

# Novell Identity Manager Driver for Exchange 5.5

1.6.2

[www.novell.com](http://www.novell.com)

实施指南

2005 年 11 月 23 日



**Novell®**

## 法律声明

Novell, Inc. 对本文档的内容或使用不做任何声明或保证，特别是对适销性或针对特定用途的适用性不做任何明示或暗示保证。另外，Novell, Inc. 保留随时修改本出版物及其内容的权利，并且无义务将此类修改通知任何个人或实体。

另外，Novell, Inc. 对所有软件不做任何声明或保证，特别是对适销性或针对特定用途的适用性不做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，并且没有义务将此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 软件的详细信息，请参考 [www.novell.com/info/exports/](http://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、传送此出版物的任何部分或将其储存在检索系统上。

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/> 中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](http://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](http://www.novell.com/documentation)。

## **Novell 商标**

ConsoleOne 是 Novell, Inc. 在美国和其它国家 / 地区的注册商标。

eDirectory 是 Novell, Inc. 的商标。

DirXML 是 Novell, Inc. 的注册商标。

Novell 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相应拥有者的财产。



# 目录

关于本指南	3
<b>1 Identity Manager Driver for Exchange 简介</b>	<b>5</b>
1.1 概述	5
1.2 术语变更	5
1.3 驱动程序功能	5
1.4 主要术语	6
1.5 优势	7
1.6 所需技能	7
1.7 添加到 Identity Manager 基本功能	7
1.7.1 事件处理支持	7
1.7.2 策略	8
1.7.3 关联	8
<b>2 安装和配置驱动程序</b>	<b>9</b>
2.1 前提条件	9
2.1.1 软件要求	9
2.1.2 硬件要求	9
2.2 升级到 Identity Manager 3	9
2.3 安装 Exchange 驱动程序 Shim	9
2.4 安装后的任务	11
2.4.1 导入驱动程序配置文件	11
2.4.2 配置 Exchange Server	13
2.4.3 安装远程 Exchange 驱动程序	15
2.4.4 配置驱动程序过滤器	15
2.4.5 启动驱动程序	16
2.4.6 迁移和重新同步数据	17
2.4.7 激活驱动程序	18
<b>3 升级</b>	<b>19</b>
3.1 运行 Normalize Exchange Associations 实用程序	19
3.2 升级驱动程序 Shim	20
3.3 升级驱动程序配置	20
<b>4 自定义 Identity Manager Driver for Exchange</b>	<b>23</b>
4.1 将 Identity Manager Driver for Exchange 与 Identity Manager Driver for NT Domain 进行集成	23
4.2 管理外部收件人	25
4.3 同步代理地址和目标地址特性	26
4.4 使用授权联结	27
4.5 使用自定义联结	27
4.6 指定 LDAP 端口	28

<b>5</b>	<b>排查驱动程序错误</b>	<b>29</b>
5.1	查错 . . . . .	29
5.2	驱动程序错误讯息 . . . . .	29

# 关于本指南

本指南介绍了如何安装和配置 Identity Manager Driver for Microsoft\* Exchange 5.5。

- ◆ 第 1 章 “Identity Manager Driver for Exchange 简介” 在第 5 页
- ◆ 第 2 章 “安装和配置驱动程序” 在第 9 页
- ◆ 第 3 章 “升级” 在第 19 页
- ◆ 第 4 章 “自定义 Identity Manager Driver for Exchange” 在第 23 页
- ◆ 第 5 章 “排查驱动程序错误” 在第 29 页

## 读者

本文档适用于具备 Exchange 和 Novell® Identity Manager 专业知识的管理员。

## 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](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 Exchange*。

## 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 Exchange 简介

# 1

- ◆ “概述” 在第 5 页
- ◆ “术语变更” 在第 5 页
- ◆ “驱动程序功能” 在第 5 页
- ◆ “主要术语” 在第 6 页
- ◆ “优势” 在第 7 页
- ◆ “所需技能” 在第 7 页
- ◆ “添加到 Identity Manager 基本功能” 在第 7 页

## 1.1 概述

Identity Manager Driver for Exchange 是一个在 Identity Vault 和 Microsoft Exchange 之间同步数据的连接器。通过此同步，可以在 Identity Vault 中管理 Exchange 帐户，而不再需要分别管理用户的 Identity Vault 和 Exchange 帐户。Identity Manager Driver for Exchange 允许您使用一个单独的管理工具将 Identity Vault 和 Exchange 帐户作为一个帐户进行管理，从而提高了网络管理的效率。

Identity Manager Driver for Exchange 在 Windows\* NT\* 上运行。

该驱动程序仅支持《分发列表》、《远程》和《邮箱》类。

有关 Identity Manager 中新增功能的信息，请参见《*Identity Manager 3.0 安装指南*》中的《*Identity Manager 3 中的新增功能*》。

## 1.2 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（指 eDirectory 特性或类时除外）

## 1.3 驱动程序功能

- ◆ 通过 AuthoritativeBind 参数可以使用授权 LDAP 联结而非匿名 LDAP 联结。请参见“使用授权联结” 在第 27 页。

- ◆ 可以使用 Assoc-NT-Account 特性在 Exchange 中进行查询。
- ◆ 现在，在 eDirectory 中使用名为 DirXML-NTAccountName 的特性代替 preferredName。请参见“将 Identity Manager Driver for Exchange 与 Identity Manager Driver for NT Domain 进行集成。”在第 23 页。  
但仍可以使用 preferredName 特性。
- ◆ 支持《基于职能的权利》功能。可以在导入过程中选择此选项。  
使用《基于职能的权利》是设计使然。选择此选项之前，请参见《Novell Identity Manager 3.0 管理指南》中的《创建和使用权利》。
- ◆ 可以自定义驱动程序以提供驱动程序心跳。请参见《Novell Identity Manager 3.0 管理指南》中的《添加驱动程序心跳》。

## 1.4 主要术语

**驱动程序 Shim。**由 Identity Manager 或远程装载程序直接装载的动态链接库 (Exchange55Shim.dll)。Shim 收集要从 Exchange 发送到 Identity Vault 的更改，将更改从 Identity Vault 传递到 Exchange，并作为连接 Identity Vault 和 Exchange 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。Identity Manager Driver for Exchange 是 Microsoft Exchange 和 Identity Vault 之间的一个双向同步连接器。该连接器使用 XML 将 Exchange 对象转换为 Identity Vault 对象，反之亦然。

