

Novell Identity Manager 基于角色的供 应模块

3.6

www.novell.com

USER APPLICATION: 安装指南

2008 年 1 月 18 日

N

Novell®

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 \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/)。如果您未能获得任何必要的出口许可，Novell 对此不承担任何责任。

版权所有 © 2008 Novell, Inc. 保留所有权利。未经出版商的明确书面许可，不得复制、影印、传送此出版物的任何部分或将其储存在检索系统上。

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 \(http://www.novell.com/company/legal/patents/\)](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，请参见 [Novell 文档万维网页 \(http://www.novell.com/documentation\)](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 \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](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	7
1 概述	9
1.1 安装概述	9
1.2 关于安装程序	10
1.3 系统要求	10
2 安装的前提条件。	17
2.1 Java 开发工具包	17
2.2 安装 Identity Manager Metadirectory	18
2.3 安装 JBoss Application Server	18
2.3.1 安装 JBoss Application Server 和 MySQL 数据库	18
2.3.2 安装 JBoss Application Server 作为一项服务	21
2.4 安装 WebSphere Application Server	22
2.5 数据库	22
2.5.1 安装 MySQL	22
2.5.2 配置 MySQL 数据库	23
2.6 安全性先决条件	24
2.7 下载产品	24
2.8 安装 prerequisitefiles.zip 文件的内容	25
2.8.1 扩展基于角色的供应模块版本 3.6 的 eDirectory 纲要	25
2.8.2 为角色服务驱动程序复制 JAR 文件	26
2.8.3 复制角色服务驱动程序配置文件	26
2.8.4 复制 User Application 驱动程序配置文件	27
2.8.5 复制 dirxml.lsc 文件	27
2.9 为角色安装 iManager 图标	27
3 创建驱动程序	29
3.1 在 iManager 中创建 User Application 驱动程序	29
3.2 在 iManager 中创建角色服务驱动程序	33
4 在 JBoss 上使用 GUI 安装	35
4.1 运行安装程序 GUI	35
4.2 选择应用程序服务器平台	36
4.3 迁移数据库	37
4.4 指定 WAR 的位置	39
4.5 选择安装文件夹	39
4.6 选择数据库平台	40
4.7 指定数据库主机和端口	41
4.8 指定数据库名称和特权用户	42
4.9 指定 Java 根目录	43
4.10 选择应用程序服务器配置类型	44
4.11 指定 JBoss Application Server 设置	45
4.12 启用 Novell Audit 日志记录	46
4.13 指定主密钥	47

4.14	配置 User Application	49
4.15	使用口令 WAR	59
4.15.1	指定外部口令管理 WAR	59
4.15.2	指定内部口令 WAR	60
4.16	校验选项和安装	60
4.17	查看日志文件	60
5	从控制台或使用单条命令安装	61
5.1	从控制台安装 User Application	61
5.2	使用单个命令安装 User Application	61
6	在 WebSphere Application Server 上安装	69
6.1	起动安装程序 GUI	69
6.2	选择应用程序服务器平台	70
6.3	指定 WAR 的位置	71
6.4	选择安装文件夹	72
6.5	选择数据库平台	73
6.6	指定 Java 根目录	74
6.7	启用 Novell Audit 日志记录	75
6.8	指定主密钥	76
6.9	配置 User Application	78
6.10	校验选项和安装	89
6.11	查看日志文件	89
6.12	添加 User Application 配置文件和 JVM 系统属性	89
6.13	将 eDirectory 可信根导入 WebSphere 密钥存储区	90
6.13.1	通过 WebSphere 管理员控制台导入证书	90
6.13.2	通过命令行导入证书	91
6.14	部署 IDM WAR 文件	91
6.15	启动应用程序	92
6.16	访问 User Application 门户	92
7	安装后任务	93
7.1	记录主密钥	93
7.2	安装后配置	93
7.3	检查群集安装	93
7.4	在 JBoss 服务器间配置 SSL 通讯	94
7.5	访问外部口令 WAR	94
7.6	升级忘记口令设置	94
7.7	设置电子邮件通知	94
7.8	测试安装在 JBoss Application Server 上	95
7.9	设置供应小组和请求	95
7.10	在 eDirectory 中创建索引	96
7.11	安装后重置 IDM WAR 文件	96
7.12	查错	96

关于本指南

Novell® Identity Manager 基于角色的供应模块 3.6 由具有基于角色的供应的 Identity Manager User Application 组成。本指南说明了如何安装 Novell Identity Manager 基于角色的供应模块 3.6。包括以下几部分：

- ◆ 第 1 章 “概述”（第 9 页）
- ◆ 第 2 章 “安装的前提条件。”（第 17 页）
- ◆ 第 3 章 “创建驱动程序”（第 29 页）
- ◆ 第 4 章 “在 JBoss 上使用 GUI 安装”（第 35 页）
- ◆ 第 5 章 “从控制台或使用单条命令安装”（第 61 页）
- ◆ 第 6 章 “在 WebSphere Application Server 上安装”（第 69 页）
- ◆ 第 7 章 “安装后任务”（第 93 页）

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 \(http://www.novell.com/documentation/lg/dirxmldrivers/index.html\)](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) 用于表示 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。

本部分概述了安装并说明了系统要求。包括以下主题：

- ◆ 第 1.1 节 “安装概述”（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）

1.1 安装概述

Novell® Identity Manager 基于角色的供应模块 3.6 的安装过程安装支持角色的 User Application 和基于角色的供应模块。安装包括以下步骤：

- 1 如果您要迁移到 Identity Manager 基于角色的供应模块，请参考《*Identity Manager User Application: 迁移指南* (<http://www.novell.com/documentation/idmrbpm36/pdfdoc/migration/migration.pdf>)》。
- 2 确保符合系统要求。请参阅第 1.3 节 “系统要求”（第 10 页）。
- 3 安装 Identity Manager Metadirectory。有关指导，请参考《*Identity Manager 3.5.1 安装指南* (<http://www.novell.com/documentation/idm35/pdfdoc/install/install.pdf>)》。Identity Manager Metadirectory 服务器必须在创建所需驱动程序和安装 User Application 及基于角色的供应模块之前进行安装。
- 4 满足安装的先决条件。请参阅第 2 章 “安装的前提条件。”（第 17 页）。
- 5 在下载目录中，找到并解压缩 prerequisitefiles.zip 文件。手动安装或应用解压缩的文件。
- 6 如果使用 Designer 创建和配置驱动程序，请安装 Designer 2.1.1。请参阅 “安装 Designer。” (http://www.novell.com/documentation/designer21/admin_guide/index.html?page=/documentation/designer21/admin_guide/data/gsininstall.html)。
- 7 在 iManager 或 Designer 2.1.1 中创建 User Application 驱动程序。关于在 iManager 中创建驱动程序的指导位于第 3.1 节 “在 iManager 中创建 User Application 驱动程序”（第 29 页）。

安装 Novell Identity Manager User Application 和基于角色的供应模块之前，必须已经存在（但未打开）User Application 驱动程序。

- 8 在 iManager 或 Designer 2.1.1 中创建角色服务驱动程序。关于在 iManager 中创建驱动程序的指导位于第 3.2 节 “在 iManager 中创建角色服务驱动程序”（第 33 页）。

安装 Novell Identity Manager User Application 和基于角色的供应模块之前，必须已经存在（但未打开）角色服务驱动程序。

- 9 安装和配置 Novell Identity Manager User Application 及基于角色的供应模块。参见：
 - ◆ 第 4 章 “在 JBoss 上使用 GUI 安装”（第 35 页）
 - ◆ 第 5 章 “从控制台或使用单条命令安装”（第 61 页）
 - ◆ 第 6 章 “在 WebSphere Application Server 上安装”（第 69 页）

注释：如果使用 WebSphere*，则必须手动部署 WAR 文件。

- 10 执行安装后任务。

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*。该数据库存储 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 上必须手动部署 WAR。
- ◆ 根据需要启用 Novell Audit 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。

可以以下三种模式之一运行安装程序：

- ◆ 图形用户界面。请参阅第 4 章“在 JBoss 上使用 GUI 安装”（第 35 页）或第 6 章“在 WebSphere Application Server 上安装”（第 69 页）。
- ◆ 控制台（命令行）界面。请参阅第 5.1 节“从控制台安装 User Application”（第 61 页）。
- ◆ 静默安装。请参见第 5.2 节“使用单个命令安装 User Application”（第 61 页）。

1.3 系统要求

要使用 Novell Identity Manager 基于角色的供应模块 3.6，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	注释
Metadirectory 系统 (Identity Manager 3.5.1)	下列操作系统之一：	如果使用 Metadirectory 系统平台，将支持在实施中使用 VMware*。
<ul style="list-style-type: none"> ◆ Metadirectory 引擎 ◆ Novell Audit 代理 ◆ 服务驱动程序 ◆ Identity Manager 驱动程序 ◆ 实用程序 (包括应用程序工具和 Novell Audit 设置工具) 	<ul style="list-style-type: none"> ◆ Netware® 6.5 SP6 ◆ 带最新 Support Pack 的 Novell Open Enterprise Server (OES) 1.0 ◆ Novell Open Enterprise Server (OES) 2.0 ◆ 带最新 Service Pack 的 Windows* 2000 Server (32 位) ◆ 带最新 Service Pack 的 Windows Server 2003 (32 位) ◆ Linux Red Hat 3.0、4.0 或 5.0 ES 及 AS (同时支持 32 位和 64 位) ◆ 带最新 Support Pack 的 SUSE Linux Enterprise Server 9 和 10 (同时支持 32 位和 64 位) ◆ Solaris* 9 或 10 ◆ AIX* 5.2L, 版本 5.2 或 5.3 <p>以下 eDirectory™ 版本之一：</p> <ul style="list-style-type: none"> ◆ eDirectory 8.7.3.10 ◆ eDirectory 8.8.1 或 8.8.2 <p>Security Services 2.0.5 (NMAST™ 3.1.3)</p>	<p>此发行版中的所有 Identity Manager 软件组件都为 32 位，即使它们在 64 位处理器或 64 位操作系统上运行。除非另行指定，否则 OES、NetWare、Windows 和 Linux 平台 (Red Hat* 和 SUSE®) 支持以下所有 32 位模式的处理器：</p> <ul style="list-style-type: none"> ◆ Intel* x86-32 ◆ AMD* x86-32 ◆ Intel EM64T ◆ AMD Athlon64* 和 Opteron* <p>Identity Manager 支持 eDirectory 8.8 的以下功能：</p> <ul style="list-style-type: none"> ◆ 同一服务器上的多个 eDirectory 实例 ◆ 加密的属性 <p>eDirectory 8.8 支持 64 位 Red Hat Linux 4.0。</p> <p>可提供 Windows Server 2003 上的 64 位版的口令同步。</p> <p>安装 eDirectory 8.8 之前，请务必完全备份 eDirectory 数据库。eDirectory 8.8 将会升级数据库结构的某些部分，并且在完成升级过程后不允许数据库结构回滚。</p> <p>在超虚拟化模式下，当 Xen Virtual Machine (VM) 运行 SLES 10 以作为 guest 操作系统时，SUSE Linux Enterprise Server 10 上现在支持 Xen* 虚拟化。需要针对 SLES 10 的 Xen 增补程序 (请参见 TID # 3915180 (http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3915180&sliceId=SAL_Public&dialogID=52670386&stated=1%20%204926187))。</p>

必需的系统组件	系统要求	注释
基于万维网的管理服务器	<p>下列操作系统之一：</p> <ul style="list-style-type: none"> ◆ 带最新 Support Pack 的 NetWare 平台上的 Novell Open Enterprise Server (OES) 1.0 ◆ Novell Open Enterprise Server (OES) 2.0 ◆ 带最新 Support Pack 的 NetWare 6.5 ◆ 带最新 Service Pack 的 Windows 2000 Server (32 位) ◆ 带最新 Service Pack 的 Windows Server 2003 (32 位) ◆ Microsoft Windows Vista* ◆ Linux 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 Support Pack 的 Solaris* 9 或 10 ◆ 带最新 Support Pack 的 SUSE Linux Enterprise Server 9 或 10 (同时支持 32 位和 64 位) <p>通过 iManager 工作站支持操作系统：</p> <ul style="list-style-type: none"> ◆ 带最新 Service Pack 的 Windows 2000 Professional ◆ 带 SP2 的 Windows XP ◆ SUSE Linux Enterprise Desktop 10 ◆ SUSE Linux 10.1 <p>以下软件：</p> <ul style="list-style-type: none"> ◆ 带最新 Support Pack 和插件的 Novell iManager 2.6 或 2.7。 	<p>此发行版中的所有 Identity Manager 软件组件都为 32 位，即使它们在 64 位处理器或 64 位操作系统上运行。除非另有规定，否则 OES、NetWare、Windows 和 Linux 平台 (Red Hat 和 SUSE) 支持下列所有 32 位模式的处理器：</p> <ul style="list-style-type: none"> ◆ Intel x86 ◆ AMD x86 ◆ Intel EM64T ◆ AMD Athlon64 和 Opteron ◆ 浏览器支持由 iManager 2.6 确定。目前该列表包括： <ul style="list-style-type: none"> ◆ Internet Explorer* 6 SP1 和更高版本 ◆ Internet Explorer 7 ◆ Firefox* 2.0 及更高版本 ◆ 必须使用 iManager 配置向导或 Designer 实用程序将门户内容安装或部署到 eDirectory 中。 ◆ (Windows) 可以从 Novell 软件下载 (http://download.novell.com/index.jsp) 获取 Novell Client™ 4.9。 ◆ 使用 iManager 登录到其他树以管理远程 Identity Manager 服务器时，如果使用该远程服务器的名称而不是 IP 地址，则可能会遇到错误。 ◆ 口令同步代理只在 64 位 Windows 2003 上受支持。

必需的系统组件	系统要求	注释
安全日志记录服务	对于安全日志记录服务器，需要下列操作系统之一：	OES、NetWare、Windows 和 Linux 平台（Red Hat 和 SUSE）支持下列所有 32 位模式的处理器：
<ul style="list-style-type: none"> ◆ 安全日志记录服务器 ◆ 平台代理（客户机组件） ◆ Novell Audit 2.0.2 或 Sentinel™ 5.1.3 	<ul style="list-style-type: none"> ◆ 带最新 Support Pack 的 Novell Open Enterprise Server (OES) 1.0 或 2.0 ◆ 带最新 Support Pack 的 NetWare 6.5 ◆ 带最新 Service Pack 的 Windows 2000 Server（32 位） ◆ 带最新 Service Pack 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 Support Pack 的 Solaris 9 或 10 ◆ 带最新 Support Pack 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 Support Pack 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） 	<ul style="list-style-type: none"> ◆ Intel x86 ◆ AMD x86 ◆ Intel EM64T ◆ AMD Athlon64 和 Opteron
	对于平台代理，需要下列操作系统之一：	最低安全服务器要求包括：
	<ul style="list-style-type: none"> ◆ Novell Open Enterprise Server (OES) 1.0 SP1 或带最新 Support Pack ◆ 带最新 Support Pack 的 NetWare 6.5 ◆ Windows 2000 或 2000 Server、XP 或带最新 Service Pack 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） 	<ul style="list-style-type: none"> ◆ 单处理器、服务器级 PC（具有 Pentium II 400 MHz） ◆ 最少 40 MB 磁盘空间 ◆ 512 MB RAM
	带最新 Support Pack 和插件的 iManager 2.6 或 2.7	eDirectory Instrumentation 用于记录 eDirectory 事件，它支持下列 eDirectory 版本： <ul style="list-style-type: none"> ◆ eDirectory 8.7.3（NetWare、Windows、Linux 和 Solaris） ◆ 带最新 Support Pack 的 eDirectory 8.8 NetWare Instrumentation 允许记录 NetWare 事件，它支持下列 NetWare 版本： <ul style="list-style-type: none"> ◆ 带最新 Support Pack 的 NetWare 5.1 ◆ 带最新 Support Pack 的 NetWare 6.0 ◆ NetWare 6.5 或带最新 Support Pack 的 NetWare 6.5 ◆ 带最新 Support Pack 的 Novell Open Enterprise Server (OES)

