Novell Identity Manager

3.0

www.novell.com

管理指南

2006 年 4 月 28 日

Novell®

法律声明

Novell, Inc. 对本文档的内容或使用不做任何陈述或保证，特别是商用性或针对特定目的之适用性的任何明确或隐含的保证。此外， Novell, Inc. 保留随时全部或部分地修改此出版物和更改其内容的权利，并且无义务将这些修改通知任何人或任何实体。

此外， Novell, Inc. 对任何软件不做任何声明或保证，特别是对用于任何具体目的的适销性或适用性不做任何明示或暗示保证。此外， Novell, Inc. 保留随时修改 Novell 软件任何部分或全部内容的权利，并且没有义务就此类修订或修改通知任何个人或实体。

依据本协议提供的任何产品或技术信息都将受到美国出口控制和其他国家 / 地区的贸易法律的约束。您同意遵守所有的出口控制法规，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。您同意不向目前的美国出口排除列表上的实体，或者向美国出口法律中规定的任何被禁运的或支持恐怖主义的国家 / 地区进行出口或再出口。您已经同意不将可交付产品用于禁止的核、导弹或生物化学武器的终端使用。有关出口 Novell 软件的详细信息，请参考 www.novell.com/info/exports/。如果您未能获得任何必要的出口许可， Novell 对此不负任何责任。

版权所有 © 2005 Novell, Inc. 保留所有权利。未经出版商的明确书面许可，不得复制、影印、传送此出版物的任何部分或将其储存在检索系统上。

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

联机文档：要访问本产品和其它 Novell 产品的联机文档并获取产品的更新资料，请参见 www.novell.com/documentation。

Novell 商标

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

第三方材料

所有第三方商标是其各自拥有者的资产。

目录

关于本指南

Novell® Identity Manager 3 （其前身为 DirXML® ）是一项数据共享和同步的服务，用于实现应用程序、目录以及数据库之间的信息共享。它将分散的信息链接在一起，从而可以通过创建策略来管理指定系统在身份发生更改时的自动更新。Identity Manager 为帐户供应、安全性、用户自助服务、鉴定、授权、工作流程自动化和万维网服务提供了基础。通过它可以对所分发的身份信息进行集成、管理和控制，以便安全地将适当的资源递送给适当的人员。

本指南概述 Identity Manager 技术，并介绍它的管理和配置功能。

反馈

我们希望听到您对本手册和本产品中包含的其它文档的意见和建议。请使用联机文档中每页底部的 " 用户意见 " 功能，或访问 http://www.novell.com/documentation/feedback.html 并输入您的意见。

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)。

其它文档

有关 Identity Manager 安装和升级的文档，请参见 《*Identity Manager 3.0* 安装指南》。

有关 Identity Manager 策略和过滤器的文档，请参见 《策略构建器和驱动程序自定义指南》。

有关设计和部署做法的文档，请参见 《*Designer for Identity Manager 3*：管理指南》(http://www.novell.com/documentation/designer)。

有关口令策略、口令自助服务和口令管理的文档，请参见 《口令管理管理员指南》(http://www.novell.com/documentation)。

有关 Identity Manager 驱动程序使用方法的文档，请参见 Identity Manager 驱动程序文档万维网站点 (http://www.novell.com/documentation/idmdrivers/index.html)。

文档约定

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

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

Identity Manager 3.0 体系结构概述

1

Identity Manager 包含三个主要部件。

- “Identity Manager”在第 10 页
- “用户应用程序”在第 17 页
- “Designer”在第 17 页

1.1 与较早版本相比的术语变更

如果您未使用过 DirXML® 1.1a 或 Identity Manager 2.0，则可以跳过本节。

在 DirXML 1.1a 中，术语 " 规则 " 用于描述规则集、规则集中的各个规则或每个规则中的各种条件和操作，具体取决于环境。如果环境交待不清，这种重叠就会导致混乱。

在 Identity Manager 2 中，现在使用 " 策略 " 代替 " 规则 " 来描述所发生的高级转换。您现在要定义的是策略集，其中每项策略包含一个或多个规则。而术语 " 规则 " 现在仅用于描述单个条件和操作集。

下表说明了从 DirXML 1.1a 到 Identity Manager 2.x 的术语变更情况。

表 ***1-1*** 从 *DirXML 1.1a* 到 *Identity Manager 2.x* 的术语变更情况

说明对象	DirXML 1.1a 术语	Identity Manager 2.x 术语
转换集	规则	策略集
策略集中的单个转换	规则	“策略”
单个转换中的条件和操作	规则	规则

下表说明了从 Identity Manager 2.x 到 Identity Manager 3.0 的术语变更情况。

表 ***1-2*** 从 *Identity Manager 2.x* 到 *Identity Manager 3.0* 的术语变更情况

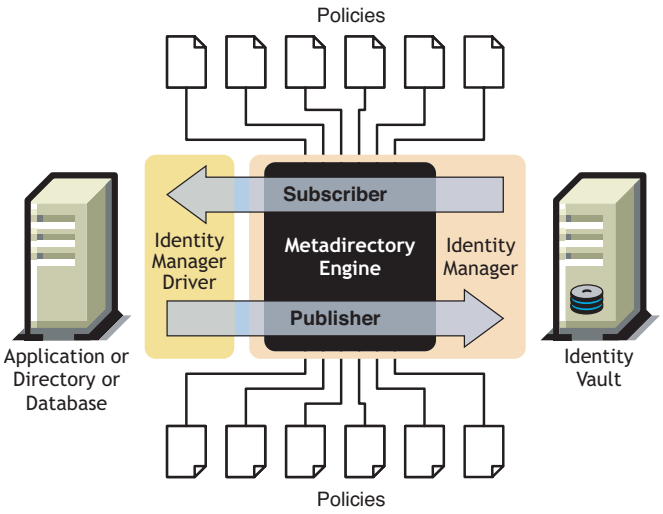
说明对象	Identity Manager 2.x 术语	Identity Manager 3 术语
产品	DirXML	Identity Manager
安装该产品的服务器	DirXML 服务器	Metadirectory 服务器
应用程序或数据库中正在同步数据的服务器	DirXML 已连接系统服务器	已连接系统服务器
对象的储存位置	eDirectory™	Identity Vault
处理部件	DirXML 引擎	Metadirectory 引擎

1.2 Identity Manager

Identity Manager 用于 Identity Vault 与已连接系统之间的数据同步。已连接系统包含应用程序、目录、数据库或文件。

Identity Manager 包括多个部件。下图说明了它的基本部件及基本部件间的关系：

图 ***1-1*** *Identity Manager* 部件



Metadirectory 引擎是 Identity Manager 体系结构中的关键模块。它提供的接口允许 Identity Manager 驱动程序与 Identity Vault 同步信息，即使完全不同的数据系统也可以连接并共享数据。

Metadirectory 引擎使用 XML 格式处理 Identity Vault 数据和 Identity Vault 事件。它利用一个规则处理器和一个数据转换引擎，对两个系统间流动的数据进行处理：

1. 读取所有 Identity Manager 驱动程序的过滤器。
2. 为相应的 Identity Vault 事件注册驱动程序。
3. 按照每个驱动程序的规格过滤数据。
4. 为传递到每个驱动程序的 Identity Vault 事件设置超速缓存。

Identity Vault 在进行初始化时执行以下步骤：

- 对事件进行超速缓存后，拥有该超速缓存的驱动程序将读取该事件。
- 驱动程序接收到 eDirectory 固有格式的 Identity Vault 数据，然后将其转化为 XDS 格式（Identity Manager 使用的 XML 词汇，可通过策略进行转换），并将该事件发送到 Metadirectory 引擎。Metadirectory 引擎读取已连接系统驱动程序中的所有策略，并根据这些策略创建 XML 格式的数据，然后将数据发送到连接系统驱动程序。该驱动程序再将数据发送到已连接系统。有关策略的更多信息，请参见 《策略构建器和驱动程序自定义指南》中的 “ 策略介绍 ”。
- 驱动程序的发布者部分收集已连接系统中的更新，并将其发送到 Identity Vault 中。当连接系统驱动程序得知两个系统的共享信息发生更改时，已连接系统驱动程序将收集改动信息，确保已将信息过滤为正确的数据集，并将数据转换为 XDS 格式，然后将数据发送到引擎。

1.2.1 Metadirectory 引擎

Metadirectory 引擎可以分为两个部件：eDirectory 接口和同步引擎。

eDirectory 接口

eDirectory 接口内置于 Metadirectory 引擎中，用于检测 eDirectory 中发生的事件。此接口通过使用事件超速缓存保证将事件递送至 Identity Manager。eDirectory 接口支持多驱动程序装载，这意味着虽然只为 eDirectory 服务器运行了一个 Identity Manager 实例，但它可以与多个已连接系统进行通讯。此接口中还内置有回送检测功能，可防止 Identity Vault 和已连接系统间发生事件循环。虽然此接口中已包含回送保护，但开发者还是应该在单个已连接系统驱动程序中构建回送检测。

同步引擎

同步引擎对引擎中出现的每个事件应用 Identity Manager 策略。这些策略是在策略构建器中使用 DirXML 底稿创建的。策略构建器允许通过 GUI 界面创建策略，而不必使用 XML 文档或以 XSLT 编写的样式页。虽然样式页仍可继续使用，但使用策略构建器将更加简单。有关策略构建器或 DirXML 底稿的更多信息，请参见 《策略构建器和驱动程序自定义指南》。

同步引擎可对源文档应用各种策略。能够完成这些转换是 Identity Manager 最强大的功能之一。Identity Vault 和已连接系统间的共享数据是实时进行转换的。

1.2.2 驱动程序配置文件

驱动程序配置是 Identity Manager 中附带的预配置 XML 文件，可以通过 iManager 和 Designer 中的向导进行导入。

这些驱动程序配置中包含样本策略。这些策略不适用于生产环境，而是作为模板供修改后使用的。

1.2.3 Identity Manager 事件超速缓存

所有通过 eDirectory 生成的事件在被成功处理完毕之前，均储存在事件超速缓存中。这样可保证数据不会因为连接错误、系统资源丢失、驱动程序不可用或任何其它网络故障而丢失。

1.2.4 驱动程序 Shim

驱动程序 Shim 充当已连接系统和 Identity Vault 之间的信息管道。Shim 可用 Java、C 或 C++ 进行编写。

Metadirectory 引擎和驱动程序 Shim 之间是以 XML 文档的形式进行通讯的，这些 XML 文档将提供对事件、查询和结果的描述。驱动程序 Shim 通常指代该驱动程序。它是 Identity Vault 和已连接系统之间传送信息的管道。

Shim 支持以下对象事件：

- 添加 （创建）
- 修改
- 删除
- 重命名

- 移动
- 查询

此外， Shim 还必须支持已定义的查询功能，以便 Identity Manager 可以对已连接系统进行查询。

当 Identity Vault 中发生的某一事件引起已连接系统中的一项操作时， Identity Manager 就会创建一个 XML 文档来描述该 Identity Vault 事件，并通过订购者通道将它提交到驱动程序 Shim。

当已连接系统中发生某一事件时，驱动程序 Shim 就会生成一个 XML 文档，来描述该已连接系统事件。然后驱动程序 Shim 通过发布者通道将生成的 XML 文档提交到 Identity Manager。Identity Manager 利用发布者策略对该事件进行处理，然后令 Identity Vault 执行相应的操作。

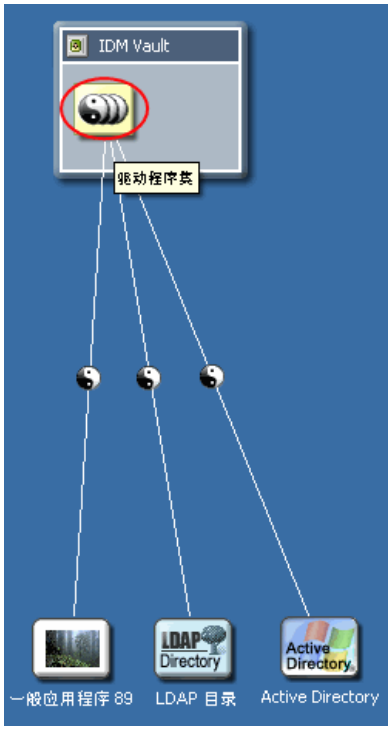
1.2.5 驱动程序集

驱动程序集是一个树枝对象，其中包含多个 Identity Manager 驱动程序。一个驱动程序集每次只能与一个服务器关联。因此，正在运行的所有驱动程序都必须分组为同一驱动程序集。

驱动程序集对象必须存在于使用它的任何服务器的完全读 / 写复本中，因此建议对驱动程序集进行分区。这样建议是为确保当用户的复本移动到其它服务器时，不会移动驱动程序对象。

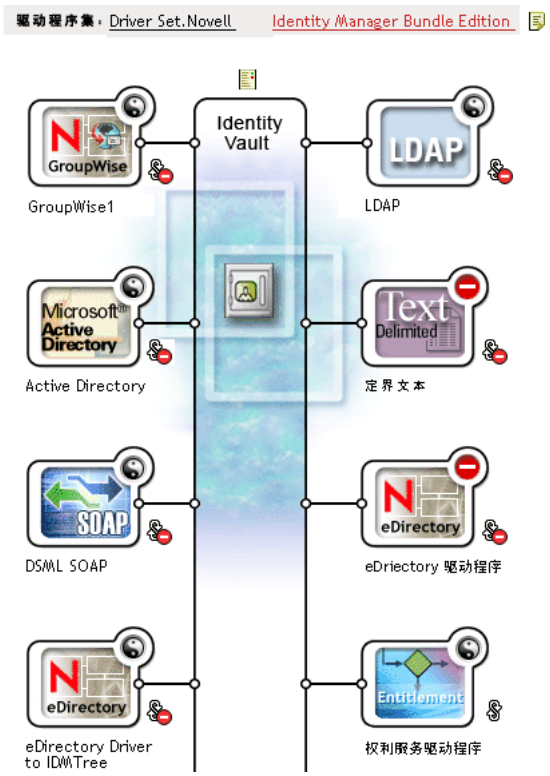
下图说明驱动程序集在 Designer 中是如何显示的。

图 ***1-2*** *Designer* 中的驱动程序集



下图说明驱动程序集在 iManager 中是如何显示的。

图 *1-3 iManager* 中的驱动程序集



在 Designer 的建模程序 （如上所示，图 1-2 在第 12 页）或 iManager 的概述页 （如上所示，图 1-3 在第 13 页）中，您可以：

- 查看和修改驱动程序集及其属性
- 查看驱动程序集中的驱动程序
- 更改驱动程序的状态
- 将驱动程序集与服务器关联
- 添加或去除驱动程序
- 查看驱动程序集的激活信息
- 查看驱动程序集的状态日志

1.2.6 驱动程序对象

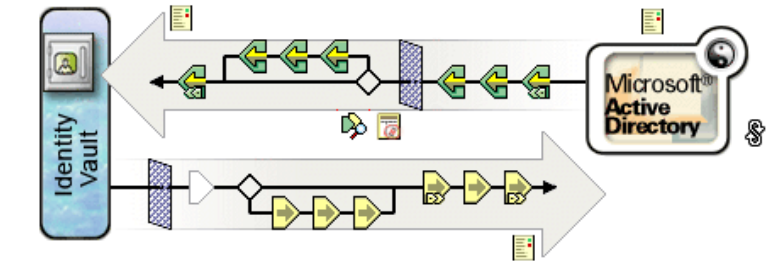
驱动程序对象表示连接到与 Identity Vault 相集成的已连接系统的驱动程序。驱动程序对象及其配置参数由以下部件组成：

- eDirectory 树中的一个驱动程序对象，包含在驱动程序集对象中。
- 一个订购者通道对象，包含在驱动程序对象中。
- 一个发布者对象，包含在驱动程序对象中。
- 若干策略对象，供驱动程序对象、订购者对象和发布者对象参照。
- 一个可执行驱动程序 Shim，供驱动程序对象参照。

- Shim 特定参数，由管理员配置。
- 驱动程序对象的 eDirectory 口令。Shim 可使用该口令鉴定 Shim 的远程部分。
- 鉴定参数，用于连接及鉴定已连接系统。
- 权利，但并不是每个驱动程序都包含权利。权利可在创建驱动程序时启用，也可在创建完毕后添加。
- 驱动程序的启动选项，包括以下三种状态：
  - 禁用：驱动程序不运行。
  - 手工：必须通过 iManager 手工启动驱动程序。
  - 自动启动：Identity Vault 启动时，驱动程序会自动启动。
- 对纲要映射策略的参照。
- 已连接系统的纲要的 XML 表示形式。这通常通过 Shim 从已连接系统中自动获得。

在 iManager 中，可以访问 Identity Manager 驱动程序概述，并修改现有驱动程序的参数、策略、样式表和权利。Identity Manager 驱动程序概述如下图所示。

图 ***1-4*** *Identity Manager* 驱动程序概述



此外，驱动程序对象还可用于检查 eDirectory 权限。无论驱动程序对象要读取或写入任何对象，都必须向该驱动程序授予足够的 eDirectory 权限。为此，可以将驱动程序对象设为与该驱动程序同步的 eDirectory 对象的受托者，或授予驱动程序对象安全性等效权限。

有关权限指派的更多信息，请参见 《*Novell eDirectory 8.8* 管理指南》中的 "eDirectory 权限 (http://www.novell.com/documentation/edir88/index.html?page=/documentation/edir88/edir88/data/fbachifb.html)"。

1.2.7 发布者通道和订购者通道

Identity Manager 驱动程序包含两个数据处理通道：发布者通道和订购者通道。发布者通道将事件从已连接系统发送到 Identity Vault 中。订购者通道将事件从 Identity Vault 发送到已连接系统中。每个通道都包含各自的策略，来定义如何处理和转换数据。

图 ***1-5*** *Designer* 中的发布者通道和订购者通道

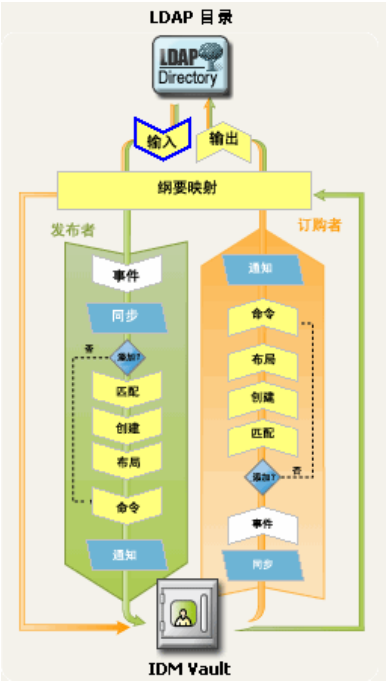
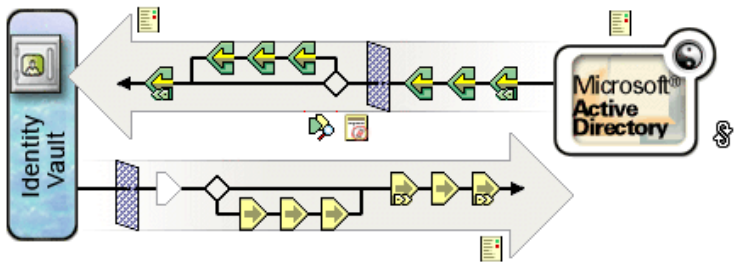


图 ***1-6*** *iManager* 中的发布者通道和订购者通道

驱动程序： Active Directory.DriverSet.South.Novell



1.2.8 事件和命令

在 Identity Manager 中，对事件和命令的区分非常重要。如果事件是发送给驱动程序的，该事件就是命令。如果事件是发送给 Identity Manager 的，该事件就是通知。当驱动程序向 Identity Manager 发送事件通知时，它是在告知 Identity Manager 已连接系统中发生了更改。随后， Metadirectory 引擎将根据可配置规则，确定必须向 Identity Vault 发送哪些命令 （如果有）。

当 Identity Manager 向驱动程序发送命令时， Identity Manager 已将一个 Identity Vault 事件视为输入，并在应用适当的策略后，确定已连接系统中此命令代表的更改是必要的。

1.2.9 策略和过滤器

使用策略和过滤器可以控制数据如何从一个系统流向另一个系统。正是通过策略中的规则，来定义如何转换起管理作用的 Identity Vault 类、特性和事件，以供在已连接系统中使用的（反之亦然）。有关策略和过滤器的详细信息，请参考 《策略构建器和驱动程序自定义指南》。

1.2.10 关联

大多数其它身份管理产品都要求在已连接系统中储存某种标识符，才能将对象从已连接系统映射到目录中。而使用 Identity Manager 则无需更改已连接系统。Identity Vault 中的每个对象都包含一个关联表，该表用已连接系统中的唯一标识符映射 Identity Vault 对象。该表采用逆序索引，这样在更新 Identity Vault 时，已连接系统就无需向驱动程序提供 Identity Vault 标识符 （例如判别名）。

当发生事件的对象尚未与 Identity Vault 中的另一对象关联时，就要在这两个对象之间创建关联。要创建关联，每个对象之间的最小可定义准则集必须匹配。例如，可以创建一项策略，声明四个特性中如果任意两个特性匹配度大于 90% （全名、电话号码、员工 ID 和电子邮件地址），则将关联对象。

匹配策略定义了确定两个对象是否相同的准则。如果未发现与已更改对象匹配的对象，可以创建一个新对象。为此，必须满足所有最低创建准则。这些准则由 " 创建 " 策略定义。最后，布局策略定义在命名层次中创建新对象的位置。

可以通过以下两种方式之一创建关联：

- 作为两个对象之间的匹配项
- 作为特定位置上新建的对象

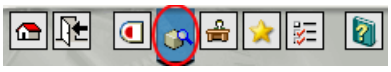
一旦对象之间形成关联，它一直保持有效，直到管理员删除对象或关联。

关联表

在 Identity Manager 中，关联指将 eDirectory 中的对象与驻留在已连接系统中的对象相匹配。最初安装 Identity Manager 时扩展了 eDirectory 纲要。此扩展包括向所有 eDirectory 对象的库类附加一个新特性。该特性就是关联表。关联表跟踪 eDirectory 对象链接的所有已连接系统对象。此表的构建和维护是自动进行的，因此，尽管经常查看此信息会很有帮助，但却没有必要手工编辑此信息。

可以在 iManager 中查看对象的关联特性。

1. 在 iManager 中，选择工具栏中的 " 查看对象 " 图标。



2. 浏览并选择对象，然后选择 " 修改对象 "。
3. 选择 "Identity Manager" 选项卡。

关联特性显示在 "Identity Manager" 选项卡中。

1.3 用户应用程序

用户应用程序是一种供应解决方案。它是 Identity Manager 3 的附加产品。用户应用程序将功能强大的批准工作流程集成到 Identity Manager 中。这样，在无需人工干预的自动规则之外，组织还可以利用人工输入来制订供应决策。有关信息，请参见用户应用程序文档 (http://www.novell.com/documentation/idm)。

1.4 Designer

Designer 是一个独立的客户端应用程序。它包括建模空间、调色板、视图、策略构建器、文档生成器和其它功能，可用于在生产效率较高的环境中对基于 Identity Manager 的解决方案进行设计、测试、记录和部署。有关 Designer 的信息，请参见 *《Designer for Identity Manager 3：管理指南》(http://www.novell.com/documentation/designer)*。

管理 Identity Manager 驱动程序 2

本节将介绍有助于创建和管理 Identity Manager 驱动程序的信息，包括以下主题：

2.1 创建和配置驱动程序

对于计划使用的每个 Identity Manager 驱动程序，都应创建一个驱动程序对象并导入一个驱动程序配置文件。驱动程序对象中包含该驱动程序的配置参数和策略。作为创建驱动程序对象过程的一部分，还需要导入特定于驱动程序的配置文件。驱动程序配置文件中包含默认的策略集。在实施数据共享模型时，这些策略可以帮您顺利开始工作。在大多数时候，需要使用附带的默认配置文件设置驱动程序，然后根据环境要求修改驱动程序配置文件。

可以使用两种方法创建驱动程序对象。

- 使用创建驱动程序任务可以创建单个驱动程序，并导入该驱动程序的配置文件。有关更多信息，请参考 “创建驱动程序对象”在第 19 页 。
- 使用导入驱动程序任务可以同时创建多个驱动程序，并导入它们的配置文件。有关更多信息，请参考 “创建多个驱动程序”在第 20 页 。

2.1.1 创建驱动程序对象

驱动程序配置 (XML) 文件创建并配置所需的对象，以确保驱动程序的正常工作。它还包括示例策略，可针对具体实施加以修改。

1. 在 iManager 中，选择 "Identity Manager 实用程序 ">" 新驱动程序 "。
2. 选择要在其中创建驱动程序的驱动程序集，然后单击 " 下一步 "。

   若要将此驱动程序放入新的驱动程序集中，则必须指定驱动程序集名称、环境和关联服务器。
3. 标记 *Import a Driver Configuration from the Server (.XML file)* （从服务器中导入驱动程序配置 （.XML 文件））并选择 .xml 文件，然后单击 " 下一步 "。

   在您设置 iManager 时，驱动程序配置文件便安装在万维网服务器上。

4 按照提示完成驱动程序配置导入。

这样便创建了所需的 Identity Manager 对象。如果在导入过程中未定义安全性等效或排除管理用户，则可以通过修改驱动程序对象的属性来完成这些任务。

注释 **:** 如果在导入过程中未启用权利，则不会创建权利策略。如果希望在将来使用权利，则必须在创建新驱动程序时启用权利。

2.1.2 创建多个驱动程序

Identity Manager 可提供一次创建多个驱动程序的功能。此过程与创建单个驱动程序相似，它仍需要使用驱动程序配置 (XML) 文件来创建并配置所需的对象，才能确保驱动程序正常工作。

同时导入多个驱动程序：

1 在 iManager 中，选择 "Identity Manager 实用程序 ">" 导入驱动程序 "。

2 选择要在其中新建驱动程序的驱动程序集，然后单击 " 下一步 "。

若要将这些驱动程序放入新的驱动程序集中，则必须指定驱动程序集名称、环境和关联服务器。

3 选择要添加至驱动程序集的应用程序配置，然后单击 " 下一步 "。

4 按照提示操作，并指定请求的数据，然后单击 " 下一步 "。

如果一次选择导入多个配置，将逐个显示应用程序的配置页。

这样便为每个驱动程序创建了所需的 Identity Manager 对象。如果在导入过程中未定义安全性等效或排除管理用户，则可以通过修改驱动程序对象的属性来完成这些任务。

2.2 在 Identity Manager 环境中管理 DirXML 1.1a 驱动程序

为 DirXML 1.1a 创建的现有驱动程序可继续用于 Identity Manager。

Identity Manager 3.0 附带的 Metadirectory 引擎向后兼容旧版驱动程序（前提是旧版驱动程序的 Shim 和配置已用最新的产品更新和增补程序更新）。由于引擎可向后兼容，因此可以根据需要在 Identity Manager 服务器上运行 DirXML 1.1a 驱动程序，无需对它们进行任何更改。

然而， iManager 插件仅具备有限的向后兼容性。可以在驱动程序集的概述中查看旧版驱动程序，但如果不转换驱动程序，则无法查看或编辑驱动程序配置。当您在驱动程序集概述中单击一个 DirXML 1.1a 驱动程序时， Identity Manager 插件将发现该驱动程序使用 DirXML 1.1a 格式，随即会提示使用向导将其转换为 3.0 格式。

如果尚不希望对现有驱动程序进行任何更改，可以取消此向导。

若要编辑采用 1.1a 格式的 1.1a 驱动程序，则必须使用 DirXML 1.1a 插件。为此，必须使用单独的 iManager 万维网服务器并在其上安装 1.1a 插件。如果不将驱动程序转换为 Identity Manager 3.0 格式，则无法使用 Identity Manager 附带的 Identity Manager 插件来编辑驱动程序配置。

2.3 将驱动程序配置从 DirXML 1.1a 格式升级至 Identity Manager 格式

受支持的 DirXML 1.1a 升级途经为安装 Identity Manager 3。 Identity Manager 3 安装操作将安装新的驱动程序 Shim，但不会更改现有的驱动程序对象或驱动程序配置。

为 DirXML 1.1a 创建的现有驱动程序配置可继续用于 Identity Manager。然而， Identity Manager 插件仅允许编辑 Identity Manager 格式的驱动程序。

重要 **:** 不支持对 DirXML 1.1a 引擎运行 Identity Manager 驱动程序 Shim 或驱动程序配置。

本软件中还提供一个向导，可帮助您将 DirXML 1.1a 驱动程序转换为 Identity Manager 格式。

启动该向导：

1. 在 iManager 中，单击 *Identity Manager* >"Identity Manager 概述 "。
2. 选择要转换的驱动程序所在的驱动程序集，然后单击 " 搜索 "。
3. 单击要转换的驱动程序的图标。

   系统将提示您将驱动程序转换为新格式。
4. 按照向导中的步骤完成转换操作。

2.4 启动、停止或重启动驱动程序

1. 在 iManager 中，单击 *Identity Manager* >"Identity Manager 概述 "。
2. 浏览至驱动程序所在的驱动程序集，然后单击 " 搜索 "。
3. 单击要更改其状态的驱动程序图标的右上角。如果驱动程序已停止，请单击 " 启动驱动程序 "；如果驱动程序正在运行，则请单击 " 停止驱动程序 "。

2.5 驱动程序参数

每个驱动程序的属性都带有驱动程序参数。参数中储存着驱动程序的特定信息，例如巡回检测间隔、鉴定方法、 SSL 使用情况或驱动程序心跳设置等。

2.6 使用全局配置值

全局配置值 (GCV) 是与驱动程序参数相似的设置。可以为驱动程序集和单个驱动程序指定全局配置值。如果某个驱动程序没有 GCV 值，则它将继承驱动程序集的 GCV 值。

通过 GCV，可以为 Identity Manager 功能 （例如口令同步和驱动程序心跳）指定设置，也可以为单个驱动程序配置特有的功能指定设置。某些 GCV 随驱动程序提供，但您也可以自行添加。可以参考策略中的这些值，以便于自定义驱动程序配置。

重要 **:** 口令同步设置属于 GCV，但最好不要在 GCV 页面中编辑，而应该在驱动程序的 " 服务器变量 " 页上使用提供的图形界面进行编辑。" 服务器变量 " 页以选项卡的形式显示 " 口令同步 " 设置，此设置可以像访问其它驱动程序参数一样进行访问，也可以通过以下方式访

问：单击 " 口令管理 ">" 口令同步 "，搜索驱动程序，然后单击驱动程序名称。该页包含每项口令同步设置的联机帮助。

添加、去除或编辑与 Identity Manager 口令同步不相关的 GCV：

1. 在 iManager 中，单击 *Identity Manager* >"Identity Manager 概述 "。
2. 浏览至驱动程序集或驱动程序对象，然后进行单击，接着再单击 " 搜索 "。
3. 单击驱动程序的右上角，然后单击 " 编辑属性 "。
4. 选择 " 全局配置值 "。
5. 更改驱动程序创建过程中设置的默认值。
6. 若要添加其它信息，请单击 " 编辑 XML"。
7. 单击 " 启用 XML 编辑 "。
8. 添加、去除或编辑 XML，然后单击 " 确定 " 以应用更改。

2.7 使用 DirXML 命令行实用程序

使用 DirXML 命令行实用程序可以访问 Identity Manager 特有的 eDirectory 动词。此实用程序不可替代 iManager 或 Designer。它主要用于编写底稿。有关 DirXML 命令行实用程序的详细信息，请参见附录 A “DirXML 命令行实用程序”在第 221 页 。在日常任务中，请使用 iManager 或 Designer。

2.8 查看版本信息

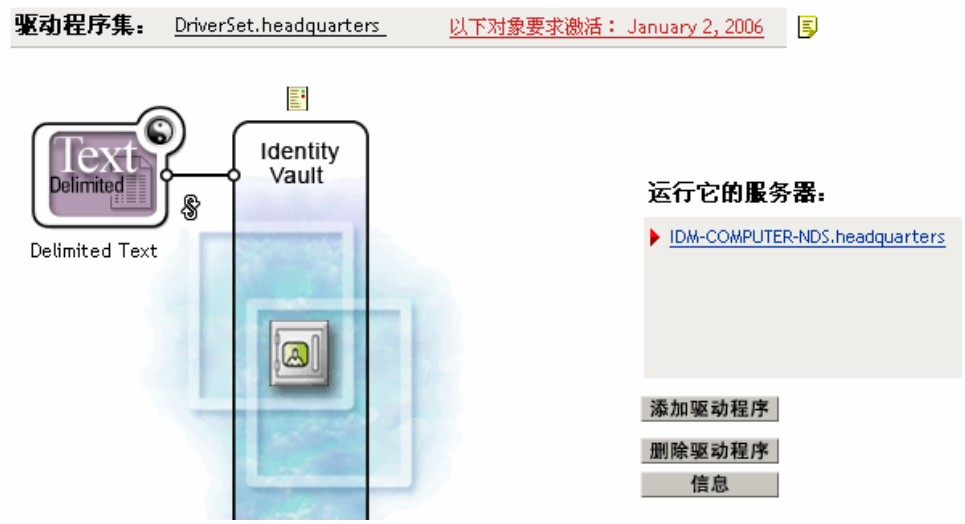
版本发现工具可用于：

- “查看版本信息的分级显示”在第 22 页
- “以文本文件的形式查看版本信息”在第 24 页
- “保存版本信息”在第 26 页

2.8.1 查看版本信息的分级显示

1. 在 iManager 中，单击 *Identity Manager* >"Identity Manager 概述 "，然后单击 " 搜索 " 以查找驱动程序集。

2 在 "Identity Manager 概述 " 屏幕中，单击 " 信息 "。



也可以选择 "Identity Manager 实用程序 ">" 版本发现 "，然后浏览并选择驱动程序集，接着再单击 " 确定 "。

3 查看顶级或未展开的版本信息显示

未展开的分级视图显示以下内容：

- 鉴定的目标 eDirector 树
- 所选的驱动程序集
- 与驱动程序集相关联的服务器

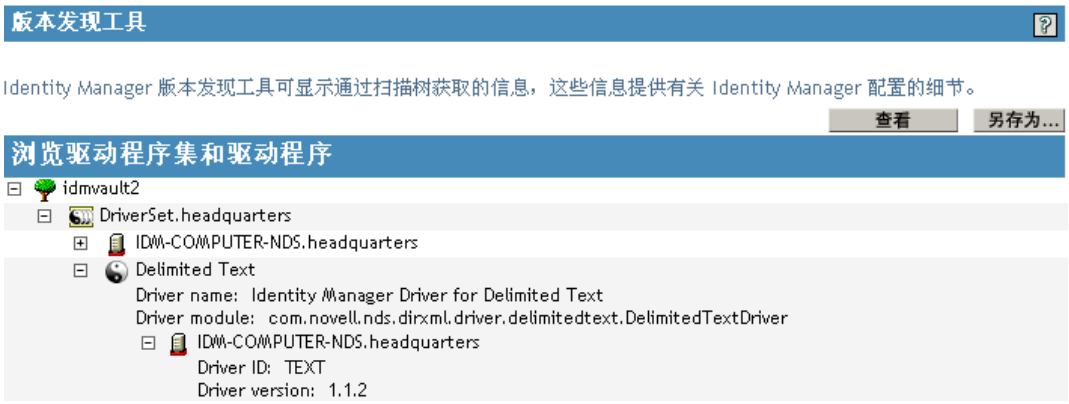
  如果驱动程序集与两台或更多的服务器相关联，则可以查看每台服务器上的 Identity Manager 信息。
- 驱动程序

4 通过展开服务器图标，查看与服务器相关的版本信息。

顶级服务器图标的展开视图显示以下内容：

- 上次日志时间
- 在此服务器上运行的 Identity Manager 的版本

5 通过展开驱动程序图标，查看与驱动程序相关的版本信息。



顶级驱动程序图标的展开视图显示以下内容：

- 驱动程序名称
- 驱动程序模块 （例如，com.novell.nds.dirxml.driver.delimitedtext.DelimitedTextDriver）

驱动程序图标下的服务器的展开视图显示以下内容：

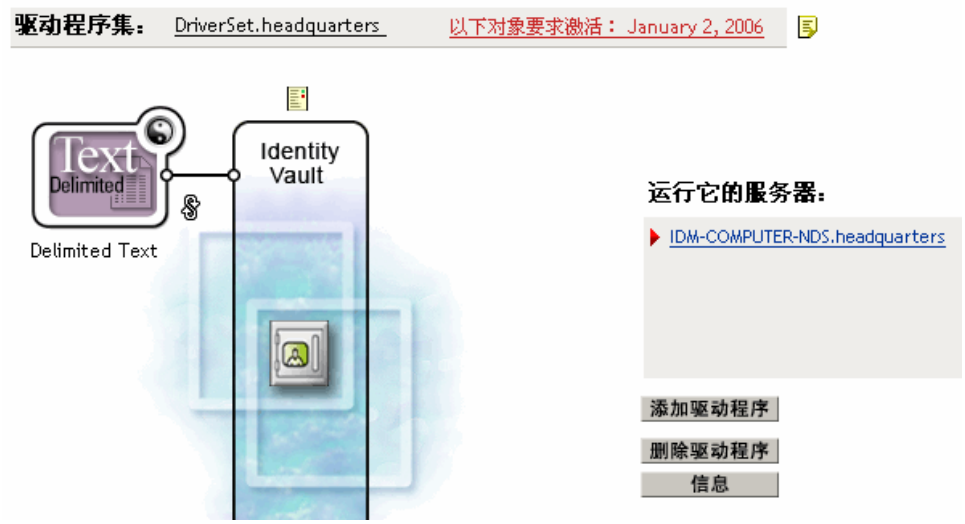
- 驱动程序 ID
- 在此服务器上运行的驱动程序实例的版本

2.8.2 以文本文件的形式查看版本信息

Identity Manager 将版本信息发布至文件。可以按文本格式查看此信息。文本表示与包含在分级视图中的信息是相同的。

1 在 iManager 中，单击 *Identity Manager* >"Identity Manager 概述 "，然后单击 " 搜索 " 以查找驱动程序集。

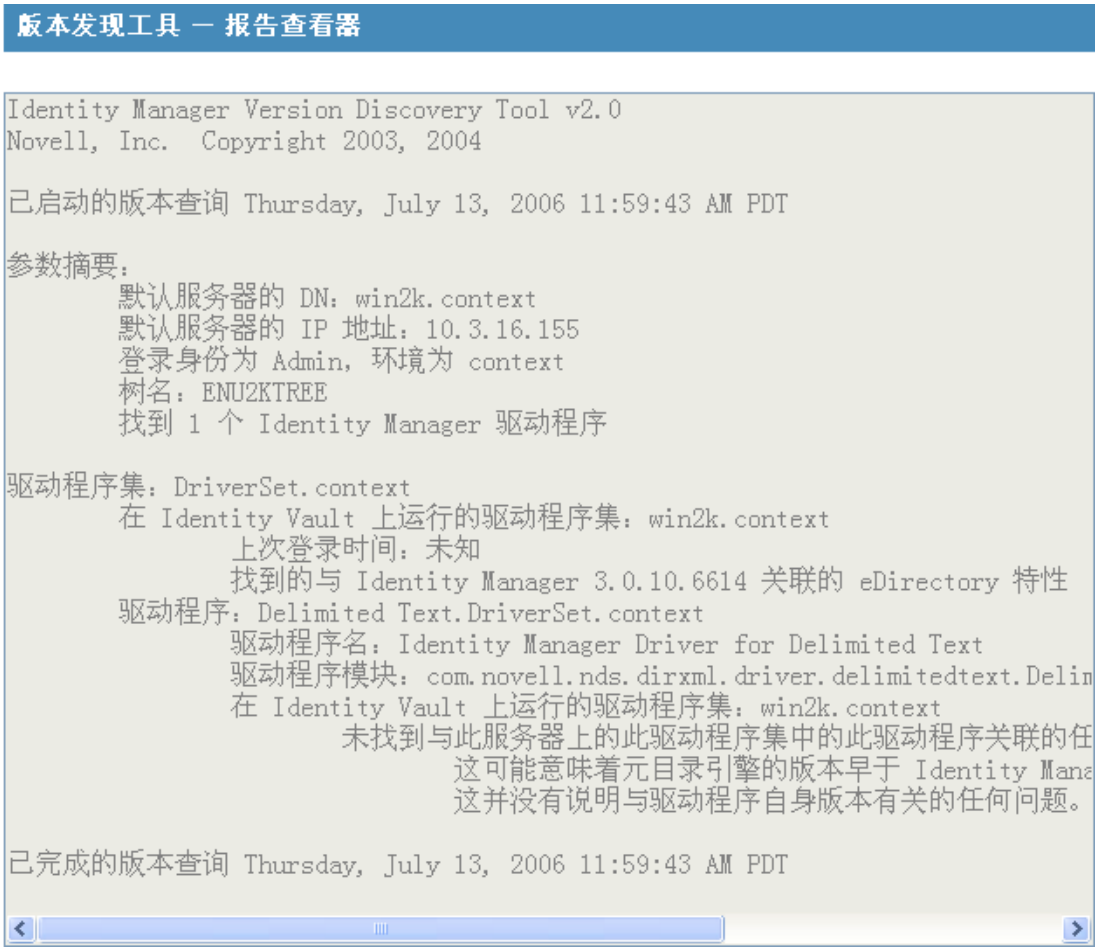
2 在 "Identity Manager 概述 " 屏幕中，单击 " 信息 "。



也可以选择 "Identity Manager 实用程序 ">" 版本发现 "，然后浏览并选择驱动程序集，接着再单击 " 信息 "。

3 在 " 版本发现工具 " 对话框中，单击 " 查看 "。

信息将以文本文件的形式显示在 " 报告查看器 " 窗口中。

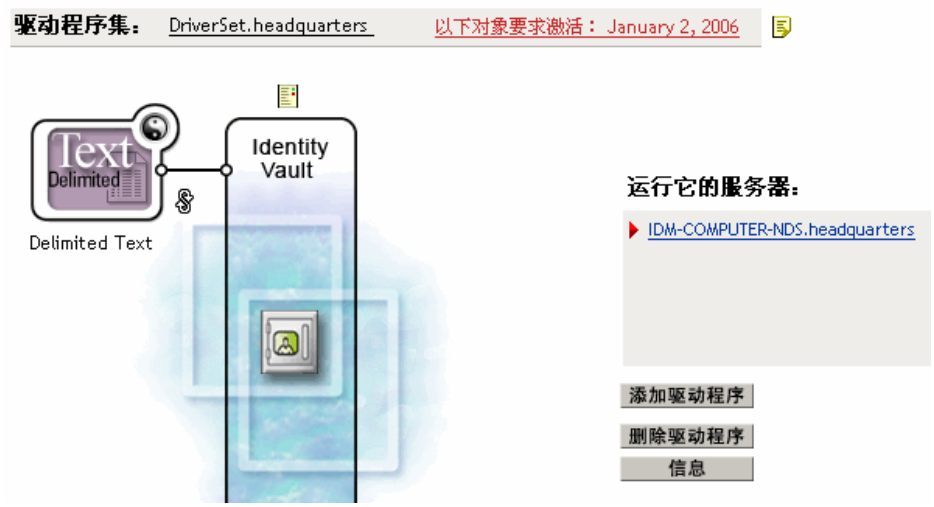


2.8.3 保存版本信息

可以将版本信息保存至本地或网络驱动器上的文本文件中。

1 在 iManager 中，单击 *Identity Manager* >"Identity Manager 概述 "，然后单击 " 搜索 " 以查找驱动程序集。

2 在 "Identity Manager 概述 " 屏幕中，单击 " 信息 "。



也可以选择 "Identity Manager 实用程序 ">" 版本发现 "，然后浏览并选择驱动程序集，接着再单击 " 信息 "。

3 在 " 版本发现工具 " 对话框中，单击 " 另存为 "。

4 在 " 文件下载 " 对话框中，单击 " 保存 "。

5 导航至所需的目录，键入文件名，然后单击 " 保存 "。

Identity Manager 会将数据保存至文本文件中。

2.9 使用命名口令

通过 Identity Manager 可以安全地储存某一特定驱动程序的多个口令。此功能便称为命名口令。每个不同的口令均通过密钥或名称来访问。

还可以使用命名口令功能安全地储存其它信息，例如用户名。

若要在驱动程序策略中使用命名口令，应使用其名称来参照该口令，而不要使用实际口令，Metadirectory 引擎会将此口令发送至驱动程序。本节描述了储存和检索命名口令的方法，此方法可用于任何驱动程序，无需对驱动程序 Shim 进行更改。

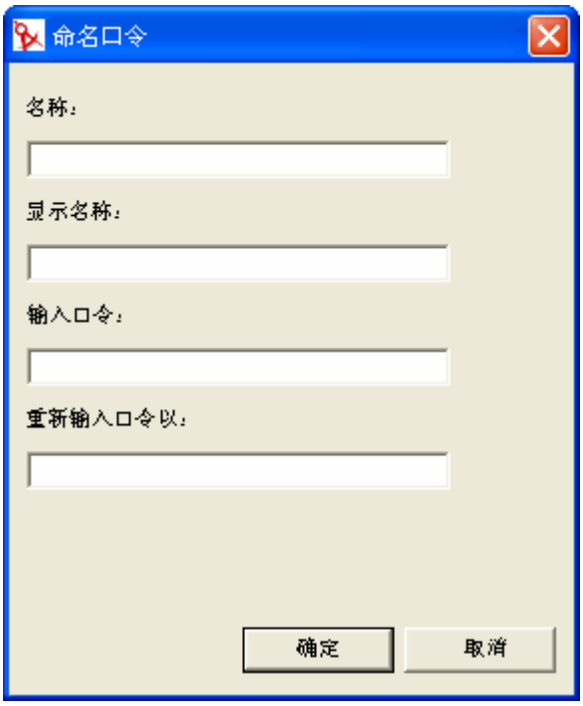
注释：为 Identity Manager Driver for Lotus Notes 提供的样本配置包括了以此方法使用命名口令的示例。Notes 驱动程序 Shim 还经过自定义，支持命名口令的其它用法。此外还包括了这些方法的示例。有关更多信息，请参见 《*Identity Manager Driver for Lotus Notes*：实施指南》中有关命名口令的章节。

本节包括：

- “使用 Designer 配置命名口令”在第 28 页
- “使用 iManager 配置命名口令”在第 28 页
- “在驱动程序策略中使用命名口令”在第 30 页
- “使用 DirXML 命令行实用程序配置命名口令”在第 31 页

2.9.1 使用 Designer 配置命名口令

1. 选择驱动程序对象，然后右击并选择 " 属性 "。
2. 选择 " 命名口令 "，然后单击 " 新建 "。



3. 指定命名口令的 " 名称 "。
4. 指定命名口令的 " 显示名称 "。
5. 指定命名口令，然后重新输入该口令。
6. 单击 " 确定 " 两次。

2.9.2 使用 iManager 配置命名口令

1. 在 iManager 中，单击 *Identity Manager* >"Identity Manager 概述 "。

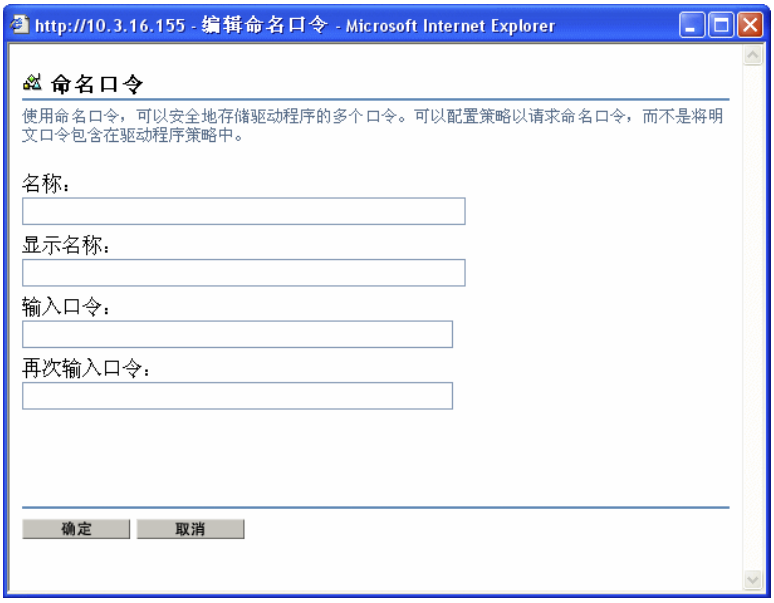
2 搜索驱动程序集，或浏览并选择包含驱动程序集的树枝。将出现驱动程序集的图形表示。

3 在 "Identity Manager 概述 " 屏幕中，单击驱动程序图标的右上角，然后单击 " 编辑属性 "。

4 在 "Identity Manager" 选项卡的 " 修改对象 " 页上，单击 " 命名口令 "。

将显示 " 命名口令 " 页，其中列出了该驱动程序的当前命名口令。如果尚未设置任何命名口令，则此列表为空。

5 若要添加命名口令，请单击 " 添加 "，在填写完各个字段后，单击 " 确定 "。



6 指定名称、显示名称和口令，然后单击 " 确定 " 两次。

请记住，可以使用此功能安全地储存其它类型的信息，例如用户名。

7 将显示一条讯息："Do you want to restart the driver to put your changes in effect?"（您要重启动此驱动程序以使更改生效吗？ （" 确定 "= 是， " 取消 "= 否））单击 " 确定 "。

8 若要去除命名口令，请单击 " 去除 "。将去除口令，而不会提示您确认此操作。

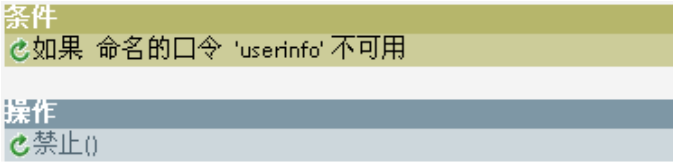
2.9.3 在驱动程序策略中使用命名口令

- “使用策略构建器”在第 30 页
- “使用 XSLT”在第 30 页

使用策略构建器

策略构建器允许调用命名口令。新建一条规则并选择命名口令作为条件。设置的操作取决于命名口令是否可用。下面的示例说明，当命名口令用户信息不可用时，事件将被禁止。

图 *2-1* 使用命名口令的策略



使用 XSLT

下面的示例说明如何在 XSLT 的订购者通道的驱动程序策略中参照命名口令：

```
<xsl:value-of
select=”query:getNamedPassword($srcQueryProcessor,'mynamedpassword')”
```

```
xmlns:query="http://www.novell.com/java/
com.novell.nds.dirxml.driver.XdsQueryProcessor/>
```

2.9.4 使用 DirXML 命令行实用程序配置命名口令

- “在 DirXML 命令行实用程序中创建命名口令”在第 31 页
- “在 DirXML 命令行实用程序中去除命名口令”在第 32 页

在 **DirXML** 命令行实用程序中创建命名口令

1. 运行 DirXML 命令行实用程序。

   有关信息，请参见附录 A “DirXML 命令行实用程序”在第 221 页。
2. 输入用户名和口令。

   将出现下面的选项列表。

   ```
   DirXML commands


   1: Start driver 2: Stop driver 3: Driver operations... 4: Driver
   set operations... 5: Log events operations... 6: Get DirXML
   version99: Quit


   Enter choice:
   ```
3. 输入 3 选择驱动程序操作。

   将出现带编号的驱动程序列表。
4. 输入要添加命名口令的驱动程序的编号。

   将出现下面的选项列表。

   ```
   Select a driver operation for:driver_name


   1: Start driver 2: Stop driver 3: Get driver state 4: Get driver
   start option 5: Set driver start option 6: Resync driver 7: Migrate
   from application into DirXML 8: Submit XDS command document to
   driver 9: Check object password 10: Initialize new driver object
   11: Passwords operations 12: Cache operations99: Exit


   Enter choice:
   ```
5. 输入 11 选择口令操作。

   将出现下面的选项列表。

```
Select a password operation


1: Set shim password 2: Reset shim password 3: Set named password
4: Clear named password(s) 5: List named passwords99: Exit


Enter choice:
```

6 输入 3 设置新的命名口令。

将显示以下提示：

```
Enter password name:
```

7 输入要用来参照命名口令的名称。

8 出现以下提示时，输入要保护的实际口令：

```
Enter password:
```

键入的口令字符将不会显示出来。

9 出现以下提示时，再次输入口令进行确认：

```
Confirm password:
```

10 输入并确认口令后，将返回口令操作菜单。

完成此过程后，使用 99 选项两次，即可退出此菜单并退出 DirXML 命令行实用程序。

在 DirXML 命令行实用程序中去除命名口令

此选项在不再需要先前创建的命名口令时有用。

1 运行 DirXML 命令行实用程序。

有关信息，请参见附录 A “DirXML 命令行实用程序”在第 221 页。

2 输入用户名和口令。

将出现下面的选项列表。

```
DirXML commands


1: Start driver 2: Stop driver 3: Driver operations... 4: Driver
set operations... 5: Log events operations... 6: Get DirXML
version99: Quit


Enter choice:
```

3 输入 3 选择驱动程序操作。

将出现带编号的驱动程序列表。

4 输入要去除命名口令的驱动程序的编号。

将出现下面的选项列表。

```
Select a driver operation for:driver_name


1: Start driver 2: Stop driver 3: Get driver state 4: Get driver
start option 5: Set driver start option 6: Resync driver 7: Migrate
from application into DirXML 8: Submit XDS command document to
driver 9: Check object password 10: Initialize new driver object
11: Passwords operations 12: Cache operations99: Exit


Enter choice:
```

5 输入 11 选择口令操作。

将出现下面的选项列表。

```
Select a password operation


1: Set shim password 2: Reset shim password 3: Set named password
4: Clear named password(s) 5: List named passwords99: Exit


Enter choice:
```

6 （可选）输入 5 查看现有命名口令的列表。

即显示现有命名口令的列表。

此步骤有助于确保去除的是要去除的口令。

7 输入 4 去除一个或多个命名口令。

8 出现以下提示时，输入 No 去除单个命名口令：

```
Do you want to clear all named passwords? (yes/no):
```

9 出现以下提示时，输入要去除的命名口令的名称：

```
Enter password name:
```

输入要去除的命名口令的名称后，将返回口令操作菜单：

```
Select a password operation


 1: Set shim password 2: Reset shim password 3: Set named password
```

```
4: Clear named password(s) 5: List named passwords 99:Exit


Enter choice:
```

10 （可选）输入 5 查看现有命名口令的列表。

即显示现有命名口令的列表。

此步骤允许您验证去除的是要去除的口令。

完成此过程后，使用 99 选项两次，即可退出此菜单并退出 DirXML 命令行实用程序。

2.10 重新将驱动程序对象与服务器相关联

驱动程序对象需要与服务器相关联。

出现以下情况之一，则说明此关联因某种原因而失效：

- 在 Identity Manager 服务器上升级 eDirectory 时，收到 "UniqueSPIException error -783" 错误。
- 在 "Identity Manager 概述 " 屏幕中，驱动程序旁边未列出任何服务器。
- 在 "Identity Manager 概述 " 屏幕中，驱动程序旁边列出了一个服务器，但其名称为乱码。

若要解决此问题，必须取消驱动程序对象和服务器之间的关联，然后将二者重新关联。

登录到 iManager 中并转至 "Identity Manager 概述 " 屏幕中的驱动程序对象。在驱动程序图标旁边的服务器名称列表中，使用适当的图标先去除然后再添加某一服务器。通过这一操作，可将服务器与驱动程序对象重新关联。

2.11 添加驱动程序心跳

驱动程序心跳是 Identity Manager 2 和更高版本中附带的一项 Identity Manager 驱动程序功能（可选）。可使用指定了时间间隔的驱动程序参数对驱动程序心跳进行配置。如果心跳参数存在并具有非 0 的间隔值，且发布者通道在指定的时间间隔内没有通讯时，驱动程序将向 Metadirectory 引擎发送检测信号文档。

驱动程序心跳旨在提供一个触发器，当驱动程序未按照预期的操作频率在发布者通道中通讯时，就以规则的间隔启动一项操作。如果要利用此心跳，必须自定义驱动程序配置或其它工具。否则， Metadirectory 引擎将只接受心跳文档，但不会因此执行任何操作。

对于大多数驱动程序，样本配置中并未使用驱动程序的心跳参数，但您可以添加该参数。

不随 Identity Manager 提供的自定义驱动程序同样可以提供心跳文档，前提是驱动程序开发者编写的驱动程序支持此功能。

若要配置心跳，请执行以下操作：

1 在 iManager 中，单击 *Identity Manager* >"Identity Manager 概述 "。

2 浏览并选择所需的驱动程序集，然后单击 " 搜索 "。

3 在 "Identity Manager 概述 " 屏幕中，单击驱动程序图标的右上角，然后单击 " 编辑属性 "。

4 在 "Identity Manager" 选项卡上，单击 " 驱动程序配置 "，向下滚动至 " 驱动程序参数 "，然后寻找 "Heart Beat" 或相似的显示名称。

   如果驱动程序参数中已存在心跳，则可以更改间隔并保存更改，即可完成配置。

   间隔的值不能小于 1。如果值为 0，则表示此功能已关闭。

   时间单位通常是分钟；但是，部分驱动程序可能会选择不同的时间单位，例如使用秒钟。

5 如果不存在与心跳对应的驱动程序参数，则单击 " 编辑 XML"。

6 如下例所示，添加驱动程序参数项，作为 <publisher-options> 的子。（对于 AD 驱动程序，添加为 <driver-options> 的子）。

```
<pub-heartbeat-interval display-name="Heart Beat">10</pub-
heartbeat-interval>
```

提示 : 如果重启动后驱动程序未生成心跳文档，请检查驱动程序参数在 XML 中的布局。

---

7 保存更改，确保驱动程序已停止并重启动。

添加驱动程序参数后，可以使用图形视图编辑时间间隔。另一个选项是创建对时间间隔的全局配置值 (GCV) 的参照。如同其它全局配置值一样，驱动程序心跳可以设置在驱动程序集级别上，而不设置在各单独的驱动程序对象上。如果驱动程序不具有特定的全局配置值，而驱动程序集具有此值，则驱动程序将从驱动程序集继承此值。

下面是 Notes 驱动程序发出的心跳状态文档的示例：

```
<nds dtdversion="2.0" ndsversion="8.x"> <source> <product
build="20031112_1037" instance="blackcap" version="2.0">DirXML Driver
for Lotus Notes</product> <contact>Novell, Inc.</contact> </source>
<input> <status level="success" type="heartbeat"/> </input> </nds>
```

2.12 查看 Identity Manager 进程

若要查看 Identity Manage 处理事件，请使用 DSTRACE。此工具仅用于对 Identity Manager 进行测试和查错。在生成驱动程序的同时运行 DSTRACE，会增加 Identity Manager 服务器的利用率，并导致事件处理非常缓慢。

为了在 DSTRACE 中查看 Identity Manager 进程，将向驱动程序集和驱动程序对象添加值。可以在 Designer 和 iManager 中进行此操作。

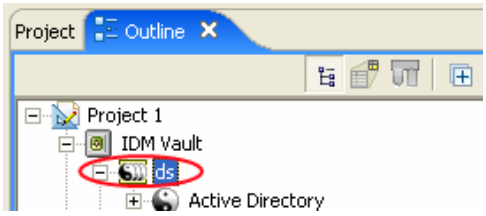
- “在 Designer 中添加跟踪级别”在第 35 页
- “在 iManager 中添加跟踪级别”在第 37 页
- “将 Identity Manager 进程截获至文件”在第 38 页

2.12.1 在 Designer 中添加跟踪级别

可以向驱动程序集对象或向各个驱动程序对象添加跟踪级别。

驱动程序集

1 在 Designer 打开的项目中，在 " 大纲 " 视图下选择驱动程序集对象。



2 右键单击并选择 " 属性 "，然后单击 "5. 跟踪 "。

3 设置跟踪参数，然后单击 " 确定 "。有关驱动程序集跟踪参数的更多信息，请参见表 2-1 在第 36 页。

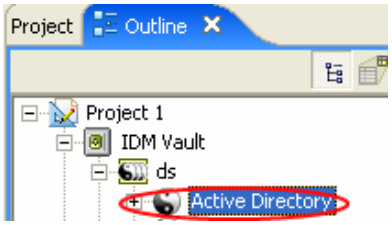
如果对驱动程序集对象设置跟踪级别， DSTRACE 日志中将出现所有驱动程序。

表 ***2-1*** 驱动程序集跟踪参数

参数	说明
Driver trace level （驱动程序跟踪级别）	随着驱动程序对象跟踪级别的提高， DSTRACE 中显示的信息量也会增加。 跟踪级别 1 只显示错误，但不显示导致错误的原因。如果希望查看口令同步信息，请将跟踪级别设置为 5。
XSL trace level （XSL 跟踪级别）	DSTRACE 会显示 XSL 事件。仅在对 XSL 样式表进行查错时设置此跟踪级别。如果不希望看到 XSL 信息，请将级别设置为 0。
Java debug port （Java 调试端口）	允许开发者挂接 Java 调试程序。
Java trace file （Java 跟踪文件）	在此字段中设置值后，驱动程序集对象的所有 Java 信息都会写入一个文件中。此字段的值是该文件的增补程序。 只要指定了文件， Java 信息就将写入此文件中。如果不需要调试 Java，请将此字段留为空。
Trace file size limit （跟踪文件大小限制）	允许设置 Java 跟踪文件大小限制。如果将文件大小设置为无限制，则此文件可以大到占据所有磁盘剩余空间。

驱动程序

1 在 Designer 打开的项目中，在 " 大纲 " 视图下选择驱动程序对象。



2 右键单击并选择 " 属性 "，然后单击 "8. 跟踪 "。

3 设置跟踪参数，然后单击 " 确定 "。有关这些参数的更多信息，请参见表 2-2 在第 37 页。

如果仅对驱动程序对象设置参数， DSTRACE 日志中将仅出现该驱动程序的信息。

表 **2-2** 驱动程序跟踪参数

参数	说明
Trace level （跟踪级别）	随着驱动程序对象跟踪级别的提高， DSTRACE 中显示的信息量也会增加。 跟踪级别 1 只显示错误，但不显示导致错误的原因。如果希望查看口令同步信息，请将跟踪级别设置为 5。 如果选择 *Use setting from Driver Set* （使用驱动程序集的设置），将采用驱动程序集对象的值。
Trace file （跟踪文件）	指定文件名和所选驱动程序的 Identity Manager 信息的写入位置。 如果选择 " 使用驱动程序集的设置 "，将采用驱动程序集对象的值。
Trace file size limit （跟踪文件大小限制）	允许设置 Java 跟踪文件大小限制。如果将文件大小设置为无限制，则此文件可以大到占据所有磁盘剩余空间。 如果选择 " 使用驱动程序集的设置 "，将采用驱动程序集对象的值。
Trace name （跟踪名称）	追加在驱动程序跟踪讯息前的为所输入的值，而不是驱动程序名称。用于驱动程序名称过长的情况。

2.12.2 在 iManager 中添加跟踪级别

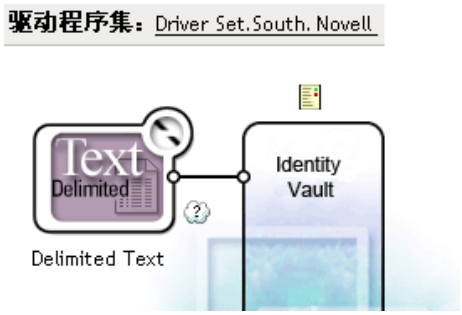
可以向驱动程序集对象或向各个驱动程序对象添加跟踪级别。

驱动程序集

1 在 iManager 中，选择 *Identity Manager* >"Identity Manager 概述 "。

2 浏览到驱动程序集对象，然后单击 " 搜索 "。

3 单击驱动程序集名称。



4 选择驱动程序集对象的 " 杂项 " 选项卡。

5 设置跟踪参数，然后单击 " 确定 "。有关这些参数的更多信息，请参见表 2-1 在第 36 页。

驱动程序

1 在 iManager 中，选择 *Identity Manager* >"Identity Manager 概述 "。

2 浏览到驱动程序对象所在的驱动程序集对象，然后单击 " 搜索 "。

3 单击驱动程序对象的右上角，然后单击 " 编辑属性 "。

4 选择驱动程序集对象的 " 杂项 " 选项卡。

5 设置跟踪参数，然后单击 " 确定 "。有关更多信息，请参见表 2-2 在第 37 页。

注释：iManager 中不存在 " 使用驱动程序集的设置 " 选项。

2.12.3 将 Identity Manager 进程截获至文件

若要将 Identity Manager 进程保存到文件，请通过驱动程序对象的参数或通过 DSTRACE 保存。驱动程序对象的参数是跟踪文件参数。

下列方式有助于在不同的操作系统平台上通过 DSTRACE 截获并保存 Identity Manager 进程。

NetWare

使用 DSTRACE.NLM 在系统控制台上显示跟踪讯息或将跟踪讯息保存到文件中 (SYS:\SYSTEM\DSTRACE.LOG)。DSTRACE.NLM 会将跟踪讯息显示在标为 "DSTRACE Console" （DSTRACE 控制台）的屏幕中。

1 在服务器控制台中键入 DSTRACE.NLM。

此操作将 DSTRACE.NLM 装载到内存中。

2 在服务器控制台中键入 DSTRACE SCREEN ON。

使跟踪讯息显示在 "DSTRACE 控制台 " 屏幕上。

3 在服务器控制台中键入 DSTRACE FILE ON。

将发送至 DSTRACE 控制台的讯息截获到 DSTRACE.LOG 中。

4 在服务器控制台中键入 DSTRACE -ALL。

关闭所有跟踪标志。

5 在服务器控制台中键入 DSTRACE +DXML DSTRACE +DVRS。

显示 Identity Manager 事件。

6 在服务器控制台中键入 DSTRACE +TAGS DSTRACE +TIME

显示讯息标签和时戳。

7 转换至 "DSTRACE 控制台 " 屏幕并监视经过的事件。

8 转换回服务器控制台。

9 在服务器控制台中键入 DSTRACE FILE OFF。

停止将跟踪讯息截获到日志文件中。同时还会停止向此文件中记录信息。

10 在文本编辑器中打开 DSTRACE.LOG，然后搜索已修改的事件或对象。

Windows

1 打开 " 控制面板 ">"NDS 服务 ">"dstrace.dlm"，然后单击 " 开始 "。

将打开名为 "NDS 服务器跟踪实用程序 " 的窗口。

2 选择 " 编辑 ">" 选项 "，然后单击 " 全部清除 "。

此操作将清除所有默认标志。

3 选择 "DirXML" 和 "DirXML 驱动程序 "。

4 单击 " 确定 "。

5 选择 " 文件 ">" 新建 "。

6 指定文件名和 DSTRACE 信息的保存位置，然后单击 " 打开 "。

7 等待事件发生。

8 选择 " 文件 ">" 关闭 "。

此操作将停止向日志文件写入信息。

9 在文本编辑器中打开文件，并搜索已修改的事件或对象。

UNIX

1 键入 ndstrace 启动 ndstrace 实用程序。

2 键入 set ndstrace=nodebug

关闭当前设置的所有跟踪标志。

3 键入 set ndstrace on

在控制台上显示跟踪讯息。

4 键入 set ndstrace file on

将跟踪讯息截获至文件 ndstrace.log，该文件位于 eDirectory 的安装目录中。默认目录为 /var/nds。

5 键入 set ndstrace=+dxml

显示 Identity Manager 事件。

6 键入 set ndstrace=+dvrs

显示 Identity Manager 驱动程序事件。

7 等待事件发生。

8 键入 set ndstrace file off

此操作将停止向此文件中记录信息。

9 键入 exit，退出 ndstrace 实用程序。

10 在文本编辑器中打开文件。搜索已修改的事件或对象。

iMonitor

使用 iMonitor 可以从万维网浏览器获取 DSTRACE 信息。它与 Identity Manager 的运行位置无关。运行 iMonitor 的文件有：

- NDSIMON.NLM，运行在 NetWare 中。
- NDSIMON.DLM，运行在 Windows 中。
- ndsimonitor，运行在 UNIX 中。

1 从 http:// 服务器 *IP* 地址 :8008/nds 访问 iMonitor。

默认端口为 8008 端口。

2 输入具有管理权限的用户名和口令，然后单击 " 登录 "。

3 从左侧选择 " 跟踪配置 "。

4 单击 " 全部清除 "。

5 选择 "DirXML" 和 "DirXML 驱动程序 "。

6 单击 " 跟踪启动 "。

7 选择左侧的 " 跟踪历史 "。

8 单击 " 修改时间 " 设为 " 当前 " 的文档，以查看在线跟踪情况。

9 若要更频繁地查看信息，请更改 " 刷新间隔 "。

10 选择左侧的 " 跟踪配置 "，然后单击 " 跟踪关闭 "，以关闭跟踪。

11 选择 " 跟踪历史 " 后，即可查看跟踪历史。可根据时戳来判别这些文件。

如果需要 HTML 文件的拷贝，默认位置为：

- NetWare：SYS:\SYSTEM\ndsimon\DSTRACE*.htm
- Windows：驱动器 _ 字母 :\Novell\NDS\ndsimon\dstrace*.htm
- UNIX：/var/nds/dstrace/*.htm

设置已连接系统

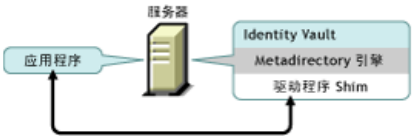
3

本节提供了以下信息：

3.1 概述

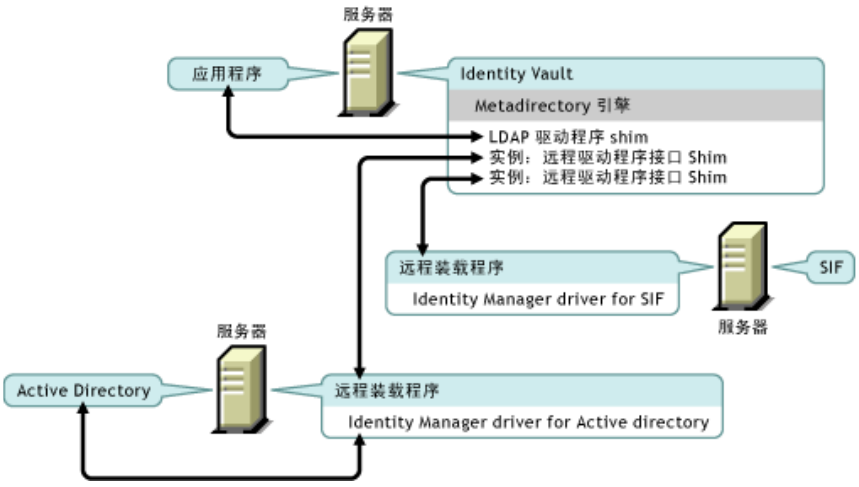
如下图所示， Metadirectory 引擎作为 eDirectory 的一部分在服务器上运行。Identity Manager 驱动程序 Shim 及其已配置的驱动程序与应用程序和 Metadirectory 引擎进行通讯。

图 **3-1** 运行在 *eDirectory* 下的 *Metadirectory* 引擎



如下图所示，已连接系统在多个应用程序间扩展 Identity Manager 功能：

图 **3-2** 包括远程装载程序的已连接系统



已连接系统需要远程装载程序。此服务使 Metadirectory 引擎可以与作为不同进程运行在不同位置的 Identity Manager 驱动程序交换数据，这些驱动程序包括：

- 在 Metadirectory 引擎运行的服务器上作为单独的进程

  Metadirectory 引擎作为 eDirectory 进程的一部分运行。Identity Manager 驱动程序可以在 Metadirectory 引擎运行的服务器上运行。事实上，像 Metadirectory 引擎一样，它们可以作为同一进程的一部分来运行。

但是，出于战略性原因，可能希望 Identity Manager 驱动程序在服务器上作为单独的进程运行。尽管如此， Identity Manager 驱动程序通常运行在单独的服务器上。

如果驱动程序作为单个进程运行，远程装载程序会提供 Metadirectory 引擎和驱动程序之间的通讯通道。

- 在 Metadirectory 引擎未运行的服务器上

  在 Metadirectory 引擎运行的服务器上，部分 Identity Manager 驱动程序无法运行。使用远程装载程序可以使 Metadirectory 引擎运行的环境与运行 Identity Manager 驱动程序的服务器所在的环境不同。例如， Active Directory 驱动程序无法在 NetWare 服务器上运行。Metadirectory 引擎可以在 NetWare 服务器上运行，而远程装载程序在 Active Directory 服务器上运行。

  方案：单独的服务器。Metadirectory 引擎在 NetWare 服务器中运行。需要运行 Active Directory 的 Identity Manager 驱动程序。此驱动程序无法在 NetWare 服务器上运行，因为它必须运行在 Active Directory 环境中。需要在 Windows 2003 服务器上安装和运行远程装载程序。远程装载程序提供了 Active Directory 驱动程序和 Metadirectory 引擎之间的通讯通道。

  方案：非托管。Metadirectory 引擎在 Solaris 中运行。您需要与希望供应用户帐户的 NIS 系统进行通讯。该系统通常不托管 Metadirectory 引擎。需要在 NIS 系统中为 NIS 安装远程装载程序和 Identity Manager 驱动程序。NIS 系统中的远程装载程序运行 NIS 驱动程序，并且允许 Metadirectory 引擎和 NIS 驱动程序进行数据交换。

Identity Manager 3 通过 dirxml_remote、 rdxml 或 dirxml_jremote 提供远程装载程序功能。

Dirxml_remote

Dirxml_remote 是一个可执行文件，可以使 Metadirectory 引擎与运行在 Windows 中的 Identity Manager 驱动程序进行通讯。

远程装载程序控制台使用 dirxml_remote.exe。如果在命令行中不带任何参数指定 dirxml_remote.exe，将启动 " 远程装载程序应用程序向导 "。如果键入 dirxml_remote.exe 然后再输入参数，则将启动远程装载程序。

Rdxml

Rdxml 是一种可执行文件，可以使 Metadirectory 引擎与运行在 Solaris、Linux 或 AIX 环境中的 Identity Manager 驱动程序进行通讯。

Rdxml 支持本机和 Java 驱动程序。

Dirxml_jremote

Dirxml_jremote 是一种纯 Java 远程装载程序。它可以使运行在一台服务器上的 Metadirectory 引擎和运行在其它位置 （rdxml 或 Dirxml_jremote 未运行的位置）的 Identity Manager 驱动程序进行数据交换。Dirxml_jremote 理论上可以在装有兼容的 JRE （最低版本为 1.4.0、推荐 1.4.2 或更高版本）和 Java Sockets 的任何系统中运行，但是仅有如下系统正式支持该程序：

- HP-UX
- AS/400
- OS/390
- z/OS

概述：主要任务

使用远程装载程序涉及以下任务：

- 如果希望使用安全套接层 (SSL)，请提供安全数据传送证书。
- 安装、配置并运行远程装载程序。
- 导入、配置并启动 Identity Manager 驱动程序。

某些管理员更愿意在设置远程装载程序之前导入和配置 Identity Manager 驱动程序。例如，可能希望将某个正在运行的驱动程序变为远程运行驱动程序。

另一方面，如果远程装载程序正在运行，则可以导入、配置和启动驱动程序，然后立即检查 Metadirectory 引擎、远程装载程序和 Identity Manager 驱动程序之间是否正在进行正确的通讯。

3.2 提供安全数据传送

如果希望使用安全套接层 (SSL) 以便可以提供安全数据传送，则请完成以下任务：

1. 创建服务器证书。

   如果对证书不熟悉，请创建新证书。

   但是，如果 SSL 服务器证书已经存在并且您已经使用过 SSL 证书，则可以使用现有的证书而无需创建和使用新证书。

   如果服务器加入树， eDirectory 将创建以下默认证书：

   - SSL CertificateIP
   - SSL CertificateDNS
2. 导出自我签名证书。

3.2.1 创建服务器证书

1 在 Novell iManager 中，单击 "Novell 证书服务器 ">" 创建服务器证书 "。

2 选择要拥有该证书的服务器，并给证书取一个绰号 （例如， remotecert）。

重要 : 建议证书绰号中不要使用空格。例如，使用 remotecert 而不使用 remote cert。还需要记录证书绰号。您将在驱动程序的远程连接参数中使用此绰号作为 KMO 名称。

3 将 " 创建方式 " 设置为 " 标准 "，然后单击 " 下一步 "。

4 审阅摘要，单击 " 完成 "，然后单击 " 关闭 "。

服务器证书即创建完成。单击 “导出自我签名证书”在第 44 页 继续。

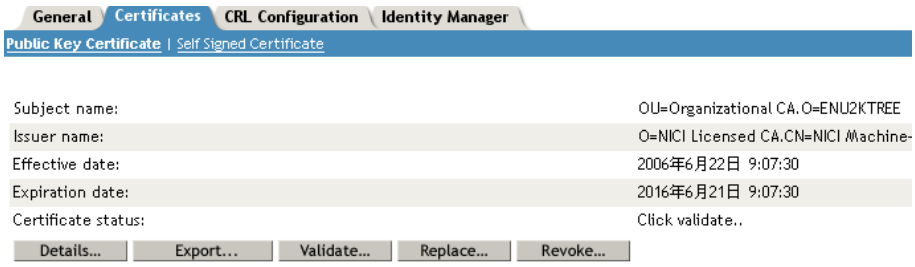
3.2.2 导出自我签名证书

1 在 iManager 中，单击 "eDirectory 管理 ">" 修改对象 "。

2 浏览并选择安全性树枝中的证书授权者，然后单击 " 确定 "。

根据树名 (Treename-CA.Security) 命名证书授权者 (CA)。

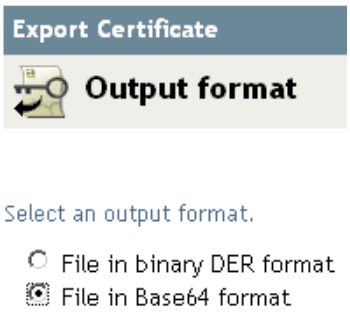
3 单击 " 证书 " 选项卡、 " 自我签名证书 "，然后单击 " 导出 "。



4 在 " 导出证书向导 " 中，选择 " 否 "，然后单击 " 下一步 "。

您不希望将私用密钥和证书一起导出。

5 选择 *File in Base64 format* （Base64 格式的文件）（例如， akranes-tree CA.b64），然后单击 " 下一步 "。



