

## 安装指南

# Novell® Identity Manager

**4.0.1**

2011 年 04 月 15 日

[www.novell.com](http://www.novell.com)



## 法律声明

Novell, Inc. 对于本文档的内容或使用不做任何陈述或保证，特别是对用于任何特定目的的适销性或适用性不做任何明示或暗示的保证。另外，Novell, Inc. 保留随时修订本出版物和更改其内容的权利，并且没有义务将这些修订或更改通知任何个人或实体。

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

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

版权所有 © 2007-2011 Novell, Inc. 保留所有权利。未经出版商的明确书面许可，不得复制、影印、传送此出版物的任何部分或将其储存在检索系统上。

Novell, Inc.  
404 Wyman Street, Suite 500  
Waltham, MA 02451  
U.S.A.  
[www.novell.com](http://www.novell.com)

*联机文档:* 要访问该 Novell 产品及其他 Novell 产品的最新联机文档，请参见 [Novell 文档网页 \(http://www.novell.com/documentation/\)](http://www.novell.com/documentation/)。

## Novell 商标

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

## 第三方资料

所有第三方商标均属其各自所有者的财产。

# 目录

关于本指南	7
<b>I 规划</b>	<b>9</b>
<b>1 建立开发环境</b>	<b>11</b>
<b>2 创建项目计划</b>	<b>13</b>
2.1 发现阶段	13
2.1.1 定义当前业务流程	13
2.1.2 定义 Identity Manager 解决方案影响当前业务流程的方式	15
2.1.3 确定关键的业务和技术利害关系人	15
2.1.4 与所有利害关系人面谈	15
2.1.5 创建高级别策略和达成一致的执行途径	16
2.2 需求和设计分析阶段	16
2.2.1 定义业务需求	17
2.2.2 分析业务流程	18
2.2.3 设计企业数据模型	18
2.3 概念验证	20
2.4 数据验证和准备	20
2.5 试生产	20
2.6 生产试点规划	20
2.7 生产部署	21
<b>3 技术准则</b>	<b>23</b>
3.1 管理工具准则	23
3.1.1 Analyzer 准则	24
3.1.2 Designer 准则	25
3.1.3 iManager 准则	25
3.1.4 角色映射管理器准则	25
3.2 元目录服务器准则	25
3.3 eDirectory 准则	26
3.3.1 eDirectory 中的 Identity Manager 对象	27
3.3.2 在服务器上复制 Identity Manager 需要的对象	27
3.3.3 使用“范围过滤”管理不同服务器上的用户	28
3.4 User Application	30
3.5 审计和报告准则	31
<b>II 安装</b>	<b>33</b>
<b>4 基本 Identity Manager 系统核对清单</b>	<b>35</b>
4.1 先决条件	35
4.2 规划	36
4.3 安装	36
4.4 带有 Remote Loader 的驱动程序配置	36
4.5 不带 Remote Loader 的驱动程序配置	37

4.6	其他配置	37
<b>5</b>	<b>从何处获取 Identity Manager</b>	<b>39</b>
<b>6</b>	<b>系统要求</b>	<b>43</b>
6.1	eDirectory 和 iManager	44
6.2	元目录服务器	45
6.2.1	支持的处理器	45
6.2.2	服务器操作系统	46
6.3	Remote Loader	47
6.4	User Application	48
6.5	审计和报告	49
6.6	工作站	49
6.6.1	工作站平台	50
6.6.2	Web 浏览器	51
6.7	资源要求	51
<b>7</b>	<b>安装 Identity Manager</b>	<b>53</b>
7.1	安装 Analyzer	53
7.2	安装 Designer	54
7.3	安装 eDirectory	54
7.4	安装 iManager	55
7.5	安装元目录服务器	55
7.5.1	元目录服务器的非根安装	56
7.5.2	元目录服务器的无提示安装	57
7.6	安装 Remote Loader	58
7.6.1	要求	59
7.6.2	支持的驱动程序	59
7.6.3	安装过程	60
7.6.4	Remote Loader 的无提示安装	61
7.6.5	在 UNIX 或 Linux 上安装 Java Remote Loader	62
7.6.6	32 位与 64 位 Remote Loader 的共存	62
7.7	安装驱动程序文件	63
7.8	安装 Roles Based Provisioning Module	64
7.9	安装自定义驱动程序	64
7.10	安装角色映射管理器	64
7.11	安装身份报告模块或 Sentinel	65
<b>8</b>	<b>激活 Novell Identity Manager 产品</b>	<b>67</b>
8.1	购买 Identity Manager 产品许可证	67
8.2	安装产品激活身份凭证	67
8.3	查看 Identity Manager 和驱动程序的产品激活	68
8.4	激活 Identity Manager 驱动程序	68
8.5	激活 Analyzer	69
8.6	激活 Designer 和角色映射管理器	69

<b>9 Identity Manager 查错</b>	<b>71</b>
<b>10 新功能</b>	<b>77</b>
10.1 Identity Manager 4.0.1 新功能	77
10.1.1 Identity Manager Advanced Edition 与 Standard Edition	77
10.1.2 Telemetry	77
10.1.3 资源请求活动	77
10.1.4 身份报告模块中添加了新报告	77
10.1.5 Designer 调色板中添加了应用程序	78
10.2 Identity Manager 4.0 新功能	78
10.2.1 身份报告模块	78
10.2.2 新驱动程序	78
10.2.3 支持 XDAS 审计	79
10.2.4 包替换了驱动程序配置文件	79
10.2.5 角色映射管理器	79
10.2.6 Analyzer	79
10.2.7 集成安装程序	79
<b>III 升级 Identity Manager</b>	<b>81</b>
<b>11 升级与迁移</b>	<b>83</b>
<b>IV 卸装 Identity Manager</b>	<b>85</b>
<b>12 卸装 Identity Manager 组件</b>	<b>87</b>
12.1 去除 eDirectory 中的对象	87
12.2 卸装元目录服务器	87
12.2.1 在 Linux/UNIX 上卸装	88
12.2.2 在 Windows 上卸装	88
12.2.3 卸装非根安装	88
12.3 卸装 Remote Loader	88
12.3.1 在 Linux/UNIX 上卸装	88
12.3.2 在 Windows 上卸装	88
12.4 卸装 Roles Based Provisioning Module	89
12.4.1 删除驱动程序	89
12.4.2 卸装 User Application	89
12.4.3 卸装应用程序服务器和数据库	89
12.5 卸装身份报告模块组件	90
12.5.1 删除报告驱动程序	90
12.5.2 卸装身份报告模块	91
12.5.3 卸装事件审计服务	91
12.6 卸装 iManager	91
12.7 卸装 eDirectory	91
12.8 卸装 Analyzer	92
12.9 卸装 Designer	92
12.10 卸装角色映射管理器	93



# 关于本指南

Novell Identity Manager 是一种数据共享和同步服务，它使应用程序、目录和数据库可以共享信息。它链接分散的信息；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 Web 服务提供了基础。通过它可以集成、管理和控制分发的身份信息，以便安全地将适当的资源递送给适当的人员。

本指南包含有关如何规划、安装或升级有益于您环境的 Identity Manager 系统的信息。

- ◆ 第 I 部分“规划”（第 9 页）
  - ◆ 第 1 章“建立开发环境”（第 11 页）
  - ◆ 第 2 章“创建项目计划”（第 13 页）
  - ◆ 第 3 章“技术准则”（第 23 页）
- ◆ 第 II 部分“安装”（第 33 页）
  - ◆ 第 4 章“基本 Identity Manager 系统核对清单”（第 35 页）
  - ◆ 第 5 章“从何处获取 Identity Manager”（第 39 页）
  - ◆ 第 6 章“系统要求”（第 43 页）
  - ◆ 第 7 章“安装 Identity Manager”（第 53 页）
  - ◆ 第 8 章“激活 Novell Identity Manager 产品”（第 67 页）
  - ◆ 第 9 章“Identity Manager 查错”（第 71 页）
  - ◆ 第 10 章“新功能”（第 77 页）
- ◆ 第 III 部分“升级 Identity Manager”（第 81 页）
  - ◆ 第 11 章“升级与迁移”（第 83 页）
- ◆ 第 IV 部分“卸载 Identity Manager”（第 85 页）

## 适用对象

本指南面向规划 Identity Manager 并将其实施到网络环境中的管理员、顾问和网络工程师。

## 文档更新

有关本文档的最新版本，请访问 [Identity Manager 文档网站 \(http://www.novell.com/documentation/idm401/index.html\)](http://www.novell.com/documentation/idm401/index.html)。

## 其他文档

有关其他 Identity Manager 驱动程序文档，请参见 [Identity Manager 驱动程序文档网站 \(http://www.novell.com/documentation/idm401drivers/index.html\)](http://www.novell.com/documentation/idm401drivers/index.html)。

有关 User Application 文档，请参见 [Identity Manager Roles Based Provisioning Module 文档网站 \(http://www.novell.com/documentation/idmrbpm401/index.html\)](http://www.novell.com/documentation/idmrbpm401/index.html)。





# 规划

Identity Manager 4.0.1 帮助您管理企业中的身份和资源。它还可使当前为手动任务的许多业务流程自动化。

如果您对构成 Identity Manager 解决方案的不同组件有任何问题，请参见 《[Identity Manager 4.0.1 概述指南](#)》了解有关各个组件的更多信息。

要为环境创建一个有效的 Identity Manager 解决方案，首先必须花些时间来规划和设计解决方案。规划主要有两个方面：建立测试实验室以熟悉产品；创建项目计划以实施 Identity Manager 解决方案。创建项目计划时，定义业务流程并创建实施计划。大多数公司具有由众多不同人员管理的众多不同业务流程。一个完整的 Identity Manager 解决方案会影响其中大多数流程。花点时间来规划 Identity Manager 解决方案是极其重要的，这样就可环境中有效实施。

如果您正在创建一个新的 Identity Manager 解决方案，其中所有组件都位于同一服务器上，请使用 《[Identity Manager 4.0.1 集成安装指南](#)》帮助安装。这是一款简化的安装程序，有助于更快速地设置系统。

强烈建议您聘请一位 Identity Manager 专家，便于在 Identity Manager 实施的每个阶段提供帮助。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 \(http://www.novell.com/partners/\)](http://www.novell.com/partners/)。Novell 培训还提供与 Identity Manager 实施有关的课程。

- ◆ 第 1 章“建立开发环境”（第 11 页）
- ◆ 第 2 章“创建项目计划”（第 13 页）
- ◆ 第 3 章“技术准则”（第 23 页）



# 建立开发环境

开始 Identity Manager 部署的规划阶段前，必须熟悉 Identity Manager 产品，以便创建一个有用的计划。建立开发环境（可以在该环境中测试、分析和开发 Identity Manager 解决方案）允许您了解 Identity Manager 的各个组件并查找可能出现的不可预见问题。

例如，在不同系统间同步信息时，每个系统的信息呈现方式均有所不同。通过更改数据以查看它如何在这两个系统间同步，便可查看此更改是否会影响使用此相同信息的其他系统。

建立开发环境的另一重要原因是在将解决方案应用于在线数据前确保解决方案有效。Identity Manager 可处理和删除数据。拥有测试环境可使您执行更改，但不会对生产环境中的数据造成任何损失。

应对每个 Identity Manager 部署均建立开发环境。每个部署均不同。有不同的系统、业务策略和过程需要包含在 Identity Manager 解决方案中。通过开发环境，您可创建对于各种情况都最佳的解决方案。

开发 Identity Manager 解决方案时，要使用的最重要工具是 Designer。使用该工具可捕获有关环境的所有信息，然后使用该信息来创建适合需求的 Identity Manager 解决方案。在整个规划期间都应使用 Designer 来截获所有信息。使用 Designer 可更加轻松地创建包括业务信息和技术信息的项目计划。有关 Designer 的更多信息，请参见《[Designer 4.0.1 for Identity Manager 4.0.1 管理指南](#)》。

要建立开发环境，请使用第 4 章“[基本 Identity Manager 系统核对清单](#)”（第 35 页）中的信息。其中是一个所有 Identity Manager 组件的安装核对清单。使用此清单可确保已安装并配置了用于开发项目计划的 Identity Manager 的所有组件。建立开发环境时请使用第 3 章“[技术准则](#)”（第 23 页）中的信息，以便了解有关安装和配置 Identity Manager 的各个组件时的技术注意事项。

创建开发环境后，下一步骤是创建项目计划以实施 Identity Manager 解决方案。使用第 2 章“[创建项目计划](#)”（第 13 页）中的信息来创建项目计划。



# 创建项目计划

# 2

此规划材料概述了通常属于 Identity Manager 项目的活动，从最初到完整的生产部署。实施身份管理策略要求发现当前业务流程的全部内容、这些流程的需求、环境中的利害关系人，然后设计解决方案、获得利害关系人的认同然后测试并试点解决方案。本部分旨在帮助您充分了解该过程，以便您能够通过使用 Identity Manager 获得最大的收益。

本部分并未详尽说明；不旨在讲述所有可能的配置，也不是为了要求严格执行配置。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。

- ◆ 第 2.1 节“发现阶段”（第 13 页）
- ◆ 第 2.2 节“需求和设计分析阶段”（第 16 页）
- ◆ 第 2.3 节“概念验证”（第 20 页）
- ◆ 第 2.4 节“数据验证和准备”（第 20 页）
- ◆ 第 2.5 节“试生产”（第 20 页）
- ◆ 第 2.6 节“生产试点规划”（第 20 页）
- ◆ 第 2.7 节“生产部署”（第 21 页）

## 2.1 发现阶段

Identity Manager 解决方案将影响业务的众多方面。要创建有效的解决方案，您必须花点时间来定义所有当前业务流程；然后确定 Identity Manager 的实施将如何更改这些流程；这些更改将影响谁以及如何实施更改。

发现阶段能使所有利害关系人对问题和解决方案达成共识。该阶段创建一个包含受 Identity Manager 解决方案影响的关键业务和系统信息的计划或路线图。该阶段还允许所有利害关系人参与 Identity Manager 解决方案的创建，以便他们可以理解该解决方案将如何影响其业务领域。

以下列表指出一个成功的发现阶段所需的步骤。在处于发现和设计阶段时，您可能发现还有其他项要添加到该列表中。

- ◆ 第 2.1.1 节“定义当前业务流程”（第 13 页）
- ◆ 第 2.1.2 节“定义 Identity Manager 解决方案影响当前业务流程的方式”（第 15 页）
- ◆ 第 2.1.3 节“确定关键的业务和技术利害关系人”（第 15 页）
- ◆ 第 2.1.4 节“与所有利害关系人面谈”（第 15 页）
- ◆ 第 2.1.5 节“创建高级别策略和达成一致的执行途径”（第 16 页）

### 2.1.1 定义当前业务流程

Identity Manager 将业务流程自动化以轻松地管理环境中的身份。如果不知道当前业务流程的内容，则无法设计使这些流程自动化的 Identity Manager 解决方案。可使用 Designer 的“体系结构”方式来捕获当前业务流程并用图形方式显示。有关更多信息，请参见《*Designer 4.0.1 for Identity Manager 4.0.1 管理指南*》中的“设计者模式”。

例如，您的企业可能见过以下业务流程：

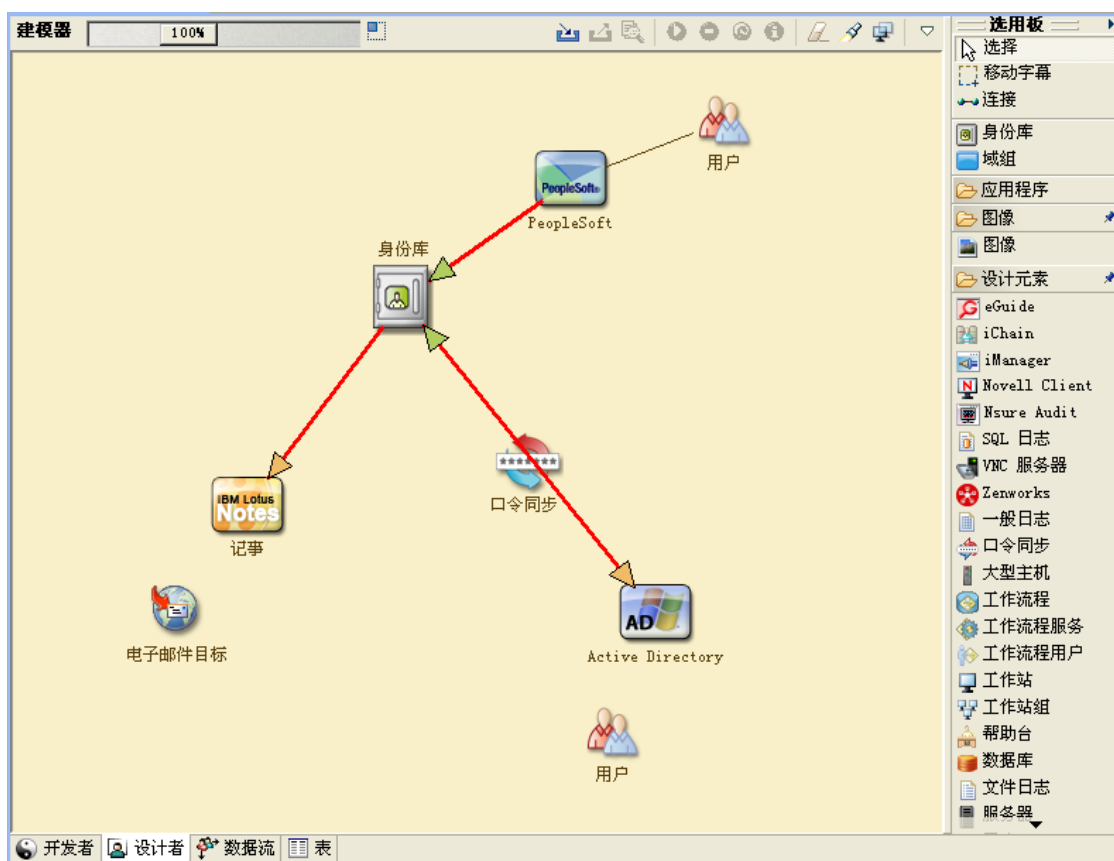
- ◆ 解雇某个员工时，删除电子邮件系统中的该用户帐户，但在所有其他系统中禁用（而非删除）该用户的帐户。
- ◆ 用户电子邮件地址的格式。
- ◆ 销售人员可访问的系统或资源。
- ◆ 经理可访问的系统或资源。
- ◆ 哪些系统生成新帐户？是人力资源系统还是通过工作流程请求？
- ◆ 公司的口令策略，定义口令更改的频率、口令的复杂程度以及同步口令的系统。

定义业务流程时，请使用以下列表项来帮助您了解所有流程：

- ◆ 定义或声明当前业务问题。
- ◆ 确定解决这些问题需要哪些计划。
- ◆ 确定受这些计划影响的服务和系统。

通过此步骤可创建有关业务的当前内容以及需要改进的流程的高级概述。例如，图 2-1 使用 Designer 显示了新用户帐户是如何从 PeopleSoft 系统中生成的。这些用户帐户先同步到身份库，然后又同步到 Lotus Notes 和 Active Directory。口令在 Active Directory 和身份库之间同步。帐户会同步到 Notes 系统，但没有任何帐户会向后同步到身份库。

图 2-1 业务流程的示例



确定流程后，您开始思考如何才能使 Identity Manager 参与这个流程。继续第 2.1.2 节“定义 Identity Manager 解决方案影响当前业务流程的方式”（第 15 页）。

## 2.1.2 定义 Identity Manager 解决方案影响当前业务流程的方式

定义当前业务流程后，需要决定将哪些流程合并到 Identity Manager 解决方案中。

最好先查看整个解决方案，然后确定应实施的流程的优先顺序。Identity Manager 包含业务的众多方面，因此规划整个解决方案比起将每个业务流程作为各自的解决方案来实现更容易。

创建要自动化的业务流程的优先级列表，然后确定这些更改将会影响的系统。然后继续第 2.1.3 节“确定关键的业务和技术利害关系人”（第 15 页）。

## 2.1.3 确定关键的业务和技术利害关系人

确定 Identity Manager 解决方案所涉及的所有利害关系人对于解决方案的成功非常重要。在大多数公司中，您可以接触到的了解业务流程所有业务和技术方面的人不止一位。必须确定哪些服务和系统将会受到 Identity Manager 解决方案的影响，并且还必须确定负责该服务或系统的人员。

例如，如果要将电子邮件系统合并到解决方案中，则需要列出电子邮件系统的类型、电子邮件系统的管理员及其联系信息。可将所有此类信息添加到 Designer 项目中。每个应用程序图标都有一个用于存储有关系统和系统管理员信息的位置。有关更多信息，请参见《*Designer 4.0.1 for Identity Manager 4.0.1 管理指南*》中的“配置应用程序属性”。

确定每个业务流程所涉及的所有人员后，下一步在第 2.1.4 节“与所有利害关系人面谈”（第 15 页）中。

## 2.1.4 与所有利害关系人面谈

通过与关键的业务和技术利害关系人面谈，可收集 Identity Designer 解决方案的完整设计所需的信息。通过面谈，您还可使各个利害关系人理解 Identity Manager 解决方案以及该解决方案对其造成的影响。以下是进行面谈时涵盖的事项列表：

- ◆ 定义或声明 Identity Manager 解决方案处理的业务流程。您面谈的人可能具有可更改当前计划的信息。
- ◆ 确定该解决方案将如何影响利害关系人以及如何解决其关注的问题。还要询问利害关系人该解决方案在他们相关的部分可能花费的时间。他们可能或不能进行估计，但收集此信息有助于确定解决方案的范围。
- ◆ 捕获来自利害关系人的关键业务和系统信息。有时，提议的计划可能会对业务流程或系统造成负面影响。通过捕获此信息，可做出有关 Identity Manager 解决方案的合理决策。

与关键利害关系人面谈后，下一步在第 2.1.5 节“创建高级别策略和达成一致的执行途径”（第 16 页）中。

## 2.1.5 创建高级别策略和达成一致的执行途径

收集所有信息后，需要为 Identity Manager 解决方案创建高级别策略或路线图。添加要包含在 Identity Manager 解决方案中的所有功能。例如，新用户帐户通过某个工作流程从某个请求生成，但用户类型取决于允许用户访问的资源。

将此高级别策略展示给同一会议中的所有利害关系人（如果可能）。这使您能够完成很多事情：

- ◆ 验证所包括的计划是否是最正确的并确定哪些具有最高优先级。
- ◆ 确定规划活动，为需求和设计阶段作准备。
- ◆ 确定执行其中一项或多项计划需要哪些操作。
- ◆ 为 Identity Manager 解决方案创建达成一致的执行途径。
- ◆ 定义针对利害关系人的其他培训。

发现能使所有利害关系人对问题和解决方案达成共识。它为分析阶段提供了极好的基础，分析阶段需要股东对目录、Novell eDirectory、Novell Identity Manager 和 XML 集成大体上有基本的了解。

完成发现阶段后，请继续第 2.2 节“需求和设计分析阶段”（第 16 页）。

## 2.2 需求和设计分析阶段

利用在发现阶段创建的高级别路线图作为此分析阶段的起点。文档和 Designer 项目都需要添加技术和业务细节。这可产生用于实施 Identity Manager 解决方案的数据模型和高级别 Identity Manager 体系结构设计。

应将设计重心专门放在身份管理上，但是，也可以涉及到通常与资源管理目录（例如文件和打印）相关的许多元素。Identity Manager 将用户帐户同步到对操作系统的文件系统没有直接访问权的目录。例如，您可在 Active Directory 中具有用户帐户，但这并不会授予您对 Active Directory 服务器上文件系统的访问权。

使用在发现阶段收集的信息，回答以下示例问题，从而了解还需收集的其他信息。这可能要求与利害关系人再次进行面谈。

- ◆ 所使用的系统软件的版本是什么？
- ◆ eDirectory 设计是否恰当？例如，Identity Manager 服务器是否包含正在同步的用户对象的主复本或读/写复本？如果不包含，则 eDirectory 设计不恰当。
- ◆ 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施业务策略。）例如，要同步的系统中可能存在用户的重复帐户，或各个系统的数据格式可能不一致。在同步信息前，必须先评估各个系统的数据。
- ◆ 环境是否需要数据处理？例如，用户的雇用日期格式在人力资源系统中只能是 2008/02/23，而身份库中的雇用日期是 02-23-2008。这要求处理数据以使同步能够进行。

