Novell Identity Manager

3.0

www.novell.com

安装指南

2006 年 4 月 19 日

Novell®

法律声明

Novell, Inc. 对本文档的内容或使用不做任何声明或保证，特别是对用于任何具体目的的适销性或适用性不做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，并且没有义务将这类修改通知任何个人或实体。

Novell, Inc. 对任何软件不做任何声明或保证，特别是对用于任何具体目的的适销性或适用性不做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，并且没有义务将这类修改通知任何个人或实体。

本 《许可协议》中提供的任何产品或技术信息可能受美国出口管制规定和其它国家 / 地区的贸易法制约。您已经同意遵守所有的出口控制法规，并同意在出口、再出口或进口可交付产品之前取得任何必要的许可证或分类证书。您已经同意不向目前的美国出口排除列表上的国家 / 地区或组织或者向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 / 地区进行出口或再出口。您已经同意不将可交付产品用于禁止的核、导弹或生物化学武器的终端使用。有关出口 Novell 软件的详细信息，请参考 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。特别是，这些知识产权包括但不限于 http://www.novell.com/company/legal/patents/ 列出的一项或多项美国专利，以及在美国和其它国家 / 地区的一项或多项其它专利或申请中的专利。

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

联机文档：要访问本产品和其它 Novell 产品的联机文档或获取产品的更新，请参见 Novell 联机文档 (http://www.novell.com/documentation)。

Novell 商标

DirXML 是 Novell, Inc. 在美国和其它国家 / 地区的注册商标。
eDirectory 是 Novell, Inc. 的商标。
exteNd 是 Novell, Inc. 的商标。
exteNd Director 是 Novell, Inc. 的商标。
GroupWise 是 Novell, Inc. 在美国和其它国家 / 地区的注册商标。
NDS 是 Novell, Inc. 在美国和其它国家 / 地区的注册商标。
NetWare 是 Novell, Inc. 在美国和其它国家 / 地区的注册商标。
NMAS 是 Novell, Inc. 的商标。
Novell 是 Novell, Inc. 在美国和其它国家 / 地区的注册商标。
Novell Certificate Server 是 Novell, Inc. 的商标。
Novell Client 是 Novell, Inc. 的商标。
SUSE 是 SUSE AG （Novell 控股公司）的注册商标。

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

Novell® Identity Manager （以前称 DirXML® ）是一种数据共享和同步服务，应用程序、目录和数据库可以使用它来共享信息。它可以链接分散的信息；发生身份更改后，还可以使用它来建立策略，用于控制对指定系统的自动更新。Identity Manager 为帐户供应、安全性、一次签到、用户自助服务、鉴定、授权、自动工作流程和万维网服务提供了基础。它允许您集成、管理和控制分布式身份信息，以便将正确的资源安全地递送给适当的人员。

本指南概述了 Identity Manager 技术，同时介绍了安装、管理和配置功能。

本指南包括：

文档更新

有关本文档的最新版本，请参见 Identity Manager 文档万维网站点 (http://www.novell.com/documentation/idm/index.html)

文档约定

在本文档中，大于号 (>) 用于分隔同一步骤中的各项操作，以及交叉参照路径中的各个项目。

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

概述

1

1.1 Identity Manager 简介

Novell® Identity Manager 3 是屡获殊荣的数据共享和同步解决方案，它革新了数据的管理方式。该服务利用集中式数据储存 （即 Identity Vault）在应用程序、数据库和目录之间同步、转换和分发信息。

当一个系统中的数据发生更改时， Identity Manager 包含的 Metadirectory 引擎将会根据定义的业务规则检测这些更改，并将这些更改传播到其它已连接系统。使用此解决方案，可对任何特定数据段强制使用授权数据源 （例如， HR 应用程序拥有用户的 ID，而讯息交换系统可能拥有用户的电子邮件帐户信息）。

通过 Identity Manager，已连接系统 （例如 SAP*、 PeopleSoft*、 Lotus Notes*、 Microsoft* Exchange、 Active Directory* 等等）可实现下列目的：

- 与 Identity Vault 共享数据。
- 在已连接系统中修改共享的数据后，与 Identity Vault 同步和转换此数据。
- 在 Identity Vault 中修改共享的数据后，与已连接系统同步和转换此数据。

Identity Manager 通过提供一个双向框架来实现此目的，而管理员可使用该框架指定哪些数据从 Identity Vault 流向应用程序，以及哪些数据从应用程序流向 Identity Vault。该框架使用 XML 来提供数据和事件转换功能，将 Identity Vault 数据和事件转换为指定的应用程序特定的格式。它还将应用程序特定的格式转换为可以被 Identity Vault 识别的格式。与应用程序的所有交互都是使用该应用程序本身的 API 进行的。

使用 Identity Manager 可以只选择与相关已连接系统特定的记录和字段相对应的特性和类。例如，目录数据库可以选择只与人力资源数据库共享用户类型对象，而不共享网络资源对象，例如服务器、打印机和卷。同样，人力资源数据储存也可以只与目录数据储存共享用户的名字、姓氏、姓名首字母、电话号码和工作地点，但不共享用户的家庭成员信息和工作经历。

如果 Identity Vault 中没有用于要与其它应用程序共享的数据的类或特性，则可以通过扩展 eDirectory 纲要将其加入。在这种情况下， Identity Vault 就成为一个储存其不需要的信息的库，但其它应用程序可以使用这些信息。应用程序特定的数据储存只维护用来储存该应用程序所需信息的库。

Identity Manager 可以完成下列任务：

- 使用事件截获 Identity Vault 中发生的更改。

- 如同集线器那样将所有数据集中在一起，从而实现数据管理的集中或分发。
- 以 XML 格式显示目录数据，以便 XML 应用程序或通过 Identity Manager 集成的应用程序可以使用和共享这些数据。
- 使用特定过滤器来管理系统中定义的数据要素，从而控制数据流。
- 使用许可权限和过滤器实施授权数据源。
- 将规则应用到 XML 格式的数据储存数据。当更改流经 Identity Manager 时，这些规则将会控制数据的解释和转换。
- 将数据从 XML 格式转换为几乎任何一种数据格式。这使 Identity Manager 能够与任何应用程序共享数据。
- 精心维护 Identity Vault 对象与其它所有集成系统内的对象之间的关联，以确保所有已连接系统能够适当地反映数据发生的更改。

使用 Identity Manager，企业可以简化 HR 过程，减少数据管理成本，通过自定义程度较高的服务建立客户关系，以及消除对成功产生约束的互操作性障碍。下面是通过 Identity Manager 实施的某些示例活动：

表 ***1-1*** *Identity Manager* 的功能

活动	Identity Manager 解决方案
管理用户帐户	通过单一操作： Identity Manager 几乎立即可以授予或去除某个员工对资源的访问权限。 Identity Manager 提供自动员工供应功能，用于向新员工指定对网络、电子邮件、应用程序、资源等的访问权限。 Identity Manager 还可以针对辞职或离职限制或禁用访问权限。
跟踪和集成资产库存	Identity Manager 可以将所有资产库存项目 （计算机、监视器、电话、库资源、椅子、桌子等）的简报添加到 Identity Vault，并将这些简报与个人、部门或组织等用户简报集成。
自动创建白页 / 黄页目录	Identity Manager 可以使用不同级别的信息创建统一的目录，以供内部和外部使用。外部目录可能只包括电子邮件地址；内部目录可能包括位置、电话号码、传真号码、手机号码、住宅地址等等。
增强用户简报	Identity Manager 通过添加或同步电子邮件地址、电话号码、住宅地址、喜好、报告关系、硬件资产、电话、钥匙、库存等信息来增加用户简报。
统一通讯访问权限	Identity Manager 可以简化各个用户或组的网络、电话、寻呼机、万维网或无线访问权限，方法是将每种通讯的目录同步到一个通用的管理界面。
加强合作伙伴关系	Identity Manager 可以加强合作伙伴关系，方法是在防火墙以外的合作伙伴系统中创建简报 （员工、客户等），使合作伙伴能够按需提供即时服务。
改善供应链	Identity Manager 可通过识别和合并每个客户的多个帐户的实例来改善客户服务。

活动	Identity Manager 解决方案
建立客户忠诚度	由于可以查看事先隔离在独立应用程序或区域中的一个位置的数据，因此， Identity Manager 可以在识别客户需求后提供新的服务。
自定义服务	Identity Manager 可以为用户 （员工、客户、合作伙伴等）提供使用已同步信息 （包括关系、状态和服务记录）完成的简报。 这些简报可用于提供对服务和信息的不同级别的访问权限，以及根据客户的信誉提供实时和自定义的服务。

1.2 术语的更改

下列术语与以前的发行版相比有所更改：

表 *1-2* 术语的更改

以前的术语	新术语
DirXML®	Identity Manager
DirXML 服务器	Metadirectory 服务器
DirXML 引擎	Metadirectory 引擎
eDirectory	Identity Vault （指 eDirectory 特性或类时则例外）

1.3 Identity Manager 3 有哪些新功能？

Identity Manager 3 有以下新功能：

- “Designer for Identity Manager”在第 7 页
- “基于工作流程的供应的权利以及对基于职能的权利的增强”在第 10 页
- “Novell Identity Manager 用户应用程序和基于工作流程的供应”在第 11 页
- “Novell 身份凭证供应策略”在第 11 页

1.3.1 Designer for Identity Manager

Identity Manager 3 包括一个极其灵活且功能强大的建模工具，即 Designer 1.2。Designer 是一个独立的客户应用程序，可用于在高生产力环境中设计、部署和记录基于 Identity Manager 的解决方案。

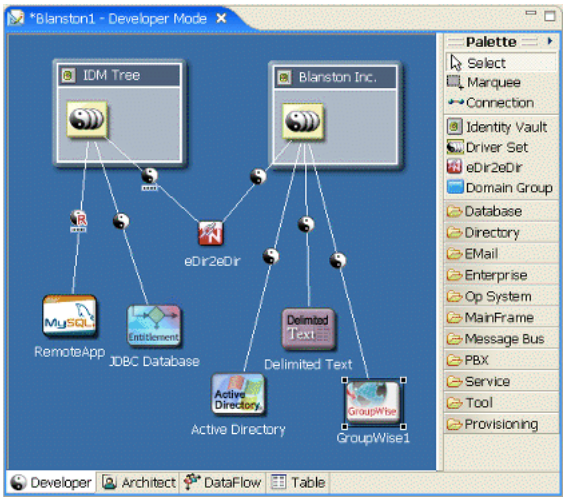
使用 Designer 可执行下列操作：

- 在本地设计解决方案，对其进行测试，然后将其部署到网络。
- 将网络中现有的解决方案导入到 Designer，并对其进行操作。
- 与部署的解决方案交互，以更新任何设置，及查看任何驱动程序或系统的状态。

Designer 具有 Novell iManager 提供的大多数配置功能，此外还具有设计程序的多种新功能和优势。可以在 Designer 中执行的某些任务包括：

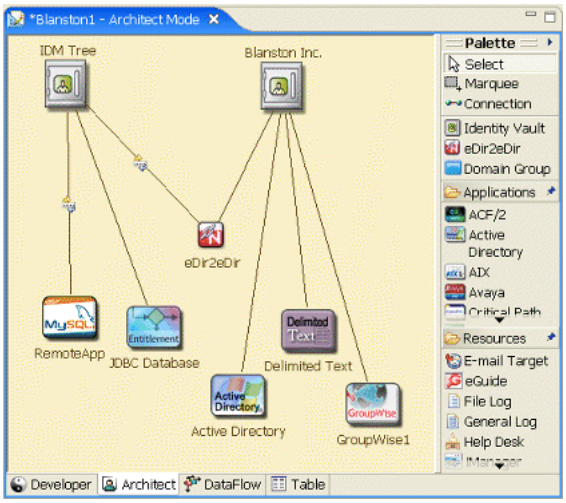
- 使用所有的 Identity Manager 组件、终端系统和应用程序及其它视觉要素，并通过强大的建模功能为企业创建身份管理的整体流程图。将系统组织成组，从而将整体流程图划分为较小的连接图。平移、扫描和缩放。按以往不可能的方法，对连接到一个系统的应用程序子系统、 eDir 对 eDir 和多个驱动程序建模。

图 ***1-1*** 在 *Designer* 中轻松创建整体流程图



- 以高级别设计师或低级别开发者的身份按不同的方式工作，并且可以方便地从一个方式转换为另一个方式。

图 ***1-2*** 选择开发者模式或设计师模式



- 直观地查看和控制数据在整个企业内的流动方式。
- 只需按下按钮，便可以使用所有系统的详细表、图表和图形来编制解决方案文档。可以记录策略、纲要、 Identity Manager 组件、自定义内容和项目信息 （包括目录、附录和页码）。可以自由定义文档的内容和格式。
- 使用内置的策略模拟器和 Identity Manager 引擎以脱机方式测试策略。

- 方便地创建、复制、移动和共享跨越整个企业的项目。由于项目就在本地，并且基于现场，因此可以方便地备份整个解决方案并对其设置版本。
- 使用项目范围内的即时搜索功能和编辑功能。
- 在具有本机感观的高生产力富客户机环境中工作。
- 外出期间在未连线的移动环境中方便地工作
- 使用功能强大的视觉编辑器、最小的弹出窗口以及充分同步的视图，从而能最大程度地提高生产力。
- 使用向导帮助自己入门和配置项目。
- 自动创建对象、自动值、自动连接和自动布局。
- 在编辑器内部和编辑器之间使用功能强大的复制 / 粘贴功能，以及在大多数编辑器和视图中使用完整的复原 / 重做功能。
- 设置多个自选设置和选项，以针对您使用本产品的方式定制 UI。
- 通过上下文相关的帮助以及强大的可搜索帮助系统来获取帮助。
- 自动更新安装功能可就任何更新向您发出通知，并且可以方便地将这些更新纳入系统。

Designer 还附带了许多可供开发者使用的功能：

- 可以方便地添加发运版本中未包含的某个项目并对其建模。例如，可以添加自己的应用程序、驱动程序、资源和图标。
- 可以配置 Designer 以使用不同的编辑器。配置所有文件类型 （例如 .xml 和 .txt）以使用选择的编辑器。基于 Eclipse 的编辑器工作状况最佳，但是您也可以加入各种软件生成物 （例如字处理文档和电子表格）。如果平台支持本机编辑器，本机编辑器将自动集成到 Designer。
- 可以在 Java 中开发和调试。如果将 Designer 插件安装为一个完整的 Eclipse 安装，则可以执行 Java 开发和调试，以及 ANT、 C# 和 UML 建模，而所有工作都可以使用 Designer 提供的相同工具。对于希望将所有工具放在一起的 Identity Manager 驱动程序编写者 （Java 或 C）来说，这种功能特别有价值。
- 可以使用公共 API。Novell 使用完全公开的公共 Eclipse API、在格式上符合开放式工业标准的基础项目数据模型，以及公开的 Eclipse 扩展点。

目标用户

Designer 是针对下列目标用户创建的：

- 企业 IT 开发者
- 顾问
- 销售工程师
- 设计师或系统设计人员
- 系统管理员

此工具供符合下列条件的信息技术专业人员使用：

- 全面了解目录、数据库及其信息环境
- 担任基于身份的解决方案的设计人员或设计师角色

要完全利用此工具的各个方面，您不需要是开发者或程序员。我们为开发者提供了许多功能，以便他们根据自己的需求扩展此工具。通过向导可以轻松地了解该工具，以及将它方便

地用于构建身份管理解决方案。经验丰富的用户可以绕过向导，以任何细节级别直接与系统交互。

还可以将 Designer 用作一种有效且有价值的工具，以帮助与组织中的战略性决策者沟通有关主要身份解决方案概念和设计的问题。可以使用可视建模程序以及能够截取和显示 Designer 数据的文档。

Designer 与 iManager 工具有哪些相关性

iManager 主要用于管理。将会使用用于管理和监视已部署解决方案的新功能持续更新 iManager。 iManager 的基于万维网的环境始终具有以下优势：

- 远程访问
- 集中式管理
- 支持职能
- 与其它基于万维网的工具集成

iManager 和 Designer 有相似之处，但是，已针对各自的目标用户和环境优化了各自的功能和最终用户体验。两者相互兼容。可以将一个应用程序中的信息 （例如驱动程序集或驱动程序）导出到另一个应用程序。同时，某些主要和常用的用户界面要素相类似，以便您可以在工具之间有效地转移。

1.3.2 基于工作流程的供应的权利以及对基于职能的权利的增强

Identity Manager 可用于同步已连接系统之间的数据。使用权利可以为个人或组设置准则，如果符合该准则，则发送一个事件，以授予或取消对已连接系统中业务资源的访问权限。这样，您便多了一个控制级别，并且可以自动授予和取消资源。

要使权利发挥作用，需要注意以下两个方面：创建权利和管理权利。可以通过 iManager 或 Designer 创建权利。要通过 iManager 创建权利，请在 iManager 中，选择 《Identity Manager 实用程序》标题下方的 《创建权利》选项 > 。有关更多信息，请参见 *《Novell Identity Manager 3.0 Administration Guide》*（Novell Identity Manager 3.0 管理指南）中的 《Creating and Using Entitlements》（创建和使用权利）。

还可以使用 Designer 创建权利，并将其部署到现有的 Identity Manager 驱动程序。Designer 允许您通过权利向导创建权利，该向导提供了一个可用于创建权利的图形界面，并逐步引导您完成整个过程。可以在 iManager 中通过一个简单的界面创建权利，但是需要通过 XML 编辑器添加其它属性。Designer 有一个图形界面，因此建议使用它来创建和编辑权利。

创建权利后 （或使用通过特定的 Identity Manager 驱动程序预配置的权利后），需要对权利进行管理。由两个包或代理管理权利：在 iManager 中通过基于职能的权利策略进行管理，或者使用基于工作流程的供应并通过用户应用程序进行管理。

如果符合准则，则可以使用基于职能的权利策略授予业务资源。例如，如果用户符合准则 1、 2 和 3，则基于职能的权利策略可以将该用户添加到组 H，但如果用户符合准则 4 和 5，则他 （她）将成为组 I 的成员。要使此权利配合基于工作流程的供应，首先需要进行批准。

在 Designer 1.2 中创建的权利不能在版本低于 Identity Manager 3.0 的 Identity Manager 引擎上工作。在 Designer 中，可以从建模程序或 《大纲》视图访问权利向导。

- 在 《大纲》视图中，右击一个 Identity Manager 驱动程序。选择 *Add Entitlement* （添加权利）。
- 在 《建模程序》视图中，右击一个驱动程序对象，然后选择 《权利》 > 《添加权利》。

1.3.3 Novell Identity Manager 用户应用程序和基于工作流程的供应

Novell Identity Manager 用户应用程序是一个功能强大的万维网应用程序，包含用于供应的支持工具。基于工作流程的供应是管理用户对组织中安全资源的访问权限的过程。用户请求资源后，一个或多个具有批准权利的人员 （包括委托或代理）可以批准或拒绝请求。用户还可以查看请求的状态。

如果结合 Provisioning Module for Identity Manager 和 Novell Audit 使用， Identity Manager 用户应用程序可提供安全、可缩放和易于管理的完整端到端供应解决方案。

用户应用程序提供以下基于万维网的最终用户功能：

- 白页
- 组织结构图
- 用户搜索 （能够保存自定义搜索配置）
- 自助服务口令管理
- 轻量级用户管理工具
- 发送和监视供应请求 （如果已安装供应模块）
- 管理个人任务和 / 或小组任务 （如果已安装供应模块）
- 委托和代理功能
- 自助服务用户简报管理 （用户可以编辑其公共简报上的选定信息）
- 供应任务的电子邮件通知
- 作为身份入口一部分的 85 个入口小程序，用于为用户创建自定义的内部网页面
- 支持自我供应和基于批准的供应工作流程

对于系统管理员，用户应用程序提供了多种多样的配置和管理功能，包括：

- iManager 插件，用于设置和管理代理和委托权限
- 访问日志记录工具和自定义的 Crystal Reports
- 基于向导的工作流程配置 （如果已安装供应模块）
- 工作流程管理 （如果已安装供应模块），包括启用和禁用工作流程，以及暂停正在进行的流程
- 基于 Eclipse RCP 的 Designer，用于创建自定义的虚拟目录对象定义和关系

支持基于工作流程的供应是 Identity Manager 3 的主要功能，需要独立购买该功能。Identity Manager 2 不支持基于工作流程的供应。

1.3.4 Novell 身份凭证供应策略

开发 Identity Manager 3 的 Novell 身份凭证供应策略旨在能够同时将应用程序身份凭证供应给 Novell SecretStore® 和 Novell SecureLogin (NSL) 身份凭证储存库，从而增强任何 Identity Manager 驱动程序的用户供应功能。此外，该产品还可以在需要无否决功能的环境中供应 NSL Passphrase 问题和答案。这些产品功能可以增强用户一次签到 (SSO) 的体验，同时通过排除 NSL 帐户的初始设置、向应用程序身份凭证提供附加的安全性，以及减少重复工作（通常与供应用户的 SSO 身份凭证储存有关），来增加 SSO 技术的投资回报。请务必注意，该产品可以使用 IDM 策略自动取消供应应用程序身份凭证，以防止访问应用程序数据。有

关更多信息，请参见 《*Policy Builder and Driver Customization Guide*》（策略构建器和驱动程序自定义指南）中的 《Novell Credential Provisioning Policies》（Novell 身份凭证供应策略）。

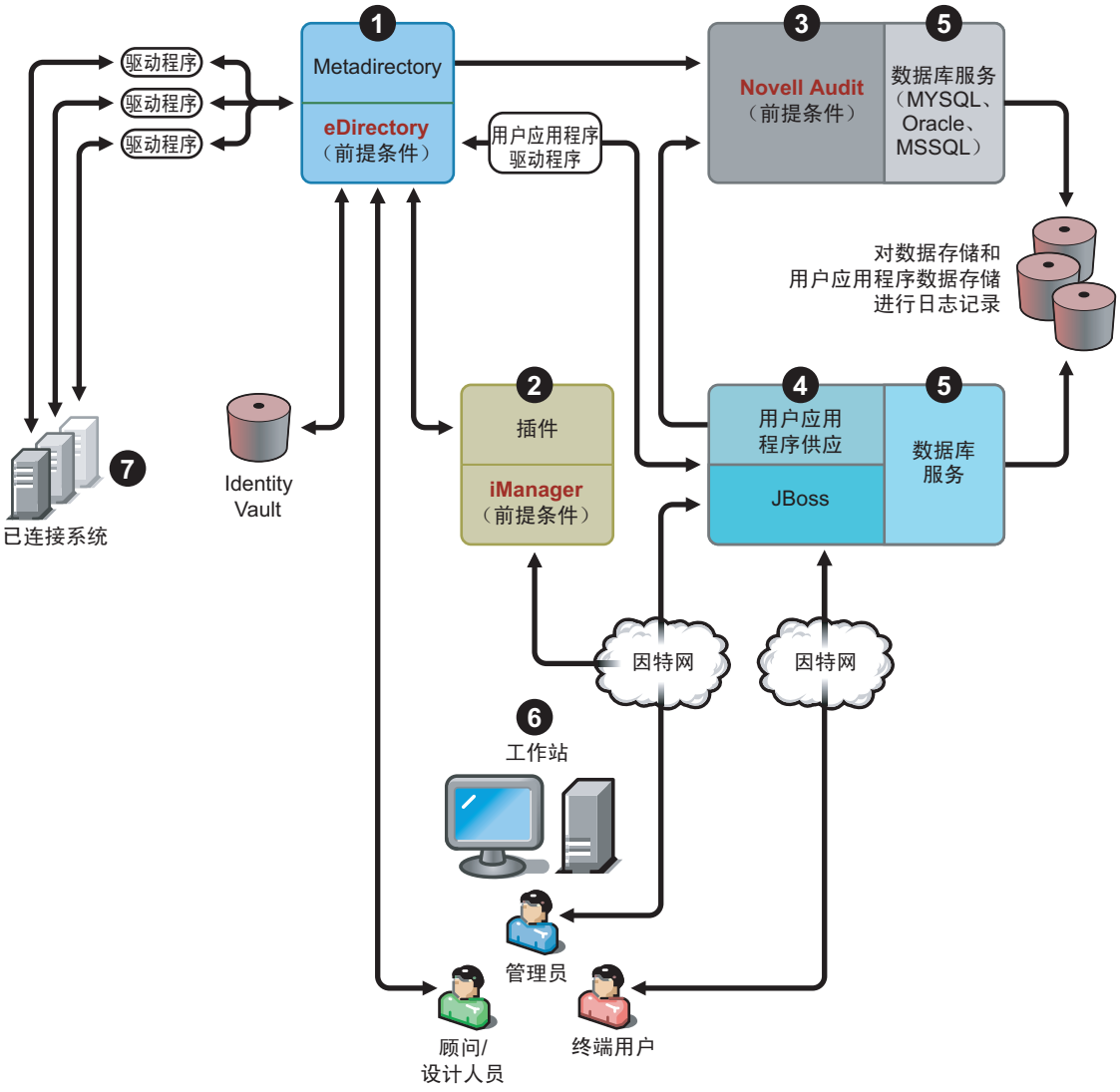
1.4 Identity Manager 安装程序和服务

以下各节介绍 Identity Manager 的安装程序和服务。

1.4.1 安装程序

Identity Manager 有三个独特的安装程序，以及七个需要安装和配置的服务。

图 ***1-3*** *Identity Manager* 提供的七个服务的图形概述



下面是安装程序的列表以及每个安装过程的任务：

- “Identity Manager Metadirectory 系统安装”在第 13 页
- “用于供应安装的用户应用程序和工作流程服务”在第 13 页

- “Designer 安装”在第 13 页

注释：安装 Identity Manager 组件之前，需要安装先期必要的软件，包括 eDirectory 8.7.3 或更高版本、 iManager 2.5 或更高版本，以及 Novell Audit 1.0.3 Starter Pack。可以从 Novell 下载万维网站点 (http://download.novell.com) 获取先期必要的软件。

Identity Manager Metadirectory 系统安装

安装过程执行下列功能：

- 将 Identity Manager 产品的 eDirectory 纲要作为一个整体进行扩展。
- 安装 Metadirectory 引擎和系统服务。
- 安装 iManager 的 Identity Manager 插件。
- 安装 Metadirectory 系统远程装载程序 （如果已选择）。
- 安装已连接系统驱动程序。 （将会安装驱动程序，但是在启动以供使用之前，这些驱动程序将处于休眠状态）。
- 安装 Identity Manager 报告，以及任何 Metadirectory 系统实用程序和工具。

用于供应安装的用户应用程序和工作流程服务

将在 Linux 和 Windows 上安装下列服务：

- JBoss 和 MySQL （如果已选择）。
- 轻量级入口软件和目录抽象层软件。
- 用户应用程序入口小程序以及支持软件，包括工作流程最终用户任务。
- 工作流程引擎。

Designer 安装

Linux 和 Windows 各有一个安装程序：

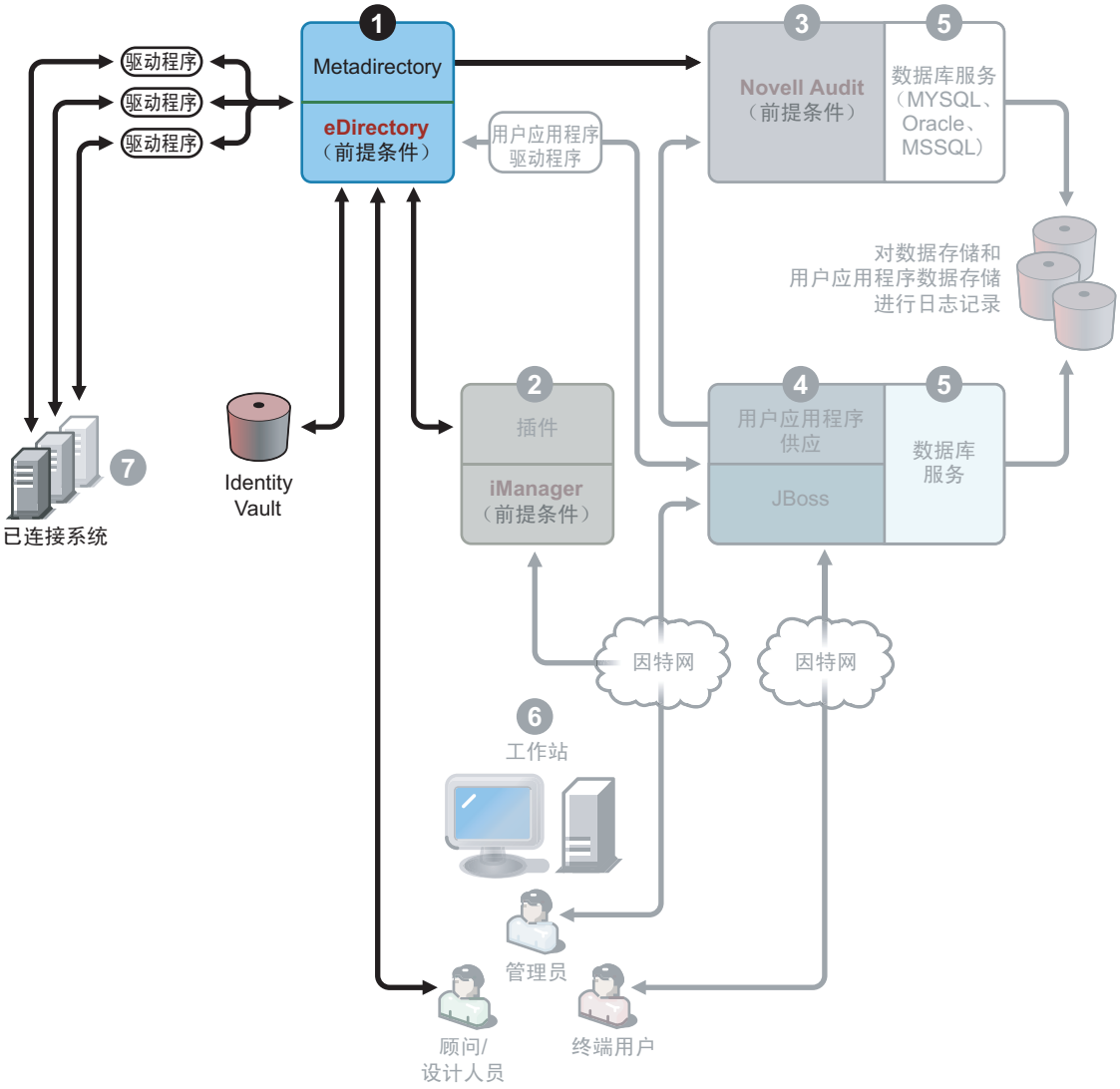
- 安装 Eclipse 框架。
- 安装基本插件。
- 安装 Metadirectory 插件。

1.4.2 服务

Identity Manager 附带有七个可以安装和配置的服务。尽管不建议对生产环境这么做，但可以在一台计算机上安装和配置所有七个服务。也可以在每台计算机上部署一个服务，或个数

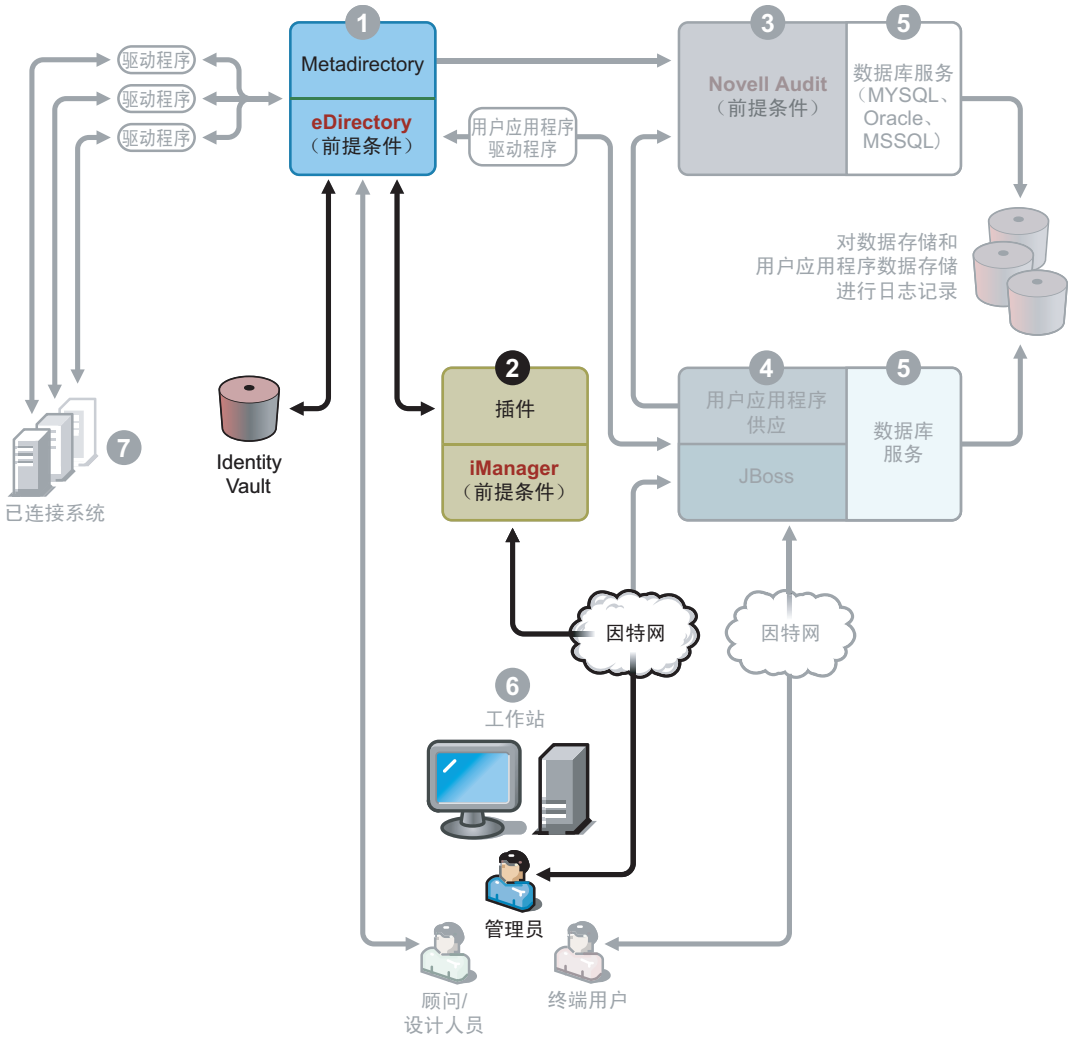
介于一和七之间的服务。“Identity Manager 的系统要求”在第 20 页中包含了每个服务支持的硬件和软件前提条件。

