概述指南

Novell®
Identity Manager

4.0.1

2011 年 04 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.
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

本指南向您介绍 Novell Identity Manager，它是一种用于跨物理环境、虚拟环境和云环境管理身份与访问权限的 WorkloadIQ 产品。本指南说明 Identity Manager 在帮您降低成本和保证合规性的同时可帮您解决的业务问题。它还从技术方面简要介绍可用于创建 Identity Manager 解决方案的 Identity Manager 组件和工具。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 文档网站 (http://www.novell.com/documentation/idm401/index.html)。

其他文档

有关 Identity Manager 驱动程序相关的文档，请参见 Identity Manager 驱动程序网站 (http://www.novell.com/documentation/idm401drivers/index.html)。

Identity Manager 和业务流程自动化

1

本部分确定通过实施 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 4 章 “Identity Manager 体系结构 ”（第 21 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 希望拥有 Oracle 财务数据库的访问权，这需要您为其获得其他三位经理的批准。
- 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、审计和报告这些功能都使用由业务策略驱动的多系统数据同步来实现涉及供应用户和管理口令的流程自动化，它们是 IT 组织最困难也是最耗时的两项职责。

图 1-1 Identity Manager 核心功能

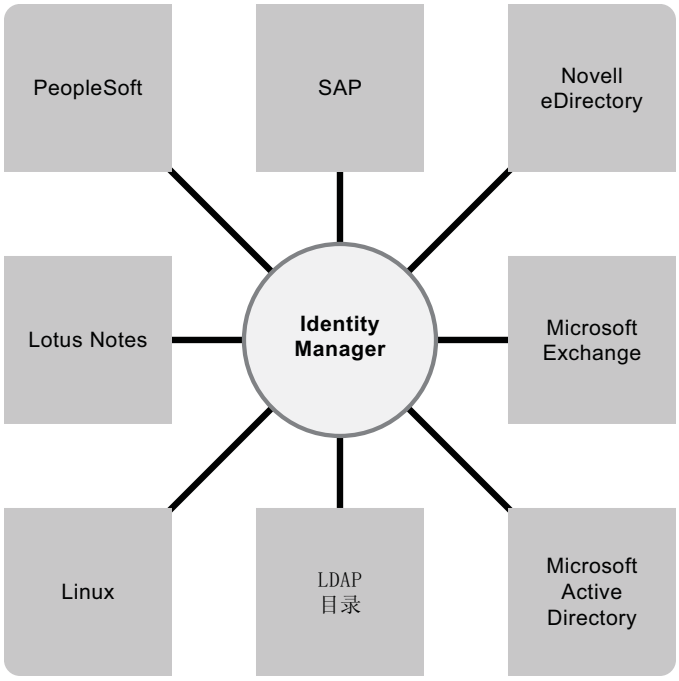
以下各节向您介绍 Identity Manager 的这些功能以及这些功能可如何帮助您成功地满足贵组织中的身份需求：

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同步、转换和分布信息，例如 SAP、 PeopleSoft、 Salesforce、 Microsoft SharePoint、 Lotus Notes、 Microsoft Exchange、 Microsoft Active Directory、 Novell eDirectory、 Linux 和 UNIX 以及 LDAP 目录。

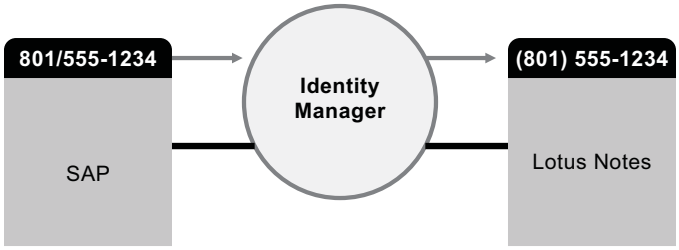
图 1-2 连接多个系统的 Identity Manager



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。

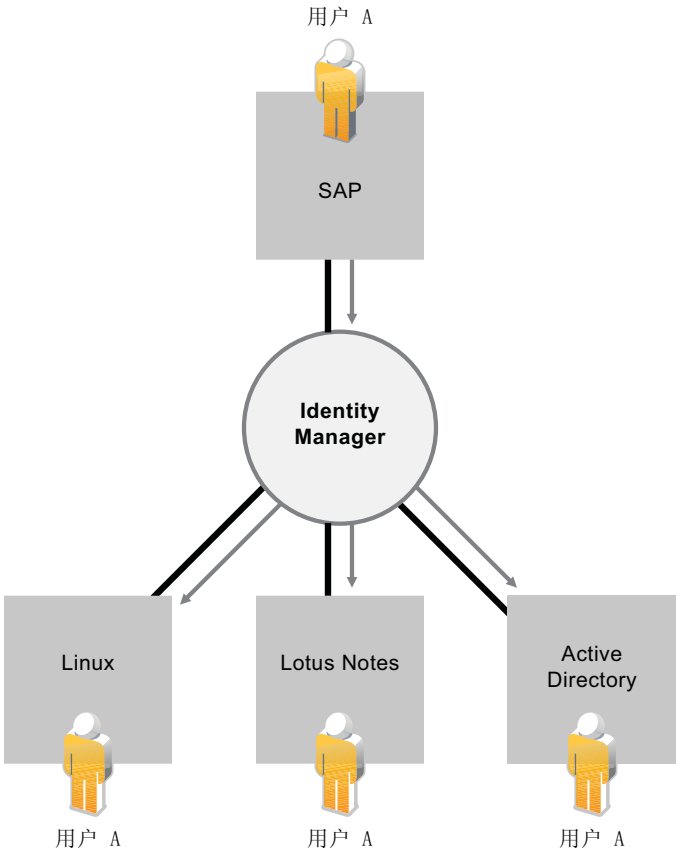
在以下图表中，SAP HR 数据库是用户的电话号码的权威来源。Lotus Notes 系统也使用电话号码，因此 Identity Manager 将号码转换为需要的格式并将其与 Lotus Notes 系统共享。只要 SAP HR 系统中的电话号码发生更改，更改的号码就会同步到 Lotus Notes 系统中。

图 1-3 已连接系统之间的数据同步



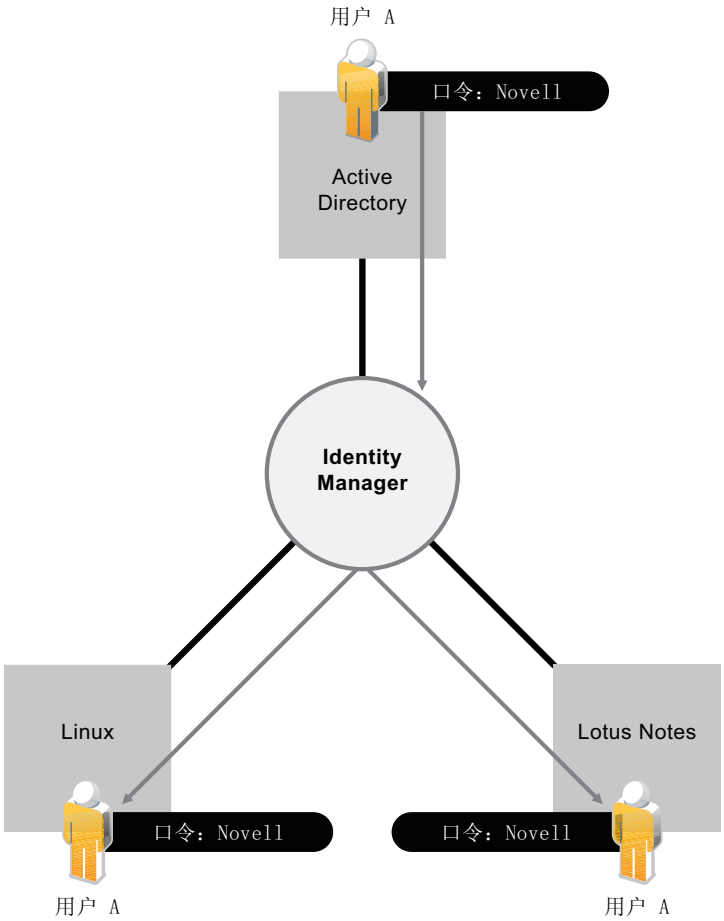
管理现有用户的数据仅仅是 Identity Manager 的数据同步功能的开始。此外， Identity Manager 还可在目录 （如 Active Directory）、系统 （如 PeopleSoft 和 Lotus Notes）和操作系统 （如 UNIX 和 Linux）中创建新用户帐户及去除现有帐户。例如，向 SAP HR 系统中添加新员工时， Identity Manager 可自动在 Active Directory 中创建新用户帐户，在 Lotus Notes 中创建新帐户以及在 Linux NIS 帐户管理系统中创建新帐户。

