Sun Java™ System

Identity Synchronization for Windows 1
安装和配置指南

2004Q3

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

文件号码：817-7848

目录

图列表

表格列表

前言

Sun Java™ System Identity Synchronization for Windows 1 2004Q3 （原为 Sun™ ONE Identity Synchronization for Windows）允许密码及其它指定的用户属性在 Sun Java™ System Directory Server 及其它系统之间流动。

本指南说明如何安装和配置 Sun Java System Identity Synchronization for Windows 以用于生产环境。

有关本版本 Identity Synchronization for Windows 的新功能和增强功能的最新信息，请参阅联机发行说明，网址为：

http://docs.sun.com/db/doc

注意 本文档中描述的用户界面随产品今后版本的更改而变化。

本前言含有以下信息：

哪些人应阅读本书

本 *安装和配置指南*专供要通过安装和配置 Identity Synchronization for Windows 在 Sun Java™ System Directory Server 和 Windows Active Directory/NT 机器之间建立双向密码和用户属性同步的管理员、系统工程师以及专职服务工程师使用。

本书读者应熟悉以下内容：

- Directory Server 和 Windows Active Directory/NT 的配置和操作
- 轻量级目录访问协议 (LDAP)
- Java 技术
- 可扩展标记语言 (XML)
- 公共密钥密码学和 “安全套接字层” (SSL) 协议的基本概念
- 内联网、外联网和 Internet 安全的基本概念以及数字证书在企业中的作用

阅读本书之前

*《Sun Java System Identity Synchronization for Windows 1 2004Q3 发行说明》*含有关于本产品的最新信息 — 包括可能替换本书提供的说明的信息。请务必在尝试执行本书说明的步骤前阅读本 “发行说明”。

由于 Sun Java System Directory Server 是作为 Identity Synchronization for Windows 部署中的数据存储器使用，因此您应熟悉与该产品一起提供的文档。Directory Server 文档可以通过在线访问 http://docs.sun.com/coll/DirectoryServer_04q2 获得。

本书的内容安排

Sun Java System Identity Synchronization for Windows 1 2004Q3 安装和配置指南 编排为以下各章：

- 第 1 章，“了解产品”：解释有关 Identity Synchronization for Windows 的一些基本概念，如产品功能、系统组件、命令行实用程序、系统组件分配和部署示例等。
- 第 2 章，“准备安装”：介绍安装和配置过程，并提供可能有助于准备本产品安装的信息。
- 第 3 章，“安装核心”：介绍如何使用 Identity Synchronization for Windows 安装程序以及如何安装 Identity Synchronization for Windows 核心组件。
- 第 4 章，“配置核心资源”：介绍如何使用“控制台”添加和配置“核心”资源。
- 第 5 章，“安装连接器和 Directory Server 插件”：提供安装 Identity Synchronization for Windows 连接器和 Directory Server 插件的说明。
- 第 6 章，“同步现有用户”：介绍如何为新的 Identity Synchronization for Windows 安装链接和重新同步现有用户。
- 第 7 章，“移植到 Identity Synchronization for Windows 1 2004Q3”：介绍如何将系统从 Sun Java System Identity Synchronization for Windows 版本 1.0 移植到版本 1 2004Q3。
- 第 8 章，“删除软件”：介绍如何删除 Identity Synchronization for Windows，包括如何准备卸载及如何手动卸载 “控制台”。
- 第 9 章，“故障排除”：提供可用来排除 Identity Synchronization for Windows 安装故障的信息。
- 第 10 章，“了解审计和错误文件”：提供有关审计和错误日志记录的信息，包括如何设置日志记录级别、查看和了解日志文件和目录源状态。
- 第 11 章，“配置安全性”：介绍如何配置安全系统。提供的信息包括加强安全性、保护复制配置、启用 SSL 和将 Active Directory CA 证书添加到证书数据库。
- 附录 A，“使用 Identity Synchronization for Windows 命令行实用程序”：介绍如何使用 Identity Synchronization for Windows 命令行实用程序执行各种任务。
- 附录 B，“LinkUsers XML 文档范例”：提供一个 Linkusers XML 范例文档 (`linkusers-simple.cfg`)，您可据此定制自己的环境。
- 附录 C，“在 Solaris 上以非超级用户身份运行服务”：介绍如何以非超级用户身份运行 Identity Synchronization for Windows 服务。

- 附录 D，“定义和配置同步用户列表”：提供关于“同步用户列表”定义和多域配置的信息。
- 附录 E，“复制环境的安装注意事项”：概述配置和保护多主复制 (MMR) 部署必需执行的步骤。

本书使用的约定

本节的表中说明了本书使用的约定。内容具体安排如下：

- 第 19 页的 “印刷约定”
- 第 19 页的 “符号”
- 第 20 页的 “助记符”
- 第 20 页的 “默认路径和文件名”

印刷约定

下表说明了本书使用的印刷约定。

表 1 印刷约定

字样	含义	示例
AaBbCc123 （等宽）	API 和语言元素、 HTML 标记、网站的 URL、命令名、文件名、目录路径名、计算机屏幕输出、示例代码。	编辑 `.login` 文件。 使用 `ls -a` 列出所有文件。 `% You have mail。`
AaBbCc123 （等宽粗体）	键入的内容 （在与计算机屏幕输出对比时）。	**`% su`** `Password:`
AaBbCc123 （斜体）	书的标题、新的术语、要强调的词。 在命令或路径名中要用实际名称或值替换的占位符。	阅读*用户指南*中的第 6 章。 这些称为*类*选项。 *不要*保存文件。 文件位于 *install-dir*`/bin` 目录中。

符号

下表说明了本书使用的符号约定。

表 2 符号约定

符号	说明	示例	含义
`[ ]`	包含可选命令选项。	`ls [-l]`	`-l` 选项不是必需的选项。
`{ | }`	含有必需命令选项的选项集合。	`-d {y|n}`	`-d` 选项要求使用 `y` 参数或 `n` 参数。
-	将同时按下的多个键连接。	Control-A	按下 A 键的同时按下 Control 键。
+	将依次按下的多个键连接。	Ctrl+A+N	按下 Control 键，然后释放它，再依次按下后面的键。
>	指示图形用户界面中的菜单选项。	文件 > 新建 > 模板	从 “文件” 菜单中选择 “新建”。从 “新建” 子菜单中选择 “模板”。

助记符

Identity Synchronization for Windows 在整个用户界面中使用*助记符*（带下划线的字母），为用户执行某些任务提供更加快捷的方式。您只需键入带下划线的字母便可执行相应任务。助记符不区分大小写。要访问它们，请同时按下 Alt 键。

默认路径和文件名

下表说明了本书中使用的默认路径和文件名。

表 3 默认路径和文件名

条目	说明
<serverroot>	表示 Identity Synchronization for Windows 安装位置的父目录。
`isw-`*<hostname>*	表示 Identity Synchronization for Windows 实例目录。
<current-working-directory>`/cert8.db`	表示客户机证书数据库的默认路径和文件名。
<installation_root>`/isw-`*<machine_name>*`/logs/central/`	表示 Identity Synchronization for Windows 中心日志的默认路径。
<installation_root>`/isw-`*<machine_name>*`/logs/`	表示通向 Identity Synchronization for Windows 本地日志 （对系统管理器、每个连接器和中心记录器而言）的默认路径。
`/usr/sfw/bin`	在 Solaris 上，默认情况下， certutil 安装到此目录位置。

相关文档

您可以通过 http://docs.sun.com 网站访问 Sun 在线技术文档。您可以浏览存档文件或搜索特定的书名或主题。

本文档集包含的书籍

下表概述了 Identity Synchronization for Windows 文档集包含的书籍。

表 4 本文档集包含的书籍

书名	说明
Sun Java System Identity Synchronization for Windows 1 2004Q3 安装和配置指南 (http://docs.sun.com/doc/817-6199)	介绍如何安装和配置 Identity Synchronization for Windows 以用于生产环境。
Sun Java System Identity Synchronization for Windows 1 2004Q3 Deployment Planning Guide (http://docs.sun.com/doc/817-6200)	提供计划和部署 Identity Synchronization for Windows 的一般性指导和最佳实践方法。
Sun Java System Identity Synchronization for Windows 1 2004Q3 发行说明 (http://docs.sun.com/doc/817-6202)	可以在产品发行后获得。含有最新信息，包括此当前版本的新功能的说明、已知问题和限制、安装说明以及如何报告软件或文档方面的问题。

其它文档

由于您将使用 Directory Server 和 Sun Java™ System Message Queue，因此可能需要参考相应的产品文档。可从以下位置访问相应文档：

- Sun Java System Directory Server 文档
  http://docs.sun.com/coll/DirectoryServer_04q2
- Sun Java System Message Queue 文档
  http://docs.sun.com/db/prod/2296#hic

有关公共密钥密码学、“安全套接字层” (SSL) 协议、内联网、外联网和 Internet 安全的基本概念以及数字证书在企业中的作用的信息，请阅读 《*Managing Servers with iPlanet Console 5.0*》手册中与安全相关的附录。

有关 Windows 2003 Server 和 “Windows 密码策略”的信息，请阅读以下 Microsoft 出版物：

- *Using Secedit.exe to Force Group Policy to Be Applied Again - Windows 2000 Servers Microsoft KB #227448*
- *A Description of the Group Policy Update Utility - Windows 2003 Servers Microsoft KB #298444*
- *Microsoft Knowledge Base Article 232690*

访问 Sun 在线资源

要获得产品下载、专业服务、修补程序和支持以及其他开发者信息，请访问以下网址：

- 开发者信息
  http://developers.sun.com/prodtech/index.html
- 下载中心
  http://wwws.sun.com/software/download/
- 产品数据表
  http://www.sun.com/software/
- 在线产品文档
  http://docs.sun.com
- 产品支持和状态
  http://www.sun.com/service/support/software/
- 专业服务
  http://www.sun.com/service/sunps/sunone/index.html
- Sun 企业服务、 Solaris 修补程序和支持
  http://sunsolve.sun.com
- 支持和培训
  http://www.sun.com/supportraining/

联系 Sun 技术支持

如果您对本产品有文档中未进行解答的技术问题，请访问：

http://www.sun.com/service/contacting

相关的第三方 Web 站点引用

本出版物涉及以下第三方网站：

- 有关 Windows 2003 密码策略的信息：

  http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dsscc_aut_xbby.asp

- 有关在 Windows 2003 中应用或修改密码和组策略的信息：

  http://www.microsoft.com/resources/documentation/windowsserv/2003/standard/proddocs/en-us/password_grouppolicy.asp

- 有关 Microsoft Certificate Services Enterprise Root 证书授权机构的信息：

  http://support.microsoft.com/default.aspx?scid=kb;en-us;q247078

- 有关通过 SSL 配置 LDAP 的信息：

  http://support.microsoft.com/default.aspx?scid=kb;en-us;321051

Sun 对本文档中涉及的第三方网站的可用性概不负责。对于此类站点或资源直接或间接提供的任何内容、广告、产品或其它资料， Sun 不作任何担保，也不承担任何责任。对于因上述站点或资源直接或间接提供的上述任何内容、物品或服务导致的或声称由其导致的或与其使用或可靠性相关的任何实际的或声称的损害或损失，Sun 不负任何责任。

Sun 欢迎您提出宝贵意见

Sun 非常愿意改进其文档，并欢迎您提出意见和建议。

要提出意见，请访问 http://docs.sun.com 然后单击 Send Comments。在在线表格中，提供文档标题和文件号码。文件号码是一个七位或九位数字，可以在相应书籍的标题页或文档顶部找到。

例如，本书的标题为 *Sun Java System Identity Synchronization for Windows 1 2004Q3 安装和配置指南*，文件号码为 817-7848。

安装和配置

第 1 章

了解产品

Identity Synchronization for Windows 提供在 Sun Java™ System Directory Server 5 2004Q2 和以下目录环境之间的双向密码和用户属性同步：

- Windows 2000 或 Windows 2003 Server Active Directory
- Windows NT SAM Registry

Identity Synchronization for Windows 处理同步事件：

- **安全**：Identity Synchronization for Windows 从不发送明文密码，并且将系统访问权限限制在管理员范围内。
- **稳定**：Identity Synchronization for Windows 保持各个目录同步 — 即使单个组件暂时不可用。
- **高效**：Identity Synchronization for Windows 同步方法仅在目录服务器上加载极少量负荷。

在安装 （或移植至） Sun Java System Identity Synchronization for Windows 版本 1 2004Q3 之前，应先熟悉本章中介绍的概念。本章包含以下各节：

产品特性

Identity Synchronization for Windows 具有以下特性和功能：

- **双向密码同步**：使您能够在 Sun Java System 目录源与 Windows Active Directory 和 Windows NT 目录源之间同步用户密码。

  同步密码可以使用户访问使用上述目录源进行登录验证的应用程序，从而使用户只需记住一个密码。另外，在用户必须对密码进行定期更新时，他们也只需在一个环境中更新密码。

- **双向用户属性同步**：使您能够在一种目录环境中创建、修改和删除选定属性，并自动把这些值传播至其它目录环境。

- **双向用户帐户创建同步**：使您能够在一个目录环境中创建或删除用户帐户，并自动将新帐户传播至其它目录环境。

- **双向对象删除、激活和禁用**：使您能控制在 Directory Server 和 Active Directory 目录源 （对 Windows NT 不适用）之间的对象删除以及对象激活和禁用的流动。

- **与多个域同步**：使您能与多个 Active Directory 和 Windows NT 域同步，并能与多个 Active Directory 森林结构同步。

- **集中的系统审计**：使您能监控安装和配置状态、日常系统操作和与单一、集中位置的部署有关的任何错误状况。

不必修改 Windows 目录中的条目或更改使用相应目录的应用程序。

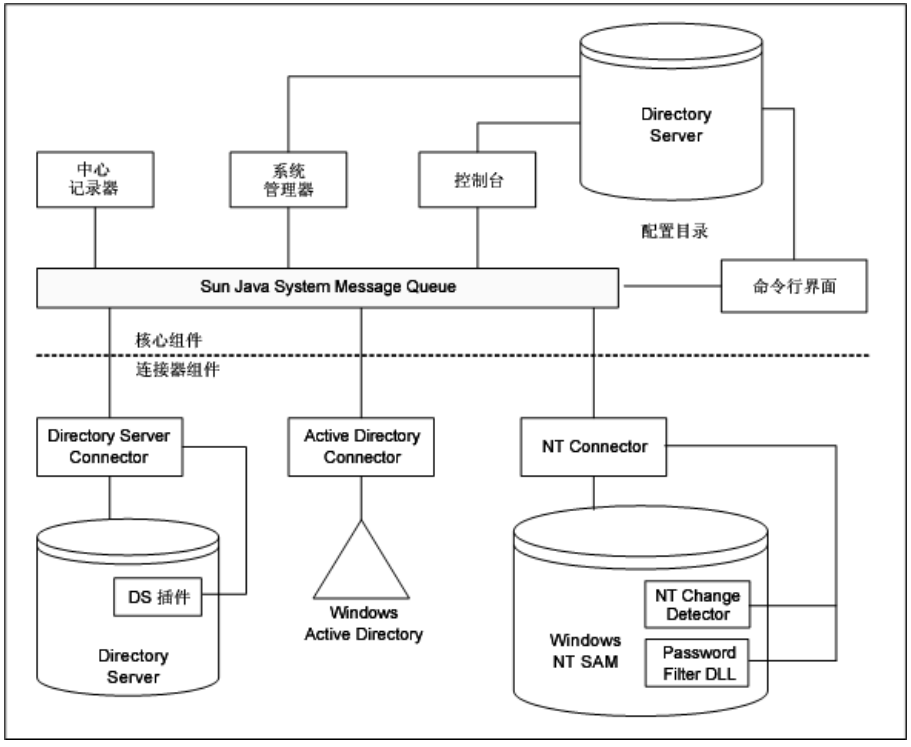
如果要使用 Identity Synchronization for Windows 以实现 Directory Server 和 Active Directory 之间的同步，则无需在 Windows 操作环境中安装任何组件。

如果要在 Directory Server 和 Windows NT 之间实现同步，则必须在 Windows NT 环境中安装本产品的 NT 组件。

系统组件

Identity Synchronization for Windows 由一组核心组件和任意数量的单独*连接器*和*连接器子组件*构成，它们可在 Sun Java System Directory Server 和各 Windows 目录之间实现密码和用户属性更新的同步 （参见图 1-1）。

图 1-1 系统组件



本节将对 Identity Synchronization for Windows 的每个组件进行定义和说明，按如下方式编排：

- 第 30 页的 “监视器进程”
- 第 30 页的 “核心”
- 第 34 页的 “连接器”
- 第 34 页的 “连接器子组件”

监视器进程

监视器是一个 Identity Synchronization for Windows java 进程，该进程负责启动、重启和停止单个后台 java 进程。监视器启动并监控中心记录器、系统管理器和连接器 （但不监控子组件、 Message Queue 或 Identity Synchronization for Windows 控制台）。

监视器安装在 “核心”安装的位置，可作为 Solaris 守护进程或 Windows 服务启动。（有关启动和停止服务的信息，请参阅第 181 页的 “启动和停止服务”。）

核心

安装 Identity Synchronization for Windows 时，先安装*核心*组件，然后根据环境对其进行配置。

“核心”由下列组件构成，这些组件中的任何一个都是独立的 java 进程。对每个组件的说明开始于如下参考页：

- 第 31 页的 “配置目录”
- 第 31 页的 “控制台”
- 第 32 页的 “命令行实用程序”
- 第 32 页的 “系统管理器”
- 第 33 页的 “中心记录器”

注意 监视器安装在 “核心”的安装位置，负责启动和监控中心记录器和系统管理器。

有关详细信息，请参阅第 30 页的 “监视器进程”。

配置目录

Identity Synchronization for Windows 将其配置数据*存储*在 Directory Server 配置目录中 （程序不安装配置目录）。

控制台、系统管理器、命令行实用程序和安装程序都会在配置目录中读出或写入产品的配置数据，包括：

- 关于每个组件的运行状况的安装信息
- 每个目录、域、连接器和 Directory Server 插件的配置信息
- 连接器状态
- 说明用户创建、用户删除和属性修改方向的同步设置信息
- 要同步的属性和两个目录环境 Active Directory 和 Directory Server （或 Windows NT 和 Directory Server）之间的属性映射
- 每个目录拓扑中的 “同步用户列表”
- 日志设置

控制台

Identity Synchronization for Windows 提供的控制台集中了所有的产品组件配置和管理任务。

控制台可用于：

- 配置需要同步的目录源
- 为除密码外其它要同步的用户条目属性定义映射
- 指定目录或域拓扑中哪些用户和属性将要 （或将不会）被同步
- 监控系统状态
- 启动和停止同步

命令行实用程序

Identity Synchronization for Windows 还提供了命令行实用程序，使您能直接从命令行执行如下任务：

- 根据配置和 SSL 设置显示证书信息
- 更改 Identity Synchronization for Windows 配置密码
- 导入已导出的 Identity Synchronization for Windows 版本 1.0 配置 XML 文档
- 准备供 Identity Synchronization for Windows 使用的 Sun Java System Directory Server 源
- 显示要完成安装 / 配置过程所必须执行的步骤，并查看已安装的连接器、系统管理器和 Message Queue 的状态
- 将配置目录中的连接器状态重设为 *尚未安装*
- 同步和链接两个目录中的现有用户，并作为安装过程的一部分预先填充目录。
- 启动同步
- 停止同步

有关产品的命令行实用程序及其用法的详细说明，请参阅附录 A，“使用 Identity Synchronization for Windows 命令行实用程序”。

系统管理器

Identity Synchronization for Windows 系统管理器是一个独立的 java 进程，它能够：

- 利用本产品的后端网络化工具动态地向连接器传送配置更新信息
- 保持每个连接器和所有连接器子组件的状态
- 协调用于两个目录初始同步的 `idsync resync` 操作

中心记录器

连接器的安装可能会跨远程地理位置而广泛分布；因此，集中所有日志信息具有重大的管理价值，允许管理员从单一位置监控同步活动、检测错误以及评估整个系统的运行状况。

管理员可以使用中心记录器日志实现以下目的：

- 检查系统运行是否正常
- 检测和处理个别组件以及系统范围的故障
- 审计个别以及系统范围的同步活动
- 跟踪不同目录环境间的用户密码同步

日志的类型有两种：

- **审计日志**提供系统日常活动有关的信息，包括诸如用户密码在不同目录间同步等重要事件。您可以通过增加或减少日志消息中提供的细节信息控制在审计日志中记录信息的详细程度。

注意	Identity Synchronization for Windows 还可以将全部错误日志消息写入审计日志，从而简化了与其它事件的相关性。

- **错误日志**提供达到严重错误和警告条件的信息。由于所有错误日志条目都值得注意，因此不能人为阻止对错误信息的记录。当某个错误状态出现时，它总会记录到错误日志中。

连接器

连接器是一个 java 进程，该进程使用单一数据源类型管理同步进程。连接器检测数据源中的用户更改，并通过 Message Queue 将这些更改发布到远程连接器。

Identity Synchronization for Windows 提供如下特定于目录的连接器，这些连接器负责在不同目录和域之间双向同步用户属性和密码更新：

- **Directory Server Connector**：支持 Directory Server 中的单个根后缀 （例如后缀 / 数据库）
- **Active Directory Connector**：支持 Windows 2000 或 Windows 2003 Server Active Directory 环境中的单个实例。您可以为附加域使用多个连接器
- **Windows NT Connector**：支持 Windows NT 环境中的单个域

注意 监视器安装在任何安装了连接器的位置，并负责启动、重启和停止连接器。有关详细信息，请参阅第 30 页的 “监视器进程”。

连接器子组件

子组件是一个独立于连接器运行的轻量进程或库。连接器使用子组件访问不能远程访问的本机资源，例如捕获 Directory Server 或 Windows NT 内部的密码。

以下连接器子组件随要同步的目录一同安装，并通过加密连接与相应的连接器进行通信。

- 第 34 页的 “Directory Server 插件”
- 第 35 页的 “Windows NT Connector 子组件”

注意 Active Directory Connector 不需要子组件。

Directory Server 插件

“Directory Server 插件”是 Directory Server Connector 的一个子组件。在每个要同步的 Directory Server 中安装 Directory Server 插件。

此插件

- 通过将加密的密码存储在 Retro Changelog 中，增强了 Directory Server Connector 的更改检测特性

- 对 Active Directory 和 Directory Server 之间的用户属性和密码同步提供双向支持 （请参阅第 42 页的 “使用即时请求密码同步来获取明文密码”）

注意 Directory Server 插件用于四路多主复制 (MMR) 环境。（以前，Identity Synchronization for Windows 仅支持两路 MMR。）

Windows NT Connector 子组件

如果您的安装要求与 Windows NT SAM Registry 同步，则 Identity Synchronization for Windows 安装程序会在安装 Windows NT Connector 的同时将以下子组件安装到 “主域控制器” (PDC) 中：

- **Change Detector**：通过监视 “安全日志”检测用户条目和密码更改事件，然后将这些更改传递到连接器
- **密码过滤器**：捕获在 “NT 域控制器”上的密码更改，并将其安全传送到 NT 连接器

Message Queue

Identity Synchronization for Windows 使用 Message Queue （一个使用发布 / 订阅模式的持久消息队列机制）在目录源之间传播属性和密码更改，并将管理和配置信息分发到管理这些目录源同步的连接器。

Message Queue 是一个执行 Java Message Service (JMS) 开放标准的企业消息系统。JMS 规范描述了一组编程界面，这些编程界面为 java 应用程序在分布环境中创建、发送、接收和读取消息提供了通用方法。

Message Queue 由使用通用消息服务交换消息的消息发布者和订阅者组成。此消息服务由一个或多个专用消息代理程序组成，代理程序负责控制对消息队列的访问，维护有关活动发布者和订阅者的信息以及确保消息传送。

Message Queue 是最佳途径，因为它能够：

- 在连接器之间建立起一个信任系统
- 简化所有组件的安全访问控制
- 方便端到端密码加密
- 确保传送所有密码更新消息
- 降低连接器间的通讯复杂度和安全风险

- 实现分布配置信息的中心授权
- 允许将所有连接器日志集中到一个中心位置

系统组件分布

在制定有效部署方案之前，必须了解 Identity Synchronization for Windows 组件的组织方式和该产品的工作方式。本节内容安排如下：

了解本节和 Deployment Scenario 示例 （第 46 页）中介绍的基本概念后，就应能够以此类推，为更复杂、更灵活的方案创建部署策略 （如混合 Active Directory 和 Windows NT 环境或多服务器环境）。

核心

首先需要将所有 “核心”组件一次性地安装到支持的任何操作系统的目录服务器中。“管理服务器”必须与 “核心”位于相同的机器上。必须在安装 “核心”之前安装 Message Queue 3.5 SP1 Enterprise Edition。

Directory Server Connector 和 Directory Server 插件

可以将 Directory Server Connector 安装到任何支持的操作系统中 （列在第 52 页的 “操作系统要求”中）。不必将 Directory Server Connector 安装在要同步的 Directory Server 所运行的机器上。但是，必须为每个已配置的 Directory Server 源安装一个 Directory Server Connector。

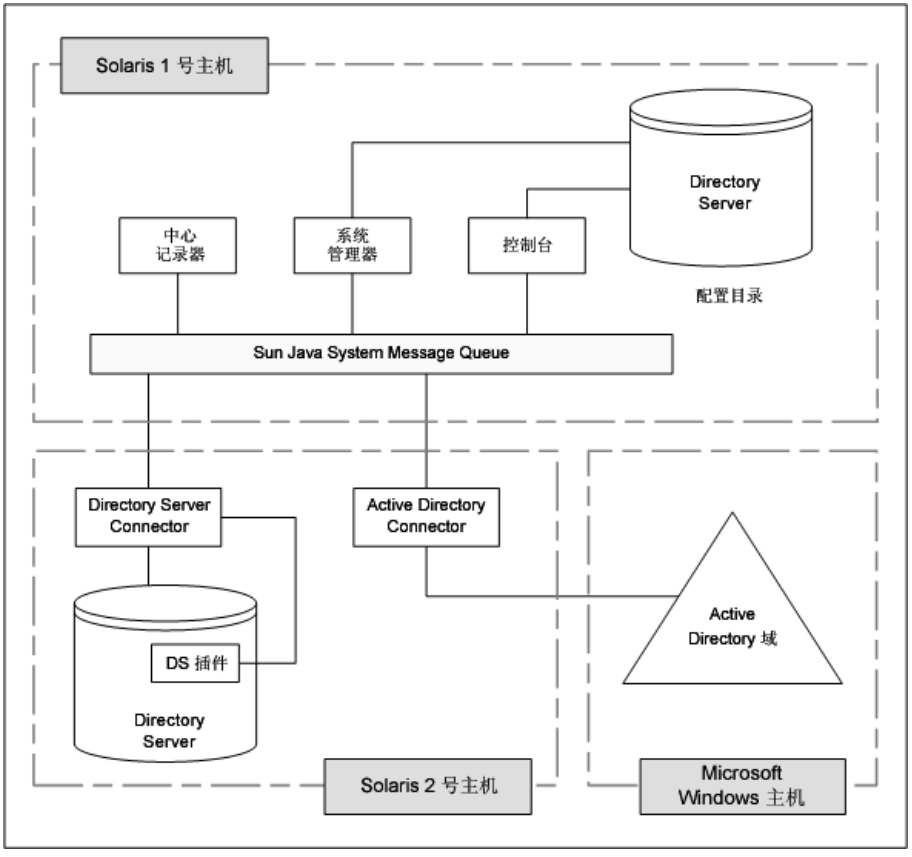
必须在要同步的 Directory Server 所在的每台主机上安装 Directory Server 插件。

注意 需要为每个 Directory Server 源安装单个 Directory Server Connector。但是，应当为每个要同步的主服务器、集线器和用户副本安装 Directory server 插件。

Active Directory Connector

可以在任何支持的操作系统上安装 Active Directory Connector （参见图 1-2）。在 Windows 环境中不必安装 Active Directory Connector ； 但是，每个 Active Directory 域必须安装一个 Active Directory Connector。

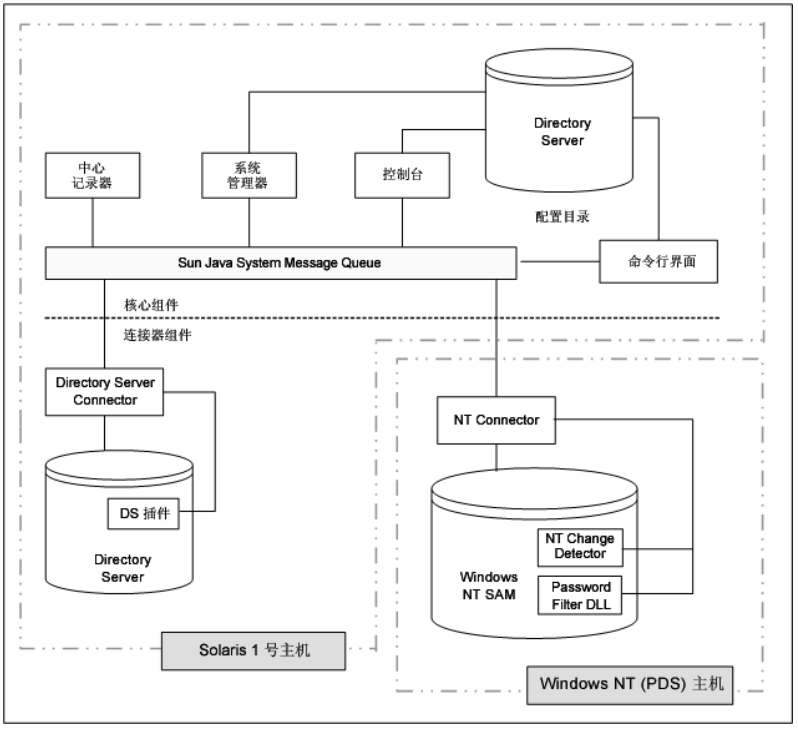
图 1-2 Directory Server 和 Active Directory 组件分布



Windows NT Connector 和子组件

要与 Windows NT SAM Registry 同步 （参见图 1-3），必须在 “主域控制器” (PDC) 中安装 Windows NT Connector。另外，安装程序会将 NT Domain 的 PDC 中连接器与两个 NT Connector 子组件 （Change Detector 和 Password Filter DLL）一同安装。单个 NT Connector 只同步单个 NT 域的用户和密码。

图 1-3 Directory Server 和 NT 组件分布



Identity Synchronization for Windows 如何检测目录源中的更改

本节介绍了 Sun Java System Directory Server (Directory Server)、Windows Active Directory 和 Windows NT Connector 如何检测用户条目和密码更改。

