

Novell Identity Manager Driver for eDirectory™

3.0

www.novell.com

实施指南

2006 年 5 月 8 日



Novell®

法律声明

Novell, Inc. 对本文档的内容或使用不作任何陈述或保证，特别是对适销性或针对任何特定用途的适用性不作任何明示或暗示的保证。另外，Novell, Inc. 保留随时修改本出版物及其内容的权利，并且没有义务将这类修改通知任何个人或实体。

另外，Novell, Inc. 对所有软件不作任何陈述或保证，特别是对适销性或针对任何特定用途的适用性不作任何明示或暗示的保证。同时，Novell, Inc. 保留随时修改 Novell 软件全部或部分内容的权利，并且没有义务将这类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它国家 / 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 软件的更多信息，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 对此不承担任何责任。

Copyright © 2000-2005 Novell, Inc. 版权所有。未经出版商的明确书面许可，不得复制、影印、在检索系统中储存或传送该出版物的任何部分。

Novell, Inc. 对本文档中介绍的产品中所包含的相关技术拥有知识产权。特别是，这些知识产权包括但不限于 <http://www.novell.com/company/legal/patents/> 列出的一项或多项美国专利，以及在美国和其它国家 / 地区的一项或多项其它专利或申请中的专利。

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

联机文档：要访问本产品和其它 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

要查看 Novell 商标的列表，请参见[商标 \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html)。

第三方材料

所有第三方商标是其相应拥有者的财产。

目录

| | |
|--|-----------|
| 关于本指南 | 3 |
| 1 概述 | 5 |
| 1.1 术语变更 | 5 |
| 1.2 主要术语 | 5 |
| 2 安装 Identity Manager Driver for eDirectory | 7 |
| 2.1 驱动程序 Shim 的安装位置 | 7 |
| 2.2 驱动程序前提条件 | 7 |
| 2.3 升级到 Identity Manager 3 | 7 |
| 2.4 安装驱动程序 Shim | 7 |
| 2.4.1 安装到 Windows | 8 |
| 2.4.2 安装到 NetWare | 10 |
| 2.4.3 安装到 Linux、Solaris 或 AIX | 12 |
| 2.5 激活驱动程序 | 14 |
| 3 升级 Identity Manager Driver for eDirectory | 15 |
| 3.1 准备升级 | 15 |
| 3.2 升级驱动程序 Shim | 15 |
| 3.3 升级驱动程序配置 | 16 |
| 3.4 eDirectory 驱动程序的升级问题 | 16 |
| 4 样本驱动程序配置文件 | 17 |
| 4.1 导入样本驱动程序配置 | 17 |
| 4.1.1 使用 iManager 导入 | 17 |
| 4.1.2 使用 Designer for Identity Manager 导入 | 18 |
| 4.2 配置安全 Identity Manager 数据传送 | 19 |
| 4.2.1 了解 eDirectory 驱动程序安全性 | 19 |
| 4.2.2 设置 KMO | 19 |
| 4.3 同步哪些特性 | 20 |
| 4.4 口令同步 | 21 |
| 5 配置驱动程序 | 23 |
| 5.1 配置驱动程序对象属性 | 23 |
| 5.1.1 鉴定参数 | 24 |
| 5.2 配置过滤器 | 25 |
| 5.3 配置发布者通道上的规则 | 26 |
| 5.4 使用驱动程序对象口令 | 26 |
| 5.5 迁移或复制对象 | 27 |
| A 文档更新 | 29 |
| A.1 2006 年 5 月 8 日 | 29 |

关于本指南

本指南介绍了如何安装和配置 Identity Manager Driver for eDirectory

- ◆ 第 1 章 “概述” 在第 5 页
- ◆ 第 2 章 “安装 Identity Manager Driver for eDirectory” 在第 7 页
- ◆ 第 3 章 “升级 Identity Manager Driver for eDirectory” 在第 15 页
- ◆ 第 4 章 “样本驱动程序配置文件” 在第 17 页
- ◆ 第 5 章 “配置驱动程序” 在第 23 页

读者

本指南适用于正在使用 Identity Manager Driver for eDirectory 的 Novell® eDirectory 和 Identity Manager 管理员。

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。使用联机文档中每页底部的《用户意见》功能，或访问 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，请参见 [Novell 文档万维网站点 \(http://www.novell.com/documentation\)](http://www.novell.com/documentation) 上 Identity Manager 驱动程序部分中的 *Identity Manager Driver for eDirectory*。

其它文档

有关 Identity Manager 和其它 Identity Manager 驱动程序的信息，请参见 [Novell 文档万维网站点 \(http://www.novell.com/documentation\)](http://www.novell.com/documentation)。

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 Driver for eDirectory™ 可同步不同 eDirectory 树之间的对象和特性。

此驱动程序不同于所有其它 Identity Manager 驱动程序。由于要在 eDirectory 树之间同步数据，因此始终要安装两个驱动程序，每棵树中各安装一个。一棵树中的驱动程序可与另一棵树中的驱动程序进行通讯。

例如，A 树中的发布者通道与 B 树中的订购者通道进行通讯；反之，B 树中的发布者通道与 A 树中的订购者通道进行通讯。因此，必须进行两次驱动程序的安装和配置：一次是为 A 树中的 eDirectory 驱动程序，一次是为 B 树中的驱动程序。

有关 Identity Manager 中的新功能的信息，请参见《*Identity Manager 3.0 安装指南*》中的《*Identity Manager 3 中有哪些新功能?*》。

1.1 术语变更

下列术语与早期版本中的术语有所不同：

表 1-1 术语变更

| 早期版本中的术语 | 新术语 |
|------------|---------------------------------------|
| DirXML® | Identity Manager |
| DirXML 服务器 | Metadirectory 服务器 |
| DirXML 引擎 | Metadirectory 引擎 |
| eDirectory | Identity Vault（当指 eDirectory 特性或类时除外） |

1.2 主要术语

驱动程序 Shim。由 Identity Manager 直接装载的 Java 文件 (NdsToNds.jar)。将要发送的事件更改从 Identity Manager Driver for eDirectory 传送到 Identity Vault、将更改从 Identity Vault 传送到 Identity Manager Driver for eDirectory，并可作为连接 Identity Vault 和 Identity Vault Driver 对象的链接运行。

驱动程序。一组策略、过滤器和对象，可充当 Identity Vault 和驱动程序 Shim 之间的连接器。

应用程序可以使用该软件将事件从应用程序发布到目录，从目录订购事件，还可以在目录与应用程序之间同步数据。

要在 Metadirectory 引擎与 Identity Vault 之间建立连接，需要指定驱动程序的配置和连接参数、策略以及过滤器值。

驱动程序对象。通道、策略、规则和过滤器的集合，用于将应用程序连接到运行 Identity Manager 的 Identity Vault。

每个驱动程序执行不同的任务。策略、规则和过滤器会指示驱动程序如何处理数据以执行这些任务。

驱动程序对象显示有关驱动程序的配置、策略和过滤器的信息。可以使用该对象管理驱动程序并提供对驱动程序 Shim 参数的 eDirectory 管理。

Identity Vault。应用程序和目录向其发布更改的中心。然后，Identity Vault 向订购更改的应用程序和目录发送这些更改。这一过程产生两个主要的数据流：发布者通道和订购者通道。

安装 Identity Manager Driver for eDirectory

2

- ◆ “驱动程序 Shim 的安装位置” 在第 7 页
- ◆ “驱动程序前提条件” 在第 7 页
- ◆ “升级到 Identity Manager 3” 在第 7 页
- ◆ “安装驱动程序 Shim” 在第 7 页
- ◆ “激活驱动程序” 在第 14 页