Identity Manager 包含一种有助于简化数据分析和清理过程的工具。有关更多信息，请参见《*Analyzer 4.0.1 for Identity Manager 管理指南*》。

请查看第 3 章“技术准则”（第 23 页）中的信息以帮助做出有关环境的正确决策。



完成需求分析后，可为实施建立范围和项目计划，并确定是否需要执行任何先决活动。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。以下是可能的需求的列表：

- ◆ 数据模型，显示所有系统、数据权威来源、事件、信息流、数据格式标准，以及 Identity Manager 中已连接系统和属性之间的映射关系。
- ◆ 解决方案的相应 Identity Manager 体系结构。
- ◆ 其他系统连接要求的细节。
- ◆ 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。

在需求和设计评估过程中，应完成下列任务：

- ◆ [定义业务需求（第 17 页）](#)
- ◆ [分析业务流程（第 18 页）](#)
- ◆ [设计企业数据模型（第 18 页）](#)

## 2.2.1 定义业务需求

在发现阶段中，您收集了贵组织的业务流程以及定义这些业务流程的业务需求。创建这些业务需求的列表，然后通过完成以下任务开始在 Designer 中映射这些流程：

- ◆ 创建业务需求的列表并确定受此流程影响的系统。例如，解雇一个员工的业务需求可能是，在解雇该员工的当天必须去除该员工的网络和电子邮件帐户访问权限。电子邮件系统和身份库受此解雇流程的影响。
- ◆ 建立流程、流程触发器和数据映射关系。  
例如，如果某个流程中有事情发生，那么会触发其他哪些流程呢？
- ◆ 在应用程序之间映射数据流。Designer 允许您查看此信息。有关更多信息，请参见《[Designer 4.0.1 for Identity Manager 4.0.1 管理指南](#)》中的“[管理数据流](#)”。
- ◆ 认识从一种格式到另一种格式的数据转换，例如 2/25/2007 到 25 Feb 2007，并使用 Analyzer 更改数据。有关更多信息，请参见《[Analyzer 4.0.1 for Identity Manager 管理指南](#)》。
- ◆ 记录存在的数据依赖性。

如果更改了某个值，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规划路线图。

将部署分阶段进行（使一部分部署早点实施，其余部分晚点实施），或使用分阶段进行的部署（基于组织中的人员分组）可能比较有利。

- ◆ 定义前提条件。

应该记录实施部署的特定阶段所需的先决条件。这包括对需要与 Identity Manager 连接的已连接系统的访问权限。

- ◆ 确定权威数据源。

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保持认可。

例如，帐户管理员可能需要为员工授予特定文件和目录访问权限的所有权。在帐户系统中实施本地受托者指派可以达到此目的。

定义业务需求后，请转到[第 2.2.2 节“分析业务流程”](#)（第 18 页）。

## 2.2.2 分析业务流程

完成业务需求的分析后，您需要收集更多信息以帮助您专注于 Identity Manager 解决方案。您需要与实际使用该应用程序或系统的重要人士面谈，如经理、管理员和员工。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（收集和 / 或编辑）的工作惯例是什么？
- ◆ 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？
- ◆ 系统驻留在何处（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，可以对人力资源的 PeopleSoft 系统管理员提出以下问题：

- ◆ 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？
- ◆ 供应系统中必须反映哪些操作（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 / 行为？
- ◆ 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他区域，这样可以更清楚地展现整个过程。

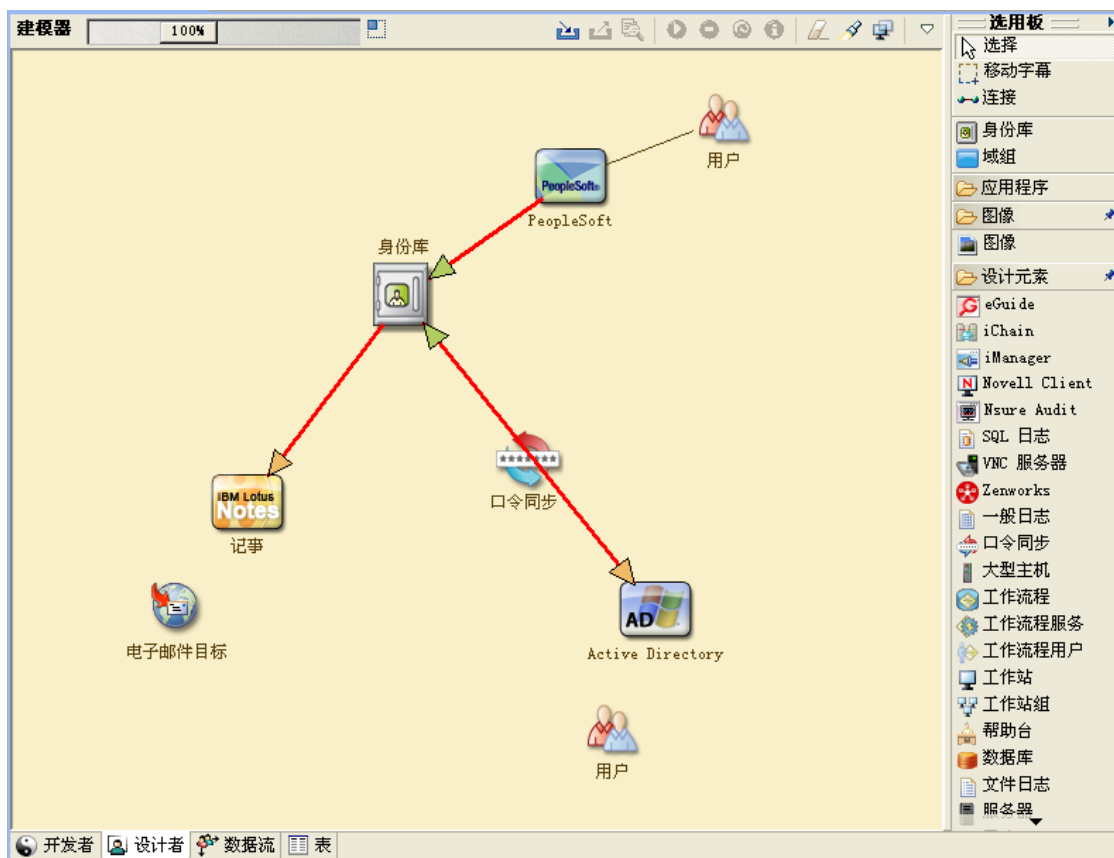
收集所有此类信息后，即可为您的环境设计正确的企业数据模型。请转到[第 2.2.3 节“设计企业数据模型”](#)（第 18 页）以开始设计。

## 2.2.3 设计企业数据模型

定义业务流程后，可使用 Designer 开始设计反映当前业务流程的数据模型。

Designer 中的模型应该阐明数据的来源、要移至的位置以及不能移至的位置。它还应说明关键事件如何影响数据流。例如，[图 2-2](#) 显示数据来自 PeopleSoft，但没有数据会向后同步到 PeopleSoft。

图 2-2 通过 Designer 的数据流



您还可能希望制作图表，用于演示建议的业务流程以及在该流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 中的员工状态字段可能三个设置值：员工、合同工和实习生。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”状态与 Active Directory 中的“永久”和“临时”值之间的关系。

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属性需要同步。设计完成后，下一步是创建概念检验。转到第 2.3 节“概念验证”（第 20 页）。

## 2.3 概念验证

通过在实验室环境中使用样本实施，创建对概念验证的测试，以反映企业的业务策略和数据流。该实施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。在[第 1 章“建立开发环境”（第 11 页）](#)中创建的实验室里执行测试。

---

**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。

---

[第 3 章“技术准则”（第 23 页）](#)包含可帮助您进行概念检验的信息。它包含帮助您成功部署 Identity Manager 的技术准则。

创建概念检验时，您还需要创建一个计划以验证系统中具有的数据。此步骤帮助您确保系统间不会发生冲突。请转到[第 2.4 节“数据验证和准备”（第 20 页）](#)以确保这些冲突不会发生。

## 2.4 数据验证和准备

生产系统中数据的质量和一致性可能有所不同，因此同步系统时可能会造成不一致的情况。此阶段明确显示资源实施团队与业务单位或组（“拥有”或管理系统中要集成的数据）之间的分隔点。相关的风险和成本因素有时可能不属于供应项目。

您需要使用已在分析和设计阶段完成的数据模型。您还应定义可能的记录匹配和数据格式策略，以便正确地准备数据。在定义了数据模型和格式策略后，可以完成两个重要步骤：

- ◆ 创建适合装载到身份库的生产数据集（已在分析和设计活动中确定）。这包括可能的装载方法（批量装载或通过连接器装载）。同时确定已验证或格式化的数据需求。
- ◆ 确定性能因素，并针对正在使用的设备和 Identity Manager 部署的整体分布式体系结构验证这些因素。

准备好数据后，请转到[第 2.5 节“试生产”（第 20 页）](#)。

## 2.5 试生产

试生产是迁移到生产环境的第一步。在此阶段可能有其他自定义操作发生。在此有限的简介中，可确认前面的活动所需的结果，并获得生产试点的协议。试生产验证流程中目前为止创建的计划。

---

**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里程碑和路线。

---

试行解决方案为数据模型以及所需流程结果提供真实的概念检验和验证。完成试生产后，请转到[第 2.6 节“生产试点规划”（第 20 页）](#)。

## 2.6 生产试点规划

在此阶段中规划生产部署。规划应完成以下任务：

- ◆ 确认服务器平台、软件修订版和 Service Pack
- ◆ 确认常规环境
- ◆ 确认身份库的设计在混合共存环境中
- ◆ 确认业务逻辑正确

- ◆ 确认数据同步按计划进行
- ◆ 计划传统过程的交接
- ◆ 计划回滚应变策略

该计划需要包含试点中各个步骤的实施和完成日期。每个利害关系人均输入这些日期并同意可以使用这些日期。这使得试点所涉及的每个人均了解更改的开始时间和完成时间。

完成生产试点计划后，请转到[第 2.7 节“生产部署”](#)（第 21 页）。

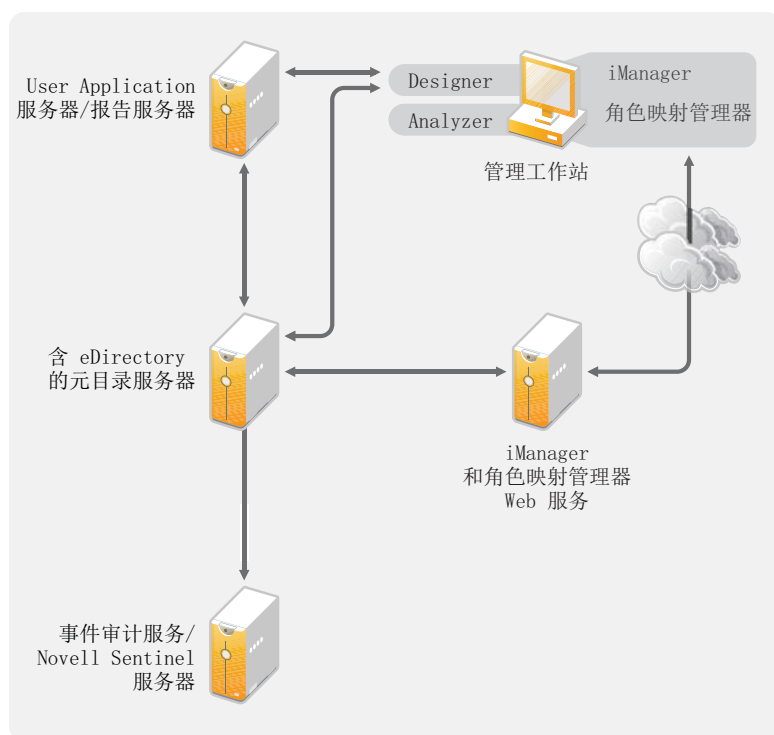
## 2.7 生产部署

生产部署阶段将所有计划付诸于行动，这样就在在线环境中创建了 Identity Manager 解决方案。使用生产试点计划将 Identity Manager 解决方案的不同部分融合到一起。根据计划的复杂性，该阶段可能快速完成，也可能需要一些时间来完成。



借助在 Designer 中收集的信息，您可做出有关 Identity Manager 各个组件的技术决策，例如安装位置和配置选项。有关各个组件的介绍，请参见《[Identity Manager 4.0.1 概述指南](#)》。[图 3-1](#) 是 Identity Manager 解决方案的一个可能配置。

**图 3-1** Identity Manager 组件



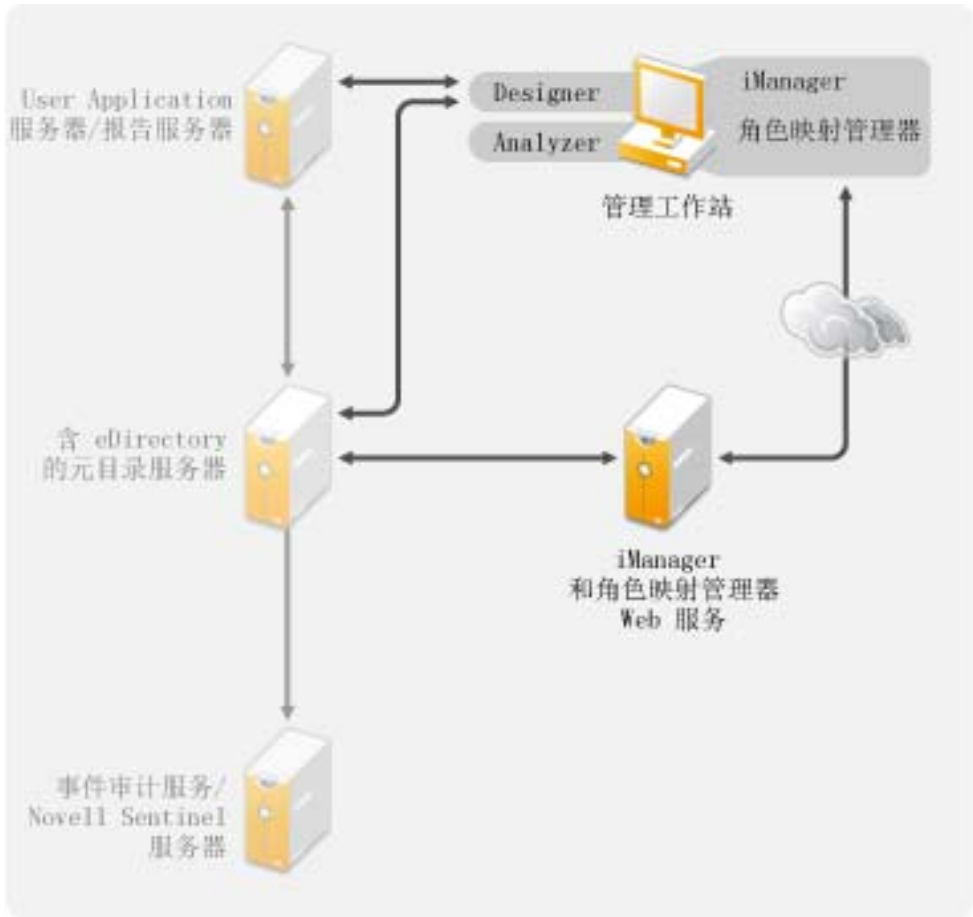
Identity Manager 的自定义程度很高。以下部分包含技术最佳实践准则，可帮助您建立并配置为您的环境提供最佳服务的 Identity Manager 解决方案。影响这些准则对环境的适用程度的可变因素包括：服务器具有的硬件类型、WAN 的配置方式以及正在同步的对象数量。

- ◆ [第 3.1 节“管理工具准则”](#)（第 23 页）
- ◆ [第 3.2 节“元目录服务器准则”](#)（第 25 页）
- ◆ [第 3.3 节“eDirectory 准则”](#)（第 26 页）
- ◆ [第 3.4 节“User Application”](#)（第 30 页）
- ◆ [第 3.5 节“审计和报告准则”](#)（第 31 页）

## 3.1 管理工具准则

Identity Manager 解决方案的两个主要管理工具是 Designer 和 iManager，如[图 3-2](#) 中所示。Designer 在规划和创建 Identity Manager 解决方案期间使用，而 iManager 用于 Identity Manager 解决方案的日常管理任务。

图 3-2 Identity Manager 管理工具



User Application 使用基于 Web 的管理页面。有关 User Application 的更多信息，请参见《*Identity Manager Roles Based Provisioning Module 4.0 User Application: 管理指南*》中的“管理 User Application”。

- ◆ 第 3.1.1 节“Analyzer 准则”（第 24 页）
- ◆ 第 3.1.2 节“Designer 准则”（第 25 页）
- ◆ 第 3.1.3 节“iManager 准则”（第 25 页）
- ◆ 第 3.1.4 节“角色映射管理器准则”（第 25 页）

### 3.1.1 Analyzer 准则

Analyzer 是安装在工作站上的富客户端。Analyzer 用于检查和清理您要添加到 Identity Manager 解决方案中的系统数据。在规划阶段使用 Analyzer 有助于了解需要进行的更改及这些更改的效果。

对于使用 Analyzer，没有重要的注意事项。有关更多信息，请参见《*Analyzer 4.0.1 for Identity Manager 管理指南*》。



### 3.1.2 Designer 准则

Designer 是一个安装在 workstation 上的富客户端。Designer 用于设计、测试、记录以及部署 Identity Manager 解决方案。在整个规划阶段使用 Designer 可帮助您在一个位置捕获信息。当您同时查看解决方案的所有组件时，它还帮助您发现没有注意到的问题。

不存在使用 Designer 的主要注意事项，除非有多个人在处理同一个项目。Designer 允许对项目进行版本控制。有关更多信息，请参见《*Designer 4.0.1 for Identity Manager 4.0.1 管理指南*》中的“版本控制”。

### 3.1.3 iManager 准则

iManager 是一款 Web 应用程序，是 Identity Manager 的管理工具。安装 Identity Manager 时，安装程序期望您已在 eDirectory 树中安装了 iManager 服务器。

如果您有 10 个以上的管理员经常同时使用 iManager，则应具有一个仅托管 iManager 的服务器。图 3-2 在第 24 页表示 Identity Manager 解决方案的这种配置。如果仅具有一个管理员，则可在元目录服务器上运行 iManager，而不会造成混乱。

### 3.1.4 角色映射管理器准则

角色映射管理器是一款 Web 应用程序，可发现您主要 IT 系统内可授予的授权和许可权限。它允许业务分析员（而不仅仅是 IT 管理员）定义和维护哪些授权与哪些业务角色关联。

对于使用角色映射管理器，没有重要的注意事项。可以在独立的服务器上运行角色映射管理器（如图 3-2 在第 24 页所示），也可以在元目录服务器上运行。有关更多信息，请参见《*Identity Manager 角色映射管理器 4.0.1 安装和配置指南*》。

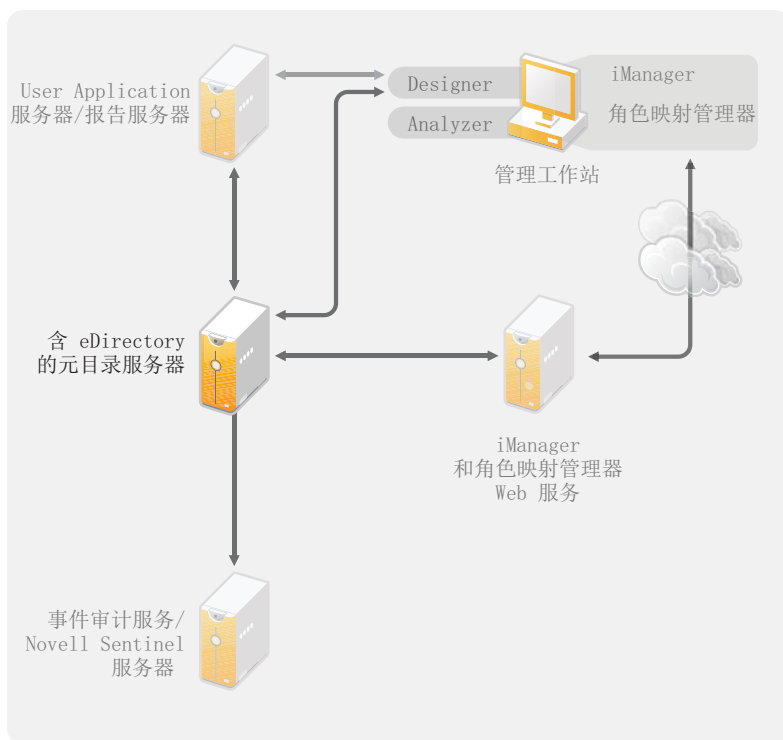
## 3.2 元目录服务器准则

Identity Manager 解决方案中可具有一个或多个元目录服务器，具体取决于服务器工作负载。元目录服务器要求安装 eDirectory，如图 3-3 中所示。您可添加 Remote Loader 服务器（该图中不存在）以帮助处理环境中的工作负载或配置。

驱动程序必须与已连接应用程序运行在同一服务器上。例如，要配置 Active Directory 驱动程序，图 3-3 中的服务器必须是成员服务器或域控制器。如果不希望在成员服务器或域控制器上安装 eDirectory 和 Identity Manager，则可在成员服务器或域控制器上安装 Remote Loader。Remote Loader 会将来自 Active Directory 的所有事件发送到元目录服务器。Remote Loader 从元目录服务器接收任何信息并传递给已连接应用程序。

Remote Loader 为您的 Identity Manager 解决方案提供了更多的灵活性。有关更多信息，请参见《*Identity Manager 4.0.1 Remote Loader 指南*》。

图 3-3 元目录服务器



有许多可变因素会影响服务器的性能。标准建议是在一台元目录服务器上运行的驱动程序不要多于 10 个。但是，如果每个驱动程序要同步数以百万计的对象，则可能无法在一个服务器上运行 10 个驱动程序。另一方面，如果每个驱动程序同步 100 个对象，则或许能在一台服务器上运行 10 个以上的驱动程序。

通过在实验室环境中建立 Identity Manager 解决方案，可测试服务器将如何执行。可使用 iManager 中的状态监视工具来获取基线，然后即可做出有关环境的最佳决策。有关状态监视工具的更多信息，请参见《Identity Manager 4.0.1 常用驱动程序管理指南》中的“[监视驱动程序状态](#)”。

有关每个驱动程序的注意事项，请参见 Identity Manager 驱动程序文档网站 (<http://www.novell.com/documentation/idm36drivers/index.html>)。特定于驱动程序的信息在各个驱动程序指南中都提供。

## 3.3 eDirectory 准则

eDirectory 是存储通过 Identity Manager 解决方案同步的对象的身份库。以下部分包含帮助您规划 eDirectory 部署的准则。

- ◆ [第 3.3.1 节“eDirectory 中的 Identity Manager 对象”](#)（第 27 页）
- ◆ [第 3.3.2 节“在服务器上复制 Identity Manager 需要的对象”](#)（第 27 页）
- ◆ [第 3.3.3 节“使用“范围过滤”管理不同服务器上的用户”](#)（第 28 页）

### 3.3.1 eDirectory 中的 Identity Manager 对象

以下列表指出 eDirectory 中存储的主要 Identity Manager 对象以及这些对象如何彼此互相关联。安装 Identity Manager 过程中不会创建任何对象。Identity Manager 对象在配置 Identity Manager 解决方案过程中创建。

- ◆ **驱动程序集：**驱动程序集是保存 Identity Manager 驱动程序和库对象的容器。在任何时候，一台服务器上只能有一个驱动程序集处于活动状态。但可能有多台服务器与一个驱动程序集关联。且一个驱动程序也可以同时与多台服务器关联。但此驱动程序在任何时候只应在一台服务器上运行。此驱动程序在其他服务器上应处于禁用状态。与驱动程序集关联的任何服务器上都必须已安装元目录服务器。
- ◆ **库：**库对象是可从多个位置参照的常用策略的储存库。库存储在驱动程序集中。可将策略放置在库中，以便驱动程序集中的每个驱动程序均可参照它。
- ◆ **驱动程序：**驱动程序连接应用程序与身份库。它还允许在系统间进行数据同步和共享。驱动程序存储在驱动程序集中。
- ◆ **作业：**作业就是将重现的任务自动化。例如，某个作业可以将系统配置为在特定一天禁用帐户，或启动工作流程以请求延长某用户对公司资源的访问时限。作业存储在驱动程序集中。

