Novell Identity Manager Driver for LDAP

1.9.2

www.novell.com

实施指南

2006 年 5 月 25 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。

Novell, Inc. 拥有本文档所述产品中所含技术的知识产权。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

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

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

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

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

读者

本指南适用于使用 Identity Manager Driver for LDAP 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) 上 Identity Manager 驱动程序部分的 《*Identity Manager Driver for LDAP*》。

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)。

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 LDAP 简介

1

1.1 新功能

表 *1-1* 发布功能的摘要

功能	LDAP 驱动程序版本	说明
支持 PasswordModify 扩展操作	1.9	Identity Manager Driver for LDAP 支持 RFC 3062 中定义的 PasswordModify 扩展操作。 如果您使用的 LDAP 目录支持 PasswordModify 扩展操作 （如 OpenLDAP），那么当在订购者通道上设置或修改口令时，Driver for LDAP 将使用该扩展操作。 如果 LDAP 目录不支持 PasswordModify 扩展操作，那么 Driver for LDAP 将为 UserPassword 特性设置一个值，就像先前版本的驱动程序那样。该值会被安全散列和储存。 此功能无需您进行任何配置。此驱动程序能够检测 LDAP 服务器是否支持此操作。
控制是否将 ;binary 选项添加到特性名称中	1.9.2	订购者通道参数控制在对值进行编码时是否将 ;binary 选项添加到特性名称中。请参见 “LDAP 订购者设置”在第 26 页 。
控制是否同步初始搜索结果	1.9.2	LDAP-Search 发布方法的参数控制是同步初始搜索结果还是只同步后续更改。请参见 “LDAP 发布者设置：LDAP-Search 方法”在第 30 页 。

1.2 计划更新

在未来的更新中计划包括下列增强功能：

- 支持发布者通道移动事件
- 当 LDAP 服务器为 Sun* 目录服务器时，支持发布者通道口令同步。

  通过更新的驱动程序和 Sun 目录插件提供支持。您需要在 Sun 目录中安装和配置该插件。

1.3 术语变更

下列术语与早期版本中的术语有所不同：

表 *1-2* 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）

1.4 驱动程序概述

Identity Manager Driver for LDAP 可以同步 Identity Vault 和 LDAP 兼容目录之间的数据。此驱动程序可以在运行 Identity Vault 的所有平台上 （包括 Windows*、 NetWare® 、 Linux*、Solaris* 和 AIX*）运行。此外，此驱动程序还可以在运行 Metadirectory 服务器或 Identity Manager 远程装载程序的任何位置运行。

此驱动程序使用轻量级目录访问协议来双向同步 Identity Vault 与已连接的 LDAP 兼容目录之间的更改。

由于这种灵活的通讯模式，此驱动程序可以和与 LDAP 兼容的、在不受 Identity Vault 支持的平台 （例如 HP-UX*、 OS/400 和 OS/390）上运行的目录同步。

此驱动程序可以使用两种发布方法的任何一种来识别数据更改，并通过 Identity Manager 将这些数据更改发送给 Identity Vault。

- changelog 方法

  如果有更改日志，此方法是首选方法。可以在以下各项中找到更改日志：

  - Netscape* Directory Server
  - iPlanet* Directory Server
  - IBM* SecureWay Directory
  - Critical Path* InJoin* Directory
  - Oracle* Internet Directory

  请参见 “LDAP 发布者设置：changelog 和 LDAP-Search 方法”在第 27 页 和 “LDAP 发布者设置：仅 changelog 方法”在第 28 页 。

- LDAP-Search 方法

  某些服务器不使用 changelog 机制。LDAP-Search 方法使 LDAP 驱动程序可以将有关 LDAP 服务器的数据发布到 Identity Vault。

  不需要其它软件，也不需要更改 LDAP 兼容目录。

  请参见 “LDAP 发布者设置：LDAP-Search 方法”在第 30 页

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》。

1.5 驱动程序默认配置

本节讨论了特定于此驱动程序的实施、增添的内容或异常。有关 Identity Manager 基础知识的信息，请参见 《*Novell Identity Manager 3.0* 管理指南》。

1.5.1 数据流

本节提供了有关控制数据流的通道、过滤器和策略的信息。

出版者通道和订购者通道

此驱动程序支持 《发布者》通道和 《订购者》通道：

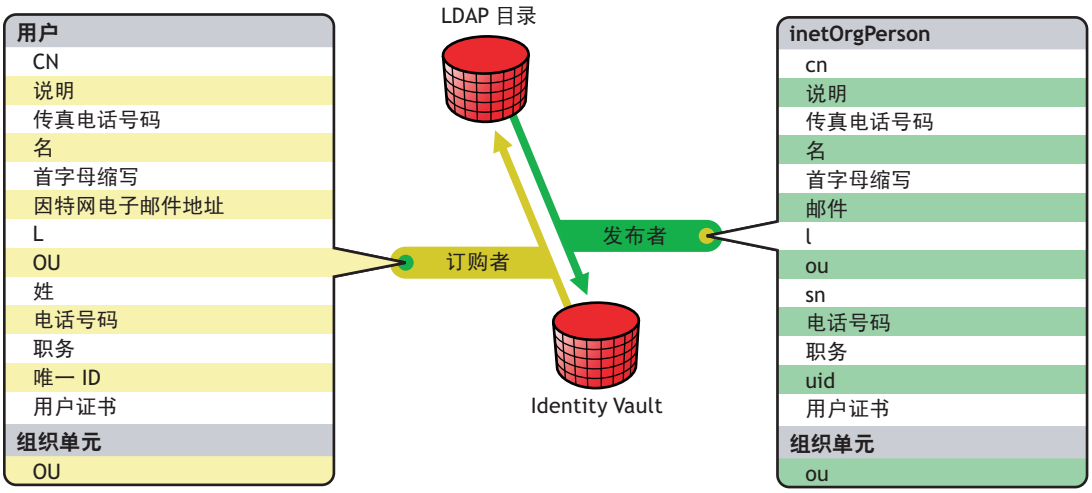
- 发布者通道从 LDAP 目录更改日志或 LDAP 搜索结果中读取信息，并通过 Metadirectory 引擎将这些信息提交给 Identity Vault。

  默认情况下，发布者通道每 20 秒对日志进行一次检查，从第一个未处理的条目开始，每次可处理多达 1000 条。
- 订购者通道检查 Identity Vault 对象的添加和修改，并发出更改 LDAP 目录的 LDAP 命令。

过滤器

Identity Manager 使用过滤器来控制共享哪些对象和特性。LDAP 驱动程序的过滤器默认配置允许共享对象和特性，如下图所示：

图 ***1-1*** *LDAP* 驱动程序过滤器



策略

策略用于控制驱动程序和 Identity Vault 之间的数据同步。LDAP 驱动程序附带有两个用于设置策略的预配置选项。

- 《平面》选项可为两个目录中的用户实施平面结构。

如果使用该配置，在一个目录中创建用户对象后，它们会被放置在为另一个目录进行驱动程序设置过程中指定的树枝根中。（树枝名称在 Identity Vault 和 LDAP 目录中不必相同。）更新现有对象时，将保留其环境。

- 《镜像》选项将两个目录中的分级结构进行匹配。

  如果使用该配置，在一个目录中创建用户对象后，它们会被放置在另一个目录中镜像树枝的匹配分级级别中。更新现有对象时，将保留其环境。

除了布局策略以及平面配置不同步组织单元对象这两点之外，这些选项的策略设置是相同的。

下表提供了有关默认策略的信息。这些策略及其包含的每条规则都可以通过 Novell iManager 来自定义，如第 4 章 “自定义 LDAP 驱动程序”在第 25 页中所述。

表 ***1-3*** 默认策略

策略	说明
映射	将 Identity Vault 用户对象和所选属性映射到 LDAP inetOrgPerson。 将 Identity Vault 组织单元映射到 LDAP organizationalUnit。 默认情况下，将映射十多条标准属性。
创建发布者	指定为了在 Identity Vault 中创建用户，必须定义 cn、 sn 和邮件特性。要创建组织单元，必须定义 ou 特性。
发布者布局	如果选择 《简单》布局选项，在 LDAP 目录中创建的新用户对象会被放置在导入驱动程序配置时指定的 Identity Vault 中的树枝中。用户对象将以 cn 的值命名。 如果选择 《镜像》布局选项，在 LDAP 目录中创建的新用户对象会被放置在一个 Identity Vault 树枝中 （该树枝镜像对象的 LDAP 树枝）。
匹配	指定当电子邮件特性匹配时， Identity Vault 中的用户对象与 LDAP 目录中的 inetOrgPerson 对象相同。
创建订购者	指定为了在 LDAP 目录中创建用户，必须定义 CN、姓氏和因特网电子邮件地址特性。要创建组织单元，必须定义 OU 特性。
订购者布局	如果在导入驱动程序配置过程中选择 《平面》布局选项，则根据在导入过程中指定的值在 Identity Vault 中创建新用户对象。 如果在导入驱动程序配置过程中选择 《镜像》布局选项，在 Identity Vault 中创建的新用户对象会被放置在一个 LDAP 目录树枝中 （该树枝镜像对象的 Identity Vault 树枝）。

升级

2

2.1 升级驱动程序 Shim

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。新的驱动程序 Shim 可以运行 DirXML® 1.*x* 配置，无需进行任何更改。

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。

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。查看正在使用的驱动程序版本的所有 TID 和产品更新。

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。

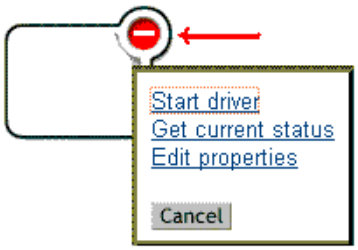
可以在安装 Metadirectory 引擎的同时，或者在安装该引擎后执行此操作。请参见第 3 章 “安装 LDAP 驱动程序”在第 11 页 。