6 单击 *Save the exported certificate to a file* （将导出的证书保存为文件）链接，指定文件名和保存位置，然后单击 " 保存 "。

根文件名称需要以 .pem 为扩展名。

7 在 " 另存为 " 对话框中，将此文件复制到本地目录中。

8 单击 " 关闭 "。

3.3 设置远程装载程序

本节提供了以下信息：

- “安装远程装载程序”在第 46 页
- “配置远程装载程序”在第 48 页
- “在 Solaris、 Linux 或 AIX 中设置环境变量”在第 58 页
- “启动远程装载程序”在第 58 页 “停止远程装载程序”在第 61 页
- “停止远程装载程序”在第 61 页

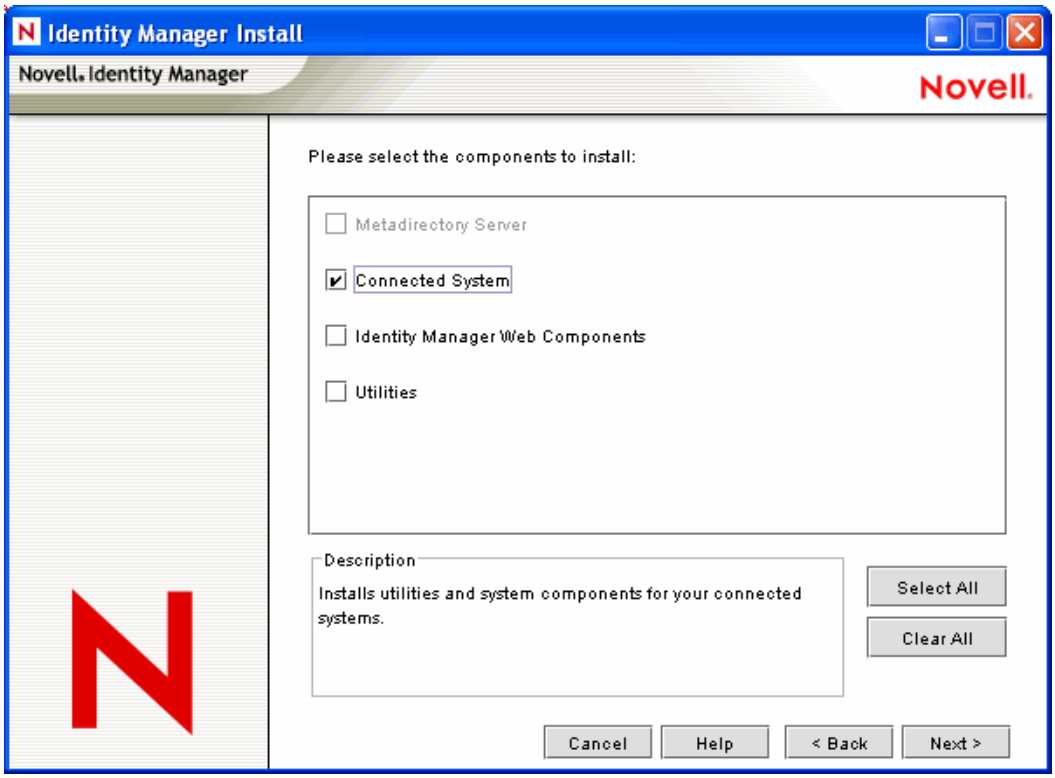
3.3.1 安装远程装载程序

本节提供了以下信息：

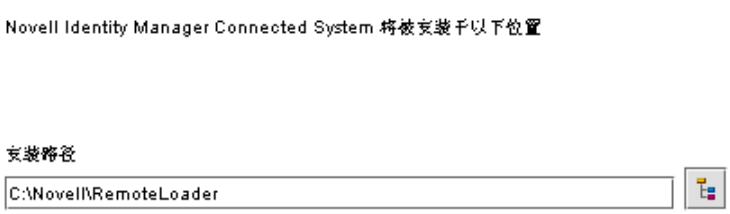
- “在 Windows Server 中安装远程装载程序。”在第 46 页
- “在 Solaris、 Linux 或 AIX 中安装远程装载程序”在第 47 页
- “在 HP-UX、 AS/400、 OS/390 或 z/OS 中安装远程装载程序”在第 48 页

在 **Windows Server** 中安装远程装载程序。

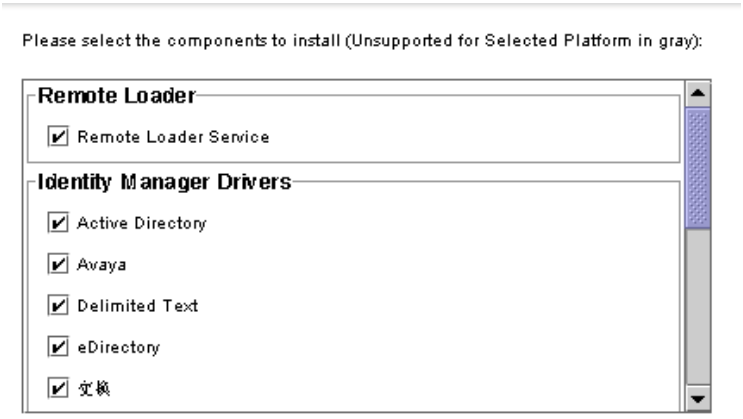
1. 运行 Identity Manager 3 安装程序 （例如， \nt\install.exe）。
2. 查看欢迎页，接受许可协议，并查看概述页 （共两页）。
3. 在 "Identity Manager Install" （安装 Identity Manager）对话框中，取消选择 *Connected System* （已连接系统）之外的所有组件，然后单击 " 下一步 "。



4. 选择已连接系统 （远程装载程序和远程驱动程序 Shim）的安装位置，然后单击 " 下一步 "。



5 选择 *Remote Loader Service* （远程装载程序服务）和远程驱动程序 Shim （驱动程序），然后单击 " 下一步 "。



6 确认激活请求，查看要安装的产品，然后单击 " 完成 "。

7 选择是否将 " 远程装载程序控制台 " 图标添加到桌面上。

在 Solaris、 Linux 或 AIX 中安装远程装载程序

本节假定您已下载和展开了 Identity Manager 3。如果需要下载 Identity Manager，请转至 Novell 下载万维网站点 (http://download.novell.com)。

展开从 Novell 万维网站点下载的 Identity Manager 3 文件后，请完成以下步骤：

1 根据您的平台，运行下列安装文件之一：

- dirxml_solaris.bin
- dirxml_linux.bin
- dirxml_aix.bin

2 接受许可协议后，按 Enter 键转至 "Choose Install Set" （选择安装设置）页：

```
===============================================================================
Choose Install Set
------------------

Please choose the Install Set to be installed by this installer.

  ->1- Metadirectory Server
    2- Connected System Server
    3- Web-based Administrative Server

    4- Customize...

ENTER THE NUMBER FOR THE INSTALL SET, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
   :
```

3 键入 2 选择 "Connected System Server" （已连接系统服务器），然后按 Enter 键。

4 在 "Pre-Installation Summary" （预安装摘要）屏幕中，查看所选的安装组件，然后按 Enter 键。

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

Please Review the Following Before Continuing:

Install Set
    Connected System Server

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


PRESS <ENTER> TO CONTINUE:
```

在 HP-UX、 AS/400、 OS/390 或 z/OS 中安装远程装载程序

HP-UX、 AS/400、 OS/390 和 z/OS 平台需要 Java 远程装载程序。

1 在要运行 Java 远程装载程序的目标系统中创建目录。

2 将 Identity Manager 3 CD 或下载映像的 /java_remoteloader 目录下的相应文件复制到第 1 步中创建的目录中：

平台	文件
HP-UX AS/400 z/OS OS/390	dirxml_jremote.tar.gz dirxml_jremote.tar.gz dirxml_jremote_mvs.tar dirxml_jremote_mvs.tar

3 对于 HP-UX、 AS/400 或 z/OS 平台，请解压缩 dirxml_jremote 文件。

4 解压缩刚复制的文件。

现在可以配置 Java 远程装载程序了。因为压缩文件中不包含驱动程序，所以必须手工将驱动程序复制到 lib 目录中。lib 目录位于发生解压缩的目录下。

有关 MVS 的信息，请对 dirxml_jremote_mvs.tar 文件进行解压缩。然后请参考 usage.html 文档。

3.3.2 配置远程装载程序

远程装载程序可以托管 .dll、 .so 或 .jar 文件中包含的 Identity Manager 应用程序 Shim。Java 远程装载程序仅能托管 Java 驱动程序 Shim，而不能装载或托管本机 (C++) 驱动程序 Shim。

- “在 Windows 中配置远程装载程序”在第 49 页
- “使用命令行选项配置远程装载程序”在第 53 页
- “启动远程装载程序”在第 58 页

- “停止远程装载程序”在第 61 页

在 **Windows** 中配置远程装载程序

- “使用远程装载程序控制台实用程序”在第 49 页
- “添加远程装载程序实例”在第 50 页
- “编辑远程装载程序实例”在第 53 页

使用远程装载程序控制台实用程序

远程装载程序控制台只能在 Windows 中运行。可以使用此控制台管理计算机中的远程装载程序下运行的所有 Identity Manager 驱动程序：

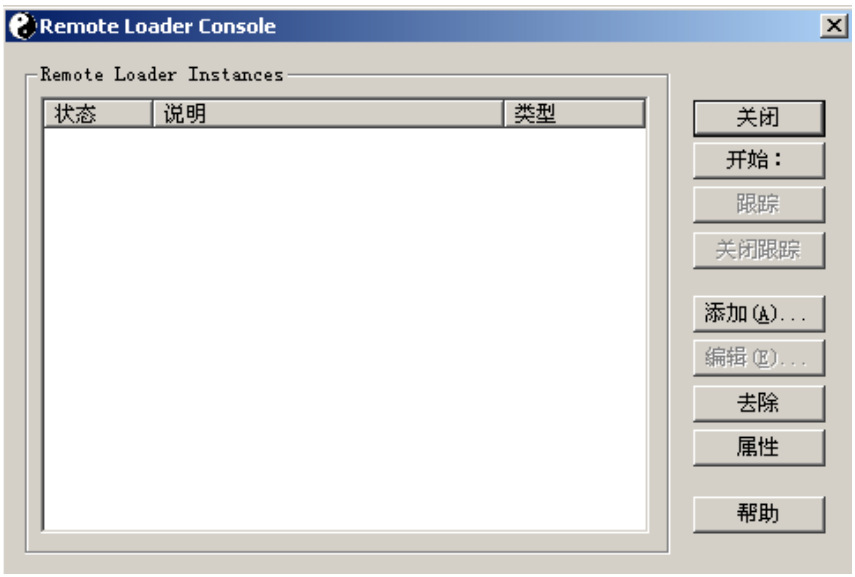
如果要升级到 Identity Manager 3，控制台将检测并导入远程装载程序的现有实例。（若要进行自动导入，驱动程序配置必须储存在远程装载程序目录中，通常为 c:\novell\remoteloader。）然后，就可以使用控制台管理远程驱动程序。

要启动远程装载程序控制台，请单击桌面上的 " 远程装载程序控制台 " 图标。

图 ***3-3*** ″远程装载程序控制台 ″图标

可以使用远程装载程序控制台启动、停止、添加、去除和编辑远程装载程序服务的每个实例。

图 ***3-4*** 远程装载程序控制台



如果在命令行中键入不带任何参数的 dirxml_remote.exe ，将启动 " 远程装载程序应用程序向导 "。

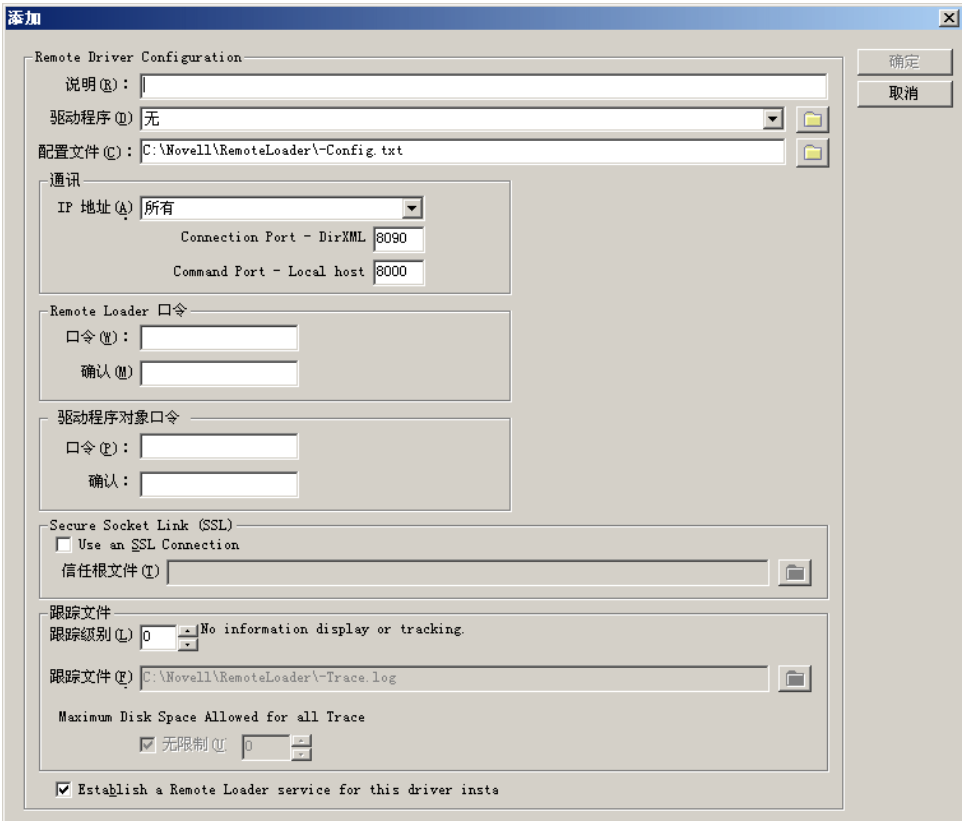
注释：同时使用向导和控制台会引发意外行为。因此，建议您先启动远程装载程序控制台，并将现有配置升级至控制台中。

添加远程装载程序实例

要添加远程装载程序实例，请单击 " 添加 "，然后提供以下信息：

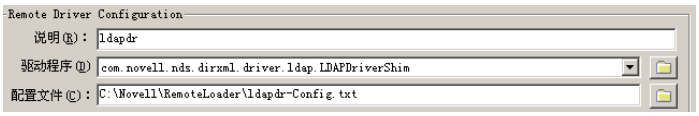
- “远程驱动程序配置”在第 51 页
- “通讯参数”在第 51 页
- “远程装载程序口令”在第 51 页
- “驱动程序对象口令”在第 52 页
- “安全套接链接 （安全套接层）”在第 52 页
- “跟踪文件”在第 52 页
- “为此驱动程序实例建立远程装载程序服务”在第 53 页

图 ***3-5*** 远程装载程序配置参数



远程驱动程序配置

图 ***3-6*** 远程驱动程序配置

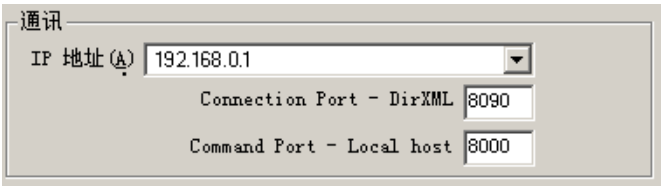


- 说明：指定说明以识别远程装载程序实例。
- 驱动程序：浏览并选择驱动程序的相应 Shim。
- 配置文件：指定配置文件的名称。

  远程装载程序控制台将配置参数置于此文本文件中，并在运行时使用这些参数。

通讯参数

图 ***3-7*** 通讯参数



- IP 地址：指定 IP 地址，远程装载程序利用此地址监听与 Metadirectory 服务器的连接。
- 连接端口 - Metadirectory 服务器：指定 TCP 端口，远程装载程序通过此端口监听与 Metadirectory 服务器的连接。

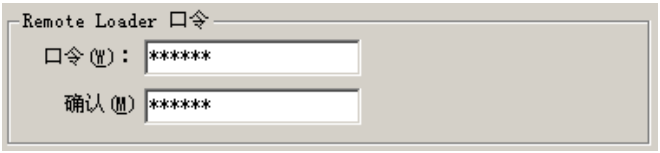
  此连接的默认 TCP/IP 端口为 8090。每创建一个新实例，默认端口号将自动加 1。
- 命令端口 - 仅用于本地主机通讯：指定 TCP 端口号，远程装载程序利用此端口号监听命令 （如 " 停止 " 和 " 更改跟踪级别 "）。

  运行在特定计算机上的远程装载程序的每个实例都必须具有一个不同的命令端口号。默认的命令端口是 8000。每创建一个新实例，默认端口号将自动加 1。

  注释 **:** 通过指定不同的连接端口和命令端口，可以在托管不同驱动程序实例的同一服务器上，运行远程装载程序的多个实例。

远程装载程序口令

图 ***3-8*** 远程装载程序口令



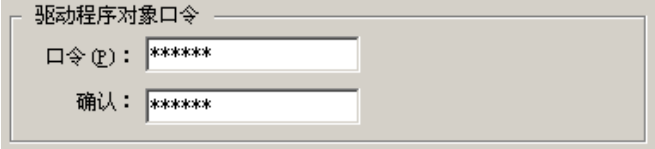
- 口令：此口令用来控制驱动程序对远程装载程序实例的访问。

  此口令必须与配置驱动程序时在 " 输入远程装载程序的口令 " 编辑框中键入的区分大小写的口令相同，该编辑框出现在 "Identity Manager 配置 " 页中的 " 鉴定 " 部分。

- 确认：重新输入口令。

驱动程序对象口令

图 ***3-9*** 驱动程序对象口令

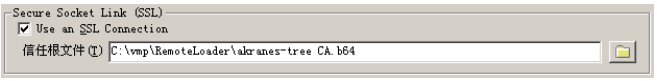


- 口令：远程装载程序使用此口令将其自身鉴定到 Metadirectory 服务器。

  此口令必须与配置驱动程序时在 " 驱动程序对象口令 " 编辑框中键入的口令相同，该编辑框出现在 " 驱动程序配置 " 页中。
- 确认：重新输入口令。

安全套接链接 （安全套接层）

图 ***3-10*** 安全套接链接 （安全套接层）

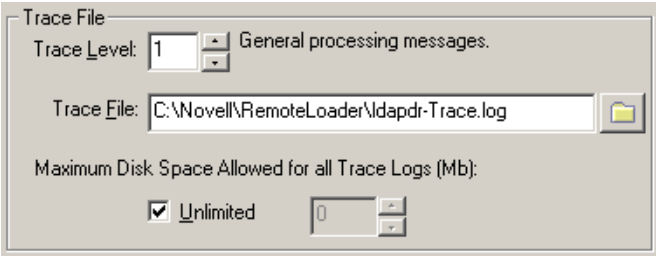


- 使用 SSL 连接：要指定 SSL 连接，请选择此选项。
- 可信根文件：浏览并选择可信根文件。

  这是从 eDirectory 树的组织证书授权者中导出的自我签名证书。请参见 “导出自我签名证书”在第 44 页 。

跟踪文件

图 ***3-11*** 跟踪文件



- 跟踪级别：若要使远程装载程序实例显示跟踪窗口，其中包含远程装载程序和驱动程序的信息类讯息，请将跟踪级别设置为大于零。一般将跟踪级别设置为 3。

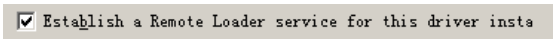
  如果将跟踪级别设置为 0，将不出现跟踪窗口，也不显示讯息。
- 跟踪文件：指定写入跟踪讯息的跟踪文件名。

  运行在特定计算机上的每个远程装载程序实例都必须使用不同的跟踪文件。仅在跟踪级别大于零时才将跟踪讯息写入跟踪文件中。

- 所有跟踪日志允许的最大磁盘空间 (MB)：指定此实例的跟踪文件数据在磁盘上可以占用的最大空间 （近似值）。

为此驱动程序实例建立远程装载程序服务

图 *3-12* 为此驱动程序实例建立远程装载程序服务



- 要将远程装载程序实例配置为一项服务，请选择此选项。启用此选项后，计算机启动时，操作系统将自动启动远程装载程序。

编辑远程装载程序实例

1. 从 " 说明 " 列中选择远程装载程序实例。
2. 单击 " 停止 "，键入远程装载程序口令，然后单击 " 确定 "。
3. 单击 " 编辑 "，然后修改配置信息。这些字段与添加远程装载程序实例时出现的字段相同。

使用命令行选项配置远程装载程序

要运行远程装载程序，所有的平台都需要使用配置文件 （例如， LDAPShim.txt）。可以使用命令行选项创建或编辑配置文件。以下步骤提供了配置文件基本参数的信息。有关附加参数的信息，请参见附录 B “用于配置远程装载程序的选项”在第 233 页 。

1. 打开文本编辑器。
2. （可选）使用 -description 选项指定说明。

选项	别名	参数	说明
-description	-desc	简短说明	指定简短说明字符串 （例如， SAP），作为跟踪窗口标题，并用于 Nsure Audit 日志记录。 示例： -description SAP -desc SAP 远程装载程序控制台在配置文件中使用长格式。可以使用长格式 （例如 -description）或者短格式 （例如 -desc）。

3. 使用 -commandport 选项指定远程装载程序实例将要使用的 TCP/IP 端口。

选项	别名	参数	说明
-commandport	-cp	端口号	指定远程装载程序实例进行控制时使用的 TCP/IP 端口。如果远程装载程序实例托管应用程序 Shim，则命令端口将是其它远程装载程序实例与托管 Shim 的实例通信的端口。如果远程装载程序实例要将命令发送至托管应用程序 Shim 的实例，则命令端口将是托管实例监听的端口。如果没有指定命令端口，则默认端口为 8000。通过指定不同的连接端口和命令端口，远程装载程序的多个实例可以在托管不同驱动程序实例的同一台服务器上运行。 示例： -commandport 8001 -cp 8001

4 使用 -connection 选项，为运行 Identity Manager 远程接口 Shim 的 Metadirectory 服务器的连接指定参数。

键入 -connection " 参数 [parameter] [parameter]"。

例如，键入以下示例之一：

```
-connection "port=8091 rootfile=server1.pem" -conn "port=8091
rootfile=server1.pem"
```

所有参数都必须包含在引号中。参数包括：

选项	别名	参数	说明
-connection	-conn	连接配置字符串	为运行 Identity Manager 远程接口 Shim 的 Metadirectory 服务器的连接指定连接参数。远程装载程序的默认连接方式是使用 SSL 的 TCP/IP。此连接的默认 TCP/IP 端口是 8090。远程装载程序的多个实例可以在同一台服务器上运行。远程装载程序的每个实例都托管一个单独的 Identity Manager 应用程序 Shim 实例。通过为每个远程装载程序实例指定不同的连接端口和命令端口，可以区分远程装载程序的多个实例。 示例： -connection "port=8091 rootfile=server1.pem" -conn "port=8091 rootfile=server1.pem"
port		decimal port number	必需参数。它指定远程装载程序监听与远程接口 Shim 的连接所使用的 TCP/IP 端口。 示例： port=8090

选项	别名	参数	说明
address		IP address	可选参数。指定远程装载程序监听特定本地 IP 地址。如果托管远程装载程序的服务器有多个 IP 地址，但远程装载程序只能监听其中一个地址时，这个参数将非常有用。 可以选择以下三项操作之一：address= *地址号* address= 誰 ocalhost' 不使用此参数。 如果不使用 -address，则远程装载程序监听所有本地 IP 地址。 示例：address=137.65.134.83
rootfile			条件性参数。如果要运行 SSL 并需要远程装载程序与本机驱动程序通讯，请键入 rootfile=' *可信证书名* '
keystore			条件性参数。仅适用于包含在 .jar 文件中的 Identity Manager 应用程序 Shim。 指定 Java 密钥存储区文件名，密钥存储区中包含远程接口 Shim 所使用证书的颁发者的可信根证书。通常由 eDirectory 树的证书授权者托管远程接口 Shim。 如果要运行 SSL 并需要远程装载程序与 Java 驱动程序通讯，请键入键 - 值对： keystore=' *密钥存储区名* ' storepass=' *口令* '
-storepass		storepass	仅适用于包含在 .jar 文件中的 Identity Manager 应用程序 Shim。指定由 keystore 参数指定的 Java 密钥存储区口令。 示例： storepass=mypassword 此选项仅应用于 Java 远程装载程序。

5 （可选）使用 -trace 选项指定跟踪参数。

选项	别名	参数	说明
-trace	-t	integer	指定跟踪级别。仅当托管应用程序 Shim 时才可使用此选项。跟踪级别与 Metadirectory 服务器中使用的级别相对应。 示例： -trace 3 -t 3

6 （可选）使用 -tracefile 选项指定跟踪文件。

选项	别名	参数	说明
-tracefile	-tf	filename	指定要写入跟踪讯息的文件。如果跟踪级别大于 0，则将跟踪讯息写入此文件。即使未打开跟踪窗口，也可将跟踪讯息写入此文件。 示例： -tracefile c:\temp\trace.txt -tf c:\temp\trace.txt

7 （可选）使用 -tracefilemax 选项限制跟踪文件的大小。

例如，键入以下示例之一：

```
-tracefilemax 1000M -tfm 1000M
```

本示例中，跟踪文件大小只能为 1 GB。

选项	别名	参数	说明
-tracefilemax	-tfm	size	指定跟踪文件数据可占用的最大磁盘空间 （近似值）。如果指定此选项，将有一个由 tracefile 选项指定其名称的跟踪文件，以及最多 9 个附加的 " 翻转 " 文件。翻转文件以其主跟踪文件的文件名作为基本名，后跟 "*_n*"，其中 n 为从 1 到 9 的数字。 大小参数为字节数。可使用后缀 K、M 或 G 来指定大小，它们分别代表 KB、 MB 或 GB。 如果启动远程装载程序时跟踪文件数据大于指定的最大值，则在所有 10 个文件都完成翻转之前，跟踪文件数据都将大于指定的最大值 示例： -tracefilemax 1000M -tfm 1000M 本示例中，跟踪文件大小只能为 1 GB。

8 使用 -class 选项指定类或使用 -module 选项指定模块。

选项	别名	参数	说明
-class	-cl	Java 类名	指定被托管的 Identity Manager 应用程序 Shim 的 Java 类名称。 例如，对于 Java 驱动程序，键入以下内容之一： -class com.novell.nds.dirxml.driver.ldap.LDAPDriverShim -cl com.novell.nds.dirxml.driver.ldap.LDAPDriverShim Java 使用密钥存储区读取证书。-class 选项和 -module 选项互相排斥。 要查看 Java 类名称列表，请参见附录 B “用于配置远程装载程序的选项”在第 233 页 中的表 B-2 在第 238 页。
-module	-m	modulename	指定包含被托管的 Identity Manager 应用程序 Shim 的模块。 例如，对于本机驱动程序，请键入以下内容之一： -module "c:\Novell\RemoteLoader\Exchange5Shim.dll" -m "c:\Novell\RemoteLoader\Exchange5Shim.dll" 或者 -module "usr/lib/dirxml/NISDriverShim.so" -m "usr/lib/dirxml/NISDriverShim.so" -module 选项使用 rootfile 证书。-module 选项和 -class 选项互相排斥。

9 命名并保存文件。

可以在远程装载程序运行时更改某些设置。有关这些设置的信息，请参考附录 B “用于配置远程装载程序的选项”在第 233 页。

参数	说明
-commandport	指定远程装载程序实例。
-config	指定配置文件。
-javadebugport	指定该远程装载程序实例将会在指定端口启用 Java 调试。
-password	允许通过命令发送。
-service	将实例作为一项服务进行安装。仅适用于 Windows。
-tracechange	更改跟踪级别。
-tracefilechange	更改写入内容的跟踪文件名称。
-unload	卸载远程装载程序实例。

参数	说明
-window	在远程装载程序实例中打开或关闭跟踪窗口。仅适用于 Windows。

在 Solaris、 Linux 或 AIX 中设置环境变量

安装远程装载程序后，即可设置环境变量 RDXML_PATH，从而更改 rdxml 的当前目录。此目录将作为随后创建文件的基本路径。要设置 RDXML_PATH 变量值，请输入以下命令：

- set RDXML_PATH=*path*
- export RDXML_PATH

启动远程装载程序

- “在 Windows 中启动远程装载程序”在第 58 页
- “通过命令行启动远程装载程序”在第 59 页

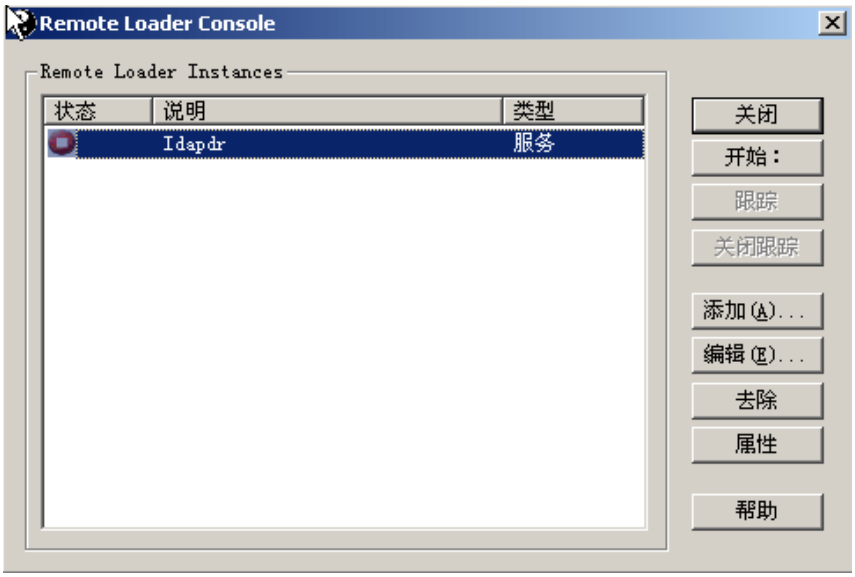
在 Windows 中启动远程装载程序

若要在 Windows 中运行远程装载程序：

图 ***3-13*** ″远程装载程序控制台″图标

1 单击桌面上的 " 远程装载程序控制台 " 图标。

图 *3-14* 远程装载程序控制台



2 选择一个驱动程序实例，然后单击 " 启动 "。

通过命令行启动远程装载程序

在 Solaris、 Linux 或 AIX 中，由二进制部件 rdxml 提供远程装载程序功能。此部件位于 /usr/bin/ 目录下。在 Windows 中，默认目录为 c:\novell\RemoteLoader。

若要运行远程装载程序：

1 设置口令。

平台	命令
Windows	dirxml_remote -config *配置文件路径* -sp *口令 口令*
Solaris Linux AIX	rdxml -config *配置文件路径* -sp *口令 口令*
HP-UX AS/400 OS/390 z/OS	dirxml_jremote -config *配置文件路径* -sp *口令 口令*

选项	别名	参数	说明
-password	-p	口令	指定用于命令鉴定的口令。此口令必须与用 **setpasswords** 指定的装载程序实例 （通过命令设置）的第一个口令相同。如果指定了一个命令选项（例如， unload 或 tracechange），但未指定 **password** 选项，则系统将提示用户输入此命令的目标装载程序的口令。 示例： -password novell4 -p novell4

选项	别名	参数	说明
-setpasswords	-sp	password password	指定远程装载程序实例口令，以及与此远程装载程序通讯的远程接口 Shim 的 Identity Manager 驱动程序对象口令。自变量中的第一个口令是远程装载程序的口令。可选自变量中的第二个口令是与 Metadirectory 服务器上远程接口 Shim 关联的 Identity Manager 驱动程序对象的口令。可以不指定口令，但如果指定，则必须同时指定两个口令。如果未指定口令，则远程装载程序将提示输入口令。这是一个配置选项。使用此选项可用指定的口令配置远程装载程序实例，但不能装载 Identity Manager 应用程序 Shim，也不能与其它装载程序实例通讯。 示例： -setpasswords novell4 staccato3 -sp novell4 staccato3

2 启动远程装载程序。

平台	命令
Windows	dirxml_remote -config *配置文件路径*
Solaris Linux AIX	rdxml -config *配置文件路径*
HP-UX AS/400 OS/390 z/OS	dirxml_jremote -config *配置文件路径*

3 使用 iManager 启动驱动程序。

4 确认远程装载程序可正常工作。

仅在远程装载程序与 Metadirectory 服务器上的远程接口 Shim 通讯时，远程装载程序才装载 Identity Manager 应用程序 Shim。这意味着，如果远程装载程序失去与 Metadirectory 服务器的通讯，应用程序 Shim 将关闭。

在 Linux、Solaris 或 AIX 中，使用 ps 命令或跟踪文件查找命令和连接端口是否在监听。

在 HP-UX 和与其类似的平台上，对跟踪文件使用 tail 命令监视 Java 远程装载程序：

```
tail -f ³ŽÞŸŒƒf°žÐ°
```

如果日志的最后一行如下所示，则表示装载程序正在正常运行并等待与 Identity Manager 远程接口 Shim 的连接：

```
TRACE:Remote Loader: Entering listener accept()
```

要配置远程装载程序 (rdxml) 以在 UNIX 中自动启动，请参见 TID 10097249 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10097249.htm)。

停止远程装载程序

平台	命令
Windows	使用远程装载程序控制台停止驱动程序实例。
Solaris Linux AIX	rdxml -config *配置文件路径* -u
HP-UX AS/400 OS/390 z/OS	dirxml_jremote -config *配置文件路径* -u

如果计算机中同时运行远程装载程序的多个实例，请传递 -cp 命令端口 选项，远程装载程序即可停止相应的实例。

要想停止远程装载程序，必须有足够的权限或输入远程装载程序口令。

方案：足够的权限。远程装载程序正在作为一项 Windows 服务运行。您拥有停止它的足够权限。您输入了一个口令，但意识到该口令并不正确。但远程装载程序还是停止了。

远程装载程序不 " 接受 " 此口令。由于在这种情况下此口令冗余，因此忽略了此口令。如果远程装载程序是作为应用程序运行，而不是作为服务运行的，则可以使用此口令。

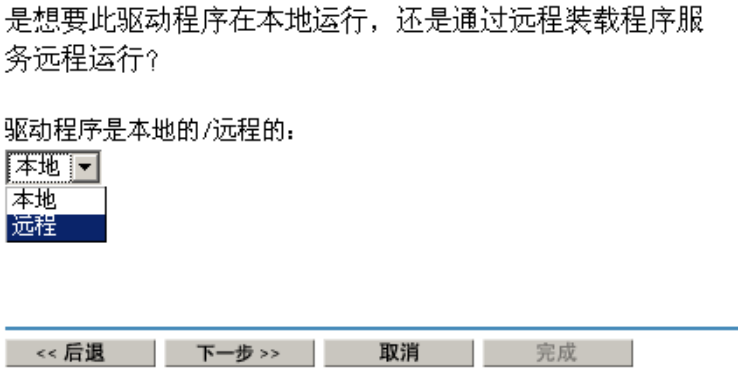
3.4 配置 Identity Manager 驱动程序，与远程装载程序配合使用

可以配置新的驱动程序或启用现有的驱动程序，与远程装载程序进行通讯。本节提供配置驱动程序的一般信息，以实现驱动程序与远程装载程序的通讯。有关附加信息和驱动程序特定的信息，请参考相关的驱动程序实施指南。

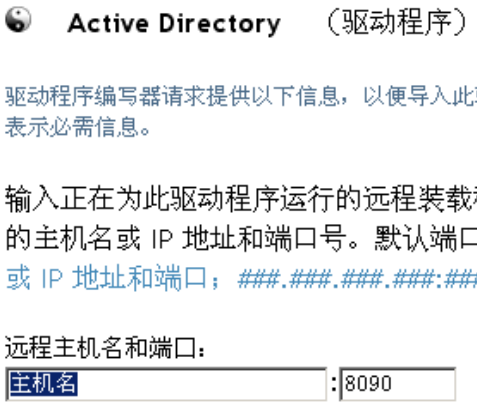
- “导入和配置新驱动程序”在第 61 页
- “配置现有的驱动程序”在第 62 页
- “创建密钥存储区”在第 64 页

3.4.1 导入和配置新驱动程序

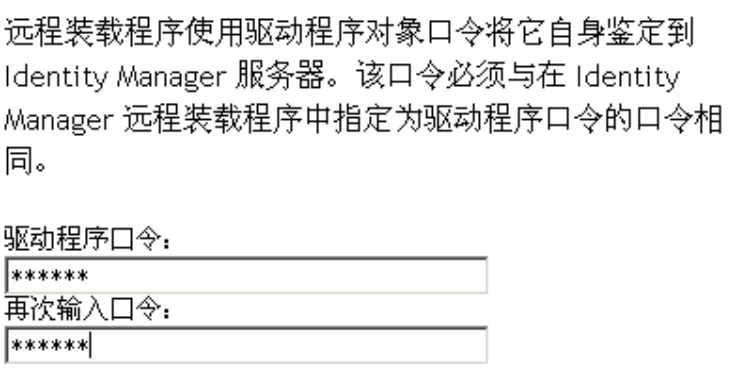
1. 在 Novell iManager 中，导入或创建新驱动程序并进行配置。
2. 滚动至 " 配置 " 选项底部，从下拉列表中选择 " 远程 "，然后单击 " 下一步 "。



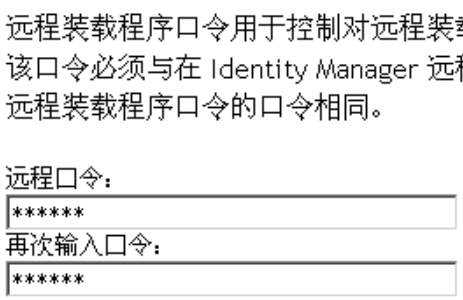
3 输入远程主机名和端口。



4 键入并再次输入驱动程序对象口令。



5 输入并再次输入远程装载程序口令，然后单击 " 下一步 "。



6 定义安全性等效用户，单击 " 下一步 "，然后单击 " 完成 "。

3.4.2 配置现有的驱动程序

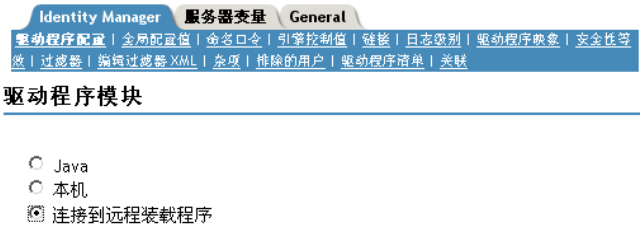
指定驱动程序对象的参数，以连接到远程装载程序。

1 在 Novell iManager 中，单击 *Identity Manager* >"Identity Manager 概述 "。

2 浏览并选择希望修改的驱动程序。

3 单击驱动程序状态图标，然后单击 " 编辑属性 "。

4 在 " 驱动程序模块 " 部分，选中 " 连接到远程装载程序 "。



5 在 " 鉴定 " 部分，输入远程装载程序参数。

- 远程装载程序连接参数

  之前已导出了自我签名证书。（请参见 “导出自我签名证书”在第 44 页 。）若使用 SSL，还需要自我签名证书的绰号。

  在 " 远程装载程序连接参数 " 编辑框中，以键 - 值对的形式键入参数。例如，键入

  ```
  hostname=192.168.0.1 port=8090 kmo=remotecert
  hostname=192.168.0.1 port=8090 kmo='remote cert'
  ```

  - hostname

主机名或 IP 地址 （例如， 190.162.0.1）。指定运行远程装载程序的计算机地址或名称。如果未指定 IP 地址或服务器名称，则默认值为 localhost。

- port

  远程装载程序接受与远程接口 Shim 连接的位置。如果未指定此通讯参数，则默认值为 8090。

- kmo

  指定密钥材料对象 (KMO) 的密钥名称 （例如， kmo=remotecert），而此 KMO 中包含 SSL 所用的密钥和证书。

  如果证书名称中包含空格，需要将 KMO 对象绰号放在单引号中。

  提示 **:** KMO 对象名称为 “创建服务器证书”在第 44 页 第 2 步中指定的绰号值。

- 输入应用程序口令

  指定应用程序用户 ID 的口令。通常情况下，驱动程序 Shim 需要此口令将驱动程序与应用程序相连接。

- 输入远程装载程序口令

  指定远程装载程序口令。远程接口 Shim 使用此口令将其自身鉴定到远程装载程序中。

  注释 **:** 请同时设置或重设置应用程序口令和远程装载程序口令。

6 单击 " 确定 "。

3.4.3 创建密钥存储区

密钥存储区是一个 Java 文件，其中包含加密钥、可能还包含证书 （可选）。如果要在远程装载程序和 Metadirectory 引擎间使用 SSL，而且将会使用 Java Shim，则需创建一个密钥存储区文件。

- “Windows 中的密钥存储区”在第 64 页
- “Solaris、 Linux 或 AIX 中的密钥存储区”在第 64 页
- “所有平台中的密钥存储区”在第 65 页

Windows 中的密钥存储区

在 Windows 中，运行 Keytool 实用程序，该程序通常位于 c:\novell\remoteloader\jre\bin 目录下。

Solaris、 Linux 或 AIX 中的密钥存储区

在 Solaris、 Linux 或 AIX 环境中，使用 create_keystore 文件。Create_keystore 与 rdxml 一同安装，同时也包括在 dirxml_jremote.tar.gz 文件中，该文件位于 \dirxml\java_remoteloader 目录下。create_keystore 文件为调用 Keytool 实用程序的壳层底稿。

在 UNIX 中，如果使用自我签名证书创建密钥存储区，可以将该证书以 Base64 或二进制 .der 格式导出。

在命令行中输入以下内容：

create_keystore 自我签名证书名 密钥存储区名

例如，键入以下任意一条内容