图 ***1-4*** *Metadirectory* 系统服务



1. Metadirectory 系统服务。该系统将用作 Identity Vault，在生产环境中只需要 Metadirectory 引擎的一个实例。要安装 Identity Manager 和该服务，请参见第 4 章 “安装 Identity Manager”在第 53 页。

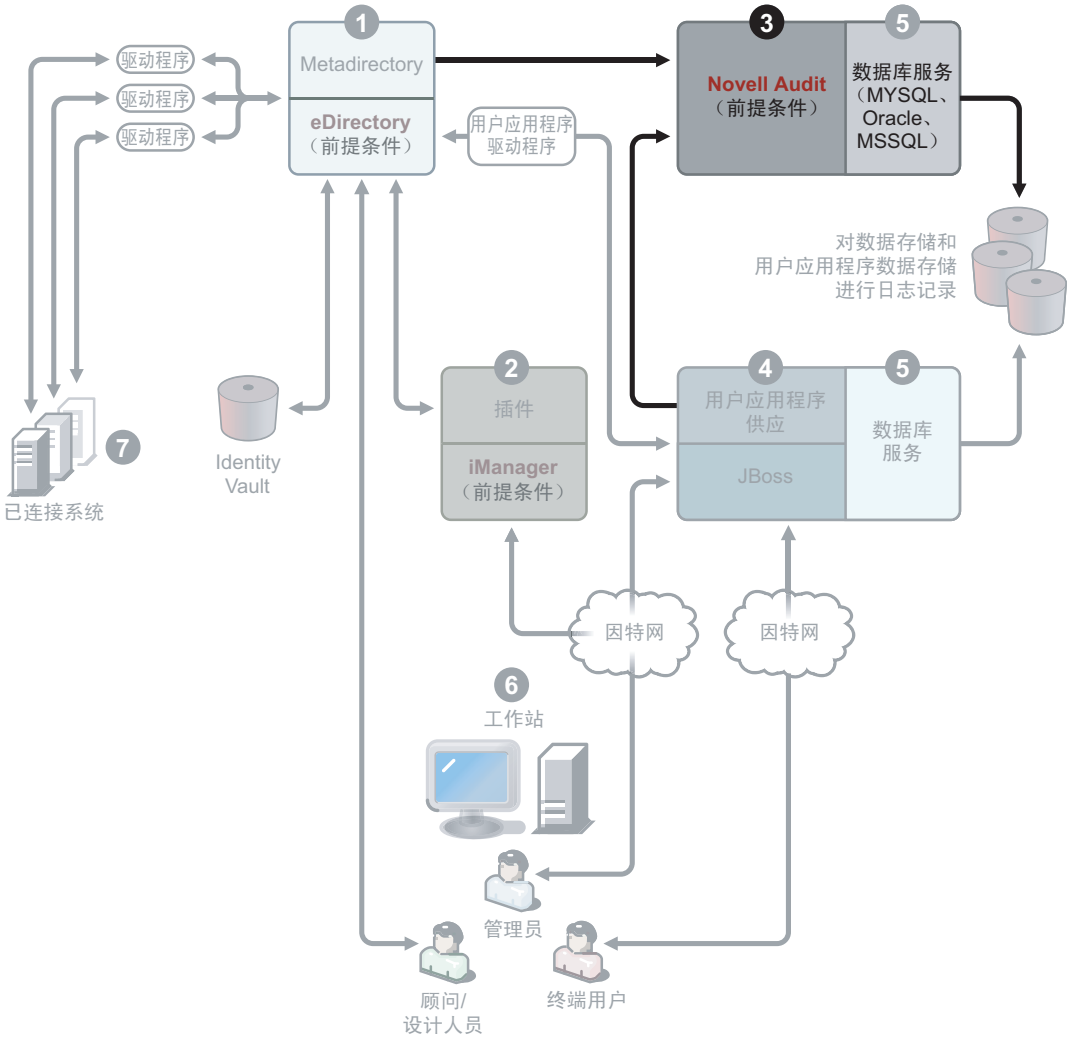
图 ***1-5*** 基于万维网的管理服务



2. 基于万维网的管理服务。在安装了 Identity Manager 和用户应用程序插件的情况下，可使用该服务并通过 iManager 2.5 和更高版本来管理 eDirectory 和 Metadirectory 系统。将

Identity Manager 插件安装到 Identity Manager 所在服务器上的 iManager 中。要安装 Identity Manager 插件和该服务，请参见第 4 章 “安装 Identity Manager”在第 53 页。

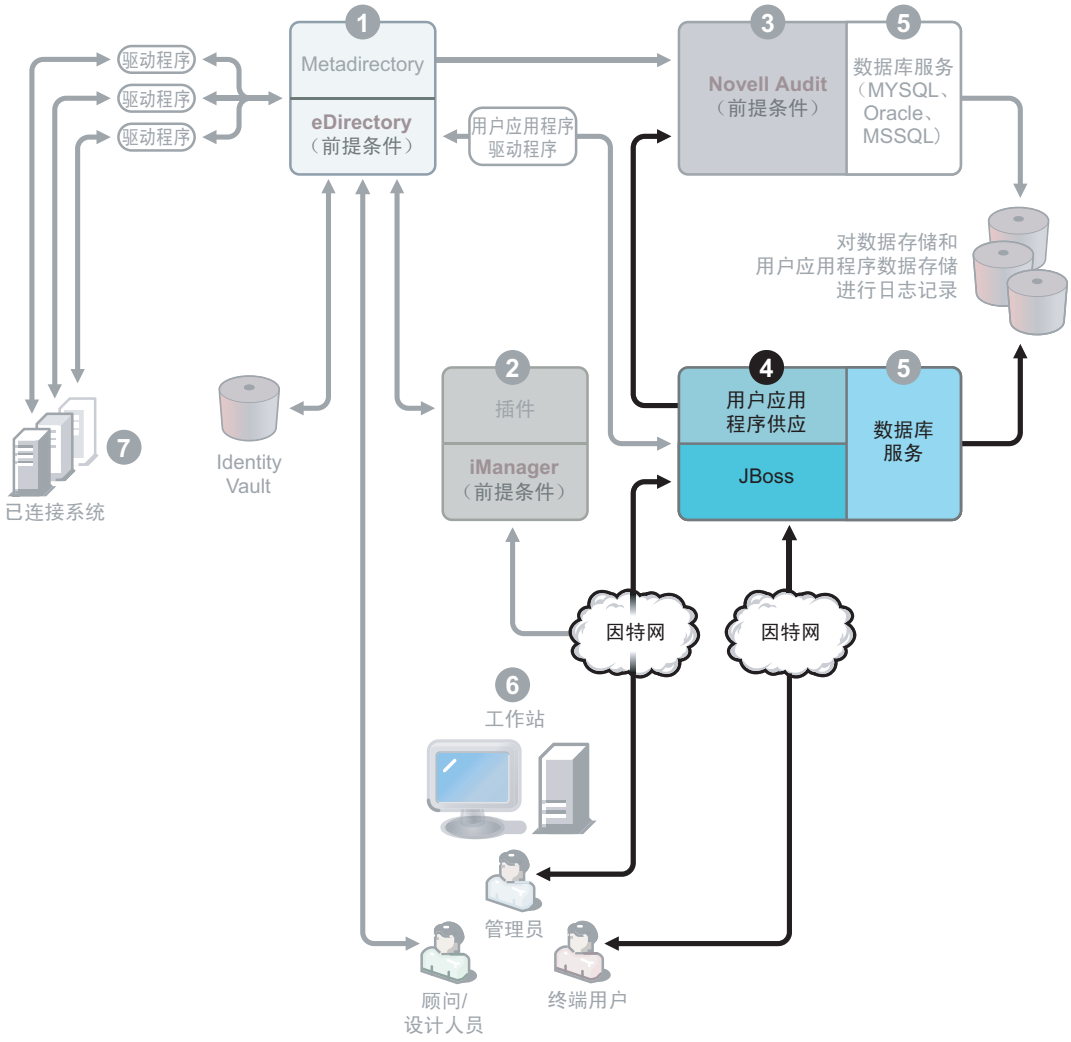
图 *1-6* 安全日志记录服务



3. 安全日志记录服务。日志记录事件的储存库 （此服务器上未安装 Identity Manager 软件，但必须有安全日志记录服务）。这是 Identity Manager、最终用户应用程序和工作流程系统服务使用的中央服务，需要从 Novell 下载万维网站点 (http://download.novell.com) 单独下载该服务。

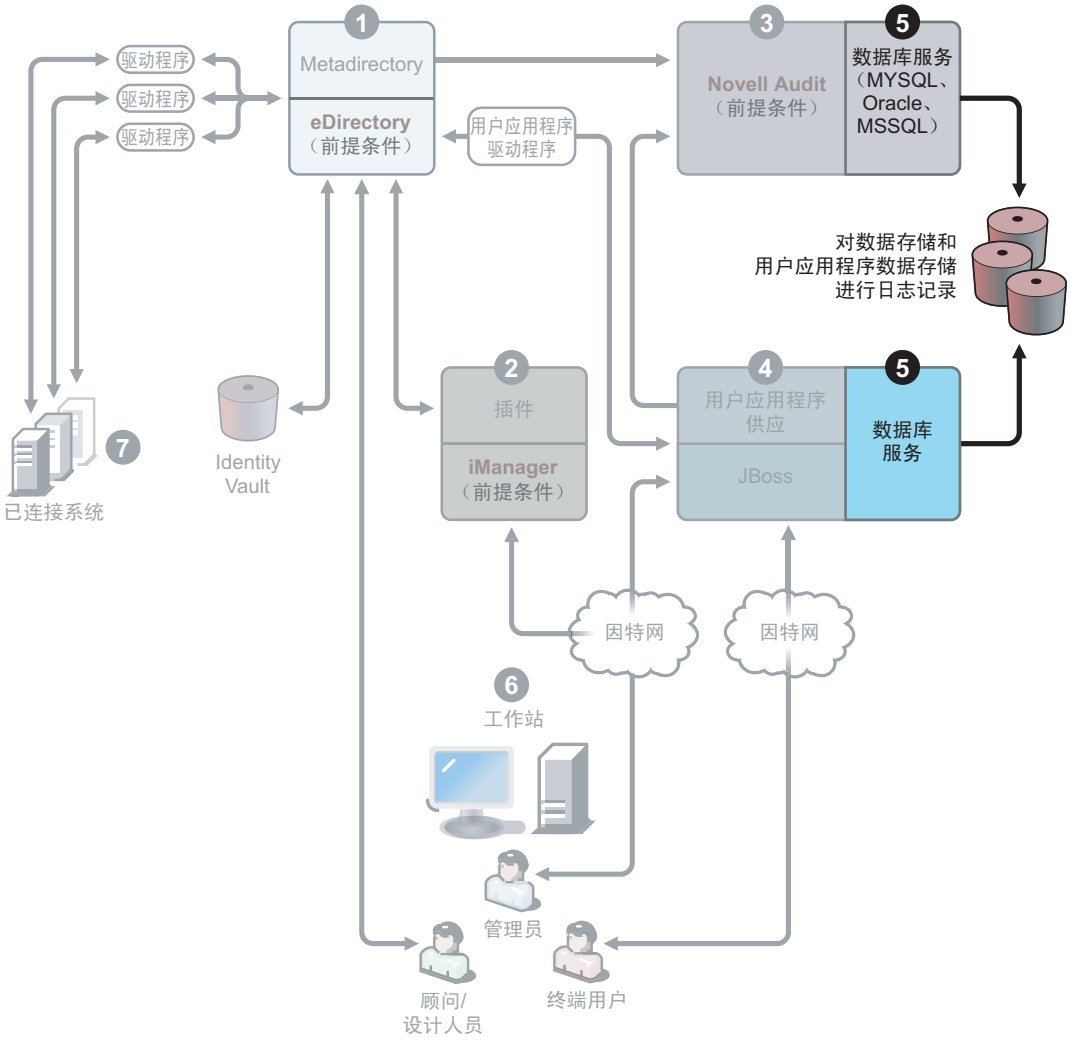
在下载万维网站点上的 《产品或技术》下拉菜单中，选择 *Novell Audit*，然后单击 《搜索》。单击 *Novell Nsure Audit 1.0.3 Starter Pack*。遵循 Starter Pack 包含的安装指导。

图 ***1-7*** 用户应用程序和基于工作流程的供应服务



4. 用户应用程序和基于工作流程的供应服务。要安装该服务，请参见第 5 章 “安装用户应用程序” 在第 77 页 。

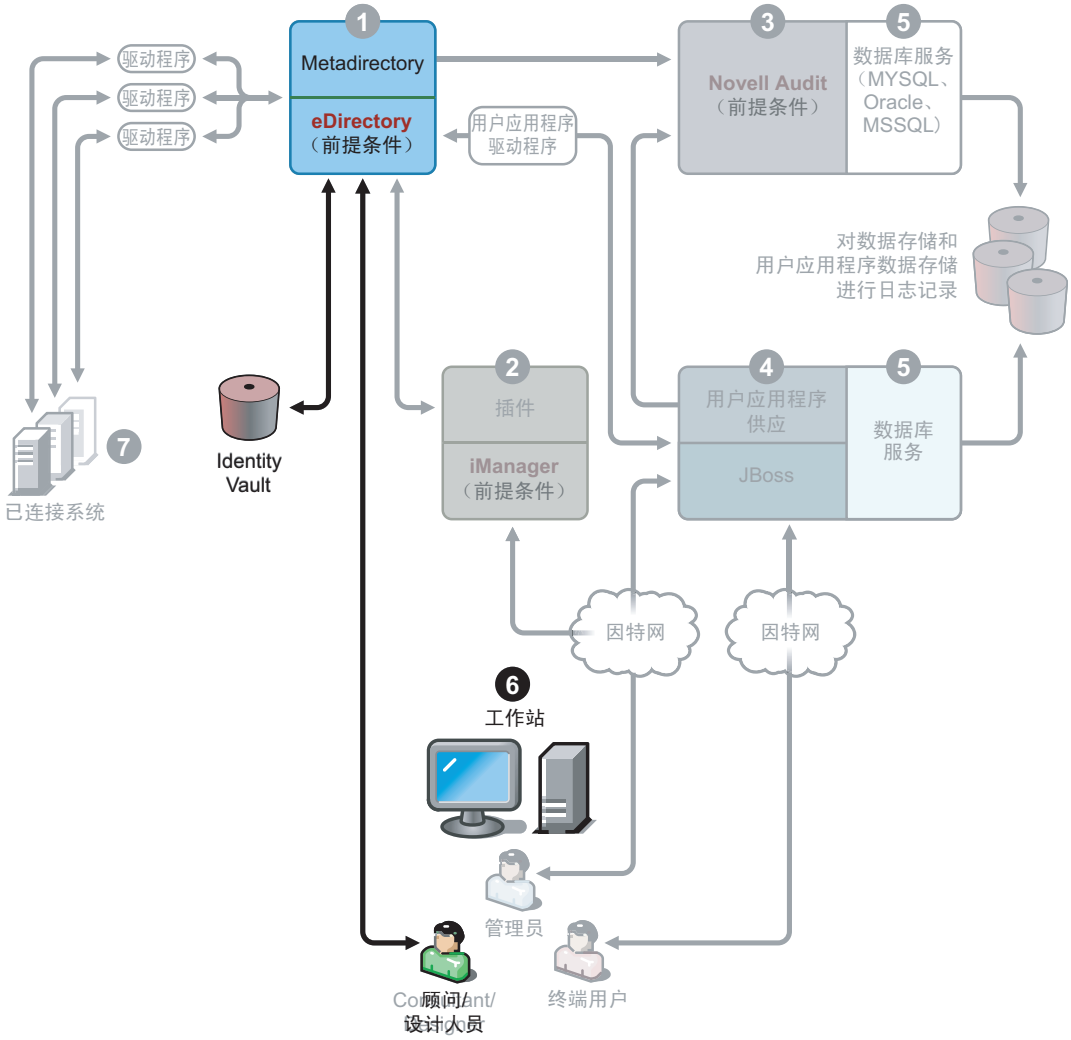
图 ***1-8*** 数据库服务



5. 数据库服务。安全日志记录服务和最终用户应用程序 / 工作流程系统都需要数据库。可以设置一个数据库来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。但是，可以使用用户应用程序和供应附带的 MySQL 数据库。用户应用程序附带有 JBoss Application Server 版本 4.0.2，以及 MySQL 版本 4.1.12。要安装该服务，请参见 “安装和配置”在第 78 页。

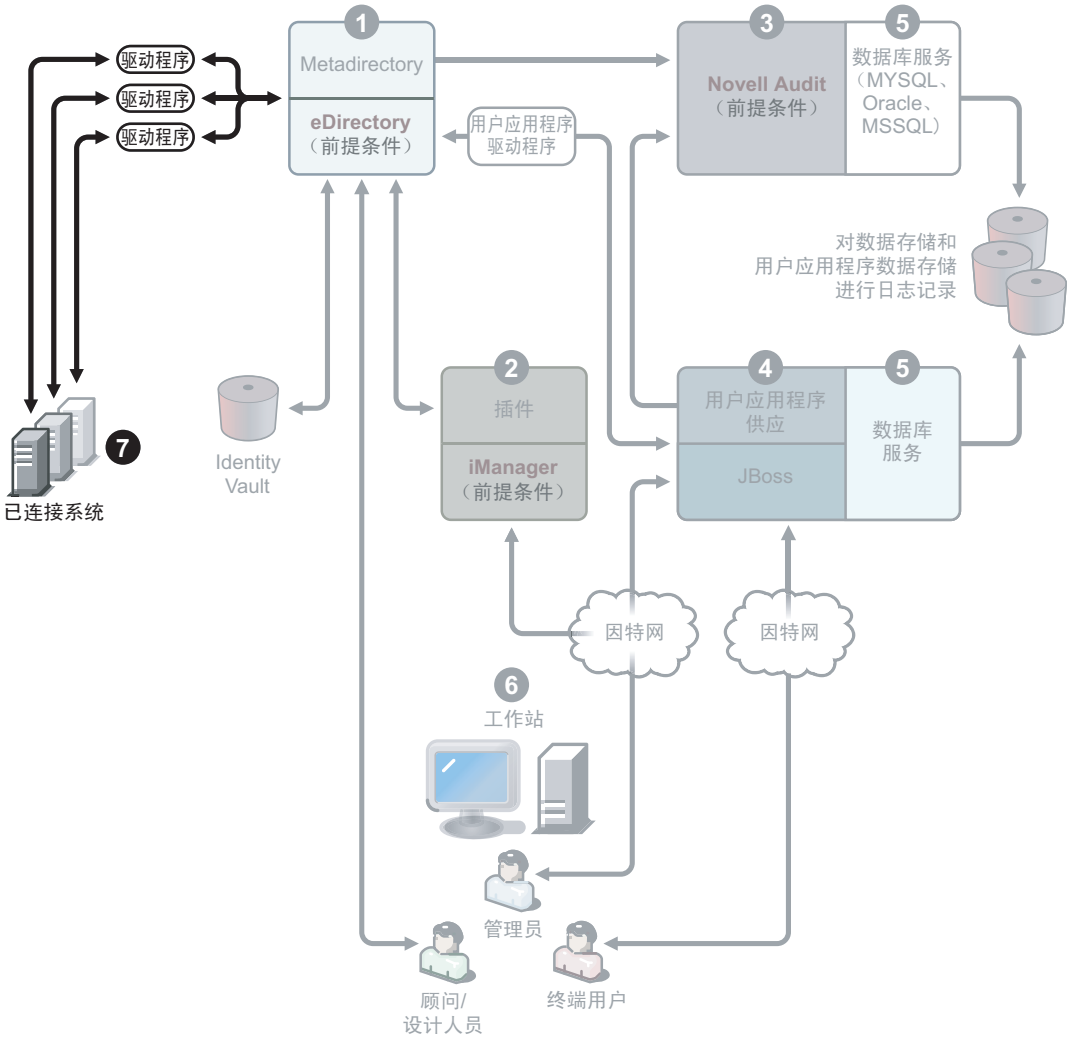
图 ***1-9*** *Designer* 的工作站服务



6. 工作站。Designer 使用该服务设计、部署 Identity Manager 系统并为 Identity Manager 系统编制文档，此外，可使用该服务获取产品包含的实用程序、报告和工具。要在工作站上安装 Designer，请参见 *《Designer for Identity Manager 3: Administration Guide》*

（Designer for Identity Manager 3：管理指南）中的 《Installing Designer》（安装 Designer）。

图 *1-10* 已连接系统



7. 已连接系统。这是承载驱动程序的位置，这些已连接系统可以是应用程序、数据库、服务器和其它服务。每个连接的应用程序都要求个人具有应用程序特定的知识并承担相关责任。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。

   可以将驱动程序的安装作为 Identity Manager 安装过程的一部分。要安装 Identity Manager 和该服务，请参见第 4 章 “安装 Identity Manager”在第 53 页 。要了解有关配置驱动程序的更多信息，应该阅读 Identity Manager 驱动程序文档万维网站点 (http://www.novell.com/documentation/idmdrivers) 上的驱动程序特定文档。

1.5 Identity Manager 的系统要求

Novell Identity Manager 包含可以在环境中的多个系统和平台上安装的组件。根据系统配置的不同，可能需要多次运行 Identity Manager 安装程序才能在相应的系统上安装 Identity Manager 组件。

下表列出了 Identity Manager 的安装组件以及每个组件的要求。

表 ***1-3*** *Identity Manager* 系统组件

系统组件	系统要求	注释
Metadirectory 服务器 ◆ Metadirectory 引擎 ◆ Novell Audit 代理 ◆ 服务驱动程序 ◆ Identity Manager 驱动程序 ◆ NMAS™ 方法和纲要 ◆ 实用程序（包括许可证监查工具、应用程序工具和 Novell Audit 设置工具）	下列操作系统之一： ◆ 带最新 Support Pack 的 NetWare® 6.5 ◆ 带最新 Support Pack 的 Novell Open Enterprise Server (OES) ◆ Windows* NT ◆ 带最新 Service Pack 的 Windows 2000 Server（32 位） ◆ 带最新 Service Pack 的 Windows Server 2003 R2（不支持 2003 64 位） ◆ Linux Red Hat* AS 3.0 ◆ Linux Red Hat AS 4.0 for AMD 64/EM64T ◆ 带最新 Support Pack 的 SUSE® Linux Enterprise Server 8、 9 或 10 ◆ Solaris 8、 9 或 10 ◆ AIX 5.2L 下列 eDirectory 版本之一： ◆ 带最新 Support Pack 的 eDirectory 8.7.3 ◆ 带最新 Support Pack 的 eDirectory 8.8 ◆ 带最新 Support Pack 的 eDirectory 8.8.1 建议将 eDirectory 8.8 升级到 8.8.1。	如果使用支持 Metadirectory 服务器的平台，则支持在实施中使用 VMWare。 除非另行指定，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： ◆ Intel x86 ◆ AMD x86 ◆ Intel EM64T ◆ AMD Athlon64 和 Opteron eDirectory 8.8 及更高版本支持下列高级功能： ◆ 同一服务器上的多个 eDirectory 实例 ◆ 加密的特性 尽管 eDirectory 8.8 及更高版本包括对非根用户安装的支持，但您必须以根用户的身份安装 Identity Manager。 eDirectory 8.8.1 支持 64 位 Red Hat Linux AS 和 ES 4.0。但是， eDirectory 8.8.x 不支持 Solaris 8。 安装 eDirectory 8.8.1 之前，请务必完全备份 eDirectory 数据库。 eDirectory 8.8.1 将会升级数据库结构的某些部分，并且在完成升级过程后，它不允许数据库结构回滚。 SUSE Linux Enterprise Server 10 不支持 XEN 虚拟化。

系统组件	系统要求	注释
基于万维网的管理服务器 • Identity Manager 和口令管理 • iManager 2.6 和插件 • 驱动程序配置	下列操作系统之一： • 带最新 Support Pack 的 Novell Open Enterprise Server (OES) • 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 R2（不支持 2003 64 位） • Linux Red Hat AS 3.0 （Glibc 版本 2.1.1 或更高版本，内核版本 2.2.*xx* 或更高版本。） • Linux Red Hat AS 4.0 for AMD 64/EM64T • Solaris 9 或 10 • 带最新 Support Pack 的 SUSE Linux Enterprise Server 8、 9 或 10 通过 iManager 工作站支持操作系统： • 带最新 Service Pack 的 Windows 2000 Professional • Windows XP • Red Hat Enterprise Linux Workstation • SUSE Linux 9.1 或 9.3 下列软件。 • Novell iManager 2.6 Support Pack 2 或更高版本 （包括 Apache 2.0.52 或更高版本，以及 Tomcat 4.1.18 或更高版本）	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： • 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： • Internet Explorer 6 SP1 和更高版本 • Firefox 1.5.0.x 和更高版本 • Mozilla 1.7 和更高版本 • 必须使用 iManager 配置向导或 Designer 实用程序将入口内容安装或部署到 eDirectory。 • 如果将 iManager 2.6 安装在 eDirectory 所在的同一台服务器上，则 eDirectory 的版本必须为 8.7.3 或更高。 • (Windows) 可以从 Novell 软件下载 (http://download.novell.com/index.jsp) 获取 Novell Client™ 4.9。 • 使用 iManager 登录到其它树以管理远程 Identity Manager 服务器时，如果使用该远程服务器的服务器名而不是 IP 地址，则可能会遇到错误。

系统组件	系统要求	注释
安全日志记录服务 ◆ 安全日志记录服务器 ◆ 平台代理 （客户机组件）	对于安全日志记录服务器，下列操作系统之一： ◆ 带最新 Support Pack 的 Novell Open Enterprise Server (OES) ◆ 带最新 Support Pack 的 NetWare 6.5，带最新 Support Pack 的 NetWare 6.0 ◆ 带最新 Service Pack 的 Windows 2000 Server ◆ Linux Red Hat AS 3.0、 AS 和 ES 2.1 （Glibc 版本 2.1.1 或更高版本，内核版本 2.2.*xx* 或更高版本。） ◆ Linux Red Hat AS 4.0 for AMD 64/EM64T ◆ Solaris 8、 9 或 10 ◆ SUSE Linux Enterprise Server 8、 9 或 10 ◆ Novell eDirectory 8.5 或更高版本 对于平台代理，下列操作系统之一： ◆ NetWare 5.1 和更高版本（带最新 Support Pack） ◆ Windows 2000 或 2000 Server、 XP，或者带最新 Service Pack 的 Windows Server 2003 （不支持 2003 64 位） ◆ Linux Red Hat 7.3、 8、 AS 和 ES 2.1 ◆ Solaris 8、 9 或 10 ◆ SUSE Linux Enterprise Server 8	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： ◆ Intel x86 ◆ AMD x86 ◆ Intel EM64T ◆ AMD Athlon64 和 Opteron 最低安全服务器要求包括： ◆ 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 eDirectory Instrumentation 用于记录 eDirectory 事件，它支持下列 eDirectory 版本： ◆ NDS® 8.xeDirectory 8.6 （NetWare、 Windows、 Linux 和 Solaris） ◆ eDirectory 8.7 （NetWare、 Windows、 Linux 和 Solaris） NetWare Instrumentation 用于记录 NetWare 事件，它支持下列 NetWare 版本： ◆ 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)

系统组件	系统要求	注释
用户应用程序和工作流程系统服务 ◆ Identity Vault 访问 ◆ IDM 用户应用程序储存	SUSE Linux Enterprise Server 9 和 10 Windows 2000 Server 带最新 Service Pack 的 Windows Server 2003 R2 （不支持 64 位）	除非另有规定，否则 SUSE Linux Enterprise Server 支持下列所有 32 位模式的处理器： ◆ Intel x86 ◆ AMD x86 ◆ Intel EM64T ◆ AMD Athlon64 和 Opteron 用户应用程序需要身份凭证才能登录 Identity Vault。用于访问 Identity Vault 的身份凭证必须： ◆ 具有对 Identity Vault 的全部权限 ◆ 在安装 Identity Manager 3 用户应用程序之前，在 Identity Vault 中存在。 安装过程中将提示您提供这些身份凭证。该用户被称为 《用户应用程序管理员》。 在其中安装用户应用程序的计算机必须具有 320 MB 可用储存。 对于 Linux： ◆ 运行级别。用户应用程序安装程序需要 X 服务器 (X Windows)，因此必须将 Linux 运行级别设置为 5 或更高。 ◆ 建议以没有根特权的用户的身份运行安装。 ◆ 确保安装目录可写。通常在用户的 home 目录中使用目录结构 novell/idm 来安装用户应用程序，但可以更改此默认值。

系统组件	系统要求	注释
数据库服务器和服务 ◆ JBoss ◆ MySQL	本地访问表示数据库在应用程序服务器所在的同一框架上运行。远程访问表示产品通过线路访问数据库。 在用户应用程序产品中包括： ◆ JBoss Application Server 版本 4.0.2 在用户应用程序产品中包括以下项目，以本地访问和远程访问的方式工作： ◆ MySQL 版本 4.1.12 不包括下列数据库，它们仅可用于远程访问： ◆ Oracle 9i (9.2.0.4) ◆ Oracle 10g (10.2.0.1.0) ◆ MS SQL 2000 SP4	注释：如果要实现群集，则必须下载和安装 JBoss 4.0.3 SP1。 可以使用 JBoss Application Server 来承载用户应用程序和 MySQL，也可以使用其它受支持的数据库。用户应用程序使用数据库来完成各种任务，例如，储存用户应用程序配置数据，以及储存任何正在进行的工作流程活动的数据。 安全日志记录服务以及用户应用程序和工作流程供应都需要数据库。可以设置一个数据库来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。 对于 JBoss： ◆ 运行用户应用程序时 JBoss 的最低建议 RAM 为 512 MB。 ◆ 用于安装 JBoss 的计算机的端口 8080 应该处于空闲状态。默认情况下， JBoss 允许 Tomcat 使用端口 8080。应该在该端口空闲的计算机上安装 JBoss。 ◆ 如果目标计算机上也有 iManager 的实例 （或者其它任何使用其自身的 Tomcat 实例的应用程序），结果可能是多个 Tomcat 实例争用同一个端口。应该关闭其它 Tomcat 实例，或者将其它实例设置为不使用端口 8080。 对于 MySQL： ◆ 用于安装 MySQL 的计算机的端口 63306 应该处于空闲状态。默认情况下，用户应用程序安装程序将在端口号 63306 的位置安装 MySQL，以避免与计算机上运行的其它任何 MySQL 服务器冲突。

系统组件	系统要求	注释
工作站 ◆ Designer ◆ iManager 万维网访问	已在下列平台上测试了 Designer： Windows： ◆ Windows 2000 Professional 和 Windows 2000 Server ◆ Windows XP Professional ◆ 带最新 Service Pack 的 Windows Server 2003 R2（不支持 2003 64 位） Linux： ◆ SUSE Linux Enterprise Server 9.2、 9.3 和 10 ◆ SUSE Linux Enterprise Server 9 SP1、 SP2 ◆ SUSE Linux Enterprise Server 10 ◆ Red Hat Linux 9 ◆ Novell Linux Desktop ◆ GNOME、 KDE、 Red Hat Fedora	Designer 将 Eclipse 用作其开发平台。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： ◆ 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： ◆ Microsoft Internet Explorer 6.0 SP1 ◆ 或 Mozilla 1.7 ◆ 或 Mozilla Firefox 1.5.0.x
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） ◆ 远程装载程序 ◆ 远程装载程序配置工具（仅限 Windows） ◆ Novell Audit 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/idmdrivers)。	每个连接的应用程序都要求个人具有应用程序特定的知识并承担相关责任。 远程装载程序系统： ◆ Windows NT 4.0、 Windows 2000 或 Windows 2003 ◆ Red Hat Linux AS 3.0 ◆ Linux Red Hat AS 4.0 for AMD 64/EM64T ◆ SUSE Linux Enterprise Server 8、 9 或 10 ◆ Solaris 8、 9 或 10 ◆ AIX 5L v5.2 Java 远程装载程序系统： ◆ HP-UX 11i ◆ OS/400 ◆ zOS ◆ 应该可以在具有 JVM 1.4.2 或更高版本的任何系统上使用

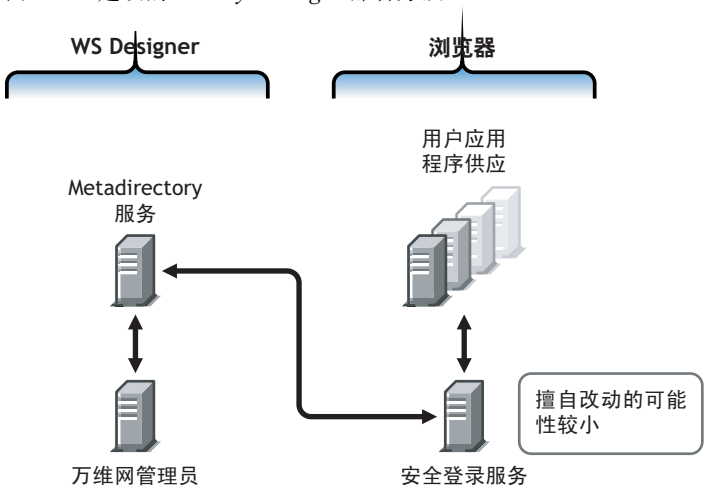
1.6 建议的部署策略

如前所述， Identity Manager 附带有七个必须安装和配置的服务。尽管不建议对生产环境这么做，但可以在一台服务器上安装和配置所有七个服务。也可以在每台服务器上部署一个服务，或个数介于一和七之间的服务。

设置 Identity Manager 部署时，工作负载是一个主要因素。能够分散的交通量越大，应用程序拥有潜在吞吐量就越大。

在图 1-3 中，建议对 Metadirectory 服务使用一台服务器，对基于万维网的管理服务使用一台服务器，对安全日志记录服务使用一台服务器，对用户应用程序和基于工作流程的供应服务使用一台服务器。