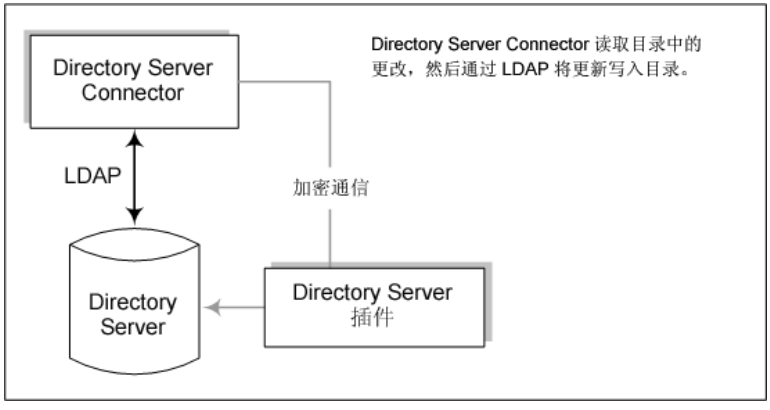
内容具体安排如下：

Directory Server Connector 如何检测更改

Directory Server Connector 通过 LDAP 检查 Directory Server Retro-Changelog，以检测用户条目和密码更改事件。 Directory Server 插件帮助连接器：

- 通过对密码加密，然后使之可在 Retro Changelog 中使用，以捕获明文密码。如果没有插件，则 Retro Changelog 中仅出现散列密码，而散列的密码不能被同步。
- 若执行与 Active Directory 的即时请求密码同步，则无需在 Windows 环境中安装任何 Identity Synchronization for Windows 组件 （请参阅第 42 页的 “使用即时请求密码同步来获取明文密码”）。

图 1-4 Directory Server Connector 检测更改的方式



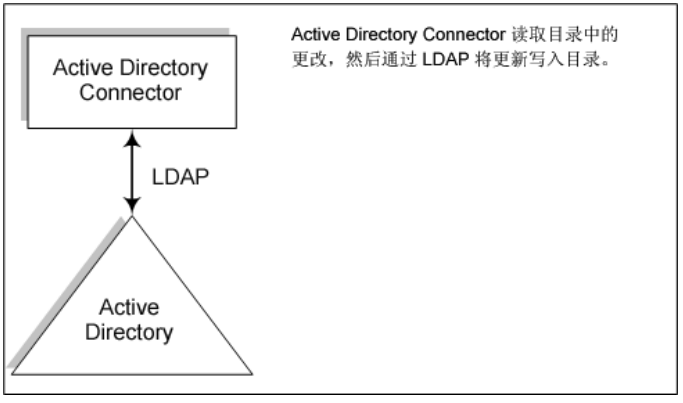
Active Directory Connector 检测更改的方式

Windows 2000/2003 Server Active Directory Connector 通过检查 Active Directory 的 `USNChanged` 和 `PwdLastSet` 属性值来检测用户条目和密码更改。

与 Directory Server 的 Retro Changelog 不同，当更改某个条目中的属性时，Active Directory 不报告哪些属性被更改。取而代之的是， Active Directory 通过累加 `USNchanged` 属性值来确定条目更改。为了检测各个属性的更改， Active Directory 和 Windows NT Connector 使用一个称为*对象高速缓存*的进程内数据库。对象高速缓存中存储每个 Active Directory 条目的一个散列副本，这使得连接器能准确判断条目中哪些属性被修改。

无需在 Windows 环境中安装 Active Directory Connector。它们可运行在其它环境（如 Solaris 计算机）并通过 LDAP 远程检测或进行更改。

图 1-5 Active Directory Connector 检测更改的方式

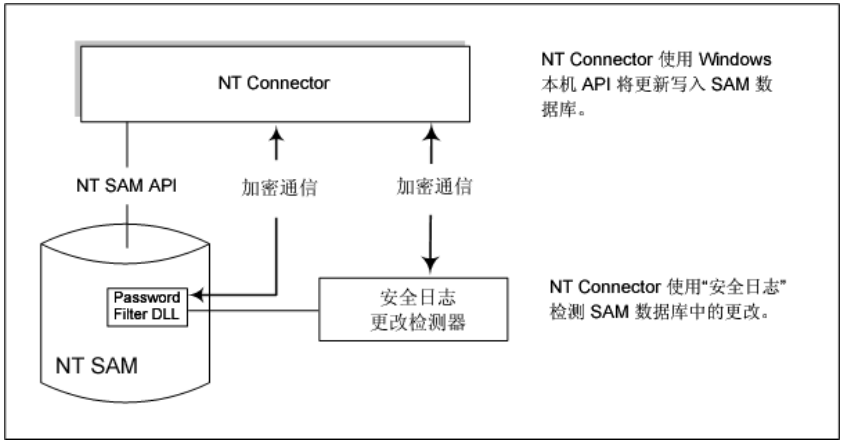


Windows NT Connector 检测更改的方式

Windows NT Connector 通过检查安全日志关于用户对象的审计事件来检测用户条目和密码更改。

要与 Windows NT SAM Registry 同步 （参见图 1-3），必须在 “主域控制器” (PDC) 中安装 Windows NT Connector。另外，安装程序会将 NT 域的 PDC 中的连接器与两个 NT Connector 子组件 （Change Detector 和 Password Filter DLL）一同安装。单个 NT Connector 只同步单个 NT 域的用户和密码。

图 1-6 Windows NT Connector 检测更改的方式



注意 如果部署中有一台 Windows NT 计算机，则必须启用审计，否则 Identity Synchronization for Windows 不能记录来自该计算机的消息。要检验是否在 Windows NT 计算机上启用了审计日志，请参阅第 277 页的 “在 Windows NT 机器上启用审计”。

关于 Change Detector 和 Password Filter DLL 子组件的说明，请查看第 35 页的 “Windows NT Connector 子组件”。

传播密码更新

本节介绍了以下获得在 Windows 系统和 Directory Server 系统之间传播密码更改所需的明文密码的方法：

- 第 42 页的 “使用 Password Filter DLL 来获取明文密码”
- 第 42 页的 “使用即时请求密码同步来获取明文密码”

使用 Password Filter DLL 来获取明文密码

Windows NT Connector 必须获得明文密码才能将密码更新传播到 Sun Java System Directory Server。但是，当密码被存储到 Windows 目录中后，就无法从中提取明文密码，因为此时这些密码已经被加密。

Windows NT 提供了一个 Password Filter DLL 界面，允许组件在明文密码被永久存储到目录之前捕获它们。

使用即时请求密码同步来获取明文密码

尽管 Active Directory 与 Windows NT 支持相同的密码过滤器，但仍必须在每个域控制器上安装 Password Filter DLL，而不能只在主域控制器 (PDC) 上安装。由于这是一个明显的安装负担， Identity Synchronization for Windows 使用一种不同的方法来同步从 Active Directory 到 Directory Server 的密码更改，该方法称为*即时请求密码同步*。

当用户在 Windows 2000 上更改了密码后，如果试图登录 Directory Server，则即时请求密码同步为其提供了一种可在 Directory Server 上获取新密码值的方法。

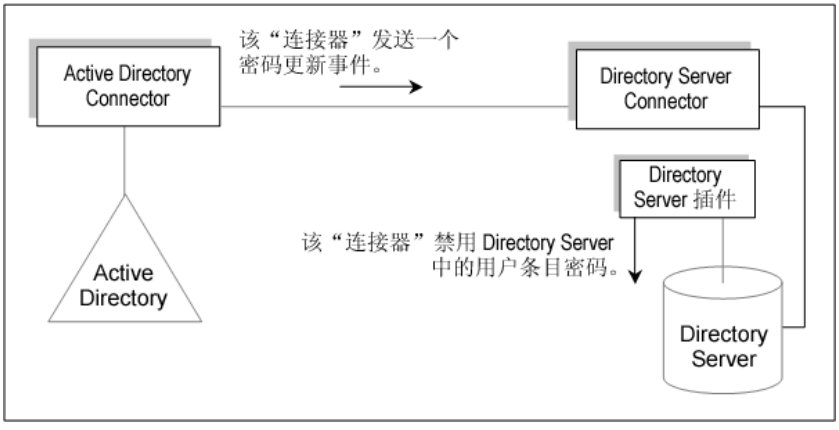
即时请求密码同步还允许同步 Active Directory 上的密码，而无需 Password Filter DLL。

即时请求密码同步过程在下述情况下发生：

1. 用户在 Windows 工作站上按下 Ctrl-Alt-Del，并更改密码。新密码存储到 Active Directory 中。
2. Active Directory Connector 以预定间隔轮询系统。

   当连接器检测到密码更改 （基于对 `USNchanged` （更新序列号）和 `PwdLastSet` 属性的更改）时，连接器在 Message Queue 上发布关于密码更改的消息。消息在 SSL 加密的频道中传输。

图 1-7 即时请求密码同步 — 第一部分

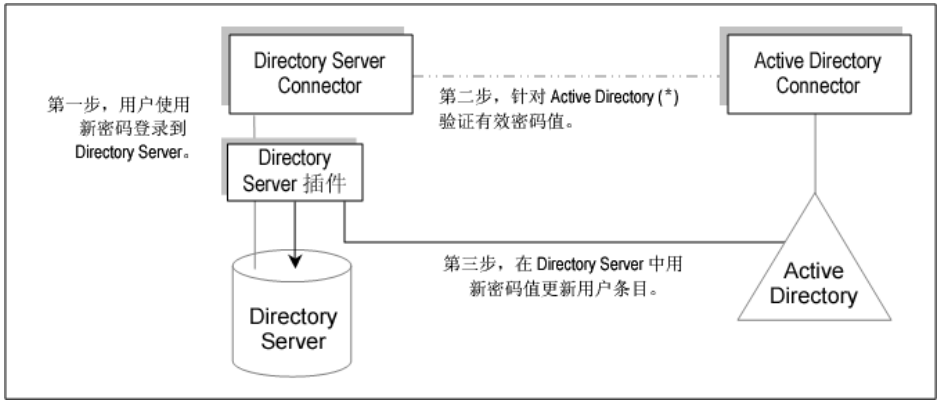


3. Directory Server Connector （通过 SSL）从 Message Queue 中接收密码更改消息。
4. Directory Server Connector 将用户条目的 `dspswvalidate` 属性设置为 `true`，这将使旧密码失效并对 Directory Server 插件发出密码更改警告。
5. 当用户试图登录 Directory Server 并使用 LDAP 应用程序 （例如 Portal Server）来验证登录时， Sun Java System Directory Server 插件会检测出 Directory Server 条目中的密码值无效。
6. Directory Server 插件在 Active Directory 中搜索相应用户。当插件找到该用户时，会尝试使用用户试图登录进入 Directory Server 时提供的密码来绑定到 Active Directory。

注意 即时请求密码同步要求应用程序使用简单的 Directory Server 验证代替更为复杂的验证机制，如 SASL Digest-MD5。

7. 如果成功绑定到 Active Directory，用户提供新的 Active Directory 密码，Directory Server 插件设置密码并从 Directory Server 上的用户条目中清除无效密码标记。

图 1-8 即时请求密码同步 — 第二部分



注意 如果用户验证失败，用户条目密码会保留在 Directory Server 中，同时 Directory Server 和 Active Directory 上的密码将不同步，直到用户使用有效密码登录为止 （对 Active Directory 进行登录验证的密码）。

可靠同步

Identity Synchronization for Windows 采取多项预防措施来确保不丢失用户更改事件 — 即使组件暂时不可用。 Identity Synchronization for Windows 的可靠性与 TCP 网络协议类似。 TCP 可确保即便使用有损耗和时断时续连接的网路，最终也将正确传输所有数据。在网络临时中断期间发送的数据在网络断开时排队等待，一旦连接恢复将被再次传送。如果下列组件之一临时失效，则 Identity Synchronization for Windows 将最终检测和应用用户更改事件：

- 连接器
- Directory Server
- Message Queue
- Active Directory 域控制器
- Windows NT 主域控制器
- 系统管理器
- 配置目录

如果这些组件之一不可用， Identity Synchronization for Windows 将延迟同步，直到受影响的组件可用且未丢失任何更改 （甚至密码）。该版本 Identity Synchronization for Windows 不支持 Sun Cluster 或其它正确、高可用性解决方案。由于 Identity Synchronization for Windows 是一个后台应用程序，用户不直接与其交互，因此通常不要求高可用性。如果曾遇到灾难性故障，可以重新安装 Identity Synchronization for Windows 组件并使用 `idsync resync` 命令重新同步所有目录源。

在多数情况下，当一个组件不可用时，程序将对同步事件进行排队，并仅当组件变为可用时应用这些事件。该过程有两个例外：

- 在多主复制 (MMR) Directory Server 环境中，对 Windows 用户的外部更改可被同步到首选或备用 Directory Server。

  如果首选 Directory Server 不可用， Directory Server Connector 会将更改应用到备用服务器上。 Identity Synchronization for Windows 将不检测和传播在任何 Directory Server 主机上进行的外部更改，直到首选主机可用。

- 由于 Active Directory Connector 仅可与单独的 Active Directory 域控制器通信，当执行即时请求密码同步时，所有 Active Directory 域控制器之间的 Directory Server 插件可能会失败。这就是执行故障转移最为重要的原因 — 如果 Directory Server 插件不能联系 Active Directory 域控制器以检验用户的新密码，则用户将不能登录到 Directory Server。

部署示例：两台机器配置

本节介绍了一个部署方案，在该方案中，使用 Identity Synchronization for Windows 同步 Sun 和 Windows 目录之间的用户对象创建和双向密码修改操作。

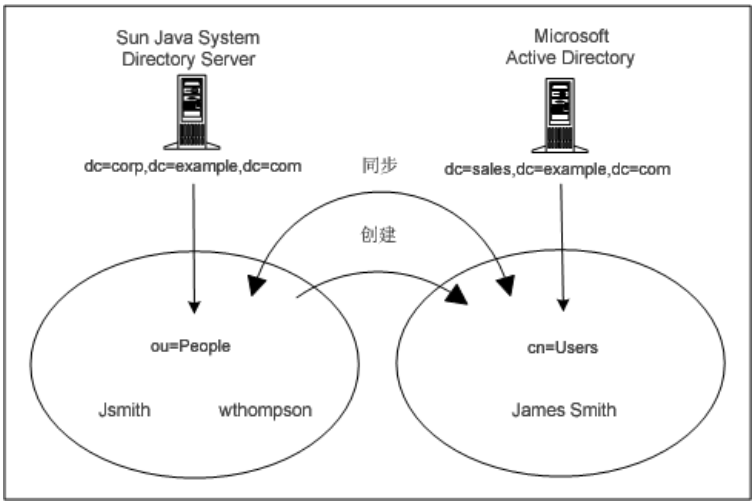
该部署方案由两个系统组成：

- 运行 Sun Java System Directory Server 的系统 （主机名：*corp.example.com*）
- 在 Windows 2000 服务器上运行 Active Directory 的系统 （主机名：*sales.example.com*）

注意 虽然在本方案中未使用 NT，但请注意 Identity Synchronization for Windows 同样支持与 NT 域同步。

图 1-9 说明了用于本部署方案的同步要求 （节点结构和相关属性值）。

图 1-9 同步要求



本方案要达到两个目标：

- 在*用户子树*（Directory Server 中的 *ou=people* 和 Active Directory 中的 *cn=users*）之间双向同步用户密码，即无论何时更改其中一个目录中的用户密码，该密码更改都会同步到另一个目录中的关联用户。

  例如，如果您更改了 Directory Server 上 *ou=people* 容器中 uid=JSmith 的密码，则新密码将自动同步到 Active Directory 服务器上 *cn=users* 容器的 cn=Joe Smith。

- 只从 Directory Server 用户子树到 Active Directory 用户子树同步用户对象创建操作。

  例如，如果您创建含有指定属性集的新用户 （*ou=People* 容器中 uid=Wthompson），则 Identity Synchronization for Windows 将在 Active Directory 上为 Wthompson （*cn=Users* 容器中 cn=William Thompson）创建具有相同属性集的新帐户。

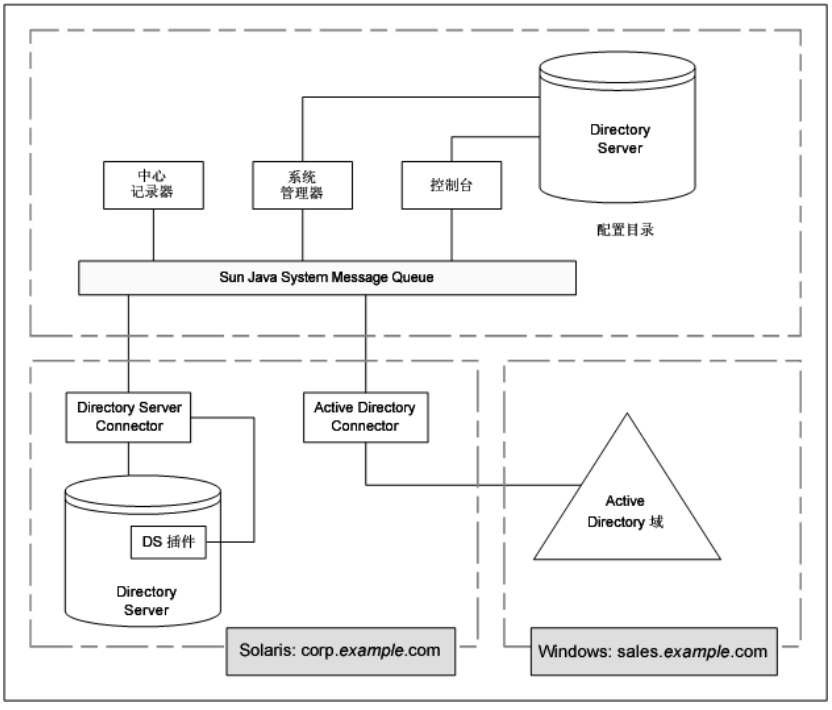
注意 Identity Synchronization for Windows 支持相同类型的多个同步源（例如，您可以在部署中拥有多个 Directory Server 或多个 Active Directory 域）。

创建、修改和删除同步设置是整个目录集的全局设置，不能指定用于单个目录源。如果从 Sun 至 Windows 同步用户对象创建，则用户对象创建将从*所有* Sun Directory Server 传播至安装中所配置的*所有* Active Directory 域和 Windows NT 域。

物理部署

图 1-10 说明当 Active Directory 域驻留在未安装任何组件的单独 Active Directory 域控制器中时，如何在单个 Solaris 主机中对所有产品的组件进行物理部署。

图 1-10 Directory Server 和 Active Directory 方案



组件分布

主机 *corp.example.com* 是安装在 Solaris 操作系统中的 Directory Server。要同步的 Directory Server 的根后缀是 *dc=corp,dc=example,dc=com*。

此机器含有：

- Identity Synchronization for Windows “核心”组件
- Identity Synchronization for Windows Directory Server Connector
- Identity Synchronization for Windows Directory Server 插件
- Identity Synchronization for Windows 配置目录（位于与要同步的 Directory Server 机器不同的 Directory Server 示例上）

主机 *sales.example.com* 是要同步的 Active Directory 域。

第 2 章

准备安装

在安装 Identity Synchronization for Windows 1 2004Q3 或从版本 1.0 移植至版本 1 2004Q3 之前，应先熟悉安装及配置过程。

本章介绍了这些过程，并提供有助于准备本产品安装的其它信息。这些信息被编排在以下各节中：

安装要求

本节说明 Identity Synchronization for Windows 的安装要求，包括操作系统版本、修补程序和每个平台的实用程序。

操作系统要求

以下各表描述了本版本 Identity Synchronization for Windows 的操作系统要求：

表 2-1 Solaris 要求

组件	Solaris 要求
核心组件	Solaris 8™ for UltraSPARC®（32 位和 64 位） Solaris 9™ SPARC® Platform Edition （32 位和 64 位） Solaris 9™ 操作系统 （x86 Platform Edition for Pentium II 或更高版本） IA-32
用于 Sun Java™ System Directory Server 和 Windows Active Directory 的连接器	Solaris 8 for UltraSPARC （32 位和 64 位） Solaris 9 for SPARC 平台 （32 位和 64 位） Solaris 9 操作系统 （x86 Platform Edition for Pentium II 或更高版本） IA-32
用于 Sun Java™ System Directory Server 的插件	Solaris 8 for UltraSPARC （32 位和 64 位） Solaris 9 for SPARC 平台 （32 位和 64 位） Solaris 9 操作系统 （x86 Platform Edition for Pentium II 或更高版本） IA-32

表 2-2 Windows 要求

组件	Windows 要求
核心	Windows 2000 Server SP4 Windows 2000 Advanced Server SP4
	Windows 2003 Server 标准版 （具有最新的安全更新）
	Windows 2003 Server 企业版 （具有最新的安全更新）
用于 Sun Java™ System Directory Server 和 Windows Active Directory 的连接器	Windows 2000 Server SP4 Windows 2000 Advanced Server SP 4
	Windows 2003 Server 标准版 （具有最新的安全更新）
	Windows 2003 Server 企业版 （具有最新的安全更新）
用于 Sun Java™ System Directory Server 的插件	Windows 2000 Server SP4 Windows 2000 Advanced Server SP 4
	Windows 2003 Server 标准版 （具有最新的安全更新）
	Windows 2003 Server 企业版 （具有最新的安全更新）
NT Connector 和子组件	Windows Primary Domain Controller NT 4.0 Server SP 6A （仅限 x86）

硬件要求

要运行 Identity Synchronization for Windows，您的硬件 （所有平台）必须满足以下最低要求：

- 在 Directory Server 上进行最小安装需要大约 400 MB 磁盘空间。
- 运行任何 Identity Synchronization for Windows 组件的服务器需要至少 512 MB RAM。（最好有更多内存。）

Sun Java System 软件要求

在安装 Identity Synchronization for Windows 之前，必须先安装以下 Sun Java System 软件组件：

- Sun Java System Directory Server 版本 5 2004Q2 修补程序 117907-02 （或更高版本）

  该修补程序为安装在 Directory Server 5 2004Q2 中的 Identity Synchronization for Windows 1 2004Q2 启用了删除功能。

  - **对于 Solaris SPARC 软件包格式**：修补程序编号 117907-02 或更高
  - **对于 Solaris SPARC 压缩归档安装**：修补程序 5077789
  - **对于 Solaris x86 软件包格式**：修补程序编号 117908-02 或更高
  - **对于 Solaris x86 压缩归档安装**：修补程序 5077789
  - **对于 Windows 压缩归档安装**：修补程序 5077789

  有关这些修补程序的更多详细信息及如何将其应用于 Directory Server 环境的信息，请参阅 `README.patch` 文件，该文件位于 Identity Synchronization for Windows 下载包的以下目录中：

  `<`*`download_root`*`>/patches/directory/README.patch`

  有关在 Solaris 上安装 Directory Server 5 2004Q2 所需的修补程序的最新信息，请参阅 《*Sun Java System Directory Server 5 2004Q2 Installation and Tuning Guide*》和 《*Sun Java System Directory Server 5 2004Q2 发行说明*》。它们可以在下面的网站中找到：

  `http://docs.sun.com/db/coll/DirectoryServer_04q2`

- Sun Java System Message Queue （以前是 Sun ONE Message Queue）版本 3.5 SP1 企业版。

注意	Identity Synchronization for Windows 版本 1.0 已安装 Message Queue，*而版本 1 2004Q3 未安装*。 要在*已存在* Sun Java System Message Queue 的安装上安装 Identity Synchronization for Windows “核心”，必须使用 Message Queue 版本 3.5 SP1 企业版。试图在不适当的 Message Queue 版本上安装 “核心”将会失败。

Identity Synchronization for Windows 下载包中包含 Message Queue。可从各平台的 /messagequeue 目录中获取该软件，如下所示：

- **Solaris SPARC**：/messagequeue/imq3_5-ent-solsparc.zip
- **Solaris x86**：/messagequeue/imq3_5-ent-soli386.zip
- **Windows**：/messagequeue/imq3_5-ent-win.exe

- Java Runtime Environment

  Java Runtime Environment (JRE) 不随本产品一起提供。

  - 必须安装 J2SE （或 JRE） 1.4.2_04 （或更高版本）才能在 Solaris 或 Windows 上运行 Identity Synchronization for Windows 安装程序。
  - 必须在 Windows NT 上安装 JRE 1.4.1_03 （或更高版本）。

安装证书

要安装 Identity Synchronization for Windows，必须为以下目标提供证书：

- 配置目录
- 要同步的 Directory Server
- Active Directory （有关详细信息，请参阅 “安装核心”。）

此外，必须具有以下权限才能安装 Identity Synchronization for Windows：

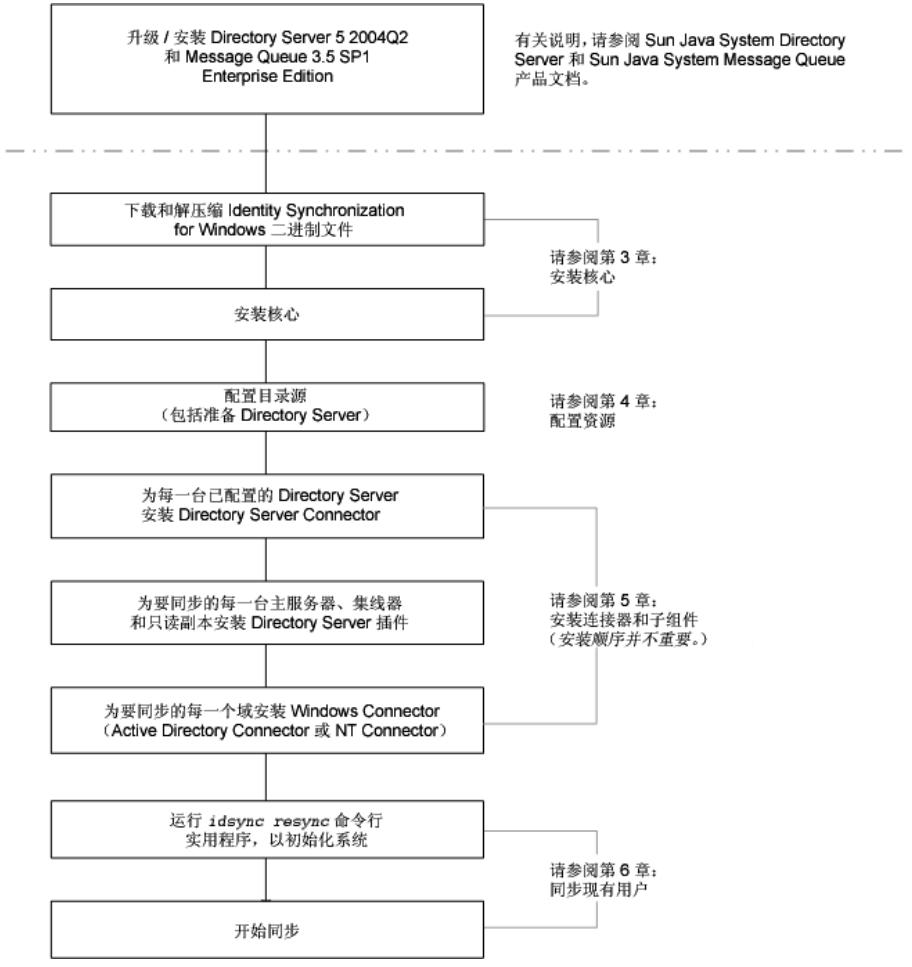
- **在 Solaris 系统中**：必须以*超级用户*身份安装。
- **在 Windows 系统中**：必须以*管理员*身份安装。

注意 使用基于文本的安装程序输入密码时，程序将自动屏蔽密码，从而密码不会以明文显示。只有 Solaris 系统支持基于文本的安装程序。

安装概述

图 2-1 说明在单主机部署中安装本产品的过程。

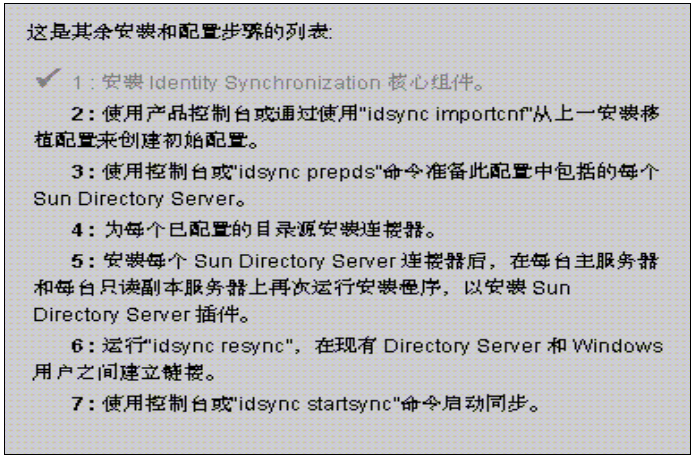
图 2-1 在单主机部署中安装



某些组件必须按照特别的顺序进行安装，因此请务必仔细阅读全部安装说明。

Identity Synchronization for Windows 提供 “待执行”列表，它在整个安装和配置过程中显示。此信息面板列出要成功安装和配置本产品所必须遵循的所有步骤。

图 2-2 Identity Synchronization for Windows 待执行列表



当您逐步执行安装和配置过程时，程序会将列表中所有已完成的步骤变灰 （如图 2-2 所示）。

本节的其余部分提供安装和配置过程的概述，并编排为如下内容：

- 第 58 页的 “安装核心”
- 第 58 页的 “配置产品”
- 第 58 页的 “准备 Directory Server”
- 第 59 页的 “安装连接器和 Directory Server 插件”
- 第 60 页的 “同步现有用户”

注意 本手册后面的部分会提供详细的安装和配置说明。

安装核心

安装 “核心”时，将安装以下组件：

- **控制台**：提供一个集中位置，以执行产品组件的所有配置和管理任务
- **中心记录器**：将所有审计和错误日志信息集中到一个中心位置
- **系统管理器**：动态地向连接器提供配置更新，并保持每个连接器的状态

注意	有关安装 “核心”的说明，请参阅第 3 章，“安装核心”。

配置产品

安装 “核心”之后，便可使用 “控制台”从一个集中位置对全部要同步的目录源（及其它部署特性）进行初始配置。

注意	有关配置目录源的说明，请参阅第 4 章，“配置核心资源”。

准备 Directory Server

Directory Server Connector 支持 Sun Java System Directory Server 5 2004Q2。

在能够安装 Directory Server Connector 之前，必须为每个已配置并要同步的 Directory Server 主服务器 （包括首选主服务器和备用主服务器）准备一个 Sun Java System Directory Server 源。

可以从 “控制台”或从命令行使用 `idsync prepds` 子命令执行此任务。

注意	有关准备 Directory Server 的说明，请参阅第 109 页的 “准备 Directory Server”。

安装连接器和 Directory Server 插件

可以安装任意数量的连接器和 Directory Server 插件，具体数量视系统包含的已配置目录数而定。

注意 “控制台”和安装程序都使用要同步目录的*标签*将连接器与该目录相关联。表 2-3 描述 Identity Synchronization for Windows 的标签命名约定。

表 2-3 标签命名约定

连接器类型	目录源标签	子组件
Directory Server Connector	根后缀或后缀 / 数据库	Directory Server 插件 在每个 Directory Server （主服务器或用户服务器）中为要同步的根后缀安装一个 “插件”。
AD Connector	域名	无
NT Connector	域名	（自动与 Window NT Connector 一起安装） Change Detector 和 Password Filter DLL 子组件共同安装在同一安装中。 必须使用图形用户界面 (GUI) 安装程序安装 Windows NT Connector。