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 9 页 。

2.2 升级驱动程序配置

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 （无需做任何更改）。

但是，如果要利用新功能，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 格式并向其添加策略。

- 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。
- 要转换现有驱动程序配置，以便可以使用新的 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》。
- 要向现有的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》。

安装 LDAP 驱动程序

3

3.1 计划考虑事项

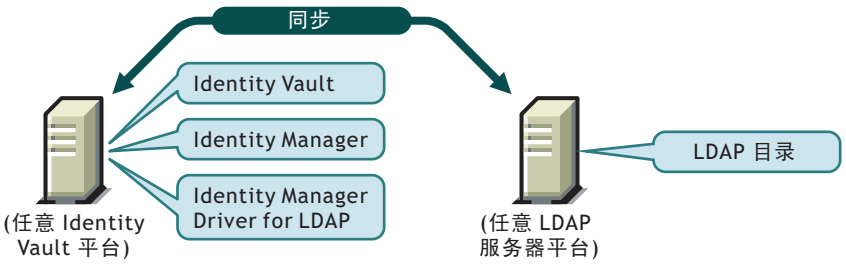
LDAP Driver for Identity Manager 可以与大多数兼容 LDAP v3 的 LDAP 服务器协同工作。此驱动程序已被写进 LDAP 的 RFC 2251 规范中。有关兼容性问题的信息，请参见“LDAP v3 兼容性”在第 39 页。

3.1.1 LDAP 驱动程序的安装位置

Identity Manager 驱动程序可以与 Identity Vault 和 Metadirectory 引擎安装在同一台计算机上。这种安装称作本地配置。

在本地配置中，将 LDAP 驱动程序与 Identity Vault 和 Metadirectory 引擎安装在同一台计算机上，如下图所示：

图 *3-1* 本地配置



如果由于平台或策略限制而难以采用本地配置，则可以将 Identity Manager 驱动程序安装在承载目标应用程序的计算机上。这种安装称作远程配置。

虽然远程配置可以安装 LDAP 驱动程序，但是由于下列原因，它几乎没有其它灵活性：

- 此驱动程序可以在任何 Identity Vault 平台上运行。
- 此驱动程序可以通过 LDAP 协议与任何联网平台上的 LDAP 服务器通讯。

3.1.2 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 LDAP（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。

3.1.3 要收集的信息

安装和设置过程中，系统将提示您提供如下信息：

- 使用 《平面》还是 《镜像》选项来同步分级结构。请参见 “策略”在第 7 页 。
- 要存放已同步对象的 Identity Vault 和 LDAP 目录树枝。
- 要指派为驱动程序的安全性等效的 Identity Vault 用户对象以及不要同步的对象。
- 用于提供对 LDAP 目录的驱动程序访问的 LDAP 对象和口令。

请参见 “导入样本驱动程序配置文件”在第 21 页 中的表。

3.1.4 有关 LDAP 数据源的假定

如果使用发布者通道将有关在 LDAP 目录中所做更改的数据发送至 Identity Vault，那么必须了解驱动程序用来发布数据所采用的两种方法：

- changelog 方法

  更改日志是 LDAP 目录中的一种机制。更改日志可以为驱动程序提供 LDAP 事件信息。如果有更改日志，此方法是首选方法。

- LDAP-Search 方法

  该方法使 LDAP 驱动程序可以将有关不使用更改日志的 LDAP 服务器的数据发布到 Identity Vault。

3.2 系统前提条件

- ❑ Novell® Identity Manager
- ❑ Identity Manager 或更高版本的系统要求
- ❑ 如果使用 changelog 方法，则选择下列 LDAP 目录之一：
  - Netscape Directory Server 4.*x* 或 6
  - iPlanet Directory Server 5.0 或更高版本
  - IBM SecureWay Directory 3.2、 4.1.1 或 5.1
  - Critical Path InJoin Directory 3.1
  - Oracle Internet Directory 2.1.1 或更高版本
  - Sun ONE* 5.2
  - 与 LDAP 版本 3 兼容的目录

3.3 安装

- “安装 LDAP 驱动程序”在第 13 页

- “设置驱动程序”在第 18 页

3.3.1 安装 LDAP 驱动程序

可以在安装 Metadirectory 引擎后单独安装此驱动程序。

- “在 Windows 上安装”在第 13 页
- “在 NetWare 上安装”在第 15 页
- “在 Linux、 Solaris 或 AIX 上安装”在第 16 页

在 **Windows** 上安装

将 Identity Manager Driver for LDAP 安装在 Windows NT* 2003 服务器或带有 Support Pack 2 的 Windows NT 2000 上。

1. 从 Identity Manager 2.0 CD 或下载映象运行安装程序。

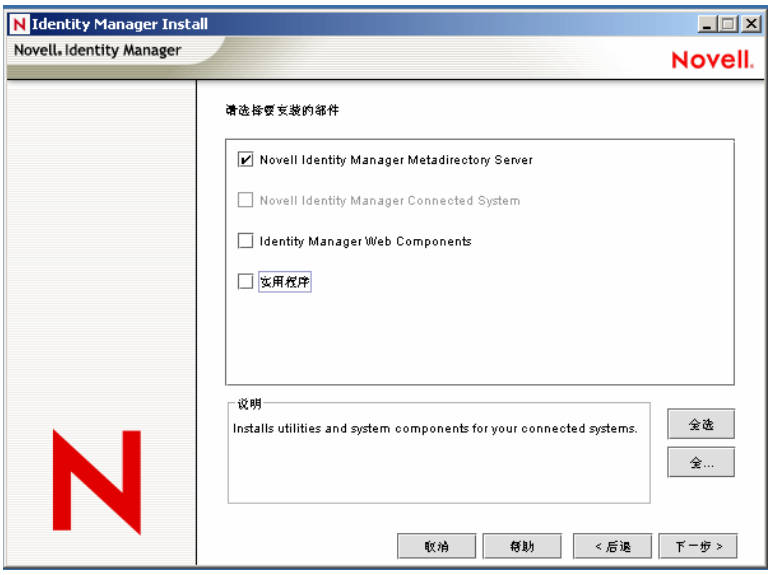
   可下载文件位于 Novell 下载 (http://download.novell.com/index.jsp)。

   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》。

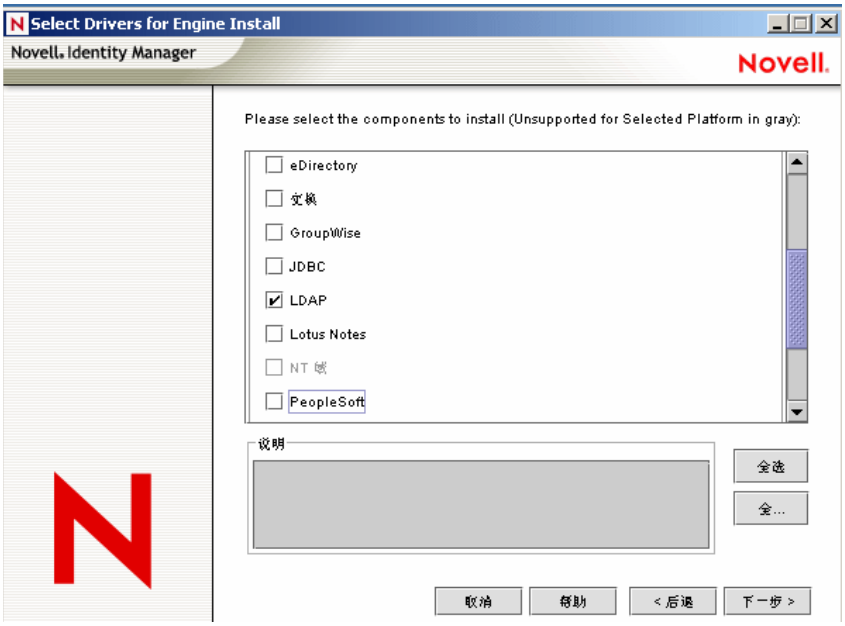
   此对话框提供有关以下两项的信息：
   - Metadirectory 服务器
   - 已连接 Identity Manager 的服务器系统
4. 在第二个 《Identity Manager 概述》对话框中，查看其中信息，然后单击 《下一步》。

   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 Select Drivers for Engine Install （选择要安装的引擎驱动程序）对话框中，仅选择 *LDAP*，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 《纲要扩展》对话框中，键入用户名和口令，然后单击 《下一步》。