图 ***1-11*** 建议的 *Identity Manager* 部署方法



Metadirectory 服务

部署 Identity Manager 服务的方式取决于服务的工作负荷。例如，可以在一台与已连接系统通讯的服务器上安装 Identity Manager 的 Metadirectory 服务。只需要在一台运行 eDirectory 的服务器上安装 Metadirectory 引擎。

由于 iManager 的潜在吞吐量较大，因此您可能不希望将基于万维网的管理服务与 Metadirectory 服务安装在一起。如果确实要将 iManager 安装在 Identity Manager 所在的同一台服务器上，则请先安装 iManager，然后安装 Identity Manager 及其插件。

基于万维网的管理服务

如果已经在服务器上安装了 iManager 2.5 或 2.6，则只需要运行 Identity Manager 安装，然后安装 iManager 的 Identity Manager 插件。如果安装的是用户应用程序和工作流程系统服务，则还必须运行用户应用程序安装，然后只安装 iManager 的用户应用程序插件。需要针对用户应用程序或带有供应安装的用户应用程序 （它们是两个不同的产品）执行此操作。

用户应用程序和安全日志记录服务

如果执行大量的供应，则建议将用户应用程序安装在其自身的服务器上。必要时还可以设置群集。用户应用程序包含 MySQL 4.1.12，因此，如果将该数据库的部署作为用户应用程序安装的一部分，或者作为具有基于工作流程的供应的用户应用程序安装的一部分，则不需要设置另一个数据库服务。

但是，安全日志记录服务不包括特定的数据库，而安全日志记录服务和最终用户应用程序 / 工作流程供应服务都需要数据库。可以设置一个数据库来为两个应用程序提供服务，也可以为每个服务设置独立的数据库。这取决于执行供应的数量以及日志记录服务的工作负荷。

注释：如果要在独立的 （远程）服务器上设置 Oracle 9i 或 10g，则需要安装 Oracle，然后配置应用程序服务器，以提供对数据库的远程连接。

使用远程装载程序配置

在安装 Identity Manager 过程中，如果不需要在已连接系统服务器上安装 eDirectory 服务和 Metadirectory 引擎，则可以使用 《已连接系统》选项。远程装载程序还在 Metadirectory 引擎和使用 SSL 技术的驱动程序之间提供安全的通讯路径。将系统连接到 Identity Manager 时请记住这一点。

1.7 从何处获取 Identity Manager 3 及其服务

- “安装 Identity Manager 3”在第 29 页
- “激活 Identity Manager 3 产品”在第 30 页

要下载 Identity Manager 3 及其服务，请访问 Novell 下载万维网站点 (http://download.novell.com)。

1. 在 《产品或技术》菜单中，选择 *Novell Identity Manager*，然后单击 《搜索》> > 。
2. 在 《Novell Identity Manager 下载》页上，单击所需文件旁边的 《下载》按钮。
3. 遵循屏幕提示，将该文件下载到计算机上的某个目录中。
4. 从第 2 步开始重复，直到下载了所有需要的文件。大多数安装需要多个 ISO 映象。

下列 Identity Manager 组件可用于下载。

表 ***1-4*** *ISO* 映象的工作方式

Identity Manager 组件	平台	ISO
Identity Manager DVD 可以在一个用于烧录 DVD 的 ISO 映象上使用下列 Identity Manager 组件。这些组件还可用于每次下载。 ◆ Identity Manager 和驱动程序 ◆ Designer for Identity Manager ◆ Integration Module for Midrange and Mainframe	Identity Manager： Linux、NetWare、Windows 和 UNIX Designer： Linux 和 Windows Integration Module for Midrange and Mainframe：请参见下面的 Integration Module for Midrange and Mainframe 平台列表。	Identity_Manager_3.iso
Identity Manager 和驱动程序	Linux、 NetWare 和 Windows	Identity_Manager_3_Linux_NW_Win.iso
Identity Manager 和驱动程序	UNIX	Identity_Manager_3_Unix.iso

Identity Manager 组件	平台	ISO
用户应用程序 这是您购买的 Identity Manager 3 中包含的用户应用程序的标准版本。	Linux 和 Windows	Identity_Manager_3_User_Application.iso
带有 Provisioning Module for Identity Manager 的用户应用程序 这是用户应用程序的 《供应》版本，它是 Identity Manager 的附加产品，需要单独购买。	Linux 和 Windows	Identity_Manager_3_User_Application_Provisioning.iso
Designer for Identity Manager	Linux 和 Windows	Identity_Manager_3_Designer.iso
Identity Manager Integration Module for Midrange and Mainframe	大型主机： z/OS：RACF、 CA ACF2、CA TopSecret 中型机： OS/400、 i5os	Identity_Manager_3_Midrange_Mainframe.iso

Identity Manager 采购产品包括多个常见的客户系统 （您可能已获得这些系统的许可证）的集成模块：Novell eDirectory、Microsoft Active Directory、Microsoft Windows NT、LDAP v3 Directories、 Novell GroupWise、 Microsoft Exchange 和 Lotus Notes。其它所有 Identity Manager 集成模块必须单独购买。

用户应用程序组件附带了两个 ISO 映象：用户应用程序 ISO 映象为标准版本，它包含在 Identity Manager 3 采购产品中。带有 Provisioning Module for Identity Manager 的用户应用程序是一个附加产品，它与功能强大的批准工作流程集成。该供应模块附带了一个独立的 ISO 映象，需要单独购买该模块。

Identity Manager 采购产品还包含 Designer for Identity Manager，这是一个功能强大且灵活的管理工具，可以显著地简化配置和部署。

1.7.1 安装 Identity Manager 3

- 要在 Windows、 NetWare 和 Linux 上安装 Identity Manager 3，请参见第 4 章 “安装 Identity Manager”在第 53 页
- 要安装用户应用程序或带有供应模块的用户应用程序，请参见第 5 章 “安装用户应用程序”在第 77 页
- 要安装 Designer，请参见 《*Novell Identity Manager 3.0 Administration Guide*》（Novell Identity Manager 3.0 管理指南）中的 《Installing Designer》（安装 Designer）

注释 **:** Linux & UNIX （以前为 NIS）、 Mainframe 和 Midrange 驱动程序安装程序位于 /platform/setup 目录中。不得在运行 Identity Manager 和用户应用程序安装程序的同时运行这些安装。

有关已知问题的列表，请参见 Identity Manager 附带的 README 文件。

1.7.2 激活 Identity Manager 3 产品

Identity Manager 产品需要激活 （除 Designer 外）。下列产品可以在 90 天的评估期内使用，其后您必须停止使用这些产品，或购买激活口令。

- Identity Manager 3
- 带有 Provisioning Module for Identity Manager 的用户应用程序
- 集成模块

重要：要成功激活用户应用程序，必须下载正确的 ISO 映象。例如，如果购买了 Identity Manager 3，随后又下载了用户应用程序供应模块，但没有单独购买供应模块，则您的用户应用程序实施将在 90 天后停止工作。

有关激活的其它信息，请参见第 6 章 “激活 Novell Identity Manager 产品”在第 101 页 。

计划

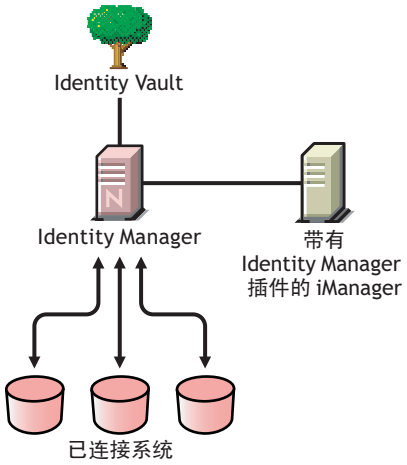
2

2.1 常见安装实例

下列实例说明可能会使用 Identity Manager 的环境。为每个实例提供了一些准则，以帮助您完成实施。

2.1.1 Identity Manager 的全新安装

图 *2-1* 全新安装



Identity Manager 是一个数据共享解决方案，它可以利用 Identity Vault 在应用程序、数据库和目录之间自动同步、转换和分发信息。

Identity Manager 解决方案包括下列组件：

带有 **Identity Manager** 的 **Identity Vault**

Identity Vault 包含需要与其它已连接系统共享或同步的用户数据或对象数据。建议将 Identity Manager 安装在其自身的 eDirectory™ 实例中，并将其用作 Identity Vault。

带有 **Identity Manager** 插件的 **iManager Server**

可以使用 Novell® iManager 和 Identity Manager 插件来管理 Identity Manager 解决方案。

已连接系统

已连接系统可能包含需要与 Identity Vault 共享其中的数据的其它应用程序、目录和数据库。要在 Identity Vault 和已连接系统之间建立连接，请安装该已连接系统的相应驱动程序。有关特定的指导，请参考驱动程序实施指南 (http://www.novell.com/documentation/dirxmldrivers/index.html)。

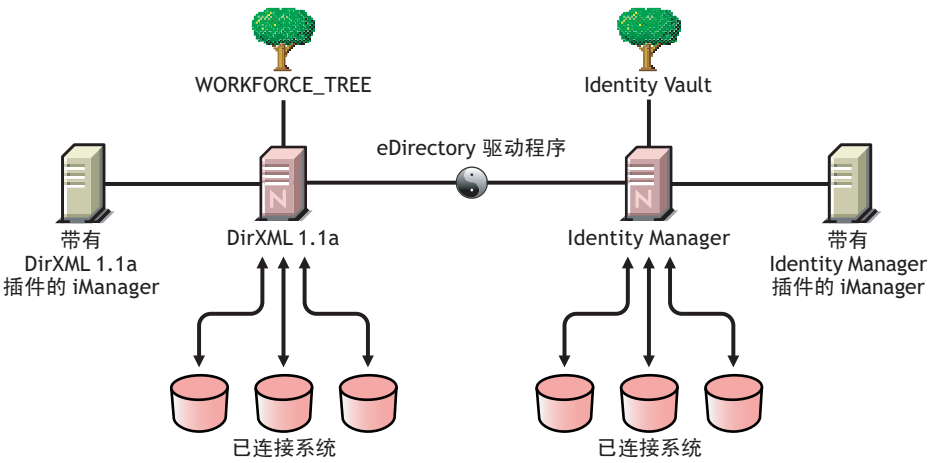
常见的 **Identity Manager** 任务

- 安装系统组件：由于 Identity Manager 解决方案可能要分布在多个计算机、服务器或平台上，因此应该在每个系统上运行安装程序，并安装相应的组件。有关更多信息，请参考 “Identity Manager 组件和系统要求”在第 53 页。
- 设置已连接系统：有关特定的指导，请参考 “Identity Manager 组件和系统要求”在第 53 页 和驱动程序实施指南 (http://www.novell.com/documentation/dirxmldrivers/index.html)。
- 激活您的解决方案：Identity Manager 产品 （专业版和服务器版、集成模块和用户应用程序）需要在安装后的 90 天内激活。请参见附录 6 “激活 Novell Identity Manager 产品”在第 101 页。
- 定义业务策略：可以使用业务策略自定义信息流向特定环境的 Identity Vault，以及从其中流出。策略还可以创建新对象、更新特性值、生成纲要转换、定义匹配准则、维护 Identity Manager 关联，以及执行其它许多任务。 《*Policy Builder and Driver Customization Guide*》（策略构建器和驱动程序自定义指南）包含了策略的详细指南。
- 配置口令管理：使用口令策略，并针对用户创建其口令的方式设置规则，可以提高安全性。还可以通过为用户提供用于解决忘记口令问题和重设置口令的自助服务选项，来减少服务台成本。有关口令管理的详尽信息，请参考管理口令指南中的 《使用口令策略管理口令》。
- 配置权利：使用权利定义，可以向 Identity Vault 中定义的用户组授予对已连接系统的权利。使用权利策略，可以简化业务策略的管理，减少配置 Identity Manager 驱动程序的需要。有关更多信息，请参见 《*Novell Identity Manager 3.0 Administration Guide*》（Novell Identity Manager 3.0 管理指南）中的 《Creating and Using Entitlements》（创建和使用权利）。
- 使用 **Novell Audit** 记录事件：安装 Identity Manager 后，可以使用 Novell Audit 进行审计和报告。Novell Audit 是一个技术集合，可提供监视、日志记录、报告和通知功能。通过与 Novell Audit 集成， Identity Manager 可以提供驱动程序的当前和历史状态以及引擎活动的有关详细信息。这些信息由一组预配置报告、标准通知服务和用户定义的日志记录提供。请参考 《*Novell Identity Manager 3.0 Administration Guide*》（Novell Identity Manager 3.0 管理指南）中的 《Logging and Reporting Using Novell Audit》（使用 Novell Audit 进行日志记录和报告）。
- 工作流程批准和用户应用程序：Novell Identity Manager 用户应用程序是一个功能强大的万维网应用程序 （和支持工具），它可以在复杂的身份服务框架上提供丰富、直观、

高度可配置和高度可管理的万维网 UI 体验。如果结合 Provisioning Module for Identity Manager 和 Novell Audit 使用， Identity Manager 用户应用程序可提供安全、可缩放和易于管理的完整端到端供应解决方案。请参考用户应用程序文档 (http://www.novell.com/documentation/idm)。

2.1.2 在同一环境中使用 Identity Manager 和 DirXML 1.1a

图 **2-2** 在 *DirXML 1.1a* 所在的同一个树中安装 *Identity Manager*



如果在同一环境中运行 Identity Manager 和 DirXML® 1.1a，请记住下列注意事项。

- “创建 Identity Vault”在第 33 页
- “管理工具”在第 33 页
- “向后兼容”在第 33 页
- “口令管理”在第 34 页

创建 Identity Vault

- 建议将 Identity Manager 安装在独立的 eDirectory 实例中，并将其用作 Identity Vault。

管理工具

- DirXML 1.1a 支持 ConsoleOne® ，但 Identity Manager 不支持。
- 必需两个 iManager 服务器，一个用于 DirXML 1.1a 插件，另一个用于 Identity Manager 插件。这是因为插件已得到增强，并且 Identity Manager 使用 DirXML 底稿。
- DirXML 1.1a 的 iManager 插件不能读取在大多数 Identity Manager 驱动程序的已定义驱动程序配置中使用的 DirXML 底稿。

向后兼容

- 可以在 Identity Manager 服务器上运行 DirXML 1.1a 驱动程序 Shim 和配置，并且可以在驱动程序集的 Identity Manager 概述中查看 iManager 中的驱动程序。但是，将驱动程序配置转换为 Identity Manager 格式之前，不能使用 Identity Manager 插件查看或编辑这些驱动程序配置。

在 Identity Manager 插件中，如果单击一个 1.1a 格式的驱动程序，则系统会提示您完成转换。这是一个通过向导完成的简单的过程，并且该过程不会更改驱动程序配置的功能。作为该过程的一部分，将会保存 DirXML 1.1a 版本的备份拷贝。

- 将 DirXML 1.1a 驱动程序与 Identity Manager 引擎一起运行时，这些驱动程序的激活仍然有效。但是，如果将驱动程序 Shim 升级为 Identity Manager 版本，则需要获取新的激活身份凭证。有关详细信息，请参见附录 6 “激活 Novell Identity Manager 产品”在第 101 页。
- 在多数情况下， Identity Manager 驱动程序 Shim 可以与 DirXML 1.1a 配置一起运行。有关升级信息，请参见各个驱动程序实施指南 (http://www.novell.com/documentation/dirxmldrivers/index.html)。

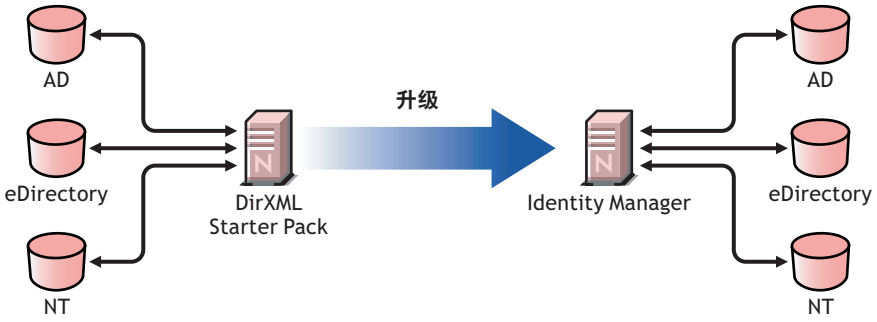
  一个值得注意的例外是，升级驱动程序 Shim 后，除非添加某些额外的驱动程序策略，否则 Password Synchronization 1.0 对 AD 和 NT 不能正常运行。有关指导，请参见 Identity Manager Drivers for Active Directory and NT Domain 的驱动程序实施指南 (http://www.novell.com/documentation/dirxmldrivers/index.html) 中有关口令同步的章节。
- 不支持将 Identity Manager 驱动程序 Shim 和驱动程序配置与 DirXML 1.1a 引擎一起运行。
- 不支持将 Identity Manager 驱动程序配置与 DirXML 1.1a 驱动程序 Shim 一起运行。
- 如果在多个服务器上运行同一个 Identity Manager 驱动程序配置，请确保这些服务器运行相同的 Identity Manager 版本，并且运行相同的 eDirectory 版本。

口令管理

- 可以创建为用户提供某些功能 （例如要求使用更强口令的高级口令规则、忘记口令自助服务和重设置口令自助服务）的口令策略。请参见口令管理指南中的以下章节：
  - “管理口令同步”
- 如果开始使用带有 NetWare 6.5® 初始发行版的通用口令，则只有在完成某些升级步骤后才能使用新的口令策略功能。请参见口令管理指南中的 《（仅限 NetWare 6.5）重新创建通用口令指派》。如果开始使用带有 NetWare 6.5 SP2 的通用口令，则不需要该过程。
- Identity Manager 口令同步提供双向口令同步，并且除了支持 Password Synchronization 1.0 以外，还支持其它多种平台。
- 如果对 AD 或 NT 使用 Password Synchronization 1.0，请确保在安装新的驱动程序 Shim 之前查看升级指导。请参见“从 Password Synchronization 1.0 升级为 Identity Manager 口令同步”在第 37 页。
- 提供了驱动程序策略 《覆盖》，以帮助您将双向口令同步功能添加到现有的驱动程序。请参见 《*Novell Identity Manager 3.0 Administration Guide*》（Novell Identity Manager 3.0 管理指南）中的 《Upgrading Existing Driver Configurations to Support Password Synchronization》（升级现有的驱动程序配置以支持口令同步）。

2.1.3 从 Starter Pack 升级为 Identity Manager

图 *2-3* 从 *Starter Pack* 升级为 *Identity Manager*



其它 Novell 产品中包含的 Identity Manager Starter Pack 解决方案可提供 NT Domain、 Active Directory 和 eDirectory 中保存的信息的已许可同步。此外，还包含了其它多个系统 （包括 PeopleSoft*、 GroupWise® 和 Lotus Notes*）的评估驱动程序，用于浏览其它系统的数据同步。

该解决方案还提供用于同步用户口令的功能。使用 PasswordSync，用户只需要记住一个口令便可以登录其中的任何一个系统。管理员可以管理所选系统中的口令。无论何时其中一个环境中的某个口令发生更改，将会更新所有环境中的该口令。

NetWare 6.5 和 Nterprise™ Linux Services 1.0 附带的 Identity Manager Starter Pack 基于 DirXML 1.1a 技术。从 Starter Pack 升级为 Identity Manager 的最新版本时，请记住下列注意事项：

- “管理工具”在第 35 页
- “向后兼容”在第 35 页
- “口令管理”在第 36 页
- “激活”在第 36 页

管理工具

- DirXML 1.1a 支持 ConsoleOne，但 Identity Manager 不支持。

向后兼容

- 可以在 Identity Manager 服务器上运行 DirXML 1.1a 驱动程序 Shim 和配置，并且可以在驱动程序集的 Identity Manager 概述中查看 iManager 中的驱动程序。但是，将驱动程序配置转换为 Identity Manager 格式之前，不能使用 Identity Manager 插件查看或编辑这些驱动程序配置。

  在 Identity Manager 插件中，如果单击一个 1.1a 格式的驱动程序，则系统会提示您完成转换。这是一个通过向导完成的简单的过程，并且该过程不会更改驱动程序配置的功能。作为该过程的一部分，将会保存 DirXML 1.1a 版本的备份拷贝。
- 将 DirXML 1.1a 驱动程序与 Identity Manager 引擎一起运行时，这些驱动程序的激活仍然有效。但是，如果将驱动程序 Shim 升级到 Identity Manager 版本，则需要新的激活身份凭证。

- 在多数情况下， Identity Manager 驱动程序 Shim 可以与 DirXML 1.1a 配置一起运行。有关升级信息，请参见各个驱动程序实施指南 (http://www.novell.com/documentation/dirxmldrivers/index.html)。

  一个值得注意的例外是，升级驱动程序 Shim 后，除非添加某些额外的驱动程序策略，否则 Password Synchronization 1.0 对 AD 和 NT 不能正常运行。有关指导，请参见 Identity Manager Drivers for Active Directory and NT Domain 的驱动程序实施指南 (http://www.novell.com/documentation/dirxmldrivers/index.html) 中有关口令同步的章节。
- 不支持将 Identity Manager 驱动程序 Shim 和驱动程序配置与 DirXML 1.1a 引擎一起运行。
- 不支持将 Identity Manager 驱动程序配置与 DirXML 1.1a 驱动程序 Shim 一起运行。
- 如果在多个服务器上运行同一个 Identity Manager 驱动程序配置，请确保这些服务器运行相同的 Identity Manager 版本，并且运行相同的 eDirectory 版本。

口令管理

- 升级驱动程序 Shim 后，除非添加某些额外的驱动程序策略，否则 Starter Packs (DirXML 1.1a) 附带的 Password Synchronization 1.0 对 AD 和 NT 不能正常运行。有关指导，请参见 Identity Manager Drivers for Active Directory and NT Domain 的驱动程序实施指南 (http://www.novell.com/documentation/dirxmldrivers/index.html) 中有关口令同步的章节。
- 有关此升级过程的特定指导，请参考 “从 Password Synchronization 1.0 升级为 Identity Manager 口令同步”在第 37 页 。

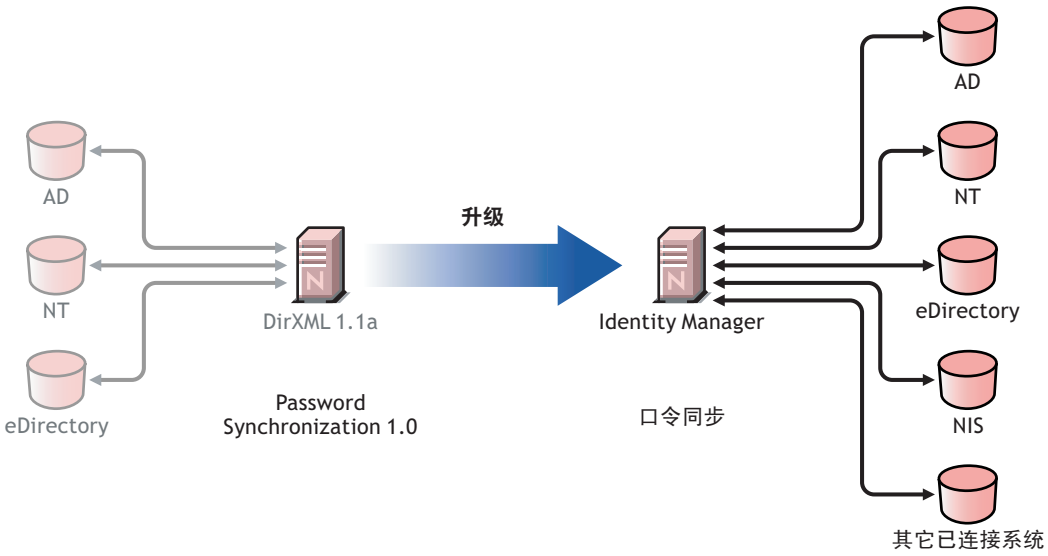
激活

- 所有 Identity Manager 产品必须在 90 天内激活。如果购买了其它 Novell 软件， DirXML Starter Pack 会包含 DirXML 1.1a 引擎、 NT、 AD 和 eDirectory 驱动程序的激活身份凭证。从 Identity Manager Starter Pack 升级后，需要重新应用这些驱动程序的激活身份凭证。

  有关激活的更多信息，请参考附录 6“激活 Novell Identity Manager 产品”在第 101 页 。

2.1.4 从 Password Synchronization 1.0 升级为 Identity Manager 口令同步

图 **2-4** 从 *Password Synchronization 1.0* 升级为 *Identity Manager* 口令同步



Identity Manager 口令同步提供许多功能，包括双向口令同步、附加平台，以及口令同步失败时的电子邮件通知。

如果使用带有 Active Directory 或 NT Domain 的 Password Synchronization 1.0，请务必在安装新的驱动程序 Shim 之前，查看升级指导。

如果运行带有 Password Synchronization 2.0 的 Identity Manager 2.x，则不需要遵循这些步骤。

有关 Identity Manager 口令同步的一般信息，请参见 《*Novell Identity Manager 3.0 Administration Guide*》（Novell Identity Manager 3.0 管理指南）中的 《Password Synchronization across Connected Systems》（在已连接系统间同步口令）。该节包含概念性信息，包括新旧功能的比较、前提条件、每个已连接系统支持的功能的列表、向现有驱动程序添加支持的指导，以及显示新功能使用方式的多个案例。

本节包括：

- “升级 AD 或 NT 的口令同步”在第 37 页
- “升级 eDirectory 的口令同步”在第 38 页
- “升级其它已连接系统驱动程序”在第 38 页
- “处理敏感信息”在第 38 页

升级 AD 或 NT 的口令同步

新的口令同步功能是由驱动程序策略执行的，而不是由独立的代理执行的。这意味着如果在安装新的驱动程序 Shim 的同时不升级驱动程序配置，Password Synchronization 1.0 只能对现有用户继续发挥作用。在完成驱动程序配置的升级之前，新用户、已移动的用户或重命名的用户不参与口令同步。

使用下列常规步骤进行升级：

1. 升级环境使之支持通用口令，包括升级 Novell Client （如果使用的话）。
2. 安装 Identity Manager 3.0 驱动程序 Shim，以替换 AD 或 NT 的 DirXML 1.1a 驱动程序 Shim。
3. 将新的策略添加到驱动程序配置，立即创建 Password Synchronization 1.0 的向后兼容性。

   执行该步骤后，在切换到 Identity Manager 口令同步之前， Password Synchronization 1.0 可持续正常运行。
4. 使用驱动程序策略为新的 Identity Manager 口令同步添加支持。
5. 安装和配置新的口令同步过滤器。
6. 必要时设置 SSL。
7. 必要时使用口令策略打开通用口令。
8. 设置需要使用的 Identity Manager 口令同步方案。

   请参见 《*Novell Identity Manager 3.0 Administration Guide*》（Novell Identity Manager 3.0 管理指南）中的 《Implementing Password Synchronization》（实现口令同步）。
9. 去除 Password Synchronization 1.0

有关详细指导，请参见 Identity Manager Drivers for Active Directory and NT Domain 的驱动程序实施指南 (http://www.novell.com/documentation/dirxmldrivers/index.html)。

升级 **eDirectory** 的口令同步

对 eDirectory 进行升级相当简单，并且，假定驱动程序 Shim 和配置具有最新增补程序的话，驱动程序 Shim 将会配合现有的 DirXML 1.1a 驱动程序配置且不发生更改。有关指导，请参见 《*Identity Manager Driver for eDirectory: Implementation Guide*》（Identity Manager Driver for eDirectory：实施指南）。

升级其它已连接系统驱动程序

除了支持 Password Synchronization 1.0 以外， Identity Manager 口令同步还支持其它许多已连接系统。

有关受支持的其它系统的功能列表，请参见 《*Novell Identity Manager 3.0 Administration Guide*》（Novell Identity Manager 3.0 管理指南）中的 《Connected System Support for Password Synchronization》（口令同步支持的已连接系统）。

提供了驱动程序策略 《覆盖》，以帮助您将双向口令同步功能添加到以前不支持的已连接系统的现有驱动程序。请参见 《*Novell Identity Manager 3.0 Administration Guide*》（Novell Identity Manager 3.0 管理指南）中的 《Upgrading Existing Driver Configurations to Support Password Synchronization》（升级现有的驱动程序配置以支持口令同步）。

处理敏感信息

通用口令受到 eDirectory 中四个加密层的保护，因此它在该环境中非常安全。如果选择使用双向口令同步，并且将通用口令与分发口令同步，请记住这是在抽取 eDirectory 口令，并将它发送到另一个已连接系统。需要对口令的传输进行保护，同时还要保护口令同步到的已连接系统。请参见 《*Novell Identity Manager 3.0 Administration Guide*》（Novell Identity Manager 3.0 管理指南）中的 《Security: Best Practices》（安全性：最佳做法）。

2.2 计划 Identity Manager 实施的项目管理方面

本节概述了实施 Identity Manager 的高级政治管理和项目管理方面。（有关技术方面的信息，请参见 “计划 Identity Manager 实施的技术方面”在第 44 页。）

本计划材料概述从 Identity Manager 项目的成形到完全在生产中部署的过程中，通常要执行的活动的类型。实施身份管理策略需要发现需求以及环境中的利害关系人、设计解决方案、获得利害关系人的认可，以及测试和推行解决方案。本节旨在帮助您充分了解该过程，以便您能够从 Identity Manager 的使用中获得最大的收益。

强烈建议聘任一个 Identity Manager 专家来为解决方案部署的每个阶段提供支援。有关合作伙伴关系选项的更多信息，请参见 Novell 解决方案合作伙伴万维网站点 (http://www.novell.com/partners/)。Novell 培训还提供与 Identity Manager 实施有关的课程。

本节尚有未尽事宜，其目的并不是讲述所有可能的配置，也不是具体讲述配置的执行。每个环境都存在差异，因此在使用的活动类型上需要灵活处理。

2.2.1 Novell Identity Manager 部署

可以将下列多项活动建议为部署 Identity Manager 时的最佳做法：

- “发现”在第 39 页
- “需求和设计分析”在第 40 页
- “概念认证”在第 43 页
- “数据验证和准备”在第 43 页
- “试生产”在第 43 页
- “生产成品计划”在第 44 页
- “生产部署”在第 44 页

发现

Identity Manager 实施可以从发现过程开始，该过程实现以下目的：

- 确定身份信息管理的主要目标
- 定义或阐明要解决的业务问题
- 确定解决突出问题需要完成哪些初期工作
- 确定执行其中一项或多项初期工作需要哪些东西
- 制定高级策略或《解决方案路标》，以及受到认可的执行途径

发现能使所有利害关系人对问题和解决方案形成共识。它为分析阶段提供了一个极好的基础，该阶段需要利害关系人对目录、Novell eDirectory、Novell Identity Manager 和 XML 集成有一个基本的了解。

- 它可以在所有利害关系人之间建立基本级别的理解
- 它可以从利害关系人那里获得主要业务信息和系统信息
- 它可以促成解决方案路标的制定

发现还将确定紧随其后的步骤，这些步骤可能包括以下项目：

- 确定计划活动，以便为需求阶段和设计阶段作准备
- 为利害关系人定义其它培训

主要交付产品

- 与主要业务和技术利害关系人进行有序的面谈
- 业务和技术问题的高级摘要报告
- 后续步骤的建议
- 概述发现结果的决策陈述

需求和设计分析

此分析阶段将获得项目的技术和业务方面的详细信息，以及生成数据模型和 Identity Manager 高级体系结构设计。此活动是至关重要的第一步，解决方案的实施将从这一步开始。

应该明确地将设计重心放在身份管理上，但是，也可以涉及到在传统上与资源管理目录（例如文件和打印）相关的许多要素。下面是可能需要评估的项目的样本：

- 所使用的系统软件的版本是什么？
- 目录设计是否恰当？
- 当前是否使用该目录来承载 Identity Vault 和 Identity Manager，或者是否使用它来扩展其它服务？
- 所有系统中的数据质量是否合格？ （如果数据达不到可用的质量，则可能无法根据需要实现业务策略。）
- 环境是否需要数据处理？

完成需求分析后，可为实施建立范围和项目计划，并可确定是否需要执行任何先期必要的活动。为避免出现代价高昂的失误，请尽量完整地收集信息和记录需求。

在需求评估过程中，可能需要完成下列任务：

- “定义业务需求”在第 40 页
- “分析业务流程”在第 41 页
- “设计企业数据模型”在第 42 页

定义业务需求

收集组织的业务过程以及定义这些业务过程的业务需求。

例如，解雇一个员工的业务需求可能是，在解雇该员工的同一天，必须去除该员工的网络和电子邮件帐户访问权限。

下列任务可以引导您定义业务需求：

- 建立流程、过程触发器和数据映射关系。

  例如，如果某件事将在特定的过程中发生，那么该过程会导致发生什么事？ 将会触发其它哪些过程？
- 在应用程序之间映射数据流。

- 确定发生时需要从一种格式转换为另一种格式的数据转换，例如 2/25/2006 转换为 25 Feb 2006。
- 记录存在的数据依赖性。

  如果更改了某个特定的值，则务必要知道该值是否存在依赖性。如果更改了特定的过程，则务必要知道该过程是否存在依赖性。

  例如，选择人力资源系统中某个 《临时》 员工状态值，可能意味着 IT 部门需要在 eDirectory 中创建一个用户对象，该用户对象在特定的小时数内对网络的权限和访问权限将受到限制。
- 列出优先级。

  并不是每一方的每个需求、愿望或期望都可以立即实现。设计和部署供应系统的优先级有助于计划路标。

  将部署划分为多个阶段是有利的做法，这样可以先实施部署的一部分，后实施部署的其它部分。也可以采取分阶段的部署方法。这种方法应该基于组织中的员工小组。
- 定义前提条件。

  应该记录实施部署特定阶段所需的前提条件。这包括对需要与 Identity Manager 连接的已连接系统的访问权限。
- 确定授权数据源。

  事先了解系统管理员和经理认为属于他们的信息项目，有助于获取各方的认可并让他们持续认可。

  例如，帐户管理员可能希望有权为员工授予对特定文件和目录的权限。在帐户系统中执行本地受托者指派可以达到此目的。

分析业务流程

业务流程的分析通常由会见关键人 （例如实际使用应用程序或系统的经理、管理员和员工）开始。要解决的问题包括：

- 数据源于何处？
- 数据流向何处？
- 数据由何人负责？
- 谁拥有对数据所属业务功能的所有权？
- 需要联系何人更改数据？
- 更改数据牵涉到的各个方面有哪些？
- 数据处理的工作惯例是什么 （收集和 / 或编辑）？
- 执行何种类型的操作？
- 使用什么方法保证数据的质量和完整性？
- 系统寄存在何处 （在哪些服务器上，在哪些部门中）？
- 哪些过程不适用于自动处理？

