_driver_install_linux.bin	适用于基于角色的供应模块元目录组件的 Linux 安装程序（角色和资源服务驱动程序、 User Application 驱动程序和 eDirectory 纲要）。
rbpm_driver_install_solaris.bin	适用于基于角色的供应模块元目录组件的 Solaris 安装程序（角色和资源服务驱动程序、 User Application 驱动程序和 eDirectory 纲要）。

安装 Identity Manager 基于角色的供应模块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，但此目录必须在安装开始前已存在并且是可写的（如果在 Linux 或 Solaris 中，必须是非根用户也可以写）。

2.3 安装应用程序服务器

- 第 2.3.1 节 “ 安装 JBoss 应用程序服务器 ”（第 18 页）
- 第 2.3.2 节 “ 安装 WebLogic 应用程序服务器 ”（第 22 页）
- 第 2.3.3 节 “ 安装 WebSphere 应用程序服务器 ”（第 22 页）

2.3.1 安装 JBoss 应用程序服务器

如果计划使用 JBoss 应用程序服务器，您可以：

- 根据制造商的指导下载并安装 JBoss 应用程序服务器。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 应用程序服务器 （可选安装 MySQL）。有关指导，请参阅安装 JBoss 应用程序服务器和 MySQL 数据库 （第 19 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 应用程序服务器最低推荐要求

组件	推荐
RAM	运行 Identity Manager 基于角色的供应模块时，建议 JBoss 应用程序服务器 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，请参见第 9.5 节 “ 配置外部忘记口令管理 ”（第 99 页）和 《*User Application：管理指南* (http://www.novell.com/documentation/idmrbpm37/index.html)》。

安装 JBoss 应用程序服务器和 MySQL 数据库

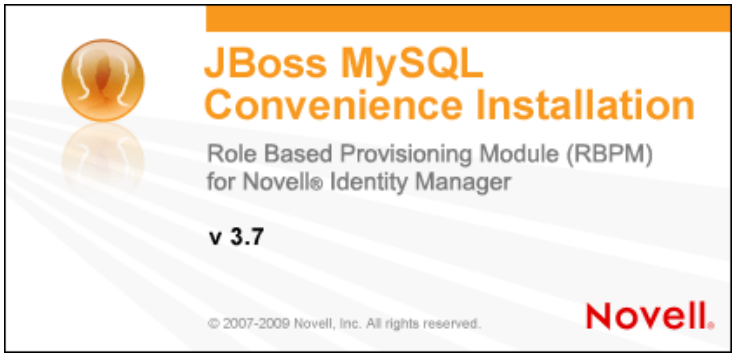
JBossMysql 实用程序在您的系统上安装 JBoss 应用程序服务器和 MySQL。此实用程序不支持控制台方式，它需要图形用户界面环境。对 Linux/Unix 用户，建议您以非根用户身份安装它。

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

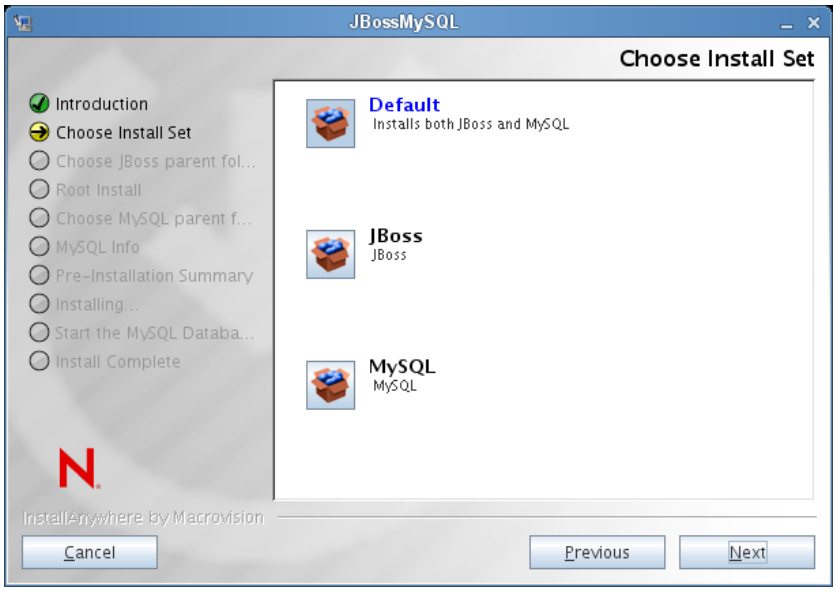
/linux/jboss/JBossMySQL.bin （对于 Linux）
/nt/jboss/JBossMySQL.exe （对于 Windows）

Solaris 不提供此实用程序。

JBossMySQL 实用程序显示其启动屏幕：

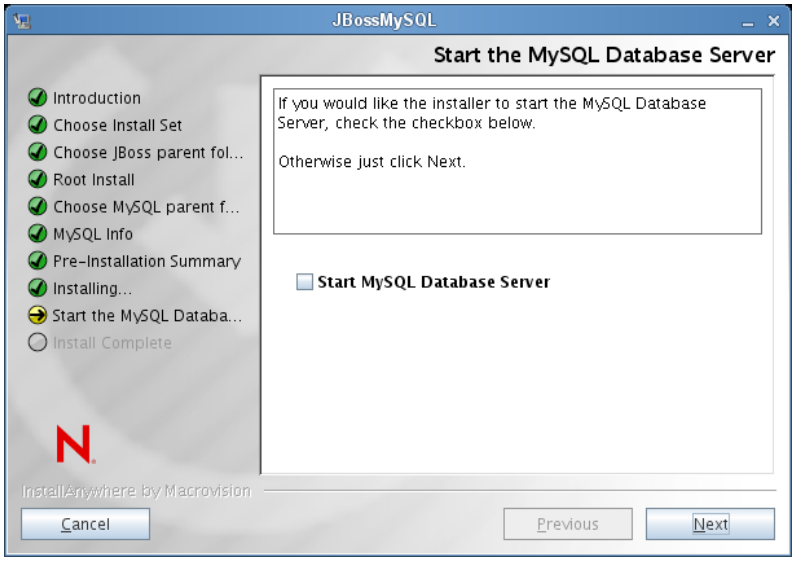


随后，此实用程序显示*选择安装集*屏幕：



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。 ◆ *默认*：将 JBoss 和 MySQL 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。 ◆ *JBoss*：将 JBoss 应用程序服务器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 应用程序服务器作为 Windows 服务安装。有关指导，请参阅将 JBoss 应用程序服务器作为服务或守护程序安装 （第 21 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*。

安装屏幕	说明
启动 MySQL 数据库服务器	如果已安装 MySQL 数据库，实用程序将提示您启动数据库服务器：  需要在继续 User Application 安装之前启动数据库服务器。如果计划立即安装 User Application，请选择*启动 MySQL 数据库服务器*并单击*下一步*。 如果已安装 MySQL 数据库，则还需要按第 2.4.1 节 “ 有关配置 MySQL 数据库的说明 ”（第 22 页）中所述配置此数据库。
安装完成	安装选定产品之后，实用程序将显示一条成功完成的讯息： `The Installer has completed successfully.  Thank you for choosing Novell` **重要**：请注意，JBossMySQL 实用程序不保护 JMX 控制台或 JBoss Web 控制台的安全。这会使 JBoss 环境处于完全开放的状态。完成安装之后，必须立即防范环境，以消除安全隐患风险。

将 JBoss 应用程序服务器作为服务或守护程序安装

要将 JBoss 应用程序作为守护程序启动，请参见来自 JBoss (http://www.jboss.org/community/wiki/StartJBossOnBootWithLinux) 的指导。

使用 JavaServiceWrapper 使用 JavaServiceWrapper，可以安装、启动和停止 JBoss 应用程序服务器，以作为 Windows 服务或 Linux 或 UNIX 守护程序进程。请访问 http://www.jboss.org/community/wiki/RunJBossAsAServiceOnWindows (http://www.jboss.org/community/wiki/RunJBossAsAServiceOnWindows) 参见 JBoss 提供的说明。此类封装程序中的一个位于 http://wrapper.tanukisoftware.org/doc/english/integrate-simple-win.html (http://wrapper.tanukisoftware.org/doc/english/integrate-simple-win.html)：通过 JMX 来管理 （请参见 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 服务来安装、启动和停止 JBoss 应用程序服务器，但 JBoss 不再推荐使用 JavaService。有关细节，请参见 http://www.jboss.org/wiki/JavaService (http://www.jboss.org/community/wiki/JavaService)。

2.3.2 安装 WebLogic 应用程序服务器

如果计划使用 WebLogic 应用程序服务器，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 应用程序服务器

如果计划使用 WebSphere 应用程序服务器，请下载并安装。请参见第 1.3 节 “ 系统要求 ” （第 10 页）获取有关受支持版本的信息。

有关 DB2 配置的说明，请参见有关配置 DB2 数据库的说明 （第 25 页）。

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和 User Application 前，必须已安装并配置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，以便在 User Application 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， User Application 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 文件的名称来命名文件。对于 WebSphere 和 WebLogic，请在安装前手动配置数据源。
- ❑ 对于 Unicode 编码，必须启用数据库。

  User Application 要求数据库字符集使用 Unicode 编码。例如， UTF-8 就是一种使用 Unicode 编码的字符集，而 Latin1 则不使用 Unicode 编码。在安装 User Application 之前，请校验您的数据库是否是用 Unicode 编码的字符集配置的。

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 （即要迁移的源安装版本）所用的同一 User Application 数据库。

2.4.1 有关配置 MySQL 数据库的说明

对于 MySQL， User Application 要求特定的配置选项。如果自行安装 MySQL，请配置这些设置。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 23 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。

设置 default-table-type=innodb 选项的备选方法是，可以将 ENGINE=InnoDB 选项追加到数据库的 SQL 脚本中的 Create Table 语句。

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;connectionCollati
on=utf8_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）。

Ansi 设置

如果选择使用您自己的 MySQL 5.1 安装程序，则需要将 ansi 项添加到 my.cnf （在 Linux 上）或 my.ini 文件 （在 Windows 上）。如果不添加此项，则将创建 RBPM 表，但不会执行此表的初始数据加载，并且可能显示 “ 找不到 Guest 容器页面定义 ” 错误讯息。

添加 ansi 项之后， my.cnf （或 my.ini）文件应类似于如下：

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

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

要确认对使用 ansi 模式的更改是否已生效，可以在您的 MySQL 服务器上执行以下 SQL：

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

用户帐户要求

在安装过程中所用的用户帐户必须具有对 User Application 将要使用的数据库的完全访问权限 （即是此数据库的拥有者）。此外，此帐户还需要对系统中的表的访问权限。根据环境的不同，表可能有所不同。

创建用户以登录 MySQL 服务器并对用户授予特权，例如：

GRANT ALL PRIVILEGES ON <dbname.>* TO <username>@<host> IDENTIFIED BY ‘password’

最低特权集为：CREATE、 INDEX、 INSERT、 UPDATE、 DELETE 和 LOCK TABLES。关于 GRANT 命令的文档，请参阅 http://www.mysql.org/doc/refman/5.0/en/grant.html (http://www.mysql.org/doc/refman/5.0/en/grant.html)。

重要：用户帐户还必须具有对 mysql.user 表的选择权限。以下是授予适当权限所需的 SQL 语法：

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

2.4.2 有关配置 Oracle 数据库的说明

创建 Oracle 数据库时，需要确保使用 AL32UTF8 来指定基于 Unicode 编码的字符集。（请参见 AL32UTF8 (http://download-east.oracle.com/docs/cd/B19306_01/server.102/b14225/glossary.htm#sthref2039)。）

为 Oracle 数据库创建用户时，需要使用 SQL Plus 实用程序发出以下语句。这些语句用于创建用户并设置此用户的特权。授予用户 CONNECT 和 RESOURCE 特权，例如：

CREATE USER *idmuser* IDENTIFIED BY *password*

GRANT CONNECT, RESOURCE to *idmuser*

Oracle 11g 上的 UTF-8 在 Oracle 11g 上，可以发出以下命令以确认是否已针对 UTF-8 启用设置：

```
select * from nls_database_parameters;
```

如果未针对 UTF-8 进行设置，则将返回以下数据：

```
NLS_CHARACTERSET
WE8MSWIN1252
```

如果已针对 UTF-8 进行设置，则将返回以下数据：

```
NLS_CHARACTERSET
AL32UTF8
```

2.4.3 有关配置 MS SQL Server 数据库的说明

按以下方式设置 MS SQL Server 数据库：

1. 安装 MS SQL Server。
2. 连接服务器并打开创建数据库和数据库用户的应用程序 （通常是 SQL Server Management Studio 应用程序）。
3. 创建一个数据库。 SQL Server 不允许用户选择数据库的字符集。IDM User Application 以支持 UTF-8 的 NCHAR 列类型储存 SQL Server 字符数据。
4. 创建登录。
5. 作为数据库用户添加登录。
6. 将以下特权授予登录：CREATE TABLE、 CREATE INDEX、 SELECT、 INSERT、 UPDATE 和 DELETE。

User Application 要求使用 Microsoft SQL Server 2005 JDBC 驱动程序版本 1.0.809.102。请注意，此 JDBC 驱动程序仅官方支持 Sun Solaris、 Red Hat Linux 和 Windows 2000 或更高版本的操作系统。

2.4.4 有关配置 DB2 数据库的说明

本节提供有关 DB2 配置的说明。

提供数据库驱动程序 JAR

安装过程中，需要在*数据库用户名和口令*屏幕上选定数据库驱动程序 JAR 文件。但*数据库驱动程序 JAR 文件*字段的浏览按钮仅允许您选择一个 (1) JAR。对于 DB2，必须提供两个 (2) JAR：

- db2jcc.jar
- db2jcc_license_cu.jar

因此，如果正在运行针对 WebSphere （DB2 唯一支持的应用程序服务器）的安装程序，可以选择一个 JAR，但应使用对于正在运行安装程序的操作系统而言正确的文件分隔符手动输入第二个 JAR。或者，可以手动输入上述两项。

例如，在 Windows 上：

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

例如，在 Solaris 和 Linux 上：

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

微调 DB2 数据库，防止死锁和超时

使用 DB2 时，如果看到错误 “ 由于死锁或超时，当前事务已回滚 ”，则问题可能是由用户和数据库并发程度高引起的。

DB2 提供了许多解决锁定冲突的技巧，包括微调基于成本的优化程序。 DB2 管理文档中所含的*性能指南*是包含关于微调主题更多信息的一个很好来源。

由于数据的并发程度和大小各异，不存在适用于所有安装的规定微调值。但是，有一些可能和您的安装相关的 DB2 微调提示：

- reorgchk update statistics 命令会更新优化程序所用的统计数字。定期更新这些统计数字可能就足以缓解该问题了。
- 使用 DB2 注册表参数 DB2_RR_TO_RS 可通过不锁定插入或更新的行的下个键值，改进并发性能。
- 增大数据库的 MAXLOCKS 和 LOCKLIST 参数。
- 增大数据库连接池的 currentLockTimeout 属性。
- 使用 Database Configuration Advisor，为加快事务处理进行优化。
- 将所有 User Application 表变为 VOLATILE，向优化程序指示表的基数将有显著变化。例如，要使 AFACTIVITY 表变为 VOLATILE，可发出命令：ALTER TABLE AFACTIVITY VOLATILE