注意 有关安装和配置 “连接器”和 Directory Server 插件的说明，请参阅第 5 章，“安装连接器和 Directory Server 插件”。

同步现有用户

安装连接器、插件和子组件后，必须运行 `idsync resync` 命令行实用程序以引导包含现有用户的部署。此命令使用管理员指定的匹配规则实现：

- 链接现有条目 （有关*链接*的定义，请参阅第 176 页的 “链接用户”。）
- 用远程目录的内容填充空目录
- 在两个现有用户群体之间批量同步属性值 （包括密码），在这两个用户群体中，会唯一确定 Windows 和 Directory Server 目录中的条目，并彼此链接。

注意 有关在部署中同步现有用户的说明，请参阅第 6 章，“同步现有用户”。

配置概述

安装本产品之后，必须配置产品部署，其中包括：

- 配置要同步的目录和全局目录
- 指定用于属性修改和对象激活 / 禁用的同步设置
- 指定在已配置目录之间进行用户条目创建和删除同步的设置 （可选）

本节概括说明了以下配置元素概念：

- 第 61 页的 “目录”
- 第 62 页的 “配置目录和全局目录”
- 第 62 页的 “同步设置”
- 第 63 页的 “对象类”
- 第 63 页的 “属性和属性映射”
- 第 65 页的 “同步用户列表”

注意 本手册的后面部分会提供详细的配置说明。

目录

目录代表：

- 一个或多个 Sun Java System Directory Server 中的单个根后缀 （后缀 / 数据库）
- Windows 2000 或 Windows 2003 Server Active Directory 森林结构中的单个 Active Directory 域
- 单个 Windows NT 域

可为每类目录配置任意数量的目录。

配置目录和全局目录

Identity Synchronization for Windows 将 Sun Java System Directory Server 配置目录和 Active Directory 全局目录用作信息库，在其中获取 Directory Server 或 Active Directory 目录拓扑以及这些目录的模式信息。

同步设置

同步设置用于控制在 Sun 和 Windows 目录之间传播对象创建、对象删除、密码及其它属性修改的方向。同步流动选项列出如下：

- 从 Sun 至 Windows
- 从 Windows 至 Sun
- 双向

注意 在包含 Active Directory 和 Windows NT 的配置中，无法保存这样的配置，即，用于在 Windows NT 和 Sun 以及 Active Directory 和 Sun 之间同步创建或修改的不同同步设置。

对象类

配置资源时，您将根据条目的*对象类*来指定要同步的条目。对象类可确定哪些*属性*可用于 Directory Server 和 Active Directory 同步。

注意 对象类不适用于 Windows NT。

Identity Synchronization for Windows 支持两种类型的对象类：

- **结构对象类**：从选定 Directory Server 创建或同步的每个条目必须至少含有一个结构对象类。从下拉列表中选择结构对象类。（在 Directory Server 上*默认为 inetorgperson*，而在 Active Directory 上默认为 *User*）
- **辅助对象类**：
  - **Directory Server** 允许从“可用辅助对象类”列表窗格中选择一个或多个对象类，以扩充选定的结构类，从而提供更多同步属性。
  - **Active Directory** 对辅助对象类更具限制性。选定结构对象类中所有有效辅助对象类的属性均可进行同步。

注意 关于配置对象类和属性的详细信息，请参阅第 4 章，“配置核心资源”。

属性和属性映射

属性保留与用户条目有关的说明性信息。每个属性都有一个标签、一个或多个值，并且遵循可作为属性值存储的信息类型的标准语法。

注意 可从“控制台”定义属性。在第 4 章中提供了有关定义属性的操作说明。

属性类型

Identity Synchronization for Windows 以下述方式同步*重要*属性和*创建*用户属性：

- **重要属性**：只要修改属性，便按照指定的修改同步设置在 Sun 和 Windows 目录间实现同步。

- **创建属性**：只要创建新用户，便按照指定的对象创建同步设置在 Sun 和 Windows 目录间实现同步。

  *强制创建属性*是被视为 “强制”创建的属性，用以在目标目录中成功完成创建操作。例如， Active Directory 期望在创建时， cn 和 samaccountname 都具有有效的值。在 Sun 端，如果配置 user 对象类的 inetorgperson，则 Identity Synchronization for Windows 会将 cn 和 sn 视为强制创建属性。

  *仅*当自原始目录传播的属性中不含值时，才会使用创建属性的默认值更新目标目录的创建属性。（创建属性的默认值可以视其它属性值而定。请参阅第 64 页的 “参数化属性默认值”。）

注意	重要属性自动作为创建属性而进行同步，反之则不然。创建属性仅在用户创建期间被同步。

参数化属性默认值

Identity Synchronization for Windows 允许使用其它创建属性或重要属性为创建属性创建*参数化*默认值。

要创建参数化默认属性值，请在表达式字符串中插入现有创建属性或重要属性的名称 （前后加上百分号 (%<*attribute_name*>%)）。例如， homedir=/home/%uid% 或 cn=%givenName%.%sn%。

创建这些属性默认值时：

- 可在创建表达式 (cn=%givenName% %sn%) 中使用多个属性，但 %<*attribute_name*>% 中的属性必须有单个值。
- 如果 A=%B%，则 B 只能有一个默认值。
- 引用时可使用反斜杠符号 (\) （例如， diskUsage=0\%）。
- 请勿使用有循环代换条件的表达式 （例如， sn=%uid% 和 uid= %sn%）。

映射属性

定义要同步的属性后，必须在 Sun 和 Windows 系统间映射属性名称。例如，必须将 Sun inetorgperson 属性映射到 Active Directory user 属性。

注意	属性映射用于 “重要”和 “创建”两类属性，而且必须为每种目录类型中的所有 “强制创建属性”配置属性映射。

同步用户列表

可创建 “同步用户列表” (SUL) 来定义 Sun 和 Windows 目录中要同步的具体用户。这些定义可以实现平面 “目录信息树” (DIT) 到分层目录树的同步。

以下概念用于定义 “同步用户列表”：

- **基本 DN**（不适用于 Windows NT）：包括该 DN 中的所有用户，除非另一个 SUL 更具体，或有的用户已被过滤器排除。
- **过滤器**：使用用户条目中的属性排除同步的用户，或将具有相同基本 DN 的用户分为多个 SUL。此过滤器使用 LDAP 过滤器语法。
- **创建表达式**（不适用于 Windows NT）：建立创建新用户的 DN，例如，`cn=%cn%,ou=sales,dc=example,dc=com` ，其中 `%cn%` 用现有用户条目的 `cn` 值替换。创建表达式必须以基本 DN 结束。

SUL 包括两个定义，每个定义都按照拓扑意义上的目录类型确定要同步的用户组。

- 一个定义确定要同步的 Directory Server 用户 （例如：`ou=people, dc=example, dc=com`）
- 另一个定义确定要同步的 Windows 用户 （例如：`cn=users, dc=example, dc=com`）

准备创建 SUL 时，请考虑以下问题：

- 要同步哪些用户？
- 哪些用户不在同步之列？
- 应在何处创建新用户？

注意 有关创建 SUL 的详细信息，请参阅附录 D。

移植至版本 1 2004Q3

从 Identity Synchronization for Windows 版本 1.0（或版本 1.0 SP1）进行移植所用的步骤与首次安装 1 2004Q3 的步骤类似，少数步骤除外。

注意 在第 7 章中介绍了相关的移植步骤

在移植至 Identity Synchronization for Windows 1 2004Q3 之前，应注意以下几点：

- 在安装连接器之后，必须手动恢复 Directory Server Connector 状态文件以及 Active Directory 和 NT Connector 对象高速缓存文件。请确保有足够的磁盘空间（根据 `/isw-home/persist` 目录和子目录的大小）用于保存每个 Active Directory 和 NT Connector 对象高速缓存的副本。
- 必须卸载版本 1.0 和 1.0 SP1 的所有组件。

  如果版本 1 2004Q3 的安装程序发现版本 1.0 系统的残留内容，则可能导致安装到 Directory Server 上的 Identity Synchronization for Windows 模式和实际安装到机器上的 Identity Synchronization for Windows 二进制文件出现问题。

  注意 有关详细信息，请参阅第 205 页的 “如果 1.0 卸载失败应采取何种措施”。

- 必须将 Identity Synchronization for Windows 1 2004Q3 组件安装到安装版本 1.0 的平台和硬件体系结构上。

与 Active Directory 同步密码

Windows 2000 上的默认密码策略在 Windows 2003 中已更改，以在默认情况下强制实施严格的密码。

Identity Synchronization for Windows 服务有时必须创建没有密码的条目 （例如，在从 Directory Server 到 Active Directory 的 `resync -c` 期间）。因此，如果在 Active Directory （Windows 2000 或 2003 上）上或在 Directory Server 上启用了密码策略，会导致用户创建错误。

虽然不必禁用 Active Directory 或 Directory Server 上的密码策略，但应了解在不同系统上强制实施密码策略的相关问题。

如果您要与 Windows 2003 Server 标准版或企业版上的 Active Directory 同步密码，则下面的安装信息非常重要：

- 如果安装在 Windows 上，则可在 Solaris 上安装 Active Directory Connector。

  注意 Active Directory Connector 将与 Windows 2000 和 Windows 2003 Server 上的 Active Directory 一起工作。

- 使用对 Windows 2000 上的 Active Directory 所采取的相同步骤，为 Windows 2003 Server 创建目录源、全局目录和 “同步用户列表”。
- 在 Windows 2003 Server 上，默认密码策略强制实施严格的密码，该密码策略并不是 Windows 2000 上的默认密码策略。

本节余下的内容编排如下：

- 第 68 页的 “强制实施密码策略”：如果必须在 Windows 或 Directory Server 上强制实施密码策略，请阅读本节提供的信息，以了解密码策略如何能够影响 Active Directory 和 Directory Server 间的同步结果。
- 第 73 页的 “密码策略示例”：本节提供一些用于不同方案的密码策略示例。

强制实施密码策略

本节解释 Active Directory （在 Windows 2003 Server 和 Windows 2000 环境下）以及 Sun Java System Directory Server 5 2004Q2 的密码策略如何能够影响同步结果。

内容具体安排如下：

概述

如果在 Active Directory （或 Directory Server）上创建的用户满足相应系统要求的密码策略，则可创建这些用户，并可在两个系统间正确同步。如果在两个系统上都启用了密码策略，则密码必须同时满足两个系统的策略，否则同步用户创建将失败。

- 如果在 Active Directory 上启用了密码策略功能，则应在 Directory Server 上启用类似配置或匹配的密码策略。
- 如果不能在 Active Directory 和 Directory Server 上创建一致的密码策略，则应启用您认为对密码和用户创建更为可靠的源上的密码策略。但是在某些情况下，由于某些密码策略配置原因，用户创建将无法按预期执行。

重要说明

以下各节提供关于密码策略的重要信息：

Directory Server 密码策略

如果在 Active Directory 中创建的用户所具有的密码违反 Directory Server 的密码策略，则尽管*仍会*创建这些用户并在 Directory Server 中同步，但创建的条目将不含密码。新用户登录到 Directory Server （此时将触发即时请求密码同步）之前将不会设置密码。而由于登录密码违反 Directory Server 密码策略，此时的登录将失败。

可以采用几种方法从这种状况恢复：

- 强制用户在下次登录 Active Directory 时更改其密码

- 更改 Active Directory 上的用户密码，并确保新密码满足 Directory Server 密码策略要求

您可能要查看 Active Directory 和 Directory Server 上设置的密码策略是否等效（或尽可能相似）。

Active Directory 密码策略

如果在 Active Directory 上创建了不符合 Active Directory 密码策略的用户，则在 Directory Server 上*将会*创建这些用户。

- 如果密码不符合 Active Directory 密码策略要求，则 Active Directory 实际上只是临时创建用户，随后即会删除相应条目。因此， Active Directory Connector 会发现此类临时 `ADD`，然后在 Directory Server 端创建用户。这些用户在 Directory Server 中不具有密码，因此没有人能够以这种用户身份登录。另外，这些条目不会链接到 Active Directory 中的有效条目。如果是从 Active Directory 到 Directory Server 对删除操作进行同步，这些临时创建的用户将会被自动删除。
- 在 Directory Server 上创建了没有密码的用户。除非用户条目中包含密码，否则 Directory Server 不会对用户创建强制实施密码策略。

可以采用几种方法从这种状况进行恢复。首选方法是从 Active Directory 到 Directory Server 同步删除。或者，可从 Directory Server 中删除用户，然后使用符合 Active Directory 密码策略的有效密码将它们添加至 Active Directory。此方法可以确保在 Directory Server 上创建用户并且链接正常。当 Directory Server 上的用户首次登录 Active Directory 并更改密码后，他们将使其密码失效。

- 如果不从 Directory Server 中删除用户，然后试图使用新密码重新添加该 Active Directory 用户，则将用户添加到 Directory Server 的 `ADD` 操作将失败，因为 Directory Server 中已经存在该用户。这些条目将不会链接在一起，您必须运行 `idsync resync` 命令才能链接两个单独帐户。
- 如果运行 `idsync resync` 命令，则必须确保为链接至 Directory Server 条目的 Active Directory 上的帐户重设密码。重设密码操作会使 Directory Server 上的相应密码失效，从而在用户下次以其新的 Active Directory 密码进行 Directory Server 验证时强制执行即时请求同步，以更新 Directory Server 密码。

创建没有密码的帐户

在某些情况下 （如重新同步）， Identity Synchronization for Windows 必须创建没有密码的帐户。

Directory Server 当 Identity Synchronization for Windows 在 Directory Server 中创建没有密码的条目时，它会将 `userpassword` 属性设置为 `{PSWSYNC}*INVALID*PASSWORD*`。在重设密码之前，用户将不能登录至 Directory Server。其中的一个例外是运行含有 `-i NEW_USERS` 或 `NEW_LINKED_USERS` 选项的 `resync` 命令。此时， resync 将使新用户的密码失效，并会在用户下次登录时触发即时请求密码同步。

Active Directory 当 Identity Synchronization for Windows 在 Active Directory 中创建没有密码的条目时，它会将用户密码设置为随机选择的重要密码，该密码符合 Active Directory 密码策略要求。此时，会记录一条警告消息，且在重设密码前，用户不能登录至 Active Directory。

下面的表格说明在您使用 Identity Synchronization for Windows 时可能遇到的一些不同方案：

- 表 2-4 说明密码策略如何影响同步。
- 表 2-5 说明密码策略如何影响重新同步。

这些信息可以作为帮助确保密码保持同步的指导原则。（由于系统配置各不相同，故这些表格并不包含所有可能的配置方案。）

表 2-4 密码策略如何影响同步行为

方案			结果		
用户最初创建于	**用户符合的密码策略**		**用户创建于**		
	Directory Server	**Active Directory**	**Directory Server**	**Active Directory**	**注释**
Active Directory	是	是	是	是	
	是	否	**是（参见注释）**	否	用户将创建于 Directory Server 中。不过，如果从 Active Directory 到 Directory Server 同步删除，则会立即删除此用户。 有关详细信息，请参阅第 69 页的“Active Directory 密码策略”。
	否	是	**是**	是	有关详细信息，请参阅第 68 页的“重要说明”。
	否	否	**是（参见注释）**	否	用户创建于 Directory Server 中。不过，如果从 Active Directory 到 Directory Server 同步删除，则会立即删除此用户。 有关详细信息，请参阅第 69 页的“Active Directory 密码策略”。
Directory Server	是	是	是	是	
	是	否	是	否	
	否	是	否	否	
	否	否	否	否	

表 2-5 密码策略如何影响重新同步行为

Resync 命令	方案 用户满足的密码策略		结果
	Directory Server	Active Directory	
`resync -c -o Sun`	N/A	是	用户创建于 Active Directory 中，但不能登录。 有关详细信息，请参阅第 69 页的 “创建没有密码的帐户”。
	N/A	否	用户创建于 Active Directory 中，但不能登录。 有关详细信息，请参阅第 69 页的 “创建没有密码的帐户”。
`resync -c -i NEW_USERS | NEW_LINKED_USERS`	是	N/A	用户将创建于 Directory Server 中，并在该用户首次登录时设置其密码。 有关详细信息，请参阅第 69 页的 “创建没有密码的帐户”。
	否	N/A	用户将创建于 Directory Server 中，但由于这些用户的密码违反 Directory Server 密码策略，他们无法登录。 有关详细信息，请参阅第 68 页的 “重要说明”和第 69 页的 “创建没有密码的帐户”。
`resync -c`	是	N/A	用户将创建于 Directory Server 中，但在 Active Directory 或 Directory Server 中设置新的密码值之前，这些用户无法登录。 有关详细信息，请参阅第 69 页的 “创建没有密码的帐户”。
	否	N/A	用户将创建于 Directory Server 中，但在 Active Directory 或 Directory Server 中设置新的密码值之前，这些用户无法登录。 有关详细信息，请参阅第 69 页的 “创建没有密码的帐户”。

密码策略示例

本节介绍使用以下规范的 Active Directory 和 Directory Server 密码策略的不同方案的示例：

- **对于 Active Directory：**
  - 强制实施密码历史：20 天
  - 密码最长使用期限：30 天
  - 密码最短使用期限：0 天
  - 密码长度最小值：7 个字符
  - 密码必须满足复杂性要求：已启用
- **对于 Directory Server：**
  - 用户必须在重设密码后更改密码
  - 用户可以更改密码
  - 在历史记录中保留 20 个密码
  - 密码在 30 天后到期
  - 在密码到期前 5 天发送警告
  - 检查密码语法：密码最小长度为 7 个字符

错误消息

在 “核心” 系统的中心记录器 `audit.log` 文件中检查以下错误消息：

由于密码策略的原因而无法在即时请求同步期间更新 DS 上的密码：

```
WARNING 125 CNN100 hostname "DS Plugin (SUBC100):unable to update password
of entry 'cn=John Doe,ou=people,o=sun', reason:possible conflict with local
password policy"
```

注意 有关 Windows 2003 密码策略的详细信息，请参阅 http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dsscc_aut_xbby.asp

有关 Directory Server 5 2004Q2 密码策略的详细信息，请参阅

http://docs.sun.com/db/coll/DirectoryServer_04q2

配置 Windows 以使用 SSL 操作

如果计划将密码更改从 Directory Server 传播至 Windows Active Directory 服务器，则必须将每个 Active Directory 服务器都配置为使用 SSL 且必须安装高级加密包。

如果 Active Directory 中基于 SSL 的 LDAP 已经通过从 Microsoft Certificate Services Enterprise Root 证书授权机构自动获得证书而启用，则 Identity Synchronization for Windows Active Directory Connector 安装程序能够自动在 Active Directory Connector 中建立 SSL，如以下网站中所述：

http://support.microsoft.com/default.aspx?scid=kb;en-us;q247078

但是，基于 SSL 的 LDAP 可以按照以下 MSDN 技术说明中提供的信息更方便地进行配置：

http://support.microsoft.com/default.aspx?scid=kb;en-us;321051

此时，如果决定使用需要信任证书进行 SSL 通信，则必须在连接器的证书数据库中手动安装该证书，如第 296 页的 “在 Active Directory Connector 中启用 SSL”中所述。

安装和配置决策

本节提供了安装和配置概要，并详细说明了部署 Identity Synchronization for Windows 时需要做出的选择。在开始安装过程之前，请获取以下信息。本节包括：

核心安装

安装 “核心”时，必须提供以下信息：

- **配置目录主机和端口**：为要存储 Identity Synchronization for Windows 配置信息的 Directory Server 实例指定配置目录主机和端口。

  可将 SSL 端口指定为配置目录端口，此后，必须在安装过程期间将该端口标识为 SSL 端口。

  注意 Identity Synchronization for Windows 不支持将配置目录安装为 `localhost`。

- **根后缀**：指定配置目录的根后缀。在此后缀下存储所有配置信息。
- **管理员的名称和密码**：指定配置 Directory Server 的证书。
- **配置密码**：指定安全密码以保护敏感性配置信息。
- **文件系统目录**：指定要安装 Identity Synchronization for Windows 的位置。必须将 “核心”与 Directory Server 管理服务器安装于相同的目录。
- **未使用的端口号**：指定 Message Queue 实例的可用端口号。

核心配置

配置 “核心”时，必须提供以下信息：

- **Sun Java System Directory 模式服务器**：指定需要从配置目录加载的 Directory Server 数据。
- **用户对象类 （仅限 Directory Server）**：指定用于确定用户类型的 user 对象类。 Identity Synchronization for Windows 会基于此对象类派生属性 （包括密码属性）列表。此列表从模式中填充而来。
- **已同步的属性**：指定要在 Directory Server 和 Windows 环境之间同步的用户条目属性。
- **修改、创建和删除的流动**：指定需要如何在 Sun 和 Windows 系统之间传播修改、创建和删除操作。选项包括：
  - 从 Sun 至 Windows
  - 从 Windows 至 Sun
  - 双向

  指定是否将 Sun 和 Windows 系统之间传播的对象激活和禁用同步，并指定同步这些对象的方法。
- **全局目录**：指定全局目录 （Active Directory 拓扑的信息库和模式信息）。
- **Active Directory 模式控制器**：指定要从 Windows 全局目录检索的 Active Directory 模式源的 “全限定域名” (FQDN)。
- **配置目录**：指定存储 Identity Synchronization for Windows 配置的 Directory Server。
- **Active Directory 源**：指定用于同步 Active Directory 域的源。
- **Windows NT 主域控制器**：指定要执行同步的 Windows NT 域以及每个域的 “主域控制器”名称。
- **同步用户列表**：使用 LDAP DIT 和过滤器信息指定要在 Directory Server、Active Directory 和 NT 上同步的用户。
- **Sun Java System Directory Server**：指定用于存储要同步的用户的 Directory Server 实例。

连接器和 Directory Server 插件安装

在安装连接器和 Directory Server 插件时，必须提供以下信息：

- **配置目录主机和端口**：为要存储 Identity Synchronization for Windows 配置信息的 Directory Server 实例指定配置目录主机和端口。
- **根后缀**：指定配置目录的根后缀。使用 “核心”安装期间指定的根后缀。
- **管理员的名称和密码**：指定配置目录服务器的证书。
- **配置密码**：指定安全密码以保护敏感性配置信息。
- **文件系统目录**：指定要安装 Identity Synchronization for Windows 的位置。安装在同一机器上的所有组件的安装路径必须相同。
- **目录源**：指定要安装连接器或插件的目录源。

安装 Directory Server 和 Windows NT Connector 时，必须指定一个未使用的端口。

安装 Directory Server Connector 和插件时，必须为与该连接器和插件相对应的 Directory Server 指定主机、端口和证书。

使用命令行实用程序

Identity Synchronization for Windows 允许您使用以下实用程序从命令行执行各种任务：

- 使用含有以下子命令的 `idsync` 脚本执行 Identity Synchronization for Windows 命令行实用程序：
  - `certinfo`：基于您的配置和 SSL 设置显示证书信息
  - `changepw`：更改 Identity Synchronization for Windows 配置密码
  - `prepds`：准备供 Identity Synchronization for Windows 使用的 Sun Java System Directory Server 源
  - `printstat`：打印已安装的连接器、系统管理器和 Message Queue 的状态

    还可使用 `printstat` 命令显示其余要完成安装过程所必须执行的安装和配置步骤。
  - `resetconn`：将配置目录中的连接器状态重设为*尚未安装*（仅在硬件或卸载程序发生故障时）
  - `resync`：作为安装过程的一部分，重新同步和链接已有用户并预先填充目录
  - `startsync`：启动同步
  - `stopsync`：停止同步

注意 有关上述实用程序的详细信息，请参阅附录 A。

- 使用以下实用程序将 Identity Synchronization for Windows 1.0 或 1.0 SP1 移植到 Identity Synchronization for Windows 1 2004Q3：
  - `forcepwchg`：在从 Identity Synchronization for Windows 版本 1.0 移植至版本 1 2004Q3 的过程中，对于已更改了密码的用户，需要提供密码更改
  - `importcnf`：导入已导出的版本 1.0 配置 XML 文档

注意 有关上述实用程序的详细信息，请参阅第 7 章。

安装清单

以下清单旨在对安装过程提供帮助。请将它们打印出来，并在安装 Identity Synchronization for Windows 以前记录以下信息。

表 2-6 核心安装清单

必需的信息	条目
配置目录主机和端口	
配置目录的根后缀 （例如 dc=example,dc=com）	
要安装 Identity Synchronization for Windows 的文件系统目录	
配置目录服务器管理员的名称和密码	
用于保护敏感配置信息的安全配置密码	
Message Queue 实例的端口号	

表 2-7 核心配置清单

必需的信息	条目
Active Directory 全局目录 （如果合适）	
Directory Server 模式服务器	
Directory Server 用户结构和辅助对象类	
已同步的属性	
用户条目创建的流动	
用户条目修改的流动	
用户条目激活和禁用的流动	
用户条目删除的流动	
Sun Java System Directory Server 目录源	
Active Directory 目录源	
同步用户列表	
Windows 源过滤器创建表达式	
Sun Java System 源过滤器创建表达式	

表 2-8 连接器和 Directory Server 插件安装清单

必需的信息	条目
配置目录主机和端口	
配置目录的根后缀	
在其中安装连接器的文件系统目录	
配置 Directory Server 管理员的名称和密码	
用于保护敏感配置信息的安全配置密码	
目录源	
Directory Server 和 Windows NT 的未用端口	
对应于连接器和插件的 Directory Server 的主机、端口和证书	

表 2-9 链接用户清单

必需的信息	条目
要链接的同步用户列表	
用于匹配等价用户的属性	
XML 配置文件	

表 2-10 重新同步清单

必需的信息	条目
同步用户列表选定对象	
同步源。	
如果在目标目录源中未找到相应用户，是否自动创建一个用户条目？	
要使 Directory Server 密码失效吗？	
是否仅同步与指定 LDAP 过滤器匹配并位于选定 SUL 中的用户？	

第 3 章

安装核心

本章介绍如何使用 Identity Synchronization for Windows 安装程序和如何安装 Identity Synchronization for Windows 核心组件。

这些信息被编排在以下各节中：

开始之前

开始 Identity Synchronization for Windows 安装过程前：

- 请阅读第 2 章，“准备安装”。本章包含安装前提条件、清单及管理员权限要求等重要信息。
- Java Runtime Environment (JRE) 不随本产品一起提供。如有必要，可从以下位置下载 Java Development Kit：

  `http://java.sun.com` 或 `http://www.java.com`

  必须安装 JRE 1.4.2_04（或更高版本）才能在 Solaris 或 Windows 2000/2003 系统上运行 Identity Synchronization for Windows 安装程序。
- **仅在 Windows 系统中**：启动 “核心”安装程序前必须关闭所有打开的 “服务控制面板”窗口，否则安装会失败。
- 如果您的机器上还安装了 Identity Synchronization for Windows 1.0 版（或 1.0 SP1），请阅读第 7 章，“移植到 Identity Synchronization for Windows 1 2004Q3”。

注意 如果未注册用于其它应用程序（而不是 Identity Synchronization for Windows 1.0）注册使用， Identity Synchronization for Windows 1.0 卸载程序将删除 `SUNWjss` 软件包。特别是在 Solaris 机器上安装了压缩版的 Directory Server 5.2.2 时，更会出现这种情况，此时卸载程序会从 `/usr/share/lib/mps/secv1` 删除 `jss3.jar` 文件。

如果在移植到 Identity Synchronization for Windows 11 2004Q3 时遇到这种情况，安装程序会报告缺少必需文件，并将文件名记录到安装日志中。出现这种情况时，必须重新安装必需的补丁程序（请参阅第 54 页的 “Sun Java System 软件要求”）并重新启动安装程序。

- Identity Synchronization for Windows 版本 1.0 已安装 Message Queue，*而版本 1 2004Q3 则不然*。您应安装 Message Queue 3.5 SP1 Enterprise Edition。

  在 Solaris 系统中：请勿在同一目录下安装 Message Queue 和 Identity Synchronization for Windows。

启动安装程序

本节介绍如何在以下平台上下载、解压缩和运行 Identity Synchronization for Windows 安装程序：

- 第 82 页的 “在 Solaris SPARC 中”
- 第 83 页的 “在 Solaris x86 中”
- 第 84 页的 “在 Windows 中”

在 Solaris SPARC 中

请按以下步骤在 Solaris SPARC 操作系统上准备和运行 Identity Synchronization for Windows 安装程序：

1. 以超级用户身份登录。
2. 键入 **`# mkdir isw12004Q3`** 以创建新目录，然后更改 (**`cd`**) 到此目录。

3. 如果尚未进行此操作，请将产品二进制文件 (isw-12004Q3.sparc-sun-solaris.tar.gz) 下载到安装目录。
4. 使用以下命令解压缩产品二进制文件：

   # gunzip -dc isw-12004Q3.sparc-sun-solaris.tar.gz | tar -xvof -

5. 从 isw12004Q3 目录更改到 installer 目录，然后键入 **./runInstaller.sh** 以执行安装程序。

注意 要在基于文本的模式下运行安装程序，请键入

./runInstaller.sh -nodisplay

运行 runInstaller.sh 程序时， Identity Synchronization for Windows 将自动屏蔽密码，从而密码不会以明文显示。

在 Solaris x86 中

请按以下步骤在 Solaris x86 操作系统上准备和运行 Identity Synchronization for Windows 安装程序：

1. 以超级用户身份登录。
2. 键入 **# mkdir isw12004Q3** 以创建新目录，然后更改 (**cd**) 到此目录。
3. 如果尚未进行此操作，请将产品二进制文件 (isw-12004Q3.x86-sun-solaris.tar.gz) 下载到安装目录。
4. 使用以下命令解压缩产品二进制文件：

   # gunzip -dc isw-12004Q3.x86-sun-solaris.tar.gz | tar -xvof -

5. 从 isw12004Q3 目录更改到 installer 目录，然后键入 **./runInstaller.sh** 以执行安装程序。

注意 要在基于文本的模式下运行安装程序，请键入

./runInstaller.sh -nodisplay

运行 runInstaller.sh 程序时， Identity Synchronization for Windows 将自动屏蔽密码，从而密码不会以明文显示。

在 Windows 中

请按以下步骤在 Windows 操作系统上准备和运行 Identity Synchronization for Windows 安装程序：

1. 以管理员身份登录。
2. 键入 **# mkdir isw12004Q3** 以创建一个新目录
3. 更改 (**cd**) 到 `isw12004Q3` 目录。
4. 如果尚未进行此操作，请将产品二进制文件 (`isw-12004Q3-windows.zip`) 下载到安装目录。
5. 将 `isw-12004Q3-windows.zip` 文件解压缩到某个空目录。
6. 通过使用 **cd** 命令，从 `isw12004Q3` 目录更改到 `installer` 目录，然后键入 **setup.exe** 以执行安装程序。

   将显示 Identity Synchronization for Windows 安装向导。

注意 由于要在 Administration Server 根目录中安装 “核心”，Identity Synchronization for Windows 向导会检测安装所需的大多数信息 （如目录路径和目录名），并会自动填写向导面板中的某些字段。

如果有丢失或错误信息，可以手动输入所需信息。

有关 “核心”安装的说明，请继续阅读下一节。

安装核心

本节介绍在 Solaris 和 Windows 操作系统上安装 Identity Synchronization for Windows 核心的过程。

安装 “核心”前，应了解以下要求：

- **在 Solaris 系统中**：必须具有超级用户权限才能安装和运行 Solaris 服务。

  注意 必须以超级用户身份安装该程序，但安装后可将软件配置为以非超级用户身份运行 Solaris 服务。（请参阅附录 C，“在 Solaris 上以非超级用户身份运行服务”。）