必需的系统组件	系统要求	注释
User Application 应用程序服务器	<p>User Application 在 JBoss* 和 WebSphere 上运行，如下所述。</p> <p>以下各操作系统支持 JBoss 4.0.5 GA :</p> <ul style="list-style-type: none"> ◆ Novell Open Enterprise Server (OES) 1.0 SP2 或带最新 Support Pack - 仅 Linux ◆ SUSE Linux Enterprise Server 9 SP2 (包含在 OES 1.0 SP2 中) 或 10.1.x (64 位 JVM*) ◆ 带 SP4 的 Windows 2000 Server (32 位) ◆ 带 SP1 的 Windows 2003 Server (32 位) ◆ Solaris 10 Support Pack (日期为 6/06) <p>以下各操作系统支持 WebSphere 6.1 :</p> <ul style="list-style-type: none"> ◆ Solaris 10 (64 位) ◆ Windows 2003 SP1 <p>User Application 需要 JRE* 1.5.0_14。</p>	<p>SUSE Linux Enterprise Server 支持以下 32 位模式下的处理器 :</p> <ul style="list-style-type: none"> ◆ Intel x86 ◆ AMD x86 ◆ Intel EM64T ◆ AMD Athlon64 和 Opteron <p>采用以下处理器时，SUSE Linux Enterprise Server 将以 64 位模式运行 :</p> <ul style="list-style-type: none"> ◆ Intel EM64T ◆ AMD Athlon64 ◆ AMD Opteron ◆ Sun* SPARC* <p>现在，当 Xen 虚拟机 (VM) 在半虚拟模式下将 SLES 10 作为 guest 操作系统运行时，在 SUSE Linux Enterprise Server 10 上将支持 Xen* 虚拟化。需要针对 SLES 10 的 Xen 增补程序 (请参见 TID # (http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3915180&sliceId=SAL_Public&dialogID=52670386&stated=1%20%204926187))。</p>
User Application 浏览器	<p>User Application 同时支持 Firefox 和 Internet Explorer，如下所述。</p> <p>以下各操作系统支持 Firefox 2 :</p> <ul style="list-style-type: none"> ◆ 带 SP4 的 Windows 2000 Professional ◆ 带 SP2 的 Windows XP ◆ Red Hat Enterprise Linux WS 4.0 ◆ Novell Linux Desktop 9 ◆ SUSE Linux 10.1 ◆ SUSE Linux Enterprise Desktop 10 <p>以下各操作系统支持 Internet Explorer 7 :</p> <ul style="list-style-type: none"> ◆ 带 SP4 的 Windows 2000 Professional ◆ 带 SP2 的 Windows XP ◆ Windows Vista Enterprise V6 <p>以下各操作系统支持 Internet Explorer 6 SP1 :</p> <ul style="list-style-type: none"> ◆ 带 SP4 的 Windows 2000 Professional ◆ 带 SP2 的 Windows XP 	

必需的系统组件	系统要求	注释
User Application 的数据库服务器 <ul style="list-style-type: none"> ◆ MySQL ◆ Oracle ◆ MS SQL ◆ DB2 	JBoss 支持以下数据库 : <ul style="list-style-type: none"> ◆ MySQL V5.0.27 ◆ 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 : <ul style="list-style-type: none"> ◆ Oracle 10g R2 (10.2.0) ◆ MS SQL 2005 SP1 ◆ DB2 DV2 v9.1.0.0 	User Application 使用数据库来完成各项任务，如存储配置数据和存储任何正在进行的工作流程活动的数据库。 安全日志记录服务以及 User Application 和工作流程供应都需要数据库。可以设置一个数据库同时为两个应用程序提供服务，也可以为每个应用程序设置独立的数据库。安全日志记录服务不包括特定的数据库。 瘦客户机驱动程序和 OCI 客户机驱动程序都支持 Oracle。
工作站 <ul style="list-style-type: none"> ◆ Designer 2.1.1 for Identity Manager 3.5.1 ◆ iManager 万维网访问 	已在下列平台上测试了 Designer : <p>Windows :</p> <ul style="list-style-type: none"> ◆ 带最新 Service Pack 的 Windows 2000 Professional ◆ Windows XP SP2 ◆ Microsoft Windows Vista <p>Linux :</p> <ul style="list-style-type: none"> ◆ SUSE Linux Enterprise Server 10 (仅对于 Designer) ◆ SUSE Linux 10.1 ◆ SUSE Linux Enterprise Desktop 10 ◆ Red Hat Enterprise Linux WS 4.0 (仅对于 Designer) , Gnome* 默认 ◆ Red Hat Fedora Core 5 (仅对于 Designer) , Gnome 默认 ◆ Novell Linux Desktop 9 , KDE 默认 	Designer 使用 Eclipse 作为其开发平台。有关平台特定信息，请参考 Eclipse 万维网站点 (http://www.eclipse.org) 。 Designer 的最低和建议硬件要求 : <ul style="list-style-type: none"> ◆ 最低 1 GHz ; 建议 2 GHz 或更高 ◆ 最低 512 MB RAM ; 建议 1 GB RAM 或更高 ◆ 最低 1024 x 768 分辨率 ; 建议 1280 x 1024 先期必要的软件 : <ul style="list-style-type: none"> ◆ Microsoft Internet Explorer 6.0 SP1 ◆ Microsoft Internet Explorer 7 ◆ 或 Mozilla* Firefox 2.0

必需的系统组件	系统要求	注释
已连接系统服务器 (由运行远程装载程序的独立服务器承载) <ul style="list-style-type: none"> ◆ 远程装载程序 ◆ Remote Loader 配置工具 (仅限 Windows) ◆ Novell Audit 代理 ◆ 口令同步代理 ◆ 已连接系统的驱动程序 Shim ◆ 已连接系统的工具 	每个驱动程序都要求已连接系统可用，并且提供了相关的 API。 有关每个系统特定的操作系统要求和已连接系统要求，请参考 Identity Manager 驱动程序文档 (http://www.novell.com/documentation/idm35drivers) 。	每个连接的应用程序都要求个人具有特定于应用程序的知识并承担相关责任。 Remote Loader System : <ul style="list-style-type: none"> ◆ Windows NT* 4.0、Windows 2000 Server 或带最新 Support Pack 的 Windows Server 2003 ◆ 带最新 Service Pack 的 Windows Server* 2003 (64 位) ◆ 口令同步代理在 Windows Server 2003 (64 位) 上受支持 ◆ Red Hat Linux 3.0、4.0 或 5.0 ES 或者 AS ◆ SUSE Linux Enterprise Server9 或 10 ◆ AIX 5.2L , 版本 5.2 或 5.3 Java Remote Loader System : <ul style="list-style-type: none"> ◆ HP-UX* 11i ◆ OS/400 ◆ xOS* ◆ 应该可以在具有 JVM 1.4.2 或更高版本的任何系统上使用它
Audit	Novell Audit 2.0.2	
User Application SSO 集成	需要 Novell Access Manager 3.0.1。	包括用 JDK* 1.5 构建的 saslsaml.jar 版本。

安装的前提条件。

本部分说明了安装 Identity Manager 基于角色的供应模块的先决条件。包括以下主题：

- ◆ 第 2.1 节 “Java 开发工具包”（第 17 页）
- ◆ 第 2.2 节 “安装 Identity Manager Metadirectory”（第 18 页）
- ◆ 第 2.3 节 “安装 JBoss Application Server”（第 18 页）
- ◆ 第 2.4 节 “安装 WebSphere Application Server”（第 22 页）
- ◆ 第 2.5 节 “数据库”（第 22 页）
- ◆ 第 2.6 节 “安全性先决条件”（第 24 页）
- ◆ 第 2.7 节 “下载产品”（第 24 页）
- ◆ 第 2.8 节 “安装 prerequisitefiles.zip 文件的内容”（第 25 页）
- ◆ 第 2.9 节 “为角色安装 iManager 图标”（第 27 页）

2.1 Java 开发工具包

JBoss、WebSphere 和身份库都有各自的 Java 开发工具包要求。

JBoss Application Server: 在 JBoss Application Server 上使用 Java 2 平台标准版开发工具包 (Java 2 Platform Standard Edition Development Kit) 版本 1.5.0_14。

使用此版本的 Sun JDK 启动基于角色的供应模块安装程序，如下所示：

Linux/Solaris:

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

Windows:

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

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/jdk1.5.0_10
```

注释：SLES 用户：不要使用 SLES 附带的 IBM JDK。此版本与部分安装过程不兼容。

WebSphere Application Server: 在 WebSphere* Application Server 上，使用与 WebSphere Application Server 6.1.0.9 一起提供的 IBM JDK，并应用无限制的策略文件。应用 WAS JDK fixpack for 6.1.0.9。

身份库 (Metadirectory) 安装程序: 身份库 (Metadirectory) 安装程序会在除 NetWare® 外的所有平台上安装它自己的 JVM 副本。在 NetWare 上，身份库使用系统上安装的任何 Java 版本。

2.2 安装 Identity Manager Metadirectory

安装 Identity Manager 3.5.1 Metadirectory。在《*Novell Identity Manager 3.5.1 安装指南* (<http://www.novell.com/documentation/idm35/pdfdoc/install/install.pdf>)》中有相关指导。

允许 Identity Manager 基于角色的供应模块管理员访问身份库。要执行此操作，请在 iManager 中为管理员指派对 Identity Manager 基于角色的供应模块用户所在环境的访问权限。

2.3 安装 JBoss Application Server

如果计划使用 JBoss* Application Server，请执行以下任一操作：

- ◆ 根据制造商的指示下载并安装 JBoss 4.2.0 Application Server
- ◆ 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（选择性安装 MySQL）。有关指导，请参阅第 2.3.1 节“**安装 JBoss Application Server 和 MySQL 数据库**”（第 18 页）。

等到安装完 Identity Manager 基于角色的供应模块后，再启动 JBoss 服务器。启动 JBoss 服务器是安装后任务。

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：记录应用程序服务器使用的端口，基于角色的供应模块安装程序需要此端口。（应用程序服务器的默认端口为 8080。）

SSL：如果计划使用外部口令管理，请在部署 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。有关启用 SSL 的指导，请参阅 JBoss 文档。还需要确保在防火墙上打开 SSL 端口。有关 IDMPwdMgt.war 文件的信息，请参阅第 7.5 节“**访问外部口令 WAR**”（第 94 页）以及《*IDM User Application：管理指南* (<http://www.novell.com/documentation/idmrbpm36/index.html>)》。

2.3.1 安装 JBoss Application Server 和 MySQL 数据库

可以使用 JbossMysql 实用程序在系统中安装 JBoss Application Server 和 MySQL。

注释：此实用程序并不安装 JBoss Application Server 作为 Windows 服务。要将 JBoss Application Server 作为 Windows 系统上的一个服务来安装，请参见第 2.3.2 节“**安装 JBoss Application Server 作为一项服务**”（第 21 页）。

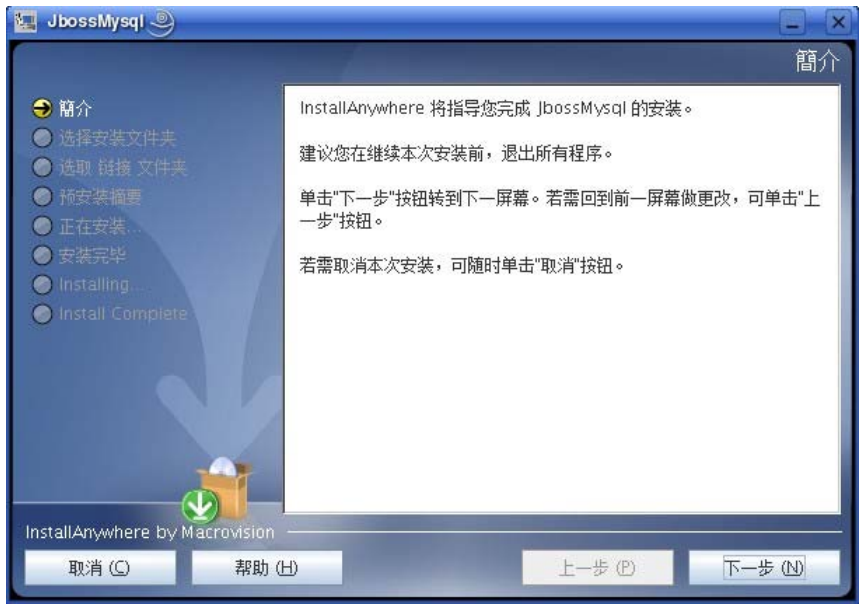
- 1 找到并执行 JbossMysql.bin 或 JbossMysql.exe。可在以下位置找到绑定在 User Application 上的此实用程序：

/linux/user_application（对于 Linux）

/nt/user_application（对于 Windows）

Solaris 不提供此实用程序。

- 2 选择区域设置。
- 3 阅读介绍页面，然后单击 **下一步**。



4 选择要安装的产品，然后单击 下一步。



5 单击 选择 以选择要安装选定产品的根文件夹，然后单击 下一步。



6 指定数据库的名称。User Application 安装需要此名称。

7 指定数据库 root 用户口令。



8 单击 下一步。

9 在“预安装摘要”中检查指定的设置，然后单击 安装。



安装选定产品之后，实用程序将显示一条成功完成安装的讯息。如果安装了 MySQL 数据库，请继续第 2.5.2 节“配置 MySQL 数据库”（第 23 页）。

2.3.2 安装 JBoss Application Server 作为一项服务

要作为一项服务运行 JBoss Application Server，请使用 Java Service Wrapper 或第三方实用程序。请访问 <http://wiki.jboss.org/wiki/Wiki.jsp?page=RunJBossAsAServiceOnWindows> (<http://wiki.jboss.org/wiki/Wiki.jsp?page=RunJBossAsAServiceOnWindows>)，了解 JBoss 的指导。

本部分包括以下主题：

- ◆ 使用 Java Service Wrapper（第 21 页）
- ◆ 使用第三方实用程序（第 22 页）

使用 Java Service Wrapper

通过 Java Service Wrapper，可以安装、启动和停止 JBoss Application Server 作为 Windows 服务或 Linux 或 UNIX 守护进程。请在因特网上查找可用的实用程序和下载站点。

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 管理此封装程序（请参见 <http://wrapper.tanukisoftware.org/doc/english/jmx.html#jboss> (<http://wrapper.tanukisoftware.org/doc/english/jmx.html#jboss>)）。某些示例配置文件包括：

```
wrapper.conf :
wrapper.java.command=%JAVA_HOME%/bin/java
wrapper.java.mainclass=org.tanukisoftware.wrapper.WrapperSimpleApp
wrapper.java.classpath.1=%JBOSS_HOME%/server/default/lib/wrapper.jar
wrapper.java.classpath.2=%JAVA_HOME%/lib/tools.jar wrapper.java.classpath.3=./run.jar
wrapper.java.library.path.1=%JBOSS_HOME%/server/default/lib wrapper.java.additional.1=-
server wrapper.app.parameter.1=org.jboss.Main wrapper logfile=%JBOSS_HOME%/server/
```

```
default/log/wrapper.log wrapper.ntsvice.name=JBoss wrapper.ntsvice.displayName=JBoss
Server
```

重要：必须正确设置 `JBOSS_HOME` 环境变量。封装程序本身不设置此变量。

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

使用第三方实用程序

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 Application Server。

重要：JBoss 不再建议使用 JavaService。有关详细信息，请参见 <http://wiki.jboss.org/wiki/Wiki.jsp?page=JavaService> (<http://wiki.jboss.org/wiki/Wiki.jsp?page=JavaService>)。

2.4 安装 WebSphere Application Server

如果计划使用 WebSphere Application Server，请下载并安装 WebSphere 6.1.0.9 Application Server。应用 WAS JDK fixpack for 6.1.0.9。

2.5 数据库

安装数据库和数据库驱动程序，并创建数据库或数据库实例。记录以下数据库参数，以用于 Identity Manager 基于角色的供应模块的安装过程中：

- ◆ 主机和端口
- ◆ 数据库名称、用户名和用户口令

数据源文件必须指向数据库。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，请在安装前手动配置数据源。

数据库必须启用了 UTF-8。

- ◆ [第 2.5.1 节 “安装 MySQL”](#)（第 22 页）
- ◆ [第 2.5.2 节 “配置 MySQL 数据库”](#)（第 23 页）

2.5.1 安装 MySQL

无论您是通过 IDM User Application 实用程序安装 MySQL* 还是在自己的计算机上安装 MySQL，都请阅读 [第 2.5.2 节 “配置 MySQL 数据库”](#)（第 23 页）。

注释：如果计划迁移数据库，在安装程序中选择迁移选项之前，请启动该数据库。如果不迁移数据库，则安装 Identity Manager 基于角色的供应模块过程中无需运行数据库。只需启动数据库后再启动应用程序服务器即可。

2.5.2 配置 MySQL 数据库

必须设置 MySQL 配置，以使 MySQL 和 Identity manager 3.5.1 能够配合工作。如果自己安装 MySQL，必须自行设置。如果通过 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 存储引擎和表类型**（第 23 页）
- ◆ **字符集**（第 23 页）
- ◆ **区分大小写**（第 23 页）

INNODB 存储引擎和表类型

User Application 使用了 INNODB 存储引擎，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 UTF8。要在整个服务器范围内指定 UTF8，可在 my.cnf（Linux 或 Solaris）或 my.ini（Windows）中加入以下选项：