```
create_keystore tree-root.b64 mystore create_keystore tree-root.der
mystore
```

create_keystore 底稿指定密钥存储区口令的 "dirxml" 硬编码口令。由于密钥存储区中仅储存一个公共证书和一个公共密钥，因此不具有安全风险。

所有平台中的密钥存储区

要在任意平台上创建密钥存储区，可以在命令行中输入以下内容：

keytool -import -alias trustedroot -file 自我签名证书名 -keystore 文件名 -storepass

文件名 可以是任意名称 （例如， rdev_keystore）。

创建策略

4

可以使用策略在特定环境中自定义流入、流出 Identity Vault 的信息流。

例如，某个公司可能使用 inetorgperson 作为主用户类，而另一个公司则可能使用 User。要解决这个问题，需要创建策略将每个系统中的用户名通知 Metadirectory 引擎。只要在已连接系统间传递对用户产生影响的操作， Identity Manager 都将应用策略以进行上述更改。

也可利用策略创建新对象、更新特性值、进行纲要转换、定义匹配准则、维护 Identity Manager 关联，或实现其它目的。

有关策略的详细指南，包含在 《策略构建器和驱动程序自定义指南》 中。此指南包括：

- 每种可用策略的详细说明
- 关于策略构建器全面详尽的用户指南和参照，包括每个条件、操作、名词和动词的示例和语法。
- 讨论如何使用 XSLT 样式表创建策略。

有关策略的信息，请参考 《策略构建器和驱动程序自定义指南》。

已连接系统间的口令同步

5

5.1 概述

Identity Manager 利用通用口令和已连接系统对发布或订购口令的支持，提供了双向口令同步。

可以选择授权数据源，就像选择用户帐户的其它特性一样。

5.1.1 口令概述

NDS® 口令、简单口令、分发口令和通用口令分别用于不同的目的。在 eDirectory™ 和 Identity Manager 以前的版本中，已连接系统只能以单向同步的方法更新 NDS 口令。

Identity Manager 使用通用口令，该口令是可与其它 Identity Vault 口令同步的可逆口令。在 eDirectory 8.7.1 中开始引入通用口令，该口令受三层加密保护。

NMAS™ 用于控制通用口令和其它 Identity Vault 口令之间的关系。例如， NMAS 可控制通用口令是否与 NDS 口令、简单口令或分发口令保持同步。NMAS 截获进来的请求以更改口令，并根据 NMAS 口令策略中的设置处理这些请求。

Identity Manager 控制 Identity Vault 口令和已连接系统口令之间的关系。为此，它使用分发口令，该口令位于 Identity Vault 中，可以提供给已连接系统。与通用口令相同，分发口令也是受三层加密保护的可逆口令。

可以使用 NMAS 口令策略指定分发口令是否应与通用口令相同。（此设置为 " 在设置通用口令时同步分发口令 "）。如果分发口令与通用口令相同，且选择与已连接系统进行双向口令同步，请记住，此操作将使用 Identity Manager 从 eDirectory 中抽取通用口令并将该口令发送到其它已连接系统。需要确保口令的传输安全和储存该口令的已连接系统的安全。（请参见第 7 章 “安全性：最佳实践”在第 179 页。）

如果分发口令与通用口令不同（由于在 NMAS 口令策略中禁用此设置），则可以在使用分发口令的已连接系统间对口令执行 " 隧道通讯进程 "，而不必使用或影响通用口令或 NDS 口令。请记住，隧道通讯进程仅在已连接系统间同步口令。如果启用隧道通讯进程，也不会设置 Identity Vault/ 通用口令。

有关不同 eDirectory 口令的更多信息，请参见 《*Novell Modular Authentication Services (NMAS) 2.3* 管理指南》(http://www.novell.com/documentation/nmas23/index.html)。有关使用口令与 Identity Manager 同步的不同方法示例，请参见 “实施口令同步”在第 98 页。

5.1.2 什么是双向口令同步？

双向口令同步包括 Identity Manager 从指定的已连接系统接受口令，以及将口令分发到指定的已连接系统。

是否能够与特定的已连接系统进行双向口令同步取决于此已连接系统支持的内容。

一些已连接系统可接受来自 Identity Manager 的新的和修改过的口令，也可向 Identity Manager 提供用户的实际口令。这些已连接系统就是支持与 Identity Manager 之间的双向口令同步的系统：

- Active Directory
- Novell® eDirectory
- 网络信息服务 (NIS)
- NT 域

对于这些已连接系统，用户可以在其中一个系统中更改口令，并通过 Identity Manager 将此口令同步到其它系统。但如果在 NMAS 口令策略中使用高级口令规则，那么最好在 iManager 自助控制台中进行口令更改。由于这里列出了该用户口令必须遵守的所有规则，因此这是更改口令的最佳位置。

由于其它已连接系统不能提供用户的实际口令，因此它们不能支持完全双向口令同步。但它们可以在驱动程序配置中定义策略，从而提供用于创建口令的数据，并将它们发送到 Identity Manager。

其它一些系统可以接受 Identity Manager 的口令，包括为新用户设置初始口令、修改口令或进行这两种操作。请参见 “已连接系统支持口令同步”在第 77 页。

5.1.3 比较 Password Synchronization 1.0 和 Identity Manager 口令同步

表 *5-1* 比较：*Password Synchronization 1.0* 和 *Identity Manager* 口令同步

	Password Synchronization 1.0	Identity Manager 2 和 3 的口令同步
产品递送	独立于 Identity Manager 的产品。	包括在 Identity Manager 中，不单独销售的产品。
平台	◆ Active Directory ◆ NT 域 ◆ eDirectory	以下平台支持完全双向口令同步： ◆ Active Directory ◆ eDirectory ◆ NIS ◆ NT 域 这些已连接系统支持向 Identity Manager 发布用户口令。由于通用口令和分发口令是可逆的，因此 Identity Manager 可以将口令分发到已连接系统。 任何支持订购者口令要素的已连接系统都可以从 Identity Manager 订购口令。 请参见 “已连接系统支持口令同步”在第 77 页 。
Identity Vault 中使用的口令	NDS 口令 （不可逆）	通用口令 （可逆）或分发口令 （可逆）。如果需要，也可以使 NDS 口令保持同步。有关示例方案，请参见 “实施口令同步”在第 98 页 。
Windows 已连接系统的主要功能	向 Identity Manager 发送口令，使 Identity Vault 口令与 Windows 口令同步。因为 NDS 口令不可逆，所以不会将该口令发送回 NT 或 AD。	提供双向口令同步。因为通用口令和分发口令均为可逆口令，所以可以双向同步这些口令。
LDAP 更改	不支持。	支持
Novell® Client™	需要。	不需要。
nadLoginName 特性	用于保持口令更新。	不使用。
包含口令同步功能的部件	包含更新 nadLoginName 功能的 Identity Manager 驱动程序。	驱动程序配置中的 Identity Manager 策略提供口令同步功能。驱动程序仅需执行 Metadirectory 引擎根据策略逻辑安排的任务。驱动程序清单、全局配置值和驱动程序过滤器设置也必须支持口令同步。这些都包括在样本驱动程序配置中，也可以添加到现有的驱动程序中。请参见 “升级现有驱动程序配置以支持口令同步”在第 90 页 。
代理	独立的软件。	未安装代理；现在驱动程序中即包含此功能。

5.1.4 Identity Manager 口令同步的功能

Identity Manager 口令同步是双向的。口令可以从已连接系统发出，由 Identity Manager 接受；也可以从 Identity Manager 分发，由已连接系统接受。

接受来自已连接系统的口令

如同 DirXML® 和 Identity Manager 的之前版本一样，任何已连接系统都可以向 Identity Vault 发布口令。

可以指定 Identity Manager 从哪个已连接系统应用程序接受口令。甚至可以选择 Identity Manager 要对运行 Identity Manager 的同一 Identity Vault 中的用户更新口令，还是仅充当管道或 " 隧道 " 在已连接系统间同步口令。这意味着如果需要，可以将 Identity Vault 口令和 Identity Manager 分发给已连接系统的口令分开。

一些已连接系统 （AD、其它 Identity Vault、 NT 和 NIS）可以提供用户的实际口令，这意味着当用户在一个已连接系统中更改口令时，所做的更改可以被同步到 Identity Manager，并由其它已连接系统收回。

其它已连接系统则不支持提供用户的实际口令，但可以将它们配置为向 Identity Manager 提供在样式表中生成的口令，例如，根据姓或员工 ID 生成的初始口令。

向已连接系统分发口令

Identity Manager 口令同步可以将通用口令分发到已连接系统。

在 Identity Manager 之前的版本中，驱动程序可以从已连接系统的用户帐户向 Identity Manager 发送口令，还可以使用此口令在 eDirectory 中更新相应的用户。但由于 eDirectory 中的 NDS 口令是不可逆的，因此无法从中央 Identity Manager Identity Vault 向多个已连接系统送出口令。只有在 eDirectory 口令储存于 eDirectory 前将其捕获，才能获取此口令 （例如，可通过 Novell Client）。

eDirectory 8.7.3 提供的通用口令为可逆口令，可以分发。

Identity Manager 可以从已连接系统接受口令。由于通用口令是可逆的，因此 Identity Manager 可以将口令从 Identity Vault 分发到已连接系统，该系统须支持为新帐户设置初始口令和修改口令。

不管口令从哪里发出， Identity Manager 都使用分发口令作为储存库，从中将口令分发到已连接系统。可以对分发口令和通用口令实施口令策略。

有关在同步口令时使用通用口令和分发口令的信息，请参见 “实施口令同步”在第 98 页 。

如同用户的其它特性一样，可以决定哪个系统为口令授权源。Identity Manager 将口令从授权源分发到其它已连接系统。

可以在支持双向口令同步的已连接系统中设置双向口令同步。

在数据储存器和已连接系统上实施口令策略

通过调用 NMAS， Identity Manager 可以对进来的口令实施口令策略。如果已连接系统向 Identity Manager 发布的口令不符合策略，可以指定 Identity Manager 不允许口令进入 Identity Vault。这也意味着不符合策略的口令将不能被分发到其它已连接系统。

另外， Identity Manager 还可以对已连接系统实施口令策略。如果向 Identity Manager 发布的口令不符合策略中的规则，可以指定 Identity Manager 不接受口令进行分发，还可以使用 Identity Vault 中当前的分发口令重设置已连接系统中不符合规则的口令。

例如，口令中需要至少包括一个数字字符。但已连接系统本身没有能力实施此策略。则可以指定 Identity Manager 重设置从已连接系统流出的但不符合策略中规则的口令。

如果要使用高级口令规则和 Identity Manager 口令同步，建议调查所有已连接系统的口令策略，确保 eDirectory 口令策略中的高级口令规则相互兼容。此调查有助于使口令同步成功。

请记住，必须确保被指派 NMAS 口令策略的用户与应当加入已连接系统口令同步的用户相匹配。

NMAS 口令策略是以树为中心指派的。与此相反，口令同步是在每个驱动程序上分别设置的。同样，驱动程序安装在每台服务器上，且只能管理主复本或读 / 写复本中的用户。要获得预期的口令同步结果，请确保运行口令同步驱动程序的服务器上的主复本或读 / 写复本中的树枝与已指派口令策略 （该策略启用通用口令）的树枝相匹配。将口令策略指派给分区根树枝可确保将此口令策略指派给树枝和子树枝中的所有用户。

有关如何将 NMAS 口令策略指派给用户的信息，请参见 《口令管理管理员指南》(http://www.novell.com/documentation/password_management/index.html) 中的 " 为用户指派口令策略 "。

口令同步方案

可以使用 Identity Manager 指定口令权威来源系统，还可以决定口令流动方式。

Identity Manager 口令同步的许多功能取决于通用口令，该口令是由 Identity Vault 提供的可逆口令功能。但某些方案不需要部署通用口令。

Identity Manager 口令同步还取决于分发口令。可以对分发口令实施策略，如同对通用口令实施策略一样。

有关实施口令同步的基本方法，请参见 “实施口令同步”在第 98 页 。可以将这些方案结合起来，以满足环境的需要。

在未安装 **Novell Client** 的 **Windows** 中同步口令

在 Active Directory 和 NT 域中，不再需要 Novell Client 进行口令同步。

通知用户口令同步失败

在数据储存器和已连接系统上实施口令策略一节介绍了 Identity Manager 可以不接受来自已连接系统的不符合策略的口令，从而实施口令策略。

使用电子邮件通知功能，可以指定 Identity Manager 在用户进行口令更改失败时通知用户。

方案。已将 Identity Manager 设置为当从 NT 域进来的口令不符合口令策略时，不接受此口令。已启用电子邮件通知功能。NMAS 口令策略中的一个规则指定，不能将公司名称用作口令。某个用户将 NT 域已连接系统的口令更改为公司名称。NMAS 不接受此口令，则 Identity Manager 向用户发送电子邮件讯息，声明未同步口令更改。

在使用此功能前，必须先设置电子邮件服务器和模板。可自定义以下内容：

- Identity Manager 发送的讯息文本
- 通知，并将复本发送给管理员

有关更多信息，请参见 “配置电子邮件通知”在第 131 页。

检查用户的口令同步状态

可以使用 Identity Manager 查询已连接系统，以检查用户的口令同步状态。如果已连接系统支持检查口令功能，则可以检查口令是否成功同步。

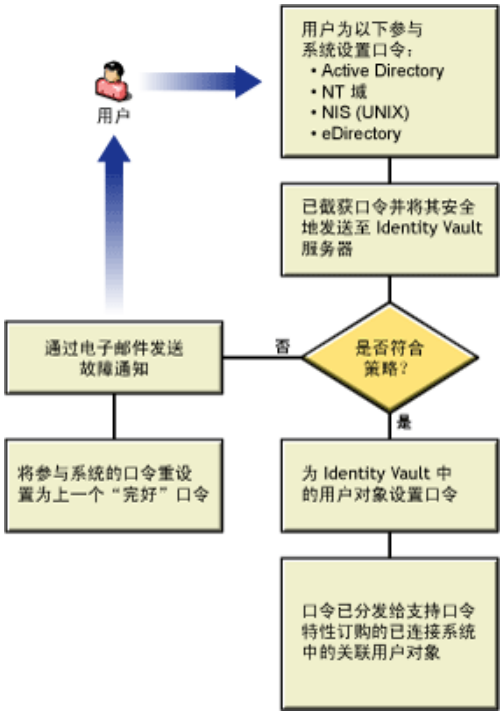
有关如何检查口令的信息，请参见 “检查用户的口令同步状态”在第 130 页。

有关支持检查口令的系统列表，请参见 “已连接系统支持口令同步”在第 77 页。

5.1.5 口令同步流程概述图

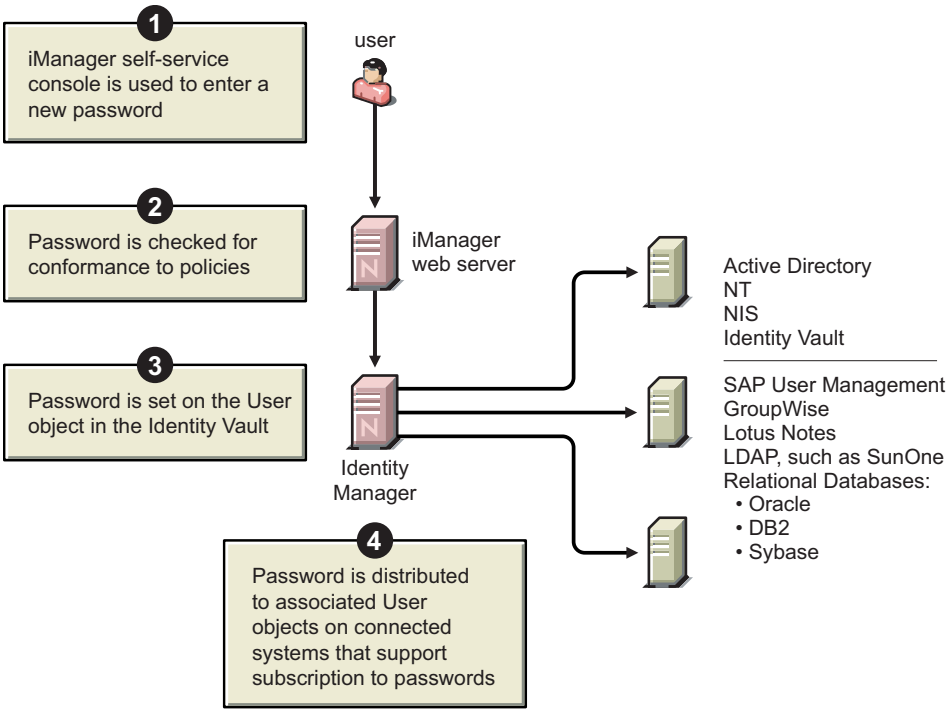
下图说明了已连接系统如何向 Identity Manager 发布口令。

图 ***5-1*** 已连接系统如何向 *Identity Manager* 发布口令。



下图说明了 Identity Manager 如何向已连接系统分发口令。

图 **5-2** *Identity Manager* 如何向已连接系统分发口令

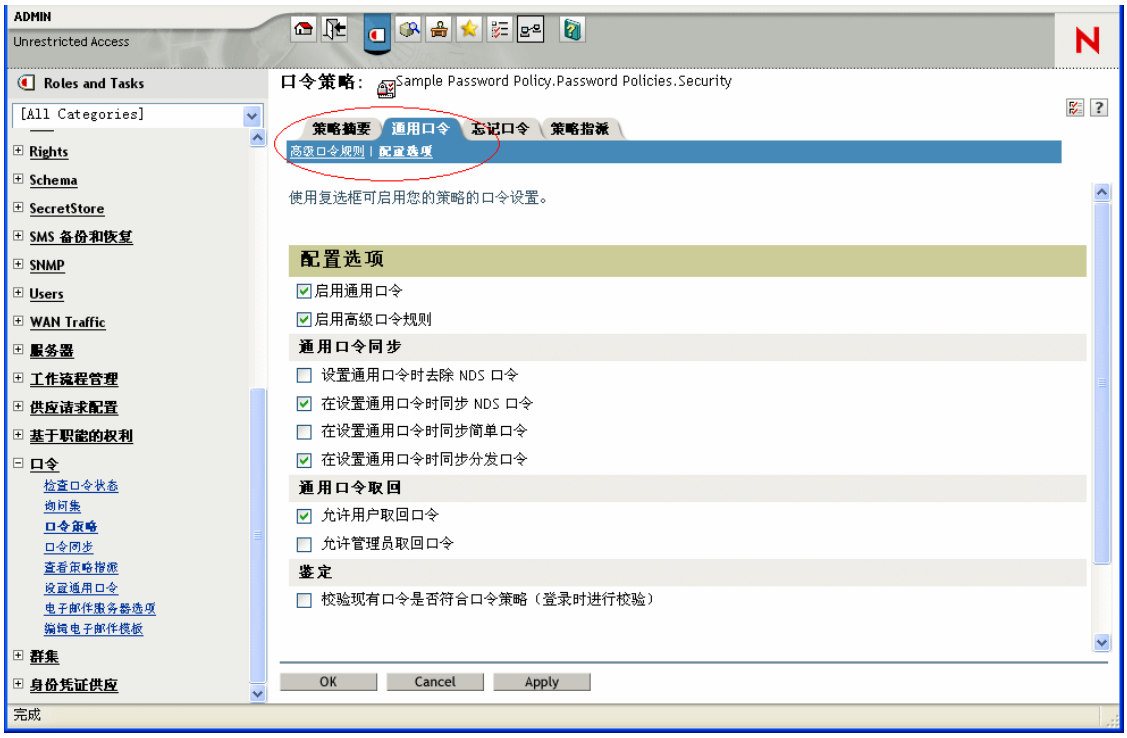


5.1.6 图的显示方式

此文档中经常使用图来说明 iManager 中的选项。这些选项在桌面上的实际显示方式取决于所使用的浏览器。

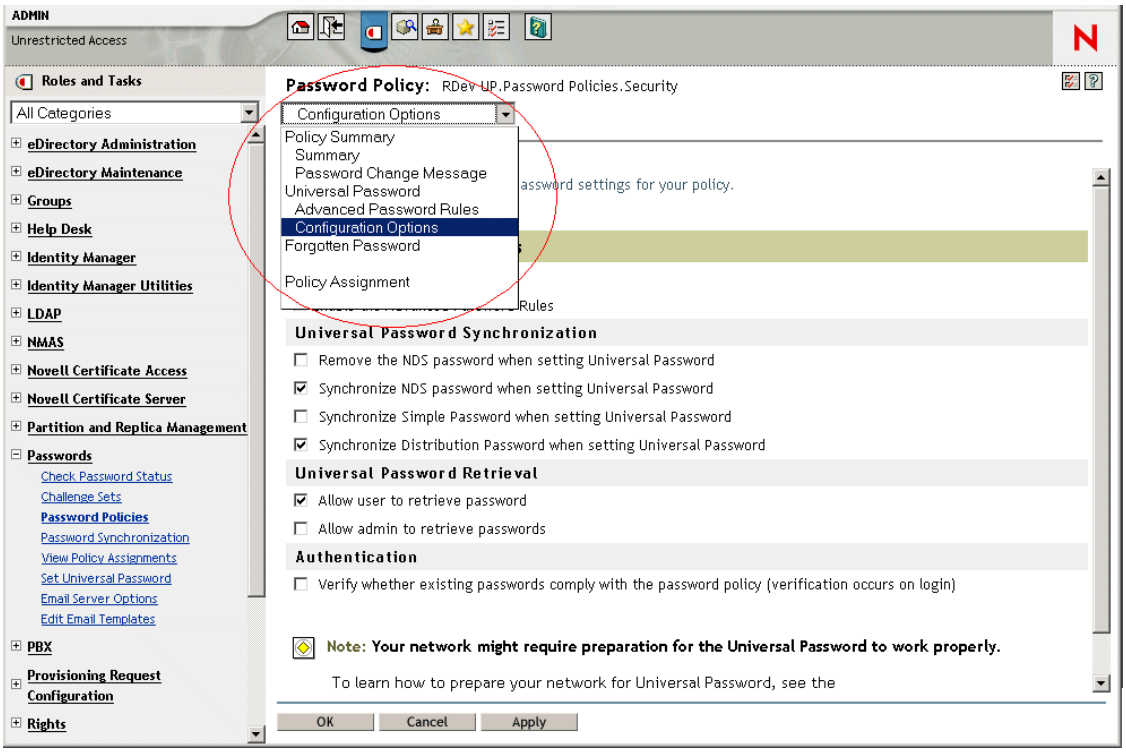
例如， Internet Explorer 使用选项卡显示 iManager 选项。

图 ***5-3*** *iManager* 中的选项卡



但 Firefox 浏览器通过下拉列表显示 iManager 选项。

图 **5-4** *iManager* 中的下拉列表



在此文档中图的显示方式与 Firefox 浏览器中相同。

5.2 已连接系统支持口令同步

创建用户对象后， Identity Manager 始终可以接受已连接系统的口令，即使已连接系统不支持从本系统提供用户实际口令。

AD、 NT、 eDirectory 和 NIS 可以接受 Identity Manager 的口令，也支持向 Identity Manager 发送用户实际口令。这意味着它们完全支持双向口令同步。

在发布者通道的驱动程序配置中定义策略时，其它系统可提供用于创建口令的数据。大多数驱动程序的示例驱动程序配置包含一个示例策略，该策略提供一个根据姓氏确定的默认口令。

已连接系统具有多种功能，可从 Identity Manager 接受口令。某些已连接系统支持为新帐户设置初始口令集，但不支持口令修改事件。

样本驱动程序配置的功能在驱动程序清单中进行说明。下表提供了驱动程序清单中没有列出的附加信息。这些表指出应用程序是接受新帐户的初始口令集，还是可以接受对现有口令进行修改。而清单仅指出已连接系统能接受口令，并不显示此差别。

所有驱动程序都归类分组，这样就可以查看具有相似功能的样本驱动程序配置。

5.2.1 支持双向口令同步的系统

以下已连接系统支持双向口令同步。它们可以提供已连接系统中的用户实际口令，并从 Identity Manager 接受口令。

表 *5-2* 支持双向口令同步的系统

已连接系统驱动程序	订购者通道	订购者通道	订购者通道	发布者通道
	应用程序可接受初始口令设置	应用程序可接受口令修改	应用程序支持口令检查	应用程序可提供（同步）口令
Active Directory	是	是	是	是
eDirectory[1]	是	是	是	是
NT 域	是	是	否	是
NIS	是	是	是	是
SIF	是	是	否	是

[1] 在 Identity Vault 树之间，即使尚未对用户启用通用口令，这些用户也可使用双向口令同步。请参见 “方案 1：使用 NDS 口令在两个 Identity Vault 间进行同步”在第 100 页 。

5.2.2 从 Identity Manager 接受口令的系统

以下已连接系统在某种程度上可从 Identity Manager 接受口令。它们无法向 Identity Manager 提供已连接系统中的用户实际口令。

尽管这些系统无法提供用户实际口令，但可以根据已连接系统中的其它用户数据，使用发布者通道上的策略对其进行配置，从而创建口令。（样本驱动程序配置所示为根据姓氏确定的默认口令。）

表 *5-3* 从 *Identity Manager* 接受口令的系统

已连接系统驱动程序	订购者通道	订购者通道	订购者通道	发布者通道
	应用程序可接受初始口令设置	应用程序可接受口令修改	应用程序支持口令检查	应用程序可提供（同步）口令
GroupWise®	是	是	否	否[2]
JDBC	是[3]	否[4]	否	否[5]
LDAP	是[6]	是[6]	是	否
Notes	是	是[7]	是[7]	否
SAP 用户管理	是	是	否	否

[2] GroupWise 支持两种鉴定方法：

- GroupWise 自身提供鉴定并维护用户口令。

- GroupWise 使用 LDAP 鉴定 eDirectory，并且不维护口令。

  使用该选项时， GroupWise 将忽略与驱动程序同步的口令。

[3] 对于操作系统用户帐户不同于数据库用户帐户的所有数据库，都有设置初始口令的功能，例如 Oracle*、 MS SQL、 MySQL* 和 Sybase*。

[4] JDBC 的 Identity Manager 驱动程序可用于修改已连接系统中的口令，但样本驱动程序配置中未说明该功能。

[5] 口令储存在表中时，可作为数据进行同步。

[6] 目标 LDAP 服务器允许设置 userpassword 特性时成立。

[7] Notes 驱动程序可接受口令修改，并且只检查 Lotus Notes 中 HTTPPassword 字段的口令。

5.2.3 不接受或不提供口令的系统

以下已连接系统无法使用样本驱动程序配置接受口令或提供已连接系统的用户口令。

尽管这些系统无法向 Identity Manager 提供用户口令，但可以根据已连接系统中的其它用户数据，使用发布者通道上的策略对其进行配置，从而创建口令。（样本驱动程序配置所示为根据姓氏确定的默认口令。）

表 ***5-4*** 不接受或不提供口令的系统

已连接系统驱动程序	订购者通道	订购者通道	订购者通道	发布者通道
	应用程序可接受初始口令设置	应用程序可接受口令修改	应用程序支持口令检查	应用程序可提供 （同步）口令
定界文本	否[8]	否[8]	否[8]	否[8]
Exchange 5.5	否	否	否	否
PeopleSoft 3.6	否	否	否	否
PeopleSoft 4.0	否	否	否	否
SAP HR	否	否	否	否

[8] 定界文本的 Identity Manager 驱动程序的驱动程序 Shim 中没有直接支持口令同步的功能。但是，可根据所同步的已连接系统，对驱动程序进行配置以处理口令。

5.2.4 不支持口令同步的系统

以下已连接系统不会使用口令同步。

表 *5-5* 不支持口令同步的系统

已连接系统驱动程序	订购者通道	订购者通道	订购者通道	发布者通道
	应用程序可接受初始口令设置	应用程序可接受口令修改	应用程序支持口令检查	应用程序可提供（同步）口令
Avaya* PBX	否	否	否	否
权利服务驱动程序	否	否	否	否
回送服务驱动程序	否	否	否	否
手工任务服务驱动程序	否	否	否	否

5.3 口令同步的前提条件

进行口令同步需要具备以下要素：

- “支持通用口令”在第 80 页
- “驱动程序清单中声明的口令同步功能”在第 80 页
- “使用全局配置值控制口令同步”在第 81 页
- “驱动程序配置中所需的策略”在第 83 页
- “安装在已连接系统中，用于截获口令的过滤器”在第 86 页
- “为用户创建的 NMAS 口令策略”在第 86 页
- “NMAS 登录方法”在第 86 页

5.3.1 支持通用口令

要在不同已连接系统间使用口令同步， Identity Manager 需要通用口令。参见：

- 《口令管理管理员指南》(http://www.novell.com/documentation/password_management/index.html) 中的 " 部署通用口令 "
- “准备使用通用口令”在第 87 页

5.3.2 驱动程序清单中声明的口令同步功能

驱动程序清单声明已连接系统是否支持以下口令同步功能：

- 向 Identity Manager 发布用户实际口令
- 从 Identity Manager 接受口令

  清单中不区分接受初始口令创建还是接受口令修改。
- 令 Identity Manager 检查已连接系统中的口令，以确定用户的口令同步状态

注释：驱动程序清单由创建驱动程序配置的驱动程序开发者或 Identity Manager 专家编写，而不应由网络管理员编辑。驱动程序清单显示驱动程序 Shim 和配置的真实功能。仅更改清单并不会改变功能。要添加功能，则需要增强驱动程序 Shim、已连接系统或驱动程序配置。

Identity Manager 递送的样本驱动程序配置中包含驱动程序清单项。要将它们添加到现有驱动程序中，请参见 “升级现有驱动程序配置以支持口令同步”在第 90 页 。

5.3.3 使用全局配置值控制口令同步

可使用全局配置值设置策略中可参照的常量值。全局配置值有时称为服务器变量，因为这些值所暂挂的特性存在于每个复本中。

进行口令同步时，可使用全局配置值创建流入和流出 Identity Manager 的口令设置。由于编写驱动程序配置中的 Identity Manager 口令同步策略时就考虑到根据全局配置值中的设置进行不同的行为，因此无需编辑策略就可以轻松更改口令流。

使用全局配置值可以分别控制每个已连接系统的如下设置。

表 *5-6* 已连接系统的设置

设置	说明
Identity Manager 是否接受已连接系统的口令	该设置适用于已连接系统提供的口令，以及可由发布者通道的驱动程序配置中的 Identity Manager 策略创建的口令。如果禁用该设置，那么这两种口令都会被去除，使其无法到达 Identity Manager。
Identity Manager 使用的同步方法：直接更新通用口令，或直接更新分发口令	Identity Manager 控制项点 （Identity Manager 更新的口令）。NMAS 根据 NMAS 口令策略中的设置，控制每种不同口令之间的口令流动。要查看 NMAS 口令策略： 1. 在 iManager 中，选择 " 口令 ">" 口令策略 "。 2. 在 " 口令策略列表 " 中选择一项策略。 3. 单击 " 编辑 "。 4. 从下拉列表或选项卡中选择一个选项 （取决于所使用的 iManager 版本）。 有关使用这些方法的方案，请参见第 5.8 节， " 实施口令同步 "。
是否对从已连接系统进入 Identity Manager 的口令实施 NMAS 口令策略	如果实施这些策略，将不会把进来的不符合策略的口令写入 Identity Manager 数据储存器。
Identity Manager 是否通过重设置不符合策略规则的口令，使用 Identity Manager 口令在已连接系统上实施 NMAS 口令策略。	如果已连接系统不支持该选项 （已在驱动程序清单中声明），则 NMAS 界面中该选项灰显。发布者通道上的口令操作失败时，才需重设置口令。
已连接系统是否接受口令	由 Identity Manager 分发的口令，以及通过订购者通道的驱动程序配置中的 Identity Manager 策略创建的口令，均可应用该设置。如果禁用该设置，那么这两种口令都会被去除，使其无法到达已连接系统。 如果已连接系统不支持该选项 （已在驱动程序清单中声明），则界面中该选项灰显。
口令不同步时，是否通过电子邮件通知用户	自动给受影响的用户发送电子邮件。

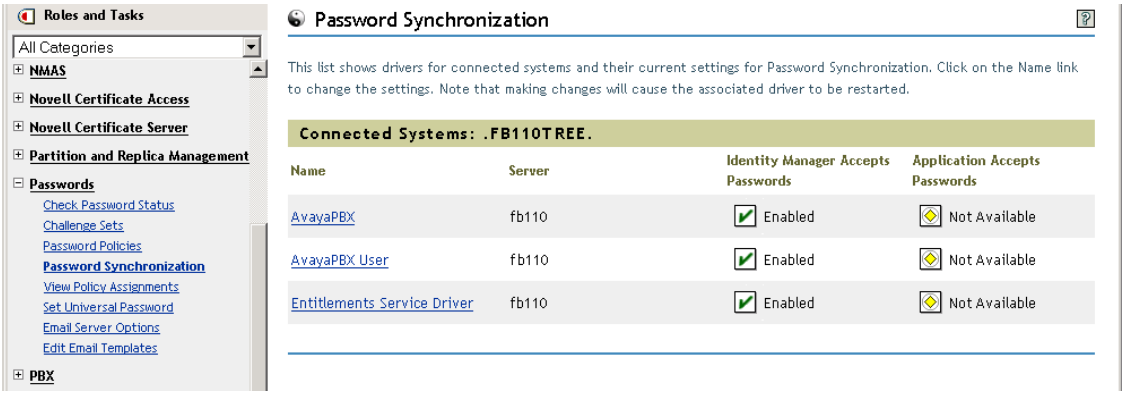
Identity Manager 递送的驱动程序配置中包含驱动程序清单项。要将它们添加到现有驱动程序中，请参见 “升级现有驱动程序配置以支持口令同步”在第 90 页 。

要编辑全局配置值：

1 在 iManager 中，选择 " 口令 ">" 口令同步 "。

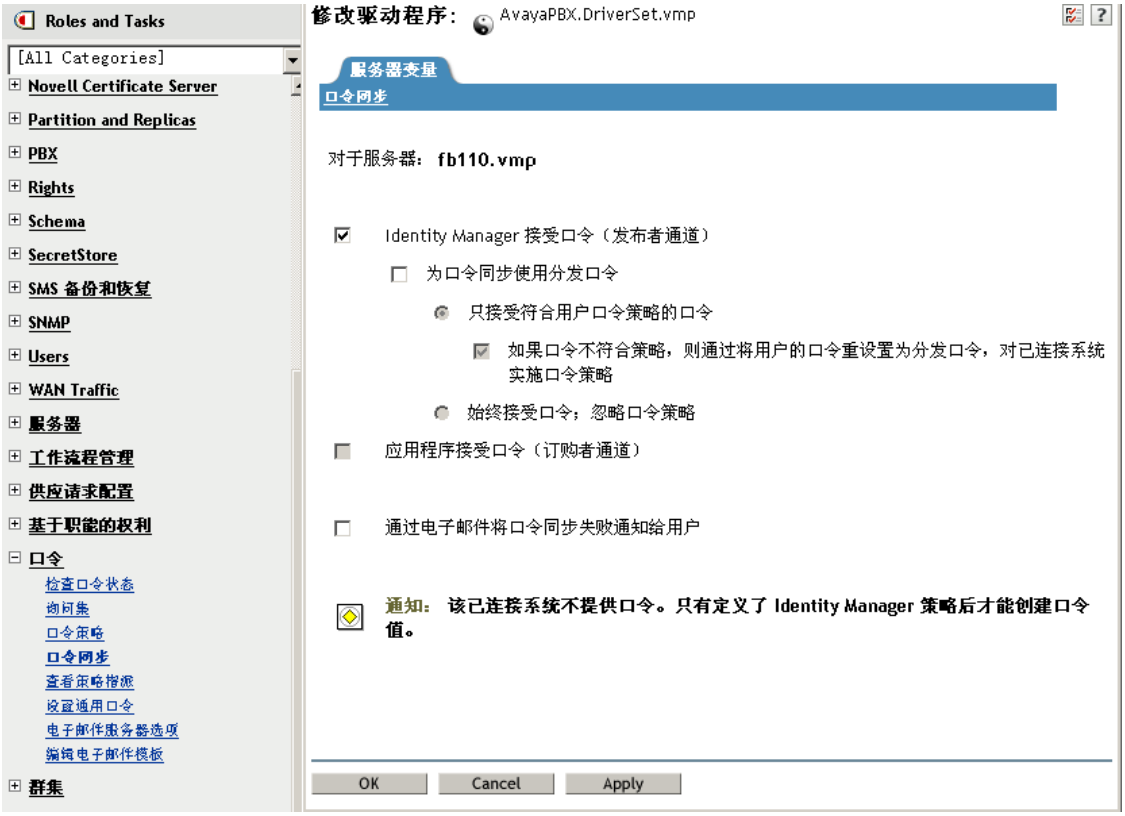
2 搜索驱动程序。

指定已连接系统驱动程序的搜索位置之后， iManager 将显示找到的所有已连接系统驱动程序的口令流设置概述。



3 要查看设置，请单击驱动程序名称。

" 修改驱动程序 " 页显示口令同步的全局配置值。



如果此页中的某个选项灰显，驱动程序清单中会显示已连接系统不支持该选项。

4 进行更改，然后单击 " 确定 "。

注释：可以对每个驱动程序分别设置全局配置值。驱动程序的全局配置值会覆盖驱动程序集的全局配置值。对特定的驱动程序设置此值有助于进行更细微的控制。该页仅显示单个驱动程序上出现的全局配置值。

如果对驱动程序集对象设置全局配置值，而驱动程序集中的某个驱动程序自身没有值，则该驱动程序将继承这些值。如果驱动程序自身没有设置，而是从驱动程序集继承了全局配置值，则 iManager 不会显示这些值。尽管 iManager 不会显示继承的全局配置值，口令同步策略仍将采用这些值。

5.3.4 驱动程序配置中所需的策略

每个驱动程序的发布者通道和订购者通道上的 Identity Manager 策略，都会根据上文中所述的全局配置变量中的设置来管理口令流。这些策略包含在 Identity Manager 的驱动程序配置中。

如果要升级现有驱动程序配置，而不是进行替换，则必须向此配置添加某些策略。（请参见“升级现有驱动程序配置以支持口令同步”在第 90 页。）要使口令同步正常工作，这些策略必须位于驱动程序配置中的正确位置。

- “发布者命令转换集中所需的策略”在第 83 页
- “发布者输入转换策略集中所需的策略”在第 84 页
- “订购者命令转换策略集中所需的策略”在第 85 页
- “订购者输出转换策略集中所需的策略”在第 85 页

发布者命令转换集中所需的策略

" 口令同步策略名称 " 列所列出的策略必须按列出的顺序出现。同样，它们也必须是发布者命令转换集中最后的策略。

表 ***5-7*** 发布者命令转换集中所需的策略

驱动程序配置中的位置	口令同步策略名称	该策略的作用
发布者命令转换	口令 （发布） - 默认口令策略	如果 " 添加 " 对象中不包含任何口令，则将默认口令添加到 " 添加 " 对象中。 只能修改或去除该策略以及 Password(Sub)-Default Password Policy。要使口令同步功能正常工作，不应更改其它策略。
	口令 （发布） - 检查口令 GCV	检查 GCV 以确定是否指定了 Identity Manager 从该已连接系统接受口令。如果未指定，将去除所有口令要素。 GCV 的名称为 enable-password-publish，显示名称为 *Identity Manager accepts passwords from application*。
	口令 （发布） - 发布分发口令	将 <password> 要素转换为某种形式，允许它更新通用口令。 该策略参照以下 GCV： ◆ publish-password-to-dp ◆ enforce-password-policy
	口令 （发布） - 发布 NDS 口令	如果指定应更新 NDS 口令，将允许 <password> 要素通过检查。如果未指定，将去除 <password> 要素。 该策略将参照名为 publish-password-to-nds 的 GCV。
	口令 （发布） - 添加口令有效负载	放入引擎中传送的有效负载数据，用于电子邮件通知。
	口令 （订购） - 添加口令有效负载	放入引擎中传送的有效负载数据，用于电子邮件通知。

发布者输入转换策略集中所需的策略

如果输入转换中有多项策略，建议将口令 （发布） - 订购电子邮件通知策略列在最后。

表 ***5-8*** 发布者输入转换策略集中所需的策略

驱动程序配置中的位置	口令同步策略名称	该策略的作用
发布者输入转换	口令（发布）- 订购电子邮件通知	如果出现口令有效载荷信息，且状态显示出现问题，将向用户发送电子邮件。它将邮件发送至用户的电子邮件地址，eDirectory 的 Internet EMail Address（因特网电子邮件地址）特性中指明了该地址。 该策略将参照名为 notify-user-on-password-dist-failure 的 GCV，以确定是否发送通知电子邮件。

订购者命令转换策略集中所需的策略

" 口令同步策略名称 " 列所列出的策略必须按列出的顺序出现。同样，它们也必须是订购者命令转换集中最后的策略。

表 ***5-9*** 订购者命令转换策略集中所需的策略

驱动程序配置中的位置	口令同步策略名称	该策略的作用
订购者命令转换	口令 （订购） - 转换分发口令	将通用口令转换为 <password> 要素。
	口令 （订购） - 默认口令策略	如果 " 添加 " 对象中不包含任何口令，则将默认口令添加到 " 添加 " 对象中。 只能修改或去除该策略以及 Password(Pub)-Default Password Policy。要使口令同步功能正常工作，不应更改其它策略。
	口令 （订购） - 检查口令 GCV	检查 GCV 以确定是否指定了已连接系统接受口令。如果未指定，将去除所有口令要素。 GCV 的名称为 enable-password-subscribe，显示名称为 *Application accepts passwords from Identity Manager data store*。
	口令（订购）- 添加口令有效负载	放入引擎中传送的有效负载数据，以用于电子邮件通知。

订购者输出转换策略集中所需的策略

如果输出转换中有多项策略，建议将口令 （订购） - 发布电子邮件通知策略列在最后。

表 *5-10* 订购者输出转换策略集中所需的策略

驱动程序配置中的位置	口令同步策略名称	该策略的作用
订购者输出转换	口令（订购）- 发布电子邮件通知	如果出现口令有效载荷信息，且状态显示出现问题，将向用户发送电子邮件。 该策略将参照名为 notify-user-on-password-dist-failure 的 GCV，以确定是否发送通知电子邮件。

5.3.5 安装在已连接系统中，用于截获口令的过滤器

对于 AD、 NT 域和 NIS，必须安装过滤器以截获用户口令。

请参见 “设置口令过滤器”在第 127 页 。

5.3.6 为用户创建的 NMAS 口令策略

尽管没有通用口令也可以使用口令同步的某些功能，但要为用户启用通用口令，则必须使用 NMAS 口令策略。还可使用此口令策略指定高级口令规则，并指定是否检查用户现有的口令是否遵从规则。

要使用 Identity Manager 口令同步，必须了解口令策略。口令策略在 《口令管理管理员指南》(http://www.novell.com/documentation/password_management/index.html) 的 " 使用口令策略管理口令 " 中有说明。

5.3.7 NMAS 登录方法

在某些情况下，必须依靠 NMAS 简单口令登录方法才能使用口令功能。例如， LDAP 就需要这种登录方法。

有关登录方法的信息，请参见 《*Novell Modular Authentication Services (NMAS) 3.0* 管理指南》(http://www.novell.com/documentation/nmas30/index.html)。

5.4 准备使用 Identity Manager 口令同步和通用口令

5.4.1 将用户从 NDS 口令切换到通用口令

使用口令策略对一组用户开启通用口令时，用户需要通用口令被填充。

如果之前一直使用口令同步更新 NDS 口令，则需要进行用户口令转换。要切换到使用通用口令，可进行以下操作之一，使用户创建通用口令：

- 如果使用 Novell Client，请使用支持通用口令的 Novell Client。

  Identity Manager 口令同步不需要使用 Novell Client。

  如果使用 Novell Client，用户下次使用 Novell Client 登录时， Novell Client 将在对 NDS 口令进行哈希处理之前先截获它，并用它填充通用口令。（请参见 《口令管理指南》中的 " 计划用户的登录和口令更改方法 "。）
- 如果未使用 Novell Client，用户可以登录 iManager 自助服务控制台。这种登录方法会填充通用口令。要访问 iManager 自助服务控制台，请转至 iManager 服务器上的 /nps。例如， https://www.myiManager.com/nps。
- 通过使用任意服务令用户登录，该服务由启用通用口令的 LDAP 服务器进行鉴定。例如，通过公司入口登录。

5.4.2 帮助用户更改口令

用户在 iManager 中更改口令时，将显示 iManager 自助服务控制台、 Novell Client 或 NMAS 口令策略的高级口令规则。查看规则后，用户无需猜测规则即可创建遵从口令。

根据口令流的设置，用户可更改已连接系统的口令，并且该口令会与 Identity Manager 和其它已连接系统同步。但是，用户更改口令时，已连接系统不会显示高级口令规则。

如果要实施高级口令规则并避免出现不符合规则的口令，最好要求用户只在 iManager 自助服务控制台或 Novell Client 中更改口令，或至少确保用户已充分了解高级口令规则。

在已连接系统中，允许用户不查看口令策略规则即更改口令。因此，用户可能无法正确记住这些规则。用户首次进行更改时，仅实施已连接系统本身的策略。在已连接系统上创建不符合规则的口令时，可能会出现以下问题，这取决于 Identity Manager 设置：

- 如果已启用对口令 （从已连接系统至 Identity Manager）实施策略的设置，用户的新口令也不会与 Identity Vault 同步。如果已设置 Identity Manager 向用户通知所发生的故障，用户可以通过电子邮件获知口令未同步。
- 如果还设置了令 Identity Manager 替换已连接系统中不符合规则的口令，用户使用所选的新口令将无法登录到已连接系统。

  Identity Manager 将已连接系统中的口令重设置为分发口令，这可能是该用户创建的最后一个遵从口令。

5.4.3 准备使用通用口令

要准备使用通用口令，请参考 《口令管理管理员指南》(http://www.novell.com/documentation/password_management/index.html) 中的 " 部署通用口令 "。您所需的大多数信息都可在该章中找到。

另外，请记住以下几点要求：

- 使用通用口令需要 eDirectory 8.7.1 或更高版本。不需要 NetWare® 6.5。
- Identity Manager 口令同步需使用通用口令和分发口令。分发口令是 Identity Manager 向已连接系统分发口令的储存库。和通用口令一样，也可对分发口令实施 NMAS 策略。

- Identity Manager 附带的 Identity Manager iManager 插件中包含口令管理插件。利用这些插件可以创建口令策略，并确定通用口令与 NDS 口令、简单口令和分发口令的同步方式。

  这些插件替换了 NetWare 6.5 中附带的通用口令插件。在 《口令管理管理员指南》(http://www.novell.com/documentation/password_management/index.html) 中的 " 使用口令策略管理口令 " 中进行了说明。
- Identity Manager 正在使用的树不能使用 eDirectory 8.6.2。但是，口令同步功能的子集支持 eDirectory 8.6.2。因此，如果不准备升级整个环境，可将 eDirectory 8.6.2 用于其它树。
- 为了部署通用口令而升级软件时，降低影响的一种方法是，为 Identity Manager 创建一个单独的树作为 Identity Vault。许多环境已对 Identity Manager 和驱动程序使用了 Identity Vault。
- 通用口令可提供原来的口令管理工具所不支持的功能，例如实施口令策略和使用特殊字符功能。
- 升级 Novell Client 和其它实用程序很重要，这样可避免 NDS 口令与通用口令不同步（有时称为 " 口令偏移 "）。请参见 《口令管理管理员指南》(http://www.novell.com/documentation/password_management/index.html) 中的 " 计划用户登录和更改口令方法 "。
- Novell Client 的最新版本支持通用口令，首次对用户启用通用口令时可填充该用户的通用口令，并且用户在更改口令时可显示和实施 NMAS 口令策略。
- 已连接系统不显示口令策略中创建的高级口令规则。在这种情况下，尽管 Novell Client 会实施这些规则，但也不会显示它们。

  最好要求用户只在 iManager 自助服务控制台中更改口令。

  如果允许用户在已连接系统中或使用 Novell Client 的最新版本更改口令，应确保用户充分了解口令策略规则，以帮助用户成功创建遵从口令。
- 确保管理员和服务台了解，只有在 NetWare® 6.5 服务器或更高版本上使用 ConsoleOne ® 时，或在具有最新 Novell Client 的计算机上使用 ConsoleOne ® 时，才支持通用口令。
- 确保管理员和服务台用户了解，使用仅支持 NDS 口令的实用程序的含意。这些实用程序可用于登录，但不能用于更改口令。该样可避免口令偏移。

  Novell Modular Authentication Services (NMAS) 3.0 管理指南 (http://www.novell.com/documentation/nmas30/index.html) 参照 TID，其中列出了实用程序及其对通用口令的支持。

5.4.4 匹配树枝

NMAS 口令策略是以树为中心指派的。与此相反，口令同步是在每个驱动程序上分别设置的。驱动程序安装在每台服务器上，且只能管理主复本或读 / 写复本中的用户。

要获得预期的口令同步结果，请确保运行口令同步驱动程序的服务器上的主复本或读 / 写复本中的树枝与已指派口令策略 （该策略启用通用口令）的树枝相匹配。将口令策略指派给分区根树枝可确保将此口令策略指派给树枝和子树枝中的所有用户。

5.4.5 设置电子邮件通知

要使用电子邮件通知功能，必须执行以下操作：

- 使用 iManager 中的通知配置任务设置电子邮件服务器。

- 如果需要，使用 iManager 中的通知配置任务自定义电子邮件模板。
- 确保 Identity Vault 用户的因特网电子邮件地址特性已填充。

请按照 “配置电子邮件通知”在第 131 页 中的指导操作。

5.5 配置和同步新驱动程序

如果尚未在环境中使用 Password Synchronization 1.0，并且要创建驱动程序或使用新的 Identity Manager 配置替换现有配置，请设置 Identity Manager 口令同步功能。

1 请确保环境已就绪，可使用通用口令。

请参见 “准备使用 Identity Manager 口令同步和通用口令”在第 86 页 。

2 创建驱动程序，或使用 Identity Manager 3 配置替换现有驱动程序配置。

Identity Manager 配置包含 Identity Manager 策略和 Identity Manager 口令同步所需的其它项目。有关导入新样本驱动程序配置的信息，请参见 Identity Manager 驱动程序指南 (http://www.novell.com/documentation/beta/dirxmldrivers)。

3 创建已启用通用口令的 NMAS 口令策略，开启用户的通用口令。

请参见 《口令管理管理员指南》(http://www.novell.com/documentation/password_management/index.html) 中的 " 创建口令策略 "。如果之前在 NetWare 6.5 中使用过通用口令，则 《口令管理管理员指南》 的 " （仅 NetWare 6.5）重新创建通用口令指派 " 中还描述了一些额外的步骤。

建议在树中尽可能高的位置指派口令策略。

可在 " 配置选项 " 页中选择 NMAS 同步不同种类口令的方式。

有关使用口令同步的方案，以及如何相应调整 Identity Manager 口令策略，请参见 “实施口令同步”在第 98 页 。另请参见联机帮助。

4 （仅 Active Directory、 NIS 或 NT 域）如果希望已连接系统向 Identity Manager 提供用户口令，请安装新口令同步过滤器并进行配置。

有关指导，请参见 Identity Manager 驱动程序 (http://www.novell.com/documentation/lg/dirxmldrivers/index.html) 中每个驱动程序的实施指南。

5 请确保每个已连接系统的口令流方向设置正确。

5a 在 iManager 中，单击 " 口令 ">" 口令同步 "，并搜索要管理的已连接系统的驱动程序。

5b 查看口令流的当前设置。

这是全局配置值 (GCV) 的图形界面。单击某一驱动程序的名称进行编辑。可以编辑以下设置：

- Identity Manager 是否从该系统接受口令。
- 希望 Identity Manager 更新哪个口令：直接更新通用口令还是直接更新分发口令。

  Identity Manager 控制项点，即 Identity Manager 更新哪个口令。NMAS 根据 " 配置选项 " 中对口令策略的设置，控制不同种类的各口令间的口令流。请参见 步骤 3 在第 89 页 中的图。
- 是否对进入 Identity Manager 的口令更改实施用户口令策略。
- 是否通过重设置不符合规则的口令，对已连接系统实施用户口令策略。
- 该已连接系统是否接受口令。
- 口令同步失败后是否发送电子邮件通知。

6 测试口令同步。

- 确认 Identity Manager 口令已分发到所指定的系统。
- 确认指定的已连接系统是否正在向 Identity Manager 发布口令。

有关查错提示，请参见 “实施口令同步”在第 98 页 。

5.6 升级 Password Synchronization 1.0

本任务仅适用于 Password Synchronization 1.0 所使用的 Active Directory 和 NT 域中现有 Identity Manager 驱动程序。

升级 Password Synchronization 1.0 时，遵循正确的步骤很重要。

有关指导，请参见 Identity Manager 驱动程序 (http://www.novell.com/documentation/dirxmldrivers/index.html) 中关于 Active Directory 和 NT 域的 Identity Manager 驱动程序实施指南。

5.7 升级现有驱动程序配置以支持口令同步

本节解释如何将 Identity Manager 口令同步的支持添加到现有的驱动程序配置中，而不使用 Identity Manager 样本配置替换现有的驱动程序配置。

对每个将加入口令同步的驱动程序添加支持。要实现此目的，需导入 "overlay" 配置文件，一次性添加策略、驱动程序清单和 GCV。

添加策略、驱动程序清单和 GCV 后，还必须将 nspmDistributionPassword 特性添加到驱动程序过滤器中。

重要：如果要升级 AD 或 NT 域的 Identity Manager 驱动程序，并且 Password Synchronization 1.0 正在使用该驱动程序，请遵循 Active Directory 和 NT 域的 Identity Manager 驱动程序升级指导，该指导位于 Identity Manager 驱动程序 (http://www.novell.com/documentation/dirxmldrivers/index.html) 的驱动程序实施指南中。

此步骤中添加的策略使用通用口令和分发口令来支持口令同步。如果仅使用 Identity Manager 驱动程序同步 NDS 口令，则不需使用 Identity Manager 驱动程序配置中的策略。使用 Public Key （公共密钥）和 Private Key （私用密钥）特性就可同步 NDS 口令，而无需使用这些策略，详情请见“方案 1：使用 NDS 口令在两个 Identity Vault 间进行同步”在第 100 页。

- “第 1 步：将驱动程序转换为 Identity Manager 3 格式”在第 91 页
- “第 2 步：添加至驱动程序配置”在第 94 页
- “第 3 步：更改过滤器设置”在第 95 页
- “第 4 步：设置口令同步流”在第 97 页

前提条件

- ❑ 使用 " 导出驱动程序向导 " 创建现有驱动程序的备份。
- ❑ 请确保已安装新的驱动程序 Shim。

  没有新的 Identity Manager 驱动程序 Shim，某些口令同步功能 （例如，检查口令状态）无法工作。

  重要：如果要升级 AD 或 NT 域的 Identity Manager 驱动程序，并且 Password Synchronization 1.0 正在使用该驱动程序，请先阅读升级指导，再安装驱动程序 Shim。请遵循 Active Director 和 NT 域的 Identity Manager 驱动程序升级指导，该指导位于 Identity Manager 驱动程序 (http://www.novell.com/documentation/dirxmldrivers/index.html) 的驱动程序实施指南中。

5.7.1 第 1 步：将驱动程序转换为 Identity Manager 3 格式

1. 请确保环境已就绪，可使用通用口令。

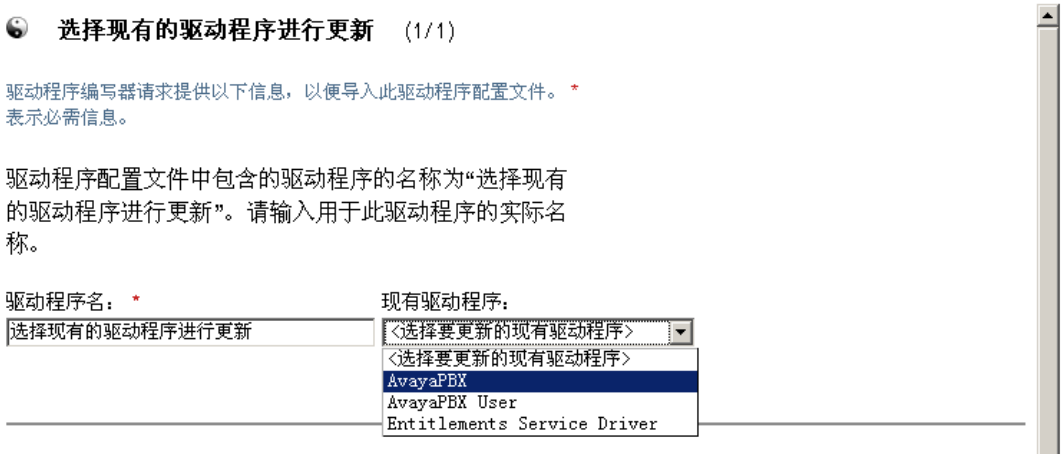
   请参见“准备使用 Identity Manager 口令同步和通用口令”在第 86 页。

   如果使用 DirXML® 1.1a，请参见“将驱动程序配置从 DirXML 1.1a 格式升级至 Identity Manager 格式”在第 21 页。
2. 在 iManager 中，单击 "Identity Manager 实用程序 ">" 导入驱动程序 "。
3. 选择现有的驱动程序所在的驱动程序集，然后单击 " 下一步 "。

4 在出现的驱动程序配置列表中，滚动到 *Additional Policies* （附加策略），然后仅选择 *Password Synchronization 2.0 Policies*"Password Synchronization 2.0 策略 "。

5 单击 " 下一步 "。

6 在 " 现有驱动程序 " 下拉列表中，选择要更新的现有驱动程序。



7 在 " 已连接系统 " 下拉列表中，选择已连接系统的类型。

如果驱动程序名称未出现在下拉列表中，则选择 " 其它系统 "。

根据驱动程序的类型， " 导入驱动程序向导 " 会将驱动程序清单中的项设置为指示驱动程序配置和已连接系统的功能：

- 已连接系统能否向 Identity Manager 提供口令。

此口令是指已连接系统上的用户实际口令，而不是使用样式表就可以创建的口令。只有 AD、 eDirectory 和 NIS 可以创建实际口令。

- 已连接系统能否接受来自 Identity Manager 的口令
- 已连接系统能否对口令进行检查，以确定它是否与 Identity Manager 中的口令相匹配。

驱动程序清单中的项必须正确，才能使口令同步策略正常工作。驱动程序清单指示已连接系统、 Identity Manager 驱动程序 Shim 和驱动程序配置策略的综合性能。通常情况下，网络管理员不应编辑这些内容。

8 单击 " 下一步 "。

9 如果没有要保存的驱动程序清单或 GCV 值，则选择 " 更新有关该驱动程序的所有方面 "。

此选项可提供口令同步所必需的驱动程序清单、全局配置值 (GCV) 以及 Identity Manager 策略。

驱动程序清单和 GCV 会重写已有的任何值。由于这些类型的驱动程序参数是 Identity Manager 2 中新增的，因此 DirXML 1.*x* 驱动程序应没有要被重写的现有值。

口令同步策略不重写任何现有策略对象。它们只是附加到驱动程序对象上。

注释 **:** 如果确实有要保存的驱动程序清单或 GCV 值，则选择 " 只更新该驱动程序中的选定策略 "，然后选中所有策略的复选框。此选项导入口令策略，但不更改驱动程序清单或 GCV。对于任何附加值，则需要手工粘贴。

---

10 单击 " 下一步 "，然后单击 " 完成 " 结束向导。

至此，新策略已创建为驱动程序对象下的策略对象，但它们仍不是驱动程序配置的一部分。若要将新策略链接到配置中，必须在订购者和发布者通道上，手工将每个新策略插入到驱动程序配置中的正确位置。

5.7.2 第 2 步：添加至驱动程序配置

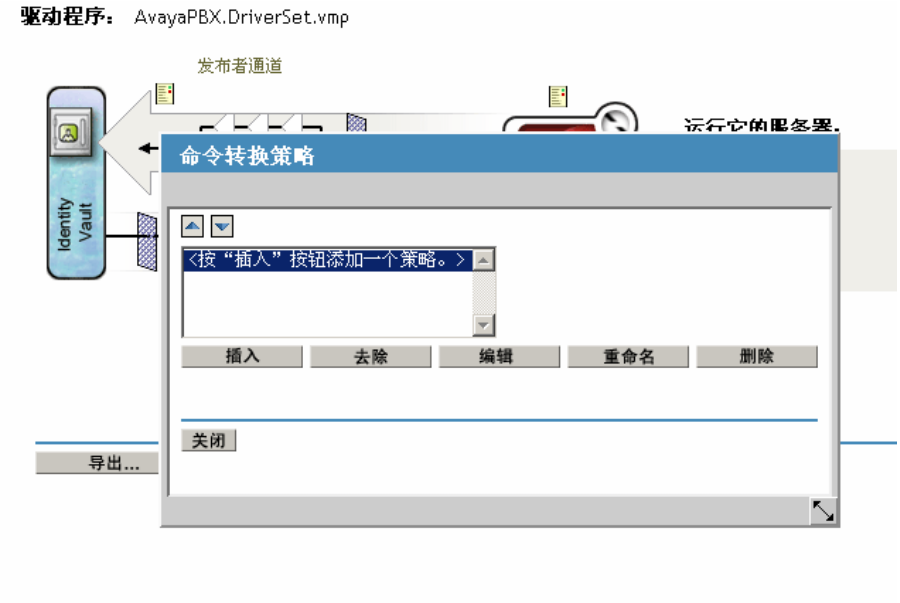
有关要添加的策略列表以及这些策略的插入位置，请参见 “驱动程序配置中所需的策略”在第 83 页 。

将每个新策略插入到现有驱动程序配置中的正确位置。

如果策略集包含多个策略，请确保最后列出 Identity Manager 口令同步策略。

对每个策略重复以下步骤。

1. 选择 *Identity Manager* >"Identity Manager 概述 "，然后搜索更新的驱动程序所在的驱动程序集。
2. 单击刚刚更新的驱动程序 （例如， AvayaPBX）。
3. 对需要添加一个新策略的位置，单击相应的图标 （例如，发布者通道上的命令转换策略）。



4 单击 " 插入 " 添加新策略。

5 单击 " 使用现有策略 "，浏览新策略对象，然后单击 " 确定 "。

6 如果对于任何新策略，列表中都有多个策略，请使用箭头按钮 将新策略移到列表中的正确位置。

请确保策略的顺序与 “驱动程序配置中所需的策略”在第 83 页 中列出的顺序相同。

5.7.3 第 3 步：更改过滤器设置

1 对于要同步口令的对象类 （如 User），请确保过滤器中包含 nspmDistributionPassword 特性，并且具有以下设置：

- 对于发布者通道，将过滤器的 *nspmDistributionPassword* 特性设置为 " 忽略 "。
- 对于订购者通道，将过滤器的 *nspmDistributionPassword* 特性设置为 " 通知 "。

若要查看特性，必须滚动并选择类 （例如， User），然后通过滚动浏览特性。

如果未列出 nspmDistributionPassword，请执行以下操作：

1a 确保已选择类，然后单击 " 添加特性 "。

1b 滚动至 nspmDistributionPassword 并选择它，然后单击 " 确定 "。

2 对于 *nspmDistributionPassword* 特性设置为 " 通知 " 的所有对象，请将公共密钥和私用密钥特性设置为 " 忽略 "。

3 对于要升级以加入口令同步的每个驱动程序，请重复步骤 2 在第 91 页 （在 " 将驱动程序转换为 Identity Manager 3 格式 " 中）到本节中的步骤 2 （" 更改过滤器设置 "）。

至此，驱动程序已具有新驱动程序 Shim、 Identity Manager 格式以及驱动程序配置支持口令同步所必需的其它要素：驱动程序清单、 GCV、口令同步策略和过滤器设置。

4 检查各个驱动程序实施指南中否有关于设置 Identity Manager 口令同步的其它步骤或信息。请参见 Identity Manager 驱动程序 (http://www.novell.com/documentation/lg/dirxmldrivers/index.html)。

5 通过创建启用了通用口令的口令策略，为用户启用通用口令。

请参见 《口令管理管理员指南》(http://www.novell.com/documentation/password_management/index.html) 中的 " 创建口令策略 "。如果之前在 NetWare 6.5 中使用过通用口令，则 《口令管理管理员指南》的 " （仅限 NetWare 6.5）重新创建通用口令指派 " 中还描述了一些额外的步骤。

建议在树中尽可能高的位置指派口令策略。

" 配置选项 " 页中提供了一些选项，可供您选择 NMAS 保持不同类型口令同步的方式。默认设置应适用于大多数实施。有关更多信息，请参见该页的联机帮助。

有关使用口令同步以及如何适应口令策略的方案，请参见 “实施口令同步”在第 98 页 。

NMAS 口令策略是以树为中心指派的。与此相反，口令同步是在每个驱动程序上分别设置的。驱动程序安装在每台服务器上，且只能管理主复本或读 / 写复本中的用户。

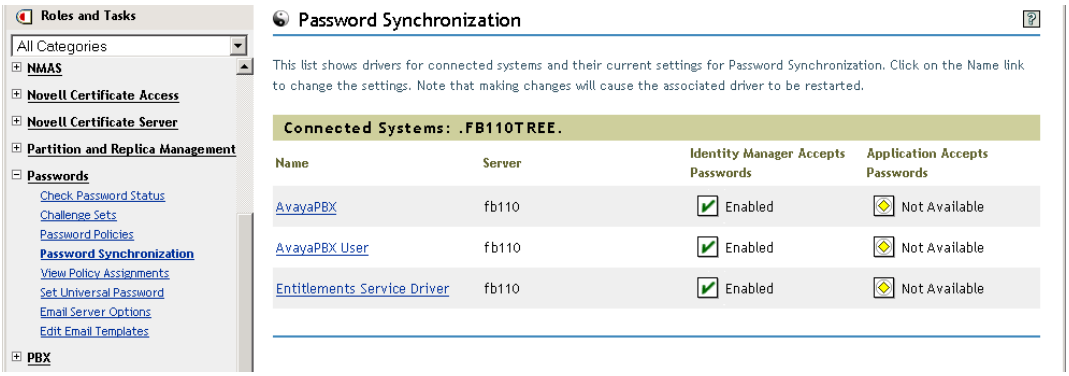
要获得预期的口令同步结果，请确保在要运行口令同步的驱动程序的服务器上，主复本或读 / 写复本中的树枝与已指派启用了通用口令的口令策略的树枝相匹配。将口令策略指派给分区根树枝可确保将此口令策略指派给树枝和子树枝中的所有用户。

5.7.4 第 4 步：设置口令同步流

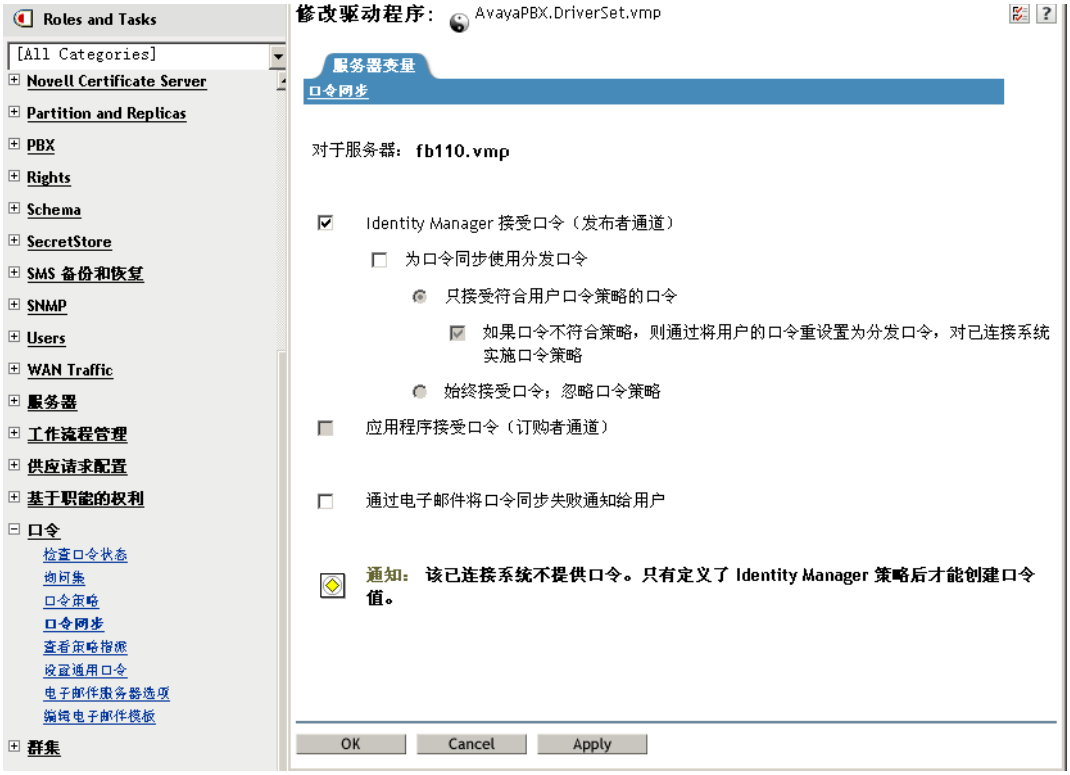
请确保按照所需的方式为每个已连接系统设置口令流。

1 在 iManager 中，选择 " 口令 ">" 口令同步 "。

2 在树或树枝中搜索要管理的已连接系统的驱动程序。



3 通过选择驱动程序来查看口令流的当前设置



此页列出了全局配置值 (GCV)。可通过选择适当的选项更改它们。

Identity Manager 控制项点 （Identity Manager 更新其口令）。NMAS 根据 " 配置选项 " 中设置的选项控制不同类型口令间的口令流 (步骤 3 在第 82 页 显示了 " 配置选项 " 页）。如果选择 " 为口令同步使用分发口令 "，则 Identity Manager 直接使用分发口令。如果取消选择此选项，则 Identity Manager 直接使用通用口令。

有关这些选项的信息 （包括插图），请参见 “实施口令同步”在第 98 页 。另请参见联机帮助。

4 测试口令同步。

确认 Identity Manager 口令已分发到所指定的系统。

确认指定的已连接系统是否正在向 Identity Manager 发布口令。

有关查错提示，请参见 “实施口令同步”在第 98 页 。

5.8 实施口令同步

Identity Manager 中提供的口令同步功能允许实施多种不同的方案。本节概述了一些基本方案，以帮助您了解 Identity Manager 口令同步和 NMAS 口令策略中的设置是如何影响口令同步的。可以使用其中的一个或多个方案，以满足环境的要求。

- “Identity Manager 与 NMAS 的关系概述”在第 99 页
- “方案 1：使用 NDS 口令在两个 Identity Vault 间进行同步”在第 100 页
- “方案 2：使用通用口令同步”在第 102 页

- “方案 3：通过 Identity Manager 更新分发口令同步 Identity Vault 和已连接系统”在第 111 页
- “方案 4：隧道通讯进程同步已连接系统而不是 Identity Vault，同时由 Identity Manager 更新分发口令”在第 120 页
- “方案 5：将应用程序口令与简单口令同步”在第 124 页

5.8.1 Identity Manager 与 NMAS 的关系概述

- “实用程序和 NMAS”在第 99 页
- “Identity Manager 和 NMAS”在第 99 页

实用程序和 NMAS

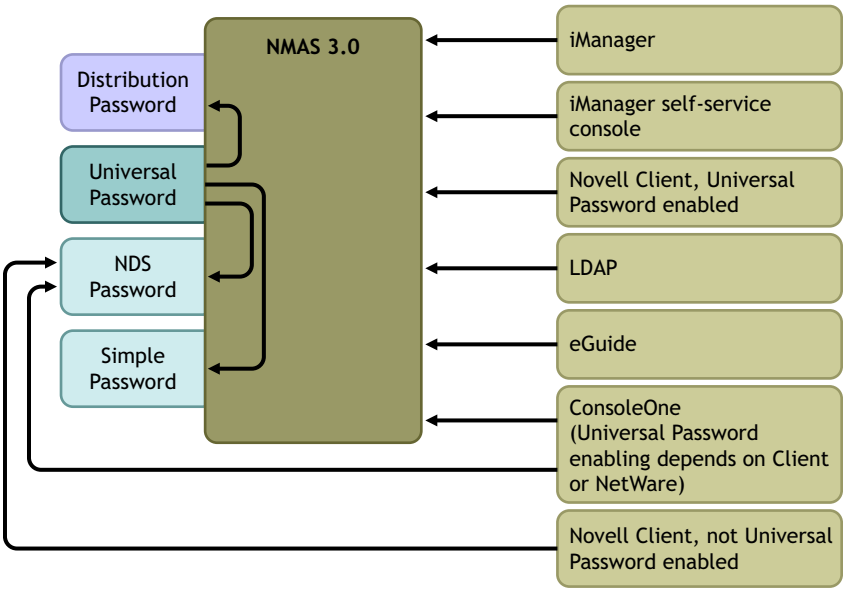
实用程序 （如 iManager 和 Novell Client）与 NMAS 进行通讯，而不是直接更新特定的口令。NMAS 是决定要更新的口令的实体。

NMAS 根据 NMAS 口令策略中的设置在 Identity Vault 中同步口令。

未启用通用口令的旧式实用程序直接更新 NDS 口令，而不是与 NMAS 进行通讯来让 NMAS 决定更新哪些口令。请注意用户和服务台管理员是如何在环境中使用旧式实用程序的。由于旧式实用程序不通过 NMAS 而直接更新 NDS 口令，因此，如果使用通用口令和 NMAS 2.3，则会出现口令偏移 （通用口令和 NDS 口令不同步）。

例如，要保证支持通用口令，请确保将用户升级为 Novell Client，并且服务台用户仅在最新的 Novell Client 或 NetWare 发行版上使用 ConsoleOne。

图 *5-5* 使用 *NMAS* 同步口令



Identity Manager 和 NMAS

Identity Manager 控制 " 项点 " （直接更新通用口令或分发口令）。NMAS 控制 Identity Vault 内部的同步口令流。

在方案 1 中， Identity Manager Driver for eDirectory 可用于直接更新 NDS 口令。此方案与 DirXML 1.*x* 中提供的方案基本相同。

在方案 2、方案 3 和方案 4 中， Identity Manager 用于更新通用口令或分发口令。Identity Manager 通过 NMAS 更改口令。这允许 NMAS 根据 NMAS 口令策略设置更新其它 Identity Vault 口令，还允许 NMAS 对与已连接系统进行同步的口令实施 NMAS 口令策略中的高级口令规则。在这些方案中， Identity Manager 分发给已连接系统的口令始终是分发口令。

方案 2、方案 3 和方案 4 的不同之处在于，它们对每个已连接系统驱动程序使用不同的 NMAS 口令策略设置和 Identity Manager 口令同步设置组合。

5.8.2 方案 1：使用 NDS 口令在两个 Identity Vault 间进行同步

同 Password Synchronization 1.0 一样，可以通过使用 eDirectory 驱动程序在两个 Identity Vault 间同步 NDS 口令。此方案不需要实施通用口令，可用于 eDirectory 8.6.2 或更高版本。此类型口令同步的另一名称是同步公共 / 私用密钥对。

此方法仅适用于在 Identity Vault 之间同步口令。它不使用 NMAS，因此无法用于同步已连接应用程序的口令。

- “方案 1 的优点和缺点”在第 100 页
- “设置方案 1”在第 101 页
- “对方案 1 查错”在第 102 页

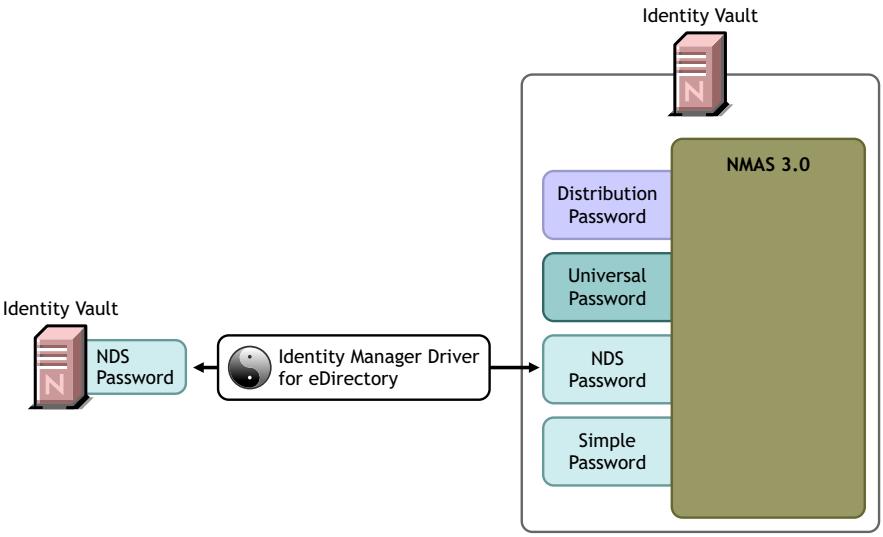
方案 **1** 的优点和缺点

表 ***5-11*** 优点：使用 *NDS* 口令实施 *eDirectory* 到 *eDirectory* 口令同步

优点	缺点
配置简单。只需在驱动程序过滤器中包含正确的特性。 如果要分阶段部署 Identity Manager 3 和 eDirectory 8.7.3，则此方法可帮助您循序部署。 ◆ 无需向驱动程序配置中添加新口令同步策略。 ◆ 无需在 Identity Vault 中实施通用口令。 ◆ 可用于运行 eDirectory 8.6.2 或更高版本的已连接 Identity Vault。 ◆ 无需使用 NMAS 2.3。 实施可为 NDS 口令设置的基本口令限制。	此方法可在 Identity Vault 之间同步口令。但不能同步其它已连接系统的口令。 不更新通用口令或分发口令。 由于此方法不使用 NMAS，因此无法验证来自另一 Identity Vault 的口令是否违反了口令策略中的高级口令规则。 由于此方法不使用 NMAS，因此如果口令与 NMAS 口令策略不符，则无法重设置已连接 Identity Vault 中的口令。 口令同步失败时，不提供电子邮件通知。 不支持在 iManager 任务中的检查口令状态操作（此功能需要使用分发口令）。

下图表明，与 DirXML 1.*x* 一样， Identity Manager Driver for eDirectory 也可用于同步两个 Identity Vault 间的 NDS 口令。此方案不通过 NMAS 操作。

图 ***5-6*** 使用 *NDS* 口令在两个 *Identity Vault* 间进行同步



设置方案 **1**

若要设置此类型的口令同步，需配置驱动程序。

通用口令部署

非必需。

口令策略配置

无。

口令同步设置

无。驱动程序 " 口令同步 " 页中的设置对此 NDS 口令同步方法没有影响。

驱动程序配置

去除 “驱动程序配置中所需的策略”在第 83 页 中列出的口令同步策略。这些策略旨在支持通用口令和分发口令。同步 NDS 口令时，将使用公共密钥和私用密钥特性，而不使用这些策略。

请确保，对于应同步口令的所有对象类，两个 Identity Vault 驱动程序的驱动程序过滤器正在同步其公共密钥和私用密钥特性。下图是一个示例。

图 *5-7* 同步私用密钥和公共密钥特性

对方案 **1** 查错

- 启用 DSTrace 选项。
- 检查驱动程序过滤器，确保公共密钥和私用密钥特性已同步，未被忽略。
- 另请参见 “查错口令同步”在第 142 页 中的提示。

5.8.3 方案 2：使用通用口令同步

使用 Identity Manager，可将已连接系统的口令与 Identity Vault 中的通用口令同步。

更新通用口令时，也会根据 NMAS 口令策略中的设置更新 NDS 口令、分发口令或简单口令。

任何已连接系统都可以向 Identity Manager 发布口令，但并非所有已连接系统都可以提供用户的实际口令。例如， Active Directory 可以向 Identity Manager 发布用户的实际口令。虽然 PeopleSoft 不从 PeopleSoft 系统自身提供口令，但它可以提供驱动程序配置策略中创建的初始口令，如基于用户的员工 ID 或姓的口令。并非所有驱动程序都可以订购 Identity Manager 中的口令更改。请参见 “已连接系统支持口令同步”在第 77 页 。

- “方案 2 的优点和缺点”在第 103 页
- “设置方案 2”在第 104 页
- “对方案 2 查错”在第 108 页

方案 2 的优点和缺点

表 *5-12* 优点：使用通用口令同步

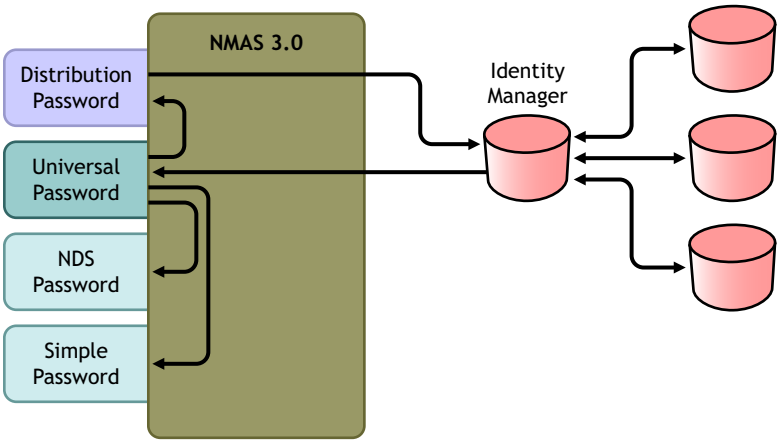
优点	缺点
允许在 Identity Vault 和已连接系统间同步口令。 允许验证口令是否违反了 NMAS 口令策略。 允许在口令操作失败（例如，来自已连接系统的口令与 " 口令 " 不符）时发送电子邮件通知。 如果要同步通用口令和分发口令，并且已连接系统支持口令检查，则此方案支持在 iManager 中执行检查口令状态任务。 如果已启用口令策略中的高级口令规则，则 NMAS 将实施这些规则。如果来自已连接系统的口令不符合这些规则，则会生成错误并发送电子邮件通知（前提是已指定此选项）。 如果不希望实施口令策略，则可以取消选择 NMAS 口令策略中的 " 启用高级口令规则 "。	从设计上讲，此方案不支持重设置已连接系统中的口令，原因是根据口令策略中的设置，分发口令和通用口令可能并不相同。

此方案的流程图如下：

1. 口令经 Identity Manager 进入。
2. Identity Manager 通过 NMAS 直接更新通用口令。
3. NMAS 根据 NMAS 口令策略设置，使用分发口令和其它口令同步通用口令。
4. Identity Manager 检索分发口令以向设置为接受口令的已连接系统分发口令。

在此图中，虽然多个已连接系统显示为同时与 Identity Manager 相连，但请记住，应单独为每个已连接系统的驱动程序创建设置。

图 *5-8* 使用通用口令同步口令



设置方案 **2**

设置此类型的口令同步：

- “通用口令部署”在第 104 页
- “口令策略配置”在第 104 页
- “口令同步设置”在第 105 页
- “驱动程序配置”在第 107 页

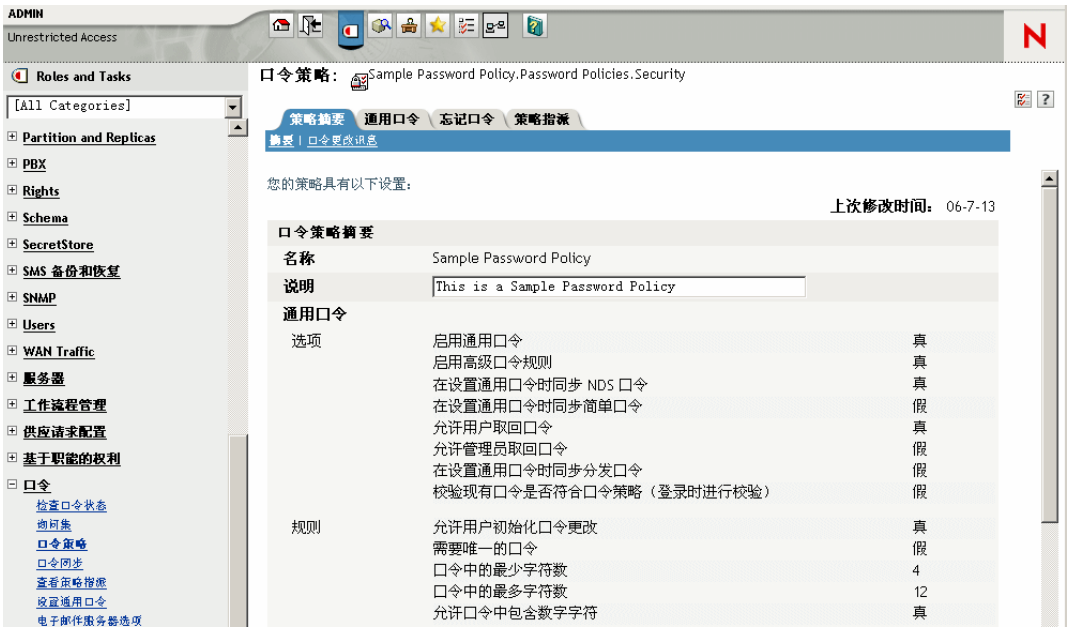
通用口令部署

请确保环境已就绪，可使用通用口令。请参见 “准备使用 Identity Manager 口令同步和通用口令”在第 86 页 。

口令策略配置

请确保已向要进行此种口令同步的 Identity Vault 部分指派了 NMAS 口令策略。

1. 在 iManager 中，选择 " 口令 ">" 口令策略 "。
2. 选择一个策略，然后单击 " 编辑 "。
3. 浏览并选择您希望发生口令同步的对象。



可以将策略指派给整个树结构 （方法是浏览并选择 " 安全性 " 树枝中的 " 登录策略 " 对象）、分区根树枝、树枝或特定用户。为简化管理，建议在树中尽可能高的位置指派口令策略。

4 在口令策略中，确保已选中以下选项：

- 启用通用口令
- 设置通用口令时，同步 *NDS* 口令
- 在设置通用口令时同步分发口令

  由于 Identity Manager 检索分发口令以向已连接系统分发口令，因此必须选中此选项，才能允许口令双向同步。

5 根据需要完成口令策略。

如果已启用口令策略中的高级口令规则，则 NMAS 将实施这些规则。如果不希望实施口令策略规则，请取消选择 " 启用高级口令规则 "。

如果使用高级口令规则，请确保它们不与任何要订购口令的已连接系统中的口令策略冲突。

口令同步设置

1 在 iManager 中，选择 " 口令 ">" 口令同步 "。

2 搜索已连接系统的驱动程序，然后选择驱动程序。

3 为已连接系统的驱动程序创建设置。

请确保已选中以下选项：

- *Identity Manager* 接受口令 （发布者通道）

  如果驱动程序清单不包含 " 口令发布 " 功能，则页面中将显示一条讯息。这是在通知用户：无法从应用程序检索口令，并且仅能通过使用策略在驱动程序配置中创建口令来发布口令。

- 应用程序接受口令 （订购者通道）

  如果已连接系统不支持接受口令，则此选项将被禁用。

如果已连接系统支持口令双向同步，则这些设置将允许执行口令双向同步。

可以调整设置，使之与口令的权威来源的业务策略相匹配。例如，如果已连接系统订购口令但不发布口令，则应只选择 " 应用程序接受口令 （订购者通道） "。

4 请确保未选中 " 为口令同步使用分发口令 "：

在此方案中， Identity Manager 直接更新通用口令。分发口令仍用于向已连接系统分发口令，但将由 NMAS 而不是 Identity Manager 从通用口令更新分发口令。

5 （可选）根据需要选择以下选项：

- 通过电子邮件将口令同步失败通知给用户

  请记住，电子邮件通知需要填充 eDirectory 用户对象的因特网电子邮件地址特性。

  电子邮件通知是非侵害性的。它们并不影响触发电子邮件的 XML 文档的处理。如果电子邮件通知失败，则除非重试操作本身，否则不会重试发送通知。但是，电子邮件通知的调试讯息会写入跟踪文件。

1 对于要加入口令同步的每个驱动程序，请确保其驱动程序配置中包括了所需的 Identity Manager 底稿口令同步策略。

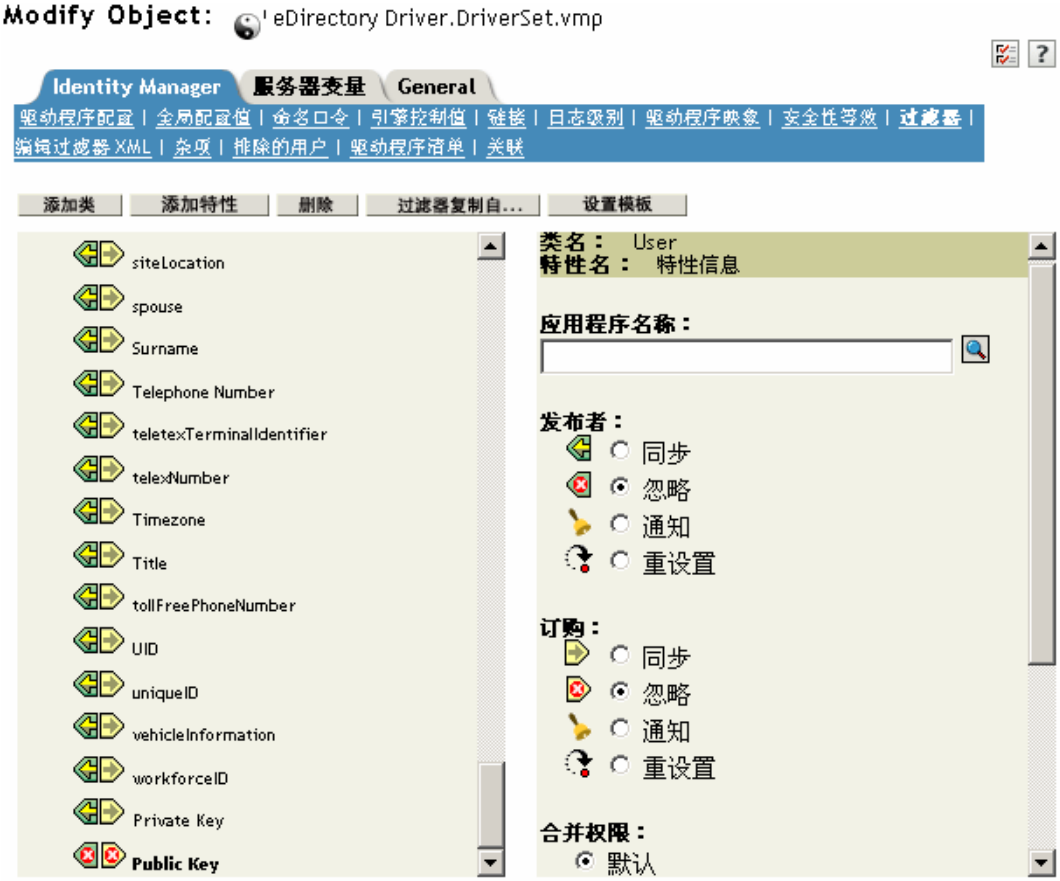
这些策略在驱动程序配置中的位置和顺序必须正确。有关策略列表，请参见 “驱动程序配置中所需的策略”在第 83 页 。

Identity Manager 样本配置已包含这些策略。如果要升级现有的驱动程序，则可以按照 “升级现有驱动程序配置以支持口令同步”在第 90 页 中的指导来添加策略。

2 正确设置 nspmDistributionPassword 特性的过滤器：

- 在发布者通道中，对于所有对象类的 nspmDistributionPassword 特性，将驱动程序过滤器设置为 " 忽略 "。
- 在订购者通道中，对于要订购口令更改的所有对象类的 nspmDistributionPassword 特性，将驱动程序过滤器设置为 " 通知 "。

3 对于 nspmDistributionPassword 特性设置为 " 通知 " 的所有对象，请将其公共密钥和私用密钥特性设置为 " 忽略 "。



4 为保证口令安全性，请确保您可以控制谁具有 Identity Manager 对象的权限。

对方案 **2** 查错

- “方案 2 的流程图”在第 108 页
- “登录到 Identity Vault 时出现问题”在第 110 页
- “登录到另一个用于订购口令的已连接系统时出现问题”在第 110 页
- “口令失败时不生成电子邮件”在第 111 页
- “使用检查对象口令时出现错误”在第 111 页
- “有用的 DSTrace 命令”在第 111 页

另请参见 “查错口令同步”在第 142 页 中的提示。

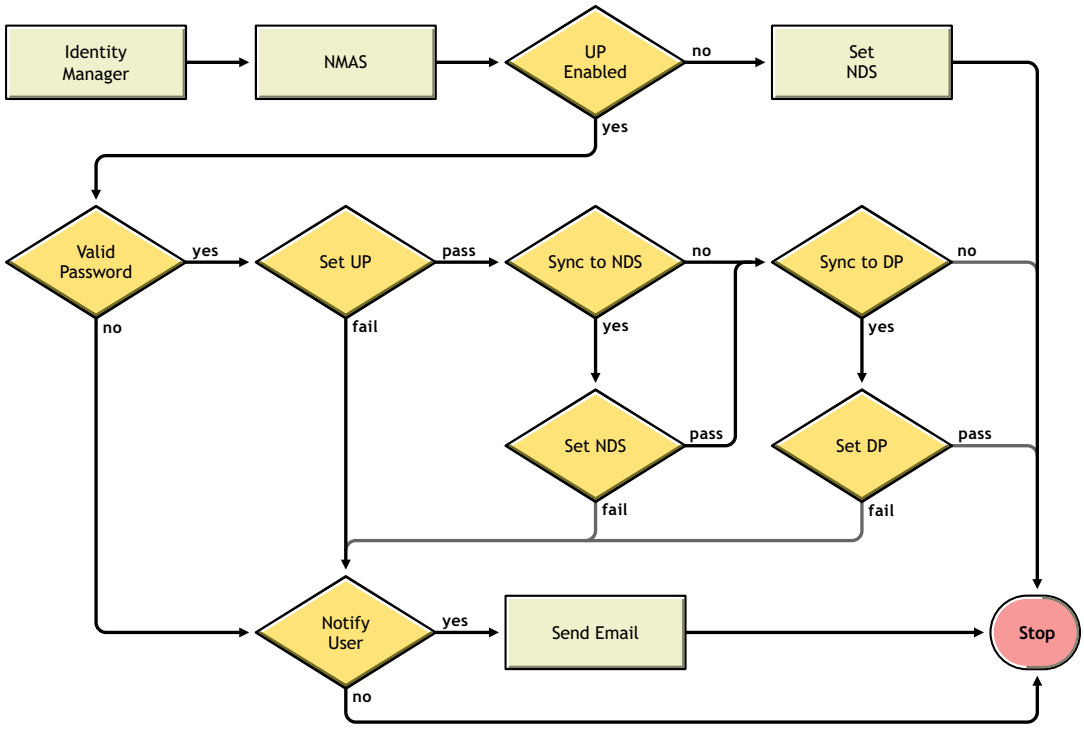
方案 2 的流程图

以下流程图阐释 NMAS 如何处理它从 Identity Manager 接收到的口令。在此方案中，此口令与通用口令同步。NMAS 根据以下设置来决定如何处理此口令：

- NMAS 口令策略中是否已启用通用口令。
- 是否已启用进来的口令必须符合的高级口令规则。

- 用于同步通用口令与其它口令的口令策略中还有哪些其它设置。

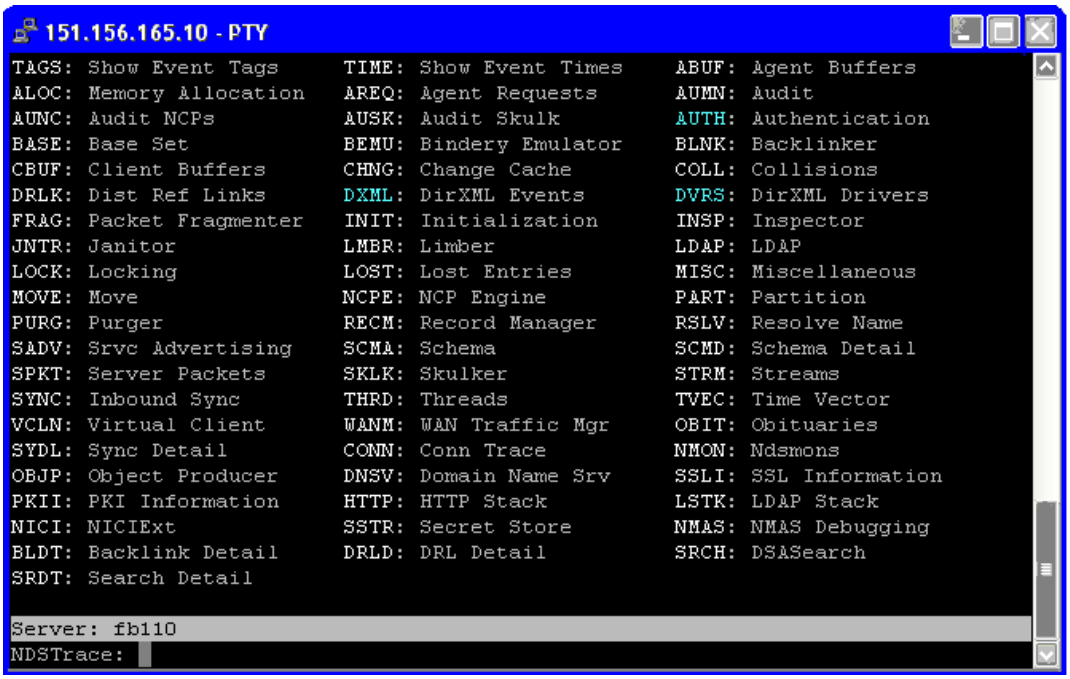
图 **5-9** *NMAS* 如何处理它从 *Identity Manager* 接收到的口令



登录到 Identity Vault 时出现问题

- 启用 DSTrace 中的 *+AUTH*、 *+DXML* 和 *+DVRS* 设置。

图 ***5-10*** *DSTrace 命令*



- 校验是否正在向 Identity Manager 传递 <password> 或 <modify-password> 要素。若要校验是否正在传递它们，请观察已启用这些选项的跟踪屏幕。
- 根据口令策略的规则校验口令是否有效。
- 检查 NMAS 口令策略配置和指派。尝试将策略直接指派给某一用户，以确保使用了正确的策略。
- 在驱动程序的 " 口令同步 " 页中，请确保已选中 "DirXML 接受口令 "。
- 在口令策略中，请确保已选中 " 在设置通用口令时同步分发口令 "。

登录到另一个用于订购口令的已连接系统时出现问题

本节旨在对案例查错，在这些案例中，该已连接系统正在向 Identity Manager 发布口令，但要订购口令的另一已连接系统似乎没有接收到该系统的更改。这一关系又称为次已连接系统，意思是它通过 Identity Manager 接收来自第一个已连接系统的口令。

- 启用 DSTrace 中的 *+DXML* 和 *+DVRS* 设置以查看 Identity Manager 规则处理
- 将驱动程序的 Identity Manager 跟踪级别设置为 *3*。
- 请确保已选中口令同步的 "Identity Manager 接受口令 " 选项。
- 检查驱动程序过滤器，确保已按步骤 2 在第 107 页 中所述正确设置了 nspmDistributionPassword 特性。
- 校验用于添加操作的 < 口令 > 或 <modify-password> 要素是否正发送至已连接系统。若要进行校验，请观察已启用跟踪选项 （如第一批项目中所述）的 DSTrace 屏幕或文件。

- 校验驱动程序配置中包括的 Identity Manager 底稿口令策略是否处于正确的位置和顺序，详情请见 “驱动程序配置中所需的策略”在第 83 页 。
- 将 Identity Vault 中的 NMAS 口令策略与已连接系统实施的任何口令策略进行比较，确保它们相互兼容。

口令失败时不生成电子邮件

- 启用 DSTrace 中的 *+DXML* 设置，以查看 Identity Manager 规则处理。
- 将驱动程序的 Identity Manager 跟踪级别设置为 *3*。
- 校验是否已选择生成电子邮件的规则。
- 校验 Identity Vault 对象在因特网电子邮件地址特性中是否包含正确的用户电子邮件地址。
- 在通知配置任务中，请确保已正确配置 SMTP 服务器和电子邮件模板。请参见 “配置电子邮件通知”在第 131 页 。

使用检查对象口令时出现错误

iManager 中的检查口令状态任务会引起驱动程序执行检查对象口令的操作。如果出现问题，请审阅以下内容：

- 如果 " 检查对象口令 " 返回 -603，则说明 Identity Vault 对象不包含 nspmDistributionPassword 特性。检查驱动程序过滤器的 nspmDistributionPassword 特性的设置是否正确。另外，请确保已选中 " 在设置通用口令时同步分发口令 " 口令策略。
- 如果 " 检查对象口令 " 返回 Not Synchronized，请校验驱动程序配置是否包含适当的口令同步策略。
- 将 Identity Vault 中的 NMAS 口令策略与已连接系统实施的任何口令策略进行比较，确保它们相互兼容。
- 从分发口令执行检查对象口令操作。如果分发口令未进行更新，则"检查对象口令"可能不会报告口令已同步。
- 请记住，仅对于 Identity Manager 驱动程序，" 检查口令状态 " 才会检查 NDS 口令，而不是检查分发口令。

有用的 DSTrace 命令

+DXML：用于查看 Identity Manager 规则处理和潜在的错误讯息

+DVRS：用于查看 Identity Manager 驱动程序讯息

+AUTH：用于查看 NDS 口令修改

5.8.4 方案 3：通过 Identity Manager 更新分发口令同步 Identity Vault 和已连接系统

在此方案中， Identity Manager 直接更新分发口令，并且允许 NMAS 决定如何同步其它 Identity Vault 口令。

任何已连接系统都可以向 Identity Manager 发布口令，但并非所有已连接系统都可以提供用户的实际口令。例如， Active Directory 可以向 Identity Manager 发布用户的实际口令。虽然 PeopleSoft 不从 PeopleSoft 系统自身提供口令，但它可以提供驱动程序配置策略中创建的初

始口令，如基于用户的员工 ID 或姓的口令。并非所有驱动程序都可以订购 Identity Manager 中的口令更改。请参见 “已连接系统支持口令同步”在第 77 页。

- “方案 3 的优点和缺点”在第 112 页
- “设置方案 3”在第 113 页
- “对方案 3 查错”在第 116 页

方案 3 的优点和缺点

表 *5-13* 优点：通过更新分发口令同步 *Identity Vault* 和已连接系统

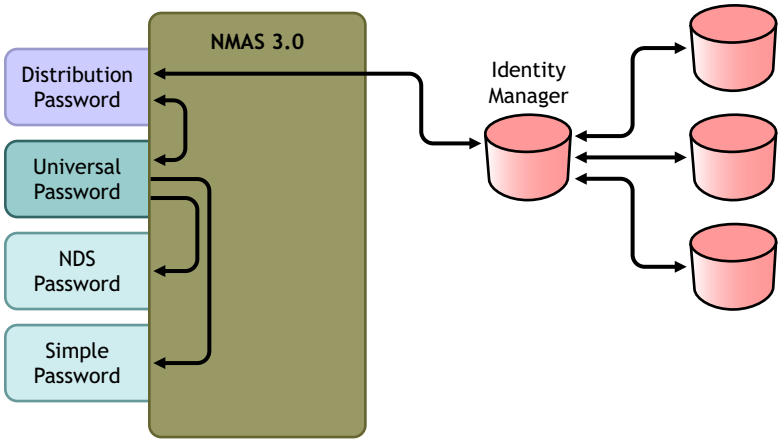
优点	缺点
允许在 Identity Vault 和已连接系统间同步口令。 允许选择是否对来自已连接系统的口令实施口令策略。 可以指定在口令同步失败时发送通知。 如果要实施口令策略，但口令不符合策略规则，则可以选择将已连接系统的口令重设置为分发口令。	

此方案的流程图如下：

1. 口令经 Identity Manager 进入。
2. Identity Manager 通过 NMAS 直接更新分发口令
3. Identity Manager 还使用分发口令向已指定为接受口令的已连接系统分发
4. NMAS 根据口令策略设置，使用分发口令和其它口令同步通用口令。

在此图中，虽然多个已连接系统显示为同时与 Identity Manager 相连，但请记住，应单独为每个已连接系统的驱动程序创建设置。

图 *5-11* 通过更新分发口令同步 *Identity Vault* 和已连接系统



设置方案 **3**

设置此类型的口令同步：

- “通用口令部署”在第 113 页
- “口令策略配置”在第 113 页
- “口令同步设置”在第 114 页
- “驱动程序配置”在第 115 页

通用口令部署

请确保环境已就绪，可使用通用口令。请参见 “准备使用 Identity Manager 口令同步和通用口令”在第 86 页 。

口令策略配置

1. 在 iManager 中，选择 " 口令 ">" 口令策略 "。
2. 请确保已向要进行此种口令同步的 Identity Vault 树部分指派了口令策略。该策略可以指派给整个树结构、分区根树枝、树枝或特定的用户。为简化管理，建议在树中尽可能高的位置指派口令策略。
3. 在口令策略中，请确保已选中以下选项：

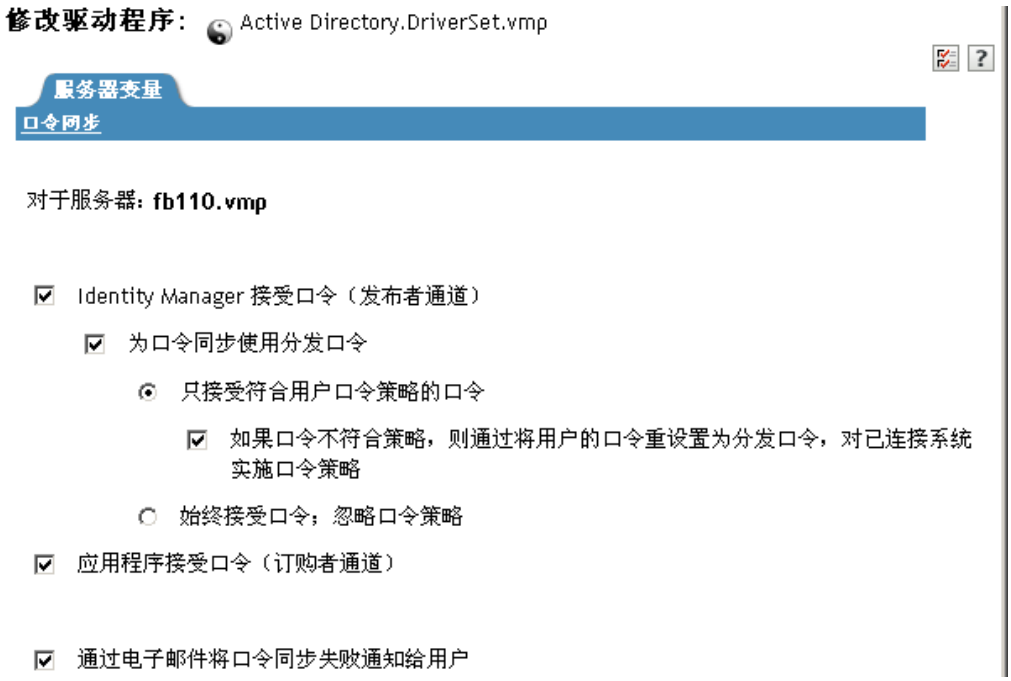
   - 启用通用口令
   - 设置通用口令时，同步 *NDS* 口令
   - 在设置通用口令时同步分发口令

     由于 Identity Manager 检索分发口令以向已连接系统分发口令，因此必须选中此选项，才能允许口令双向同步。

4 如果使用高级口令规则，请确保它们不与要订购口令的任何已连接系统上的口令策略冲突。

口令同步设置

1 在 iManager 中，选择 " 口令 ">" 口令同步 "。
2 搜索已连接系统的驱动程序，然后选择驱动程序。
3 为已连接系统的驱动程序创建设置。



请确保已选中以下选项：

- *Identity Manager* 接受口令 （发布者通道）
- 为口令同步使用分发口令

  如果驱动程序清单不包含 " 口令发布 " 功能，则页面中将显示一条讯息。这是在通知用户无法从应用程序检索口令，并且只能通过使用策略在驱动程序配置中创建口令来发布口令。
- 应用程序接受口令 （订购者通道）

如果已连接系统支持口令双向同步，则这些设置将允许执行口令双向同步。

可以调整设置，使之与口令的权威来源的业务策略相匹配。例如，如果已连接系统订购口令但不发布口令，则应只选择 " 应用程序接受口令 （订购者通道） "。

4 使用 " 为口令同步使用分发口令 " 下的选项，指定是要实施还是要忽略 NMAS 口令策略。
5 （条件）如果已指定要实施的口令策略，则还应指定当已连接系统口令不符合这些策略时，是否希望 Identity Manager 重设置该口令。
6 （可选）根据需要选择以下选项：

- 通过电子邮件将口令同步失败通知给用户

  请记住，电子邮件通知需要填充 eDirectory 用户对象的因特网电子邮件地址特性。

电子邮件通知是非侵害性的。它们并不影响触发电子邮件的 XML 文档的处理。如果电子邮件通知失败，则除非重试操作本身，否则不会重试发送通知。但是，电子邮件通知的调试讯息会写入跟踪文件。

驱动程序配置

1 对于要加入口令同步的每个驱动程序，请确保其驱动程序配置中包括了所需的 Identity Manager 底稿口令同步策略。

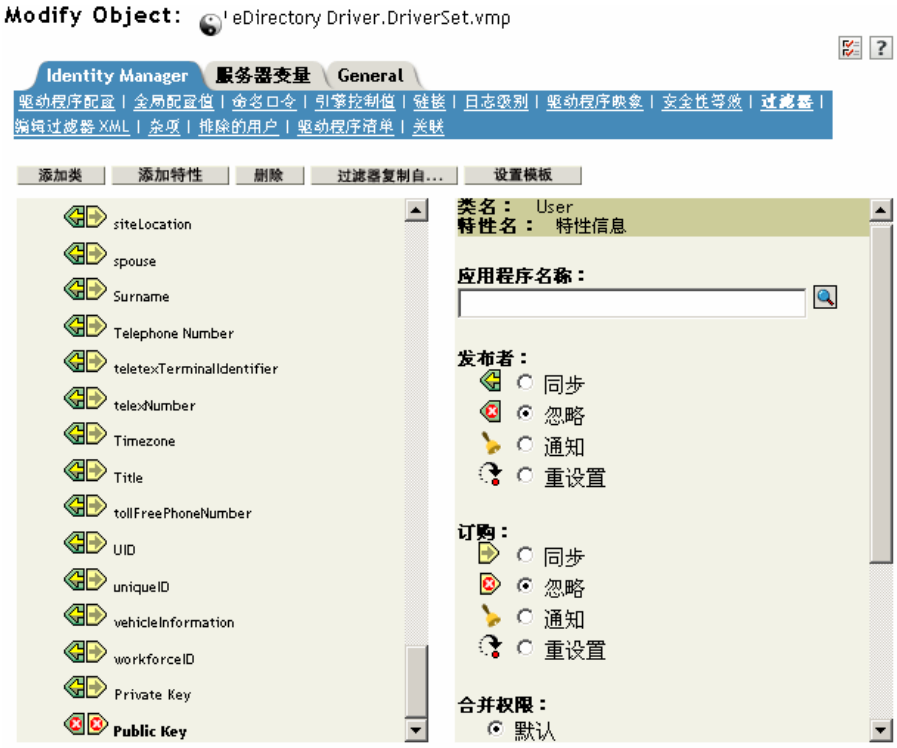
这些策略在驱动程序配置中的位置和顺序必须正确。有关策略列表，请参见 “驱动程序配置中所需的策略”在第 83 页。

Identity Manager 样本配置已包含这些策略。如果要升级现有的驱动程序，则可以按照 “升级现有驱动程序配置以支持口令同步”在第 90 页 中的指导来添加策略。

2 正确设置 nspmDistributionPassword 特性的过滤器：

- 在发布者通道中，对于所有对象类的 nspmDistributionPassword 特性，将驱动程序过滤器设置为 " 忽略 "。
- 在订购者通道中，对于要订购口令更改的所有对象类的 nspmDistributionPassword 特性，将驱动程序过滤器设置为 " 通知 "。

3 对于 nspmDistributionPassword 特性设置为 " 通知 " 的所有对象，请将驱动程序过滤器中的公共密钥和私用密钥特性设置为 " 忽略 "。



4 为保证口令安全性，请确保您可以控制谁具有 Identity Manager 对象的权限。

对方案 3 查错

- “方案 3 的流程图”在第 116 页
- “登录到 eDirectory 中时发生问题”在第 118 页
- “登录到订购口令的其它已连接系统时出现问题”在第 119 页
- “口令失败时不生成电子邮件”在第 119 页
- “使用 " 检查口令状态 " 时出错”在第 119 页
- “有用的 DSTrace 命令”在第 120 页

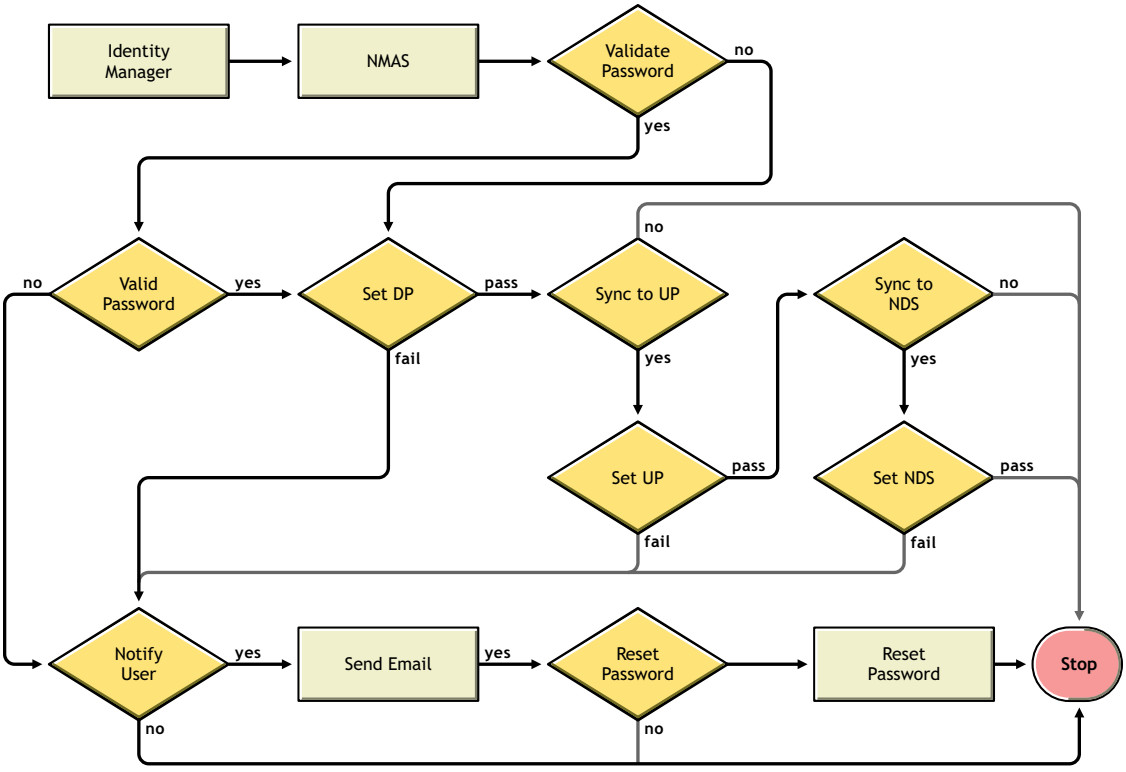
另请参见 “查错口令同步”在第 142 页 中的提示。

方案 3 的流程图

以下流程图阐释 NMAS 如何处理它从 Identity Manager 接收到的口令。在此方案中，此口令将与分发口令同步，并由 NMAS 决定以下内容：

- 如何处理口令，这将基于您是否已指定根据口令策略规则来验证进来的口令 （如果已启用通用口令和高级口令规则）。
- 用于同步通用口令与其它口令的口令策略中还有哪些其它设置。

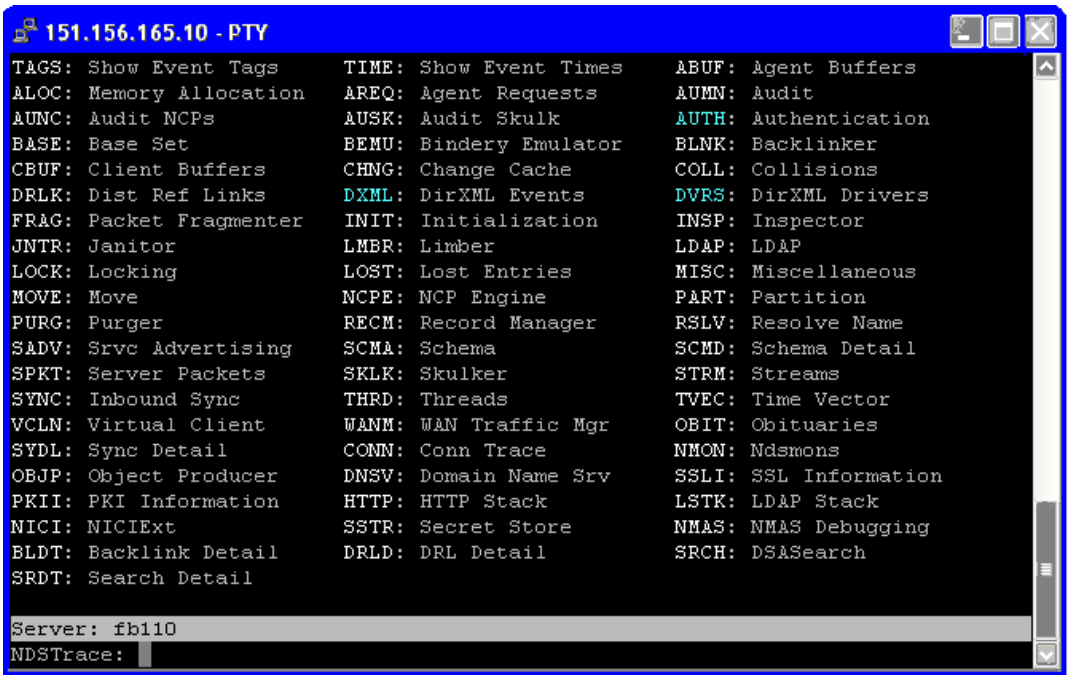
图 **5-12** 将 *Identity Manager* 中的口令与分发口令同步



登录到 eDirectory 中时发生问题

- 启用 DSTrace 中的 *+AUTH*、 *+DXML* 和 *+DVRS* 设置

图 ***5-13*** *DSTrace 命令*



- 校验是否正在向 Identity Manager 传递 <password> 或 <modify-password> 要素。为此，请使用上述第一项设置启用跟踪选项，然后观察 DSTrace 屏幕或文件。
- 根据 NMAS 口令策略规则校验口令是否有效。
- 检查 NMAS 口令策略配置和指派。尝试将策略直接指派给用户，以确保使用了正确的策略。
- 在驱动程序的 " 口令同步 " 页上，请确保已选中 "Identity Manager 接受口令 （发布者通道） "。
- 在 NMAS 口令策略中，请确保已选中 " 在设置通用口令时同步分发口令 "。
- 在 NMAS 口令策略中，请确保已选中 " 设置通用口令时同步 NDS 口令 "（如果需要）。
- 如果用户通过 Novell Client 或 ConsoleOne 登录，请检查其版本。如果通用口令未与 NDS 口令同步，则遗留的 Novell Client 和 ConsoleOne 可能无法登录到 Identity Vault 中。

  兼容通用口令的 Novell Client 和 ConsoleOne 的版本可用。请参见 《*NMAS 3.0* 管理指南》(http://www.novell.com/documentation/nmas30/index.html)。
- 某些遗留的实用程序使用 NDS 口令进行鉴定，如果通用口令未与 NDS 口令同步，则它们也无法登录到 Identity Vault 中。如果您不希望对大多数用户使用 NDS 口令，但有些管理员和服务台用户需要用遗留实用程序进行鉴定，请尝试为服务台用户使用不同的口令策略，以便为他们指定不同的通用口令同步选项。

登录到订购口令的其它已连接系统时出现问题

本节旨在对以下情况进行查错：该已连接系统正在向 Identity Manager 发布口令，但要订购口令的另一已连接系统似乎没有接收该系统的更改。这一关系又称为次已连接系统，意思是它通过 Identity Manager 接收来自第一个已连接系统的口令。

- 启用 DSTrace 中的 *+DXML* 和 *+DVRS* 设置以查看 Identity Manager 规则处理和潜在错误
- 将驱动程序的 Identity Manager 跟踪级别设置为 *3*。
- 请确保已选中 " 口令同步 " 页上的 "Identity Manager 接受口令 （发布者通道） " 选项。
- 在口令策略中，请确保未选中 " 在设置通用口令时同步分发口令 "。

  Identity Manager 使用分发口令同步已连接系统的口令。使用此同步方法时，通用口令必须与分发口令同步。
- 检查驱动程序过滤器的 nspmDistributionPassword 特性。
- 校验添加或 <modify-password> 要素的 <password> 要素是否已转换为 nspmDistributionPassword 的添加或修改特性操作。为此，请使用上述第一项设置启用相应选项，然后观察 DSTrace 屏幕或文件。
- 校验驱动程序配置中包括的 Identity Manager 底稿口令策略是否处于正确的位置和顺序，详情请见 “驱动程序配置中所需的策略”在第 83 页 。
- 将 Identity Vault 中的口令策略与已连接系统实施的任何口令策略进行比较，确保它们相互兼容。

口令失败时不生成电子邮件

- 启用 DSTrace 中的 *+DXML* 设置以查看 Identity Manager 规则处理
- 将驱动程序的 Identity Manager 跟踪级别设置为 *3*。
- 校验是否已选择生成电子邮件的规则。
- 校验 Identity Vault 对象的因特网电子邮件地址特性中是否包含正确的值。
- 在通知配置任务中，请确保已配置 SMTP 服务器和电子邮件模板。请参见 “配置电子邮件通知”在第 131 页 。

电子邮件通知是非侵害性的。它们并不影响触发电子邮件的 XML 文档的处理。如果电子邮件通知失败，则除非重试操作本身，否则不会重试发送通知。电子邮件通知的调试讯息将写入跟踪文件。

使用 " 检查口令状态 " 时出错

iManager 中的检查口令状态任务可导致驱动程序执行检查对象口令的操作。

- 请确保已连接系统支持口令检查。请参见 “已连接系统支持口令同步”在第 77 页 。

  如果驱动程序清单未指示已连接系统是否支持口令检查功能，则无法通过 iManager 执行此操作。
- 如果 " 检查对象口令 " 返回 -603，则说明 Identity Vault 对象不包含 nspmDistributionPassword 特性。检查驱动程序过滤器以及口令策略中的 *Synchronize Universal to Distribution* （将通用与分发同步）选项。
- 如果检查对象口令操作返回 Not Synchronized，请校验驱动程序配置是否包含适当的 Identity Manager 口令同步策略。

- 将 Identity Vault 中的口令策略与已连接系统实施的任何口令策略进行比较，确保它们相互兼容。
- "检查对象口令"检查分发口令。如果未更新分发口令，则"检查对象口令"可能会不报告口令已同步
- 请记住，对于 Identity Vault，" 检查口令状态 " 检查的是 NDS 口令而不是通用口令。这意味着，如果用户的口令策略未指定将 NDS 口令与通用口令同步，则始终报告未同步口令。而实际上，分发口令和已连接系统上的口令可能是同步的，但如果 NDS 口令和分发口令与通用口令不同步，则 " 检查口令状态 " 将不会报告准确的结果。

有用的 DSTrace 命令

+DXML：用于查看 Identity Manager 规则处理情况和潜在的错误讯息。

+DVRS：用于查看 Identity Manager 驱动程序讯息

+AUTH：：用于查看 NDS 口令修改

5.8.5 方案 4：隧道通讯进程同步已连接系统而不是 Identity Vault，同时由 Identity Manager 更新分发口令

Identity Manager 允许您同步已连接系统间的口令，同时将 Identity Vault 口令保持独立。这称为 " 隧道通讯进程 "。

在此方案中， Identity Manager 直接更新分发口令。此方案几乎与 “方案 3：通过 Identity Manager 更新分发口令同步 Identity Vault 和已连接系统”在第 111 页 描述的内容相同。差别是您需要确保不同步通用口令与分发口令。若要实现此目的，可以不使用 NMAS 口令策略，或在使用这些口令策略的同时禁用 " 在设置通用口令时同步分发口令 " 选项。

- “方案 4 的优点和缺点”在第 121 页
- “设置方案 4”在第 122 页
- “对方案 4 查错”在第 123 页

方案 **4** 的优点和缺点

表 ***5-14*** 隧道通讯进程的优点

优点	缺点
允许同步已连接系统间的口令，同时将 Identity Vault 口令保持独立。 无需使用口令策略。 如果要使用口令策略，则无需对该策略启用通用口令。但是，环境必须支持通用口令。 支持 iManager 中的 " 检查口令状态 " 任务，条件是已连接系统也支持该任务。 可以指定在口令同步失败时发送通知。 可以重设置不符合口令策略的已连接系统口令。 如果启用了通用口令和高级口令规则，则可以实施口令策略 （如果指定），并且可以重设置已连接系统上的口令。	如果未启用通用口令和高级口令规则，则将不实施口令策略，并且无法重设置已连接系统上的口令。

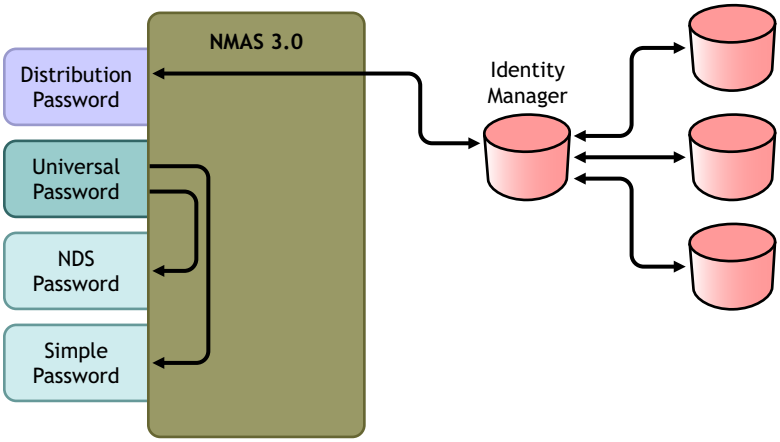
此方案的流程图如下：

1. 口令经 Identity Manager 进入。
2. Identity Manager 通过 NMAS 直接更新分发口令。
3. Identity Manager 还使用分发口令向已指定为接受口令的已连接系统分发口令。

此方案的关键在于，在 NMAS 口令策略中应禁用 " 将通用口令与分发口令同步 "。由于分发口令不与通用口令同步，因而 Identity Manager 可同步已连接系统间的口令而不影响 Identity Vault 中的口令。

在此图中，虽然多个已连接系统显示为同时与 Identity Manager 相连，但请记住，应单独为每个已连接系统的驱动程序创建设置。

图 ***5-14*** *Identity Manager* 更新分发口令时的隧道通讯进程



设置方案 **4**

若要设置此类口令同步，请配置以下内容：

- “通用口令部署”在第 122 页
- “口令策略配置”在第 122 页
- “口令同步设置”在第 123 页
- “驱动程序配置”在第 123 页

通用口令部署

虽然您不必启用通用口令的口令策略，但环境仍必须使用支持通用口令的 eDirectory 8.7.3。请参见 “准备使用 Identity Manager 口令同步和通用口令”在第 86 页 。

口令策略配置

此方法中， Identity Vault 用户不需要口令策略。

但是，如果使用口令策略，则必须执行以下操作：

1 请确保未选中以下选项：

- 在设置通用口令时同步分发口令

  这是通过隧道通讯口令而不影响 Identity Vault 口令的关键。通过不同步通用口令和分发口令，可将分发口令保持独立，使其仅供已连接系统的 Identity Manager 使用。Identity Manager 充当一种管道，它在其它已连接系统间分发口令，而不影响 Identity Vault 口令。

2 根据需要完成其它口令策略设置。

口令策略中的其它口令设置可选。

口令同步设置

使用的设置与 “方案 3：通过 Identity Manager 更新分发口令同步 Identity Vault 和已连接系统”在第 111 页 中的口令同步设置相同。

驱动程序配置

使用的设置与 “方案 3：通过 Identity Manager 更新分发口令同步 Identity Vault 和已连接系统”在第 111 页 中的驱动程序配置相同。

对方案 **4** 查错

如果设置隧道通讯进程口令同步，则分发口令将不同于通用口令和 NDS 口令。

- “登录到订购口令的其它已连接系统时出现问题”在第 123 页
- “口令发生故障时不生成电子邮件”在第 123 页
- “使用 " 检查口令状态 " 时出错”在第 124 页
- “有用的 DSTrace 命令”在第 124 页

另请参见 “查错口令同步”在第 142 页 中的提示。

登录到订购口令的其它已连接系统时出现问题

本节旨在对以下情况进行查错：该已连接系统正在向 Identity Manager 发布口令，但要订购口令的另一已连接系统似乎没有接收该系统的更改。这一关系又称为次已连接系统，意思是它通过 Identity Manager 接收来自第一个已连接系统的口令。

- 启用 DSTrace 中的 *+DXML* 和 *+DVRS* 设置以查看 Identity Manager 规则处理和潜在错误。
- 将驱动程序的 Identity Manager 跟踪级别设置为 *3*。
- 请确保已选中 " 口令同步 " 页上的 "Identity Manager 接受口令 （发布者通道） " 选项。
- 在口令策略中，请确保未选中 " 在设置通用口令时同步分发口令 "。

  Identity Manager 使用分发口令同步已连接系统的口令。使用此同步方法时，必须将通用口令与分发口令同步。
- 请确保驱动程序过滤器的 nspmDistributionPassword 特性具有正确的设置。
- 校验添加特性或 <modify-password> 要素的 <password> 要素是否已转换为 nspmDistributionPassword 的添加或修改特性操作。为此，请使用上述第一项启用跟踪选项，然后观察 DSTrace 屏幕或文件。
- 校验驱动程序配置中包括的 Identity Manager 底稿口令策略是否处于正确的位置和顺序，详情请见 “驱动程序配置中所需的策略”在第 83 页 。
- 将 Identity Vault 中的口令策略与已连接系统实施的任何口令策略进行比较，确保它们相互兼容。

口令发生故障时不生成电子邮件

- 启用 DSTrace 中的 *+DXML* 设置，以查看 Identity Manager 规则处理。
- 将驱动程序的 Identity Manager 跟踪级别设置为 *3*。
- 校验是否已选择生成电子邮件的规则。
- 校验 Identity Vault 对象的因特网电子邮件地址特性中是否包含正确的值。

- 在通知配置任务中，检查 SMTP 服务器和电子邮件模板。请参见 “配置电子邮件通知”在第 131 页 。

电子邮件通知是非侵害性的。它们并不影响触发电子邮件的 XML 文档的处理。如果电子邮件通知失败，则除非重试操作本身，否则不会重试发送通知。电子邮件通知的调试讯息将写入跟踪文件。

使用 " 检查口令状态 " 时出错

iManager 中的检查口令状态任务可导致驱动程序执行检查对象口令的操作。

- 请确保已连接系统支持口令检查。请参见 “已连接系统支持口令同步”在第 77 页 。

  如果驱动程序清单未指示已连接系统是否支持口令检查功能，则无法通过 iManager 执行此操作。
- 如果检查对象口令操作返回 -603，则表明 Identity Vault 对象不包含 nspmDistributionPassword 特性。检查 Identity Manager 特性过滤器以及口令策略中的 " 将通用与分发同步 " 选项。
- 如果检查对象口令操作返回 Not Synchronized，请校验驱动程序配置是否包含适当的 Identity Manager 口令同步策略。
- 将 Identity Vault 中的口令策略与已连接系统实施的任何口令策略进行比较，确保它们相互兼容。
- 检查对象口令操作将检查分发口令。如果未更新分发口令，则"检查对象口令"可能会不报告口令已同步

有用的 DSTrace 命令

+*DXML*：用于查看 Identity Manager 规则处理和潜在的错误讯息。

+*DVRS*：用于查看 Identity Manager 驱动程序讯息

+*AUTH*：用于查看 NDS 口令修改

+*DCLN*：用于查看 NDS DCLient 讯息

5.8.6 方案 5：将应用程序口令与简单口令同步

此方案是口令同步功能的一种特殊用法。使用 Identity Manager 和 NMAS，可以从已连接系统获得口令，并将其直接与 Identity Vault 简单口令同步。如果已连接系统仅提供散列口令，则可以在不反转散列的情况下将这些口令与简单口令同步。然后，其它应用程序便可以通过 LDAP 或 Novell Client 使用同一明文或散列口令，并将 NMAS 部件配置为使用简单口令作为登录方法，以此鉴定到 Identity Vault。

如果已连接系统中的口令为明文口令，则当其从已连接系统进入 Identity Vault 简单口令储存中时，可以发布该口令。

如果已连接系统仅提供散列口令 （支持 MD5、 SHA、 SHA1、或 UNIX Crypt），则必须将它们发布到带有这种散列指示的简单口令 （如 {MD5}）中。

对于要使用同一口令进行鉴定的其它应用程序，需要将另一个应用程序自定义为接受用户口令并鉴定到使用 LDAP 的简单口令。

NMAS 将应用程序中的口令值与简单口令中的值进行比较。如果储存在简单口令中的口令为散列值，则在比较之前， NMAS 将首先使用应用程序中的口令值来创建正确类型的散列值。如果应用程序中的口令与简单口令相同，则 NMAS 将对用户进行鉴定。

在此方案中，不能使用通用口令。

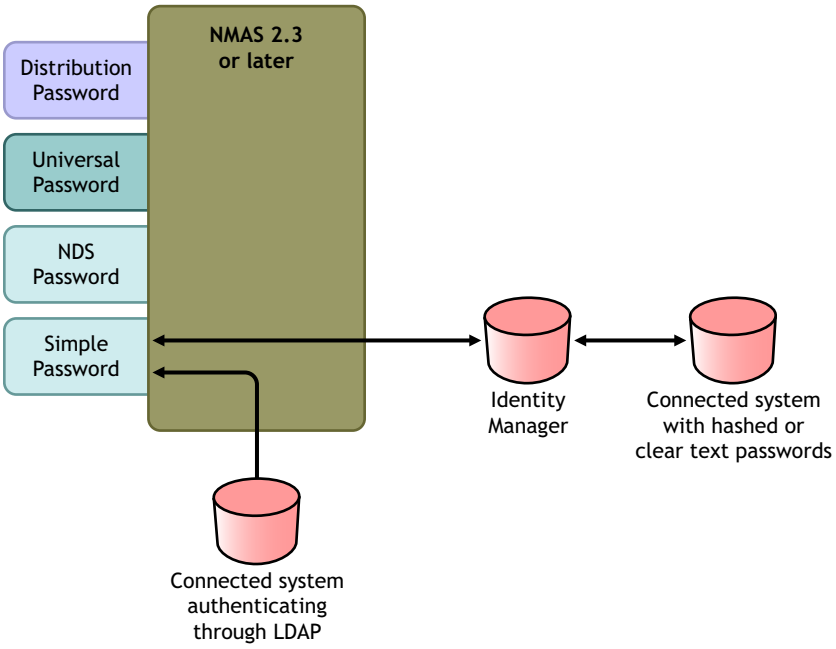
- “与 NDS 口令同步的优点”在第 125 页
- “设置方案 5”在第 125 页

与 NDS 口令同步的优点

表 *5-15* 与 *NDS* 口令同步的优点

优点	缺点
◆ 允许直接更新简单口令。 ◆ 允许同步散列口令，且无需反转散列便可将其用于鉴定多个应用程序。	◆ 此方案不允许使用通用口令。 ◆ 忘记口令和口令自助服务功能仍然可以用于 NDS 口令支持的范围，但不能用于简单口令。 ◆ 因为设置通用口令任务依赖于通用口令，所以管理员无法通过使用此任务在 Identity Vault 中设置用户口令。

图 *5-15* 与 *NDS* 口令同步



设置方案 5

- “口令策略配置”在第 126 页
- “口令同步设置”在第 126 页
- “驱动程序配置”在第 126 页

口令策略配置

在此方案中，用户无需使用口令策略，也无法使用通用口令。

口令同步设置

在此方案中，使用 Identity Manager 底稿直接修改 SAS:Login Configuration 特性。这意味着，通过使用 iManager 中的 " 口令同步 " 页设置的口令同步全局配置值 (GCV) 无效。

驱动程序配置

1 请确保过滤器中的 SAS:Login Configuration 特性对于发布者通道和订购者通道均具有 " 同步 " 设置。

2 将驱动程序策略配置为发布来自已连接系统的口令。

3 对于散列口令，将驱动程序策略配置为在前面追加此类散列 （如果应用程序尚未提供）：

- {MD5} 散列口令

  此口令以 Base 64 编码。

- {SHA} 散列口令

  此口令以 Base 64 编码。

- {CRYPT} 散列口令

明文口令和 Unix Crypt 口令散列不是 Base64 编码。

4 若要将该口令放入简单口令中，请将驱动程序策略配置为修改 SAS:Login Configuration 特性。

以下示例说明了如何在修改操作中使用 modify-attr 要素将简单口令更改为 MD5 散列口令：