- **在 Windows 2000/2003 系统中**：必须具有管理员权限才能安装 Identity Synchronization for Windows。
- 必须将 “核心”安装到某个目录，且该目录目前有一个由 Administration Server （版本 5 2004Q2 或更高）管理的服务器根，否则安装程序会失败。（您可以使用 Directory Server 5 2004Q2 安装程序安装 Administration Server。）

请按如下步骤使用安装向导安装 Identity Synchronization for Windows 核心组件：

1. 显示 “欢迎”屏幕时，请阅读屏幕信息，然后单击 “下一步”进入 “软件许可证协议”面板。
2. 阅读许可证协议，然后选择
   - **是 （接受许可证）**，接受许可证条款并转到下一面板。
   - **否**，停止安装过程并退出安装程序。
3. 将显示 “配置位置”面板 （图 3-1），可以在此指定配置目录位置。

图 3-1 指定配置目录位置

提供以下信息：

- **配置目录主机**：输入要存储 Identity Synchronization for Windows 配置信息的 Sun Java System Directory Server 实例 （附属于本地 Administration Server）的全限定域名 (FQDN)。

  您可以指定本地机器上的实例或在其它机器上运行的实例。

注意	为避免出现无效证书或主机名之类的警告，请确保为运行安装程序的机器指定一个可进行 DNS 解析的主机名。

- **配置目录端口**：指定安装配置目录的端口。（*默认端口为 389*。）

  要启用安全通信，请启用 “安全端口”选项并指定 SSL 端口。（*默认 SSL 端口为 636*。）

  当程序确认配置目录已启用 SSL 后，所有 Identity Synchronization for Windows 组件都将使用 SSL 与配置目录通信。

注意 Identity Synchronization for Windows 在将敏感配置信息发送到配置 Directory Server 前会先对其进行加密。

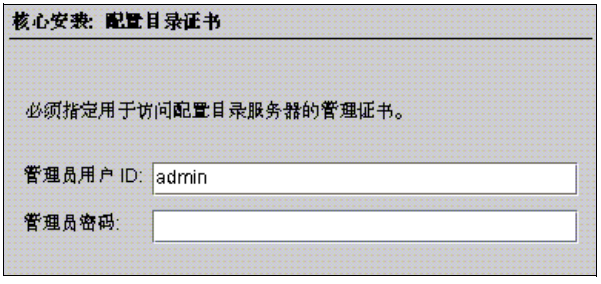
但是，如果要对 “控制台”和配置目录间的传输内容进行额外加密，则务必要同时为 Administration Server 和配置 Directory Server 启用 SSL。然后配置与 Administration Server 间的安全连接，您将向 Administration Server 验证 “Directory Server 控制台”。（有关信息，请参阅《*Sun Java System Administration Server 5 2004Q2 Administration Guide*》。）

- **配置根后缀**：从菜单中选择用于存储 Identity Synchronization for Windows 配置的根后缀。

注意 如果程序无法检测到根后缀，且必须手动输入信息 （或者更改默认值）时，必须单击 “刷新”来重新生成根后缀列表。（必须指定配置 Directory Server 上存在的根后缀。）

4. 单击 “下一步”打开 “配置目录证书”面板。

图 3-2 指定管理员证书

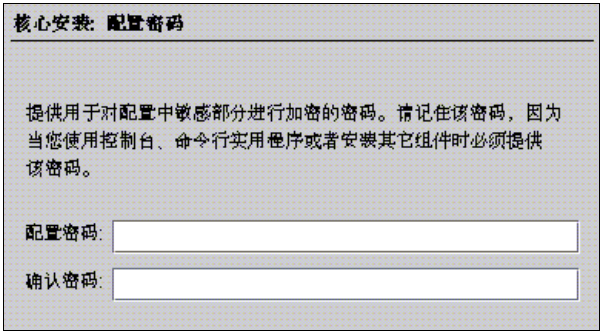


5. 输入配置目录管理员的用户 ID 和密码。
   - 如果指定 admin 作为用户 ID，则无需指定 “用户 ID”作为 DN。
   - 如果使用其它用户 ID，则必须指定 ID 作为完整 DN。
     例如， *cn=Directory Manager*。

注意 如果不使用 SSL 与配置目录通信 （请参阅步骤 3，第 86 页），则这些证书不经过加密便被发送。

6. 完成后单击 “下一步”，打开 “配置密码”面板。

图 3-3 指定配置密码



7. 必须输入并确认将用于加密诸如证书等敏感配置信息的密码。完成后，单击 “下一步”。

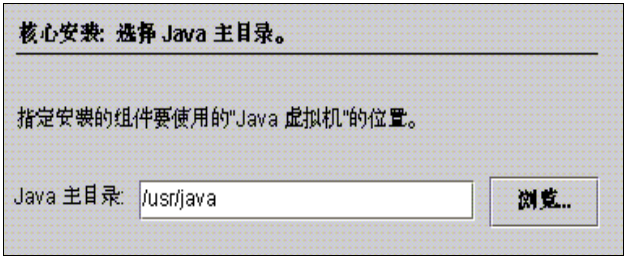
注意 请务必记住此密码，因为每次进行以下操作时都需要此密码

- 访问 Identity Synchronization for Windows 控制台
- 创建或编辑配置
- 安装组件
- 运行任意命令行实用程序

有关更改配置密码的信息，请参阅第 311 页的 “使用 changepw”。

将显示 “选择 Java 主目录” 面板 （参见图 3-4）。程序将自动插入已安装组件将使用的 “Java 虚拟机” 目录的位置。

图 3-4 指定 Java 主目录



8. 检查 Java 主目录 （必须为 JDK/JRE 1.4.2_04 或更高）：
   - 如果位置符合要求，请单击 “下一步” 进入 “选择安装目录” 面板 （第 89 页的图 3-5）。
   - 如果位置不正确，请单击 “浏览” 搜索并选择安装 Java 的目录，例如：
     - **在 Solaris 中**：`/var/java`
     - **在 Windows 中**：`C:\Program Files\j2sdk1.4.2_04`

图 3-5 指定安装目录

9. 在提供的文本字段中输入以下信息，或单击 “浏览” 以搜索并选择可用目录：
   - **服务器根目录**：指定 Directory Server 安装服务器根目录的路径和目录名。将在此位置安装 “控制台”。

注意 Windows 操作系统中只有一个服务器根目录，所有产品都将安装到该位置。

- **安装目录**（*仅当在 Solaris 中安装“核心”时才可用*）：指定安装目录的路径和目录名。核心二进制文件、库和可执行文件将安装到此目录。
- **实例目录**（*仅当在 Solaris 中安装“核心”时才可用*）：指定实例目录的路径和目录名。变动的配置信息（例如日志文件）将存储在此目录。

10. 单击“下一步”进入“Message Queue 配置”面板。

注意 安装 Identity Synchronization for Windows 前应先安装 Message Queue 3.5 SP1 Enterprise Edition。

在 Solaris 系统中：请勿在同一目录下安装 Message Queue 和 Identity Synchronization for Windows。

在 Windows 系统中：继续操作前必须关闭所有打开的“服务控制面板”窗口，否则“核心”安装会失败。

图 3-6 配置 Message Queue

11. 在提供的文本字段中输入以下信息，或单击“浏览”以搜索并选择可用目录：
    - **安装目录**：指定 Message Queue 安装目录的路径。
    - **配置目录**：指定 Message Queue 实例目录的路径和目录名。

- **全限定本地主机名**：指定本地主机的全限定域名 (FQDN)。（每个主机只能运行一个 Message Queue 代理程序实例。）
- **代理程序端口号**：指定 Message Queue 代理程序要使用的未用端口号。（*默认端口为 7676*。）

12. 单击 “下一步”，显示 “安装准备就绪”面板。

此面板将提供有关安装的信息，例如 “核心”的安装目录以及所需的空间。

- 如果显示的信息符合要求，请单击 “立即安装”以安装 “核心”组件 （安装程序将安装二进制文件、文件和软件包）。
- 如果信息不正确，单击 “上一步”进行更改。

将短时显示 “正在安装”消息，接着在安装程序将配置数据添加到指定的配置 Directory Server 时会显示 “组件配置”面板。此操作包括：

- 创建 Message Queue 代理程序实例
- 将模式上载到配置目录
- 将部署专用配置信息上载到配置目录

此操作需要耗时数分钟并会出现周期性的暂停，因此若此过程未超过十分钟，请不必担心。（观察进度条以监控安装程序的状态。）

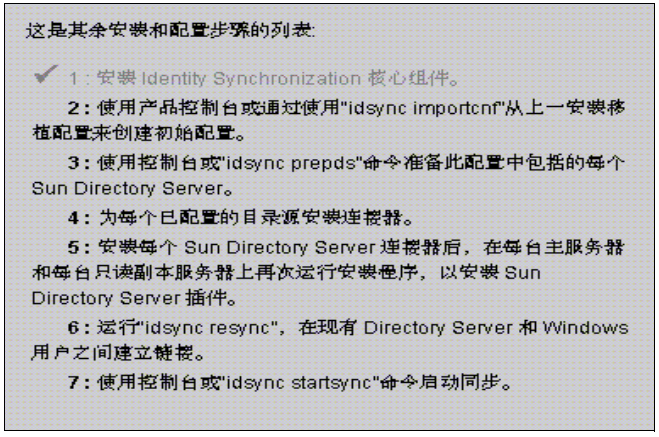
13. 完成组件配置操作后，会显示 “安装摘要”面板，以确认已成功安装 Identity Synchronization for Windows。

可单击 “详细信息”按钮查看已安装文件的列表及其安装位置。

14. 单击 “下一步”，程序会确定要成功安装和配置 Identity Synchronization for Windows 必须执行的其余步骤。

    将短时显示 “正在加载 ...” 消息和 “其余安装步骤” 面板，接下来将显示以下面板 （图 3-7）。此面板包含其余安装和配置步骤的 “待执行” 列表。（也可从 “控制台” 的 “状态” 选项卡访问此面板。）

图 3-7 Identity Synchronization for Windows 待执行列表



    在整个安装和配置过程中会重新显示 “待执行” 面板。程序会以灰色显示列表中所有完成的步骤。

    此时，“待执行” 列表中会包含一个一般步骤列表。保存配置后，程序会提供一个特定于您的部署 （例如，必须安装哪些连接器）定制的步骤列表。

15. 阅读步骤列表中的内容后，单击 “下一步”，此时将显示 “启动控制台选项” 面板，指示您已完成 “核心” 安装。

图 3-8 启动控制台

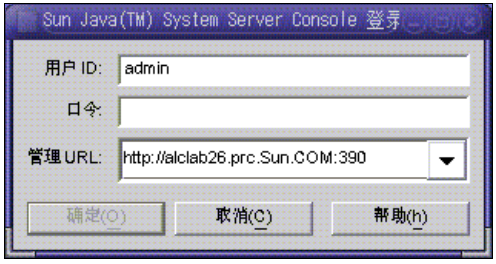
16. 接下来，必须配置 “核心”组件，这可通过 Sun Java System 控制台 （*默认情况下将启用*启动 Sun Java System 控制台*选项*）完成。

    如果从 Identity Synchronization for Windows 版本 1.0 或 SP1 移植到 Identity Synchronization for Windows 1 2004Q3，则可使用 `idsync importcnf` 命令行实用程序导入导出的版本 1.0 或 SP1 配置 XML 文档。有关说明，请参阅第 7 章，“移植到 Identity Synchronization for Windows 1 2004Q3”。

17. 单击 “已完成”。

18. 如果选择使用 “控制台”，会显示 “Sun Java System Server Console 登录”对话框 （参见图 3-9）。

图 3-9 登录到控制台



必须输入以下信息才能登录 “控制台”：

- **用户 ID**：输入在机器上安装 Administration Server 时所指定的管理员的用户 ID。
- **口令**：输入在 Administration Server 安装过程中指定的管理员密码。
- **管理 URL**：按以下格式输入 Administration Server 的当前 URL 位置：

  http://<*hostname.your_domain.domain:port_number*>

  其中：

  - *hostname.your_domain.domain* 是安装 Administration Server 时选择的计算机主机名。
  - *port_number* 是为 Administration Server 指定的端口。

19. 提供证书后，单击 “确定” 关闭该对话框。

20. 此时，系统会提供您输入配置密码。输入该密码，然后单击 “确定”。

当显示 “Sun Java System 服务器控制台” 窗口时，就可以开始配置 “核心” 了。有关说明，请继续阅读第 4 章，“配置核心资源”。

第 4 章

配置核心资源

必须在安装 Identity Synchronization for Windows 核心 （如第 3 章所述）后，立即对 “核心”资源进行初始配置。

本章说明如何使用 “控制台”添加和配置这些资源，内容编排在以下各节中：

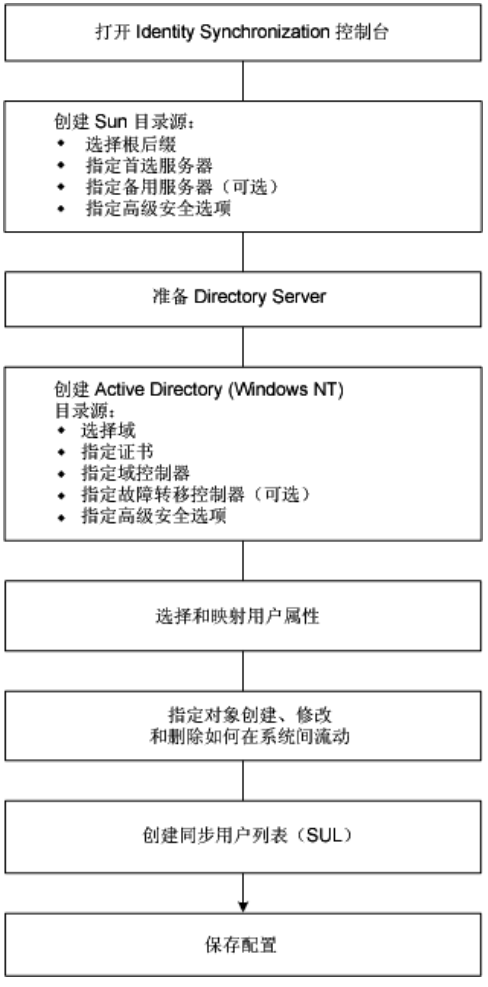
注意 要有效配置 “核心”资源，必须了解如何配置和操作 Directory Server 和 Active Directory。

不必按特定顺序配置这些资源 （除非文中另有说明）；但是，在熟悉本产品前按本章说明的顺序进行配置可以节省时间，避免错误。

配置概述

图 4-1 说明了针对您的部署而配置 “核心”资源将采取的步骤。

图 4-1 针对您的部署配置核心资源

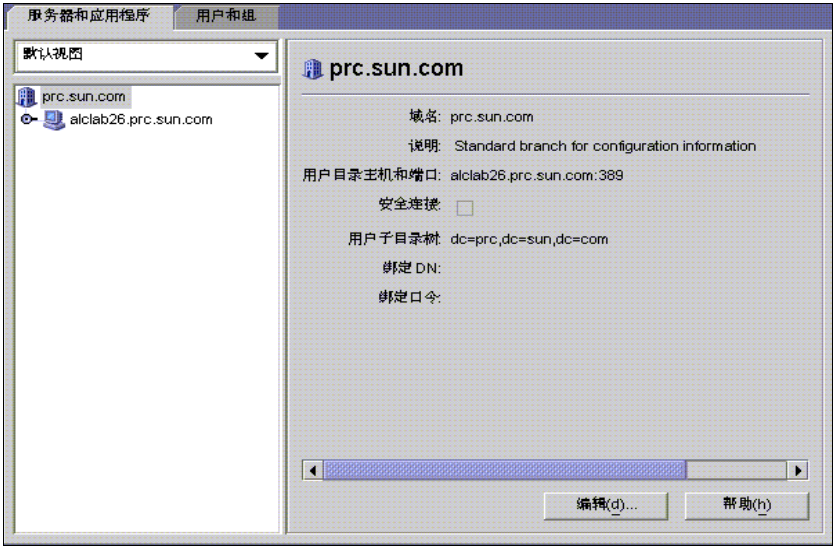


打开 Identity Synchronization for Windows 控制台

注意 如果尚未登录到 Sun Java System Server Console，请返回到第 93 页查看相关说明。

Sun Java System Server Console 窗口 （图 4-2）列出在您控制之下的所有服务器和资源，并提供有关您的系统的信息。

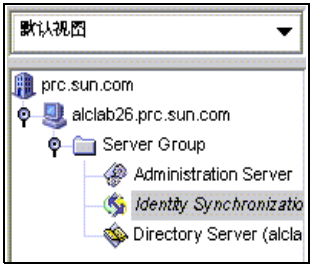
图 4-2 Sun Java System Server Console



要打开 Identity Synchronization for Windows 控制台：

1. 在 “服务器和应用程序” 选项卡中，在含有 Identity Synchronization for Windows 实例所属的 “服务器组” 的导航树中选择主机名节点。
2. 展开 “服务器组” 节点，并选择 Identity Synchronization for Windows 节点（参见图 4-3）。

图 4-3 展开服务器组



信息面板变为提供关于 Identity Synchronization for Windows 和系统信息的面板 （例如图 4-4 中所示）。

图 4-4 Identity Synchronization for Windows 信息面板

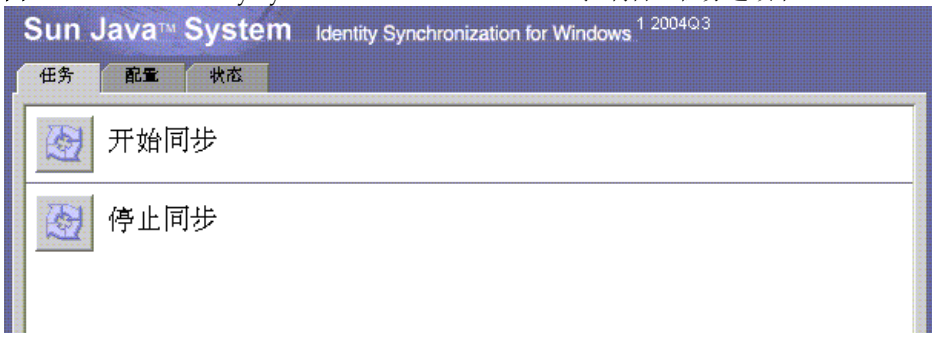
3. 单击 “打开” 按钮 （位于面板的右上角）。

注意 “编辑” 按钮 （位于面板的底部）可用来编辑 “服务器名” 和 “说明”。

4. 将提示您输入安装 “核心”时指定的配置密码 （请参阅第 88 页）。输入该密码，然后单击 “确定”。

   将显示 Identity Synchronization for Windows 控制台，如下所示：

图 4-5 Identity Synchronization for Windows 控制台：任务选项卡



此窗口含有三个选项卡和一个 “状态条”：

- **任务** （*默认*）：使用此选项卡可以停止和启动 Sun 和 Windows 系统间的同步。（有关启动和停止服务的信息，请参阅第 6 章，“同步现有用户”。）

  注意 不要将启动和停止 “同步服务”与启动和停止 Windows 服务混淆。

  要启动或停止 Windows 服务，必须通过 “Windows 控制台”进行操作，方法是选择 “开始” > “控制台” > “管理工具” > “计算机管理” > “服务”。

- **配置**：使用此选项卡可以配置系统，以便进行同步。
- **状态**：使用此选项卡可进行以下操作：
  - 监视系统组件 （如 “连接器”）的状态。
  - 查看在配置和同步过程中由 Identity Synchronization for Windows 生成的审计和错误日志。
  - 更新和检查安装和配置 “待执行”列表。
  - **状态条**：查看此位置可获知简要的系统状态信息。

  注意 有关 “状态”选项卡的详细信息，请参阅第 10 章。

5. 选择 “配置”选项卡 （参见图 4-6）。

图 4-6 Identity Synchronization for Windows 控制台：配置选项卡

“配置”面板包括以下选项卡：

- **属性**：使用此选项卡可以指定要在系统间同步的属性。
- **属性修改**：使用此选项卡可以指定密码、属性修改和对象禁用如何在系统间传播。
- **对象创建**：使用此选项卡可以指定新创建的密码和属性如何在系统间传播，并指定在同步过程中由 Identity Synchronization for Windows 创建的对象的初始值。
- **对象删除**：使用此选项卡可以指定删除的密码和属性如何在系统间传播。

必须至少配置一个 Sun Java System Directory Server 目录源和一个 Windows 服务器目录源（Active Directory 或 Windows NT）。有关说明，请继续阅读下面的小节。

创建目录源

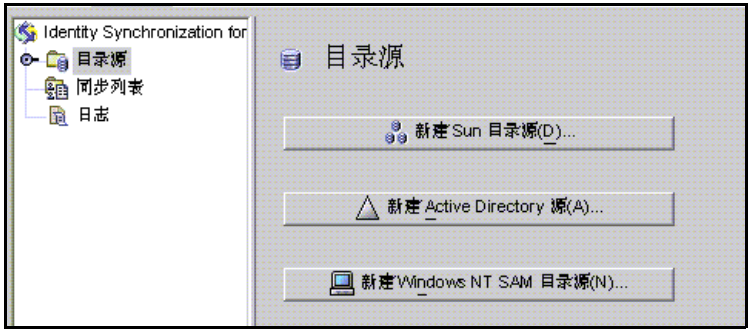
必须按以下顺序创建目录源 （基于要同步哪些源来创建）：

1. 第 102 页的 “创建 Sun Java System Directory 源”
2. 第 109 页的 “准备 Directory Server”
3. 第 113 页的 “创建 Active Directory 源”
4. 第 121 页的 “创建 Windows NT SAM 目录源”

注意 必须至少配置一个 Sun Java System Directory 源和一个 Windows 目录源 （Active Directory 和 / 或 NT SAM）。

选择导航树中的 “目录源”节点，将显示 “目录源”面板 （参见图 4-7）。

图 4-7 访问目录源面板



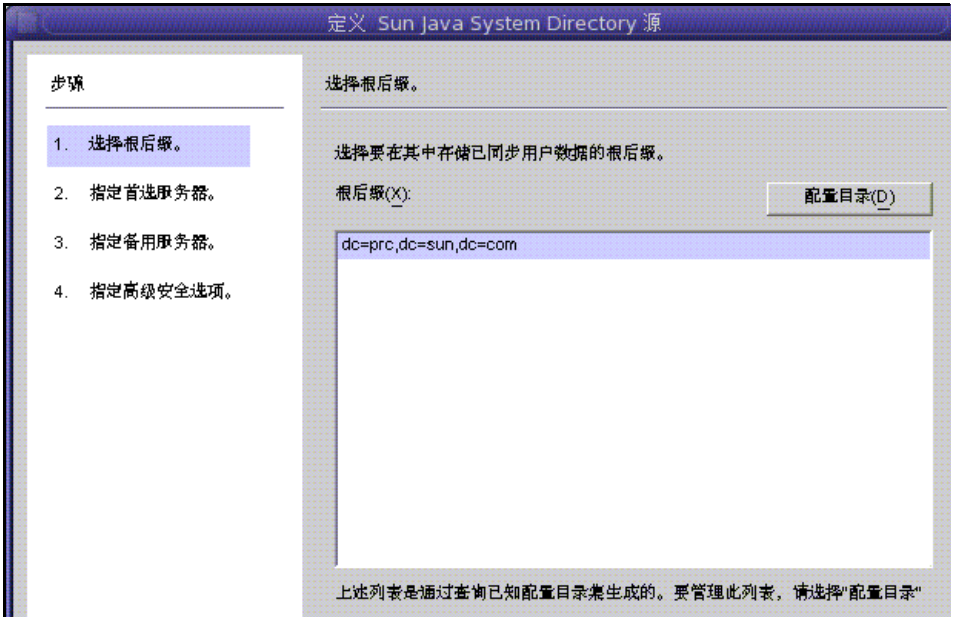
创建 Sun Java System Directory 源

注意 每个 Sun Java System 目录源都与一个 “连接器”和可以部署在最多四台主服务器的复制方案中的一组 “插件”关联。任何 Directory Server 插件都可以从 Windows 目录源执行密码有效性检查，而且用户可以在任何主服务器上更改密码；但是， Directory Server Connector 仅能对最多两台主服务器 （首选服务器或备用服务器）的 Windows 目录源的更改进行同步。 Directory Server 复制会将这两台服务器中的一台服务器的更改复制到部署中的其它服务器。

执行以下步骤可以创建新的 Sun Java System 目录源：

1. 单击 “新建 Sun 目录源”按钮，以调用 “定义 Sun Java System Directory 源”向导。

图 4-8 选择根后缀



该程序查询一组已知的配置目录源，并在列表面板中显示现有根后缀 （又称为*命名上下文*）。

默认情况下，该程序知道安装本产品的配置目录，而且配置目录知道的根后缀将在列表窗格中列出。

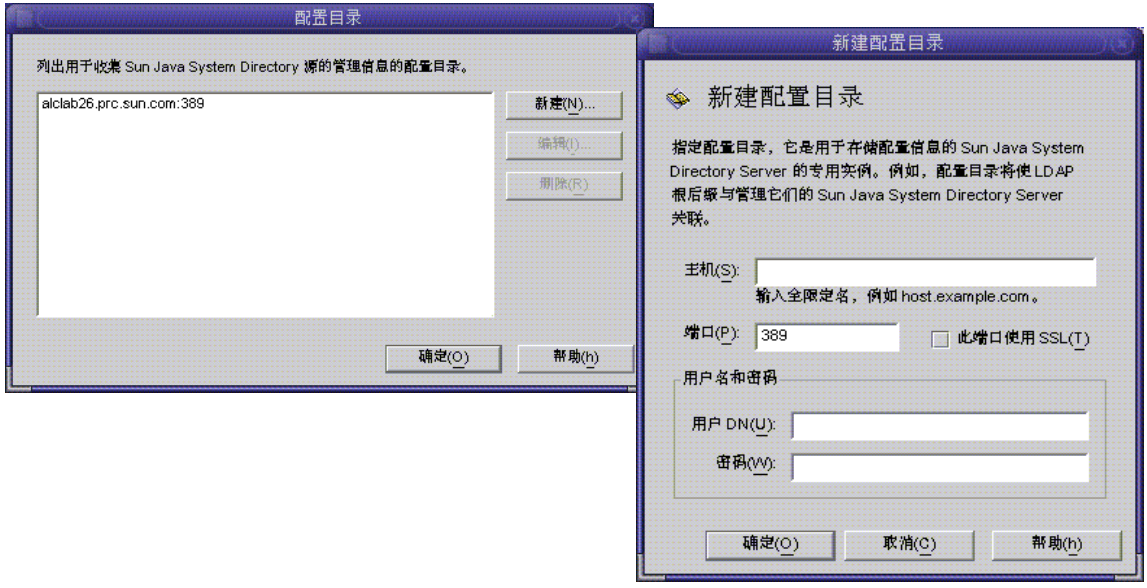
2. 从列表窗格中选择用户所在的根后缀。（如果列出了多个根后缀，请选择用户所在的那个根后缀。）单击 “下一步”，然后继续执行步骤 3。

   如果需要与之同步的根后缀不附属于使用 Identity Synchronization for Windows 注册的配置目录，则请指定一个新的配置目录，如下所述：

   a. 单击 “配置目录”按钮，以指定一个新的配置目录。

   b. 出现 “配置目录”对话框 （图 4-9）后，单击 “新建”按钮打开 “新建配置目录”对话框。

图 4-9 选择新配置目录



c. 输入以下信息，然后单击 “确定”保存更改，并关闭对话框。

- **主机**：输入全限定主机名。

  例如：**machine1.example.com**

- **端口**：输入一个有效的未用 LDAP 端口号。（*默认值为 389*。）

  如果 Identity Synchronization for Windows 使用 SSL （安全套接字层）端口与配置目录通信，则启用 “此端口使用 SSL”框。

- **用户 DN**：输入管理员的 （绑定）识别名。

  例如：

  uid=admin,ou=Administrators,ou=TopologyManagement,o=NetscapeRoot

- **密码**：输入管理员密码。

向导将查询指定的配置目录，以确定由该目录管理的所有目录服务器。

注意 Identity Synchronization for Windows 对每个 Sun Java System Directory Server 源仅支持一个根后缀。

注意

编辑和删除配置目录

还可以使用 “配置目录”对话框管理配置目录列表，如下所述：

- 从列表窗格中选择一个配置目录，然后单击 “编辑”按钮。出现“编辑配置目录”对话框后，可以更改“主机”、“端口”、“安全端口”、“用户名”和 “密码”参数。
- 从列表窗格中选择一个配置目录，然后单击 “删除”从列表中删除该目录。

d. 单击 “确定” 关闭 “配置目录” 对话框，列表窗格中出现新选定的配置目录的根后缀。

默认情况下， Directory Server 创建一个前缀与机器的 DNS 域条目组件对应的根后缀。它使用以下后缀：

dc=<*your_machine's_DNS_domain_name*>

即，如果您的机器域是 *example.com*，则应为您的服务器配置后缀 `dc=example, dc=com`。由选定后缀命名的条目必须已经存在于目录中。

e. 选择该根后缀，然后单击 “下一步”。

将显示 “指定首选服务器” 面板 （参见图 4-10）。

图 4-10 指定首选服务器

Identity Synchronization for Windows 使用首选 Directory Server 检测在任何 Directory Server 主服务器上进行的更改。首选服务器还作为主位置使用，在该位置处，对 Windows 系统上的更改将应用于 Sun Java System 目录系统。

如果首选服务器出现故障，则备用服务器可以存储这些更改，直到首选服务器恢复联机状态为止。

3. 使用以下方法之一选择首选服务器：

   - 启用 “选择已知服务器”按钮，然后从下拉列表中选择一个服务器名称。

     注意 只有正在运行的 Directory Server 才能显示在列表中。如果服务器临时关闭，请启用 “通过提供主机名和端口指定服务器”按钮，然后手动输入该服务器的信息。

     如果希望 Directory Server 使用 SSL 通信，请启用 “使用 SSL 进行安全通信”框。但是，如果启用此功能，则必须在安装完成后执行一些附加设置步骤。有关详细信息，请参阅第 293 页的 “在 Directory Server 中启用 SSL”。