```
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：

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

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）。

2.6 安全性先决条件

打开 Novell Access Manager™ 或 iChain® 中的 Cookie 转发选项，可以启用 Identity Manager 基于角色的供应模块中的“同时注销”。有关指导，请参阅《Novell Access Manager 3.0 SP1 管理指南 (<http://www.novell.com/documentation/novellaccessmanager/adminguide/index.html?page=/documentation/novellaccessmanager/adminguide/data/b5pqck8.html>)》中的“插入 Cookie 标题”。

2.7 下载产品

从 [Novell Downloads \(http://download.novell.com/index.jsp\)](http://download.novell.com/index.jsp) 获取 Identity Manager 基于角色的供应模块 3.6 产品。

向系统中下载正确的 User Application .iso 映像文件：
Identity_Manager_3_6_0_User_Application_Provisioning.iso

.iso 文件包含以下递送目录：

- /linux/user_application （对于 Linux）
- /nt/user_application （对于 Windows）
- /solaris/user_application （对于 Solaris）
- /36MetaDirSupport （包括更新 IDM 3.5.1 Metadirectory 所需的文件以支持 IDM 3.6 User Application）

表 2-1 列出安装 Identity Manager 基于角色的供应模块 3.6 所需的文件和脚本。

表 2-1 安装 Identity Manager 3.6 User Application 所需的文件和底稿

文件	说明
IDMProv.war	这是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 User Application。
IDMUserApp.jar	这是基于角色的供应模块安装程序。
silent.properties	此文件包括静默安装所需的安装参数。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。
prerequisitefiles.zip	此 ZIP 文件包含要求手动安装的其他文件。
UserApplication_3_6_0-IDM3_5_1-V1.xml	这是 User Application 驱动程序的配置文件。
iManager_icons_for_roles.zip	这包含 eDirectory 中角色对象的 iManager 图标。

提示：在 /36MetaDirSupport 目录下可以找到 iManager_icons_for_roles.zip 和 prerequisitefiles.zip。其他文件位于 <operating_system> /user_application 目录中。

安装 Identity Manager 基于角色的供应模块的系统必须至少有 320 MB 的可用储存空间。

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）。

2.8 安装 prerequisitefiles.zip 文件的内容

在下载到的 .iso 映像中，找到 prerequisitefiles.zip 文件并进行解压缩。它包含必须手动安装的文件，如表 2-2 中所列：

表 2-2 需要手动安装的文件

文件名	说明	目录
nrf-extensions.sch	eDirectory™ 纲要文件	第 2.8.1 节 “扩展基于角色的供应模块版本 3.6 的 eDirectory 纲要”（第 25 页）
nrfdriver.jar	角色服务驱动程序 JAR	第 2.8.2 节 “为角色服务驱动程序复制 JAR 文件”（第 26 页）
RoleService-IDM3_5_1-V1.xml	角色服务驱动程序配置文件	第 2.8.3 节 “复制角色服务驱动程序配置文件”（第 26 页）
UserApplicationn_3_6_0-IDM3_5_1-V1.xml	支持基于角色的供应模块的 User Application 驱动程序配置文件	第 2.8.4 节 “复制 User Application 驱动程序配置文件”（第 27 页）
dirxml.lsc	记录应用程序日志纲要文件	第 2.8.5 节 “复制 dirxml.lsc 文件”（第 27 页）

- ◆ 第 2.8.1 节 “扩展基于角色的供应模块版本 3.6 的 eDirectory 纲要”（第 25 页）
- ◆ 第 2.8.2 节 “为角色服务驱动程序复制 JAR 文件”（第 26 页）
- ◆ 第 2.8.3 节 “复制角色服务驱动程序配置文件”（第 26 页）
- ◆ 第 2.8.4 节 “复制 User Application 驱动程序配置文件”（第 27 页）
- ◆ 第 2.8.5 节 “复制 dirxml.lsc 文件”（第 27 页）

2.8.1 扩展基于角色的供应模块版本 3.6 的 eDirectory 纲要

如以下各部分中所说明的，扩展基于角色的供应模块的 eDirectory 纲要：

- ◆ 扩展 Windows 上的纲要（第 25 页）
- ◆ 扩展 UNIX/Linux 上的纲要（第 26 页）
- ◆ 扩展 NetWare 上的纲要（第 26 页）

扩展 Windows 上的纲要

使用 NDSCons.exe 扩展 Windows 服务器上的纲要。eDirectory 中附带的纲要文件 (*.sch) 默认安装到 C:\Novell\NDS 目录中。

- 1 单击 *开始* > *设置* > *控制面板* > *Novell eDirectory 服务*。
- 2 单击 *install.dlm*，然后单击 *开始*。

- 3 单击 *安装附加纲要文件*，然后单击 *下一步*。
- 4 以具有管理权限的用户身份登录，然后单击 *确定*。
- 5 指定纲要文件路径和名称（例如，c:\Novell\NDS\nrf-extensions.sch）。
- 6 单击 *完成*。

扩展 UNIX/Linux 上的纲要

要扩展 UNIX/Linux 平台上基于角色的供应模块的 eDirectory 纲要，请执行以下步骤：

- 1 添加基于角色的供应模块纲要文件：nrf-extensions.sch。要执行此操作，请从命令行使用 ndssch 命令：

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

扩展 NetWare 上的纲要

使用 NWConfig.nlm 扩展 NetWare 上的纲要。eDirectory 中附带的纲要文件 (*.sch) 安装到 sys:\system\schema 目录中。

- 1 在服务器控制台上，输入 nwconfig。
- 2 选择 *目录选项 > 扩展纲要*。
- 3 以具有管理权限的用户身份登录。
- 4 按 F3 指定其他路径，然后键入 sys:\system\schema（或 *.sch 文件的路径）和 nrf-extensions.sch 纲要文件。
- 5 按 Enter。

2.8.2 为角色服务驱动程序复制 JAR 文件

在 Metadirectory 服务器上手动安装角色服务驱动程序。要执行此操作，请将可执行角色服务 JAR 文件 nrfdriver.jar 从解压缩的 prerequisitefiles.zip 存档中复制到正确的系统目录下：

表 2-3 角色服务驱动程序 JAR 文件的位置

操作系统	目录
UNIX (eDirectory 8.7.x)	/usr/lib/dirxml/classes
UNIX (eDirector 8.8.x)	/opt/novell/eDirectory/lib/dirxml/classes
Windows	<drive>:\novell\nds\lib
NetWare	SYS:SYSTEM\LIB

2.8.3 复制角色服务驱动程序配置文件

将角色服务驱动程序配置文件 RoleService_IDM3_5_1-V1.xml 手动安装到正确的系统目录下：

表 2-4 角色服务驱动程序配置文件的位置

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

2.8.4 复制 User Application 驱动程序配置文件

将 User Application 驱动程序配置文件 UserApplication_3_6_0-IDM3_5_1-V1.xml 手动安装到正确的系统目录下：

表 2-5 User Application 驱动程序配置文件的位置

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

2.8.5 复制 dirxml.lsc 文件

按《Identity Manager User Application: 管理指南 (<http://www.novell.com/documentation/idmr36/pdfdoc/agpro/agpro.pdf>)》的“设置日志记录”部分中的指导，将 dirxml.lsc 文件复制到 Audit 服务器中。

2.9 为角色安装 iManager 图标

在下载到的 .iso 映像中找到 iManager_icons_for_roles.zip 文件并进行解压缩。将提取的图标文件复制到 nps/portal/modules/dev/images/dir 目录中。重新启动 iManager 以便使用新图标。

创建驱动程序

本部分说明了如何创建使用基于角色的供应模块所必需的驱动程序。包括以下主题：

- ◆ 第 3.1 节 “在 iManager 中创建 User Application 驱动程序”（第 29 页）
- ◆ 第 3.2 节 “在 iManager 中创建角色服务驱动程序”（第 33 页）

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)。

允许的驱动程序配置为：

- ◆ 在 iManager 中，每个驱动程序集可以添加一个角色服务驱动程序。
- ◆ 可以将一个 User Application 驱动程序与一个角色服务驱动程序相关联。
- ◆ 可以将一个 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

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。有关在群集上运行基于角色的供应模块的信息，请参阅《*Identity Manager User Application：管理指南* (<http://www.novell.com/documentation/idmrpbpm36/index.html>)》。

基于角色的供应模块在 User Application 驱动程序中存储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 workflow 引擎配置。

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。所导致的问题的来源难以检测。

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 2.6 或更高版本。
- 2 转至 **角色和任务 > Identity Manager 实用程序**，然后选择 **新建驱动程序** 启动 “创建驱动程序” 向导。



Identity Manager 产品包括所有产品组件。您有权部署的驱动程序取决于您所采购的驱动程序。

应用程序驱动程序包含在驱动程序集中。创建驱动程序时，请确保与驱动程序集关联的服务器包含该驱动程序集所属分区的非过滤的可写副本。如果该服务器未包含这样的副本，则会添加一个读/写副本，或者将现有副本转换为读/写副本。

要将新驱动程序放在哪个位置？

在现有驱动程序集中

在新的驱动程序集中



- 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。



定义新的驱动程序集属性。

名称:

环境:  

服务器:  

在该驱动程序集上创建新的分区

<< 后退 下一步 >> 取消 完成

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 *UserApplication_3_6_0-IDM3_5_1-V1.xml*。这是支持基于角色的供应模块的 User Application 驱动程序配置文件。

如果 *UserApplication_3_6_0-IDM3_5_1-V1.xml* 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 2.8.4 节“复制 User Application 驱动程序配置文件”（第 27 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	创建的驱动程序名称。
鉴定 ID	User Application 管理员的判别名。这是将赋予其管理 User Application 门户权限的 User Application 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。

字段	说明
允许覆盖启动程序： (值为“否”/“是”)	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”窗口并显示摘要页。



- 13 如果信息准确无误，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。

Identity Manager 概述

在以下位置找到 1 个驱动程序集: TestDriverSet.context
[对象](#) 在 TestDriverSet.context 中找到



3.2 在 iManager 中创建角色服务驱动程序

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 2.6 或更高版本。
- 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 (UserApplication_3_6_0-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。

每个驱动程序集只能有一个角色服务驱动程序。

- 3 单击 *添加驱动程序*。
- 4 在新的驱动程序向导中，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-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 *RoleService-IDM3_5_1-V1.xml* 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 2.8.3 节“[复制角色服务驱动程序配置文件](#)”（第 26 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。尝试重新启动 iManager 会话（关闭所有浏览器并重新登录到 iManager）。或尝试重新启动服务器。

- 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	<p>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。</p> <p>使用 <i>浏览</i> 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。</p>
User Application 驱动程序 DN	<p>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。</p>
User Application URL	<p>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 <i>http://host:port/IDM</i>。这是一个必需的字段。</p>
User Application 身份	<p>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。</p>
User Application 口令	<p>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。</p>
重输门户令	<p>重输入 User Application 管理员口令。</p>

7 填充信息后，单击 *完成*。

在 JBoss 上使用 GUI 安装

4

本部分说明如何在 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。如果更希望在 JBoss 上通过控制台或通过使用单条命令安装该模块，请参阅第 5 章“从控制台或使用单条命令安装”（第 61 页）。

- ◆ 第 4.1 节 “运行安装程序 GUI”（第 35 页）
- ◆ 第 4.2 节 “选择应用程序服务器平台”（第 36 页）
- ◆ 第 4.3 节 “迁移数据库”（第 37 页）
- ◆ 第 4.4 节 “指定 WAR 的位置”（第 39 页）
- ◆ 第 4.5 节 “选择安装文件夹”（第 39 页）
- ◆ 第 4.6 节 “选择数据库平台”（第 40 页）
- ◆ 第 4.7 节 “指定数据库主机和端口”（第 41 页）
- ◆ 第 4.8 节 “指定数据库名称和特权用户”（第 42 页）
- ◆ 第 4.9 节 “指定 Java 根目录”（第 43 页）
- ◆ 第 4.10 节 “选择应用程序服务器配置类型”（第 44 页）
- ◆ 第 4.11 节 “指定 JBoss Application Server 设置”（第 45 页）
- ◆ 第 4.12 节 “启用 Novell Audit 日志记录”（第 46 页）
- ◆ 第 4.13 节 “指定主密钥”（第 47 页）
- ◆ 第 4.14 节 “配置 User Application”（第 49 页）
- ◆ 第 4.15 节 “使用口令 WAR”（第 59 页）
- ◆ 第 4.16 节 “校验选项和安装”（第 60 页）
- ◆ 第 4.17 节 “查看日志文件”（第 60 页）

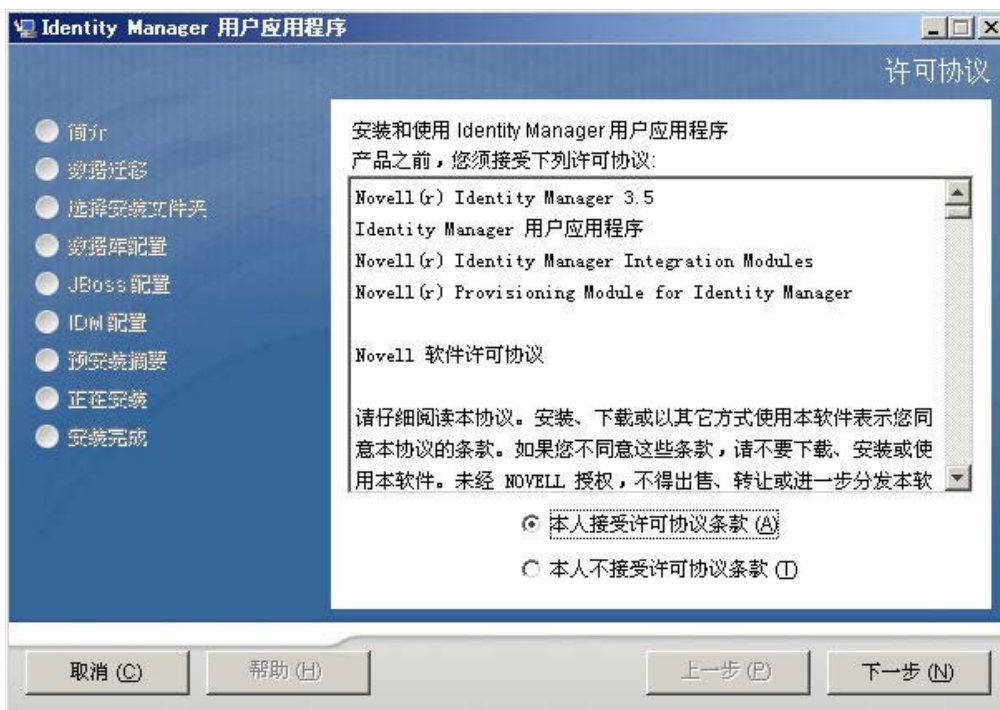
如果要使用命令行进行安装，请参阅第 5 章“从控制台或使用单条命令安装”（第 61 页）。

4.1 运行安装程序 GUI

- 1 浏览找到包含安装文件的目录，如表 2-1 在第 24 页中所述。
- 2 从命令行起动平台的安装程序：
`java -jar IdmUserApp.jar`
- 3 从下拉菜单中选择一种语言，然后单击 *确定*。