要使口令有效，必须具有对根的权限。

9 在 《摘要》对话框中，查看选定的选项，然后单击 《完成》。

10 在 《安装完毕》对话框中，单击 《关闭》。

在安装后，必须按 “设置驱动程序”在第 18 页 中的说明来配置此驱动程序。

在 **NetWare** 上安装

1 在 NetWare® 服务器上，插入 Identity Manager 3 CD 并将其作为卷装入。

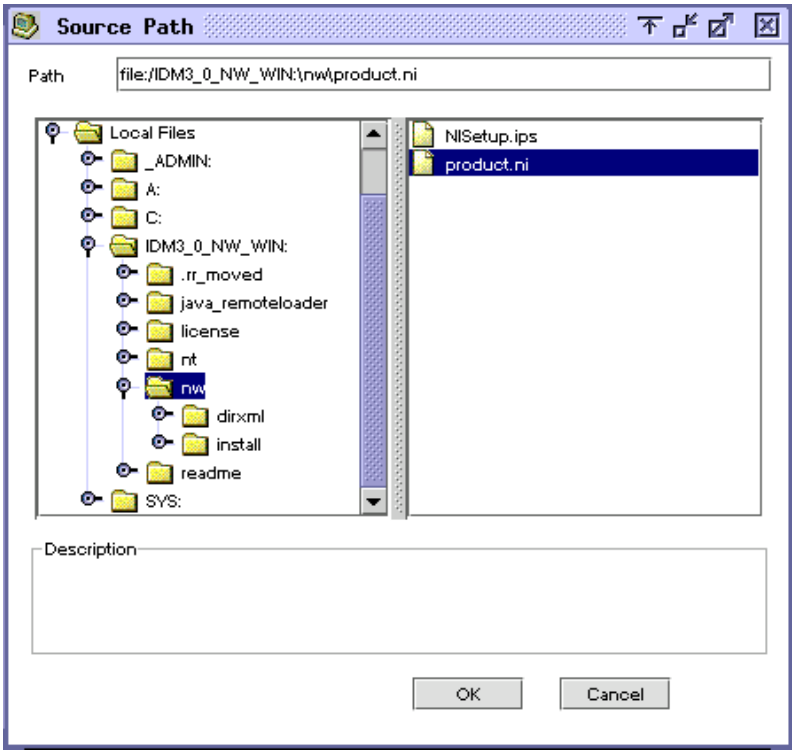
要装入此 CD，请输入 m cdrom。

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 找到并展开先前装入的 CD 卷。

5b 展开 nw 目录，选择 product.ni，然后单击 《确定》两次。

6 在 《欢迎使用》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 在 《选择要安装的引擎驱动程序》对话框中，仅选择 《定界文本》。

取消选择以下项：

- Metadirectory 引擎
- 除 LDAP 之外的所有驱动程序

9 单击 《下一步》。

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 《纲要扩展》对话框中，键入用户名和口令，然后单击 《下一步》。

12 在 《摘要》页中，查看选定的选项，然后单击 《完成》。

13 单击 《关闭》。

在安装后，必须按 “设置驱动程序”在第 18 页 中的说明来配置此驱动程序。

在 Linux、 Solaris 或 AIX 上安装

默认情况下，在安装 Metadirectory 引擎的同时会安装 Identity Manager Driver for LDAP。如果那时未安装此驱动程序，本节将帮助您安装它。

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 3.0 CD 并装入它。

通常，此 CD 将自动装入。但是，也可以手动装入。例如，对于 SUSE® ，请键入 mount /media/cdrom。

3 更改到安装目录。

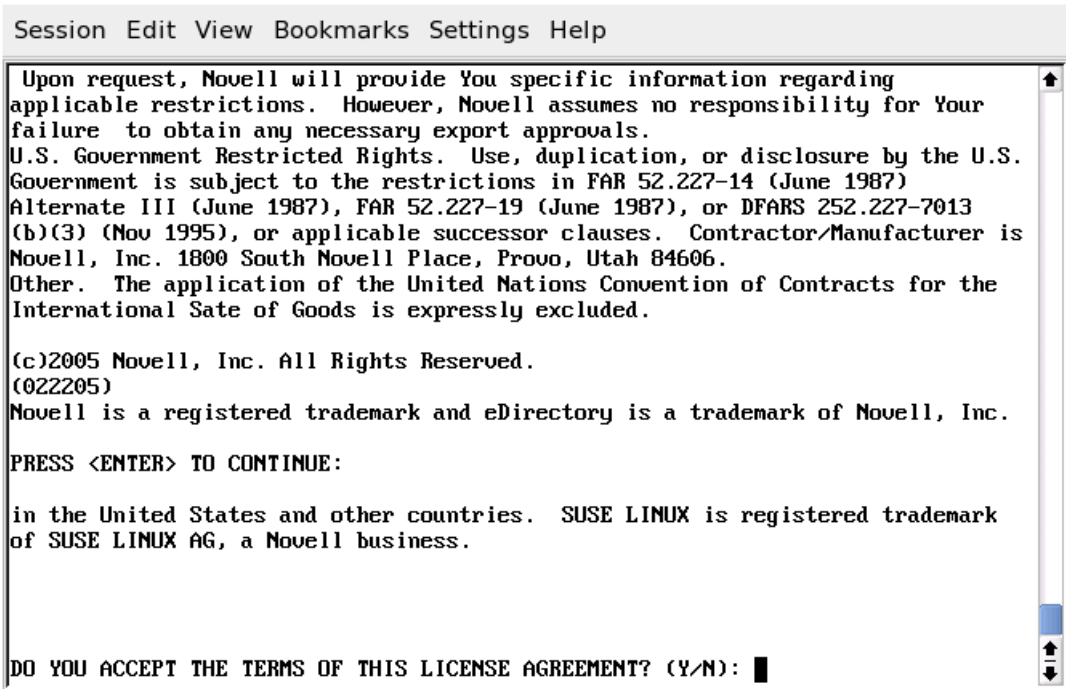
平台	路径
Red Hat	/mnt/cdrom/linux/setup/
SUSE	/media/cdrom/linux/setup/
Solaris	/cdrom/solaris/_idm_2/setup/
AIX	/media/cdrom/aix/setup/

4 运行安装程序。

例如，对于 SUSE，请运行 ./dirxml_linux.bin。

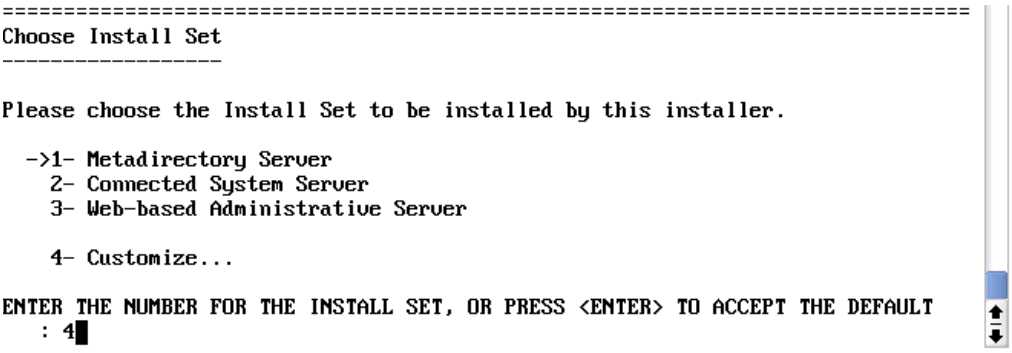
5 在 《介绍》部分中，按 Enter 键。

6 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）提示，键入 y 以接受许可协议，然后按 Enter 键。



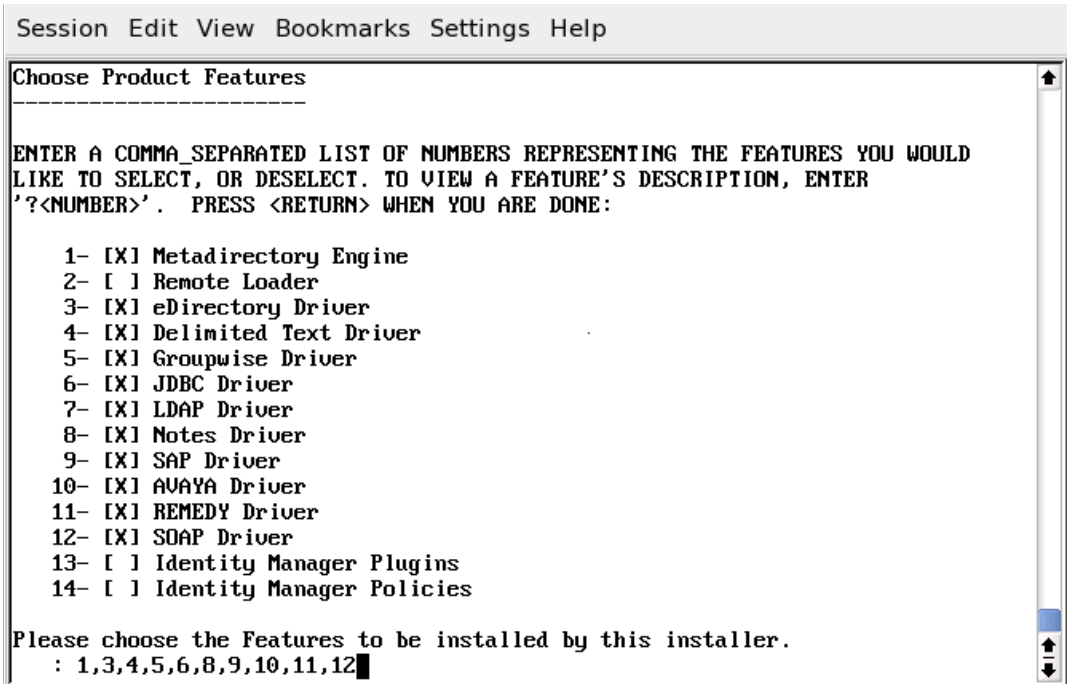
7 在 *Choose Install Set*（选择安装集）部分中，选择 《自定义》选项。

键入 4，然后按 Enter 键。

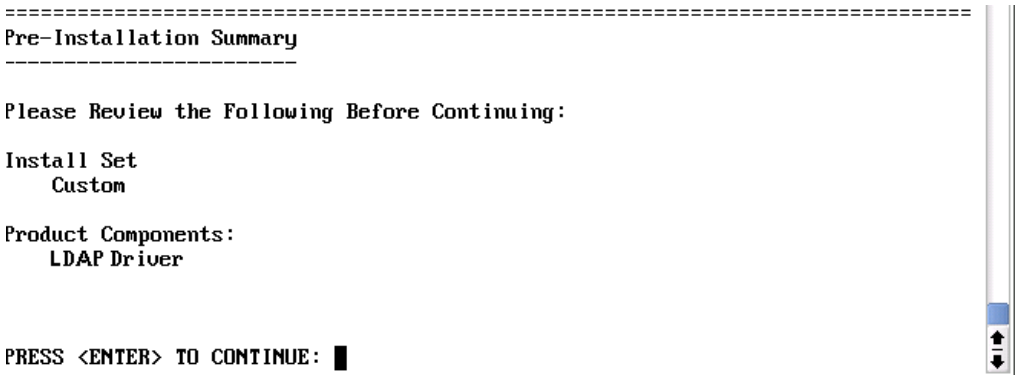


8 在 *Choose Product Features*（选择产品功能）部分中，取消选择除 LDAP 之外的所有功能，然后按 Enter 键。

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，请键入 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。

