概述

Novell®
Identity Manager

3.6.1

2009 年 5 月 15 日

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)。如果您未能获得任何必要的出口许可，则 Novell 对此概不负责。

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/) 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

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

Novell 商标

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

第三方资料

所有第三方商标均属其各自所有者的财产。

目录

关于本指南

本指南介绍 Novell® Identity Manager 可帮助您解决的业务问题，并概述可在解决方案中使用的 Identity Manager 软件组件和工具的技术。本指南的组织方式如下：

适用对象

本指南适用于需要深入了解 Identity Manager 业务解决方案、技术和工具的管理员、顾问及网络工程师。

文档更新

有关本文档的最新版本，请访问 Identity Manager 文档万维网站点 (http://www.novell.com/documentation/idm36/index.html)。

其他文档

有关其他 Identity Manager 驱动程序的文档的信息，请参见 Identity Manager 驱动程序万维网站点 (http://www.novell.com/documentation/idm36drivers/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。

Identity Manager 和业务流程自动化

1

以下信息标识了通过实施 Novell® Identity Manager 系统可自动化的一些业务流程。如果您已对 Identity Manager 提供的业务自动化解决方案有所了解，您可能希望跳至第 2 章 “Identity Manager 体系结构 ”（第 17 页）中提供的技术介绍。

管理身份需求是大多数业务的核心功能。例如，假设这是星期一的早上。您向下滚动队列中的请求列表：

- Jim Taylor 的手机号码已经更改。您需要在 HR 数据库以及其他四个独立系统中将其更新。
- Karen Hansen 刚过完长假归来，她忘记了电子邮件口令。您需要帮助她重新找回口令或重设置口令。
- Jose Altimira 刚刚雇用了一名新员工。您需要授予该员工网络访问权以及电子邮件帐户。
- Ida McNamee 希望访问获得 Oracle* 财务数据库的访问权，这需要您获得三个其他经理的批准。
- John Harris 刚刚从应付款部门转到了法律部门。您需要授予他访问权，以使其能够访问法律小组的其他成员可访问的相同资源，并去除其对应付款资源的访问权。
- Karl Jones 是您的上司，他看到了 Ida McNamee 希望获取 Oracle 财务数据库访问权的请求的副本，并且想要知道具有该访问权的人数。您需要为他生成一份显示具有该数据库访问权的所有人的报告。

您做一个深呼吸然后开始处理第一个请求，意识到要满足所有请求将会压力巨大，更不必说有时间完成指派给您的其他项目。

如果这听起来像是您或贵组织中的其他人的一个普通工作日，那么 Identity Manager 可能很有帮助。实际上， Identity Manager 的核心功能 （如下图所示）可帮助您将所有这些任务以及更多任务自动化。工作流程、角色、证明、自助服务、审计和报告功能相结合，着重于由业务策略驱动的多系统数据同步，可将供应用户和管理口令 （IT 组织中两个最困难、最耗时的任务）所涉及的流程自动化。

图 1-1 Identity Manager 核心功能

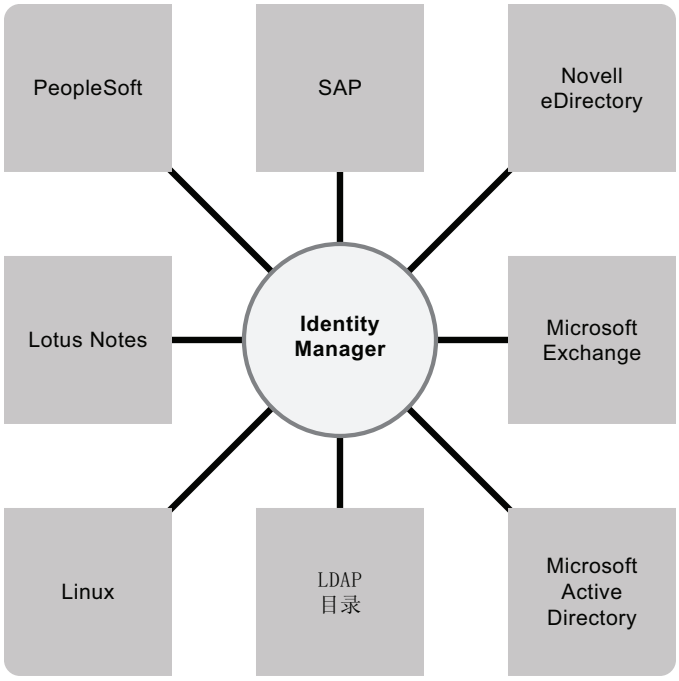
以下各节向您介绍 Identity Manager 的这些功能以及这些功能可如何帮助您成功地满足贵组织中的身份需求：

1.1 数据同步

如果贵组织与大多数组织一样，将身份数据储存在多个系统中。或者，将身份数据储存在一个可以在其他系统中真正使用的系统中。则无论采用哪种方式，您都需要能够在系统间轻松地共享和同步数据。

Identity Manager 允许您在多种应用程序、数据库、操作系统和目录之间 （如 SAP*、PeopleSoft*、 Lotus Notes*、 Microsoft* Exchange、 Microsoft Active Directory*、 Novell eDirectory™、 Linux 和 UNIX 以及 LDAP 目录）同步、转换和分发信息。