4 阅读许可证协议，单击本人接受许可证协议中的条款，然后单击下一步。



5 阅读安装向导的“简介”页，然后单击下一步。

6 继续第 4.2 节“选择应用程序服务器平台”（第 36 页）。

4.2 选择应用程序服务器平台

完成第 4.1 节“运行安装程序 GUI”（第 35 页）中的安装过程，然后继续以下步骤：

1 选择 JBoss Application Server 平台，然后单击下一步。



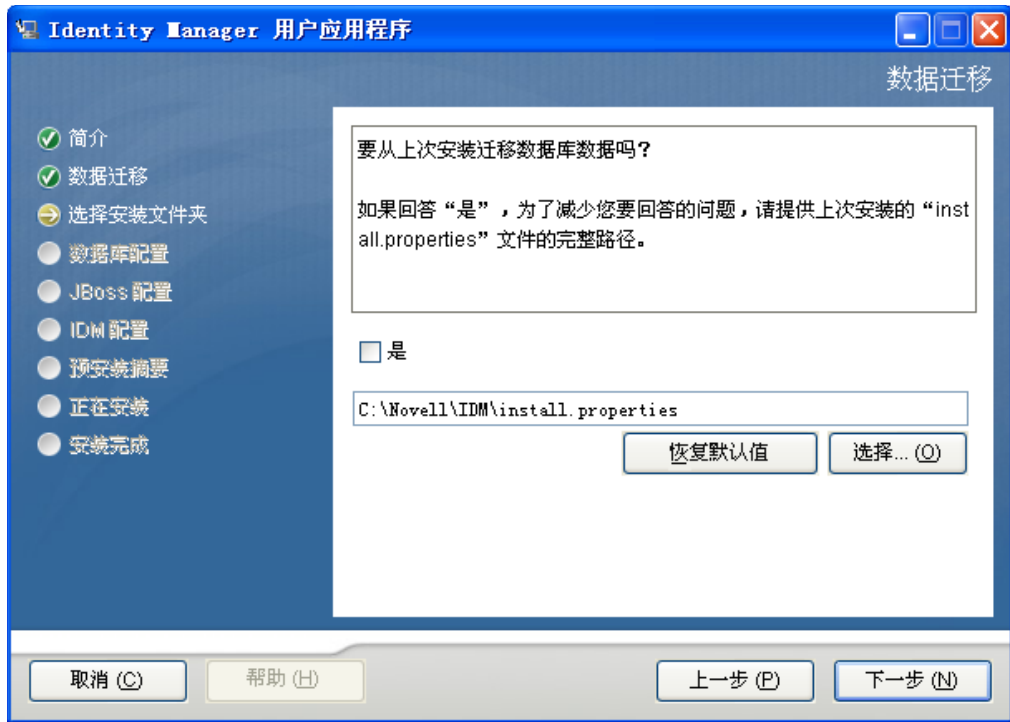
4.3 迁移数据库

- 1 如果不想迁移数据库，请单击 **下一步**，然后继续第 4.4 节 “指定 WAR 的位置”（第 39 页）。

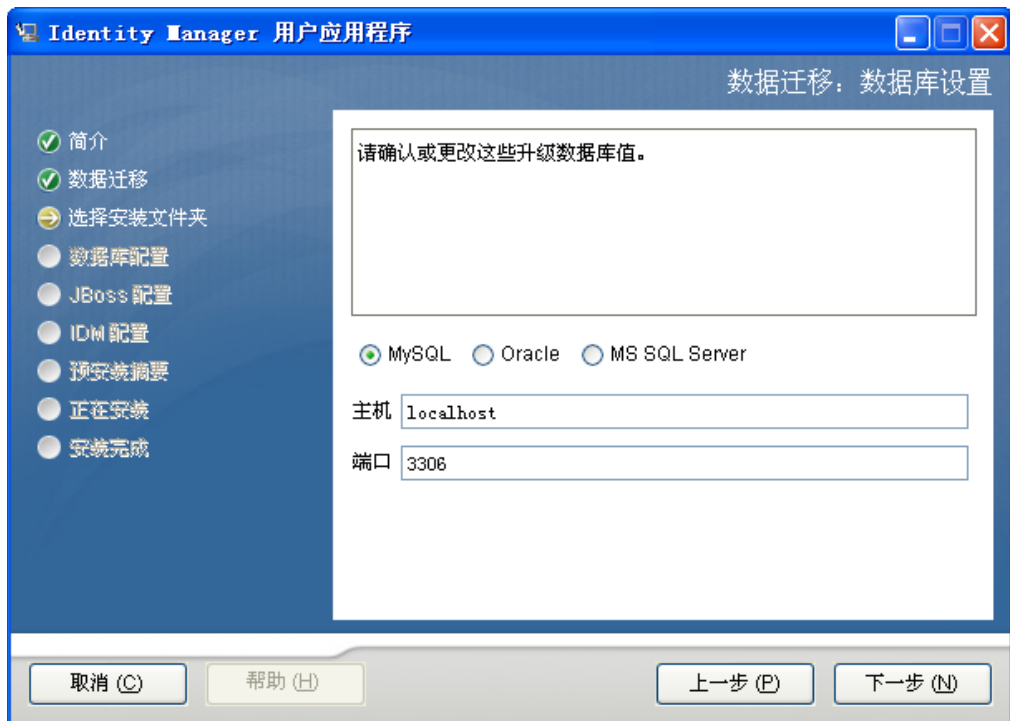
如果要使用来自版本 3.0 或版本 3.01 User Application 的现有数据库，则必须迁移数据库。继续下一步。

- 2 校验已启动了要迁移的数据库。
- 3 单击安装程序的“数据迁移”页中的 **是**。
- 4 单击 **选择** 浏览 Identity Manager 3.0 或 3.01 User Application 安装目录中的 `install.properties` 文件。

通过指定以前安装的 `install.properties` 文件的位置，可以减少必须在以下页面中指定的项目数。



5 系统要求您确认数据库类型、主机名和端口。完成此操作后，单击 **下一步**。



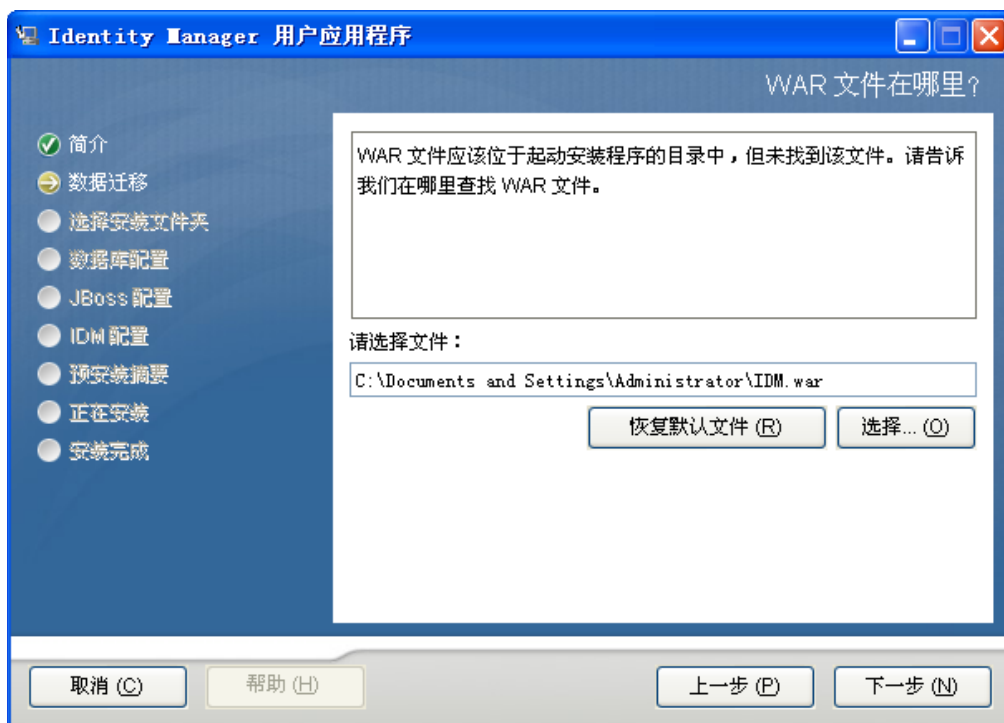
6 单击 **下一步** 继续到第 4.4 节 “指定 WAR 的位置” (第 39 页) 或第 4.5 节 “选择安装文件夹” (第 39 页)。

User Application 安装程序更新 User Application，并将 V3.0 或 3.0.1 数据库中的数据迁移到 V3.5.1 所使用的数据库。有迁移数据库的信息及其其他步骤，请参见《*Identity Manager User Application: 迁移指南* (<http://www.novell.com/documentation/idmrbpm36/index.html>)》。

4.4 指定 WAR 的位置

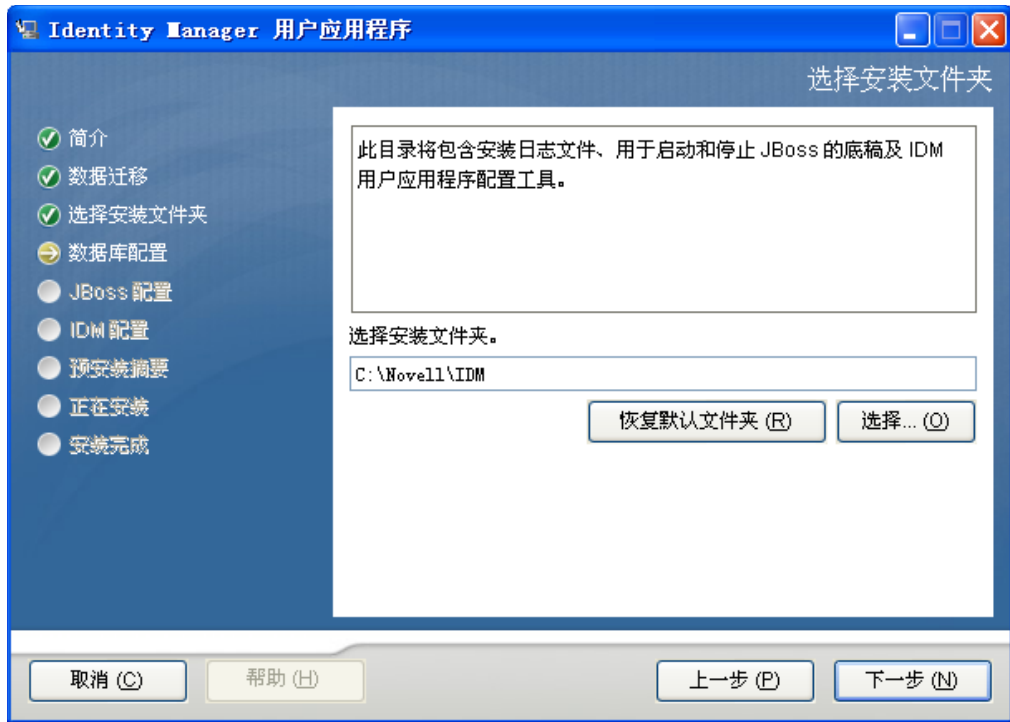
如果 Identity Manager User Application WAR 文件所在的目录不同于安装程序，安装程序将提示提供 WAR 的路径。

- 1 如果 WAR 在默认位置，请单击 *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。
- 2 单击 *下一步*，然后继续第 4.5 节“选择安装文件夹”（第 39 页）。



4.5 选择安装文件夹

- 1 在“选择安装文件夹”页，选择安装 User Application 的位置。如果要记住和使用默认位置，单击 *恢复默认文件夹*；如果要为安装文件选择其他位置，单击 *选择* 并浏览某个位置。
- 2 单击 *下一步*，然后继续第 4.6 节“选择数据库平台”（第 40 页）。



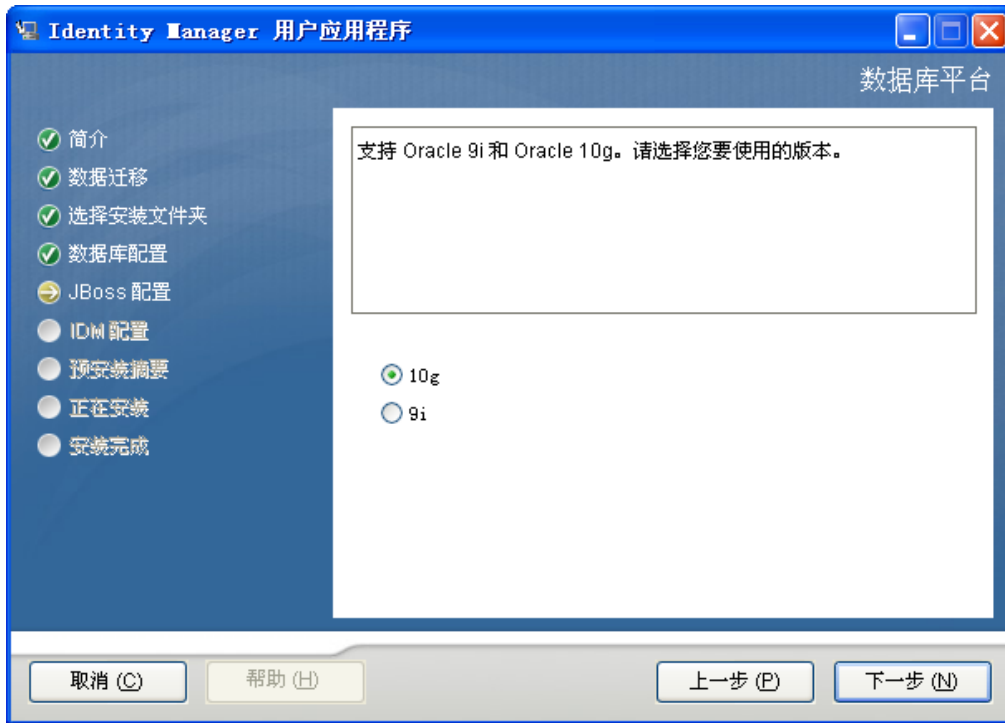
4.6 选择数据库平台

- 1 选择要使用的数据库平台。



- 2 如果使用的是 Oracle 数据库，请继续 [步骤 3](#)。否则，请跳至 [步骤 4](#)。

3 如果使用的是 Oracle 数据库，安装程序将询问所使用的版本。选择使用的版本。



4 单击 **下一步**，然后继续第 4.7 节“指定数据库主机和端口”（第 41 页）。

4.7 指定数据库主机和端口

1 填写以下字段：



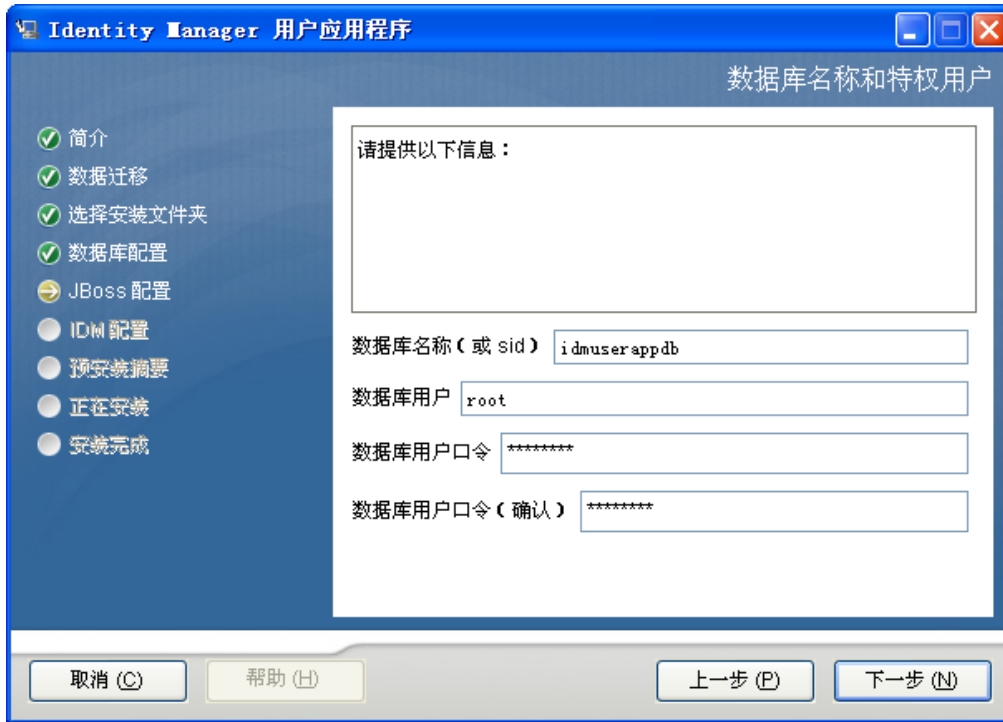
字段	说明
----	----

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	指定数据库的侦听器端口号。 对于群集，对其中每个成员指定相同的端口。

