

## 安装指南

# Novell® Identity Manager

**3.6.1**

2009 年 5 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 Novell 软件出口的详细信息，请参见 [International Trade Services \(http://www.novell.com/company/policies/trade\\_services\)](http://www.novell.com/company/policies/trade_services)。如果您未能获得任何必要的出口许可，则 Novell 对此概不负责。

版权所有 © 2007-2009 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存储在检索系统上。

Novell, Inc. 拥有与本文档所述产品中包含的技术相关的知识产权。特别是，这些知识产权包括但不限于 [Novell Legal Patents 网页 \(http://www.novell.com/company/legal/patents/\)](http://www.novell.com/company/legal/patents/) 中列出的一项或多项美国专利，以及美国和其他国家 / 地区的一项或多项其他专利或正在申请的专利。

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	9
<b>I 规划</b>	<b>11</b>
<b>1 建立开发环境</b>	<b>13</b>
<b>2 创建项目计划</b>	<b>15</b>
2.1 发现阶段	15
2.1.1 定义当前业务流程	15
2.1.2 定义 Identity Manager 解决方案影响当前业务流程的方式	16
2.1.3 确定关键的业务和技术利害关系人	17
2.1.4 与所有利害关系人面谈	17
2.1.5 创建高级别策略和达成一致的执行途径	17
2.2 需求和设计分析阶段	18
2.2.1 定义业务需求	19
2.2.2 分析业务流程	19
2.2.3 设计企业数据模型	20
2.3 概念检验	21
2.4 数据验证和准备	22
2.5 试生产	22
2.6 生产试点规划	22
2.7 生产部署	23
<b>3 技术准则</b>	<b>25</b>
3.1 管理工具准则	25
3.1.1 Designer 准则	26
3.1.2 iManager 准则	26
3.2 元目录服务器准则	27
3.3 eDirectory 准则	28
3.3.1 eDirectory 中的 Identity Manager 对象	28
3.3.2 在服务器上复制 Identity Manager 需要的对象	28
3.3.3 使用“范围过滤”管理不同服务器上的用户	29
3.4 User Application	31
3.5 审计和报告准则	32
<b>II 安装</b>	<b>35</b>
<b>4 基本 Identity Manager 系统核对清单</b>	<b>37</b>
4.1 先决条件	37
4.2 规划	38
4.3 安装	38
4.4 带有 Remote Loader 的驱动程序配置	38
4.5 不带 Remote Loader 的驱动程序配置	39
4.6 其他配置	39

<b>5</b>	<b>从何处获取 Identity Manager</b>	<b>41</b>
<b>6</b>	<b>系统要求</b>	<b>43</b>
6.1	eDirectory 和 iManager	43
6.2	元目录服务器	44
6.2.1	支持的处理器	45
6.2.2	服务器操作系统	45
6.3	Remote Loader	46
6.4	User Application	48
6.5	审计和报告	48
6.6	工作站	49
6.6.1	工作站平台	49
6.6.2	iManager 和 Web 浏览器	50
<b>7</b>	<b>安装 Identity Manager</b>	<b>51</b>
7.1	安装 Designer	51
7.2	安装元目录服务器	51
7.2.1	元目录服务器的非根安装	53
7.2.2	元目录服务器的无提示安装	54
7.3	安装 Remote Loader	54
7.3.1	要求	55
7.3.2	支持的驱动程序	55
7.3.3	安装过程	56
7.3.4	Remote Loader 的无提示安装	57
7.3.5	在 UNIX、Linux 或 AIX 上安装 Java Remote Loader	58
7.4	安装基于角色的供应模块	59
7.5	安装自定义驱动程序	59
7.6	安装 Identity Audit 或 Sentinel	59
7.7	在群集环境中安装 Identity Manager	59
<b>8</b>	<b>激活 Novell Identity Manager 产品</b>	<b>61</b>
8.1	购买 Identity Manager 产品许可证	61
8.2	安装产品激活身份凭证	61
8.3	查看 Identity Manager 和驱动程序的产品激活	62
<b>9</b>	<b>Identity Manager 查错</b>	<b>63</b>
<b>III</b>	<b>升级</b>	<b>65</b>
<b>10</b>	<b>新增功能</b>	<b>67</b>
10.1	支持 64 位操作系统	67
10.2	支持在 64 位操作系统上安装 32 位 Remote Loader	67
<b>11</b>	<b>受支持的升级版本和系统要求</b>	<b>69</b>
11.1	受支持的升级版本	69
11.2	系统要求	69

<b>12 就地升级与迁移</b>	<b>71</b>
12.1 就地升级	71
12.2 迁移	71
12.3 与单个驱动程序集相关联的多个服务器	72
<b>13 执行就地升级</b>	<b>73</b>
13.1 创建当前配置的备份	74
13.1.1 确保 Designer 项目是最新的	75
13.1.2 创建驱动程序的导出	76
13.2 停止驱动程序	77
13.2.1 使用 Designer 停止驱动程序	77
13.2.2 使用 iManager 停止驱动程序	77
13.3 在 Linux/UNIX 平台上将文件添加到正确位置	77
13.4 升级 Designer	78
13.5 升级元目录引擎和驱动程序配置文件	78
13.6 升级 Remote Loader	79
13.7 用新的驱动程序配置文件覆盖现有驱动程序	79
13.7.1 使用 Designer 用新驱动程序配置文件覆盖现有驱动程序	79
13.7.2 使用 iManager 用新驱动程序配置文件覆盖现有驱动程序	80
13.8 将自定义策略和规则恢复为驱动程序	80
13.8.1 使用 Designer 将自定义策略和规则恢复为驱动程序	80
13.8.2 使用 iManager 将自定义策略和规则恢复为驱动程序	81
13.9 部署已转换的项目	82
13.10 启动驱动程序	82
13.10.1 使用 Designer 启动驱动程序	82
13.10.2 使用 iManager 启动驱动程序	82
<b>14 执行迁移</b>	<b>85</b>
14.1 将该新服务器添加到驱动程序集中	86
14.2 更改特定于服务器的信息	86
14.2.1 在 Designer 中更改特定于服务器的信息	87
14.2.2 在 iManager 中更改特定于服务器的信息	87
14.3 从驱动程序集中去除旧服务器	88
14.3.1 使用 Designer 从驱动程序集中去除旧服务器	88
14.3.2 使用 iManager 从驱动程序集中去除旧服务器	88
14.3.3 弃用旧服务器	88
<b>IV 卸载 Identity Manager</b>	<b>89</b>
<b>15 去除 eDirectory 中的对象</b>	<b>91</b>
<b>16 卸载元目录服务器和驱动程序</b>	<b>93</b>
16.1 在 Windows 上卸载	93
16.2 在 Linux/UNIX 上卸载	93
<b>17 卸载 Designer</b>	<b>95</b>



# 关于本指南

Novell® Identity Manager 是一种数据共享和同步服务，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 11 页）
  - ◆ 第 2 章“创建项目计划”（第 15 页）
  - ◆ 第 3 章“技术准则”（第 25 页）
- ◆ 第 II 部分“安装”（第 35 页）
  - ◆ 第 4 章“基本 Identity Manager 系统核对清单”（第 37 页）
  - ◆ 第 5 章“从何处获取 Identity Manager”（第 41 页）
  - ◆ 第 6 章“系统要求”（第 43 页）
  - ◆ 第 7 章“安装 Identity Manager”（第 51 页）
  - ◆ 第 8 章“激活 Novell Identity Manager 产品”（第 61 页）
- ◆ 第 III 部分“升级”（第 65 页）
  - ◆ 第 10 章“新增功能”（第 67 页）
  - ◆ 第 11 章“受支持的升级版本和系统要求”（第 69 页）
  - ◆ 第 12 章“就地升级与迁移”（第 71 页）
  - ◆ 第 13 章“执行就地升级”（第 73 页）
  - ◆ 第 14 章“执行迁移”（第 85 页）
- ◆ 第 IV 部分“卸载 Identity Manager”（第 89 页）
  - ◆ 第 15 章“去除 eDirectory 中的对象”（第 91 页）
  - ◆ 第 16 章“卸载元目录服务器和驱动程序”（第 93 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 \(http://www.novell.com/documentation/idm361/index.html\)](http://www.novell.com/documentation/idm361/index.html)。

## 其他文档

有关其他 Identity Manager 文档，请参见 [Identity Manager 文档网站 \(http://www.novell.com/documentation/idm361/index.html\)](http://www.novell.com/documentation/idm361/index.html)。

有关 User Application 文档，请参见 [Identity Manager 基于角色的供应模块文档网站 \(http://www.novell.com/documentation/idmrbpm361/index.html\)](http://www.novell.com/documentation/idmrbpm361/index.html)。

## 文档约定

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

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

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

# 规划

Identity Manager 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 3.6.1 概述指南*》以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，首先必须花点时间来规划和设计 Identity Manager 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，这样就可在环境中有效实施。

强烈建议聘请一个 Identity Manager 专家，便于在 Identity Manager 实施的每个阶段随时提供帮助。有关合作伙伴关系选项的更多信息，请参见 Novell® 解决方案合作伙伴网站 (<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 13 页）
- ◆ 第 2 章“创建项目计划”（第 15 页）
- ◆ 第 3 章“技术准则”（第 25 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和因素。

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。通过更改要在这两个系统间同步的数据，您可查看是否此更改会影响使用此相同信息的其他系统。

建立开发环境的另一主要原因是为了确保解决方案起作用，同时不会影响在线数据。Identity Manager 可操纵数据，包括删除数据。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。在整个规划期间均使用 Designer 来捕获所有信息。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 3.0.1 for Identity Manager 3.6 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 37 页）中的信息。其中是一个所有 Identity Manager 组件的安装核对清单。使用此核对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 25 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 15 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 项目的活动类型，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 15 页）
- ◆ 第 2.2 节“需求和设计分析阶段”（第 18 页）
- ◆ 第 2.3 节“概念检验”（第 21 页）
- ◆ 第 2.4 节“数据验证和准备”（第 22 页）
- ◆ 第 2.5 节“试生产”（第 22 页）
- ◆ 第 2.6 节“生产试点规划”（第 22 页）
- ◆ 第 2.7 节“生产部署”（第 23 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 15 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 16 页）
- ◆ 第 2.1.3 节“确定关键的业务和技术利害关系人”（第 17 页）
- ◆ 第 2.1.4 节“与所有利害关系人面谈”（第 17 页）
- ◆ 第 2.1.5 节“创建高级别策略和达成一致的执行途径”（第 17 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 3.0.1 for Identity Manager 3.6 管理指南*》中的“体系结构方式”。

以下是一些业务流程示例：

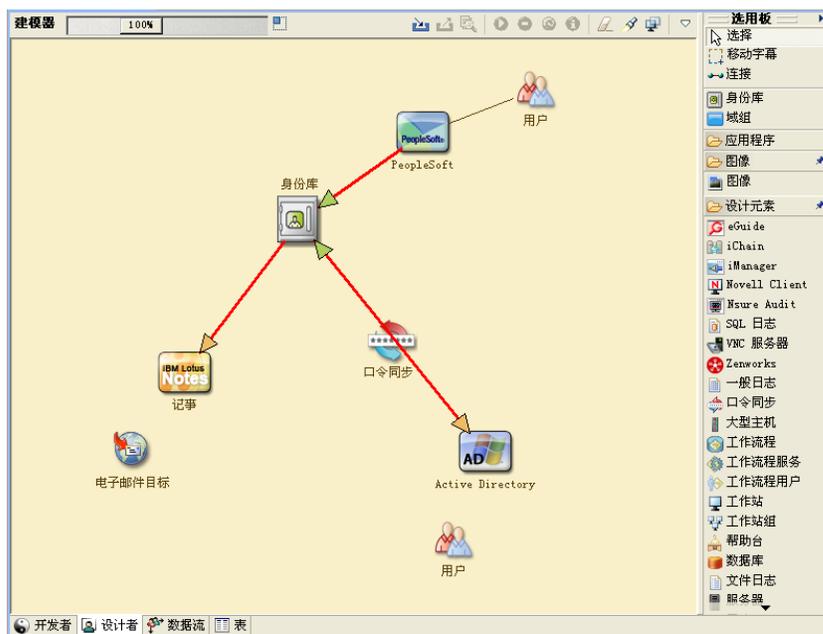
- ◆ 解雇某个员工时，删除电子邮件系统中的该用户帐户，但在所有其他系统中禁用（而非删除）该用户的帐户。
- ◆ 用户电子邮件地址的格式。
- ◆ 销售人员可访问的系统或资源。
- ◆ 经理可访问的系统或资源。
- ◆ 哪些系统生成新帐户？是人力资源系统还是通过工作流程请求？
- ◆ 公司的口令策略，定义口令更改的频率、口令的复杂程度以及同步口令的系统。

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别概述。例如，图 2-1 来自 Designer，显示了新用户帐户是从 PeopleSoft\* 系统生成的。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



下一步在第 2.1.2 节“定义 Identity Manager 解决方案影响当前业务流程的方式”（第 16 页）中。

## 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。下一步在 [第 2.1.3 节“确定关键的业务和技术利害关系人”](#)（第 17 页）中。

### 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 3.0.1 for Identity Manager 3.6 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 17 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 17 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）。这允许您：

- ◆ 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，分析阶段需要利害关系人对目录、Novell eDirectory™、Novell Identity Manager 和 XML 集成具有基本的了解。

完成发现阶段后，请转到第 2.2 节“需求和设计分析阶段”（第 18 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，则可能无法根据需求实施业务策略。）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。

请查看第 3 章“技术准则”（第 25 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 19 页）
- ◆ 分析业务流程（第 19 页）
- ◆ 设计企业数据模型（第 20 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，如果某事件将在特定过程中发生，那么该过程会导致什么结果？将会触发其他哪些流程？

- ◆ 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 3.0.1 for Identity Manager 3.6 管理指南*》中的“[管理数据流](#)”。

- ◆ 确定从一种格式转换为另一种格式（例如 2/25/2007 转换为 2007 年 2 月 25 日）需要执行的数据转换。

- ◆ 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。

将部署划分为多个阶段是很有利的，这样可以先实施部署的某一部分，然后实施部署的其他部分。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 19 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，人力资源部的 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 / 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它区域，这样可以更清楚地展现整个过程。

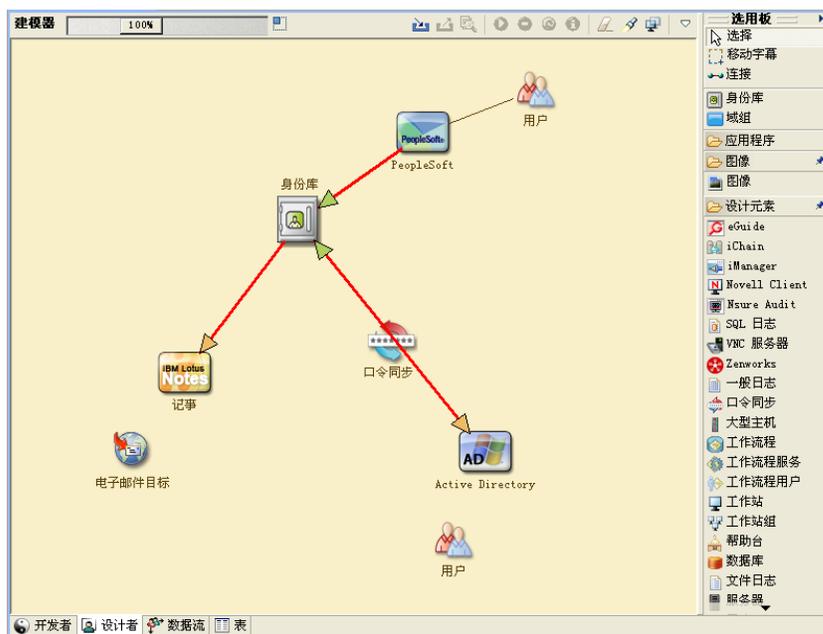
收集所有此类信息后，即可为您的环境设计正确的企业数据模型。请转到第 2.2.3 节“设计企业数据模型”（第 20 页）以开始设计。