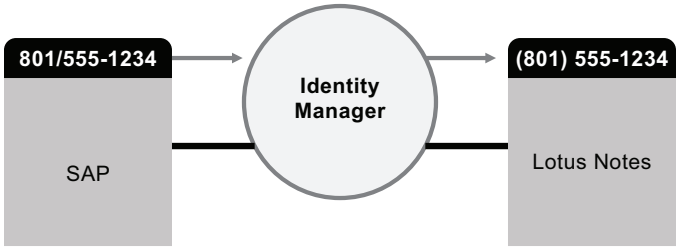
图 1-2 连接多个系统的 Identity Manager



您可以控制已连接系统之间的数据流。其中，您确定要共享的数据、数据块的权威来源系统以及对数据进行解释和转换以满足其他系统要求的方法。

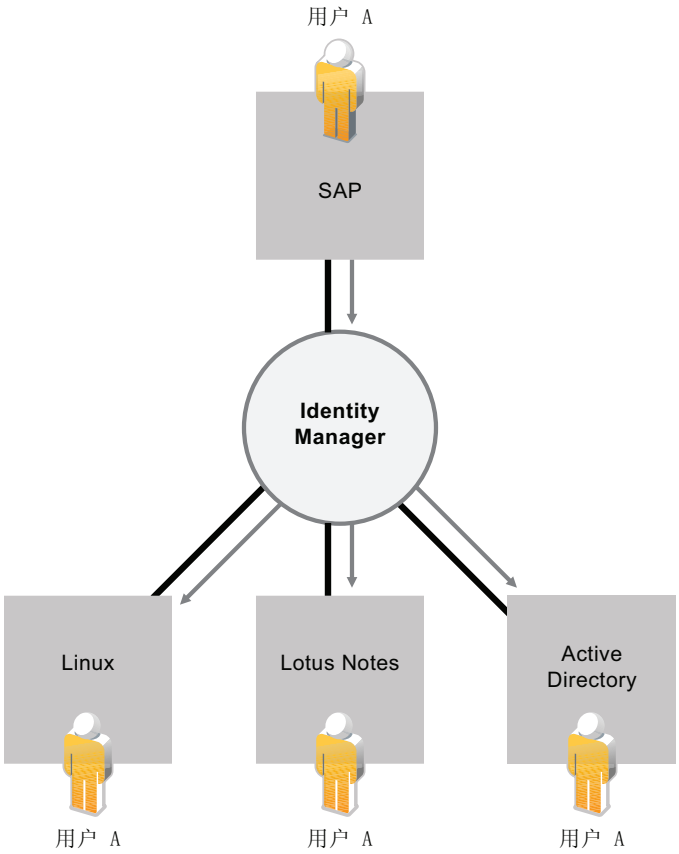
在以下图表中，SAP HR 数据库是用户的电话号码的权威来源。Lotus Notes 系统也使用电话号码，因此 Identity Manager 将号码转换为需要的格式并将其与 Lotus Notes 系统共享。只要 SAP HR 系统中的电话号码发生更改，更改的号码就会同步到 Lotus Notes 系统中。

图 1-3 已连接系统之间的数据同步



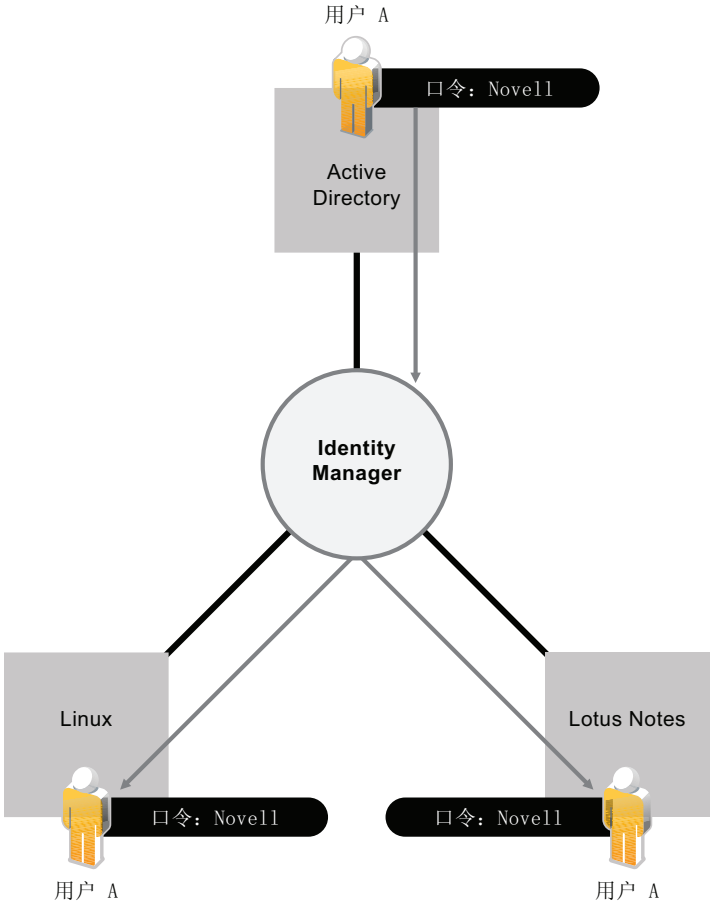
管理现有用户的数据仅仅是 Identity Manager 的数据同步功能的开始。此外， Identity Manager 还可在目录 （如 Active Directory）、系统 （如 PeopleSoft 和 Lotus Notes）和操作系统 （如 UNIX 和 Linux）中创建新用户帐户及去除现有帐户。例如，向 SAP HR 系统中添加新员工时， Identity Manager 可自动在 Active Directory 中创建新用户帐户，在 Lotus Notes 中创建新帐户以及在 Linux NIS 帐户管理系统中创建新帐户。

图 1-4 在已连接系统中创建用户帐户



作为其数据同步功能的一部分， Identity Manager 还可帮助您在系统之间同步口令。例如，如果用户更改了在 Active Directory 中的口令， Identity Manager 可将该口令同步到 Lotus Notes 和 Linux。

图 1-5 已连接系统之间的口令同步

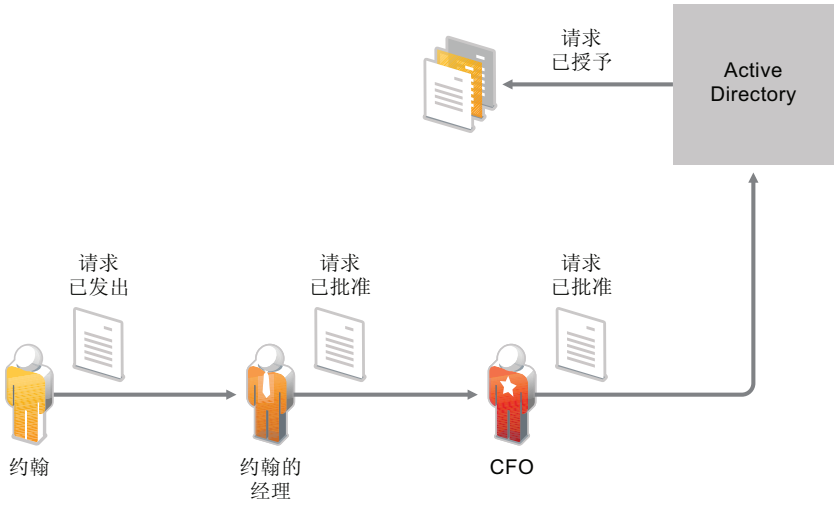


1.2 工作流程

更有可能的是，用户对贵组织中许多资源的访问不需要任何人的批准。但是，可能该用户对其他资源的访问受到限制并需要一个或多个人的批准。

Identity Manager 提供工作流程功能以确保供应流程包括了相应的资源批准者。例如，假设 John （已获得 Active Directory 帐户）需要通过 Active Directory 访问一些财务报告。这需要 John 的直接经理和 CFO 的批准。幸运的是，您已建立一个批准工作流程，可将 John 的请求路由到他的经理，待经理批准后，再将请求路由到 CFO。 CFO 的批准将触发 John 访问和查看财务单据所需的 Active Directory 权限的自动供应。