在安装后，必须按 “设置驱动程序”在第 18 页 中的说明来配置此驱动程序。

3.3.2 设置驱动程序

如果是升级现有的驱动程序，则无需设置。

如果第一次使用 LDAP 驱动程序，则需完成以下各节中的设置任务：

- “准备 LDAP 服务器”在第 19 页

- “导入样本驱动程序配置文件”在第 21 页
- “启动驱动程序”在第 23 页
- “迁移和重新同步数据”在第 23 页
- “激活驱动程序”在第 23 页

准备 LDAP 服务器

如果此驱动程序只用于将数据从 Identity Vault 同步到 LDAP 服务器 （在订购者通道上）的数据，那么大多数 LDAP 服务器和应用程序均可运行 （无需任何其它配置）。

始终要创建一个具有必需权限的用户对象，以便驱动程序可以鉴定到 LDAP 服务器。

但是，如果需要将 LDAP 服务器上的项目更改同步回 Identity Vault （在订购者通道上），并且如果计划使用 changelog 方法，那么在运行此驱动程序之前，至少需要对 LDAP 服务器执行另外一个配置任务。校验是否启用了 LDAP 服务器的更改日志机制。

重要 **:** 如果 LDAP 服务器没有 changelog 机制，则使用 LDAP-Search 方法。否则，此驱动程序将无法发布此服务器的事件。

创建具有鉴定权限的 LDAP 用户对象

使用 changelog 发布方法时，此驱动程序尝试防止发生以下回送情况：在订购者通道上发生的事件被发送回发布者通道上的 Metadirectory 引擎。但是， LDAP-Search 方法依赖于 Metadirectory 引擎来防止回送。

如果使用 changelog 方法，此驱动程序防止发生回送的方法之一是在更改日志中查找哪位用户做出了更改。如果做出更改的用户就是该驱动程序用于鉴定的用户，发布者将假定更改是由驱动程序的订购者通道做出的。

注释 **:** 如果使用 Critical Path InJoin 服务器，那么在该服务器上的更改日志实施将受到一定限制，因为服务器未提供可以启动更改的对象的 DN。因此，创建者 / 修改者 DN 不能用于确定更改是否来自 Identity Vault。

这种情况下，在更改日志中找到的所有更改都由发布者发送至 Metadirectory 引擎，同时优化 / 修改将丢弃不必要或重复的更改。

要防止发布者通道丢弃合法的更改，请确保未将该驱动程序用于鉴定的用户对象用于任何其它目的。

例如，假设使用的是 Netscape Directory Server，并已将此驱动程序配置为使用管理员帐户 CN=Directory Manager。如果要手动在 Netscape Directory Server 中进行更改并同步此更改，则无法利用 CN=Directory Manager 登录并进行更改，而必须使用另一个帐户。

避免此问题：

1. 创建此驱动程序专用的用户帐户。
2. 指派该用户帐户权限以查看更改日志，并进行希望此驱动程序能够实现的更改

   例如，在 VMP 公司，为驱动程序创建名为 uid=ldriver,ou=Directory Administrators,o=lansing.vmp.com 的用户帐户。然后，通过使用 LDAPModify 工具或 Novell 导入 / 转换 / 导出实用程序将下列 LDIF 应用到服务器，从而将适当的权限指派给此用户帐户。

```
# give the new user rights to read and search the changelog


dn: cn=changelog


changetype:modify


add: aci


aci: (targetattr = "*")(version 3.0; acl "LDAP DirXML Driver";
allow (compare,read,search) userdn = "ldap:///
uid=ldriver,ou=Directory Administrators,o=lansing.vmp.com"; )


-


# give the new user rights to change anything in the
o=lansing.vmp.com container


dn: o=lansing.vmp.com


changetype:modify


add: aci


aci: (targetattr = "*")(version 3.0; acl "LDAP DirXML Driver";
allow (all) userdn = "ldap:///uid=ldriver,ou=Directory
Administrators,o=lansing.vmp.com"; )


-
```

启用更改日志

更改日志是 LDAP 服务器的一部分，它使此驱动程序能够识别需要从 LDAP 目录发布到 Identity Vault 的更改。受此驱动程序支持的 LDAP 目录支持 changelog 机制。

默认情况下， Critical Path InJoin 和 Oracle Internet Directory 都启用了更改日志。除非更改日志已关闭，否则不需要执行其它任何步骤即可启用它。

IBM SecureWay、 Netscape Directory Server 和 iPlanet Directory Server 需要您在安装后启用更改日志。有关启用更改日志的信息，请参考适用于您的 LDAP 目录的文档。

提示 **:** iPlanet 更改日志需要您启用 Retro Changelog 插件。

导入样本驱动程序配置文件

- “使用 iManager 导入”在第 21 页
- “使用 Designer for Identity Manager 导入”在第 22 页

使用 iManager 导入

按照 《*Novell Identity Manager 3.0* 管理指南》中的 《创建和配置驱动程序》中导入驱动程序的说明来导入 LDAP 驱动程序配置。

在导入过程中，提供驱动程序配置的下列信息。

表 ***3-1*** *LDAP* 驱动程序的设置

字段	说明
驱动程序名	要指派到此驱动程序或要更新其配置的现有驱动程序的 Identity Vault 对象名。
布局类型	如果选择 《简单》布局选项，在 LDAP 目录中创建的新用户对象会被放置在导入驱动程序配置时指定的 Identity Vault 中的树枝中。用户对象将以 cn 的值命名。 如果选择 《镜像》布局选项，在 LDAP 目录中创建的新用户对象会被放置在一个 Identity Vault 树枝中 （该树枝镜像对象的 LDAP 树枝）。
eDirectory 树枝	应在其中创建新用户的 Identity Vault 中的树枝。 如果此树枝不存在，则必须在启动驱动程序之前创建它。 对于 LDAPMirrorSample.xml 配置，该目录是驱动程序布局策略的起始点。从属树枝的名称应与 LDAP 镜像树枝中的从属树枝的名称相同。 对于 《平面》配置，该树枝包含所有用户对象。
LDAP 树枝	应在其中创建新用户的 LDAP 目录中的树枝。 如果此树枝不存在，则必须在启动驱动程序之前创建它。 对于 《平面》配置，该目录是驱动程序布局策略的起始点。 对于 LDAPSimplePlacementSample.xml 配置，该树枝包含所有用户对象。
LDAP 服务器	LDAP 服务器的主机名或 IP 地址以及端口。
LDAP 鉴定 DN	指定为 LDAP 驱动程序创建的管理员帐户的 LDAP DN。
LDAP 鉴定口令	LDAP 驱动程序管理员帐户的口令。可以通过在下一字段中重新输入该口令对其进行确认。 这是已鉴定用户的必需口令。 如果只有 LDAP 驱动程序使用 Directory Manager，那么默认的已鉴定用户可以正常运行。但是，如果该用户被用于任何其它目的，那么在驱动程序运行后可能需要更改默认设置。请参见 “创建具有鉴定权限的 LDAP 用户对象”在第 19 页 。
SSL	加密 LDAP 协议通讯。

字段	说明
配置数据流	• 《双向》意味着 LDAP 和 Identity Vault 都是在它们之间同步的数据的授权源。 • LDAP to eDirectory （LDAP 到 eDirectory）意味着 LDAP 是授权源。 • eDirectory to LDAP （eDirectory 到 LDAP）意味着 Identity Vault 是授权源。
Install Driver as Remote/Local （安装为远程 / 本地驱动程序）	选择 《远程》，可将驱动程序配置为用于远程装载程序服务；选择 《本地》，可将驱动程序配置为在本地使用。
远程主机名和端口	为此驱动程序指定主机名或 IP 地址以及端口号 （已在该主机上安装了远程装载程序服务且该服务正在运行）。默认端口为 8090。
驱动程序口令	远程装载程序使用驱动程序对象的口令向 Metadirectory 服务器鉴定自己的身份。驱动程序对象口令必须与 Identity Manager 远程装载程序上指定的驱动程序对象口令相同。
远程口令	该口令仅用于远程装载程序配置中，它允许远程装载程序鉴定到 Metadirectory 引擎。 远程装载程序口令用于控制对远程装载程序实例的访问。远程装载程序口令必须与指定为 Identity Manager 远程装载程序上的远程装载程序口令相同。
口令失败通知用户	当口令失败时，向指定用户发送电子邮件通知。
Enable Entitlements （启用权利）	选择 《是》或 《否》。因为这是一个设计决定，所以应在选择使用权利之前应该先对其进行了解。 有关权利的信息，请参见 *《Novell Identity Manager 3.0 管理指南》* 中的 《创建和使用权利》。

使用 Designer for Identity Manager 导入

可以使用 Designer for Identity Manager 导入 LDAP 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 *LDAP.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。有关这些设置的信息，请参见 “使用 iManager 导入”在第 21 页 中的表。
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。

   请参见 *《Designer for Identity Manager 3：管理指南》* 中的 《将项目部署到 Identity Vault 中》。

启动驱动程序

如果在配置过程中更改了默认数据位置，请确保在启动驱动程序之前新位置已存在。

1. 在 iManager 中，选择 *Identity Manager* > 《Identity Manager 概述》。
2. 在所属驱动程序集中找到此驱动程序。
3. 单击驱动程序图标右上角的驱动程序状态指示器，然后单击 《启动驱动程序》。