2.1 驱动程序 Shim 的安装位置

需要在两台 Novell® eDirectory 服务器上以及要同步的树中安装 Identity Manager 和 eDirectory™ 驱动程序 Shim。由于某一树中的驱动程序与另一树中的驱动程序直接通讯，因此该驱动程序不使用《远程装载程序》技术。

此驱动程序使用 Novell Certificate Server™ 和证书授权者 (CA) 来确保数据安全。各树之间的所有事务均通过 SSL 技术来确保安全。有关数据安全的信息，请参见“配置安全 Identity Manager 数据传送” 在第 19 页。

2.2 驱动程序前提条件

- ❑ Identity Manager 的要求。请参见《Identity Manager 3.0 安装指南》。
- ❑ 在每台服务器上运行的、承载 eDirectory 驱动程序的 Novell Certificate Server。
- ❑ 证书授权者 (CA)，以便 SSL 加密能够运行。

2.3 升级到 Identity Manager 3

在安装 Identity Manager 期间，可以同时安装 Metadirectory 引擎和 Driver for eDirectory（及其它 Identity Manager 驱动程序）。请参见《Identity Manager 3.0 安装指南》。可以从 DirXML 1.1a 或 Identity Manager 2 升级到 Identity Manager 3。

2.4 安装驱动程序 Shim

可以在安装 Metadirectory 引擎的同时，安装 Identity Manager eDirectory 驱动程序 Shim（及其它 Identity Manager 驱动程序）。

也可以在安装 Metadirectory 引擎后，单独安装此驱动程序。本节假定您已在服务器上安装了 Metadirectory 引擎（很可能还安装了其它驱动程序），且只需要安装 eDirectory 驱动程序。

如果您没有 CD，请下载您的平台所需的文件（例如 Identity_Manager_3_Linux_NW_Win.iso），并创建一张 CD。可从 [Novell Downloads \(http://download.novell.com/index.jsp\)](http://download.novell.com/index.jsp) 下载。

重要：由于需要在两台单独的 Identity Vault (eDirectory) 服务器上安装此驱动程序，因此必须对每台服务器完成相应的过程。

在安装期间，将 NdsToNds.jar 复制到相应的目录。下表显示了每个平台上的这些位置：

| 操作系统 | 目录 |
|------------------------|--|
| Linux*、Solaris* 或 AIX* | /usr/lib/dirxml/classes（对于 eDirectory 8.8: opt/novell/eDirectory/lib/dirxml/classes） |
| NetWare® | sys:system\lib |
| Windows* NT*/2000 | 默认位置是 novell\nds，但您可以指定任何目录。 |

在程序安装结束后，请按照“配置安全 Identity Manager 数据传送”在第 19 页中的说明来配置安全性。

2.4.1 安装到 Windows

- 1 从 Identity Manager 3.0 CD 运行安装程序。

如果安装程序没有自动启动，可以运行 \nt\install.exe。

- 2 在《欢迎使用》对话框中，单击《下一步》，然后接受许可协议。
- 3 在第一个《Identity Manager 概述》对话框中，查看概述信息，然后单击《下一步》。此对话框提供有关以下两项的信息：