图 1-6 用户供应的批准工作流程



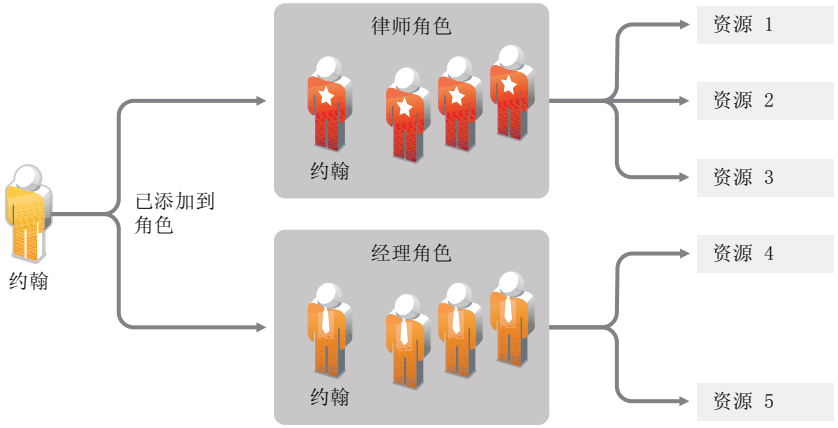
工作流程可在某个特定事件发生时 （例如，向 HR 系统中添加新用户）自动启动，也可通过用户请求手动启动。要确保批准能够及时发生，可设置代理批准者和批准小组。

1.3 角色和证明

用户通常根据其在组织中的角色来请求对资源的访问权。例如，某个法律公司的律师和该公司的律师助理可能需要访问不同的资源组。

Identity Manager 允许您根据其在组织中的角色来供应用户。您可根据组织需求定义角色并进行指派。将用户指派给角色后， Identity Manager 可向该用户供应与该角色关联的资源的访问权。如果将用户指派给多个角色，则该用户会收到与所有角色关联的资源的访问权，如下图所示。

图 1-7 基于角色的资源供应



您可基于组织中发生的事件而将用户自动添加到角色，例如，有新用户添加到 SAP HR 数据库且职称为 “ 律师 ”。如果将某个用户添加到角色需要批准，则可建立工作流程以将角色请求路由到相应批准者。也可手动将用户指派给角色。

在某些情况下，某些角色可能由于冲突而不应指派给同一个人。 Identity Manager 提供了“责任分离”功能，使用该功能可避免将用户指派给冲突角色，除非组织中有人将该冲突作为例外。

由于角色指派确定了用户对组织内资源的访问权，因此确保正确的指派非常重要。错误的指派可能会危及与公司和政府规定的一致性。 Identity Manager 可通过证明流程帮助您验证角色指派的正确性。使用此流程，贵组织中的负责人可认证与角色关联的数据：

- **用户简介证明：**所选用户证明其自身的简介信息（姓、名、职位、部门、电子邮件等等）并纠正所有错误信息。准确的简介信息对于正确的角色指派非常重要。
- **责任分离违反证明：**负责人审阅“责任分离”违反报告并证明报告的准确性。该报告列出了允许将用户指派给冲突角色的所有例外。
- **角色指派证明：**负责人审阅列出了所选角色和指派给每个角色的用户、组以及角色的报告。然后负责人必须证明该信息的准确性。
- **用户指派证明：**负责人审阅列出了所选用户以及将其指派给的角色的报告。然后负责人必须证明该信息的准确性。

这些证明报告主要是为了帮助您确保角色指派准确，并确保存在允许冲突角色例外的有效原因。

1.4 自助服务

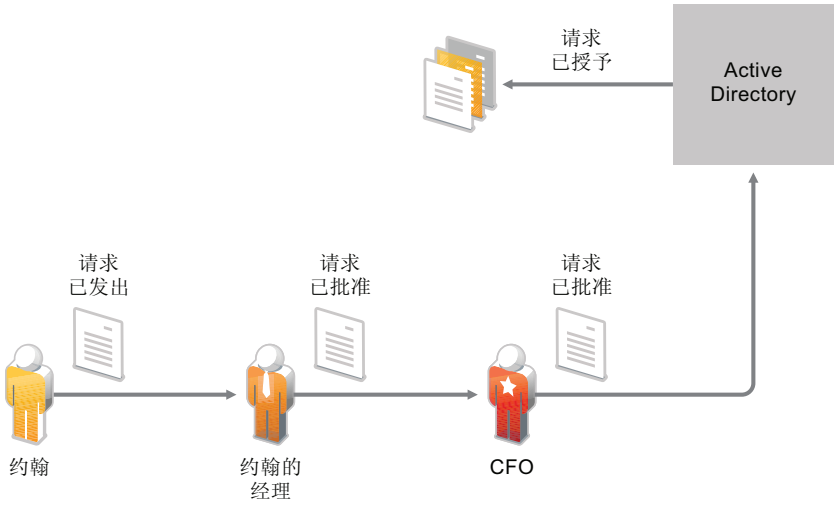
您的许多业务经理和部门可能强烈要求自己管理用户信息和访问需求，而不是依赖您或您的手下。您是不是不止一次听到“为什么我不能在我的公司目录中更改自己的手机号码？”或“我就是在市场部。为什么我必须要致电咨询台才能访问营销信息数据库？”

使用 Identity Manager，您可将管理责任委托给应对上述人员负责的人。例如，您可使个人用户：

- 在公司目录中管理各自的个人数据。不必由您来更改手机号码，他们也可在某个位置更改手机号码，并可在您已通过 Identity Manager 同步的所有系统中更改。
- 更改口令、设置忘记口令的提示以及设置忘记口令的提示问题和答案。在他们忘记口令的情况下，不必让您来重设置口令，他们可在收到提示或回答询问问题后自行进行该操作。
- 请求对诸如数据库、系统和目录等资源的访问权。不必致电给您来请求对某个应用程序的访问权，他们可从可用资源列表中选择该应用程序。