## 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“概念检验”（第 21 页）。

## 2.3 概念检验

此活动的结果是提供一份实验室环境中的实施样本，用于反映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。

---

第 3 章“技术准则”（第 25 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 22 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。

您需要具有已在分析和设计阶段完成的数据模型。您还应定义建议的记录匹配和数据格式以便正确地准备数据。定义数据模型和格式策略后，您可以：

- ◆ 创建适合装载进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程序装载）。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 22 页）。

## 2.5 试生产

此活动的目的是开始执行到生产环境的迁移。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 22 页）。

## 2.6 生产试点规划

在此阶段中规划生产部署。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 23 页）。

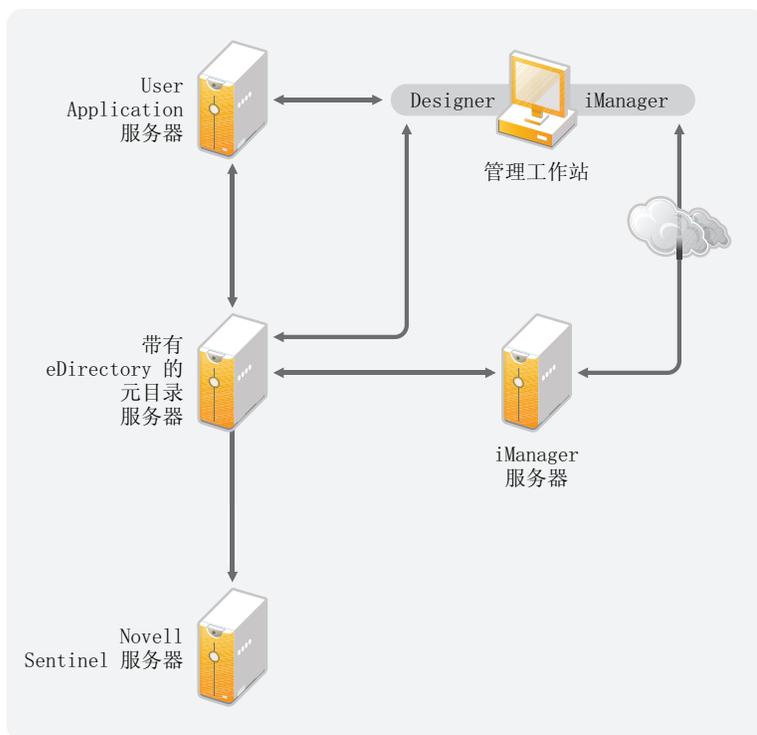
## 2.7 生产部署

生产部署阶段将所有计划付诸于操作，且 Identity Manager 解决方案在在线环境中创建。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。这可能要花费一夜时间，或在更长的时间段内进行。具体取决于计划包含的内容。



借助在 Designer 中收集的信息，您可做出有关 Identity Manager 的各个组件的技术决策，如安装位置和配置选项。有关各个组件的介绍，请参见《*Identity Manager 3.6.1 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



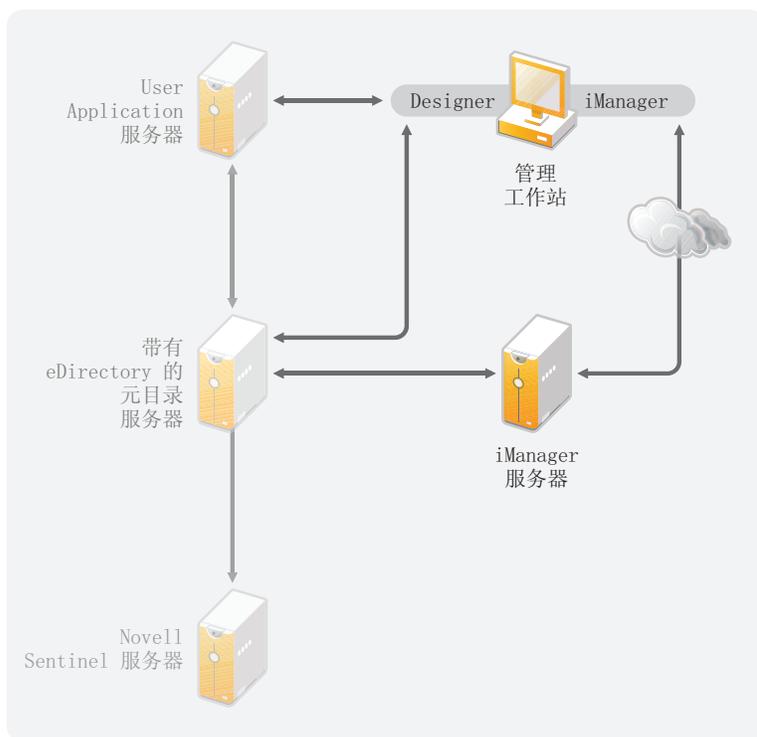
Identity Manager 的自定义程度很高。以下部分包含技术最佳实践准则，可帮助您建立并配置为您的环境提供最佳服务的 Identity Manager 解决方案。影响这些准则对环境的适用程度的可变因素包括：服务器具有的硬件类型、WAN 的配置方式以及正在同步的对象数量。

- ◆ [第 3.1 节“管理工具准则”](#)（第 25 页）
- ◆ [第 3.2 节“元目录服务器准则”](#)（第 27 页）
- ◆ [第 3.3 节“eDirectory 准则”](#)（第 28 页）
- ◆ [第 3.4 节“User Application”](#)（第 31 页）
- ◆ [第 3.5 节“审计和报告准则”](#)（第 32 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



本文档仅包含有关 Designer 和 iManager 的信息。User Application 使用基于 Web 的管理页面（此处不讨论）。有关 User Application 的更多信息，请参见《User Application 管理指南》中的“管理 User Application (<http://www.novell.com/documentation/idmr/bpm361/agpro/data/agpropartadminapp.html>)”。

- ◆ 第 3.1.1 节“Designer 准则”（第 26 页）
- ◆ 第 3.1.2 节“iManager 准则”（第 26 页）

### 3.1.1 Designer 准则

Designer 是一个安装在工作站上的富客户端。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 3.0.1 for Identity Manager 3.6 管理指南》中的“版本控制”。

### 3.1.2 iManager 准则

iManager 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 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。

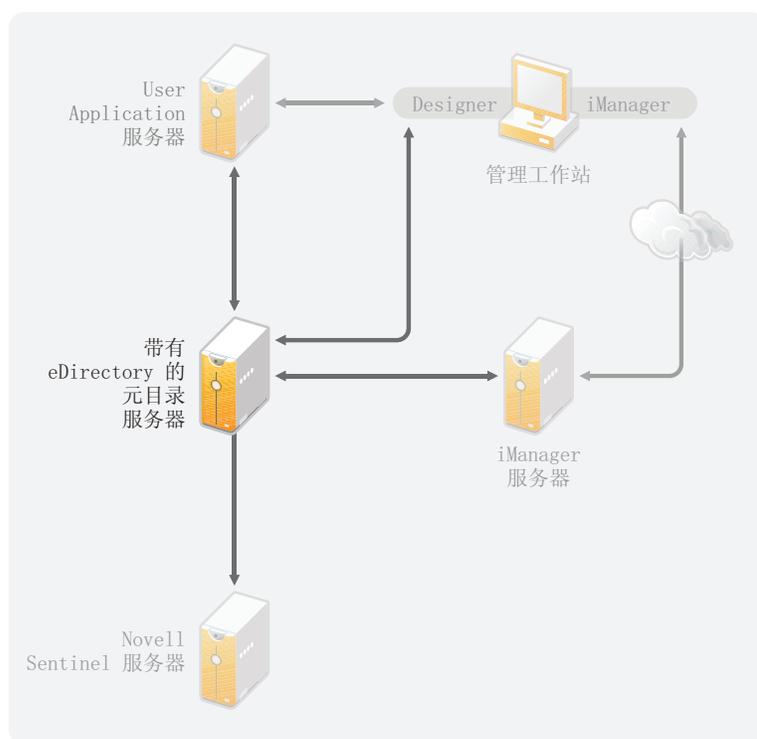
## 3.2 元目录服务器准则

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 3.6.1 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 3.6.1 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 \(http://www.novell.com/documentation/idm36drivers/index.html\)](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 28 页）
- ◆ 第 3.3.2 节“在服务器上复制 Identity Manager 需要的对象”（第 28 页）
- ◆ 第 3.3.3 节“使用“范围过滤”管理不同服务器上的用户”（第 29 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引擎。
- ◆ **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。可将策略放置在驱动程序集中的每个驱动程序均可参照的库中。
- ◆ **驱动程序：**驱动程序连接应用程序与身份库。驱动程序是实现系统间的数据同步和共享的连接器。驱动程序存储在驱动程序集中。
- ◆ **作业：**作业的用途是完成多次出现的任务。例如，某个作业可以将系统配置为在特定一天禁用帐户，或启用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 环境访问多个服务器以运行多个 Identity Manager 驱动程序，那么规划时要确保在运行这些 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 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：**当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 29 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”的容器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容器的主复本或读 / 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。

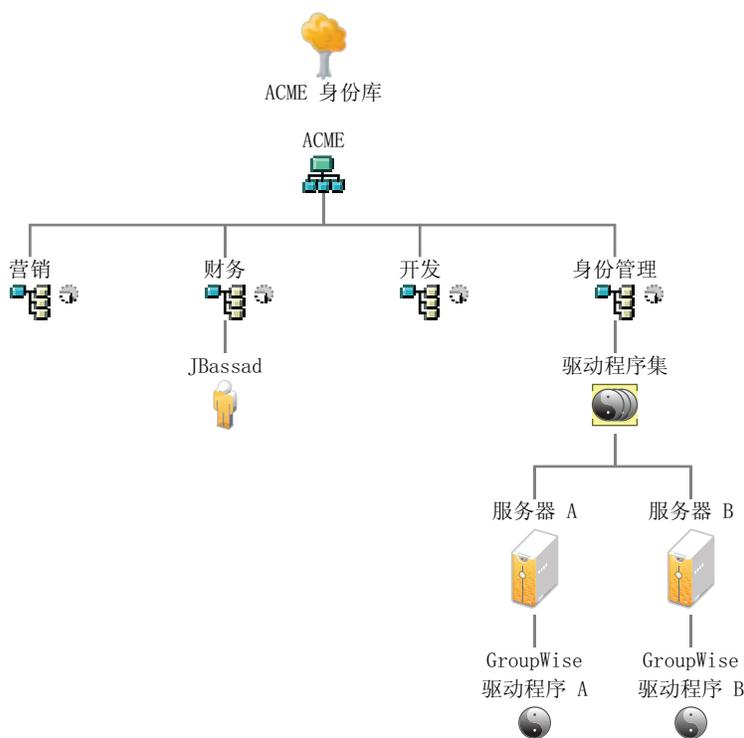
要同步所有用户且不将其复制到单台服务器上，则需要确定由哪个服务器集保存所有用户，然后在其中的每台服务器上创建 **Identity Manager** 驱动程序的实例。为防止驱动程序的两个实例尝试与相同的用户同步，您将需要使用“范围过滤”来定义驱动程序的每个实例应该同步的用户。

**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 31 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。

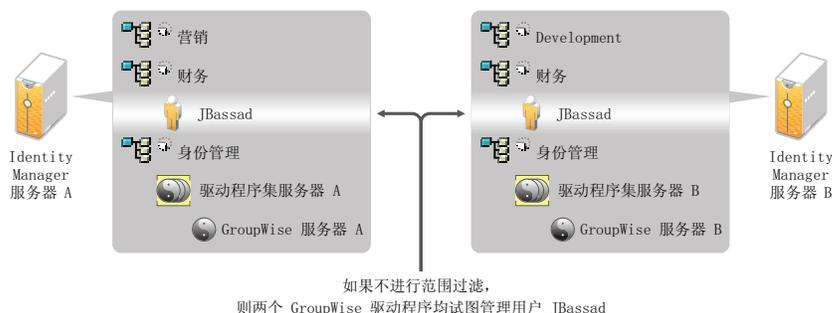
管理员希望通过 **GroupWise**<sup>®</sup> 驱动程序同步树中的所有用户，但是不希望将这些用户的复本聚合到单台服务器。他选择使用 **GroupWise** 驱动程序的两个实例，每台服务器使用一个。他在每台 **Identity Manager** 服务器上安装 **Identity Manager**，然后设置 **GroupWise** 驱动程序。

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。

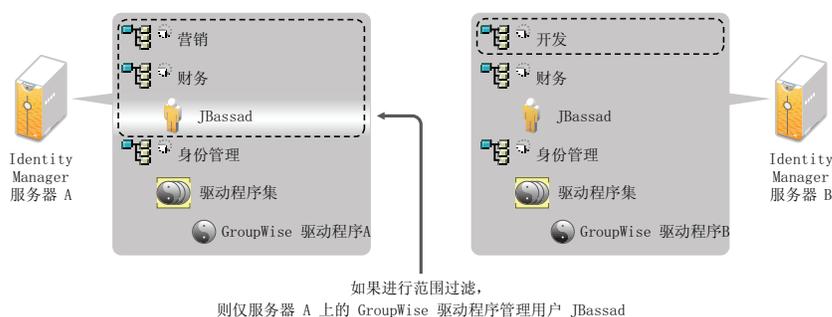
由于服务器 A 和服务器 B 均保存了“财务”容器的复本，因此这两个服务器均保存了“财务”容器中的用户 JBassad。如果不使用范围过滤， GroupWise 驱动程序 A 和 GroupWise 驱动程序 B 都会同步 JBassad。

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由哪些驱动程序同步每个容器，因此它可以防止驱动程序的两个实例管理相同的用户。

图 3-6 范围过滤定义由哪些驱动程序同步每个容器



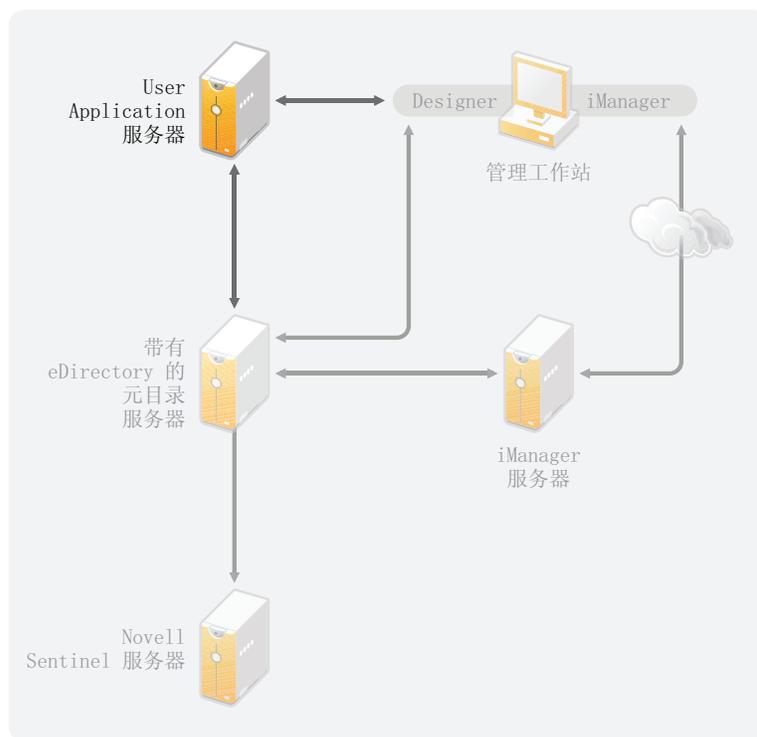
Identity Manager 3.6.1 附带一些预定义的规则。有两个规则可帮助执行范围过滤。“事件转换 — 范围过滤 — 包含子树”和“事件转换 — 范围过滤 — 不包含子树”在《[了解 Identity Manager 3.6 的策略](#)》中有所论述。