例如，人力资源的 PeopleSoft 系统管理员可能面临的问题包括

- 将哪些数据储存在 PeopleSoft 数据库中？
- 员工帐户的各种面板上显示哪些内容？
- 供应系统中需要反映哪些操作 （例如添加、修改或删除）？

- 其中哪些是必需的？ 哪些是可选的？
- 需要根据 PeopleSoft 中执行的操作触发哪些操作？
- 要忽略哪些操作 / 事件 / 动作？
- 如何转换数据，以及将其映射到 Identity Manager？

会见关键人可了解组织的其它区域，这样可以更清楚地展现整个过程。

设计企业数据模型

定义业务过程后，可以开始设计反映当前业务流程的数据模型。

模型应该演示数据的来源、其转移到的位置以及不能转移到的位置。它还应说明关键事件如何影响数据流。

您还可能希望制作图表，用于演示建议的业务过程以及在该过程中实现自动供应的优势。

此模型的开发由回答类似以下的问题开始：

- 正在移动哪些类型的对象 （用户、组等等）？
- 哪些是相关事件？
- 哪些特性需要同步？
- 在整个业务过程中，针对被管理的各种类型的对象储存了哪些数据？
- 同步是单向还是双向的？
- 哪个系统是哪些特性的权威来源？

考虑系统之间不同值的相互关系也很重要。

例如， PeopleSoft 的员工状态字段可能有三个设置值：员工、合同工和试用员工。但是，Active Directory 系统可能只有两个值： 《永久》和 《临时》。在此情况下，需要确定 PeopleSoft 中的 《合同工》状态，以及 Active Directory 中的 《永久》和 《临时》值。

此工作的重点应是了解每个目录系统、它们如何彼此相关，以及在整个系统中哪些对象和特性需要同步。

主要交付产品

- 数据模型，显示所有系统、授权数据源、事件、信息流和数据格式标准，以及 Identity Manager 中已连接系统和特性之间的映射关系。
- 解决方案的相应 Identity Manager 体系结构
- 附加系统连接要求的详细信息
- 数据验证和记录匹配的策略
- 用于支持 Identity Manager 基础结构的目录设计

相关性

- 熟悉所有外部系统的职员 （如 HR 数据库管理员、网络和讯息系统管理员）
- 系统纲要和样本数据的可用性
- 来自分析和设计阶段的数据模型
- 组织结构图、 WAN 和服务器基础结构等基本信息的可用性

概念认证

此活动的结果是提供一份在实验室环境下使用的实施样本，用于反映贵公司的业务策略和数据流。该结果基于在需求分析和设计过程中开发的数据模型设计，并且是试生产前的最后一个步骤。

注释：此步骤通常有助于获得管理层的支持，以及为最终实施工作获得资金。

主要交付产品

- 在所有系统连接均正常工作的情况下完成的可行的 Identity Manager 概念认证

相关性

- 硬件平台和设备
- 必需软件
- 确定必需连接的分析和设计阶段
- 供测试使用的其它系统的可用性以及对这些系统的访问权限
- 来自分析和设计阶段的数据模型

数据验证和准备

在生产系统中数据的质量和一致性可能不同，因此同步系统时可能会造成不一致的情况。此阶段明确展示资源实施小组与业务单位或组 （《拥有》或管理要集成的系统中的数据）之间的分隔点。相关的风险和成本因素有时不能纳入供应项目。

主要交付产品

- 适合载入 Identity Vault 的生产数据集 （已在分析和设计活动中确定）。这包括装载的可能性方法 （大批量装载或通过连接程序）。同时确定已验证或格式化的数据的要求。
- 同时针对使用的设备以及 Identity Manager 部署的整体分布式结构确定并验证性能因子。

相关性

- 来自分析和设计阶段的数据模型 （建议的记录匹配和数据格式策略）
- 对生产数据集的访问权限

试生产

此活动的目的是开始迁移到生产环境中。在此阶段可能有其它自定义操作发生。在此有限的简介中，可确认前面的活动所需的结果，并获得生产成品的协议。

注释：此阶段可提供解决方案的验收准则以及达到全面生产所必需的路标和路线。

主要交付产品

- 试行解决方案，为数据模型以及所需的过程结果提供真实的概念认证和验证

相关性

- 所有以前的活动 （分析和设计、 Identity Manager 技术平台）。

生产成品计划

在此阶段计划生产部署。计划应：

- 确认服务器平台、软件修订版和 Service Pack
- 确认常规环境
- 确认在混合共存中 Identity Vault 的简介
- 确认分区和复制策略
- 确认 Identity Manager 实施
- 计划传统过程的交接
- 计划回滚应变策略

主要交付产品

- 生产成品计划
- 传统过程交接计划
- 回滚应变计划

相关性

- 所有以前的活动

生产部署

将在此阶段展开试行解决方案，以影响生产环境中的所有实际数据。它通常遵循这样的协议：试生产符合所有的技术和业务要求。

主要交付产品

- 生产解决方案已准备好进行转换

相关性

- 所有以前的活动

2.3 计划 Identity Manager 实施的技术方面

- “使用 Designer”在第 44 页
- “在服务器上复制 Identity Manager 需要的对象”在第 45 页
- “使用范围过滤管理不同服务器上的用户”在第 46 页

2.3.1 使用 Designer

Identity Manager 3.0 附带一个称作 《Designer》的新工具。Designer 可用于设计、测试和记录 Identity Manager 驱动程序。Designer 还可用于查看口令同步和数据流动的方式。有关更

多信息，请参见 《*Designer for Identity Manager 3:Administration Guide*》（Designer for Identity Manager 3：管理指南）。

2.3.2 在服务器上复制 Identity Manager 需要的对象

如果 Identity Manager 环境访问多个服务器以运行多个 Identity Manager 驱动程序，那么作为计划的一部分，您需要确保在运行这些 Identity Manager 驱动程序的服务器上复制某些 eDirectory 对象。

只要已过滤复本中包括驱动程序需要读取或同步的所有对象和特性，就可以使用这些复本。

请记住，必须为 Identity Manager 驱动程序对象授予对任何要同步的对象的足够 eDirectory 权限，方法是通过显式授权，或者使驱动程序对象的安全性等效于具有所需权限的对象。

运行 Identity Manager 驱动程序的 eDirectory 服务器 （如果使用远程装载程序，则是驱动程序参照的 eDirectory 服务器）必须保存下列主复本或读 - 写复本：

- 该服务器的驱动程序集对象。

  运行 Identity Manager 的每个服务器都应该有一个驱动程序集对象。除非有特定的需求，否则不要将多个服务器与同一个驱动程序集对象关联。

  注释：创建驱动程序集对象时，默认设置是创建独立的分区。Novell 建议在驱动程序集对象上创建独立的分区。要使 Identity Manager 正常运行，服务器需要保存驱动程序集对象的完整复本。如果服务器具有驱动程序集对象的安装位置的完整复本，则不需要分区。

- 该服务器的服务器对象。

  由于驱动程序使用服务器对象为对象生成密钥对，因此服务器对象是必需的。对于远程装载程序鉴定来说它也很重要。

- 需要驱动程序的该实例与其同步的对象。

  除非对象的复本与驱动程序位于同一台服务器上，否则驱动程序不能同步这些对象。事实上，除非创建规则以另行指定 （《范围过滤》的规则），否则， Identity Manager 驱动程序将同步在服务器上复制的所有树枝中的对象。

  例如，如果需要驱动程序与所有用户对象同步，则最简单的方法就是使用服务器上的驱动程序的一个实例，该服务器保存所有用户的主复本或读 / 写复本。

  但是，许多环境都没有包含所有用户复本的单台服务器。而是整个用户集分布在多台服务器上。在这种情况下，存在两种选择：

  - 将用户聚合到单台服务器。可通过向现有服务器添加复本来创建保存所有用户的单台服务器。如果需要，只要必需的用户对象和特性是已过滤复本的一部分，就可以使用已过滤复本减少 eDirectory 数据库的大小。
  - 在启用范围过滤的情况下，使用多台服务器上的驱动程序的多个实例。如果不希望将用户聚合到单台服务器，则需要确定由哪个服务器集保存所有用户，同时在其中的每个服务器上设置 Identity Manager 驱动程序的一个实例。

    为防止驱动程序的不同实例尝试与相同的用户同步，需要使用 《范围过滤》来定义驱动程序的每个实例应该同步的用户。范围过滤表示向每个驱动程序添加规则，以将驱动程序的管理范围限制到特定的树枝。请参见 “使用范围过滤管理不同服务器上的用户”在第 46 页 。

- 在没有启用范围过滤的情况下，使用多台服务器上的驱动程序的多个实例。如果要使驱动程序的多个实例在不同服务器上运行且不使用已过滤复本，则需要对不同的驱动程序实例定义策略，使驱动程序能够处理相同 Identity Vault 中的不同对象集。

- 创建用户时需要驱动程序使用的模板对象 （如果选择使用模板）。

  Identity Manager 驱动程序不要求指定用于创建用户的 eDirectory 模板对象。但是，如果指定驱动程序在 eDirectory 中创建用户时应使用模板，则必须在运行驱动程序的服务器上复制模板对象。

- Identity Manager 驱动程序管理用户时需要使用的任何树枝。

  例如，如果创建了一个名称为 《Inactive Users》的树枝以保存禁用的用户帐户，则必须在运行驱动程序的服务器上，提供该树枝的主复本或读 / 写复本 （最好是主复本）。

- 驱动程序需要参照的其它任何对象 （例如， Avaya PBX 驱动程序的工作指令对象）。

  如果驱动程序只是读取而不是更改其它对象，则服务器上的这些对象的复本可以是只读复本。

2.3.3 使用范围过滤管理不同服务器上的用户

范围过滤表示向每个驱动程序添加规则，以将驱动程序的操作范围限制到特定的树枝。在以下两种情况下，可能需要使用范围过滤：

- 希望驱动程序只同步特定树枝中的用户。

  默认情况下， Identity Manager 驱动程序将同步运行该驱动程序的服务器上复制的所有树枝中的对象。要缩小该范围，必须创建范围过滤规则。

- 希望 Identity Manager 驱动程序同步所有用户，但不希望在同一服务器上复制所有用户。

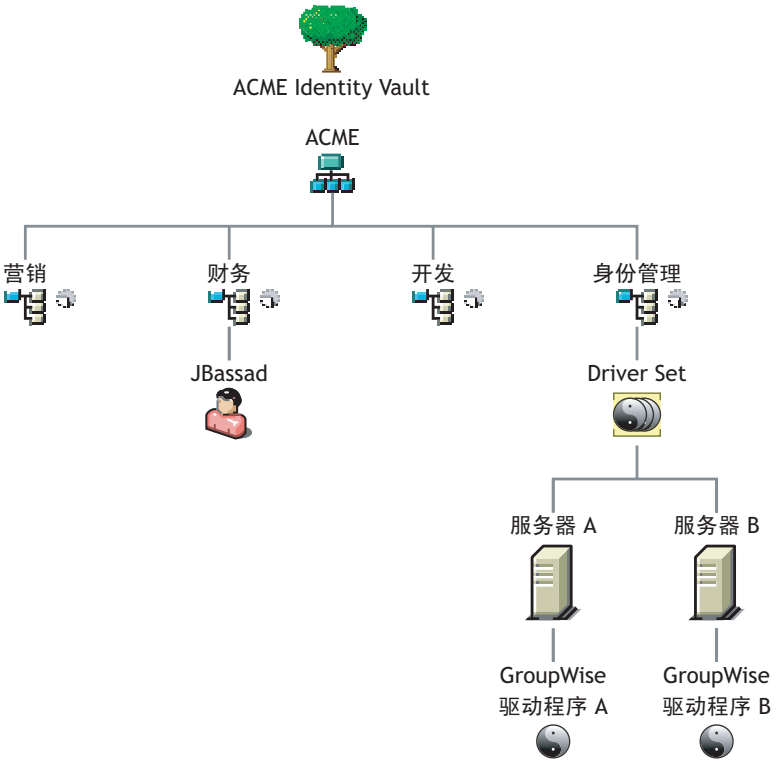
  要同步所有用户且不在单台服务器上复制它们，需要确定由哪个服务器集保存所有用户，然后在其中的每台服务器上创建 Identity Manager 驱动程序的实例。为防止驱动程序的两个实例尝试与相同的用户同步，需要使用 《范围过滤》来定义驱动程序的每个实例应该同步的用户。

注释 **:** 即使服务器的复本当前未重叠，也应该使用范围过滤。以后，服务器上可能会添加复本，因而在无意中产生重叠。如果实施了范围过滤， Identity Manager 驱动程序就不会尝试同步相同的用户，即使以后向服务器添加复本，也是如此。

下面是范围过滤使用方法的范例。

下图显示了一个 Identity Vault，它带有保存用户的三个树枝：Marketing、 Finance 和 Development。同时该图还显示保存驱动程序集的 Identity Manager 树枝。其中每个树枝都是一个独立的分区。

图 ***2-5*** 范围过滤的示例树



在此示例中， Identity Manager 管理员有两个 Identity Vault 服务器：服务器 A 和服务器 B，如下图所示。两个服务器都不包含所有用户的拷贝。每个服务器包含三个分区中的两个，因此服务器保存项目的范围重叠。

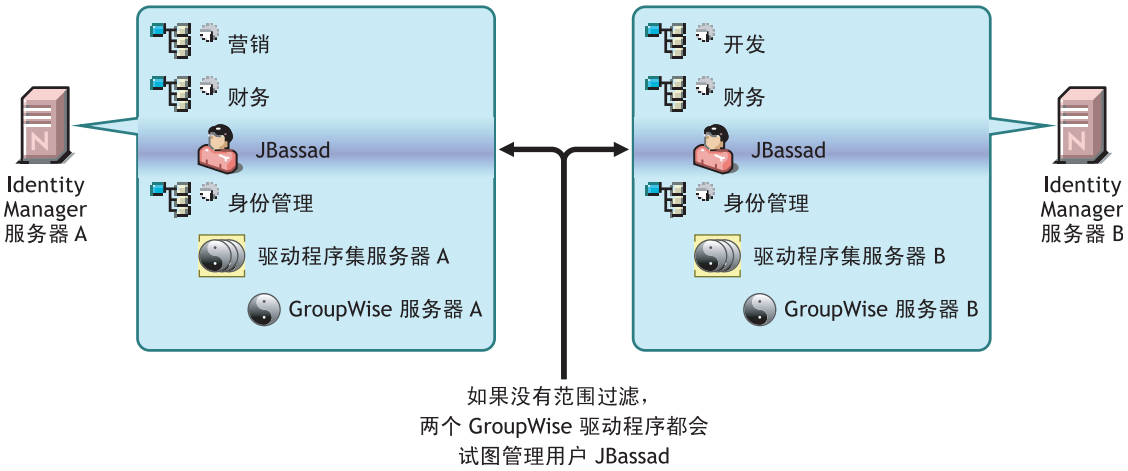
管理员希望通过 GroupWise® 驱动程序同步树中的所有用户，但是不希望将这些用户的复本聚合到单台服务器。他选择使用 GroupWise 驱动程序的两个实例，两台服务器各使用一个。他在每台 Identity Manager 服务器上安装 Identity Manager，然后设置 GroupWise 驱动程序。

服务器 A 保存 Marketing 和 Finance 树枝的复本。同时， Identity Management 树枝的复本也在该服务器上，该树枝保存服务器 A 的驱动程序集以及服务器 A 的 GroupWise 驱动程序对象。

服务器 B 保存 Development 和 Finance 树枝的复本，同时， Identity Management 树枝也在该服务器上，该树枝保存服务器 B 的驱动程序集和服务器 B 的 GroupWise 驱动程序对象。

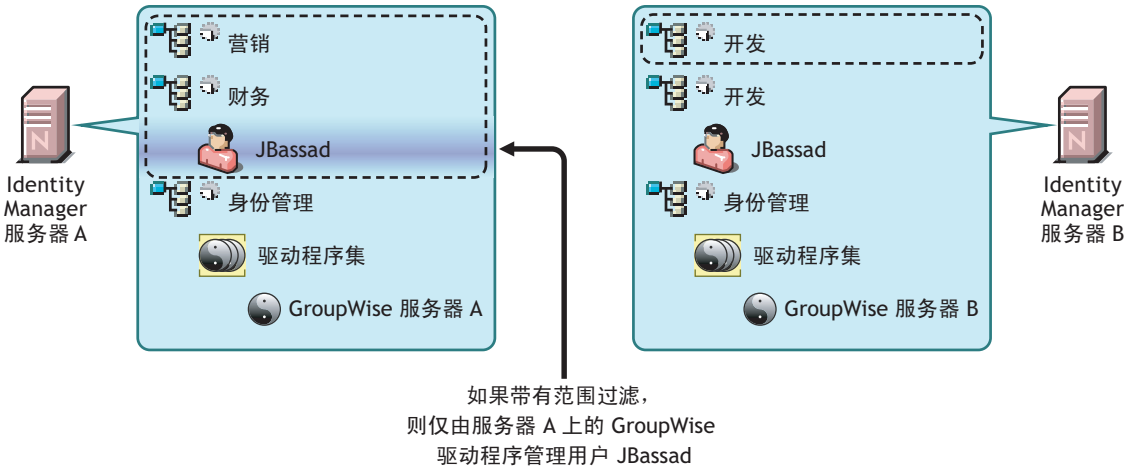
由于服务器 A 和服务器 B 均保存了 Finance 树枝的复本，因此这两个服务器均保存了 Finance 树枝中的用户 Jbassad。如果不使用范围过滤， GroupWise 驱动程序 A 和 GroupWise 驱动程序 B 都会同步 Jbassad。

图 **2-6** 带重叠复本的两个服务器，不使用范围过滤



下图显示由于范围过滤已定义了由哪些驱动程序同步每个树枝，因此它可以防止驱动程序的两个实例管理相同的用户。

图 **2-7** 范围过滤定义由哪些驱动程序同步每个树枝



Identity Manager 3.0 附带了预定义规则。有两个规则可帮助执行范围过滤。 《*Policy Builder and Driver Customization Guide*》（策略构建器和驱动程序自定义指南）中记录的 《Event Transformation - Scope Filtering - Include Subtrees》（事件转换 – 范围过滤 – 包括子树）和 《Event Transformation - Scope Filtering - Exclude Subtrees》（事件转换 – 范围过滤 – 排除子树）。

对于此示例，可以对服务器 A 和服务器 B 使用 《包括子树》预定义规则。可为每个驱动程序定义不同的范围，以便它们只同步指定的树枝中的用户。服务器 A 将同步 Marketing 和 Finance。服务器 B 将同步 Development。

升级

3

Identity Manager 有许多不同的组成部分。要升级 Identity Manager，需确保已考虑产品的各个方面，这样升级才能成功。

“常见安装实例”在第 31 页 中说明了一些升级方案。

3.1 升级路径

下表包含 Identity Manager 各版本支持的升级方案。以支持或不支持的形式列出了每种方案。

表 *3-1* 升级路径方案

安装的版本	当前版本	是否支持升级？
DirXML® 1.1a	Identity Manager 3.0	是
Identity Manager 2.x	Identity Manager 3.0	是

3.2 升级过程

要成功地升级到 Identity Manager 3.0，需要完成下列步骤。

3.2.1 导出驱动程序

升级之前的最重要步骤是获取当前驱动程序的备份及其配置信息。要获取驱动程序的备份，需要导出驱动程序。

从 **ConsoleOne** 导出

1 在 ConsoleOne 中，右击驱动程序集对象，然后选择 《属性》 > 《DirXML》 > 《驱动程序》。

2 选择要为其创建导出的驱动程序，然后单击 《导出》。

3 指定一个文件名。保留默认的扩展名 .xml，然后单击 《保存》。

4 单击 《导出配置》。

在 iManager 中，可以导出一个驱动程序，也可以导出整个驱动程序集。如果导出驱动程序集，则会创建单个配置文件。如果导出每个驱动程序，则为每个驱动程序创建一个配置文件。

从 **iManager** 导出

1 在 iManager 中选择 《DirXML 实用程序》 > 《导出驱动程序》。

2 浏览并选择要导出的驱动程序或驱动程序集，然后单击 《下一步》。

3 将提示字段留空，以便按原样创建驱动程序的拷贝，然后单击 《下一步》。

4 如果选择驱动程序集对象，则会收到每个驱动程序的提示页。将每个驱动程序的字段留空，以便按原样创建拷贝。

5 单击 《另存为》。

6 在 《文件下载》窗口单击 《保存》。

7 浏览并指定文件位置和导入的名称，然后单击 《保存》。

重要：保存文件后，该文件的扩展名必须是 .xml。

完成驱动程序的导出后，在实验室环境下测试该导出。导入驱动程序导出并测试驱动程序，以确保所有参数正确，且没有丢失任何功能。

3.2.2 校验最低要求

要升级到 Identity Manager 3.0，运行 Identity Manager 服务的服务器需满足最低要求。有关每个平台的最低要求的列表，请参见 “Identity Manager 组件和系统要求”在第 53 页 。

如果需要升级支持组件，请按以下顺序完成升级：

1. 将 OS 升级为受支持的版本。例如，将 NetWare® 6.0 升级到 NetWare 6.5。
2. 将 eDirectory™ 升级到带有最新增补程序的 eDirectory 8.73，或者升级到 eDirectory 8.8.1。
3. 将 iManager 升级到 iManager 2.6 SP2 （包括升级 Apache 2.0.52 或更高版本，以及 Tomcat 4.1.18 或更高版本）。
4. 升级 Identity Manager。
5. 激活 Metadirectory 引擎和任何已升级的驱动程序。

3.2.3 升级引擎

升级支持组件后，即会升级 DirXML 或 Identity Manager 引擎。

1 确保具有驱动程序的有效导出。

2 停止驱动程序。

2a 在 iManager 中选择 《Identity Manager》 > 《Identity Manager 概述》。

2b 浏览并选择驱动程序集对象，然后单击 《搜索》。

2c 单击驱动程序图标的右上角，然后选择 《停止驱动程序》。

3 将驱动程序设置为手动启动。

3a 在 iManager 中选择 《Identity Manager》 > 《Identity Manager 概述》。

3b 浏览并选择驱动程序集对象，然后单击 《搜索》。

3c 单击驱动程序图标的右上角，然后选择 《编辑属性》。

3d 在 《驱动程序配置》 页中的 《启动选项》 下选择 《手动》。

4 安装 Identity Manager 3.0。升级到 Identity Manager 3.0 的步骤与安装 Identity Manager 3.0 时执行的步骤相同。有关如何安装 Identity Manager 的指导，请参见第 4 章 “安装 Identity Manager”在第 53 页。

5 设置驱动程序启动选项。

5a 在 iManager 中选择 《Identity Manager》 > 《Identity Manager 概述》。

5b 浏览并选择驱动程序集对象，然后单击 《搜索》。

5c 单击驱动程序图标的右上角，然后选择 《编辑属性》。

5d 在 《驱动程序配置》 页中的 《启动选项》 下，选择 《自动启动》，或选择优先的驱动程序启动方法。

6 查看驱动程序参数和策略，确保一切均按需要进行设置。

7 启动驱动程序。

7a 在 iManager 中选择 《Identity Manager》 > 《Identity Manager 概述》。

7b 浏览并选择驱动程序集对象，然后单击 《搜索》。

7c 单击驱动程序图标的右上角，然后选择 《启动驱动程序》。

3.2.4 升级远程装载程序

如果运行远程装载程序，则还需要升级远程装载程序文件。

1 创建远程装载程序配置文件的备份。这些文件的默认位置为：

- Windows C:\Novell\RemoteLoader*remoteloadername*-config.txt
- Linux – 在 rdxml 路径中创建自己的配置文件。

2 停止远程装载程序服务或守护程序。

3 运行远程装载程序的安装程序。这将更新现有版本的文件和二进制格式。请参见 《*Novell Identity Manager 3.0 Administration Guide*》（Novell Identity Manager 3.0 管理指南）中的 《Installing Remote Loaders》（安装远程装载程序）。

3.3 升级口令同步

如果从 DirXML 1.1a 升级到 Identity Manager 3.0，则需要升级口令同步。请参见 《*Novell Identity Manager 3.0 Administration Guide*》（Novell Identity Manager 3.0 管理指南）中的 《Upgrading Password Synchronization 1.0》（升级 Password Synchronization 1.0）。

如果从 Identity Manager 2.x 升级，则不执行升级，原因是口令同步相同。

3.4 从 RNS 升级到 Novell Audit

反对使用报告和通知服务 (RNS)，尽管在当前使用 RNS 的情况下，引擎仍会继续处理 RNS 功能。应计划改用 Novell® Audit，因为 Novell Audit 扩展了 RNS 提供的功能 , 而 Identity Manager 将来的发行版可能不支持 RNS。

有关更多信息，请参见 《*Novell Identity Manager 3.0 Administration Guide*》（Novell Identity Manager 3.0 管理指南）中的 《Logging and Reporting Using Novell Audit》（使用 Novell Audit 进行日志记录和报告）。

3.5 升级 DirXML 1.1a 驱动程序配置

如果从 DirXML 1.1a 升级到 Identity Manager 3.0，则会升级驱动程序配置。升级驱动程序配置有两个方面的问题：

- 将规则转换为 Identity Manager 策略。该操作可通过转换工具完成，同时它不会增强驱动程序的功能。不需要此转换即可运行旧的驱动程序，但可以通过转换查看 Identity Manager iManager 插件中的现有驱动程序配置。
- 升级驱动程序策略以添加新功能。最好由 Identity Manager 专家来处理此操作。

请参见 《*Novell Identity Manager 3.0 Administration Guide*》（Novell Identity Manager 3.0 管理指南）中的 《Upgrading a Driver Configuration from DirXML 1.1a to Identity Manager Format》（将驱动程序配置由 DirXML 1.1a 升级为 Identity Manager 格式）和 《Managing DirXML 1.1a Drivers in an Identity Manager Environment》（在 Identity Manager 环境中管理 DirXML 1.1a 驱动程序）。

另一种做法是首先进行 Identity Manager 驱动程序配置，然后自定义这些配置，使它们的功能与 DirXML 1.1a 配置的功能相同。

3.6 激活 Identity Manager 3.0

升级完成后，可以在 90 天内激活 Metadirectory 引擎和已经升级的任何驱动程序。如果不激活引擎和驱动程序， 90 天过后它们将停止工作。有关激活 Identity Manager 3.0 的指导，请参见第 6 章 “激活 Novell Identity Manager 产品”在第 101 页 。

安装 Identity Manager

4

本节包含安装 Identity Manager 和 Identity Manager 驱动程序的要求和指导。

4.1 安装前

安装 Identity Manager 之前，请参考第 2 章 “计划”在第 31 页 。

4.2 Identity Manager 组件和系统要求

Novell Identity Manager 包含可以在环境中的多个系统和平台上安装的组件。根据系统配置的不同，可能需要多次运行 Identity Manager 安装程序才能在相应的系统上安装 Identity Manager 组件。

下表列出了四个 Identity Manager 安装组件以及对每个系统的要求。

系统组件	系统要求	注释
Metadirectory 服务器 ◆ Metadirectory 引擎 ◆ Novell® Audit 代理 ◆ 服务驱动程序 ◆ Identity Manager 驱动程序	下列操作系统之一。 ◆ 带最新 Support Pack 的 NetWare® 6.5 ◆ 带最新 Support Pack 的 Novell Open Enterprise Server (OES) ◆ Windows* NT ◆ 带最新 Service Pack 的 Windows 2000 Server （32 位） ◆ 带最新 Service Pack 的 Windows Server 2003 R2（不支持 2003 64 位） ◆ Linux Red Hat* AS 3.0 ◆ Linux Red Hat AS 4.0 for AMD 64/EM64T ◆ 带最新 Support Pack 的 SUSE® Linux Enterprise Server 8、 9 或 10 ◆ Solaris 8、 9 或 10 ◆ AIX 5.2L 下列 eDirectory 版本之一： ◆ 带最新 Support Pack 的 eDirectory 8.7.3 ◆ 带最新 Support Pack 的 eDirectory 8.8 ◆ 带最新 Support Pack 的 eDirectory 8.8.1 建议将 eDirectory 8.8 升级到 8.8.1。	如果 VMWare 安装在一个受支持的 Metadirectory 服务器平台上，则可以在实施中使用该 VMWare。 除非另行指定，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： ◆ Intel x86 ◆ AMD x86 ◆ Intel EM64T ◆ AMD Athlon64 和 Opteron eDirectory 8.8 及更高版本支持下列高级功能： ◆ 同一服务器上的多个 eDirectory 实例 ◆ 加密的特性 尽管 eDirectory 8.8 及更高版本包括对非根用户安装的支持，但您必须以根用户的身份安装 Identity Manager。 eDirectory 8.8.1 支持 64 位 Red Hat Linux AS 和 ES 4.0。但是， eDirectory 8.8.x 不支持 Solaris 8。 安装 eDirectory 8.8.1 之前，请务必完全备份 eDirectory 数据库。 eDirectory 8.8.1 将会升级数据库结构的某些部分，并且在完成升级过程后，它不允许数据库结构回滚。 SUSE Linux Enterprise Server 10 不支持 XEN 虚拟化。
已连接系统服务器 ◆ 远程装载程序 ◆ 远程装载程序配置工具 （仅限 Windows） ◆ Novell Audit 代理 ◆ 已连接系统的驱动程序 Shim ◆ 已连接系统的工具	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/dirxmldrivers)。	

系统组件	系统要求	注释
基于万维网的管理服务器 • Identity Manager 和口令管理 iManager 插件 • 驱动程序配置 • 最终用户口令自助服务	下列操作系统之一： • 带最新 Support Pack 的 Novell Open Enterprise Server (OES) • 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 R2 （不支持 2003 64 位） • Linux Red Hat AS 3.0 （Glibc 版本 2.1.1 或更高版本，内核版本 2.2.*xx* 或更高版本。） • Linux Red Hat AS 4.0 for AMD 64/EM64T • Solaris 9 或 10 • 带最新 Support Pack 的 SUSE Linux Enterprise Server 8、 9 或 10 通过 iManager 工作站支持操作系统： • 带最新 Service Pack 的 Windows 2000 Professional • Windows XP • Red Hat Enterprise Linux Workstation • SUSE Linux 9.1 或 9.3 下列软件。 • Novell iManager 2.6 Support Pack 2 或更高版本 （包括 Apache 2.0.52 或更高版本，以及 Tomcat 4.1.18 或更高版本）	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： • 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： • Internet Explorer 6 SP1 和更高版本 • Firefox 1.5.0.x 和更高版本 • Mozilla 1.7 和更高版本 • 必须使用 iManager 配置向导或 Designer 实用程序将入口内容安装或部署到 eDirectory。 • 如果将 iManager 2.6 安装在 eDirectory 所在的同一台服务器上，则 eDirectory 的版本必须为 8.7.3 或更高。 • (Windows) 可以从 Novell 软件下载 (http://download.novell.com/index.jsp) 获取 Novell Client™ 4.9。 • 使用 iManager 登录到其它树以管理远程 Identity Manager 服务器时，如果使用该远程服务器的服务器名而不是 IP 地址，则可能会遇到错误。

系统组件	系统要求	注释
实用程序 • 许可证监查工具 • 应用程序工具（AD、 Notes、SAP、PeopleSoft 和 JDBC） • Novell Audit 设置工具	有关每个系统特定的要求，请参考 Identity Manager 驱动程序文档 (http://www.novell.com/documentation/dirxmldrivers)。	每个连接的应用程序都要求个人具有应用程序特定的知识并承担相关责任。 远程装载程序系统： • Windows NT 4.0、 Windows 2000 或 Windows 2003 • Red Hat Linux AS 3.0 • Linux Red Hat AS 4.0 • SUSE Linux Enterprise Server 8、 9 或 10 • Solaris 8、 9 或 10 • AIX 5L v5.2 Java 远程装载程序系统： • HP-UX 11i • OS/400 • zOS • 应该可以在具有 JVM 1.4.2 或更高版本的任何系统上使用

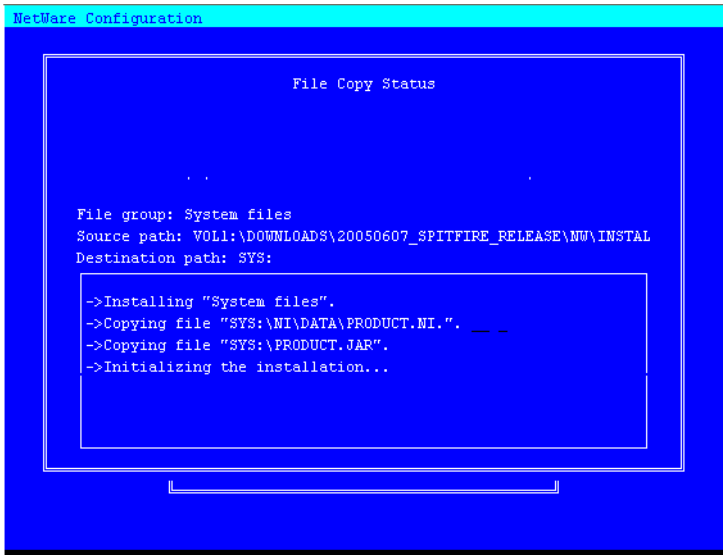
4.3 在 NetWare 上安装 Identity Manager

该过程包括适用于 NetWare 的 Metadirectory 服务器、万维网组件和实用程序的安装。开始之前，请确保系统符合 “Identity Manager 组件和系统要求”在第 53 页 中列出的要求。

1. 下载并解压缩 Identity Manager 安装文件。可以从 Novell 下载站点 (http://download.novell.com) 下载 Identity Manager 安装文件。
2. 将文件解压缩后，在服务器控制台提示符下键入 nwconfig。
3. 选择 《产品选项》 > 《安装未列出的产品》。
4. 按 F3 键 （如果您使用 RCONSOLE，则按 F4 键），然后指定 \NW 目录中 Identity Manager NetWare 安装文件的路径。