  User Application 启动一次并且创建数据库表之后，必须运行 ALTER TABLE 命令。有关该语句的更多信息，请参阅 ALTER TABLE 文档。以下是适用于所有 User Application 表的 SQL 语句：

```
ALTER TABLE AFACTIVITY VOLATILE
ALTER TABLE AFACTIVITYTIMERTASKS VOLATILE
ALTER TABLE AFBRANCH VOLATILE
ALTER TABLE AFCOMMENT VOLATILE
ALTER TABLE AFDOCUMENT VOLATILE
ALTER TABLE AFENGINE VOLATILE
ALTER TABLE AFENGINESTATE VOLATILE
ALTER TABLE AFMODEL VOLATILE
ALTER TABLE AFPROCESS VOLATILE
ALTER TABLE AFPROVISIONINGSTATUS VOLATILE
ALTER TABLE AFQUORUM VOLATILE
ALTER TABLE AFRESOURCEREQUESTINFO VOLATILE
ALTER TABLE AFWORKTASK VOLATILE
ALTER TABLE AF_ROLE_REQUEST_STATUS VOLATILE
ALTER TABLE ATTESTATION_ATTESTER VOLATILE
ALTER TABLE ATTESTATION_ATTRIBUTE VOLATILE
ALTER TABLE ATTESTATION_QUESTION VOLATILE
ALTER TABLE ATTESTATION_REPORT VOLATILE
ALTER TABLE ATTESTATION_REQUEST VOLATILE
ALTER TABLE ATTESTATION_RESPONSE VOLATILE
ALTER TABLE ATTESTATION_SURVEY_QUESTION VOLATILE
ALTER TABLE ATTESTATION_TARGET VOLATILE
ALTER TABLE AUTHPROPS VOLATILE
ALTER TABLE DATABASECHANGELOG VOLATILE
```

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

2.5 安装 Java 开发工具包

User Application 安装程序要求您使用适用于应用程序服务器的 Java 环境的正确版本，如下所述：

- 对于 JBoss 5.01，需要使用 Sun 提供的 Java 2 Platform Standard Edition Development V1.6（JDK 或 JRE）。

  注释：方便起见， JBossMySQL 实用程序将为 JBoss 安装正确版本的 JRE。

- 对于 WebSphere 6.1，需要使用 IBM 提供的 1.5 JDK。
- 对于 WebSphere 7.0，需要使用 IBM 提供的 1.6 JDK。
- 对于 WebLogic 10.3，需要使用 JRockit 提供的 1.6 JDK。

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。

在元目录上安装基于角色的供应模块 3

本节说明如何将基于角色的供应模块 (RBPM) 的元目录组件安装到 Identity Manager 中。包括以下主题：

重要：在较早版本的 Identity Manager （如 Identity Manager 3.6 或 3.6.1）上安装基于角色的供应模块时，需要用到本节所述步骤。Identity Manager 3.7 将为您自动安装 RBPM 的核心组件。

3.1 关于基于角色的供应模块的安装

Identity Manager 基于角色的供应模块 (RBPM) 的安装程序会将若干组件安装到 Identity Manager 元目录中。这些组件包括以下项目：

- 角色和资源驱动程序
- User Application 驱动程序
- eDirectory 纲要

需要在已安装 Identity Manager 元目录环境的计算机上执行 RBPM 安装程序。

将这些项目安装到 Identity Manager 中之后，需要按照第 4 章 “ 创建驱动程序 ”（第 41 页）中所述步骤创建运行 User Application 所需的驱动程序。

重要：如果在使用先前版本的 RBPM 创建的 eDirectory 树中有 User Application 驱动程序，则需要在运行基于角色的供应模块安装程序之前运行 NrfCaseUpdate 实用程序。如果未这样做，则安装将失败。

3.2 运行 NrfCaseUpdate 实用程序

本节提供有关 NrfCaseUpdate 实用程序的细节。包括以下主题：

3.2.1 NrfCaseUpdate 概述

NrfCaseUpdate 过程是对角色和资源进行大小写字母混合搜索必不可少的环节。此过程通过修改 User Application 驱动程序使用的 nrfLocalizedDescs 和 nrfLocalizedNames 属性更新纲要。在安装 RBPM 3.7 以及在 Designer 3.5 中迁移现有驱动程序之前需要执行此过程。

3.2.2 安装概述

本节提供升级和迁移您的现有 RBPM 环境的步骤概述。本概述强调在继续进行任何升级之前使用 Designer 3.5 来创建 User Application 驱动程序的备份。本概述还假设 IDM 版本为 3.6 或更高版本。

1. 安装 Designer 3.5。
2. 运行身份库状态检查以确保纲要正确扩展。使用 TID 3564075 完成状态检查。
3. 将现有 User Application 驱动程序导入到 Designer 3.5 中。
4. 对 Designer 项目存档。它代表驱动程序在安装 RBPM 3.7 之前的状态。
5. 运行 NrfCaseUpdate 过程。
6. 创建新的 Designer 3.5 项目并导入 User Application 驱动程序以准备进行迁移。
7. 安装 RBPM 3.7。
8. 使用 Designer 3.5 迁移驱动程序。
9. 部署迁移后的驱动程序。

3.2.3 NrfCaseUpdate 如何影响纲要

当 NrfCaseUpdate 实用程序在 eDirectory 纲要中更新现有属性时，那些属性的任何现有实例都将有效删除。 User Application 驱动程序将使用这些属性，因此会受到此纲要更新 （特别是角色以及责任分离名称和说明、自定义证明请求和报告）的影响。

NrfCaseUpdate 过程通过在运行纲要更新之前提供用于导出现有 User Application 驱动程序的实用程序来更新现有 User Application 驱动程序。在纲要更新之后导入 LDIF 文件可有效地重创建在纲要更新期间删除的任何对象。

通常，对现有 User Application 驱动程序进行备份是非常重要的预防措施。请记住，纲要更新将影响所有 IDM 分区，因此使用 NrfCaseUpdate 导出树中所有 User Application 驱动程序至关重要。

3.2.4 创建 User Application 驱动程序的备份

建议使用 Designer 创建 User Application 驱动程序的备份。在运行 NrfCaseUpdate 过程之前，应按照此过程备份您的现有 User Application 驱动程序：

1. 安装随 RBPM 3.7 提供的 Designer 3.5。
2. 创建身份库并将其映射到包含 User Application 驱动程序的 IDM 服务器。
3. 使用 *在线 -> 导入*命令导入驱动程序集和 User Application 驱动程序。
4. 保存并对此 Designer 项目存档。

3.2.5 使用 NrfCaseUpdate

NrfCaseUpdate 将提示您导出每个驱动程序，然后执行纲要更新。如果不确定现有 User Application 驱动程序是否存在或其位置，则不应继续执行操作，因为纲要更新可能会使任何现有 User Application 驱动程序无效。

在 IDM 安装目录下提供的 JRE （通常为 /root/idm/jre）可用于运行 NrfCaseUpdate。如果需要到 eDirectory 的 SSL 连接，则需要按照第 3.2.7 节 “ 启用 SSL 连接的 JRE”（第 33 页）中的指导启用 SSL 连接的 JRE。

或者，可以从带 JRE （包含 eDirectory 证书）的主机 （如 User Application 服务器主机）远程运行 NrfCaseUpdate 实用程序。在这种情况下，您需要在将所有驱动程序导出到 LDIF 后且在纲要更新前使用 CTRL-C 退出 NrfCaseUpdate 实用程序。然后，您可以使用 ndssch 命令在 eDirectory 主机上手动更新纲要，如下所示：

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

注释：NrfCaseUpdate 可接受若干命令行自变量。传递命令 -help 或 -? 以获取更多信息。

按照以下步骤运行 NrfCaseUpdate：

1. 在运行 NrfCaseUpdate 实用程序前，请校验是否已完成身份库状态检查。使用 TID 3564075 完成状态检查。
2. 在启动实用程序之前，标识现有 User Application 驱动程序的所有 DN。需要鉴定身份凭证以将这些驱动程序导出到 LDIF。
3. 运行 NrfCaseUpdate 实用程序。可以传递 -v 选项以获取更多详细输出：

   ```
   /root/idm/jre/bin/java -jar NrfCaseUpdate.jar -v
   ```

4. 系统将询问您是否具有现有 User Application 驱动程序。如果有现有 User Application 驱动程序，请回答 True。否则，请回答 False 并跳转至步骤 6 （第 31 页）。

   ```
   Do you currently have a User Application Driver configured [DEFAULT true]
   :
   ```

5. 接下来，实用程序将询问您是否有多个 User Application 驱动程序。如果有多个 User Application 驱动程序，请回答 True：

   ```
   Do you currently have more than one (1) User Application Driver configured
   [DEFAULT false] :
   ```

6. 指定带适当身份凭证的管理员 DN 以导出 User Application 驱动程序：

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

7. 输入此管理员的口令：

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

8. 输入 User Application 驱动程序所在的 IDM 服务器的主机名或 IP 地址：

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

9. 指定要用于连接的端口：

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

10 下一个问题是询问您是否要使用 SSL 进行连接。如果要使用 SSL，则 JRE 需要将放在可信储存区中的 eDirectory 证书。要保留证书，请按第 3.2.7 节 “ 启用 SSL 连接的 JRE”（第 33 页）中的指导操作。

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

11 指定要导出的 User Application 驱动程序的完全限定判别名：

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

12 指定要将 User Application 导出到的 LDIF 文件的名称：

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

13 实用程序将张贴有关保存到 LDIF 的对象的信息。

14 如果指出具有多个驱动程序，则将看到以下提示：

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

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

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

15 系统将提示您 ndssch 实用程序的位置及其常规位置。 ndssch 实用程序用于更新纲要。

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

16 实用程序将张贴纲要更新的状态讯息：

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

注释：确保给予 eDirectory 足够的时间以同步纲要更改。如果未给予足够的时间，则 LDIF 文件的导入将失败。

---

17 运行其他身份库状态检查，以在导入 LDIF 文件前校验纲要是否已正确扩展。使用 TID 3564075 完成状态检查。

18 导出所有驱动程序并成功应用纲要更新后，需要导入每个 LDIF 文件。应指出允许在 ice 命令中转发参照。建议的命令行如下所示：

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

19 重新导入所有驱动程序后，请校验 NrfCaseUpdate 过程是否成功。有关更多信息，请参见第 3.2.6 节 “NrfCaseUpdate 过程的校验 ”（第 32 页）。

20 校验完 NrfCaseUpdate 过程已成功后，可以继续 RBPM 3.7 的安装。

3.2.6 NrfCaseUpdate 过程的校验

重新导入所有驱动程序后，请通过在 User Application 中审阅以下各项来校验恢复是否成功：

- 角色名称和说明

- 责任分离名称和说明
- 证明请求，包括自定义请求
- 报告

完成校验后，可以继续安装并升级至 RBPM 3.7。

3.2.7 启用 SSL 连接的 JRE

本节说明如何配置 JRE 以使用 SSL 连接。

首先，在身份库中从证书颁发机构导出自我签名证书：

1. 在 iManager 的*角色和任务*视图中，单击*目录管理 > 修改对象*。
2. 选择身份库的证书颁发机构对象，然后单击*确定*。通常可在安全性容器中找到它，其名称为 *TREENAME* CA.Security。
3. 单击*证书 > 自我签名证书*。
4. 单击*导出*。
5. 当系统询问您是否要导出带证书的私用密钥时，请单击*否*，然后单击*下一步*。
6. 选择二进制 DER 格式。
7. 单击链接*保存导出的证书*。
8. 在计算机上浏览到要保存此文件的位置，然后单击*保存*。
9. 单击*关闭*。

接下来，将自我签名证书导入到 JRE 的可信储存区中。

1. 使用 JRE 中包含的密钥工具实用程序。
2. 通过在命令提示符处输入以下命令，将证书导入 Role Mapping Administrator 的可信储存区：

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

   例如：

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

3.2.8 恢复无效的 User Application 驱动程序

如果在使用 NrfCaseUpdate 处理现有 User Application 驱动程序之前就将纲要更新应用到此驱动程序，则此驱动程序将无效，并且您需要使用备份恢复此驱动程序。

重要：*请勿*删除或重命名无效的 User Application 驱动程序，这一点至关重要，因为这样做会使此驱动程序的所有关联项也变得无效。此外，如果角色和资源服务驱动程序正在运行，而您删除 User Application 驱动程序，则角色和资源服务驱动程序将检测到角色删除并去除所指派用户的角色。

此外，也不能将备份后的驱动程序重部署到 IDM，因为在这种情况下无法调整纲要更改。以下过程执行恢复，方法是部署此驱动程序的重命名副本以生成要恢复的数据。

以下过程概述了使用 Designer 3.5 恢复 User Application 驱动程序备份的过程：

1. 重启动 eDirectory 服务器以确保纲要修改已生效。
2. 打开包含 User Application 驱动程序备份 （即 UserAppDriver）的 Designer 3.5 项目的副本。由于此过程会修改驱动程序名称，因此最好使用项目副本。
3. 选择 User Application 驱动程序和身份库之间的连接器，右键单击并选择*属性*。
4. 指定一个新名称，如 UserAppDriver_restore。选择*应用*和*确定*。
5. 单击*保存*以保存项目。
6. 通过选择 ID 库并依次选择*在线* -> *纲要* -> *比较*同步 ID 库，然后选择*更新 Designer 以执行调整操作*。
7. 保存此项目。
8. 通过选择驱动程序并依次选择*驱动程序* -> *部署*来部署重命名的驱动程序。
9. 运行 NrfCaseUpdate 并将新命名的驱动程序导出到 LDIF 文件。
10. 制作 LDIF 文件的副本以进行编辑。
11. 编辑 LDIF 文件并重命名所有驱动程序参照以反映正在恢复的 User Application 驱动程序。例如，如果原始 User Application 驱动程序为 cn=UserAppDriver，然后您将 cn=UserAppDriver_restore 重命名为 cn=UserAppDriver。此步骤有效构建了能够反映真实 User Application 驱动程序的 LDIF 文件。
12. 使用 ice 导入修改后的 LDIF 文件：

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

13. 注意使用 ice 导入的状态，以确保导入成功。
14. 按照第 3.2.6 节 “NrfCaseUpdate 过程的校验 ”（第 32 页）中的指导校验驱动程序的恢复。
15. 从驱动程序集中删除重命名的驱动程序。