应用程序可以通过驱动程序将事件从应用程序发布到目录，从目录订购事件，同时驱动程序可以同步目录和应用程序之间的数据。

要在 Metadirectory 引擎和 Exchange 之间建立连接，请指定驱动程序的配置及连接参数、策略和过滤器值。

**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，让 Identity Vault 管理驱动程序 Shim 的各个参数。

**Identity Vault。**其它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
- ◆ 订购者通道

Identity Manager Driver for Exchange 是 Microsoft Exchange 和 Identity Vault 之间的一个双向同步连接器。该连接器使用 XML 将 Exchange 对象转换为 Identity Vault 对象，反之亦然。

**发布者通道。**从您的 Exchange Server 读取信息，并通过 Metadirectory 引擎向 Identity Vault 提交该信息。

发布者通道使用 Poll 参数巡回检测 Exchange 服务器上对象的更改。如果 Identity Manager Driver for Exchange 在 Exchange 中检测到更改，则会同步 Exchange 和 Identity Vault 之间的数据。如果更改是由订购者向 Exchange 发送的数据引起的，则没有必要进行同步。

订购者通道。检查对 Identity Vault 对象的添加和修改，并通过 Metadirectory 引擎在 Exchange 服务器上创建更改。

订购者通道同步在 Identity Vault 中所做的更改和 Exchange 服务器上的数据。如果在 Identity Vault 中更改了关联对象，则订购者通道会使用新信息更新 Exchange 服务器。

## 1.5 优势

您可以按以下方式使用驱动程序来自动完成业务进程并对其进行维护：

- ◆ 从 Exchange 对象自动创建 Identity Vault 对象。
- ◆ 双向同步 Exchange 和 Identity Vault 之间的数据。
- ◆ 保证 Identity Vault ID 的准确和一致。
- ◆ 使用 Identity Manager 和 Identity Vault，在 Exchange 和多个应用程序（例如 Identity Vault、Lotus Notes\*、Netscape\*、SAP\* 和 Active Directory\*）之间实现集成。
- ◆ 管理 Exchange 分发列表和远程对象。

可以采用策略的形式使用自定义业务逻辑来配置 Identity Manager Driver for Exchange，以提高组织进程的效率。安装和配置驱动程序之前，应评估和定义这些进程。在安装驱动程序期间，请配置其策略以便尽可能自动完成这些进程。

## 1.6 所需技能

实施驱动程序需要具备 Exchange 和 Identity Manager 专业知识。本文档假定您具备以下某一人所具有的 Exchange 专业知识：

- ◆ Exchange 开发人员
- ◆ Exchange 管理员
- ◆ 应用程序设计人员
- ◆ 升级管理员
- ◆ 数据库管理员

本文档假定您具备 eDirectory 管理员或 Identity Manager 管理员所具有的 Identity Manager 专业知识。

## 1.7 添加到 Identity Manager 基本功能

下列 Identity Manager 功能对驱动程序很重要：

- ◆ “事件处理支持” 在第 7 页
- ◆ “策略” 在第 8 页
- ◆ “关联” 在第 8 页

### 1.7.1 事件处理支持

驱动程序支持发布者通道和订购者通道上的以下事件。

表 1-2 支持的事件

功能	事件
发布者	添加、修改、删除、重命名
订购者	添加、修改、删除、重命名

驱动程序还支持定义的查询功能，以便 Identity Manager 可以查询同步的应用程序或目录。

## 1.7.2 策略

策略用于控制驱动程序与 Identity Vault 和应用程序、数据库或目录的同步。策略可帮助 Identity Manager 将通道输入上的事件转换为通道输出上的一组命令。

可以使用 Identity Manager 的 iManager 插件配置策略。样本驱动程序配置包括下列几组策略：

表 1-3 样本配置文件中的策略

策略	说明
位置	在发布者通道和订购者通道上运行
匹配	在发布者通道和订购者通道上运行
映射	在驱动程序对象上配置
输入转换	在驱动程序对象上配置
输出转换	在驱动程序对象上配置
创建	在发布者通道和订购者通道上运行
事件转换	在发布者通道上运行
命令转换	在发布者通道上运行

有关创建您自己的策略的更多信息，请参见 [《策略构建器和驱动程序自定义指南》](#)。

## 1.7.3 关联

驱动程序使用 Exchange DN 进行关联。可为与 Exchange 对象相关的记录创建唯一的 ID 或唯一的用户名。但是，Identity Manager 不需要共享这些相同的唯一 ID。

根据所安装并启用的每个 Exchange 驱动程序，从 Exchange 接收的关联特性对于 Exchange 应用程序是唯一的。如果安装了其它驱动程序，它们将使用特定于该应用程序的关联。此关联具有多值特性。因此，如果使用 Identity Manager 连接多个应用程序，则可以使用此特性存储这些应用程序的所有关联。

唯一 ID 关联将 Exchange 中的对象链接到它在 Identity Vault 中的关联对象。此关联允许驱动程序对相应对象执行后续任务。

《关联》字段存储在 Identity Manager 属性页的 Identity Vault 对象上。

# 安装和配置驱动程序

- “前提条件” 在第 9 页
- “安装 Exchange 驱动程序 Shim” 在第 9 页
- “安装后的任务” 在第 11 页

## 2.1 前提条件

本节列出了运行 Identity Manager Driver for Exchange 所需的软件和硬件要求。

### 2.1.1 软件要求

- Novell® Identity Manager 2 或更新版本，及其前提条件
- 带有最新增补程序和 Service Pack（SP6a 或更新版本）的 Windows NT 4
- 带有 Service Pack 4（或更新版本）和最新增补程序的 Exchange 5.5

---

注释：如果 Exchange Server 未安装最新增补程序，则《权利策略》将无法正确指派 Exchange 分发列表中的成员资格。同时，Exchange 中的缺陷会导致无法正确处理代理地址。

---

### 2.1.2 硬件要求

- 128 MB RAM（推荐使用 256 MB 或更大）

## 2.2 升级到 Identity Manager 3

在安装 Identity Manager 的过程中，可以在安装 Metadirectory 引擎的同时安装 Driver for Exchange 5.5（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。

## 2.3 安装 Exchange 驱动程序 Shim

可以在安装 Metadirectory 引擎的同时安装 Driver for Exchange（及其它 Identity Manager 驱动程序）。请参见《*Identity Manager 3.0 安装指南*》。