   如果有更改日志，那么驱动程序将处理更改日志中的所有更改。要强制初始同步，请参见 “迁移和重新同步数据”在第 23 页 。

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： 使您可以选择希望从 Identity Vault 迁移到 LDAP 服务器的树枝或对象。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。

  注释：当将数据从 Identity Vault 迁移到 LDAP 目录中时，可能需要更改您的 LDAP 服务器设置以允许迁移大量对象。请参见 “将用户迁移到 Identity Vault 中”在第 39 页 。

- 将数据迁移到 **eDirectory** 中： 使您可以定义 Identity Manager 用于将对象从 LDAP 服务器迁移到 Identity Vault 中的准则。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 Identity Vault 中。
- 同步： Identity Manager 在订购者类过滤器中查找并处理这些类的所有对象。关联对象被合并，为关联的对象作为添加事件进行处理。

使用其中的一个选项：

1. 在 iManager 中，选择 *Identity Manager* > 《Identity Manager 概述》。
2. 找到包含 Identity Manager Driver for LDAP 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。

激活驱动程序

在安装后的 90 天内激活驱动程序。否则，驱动程序将无法运行。

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》。

自定义 LDAP 驱动程序

4

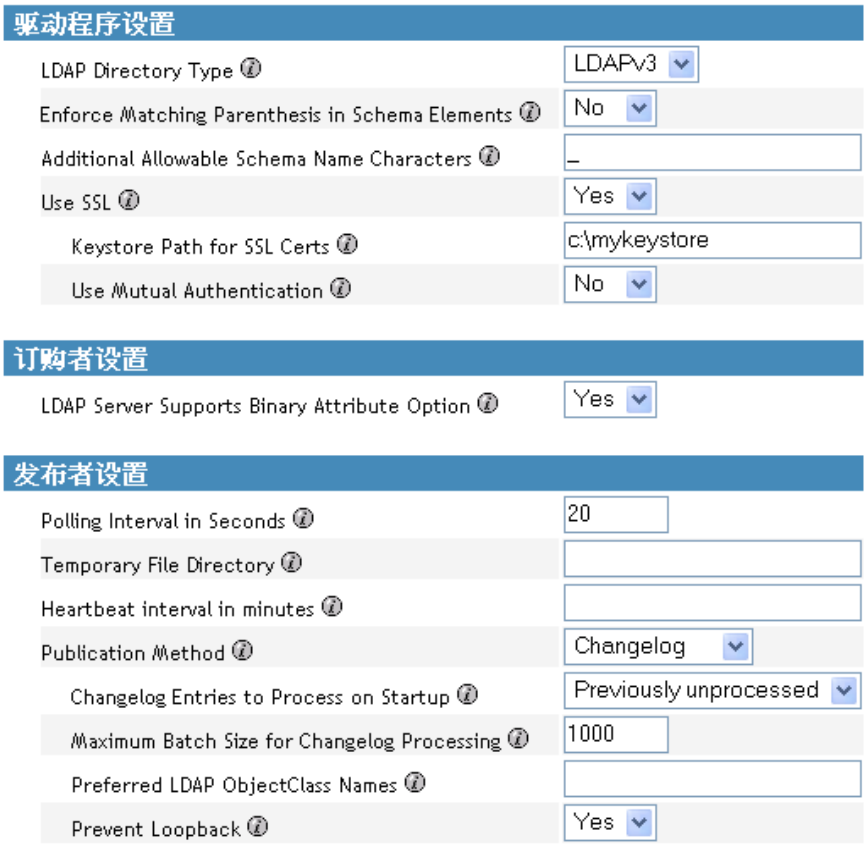
LDAP 驱动程序包括示例配置，您可以使用这些配置作为您部署的起点。但是，大多数 Identity Manager 部署都需要您修改这些示例。

本节包括：

注释：在自定义数据同步时，必须采用要同步的操作系统和帐户所支持的标准和约定。如果数据包含的字符在一个环境中有效而在另一环境中无效，则会导致错误。

4.1 控制从 LDAP 目录到 Identity Vault 的数据流

图 *4-1* 样本配置文件中的设置

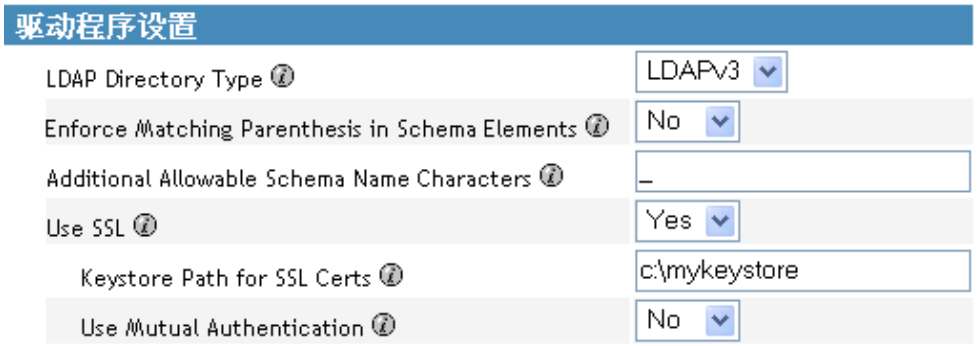


通过调整驱动程序的操作参数，可以调整驱动程序行为，使其符合您的网络环境要求。例如，您可能会发现默认发布者通道巡回检测间隔比同步需求所要求的间隔短。增大间隔可提高网络性能，并保持正确的同步。

如果 LDAP 服务器有更改日志，建议使用 changelog 发布方法。如果没有更改日志，则可以使用 LDAP-Search 发布方法。changelog 方法是首选方法。

4.1.1 LDAP 驱动程序设置

图 ***4-2*** *LDAP* 驱动程序设置

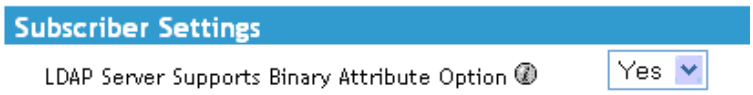


1. 在 iManager 中，选择 *Identity Manager* > 《Identity Manager 概述》，然后搜索驱动程序集。
2. 在驱动程序集中，单击 LDAP 驱动程序图标。
3. 在驱动程序视图中，再次单击 LDAP 驱动程序图标。
4. 滚动至 《驱动程序参数》。
5. 在 《驱动程序设置》部分中，选择所需选项。

   有关设置的信息，请单击信息图标。

4.1.2 LDAP 订购者设置

图 ***4-3*** *LDAP* 订购者设置



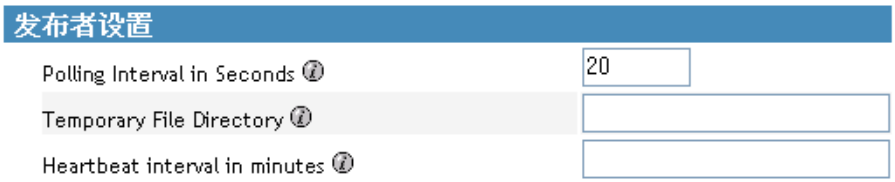
导入样本配置文件时，系统不会提示您进行此设置。但是，您可以在导入该文件后更改此设置。在 《订购者设置》部分中，选择所需选项。

默认设置为 《是》。大部分 LDAP 服务器都支持使用 RFC 2251 的 4.1.5.1 小节中规定的二进制特性选项。

如果不知道与此驱动程序相连接的 LDAP 服务器是否支持二进制特性选项，请选择 《是》。

4.1.3 LDAP 发布者设置：changelog 和 LDAP-Search 方法

图 *4-4* *LDAP* 普通发布者设置



有些设置同时适用于 changelog 和 LDAP-Search 发布方法 , 而有些设置仅适用于 changelog 发布方法。其它设置则仅适用于 LDAP-Search 发布方法。

巡回检测间隔 （秒）

驱动程序检查 LDAP 服务器的 changelog 或 LDAP-Search 方法的间隔。当找到新更改时，这些新更改会应用于 Identity Vault。

建议将巡回检测间隔设置为 120 秒。

临时文件目录

将此值设置为本地文件系统（驱动程序在其上运行）上的、用于写入临时状态文件的目录。如果未指定路径，则驱动程序将使用默认驱动程序路径。

表 *4-1* 临时文件目录

平台或环境	默认目录
eDirectory	DIB 文件目录
远程装载程序	远程装载程序的根目录

这些文件可以起到以下作用：

- 保持驱动程序的一致性 （即使在驱动程序关闭时）
- 防止搜索的数据量较大时内存不足

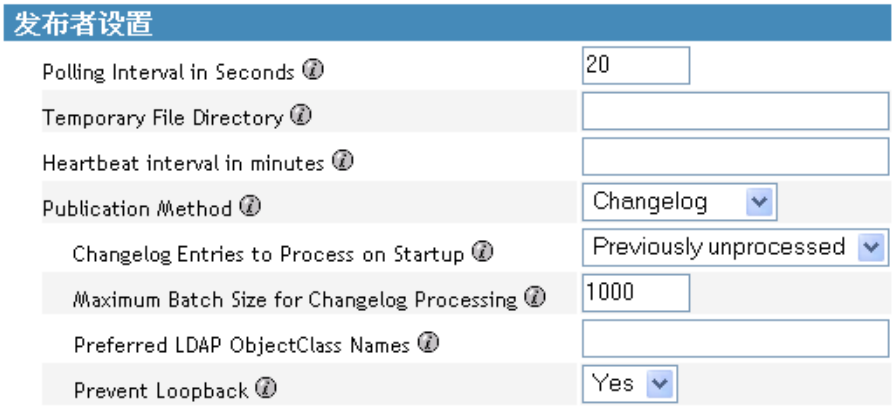
心跳间隔 （分）

要打开心跳，请键入数值。要关闭心跳，请将该字段保留为空。

有关驱动程序心跳的信息，请参见 《*Novell Identity Manager 3.0* 管理指南》中的 《添加驱动程序心跳》。

4.1.4 LDAP 发布者设置：仅 changelog 方法

图 *4-5 LDAP* 发布者通道上的 *changelog* 设置



启动时处理的 **changelog** 项目

此参数指定启动时要处理哪些项目。

- 全部：发布者尝试处理在更改日志中找到的全部更改，直到处理完全部更改。它会根据巡回检测速率处理新更改。
- 无：当驱动程序开始运行时，发布者不会处理任何已经存在的项目。它会根据巡回检测速率处理新更改。
- 未处理项：这是默认设置。如果驱动程序是第一次运行，则它会像 1- 《全部》一样，处理所有新更改。