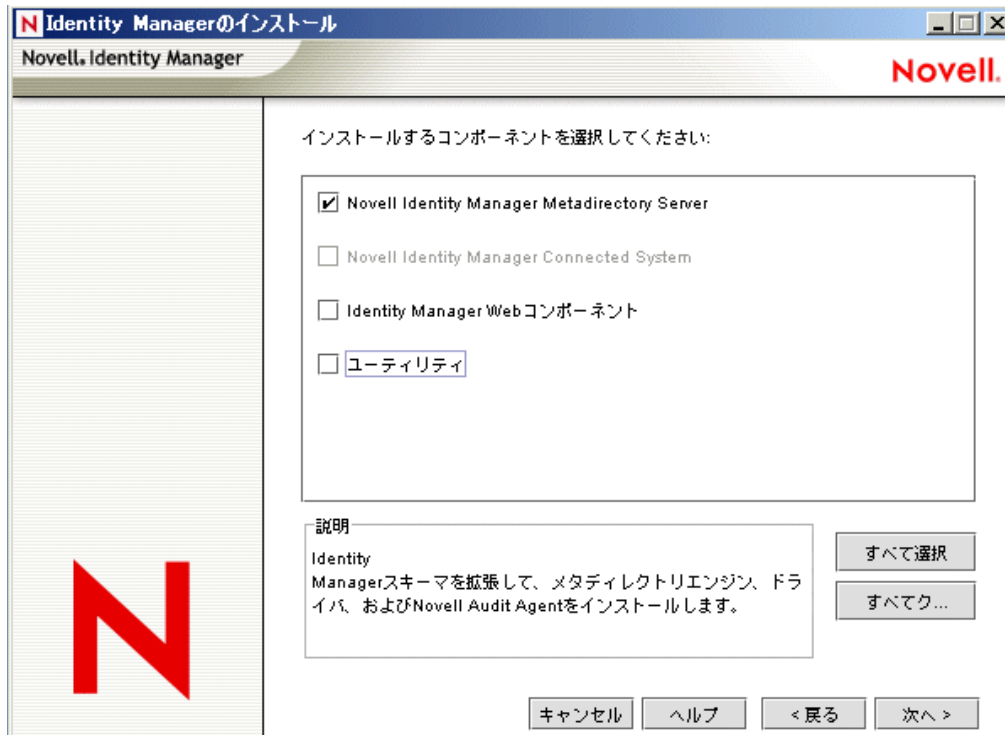
- ◆ Metadirectory 服务器
- ◆ 已连接的服务器系统

- 4 在第二个《Identity Manager 概述》对话框中，查看其中的信息，然后单击《下一步》。

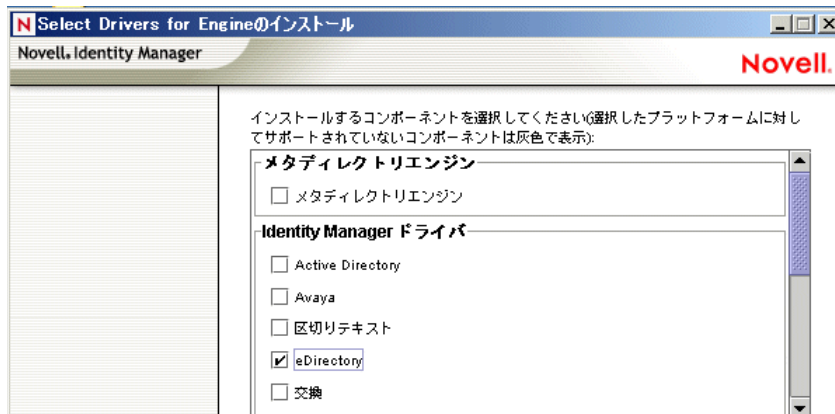
此对话框提供有关以下两项的信息：

- ◆ 基于万维网的管理服务器
- ◆ Identity Manager 实用程序

- 5 在《请选择要安装的部件》对话框中，仅选择 *Metadirectory Server*（Metadirectory 服务器），然后单击《下一步》。



- 6 在《选择要安装的引擎驱动程序》对话框中，仅选择 *eDirectory*，然后单击《下一步》。

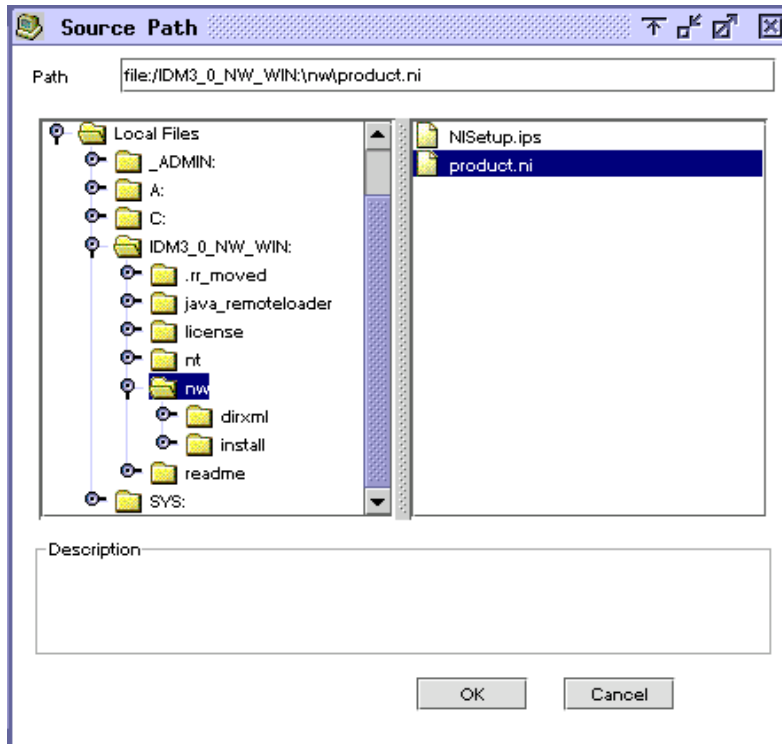


- 7 在《Identity Manager 升级警告》对话框中，单击《确定》。
8 在《摘要》对话框中，查看选定的选项，然后单击《完成》。
9 在《安装完毕》对话框，单击《关闭》。

安装后，请按照“配置驱动程序”在第 23 页中的说明来配置此驱动程序。

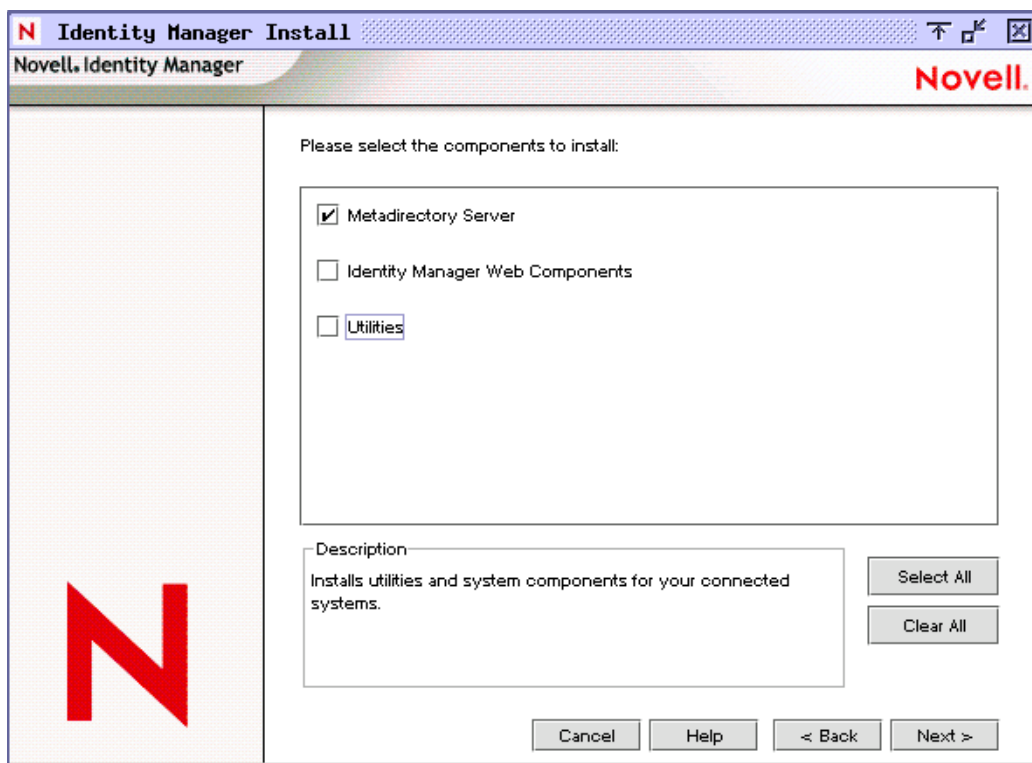
2.4.2 安装到 NetWare

- 1 在 NetWare 服务器上，插入 Identity Manager CD 并将其作为卷装入。
要装入此 CD，请输入 `m cdrom`。
- 2 （视情况而定）如果图形实用程序未装载，请输入 `startx` 来装载它。
- 3 在图形实用程序中，单击 *Novell* 图标，然后单击 《安装》。
- 4 在 《安装的产品》对话框中，单击 《添加》。
- 5 在 《源路径》对话框中，浏览并选择 `product.ni` 文件。



- 5a 浏览并展开先前装入的 CD 卷 (`Identity_Manager_3_Linux_NW_WIN`)。
- 5b 展开 `nw` 目录，选择 `product.ni`，然后单击 《确定》两次。
- 6 在 《欢迎使用 Novell Identity Manager 3.0 安装程序》对话框中，单击 《下一步》，然后接受许可协议。

7 在《Identity Manager 安装》对话框中，仅选择《Metadirectory 服务器》。

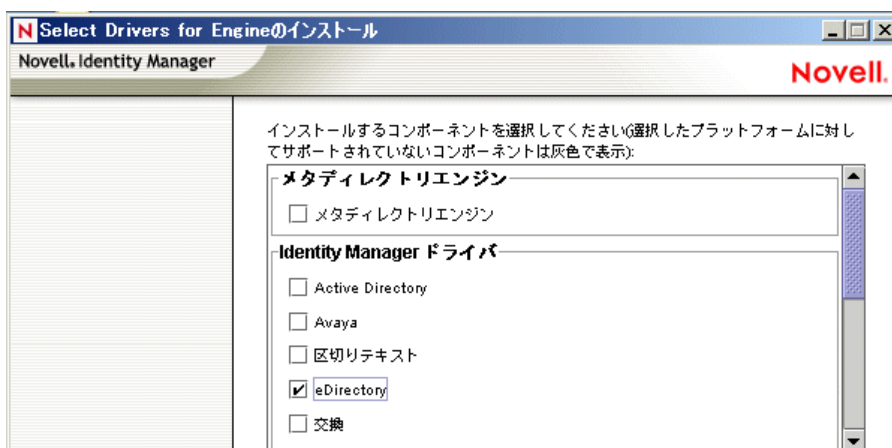


取消选择以下项：

- ◆ Identity Manager 万维网部件
- ◆ 实用程序

8 单击《下一步》。

9 在《选择要安装的引擎驱动程序》对话框中，仅选择 *eDirectory*。



取消选择以下项：

- ◆ *Metadirectory* 引擎
- ◆ 除 *eDirectory* 之外的所有驱动程序

10 在《Identity Manager 升级警告》对话框中，单击《确定》。

此对话框将建议您在 90 天内激活驱动程序的许可证。

11 在《摘要》页中，查看选定的选项，然后单击《完成》。

12 单击《关闭》。

安装后，请按照“配置驱动程序”在第 23 页中的说明来配置此驱动程序。

2.4.3 安装到 Linux、Solaris 或 AIX

默认情况下，在安装 Metadirectory 引擎的同时会安装 Identity Manager Driver for eDirectory。如果未同时安装此驱动程序，本节中的步骤将帮助您安装它。