对于此示例，可以对服务器 A 和服务器 B 使用“包含子树”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



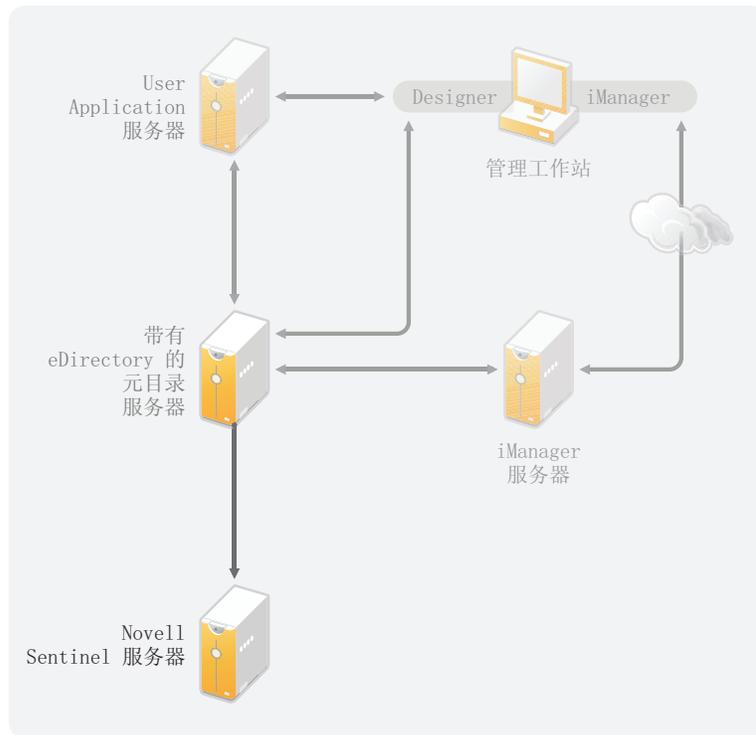
使用《User Application 管理指南》的“性能调优 (<http://www.novell.com/documentation/idmrpbm361/agpro/data/b2gx735.html>)”部分中的信息来确定如何最佳配置 User Application 服务器。

如果 User Application 服务器非常繁忙，您可能需要考虑对 User Application 服务器使用群集。群集有助于实现高可用性、可伸缩性和负载平衡。有关更多信息，请参见《User Application 管理指南》中的“群集 (<http://www.novell.com/documentation/idmrpbm361/agpro/data/b2gx73a.html>)”。

### 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™。建议您在各自所位于的服务器上运行 Identity Audit 或 Sentinel，如图 3-8 中所示。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



以下部分包含安装 Identity Manager 系统所需的信息。

- ◆ 第 4 章“基本 Identity Manager 系统核对清单”（第 37 页）
- ◆ 第 5 章“从何处获取 Identity Manager”（第 41 页）
- ◆ 第 6 章“系统要求”（第 43 页）
- ◆ 第 7 章“安装 Identity Manager”（第 51 页）
- ◆ 第 8 章“激活 Novell Identity Manager 产品”（第 61 页）
- ◆ 第 9 章“Identity Manager 查错”（第 63 页）



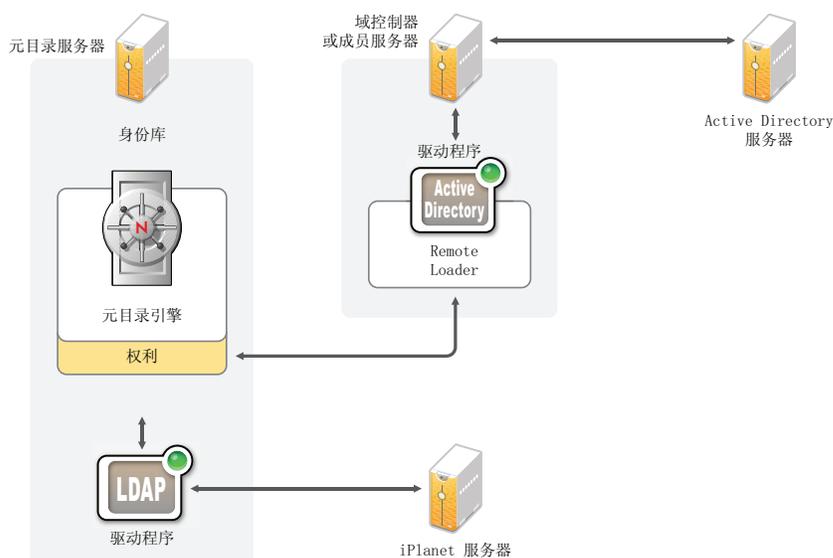
# 基本 Identity Manager 系统核对清单

# 4

有多种方法可配置 Identity Manager 以利用其全部功能。图 4-1 展示了 Identity Manager 的基本配置，即通过同步数据来供应用户。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 37 页）
- ◆ 第 4.2 节“规划”（第 38 页）
- ◆ 第 4.3 节“安装”（第 38 页）
- ◆ 第 4.4 节“带有 Remote Loader 的驱动程序配置”（第 38 页）
- ◆ 第 4.5 节“不带 Remote Loader 的驱动程序配置”（第 39 页）
- ◆ 第 4.6 节“其他配置”（第 39 页）

## 4.1 先决条件

- ❑ 在要运行 Identity Manager 的服务器上安装 Novell® eDirectory™ 8.8.5 或更高版本。确保在安装 eDirectory 过程中安装了 NMAS™。有关更多信息，请参见 [eDirectory 8.8 文档网站 \(http://www.novell.com/documentation/edir88/index.html\)](http://www.novell.com/documentation/edir88/index.html)。
- ❑ 在同一服务器上安装 Novell iManager 2.7.3。有关更多信息，请参见 [iManager 文档网站 \(http://www.novell.com/documentation/imanager27/index.html\)](http://www.novell.com/documentation/imanager27/index.html)。
- ❑ 下载 Identity Manager 产品。有关如何访问 Identity Manager 软件的指导，请参见第 5 章“从何处获取 Identity Manager”（第 41 页）。
- ❑ 在工作站上安装 Designer 3.0.1。有关更多信息，请参见第 7.1 节“安装 Designer”（第 51 页）。

## 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 13 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 15 页）。

## 4.3 安装

- ❑ 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 51 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 61 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以权利的形式创建并定义业务逻辑，然后使该逻辑应用到多个驱动程序。如果需要进行更改，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 3.6.1 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引擎之间通讯，以便 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 3.6.1 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 3.6.1 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 3.6.1 驱动程序文档网站 (<http://www.novell.com/documentation/idm36drivers/>)。

- (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 3.6.1 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 3.6.1 驱动程序文档网站* (<http://www.novell.com/documentation/idm36drivers/>)。
- (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 3.6.1 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:** 如果希望使用 Identity Manager 管理口令, 则还有其他必需配置。使用《*Identity Manager 3.6.1 口令管理指南*》中的“**口令管理核对清单**”来验证是否已完成所有配置步骤。
- **基于角色的供应:** 如果要向 Identity Manager 解决方案中添加基于角色的供应, 请使用《*User Application 安装指南* (<http://www.novell.com/documentation/idmr bpm361/install/data/bookinfo.html>)》中的核对清单以验证是否所有配置步骤均已完成。
- **审计和报告:** 通过向 Identity Manager 解决方案中添加审计和报告, 使您可以证明您的业务策略遵从了公司的策略。可将 Identity Audit 或 Novell Sentinel 添加到 Identity Manager 解决方案中以进行审计和报告。有关 Identity Audit 的更多信息, 请参见《*Identity Manager 3.6.1 集成指南 (用于 Identity Audit)*》。有关 Novell Sentinel 的更多信息, 请参见《*Identity Manager 3.6.1 报告指南 (用于 Novell Sentinel)*》。



# 从何处获取 Identity Manager

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“下载”按钮。
- 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 自第 2 步重复操作，直至下载完所有需要的文件。大多数安装需要多个 ISO 映像。

**表 5-1** ISO 映像的工作方式

Identity Manager 组件	平台	iso
Identity Manager DVD	Identity Manager: Linux、Windows* 和 UNIX  Designer: Linux 和 Windows	Identity_Manager_3_6_1_DVD.iso
Identity Manager 和驱动程序 CD	Windows	Identity_Manager_3_6_1_Win.iso
Identity Manager 和驱动程序 CD	Linux	Identity_Manager_3_6_1_Linux.iso
Identity Manager 和驱动程序 CD	Solaris	Identity_Manager_3_6_1_Solaris.iso
Identity Manager 和驱动程序 CD	AIX	Identity_Manager_3_6_1_AIX.iso
Designer for Identity Manager CD	Windows	Identity_Manager_3_6_1_Designer_Win.iso
Designer for Identity Manager CD	Linux	Identity_Manager_3_6_1_Designer_Linux.iso
User Application		有关此信息，请参见《 <i>User Application 安装指南</i> ( <a href="http://www.novell.com/documentation/idmrpbm361/index.html">http://www.novell.com/documentation/idmrpbm361/index.html</a> )》。

购买的 Identity Manager 中包含几个常用系统的集成模块，您可能已具有许可证：Novell® eDirectory™、Microsoft\* Active Directory、LDAP v3 Directories、Novell GroupWise®、和 Lotus\* Notes\*。其他所有 Identity Manager 集成模块必须单独购买。

User Application ISO 映像是购买 Identity Manager 3.6.1 产品时随附的标准版本。User Application 基于角色的供应模块是一个附加产品，为管理用户身份增加了强大的基于角色的批准工作流程。基于角色的供应模块需要一个独立的 ISO 映像，需单独购买。有关更多信息，请参见《*User Application 安装指南* (<http://www.novell.com/documentation/idmrpbm361/index.html>)》。

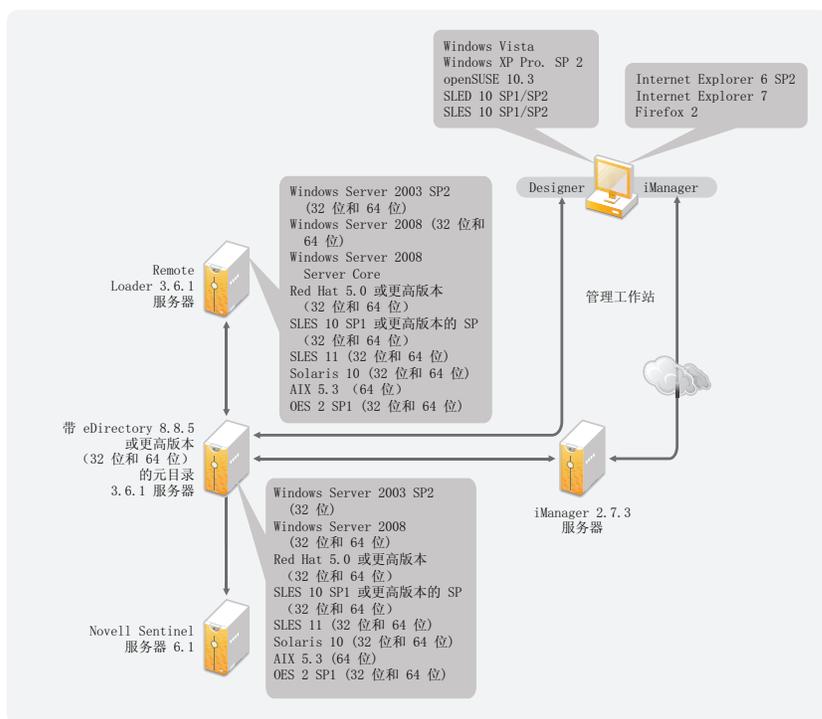
购买的 Identity Manager 产品还包含 Designer for Identity Manager，这是一个功能强大且灵活的管理工具，可以显著地简化配置和部署。

# 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



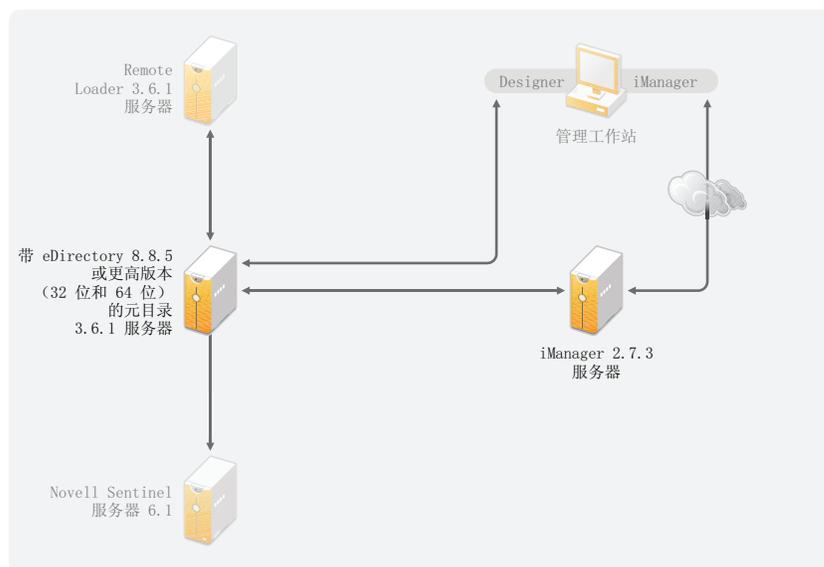
根据系统配置的不同，可能需要多次运行 Identity Manager 安装程序，才能在相应的系统上安装 Identity Manager 组件。

- ◆ 第 6.1 节“eDirectory 和 iManager” (第 43 页)
- ◆ 第 6.2 节“元目录服务器” (第 44 页)
- ◆ 第 6.3 节“Remote Loader” (第 46 页)
- ◆ 第 6.4 节“User Application” (第 48 页)
- ◆ 第 6.5 节“审计和报告” (第 48 页)
- ◆ 第 6.6 节“工作站” (第 49 页)

## 6.1 eDirectory 和 iManager

Identity Manager 要求安装 eDirectory™ 和 iManager。这些产品提供了 Identity Manager 的基础。图 6-2 说明了这些组件。

图 6-2 Identity Manager 的基本产品



以下列表说明了这些产品的必需版本:

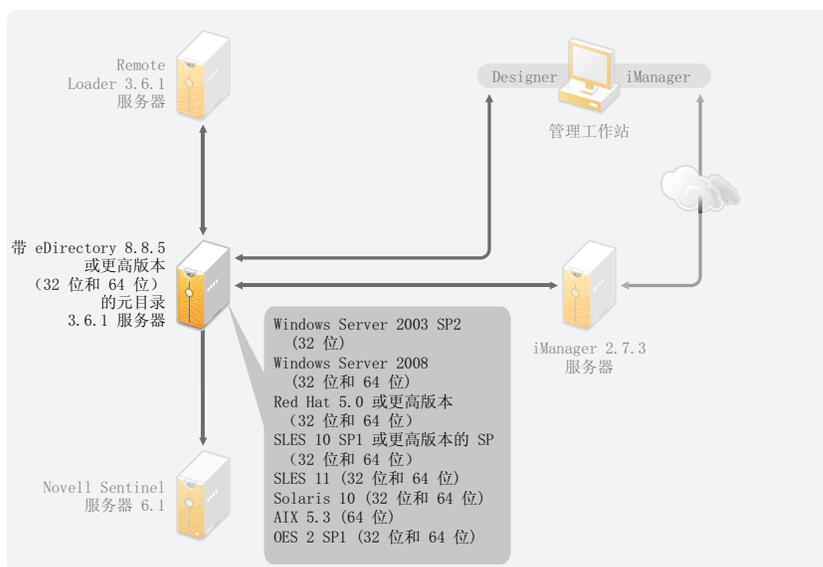
- ◆ eDirectory 8.8.5 或更高版本 (32 位或 64 位)
- ◆ iManager 2.7.3

有关 eDirectory 的系统要求, 请参见《[Novell eDirectory 8.8 SP5 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)》。

## 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是使用 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 8.8.5 或更高版本（32 位或 64 位），否则安装程序无法继续安装。

- ◆ 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 45 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\*

## 6.2.2 服务器操作系统

可在 64 位操作系统上将元目录引擎作为 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。

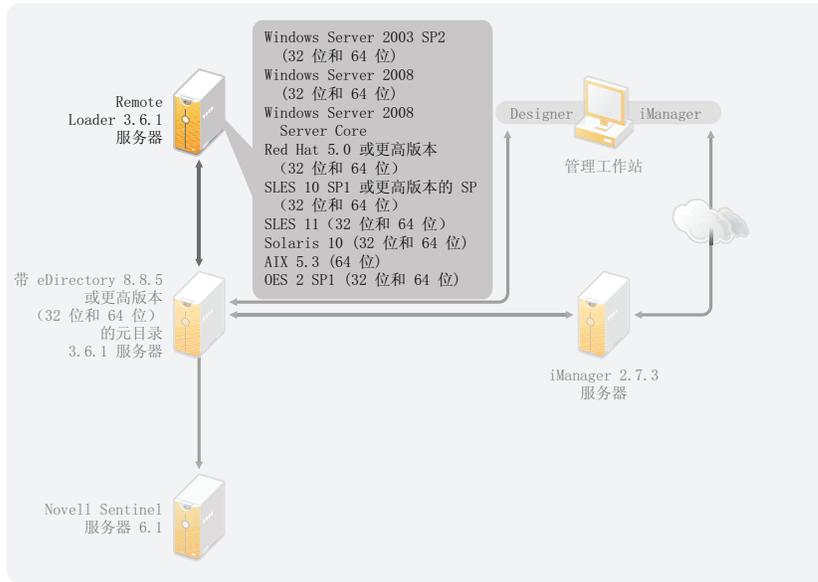
表 6-1 支持的服务器操作系统

服务器操作系统版本	注释
Windows Server* 2003 SP2 (32 位)	元目录服务器仅在 32 位模式中运行。
Windows Server 2008 (32 位和 64 位)	元目录服务器在 32 位或 64 位模式中运行。
Red Hat 5.0 或更高版本 (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 SP1 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。
Solaris 10 (32 位和 64 位)	元目录服务器在 32 位或 64 位模式中运行。
Solaris Zones (32 位和 64 位)	元目录服务器在 32 位或 64 位模式中运行。
AIX* 5L v5.3 (64 位)	元目录服务器仅在 32 位模式中运行。
Xen*	当 Xen 虚拟机在半虚拟化模式中将 SLES 10/OES 2/OES 2 SP1 作为虚拟机运行时, 支持 Xen。
VMware*	元目录服务器在 32 位或 64 位模式中运行。
Open Enterprise Server 2 SP1 (32 位和 64 位)	元目录服务器在 32 位或 64 位模式中运行。

## 6.3 Remote Loader

Remote Loader 使您的 Identity Manager 解决方案配置具有灵活性。它支持 32 位或 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。有关在 64 位操作系统上安装 32 位 Remote Loader 信息, 请参见在 [64 位操作系统上安装 32 位 Remote Loader \(第 57 页\)](#)。图 6-4 列出了 Remote Loader 支持的操作系统。

图 6-4 Remote Loader 支持的操作系统



如果已在 64 位操作系统上作为 32 位应用程序安装了元目录引擎，则无法在同一计算机上安装 64 位 Remote Loader。32 位元目录引擎和 64 位 Remote Loader 的库名称相同。如果将它们安装在同一台计算机上，则会导致冲突。

表 6-2 列出了 Remote Loader 支持的操作系统。

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)	该 Remote Loader 以 32 位或 64 位方式运行。
Windows Server 2008 (32 位和 64 位)	该 Remote Loader 以 32 位或 64 位方式运行。
Windows Server 2008 Server Core (32 位和 64 位)	该 Remote Loader 以 32 位或 64 位方式运行。
Red Hat 5.0 或更高版本 (32 位和 64 位)	该 Remote Loader 以 32 位或 64 位方式运行。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 SP1 或更高版本的支持包 (32 位和 64 位)	该 Remote Loader 以 32 位或 64 位方式运行。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)	该 Remote Loader 以 32 位或 64 位方式运行。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。
Solaris 10 (32 位和 64 位)	该 Remote Loader 以 32 位或 64 位方式运行。
Solaris Zones (32 位和 64 位)	该 Remote Loader 以 32 位或 64 位方式运行。

服务器操作系统版本	注释
AIX* 5L v5.3 (64 位)	Remote Loader 仅在 32 位模式中运行。不支持 64 位 Remote Loader。
Open Enterprise Server 2 SP1 (32 位和 64 位)	该 Remote Loader 以 32 位或 64 位方式运行。

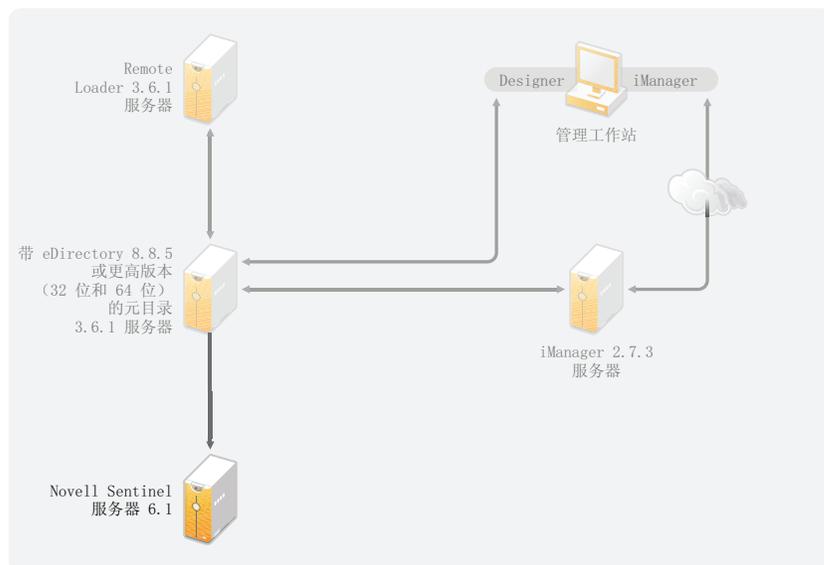
## 6.4 User Application

有关 User Application 系统要求的列表，请参见《*User Application 安装指南* (<http://www.novell.com/documentation/idmrpbpm361/index.html>)》。

## 6.5 审计和报告

Identity Audit 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 3.6.1 支持的 Sentinel 版本。

图 6-5 Sentinel



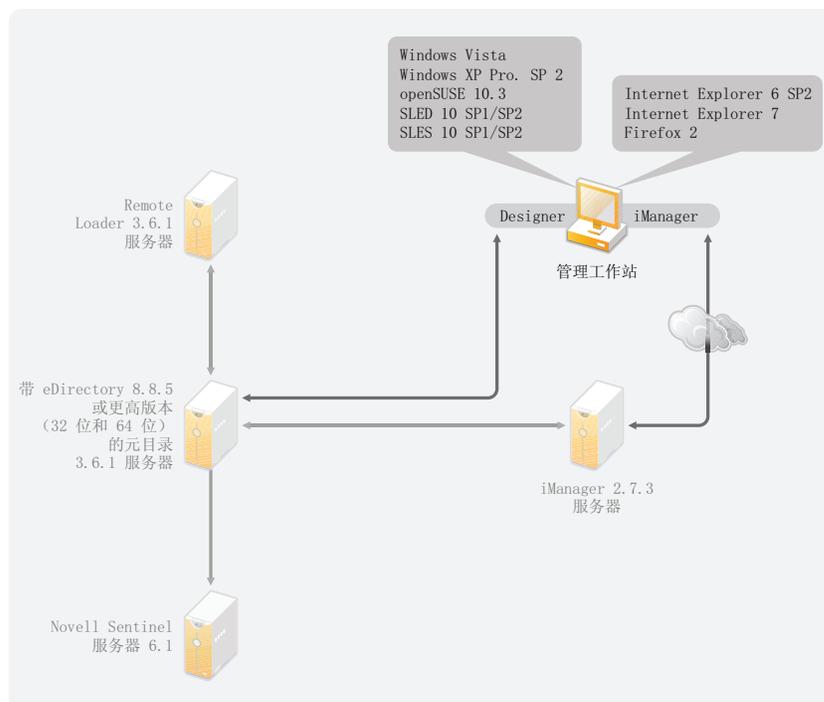
这是对 Identity Manager 解决方案的一个可选补充。通过添加审计和报告，您可满足许多公司必须遵守的合规性标准。它为需要跟踪的所有事件创建审计跟踪，还可生成报告以满足公司的审计标准。

有关在 Identity Manager 中配置 Identity Audit 的信息，请参见《*Identity Manager 3.6.1 集成指南 (用于 Identity Audit)*》。有关 Sentinel with Identity Manager 的配置信息，请参见《*Identity Manager 3.6.1 报告指南 (用于 Novell Sentinel)*》。有关 Identity Audit 的系统要求信息，请参见《*Identity Audit 指南* (<http://www.novell.com/documentation/identityaudit/index.html>)》。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>)》。

## 6.6 工作站

工作站用于 Designer、iManager 或 User Application 管理网页。图 6-6 列出了 Identity Manager 3.6.1 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 49 页）
- ◆ 第 6.6.2 节“iManager 和 Web 浏览器”（第 50 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。

表 6-3 支持的工作站平台

平台	细节
Windows Vista*	支持 Ultimate Edition 和 Business Edition。
Windows XP Professional SP2	
openSUSE® 10.3	通过自动更新工具应用最新增补程序。
SUSE Linux Enterprise Desktop 10 SP1/SP2	通过自动更新工具应用最新增补程序。
SUSE Linux Enterprise Server 10 SP1/SP2	通过自动更新工具应用最新增补程序。

## 6.6.2 iManager 和 Web 浏览器

Identity Manager 3.6.1 支持的 iManager 版本为 iManager 2.7.3。它运行配置和管理 Identity Manager 所需的所有插件。

用于管理 Identity Manager 的受支持 Web 浏览器包括：

- ◆ Internet Explorer \* 6 SP2
- ◆ Internet Explorer 7
- ◆ Firefox \* 2

# 安装 Identity Manager

Identity Manager 具有用于不同组件的单独安装过程。务必在 Identity Manager 实施的整个规划阶段安装并使用 Designer。有关更多信息，请参见第 2 章“创建项目计划”（第 15 页）。

然后以任何所需的顺序安装元目录服务器或 Remote Loader。其他组件需要按照列出的顺序进行安装。有关不同组件的解释，请参见《Identity Manager 3.6.1 概述指南》。

- ◆ 第 7.1 节“安装 Designer”（第 51 页）
- ◆ 第 7.2 节“安装元目录服务器”（第 51 页）
- ◆ 第 7.3 节“安装 Remote Loader”（第 54 页）
- ◆ 第 7.4 节“安装基于角色的供应模块”（第 59 页）
- ◆ 第 7.5 节“安装自定义驱动程序”（第 59 页）
- ◆ 第 7.6 节“安装 Identity Audit 或 Sentinel”（第 59 页）
- ◆ 第 7.7 节“在群集环境中安装 Identity Manager”（第 59 页）

## 7.1 安装 Designer

Designer 3.0.1 是一个基于工作站的工具，使用该工具可设计您的 Identity Manager 解决方案。首先安装 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 11 页）。

- 1 验证是否支持您的工作站的操作系统。有关更多信息，请参见第 6.6 节“工作站”（第 49 页）。
- 2 通过执行适用于您的工作站平台的正确程序来启动安装。
  - ◆ **Windows:** IDM3.6.1\_Designer\_Win:/windows/designer/install.exe
  - ◆ **Linux:** IDM3.6.1\_Designer\_Linux:/linux/designer/install  
要执行二进制文件，请输入 ./install。
- 3 使用以下信息完成安装：
  - ◆ **安装文件夹:** 在工作站上指定用于安装 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。
- 4 有关更多信息，请参见《Designer 3.0.1 for Identity Manager 3.6 管理指南》。

## 7.2 安装元目录服务器

对于 Linux\UNIX 平台，可作为根或非根用户安装元目录服务器。可作为非根用户安装 Identity Manager 以增加服务器上的安全性。必须由非根用户安装 eDirectory 才能使非根安装起效。如果使用非根安装，则安装过程不同。有关安装指导，请参见第 7.2.1 节“元目录服务器的非根安装”（第 53 页）。

此过程包括安装元目录服务器、Web 组件以及用于 Identity Manager 支持的不同平台的实用程序。

- 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 (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>)”。

- 3 使用适用于您的平台的正确程序启动安装。

- ◆ **Windows:** IDM3.6.1\_Win:windows\setup\idm\_install.exe
- ◆ **Linux — GUI 安装:** IDM3\_6\_1\_Lin/install.bin [-i gui]
- ◆ **Linux — 命令行安装:** IDM3\_6\_1\_Lin/install.bin -i console
- ◆ **Solaris - GUI 安装:** IDM3\_6\_1\_Solaris/install.bin [-i gui]
- ◆ **Solaris - 命令行安装:** IDM3\_6\_1\_Solaris/install.bin -i console
- ◆ **AIX - GUI 安装:** IDM3\_6\_1\_AIX/install.bin [-i gui]
- ◆ **AIX - 命令行安装:** IDM3\_6\_1\_AIX/install.bin -i console

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

- 4 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:** 此选项要求将身份库安装在此服务器上。此选项扩展 Identity Manager 的纲要，安装元目录引擎、Identity Manager 驱动程序和 Novell® Audit Agent。
  - ◆ **Novell Identity Manager 已连接系统服务器:** 此选项不要求将身份库安装在此服务器上。仅当在安装 Remote Loader 时才选择此选项。有关更多信息，请参见第 7.3 节“安装 Remote Loader”（第 54 页）。
  - ◆ **无:** 如果需要在此服务器上安装 iManager 插件或实用程序，而不安装元目录服务器或已连接系统服务器，则选择此选项。
  - ◆ **Novell Identity Manager 基于 Web 的管理服务器:** 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。因此在选择此选项前，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。