  如果驱动程序以前已运行，则此设置会使发布者只处理从驱动程序上次运行到现在所产生的新更改。此后，它会根据巡回检测速率处理新更改。

当使用 changelog 方法时，驱动程序会查找批大小设置和 Prevent Loopback （防止回送）设置。

changelog 处理的最大批大小

当发布者通道处理来自 LDAP 更改日志的新项目时，发布者会请求大小为此值的批中的项目。如果更改日志中项目的数量小于此值，则会立即处理所有项目。如果大于此值，则会将项目分成大小为此值的批，分批连续处理。

首选 **LDAP** 对象类名称

Preferred LDAP ObjectClass Name （首选 LDAP 对象类名称）设置是用来指定发布者通道上首选对象类的可选驱动程序参数。

Identity Manager 要求使用单一对象类对所有对象都进行标识。但是，许多 LDAP 服务器和应用程序都可以为一个对象列出多个对象类。默认情况下，当 Identity Manager Driver for LDAP 在 LDAP 服务器或应用程序上找到被添加、删除或修改过的对象时，它会向 Metadirectory 引擎发送事件，并使用在纲要定义中具有最多继承级别的对象类来标识该对象。

例如，在 LDAP 中，能够标识用户对象的对象类有 inetorgperson、 organizationalperson、 person 和 top。inetorgperson 在纲要具有最多继承级别 （inetorgperson 从 organizationalperson 继承， organizationalperson 从 person 继承， person 从 top 继承）。默认情况下，驱动程序会将 inetorgperson 用作它向 Metadirectory 引擎报告的对象类。

如果要更改驱动程序的默认行为，可以添加 preferredObjectClasses 参数，该参数为可选驱动程序发布者参数。此参数的值可以是一个 LDAP 对象类，也可以是 LDAP 对象类列表 （以空格分隔）。

当此参数存在时， Identity Manager Driver for LDAP 会检查发布者通道中的每个对象，以查看是否包括列表中的某个对象类。它会按这些对象在 preferredObjectClasses 参数中显示的顺序来查找它们。如果它发现列出的某个对象类与 LDAP 对象的 objectclass 特性的某个值相匹配，则它会将该对象类用作它向 Metadirectory 报告的对象类。如果没有匹配的对象类，则它会采取其报告主要对象类的默认行为。

防止回送

《防止回送》参数只用于 changelog 发布方法。除了 Metadirectory 引擎中内置的回路阻止外， LDAP-Search 方法不防止回路。

发布者通道的默认行为是避免发送订购者通道所做的更改。发布者通道通过搜索 LDAP 更改日志的 creatorsname 或 modifiersname 特性来检测订购者通道的更改，以便查看进行更改的已鉴定项目是否与驱动程序用来鉴定到 LDAP 服务器的项目相同。如果相同，发布者通道会假定此更改是由驱动程序的订购者通道做出，从而不会同步更改。

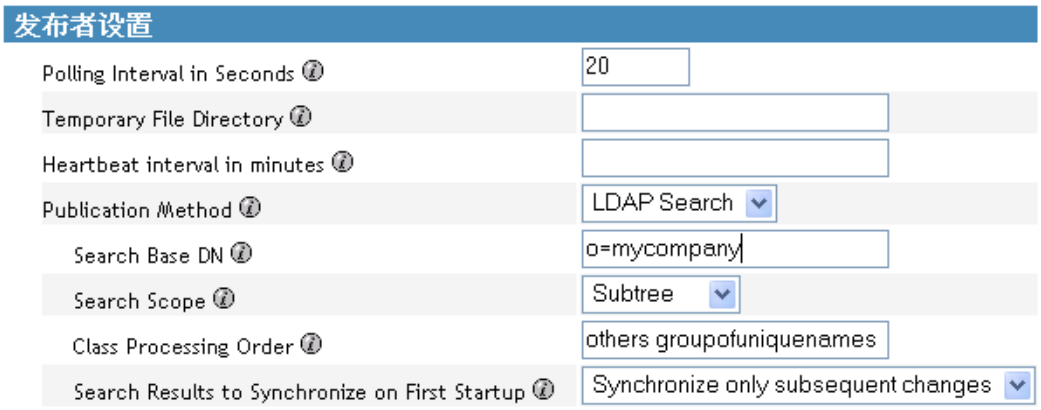
例如，您可能没有为此驱动程序配置订购者通道，但希望能够使用其它进程所用的相同 DN 和口令进行更改。

如果您确定要允许发生此类型的回送，请编辑驱动程序参数：

1. 在 iManager 中，选择 《Identity Manager 管理》 > 《Identity Manager 概述》。
2. 在所属驱动程序集中找到此驱动程序。
3. 单击此驱动程序以打开 《驱动程序概述》页，然后再次单击此驱动程序以打开 《更改对象》页。
4. 滚动至 《发布者设置》部分，然后将 《阻止回送》设置为 《否》。
5. 单击 《确定》，单击 《应用》，然后重新启动驱动程序，使此参数生效。

4.1.5 LDAP 发布者设置：LDAP-Search 方法

图 *4-6 LDAP 发布者通道的 LDAP-Search 设置*



过去，LDAP 驱动程序只能通过读取 LDAP 服务器的更改日志来检测该服务器中的更改。但是，有些服务器不使用 changelog 机制，这实际上不属于 LDAP 标准。在没有更改日志的情况下， LDAP 驱动程序以前无法将有关这些 LDAP 服务器的数据发布到 Identity Vault。

但是，LDAP-Search 发布方法不需要更改日志。此方法使用标准 LDAP 搜索，然后比较每个搜索间隔与下一间隔的结果来检测更改。

您可以将 LDAP-Search 发布方法用作传统 changelog 发布方法的替代方法。Identity Manager Driver for LDAP 对这两种方法都支持。但是， changelog 方法的性能较好，所以当有更改日志时， changelog 方法是首选方法。

如果没有更改日志，请设置下列参数：

- “搜索基本 DN”在第 30 页
- “搜索范围 （1 - 子树、 2 - 一级、 3- 基本）”在第 30 页
- “类处理顺序”在第 31 页
- “首次启动时同步的搜索结果”在第 31 页

搜索基本 **DN**

当使用发布者通道时，如果没有更改日志，则需要该参数。将该参数设置为巡回检测搜索起始树枝的 LDAP 判别名 (DN) （例如， ou=people,o=company）。

要使用更改日志，请将此参数保留为空。

搜索范围 （**1 -** 子树、 **2 -** 一级、 **3-** 基本）

指示巡回检测搜索的深度。此参数的默认值是搜索 《搜索基本 DN》所指向的整棵子树。

没有更改日志时，请使用此参数。

类处理顺序

当参照特性有问题时，发布者通道用来排列某些事件顺序的可选参数。该参数的值为 LDAP 服务器的类名称列表 （以空格分隔）。例如，为了确保先创建新用户，然后再将其添加到组，要求 interorgperson 在 groupofuniquenames 的前面。

Identity Manager Driver for LDAP 定义了一个特殊的类名称 《others》，用来表示除显式列出的类之外的所有类。

此参数的默认值是 《other groupofuniquenames》。

没有更改日志时，请使用此参数。

首次启动时同步的搜索结果

LDAP 驱动程序首次启动时，它会执行已定义的 LDAP 搜索。*Search Results to Synchronize on First Startup* （首次启动时同步的搜索结果）设置可定义是同步首次搜索结果，还是只同步后续更改。

《首次启动时同步的搜索结果》选项只在 《发布方法》参数设置为 *LDAP-Search* 时才会出现。导入配置文件时，系统不会提示您进行此设置。但是，您可以在导入文件后更改此设置。

1. 在 iManager 中，选择 *Identity Manager* > 《Identity Manager 概述》，然后搜索驱动程序集。
2. 在驱动程序集中，单击 LDAP 驱动程序图标。
3. 在驱动程序视图中，再次单击 LDAP 驱动程序图标。
4. 滚动至 《驱动程序参数》。
5. 在 《发布者设置》部分中，选择所需选项。

   默认设置为 *Synchronize only subsequent changes* （仅同步后续更改）。

4.2 配置数据同步

- “确定要同步哪些对象”在第 31 页
- “定义纲要映射”在第 32 页
- “在 Netscape 中定义对象替换”在第 33 页
- “使用 eDirectory 组和 Netscape”在第 34 页

4.2.1 确定要同步哪些对象

Identity Manager 使用发布者和订购者通道上的过滤器来控制要同步哪些对象，以及定义这些对象的授权数据源。

有关默认过滤器的图解，请参见 “过滤器”在第 7 页 。使用下列步骤可更改默认过滤器。

编辑发布者和订购者过滤器

1. 在 iManager 中，选择 *Identity Manager* > 《Identity Manager 概述》。
2. 在所属驱动程序集中找到此驱动程序。
3. 单击驱动程序，打开 《Identity Manager 驱动程序概述》页。