过一段时间后，图形安装实用程序将会启动。

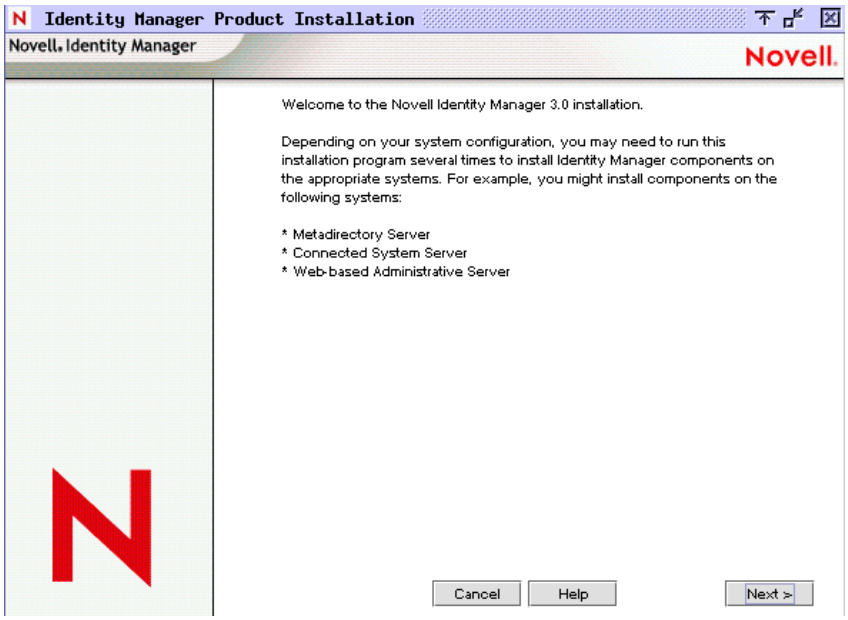
图 **4-1** *Identity Manager* 安装文件的初始设置



还可以直接转至服务器 GUI 并从 Novell 图标的位置选择 《安装》来开始安装过程。在 《安装的产品》屏幕上选择 《添加》，然后在 《源路径》屏幕上键入指向 \NW 目录中的 products.ni 文件的路径。单击 《确定》。

5 完成文件的复制后，将显示 《Identity Manager 产品安装》页。单击 《下一步》开始安装。

图 **4-2** *Identity Manager* 初始安装页



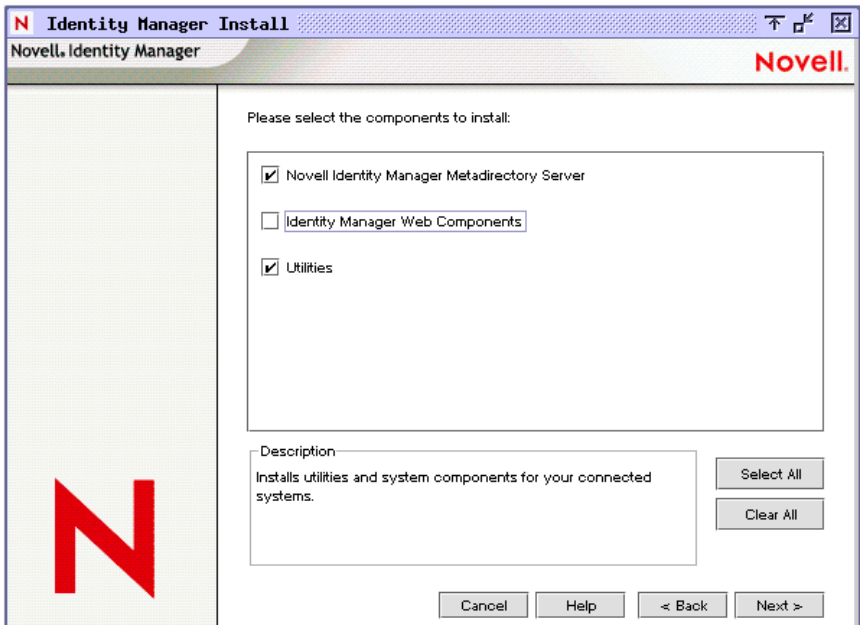
6 阅读许可协议，然后单击 《我接受》。

7 查看描述系统类型 （包括 《Metadirectory 引擎》、《万维网组件》和 《实用程序》）的 《概述》页。单击 《下一步》继续。

“Identity Manager 组件和系统要求”在第 53 页 中的表内也包括了这些信息。

8 在 《Identity Manager 安装》页上，选择要安装的组件：请参见 “Identity Manager 组件和系统要求”在第 53 页 。

图 *4-3* *Identity Manager* 安装选项



下面是可用选项。对于大多数安装，可以选择所有的组件。

- **Metadirectory** 服务器：安装 Metadirectory 引擎和服务驱动程序。在 NetWare 平台上，这些安装项目包括 Identity Manager Drivers for eDirectory、 LDAP、 JDBC、 GroupWise、Delimited Text、Composer、Avaya、SOAP、SIF 和 Novell Audit 代理。选择该选项还会扩展 eDirectory 纲要。

  只有在安装 Novell eDirectory 后才能安装该选项。如果要运行 Identity Manager 的 Metadirectory 引擎，请安装 Metadirectory 服务器组件。

- 已连接系统：安装远程装载程序，用于在已连接系统和运行 Metadirectory 引擎的服务器之间建立链接。对于 NetWare，该选项还将安装下列驱动程序：LDAP、JDBC、 GroupWise、 Composer、 Avaya、 SOAP、 SIF 和 Delimited Text。

  注释 : 对于 Identity Manager 的 NetWare 安装，该选项不可用，并且不在 《安装》屏幕上显示。

- **Identity Manager** 万维网组件：该选项将安装 Identity Manager 插件和驱动程序配置。

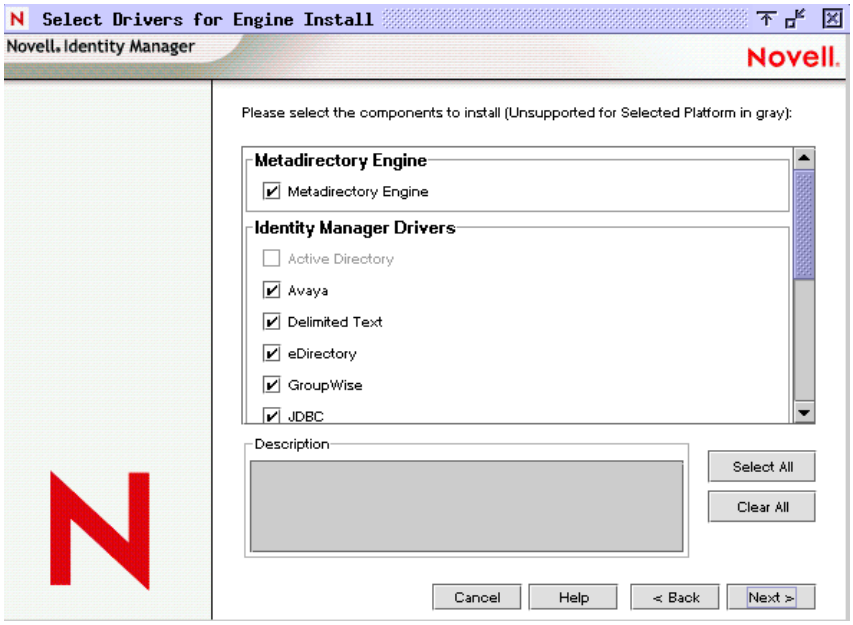
  只有安装了 Novell iManager 才能安装该选项。

- 实用程序：安装 JDBC 驱动程序的其它底稿，以及其它驱动程序的实用程序。大多数驱动程序没有与实用程序连接。

9 单击 《下一步》。

10 选择要安装的驱动程序，然后单击 《下一步》。

图 ***4-4*** 选择 *Metadirectory* 引擎的驱动程序



《Select Drivers for Engine Install （选择用于安装引擎的驱动程序）》页显示可以在相应平台上安装哪些驱动程序。例如，在 NetWare 服务器上，无法安装 Windows Active Directory 驱动程序。

默认情况下，将选择选项的所有可用驱动程序。建议安装所有选定的驱动程序文件，这样，如果以后想要另一个驱动程序，就不需要运行安装程序。通过 iManager 或 Designer 配置驱动程序且将其部署之前，不使用这些驱动程序文件。

注释：如果此时不安装所有的驱动程序，则需要重新运行安装程序来安装。或者可以使用 Designer 创建、修改和部署驱动程序文件。

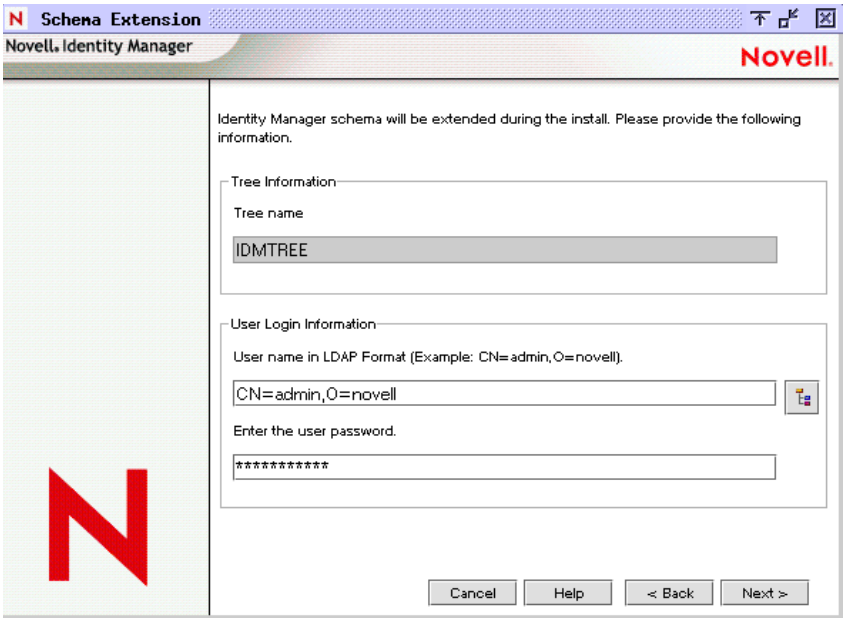
---

11 显示提醒有关产品激活的信息性讯息时，单击 《确定》。

需要在安装驱动程序后的 90 天内对其激活，否则它们将会关闭。

12 在 《纲要扩展》页上，指定下列项目：

图 *4-5* 纲要扩展页

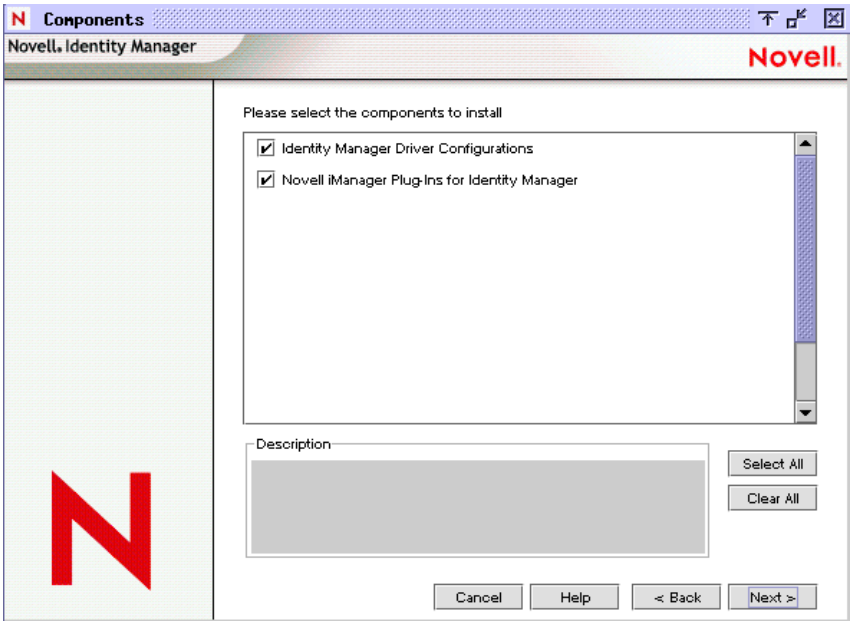


- 用户名： 指定有权扩展纲要的用户的用户名 （使用 LDAP 格式，例如 CN=admin,O=novell）。在此屏幕上，选择有足够权限扩展 eDirectory 纲要的用户（例如 Admin）。
- 用户口令：指定用户的口令。

13 单击 《下一步》。验证用户信息后，将显示第一个 （共三个）《组件》页：

14 在第一个 《组件》页上，选择驱动程序配置和 iManager 插件，然后单击 《下一步》。

图 *4-6* 第一个组件页



15 在第二个 《组件》页上，单击 《下一步》。

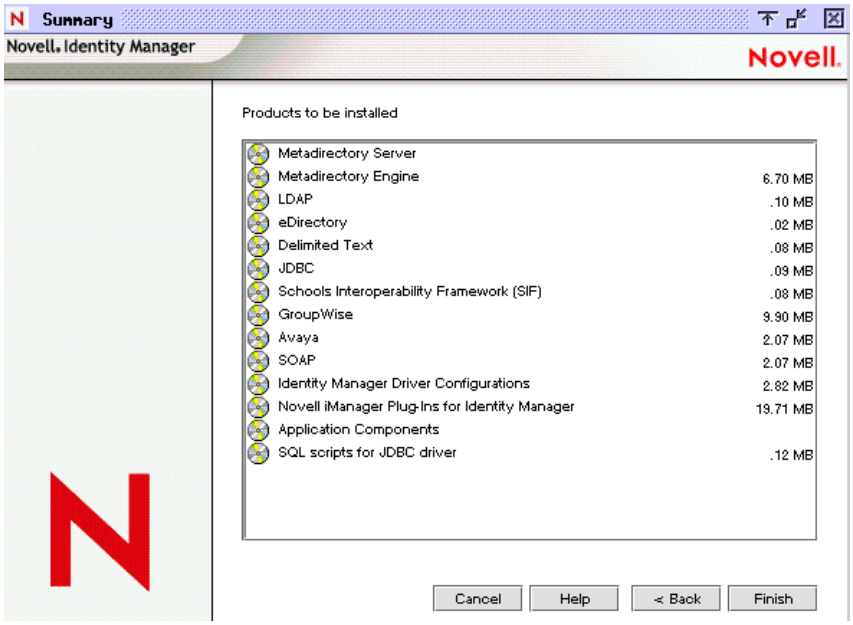
如果在服务器上安装了 Novell Audit System，则 《Novell Audit System Components for Identity Manager》将会高亮显示。否则，将不会选择该项。 《应用程序组件》选项用于安装 JDBC 和 PeopleSoft 等应用程序系统的组件。

16 第三个 《组件》页用于安装实用程序。单击 《下一步》。

如果平台特定的实用程序不可用于在其上执行安装的平台，则这些实用程序将会灰显。对于 NetWare，唯一可用的选项为 《SQL Scripts for JDBC Driver》。

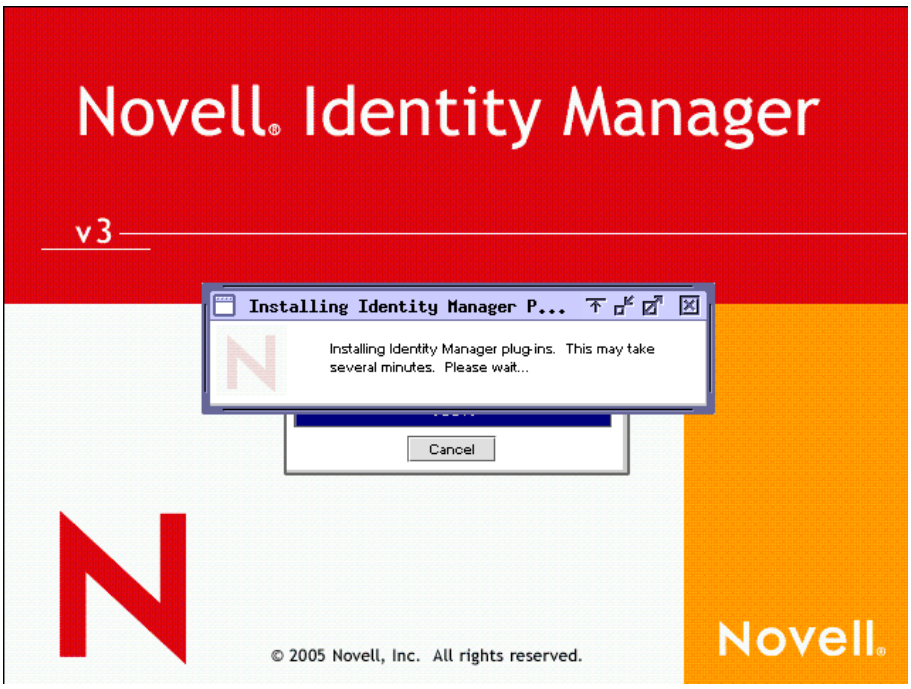
17 在 《摘要》页上阅读并确认选项，然后单击 《完成》。

图 *4-7* 摘要页显示要安装的产品和组件



Novell Identity Manager 安装过程将会关闭 eDirectory 以扩展纲要。安装过程开始安装选定的产品和组件。

图 **4-8** *NetWare* 服务器上的安装过程



18 安装完成并显示 《安装完成》对话框后，单击 《关闭》。重启动服务器以完成 Metadirectory 引擎的安装，然后重启动 Tomcat。

4.4 在 Windows 上安装 Identity Manager

该过程包括适用于 Windows 的 Metadirectory 服务器、万维网组件和实用程序的安装。

开始之前，请确保系统符合 “Identity Manager 组件和系统要求”在第 53 页 中列出的要求。

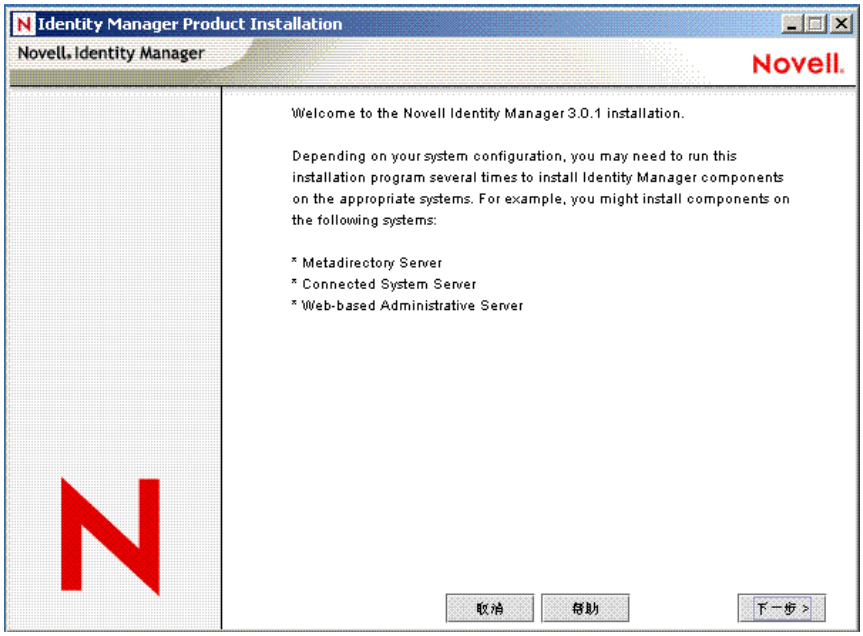
1 下载并解压缩 Identity Manager 安装文件。

可以从 Novell 下载站点 (http://download.novell.com) 下载 Identity Manager 安装文件

2 解压缩文件后，双击 \NT 目录中显示的 install.exe 文件。

完成文件的复制后，将显示 《Identity Manager 产品安装》屏幕。

图 **4-9** *Identity Manager* 初始安装页



3 单击 《下一步》开始安装。

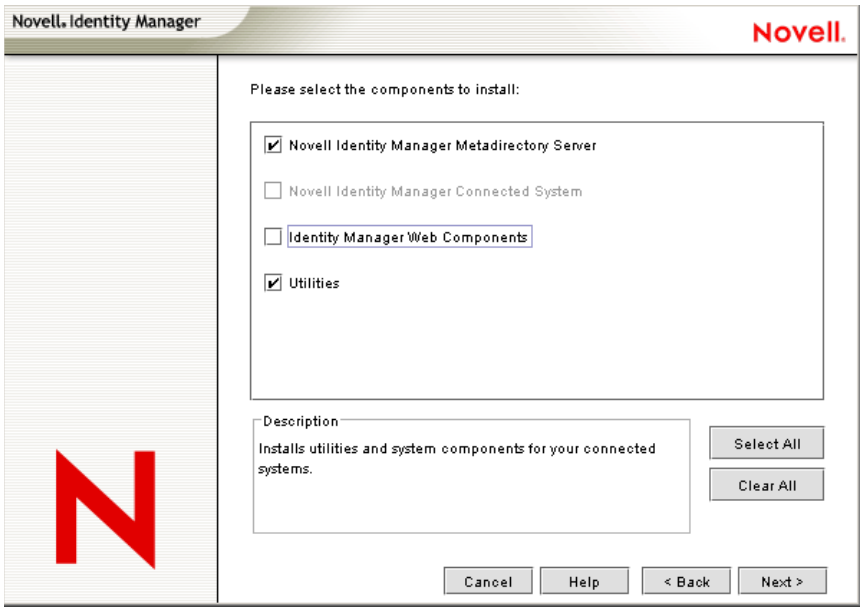
4 阅读许可协议，然后单击 《我接受》。

5 查看描述系统类型 （包括 《Metadirectory 引擎》、《万维网组件》和 《实用程序》）的 《概述》页。然后单击 《下一步》继续。

“Identity Manager 组件和系统要求”在第 53 页 中的表内也包括了这些信息。

6 在 《Identity Manager 安装》页上，选择要安装的组件：

图 **4-10** *Identity Manager* 安装选项



下面是可用选项：

- **Metadirectory** 服务器：安装 Metadirectory 引擎和服务驱动程序。这些安装项目包括 Identity Manager Drivers for eDirectory、 LDAP、 JDBC、 GroupWise、 Delimited Text、 Composer、 Remedy、 Avaya、 SOAP、 SIF 和 Novell Audit 代理。选择该选项还会扩展 eDirectory 纲要。

  只有在安装 Novell eDirectory 后才能安装该选项。如果要运行 Identity Manager 的 Metadirectory 引擎，请安装 Metadirectory 服务器组件。

- 已连接系统：安装远程装载程序，用于在已连接系统和运行 Metadirectory 引擎的服务器之间建立链接。对于 Windows，该选项将安装下列驱动程序：Active Directory、 Delimited Text、 Exchange、 GroupWise、 JDBC、 LDAP、 Lotus Notes、 NT Domain、 PeopleSoft、 Composer、 Remedy、 Avaya、 SOAP、 SAP 和 SIF。

  安装已连接系统，使应用程序能够从应用程序服务器连接到运行 Metadirectory 引擎的、基于 eDirectory 的服务器。 “在 Windows 上安装已连接系统选项”在第 67 页 中包括该过程。

- 万维网组件：该选项用于安装驱动程序配置、 iManager 插件、应用程序底稿和实用程序。

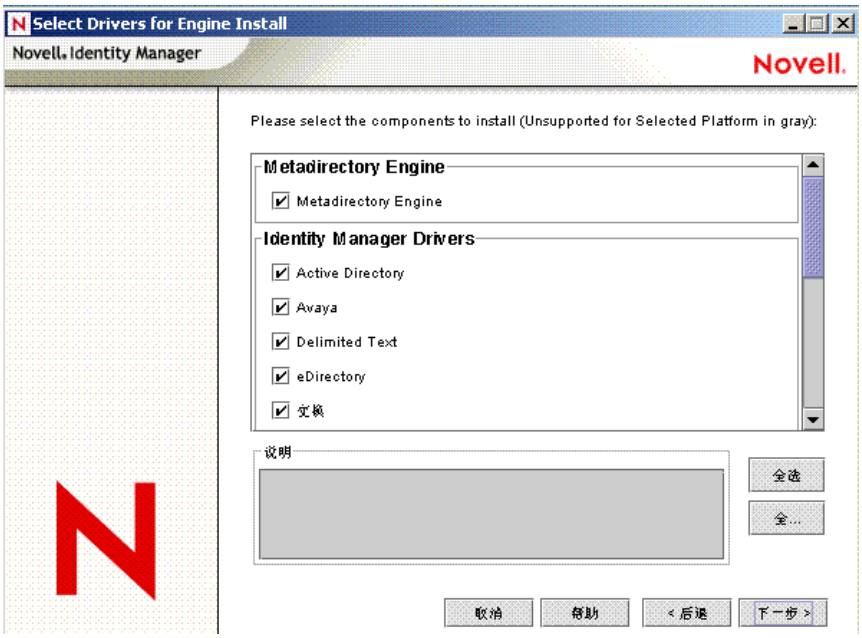
  只有在安装 Novell iManager 后才能安装该选项。

- 实用程序：安装 JDBC 驱动程序的其它底稿，以及其它驱动程序的实用程序。大多数驱动程序没有与实用程序连接。

7 单击 《下一步》。

8 选择要安装的驱动程序，然后单击 《下一步》。

图 ***4-11*** 选择 *Metadirectory* 引擎的驱动程序。



《选择用于安装引擎的驱动程序》页显示可以在相应平台上安装哪些驱动程序。默认情况下，将选择选项的所有可用驱动程序。

建议安装所有选定的驱动程序文件，这样，如果以后想要另一个驱动程序，就不需要运行安装程序。通过 iManager 或 Designer 配置驱动程序之前，不使用这些驱动程序文件。

9 显示提醒有关产品激活的信息性讯息时，单击 《确定》。

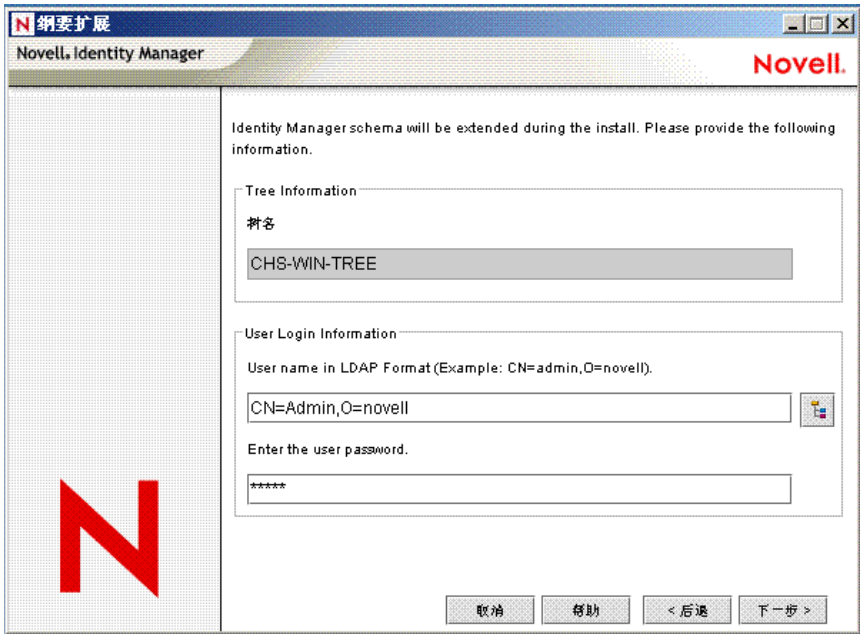
需要在安装驱动程序后的 90 天内对其激活，否则它们将会关闭。

10 同时还会显示 《口令同步升级警告！》讯息。单击 《确定》。

此讯息适用于运行 Password Synchronization 1.0 的 Windows 服务器。如果希望版本 1.0 具有向后兼容性，则必须将额外的策略添加到驱动程序配置文件。如果没有这些策略，Password Synchronization 1.0 只对现有帐户起作用，而对新帐户或重命名的帐户不起作用。

11 在 《纲要扩展》页上，指定下列项目：

图 *4-12* 纲要扩展页

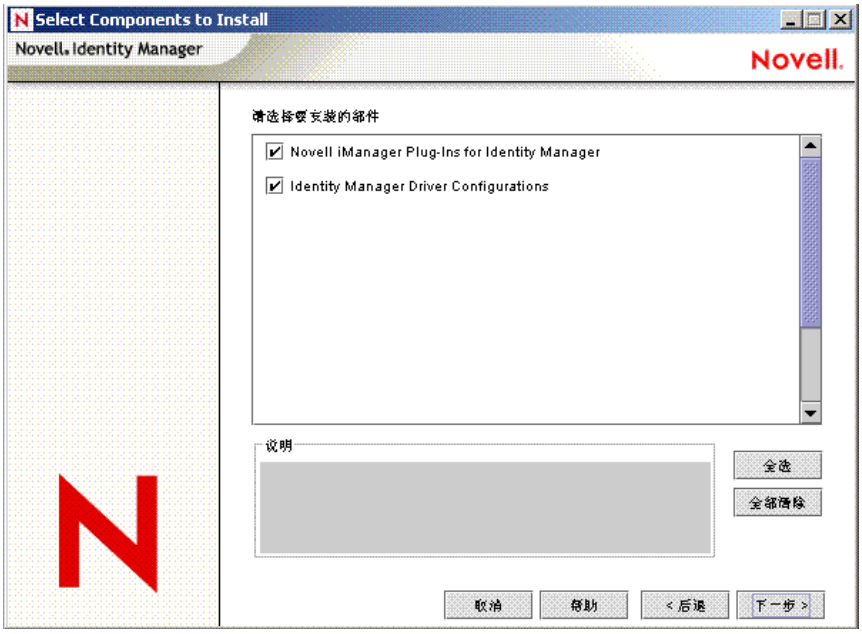


- 用户名： 指定有权扩展 eDirectory 纲要的用户的用户名 （使用 LDAP 格式，例如 CN=admin,O=novell）。
- 用户口令：指定用户的口令。

12 单击 《下一步》。验证用户信息后，将显示第一个 （共三个）《组件》页：

13 在第一个 《组件》页上，选择驱动程序配置和 iManager 插件，然后单击 《下一步》。

图 *4-13* 第一个组件页



将显示另一个屏幕，该屏幕用于通过 SSL 端口 443 安装 iManager 的 Identity Manager 插件。单击 《下一步》。

14 在第二个 《组件》页上，单击 《下一步》。

如果在服务器上安装了 Novell Audit System，则 《Novell Audit System Components for Identity Manager》将会高亮显示。否则，将不会选择该项。 《应用程序组件》选项用于安装 JDBC 和 PeopleSoft 等应用程序系统的组件。

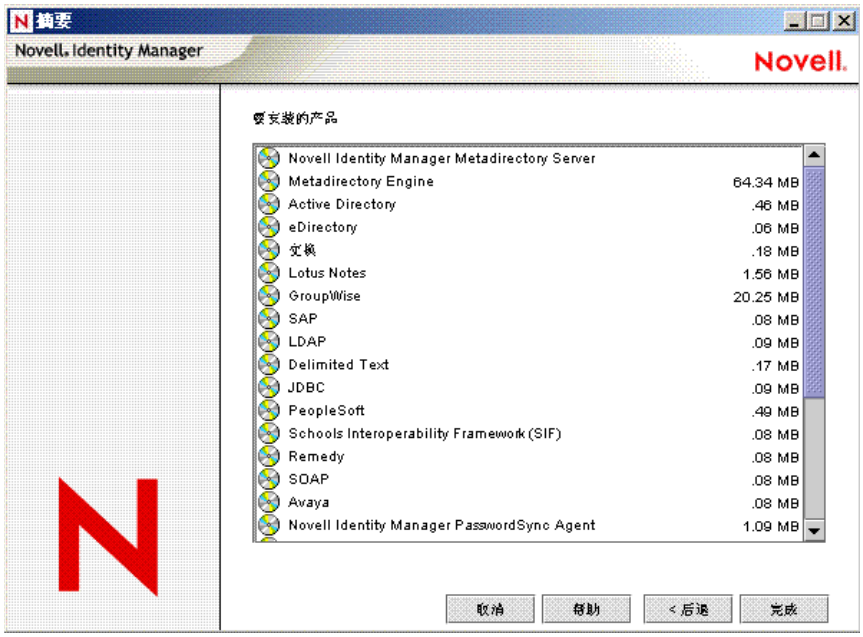
15 第三个 《组件》页用于安装实用程序。单击 《下一步》。

Windows 安装将出现另一个屏幕，其中显示放置应用程序组件的目录。默认值为 C:\Novell\NDS\DirXMLUtilities。单击 《下一步》。

16 在 《Select Components to Install （选择要安装的组件）》页上，如果平台特定的实用程序不可用于在其上执行安装的平台，则这些实用程序将会灰显。对于 Windows，所有组件均可用，这些组件包括 SQL Scripts for JDBC Driver、 PeopleSoft 组件、许可证监查工具、 Active Directory 发现工具、 Lotus Notes 发现工具和 SAP 实用程序。

17 在 《摘要》页上阅读并确认选项，然后单击 《完成》。

图 *4-14* 产品和组件的摘要屏幕



Novell Identity Manager 安装过程将会关闭 eDirectory 以扩展纲要。安装过程开始安装选定的产品和组件。

18 安装完成并显示 《安装完成》对话框后，单击 《关闭》。重启动服务器以完成 Metadirectory 引擎的安装，然后重启动 Tomcat。

4.5 在 Windows 上安装已连接系统选项

“在 Windows 上安装 Identity Manager”在第 62 页 包括适用于 Windows 的 Metadirectory 服务器、万维网组件和实用程序的安装。由于 Windows 服务器可以使用 《已连接系统》选项，因此这里也包括了用于安装已连接系统的选项。

如果不希望将 eDirectory 服务和 Metadirectory 引擎的开销施加到应用程序服务器，请使用 《已连接系统》选项。使用远程装载程序，便可以通过 Identity Manager 实现所需的同步，而不需要装载从其它位置即可访问的应用程序。