3.3 运行 RBPM 安装程序

1. 起动适用于您的平台的安装程序：

   Linux

   ```
   rbpm_driver_install_linux.bin
   ```

   Solaris

   ```
   rbpm_driver_install_solaris.bin
   ```

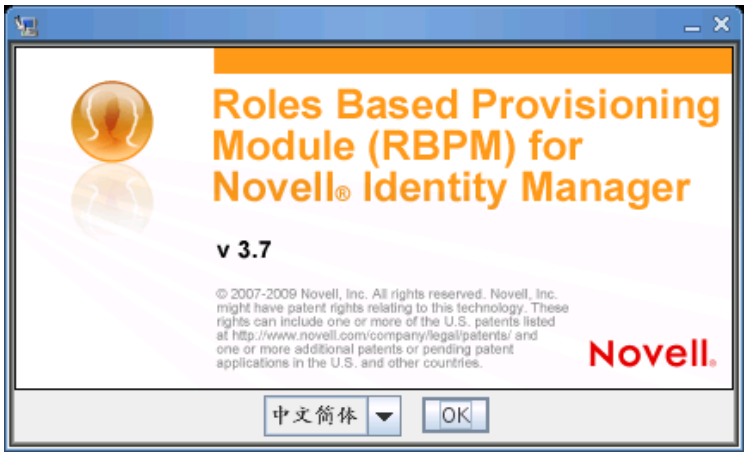
   AIX

   ```
   rbpm_driver_install_aix.bin
   ```

   Windows

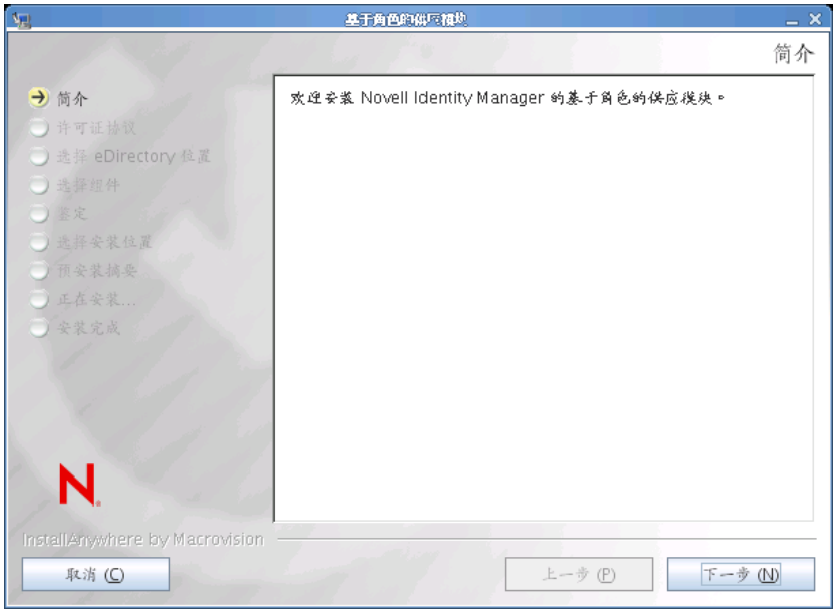
   ```
   rbpm_driver_install.exe
   ```

   安装程序起动后，系统会提示您选择语言：



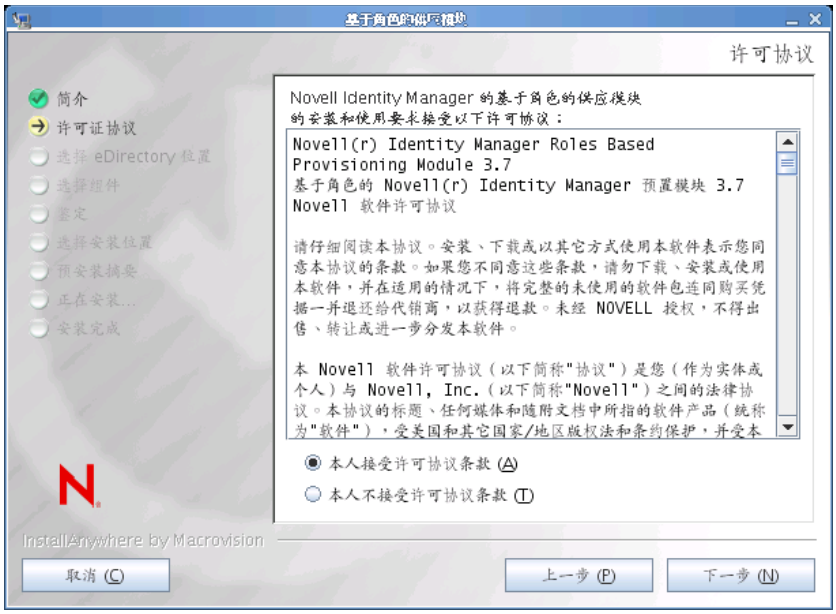
2 选择安装语言并单击 “ 确定 ”。

安装程序显示 “ 简介 ” 屏幕。



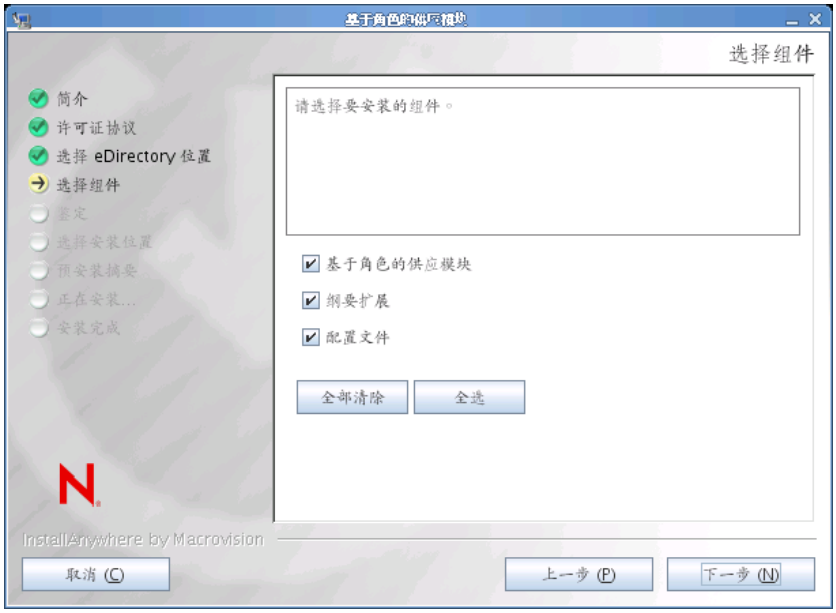
3 单击 *下一步*。

安装程序显示 “ 许可协议 ” 屏幕。



4 确认许可协议并单击 *下一步*。

安装程序显示 “ 选择组件 ” 屏幕，其中已列出要运行 RBPM User Application 所需的元目录组件：



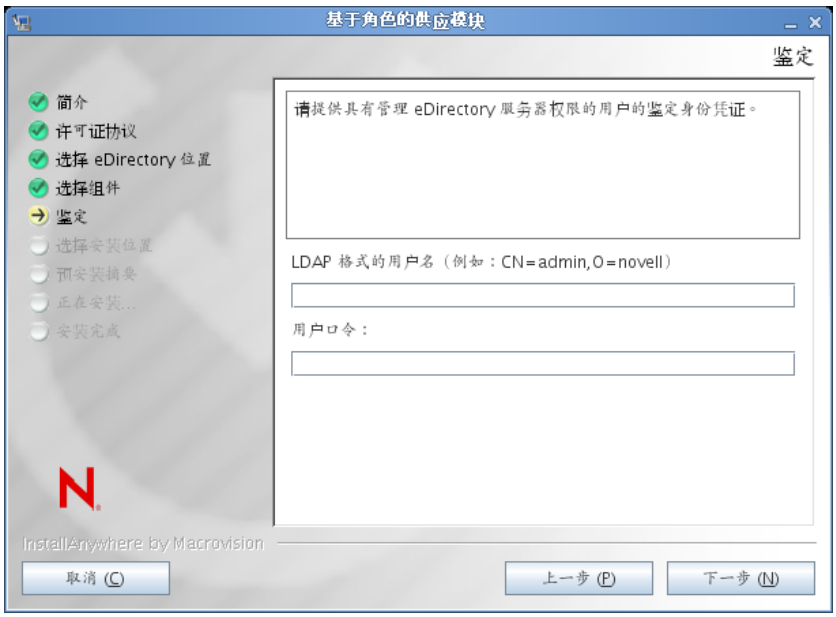
这些组件如下所述：

组件	说明
基于角色的供应模块	安装 User Application 驱动程序以及角色和资源驱动程序。
纲要扩展	安装 eDirectory 纲要扩展。

组件	说明
配置文件	安装驱动程序配置文件。

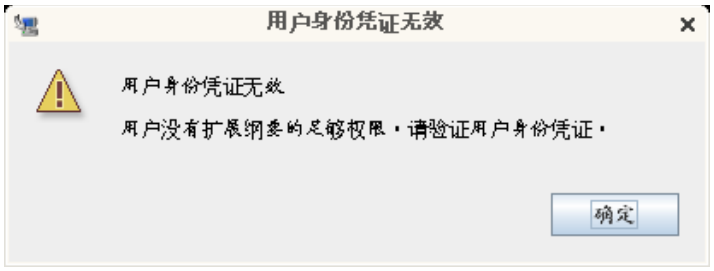
5 选择要安装的组件，然后单击 *下一步*。通常，需要安装所有组件。

安装程序显示 “ 鉴定 ” 屏幕：



6 以 LDAP 格式提供用户名并键入口令：

如果用户身份凭证无效，或者如果用户不具有必要的权限，则安装程序会显示出错屏幕：



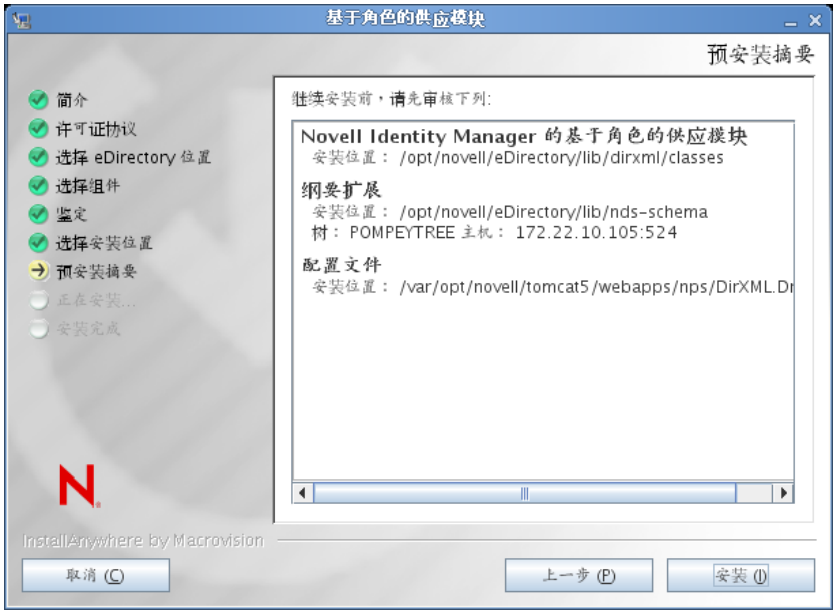
如果用户身份凭证有效，并且用户具有适当的权限，则安装程序会显示“驱动程序配置文件的安装位置”屏幕：

7 指定要储存驱动程序配置文件的磁盘目标位置，然后单击 *下一步*。

安装程序显示“驱动程序的安装位置”屏幕：

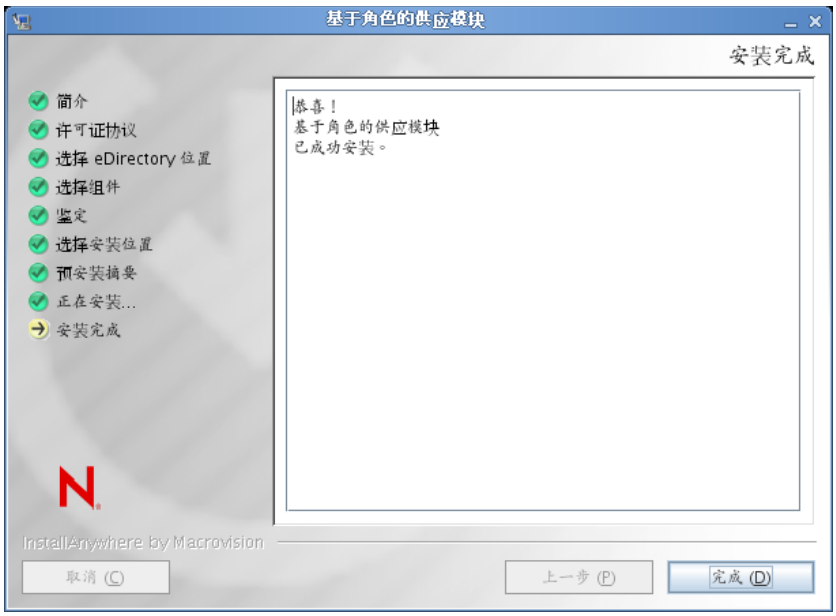
8 指定驱动程序的目标位置，然后单击 *下一步*。

安装程序显示 “ 预安装摘要 ” 屏幕：



9 如果您认为摘要信息是正确的，请单击 *安装*以开始安装过程。

安装过程完成时，安装程序显示 “ 安装完成 ” 屏幕：



创建驱动程序

4

本节说明如何创建使用基于角色的供应模块 (RBPM) 所需的驱动程序。包括以下主题：

重要：在创建角色和资源服务驱动程序前，需要创建 User Application 驱动程序。需要先创建 User Application 驱动程序，因为角色和资源服务驱动程序参照 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和资源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。

4.1 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。

必须为每个 RBPM User Application 创建单独的 User Application 驱动程序，群集中的 RBPM User Application 除外。同一群集中的 User Application 必须共享一个 User Application 驱动程序。有关运行群集中的 User Application 的信息，请参见 《*User Application：管理指南* (http://www.novell.com/documentation/idmrbpm37/index.html)》。

重要：配置一组非群集 RBPM User Application 来共享一个驱动程序会使在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 Web 浏览器中打开 iManager。
2. 转至*角色和任务* > *Identity Manager 实用程序*并选择*导入配置*。
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*，单击对象选择器图标，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_7_0-IDM3_6_0-V1.xml

如果此文件不在列表中，基于角色的供应模块的驱动程序安装可能无法正确进行。

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 RBPM User Application 时需要用到它们。

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*，选择要从驱动程序操作 （如管理角色）中排除的用户 , 然后单击 *确定*。

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 如果信息正确，请单击 *完成*。

重要：默认情况下，驱动程序为关闭状态。将驱动程序保持为关闭状态，直到安装好 RBPM User Application。

4.2 在 iManager 中创建角色和资源服务驱动程序

在 iManager 中创建和配置角色和资源服务驱动程序：

1 在 Web 浏览器中打开 iManager。

2 转至 *角色和任务* > *Identity Manager 实用程序* 并选择 *导入配置*。

先安装角色和资源服务驱动程序，再安装 User Application 驱动程序。将 User Application 驱动程序版本 3.7.0 (UserApplication_3_7_0-IDM3_6_0-V1.xml) 与 角色和资源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，则角色和资源编目可能不可用。

3 在该向导中，保留*现有驱动程序集*中的默认值。浏览至在第 4.1 节 “ 在 iManager 中创建 User Application 驱动程序 ”（第 41 页）中创建的驱动程序集。单击 *下一步*。

注释：User Application 驱动程序以及角色和资源驱动程序应在同一驱动程序集中。

4 从下拉列表中选择 *RoleResourceService_3_7_0-IDM3_6_0-V1.xml*。这是支持基于角色的供应模块的角色和资源服务驱动程序配置文件。