- 5 激活 Identity Manager。有关更多信息，请参见第 8 章“激活 Novell Identity Manager 产品”（第 61 页）。
- 6 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/idm36drivers/>)》。

## 7.2.1 元目录服务器的非根安装

您可作为非根用户安装 Identity Manager 以增强 UNIX/Linux 服务器的安全性。如果 eDirectory 是由根用户安装的，则您无法作为非根用户安装 Identity Manager。

非根安装不能安装以下项：

- ◆ **Remote Loader:** 如果需要作为非根用户安装 Remote Loader，则使用 Java Remote Loader。有关更多信息，请参见第 7.3.5 节“在 UNIX、Linux 或 AIX 上安装 Java Remote Loader”（第 58 页）。
- ◆ **UNIX/Linux 帐户驱动程序:** 需要根特权才能生效。
- ◆ **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。非根用户应对生成事件日志文件的位置（默认为 /var/opt/novell/sentinelpa/data/AuditEvents.log）具有 write（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 以非根用户身份安装 eDirectory 8.8.5 或更高版本。有关更多信息，请参见“非根用户安装 eDirectory 8.8 (<http://www.novell.com/documentation/edir88/edirin88/index.html?page=documentation/edir88/edirin88/data/a79kg0w.html#bs6a3gs>)”。
- 2 作为用于安装 eDirectory 的非根用户登录。  
应当作为用于安装 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。
- 3 执行适用于您的平台的安装程序。
  - ◆ **Linux:** IDM3.6.1\_Lin/linux/setup/idm-nonroot-install
  - ◆ **AIX:** IDM3.6.1\_Unix/aix/setup/idm-nonroot-install

---

**重要：**唯一支持的 AIX 维护级别是 5300-09。更新或更旧的维护级别不受支持。

---

- ◆ **Solaris:** IDM3.6.1\_solaris/setup/idm-nonroot-install  
要执行脚本文件，请输入 ./idm-nonroot-install
- 4 使用以下信息完成安装：
    - ◆ **eDirectory 非根安装的基本目录:** 指定用于 eDirectory 非根安装的目录。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。系统提示您将扩展由 eDirectory 的非根安装托管的非根用户所拥有每个 eDirectory 实例的纲要。  
如果确实选择扩展纲要，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。有关作为非根用户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/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。所有实用程序均位于 `IDM3.6.1_platform/setup/utilities` 目录中。
- 5 激活 Identity Manager。有关更多信息，请参见第 8 章“激活 Novell Identity Manager 产品”（第 61 页）。
  - 6 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/idm36drivers/>)。

## 7.2.2 元目录服务器的无提示安装

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：** `IDM3_6_1_Lin/install.bin -i silent -f <文件名>.properties`
- ◆ **Solaris：** `IDM3_6_1_Solaris/install.bin -i silent -f <文件名>.properties`
- ◆ **AIX：** `IDM3_6_1_AIX/install.bin -i silent -f <文件名>.properties`

在运行 Identity Manager 安装程序的位置中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
WEB_ADMIN_SELECTED=false
UTILITIES_SELECTED=false
```

有关默认安装位置，请参见 `/tmp/idmInstall.log`。

---

**注释：**如果已安装 iManager，并且以后要安装 iManager 插件，则必须将 `WEB_ADMIN_SELECTED` 值设置为 `true`。

---

---

**注释：**如果要在多个实例上安装（无提示安装）Identity Manager，则必须确保 `<文件名>.properties` 文件的设置如下：

```
EDIR_NCP_PORT=1524
EDIR_NDS_CONF=/etc/opt/novell/eDirectory/conf
EDIR_IP_ADDRESS=<xxx.xx.xx.xx>
```

---

## 7.3 安装 Remote Loader

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引擎即可访问已连接系统，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 25 页）。

- ◆ 第 7.3.1 节“要求”（第 55 页）

- ◆ 第 7.3.2 节“支持的驱动程序”（第 55 页）
- ◆ 第 7.3.3 节“安装过程”（第 56 页）

如果要使用非根用户安装 Remote Loader，请使用 Java Remote Loader。当自定义环境以及在不受支持的平台（如 HP-UX\*）上安装 Remote Loader 时，也可使用 Java Remote Loader。有关更多信息，请参见第 7.3.5 节“在 UNIX、Linux 或 AIX 上安装 Java Remote Loader”（第 58 页）。

### 7.3.1 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 \(http://www.novell.com/documentation/idm36drivers\)](http://www.novell.com/documentation/idm36drivers)。

### 7.3.2 支持的驱动程序

并非所有 Identity Manager 驱动程序都受 Remote Loader 支持。表 7-1 列出了 Remote Loader 支持的驱动程序。

**表 7-1** Remote Loader 支持的驱动程序

Active Directory	Avaya* PBX
定界文本	GroupWise®
JDBC*	JMS
LDAP	Linux 和 UNIX 的驱动程序
Lotus Notes*	PeopleSoft* 5.2
Remedy* ARS	SAP* HR
SAP User Management	脚本编写
SOAP	工作指令
手动任务服务	空服务
回写	

表 7-2 列出的驱动程序不能使用 Remote Loader。

**表 7-2** 没有 Remote Loader 功能

eDirectory	权利服务
角色服务	User Application

## 7.3.3 安装过程

Remote Loader 具有用于不同平台的不同程序，使用这些程序可与元目录引擎通讯。

- ◆ **Windows:** Remote Loader 控制台使用 rlconsole.exe 与 dirxml\_remote.exe 交互，后者是一个使元目录引擎能与 Windows 上运行的 Identity Manager 驱动程序通讯的可执行文件。
- ◆ **Linux/UNIX:** Rdxml 是一种可执行文件，可以使元目录引擎与运行在 Solaris、Linux 或 AIX 环境中的 Identity Manager 驱动程序进行通讯。

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 使用适用于您的平台的正确程序启动安装。

- ◆ **Windows:** IDM3.6.1\_Win:windows\setup\idm\_install.exe
- ◆ **Linux — GUI 安装:** IDM3\_6\_1\_Lin/install.bin [-i gui]
- ◆ **Linux — 命令行安装:** IDM3\_6\_1\_Lin/install.bin -i console
- ◆ **Solaris - GUI 安装:** IDM3\_6\_1\_Solaris/install.bin [-i gui]
- ◆ **Solaris - 命令行安装:** IDM3\_6\_1\_Solaris/install.bin -i console
- ◆ **AIX - GUI 安装:** IDM3\_6\_1\_AIX/install.bin [-i gui]
- ◆ **AIX - 命令行安装:** IDM3\_6\_1\_AIX/install.bin -i console

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

---

**重要:** 唯一支持的 AIX 维护级别是 5300-09。更新或更旧的维护级别不受支持。

---

- 3 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 7.2 节“安装元目录服务器”（第 51 页）。
  - ◆ **Novell Identity Manager 已连接系统服务器:** 此选项不要求将身份库安装在此服务器上。此选项在您的应用程序服务器上安装 Remote Loader 服务。
  - ◆ **无:** 如果需要在此服务器上安装 iManager 插件或实用程序，而不安装元目录服务器或已连接系统服务器，则选择此选项。
  - ◆ **Novell Identity Manager 基于 Web 的管理服务器:** 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。

---

**警告:** 对于安装 Identity Manager 3.6.1，请勿选择实用程序组件。如果选择实用程序组件，则安装无法继续。

---

- ◆ **自定义:** 如果要自定义安装的功能，则选择此选项。允许您选择以下选项：
  - ◆ **Remote Loader 服务:** 与元目录引擎通讯的服务。

- ◆ **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。
- ◆ **注册用于 Identity Manager 的 Identity Audit 系统组件：**如果安装了 Identity Audit 或 Novell Sentinel，则选择此选项。

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）实用程序的安装位置：**指定用于安装实用程序的目录。
- 4 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 \(http://www.novell.com/documentation/idm36drivers/\)](http://www.novell.com/documentation/idm36drivers/)。
  - 5 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 3.6.1 Remote Loader 指南*》中的“[通过创建配置文件为 Linux\UNIX 配置 Remote Loader](#)”。

## 在 64 位操作系统上安装 32 位 Remote Loader

在 Windows 上：

- 1 浏览 32bit\_RL\_Install.properties 文件（位于 `..\Windows\setup\` 文件夹中）并按如下所示将 `RL_32BIT_INSTALL_ON_64BIT` 属性值设置为 `true`：  
`RL_32BIT_INSTALL_ON_64BIT=true`
- 2 在命令提示中，将目录路径更改为 IDM 3.6.1 安装文件夹（例如 `C:\IDM3.6.1\windows\setup`）并输入以下命令：  
`idm_install.exe -i gui[console] -f 32bit_RL_Install.properties`
- 3 按照第 7.3.3 节“[安装过程](#)”（第 56 页）的**步骤 3**完成安装。

在 Linux 上：

- 1 浏览 32bit\_RL\_Install.properties 文件（位于 `../linux/setup` 文件夹中）并按如下所示将 `RL_32BIT_INSTALL_ON_64BIT` 属性值设置为 `true`：  
`RL_32BIT_INSTALL_ON_64BIT=true`
- 2 在终端中，将目录路径更改为 IDM 3.6.1 安装文件夹（例如 `../linux/setup`）并输入以下命令：  
`idm_linux.bin -i gui[console] -f 32bit_RL_Install.properties`
- 3 按照第 7.3.3 节“[安装过程](#)”（第 56 页）的**步骤 3**完成安装。

## 7.3.4 Remote Loader 的无提示安装

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：** `IDM3_6_1_Lin/install.bin -i silent -f <文件名>.properties`
- ◆ **Solaris：** `IDM3_6_1_Solaris/install.bin -i silent -f <文件名>.properties`
- ◆ **AIX：** `IDM3_6_1_AIX/install.bin -i silent -f <文件名>.properties`

在运行 Identity Manager 安装程序的位置中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=false
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。

---

**注释：**如果已安装 iManager，并且以后要安装 iManager 插件，则必须将 WEB\_ADMIN\_SELECTED 值设置为 true。

---

### 7.3.5 在 UNIX、Linux 或 AIX 上安装 Java Remote Loader

dirxml\_jremote 是一种纯 Java Remote Loader。它可以使运行在一台服务器上的元目录引擎和运行在其他位置（rdxml 未运行的位置）的 Identity Manager 驱动程序进行数据交换。它应能在具有兼容的 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 确认 Java 1.5.x JDK\*/JRE 在主机系统上可用。
- 2 将 dirxml\_jremote\_dev.tar.gz 文件复制到远程服务器上的所需位置。
- 3 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  
该文件在 Linux 或 UNIX ISO 映像中位于相同位置。文件位于 ISO 映像的根的 java\_remoteloader 文件夹中。有关 mvs 的信息，请解压缩 dirxml\_jremote\_mvs.tar 文件，然后参考 usage.html 文档。
- 4 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
- 5 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。  
因为压缩文件中不包含驱动程序，所以必须手动将驱动程序复制到 lib 目录中。lib 目录位于执行解压缩的目录下。
- 6 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。
- 7 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 3.6.1 Remote Loader 指南》《Identity Manager 3.6.1 Remote Loader 指南》中的“通过创建配置文件为 Linux\UNIX 配置 Remote Loader”

## 7.4 安装基于角色的供应模块

要安装基于角色的供应模块，请参见基于角色的供应模块的《[安装指南](http://www.novell.com/documentation/idmrpbm361/index.html)》。

## 7.5 安装自定义驱动程序

可创建用于您的环境的自定义驱动程序。有关创建或安装自定义驱动程序的更多信息，请参见 [Novell Developer Kit](http://developer.novell.com/wiki/index.php/Dirxml) (Novell 开发人员包)。

## 7.6 安装 Identity Audit 或 Sentinel

这是对 Identity Manager 解决方案的一个可选补充。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。它为需要跟踪的所有事件创建审计跟踪，还可生成报告以确保满足公司的所有审计标准。

有关在 Identity Manager 中配置 Identity Audit 的信息，请参见《[Identity Manager 3.6.1 集成指南 \(用于 Identity Audit\)](#)》。有关 Sentinel with Identity Manager 的配置信息，请参见《[Identity Manager 3.6.1 报告指南 \(Novell Sentinel\)](#)》。有关 Identity Audit 的系统要求信息，请参见《[Identity Audit 指南](http://www.novell.com/documentation/identityaudit/index.html)》。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)》。

## 7.7 在群集环境中安装 Identity Manager

如果在群集环境中部署 Identity Manager，Novell 支持在群集中运行 Identity Manager，尽管大多数情况下并不支持群集本身。以下两种情境说明了给定支持的扩展：

- ◆ 如果在 SUSE Linux Enterprise Server (SLES) 上运行 Identity Manager 引擎或 Remote Loader，并使用检测信号来管理高可用性，则支持所有内容。
- ◆ 如果在群集环境或任何其他受支持的平台上运行 Identity Manager 引擎或 Remote Loader，则为除群集管理系统之外的所有内容扩展支持。

---

**注释：** SLES 是群集环境中完全受支持的唯一平台。

---

有关如何使用 Identity Manager 配置群集的更多信息，请参见以下资源：

- ◆ “为 IDM 3 和 eDirectory 8.8 配置 Linux 高可用性群集”AppNote，位于 [Novell 超酷解决方案网站](http://www.novell.com/cool solutions/appnote/18591.html)。
- ◆ “Windows 2003 上的群集 eDirectory 和 IDM”AppNote，位于 [Novell 超酷解决方案网站](http://www.novell.com/cool solutions/appnote/14856.html)。
- ◆ “PolyServe 群集上的高可用性”AppNote，位于 [Novell 超酷解决方案网站](http://www.novell.com/cool solutions/appnote/16131.html)。
- ◆ “在 Windows 上设置 Identity Manager 群集”，位于 [Novell 支持网站](http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3575742&sliceId=SAL_Public&dialogID=310596&stateId=1%200%20308676)。该文档编号为 3575742。



# 激活 Novell Identity Manager 产品

# 8

以下信息说明激活如何影响基于 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 61 页）
- ◆ 第 8.2 节“安装产品激活身份凭证”（第 61 页）
- ◆ 第 8.3 节“查看 Identity Manager 和驱动程序的产品激活”（第 62 页）

## 8.1 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”网页 (<http://www.novell.com/products/identitymanager/howtobuy.html>)。

在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身份凭证。如果您记不起或者没有收到客户 ID，美国内请拨打 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 区域代码拨打会收取费用。）

## 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)，一直复制到最后  
一个破折号 (-) (END PRODUCT ACTIVATION CREDENTIAL---)。
- 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：**需要激活每个包含驱动程序的驱动程序集。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引擎和 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  以在树结构中浏览并选择驱动程序集，然后单击 。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。

---

# Identity Manager 查错

# 9

安装 Identity Manager 时请记住以下信息：

- ◆ 在 AIX 5.3 上，如果 NFS 装入发生故障，则 IDM 3.6.1 安装将停止。此行为也适用于以下实例：IDM 安装程序 iso 位于同一台计算机 (AIX) 上且任何装入的分区发生故障。

解决方法：卸载并再启动发生故障的安装，然后继续安装。

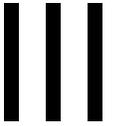
- ◆ 在 Solaris 10 上以非根身份安装 IDM 3.6.1 时，可能遇到针对 Lotus Notes 驱动程序的以下错误讯息：