除了个人用户的自助服务， Identity Manager 还为负责辅助、监视和批准用户请求的各种职能（管理层、咨询台等等）提供了自助管理。例如，假设存在第 1.2 节“工作流程”（第 13 页）中使用的场景并如下所示。

图 1-8 自助服务的供应工作流程



不仅 John 使用 Identity Manager 自助服务功能请求对所需单据的访问权，而且 John 的经理和 CFO 也使用自助服务功能来批准请求。已建立的批准工作流程使 John 可以启动并监视其请求的进度，并使 John 的经理和 CFO 可以响应其请求。 John 的经理和 CFO 对请求的批准触发了 John 访问和查看财务单据所需的 Active Directory 权限的供应。

1.5 审计和报告

如果没有 Identity Manager，供应用户可能是件单调乏味且耗时费财的事情。但是，这种努力与校验供应活动是否符合贵组织的策略、要求和规定相比较，可能无足轻重。是否正确的人对正确的资源有访问权？是否对不适当的人封锁了同一批资源？昨天开始上班的员工是否具有对网络、电子邮件以及其工作所需的六个其他系统的访问权？是否取消了上周离职员工的访问权？

使用 Identity Manager，您可知道所有用户供应活动都得以跟踪和记录以供审计之用，从而尽可放心。 Identity Manager 对发生的所有活动均发出事件讯息。通过使用 Novell Sentinel™，您可以收集这些讯息以便生成以下类型的报告：

- 特定时间段内的所有批准工作流程，且记录有关每个工作流程的操作 （已启动、已转发、已拒绝、已批准等等）。
- 特定时间段内供应的所有资源，且记录有关每个资源的操作 （已提交、已授予、已撤消、成功等等）。
- 特定时间段内，某个用户的所有工作流程状态、口令更改和管理更改。
- 特定时间段内某个用户的所有资源供应。
- 特定时间段内所有用户的所有资源供应。

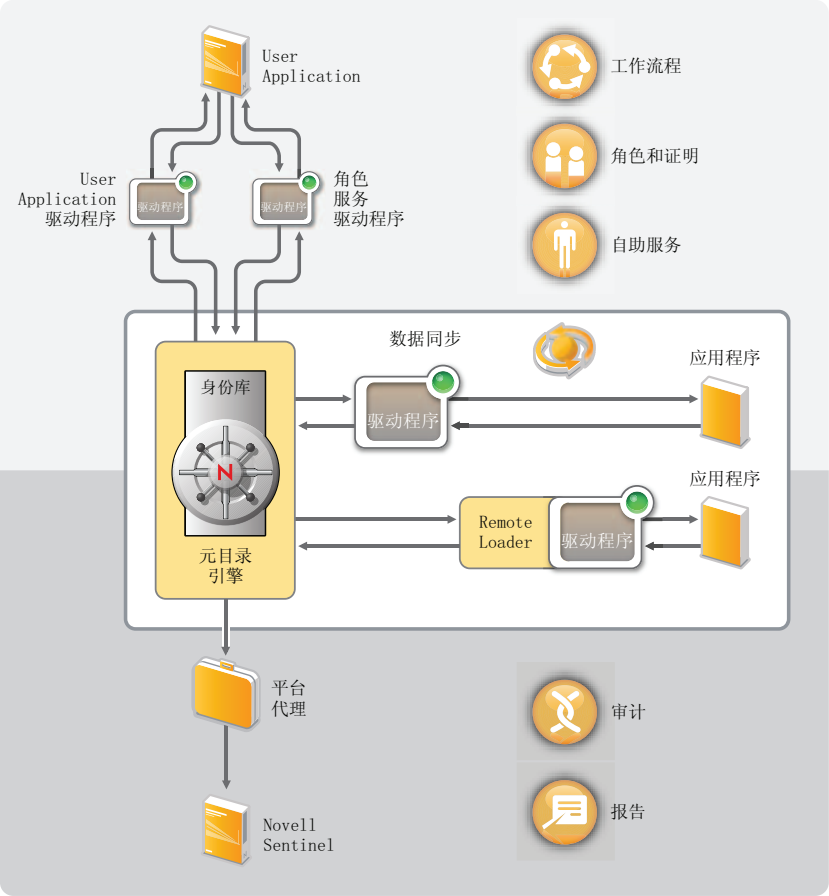
Novell Sentinel 与 Identity Manager 分开销售。

Identity Manager 体系结构

2

以下图表显示了高级体系结构组件，提供了第 1 章 “Identity Manager 和业务流程自动化 ”（第 9 页）中介绍的 Novell® Identity Manager 功能：数据同步、工作流程、角色、证明、自助服务和审计 / 报告。

图 2-1 *Identity Manager 高级体系结构*



以下各节中将分别介绍每种组件：

- 第 2.1 节 “ 数据同步 ”（第 17 页）
- 第 2.2 节 “ 工作流程、角色、证明和自助服务 ”（第 21 页）
- 第 2.3 节 “ 审计和报告 ”（第 22 页）