如果此文件不在列表中，基于角色的供应模块的安装程序可能无法正确进行。

单击 *下一步*。

5 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	描述
驱动程序名	指定驱动程序名称或保留角色和资源服务驱动程序的默认名称 Role and Resource Service。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。如果存在组角色或资源指派，则角色和资源服务驱动程序将仅授予 / 撤消容器域内成员的角色或资源。
User Application 驱动程序 DN	主管角色或资源系统的 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。
重输入口令	重输入 User Application 管理员口令。

6 填充信息后，单击 *下一步*。

7 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。

8 （可选，但不推荐）单击*排除管理角色*。

9 单击*添加*，选择要从驱动程序操作 （如管理角色）中排除的用户 , 然后单击*确定*。

10 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。

11 如果信息正确，请单击*完成*。

在 JBoss 上安装 User Application

5

本节说明如何在 JBoss 应用程序服务器上通过使用安装程序的图形用户界面版本为基于角色的供应模块安装 User Application。它包含以下主题：

- 第 5.1 节 “ 安装和配置 User Application WAR”（第 45 页）
- 第 5.2 节 “ 测试安装 ”（第 57 页）

如果要使用命令行进行安装，请参阅第 8 章 “ 从控制台或使用单条命令进行安装 ”（第 89 页）。

以非根用户身份运行安装程序。

数据迁移 有关迁移的信息，请参见 《*User Application：迁移指南* (http://www.novell.com/documentation/idmrbpm37/index.html)》。

5.1 安装和配置 User Application WAR

注释：对于 JBoss 5.0.1，安装程序需要使用 Sun 提供的 Java 2 Platform Standard Edition Development Kit 版本 1.6 （JRE 或 JDK）。如果使用其他版本，则安装过程将无法成功配置 User Application WAR 文件。安装看似成功，但尝试启动 User Application 时遇到错误。

1 从命令行起动适用于平台的安装程序：

确保使用 Sun JDK 版本按以下方式启动 User Application 安装程序：

Linux/Solaris

```
$ /opt/jdk1.6.0_14/bin/java -jar IdmUserApp.jar
```

Windows

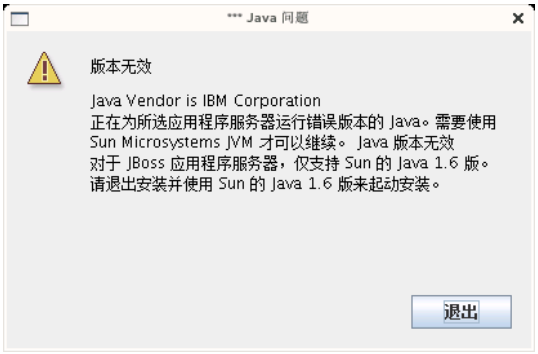
```
C:\Novell\InstallFiles\> "C:\Program Files\Java\jdk1.6.0_14\bin\java.exe"
-jar IdmUserApp.jar
```

当安装过程中需要安装 Java 的完整路径时，提供 Sun JDK 的根路径。例如，在 Linux 上的根路径可能是 /opt/jkd1.6.0_14。

注释：SLES 用户：请勿使用 SLES 随附的 IBM* JDK。此版本与安装的某些方面不兼容，并且可能导致主密钥损坏错误。

安装程序起动后，系统会提示您选择语言：

2 使用以下信息选择语言，确认许可协议，并选择应用程序服务器平台：

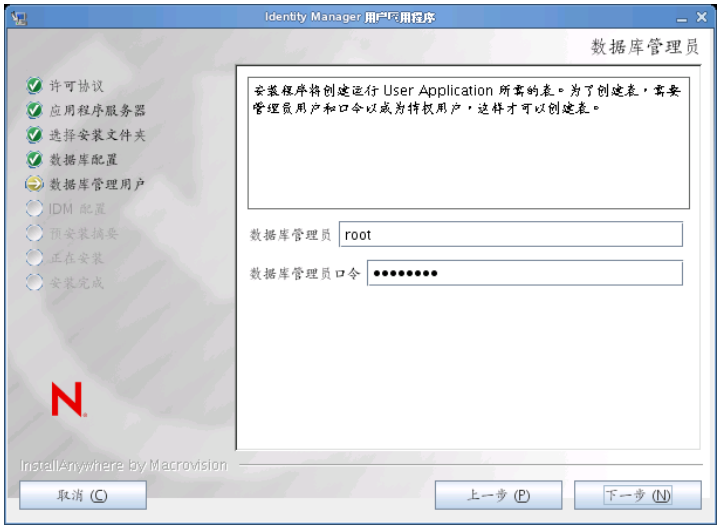
安装屏幕	说明
User Application 安装	选择安装程序的语言。默认为英语。
许可证协议	阅读许可协议，然后选择*我接受本许可协议的条款*。
应用程序服务器平台	选择 *JBoss*。 在 JBoss 上进行安装时，需要使用 Sun Java 环境起动安装程序。如果选择 JBoss 作为应用程序服务器且不使用 Sun Java 来起动安装，您将看到一条弹出式错误讯息，并且安装将终止： 

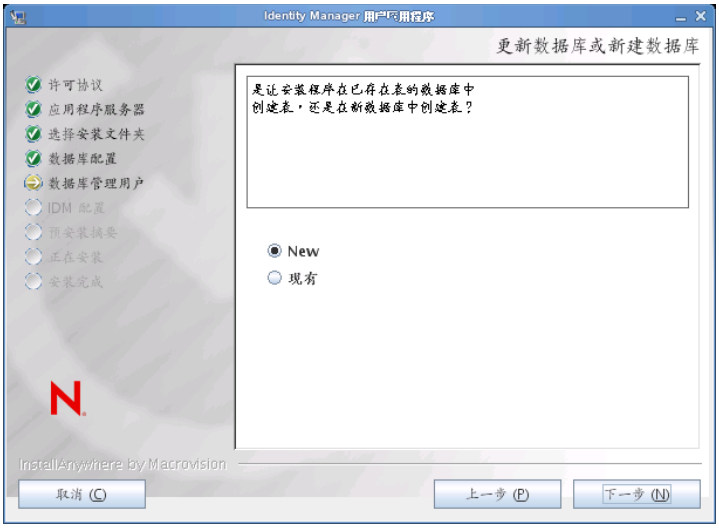
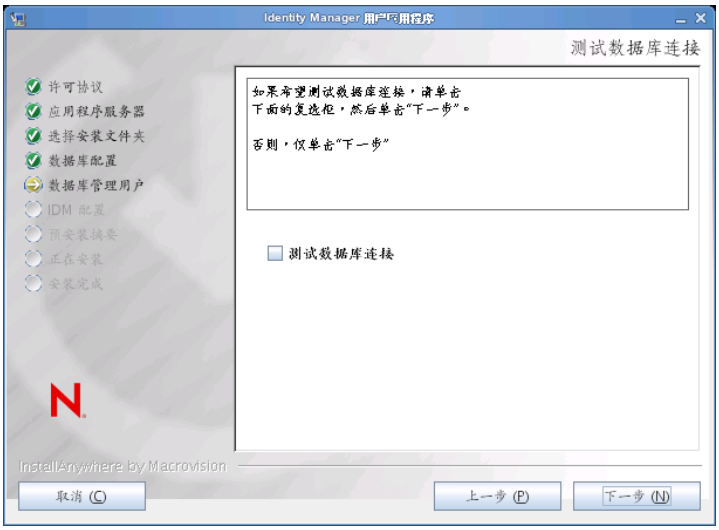
3 使用以下信息选择安装类型，选择安装文件夹，并配置数据库：

安装屏幕	说明
安装类型	*基于角色的供应*：选择此选项来安装基于角色的供应模块。这是此版本支持的唯一安装类型。
选择安装文件夹	指定安装程序放置这些文件的位置。

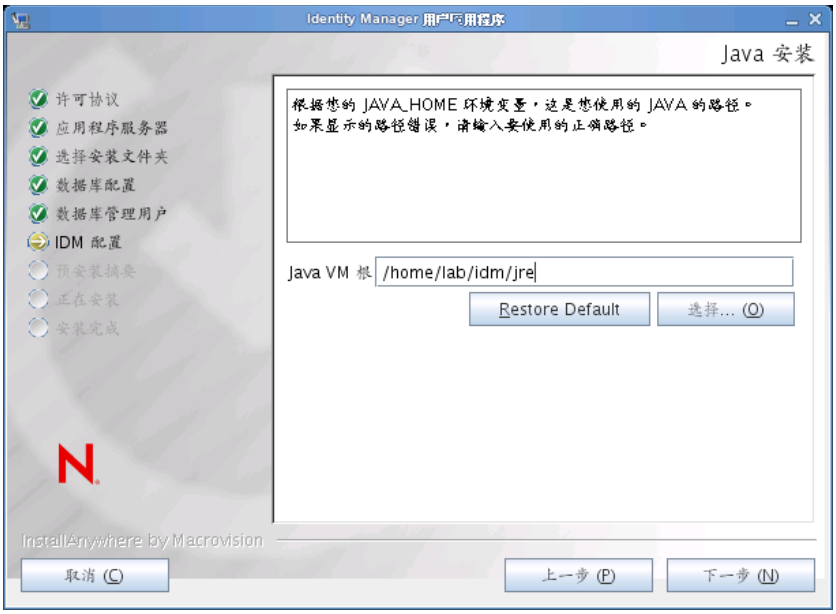
安装屏幕	说明
数据库平台	选择数据库平台。必须已安装数据库和 JDBC 驱动程序。对于 JBoss，选项如下： ◆ MySQL ◆ Oracle （仅支持 Oracle 10g 和 11g ； 不再支持 Oracle 9i） ◆ PostgreSQL （仅当安装 JBoss 时可用） ◆ Microsoft SQL Server ◆ IBM DB2 （仅支持版本 9.5 ； 不再支持版本 9.1）
数据库主机和端口	*主机*：指定数据库服务器的主机名或 IP 地址。对于群集，对其中每个成员指定相同的主机名或 IP 地址。 *端口*：指定数据库监听程序的端口号。对于群集，对其中每个成员指定相同的端口。 

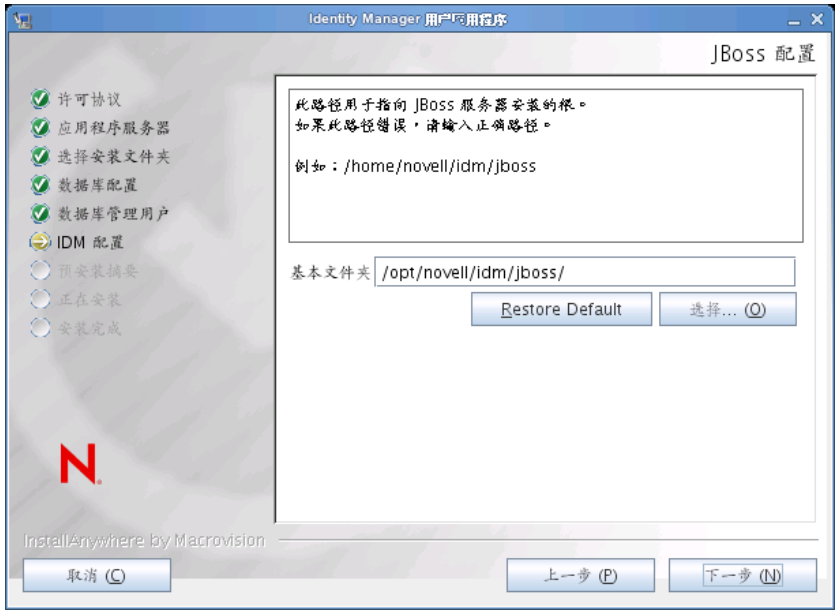
安装屏幕	说明
数据库用户名和口令	*数据库名称*（或 SID）：对于 MySQL、 MS SQL Server 或 PostgreSQL，请提供预定数据库的名称。对于 Oracle，请提供以前创建的 Oracle 系统标识符 (SID)。对于群集，对其中每个成员指定相同的数据库名称或 SID。 *数据库用户*名：指定数据库的用户。对于群集，对其中每个成员指定相同的数据库用户。 *数据库口令*：指定数据库的口令。对于群集，对其中每个成员指定相同的数据库口令。 *数据库驱动程序 JAR 文件*：为数据库服务器提供瘦客户端 JAR。此项是必需的。 

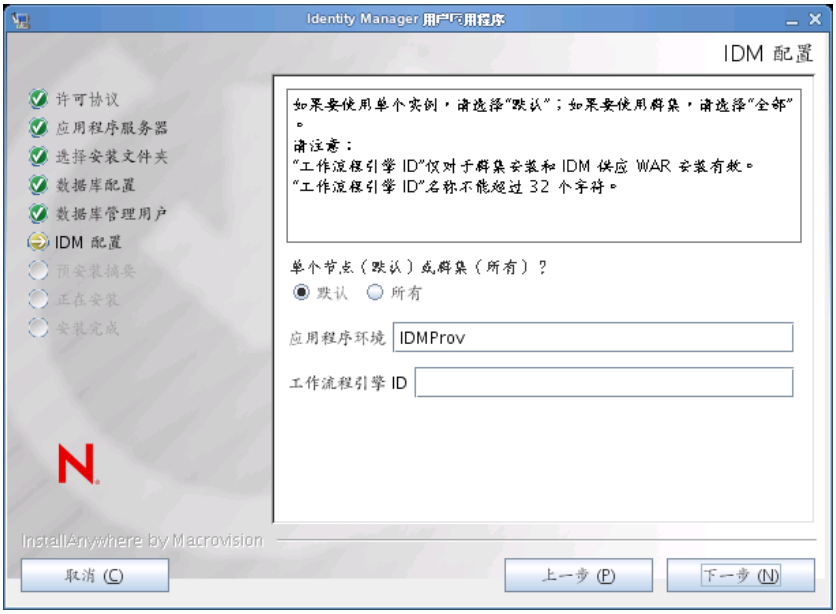
安装屏幕	说明
SQL 输出文件	在此版本中，可在 User Application 安装期间而不是在应用程序服务器启动时创建数据库表 （如同在先前版本中）。 “SQL 输出文件 ” 屏幕提供创建纲要文件的选项，数据库管理员可用来创建表，而不是让安装程序创建表。 如果要生成纲要文件，请选中*将 SQL 写入文件*复选框，并在*纲要输出文件*字段中提供文件名。 
数据库管理员	此屏幕将用 “ 数据库用户名和口令 ” 页面中的同一用户名和口令进行预填充。如果先前指定的数据库用户不具有在数据库服务器中创建表的足够许可权限，则需要输入具有必要权限的其他用户 ID。 