```
<modify-attr attr-name="SAS:Login Configuration> <add-value>
<value>{MD5}2tEgXrIHtAnGHOzH3ENslg==</value> </add-value> </
modify-attr>
```

对于明文口令，请参照以下示例。

```
<modify-attr attr-name="SAS:Login Configuration> <add-value>
<value>clearpwd</value> </add-value> </modify-attr>
```

对于添加操作， add-attr 要素将包含下列内容之一：

```
<add-attr attr-name="SAS:Login Configuration>
<value>{MD5}2tEgXrIHtAnGHOzH3ENslg==</value> </add-attr>
```

或者

```
<add-attr attr-name="SAS:Login Configuration> <value>clearpwd</
value> </add-attr>
```

5.9 设置口令过滤器

某些已连接系统可以将用户的实际口令提供给 Identity Manager。

若要捕获 Active Directory、 NIS、以及 NT 域上的口令，则必须在已连接系统上安装口令过滤器，而这需要进行一些次要安装。

- “为 Active Directory 和 NT 域设置口令同步过滤器”在第 127 页
- “为 NIS 设置口令同步过滤器”在第 128 页

5.9.1 为 Active Directory 和 NT 域设置口令同步过滤器

有关信息，请参见 《Identity Manager 驱动程序》(http://www.novell.com/documentation/dirxmldrivers/index.html) 中的 Active Directory 和 NT 域的 Identity Manager 驱动程序实施指南中的 " 口令同步 " 部分。

仅需在一台 Windows 计算机上安装用于 AD 或 NT 域的 Identity Manager 驱动程序。其它域控制器不需要安装该驱动程序，但是每个域控制器确实需要安装一个 pwfilter.dll 文件来捕获口令，以便将口令发送至 Identity Manager。

为简化安装和管理，还提供有一个实用程序，它允许您从安装该驱动程序的 Windows 计算机上对所有域控制器执行此操作。

5.9.2 为 NIS 设置口令同步过滤器

Identity Manager Driver for NIS 3.0 可以处理三种 UNIX 鉴定数据储存器：文件、 NIS 和 NIS+。它提供了一个 PAM 模块，用于捕获口令并将它们发送至 Identity Manager Driver for NIS。

有关部署 NIS 驱动程序的 PAM 模块的信息，请参见 Identity Manager 驱动程序 (http://www.novell.com/documentation/lg/dirxmldrivers/index.html) 的 《*Identity Manager Driver for NIS* 实施指南》。

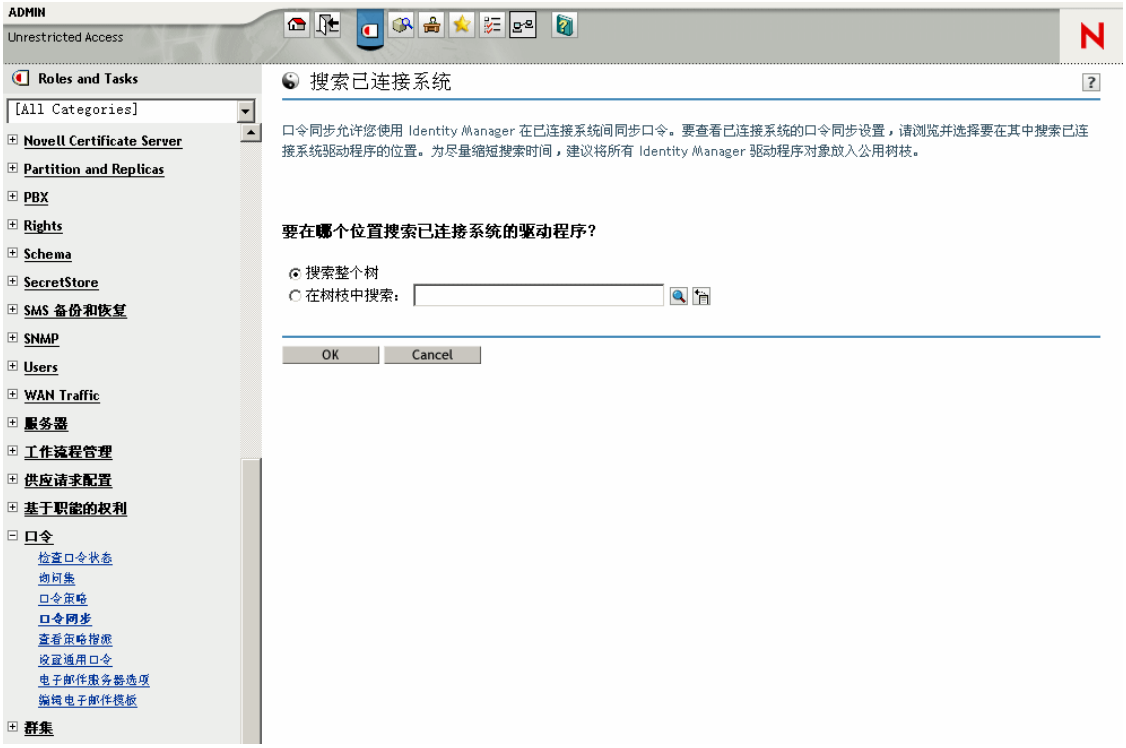
5.10 管理口令同步

- “设置口令在系统间的流动方式”在第 128 页
- “在已连接系统中实施口令策略”在第 129 页
- “将 eDirectory 口令与已同步口令分离”在第 130 页

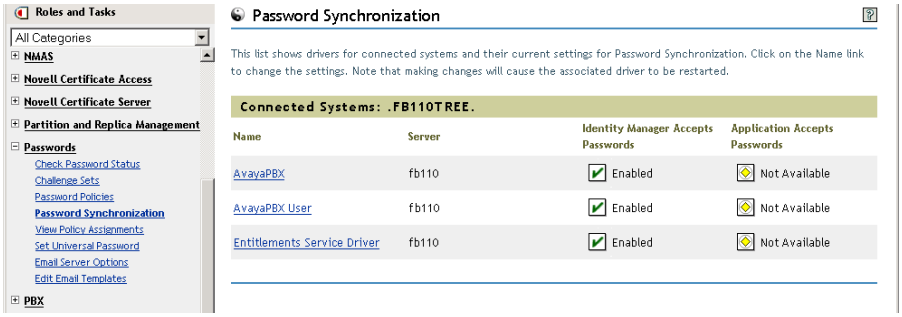
5.10.1 设置口令在系统间的流动方式

查看如何将系统设置为接受或发布口令：

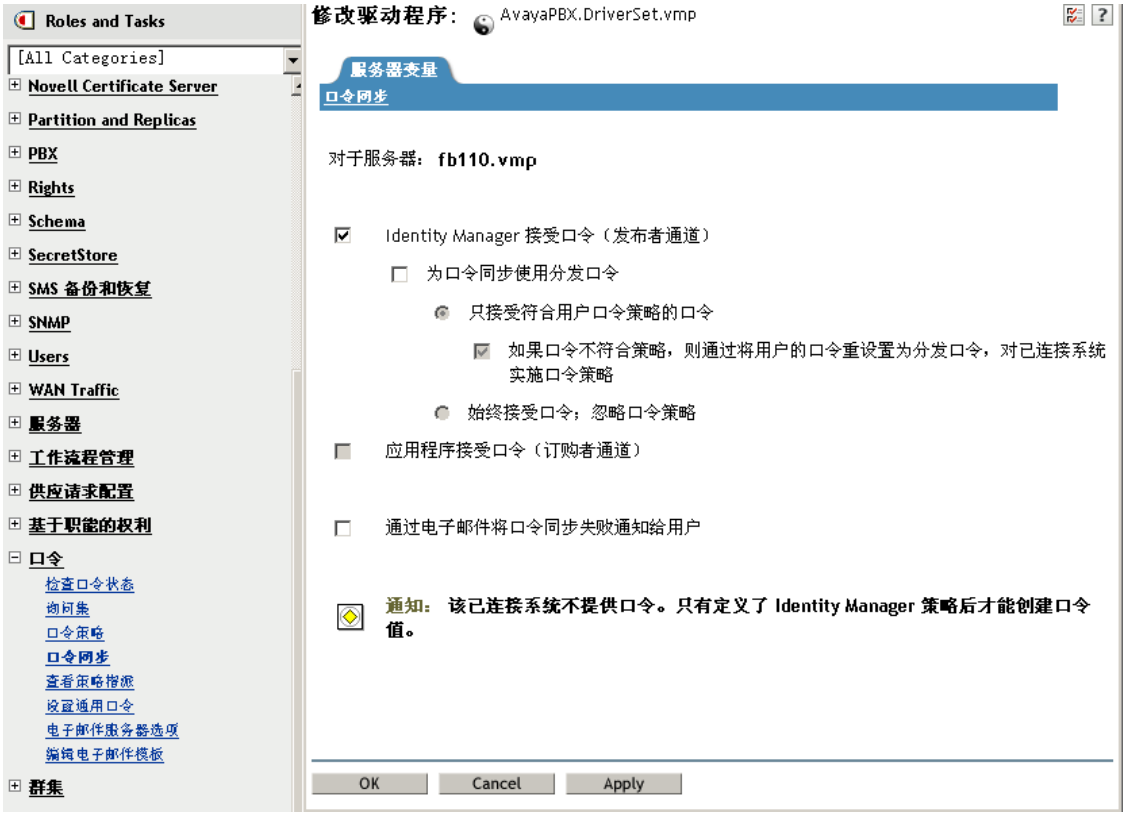
1. 在 iManager 中，选择 " 口令 ">" 口令同步 "。
2. 搜索已连接系统的驱动程序。



搜索结果显示口令在 Identity Manager 和已连接系统间的流动设置。



若要对这些设置进行更改，请单击已连接系统的驱动程序名称。



在 " 修改驱动程序 " 页上，可以设置是否对进入 Identity Manager 的口令实施口令策略，以及是否通过重设置已连接系统口令在已连接系统上实施口令策略。

此页面上的设置均为全局配置值 (GCV)，这些值储存于每个服务器上。请参见 “使用全局配置值控制口令同步”在第 81 页 。

5.10.2 在已连接系统中实施口令策略

如果要使用高级口令规则和 Identity Manager 口令同步，建议执行以下操作：

1. 研究所有已连接系统的口令策略。
2. 确保高级口令规则与已连接系统中的口令策略兼容。

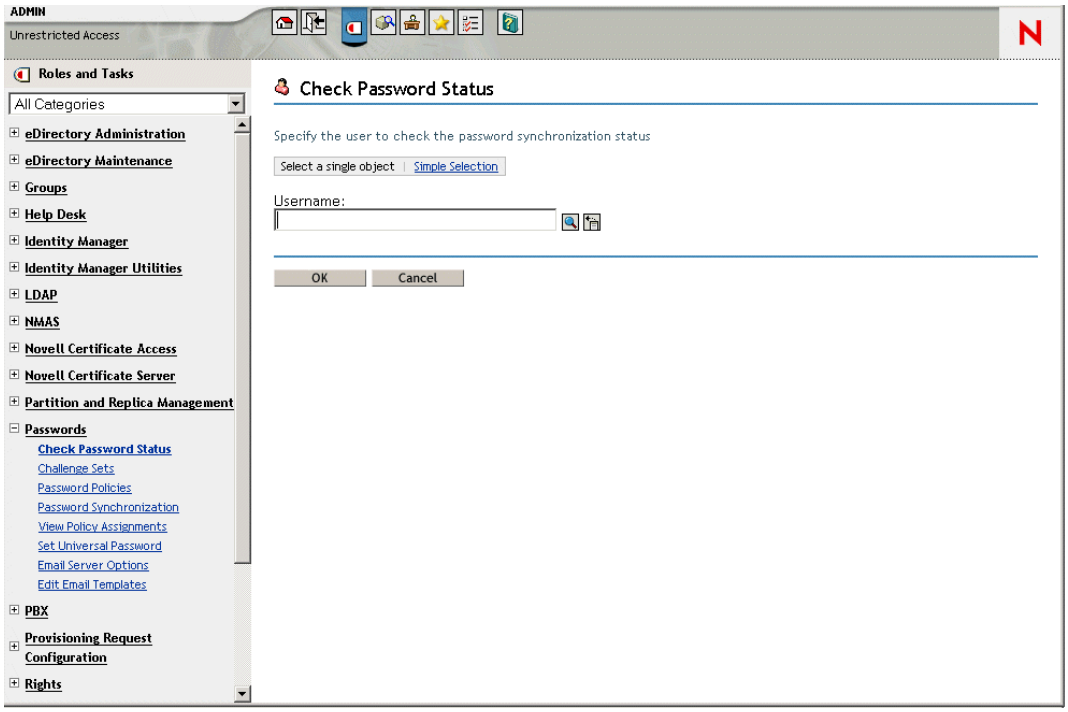
5.10.3 将 eDirectory 口令与已同步口令分离

此方案在 “方案 4：隧道通讯进程同步已连接系统而不是 Identity Vault，同时由 Identity Manager 更新分发口令”在第 120 页 中有详细的描述。

5.11 检查用户的口令同步状态

可以确定特定用户的分发口令是否与已连接系统中的口令相同。

1 在 iManager 中，选择 " 口令 ">" 检查口令状态 "。



2 浏览并选择用户。

检查口令状态的任务可使驱动程序执行检查对象口令的操作。

并非所有驱动程序都支持口令检查。支持口令检查的驱动程序的清单中必须包含口令检查功能。 iManager 不允许将口令检查操作发送至驱动程序清单中不包含此功能的驱动程序。

检查对象口令操作将检查分发口令。如果分发口令未更新，检查对象口令操作可能会报告口令未同步。

如果发生以下情况之一，则不会更新分发口令：

- 正在使用 “方案 1：使用 NDS 口令在两个 Identity Vault 间进行同步”在第 100 页 中描述的同步方法。
- 正在同步通用口令（如 “方案 2：使用通用口令同步”在第 102 页 中所述），但是尚未启用口令策略配置选项来同步通用口令与分发口令。

注释：请记住，对于 Identity Vault 而言，检查口令状态操作将检查 NDS 口令而不是通用口令。因此，如果用户口令策略中未指定将 NDS 口令与通用口令同步，则始终报告未同步口令。而实际上，分发口令和已连接系统上的口令可能是同步的，但如果 NDS 口令和分发口令与通用口令不同步，则 " 检查口令状态 " 将不会报告准确的结果。

5.12 配置电子邮件通知

可以通过 iManager 任务指定电子邮件服务器，并自定义电子邮件通知模板。

有了电子邮件模板，口令同步和口令自助服务就可以自动向用户发送电子邮件。

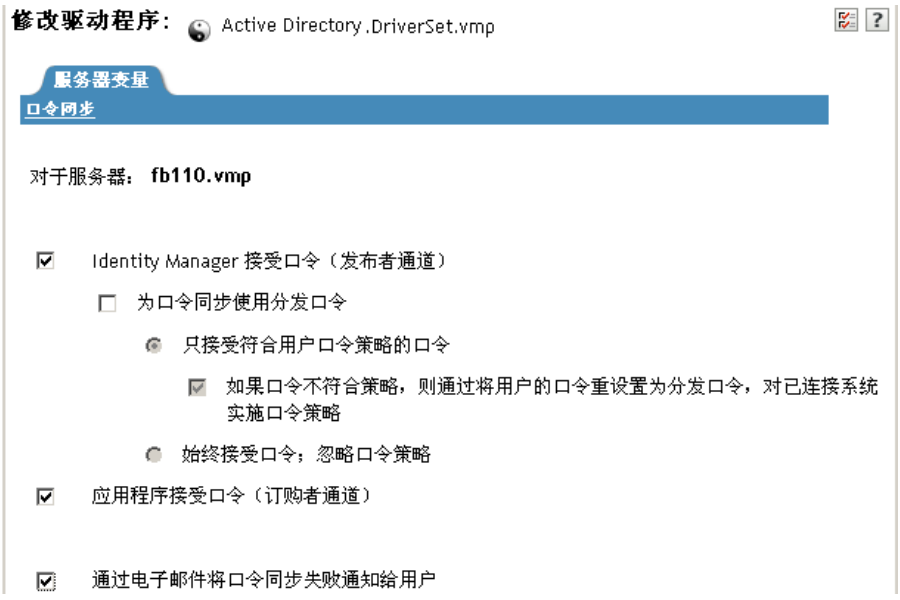
无需亲自动手创建模板。使用模板的应用程序会提供模板。在 Identity Vault 中，电子邮件模板是模板对象，它们位于通常可在树根处找到的安全性树枝中。虽然这些模板是 Identity Vault 对象，但应该通过 iManager 进行编辑。

这是模块化框架。添加使用电子邮件模板的新应用程序时，会同时安装应用程序与这些应用程序使用的模板。

可以根据 iManager 中的选择，控制是否发送电子邮件讯息。在忘记口令的情况下，只有选择以下任意一种忘记口令操作时，才会发送电子邮件通知：以电子邮件形式将口令发送给用户，或以电子邮件形式将口令提示发送给用户。请参见 《口令管理管理员指南》(http://www.novell.com/documentation/password_management/index.html) 中的 " 向用户提供忘记口令自助服务 "。

如果选择 " 通过电子邮件将口令同步失败通知给用户 "，就会将口令同步配置为仅在口令同步操作失败时发送电子邮件，并且仅限于所指定的驱动程序。

图 *5-16* 配置口令同步



另外，还需要确保驱动程序策略中包括 SMTP 鉴定信息。

- “前提条件”在第 132 页
- “设置 SMTP 服务器以发送电子邮件通知”在第 133 页

- “设置通知的电子邮件模板”在第 134 页
- “在驱动程序策略中提供 SMTP 鉴定信息”在第 134 页
- “将自己的替换标记添加到电子邮件通知模板中”在第 136 页
- “向管理员发送电子邮件通知”在第 142 页
- “本地化电子邮件通知模板”在第 142 页

5.12.1 前提条件

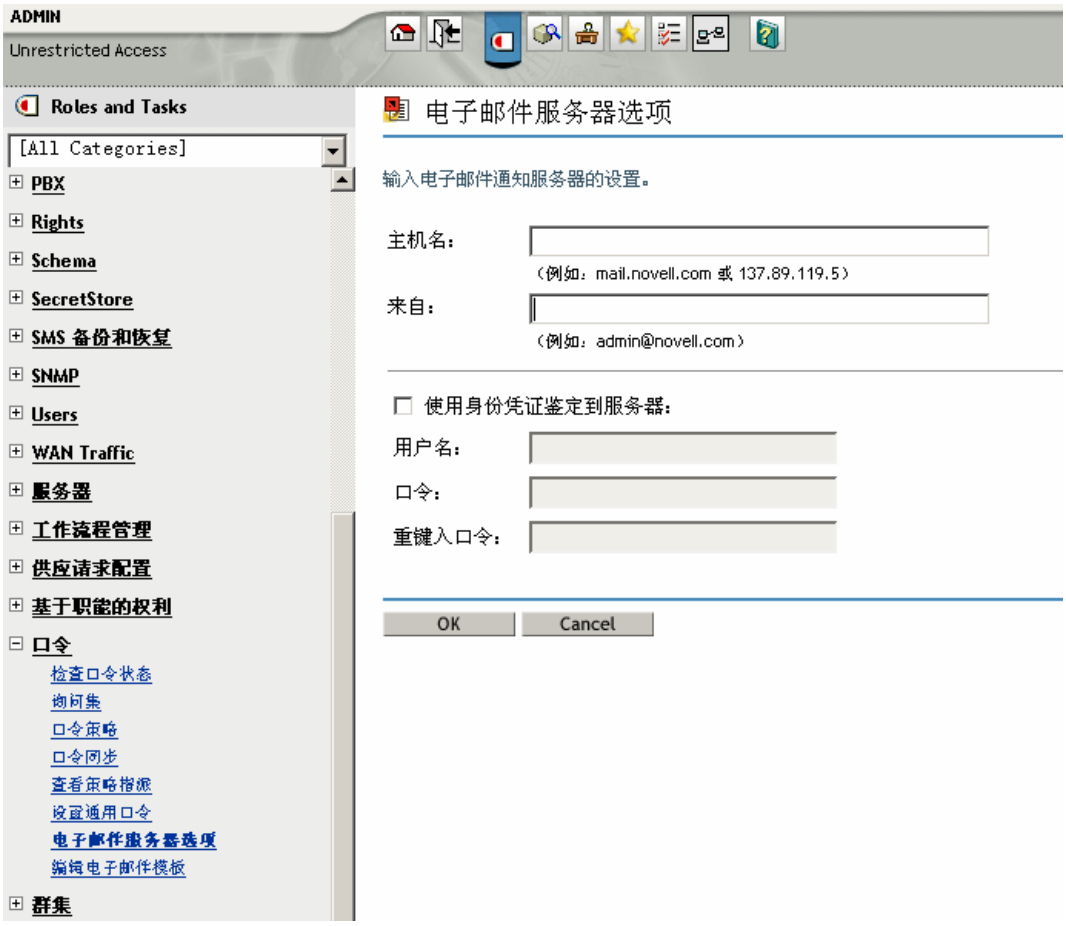
- ❑ 确保 Identity Vault 中用户的因特网电子邮件地址特性已填充。
- ❑ 如果口令同步要使用电子邮件通知，请确保口令同步驱动程序策略中包含 SMTP 服务器的口令。请参见 “在驱动程序策略中提供 SMTP 鉴定信息”在第 134 页 。
- ❑ 如果担心某些用户可能没有填充电子邮件地址，或者需要所有通知失败的电子邮件记录，请考虑选择一个口令管理员帐户，除了向用户发送外，所有电子邮件通知都将发送到此帐户。

  此电子邮件地址应在 Identity Manager 底稿策略的 " 收件人 " 字段中。有关更多信息，请参见 “向管理员发送电子邮件通知”在第 142 页 。
- ❑ 如果 eDirectory 和 Identity Manager 位于 UNIX 服务器中，该服务器上必须保存此电子邮件模板对象的复本。

  这些对象位于安全性树枝的根处。这意味着该服务器可能需要根分区的复本。

5.12.2 设置 SMTP 服务器以发送电子邮件通知

1 在 iManager 中，选择 " 口令 ">" 电子邮件服务器选项 "。



2 键入以下信息：

- 主机名
- 电子邮件讯息的 " 发件人 " 字段中希望出现的名称 （例如， Administrator）
- 鉴定到服务器的用户名和口令 （如有必要）。

3 单击 " 确定 "。

4 如果要同时使用 Identity Manager 驱动程序和口令同步，并希望使用电子邮件通知功能，还必须进行以下操作：

4a 如果 SMTP 服务器在发送电子邮件之前需要鉴定，请确保驱动程序策略中包含口令。有关指导，请参见 “在驱动程序策略中提供 SMTP 鉴定信息”在第 134 页 。

根据步骤 2 在 " 电子邮件服务器选项 " 页中指定鉴定信息，这些信息足以生成忘记口令通知，但不足以生成口令同步通知。

4b 重启动 Identity Manager 驱动程序，对所做的更改进行更新。

驱动程序只在启动时读取模板和 SMTP 服务器信息。

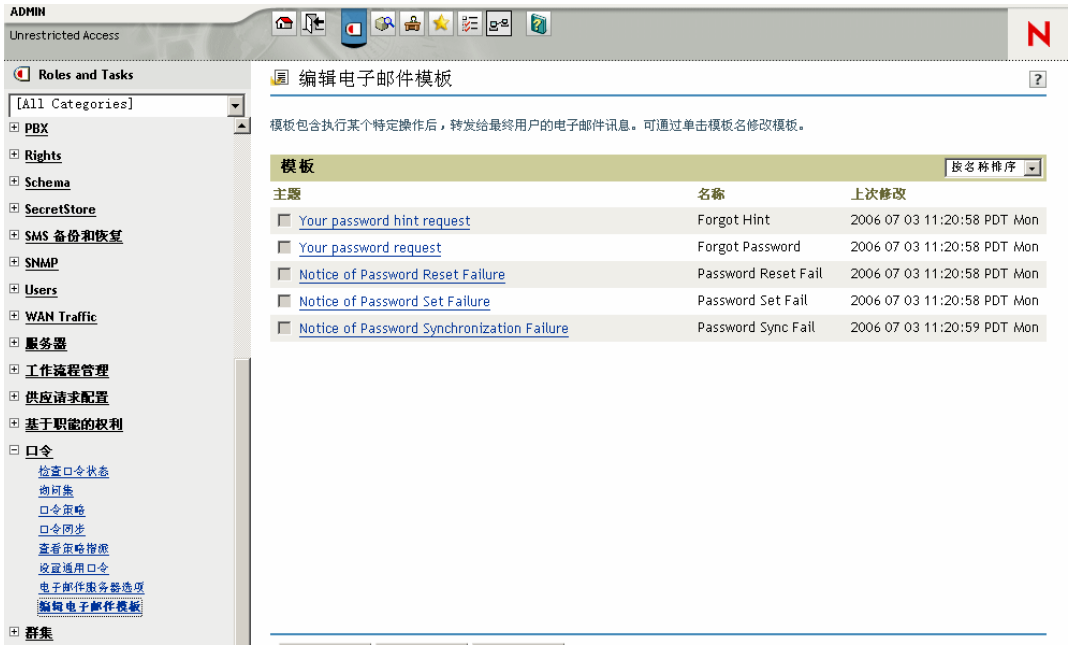
5 自定义电子邮件模板，详情请见 “设置通知的电子邮件模板”在第 134 页 。

电子邮件服务器设置完毕之后，如果使用了可发送讯息的功能，那么使用电子邮件信息的应用程序就可以进行发送。

5.12.3 设置通知的电子邮件模板

可以使用自己的文本自定义这些模板。模板的名称表示模板的用途。

1 在 iManager 中，选择 " 口令 ">" 编辑电子邮件模板 "。



2 根据需要编辑模板。

请记住，如果要添加替换标记，可能需要执行某些附加任务。请按照 “将自己的替换标记添加到电子邮件通知模板中”在第 136 页 中的指导操作。

3 重启动 Identity Manager 驱动程序，对所做的更改进行更新。

驱动程序只在启动时读取模板和 SMTP 服务器信息。

5.12.4 在驱动程序策略中提供 SMTP 鉴定信息

指定 SMTP 服务器用户名和口令的操作，详见 “设置 SMTP 服务器以发送电子邮件通知”在第 133 页 。这些信息足以生成忘记口令电子邮件通知。

但是，对于口令同步电子邮件通知，还需要在驱动程序策略中提供口令。Metadirectory 引擎可以访问用户名，但无法访问口令，口令必须由驱动程序策略提供。

如果存在以下情况，则必须完成此过程：

- SMTP 服务器处于可靠状态，需要在发送电子邮件之前进行鉴定。
- 同时使用 Identity Manager 口令同步和 Identity Manager 驱动程序
- 在驱动程序的口令同步设置中，已选择 " 通过电子邮件将口令同步失败通知给用户 "。

要将 SMTP 服务器口令添加到驱动程序策略中：

1 确保驱动程序具有使用口令同步所必需的策略。

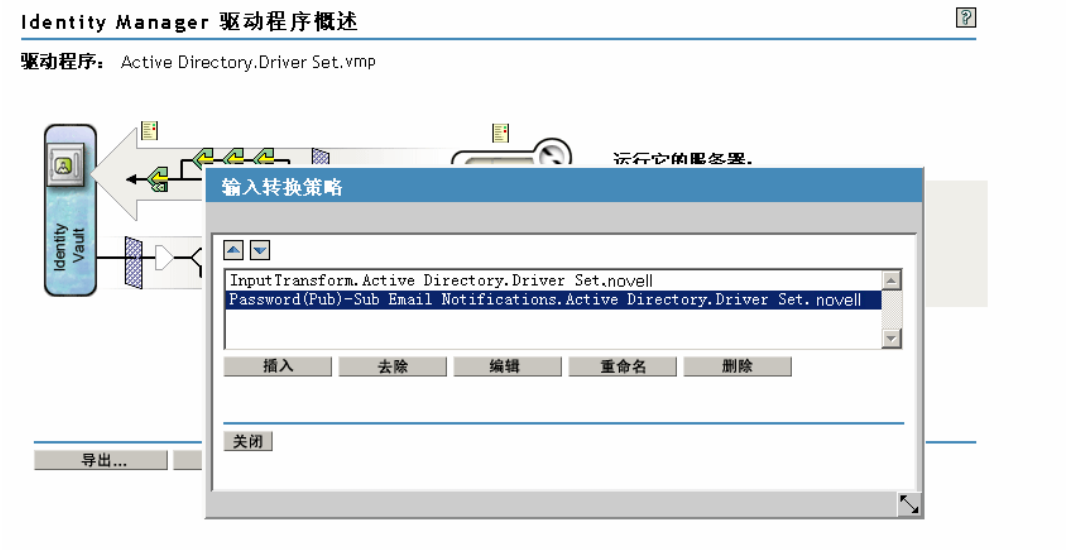
样本驱动程序配置中已提供了这些策略，也可以添加策略，详情请见 “升级现有驱动程序配置以支持口令同步”在第 90 页 。

2 在 iManager 中，选择 *Identity Manager* >"Identity Manager 概述 "。

3 搜索驱动程序集，或浏览并选择暂挂驱动程序集的树枝。

4 在 Identity Manager 驱动程序概述中，单击驱动程序图标。

5 选择 " 输入转换 " 图标或 " 输出转换 " 图标。



6 选择一个策略，然后单击 " 编辑 "。

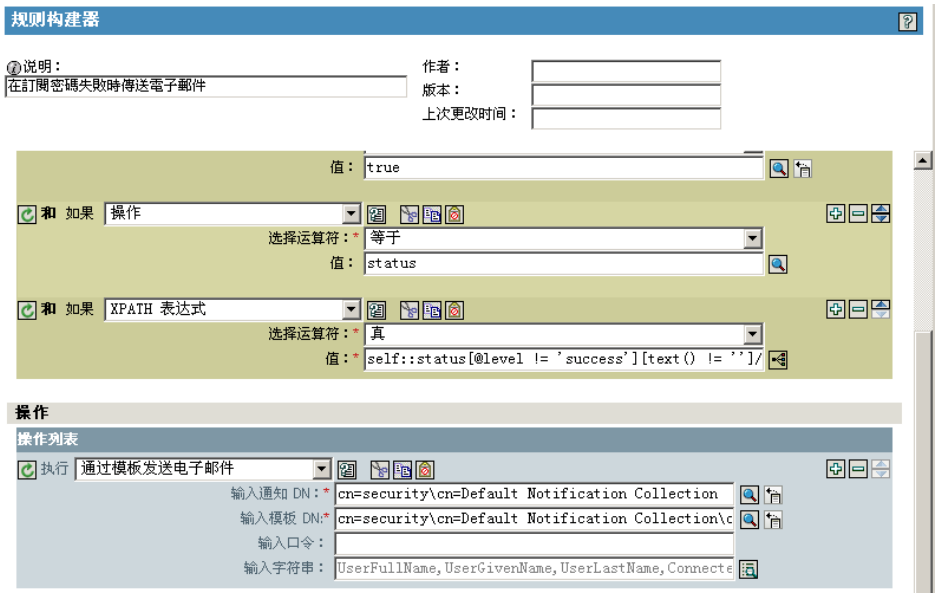
7 单击一条规则。

8 在包括从模板发送电子邮件操作的规则中，指定 SMTP 服务器的口令。

例如，如果要使用样本驱动程序配置，则需要修改以下口令同步策略。

策略集	策略名	规则名
输入转换	口令 （发布） - 订购电子邮件通知	◆ 订购口令失败时，发送电子邮件 ◆ 使用 Identity Manager 数据储存器口令重设置已连接系统口令失败时，发送电子邮件
输出转换	口令 （订购） - 发布电子邮件通知	◆ 发布口令操作失败时，发送电子邮件

下图为需要口令的从模板发送电子邮件操作示例。



对储存在 Identity Vault 中的口令进行模糊处理。

9 选择 （标记）规则，然后单击 " 确定 "。

5.12.5 将自己的替换标记添加到电子邮件通知模板中

在默认情况下，电子邮件通知模板中有一些标签是已定义的，有助于进行用户讯息的个性化。也可以添加自己的标签。

是否能够添加标签，取决于使用电子邮件模板的应用程序。

- “将替换标记添加到口令同步电子邮件通知模板中”在第 136 页
- “将替换标记添加到忘记口令电子邮件通知模板中”在第 141 页

将替换标记添加到口令同步电子邮件通知模板中

可以将替换标记添加到口令同步的电子邮件通知模板中，但如果不同时在参考该电子邮件通知模板的每个口令同步策略规则中定义这些标签，它们将不起作用。使用 " 从模板发送电子邮件 " 操作时，在模板内部声明的所有替换标记都必须定义为此操作的子 arg-string 要素。

例如，Identity Manager 提供了默认替换标记，包括在电子邮件通知模板中。Identity Manager 还在驱动程序配置中提供了默认口令同步策略。电子邮件模板中提供的每个默认标签也在使用该电子邮件模板的口令同步策略的每个规则中进行定义。

例如，" 用户名 " 标签是在名为 " 口令集失败 " 的电子邮件模板中定义的一个默认标签。名为 " 订购口令失败时发送电子邮件 " 的策略规则参考 " 从模板发送电子邮件 " 操作中的电子邮件模板。此规则用于通知用户口令同步失败的策略中。相同的 " 用户名 " 标签在该规则中已定义为 arg-string 要素。

与此示例相同，所添加的每个新标签都必须同时在电子邮件模板和参考此电子邮件模板的策略规则中进行定义，以便 Metadirectory 引擎了解在向用户发送电子邮件时如何将正确的数据插入替换标记的位置。

可参考 Identity Manager 附带的 Identity Manager 驱动程序配置中的标签，以此为例。

请牢记以下准则：

- 在电子邮件模板中称为替换标记的项目在策略构建器环境中称为令牌。
- 按照本节中的步骤说明，可使用策略构建器更便捷地定义替换标记的自变量字符串。
- 所添加的标签可能被定义为以下内容：
  - 用户的任意源特性或目标特性

    与忘记口令电子邮件模板添加标签的操作不同，简单地添加一个与 Identity Vault 中用户对象的某一特性名称相同的标签，该标签将不起作用。与对口令同步电子邮件通知模板中的所有标签的要求一样，还必须定义参考电子邮件模板的策略中的标签。
  - 全局配置值
  - XPATH 表达式

  忘记口令电子邮件模板中的标签仅限于 eDirectory 用户特性，与本标签不同。
- 与忘记口令电子邮件模板添加标签的操作不同 （要求使用 eDirectory 用户特性的确切名称），可以将替换标记命名为任意名称，此名称只需与参照此电子邮件模板的策略中所定义的标签使用的名称相匹配。

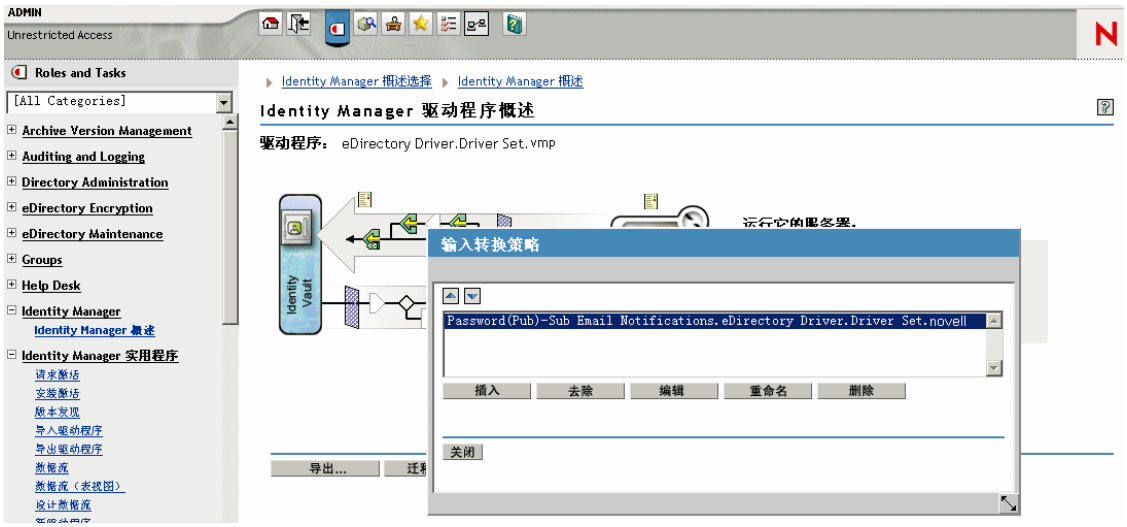
要定义策略中的标签，请找到参照此电子邮件通知模板的所有策略，并使用策略构建器向策略中添加标签。在各策略中，编辑参考此模板的各个规则。

确认已找到参考电子邮件通知模板的所有策略的一种方法是导出驱动程序配置，然后搜索发送电子邮件操作的 XML，其中的模板名称需与电子邮件通知模板名称相同。

1. 在 iManager 中，选择 *Identity Manager* >"Identity Manager 概述 "。
2. 选择驱动程序集，对其中的驱动程序的策略进行编辑。
3. 单击驱动程序的图标，其中包含需编辑的策略。
4. 在发布者或订购者通道上，单击某一策略集，其中包含需编辑的策略。

   例如，Identity Manager 附带的 eDirectory 驱动程序的驱动程序配置中的输入转换策略集包含一个策略，该策略参考两个口令同步电子邮件通知模板。
5. 单击该策略，然后单击 " 编辑 "。

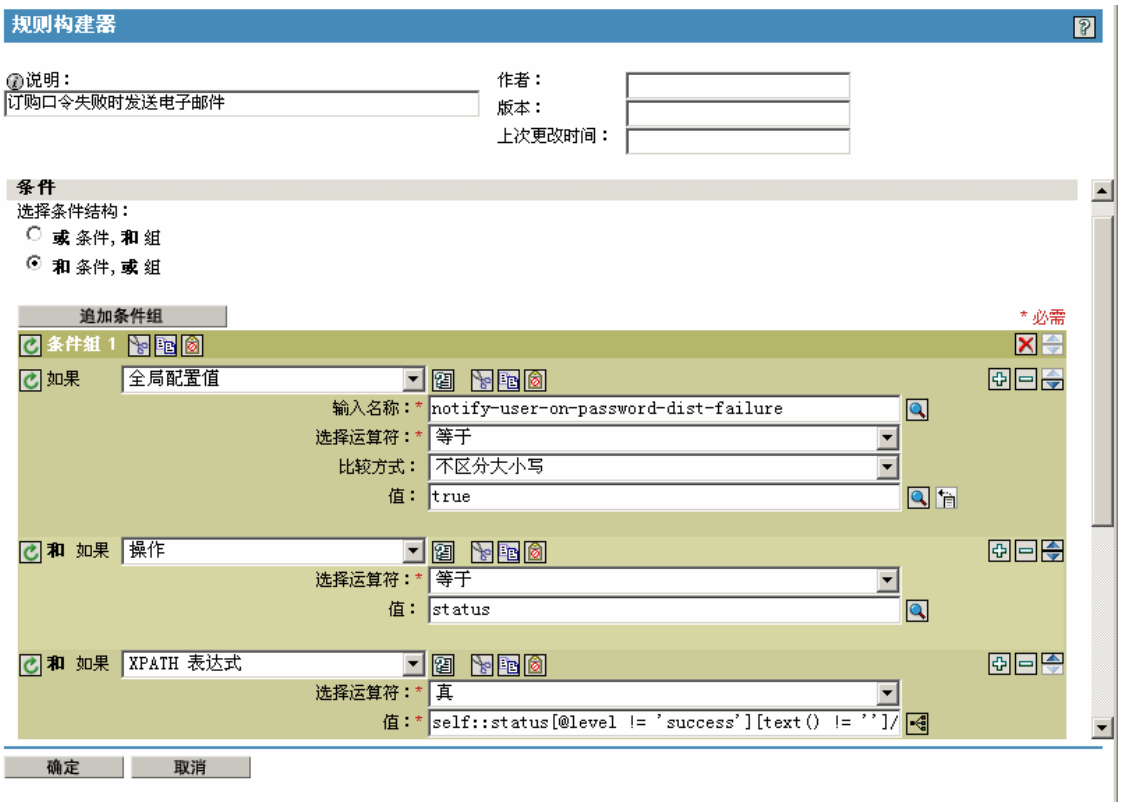
下图阐释了如何编辑 eDirectory 驱动程序的 " 口令 （发布） - 订购电子邮件通知 " 策略：



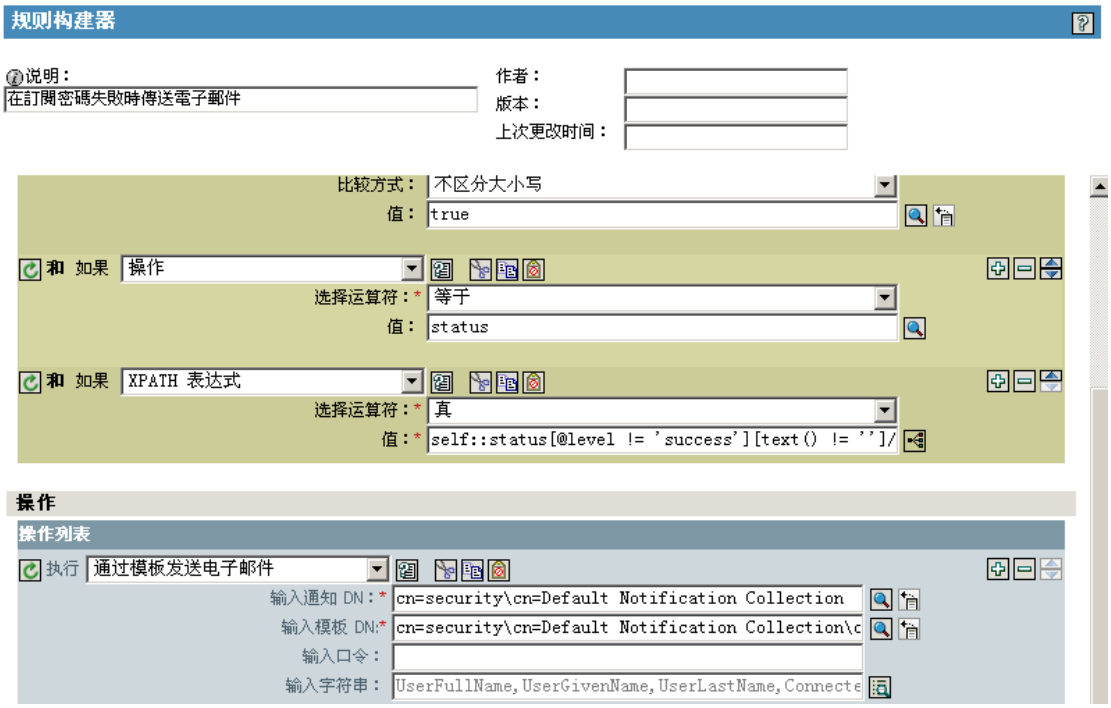
6 在打开的规则列表中，单击参考电子邮件通知模板的规则。

例如，在 " 口令 （发布） - 订购电子邮件通知 " 策略中，可以查看此规则列表。这两个规则同时参照其中一个口令同步电子邮件模板。如果要将标签添加到两个模板中，则需要编辑这两个规则。

如果单击第一条规则，则出现以下页：



7 滚动至 " 操作 " 部分。



8 对于 " 从模板发送电子邮件 " 规则，请单击 " 输入字符串 " 字段旁的浏览按钮 。

此操作将打开字符串构建器。下图显示了示例规则中可看到的字符串列表。请注意，电子邮件通知模板中使用的默认标签已在口令同步策略中进行定义 （该策略是 Identity Manager 驱动程序配置的一部分），与本示例相同。可以将默认标签作为示例。

9 若要定义可以在电子邮件通知模板中使用的标签，请单击 " 追加新字符串 "，然后输入该标签的名称。

请确保该名称与电子邮件通知模板中使用的名称完全相同。

10 在 " 字符串值 " 字段中，单击浏览按钮 定义标签。

11 在 " 自变量生成器 " 页中，指定在电子邮件通知模板中使用此标签时将输入的值。

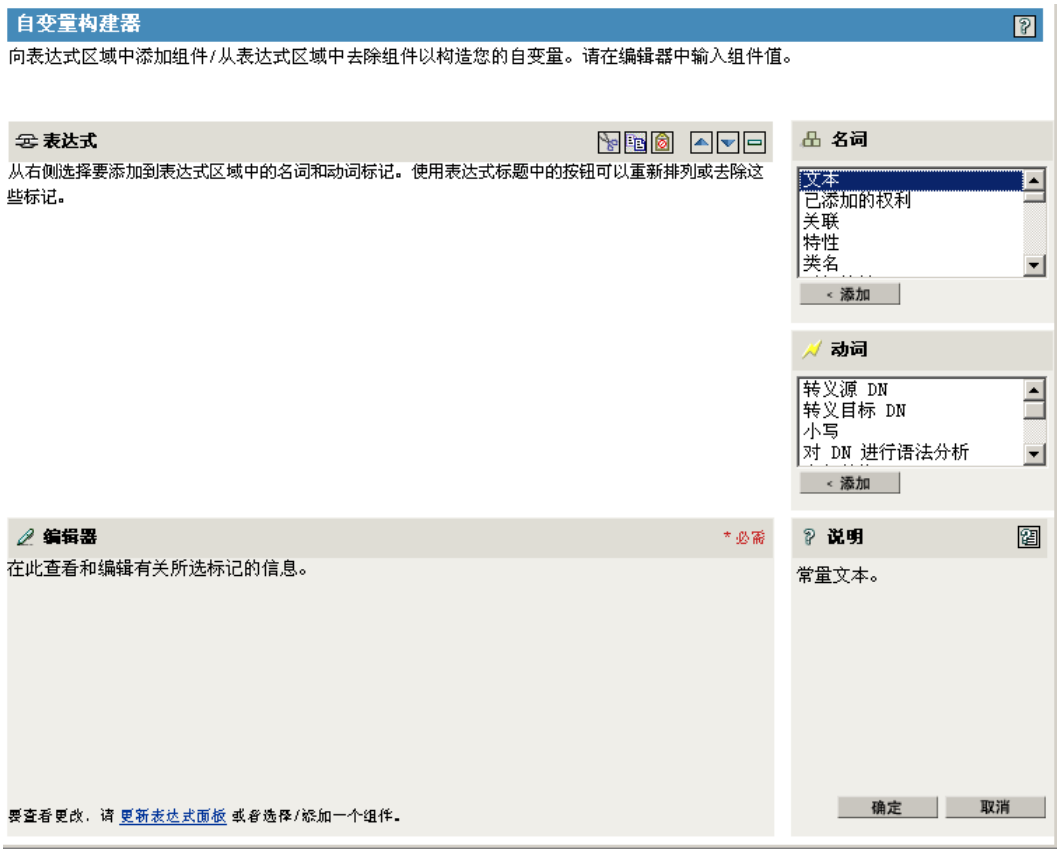
可以将标签定义为以下内容：

- 用户的任意源特性或目标特性

  与忘记口令电子邮件模板添加标签的操作不同，简单地添加一个与 Identity Vault 中用户对象的某一特性名称相同的标签，该标签将不起作用。与对口令同步电子邮件通知模板中使用的所有标签一样，还必须定义参考电子邮件模板的策略中的标签。

- 全局配置值
- XPATH 表达式

下图阐释如何定义标签：



完成标签定义并单击 " 确定 " 之后，它将以字符串的形式显示在 " 字符串构建器 " 页中。

12 请确保单击 " 确定 " 来完成所有页，以便保存对策略所做的更改。

13 重复这些步骤，以编辑参考电子邮件通知模板的所有策略中的规则。

14 将策略中定义的标签添加到电子邮件通知模板中，请使用与策略中完全相同的名称。

这样，就可以在电子邮件通知模板正文中使用标签名称了。

15 保存更改，然后重启动驱动程序。

将替换标记添加到忘记口令电子邮件通知模板中

使用以下准则，将标签添加到忘记口令电子邮件通知模板中：

- 在收到讯息的用户对象中，可以只添加与 LDAP 特性对应的标签。
- 所添加的标签名称必须与用户对象中 LDAP 特性名称完全相同。

  要查看 LDAP 特性与 eDirectory 特性名称的对应情况，可以参考 LDAP 的 Identity Manager 驱动程序中提供的纲要映射策略。
- 不需要其它配置。

5.12.6 向管理员发送电子邮件通知

电子邮件通知的默认配置是仅向用户发送。Identity Manager 附带的策略使用受影响用户的 Identity Vault 对象的电子邮件地址。

但是，可以配置口令同步策略，将电子邮件通知同时发送给管理员。要实现此目的，必须修改其中一个策略的 Identity Manager 底稿。

定义包含管理员电子邮件地址的令牌，向管理员发送密送件。

要抄送管理员，请修改生成电子邮件的策略 （例如 PublishPasswordEmails.xml，策略根据其中的电子邮件地址发送通知）并添加包含管理员电子邮件地址的附加 <arg-string> 要素。

以下示例说明了附加 arg-string 要素：

```
[XXX] <arg-string name="to">

     <token-text>Admin@company.com</token-text>

      </arg-string>
```

请确保在进行更改后重启动驱动程序。

5.12.7 本地化电子邮件通知模板

请牢记以下几点：

- 默认模板是英文版，但可以使用其它语言编辑该文本。
- 替换标记的名称和定义必须保留为英文，使策略中的 arg-string 令牌定义与替换标记的名称相匹配。
- 若要指定邮件项目使用的编码，则需要在 portalservlet.properties 文件中添加一个设置（仅适用于忘记口令电子邮件通知）。例如：