开始之前，请确保系统符合 “Identity Manager 组件和系统要求”在第 53 页 中列出的要求。

1 下载并解压缩 Identity Manager 安装文件。

可以从 Novell 下载站点 (http://download.novell.com) 下载 Identity Manager 安装文件

2 从 NT 目录运行 install.exe。

3 阅读欢迎信息，然后单击 《下一步》。

4 阅读许可协议，然后单击 《我接受》。

5 查看有关各个系统和组件的 《概述》页，然后单击 《下一步》开始安装。

6 在 《Identity Manager 安装》页上，选择组件 《已连接系统》和 《实用程序》：

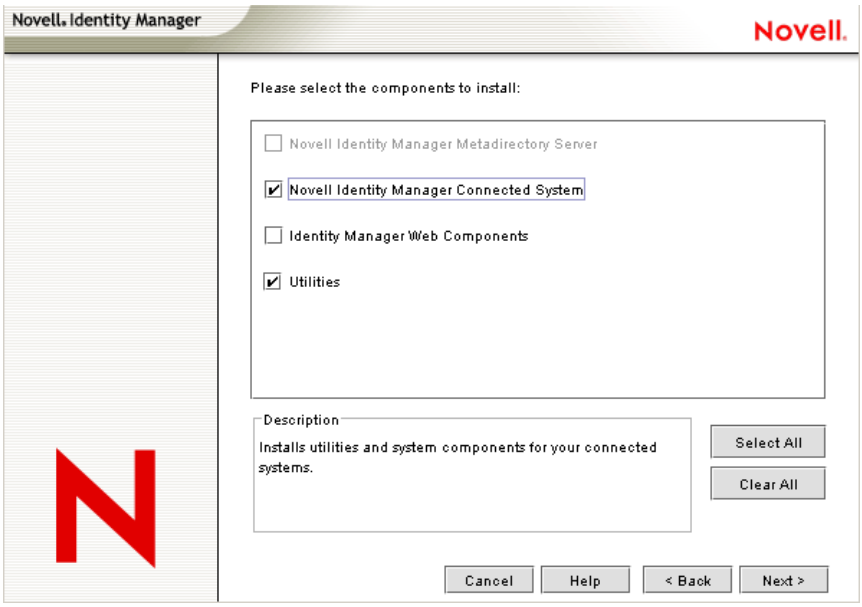
- 已连接系统：安装远程装载程序，用于在已连接系统和运行 Metadirectory 引擎的服务器之间建立链接。该选项可安装下列驱动程序：Active Directory、 Delimited

Text、 Exchange、 GroupWise、 JDBC、 LDAP、 Lotus Notes、 NT Domain、 PeopleSoft、 Composer、 Remedy、 Avaya、 Soap、 SAP 和 SIF，或仅仅是选定的驱动程序。

- 实用程序：安装 JDBC 驱动程序的其它底稿，以及选定的其它应用程序实用程序。

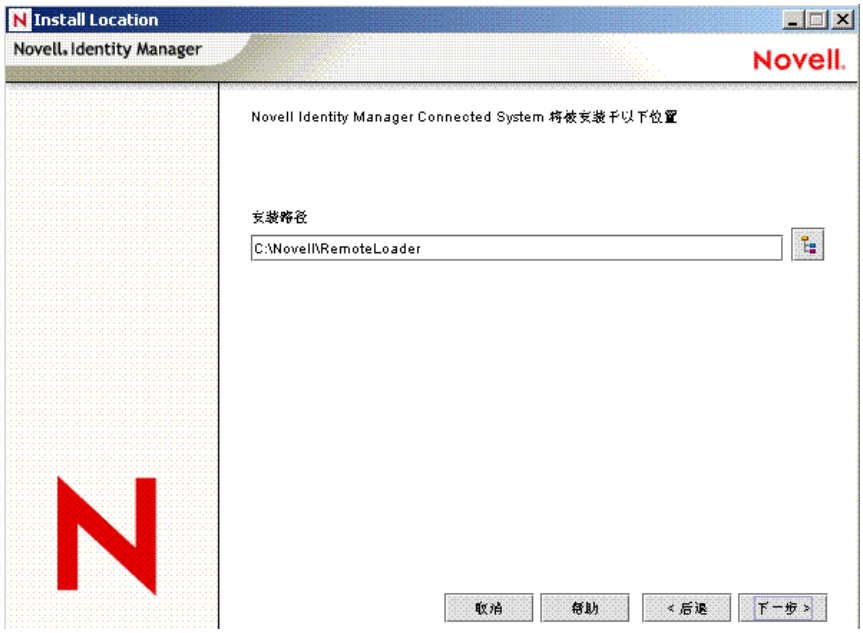
要选择 《已连接系统》选项，请先单击 《全部清除》，然后选择 《已连接系统》和 《实用程序》。如果在此服务器上安装了 iManager 实用程序，并且需要添加 Identity Manager 的 Identity Manager 插件以及驱动程序配置，则还应选择 《万维网组件》。

图 ***4-15*** 已连接系统选项



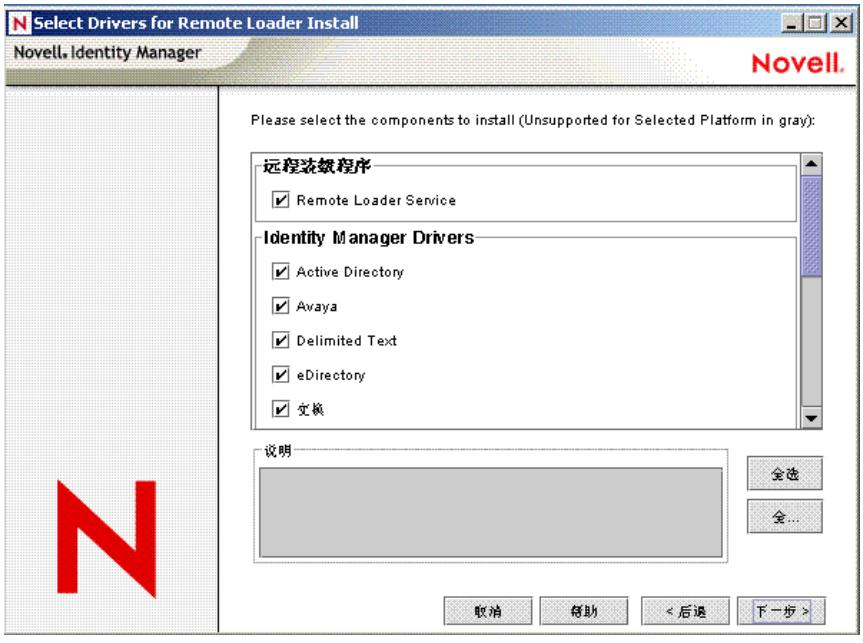
7 在 《安装位置》页上，单击 《下一步》接受默认的目录路径，即 C:\Novell\RemoteLoader。

图 *4-16* 选择安装位置。



8 在 《Select Drivers for Remote Loader Install （选择用于安装远程装载程序的驱动程序）》页上，选择需要装载的 Identity Manager 驱动程序，然后单击 《下一步》。选项包括 Active Directory、 Avaya、 Delimited Text、 eDirectory、 Exchange、 GroupWise、 JDBC、 LDAP、 Lotus Notes、 PeopleSoft、 Remedy、 SAP、 SIF 和 SOAP。

图 *4-17* 远程装载程序和 *Identity Manager* 驱动程序



9 显示提醒有关产品激活的信息性讯息时，单击 《确定》。

需要在安装驱动程序后的 90 天内对其激活，否则它们将会关闭。

10 同时还会显示 《口令同步升级警告！》讯息。单击 《确定》。

此讯息适用于运行 Password Synchronization 1.0 的 Windows 服务器。如果希望版本 1.0 具有向后兼容性，则必须将额外的策略添加到驱动程序配置文件。如果没有这些策略，Password Synchronization 1.0 只对现有帐户起作用，而对新帐户或重命名的帐户不起作用。

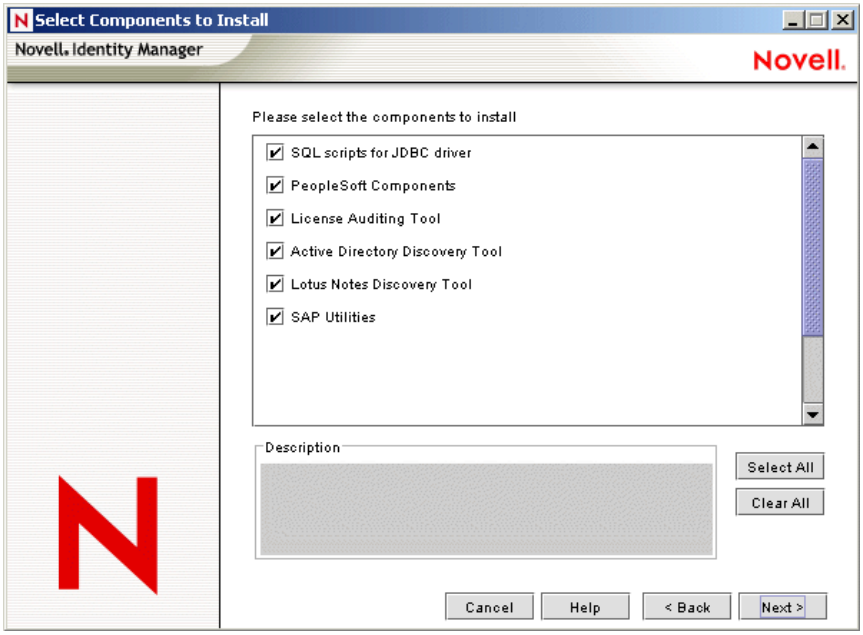
11 在 《要安装的组件》页上，单击 《下一步》。

如果在服务器上安装了 Novell Audit System，则 《Novell Audit System Components》将会高亮显示。否则，将不会选择该项。 《应用程序组件》选项用于安装 JDBC 和 PeopleSoft 等应用程序系统的组件。选择要安装的实用程序。

12 单击 《下一步》接受 Identity Manager 实用程序的默认安装路径 (C:\Novell\NDS\DirXMLUtilities)。

13 选择要安装的系统组件，然后单击 《下一步》。

图 ***4-18*** 系统组件



14 查看 《摘要》页列出的项目。如果认可，请单击 《完成》以安装组件。

15 单击 《是》在 Windows 服务器的桌面上添加一个快捷方式。

16 单击 《关闭》退出安装程序。

4.6 在 UNIX/Linux 平台上安装 Identity Manager

开始之前，请确保系统符合 “Identity Manager 组件和系统要求”在第 53 页 中列出的要求。

1 下载 tar 文件，并将其解压缩到所选的位置。

可以从 Novell 下载站点 (http://download.novell.com) 下载 Identity Manager 安装文件

2 在主机上以根用户的身份登录。

3 从安装目录执行 .bin 文件。

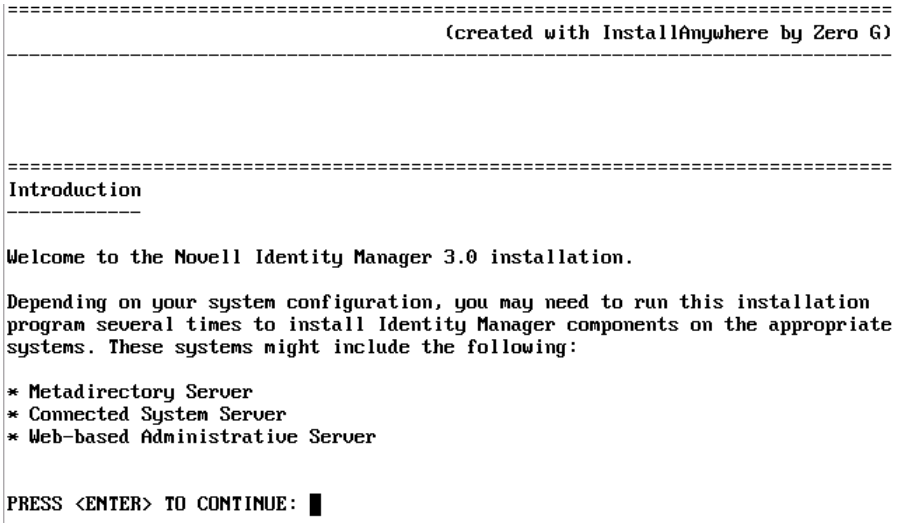
将当前的工作目录更改为安装目录，即安装所在的位置。然后输入下列命令之一，以运行安装。

平台	示例路径	安装文件
Linux	linux/setup/	dirxml_linux.bin
Solaris	solaris/setup/	dirxml_solaris.bin
AIX	aix/setup/	dirxml_aix.bin

这些路径相对于安装映象的根，可以在任何位置展开此映象，也可以将它装入 CD。除非当前的工作目录是安装程序所在的目录，否则安装程序将无法找到要安装的包。

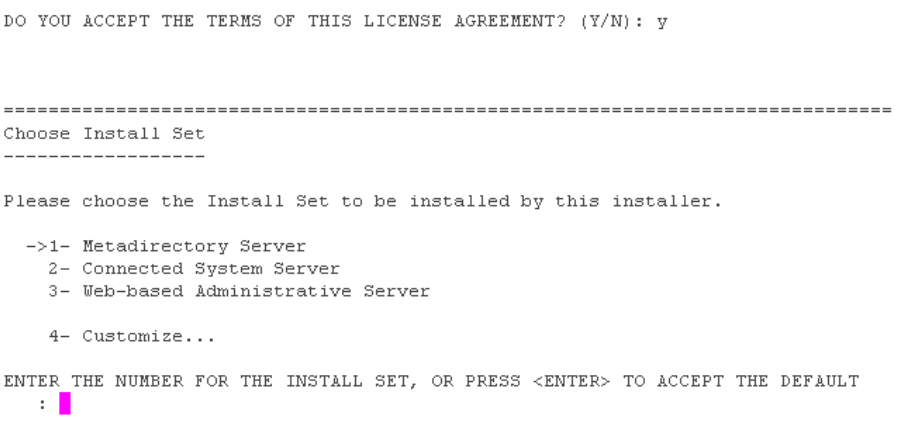
4 查看欢迎信息，然后按 Enter 键继续安装。

图 *4-19* 欢迎屏幕



5 按 Enter 键浏览许可协议，如果同意这些使用条款，请输入 Y。如果不同意，请输入 N 退出安装程序。

图 *4-20* 选择安装集



6 指定要安装的安装集的相应编号 (1-4)。安装集包含下列组件：

- **Metadirectory** 服务器：安装 Metadirectory 引擎和服务驱动程序、 Identity Manager 驱动程序、 Novell Audit 代理，并扩展 eDirectory 纲要。

  只有在安装 Novell eDirectory 后才能安装该选项。

- 已连接系统服务器：安装远程装载程序和下列驱动程序：LDAP、 JDBC、eDirectory、SAP、Delimited Text、GroupWise、Composer、Remedy、Avaya、Soap 和 Lotus Notes。如果不希望将 eDirectory 服务和 Metadirectory 引擎的开销施加到应用程序服务器，则可以选择 《已连接系统服务器》选项。

- 基于万维网的管理服务器：安装 Identity Manager 插件和 Identity Manager 驱动程序策略。

  只有在安装 Novell iManager 后才能安装该选项。

- 自定义：安装从所有组件的列表中选择的特定组件。

图 ***4-21*** 产品功能

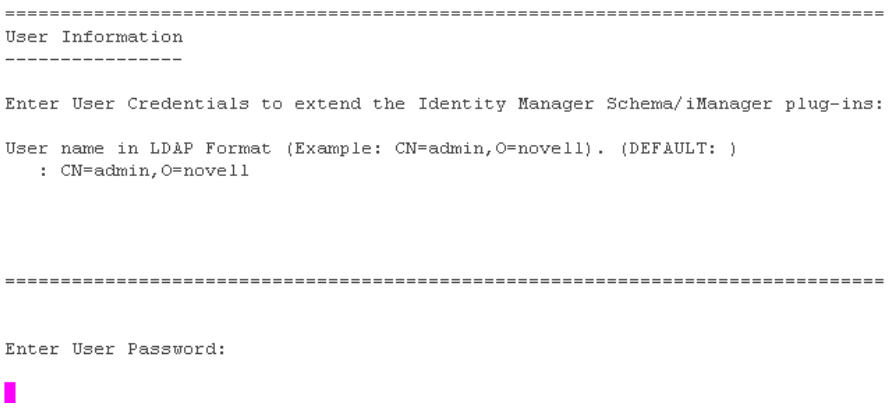
```
================================================================================
Choose Product Features
-----------------------

ENTER A COMMA_SEPARATED LIST OF NUMBERS REPRESENTING THE FEATURES YOU WOULD
LIKE TO SELECT, OR DESELECT. TO VIEW A FEATURE'S DESCRIPTION, ENTER
'?<NUMBER>'.  PRESS <RETURN> WHEN YOU ARE DONE:

    1- [X] Metadirectory Engine
    2- [ ] Remote Loader
    3- [X] eDirectory Driver
    4- [X] Delimited Text Driver
    5- [X] Groupwise Driver
    6- [X] JDBC Driver
    7- [X] LDAP Driver
    8- [X] Notes Driver
    9- [X] SAP Driver
   10- [X] AVAYA Driver
   11- [X] REMEDY Driver
   12- [X] SOAP Driver
   13- [ ] Identity Manager Plugins
   14- [ ] Identity Manager Policies

Please choose the Features to be installed by this installer.
   :
```

注释 **:** 输入 prev 可返回上级菜单，及修改安装选项。

7 （可选）根据选择的选项 （例如 《Metadirectory 服务器》），系统可能会提示您设置 LD_LIBRARY_PATH 环境变量。要执行此操作，请键入 . /opt/novell/eDirectory/bin/ndspath 以执行 /opt/novell/eDirectory/bin/ndspath 底稿，然后重新运行安装。

如果选择安装 Metadirectory 服务器，则系统会提示您提供 LDAP 用户名和口令 (CN=admin,O=novell)。选择有足够权限扩展 eDirectory 纲要的用户 （例如 Admin）。

图 **4-22** 以 *LDAP* 格式指定用户名和口令

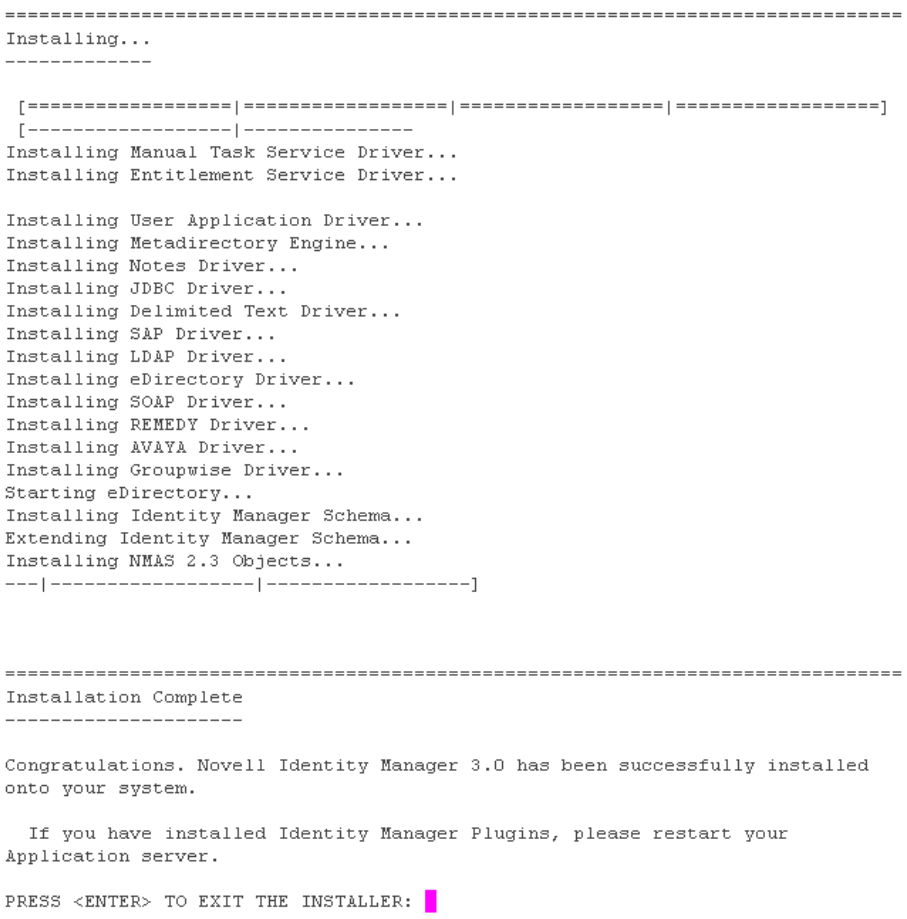


重要：（仅限 Solaris 安装）如果在 eDirectory 驻留的同一台服务器上安装基于万维网的管理服务器，当系统提示提供万维网服务器安全端口时，请将默认值更改为某个空闲的端口，例如 8443。

---

8 校验摘要中包含的信息是否正确，然后按 Enter 键开始安装包。

图 **4-23** *Metadirectory* 服务器的安装屏幕



安装 Metadirectory 引擎和纲要文件时， eDirectory 将暂时关闭。默认情况下，将安装所有可用的驱动程序，这样，如果以后想要另一个驱动程序，就不需要运行安装程序。通过 iManager 或 Designer 配置驱动程序且将其部署之前，不使用这些驱动程序文件。

9 显示 《安装完成》屏幕时，按 Enter 键关闭安装程序。

4.7 在 UNIX/Linux 上安装已连接系统选项

“在 UNIX/Linux 平台上安装 Identity Manager”在第 70 页 包括 UNIX 平台上的 Metadirectory 服务器、万维网组件和实用程序的安装。由于 UNIX 或 Linux 服务器可以使用 《已连接系统》选项，因此这里也包括了用于安装已连接系统的选项。

如果不希望将 eDirectory 服务和 Metadirectory 引擎的开销施加到应用程序服务器，请使用《已连接系统》选项。使用远程装载程序，便可以通过 Identity Manager 实现所需的同步，而不需要装载从其它位置即可访问的应用程序。

开始之前，请确保系统符合 “Identity Manager 组件和系统要求”在第 53 页 中列出的要求。

1 下载 tar 文件，并将其解压缩到所选的位置。

可以从 Novell 下载站点 (http://download.novell.com) 下载 Identity Manager 安装文件

2 在主机上以根用户的身份登录。

3 从安装目录执行 .bin 文件。

将当前的工作目录更改为安装目录，即安装所在的位置。然后输入下列命令之一，以运行安装。

平台	示例路径	安装文件
Linux	linux/setup/	dirxml_linux.bin
Solaris	solaris/setup/	dirxml_solaris.bin
AIX	aix/setup/	dirxml_aix.bin

这些路径相对于安装映象的根，可以在任何位置展开此映象，也可以将它装入 CD。

除非当前的工作目录是安装程序所在的目录，否则安装程序将无法找到要安装的包。

4 查看欢迎信息，然后按 Enter 键继续安装。

5 按 Enter 键浏览许可协议，如果同意这些使用条款，请输入 Y。如果不同意，请输入 N 退出安装程序。

6 指定编号 2 以安装已连接系统服务器。安装集包含下列项目：

- 已连接系统服务器：安装远程装载程序和下列驱动程序：LDAP、 SAP、 JDBC、Delimited Text、GroupWise、Composer、Remedy、Avaya、Soap 和 Lotus Notes。如果不希望将 eDirectory 服务和 Metadirectory 引擎的开销施加到应用程序服务器，则可以选择 《已连接系统服务器》选项。

图 ***4-24*** 预安装摘要

```
================================================================================
Pre-Installation Summary
------------------------

Please Review the Following Before Continuing:

Product Name:
    Novell Identity Manager

Install Set
    Connected System Server

Product Components:
    LDAP Driver,
    SAP Driver,
    JDBC Driver,
    Delimited Text Driver,
    Notes Driver,
    Remote Loader,
    Groupwise Driver,
    AVAYA Driver,
    SOAP Driver,
    REMEDY Driver


PRESS <ENTER> TO CONTINUE:
```

7 查看 《预安装摘要》屏幕列出的项目。按 Enter 键安装组件。

图 ***4-25*** 已连接系统服务器的安装屏幕

```
================================================================================
Installing...
-------------

 [==================|==================|==================|==================]
 [------------------|------------------|------------------|-----
Installing Manual Task Service Driver...
Installing Entitlement Service Driver...

Installing User Application Driver...
Installing Remote Loader...
Installing Notes Driver...
Installing JDBC Driver...
Installing Delimited Text Driver...
Installing SAP Driver...
Installing LDAP Driver...
Installing SOAP Driver...
Installing REMEDY Driver...
Installing AVAYA Driver...
Installing Groupwise Driver...
-------------]



================================================================================
Installation Complete
---------------------

Congratulations. Novell Identity Manager 3.0 has been successfully installed
onto your system.

  If you have installed Identity Manager Plugins, please restart your
Application server.

PRESS <ENTER> TO EXIT THE INSTALLER:
```

默认情况下，将安装所有可用的驱动程序，这样，如果以后想要另一个驱动程序，就不需要运行安装程序。通过 iManager 或 Designer 配置驱动程序且将其部署之前，不使用这些驱动程序文件。

8 显示 《安装完成》屏幕时，按 Enter 键关闭安装程序。

4.8 安装后的任务

如果驱动程序的某个参数设置为 Autostart，并且驱动程序和 eDirectory 正在运行，则驱动程序将自动启动 Identity Manager 模块。不需要手动装载或卸载 Identity Manager。安装 Identity Manager 之后，应配置所安装的驱动程序，以符合业务过程定义的策略和要求。安装后的任务通常包括下列项目：

- 配置已连接系统。有关驱动程序特定的配置指导，请参考 Identity Manager 驱动程序文档 (http://www.novell.com/documentation/dirxmldrivers)。
- “创建和配置驱动程序”
- “定义策略”
- “启动、停止或重启动驱动程序”
- “激活 Identity Manager 产品”在第 76 页

4.9 激活 Identity Manager 产品

需要激活 Identity Manager 产品。有关更多信息，请参考第 6 章 “激活 Novell Identity Manager 产品”在第 101 页 。

4.10 安装自定义驱动程序

自定义驱动程序可能包括下列项目：

- 一组 .jar 文件或本机 （.dll、 .nlm 或 .so）文件
- 用于配置驱动程序的 XML 规则文件
- 文档

有关创建或安装自定义驱动程序的更多信息，请参见 Novell 开发者工具 (http://developer.novell.com/ndk/dirxml-index.htm)。

安装用户应用程序

5

本节介绍如何安装 Identity Manager 用户应用程序。主题包括：

5.1 前提条件

开始之前，请校验环境是否支持下列项目：

环境	说明
Identity Vault 访问	用户应用程序需要身份凭证才能登录 Identity Vault。用于访问 Identity Vault 的身份凭证必须： ◆ 具有对 Identity Vault 的全部权限 ◆ 在安装 Identity Manager 3 用户应用程序之前，在 Identity Vault 中存在。 安装过程中将提示您提供这些身份凭证。该用户被称为 《用户应用程序管理员》。
IDM 用户应用程序储存	在其中安装用户应用程序的计算机必须具有 320 MB 可用储存。
JBoss	**RAM**：运行用户应用程序时 JBoss* 的最低建议 RAM 为 512 MB。 **端口**：用于安装 JBoss 的计算机的端口 8080 应该处于空闲状态。默认情况下， JBoss 允许 Tomcat 使用端口 8080。建议在该端口空闲的计算机上安装 JBoss。 如果目标计算机上也有 iManager 的实例（或者其它任何使用其自身的 Tomcat 实例的应用程序），结果可能是多个 Tomcat 实例争用同一个端口。应该关闭其它 Tomcat 实例，或者将其它实例设置为不使用端口 8080。
MySQL	用于安装 MySQL 的计算机的端口 63306 应该处于空闲状态。默认情况下，用户应用程序安装程序将在端口号 63306 的位置安装 MySQL，以避免与计算机上运行的其它任何 MySQL 服务器冲突。
Linux	**运行级别**：用户应用程序安装程序需要 XServer (XWindows)，因此必须将 Linux 运行级别设置为 5 或更高。 **帐户**：建议以没有根特权的用户的身份运行安装。 **安装目录**：确保该目录可写。通常在用户的 home 目录中使用目录结构 novell/idm 来安装用户应用程序，但可以更改此默认值。

5.2 安装和配置

安装所有先期必要的软件且确认计算机已正确设置后，便可以安装用户应用程序。执行这些任务时遵循的顺序非常重要。

- 用户应用程序在运行时需要某些软件生成物在 Identity Vault 中存在。
- 用户应用程序依赖用户应用程序驱动程序与 Identity Manager 3 引擎进行运行时通讯。（反之，如果用户应用程序不存在，则用户应用程序驱动程序在打开时可能会产生错误。）

1. 将用户应用程序驱动程序注册到给定的驱动程序集。但是不要打开该驱动程序。该步骤将在 Identity Vault 中使用某些项目的默认数据值创建新对象。

   如果尚未安装 Identity Manager，则该步骤将会失败。有关详细信息，请参见 “创建用户应用程序驱动程序”在第 79 页。

2. 运行用户应用程序的安装程序。有关详细信息，请参见 “安装用户应用程序”在第 82 页。

3. 启动数据库。默认的安装将使 MySQL 保持运行。

   如果选择默认安装，安装程序将自动启动 MySQL。但是，在重引导后，请使用 start-mysql.sh 底稿 （在 Linux 上）或 start-mysql.bat （在 Windows 上）。该底稿位于安装文件夹的 mysql 目录中。

4. 启动 JBoss。如果使用用户应用程序安装程序来安装 JBoss 应用程序服务器，该安装程序将提供一组启动和关闭底稿。这些底稿位于 /idm 安装目录中。例如：

   在 Linux 上：

   ```
   /idm/start-jboss.sh
   ```

   在 Windows 上：

   ```
   \idm\start-jboss.bat
   ```

   这是启动 JBoss 的建议方法。

   - 如果使用现有的 JBoss 应用程序服务器，则不能使用这些底稿，同时需要执行下列操作之一，以避免发生可信证书错误。
   - 确保 JAVA_HOME 指向用户应用程序安装程序安装的 JRE。

   或者

   - 更改密钥存储区路径值，使之指向现有 JBoss 安装的密钥存储区。安装用户应用程序过程中， Identity Vault 证书将被下载到该位置。

5. 打开用户应用程序驱动程序。这样，用户应用程序和驱动程序之间便开始通讯。要打开用户应用程序驱动程序，请执行下列操作：

   a. 登录 iManager。

   b. 在 《职能和任务》（左导航帧）中，打开 *Identity Manager* 标题，然后选择《Identity Manager 概述》。

   c. 在显示的内容视图中，指定包含用户应用程序驱动程序的驱动程序集，然后单击《搜索》。

d. 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。单击 《用户应用程序驱动程序》图标右上角的红圈区域中的减号可打开驱动程序。

注释：驱动程序启动后，将尝试与用户应用程序握手。如果未运行 JBoss，或者未成功部署 WAR，驱动程序将会出错。

---

6. 启动并登录用户应用程序。使用万维网浏览器转至：

   http://hostname:port/ApplicationName

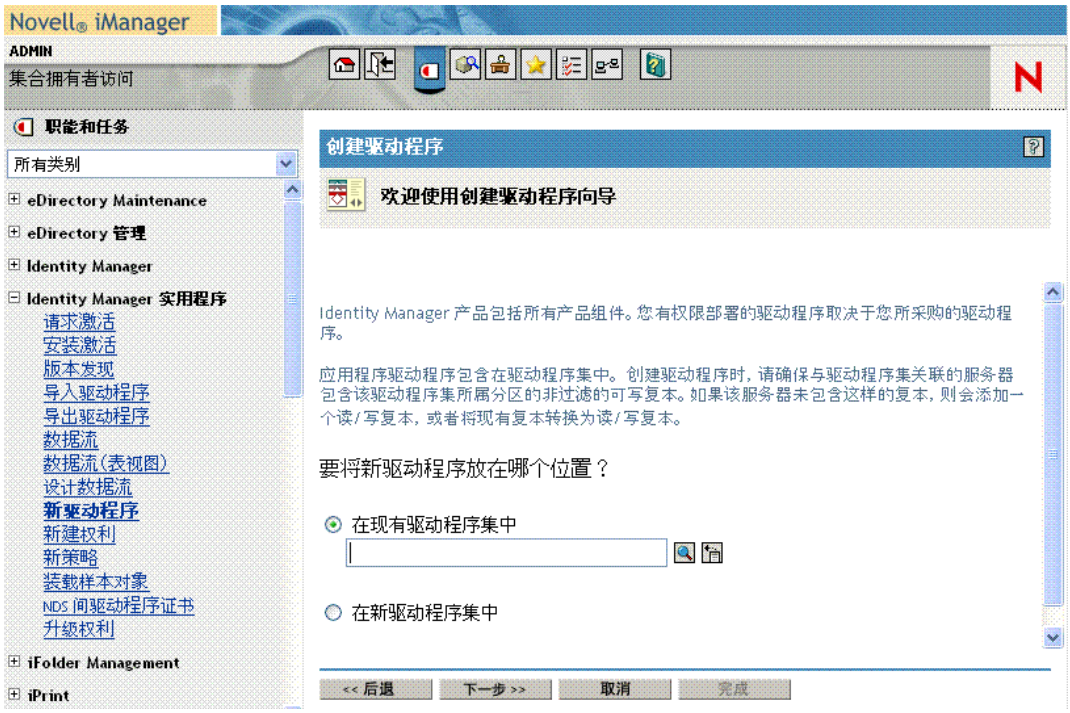
   默认情况下，其中的 *hostname:port* 为 JBoss 应用程序服务器， *ApplicationName* 为 IDM。在安装过程中，提供 JBoss 配置信息时已指定了应用程序名称。应显示 Novell Identity Manager 用户应用程序主页。在该页的右上角，单击 《登录》可登录用户应用程序。