### 3.3.2 在服务器上复制 Identity Manager 需要的对象

如果 Identity Manager 环境需要多个服务器以运行多个 Identity Manager 驱动程序，则计划应确保在运行这些 Identity Manager 驱动程序的服务器上复制了某些 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 Remote Loader，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具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。

服务器对象是必需的，因为驱动程序使用它为对象生成密钥对。对于 Remote Loader 鉴定来说，它也至关重要。

- ◆ 需要同步驱动程序的该实例的对象。

除非这些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对象。事实上，Identity Manager 驱动程序将同步在服务器上复制的**所有**容器中的对象，除非您创建用于范围过滤的规则以另行指定。

例如，如果需要驱动程序同步所有用户对象，最简单的方法是使用驱动程序的一个实例，该驱动程序位于保存所有用户的主复本或读 / 写复本的服务器上。

但是，许多环境都没有包含所有用户复本的单台服务器。相反，完整用户集分布在多台服务器上。在这种情况下，有三种选择：

- ◆ **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同步相同的用户，您将需要使用范围过滤来定义每个驱动程序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容器。请参见[使用“范围过滤”管理不同服务器上的用户（第 28 页）](#)。
- ◆ **在没有范围过滤的情况下，使用多台服务器上的驱动程序的多个实例：**如果要在不同服务器上运行驱动程序的多个实例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，以使驱动程序能够处理同一 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，如果指定在 eDirectory 中创建用户时驱动程序应使用模板，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容器。  
例如，如果创建了一个名称为“非活动用户”的树枝以保存禁用的用户帐户，则必须使运行驱动程序的服务器上具有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他任何对象（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他对象，则服务器上的这些对象的复本可以是只读复本。

### 3.3.3 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容器。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容器中的用户。

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容器中的对象。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将其复制到单台服务器上，则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，您将需要使用“范围过滤”来定义驱动程序的每个实例应该同步的用户。

---

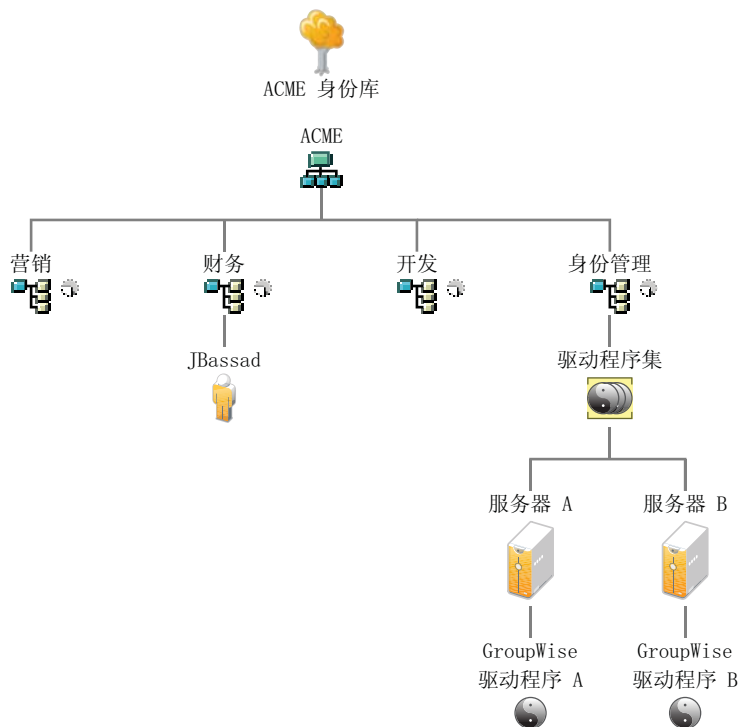
**注释：**即使服务器的复本当前未重叠，也应该使用范围过滤。以后，服务器上可能会添加复本，因而可能无意中产生重叠。如果实施了范围过滤，Identity Manager 驱动程序就不会尝试同步相同的用户，即使以后向服务器添加复本，也是如此。

---

下面给出了如何使用范围过滤的示例：

下图显示了一个 Identity Vault，它带有三个保存用户的容器：市场营销、财务和开发。同时它还显示保存驱动程序集的身份管理容器。其中每个容器都是一个独立的分区。

图 3-4 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，如图 3-5 在第 30 页 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。

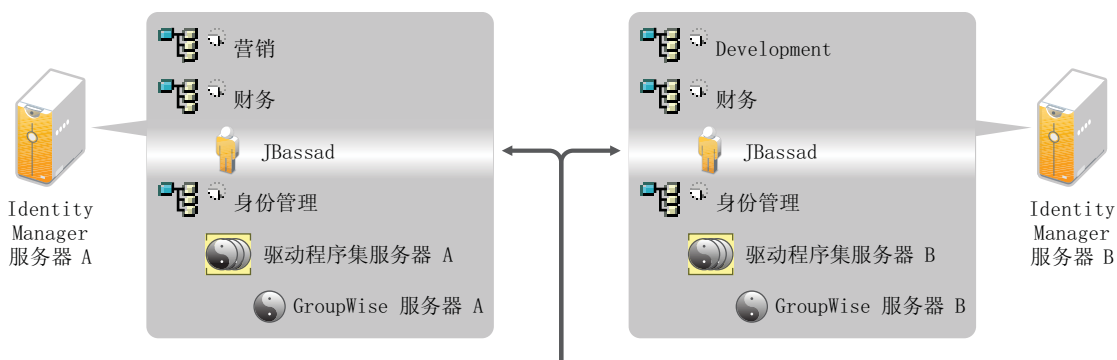
管理员希望通过 GroupWise 驱动程序同步树中的所有用户，但是不希望将这些用户的复本聚合到单台服务器。他选择使用 GroupWise 驱动程序的两个实例，每台服务器使用一个。他在每台 Identity Manager 服务器上安装 Identity Manager，然后设置 GroupWise 驱动程序。

服务器 A 保存“市场营销”和“财务”容器的复本。同时，身份管理容器的复本也在该服务器上，该容器保存服务器 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 保存开发容器和财务容器的复本，同时，身份管理容器的复本也在该服务器上，该容器保存服务器 B 的驱动程序集和服务器 B 的 GroupWise 驱动程序对象。

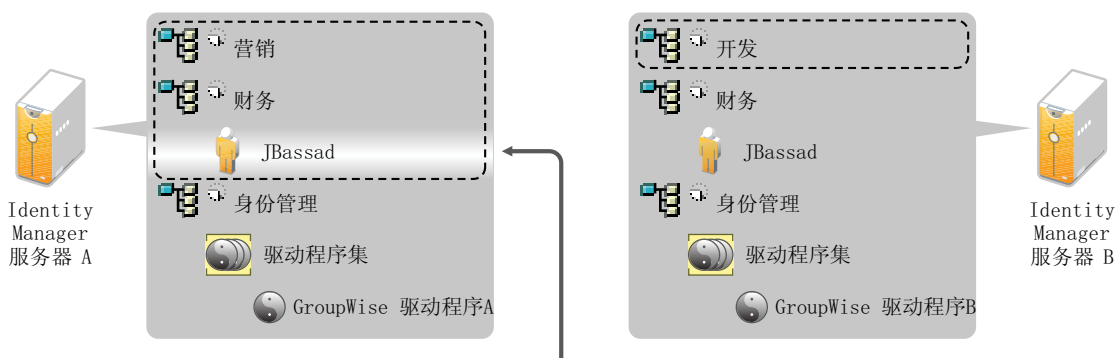
由于服务器 A 和服务器 B 均保存了“财务”容器的复本，因此这两个服务器均保存了“财务”容器中的用户 JBassad。如果不使用范围过滤，GroupWise 驱动程序 A 和 GroupWise 驱动程序 B 都会同步 JBassad。

图 3-5 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同步每个容器的驱动程序，因此它可以防止驱动程序的两个实例管理同一用户。

图 3-6 范围过滤定义同步每个容器的驱动程序



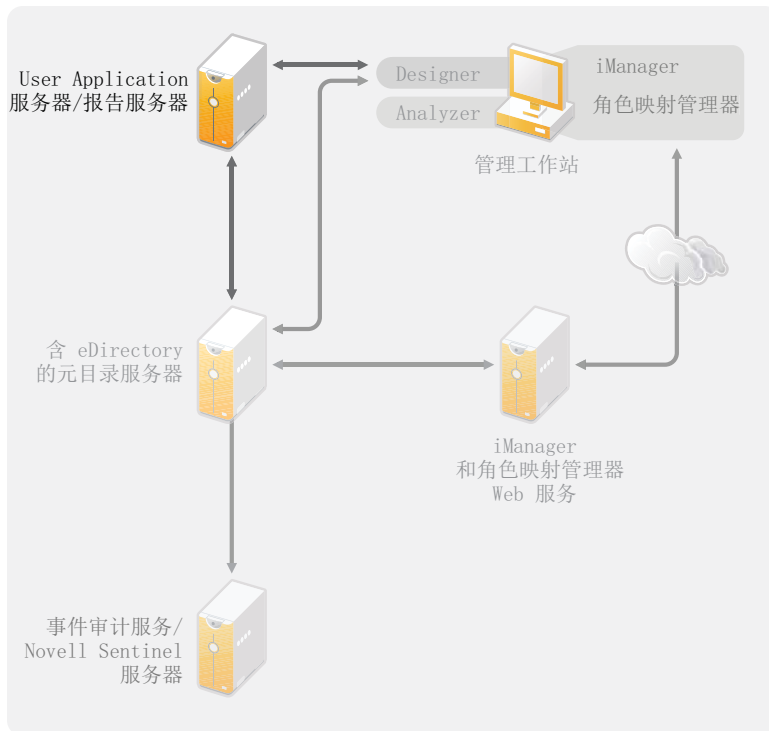
Identity Manager 附带一些预定义的规则。有两个规则可帮助执行范围过滤：“事件转换 — 范围过滤 — 包括子树”和“事件转换 — 范围过滤 — 排除子树”，具体说明请参见《[了解 Identity Manager 4.0.1 的策略](#)》。

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容器中的用户。服务器 A 将同步“市场营销”和“财务”。服务器 B 将同步开发容器。

## 3.4 User Application

User Application 应在自身的服务器上运行，如图 3-7 中所示。您可能需要多个 User Application 服务器。

图 3-7 User Application

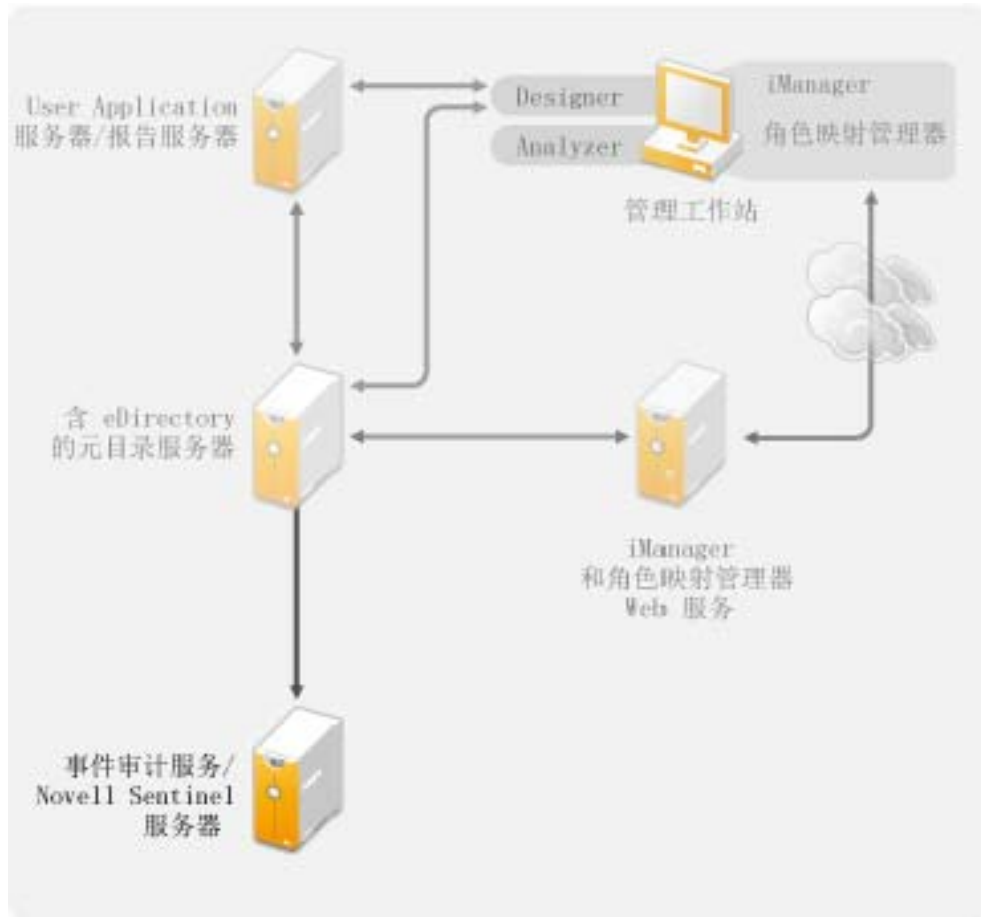


使用《User Application 管理指南》的“性能调优 (<http://www.novell.com/documentation/idmrbpm40/agpro/data/b2gx735.html>)”部分中的信息来确定如何最佳配置 User Application 服务器。

### 3.5 审计和报告准则

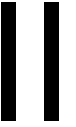
如果需要将审计和报告作为 Identity Manager 解决方案的一部分，则需要实施 Identity Audit 或 Novell Sentinel。事件审计服务或 Sentinel 应在其自身的服务器上运行，如图 3-8 所示。您的解决方案所需的服务器数量取决于环境中驱动程序的数量以及定义进行审计的事件数量。

图 3-8 Sentinel





# 安装



下面的章节包含不使用集成安装程序安装 Identity Manager 系统所需的信息。如果想要简单的安装和配置，则应使用新的集成安装程序，而非分别安装组件。有关集成安装程序的更多信息，请参见《*Identity Manager 4.0.1 集成安装指南*》。

但是，如果需要安装一个或分别安装多个 Identity Manager 组件，请使用这些章节中的信息来完成安装。

- ◆ 第 4 章“基本 Identity Manager 系统核对清单”（第 35 页）
- ◆ 第 5 章“从何处获取 Identity Manager”（第 39 页）
- ◆ 第 6 章“系统要求”（第 43 页）
- ◆ 第 7 章“安装 Identity Manager”（第 53 页）
- ◆ 第 8 章“激活 Novell Identity Manager 产品”（第 67 页）
- ◆ 第 9 章“Identity Manager 查错”（第 71 页）
- ◆ 第 10 章“新功能”（第 77 页）



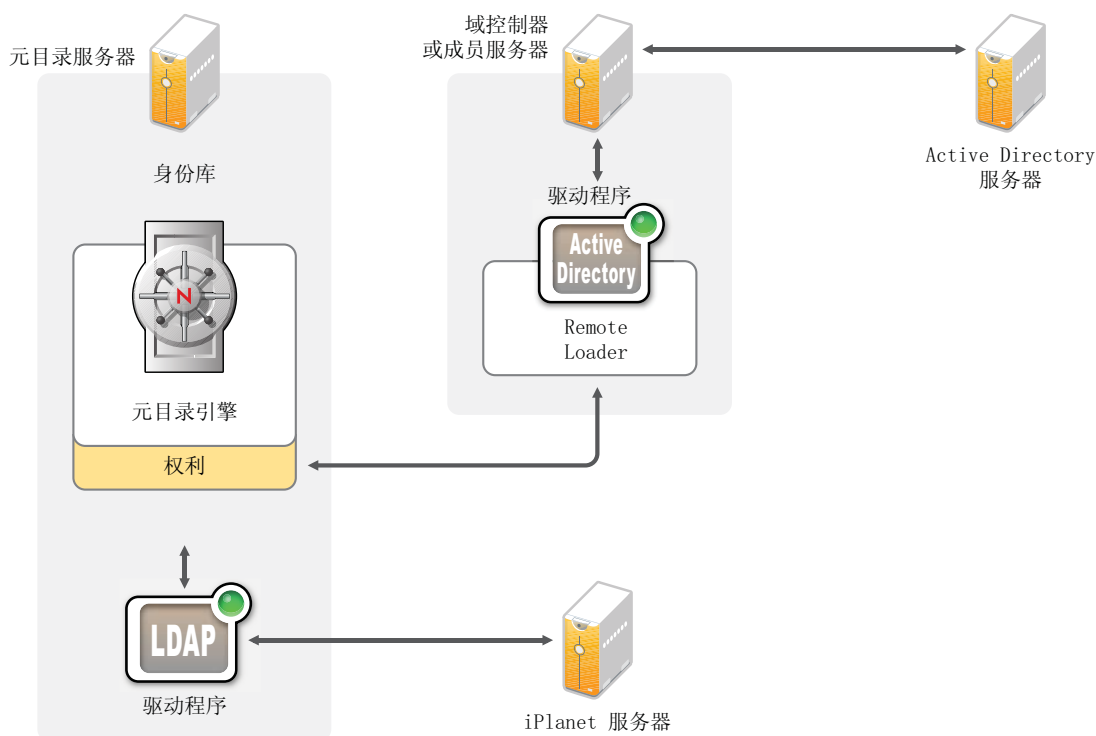
# 基本 Identity Manager 系统核对清单

# 4

有多种方法可配置 Identity Manager 以利用其全部功能。图 4-1 代表了 Identity Manager 的基本配置。该配置向用户提供同步数据。无论如何配置 Identity Manager，都始终从一个基本系统开始。

配置 Identity Manager 系统时，请使用此核对清单来确保所有步骤均已完成。

图 4-1 基本 Identity Manager 系统



- ◆ 第 4.1 节“先决条件”（第 35 页）
- ◆ 第 4.2 节“规划”（第 36 页）
- ◆ 第 4.3 节“安装”（第 36 页）
- ◆ 第 4.4 节“带有 Remote Loader 的驱动程序配置”（第 36 页）
- ◆ 第 4.5 节“不带 Remote Loader 的驱动程序配置”（第 37 页）
- ◆ 第 4.6 节“其他配置”（第 37 页）

## 4.1 先决条件

- 请校验您的系统是否满足第 6 章“系统要求”（第 43 页）中所列的系统要求。

## 4.2 规划

规划是成功实施和部署 Identity Manager 的关键。

- ❑ 创建开发环境。务必具有对 Identity Manager 系统的访问权以验证 Identity Manager 解决方案。您希望在更改生产环境前，先在开发环境中进行所有测试和开发。有关更多信息，请参见第 1 章“建立开发环境”（第 11 页）。
- ❑ 创建用于部署 Identity Manager 的项目计划。项目计划包括定义关键业务流程、创建使这些流程自动化的 Identity Manager 解决方案以及创建技术实施计划。要成功部署 Identity Manager，必须具有项目计划。有关更多信息，请参见第 2 章“创建项目计划”（第 13 页）。
- ❑ 项目计划创建完成后，使用 Analyzer 清理和准备数据以便同步。有关更多信息，请参见《*Analyzer 4.0.1 for Identity Manager 管理指南*》。

## 4.3 安装

- ❑ 安装 Analyzer。有关更多信息，请参见第 7.1 节“安装 Analyzer”（第 53 页）。
- ❑ 安装 Designer。有关更多信息，请参见第 7.2 节“安装 Designer”（第 54 页）。
- ❑ 安装 eDirectory。有关更多信息，请参见第 7.3 节“安装 eDirectory”（第 54 页）。
- ❑ 安装 iManager。有关更多信息，请参见第 7.4 节“安装 iManager”（第 55 页）。
- ❑ 安装元目录服务器和驱动程序。有关更多信息，请参见第 7 章“安装 Identity Manager”（第 53 页）。
- ❑ 激活 Identity Manager。有关更多信息，请参见第 8 章“激活 Novell Identity Manager 产品”（第 67 页）。
- ❑ （可选）设计和创建 Identity Manager 系统的权利。

权利是指针对某个人或组的可应用于多个驱动程序的一组已定义准则。在满足准则后，权利将启动一个事件以授予或撤消对业务资源的访问权。权利增加了控制和自动化资源的授予及撤消的额外级别。

权利的关键优势在于创建和定义业务逻辑，然后将该逻辑应用到多个驱动程序。如果需要更改，可在权利中更改而不必在各个驱动程序中进行更改。

权利通过三个代理实施：

- ◆ 使用权利服务驱动程序的基于角色的权利
- ◆ 工作流程
- ◆ 基于角色的供应模块

有关权利的更多信息，请参见《*Identity Manager 4.0.1 权利指南*》。

## 4.4 带有 Remote Loader 的驱动程序配置

通过 Remote Loader 可将信息同步到已连接系统，而不必在已连接系统上安装 eDirectory。Remote Loader 将信息同步到元目录服务器，而后者存储身份库中的数据。Identity Manager 使用 eDirectory 作为身份库。

- ❑ 在与已连接系统通讯的计算机上安装 Remote Loader。Remote Loader 在已连接系统和元目录服务器之间通讯，使 Identity Manager 能够与未安装 eDirectory 的计算机通讯。有关更多信息，请参见《*Identity Manager 4.0.1 Remote Loader 指南*》中的“安装 Remote Loader”。

- ❑ 为驱动程序配置 Remote Loader。可定义 Remote Loader 的特定实例与特定驱动程序通讯。有关更多信息，请参见 《*Identity Manager 4.0.1 Remote Loader 指南*》中的“配置 Remote Loader”。
- ❑ 配置要与 Remote Loader 通讯的驱动程序。每个驱动程序均有一个驱动程序指南。有关您的驱动程序的特定信息，请参见 *Identity Manager 4.0.1 驱动程序文档网站* (<http://www.novell.com/documentation/idm401drivers/>)。
- ❑ (可选) 启用有关驱动程序的权利。验证您已使执行权利的正确策略就位。有关更多信息，请参见 《*Identity Manager 4.0.1 权利指南*》。
- ❑ 对环境中具有的每个驱动程序重复这些步骤。

## 4.5 不带 Remote Loader 的驱动程序配置

- ❑ 创建并配置驱动程序。每个驱动程序均有一个驱动程序指南。有关您的驱动程序的特定信息，请参见 *Identity Manager 4.0.1 驱动程序文档网站* (<http://www.novell.com/documentation/idm401drivers/>)。
- ❑ (可选) 启用有关驱动程序的权利。验证您已使执行权利的正确策略就位。有关更多信息，请参见 《*Identity Manager 4.0.1 权利指南*》。
- ❑ 对环境中具有的每个驱动程序重复这些步骤。

## 4.6 其他配置

安装和配置基本 Identity Manager 系统后，即可添加以下功能：

- ❑ **口令管理：**如果想要使用 Identity Manager 管理口令，则还需要进行一些配置。使用 《*Identity Manager 4.0.1 口令管理指南*》中的“口令管理核对清单”校验是否已完成所有配置步骤。
- ❑ **角色管理：**如果想要从一个位置管理不同系统中的角色，Identity Manager 包含一种称为角色映射管理器的工具。它可以将业务角色从一个系统映射到另一个系统，而无需知道 IT 基础设施。有关更多信息，请参见 《*Identity Manager 角色映射管理器 4.0.1 安装和配置指南*》。
- ❑ **Roles Based Provisioning：**如果想要将 Roles Based Provisioning 添加到 Identity Manager 解决方案中，请使用 《*Identity Manager Roles Based Provisioning Module 4.0.1 User Application: 安装指南*》中的“安装核对清单”校验是否已完成所有配置步骤。
- ❑ **审计和报告：**通过向 Identity Manager 解决方案中添加审计和报告，可以证明您的业务策略符合公司的策略。可将身份报告模块或 Novell Sentinel 添加到 Identity Manager 解决方案中以进行审计和报告。有关身份报告模块的更多信息，请参见 《*身份报告模块指南*》。有关 Novell Sentinel 的更多信息，请参见 《*Novell Sentinel 的 Identity Manager 4.0.1 报告指南*》。