   - 启用 “通过提供主机名和端口指定服务器”按钮，然后将该服务器的 “主机名”和 “端口”键入提供的文本字段。

     如果指定的端口使用 SSL，请启用 “此端口使用 SSL”框。

4. 单击 “下一步”，将显示 “指定备用服务器”面板。

图 4-11 指定备用服务器

- 要指定备用 Directory Server，请从下拉列表中选择一个名称或手动输入该信息（使用与指定首选服务器相同的步骤），然后单击“下一步”。

注意 Directory Server 必须正在运行，否则该服务器的名称*不会*在下拉列表中出现。如果该服务器临时关闭，请手动输入该服务器的信息。

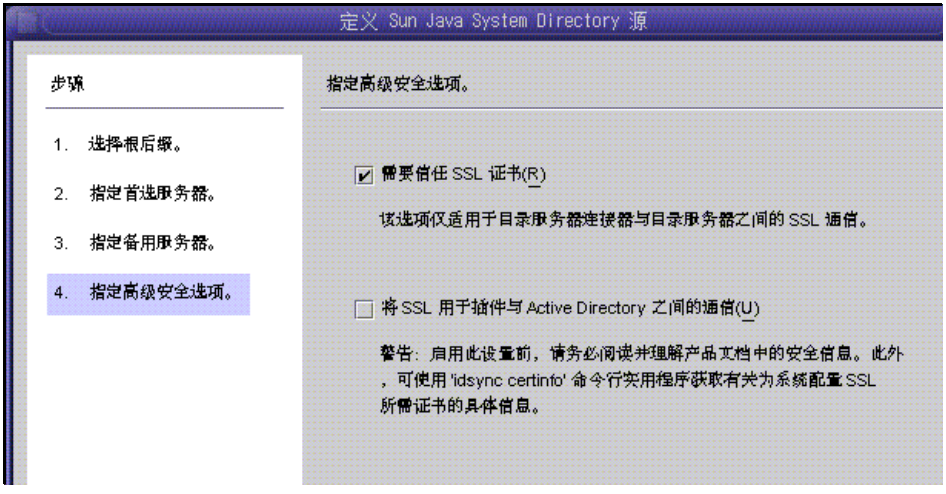
- 如果不想使用备用服务器，只需单击“下一步”即可。

注意

- 不要在 Sun 目录源中对首选服务器和备用服务器使用相同的主机名和端口。
- 如果启用“安全端口”功能，则必须在安装完成后执行一些附加设置步骤。有关详细信息，请参阅第 293 页的“在 Directory Server 中启用 SSL”。

将出现“指定高级安全选项”面板，如下所示：

图 4-12 指定高级安全选项



作为安装过程的一部分，必须将 Directory Server 插件安装到每个要进行用户绑定或密码更改的 Directory Server （任何主服务器、副本服务器或集线器）上。

当 Directory Server 插件将密码和属性同步到 Active Directory 时，它必须绑定到 Active Directory 才能搜索用户及其密码。另外，“插件”会将日志消息写入中心日志和 Directory Server 的日志中。默认情况下，上述通信不通过 SSL 完成。

5. 如果要使用安全 SSL 通信，*请阅读所提供的警告说明*，然后启用以下两个选项或其中之一：

   - 要仅加密频道通信，或加密频道通信并使用证书，以确保在 Directory Server 和 Directory Server Connector 间对参与者进行身份验证，请启用“需要 SSL 证书”框。

     如果不想信任证书，请清除该复选框。

   - 要在 Directory Server 插件和 Active Directory 之间使用安全 SSL 通信，请启用 “将 SSL 用于插件与 Active Directory 之间的通信”框。

注意

- 如果启用这些功能，则在安装后需要执行附加设置。有关详细信息，请参阅第 11 章，“配置安全性”。
- 可以使用 `idsync certinfo` 命令行实用程序确定必须为每个 Directory Server 插件和 / 或 “连接器”证书数据库添加哪些证书。请参阅第 310 页的 “使用 certinfo”。
- 如果主 Directory Server 和备用 Directory Server 是多主复制 (MMR) 部署的一部分，请参阅附录 E，“复制环境的安装注意事项”获得详细说明。

6. 完成 “指定高级安全选项”面板上的操作后，请单击 “完成”。

   该程序将选定的目录源添加至 “目录源”下的导航树中，并显示 “现在准备 Directory Server？”对话框。

   必须准备要由 Identity Synchronization for Windows 使用的 Directory Server。可以选择现在或以后执行此任务 — 但必须在安装 “连接器”前准备 Directory Server。（有关安装 “连接器”的说明，请参阅第 5 章。）

   - 如果需要现在准备 Directory Server，则单击 “是”打开向导，然后继续阅读下一节第 109 页的 “准备 Directory Server”。
   - 如果希望以后执行此过程，则单击 “否”，然后继续阅读第 113 页的 “创建 Active Directory 源”。

准备 Directory Server

本节说明如何准备由 Identity Synchronization for Windows 使用的 Sun Java System Directory Server 源。

准备 Directory Server

- 创建首选主机上可用的 Retro-Changelog 数据库和访问控制实例
- 创建首选主机上的可用 “连接器”用户和用户访问控制实例
- 在首选主机和备用主机上创建等同索引

注意

- 可以使用 `idsync prepds` 命令行实用程序代替 “控制台”，以准备 Directory Server。有关详细信息，请参阅第 313 页的 “使用 prepds”。
- 要使用 `idsync prepds` 命令行实用程序准备 Directory Server，必须知道要使用哪些主机和后缀，还必须拥有 “目录管理员”证书。

可使用 “准备 Directory Server” 向导 （图 4-13）准备 Directory Server。

图 4-13 输入 “目录管理员” 证书

要访问此向导，请使用以下方法之一：

- 出现 “现在准备 Directory Server？” 对话框后，单击 “是” 按钮。
- 出现 “Sun 目录源” 面板 （在 “配置” 选项卡上）后，单击 “准备 Directory Server” 按钮。

准备 Directory Server 源：

1. 输入 “目录管理员” 帐户的以下证书。
   - **目录管理员用户名**
   - **目录管理员密码**

   如果使用的是备用主机 （MMR 配置），则 “备用主机” 选项将处于活动状态，并且还必须为这些主机指定证书。

2. 完成后，单击 “下一步”，将显示 “指定准备配置”面板 （图 4-14）。

图 4-14 指定准备配置

阅读警告信息，然后确定现在还是以后创建 Directory Server 索引。

注意

- 此操作可能需要几秒或几分钟，具体情况由数据库大小决定。
- 当数据库处于只读模式时，任何更新数据库信息的尝试都将失败。
- 使数据库脱机可以加快索引的创建速度。

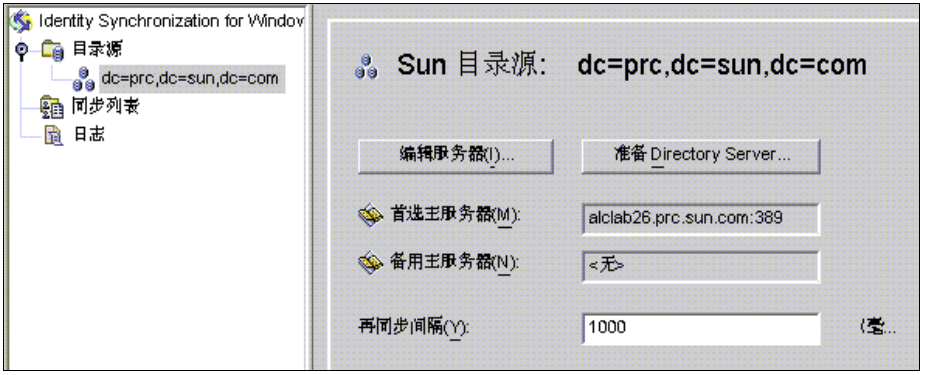
  - 要现在创建索引，请启用 “创建数据库的索引”框，然后单击 “下一步”。
  - 要以后创建索引 （不论手动还是通过再次运行此向导），请清除 “创建数据库索引”框，然后单击 “下一步”。

3. 将显示 “准备状态”面板，此面板提供关于 Directory Server 准备进度的信息。

  - 当在消息窗格底部显示 “成功”消息时，单击 “完成”。
  - 如果显示错误消息，则必须在继续执行前纠正报告的问题。查看错误日志（参见 “状态”选项卡）获得详细信息。

4. 返回到 “控制台”中的 “配置”选项卡。选择导航树中的 “Sun 目录源”节点以查看 “Sun 目录源”面板 （参见图 4-15）。

图 4-15 Sun 目录源面板



从此面板可以执行以下任务：

- **编辑服务器**：单击此按钮可以重新打开 “定义 Sun Java System Directory 源”面板，在该面板中可以更改任何服务器配置参数。如果需要，请查看为 “创建 Sun Java System Directory 源”提供的说明。
- **准备 Directory Server**：单击此按钮，然后按照第 109 页的 “准备 Directory Server”的说明准备 Directory Server。

  如果在初次准备 Directory Server 后，该服务器发生了某些变化 （例如，某个索引被删除或 Retro-Changelog 数据库丢失），则可以重新准备该服务器。

  注意 如果为首选 Sun 目录源重新创建 Retro-Changelog 数据库，则默认的访问控制设置将不允许 Directory Server Connector 读取数据库内容。

  要为新 Retro-Changelog 数据库恢复访问控制设置，请运行 `idsync prepds` 或在 “控制台”中选择相应的 Sun 目录源，然后单击 “准备 Directory Server”按钮。

- **再同步间隔**：指定希望 Directory Server Connector 检查更改的频率。（*默认值为 1000 毫秒。*）

5. 为要同步的 Sun Java System Directory Server 企业中的每个用户群体添加 Directory Server 目录源。

完成后，必须至少创建一个 Windows 目录源：

- 要创建 Active Directory 目录源，请继续阅读下一节第 113 页的 “创建 Active Directory 源”。
- 要创建 Windows NT 目录源，请继续阅读第 121 页的 “创建 Windows NT SAM 目录源”。

创建 Active Directory 源

应该为网络中每个要同步的 Windows 域添加 Active Directory 目录源。

每个 Active Directory 部署至少拥有一个全局目录，它了解跨越所有 Active Directory 域的所有全局信息。

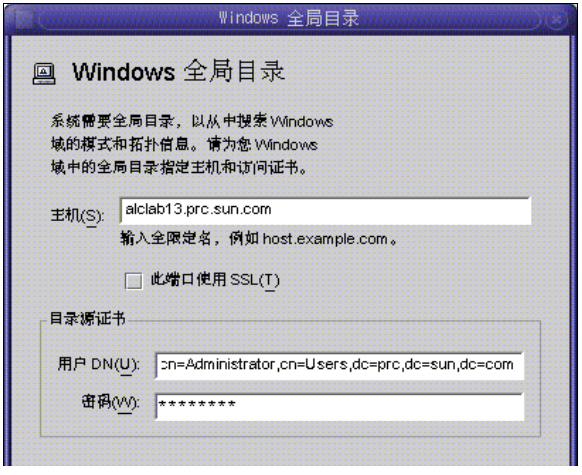
注意 每个 Active Directory 服务器都可以是一个全局目录，而且一个部署可以拥有多个全局目录，但只需指定一个全局目录。

如果网络中存在 Windows Active Directory 服务器，请执行以下步骤：

1. 选择导航树中的 “目录源”节点，然后单击 “目录源”面板上的 “新建 Active Directory 源”按钮。

   将显示 “Windows 全局目录”对话框 （图 4-16）。

图 4-16 Windows 全局目录



2. 输入以下信息，然后单击 “确定”：

   - **主机**：输入含有 Active Directory 森林结构全局目录的机器的全限定主机名。

     例如：**machine2.example.com**

   - **此端口使用 SSL**：如果 Identity Synchronization for Windows 使用 SSL 端口与全局目录通信，请启用此选项。

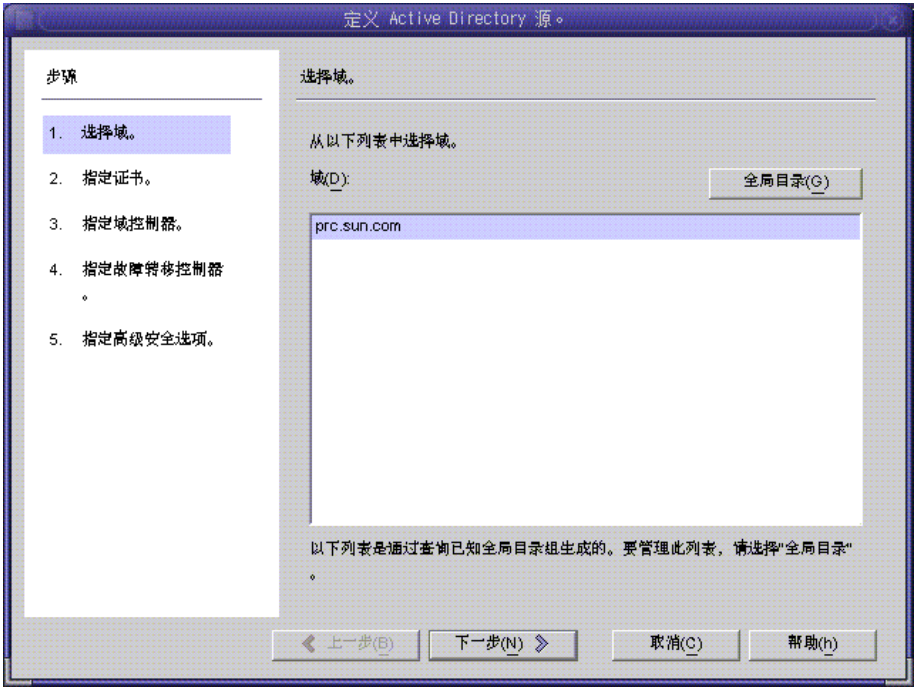
   - **用户 DN**：输入管理员的 （绑定）全限定识别名。（可以是任何能使您浏览模式和确定系统中的可用 Active Directory 域的证书。）

     例如：**cn=Administrator,cn=Users,dc=example,dc=com**

   - **密码**：输入指定用户的密码。

3. 将显示 “定义 Active Directory 源”向导，如下所示：

图 4-17 定义 Active Directory 源向导



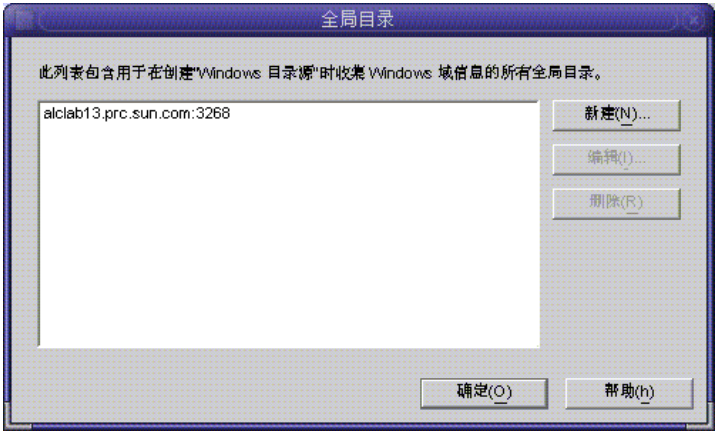
此向导查询 Active Directory 全局目录以确定其它存在的域，并在 “域”列表窗格中显示这些域。

4. 从列表窗格中选择一个名称，以指定一个 Active Directory 域，单击 “确定”，然后继续执行第 116 页的步骤 5。

   如果要使用的域未显示在列表中，必须按下面的步骤添加知道该域的全局目录：

   a. 单击 “全局目录”按钮，将显示 “全局目录”向导 （图 4-18）。

图 4-18 指定新的全局目录



   b. 单击 “新建”按钮。

   c. 出现 “Windows 全局目录”对话框后，提供全局目录的主机名和 “目录源”证书 （如第 114 页所述），然后单击 “确定”。

   d. 新的全局目录和端口将显示在 “全局目录”列表窗格中。选择目录名，然后单击 “确定”。

   e. 如果要将更多全局目录 （域）添加到系统中，请重复上述步骤。

   f. 完成后，单击 “选择域”窗格中的 “下一步”按钮。

5. 出现 “指定证书”面板后，查看 “用户 DN”字段中的值。

图 4-19 指定此 Active Directory 源的证书

如果程序未将管理员的识别名自动输入到 “用户 DN”字段 （或者您不想使用管理员证书），请手动输入 “用户 DN”和密码。

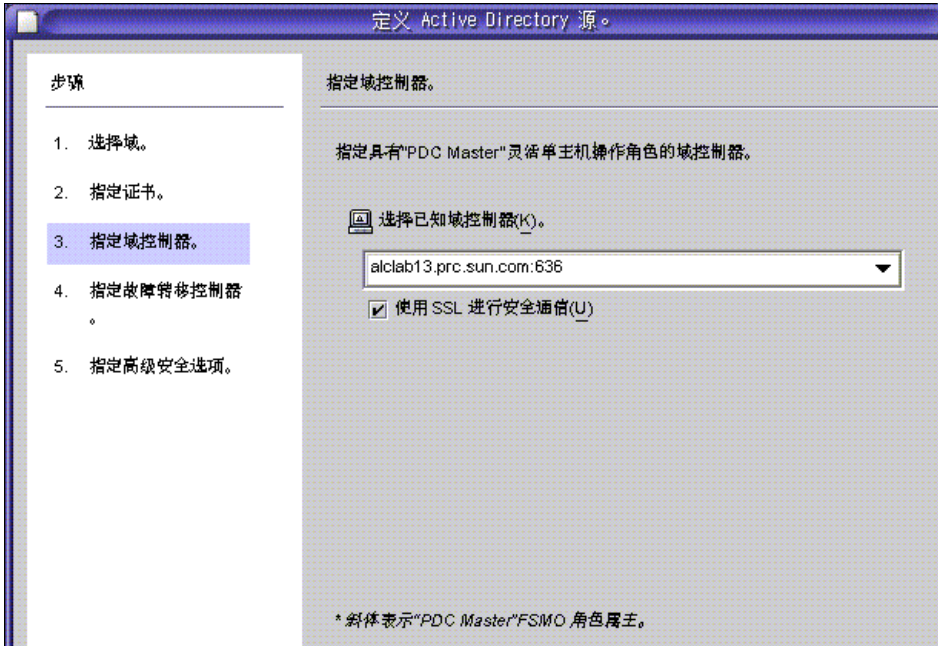
当配置 Active Directory 源时，必须提供 Active Directory Connector 能用来连接 Active Directory 的用户名和密码。

注意 “连接器”需要特定的访问权限。最小权限取决于同步的方向，如下所述：

- 如果配置的同步仅从 Active Directory 流向 Directory Server，则为 Active Directory Connector 提供的用户不需要许多特权。拥有在要被同步的域中 “查看所有属性”额外特权的一般用户就可以。
- 如果配置的同步是从 Directory Server 流动到 Active Directory，则 “连接器”用户必须拥有更多特权，因为同步会更改 Active Directory 中的用户条目。在此设置中，“连接器”用户必须拥有 “完全控制”特权或者是 “管理员”组的成员。

6. 单击 “下一步”打开 “指定域控制器”面板。

图 4-20 指定域控制器



使用此面板可以选择要在指定域内同步的控制器。（就概念而言，域控制器与 Directory Server 的首选服务器类似。）

如果选定的 Active Directory 域拥有多个域控制器，则选择拥有 “主域控制器” FSMO 角色的域控制器进行同步。

默认情况下，在所有域控制器进行的密码更改会被立即复制到 “主域控制器” FSMO 角色属主。如果选择此域控制器， Identity Synchronization for Windows 会立即将这些密码更改同步至 Directory Server。

在某些部署中， `AvoidPdcOnWan` 属性可以在 Windows 注册表中设置，因为到 PDC 有相当一段网络 “距离”，因此会将同步明显延迟。（有关详细信息，请参阅 *Microsoft Knowledge Base Article 232690*。）

7. 从下拉列表中选择域控制器。

8. 如果希望 Identity Synchronization for Windows Connector 通过安全端口与域控制器通信，请启用 “使用安全端口” 框。

注意 如果使用的是 Microsoft 证书服务器，则程序会自动在 Active Directory Connector 中安装 CA 证书。如果使用的不是 Microsoft 证书服务器，则必须手动在 Active Directory Connector 中添加 CA 证书 （请参阅第 296 页的 “在 Active Directory Connector 中启用 SSL”）。另外，如果在初次配置后对流设置进行了更改，上述步骤也适用。

9. 完成后，单击 “下一步”。

将显示 “指定故障转移控制器” 面板 （参见图 4-21）。可以使用此面板指定任意数量的故障转移域控制器。

图 4-21 指定故障转移控制器

Active Directory Connector 仅与一个 Active Directory 域控制器通信，Identity Synchronization for Windows 不支持由该 “连接器” 应用的故障转移更改。但是，在对 Directory Server 进行密码更改验证后， Directory Server 插件将与任意数量的域控制器通信。

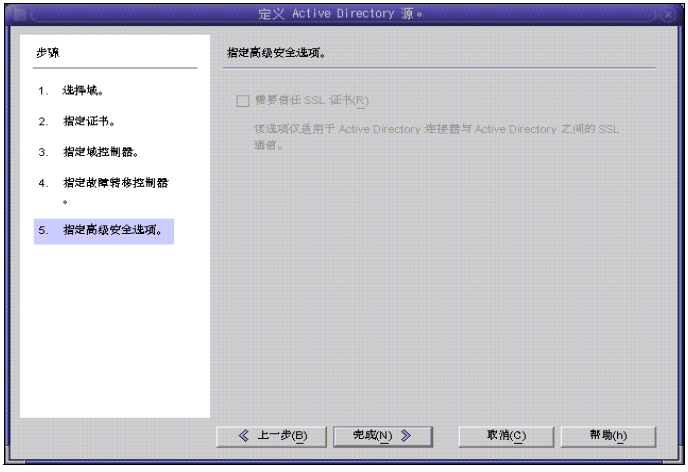
如果 Directory Server 尝试连接到一个 Active Directory 域控制器，而该域控制器不可用，则 Directory Server 将反复尝试连接到指定的故障转移域控制器。

10. 选择 “故障转移服务器”列表窗格中列出的一个或多个服务器名称 （或单击 “全选”按钮指定列表中的所有服务器），然后单击 “下一步”。

11. 将出现 “指定高级安全选项”面板 （图 4-22）。

    仅当启用 “指定域控制器”面板 （参见图 4-20）上的 “使用 SSL 进行安全通信”框时，“需要信任 SSL 证书”选项才处于活动状态。

图 4-22 指定高级安全选项



- 如果禁用 “需要信任 SSL 证书”框 （*默认设置*）， Active Directory Connector 将通过 SSL 连接到 Active Directory，而不验证是否信任通过 Active Directory 的证书。

  禁用此选项可简化设置过程，因为不必将 “Active Directory 证书”放入 Active Directory 证书数据库中。

- 如果启用 “需要信任 SSL 证书”框，则 Active Directory Connector 将通过 SSL 连接到 Active Directory，而且必须验证是否信任通过 Active Directory 的证书。

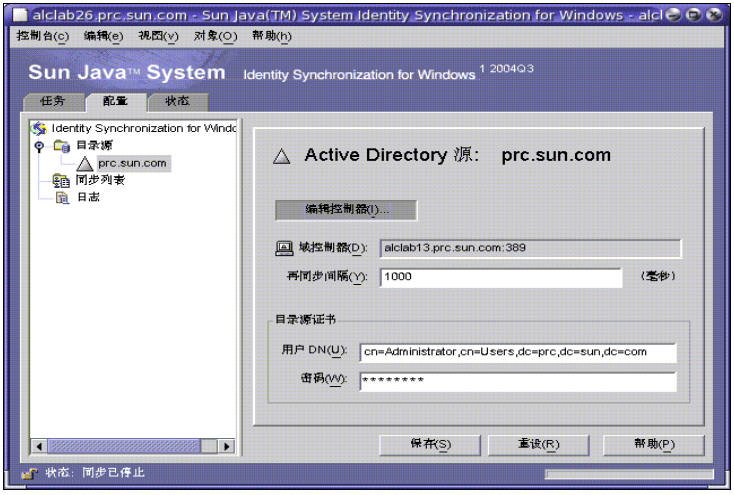
注意 必须将 “Active Directory 证书”添加到 Active Directory Connector 的证书数据库中。有关说明，请参阅第 299 页的 “将 Active Directory 证书添加到连接器的证书数据库中”。

12. 完成 “高级安全选项”面板上的操作后，请单击 “完成”按钮。

    程序将新指定的 Active Directory 目录源添加至 “目录源”下的导航树。

13. 选择 Active Directory 目录源节点以查看 “Active Directory 源”面板 （参见图 4-23）。

图 4-23 Active Directory 源面板



从此面板可以执行以下任务：

- **编辑控制器**：单击此按钮可以重新打开 “指定域控制器”面板，在该面板中可以更改任何域控制器配置参数。如果需要，请查看为 “创建 Active Directory 源”提供的说明。
- **再同步间隔**：指定希望 Active Server Connector 检查更改的频率。（*默认值为 1000 毫秒*。）
- **目录源证书**：更改指定的 “用户 DN”和 / 或密码。

创建完 Active Directory 目录源后：

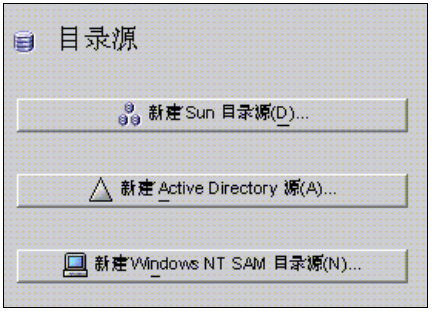
- 要创建 Windows NT 目录源，请继续阅读下一节 “创建 Windows NT SAM 目录源”。
- 要创建和映射要同步的属性，请继续阅读第 124 页的 “选择和映射用户属性”。

创建 Windows NT SAM 目录源

要在 Windows NT 平台上部署 Identity Synchronization for Windows，请指定 NT SAM 目录源，如下所述：

1. 选择导航树中的 “目录源”节点，然后单击 “新建 Windows NT SAM 目录源”按钮。

图 4-24 目录源面板

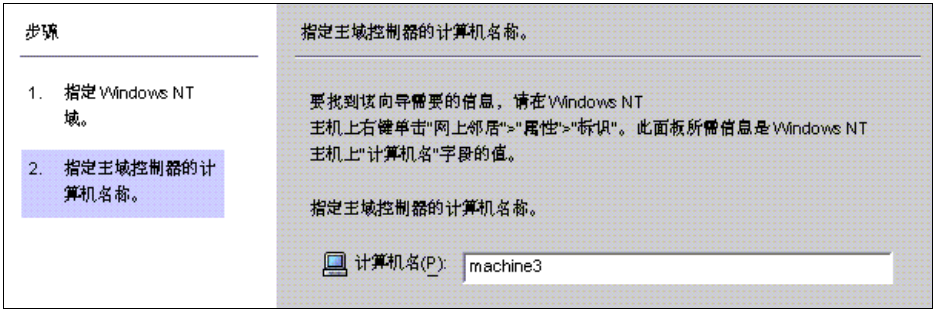


2. 显示 “定义 Windows NT SAM 目录源”面板后 （参见图 4-25），按照查找 Windows NT 域名的步骤进行操作，然后在 “域”字段中输入唯一的 NT 目录源域名。完成后，单击 “下一步”。

图 4-25 指定 Windows NT SAM 域名

3. 显示 “指定主域控制器的计算机名称” 面板后 （参见图 4-26），按照查找 “主域控制器” 计算机名称的步骤进行操作，然后在 “计算机名” 字段中输入信息。

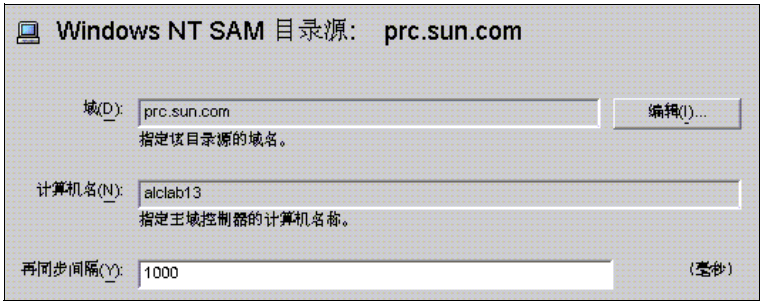
图 4-26 指定主域控制器的名称



4. 单击 “完成”。

程序将新指定的 Windows NT SAM 目录源添加至 “目录源” 下的导航树。选择该新的目录源节点可以查看 “Windows NT SAM 源” 面板（参见图 4-27）。

图 4-27 Windows NT SAM 目录源面板



从此面板可以执行以下任务：

- **编辑**：单击此按钮可以重新打开 “指定域控制器” 面板，在该面板中可以更改任何域控制器配置参数。如果需要，请查看为 “创建 Active Directory 源” 提供的说明。
- **再同步间隔**：指定希望 Identity Synchronization for Windows 检查 Windows NT 上的更改的频率。（*默认值为 1000 毫秒*。）

5. 为网络中的每台 Windows NT 机器添加一个 Windows NT 目录源。

创建完 Windows NT SAM 目录源后，就可以创建和映射要同步的属性了。有关说明请继续阅读第 124 页的 “选择和映射用户属性”。

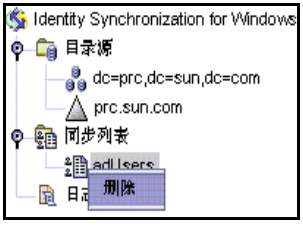
删除目录源

注意 如果已经安装了与目录源关联的连接器，则必须在删除该目录源*之前*卸载连接器。

如果必须删除目录源，请执行以下步骤：

1. 在删除目录源以前，必须首先删除所有与该源关联的 “同步用户列表” (SUL)。
   a. 右键单击导航树中 “同步列表”下列出的相关 “同步用户列表”节点。
   b. 出现弹出菜单后，选择 “删除”将该 SUL 删除。

图 4-28 删除同步用户列表



2. 右键单击导航树中 “目录源”下列出的该目录源节点。
3. 出现弹出菜单后，选择 “删除”将该目录源删除。

选择和映射用户属性

完成 Directory Server 和 Windows 目录源的创建和配置后，必须确定要同步哪些用户属性，然后在系统间映射这些属性。

本节的内容编排如下：

选择和映射属性

属性分为两种类型：

- **重要**：创建或修改用户条目时，在系统间同步的属性。
- **创建**：仅当创建用户条目时在系统间同步的属性。

  根据每个平台使用的模式，某些创建属性是*强制*同步的属性。这些属性是进行密码同步所必需的，而且必须映射到 Sun 属性才能在 Active Directory 服务器上成功创建 `user` 对象类条目。

本节说明如何选择用于同步的用户属性，以及如何 （一对一）映射这些属性，以便在为 Directory Server 指定一个属性后，相应属性会在 Active Directory 和 / 或 Windows NT 环境中显示 （反之亦然），而且关联的 Windows 属性会同步更新它们的值。

选择和映射用于同步的属性：

1. 选择导航树顶部的 Identity Synchronization for Windows 节点 （参见图 4-29）。

图 4-29 属性选项卡

2. 选择“属性”选项卡，然后单击“新建”按钮。

   将显示“定义重要属性映射”对话框（图 4-30）。使用此对话框可将属性从 Directory Server 映射到 Windows 系统（Active Directory 和 / 或 Windows NT）。

图 4-30 定义重要属性映射

注意 哪些创建属性是 Directory Server （或 Active Directory）的强制属性取决于为 Sun 端 （或 Active Directory 端）用户条目配置的对象类。

3. 从 Sun Java System 属性下拉列表中选择一个属性 （例如 *cn*），然后从 Active Directory 属性和 / 或 Windows NT SAM 属性下拉菜单中选择等同属性。
4. 完成后，单击 “确定”。
5. 要指定附加属性，请重复步骤 2 至步骤 4。

完成后的 “已同步属性”表看起来可能类似下面的示例，其中显示出 Directory Server 属性 `userpassword`、`cn` 和 `telephonenumber` 分别被映射至 Active Directory 属性 `unicodepwd`、 `cn` 和 `telephonenumber`。

图 4-31 完成的已同步属性表

Directory Server	Active Directory	Windows NT SAM
userpassword	unicodepwd	<无>
cn	cn	<无>
telephonenumber	telephonenumber	<无>