2 单击 **下一步**，然后继续第 4.8 节“指定数据库名称和特权用户”（第 42 页）。

4.8 指定数据库名称和特权用户

1 填写以下字段：

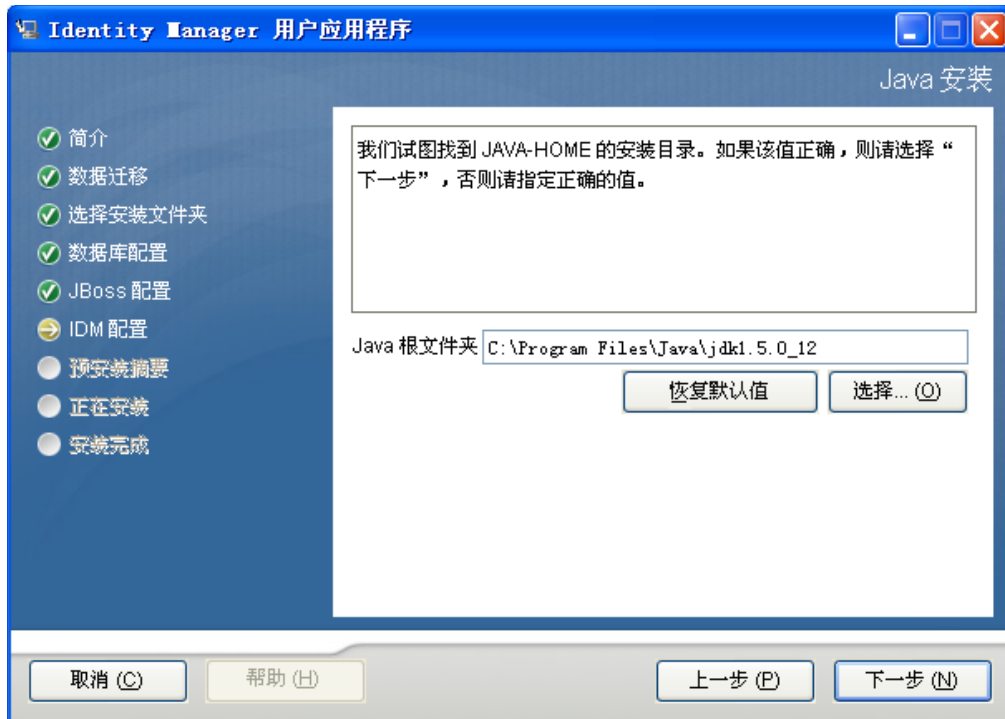


字段	说明
数据库名称 (或 SID)	对于 MySQL 或 MS SQL Server，提供预配置数据库的名称。对于 Oracle，提供以前创建的 Oracle 系统标识符 (SID)。 对于群集，对其中每个成员指定相同的数据库名称或 SID。
数据库用户	指定数据库用户。 对于群集，对其中每个成员指定相同的数据库用户。
数据库口令 / 确认口令	指定数据库口令。 对于群集，对其中每个成员指定相同的数据库口令。

- 单击 **下一步**，然后继续第 4.9 节“指定 Java 根目录”（第 43 页）。

4.9 指定 Java 根目录

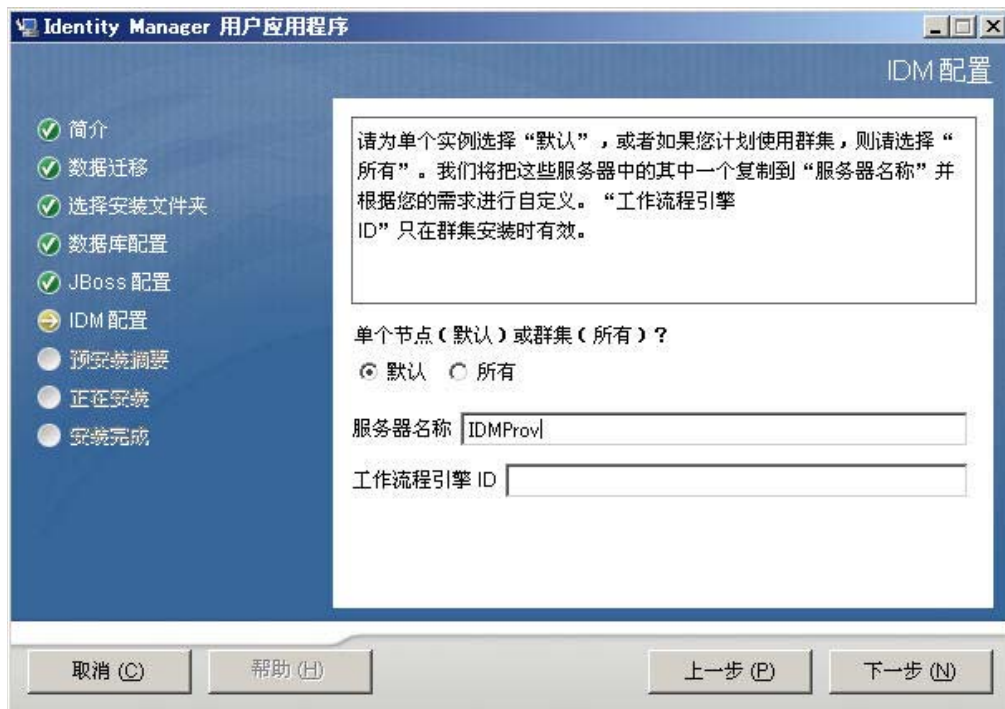
- 单击 **选择** 浏览 Java 根文件夹。要使用默认位置，请单击 **恢复默认值**。



- 2 单击 **下一步**，然后继续第 4.11 节“指定 JBoss Application Server 设置”（第 45 页）。

4.10 选择应用程序服务器配置类型

- 1 填写以下字段：



选项	说明
单个节点（默认）或群集（所有）	<p>选择应用程序服务器配置的类型：</p> <ul style="list-style-type: none"> ◆ 如果此安装是群集中的一部分，选择<i>全部</i> ◆ 如果此安装是单独节点，而不是群集的一部分，选择<i>默认</i>
服务器名称	<p>指定服务器名称。</p> <p>服务器名称为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。安装底稿创建服务器配置，并默认根据<i>应用程序名称</i>命名配置。</p> <p>将应用程序名称记录下来，当从浏览器启动 Identity Manager User Application 时，将其添加到 URL 中。</p>
工作流程引擎 ID	<p>群集中的每个服务器都必须具有唯一的工作流程引擎 ID。有关工作流程引擎 ID 的说明，请参见《<i>Identity Manager User Application：管理指南</i>》中的 3.5.4 节：对群集配置工作工作流。</p>

2 单击下一步，然后继续第 4.12 节“启用 Novell Audit 日志记录”（第 46 页）。

4.11 指定 JBoss Application Server 设置

在此页上，为 User Application 指定查找 JBoss Application Server 的位置。

此安装过程不安装 JBoss Application Server。有关安装 JBoss Application Server 的指导，请参阅第 2.3.1 节“安装 JBoss Application Server 和 MySQL 数据库”（第 18 页）。

1 提供根文件夹、主机和端口：



字段	说明
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侦听器端口号。JBoss 默认端口为 8080。

2 单击 **下一步**，然后继续第 4.10 节“选择应用程序服务器配置类型”（第 44 页）。

4.12 启用 Novell Audit 日志记录

（可选）要对 User Application 启用 Novell Audit 日志记录，请执行下列操作：

1 填写以下字段：



选项	说明
启用	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, 请参见 《Identity Manager User Application : 管理指南》。
关	对 User Application 禁用 Novell Audit 日志记录。以后可以使用 User Application 的 <i>管理</i> 选项卡来启用该功能。 有关启用 Novell Audit 日志记录的更多信息, 请参见 《Identity Manager User Application : 管理指南》。
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。

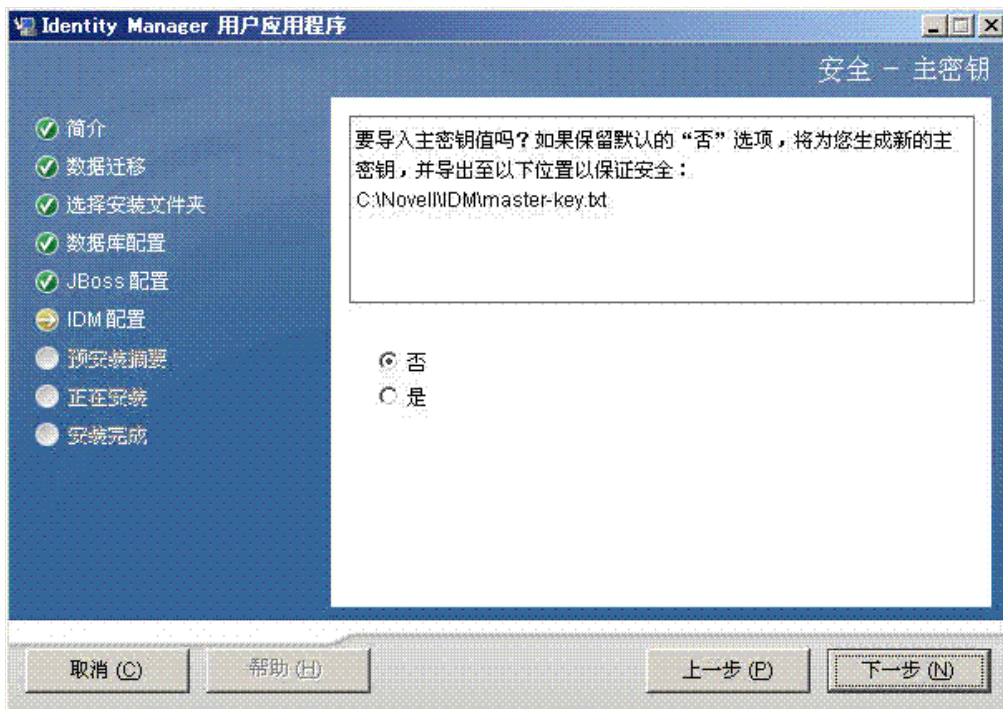
2 单击 **下一步**, 然后继续第 4.14 节 “配置 User Application” (第 49 页)。

4.13 指定主密钥

指定是要导入现有主密钥还是新建主密钥。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 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。这样可以获得以前存储的加密数据的访问权。

1 单击 **是** 导入现有主密钥, 或者单击 **否** 新建主密钥。



2 单击 **下一步**。

安装过程中会将经过加密的主密钥写到安装目录中的 `master-key.txt` 文件中。

如果选择 **否**, 跳至 [第 4.14 节 “配置 User Application” \(第 49 页\)](#)。完成安装后, 必须手动记录主密钥, 如 [第 7.1 节 “记录主密钥” \(第 93 页\)](#) 中所述。

如果选择 **是**, 继续 [步骤 3](#)。

3 如果选择导入现有经过加密的主密钥, 请将密钥剪切和粘贴到安装过程窗口。



4 单击 *下一步*。

4.14 配置 User Application

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。

1 设置基本 User Application 配置参数（参见表 4-1 中的说明），然后继续步骤 2。

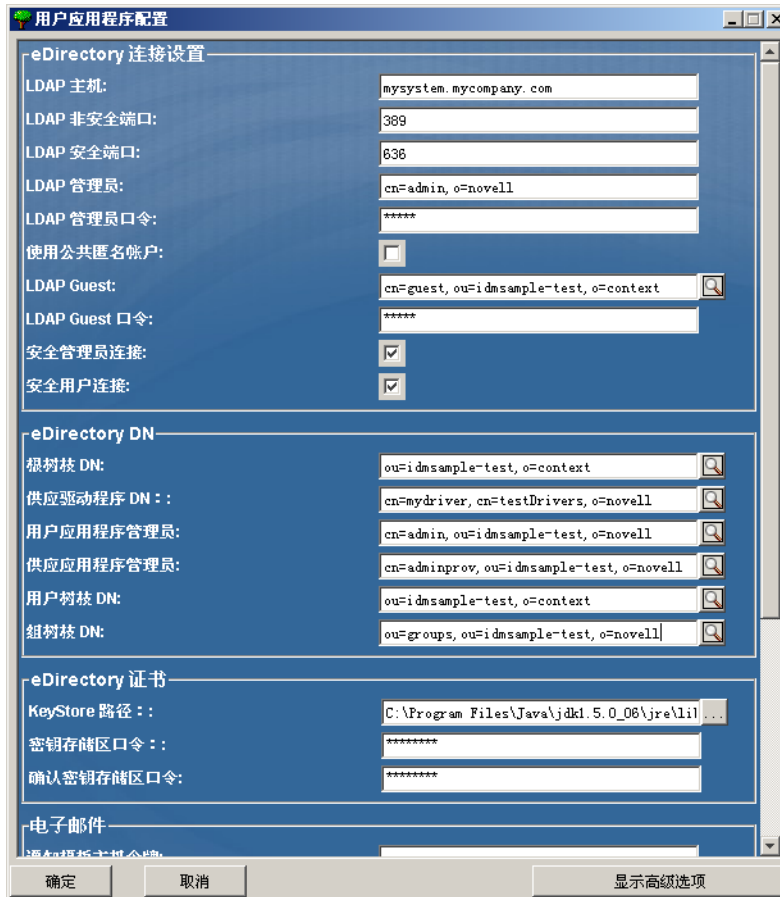


表 4-1 User Application 配置: 基本参数

设置类型	字段	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。
	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 <i>使用公开匿名帐户</i> 。要禁用 Guest 用户，请选择 <i>使用公开匿名帐户</i> 。
	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	字段	说明
eDirectory DN	<i>根容器 DN</i>	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。
	<i>供应驱动程序 DN</i>	必需。指定以前在 第 3.1 节“在 iManager 中创建 User Application 驱动程序” (第 29 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： <code>cn=UserApplicationDriver,cn=myDriverSet,o=myCompany</code>
	<i>User Application Admin</i>	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 <i>管理</i> 选项卡管理门户。 如果 User Application 管理员参与 iManager、Designer for Identity Manager 或 User Application (<i>请求和批准</i> 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，请参见 <i>《IDM User Application : 管理指南》</i> 。 要在部署 User Application 之后更改指派，必须使用 User Application 中的 <i>管理 > 安全</i> 页面。
eDirectory DN (续)	<i>供应应用程序 Admin</i>	供应应用程序管理员使用 <i>供应</i> 选项卡 (<i>管理</i> 选项卡下) 管理供应工作流程功能。用户可以通过 User Application 的 <i>请求和批准</i> 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 <i>管理 > 安全</i> 页面。
	<i>角色管理员</i>	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，授予或撤销指派给任何用户、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 <i>角色 > 角色指派</i> 页面。
	<i>用户容器 DN</i>	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： 如果要使用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。

设置类型	字段	说明
eDirectory 证书	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。
	密钥存储区路径	必需。指定应用程序服务器用于运行的、JDK 密钥存储区 (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。
电子邮件	密钥存储区口令 / 确认密钥存储区口令	必需。指定 cacerts 口令。默认值为 changeit。
	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： <code>myapplication serverServer</code> 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连接。
	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 <i>使用外部口令 WAR</i> ，则必须提供 <i>忘记口令链接</i> 和 <i>忘记口令返回链接</i> 的值。 如果没有选择 <i>使用外部口令 WAR</i> ，则 IDM 将使用默认的内部口令管理功能。 <code>/jsps/pwdmgt/ForgotPassword.jsf</code> (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 <code>ForgotPassword.jsf</code> 文件。有关细节，请参见 使用口令 WAR (第 59 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 <code>https://idmhost:sslport/idm</code> 。

2 如果要设置其他 User Application 配置参数，请单击 *显示高级选项*。（通过滚动查看整个面板。）表 4-2 说明了“高级选项”参数。

如果不想设置此步骤中所述的其他参数，请跳至 **步骤 3**。

表 4-2 *User Application 配置：所有参数*

设置类型	字段	说明
eDirectory 连接设置	<i>LDAP 主机</i>	必需。为 LDAP 服务器指定主机名或 IP 地址。 例如： myLDAPhost
	<i>LDAP 非安全端口</i>	为 LDAP 服务器指定非安全端口。例如：389。
	<i>LDAP 安全端口</i>	为 LDAP 服务器指定安全端口。例如：636。
	<i>LDAP 管理员</i>	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。
	<i>LDAP 管理员口令</i>	必需。指定 LDAP 管理员口令。此口令已使用主密钥进行过加密。
	<i>使用公开匿名帐户</i>	允许没有登录的用户访问 LDAP 公开匿名帐户。
	<i>LDAP Guest</i>	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 <i>使用公开匿名帐户</i> 。要禁用 Guest 用户，请选择 <i>使用公开匿名帐户</i> 。
	<i>LDAP Guest 口令</i>	指定 LDAP Guest 口令。
	<i>安全 Admin 连接</i>	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。
	<i>安全用户连接</i>	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	字段	说明
eDirectory DN	<i>根容器 DN</i>	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。
	<i>供应驱动程序 DN</i>	必需。指定以前在 第 3.1 节 “在 iManager 中创建 User Application 驱动程序” (第 29 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： <code>cn=UserApplicationDriver,cn=myDriverSet,o=myCompany</code>
	<i>User Application Admin</i>	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 <i>管理</i> 选项卡管理门户。 如果 User Application 管理员参与 iManager、Designer for Identity Manager 或 User Application (<i>请求和批准</i> 选项卡) 中显示的 workflow 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，请参见《IDM 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 <i>管理 > 安全</i> 页面。
<i>供应应用程序 Admin</i>	供应应用程序管理员通过 User Application 的 <i>请求和批准</i> 选项卡管理可用的供应 workflow 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 <i>管理 > 安全</i> 页面。	