5.3 创建用户应用程序驱动程序

要创建用户应用程序驱动程序，并将其与驱动程序集关联，请执行下列操作：

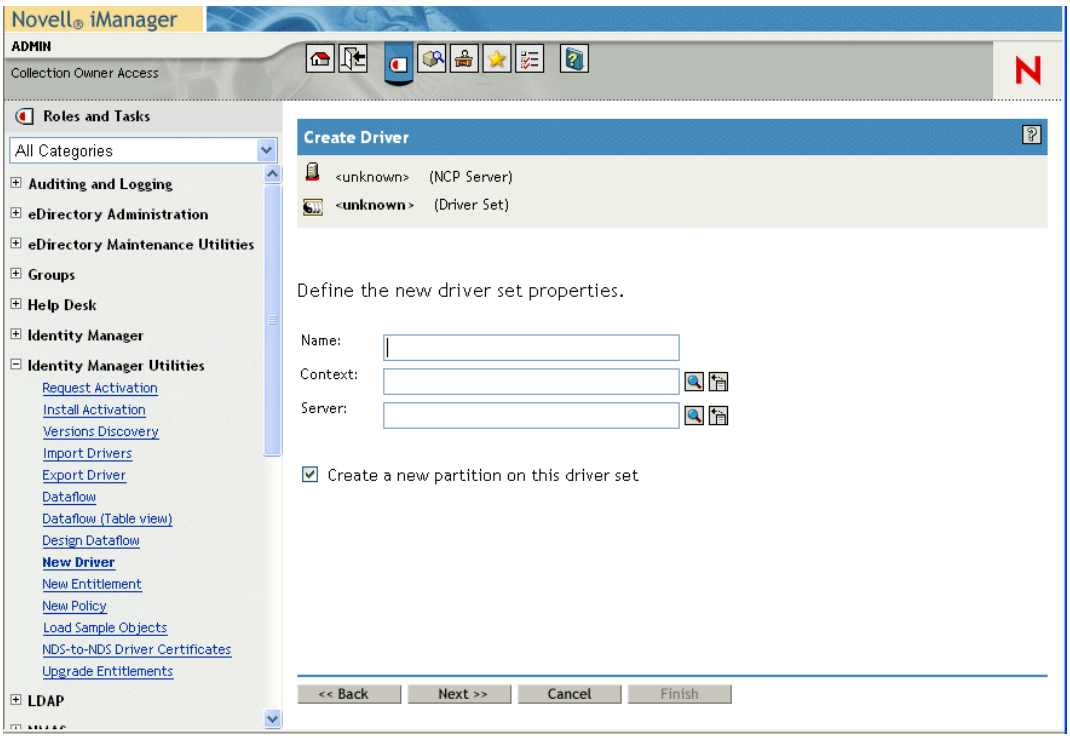
1 登录 Identity Vault with iManager （如果尚未登录的话）。

2 转至 《职能和任务》 > 《实用程序》，然后选择 《新驱动程序》启动创建驱动程序向导 > 。



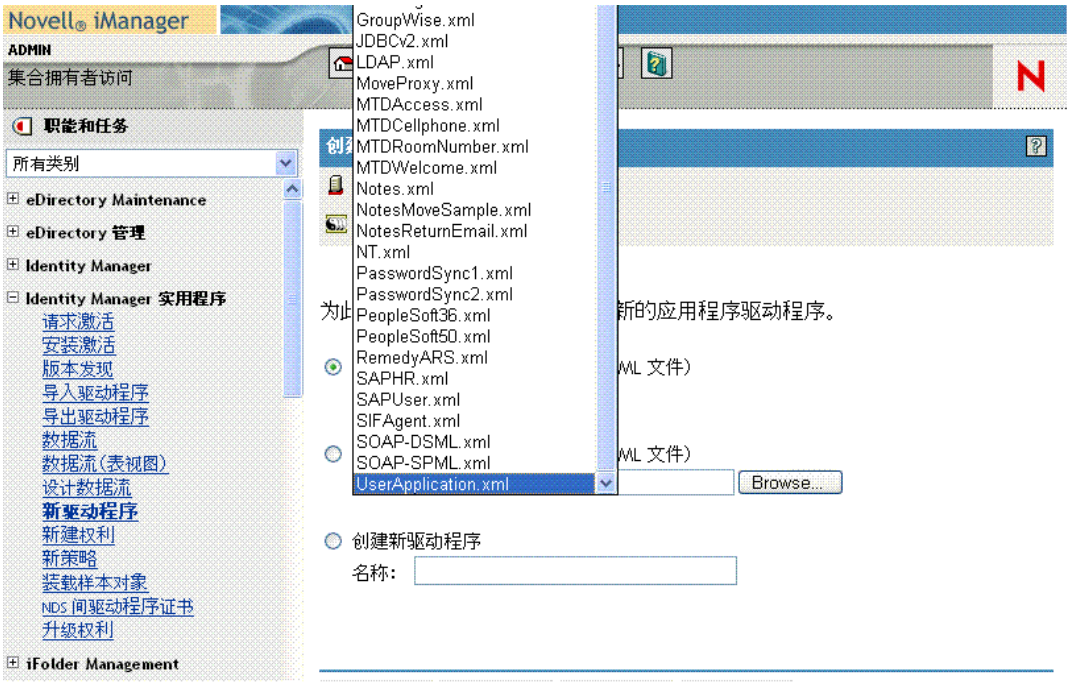
3 要在现有的驱动程序集中创建驱动程序，请单击 《浏览》按钮以找到该驱动程序集。然后单击 《下一步》并继续步骤 4。或者在新的驱动程序集中创建驱动程序，选择 《在新驱动程序集中》，然后单击 《下一步》> 。

如果选择 《在新驱动程序集中》，系统将提示您定义新驱动程序集的属性。



3a 指定驱动程序集的名称、环境和服务器，然后单击 《下一步》。系统将提示您提供驱动程序 XML 文件。

4 单击 《从服务器中导入驱动程序配置 （.XML 文件）》，然后打开驱动程序的下拉列表。



5 选择 *UserApplication.xml*，然后单击 《下一步》。

注释：如果该下拉列表中未列出 UserApplication.xml，则可能是没有运行 Identity Manager 3 安装的基于万维网的管理服务器部分。

6 填写以下字段：

字段	说明
驱动程序名	创建的驱动程序的名称。
鉴定 ID/ 口令	用户应用程序管理员的判别名和关联的口令。例如： `cn=admin,ou=orgunit,o=novell`
应用程序环境	用户应用程序环境的名称 （安装时已指定，例如 IDM）。
主机	在其中部署 Identity Manager 用户应用程序的应用程序服务器的主机名或 IP 地址。 如果用户应用程序在群集中运行，请键入发送程序的主机名或 IP 地址。
端口	上述主机的端口。

7 单击 《下一步》。

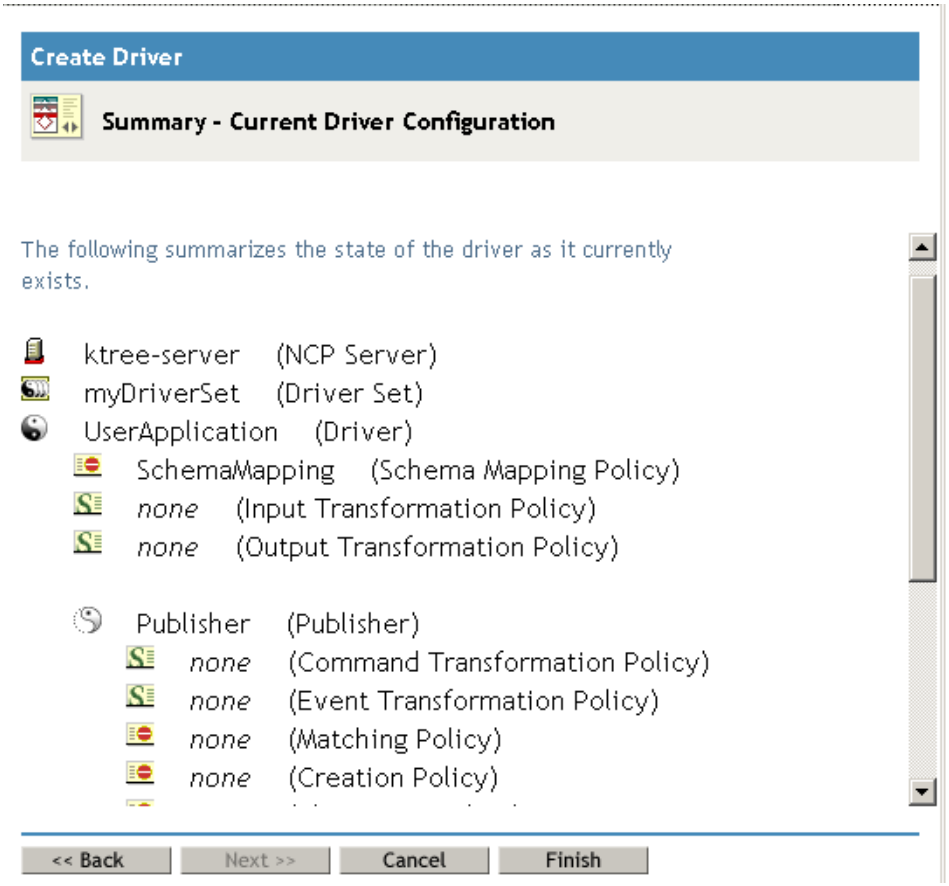
8 输入或编辑驱动程序的配置参数，然后单击 《下一步》

9 单击 《Define Security Equivalences （定义安全性等效）》显示 《安全性等效》窗口。使用导航控件导航并选择一个管理员 （或其他主管）对象。然后单击 《添加》使驱动程序等效于所选对象。

此步骤可为驱动程序指定其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详细信息。

10 （可选操作，但建议使用）。单击 《排除怨苇碇澳苷》。单击 《添加》，选择 《管理员》，单击 《确定》，再单击 《确定》> 。然后单击底端的 《下一步》按钮。单击 《确定》关闭弹出窗口。

将显示摘要屏幕。



11 单击 《完成》接受信息。如果页上显示了 《完成概述》按钮，请单击该按钮。

现在应该会显示驱动程序集及其附带的驱动程序。驱动程序已关闭 （位于驱动程序图形右上角的小红圈中将显示一个减号）。

重要：将驱动程序保持为关闭状态，直到已安装用户应用程序。

5.4 安装用户应用程序

创建用户应用程序之后，便可以安装 Identity Manager 用户应用程序。

5.4.1 关于安装程序

Novell Identity Manager 用户应用程序是一个需要部署到 JBoss 应用程序服务器的 Java 万维网应用程序档案 (WAR) 文件。它使用数据库 （默认情况下为 MySQL）储存配置信息。根据选择的安装类型，用户应用程序安装程序还可以完成下列任务：

- 安装 JBoss 或用于指定 JBoss 的现有版本
- 安装 MySQL，或用于指定 MySQL、 Oracle 或 Microsoft SQL Server 2000 的现有版本。
- 配置 JRE 的证书文件，以便用户应用程序 （在 JBoss 上运行）能够安全地与 Identity Vault 和用户应用程序驱动程序通讯。
- 配置 WAR 文件并将其部署到 JBoss 应用程序服务器。
- 启用 Novell Audit 日志记录。

安装底稿和可执行文件

要安装 Novell Identity Manager 用户应用程序，需要下列文件：

文件	说明
Linux 平台： • IdmUserApp.bin **Windows 平台：** • IdmUserApp.exe	启动安装程序。
用户应用程序 WAR	IDM.war: 包括具有身份自助服务功能的 Identity Manager 3 用户应用程序。 IDMProv.war：安装 Provisioning Module for Identity Manager 3。

提示 **:** 确保在安装计算机上停止其它任何 MySQL 版本。在安装过程中，如果有其它版本在运行，安装程序将不会启动新的 MySQL 服务器，并且不会创建新的数据库。

要启动安装程序，请执行下列操作：

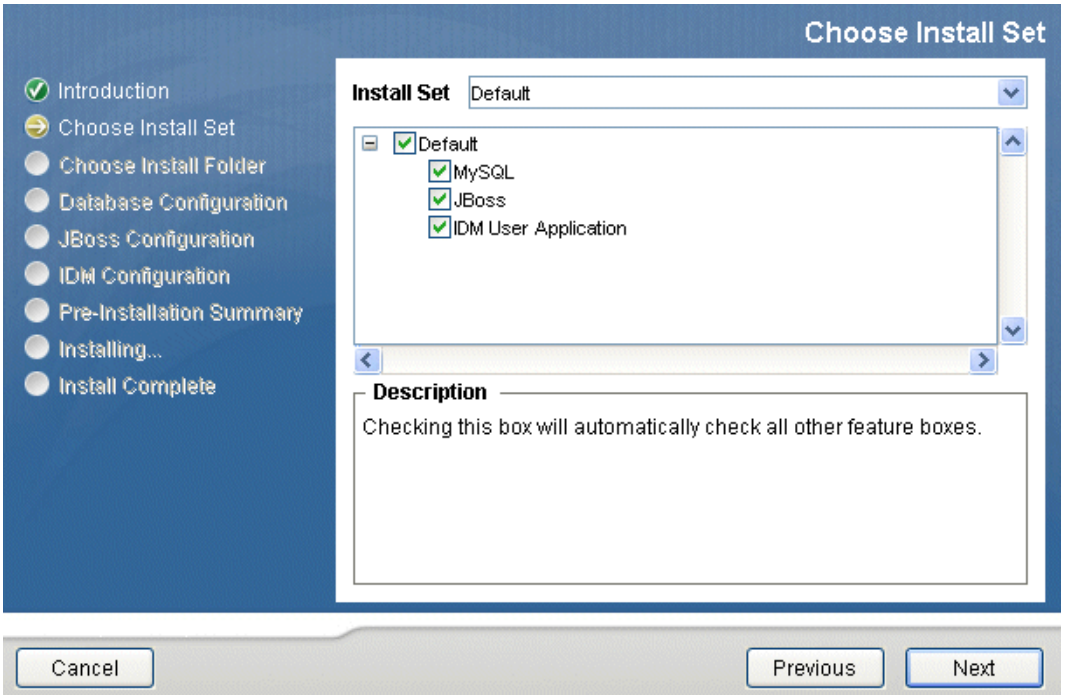
1 获取 “安装底稿和可执行文件”在第 83 页 中说明的相应安装文件。

2 如下所述启动适用于您的平台的程序：

平台	操作
Linux	1. 以非根帐户的身份登录，并打开一个终端会话。 必须以根用户以外的身份登录 Linux 计算机。如果已经以根用户的身份登录，请注销后以其他用户的身份重新登录。不要只是对终端会话中的另一个帐户执行 《su》操作，因为图形状态不会转换为另一个帐户。（也不建议执行 《sux》操作。） 2. 在控制台上执行以下命令： `./IdmUserApp.bin` 底稿将会解包 Java 运行时环境 (JRE)，并启动 Zero-G 安装程序。
Windows	在 Windows 上，双击 \NT 目录中的 IdmUserApp.exe 文件。

3 阅读许可协议，然后单击 《I accept the terms of the License Agreement （我接受本许可协议的条款）。

4 在安装向导的 《简介》页中单击 《下一步》。



5 选择安装集，然后单击 《下一步》。

安装选项	功能
默认	安装和配置以下项目： ◆ **IDM 用户应用程序 WAR** ◆ **JBoss**：安装 JBoss 应用程序服务器，或配置现有的 JBoss 应用程序服务器。对于新的应用程序服务器，该选项将： ◆ 创建一个服务器配置，该配置的名称就是在 《应用程序名称》字段中提供的名称 （该名称在安装过程中指定）。配置基于 《默认》或《所有》配置。 ◆ 创建用于启动和停止服务器的底稿。 ◆ **MySQL**：安装 MySQL，或配置一个现有的 MySQL 数据库。对于新的 MySQL 安装，该选项将创建用于启动或停止数据库服务器的底稿。
自定义：	**IDM 用户应用程序** ◆ 安装 IDM 用户应用程序，并用于指定现有的数据库和 JBoss 服务器。支持的数据库类型为 MySQL、 Oracle9i、 Oracle10g 和 Microsoft SQL Server 2000。 **JBoss** ◆ 安装 JBoss 应用程序服务器，或用于选择现有的 JBoss 应用程序服务器以供使用。安装新的应用程序服务器时，该选项将完成以下两项任务： ◆ 创建一个服务器配置，该配置的名称就是在 《应用程序名称》字段中提供的名称 （该名称在安装过程中指定）。配置基于 《默认》或《所有》配置。 ◆ 创建用于启动和停止服务器的底稿。 **MySQL** ◆ 安装 MySQL。该选项不创建用于启动和停止的底稿 （与 《默认》选项不同）。

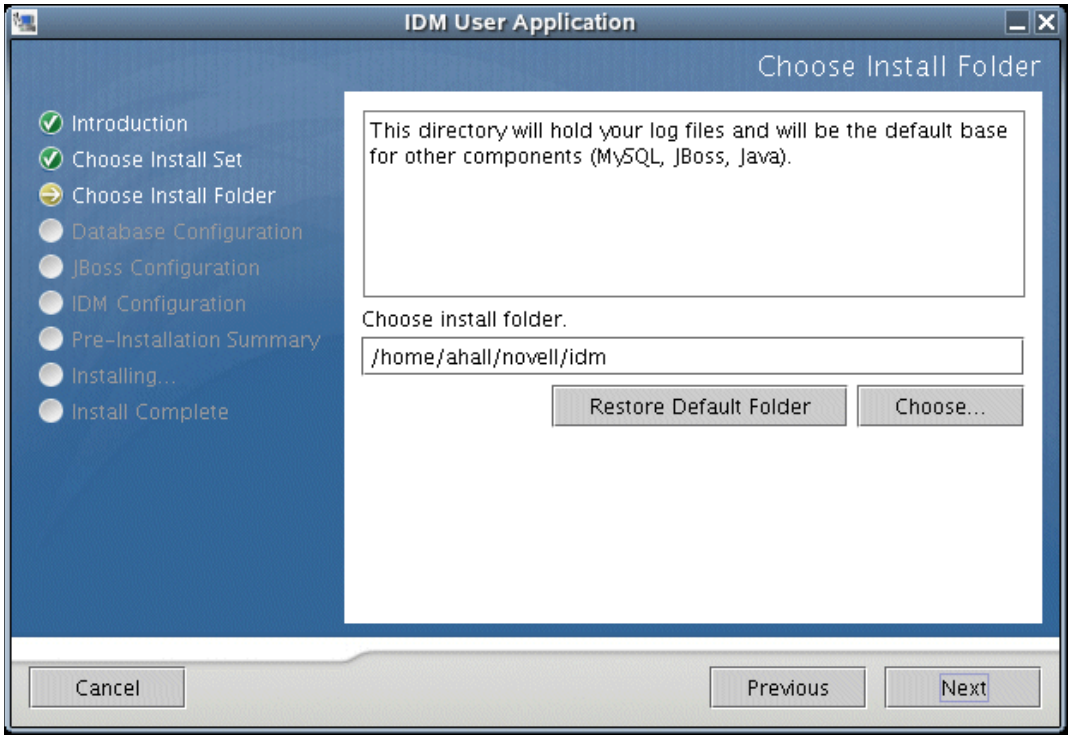
6 请遵循安装类型的相应指导：

安装类型	操作
默认安装	转至： ◆ “选择安装文件夹”在第 86 页 ◆ “指定 MySQL 细节”在第 87 页 ◆ “指定数据库主机和端口”在第 88 页 ◆ “指定 JBoss 服务器设置”在第 89 页 ◆ “选择 JBoss 服务器配置类型”在第 90 页 ◆ “启用 Novell Audit 日志记录”在第 90 页 ◆ “配置用户应用程序”在第 92 页
自定义：JBoss	转至： ◆ “指定 JBoss 服务器设置”在第 89 页
自定义：MySQL	转至： ◆ “指定 MySQL 细节”在第 87 页

安装类型	操作
自定义：IDM 用户应用程序	转至： ◆ “选择安装文件夹”在第 86 页 ◆ “选择数据库平台”在第 96 页 ◆ “指定数据库主机和端口”在第 88 页 ◆ “指定数据库名称和特权用户”在第 97 页 ◆ “指定 JBoss 服务器设置”在第 89 页 ◆ “选择 JBoss 服务器配置类型”在第 90 页 ◆ “启用 Novell Audit 日志记录”在第 90 页 ◆ “配置用户应用程序”在第 92 页

5.4.2 选择安装文件夹

1 完成以下页中的选项：



注释：在 Linux 上，如果在路径的任何位置看到 */root*，请取消安装，并以非根用户的身份重新登录。

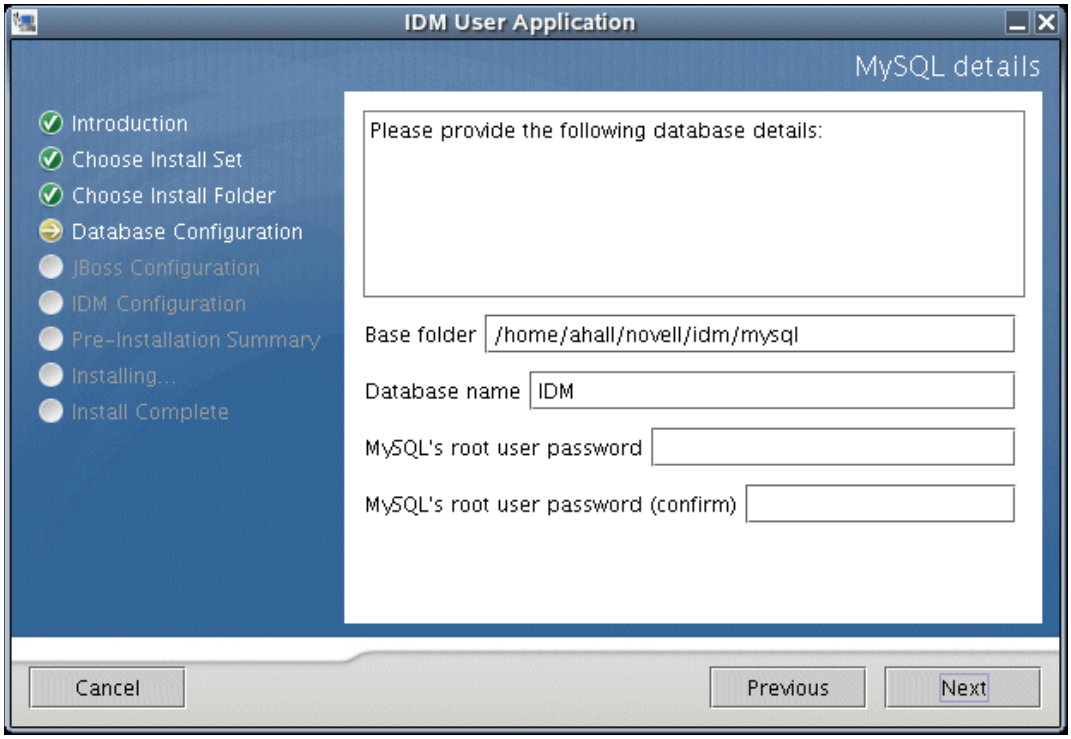
2 单击 《下一步》。

如果选择：

- 默认：转至 “指定 MySQL 细节”在第 87 页 。
- 自定义：*IDM* 用户应用程序：转至 “选择数据库平台”在第 96 页 。

5.4.3 指定 MySQL 细节

1 完成以下页中的选项：

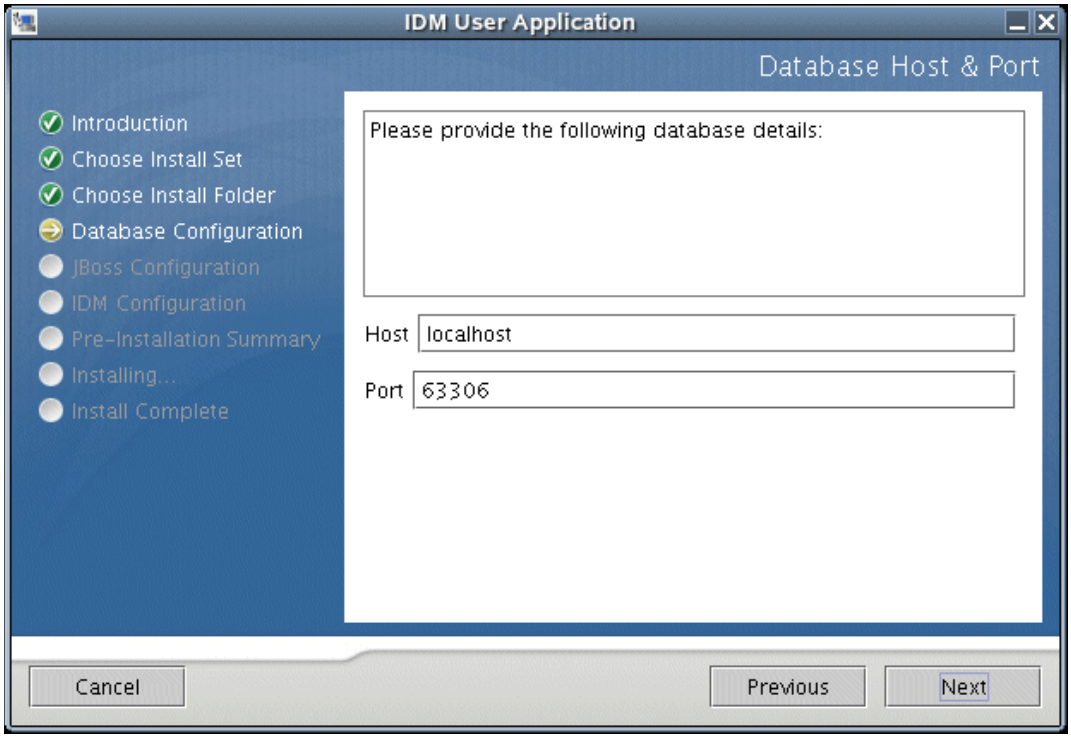


字段	说明
基本文件夹	指定安装程序将在其中创建新 MySQL 数据库的位置。
数据库名称	指定安装程序创建的数据库的名称。
MySQL 的根用户口令	输入 MySQL 数据库用户使用的数据库口令。 这与 Linux 根用户帐户口令不同。IdmUserApp 安装程序将在计算机上创建一个新的 MySQL 安装，在此过程中，它还会创建数据库根帐户。需要指定 MySQL 帐户的口令。

2 单击 《下一步》可访问 “指定数据库主机和端口”在第 88 页 中显示的页。

5.4.4 指定数据库主机和端口

1 完成以下页中的选项：



字段	说明
主机	指定数据库服务器的主机名或 IP 地址
端口	指定数据库的监听器端口号。 MySQL 的默认值为 63306。

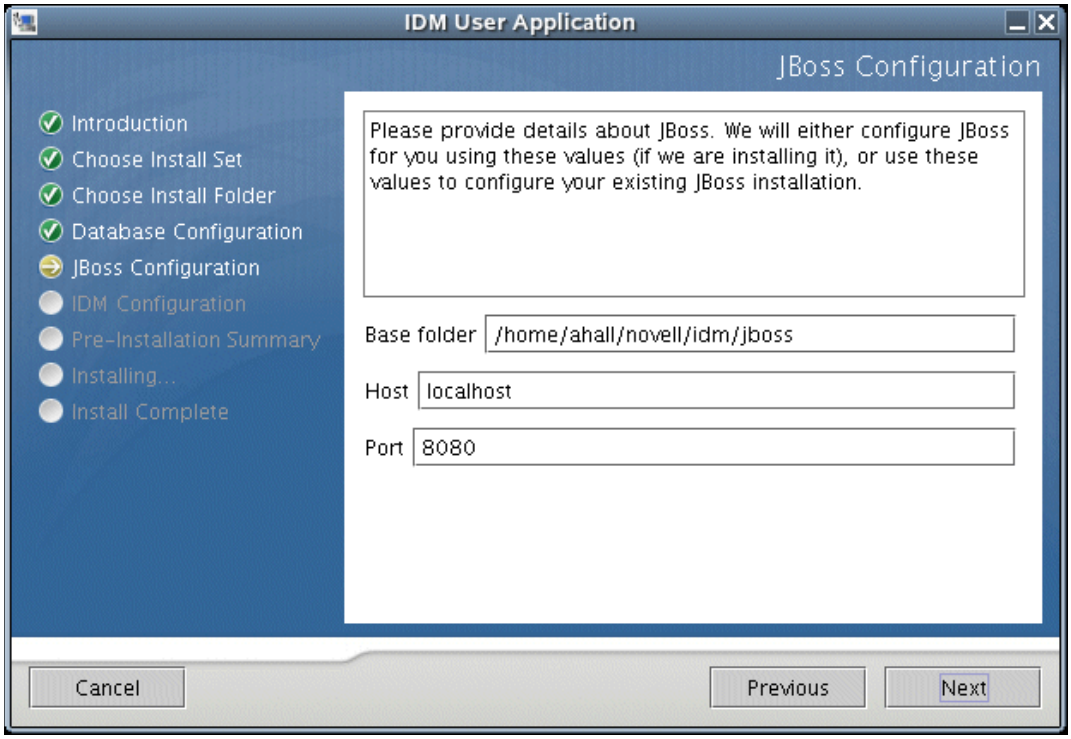
2 单击 《下一步》。

如果选择：

- 自定义：*MySQL* 安装：将显示 《Pre-Install Summary （预安装摘要）》。如果所有项目都合意，请单击 《安装》。
- 自定义：*IDM* 用户应用程序：转至 “指定数据库名称和特权用户”在第 97 页 。
- 其它安装集：转至 “指定 JBoss 服务器设置”在第 89 页 。

5.4.5 指定 JBoss 服务器设置

1 完成以下页中的选项：



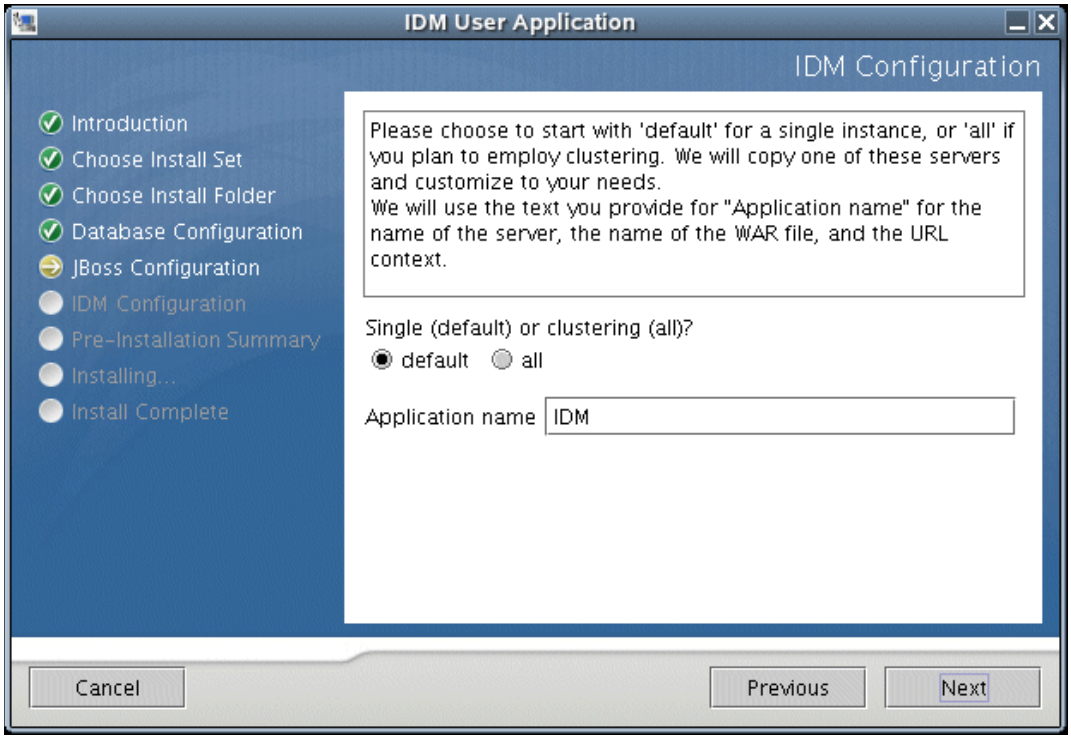
字段	说明
基本文件夹	指定安装程序将在其中创建新 JBoss 数据库的位置。
主机	指定应用程序服务器的主机名或 IP 地址。
端口	指定 JBoss 监听器端口号。默认值为 8080。

2 单击 《下一步》。如果选择：

- 自定义：*JBoss* 安装：将显示 《预安装摘要》。如果所有项目都合意，请单击 《安装》。
- 其它安装集 - 转至 “选择 JBoss 服务器配置类型”在第 90 页 。

5.4.6 选择 JBoss 服务器配置类型

1 完成以下页中的选项：



选项	说明
单个 （默认）或群集 （所有）	选择 JBoss 服务器配置的类型 （《所有》适用于群集，《默认》适用于其它类型） 安装底稿将根据选择的服务器基创建服务器配置。配置名称与接下来指定的应用程序名称相同。
应用程序名称	指定用户应用程序环境名称。该名称是用于访问用户应用程序的 URL 的一部分。

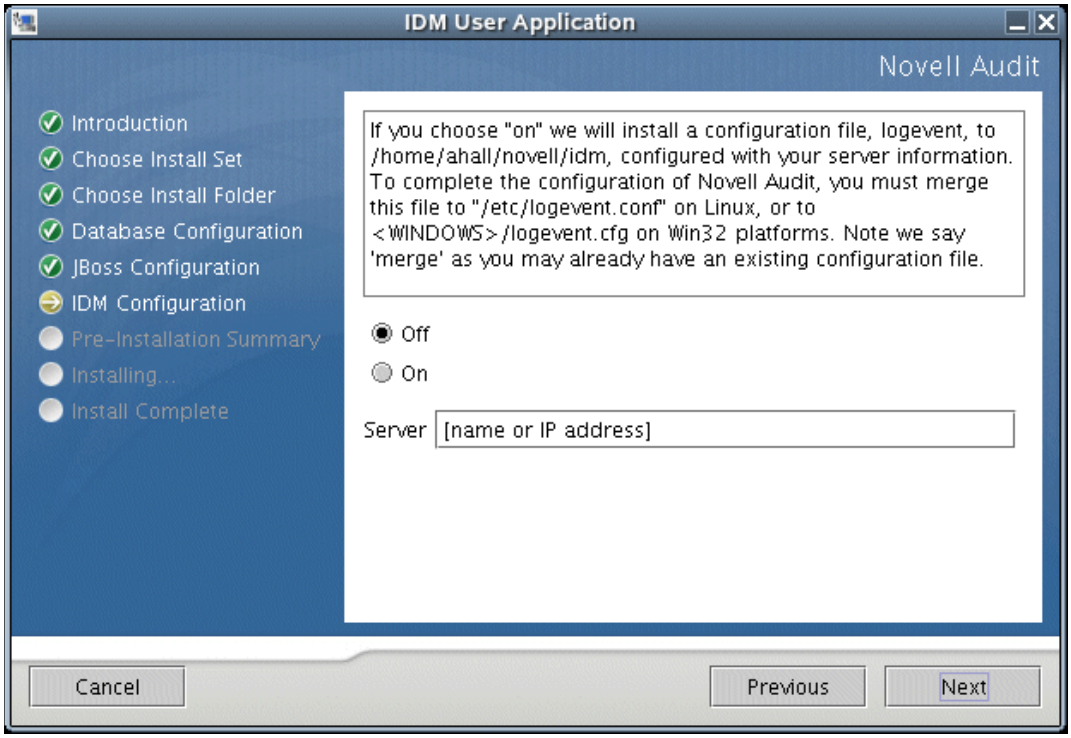
2 单击 《下一步》。如果选择：

- 自定义：*JBoss* 安装：将显示 《预安装摘要》。如果所有项目都合意，请单击 《安装》。
- 其它安装集：转至 “启用 Novell Audit 日志记录”在第 90 页 。