注意 指定全局目录后，程序会自动将 *inetOrgPerson* 用作 Sun Java System Directory Server 的默认对象类并加载 Active Directory 模式。所以，除非要更改默认模式，否则不要使用 “加载模式”按钮。

如果要更改默认模式源，请参阅第 127 页的 “更改模式源”以获取有关说明。

创建参数化默认属性值

Identity Synchronization for Windows 允许使用其它创建或重要属性为属性创建*参数化*默认值。

要创建参数化默认属性值，请在表达式字符串中插入现有创建或重要属性名 （前后加上百分号 (%<*attribute_name*>%)）。例如， `homedir=/home/%uid%` 或 `cn=%givenName% %sn%`。

创建这些属性值时：

- 可在创建表达式中使用多个属性 (`cn=%givenName% %sn%`)。
- 如果 `A=%B%`，则 `B` 只能有一个默认值。
- 引用时可使用反斜杠符号 (\) （例如， `diskUsage=0\%`）。
- 请勿使用有循环代换条件的表达式 （例如，如果指定 `description=%uid%`，则不能使用 `uid=%description%` 。）

更改模式源

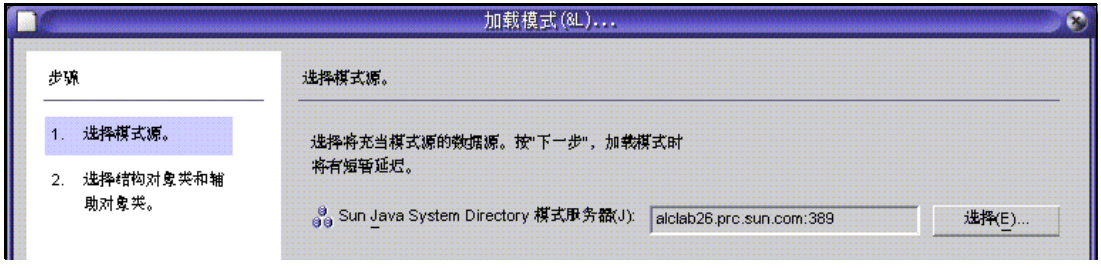
程序将自动提供默认模式源，但允许您更改默认模式。

按照以下步骤更改默认模式源：

1. 单击 “定义重要属性映射”对话框上的 “加载模式”按钮。

   将显示 “选择模式源”面板 （图 4-32）。

图 4-32 选择模式源



使用此面板指定希望从哪个 Sun Java System Directory Server 模式服务器读取模式。此模式含有系统上可用的对象类，对象类定义哪些属性对系统上的用户可用。

默认情况下，程序将配置目录添加至 “Sun Java System Directory 模式服务器”字段。

2. 要选择不同的服务器，请单击 “选择”按钮。

   将显示 “选择 Sun 模式主机”对话框。此对话框包含一个配置目录列表，其中汇集了有关目录源的管理信息。

   从此对话框，可以：

   - 创建新配置目录并将其添加到列表中。

     单击 “新建”，出现 “新建配置目录”对话框后，指定 “主机”、“端口”、“用户 DN”和 “密码”。完成后，单击 “确定”。

   - 编辑现有目录。

     单击 “编辑”，出现 “编辑配置目录”对话框后，可以更改 “主机”、“端口”、“用户 DN”和 / 或 “密码”。完成后，单击 “确定”。

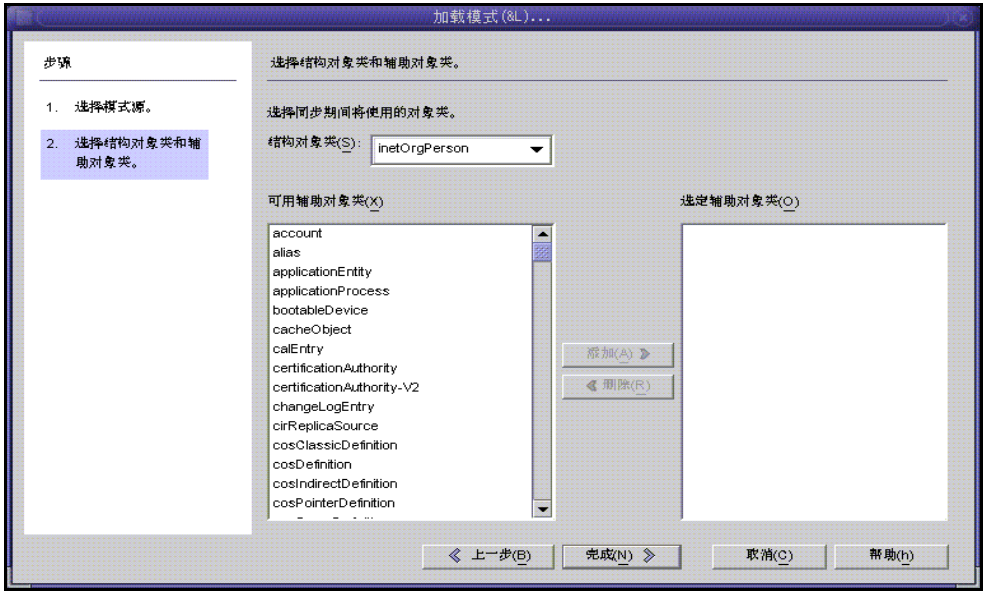
   - 从列表中删除目录。

     从列表中选择一个目录名，然后单击 “删除”按钮。

3. 从列表中选择一个服务器，并在完成后单击 “确定”。（一般来说，最好选择 Sun 同步主机中的一台主机作为模式源。）

4. 单击 “下一步”按钮，将显示 “选择结构对象类和辅助对象类”面板（图 4-33）。

图 4-33 选择结构对象类和辅助对象类



使用此面板指定要同步的对象类，如下所述：

- **结构对象类**：从选定的 Directory Server 创建或同步的每个条目都必须至少含有一个结构对象类。
- **辅助对象类**：这些对象类扩充了选定的结构类，并提供了用于同步的附加属性。

要指定结构和辅助对象类：

a. 从下拉列表中选择一个结构对象类。（*默认值为 inetorgperson*。）

b. 从 “可用辅助对象类”列表窗格中选择一个或多个对象类，然后单击 “添加”将选择的对象类移至 “选定辅助对象类”列表窗格中。

选定的对象类决定可选择哪些 Directory Server 源属性作为重要属性或创建属性。这些对象类还决定强制创建属性。

要从 “选定辅助对象类”列表中删除选择的对象类，请单击对象类名称，然后单击 “删除”按钮。

c. 完成后，单击 “完成”，程序将载入模式和选定的对象类。

在系统间传播用户属性

在创建和映射要同步的用户属性后，必须告诉 Identity Synchronization for Windows 如何在 Sun 和 Windows 系统间传播 （流动）属性创建、修改和删除。

默认情况下， Identity Synchronization for Windows

- 仅执行从 Windows 到 Sun Java System Directory Server 的同步
- 仅同步密码属性 （除非在上一节中指定了重要属性）
- 不同步条目创建或删除。

本节说明如何配置系统间的属性同步。内容具体安排如下：

- 第 131 页的 “指定对象创建如何流动”
- 第 136 页的 “指定对象修改如何流动”
- 第 146 页的 “指定删除如何流动”

指定对象创建如何流动

执行以下步骤可以指定对象创建如何在 Directory Server 和 Active Directory 系统间流动：

1. 单击“对象创建”选项卡。

图 4-34 选择和传播创建

2. 可以启用或禁用创建的流动，如下所述：
   - 启用 **“对象创建从 Sun Java System Directory Server 流向 Windows”** 可以将创建从 Directory Server 环境传播至 Windows 服务器。
   - 启用 **“对象创建从 Windows 流向 Sun Java System Directory Server”** 可以将创建从 Windows 环境传播至 Directory Server。
   - 同时启用上述两个选项可以实现双向流动。
   - 同时禁用上述两个选项可以阻止用户创建从一个系统传播到另一个系统。（*默认*）

3. 要添加、编辑或删除要在系统间同步的创建属性，请单击选定选项下的 “创建属性”按钮。

   将显示 “创建属性映射和值”对话框 （参见图 4-35 和图 4-36）。

图 4-35 创建属性映射和值：Directory Server 到 Windows

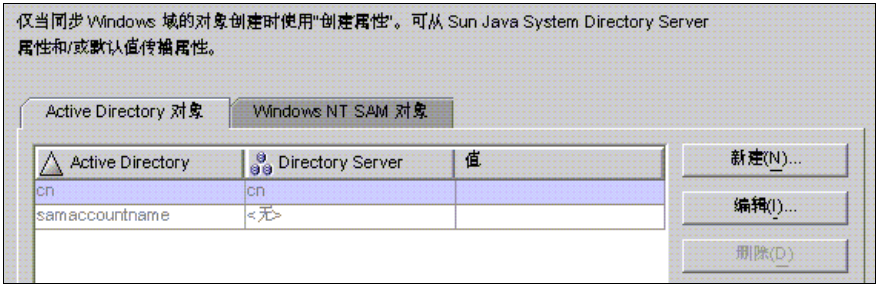
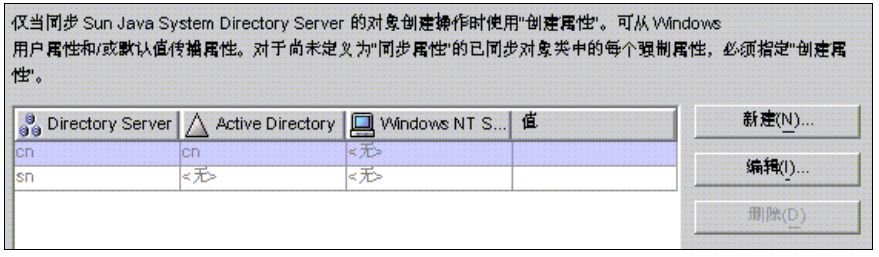


图 4-36 创建属性映射和值：Windows 到 Directory Server



可使用任一对话框进行以下操作：

- 指定新的创建属性 （第 133 页）

  注意 为满足有关用户对象类所需属性的模式约束，有必要指定用户创建期间要在系统中流动的其它属性。

  如果将所需属性指定为 *修改*属性则无需指定其它属性 （如第 124 页的 “选择和映射用户属性”中所述）。

- 编辑现有属性 （请参阅第 133 页）
- 删除现有属性 （请参阅第 133 页）

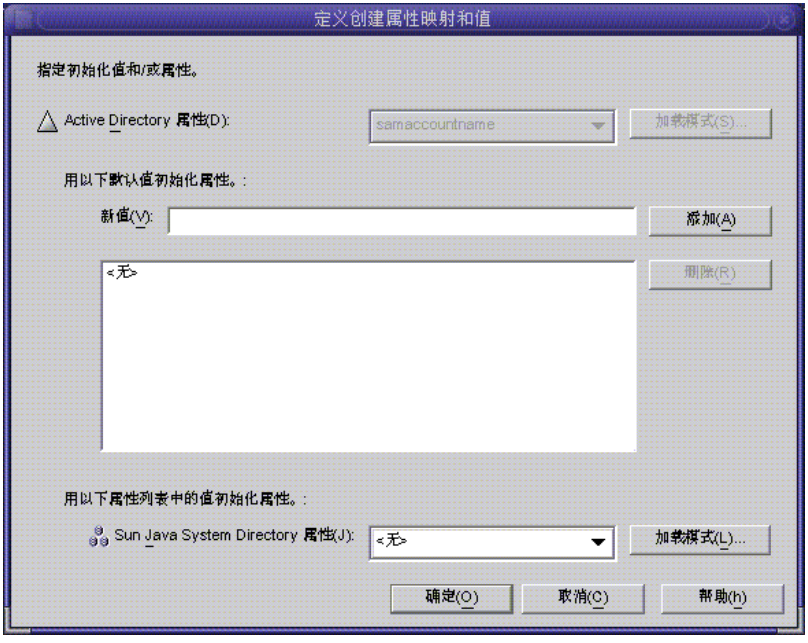
指定新的创建属性

以下说明介绍如何添加和映射从 Active Directory 流向 Directory Server 的创建属性。（从 Directory Server 流向 Windows 的创建属性与从 Windows 流向 Directory Server 的创建属性的添加和映射步骤相似。）

1. 单击 “创建属性映射和值”对话框中的 “新建”按钮。

   将显示 “定义创建属性映射和值” 对话框 （图 4-37）。

图 4-37 定义创建属性映射和值



2. 从 Active Directory 属性下拉列表中选择某个属性值。

图 4-38 选择新的 Active Directory 属性

Identity Synchronization for Windows 允许使用多个值初始化一个属性 （如果该属性本身接受多个值）。

例如，如果贵公司有三个传真电话号码，您可以为 Sun Java System Directory Server 和 Active Directory 同时设置 `facsilimiletelephonenumber` 属性，并为该属性指定三个号码。

*必须知道哪些属性能接受多个值。*如果尝试将多个值添加到不接受这些值的某个属性中，则在程序试图创建该对象的运行时期间，会出现错误。

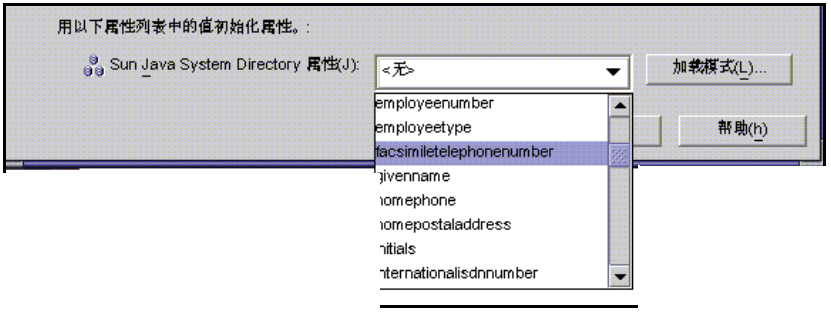
3. 在 “新值”字段中输入一个值，然后单击 “添加”。

   程序将该属性值添加至列表窗格中。根据需要重复执行此步骤，以添加多个属性值。

图 4-39 为创建属性指定多个值

4. 要将该属性映射到 Directory Server，请从 Directory Server 属性下拉列表中选择一个属性名称。

图 4-40 映射 Directory Server 属性



5. 完成后，单击 “确定”。

   根据示例，完成的 “创建属性和映射”表应类似下图中的一个表：

图 4-41 完成的 “创建属性和映射”表

Active Directory	Directory Server	值
cn	cn	
samaccountname	<无>	
facsimiletelephonenumber	facsimiletelephonenumber	[222-222-2222,555-555-5...

6. 要指定附加属性，请重复上述步骤。

编辑现有属性

要编辑创建属性的任何映射或值

1. 选择 “对象创建”选项卡，然后单击选定创建选项下的 “创建属性”按钮。
2. 出现 “创建映射和值”对话框后，从表中选择属性，然后单击 “编辑”按钮。

   将显示 “定义创建映射和值”对话框。
3. 使用下拉菜单更改 Directory Server 和 Active Directory （或 Windows NT）间的现有映射。

   例如，如果已将 Sun Java System Directory Server 的 homephone 属性映射至 Active Directory 的 othertelephone 属性。可使用 Active Directory 属性下拉列表将映射更改为 homephone。
4. 还可以添加或删除属性值：
   - 要添加值，请在 “新值”字段中输入相应信息，然后单击 “添加”。
   - 要删除值，请从列表窗格中选择值，然后单击 “删除”。
5. 完成后，单击 “确定”应用更改，并关闭 “定义创建映射和值”对话框。
6. 再次单击 “确定”关闭 “创建映射和属性”对话框。

删除属性

要删除创建属性映射或值

1. 选择 “对象创建”选项卡，然后单击选定创建选项下的 “创建属性”按钮。
2. 出现 “创建映射和值”对话框后，从表中选择属性，然后单击 “删除”按钮。

   该属性立即被从表中删除。
3. 完成后，单击 “确定”关闭 “创建映射和属性”对话框。

指定对象修改如何流动

使用 “属性修改”选项卡（图 4-42）控制对用户属性和密码进行的修改如何在 Sun 和 Windows 系统间传播 （流动）。

图 4-42 属性修改选项卡

使用此选项卡可进行以下配置：

- 指定修改在 Directory Server 和 Windows 目录源间的流动方向。
- 控制是否在 Directory Server 和 Active Directory 目录源间同步对象激活和禁用（Active Directory 上的*启用*和*禁用*），并指定激活和禁用用户帐户的方法。

注意 不能与 Windows NT 目录源同步帐户状态。

指定方向

选择以下按钮之一可控制在 Directory Server 和 Windows 环境下进行的更改如何在系统间传播。

- **属性修改从 Sun Java System Directory Server 流向 Windows**：将在 Directory Server 环境中进行的修改传播至 Windows 服务器。
- **属性修改从 Windows 流向 Sun Java System Directory Server**（*默认*）：将在 Windows 环境中进行的更改传播至 Directory Server。
- **属性修改双向流动**：双向传播更改（从一个环境至另一个环境）。

配置和同步对象激活和禁用

如果启用“与 Active Directory 同步对象激活 / 禁用”框（参见图 4-43），可在 Directory Server 和 Active Directory 目录源之间同步对象激活和禁用（称为在 Active Directory 中*启用*和*禁用*）。

注意 不能与 Windows NT 目录源同步激活和禁用。

图 4-43 同步对象激活和禁用

要同步对象激活 / 禁用：

1. 启用 “在 Directory Server 和 Active Directory 间同步对象禁用”框。
2. 启用以下按钮之一可指定 Identity Synchronization for Windows 检测和同步对象激活和禁用的方法：
   - **与 Directory Server 工具交互操作** （请参阅第 138 页）
   - **直接修改 Directory Server 的 nsAcountlock 属性** （请参阅第 139 页）
   - **为 Directory Server 使用自定义方法** （请参阅第 140 页）

注意 这些选项互斥。

- 启用 “与 Directory Server 工具交互操作”选项，则 Identity Synchronization for Windows 无法直接设置或删除 `nsAccountLock` 属性。另外，该程序无法检测已经使用其它角色 （如 `cn=nsdisabledrole`、`<`*database suffix*`>`）或嵌套在其它角色中的角色 （如 `cn=nsdisabledrole, <`*database suffix*`>` 或 `cn=nsmanageddisabledrole, <`*database suffix*`>`）禁用的对象。
- 如果启用 “修改 Directory Server 的 `nsAccountLock` 属性”选项，则 Identity Synchronization for Windows 将不检测使用 “Directory Server 控制台”或命令行实用程序激活 / 禁用的对象。
- 如果启用 “对 Directory Server 使用自定义方法”选项，则 Identity Synchronization for Windows 无法锁定目录外的对象，除非对该目录的访问是通过外部应用程序 （如 Sun Java™ System Access Manager，原来称为 Sun JES Identity Server）控制的。

与 Directory Server 工具交互操作

如果使用 “Directory Server 控制台”或命令行工具激活 / 禁用某个对象，则可选择此选项。

- 为激活对象， Identity Synchronization for Windows 会从 `nsroledn` 属性中将 `cn=nsmanageddisabledrole,<`*database suffix*`>` 值删除。
- 为禁用对象， Identity Synchronization for Windows 会将 `cn=nsmanageddisabledrole,<`*database suffix*`>` 值添加到 `nsroledn` 属性中。

注意 如果启用 “与 Directory Server 工具交互操作”选项，则 Identity Synchronization for Windows 无法直接设置或删除 nsAccountLock 属性。另外， Identity Synchronization for Windows 无法检测已使用其它角色禁用的对象。

例如， cn=nsdisabledrole, <*database suffix*> 或嵌套在其它角色中的角色，如 cn=nsdisabledrole, <*database suffix*> 或 cn=nsmanageddisabledrole, <*database suffix*>。

表 4-1 说明启用 “与 Directory Server 工具交互操作”选项后， Identity Synchronization for Windows 如何检测和同步对象激活 / 禁用：

表 4-1 与 Directory Server 工具交互操作

激活	禁用
仅当从对象中删除 cn=nsmanageddisabledrole,<*database suffix*> 角色后， Identity Synchronization for Windows 才检测激活。	仅当条目的 nsroledn 属性包括 cn=nsmanageddisabledrole,<*database suffix*> 角色时， Identity Synchronization for Windows 才检测禁用。
从 Active Directory 同步对象激活时， Identity Synchronization for Windows 将通过从对象中删除 cn=nsmanageddisabledrole,<*database suffix*> 角色来激活对象。	从 Active Directory 同步对象禁用时， Identity Synchronization for Windows 会通过将 cn=nsmanageddisabledrole,<*database suffix*> 角色添加到对象中来禁用对象。

直接修改 Directory Server 的 NsAccountLock 属性

如果 Directory Server 激活和禁用是基于 Directory Server 的操作属性 nsAccountLock，则使用此方法。此属性按以下方式控制对象状态：

- 如果 nsAccountLock=true，则对象被禁用且用户无法登录。
- 如果 nsAccountLock=false （或无值），则对象被激活。

表 4-2 说明启用 “直接修改 Directory Server 的 nsAccountLock 属性”选项后，Identity Synchronization for Windows 如何检测和同步对象激活 / 禁用：

表 4-2 直接修改 Directory Server 的 nsAccountLock 属性

激活	禁用
Identity Synchronization for Windows 仅在将 nsAccountLock 属性设置为 **true** 时才会检测禁用的对象。	Identity Synchronization for Windows 仅在没有 nsAccountLock 属性或其值被设置为 **false** 时才检测激活的对象。
从 Active Directory 同步对象禁用时， Identity Synchronization for Windows 会删除 nsAccountLock 属性。	从 Active Directory 同步对象激活时， Identity Synchronization for Windows 会将 nsAccountLock 属性设置为 **true** 。

对 Directory Server 使用自定义方法

如果 Directory Server 激活和禁用是通过外部应用程序 （如 Sun Java™ System Access Manager，原名 Sun JES Identity Server）专门控制的，请使用此方法。

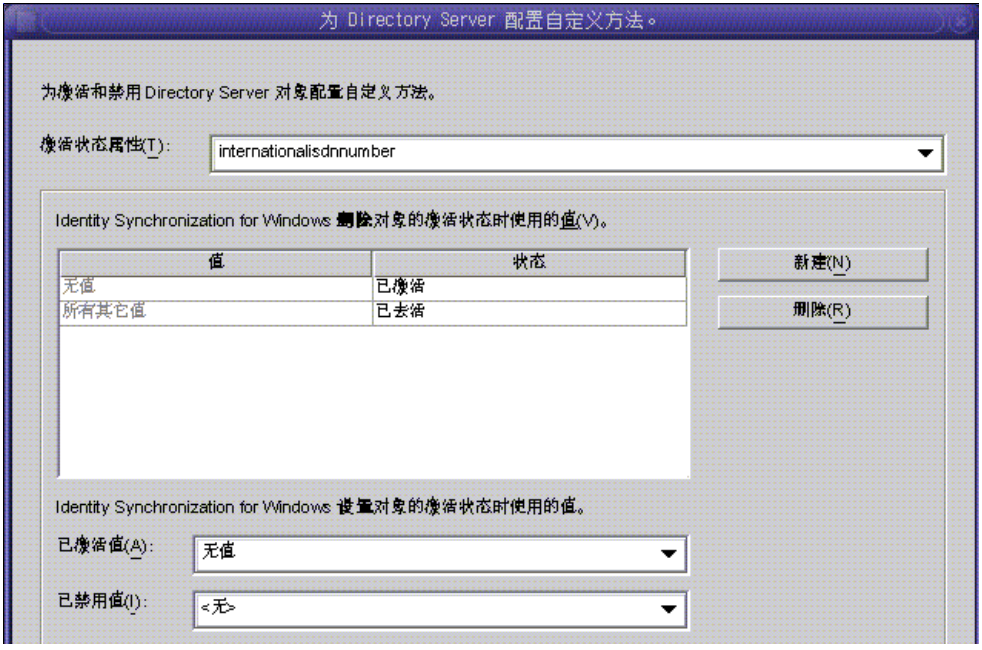
为 Directory Server 配置自定义方法时，必须指定：

- Identity Synchronization for Windows 如何检测外部应用程序是否已激活或禁用 Directory Server 中的某个对象
- 从 Active Directory 同步到 Directory Server 时， Identity Synchronization for Windows 如何激活或禁用对象

注意 如果启用 “对 Directory Server 使用自定义方法”选项，则 Identity Synchronization for Windows 无法锁定目录外的对象，除非对该目录的访问是通过外部应用程序 （如 Access Manager）控制的。

要为激活和禁用配置 “自定义” 方法，请单击 “配置” 按钮，将会显示 “为 Directory Server 配置自定义方法” 对话框 （参见图 4-44）。

图 4-44 为激活和禁用配置自定义方法



此对话框包含以下功能：

- **激活状态属性下拉列表**：使用此列表可指定 Identity Synchronization for Windows 用来在 Directory Server 和 Active Directory 间同步激活和禁用的属性。

  该列表包含用于当前选定 Directory Server 结构和辅助对象类模式中的所有属性。

- **值和状态表**：使用此表可指定何时激活或禁用与选定属性相关的值。

  - **值列**：使用此列 （与 “新建” 和 “删除” 按钮联用）可指定用于指示活动或非活动状态的属性值。

程序会在此列中自动提供两个值：

- **无值**：其中，处于 “已激活”状态的属性不含有值。
- **所有其它值**：其中的 “已激活”状态属性有一个值，但该值未在此 “值和状态”表中指定。

- **状态列**：使用此列可指定是激活还是禁用了与某个对象相对应的 “值”条目 （位于同一行中）。

表 4-3 指定已激活和已去活状态

值	状态	结果
无值	已激活	如果缺少属性或者没有值， Identity Synchronization for Windows 会将对象检测为已激活。
	已去活	如果缺少属性或者没有值， Identity Synchronization for Windows 会将对象检测为已去活。
< *用户自定义* > 值	已激活	如果属性有 < *用户自定义* > 属性，Identity Synchronization for Windows 会将对象检测为已激活。
	已去活	如果属性有用户自定义属性， Identity Synchronization for Windows 会将对象检测为已去活。
所有其它值	已激活	如果属性具有值，但该值未在表中指定， Identity Synchronization for Windows 会将对象检测为已激活。
	已去活	如果属性具有值，但该值未在表中指定， Identity Synchronization for Windows 会将对象检测为已去活。

- **“新建”按钮**：单击此按钮可将新条目添加到 “值”列中。
- **“删除”按钮**：在 “值”列中选择某个条目，然后单击此按钮可删除该条目。
- **“已激活值”和 “已禁用值”下拉列表**：使用这两个列表可指定 Identity Synchronization for Windows 用来 *设置*对象状态的值。

同步激活和禁用 使用以下步骤可将 Identity Synchronization for Windows 配置为在 Directory Server 和 Active Directory 间检测和同步对象状态：

1. 从 “激活状态属性”下拉列表中选择某个属性。
2. 单击 “新建”按钮将属性值添加到表的 “值”列中。
3. 单击每个 “值”条目旁的 “状态”列，显示下拉列表后，选择 “已激活”或 “已去活”。

图 4-45 选择状态

例如，如果使用 Access Manager：

1. 从 “激活状态属性”下拉列表中选择 **`inetuserstatus`** 属性。
2. 单击 “新建”按钮并在表的 “值”列中输入**活动的**、**非活动**和**已删除**属性值。
3. 在 “状态”列中单击并为每个值选择 “已激活”或 “已禁用”，具体如下：
   - **无值**：已激活
   - **活动的**：已激活
   - **非活动**：已禁用
   - **已删除**：已禁用
   - **所有其它值**：已禁用

表 4-4 以此示例为基础，介绍了启用 “对 Directory Server 使用自定义方法”选项后， Identity Synchronization for Windows 如何检测和同步激活 / 禁用 （使用 `inetuserstatus` 示例）。

表 4-4 使用 inetuserstatus 值的示例结果

值	状态	结果
无值	已激活	如果缺少 `inetuserstatus` 属性或者它没有值，则 Identity Synchronization for Windows 会将对象检测为已激活。
活动的	已激活	如果属性为**活动的**，则 Identity Synchronization for Windows 会将对象检测为已激活。
非活动	已禁用	如果属性值为**非活动**，则 Identity Synchronization for Windows 会将对象检测为已禁用。
已删除	已禁用	如果属性值为**已删除**，则 Identity Synchronization for Windows 会将对象检测为已禁用。
所有其它值	已禁用	如果属性具有值，但该值未在表中指定， Identity Synchronization for Windows 会将对象检测为已禁用。

设置激活和禁用 用条目内容填充“值”和“状态”表时，Identity Synchronization for Windows 会自动填充**已激活值**和**已禁用值**下拉列表，具体如下：

- “已激活值”列表包含所有状态为 “已激活”的值 （例如**无值**和**活动的**）。
- “已禁用值”列表包含所有状态为 “已禁用”的值 （例如**非活动**和**已删除**）。
- 这两个列表中均不包含值 “所有其它值”。

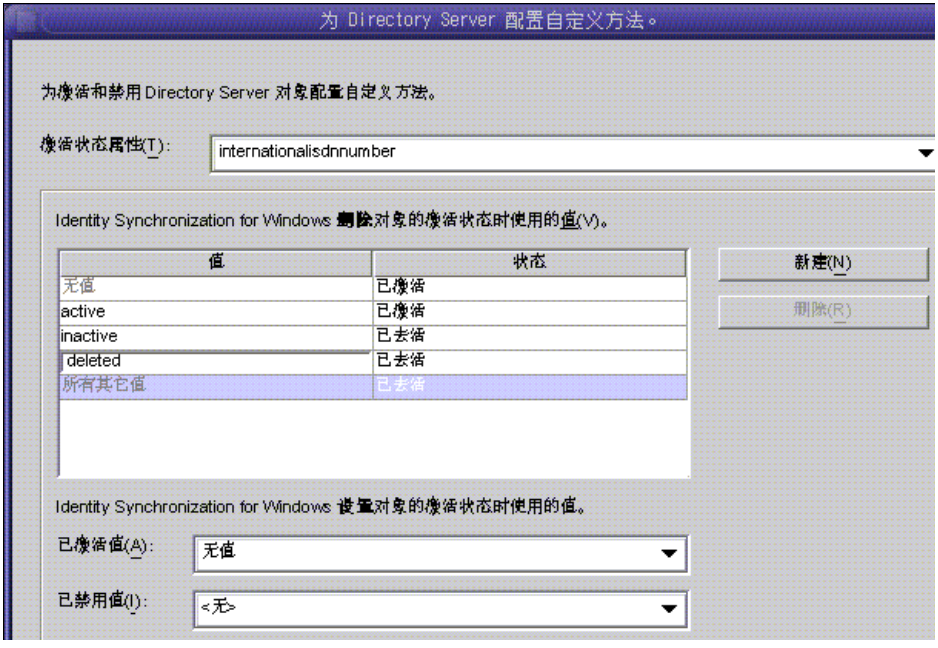
从“已激活值”和 / 或“已禁用值”下拉列表选择一个值，以指定从 Active Directory 同步时 Identity Synchronization for Windows 如何激活和 / 或禁用对象。