4 单击发布者或订购者过滤器图标，进行相应更改。

发布者过滤器必须包括 Identity Vault 必备特性。订购者过滤器必须包括 LDAP 服务器必需的特性。

除非两个目录中的类或特性名称相同，否则对于每个在过滤器中选定的对象和特性，《映射》策略必须有相应的项目。在映射特性之前，请校验目标目录中是否实际存在相应的特性。

4.2.2 定义纲要映射

不同的 LDAP 服务器有不同的纲要。驱动程序首次启动时，它会向服务器查询特定的纲要。

您必须熟悉 eDirectory 特性和 LDAP 服务器特性的特征。驱动程序将处理所有 LDAP 特性类型 （cis、 ces、 tel、 dn、 int、 bin）。它还处理 eDirectory 传真电话号码。

映射特性时遵循以下准则：

- 校验每个在订购者和发布者策略中指定的类和特性是否都已在映射策略中映射 （除非两个目录中的类或特性名称相同）。
- 将 eDirectory™ 特性映射为 LDAP 服务器特性之前，校验 LDAP 服务器特性是否实际存在。例如，为 Identity Vault 上的用户对象定义了 Fullname 特性，但 Netscape 中的 inetOrgPerson 对象中不存在 Fullname。
- 始终将特性映射为相同类型的特性。例如，将字符串特性映射为字符串特性，将八位特性映射为二进制特性，或将电话号码特性映射为电话号码特性。
- 将多值特性映射为多值特性。

驱动程序不提供不同特性类型之间的转换，或者从多值特性到单值特性的转换。驱动程序也不识别除 《传真电话号码》和 《邮递地址》以外的结构化的特性。

Identity Manager 可以灵活处理它接受的来自发布者的语法：

- 接受非结构化 / 非八位语法 。只要实际数据可以强制转换为相应类型，Identity Manager 就可以接受任何非结构化 / 非八组语法转换为其它任何非结构化 / 非八位语法。也就是说，如果 Identity Vault 正在查找数字值，则实际数据应当是数值。
- 将数据强制转换为八位数据 。如果 Identity Manager 需要八位数据而获取的却是一个非八位 / 非结构化类型，则通过将字符串值序列化为 UTF-8， Identity Manager 就可以将数据强制转换为八位数据。
- 将数据强制转换为字符串 。当 Identity Manager 传送八位数据，同时又需要一个非结构化类型时， Identity Manager 会通过解码 Base64 数据，将数据强制转换为字符串。然后， Identity Manager 会尝试将结果解释为 UTF-8 编码字符串 （如果不是有效的 UTF-8 字符串，则解释为平台的默认字符编码），然后会应用与 《接受非结构化 / 非八位语法》相同的规则。
- 传真号码 。对于传真号码，如果已传进非结构化类型，则 《接受非结构化 / 非八位语法》和 《将数据强制转换为字符串》规则将应用于数据，以获取传真号码中的电话号码部分。而其它字段则使用默认值。
- 状态。状态。对于状态， False、 No、 F、 N（不区分大小写）、 0 和 ""（空字符串）解释为 False，任何其它值都解释为 True。

配置纲要映射策略：

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

2 在所属驱动程序集中找到此驱动程序。

3 单击驱动程序，打开 《Identity Manager 驱动程序概述》 页。

4 单击发布者或订购者通道上的纲要映射图标。

5 编辑该策略以符合您的设置。

4.2.3 在 Netscape 中定义对象替换

我们建议对 Netscape Directory Server 中的对象应用以下 Netscape 命名规则。为方便起见，以下提供了对命名规则的简要说明。

目录包含表示人员的项目。这些人员项目必须具有名称。换而言之，您必须决定每个人员项目所使用的相对判别名 (RDN)。 DN 必须是一个唯一、易于识别、永久的值。我们建议使用 uid 特性来指定与人员关联的唯一值。以下是人员项目的 DN 示例：

uid=jsmith,o=novell

目录还将包含表示除人员外的许多内容的项目 （例如，组、设备、服务器、网络信息或其它数据）。我们建议在 RDN 中使用 cn 特性。因此，如果您要命名一个组项目，命名方法则如下所示：

cn=administrators,ou=groups,o=novell

此目录还包含分支点或树枝。您需要决定用于标识分支点的特性。由于特性名是有意义的，因此应使用具有它表示的项目类型的特性名。 Netscape 建议按如下方式定义特性：

表 *4-2* *Netscape* 建议特性

特性名	定义
c	国家 / 地区名称
o	组织名称
ou	组织单元
st	州 / 省
l	位置
dc	域部件

订购者布局策略指定类名的命名特性。以下是用户类名的示例。 <placement> 语句指定 uid 用作命名特性。

```
<placement-rule> <match-class class-name="User"/> <match-path
prefix="\Novell-Tree\Novell\Users"/> <placement>uid=<copy-name/
>,ou=People,o=Netscape</ placement> </placement-rule>
```

以下的订购者布局指定 ou 用作类名组织单元的命名特性。

```
<placement-rule> <match-class class-name="Organizational Unit"/>
<match-path prefix="\Novell-Tree\Novell\Users"/> <placement>ou=<copy-
```

```
name/>,ou=People,o=Netscape</placement> </placement-rule>
```

配置布局策略

1. 在 iManager 中，单击 *Identity Manager* > 《Identity Manager 概述》。
2. 在所属驱动程序集中找到此驱动程序。
3. 单击驱动程序，打开 《Identity Manager 驱动程序概述》页。
4. 单击发布者或订购者策略图标，然后进行相应更改。

4.2.4 使用 eDirectory 组和 Netscape

由于 Identity Vault 和 Netscape Directory Server 中的组特性不同，因此驱动程序需要一些特殊处理。在发布者通道上，当驱动程序发现类名 *groupofuniquenames* 中有 *uniquemember* 特性时，需要进行特殊处理。

驱动程序还将在 eDirectory 组中设置 《与我等效》特性。该特性必须包括在发布者过滤器中。特性 《与我等效》无需在纲要映射策略中，因为 eDirectory 特性名已被使用。 Netscape Directory Server 中不存在等效特性名。不要求对订购者通道进行特殊处理。

4.3 配置 SSL 连接

驱动程序使用 LDAP 协议与 LDAP 服务器通讯。大多数 LDAP 服务器都允许非加密 （纯文本）连接。此外，配置正确时，有些 LDAP 服务器允许 SSL 加密连接。通过使用公共 / 私用密钥对， SSL 连接对所有 TCP/IP 套接字进行加密。实际的 LDAP 协议并不会更改，但通讯通道会执行加密。

根据 LDAP 服务器的不同，启用 SSL 连接的步骤也会有所差别。本文档介绍了当使用 Netscape Directory Server 4.12 时启用 SSL 连接的过程。

- “步骤 1：生成服务器证书”在第 34 页
- “步骤 2：发送证书请求”在第 35 页
- “步骤 3：安装证书”在第 36 页
- “步骤 4：在 Netscape Directory Server 4.12 中激活 SSL”在第 36 页
- “步骤 5：从 eDirectory 树中导出可信根”在第 36 页
- “步骤 6：导入可信根证书”在第 37 页
- “步骤 7：调整驱动程序设置”在第 38 页

如果使用其它 LDAP 服务器，步骤是类似的。

4.3.1 步骤 1：生成服务器证书

首先，需要安装服务器证书。LDAP 服务器本身可以生成证书，但是该证书必须得到服务器所信任的 CA 的签名。您可以使用 Identity Vault 附带的 CA 来对证书签名。

生成证书请求：

1. 在 Netscape 控制台的导航树中，选择驱动程序要与其通讯的服务器。
2. 单击 *Open Server* （打开服务器）。

3 单击 《任务》 > *Certificate Setup Wizard* （证书安装向导）。

4 提供相关信息以请求证书。

根据可能已安装在主机系统上的证书或令牌，您可能会看到下列部分或全部字段：

Select a Token (Cryptographic Device) （选择令牌 （加密设备））：选择 *Internal (Software)* （内部 （软件））。

Is the Server Certificate Already Requested and Ready to Install? （服务器证书是否已请求并准备好安装？）选择 《否》。

如果该主机的信任数据库不存在，则会为您生成一个。

信任数据库是指安装在本地主机上的密钥对和证书数据库。当使用内部令牌时，信任数据库是您在其中安装密钥和证书的数据库。

5 键入并确认口令。

口令必须至少包含八个字符，其中必须至少有一个数字。此口令帮助确保对您创建的新密钥数据库访问的安全。

6 根据提示继续提供相关信息，然后单击 《下一步》。

7 创建信任数据库后，单击 《下一步》。

8 键入请求的信息，然后单击 《下一步》。

9 键入您先前选择的令牌的口令，然后单击 《下一步》。

《证书安装向导》会为您的服务器生成证书请求。当您看到这一页时，可以向证书授权者发送证书请求。

4.3.2 步骤 2：发送证书请求

1 将服务器证书请求复制到记事本或其它文本编辑器中。

2 将文件另存为 csr.txt。

证书请求电子邮件应符合下面的格式：

```
-----BEGIN NEW CERTIFICATE REQUEST-----

        .

        .

        . -----END NEW CERTIFICATE REQUEST----
```

3 在 iManager 中，选择 《Novell 证书服务器》> *Issue Certificate* （颁发证书）。

4 在 《文件名》字段中找到 csr.txt，然后单击 《下一步》。

5 选择 *Organizational Certificate Authority* （组织证书授权者）。

6 将 SSL 指定为密钥类型，然后单击 《下一步》。

7 指定证书参数，单击 《下一步》，然后单击 《完成》。

8 将证书以 Base64 格式另存在本地磁盘或软盘中，名称为 cert.b64。

4.3.3 步骤 3：安装证书

1. 在 Netscape 控制台的导航树中，选择驱动程序要与其连接的服务器。
2. 单击 《打开》。
3. 单击 《任务》 > 《证书安装向导》。
4. 启动向导，表示您已准备好安装证书。
5. 得到提示后，提供以下信息：