5.4.7 启用 Novell Audit 日志记录

要启用用户应用程序的 Novell Audit 日志记录，请执行下列操作：

1 完成以下页中的选项：



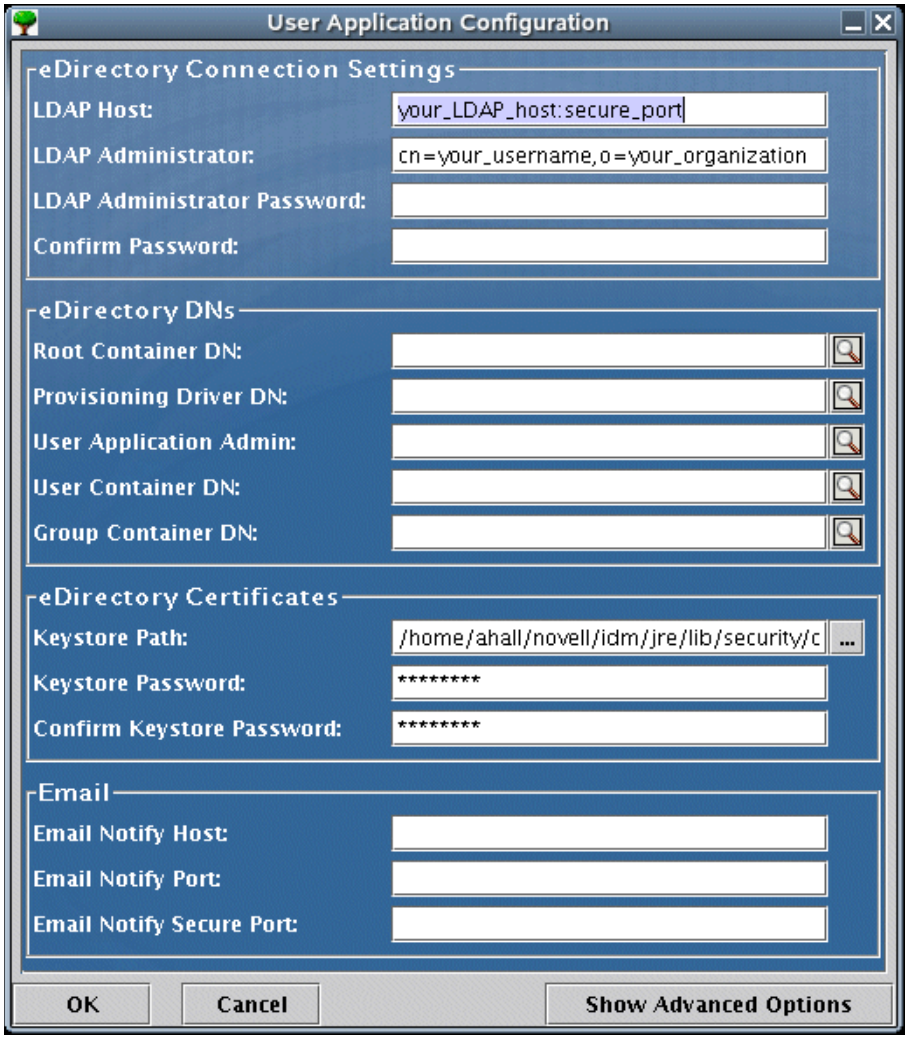
字段	说明
开	启用用户应用程序的 Novell Audit 日志记录。 有关设置 Novell Audit 日志记录的更多信息，请参见 *《Identity Manager 用户应用程序：管理指南》*。
关	禁用用户应用程序的 Novell Audit 日志记录。以后可以使用用户应用程序的 《管理》选项卡来启用该功能。 有关启用 Novell Audit 日志记录的更多信息，请参见 *《Identity Manager 用户应用程序：管理指南》*。
服务器	指定 Novell Audit 服务器的主机名或 IP 地址。

2 单击 《下一步》，然后继续 “配置用户应用程序”在第 92 页 。

5.4.8 配置用户应用程序

此配置有两页。一页用于提供基本的配置信息，另一页供高级用户使用，以及用于配置其它参数。

1 完成以下页中的选项：

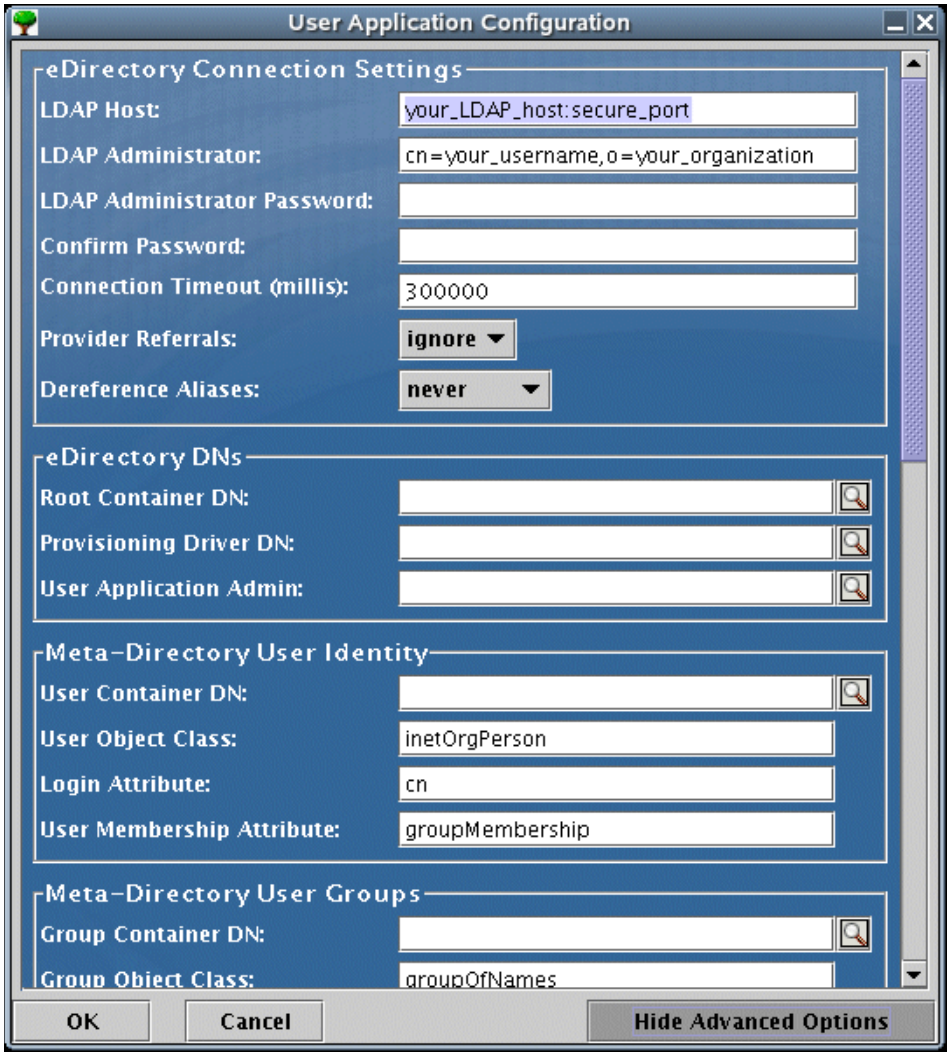


字段	说明
LDAP 主机	必需。指定 LDAP 服务器的主机名或 IP 地址，以及它的安全端口。例如： `myLDAPhost:636`
LDAP 管理员和口令	必需。为 LDAP 管理员指定身份凭证。该用户必须已经存在。用户应用程序将使用此帐户来建立与 Identity Vault 的管理连接。

字段	说明
根树枝 DN	必需。指定根树枝的 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。指定以前在 “创建用户应用程序驱动程序”在第 79 页 一节中创建的用户应用程序驱动程序的判别名。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`
用户应用程序管理员	必需。Identity Vault 中的现有用户，有权在 Identity Vault 中执行任何管理任务。 该用户可以： ◆ 使用用户应用程序的 《管理》选项卡 ◆ 使用 iManager 管理工作流程任务 ◆ 创建新的供应请求
用户树枝 DN	必需。指定用户树枝的 LDAP 判别名 (DN) 或完全限定的 LDAP 名称。 这将会定义用户和组的搜索范围。 允许该树枝 （以及该级别以下）中的用户登录用户应用程序。 重要：如果要使该用户能够执行工作流程，请确保在设置用户应用程序驱动程序的过程中指定的用户应用程序管理员在该树枝中存在。
组树枝 DN	必需。指定组树枝的 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。指定运行 JBoss 应用程序服务器时使用的 JRE 的密钥存储区 (cacerts) 文件的完整路径，否则，请单击较小的浏览器按钮，然后导航到 /idm/jre/lib/security/ 路径中的 cacerts 文件，并选择该文件。 实用程序必须有权写入该文件。
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*。
电子邮件通知主机	指定承载 Identity Manager 用户应用程序的 JBoss 服务器。例如： `myJBossServer` 该值将替换电子邮件模板中的 $HOST$ 令牌。构建好的 URL 就是指向供应请求任务和批准通知的链接。

字段	说明
电子邮件通知端口	用于替换供应请求任务和批准通知使用的电子邮件模板中的 $PORT$ 令牌。
电子邮件通知安全端口	用于替换供应请求任务和批准通知使用的电子邮件模板中的 $SECURE_PORT$ 令牌。

2 （可选）单击 《显示高级选项》完成以下页中的选项：



字段	说明
连接超时 （毫秒）	用户连接到 LDAP 服务器时，超时之前的等待时间 （单位为毫秒）。
Provider referrals （提供程序参照）	将该特性从 JNDI 应用程序发送到 LDAP 服务器，以指明如何处理参照。有效值为 《忽略》、《Follow （遵循）》和 《Throw （丢弃）》。

字段	说明
延迟别名	该特性包含从 LDAP 操作返回的项，用于指明这些项是已延迟（真路径）还是没有延迟 （别名）。有效值为 《从不》、《始终》、《查找》和 《搜索》。
用户对象类	LDAP 用户对象类 （通常为 inetOrgPerson）。
登录特性	代表用户登录名的特性 （例如 CN）。
用户成员资格特性	可选。代表用户的组成员资格的特性。不允许空格。
组对象类	LDAP 组对象类。
组成员资格特性	代表用户的组成员资格的特性。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。
已启用 ICS 注销	如果选择该选项，应用程序将支持同时注销用户应用程序和 iChain® 。
ICS 注销页	iChain 注销页的 URL。
电子邮件通知协议	指定下列值之一： ◆ HTTP ◆ HTTPS 用于替换供应请求任务和批准通知使用的电子邮件模板中的 $PROTOCOL$ 令牌。
电子邮件通知安全协议	用于替换供应请求任务和批准通知使用的电子邮件模板中的 $SECURE_PROTOCOL$ 令牌。
会话超时	指定用户会话可以处于非活动状态的分钟数。默认情况下，会话中的用户应用程序将在 20 分钟后超时。
数据源	指定连接池的 JNDI 名称。默认情况下，连接池 JNDI 名称为 java:/IDM。
Add a New Container Object （添加新的树枝对象）	输入可用作树枝的某个对象类的 LDAP 名称。

注释 **:** 要在完成安装后修改这些值，请运行 configupdate.sh 底稿 （在 Linux 上）或 configupdate.bat 文件 （在 Windows 上）。这些文件位于安装子目录中。如果在启动时使用 -use_ssl 参数，更新实用程序可以使用 SSL 连接到 eDirectory。否则，它将以非 SSL 方式连接到 eDirectory。

3 单击 《确定》。

4 查看 《预安装摘要》页。如果每一项都正确，请单击 《安装》继续安装。

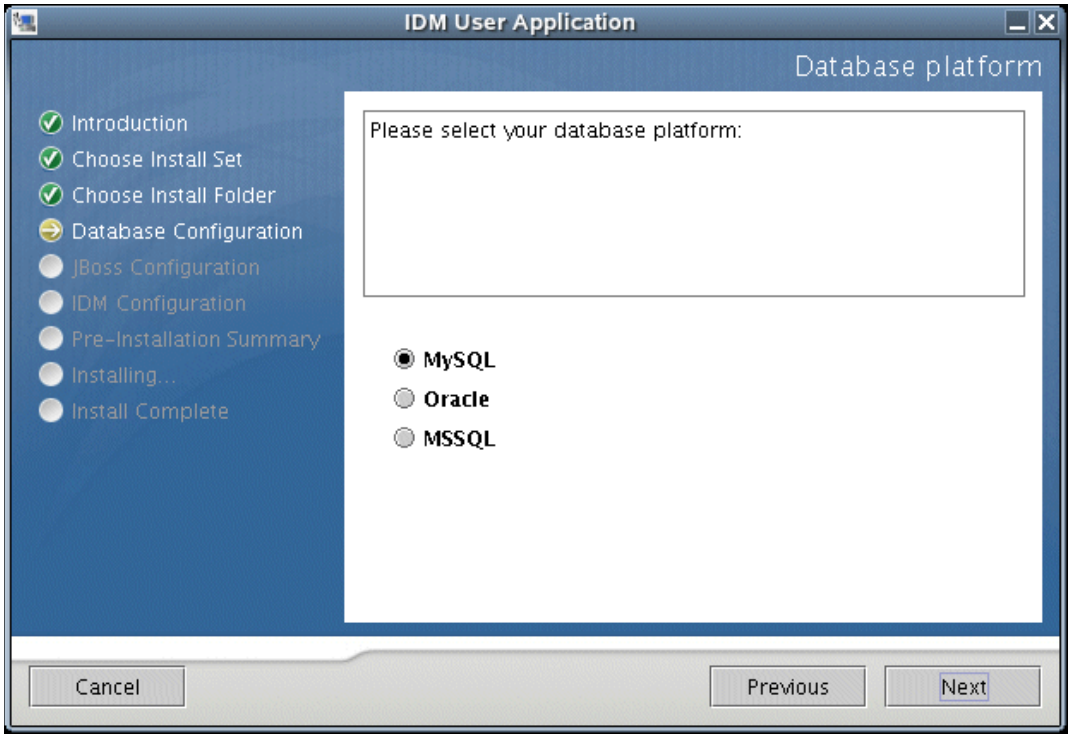
5 安装完成后单击 《完成》。

6 打开安装目录中的 README 文件。

7 转至 “安装后的任务”在第 98 页 。

5.4.9 选择数据库平台

1 完成以下页中的选项：



2 选择数据库平台。根据您的选择，请遵循下表中的配置步骤：

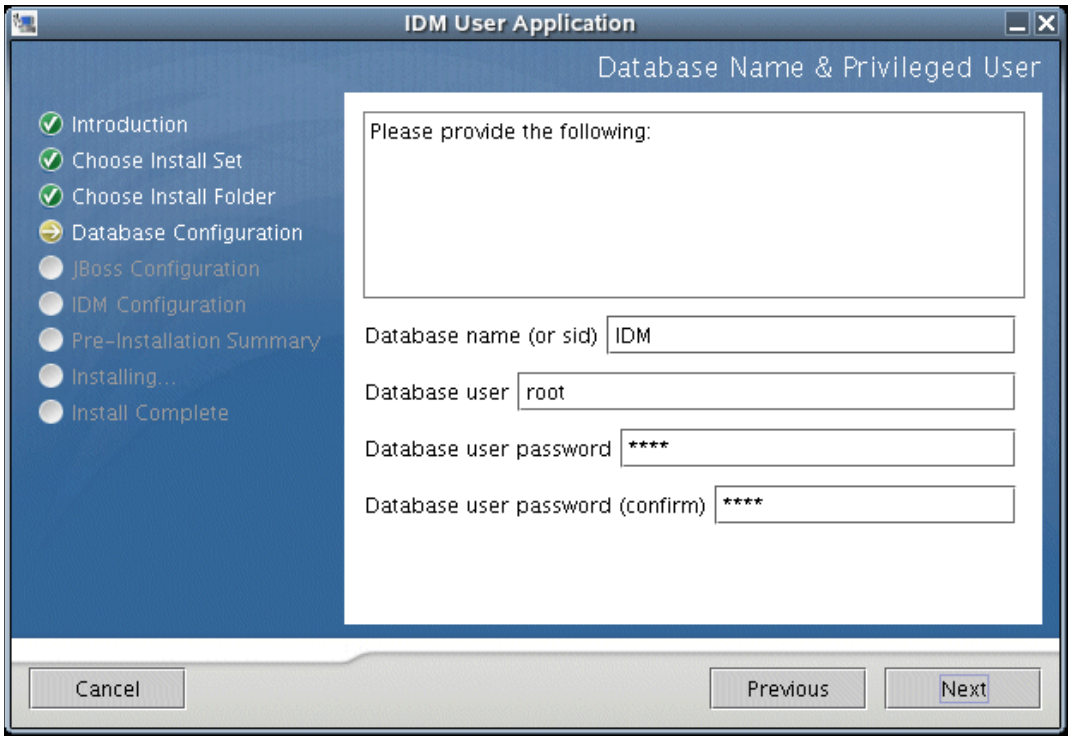
数据库	说明和配置细节
MySQL	对于远程 MySQL 环境，为“指定 MySQL 细节”在第 87 页中指定的名称创建数据库。 提示：安装程序将使用用户应用程序 WAR 文件的名称创建 JBoss 数据源文件。
Oracle	要将 Oracle 数据库与用户应用程序一起使用，请执行下列操作： 1. 在 Oracle 实例上创建数据库（确保名称与在“指定数据库名称和特权用户”在第 97 页中指定的名称相同。） 2. 从 Oracle 的下载站点下载 ojdbc14.jar 驱动程序，并将其复制到 /idm/jboss/server/<*server-name*>/lib 提示：安装程序将使用用户应用程序 WAR 文件的名称创建 JBoss 数据源文件。

数据库	说明和配置细节
MS SQL	要将 MS SQL 数据库与用户应用程序一起使用，请执行下列操作： 1. 在 MS SQL 实例上创建数据库 （确保名称与在 “指定数据库名称和特权用户”在第 97 页 中指定的名称相同。） 2. 从 Microsoft 下载站点下载 MS SQL JDBC 驱动程序 (msbase.jar、mssqlserver.jar 和 msutil.jar)，并将其复制到 /idm/jboss/server/<*server-name*>/lib 3. 创建指向该数据库的 JBoss 数据源文件。 **提示：**安装程序将使用用户应用程序 WAR 文件的名称创建 JBoss 数据源文件。

3 单击 《下一步》，然后继续 “指定数据库主机和端口”在第 88 页 。

5.4.10 指定数据库名称和特权用户

1 完成以下页中的选项：



字段	说明
数据库名称 （或 SID）	指定储存用户应用程序配置信息的数据库的名称。
数据库用户	指定数据库根用户。
数据库口令 / 确认口令	指定数据库根口令。

2 单击 《下一步》，然后继续 “指定 JBoss 服务器设置”在第 89 页 。

5.4.11 安装后的任务

忘记口令和工作流程电子邮件通知功能要求执行下列安装后的任务：

1 在 iManager 中，选择 《口令职能》。
2 在 《口令》中，选择 《电子邮件服务器选项》> 。
3 在 《主机名》字段中提供 SMTP 服务器名。
4 在 《从》字段中指定一个电子邮件地址 （例如 noreply@novell.com），然后单击 《确定》> 。

5.4.12 测试安装

要校验安装状况是否良好，请完成 “安装和配置”在第 78 页 中概述的剩余步骤。完成这些步骤后，如果浏览器中未显示 《Identity Manager 用户应用程序》页，请检查终端控制台上是否出现与 MySQL、 JBoss 和用户应用程序相关的错误讯息，并请参见 “查错”在第 98 页 。

5.5 查错

如果在安装过程中遇到问题，请尝试这些查错步骤。如果这些步骤不能解决问题，请与 Novell 支持联系。Novell 代表将会仔细研究您可能存在的任何安装和配置问题。

问题	建议的操作

需要修改在安装过程中执行的用户应用程序配置设置。这包括类似于下列项目的配置：
◆ Identity Vault 连接和证书
◆ 电子邮件设置
◆ Metadirectory 用户身份、用户组
◆ iChain 设置
	可以运行配置实用程序，而不论是否运行了安装程序。
	在 Linux 上，从安装目录 （默认情况下为 /home/user/novell/idm）运行以下命令：
	`configupdate.sh`
	在 Windows 上，从安装目录 （默认情况下为 c:\novell\idm）运行以下命令：
	`configupdate.bat`

启动 JBoss 时引发异常，并显示日志讯息 《端口 8080 已在使用》	关闭 Tomcat （或其它服务器软件）的可能正在运行的任何实例。如果决定重配置 JBoss 以使用除 8080 以外的其它端口，请记住在 iManager 中编辑用户应用程序驱动程序的配置设置。
启动 JBoss 时，将显示一条讯息，指明找不到可信的证书。	确保使用在用户应用程序上安装的 JRE 启动 JBoss。
无法登录入口管理页。	确保存在用户应用程序管理员帐户。不要将此帐户与 iManager Admin 帐户相混淆。这是两个不同的 Admin 对象。

问题	建议的操作
能够以 Admin 身份登录，但是无法创建新用户。	用户应用程序管理员必须是顶层树枝的受托者，并且需要有主管权限。作为权宜之计，可以尝试将用户应用程序管理员的权限设置为等效于 LDAP 管理员的权限 （使用 iManager）。
启动 JBoss 时发生 MySQL 连接错误。	不要以根用户的身份运行。 确保 MySQL 正在运行 （并且适当的拷贝正在运行）。停止 MySQL 的其它任何实例。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，改正任何看上去可疑的值。然后运行底稿，再运行 /idm/start-jboss.sh。

启动 JBoss 应用程序服务器时遇到密钥存储区错误	JBoss 应用程序服务器没有使用用户应用程序安装程序所安装的 JRE，该 JRE 使用默认路径：
	
	`/idm/jre/lib/security/cacerts`
	
	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*。
	◆ 默认的密钥存储区口令为 *changeit* （如果有其它口令，请指定）。

激活 Novell Identity Manager 产品

6

以下信息说明激活如何影响基于 Novell® Identity Manager 的产品。必须在安装 Identity Manager、集成模块和供应模块后的 90 天内对其进行激活，否则它们将会关闭。可以在这 90 天期限内的任何时间，或者此后的任何时间，选择激活 Identity Manager 产品。

可以使用以下两种方法之一来激活 Identity Manager 和驱动程序。第一种方法包括以下任务：

- 购买 Identity Manager 产品许可证
- 使用通用身份凭证激活 Identity Manager 产品

第二种方法包括以下任务：

- 购买 Identity Manager 产品许可证
- 生成产品激活请求
- 提交产品激活请求
- 安装产品激活身份凭证

本小节还包含以下主题：

- “查看 Identity Manager 和驱动程序的产品激活”在第 105 页

6.1 购买 Identity Manager 产品许可证

要购买 Identity Manager 产品许可证，请参见 Novell Identity Manager 《如何购买》万维网网页 (http://www.novell.com/products/nsureidentitymanager/howtobuy.html)

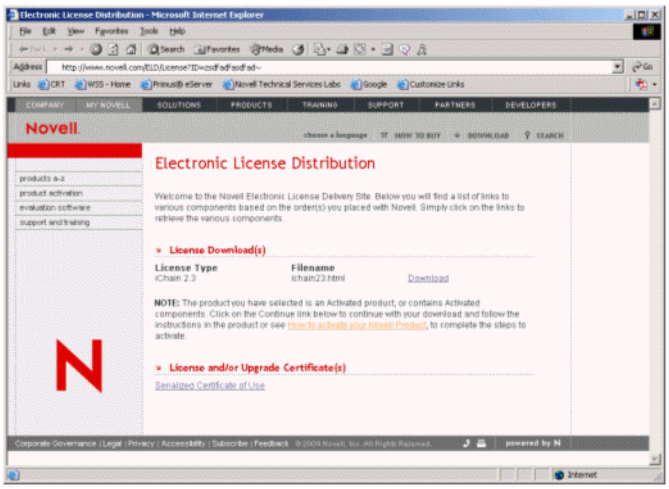
您购买产品许可证后， Novell 将通过电子邮件向您发送一个客户 ID。该电子邮件还包含可以在其中获取通用身份凭证的 Novell 站点的 URL。如果不记得或未收到客户 ID，请致电 Novell 激活中心：在美国请拨打 1-800-418-8373，在其它所有地区请拨打 1-801-861-8373。（如果您使用 801 区号通话，则会向您收费。）

6.2 使用通用身份凭证激活 Identity Manager 产品

1 购买许可证后，您将会收到 Novell 发送的电子邮件，其中包含了您的客户 ID。该电子邮件的 《订单细节》区域下方有一个链接，该链接指向可以在其中获取您的通用身份凭证的站点。单击该链接可转至该站点。

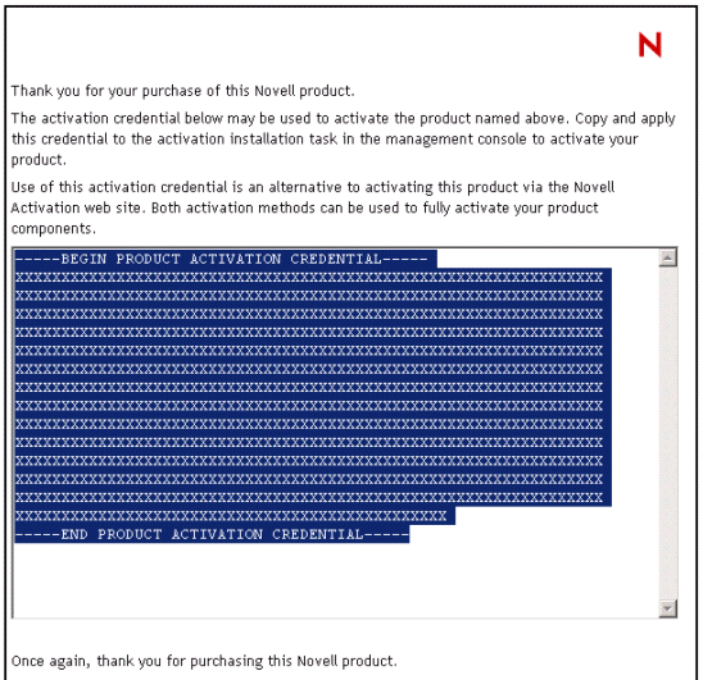
重要：只能使用三个不同的电子邮件地址来访问可以在其中获取通用身份凭证的链接。如果尝试使用三个以上的电子邮件地址访问该链接，则这种行为将被视为一种安全风险，因此站点将会拒绝您的访问。此外，只有指定为客户 ID 拥有者 / 契约人的电子邮件地址才能收到包含 《订单细节》区域 （提供有关获取通用许可证的信息）的电子邮件。如果响应电子邮件不包含 《订单细节》区域，则需要与组织中的客户 ID 受理人员联系，以获取通用身份凭证。

单击链接后，应该会显示类似于下图的页面：



2 单击许可证下载链接，然后保存 （下载）或打开 .html 文件。

文件打开后，其内容应类似于下图中显示的内容：



3 要获取有关如何激活 Identity Manager 和驱动程序的指导，请继续 “安装产品激活身份凭证”在第 104 页 。

6.3 生成产品激活请求

可以使用客户 ID 生成产品激活请求。您购买 Identity Manager 产品后，Novell 将向贵公司的主要联系人 （购买产品许可证的人员）发送一封包含客户 ID 的电子邮件。

如果忘记了或未收到客户 ID，请致电 Novell 激活中心：在美国请拨打 1-800-418-8373，在其它所有地区请拨打 1-801-861-8373。（如果可行，将会向您收取使用 801 区号通话的长途话费。）

注释：购买产品许可证的个人将会收到包含客户 ID 的电子邮件。如果贵公司指派采购代理来处理此交易，则您可能需要与此人核实以获取客户 ID。

应该先创建一个驱动程序集对象，然后再生成产品激活请求以激活 Identity Manager。

1. 转至 http://*serveripaddress*/nps/iManager.html 启动 iManager。
2. 单击 《Identity Manager 实用程序》 > 《请求激活》 >
3. 通过浏览找到要激活的驱动程序集，然后单击 《下一步》。

   注释：如果驱动程序集没有与某个服务器关联，或者与多个服务器关联，则系统会提示您选择与该驱动程序集关联的服务器。

   ---

4. 输入 Novell 客户 ID，然后单击 《下一步》构建激活请求文件。

   您的客户 ID 以及有关服务器树的标识信息将储存在产品激活请求中。
5. 将位于文本区域的产品激活请求复制到剪贴板，或者直接将请求保存到文件，然后单击《下一步》。

   以后进入 Novell 产品激活万维网站点时将会需要这些信息。

   重要：不要编辑产品激活请求的内容。

   ---

6. 单击超链接启动 Novell 产品激活万维网站点 (http://www.novell.com/products/activation)。

   或者

   单击 《完成》返回 iManager 的主菜单。

注释：要继续激活过程，需要在 Novell 产品激活万维网站点 (http://www.novell.com/products/activation) 上向 Novell 提交该产品激活请求。有关信息，请参见“提交产品激活请求”在第 103 页。

6.4 提交产品激活请求

创建产品激活请求后，可通过 Novell 产品激活万维网站点 (http://www.novell.com/products/activation) 将其提交给 Novell。随后， Novell 将会发送一封包含产品激活身份凭证的电子邮件。可使用该身份凭证激活套件或驱动程序组。

1. 转至产品激活万维网站点 (http://www.novell.com/products/activation)，然后单击《Identity Manager 产品》。
2. 遵循介绍性的屏幕内容，然后在出现提示时，使用 MyNovell 帐户登录。

   要访问产品激活万维网站点，必须具有 MyNovell 帐户。如果尚未获得该帐户，则可以在访问产品激活站点时创建该免费帐户。
3. 单击 《浏览》指定产品激活请求文件的路径，或者将产品激活请求的文本粘贴到文本区域。

   如果已将产品激活请求复制到磁盘，请确保所使用的计算机中存在该请求。

重要：不要编辑产品激活请求的内容。

4 单击 《提交》。

将显示可以激活的采购产品。

5 对正在激活的采购产品做标记。

一次只能激活一个采购产品。对当前正在激活的采购产品做标记。如果需要激活所列出的其它任何产品，并且这些产品将在同一树中使用，请再次提交产品激活请求。如果这些产品在不同的树中使用，则必须创建新的产品激活请求，然后提交该请求以获取身份凭证。

6 单击 《提交》。

Novell 将根据您提交的产品激活请求生成产品激活身份凭证，然后通过电子邮件向您发送该身份凭证。同时，还会向主要联系人发送该身份凭证的拷贝。

注释：某些公司对有权接收身份凭证的员工的列表进行了限制。您可能无权使用客户 ID。在这种情况下，单击 《提交》后，系统会向主要联系人发送通知。只有主要联系人批准了您使用客户 ID 后，您才能通过电子邮件接收身份凭证。

6.5 安装产品激活身份凭证

应该通过 iManager 安装产品激活身份凭证。以下过程说明如何安装产品激活身份凭证。

1 打开包含产品激活身份凭证的 Novell 电子邮件。

2 执行下列步骤之一：

- 保存产品激活身份凭证文件。

  或者

- 打开产品激活身份凭证文件，然后将其内容复制到剪贴板。

  重要：不要编辑产品激活身份凭证的内容。

3 打开 iManager。

4 选择 《Identity Manager 实用程序》 > 《安装激活》 > 。

5 选择驱动程序集，或通过浏览找到驱动程序集，然后单击 《下一步》。

重要：确保选择的驱动程序集所在的树与最初创建产品激活请求时所在的树相同。

6 如果驱动程序集没有与某个服务器关联，或者与多个服务器关联，请选择要与驱动程序集关联的服务器，然后单击 《下一步》。

将显示安装对话框。

7 执行下列步骤之一：

- 指定 Identity Manager 激活身份凭证保存的位置，然后单击 《下一步》。

  或者

- 将 Identity Manager 激活身份凭证的内容粘贴到文本区域，然后单击 《下一步》。

8 单击 《完成》。

注释：需要激活每个包含驱动程序的驱动程序集。可以使用相同的产品激活身份凭证来激活其它驱动程序集，前提是这些驱动程序集在同一树中。只能在创建产品激活请求时所在的树中使用产品激活身份凭证。

如果使用通用身份凭证，则可以激活任何树。

6.6 查看 Identity Manager 和驱动程序的产品激活

对于每个驱动程序集，都可以查看为 Metadirectory 引擎和 Identity Manager 驱动程序安装的产品激活身份凭证。要查看产品激活身份凭证，请执行下列操作：

1. 打开 iManager。
2. 单击 《Identity Manager》 > 《Identity Manager 概述》 >
3. 在对象名字段中输入要查看其激活信息的驱动程序集或驱动程序。

   或者

   通过浏览找到要查看其激活信息的驱动程序集或驱动程序。
4. 找到要查看其激活信息的驱动程序集，然后单击该驱动程序集的名称。
5. 选择 《激活》 选项卡。

   可以查看激活身份凭证的文本，或者，如果报告了错误，则可以去除激活身份凭证。

   注释：为驱动程序集安装了有效的产品激活身份凭证后，驱动程序名的旁边可能仍然会显示 《要求激活》。如果存在这种情况，请重启动驱动程序，此后该讯息应会消失。