也可以在安装 Metadirectory 引擎后单独安装该驱动程序。如果没有 CD，请下载 Identity\_Manager\_3\_NW\_Win.iso，然后创建一张 CD。可以从 [Novell 下载 \(http://download.novell.com/index.jsp\)](http://download.novell.com/index.jsp) 下载。

- 1 请从 CD 或下载映像运行安装程序。

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《DirXML 概述》对话框中，查看信息，然后单击《下一步》。

此对话框提供有关以下两项的信息：

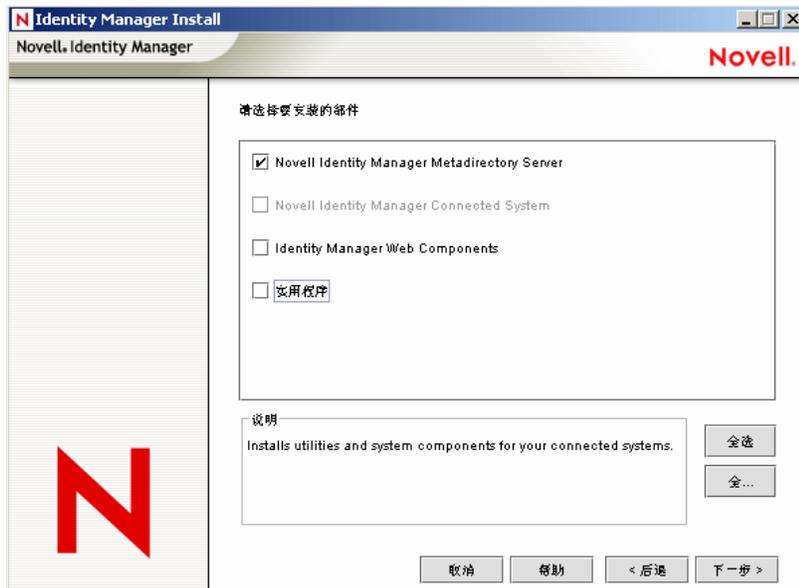
- ◆ Metadirectory 服务器
- ◆ 已连接的服务器系统

4 在第二个《DirXML 概述》对话框中，查看信息，然后单击《下一步》。

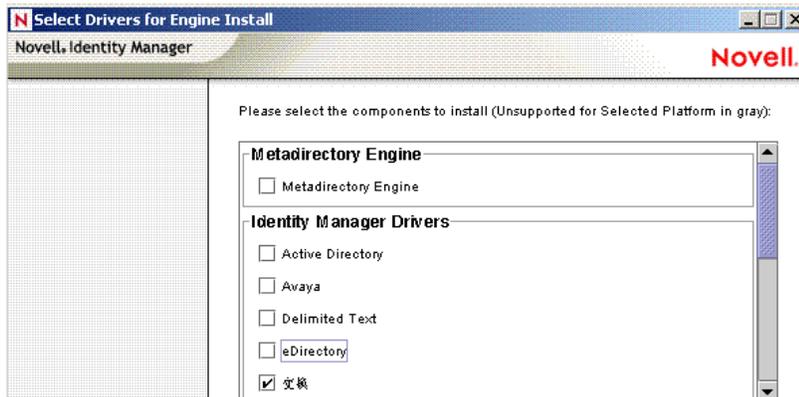
此对话框提供有关以下两项的信息：

- ◆ 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《Exchange》，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》对话框中，单击《关闭》。

安装驱动程序 Shim 后，请创建和配置驱动程序对象。通过完成“安装后的任务”在第 11 页来执行此操作。

## 2.4 安装后的任务

- ◆ “导入驱动程序配置文件” 在第 11 页
- ◆ “配置 Exchange Server” 在第 13 页
- ◆ “安装远程 Exchange 驱动程序” 在第 15 页
- ◆ “配置驱动程序过滤器” 在第 15 页
- ◆ “启动驱动程序” 在第 16 页
- ◆ “迁移和重新同步数据” 在第 17 页
- ◆ “激活驱动程序” 在第 18 页

### 2.4.1 导入驱动程序配置文件

Exchange 5.5 驱动程序样本配置可创建和配置驱动程序正常运行所需的对象。

例如，请考虑下面的情形：

您在实验室中创建了一个驱动程序集和驱动程序对象。配置驱动程序后，保存了该配置。为了节省时间和保持在实验室中正常运行所需的相同设置，可将驱动程序的配置文件从实验室环境导入生产环境。

使用 **iManager** 导入

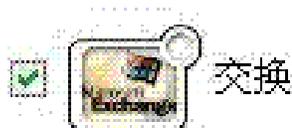
- 1 在 iManager 中，选择《Identity Manager 实用程序》>《导入驱动程序》。
- 2 选择是否将配置文件放到一个新的或现有的驱动程序集中。

在下列情况下，请选择《在现有驱动程序集中》：

- ◆ 需根据树中的其它驱动程序，对该驱动程序进行逻辑分组。
- ◆ 服务器可以处理新驱动程序生成的其它通讯。
- ◆ 您希望更新或自定义现有驱动程序。

例如，可以将驱动器指向另一个树枝，但保留已设置的所有规则。

- 3 在《导入驱动程序》对话框中，选择 Exchange\_5\_5 驱动程序，然后单击《下一步》。



- 4 滚动至下列参数并提供所需信息。请参考界面中提供的说明。
  - ◆ 驱动程序名
  - ◆ 域名
  - ◆ *IP address of the Exchange Server* (*Exchange Server* 的 *IP* 地址)
  - ◆ *Authoritative Bind* (授权联结)  
请参见“使用授权联结”在第 27 页。

- ◆ *Exchange Server Name* (*Exchange* 服务器名)
- ◆ *Exchange Site Organization* (*Exchange* 站点组织)
- ◆ *Exchange Site* (*Exchange* 站点)
- ◆ *Polling Frequency* (巡回检测频率)
- ◆ *Authoritative User* (授权用户)
- ◆ 用户口令
- ◆ *eDir Users Container* (*eDir* 用户树枝)
- ◆ *eDir Groups Container* (*eDir* 组树枝)
- ◆ *Configure Data Flow* (配置数据流)



- ◆ 口令失败通知用户
- ◆ *Enable Entitlements* (启用权利)
 

使用《基于职能的权利》是设计使然。除非您已查阅了《*Novell Identity Manager 3.0 管理指南*》中的《*创建和使用权利*》，否则请勿选择此选项。