当您执行安装程序中的步骤时，可以通过输入 previous 来返回到上一部分（屏幕）。

1 在终端会话中，以根用户的身份登录。

2 插入 Identity Manager CD 并装入它。

通常，此 CD 将自动装入。下表列出了手动装入 CD 的示例。您输入的实际命令取决于系统的配置方式和操作系统：

| 平台 | 键入的内容 |
|-----------------|--|
| AIX* 或 Red Hat* | mount /mnt/cdrom, 然后按 Enter 键 |
| Solaris | mount /cdrom, 然后按 Enter 键 |
| SUSE® | mount /media/cdrom, 然后按 Enter 键; 或 mount /media/dvd, 然后按 Enter 键 |

3 更改到安装目录。

例如，更改到 *mount point/platform/setup*

- ◆ *mount point* 是装入 CD/DVD 的位置。
- ◆ *platform* 是平台的名称（solaris、linux 或 aix）。

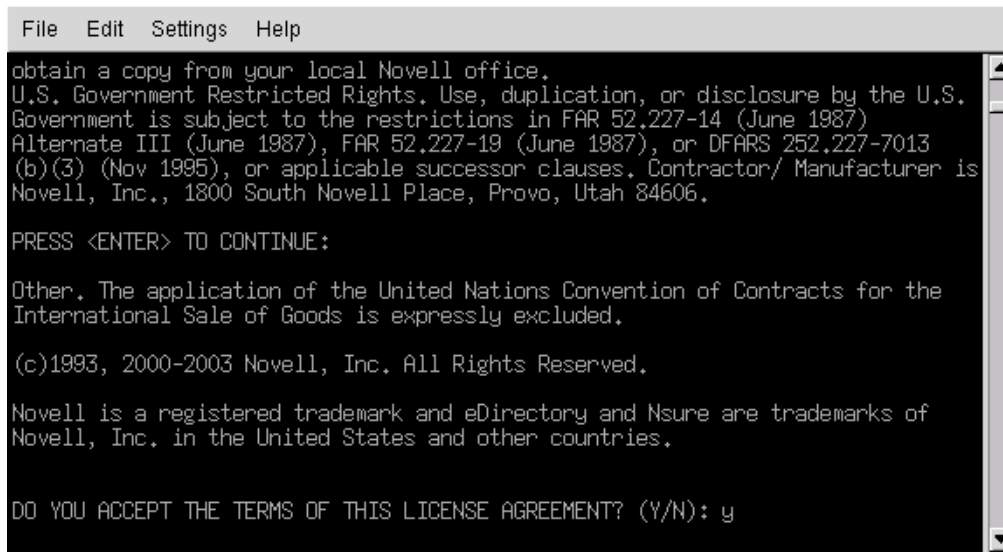
4 运行安装程序。

例如，对于 Linux 键入 *./dirxml_linux.bin*。

5 在《介绍》部分中，按 Enter 键。

6 接受许可协议。

按 Enter 键，直到看到 *DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT*（是否接受该许可协议中的条款），键入 y，然后按 Enter 键。



```
File Edit Settings Help
obtain a copy from your local Novell office.
U.S. Government Restricted Rights. Use, duplication, or disclosure by the U.S.
Government is subject to the restrictions in FAR 52.227-14 (June 1987)
Alternate III (June 1987), FAR 52.227-19 (June 1987), or DFARS 252.227-7013
(b)(3) (Nov 1995), or applicable successor clauses. Contractor/ Manufacturer is
Novell, Inc., 1800 South Novell Place, Provo, Utah 84606.

PRESS <ENTER> TO CONTINUE:

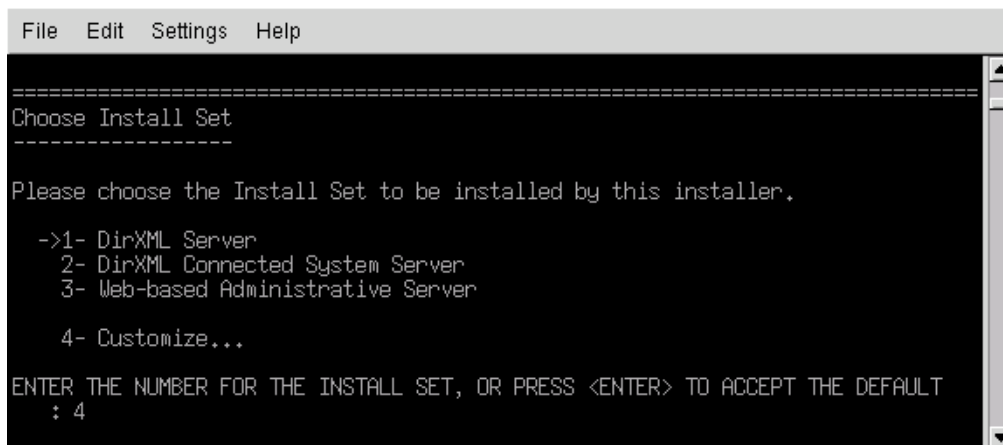
Other. The application of the United Nations Convention of Contracts for the
International Sale of Goods is expressly excluded.

(c)1993, 2000-2003 Novell, Inc. All Rights Reserved.

Novell is a registered trademark and eDirectory and Nsure are trademarks of
Novell, Inc. in the United States and other countries.

DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT? (Y/N): y
```

7 在 *Choose Install Set*（选择安装集）部分中，选择《自定义》选项。
键入 4，然后按 Enter 键。



```
File Edit Settings Help
=====
Choose Install Set
-----

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

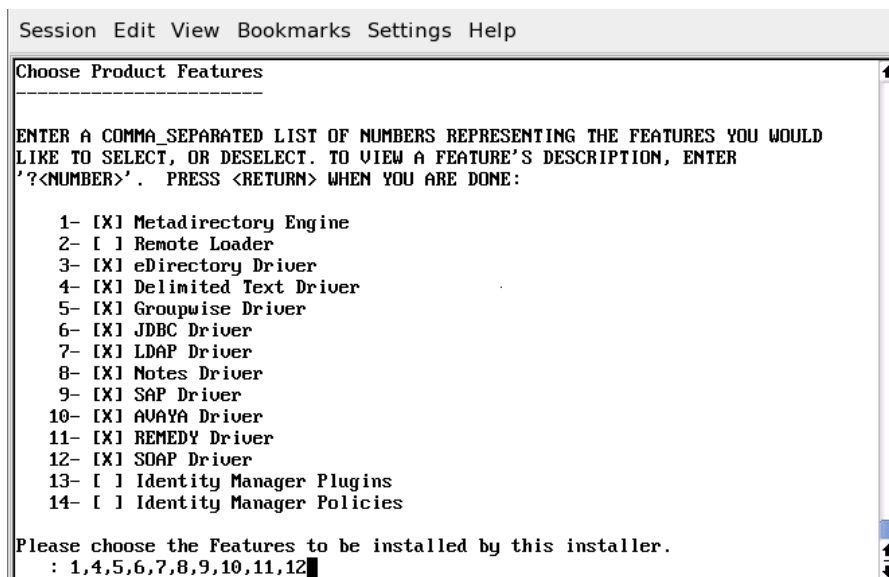
->1- DirXML Server
  2- DirXML Connected System Server
  3- Web-based Administrative Server

  4- Customize...

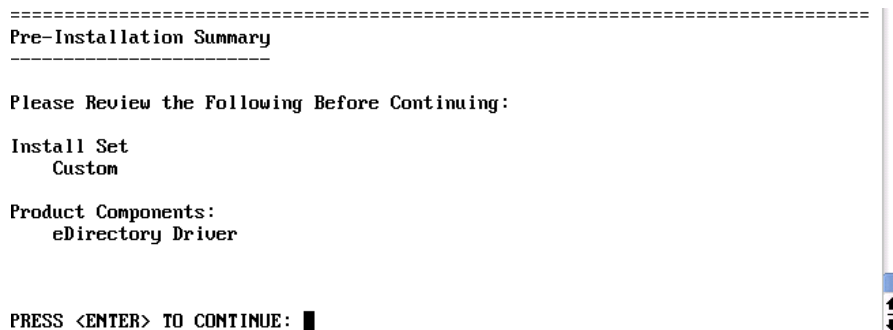
ENTER THE NUMBER FOR THE INSTALL SET, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
: 4
```