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

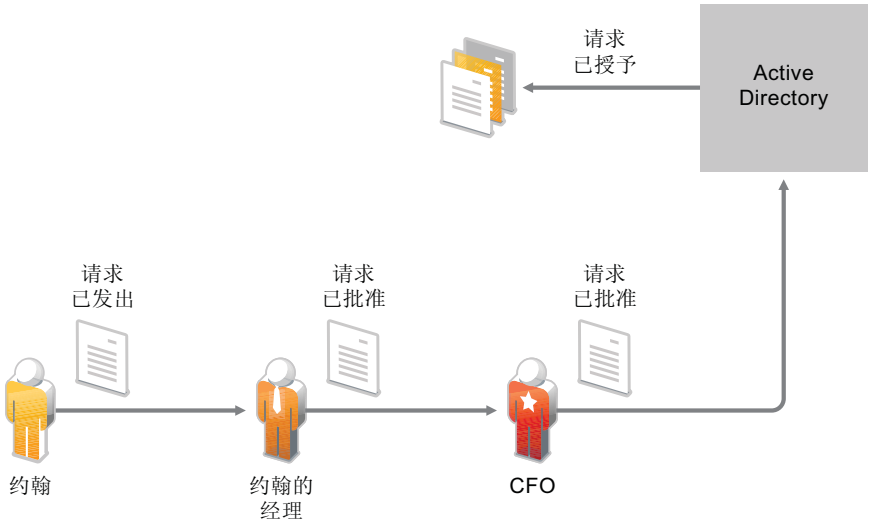


1.2 工作流程

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*



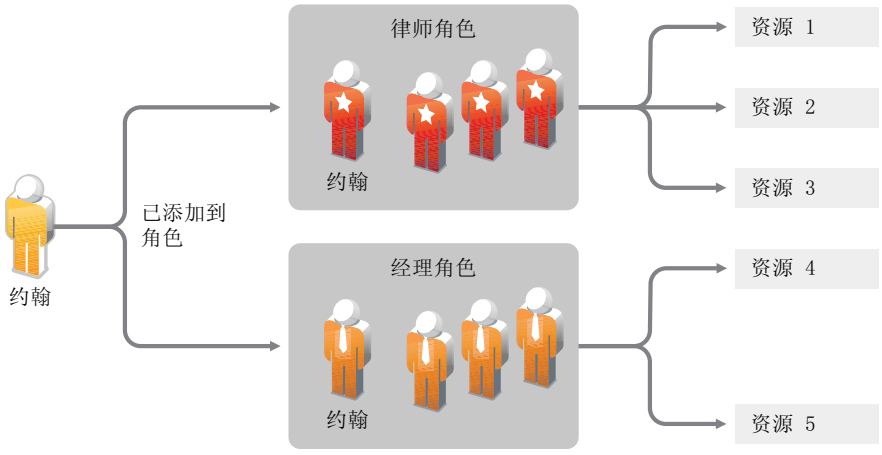
工作流程可在某个特定事件发生时 （例如，向 HR 系统中添加新用户）自动启动，也可通过用户请求手动启动。要确保批准能够及时发生，可设置代理批准者和批准小组。

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*



您可以将用户自动添加到角色中，以作为组织中所发生的事件的结果 （例如，将职称为律师的新用户添加到您的 SAP HR 数据库）。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

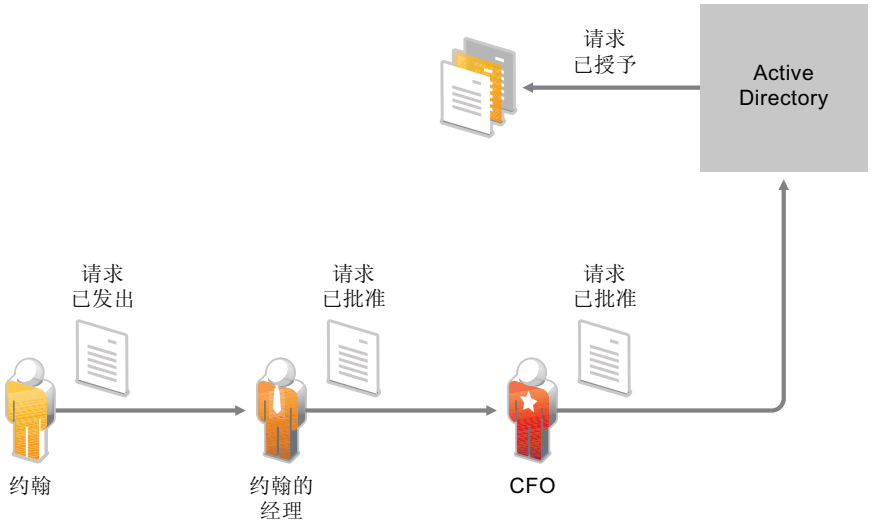
您的许多业务经理和部门可能强烈要求自己管理用户信息和访问需求，而不是依赖您或您的手下。您是不是不止一次听到“为什么我不能在我的公司目录中更改自己的手机号码？”或“我就是在市场部。为什么我必须要致电咨询台才能访问营销信息数据库？”

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 11 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、报告和合规性

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？

有了 Identity Manager 您会感到很轻松，因为无论是过去的还是现在的所有用户供应活动都会针对审计目的进行跟踪和记录。 Identity Manager 包含一个智能储存库，储存有关贵组织中身份库和受管系统的实际状态和所需状态的信息。通过查询仓库，可检索确保贵组织完全符合相关业务法律和规定的所有所需信息。

该仓库使您能够全面了解业务权利，提供了解授予组织中用户身份的授权和许可权限的过去和当前状态的所需信息。掌握这些信息后，您甚至可以回答最复杂的管理风险和合规性 (GRC) 问题。

Identity Manager 包含预定义报告，使您能够针对身份信息仓库执行查询以证明符合业务、IT 和公司策略。如果预定义报告不能满足您的需求，还可以创建自定义报告。

Identity Manager 4.0.1 功能

2

Novell Identity Manager 4.0.1 提供智能身份框架，它通过降低成本并确保跨物理、虚拟和云环境的合规性来利用您现有 IT 资产和新计算模型 （如软件即服务 (SaaS)）。借助于 Novell Identity Manager 解决方案，您可以确保自己的企业具有最新的用户身份信息。可以通过管理、供应和取回防火墙内的身份并扩展至云来保留企业层面的控制。 Identity Manager 还有助于您将合规性管理扩展至云。

Identity Manager 4.0.1 为您提供集成身份管理、角色管理、报告以及包管理功能，以预配置和自定义 Identity Manager 驱动程序策略。您还可以在各种系统域内应用安全性策略。Identity Manager 允许您在不断增长的监管要求下管理用户生命周期，通过更具战略性的用户供应来实行更具体的保护，以达到防火墙内或云环境中倍受关注的安全性要求。智能身份框架帮助您利用现有基础结构和新计算模型 （如 SaaS）。

2.1 Identity Manager 4.0.1 新功能

- **资源请求活动：**资源请求活动允许您实现向用户授予或撤消资源的自动化。例如，您可以写一个供应请求定义，在某新员工入职第一天供应他 / 她需要的所有资源。使用资源请求活动，您可以自动化对该员工使用指定资源的批准。有关资源请求活动的更多细节，请参见 《*User Application：设计指南*》中的 “ *资源请求活动* ”。
- **Telemetry：**Identity Manager Telemetry 是 Identity Manager 4.0.1 引入的一项新作业。该作业充当用量计数工具或许可证监视工具，向 Identity Manager 客户提供值，因为他们可以添加更多许可证或淘汰不使用的许可证。客户还可以获得不活动用户定价等好处。

  Telemetry 作业收集有关安装的 Identity Manager 软件和硬件以及客户环境中 Identity Manager 驱动程序用量的细节。客户在 Novell Customer Center 中注册后，信息将发送到 Novell。此信息允许 Novell 更好地支持客户，更高效且有效地开发和测试 Identity Manager，并在将来做出重要决策。有关更多信息，请参见 《*Identity Manager 4.0.1 作业指南*》。
- **报告：** 身份报告模块中添加了以下报告：
  - **身份库中的用户状态更改：**显示身份库用户的重要事件。
  - **身份库中的用户口令更改：**显示身份库中的所有用户口令更改。
  - **按接收人排列的访问请求：**显示按接收人分组的资源指派工作流程过程。
  - **按请求者排列的访问请求：**显示按请求者分组的资源指派工作流程过程。
  - **按资源排列的访问请求：**显示按资源分组的资源指派工作流程过程。