# 从何处获取 Identity Manager

Identity Manager 4.0.1 提供了 Advanced Edition 和 Standard Edition。每种版本都有单独的 ISO。Identity Manager 4.0.1 Advanced Edition 包括用于企业级用户供应的全部功能。为满足不同的客户需求，Identity Manager Standard Edition 包括 Identity Manager Advanced Edition 的部分功能。Standard Edition 继续提供 Identity Manager 先前版本中的所有功能。有关 Identity Manager 4.0.1 Advanced Edition 和 Standard Edition 所提供功能的更多信息，请参见《[Identity Manager 4.0.1 概述指南](#)》中的“[Identity Manager 4.0.1 功能](#)”。

您可以下载 Identity Manager 的评估版，并免费使用 90 天。但是，必须在安装后的 90 天内激活 Identity Manager 组件，否则它们将关闭。在这 90 天内或之后的任何时间，您都可以选择购买产品许可证并激活 Identity Manager。有关更多信息，请参见第 8 章“[激活 Novell Identity Manager 产品](#)”（第 67 页）。

要下载 Identity Manager 及其服务：

- 1 转至 [Novell 下载网站 \(http://download.novell.com\)](http://download.novell.com)。
- 2 在 [产品或技术菜单](#)中，选择 *Novell Identity Manager*，然后单击 [搜索](#)。
- 3 在 Novell Identity Manager 下载页上，单击所需文件旁边的 *Download*（下载）按钮。表 5-1 包含每个文件的说明。

您可以根据需要选择合适的 ISO。每个 ISO 都包含产品的 32 位和 64 位版本。

---

**重要：**要从 Identity Manager Advanced Edition 切换到 Standard Edition，请卸载 Advanced Edition，然后从 Identity Manager 媒体安装 Standard Edition ISO。要从 Standard Edition 升级到 Advanced Edition，请使用 Identity Manager Advanced Edition ISO。您需要应用正确的激活才能升级到 Advanced Edition。有关从 Standard Edition 升级到 Advanced Edition 的更多信息，请参见《[Identity Manager 4.0.1 升级和迁移指南](#)》。

---

- 4 遵循屏幕提示，将该文件下载到计算机上的某个目录中。
- 5 重复 [步骤 3](#)，直到下载完需要的所有文件。
- 6 将下载的 .iso 文件作为卷装入，或者使用 .iso 文件创建软件的 DVD。如果尚未校验刻录的媒体是否有效，则可以使用 [媒体检查](#)选项进行检查。

---

**注释：**Linux ISO 文件由于文件较大应该复制到双层 DVD 上。

---

表 5-1 Identity Manager ISO 映像

ISO	平台	说明
Identity_Manager_4.0.1_Windows_Advanced.iso	Windows	包含元目录服务器、Designer、iManager、角色映射管理器、Analyzer、身份报告模块及 Roles Based Provisioning Module 的 DVD 映像。
Identity_Manager_4.0.1_Windows_Standard.iso	Windows	包含元目录服务器、Designer、iManager、Analyzer、身份报告模块及 Roles Based Provisioning Module 的 DVD 映像。

ISO	平台	说明
Identity_Manager_4.0.1_Linux_Advanced.iso	Linux	包含元目录服务器、Designer、iManager、角色映射管理器、Analyzer、身份报告模块及 Roles Based Provisioning Module 的 DVD 映像。
Identity_Manager_4.0.1_Linux_Standard.iso	Linux	包含元目录服务器、Designer、iManager、Analyzer、身份报告模块及 Roles Based Provisioning Module 的 DVD 映像。
Identity_Manager_4.0.1_Solaris_Advanced.iso	Solaris	包含元目录服务器的 DVD 映像。其他组件在 Solaris 平台上不受支持。
Identity_Manager_4.0.1_Solaris_Standard.iso	Solaris	包含元目录服务器的 DVD 映像。其他组件在 Solaris 平台上不受支持。

购买 Identity Manager 包括激活服务驱动程序及若干通用驱动程序。

- ◆ **服务驱动程序：**下面列出了激活元目录服务器时激活的服务驱动程序：
  - ◆ 数据收集服务
  - ◆ 权利服务
  - ◆ ID 提供程序
  - ◆ 回写服务
  - ◆ 受管系统网关
  - ◆ 手动任务服务
  - ◆ 空服务
  - ◆ Role and Resource Service
  - ◆ User Application
  - ◆ WorkOrder
- ◆ **通用驱动程序：**下面列出了激活元目录服务器时激活的通用驱动程序：
  - ◆ Active Directory
  - ◆ ADAM
  - ◆ eDirectory
  - ◆ GroupWise
  - ◆ LDAP
  - ◆ Lotus Notes

所有其他 Identity Manager 驱动程序的激活都必须单独购买。驱动程序的激活是作为 Identity Manager 集成模块出售的。一个 Identity Manager 集成模块可以包含一个或多个驱动程序。您每购买一个 Identity Manager 集成模块，就会收到一个产品激活身份凭证。有关更多信息，请参见 [Identity Manager 驱动程序产品网页 \(http://www.novell.com/products/identitymanager/drivers/\)](http://www.novell.com/products/identitymanager/drivers/)。

Identity Manager Advanced Edition 和 Standard Edition 有各自的激活。有关详细信息，请参见 [激活 Novell Identity Manager 产品 \(第 67 页\)](#)。不支持从 Identity Manager Advanced Edition 切换到 Standard Edition。要使用 Identity Manager Standard Edition，需要从 Identity Manager 媒体安装。



购买 Identity Manager 时即包括了 User Application Roles Based Provisioning Module。它添加了一个强大的基于角色的批准工作流程来管理用户身份。

购买的 Identity Manager 中还包括许多工具，用来帮助设计、创建和管理 Identity Manager 解决方案：

- ◆ Analyzer
- ◆ Designer
- ◆ iManager
- ◆ 角色映射管理器

---

**注释：** Identity Manager 4.0.1 Standard Edition 没有角色映射管理器。

---

身份报告模块是 Identity Manager 的又一组件，用来审计和创建有关 Identity Manager 解决方案的报告。您可以使用这些报告来帮助满足企业的合规性法规。

有关 Identity Manager 组件的更多信息，请参见 《[Identity Manager 4.0.1 概述指南](#)》。



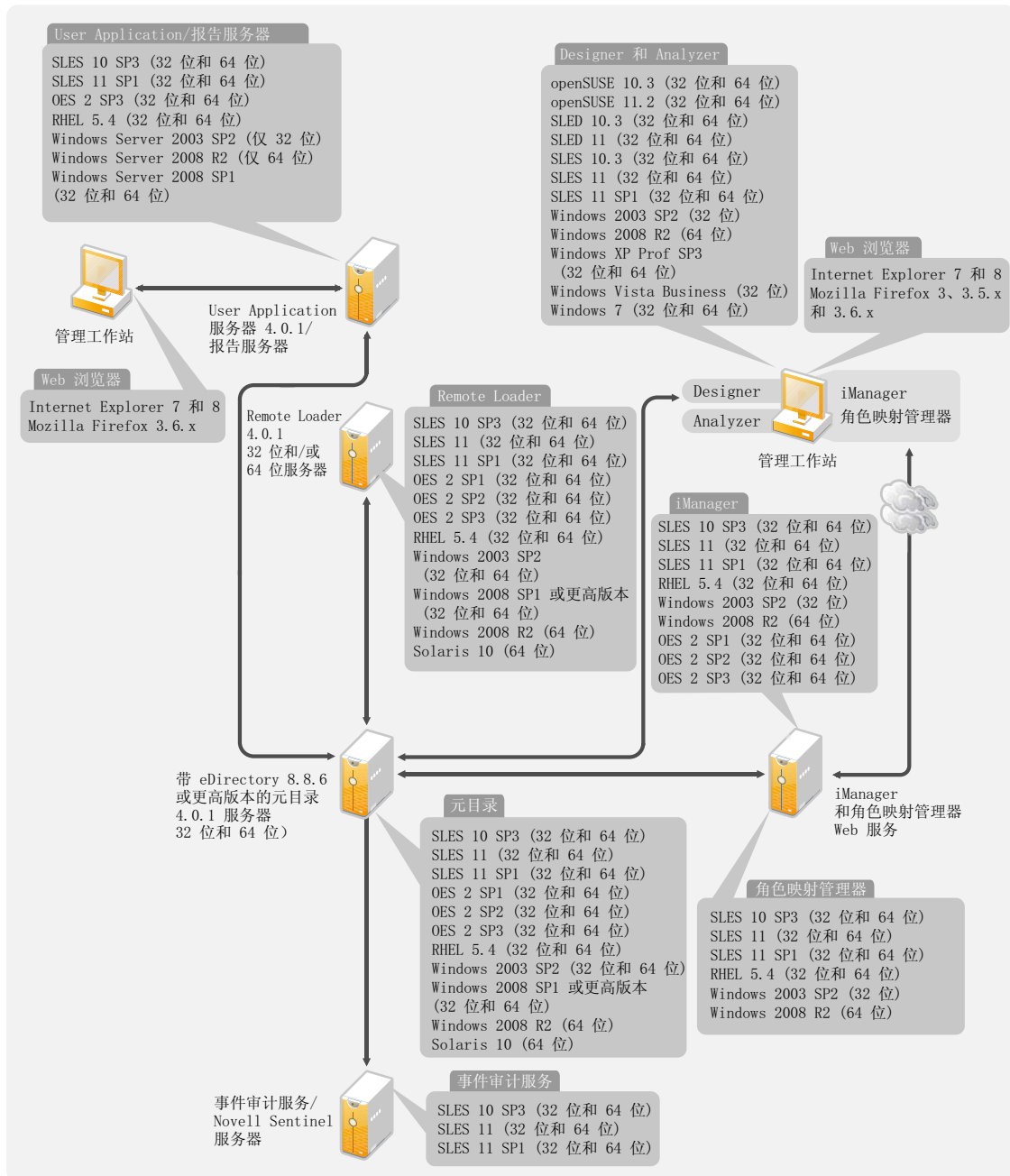
# 系统要求

# 6

Novell Identity Manager 的组件可安装在多个系统和平台上。

图 6-1 显示了支持的平台和系统。

图 6-1 Identity Manager 组件的系统要求



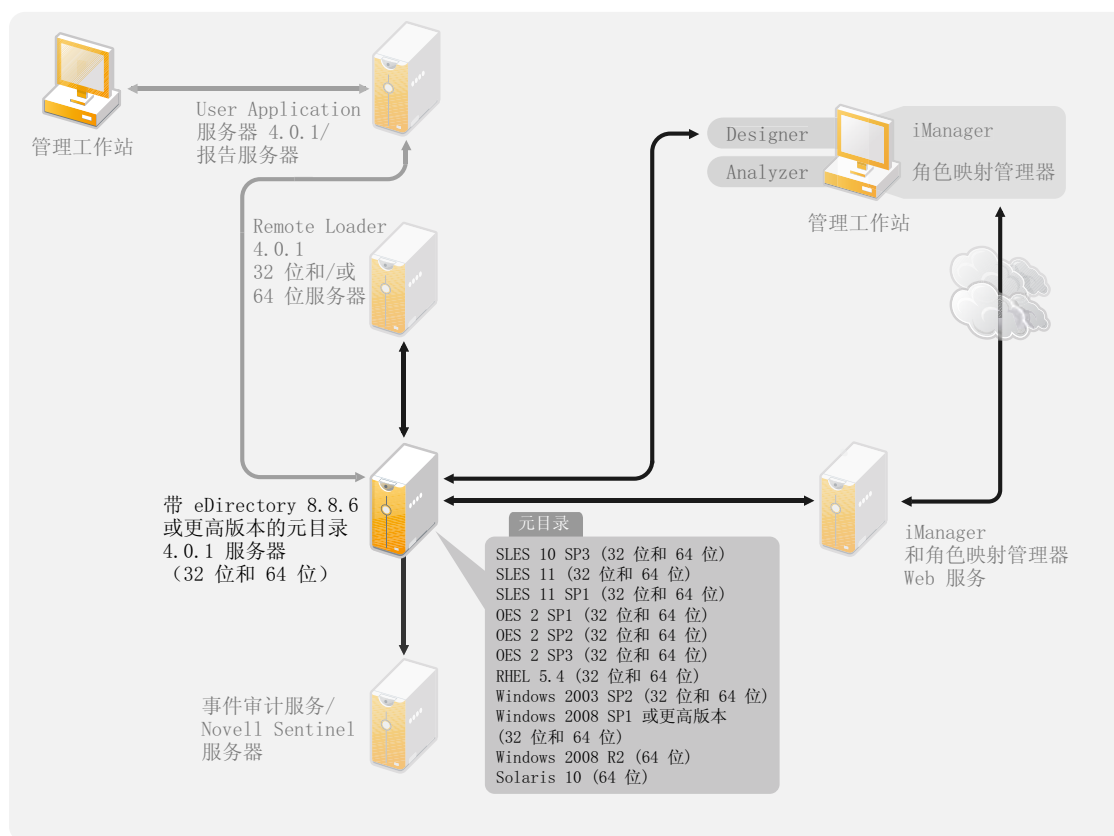
根据系统配置的不同，可能需要多次运行 Identity Manager 安装程序，才能在相应的系统上安装 Identity Manager 组件。

- ◆ 第 6.1 节“eDirectory 和 iManager”（第 44 页）
- ◆ 第 6.2 节“元目录服务器”（第 45 页）
- ◆ 第 6.3 节“Remote Loader”（第 47 页）
- ◆ 第 6.4 节“User Application”（第 48 页）
- ◆ 第 6.5 节“审计和报告”（第 49 页）
- ◆ 第 6.6 节“工作站”（第 49 页）
- ◆ 第 6.7 节“资源要求”（第 51 页）

## 6.1 eDirectory 和 iManager

Identity Manager 要求安装 eDirectory 和 iManager。这些产品是 Identity Manager 的基础，它们包括在 Identity Manager Advanced Edition ISO 映像中。图 6-2 说明了这些组件。

图 6-2 Identity Manager 的基本产品



您需要这些产品的以下版本：

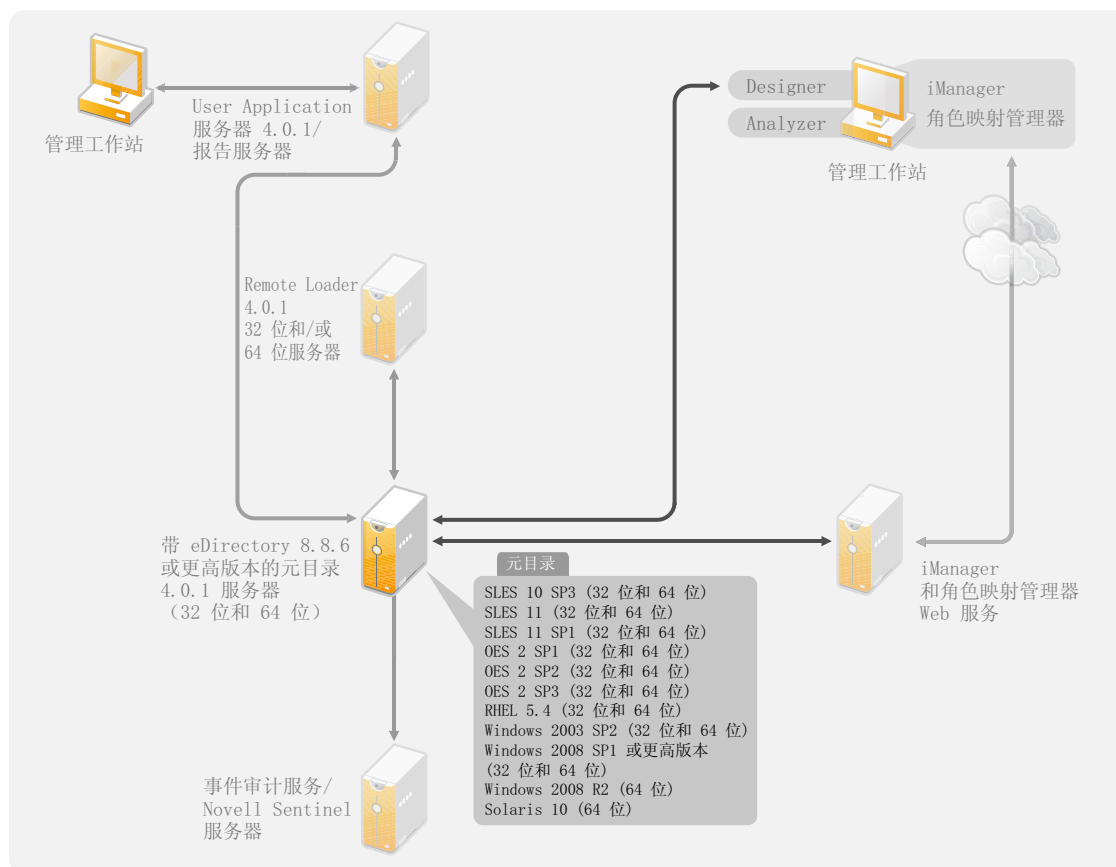
- ◆ eDirectory 8.8.6 或更高版本（32 位或 64 位）
- ◆ iManager 2.7.4

有关 eDirectory 系统要求，请参见《[Novell eDirectory 8.8 安装指南](http://www.novell.com/documentation/edir88/index.html)》。有关 iManager 的系统要求，请参见《[iManager 2.7 安装指南](http://www.novell.com/documentation/imanager27/index.html)》中的[安装 iManager](http://www.novell.com/documentation/imanager27/imanager_install_274/data/alw39eb.html)一节。

## 6.2 元目录服务器

元目录服务器处理来自驱动程序的事件，无论这些驱动程序是否使用 Remote Loader 配置的。有关支持的操作系统的列表，请参见图 6-3。

图 6-3 元目录服务器支持的操作系统



在安装元目录服务器过程中，安装程序将检测已安装的 eDirectory 版本。

**注释：**必须已安装 eDirectory 8.8.6 或更高版本（32 位或 64 位），否则安装程序无法继续。

- ◆ 第 6.2.1 节“支持的处理器”（第 45 页）
- ◆ 第 6.2.2 节“服务器操作系统”（第 46 页）

### 6.2.1 支持的处理器

此处列出的处理器是在 Identity Manager 测试过程中使用的。SPARC 处理器用于 Solaris 测试。

Linux（Red Hat 和 SUSE Linux Enterprise Server）和 Windows 操作系统支持的 32 位处理器包括：

- ◆ Intel x86-32
- ◆ AMD x86-32

Linux（Red Hat 和 SUSE Linux Enterprise Server）和 Windows 操作系统支持的 64 位处理器包括：

- ◆ Intel EM64T
- ◆ AMD Athlon64
- ◆ AMD Opteron

所有操作系统都应有最新的支持包。

## 6.2.2 服务器操作系统

可在 64 位操作系统上将元目录服务器作为 32 位应用程序安装。表 6-1 包含可用于运行元目录服务器的受支持服务器操作系统列表。

表 6-1 支持的服务器操作系统

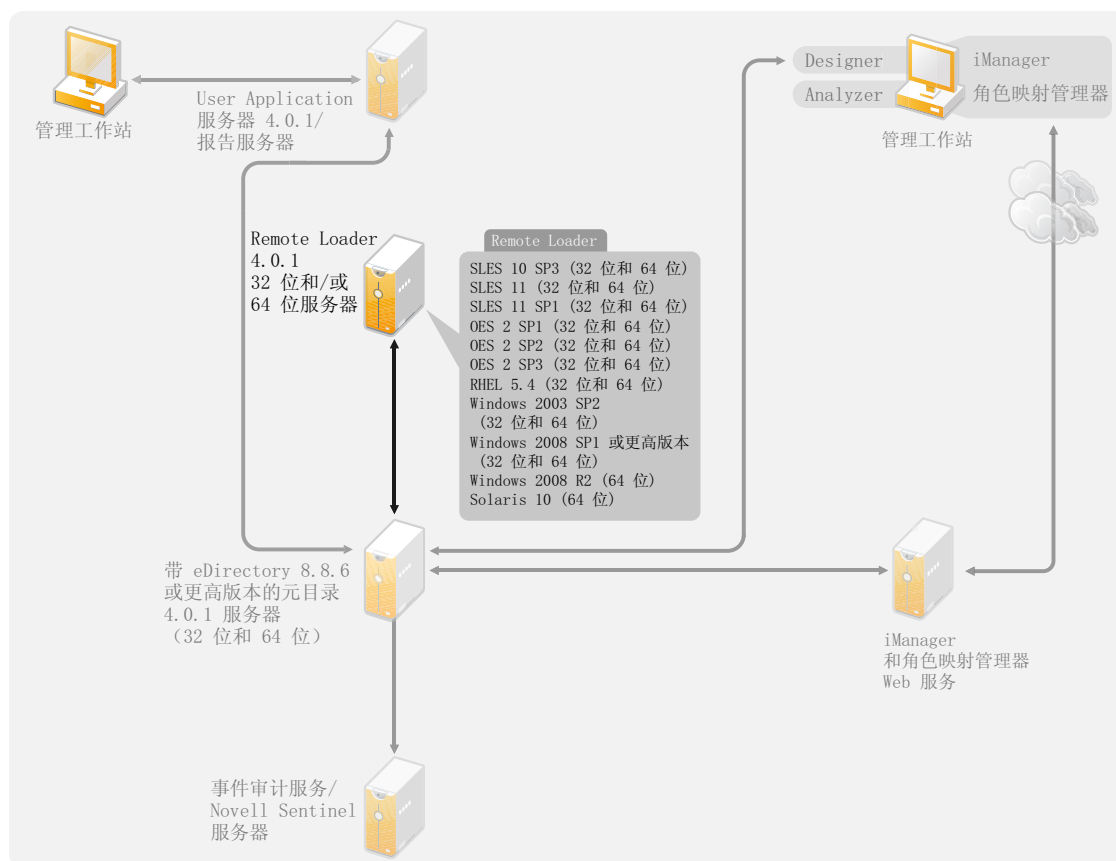
服务器操作系统版本	注释
Windows Server 2003 SP2 或更高版本（32 位）	元目录服务器仅在 32 位模式下运行。
Windows 2008 或更高版本支持包（32 位和 64 位）	元目录服务器在 32 位或 64 位模式下运行。
Windows Server 2008 R2（64 位）	元目录服务器仅在 64 位模式下运行。
Red Hat 5.4（32 位和 64 位）	元目录服务器在 32 位或 64 位模式中运行。Novell 建议您在安装 Identity Manager 前，先通过制造商的自动更新工具应用最新的 OS 增补程序。
SUSE Linux Enterprise Server 10 SP3 或更高版本的支持包（32 位和 64 位）	元目录服务器在 32 位或 64 位模式中运行。Novell 建议您在安装 Identity Manager 前，先通过制造商的自动更新工具应用最新的 OS 增补程序。
SUSE Linux Enterprise Server 11（32 位和 64 位）	元目录服务器在 32 位或 64 位模式中运行。Novell 建议您在安装 Identity Manager 前，先通过制造商的自动更新工具应用最新的 OS 增补程序。
SUSE Linux Enterprise Server 11 SP1（32 位和 64 位）	元目录服务器在 32 位或 64 位模式中运行。Novell 建议您在安装 Identity Manager 前，先通过制造商的自动更新工具应用最新的 OS 增补程序。
OES 2 SP1（32 位和 64 位）	元目录服务器在 32 位和 64 位模式下运行。
OES 2 SP2（32 位和 64 位）	元目录服务器在 32 位和 64 位模式下运行。
OES 2 SP3（32 位和 64 位）	元目录服务器在 32 位和 64 位模式下运行。
Solaris 10（64 位）	元目录服务器仅在 64 位模式下运行。

服务器操作系统版本	注释
Xen	当 Xen 虚拟机在半虚拟化模式下将 SLES 10/SLES 11 作为虚拟机运行时，支持 Xen。
VMware ESX	元目录服务器在 32 位或 64 位模式下运行。
Red Hat Enterprise Linux 5 虚拟化	元目录服务器在 32 位或 64 位模式下运行。
Windows Server 2008 R2 虚拟化（带 Hyper-V）	元目录服务器在 32 位或 64 位模式下运行。