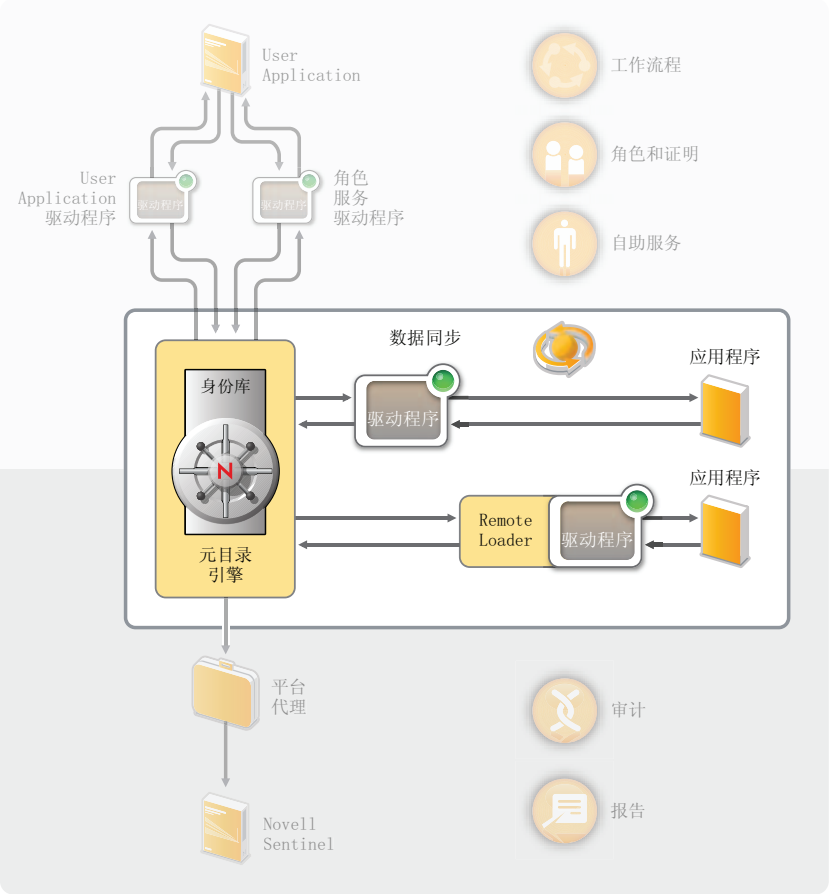
2.1 数据同步

数据同步提供了业务流程自动化的基础。数据同步最简单的形式是：数据从一个位置 （数据项发生更改的位置）移动到另一个位置 （需要该数据项的位置）。例如，如果某个员工的电话号码在公司的人力资源系统中发生了更改，则理想情况是，该更改自动显示在储存该员工电话号码的所有其他系统中。

Identity Manager 不限于身份数据的同步。 Identity Manager 可同步储存在已连接应用程序或身份库中的任何类型的数据。

数据同步 （包括口令同步）由 Identity Manager 解决方案的五个基本组件提供：身份库、元目录引擎、驱动程序、 Remote Loader 和已连接应用程序。这些组件如下表所示。

图 2-2 *Identity Manager 体系结构组件*



以下各节描述了其中各个组件并解释应该了解的概念，以便有效地在贵组织中的各个系统之间同步数据。

- 第 2.1.1 节 “ 组件 ”（第 18 页）
- 第 2.1.2 节 “ 主要概念 ”（第 19 页）

2.1.1 组件

身份库：身份库充当您要在应用程序之间同步的数据的元目录。例如，从 PeopleSoft 系统同步到 Lotus Notes 的数据将首先添加到身份库，然后再发送给 Lotus Notes 系统。此外，身份库还储存特定于 Identity Manager 的信息，如驱动程序配置、参数和策略。 Novell eDirectory™ 用于身份库。

元目录引擎：当数据在身份库或已连接应用程序中发生更改时，元目录引擎将处理更改。对于身份库中发生的事件，引擎将处理更改并通过驱动程序向应用程序发出命令。对于应用程序中发生的事件，引擎将接收驱动程序中的更改、处理更改然后向身份库发出命令。元目录引擎也称为 *Identity Manager 引擎*。

驱动程序：驱动程序连接到需要管理其身份信息的应用程序。驱动程序有两个基本责任：1) 将应用程序中的数据更改 （事件）报告给元目录引擎， 2) 执行由元目录引擎提交给应用程序的数据更改 （命令）。

Remote Loader：驱动程序必须在与连接到的应用程序所在的同一服务器上安装并运行。如果应用程序位于与元目录引擎相同的服务器上，则您需要进行的操作是将驱动程序安装到该服务器上。但是，如果应用程序没有位于与元目录引擎相同的服务器上 （也就是说，应用程序所在服务器相对于引擎的服务器是远程而非本地的），则您必须将驱动程序和 Remote Loader 安装到该应用程序的服务器上。 Remote Loader 装载驱动程序并代表该驱动程序与元目录引擎通讯。

应用程序：驱动程序连接到的系统、目录、数据库或操作系统。该应用程序必须提供驱动程序可用于确定应用程序数据更改和影响应用程序数据更改的 API。应用程序也经常称为 *已连接系统*。

2.1.2 主要概念

通道：数据在身份库和已连接系统之间沿着两个单独的*通道*流动。*订购者通道*提供了从身份库到已连接系统的数据流；也就是说，已连接系统从身份库订购数据。*发布者通道*提供从已连接系统到身份库的数据流；也就是说，已连接系统将数据发布到身份库。

数据表示：数据作为 *XML 文档*流过通道。当身份库或已连接系统中发生更改时，即会创建 XML 文档。XML 文档将传递给元目录引擎，后者通过一组与驱动程序通道关联的过滤器和策略来处理文档。将所有处理应用到 XML 文档后，元目录引擎将使用文档启动对身份库 （发布者通道）的相应更改，或驱动程序使用文档启动已连接系统 （订购者通道）中的相应更改。

数据处理：XML 文档流过驱动程序通道时，文档数据会受到与该通道关联的*策略*的影响。

策略可用于很多操作，包括更改数据格式、在身份库和已连接系统之间映射属性、有条件地阻止数据流、生成电子邮件通知以及修改数据更改的类型。

数据流控制：*过滤器*或*过滤器策略*控制数据流。过滤器指定要在身份库和已连接系统之间同步的数据项。例如，通常会在系统之间同步用户数据。因此，对于大多数已连接系统，用户数据会在过滤器中列出。但是，打印机通常不受大多数应用程序的重视，因此，对于大多数已连接系统，打印机数据不显示在过滤器中。

身份库和已连接系统之间的每种关系都有两个过滤器：订购者通道上的过滤器，用于控制从身份库到已连接系统的数据流；发布者通道上的过滤器，用于控制从已连接系统到身份库的数据流。

权威来源：与身份关联的大多数数据项都具有一个概念性拥有者。将数据项的拥有者视为该项的*权威来源*。通常，仅允许数据项的权威来源对数据项进行更改。

例如，通常将公司电子邮件系统视为员工的电子邮件地址的权威来源。如果公司白页目录的管理员在该系统中更改了员工的电子邮件地址，则该更改对于员工是否实际从更改后的地址接收电子邮件没有任何影响，因为必须对电子邮件系统进行更改后此操作才生效。

Identity Manager 使用过滤器来指定某个项的权威来源。例如，如果 PBX 系统和身份库之间关系的过滤器允许员工的电话号码从 PBX 系统流向身份库，但不允许从身份库流向 PBX 系统，则 PBX 系统是电话号码的权威来源。如果所有其他已连接系统关系允许电话号码从身份库流向已连接系统，但不允许反向流动，则最后效果是 PBX 系统是企业中员工电话号码的唯一权威来源。

自动化供应：自动化供应借助于 Identity Manager 的功能来生成用户供应操作，而非简单地同步数据项。

例如，在典型的 Identity Manager 系统中，其中人力资源 (HR) 数据库是大多数员工数据的权威来源，向 HR 数据库中添加员工将触发在身份库中自动创建相应帐户的操作。创建身份库帐户反过来又触发在电子邮件系统中自动为该员工创建电子邮件帐户的操作。用于供应给电子邮件系统帐户的数据从身份库中获取，其中可能包括员工姓名、位置、电话号码等。