2.2 Identity Manager 4.0 功能

除了本节前面列出的新增功能外， Identity Manager 4.0.1 还包括 Identity Manager 4.0 中引入的以下功能。

- **综合的即用型报告：**Novell Identity Manager 4.x 产品套件的集成报告模块增强了跨内部部署及云部署合规性的可见性。报告功能使您能够看到用户的身份状态和访问权限，或报告用户操作和供应历史记录。有关更多信息，请参见 《*身份报告模块指南*》。
- **增强了集成功能：**为了创建所有组件都位于同一服务器上的新 Identity Manager 解决方案， Novell Identity Manager 4.x 包括一个集成安装程序，它简化了安装过程，使您能够更快速地设置系统。使用集成安装程序可以在一次操作中安装所有组件，而不再需要分别安装每个 Identity Manager 组件。有关更多信息，请参见 《*Identity Manager 4.0.1 集成安装指南*》。
- **包管理：**Identity Manager 4.x 包括一个新概念，称为包管理。包管理是一种用于创建、分发和消耗 Identity Manager 策略内容的高质量构建块的系统。有关 Identity Manager 包的更多信息，请参见 《*Designer 4.0.1 for Identity Manager 4.0.1 管理指南*》中的*配置包*。
- **云就绪驱动程序：**Identity Manager 4.x 提供多个与 SaaS 即用集成的驱动程序。这些驱动程序通过提供诸如供应、取回、请求 / 批准过程、口令更改、身份配置文件更新以及报告等功能，可与 SaaS 和托管的解决方案无缝集成。新增的 SharePoint 和 Salesforce.com 驱动程序有助于贵公司的身份与云应用程序集成。有关云就绪驱动程序的更多信息，请参见 《*Identity Manager 4.0.1 Driver for Salesforce.com 实施指南*》和 《*Identity Manager 4.0.1 Driver for SharePoint 实施指南*》。
- **嵌入式身份库：**Novell Identity Manager 4.x 产品的体系结构包括一个可选的内置身份库，因此您无需为身份创建和管理单独的目录结构。而且， Novell Identity Manager 4.x 产品系列还包括多个驱动程序，可轻松将身份库与您企业中的其他身份信息储存库集成，例如 Active Directory 或各种数据库。有关更多信息，请参见 《*Identity Manager 4.0.1 集成安装指南*》。
- **简化了身份和角色管理：**Novell Identity Manager 4.x 产品系列简化了将不同角色储存库集成到一个统一位置的过程，这意味着您无需管理各个身份信息源。通过使用角色映射管理器及其新直观界面，您甚至可以将第三方角色和配置文件映射到 Novell Identity Manager 4.x。有关更多信息，请参见 《*Novell Identity Manager 角色映射管理器 4.0.1 用户指南*》。
- **增强的工具：**Designer 是一个重要的工具，它包括的业务和技术信息可创建满足您需要的 Identity Manager 解决方案。我们对 Designer 4.x 进行了几处增强。请查看*新功能* (http://www.novell.com/documentation/designer401/resources/whatsnew/index.html) 中的 Designer 增强功能列表。有关 Designer 功能和管理的信息，请参见 《*Designer 4.0.1 for Identity Manager 4.0.1 管理指南*》。此外， Identity Manager 包含一种有助于简化数据分析和清理过程的工具。有关更多信息，请参见 《*Analyzer 4.0.1 for Identity Manager 管理指南*》。

Identity Manager 系列

3

为满足不同的客户需求， Identity Manager 系列分为三个不同的产品组：

- Identity Manager Advanced Edition
- Identity Manager Standard Edition
- Compliance Management Platform

Identity Manager Advanced Edition 包括 Identity Manager Standard Edition 的 Identity Manager 功能及其他功能。 Compliance Management Platform 包括 Identity Manager Advanced Edition 和 Standard Edition 功能及其他工具。

图 3-1 *Identity Manager 产品组*

有关 Identity Manager Advanced Edition 和 Standard Edition 的功能比较，请参见 Identity Manager 版本比较 (http://www.novell.com/products/identitymanager/features/identitymanager-version-comparison.html)。

- 第 3.1 节 “Identity Manager Advanced Edition” （第 18 页）
- 第 3.2 节 “Identity Manager Standard Edition” （第 18 页）
- 第 3.3 节 “Compliance Management Platform” （第 20 页）
- 第 3.4 节 “ 激活 Identity Manager Standard Edition 和 Advanced Edition” （第 20 页）

3.1 Identity Manager Advanced Edition

Identity Manager 4.0.1 Advanced Edition 包括产品的全部功能，主要针对企业级用户供应。它包括 Standard Edition 的身份自助服务功能，以及所有基于工作流程的供应系统功能。Advanced Edition 使您能够启动工作流程批准过程，供应角色和资源，以及利用合规性功能。 Advanced Edition 还包括工作仪表板。

Identity Manager 4.0.1 Advanced Edition 是作为单独的 ISO 提供的。

注释：Identity Manager 4.0.1 Advanced Edition 有一个 90 天评估包。

3.2 Identity Manager Standard Edition

为满足不同的客户需求， Novell 引入了 Identity Manager 4.0.1 Standard Edition。 Standard Edition 包括 Identity Manager Advanced Edition 的部分功能。

Standard Edition 继续提供 Identity Manager 先前版本中的所有功能：

- 身份同步
- 基于规则的自动化供应
- 口令管理和口令自助服务
- 带现有白页和组织结构图功能的身份自助服务

  注释：集成模块对于 Identity Manager Advanced Edition 和 Standard Edition 继续保持一致。

除了上面列表列出的功能外， Standard Edition 还包括 Advanced Edition 中提供的以下功能：

- 用户界面外观
- 报告模块
- 内容打包框架
- 支持 REST API 和单点登录 (SSO)
- 用于调解的 Analyzer 工具

Identity Manager 4.0.1 Standard Edition 提供了单独的可下载 ISO。要从 Standard Edition 升级到 Advanced Edition，请使用 Identity Manager Advanced Edition ISO。您需要应用正确的激活才能升级到 Advanced Edition。有关从 Standard Edition 升级到 Advanced Edition 的更多信息，请参见 《*Identity Manager 4.0.1 升级和迁移指南*》。

不能使用 Identity Manager Standard Edition ISO 从现有 Identity Manager Advanced Edition 切换到 Standard Edition。要从 Identity Manager Advanced Edition 切换到 Standard Edition，请从服务器卸装 Advanced Edition，然后从 Identity Manager 媒体安装 Standard Edition ISO。

Identity Manager Standard Edition 中没有以下功能：

- 没有角色映射管理器 (RMA)。
- 对 User Application 有以下限制：
  - **“身份自助服务”选项卡是唯一对企业用户可用的选项卡：**在 Standard Edition 中，如果您以企业用户身份登录 User Application，则只能看到*身份自助服务*选项卡。如果以 User Application 管理员身份登录，则还可以看到*管理*选项卡。

- **不支持角色和资源：**使用角色和资源需要 Advanced Edition。 Standard Edition 中没有*角色和资源*选项卡。
- **不支持“合规性”选项卡：***合规性*选项卡需要 Identity Manager 4.0.1 Advanced Edition。 Standard Edition 中没有*合规性*选项卡。
- **没有工作仪表板：** Standard Edition 中没有*工作仪表板*选项卡。
- **不支持自定义角色：**没有定义自定义角色的功能。 Standard Edition 仅支持系统角色。
- **不支持工作流程：**不支持启动批准工作流程的功能。
- **REST API：**没有与角色、资源、工作流程等相关的 REST API。
- **简化了安全模式：**Standard Edition 提供了具体的安全模式，以避免误用 Advanced Edition 中提供的功能。您只需要指派以下管理员角色：
  - **用户应用程序管理员：**User Application 管理员有权执行与 Identity Manager User Application 相关的所有管理功能。这包括访问 Identity Manager 用户界面的*管理*选项卡以执行其支持的任何管理操作。
  - **报告管理员：**该用户具有报告域内的所有功能。报告管理员可以对报告域内的所有对象执行所有操作。
  - **安全管理员：**此角色为成员提供安全域内的所有功能。安全管理员可以对安全域内的所有对象执行所有可能的操作。该角色可以委托和授予用户对所有 Identity Manager Advanced Edition 功能的访问权；因此，它与 User Application 管理角色和报告管理角色是分开的。

注释：出于测试目的， Novell 没有锁定 Standard Edition 中的安全模式。因此，安全管理员可以指派所有域管理员、委托的管理员以及其他安全管理员。但是，如“最终用户许可协议”中所述，生产中不支持使用这些高级功能。在生产环境中，所有管理员指派都受到许可限制。Novell 可以收集审计数据库中的监视数据以确保生产环境符合要求。同时， Novell 建议仅给予一个用户安全管理员的许可权限。

有关 User Application 功能的更多信息，请参见《*Identity Manager Roles Based Provisioning Module 4.0 User Application：管理指南*》。

- 对身份报告模块有以下限制：
  - **Managed System Gateway Driver 是禁用的：**Managed System Gateway Driver 可以从 Identity Manager 4.0.1 中已启用进行数据收集的任何受管系统提取信息，只要该受管系统支持权利。

    Managed System Gateway Driver 在 Identity Manager Standard Edition 中是禁用的。
  - **报告仅显示身份库数据：**使用 Identity Manager Standard Edition 生成的报告仅显示身份库数据，不显示有关受管（已连接）系统的数据。
  - **报告不显示历史数据：**Standard Edition 不提供收集历史状态数据进行报告的功能。在 Standard Edition 中，只能查看当前状态数据。
  - **未提供部分报告：**Identity Manager 4.0 和 4.0.1 中添加了几个新报告。 Standard Edition 不包括适用于已连接系统和历史数据的报告。
  - **部分报告不包含任何数据：**部分报告仅当您购买了 Identity Manager Advanced Edition 时才有意义，因为这些报告使用 Standard Edition 中未提供的数据，例如角色、资源和工作流程过程。

3.3 Compliance Management Platform

Novell Compliance Management Platform 将 Novell 身份、访问和安全管理产品与一个经证实的工具集合并，从而简化了解决方案的实施和管理。该平台将身份和访问信息与安全信息和事件管理技术集成，以便您能够实时、整体地查看整个企业中的所有网络事件。这种紧密的集成提供了强大的风险管理功能，以确保业务策略成为自动化的 IT 实践。有关更多信息，请参见 Compliance Management Platform 网站 (http://www.novell.com/documentation/ncmp10/) 。