```
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
```

解决方法：应手动创建符号链接。有关检查和重创建符号链接的信息，请参见《Identity Manager 3.6.1 Driver for Lotus Notes 实施指南》中的“[安装问题查错](#)”。



# 升级



以下部分包含有关升级现有 Identity Manager 解决方案的信息：

- ◆ 第 10 章“新增功能”（第 67 页）
- ◆ 第 11 章“受支持的升级版本和系统要求”（第 69 页）
- ◆ 第 12 章“就地升级与迁移”（第 71 页）
- ◆ 第 13 章“执行就地升级”（第 73 页）
- ◆ 第 14 章“执行迁移”（第 85 页）



- 第 10.1 节“支持 64 位操作系统”（第 67 页）
- 第 10.2 节“支持在 64 位操作系统上安装 32 位 Remote Loader”（第 67 页）

## 10.1 支持 64 位操作系统

Identity Manager 现在支持 64 位操作系统。有关受支持的操作系统的列表，请参见第 6.2.2 节“服务器操作系统”（第 45 页）。

## 10.2 支持在 64 位操作系统上安装 32 位 Remote Loader

Identity Manager 支持在 64 位操作系统上安装 32 位 Remote Loader。有关受支持操作系统的列表，请参见第 6.3 节“Remote Loader”（第 46 页）。



# 受支持的升级版本和系统要求

- ◆ 第 11.1 节“受支持的升级版本”（第 69 页）
- ◆ 第 11.2 节“系统要求”（第 69 页）

## 11.1 受支持的升级版本

该表说明了 Identity Manager 的先前版本的受支持升级。

表 11-1 受支持的升级版本

已安装的版本	最新版本	支持的升级
DirXML <sup>®</sup> 1.1a	Identity Manager 3.6.1	否
Identity Manager 2.x	Identity Manager 3.6.1	否
Identity Manager 3.0.x	Identity Manager 3.6.1	否
Identity Manager 3.5.x	Identity Manager 3.6.1	是

注释：Identity Manager 3.5.x 可用于支持 Remote Loader 3.6 和 3.6.1 的平台。

## 11.2 系统要求

要升级到 Identity Manager 3.6.1，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，请参见第 6 章“系统要求”（第 43 页）。



# 就地升级与迁移

有两种不同升级方法：就地升级或迁移。每种方法都有优点和缺点，并且存在只能使用一种方法的情况。

- ◆ [第 12.1 节“就地升级”](#)（第 71 页）
- ◆ [第 12.2 节“迁移”](#)（第 71 页）
- ◆ [第 12.3 节“与单个驱动程序集相关联的多个服务器”](#)（第 72 页）

## 12.1 就地升级

就地升级是指在现有服务器上安装新版本的 Identity Manager。要安装 Identity Manager，必须将操作系统和 eDirectory™ 的当前版本升级到 Identity Manager 3.6.1 支持的版本。有关受支持的平台的列表，请参见 [第 6 章“系统要求”](#)（第 43 页）。

优点是：

- ◆ 无需新硬件
- ◆ 无需迁移数据

缺点是：

- ◆ 更新操作系统以及重引导服务器时需要停机
- ◆ 更新并重启动 eDirectory 时需要停机

在某些情况下，就地升级并不可行，或必须执行多个就地升级。由于仅 Identity Manager 3.5.x 和更高版本是受支持的迁移路径，因此以下方案中仅包含这些版本：

就地升级仅支持将 Identity Manager 3.5.x 安装在受支持操作系统上的情形。但在部分方案中就地升级不可行。以下是就地升级不可行的一些示例：

- ◆ **不受支持的操作系统：**如果 Identity Manager 3.6.1 不支持当前版本的操作系统，则唯一支持的升级路径是迁移到新服务器。
- ◆ **Identity Manager 3.0.x：**如果 Identity Manager 的当前版本为 3.0.x，则无法直接执行就地升级。两个选项为：
  - ◆ 执行就地升级到 Identity Manager 3.5.1，升级到 eDirectory 8.8.5，然后执行就地升级到 Identity Manager 3.6.1。
  - ◆ 迁移到新服务器。

如果要执行就地升级，请转到 [第 13 章“执行就地升级”](#)（第 73 页）。

## 12.2 迁移

迁移是指在新服务器上安装 Identity Manager 3.6.1，然后将现有数据迁移到这个新服务器。遵从 [第 4 章“基本 Identity Manager 系统核对清单”](#)（第 37 页）以校验安装是否完成。

优点是：

- ◆ 驱动程序的停机时间最短

缺点是：

- ◆ 需要新硬件

如果要执行迁移，请转到第 14 章“执行迁移”（第 85 页）。

## 12.3 与单个驱动程序集相关联的多个服务器

如果具有与驱动程序集相关联的多个服务器，则可以一次在一个服务器上执行就地升级或迁移。如果没有时间同时升级服务器，则驱动程序继续与其他版本的 Identity Manager 协作，直到完成每个服务器的升级。

Identity Manager 引擎向后兼容，因此 Identity Manager 3.6.1 引擎可以正确运行 Identity Manager 3.5.x 驱动程序。

---

**警告：**如果启用的驱动程序的功能仅在 Identity Manager 3.6.1 上受支持，则驱动程序将在混合版本的服务器上停止工作。较旧的引擎无法处理新功能。这将暂停驱动程序，在所有服务器升级到 Identity Manager 3.6.1 后才可重新使用。

---

# 执行就地升级

在开始前，请确保已了解就地升级和迁移之间的差异。请参见第 12 章“就地升级与迁移”（第 71 页）。

使用以下核对清单校验是否以正确顺序完成了所有步骤，以便成功地就地升级 Identity Manager 系统。对于环境中的每个 Identity Manager 服务器，请遵从以下步骤。

- 创建 Identity Manager 解决方案的当前配置的备份。通过创建驱动程序的导出或创建 Identity Manager 解决方案的 Designer 项目来完成此操作。有关更多信息，请参见第 13.1 节“创建当前配置的备份”（第 74 页）。
- 校验运行 Identity Manager 的服务器上的操作系统是否是受支持的版本。有关受支持的操作系统的列表，请参见第 6 章“系统要求”（第 43 页）。如果操作系统仅需要一个服务包即能满足系统要求，则继续就地升级。如果需要多个服务包，则必须执行迁移，而非就地升级。如果操作系统是以下版本之一，则继续第 14 章“执行迁移”（第 85 页）：
  - ◆ NetWare®
  - ◆ Windows NT
  - ◆ Windows 2000
  - ◆ Red Hat Linux 3
  - ◆ SLES 8
  - ◆ Solaris 8 或 9
- 将 iManager 服务器升级到 iManager 2.7.3。有关更多信息，请参见《iManager 安装指南 ([http://www.novell.com/documentation/imanager27/imanager\\_install\\_27/data/hk42s9ot.html](http://www.novell.com/documentation/imanager27/imanager_install_27/data/hk42s9ot.html))》。
- 停止与您正在升级的服务器相关联的驱动程序。有关更多信息，请参见第 13.2 节“停止驱动程序”（第 77 页）。
- 在运行 Identity Manager 的服务器上将 eDirectory™ 升级到 8.8.5 或更高版本。有关详细信息，请参见《eDirectory 安装指南 (<http://www.novell.com/documentation/edir88/index.html>)》。
- （视条件而定）如果平台是 Linux、UNIX 或 Solaris，则要将文件添加到正确位置，必须完成附加步骤。有关详细信息，请参见第 13.3 节“在 Linux/UNIX 平台上将文件添加到正确位置”（第 77 页）。
- 启动驱动程序并校验驱动程序是否已启动。这还将校验是否已成功升级到 eDirectory 8.8.5。有关详细信息，请参见第 13.10 节“启动驱动程序”（第 82 页）。
- 升级到 Designer 3.0.1。有关更多信息，请参见《Designer 3.0.1 for Identity Manager 3.6 管理指南》中的“更新 Designer”。
- 转换 Designer 项目。有关更多信息，请参见《Designer 3.0.1 for Identity Manager 3.6 管理指南》中的“转换早期的项目”。
- 停止与您正在升级的服务器相关联的驱动程序。有关更多信息，请参见第 13.2 节“停止驱动程序”（第 77 页）。
- 升级元目录服务器。有关更多信息，请参见第 13.5 节“升级元目录引擎和驱动程序配置文件”（第 78 页）。

- (视情况而定) 如果此服务器的驱动程序集中的任一驱动程序是 Remote Loader 驱动程序, 请升级每个驱动程序的 Remote Loader 服务器。有关详细信息, 请参见第 13.6 节“升级 Remote Loader”(第 79 页)。
- (视情况而定) 如果此服务器是 User Application 服务器, 则执行以下附加步骤:
  - User Application 驱动程序必须在 Designer 中迁移。有关更多信息, 请参见《[基于角色的供应模块迁移指南](http://www.novell.com/documentation/idmrpbpm361/index.html)》。
  - 创建一个新的角色服务驱动程序。角色服务驱动程序未迁移。如果具有用于版本 3.6.1 的现有角色服务驱动程序, 则必须为版本 3.6.1 创建新的驱动程序, 有关更多信息, 请参见《[基于角色的供应模块迁移指南](http://www.novell.com/documentation/idmrpbpm361/index.html)》。
  - 将已迁移的 User Application 驱动程序部署到身份库。有关更多信息, 请参见《[基于角色的供应模块迁移指南](http://www.novell.com/documentation/idmrpbpm361/index.html)》。
  - 升级 User Application。有关更多信息, 请参见《[基于角色的供应模块迁移指南](http://www.novell.com/documentation/idmrpbpm361/index.html)》。
- (可选) 用新的驱动程序配置文件覆盖现有驱动程序以获取新策略。仅当一个驱动程序的策略中存在您希望添加到现有驱动程序的新功能时, 这才是必需的。有关更多信息, 请参见第 13.7 节“用新的驱动程序配置文件覆盖现有驱动程序”(第 79 页)。
- (可选) 将自定义策略和规则恢复到驱动程序。覆盖新驱动程序配置文件时, 将重写策略, 因此仅当覆盖了新驱动程序配置文件时才需要恢复策略。有关更多信息, 请参见第 13.8 节“将自定义策略和规则恢复为驱动程序”(第 80 页)。
- 将已转换的 Designer 项目部署到身份库。有关更多信息, 请参见《*Designer 3.0.1 for Identity Manager 3.6 管理指南*》中的“部署和导出”。
- 启动与此服务器相关联的驱动程序。有关详细信息, 请参见第 13.10 节“启动驱动程序”(第 82 页)。
- 如果使用的是 Novell Sentinel™, 则必须更新到 Novell Sentinel 6.1。有关升级 Sentinel 的更多信息, 请参见《[Sentinel 安装指南](http://www.novell.com/documentation/sentinel6/pdfdoc/sentinel60_installationguide.pdf)》。
- 激活元目录引擎和任何已升级的驱动程序。有关更多信息, 请参见第 8 章“激活 Novell Identity Manager 产品”(第 61 页)。

## 13.1 创建当前配置的备份

在升级前, 务必创建 Identity Manager 系统的当前配置的备份。如果正在使用 User Application, 则不再需要其他步骤。所有 User Application 配置均储存在 User Application 驱动程序中。可以通过两种方法来创建备份:

- ◆ 第 13.1.1 节“确保 Designer 项目是最新的”(第 75 页)
- ◆ 第 13.1.2 节“创建驱动程序的导出”(第 76 页)

## 13.1.1 确保 Designer 项目是最新的

Designer 项目包含纲要和所有驱动程序配置信息，但基于角色的权利驱动程序除外。通过创建 Identity Manager 解决方案项目，您可以一步创建所有驱动程序的导出，而非为每个驱动程序创建一个不同的导出文件。

- ◆ [导出当前项目（第 75 页）](#)
- ◆ [通过身份库创建新项目（第 75 页）](#)

### 导出当前项目

如果已具有 Designer 项目，请校验项目中的信息是否与身份库中的信息同步。

- 1 在 Designer 中，打开项目。
- 2 在建模器中，右键单击身份库，然后选择 *在线 > 比较*。
- 3 评估项目并协调所有差异，然后单击 *确定*。

有关更多信息，请参见《*Designer 3.0.1 for Identity Manager 3.6 管理指南*》中的“[部署时使用比较功能](#)”。

- 4 在工具栏上，选择 *项目 > 导出*。
- 5 单击 *全选* 以选择导出所有资源。
- 6 选择保存项目的位置和格式，然后单击 *完成*。

将项目保存在除当前工作空间外的任何位置。升级到 Designer 3.0.1 时，必须创建一个新的工作空间位置。有关更多信息，请参见《*Designer 3.0.1 for Identity Manager 3.6 管理指南*》中的“[导出项目](#)”。

### 通过身份库创建新项目

如果不具有 Identity Manager 解决方案的 Designer 项目，则使用以下过程：

- 1 下载并安装 Designer 3.0.1。  
可以创建具有 Designer 3.0.1 的 Identity Manager 3.6.x 项目。有关更多信息，请参见 [第 7.1 节“安装 Designer”（第 51 页）](#)。
- 2 启动 Designer，然后指定工作空间的位置。
- 3 选择是否要查找联机更新，然后单击 *确定*。
- 4 在“欢迎”页面上，单击 *运行 Designer*。
- 5 在工具栏上，选择 *项目 > 导入项目 > 身份库*。
- 6 指定项目的名称，然后对项目使用默认位置或选择其他位置。
- 7 单击“下一步”。
- 8 指定身份库连接信息：
  - ◆ **主机名：**指定身份库服务器的 IP 地址或 DNS 名称。
  - ◆ **用户名：**指定用于鉴定到身份库的用户的 DN。
  - ◆ **口令：**指定鉴定用户的口令。
- 9 单击“下一步”。
- 10 使“身份库纲要”和“默认通知集合”保留选中状态。
- 11 展开“默认通知集合”，然后取消选中不需要的语言。

“默认通知集合”已翻译为许多种不同语言。可导入所有语言，或仅选择您使用的语言。

- 12 单击 *浏览*，然后浏览到并选择要导入的驱动程序集。
- 13 对此身份库中的每个驱动程序集重复 [步骤 12](#)，然后单击 *完成*。
- 14 在导入项目后单击 *确定*。
- 15 如果您仅有一个身份库，则已完成。如果您有多个身份库，请继续 [步骤 16](#)。
- 16 在工具栏上单击 *在线 > 导入*。
- 17 对每个附加身份库重复 [步骤 8](#) 到 [步骤 14](#)。

### 13.1.2 创建驱动程序的导出

通过创建驱动程序的导出，可备份当前配置。但是，Designer 当前不会创建基于角色的权利驱动程序和策略的备份。使用 iManager 以校验是否具有基于角色的权利驱动程序的导出。

- ◆ [使用 Designer 创建驱动程序的导出](#) (第 76 页)
- ◆ [使用 iManager 创建驱动程序的导出](#) (第 76 页)

#### 使用 Designer 创建驱动程序的导出

- 1 确认 Designer 中的项目具有最新版本的驱动程序。有关指导，请参见 [《Designer 3.0.1 for Identity Manager 3.6 管理指南》](#) 中的“[从身份库导入库、驱动程序集或驱动程序](#)”。
- 2 在建模器中，右键单击正在升级的驱动程序的驱动程序行。
- 3 选择 *导出到配置文件*。
- 4 浏览到保存配置文件的位置，然后单击 *保存*。
- 5 在结果页面上单击 *确定*。
- 6 对每个驱动程序重复 [步骤 1](#) 到 [步骤 5](#)。

#### 使用 iManager 创建驱动程序的导出

- 1 在 iManager 中，选择 *Identity Manager > Identity Manager 概述*。
- 2 浏览到并选择树中要搜索驱动程序集对象的位置，然后单击搜索图标 。
- 3 单击保存要升级的驱动程序的驱动程序集对象。
- 4 单击要升级的驱动程序，然后单击 *导出*。
- 5 单击 *下一步*，然后选择 *导出所有包含的策略，无论是否链接到配置*。
- 6 单击 *下一步*，然后单击 *另存为*。
- 7 选择 *保存到磁盘*，然后单击 *确定*。
- 8 单击 *完成*。
- 9 对每个驱动程序重复 [步骤 1](#) 到 [步骤 8](#)。

## 13.2 停止驱动程序

在升级任何文件前，务必停止驱动程序。

- 第 13.2.1 节“使用 Designer 停止驱动程序”（第 77 页）
- 第 13.2.2 节“使用 iManager 停止驱动程序”（第 77 页）

### 13.2.1 使用 Designer 停止驱动程序

- 1 在大纲选项卡中选择身份库  对象。
- 2 在建模器工具栏中，单击停止所有驱动程序图标 。  
这将停止属于该项目的所有驱动程序。
- 3 将驱动程序设置为手动启动以确保在升级过程完成前，驱动程序不会启动。
  - 3a 双击大纲选项卡中的驱动程序图标 。
  - 3b 选择驱动程序配置 > 启动选项。
  - 3c 单击手动，然后单击确定。
  - 3d 对每个驱动程序重复步骤 3a 到步骤 3c。

### 13.2.2 使用 iManager 停止驱动程序

- 1 在 iManager 中，选择 Identity Manager > Identity Manager 概述。
- 2 浏览到并选择树中要搜索驱动程序集对象的位置，然后单击搜索图标 。
- 3 单击驱动程序集对象。
- 4 单击驱动程序 > 停止所有驱动程序。
- 5 对每个驱动程序集对象重复步骤 2 到步骤 4。
- 6 将驱动程序设置为手动启动以确保在升级过程完成前，驱动程序不会启动。
  - 6a 在 iManager 中，选择 Identity Manager > Identity Manager 概述。
  - 6b 浏览到并选择树中要搜索驱动程序集对象的位置，然后单击搜索图标 。
  - 6c 单击驱动程序集对象。
  - 6d 在驱动程序图标右上角，单击编辑属性。
  - 6e 在“驱动程序配置”页中的启动选项下选择手动，然后单击确定。
  - 6f 对树中的每个驱动程序重复步骤 6a 到步骤 6e。

## 13.3 在 Linux/UNIX 平台上将文件添加到正确位置

执行从 eDirectory 8.7.3 到 eDirectory 8.8.5 的就地升级时，安装会将 eDirectory 文件置于不同的位置。因为已安装 Identity Manager，所以除非特定的 Identity Manager 文件在适当位置，否则 eDirectory 将不会启动。完成以下步骤，将文件添加至正确的位置：

- 1 在将 eDirectory 升级为 8.8.5 后，使用以下命令运行 Identity Manager 安装程序：