## 6.3 Remote Loader

Remote Loader 使您可灵活配置 Identity Manager 解决方案。它同时支持 32 位和 64 位。默认情况下，安装程序会检测操作系统的版本，然后安装相应版本的 Remote Loader。

图 6-4 Remote Loader 支持的操作系统的



如果已在 64 位操作系统上将元目录服务器作为 32 位应用程序安装，则可以在同一计算机上同时安装 32 位和 64 位 Remote Loader。

表 6-2 列出了 Remote Loader 支持的操作系统的。

表 6-2 Remote Loader 支持的操作系统

服务器操作系统版本	注释
Windows Server 2003 SP2 (32 位和 64 位)	Remote Loader 在 32 位和 64 位模式下运行。
Windows Server 2008 或更高版本支持包 (32 位和 64 位)	Remote Loader 在 32 位和 64 位模式下运行。
Windows Server 2008 R2 (64 位)	Remote Loader 仅在 64 位模式下运行。
Red Hat 5.4 (32 位和 64 位)	Remote Loader 在 32 位和 64 位模式下运行。Novell 建议您在安装 Identity Manager 前, 先通过制造商的自动更新工具应用最新的 OS 增补程序。
SUSE Linux Enterprise Server 10 SP3 (32 位和 64 位)	Remote Loader 在 32 位和 64 位模式下运行。Novell 建议您在安装 Identity Manager 前, 先通过制造商的自动更新工具应用最新的 OS 增补程序。
SUSE Linux Enterprise Server 11 (32 位和 64 位)	Remote Loader 在 32 位和 64 位模式下运行。Novell 建议您在安装 Identity Manager 前, 先通过制造商的自动更新工具应用最新的 OS 增补程序。
SUSE Linux Enterprise Server 11 SP1 (32 位和 64 位)	Remote Loader 在 32 位和 64 位模式下运行。Novell 建议您在安装 Identity Manager 前, 先通过制造商的自动更新工具应用最新的 OS 增补程序。
OES 2 SP1 (32 位和 64 位)	Remote Loader 在 32 位和 64 位模式下运行。
OES 2 SP2 (32 位和 64 位)	Remote Loader 在 32 位和 64 位模式下运行。
OES 2 SP3 (32 位和 64 位)	Remote Loader 在 32 位和 64 位模式下运行。
Solaris 10 (64 位)	Remote Loader 仅在 64 位模式下运行。
Xen	当 Xen 虚拟机在半虚拟化模式下将 SLES 10/ SLES 11 作为虚拟机运行时, 支持 Xen。
VMware ESX (64 位)	Remote Loader 在 32 位和 64 位模式下运行。
Red Hat Enterprise Linux 5 虚拟化 (64 位)	Remote Loader 在 32 位和 64 位模式下运行。
Windows Server 2008 R2 虚拟化 (带 Hyper-V, 64 位)	Remote Loader 在 32 位和 64 位模式下运行。

Java Remote Loader 在本地 Remote Loader 不可用的平台上受支持。 .NET Remote Loader 在 .NET 平台版本 2 上受支持。

## 6.4 User Application

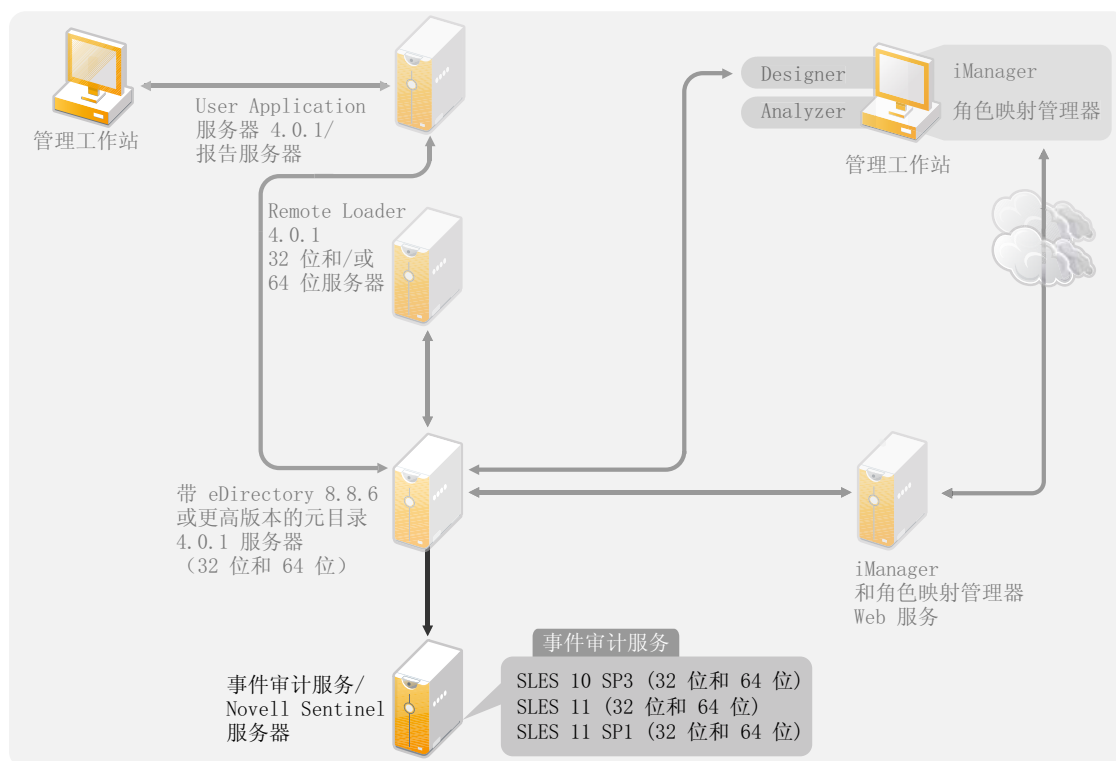
有关 User Application 系统要求, 请参见 [《Identity Manager Roles Based Provisioning Module 4.0.1 User Application: 安装指南》](#) 中的“系统要求”一节。Roles Based Provisioning Module 4.0.1 使用 JBoss 5.1 作为应用程序服务器, 使用 PostgreSQL 8.4.3 作为数据库。



## 6.5 审计和报告

身份报告模块和 Novell Sentinel 是用于收集有关 Identity Manager 的审计和报告信息的两种不同工具。图 6-5 列出了 Identity Manager 4.0.1 支持的 Sentinel 版本。

图 6-5 Sentinel



身份报告模块是 Identity Manager Advanced Edition 的组件。Novell Sentinel 是一个可选组件，您可以将其添加到 Identity Manager 系统中，但是 Sentinel 不随 Identity Manager 提供。

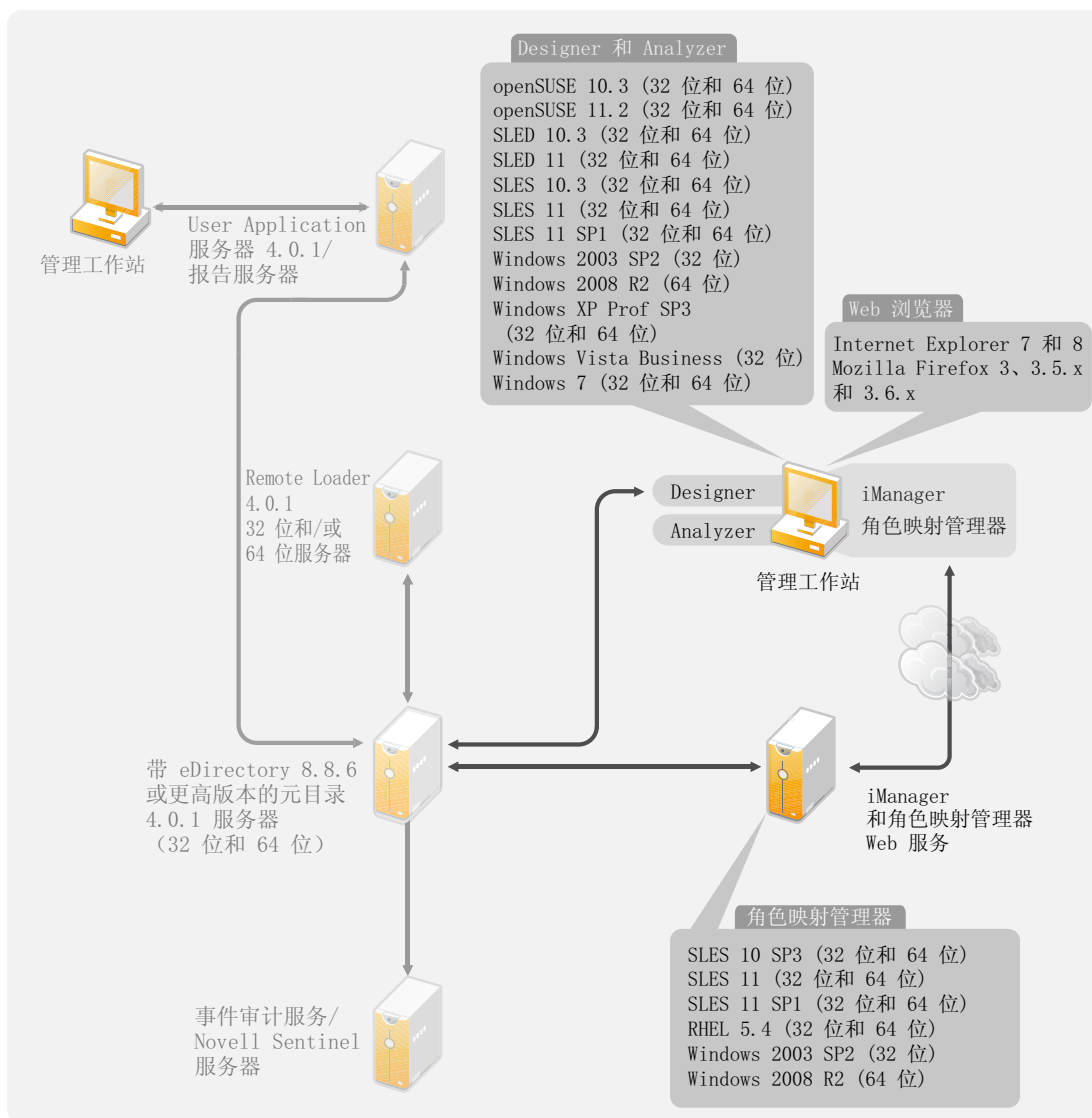
通过添加审计和报告，您可满足许多公司必须遵守的合规性标准。您可以为需要跟踪的任何事件创建审计追踪，也可以生成报告以满足公司的审计标准。

有关身份报告模块的系统要求和配置信息，请参见《[身份报告模块指南](#)》中的“系统要求”一节。有关配备了 Identity Manager 的 Sentinel 的配置信息，请参见《[Novell Sentinel 的 Identity Manager 4.0.1 报告指南](#)》。有关 Novell Sentinel 的系统要求信息，请参见《[Novell Sentinel 安装指南](#) (<http://www.novell.com/documentation/sentinel6/index.html>)》中的“支持的平台和最佳实践”一章。

## 6.6 工作站

工作站用于访问 Designer、iManager、角色映射管理器或 User Application 管理网页。图 6-6 列出了 Identity Manager 4.0.1 支持的工作站的不同组件。

图 6-6 工作站支持的组件



有三种不同项目可影响工作站：

- ◆ 第 6.6.1 节“工作站平台”（第 50 页）
- ◆ 第 6.6.2 节“Web 浏览器”（第 51 页）

## 6.6.1 工作站平台

表 6-3 包含 Designer 和 iManager 支持的工作站平台列表。

有关系统要求信息，请参考各个组件文档。

- ◆ **iManager:** 请参见《Novell iManager 2.7 安装指南》中的安装 iManager ([http://www.novell.com/documentation/imanager27/imanager\\_install\\_274/data/alw39eb.html](http://www.novell.com/documentation/imanager27/imanager_install_274/data/alw39eb.html)) 一节。
- ◆ **Designer:** 请参见《Designer 4.0.1 for Identity Manager 4.0.1 管理指南》中的“系统要求”一节。

表 6-3 支持的工作站平台

平台	细节
Windows 7 (32 位和 64 位)	支持 32 位和 64 位版本。
Windows Vista (32 位)	仅支持 32 位版本。
Windows XP Professional SP3 (32 位和 64 位)	支持 32 位和 64 位版本。
Windows 2003 SP2 (32 位)	仅支持 32 位版本。
Windows 2008 R2 (64 位)	仅支持 64 位 Business Edition。
openSUSE 10.3 (32 位和 64 位)	通过自动更新工具应用最新增补程序。
openSUSE 11.2 (32 位和 64 位)	通过自动更新工具应用最新增补程序。
SUSE Linux Enterprise Desktop 10 SP3 (32 位和 64 位)	通过自动更新工具应用最新增补程序。
SUSE Linux Enterprise Desktop 11 (32 位和 64 位)	通过自动更新工具应用最新增补程序。
SUSE Linux Enterprise Server 10 SP3 (32 位和 64 位)	通过自动更新工具应用最新增补程序。
SUSE Linux Enterprise Server 11 (32 位和 64 位)	通过自动更新工具应用最新增补程序。
SUSE Linux Enterprise Server 11 SP1 (32 位和 64 位)	通过自动更新工具应用最新增补程序。

## 6.6.2 Web 浏览器

iManager 运行管理 Identity Manager 所需的所有插件。角色映射管理器可以在不同系统间映射业务角色，而无需知道 IT 基础设施。这两个应用程序都通过 Web 浏览器进行访问。

iManager 和角色映射管理器支持的 Web 浏览器包括：

- ◆ Internet Explorer 7 和 8
- ◆ Mozilla Firefox 3、3.5.x 和 3.6.x

有关角色映射管理器的系统要求列表，请参见《[Identity Manager 角色映射管理器 4.0.1 安装和配置指南](#)》中的“系统要求”部分。

## 6.7 资源要求

表 6-4 Identity Manager 资源要求

Identity Manager 组件	最低要求
元目录服务器	2048 MB
Remote Loader	256 MB
驱动程序	200 MB

---

Identity Manager 组件	最低要求
iManager 插件	80 MB

---

# 安装 Identity Manager

# 7

Identity Manager 包含一个集成安装程序，它简化了安装过程，可同时安装和配置所有组件。如果是首次安装 Identity Manager 系统，请使用集成安装程序。有关更多信息，请参见《[Identity Manager 4.0.1 集成安装指南](#)》。

如果具有 Identity Manager 的相关经验，想要分别安装各个项目，则 Identity Manager 对不同组件都有独立的安装程序。

务必在 Identity Manager 实施的规划阶段安装和使用 Analyzer 和 Designer。有关更多信息，请参见第 2 章“创建项目计划”（第 13 页）。

按所列顺序安装组件。有关不同组件的说明，请参见《[Identity Manager 4.0.1 概述指南](#)》。

- ◆ 第 7.1 节“安装 Analyzer”（第 53 页）
- ◆ 第 7.2 节“安装 Designer”（第 54 页）
- ◆ 第 7.3 节“安装 eDirectory”（第 54 页）
- ◆ 第 7.4 节“安装 iManager”（第 55 页）
- ◆ 第 7.5 节“安装元目录服务器”（第 55 页）
- ◆ 第 7.6 节“安装 Remote Loader”（第 58 页）
- ◆ 第 7.7 节“安装驱动程序文件”（第 63 页）
- ◆ 第 7.8 节“安装 Roles Based Provisioning Module”（第 64 页）
- ◆ 第 7.9 节“安装自定义驱动程序”（第 64 页）
- ◆ 第 7.10 节“安装角色映射管理器”（第 64 页）
- ◆ 第 7.11 节“安装身份报告模块或 Sentinel”（第 65 页）

## 7.1 安装 Analyzer

Analyzer 是一款基于工作站的工具，它可以分析、清理和准备数据以便与 Identity Manager 同步。您应安装 Analyzer 并在 Identity Manager 实施的整个规划部分始终使用 Analyzer。有关规划的更多信息，请参见第 I 部分“规划”（第 9 页）。

- 1 请校验您的工作站的操作系统是否受支持。  
有关更多信息，请参见第 6.6 节“工作站”（第 49 页）。
- 2 请确保您已从 Novell 下载网站下载了必需的 Identity Manager 文件。有关更多信息，请参见第 5 章“从何处获取 Identity Manager”（第 39 页）。
- 3 通过执行适用于您的工作站平台的正确程序来启动安装。

**Linux:** IDM4.0.1\_Lin/products/Analyzer/install

要执行二进制文件，请输入 `./install`。

**Windows:** IDM4.0.1\_Win/products/Analyzer/install.exe

- 4 使用以下信息完成安装：

**安装位置:** 指定在工作站上安装 Analyzer 的位置。

**创建快捷方式并选择语言：**选择是否要在桌面上创建 Analyzer 快捷方式，及选择要用于安装 Analyzer 的语言。

现在，Analyzer 已安装。首次起动 Analyzer 时，系统会提示您激活。只有在激活后才能使用 Analyzer。有关更多信息，请参见第 8 章“激活 Novell Identity Manager 产品”（第 67 页）。

## 7.2 安装 Designer

Designer 是一个基于工作站的工具，可用于设计您的 Identity Manager 解决方案。您应安装 Designer 并在 Identity Manager 实施的整个规划部分始终使用 Designer。有关规划的更多信息，请参见第 I 部分“规划”（第 9 页）。

- 1 验证是否支持您的工作站的操作系统。为了使 Designer 正常运行，请安装 32 位 NCI 包。如果是在 64 位系统上安装 Designer，请确保在安装 Designer 前已安装 libgthread-2.0-0-32bit-2.17.2+2.17.3+20080708+r7171-3.1.x86\_64.rpm 兼容库。有关更多信息，请参见第 6.6 节“工作站”（第 49 页）及《*Designer 4.0.1 for Identity Manager 4.0.1 管理指南*》。
- 2 请确保您已从 Novell 下载网站下载了必需的 Identity Manager 文件。有关更多信息，请参见第 5 章“从何处获取 Identity Manager”（第 39 页）。
- 3 通过执行适用于您的工作站平台的正确程序来启动安装。

**Linux:** IDM4.0.1\_Lin/products/Designer/install

要执行二进制文件，请输入 `./install`。

**Windows:** IDM4.0.1\_Win:\products\Designer\install.exe

- 4 使用以下信息完成安装：

**安装文件夹：**指定在工作站上安装 Designer 的位置。

**创建快捷方式：**选择是否将快捷方式放置在桌面上和桌面菜单中。

在安装 Designer 前，请确保已安装此包。您可以使用 YaST 检查依赖性和已安装的包。有关更多信息，请参考《*Designer 4.0.1 for Identity Manager 4.0.1 管理指南*》。

## 7.3 安装 eDirectory

请确保您已从 Novell 下载网站下载了必需的 Identity Manager 文件。有关更多信息，请参见第 5 章“从何处获取 Identity Manager”（第 39 页）。

Identity Manager 媒体上提供了 eDirectory 8.8.6。对于 32 位和 64 位平台，都有适用的安装程序。安装程序的位置取决于平台：

- **Linux 32 位：** IDM4.0.1\_Lin/products/eDirectory/x86/setup/nds-install
  - **Linux 64 位：** IDM4.0.1\_Lin/products/eDirectory/x64/setup/nds-install
  - **Solaris 32 位：** IDM4.0.1\_Solaris/products/eDirectory/x86/setup/nds-install
  - **Solaris 64 位：** IDM4.0.1\_Solaris/products/eDirectory/x64/setup/nds-install
- 要执行二进制文件，请输入 `./nds-install`。
- **Windows 32 位：** IDM4.0.1\_Win:\products\eDirectory\x86\nt\Setup.exe
  - **Windows 64 位：** IDM4.0.1\_Win:\products\eDirectory\x64\windows\Setup.exe

有关如何安装 eDirectory 的说明因平台而异。有关各平台的安装说明，请参见《[Novell eDirectory 8.8 安装指南](http://www.novell.com/documentation/edir88/edirin88/data/a2iii88.html)》中的相应章节。

---

**注释：**对于 Linux 和 Solaris，在安装 eDirectory 后必须进行配置，然后才能安装元目录服务器。有关配置说明，请参见《[Novell eDirectory 8.8 安装指南](http://www.novell.com/documentation/edir88/edirin88/data/bnn8z89.html)》中的“在 Linux、Solaris 或 AIX 系统上配置 Novell eDirectory”。

---

## 7.4 安装 iManager

请确保您已从 Novell 下载网站下载了必需的 Identity Manager 文件。有关更多信息，请参见第 5 章“[从何处获取 Identity Manager](#)”（第 39 页）。

Identity Manager 媒体上提供了 iManager 2.7.4。对于 Windows 和 Linux，都有适用的安装程序。iManager 在 Solaris 上不受支持。安装程序的位置取决于平台：

- ◆ **Linux:** IDM4.0.1\_Lin/products/iManager/installs/linux/iManagerInstallLinux.bin  
要执行二进制文件，请输入 `./iManagerInstallLinux.bin`。
- ◆ **Windows:** IDM4.0.1\_Win:\products\iManager\installs\win\iManagerInstall.exe

有关如何安装 iManager 的说明因平台而异。有关安装说明，请参见《[iManager 安装指南](http://www.novell.com/documentation/imanager27/imanager_install_27/data/hk42s9ot.html)》中的相应章节。

## 7.5 安装元目录服务器

对于 Linux\UNIX 平台，可以根用户或非根用户身份安装元目录服务器。如果使用非根安装，则安装过程不同。有关安装说明，请参见第 7.5.1 节“[元目录服务器的非根安装](#)”（第 56 页）。

此过程包括元目录服务器、Web 组件以及用于 Identity Manager 支持的不同平台的实用程序的 GUI 安装。如果想要进行这些组件的无提示安装，请参见第 7.5.2 节“[元目录服务器的无提示安装](#)”（第 57 页）。

- 1 请校验您是否满足第 6 章“[系统要求](#)”（第 43 页）中列出的系统要求。
- 2 请确保您已从 Novell 下载网站下载了必需的 Identity Manager 文件。有关更多信息，请参见第 5 章“[从何处获取 Identity Manager](#)”（第 39 页）。
- 3（仅 Linux\UNIX）要在 Linux/UNIX 上开始安装前验证是否已导出 eDirectory 的环境变量，请转到命令提示符并输入：

```
set | grep PATH
```

环境变量设置 eDirectory 的安装路径。如果设置了环境变量，则列出 eDirectory 安装路径。如果未设置环境变量，则 Identity Manager 安装失败。

设置当前壳层的环境变量：

```
./opt/novell/eDirectory/bin/ndspath
```

必须在 `.` 和 `/` 之间保留空格才能使命令起效。有关更多信息，请参见“[使用 nds-install 实用程序安装 eDirectory 组件](http://www.novell.com/documentation/edir88/edirin88/index.html?page=/documentation/edir88/edirin88/data/a79kg0w.html#ai39feq)”。



#### 4 使用适用于平台的程序启动安装。

**Linux — GUI 安装:** IDM4.0.1\_Lin/products/IDM/install.bin [-i gui]

**Linux — 命令行安装:** IDM4.0.1.1\_Lin/products/IDM/install.bin -i console

**Solaris — GUI 安装:** IDM4.0.1\_Solaris/products/IDM/install.bin [-i gui]

**Solaris — 命令行安装:** IDM4.0.1\_Solaris/products/IDM/install.bin -i console

要在 Linux 或 Solaris 上执行二进制文件，请输入 `./install.bin [-i {gui | console}]`。

**Windows:** IDM4.0.1\_Win:\products\IDM\windows\setup\idm\_install.exe

#### 5 使用以下信息完成安装:

**选择组件:** 选择元目录服务器、iManager 插件和实用程序以安装元目录服务器。

- ◆ **Novell Identity Manager 元目录服务器:** 此选项要求此服务器上安装了身份库，并安装 64 位版本的 Identity Manager。它扩展了 Identity Manager 的纲要，并安装元目录服务器、Identity Manager 驱动程序和 Novell Audit 代理。
- ◆ **Novell Identity Manager 元目录服务器 (32 位):** 此选项要求此服务器上安装了身份库，并安装 32 位版本的 Identity Manager。它扩展了 Identity Manager 的纲要，并安装元目录服务器、Identity Manager 驱动程序和 Novell Audit 代理。
- ◆ **Novell Identity Manager 已连接系统服务器 (64 位):** 此选项不要求将身份库安装在此服务器上。仅当安装 64 位 Remote Loader 时才选择此选项。有关更多信息，请参见第 7.6 节“安装 Remote Loader” (第 58 页)。
- ◆ **Novell Identity Manager 已连接系统服务器 (.NET):** 此选项 (仅 Windows) 在此服务器上安装 .NET Remote Loader 服务及 SharePoint 驱动程序。
- ◆ **Novell Identity Manager 插件:** 如果在此服务器上安装了 iManager，则选择此选项。此选项将安装用于 Identity Manager 的 iManager 插件。
- ◆ **实用程序:** 安装用于为已连接系统配置驱动程序的实用程序。并非所有驱动程序都具有实用程序。如果您不确定是否需要此实用程序，请选择它。它不会使用太多磁盘空间。
- ◆ **自定义所选组件:** 此选项使您能够自定义已选择安装的组件。在选择此选项前，应选择要安装的相关组件。