3.4 激活 Identity Manager Standard Edition 和 Advanced Edition

您必须在安装后的 90 天内激活 Identity Manager Advanced Edition 和 Standard Edition，否则它们将关闭。Identity Manager Advanced Edition 和 Standard Edition ISO 将工作 90 天整。在这 90 天内或之后的任何时间，您都可以选择激活 Identity Manager 产品。有关更多信息，请参见《*Identity Manager 4.0.1 Framework 安装指南*》中的 “ 激活 Novell Identity Manager 产品 ”。

如果将 Standard Edition 激活应用于现有未激活的 Advanced Edition 系统，则元目录服务器和驱动程序将停止工作。

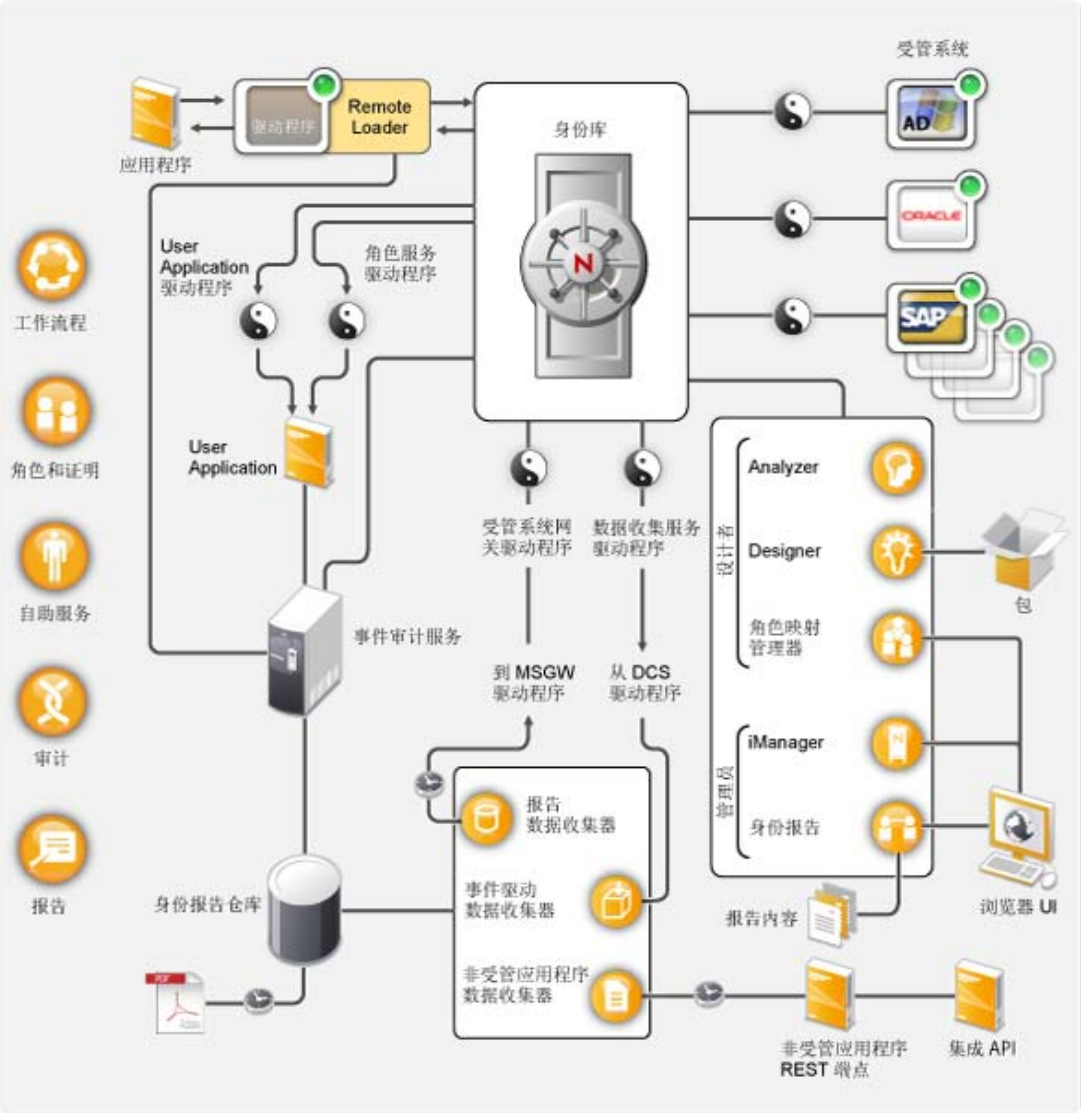
注释：如果您同时拥有 Identity Manager Advanced Edition 和 Identity Manager Standard Edition，请确保在正确的服务器上使用了正确的激活。

Identity Manager 体系结构

4

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 7 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 4-1 *Identity Manager 高级体系结构*



以下各节中将分别介绍每种组件：

- 第 4.1 节 “ 数据同步 ”（第 22 页）
- 第 4.2 节 “ 工作流程、角色、证明和自助服务 ”（第 25 页）
- 第 4.3 节 “ 审计和报告 ”（第 27 页）

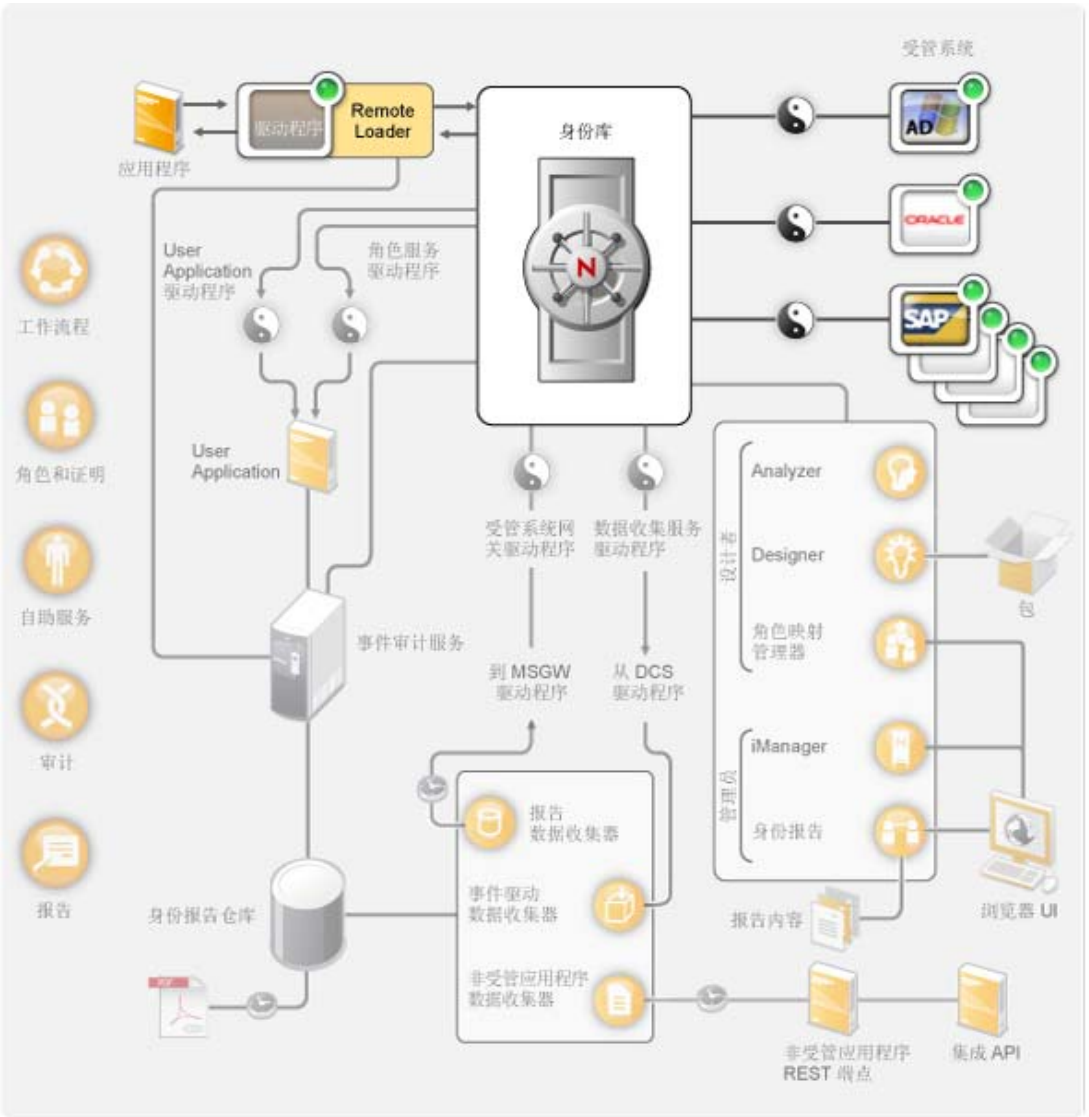
4.1 数据同步

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，该更改会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、Identity Manager 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 4-2 *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 4.1.1 节 “ 组件 ”（第 23 页）
- 第 4.1.2 节 “ 主要概念 ”（第 23 页）

4.1.1 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。

Identity Manager 引擎 : 当数据在身份库或已连接应用程序中发生更改时， Identity Manager 引擎将处理这些更改。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。 Identity Manager 引擎也称为元目录引擎。