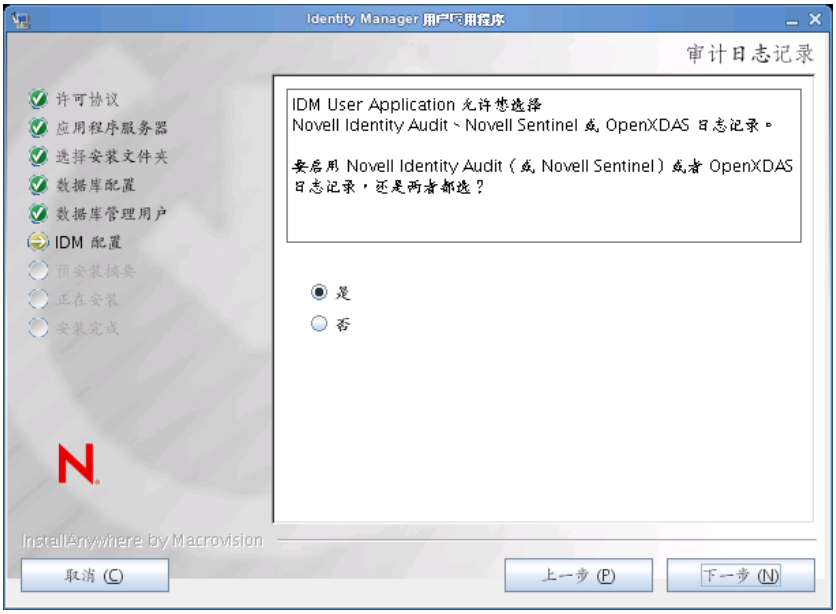
安装屏幕	说明
更新数据库或新建数据库	如果要使用的数据库是新的或空的，请选择*新建*按钮。如果数据库是先前安装中的现有数据库，请选择*现有*按钮。 
测试数据库连接	要确认先前屏幕中提供的信息是否正确，可以选中*测试数据库连接*复选框来测试数据库连接： 

4 使用以下信息配置 Java、 JBoss 安装和 IDM，以及审计设置和安全性。

安装屏幕	说明
Java 安装	指定 Java 安装根文件夹。 Java 安装根据 JAVA_HOME 环境变量提供 Java 路径，并提供用于更正此路径的选项：  此时，安装程序会验证选定的 Java 对于选定的应用程序服务器而言是否正确。此外，安装程序还会验证它是否能写入所指定的 JRE 中的 cacerts。 然后，系统会出现提示，询问您有关 JBoss 应用程序服务器的安装位置的信息：

安装屏幕	说明
JBoss 配置	告知 User Application JBoss 应用程序服务器所在的位置。 此安装过程不安装 JBoss 应用程序服务器。有关安装 JBoss 应用程序服务器的指导，请参阅安装 JBoss 应用程序服务器和 MySQL 数据库 （第 19 页）。 *基本文件夹*：指定应用程序服务器的位置。 

安装屏幕	说明
IDM 配置	选择应用程序服务器配置的类型： ◆ 如果此安装位于不属于群集的单独节点，则选择*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。 ◆ 如果此安装是群集中的一部分，则选择*全部*。 *应用程序环境*：应用程序服务器配置的名称、应用程序 WAR 文件的名称，以及 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”仅对于群集安装和 IDM 供应 WAR 安装有效。引擎 ID 不能超过 32 个字符。有关“工作流程引擎 ID”的说明，请参见《*User Application：管理指南*》中有关为群集配置工作流程的小节。 

安装屏幕	说明
Audit 日志记录	要启用日志记录，请单击*是*。要禁用日志记录，请单击*否*。  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 Identity Audit 或 Novell Sentinel*：通过适用于 User Application 的 Novell Client 启用日志记录。 ◆ *OpenXDAS*：事件将记录到 OpenXDAS 日志记录服务器中。 有关设置日志记录的更多信息，请参见 《*User Application：管理指南*》。 

安装屏幕	说明
Novell Audit	*服务器*：如果启用日志记录，请指定服务器的主机名或 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 9.1 节 “ 记录主密钥 ”（第 97 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。

5 单击 *下一步*以显示 “ 基于角色的供应模块配置 ” 面板。（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 27 页）中所述的步骤。）

“ 基于角色的供应模块配置 ” 面板的默认视图显示以下六个字段：

安装程序将调用 “ 根容器 DN” 中的值并将其应用于以下值：

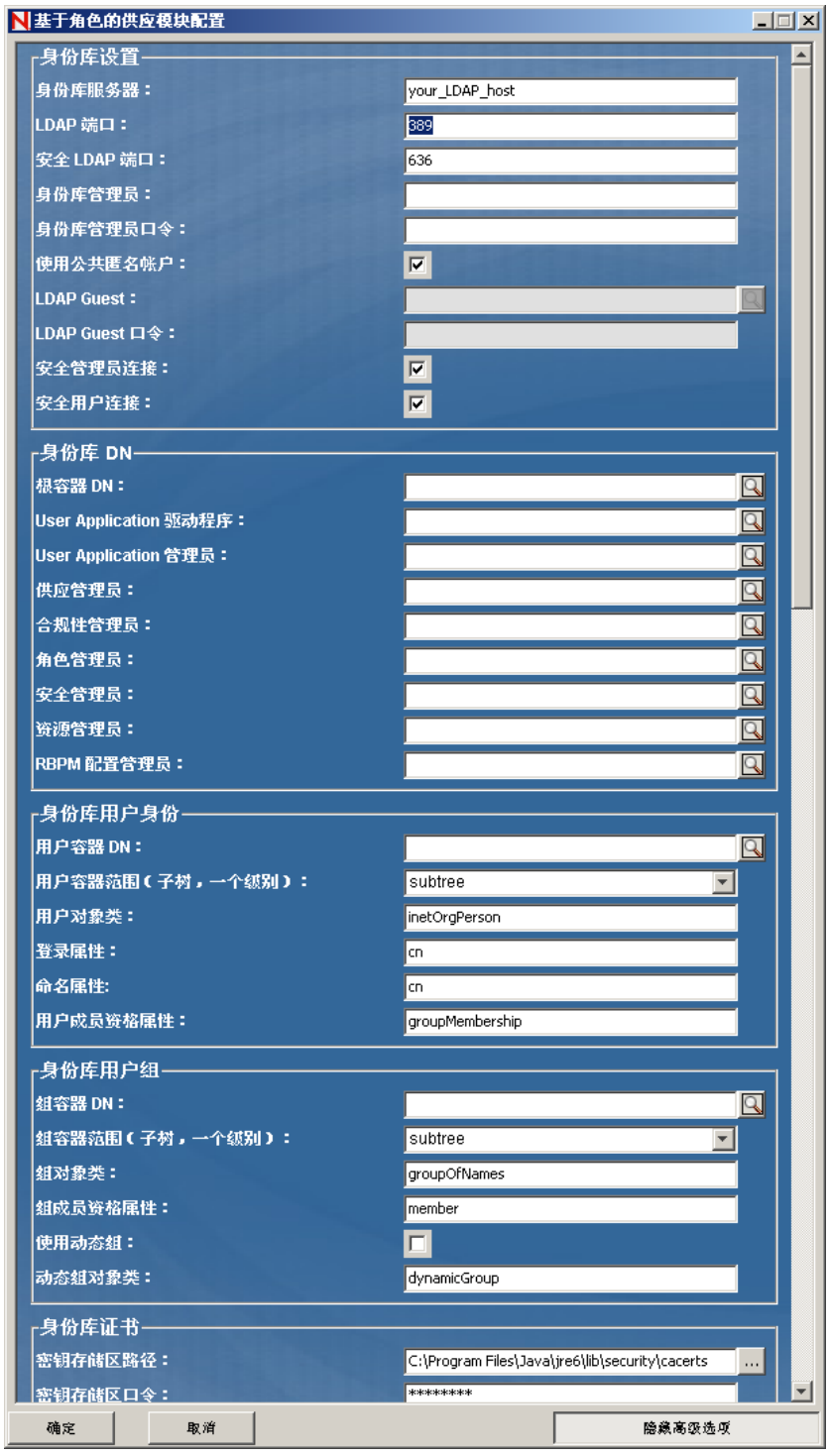
- 用户容器 DN
- 组容器 DN

安装程序将调用 “User Application 管理员 ” 字段中的值并将其应用于以下值：

- 供应管理员
- 合规性管理员
- 角色管理员
- 安全管理员

- 资源管理员
- RBPM 配置管理员

如果要能显式指定这些值，可以单击*显示高级选项*按钮并进行更改：



6 使用以下信息完成安装。

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，参见参数说明中的注释。 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 103 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。

5.1.1 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。

5.2 测试安装

1 启动数据库。有关指导，请参见数据库文档。

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 是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，并参见第 9.8 节 “ 查错 ” （第 101 页）。

在 WebSphere 上安装 User Application

6

本节说明如何在 WebSphere 应用程序服务器上通过使用安装程序的图形用户界面版本为基于角色的供应模块安装 User Application。

以非根用户身份运行安装程序。

数据迁移 有关迁移的信息，请参见 《*User Application：迁移指南* (http://www.novell.com/documentation/idmrbpm37/index.html)》。

6.1 安装和配置 User Application WAR

注释：对于 WebSphere 6.1，安装程序需要使用 IBM 提供的 Java 2 Platform Standard Edition Development Kit 版本 1.5 JDK。对于 WebSphere 7.0，安装程序需要使用 IBM 提供的 1.6 JDK。如果使用其他版本，安装过程将无法成功配置 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 使用 IBM Java 环境起动安装程序，如下所示：

Solaris

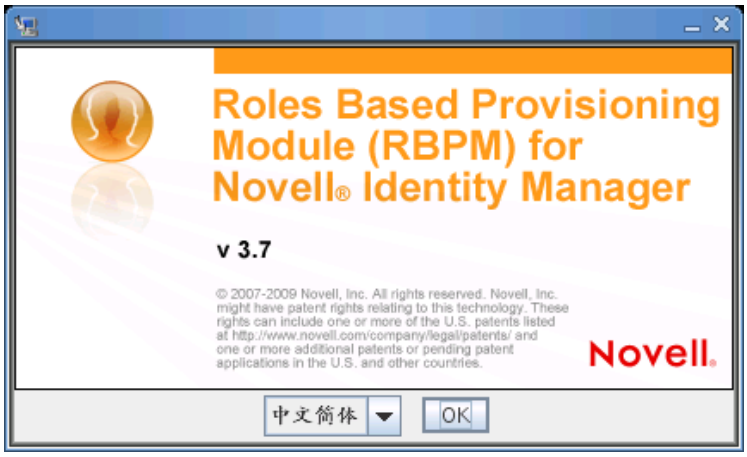
```
$ /opt/WS/IBM/WebSphere/AppServer/java/bin/java -jar IdmUserApp.jar
```

Windows

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

重要：对于 WebSphere，必须使用应用了无限制策略文件的 IBM JDK。如无上述无限制策略文件，则会发生一个错误，即 “ 非法密钥大小 ”。出现此问题的根本原因是缺少无限制策略文件，因此请确保使用正确的 IBM JDK。

当安装程序起动时，系统将提示您选择语言。



3 使用以下信息选择语言，确认许可协议，并选择应用程序服务器平台：

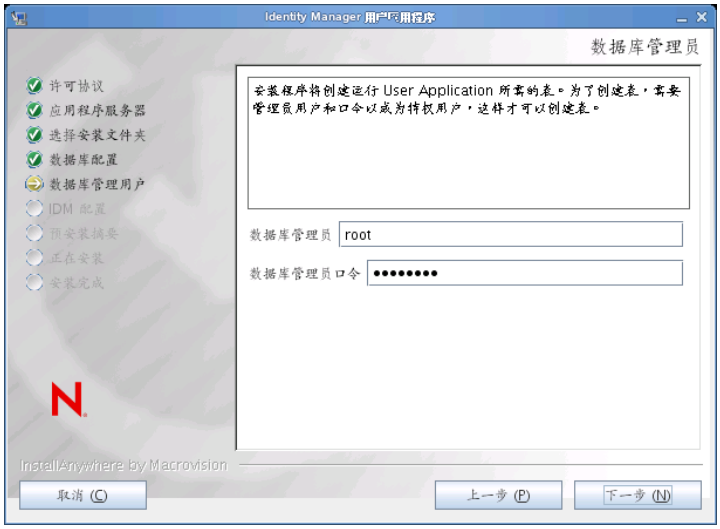
安装屏幕	说明
Novell Identity Manager 基于角色的供应模块 (RBPM)	选择安装程序的语言。默认为英语。
许可证协议	阅读许可证协议，然后选择*我接受本许可证协议的条款*。
应用程序服务器平台	选择 *WebSphere*。 如果 User Application WAR 文件所在的目录不同于安装程序，安装程序将提示提供 WAR 的路径。 如果 WAR 在默认位置，可以单击*恢复默认文件夹*。或者，要指定 WAR 文件的位置，单击*选择*并选择某个位置。 在 WebSphere 上进行安装时，需要使用 IBM Java 环境起动安装程序。如果选择 WebSphere 作为应用程序服务器且不使用 IBM Java 来起动安装，您将看到一条弹出式错误讯息，并且安装将终止： 

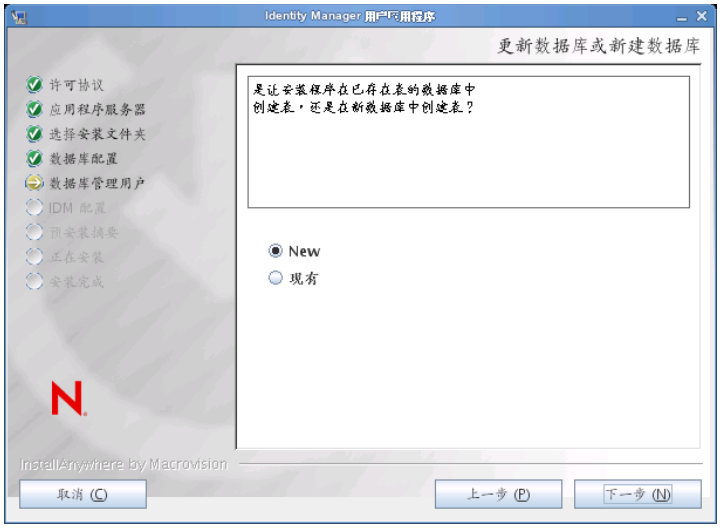
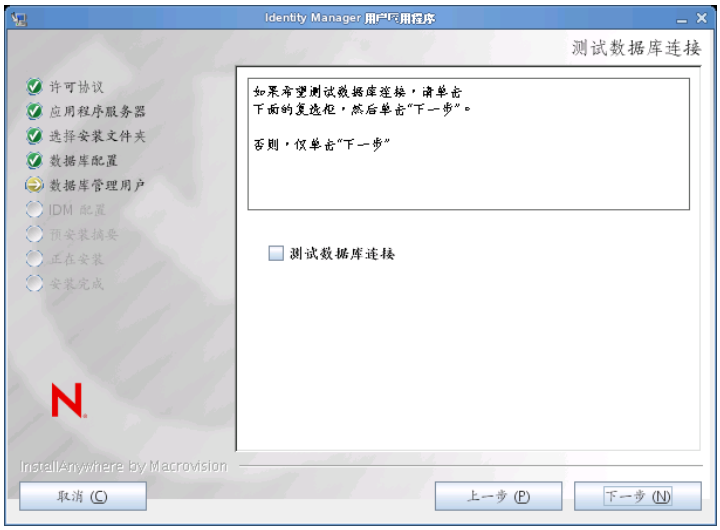
4 使用以下信息选择安装类型，选择安装文件夹，并配置数据库：

安装屏幕	说明
安装类型	*基于角色的供应*：选择此选项来安装基于角色的供应模块。这是此版本支持的唯一安装类型。
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。对于 WebSphere，选项如下： ◆ MySQL ◆ Oracle （仅支持 Oracle 10g 和 11g ；不再支持 Oracle 9i） ◆ Microsoft SQL Server ◆ IBM DB2 （仅支持版本 9.5 ；不再支持版本 9.1）
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。 