8 在 *Choose Product Features*（选择产品功能）部分中，取消选择除 *eDirectory* 之外的所有功能，然后按 Enter 键。

要取消选择某一功能，请键入其编号。在要取消选择的其它功能之间键入逗号。



9 在 *Pre-Installation Summary*（预安装摘要）部分中，查看其中选项。



要返回到上一部分，键入 `previous`，然后按 `Enter` 键。

要继续，请按 `Enter` 键。

10 在安装完成后，按 `Enter` 键退出安装。

安装后，请按照“配置驱动程序”在第 23 页中的说明来配置此驱动程序。

2.5 激活驱动程序

在安装后的 90 天内激活驱动程序。否则，此驱动程序将停止运行。

有关激活的信息，请参考《*Identity Manager 3.0 安装指南*》中的《*激活 Novell Identity Manager 产品*》。

升级 Identity Manager Driver for eDirectory

3

- “准备升级” 在第 15 页
- “升级驱动程序 Shim” 在第 15 页
- “升级驱动程序配置” 在第 16 页
- “eDirectory 驱动程序的升级问题” 在第 16 页

3.1 准备升级

确保您已查看了针对所用驱动程序版本的所有 TID 和产品更新。

新的驱动程序 Shim 旨在与现有驱动程序配置一起使用（无需任何更改），并假定驱动程序 Shim 和配置包含最新的修复功能。

3.2 升级驱动程序 Shim

- 1 确保已经用当前运行版本的所有增补程序更新了驱动程序。

为最大程度地减少升级问题，建议您对所有驱动程序执行此步骤。

- 2 安装新驱动程序 Shim。

可以在安装 Metadirectory 引擎的同时，或者在安装该引擎后执行此操作。请参见“[安装驱动程序 Shim](#)” 在第 7 页。

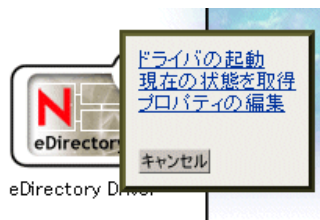
升级时，新的驱动程序 Shim 将取代以前的驱动程序 Shim，但保留以前驱动程序的配置。

- 3 安装 Shim 后，请重新启动驱动程序。

3a 在 iManager 中，选择 *Identity Manager* > 《Identity Manager 概述》。

3b 浏览至驱动程序所在的驱动程序集。

3c 选择要重新启动的驱动程序，单击状态图标，然后选择《启动驱动程序》。



- 4（视情况而定）使用 Identity Manager 激活身份凭证激活驱动程序 Shim。

每个驱动程序集只需激活一次，而不是每个驱动程序激活一次。您很可能已经激活了驱动程序集，那么可以跳过该步骤。

有关激活的信息，请参见《[Identity Manager 3.0 安装指南](#)》中的《[激活 Novell Identity Manager 产品](#)》。

安装驱动程序 Shim 后，请升级驱动程序配置。请参见“升级驱动程序配置”在第 16 页。

3.3 升级驱动程序配置

重要：本节仅适用于从 DirXML® 1.x 升级。

由于需要在两台单独的 Identity Vault 服务器上升级驱动程序，因此必须对每台服务器完成升级过程。

安装驱动程序 Shim 不会改变现有配置。现有配置将继续用于新驱动程序 Shim。

但是，要利用新功能，则必须升级驱动程序配置，方法是：使用新的样本配置替换驱动程序配置，或者将现有配置转换为 Identity Manager 3 格式并向其中添加策略。

- ◆ 要替换现有配置，请为现有驱动程序对象导入新的样本配置。

样本配置包含所有较新的功能，如支持 Identity Manager 口令同步和基于职能的权利。

- ◆ 要转换现有驱动程序配置，以使用新的 Identity Manager 插件对其进行编辑，请参见《Novell Identity Manager 3.0 管理指南》中的《将驱动程序配置从 DirXML 1.1a 升级到 Identity Manager 格式》。

- ◆ 要向现有驱动程序配置中添加《Identity Manager 口令同步》功能，请参见《Novell Identity Manager 3.0 管理指南》中的《升级现有驱动程序配置以支持口令同步》。

用于口令同步的新策略可支持通用口令和分发口令。如果打算只同步 NDS® 口令，则不应将这些策略添加到驱动程序配置中。同步 NDS 口令时，需要使用公共密钥和私用密钥特性，而不使用这些策略。

3.4 eDirectory 驱动程序的升级问题

重要：本节仅适用于从 DirXML 1.x 升级。

如果要升级 Identity Manager 和 eDirectory 驱动程序，而您的证书均已失效（或两个证书中的一个已失效），则可能会遇到数据同步错误。

如果在具有有效证书的服务器上创建了一个用户，则该用户不会与包含无效证书的服务器同步。同时，可能还会在 DStTrace 中看到以下错误：

```
SSL handshake failed, X509_V_CERT_HAS_EXPIRED
```

```
SSL handshake failed, SSL_ERROR_ZERO_RETURN,
```

如果在证书已失效的服务器上创建了一个用户，则该用户仍会与包含有效证书的服务器同步。同时，可能还会在 DStTrace 中看到以下错误：

```
Error: 14094415: SSL Routines: SSL_READ_BYTES: sslv3 alert certificate expired.
```

要解决此问题，请创建新的证书。

样本驱动程序配置文件

- ◆ “导入样本驱动程序配置” 在第 17 页
- ◆ “配置安全 Identity Manager 数据传送” 在第 19 页
- ◆ “同步哪些特性” 在第 20 页
- ◆ “口令同步” 在第 21 页

4.1 导入样本驱动程序配置

- ◆ “使用 iManager 导入” 在第 17 页
- ◆ “使用 Designer for Identity Manager 导入” 在第 18 页

4.1.1 使用 iManager 导入

1 创建新的驱动程序或将配置 eDirectory.xml 导入现有驱动程序。

在 Novell iManager 中，选择 Identity Manager 实用程序，然后按照 《Novell Identity Manager 3.0 管理指南》中《管理 Identity Manager 驱动程序》中的说明使用某个任务。