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：将应用程序中的数据更改 （事件）报告给 Identity Manager 引擎，以及执行由 Identity Manager 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。如果应用程序与 Identity Manager 引擎位于同一服务器上，则您只需要将驱动程序安装到该服务器上即可。但是，如果应用程序与 Identity Manager 引擎位于不同的服务器上 （也就是说，应用程序所在的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 Identity Manager 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*。

4.1.2 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 Identity Manager 引擎，后者通过与驱动程序通道关联的过滤器和策略集来处理该文档。将所有处理应用到 XML 文档后， Identity Manager 引擎将使用该文档启动对身份库 （发布者通道）的相应更改，或驱动程序使用该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构建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电子邮件，请求在财务系统中批准新建一个员工帐户。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，为员工指派 “ 会计 ” 角色。 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 Identity Manager 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。

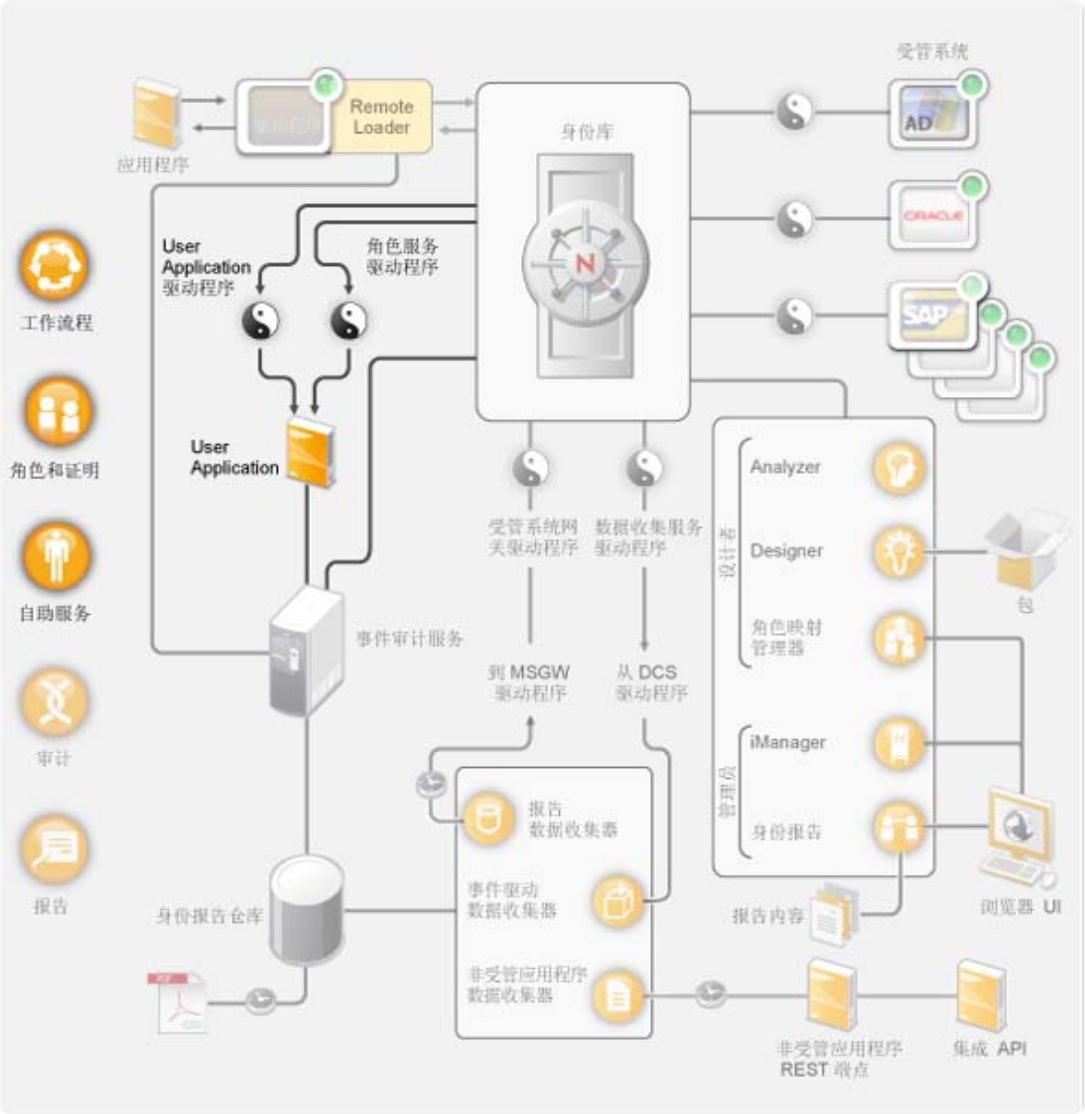
4.2 工作流程、角色、证明和自助服务

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 Roles Based Provisioning Module 是 Identity Manager 4.0.1 Advanced Edition 的一部分。它包括带有高级自助服务、批准工作流程、基于角色的供应、责任分离限制和证明功能的标准 User Application。 Identity Manager 4.0.1 Advanced Edition 包含标准功能和 Roles Based Provisioning Module 功能。

图 4-3 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 4.2.1 节 “ 组件 ”（第 26 页）
- 第 4.2.2 节 “ 主要概念 ”（第 27 页）

4.2.1 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。

Role and Resource Service 驱动程序：Role and Resource Service 驱动程序可管理所有角色和资源指派，启动角色和资源指派请求 （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。

4.2.2 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让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有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。

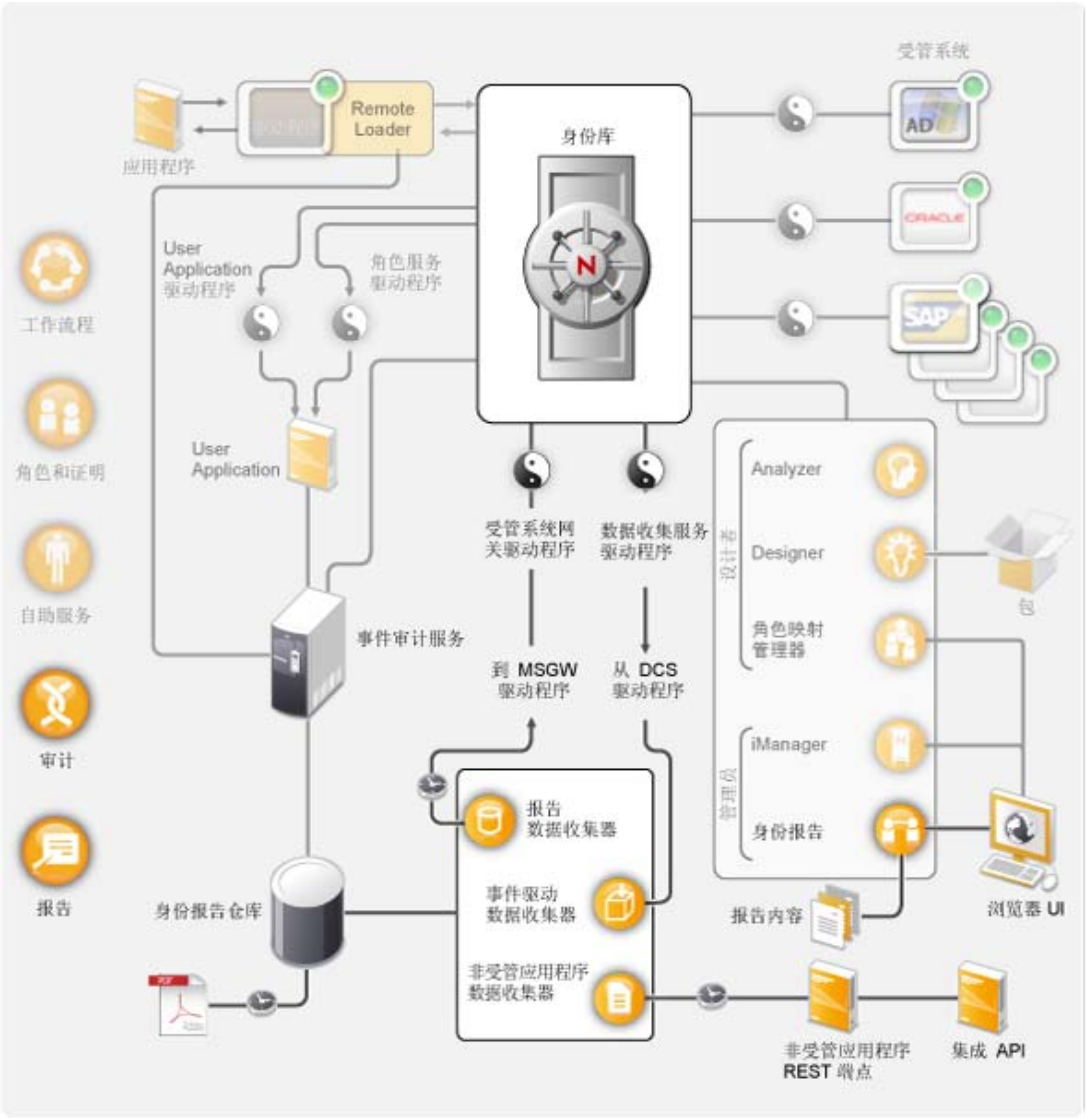
“ 角色管理员 ” 除了可执行与 “ 角色模块管理员 ” 相同的操作之外，还能管理责任分离约束、配置角色系统和运行所有报告。 “ 角色模块管理员 ” 在角色系统中没有范围限制，而 “ 角色管理员 ” 的范围限于特定用户、组和角色。