安装屏幕	说明

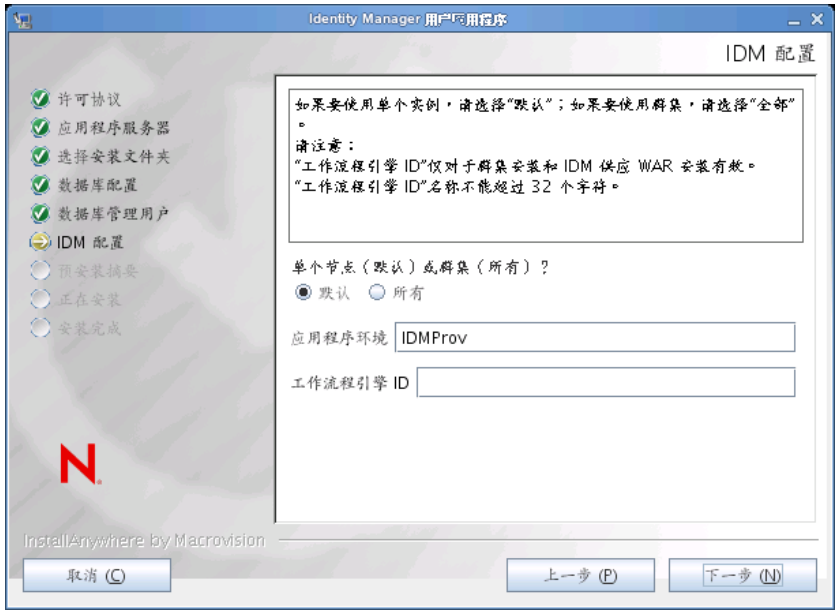
数据库用户名和口令	*数据库名称*（或 SID）：对于 MySQL、 MS SQL Server 或 PostgreSQL，请提供预配置数据库的名称。对于 Oracle，请提供以前创建的 Oracle 系统标识符 (SID)。对于群集，对其中每个成员指定相同的数据库名称或 SID。
	
	*数据库用户*名：指定数据库的用户。对于群集，对其中每个成员指定相同的数据库用户。
	
	数据库口令：指定数据库的口令。对于群集，对其中每个成员指定相同的数据库口令。
	
	数据库驱动程序 JAR 文件：为数据库服务器提供瘦客户端 JAR。此项是必需的。
	
	重要：*数据库驱动程序 JAR 文件*字段的浏览按钮允许您选择一个 (1) JAR。对于 DB2，必须提供两个 (2) JAR：
	◆ db2jcc.jar
	◆ db2jcc_license_cu.jar
	
	因此，可以选择一个 JAR，但应使用对于正在运行安装程序的操作系统而言正确的文件分隔符手动输入第二个 JAR。或者，可以手动输入上述两项。
	
	例如，在 Windows 上：
	
	`c:\db2jars\db2jcc.jar;c:\db2jars\db2jcc_license_cu.jar`
	
	例如，在 Solaris 和 Linux 上：
	
	`/home/lab/db2jars/db2jcc.jar:/home/lab/db2jcc_license_cu.jar`
	
	 

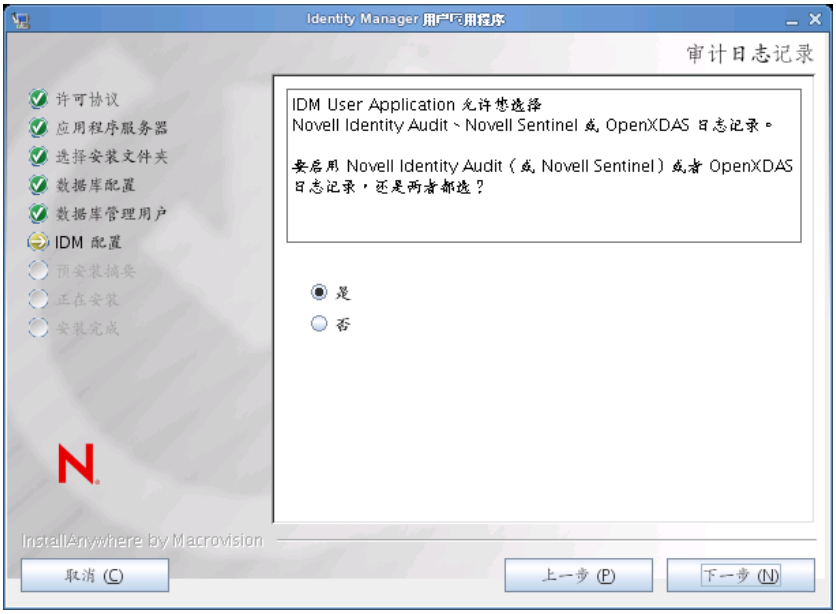
安装屏幕	说明
SQL 输出文件	在此版本中，可在 User Application 安装期间而不是在应用程序服务器启动时创建数据库表 （如同在先前版本中）。 “SQL 输出文件 ” 屏幕提供创建纲要文件的选项，数据库管理员可使用此选项来创建表，而不是让安装程序创建表。 如果要生成纲要文件，请选中*将 SQL 写入文件*复选框，并在*纲要输出文件*字段中提供文件名。 
数据库管理员	此屏幕将用 “ 数据库用户名和口令 ” 页面中的同一用户名和口令进行预填充。如果先前指定的数据库用户不具有在数据库服务器中创建表的足够许可权限，则需要输入具有必要权限的其他用户 ID。 

安装屏幕	说明
更新数据库或新建数据库	如果要使用的数据库是新的或空的，请选择*新建*按钮。如果数据库是先前安装中的现有数据库，请选择*现有*按钮。 
测试数据库连接	要确认在先前屏幕中提供的信息是否正确，可以选中*测试数据库连接*复选框来测试数据库连接： 

5 使用以下信息配置 Java 和 IDM，以及审计设置和安全性。

安装屏幕	说明
Java 安装	指定 Java 安装根文件夹。 Java 安装根据 JAVA_HOME 环境变量提供 Java 路径，并提供用于更正此路径的选项：  此时，安装程序会验证选定的 Java 对于选定的应用程序服务器而言是否正确。此外，安装程序还会验证它是否能写入所指定的 JRE 中的 cacerts。

安装屏幕	说明
IDM 配置	选择应用程序服务器配置的类型： ◆ 如果此安装位于不属于群集的单独节点，则选择*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。 ◆ 如果此安装是群集中的一部分，则选择*全部*。 *应用程序环境*：应用程序服务器配置的名称、应用程序 WAR 文件的名称，以及 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。 

安装屏幕	说明
Audit 日志记录	要启用日志记录，请单击*是*。要禁用日志记录，请单击*否*。  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 Identity Audit 或 Novell Sentinel*：启用适用于 User Application 的 Novell® Audit Logging。 ◆ *OpenXDAS*：事件将记录到 OpenXDAS 日志记录服务器中。 有关设置日志记录的更多信息，请参见 《*User Application：管理指南*》。 

安装屏幕	说明
Novell Audit	*服务器*：如果启用日志记录，请指定服务器的主机名或 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 9.1 节 “ 记录主密钥 ”（第 97 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。

6 单击 *下一步*以显示 “ 基于角色的供应模块配置 ” 面板。（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 27 页）中所述的步骤。）

“ 基于角色的供应模块配置 ” 面板的默认视图显示以下六个字段：

安装程序将调用 “ 根容器 DN” 中的值并将其应用于以下值：

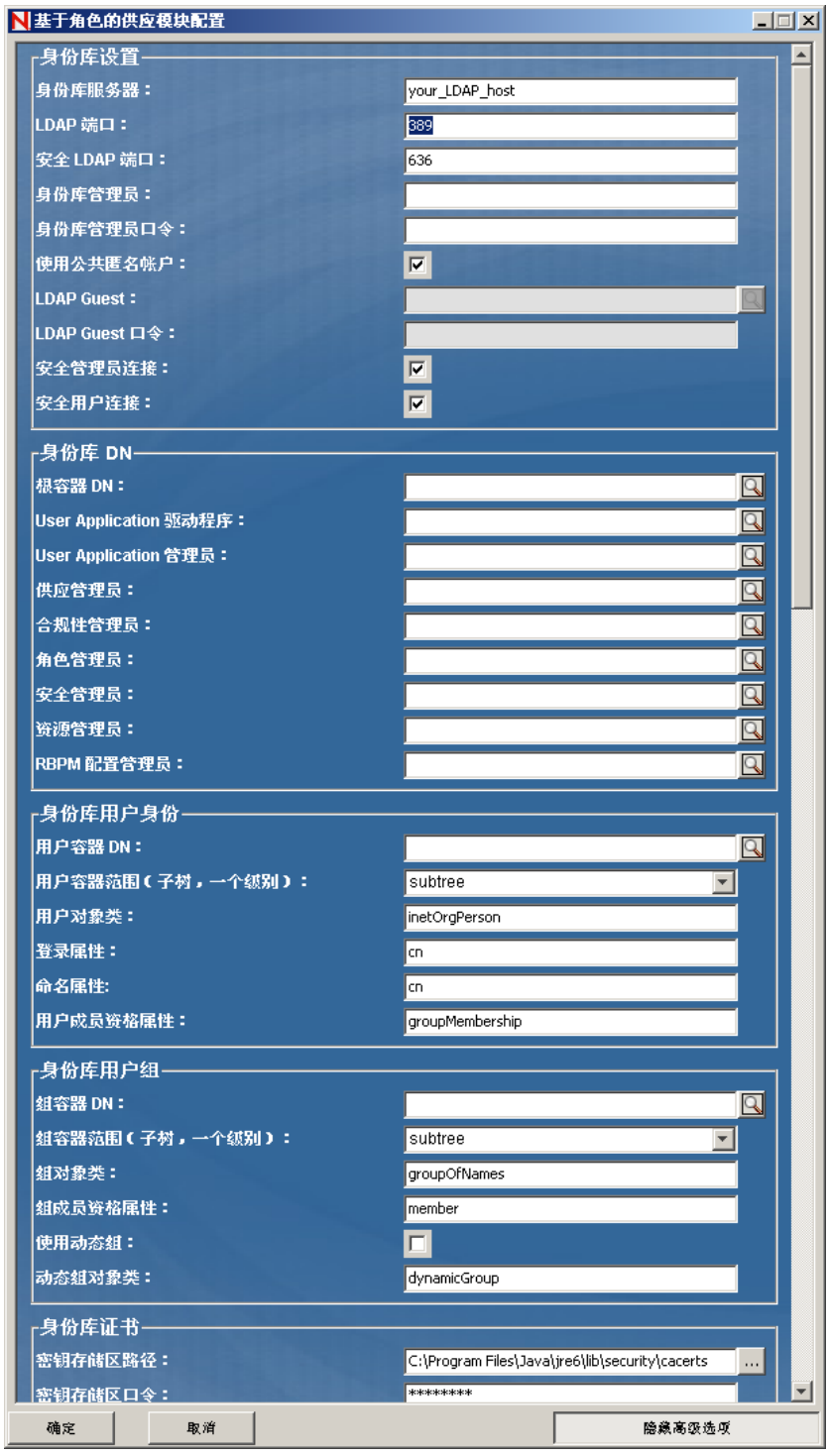
- 用户容器 DN
- 组容器 DN

安装程序将调用 “User Application 管理员 ” 字段中的值并将其应用于以下值：

- 供应管理员
- 合规性管理员
- 角色管理员
- 安全管理员

- 资源管理员
- RBPM 配置管理员

如果要能显式指定这些值，可以单击*显示高级选项*按钮并进行更改：



7 使用以下信息完成安装。

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，参见参数说明中的注释。 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 103 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。

6.1.1 查看安装日志文件

如果安装成功完成，没有错误，请继续第 6.2.1 节 “ 添加 User Application 配置文件和 JVM 系统属性 ”（第 70 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。

6.2 配置 WebSphere 环境

- 第 6.2.1 节 “ 添加 User Application 配置文件和 JVM 系统属性 ”（第 70 页）
- 第 6.2.2 节 “ 将 eDirectory 可信根导入 WebSphere 密钥储存区 ”（第 71 页）

6.2.1 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。

6.2.2 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 71 页）) 或通过命令行 (通过命令行导入证书 （第 72 页）) 执行此操作。

3 导入证书后，继续执行第 6.3 节 “ 部署 WAR 文件 ” （第 72 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。

6.3 部署 WAR 文件

使用 WebSphere 部署工具部署 WAR 文件。

6.3.1 WebSphere 6.1 的其他配置

如果您使用的是 WebSphere 6.1，则需要在部署 WAR 后更新 ibm-web-ext.xmi 文件。在部署 WAR 后，您需要在 ibm-web-ext.xmi 文件中添加类似如下的项：

```
<jspAttributes xmi:id="JSPAttribute_3" name="jdkSourceLevel" value="15"/>
```

名称必须为 jdkSourceLevel，值必须为 15。对于 JSPAttribute ID，则需要使用 _3 或以上值。有关更多信息，请参见以下链接：

- *http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.express.doc/info/exp/ae/tweb_jspengine.html* (http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.express.doc/info/exp/ae/tweb_jspengine.html)
- *http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.express.doc/info/exp/ae/rweb_jspengine.html* (http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.express.doc/info/exp/ae/rweb_jspengine.html)

完成 WAR 的部署后，请执行以下步骤：

1. 停止 WebSphere 应用程序服务器。
2. 按上述方法修改 ibm-web-ext.xmi 文件。文件位置应在 IBM 文档中有所指定。例如，文件可能位于以下位置：

   ```
   /opt/IBM/WebSphere/AppServer/profiles/AppSrv01/installedApps/
   MyNode01Cell/IDMProv_war.ear/IDMProv.war/WEB-INF
   ```

3. 重启动 WebSphere 应用程序服务器。

6.4 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

在 WebLogic 上安装 User Application

7

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

- 第 7.1 节 “WebLogic 安装核对清单 ”（第 75 页）
- 第 7.2 节 “ 安装和配置 User Application WAR”（第 75 页）
- 第 7.3 节 “ 准备 WebLogic 环境 ”（第 86 页）
- 第 7.4 节 “ 部署 User Application WAR”（第 88 页）
- 第 7.5 节 “ 访问 User Application”（第 88 页）

要了解使用非图形用户界面进行安装的信息，请参阅第 8 章 “ 从控制台或使用单条命令进行安装 ”（第 89 页）。

以非根用户身份运行安装程序。

数据迁移 有关迁移的信息，请参见 《*User Application：迁移指南* (http://www.novell.com/documentation/idmrbpm37/index.html)》。

7.1 WebLogic 安装核对清单

- ❑ 安装 WebLogic。

  按照 WebLogic 文档中的安装指导执行操作。
- ❑ 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 7.2 节 “ 安装和配置 User Application WAR”（第 75 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 7.3 节 “ 准备 WebLogic 环境 ”（第 86 页）。
- ❑ 部署 WAR。

  请参阅第 7.4 节 “ 部署 User Application WAR”（第 88 页）。

7.2 安装和配置 User Application WAR

注释：对于 WebLogic 10.3，安装程序需要使用 JRockit 提供的 Java 2 Platform Standard Edition Development Kit 版本 1.6 JDK。如果使用其他版本，安装过程将无法成功配置 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. 使用 JRockit Java 环境，通过命令行起动适用于您的平台的安装程序：