**鉴定:** 指定在 eDirectory 中具有扩展纲要的足够权限的用户和口令。以 LDAP 格式指定用户名。例如，`cn=idmadmin,o=company`。

#### 6 激活 Identity Manager。有关更多信息，请参见第 8 章“激活 Novell Identity Manager 产品” (第 67 页)。

#### 7 创建并配置驱动程序对象。此信息包含在各个驱动程序指南中。有关更多信息，请参见 Identity Manager 驱动程序文档 (<http://www.novell.com/documentation/idm40drivers/>)。

## 7.5.1 元目录服务器的非根安装

您可以非根用户身份安装 Identity Manager 以增强 UNIX/Linux 服务器的安全性。如果 eDirectory 是以根身份安装的，则无法以非根用户身份安装 Identity Manager。

非根安装不能安装以下项目:

- ◆ **Remote Loader:** 如果需要以非根用户身份安装 Remote Loader，请使用 Java Remote Loader。有关更多信息，请参见第 7.6.5 节“在 UNIX 或 Linux 上安装 Java Remote Loader” (第 62 页)。



- ◆ **UNIX/Linux 帐户驱动程序：**需要根特权才能正常工作。
- ◆ **Novell Sentinel 平台代理：**以 root 身份安装 Novell Sentinel 平台代理。在 /etc/opt/novell/sentinelpa/conf 目录中创建 Dirxml.properties。非根用户对生成事件日志文件的位置（/var/opt/novell/sentinelpa/data/AuditEvents.log 是默认位置）应具有写许可权限。

使用以下过程运行元目录服务器的非根安装：

- 1 请确保您已从 Novell 下载网站下载了必需的 Identity Manager 文件。有关更多信息，请参见第 5 章“从何处获取 Identity Manager”（第 39 页）。
- 2 以非根用户身份安装 eDirectory 8.8.6 或更高版本。有关更多信息，请参见“非根用户安装 eDirectory 8.8.6”(<http://www.novell.com/documentation/edir88/edirin88/index.html?page=/documentation/edir88/edirin88/data/a79kg0w.html#bs6a3gs>)。

- 3 以用于安装 eDirectory 的非根用户身份登录。

应以用于安装 eDirectory 非根版本的相同用户来安装 Identity Manager。安装 Identity Manager 的用户必须对非根 eDirectory 安装的目录和文件具有写访问权限。

- 4 执行适用于您的平台的安装程序。

**Linux:** IDM4.0.1\_Lin/products/IDM/linux/setup/idm-nonroot-install

**Solaris:** IDM4.0.1\_Solaris/products/IDM/solaris/setup/idm-nonroot-install

- 5 使用以下信息完成安装：

**非根 eDirectory 安装的基本目录：**指定非根 eDirectory 安装的目录。例如 /home/user/install/eDirectory。

**扩展 eDirectory 纲要：**如果这是 eDirectory 的此实例中安装的首个 Identity Manager 服务器，则输入 Y 以扩展纲要。如果纲要未扩展，则 Identity Manager 无法生效。

系统会提示您扩展由非根 eDirectory 安装托管的非根用户所拥有的每个 eDirectory 实例的纲要。

如果选择扩展纲要，请指定有权扩展该纲要的 eDirectory 用户的完整判别名 (DN)。用户必须具有对整个树的主管权限才能扩展纲要。有关以非根用户身份扩展纲要的更多信息，请参见位于各个 eDirectory 实例的 data 目录中的 schema.log 文件。

运行 /opt/novell/eDirectory/bin/idm-install-schema 程序以在安装完成后在其他 eDirectory 实例上扩展纲要。

**实用程序：**（可选）如果需要 Identity Manager 驱动程序实用程序，则必须将实用程序从 Identity Manager 安装媒体复制到 Identity Manager 服务器。所有实用程序都位于 IDM4.0.1\_平台/product/IDM/平台/setup/utilities 目录中。

- 6 激活 Identity Manager。有关更多信息，请参见第 8 章“激活 Novell Identity Manager 产品”（第 67 页）。
- 7 创建并配置驱动程序对象。此信息包含在各个驱动程序指南中。有关更多信息，请参见 Identity Manager 驱动程序文档 (<http://www.novell.com/documentation/idm40drivers/>)。

## 7.5.2 元目录服务器的无提示安装

为了运行 Identity Manager 的无提示安装，必须创建一个具有完成安装所需参数的属性文件。Identity Manager 媒体上有一个样本文件：

- ◆ **Linux:** IDM4.0.1\_Lin/products/IDM/linux/setup/silent.properties
- ◆ **Solaris:** IDM4.0.1\_Solaris/products/IDM/solaris/setup/silent.properties

- ◆ **Windows:** IDM4.0.1\_Win:\products\IDM\windows\setup\silent.properties

通过使用适用于您的平台的正确程序来启动无提示安装:

- ◆ **Linux:** IDM4.0.1\_Lin/products/IDM/install.bin -i silent -f < 文件名 >.properties
- ◆ **Solaris:** IDM4.0.1\_Solaris/products/IDM/install.bin -i silent -f < 文件名 >.properties
- ◆ **Windows:** IDM4.0.1\_Win:\products\IDM\windows\setup\idm\_install.exe -i silent -f < 文件名 >.properties

在运行 Identity Manager 安装程序的位置创建具有以下属性的属性文件 < 文件名 >.properties:

```
EDIR_USER_NAME=cn=admin,o=test
EDIR_USER_PASSWORD=test
METADIRECTORY_SERVER_SELECTED=true
CONNECTED_SYSTEM_SELECTED=false
X64_CONNECTED_SYSTEM_SELECTED=false
WEB_ADMIN_SELECTED=false
UTILITIES_SELECTED=false
```

有关默认安装位置, 请参见 /tmp/idmInstall.log。

如果已安装 iManager, 以后还想安装 iManager 插件, 则必须将 WEB\_ADMIN\_SELECTED 值设置为 true。

如果想要在多个实例上运行 Identity Manager 的无提示安装, 则必须确保 < 文件名 >.properties 文件具有以下行:

```
EDIR_NCP_PORT=524
EDIR_NDS_CONF=/etc/opt/novell/eDirectory/conf
EDIR_IP_ADDRESS=<xxx.xx.xx.xx>
```

口令储存在用于元目录的无提示安装的某个文件中。也可以使用 EDIR\_USER\_PASSWORD 环境变量来提供口令, 而不是将口令写入文件中。如果属性文件中未设置 EDIR\_USER\_PASSWORD 变量, 则安装程序将从 EDIR\_USER\_PASSWORD 环境变量读取值。

## 7.6 安装 Remote Loader

通过使驱动程序无需在与已连接系统相同的服务器上安装身份库和元目录服务器即可访问已连接系统, Remote Loader 扩展了 Identity Manager 的功能。作为规划流程的一部分, 您需要决定是否要使用 Remote Loader。有关规划流程的更多信息, 请参见第 3 章“技术准则”(第 23 页)。

- ◆ 第 7.6.1 节“要求”(第 59 页)
- ◆ 第 7.6.2 节“支持的驱动程序”(第 59 页)
- ◆ 第 7.6.3 节“安装过程”(第 60 页)
- ◆ 第 7.6.4 节“Remote Loader 的无提示安装”(第 61 页)
- ◆ 第 7.6.5 节“在 UNIX 或 Linux 上安装 Java Remote Loader”(第 62 页)
- ◆ 第 7.6.6 节“32 位与 64 位 Remote Loader 的共存”(第 62 页)

如果要通过非根用户身份安装 Remote Loader，请使用 Java Remote Loader。Java Remote Loader 还可用于自定义环境及在不受支持的平台（例如 HP-UX）上安装 Java Remote Loader。有关更多信息，请参见第 7.6.5 节“在 UNIX 或 Linux 上安装 Java Remote Loader”（第 62 页）。

## 7.6.1 要求

Remote Loader 要求每个驱动程序的已连接系统可用并且提供相关 API。有关每个驱动程序特定的操作系统和已连接系统要求，请参见 [Identity Manager 驱动程序文档 \(http://www.novell.com/documentation/idm40drivers\)](http://www.novell.com/documentation/idm40drivers)。

## 7.6.2 支持的驱动程序

并非所有 Identity Manager 驱动程序都受 Remote Loader 支持。下面列出了具有 Remote Loader 功能的驱动程序。

- ◆ Active Directory
- ◆ Avaya PBX
- ◆ 数据收集服务
- ◆ Delimited Text
- ◆ GroupWise（仅对 32 位 Remote Loader 可用）
- ◆ JDBC
- ◆ JMS
- ◆ LDAP
- ◆ Linux 和 UNIX 的驱动程序
- ◆ Lotus Notes
- ◆ 受管系统网关
- ◆ 手动任务服务
- ◆ PeopleSoft 5.2
- ◆ Remedy ARS
- ◆ RACF
- ◆ Salesforce.com
- ◆ SAP 业务逻辑
- ◆ SAP GRC（仅 CMP）
- ◆ SAP HR
- ◆ SAP 门户
- ◆ SAP User Management
- ◆ 脚本编写
- ◆ SharePoint
- ◆ SOAP
- ◆ 工作指令

下列驱动程序不能使用 Remote Loader。

- ◆ eDirectory
- ◆ 权利服务
- ◆ 角色服务
- ◆ User Application

### 7.6.3 安装过程

Remote Loader 具有不同程序适用于不同平台，因此它可与元目录服务器通讯。

- ◆ **Linux/UNIX:** rdxml 是一种可执行文件，可以使元目录服务器与在 Solaris 或 Linux 环境中运行的 Identity Manager 驱动程序通讯。
- ◆ **Windows:** Remote Loader 控制台使用 rlconsole.exe 与 dirxml\_remote.exe 交互，后者是一个可执行文件，可使元目录服务器与在 Windows 上运行的 Identity Manager 驱动程序通讯。

安装 Remote Loader:

- 1 验证您是否满足第 6 章“系统要求”（第 43 页）中列出的系统要求。
- 2 请确保您已从 Novell 下载网站下载了必需的 Identity Manager 文件。有关更多信息，请参见第 5 章“从何处获取 Identity Manager”（第 39 页）。
- 3 使用适用于平台的程序启动安装。

**Linux — GUI 安装:** IDM4.0.1\_Lin/products/IDM/install.bin [-i gui]

**Linux — 命令行安装:** IDM4.0.1\_Lin/products/IDM/install.bin -i console

**Solaris — GUI 安装:** IDM4.0.1\_Solaris/products/IDM/install.bin [-i gui]

**Solaris — 命令行安装:** IDM4.0.1\_Solaris/products/IDM/install.bin -i console

**Windows:** IDM4.0.1\_Win:\products\IDM\windows\setup\idm\_install.exe

要在 Linux 或 Solaris 上执行二进制文件，请输入 ./install.bin [-i {gui | console}]。

- 4 使用提供的以下信息完成安装:

**选择组件:** 选择已连接系统服务器和实用程序以安装 Remote Loader。

- ◆ **Novell Identity Manager 元目录服务器:** 仅当在安装元目录服务器时才选择此选项。此选项要求将身份库安装在此服务器上。有关更多信息，请参见第 7.5 节“安装元目录服务器”（第 55 页）。
- ◆ **Novell Identity Manager 已连接系统服务器 (32 位):** 此选项不要求将身份库安装在此服务器上。它在应用程序服务器上安装 32 位版本的 Remote Loader 服务。
- ◆ **Novell Identity Manager 已连接系统服务器 (64 位):** 此选项不要求将身份库安装在此服务器上。它在应用程序服务器上安装 64 位版本的 Remote Loader 服务。
- ◆ **Novell Identity Manager 已连接系统服务器 (.NET):** 此选项（仅 Windows）在此服务器上安装 .NET Remote Loader 服务及 SharePoint 驱动程序。
- ◆ **Novell Identity Manager 插件:** 如果在此服务器上安装了 iManager，则选择此选项。此选项将安装用于 Identity Manager 的 iManager 插件。
- ◆ **实用程序:** 安装用于为已连接系统配置驱动程序的实用程序。并非所有驱动程序都具有实用程序。如果您不确定是否需要此实用程序，请选择它。它不会使用太多磁盘空间。

- ◆ **自定义：** 如果要自定义安装的功能，则选择此选项。它允许选择下列选项。在选择此选项前，应选择要安装的组件：
  - ◆ **Remote Loader 服务（32 位）：** 与元目录服务器通讯的服务。
  - ◆ **Remote Loader 服务（64 位）：** 与元目录服务器通讯的服务。
  - ◆ **驱动程序：** 选择要安装的驱动程序文件。应安装所有驱动程序文件。如果需要添加其他 Remote Loader 实例，无需再次运行安装。
  - ◆ **Novell Identity Manager 已连接系统服务器 (.NET)：**（仅 Windows）安装 .NET Remote Loader 服务及 SharePoint 驱动程序。

选择自定义以继续安装时，必须选择其他选项。

**（仅 Windows）已连接系统服务器的安装位置：** 指定用于安装已连接系统服务器的目录。

**（仅 Windows）.NET Remote Loader 的安装位置：** 指定 .NET Remote Loader 的安装目录。

**（仅 Windows）实用程序的安装位置：** 指定用于安装实用程序的目录。

- 5 创建并配置要使用 Remote Loader 的驱动程序对象。此信息包含在各个驱动程序指南中。有关更多信息，请参见 [Identity Manager 驱动程序文档 \(http://www.novell.com/documentation/idm40drivers/\)](http://www.novell.com/documentation/idm40drivers/)。
- 6 创建一个要用于已连接系统的 Remote Loader 配置文件。有关更多信息，请参见《*Identity Manager 4.0.1 Remote Loader 指南*》中的“通过创建配置文件为 Linux/UNIX 配置 Remote Loader”。

## 7.6.4 Remote Loader 的无提示安装

为了运行 Remote Loader 的无提示安装，必须创建一个具有完成安装所需参数的属性文件。Identity Manager 媒体上有一个样本文件：

- ◆ **Linux：** IDM4.0.1\_Lin/products/IDM/linux/setup/silent.properties
- ◆ **Solaris：** IDM4.0.1\_Solaris/products/IDM/solaris/setup/silent.properties
- ◆ **Windows：** IDM4.0.1\_Win:\products\IDM\windows\setup\silent.properties

通过使用适用于您的平台的正确程序来启动无提示安装：

- ◆ **Linux：** IDM4.0.1\_Lin/products/IDM/install.bin -i silent -f < 文件名 >.properties
- ◆ **Solaris：** IDM4.0.1\_Solaris/products/IDM/install.bin -i silent -f < 文件名 >.properties
- ◆ **Windows：** IDM4.0.1\_Win:\products\IDM\windows\setup\idm\_install.exe -i silent -f < 文件名 >.properties

在运行 Identity Manager 安装程序的位置创建具有以下属性的属性文件 < 文件名 >.properties：

```
METADIRECTORY_SERVER_SELECTED=false
CONNECTED_SYSTEM_SELECTED=true
X64_CONNECTED_SYSTEM_SELECTED=true
WEB_ADMIN_SELECTED=false
UTILITIES_SELECTED=false
```

有关默认安装位置，请参见 /tmp/idmInstall.log。

如果已安装 iManager，以后还想安装 iManager 插件，则必须将 WEB\_ADMIN\_SELECTED 值设置为 true。

## 7.6.5 在 UNIX 或 Linux 上安装 Java Remote Loader

dirxml\_jremote 是一种纯 Java Remote Loader。它用于在运行于一个服务器上的元目录服务器与运行于其他位置（该位置没有运行 rdxml）的 Identity Manager 驱动程序之间交换数据。它应在具有兼容的 JRE（最低 1.5.0）和 Java 套接字的任何系统上运行。Identity Manager 所支持的 Linux/UNIX 平台上支持它。

- 1 请校验 Java 1.5.x JDK/JRE 在主机系统上是否可用。
- 2 请确保您已从 Novell 下载网站下载了必需的 Identity Manager 文件。有关更多信息，请参见第 5 章“从何处获取 Identity Manager”（第 39 页）。
- 3 在 Identity Manager 媒体上查找 Java Remote Loader 安装文件：  
**Linux:** IDM4.0.1\_Lin/products/IDM/java\_remoteloader  
**Solaris:** IDM4.0.1\_Solaris/products/IDM/java\_remoteloader
- 4 将 dirxml\_jremote\_dev.tar.gz 文件复制到远程服务器上的所需位置。
- 5 将 dirxml\_jremote.tar.gz 或 dirxml\_jremote\_mvs.tar 文件复制到远程服务器上的所需位置。  
例如：/usr/idm  
有关 mvs 的信息，请解压缩 dirxml\_jremote\_mvs.tar 文件，然后参考 usage.html 文档。
- 6 解压缩并提取 dirxml\_jremote.tar.gz 文件和 dirxml\_jremote\_dev.tar.gz 文件。  
例如：gunzip dirxml\_jremote.tar.gz 或 tar -xvf dirxml\_jremote\_dev.tar
- 7 将应用程序 shim.jar 文件复制到提取 dirxml\_jremote.tar 文件时创建的 lib 子目录中。  
因为 tar 文件不包含 .jar 文件，所以必须手动将这些 .jar 文件从元目录服务器复制到 lib 目录中。lib 目录位于执行解压缩的目录下。  
在元目录服务器上，.jar 文件的默认安装目录是 /opt/novell/eDirectory/lib/dirxml/classes。
- 8 通过执行以下操作之一自定义 dirxml\_jremote 脚本：
  - ◆ 通过设置环境变量 RDXML\_PATH 来验证是否可通过 PATH 环境变量获得 Java 可执行文件。请输入以下命令以设置环境变量：
    1. set RDXML\_PATH=path
    2. export RDXML\_PATH
  - ◆ 编辑 dirxml\_jremote 脚本，并在脚本行中向执行 Java 的 Java 可执行文件预先添加路径。
- 9 配置要用于您的应用程序 shim 的 config8000.txt 样本文件。有关更多信息，请参见《Identity Manager 4.0.1 Remote Loader 指南》中的“通过创建配置文件为 Linux/UNIX 配置 Remote Loader”。

## 7.6.6 32 位与 64 位 Remote Loader 的共存

Identity Manager 4.0.1 允许在 64 位操作系统上同时存在 32 位和 64 位 Remote Loader。如果是升级 64 位操作系统上安装的 32 位 Remote Loader，则会升级 32 位 Remote Loader，同时安装 64 位 Remote Loader。同一计算机上可以同时存在 32 位和 64 位 Remote Loader。



如果选择在同一台计算机上同时具有 32 位和 64 位 Remote Loader，则只对 64 位 Remote Loader 生成审计事件。如果在安装 32 位 Remote Loader 前已安装 64 位 Remote Loader，则事件将记录到 32 位 lcache。

## 7.7 安装驱动程序文件

您可以在不安装元目录服务器或 Remote Loader 的情况下安装驱动程序文件。驱动程序文件由驱动程序 Shim 和驱动程序实用程序组成。

要安装驱动程序文件：

- 1 请确保您已从 Novell 下载网站下载了必需的 Identity Manager 文件。有关更多信息，请参见第 5 章“从何处获取 Identity Manager”（第 39 页）。

- 2 使用适用于平台的程序启动安装。

**Linux — GUI 安装：** IDM4.0.1\_Lin/products/IDM/install.bin [-i gui]

**Linux — 命令行安装：** IDM4.0.1\_Lin/products/IDM/install.bin -i console

**Solaris — GUI 安装：** IDM4.0.1\_Solaris/products/IDM/install.bin [-i gui]

**Solaris — 命令行安装：** IDM4.0.1\_Solaris/products/IDM/install.bin -i console

要在 Linux 或 Solaris 上执行二进制文件，请输入 ./install.bin [-i {gui | console}]。

**Windows：** IDM4.0.1\_Win:\products\IDM\windows\setup\idm\_install.exe

- 3 阅读并接受许可协议，然后单击 *下一步*。

- 4 在“选择组件”页面上，选择以下选项：

**Novell Identity Manager 元目录服务器：** 您可以选择该选项或选择 *已连接系统服务器* 选项。不需要同时选择这两个选项。

该选项包括驱动程序文件。

**Novell Identity Manager 已连接系统服务器：** 您可以选择该选项或选择 *元目录服务器* 选项。不需要同时选择这两个选项。

该选项包括驱动程序文件。

**Novell 实用程序：** 选择该选项安装实用程序以帮助配置某些驱动程序。

**自定义所选组件：** 允许您仅选择驱动程序文件而不安装元目录服务器或 Remote Loader。

- 5 单击 *下一步*。

- 6 取消选择 *元目录引擎* 选项及 *Remote Loader 服务* 选项。

- 7 校验是否已选择 *元目录服务器* 选项或 *已连接系统服务器* 选项下的 *驱动程序* 选项。

您可以展开 *驱动程序* 选项并仅选择您要安装的驱动程序。默认情况下，将选择所有驱动程序。

- 8 单击 *下一步*。

- 9 在 *鉴定* 页面上，指定在 eDirectory 中具有足够权限扩展纲要的用户和口令。以 LDAP 格式指定用户名。例如，cn=idmadmin,o=company。

- 10 单击 *下一步*。

- 11 查看安装摘要，然后单击 *下一步*。

- 12 查看安装完成讯息，然后单击 *完成*。

现在，驱动程序文件已随 Remote Loader 或元目录服务器安装。

## 7.8 安装 Roles Based Provisioning Module

要安装 Roles Based Provisioning Module，请参见《*Identity Manager Roles Based Provisioning Module 4.0.1 User Application: 安装指南*》。

## 7.9 安装自定义驱动程序

您可以创建一个自定义驱动程序以在您的环境中使用。有关创建或安装自定义驱动程序的更多信息，请参见 [Novell 开发人员套件 \(http://developer.novell.com/wiki/index.php/Dirxml\)](http://developer.novell.com/wiki/index.php/Dirxml)。

## 7.10 安装角色映射管理器

角色映射管理器是一个 Web 服务，可发现您主要 IT 系统内可授予的授权和许可权限。

---

**注释：** Standard Edition 没有角色映射管理器。

---

要安装角色映射管理器：

- 1 请确保您已从 Novell 下载网站下载了必需的 Identity Manager 文件。有关更多信息，请参见第 5 章“[从何处获取 Identity Manager](#)”（第 39 页）。

- 2 在 Identity Manager 媒体上的以下位置查找角色映射管理器安装文件：

**Linux:** IDM4.0.1\_Lin/products/RMA/IDMRMAP.jar

**Windows:** IDM4.0.1\_Win:\products\RMA\IDMRMAP.jar

- 3 从命令行访问角色映射管理器安装目录，然后输入 `java -jar IDMRMAP.jar`。

---

**注释：** 出于安全原因，如果是使用 Linux，则应以非根用户身份安装角色映射管理器。

---

- 4 输入 Yes 接受许可协议。

- 5 指定角色映射管理器的安装目录。默认路径是当前位置。

- 6 指定代表角色映射管理器名称的 URL 部分。默认值是 IDMRMAP。

- 7 指定 HTTP 端口。默认值是 8081。

- 8 指定配置管理员的口令。

现在，角色映射管理器已安装。该应用程序不会在安装完成后自动启动。使用安装目录中的以下脚本停止和启动应用程序。

- ◆ **Linux:** 启动脚本是 `start.sh`，停止脚本是 `stop.sh`。
- ◆ **Windows:** 启动脚本是 `start.bat`，停止脚本是 `stop.bat`。