设置类型	字段	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。 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： 如果要使用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。
	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，授予或撤销指派给任何用户、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 <i>角色 > 角色指派</i> 页面。
Metadirectory 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。
	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。
eDirectory 证书	动态组对象类	LDAP 动态组对象类 (一般 dynamicGroup)。
	密钥存储区路径	必需。指定应用程序服务器用于运行的、JRE 的密钥存储区 (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存储区文件。在 Linux 或 Solaris 上，用户必须具有写此文件的权限。
	密钥存储区口令	必需。指定 cacerts 口令。默认值为 changeit。
	确认密钥存储区口令	

设置类型	字段	说明
私有密钥存储区	<i>私有密钥存储区路径</i>	私有密钥存储区包含 User Application 的私有密钥和证书。保留。如果保留为空的话，将采用默认路径 <code>/jre/lib/security/cacerts</code> 。
	<i>私有密钥存储区口令</i>	口令为 <code>changeit</code> ，除非另行指定。此口令已使用主密钥进行过加密。
	<i>私有密钥别名</i>	别名为 <code>novellIDMUserApp</code> ，除非另行指定。
	<i>私有密钥口令</i>	口令为 <code>novellIDM</code> ，除非另行指定。此口令已使用主密钥进行过加密。
可信密钥存储区	<i>可信存储区路径</i>	可信密钥存储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 <code>javax.net.ssl.trustStore</code> 中获取路径。如果那里没有路径，则假定为 <code>jre/lib/security/cacerts</code> 。
	<i>可信存储口令</i>	如果此字段为空的话，User Application 将从系统属性 <code>javax.net.ssl.trustStorePassword</code> 中获取口令。如果那里没有值，则使用 <code>changeit</code> 。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。
	<i>Novell Audit 数字签名证书</i>	显示数字签名证书。
	<i>Novell Audit 数字签名私用密钥</i>	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	<i>已启用同步注销</i>	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，则将用户重路由到同步注销页。
	<i>同步注销页面</i>	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。如果启用了同步注销并且用户要注销 User Application，则将用户重路由到此页面。以下两个 URL 之一将根据您的环境将同步注销功能定向到正确的页面： Access Manager : <code>https://yourAccessGatewayServer/AGLogout</code> iChain : <code>https://youriChainServer/cmd/ICSLogout</code>

设置类型	字段	说明
电子邮件	<i>通知模板 Host 令牌</i>	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连接。
	<i>通知模板 Port 令牌</i>	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。
	<i>通知模板 Secure Port 令牌</i>	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。
	<i>通知模板 PROTOCOL 令牌</i>	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。
	<i>通知模板 SECURE PROTOCOL 令牌</i>	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。
	<i>通知 SMTP 电子邮件发件人：</i>	指定供应电子邮件中发送电子邮件的用户。
	<i>通知 SMTP 电子邮件主机：</i>	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		
	<i>使用外部口令 WAR</i>	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 <i>使用外部口令 WAR</i> ，则必须提供 <i>忘记口令链接</i> 和 <i>忘记口令返回链接</i> 的值。 如果没有选择 <i>使用外部口令 WAR</i> ，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。
	<i>忘记口令链接</i>	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，请参见 使用口令 WAR（第 59 页） 。
	<i>忘记口令返回链接</i>	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。

设置类型	字段	说明
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 <code>http://host:port/ocspLocal</code> 。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。
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 <i>添加新容器对象</i> 下面添加这些容器。
	容器特性名称	列出与容器对象类型相关的特性类型名称。
	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的对象类的 LDAP 名称。 有关容器的信息，请参阅《 <i>Novell iManager 2.6 管理指南</i> (http://www.novell.com/documentation/imanager26/pdfdoc/imanager_admin_26/imanager_admin_26.pdf)》。
	添加新的容器对象：容器特性名称	提供容器对象的特性名称。

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。

3 完整设置配置之后，单击 *确定*，然后继续第 4.16 节“*校验选项和安装*”（第 60 页）。

4.15 使用口令 WAR

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 4.15.1 节“*指定外部口令管理 WAR*”（第 59 页）
- ◆ 第 4.15.2 节“*指定内部口令 WAR*”（第 60 页）

4.15.1 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。另请参见第 7.4 节“在 JBoss 服务器间配置 SSL 通讯”（第 94 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（第 60 页）。
- ◆ 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（第 60 页）。

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。

4.15.2 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。

4.16 校验选项和安装

- 1 阅读“安装前摘要”页，校验所选择的安装参数。
- 2 如有必要，使用 *后退* 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。

- 3 当安装和配置参数满意之后，返回“安装前摘要”页，然后单击 *安装*。

4.17 查看日志文件

- 1 如果安装成功完成，没有错误，请转至第 7 章“安装后任务”（第 93 页）。
- 2 如果安装提示出现错误或警告，请检查日志忘记以确定问题：
 - ◆ `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 配置有关解决问题的帮助，请参阅第 7.12 节“查错”（第 96 页）。

从控制台或使用单条命令安装

本部分说明了可用来代替第 4 章“在 JBoss 上使用 GUI 安装”（第 35 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 5.1 节“从控制台安装 User Application”（第 61 页）
- 第 5.2 节“使用单个命令安装 User Application”（第 61 页）

5.1 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。

- 1 获取表 2-1 在第 24 页中说明的相应安装文件。
- 2 登录并打开终端会话。
- 3 按如下所述，为使用 Java 的平台起动安装程序：

```
java -jar IdmUserApp.jar -i console
```
- 4 在导入步骤或创建主密钥步骤中，按照第 4 章“在 JBoss 上使用 GUI 安装”（第 35 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。
- 5 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 4.14 节“配置 User Application”（第 49 页）中所述的值。
- 6 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。
- 7 继续第 7 章“安装后任务”（第 93 页）。

5.2 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 2-1 在第 24 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 5-1。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 5-1 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。 必需。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。 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。
NOVL_CONFIG_LDAPADMINPASS=	eDirectory 连接设置：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。
NOVL_CONFIG_ROOTCONTAINERNAME=	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。
NOVL_CONFIG_PROVISIONROOT=	eDirectory DN：供应驱动程序 DN。 必需。指定以前在 第 3.1 节“在 iManager 中创建 User Application 驱动程序” （第 29 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： <code>cn=UserApplicationDriver,cn=myDriverSet,o=myCompany</code>
NOVL_CONFIG_LOCKSMITH=	eDirectory DN：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，请参见 《IDM 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=	<p>eDirectory DN : 供应应用程序 Admin。</p> <p>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 <i>供应</i>选项卡 (<i>管理</i>选项卡下) 来管理供应工作流程功能。用户可以通过 User Application 的 <i>请求和批准</i>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。</p> <p>要在部署 User Application 之后更改指派, 必须使用 User Application 中的 <i>管理 > 安全</i> 页面。</p>
NOVL_CONFIG_ROLECONTAINERDN=	<p>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, 授予或撤销指派给任何用户、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。</p> <p>要在部署 User Application 后更改此指派, 请使用 User Application 中的 <i>角色 > 角色指派</i> 页面。</p>
NOVL_CONFIG_USERCONTAINERDN=	<p>Meta-Directory 用户身份 : 用户容器 DN。</p> <p>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。</p> <hr/> <p>重要 : 如果要使用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。</p>
NOVL_CONFIG_GROUPCONTAINERDN=	<p>Meta-Directory 用户组 : 组容器 DN。</p> <p>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。</p>
NOVL_CONFIG_KEYSTOREPATH=	<p>eDirectory 证书 : 密钥存储区路径。必需。</p> <p>指定应用程序服务器所使用的 JRE 的密钥存储区 (cacerts) 文件。User Application 安装过程中将修改密钥存储区文件。在 Linux 或 Solaris 上, 用户必须具有写此文件的权限。</p>
NOVL_CONFIG_KEYSTOREPASSWORD=	<p>eDirectory 证书 : 密钥存储区口令。</p> <p>必需。指定 cacerts 口令。默认值为 changeit。</p>
NOVL_CONFIG_SECUREADMINCONNECTION=	<p>eDirectory 连接设置 : 安全 Admin 连接。</p> <p>通过指定为 <i>True</i>, 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。</p> <p>如果 Admin 帐户不使用安全套接字通讯, 则指定为 <i>False</i>。</p>

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_SECUREUSERCONNECTION=	<p>eDirectory 连接设置：安全用户连接。</p> <p>通过指定为 <i>True</i>，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。</p> <p>如果用户帐户不使用安全套接字通讯，则指定为 <i>False</i>。</p>
NOVL_CONFIG_SESSIONTIMEOUT=	<p>杂项：会话超时。</p> <p>指定应用程序会话超时时间间隔。</p>
NOVL_CONFIG_LDAPPLAINPORT=	<p>eDirectory 连接设置：LDAP 非安全端口。</p> <p>为 LDAP 服务器指定非安全端口，比如 389。</p>
NOVL_CONFIG_LDAPSECUREPORT=	<p>eDirectory 连接设置：LDAP 安全端口。</p> <p>为 LDAP 服务器指定安全端口，比如 636。</p>
NOVL_CONFIG_ANONYMOUS=	<p>eDirectory 连接设置：使用公开匿名帐户。</p> <p>指定为 <i>True</i> 可以允许未登录的用户访问 LDAP 公开匿名帐户。</p> <p>指定为 <i>False</i> 则启用 NOVL_CONFIG_GUEST。</p>
NOVL_CONFIG_GUEST=	<p>eDirectory 连接设置：LDAP Guest。</p> <p>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 <i>使用公开匿名帐户</i>。身份库中必须已经存在 Guest 用户帐户。要禁用 Guest 用户，请选择 <i>使用公开匿名帐户</i>。</p>
NOVL_CONFIG_GUESTPASS=	eDirectory 连接设置：LDAP Guest 口令。
NOVL_CONFIG_EMAILNOTIFYHOST=	<p>电子邮件：通知模板 HOST 令牌。</p> <p>指定主管 Identity Manager User Application 的应用程序服务器。例如：</p> <pre>myapplication serverServer</pre> <p>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。</p>
NOVL_CONFIG_EMAILNOTIFYPORT=	<p>电子邮件：通知模板 Port 令牌。</p> <p>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。</p>
NOVL_CONFIG_EMAILNOTIFYSECUREPORT=	<p>电子邮件：通知模板 Secure Port 令牌。</p> <p>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。</p>
NOVL_CONFIG_NOTFSMTPEMAILFROM=	<p>电子邮件：通知 SMTP 电子邮件发件人。</p> <p>指定供应电子邮件中发送电子邮件的用户。</p>

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_NOTFSMTPEMAILHOST=	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。
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 <i>True</i> 。如果指定为 <i>True</i> ，则还必须提供 <i>NOVL_CONFIG_EXTPWDWARPTH</i> 和 <i>NOVL_CONFIG_EXTPWDWARRTNPATH</i> 的值。 指定为 <i>False</i> 可以使用默认的内部口令管理功能。 / <i>jsps/pwdmgt/ForgotPassword.jsf</i> (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 <i>ForgotPassword.jsf</i> 。或者接受默认的内部口令管理 WAR。有关细节，请参见 使用口令 WAR (第 59 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 <i>https:// idmhost:sslport/ idm</i> 。
NOVL_CONFIG_USEROBJECTATTRIBUTE=	Meta-Directory 用户身份：用户对象类。 LDAP 用户对象类 (通常为 <i>inetOrgPerson</i>)。
NOVL_CONFIG_LOGINATTRIBUTE=	Meta-Directory 用户身份：登录属性。 代表用户的登录名的 LDAP 特性 (比如 <i>CN</i>)。
NOVL_CONFIG_NAMINGATTRIBUTE=	Meta-Directory 用户身份：命名属性。 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。
NOVL_CONFIG_USERMEMBERSHIPATTRIBUTE =	Metadirectory 用户身份：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。
NOVL_CONFIG_GROUPOBJECTATTRIBUTE=	Meta-Directory 用户组：组对象类。 LDAP 组对象类 (通常是 <i>groupofNames</i>)。
NOVL_CONFIG_GROUPMEMBERSHIPATTRIBUTE =	Meta-Directory 用户组：组成员资格属性。 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。

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_USEDYNAMICGROUPS=	Meta-Directory 用户组：使用动态组。 要使用动态组，请指定 <i>True</i> 。否则，指定 <i>False</i> 。
NOVL_CONFIG_DYNAMICGROUPOBJECTCLASS=	Meta-Directory 用户组：动态组对象类。 指定 LDAP 动态组对象类（一般为 <i>dynamicGroup</i> ）。
NOVL_CONFIG_PRIVATESTOREPATH=	私用密钥存储区：私用密钥存储区路径。 指定包含 User Application 的私用密钥和证书的私用密钥存储区的路径。保留。如果保留为空的话，将采用默认路径 <i>/jre/lib/security/cacerts</i> 。
NOVL_CONFIG_PRIVATESTOREPASSWORD=	私用密钥存储区：私用密钥存储区口令。
NOVL_CONFIG_PRIVATEKEYALIAS=	私用密钥存储区：私用密钥别名。 别名为 <i>novellIDMUserApp</i> ，除非另行指定。
NOVL_CONFIG_PRIVATEKEYPASSWORD=	私用密钥存储区：私用密钥口令。
NOVL_CONFIG_TRUSTEDSTOREPATH=	可信密钥存储区：可信存储路径。 可信密钥存储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 <i>javax.net.ssl.trustStore</i> 中获取路径。如果那里没有路径，则假定为 <i>jre/lib/security/cacerts</i> 。
NOVL_CONFIG_TRUSTEDSTOREPASSWORD=	可信密钥存储区：可信存储口令。
NOVL_CONFIG_AUDITCERT=	Novell Audit 数字签名证书
NOVL_CONFIG_AUDITKEYFILEPATH=	Novell Audit 数字签名私用密钥文件路径。
NOVL_CONFIG_ICSSLOGOUTENABLED=	Access Manager 和 iChain 设置：已启用同时注销。 通过指定为 <i>True</i> ，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 <i>False</i> 。
NOVL_CONFIG_ICSSLOGOUTPAGE=	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 <i>\$PROTOCOL\$</i> 令牌。

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_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。

在 WebSphere Application Server 上安装

6

本部分说明如何在 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。

- ◆ 第 6.1 节 “起动安装程序 GUI” (第 69 页)
- ◆ 第 6.2 节 “选择应用程序服务器平台” (第 70 页)
- ◆ 第 6.3 节 “指定 WAR 的位置” (第 71 页)
- ◆ 第 6.4 节 “选择安装文件夹” (第 72 页)
- ◆ 第 6.5 节 “选择数据库平台” (第 73 页)
- ◆ 第 6.6 节 “指定 Java 根目录” (第 74 页)
- ◆ 第 6.7 节 “启用 Novell Audit 日志记录” (第 75 页)
- ◆ 第 6.8 节 “指定主密钥” (第 76 页)
- ◆ 第 6.9 节 “配置 User Application” (第 78 页)
- ◆ 第 6.10 节 “校验选项和安装” (第 89 页)
- ◆ 第 6.11 节 “查看日志文件” (第 89 页)
- ◆ 第 6.12 节 “添加 User Application 配置文件和 JVM 系统属性” (第 89 页)
- ◆ 第 6.13 节 “将 eDirectory 可信根导入 WebSphere 密钥存储区” (第 90 页)
- ◆ 第 6.14 节 “部署 IDM WAR 文件” (第 91 页)
- ◆ 第 6.15 节 “启动应用程序” (第 92 页)
- ◆ 第 6.16 节 “访问 User Application 门户” (第 92 页)