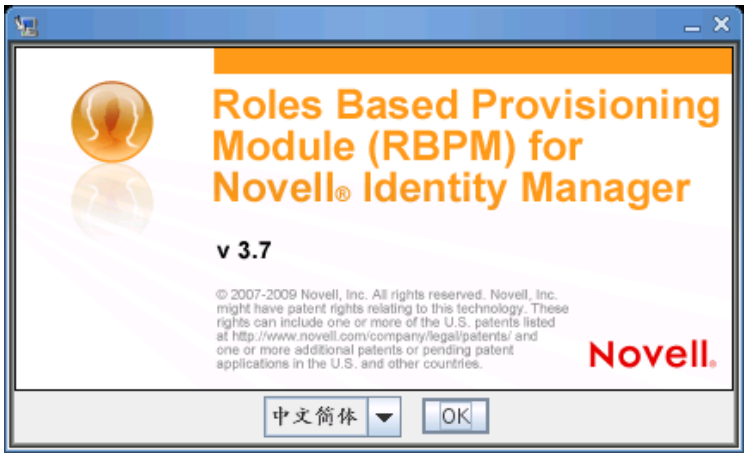
   Solaris

   ```
   $ /opt/WL/bea/jrockit_160_05/bin/java -jar IdmUserApp.jar
   ```

Windows

```
C:\WL\bea\jrockit_160_05\bin\java -jar IdmUserApp.jar
```

当安装程序起动时，系统将提示您选择语言。



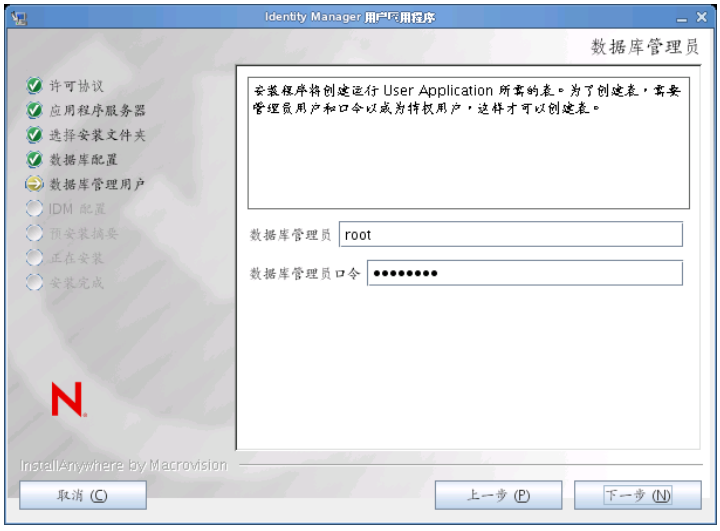
3 使用以下信息选择语言，确认许可协议，并选择应用程序服务器平台：

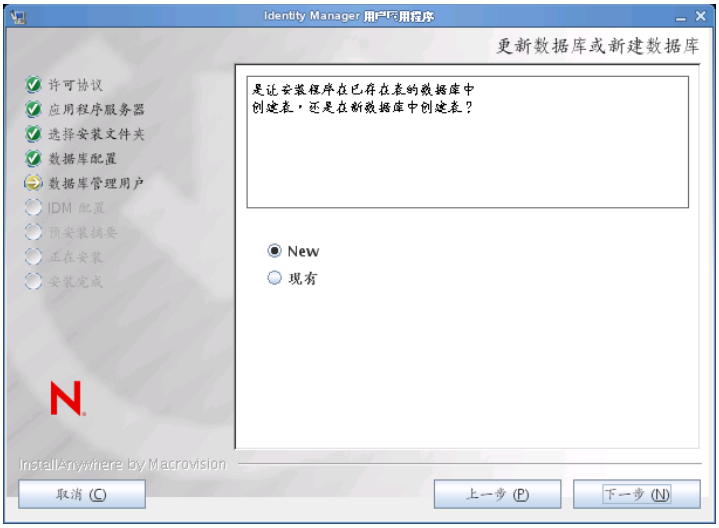
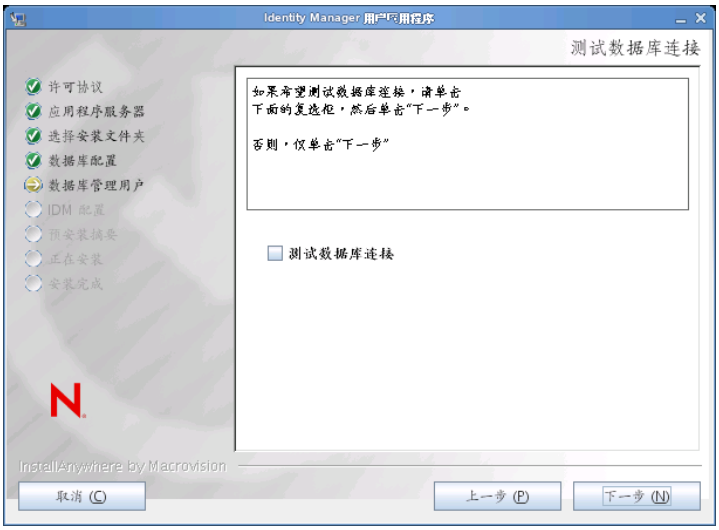
安装屏幕	说明
Novell Identity Manager 基于角色的供应模块 (RBPM)	选择安装程序的语言。默认为英语。
许可证协议	阅读许可证协议，然后选择 *我接受本许可证协议的条款*。
应用程序服务器平台	选择 *WebLogic*。 如果 User Application WAR 文件所在的目录不同于安装程序，安装程序将提示提供 WAR 的路径。 如果 WAR 在默认位置，可以单击 *恢复默认文件夹*。或者，要指定 WAR 文件的位置，单击 *选择*并选择某个位置。 在 WebLogic 上进行安装时，需要使用 BEA Java 环境 (jrockit) 起动安装程序。如果选择 WebLogic 作为应用程序服务器且不使用 jrockit 来起动安装，您将看到一条弹出式错误讯息，并且安装将终止： 

4 使用以下信息选择安装类型，选择安装文件夹，并配置数据库：

安装屏幕	说明
安装类型	*基于角色的供应*：选择此选项来安装基于角色的供应模块。这是此版本支持的唯一安装类型。
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。对于 WebLogic，选项如下： ◆ Oracle （仅支持 Oracle 10g 和 11g ；不再支持 Oracle 9i） ◆ Microsoft 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。 

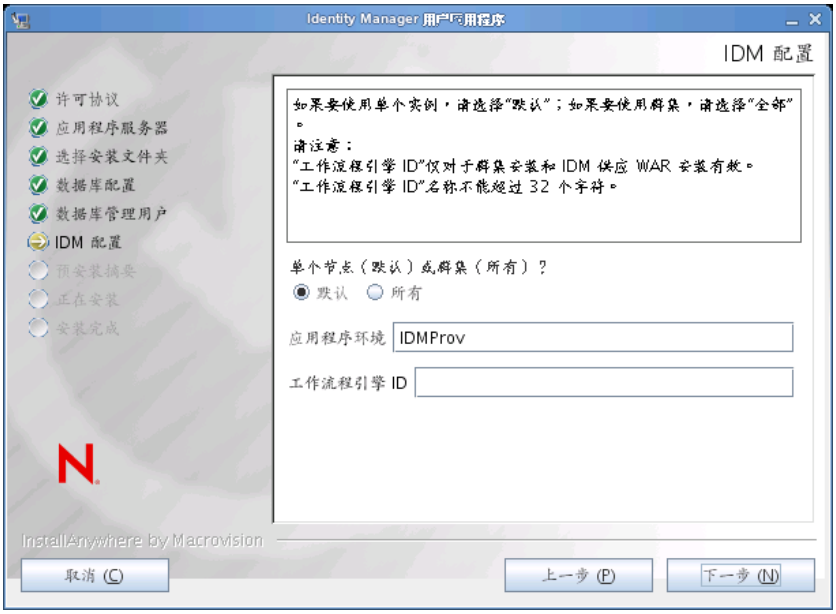
安装屏幕	说明
数据库用户名和口令	*数据库名称*（或 SID）：对于 MySQL、 MS SQL Server 或 PostgreSQL，请提供预配置数据库的名称。对于 Oracle，请提供以前创建的 Oracle 系统标识符 (SID)。对于群集，对其中每个成员指定相同的数据库名称或 SID。 *数据库用户*名：指定数据库的用户。对于群集，对其中每个成员指定相同的数据库用户。 *数据库口令*：指定数据库的口令。对于群集，对其中每个成员指定相同的数据库口令。 *数据库驱动程序 JAR 文件*：为数据库服务器提供瘦客户端 JAR。此项是必需的。 

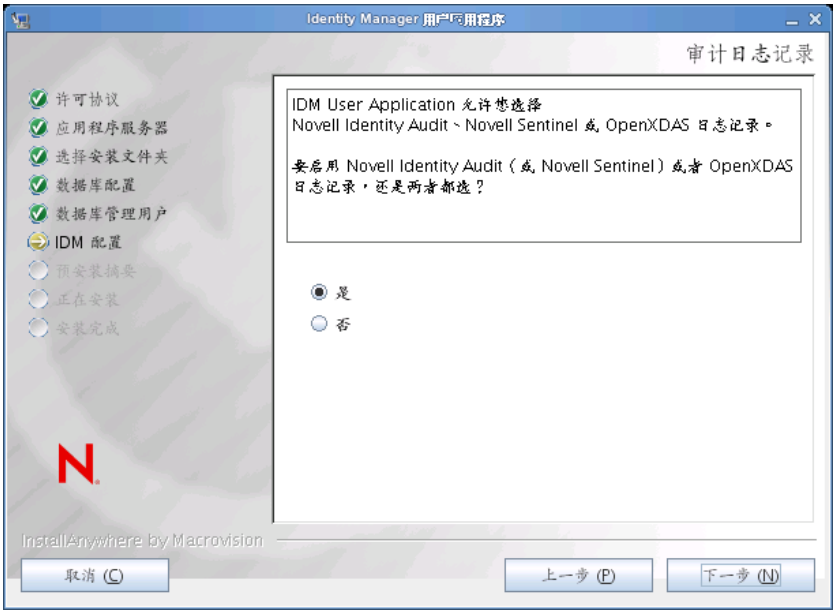
安装屏幕	说明
SQL 输出文件	在此版本中，可在 User Application 安装期间而不是在应用程序服务器启动时创建数据库表 （如同在先前版本中）。 “SQL 输出文件 ” 屏幕提供创建纲要文件的选项，数据库管理员可使用此选项来创建表，而不是让安装程序创建表。 如果要生成纲要文件，请选中*将 SQL 写入文件*复选框，并在*纲要输出文件*字段中提供文件名。 
数据库管理员	此屏幕将用 “ 数据库用户名和口令 ” 页面中的同一用户名和口令进行预填充。如果先前指定的数据库用户不具有在数据库服务器中创建表的足够许可权限，则需要输入具有必要权限的其他用户 ID。 

安装屏幕	说明
更新数据库或新建数据库	如果要使用的数据库是新的或空的，请选择*新建*按钮。如果数据库是先前安装中的现有数据库，请选择*现有*按钮。 
测试数据库连接	要确认在先前屏幕中提供的信息是否正确，可以选中*测试数据库连接*复选框来测试数据库连接： 

5 使用以下信息配置 Java 和 IDM，以及审计设置和安全性。

安装屏幕	说明
Java 安装	指定 Java 安装根文件夹。 Java 安装根据 JAVA_HOME 环境变量提供 Java 路径，并提供用于更正此路径的选项：  此时，安装程序会验证选定的 Java 对于选定的应用程序服务器而言是否正确。此外，安装程序还会验证它是否能写入所指定的 JRE 中的 cacerts。

安装屏幕	说明
IDM 配置	选择应用程序服务器配置的类型： ◆ 如果此安装位于不属于群集的单独节点，则选择*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。 ◆ 如果此安装是群集中的一部分，则选择*全部*。 *应用程序环境*：应用程序服务器配置的名称、应用程序 WAR 文件的名称，以及 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。 

安装屏幕	说明
Audit 日志记录	要启用日志记录，请单击*是*。要禁用日志记录，请单击*否*。  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 Identity Audit 或 Novell Sentinel*：通过适用于 User Application 的 Novell 审计客户端启用日志记录。 ◆ *OpenXDAS*：事件将记录到 OpenXDAS 日志记录服务器中。 有关设置日志记录的更多信息，请参见 《*User Application：管理指南*》。 

安装屏幕	说明
Novell Audit	*服务器*：如果启用日志记录，请指定服务器的主机名或 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 9.1 节 “ 记录主密钥 ”（第 97 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。

6 单击 *下一步*以显示 “ 基于角色的供应模块配置 ” 面板。（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 27 页）中所述的步骤。）

“ 基于角色的供应模块配置 ” 面板的默认视图显示以下六个字段：

安装程序将调用 “ 根容器 DN” 中的值并将其应用于以下值：

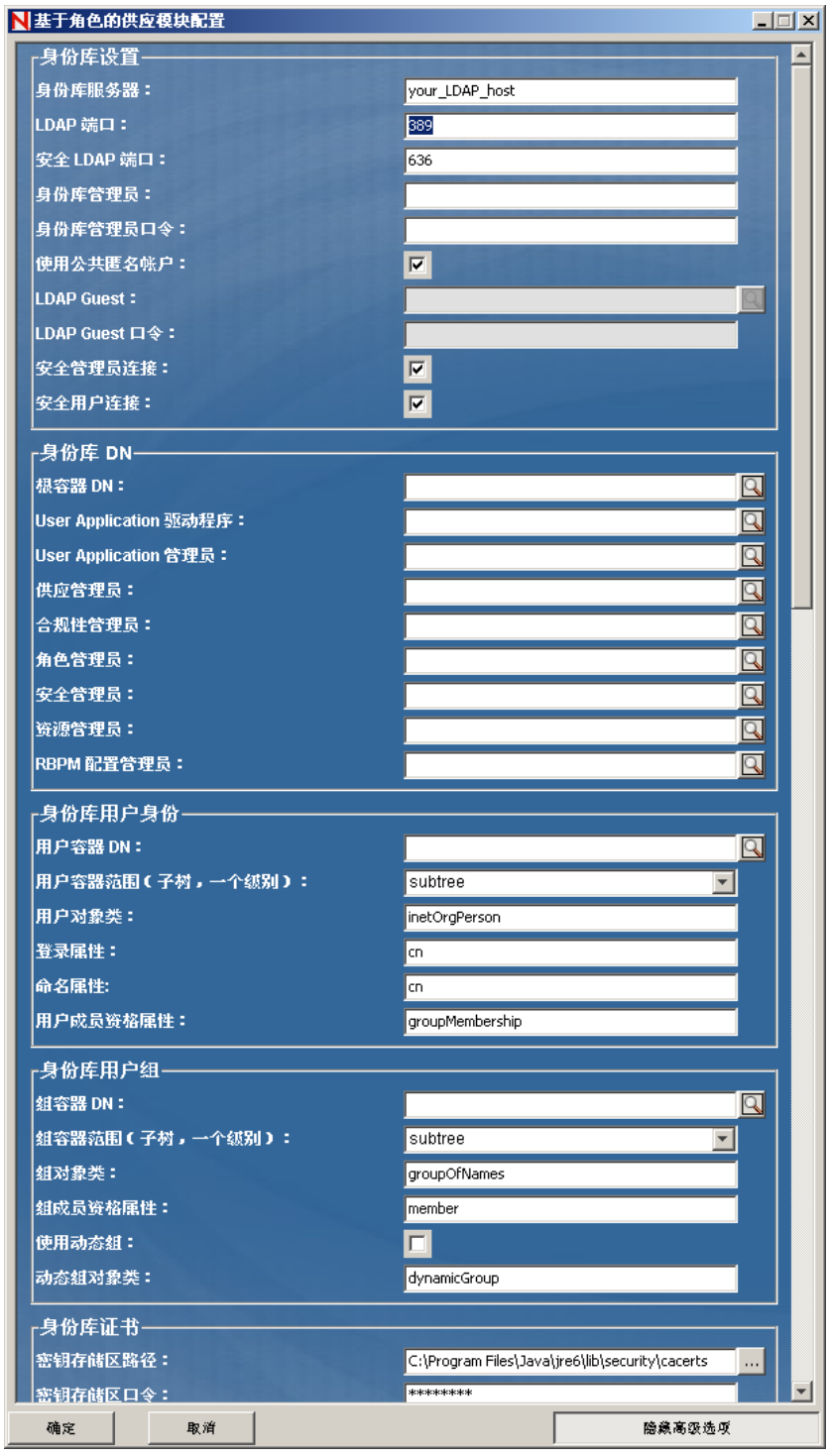
- 用户容器 DN
- 组容器 DN

安装程序将调用 “User Application 管理员 ” 字段中的值并将其应用于以下值：

- 供应管理员
- 合规性管理员
- 角色管理员
- 安全管理员

- 资源管理员
- RBPM 配置管理员

如果要能显式指定这些值，可以单击*显示高级选项*按钮并进行更改：



7 使用以下信息完成安装。

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，参见参数说明中的注释。 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 103 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。