2 请按照 “配置安全 Identity Manager 数据传送” 在第 19 页 中的说明配置驱动程序。

向导会提示您提供以下信息：

| 项目 | 说明 |
|--|---|
| Remote Tree Address and Port (远程树地址和端口) | 指定远程树中 Identity Manager 服务器的 DNS 主机名或 IP 地址和端口。例如： 151.155.144.23:8196 主机名：8196 |
| Configure Data Flow (配置数据流) | 双向： 两棵 eDirectory™ 树都是在它们之间同步的数据的授权源。 授权： 本地树是授权源。 从属： 本地树不是授权源。 |

| 项目 | 说明 |
|--------------------------------|--|
| 配置选项 | <p>镜像: 在本地树和远程树之间分级同步对象。</p> <p>如果选择此选项, 请使用相同的选项配置要同步的两棵 eDirectory 树。</p> <p>驱动程序配置中的此选项可同步用户、组、组织、国家 / 地区和组织单元对象。它还镜像另一棵树中子树的结构。</p> <p>平面: 将所有用户和组同步到特定树枝中。</p> <p>此选项同步用户和组对象, 并将所有用户放在一个树枝中, 将所有组放在另一个树枝中。</p> <p>此选项通常与其它树中的《部门》选项 (或类似配置) 结合使用。</p> <p>此选项不会创建包含用户和组的树枝, 必须手动创建这些树枝。</p> <p>部门: 按部门 (OU) 同步用户和组。</p> <p>此选项同步用户和组对象, 并基于管理控制台中的《部门》字段将所有用户和组放在一个树枝中。</p> <p>此配置通常与另一棵树中的《平面》选项 (或类似配置) 结合使用。</p> <p>此选项不会为每个部门创建树枝, 必须手动创建它们。这些树枝必须与导入过程中指定的树枝相同。</p> |
| Remote Base Container (远程基本树枝) | <p>只用于《镜像》选项。</p> <p>在远程树中为同步指定基本树枝, 例如 Users.MyOrganization。</p> |
| Base Container (基本树枝) | <p>用于《镜像》、《平面》和《部门》选项。</p> <p>在本地树中为同步指定基本树枝, 例如 Users.MyOrganization。</p> <p>如果用于《镜像》: 镜像上述《远程基本树枝》的本地基本树枝。</p> <p>如果用于《平面》: 放置用户的树枝。</p> <p>如果用于《部门》: 部门树枝的父树枝。</p> |
| 组树枝 | <p>只用于《平面》。</p> <p>在本地树中为同步指定放置组的基本树枝, 例如, Groups.MyOrganization。</p> |

4.1.2 使用 Designer for Identity Manager 导入

可以使用 Designer for Identity Manager 导入 eDirectory 驱动程序的基本驱动程序配置文件。此基本文件可创建和配置驱动程序正常运行所需的对象和策略。

下面的过程介绍了导入样本配置文件的多种方法之一:

- 1 在 Designer 中打开一个项目。
- 2 在建模器中, 右键单击《驱动程序集》对象, 然后选择 *Add Connected Application* (添加连接的应用程序)。
- 3 从下拉列表中选择 *eDirectory.xml*, 然后单击《运行》。
- 4 在 Perform Prompt Validation (执行提示验证) 窗口中, 单击《是》。
- 5 填写各个字段以配置驱动程序。

指定特定于所在环境的信息。有关这些设置的信息，请参见 [步骤 2 在第 17 页](#) 中的表。

6 指定参数后，单击《确定》以导入驱动程序。

7 自定义并测试驱动程序。

8 将驱动程序部署到 Identity Vault 中。

请参见 [《Designer for Identity Manager 3: 管理指南》](#) 中的 [《将项目部署到 Identity Vault 中》](#)。

4.2 配置安全 Identity Manager 数据传送

可以通过 SSL 来确保所有 eDirectory 驱动程序通信的安全。要配置您的 eDirectory 系统以便安全传送 Identity Manager 数据，请运行 Novell iManager 中的 NDS2NDS 向导。

- ◆ [“了解 eDirectory 驱动程序安全性” 在第 19 页](#)
- ◆ [“设置 KMO” 在第 19 页](#)

4.2.1 了解 eDirectory 驱动程序安全性

下列各项可帮助您了解 eDirectory 驱动程序安全性：

- ◆ 此驱动程序使用 SSL 套接字提供鉴定和安全连接。SSL 使用数字证书，从而使 SSL 连接中的各方可以相互鉴定。Identity Manager 也可以使用 Novell Certificate Server 证书对敏感数据进行安全管理。
- ◆ 要使用此驱动程序，每棵树都必须运行 Novell Certificate Server。建议您使用包含驱动程序的某棵树中的证书授权者，以颁发用于 SSL 的证书。如果您的树没有证书授权者，则需要创建一个。可以使用外部证书授权者。
- ◆ 驱动程序使用的 SSL 的 Novell 实施基于 eDirectory 8.7.x 的 eDirectory 和 NTLS 的 Novell 安全鉴定服务 (SAS)。必须在运行驱动程序的服务器上安装和配置它们。eDirectory 通常会自动完成此操作。
- ◆ 要配置驱动程序安全性，需要创建和参考要使用驱动程序进行连接的 eDirectory 树中的证书。eDirectory 中的证书对象称为《密钥材料对象》(KMO)，因为这些对象可以安全地保存证书数据（包括公共密钥）以及与证书相关联的私用密钥。

必须至少创建两个 KMO（每棵树一个 KMO），以便用于 Identity Manager Driver for eDirectory。本节说明每棵树使用一个 KMO 的情况。

NDS2NDS 驱动程序证书向导可设置 KMO。

- ◆ 有关详细信息，请参见：
 - ◆ 有关 Novell Certificate Server 的概述，请参见 [Novell Certificate Server 联机文档 \(http://www.novell.com/documentation/crtsrv20/index.html\)](http://www.novell.com/documentation/crtsrv20/index.html)。
 - ◆ 有关 CA 的更多信息，特别是有关设置树中证书授权者的信息，请参见 [设置 Novell PKI 服务 \(http://www.novell.com/documentation/lg/ndsse/ndsseenu/data/h6172k4q.html\)](http://www.novell.com/documentation/lg/ndsse/ndsseenu/data/h6172k4q.html)。

4.2.2 设置 KMO

配置 Identity Vault 系统以便安全传送 Identity Manager 数据：

- 1 找到目标服务器的树名或 IP 地址。

2 启动 iManager 并鉴定到第一棵树。

3 单击《Identity Manager 实用程序》>《NDS2NDS 驱动程序证书》。

4 在《欢迎使用》页上，输入第一棵树请求的信息。

启动 iManager 时，会使用所鉴定树中的对象提供默认值。您必须输入或确认下列信息：

- ◆ 驱动程序 DN：键入 eDirectory 驱动程序的判别名（例如，EDir-Workforce.Employee Provisioning.Services.YourOrgName）。
- ◆ 树名：指定 Workforce 树的 IP 地址。
- ◆ 具有 Admin 特权的帐户的用户名（例如，Admin）。
- ◆ 该用户的口令。
- ◆ 用户的环境（例如，Services.YourOrgName）。

5 单击《下一步》。

向导使用您输入的信息来鉴定到第一棵树，校验驱动程序 DN，并校验驱动程序是否与服务器关联。

6 指定第二棵树请求的信息。

在《欢迎使用》页上，输入第一棵树请求的信息。

指定或确认下列信息：

- ◆ 驱动程序 DN：键入 eDirectory 驱动程序的判别名（例如，EDir-Account.DriverSet.YourOrgName）。
- ◆ 树名：键入 Account 树的树名或 IP 地址。
- ◆ 具有 Admin 特权的帐户的用户名（例如，Admin）。
- ◆ 该用户的口令。
- ◆ 用户的环境（例如，London.YourOrgName）。