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。

4.3 审计和报告

审计和报告是 Identity Manager 4.0.1 的一项新功能，由身份报告模块提供，如下面的图表所示。

图 4-4 Identity Manager 审计和报告



身份报告模块生成显示 Identity Manager 配置各方面相关的重要业务信息，包括从身份库和受管系统 （如 Active Directory 或 SAP）中收集的信息。身份报告模块使用以下组件管理数据：

事件审计服务：该服务捕获与在报告模块中所执行的操作 （比如报告的导入、修改、删除或安排）关联的日志事件。事件审计服务 (EAS) 捕获与在基于角色的供应模块 (RBPM) 和角色映射管理器 (RMA) 中所执行的操作关联的日志事件。

身份信息仓库：是以下类型信息的储存库：

- 报告管理信息 （比如报告定义、报告安排和已完成报告）、用于报告的数据库视图以及配置信息。
- 报告数据收集器、事件驱动的数据收集器和非受管应用程序数据收集器收集的身份数据。
- 审计数据，其中包括事件审计服务收集的事件。

身份信息仓库将其数据储存在 Security Information and Event Management (SIEM) 数据库中。

数据收集服务：该服务从组织内的各种源收集信息。数据收集服务包括三个子服务：

- **报告数据收集器：**使用拉式设计模型从一个或多个身份库数据源中检索数据。它根据一组配置参数确定的周期定期运行收集。为了检索数据，收集器需调用受管系统网关驱动程序。
- **事件驱动的数据收集器：**使用推式设计模型收集由数据收集服务驱动程序捕获的事件数据。
- **非受管应用程序数据收集器：**通过调用专门为每个应用程序编写的 REST 端点，从一个或多个非受管应用程序中检索数据。非受管应用程序是指您企业中未连接到身份库的应用程序。有关详细信息，请参见 《*身份报告模块指南*》中的 “ 用于报告的 REST 服务 ”。

数据收集服务驱动程序：该驱动程序捕获身份库中储存的对象 （比如帐户、角色、资源、组和小组成员资格）的更改。数据收集服务驱动程序向数据收集服务进行注册，并将更改事件 （比如数据同步、添加、修改和删除事件）推入数据收集服务。

捕获的信息记录对以下对象所做的更改：

- 用户帐户和身份
- 角色和角色级别
- 组

  注释：报告模块不支持动态组，只能生成静态组数据的报告。

- 组成员资格
- 供应请求定义
- 责任分离定义和违反
- 用户权利关联
- 资源定义和资源参数
- 角色和资源指派
- 身份库权利、权利类型和驱动程序

受管系统网关驱动程序：该驱动程序从受管系统中收集信息。为了检索受管系统数据，该驱动程序需查询身份库。检索的数据包括以下内容：

- 所有受管系统列表
- 所有受管系统帐户列表
- 受管系统的权利类型、值和指派以及用户帐户配置文件

身份报告：报告模块的用户界面使安排报告在非高峰时段运行以优化性能变得非常简单。有关身份报告模块的详细信息，请参见 《*身份报告模块指南*》。

报告：Identity Manager 包括的预定义报告以有用、能耗尽的方式显示身份信息仓库中的信息。您也可以创建自定义报告。有关报告的详细信息，请参见 *使用 Identity Manager 4.0 报告*。有关自定义报告的信息，请参见 《*身份报告模块指南*》中的 “ 创建自定义报告定义 ”。

非受管应用程序 REST 端点：非受管应用程序是指未连接到身份库，但仍包括您要报告的数据的应用程序。通过为应用程序定义 REST 端点，可以让报告模块从该应用程序中收集数据。

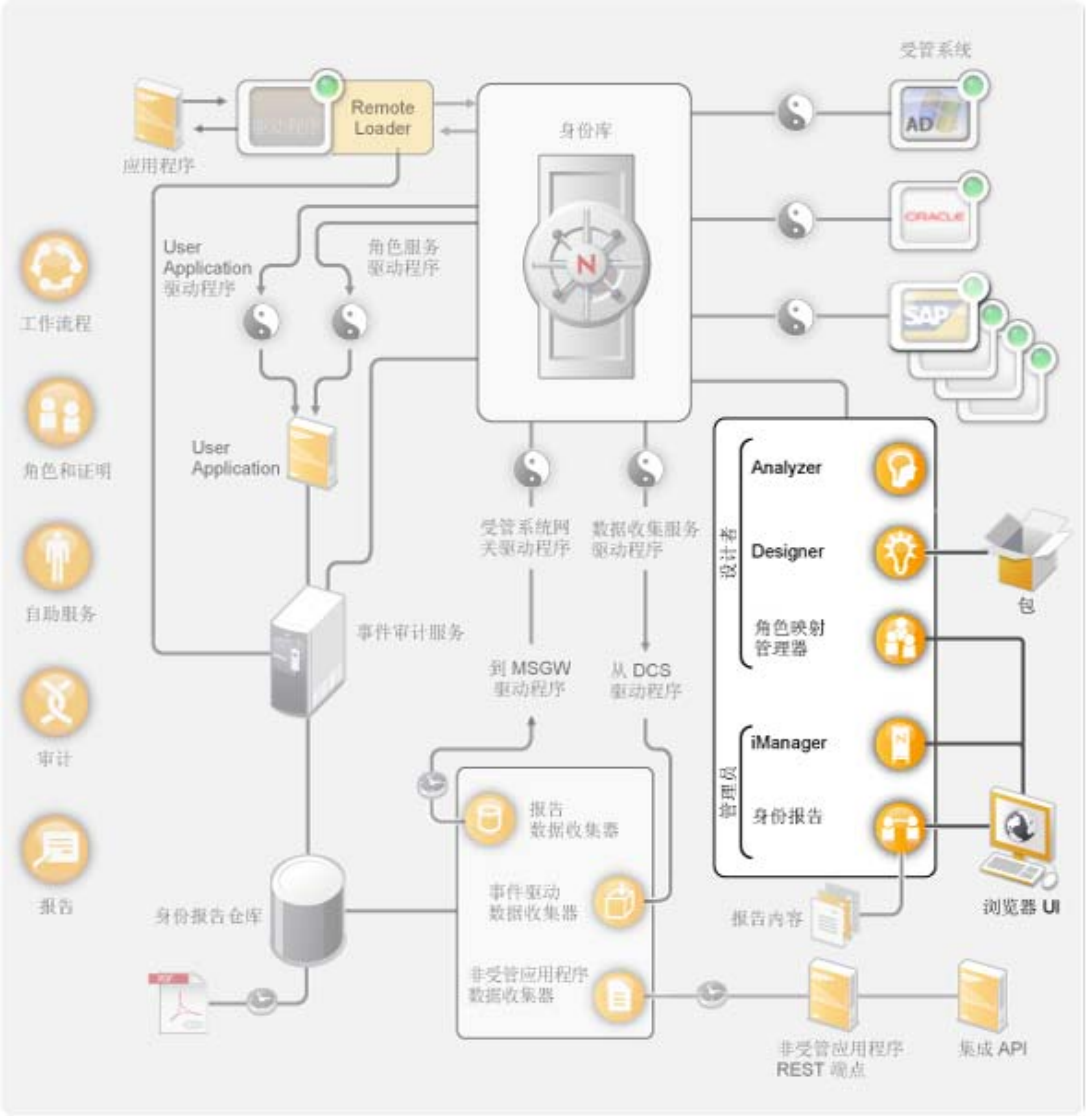
集成 API：身份报告模块提供了一组 REST API，允许为非受管应用程序实施 REST 端点，并编写自定义报告应用程序。

Identity Manager 工具

5

Identity Manager 提供帮助您创建和维护 Identity Manager 解决方案的工具。每种工具都具有特定的功能。

图 5-1 *Identity Manager 工具*



使用 Designer 可在脱机环境中设计、创建和配置 Identity Manager 系统，然后将更改部署到在线系统。 Designer 还提供了包管理功能，用于预配置和自定义 Identity Manager 驱动程序策略。在创建 Identity Manager 解决方案时使用 Analyzer 来分析、清理和准备数据以进行同步。