帐户、访问权和数据的自动供应可通过各种方式控制，包括：

- *数据项值*：例如，在访问数据库中为各种建筑自动创建帐户可由员工的位置属性中的某个值控制。
- *批准工作流程*：例如，在财务部门中创建员工可触发自动向财务部门领导发送一封电子邮件，请求在财务系统中批准一个新员工帐户。财务部门领导按照电子邮件的指示打开一个网页，在此页面中，部门领导可以批准或拒绝该请求。然后批准操作可触发在财务系统中为该员工自动创建帐户的操作。
- *角色指派*：例如，将 “ 会计 ” 角色授予某员工。Identity Manager 通过系统工作流程（无需人为干预）和 / 或人为批准流程向员工供应所有帐户、访问权和指派给该帐户角色的数据。

权利：权利表示已连接系统中的某个资源，如帐户或组成员资格。如果用户满足为已连接系统中针对某个权利建立的准则， Identity Manager 将处理导致授予该用户资源访问权的用户事件。当然，这要求所有策略均已就绪以便能够访问资源。例如，如果某个用户满足 Active Directory 中 Exchange 帐户的准则，则元目录引擎将通过提供 Exchange 帐户的 Active Directory 驱动程序策略集来处理该用户。

权利的关键优势是您可在一个权利中定义用于访问资源的业务逻辑，而非定义多个驱动程序策略。例如，您可定义一个 “ 帐户 ” 权利，用于在四个已连接系统中向用户提供帐户。是否向用户提供帐户由权利决定，这就是说所有四个驱动程序的策略不需要包括业务逻辑。而是策略仅需要提供授予帐户的机制。如果您需要进行业务逻辑更改，则只需在权利中 （而无需在每个驱动程序中）更改它。

作业：大多数情况下， Identity Manager 响应数据更改或用户请求。例如，当某数据块在一个系统中发生更改时， Identity Manager 会更改其他系统中的相应数据。或者，当用户请求访问某个系统时， Identity Manager 会启动相应的流程 （工作流程、资源供应等）以提供访问权。

作业使 Identity Manager 可执行不是由数据更改或用户请求启动的操作。作业由储存在身份库中的配置数据和相应的实施代码段组成。 Identity Manager 包括预定义作业，可执行诸如以下的操作：启动或停止驱动程序、发送口令失效的电子邮件通知及检查驱动程序的运行状态。您还可实施自定义作业以执行其他操作；自定义作业要求您 （或开发人员 / 顾问）创建执行所需操作必需的代码。

工作指令：通常，对身份库或已连接应用程序中的数据更改是即时处理的。工作指令使您可以安排在特定日期和时间要执行的任务。例如，雇用了一名新员工，但安排在一个月后上班。需要将该员工添加到 HR 数据库，但在开始日期前不应授予他对公司任何资源 （电子邮件、服务器等）的访问权。如果没有工作指令，将立刻授予该用户访问权。通过实施工作指令，将会创建仅在开始日期才启动帐户供应的工作指令。

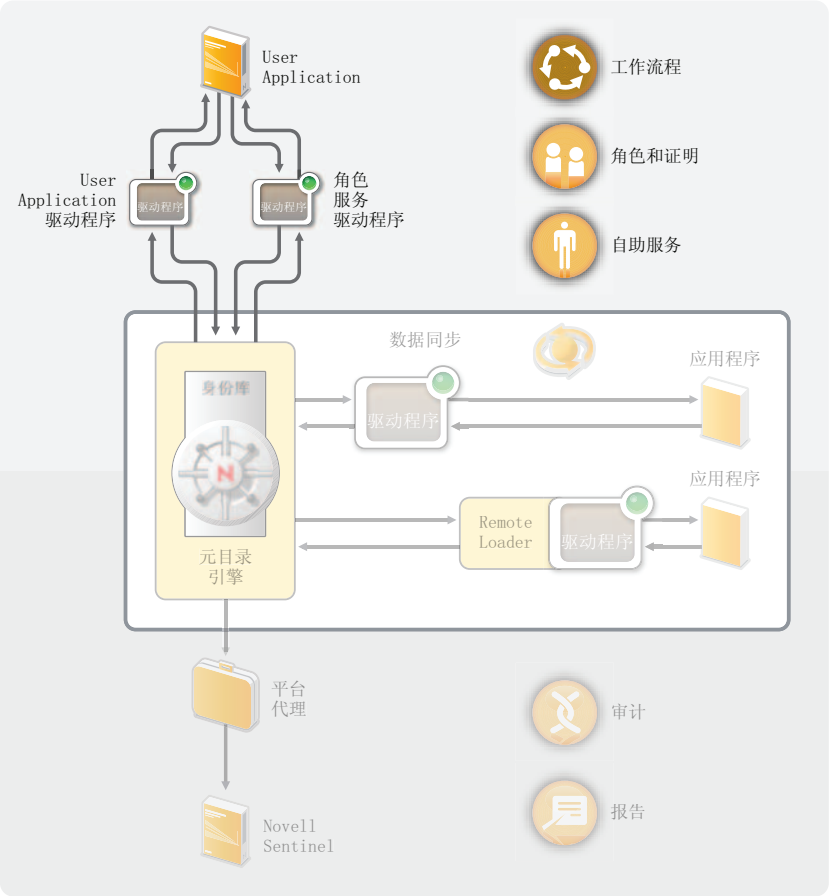
2.2 工作流程、角色、证明和自助服务

Identity Manager 提供了专门的应用程序：User Application，该应用程序可提供批准工作流程、角色指派、证明和身份自助服务。

Identity Manager 中包含标准的 User Application。标准版本提供了以下功能：口令自助服务，可帮助用户记住或重设置忘记的口令；组织结构图，可帮助管理用户目录信息；用户管理功能，可在身份库中创建用户；以及基本身份自助服务，如管理用户简介信息。

User Application 基于角色的供应模块是单独销售的 Identity Manager 附加产品。添加基于角色的供应模块时，标准 User Application 功能会扩展为包括高级自助服务、批准工作流程、基于角色的供应、责任分离约束和证明。