7.2.1 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。

7.3 准备 WebLogic 环境

7.3.1 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。
- ❑ 将 antlr-2.7.6.jar 和 log4j.jar 从 User Application 安装目录复制到域 lib 文件夹 （例如，c:\bea\user_projects\domains\idm\lib\）。另请将 commons-logging.jar 从 c:\bea\tools\eclipse 文件夹复制到域 lib 文件夹。
- ❑ 创建数据源。

  遵循 WebLogic 文档中创建数据源的指导。

  请注意，无论您在创建 User Application WAR 时为数据源或数据库指定的名称如何，数据源的 JNDI 名称都必须为 jdbc/IDMUADataSource。

7.3.2 指定 RBPM 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==<directory-path>：指定包含 sys-configuration.xml 文件的文件夹（不是文件本身）。
- -Didmuserapp.logging.config.dir==<directory-path>：指定包含 idmuserapp_logging.xml 文件的文件夹 （不是文件本身）。

例如，在 Windows 上：

```
set JAVA_OPTIONS=-Dextend.local.config.dir=c:\novell\idm
set JAVA_OPTIONS=%JAVA_OPTIONS% -
Didmuserapp.logging.config.dir=c:\novell\idm
```

4 设置环境变量 EXT_PRE_CLASSPATH 以指向 antlr.jar，以及 log4j.jar 和 commons-logging.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;C:\bea\user_projects\domain\base_domain\lib\log4j.jar;C:\be
a\user_projects\domains\base_domain\lib\commons-logging.jar
```

例如，在 Linux 上：

```
export EXT_PRE_CLASSPATH=/opt/bea/user_projects/domains/base_domain/
lib/antlr-
2.7.6.jar;C:\bea\user_projects\domain\base_domain\lib\log4j.jar;C:\be
a\user_projects\domains\base_domain\lib\commons-logging.jar
```

5 保存并退出该文件。

配置后的实用程序也会使用 XML 文件；因此，需要按以下方式编辑 configupdate.bat 或 configupdate.sh 文件：

1 打开 configupdate.bat 或 configupdate.sh。

2 查找以下行：

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

3 更新现有行以包括：

```
-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。如果未使用在安装期间指定的相同 JDK，则必须在 WAR 上运行 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。

configupdate 实用程序中的身份库证书值必须指向以下位置：

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

7.3.3 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. 在 <*WLHome*>\user_projects\domains\idm\config\ 文件夹中打开 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。

7.4 部署 User Application WAR

- 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。

7.5 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

8

本部分说明了可用来代替第 5 章 “ 在 JBoss 上安装 User Application”（第 45 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 8.1 节 “ 从控制台安装 User Application”（第 89 页）
- 第 8.2 节 “ 使用单个命令安装 User Application”（第 89 页）

8.1 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 （第 17 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 5 章 “ 在 JBoss 上安装 User Application”（第 45 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 103 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 9 章 “ 安装后任务 ”（第 97 页）。

8.2 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 （第 17 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，请参见 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，请参见表 8-1。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 /*yourdirectorypath*/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 8-1 *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 4.1 节 “ 在 iManager 中创建 User Application 驱动程序 ”（第 41 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`
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、Novell 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限。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。

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_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。
NOVL_CONFIG_KEYSTOREPATH=	eDirectory 证书：密钥储存区路径。必需。 指定应用程序服务器当前正在使用的 JRE 密钥储存区 (cacerts) 文件的完整路径。 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。

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_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。
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。

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_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 *False* 以使用默认的内部口令管理功能。 /jsps/pwdmgt/ForgotPassword.jsp （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。 在外部或内部口令管理 WAR 中指定 “ 忘记口令 ” 功能页面 ForgotPassword.jsp 的 URL。或者接受默认的内部口令管理 WAR。有关细节，请参阅配置外部忘记口令管理 （第 99 页）。
NOVL_CONFIG_EXTPWDWARRTNPATH=	口令管理：忘记口令返回链接。 指定 “ 忘记口令返回链接 ” 供用户在执行完忘记口令操作后进行单击。
NOVL_CONFIG_FORGOTWEBSERVICEURL=	口令管理：忘记口令 Web Service URL。 这是外部忘记口令 WAR 用来回拨 User Application 以执行核心忘记口令功能的 URL。此 URL 的格式为： `https://<idmhost>:<sslport>/<idm>/pwdmgt/service`
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）。
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 特性 （比如 CN）。

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_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 特性。这不同于登录特性，登录特性仅在登录时使用，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 特性。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特性。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_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=	数字签名证书。
NOVL_CONFIG_AUDITKEYFILEPATH=	数字签名私用密钥文件的路径。
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*。

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_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。
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。
NOVL_DATABASE_NEW	指示数据库是新的还是现有的。如果是新数据库，则指定 *True*。如果是现有数据库，则指定 *False*。

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_RBPM_SEC_ADMINDN	安全管理员。 此角色为成员提供安全域内的所有功能。 安全管理员可以对安全域内的所有对象执行所有可能的操作。安全域允许安全管理员使用基于角色的供应模块配置所有域内所有对象的访问权限。安全管理员可以配置小组，还可以指派域管理员、委托管理员及其他安全管理员。
NOVL_RBPM_RESOURCE_ADMINDN	资源管理员。 此角色为成员提供资源域内的所有功能。资源管理员可以对资源域内的所有对象执行所有可能的操作。
NOVL_RBPM_CONFIG_ADMINDN	此角色为成员提供配置域内的所有功能。 RBPM 配置管理员可以对配置域内的所有对象执行所有可能的操作。 RBPM 配置管理员控制对基于角色的供应模块内的导航项目的访问。此外， RBPM 配置管理员还配置委托和代理服务、数字签名服务、供应用户界面及工作流程引擎。

安装后任务

9

本部分说明安装后任务。包括以下主题：

9.1 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。

9.2 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管理指南*》中，该节的标题为 “ 配置 User Application 环境 ”。
- 《*Novell IDM 基于角色的供应模块设计指南*》。

9.2.1 设置日志记录

要配置日志记录，请按照 《User Application：管理指南 (http://www.novell.com/documentation/idmrbpm37/index.html)》中 “ 设置日志记录 ” 一节中的指导执行操作。

9.3 配置 eDirectory

9.3.1 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 （如表 A-2 （第 105 页）中所述），或请参考 《*Novell eDirectory 管理指南* (http://www.novell.com/documentation)》获取有关使用引擎管理器创建索引的说明。

9.3.2 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。）

9.4 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 103 页）和表 8-1 （第 90 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。

9.5 配置外部忘记口令管理

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 9.5.1 节 “ 指定外部忘记口令管理 WAR”（第 100 页）
- 第 9.5.2 节 “ 指定内部口令 WAR”（第 100 页）
- 第 9.5.3 节 “ 测试外部忘记口令 WAR 配置 ”（第 100 页）
- 第 9.5.4 节 “ 在 JBoss 服务器间配置 SSL 通讯 ”（第 100 页）

9.5.1 指定外部忘记口令管理 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，例如 http://localhost:8080/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsp。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*，指定用户执行完忘记口令过程后将显示的链接。用户单击此链接，即可重定向到指定的链接。

5 对于*忘记口令 Web Service URL*，提供 Web Service 的 URL，外部转发口令 WAR 使用此 URL 回拨 User Application。此 URL 的格式必须为：https://*<idmhost>*:*<sslport>*/*<idm>*/pwdmgt/service。

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。另请参见第 9.5.4 节 “ 在 JBoss 服务器间配置 SSL 通讯 ”（第 100 页）。

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。

9.5.2 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。

9.5.3 测试外部忘记口令 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 ” 页面，例如 http://localhost:8080/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsp。
- 在 “User Application 登录 ” 页上，单击*忘记口令*链接。

9.5.4 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*使用外部口令 WAR*，则必须配置部署 User Application WAR 和外部忘记口令管理 WAR 文件的 JBoss 服务器之间的 SSL 通讯。有关指导，请参阅 JBoss 文档。

9.6 更新忘记口令设置

安装后可以更改*忘记口令链接*、*忘记口令返回链接*和*忘记口令 Web Service URL* 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.jsp）
- *忘记口令返回链接*（例如：http://localhost/IDMProv）
- *忘记口令 Web Service URL*（例如：https://<*idmhost*>:<*sslport*>/<*idm*>/pwdmgt/service）

9.7 安全考虑因素

在安装过程中，安装程序会将日志文件写入安装目录。这些文件包含有关您的配置的信息。配置完您的环境后，应考虑删除这些日志文件或将其储存在安全位置。

在安装过程中，可以选择将数据库纲要写入文件。由于此文件包含有关数据库的描述性信息，因此在安装过程完成后应将其移至安全位置。

9.8 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 root 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	描述
身份库设置	*身份库服务器*	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`
	身份库管理员	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。
	身份库管理员口令	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。

设置类型	选项	描述
身份库 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。
	User Application 驱动程序 DN	必需。指定 User Application 驱动程序的判别名（如第 4.1 节“在 iManager 中创建 User Application 驱动程序”（第 41 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 管理员	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、 Novell 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限。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。

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	描述
身份库设置	*身份库服务器*	必需。为 LDAP 服务器指定主机名或 IP 地址。例如： myLDAPhost
	LDAP 端口	为 LDAP 服务器指定非安全端口。例如：389。
	安全 LDAP 端口	为 LDAP 服务器指定安全端口。例如：636。
	身份库管理员	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。
	身份库管理员口令	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。
	安全管理员连接	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	描述
身份库 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。
	User Application 驱动程序 DN	必需。指定 User Application 驱动程序的判别名（如第 4.1 节“在 iManager 中创建 User Application 驱动程序”（第 41 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 管理员	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限。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。
	供应管理员	供应管理员管理 User Application 所有可用的供应工作流程功能。在将用户指定为供应管理员之前，身份库中必须存在此用户。 要在部署 User Application 后更改此指派，请使用 User Application 中的*管理* > *管理员指派*页面。
	合规性管理员	合规性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管理员时，对此值的更改才会生效。如果存在有效的合规性管理员，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*管理* > *管理员指派*页面。
	角色管理员	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*管理* > *管理员指派*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	描述
	安全管理员	此角色为成员提供安全域内的所有功能。 安全管理员可以对安全域内的所有对象执行所有可能的操作。安全域允许安全管理员使用基于角色的供应模块配置所有域内所有对象的访问权限。安全管理员可以配置小组，还可以指派域管理员、委托管理员及其他安全管理员。 要在部署 User Application 后更改此指派，请使用 User Application 中的*管理* > *管理员指派*页面。
	资源管理员	此角色为成员提供资源域内的所有功能。资源管理员可以对资源域内的所有对象执行所有可能的操作。 要在部署 User Application 后更改此指派，请使用 User Application 中的*管理* > *管理员指派*页面。
	RBPM 配置管理员	此角色为成员提供配置域内的所有功能。RBPM 配置管理员可以对配置域内的所有对象执行所有可能的操作。 RBPM 配置管理员控制对基于角色的供应模块内的导航项目的访问。此外，RBPM 配置管理员还配置委托和代理服务、数字签名服务、供应用户界面及工作流程引擎。 要在部署 User Application 后更改此指派，请使用 User Application 中的*管理* > *管理员指派*页面。
身份库用户身份	*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）。
	登录特性	代表用户的登录名的 LDAP 特性 （比如 CN）。
	命名特性	用作查找用户或组时的标识符的 LDAP 特性。这不同于登录特性，登录特性仅在登录时使用，在用户 / 组搜索时不使用。
	用户成员资格特性	可选。代表用户的组成员资格的 LDAP 特性。不要在该名称中使用空格。

设置类型	选项	描述
身份库用户组	*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）。
	组成员资格特性	代表用户组成员资格的特性。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）。
身份库证书	*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	
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。
	密钥储存区类型 JKS	指示要使用的数字签名的类型。如果已选中此字段，则将指示可信储存区路径的类型是否为 JKS。
	密钥储存区类型 PKCS12	指示要使用的数字签名的类型。如果已选中此字段，则将指示可信储存区路径的类型是否为 PKCS12。
Novell Audit 数字签名和证书密钥		包含审计服务的数字签名密钥及证书。
	Novell Audit 数字签名证书	显示审计服务的数字签名证书。
	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。

设置类型	选项	描述
Access Manager 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。
电子邮件服务器配置	*通知模板主机*	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。
	通知模板端口	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。
	通知模板安全端口	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。
	通知模板协议	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。
	通知模板安全协议	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。
	SMTP 服务器名称：	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*、*忘记口令返回链接*和*忘记口令 Web Service URL* 的值。 如果未选择*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.jsp （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。在外部或内部口令管理 WAR 中指定 ForgotPassword.jsp 文件。
	忘记口令返回链接	指定*忘记口令返回链接*供用户在执行完忘记口令操作后进行单击。

设置类型	选项	描述
	忘记口令 Web Service URL	这是外部忘记口令 WAR 用来回拨 User Application 以执行核心忘记口令功能的 URL。此 URL 的格式为： `https://<idmhost>:<sslport>/<idm>/pwdmgt/service`
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。
	创建身份库索引	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 9.3.1 节 “ 在 eDirectory 中创建索引 ”（第 98 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。
	去除身份库索引	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。
	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。