- **已激活值**：控制对象的活动状态。
  - **无值**：如果对象包含活动的值，则 Identity Synchronization for Windows 会在 Directory Server 中将状态设置为已激活。
  - **活动的**：如果对象包含活动的值，则 Identity Synchronization for Windows 会在 Directory Server 中将状态设置为已激活。
- **已禁用值**：控制对象的活动状态。
  - **非活动**或**已删除**：Identity Synchronization for Windows 会在 Directory Server 中将对象状态设置为非活动。
  - **<** *无* **>**：不是有效设置。必须选择一个值。

注意 必须指定 “已禁用值”，否则配置将无效。

图 4-46 显示了已完成的 “为 Directory Server 配置自定义方法”对话框。

图 4-46 示例：已完成的对话框



指定删除如何流动

使用 “对象删除”选项卡指定删除的用户条目应如何在 Directory Server 和 Active Directory 系统间流动。

注意 不能为 Windows NT 指定 “对象删除”流动。

1. 选择导航窗格顶部的 Identity Synchronization for Windows 节点，然后单击“对象删除”选项卡。

图 4-47 传播用户条目删除

2. 启用或禁用删除的流动，如下所述：
   - 启用**对象删除从 Sun Java System Directory Server 流向 Active Directory** 可以将删除从 Directory Server 环境传播至 Active Directory 服务器。
   - 启用**对象删除从 Active Directory 流向 Sun Java System Directory Server** 可以将删除从 Active Directory 环境传播至 Directory Server。
   - 同时启用上述两个选项可以实现双向流动。
   - 同时禁用上述两个选项可以阻止用户删除从一个系统传播到另一个系统。（*默认设置*）

创建同步用户列表

“同步用户列表” (SUL) 指定两个目录源中的哪些用户将被同步。 SUL 中的每个条目都要通过 “连接器”，并针对为该 SUL 配置的限制条件进行评估。

每个 SUL 包含两个元素，一个用于确定要同步的 Directory Server 用户，一个用于确定要同步的 Windows 用户。

注意 如果要同步 Directory Server 中有多个 Active Directory 域的用户，必须为每个 Active Directory 域定义一个 SUL。

有关定义和配置 SUL （包括定义的组件、如何定义多个 SUL、如何处理多个 SUL 以及如何配置多个 Windows 域支持）的详细信息，请参阅第 331 页的附录 D，“定义和配置同步用户列表”。

SUL 的以上两个元素都含有三个定义，可确定要同步的用户：

- **基本 DN**：将被同步的用户的位置 （不适用于 NT）
- **命名属性**：用于新建的用户的属性 （创建表达式）（不适用于 NT）
- **过滤器**：将指定用户排除在同步范围之外

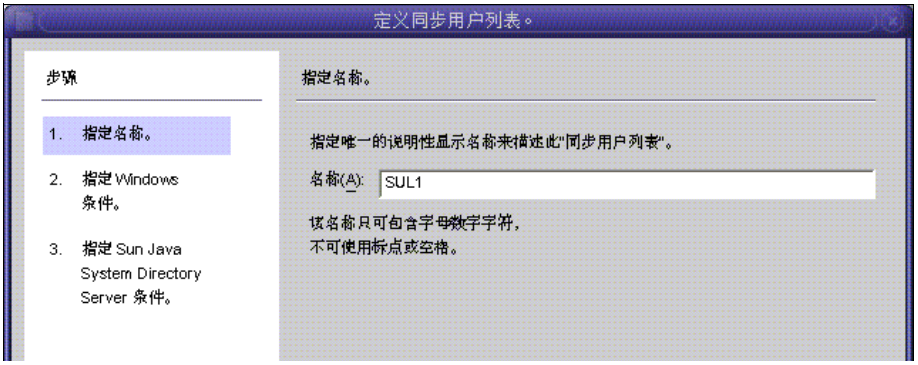
要在服务器间标识和链接用户类型：

1. 选择导航树中的“同步用户列表”节点，然后单击“新建同步用户列表”按钮。

图 4-48 创建新的同步用户列表

将显示“定义同步用户列表”向导，如下所示：

图 4-49 指定 SUL 的名称



程序将第一个“同步用户列表”默认为 *SUL1*。

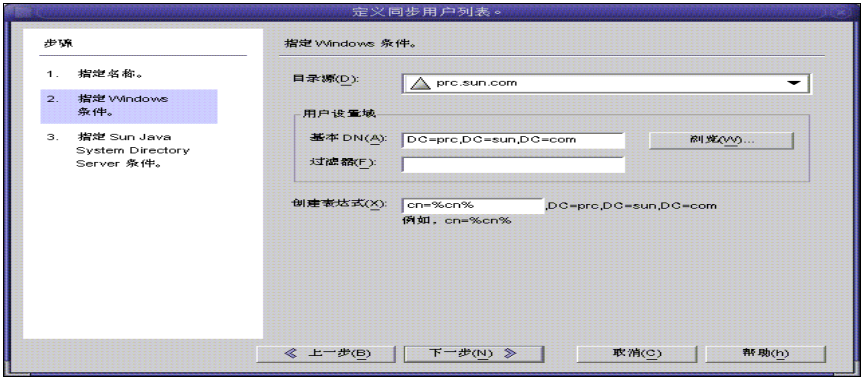
- 如果默认名可接受，请单击“下一步”。
- 如果要使用不同的名称，请在“名称”字段中键入不同的名称，然后单击“下一步”。

注意

- 不要在 SUL 名称中使用空格或任何标点符号。
- 必须指定在系统内唯一的名称。

将显示如图 4-50 中所示的“Windows 条件”面板。

图 4-50 指定 Windows 条件



2. 从下拉列表中选择 “Windows 目录源”。

注意 创建 SUL *后*不能再编辑此目录源。

3. *用户设置域*是要同步的所有用户的设置。使用以下方法之一输入 “用户设置域” 的 “基本 DN”：

   - 将名称键入文本字段中 （例如 **`DC=example,DC=com`**）。
   - 单击 “浏览”按钮打开 “设置基本 DN”对话框，以便可以查找和选择一个 “基本 DN”。

图 4-51 选择基本 DN

除非使用过滤器明确地将用户排除在此 SUL 以外，否则位于该指定的 “基本 DN”下的所有用户都将包括在此 SUL 中。

注意 Windows NT 系统不允许使用 “基本 DN”和创建表达式。

4. 可以输入一个等同、存在或子字符串 “过滤器”，以指定此基本 DN 中的哪些用户将被同步。例如，如果对多个同步用户列表使用相同的基本 DN，则可能需要使用过滤器区分它们。

   等同过滤器语法类似于 LDAP 查询语法，只是等同字符串仅允许使用 *、 &、 |、 =、 ！字符。例如，可以使用以下过滤器将管理员从 SUL 中排除：

   (!(cn=Administrator))

   程序将自动填写 “创建表达式”字段。

   注意 创建表达式定义新条目从 Active Directory 传播至 Directory Server 时使用的父 DN 和命名属性。

   创建表达式不适用于 Sun 目录，除非已将用户属性创建配置为从 Active Directory 流向 Directory Server （请参阅第 131 页的 “指定对象创建如何流动”）。

5. 如果缺少创建表达式，或者要更改现有条目，可以为所有的 Windows Active Directory 同步用户列表输入一个创建表达式；例如：

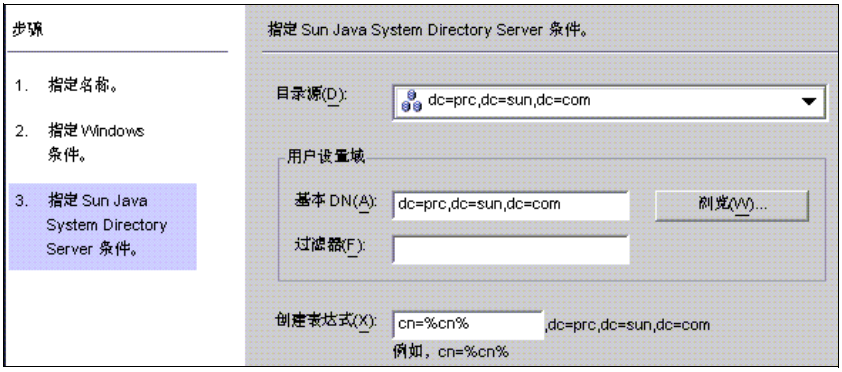
   cn=%*cn*%,cl=*users*,dc=example,dc=com

   如果要更改创建表达式，必须选择一个要同步的属性。如果需要，可以返回到 “对象创建”选项卡，并使用 “创建属性”按钮添加和映射此属性。

6. 单击 “下一步”指定 Sun Java System Directory Server 条件。

7. 出现 “指定 Sun Java System Directory Server 条件”面板后，重复步骤 2 至步骤 5，以提供 Directory Server 条件。

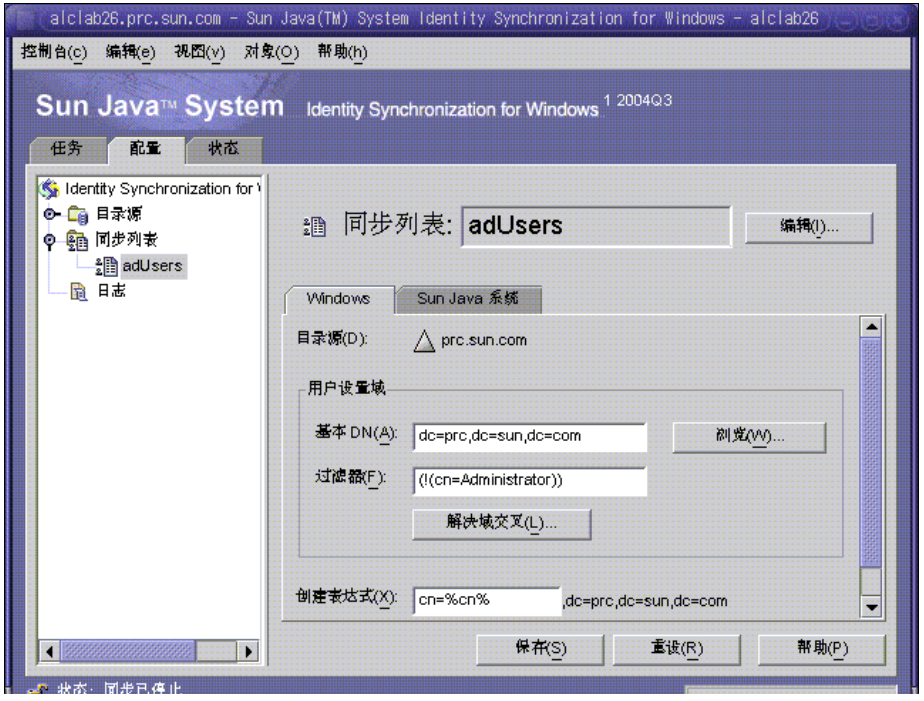
图 4-52 指定 Directory Server 条件



注意 单击 “完成”按钮创建 SUL 后，不能再编辑此 SUL 中所包括的 Active Directory 或 Directory Server 目录源。

8. 完成后，单击 “完成”。
9. 程序会将新的 SUL 节点添加至导航树，并且 “配置”选项卡上将显示 “同步用户列表”面板。

图 4-53 同步列表面板



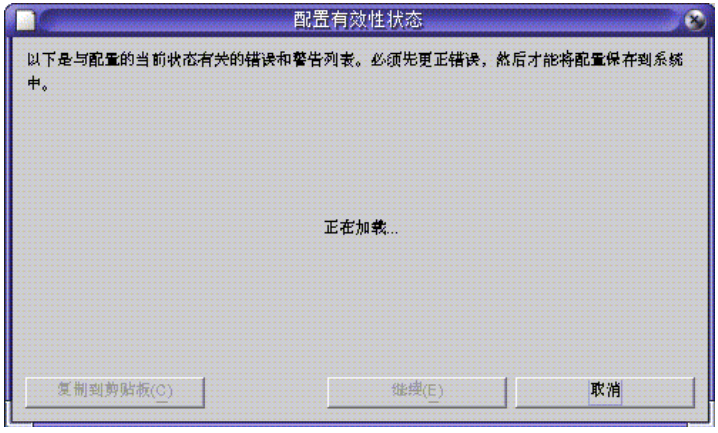
10. 在一个用户与多个列表匹配的情况下，单击“解决域交叉”按钮定义同步用户列表的首选项。（有关详细信息，请参阅第 331 页的“了解同步用户列表定义”。）
11. 创建一个包括网络中除 Directory Server 以外所有目录源的 “同步用户列表”。

保存配置

从任意 “控制台” 面板保存当前配置

1. 单击 “保存” 可以存储当前的设置。
2. 当程序检查配置设置时，将显示 “配置有效性状态” 窗口。

图 4-54 配置有效性状态窗口



保存配置可能需要几分钟时间，因为程序要将信息重新写入配置目录，并通知系统管理器。

系统管理器 （核心组件之一）负责将配置设置分发到需要该信息的各组件中。

注意 配置有效性错误以红色显示，警告以黄色显示。

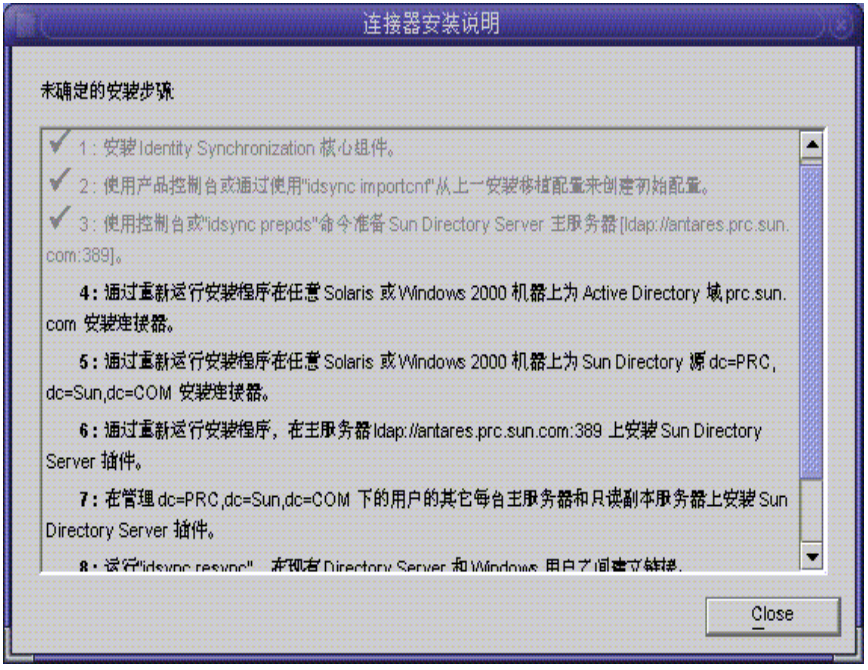
- 不能保存含有错误的配置。
- 可以保存含有警告的配置，但最好先尝试清除警告。

3. 如果配置有效，则单击 “继续” 保存该配置。

将出现 “连接器安装说明” 对话框 （类似于图 4-55 中的列表），提供如何继续安装 Identity Synchronization for Windows 连接器和子组件的说明。

此列表现在已用针对部署而自定义的 “待执行” 列表更新。（至此所介绍的均为常用步骤。）请注意，您也可从 “Identity Synchronization for Windows 控制台” 的 “状态” 选项卡访问和更新 “待执行” 列表。

图 4-55 连接器安装说明



4. 请仔细阅读该信息，然后单击 “确定”。

完成 “核心”初始配置后，就可以安装 Identity Synchronization for Windows 连接器和子组件了。有关说明，请继续阅读第 5 章，“安装连接器和 Directory Server 插件”。

第 5 章

安装连接器和 Directory Server 插件

本章介绍 Identity Synchronization for Windows 连接器和 Directory Server 插件的安装说明。内容具体安排如下：

Identity Synchronization for Windows 使用 “连接器”在目录源之间同步用户密码，并使用子组件增强 “连接器”的更改检测和双向同步支持。

开始之前

开始安装连接器 /Directory Server 插件之前，应注意以下几点：

- 在安装过程开始之前，关闭 “控制台”。如果在安装 “连接器”或 “插件”时，“控制台”处于打开状态，则程序会发现组件向服务器添加配置数据的冲突，并生成一条错误消息。
- 必须在部署中存储将被同步的用户的每一台 Directory Server 机器上都 （包括主服务器、副本和集线器）安装 Directory Server 插件。
- Active Directory Connector 没有子组件。
- Windows NT Connector 和子组件将被同时安装。
- 可以在安装 “核心”的机器上安装 Directory Server Connector 或 Active Directory Connector，或者将它们安装在另一台机器上。（Windows NT Connector 必须安装到要同步的域的 “主域控制器” (PDC) 上。）

- 如果将 “连接器”与 “核心”安装在相同的机器上，则程序会自动将 “连接器”安装在 “核心”所在的目录中。
- 如果在另一台机器上安装 “连接器”，则程序会提示您指定
  - 安装 “核心”期间提供的配置目录信息
  - 安装目录

- 每次安装 “连接器”或 Directory Server 插件时，都必须运行安装程序。

  例如，如果要安装 Directory Server Connector、单个 Directory Server 插件和 Active Directory Connector，则需要在安装 “核心”后分别运行三次安装程序。

运行安装程序

执行以下步骤重新启动并运行安装程序。每次安装 “连接器”或 Directory Server 插件时都要重复执行这些步骤：

1. 在想要安装 “连接器”的机器上重新运行安装程序，如下所述：
   - **在 Solaris 中**：变换到 `installer` 目录，然后键入 **`./runInstaller.sh`** 执行安装程序。

注意	要在基于文本的模式下运行安装程序，请键入 **`./runInstaller.sh -nodisplay`** 运行 `runInstaller.sh` 程序时， Identity Synchronization for Windows 将自动屏蔽密码，从而密码不会以明文显示。

   - **在 Windows 中**：变换到 `installer` 目录，然后键入 **`setup.exe`** 执行安装程序。
2. 显示 “欢迎”屏幕时，请阅读屏幕信息，然后单击 “下一步”进入 “软件许可证协议”面板。
3. 阅读许可证协议，然后选择
   - **是 （接受许可证）**，接受许可证条款并转到下一面板。
   - **否**，停止安装过程并退出安装程序。

4. 将显示 Sun Java System Directory Server 面板。指定配置目录位置，如下所述：

   - **配置目录主机**：输入存储 Identity Synchronization for Windows 配置信息的 Sun Java System Directory Server 实例 （与 Administration Server 关联）的全限定域名 (FQDN)。指定的实例必须与 “核心” 安装期间指定的实例相同。
   - **配置目录端口** （*默认为端口 389*）：指定配置目录的端口。可以保留端口的默认值，或更改为一个不同的可用端口。

     要在 “核心” 与配置目录之间启用 SSL （安全套接字层），请启用 “安全端口” 选项，并指定一个 SSL 端口 （*默认 SSL 端口是 636*）。启用此选项可以防止敏感信息以明文形式通过网络传递。
   - **配置根后缀**：从菜单中选择 “核心” 安装期间指定的根后缀。 Identity Synchronization for Windows 配置将被存储在此根后缀中。

   注意 如果程序无法检测到根后缀并且您手动输入服务器信息，则必须单击 “刷新” 重新填充根后缀列表。

5. 单击 “下一步” 打开 “配置目录证书” 面板。
6. 输入配置目录管理员的用户 ID 和密码。
   - 如果指定 `admin` 作为用户 ID，则无需指定 “用户 ID” 作为 DN。
   - 如果使用其它用户 ID，则必须指定 ID 作为完整 DN。
     例如， *cn=Directory Manager*。

   注意 除非在步骤 4 中启用了 SSL，否则这些证书不经加密就会被发送出去。

7. 单击 “下一步” 打开 “配置密码” 面板，必须在该面板中输入安装 “核心” 时指定的配置密码。

   同时，若此机器上尚未安装 “核心”，则将提示您提供 Java 主目录的位置 （请参阅第 89 页）。
8. 完成后，单击 “下一步”。

注意 此时，安装过程将特定于 Directory Server 插件或正在安装的 “连接器” 类型。

- 要安装 “连接器”，请继续阅读第 158 页的 “安装连接器”。
- 要安装 Directory Server 插件，请继续阅读第 169 页的 “安装 Directory Server 插件”。

安装连接器

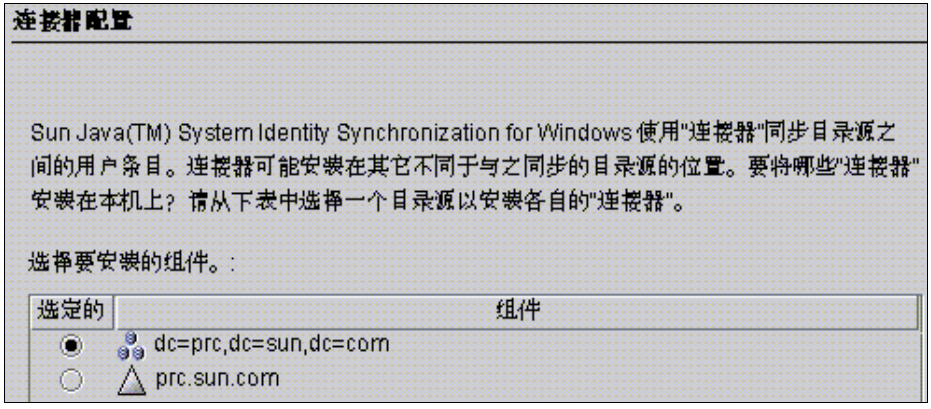
本节说明如何安装三种类型的 Identity Synchronization for Windows 连接器，具体内容如下：

注意 不必按特定顺序安装 “连接器”，但不要试图同时安装所有 “连接器”。

安装 Directory Server Connector

完成第 156 页的 “运行安装程序”中说明的步骤后，将显示 “连接器配置”面板。

图 5-1 选择 Directory Server Connector



“选择要安装的组件”列表仅包含尚未安装的 “连接器”组件。例如，安装 Directory Server Connector（图 5-1 中的 dc=example,dc=com）后，程序将从列表窗格中删除相应条目。

下表中含有一些目录源条目示例：

表 5-1 目录源示例

目录源	示例条目
Sun Java System Directory Server	`dc=example,dc=com`
Windows Active Directory	`example.com`
Windows NT SAM	`EXAMPLE`

安装 Directory Server Connector：

1. 启用 Directory Server Connector 组件旁的按钮，然后单击 “下一步”。

   将显示 “Directory Server 连接器证书”面板 （图 5-2）。

图 5-2 输入 Directory Server 连接器证书信息

注意 程序将自动使用全限定 “目录管理员”识别名来填写 “用户 DN”字段，但您可根据需要更改信息。

输入以下信息：

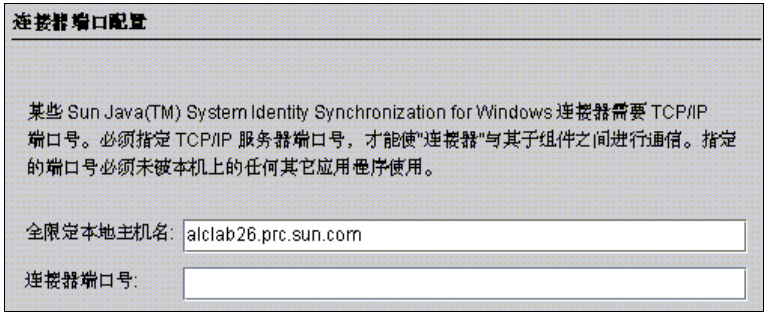
- **主目录服务器用户 DN**：如果需要，通过输入全限定 “目录管理员”识别名来更改默认用户 DN。
- **主目录服务器密码**：输入 “目录管理员”密码。

如果使用的是备用主服务器，则 “备用目录服务器用户名”和 “备用目录服务器密码”字段将处于活动状态。程序将使用为 “主目录服务器用户 DN”和 “主目录服务器密码”字段提供的相同条目自动填写 “目录管理员 DN”字段。可根据需要更改此信息。

程序将检查 Directory Server 是否已准备好并可以同步数据。准备好 Directory Server 后 （第 109 页），程序会创建一个帐户，“连接器”将使用该帐户连接至 Directory Server （例如， uid=PSWConnector,*suffix*）。

2. 单击 “下一步”，转到 “连接器端口配置”窗格。

图 5-3 指定连接器本地主机和端口

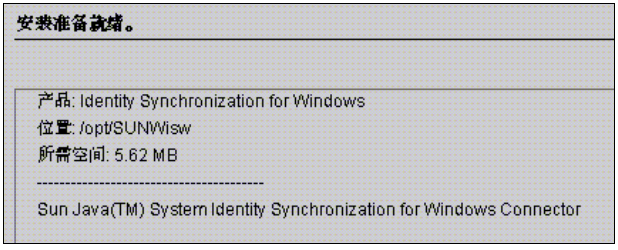


3. 输入带有域的 “全限定本地主机名”和 “连接器”侦听的可用端口号。（指定已使用的端口将导致出现错误消息。）

   Directory Server 插件需要访问您保存在 “控制台”中的配置信息。为获得此信息，“插件”将通过此端口上的服务器套接字与 Directory Server Connector 进行通信。另外，该 “插件”通过此频道记录消息，因此消息能够转到中心日志。

4. 单击 “下一步”，将显示 “安装准备就绪”窗格，提供有关 “连接器”安装位置和安装所需磁盘空间的信息。当一切就绪后，单击 “立即安装”按钮。

图 5-4 安装准备就绪窗格



注意 若在本地机上安装了 “核心”，则 “安装准备就绪”窗格会指示安装 “连接器”不需要任何空间。出现此种情况的原因是 “核心”安装已安装了 “连接器”二进制文件。由于不需要安装其它二进制文件，因此无需另外的空间。

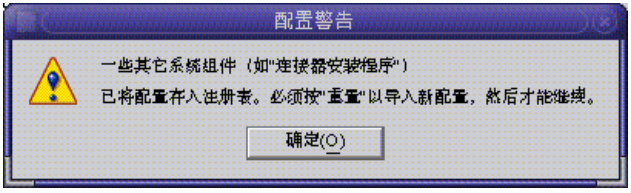
若要将 “连接器”安装到未安装 “核心”的机器上，则 “安装准备就绪”窗格会指示在本机上完成 “连接器”安装所需的空间。

“连接器”的安装分两步完成：

- 程序安装二进制文件时，显示带有进度条的 “安装”窗格。
- 接下来，会显示 “组件配置”窗格。由于此步骤需要数分钟才能完成，所以会显示一个进度条。

注意 如果在开始安装前未关闭 “控制台”，则会显示以下警告信息 （图 5-5）。单击 “控制台”中的 “重设”重新加载 “连接器”的配置设置。

图 5-5 配置警告对话框



当两步都完成后，会显示 “安装摘要”窗格。

5. 如果要查看安装日志，请单击 “详细信息”按钮。
   - **在 Solaris 中**：安装日志被写入 `/var/sadm/install/logs/` 中
   - **在 Windows 中**：安装日志被写入 `%TEMP%` 目录，它通常是 `Local Settings` 文件夹的子目录，该文件夹在 `C:\Documents and Settings\Administrator` 下

注意 在某些 Windows 系统中 （如 Windows 2000 Advanced Server）， `Local Settings` 文件夹是隐藏文件夹。

要查看此文件夹和 `Temp` 子目录，请打开 “Windows 资源管理器”，然后从菜单条中选择 “工具” > “文件夹选项”。显示 “文件夹选项”对话框后，选择 “查看”选项卡，并启用 “显示隐藏的文件”选项。

6. 单击 “下一步”，将显示 “待执行列表”窗格 （图 5-6），显示已成功完成的步骤和尚未完成的步骤。

图 5-6 待执行列表

7. 完成此面板的操作后，单击 “已完成”。

安装 Directory Server Connector 后，可以安装在配置资源时配置的其它 “连接器”和 / 或 Directory Server 插件 （第 4 章）：

- 安装附加 Directory Server Connector：重新启动安装程序 （遵循第 156 页的 “运行安装程序”中的说明），然后重复执行步骤 1 至步骤 7。
- 安装 Active Directory Connector：转至第 164 页的 “安装 Active Directory Connector”。
- 安装 Windows NT Connector：转至第 168 页的 “安装 Windows NT Connector”。
- 安装 Directory Server 插件：转至第 169 页的 “安装 Directory Server 插件”。

安装 Active Directory Connector

完成第 156 页的“运行安装程序”中说明的步骤后，将显示“组件类型选择”面板。

注意 安装 Directory Server Connector 后，如果还要安装其它已配置的“连接器”，则安装程序将在显示“连接器配置”窗格（图 5-7）前提供安装“连接器”或 Directory Server 插件的选项。

图 5-7 选择连接器

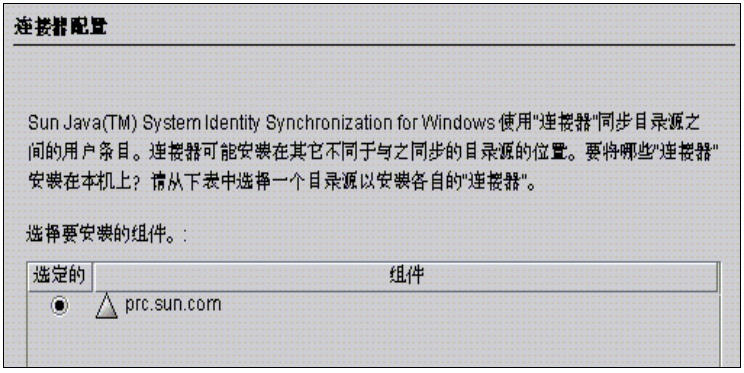
组件列表仅包含尚未安装的“连接器”组件。例如，如果已安装了 Directory Server Connector（此例中为 dc=example,dc=com），则该“连接器”不会显示在列表中。

安装 Active Directory Connector：

1. 启用“连接器”按钮，然后单击“下一步”。

   将显示“连接器配置”面板（参见图 5-8）。

图 5-8 选择 Active Directory Connector

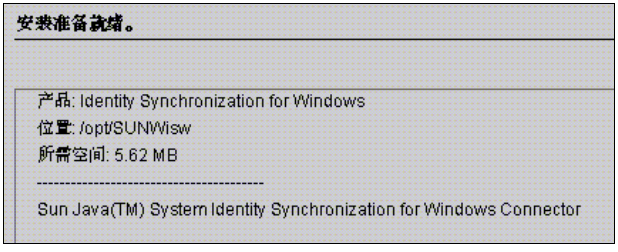


“选择要安装的组件”列表仅包含尚未安装的 “连接器”组件。例如，安装 Directory Server Connector （此例中为 dc=example,dc=com）后，程序将从此列表窗格中删除相应条目。

2. 启用 Active Directory 组件旁的按钮，然后单击 “下一步”。

   将显示 “安装准备就绪”窗格 （图 5-9），提供有关该 “连接器”安装位置以及安装所需磁盘空间的信息。

图 5-9 安装准备就绪窗格



注意 若在本地机上安装了 “核心”，则 “安装准备就绪”窗格会指示安装 “连接器”不需要任何空间。出现此种情况的原因是 “核心”安装已安装了 “连接器”二进制文件。由于不需要安装其它二进制文件，因此无需另外的空间。