  ```
  ForgottenPassword.MailEncoding=EUC-JP
  ```

  如果该设置不存在，在转换邮件时将不使用任何编码。
- 对于口令同步电子邮件讯息，可以对以下要素指定名为 "charset" 的 XML 特性：<mail>、<message> 和 <‘>。

  有关使用这些要素的信息，请参见 《手工任务服务的 *DirXML* 驱动程序实施指南》(http://www.novell.com/documentation/dirxmldrivers/index.html)，其中提供了有关电子邮件模板的详细信息。

5.13 查错口令同步

- 请参见 “实施口令同步”在第 98 页 中的提示。
- 请确保 NMAS 安装了简单口令登录方法。

- 请确保服务器上有树根的复本，而且该服务器需要 NMAS 对 eDirectory 登录方法实施口令策略，或对由 Identity Manager 同步的已连接系统中的口令实施口令策略。
- 请确保已将需要同步口令的用户复制到了正在同步该口令的驱动程序所在的同一服务器上。与其它驱动程序的功能相同，该驱动程序只能管理同一服务器上主复本或读 / 写复本中的用户。
- 请确保已正确配置万维网服务器和 Identity Vault 之间的 SSL。
- 如果在初始创建用户时发现口令不符合的错误，但 Identity Vault 中的口令设置正确，则驱动程序策略中的默认口令可能不符合该用户所应用的口令策略。

  以下方案使用 Active Directory 驱动程序。但是，相同的事件也可能发生在其它驱动程序上。

  提供初始口令： 当 Active Directory 驱动程序在 Identity Vault 中创建新用户对象以匹配 Active Directory 中的用户时，希望该驱动程序提供该用户的初始口令。Active Directory 驱动程序的样本配置将发送初始口令作为一项独立操作，但不添加用户；如果 Active Directory 未提供任何口令，样本配置中还包括向用户提供默认口令的策略。

  由于添加用户和设置口令的操作是分别进行的，在这种情况下新用户通常会立即收到默认口令。由于 Active Directory 驱动程序在添加用户后会立即发送口令，因此默认口令随后将被更新。如果默认口令不符合用户 Identity Vault 的口令策略，将出现错误。

  例如，如果使用用户的姓氏创建的默认口令过短，不符合口令策略，可能会出现 -216 错误，提示口令过短。但是，如果 Active Directory 驱动程序接着发送了符合策略的初始口令，将很快纠正这种情况

  无论所使用的是哪个驱动程序，若希望创建用户对象的已连接系统提供初始口令，请考虑执行以下某项操作。如果 " 添加 " 事件未提供初始口令而在后续事件中提供了初始口令，这些措施则更加重要。

  - 在创建默认口令的发布者通道上更改策略，使默认口令符合已在 Identity Vault 中为组织定义的口令策略。（选择 " 口令 "，然后选择 " 口令策略 "。）

    如果初始口令来自授权应用程序，将替换默认口令。

    由于建议保留默认口令策略以维持系统内部的高级别安全性，因此该选项更加适用。
  - 在发布者通道上，去除创建默认口令的策略。在样本配置中，命令转换策略集提供该策略。Identity Vault 中允许添加无口令的用户。此选项假设新创建用户对象的口令最终将通过发布者通道，所以用户对象只是短时间无口令。
- 口令策略是以树为中心指派的。与此相反，口令同步是在每个驱动程序上分别设置的。驱动程序安装在每台服务器上，且只能管理主复本或读 / 写复本中的用户。

  要获得预期的口令同步结果，请确保运行口令同步驱动程序的服务器上的主复本或读 / 写复本中的树枝与已指派口令策略 （该策略启用通用口令）的树枝相匹配。将口令策略指派给分区根树枝可确保将此口令策略指派给树枝和子树枝中的所有用户。
- 有用的 DSTrace 命令：

  +DXML：用于查看 Identity Manager 规则处理情况和潜在的错误讯息。

  +DVRS：用于查看 Identity Manager 驱动程序讯息

  +AUTH：用于查看 NDS 口令修改

  +DCLN：用于查看 NDS DCLient 讯息

创建及使用权利

6

可使用 Identity Manager 同步已连接系统间的数据。可使用权利为个人或组设置准则，一旦满足准则，则启动事件授予或取消对已连接系统内部业务资源的访问权限。这样，就增加了一个控制级别，还可以自动授予和取消资源。

要使用权利，需进行以下两方面操作：创建权利和管理权利。可通过 iManager 或 Designer 创建权利。要通过 iManager 创建权利，请选择 iManager 中 Identity Manager 实用程序标题中的 " 创建权利 " 选项。有关更多信息，请参见 “通过 iManager 使用 XML 编写权利”在第 150 页 。

也可以使用 Designer 创建权利，并将这些权利部署到现有的 Identity Manager 驱动程序中。在 Designer 中，可以通过 " 权利向导 " 创建权利，该向导提供一个图形界面，完成该界面中的各进程步骤，即可创建权利。在 iManager 中，可通过简单界面创建权利，但需通过 XML 编辑器添加附加属性。由于 Designer 具有图形界面，因此建议使用 Designer 创建和编辑权利。

创建权利 （或使用某些 Identity Manager 驱动程序中预配置的权利）后，需要对权利进行管理。权利可由两个包或代理进行管理：作为基于职能的权利策略通过 iManager 进行管理，或在基于工作流程的配置信息提供中通过用户应用程序进行管理。有关基于工作流程的配置信息提供中使用的权利，请参见“基于工作流程的配置信息提供的介绍”。基于职能的权利的有关信息，请参见 “管理基于职能的权利概述”在第 162 页 。

如果满足准则，就可以通过基于职能的权利策略授予业务资源。例如，如果用户满足准则 1、2 和 3，则可通过基于职能的权利策略成为 H 组的成员；但如果用户满足准则 4 和 5，则成为 I 组的成员。若要在基于工作流程的配置信息提供中使用此权利，首先要经过批准。

6.1 术语

以下是本章中可能出现的一些术语。

表 *6-1* 术语

术语	解释
权利	表示已连接系统中业务资源的 Identity Vault 对象。
权利代理	授予和取消权利。对于基于职能的权利，代理为权利服务驱动程序。
授予或取消	授予或取消权利的意义由 Identity Manager 驱动程序的全局配置变量 (GCV) 进行控制。
权利用户	使用权利的相关信息的所有内容。权利用户包括 iManager、用户应用程序和 Identity Manager 策略。

6.2 创建权利：概述

- “预配置支持权利的 Identity Manager 驱动程序”在第 146 页
- “启用其它 Identity Manager 驱动程序中的权利”在第 147 页

必须首先了解要利用权利实现的目标。权利如何发挥作用取决于 Identity Manager 驱动程序中通过策略构建的功能。这些驱动程序策略实施规则，并处理 Identity Vault 和已连接系统间的事件。如果 Identity Manager 驱动程序中的策略未指定要进行的操作，权利将不起作用。例如，如果不指定命令策略中检查组成员资格的用户修改规则的操作部分，将忽略授予或取消组成员资格权利的尝试。

应明确要利用 Identity Manager 实现的目标，然后才能正确地设计所有已连接系统资源的授予和取消功能。以下四步过程有助于计划如何创建和使用权利：

1. 了解在当前业务形势下需达到的目标。通过 Identity Manager，几乎可以设计和实施所有事项，但在实施尚未定义的事项之前还需了解要达到的目标。将要达到的目标编制一份编号列表。
2. 定义一项权利，代表编号列表中的一项。可以创建无值权利和有值权利。可从外部查询中获取有值权利的值，它们可以由管理员定义，或以自由格式存在。请参见 “权利示例，协助创建个人权利”在第 158 页 中的示例。
3. 将策略添加到 Identity Manager 驱动程序中，以实施所设计的权利。要创建 Identity Manager 驱动程序的策略，需要熟悉 XSLT 或 DirXML 底稿、已连接系统处理和接收信息的方式、以及 Novell® eDirectory™ 储存信息的方式。如果您不是一位优秀的 DirXML* 编程人员，请把这项工作交给顾问处理。
4. 设置一个管理代理以授予或取消权利。如果希望自动处理，需使用基于职能的权利；如果希望手工处理，请使用基于工作流程的配置信息提供。

6.2.1 预配置支持权利的 Identity Manager 驱动程序

Identity Manager 中包含多个具有预配置的驱动程序，这些预配置中已包含权利和实施权利的策略， Identity Manager 中还有允许监听权力活动的驱动程序。最初安装驱动程序时必须启用权利，这样预配置要素才能成为驱动程序的一部分。以下驱动程序具有支持权利的预配置：

- Active Directory*
- Exchange
- GroupWise®

- LDAP
- NIS
- Lotus* Notes*
- NT 域
- RACF

这些预配置的驱动程序已完成了以上四步的前三步。驱动程序中包含的权利示例的类型可用于大多数常用方案：授予和取消用户帐户、组和电子邮件分发列表。其中包括：

- Active Directory：授予和取消帐户、组成员资格和 Exchange 邮箱
- Exchange 5.5：授予和取消邮箱和组成员资格
- GroupWise：授予和取消帐户，授予和取消分发列表中的成员
- LDAP：授予和取消用户帐户
- Linux* 和 UNIX*：授予和取消帐户
- Lotus Notes：授予和取消用户帐户和组成员资格
- NT 域：授予和取消用户帐户和组成员资格
- RACF：授予和取消组帐户和组成员资格

如果这些权利和策略示例可以满足您的需要，即可直接使用；也可对其进行修改以满足您的需要，还能以此为例，通过 iManager 或 Designer 自己创建权利和策略。需要重申的是，若要使用预配置驱动程序中的权利，最初在 Designer 或 iManager 中创建预配置驱动程序时，必须启用权利；以后将无法添加预配置的权利，除非重新创建驱动程序。

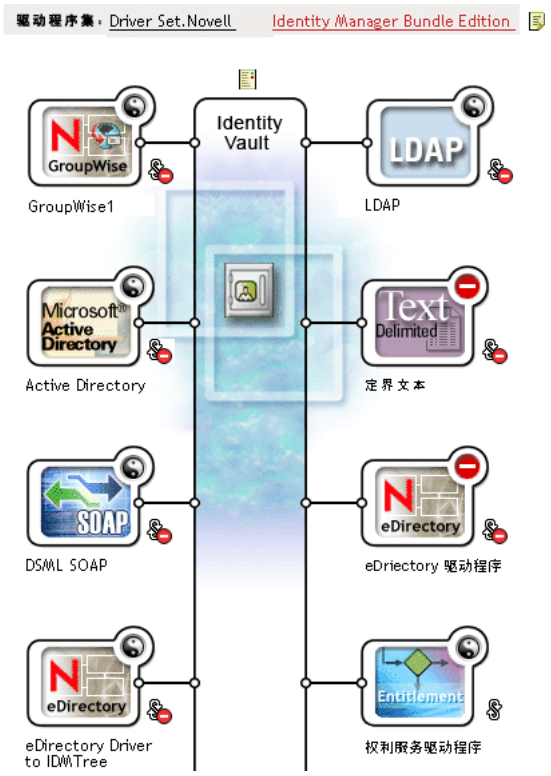
如果要在 Identity Manager 3 中使用那些已在 Identity Manager 2.x 中使用的权利，请运行 "Identity Manager 实用程序 " 下的 " 升级权利 " 选项。

6.2.2 启用其它 Identity Manager 驱动程序中的权利

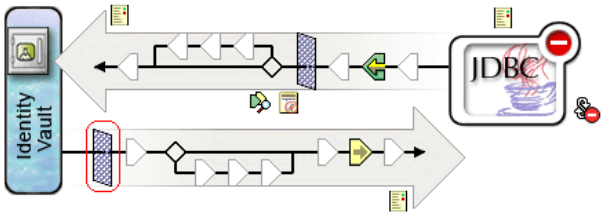
也可以使用不包含权利预配置的 Identity Manager 驱动程序中的权利。要启用驱动程序，使其支持权利，请将 DirXML-EntitlementRef 特性添加到驱动程序过滤器中。要进行设置，请执行以下操作：

1. 选择 "Identity Manager">"Identity Manager 概述 "。
2. 浏览该驱动程序所在的驱动程序集，并单击 " 搜索 "。

3. 在 "Identity Manager 概述 " 屏幕中，选择出现的驱动程序集中的驱动程序对象。



4. 双击驱动程序集中的驱动程序，调出此驱动程序的屏幕。单击 Identity Vault 右侧的 " 驱动程序过滤器 " 图标 （红线圈住的部分）。



5. 在 " 过滤器 " 页中，选择 " 添加特性 "，然后滚动至底部并选择 " 显示所有特性 "。选择 *DirXML-EntitlementRef* 特性，然后单击 " 确定 "。

6. 选择 " 过滤器 " 页中的 *DirXML-EntitlementRef*。选择 " 订购 " 标题下的 " 通知 "。单击 " 确定 "。

7. 如果使用 Designer 在驱动程序上创建权利，将自动执行此进程。

6.3 权利的前提条件

- ❑ eDirectory 8.7.3 或更高版本
- ❑ Identity Manager 2 或 3
- ❑ 权利服务驱动程序

  在使用权利的每个驱动程序集中都必须具有一个权利服务驱动程序。因此需要对每个驱动程序集进行简单的一次性设置。
- ❑ 支持权利的驱动程序配置

在已连接系统中使用权利之前，请执行以下其中一项操作：

- 导入驱动程序的 Identity Manager 驱动程序配置，并指定该驱动程序已启用权利。
- 启用驱动程序对权利的支持。要进行设置，请执行以下操作：
  a. 使用 iManager 或 Designer 创建权利 （建议使用 Designer）。
  b. 将 DirXML-EntitlementRef 特性添加到驱动程序过滤器中，详情请见 “启用其它 Identity Manager 驱动程序中的权利”在第 147 页 。
  c. 编写策略，实施第 1 步中创建的权利。

6.4 通过 iManager 使用 XML 编写权利

为了更好地了解权利中的内容，可以查看已启用权利的预配置驱动程序 Active Directory (AD) 中的权利和策略。其中包括检查 Novell 的权利 DTD （文档类型定义），并查看根据 DTD 编写权利的 XML 示例。

本节包括：

6.4.1 启用权利后 Active Directory 驱动程序添加的内容

启用权利的 AD 驱动程序的结构发生以下改变：

- 将 DirXML-EntitlementRef 特性添加到驱动程序过滤器中。DirXML-EntitlementRef 特性允许驱动程序过滤器监听权利活动。
- 创建用户帐户权利。用户帐户权利授予或取消用户在 Active Directory 中的帐户。授予帐户后，即为用户提供了一个已启用的登录帐户。取消帐户后，登录帐户会被禁用或删除，具体取决于驱动程序的配置方式。
- 创建组成员资格权利。组权利授予或取消 Active Directory 的组中的成员资格。该组必须与 Identity Vault 中的组相关联。取消成员资格后，会从该组中去除该用户。组成员资格权利不在发布者通道上实施；如果通过某些外部工具将用户添加到 Active Directory 的受控组中，该用户将不会被驱动程序去除。此外，如果是从用户对象中去除权利，而不是简单地将其取消， AD 驱动程序将不进行任何操作。
- 创建 Exchange 邮箱权利。组权利授予或取消 Microsoft Exchange 中用户的 Exchange 邮箱。
- 将权利信息添加到多项策略中。

以下策略中包含可以使权利正常发挥作用的附加规则：

- 输入转换（驱动程序级别）。该策略中的 " 检查组成员资格权利添加关联的目标 " 规则可检查组成员资格权利 " 添加关联 " 的目标。在 Active Directory 中，成功创建用户后，才能处理指派给该用户的组成员资格权利。添加关联发出信号，说明 Active Directory 中

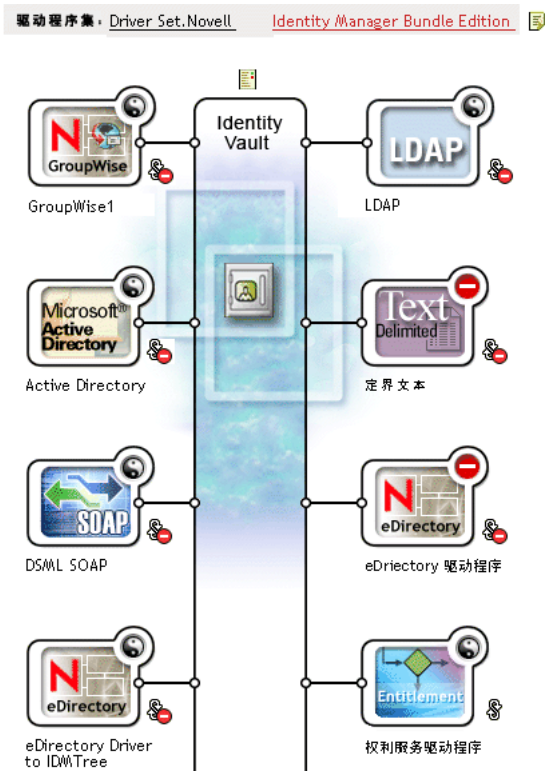
的驱动程序已创建了对象。如果该对象也被标记为需进行组权利处理，则会立即执行处理工作。

- 事件转换 （发布者通道）。该策略中的 " 不允许删除用户帐户 " 规则不允许在 Identity Vault 中删除用户帐户。使用用户帐户权利时，被管理的用户帐户由 Identity Vault 中的权利进行控制。删除 Active Directory 中的帐户不会删除 Identity Vault 中的控制对象。将来对 Identity Vault 中的对象进行更改或合并操作可能导致在 Active Directory 中重新创建该帐户。
- 命令 （订购者通道）。命令策略包含以下与权利有关的规则：
  - " 用户帐户权利更改 （删除选项） " 规则。此用户帐户权利在 Active Directory 中授予用户一个已启用的帐户。取消此项权利会禁用或删除 Active Directory 帐户，具体操作取决于取消帐户权利 全局变量所选的值。更改权利并选择了 " 删除 " 选项时，将执行此规则。
  - " 用户帐户权利更改 （禁用选项） " 规则。此用户帐户权利在 Active Directory 中授予用户一个已启用的帐户。取消此项权利会禁用或删除 Active Directory 帐户，具体操作取决于取消帐户权利 全局变量所选的值。更改权利并选择了 " 禁用 " 选项时，将执行此规则。
  - " 检查对授予或取消的组成员资格的用户修改 " 规则。
  - " 检查对授予或取消的 Exchange 邮箱的用户修改 " 规则。
- 匹配 （订购者通道）。以下为帐户权利：该策略的 " 不要匹配现有的帐户 " 规则。使用 Identity Manager 用户应用程序中的用户帐户权利或使用基于职能的权利时，通过授予或取消该权利即可创建和删除 （或禁用）帐户。如果在 Active Directory 中未对用户授权帐户，默认策略将不匹配 Active Directory 中现有的帐户。若要将权利策略应用于 Active Directory 中的匹配帐户，请修改或去除此规则。这可能导致删除或禁用 Active Directory 帐户。
- 创建 （订购者通道）。创建策略以下与权利有关的规则：
  - 帐户权利：未授予权利时阻止帐户创建。使用 Identity Manager 用户应用程序中的用户帐户权利或使用基于职能的权利时，仅为特别授予此帐户权利的用户创建帐户。如果未授予此权利，该规则将禁止创建用户帐户。
  - 如果未禁用登录则启用 Identity Vault 帐户。
  - 添加之后准备检查组权利。在添加完成之后处理组权利，因为添加的对象只有存在才能被添加到组中。添加操作以操作属性为标志，添加操作处理完成时将在输入转换中检查此属性。
  - 添加之后发送需要检查 Exchange 权利的信号。
  - 将用户名映射到 Windows 登录名称。如果将 userPrincipalName 配置为遵循 eDirectory 用户名，请将 userPrincipalName 设置为 eDirectory 对象名称加上 Active Directory 的域名。

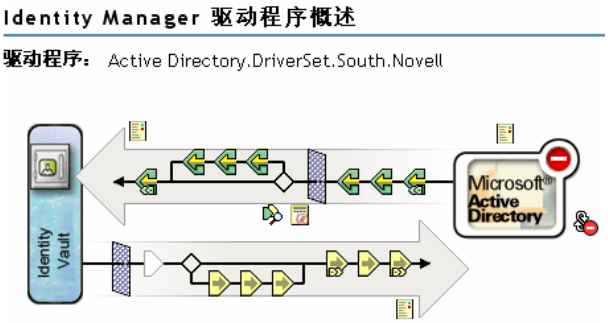
在 iManager 中执行以下步骤，可以查看每个策略的实际 XML 代码：

1. 选择 "Identity Manager">"Identity Manager 概述 "。
2. 浏览该驱动程序所在的驱动程序集，并单击 " 搜索 "。

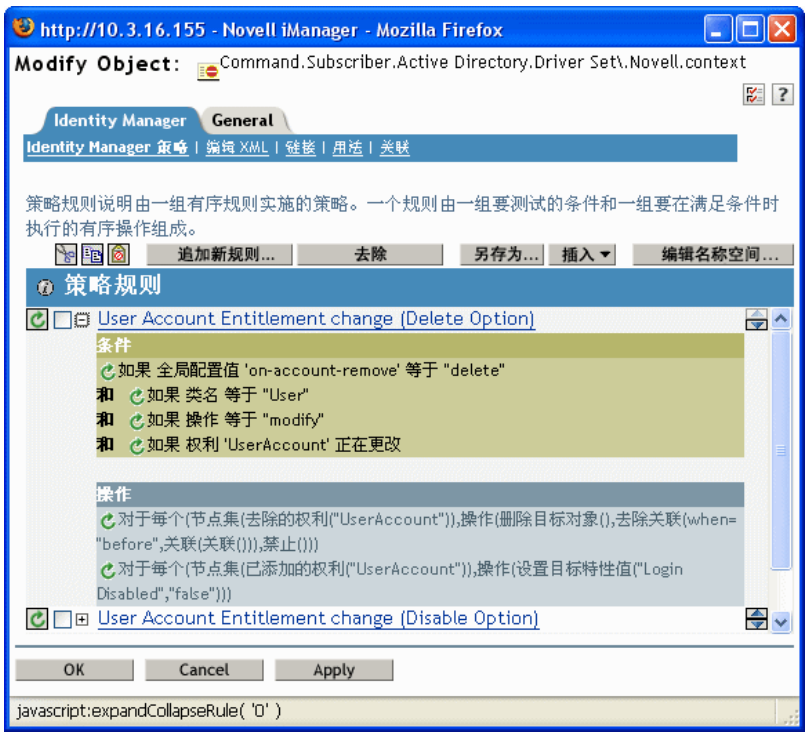
3. 在 "Identity Manager 概述 " 页中，选择显示出的驱动程序集中的驱动程序对象。



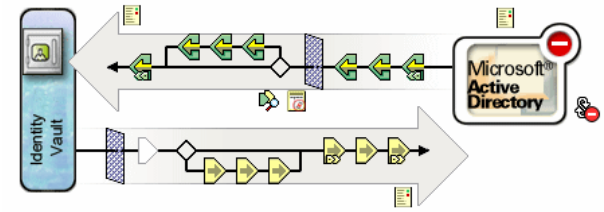
4. 双击驱动程序集中的驱动程序，调出驱动程序页。单击位于驱动程序中央的 " 查看所有策略 " 图标 （红线圈住的部分）。



5. 从 " 显示所有策略 " 屏幕中选择了一项策略后，即可查看构成该策略的条件和操作。



6. 要查看该策略的实际 XML 代码，请从下拉菜单 （此菜单为 Identity Manager 策略的默认菜单）中选择 " 编辑 XML"。有关创建和编辑策略的信息，请参见 《策略构建器和驱动程序自定义指南》，以及针对特定驱动程序构建策略的 Identity Manager 驱动程序指南 (http://www.novell.com/documentation/dirxmldrivers/index.html)。
7. 要查看已启用权利的预配置驱动程序 （示例为 Active Directory）中提供的权利，请遵循第 1 步到第 4 步。同时请选择此驱动程序中央的 " 查看所有权利 " 图标 （红线圈住的部分）。



8. 在 " 管理权利 " 页上，单击权利名称，在 XML 查看器中调出此权利。要编辑权利的代码，请单击 " 启用 XML 编辑 "。

已启用权利的 Active Directory 驱动程序具有以下三个权利：用户帐户、组和 Exchange 邮箱。

图 *6-1 AD* 驱动程序中的权利

可以在 “权利示例，协助创建个人权利”在第 158 页 中查看这些作为编写样本的权利的 XML 代码。

6.4.2 使用 Novell 的权利文档类型定义 (DTD)

在已启用权利的驱动程序上具有一些预定义的权利。可以直接使用这些权利，也可以在 iManager 或 Designer 中创建自己的权利。若要创建自己的权利，可用以下 Novell 权利 DTD 作为创建权利的示例。

此 DTD 的解释还附带有四个示例，来说明如何以此 XML 格式通过 iManager 编写权利。如果不想在 XML 格式上伤太多脑筋，可以使用 Designer 中的 " 权利向导 "，以一种更简单的方式创建权利。

Novell 的权利 DTD

```
<!-************************************************************->
<!-- DirXML Entitlements DTD <!-- Novell Inc. <!-- 1800 South Novell
Place <!-- Provo, UT 84606-6194 <!-- Version=1.0.0 <!-- Copyright 2005
Novell, Inc. All rights reserved --> <!--
********************************************************** --> <!--
Entitlement definition stored in the XmlData attribute of a DirXML-
Entitlement object. --> <!ELEMENT entitlement (values?)> <!ATTLIST
entitlement conflict-resolution (priority | union) "priority" display-
name CDATA #REQUIRED description CDATA #REQUIRED > <!ELEMENT values
(query-app | value+)?> <!ATTLIST values multi-valued (true | false)
"true" > <!ELEMENT value (#PCDATA)> <!ELEMENT query-app (query-xml,
result-set)> <!ELEMENT query-xml ANY> <!ELEMENT result-set (display-
name, description, ent-value)> <!ELEMENT display-name(token-attr |
token-src-dn | token-association)> <!ELEMENT ent-value (token-
association | token-src-dn | token-attr)> <!ELEMENT description
(token-association | token-src-dn | token-attr)> <!ELEMENT token-
association EMPTY> <!ELEMENT token-attr EMPTY> <!ATTLIST token-attr
attr-name CDATA #REQUIRED > <!ELEMENT token-src-dn EMPTY> <!--
Entitlement reference stored in the DirXML-EntitlementRef attribute of
a DirXML-EntitlementRecipient or a DirXML-SharedProfile object. -->
<!ELEMENT ref (src?, id?, param?)> <!ELEMENT param (#PCDATA)>
<!ELEMENT id (#PCDATA)> <!ELEMENT src (#PCDATA)> <!-- Entitlement
```

```
result stored in the DirXML-EntitlementResult attribute of a DirXML-
EntitlementRecipient object. --> <!ELEMENT result(dn, src, id?,
param?, state, status, msg?,timestamp)> <!ELEMENT dn (#PCDATA)>
<!ELEMENT state (#PCDATA)> <!ELEMENT status (#PCDATA)> <!ELEMENT msg
ANY> <!ELEMENT timestamp (#PCDATA)> <!-- Cached query results stored
in the DirXML-SPCachedQuery attribute of a DirXML-Entitlement object.
--> <!ELEMENT items (item*)> <!ELEMENT item (item-display-name?, item-
description?, item-value)> <!ELEMENT item-display-name (#PCDATA)>
<!ELEMENT item-description (#PCDATA)> <!ELEMENT item-value (#PCDATA)>
<!-- Representation of a DirXML-EntitlementRef within the DirXML
Script and within the operation-data of an operation in an XDS
document. --> <!ELEMENT entitlement-impl (#PCDATA)> <!ATTLIST
entitlement-impl name CDATA #REQUIRED src CDATA #REQUIRED id CDATA
#IMPLIED state (0 | 1) #REQUIRED src-dn CDATA #REQUIRED src-entry-id
CDATA #IMPLIED >
```

6.4.3 权利 DTD 的说明

权利 DTD 分为五部分：定义、参照、结果、已超速缓存的查询和内部参照信息。标题仅为可选的注释。在 DTD 中，权利定义的标题为：

<!-- Entitlement definition stored in the XmlData attribute of a DirXML-Entitlement object. -->

标题后跟要素 (ELEMENT) 和特性列表 (ATTLIST)。以下为权利定义标题下各要素和特性的详细说明，这些标题是创建权利时需注意的主标题。

<!ELEMENT entitlement (values?)>

根级别要素为 <entitlement>，它包含一个单一可选的子 <values> 要素。后面为特性列表，其中包括冲突解析、显示名称和说明。冲突解析使用 Priority 或 Union 特性值。

conflict-resolution (priority | union) "priority"

基于职能的权利使用冲突解析确定有值权利多次应用于同一对象时将发生的情况。例如，假设用户 U 是权利策略 A 和权利策略 B 的一个成员，这两个策略均参照同一个有值权利 E，但值集却不相同。权利策略 A 的权利 E 具有值（a、b、c）。权利策略 B 的权利 E 具有值集（c、 d、 e）。

冲突解析特性可决定用户 U 将应用哪组值。如果设置为 union，则将两组值（a、 b、 c、 d、 e）都赋予用户 U。如果设置为 priority，用户 U 仅能获取一组值，具体获取哪组值取决于哪个权利策略优先级更高。

如果是单值权利，则必须通过优先级解决冲突，因为合并值可能导致同时应用多个值。目前基于职能的权利使用此特性，将来工作流程权利也可能使用它。

display-name CDATA #REQUIRED description CDATA #REQUIRED

权利的文字名称并非权利必须显示的内容。Display-name （显示名称）和 Description （说明）特性用于终端用户的显示。 （在 Designer 中，可选择使用权利的显示名称而不使用权利的实际名称。）

<!ELEMENT values (query-app | value+)?> <!ATTLIST values multi-valued (true | false) "true"

<values> 要素是可选的，表示某权利有值。如果不使用此要素，则意味着权利无值。有值权利的一个示例是授予分发列表的权利。无值权利的一个示例是在应用程序中授予帐户的权利，例如 Active Directory 驱动程序提供的用户帐户权利。

有值权利的值有以下三个来源。一个来源为外部应用程序 （由 <query-app> 要素指定）。另一个来源是列举值的预定义列表 （一个或多个 <value> 要素）。第三个来源是权利客户程序（不含子 <value> 的 <values> 要素）。这些示例有助于说明值的工作方式。

有值的权利可能为单值或多值，默认为多值。权利客户程序有责任实施此限制。

<!ELEMENT value (#PCDATA)>

权利值为未键入的字符串。

<!ELEMENT query-app (query-xml, result-set)>

如果这些值来自外部应用程序 （例如电子邮件分发列表），则必须通过 < query-xml> 要素指定应用程序查询，并通过 <result-set> 要素抽取查询结果。在“示例 2：应用程序查询权利：外部查询”在第 159 页 中有两个示例。

<!ELEMENT query-xml ANY>

XML 查询为 XDS 格式。<query-xml> 命令用于从已连接应用程序中查找和读取对象。DirXML 规则和对象迁移等的功能取决于驱动程序对查询命令的实施情况。有关 XML 查询的更多信息，请参见有关查询的 Novell 开发者文档 (http://developer.novell.com/ndk/doc/dirxml/dirxmlbk/ref/ndsdtd/query.html)。

<!ELEMENT result-set (display-name, description, ent-value)> <!ELEMENT display-name(token-attr | token-src-dn | token-association)> <!ELEMENT ent-value (token-association | token-src-dn | token-attr)> <!ELEMENT description (token-association | token-src-dn | token-attr)> <!ELEMENT token-association EMPTY> <!ELEMENT token-attr EMPTY> <!ATTLIST token-attr attr-name CDATA #REQUIRED

可使用结果集要素协助解释外部应用程序查询的结果。存在三条相关的数据：值的显示名称（display-name 子要素）、值的说明 （description 子要素）以及未显示的权利文字值 （ent-value 子要素）。

令牌要素 <token-src-dn>、 <token-association> 和 <token-attr> 为 XPATH 表达式的实际占位符，该表达式抽取了 src-dn 特性值、关联值或 XDS 格式的 XML 文档中分别出现的任意特性值。DTD 假定查询结果为 XDS 格式。

DTD 中的其它标题

权利 DTD 中的其余权利标题可提供不同的功能，但并非创建权利时需关注的项目。

<!-- Entitlement reference stored in the DirXML-EntitlementRef attribute of a DirXML-EntitlementRecipient or a DirXML-SharedProfile object. -->

储存在 DTD 权利参照部分的信息指向权利对象。该信息由管理代理置于此处 （例如，基于职能的权利驱动程序，Entitlement.xml ；或批准流程驱动程序，UserApplication.xml）。这是一个触发事件，用于在已连接系统中触发一项操作。无需对此标题下的 DTD 进行任何操作，但可以使用此信息确保正在参照此权利对象。

<!-- Entitlement result stored in the DirXML-EntitlementResult attribute of a DirXML-EntitlementRecipient object. -->

权利结果部分报告了是否授予或取消权利的结果。该信息包括此事件的情形和状态，以及授予或取消事件的时间 （通过时戳）。无需对此标题下的要素和特性进行任何操作。

<!-- Cached query results stored in the DirXML-SPCachedQuery attribute of a DirXML-Entitlement object. -->

权利查询部分包含从外部应用程序搜集到的权利值。如果权利客户程序需要显示此信息，则可以再次使用此信息。这些值储存在权利对象的 DirXML-SPCachedQuery 特性中。无需对此标题下的要素和特性进行任何操作。

<!-- Representation of a DirXML-EntitlementRef within the DirXML Script and within the operation-data of an operation in an XDS document. -->

由于 DTD 定义了多个文档的值，因此 EntitlementRef 部分实际上不是权利定义的一部分。无需对此标题下的要素和特性进行任何操作。

6.4.4 通过 Designer 创建权利

虽然 “在 iManager 中创建和编辑权利”在第 157 页 中的示例显示了编写权利的实际 XML 代码，但编写权利更便捷的方法是使用 Identity Manager 附带的 Designer 实用程序。将 Identity Manager 驱动程序添加到 Designer 的建模程序中的 Identity Vault 后，即可在大纲视图中右键单击该驱动程序，并选择 " 添加权利 "。" 权利向导 " 会提示您指定所需的权利类型、之后协助您逐步创建权利。

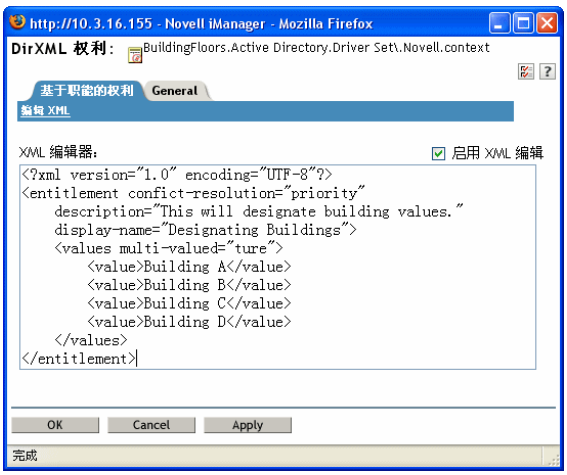
有关使用 " 权利向导 " 的更多信息，请参见 《Designer for Identity Manager 3：管理指南》。

6.4.5 在 iManager 中创建和编辑权利

虽然建议使用 Designer 中的 " 权利向导 " 创建权利，但也可以通过 iManager 创建权利。

1. 选择 Identity Manager 实用程序标题下的 " 创建权利 " 选项。
2. 在 " 创建权利 " 页中，键入权利的名称，然后使用 " 对象浏览器 " 查找该权利所属的 Identity Manager 驱动程序对象。

3. 如果选中 " 定义附加属性 "，则出现 "XML 编辑器 " 页，可在其中定义此权利的要素。



4. 选中 " 启用 XML 编辑 "，将要素添加到权利中。

注释：最好不要更改权利名称。如果随后更改权利名称，还需要更改实施此权利的策略中的所有参照。权利名称储存在此策略内的 Ref 和 Result 特性中。

6.4.6 权利示例，协助创建个人权利

可以创建两种类型的权利：无值和有值。有值权利可从外部查询、管理员定义的列表获取值，或获取自由格式的值。以下是可以创建的四类权利的示例。

注释：如果看到一行代码前没有小于号 (<)，则意味着这行代码已换行，而信息通常显示在一行代码中，而不是两行 （或三行）。另请记住，除了帐户权利，其余权利只是可创建的各类有值权利的示例。

示例 **1**：帐户权利：无值

```
<?xml version="1.0" encoding="UTF-8"?> <entitlement conflict-
resolution="priority" description="This is an Account Entitlement"
display-name="Account Entitlement"/>
```

在此示例中，无值权利的名称为 Account。接下来是默认设置为 Priority 的冲突解析行，在大多数情况下，这意味着如果基于职能的权利使用该权利，该值将设置为具有优先级的 RBE。 （但是，由于这是无值权利的示例，将不应用有值设置。）权利说明为 This is an Account Entitlement，且显示名称为 Account Entitlement。该信息为创建帐户权利所需的所有内容，随后还可以使用它授予应用程序中的帐户。

已启用权利的 Active Directory 驱动程序具有用户帐户权利， Active Directory 使用该权利授予或取消用户帐户。

```
<?xml version="1.0" encoding="UTF-8"?> <entitlement conflict-
resolution="union" description="The User Account entitlement grants or
denies an account in ActiveDirectory for the user. When granted, the
```

```
user is given an enabled logon account.When revoked, the logon account
is either disabled or deleted depending on how the drive is
configured."display-name="User Account Entitlement"
name="UserAccount"> </entitlement>
```

在此示例中，冲突解析为 Union，允许权利合并所赋的值。（再次重申，有值设置不能应用于无值权利。）" 说明 " 字段解释了此权利的用途以及创建原因。将来对此权利进行修改时，该信息将非常有用。此权利的实际名称为 UserAccount，而 <display-name> 在管理代理中显示为 User Account Entitlement。

示例 **2**：应用程序查询权利：外部查询

已启用权利的 Active Directory 驱动程序中包含的组权利和 Exchange 邮箱权利提供了应用程序查询的示例。如果需要已连接系统提供外部信息执行事件，请使用此权利类型。

```
<?xml version="1.0" encoding="UTF-8"?> <entitlement conflict-
resolution="union" description="The Group Entitlement grants or denies
membership in a group in Active Directory. The group must be associated
with a group in the Identity Vault. When revoked, the user is removed
from the group. The group membership entitlement is not enforced on the
publisher channel: If a user is added to a controlled group in Active
Directory by some external tool, the user is not removed by the driver.
Further, if the entitlement is removed from the user object instead of
being simply revoked, the driver takes no action."   display-
name="Group Membership Entitlement" name="Group"> <values> <query-app>
<query-xml> <nds dtd-version="2.0"> <input> <query class-name="Group"
scope="subtree"> <search-class class-name="Group"/> <read-attr attr-
name="Description"/> </query> </input> </nds> </query-xml> <result-
set> <display-name> <token-src-dn/> </display-name> <description>
<token-attr attr-name="Description"/> </description> <ent-value>
<token-association/> </ent-value> </result-set> </query-app> </values>
</entitlement>
```

在本示例中，如果对同一对象多次应用组权利，此权利将使用 Union 来解决冲突。Union 特性合并了涉及到的所有基于职能的权利策略中的权利，所以当某一策略取消一项权利而另一策略授予这项权利时，最终会授予这项权利。

组说明十分有用，因为其细节说明了通过驱动程序策略中的规则所设置的内容。本说明是一个不错的示例，其中包括定义权利时需要首先考虑的细节。

<display-name> 是组成员资格权利，出现在管理代理（例如基于职能权利的 iManager）中。该名称是权利的相对判别名 (RDN)。如果没有定义显示名称，则权利的名称就是它的 RDN。

初始查询值将在树的顶端查找组的类名称，如果没有找到则在其子树中继续查找。这些值属于已连接 Active Directory 服务器，应用程序查询从 <nds> 标签位置开始。在 <query-xml> 标签下，此查询将接收到与以下内容类似的信息：

```
<instance class-name="Group" src-dn="o=Blanston,cn=group1">
<association>o=Blanston,cn=group1</association> <attr attr-
name="Description"> the description for group1</attr> </instance>
<instance class-name="Group" src-dn="o=Blanston,cn=group2">
<association>o=Blanston,cn=group2</association> <attr attr-
```

```
name="Description"> the description for group2</attr> </instance>
<instance class-name="Group" src-dn="o=Blanston,cn=group3">
<association>o=Blanston, cn=group3</association> <attr attr-
name="Description"> the description for group3</attr> </instance> <!--
... ->
```

而在 <result-set> 标签下，查询得到的信息将填充各字段。例如，<display-name> 字段将接收 o=Blanston,cn=group1。<description> 字段将接收 the description for group1， <ent-value> 字段将接收 o=Blanston,cn=group1。由于存在多个组并且不止一个组符合查询准则，因此还要收集此信息并以其它实例来显示。

注释 **:** 因为每个外部系统的关联格式值是唯一的，所以查询每个外部系统所用的格式和语法都不同。

另一个示例是 Exchange 邮箱权利。

```
<?xml version="1.0" encoding="UTF-8"?> <entitlement conflict-
resolution="union" description="The Exchange Mailbox Entitlement
grants or denies an Exchange mailbox for the user in Microsoft
Exchange." display-name="Exchange Mailbox Entitlement"
name="ExchangeMailbox"> <values> <query-app> <query-xml> <nds dtd-
version="2.0"> <input> <query class-name="msExchPrivateMDB" dest-
dn="CN=Configuration," scope="subtree"> <search-class class-
name="msExchPrivateMDB"/> <read-attr attr-name="Description"/> <read-
attr attr-name="CN"/> </query> </input> </nds> </query-xml> <result-
set> <display-name> <token-attr attr-name="CN"/> </display-name>
<description> <token-attr attr-name="Description"/> </description>
<ent-value> <token-src-dn/> </ent-value> </result-set> </query-app> </
values> </entitlement>
```

在本示例中，如果对同一对象多次应用 Exchange 邮箱权利，此权利将使用 Union 来解决冲突。Union 特性合并了涉及到的所有基于职能的权利策略中的权利，所以当某一策略取消一项权利而另一策略授予这项权利时，最终会授予这项权利。

而说明对于此权利的作用进行了足够详尽的说明，描述了此权利可以授予或取消 Microsoft Exchange 用户的 Exchange 邮箱。出现在管理代理 （例如，基于职能权利的 iManager）中的显示名称为 Exchange Mailbox Entitlement。该名称是权利的相对判别名 (RDN)。如果没有定义显示名称，则权利的名称就是它的 RDN。

初始查询值将寻找 msExchPrivateMDB 类名称，它是一个 Microsoft Exchange 函数调用，先在 " 配置 " 树枝中进行寻找，如果没有找到将在子树中继续寻找。这些值属于已连接的 Active Directory 数据库，应用程序查询从 <nds> 标签位置开始。msExchPrivateMDB 类在 eDirectory 中没有等效类，所以熟悉 Microsoft Exchange 函数调用才能进行这样的查询。但是由于在 Active Directory 驱动程序中已经找到了规则和策略，所以该查询已经完成。

权利用户可以使用通过查询检索到的信息。例如，通过 DirXML-EntitlementRef 特性可以将权利值 (ent-value) 传递给 Identity Manager 策略。显示名称和说明信息可通过 iManager 或用户应用程序显示，并且储存在 DirXML-SPCachedQuery 特性中。

示例 **3**：管理员定义的权利：带有列表

第三个示例是由管理员定义的权利，使用该权利可以在选择某一列表项后创建授予事件或取消事件。

```
<?xml version="1.0" encoding="UTF-8"?> <entitlement conflict-
resolution="union" description="This will show Administrator-defined
Values"> <display-name="Admin-defined Entitlement"/> <values multi-
valued="true"> <value>Building A</value> <value>Building B</value>
<value>Building C</value> <value>Building D</value> <value>Building
E</value> <value>Building F</value> </values> </entitlement>
```

在本示例中，权利名称是 Admin-defined，而定义的显示名称是 Admin-defined Entitlement。（如果您希望权利的显示名称与 RDN 不同，只需要输入显示名称即可。）Conflict-resolution 行显示了 Union 设置，该设置允许权利合并所赋的值。

权利说明是 *This will show Administrator-defined Values*。多值特性设置为 true，允许此权利多次赋值。在本示例中，值是公司的大厦字母：从 Building A 到 Building F。然后，通过权利客户程序 （例如， iManager RBE 任务）或通过用户应用程序，用户或已定义的任务管理员可以指定大厦信息，该信息将包括在外部应用程序中 （例如， Novell eDirectory）。

示例 **4**：管理员定义的权利：不带列表

第四个示例是管理员定义的权利，在权利授予或取消某事件之前，强制管理员键入一个值。如果在初始设置时信息不全，无法创建任务列表，就可以使用此种权利。

```
<?xml version="1.0" encoding="UTF-8"?> <entitlement conflict-
resolution="priority" description="There will be no pre-defined list">
<values multi-valued="false"/> </entitlement>
```

在本示例中，权利名称为 Admin-defined (no list)，由于没有显示名称项，将使用权利名称作为显示名称。冲突解析将再次设置为默认的 Priority，这意味着如果基于职能的权利使用该权利，该值将设置为具有优先级的 RBE。通过权利客户程序 （例如， iManager RBE 任务）或通过用户应用程序，可以指定大厦信息，该信息包括在外部应用程序中 （例如，eDirectory）。

6.4.7 完成权利创建步骤

权利创建示例已经说明了如何创建和使用权利的前两步，详情请见 “创建权利：概述”在第 146 页 。其中包括：第 1 步，列出希望使用权利完成的任务清单；第 2 步，编写权利，处理清单中的项目。第 3 步，创建 Identity Manager 驱动程序策略 （本章不作介绍）。有关创建和编辑策略的信息，请参见 《策略构建器和驱动程序自定义指南》以及相应的 Identity Manager 驱动程序指南 (http://www.novell.com/documentation/idmdrivers/index.html)。

创建权利 （或使用某些 Identity Manager 驱动程序中预配置的权利）后，需要对权利进行管理（见第 4 步）。权利可由两个包或代理进行管理：作为基于职能的权利策略通过 iManager 进行管理，或在基于工作流程的配置信息提供中通过用户应用程序进行管理。有关基于工作流程的配置信息提供中使用的权利，请参见“基于工作流程的配置信息提供的介绍”。本章的剩余部分重点介绍基于职能的权利。

6.5 管理基于职能的权利概述

- “权利服务驱动程序如何运行”在第 162 页

一般来说，已连接系统中的权利是在每个驱动程序中分别管理的，这些权利通过创建和编辑驱动程序配置策略 （如使用策略构建器创建的策略）来进行管理。在这种传统的分布式模型中，通常由另一个管理员控制每个 Identity Manager 驱动程序和已连接系统，并且在每个已连接系统驱动程序的驱动程序配置策略中，确定用户在该系统中是否可以获得资源的业务策略是分别进行 " 硬编码 " 的。

基于职能的权利模型适合于那些一个或几个管理员有权控制权利策略的环境。这种管理员只需要大体了解 Identity Manager，没有必要掌握大量使用基于职能的权利界面所需的 Identity Manager、 XSLT 或 DirXML 底稿专业知识。

如果满足准则，基于职能的权利策略将允许自动授予或取消业务资源。权利就像访问资源的许可证。具有许可证，就有权访问指定资源，没有许可证，则无权访问。您可以指定以下有效示例：如果用户满足准则 1、 2 和 3，就能通过基于职能的权利策略成为 H 组的成员；但如果用户满足准则 4 和 5，他 （她）将成为 I 组的成员。

可以通过以下三步设置管理基于职能的权利：

1. 如果还没有设置，请启用 Identity Manager 驱动程序对象中的 DirXML-EntitlementRef 特性，详情请见 “启用其它 Identity Manager 驱动程序中的权利”在第 147 页 。
2. 安装权利服务驱动程序 (Entitlement.xml) 的步骤详见 “创建权利服务驱动程序对象”在第 163 页 。
3. 在 iManager 中创建基于职能的权利策略，详情请见 “创建权利策略”在第 164 页 。

6.5.1 权利服务驱动程序如何运行

基于职能的权利依赖于权利服务驱动程序 (Entitlement.xml)。此驱动程序是一种引擎服务，用来监视用户在一项权利策略中是否具有成员资格。如果用户符合权利策略动态组的动态成员资格准则，或已静态地属于该组，则权利服务驱动程序将更新用户对象 DirXML-EntitlementRef 特性的信息。

对于 “预配置支持权利的 Identity Manager 驱动程序”在第 146 页 中所列的系统，在导入 Identity Manager 驱动程序配置时可以启用权利。Identity Manager 中包含多个具有预配置的驱动程序，这些预配置中已包含权利和实施权利的策略， Identity Manager 中还有允许监听权力活动的驱动程序。您可以审阅所提供的策略。这些策略通过监视 DirXML-EntitlementRef 特性以及授予或取消权利来支持权利。

仅在发生以下状况之一时，权利服务驱动程序才更新 DirXML-EntitlementRef 特性：

- 使用再评估成员资格任务
- 指定在树的哪一部分对用户进行再评估
- 已移动用户
- 已对用户进行重命名
- 权利策略中成员资格所使用的某一特性已修改

可使用权利策略在已连接系统中授予权利，还可以在 Identity Vault 中授予权限。已连接系统中的权利可以是以下任意一项：

- 帐户

- 电子邮件分发列表中的成员资格
- 组成员资格
- 已连接系统中相应对象的特性 （由指定值填充）
- 位置
- 自定义的其它权利

在已启用权利的驱动程序配置中，对可以通过权利进行创建的某些选项进行了说明。

因为每个驱动程序集中仅使用一个权利服务驱动程序，所以权利策略只能管理与此驱动程序集关联的服务器中位于读 / 写复本或主复本中的用户。

基于职能的权利策略功能基于 Identity Manager。因此，要管理已连接系统，必须正确安装和配置 Identity Manager 驱动程序以及所安装的 Identity Manager 插件。

另外，为避免权利策略指派和 Identity Manager 驱动程序配置之间可能发生的冲突，应该注意业务策略以及如何通过 Identity Manager 对其进行管理。Identity Manager 权利策略和驱动程序配置中的策略在管理某个特性时不应重叠或冲突。

6.6 创建权利服务驱动程序对象

在创建权利策略之前，需要权利服务驱动程序对象。必须为每个驱动程序集创建一个权利服务驱动程序对象。

如果没有此对象，在单击基于职能的权利职能和任务时将提示您创建。

1 确定是否已有权利服务驱动程序。

在 iManager 中，单击 *Role-Based Entitlements* （基于职能的权利） >" 基于职能的权利 "，然后选择驱动程序集。

- 如果出现 " 无权利服务驱动程序 " 页，请继续执行步骤 2，以创建权利服务驱动程序对象。
- 如果出现带有权利策略列表的 " 基于职能的权利 " 页，则表示已有权利服务驱动程序对象。不需要完成此过程。单击 “创建权利策略”在第 164 页 继续。

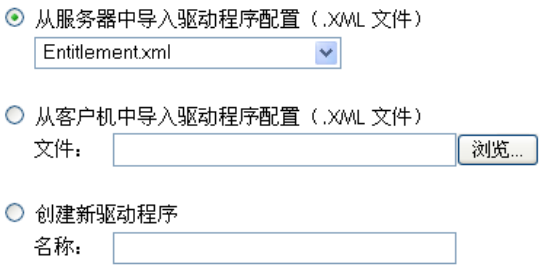
2 在 " 无权利服务驱动程序 " 页中，单击 " 是 "。

出现 " 创建驱动程序向导 "。

还可以单击 "DirXML 实用程序 ">" 导入驱动程序 "。

3 在 " 创建驱动程序向导 " 页中，选择 " 在现有驱动程序集中 "，然后单击 " 下一步 "。

4 在 *Import a Driver Configuration from the Server (.XML file)*（从服务器中导入驱动程序配置（.XML 文件））下拉列表中，选择 *Entitlement.xml*。



5 为权利服务驱动程序对象命名（或使用默认名称），然后单击 " 下一步 "。

将自动选择正确的驱动程序配置文件。只需为驱动程序对象命名或使用默认名称。

6 建议您定义安全性等效并且排除管理员职能。为这两个选择添加用户 Admin，然后单击 " 下一步 "。

7 审阅摘要，然后单击 " 完成 "。

默认情况下，在安装 Identity Manager 时，将安装权利驱动程序的驱动程序 Shim。在 iManager 服务器上安装 Identity Manager 插件时，默认安装权利驱动程序配置文件。

完成向导后，可以访问权利的插件，并且可以开始为此驱动程序集创建基于职能的权利策略。

6.7 创建权利策略

- “定义权利策略的成员资格”在第 166 页
- “选择权利策略的权利”在第 167 页

要创建权利策略，可以使用所提供的向导。

1 确保已经设置了权利服务驱动程序并创建了必要的驱动程序配置。

2 在 iManager 中，单击 " 基于职能的权利 ">" 基于职能的权利 "。

3 选择一个驱动程序集。

每个驱动程序集只能有一个权利策略。

将打开现有的权利策略列表，与下图中显示的页面类似。如果是第一次使用基于职能的权利，则列表中没有策略。

4 单击 " 新建 "。

" 权利策略向导 " 打开。

5 根据向导中的第 1 步至第 6 步创建新策略。有关向导中每一步骤的信息，请参考联机帮助。

5a 第 1 步，对策略进行命名和说明。

5b 第 2 步，定义成员资格过滤器 （搜索参数）。

5c 第 3 步，通过在搜索准则中包括和排除成员，定义静态成员。

5d 第 4 步，选择 Identity Manager 驱动程序并提供所包括的权利。在 “通过 iManager 使用 XML 编写权利”在第 150 页 中创建权利。单击 " 添加驱动程序 "，然后选择要添加的权利。

5e 第 5 步，浏览并找到希望此权利策略成为受托者的对象。

5f 第 6 步，读取摘要以确保此权利策略执行正确操作。如果正确，请单击 " 完成 "；如果不正确，请单击 " 返回 "。

6 权利策略创建完成后会关闭权利服务驱动程序。请单击 " 重启动 " 完成该会话。

6.7.1 定义权利策略的成员资格

和 Identity Manager 驱动程序一样，每个权利策略仅能管理该策略所指派的服务器的主复本或读 / 写复本中的对象。每个权利策略都和被指派给某个特定服务器的单个驱动程序集对象关联。

仅有用户对象 （以及从用户类衍生出的其它对象类型）可以成为权利策略的成员。要转至权利策略中的 " 成员资格 " 页，请选择 " 基于职能的权利 ">" 基于职能的权利 "，然后在权利策略列表中突出显示要编辑的权利策略，并选择 " 编辑 "。在 Internet Explorer 浏览器中，选择 " 成员资格 " 选项卡，在 Firefox 浏览器中，从下拉菜单中选择 " 编辑动态成员 "。

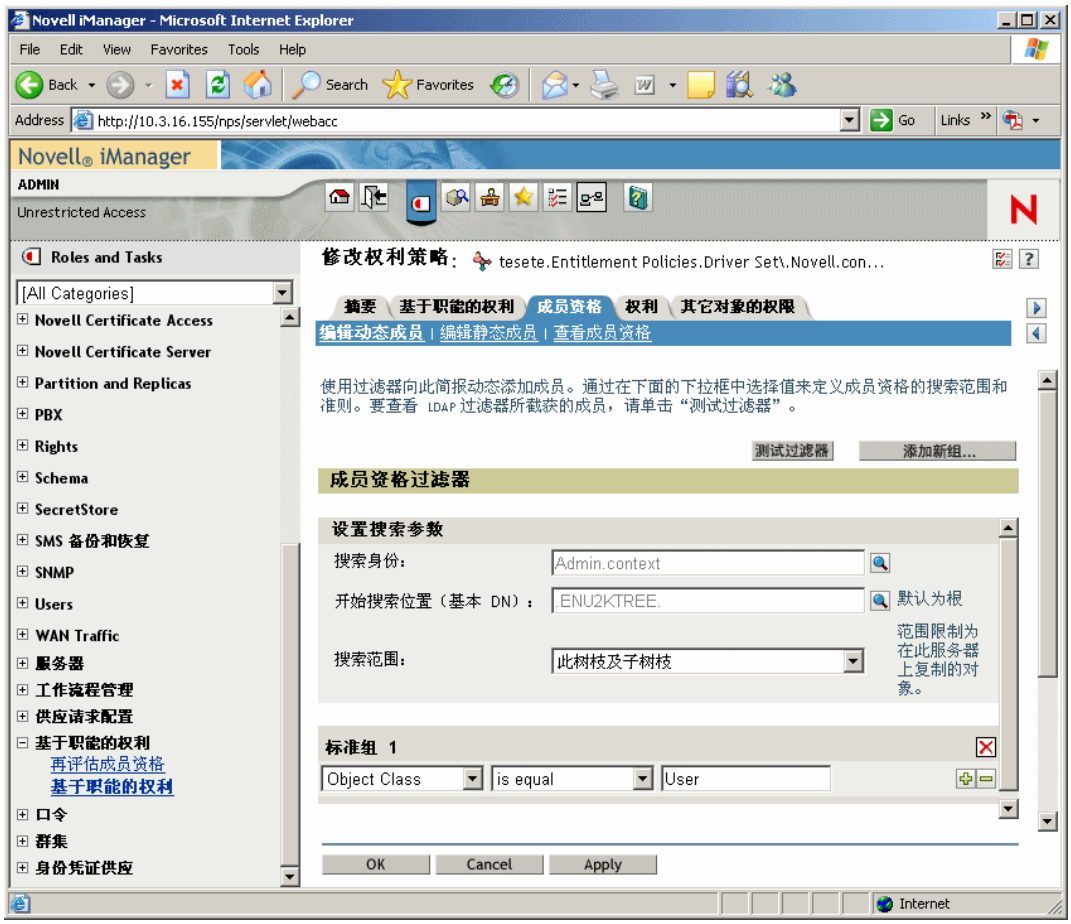
权利策略是动态组对象。可以使用动态和静态两种方式定义权利策略的成员资格。还可以在同一个权利策略中使用这两种方式。

- 动态： 可以根据对象特性值定义成员资格的准则，例如，作业标题中是否包括 "Manager"。所指定的准则将转换到 LDAP 过滤器中。

  满足此准则的用户将自动成为权利策略的一部分，而不需要将每个用户专门添加到该策略中。动态成员资格和动态组对象相同。

如果更改对象使其不再满足动态成员资格准则，将自动取消权利。

图 *6-2* 编辑动态和静态成员



- 静态： 除了创建动态成员资格的准则 （LDAP 过滤器），还可以包含或排除特定的用户。

  可以静态添加不满足过滤器准则的成员。还可以排除满足过滤器准则但不应包含在权利策略中的成员。

6.7.2 选择权利策略的权利

- “已连接系统中的帐户”在第 168 页
- “电子邮件分发列表和 NOS 列表中的成员资格”在第 169 页
- “已连接系统的特性值”在第 170 页

使用权利可以授予或取消对已连接系统的服务和 Identity Vault 中的权限的访问权。

所安装的已启用权利的驱动程序带有一个权利列表，可使用权利策略指派这些权利。还可以自己创建可在权利策略中使用的权利。驱动程序能够提供的权利是该驱动程序的子对象，它是由驱动程序开发者创建的，代表了驱动程序和已连接系统的功能。

Identity Vault 中对象的受托者权限将直接授予权利策略的成员。默认情况下，在第二次为用户修改权利策略成员资格的特性时，或将用户移至不同的树枝或对其重命名时，会将已连接系统中的权利授予权利策略的每个成员。

已连接系统中的权利可以是以下任意一项：

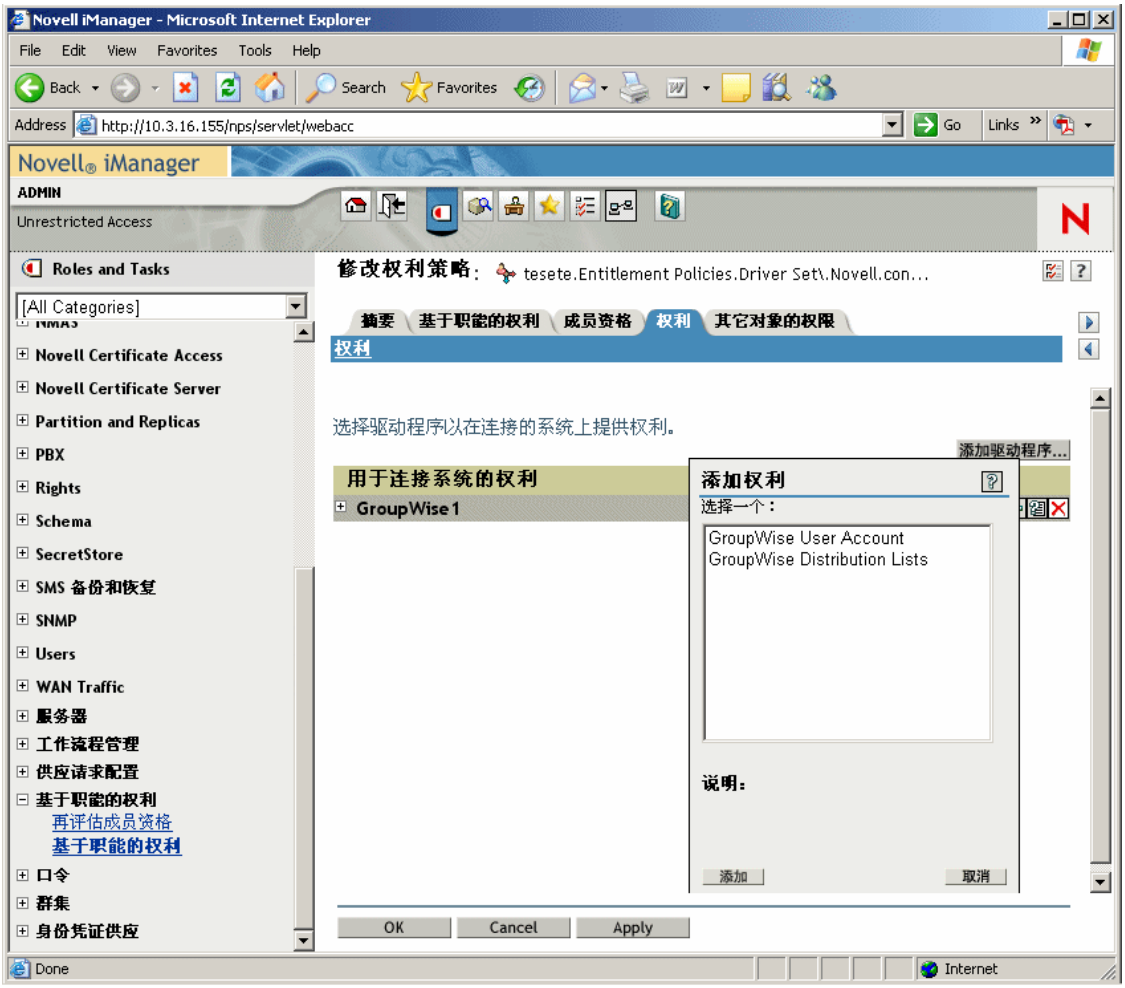
- 帐户
- 电子邮件分发列表中的成员资格
- NOS 列表中的组成员资格
- 已连接系统中相应对象的特性 （由指定值填充）
- 自定义的其它权利

已连接系统中的帐户

要将权利添加至权利策略，请转至 " 权利 " 页并选择一个驱动程序。将弹出一个窗口，显示此驱动程序提供的权利。

例如，在下图中，可以看到 GroupWise 驱动程序所提供的两种权利，列表中的第一个权利是 GroupWise User Account。

图 *6-3* 用于定义权利的界面



电子邮件分发列表和 **NOS** 列表中的成员资格

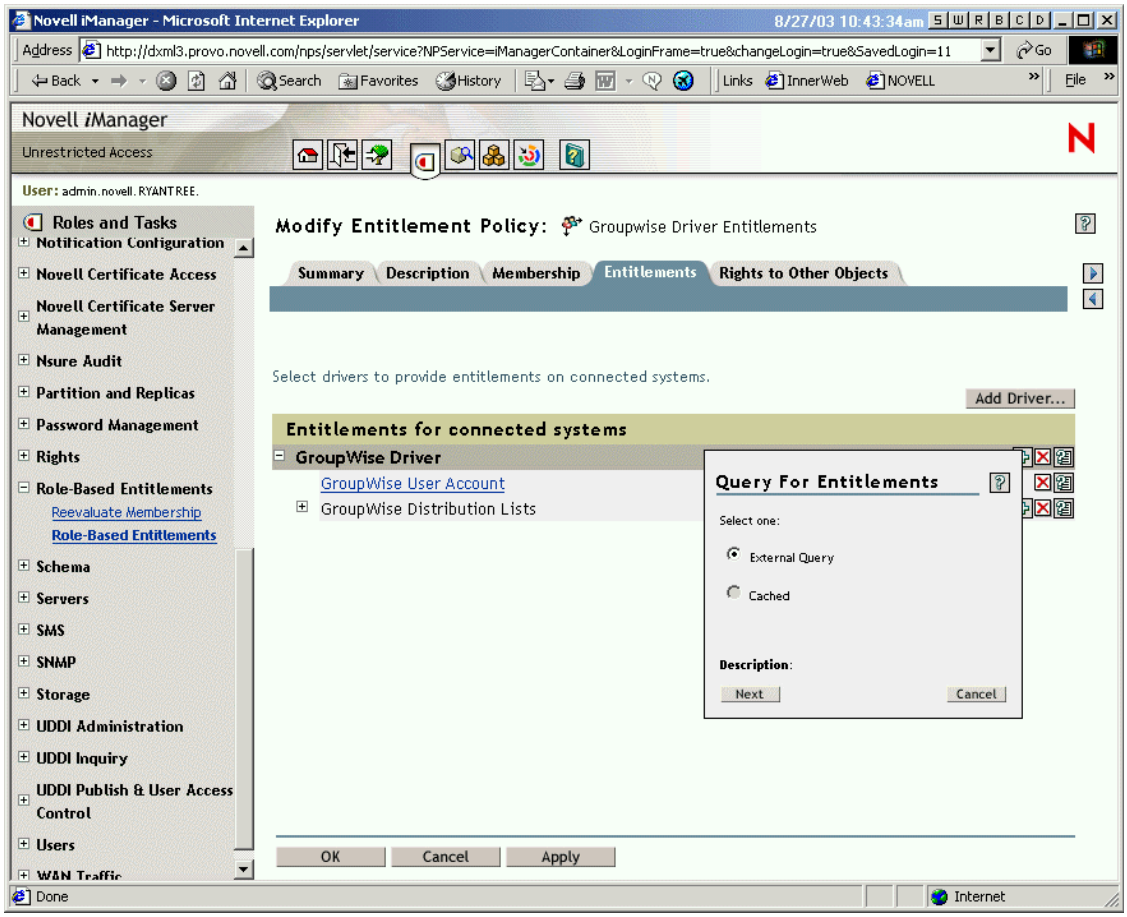
要在已连接系统的组中指派成员资格，请从该驱动程序所提供的权利列表中选择成员资格权利。

在下图的示例中， GroupWise Distribution Lists 位于列表中的第二位。

图 ***6-4*** 选择 *GroupWise Distribution Lists*

如果在本示例中选择 *GroupWise Distribution Lists*，将显示一个查询弹出窗口 （如下图中的示例所示）。

图 ***6-5*** 查询权利



" 权利策略 " 界面可以查询电子邮件分发列表或 NOS 列表的列表。执行查询后，可以选择查看超速缓存列表。

已对驱动程序进行配置，使其可返回完整列表，所以可以从已连接系统现有的列表中进行选择。

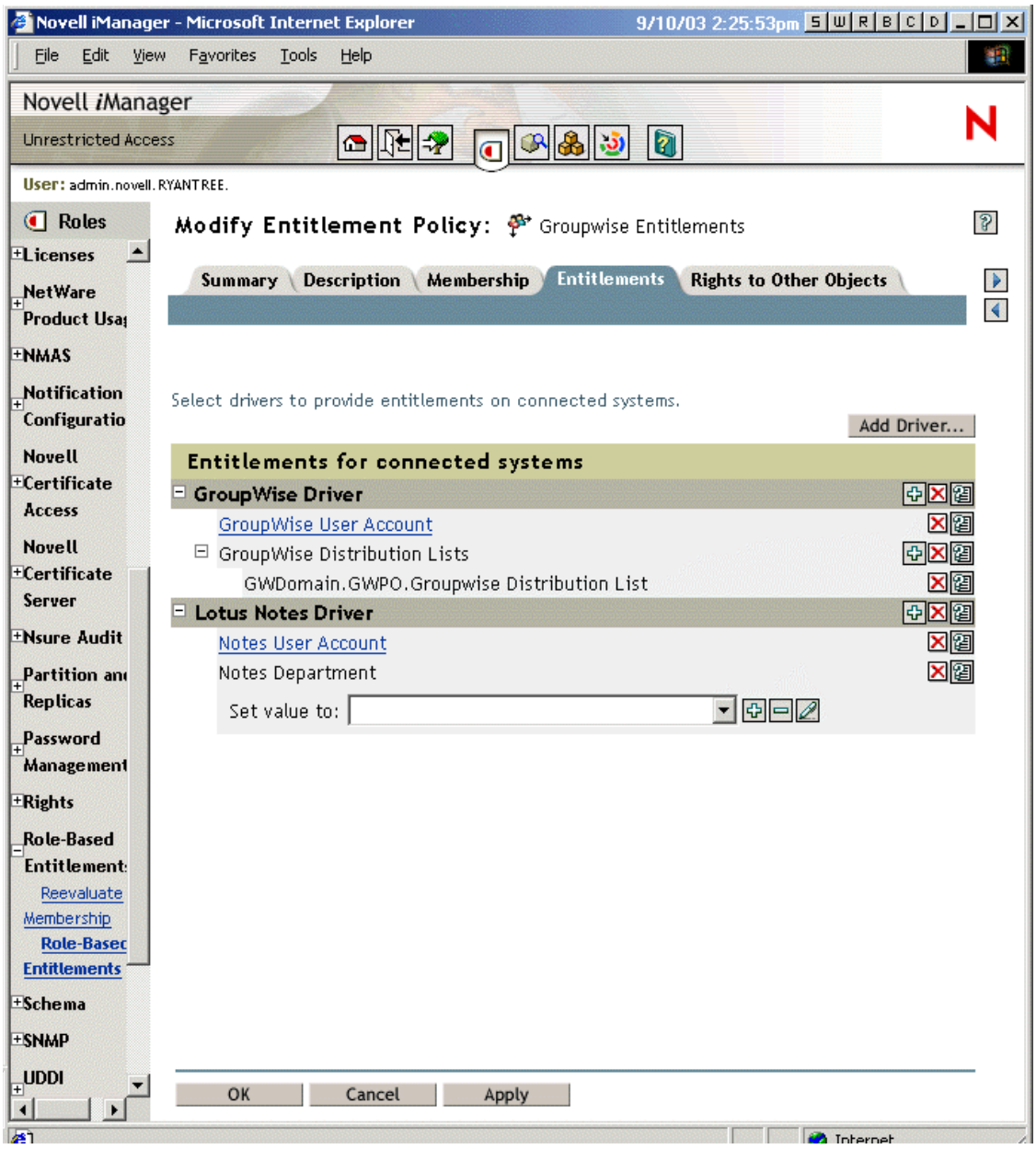
注释：可以自定义驱动程序，来限制所指定的组名称列表，而不是令查询返回完整列表。

已连接系统的特性值

可以为已连接系统中的用户帐户指派特性值。可以在该界面中键入希望用户帐户具有的值。

下图显示了为 Notes 特性添加特性值 Department 的示例。

图 *6-6* 添加特性值



6.8 基于职能的权利策略之间的冲突解析

- “冲突概述”在第 172 页
- “为个别权利更改冲突解析方法”在第 173 页
- “区分权利策略的优先级”在第 175 页

6.8.1 冲突概述

创建权利策略时，影响特定用户的多项策略在将权利指派给该用户时可能会发生冲突。

以下是解析冲突的方法。对于某些权利，您可以更改冲突解析。

- 不具有值的权利是加性的。大多数情况下，帐户权利不具有值。如果通过任何权利策略向用户授予已连接系统中的帐户，此用户将在该系统中接收帐户。其它权利策略是否冲突并不重要；因为结果是加性的。

  授予帐户的冲突解析方法始终是不能更改的。

  不具有值的权利就如同电灯开关一样，不是打开就是关闭，如同授予或未授予。

  例如，如果管理员权利策略授予 Jean Chandler 一个 Exchange 帐户，但是 Jean Chandler 却被同样授予 Exchange 帐户的收发室员工权利策略排除在外，则 Jean 仍可以获得 Exchange 帐户。

- 默认情况下，有值权利是加性的，但是可以选择按优先级进行解析。权利 （如组成员资格权利）的值具有组名称列表，或权利的特性具有值。默认情况下，这些权利也是加性的。

  如果需要，可以更改这些权利的冲突解析。

  管理每个权利冲突解析的设置是在该权利中定义的。驱动程序提供的每种权利都分别列在清单中。有值的权利具有冲突解析特性，该特性是单独为每个权利设置的。默认设置为 conflict-resolution="priority"。其它可能的值为 conflict-resolution="union"。

  - **conflict-resolution="union" ---** "Union" 值表示该权利是加性的。将授予用户任何策略中的成员资格所指派的所有权利。不同的权利值将会简单相加，然后用户就可以获得所有值。

    例如，如果 Jameel 是商业展示承包人策略的成员，该策略授予 GroupWise 电子邮件分发列表 （名称为商业展示邮件列表）的成员资格；而在同样也指派电子邮件分发列表 （名称为商业展示邮件列表）的商业展示管理员策略中 Jameel 却被排除在成员资格之外，则他在电子邮件分发列表中仍能接收成员资格。

    再举一例，如果在 AD 组 （名称为收发室全体员工）中通过收发室策略授予 Consuela 成员资格，同样还在 AD 组 （名称为紧急响应）中通过紧急志愿者策略授予 Consuela 成员资格，则在 AD 的两个组中都将授予她成员资格。

    如果这样设置，则策略列表中权利策略的顺序对权利并不重要。

  - **conflict-resolution="priority" ---** "Priority" 值表示如果两个不同策略中的值发生冲突，或者某个策略包含一个用户而其它策略却排除该用户，则授予该用户的权利只是那些位于权利策略列表中较高位置的权利。

    如果使用此设置，之前的示例会有截然不同的结果。

    在以上有关 Jameel 的示例中，如果 GroupWise 电子邮件分发列表权利具有 "priority" 值并且在列表中商业展示管理员策略的位置高于商业展示承包人策略，则在商业展示邮件列表中将不授予 Jameel 成员资格。

    在以上有关 Consuela 的示例中，如果 AD NOS 组成员资格具有 "priority" 值，并且在列表中收发室策略的位置高于紧急志愿者策略，则将仅在收发室全体员工组中授予 Consuela 成员资格。在紧急响应组中将不授予 Consuela 成员资格，因为冲突解析是按优先级进行的，而不是加性的。

    例如，如果对环境进行配置，使用基于职能的权利将用户置于另一系统的分级结构中，此功能会很有用。您一定希望将用户放置在某个位置上，而不是同时置于两个位置。

请牢记，该设置对于每个驱动程序提供的每个权利都是独立的。

作为一般规则，如果使用 "Priority" 设置，在列表中应该将管理员 (administrator) 或管理员 (manager) 策略置于高于终端用户或个别贡献者策略的位置。应该使成员资格限制严格的组高于成员资格限制宽松的组。

6.8.2 为个别权利更改冲突解析方法

1 在 iManager 中，单击 *Identity Manager* >"Identity Manager 概述 "，然后选择驱动程序集。

将显示驱动程序集中所有驱动程序图形展示的页。

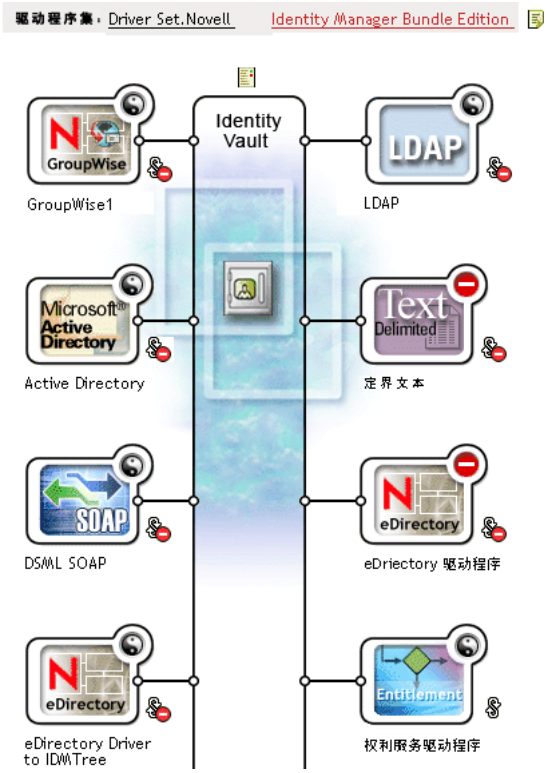
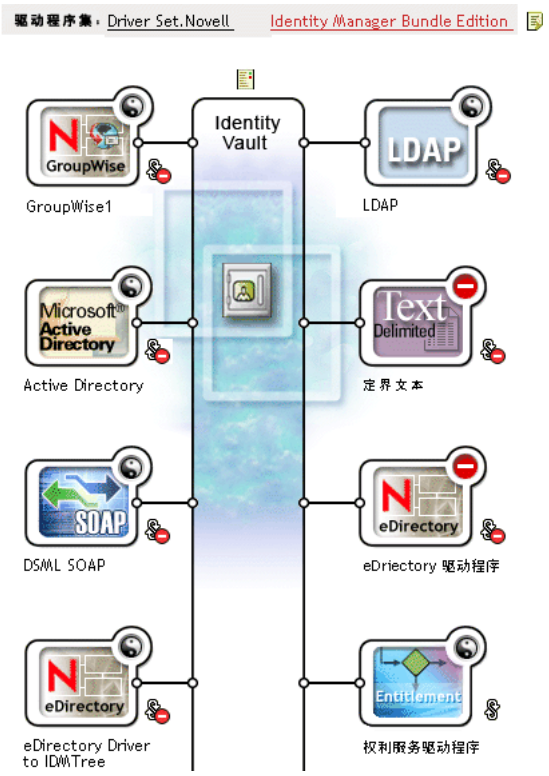


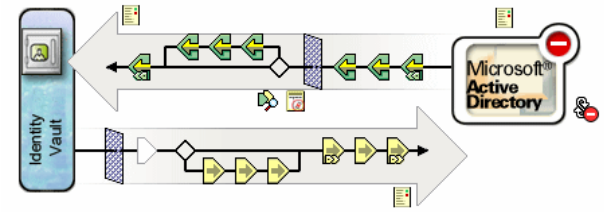
图 *6-7* 驱动程序集



2 单击驱动程序状态按钮并选择 " 停止驱动程序 "。

3 单击驱动程序图标，该驱动程序提供要更改的权利。

将出现显示该驱动程序策略图标和该驱动程序图标的页。在屏幕的中间位置，选择 " 查看所有权利 " 图标 （红线圈住部分）。



4 在 " 管理权利 " 页，单击权利名称，在 XML 查看器中调出此权利。

5 选择 " 启用 XML 编辑 " 复选框。

6 在 XML 中，找出要更改的权利定义。

以下是要查找的行的示例：

```
<entitlement conflict-resolution="union" description="Grants
membership to GroupWise Distribution lists" display-name="GroupWise
Distribution Lists" name="gwDistLists">
```

7 更改 conflict-resolution 值。以下是两个可能的值：