安装并启动角色映射管理器后，必须对其进行配置。有关配置信息，请参见《*Identity Manager 角色映射管理器 4.0.1 安装和配置指南*》中的“[配置应用程序](#)”部分。



## 7.11 安装身份报告模块或 Sentinel

可选择在 Identity Manager 解决方案中添加身份报告模块和 Sentinel。通过添加审计和报告，您可满足许多公司必须遵守的合规性标准。您可以为需要跟踪的任何事件创建审计追踪，也可以生成报告以确保满足公司的任何审计标准。

有关身份报告模块的安装和配置信息，请参见《[身份报告模块指南](#)》。有关配备了 Identity Manager 的 Sentinel 的配置信息，请参见《[Novell Sentinel 的 Identity Manager 4.0.1 报告指南](#)》。有关 Sentinel 的系统要求信息，请参见《[Novell Sentinel 安装指南 \(http://www.novell.com/documentation/sentinel6/index.html\)](#)》。



# 激活 Novell Identity Manager 产品

# 8

以下信息说明如何激活基于 Novell Identity Manager 的产品。Identity Manager、集成模块和供应模块都必须在安装后 90 天内进行激活，否则它们将会关闭。可以在这 90 天期限之内或之后的任何时间，选择激活 Identity Manager 产品。

可以通过完成以下任务激活 Identity Manager 和驱动程序：

- ◆ 第 8.1 节“购买 Identity Manager 产品许可证”（第 67 页）
- ◆ 第 8.2 节“安装产品激活身份凭证”（第 67 页）
- ◆ 第 8.3 节“查看 Identity Manager 和驱动程序的产品激活”（第 68 页）
- ◆ 第 8.4 节“激活 Identity Manager 驱动程序”（第 68 页）
- ◆ 第 8.5 节“激活 Analyzer”（第 69 页）
- ◆ 第 8.6 节“激活 Designer 和角色映射管理器”（第 69 页）

## 8.1 购买 Identity Manager 产品许可证

要购买 Identity Manager 产品许可证以激活产品，请参见 Novell Identity Manager“如何购买”网页 (<http://www.novell.com/products/identitymanager/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 Novell 站点的 URL，您可以从该站点获取产品激活身份凭证。如果您不记得或者没有收到客户 ID，美国境内请拨打 1-800-418-8373 联系 Novell 激活中心，对于其他所有地方，请拨打 1-801-861-8373（使用 801 区号拨打会收取费用）。您也可以与我们的在线聊天 (<http://support.novell.com/chat/activation>)。

## 8.2 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。


- 1 在您购买许可证之后，Novell 会向您发送一封电子邮件，其中包含您的客户 ID。在该电子邮件的“订单细节”部分下方，还包含一个链接，指向可获得您的身份凭证的站点。单击该链接可转至该站点。
- 2 单击许可证下载链接并执行以下操作之一：
  - ◆ 保存产品激活身份凭证文件。
  - 或
  - ◆ 打开产品激活身份凭证文件，然后将其内容复制到剪贴板。复制内容时要细心，确保没有包含额外的行或空格。应从身份凭证的第一个破折号 (-) 开始复制 (----BEGIN PRODUCT ACTIVATION CREDENTIAL)，一直复制到其最后一个破折号 (-) (END PRODUCT ACTIVATION CREDENTIAL----)。

---

**警告：**如果将 Standard Edition 激活应用于现有未激活的 Advanced Edition 系统，则会停止 Identity Manager 元目录服务器和驱动程序。

---

- 3 打开 iManager。

- 4 选择 *Identity Manager > Identity Manager 概述*。
- 5 单击  以在树结构中浏览并选择驱动程序集。
- 6 在“Identity Manager 概述”页面上，单击包含要激活的驱动程序的驱动程序集。
- 7 在“驱动程序集概述”页面上，单击 *激活 > 安装*。
- 8 选择要激活 Identity Manager 组件的驱动程序集，然后单击 *下一步*。
- 9 执行以下步骤之一：
  - ◆ 指定 Identity Manager 激活身份凭证保存的位置，然后单击“下一步”。
  - 或
  - ◆ 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”。
- 10 单击“完成”。



---

**注释：** 您需要激活包含要使用的驱动程序的每个驱动程序集。可以使用身份凭证激活所有树。

---

## 8.3 查看 Identity Manager 和驱动程序的产品激活

对于每个驱动程序集，都可以查看为元目录服务器和 Identity Manager 驱动程序安装的产品激活身份凭证：

- 1 打开 iManager。
  - 2 单击 *Identity Manager > Identity Manager 概述*。
  - 3 单击  以在树型结构中浏览并选择驱动程序集，然后单击  以执行搜索。
  - 4 在“Identity Manager 概述”页面上，单击要查看激活信息的驱动程序集。
  - 5 在“驱动程序集概述”页面上，单击 *激活 > 信息*。
- 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”。如果出现这种情况，请重新启动驱动程序，此后该讯息应会消失。

---

## 8.4 激活 Identity Manager 驱动程序

购买 Identity Manager 包括激活服务驱动程序及若干通用驱动程序。

- ◆ **服务驱动程序：** 激活元目录服务器时将激活以下服务驱动程序：
  - ◆ 数据收集服务
  - ◆ 权利服务
  - ◆ ID 提供程序
  - ◆ 回写服务
  - ◆ 受管系统网关
  - ◆ 手动任务服务
  - ◆ 空服务
  - ◆ 角色服务

- ◆ User Application
- ◆ WorkOrder
- ◆ **通用驱动程序：** 激活元目录服务器时将激活以下通用驱动程序：
  - ◆ Active Directory
  - ◆ ADAM
  - ◆ eDirectory
  - ◆ GroupWise
  - ◆ LDAP
  - ◆ Lotus Notes

所有其他 Identity Manager 驱动程序的激活都必须单独购买。驱动程序的激活是作为 Identity Manager 集成模块出售的。一个 Identity Manager 集成模块可以包含一个或多个驱动程序。您每购买一个 Identity Manager 集成模块，就会收到一个产品激活身份凭证。

必须对每个 Identity Manager 集成模块执行第 8.2 节“安装产品激活身份凭证”（第 67 页）中的步骤才能激活驱动程序。

## 8.5 激活 Analyzer

首次起动 Analyzer 时，系统会提示您激活。如果不进行激活，则无法使用 Analyzer。有关更多信息，请参见《*Analyzer 4.0.1 for Identity Manager 管理指南*》中的“激活 Analyzer”。

## 8.6 激活 Designer 和角色映射管理器

Designer 和角色映射管理器只需要激活元目录服务器或驱动程序即可。



# Identity Manager 查错

# 9

安装 Identity Manager 时请记住以下信息：

- ◆ 安装 Identity Manager 时的 Lotus Notes 驱动程序问题（第 71 页）
- ◆ 在 Windows 2008 SP2 32 位平台上安装 Identity Manager 偶尔会失败（第 71 页）
- ◆ 当语法流属性上发生两个事件时，第一个属性更改将丢失（第 75 页）
- ◆ Identity Manager 升级期间的 lcache 问题（第 75 页）
- ◆ 升级 Identity Manager 需要正确的管理员帐户以避免丢失询问应答的回答（第 75 页）

## 安装 Identity Manager 时的 Lotus Notes 驱动程序问题

源： 在 Solaris 10 上以非根身份安装 Identity Manager 4.0.1 时，可能遇到针对 Lotus Notes 驱动程序的以下错误讯息：

```
ln: cannot create /usr/lib/locale/ja/wnn//ndsrep: File exists
ln: cannot create
cp: cannot create /usr/lib/locale/ja/wnn//
libnotesdrvjni.so.1.0.0: Permission
denied
ln: cannot create /usr/lib/locale/ja/wnn//
libnotesdrvjni.so.1: File exists
ln: cannot create /usr/lib/locale/ja/wnn//libnotesdrvjni.so:
File exists
```

操作： 手动创建符号链接。有关检查和重建符号链接的信息，请参见《*Identity Manager 4.0.1 Driver for Lotus Notes 实施指南*》中的“[安装问题查错](#)”。

## 在 Windows 2008 SP2 32 位平台上安装 Identity Manager 偶尔会失败

源： 框架安装程序显示以下错误：

```
Java Platform SE binary has stopped working.
```

操作： 要解决此问题，请：

- 1 使用 `-DCLUSTER_INSTALL="true"` 选项运行 Identity Manager 安装程序。这样只安装 Identity Manager 文件，而不安装 eDirectory 纲要及其他文件。

```
<install_drive>:\windows\setup\idm_install.exe -
DCLUSTER_INSTALL="true"
```

- 2 使用 eDirectory 维护下的导入转换导出向导通过 iManager 扩展 Identity Manager 纲要。
- 3 使用 LDIF 文件创建默认对象。
  - ◆ 默认口令策略 LDIF 文件





Collection, cn=Security  
notifMergeTemplateSubject: Notice of Password Reset  
Failure  
notifMergeTemplateData::  
PGh0bWwgeG1sbnM6Zm9ybT0iaHR0cDovL3d3dy5ub3Z1bGwuY29tL  
2RpcnhtbC93b3JrZmxvdy9mb3JtIj4NCiAgPGZvcvcm06dG9rZW4tZG  
VzY3JpcHRpb25zPg0KICAgIDxmb3JtOnRva2VuLWRlc2NyaXB0aW9  
uIGl0ZW0tbmFtZT0iVXNlckZ1bGxOYW11IiBkZXNjcmlwdGlvbj0i  
VGhlIHVzZXIncyBmdWxsIG5hbWUiLz4NCiAgICA8Zm9ybTp0b2t1b  
i1kZXNjcmlwdGlvbiBpdGVtLW5hbWU9IlVzZXJHaXZ1bk5hbWUiIG  
Rlc2NyaXB0aW9uPSJUaGUgdXNlciZIGdpdmVuIG5hbWdDT0xPUj0  
iI0ZGRkZGRiI+DQogIDxwPkRlYXJgJFVzZXJGdWxsTmFtZSQsPC9w  
Pg0KICA8cD5UaGlzIGlzIGEGbm90aWNlIHROYYQgeW91ciBwYXNzd  
29yZCBjb3VsZCBub3QgYmUgcmlvZmVzZXQgaW4gdGhlICRDb25uZWN0ZW  
RTeXN0ZW10YW11JCBzeXN0ZW0uLiAgVGhlIHJlYXNvbiBmb3IgzMf  
pbHVyZSBpcyBpbmRyY2F0ZWQgYmVsb3c6PC9wPg0KICA8cD5SZWFz  
b246ICRGYw1sdXJlUmVhc29uJDwvcD4NCiAgPHA+SWYgeW91IGhhd  
mUgYw55IGZ1cnRoZXIgcXVlc3Rpb25zLA0KICAgICBwbGVhc2UgY2  
9udGFjdCB0aGUgaGVscCBkZXNrIGF0ICgwMTIpIDM0NS02Nzg5IG9  
yIGVtYW1sdQogICAgIGF0IDxhIGhyZWY9Im1haWx0b2p0ZWxwLmRl  
c2tAbX1jb21wYW55LmNvbSI+DQogICAgIGhlbHhAuZGVza0BteWVnb  
XBhbkuY29tIDwvYT48L3A+DQogIDxwPiAtIEF1dG9tYXRlZCBTZW  
N1cm10eTwvcD4NCiAgPHA+PglzYyBTUkM9ImNpZDpwb3dlcmVxZ2J  
5X25vdmVsbC5naWYiIEFMVD0iUG93ZXJlZCBieSB0b3Z1bGwiIHdp  
ZHRoPSI4MCIgaGVpZ2h0PSIyOSIvPjwvcD4NCjwvYm9keT4NCjwva  
HRtbD4NCg==  
objectClass: notifMergeTemplate  
objectClass: Top  
cn: Password Reset Fail

dn: cn=Password Set Fail,cn=Default Notification  
Collection, cn=Security  
notifMergeTemplateSubject: Notice of Password Set  
Failure  
notifMergeTemplateData::  
PGh0bWwgeG1sbnM6Zm9ybT0iaHR0cDovL3d3dy5ub3Z1bGwuY29tL  
2RpcnhtbC93b3JrZmxvdy9mb3JtIj4NCiAgPGZvcvcm06dG9rZW4tZG  
VzY3JpcHRpb25zPg0KICAgIDxmb3JtOnRva2VuLWRlc2NyaXB0aW9  
uIGl0ZW0tbmFtZT0iVXNlckZ1bGxOYW11IiBkZXNjcmlwdGlvbj0i  
VGhlIHVzZXIncyBmdWxsIG5hbWUiLz4NCiAgICA8Zm9ybTp0b2t1b  
i1kZXNjcmlwdGlvbiBpdGVtLW5hbWU9IlVzZXJHaXZ1bk5hbWUiIG  
Rlc2NyaXB0aW9uPSJUaGUgdXNlciZIGdpdmVuIG5hbWU9IlVzZXJHaXZ1bk5hbWUiIG  
gICA8Zm9ybTp0b2t1b1kZXNjcmlwdGlvbiBpdGVtLW5hbWU9IlVz  
ZXJMYXN0TmFtZSIgZGVzY3JpcHRpb249IlRoZSB1c2VyJ3MgbGFzd  
CBuYW11Ii8+DQogICAgPGZvcvcm06dG9rZW4tZGVzY3JpcHRpb24gaX  
RlbS1uYW11PSJDb25uZWN0ZWRTeXN0ZW10YW11IiBkZXNjcmlwdG1  
vb30iVGhlIGV4dGVybmFsIGFwcGxpY2F0b24gbmFtZSIvPg0KICAg  
IDxmb3JtOnRva2VuLWRlc2NyaXB0aW9uIGl0ZW0tbmFtZT0iRmFpb  
HVyZVJlYXNvbiIgzGVzY3JpcHRpb249IlRoZSBmYW1sdXJlIHJlYX  
NvbiIvPg0KICA8L2Zvcvcm06dG9rZW4tZGVzY3JpcHRpb25zPg0KPGh  
lYWQ+DQogIDx0aXRzT50b3RyY2UgY2YgUGFzc3dvcvcm06dG9rZW4tZGVzY3JpcHRpb24gaX  
aWx1cmU8L3RpdGx1Pg0KICA8c3R5bGU+IDwhLS0gYm9keSB7IGZvb  
nQtZmFtaWx50iBUcmVidWNoZXQgTVMgfSAAtLT4gPC9zdHlsZT4NCj  
wvaGVhZD4NCjxi2R5IEJHQ09MT1I9IiINGRkZGRkYiPg0KPHA+RGV  
hciAkVXNlckZ1bGxOYW11JlVzZXJHaXZ1bk5hbWUiIGRlc2NyaXB0aW9uPSJUaGUgdXNlciZIGdpdmVuIG5hbWU9IlVzZXJHaXZ1bk5hbWUiIG  
b3RyY2UgdGhhdCB5b3VyIHh3c3N3b3JkIGNvdWxkIG5vdCBiZSBzZ  
XQgaW4gdGhlICRDb25uZWN0ZWRTeXN0ZW10YW11JCBzeXN0ZW0uLi  
AgVGhlIHJlYXNvbiBmb3IgzMfpbHVyZSBpcyBpbmRyY2F0ZWQgYmV  
sb3c6PC9wPg0KICA8cD5SZWFzb246ICRGYw1sdXJlUmVhc29uJDwv

cD4NCiAgPHA+SWYgeW91IGhhdMUGYw55IGZ1cnRoZXIgcXVlc3Rpb  
25zLA0KICAgICBwbGVhc2UgY29udGFjdCB0aGUgaGVscCBkZXNRIG  
F0ICgWMTIpIDMONS02Nzg5IG9yIGVtYWlsDQogICAgIGF0IDxhIGh  
yZWY9Im1haWx0bzpoZWxwLmRlc2tAbXljb2lwYW55LmNvbSI+DQog  
ICAgIGh1bHAuZGVza0BteWNvbXBhbnkuY29tIDwvYT48L3A+DQogI  
DxwPiAtIEF1dG9tYXRlZCBTZWN1cm10eTwvcD4NCiAgPHA+PglTzY  
BTUkM9ImNpZDpw3dlcmVhX2J5X25vdmVsbC5naWYiIEFMVD0iUG9  
3ZXJlZCBieSB0b3ZlbGwiIHdpZHRoPSI4MCIgaGVpZ2h0PSIyOSIv  
PjwvcD4NCjwvYm9keT4NCjwvaHRtbD4NCg==  
objectClass: notifMergeTemplate  
objectClass: Top  
cn: Password Set Fail

dn: cn=Password Sync Fail,cn=Default Notification  
Collection,cn=Security  
notifMergeTemplateSubject: Notice of Password  
Synchronization Failure  
notifMergeTemplateData::  
PGh0bWwgeG1sbnM6Zm9ybT0iaHR0cDovL3d3dy5ub3ZlbGwvY29tL  
2RpcnhtbC93b3JrZmxvdy9mb3JtIj4NCiAgPGZvc06dG9rZW4tZG  
VzY3JpcHRpb25zPg0KICAgIDxmb3JtOnRva2VuLWRlc2NyaXB0aW9  
uIGl0ZW0tbmFtZT0iVXNlckZ1bGx0YW11IiBkZXNjcmlwdGlvbj0i  
VGhlIHVzZXIYXyBmdWxsIG5hbWUiLz4NCiAgICA8Zm9ybTp0b2t1b  
i1kZXNjcmlwdGlvbiBpdGVtLW5hbWU9IlVzZXJHaXZ1bk5hbWUiIG  
Rlc2NyaXB0aW9uPSJUaGUgdXNlcidzIGdpdmVuIG5hbWUiLz4NCiA  
gICA8Zm9ybTp0b2t1bi1kZXNjcmlwdGlvbiBpdGVtLW5hbWU9IlVz  
ZXJMYXN0TmFtZSIZGVzY3JpcHRpb249IlRoZSB1c2VyJ3MgbGFzd  
CBuYW11Ii8+DQogICAgPGZvc06dG9rZW4tZGVzY3JpcHRpb24gaX  
RlbS1uYW11PSJDb25uZWN0ZWRTeXN0ZW10YW11IiBkZXNjcmlwdG  
lvbj0iVGhlIGV4dGVybmFsIGFwcGxpY2F0b24gbmFtZSIVP0KICAg  
IDxmb3JtOnRva2VuLWRlc2NyaXB0aW9uIGl0ZW0tbmFtZT0iRmFpb  
HVyZVJlYXNvbiIgcGVzY3JpcHRpb249IlRoZSBmYwlsdXJlIHJlYX  
NvbiIvPg0KICA8L2Zvc06dG9rZW4tZGVzY3JpcHRpb25zPg0KPGh  
lYWQ+DQogIDx0aXR5ZT5Ob3RyY2UgY2YgUGFzZ3dvc06dG9rZW4tZ  
b25pemF0aW9uIEZhaWx1cmU8L3RpdGx1Pg0KICA8c3R5bGU+IDwhL  
S0gYm9keSB7IGZvbnQtZmFtaWx5OibUcmVidWNoZXQgTVMgfSAtLT  
4gPC9zdHlsZT4NCjwvaGVhZD4NCjxi2R5IEJHQ09MT1I9IiInGRkZ  
GRkYiPg0KICA8cD5EZWFyICRvc2VyRnVsbE5hbWUKLDwvcD4NCiAg  
PHA+VGhpcyBpcyBhIG5vdG1jZSB0aGF0IHlvdXlIgcGFzZ3dvc06dG  
nJvbSB0aGUgJENvbm51Y3RlZFN5c3R1bU5hbWUKIHdhcyB1bmFibG  
UgdG8gc3luY2hyb25pemUgdG8gb3RoZXIgcY29ubmVjdGVkIHNSc3R  
lbXMuICBUaGUgcVhc29uIGZvciBmYWlsdXJlIGlZIGluZG1jYXRl  
ZCBiZWxvdzo8L3A+DQogIDxwPlJlYXNvbjogJEZhaWx1cmVSWWFzb  
24kPC9wPg0KICA8cD5JZiB5b3UgaGF2ZSBhbnkgZnVydGhlcXBxdW  
VzdGlvbnMsIHBSZWFzZSBjb250YWN0IHRoZSB0ZWxwIGRlc2sgYXQ  
gKDAxMikNCiAgICAgMzQ1LT53ODkqb3IgcW1haWwvYXQgPGEgaHJl  
Zj0ibWFpbHRvOmhlbHAuZGVza0BteWNvbXBhbnkuY29tIj4NCiAgI  
CAGA+VscC5kZXNRQG15Y29tcGFueS5jb20gPC9hPjwvcD4NCiAgPH  
A+IC0gQXV0b21hdGVkIFNlY3VyaXR5PC9wPg0KICA8cD48aW1nIFN  
SQz0iY2lkOnBvd2VyZWRfYnlfbm92ZWxsLmdpZiIgQUxUPSJQb3dl  
cmVhIGJ5IE5vdmVsbCIgd2lkdGg9IjgwIiBoZWlnaHQ9IjI5Ii8+P  
C9wPg0KPC9ib2R5Pg0KPC9odG1sPg0K  
objectClass: notifMergeTemplate  
objectClass: Top  
cn: Password Sync Fail

4 安装 NMAS 方法。

5 在 iManager 上安装 NMAS 插件后，转到 *NMAS > NMAS 登录 > 方法 > 新建*。从所需 NMAS 方法浏览并安装配置文件。

---

**注释：**请确保在应用解决方法前已查看日志文件。例如，Role Based Provisioning Module 纲要已扩展，安装 Role Based Provisioning Module 驱动程序时无需扩展它。

---

#### 当语法流属性上发生两个事件时，第一个属性更改将丢失

源： Identity Manager 4.0.1 引擎不在超速缓存中储存 STREAM 和 OCTET\_STRING 属性。当事件同步到已连接系统时，引擎从身份库读取这些属性并更新已连接系统。如果在引擎从身份库读取这些属性前它们已修改，则修改值将在已连接系统中更新，中间更改可能丢失。

操作： 如果频繁更改属性，请使用适当的语法而不是 SYN\_STREAM。

例如，如果一个 XML 对象储存在 STREAM 属性中，请使用 XMLData 语法而不是 SYN\_STREAM。

#### Identity Manager 升级期间的 lcache 问题

源： 升级 Identity Manager 后，平台代理可能没有按预期记录事件。该问题的原因是在 Linux 上升级 Identity Manager 期间，没有升级平台代理。在 Solaris 上，平台代理已升级到最新版本，但新的平台代理有不同的默认端口，需要重新启动 lcache。

操作： 必须手动停止 lcache，再启动升级。

#### 升级 Identity Manager 需要正确的管理员帐户以避免丢失询问应答的回答

源： 在 Windows 平台上升级早期版本的 Identity Manager 时，应使用安装 eDirectory 所用的同一管理员帐户。

说明： 例如，如果使用域管理员帐户安装 eDirectory，则在安装 Identity Manager 时也使用域管理员帐户。而不要使用本地管理员帐户。

操作： 如果不使用相同的管理员帐户，将无法再访问用户对询问应答问题的回答。这是因为在安装期间重创建了树密钥（由于使用了不同的管理员帐户），而新的树密钥未提供对已储存答案的正确访问。用户在登录时将得到新询问应答回答的提示。



Identity Manager 4.0.1 新增了多种功能，很多现有功能也得到增强：

- ◆ 第 10.1 节“Identity Manager 4.0.1 新功能”（第 77 页）
- ◆ 第 10.2 节“Identity Manager 4.0 新功能”（第 78 页）

## 10.1 Identity Manager 4.0.1 新功能

- ◆ 第 10.1.1 节“Identity Manager Advanced Edition 与 Standard Edition”（第 77 页）
- ◆ 第 10.1.2 节“Telemetry”（第 77 页）
- ◆ 第 10.1.3 节“资源请求活动”（第 77 页）
- ◆ 第 10.1.4 节“身份报告模块中添加了新报告”（第 77 页）
- ◆ 第 10.1.5 节“Designer 调色板中添加了应用程序”（第 78 页）