图 2-3 *Identity Manager User Application*



以下各节介绍其中各个组件并解释您应了解的概念，以便有效地实施和管理组件：

- 第 2.2.1 节 “ 组件 ”（第 22 页）
- 第 2.2.2 节 “ 主要概念 ”（第 22 页）

2.2.1 组件

User Application：User Application 是基于浏览器的万维网应用程序，使用户和业务管理员能够执行各种身份自助服务和角色供应任务，包括管理口令和身份数据、启动和监视供应及角色指派请求、管理供应请求的批准流程以及校验证明报告。它包括工作流程引擎，可通过相应的批准流程控制请求的路由。

User Application 驱动程序：User Application 驱动程序储存配置信息，并在身份库中发生更改时立即通知 User Application。还可将它配置为允许身份库中的事件触发工作流程，并向 User Application 报告工作流程供应活动的成功或失败情况，以便用户可以查看其请求的最终状态。

角色服务驱动程序：角色服务驱动程序可管理所有角色指派、启动角色指派请求 （要求批准）的工作流程以及根据组和容器成员资格维护间接角色指派。该驱动程序还根据用户的角色成员资格为其授予和撤消权利，并且执行已完成请求的清理过程。

2.2.2 主要概念

基于工作流程的供应：基于工作流程的供应为用户提供了一种请求访问资源的方法。供应请求通过预定义工作流程 （可能包括来自一个或多个人的批准）进行路由。如果所有批准均已授予，则用户将收到对资源的访问权。还可间接启动供应请求以响应身份库中发生的事件。例如，向组中添加用户可能启动授予用户对某个特定资源的访问权的请求。

基于角色的供应：基于角色的供应提供了一种根据所指派的角色使用户接收对特定资源访问权的方法。可为用户指派一个或多个角色。如果角色指派需要批准，则指派请求将启动一个工作流程。

责任分离：为避免将用户指派到冲突角色， User Application 基于角色的供应模块提供了责任分离功能。您可建立责任分离*约束*，定义视为冲突的角色。如果有角色冲突，责任分离*批准者*可批准或拒绝任何约束*例外*。已批准的例外将记录为责任分离*违反*，并可通过下述证明流程进行审阅。

角色管理：角色的管理必须由指派给*角色模块管理员*和*角色管理员*系统角色的个人完成。

“ 角色模块管理员 ” 可创建新角色、修改现有角色和去除角色、修改角色之间的关系、授予或撤消用户的角色指派以及创建、修改和去除责任分离约束。

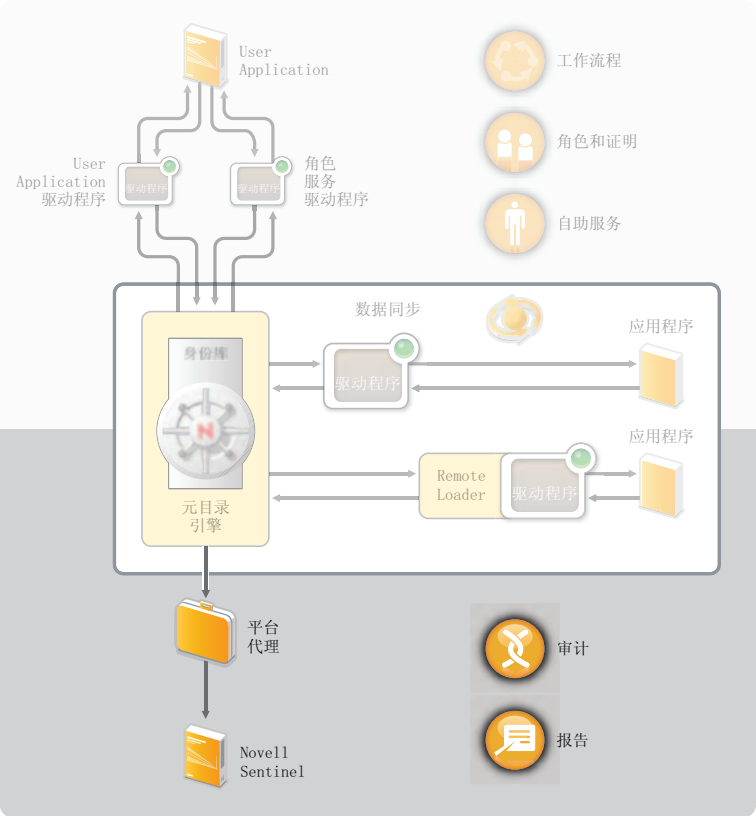
“ 角色管理员 ” 除了可执行与 “ 角色模块管理员 ” 相同的操作之外，还能管理责任分离约束、配置角色系统和运行所有报告。此外， “ 角色模块管理员 ” 在角色系统中没有范围限制，而 “ 角色管理员 ” 的范围却限制于特定用户、组和角色。

证明：角色证明可确定用户对贵组织中资源的访问权，错误的指派可能会危及与企业和政府规定的一致性。 Identity Manager 可通过证明流程帮助您验证角色指派的正确性。使用此流程，个人用户可验证各自的简介信息，而角色管理员可验证角色指派和责任分离违反。

2.3 审计和报告

审计和报告借助和 Novell Sentinel™ 的集成来提供，如以下图表所示。

图 2-4 *Identity Manager 审计和报告*



平台代理：平台代理从元目录引擎中截获事件并将事件发送到 Novell Sentinel 系统。

Novell Sentinel：Novell Sentinel 是一种安全信息和事件管理 (SIEM) 解决方案，可使系统网络、应用程序和安全日志的收集、分析与报告自动化。 Novell Sentinel 单独销售。

有关 Novell Sentinel 的更为完整的介绍 （包括如何购买该产品），请访问 Novell Sentinel 站点 (http://www.novell.com/products/sentinel/)。

Identity Manager 工具

3

Identity Manager 提供了三种主要工具来帮助您建立和维护 Identity Manager 系统：Designer、iManager 和 User Application 管理控制台。

使用 Designer 可在脱机环境中创建和配置 Identity Manager 系统，然后将更改部署到在线系统。您可使用 iManager 执行与 Designer 相同的任务，还可监视系统的运行状态；但是在 iManager 中进行的更改会立即部署，因此我们建议您将 iManager 用于简单管理任务，而将 Designer 用于要求部署前进行建模和测试的复杂配置任务。