7 单击《下一步》。

向导使用您输入的信息来鉴定到第二棵树，校验驱动程序 DN，并校验驱动程序是否与服务器关联。

8 查看《摘要》页上的信息，然后单击《完成》。

如果这些树中已包含 KMO，则向导会删除它们然后执行下列操作：

- ◆ 导出第一棵树中 CA 的可信根。
- ◆ 创建 KMO 对象。
- ◆ 发出证书签名请求。
- ◆ 将证书的密钥对名称放到驱动程序的《鉴定 ID》中。

4.3 同步哪些特性

样本驱动程序配置的过滤器可以同步下列特性：

| | | |
|------------------|-------------------------|-------------------------|
| accessCardNumber | Initials | preferredDeliveryMethod |
| ACL | instantMessagingID | preferredName |
| assistant | internationalISDNNumber | Private Key |

| | | |
|----------------------------|-------------------------------|---------------------------|
| assistantPhone | Internet EMail Address | Public Key |
| businessCategory | jackNumber | registeredAddress |
| city | jobCode | roomNumber |
| CN | L | S |
| co | Language | SA |
| company | Mailbox ID | Security Equals |
| costCenter | Mailbox Location | Security Flags |
| costCenterDescription | mailstop | See Also |
| departmentNumber | manager | siteLocation |
| Description | managerWorkforceID | Surname |
| destinationIndicator | mobile | Telephone Number |
| directReports | NSCP:employeeNumber | teletexTerminalIdentifier |
| EMail Address | otherPhoneNumber | telexNumber |
| employeeStatus | O | Timezone |
| employeeType | OU | Title |
| Equivalent To Me | pager | tollFreePhoneNumber |
| Facsimile Telephone Number | personalTitle | UID |
| Full Name | photo | uniqueID |
| Generational Qualifier | Physical Delivery Office Name | vehicleInformation |
| Given Name | Postal Address | workforceID |
| Group Membership | Postal Code | x121Address |
| Higher Privileges | Postal Office Box | x500UniqueIdentifier |

4.4 口令同步

本节包含 Identity Manager Driver for eDirectory 的特定信息，并假定您熟悉 《Novell Identity Manager 3.0 管理指南》的《实施口令同步》中的信息。

- ◆ 驱动程序 Shim 的工作方式与早期版本相同。在 Identity Manager 2.0 中，会在样本驱动程序配置中添加新的策略以支持 Identity Manager 口令同步，包括同步通用口令。
- ◆ 如果决定在多棵树中执行口令策略，请确保口令策略中的《高级口令规则》在每棵树中均兼容，以便成功进行口令同步。

如果在多棵 eDirectory 树中执行了不兼容的口令策略，并且选择如果口令不相符则重新设置（使用选项 *If password does not comply, enforce Password Policy on the connected system by resetting user's password to the Distribution Password*（如果口令不相符，则将用户口令重置为分发口令以在连接系统上强制口令策略）），则可能会遇到循环，在此循环中每个 Identity Vault 服务器均尝试更改不相符的口令。

关于口令策略的信息，请参见 《《口令管理》管理指南》(http://www.novell.com/documentation/password_management/index.html) 中的《使用口令策略管理口令》。

- ◆ 如果驱动程序的过滤器具有用于公共密钥和私用密钥特性的《同步》设置，则 NDS® 口令会在树之间同步，而不考虑已创建的其它任何设置。

如果要使用通用口令来同步口令，请确保已针对要同步通用口令的所有类的公共密钥和私用密钥特性，将 eDirectory 驱动程序的过滤器设置为《忽略》。

- ◆ 要向现有驱动程序配置中添加《Identity Manager 口令同步》功能，请参见《*Novell Identity Manager 3.0 管理指南*》中的《*升级现有驱动程序配置以支持口令同步*》。

用于口令同步的新策略可支持通用口令和分发口令。如果打算只同步 NDS 口令，则不应将这些策略添加到驱动程序配置中。同步 NDS 口令时，需要使用公共密钥和私用密钥特性，而不使用这些策略。

- ◆ 如果口令策略启用了通用口令，并且没有用于同步通用口令和 NDS 口令的选定设置，则不能对已连接系统执行 iManager 中的《检查口令状态》任务。

执行《检查口令状态》任务，可以查看 Identity Manager 中的用户口令是否与已连接系统上的口令同步。

如果您正在使用 Identity Manager Driver for eDirectory，并且某个用户的口令策略在《配置选项》选项卡中指定通用口令更新时不更新 NDS 口令，则该用户的《检查口令状态》任务将始终显示口令未同步。即使事实上已连接系统上的 Identity Manager 分发口令和通用口令相同，口令状态仍会显示为没有同步。

这是由于 Identity Vault 检查口令功能此时正在检查 NDS 口令，而没有通过 NMAST™ 参考通用口令。

默认情况下，口令策略中更新通用口令时，NDS 口令也会更新。如果选择此选项，则对于已连接系统来说，《检查口令状态》应该是准确的。

- ◆ 要使用驱动程序，每台承载驱动程序的服务器必须运行 Novell® Certificate Server。同时，还必须创建证书授权者 (CA) 以便 SSL 加密能够工作。建议由包含驱动程序的某棵树的证书授权者颁发用于 SSL 的证书。如果您的树没有证书授权者，请创建一个。可以使用外部证书授权者。

有关创建 CA 和配置证书服务器的说明，请参考“*配置安全 Identity Manager 数据传送*”在第 19 页。

配置驱动程序

- ◆ “配置驱动程序对象属性” 在第 23 页
- ◆ “配置过滤器” 在第 25 页
- ◆ “配置发布者通道上的规则” 在第 26 页
- ◆ “使用驱动程序对象口令” 在第 26 页

有关口令同步的信息，请参见 “口令同步” 在第 21 页。

5.1 配置驱动程序对象属性

通常，在导入驱动程序配置文件和运行证书向导时会自动配置驱动程序的属性。

手动配置属性：

- 1 在 iManager 中，单击 *Identity Manager* > 《Identity Manager 概述》。
- 2 找到包含 eDirectory™ 驱动程序的驱动程序集，然后单击驱动程序的图标。
- 3 在《Identity Manager 驱动程序概述》页中，单击 eDirectory 驱动程序对象（该对象显示在驱动程序配置中）。
- 4 找到《驱动程序模块》部分，然后选择 *Java*。

ドライバモジュール

- java
- ネイティブ
- リモートローダに接続

名前:

- 5 在《名称》编辑框中，键入下列 eDirectory 驱动程序 Java 类名称：

```
com.novell.nds.dirxml.driver.nds.DriverShimImpl
```

- 6 设置参数。

5.1.1 鉴定参数

認証

us-linux-srv.novell

認証ID:

認証コンテキスト:

リモートローダ接続パラメータ:

ドライブのキャッシュ上限(KB単位):

アプリケーションパスワード: [パスワードの設定](#)

リモートローダパスワード: [リモートローダで](#)

アプリケーションパスワード

パスワードの入力:

パスワードの再入力:

OK キャンセル

起動オプション

us-linux-srv.novell

自動スタート

手動

使用不可

提供允许源服务器与目标服务器通讯的信息。

鉴定 ID

如果希望源服务器和目标服务器交换安全信息（例如口令），请运行 NDS2NDS eDirectory 证书向导。本向导会创建《密钥材料对象》(KMO)，并在《鉴定 ID》字段中填写正确的 KMO 名称。

KMO 是安全套接层 (SSL) 证书：



鉴定环境

在《鉴定环境》字段中，输入目标服务器的主机名或 IP 地址以及十进制端口号（例如，187.168.1.1:8196）。

注释：如果看到《java.net.ConnectException: Connection Refused》，则表明远端没有可用的端口连接。如果存在以下某一情况，则可能出现此错误：