如果选择此选项，请同时提供 *Action - Remove Mailbox Entitlement* (操作 - 去除邮箱权利) 相关信息。
- ◆ 操作 - 去除邮箱权利
- ◆ *Driver is Remote/Local* (远程 / 本地驱动程序)
- ◆ 远程主机名和端口
- ◆ 驱动程序口令
- ◆ 远程口令

##### 5 定义安全性等效。

趋势是指派 Admin。但是，可能要创建 DriversUser (举例) 并向该用户指派安全性等效。

##### 6 标识代表《管理职能》的所有对象，并将其从复制中排除。

排除在步骤 5 中指定的安全性等效对象 (如 DriversUser)。如果删除了安全性等效对象，则表明已从驱动程序中去除了权限。因此，驱动程序无法对 Identity Vault 进行更改。

##### 7 (视情况而定) 如果您正在重新创建或更新驱动程序，请选择《更新有关该驱动程序的所有方面》，然后单击《下一步》。

##### 8 在《摘要》屏幕中，查看选项，然后单击《完成》。

如果需要更改，请单击《后退》。

导入后，请为安装配置驱动程序集对象和驱动程序对象，然后启动或重新启动驱动程序。

使用 **Designer for Identity Manager** 导入

可以使用 **Designer for Identity Manager** 导入 JDBC 的驱动程序基本配置文件。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 *Exchange55.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 填充各个字段以配置驱动程序。  
指定特定于所在环境的信息。
- 6 在指定参数后，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。

## 2.4.2 配置 **Exchange Server**

本节包含有关配置 Exchange 服务器以用于 **Identity Manager Driver for Exchange** 的信息。您应该在事先已经熟悉 Exchange 的管理和部署。

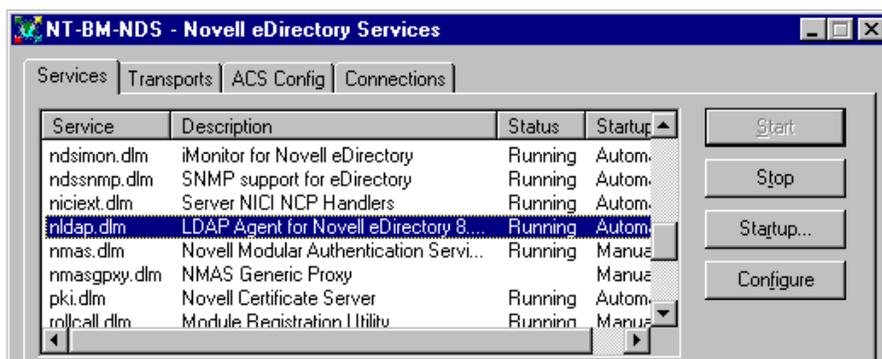
在继续操作前，您必须了解以下设置信息：

- ◆ 驱动程序将与之同步的 Exchange Server 的名称。
- ◆ 要管理的 Exchange 站点的名称。
- ◆ Exchange 服务器的 IP 地址或主机名。
- ◆ Exchange 服务帐户的名称及其口令。

如果 Exchange 服务器与 **Identity Vault** 在同一台机器上运行，请卸载 LDAP 服务器或对其重新配置以在另一个端口上运行。

卸载 LDAP：

- 1 在《控制面板》中，双击 *Novell eDirectory*。
- 2 滚动至 *ldap.dlm* 并选择它，然后单击《停止》。



重新配置 LDAP 以在另一个端口上运行：

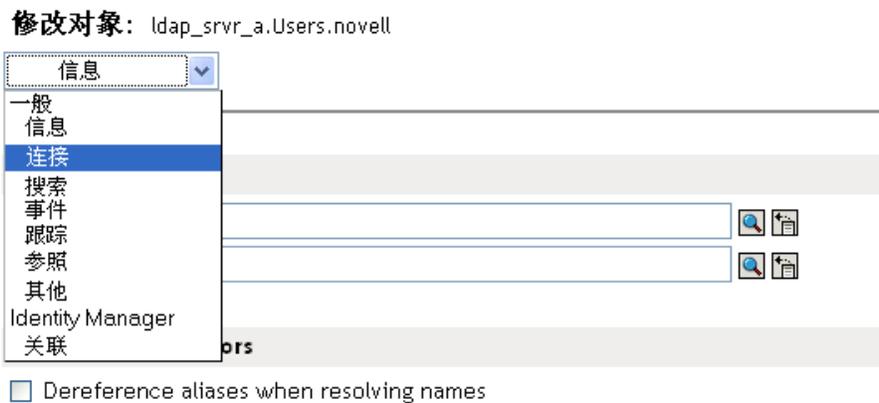
- 1 在 Novell iManager 中，选择 《eDirectory 管理》 > 《修改对象》。



- 2 导航到 LDAP 服务器对象并选择它。



- 3 从下拉列表中选择 《常规》 > 《连接》。



#### 4 滚动至《端口》部分。



**Ports**

Enable Encrypted Port  
Port:

Enable Non-Encrypted Port  
Port:

#### 5 将 *Enable Non-Encrypted Port*（启用非加密端口）更改为 389 以外的值，然后单击《确定》。

如果另一个 LDAP 服务已经使用 389，请更改 Exchange 服务器的 LDAP 端口号，使其不与其它服务冲突。如果更改了 Exchange 服务器的端口号，请同时更改 Identity Manager Driver for Exchange 查看的 LDAP 端口。请参见“指定 LDAP 端口”在第 28 页。

### 2.4.3 安装远程 Exchange 驱动程序

该驱动程序不需要与 Exchange Server 在同一台机器上运行。但在远程运行时，驱动程序只能在同属于 Exchange 服务器域的 NT 服务器或成员服务器上运行。这是 Microsoft 强加的 NT 身份凭证限制。

运行驱动程序前，安装驱动程序的 NT 服务器必须安装以下三个 Microsoft .dll 文件：libxds.dll、exchmem.dll 和 expsrv.dll。可通过 Exchange Administrator 程序安装这些文件。可以从 *Microsoft Exchange Server CD* 安装 Exchange Administrator。