角色映射管理器用于创建和管理整个 Identity Manager 解决方案中的角色。

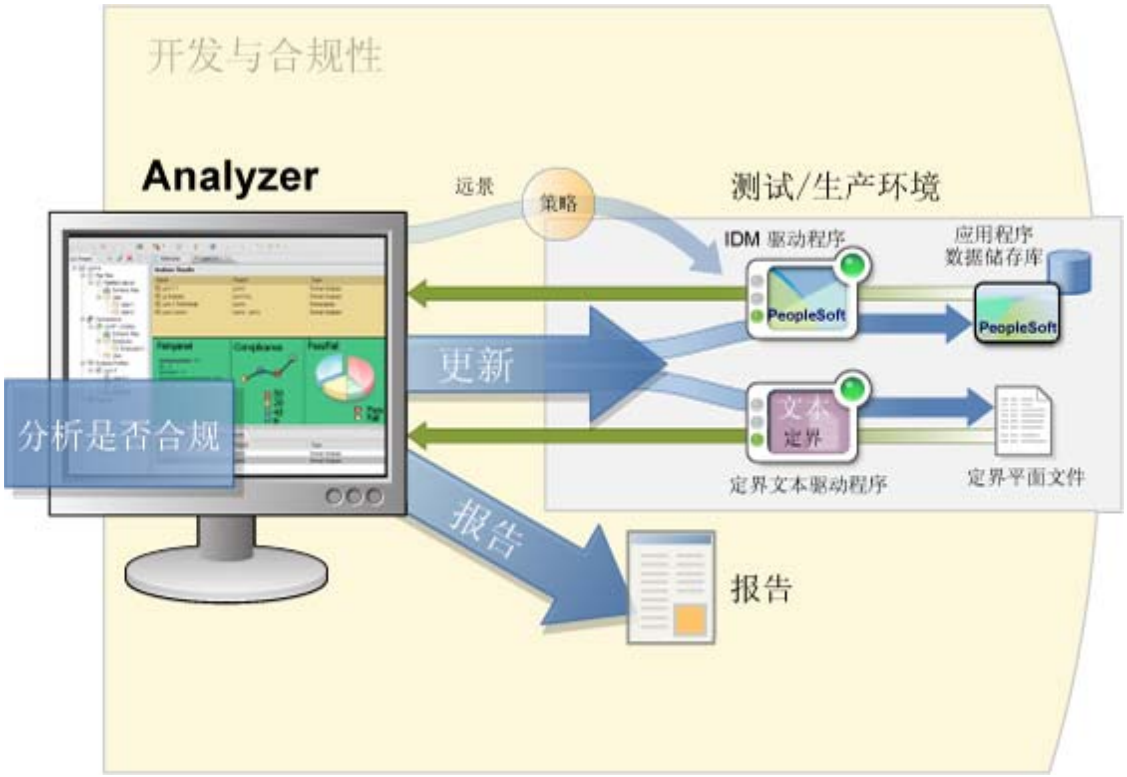
使用 iManager 可执行与 Designer 类似的任务，另外还可监视系统状态，但是在 iManager 中不支持包管理。建议将 iManager 用于管理任务，将 Designer 用于需要在部署前进行包更改、建模和测试的配置任务。

以下各部分提供有关其中各个工具的详细信息：

5.1 Analyzer

Analyzer 是基于 Eclipse 的身份管理工具集，通过提供数据分析、数据清理、数据调解以及数据监视和报告，来帮助您确保遵守内部数据质量策略。 Analyzer 允许您分析、增强和控制企业范围内储存的所有数据。

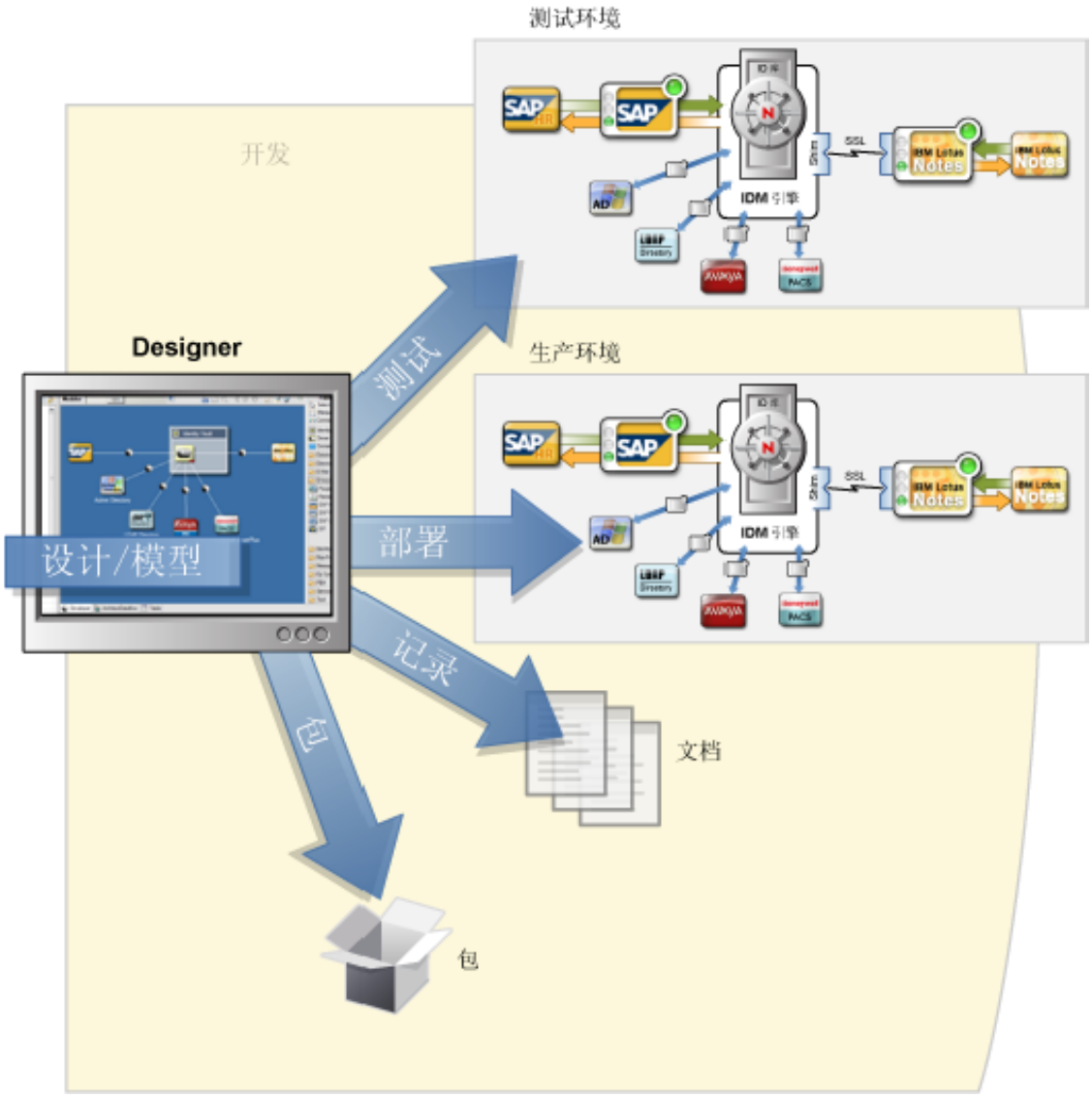
图 5-2 *Analyzer for Identity Manager*



5.2 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 5-3 Designer for Identity Manager



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。

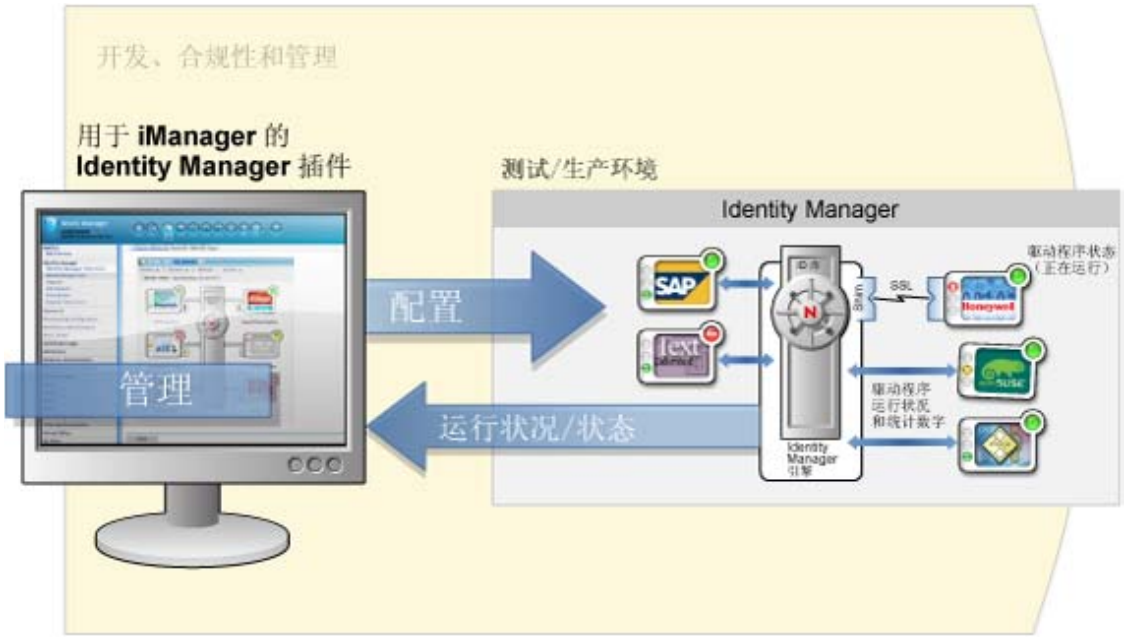
部署：仅当启动部署时，您在 Designer 中进行的操作才会部署到生产环境。这使您有机会进行试验、测试结果并解决所有问题，然后再在生产环境中实施。