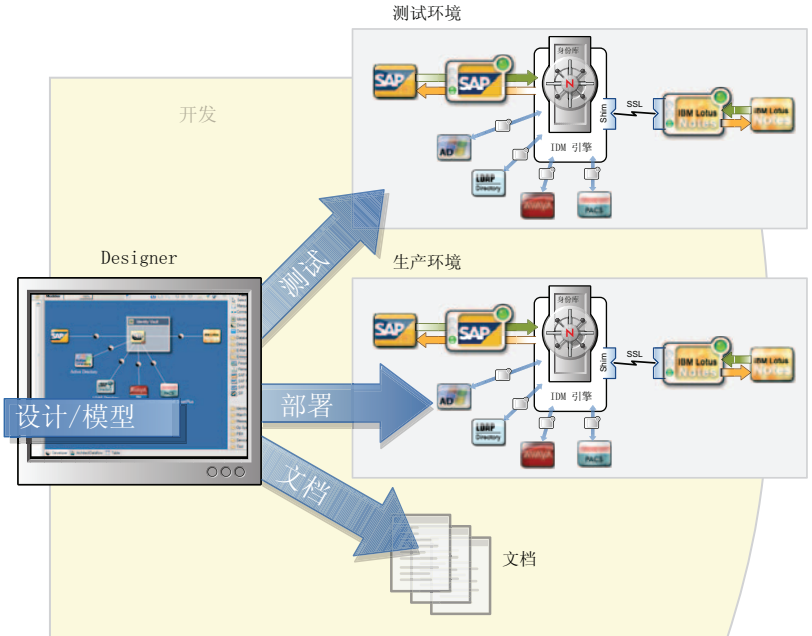
使用 User Application 管理控制台可通过创建和修改页面与 Portlet 来管理应用程序的外观。您还可修改应用程序设置 （如超速缓存和日志记录设置）并可配置特定于 User Application 的供应功能的委托和代理设置。

以下各节提供有关其中各个工具的详细信息：

3.1 Designer

Designer 是基于 Eclipse* 的工具，可帮助您设计、部署和记录 Identity Manager 系统。使用 Designer 的图形界面，您可在脱机环境中设计和测试系统、将系统部署到生产环境以及记录已部署系统的所有细节。

图 3-1 *Designer for Identity Manager*



尽管可以在不使用 Designer 的情况下建立 Identity Manager 系统，但这会困难得多，不建议这样操作。

设计：Designer 提供了一个图形界面，通过该界面，可为您的系统建模。该界面包括多个视图，允许您创建和控制 Identity Manager 与应用程序之间的连接、配置策略以及控制数据在已连接应用程序之间的流动方式。

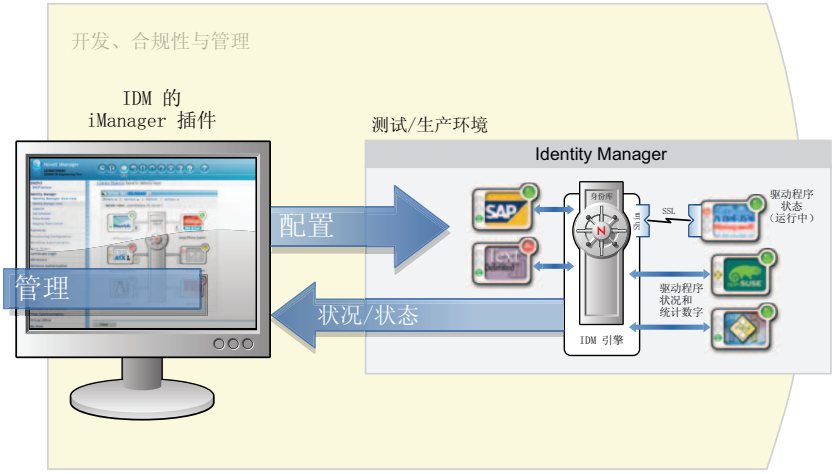
部署：仅当启动部署时，您在 Designer 中进行的操作才会部署到生产环境。这使您有机会进行试验、测试结果并解决所有问题，然后再在生产环境中实施。

文档：您可生成显示系统层次结构、驱动程序配置、策略配置等内容的详尽文档。基本上，您已具备所需的所有信息，足可了解系统的技术方面，同时还可帮助您校验是否与业务规则和策略一致。

3.2 iManager

Novell® iManager 是基于浏览器的工具，提供了对众多 Novell 产品 （包括 Identity Manager）的单点管理功能。通过使用用于 iManager 的 Identity Manager 插件，您可管理 Identity Manager 并接收有关 Identity Manager 系统的实时运行状态信息。

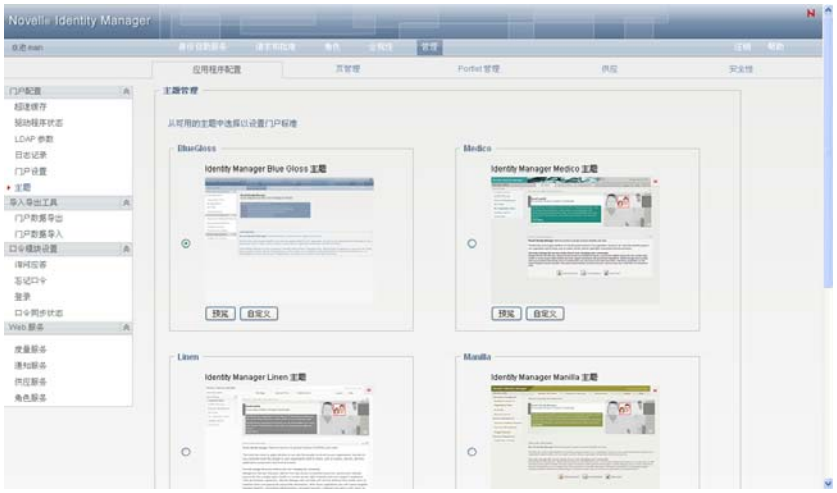
图 3-2 *Novell iManager*



3.3 User Application 管理控制台

User Application 提供了基于万维网的管理控制台，使您可以配置、管理和自定义口令自助服务、角色和供应。对于指派有管理权限的任何人，将管理控制台作为 *管理*选项卡添加在 User Application 中。

图 3-3 “User Application 管理 ” 页



“User Application 管理 ” 页提供了以下选项卡：

- **应用程序配置：** 允许您配置超速缓存、 LDAP 参数、日志记录、主题和口令模块设置。
- **页面管理：** 允许您创建新页面或自定义现有 “ 身份自助服务 ” 页
- **Portlet 管理：** 允许您创建新的 Portlet 或自定义在 “ 身份自助服务 ” 页上使用的现有 Portlet。
- **供应：** 允许您配置委托、代理、任务、数字签名服务和引擎与群集设置。
- **安全：** 允许您定义具有供应管理员和 User Application 管理员特权的人员。