创建新的 Exchange 邮箱时，远程驱动程序不会创建 NT 帐户。这仍然是由驱动程序使用的 Microsoft DAPI API 强加的限制所致。

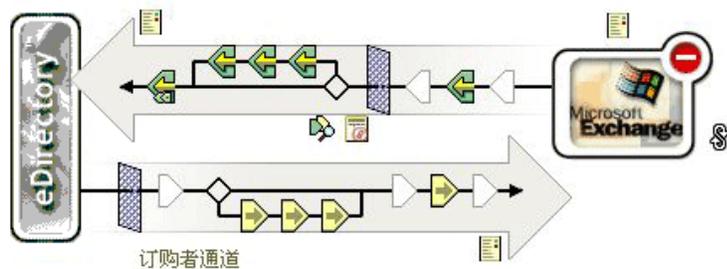
有关安装远程装载程序的说明，请参见《*Novell Identity Manager 3.0 管理指南*》中的《设置连接的系统》。

### 2.4.4 配置驱动程序过滤器

修改发布者通道和订购者通道上的过滤器，以便包括希望 Identity Manager 处理的对象类和特性。

- 1 在 iManager 中，单击 *Identity Manager* > 《Identity Manager 概述》。
- 2 找到包含 Exchange 驱动程序的驱动程序集，然后单击驱动程序的图标以显示《Identity Manager 驱动程序概述》页。

3 单击驱动程序过滤器图标。



4 (可选) 添加希望 Identity Manager 处理的类。

Exchange 驱动程序支持 《分发表》、《远程》和 《邮箱》类。

5 启用同步。

添加类时，不启用发布者通道和订购者通道，如下图中的红色 X 所示。



要启用通道，请单击通道图标，然后单击 《同步》。



6 单击 《确定》保存更改。

邮件昵称具有 Exchange Administrator 中 《常规》页上的别名特性。它是驱动程序支持、但不映射到任何现有 eDirectory 特性的 Exchange 特性名。根据组织的需要，可以通过修改纲要映射策略，在扩展纲要之后，将该 Exchange 特性映射到现有的或新的 eDirectory 特性。确保添加的任何映射的语法均有效。也可以在样式表中对其进行处理。

## 2.4.5 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，并选择它。

3 在要启动的驱动程序中，单击下拉列表图标。



4 选择 《启动驱动程序》。

启动驱动程序后，可以打开 DSTrace 查看驱动程序的处理细节。

由于对单个对象进行了更改，因此会逐个对象地进行同步。要立即进行同步，请按“**迁移和重新同步数据**”在第 17 页中所述进行同步。

## 2.4.6 迁移和重新同步数据

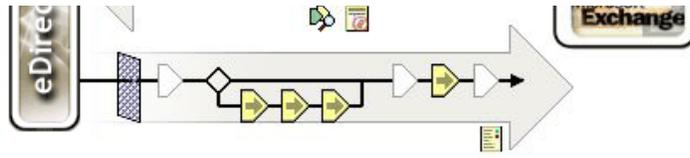
Identity Manager 在数据更改时对其进行同步。如果要立即同步所有数据，可以选择以下选项：

- ◆ 从 **eDirectory** 迁移数据：允许您选择要从 eDirectory 迁移到应用程序的树枝或对象。迁移对象时，Metadirectory 引擎会将所有《匹配》、《布局》、《创建》策略以及订购者过滤器应用于对象。
- ◆ 将数据迁移到 **eDirectory** 中：允许您定义 Metadirectory 引擎用于将对象从应用程序迁移到 Novell eDirectory 的准则。迁移对象时，Metadirectory 引擎会将所有《匹配》、《布局》、《创建》策略以及发布者过滤器应用于对象。按照类列表中指定的顺序将对象迁移到 eDirectory 中。
- ◆ 同步：Metadirectory 引擎查看订购者类过滤器并处理这些类的所有对象。合并关联对象，将不关联的对象作为添加事件进行处理。

使用上述选项之一：

- 1 在 iManager 中，选择 *Identity Manager* > 《Identity Manager 概述》。
- 2 找到包含 Exchange 驱动程序的驱动程序集，然后双击驱动程序图标。

3 单击相应的迁移按钮。



## 2.4.7 激活驱动程序

在安装后的 90 天内激活驱动程序。否则，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》](#)。

- ◆ “运行 Normalize Exchange Associations 实用程序” 在第 19 页
- ◆ “升级驱动程序 Shim” 在第 20 页
- ◆ “升级驱动程序配置” 在第 20 页

## 3.1 运行 Normalize Exchange Associations 实用程序

如果要从 DirXML® Driver 1.0 for Exchange 升级，则需要运行 Normalize Exchange Associations 实用程序。此实用程序搜索 eDirectory 树并规范 Identity Manager Driver for Exchange 关联。

---

注释：如果要从 1.0a 增补程序或更新版本升级，则不需要运行 Normalize Exchange Associations 实用程序。

---

- 1 从 Novell® 支持获取 changeAssocKey.zip 文件。
- 2 在安装 Identity Manager Driver for Exchange 的 NT 服务器上创建一个临时目录。
- 3 在该目录中展开 changeAssocKey.zip。
- 4 打开 run.bat 文件，然后编辑文件中的以下参数：

参数	值
Java	Java* 的驱动器号和路径。例如，输入 C:\Novell\consoleone\1.2\jre\bin\java 或 D:\Novell\NDS\jre\bin\java
LDAP address:port	Identity Vault 服务器的 IP 地址和端口号。通常，此参数为 localhost:389。
LDAP Bind ID	LDAP 鉴定 ID。
LDAP Bind Password	LDAP 鉴定口令。
Driver Name	驱动程序对象的名称。例如， ExchangeDriver。
Action	指定以下所需操作之一： <ul style="list-style-type: none"> <li>◆ 1 – 列出不与以上指定驱动程序关联的 Identity Vault 对象。</li> <li>◆ 2 – 列出与以上指定的驱动程序不完全关联的 Identity Vault 对象。</li> <li>◆ 3 – 列出要规范其关联的 Identity Vault 对象。</li> <li>◆ 4 – 修改 Identity Vault 中的关联并列出对象。</li> </ul>

---

注释：建议您首先将操作设置为 3，以便查看将操作设置为 4 时将要更改的关联。然后，可以将操作设置为 4 并再次运行程序。多次运行程序不会引起任何问题。如果关注关联的当前状态，可以在运行实用程序时将操作设置为 1 或 2。