```
./install.bin -i console -DCLUSTER_INSTALL=true
```

该命令在不鉴定的情况下将正确的文件添加至 eDirectory。
- 2 输入 ndsconfig upgrade，升级 eDirectory 文件。

### 3 校验 nds.conf 文件中是否存在以下条目：

n4u.server.interfaces=<ip 地址>@<端口>

例如：n4u.server.interfaces=<ip 地址>@524

如果 n4u.server.interfaces 条目不存在，则应手动设置它。要设置 n4u.server.interfaces，请执行以下步骤：

1. 运行以下命令以查找 ncp 端口：

```
ndsconfig get "n4u.server.interfaces"
```

命令会返回 ncp 端口号，例如 n4u.server.interfaces=@524

2. 运行以下命令为 n4u.server.interfaces 设置 ndsconfig：

```
ndsconfig set n4u.server.interfaces=<ip 地址>@<端口>
```

其中，

<ip 地址> 是 eDirectory 所在计算机的 ip 地址。

<端口> 是在步骤 1 中已获得的 ncp 端口号。

例如：

```
ndsconfig set n4u.server.interfaces=<ip 地址>@524
```

### 4 转到第 13.5 节“升级元目录引擎和驱动程序配置文件”（第 78 页）。

## 13.4 升级 Designer

在升级 Designer 前，请确保导出项目以创建项目的备份。有关如何导出项目的指导，请参见《*Designer 3.0.1 for Identity Manager 3.6 管理指南*》中的“导出项目”。有关升级信息，请参见《*Designer 3.0.1 for Identity Manager 3.6 管理指南*》中的“转换早期的项目”。

## 13.5 升级元目录引擎和驱动程序配置文件

升级支持组件后，即已升级元目录引擎。在升级过程中，将更新文件系统中存储的驱动程序配置文件。

- 1 验证驱动程序是否已停止。有关指导，请参见第 13.2 节“停止驱动程序”（第 77 页）。

- 2 安装 Identity Manager 3.6.1。

升级到 Identity Manager 3.6.1 的步骤与安装 Identity Manager 3.6.1 的步骤相同。有关如何安装 Identity Manager 的指导，请参见第 7 章“安装 Identity Manager”（第 51 页）。

安装 Identity Manager 3.6.1 将重写先前版本的 Identity Manager、更新二进制数据、扩展纲要并更新驱动程序配置文件。

---

**注释：**将 Identity Manager 从 32 位升级到 64 位后，Groupwise 驱动程序和本机自定义驱动程序将不起作用。

---

## 13.6 升级 Remote Loader

如果正在运行 Remote Loader，则还需要升级 Remote Loader 文件。

- 1 创建 Remote Loader 配置文件的备份。文件的默认位置如下：
  - ◆ **Windows:** C:\Novell\RemoteLoader\remoteloadername-config.txt
  - ◆ **Linux:** 在 rdxml 路径中创建自己的配置文件。
- 2 验证驱动程序是否已停止。有关指导，请参见第 13.2 节“停止驱动程序”（第 77 页）。
- 3 停止每个驱动程序的 Remote Loader 服务或守护程序。
  - ◆ **Windows:** 在 Remote Loader 控制台中，选择 Remote Loader 实例，然后单击 *停止*。
  - ◆ **Linux:** rdxml -config *path\_to\_configfile* -u
  - ◆ **Java Remote Loader:** dirxml\_jremote -config *path\_to\_configfile* -u
- 4 运行 Remote Loader 的安装程序。

安装过程将文件和二进制数据更新为最新版本。有关详细信息，请参见第 7.3 节“安装 Remote Loader”（第 54 页）。
- 5 安装完成后，验证配置文件是否包含环境的信息。
- 6（视情况而定）如果配置文件有问题，请复制在步骤 1 中创建的备份文件。否则，继续步骤 7。
- 7 启动每个驱动程序的 Remote Loader 服务或守护程序。
  - ◆ **Windows:** 在 Remote Loader 控制台中，选择 Remote Loader 实例，然后单击 *启动*。
  - ◆ **Linux:** rdxml -config *path\_to\_config\_file* -sp *password password*
  - ◆ **Java Remote Loader:** dirxml\_jremote -config *path\_to\_config\_file* -sp *password password*

---

**注释：**将 Remote Loader 从 32 位升级到 64 位后，Groupwise 驱动程序和本机自定义驱动程序将不起作用。

---

## 13.7 用新的驱动程序配置文件覆盖现有驱动程序

在开始前，请确保任何自定义策略的名称均不同于默认策略。使用新驱动程序文件覆盖驱动程序配置时，会重写现有策略。如果您的自定义策略没有唯一名称，则将丢失这些自定义策略。

用新驱动程序配置文件覆盖现有驱动程序会使用驱动程序配置文件中的任何新策略或功能更新驱动程序。

- ◆ 第 13.7.1 节“使用 Designer 用新驱动程序配置文件覆盖现有驱动程序”（第 79 页）
- ◆ 第 13.7.2 节“使用 iManager 用新驱动程序配置文件覆盖现有驱动程序”（第 80 页）

### 13.7.1 使用 Designer 用新驱动程序配置文件覆盖现有驱动程序

- 1 在建模器中，右键单击正在升级的驱动程序的驱动程序行。
- 2 选择 *运行配置向导*。
- 3 在警告页面上单击 *是*。

该警告通知您所有驱动程序设置和策略都将重设置。

---

**重要：**确保自定义策略均具有不同于默认策略的名称，以便不丢失任何数据。

---

- 4 浏览到并选择要升级的驱动程序的驱动程序配置，然后单击 *运行*。
- 5 指定该驱动程序的信息，然后单击 *下一步*。  
可能需要指定多个信息页面。
- 6 在结果页面上单击 *确定*。
- 7 查看驱动程序参数和策略，确保一切均按需要进行设置。
- 8 如果具有自定义策略，请转到第 13.8 节“将自定义策略和规则恢复为驱动程序”（第 80 页）。否则，请转到第 13.10 节“启动驱动程序”（第 82 页）。

## 13.7.2 使用 iManager 用新驱动程序配置文件覆盖现有驱动程序

- 1 在 iManager 中，选择 *Identity Manager > Identity Manager 概述*。
- 2 浏览到并选择树中要搜索驱动程序集对象的位置，然后单击搜索图标 。
- 3 单击驱动程序集对象。
- 4 单击 *驱动程序 > 添加驱动程序*，然后在“新建驱动程序向导”页面上单击 *下一步*。
- 5 选择要覆盖的驱动程序配置，然后单击 *下一步*。
- 6 在 *现有驱动程序* 字段中，浏览到并选择要升级的驱动程序。
- 7 指定该驱动程序的信息，然后单击 *下一步*。
- 8 在摘要页面上，选择 *更新有关该驱动程序和策略库的所有内容*。

---

**重要：**确保任何自定义策略均具有不同于默认值的名称，以便不丢失任何数据。

---

- 9 单击 *下一步*，然后在摘要页面上单击 *完成*。
- 10 查看驱动程序参数和策略，确保一切均按需要进行设置。
- 11 如果具有自定义策略，请转到第 13.8 节“将自定义策略和规则恢复为驱动程序”（第 80 页）。否则，请转到第 13.10 节“启动驱动程序”（第 82 页）。

## 13.8 将自定义策略和规则恢复为驱动程序

如果具有自定义策略或规则，在覆盖新驱动程序配置文件后，必须将其恢复为驱动程序。如果这些策略具有不同名称，则它们仍存储在驱动程序中，但是链接会损坏并需要重新建立。

- ◆ 第 13.8.1 节“使用 Designer 将自定义策略和规则恢复为驱动程序”（第 80 页）
- ◆ 第 13.8.2 节“使用 iManager 将自定义策略和规则恢复为驱动程序”（第 81 页）

### 13.8.1 使用 Designer 将自定义策略和规则恢复为驱动程序

可通过两种不同方法向策略集中添加策略：

- ◆ 通过大纲视图添加自定义策略（第 81 页）
- ◆ 通过“显示策略流”视图添加自定义策略（第 81 页）

## 通过大纲视图添加自定义策略

- 1 在大纲视图中，选择已升级的驱动程序以显示策略集视图。
- 2 右键单击需要将自定义策略恢复为驱动程序的策略集  图标，然后选择 **新建 > 从副本**。
- 3 浏览到并选择自定义策略，然后单击 **确定**。
- 4 指定自定义策略的名称，然后单击 **确定**。
- 5 在文件冲突讯息中单击 **是** 以保存项目。
- 6 策略构建器打开策略后，验证复制的策略中信息是否正确。
- 7 对需要恢复为驱动程序的每个自定义策略，重复 **步骤 2 到步骤 6**。
- 8 启动并测试驱动程序。

有关启动驱动程序的更多信息，请参见第 13.10 节“启动驱动程序”（第 82 页）。有关测试驱动程序的更多信息，请参见《*Designer 3.0 中的策略*》中的“使用策略模拟器测试策略”。
- 9 验证策略工作正常后，将驱动程序移动到生产环境中。

## 通过“显示策略流”视图添加自定义策略

- 1 在大纲视图中，选择已升级的驱动程序，然后单击显示策略流图标 。
- 2 右键单击需要将自定义策略恢复为驱动程序的策略集，然后选择 **添加策略 > 复制现有**。
- 3 浏览到并选择自定义策略，然后单击 **确定**。
- 4 指定自定义策略的名称，然后单击 **确定**。
- 5 在文件冲突讯息中单击 **是** 以保存项目。
- 6 策略构建器打开策略后，验证复制的策略中信息是否正确。
- 7 对需要恢复为驱动程序的每个自定义策略，重复 **步骤 2 到步骤 6**。
- 8 启动并测试驱动程序。

有关启动驱动程序的更多信息，请参见第 13.10 节“启动驱动程序”（第 82 页）。有关测试驱动程序的更多信息，请参见《*Designer 3.0 中的策略*》中的“使用策略模拟器测试策略”。
- 9 验证策略工作正常后，将驱动程序移动到生产环境中。

## 13.8.2 使用 iManager 将自定义策略和规则恢复为驱动程序

- 1 在 iManager 中，选择 **Identity Manager > Identity Manager 概述**。
- 2 浏览到并选择树中要搜索驱动程序集对象的位置，然后单击搜索图标 。
- 3 单击包含已升级的驱动程序的驱动程序集对象。
- 4 单击驱动程序图标，然后选择需要恢复自定义策略的策略集。
- 5 单击 **插入**。
- 6 选择 **使用现有策略**，然后浏览到并选择自定义策略。
- 7 单击 **确定**，然后单击 **关闭**。
- 8 对需要恢复为驱动程序的每个自定义策略，重复 **步骤 3 到步骤 7**。
- 9 启动并测试驱动程序。

有关启动驱动程序的信息，请参见第 13.10 节“启动驱动程序”（第 82 页）。iManager 中没有任何策略模拟器。要测试策略，请触发使策略能够执行的事件。例如，创建用户、修改用户或删除用户。

10 验证策略工作正常后，将驱动程序移动到生产环境中。

## 13.9 部署已转换的项目

将已转换的 Designer 项目部署到身份库。有关更多信息，请参见《*Designer 3.0.1 for Identity Manager 3.6 管理指南*》中的“部署和导出”。

## 13.10 启动驱动程序

升级完所有 Identity Manager 组件后，必须重新启动驱动程序。务必在运行驱动程序后测试驱动程序，以校验所有策略仍起效。

- 第 13.10.1 节“使用 Designer 启动驱动程序”（第 82 页）
- 第 13.10.2 节“使用 iManager 启动驱动程序”（第 82 页）

### 13.10.1 使用 Designer 启动驱动程序

- 1 在大纲选项卡中选择身份库  对象。
- 2 在建模器工具栏中单击 *启动所有驱动程序* 图标 。这将启动项目中的所有驱动程序。
- 3 设置驱动程序启动选项。
  - 3a 双击大纲选项卡中的驱动程序图标 。
  - 3b 选择 *驱动程序配置 > 启动选项*。
  - 3c 选择 *自动启动* 或选择启动驱动程序的首选方法，然后单击 *确定*。
  - 3d 对每个驱动程序重复 *步骤 3a* 到 *步骤 3c*。
- 4 测试驱动程序以验证策略是否按照设计运行。有关如何测试策略的更多信息，请参见《“*Designer 3.0 中的策略*”》中的 *使用策略模拟器测试策略*。

### 13.10.2 使用 iManager 启动驱动程序

- 1 在 iManager 中，选择 *Identity Manager > Identity Manager 概述*。
- 2 浏览到并选择树中要搜索驱动程序集对象的位置，然后单击搜索图标 。
- 3 单击驱动程序集对象。
- 4 单击 *驱动程序 > 启动所有驱动程序* 可同时启动所有驱动程序。  
或  
在驱动程序图标的右上角，单击 *启动驱动程序* 可单独启动每个驱动程序。
- 5 如果有多个驱动程序，请重复 *步骤 2* 到 *步骤 4*。
- 6 设置驱动程序启动选项：
  - 6a 在 iManager 中，选择 *Identity Manager > Identity Manager 概述*。
  - 6b 浏览到并选择树中要搜索驱动程序集对象的位置，然后单击搜索图标 。
  - 6c 单击驱动程序集对象。

- 6d** 在驱动程序图标右上角，单击*编辑属性*。
  - 6e** 在“驱动程序配置”页中的*启动选项*下，选择*自动启动*，或选择启动驱动程序的首选方法，然后单击*确定*。
  - 6f** 对每个驱动程序重复**步骤 6b** 到**步骤 6e**。
- 7** 测试驱动程序以验证策略是否按照设计运行。
- iManager 中没有任何策略模拟器。要测试策略，请触发使策略能够执行的事件。例如，创建用户、修改用户或删除用户。



在开始前，请确保已了解就地升级和迁移之间的差异。请参见第 12 章“就地升级与迁移”（第 71 页）。

使用以下核对清单校验是否以正确顺序完成了所有步骤，以便成功迁移 Identity Manager 系统。对于环境中每个 Identity Manager 服务器，请遵从以下步骤。

- ❑ 创建 Identity Manager 解决方案的当前配置的备份。通过创建驱动程序的导出或创建 Identity Manager 解决方案的 Designer 项目来完成此操作。有关更多信息，请参见第 13.1 节“创建当前配置的备份”（第 74 页）。
- ❑ 安装所需的操作系统。有关受支持平台的列表，请参见第 6 章“系统要求”（第 43 页）。
- ❑ 在服务器上安装 eDirectory™ 8.8.5。有关详细信息，请参见《eDirectory 安装指南 (<http://www.novell.com/documentation/edir88/index.html>)》。