```
conflict-resolution="union"
```

```
conflict-resolution="priority"
```

有关这些值的信息，请参见 “基于职能的权利策略之间的冲突解析”在第 171 页 。

8 单击 " 重启动 "，重启动权利服务驱动程序。

6.8.3 区分权利策略的优先级

默认情况下，不需考虑权利策略列表的顺序。因为 Identity Manager 附带的驱动程序配置将 conflict-resolution="union" 作为每个权利的冲突解析方法。

如果将任何权利更改为 conflict-resolution="priority"，则需要注意权利策略列表的顺序，但只需注意所更改的那些权利。有关这些值的信息，请参见 “基于职能的权利策略之间的冲突解析”在第 171 页 。

使用权利策略列表旁的箭头按钮，可以更改权利策略的顺序。列表中处于第一位置的策略具有最高优先级。

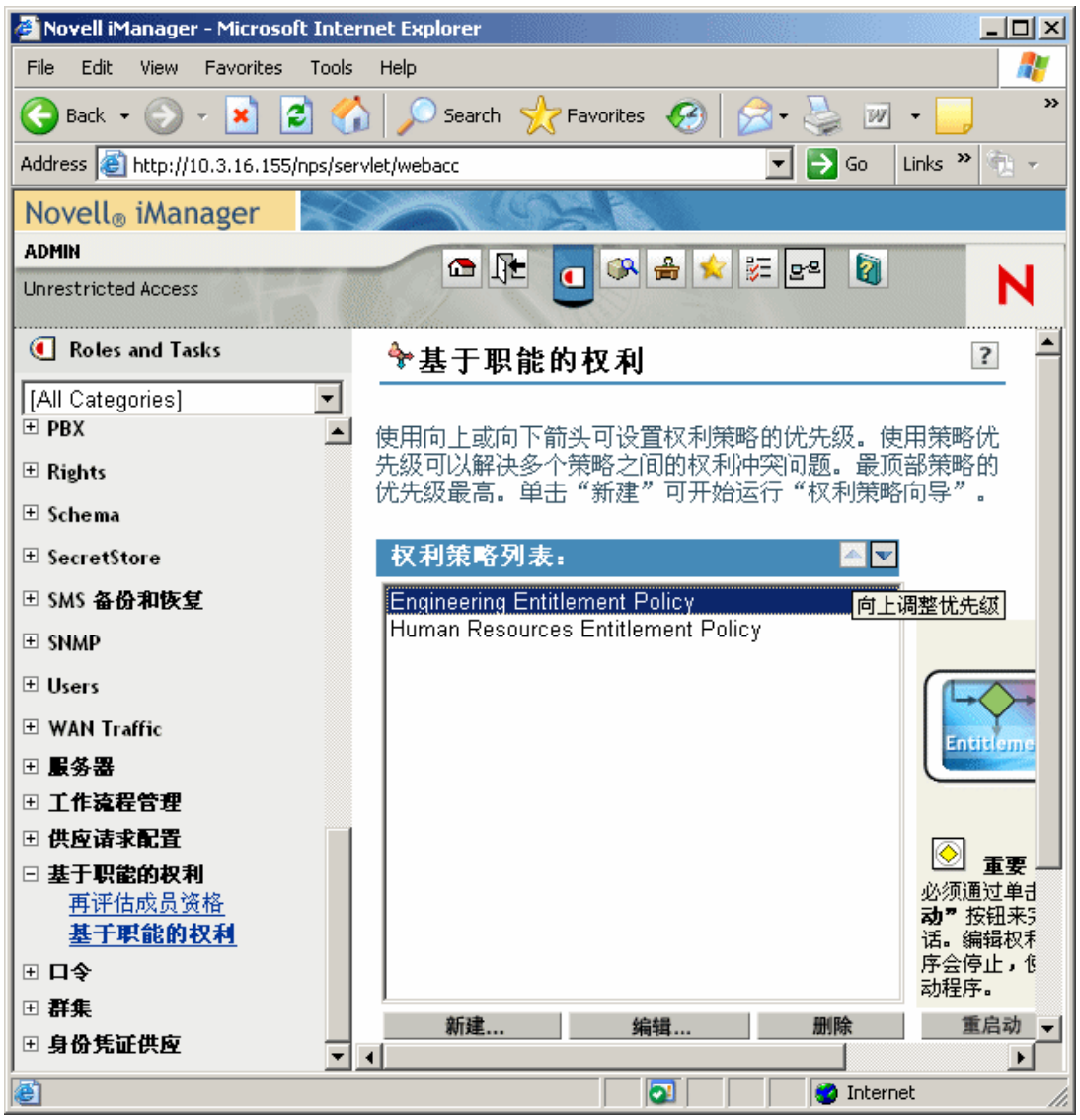
1 在 iManager 中，单击 " 基于职能的权利 ">" 基于职能的权利 "。

2 搜索并选择驱动程序集。

将出现带有权利策略列表的页。

3 使用箭头按钮在列表中将策略向上或向下移动，可更改权利策略的优先级。

将权利策略移动到列表中更高的位置，它就具有了更高的优先级。



4 单击 " 关闭 " 重启动驱动程序。

重启动驱动程序后，优先级更改才能生效。

6.9 对基于职能的权利进行查错

查错时，请牢记以下问题：

- 通过单击策略所在的页中的"新建"、"编辑"或"去除"更改策略时，将停止"权利服务驱动程序 "。只有单击 " 重启动 " 后，才会重启动驱动程序。

  此功能可防止在未完成对策略的更改前，驱动程序在产品环境中授予或取消权利。
- 同样，如果有多个人员同时编辑权利策略，权利服务驱动程序也不会启动。
- 因为每个驱动程序集中仅使用一个权利服务驱动程序，所以权利策略只能管理与此驱动程序集关联的服务器中位于读 / 写复本或主复本中的用户。

6.10 应用于基于职能的权利和基于工作流程的配置信息提供权利的权利要素

以下信息应用于所有权利而不是某个特定的实施。

- “控制授予或取消权利的意义”在第 177 页
- “防止数据丢失”在第 177 页
- “口令同步和权利”在第 177 页

6.10.1 控制授予或取消权利的意义

您可以控制授予或取消权利的结果。每个驱动程序都提供了所支持的选择列表，来控制 " 授予 " 或 " 取消 " 的意义。

例如，当添加 GroupWise 帐户时，可以将授予的实际意义指定为授予用户一个处于禁用状态的帐户，所以在用户可以访问该帐户前，管理员必须进行干预。或者，也可以选择启用该帐户 （此为默认选择）。

默认情况下，驱动程序配置将使用最有可能保留数据的选项。例如，去除 GroupWise 帐户的默认意义是将其设置为 " 禁用 "，这样管理员在对策略进行更改时，如果出现失误，就不会无意地丢失帐户。再举一例， Identity Manager 驱动程序配置不会取消具有其它系统中的用户帐户值的权利。如果在电子邮件分发列表中授予用户成员资格，而不久后该用户不再满足权利策略准则，他 （她）只会失去此成员资格。帐户将被禁用，但不会去除组成员资格和特性值。如果想要一个不同的结果， Identity Manager 专家还可以自定义驱动程序配置。

因为基于职能的权利功能可以在产品环境中对组织的权利进行彻底更改，而不需要在实验室中测试结果，所以对取消权利的解释尤为重要。

您可以在预配置的驱动程序中编辑全局配置变量，以更改授予或取消的解释设置。如果要创建自定义配置，则可以添加 GCV，对授予和取消权利进行解释。

6.10.2 防止数据丢失

依据策略中的成员资格，基于职能的权利允许您对权利 （例如，帐户）进行全面更改。然而，这就意味着要注意更改策略过程中产生的错误。Identity Manager 附带的驱动程序配置采用最佳的设置。您应理解如何使用 GCV 避免无意造成的数据丢失。

例如，建议不要将用于解释撤销帐户权利的 GCV 值设为 delete。

编辑或创建新的权限策略时，可以通过关闭驱动程序来保护数据，这样在完成策略编辑之前将不会进行更改。如果已完成，您可以使用权利策略界面中的 " 重启动 " 按钮，手工重启动驱动程序。同样，如果另一用户正在编辑权利策略，而您尝试使用 " 重启动 " 按钮重启动权利服务驱动程序，则将提示您在另一用户完成更改前不要重启动驱动程序。

6.10.3 口令同步和权利

使用基于职能的权利的驱动程序的口令同步与其它驱动程序的口令同步采用相同的管理方法，详见 “已连接系统间的口令同步”在第 69 页 。

安全性：最佳实践 7

7.1 使用 SSL

只要可能，对于所有传输都应启用 SSL。启用 SSL，在 Metadirectory 引擎与远程装载程序之间进行通讯 （请参见 “提供安全数据传送”在第 43 页），以及在 Metadirectory 引擎或远程装载程序与已连接系统之间进行通讯。

如果不启用 SSL，您将使用明码发送信息 （例如，口令）。

7.2 保证安全访问

确保安全访问 Identity Vault 和 Identity Manager 对象。

物理安全性。 保护已安装 Identity Vault 的服务器的物理位置的访问途经。

访问权限。创建 Identity Manager 对象和配置驱动程序需要管理权限。监视并控制哪些人员有权创建或修改以下内容：

- Identity Manager 驱动程序集
- Identity Manager 驱动程序
- 驱动程序配置对象 （过滤器、样式表、策略），尤其是用于口令检索或同步的策略
- 口令策略对象 （以及编辑口令策略对象的 iManager 任务），因为是由它们来控制哪些口令应彼此同步，以及应使用哪些口令自助服务选项

7.3 管理口令

如果选择在已连接系统间交换信息，应采取预防措施确保信息交换的安全。尤其要确保口令的安全。

- 口令提示特性 (nsimHint) 也可以公开查阅，以便忘记口令的未鉴定用户访问自己的口令提示。口令提示有助于减少服务台呼叫。

  出于安全性考虑，将检查口令提示，以确保其中不包含用户的实际口令。然而，用户仍能够创建可提供大量口令相关信息的口令提示。

  要在使用口令提示时增强安全性：

  - 仅允许在用于口令自助服务的 LDAP 服务器上访问 nsimHint 特性。

- 要求用户收到口令提示前回答询问问题。
- 提醒用户创建只有自己才能理解的口令提示。可通过口令策略中的口令更改讯息进行此操作。请参见 《口令管理管理员指南》(http://www.novell.com/documentation/password_management/index.html) 中的 " 添加口令更改讯息 "。

如果选择完全不使用口令提示，请确保在其它口令策略中也不使用。要防止设置口令提示，可以转到下一步并完全去除提示安装小程序，详见 《口令管理管理员指南》(http://www.novell.com/documentation/password_management/index.html) 中的 " 通过去除提示小程序禁用口令提示 "。

- 询问问题可以公开查阅，以便忘记口令的未鉴定用户通过另一种方式进行鉴定。要求回答询问问题增强了忘记口令自助服务的安全性，因为在接收到忘记的口令或口令提示，或重设置口令之前，用户必须作出正确的响应以证明自己的身份。

  对询问问题实施入侵者锁定设置，这样就可限制入侵者的错误尝试次数。

  然而，用户可创建包含口令暗示的询问问题。提醒用户创建只有自己才能理解的询问问题和答案。可通过口令策略中的口令更改讯息进行此操作。请参见 《口令管理管理员指南》(http://www.novell.com/documentation/password_management/index.html) 中的 " 添加口令更改讯息 "。
- 出于安全性考虑，只有在要求用户回答询问问题的情况下，才可使用通过电子邮件向用户发送口令 和允许用户重设置口令 等忘记口令操作。
- NMAS™ 2.3.4 增强了由管理员更改的通用口令的安全性。该操作与先前为 NDS® 口令提供的功能采用的方式基本相同。

  如果管理员更改了某个用户的口令 （例如，创建新用户或响应服务台呼叫时），并且您已启用使口令策略中口令失效的设置，则该口令将自动失效。口令策略中的此设置位于高级口令规则中，名为 " 口令失效之前的天数 (0-365)"。对于此项特殊功能，天数并不重要，但必须启用此设置。

7.4 创建高强度口令策略

口令策略对象可公开查阅，以便应用程序检查口令是否遵从。这意味着未鉴定用户可查询 Identity Vault 并找出就绪的口令策略。如果口令策略要求用户创建高强度口令，此操作不应该会带来风险，详见 《口令管理管理员指南》(http://www.novell.com/documentation/password_management/index.html) 中的 " 创建强口令策略 "。

Identity Manager 口令同步允许您简化用户口令并减少服务台成本。双向口令同步允许您以多种方式在 eDirectory 和已连接系统间共享口令，详见 “实施口令同步”在第 98 页 中的方案。

使用通用口令和口令策略允许您强制用户采用高强度口令要求。使用口令策略中的高级口令规则，以遵循业界的最佳口令实践。

例如，可要求用户口令遵循以下规则：

- 要求唯一口令。

  可以防止用户重新使用口令，并控制系统要储存在历史表中的口令数量以进行比较
- 要求口令的最少字符数。

  要求较长的口令是使口令强度更高的最好方法之一。
- 要求口令的最少数字个数。

要求口令中至少有一个数字字符，以帮助防止 " 字典攻击 "（入侵者使用字典中的词尝试登录）。

- 排除选择的口令。

  可以排除您认为存在安全性风险的词（例如，公司名称或位置，或词测试或管理）。尽管并非要将整部字典导入排除列表中，排除的词的列表也会很长。切记，冗长的排除列表会使用户登录变慢。防止字典攻击的更好方法可能是要求使用数字或特殊字符。

切记，只要在树的不同部分中存在不同的口令要求，您就可以创建多个口令策略。可以将一个口令指派给整个树、分区根树枝、树枝甚至单个用户。（为了简化管理，建议您尽量在树的高处指派口令策略。）

另外，可以使用入侵者锁定。总之，此 eDirectory 功能允许您指定锁定帐户前允许进行的登录尝试失败的次数。此设置位于父树枝上而不是口令策略中。请参见 *Novell eDirectory 8.7.3* 管理指南 (http://www.novell.com/documentation/edir873/edir873/data/afxkmdi.html#amm7bjv) 中的 " 管理用户帐户 "。

7.5 保护已连接系统的安全

切记，正进行同步数据的已连接系统能够以折中的方式储存或传输此数据。

确保与其进行口令交换的系统的安全。例如，在启用与 LDAP、NIS 和 Windows 系统的口令同步之前，必须考虑这些系统自身的安全要求。

许多软件厂商提供特定的安全性指导，使用他们的产品时应予以遵循。

7.6 Designer for Identity Manager

使用 Designer for Identity Manager 时，请考虑以下问题：

- 监视并控制哪些人有权创建或修改 Identity Manager 驱动程序。

  创建 Identity Manager 对象和配置驱动程序需要管理权限。

- 给予顾问 Identity Vault 管理员口令之前，将指派给管理员的权限限制在此顾问必须访问的树区域中。
- 删除项目文件 (.proj) 或将其保存至公司目录。

  Designer 的 .proj 文件将保留在公司的项目站点中。完成项目后，顾问不应带走这些文件。

- 不再需要项目文件、日志文件和跟踪文件时，请将它们删除。
- 丢弃或转让便携式电脑前，请核实项目文件已清除。
- 确保 Designer 到 Identity Vault 的连接是物理安全的。

  否则，他人可能监听线缆并获取敏感信息。

- 使用文档生成程序创建文档时，请注意这些文档。

  这些文档中可能包含明文形式的口令和敏感数据。

- 如果 Designer 需要读取或写入 eDirectory 特性，请勿将此特性标记为加密。

  Designer 无法读取或写入加密特性。

- 切勿储存口令，它们属于敏感信息。

当前， Designer 项目未进行加密。口令仅进行了编码。因此，不要共享已保存口令的 Designer 项目。

要保存会话口令，但不将其保存到项目中：

a. 在展开的 " 大纲 " 视图中，右键单击 "Identity Vault"。

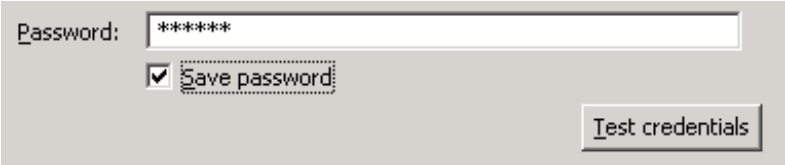
b. 选择 " 属性 "。

c. 在 " 配置 " 页上，键入口令，然后单击 " 确定 "。

每次会话可输入一个口令。关闭此项目后，口令将丢失。

要将口令保存到硬盘驱动器，请完成步骤 1-3，选择 " 保存口令 "，然后单击 " 确定 "。

图 *7-1* 保存口令



7.7 业内最佳安全性实践

遵循业内最佳安全措施实践，例如，锁定服务器上的未使用端口。

7.8 跟踪敏感信息的更改

- “使用 iManager 记录事件日志”在第 182 页
- “使用 Designer 记录事件日志”在第 184 页

7.8.1 使用 iManager 记录事件日志

可以使用 Novell Audit 记录您认为涉及安全性的重要事件的日志。有关 Novell Audit 的信息，请参见第 10 章 “使用 Novell Audit 进行日志记录和报告”在第 205 页 。

例如，通过执行下列操作，您可以记录特定 Identity Manager 驱动程序 （或驱动程序集）口令更改的日志：

1 选择 "eDirectory 管理 ">" 修改对象 ">" 日志级别 "。

根据 iManager 版本，从下拉列表进行选择或选择选项卡。

2 选择 " 日志特定事件 "。

3 要选择特定事件，请单击日志事件图标 。

4 在 " 事件 " 页上，选择以下内容：

- 在 " 操作事件 " 中，选择 " 更改口令 "。

此项可监视对 NDS 口令的直接更改。

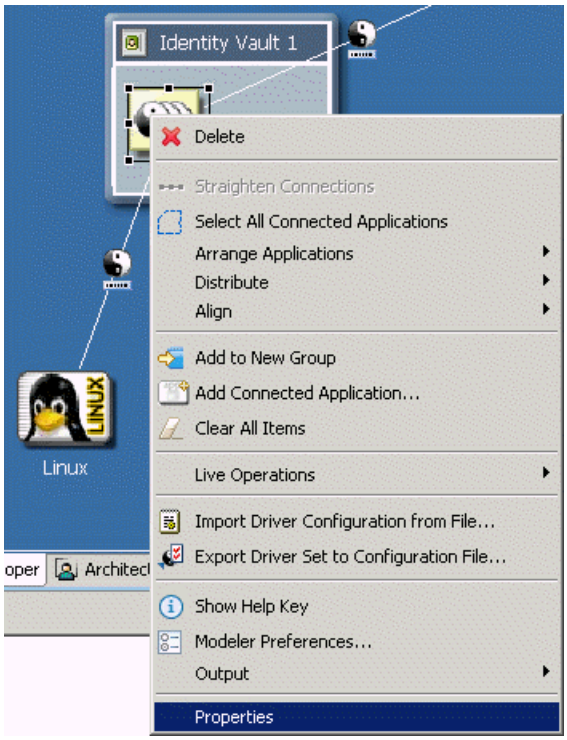
- 在"转换事件"中，选择"口令集"和"口令同步"。这两项监视通用口令和分发口令的事件。

5 单击 " 确定 " 两次。

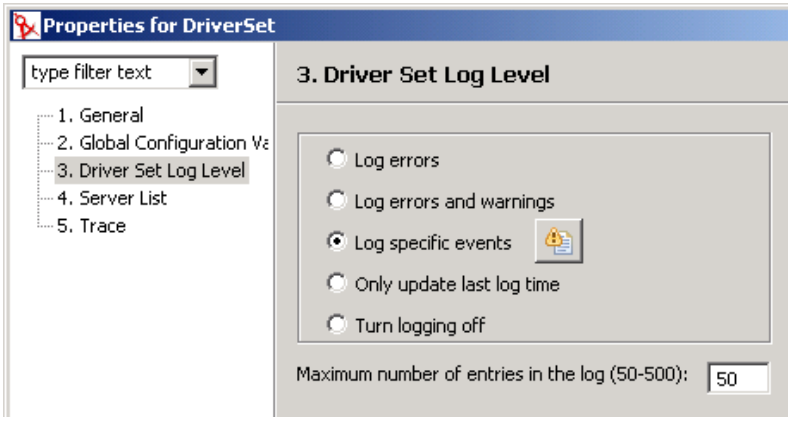
7.8.2 使用 Designer 记录事件日志

可以记录应用于驱动程序集或驱动程序的事件的日志。

记录驱动程序集事件的日志



1 在 Designer 中，右键单击一个驱动程序集，然后选择 " 属性 "。



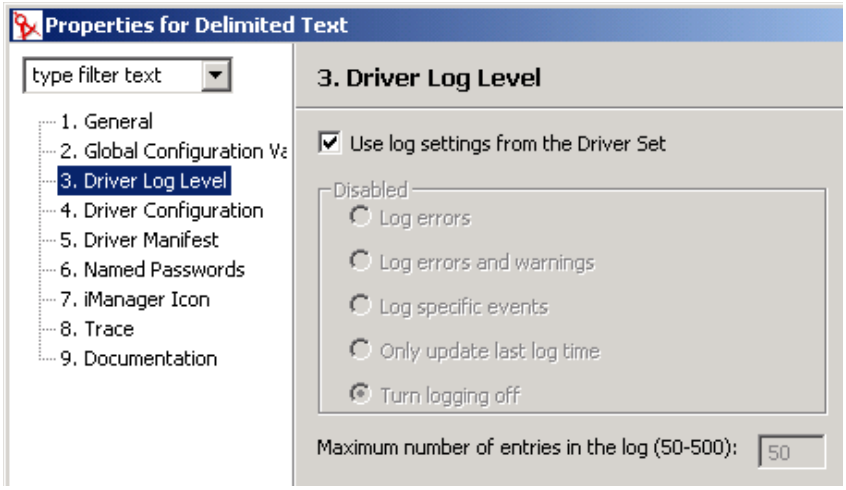
2 选择 *Driver Set Log Level*（驱动程序集日志级别），然后选择 " 日志特定事件 "。

3 单击 " 选择要记录日志的事件 " 图标。

4 选择要记录日志的事件，然后单击 " 确定 "。

记录驱动程序事件的日志

1 在 Designer 中，右键单击一个驱动程序，然后选择 " 属性 "。



2 选择 " 驱动程序日志级别 "，然后选择 " 日志特定事件 "。

若满意，可以保留驱动程序集的设置，然后单击 " 确定 "。否则，请取消选择 " 使用驱动程序集的日志设置 "，选择 " 日志特定事件 "，然后单击 " 确定 "。

3 单击 " 选择要记录日志的事件 " 图标。

4 选择要记录日志的事件，然后单击 " 确定 "。

管理引擎服务

8

下列驱动程序仅用于 Metadirectory 引擎服务，而不能用于外部已连接系统。安装 Identity Manager 时，将自动安装这些驱动程序。

8.1 权利服务驱动程序

请参见第 6 章 “创建及使用权利”在第 145 页 。

8.2 手工任务服务驱动程序

手工任务服务驱动程序用于通知一个或多个用户已发生了一个数据事件，以及是否需要用户进行任何操作。在员工提供的方案中，数据事件可能是新用户对象的创建，而用户操作可能包括：通过将数据输入 eDirectory，或在应用程序中输入数据来指定办公室编号。其它方案包括：通知管理员已创建了新用户对象，通知管理员用户对某个对象进行数据修改等。

配置手工任务服务驱动程序通常包括配置两个既相互独立又相关联的子系统：订购者通道策略和电子邮件模板，以及发布者通道万维网服务器模板和策略。

另外，必须配置驱动程序参数 （例如， SMTP 服务器名称、万维网服务器端口号等）。

本节包括：

8.2.1 安装

- 安装：使用 Identity Manager 安装程序安装 "Metadirectory 服务器 " 选项时，将自动安装手工任务服务驱动程序。
- 平台： 此驱动程序可以在 Identity Manager 和远程装载程序支持的平台上运行。
- 激活： 此驱动程序无需单独激活。激活 Metadirectory 引擎时，也就激活了该驱动程序。

8.2.2 概述

在本节中，您可以查找到有关各个驱动程序功能如何工作的信息。

- “替换标记”在第 191 页
- “替换数据”在第 191 页
- “模板操作要素”在第 191 页
- “订购者通道电子邮件”在第 192 页
- “订购者通道万维网服务器”在第 192 页

操作方式

支持两种主要操作方式：

- 数据直接请求： 发送电子邮件，要求用户将数据输入到 eDirectory （可能供其它应用程序使用）中。电子邮件收件人通过单击邮件中的 URL 来响应此邮件。URL 指向手工任务服务驱动程序发布者通道中运行的万维网服务器。用户随即与万维网服务器所生成的动态万维网页交互，以鉴定到 eDirectory™ 并输入要求的数据。
- 事件通知：向用户发送电子邮件，而不涉及发布者通道。此电子邮件可能只是通告 eDirectory 中发生的某些事件，或是要求通过发布者通道万维网服务器以外的方法 （例如， Novell iManager、其它应用程序或自定义界面）来传输的数据。

示例：订购者通道电子邮件，发布者通道万维网服务器响应

下面是一名员工提供的假设示例，在此示例中新的员工经理给该员工指定一个房间号：

1. 在 eDirectory 中创建一个新用户对象 （例如，通过公司人力资源系统的 DirXML 驱动程序）。
2. 手工任务服务驱动程序的订购者向此用户的经理和经理助理发送一封 SMTP 邮件。此 SMTP 邮件包含引用发布者通道万维网服务器的 URL。此 URL 还包含标识用户和标识那些授权给提交请求数据的数据项。
3. 经理或经理助理单击此电子邮件中的 URL，即在万维网浏览器中显示出 HTML 表格。然后，经理或助理可进行下列操作：
   - 选择其 eDirectory 用户对象的 DN 作为标识此电子邮件响应者的方法。
   - 输入其 eDirectory 口令。
   - 输入新员工的房间号。
   - 单击 " 提交 " 按钮。
4. 新员工的房间号通过手工任务服务驱动程序的发布者通道提交给 eDirectory。

示例：订购者通道电子邮件，无发布者通道响应

下面是一个假设示例，此示例中新员工经理在资产管理系统中给员工指定一台计算机：

1. 在 eDirectory 中创建一个新用户对象 （例如，通过公司人力资源系统的 DirXML 驱动程序）。
2. 手工任务服务驱动程序的订购者向此用户的经理和经理助理发送一封 SMTP 邮件。此 SMTP 邮件包含将数据输入到资产管理系统的指令。
3. 经理或助理将数据输入到资产管理系统中。
4. （可选）计算机的标识数据通过资产管理系统的 DirXML 驱动程序调入到 eDirectory 中。

如何通过手工任务服务驱动程序创建电子邮件和万维网页

电子邮件、 HTML 万维网页和 XDS 文档都可以看作文档。根据提供给驱动程序的信息，手工任务服务驱动程序可以动态地创建文档。

模板是 XML 文档，其内容包括样板文件、文档固定部分以及指示出现动态、替换、结尾部分和构造文档的替换标记。

手工任务服务驱动程序的订购者通道和发布者通道都采用模板来创建文档。其中订购者通道创建电子邮件，而发布者通道创建万维网页和 XDS 文档。

文档的动态部分通过替换数据来提供。订购者通道中的替换数据由订购者通道策略 （例如，命令转换策略）提供。发布者通道中的替换数据是由到万维网服务器的 HTTP 数据提供（URL 数据和 HTTP POST 数据）。手工任务服务驱动程序能自动地提供其已知的特定数据（例如，万维网服务器地址）。

通过 XSLT 样式表处理此模板。这些模板处理用的样式表与订购者或发布者通道中的 DirXML 策略所用的样式表是相互独立的。

替换数据是作为 XSLT 样式表的参数提供。样式表处理输出的是一个 XML、 HTML 或文本文档 （用作电子邮件正文、万维网页或发布者通道中 DirXML 提交内容）。

替换数据通过电子邮件中的 URL，从订购者通道传送到发布者通道。URL 具有一个包含替换数据项的查询部分。

对于创建电子邮件文档、 HTML 文档和 XDS 文档，手工任务服务驱动程序所附带的预定义样式表足以对模板进行处理。如果需要，还可以编写其它自定义样式表提供其它处理选项。

创建文档也有高级的方法，此方法只使用一个 XSLT 样式表和替换数据。不涉及到任何模板。然而，因为模板方法无需具备 XSLT 编程知识，并且配置和维护更简单，因此本指南将采用模板方法。

模板

本节描述文档创建模板 （如手工任务服务驱动程序中所用）。

模板是 XML 文档，此文档通过样式表处理以便生成输出文档。此输出文档可以是 XML、HTML 或纯文本 （或通过 XSLT 生成的其它格式）。

模板用于在订购者通道上生成电子邮件文本，以及在发布者通道上生成动态万维网页和 XDS 文档。

模板包含文本、要素和替换标记。在输出文档内，替换标记被替换为提供给模板处理样式表的数据。

下面是不同用途模板的几个示例。在该示例中，替换标记是位于两个 $ 字符之间且显示为粗体的字符串。

模板也可包含操作要素。操作要素是由模板处理样式表解释的控制要素。有关操作要素的信息，请参见附录 F “手工任务服务驱动程序：模板操作要素参照”在第 275 页 。以下示例中，操作要素也显示为粗体。

下面的示例模板用于生成 HTML 电子邮件正文：

```
<html xmlns:form="http://www.novell.com/dirxml/manualtask/form">
<head></head> <body> Dear $manager$,<p/> <p> This message is to inform
```

```
you that your new employee <b>$given-name$ $surname$</b> has been
hired. <p> You need to assign a room number for this individual. Click
<a href="$url$">Here</a> to do this. </p> <p> Thank you,<br/> HR
Department </p> </body> </html>
```

下面的示例模板用于生成纯文本电子邮件正文：

```
<form:text xmlns:form="http://www.novell.com/dirxml/manualtask/form">
Dear $manager$,

This message is to inform you that your new employee $given-name$
$surname$ has been hired.

You need to assign a room number for this individual. Use the following
link to do this:

$url$

Thank you,

The HR Department

</form:text>
```

要求使用 <form:text> 要素，因为模板必须是 XML 文档。<form:text> 要素将被清除，这是模板处理工作的一部分。

下面的模板用于生成 HTML 表格，该表格可用作输入数据的万维网页：

```
<html  xmlns:form="http://www.novell.com/dirxml/manualtask/form">
<head> <title>Enter room number for $subject-name$</title> </head>
<body> <link href="novdocmain.css" rel="style sheet" type="text/css"/>
<br/><br/><br/><br/> <form class="myform" METHOD="POST" ACTION="$url-
base$/process_template.xsl"> <table cellpadding="5" cellspacing="10"
border="1" align="center"> <tr><td> <input TYPE="hidden"
name="template" value="post_form.xml"/> <input TYPE="hidden"
name="subject-name" value="$subject-name$"/> <input TYPE="hidden"
name="association" value="$association$"/> <input TYPE="hidden"
name="response-style sheet" value="process_template.xsl"/> <input
TYPE="hidden" name="response-template" value="post_response.xml"/>
<input TYPE="hidden" name="auth-style sheet"
value="process_template.xsl"/> <input TYPE="hidden" name="auth-
template" value="auth_response.xml"/> <input TYPE="hidden"
name="protected-data" value="$protected-data$"/> You are:<br/>
<form:if-single-item name="responder-dn">           <input
TYPE="hidden" name="responder-dn" value="$responder-dn$"/> $responder-
dn$           </form:if-single-item>          <form:if-multiple-items
name="responder-dn">          <form:menu name="responder-dn"/>
</form:if-multiple-items> </td></tr> <tr><td> Enter your password:
<br/> <input name="password" TYPE="password" SIZE="20" MAXLENGTH="40"/
> </td></tr> <tr><td> Enter room number for $subject-name$:<br/>
<input TYPE="text" NAME="room-number" SIZE="20" MAXLENGTH="20"
```

```
value="$query:roomNumber$"/> </td></tr> <tr><td> <input TYPE="submit"
value="Submit"/> <input TYPE="reset" value="Clear"/> </td></tr> </
table> </form> </body> </html>
```

下面的模板用于生成 XDS 文档：

```
<nds> <input> <modify class-name="User" src-dn="not-applicable">
<association>$association$</association> <modify-attr attr-
name="roomNumber"> <remove-all-values/> <add-value> <value>$room-
number$</value> </add-value> </modify-attr> </modify> </input> </nds>
```

替换标记

以上示例模板中由 $ 界定的项目是替换标记。例如， $manager$ 将替换为经理的真实姓名。

替换标记可显示为文本或 XML 特性值 （注意上面第一个示例中， <a> 要素上的 href 值）。

替换数据

替换数据由字符串组成，这些字符串将代替由模板生成的输出文档中的替换标记。替换数据由订购者通道数据或发布者通道 HTTP 数据提供，或由驱动程序自动提供。替换数据的附加类型是通过 Identity Manager 从 eDirectory 检索的数据 （查询数据）。有关替换数据的完整信息，请参见附录 D “手工任务服务驱动程序：替换数据”在第 267 页 。

订购者通道数据：订购者通道替换数据有两种类型。第一种类型用作模板 （用于创建电子邮件）中替换标记的替换值。第二种类型位于 URL 的查询部分，以便在将 URL 提交到发布者万维网服务器后，便可在发布者通道上使用此数据。

HTTP 数据： 替换数据提供给发布者通道万维网服务器，用作 URL 查询字符串数据、HTTP POST 数据，或两者兼有。

自动数据： 手工任务服务驱动程序提供自动数据。有关自动数据项的信息，请参见附录 E “手工任务服务驱动程序：自动替换数据项”在第 273 页 。

查询数据：以查询开始的替换标记：视作要求从 eDirectory 获取当前数据的请求。位于查询后的标识部分：是 eDirectory 对象特性的名称。要查询的对象由某个替换数据项指定：association、 src-dn 或 src-entry-id。上述项将按在前句中出现的顺序来处理。

模板操作要素

操作要素是模板中的名称空间限定要素，此操作要素用于简单逻辑控制或创建 HTML 表格的 HTML 要素。用于限定要素的名称空间是 http://www.novell.com/dirxml/manualtask/form。在该文档和手工任务服务驱动程序附带的样本模板中，所用的前缀是 "form"。

以上示例中以粗体显示的要素是操作要素。

有关操作要素的信息，详见附录 F “手工任务服务驱动程序：模板操作要素参照”在第 275 页 。

订购者通道电子邮件

手工任务服务驱动程序的订购者通道用于发送电子邮件。为实现此功能，驱动程序支持名为 <mail> 的自定义 XML 要素。订购者通道上的策略根据对某个 eDirectory 事件 （例如，用户创建）的响应来构造 <mail> 要素。下面为 <mail> 要素的示例：

```
<mail src-dn="\PERIN-TAO\novell\Provo\Joe"> <to>JStanley@novell.com</
to> <cc>carol@novell.com</cc> <reply-to>HR@novell.com</reply-to>
<subject>Room Assignment Needed for: Joe the Intern</subject> <message
mime-type="text/html"> <stylesheet>process_template.xsl</stylesheet>
<template>html_msg_template.xml</template> <replacement-data> <item
name="manager">JStanley</item> <item name="given-name">Joe</item>
<item name="surname">The Intern</item> <url-data> <item
name="file">process_template.xsl</item> <url-query> <item
name="template">form_template.xml</item> <item name="responder-dn"
protect="yes">\PERIN-TAO\big-org\phb</item> <item name="responder-dn"
protect="yes">\PERIN-TAO\big-org\carol</item> <item name="subject-
name">Joe The Intern</item> </url-query> </url-data> </replacement-
data> <resource cid="css-1">novdocmain.css</resource> </message>
<message mime-type="text/plain">
<stylesheet>process_text_template.xsl</stylesheet>
<template>txt_msg_template.xml</template> <replacement-data> <item
name="manager">JStanley</item> <item name="given-name">Joe</item>
<item name="surname">The Intern</item> <url-data> <item
name="file">process_template.xsl</item> <url-query> <item
name="template">form_template.xml</item> <item name="responder-dn"
protect="yes">\PERIN-TAO\big-org\phb</item> <item name="responder-dn"
protect="yes">\PERIN-TAO\big-org\carol</item> <item name="subject-
name">Joe The Intern</item> </url-query> </url-data> </replacement-
data> </message> <attachment>HR.gif</attachment> </mail>
```

手工任务服务驱动程序的订购者使用 <mail> 要素中包含的信息来构造 SMTP 电子邮件。可构造一个 URL 并将其插入电子邮件中，通过这个 URL 电子邮件收件人即可响应此电子邮件。URL 可指向订购者通道万维网服务器或指向某个其它万维网服务器。

有关 <mail> 要素及其内容的信息，详见附录 G “手工任务服务驱动程序：<mail> 要素参照”在第 279 页 。

订购者通道万维网服务器

手工任务服务驱动程序的发布者通道运行着一台万维网服务器，该服务器已配置为用户可通过万维网浏览器将数据输入到 eDirectory 中。万维网服务器设计为与手工任务服务驱动程序的订购者通道发送的电子邮件一起使用。

订购者通道万维网服务器可提供静态文件和动态内容。静态文件的示例有 .css 样式表、图像等；动态内容的示例则包括：根据 URL 或 HTTP POST 数据中包含的替换数据而变化的万维网页。

通常，订购者通道万维网服务器配置为允许用户将数据输入到 eDirectory 中，作为对订购者通道发送的电子邮件的响应。用户与万维网服务器的典型交互如下：

1. 用户使用万维网浏览器，将电子邮件的 URL 提交给万维网服务器。URL 指定用于创建动态万维网页的样式表、模板和替换数据 （通常包含 HTML 表格）。

2. 万维网服务器通过使用样式表和替换数据处理模板，从而创建 HTML 页。由 URL 引用的资源将作为 HTML 页返回用户的万维网浏览器。
3. 浏览器显示 HTML 页，然后用户输入要求的信息。
4. 浏览器发送 HTTP POST 请求，其中包含已输入的信息以及源于电子邮件 URL 的其它信息。响应电子邮件的用户 DN 和用户的口令必须位于 POST 数据中。
5. 万维网服务器使用用户的 DN 和口令来鉴定用户。如果鉴定失败，则返回包含失败讯息的万维网页，它将作为 POST 请求的结果。可使用 POST 数据中指定的样式表和模板构造失败讯息。如果鉴定成功，则处理继续。
6. 万维网服务器使用 POST 数据中指定的样式表和模板构造 XDS 文档。XDS 文档将提交给订购者通道上的 Identity Manager。
7. XDS 文档的提交结果以及 POST 数据中指定的样式表和模板用于构造万维网页，此万维网页向用户指示数据提交的结果。将此万维网页发送到浏览器作为 POST 请求的结果。

8.2.3 配置

本节描述如何配置手工任务服务驱动程序的参数和模板。

驱动程序设置

本节描述驱动程序对象用户界面的 " 驱动程序设置 " 一节中出现的参数。

事实上，这些参数大多用于订购者通道万维网服务器。它们出现在驱动程序设置区域中，因为手工任务服务驱动程序订购者也需要对它们进行访问。

文档基址的 DN

此参数是树枝对象的 eDirectory DN。手工任务服务驱动程序可以从 eDirectory 和磁盘装载 XML 文档 （包括 XSLT 样式表）。如果要从 eDirectory 装载 XML 文档，则此参数将标识从其装载文档的根树枝。

从 eDirectory 装载的文档在 eDirectory 对象的特性值中。如果未指定，则此特性为 XmlData。此特性也可指定，方法是向包含此文档的对象的名称添加 # 字符 （后跟特性名称）作为后缀。

例如，假设文档基址 DN 指定为 "novell\Manual Task Documents"，并且 "Manual Task Documents" 下存在一个名为 "templates" 的树枝

如果名为 "e-mail _template" 的 DirXML 样式表位于 "templates" 目录下，则下列资源标识符可用于引用 XML 文档："templates/e-mail _template" 或 "templates/e-mail _template#XmlData"。

资源标识符可提供为替换数据、URL 数据或 HTTP POST 数据。例如，下列要素可能会显示在订购者通道上的 <message> 要素下：

```
<template>templates/e-mail _template#XmlData</template>
```

文档目录

此参数标识文件系统目录，此目录用作定位资源 （例如，订购者通道万维网服务器维护的模板、 XSLT 样式表和其它文件资源）的基本目录。示例值包括：

Windows	c:\Novell\Nds\mt_files
NetWare	SYS:\SYSTEM\mt_files
UNIX	/usr/lib/dirxml/rules/manualtask/mt_files

使用 HTTP 服务器 (true|false)

此参数指示是否要发布者通道运行万维网服务器。如果要运行万维网服务器，则参数设为 true，或如果不运行万维网服务器，则参数设为 false。

如果手工任务服务驱动程序仅用于发送电子邮件而不带有响应 URL，或带有指向其它应用程序的 URL，则不应运行 HTTP 服务器，以节省系统资源。

HTTP IP 地址或主机名

此参数允许用户指定在若干本地 IP 地址中，发布者通道万维网服务器将监听哪个 IP 地址的 HTTP 请求。

将 HTTP IP 地址或主机名参数值留为空，可使发布者通道万维网服务器监听默认的 IP 地址。对于带有单个 IP 地址的服务器，此设置已足够了。将点表示法 IP 地址置为参数值，可使发布者通道万维网服务器监听指定地址的 HTTP 请求。

请注意，如果邮件命令要素中未指定主机名或地址，则订购者通道邮件处理程序将使用为 HTTP IP 地址或主机名指定的值来构造 URL。如果参数 Use HTTP server (true|false) 设置为 fasle，则可用 HTTP IP 地址或主机名来指定用于构造邮件 URL 的万维网服务器的地址或名称。

HTTP 端口

此参数是整数值，指示发布者通道万维网服务器应监听哪个 TCP 端口的进来请求。如果未指定此值，则根据万维网服务器连接是否正使用 SSL，端口号将默认为 80 或 443。

如果 Identity Manager 服务器上正运行手工任务服务驱动程序 （即，它没有通过远程计算机的远程装载程序运行），则 HTTP 端口应设为不同于 80 或 443 的值。这是因为 iMonitor 或其它进程通常使用端口 80 和端口 443。

KMO 名称

如果不为空，则此参数为 eDirectory 密钥资料对象 （它包含发布者通道万维网服务器用于 SSL 的服务器证书和密钥）的名称。

设置此参数，可使发布者通道万维网服务器使用 SSL 来满足 HTTP 请求。

此参数优先于任何 Java* 密钥存储区参数 （见下文）。

出于安全性考虑，建议使用 SSL，因为使用发布者通道万维网服务器时， eDirectory 口令将在 HTTP POST 数据中传输

密钥存储区文件名称

此参数以及密钥存储区口令、证书名称 （密匙别名）和证书口令 （密匙口令）用于指定 Java 密钥存储区文件，此文件包含通过发布者通道万维网服务器用于 SSL 的证书和密匙。

设置此参数，可使发布者通道万维网服务器使用 SSL 来满足 HTTP 请求。

如果设置了 KMO 参数的名称，则忽略此参数及其关联的参数。

出于安全性考虑，建议使用 SSL，因为使用发布者通道万维网服务器时， eDirectory 口令将在 HTTP POST 数据中传输。

密钥存储区口令

此参数指定由密钥存储区文件参数的名称指定的 Java 密钥存储区文件的口令。

证书名称 （密钥别名）

此参数指定由密钥存储区文件参数的名称指定的 Java 密钥存储区文件中使用的证书名称。

证书口令 （密钥口令）

此参数指定使用证书名称 （密钥别名）参数指定的证书的口令。

订购者设置

本小节描述订购者通道的设置。

SMTP 服务器

此参数指定 SMTP 服务器的名称，订购者通道将使用此服务器发送电子邮件。

SMTP 帐户名

如果使用 SMTP 服务器参数指定的 SMTP 服务器要求鉴定，则此参数将指定鉴定所用的帐户名。所用的口令是与驱动程序鉴定参数相关联的应用程序口令。

默认 "From" 地址

如果已指定，此地址将是订购者通道发送的电子邮件的 "SMTP from" （SMTP 源）字段中使用的电子邮件地址。如果未指定，则发送给订购者的 <mail> 要素必须包含一个 <from> 要素。

发送给订购者的 <from> 要素 （位于 <mail> 要素下）优先于此参数。

附加处理程序

如果已指定，则为 Java 类名称的空格分隔列表。各个类名称是自定义类，该类执行 com.novell.nds.dirxml.driver.manualtask.CommandHandler 界面并处理自定义 XDS 要素。（<mail> 的处理程序是内置处理程序）。

有关自定义处理程序的附加信息，请参见附录 I “手工任务服务驱动程序：订购者通道的自定义要素处理程序”在第 293 页 。

发布者设置

本小节描述发布者通道的设置。

附加服务器小程序

如果未留空，则为 Java 类名称的空格分隔列表。各个类名称是自定义类，该类扩展 javax.servlet.http.HttpServer。自定义服务器小程序可用于扩展发布者通道万维网服务器的功能。

有关自定义服务器小程序的附加信息，请参见附录 J “手工任务服务驱动程序：发布者通道的自定义服务器小程序”在第 295 页 。

订购者通道策略

订购者通道策略的配置取决于手工任务服务驱动程序所完成的特定安装。然而，下面的准则可能会有帮助。

通常，命令转换策略是构造发送给订购者的 <mail> 要素的最好途经。原因在于，命令到达命令转换策略时已完成的 DirXML 引擎处理最多。这意味着已处理添加事件的创建策略（例如，允许禁止对象的添加事件，这些事件不具备生成电子邮件所需的全部特性）。这也意味着无关联对象的修改事件已转换为添加事件。

构造电子邮件的 XSLT 样式表可能需要或不需要查询 eDirectory 以获取附加信息。

例如，如果此电子邮件只是新员工欢迎邮件，则添加命令可包含全部所需的信息：名、姓和因特网电子邮件地址。通过在创建策略中指定 Given Name （名）、 Surname （姓）和 Internet E-mail Address （因特网电子邮件地址）是必需特性，即可完成此操作。这样可确保只有包含所需信息的添加命令可以到达命令转换。

然而，如果此电子邮件是发给员工经理的邮件，则样式表需要查询 eDirectory。可从员工用户对象的添加事件获得经理 DN，但由于经理电子邮件地址是经理用户对象的特性，所以必须进行查询以获得该信息。

另外，如果正在生成电子邮件通知，作为与驱动程序关联的对象的修改命令的结果，则必须进行查询以获得未包含在修改命令中的信息。

阻止命令到达订购者

如果要从添加事件之外的事件生成电子邮件，则必须允许添加事件到达要监视对象的订购者。允许添加事件到达订购者将导致生成关联值，此值将从订购者返回到 Identity Manager。

手工任务服务驱动程序策略监视的 eDirectory 对象应具有手工任务服务驱动程序的关联，这一点非常重要。只有具有关联的对象才能带有报告给驱动程序的删除、重命名和移动事件。另外，在订购者通道事件转换之后，无关联对象上的修改事件将转换为添加事件。

命令转换策略应阻止所有其它命令 （修改、移动、重命名和删除），并防止这些命令到达订购者。订购者仅处理 <add> 命令和 <mail> 命令。其它命令将导致订购者返回错误。

生成电子邮件

订购者发送电子邮件以响应接收 <mail> 要素，此要素描述要发送的电子邮件。请参见附录 G “手工任务服务驱动程序：<mail> 要素参照”在第 279 页 以获取有关 <mail> 要素及其内容的说明。

可以生成电子邮件以响应任何 Identity Manager 事件 （添加、修改、重命名、移动、删除）。

随 <mail> 要素的 <message> 要素子级提供的替换数据取决于两个主要因素：

- 用于生成邮件正文的模板。电子邮件模板所用的替换项目显示为 <replacement-data> 要素的子级。
- 发布者通道上万维网页模板需要的信息 （如果电子邮件将导致在发布者通道上作出响应）。万维网页模板所用的替换项目显示为 <replacement-data> 的子级 <url-data> 的子级， <url-query> 要素。

如果电子邮件应包含一个指向发布者通道万维网服务器并用于征集用户信息的 URL，则此替换数据必须至少包含一个响应程序 DN 项。响应程序 DN 项的值必须为邮件目标用户的用户对象的 DN。

如果模板中使用查询替换标记 （请参见 “替换数据”在第 191 页），则 <message> 要素的替换数据必须包含一个名为 src-dn 或 src-entry-id 的项，或具有相应值的关联。如果要查询的 eDirectory 对象已具有手工任务服务驱动程序的关联，则只能使用关联项。无法使用非关联对象的订购者生成的关联，因为发生查询时，此关联尚未写入 eDirectory 对象。

<message> 要素可指定邮件正文的 MIME 类型。如果已指定 MIME 类型，但未指定样式表（即，无 <message> 的 <stylesheet> 要素子级），则使用两个默认样式表名称的一个。MIME 类型是文本 / 纯文本，则默认样式表名称为 process_text_template.xsl。如果 MIME 类型是文本 / 纯文本之外的其它类型，则默认样式表名称为 process_template.xsl。

订购者通道电子邮件模板

电子邮件模板是包含样板文件和替换标记的 XML 文档。电子邮件模板用于生成电子邮件正文文本。有关模板的一般信息，请参见 “模板”在第 189 页。

电子邮件模板中使用的替换标记指示 <item> 要素，此要素必须作为 <replacement-data> 要素（由构造 <mail> 要素的订购者通道策略构造）的子级提供。例如，如果电子邮件模板具有替换标记 $employee-name$，则 <message> 要素的替换数据中必须存在 <item name="employee-name"> 要素。如果员工姓名项不存在，则在生成的电子邮件正文中，由模板中的替换标记占用的位置处没有文本。

电子邮件模板可用于生成邮件正文 （纯文本、 HTML 或 XML）。

如果电子邮件模板生成纯文本邮件，则必须通过将纯文本指定为输出类型的样式表对其进行处理。如果此样式表未将纯文本指定为它的输出类型，则将产生不希望出现的 XML 转义。通常使用默认的手工任务服务驱动程序样式表 (process_text_template.xsl) 来处理产生纯文本的模板。

发布者通道策略

在手工任务服务驱动程序的多数实现中，不需要发布者通道策略。这是因为手工任务服务驱动程序可以构造万维网页面和 XDS 模板，以使它们准确地生成所需的 XDS，这些 XDS 无需由策略进一步处理。

具体安装时可能需要一些策略。

发布者通道万维网页模板

万维网页模板是包含样板文件和替换标记的 XML 文档。万维网页模板用于生成万维网页文档 （通常是 HTML 文档）。有关模板的一般信息，请参见 “模板”在第 189 页。

万维网页模板中的替换标记指示订购者通道中作为 URL 查询数据提供的替换数据。获取发布者通道上的替换数据的来源是 HTTP GET 请求的 URL 查询字符串以及 HTTP POST 请求的 URL 查询字符串和 POST 数据。

以替换数据从订购者通道通过电子邮件发送到发布者通道万维网服务器为例，请考虑以下方案。

手工任务服务驱动程序配置为要求新员工的经理为新员工分配房间号。发送至经理的电子邮件的触发器为 <add> 命令，用于由订购者通道命令转换策略处理的新 User 对象。

经理单击电子邮件中的 URL，即可在经理的万维网浏览器中显示万维网页。该万维网页必须指示经理正在为哪位员工输入房间号。

为了实现此功能，订购者通道上的 <url-query> 要素包含有一个替换数据项，用于按姓名标识新用户：

```
<item name=”subject-name”>Joe the Intern</item>
```

这使得 URL 查询字符串包含 （与其它内容间杂） "subject-name=Joe%20the%20Intern"。（"%20" 为 URL 编码空间）。

经理单击电子邮件中的 URL 时，他的万维网浏览器即将该 URL 提交至发布者通道万维网服务器。万维网服务器将构造一个替换数据项，以值 Joe the Intern 来命名 subject-name。

万维网页模板也由 URL 指定，其中包含替换标记 $subject-name$。由样式表处理万维网页模板以构造万维网页时，替换标记将由 Joe the Intern 替换，该值为创建用户对象导致电子邮件发送的员工自定义万维网页。

有关完整的订购者通道至发布者通道事务的其它信息，请参见附录 H “手工任务服务驱动程序：新员工的数据流方案”在第 283 页 。

发布者通道 **XDS** 模板

XDS 模板是包含样板文件和替换标记的 XML 文档。XDS 模板用于生成 XDS 文档，这些 XDS 文档将提交至手工任务服务驱动程序的发布者通道上的 Identity Manager。有关模板的一般信息，请参阅 " 概述 " 一节下的 " 模板 "。

XDS 模板中的替换标记指示：将提供给万维网服务器的某些替换数据作为 HTTP POST 请求中的数据。

例如，考虑以下 XDS 模板：

```
<nds> <input> <modify class-name="User" src-dn="not-applicable">
<association>$association$</association> <modify-attr attr-
name="roomNumber"> <remove-all-values/> <add-value> <value>$room-
number$</value> </add-value> </modify-attr> </modify> </input> </nds>
```

模板中的替换标记指示：HTTP POST 数据必须提供一个关联值和一个房间号值。

通常，关联值将从订购者通道中产生。订购者通道电子邮件将放置关联 = 置于电子邮件中的 URL 的查询字符串中的部分值。用于在 URL 提交至万维网服务器时生成万维网页的万维网页模板通常将关联值置于隐藏的 INPUT 要素中：

```
<INPUT TYPE="hidden" NAME="association" VALUE="$association$"/>
```

将关联值作为隐藏的 INPUT 要素放置，会导致作为 HTTP POST 数据的一部提交 "association=some value" 对。

使用与下面的要素相似的 INPUT 要素将房间号值输入万维网页：

```
<input TYPE="text" NAME="room-number" SIZE="20" MAXLENGTH="20"/>
```

如果经理输入 1234 然后单击 " 提交 "，万维网浏览器将发送 "room-number=1234"，它将作为 HTTP POST 数据的一部分。

万维网服务器随后将生成一个 <item name="association"> 替换数据项和一个 <item name="room-number"> 替换数据项，这两个替换数据项将在处理 XDS 模板时使用。

通过使用 POST 数据中指定的样式表处理 XDS 模板，从而生成 XDS 文档。随后该 XDS 文档将提交至手工任务服务驱动程序的发布者通道上的 Identity Manager。

跟踪设置

手工任务服务驱动程序可输出具有多种跟踪级别的讯息：

级别	跟踪讯息说明
0	无跟踪讯息
1	跟踪基本操作的单行讯息
2	无附加讯息 （DirXML 引擎跟踪此级别及以上级别的 XML 文档）
3	无附加讯息
4	与从模板和样式表进行文档构造相关的讯息
5	跟踪的替换数据文档

8.2.4 其它信息

有关手工任务服务驱动程序设置的其它信息，请参考以下附录小节：

- 附录 D “手工任务服务驱动程序：替换数据”在第 267 页
- 附录 E “手工任务服务驱动程序：自动替换数据项”在第 273 页
- 附录 F “手工任务服务驱动程序：模板操作要素参照”在第 275 页
- 附录 G “手工任务服务驱动程序：<mail> 要素参照”在第 279 页
- 附录 H “手工任务服务驱动程序：新员工的数据流方案”在第 283 页
- 附录 I “手工任务服务驱动程序：订购者通道的自定义要素处理程序”在第 293 页
- 附录 J “手工任务服务驱动程序：发布者通道的自定义服务器小程序”在第 295 页

高可用性

9

可以使用具有共享储存器的 Identity Manager，以提供高可用性。在群集环境中，需要采取某些步骤才能使用 Novell® eDirectory™ 和 Identity Manager。

本节包括：

9.1 配置 eDirectory 和 Identity Manager 以便在 Linux 和 UNIX 上使用共享储存器

本节提供配置 eDirectory 和 Identity Manager 的步骤，以便在使用共享储存器的高可用性群集中进行故障转移。本节中的信息概况为可用于任何 Linux 或 UNIX 平台上的共享储存器高可用性群集；这些信息并非专门针对某一特定群集管理器。

要理解的基本概念是：eDirectory 和 Identity Manager 的状态数据必须位于共享储存器中，以便在当前运行服务的群集节点中可用。实际上，这意味着必须将 eDirectory 数据储存器（通常位于 /var/nds/dib 中）重新定位到群集共享储存器。Identity Manager 状态数据也位于 /var/nds/dib 中。必须配置群集节点上的每个 eDirectory 实例，才能使用共享储存器中的数据储存器。其它 eDirectory 配置数据也必须驻留在共享储存器中。

除 eDirectory 数据储存器外，还必须共享 NICI（Novell 国际密码基础结构）数据，以便在群集节点之间复制服务器特定的密钥。通常，将 NICI 数据复制到各个群集节点上的本地储存器中，要优于将 NICI 数据移至共享储存器中。这是因为即使群集节点处于辅助状态且未托管共享储存器，客户机 NICI 功能也可在群集节点上使用。

共享 eDirectory 和 NICI 数据将在以下小节中讨论，讨论基于以下假设：

- 您正在使用 NICI、 eDirectory 以及 Identity Manager 数据和配置的默认安装位置。

  不会脱离 eDirectory 数据单独讨论 Identity Manager 数据，因为感兴趣的 Identity Manager 数据与 eDirectory 数据位于同一位置
- 您熟悉 eDirectory 和 Identity Manager 安装过程。
- 您正在使用双节点群集。

  双节点群集显然是实现高可用性的最常用配置。但是，本节中的概念可以很容易地扩展至 *n* 节点群集。

本节包括：

9.1.1 安装 eDirectory

注释：作为 eDirectory 安装过程的一部分安装 NICI。

1. 在主群集节点上安装 eDirectory。
2. 在主群集节点上配置 eDirectory。在主群集节点上创建新树或将服务器安装到现有树中。设置 eDirectory 服务器名称时，应使用不同于 UNIX 服务器名称的其它名称。应使用群集的通用名称，而不是特定于某一群集节点的名称。
3. 在辅助群集节点上安装相同版本的 eDirectory。不要在辅助群集节点上配置 eDirectory。

   辅助节点没有单独的树。

9.1.2 安装 Identity Manager

1. 使用 *Metadirectory Server* （Metadirectory 服务器）选项在主群集节点上安装 Identity Manager。

   安装过程将安装 Identity Manager 文件，并配置 eDirectory 树，以便与 Identity Manager 一起使用。
2. 使用辅助群集开关、通过输入以下命令在辅助群集节点上安装同一版本的 Identity Manager

   ```
   dirxml_platform.bin -DCLUSTER_INSTALL="true"
   ```

   在安装过程中，请选择 "Metadirectory 服务器 " 选项。

   使用辅助群集开关安装 Identity Manager 文件，但不要尝试执行任何其它 eDirectory 配置。无需进行任何配置，因为辅助节点没有单独的树。

9.1.3 共享 NICI 数据

NICI 可提供 eDirectory、 Identity Manager 和 Novell 客户机应用程序所使用的密码服务。与 eDirectory 一起使用时， NICI 可提供特定于服务器的密钥。这些特定于服务器的密钥在将 eDirectory 作为群集服务运行的所有群集节点上都必须相同。

有两种方法可以共享 NICI 数据：

- 将 NICI 数据置于群集共享储存器中。

  此方法的缺点是：如果群集节点没有托管共享储存器，则依靠 NICI 的应用程序将在群集节点上发生故障。
- 将 NICI 数据从主服务器复制到辅助服务器的本地储存器。

要复制 NICI 数据：

1. 将辅助群集节点上的 /var/novell/nici 重命名为其它名称 （如 /var/novell/nici.sav）。
2. 将 /var/novell/nici 目录从主群集节点复制到辅助群集节点。

   这可以使用 scp 来完成；或在主节点上创建 /var/novell/nici 目录的压缩文件，将其传送到辅助节点，然后在辅助节点上解压缩此目录即可完成。

9.1.4 共享 eDirectory 和 Identity Manager 数据

默认情况下，eDirectory 数据储存器位于 /var/nds/dib 中。其它配置项和状态项也储存在 /var/nds 及其子目录中。eDirectory 的默认配置目录为 /etc。要配置 eDirectory 和 Identity Manager，以便在高可用性群集中使用共享储存器，需要进行以下步骤。这些步骤假设共享储存器安装在 /shared 位置。

- “在主节点上”在第 203 页
- “在辅助节点上”在第 204 页

在主节点上

1. 将 /var/nds 目录子树复制到 /shared/var/nds。
2. 重命名 /var/nds 目录 （例如，重命名为 /var/nds.sav）。

   不要求创建备份，但如果在此阶段创建备份，将使您在重新开始 （如有必要）时无需重新安装 eDirectory。
3. 创建从 /var/nds 到 /shared/var/nds 的符号链接 （例如， ln -s /shared/var/nds /var/nds）。
4. 创建以下符号链接：

链接自	链接至
/shared/var/nds/class16.conf	/etc/class16.conf
/shared/var/nds/class32.conf	/etc/class32.conf
/shared/var/nds/help.conf	/etc/help.conf
/shared/var/nds/ndsimonhealth.conf	/etc/ndsimonhealth.conf
/shared/var/nds/miscicon.conf	/etc/miscicon.conf
/shared/var/nds/ndsimon.conf	/etc/ndsimon.conf
/shared/var/nds/macaddr	/etc/macaddr

5. 创建 /etc/nds.conf 的备份拷贝。
6. 将 /etc/nds.conf 移至 /shared/var/nds。
7. 编辑 /shared/var/nds/nds.conf，并将以下条目置于文件中 （覆盖当前所有名称相同的条目）：
   - n4u.nds.dibdir=/shared/var/nds/dib
   - n4u.server.configdir=/shared/var/nds
   - n4u.server.vardir=/shared/var/nds
   - n4u.nds.preferred-server=localhost

   对于以下条目，将 eth0:0 替换为群集共享 Ethernet 接口的接口名称。还要将 lo 替换为本地主机 Ethernet 接口的接口名称。
   - n4u.nds.server.interfaces=eth0:0@524,lo@524
   - http.server.interfaces=eth0:0@8008,lo@8008
   - https.server.interfaces=eth0:0@8009,lo@8009
8. 创建从 /etc/nds.conf 至 /shared/var/nds/nds.conf 的符号链接。

9 启动 ndsd，并验证 ndsd 已与共享储存器一起运行。

10 停止 ndsd。

11 将 ndsd 置于要托管的群集管理器资源列表中。

12 将 ndsd 从 init 进程在引导时要启动的守护程序列表中去除。

在辅助节点上

1 重命名 /var/nds 目录 （例如，重命名为 /var/nds.sav）。备份并非绝对必要，但备份后无需安装 eDirectory 即可重新开始。

2 创建从 /var/nds 至 /shared/var/nds 的符号链接

3 创建 /etc/nds.conf 的备份拷贝。

4 去除 /etc/nds.conf。

5 创建从 /etc/nds.conf 至 /shared/var/nds/nds.conf 的符号链接。

6 将 ndsd 置于要托管的群集管理器资源列表中。

7 将 ndsd 从 init 进程在引导时要启动的守护程序列表中去除。

完成主节点和辅助节点的步骤后，启动群集服务。 eDirectory 和 Identity Manager 将在主节点上启动。

9.1.5 Identity Manager 驱动程序的注意事项

多数 Identity Manager 驱动程序可在群集配置中运行。但是，需要注意以下事项：

- 驱动程序可执行文件 （.jar 文件和 / 或共享对象）必须安装在所有群集节点上。
- 如果驱动程序必须在同一服务器上作为由驱动程序支持的应用程序运行，则也必须对应用程序进行配置，以便作为群集服务的一部分运行。
- 如果驱动程序具有可配置的用于特定于驱动程序状态数据的位置，则该位置也必须位于群集共享储存器中。

  这种情况的示例包括：使用 LDAP 驱动程序而不更改日志时，或者在无触发器模式下使用 JDBC 驱动程序时。
- 如果驱动程序包含储存在 eDirectory 之外的配置数据，则配置数据也必须位于共享储存器中，或者必须复制到各个群集节点上。这种情况的示例如：手工任务驱动程序的模板目录。

9.2 SuSE Linux 案例学习

有关 Identity Manager 在 SUSE LINUX Enterprise Server 8 的共享储存器中运行的说明，请参见 TID10093317 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10093317.htm)。

使用 Novell Audit 进行日志记录和报告

10

安装 Identity Manager 后，可以使用 Novell® Audit 进行审计和报告。

10.1 概述

Novell Audit 是多项技术的集合，提供监视、日志记录、报告和通知功能。集成了 Novell Audit 的 Identity Manager 可以提供有关驱动程序和引擎活动当前状态和历史状态的详细信息。这些信息通过一组预配置报告、标准通知服务和用户定义的数据日志记录提供。

使用 Novell Audit 可以实时监视 Identity Manager 事件、发送有关任何 Identity Manager 事件的电子邮件通知，并且生成 Identity Manager 活动报告。

使用插件可以控制发送至 Novell Audit 的讯息类型，这些插件类似于报告和通知服务 (RNS) 提供的插件。这些插件中添加了附加的级别，以便选择希望跟踪的操作类型或调试信息，如状态、添加项、搜索等。

报告和通知服务

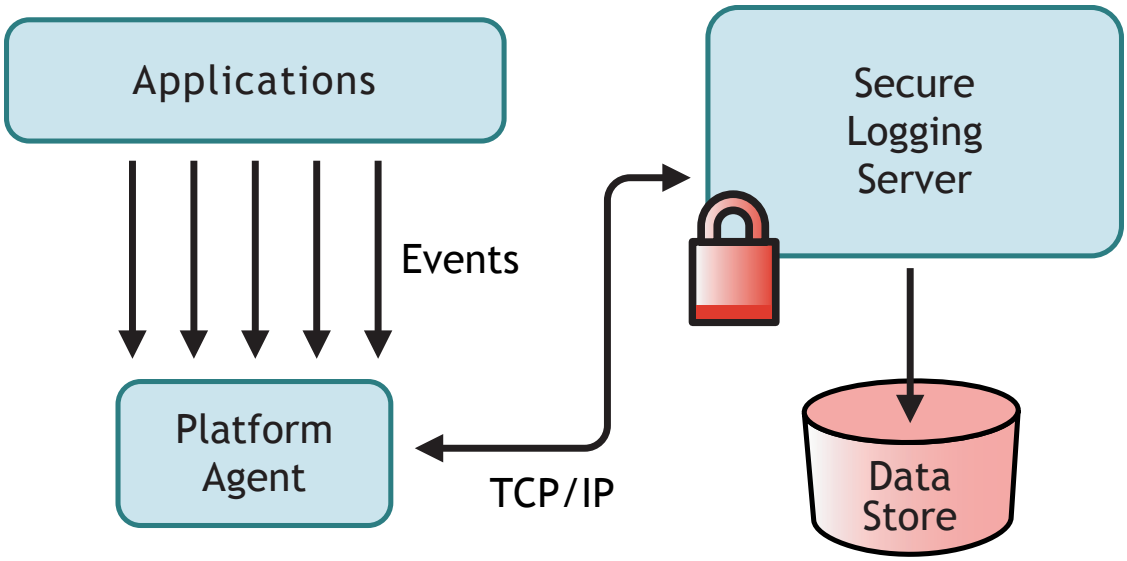
如果当前正在使用 报告和通知服务 (RNS)，虽然 Metadirectory 引擎可继续处理 RNS 功能，但还是建议您停止使用。由于 Novell Audit 扩充了 RNS 的功能，并且 Identity Manage 将来的发行版可能将不支持 RNS，因此建议使用 Novell Audit。有关 RNS 的文档，请参见《*DirXML 1.1a* 管理指南》(http://www.novell.com/documentation/lg/dirxml11a/dirxml/data/afae8bz.html)。

10.2 Novell Audit

Novell Audit 是跨平台的集中日志记录服务工具，可以将多个应用程序的数据记录到一个集中式数据储存器中。对事件数据进行日志记录后，就可以根据所记录的事件运行详细报告、自定义查询并触发通知。

下图说明了 Novell Audit 的高级体系结构：

图 *10-1* 体系结构概述



在此图中，Identity Manager 是使用平台代理向 Novell Audit 安全性日志记录服务器报告事件的应用程序之一。

10.3 安装 Novell Audit

如概述所示， Novell Audit 由两个基本部件构成：

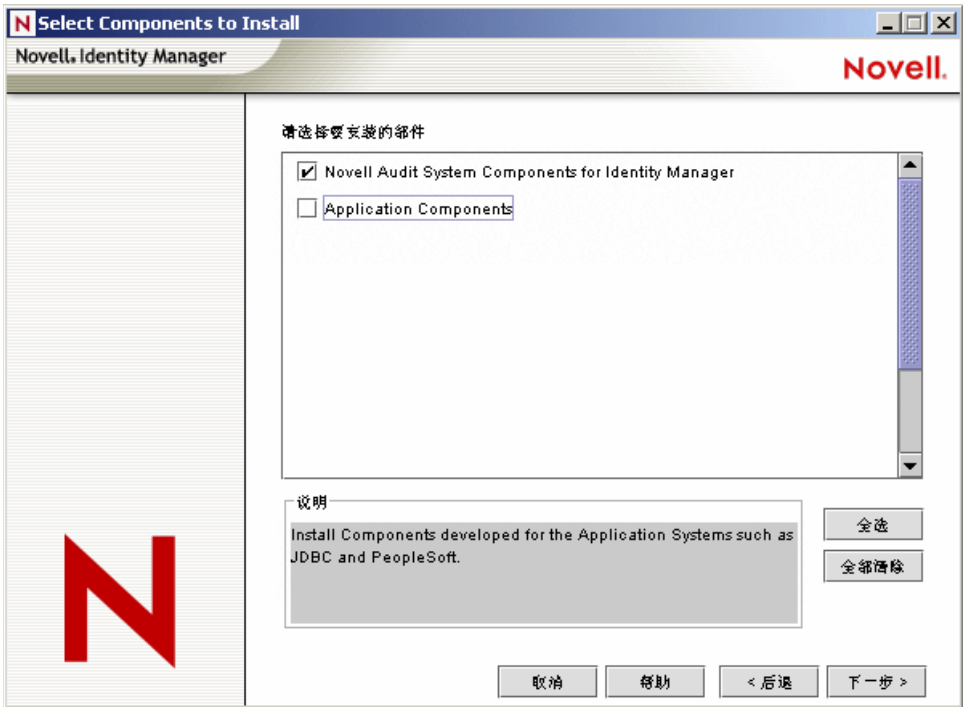
- 平台代理
- 安全性日志记录服务器

平台代理是与 Identity Manager 一起运行的部件，用于与安全性日志记录服务器对发生的事件进行通讯。该部件与 Identity Manager 共同安装。安全性日志记录服务器是从 Identity Manager 和其它应用程序接收事件数据的部件，与 Identity Manager 分开安装，是 Novell Audit 1.0.3 的一部分。

10.3.1 安装平台代理

安装 Identity Manager 时，通过选择 "Novell Audit System Components for the Identity Manager"（适用于 Identity Manager 的 Novell Audit 系统部件）选项来安装平台代理。

图 ***10-2*** 安装 *Identity Manager*



可在安装 Identity Manager 时安装平台代理，也可以稍后进行安装。

注释：如果在启动 Metadirectory 引擎后安装平台代理，则必须在链接平台代理和 Identity Manager 之前重启动 Identity Manager。Identity Manager 只在启动时尝试与平台代理进行连接。

安装完平台代理之后，请完成以下步骤以对其进行配置：

1 在文本编辑器中打开 Novell Audit 配置文件 logevent.cfg。此文件的默认位置是：

操作系统	路径
NetWare®	sys:\etc\logevent.cfg
Windows	*windows_directory*\logevent.cfg
Linux\Solaris	/etc/logevent.conf

2 将 LogHost 参数的值更改为安全性日志记录服务器的 IP 地址或 DNS 名。

3 重启动 Identity Manager。

10.3.2 安装安全性日志记录服务器

注释 **:** Identity Manager 中不包括 Novell Audit 安全性日志记录服务器。安全性日志记录服务器是 Novell Audit 1.0.3 的一部分。有关下载 Novell Audit 1.0.3 的信息，请参见 Novell Audit 产品页 (http://www.novell.com/products/nsureaudit)。

安全性日志记录服务器可运行在 NetWare 5.1 或更高版本、Windows* NT 4.0、Windows 2000 Server、Windows 2003 Server、Solaris* 8 或 9，以及包括 SUSE® Enterprise Linux Server 8 和 SUSE 9.0 在内的多个 Linux* 版本。

安全性日志记录服务器可将事件记录到 MySQL*、 Oracle*、 Microsoft* SQL Server、 Java* 应用程序中，以及包括平面文件在内的其它位置。Novell Audit 包括一个专为查询事件数据的数据库而设计的自定义应用程序，称为 Novell Audit Report。要使用这个高级报告工具，需要带有 ODBC 连接器的数据储存器。

包含安全性日志记录服务器安装指导的 《快速起步指南》适用于各个平台，安装 Novell Audit 1.0.3 时可获得此指南。也可通过万维网查看 《*Novell Audit 1.0.3* 管理指南》中的 《快速起步指南》，请登录 Novell Audit 文档万维网站点 (http://www.novell.com/documentation/nsureaudit)。

10.4 日志记录配置

Identity Manager 允许使用多个预定义级别配置进行日志记录的事件，或单独选择每个要记录的事件来进行配置。同时还会记录对配置设置的更改。

每次启用日志记录后，都会对用户定义的事件 （“用户定义的事件”在第 213 页 中讨论）进行日志记录，并且从不会被 Metadirectory 引擎过滤。

可在驱动程序集或单个驱动程序中对日志记录进行配置。驱动程序可继承驱动程序集的日志记录配置。有关包含日志信息的 eDirectory™ 特性信息，请参见 “eDirectory 对象”在第 215 页 。

默认情况下，仅记录关键事件和用户定义的事件。

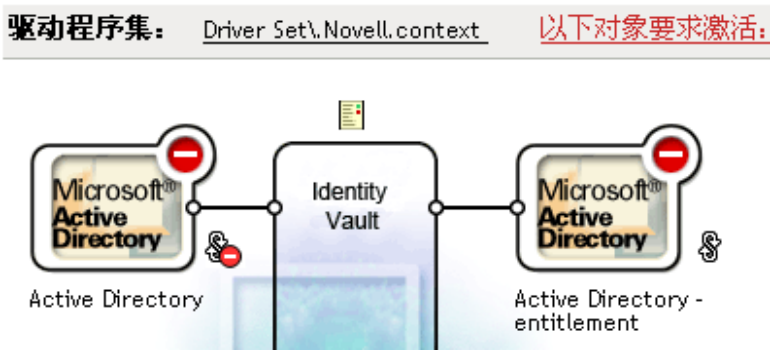
10.4.1 选择要记录的事件

可以选择驱动程序集要记录的事件或特定驱动程序要记录的事件。

驱动程序集的事件日志记录：

1. 在 iManager 中，选择 *Identity Manager* >"Identity Manager 概述 "，然后单击 " 下一步 "。
2. 浏览并选择驱动程序集对象，然后单击 " 搜索 "。

3 单击驱动程序集名称。出现 " 修改对象 " 页。



4 在 *Identity Manager* 选项卡中，选择 " 日志级别 "。

5 选择运行环境所需的日志记录选项。

选项	说明
记录错误	这是默认日志级别。此选项记录所有具有错误状态的事件以及用户定义的事件。 如果选中此选项，只会接收到 ID 为 196646 （十进制）的事件，错误讯息储存在其中的第一个文本字段中。
记录错误和警告	此选项记录所有具有错误或警告状态的事件，以及用户定义的事件。 如果选中此选项，会接收到 ID 为 196646 和 196647 （十进制）的事件，错误或警告讯息储存在其中的第一个文本字段中。

选项	说明
日志特定事件	此选项允许从列表中选择要进行日志记录的特定事件。单击 图标选择事件。任何时候都会记录用户定义的事件。 要记录除错误或警告之外的任何其它事件，必须从此列表中选择此事件。如果选中此选项，并且希望继续记录错误和警告，则必须同时选择错误和警告。有关全部可用事件的列表，请参见“Identity Manager 事件”在第 212 页。
只更新上一次日志时间	只记录用户定义的事件。事件发生时，将更新上一次日志时间，因此可以在状态日志中查看上一次错误发生的时间和日期。
注销	只记录用户定义的事件。
关闭对 DriverSet、Subscriber 和 Publisher 日志的记录	关闭对驱动程序集对象以及订购者和发布者的日志记录。
日志中的最大项数	通过此设置可以指定状态日志中记录的最大项数。有关详细信息，请参见“查看状态日志”在第 219 页。

6 选定要记录的事件后，单击 " 确定 "。

驱动程序的事件日志记录：

1 在 iManager 中，选择 *Identity Manager* >"Identity Manager 概述 "，然后单击 " 下一步 "。

2 浏览并选择驱动程序集对象，然后单击 " 搜索 "。

3 单击驱动程序图标的右上角，然后选择 " 编辑属性 "。

4 在 *Identity Manager* 选项卡中，选择 " 日志级别 "。

5 （可选）默认情况下，驱动程序对象被配置为继承其驱动程序集对象的日志设置。要单独为此驱动程序选择要记录事件，请取消选择使用驱动程序集的日志设置。

6 选择运行环境所需的日志记录选项。

选项	说明
记录错误	这是默认日志级别。此选项记录所有具有错误状态的事件以及用户定义的事件。 如果选中此选项，只会接收到 ID 为 196646 （十进制）的事件，错误讯息储存在其中的第一个文本字段中。
记录错误和警告	此选项记录所有具有错误或警告状态的事件，以及用户定义的事件。 如果选中此选项，会接收到 ID 为 196646 和 196647 （十进制）的事件，错误或警告讯息储存在其中的第一个文本字段中。
日志特定事件	此选项允许从列表中选择要进行日志记录的特定事件。单击  图标选择事件。任何时候都会记录用户定义的事件。 要记录除错误或警告之外的任何其它事件，必须从此列表中选择此事件。如果选中此选项，并且希望继续记录错误和警告，则必须同时选择错误和警告。有关全部可用事件的列表，请参见“Identity Manager 事件”在第 212 页。
只更新上一次日志时间	只记录用户定义的事件。事件发生时，将更新上一次日志时间，因此可以在状态日志中查看上一次错误发生的时间和日期。

选项	说明
注销	只记录用户定义的事件。
关闭对 DriverSet、Subscriber 和 Publisher 日志的记录。	关闭对驱动程序集对象以及订购者和发布者日志的记录。
日志中的最大项数	通过此设置可以指定状态日志中记录的最大项数。有关详细信息，请参见 “查看状态日志”在第 219 页 。

7 选定要记录的事件后，单击 " 确定 "。

Identity Manager 事件

Identity Manager 记录的全部事件列表包含在附录 C “Identity Manager 事件和报告”在第 241 页 中。

驱动程序启动和停止事件

每当驱动程序启动或停止时， Identity Manager 都可以生成事件。下表包含这些事件的详细信息：

表 ***10-1*** 驱动程序启动和停止事件

事件	日志级别	信息
EV_LOG_DRIVER_START	LOG_INFO	要记录驱动程序的启动，必须使用 " 日志特定事件 " 选项并选择此事件。
EV_LOG_DRIVER_STOP	LOG_WARNING	要记录驱动程序的停止，请选择 " 记录错误和警告 "，或使用 " 日志特定事件 " 选项并选择此事件。

根据这些事件创建 Novell Audit 通知的详细信息，请参见 “根据事件发送通知”在第 216 页 。

错误和警告事件

每次遇到错误或警告时， Identity Manager 都会生成事件。下表包含这些事件的详细信息：

表 ***10-2*** 错误和警告事件

事件	日志级别	信息
DirXML_Error	LOG_ERROR	所有 Identity Manager 错误都记录为此事件。遇到的实际错误代码储存在此事件中。 要记录错误，请选择 " 记录错误 "、" 记录错误和警告 "，或使用 " 日志特定事件 " 选项并选择此事件。

事件	日志级别	信息
DirXML_Warning	LOG_WARNING	所有 Identity Manager 警告都记录为此事件。遇到的实际警告代码储存到此事件中。 要记录警告，请选择 " 记录错误和警告 "，或使用 " 日志特定事件 " 选项并选择此事件。

根据这些事件创建 Novell Audit 通知的详细信息，请参见 “根据事件发送通知”在第 216 页 。

远程装载程序事件

从远程装载程序记录以下事件：

表 ***10-3*** 远程装载程序事件

事件	日志级别	信息
远程装载程序启动 (Remote Loader Start)	LOG_INFO	要记录远程装载程序启动的时间，则必须使用 " 日志特定事件 " 选项并选择此事件。
远程装载程序停止 (Remote Loader Stop)	LOG_INFO	要记录远程装载程序停止的时间，则必须使用 " 日志特定事件 " 选项并选择此事件。
已建立远程装载程序连接 (Remote Loader Connection Established)	LOG_INFO	要记录远程装载程序建立连接的时间，则必须使用 " 日志特定事件 " 选项并选择此事件。
远程装载程序已落线 (Remote Loader Connection Dropped)	LOG_INFO	要记录远程装载程序落线的时间，则必须使用 " 日志特定事件 " 选项并选择此事件。

根据这些事件创建 Novell Audit 通知的详细信息，请参见 “根据事件发送通知”在第 216 页 。

10.4.2 用户定义的事件

Identity Manager 允许配置记录到 Novell Audit 的自己的事件。可使用策略构建器中的操作或在样式表中记录事件。可以记录定义策略时已访问的任何信息。

事件 **ID**

1000 至 1999 间的事件 ID 是专为用户定义的事件而分配的。定义自己的事件时，必须为事件 ID 指定一个此范围内的值。在 Novell Audit 中，此 ID 与 Identity Manager 应用程序 ID 003 相组合。

日志级别

日志级别允许根据被记录的事件类型将事件分组。以下预定义的日志级别可用：

表 *10-4* 日志级别

日志级别	说明
记录紧急事件	引起 Metadirectory 引擎或驱动程序关闭的事件。
记录警报	需要立即注意的事件。
记录关键	引起 Metadirectory 引擎或驱动程序部分出现故障的事件。
记录错误	说明可由 Metadirectory 引擎或驱动程序处理的错误的事件。
记录警告	否定事件不表示问题。
记录通知	管理员可以用于了解或改进使用和操作的肯定或否定事件。
记录信息	任何重要的肯定事件。
记录调试	用于支持或用于工程师调试 Metadirectory 引擎或驱动程序操作的相关事件。

使用策略构建器生成事件

在策略构建器中，通过选择 " 生成事件 " 操作来记录事件。

1. 生成事件之前，选择要符合的条件，然后选择 " 生成事件 " 操作。
2. 指定事件 ID。
3. 选择日志级别。
4. 单击 " 输入字符串 " 字段旁的 图标启动命名字符串构建器。
5. 使用命名字符串构建器构造对应于自定义数据字段的命名字符串：

6. 单击 " 确定 " 返回到策略构建器以构造策略的其余部分。

有关如何配置策略以记录事件的信息，请参见 《策略构建器和驱动程序自定义指南》中的 “" 生成事件 "”。

使用状态文档生成事件

对于使用 <xsl:message> 要素通过样式表生成的状态文档，可使用对应于下表中指定的状态文档的级别特性的事件 ID 发送给 Novell Audit：

表 *10-5* 状态文档

状态级别	状态事件 ID
成功	EV_LOG_STATUS_SUCCESS (1)
重试	EV_LOG_STATUS_RETRY (2)

状态级别	状态事件 ID
警告	EV_LOG_STATUS_WARNING (3)
错误	EV_LOG_STATUS_ERROR (4)
致命错误	EV_LOG_STATUS_FATAL (5)
用户定义	EV_LOG_STATUS_OTHER (6)

以下示例生成 Novell Audit 事件 0x004， value1=7777，且级别为 EV_LOG_STATUS_ERROR：