   选择令牌 （加密设备）： 选择 《内部 （软件）》。

   服务器证书是否已请求并准备好安装？ 选择 《是》。
6. 单击 《下一步》。
7. 在 *Install Certificate For* （安装目标）字段中，选择 《此服务器》。
8. 在 《口令》字段中，键入您用于安装信任数据库的口令，然后单击 《下一步》。
9. 在 *Certificate Is Located in This File* （证书位于以下文件中）字段中，键入证书的绝对路径 （例如 A: \CERT.B64）。
10. 证书生成后，单击 《添加》。
11. 证书成功安装后，单击 《完成》。

4.3.4 步骤 4：在 Netscape Directory Server 4.12 中激活 SSL

安装证书后，请完成下列步骤以激活 SSL：

1. 在 Netscape 控制台的导航树中，选择您要对其应用 SSL 加密的服务器。
2. 单击 《打开》 > 《配置》 > 《加密》。
3. 输入以下信息：

   启用 **SSL**： 选择此选项。

   Cipher Family （加密法系列）： 选择 *RSA*。

   Token to Use （要使用的令牌）： 选择 《内部 （软件）》。

   Certificate to Use （要使用的证书）： 选择 *Server-Cert*。

   Client Authentication （客户机鉴定）： 由于驱动程序不支持客户机鉴定，请选择 *Allow Client Authentication* （允许客户机鉴定）。
4. 单击 《保存》。
5. 单击 《任务》，然后重新启动服务器 , 使更改生效。

4.3.5 步骤 5：从 eDirectory 树中导出可信根

1. 在 iManager 中，单击 *eDirectory Administration* （eDirectory 管理） > 《修改对象》。
2. 找到证书授权者 (CA) 对象，然后单击 《确定》。
3. 从下拉列表中选择 《证书》。
4. 单击 《导出》。
5. 显示 *Do you want to export the private key with the certificate?* （是否要导出证书的私用密钥？）提示时，单击 《否》。

6 单击 《下一步》。

7 在 《文件名》字段中，键入文件名 （例如 PublicKeyCert），然后选择 *Base64* 格式。

8 单击 《导出》。

4.3.6 步骤 6：导入可信根证书

您需要将可信根证书导入 LDAP 服务器的信任数据库和客户机的证书存储区。

导入 **LDAP** 服务器的信任数据库

您需要将可信根证书导入 LDAP 服务器的信任数据库。由于服务器证书已经由 Identity Vault 的 CA 签名，因此需要配置信任数据库以信任 Identity Vault CA。

1 在 Netscape 控制台中，单击 《任务》 > 《证书安装向导》 > 《下一步》。

2 在 《选择令牌》中，请接受默认的 《内部 （软件）》。

3 在 《服务器证书是否已请求并准备好安装》中，选择 《是》。

4 单击 《下一步》两次。

5 在 《安装目标》对话框中，选择 *Trusted Certificate Authority* （可信的证书授权者）。

6 单击 《下一步》。

7 选择 《证书位于以下文件中》，然后键入到包含可信根证书的 .b64 文件的完整路径。

8 单击 《下一步》。

9 校验屏幕上的信息，然后单击 《添加》。

10 单击 《完成》。

导入客户机的证书存储区中

您需要将可信根证书导入驱动器可以使用的证书存储区 （也称为密钥存储区）中。

1 使用 rt.jar 中的密钥工具类。

例如，如果您的公共密钥证书的名称是 PublicKeyCert.b64，保存在软盘上，并且要将其导入当前目录中名为 .keystore 的新证书存储区文件中，请在命令行处输入以下命令：

```
java sun.security.tools.KeyTool -import -alias TrustedRoot -file
a:\PublicKeyCert.b64

-keystore .keystore -storepass keystorepass
```

2 当系统询问是否信任此证书时，选择 《是》，然后按 *Enter* 键。

3 将 .keystore 文件复制到具有 Identity Vault 文件的同一文件系统中的任何目录。

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

5 搜索驱动程序。

6 单击 LDAP 驱动程序对象，然后在 《Identity Manager 概述》页中再次单击它。

7 在 *Keystore Path* （密钥存储区路径）参数中，输入 .keystore 文件的完整路径。

4.3.7 步骤 7：调整驱动程序设置

下表列出了样本配置中的驱动程序设置及其默认值。

表 *4-3* 驱动程序设置及其默认值

参数	样本配置值	说明
使用 SSL 进行 LDAP 连接	否	此参数的值为 《是》或 《否》。它指示与 LDAP 服务器通讯时是否使用 SSL 连接。要使用 SSL，还必须正确配置 LDAP 服务器。 有关更多信息，请参考 “配置 SSL 连接”在第 34 页 。
SSL 端口	636	除非 《使用 SSL 进行 LDAP 连接》设置为 《是》，否则此参数将被忽略。它指示 LDAP 服务器使用哪个端口进行安全连接。
密钥存储区路径 （SSL 证书）	[空]	当 《使用 SSL 进行 LDAP 连接》设置为 《是》时，此参数的值应为包含可信根证书的密钥存储区文件的完整路径，其中的可信根证书属于为服务器证书签名的证书授权者 (CA)。 有关创建密钥存储区文件的更多信息，请参见 “导入客户机的证书存储区中”在第 37 页 。

查错

5

5.1 将用户迁移到 Identity Vault 中

有些 LDAP 服务器具有用于限制由 LDAP 查询返回的项目数量的设置。例如， iPlanet Directory Server 5.1 的默认限制为 2000 个对象。

将数据从 LDAP 迁移到 Identity Vault 中时，驱动程序向服务器发出 LDAP 查询，并返回符合标准的对象 （例如 objectclass=User）。

在对 LDAP 查询可以返回的项目数量设置限制后，虽然 Identity Manager 驱动程序仍继续正常运行，但该限制可使迁移在完成之前停止。

要解决此问题，请更改限制。例如，在 iPlanet 中执行下列步骤：

1. 找到 《配置》选项卡，然后选择 《数据库》设置。
2. 将 LDBM 插件选项卡中的最高限制从 5000 （默认值）提高到适当的值。

   这是在执行查询时允许查询查看的记录数。
3. 找到 《配置》选项卡，选择 *Directory Server Settings* （目录服务器设置），然后选择 《性能》选项卡，并根据需要迁移的用户帐户数量来提高大小限制。

   这是允许查询返回的记录的实际数量。

   调整完这些设置后，迁移可以正确完成。

5.2 OutOfMemoryError

如果在使用 LDAP-Search 方法的情况下，驱动程序关闭并显示 java.lang.OutOfMemoryErro：

1. 尝试设置或增大 DHOST_JVM_INITIAL_HEAP 和 *DHOST_JVM_MAX_HEAP* 环境变量。
2. 重新启动驱动程序。
3. 监视驱动程序以确保变量提供足够内存。

有关更多信息，请参见 TID 10062098 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10062098.htm)。

5.3 LDAP v3 兼容性

ILDAP Driver for Identity Manager 适用于大多数与 LDAP v3 兼容的 LDAP 服务器。此驱动程序已被写进针对 LDAP 的 RFC 2251 规范中。为了使此驱动程序能够与不完全符合 RFC 2251 要求的 LDAP 服务器兼容，我们增加了对 LDAP 驱动程序的解决方法。

一个不能忽略且无法解决的兼容性问题是，根据 RFC 2251 要求，服务器允许讯息 ID 值可以高达 2,147,483,647 （四字节整数值）。

Oracle Internet Directory 2.1.1.0.0 版 （属于 Oracle 8i）只允许讯息 ID 值达到 32,767 （二字节整数值）。因此，它无法与 LDAP Driver for Identity Manager 一起正常工作。

如果需要与 Oracle Internet Directory 兼容， Novell 建议升级到 9.2.0.1.0 版（包括在 Oracle 9i 中）或更高版本。

5.4 常见问题

问题：LDAP-Search 方法在进行检索时是每次执行全面检索还是只检索上次巡回检测后的更新？

回答： LDAP-Search 方法会同步每次巡回检测到下一次巡回检测的更新。

问题：如果可以选择使用 LDAP-Search 方法或者 changelog 方法，则是否应使用 LDAP-Search 方法？

回答： changelog 方法性能较好。请使用该方法。changelog 方法是首选方法。

文档更新

A

本节包含有关 Identity Manager Driver for LDAP 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 文档均与本节列出的文档更改保持最新。

如果要了解您正在使用的 PDF 文档的副本是否为最新的，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）。

新的或更新文档发布于下列日期：

- “2006 年 5 月 25 日”在第 41 页

A.1 2006 年 5 月 25 日

表 ***A-1*** *2006 年 5 月 8 日所做的更改*

位置	更改
“新功能”在第 5 页	本主题中添加了两项。
“计划更新”在第 5 页	添加了本主题。
“计划考虑事项”在第 11 页	添加了一段关于 LDAP v3 兼容性问题和 RFC 2251 规范的内容。
“控制从 LDAP 目录到 Identity Vault 的数据流”在第 25 页	本节进行重新划分，以便更容易实施 changelog 和 LDAP-Search 方法。
“LDAP 订购者设置”在第 26 页	添加了有关新的订购者参数的信息。
“首次启动时同步的搜索结果”在第 31 页	添加了有关这一新发布者参数的信息。
“LDAP v3 兼容性”在第 39 页	添加了本节。
“常见问题”在第 40 页	添加了本节。