- ❑ 将位于当前 Identity Manager 服务器上的相同 eDirectory 复本添加到此新服务器。有关更多信息，请参见《eDirectory 管理指南 (<http://www.novell.com/documentation/edir88/pdfdoc/edir88/edir88.pdf>)》中的“管理复本 (<http://www.novell.com/documentation/edir88/edir88/data/fbgciaad.html>)”。
- ❑ 安装 Identity Manager 3.6.1。使用第 4 章“基本 Identity Manager 系统核对清单”（第 37 页）校验是否所有步骤已完成。
- ❑ 如果驱动程序集中的任一驱动程序是 Remote Loader 驱动程序，请升级每个驱动程序的 Remote Loader 服务器。有关更多信息，请参见第 13.6 节“升级 Remote Loader”（第 79 页）。
- ❑ （视情况而定）如果旧服务器是 User Application 服务器，则执行以下附加步骤：
  - ❑ User Application 驱动程序必须在 Designer 中迁移。有关更多信息，请参见《基于角色的供应模块迁移指南 (<http://www.novell.com/documentation/idmrpbm361/index.html>)》。
  - ❑ 创建新的角色服务驱动程序。角色服务驱动程序未迁移。如果具有用于版本 3.6.1 的现有角色服务驱动程序，则必须为版本 3.6.1 创建新的驱动程序，有关更多信息，请参见《基于角色的供应模块迁移指南 (<http://www.novell.com/documentation/idmrpbm361/index.html>)》。
  - ❑ 将已迁移的 User Application 驱动程序部署到身份库。有关更多信息，请参见《基于角色的供应模块迁移指南 (<http://www.novell.com/documentation/idmrpbm361/index.html>)》。
  - ❑ 在此新服务器上安装 User Application。有关更多信息，请参见《基于角色的供应模块安装指南 (<http://www.novell.com/documentation/idmrpbm361/install/data/bookinfo.html>)》。
- ❑ 将该新服务器添加到驱动程序集中。有关更多信息，请参见第 14.1 节“将该新服务器添加到驱动程序集中”（第 86 页）。
- ❑ 更改每个驱动程序的特定于服务器的信息。有关更多信息，请参见第 14.2 节“更改特定于服务器的信息”（第 86 页）。

- (视情况而定) 运行 `configupdate.sh` 或 `configupdate.bat` 以将旧服务器中特定于服务器的信息更改为 User Application 配置的新服务器。有关更多信息, 请参见《[基于角色的供应模块安装指南](http://www.novell.com/documentation/idmrbpm361/install/data/bookinfo.html)(<http://www.novell.com/documentation/idmrbpm361/install/data/bookinfo.html>)》中的“User Application 配置参照”( <http://www.novell.com/documentation/idmrbpm361/install/data/bb1zmw0.html>)。
- (可选) 用新的驱动程序配置文件覆盖现有驱动程序以获取新策略。仅当一个驱动程序的策略中存在您希望添加到现有驱动程序的新功能时, 这才是必需的。有关更多信息, 请参见第 13.7 节“用新的驱动程序配置文件覆盖现有驱动程序”(第 79 页)。
- (可选) 将自定义策略和规则恢复到驱动程序。覆盖新驱动程序配置文件时, 将重写策略, 因此仅当覆盖了新驱动程序配置文件时才需要恢复策略。有关更多信息, 请参见第 13.8 节“将自定义策略和规则恢复为驱动程序”(第 80 页)。
- 从驱动程序集中去除旧服务器。有关更多信息, 请参见第 14.3 节“从驱动程序集中去除旧服务器。”(第 88 页)。
- 如果使用的是 Novell Sentinel™, 则必须更新到 Novell Sentinel 6.1。有关升级 Sentinel 的更多信息, 请参见《[Sentinel 安装指南](http://www.novell.com/documentation/sentinel6/pdfdoc/sentinel60_installationguide.pdf)([http://www.novell.com/documentation/sentinel6/pdfdoc/sentinel60\\_installationguide.pdf](http://www.novell.com/documentation/sentinel6/pdfdoc/sentinel60_installationguide.pdf))》。
- 激活元目录引擎和任何已升级的驱动程序。有关更多信息, 请参见第 8 章“激活 Novell Identity Manager 产品”(第 61 页)。

## 14.1 将该新服务器添加到驱动程序集中

如果正在使用 iManager, 则必须将该新服务器添加到驱动程序集中。Designer 包含一个用于服务器的迁移向导, 可为您完成此步骤。如果正在使用 Designer, 请跳至第 14.2 节“更改特定于服务器的信息”(第 86 页)。如果正在使用 iManager, 请完成以下过程:

- 1 在 iManager 中, 单击  以显示“Identity Manager 管理”页面。
- 2 单击 *Identity Manager 概述* >。
- 3 浏览到并选择保存驱动程序集的容器。
- 4 单击驱动程序集名称以访问“驱动程序集概述”页。
- 5 单击 *服务器* > *添加服务器*。
- 6 浏览到并选择新 Identity Manager 3.6.1 服务器, 然后单击 *确定*。

## 14.2 更改特定于服务器的信息

必须将每个驱动程序中储存的特定于服务器的所有信息更改为新服务器的信息。特定于服务器的信息包含于:

- ◆ 全局配置值
- ◆ 引擎控制值
- ◆ 命名口令
- ◆ 驱动程序鉴定信息
- ◆ 驱动程序启动选项
- ◆ 驱动程序参数

可以在 Designer 或 iManager 中进行此操作。如果使用 Designer，则这是一个自动过程。如果使用 iManager，则这是一个手动过程。

- ◆ [第 14.2.1 节“在 Designer 中更改特定于服务器的信息”](#)（第 87 页）
- ◆ [第 14.2.2 节“在 iManager 中更改特定于服务器的信息”](#)（第 87 页）

## 14.2.1 在 Designer 中更改特定于服务器的信息

该过程影响驱动程序集中储存的所有驱动程序。

- 1 在 Designer 中，打开项目。
- 2 在 *概要* 选项卡中，右键单击服务器，然后选择 *迁移*。
- 3 阅读概述以查看迁移到新服务器的项，然后单击 *下一步*。
- 4 从可用服务器列表中选择目标服务器，然后单击 *下一步*。

仅列出当前未与驱动程序集相关联且与源服务器的 Identity Manager 版本相同或更高的服务器。

- 5 选择 *激活目标服务器*。

有三个选项，但建议使用 *激活目标服务器*。

- ◆ **激活目标服务器：**将源服务器中的设置复制到目标服务器并禁用源服务器上的驱动程序。
- ◆ **保持源服务器处于活动状态：**不要复制设置并禁用目标服务器上的所有驱动程序。
- ◆ **同时激活目标服务器和源服务器：**将源服务器中的设置复制到目标服务器，不禁用源服务器或目标服务器上的驱动程序。不建议使用此选项。如果同时启动了两个驱动程序，则相同信息会写入两个不同队列，并且这可能导致损坏。

- 6 单击 *迁移*。

迁移特定于服务器的信息后，必须将已更改的驱动程序部署到身份库。有关更多信息，请参见《[Designer 3.0.1 for Identity Manager 3.6 管理指南](#)》中的“[将驱动程序部署到身份库](#)”。

最后一步是启动驱动程序。有关更多信息，请参见[第 13.10 节“启动驱动程序”](#)（第 82 页）。

## 14.2.2 在 iManager 中更改特定于服务器的信息

- 1 在 iManager 中，单击  以显示“Identity Manager 管理”页面。
- 2 单击 *Identity Manager 概述*。
- 3 浏览到并选择保存驱动程序集的容器。
- 4 单击驱动程序集名称以访问“驱动程序集概述”页。
- 5 单击驱动程序的右上角，然后单击 *停止驱动程序*。
- 6 单击驱动程序的右上角，然后单击“*编辑属性*”。
- 7 必须将每个驱动程序参数、全局配置值、引擎控制值、命名口令、驱动程序鉴定信息和驱动程序启动选项中包含的旧服务器信息更改为新服务器信息。
- 8 单击 *确定* 保存所有更改。
- 9 单击驱动程序的右上角以启动驱动程序。
- 10 对驱动程序集中的每个驱动程序重复 [步骤 5](#) 到 [步骤 9](#)。

## 14.3 从驱动程序集中去除旧服务器。

新服务器运行所有驱动程序后，必须从驱动程序集中去除旧服务器。

- 第 14.3.1 节“使用 Designer 从驱动程序集中去除旧服务器”（第 88 页）
- 第 14.3.2 节“使用 iManager 从驱动程序集中去除旧服务器”（第 88 页）
- 第 14.3.3 节“弃用旧服务器”（第 88 页）

### 14.3.1 使用 Designer 从驱动程序集中去除旧服务器

- 1 在 Designer 中，打开项目。
- 2 在建模器中，右键单击驱动程序集，然后选择 *属性*。
- 3 选择 *服务器列表*。
- 4 在 *选定服务器列表* 中选择旧 Identity Manager 服务器，然后单击 < 从 *选定服务器列表* 中去除服务器。
- 5 单击“确定”保存更改。

必须将此更改部署到身份库。有关更多信息，请参见《*Designer 3.0.1 for Identity Manager 3.6 管理指南*》中的“*将驱动程序集部署到身份库*”。

### 14.3.2 使用 iManager 从驱动程序集中去除旧服务器

- 1 在 iManager 中，单击  以显示“Identity Manager 管理”页面。
- 2 单击 *Identity Manager 概述* > 。
- 3 浏览到并选择保存驱动程序集的容器。
- 4 单击驱动程序集名称以访问“驱动程序集概述”页。
- 5 单击 *服务器* > *去除服务器*。
- 6 选择旧 Identity Manager 服务器，然后单击 *确定*。

### 14.3.3 弃用旧服务器

此时，旧服务器不再托管任何驱动程序。如果不再需要此服务器，则必须执行其他步骤以弃用此服务器：

- 1 从此服务器中去除 eDirectory 副本。有关更多信息，请参见《*eDirectory 管理指南* (<http://www.novell.com/documentation/edir88/pdfdoc/edir88/edir88.pdf>)》中的“删除副本 (<http://www.novell.com/documentation/edir88/edir88/data/fbgciaad.html>)”。
- 2 从此服务器中去除 eDirectory。有关更多信息，请参见 TID 10056593，“从 NDS 树中永久去除服务器” ([http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=10056593&sliceId=&docTypeID=DT\\_TID\\_1\\_1&dialogID=35218849&stateId=0%20%2035214815](http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=10056593&sliceId=&docTypeID=DT_TID_1_1&dialogID=35218849&stateId=0%20%2035214815))。

# 卸装 Identity Manager

# IV

如果需要卸装 Identity Manager，请依次使用以下部分中的过程：

- ◆ 第 15 章“去除 eDirectory 中的对象”（第 91 页）
- ◆ 第 16 章“卸装元目录服务器和驱动程序”（第 93 页）
- ◆ 第 17 章“卸装 Designer”（第 95 页）



# 去除 eDirectory 中的对象

# 15

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，系统将提示您是否将该驱动程序集作为分区。

删除 Identity Manager 对象：

- 1 对 eDirectory 数据库执行状态检查如果发生任何错误，请修正错误然后再继续。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。

转到第 16 章“**卸载元目录服务器和驱动程序**”（第 93 页）。



# 卸载元目录服务器和驱动程序

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 16.1 节“在 Windows 上卸载”（第 93 页）
- ◆ 第 16.2 节“在 Linux/UNIX 上卸载”（第 93 页）

## 16.1 在 Windows 上卸载

在 Windows 上卸载 Identity Manager:

- ◆ 对于 32 位 Windows，请使用以下方法之一：
  - ◆ 访问 Windows 服务器上的控制面板。如果服务器操作系统是 Windows Server 2003，请单击*添加或删除程序*。如果服务器操作系统是 Windows Server 2008，请单击*程序和功能*。

---

**注释：**此方法不适用于 Windows Server 2008 Server Core。

---

- ◆ 执行位于 C:\Program Files\Novell\Identity Manager\Uninstall\_Identity\_Manager 的卸载脚本 (Uninstall Identity Manager.exe)。
- ◆ 对于 64 位 Windows，请使用以下方法之一：
  - ◆ 访问 Windows 服务器上的控制面板。如果服务器操作系统是 Windows Server 2003，请单击*添加或删除程序*。如果服务器操作系统是 Windows Server 2008，请单击*程序和功能*。

---

**注释：**此方法不适用于 Windows Server 2008 Server Core。

---

- ◆ 执行位于 C:\Program Files (x86)\Novell\Identity Manager\Uninstall\_Identity\_Manager 的卸载脚本 (Uninstall Identity Manager.exe)。

## 16.2 在 Linux/UNIX 上卸载

要在 Linux/UNIX 上卸载 Identity Manager，请运行位于 ~/idm/Uninstall\_Identity\_Manager/Uninstall\_Identity\_Manager 的卸载脚本。要执行脚本，请输入 ./Uninstall\_Identity\_Manager。



# 卸载 Designer

# 17

卸载 Designer 与卸载元目录服务器和驱动程序非常相似。

- ◆ 对于 Windows，请在控制面板中选择*添加或删除程序*。
- ◆ 对于 Linux/UNIX，请执行位于 `~/designer/UninstallDesigner/Uninstall_Designer_for_Identity_Manager` 的卸载脚本。