```
<xsl:message> <status level="error" text1="This would be text1"
value="7777">This data would be in the blob and in text 2, since no
value is specified for text2 in the attributes.</status> </
xsl:message>
```

以下示例生成 Novell Audit 事件 0x004， value1=7778，且级别为 EV_LOG_STATUS_ERROR：

```
<xsl:message> <status level="error" text1="This would be text1"
text2="This would be text2" value1="7778">This data would be in the
blob only for this case, since a value for text2 is specified in the
attributes.</status> </xsl:message>
```

10.4.3 eDirectory 对象

本节提供有关储存日志数据的 Novell eDirectory 特性的详细信息。由于根据 iManager 中的选择自动配置这些对象，因此不需要直接修改这些特性。

要记录的 Identity Manager 事件储存在驱动程序集对象或驱动程序对象的 DirXML-LogEvent 特性中。此特性是一个多值整数，并且每个值标识要记录的事件 ID。

记录事件之前，引擎检查当前事件类型是否违背此特性的内容，由此来决定是否要记录此事件。

Identity Manager 的以前版本使用 DirXML-DriverTraceLevel 特性来设置日志记录级别。需为每个驱动程序对象指定日志记录级别，并且不支持继承。在 Identity Manager 2 以后的版本中，驱动程序对象可从驱动程序集对象继承此信息。决定日志设置时，驱动程序对象的 DirXML-DriverTraceLevel 特性具有最高优先级。如果驱动程序对象不包含 DirXML-DriverTraceLevel 特性，则引擎使用父驱动程序集对象的日志设置。

10.5 查询和报告

Novell Audit 提供了两个可用于查询 Novell Audit 数据库中的事件的工具：Novell Audit iManager 插件和 Novell Audit Report (LReport)。

Novell Audit iManager 插件是一个基于万维网的 JDBC 数据库查询应用程序，它允许使用下拉列表和宏快速创建和储存查询。

Novell Audit Report 是一个基于 Windows 的遵从 ODBC 的应用程序，它可以使用 SQL 查询语句或 Crystal Decisions Reports 来查询 Oracle 和 MySQL 数据储存器 （或其它任何支持 ODBC 驱动程序的数据库）。

按照 《*Novell Audit* 管理指南》中的指令访问 Novell Audit iManager 插件，或安装 Novell Audit Report。此指南在 Novell Audit 文档万维网站点 (http://www.novell.com/documentation/nsureaudit) 中也可用。

10.5.1 Identity Manager 报告

Identity Manager 提供了大量 Crystal Decisions Reports (*.rpt)，可简化有关在 Identity Manager 中执行的常用操作的信息收集。这些报告包括在 Identity Manager 安装光盘中。

配置完 Novell Audit Report 后，可与任何已定义的自定义查询和报告一起执行这些报告。有关在 Novell Audit Report 中使用这些报告的信息，请参见 《*Novell Audit 1.0.3* 管理指南》中的在 Novell Audit Report 中使用报告 (http://www.novell.com/documentation/nsureaudit/nsureaudit/data/alsn2fj.html)。有关这些报告的示例，请参见附录 C “Identity Manager 事件和报告”在第 241 页 中的 “报告”在第 258 页 。

10.5.2 查看 Identity Manager 事件

1. 在 Novell Audit Report 工作空间中，单击 " 事件 " 选项卡，然后展开 *DirXML* 文件夹。

   此列表包含全部预定义的 Identity Manager 事件。双击列表中的任意事件，查看事件属性。
2. 要查询 Identity Manager 事件，则在工作空间中右击事件，然后选择 " 定义查询 "。
3. 出现 " 查询专家 " 时，指定时间帧，并验证事件。
4. 要运行此查询，则在工作空间中选择 " 查询 " 选项卡，右击查询名称，然后选择 " 运行 "。

也可使用 SQL 语句创建查询。所有 Identity Manager 事件都具有 109608 至 262144 之间的十进制事件 ID。

10.6 根据事件发送通知

Novell Audit 提供了发生或不发生特定事件时发送通知的功能。将根据一个或多个事件和包含在这些事件中的任何值发送通知。通知可发送给任何日志记录通道，允许将通知记录到数据库、 Java 应用程序、 SNMP 管理系统或其它多个位置。

有关创建通知的信息，请参见 《*Novell Audit 1.0.3* 管理指南》中的 " 配置过滤器和事件通知 " (http://www.novell.com/documentation/nsureaudit/nsureaudit/data/al0lg08.html#al0lg08)

10.7 使用状态日志

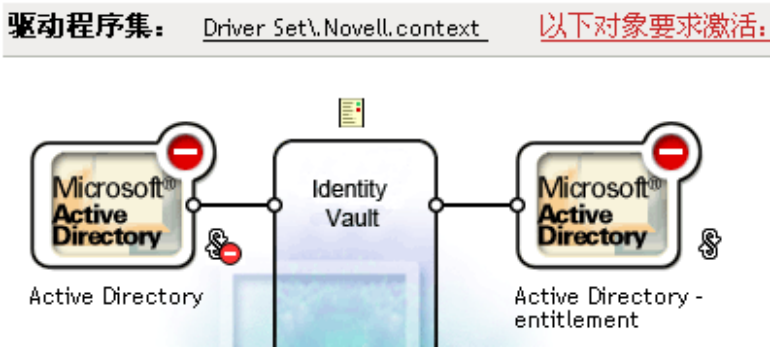
除了由 Novell Audit 提供的功能之外， Identity Manager 可以记录驱动程序集对象和驱动程序对象上指定数量的事件。这些状态日志提供了对最近 Identity Manager 活动的查看。日志达到集大小后，将永久性去除最旧的一半日志，以为更近事件清除空间。因此，应将任何要随时跟踪的事件记录到 Novell Audit 或报告和通知服务器中。

10.7.1 设置最大日志大小

可以将状态日志配置为暂挂 50 至 500 个事件。可在驱动程序集对象上配置此设置，以让集中的所有驱动程序继承它，或者也可为集中的每个驱动程序配置此设置。将单独操作已选择为要记录的事件的最大日志大小，因此可在驱动程序集中配置要记录的事件，然后为集中的每个驱动程序指定不同日志大小。

设置驱动程序集的日志大小

1. 在 iManager 中，选择 *Identity Manager* >"Identity Manager 概述 "，然后单击 " 下一步 "。
2. 浏览并选择驱动程序集对象，然后单击 " 搜索 "。
3. 单击驱动程序集名称。出现 " 修改对象 " 窗口。



4. 在 *Identity Manager* 选项卡中，选择 " 日志级别 "。

5 在 " 日志中的最大项数 " 字段中指定最大日志大小：

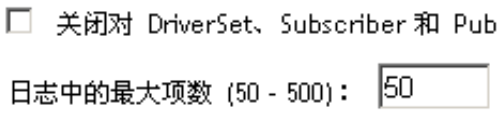
6 指定最大数之后，单击 " 确定 "。

设置驱动程序的日志大小

1 在 iManager 中，选择 *Identity Manager* >"Identity Manager 概述 "，然后单击 " 下一步 "。
2 浏览并选择驱动程序集对象，然后单击 " 搜索 "。
3 单击驱动程序图标的右上角，然后选择 " 编辑属性 "。

4 在 *Identity Manager* 选项卡中，选择 " 日志级别 "。

5 在 " 日志中的最大项数 " 字段中指定最大日志大小：



6 指定最大数之后，单击 " 确定 "。

10.7.2 查看状态日志

在 iManager 中，用状态日志图标 表示状态日志项。在 iManager 中任何可以看到此图标的地方，都可以查看短期日志。以下状态日志可用：

- 驱动程序集中的状态日志。
- 集中每个驱动程序的发布者通道中的状态日志。
- 集中每个驱动程序的订购者通道中的状态日志。

发布者和订购者通道的状态日志报告由驱动程序生成的特定通道的讯息，如非关联对象禁用的操作。

驱动程序集的状态日志仅包含由引擎生成的讯息，如驱动程序集中任何驱动程序的状态更改。将记录所有引擎讯息。

DirXML 命令行实用程序

A

安装 Identity Manager 时，实用程序和底稿应安装在所有平台。实用程序应安装在以下位置：

- Windows：\Novell\Nds\dxcmd.bat
- NetWare：sys:\system\dxcmd.ncf
- UNIX：/usr/bin/dxcmd

有两种不同的方法可使用 DirXML 命令行实用程序。

- “交互方式”在第 221 页
- “命令行方式”在第 229 页

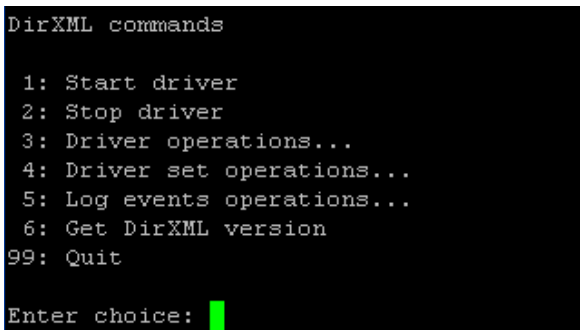
A.1 交互方式

交互方式提供了一个可控制并使用 DirXML 命令行实用程序的文本界面。

1. 在控制台中输入 dxcmd。
2. 输入具有 Identity Manager 对象的足够权限的用户名。

   示例：admin.novell
3. 输入上面指定的用户的口令。

   示例：novell



4. 输入要执行的命令号。

   表 A-1 在第 222 页 中包含了选项列表和可用功能。
5. 输入 99 退出实用程序。

注释：如果正在 Unix 或 Linux 中运行 eDirectory™ 8.8，则必须指定 -host 和 -port 参数。例如， dxcmd -host 10.0.0.1 -port 524。如果未指定这些参数，会发生 jclient 错误。

```
novell.jclient.JCException£½ ¡¨¾"£®µ¾µÿ÷²£©111 µƒŒ¥÷™¥ÌŒÛ
```

默认情况下，eDirectory 8.8 不监听本机。DirXML 命令行实用程序需要解析要鉴定的服务器 IP 地址或主机名称和端口。

表 ***A-1*** 交互方式选项

选项	说明
1: *Start Driver （启动驱动程序）*	启动驱动程序。如果存在多个驱动程序，则用编号列出每个驱动程序。输入驱动程序编号可启动驱动程序。
2: *Stop Driver （停止驱动程序）*	停止驱动程序。如果存在多个驱动程序，则用编号列出每个驱动程序。输入驱动程序编号可停止驱动程序。
3: *Driver operations （驱动程序操作）*	列出可用于驱动程序的操作。如果存在多个驱动程序，则用编号列出每个驱动程序。输入驱动程序编号可查看可用操作。有关可用操作，请参见表 A-2 在第 223 页。
4: *Driver set operations （驱动程序集操作）*	列出可用于驱动程序集的操作。 ◆ 1: 关联驱动程序集与服务器 (Associate driver set with server) ◆ 2: 解除驱动程序集与服务器的关联 (Disassociate driver set from server) ◆ 99: 退出 (Exit)
5: *Log events operations （日志事件操作）*	列出可用于通过 Novell Audit 的日志记录事件的操作。有关这些选项的说明，请参见表 A-5 在第 227 页。
6: *Get DirXML version （获取 DirXML 版本）*	列出已安装的 Identity Manager 的版本。
99: *Quit （退出）*	退出 DirXML 命令行实用程序

图 ***A-1*** 驱动程序选项

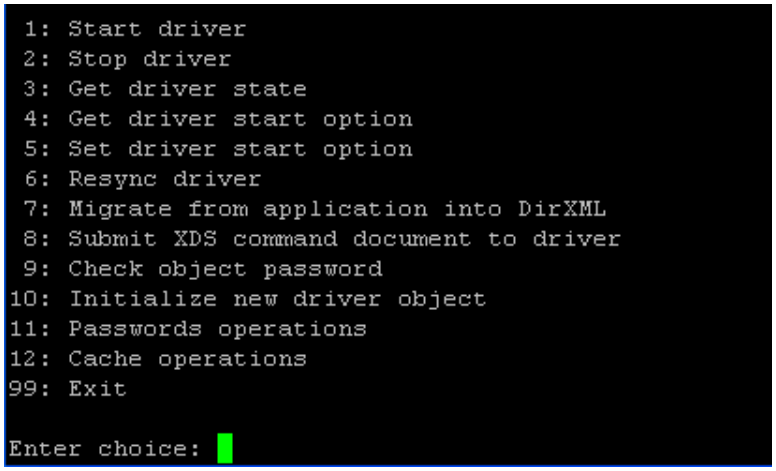


表 ***A-2*** 驱动程序选项

选项	说明
1: *Start driver （启动驱动程序）*	启动驱动程序。
2: *Stop driver （停止驱动程序）*	停止驱动程序。
3: *Get driver state （获取驱动程序状态）*	列出驱动程序的状态。 ◆ 0 - 驱动程序已停止 ◆ 1 - 驱动程序正在启动 ◆ 2 - 驱动程序正在运行 ◆ 3 - 驱动程序正在停止
4: *Get driver start option （获取驱动程序启动选项）*	列出当前驱动程序启动选项。 ◆ 1 - 禁止 ◆ 2 - 手工 ◆ 3 - 自动
5: *Set driver start option （设置驱动程序启动选项）*	更改驱动程序的启动选项。 ◆ 1 - 禁止 ◆ 2 - 手工 ◆ 3 - 自动 ◆ 99 - 退出
6: *Resync driver （重新同步驱动程序）*	强制重新同步驱动程序。它提示时间延迟：是否要为重新同步指定最小时间？ （是 / 否）。 如果输入 "yes"，则需指定发生同步的日期和时间："输入日期和时间 （格式 9/27/05 3:27 PM） "。 如果输入 "no"，则立即发生同步。
7: *Migrate from application into DirXML （从应用程序迁移至 DirXML）*	处理包含查询命令的 XML 文档：*Enter filename of XDS query document*（输入 XDS 查询文档的文件名）： 通过使用 Novell nds.dtd (http://developer.novell.com/ndk/doc/dirxml/dirxmlbk/ref/ndsdtd/query.html)，创建包含查询命令的 XML 文档。 示例： NetWare：sys:\files\query.xml Windows：c:\files\query.xml Linux：/files/query.xml

选项	说明
8: *Submit XDS command document to driver （向驱动程序提交 XDS 命令文档）*	处理 XDS 命令文档： *Enter filename of XDS command document （输入 XDS 命令文档的文件名）：* 示例： NetWare：sys:\files\user.xml Windows：c:\files\user.xml Linux：/files/user.xml *Enter name of file for response （输入用作响应的文件名）：* 示例： NetWare：sys:\files\user.log Windows：c:\files\user.log Linux：/files/user.log
9: *Check object password （检查对象口令）*	确认已连接系统中的对象的口令是否与驱动程序关联。它与对象的 eDirectory 口令匹配（分发口令，与通用口令一起使用）。 输入用户名：(Enter user name:)
10: *Initialize new driver object （初始化新驱动程序对象）*	在新驱动程序对象上执行数据的内部初始化。此操作仅用于测试目的。
11: *Password operations （口令操作）*	有九个口令选项。有关这些选项的说明，请参见表 A-3 在第 225 页。
12: *Cache operations （超速缓存操作）*	有五个超速缓存操作。有关这些选项的说明，请参见表 A-4 在第 226 页。
99: *Exit （退出）*	退出驱动程序选项。

图 ***A-2*** 口令操作

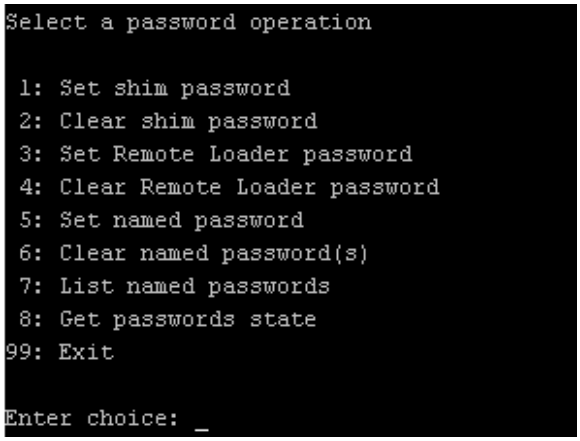


表 ***A-3*** 口令操作

操作	说明
1: *Set shim password （设置 Shim 口令）*	设置应用程序口令。这是在登录已连接系统时用于鉴定的用户帐户口令。
2: *Clear shim password （清除 Shim 口令）*	清除应用程序口令。
3: *Set Remote Loader password （设置远程装载程序口令）*	远程装载程序口令用于控制对远程装载程序实例的访问。有关更多信息，请参见第 3 章 “设置已连接系统”在第 41 页 。 输入远程装载程序口令，然后通过再输入一遍来确认口令。
4: *Clear Remote Loader password （清除远程装载程序口令）*	清除远程装载程序口令，以便驱动程序对象上不再设置有远程装载程序口令。
5: *Set named password （设置命名口令）*	允许将口令或其它安全性信息储存到驱动程序中。有关更多信息，请参见“使用命名口令”在第 27 页 。 有四个要填充的提示： ◆ 输入口令名称：(Enter password name:) ◆ 输入口令说明：(Enter password description:) ◆ 输入口令：(Enter password:) ◆ 确认口令 (Confirm password)
6: *Clear named passwords （清除命名口令）*	清除储存在驱动程序对象中的指定命名口令或全部命名口令：*是否要清除全部命名口令？ （是 / 否）*。 如果输入 "yes"，则清除全部命名口令。如果输入 "no"，则提示指定要清除的口令名称。
7: *List named passwords （列出命名口令）*	列出储存在驱动程序对象中的全部命名口令。它列出口令名称和口令说明。
8: *Get password state （获取口令状态）*	列出口令是否设置为以下状态： ◆ 驱动程序对象口令：(Driver Object password:) ◆ 应用程序口令：(Application password:) ◆ 远程装载程序口令：(Remote loader password:) dxcmd 实用程序允许设置应用程序口令和远程装载程序口令。使用此实用程序不能设置驱动程序对象口令。它显示是否已设置驱动程序对象口令。
99: *Exit （退出）*	退出当前菜单并返回到驱动程序选项。

图 ***A-3*** 超速缓存操作

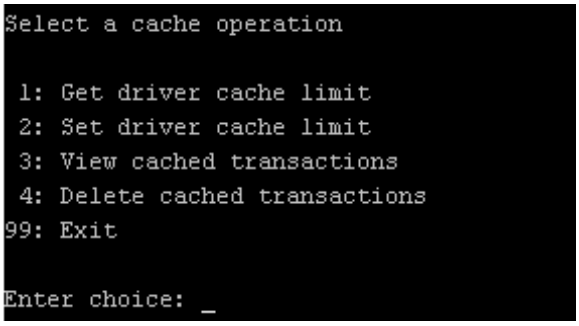


表 ***A-4*** 超速缓存操作

操作	说明
1: *Get driver cache limit （获取驱动程序超速缓存限制）*	显示为驱动程序设置的当前超速缓存限制。
2: *Set driver cache limit （设置驱动程序超速缓存限制）*	设置驱动程序超速缓存限制（以 KB 为单位）。0 值表示无限制。
3: *View cached transactions （查看已超速缓存的事务）*	用储存在超速缓存中的事件创建文本文件。可以选择要查看的事务数。 ◆ Enter option token (default=0): （输入选项令牌 （默认值 =0）：） ◆ Enter maximum transactions records to return (default=1): （输入要返回的最大事务记录（默认值 =1）：） ◆ Enter name of file for response: （输入用作响应的文件名：）
4: *Delete cached transactions （删除已超速缓存的事务）*	删除储存在超速缓存中的事务。 ◆ Enter position token (default=0): （输入位置令牌 （默认值 =0）：） ◆ Enter event-id value of first transaction record to delete (optional): （输入要删除的第一个事务记录的事件 ID 值 （可选）：） ◆ Enter number of transaction records to delete (default=1): （输入要删除的事务记录数 （默认值 =1）：）
99: *Exit （退出）*	退出当前菜单并返回到驱动程序选项。

图 ***A-4*** 日志事件操作

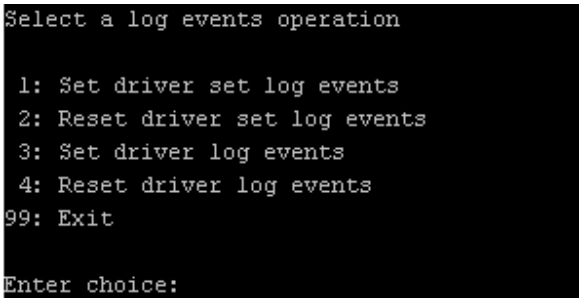


表 ***A-5*** 日志事件操作

操作	说明
1: *Set driver set log events （设置驱动程序集日志事件）*	允许记录通过 Novell Audit 的驱动程序集事件。有 49 个可选择记录的项目。有关这些选项的列表，请参见表 A-6 在第 227 页。 输入要记录的项目编号。选择项目之后，输入 99 以接受选择。
2: *Reset driver set log events （重设置驱动程序集日志事件）*	重设置全部日志事件选项。
3: *Set driver log events （设置驱动程序日志事件）*	允许记录通过 Novell Audit 的驱动程序事件。有 49 个可选择记录的项目。有关这些选项的列表，请参见表 A-6 在第 227 页。 输入要记录的项目编号。选择项目之后，输入 99 以接受选择。
4: *Reset driver log events （重设置驱动程序日志事件）*	重设置全部日志事件选项。
99: *Exit （退出）*	退出日志事件操作菜单。

表 ***A-6*** 驱动程序集和驱动程序日志事件

选项
1: Status success （成功状态）
2: Status retry （重试状态）
3: Status warning （警告状态）
4: Status error （错误状态）
5: Status fatal （致命状态）
6: Status other （其它状态）
7: Query elements （查询要素）
8: Add elements （添加要素）

选项
9: Remove elements （去除要素）
10: Modify elements （修改要素）
11: Rename elements （重命名要素）
12: Move elements （移动要素）
13: Add-association elements （添加关联要素）
14: Remove-association elements （去除关联要素）
15: Query-schema elements （查询纲要要素）
16: Check-password elements （检查口令要素）
17: Check-object-password element （检查对象口令要素）
18: Modify-password elements （修改口令要素）
19: Sync elements （同步要素）
20: Pre-transformed XDS document from shim （从 Shim 预转换 XDS 文档）
21: Post input transformation XDS document （张贴输入转换 XDS 文档）
22: Post output transformation XDS document （张贴输出转换 XDS 文档）
23: Post event transformation XDS document （张贴事件转换 XDS 文档）
24: Post placement transformation XDS document （张贴位置转换 XDS 文档）
25: Post create transformation XDS document （张贴创建转换 XDS 文档）
26: Post mapping transformation <inbound> XDS document （张贴映射转换 (入站) XDS 文档）
27: Post mapping transformation <outbound> XDS document （张贴映射转换 (出站) XDS 文档）
28: Post matching transformation XDS document （张贴匹配转换 XDS 文档）
29: Post command transformation XDS document （张贴命令转换 XDS 文档）
30: Post-filtered XDS document <Publisher> （过滤张贴的 XDS 文档 (发布者)）
31: User agent XDS command document （用户代理 XDS 命令文档）
32: Driver resync request （驱动程序重新同步请求）
33: Driver migrate from application （从应用程序迁移驱动程序）
34: Driver start （驱动程序启动）
35: Driver stop （驱动程序停止）
36: Password sync （口令同步）
37: Password request （口令请求）
38: Engine error （引擎错误）
39: Engine warning （引擎警告）
40: Add attribute （添加特性）

选项
41: Clear attribute （清除特性）
42: Add value （添加值）
43: Remove value （去除值）
44: Merge entire （全部合并）
45: Get named password （获取命名口令）
46: Unknown （未知）
47: Unknown （未知）
48: User defined IDs （用户定义的 ID）
99: Accept checked items （接受已检查的项目）

A.2 命令行方式

命令行方式允许您使用底稿或批文件。表 A-7 在第 229 页 包含各种可用选项。

若要使用命令行选项，请确定要使用的项目并将它们排在一起。

示例：dxcmd -user admin.headquarters -host 10.0.0.1 -password n0vell -start test.driverset.headquarters

此命令随即启动驱动程序。

表 ***A-7*** 命令行选项

选项	说明
配置	
-user < *用户名* >	指定用户的名称，该用户具有对要测试的驱动程序的管理权限。
-host < *主机名或 IP 地址* >	指定安装驱动程序的服务器的 IP 地址。
-password < *用户口令* >	指定前面指定的用户的口令。
-port < *端口号* >	指定端口号 （如果不使用默认端口）。
-q < *安静方式* >	执行命令时仅显示少量信息。
-v < *冗长方式* >	执行命令时显示详细信息。
-? < *显示此讯息* >	显示帮助菜单。
-help < *显示此讯息* >	显示帮助菜单。
操作	
-start < *驱动程序 dn*>	启动驱动程序。
-stop < *驱动程序 dn*>	停止驱动程序。
-getstate < *驱动程序 dn*>	显示驱动程序状态为正在运行或已停止。

选项	说明
-getstartoption < *驱动程序 dn*>	显示驱动程序的启动选项。
-setstartoption < *驱动程序 dn*> <*disabled*|*manual*|*auto*> <*resync*|*noresync*>	设置驱动程序在重引导服务器时的启动方式。设置重启动驱动程序时是否要重新同步对象。
-getcachelimit < *驱动程序 dn*>	列出驱动程序的超速缓存限制设置。
-setcachelimit < *驱动程序 dn*> <*0 或正整数* >	设置驱动程序的超速缓存限制。
-migrateapp < *驱动程序 dn*> < *文件名* >	处理包含查询命令的 XML 文档。
	通过使用 Novell nds.dtd (http://developer.novell.com/ndk/doc/dirxml/dirxmlbk/ref/ndsdtd/query.html)，创建包含查询命令的 XML 文档。
-setshimpassword < *驱动程序 dn*> < *口令* >	设置应用程序口令。这是在登录已连接系统时用于鉴定的用户帐户口令。
-clearshimpassword < *驱动程序 dn*> < *口令* >	清除应用程序口令。
-setremoteloaderpassword < *驱动程序 dn*> < *口令* >	设置远程装载程序口令。
	远程装载程序口令用于控制对远程装载程序实例的访问。有关更多信息，请参见第 3 章 “设置已连接系统”在第 41 页。
<clearremoteloaderpassword < *驱动程序 dn*>	清除远程装载程序口令。
-sendcommand < *驱动程序 dn*> < *输入文件名* > < *输出文件名* >	处理 XDS 命令文档。
	将 XDS 命令文档指定为输入文件。
	示例：
	NetWare：sys:\files\user.xml
	Windows：c:\files\user.xml
	Linux：/files/user.log
	指定输出文件名以查看结果。
	示例：
	NetWare：sys:\files\user.log
	Windows：c:\files\user.log
	Linux：/files/user.log
-setlogevents <*dn*> < *整数 ...*>	为驱动程序设置 Novell Audit 日志事件。整数是要记录项目的选项。有关可输入的整数列表，请参见表 A-6 在第 227 页。
-clearlogevents <*dn*>	清除为驱动程序设置的所有 Novell Audit 日志事件。
-setdriverset < *驱动程序集 dn*>	将驱动程序集与服务器相关联。
-cleardriverset	清除服务器与驱动程序集的关联。
-getversion	显示已安装 Identity Manager 的版本。

选项	说明
-initdriver object <*dn*>	在新驱动程序对象上执行数据的内部初始化。此选项仅用于测试。
-setnamedpassword < *驱动程序 dn*> < *名称* > < *口令* > *[说明]*	为驱动程序对象设置命名口令。指定命名口令的名称、口令和说明。
-clearnamedpassword < *驱动程序 dn*> < *名称* >	清除指定的命名口令。
-clearallnamedpaswords < *驱动程序 dn*>	清除为特定驱动程序设置的所有命名口令。

用于配置远程装载程序的选项

B

下表中的选项允许您配置远程装载程序。

表 ***B-1*** 远程装载程序选项

选项	别名	参数	说明
address		IP 地址	可选参数。指定远程装载程序监听特定本地 IP 地址。如果托管远程装载程序的服务器有多个 IP 地址，但远程装载程序只能监听其中一个地址时，这个参数将非常有用。 可以选择以下三项操作之一：address= *地址号* address= 誰 ocalhost' 不使用此参数。 如果不使用 -address，则远程装载程序将监听所有本地 IP 地址。 示例：address=137.65.134.83
-class	-cl	Java 类名	指定被托管的 Identity Manager 应用程序 Shim 的 Java 类名称。 例如，对于 Java 驱动程序，键入以下内容之一： -class com.novell.nds.dirxml.driver.ldap.LDAPDriverShim -cl com.novell.nds.dirxml.driver.ldap.LDAPDriverShim Java 使用密钥存储区读取证书。-class 选项和 -module 选项互相排斥。 若要查看 Java 类名列表，请参见表 B-2 在第 238 页。
-commandport	-cp	端口号	指定远程装载程序实例进行控制时使用的 TCP/IP 端口。如果远程装载程序实例要托管应用程序 Shim，则命令端口将是其它远程装载程序实例与托管 Shim 的实例通信的端口。如果远程装载程序实例要将命令发送至托管应用程序 Shim 的实例，则命令端口将是托管实例监听的端口。如果没有指定命令端口，则默认端口为 8000。通过指定不同的连接端口和命令端口，远程装载程序的多个实例可以在托管不同驱动程序实例的同一台服务器上运行。 示例： -commandport 8001 -cp 8001

选项	别名	参数	说明
-config	无	文件名	指定配置文件。配置文件可以包含除 config 之外的任意命令行选项。命令行中指定的选项将覆盖配置文件中指定的选项。 示例： -config config.txt
-connection	-conn	连接配置字符串	为运行 Identity Manager 远程接口 Shim 的 Metadirectory 服务器的连接指定连接参数。远程装载程序的默认连接方式为使用 SSL 的 TCP/IP。此连接的默认 TCP/IP 端口是 8090。远程装载程序的多个实例可以在同一台服务器上运行。远程装载程序的每个实例都托管一个单独的 Identity Manager 应用程序 Shim 实例。通过为每个远程装载程序实例指定不同的连接端口和命令端口，可以区分远程装载程序的多个实例。 示例： -connection "port=8091 rootfile=server1.pem" -conn "port=8091 rootfile=server1.pem"
-description	-desc	简短说明	指定要用于跟踪窗口标题和 Novell® Audit 记录的简短描述字符串 （例如 SAP）。 示例： -description SAP -desc SAP 远程装载程序控制台在配置文件中使用长格式。可以使用长格式 （例如 -description）或者短格式 （例如 -desc）。
-help	-?	无	显示帮助。 示例： -help -?
-java	-j	无	指定要为 Java Shim 实例设置口令。此选项仅在与 setpasswords 选项一起使用时才有用。如果与 -setpasswords 一起指定了 -class，则无需使用此选项。
-javadebugport	-jdp	端口号	指定该远程装载程序实例将会在指定端口启用 Java 调试。此选项对 Identity Manager 应用程序 Shim 的开发者很有用。 示例： -javadebugport 8080 -jdp 8080

选项	别名	参数	说明
密钥存储区			条件性参数。仅用于 .jar 文件中包含的 Identity Manager 应用程序 Shim。 指定 Java 密钥存储区文件名，密钥存储区中包含远程接口 Shim 所使用证书的颁发者的可信根证书。这通常是托管远程接口 Shim 的 eDirectory™ 树的证书授权者。 如果要运行 SSL 并需要远程装载程序与 Java 驱动程序通讯，请键入键值对： keystore='*keystorename*' storepass='*password*'
-module	-m	模块名	指定包含被托管的 Identity Manager 应用程序 Shim 的模块。 例如，对于本机驱动程序，请键入以下内容之一： -module "c:\Novell\RemoteLoader\Exchange5Shim.dll" -m "c:\Novell\RemoteLoader\Exchange5Shim.dll" 或者 -module "usr/lib/dirxml/NISDriverShim.so" -m "usr/lib/dirxml/NISDriverShim.so" -module 选项使用 rootfile 证书。-module 选项和 -class 选项互相排斥。
-password	-p	口令	指定用于命令鉴定的口令。通过 setpasswords 为命令所针对的装载程序实例指定的第一个口令必须与此口令相同。如果指定了某一命令选项（例如，unload 或 tracechange），而未指定 password 选项，系统将提示用户输入作为命令目标的装载程序的口令。 示例： -password novell4 -p novell4
端口		十进制端口号	必需参数。它指定远程装载程序监听与远程接口 Shim 的连接所使用的 TCP/IP 端口。 示例： port=8090
rootfile			条件性参数。如果要运行 SSL 并需要远程装载程序与本机驱动程序通讯，请键入 rootfile='*trusted certname*'

选项	别名	参数	说明
-service	-serv	无、或安装 / 未安装	若要将实例安装为服务，请使用安装自变量以及任何其它托管应用程序 Shim 所必需的自变量。例如，使用的自变量必须包括 -module，但是任何自变量都可以包括 -connection、- commandport 等。 此选项将安装 Win32 服务但不会启动此服务。 若要卸装运行为服务的实例，请使用卸装自变量以及任何其它托管应用程序 Shim 所必需的自变量。 此选项的无自变量版本仅用在运行为 Win32 服务的实例的命令行中。将实例安装为服务时，将自动设置此选项。 示例： -service install -serv uninstall 此选项不适用于 rdxml 或 Java 远程装载程序。
-setpasswords	-sp	口令 口令	指定远程装载程序实例口令、与此远程装载程序通讯的远程接口 Shim 的 Identity Manager 驱动程序对象口令。自变量中的第一个口令是远程装载程序的口令。可选自变量中的第二个口令是与 Metadirectory 服务器上远程接口 Shim 关联的 Identity Manager 驱动程序对象的口令。可以不指定口令，但如果指定，则必须同时指定两个口令。如果未指定口令，则远程装载程序将提示输入口令。这是一个配置选项。使用此选项可配置具有指定口令的远程装载程序实例，但不会加载 Identity Manager 应用程序 Shim 或与其它装载程序实例通讯。 示例： -setpasswords novell4 staccato3 -sp novell4 staccato3
-storepass		存储区口令	仅用于 .jar 文件中包含的 Identity Manager 应用程序 Shim。指定由 keystore 参数指定的 Java 密钥存储区口令。 示例： storepass=mypassword 此选项仅应用于 Java 远程装载程序。
-trace	-t	整数	指定跟踪级别。仅当托管应用程序 Shim 时才可使用此选项。跟踪级别与 Metadirectory 服务器中使用的级别相对应。 示例： -trace 3 -t 3

选项	别名	参数	说明
-tracechange	-tc	整数	支配将托管应用程序 Shim 的远程装载程序实例以更改其跟踪级别。跟踪级别与 Metadirectory 服务器中使用的级别相对应。 示例： -tracechange 1 -tc 1
-tracefile	-tf	文件名	指定要写入跟踪讯息的文件。如果跟踪级别大于 0，则将跟踪讯息写入此文件。即使未打开跟踪窗口，也可将跟踪讯息写入此文件。 示例： -tracefile c:\temp\trace.txt -tf c:\temp\trace.txt
-tracefilechange	-tfc	无，或文件名	支配将托管应用程序 Shim 的远程装载程序实例，以便开始使用跟踪文件，或关闭已使用的跟踪文件并使用一个新跟踪文件。使用此选项的无自变量版本将导致托管实例关闭正在使用的任何跟踪文件。 示例： -tracefilechange c:\temp\newtrace.txt tfc c:\temp\newtrace.txt
-tracefilemax	-tfm	大小	指定跟踪文件数据可占用的最大磁盘空间 （近似值）。如果指定此选项，将有一个由 tracefile 选项指定其名称的跟踪文件，以及最多 9 个附加的 " 翻转 " 文件。翻转文件以其主跟踪文件的文件名作为基本名，后跟 "*_n*"，其中 n 为从 1 到 9 的数字。 大小参数为字节数。可使用后缀 K、 M 或 G 来指定大小，它们分别代表 KB、 MB 或 GB。 如果启动远程装载程序时跟踪文件数据大于指定的最大值，则在所有 10 个文件都完成翻转之前，跟踪文件数据都将大于指定的最大值 示例： -tracefilemax 1000M -tfm 1000M 在此示例中，跟踪文件仅为 1 GB。
-unload	-u	无	卸载远程装载程序实例。如果远程装载程序运行为 Win32 服务，则此命令将停止该服务。 示例： -unload -u

选项	别名	参数	说明
-window	-w	打开 / 关闭	在远程装载程序实例中打开或关闭跟踪窗口。 示例： -window on -w off 此选项仅适用于 Windows 平台。不适用于 Java 远程装载程序。
-wizard	-wiz	无	启动 " 配置向导 "。运行不带有命令行参数的 dirxml_remote.exe 也可以启动此向导。如果还指定了配置文件，此选项会很有用。在这种情况下，向导启动时将使用配置文件中的值，并可使用向导更改配置，而无需直接编辑配置文件。 示例： -wizard -wiz 此选项仅适用于 Windows 平台。不适用于 Java 远程装载程序。

表 ***B-2*** *Java* 类名

Java 类名	驱动程序
com.novell.nds.dirxml.driver.avaya.PBXDriverShim	Avaya PBX 驱动程序
com.novell.nds.dirxml.driver.delimitedtext.DelimitedTextDriver	定界文本驱动程序
com.novell.nds.dirxml.driver.nds.DriverShimImpl	eDirectory 驱动程序
com.novell.nds.dirxml.driver.entitlement.EntitlementServiceDriver	权利服务驱动程序
com.novell.gw.dirxml.driver.gw.GWdriverShim	GroupWise 驱动程序
com.novell.nds.dirxml.jdbc.JDBCDriverShim	JDBC 驱动程序
com.novell.nds.dirxml.driver.ldap.LDAPDriverShim	LDAP 驱动程序
com.novell.nds.dirxml.driver.loopback.LoopbackDriverShim	回送驱动程序
com.novell.nds.dirxml.driver.manualtask.driver.ManualTaskDriver	手工任务驱动程序
com.novell.nds.dirxml.driver.nisdriver.NISDriverShim	NIS 驱动程序
com.novell.nds.dirxml.driver.notes.NotesDriverShim	Notes 驱动程序
com.novell.nds.dirxml.driver.psoftshim.PSOFTDriverShim	PeopleSoft 驱动程序
com.novell.nds.dirxml.driver.SAPShim.SAPDriverShim	SAP HR 驱动程序
com.novell.nds.dirxml.driver.sapusershim.SAPDriverShim	SAP 用户管理驱动程序
com.novell.nds.dirxml.driver.sifagent.SIFShim	SIF 驱动程序
com.novell.nds.dirxml.driver.soap.SOAPDriver	Soap 驱动程序

Java 类名	驱动程序
com.novell.idm.driver.ComposerDriverShim	用户应用程序
be.opns.dirxml.driver.ars.arsremedydrivershim.ARSDriverShim	修复 ARS 的驱动程序

Identity Manager 事件和报告

C

本节包含 Identity Manager 记录的所有 Novell® Audit 事件列表。还包含可以使用 Novell Audit 运行的报告示例。“报告”在第 258 页 包含此报告的示例。

每个事件中都存有以下信息："EventID" （事件 ID）、 "Description" （说明）、 "Originator Title" （初始程序标题）、 "Target Title" （目标标题）、 "Subtarget Title" （子目标标题）、 "Text1 Title" （文本 1 标题）、 "Text2 Title" （文本 2 标题）、 "Text3 Title" （文本 3 标题）、 "Value1 Title" （值 1 标题）、 "Value1 Type" （值 1 类型）、 "Value2 Title" （值 2 标题）、 "Value2 Type" （值 2 类型）、 "Value3 Title" （值 3 标题）、 "Value3 Type" （值 3 类型）、 "Group Title" （组标题）、 "Group Type" （组类型）、 "Data Title" （数据标题）、 "Data Type" （数据类型）、 "Display Schema" （显示纲要）。

表中包括以下部件的事件。

C.1 引擎事件

以下表中包含可以通过 Novell Audit 来审计的引擎事件的列表。

表 *C-1* 引擎事件字段：″初始程序标题 ″、 ″目标标题 ″和 ″子目标标题 ″

事件 ID	说明	初始程序标题	目标标题	子目标标题
30001	成功状态	通道	src-dn (dest-dn)	级别
30002	重试状态	通道	src-dn (dest-dn)	级别
30003	警告状态	通道	src-dn (dest-dn)	级别
30004	错误状态	通道	src-dn (dest-dn)	级别
30005	致命状态	通道	src-dn (dest-dn)	级别
30006	其它状态	通道	src-dn (dest-dn)	级别
30007	搜索	通道	dest-dn 或关联	范围

事件 ID	说明	初始程序标题	目标标题	子目标标题
30008	添加项	通道	dest-dn 或关联	特性名称
30009	删除项	通道	dest-dn 或关联	特性名称
3000A	修改项	通道	dest-dn 或关联	特性名称
3000B	重命名项	通道	dest-dn 或关联	对象类型
3000C	移动项	通道	dest-dn 或关联	移动目标
3000D	添加关联	通道	dest-dn	特性名称
3000E	去除关联	通道		特性名称
3000F	查询纲要	通道		
30010	检查口令	通道	驱动程序	
30011	检查对象口令	通道	dest-dn 或关联	
30012	更改口令	通道	dest-dn 或关联	
30013	同步	通道	dest-dn 或关联	特性名称
30014	输入 XML 文档	通道		特性名称
30015	输入转换文档	通道		
30016	输出转换文档	通道		
30017	事件转换文档	通道		
30018	布局规则转换文档	通道		
30019	创建规则转换文档	通道		
3001A	输入映射规则转换文档	通道		
3001B	输出映射规则转换文档	通道		
3001C	匹配规则转换文档	通道		
3001D	命令转换文档	通道		
3001E	发布者过滤器转换文档	通道		
3001F	用户代理请求	通道		
30020	重新同步驱动程序	通道	驱动程序	
30021	迁移	通道	关联	特性名称
30022	驱动程序启动	驱动程序集	驱动程序	
30023	驱动程序停止	驱动程序停止	驱动程序	
30024	口令同步	通道	对象	特性名称
30025	口令重设置	通道	dest-dn 或关联	特性名称
30026	DirXML 错误	通道	对象	
30027	DirXML 警告	通道	对象	

事件 ID	说明	初始程序标题	目标标题	子目标标题
30028	自定义操作	通道		
30029	清除特性	通道	dest-dn 或关联	特性名称
3002A	添加值 - 修改项	通道	dest-dn 或关联	特性名称
3002B	去除值	通道	dest-dn 或关联	特性名称
3002C	合并项	通道	对象	特性名称
3002D	获取命名口令	驱动程序或通道	对象	
3002E	重设置特性	通道	对象	通道
3002F	添加值 - 添加项	通道	dest-dn 或关联	特性名称

表 ***C-2*** 引擎事件字段：″文本 *1* 标题 ″、 ″文本 *2* 标题 ″和 ″文本 *3* 标题 ″

事件 ID	说明	文本 1 标题	文本 2 标题	文本 3 标题
30001	成功状态	类型	文档状态	事件 ID
30002	重试状态	类型	文档状态	事件 ID
30003	警告状态	类型	文档状态	事件 ID
30004	错误状态	类型	文档状态	事件 ID
30005	致命状态	类型	文档状态	事件 ID
30006	其它状态	类型	文档状态	事件 ID
30007	搜索	对象类型		事件 ID
30008	添加项	对象类型	src-dn	事件 ID
30009	删除项	对象类型	src-dn	事件 ID
3000A	修改项	对象类型	src-dn	事件 ID
3000B	重命名项	新名称	src-dn	事件 ID
3000C	移动项	移动关联	src-dn	事件 ID
3000D	添加关联	关联		事件 ID
3000E	去除关联	关联		事件 ID
3000F	查询纲要			事件 ID
30010	检查口令			
30011	检查对象口令			事件 ID
30012	更改口令	对象类型	src-dn	事件 ID
30013	同步	对象类型	关联	类型
30014	输入 XML 文档			警告讯息
30015	输入转换文档			警告讯息

事件 ID	说明	文本 1 标题	文本 2 标题	文本 3 标题
30016	输出转换文档			警告讯息
30017	事件转换文档			警告讯息
30018	布局规则转换文档			警告讯息
30019	创建规则转换文档			警告讯息
3001A	输入映射规则转换文档			警告讯息
3001B	输出映射规则转换文档			警告讯息
3001C	匹配规则转换文档			警告讯息
3001D	命令转换文档			警告讯息
3001E	发布者过滤器转换文档			警告讯息
3001F	用户代理请求			
30020	重新同步驱动程序			错误讯息
30021	迁移	对象类型		警告讯息
30022	驱动程序启动			驱动程序讯息
30023	驱动程序停止			驱动程序讯息
30024	口令同步			
30025	口令重设置		src-dn	
30026	DirXML 错误	错误讯息		
30027	DirXML 警告	警告讯息		
30028	自定义操作			
30029	清除特性		src-dn	事件 ID
3002A	添加值 - 修改项	值	src-dn	事件 ID
3002B	去除值	值	src-dn	事件 ID
3002C	合并项	对象类型	通道	关联
3002D	获取命名口令	口令名称		事件 ID
3002E	重设置特性			
3002F	添加值 - 添加项	值	src-dn	事件 ID

表 ***C-3*** 引擎事件字段：″值 *1* 标题 ″、″值 *2* 标题 ″和 ″值 *3* 标题 ″

事件 ID	说明	值 1 标题	值 2 标题	值 3 标题
30001	成功状态			
30002	重试状态			
30003	警告状态			

事件 ID	说明	值 1 标题	值 2 标题	值 3 标题
30004	错误状态			
30005	致命状态			
30006	其它状态			
30007	搜索			结果
30008	添加项			结果
30009	删除项			结果
3000A	修改项			结果
3000B	重命名项			结果
3000C	移动项			结果
3000D	添加关联			结果
3000E	去除关联			结果
3000F	查询纲要			结果
30010	检查口令			
30011	检查对象口令			
30012	更改口令			结果
30013	同步			结果
30014	输入 XML 文档			
30015	输入转换文档			
30016	输出转换文档			
30017	事件转换文档			
30018	布局规则转换文档			
30019	创建规则转换文档			
3001A	输入映射规则转换文档			
3001B	输出映射规则转换文档			
3001C	匹配规则转换文档			
3001D	命令转换文档			
3001E	发布者过滤器转换文档			
3001F	用户代理请求			结果
30020	重新同步驱动程序			结果
30021	迁移			
30022	驱动程序启动	状态		
30023	驱动程序停止	状态		

事件 ID	说明	值 1 标题	值 2 标题	值 3 标题
30024	口令同步			结果
30025	口令重设置			
30026	DirXML 错误	代码		
30027	DirXML 警告	代码		
30028	自定义操作			
30029	清除特性			结果
3002A	添加值 - 修改项			结果
3002B	去除值			结果
3002C	合并项			
3002D	获取命名口令			结果
3002E	重设置特性			
3002F	添加值 - 添加项			结果

表 ***C-4*** 引擎事件字段：″数据类型″和″触发器″

事件 ID	说明	数据类型	触发器
30001	成功状态	XML 文档	许多不同事件可以导致成功状态事件的发生。它通常表示操作已成功完成。
30002	重试状态	XML 文档	许多不同事件可以导致重试状态事件的发生。它表示操作尚未完成，必须稍后再次尝试。
30003	警告状态	XML 文档	许多不同事件可以导致警告状态事件的发生。它通常表示操作已完成，但存在小问题。
30004	错误状态	XML 文档	许多不同事件可以导致错误状态事件的发生。它通常表示操作未成功完成。
30005	致命状态	XML 文档	许多不同事件可以导致致命状态事件的发生。它通常表示操作未成功完成，而且引擎或驱动程序无法继续。
30006	其它状态	XML 文档	文档的处理状态级别与之前定义的五个级别不同时，都将创建其它状态事件。这些事件只能在样式表或规则中生成。
30007	搜索	XML 文档	在将查询文档发送至 IDM 引擎或驱动程序时发生。
30008	添加项	XML 文档	添加对象时发生。

事件 ID	说明	数据类型	触发器
30009	删除项	XML 文档	删除对象时发生。
3000A	修改项	XML 文档	修改对象时发生。
3000B	重命名项	XML 文档	重命名对象时发生。
3000C	移动项	XML 文档	移动对象时发生。
3000D	添加关联	XML 文档	添加关联时发生。可以在添加或匹配操作时发生。
3000E	去除关联	XML 文档	删除对象后，就不会出现去除关联事件。在完全不同的应用程序中删除用户对象后，如果该删除操作随后转换为去除关联的修改操作，则将发生去除关联操作。
3000F	查询纲要	XML 文档	查询纲要操作发送至 IDM 引擎或驱动程序时发生。
30010	检查口令		通过 iManager 初始化的手工功能。
30011	检查对象口令	XML 文档	在发出检查对象 （驱动程序除外）口令的请求时发生。
30012	更改口令	XML 文档	发出检查驱动程序口令的请求时发生。
30013	同步	XML 文档	请求同步事件时发生。
30014	输入 XML 文档	XML 文档	由引擎或驱动程序创建输入文档时生成。
30015	输入转换文档	XML 文档	在处理输入转换策略之后生成，允许用户查看转换的文档。
30016	输出转换文档	XML 文档	在处理输出转换策略之后生成，允许用户查看转换的文档。
30017	事件转换文档	XML 文档	在处理事件转换策略之后生成，允许用户查看转换的文档。
30018	布局规则转换文档	XML 文档	在处理布局规则策略之后生成，允许用户查看转换的文档。
30019	创建规则转换文档	XML 文档	在处理创建规则策略之后生成，允许用户查看转换的文档。
3001A	输入映射规则转换文档	XML 文档	在处理纲要映射规则之后生成，该规则将文档转换为 eDirectory 纲要
3001B	输出映射规则转换文档	XML 文档	在处理纲要映射规则之后生成，该规则将文档转换为应用程序纲要。
3001C	匹配规则转换文档	XML 文档	在处理匹配规则策略之后生成，允许用户查看转换的文档。

事件 ID	说明	数据类型	触发器
3001D	命令转换文档	XML 文档	在处理命令转换策略之后生成，允许用户查看转换的文档。
3001E	发布者过滤器转换文档	XML 文档	在处理发布者通道上的通知过滤器之后生成，允许用户查看转换的文档。
3001F	用户代理请求	XML 文档	将用户代理 XDS 命令文档发送至订购者通道上的驱动程序时发生。
30020	重新同步驱动程序		发出重新同步请求时发生。
30021	迁移		发出迁移请求时发生。
30022	驱动程序启动	XML 文档	启动驱动程序时发生。
30023	驱动程序停止	XML 文档	停止驱动程序时发生。
30024	口令同步		在对象上设置分发口令或简单口令时生成。
30025	口令重设置		在口令同步操作失败后重设置已连接应用程序的口令时生成。
30026	DirXML 错误		引擎发生内部错误时生成。
30027	DirXML 警告		引擎发生内部警告时生成。
30028	自定义操作	XML 文档	输入文档中出现未知操作时发生。添加、删除或修改都是已知操作的示例。
30029	清除特性		修改操作包含 remove-all-value 要素时发生。
3002A	添加值 - 修改项	值	修改对象过程中添加值时发生。
3002B	去除值	值	修改操作包含 remove-value 要素时发生。
3002C	合并项	XML 文档	合并两个对象时发生。
3002D	获取命名口令	XML 文档	执行获取命名口令操作时生成。
3002E	重设置特性	XML 文档	在发布者或订购者通道上发布重设置文档时发生。
3002F	添加值 - 添加项	值	创建对象过程中添加值时发生。

C.2 服务器事件

以下表中包含可以通过 Novell Audit 来审计的服务器事件的列表。

表 *C-5* 服务器事件字段：″初始程序标题 ″、 ″目标标题 ″和 ″子目标标题 ″

事件 ID	说明	初始程序标题	目标标题	子目标标题
307D0	Config:Log Events	服务器	驱动程序	特性名称

事件 ID	说明	初始程序标题	目标标题	子目标标题
307D1	Config:Driver Cache Limit	服务器	驱动程序	特性名称
307D2	Config:Driver Set	服务器	服务器	特性名称
307D3	Config:Driver Start Option	服务器	驱动程序	特性名称
307D4	驱动程序重新同步	服务器	驱动程序	
307D5	迁移应用程序服务器	服务器	驱动程序	
307D6	Shim 口令集	服务器	驱动程序	特性名称
307D7	加密口令集	服务器	驱动程序	
307D8	远程装载程序口令集	服务器	驱动程序	特性名称

表 ***C-6*** 服务器事件字段：″文本 *1* 标题 ″、 ″文本 *2* 标题 ″和 ″文本 *3* 标题 ″

事件 ID	说明	文本 1 标题	文本 2 标题	文本 3 标题
307D0	Config:Log Events			操作
307D1	Config:Driver Cache Limit			
307D2	Config:Driver Set	驱动程序集	类型	
307D3	Config:Driver Start Option			讯息
307D4	驱动程序重新同步			
307D5	迁移应用程序服务器			
307D6	Shim 口令集			
307D7	加密口令集		类型	
307D8	远程装载程序口令集			

表 ***C-7*** 服务器事件字段：″值 *1* 标题 ″、 ″值 *2* 标题 ″和 ″值 *3* 标题 ″

事件 ID	说明	值 1 标题	值 2 标题	值 3 标题
307D0	Config:Log Events			结果
307D1	Config:Driver Cache Limit	限制		结果
307D2	Config:Driver Set			结果

事件 ID	说明	值 1 标题	值 2 标题	值 3 标题
307D3	Config:Driver Start Option	启动选项		结果
307D4	驱动程序重新同步			结果
307D5	迁移应用程序服务器			结果
307D6	Shim 口令集		版本	结果
307D7	加密口令集			结果
307D8	远程装载程序口令集		版本	结果

表 ***C-8*** 服务器事件字段：″数据类型 ″和 ″触发器 ″

事件 ID	说明	数据类型	触发器
307D0	Config:Log Events	输入缓冲区	更改驱动程序对象或驱动程序集对象的日志事件特性时发生。
307D1	Config:Driver Cache Limit		驱动程序对象上的驱动程序超速缓存限制特性更改时发生。
307D2	Config:Driver Set	输入缓冲区	更改驱动程序集 / 服务器关联时发生。
307D3	Config:Driver Start Option	输入缓冲区	更改驱动程序对象的驱动程序启动选项时发生。
307D4	驱动程序重新同步		为驱动程序发布重新同步时发生。
307D5	迁移应用程序服务器	XML 文档	迁移应用程序服务器时发生。
307D6	Shim 口令集		设置应用程序口令时发生。
307D7	加密口令集		
307D8	远程装载程序口令集		设置远程装载程序口令时发生。

C.3 远程装载程序事件

以下表中包含可通过 Novell Audit 来审计的远程装载程序事件的列表。

表 ***C-9*** 远程装载程序事件字段：″初始程序标题 ″、 ″目标标题 ″和 ″子目标标题 ″

事件 ID	说明	初始程序标题	触发器
30BB8	远程装载程序启动	实例	远程装载程序启动时发生。
30BB9	远程装载程序停止	实例	远程装载程序停止时发生。
30BBA	已建立远程装载程序连接	实例	建立远程装载程序连接时发生。

事件 ID	说明	初始程序标题	触发器
30BBB	远程装载程序已落线	实例	远程装载程序落线时发生。

C.4 细节入口小程序

表 ***C-10*** 细节入口小程序字段：″初始程序标题 ″、 ″目标标题 ″和 ″子目标标题 ″

事件 ID	说明	初始程序标题	目标标题	子目标标题
31400	Delete_Entity	用户名	实体 DN	实体定义
31401	Update_Entity	用户名	实体 DN	实体定义

表 ***C-11*** 细节入口小程序字段：″组标题 ″、 ″组类型 ″和 ″触发器 ″

事件 ID	说明	组标题	组类型	触发器
31400	Delete_Entity	组号码	号码	删除对象时发生。
31401	Update_Entity	组号码	号码	修改对象时发生。

C.5 更改口令入口小程序

表 ***C-12*** 更改口令入口小程序字段：″初始程序标题 ″、 ″目标标题 ″和 ″文本 *3* 标题 ″

事件 ID	说明	初始程序标题	目标标题	文本 3 标题
31420	Change_Password_Failure	启动器 ID	目标 DN	错误讯息
31421	Change_Password_Success	启动器 ID	目标 DN	

表 ***C-13*** 更改口令入口小程序字段：″值 *3* 标题 ″、 ″值 *3* 类型 ″和 ″触发器 ″

事件 ID	说明	值 3 标题	值 3 类型	触发器
31420	Change_Password_Failure	错误号	布尔值	更改口令失败时发生。
31421	Change_Password_Success			更改口令成功时发生。

C.6 忘记口令更改口令入口小程序

表 ***C-14*** 忘记口令更改口令入口小程序字段：″初始程序标题 ″、 ″目标标题 ″和 ″文本 *3* 标题 ″

事件 ID	说明	初始程序标题	目标标题	文本 3 标题
31420	Forgot_Password_Change_Failure	启动器 ID	目标 DN	错误讯息

事件 ID	说明	初始程序标题	目标标题	文本 3 标题
31421	Forgot_Password_Change_Success	启动器 ID	目标 DN	

表 ***C-15*** 忘记口令更改口令入口小程序字段：″值 *3* 标题 ″、 ″值 *3* 类型 ″和 ″组标题 ″

事件 ID	说明	值 3 标题	值 3 类型	组标题
31420	Forgot_Password_Change_Failure	错误号	布尔值	组号码
31421	Forgot_Password_Change_Success			组号码

表 ***C-16*** 忘记口令更改口令入口小程序字段：″组类型 ″和 ″触发器 ″

事件 ID	说明	组类型	触发器
31420	Forgot_Password_Change_Failure	号码	忘记口令更改失败时发生。
31421	Forgot_Password_Change_Success	号码	忘记口令更改成功时发生。

C.7 搜索列表入口小程序

表 ***C-17*** 搜索列表入口小程序字段：″初始程序标题 ″、 ″目标标题 ″和 ″组标题 ″

事件 ID	说明	初始程序标题	目标标题	组标题
31430	Search_Request	用户 ID	搜索关键字	用户 ID
31431	Search_Saved	用户 ID	搜索关键字	用户 ID

表 ***C-18*** 搜索列表入口小程序字段：″组类型 ″、 ″数据标题 ″和 ″数据类型 ″

事件 ID	说明	组类型	数据标题	数据类型
31430	Search_Request	号码	搜索 XML	字符串
31431	Search_Saved	号码	搜索 XML	字符串

表 ***C-19*** 搜索列表入口小程序字段：″触发器 ″

事件 ID	说明	触发器
31430	Search_Request	用户执行搜索请求时发生。
31431	Search_Saved	用户选择 " 我保存的搜索 " 时发生。

C.8 创建入口小程序

表 *C-20* 创建入口小程序字段：″初始程序标题 ″、 ″目标标题 ″和 ″子目标标题 ″

事件 ID	说明	初始程序标题	目标标题	子目标标题
31440	Create_Entity	用户名	实体 DN	实体定义

表 *C-21* 创建入口小程序字段：″触发器 ″

事件 ID	说明	触发器
31440	Create_Entity	创建对象时发生。

C.9 安全环境

以下表中包含可通过 Novell Audit 来审计的安全性事件的列表。

表 *C-22* 安全环境字段：″初始程序标题 ″、 ″目标标题 ″和 ″文本 *1* 标题 ″

事件 ID	说明	初始程序标题	目标标题	文本 1 标题
31540	Create_Proxy_Definition_Success	启动器 ID	定义	细节
31541	Create_Proxy_Definition_Failure	启动器 ID	定义	细节
31542	Update_Proxy_Definition_Success	启动器 ID	定义	细节
31543	Update_Proxy_Definition_Failure	启动器 ID	定义	细节
31544	Delete_Proxy_Definition_Success	启动器 ID	定义	细节
31545	Delete_Proxy_Definition_Failure	启动器 ID	定义	细节
31546	Create_Delegatee_Definition_Success	启动器 ID	定义	细节
31547	Create_Delegatee_Definition_Failure	启动器 ID	定义	细节
31548	Update_Delegatee_Definition_Success	启动器 ID	定义	细节
31549	Update_Delegatee_Definition_Failure	启动器 ID	定义	细节
3154A	Delete_Delegatee_Definition_Success	启动器 ID	定义	细节
3154B	Delete_Delegatee_Definition_Failure	启动器 ID	定义	细节
3154C	Create_Availability_Success	启动器 ID	目标	
3154D	Create_Availability_Failure	启动器 ID	目标	细节
3154E	Delete_Availability_Success	启动器 ID	目标	细节
3154F	Delete_Availability_Failure	启动器 ID	目标	细节

表 ***C-23*** 安全环境字段：″文本 *3* 标题 ″、 ″数据标题 ″和 ″数据类型 ″

事件 ID	说明	文本 3 标题	数据标题	数据类型
31540	Create_Proxy_Definition_Success			
31541	Create_Proxy_Definition_Failure	错误讯息	堆栈跟踪	字符串
31542	Update_Proxy_Definition_Success			
31543	Update_Proxy_Definition_Failure	错误讯息	堆栈跟踪	字符串
31544	Delete_Proxy_Definition_Success			
31545	Delete_Proxy_Definition_Failure	错误讯息	堆栈跟踪	字符串
31546	Create_Delegatee_Definition_Success			
31547	Create_Delegatee_Definition_Failure	错误讯息	堆栈跟踪	字符串
31548	Update_Delegatee_Definition_Success			
31549	Update_Delegatee_Definition_Failure	错误讯息	堆栈跟踪	字符串
3154A	Delete_Delegatee_Definition_Success			
3154B	Delete_Delegatee_Definition_Failure	错误讯息	堆栈跟踪	字符串
3154C	Create_Availability_Success			
3154D	Create_Availability_Failure	错误讯息	堆栈跟踪	字符串
3154E	Delete_Availability_Success			
3154F	Delete_Availability_Failure	错误讯息	堆栈跟踪	字符串

表 ***C-24*** 安全环境字段：触发器

事件 ID	说明	触发器
31540	Create_Proxy_Definition_Success	创建代理定义成功时发生。
31541	Create_Proxy_Definition_Failure	创建代理定义失败时发生。
31542	Update_Proxy_Definition_Success	更新代理定义成功时发生。
31543	Update_Proxy_Definition_Failure	更新代理定义失败时发生。
31544	Delete_Proxy_Definition_Success	删除代理定义成功时发生。
31545	Delete_Proxy_Definition_Failure	删除代理定义失败时发生。
31546	Create_Delegatee_Definition_Success	创建受委托者定义成功时发生。
31547	Create_Delegatee_Definition_Failure	创建受委托者定义失败时发生。
31548	Update_Delegatee_Definition_Success	更新受委托者定义成功时发生。
31549	Update_Delegatee_Definition_Failure	更新受委托者定义失败时发生。
3154A	Delete_Delegatee_Definition_Success	删除受委托者定义成功时发生。
3154B	Delete_Delegatee_Definition_Failure	删除受委托者定义失败时发生。

事件 ID	说明	触发器
3154C	Create_Availability_Success	创建可用性状态成功时发生。
3154D	Create_Availability_Failure	创建可用性状态失败时发生。
3154E	Delete_Availability_Success	删除可用性状态成功时发生。
3154F	Delete_Availability_Failure	删除可用性状态失败时发生。

C.10 工作流程

以下表中包含可通过 Novell Audit 来审计的用户应用程序事件的列表。

表 *C-25* 工作流程字段：″初始程序标题 ″、 ″目标标题 ″和 ″子目标标题 ″

事件 ID	说明	初始程序标题	目标标题	子目标标题
31520	Workflow_Error	启动器 ID		
31521	Workflow_Started	启动器 ID		
31522	Workflow_Forwarded	启动器 ID	收件人	进程名称
31523	Workflow_Reassigned	启动器 ID	收件人	进程名称
31524	Workflow_Approved	启动器 ID	收件人	进程名称
31525	Workflow_Refused	启动器 ID	收件人	进程名称
31526	Workflow_Ended	启动器 ID	收件人	进程名称
31527	Workflow_Claimed	启动器 ID	收件人	进程名称
31528	Workflow_Unclaimed	启动器 ID	收件人	进程名称
31529	Workflow_Denied	启动器 ID	收件人	进程名称
3152A	Workflow_Completed	启动器 ID	收件人	进程名称
3152B	Workflow_Timedout	启动器 ID	收件人	进程名称
3152C	User_Message	启动器 ID	作者	
3152D	Provision_Error	启动器 ID	收件人	进程名称
3152E	Provision_Submitted	启动器 ID	收件人	进程名称
3152F	Provision_Success	启动器 ID	收件人	进程名称
31530	Provision_Failure	启动器 ID	收件人	进程名称
31531	Provision_Granted	启动器 ID	收件人	进程名称
31532	Provision_Revoked	启动器 ID	收件人	进程名称
31533	Workflow_Retracted	启动器 ID	收件人	进程名称

表 ***C-26*** 工作流程字段：″文本 *1* 标题 ″、 ″文本 *2* 标题 ″和 ″文本 *3* 标题 ″

事件 ID	说明	文本 1 标题	文本 2 标题	文本 3 标题
31520	Workflow_Error	活动	进程 ID	错误讯息
31521	Workflow_Started	活动	进程 ID	
31522	Workflow_Forwarded	活动	进程 ID	
31523	Workflow_Reassigned	活动	进程 ID	
31524	Workflow_Approved	活动	进程 ID	二级用户
31525	Workflow_Refused	活动	进程 ID	二级用户
31526	Workflow_Ended	活动	进程 ID	
31527	Workflow_Claimed	活动	进程 ID	二级用户
31528	Workflow_Unclaimed	活动	进程 ID	二级用户
31529	Workflow_Denied	活动	进程 ID	二级用户
3152A	Workflow_Completed	活动	进程 ID	
3152B	Workflow_Timedout	活动	进程 ID	
3152C	User_Message		讯息	
3152D	Provision_Error	活动	进程 ID	错误讯息
3152E	Provision_Submitted	活动	进程 ID	
3152F	Provision_Success	活动	进程 ID	
31530	Provision_Failure	活动	进程 ID	
31531	Provision_Granted	活动	进程 ID	
31532	Provision_Revoked	活动	进程 ID	
31533	Workflow_Retracted	活动	进程 ID	二级用户

表 ***C-27*** 工作流程字段：″值 *3* 标题 ″、 ″值 *3* 类型 ″和 ″数据标题 ″

事件 ID	说明	值 3 标题	值 3 类型	数据标题
31520	Workflow_Error	错误号	布尔值	堆栈跟踪
31521	Workflow_Started			
31522	Workflow_Forwarded			
31523	Workflow_Reassigned			
31524	Workflow_Approved			二级用户类型
31525	Workflow_Refused			二级用户类型
31526	Workflow_Ended			
31527	Workflow_Claimed			二级用户类型

事件 ID	说明	值 3 标题	值 3 类型	数据标题
31528	Workflow_Unclaimed			二级用户类型
31529	Workflow_Denied			二级用户类型
3152A	Workflow_Completed			
3152B	Workflow_Timedout			
3152C	User_Message			
3152D	Provision_Error	错误号	布尔值	堆栈跟踪
3152E	Provision_Submitted			
3152F	Provision_Success			
31530	Provision_Failure			
31531	Provision_Granted			
31532	Provision_Revoked			
31533	Workflow_Retracted			二级用户类型

表 ***C-28*** 工作流程字段：″数据类型″和″触发器″

事件 ID	说明	数据类型	触发器
31520	Workflow_Error	字符串	该事件可由很多项引发。
31521	Workflow_Started		启动工作流程时发生。
31522	Workflow_Forwarded		转发工作流程时发生。
31523	Workflow_Reassigned		重指派工作流程时发生。
31524	Workflow_Approved	字符串	批准工作流程后发生。
31525	Workflow_Refused	字符串	拒收工作流程时发生。
31526	Workflow_Ended		工作流程结束时发生。
31527	Workflow_Claimed	字符串	声明工作流程时发生。
31528	Workflow_Unclaimed	字符串	
31529	Workflow_Denied	字符串	拒绝工作流程时发生。
3152A	Workflow_Completed		完成工作流程时发生。
3152B	Workflow_Timedout		工作流程超时时发生。
3152C	User_Message		
3152D	Provision_Error	字符串	该事件可由很多项引发。
3152E	Provision_Submitted		
3152F	Provision_Success		
31530	Provision_Failure		

事件 ID	说明	数据类型	触发器
31531	Provision_Granted		
31532	Provision_Revoked		
31533	Workflow_Retracted	字符串	收回工作流程时发生。

C.11 报告

下面是 Novell Audit 报告样式的示例。可运行报告的列表如下。

- 管理操作报告
- 历史批准流程报告
- 资源供应报告
- 特定用户审计追踪
- 特定用户供应
- 用户供应

图 *C-1* 管理操作报告

Novell® Audit Report for Identity Manager

Administrative Action Report

Report Last Modified: 10/13/2005
Report Generated On: 10/13/2005
Total pages: 5

Total # Events: 121

Report Period: - 10/13/2005 8:43:50AM

Date / Time	Administrator	Subject	Action
8/18/2005 5:45:17PM	cn=admin,ou=idmsample-cts10,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample-cts10,o=novell	Entity Deleted
8/18/2005 7:07:40PM	cn=admin,ou=idmsample-cts10,o=novell	cn=testCreateUser11,ou=users,ou=idmsample-cts10,o=novell	Entity Deleted
8/18/2005 7:09:05PM	cn=admin,ou=idmsample-cts10,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample-cts10,o=novell	Entity Deleted
8/18/2005 7:12:50PM	cn=admin,ou=idmsample-cts10,o=novell	cn=testCreateUser11,ou=users,ou=idmsample-cts10,o=novell	Entity Deleted
8/18/2005 7:13:39PM	cn=admin,ou=idmsample-cts10,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample-cts10,o=novell	Entity Deleted
8/23/2005 4:56:39PM	cn=admin,ou=idmsample,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample,o=novell	Entity Deleted
8/31/2005 12:01:55PM	cn=admin,ou=idmsample,o=novell	cn=testCreateUser,ou=users,ou=idmsample,o=novell	Entity Created
8/31/2005 12:02:18PM	cn=admin,ou=idmsample,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample,o=novell	Entity Created
8/31/2005 12:19:07PM	cn=admin,ou=idmsample,o=novell	cn=testCreateUser,ou=users,ou=idmsample,o=novell	Entity Created
8/31/2005 12:19:31PM	cn=admin,ou=idmsample,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample,o=novell	Entity Created
8/31/2005 12:27:58PM	cn=admin,ou=idmsample,o=novell	cn=testCreateUser,ou=users,ou=idmsample,o=novell	Entity Created
8/31/2005 12:28:22PM	cn=admin,ou=idmsample,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample,o=novell	Entity Created
8/31/2005 2:59:39PM	cn=admin,ou=idmsample,o=novell	cn=testCreateUser,ou=users,ou=idmsample,o=novell	Entity Created
8/31/2005 3:24:30PM	cn=admin,ou=idmsample,o=novell	cn=testCreateUser,ou=users,ou=idmsample,o=novell	Entity Created
8/31/2005 8:11:59PM	cn=admin,ou=idmsample-Jeff,o=novell	cn=testCreateUser,ou=users,ou=idmsample-Jeff,o=novell	Entity Deleted
8/31/2005 8:12:23PM	cn=admin,ou=idmsample-Jeff,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample-Jeff,o=novell	Entity Deleted
8/31/2005 8:12:55PM	cn=admin,ou=idmsample-Jeff,o=novell	cn=admin,ou=idmsample-Jeff,o=novell	Entity Updated
8/31/2005 8:13:03PM	cn=admin,ou=idmsample-Jeff,o=novell	cn=admin,ou=idmsample-Jeff,o=novell	Entity Updated
9/1/2005 10:29:53AM	cn=admin,ou=idmsample-Jeff,o=novell	cn=aa,ou=users,ou=idmsample-Jeff,o=novell	Entity Deleted
9/1/2005 11:31:45AM	cn=admin,ou=idmsample,o=novell	cn=asoprano,ou=users,ou=idmsample,o=novell	Entity Created

Page 1 of 5 *Administrative Action Report*

图 ***C-2*** 历史批准流程报告

Novell® Audit Report for Identity Manager

Historical Approval Flow Report

Report Last Modified: 10/13/2005
Report Generated On: 10/13/2005
Total pages: 17

Total # Events: 351

Report Period: - 10/13/2005 8:46:17AM

WorkFlow Event: fecedbe80a3d4abd83c9476a1b576ea2

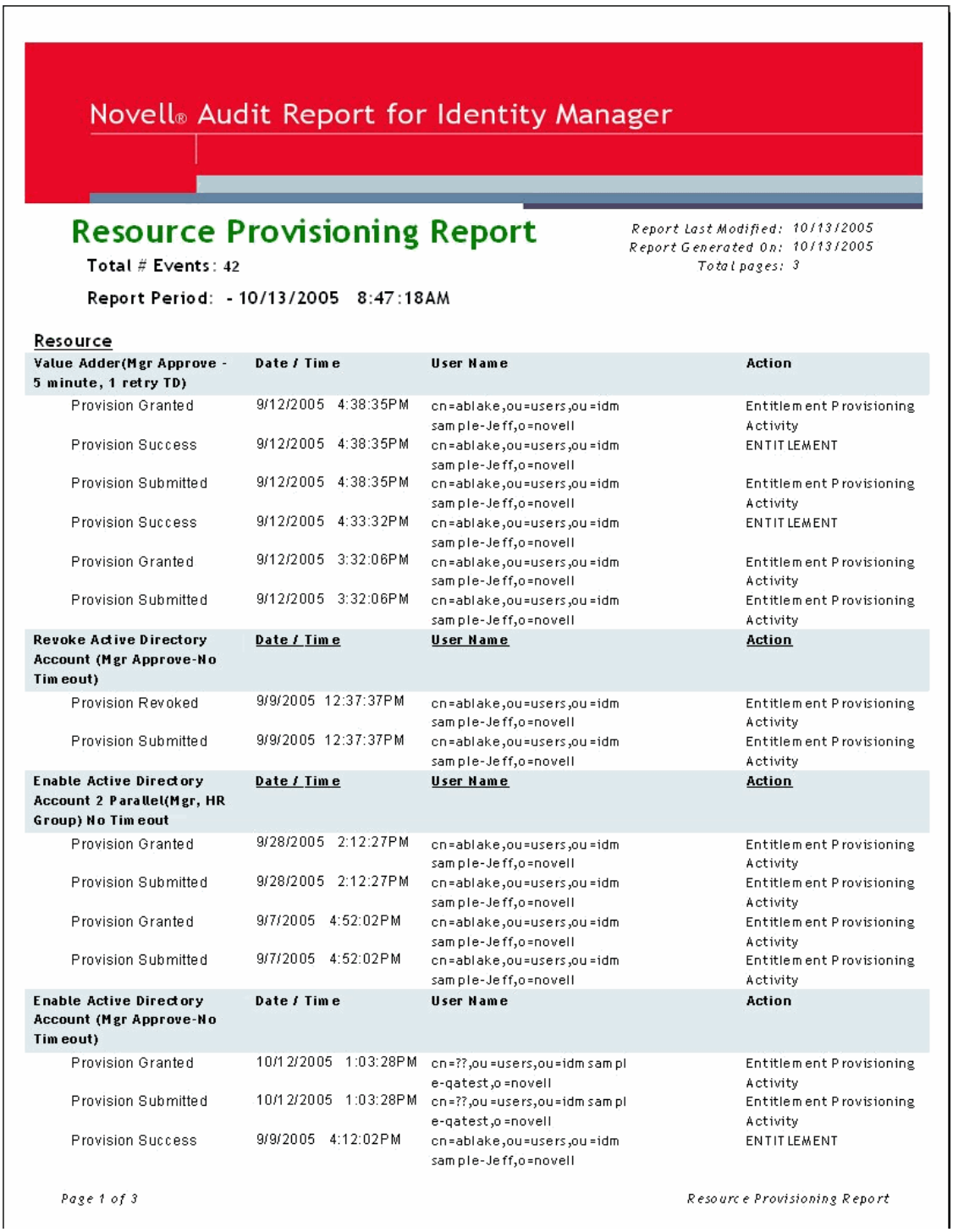
Date / Time	Action	Initiator ID	Recipient
9/12/2005 3:20:42PM	Workflow Started	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/12/2005 3:20:43PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/12/2005 3:25:43PM	Workflow Reassigned	Unclaimed	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/12/2005 3:30:44PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/12/2005 3:30:44PM	Workflow Ended	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/12/2005 3:30:44PM	Workflow Denied	System	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell

WorkFlow Event: fc6d74b1268243b3beac52261439dea0

Date / Time	Action	Initiator ID	Recipient
9/28/2005 1:12:19PM	Workflow Started	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 1:12:22PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:23PM	Workflow Approved	System	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:23PM	Workflow Approved	System	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:23PM	Workflow Completed	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:27PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:27PM	Workflow Ended	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:27PM	Provision Submitted	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:27PM	Provision Granted	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell

Page 1 of 17 *Historical Approval Flow Report*

图 ***C-3*** 资源供应报告



Novell® Audit Report for Identity Manager

Resource Provisioning Report

Report Last Modified: 10/13/2005
Report Generated On: 10/13/2005
Total pages: 3

Total # Events: 42

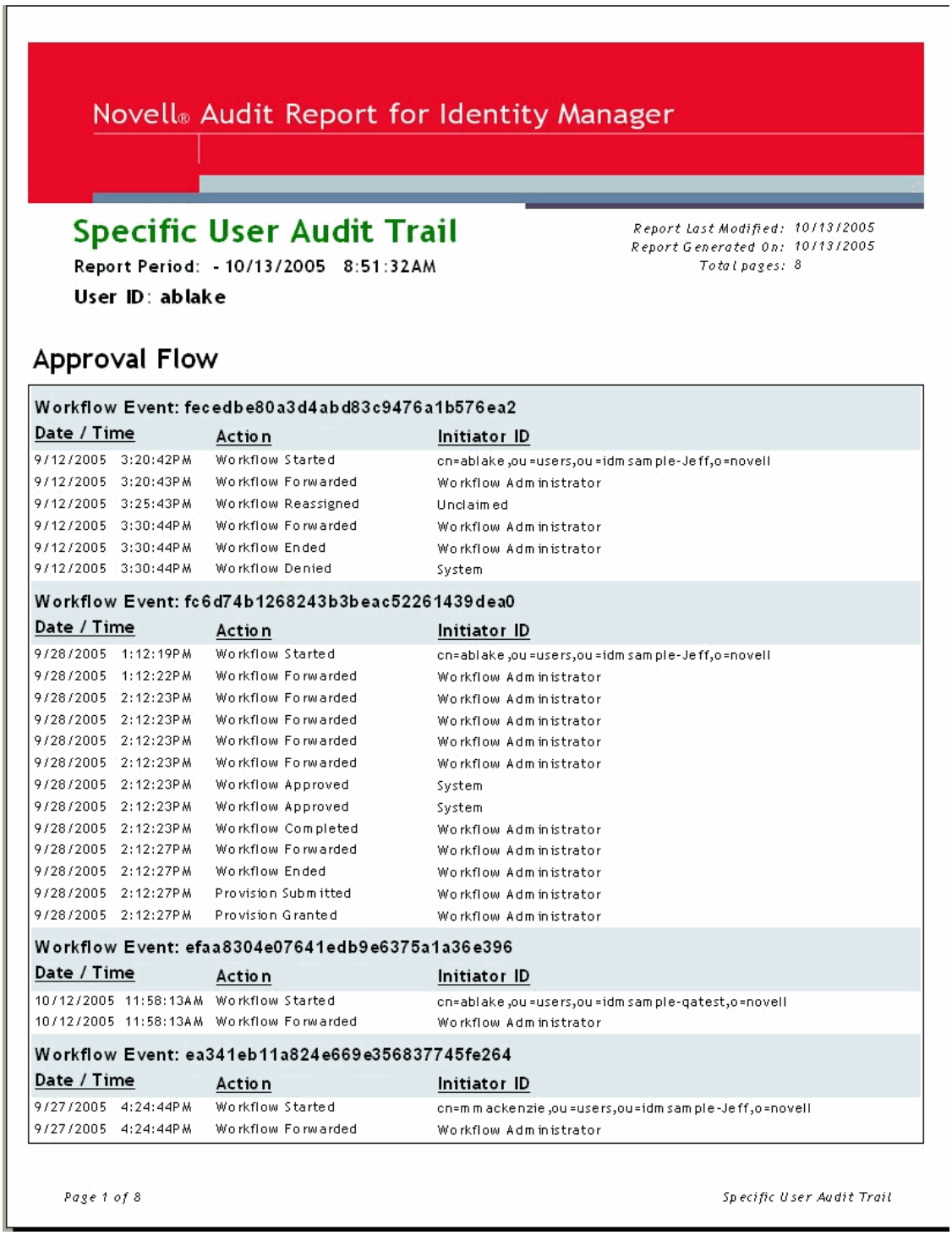
Report Period: - 10/13/2005 8:47:18AM

Resource

Value Adder(Mgr Approve - 5 minute, 1 retry TD)	**Date / Time**	**User Name**	**Action**
Provision Granted	9/12/2005 4:38:35PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Success	9/12/2005 4:38:35PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	ENTITLEMENT
Provision Submitted	9/12/2005 4:38:35PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Success	9/12/2005 4:33:32PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	ENTITLEMENT
Provision Granted	9/12/2005 3:32:06PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Submitted	9/12/2005 3:32:06PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Revoke Active Directory Account (Mgr Approve-No Timeout)	**Date / Time**	**User Name**	**Action**
Provision Revoked	9/9/2005 12:37:37PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Submitted	9/9/2005 12:37:37PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Enable Active Directory Account 2 Parallel(Mgr, HR Group) No Timeout	**Date / Time**	**User Name**	**Action**
Provision Granted	9/28/2005 2:12:27PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Submitted	9/28/2005 2:12:27PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Granted	9/7/2005 4:52:02PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Submitted	9/7/2005 4:52:02PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Enable Active Directory Account (Mgr Approve-No Timeout)	**Date / Time**	**User Name**	**Action**
Provision Granted	10/12/2005 1:03:28PM	cn=??,ou=users,ou=idm sample-qatest,o=novell	Entitlement Provisioning Activity
Provision Submitted	10/12/2005 1:03:28PM	cn=??,ou=users,ou=idm sample-qatest,o=novell	Entitlement Provisioning Activity
Provision Success	9/9/2005 4:12:02PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	ENTITLEMENT

Page 1 of 3 *Resource Provisioning Report*

图 ***C-4*** 特定用户审计追踪 *1*



Novell® Audit Report for Identity Manager

Specific User Audit Trail

Report Period: - 10/13/2005 8:51:32AM

User ID: ablake

Report Last Modified: 10/13/2005
Report Generated On: 10/13/2005
Total pages: 8

Approval Flow

Workflow Event: fecedbe80a3d4abd83c9476a1b576ea2

Date / Time	Action	Initiator ID
9/12/2005 3:20:42PM	Workflow Started	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/12/2005 3:20:43PM	Workflow Forwarded	Workflow Administrator
9/12/2005 3:25:43PM	Workflow Reassigned	Unclaimed
9/12/2005 3:30:44PM	Workflow Forwarded	Workflow Administrator
9/12/2005 3:30:44PM	Workflow Ended	Workflow Administrator
9/12/2005 3:30:44PM	Workflow Denied	System

Workflow Event: fc6d74b1268243b3beac52261439dea0

Date / Time	Action	Initiator ID
9/28/2005 1:12:19PM	Workflow Started	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 1:12:22PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Approved	System
9/28/2005 2:12:23PM	Workflow Approved	System
9/28/2005 2:12:23PM	Workflow Completed	Workflow Administrator
9/28/2005 2:12:27PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:27PM	Workflow Ended	Workflow Administrator
9/28/2005 2:12:27PM	Provision Submitted	Workflow Administrator
9/28/2005 2:12:27PM	Provision Granted	Workflow Administrator

Workflow Event: efaa8304e07641edb9e6375a1a36e396

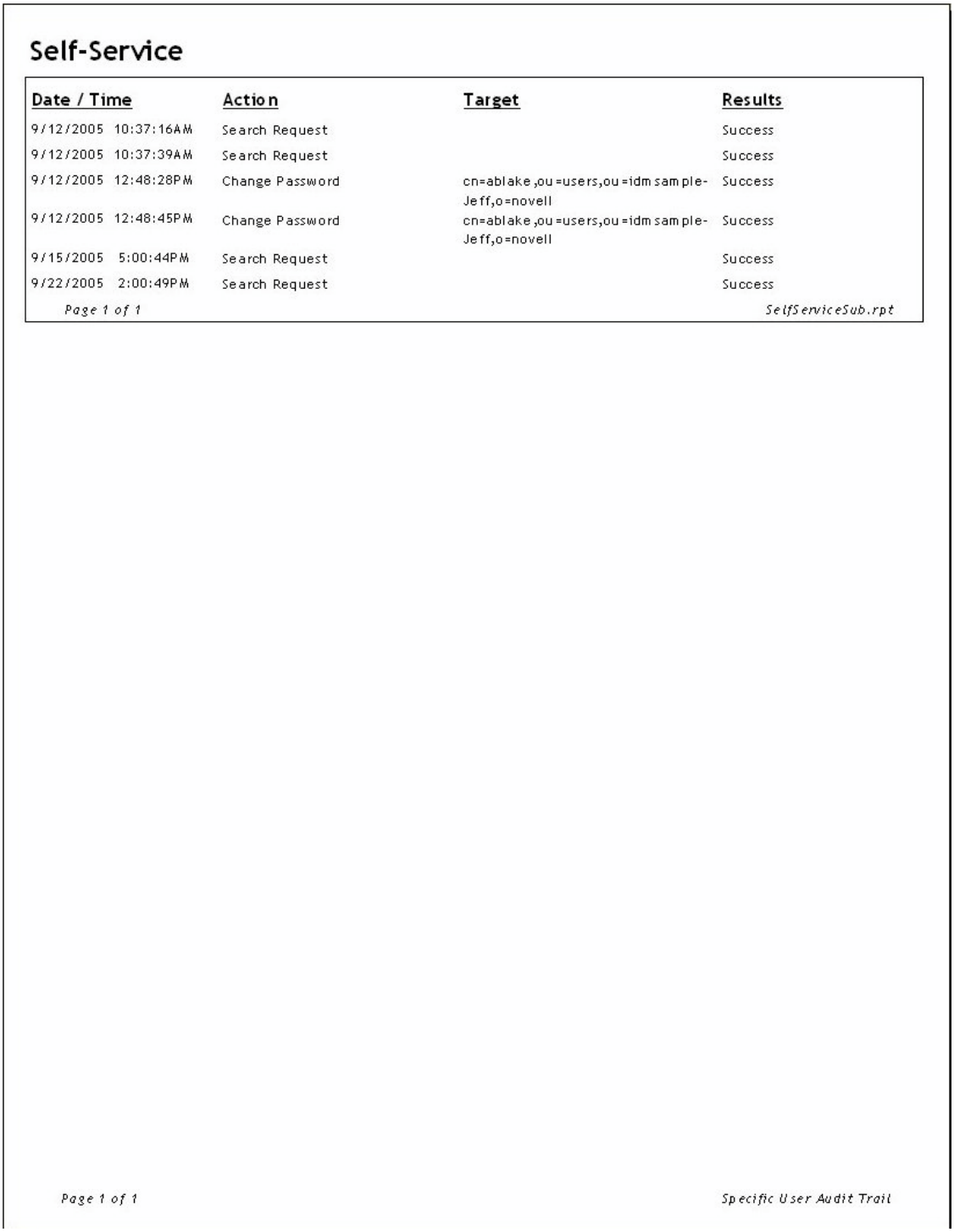
Date / Time	Action	Initiator ID
10/12/2005 11:58:13AM	Workflow Started	cn=ablake,ou=users,ou=idmsample-qatest,o=novell
10/12/2005 11:58:13AM	Workflow Forwarded	Workflow Administrator

Workflow Event: ea341eb11a824e669e356837745fe264

Date / Time	Action	Initiator ID
9/27/2005 4:24:44PM	Workflow Started	cn=mmackenzie,ou=users,ou=idmsample-Jeff,o=novell
9/27/2005 4:24:44PM	Workflow Forwarded	Workflow Administrator

Page 1 of 8 *Specific User Audit Trail*

图 ***C-5*** 特定用户审计追踪 *2*



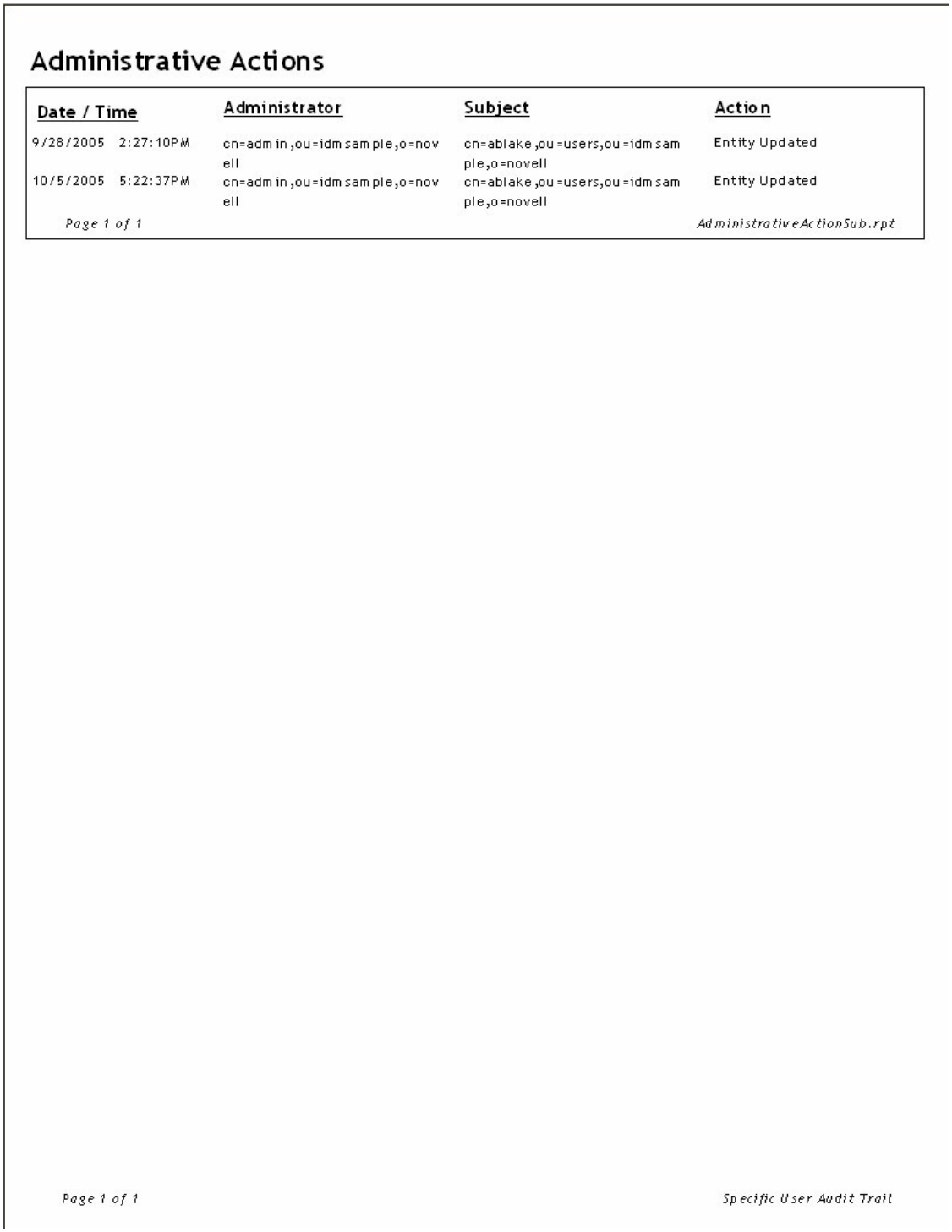
Self-Service

Date / Time	Action	Target	Results
9/12/2005 10:37:16AM	Search Request		Success
9/12/2005 10:37:39AM	Search Request		Success
9/12/2005 12:48:28PM	Change Password	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell	Success
9/12/2005 12:48:45PM	Change Password	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell	Success
9/15/2005 5:00:44PM	Search Request		Success
9/22/2005 2:00:49PM	Search Request		Success

Page 1 of 1 *SelfServiceSub.rpt*

Page 1 of 1 *Specific User Audit Trail*

图 ***C-6*** 特定用户审计追踪 *3*



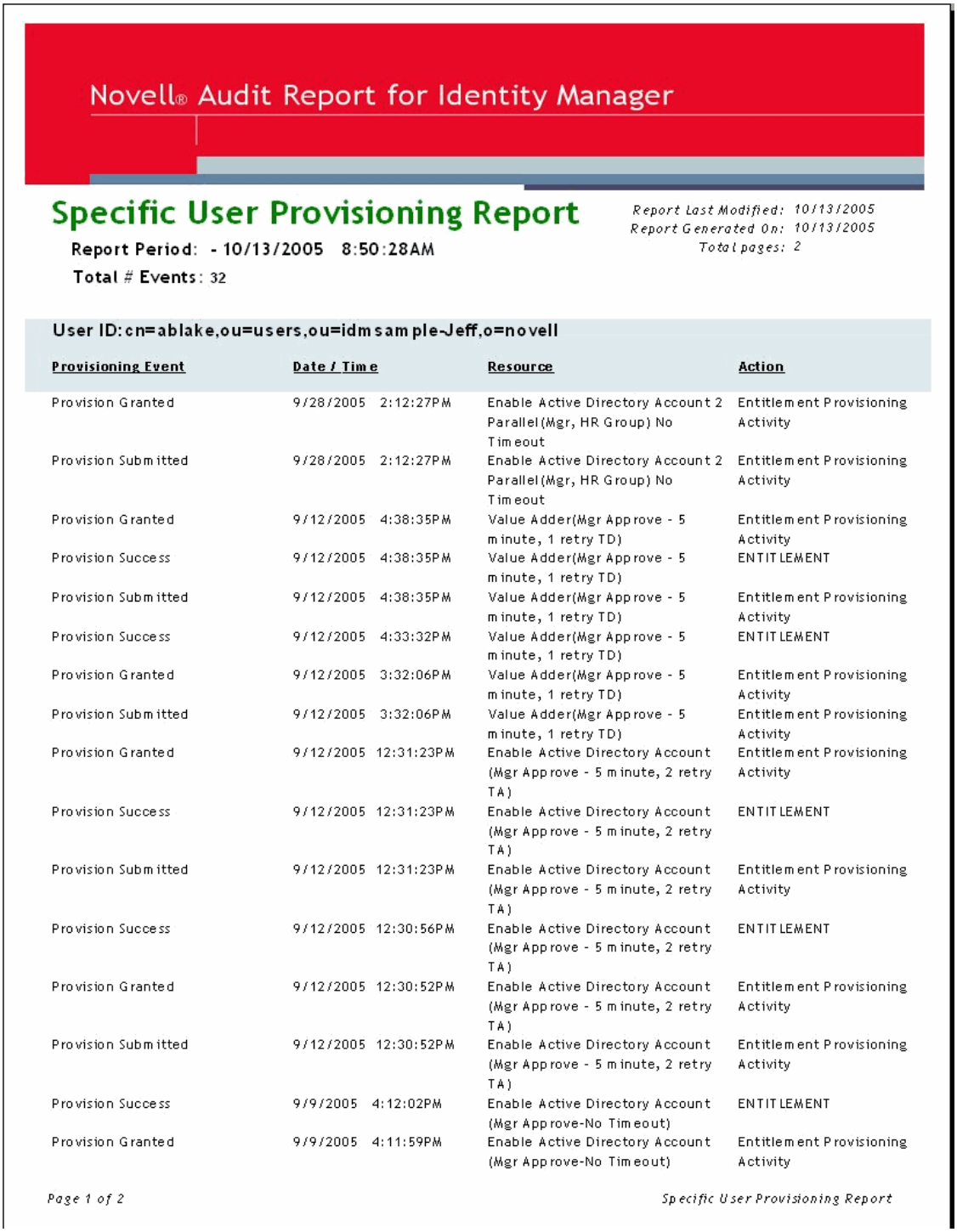
Administrative Actions

Date / Time	Administrator	Subject	Action
9/28/2005 2:27:10PM	cn=admin,ou=idmsample,o=novell	cn=ablake,ou=users,ou=idmsample,o=novell	Entity Updated
10/5/2005 5:22:37PM	cn=admin,ou=idmsample,o=novell	cn=ablake,ou=users,ou=idmsample,o=novell	Entity Updated

Page 1 of 1 *AdministrativeActionSub.rpt*

Page 1 of 1 *Specific User Audit Trail*

图 ***C-7*** 特定用户供应报告



Novell® Audit Report for Identity Manager

Specific User Provisioning Report

Report Period: - 10/13/2005 8:50:28AM

Total # Events: 32

Report Last Modified: 10/13/2005
Report Generated On: 10/13/2005
Total pages: 2

User ID: cn=ablake,ou=users,ou=idmsample-Jeff,o=novell

Provisioning Event	Date / Time	Resource	Action
Provision Granted	9/28/2005 2:12:27PM	Enable Active Directory Account 2 Parallel(Mgr, HR Group) No Timeout	Entitlement Provisioning Activity
Provision Submitted	9/28/2005 2:12:27PM	Enable Active Directory Account 2 Parallel(Mgr, HR Group) No Timeout	Entitlement Provisioning Activity
Provision Granted	9/12/2005 4:38:35PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Success	9/12/2005 4:38:35PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	ENTITLEMENT
Provision Submitted	9/12/2005 4:38:35PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Success	9/12/2005 4:33:32PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	ENTITLEMENT
Provision Granted	9/12/2005 3:32:06PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Submitted	9/12/2005 3:32:06PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Granted	9/12/2005 12:31:23PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Success	9/12/2005 12:31:23PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	ENTITLEMENT
Provision Submitted	9/12/2005 12:31:23PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Success	9/12/2005 12:30:56PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	ENTITLEMENT
Provision Granted	9/12/2005 12:30:52PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Submitted	9/12/2005 12:30:52PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Success	9/9/2005 4:12:02PM	Enable Active Directory Account (Mgr Approve-No Timeout)	ENTITLEMENT
Provision Granted	9/9/2005 4:11:59PM	Enable Active Directory Account (Mgr Approve-No Timeout)	Entitlement Provisioning Activity

Page 1 of 2 Specific User Provisioning Report

图 ***C-8*** 用户供应报告

Novell® Audit Report for Identity Manager

User Provisioning Report

Total # Events: 42

Report Period: - 10/13/2005 8:54:20AM

Report Last Modified: 10/13/2005
Report Generated On: 10/13/2005
Total pages: 3

User

cn=ablake,ou=users,ou=idmsample-Jeff,o=novell	Date / Time	Resource	Action
Provision Granted	9/28/2005 2:12:27PM	Enable Active Directory Account 2 Parallel(Mgr, HR Group) No Timeout	Entitlement Provisioning Activity
Provision Submitted	9/28/2005 2:12:27PM	Enable Active Directory Account 2 Parallel(Mgr, HR Group) No Timeout	Entitlement Provisioning Activity
Provision Granted	9/12/2005 4:38:35PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Success	9/12/2005 4:38:35PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	ENTITLEMENT
Provision Submitted	9/12/2005 4:38:35PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Success	9/12/2005 4:33:32PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	ENTITLEMENT
Provision Granted	9/12/2005 3:32:06PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Submitted	9/12/2005 3:32:06PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Granted	9/12/2005 12:31:23PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Success	9/12/2005 12:31:23PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	ENTITLEMENT
Provision Submitted	9/12/2005 12:31:23PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Success	9/12/2005 12:30:56PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	ENTITLEMENT
Provision Granted	9/12/2005 12:30:52PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Submitted	9/12/2005 12:30:52PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Success	9/9/2005 4:12:02PM	Enable Active Directory Account (Mgr Approve-No Timeout)	ENTITLEMENT
Provision Granted	9/9/2005 4:11:59PM	Enable Active Directory Account (Mgr Approve-No Timeout)	Entitlement Provisioning Activity

Page 1 of 3 User Provisioning Report

手工任务服务驱动程序：替换数据

D

替换数据与 XML 文档一起使用，而 XML 文档可作为模板构造电子邮件、万维网页和 XDS 文档。在构造输出文档的过程中，可使用执行替换操作的 XSLT 样式表处理模板文档，完成实际的替换。

替换数据通过订购者通道和发布者通道上的各种机制提供给手工任务服务驱动程序。

订购者通道

- 替换数据是 <mail> 要素的一部分。
- 提供的部分替换数据可以是 URL 数据。如果提供 URL 数据，则由自动数据项处理、完成和替换此数据 （请参见附录 E “手工任务服务驱动程序：自动替换数据项”在第 273 页）。
- 如果 <mail> 要素指定应构造关联值（即 <mail> 要素具有 src-dn 特性），则名为 " 关联 " 的自动数据项将添加到替换数据中。

发布者通道

- HTTP URL 数据和 HTTP POST 数据中提供了替换数据。
- 自动 URL 替换数据项在用于模板处理之前，会添加到替换数据中。

模板处理过程中，替换数据将显示为 XML 文档。替换数据文档被传递到样式表中，该样式表处理作为名为替换数据的参数的模板。如果未使用任何模板，则样式表将直接处理 XML 文档。

D.1 数据安全性

通过由订购者通道发送的电子邮件中包含的 URL，数据项从订购者通道传递至发布者通道。更改 URL 中的某些数据项意味着安全性威胁。例如，如果用提交到发布者通道万维网服务器的 URL 中其他用户的 DN，替换订购者通道提供的 URL 中的 responder-dn 值，则可能会允许未授权的用户更改 eDirectory 中的数据。

为了确保提交的 URL 中的数据与订购者通道最初提供的数据相同，提供了受保护数据。出于安全考虑，受保护数据无法更改。此类数据会随配置不同而有所不同，但总是包括 responder-dn 数据项，以及与其值发生更改的 eDirectory 对象相对应的数据项。

通过加密原始值以及将加密值放入 URL 查询字符串，可对数据项进行保护。发布者万维网服务器接收到加密值时，发布者将该值解密，并用它们来比较 HTTP GET 或 POST 请求提供的未加密的数据项。

如果加密数据中出现了数据项的实例，则未加密的数据项值必须与其中一个加密数据项的值相匹配。如果未加密的数据项值未能与某个加密的数据项值相匹配，则发布者通道万维网服务器将拒绝该 HTTP 请求。

此外，未包含受保护数据的任何 HTTP POST 请求都将被拒绝。

示例

在 HTTP POST 请求中，发布者通道万维网服务器使用名为 responder-dn 的未加密 POST 数据检查 POST 数据提供的口令。此操作旨在根据用户的 eDirectory 对象鉴定此响应用户。

假定订购者通道 <url-query> 要素内容指定了以下两个数据项：