### 10.1.1 Identity Manager Advanced Edition 与 Standard Edition

为了满足各种客户要求，Identity Manager 4.0.1 提供两种版本：Advanced Edition 和 Standard Edition。Advanced Edition 包括用于企业级用户供应的全部功能。Standard Edition 包括 Identity Manager Advanced Edition 的部分功能，并继续提供先前 Identity Manager 版本的所有功能。有关 Advanced Edition 和 Standard Edition 中可用的 Identity Manager 功能的比较，请参见 [Identity Manager 版本比较 \(http://www.novell.com/products/identitymanager/features/identitymanager-version-comparison.html\)](http://www.novell.com/products/identitymanager/features/identitymanager-version-comparison.html)。

### 10.1.2 Telemetry

Identity Manager Telemetry 是 Identity Manager 4.0.1 引入的一项新作业。该作业充当用量计数工具或许可证监视工具，向 Identity Manager 客户提供值，因为他们可以添加更多许可证或淘汰不使用的许可证。客户还可以获得不活动用户定价等好处。

### 10.1.3 资源请求活动

资源请求活动允许您实现向用户授予或撤消资源的自动化。例如，您可以写一个供应请求定义，在某新员工入职第一天供应他 / 她需要的所有资源。使用资源请求活动，您可以自动化对该员工使用指定资源的批准。有关资源请求活动的更多细节，请参见《[User Application: 设计指南](#)》中的“[资源请求活动](#)”。

### 10.1.4 身份报告模块中添加了新报告

添加了以下报告：

- ◆ **身份库中的用户状态更改：**显示身份库用户的重要事件。
- ◆ **身份库中的用户口令更改：**显示身份库中的所有用户口令更改。
- ◆ **按接收人排列的访问请求：**显示按接收人分组的资源指派工作流程过程。

- ◆ **按请求者排列的访问请求：** 显示按请求者分组的资源指派工作流程过程。
- ◆ **按资源排列的访问请求：** 显示按资源分组的资源指派工作流程过程。

有关新报告的更多信息，请参见 《[身份报告模块指南](#)》。

## 10.1.5 Designer 调色板中添加了应用程序

Designer 调色板中添加了以下应用程序：

- ◆ Blackboard
- ◆ Google Apps
- ◆ RSA

## 10.2 Identity Manager 4.0 新功能

- ◆ [第 10.2.1 节“身份报告模块”](#)（第 78 页）
- ◆ [第 10.2.2 节“新驱动程序”](#)（第 78 页）
- ◆ [第 10.2.3 节“支持 XDAS 审计”](#)（第 79 页）
- ◆ [第 10.2.4 节“包替换了驱动程序配置文件”](#)（第 79 页）
- ◆ [第 10.2.5 节“角色映射管理器”](#)（第 79 页）
- ◆ [第 10.2.6 节“Analyzer”](#)（第 79 页）
- ◆ [第 10.2.7 节“集成安装程序”](#)（第 79 页）

### 10.2.1 身份报告模块

身份报告模块使您能够生成显示您 Identity Manager 配置的各个方面相关信息的报告，包括从一个或多个身份库或受管系统收集的信息。报告模块提供了一组预定义的报告定义，可用于生成报告。此外，它还允许导入在第三方工具中定义的自定义报告。

身份报告模块需要两个新的服务驱动程序：

- ◆ 数据收集服务驱动程序
- ◆ 受管系统网关驱动程序

有关报告模块及这两个报告驱动程序的细节，请参见 《[身份报告模块指南](#)》。有关预定义报告的细节，请参见 《[使用 Identity Manager 4.0 报告](#)》。

### 10.2.2 新驱动程序

Identity Manager 4.0.1 包括以下新驱动程序：

- ◆ [SharePoint 驱动程序 \(.NET Remote Loader\)](#)（第 79 页）
- ◆ [Salesforce.com 驱动程序](#)（第 79 页）

## SharePoint 驱动程序 (.NET Remote Loader)

Novell Identity Manager 的 SharePoint 驱动程序可以在身份库与 SharePoint 2007 或 SharePoint 2010 站点集合之间同步用户和组成员资格事件。一个驱动程序可为一个站点集合处理这些事件，该站点集合为一个或多个 SharePoint 站点维护用户和组成员资格信息。有关更多信息，请参见《[Identity Manager 4.0.1 Driver for SharePoint 实施指南](#)》。

## Salesforce.com 驱动程序

Identity Manager 4.0.1 可自动将用户供应和同步到云应用程序。Novell Identity Manager 的新驱动程序 Salesforce.com 可向 Salesforce.com 云应用程序无缝供应用户及取回用户，这确保了用户身份信息在身份库与云应用程序之间是一致的。Salesforce.com 驱动程序还支持在身份库与 Salesforce.com 云之间进行安全口令同步，并且支持已鉴定的代理服务器和可配置的用户配置文件以实现自动用户供应。有关更多信息，请参见《[Identity Manager 4.0.1 Driver for Salesforce.com 实施指南](#)》。

## 10.2.3 支持 XDAS 审计

Identity Manager 4.0.1 支持基于 XDAS 的审计，从而增强了 Novell Audit 平台代理的审计功能。它将通用 XDAS 纲要用于 Identity Manager、NMAS、eDirectory 和角色映射管理器。新的审计服务还支持 syslog 和文件追加程序。有关更多信息，请参见《[身份报告模块指南](#)》和《[Novell Sentinel 的 Identity Manager 4.0.1 报告指南](#)》。

## 10.2.4 包替换了驱动程序配置文件

Identity Manager 4.0.1 引入了包，它包含高质量的 Identity Manager 策略内容构建块。现在都使用包来创建驱动程序，而非使用驱动程序配置文件来创建。有关更多信息，请参见《[Designer 4.0.1 for Identity Manager 4.0.1 管理指南](#)》中的“[管理 Identity Manager 内容](#)”。

## 10.2.5 角色映射管理器

角色映射管理器是一个新工具，用于分析 IT 系统中可授予的授权或许可权限，并允许您授予这些授权或许可权限。授权和许可权限可由业务分析员授予，而不仅是由 IT 人员或顾问授予。有关更多信息，请参见《[Novell Identity Manager 角色映射管理器 4.0.1 用户指南](#)》。

## 10.2.6 Analyzer

Analyzer 可诊断、清理和准备身份数据，以便 Identity Manager 管理。有关更多信息，请参见《[Analyzer 4.0.1 for Identity Manager 管理指南](#)》。

## 10.2.7 集成安装程序

Identity Manager 4.0.1 提供了一个集成安装程序，使用它即可安装和配置所有 Identity Manager 组件。该安装程序用于中小型环境中的全新安装。有关更多信息，请参见《[Identity Manager 4.0.1 集成安装指南](#)》。





# 升级 Identity Manager



要升级 Identity Manager 组件，请使用用于升级到 Identity Manager 4.0.1 的各个产品安装程序。从 Identity Manager 4.0.1 Standard Edition 升级到 Advanced Edition 具有不同的升级过程，它仅涉及配置更改。不需要为此升级运行 Identity Manager 安装程序。有关 Identity Manager 升级的更多信息，请参考《[Identity Manager 4.0.1 升级和迁移指南](#)》中的“升级”部分。



# 升级与迁移

# 11

在开始前，请确保已了解升级和迁移之间的区别。请参见 《[Identity Manager 4.0.1 升级和迁移指南](#)》中的“[升级或迁移](#)”。



# 卸载 Identity Manager

# IV

如果需要完全卸载 Identity Manager，则必须卸载每个组件。

- ◆ [第 12 章“卸载 Identity Manager 组件”](#)（第 87 页）



按所列顺序卸载 Identity Manager 组件。

- ◆ 第 12.1 节“去除 eDirectory 中的对象”（第 87 页）
- ◆ 第 12.2 节“卸载元目录服务器”（第 87 页）
- ◆ 第 12.3 节“卸载 Remote Loader”（第 88 页）
- ◆ 第 12.4 节“卸载 Roles Based Provisioning Module”（第 89 页）
- ◆ 第 12.5 节“卸载身份报告模块组件”（第 90 页）
- ◆ 第 12.6 节“卸载 iManager”（第 91 页）
- ◆ 第 12.7 节“卸载 eDirectory”（第 91 页）
- ◆ 第 12.8 节“卸载 Analyzer”（第 92 页）
- ◆ 第 12.9 节“卸载 Designer”（第 92 页）
- ◆ 第 12.10 节“卸载角色映射管理器”（第 93 页）

## 12.1 去除 eDirectory 中的对象

卸载 Identity Manager 的第一步是删除身份库中的所有 Identity Manager 对象。如果任何驱动程序集对象是 eDirectory 中的分区根对象，则必须将该分区合并到父分区，然后才能删除驱动程序集对象。创建驱动程序集时，向导将提示您将该驱动程序集作为分区。

- 1 对 eDirectory 数据库执行状态检查。如果发生任何错误，请修正错误再继续。  
有关更多信息，请参见《Novell eDirectory 8.8 管理指南》中的保持 eDirectory 稳定运行 (<http://www.novell.com/documentation/edir88/edir88/data/a5ziqam.html>)。
- 2 作为对 eDirectory 树具有完全权限的管理员用户登录到 iManager。
- 3 选择分区和复本 > 合并分区。
- 4 浏览到并选择作为分区根对象的驱动程序集对象，然后单击确定。
- 5 等待合并过程完成，然后单击确定。
- 6 删除驱动程序集对象。  
删除驱动程序集对象时，将删除与该驱动程序集相关联的所有驱动程序对象。
- 7 对 eDirectory 数据库中的每个驱动程序集对象重复步骤 3 到步骤 6，直到将它们全部删除。
- 8 重复步骤 1 以确保所有合并均已完成，且所有对象均已删除。

## 12.2 卸载元目录服务器

安装 Identity Manager 时，在 Identity Manager 服务器上放置了一个卸载脚本。使用该脚本可去除安装 Identity Manager 时创建的所有服务、包和目录。

- ◆ 第 12.2.1 节“在 Linux/UNIX 上卸载”（第 88 页）

- ◆ 第 12.2.2 节“在 Windows 上卸载”（第 88 页）
- ◆ 第 12.2.3 节“卸载非根安装”（第 88 页）

## 12.2.1 在 Linux/UNIX 上卸载

要在 Linux/UNIX 上卸载 Identity Manager，请运行位于 `/root/idm/Uninstall_Identity_Manager/Uninstall_Identity_Manager` 的卸载脚本。要执行脚本，请输入 `./Uninstall_Identity_Manager`。

如果是非根用户身份安装的 Identity Manager，则 `idm` 目录位于安装 Identity Manager 的用户的目录中。

## 12.2.2 在 Windows 上卸载

对于每个受支持的 Windows 平台，卸载元目录服务器的过程都不同。

- ◆ **Windows 2003 SP2（32 位和 64 位）**：在控制面板中选择 **添加或删除程序** > *Identity Manager*，然后单击 **更改/删除**。
- ◆ **Windows 2008 SP1（32 位和 64 位）**：单击 **程序和功能** > *Identity Manager*，然后右键单击并选择 **卸载**。

## 12.2.3 卸载非根安装

要卸载 Identity Manager 的非根安装，需要以安装 Identity Manager 的用户身份运行卸载脚本。它位于 `leDirectory 基本目录/opt/novell/eDirectory/bin/idm-uninstall`。

该脚本清理 Identity Manager 安装期间创建的用户 rpm 数据库。

## 12.3 卸载 Remote Loader

安装 Remote Loader 后，Remote Loader 服务器上有一个卸载脚本。它可以去除在安装 Remote Loader 时创建的所有服务、包和目录。

- ◆ 第 12.3.1 节“在 Linux/UNIX 上卸载”（第 88 页）
- ◆ 第 12.3.2 节“在 Windows 上卸载”（第 88 页）

### 12.3.1 在 Linux/UNIX 上卸载

要在 Linux/UNIX 上卸载 Remote Loader，请运行位于 `/root/idm/Uninstall_Identity_Manager/Uninstall_Identity_Manager` 的卸载脚本。要执行脚本，请输入 `./Uninstall_Identity_Manager`。

如果是非根用户身份安装的 Remote Loader，则 `idm` 目录位于安装 Remote Loader 的用户的目录中。

### 12.3.2 在 Windows 上卸载

对于每个受支持的 Windows 平台，卸载 Remote Loader 的过程都不同。

- ◆ **Windows 2003 SP2（32 位和 64 位）**：在控制面板中选择 **添加或删除程序** > *Identity Manager*，然后单击 **更改/删除**。



- ◆ **Windows 2008 SP1 (32 位和 64 位)**: 单击 *程序和功能* > *Identity Manager*, 然后右键单击并选择 *卸载*。

## 12.4 卸载 Roles Based Provisioning Module

Roles Based Provisioning Module 包含多个组件, 每个组件都必须卸载。

- ◆ 第 12.4.1 节 “删除驱动程序” (第 89 页)
- ◆ 第 12.4.2 节 “卸载 User Application” (第 89 页)
- ◆ 第 12.4.3 节 “卸载应用程序服务器和数据库” (第 89 页)

### 12.4.1 删除驱动程序

必须删除 User Application 驱动程序及 Role and Resource Service 驱动程序。

- 1 停止 User Application 驱动程序及 Role and Resource Service 驱动程序。
  - ◆ **Designer**: 右键单击驱动程序行, 然后单击 *在线* > *停止驱动程序*。
  - ◆ **iManager**: 在 “驱动程序集概述” 页上, 单击右上角的驱动程序, 然后单击 *停止驱动程序*。
- 2 删除 User Application 驱动程序及 Role and Resource Service 驱动程序。
  - ◆ **Designer**: 右键单击驱动程序行, 然后单击 *删除*。
  - ◆ **iManager**: 在 “驱动程序集概述” 页上, 单击 *驱动程序* > *删除驱动程序*, 然后单击要删除的驱动程序。

### 12.4.2 卸载 User Application

- ◆ **Linux/UNIX**: 执行位于 `/root/Roles_Based_Provisioning_Module_for_Novell_Identity_Manager/Uninstall Roles Based Provisioning Module for Novell Identity Manager` 的卸载脚本。

要执行脚本, 请输入 `./Uninstall\ Roles\ Based\ Provisioning\ Module\ for\ Novell\ Identity\ Manager`。
- ◆ **Windows**: 对于每个受支持的 Windows 平台, 卸载 User Application 的过程都不同。
  - ◆ **Windows 2003 SP2 (32 位和 64 位)**: 在控制面板中选择 *添加或删除程序* > *Roles Based Provisioning Module*, 然后单击 *更改/删除*。
  - ◆ **Windows 2008 SP1 (32 位和 64 位)**: 单击 *程序和功能* > *Roles Based Provisioning Module*, 然后右键单击并选择 *卸载*。

### 12.4.3 卸载应用程序服务器和数据库

User Application 在以下应用程序服务器和数据库上运行。

表 12-1 受支持的应用程序服务器和数据库

应用程序服务器	数据库
JBoss 5.1.0	<ul style="list-style-type: none"><li>◆ MS SQL 2008</li><li>◆ MySQL V5.1</li><li>◆ Oracle 11gR2</li><li>◆ PostgreSQL 8.4.3</li></ul>
WebSphere 7.0	<ul style="list-style-type: none"><li>◆ DB2 9.5b</li><li>◆ MS SQL 2008</li><li>◆ Oracle 11gR2</li><li>◆ PostgreSQL 8.4.3</li></ul>
WebLogic 10.3	<ul style="list-style-type: none"><li>◆ MS SQL 2008</li><li>◆ Oracle 11gR2</li><li>◆ PostgreSQL 8.4.3</li></ul>

以下过程说明了如何卸载 JBoss 和 PostgreSQL。如果使用的是其他应用程序服务器和数据库，请参考该产品的文档获取说明。

- ◆ **Linux/UNIX:** 执行位于 /opt/novell/idm/Postgres/JPossPostgreSQL\_Uninstaller/Uninstall\_JBossPostgreSQL 的卸载脚本。  
要执行脚本，请输入 ./Uninstall\_JBossPostgreSQL。
- ◆ **Windows:** 对于每个受支持的 Windows 平台，卸载 JBoss 和 PostgreSQL 的过程都不同。
  - ◆ **Windows 2003 SP2 (32 位和 64 位):** 在控制面板中选择 *添加或删除程序* > *JPossPostgreSQL*，然后单击 *更改/删除*。
  - ◆ **Windows 2008 SP1 (32 位和 64 位):** 单击 *程序和功能* > *JPossPostgreSQL*，然后右键单击并选择 *卸载*。

## 12.5 卸载身份报告模块组件

身份报告模块由多个组件组成。要卸载身份报告模块，就必须卸载每个组件。

- ◆ 第 12.5.1 节“删除报告驱动程序”（第 90 页）
- ◆ 第 12.5.2 节“卸载身份报告模块”（第 91 页）
- ◆ 第 12.5.3 节“卸载事件审计服务”（第 91 页）

### 12.5.1 删除报告驱动程序

必须删除数据收集驱动程序和受管系统网关驱动程序。

- 1 停止数据收集驱动程序和受管系统网关驱动程序。
  - ◆ **Designer:** 右键单击驱动程序行，然后单击 *在线* > *停止驱动程序*。
  - ◆ **iManager:** 在“驱动程序集概述”页上，单击右上角的驱动程序，然后单击 *停止驱动程序*。

2 删除数据收集驱动程序和受管系统网关驱动程序。

- ◆ **Designer:** 右键单击驱动程序行，然后单击 *删除*。
- ◆ **iManager:** 在“驱动程序集概述”页上，单击 *驱动程序* > *删除驱动程序*，然后单击要删除的驱动程序。

## 12.5.2 卸装身份报告模块

- ◆ **Linux:** 执行位于 `/opt/novell/IdentityReporting/Uninstall_Identity Reporting` 的卸装脚本。  
要执行脚本，请输入 `./Uninstall\ Identity\ Reporting`。
- ◆ **Windows:** 对于每个受支持的 Windows 平台，卸装身份报告模块的过程都不同。
  - ◆ **Windows 2003 SP2 (32 位和 64 位):** 在控制面板中选择 *添加或删除程序* > *Identity Reporting*，然后单击 *更改/删除*。
  - ◆ **Windows 2008 SP1 (32 位和 64 位):** 单击 *程序和功能* > *Identity Reporting*，然后右键单击并选择 *卸载*。

## 12.5.3 卸装事件审计服务

事件审计服务 (EAS) 仅在 Linux 上受支持。执行位于 `/opt/novell/sentinel_eas/Uninstall_Event Auditing Service/Uninstall Event Auditing Service` 的卸装脚本。要执行脚本，请输入 `./Uninstall\ Event\ Auditing\ Service`。

## 12.6 卸装 iManager

- ◆ **Linux:** 以根身份执行位于 `/var/opt/novell/iManager/nps/UninstallerData/UninstalliManager` 的卸装脚本。  
要执行脚本，请输入 `./UninstalliManager`。
- ◆ **Windows:** 对于每个受支持的 Windows 平台，卸装 iManager 的过程都不同。
  - ◆ **Windows 2003 SP2 (32 位和 64 位):** 在控制面板中选择 *添加或删除程序* > *Novell iManager*，然后单击 *更改/删除*。
  - ◆ **Windows 2008 SP1 (32 位和 64 位):** 单击 *程序和功能* > *Novell iManager*，然后右键单击并选择 *卸载*。

Tomcat 和 NICI 在控制面板中列为独立项。如果不再使用这两个程序，可以将它们卸装。如果 eDirectory 与它们安装在同一服务器上，则 eDirectory 需要 NICI 才能继续运行。如果不卸装 eDirectory，就不要卸装 NICI。

## 12.7 卸装 eDirectory

在卸装 eDirectory 前，需要了解 eDirectory 树型结构和复本布局，这样才不会在 eDirectory 树中导致问题。

请在卸装 eDirectory 前回答以下问题：

- 树中是否有多个服务器？

如果回答是，请继续回答列表中的其他问题。如果回答否，则可以去除 eDirectory。

- 该服务器是否保存了任何主复本？

如果回答是，则需要将复本环中的其他服务器提升为主，然后才能去除 eDirectory。有关更多信息，请参见《Novell eDirectory 8.8 管理指南》中的“管理分区和复本”(<http://wwwtest.provo.novell.com/documentation/edir88/edir88/data/a2iiiik.html>)。

- 该服务器是否保存了某分区的唯一副本？

如果回答是，则必须将该分区合并到父分区中，或将该分区的复本添加到其他服务器中并使其成为主复本保存者。有关更多信息，请参见《Novell eDirectory 8.8 管理指南》中的“管理分区和复本”(<http://wwwtest.provo.novell.com/documentation/edir88/edir88/data/a2iiiik.html>)。

确保准备好 eDirectory 树后，请使用以下过程卸载 eDirectory：

- 1 如果这是单服务器树，请跳到步骤 2。否则，对 eDirectory 数据库执行状态检查。如果发生任何错误，请修正错误再继续。有关更多信息，请参见《Novell eDirectory 8.8 管理指南》中的“保持 eDirectory 稳定运行”(<http://www.novell.com/documentation/edir88/edir88/data/a5ziqam.html>)。
- 2 卸载 eDirectory。
  - ◆ **Linux/UNIX：** 执行位于 /opt/novell/eDirectory/sbin/nds-uninstall 的卸载脚本。  
要执行脚本，请输入 ./nds-uninstall。
  - ◆ **Windows：** 对于每个受支持的 Windows 平台，卸载 eDirectory 的过程都不同。
    - ◆ **Windows 2003 SP2 (32 位和 64 位)：** 在控制面板中选择添加或删除程序 > Novell eDirectory，然后单击更改 / 删除。
    - ◆ **Windows 2008 SP1 (32 位和 64 位)：** 单击程序和功能 > Novell eDirectory，然后右键单击并选择卸载。
- 3 (视具体情况而定) 如果这是多服务器树，请删除树中剩余的所有特定于服务器的对象，然后再次执行状态检查。这可校验服务器是否已从树中正常去除。  
有关更多信息，请参见《Novell eDirectory 8.8 管理指南》中的“保持 eDirectory 稳定运行”(<http://www.novell.com/documentation/edir88/edir88/data/a5ziqam.html>)。

## 12.8 卸载 Analyzer

- 1 确保 Analyzer 已关闭。
- 2 要卸载 Analyzer：
  - ◆ **Linux：** 执行位于 <安装目录>/analyzer/UninstallAnalyzer/Uninstall Analyzer for Identity Manager 的卸载脚本。  
要执行脚本，请输入 ./Uninstall\ Analyzer\ for\ Identity\ Manager。
  - ◆ **Windows：** 对于每个受支持的 Windows 平台，卸载 Analyzer 的过程都不同。
    - ◆ **Windows 2003 SP2 (32 位和 64 位)：** 在控制面板中选择添加或删除程序 > Analyzer for Identity Manager，然后单击更改 / 删除。
    - ◆ **Windows 2008 SP1 (32 位和 64 位)：** 单击程序和功能 > Analyzer for Identity Manager，然后右键单击并选择卸载。

## 12.9 卸载 Designer

- 1 确保 Designer 已关闭。

## 2 要卸载 Designer:

- ◆ **Linux/UNIX:** 执行位于 < 安装目录 >/designer/UninstallDesigner/Uninstall Designer for Identity Manager 的卸载脚本。  
要执行脚本, 请输入 `./Uninstall\ Designer\ for\ Identity\ Manager`。
- ◆ **Windows:** 对于每个受支持的 Windows 平台, 卸载 Designer 的过程都不同。
  - ◆ **Windows 2003 SP2 (32 位和 64 位):** 在控制面板中选择 *添加或删除程序* > *Designer for Identity Manager*, 然后单击 *更改/删除*。
  - ◆ **Windows 2008 SP1 (32 位和 64 位):** 单击 *程序和功能* > *Designer for Identity Manager*, 然后右键单击并选择 *卸载*。

## 12.10 卸载角色映射管理器

### 1 访问角色映射管理器的安装目录。

该目录是在安装期间定义的, 所以对于各个安装可能会不同。

### 2 从命令行运行 stop 脚本来停止角色映射管理器。

- ◆ **Linux:** stop.sh  
要执行脚本, 请输入 `./stop.sh`
- ◆ **Windows:** stop.bat

### 3 从命令行运行卸载脚本。

- ◆ **Linux:** rma-uninstall.sh [-h] [-s]
  - ◆ [-h]: 指定帮助。
  - ◆ [-s]: 指定无提示模式。要执行脚本, 请输入 `./rma-uninstall.sh`。
- ◆ **Windows:** rma-uninstall.bat [-h] [-s]

### 4 删除安装目录。