---

- 5 运行 run.bat 文件。

## 3.2 升级驱动程序 Shim

注释：不支持对 DirXML 1.x 驱动程序 Shim 运行 Identity Manager 驱动程序配置。

升级时，新的驱动程序 Shim 会替换以前的驱动程序 Shim，但保留以前驱动程序的配置。新驱动程序 Shim 可以运行 DirXML 1.x 配置，无需进行任何更改。

- 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 Exchange 驱动程序 Shim](#)”在第 9 页。

- 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 用 Identity Manager 激活身份凭证激活驱动程序 Shim。

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 20 页。

## 3.3 升级驱动程序配置

可以用 Identity Manager 3.0 驱动程序 Shim 和新的 Metadirectory 引擎运行 DirXML 1.x 驱动程序配置，而无需对该配置进行任何更改。

但是，可能需要编辑 DirXML 1.x 驱动程序配置。为此，请执行下列操作之一：

- ◆ 使用 DirXML 1.x iManager 插件。

请参见《[Novell Identity Manager 3.0 管理指南](#)》中的《[在 Identity Manager 环境中管理 DirXML 1.1a 驱动程序](#)》。

- ◆ 运行将 DirXML 1.x 配置转换为 Identity Manager 格式的向导，以便可以使用 Identity Manager 的 iManager 插件。

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》。

要利用 Identity Manager 的功能，请执行以下操作：

- ◆ 查看提供的样本配置。
- ◆ 有关新功能的信息，请参见《*Novell Identity Manager 3.0 管理指南*》。



# 自定义 Identity Manager Driver for Exchange

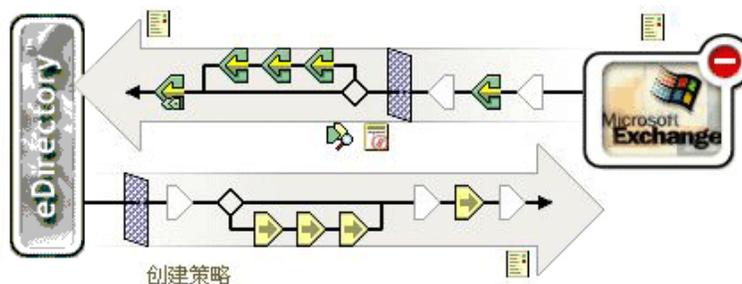
- ◆ “将 Identity Manager Driver for Exchange 与 Identity Manager Driver for NT Domain 进行集成。” 在第 23 页
- ◆ “管理外部收件人” 在第 25 页
- ◆ “同步代理地址和目标地址特性” 在第 26 页
- ◆ “使用授权联结” 在第 27 页
- ◆ “使用自定义联结” 在第 27 页
- ◆ “指定 LDAP 端口” 在第 28 页

## 4.1 将 Identity Manager Driver for Exchange 与 Identity Manager Driver for NT Domain 进行集成。

**重要：**如果要使用 Identity Manager Driver for NT Domain 和 Identity Manager Driver for Exchange，请编辑默认策略或创建新策略以解决两个驱动程序之间的帐户问题。此策略可以在 NT Domain 驱动程序创建 NT Domain 帐户之前，阻止 Exchange 驱动程序尝试创建该帐户。

Identity Manager Driver for NT Domain 具有一个名为 DirXML-NTAccountName 的用户特性。此特性包含 DomainName/UserName 值。Exchange MailBox 对象需要此值才能与域帐户关联。为正确进行关联，需要将 DirXML-NTAccountName 中的值放到 MailBox 特性 Assoc-NT-Account 中。请记住特性名称区分大小写。

- 1 创建策略，以便在未填充 DirXML-NTAccountName 特性的情况下不会创建新的 MailBox 对象。
  - 1a 在 iManager 中，选择 *Identity Manager* > 《Identity Manager 概述》。
  - 1b 选择订购者通道上的 《创建策略》对象。



1c 在《创建策略》对话框中，单击《编辑》。



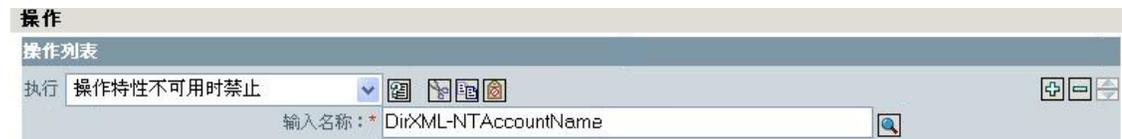
1d 单击 *User Required Attributes*（用户要求的特性）。



1e 在《操作》部分中，为 DirXML-NTAccountName 特性添加操作。  
单击 + 图标，然后从《执行》下拉列表中选择《操作特性不可用时禁止》。



从《输入名称》下拉列表中选择 *DirXML-NTAccountName*。



1f 单击《确定》。

如下图所示，将操作置于《用户要求的特性》部分中。



- 2 校验 DirXML-NTAccountName 特性是否位于以下位置：
  - ◆ Identity Manager Driver for NT Domain 上的发布者过滤器
  - ◆ Identity Manager Driver for Exchange 上的订购者过滤器
- 3 同步订购者通道。

过滤器: Exchange 5\_5.drivset.novell



- 4 重新启动这两个驱动程序。

对驱动程序进行这些更改后，在 Identity Vault 中创建用户时会出现以下控制流：

1. 向 Identity Manager Driver for NT Domain 递交创建请求。
2. 禁止 Identity Manager Driver for Exchange 创建事件，因为缺少 DirXML-NTAccountName 特性。
3. Identity Manager Driver for NT Domain 创建 NT 帐户，并将刚创建的 NT 帐户的名称发布到 DirXML-NTAccountName 特性。
4. 通知 Identity Manager Driver for Exchange。它会创建邮箱，并将邮箱与 Identity Vault 中存储的 NT 帐户信息相关联。

注释：示例使用 DirXML-NTAccountName 作为 eDirectory™ 特性以保存 NT 帐户信息，但可以选择任何对您有用的特性。

## 4.2 管理外部收件人

使用 Microsoft Exchange 目录可以创建称为《外部收件人》的特殊对象。可以将这些对象视为代表外部讯息交换系统中收件人的通讯录项。可以修改纲要映射策略，以便可以将远程对象映射到用户对象或任何其它所需的 Identity Vault 对象。例如：

```
<class-name> <nds-name>User</nds-name> <app-name>remote</app-name> </class-name>
```