```
<item name="responder-dn" protect="yes">\PERIN-TAO\novell\phb</item>


<item name="responder-dn" protect="yes">\PERIN-TAO\novell\carol</item>
```

由订购者通道生成的 URL 将包含受保护数据中的两个 responder-dn 值。

假设某个恶意用户获取了电子邮件中生成并发送的 URL。该恶意用户使用此 URL 即可获取允许用户更改 eDirectory 对象数据的 HTML 表格。

在提交到万维网服务器的 HTTP POST 请求中，该恶意用户使用他的 eDirectory DN (responder-dn=\PERIN-TAO\novell\wally) 作为未加密的 responder-dn 值。同时还在 POST 数据中提交他自己的口令，这样，万维网服务器执行的鉴定就会成功。

但当发布者通道万维网服务器收到 HTTP POST 数据时，由于它无法在加密的受保护的数据中找到 "\PERIN-TAO\novell\wally"，因此将拒绝 POST 请求。

D.2 XML 要素

下文中说明了构成替换数据文档的要素。如果没有描述要素的 XML 特性，则所有要素都不允许。

D.2.1 <replacement-data>

<replacement-data> 要素可能出现在以下位置中：

1. 作为订购者通道 <mail> 要素下的 <message> 的子要素。

   手工任务服务驱动程序将所提供的 <replacement-data> 要素作为独立的 <replacement-data> 要素，用于模板处理。将出现以下处理过程：

   a. 如果为附加 <mail> 要素创建了一个关联值，则将 <item name="association"> 要素添加到替换数据。已创建要素的值是返回 Identity Manager 的关联值。

   b. 如果 <replacement-data> 要素有一个子 <url-data> 要素，则多个包含构造 URL 数据的 <item> 要素将替换 <url-data> 要素。请参见 <url-data> 和 <url-query>。

2. 作为替换数据文档的独立顶级要素，在使用订购者通道或发布者通道中的样式表构造文档时使用。

D.2.2 <item>

<item> 要素可以为 <replacement-data> 要素、 <url-data> 要素或 <url-query> 要素的子要素。<item> 要素的内容为替代模板替换记号使用的文本。始终使用名称特性来命名 <item> 要素。

<item> 特性

name： 名称特性值指定名称，替换记号通过该名称来引用此数据项。例如，如果名称特性值为管理员，则替换记号 $manager$ 由包含在 <item name="manager"> 要素中的值替换。该名称特性为必需项。

protect： 对于 <url-query> 的子要素 <item>，保护特性指定是否将该项目添加到 URL 查询字符串的受保护数据部分 （请参见 <url-query>）。如果保护特性存在，则必须将其值设为 " 是 "。

预定义 **<item>** 名称

某些 <item> 要素的预定义含义可能是针对订购者通道的，也可能是针对发布者通道的，或同时针对这两个通道。

template： 发布者通道将模板项目值作为模板文档名称，用于生成 HTTP GET 请求的响应。

当 <item name="template"> 要素作为 <url-query> 的子要素出现在订购者通道中时，该值被放入 URL 查询数据中，用于向发布者通道万维网服务器指定响应 HTTP GET 请求要使用的模板文档名称。

responder-dn： 发布者通道将 HTTP POST 数据中的 responder-dn 项目值用作 eDirectory 对象的 DN，通过此 DN 可以验证 HTTP POST 数据中提供的口令。

万维网服务器将拒绝任何不包含 responder-dn 值和 password 值的 HTTP POST 请求。此外，如果 HTTP POST 数据中不包含受保护的数据项，则该请求也将被拒绝。

订购者通道将提供 <url-query> 要素下的一个或多个 <item name="responder-dn" protect="yes"> 要素。由于 responder-dn 项用于用户鉴定，因此必须受到保护。

password： 通过 HTTP POST 数据提供给发布者通道万维网服务器。该项目的内容即为口令，用于验证由 POST 数据中的 responder-dn 项目指定的 eDirectory 对象。通常将 password 项目输入到 HTML 表格中，以生成 HTTP POST 请求。

示例：

```
<INPUT TYPE= "password" NAME="password" SIZE="20" MAXLENGTH="40"/>
```

response-template：通过 HTTP POST 数据提供给万维网服务器。用于生成响应 POST 的万维网页。response-template 项目通常由隐藏的 INPUT 要素指定 （该要素在 HTML 表格中，用于生成 HTTP POST 请求）。

示例：

```
<INPUT TYPE="hidden" NAME="response-template" VALUE="post_form.xml"/>
```

response-stylesheet： 通过 HTTP POST 数据提供给万维网服务器。用于生成响应 POST 的万维网页。response-stylesheet 项目通常由隐藏的 INPUT 要素指定 （该要素在 HTML 表格中，用于生成 HTTP POST 请求）。

示例：

```
<INPUT TYPE="hidden" NAME="response-stylesheet"
```

```
VALUE="process_template.xsl"/>
```

auth-template：通过 HTTP POST 数据提供给万维网服务器。用于在用户鉴定失败时，生成用来响应 POST 的万维网页。auth-template 项目通常由隐藏的 INPUT 要素指定 （该要素在 HTML 表格中，用于生成 HTTP POST 请求）。

示例：

```
<INPUT TYPE="hidden" NAME="auth-template" VALUE="auth_response.xml"/>
```

auth-stylesheet：通过 HTTP POST 数据提供给万维网服务器。用于在用户鉴定失败时，生成用来响应 POST 的万维网页。auth-template 项目通常由隐藏的 INPUT 要素指定 （该要素在 HTML 表格中，用于生成 HTTP POST 请求）。

示例：

```
<INPUT TYPE="hidden" NAME="auth-stylesheet"
VALUE="process_template.xsl"/>
```

protected-data： 受保护的数据项中包含由订购者通道构造的加密数据。在订购者通道上，受保护的数据项为自动提供的项目。

在发布者通道上，可以从 HTTP GET 请求的 URL 查询字符串和 HTTP POST 请求的 POST 数据中获取受保护的数据项。

通常可以将受保护的数据项从 HTTP GET 请求传递到万维网页中，该万维网页可用于通过模板 （用于构造 HTTP GET 响应）中的替换记号来生成 HTTP POST。

示例：

```
<INPUT TYPE="hidden" NAME="protected-data" VALUE="$protected-data$"/>
```

D.2.3 <url-data>

<url-data> 要素为 <replacement-data> 的子要素，位于订购者通道中的 <message> 要素下。它包含用于构造 URL 的 <item> 要素和提供给构造电子邮件的模板的相关数据项。它也包含 <url-query> 要素。

为了使用手工任务服务驱动程序， URL 中包含了以下五部分：

1. 模式，如 http、 https 或 ftp。
2. 主机，如 www.novell.com 或 192.168.0.1。
3. 端口号。即冒号后面跟一个十进制整数。例如， :80 或 :8180。
4. 文件或资源限定词。这通常为文件名，可以包括路径信息。例如， stylesheets/process_template.xsl。
5. 查询字符串。这是由 & 字符分开的名称 - 值对的集合。例如，template=form_template.xml&protected-data=AabABJKEL=

<url-data> 中预定义的 **<item>** 名称

将忽略 <url-data> 中的 <item> 要素，除非它们属于以下项目之一。所有项均为可选项。

文件： 指定 URL 的文件部分。如果用于发布者通道万维网服务器，则该文件项目指定用于构造响应 URL 返回的初始 HTML 页的样式表。如果用于发布者通道万维网服务器以外的其它服务器，则文件项目指定 URL 将引用的资源名称。

如果未出现文件项目，则 URL 文件部分默认为 process_template.xsl。

模式： 位于 <url-data> 要素中的可选项目。如果存在，它将指定 URL 的模式部分 （例如 http 或 ftp）。通常仅在 URL 指向发布者万维网服务器以外的服务器时，才使用模式项目。

如果未出现模式项目，则 URL 模式根据发布者通道万维网服务器的配置默认为 http 或 https。

主机：位于 <url-data> 要素中的可选项目。如果存在，它将指定 URL 的主机部分。通常仅在 URL 指向发布者万维网服务器以外的服务器时，才使用主机项目。

如果未出现主机项目，则 URL 主机默认为正在运行手工任务服务驱动程序的服务器 IP 地址（即发布者通道万维网服务器的 IP 地址）。

端口： 位于 <url-data> 要素中的可选项目。如果存在，它将指定 URL 的端口部分。通常仅在 URL 指向发布者万维网服务器以外的服务器时，才使用端口项目。

如果未出现端口项目，则 URL 端口默认为发布者通道万维网服务器正在运行的端口。

D.2.4 <url-query>

<url-query> 要素为 <url-data> 的子要素。它包含用于构造电子邮件所使用的 URL 查询部分的 <item> 要素。

作为 <url-query> 子要素的每个项目都以 name="value" （其中 name 为 <item> 要素的名称特性值，而 value 为 <item> 要素的字符串内容）格式置于查询字符串中。

<url-query> 中出现的项目要素可以拥有一个保护特性，其值为 "yes"。在这种情况下，应将项目名称和值加密并置于 URL 查询字符串中生成的名称 - 值对中。生成值的名称为受保护的数据。该值为 Base64 编码和多值特性的加密名称 - 值对。

受保护数据确保将 URL 提交给发布者通道万维网服务器后，数据不被更改。例如，responder-dn 数据项需要被保护，以确保仅授权响应电子邮件的用户可以更改 eDirectory 数据。

如果生成的 URL 用于发布者通道万维网服务器，则 <url-query> 要素必须至少包含一个 <item name="responder-dn" protect="yes"> 要素，否则万维网服务器将拒绝最终 HTTP POST 请求。

手工任务服务驱动程序：自动替换数据项

E

手工任务服务驱动程序自动提供某些替换数据项要素。本部分描述这些数据项。

E.1 订购者通道自动替换数据

在处理过程中，订购者通道将以下数据项自动添加到替换数据文档：

association：如果 <mail> 要素有 <association> 子要素，或如果订购者返回 <add-association> 要素，则将 <item name="association"> 要素添加到替换数据文档。<item> 要素的内容为与被处理的电子邮件相关联的 eDirectory 对象的关联值。关联值可能尚未写入 eDirectory 对象，因此，无法在查询中使用关联值。

url： <item> 要素的内容是将在电子邮件中使用的完整 URL。在订购者通道中，根据位于 <url-data> 要素中的以下项目创建 URL 项目：模式、主机、端口、文件和位于 <url-query> 要素下的项目。如果未找到模式、主机或端口，则使用默认值。默认值由发布者通道万维网服务器的配置决定。

url-base：<item> 要素的内容为生成的 URL 部分，不包括资源标识符 （文件）和查询字符串。

url-query： <item> 要素的内容为从 <url-query> 要素下的 <item> 要素中生成的 URL 查询字符串。

url-file： <item> 要素的内容为 URL 的资源标识符。

protected-data： <item> 要素的内容为从 <url-query> 要素下的 <item> 要素中获取的名称 - 值对的加密形式。仅将保护特性被设置为 "yes" 的 <item> 要素添加到受保护的数据值。有关受保护的数据的更多信息，请参见附录 D “手工任务服务驱动程序：替换数据”在第 267 页 中的 " 数据安全性 "。

E.2 发布者通道自动替换数据

在处理过程中，发布者通道万维网服务器将以下数据项自动添加到替换数据文档：

post-status： 在处理 HTTP POST 请求的过程中，发布者通道万维网服务器创建了 <item name="post-status"> 要素，并将其添加到替换数据文档。对万维网服务器的 HTTP POST 请求的内容是将 XDS 文档提交至 Identity Manager。Identity Manager 返回作为 XDS 提交结果的状态文档。<item name="post-status"> 要素的内容为 <status> 要素的级别特性值，该值由 Identity Manager 作为提交结果返回。

post-status 项目通常用于构造作为 HTTP POST 请求结果返回的万维网页。

post-status-message： 在处理 HTTP POST 请求的过程中，发布者通道万维网服务器将创建 <item name="post-status-message"> 要素，并将其添加到替换数据文档。万维网服务器的 HTTP POST 请求为向 Identity Manager 提交 XDS 文档的请求。Identity Manager 返回作为 XDS 提交结果的状态文档。<item name="post-status-message"> 要素的内容为由 Identity Manager 返回的作为其提交结果的 <status> 要素的内容。仅在 Identity Manager 返回的 <status> 要素包含内容时，才创建 post-status-message 项目。

post-status-message 项目通常用于构造作为 HTTP POST 请求结果返回的万维网页。

url： 在处理 HTTP GET 和 HTTP POST 请求期间，发布者通道万维网服务器创建 <item name="url"> 要素并将其添加到替换数据文档中。在使用替换数据文档构造任意文档前将添加 <item> 要素。URL 模式、主机和端口由万维网服务器配置决定。

url-base： 在处理 HTTP GET 和 HTTP POST 请求期间，发布者通道万维网服务器创建 <item name="url-base"> 并将其添加到替换数据文档中。在使用替换数据文档构造任意文档前将添加 <item> 要素。发布者通道上 url-base <item> 要素的内容与 url <item> 要素的内容相同。

手工任务服务驱动程序：模板操作要素参照

F

操作要素是模板文档中名称空间限定的要素，用于简单逻辑控制或用于为 HTML 表格创建 HTML 要素。用于限定要素的名称空间是 http://www.novell.com/dirxml/manualtask/form。在本文档和随手工任务服务驱动程序一起提供的示例模板中，使用的前缀是 form。

本部分未专门涵盖的所有操作要素均被模板处理样式表从输出文档中去除 （除非样式表是自定义的）。例如，此行为允许使用 form:text 要素包含纯文本电子邮件的数据，从而使模板成为有效的 XML。

F.1 <form:input>

基于一个或多个替换数据项的存在， <form:input> 要素用于生成一个或多个 HTML INPUT 要素。创建的 INPUT 要素的数量对应于具有由 <form:input> 要素名称特性指定其名称的替换数据项的数量。

特性

Name： 指定用于创建 INPUT 要素的替换数据项的名称。此特性值用作创建的 INPUT 要素的名称特性值。

type 或 **TYPE**： 指定创建的 INPUT 要素的类型特性值。

value： 如果值特性的值等于 "yes"，则将值特性添加到创建的 INPUT 要素，这些要素的值为替换数据项的字符串值。如果值特性的值不是 "yes"，则将创建的 INPUT 要素的内容设置为替换数据项的字符串值。

示例

```
<form:input name="responder-dn" TYPE="hidden" value="yes"/>
```

创建一个或多个 INPUT 要素，类似于

```
<INPUT name="responder-dn" TYPE="hidden" value="\PERIN-
TAO\novell\phb"/>
```

F.2 <form:if-item-exists>

使用 <form:if-item-exists> 要素可有条件地将数据插入到输出文档中。仅当指定项出现在替换数据中时，才处理 <form:if-item-exists> 内容。

特性

Name： 指定替换数据项的名称。如果存在一个或多个替换数据项示例，则处理 <form:if-item-exists> 要素的内容。

示例

```
<form:if-item-exists name="post-status-message"> <tr> <td> Status
message was: $post-status-message$ </td> </tr> </form:if-item-exists>
```

此示例仅在存在名为 post-status-message 的替换数据项时才在 HTML 表中插入一行。

F.3 <form:if-multiple-items>

使用 form:if-multiple-items 要素可有条件地将数据插入到输出文档中。仅当指定项在替换数据中出现多次时，才处理 form:if-multiple-items 的内容。

特性

name： 指定替换数据项的名称。如果存在多个替换数据项示例，则处理 form:if-multiple-items 的内容。

示例

```
<form:if-multiple-items name="responder-dn"> <form:menu
name="responder-dn"/> </form:if-multiple-items>
```

如果存在多个名为 responder-dn 的替换数据项，则此示例将生成 HTML SELECT 要素 （请参见 <form:menu>）。

F.4 <form:if-single-item>

使用 form:if-single-item 要素可有条件地将数据插入到输出文档中。仅当指定项在替换数据中只出现一次时，才处理 form:if- single 衖 tem 的内容。

特性

name： 指定替换数据项的名称。仅当命名项在替换数据中只出现一次时，才处理 form:if-single-item 的内容。

示例

```
<form:if-single-item name="responder-dn"> <input TYPE="hidden"
name="responder-dn" value="$responder-dn$"/> $responder-dn$ </form:if-
single-item>
```

如果替换数据中只有一个名为 "responder-dn" 的替换数据项，则此示例将 HTML INPUT 要素和某个替换文本插入到输出文档中。

F.5 <form:menu>

可使用 form:menu 要素生成具有一个或多个 OPTION 子要素的 HTML SELECT 要素。第一个 OPTION 子要素标记为选中。

特性

name： 指定替换数据项的名称。如果命名项出现在替换数据中，则在输出文档中创建 HTML SELECT 要素。对于替换数据中每个替换数据项的实例，都将创建一个 HTML OPTION 要素作为 SELECT 要素的子要素。

示例

```
<form:menu name="responder-dn"/>
```

此示例生成类似以下内容的 HTML 要素：

```
<SELECT name="responder-dn"> <OPTION selected>\PERIN-TAO\big-org\php</
OPTION> <OPTION>\PERIN-TAO\big-org\carol</OPTION> </SELECT>
```

手工任务服务驱动程序：<mail> 要素参照

G

本部分详细介绍了 <mail> 要素及其内容。如果未列出要素的任何特性，则该要素不具有已定义的特性。

G.1 <mail>

<mail> 要素及其内容描述了构造 SMTP 邮件必需的数据。

<mail> 特性

src-dn： 包含触发电子邮件的 eDirectory 对象的 DN 值。如果为响应电子邮件需通过发布者通道的万维网服务器修改对象数据，则必需使用此特性。

G.2 <to>

<to> 要素为 <mail> 要素的子要素。一个或多个 <to> 要素包含 SMTP 邮件的主收件人电子邮件地址。必须至少有一个 <to> 要素。每个 <to> 要素必须只包含一个电子邮件地址。

G.3 <cc>

<cc> 要素为 <mail> 要素的子要素。零个或多个 <cc> 要素包含 SMTP 邮件的抄送收件人的电子邮件地址。<cc> 要素不是必选项。每个 <cc> 要素都必须只包含一个电子邮件地址。

G.4 <bcc>

<bcc> 要素为 <mail> 要素的子要素。零个或多个 <bcc> 要素包含 SMTP 邮件的密送收件人的电子邮件地址。<bcc> 要素不是必选项。每个 <bcc> 要素都必须只包含一个电子邮件地址。

G.5 <from>

<from> 要素为 <mail> 要素的子要素。<from> 要素包含电子邮件寄件人的电子邮件地址。<from> 要素不是必选项。如果 <from> 要素不存在，则使用作为手工任务服务驱动程序参数一部分提供的默认发件人地址。

G.6 <reply-to>

<reply-to> 要素为 <mail> 要素的子要素。<reply-to> 要素包含要处理的 SMTP 邮件回复实体的电子邮件地址。<reply-to> 要素不是必选项。

G.7 <subject>

<subject> 要素为 <mail> 要素的子要素。其字符串内容可用于设置 SMTP 主题字段。<subject> 要素不是必选项，但显而易见非常实用，因此建议使用。

G.8 <message>

<message> 要素为 <mail> 要素的子要素。其内容可用于构造 SMTP 邮件的邮件正文。必须至少有一个 <message> 要素。使用邮件正文的替换表示形式 （例如纯文本和 HTML，或者英语和其它语言）构造 SMTP 邮件时，可以提供多个 <message> 要素。

<message> 特性

mime-type： （可选）指定由 <message> 要素 （例如 text/plain 或 text/html）构造的邮件正文的 MIME 类型。如果 MIME 类型特性不存在，则驱动程序将自动尝试发现 MIME 类型。

电子邮件客户程序可以在 SMTP 邮件具有替换表示形式时使用 MIME 类型，以便选择最佳表示形式用于显示。

language： （可选）指定由 <message> 要素构造的邮件正文的语言。该值应遵循 SMTP 规范。如果语言特性不存在，则不提供默认值。

电子邮件客户程序可以在 SMTP 邮件具有替换表示形式时使用语言规范，以便选择最佳表示形式用于显示。

G.9 <stylesheet>

<stylesheet> 要素为 <message> 要素的子要素。<stylesheet> 要素的内容是用于构造邮件正文的 XSLT 样式表的名称。如果 <stylesheet> 要素不存在，则使用 process_template.xsl 作为样式表。

G.10 <template>

<template> 要素为 <message> 要素的子要素。<template> 要素的内容是用于构造邮件正文的 XML 文档的名称。如果 <template> 要素不存在，则由邮件样式表处理替换数据文档以构造邮件正文。

G.11 <filename>

<filename> 要素为 <attachment> 要素的子要素。<filename> 要素的内容是文件名。可使用文件名值将文件名指派给构造的附件。

G.12 <replacement-data>

<replacement-data> 要素为 <message> 要素的子要素。可将其内容用作处理邮件模板的样式表的参数，或在没有模板时，直接由邮件样式表处理。附录 D “手工任务服务驱动程序：替换数据”在第 267 页 和 附录 E “手工任务服务驱动程序：自动替换数据项”在第 273 页中介绍了 <replacement-data> 要素的内容。

G.13 <resource>

<resource> 要素为 <message> 要素的子要素。其内容被视为要合并到 SMTP 邮件的文件的名称，即邮件正文的资源。例如，可以将 HTML 邮件正文的 .css 样式表提供为资源。

<resource> 特性

cid：指定用于指代邮件正文中 URL 中资源的内容 ID。例如，如果 .css 样式表是资源，则 cid 值可能是 css-1。在 HTML 邮件正文中，可使用以下要素来指代 .css 样式表：

```
<link href="cid:css-1" rel="style sheet" type="text/css">
```

G.14 <attachment>

<attachment> 要素为 <mail> 要素的子要素。它可以与 <message> 具有相同的内容，或它可以采用文件名作为内容。零个或多个 <attachment> 要素可以显示为 <mail> 要素的子要素。

<attachment> 特性

mime-type：（可选）指定附件的 MIME 类型。如果 mime-type 特性不存在，则驱动程序将自动尝试发现 MIME 类型。

language：（可选）指定附件的语言。如果语言特性不存在，则不提供默认值。

手工任务服务驱动程序：新员工的数据流方案

H

在本部分中，在雇佣新员工时向发送员工经理电子邮件的示例环境下，对数据流进行了分步分析。电子邮件要求经理使用邮件中的 URL 输入员工的房间号值。

对于此示例方案，手工任务服务驱动程序的配置如下。

H.1 订购者通道配置

过滤器

类：User

特性：Given Name、 manager、 Surname

策略

创建策略：需要 Given Name、 manager、 Surname 等特性。

命令转换策略：将 <add> 转换为 <mail> 要素。

H.2 发布者通道配置

过滤器

类：User

特性：roomNumber

策略

无。

H.3 数据流说明

在下面的列表中，进程中通过的最重要的数据项是 responder-dn 和 association。responder-dn 项用于鉴定通过万维网服务器输入数据的用户。association 项标识将要更改其数据的 eDirectory 对象。

1. 公司雇佣了一名新员工。该新员工的数据被输入到公司的人力资源 (HR) 系统中。
2. 人力资源系统的 Identity Manager 驱动程序在 eDirectory 中创建了一个新的 User 对象。User 特性包括 Given Name、 Surname 和 manager。
3. 将新的 User 对象的以下 <add> 事件提交给手工任务服务驱动程序订购者通道：

```
<nds dtdversion="1.1" ndsversion="8.6"> <input> <add class-
name="User" src-dn="\PERIN-TAO\novell\Provo\Joe" src-entry-
```

```
id="281002" timestamp="1023314433#2"> <add-attr attr-
name="Surname"> <value type="string">the Intern</value> <add-attr>
<add-attr attr-name="Given Name"> <value type="string">Joe</value>
<add-attr> <add-attr attr-name="manager"> <value type="dn">\PERIN-
TAO\novell\Provo\phb</value> <add-attr> </add> </input> </nds>
```

a. 订购者命令转换策略使用经理的 DN 值向 eDirectory 发出查询，查询经理的电子邮件地址和经理助理的 DN。

b. 如果经理有助理，则订购者命令转换向 eDirectory 发出查询，查询助理的电子邮件地址。

c. 订购者命令转换构造一个 <mail> 要素并使用 <mail> 要素替换 <add> 命令要素。在下面的示例中，替换数据项为粗体。

```
<nds dtdversion="1.1" ndsversion="8.6"> <input> <mail src-
dn="\PERIN-TAO\novell\Provo\Joe"> <to>phb@company.com</to>
<cc>carol@company.com</cc> <bcc>HR@company.com</bcc> <reply-
to>HR@company.com</reply-to> <subject>Room Assignment Needed
for: Joe the Intern</subject> <message mime-type="text/html">
<stylesheet>process_template.xsl</stylesheet>
<template>html_msg_template.xml</template> <replacement-data>
<item name="manager">JStanley</item>           <item
name="given-name">Joe</item>          <item name="surname">the
Intern</item> <url-data> <item
name="file">process_template.xsl</item> <url-query>   <item
name="template">form_template.xml</item>               <item
name="responder-dn" protect="yes">\PERIN-TAO\novell\Provo\phb</
item>               <item name="responder-dn"
protect="yes">\PERIN-TAO\novell\Provo\carol</item>
<item name="subject-name">Joe the Intern</item> </url-query> </
url-data> </replacement-data> <resource cid="css-
1">novdocmain.css</resource> </message> </mail> </input> </nds>
```

d. 手工任务服务驱动程序订购者从 Nsure™ Identity Manager 接收 <mail> 要素。

e. 由于 <mail> 要素具有 src-dn 特性，因此订购者生成一个关联值。

f. 订购者根据 <mail> 要素中的用于构造电子邮件的数据构造替换数据文档。URL 在查询部分有各种数据项 （跟在 '?' 字符后面且为粗体的那部分 URL）。在向万维网服务器提交 URL 作为 HTTP GET 请求时，发布者通道万维网服务器将使用这些数据项。

```
<replacement-data> <item name="manager">JStanley</item> <item
name="given-name">Joe</item> <item name="surname">the Intern</
item> <item name="template">form_template.xml</item> <item
name="responder-dn">\PERIN-TAO\novell\Provo\phb</item> <item
name="responder-dn">\PERIN-TAO\novell\Provo\carol</item> <item
name="subject-name">Joe the Intern</item> <item
name="association">1671b2:ee4246a561:-7fff:192.168.0.1</item>
<item name="url-base">https://192.168.0.1:8180</item> <item
name="url-file">process_template.xsl</item> <item
name="protected-data">
rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHACAARbAA
1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB+AAFMAAlw
```

```
YXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB+AAJ4cH
VyAAJbQqzzF/gGCFTgAgAAeHAAAAAPMA0ECEIBRohGPjxEAgEKdXEAfgAEAAAA
uMSFqzHXwtMx8DkRCzkK1O46sEz1u51o3MDvHn+3+fE6SphHr3Hgjli4Jp3rUk
H7y6dXvcu7iq21Vs+9o6iZVzljTIJX/jjRrVZlR5JOuRNhk8JHFZ8FhgsmiIAH
/Fs61k4WmyEcmYfWmfqfBVeThr3Avwcim6ranS5Mm2U5i9Z/DBR13pIAobMpWY
kMaz4+G9e6oovBsiPdp6jSPzbFxcgALI2AMBh4hf9jnx7zOU9Uvd9qXtaE2rR0
AANQQkV0ABBQQkVXaXRoTUQ1QW5kREVT</item> <item name="url-
query">template=form_template.xml&amp;responder-dn=%5CPERIN-
TAO%5Cnovell%5Cprovo%5Cphb&amp;responder-dn=%5CPERIN-
TAO%5Cnovell%5Cprovo%5Ccarol&amp;subject-
name=Joe+the+Intern&amp;association=1671b2%3Aee4246a561%3A-
7fff%3A192.168.0.1&amp;protected-
data=rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHACAA
RbAA1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB%2BAAF
MAAlwYXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB%2B
AAJ4cHVyAAJbQqzzF%2FgGCFTgAgAAeHAAAAAPMA0ECEIBRohGPjxEAgEKdXEAf
gAEAAAAuMSFqzHXwtMx8DkRCzkK1O46sEz1u51o3MDvHn%2B3%2BfE6SphHr3Hg
jli4Jp3rUkH7y6dXvcu7iq21Vs%2B9o6iZVzljTIJX%2FjjRrVZlR5JouRNhk8J
HFZ8FhgsmiIAH%2FFs61k4WmyEcmYfWmfqfBVeThr3Avwcim6ranS5Mm2U5i9Z%
2FDBR13pIAobMpWYkMaz4%2BG9e6oovBsiPdp6jSPzbFxcgALI2AMBh4hf9jnx7
zOU9Uvd9qXtaE2rR0AANQQkV0ABBQQkVXaXRoTUQ1QW5kREVT</item> <item
name="url"> https://192.168.0.1:8180/
process_template.xsl?template=form_template.xml&amp;responder-
dn=%5CPERIN-TAO%5Cnovell%5CProvo%5Cphb&amp;responder-
dn=%5CPERIN-TAO%5Cnovell%5Cprovo%5Ccarol&amp;subject-
name=Joe+the+Intern&amp;association=1671b2%3Aee4246a561%3A-
7fff%3A192.168.0.1&amp;protected-
data=rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHACAA
RbAA1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB%2BAAF
MAAlwYXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB%2B
AAJ4cHVyAAJbQqzzF%2FgGCFTgAgAAeHAAAAAPMA0ECEIBRohGPjxEAgEKdXEAf
gAEAAAAuMSFqzHXwtMx8DkRCzkK1O46sEz1u51o3MDvHn%2B3%2BfE6SphHr3Hg
jli4Jp3rUkH7y6dXvcu7iq21Vs%2B9o6iZVzljTIJX%2FjjRrVZlR5JouRNhk8J
HFZ8FhgsmiIAH%2FFs61k4WmyEcmYfWmfqfBVeThr3Avwcim6ranS5Mm2U5i9Z%
2FDBR13pIAobMpWYkMaz4%2BG9e6oovBsiPdp6jSPzbFxcgALI2AMBh4hf9jnx7
zOU9Uvd9qXtaE2rR0AANQQkV0ABBQQkVXaXRoTUQ1QW5kREV </item> </
replacement-data>
```

g. 订购者使用 process_template.xsl 处理 html_msg_template.xml。替换数据文档将作为参数传递给样式表。随后是 html_msg_template.xml 文档。请注意粗体的替换令牌。替换令牌由替换数据文档中对应的 <item> 要素值替换。

```
<html xmlns:form="http://www.novell.com/dirxml/manualtask/
form"> <head> </head> <body> <link href="cid:css-1" rel="style
sheet" type="text/css"/> <p> Dear $manager$, </p> <p> This
message is to inform you that your new employee <b>$given-name$
$surname$</b> has been hired. </p> <p> Please assign a room
number for this individual. Click <a href="$url$">Here</a> to
do this. </p> <p> Thank you,<br/> HR<br/> HR Department </p> </
body> </html>
```

其后是生成的电子邮件文档。替换令牌已由替换数据文档中对应的 <item> 要素值替换。

```
<html> <head> <META http-equiv="Content-Type" content="text/
html; charset=UTF-8"> </head> <body> <link href="cid:css-1"
rel="style sheet" type="text/css"> <p> Dear J Stanley, </p> <p>
This message is to inform you that your new employee <b>Joe the
Intern</b> has been hired. </p> <p> Please assign a room number
for this individual. Click <a href="https://192.168.0.1:8180/
process_template.xsl?template=form_template.xml&responder-
dn=%5CPERIN-TAO%5Cnovell%5CProvo%5Cphb&responder-dn=%5CPERIN-
TAO%5Cnovell%5CProvo%5Ccarol&subject-
name=Joe+the+Intern&association=45f0e3%3Aee45e07709%3A-
7fff%3A192.168.0.1&protected-
data=rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHACAA
RbAA1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB%2BAAF
MAAlwYXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB%2B
AAJ4cHVyAAJbQqzzF%2FgGCFTgAgAAeHAAAAAPMA0ECIr9Z1iG%2BO3BAgEKdXE
AfgAEAAAAuMU%2FSoFRkebvh2d5SqalF91ttjRY5lyyW5%2B%2FFIfOuDdYikYi
DbOJb6607S0dPHjQzeVgu6ptIvGqaEQOEjBjDkY%2Bi4VoVjUSXS3a8fiXB8moM
dPtLJ%2FGyE8QiwbT4xbkQy48i02k99F2vGmlenRpSP6dD31kZl3dpJ0mGgq2yL
%2FeFaynKyqnjkHLMexcqD8WlVooaRl1k2RPk5vDYvC8o2bn22OKKbOnSRM5YlP
S0iWzxo0JVcnVVyt0AANQQkV0ABBQQkVXaXRoTUQ1QW5kREVT">Here</a> to
do this. </p> <p> Thank you,<br> HR<br> HR Department </p> </
body> </html>
```

h. 将 SMTP 电子邮件发送给经理和经理助理。

i. 订购者将包含 <status> 要素和 <add-association> 要素的 XML 文档返回给 Identity Manager。

4. 经理打开电子邮件并单击 " 单击此处 " 链接。

5. 经理的万维网浏览器将 URL 作为 HTTP GET 请求提交给发布者通道万维网服务器。

   a. 万维网服务器将构造以下替换数据文档。大多数数据项来自 URL 的查询部分。自动生成的 URL 项和基于 URl 项的例外。

```
<replacement-data> <item name="association">45f0e3:ee45e07709:-
7fff:192.168.0.1</item> <item name="protected-
data">rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHACA
ARbAA1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB+AAFM
AAlwYXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB+AAJ
4cHVyAAJbQqzzF/
gGCFTgAgAAeHAAAAAPMA0ECIr9Z1iG+O3BAgEKdXEAfgAEAAAAuMU/
SoFRkebvh2d5SqalF91ttjRY5lyyW5+/
FifOuDdYikYiDbOJb6607S0dPHjQzeVgu6ptIvGqaEQOEjBjDkY+i4VoVjUSXS3
a8fiXB8moMdPtLJ/
GyE8QiwbT4xbkQy48i02k99F2vGmlenRpSP6dD31kZl3dpJ0mGgq2yL/
eFaynKyqnjkHLMexcqD8WlVooaRl1k2RPk5vDYvC8o2bn22OKKbOnSRM5YlPS0i
Wzxo0JVcnVVyt0AANQQkV0ABBQQkVXaXRoTUQ1QW5kREVT</item> <item
name="template">form_template.xml</item> <item name="responder-
dn">\PERIN-TAO\novell\Provo\phb</item> <item name="responder-
dn">\PERIN-TAO\novell\Provo\carol</item> <item name="subject-
name">Joe the Intern</item> <item name="url-base">https://
192.168.0.1:8180</item> <item name="url">https://
```

```
192.168.0.1:8180</item> </replacement-data>
```

万维网服务器使用 process_template.xsl 样式表处理 form_templates.xml 文档。替换令牌和操作要素为粗体。请注意，多个数据项放置在隐藏的 INPUT 要素中，这样即可以将数据项作为 HTML POST 数据的一部分传递给万维网服务器。

此外，还有一个 $query:roomNumber$ 替换令牌，该令牌检索员工 roomNumber 特性的当前值 （如果有）。

```
<html  xmlns:form="http://www.novell.com/dirxml/manualtask/
form"> <head> <title>Enter room number for $subject-name$</
title> </head> <body> <link href="novdocmain.css" rel="style
sheet" type="text/css"/> <br/><br/><br/><br/> <form
class="myform" METHOD="POST" ACTION="$url-base$/
process_template.xsl"> <table cellpadding="5" cellspacing="10"
border="1" align="center"> <tr><td> <input TYPE="hidden"
name="template" value="post_form.xml"/> <input TYPE="hidden"
name="subject-name" value="$subject-name$"/> <input
TYPE="hidden" name="association" value="$association$"/> <input
TYPE="hidden" name="response-style sheet"
value="process_template.xsl"/> <input TYPE="hidden"
name="response-template" value="post_response.xml"/> <input
TYPE="hidden" name="auth-style sheet"
value="process_template.xsl"/> <input TYPE="hidden" name="auth-
template" value="auth_response.xml"/> <input TYPE="hidden"
name="protected-data" value="$protected-data$"/> <form:if-
single-item name="responder-dn">   You are:<br/> <input
TYPE="hidden" name="responder-dn" value="$responder-dn$"/>
$responder-dn$  </form:if-single-item>          <form:if-
multiple-items name="responder-dn"> Indicate your identity:<br/
>  <form:menu name="responder-dn"/>         </form:if-multiple-
items> </td></tr> <tr><td> Enter your password: <br/><input
name="password" TYPE="password" SIZE="20" MAXLENGTH="40"/> </
td></tr> <tr><td> Enter room number for $subject-name$:<br/>
<input TYPE="text" NAME="room-number" SIZE="20" MAXLENGTH="20"
value="$query:roomNumber$"/> </td></tr> <tr><td> <input
TYPE="submit" value="Submit"/> <input TYPE="reset"
value="Clear"/> </td></tr> </table> </form> </body> </html>
```

即生成以下 HTML 页：

```
<html> <head> <META http-equiv="Content-Type" content="text/
html; charset=UTF-8"> <title>Enter room number for Joe the
Intern</title> </head> <body> <link href="novdocmain.css"
rel="style sheet" type="text/css"> <br><br><br><br> <form
class="myform" METHOD="POST" ACTION="https://192.168.0.1:8180/
process_template.xsl"> <table cellpadding="5" cellspacing="10"
border="1" align="center"> <tr> <td> <input TYPE="hidden"
name="template" value="post_form.xml"> <input TYPE="hidden"
name="subject-name" value="Joe the Intern"> <input
TYPE="hidden" name="association" value="45f0e3:ee45e07709:-
7fff:192.168.0.1"> <input TYPE="hidden" name="response-style
sheet" value="process_template.xsl"> <input TYPE="hidden"
```

```
name="response-template" value="post_response.xml"> <input
TYPE="hidden" name="auth-style sheet"
value="process_template.xsl"> <input TYPE="hidden" name="auth-
template" value="auth_response.xml"> <input TYPE="hidden"
name="protected-data"
value="rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHAC
AARbAA1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB+AAF
MAAlwYXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB+AA
J4cHVyAAJbQqzzF/
gGCFTgAgAAeHAAAAAPMA0ECIr9Z1iG+O3BAgEKdXEAfgAEAAAAuMU/
SoFRkebvh2d5SqalF91ttjRY5lyyW5+/
FIfOuDdYikYiDbOJb6607S0dPHjQzeVgu6ptIvGqaEQOEjBjDkY+i4VoVjUSXS3
a8fiXB8moMdPtLJ/
GyE8QiwbT4xbkQy48i02k99F2vGmlenRpSP6dD31kZl3dpJ0mGgq2yL/
eFaynKyqnjkHLMexcqD8WlVooaRl1k2RPk5vDYvC8o2bn22OKKbOnSRM5YlPS0i
Wzxo0JVcnVVyt0AANQQkV0ABBQQkVXaXRoTUQ1QW5kREVT"> Indicate your
identity:<br> <SELECT name="responder-dn"> <OPTION
selected>\PERIN-TAO\novell\Provo\phb</OPTION> <OPTION>\PERIN-
TAO\novell\Provo\carol</OPTION> </SELECT> </td> </tr> <tr> <td>
Enter your password: <br>

    <input name="password" TYPE="password" SIZE="20"
MAXLENGTH="40"> </td> </tr> <tr> <td> Enter room number for Joe
the Intern:<br> <input TYPE="text" NAME="room-number" SIZE="20"
MAXLENGTH="20" value=""> </td> </tr> <tr> <td> <input
TYPE="submit" value="Submit"> <input TYPE="reset"
value="Clear"> </td> </tr> </table> </form> </body> </html>
```

b. 经理从网页菜单中选择他 / 她的 eDirectory DN，输入口令，再输入新员工的房间号，然后单击 " 提交 "。

c. 万维网浏览器将 HTTP POST 请求提交给万维网服务器。

d. 万维网服务器根据 POST 数据构造以下替换数据文档。请注意各种隐藏 <INPUT> 要素中的数据。经理在此表格中输入的数据为粗体。

```
<replacement-data>   <item name="room-number">cubicle 1234</
item> <item name="template">post_form.xml</item> <item
name="response-template">post_response.xml</item> <item
name="auth-template">auth_response.xml</item> <item
name="association">45f0e3:ee45e07709:-7fff:192.168.0.1</item>
<item name="password" is-sensitive="true"><!-content suppressed
?</item> <item name="protected-
data">rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHACA
ARbAA1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB+AAFM
AAlwYXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB+AAJ
4cHVyAAJbQqzzF/
gGCFTgAgAAeHAAAAAPMA0ECIr9Z1iG+O3BAgEKdXEAfgAEAAAAuMU/
SoFRkebvh2d5SqalF91ttjRY5lyyW5+/
FifOuDdYikYiDbOJb6607S0dPHjQzeVgu6ptIvGqaEQOEjBjDkY+i4VoVjUSXS3
a8fiXB8moMdPtLJ/
GyE8QiwbT4xbkQy48i02k99F2vGmlenRpSP6dD31kZl3dpJ0mGgq2yL/
eFaynKyqnjkHLMexcqD8WlVooaRl1k2RPk5vDYvC8o2bn22OKKbOnSRM5YlPS0i
Wzxo0JVcnVVyt0AANQQkV0ABBQQkVXaXRoTUQ1QW5kREVT</item>  <item
```

```
name="responder-dn">\PERIN-TAO\novell\Provo\phb</item> <item
name="auth-style sheet">process_template.xsl</item> <item
name="response-style sheet">process_template.xsl</item> <item
name="subject-name">Joe the Intern</item> <item name="url-
base">https://192.168.0.1:8180</item> <item name="url">https://
192.168.0.1:8180</item> </replacement-data>
```

e. 万维网服务器验证 responder-dn 项的值是否与包含在受保护数据中的 responder-dn 值匹配。如果值不匹配，则万维网服务器将中止请求。如果值匹配，则处理继续进行。

f. 万维网服务器将 <check-object-password> XDS 请求提交给发布者通道上的 Identity Manager，以鉴定提交 HTTP POST 请求的用户。

```
<nds dtdversion="1.0" ndsversion="8.6"> <source> <product
build="20020606_0824" instance="Manual Task Service Driver"
version="1.1a">DirXML Manual Task Service Driver</product>
<contact>Novell, Inc.</contact> </source> <input> <check-
object-password dest-dn="\PERIN-TAO\novell\Provo\phb" event-
id="chkpwd"> <password><!-- content suppressed --></password>
</check-object-password> </input> </nds>
```

g. Identity Manager 返回 <status level="success">。如果 Identity Manager 返回不成功的信息，则使用由数据项 auth_template 指定的模板和由数据项 auth_stylesheet 指定的样式表构造作为 POST 结果返回的网页。

h. 万维网服务器使用 process_template.xsl 样式表处理 post_form.xml 模板以生成 XDS 文档。替换令牌为粗体。

```
<nds> <input> <modify class-name="User" src-dn="not-applicable"
event-id=”wfmod”> <association>$association$</association>
<modify-attr attr-name="roomNumber"> <remove-all-values/> <add-
value> <value>$room-number$</value> </add-value> </modify-attr>
</modify> </input> </nds>
```

i. 发布者将创建的 XDS 文档提交给 Identity Manager。

```
<nds> <input> <modify class-name="User" src-dn="not-applicable"
event-id=”wfmod”> <association>45f0e3:ee45e07709:-
7fff:192.168.0.1</association> <modify-attr attr-
name="roomNumber"> <remove-all-values/> <add-value>
<value>cubicle 1234</value> </add-value> </modify-attr> </
modify> </input> </nds>
```

j. Identity Manager 返回结果文档

```
<nds dtdversion="1.1" ndsversion="8.6"> <source> <product
version="2.0">Identity Manager</product> <contact>Novell,
Inc.</contact> </source> <output> <status event-id="wfmod"
level="success"></status> </output> </nds>
```

k. 万维网服务器将替换数据项 post-status （也可能是替换数据项 post-status-message）添加到替换数据文档。添加的数据项为粗体：

```
<replacement-data> <item name="room-number">cubicle 1234</item>
<item name="template">post_form.xml</item> <item
name="response-template">post_response.xml</item> <item
name="auth-template">auth_response.xml</item> <item
name="association">45f0e3:ee45e07709:-7fff:192.168.0.1</item>
<item name="password" is-sensitive=”true”><!-content suppressed
?</item> <item name="protected-
data">rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHACA
ARbAA1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB+AAFM
AAlwYXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB+AAJ
4cHVyAAJbQqzzF/
gGCFTgAgAAeHAAAAAPMA0ECIr9Z1iG+O3BAgEKdXEAfgAEAAAAuMU/
SoFRkebvh2d5SqalF91ttjRY5lyyW5+/
FifOuDdYikYiDbOJb6607S0dPHjQzeVgu6ptIvGqaEQOEjBjDkY+i4VoVjUSXS3
a8fiXB8moMdPtLJ/
GyE8QiwbT4xbkQy48i02k99F2vGmlenRpSP6dD31kZl3dpJ0mGgq2yL/
eFaynKyqnjkHLMexcqD8WlVooaRl1k2RPk5vDYvC8o2bn22OKKbOnSRM5YlPS0i
Wzxo0JVcnVVyt0AANQQkV0ABBQQkVXaXRoTUQ1QW5kREVT</item> <item
name="responder-dn">\PERIN-TAO\novell\Provo\phb</item> <item
name="auth-style sheet">process_template.xsl</item> <item
name="response-style sheet">process_template.xsl</item> <item
name="subject-name">Joe the Intern</item> <item name="url-
base">https://192.168.0.1:8180</item> <item name="url">https://
192.168.0.1:8180</item> <status event-id="" level="success"></
status>   <item name="post-status">success</item> </
replacement-data>
```

l. 万维网服务器使用 process_template.xsl 样式表处理 post_response.xml 模板。替换令牌和操作要素为粗体。

```
<htm xmlns:form="http://www.novell.com/dirxml/manualtask/form">
<head> <title>Result of post for $subject-name$</title> </head>
<body> <link href="novdocmain.css" rel="style sheet"
type="text/css"/> <br/><br/><br/><br/> <table class="formtable"
cellpadding="5" cellspacing="20" border="1" align="center">
<tr> <td> DirXML reported status = $post-status$ </td> </tr>
<form:if-item-exists name="post-status-message"> <tr> <td>
Status message was: $post-status-message$ </td> </tr> </
form:if-item-exists> </table> </body> </html>
```

m. 将生成的网页作为 HTTP POST 结果返回。由于 <form:if-item-exists> 要素引用的 post-status-message 在替换数据文档中不存在，因此表没有第二行。

```
<html> <head> <META http-equiv="Content-Type" content="text/
html; charset=UTF-8"> <title>Result of post for Joe the
Intern</title> </head> <body> <link href="novdocmain.css"
rel="style sheet" type="text/css"> <br><br><br><br> <table
class="formtable" cellpadding="5" cellspacing="20" border="1"
align="center"> <tr> <td> DirXML reported status = success </
```

```
td> </tr> </table> </body> </html>
```

手工任务服务驱动程序：订购者通道的自定义要素处理程序

驱动程序为使用不同于简单邮件传输协议 (SMTP) 方法发送用户通知提供了一套扩展机制。例如，客户可能需要使用讯息交换应用程序编程界面 (MAPI) 而不是使用 SMTP 发送通知。

要使用不同于 SMTP 的机制发送通知，则必须写入 Java 类以处理在驱动程序的订购者通道上提交的自定义 XML 要素。

Java 自定义要素处理程序必须实现 com.novell.nds.dirxml.driver.manualtask.CommandHandler Java 界面。自定义要素类的名称在订购者配置参数的附加处理程序项中指定。

当订购者通道遇到命令要素时，它将在自己的处理程序表中查找。当它查找到自己报告能够处理此命令要素的处理程序后，即将此命令要素传递给该处理程序。处理程序随后执行必需的处理。

驱动程序中有两个内置的命令要素处理程序：<mail> 要素处理程序和 <add> 要素处理程序。

自定义命令要素由自定义处理程序的作者来定义。设计自定义命令要素合理的开始位置是 <mail> 要素的设计。

自定义要素由订购者通道上的策略使用与创建 <mail> 要素相同的方式创建。

可以在与驱动程序一起提供的 javadoc 中找到 com.novell.nds.dirxml.driver.manualtask.CommandHandler 的文档和很多实用程序和支持类的文档。javadoc 位于分发图像中名为 manual_task_docs.zip 的文件中。

I.1 构造用于发布者通道万维网服务器的 URL

要安全地使用驱动程序的发布者通道万维网服务器，必须使用实用程序类以构造要包含在通知邮件中的 URL。com.novell.nds.dirxml.driver.manualtask.URLData 是专为此任务而设计的。

SampleCommandHandler.java 中的示例代码阐释了此过程。

I.2 使用样式表和模板文档构造邮件文档

使用与 SMTP 处理程序所使用的相同方法构造文档很方便，该方法是样式表、模板文档和替换数据的组合。为此，必须获得样式表和模板文档，并有通过编程的方式来调用样式表处理器。

SampleCommandHandler.java 中的示例代码阐释了此过程。

I.3 SampleCommandHandler.java

驱动程序分发中包含示例自定义命令处理程序的源代码。源代码位于分发图像的 manual_task_docs.zip 文件中。

处理程序在 com.novell.nds.dirxml.driver.manualtask.samples.SampleCommandHandler 类中实现。

示例处理程序仅使用样式表和模板生成文档，并将生成的文档写入文件。

I.3.1 编译 SampleCommandHandler 类

可以使用任何 Java 2 编译器编译 SampleCommandHandler 类。必须将 nxsl.jar、 dirxml.jar、collections.jar 和 ManualTaskServiceBase.jar 放置在 Java 编译器类路径中。

I.3.2 尝试 SampleCommandHandler 类

从导入驱动程序的房间号示例配置开始。

编译 SampleCommandHandler 类，并将生成的类文件放入 .jar 文件中。将 .jar 文件放入运行驱动程序的平台的相应 DirXML .jar 文件目录中。

将以下 XML 要素添加到位于驱动程序属性的驱动程序参数 XML 部分中的 <subscriber-options> 要素下：

```
<output-path display-name="Sample Output Path"></output-path>
```

编辑驱动程序参数。在标记为 "Sample Output Path" （示例输出路径）的项中，放置到 SampleCommandHandler 将写入其创建的文档的目录的路径。在标记为 "Additional Handlers" （附加处理程序）的项中，添加字符串 com.novell.nds.dirxml.driver.manualtask.samples.SampleCommandHandler。

将订购者通道命令转换策略替换为与 SampleCommandHandler.java 文件位于同一目录中的 CommandXform.xsl。

创建用户对象，并添加到用户对象的经理参照。如果经理有电子邮件地址值，则将 <sample> 命令要素发送给订购者，同时 SampleCommandHandler 将在上面指定的位置写入文件。

手工任务服务驱动程序：发布者通道的自定义服务器小程序

J

驱动程序提供可用于将附加功能添加到发布者通道万维网服务器的扩展机制。自定义服务器小程序可由发布者加载，方法是在标记为 "Additional Servlets"（附加服务器小程序）的驱动程序配置项中指定 servlet 类的名称。

J.1 使用发布者通道

如果自定义服务器小程序需要向 Identity Manager 提交数据，则服务器小程序必须使用驱动程序的发布者通道。提供了 com.novell.nds.dirxml.driver.manualtask.ServletRegistrar 类和 com.novell.nds.dirxml.driver.manualtask.PublisherData 类以方便此操作。SampleServlet.java 中的示例代码阐释了此过程。

J.2 鉴定

自定义服务器小程序必须鉴定提交信息的用户。SampleServlet.java 中的示例代码阐释了此过程。然而，使用 <check-object-password> 要素执行的鉴定类型不检查 eDirectory™ 权限。如果驱动程序对象具有执行更改的权限，则允许在发布者通道上提交更改，而不管提交更改的用户是否具有权限。

如果正在使用的 URL 是通过订购者通道上的命令处理程序生成的，则必须使用 com.novell.nds.dirxml.driver.manualtask.URLData 类验证 URL，以确保 responder-dn 数据项没有被擅自改动。有关完成此操作的信息，请参见 javadoc。

J.3 SampleServlet.java

驱动程序分发中包含了示例服务器小程序的源代码。源代码位于分发图像的 manualtask_driver_docs.zip 文件中。

服务器小程序在 com.novell.nds.dirxml.driver.manualtask.samples.SampleServlet 类中实现。

示例服务器小程序接受对以 .sample 结尾的任何资源的 HTTP GET 请求。HTTP URL 的查询字符串必须包含 dest-dn 项、 attr-name 项和 value 项。

服务器小程序鉴定用户，然后通过驱动程序的发布者通道将修改请求提交给 Identity Manager。

J.3.1 编译 SampleServlet 类

可以使用任何 Java 2 编译器编译 SampleServlet 类。必须将 nxsl.jar、 dirxml.jar、 collections.jar 和 ManualTaskServiceBase.jar 放置在 Java 编译器类路径中。

J.3.2 尝试 SampleServlet 类

从导入驱动程序的房间号示例配置开始。

编译 SampleServlet 类并将生成的类文件放入 .jar 文件中。将 .jar 文件放入运行驱动程序的平台的相应 DirXML .jar 文件目录中。

编辑驱动程序参数。在标记为 " 附加服务器小程序 " 的项中，添加字符串 com.novell.nds.dirxml.driver.manualtask.samples.SampleServlet。

将电话号码添加到发布者通道过滤器。

在浏览器中提交以下 URL （假设浏览器与驱动程序运行在同一计算机上）：

https:localhost:8180/1.sample?dest-dn=username.container&attr-name=Telephone%20Number&value=555-1212

将 *username.container* 替换为树中用户的 DN。