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。

5.3 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。

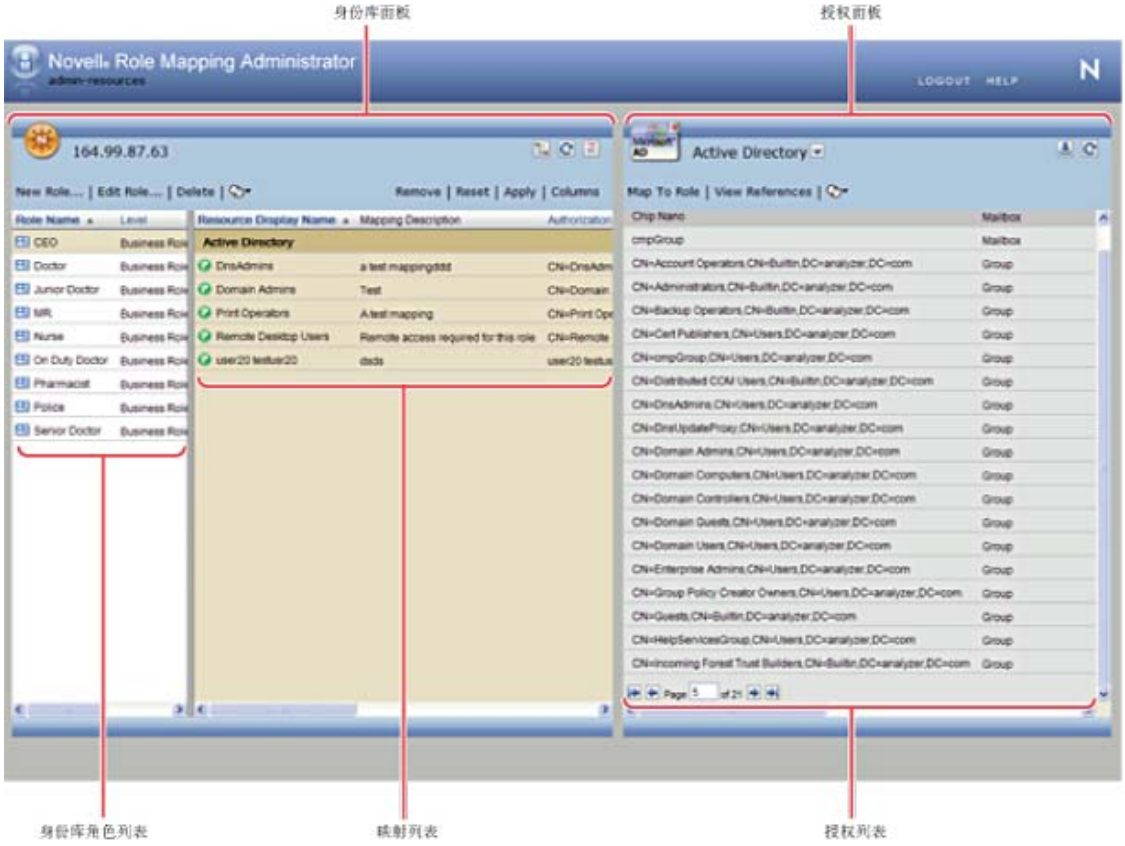
图 5-4 *Novell iManager*



5.4 角色映射管理器

角色映射管理器是一个 Web 服务，可发现您主要 IT 系统内可授予的授权和许可权限。它允许业务分析员 （而不仅仅是 IT 管理员）定义和维护哪些授权与哪些业务角色关联。

图 5-5 *角色映射管理器*



5.5 身份报告

身份报告模块生成显示有关 Identity Manager 配置各方面的重要业务信息，包括从身份库和受管系统 （如 Active Directory 或 SAP）中收集的信息。报告模块提供了一组预定义的报告定义，可用于生成报告。此外，它还允许导入在第三方工具中定义的自定义报告。报告模块的用户界面使安排报告在非高峰时段运行以优化性能变得非常简单。

图 5-6 *身份报告模块*

报告模块提供多个开放式集成点。例如，如果希望收集有关未连接到 Identity Manager 的第三方应用程序的数据，则可以实现自定义 REST 端点以从这些应用程序中收集数据。另外，还可以自定义推入身份库的数据。数据可用后，可以编写自定义报告以查看该信息。

下一步

6

了解构成 Identity Manager 4.0.1 的组件后，下一步是按本文档中的说明创建自己的 Identity Manager 解决方案。以下部分告诉您从本文档的哪些位置查找所列任务：

6.1 计划 Identity Manager 解决方案

设计 Identity Manager 解决方案的第一步是决定您的解决方案在业务中具体做什么。按照《*Identity Manager 4.0.1 框架安装指南*》的 “ 计划 ” 部分中的说明，使用 Designer 创建您的 Identity Manager 解决方案。您还可以按照 《*User Application：设计指南*》中的说明设计您的 User Application 解决方案。

使用 Designer 可以将信息捕获到项目中，与其他人共享信息。使用 Designer 还可以在开始进行更改前对解决方案建模。有关 Designer 的详细信息，请参见 *了解 Designer for Identity Manager*。

6.2 准备同步数据

制定计划后，需要准备您环境中的数据以进行同步。 Analyzer 是用于分析、清理和准备数据进行同步的工具。有关更多信息，请参见 《*Analyzer 4.0.1 for Identity Manager 管理指南*》。

6.3 安装或升级 Identity Manager

制定计划并准备好数据后，即可安装 Identity Manager。如果您拥有的是中小型 IT 环境，而且之前没有用过 Identity Manager，那么最好使用集成安装程序。集成安装程序可安装和配置 Identity Manager 自带的所有组件。有关更多信息，请参见 《*Identity Manager 4.0.1 集成安装指南*》。

如果您已有 Identity Manager 系统，或拥有的是大型 IT 环境，请根据 《*Identity Manager 4.0.1 框架安装指南*》安装或升级不同的 Identity Manager 组件。每个 Identity Manager 组件都独立安装和配置，因此您可以自定义 Identity Manager 解决方案。

- 有关安装说明，请参见 《*Identity Manager 4.0.1 框架安装指南*》中的 “ 安装 ”。
- 有关升级说明，请参见 《*Identity Manager 4.0.1 升级和迁移指南*》中的 “ 执行升级 ”。
- 如果您是将现有系统迁移到新硬件，请参见 《*Identity Manager 4.0.1 升级和迁移指南*》中的 “ 执行升级 ” 部分。
- 如果需要迁移基于角色的供应模块，请参见 《*Identity Manager Roles Based Provisioning Module 4.0 User Application：迁移指南*》。

6.4 配置 Identity Manager

安装好 Identity Manager 后，必须对各个组件进行配置才能拥有功能完全的解决方案。

- 第 6.4.1 节 “ 同步数据 ”（第 38 页）
- 第 6.4.2 节 “ 映射角色 ”（第 38 页）
- 第 6.4.3 节 “ 配置 User Application”（第 38 页）
- 第 6.4.4 节 “ 配置审计、报告和合规性 ”（第 39 页）

6.4.1 同步数据

Identity Manager 使用驱动程序同步不同应用程序、数据库、操作系统和目录之间的数据。安装 Identity Manager 后，您需要为每个要同步数据的系统创建和配置一个或多个驱动程序。

每个驱动程序都有一本文档指南，说明同步数据所需的要求及配置步骤。驱动程序指南位于 Identity Manager 4.0.1 驱动程序文档网站 (http://www.novell.com/documentation/idm401drivers/index.html) 上。

请按照特定于每个受管系统的驱动程序指南创建驱动程序以同步身份数据。

6.4.2 映射角色

了解不同系统之间的同步后，请使用角色映射管理器 (RMA) 管理不同系统中的角色。有关更多信息，请参见 《*Novell Identity Manager 角色映射管理器 4.0.1 用户指南*》。

6.4.3 配置 User Application

下一步是使用 User Application 向 Identity Manager 解决方案添加业务透视图。 User Application 使您能够解决以下业务需求：

- 为执行基于角色的供应操作提供便捷的方式。
- 确保贵组织具有验证相关人员是否完全理解组织策略并据此执行步骤的方法。
- 为用户提供自助服务、允许新用户自我注册以及提供匿名或 guest 用户访问权限。
- 确保对公司资源的访问符合组织策略，确保在公司安全性策略环境下进行供应。
- 减少输入、更新和删除公司各个系统中的用户信息的管理负担。
- 管理身份、服务、资源和资产的手动与自动化供应。
- 支持复杂的工作流程。

《*Identity Manager Roles Based Provisioning Module 4.0 User Application：管理指南*》中介绍了有关如何配置 User Application 的这些功能的信息。

6.4.4 配置审计、报告和合规性

创建 Identity Manager 解决方案的最后也是最重要的一步就是配置审计、报告和合规性功能，从而使您能验证解决方案是否符合您的业务策略。请按照以下指南设置和配置相应功能：

- **审计：**请参见《*Identity Manager 4.0.1 for Novell Sentinel 报告指南*》。
- **报告：**请参见《*身份报告模块指南*》和*使用 Identity Manager 4.0 报告*。
- **合规性：**请参见《*Identity Manager Roles Based Provisioning Module 4.0 User Application：用户指南*》中的“使用合规性选项卡”。

6.5 管理 Identity Manager

Identity Manager 解决方案创建完成后，有许多不同的指南可帮助您管理、维护 Identity Manager 解决方案，以及随着您业务的变化和增长而更改 Identity Manager 解决方案。各种管理指南都位于 Identity Manager 4.0.1 文档网站 (http://www.novell.com/documentation/idm401/index.html) 的“管理”标题下。