6.1 起动安装程序 GUI

- 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
```

注释：对于 WebSphere，必须使用应用了无限制策略文件的 IBM JDK。

- 3 从下拉菜单中选择一种语言，然后单击“确定”。



4 阅读许可证协议，单击本人接受许可证协议中的条款，然后单击下一步。



5 阅读安装向导的“简介”页，然后单击下一步。

6.2 选择应用程序服务器平台

- 1 在“应用程序服务器平台”窗口中，选择 WebSphere Application Server 平台。
- 2 选择下一步。然后继续第 6.3 节“指定 WAR 的位置”（第 71 页）。

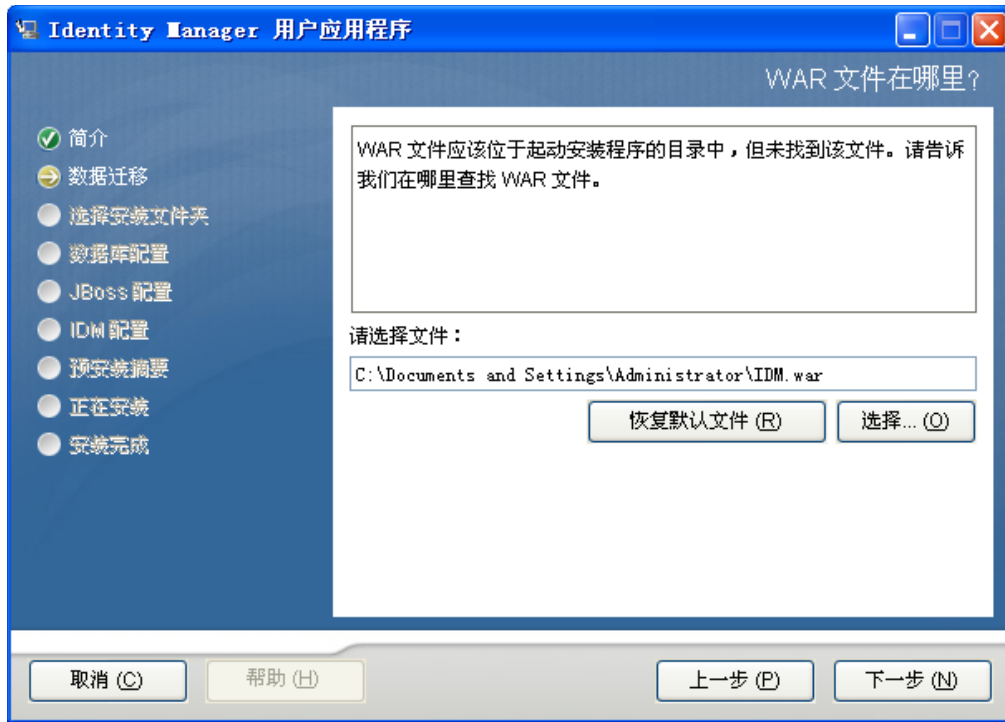


6.3 指定 WAR 的位置

完成第 6.1 节“启动安装程序 GUI”（第 69 页）中的安装过程，然后继续以下步骤：

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。

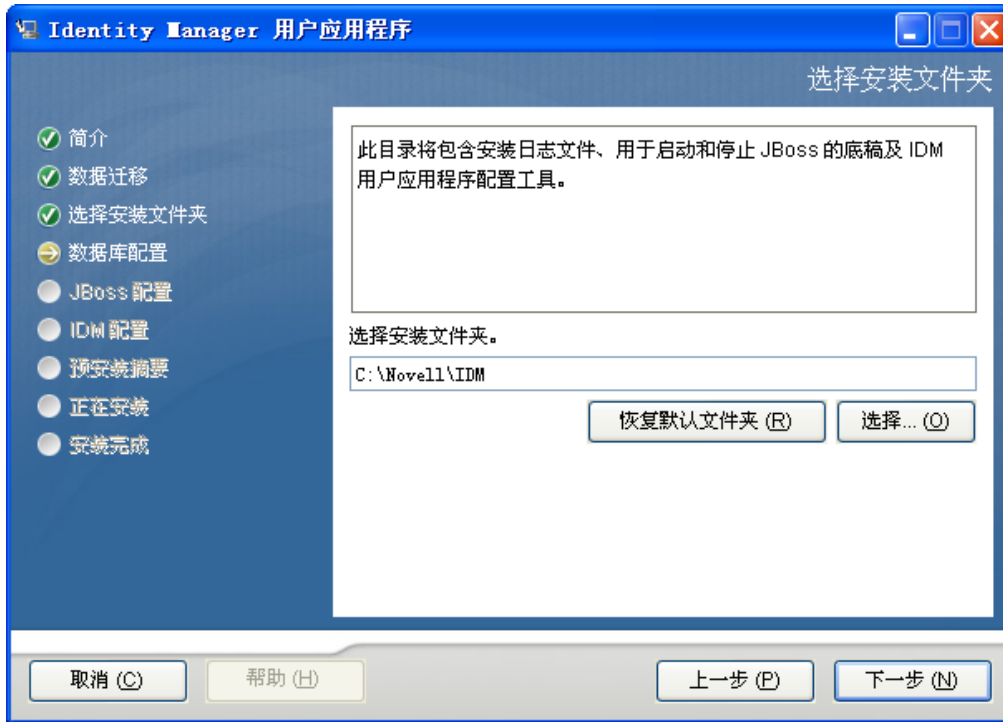
- 1 如果 WAR 在默认位置，可以单击 *恢复默认文件夹*。或者，要指定 WAR 文件的位置，单击 *选择* 并选择某个位置。



- 2 单击 **下一步**，然后继续第 6.4 节“选择安装文件夹”（第 72 页）。

6.4 选择安装文件夹

- 1 在“选择安装文件夹”页，选择安装 User Application 的位置。如果要使用默认位置，单击 **恢复默认文件夹**；如果要为安装文件选择其他位置，单击 **选择**并浏览至某个位置。



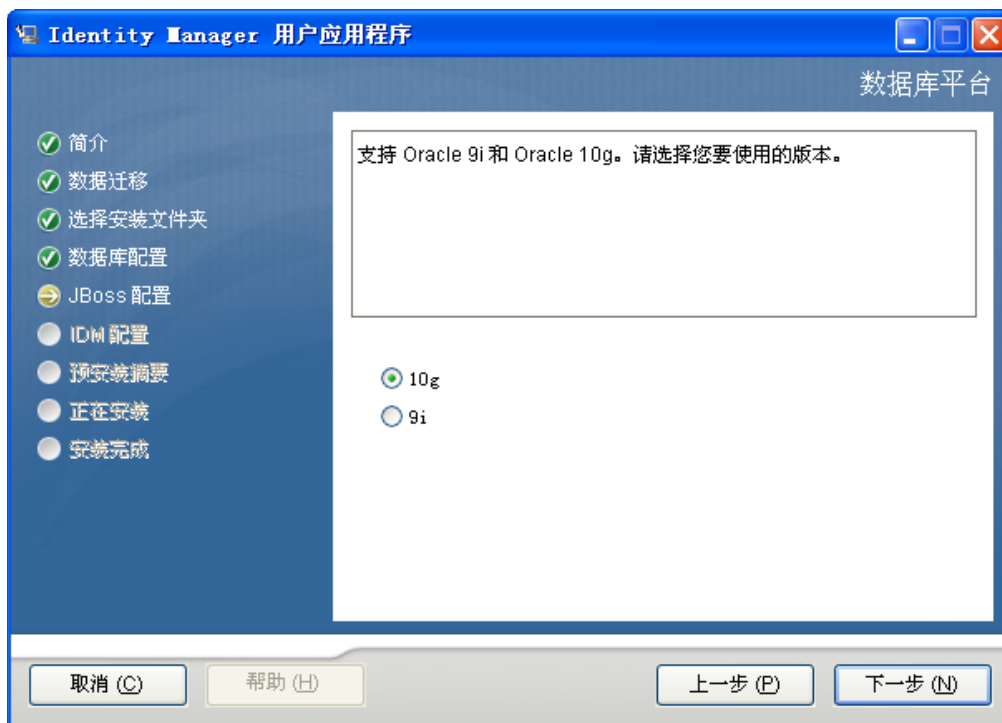
2 单击 **下一步**，然后继续第 6.5 节“选择数据库平台”（第 73 页）。

6.5 选择数据库平台

1 选择要使用的数据库平台。



- 2 如果使用的是 Oracle 数据库，请继续 [步骤 3](#)。否则，请跳至 [步骤 4](#)。
- 3 如果使用的是 Oracle 数据库，安装程序将询问所使用的版本。选择使用的版本。

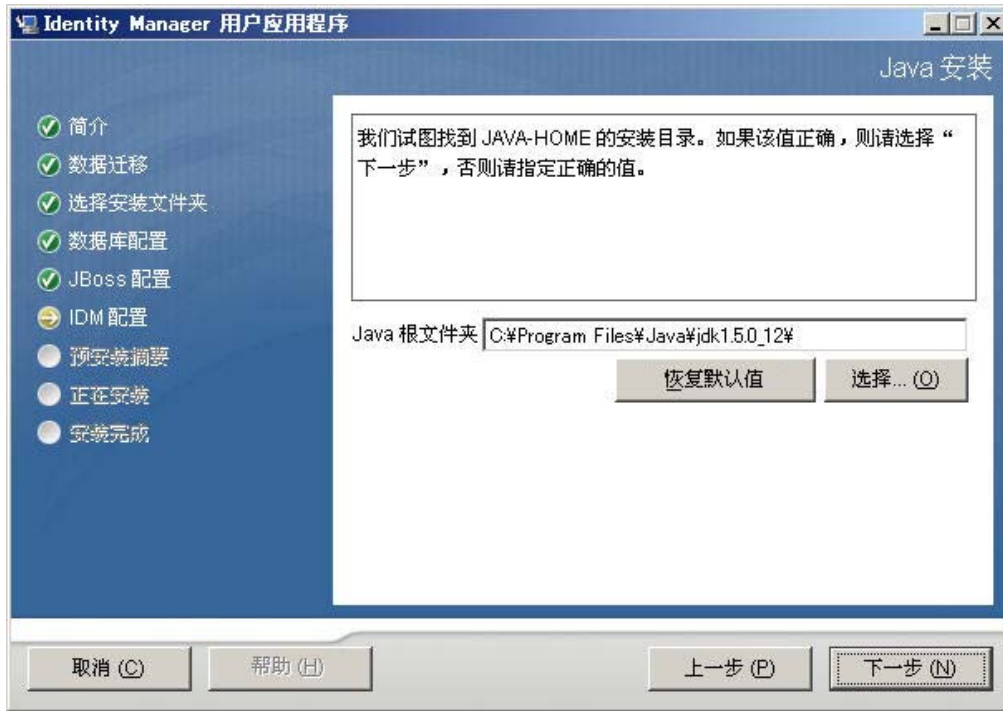


- 4 单击 [下一步](#)，然后继续 [第 6.6 节“指定 Java 根目录”](#)（[第 74 页](#)）。

6.6 指定 Java 根目录

注释：对于 WebSphere，必须使用应用了无限制策略文件的 IBM JDK。

- 1 单击 [选择](#) 浏览 Java 根文件夹。或者，要使用默认位置，请单击 [恢复默认](#)。



2 单击 **下一步**，然后继续第 6.7 节“启用 Novell Audit 日志记录”（第 75 页）。

6.7 启用 Novell Audit 日志记录

要启用 User Application 的 Novell[®] Audit 日志记录（可选），请执行下列操作：

1 填写以下字段：



选项	说明
关	对 User Application 禁用 Novell Audit 日志记录。以后可以使用 User Application 的 <i>管理</i> 选项卡来启用该功能。 有关启用 Novell Audit 日志记录的更多信息，请参见《 <i>Identity Manager User Application：管理指南</i> 》。
等于	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，请参见《 <i>Identity Manager User Application：管理指南</i> 》。
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。

2 单击 **下一步** 并继续第 6.8 节“指定主密钥”（第 76 页）。

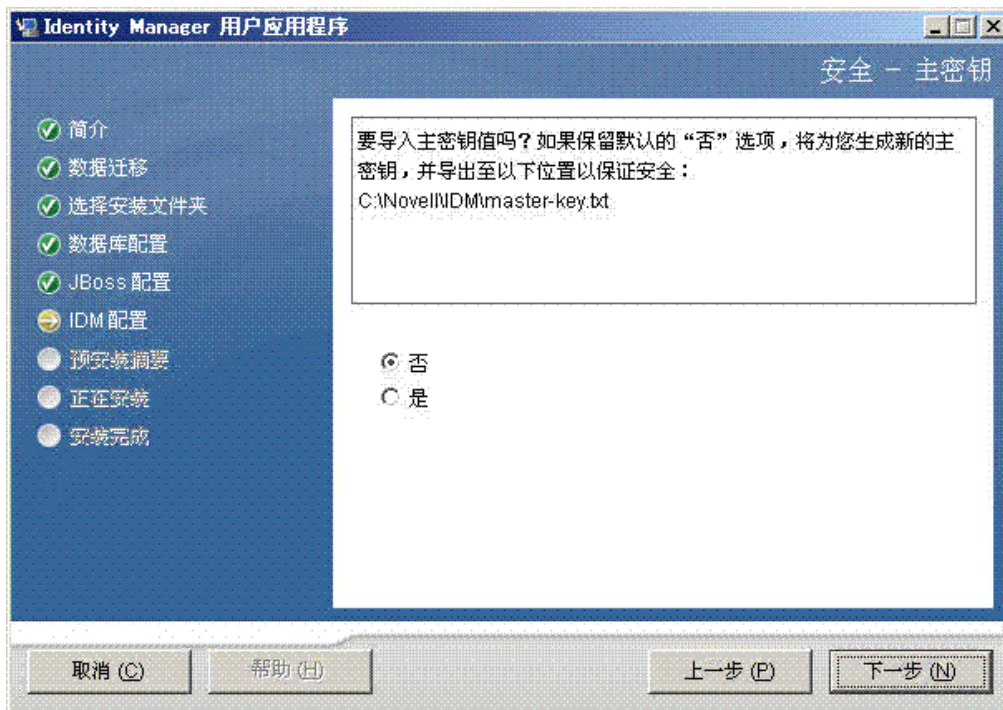
6.8 指定主密钥

指定是要导入现有主密钥还是新建主密钥。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。这样可以获得以前存储的加密数据的访问权。

1 单击是导入现有主密钥，或者单击否新建主密钥。



2 单击下一步。

安装过程中会将经过加密的主密钥写到安装目录中的 master-key.txt 文件中。

如果选择否，跳至第 6.9 节“配置 User Application”（第 78 页）。完成安装后，必须手动记录主密钥。如果选择是，则继续步骤 3（第 77 页）。

3 如果选择导入现有经过加密的主密钥，请将密钥剪切和粘贴到安装过程窗口。

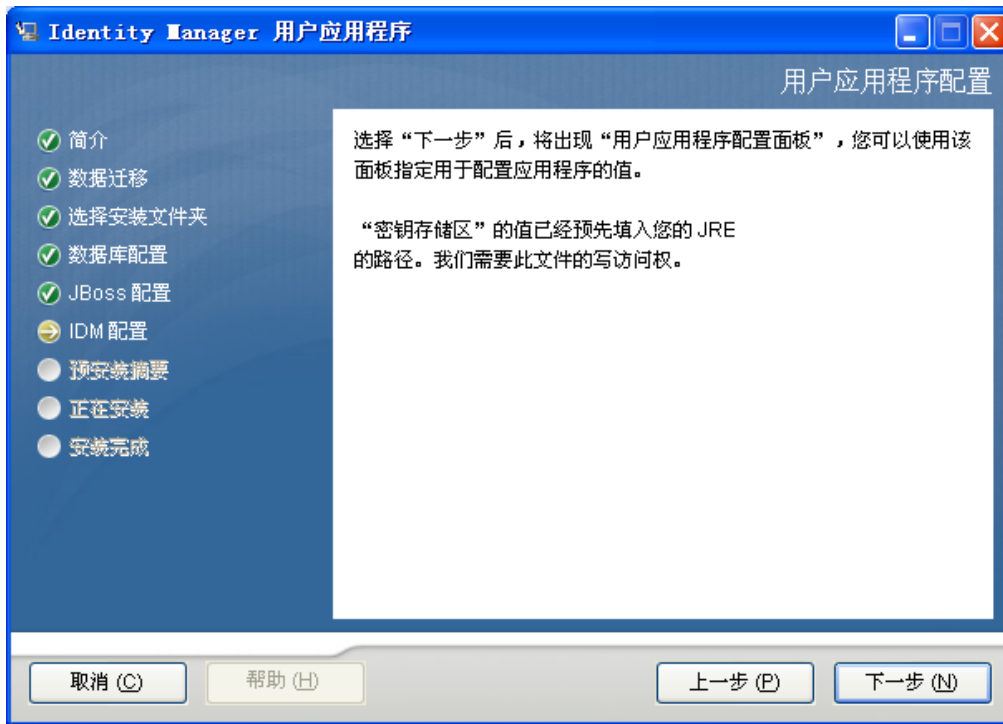


4 单击 *下一步* 并继续第 6.9 节 “配置 User Application” (第 78 页)。

6.9 配置 User Application

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后在 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。

1 单击 *下一步* 完成首个 “User Application 配置” 页。



- 2 设置基本 User Application 配置参数（参见表 表 6-1 在第 81 页 中的说明），然后继续步骤 3。

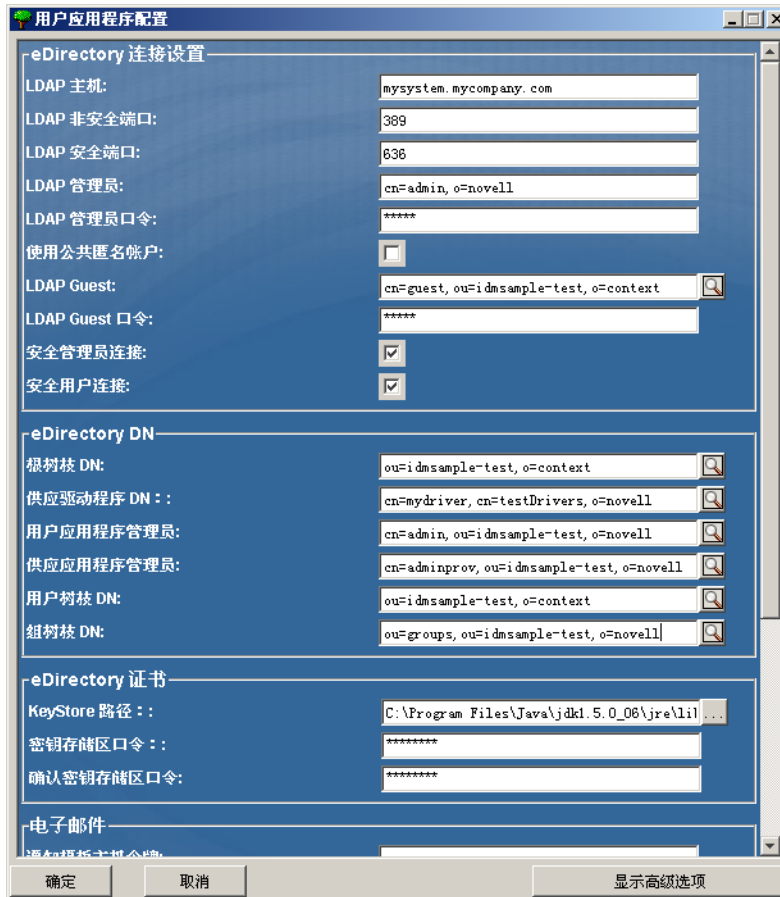


表 6-1 User Application 配置: 基本参数

设置类型	字段	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。
	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 <i>使用公开匿名帐户</i> 。要禁用 Guest 用户，请选择 <i>使用公开匿名帐户</i> 。
	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	字段	说明
eDirectory DN	<i>根容器 DN</i>	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。
	<i>供应驱动程序 DN</i>	必需。指定 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
	<i>User Application Admin</i>	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 <i>管理</i> 选项卡管理门户。 如果 User Application 管理员参与 iManager、Designer for Identity Manager 或 User Application (<i>请求和批准</i> 选项卡) 中显示的 workflow 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，请参见《IDM 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 <i>管理 > 安全</i> 页面。
	<i>供应应用程序 Admin</i>	供应应用程序管理员使用 <i>供应</i> 选项卡 (<i>管理</i> 选项卡下) 管理供应 workflow 功能。用户可以通过 User Application 的 <i>请求和批准</i> 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 <i>管理 > 安全</i> 页面。
eDirectory DN (续)	<i>角色管理员</i>	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，授予或撤销指派给任何用户、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 <i>角色 > 角色指派</i> 页面。
	<i>用户容器 DN</i>	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。 <hr/> 重要： 如果要使用该用户能够执行 workflow，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。 <hr/>

设置类型	字段	说明
eDirectory 证书	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。
	密钥存储区路径	必需。指定应用程序服务器用于运行的、JDK 密钥存储区 (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。
电子邮件	密钥存储区口令 / 确认密钥存储区口令	必需。指定 cacerts 口令。默认值为 changeit。
	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： <code>myapplication serverServer</code> 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连接。
	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 <i>使用外部口令 WAR</i> ，则必须提供 <i>忘记口令链接</i> 和 <i>忘记口令返回链接</i> 的值。 如果没有选择 <i>使用外部口令 WAR</i> ，则 IDM 将使用默认的内部口令管理功能。 <code>/jsps/pwdmgt/ForgotPassword.jsf</code> (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 <code>ForgotPassword.jsf</code> 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 <code>https://idmhost:sslport/idm</code> 。

- 3 如果要设置其他 User Application 配置参数，请单击 *显示高级选项*。（通过滚动查看整个面板。）表 6-2 在第 84 页 说明了“高级选项”参数。如果不想设置此步骤中所述的其他参数，请跳至 **步骤 4**。

表 6-2 User Application 配置：所有参数

设置类型	字段	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 <i>使用公开匿名帐户</i> 。要禁用 Guest 用户，请选择 <i>使用公开匿名帐户</i> 。
	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	字段	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。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 workflow 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，请参见《IDM 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。
	供应应用程序 Admin	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 workflow 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。
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。 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。 <hr/> 重要： 如果要使用该用户能够执行 workflow，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。 <hr/>
	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	字段	说明
	<i>角色管理员</i>	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，授予或撤销指派给任何用户、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 <i>角色 > 角色指派</i> 页面。
Metadirectory 用户组	<i>组容器 DN</i>	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。
	<i>组对象类</i>	LDAP 组对象类 (通常是 groupofNames)。
	<i>组成员资格特性</i>	代表用户组成员资格的特性。不要在该名称中使用空格。
	<i>使用动态组</i>	如果需要使用动态组，请选择该选项。
	<i>动态组对象类</i>	LDAP 动态组对象类 (一般 dynamicGroup)。
eDirectory 证书	<i>密钥存储区路径</i>	必需。指定应用程序服务器用于运行的、JRE 的密钥存储区 (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存储区文件。在 Linux 或 Solaris 上，用户必须具有写此文件的权限。
	<i>密钥存储区口令</i>	必需。指定 cacerts 口令。默认值为 changeit。
	<i>确认密钥存储区口令</i>	
私有密钥存储区	<i>私有密钥存储区路径</i>	私有密钥存储区包含 User Application 的私有密钥和证书。保留。如果保留为空的话，将采用默认路径 /jre/lib/security/cacerts。
	<i>私有密钥存储区口令</i>	口令为 changeit，除非另行指定。此口令已使用主密钥进行过加密。
	<i>私有密钥别名</i>	别名为 novellIDMUserApp，除非另行指定。
	<i>私有密钥口令</i>	口令为 novellIDM，除非另行指定。此口令已使用主密钥进行过加密。
可信密钥存储区	<i>可信存储区路径</i>	可信密钥存储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。
	<i>可信存储口令</i>	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。

设置类型	字段	说明
Access Manager 和 iChain 设置	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。
	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。
电子邮件	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。
	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连接。
	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。	

设置类型	字段	说明
口令管理	<i>使用外部口令 WAR</i>	<p>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。</p> <p>如果选择 <i>使用外部口令 WAR</i>，则必须提供 <i>忘记口令链接</i> 和 <i>忘记口令返回链接</i> 的值。</p> <p>如果没有选择 <i>使用外部口令 WAR</i>，则 IDM 将使用默认的内部口令管理功能。/jsps/pwdmgmt/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。</p>
	<i>忘记口令链接</i>	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。
	<i>忘记口令返回链接</i>	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:// <i>idmhost:sslport/idm</i> 。
杂项	<i>会话超时</i>	应用程序会话超时。
	<i>OCSP URI</i>	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。
	<i>授权配置路径</i>	授权配置文件的完全限定名。
	<i>创建 eDirectory 索引</i> <i>服务器 DN</i>	
容器对象	<i>所选</i>	选择要使用的每个数字对象类型。
	<i>容器对象类型</i>	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 <i>添加新容器对象</i> 下面添加这些容器。
	<i>容器特性名称</i>	列出与容器对象类型相关的特性类型名称。
	<i>添加新的容器对象：容器对象类型</i>	<p>指定可作为容器的身份库中的对象类的 LDAP 名称。</p> <p>有关容器的信息，请参阅《<i>Novell iManager 2.6 管理指南</i> (http://www.novell.com/documentation/imanager26/pdfdoc/imanager_admin_26/imanager_admin_26.pdf)》。</p>
	<i>添加新的容器对象：容器特性名称</i>	提供容器对象的特性名称。

4 完成设置配置之后，单击 *确定*，然后继续第 6.10 节“*校验选项和安装*”（第 89 页）。

6.10 校验选项和安装

- 1 阅读“安装前摘要”页，校验所选择的安装参数。
- 2 如有必要，使用 *后退* 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。
- 3 当安装和配置参数满意之后，返回“安装前摘要”页，然后单击 *安装*。



6.11 查看日志文件

如果安装成功完成，没有错误，请继续第 6.12 节“添加 User Application 配置文件和 JVM 系统属性”（第 89 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。

6.12 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。

注释： 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。

6.13 将 eDirectory 可信根导入 WebSphere 密钥存储区

- 1 User Application 安装过程将 eDirectory™ 可信根证书导出到安装 User Application 的目录。将这两个证书复制到主管 WebSphere 服务器的计算机。
- 2 将证书导入到 WebSphere 密钥存储区中。可以使用 WebSphere 管理员控制台 ([通过 WebSphere 管理员控制台导入证书 \(第 90 页\)](#)) 或通过命令行 ([通过命令行导入证书 \(第 91 页\)](#)) 执行此操作。
- 3 导入证书后，继续执行第 6.14 节“[部署 IDM WAR 文件 \(第 91 页\)](#)”。

6.13.1 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 *密钥存储区和证书*。
- 4 选择 *节点默认信任存储区*（或正在使用的信任存储区）。
- 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。

6.13.2 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 密钥存储区中。

注释：需要使用 WebSphere 密钥工具，否则此操作不起作用。此外，应确存储区类型为 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。

6.14 部署 IDM WAR 文件

- 1 作为管理员用户登录到 WebSphere 管理控制台。
- 2 从左面板中，转到应用程序 > 安装新应用程序。
- 3 浏览到 IDM War 文件的位置。

IDM WAR 文件在安装 User Application 期间配置。该文件位于您在安装 User Application 期间指定的 User Application 安装目录中。
- 4 为应用程序键入环境根，例如 IDMPProv。这是 URL 路径。
- 5 选中单选按钮 *只有在需要附加信息时提示我*。然后，单击下一步转到选择安装选项页面。
- 6 接受此页的所有默认值，然后单击下一步转到将模块映射到服务器页面。
- 7 接受此页的所有默认值，然后单击下一步转到将资源参照映射到资源页面。
- 8 对于鉴定方法，选择 *使用默认方法* 复选框。然后，在 *鉴定数据项* 下拉列表中选择以前创建的别名，例如， MyServerNode01/MyAlias。
- 9 在鉴定设置下方的表中，找到要部署的模块。在标题为目标资源 JNDI 名称的列下，单击浏览按钮指定一个 JNDI 名称。将显示一个资源列表。选择先前创建的数据源，然后单击 *应用* 按钮返回到将资源参照映射到资源页，（例如， MyDataSource）。
- 10 选择下一步转到映射万维网模块的虚拟主机。
- 11 接受此页的所有默认值，然后选择下一步转到摘要页面。
- 12 选择 *完成* 完成部署。
- 13 部署完成后，单击 *保存* 以保存更改。
- 14 继续第 6.15 节“启动应用程序”（第 92 页）。

6.15 启动应用程序

- 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。

6.16 访问 User Application 门户

- 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`

安装后任务

本部分说明安装后任务。包括以下主题：

- ◆ 第 7.1 节 “记录主密钥”（第 93 页）
- ◆ 第 7.2 节 “安装后配置”（第 93 页）
- ◆ 第 7.3 节 “检查群集安装”（第 93 页）
- ◆ 第 7.4 节 “在 JBoss 服务器间配置 SSL 通讯”（第 94 页）
- ◆ 第 7.5 节 “访问外部口令 WAR”（第 94 页）
- ◆ 第 7.6 节 “升级忘记口令设置”（第 94 页）
- ◆ 第 7.7 节 “设置电子邮件通知”（第 94 页）
- ◆ 第 7.8 节 “测试安装在 JBoss Application Server 上”（第 95 页）
- ◆ 第 7.9 节 “设置供应小组和请求”（第 95 页）
- ◆ 第 7.10 节 “在 eDirectory 中创建索引”（第 96 页）
- ◆ 第 7.11 节 “安装后重配置 IDM WAR 文件”（第 96 页）
- ◆ 第 7.12 节 “查错”（第 96 页）

7.1 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。

7.2 安装后配置

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 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 设计指南》

7.3 检查群集安装

在 JBoss 群集中，确保群集中每个应用程序服务器都包含以下项：

- ◆ 唯一分区名（分区名称）
- ◆ 唯一分区 UDP（partition.udpGroup）

- ◆ 唯一工作流程引擎 ID
- ◆ 同一 WAR 文件。安装过程中，默认情况下，WAR 被写到 jboss\server\IDM\deploy 目录。

在 WebSphere 群集中，确保群集中每个应用程序服务器都有唯一的工作流程引擎 ID。

有关详细信息，请参见《*Identity Manager User Application: 管理指南* (<http://www.novell.com/documentation/idmrbpm36/index.html>)》第 4 章中关于“群集”的部分。

7.4 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，请参见 JBoss 文档。

7.5 访问外部口令 WAR

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。

7.6 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>)

7.7 设置电子邮件通知

要实施“忘记口令”和“工作流程电子邮件通知”功能：

- 1 在 iManager 中，在“角色和任务”下面，选择 *工作流程管理*，然后选择 *电子邮件服务器选项*。
- 2 在 *主机名* 下面指定 SMTP 服务器的名称。
- 3 在 *收件人* 旁边，指定一个电子邮件地址 (比如 *noreply@novell.com*)，然后单击 *确定*。

7.8 测试安装在 JBoss Application Server 上

- 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)
```