- ◆ 远端驱动程序未运行。
- ◆ 驱动程序正在运行但配置为使用另一个端口。

远程装载程序连接参数

Identity Manager Driver for eDirectory 不需要（且不使用）《远程装载程序》选项。

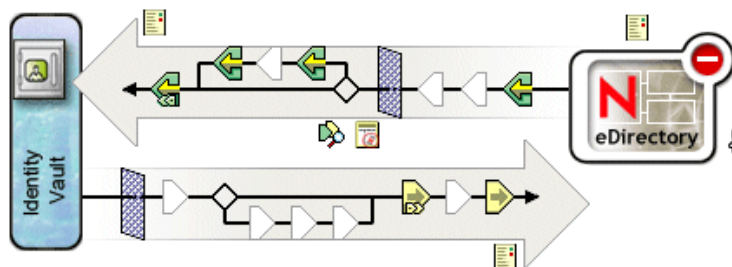
驱动程序超速缓存限制

除非 Novell 支持要求，否则请勿修改此字段。

5.2 配置过滤器

一个过滤器可同时控制发布者通道和订购者通道。应该修改过滤器以包括希望用于 Identity Manager 处理的对象类和特性。修改过滤器：

- 1 在 iManager 中，单击 *Identity Manager* > 《Identity Manager 概述》。
- 2 找到包含 eDirectory 驱动程序的驱动程序集，然后单击驱动程序图标以显示 《Identity Manager 驱动程序概述》页。
- 3 单击发布者通道上的过滤器。



- 4 自定义驱动程序。



在此示例中，《国家 / 地区》和《组》属于类。要添加类，请单击 *Add Class*（添加类），然后选择类。要删除类，请选择该类，然后单击《删除》。

在此示例中，《CN》是《组》类的特性。要添加特性，请选择类，单击《添加特性》，然后选择特性。

要修改类或特性，请选中它，然后选择右窗格中的选项。在此示例中，会在发布者通道和订购者通道上同步《国家 / 地区》特性。但不会在发布者通道上同步 GUID 特性。

要同步 GUID 特性，请选中它，然后单击《发布》部分中的《同步》。

设置为《在订购者通道上同步》的所有类都需要 GUID 特性。

通常，除了 GUID 特性，一棵树中的订购者通道过滤器应与另一颗树中的发布者通道过滤器相互匹配。

- 5 单击《应用》，然后单击《确定》。

5.3 配置发布者通道上的规则

驱动程序上的规则一般只适用于发布者对象，而不适用于订购者对象。由于订购者通道主要作为其它树中发布者通道的事件源，因此《匹配》和《布局》策略无法在订购者通道上正常运行。

有时需要在订购者通道上放置《事件转换》或《创建策略》，以便阻止通过通道发送不需要的数据。请参见《Identity Manager 3.0 安装指南》中的《使用范围过滤管理不同服务器上的用户》。

5.4 使用驱动程序对象口令

为增加安全性，除了使用 SSL 所需的必备证书外，还应该配置驱动程序以便一棵树上的订购者通道可以鉴定到远程树上的发布者通道。每棵树上的驱动程序对象口令应设置为与其它树上的应用程序口令相符。

设置树中的 Identity Manager 驱动程序对象口令：

- 1 在 iManager 中，单击 *Identity Manager* > 《Identity Manager 概述》。
- 2 找到包含 eDirectory 驱动程序的驱动程序集，然后单击驱动程序的图标。
- 3 在《Identity Manager 驱动程序概述》页中，单击 eDirectory 驱动程序对象。
- 4 选择《驱动程序配置》。
根据 iManager 版本和您的操作环境，从下拉列表或选项卡中进行选择。
- 5 找到《驱动程序对象口令》部分。

ドライバオブジェクトパスワード

ドライバオブジェクトパスワード: [パスワードの設定](#) **ドライバパスワード**

認証

us-linux-srv.novell

認証ID:

認証コンテキスト:

リモートローダ接続パラメータ:

ドライバのキャッシュ上限(KB単位):

パスワードの入力:

パスワードの再入力:

OK キャンセル

- 6 键入驱动程序对象口令。

重要：设置驱动程序对象口令后，无法去除此口令。

7 在《鉴定》部分，键入应用程序口令。

認証

us-linux-srv.novell

認証ID:

認証コンテキスト:

リモートローダ接続パラメータ:

ドライブのキャッシュ上限(KB単位):

アプリケーションパスワード: [パスワードの設定](#)

リモートローダパスワード:

起動オプション

us-linux-srv.novell

自動スタート
 手動
 使用不可

アプリケーションパスワード

パスワードの入力:

パスワードの再入力:

OK キャンセル

8 单击《应用》，然后单击《确定》。

5.5 迁移或复制对象

尽管 iManager 没有《复制》功能，但您可以使用《从 eDirectory 迁移》选项将对象从一棵 eDirectory 树复制到另一棵树。复制范围取决于驱动程序的策略。例如，根据驱动程序应用的策略，您可以将所有特性从一棵 eDirectory 树复制（同步）到另一棵树。这样的《复制》过程要求在树之间同步所有特性，在迁移过程中将对象放在同一位置，且在迁移过程中不能更改任何数据。

时戳始终与重新同步操作相关联。重新同步操作可查找已关联（已同步）但在加盖时戳后发生更改的对象。同时，还会尝试查找可能在加盖时戳后创建的对象。单击《重新同步》可能导致新用户被同步。

可以使用《从 eDirectory 迁移》选项代替《重新同步》选项来复制对象。可以使用该选项指定并同步对象列表。对于列表中每一个对象，iManager 会将数据写入目录。Identity Manager 会通知更改并为列出的对象启动同步进程。

- 1 确保源 eDirectory 树和目标 eDirectory 树中的服务器上均已安装了 Identity Manager 3。
- 2 配置源树中服务器上的 Identity Manager Driver for eDirectory。

在 eDirectory 驱动程序的《鉴定》窗格中，请提供目标服务器的名称或 IP 地址及端口。请参见“配置驱动程序对象属性”在第 23 页。

选择迁移选项：《平面》、《镜像》或《部门》。要在数据从源树迁移到目标树时保留目录结构（包括子树枝和名称），请选择《镜像》。

- 3 配置目标树中服务器上的 Identity Manager Driver for eDirectory。

在《鉴定》窗格中，请提供源服务器的名称或 IP 地址及端口。

- 4 在两棵树之间设置 SSL。

使用 NDS2NDS 向导在两棵树中创建 KMO 证书。请参见“设置 KMO”在第 19 页。

要启动 NDS2NDS 向导，请在 iManager 中选择 《Identity Manager 实用程序》 > 《NDS 间驱动程序证书》。

- 5 在 iManager 中，选择 *Identity Manager*，单击 《Identity Manager 概述》，然后单击驱动程序。
- 6 选择 《从 eDirectory 迁移》。



对于 eDirectory 间的迁移，请从源树迁移到目标树。

《迁移到 eDirectory 中》选项不适用于 Identity Manager Driver for eDirectory。

- 7 选择对象。

例如，可以选择用户对象或树枝对象。可以搜索或浏览对象，还可以添加多个对象。

- 8 单击两次 《确定》。

客户端（例如，iManager）向列表中的每个对象写入值。此更改事件会导致 Identity Manager 将数据推送到目标树。

文档更新

A

本节包含关于 Identity Manager Driver for eDirectory 的新的或更新的信息。

万维网上提供的文档采用以下两种格式：HTML 和 PDF。HTML 和 PDF 文档均为最新并包含本节列出的更改。

如果要了解您使用的 PDF 文档副本是否为最新版本，请检查 PDF 文件的发布日期。日期位于《法律声明》一节中（该节紧随标题页之后）。

A.1 2006 年 5 月 8 日

表 A-1 2006 年 5 月 8 日所做的更改

| 位置 | 更改 |
|----------------------|---|
| “安装驱动程序 Shim” 在第 7 页 | 说明以下内容： <ul style="list-style-type: none">◆ 本节假定服务器上已安装 eDirectory。◆ 本节介绍如何向服务器添加 eDirectory 驱动程序。 |