如果决定进行此更改，还应该将因特网电子邮件地址特性作为所需特性添加到《创建》策略中，如下示例所示：

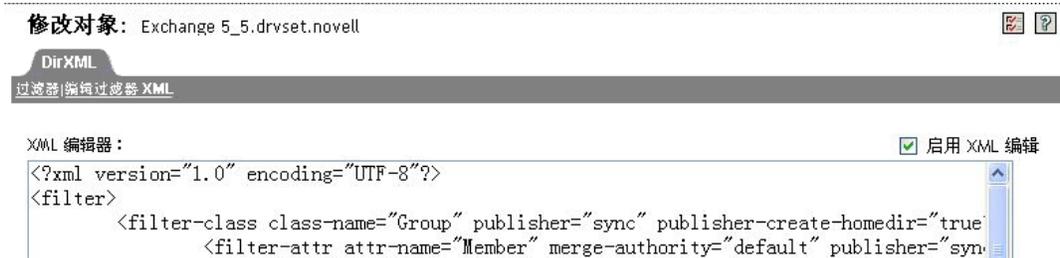
```
<create-rules> <create-rule class-name="User" <required-attr attr-name="Given Name"/> </create-rule> </create-rules>
```

在 Exchange 目录中创建《外部收件人》对象时需要因特网电子邮件地址特性。不添加因特网电子邮件地址特性会导致在尝试创建外部收件人时出现错误。

### 4.3 同步代理地址和目标地址特性

要同步多值代理地址和目标地址特性的所有电子邮件值，请将 <proxyFlg/> 标签添加到驱动程序参数中。

- 1 在 iManager 中，单击《eDirectory 管理》>《修改对象》。
- 2 找到并选择 Identity Manager Driver for Exchange 对象（如 EXCHANGE 5\_5），然后单击《确定》。
- 3 在《驱动程序配置》页的底部，找到《驱动程序参数》部分，然后单击《编辑 XML》。
- 4 单击《启用 XML 编辑》，以便可以编辑底稿。



- 5 添加 <proxyFlg/> 标签。  
可将此标签放在 <driver-options> 标签之间的任何位置。更新的参数看上去类似于以下示例：

```
<driver-options> <x-ldap-server display-name="IP address of Exchange Server (for LDAP queries):">167.55.135.28</x-ldap-server> <x-remote display-name="Remote Exchange Driver?(1=true; 0=false):">0</x-remote> <x-server display-name="Exchange Server Name:">DHEAD</x-server> <x-site display-name="Exchange Site:">/o=Novell/ou=DOMAINLIMA</x-site> <proxyFlg/> </driver-options>
```

- 6 取消选择《启用 XML 编辑》，然后返回至《驱动程序参数》部分。
- 7 单击《确定》。

## 4.4 使用授权联结

查询涉及从属或子树范围时，驱动程序使用 LDAP。过去，只能使用匿名联结。使用匿名联结时，驱动程序看不到 Exchange 中隐藏的特性。

通过新的 `AuthoritativeBind` 参数可以使用授权 LDAP 联结代替匿名 LDAP 联结。此选项是导入样本驱动程序配置时的提示之一。

建议仅在需要查看隐藏特性时（例如，要根据隐藏特性进行匹配时）才使用授权联结。

请记住在使用授权联结时，可以在跟踪中看到诸如 `NT4AccountName` 的隐藏特性。为特定目的（例如迁移用户）使用授权联结后，如果不再需要使用授权联结，则可以将驱动程序参数更改为重新使用匿名联结。

## 4.5 使用自定义联结

可能需要使用自定义联结联结到 LDAP。例如，如果要在 Exchange 中查找隐藏对象，则需要作为 `admin` 用户进行联结。

使用自定义联结：

- 1 在《驱动程序参数》部分中，单击《编辑 XML》。

### 驱动程序参数

S3K-NDS.Vmp

编辑 XML

#### 驱动程序设置

Exchange LDAP Server	<input type="text"/>
Create NT Security Account 0=Yes 1=No	<input type="text" value="0"/>
Exchange Server	<input type="text"/>
Exchange 站点:	<input "="" type="text" value="/o=/ou="/>
Authoritative Bind:	<input type="text" value="Yes"/>

- 2 单击《启用 XML 编辑》。
- 3 在 `<driver-options>` 部分中，添加指定自定义联结的标签和字符串。

例如，键入

```
<hiddenObjectBind>cn=Administrator,dc=DOMAIN,cn=admin<hiddenObjectBind/>
```

此示例使用以下字符串，您需要在配置中自定义字符串：

字符串	说明
Administrator	具有管理权限的用户
DOMAIN	您的域名

下图说明了这些标签和字符串：

图 4-1 自定义联结的语法

驱动程序： Exchange 5.5.drvset.novell  
服务器： S3K-NDS.Vmp

```
XML 编辑器:  启用 XML
<?xml version="1.0" encoding="UTF-8"?>
<driver-config name="Exchange 5.5">
  <driver-options>
    <x-ldap-server display-name="Exchange LDAP Server" id="107"></x-ldap-server>
    <x-remote display-name="Create NT Security Account 0=Yes 1=No" id="108">0</x-remote>
    <x-server display-name="Exchange Server" id="109"></x-server>
    <x-site display-name="Exchange 站点: " id="110"/>/o=/ou=</x-site>
    <authoritative-bind display-name="Authoritative Bind:" id="111">Yes</authoritative-bind>
    <hiddenObjectBind id="112">cn=Administrator,dc=DOMAIN,cn=admin</hiddenObjectBind>
  </driver-options>
  <subscriber-options>
    <x-domain display-name="NT Domain Server" id="113"></x-domain>
  </subscriber-options>
  <publisher-options>
    <x-publishInterval display-name="Polling Interval (seconds)" id="114">10</x-publishInterval>
  </publisher-options>
</driver-config>
```

4 单击两次 《确定》。

然后， Exchange 驱动程序使用标签中的字符串作为联结的用户。

同时，搜索过滤器中将加入另一个禁止已删除对象的值。

如果存在此自定义标签，它会覆盖授权联结标签。如果不存在，则授权联结优先。如果两个标签都不存在，则使用匿名联结。

## 4.6 指定 LDAP 端口

如果更改了 Exchange Server 端口号的默认值 389，则需要配置 Identity Manager Driver for Exchange，使其查看服务器使用的端口。

- 1 在 《驱动程序参数》 部分中，单击 《编辑 XML》。
- 2 单击 《启用 XML 编辑》。
- 3 在 <driver-options> 部分中，添加指定不同端口号的标签（<ldap-port></ldap-port>）和值（如 391）。