如果需要停止应用程序服务器，请使用 `stop-jboss.sh` 或 `stop-jboss.bat`，或关闭 `start-jboss.sh` 或 `start-jboss.bat` 正在运行的窗口。

如果不是在 X11 Window 系统上运行，则需要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。应用程序名称在安装过程中提供应用程序服务器配置信息时指定。

会显示 Novell Identity Manager User Application 主页。

- 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 7.12 节“*查错*”（第 96 页）。

7.9 设置供应小组和请求

设置供应小组和供应小组请求以启用工作流程任务。有关指导，请参见《*Identity Manager User Application: 管理指南* (<http://www.novell.com/documentation/idmrpbm36/index.html>)》。

7.10 在 eDirectory 中创建索引

为改进 IDM User Application 的性能，eDirectory 管理员必须创建 manager、ismanager 和 srvprvUUID 特性的索引。如果没有这些特性的索引，User Application 用户可能会遇到不良性能，尤其在群集环境中。有关使用 Index Manager 创建索引的说明，请参考《Novell eDirectory 管理指南 (<http://www.novell.com/documentation>)》。

7.11 安装后重配置 IDM WAR 文件

要更新 IDM WAR 文件：

- 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，请参阅表 4-2 在第 54 页、表 5-1 在第 62 页 或表 6-2 在第 84 页。

- 2 将新 WAR 文件部署到应用程序服务器。

7.12 查错

Novell 代表将会帮您解决遇到的任何安装和配置问题。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： <ul style="list-style-type: none">◆ 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： <pre>configupdate.sh</pre> 在 Windows 上，从安装目录（默认为 c:\opt\novell\idm）运行以下命令： <pre>configupdate.bat</pre>
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 安装中所指定的 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。	<p>请不要以 root 身份运行。(然而，如果您运行随 Identity Manager 提供的 MySQL 版本，几乎不会出现此问题。)</p> <p>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 <code>/idm/mysql/start-mysql.sh</code>，然后运行 <code>/idm/start-jboss.sh</code>。</p> <p>在文本编辑器中检查 <code>/idm/mysql/setup-mysql.sh</code>，并纠正任何可疑的值。然后运行底稿，再运行 <code>/idm/start-jboss.sh</code>。</p>
启动应用程序服务器时遇到密钥存储区错误。	<p>应用程序服务器没有运行在安装 User Application 时所指定的 JDK。</p> <p>使用 <code>keytool</code> 命令导入证书文件：</p> <pre>keytool -import -trustcacerts -alias aliasName -file certFile -keystore ..\lib\security\cacerts -storepass changeit</pre> <ul style="list-style-type: none"> ◆ 使用为该证书选择的唯一名称替换 <code>aliasName</code>。 ◆ 使用证书文件的完整路径和名称替换 <code>certFile</code>。 ◆ 默认的密钥存储区口令为 <code>changeit</code> (如果有其他口令，请指定)。
没有发送电子邮件通知。	<p>通过运行 <code>configupdate</code> 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”。</p> <p>在 Linux 或 Solaris 上，从安装目录 (默认为 <code>/opt/novell/idm</code>) 运行以下命令：</p> <pre>configupdate.sh</pre> <p>在 Windows 上，从安装目录 (默认为 <code>c:\opt\novell\idm</code>) 运行以下命令：</p> <pre>configupdate.bat</pre>