驱动程序： Exchange 5.5.drvset.novell  
服务器： S3K-NDS.Vmp

```
XML 编辑器:  启用 XML
<?xml version="1.0" encoding="UTF-8"?>
<driver-config name="Exchange 5.5">
  <driver-options>
    <x-ldap-server display-name="Exchange LDAP Server" id="115"></x-ldap-server>
    <x-remote display-name="Create NT Security Account 0=Yes 1=No" id="116">0</x-remote>
    <x-server display-name="Exchange Server" id="117"></x-server>
    <x-site display-name="Exchange 站点: " id="118"/>/o=/ou=</x-site>
    <authoritative-bind display-name="Authoritative Bind:" id="119">Yes</authoritative-bind>
    <hiddenObjectBind id="120">cn=Administrator,dc=DOMAIN,cn=admin</hiddenObjectBind>
    <ldap-port id="121">391</ldap-port>
  </driver-options>
```

4 单击两次 《确定》。

# 排查驱动程序错误

本节提供了以下信息：

- ◆ “查错” 在第 29 页
- ◆ “驱动程序错误讯息” 在第 29 页

## 5.1 查错

- ◆ 布局策略中使用的 Exchange 目录名区分大小写。
- ◆ 如果 Exchange 和 Identity Vault 在同一台机器上运行，则必须禁用 Identity Vault LDAP 服务器或将端口指派从端口 389 更改为其它端口。
- ◆ 如果在 XML 中遇到语法错误，请使用 Identity Manager 和万维网浏览器来校验语法。
- ◆ 您指定的鉴定身份凭证应该属于具有 Exchange 目录权限的 NT 帐户 / 域。
- ◆ CN 和对象类不应位于过滤器中。
- ◆ 如果过滤器中有无效的特性（例如，未定义纲要映射的一个特性），则会出现以下情况：
  - ◆ 在每个巡回检测循环中，发布者无法同步包含无效特性的类，并显示错误，指出存在不受支持的特性。
  - ◆ 驱动程序仍可启动。
  - ◆ 除非引用了无效特性，否则订购者通道仍能正常工作。引用无效特性的任务将导致错误，并且不会成功完成。

样本驱动程序配置支持 Exchange 中的标准特性，因此只有已添加到 Exchange 中的自定义特性会出现该问题。

- ◆ Identity Manager Driver for Exchange 支持以下类：
  - ◆ 分发列表
  - ◆ 远程
  - ◆ 邮箱

## 5.2 驱动程序错误讯息

以下是驱动程序可能返回的错误讯息的列表：

- ◆ USN Cache Initialized from disk（从磁盘初始化 USN 超速缓存）

这是驱动程序初始化开始时出现的信息性讯息。此讯息表明驱动程序的上一个状态是从磁盘读取的。

- ◆ USN Cache could not be initialized. Most likely reason:Insufficient memory.（无法初始化 USN 超速缓存。最可能的原因是：内存不足。）

上一个驱动程序状态未正确初始化。这意味着另一个进程对注册表或驱动程序配置文件进行了处理。如果您意外删除了某个驱动程序配置文件，则可能会发生这种情况。这会导致事件数据丢失。

- ◆ DAPIStart() failed. Please check the Event Log for details. Returned error code = (DAPIStart() 失败。请检查事件日志以获取细节。返回错误代码 =)  
这通常说明 Exchange Server 已关闭或无法连接。NT 应用程序事件日志应该包含更详细的错误说明。
- ◆ DAPIStart() encountered non fatal error. Please check the Event Log for details. Returned error code = (DAPIStart() 遇到非致命错误。请检查事件日志以获取细节。返回错误代码 =)  
Exchange 返回警告时会返回此错误讯息。返回的警告记录在 NT 应用程序事件日志中。
- ◆ Call to Import function failed. Likely cause- bad XML or too little memory. (调用导入函数失败。可能的原因 – XML 错误或内存太少。)
- ◆ Subscriber Import attempt failed. Please check the NT Event Log for details. Returned error code = (订购者导入尝试失败。请检查 NT 事件日志以获取细节。返回错误代码 =)  
尝试写入事件日志未成功。
- ◆ Subscriber Import attempt encountered non critical error. Please check the NT Event Log for details. Returned error code = (订购者导入尝试遇到非严重错误。请检查 NT 事件日志以获取细节。返回错误代码 =)
- ◆ A bad XML document was sent to the driver. Critical error in the Subscriber XML document. (向驱动程序发送了错误的 XML 文档。订购者 XML 文档中有严重错误。)
- ◆ A bad XML document was sent to the driver. The subscriber could not process the input node. (向驱动程序发送了错误的 XML 文档。订购者无法处理输入节点。)
- ◆ A bad XML document was sent to the driver. An unsupported operation type was received. (向驱动程序发送了错误的 XML 文档。收到的操作类型不受支持。)
- ◆ A bad XML document was sent to the driver. The operation node could not be processed. (向驱动程序发送了错误的 XML 文档。无法处理操作节点。)
- ◆ Bad Subscriber filter or Subscriber filter contains an unsupported attribute. Please check the Subscriber filter. (错误的订购者过滤器或订购者过滤器包含不受支持的特性。请检查订购者过滤器。)  
向订购者过滤器添加了不受支持的特性。请使用文件 ATTRIBUTES.TXT (位于 NT\DIRXML\DRIVERS\EXCHANGE\RULES 目录中) 中受支持特性的列表校验发布者过滤器。
- ◆ Could not log in to Exchange with the specified credentials. Driver will not start. (无法使用指定的身份凭证登录到 Exchange。驱动程序无法启动。)  
提供的鉴定身份凭证不正确。指定的身份凭证应该属于具有 Exchange 目录权限的 NT 帐户 / 域。
- ◆ NT Event handles could not be created. The System could be low on memory (无法创建 NT 事件句柄。系统内存可能不足)
- ◆ An expected initialization parameter was missing from the parameter list. (参数列表中缺少所需的初始化参数。)  
缺少一个或多个初始化参数。尝试重新启动。如果问题仍然存在，请尝试重新键入初始化参数。
- ◆ Could not allocate memory. (无法分配内存。)
- ◆ Failed to initialize the base of the USN cache. Driver will not start. (未能初始化 USN 超速缓存的基址。驱动程序无法启动。)