若要将 “连接器”安装到未安装 “核心”的机器上，则 “安装准备就绪”窗格会指示在本机上完成 “连接器”安装所需的空间。

3. 当一切就绪后，单击 “立即安装”按钮。

   程序安装二进制文件时，显示带有进度条的 “安装”窗格，之后将显示 “安装摘要”窗格，以确认完成安装。

4. 如果要查看安装日志，请单击 “详细信息”按钮。

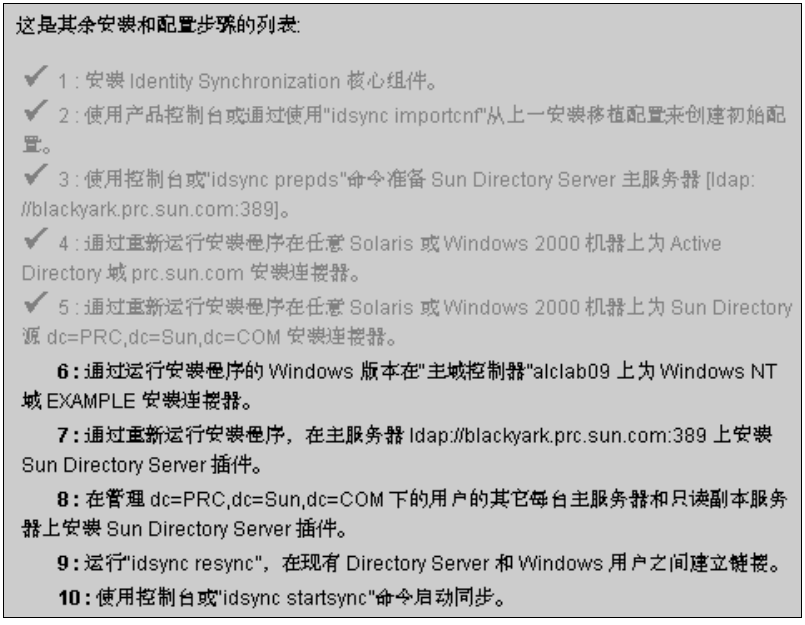
   - **在 Solaris 中**：安装日志被写入 `/var/sadm/install/logs/` 中
   - **在 Windows 中**：安装日志被写入 `%TEMP%` 目录，它是 `Local Settings` 文件夹的子目录，该文件夹在 `C:\Documents and Settings\Administrator` 下

注意 在某些 Windows 系统中 （如 Windows 2000 Advanced Server）， `Local Settings` 文件夹是隐藏文件夹。

要查看此文件夹和 `Temp` 子目录，请打开 “Windows 资源管理器”，然后从菜单条中选择 “工具” > “文件夹选项”。显示 “文件夹选项”对话框后，选择 “查看”选项卡，并启用 “显示隐藏的文件”选项。

5. 单击 “下一步”，将显示 “待执行列表”窗格 （图 5-10），显示已成功完成的步骤和尚未完成的步骤。

图 5-10 待执行列表



6. 完成此面板的操作后，单击 “已完成”，退出安装程序。

安装 Active Directory Connector 后，可以安装在配置资源时配置的其它 “连接器” 和 / 或 Directory Server 插件 （第 4 章）：

- 安装附加 Active Directory Connector：重新启动安装程序 （请参阅第 156 页的 “运行安装程序”），然后重复执行步骤 1 至步骤 6。
- 安装 Windows NT Connector：转至第 168 页的 “安装 Windows NT Connector”。
- 安装附加 Directory Server Connector：重新启动安装程序 （遵循第 156 页的 “运行安装程序”中的说明），然后重复执行步骤 1 至步骤 7。
- 安装 Directory Server 插件：转至第 169 页的 “安装 Directory Server 插件”。

安装 Windows NT Connector

注意 必须将 Windows NT Connector 安装到已配置的域的 “主域控制器” (PDC) 上。

完成第 156 页的 “运行安装程序”中说明的步骤后，将显示 “连接器配置”面板。

安装 Windows NT Connector 和 NT 子组件：

1. 启用 Windows NT Connector 按钮，然后单击 “下一步”。
2. 出现 “连接器端口配置”面板时，输入带有域的 “全限定本地主机名”和 “连接器”侦听的可用端口号。（指定已使用的端口将导致出现错误消息。）

   Directory Server 插件需要访问您保存在 “控制台”中的配置信息。要获得此信息，该 “插件”将通过此端口上的服务器套接字与 Windows NT Connector 通信。另外，该 “插件”通过此频道记录消息，因此消息能够转到中心日志。
3. 完成后，单击 “下一步”。

   将显示 “安装准备就绪”窗格，提供有关该 “连接器”安装位置以及所需磁盘空间的信息。
4. 当一切就绪后，单击 “立即安装”按钮。

   “连接器”的安装分两步完成：

   - 程序安装二进制文件时，显示带有进度条的 “安装”窗格。
   - 接下来，会显示 “组件配置”窗格。由于此步骤需要数分钟才能完成，所以会显示一个进度条。

   注意 如果在开始安装前未关闭 “控制台”，则会显示以下警告信息（参见图 5-5）。单击 “控制台”中的 “重设”重新加载 “连接器”的配置设置。

   当两步都完成后，会显示 “安装摘要”窗格。

5. 如果要查看安装日志，请单击 “详细信息”按钮。

   安装日志被写入 `%TEMP%` 目录，它是大多数 Windows NT 系统的 C:\TEMP 目录。

6. 单击 “关闭”退出安装程序。

安装 Windows NT Connector 后，可以安装在配置资源时配置的其它 “连接器”和 / 或 Directory Server 插件 （第 4 章）：

- 安装附加 Windows NT Connector：重新启动安装程序 （请参阅第 156 页的 “运行安装程序”），然后重复执行步骤 1 至步骤 6。
- 安装 Directory Server Connector：转至第 159 页的 “安装 Directory Server Connector”。
- 安装 Active Directory Connector：转至第 164 页的 “安装 Active Directory Connector”。
- 安装 Directory Server 插件：转至第 169 页的 “安装 Directory Server 插件”。

安装 Directory Server 插件

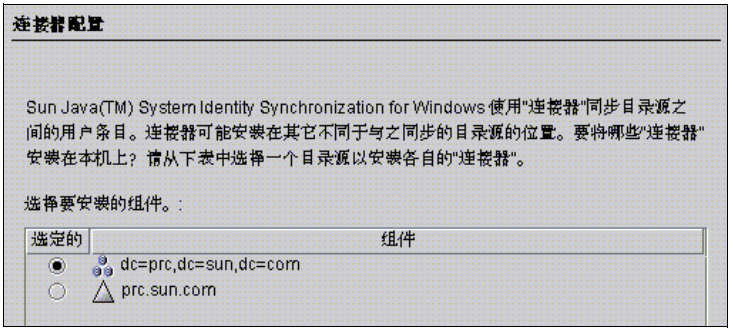
本节说明如何安装 Identity Synchronization for Windows Directory Server 插件。

注意 必须将 Directory Server 插件安装到安装 Directory Server 的机器上。

如果将该 “插件”安装到安装 “核心”或所有 “连接器”的系统中，安装程序将检测系统中 “核心”或 “连接器”的安装时间。所有附加组件都将安装到安装目录中。

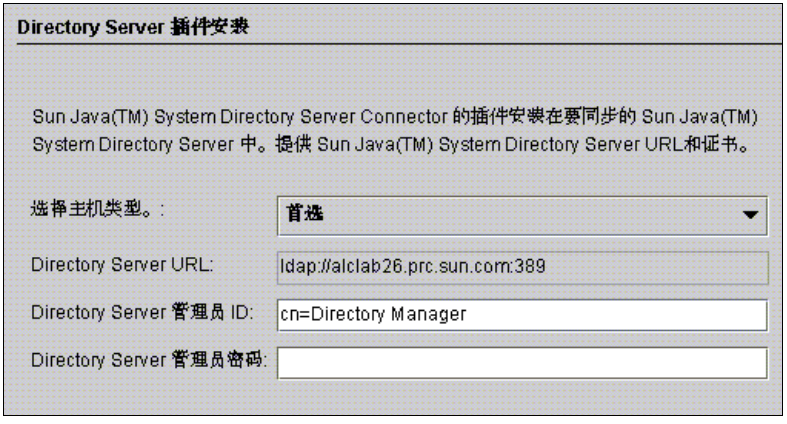
1. 完成第 156 页的 “运行安装程序”中所述步骤。

图 5-11 选择 Directory Server 插件



2. 显示 “连接器配置”面板时，启用 “Directory Server 插件” (dc=example,dc=com) 按钮，然后单击 “下一步”。
3. 将显示另一个 “Directory Server 插件安装”窗格 （图 5-12）。

图 5-12 指定 Directory Server URL 和证书



4. 从下拉列表中选择合适的 “主机类型”。
   - **首选**：如果是在首选服务器上安装 “插件”，请选择此选项。
   - **备用**：如果是在备用服务器上安装 “插件”，请选择此选项。
   - **其它**：如果既不是在首选服务器上也不是在备用服务器上安装 “插件”，请选择此选项。

5. 如果不是首选或备用主机，请输入 Directory Server 所在的 URL。
6. 输入 Directory Server 管理员的名称和密码，然后单击 “下一步”。

   将显示 “安装准备就绪”窗格，提供有关该 “插件”安装位置以及安装所需磁盘空间的信息。
7. 当一切就绪后，单击 “立即安装”按钮。

   “插件”的安装分两步完成：

   - 程序安装二进制文件时，显示带有进度条的 “安装”窗格。
   - 接下来，会显示 “组件配置”窗格。由于此步骤需要数分钟才能完成，所以会显示一个进度条。
8. 当两步都完成后，将显示下图所示提示信息。阅读该信息后，单击 “确定”关闭该对话框。

图 5-13 重新启动 Directory Server 提示信息

9. 如果要查看安装日志，请单击 “详细信息”按钮。

   - **在 Solaris 中**：安装日志被写入 `/var/sadm/install/logs/` 中
   - **在 Windows 中**：安装日志被写入 `%TEMP%` 目录，它是 `Local Settings` 文件夹的子目录，该文件夹在 `C:\Documents and Settings\Administrator` 下

注意 在某些 Windows 系统中 （如 Windows 2000 Advanced Server）， `Local Settings` 文件夹是隐藏文件夹。

要查看此文件夹和 `Temp` 子目录，请打开 “Windows 资源管理器”，然后从菜单条中选择 “工具” > “文件夹选项”。显示 “文件夹选项”对话框后，选择 “查看”选项卡，并启用 “显示隐藏的文件”选项。

---

10. 单击 “关闭” 退出安装程序。

    安装 Directory Server 插件后，可以安装在配置资源时配置的其它 “连接器” 和 / 或 Directory Server 插件 （第 4 章）：

    - 安装附加 Directory Server 插件：重新启动安装程序 （请参阅第 156 页的 “运行安装程序”），然后重复执行步骤 2 至步骤 9。

      因为 Identity Synchronization for Windows 要求您在部署中的每个 Directory Server 上安装 “插件”，因此可以不限次数地继续运行 “插件” 安装程序。

    - 安装 Directory Server Connector：转至第 159 页的 “安装 Directory Server Connector”。

    - 安装 Active Directory Connector：转至第 164 页的 “安装 Active Directory Connector”。

    - 安装 Windows NT Connector：转至第 168 页的 “安装 Windows NT Connector”。

11. 重新启动 Directory Server。

第 6 章

同步现有用户

Identity Synchronization for Windows 命令行实用程序提供 `idsync resync` 子命令，以引导包含现有用户的部署。此命令使用由管理员指定的匹配规则链接现有条目、在空目录中填充远程目录内容，或者在两个现有用户群体之间批量同步属性值（包括密码）。

本章说明如何使用 `idsync resync` 子命令为新安装的 Identity Synchronization for Windows 链接和同步现有用户。另外，本章还提供有关启动和停止同步和服务的说明。内容具体安排如下：

注意 在尝试链接和同步现有用户前，必须完成 “核心”和 “连接器”的安装。

有关 `idsync resync` 子命令的详细信息，请参阅附录 A，“使用 Identity Synchronization for Windows 命令行实用程序”。

表 6-1 基于现有用户群体概述了安装后所要执行的步骤：

表 6-1 基于现有用户群体的安装后步骤

用户所处环境		安装后步骤	
Windows	**Directory Server**	**同步现有用户**	**不同步现有用户**
否	否	无	无
否	是	通过运行 `idsync resync -o Sun -c` 在 Windows 中创建现有 Directory Server 用户。	无
是	否	通过运行 `idsync resync -c` 在 Directory Server 中创建现有 Windows 用户。	运行 `idsync resync -u` 以填充连接器用户条目本地高速缓存。
是	是	使用以下方法之一： • 通过运行 `idsync resync -f` <*filename*> 从 Active Directory 和 Directory Server 链接和同步用户。 • 通过运行 `idsync resync -f` <*filename*> `-k` 仅链接用户。 • 通过运行 `idsync resync -f` <*filename*> `-k` 仅链接用户，然后通过运行 `idsync resync -o Sun` 从 Directory Server 重新同步现有用户。	运行 `idsync resync -u` 以填充连接器用户条目本地高速缓存。

使用 idsync resync

本节讲述链接和同步过程，说明使用 idsync resync 子命令的正确语法，并阐述如何验证上述过程是否成功完成。内容具体安排如下：

重新同步用户

注意 在为您的部署启动同步之前，请检查服务器间的所有现有用户是否已同步。

可以使用 `idsync resync` 命令链接现有条目、创建用户和同步两个目录源中的用户属性。特别是，可以使用 `idsync resync` 命令：

- 将现有 Active Directory 或 Windows NT SAM 域用户填充到空 Directory Server 中
- 链接所有用户，然后同步两个现有目录源中的所有用户条目属性值 （密码除外）

注意 如果 Directory Server 和 Windows 中存在用户，则必须运行 `idsync resync -f` *<filename>* 命令链接和同步这些用户。

如果不想将现有用户同步到 Directory Server，则运行带有 `-u` 参数的 `idsync resync`，这样将只更新对象高速缓存，而不会将 Windows 条目同步到 Directory Server 中。

如果已经存在 Windows 用户，并且未运行 `idsync resync`，则对这些用户的更改可能会、也可能不会传播，而且在特定流动设置下，这些用户甚至可能在 Directory Server 中自动创建。必须再次运行 `idsync resync`，即使已经运行过该命令。

- 当两个目录源不同步时，同步用户条目。

- “预先准备好”Active Directory 和 Windows NT SAM 连接器对象高速缓存数据库。该数据库保留 Active Directory 或 Windows NT SAM 用户条目的隐式副本。

不能使用 `idsync resync` 命令同步密码 （但可以使 Directory Server 密码失效，从而在 Active Directory 环境中强制执行即时请求密码同步）。

链接用户

在 Active Directory 和 Directory Server 中填充用户并安装 Active Directory 和 Directory Server 连接器后 （在启动同步前），必须使用 `idsync resync` 命令确保*链接*了上述两个目录源中的所有现有用户。

何谓*链接*？ Identity Synchronization for Windows 通过存储以下唯一且不变的标识符使 Directory Server 和 on Windows 中的相同用户发生关联。

- 每个 Directory Server 用户条目的 `dspswuserlink` 属性
- 每个 Active Directory 用户的 `objectguid` 属性
- 每个 Windows NT SAM 用户的域名和 `RID` 的组合

存储此不可变的标识符可以使 Identity Synchronization for Windows 同步其它关键标识符，如 `uid` 和 `cn`。在以下情况下填充 `dspswuserlink` 属性：

- Identity Synchronization for Windows 在 Directory Server 中创建了新用户 （在从 Windows 或通过运行 `idsync resync -c` 同步新用户后）
- Identity Synchronization for Windows 在 Windows 上创建了新用户 （在从 Directory Server 或通过运行 `idsync resync -c -o Sun` 同步新用户后）
- 如本章所述，运行 `idsync resync -c -f` 链接已经存在于 Directory Server 和 Windows 中的用户。

要链接现有用户，必须提供在两个目录间匹配用户的规则。例如，要链接两个目录中的某个用户条目，这两个目录条目中的名和姓必须匹配。

与其说链接用户条目和解决数据冲突是一门学问，倒不如说是一种技巧。有多种原因可以说明为什么使用 `idsync resync` 子命令可能导致链接相对目录源中的两个用户失败，以及为什么该命令在很大程度上取决于这两个链接目录中的数据一致性。

使用 `idsync resync` 的一个策略是使用 `-n` 参数，这样可以在 *“安全模式”*下运行该操作，从而可以在不做实际更改的情况下，预览操作的效果。以安全模式运行可以使您对链接条件进行渐进式调整，直到获得一套最佳的用户匹配条件。

但是，应该注意在链接准确性和链接覆盖率之间找到一个平衡点。

例如，如果两个目录源中均包含员工 ID 或社会保障号，则应该先从只含有该号码的链接条件开始。您可能会觉得为了提高链接的准确性，还应在条件中包括姓氏属性。可是，这样一来，您就可能会因为数据中姓氏值不一致而无法链接本来只要 ID 匹配即可链接的条目。您不得不对链接失败的条目执行一次数据清理过程。

idsync resync 参数

idsync resync 命令接受以下参数：

表 6-2 idsync resync 用法

参数	含义
-f <*filename*>	使用 Identity Synchronization for Windows 提供的指定 XML 配置 文件之一在未链接的用户条目之间创建链接 （请参阅附录 B，“LinkUsers XML 文档范例”）
-k	仅在未链接用户间创建链接（不能创建用户或修改现有 用户）。必须将此参数与 -f 参数结合起来使用。
-a <*ldap-filter*>	指定一个 LDAP 过滤器来限制要同步的条目 此过滤器将被用作重新同步操作的源。 例如，如果指定 idsync resync -o Sun -a "usid=*"，则具有 uid 属性的所有 Directory Server 用户将被同步到 Active Directory。
-l <*sul-to-sync*>	指定要重新同步的各个 “同步用户列表” (SUL)。 **注意**：可指定多个 SUL ID 以重新同步多个 SUL，如果不指定任何 SUL ID，程序将重新同步您的所有 SUL。
-o (Sun | Windows)	指定重新同步操作的源 • **Sun**：将 Windows 条目的属性值设置为 Sun Java System Directory Server 目录源条目中的相应属性值。 • **Windows**：将 Sun Java System Directory Server 条目的属性值设置为 Windows 目录源条目中的相应属性值。 （*默认为 Windows*。）
-c	如果在目标处未找到相应用户，则自动创建用户条目 • 为 Active Directory 或 Windows NT 中创建的用户随机生成一个隐密的安全密码 • 为在 Directory Server 中创建的用户自动创建指定的密码值 ((PSWSYNC)***INVALID PASSWORD***)（除非指定了 -i 选项） **注意**：即使未配置按该方向创建， Identity Synchronization for Windows 也会尝试创建用户。例如，如果您未将 Identity Synchronization for Windows 配置为从 Windows 同步到 Sun （或相反），但指定了 -c 参数，则 Identity Synchronization for Windows 会尝试创建未找到的用户。

表 6-2 idsync resync 用法 *（续）*

参数	含义
`-i (ALL_USERS | NEW_USERS | NEW_LINKED_USERS)`	重设在 Sun 目录源中同步的用户条目的密码，从而对下次需要提供用户密码的用户强制执行当前域内的密码同步。 • **`ALL_USERS`**：对所有已同步的用户强制执行即时请求密码同步 • **`NEW_USERS`**：仅对新创建的用户强制执行即时请求密码同步 • **`NEW_LINKED_USERS`**：对所有新创建或新链接的用户强制执行即时请求密码同步 有关上述选项如何影响密码验证的详细信息，请参阅表 6-3。
`-u`	更新对象高速缓存。 该参数仅为 Windows 目录源更新用户条目的本地高速缓存，这将防止在 Directory Server 中创建已经存在的 Windows 用户。如果使用此参数，则不会将 Windows 用户条目与 Directory Server 用户条目同步。仅当同步源为 Windows 时，此参数才有效。
`-x`	删除所有与源条目不匹配的目标用户条目。
`-n`	在安全模式下运行，这样您便可以预览某个操作的效果而不进行实际更改。

表 6-3 idsync resync 会使 Directory Server 上的用户密码失效吗？

	用户在 Active Directory 和 Directory Server 上有一个链接的条目。	用户在 Active Directory 和 Directory Server 上有一个未链接的条目。	用户在 Active Directory 上有一个条目，但在 Directory Server 上没有条目。
`-i ALL_USERS`	是	是	是
`-i NEW_LINKED_USERS`	否	是	是
`-i NEW_USERS`	否	否	是
No `-i` value	否	否	否

表 6-4 提供的示例说明了不同参数联合使用的结果 （-h、 -p、 -D、 -w、 - 和 -s 为默认参数，为简便起见，将其省略）。

表 6-4 idsync resync 用法范例

参数	结果
`idsync resync`	显示一条 resync 用法说明。
`idsync resync -i ALL_USERS`	使所有用户的密码失效，以强制执行即时请求密码同步 （仅在 Active Directory 环境中有效）。 在混合环境 （含有 Active Directory 和 NT 两种域）中，必须明确列出 Active Directory SUL。
`idsync resync -c -i NEW_USERS`	创建在 Directory Server 中未找到的用户，并通过使其密码失效强制执行即时请求密码同步。使用此命令可以用现有 Windows 用户填充空 Directory Server 实例。
`idsync resync -c -l SUL_sales -l SUL_finance`	仅为 SUL_sales 和 SUL_finance SUL 在 Directory Server 上创建所有现有的 Active Directory 用户 （但不强制执行即时请求密码同步）。
`idsync resync -n`	在安全模式下运行，这样您便可以预览 resync 操作的效果而不必进行实际更改。
`idsync resync -o Sun -a "(sn=Smith)"`	同步 Windows 中姓氏 (sn) 为 Smith 的所有 Directory Server 用户。
`idsync resync -u`	仅更新 Windows 连接器的对象高速缓存，以防止在 Directory Server 中创建现有用户。实际上未同步任何用户。
`idsync resync -f link.cfg -k -i NEW_LINKED_USERS`	根据在 link.cfg 文件中指定的链接条件链接未链接的用户。 Identity Synchronization for Windows 不创建或修改用户，但新链接用户的 Directory Server 密码会被设置为 Active Directory 用户的密码。

警告 当使用 idsync resync 链接用户时，应对该操作使用已创建索引的属性。未创建索引的属性会影响性能。

如果 UserMatchingCriteria 集中有多个属性，并且至少有一个属性已创建索引，则性能或许是可接受的。但是，如果 UserMatchingCriteria 中不含已创建索引的属性，则由于目录较大的而使得性能不可接受。

查看中心日志中的结果

所有 `idsync resync` 操作的结果都记录在一个名为 `resync.log` 的特殊中心日志中。此日志将列出所有正确链接和同步的用户、链接失败的用户以及先前已链接的用户。

注意 某些预先存在的特殊 Active Directory 用户 （如管理员和临时用户）在此日志中可能显示为链接失败。

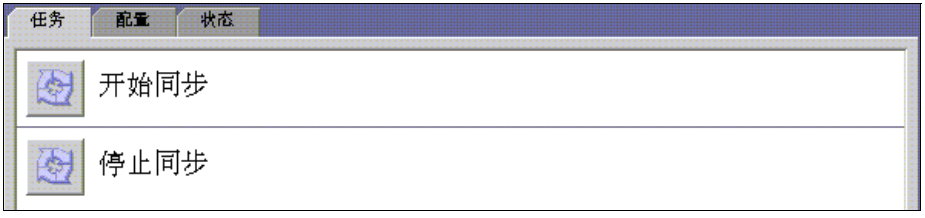
启动和停止同步

启动和停止同步 *不会*启动或停止单个的 java 进程、守护进程或服务。一旦开始同步，停止同步只能使操作暂停。当重新启动同步时，程序会从其停止处继续同步，不会丢失任何更改。

要启动或停止同步：

1. 在 “Sun Java System Server Console 的导航窗格中，选择 Identity Synchronization for Windows 实例。
2. 当显示 Identity Synchronization for Windows 窗格时，单击右上角的 “打开” 按钮。
3. 当出现提示时，输入配置密码。
4. 选择 “任务” 选项卡 （图 6-1）：

图 6-1 启动和停止同步



- 要启动同步，请单击 “开始同步”。
- 要停止同步，请单击 “停止同步”。

注意 也可以使用 `idsync startsync` 和 `idsync stopsync` 命令行实用程序启动和停止同步。有关详细说明，请参阅第 321 页的 “使用 startsync”和第 322 页的 “使用 stopsync”。

启动和停止服务

Identity Synchronization for Windows 和 Message Queue 在 Solaris 上作为*守护进程*安装，在 Windows 上作为*服务*安装。上述进程在引导系统时自动启动，但也可以执行以下步骤手动启动和停止它们：

- **在 Solaris 中**：从命令行，
  - 输入 `/etc/init.d/isw start` 启动所有 Identity Synchronization for Windows 进程。
  - 输入 `/etc/init.d/isw stop` 停止所有 Identity Synchronization for Windows 进程。
  - 输入 `/etc/init.d/imq start` 启动 Message Queue 代理程序。
  - 输入 `/etc/init.d/imq stop` 停止 Message Queue 代理程序。
- **在 Windows 中**：
  - 从 Windows 的 “开始”菜单：
    I. 选择 “开始” > “设置” > “控制面板” > “管理服务”。
    II. 出现 “管理服务”对话框时，双击 “服务”图标打开 “服务”对话框。
    III. 选择 Identity Synchronization for Windows，然后从菜单栏选择 “操作” > “启动”（或 “停止”）。对 iMQ Broker 重复执行上述步骤。
  - 从命令行输入 `net` 命令可以控制服务。

注意 在停止 Identity Synchronization for Windows 守护进程 / 服务 30 秒后，再重新启动它。连接器需要数秒时间才能完全关闭。

第 7 章

移植到 Identity Synchronization for Windows 1 2004Q3

本章介绍如何将系统从 Sun Java System Identity Synchronization for Windows 版本 1.0 移植到版本 1 2004Q3。

注意 Identity Synchronization for Windows 版本 1.0 会为您安装 Message Queue，*而 Identity Synchronization for Windows* 1 2004Q3 *则不然*。

有关安装说明，请参阅 Sun Java System Message Queue 产品文档。

这些信息被编排在以下各节中：

概述

从 Identity Synchronization for Windows 版本 1.0 （或版本 1.0 SP1）移植到 1 2004Q3 通过几个重要阶段来完成：

1. 准备要进行移植的 Identity Synchronization for Windows 版本 1.0 （或 1.0 SP1）安装。
2. 卸载 Identity Synchronization for Windows 版本 1.0 （或 1.0 SP1）。
3. 安装或升级相关产品。
4. 使用备份的配置和连接器状态安装 Identity Synchronization for Windows 1 2004Q3。

注意 在安装了 Identity Synchronization for Windows 版本 1.0 （或 1.0 SP1）的平台和体系结构上安装 Identity Synchronization for Windows 1 2004Q3。

移植准备

开始进行移植前，

- 熟悉 Sun Java System Identity Synchronization for Windows 版本 1 2004Q3 的新特性和功能。
- 阅读第 2 章，“准备安装”以获取规划移植过程适用的安装和配置信息。
- 将版本 1.0 部署和配置存档。确保记下所有自定义配置。
- 安排移植。因为移植过程至少需要四个小时，所以您可能希望将移植安排在正常工作时间之外。

如果在将系统从版本 1.0 移植至 1 2004Q3 的过程中用户输入密码或属性更改，Identity Synchronization for Windows 将按如下方式处理这些更改：

- **对于 Active Directory**：移植过程中在 Active Directory 上进行的任何密码更改都会在完成移植后通过 Directory Server 插件即时请求的方式进行同步。
- **对于 Directory Server**：移植过程中在 Directory Server 上进行的任何密码更改都不会被同步。但在完成移植后，可在 Identity Synchronization for Windows 1 2004Q3 日志中确定受影响的用户。（请参阅第 229 页的 “检查日志”。）
- **对于 Windows NT**：移植过程中在 NT 上进行的任何密码更改都不会被同步。

  但是，如果使用 `forcepwchg` 实用程序，则可确定受影响的用户并强制他们再次更改密码。（有关详细信息，请参阅第 194 页的 “在 Windows NT 上强制执行密码更改”和第 229 页的 “检查日志”。）
- 移植过程中 （在任意目录源）进行的所有其它属性更改将在完成移植后进行同步。

准备移植

您将使用以下一个或多个实用程序从版本 1.0 移植至版本 1 2004Q3：

- **`export10cnf`**：独立的实用程序，利用它可从 Identity Synchronization for Windows 1.0 配置创建导出配置文件。（有关详细信息，请参阅第 186 页的 “导出版本 1.0 配置”。）

  导出的 XML 文档将包含目录部署的拓扑以及配置 Identity Synchronization for Windows 版本 1 2004Q3 安装所需的足够信息。
- **`checktopics`**：该实用程序用于检查 1.0 安装中的 Message Queue 同步主题，并确定队列中是否仍有未传送的消息。

  停止 1.0 同步后更新内容仍保留在 Message Queue 中。继续进行移植前，必须确保 Message Queue 中不存在任何更新。（有关详细信息，请参阅第 192 页的 “检查未传送的消息”。）
- **`forcepwchg`**：一种 Windows NT 工具，利用它可确定在移植过程中更改了密码的用户，并强制他们在版本 1 2004Q3 系统就绪时再次更改密码。（移植过程中不捕获在 Windows NT 上进行的密码更改。） （有关详细信息，请参阅第 194 页的 “在 Windows NT 上强制执行密码更改”。）

注意 这些实用程序简化了 Identity Synchronization for Windows 版本 1.0 到 1 2004Q3 的移植。移植将在部署 Identity Synchronization for Windows 1.0 的环境中执行。因此，仅可从 Solaris/SPARC 和 Windows 软件包获取这些实用程序。

可在安装 `migration` 目录下找到移植实用程序；不需要其它安装步骤。

导出版本 1.0 配置

安装连接器前，可使用 `export10cnf` 实用程序将现有 1.0 版本配置文件导出为 XML 文件，然后使用 `idsync importcnf` 命令快速而准确地将该文件导入 1 2004Q3 系统。

提示 虽然使用 Identity Synchronization for Windows 控制台可以手动重新输入 1.0 配置，但是强烈建议您使用 `export10cnf` 实用程序。如果决定不使用 `export10cnf`，则将无法保留连接器的状态。

导出版本 1.0 配置具有以下优点：

- 去除了从管理控制台执行多数初始配置的过程。
- 可保证在版本 1 2004Q3 中分配的连接器 ID 与版本 1.0 中使用的连接器 ID 匹配，这样就极大地简化了保留现有连接器状态 （这些状态可直接在版本 1 2004Q3 部署中使用）的任务。

  （通常，可对 `persist` 和 `etc` 目录进行备份，并在以后恢复它们，而不必担心底层目录结构。）

可在安装 `migration` 目录下找到 `export10cnf` 实用程序，不需要其它安装步骤。

使用 export10cnf 实用程序

要将 Identity Synchronization for Windows 配置导出为 XML 文件，请从 `migration` 目录执行 `export10cnf`，如下所示：

- 打开 “终端”窗口并键入：

```
java -jar export10cnf.jar -h <hostname> -p <port> -D <bind DN>
-w <bind password> -s <rootsuffix> -q <configuration password> -Z
-P <cert-db-path> -m <secmod-db-path> -f <filename>
```

例如：

```
java -jar export10cnf.jar -D "cn=dirmanager" -w - -q - -s
"dc=example,dc=com" -f exported-configuration
```

export10cnf 实用程序与 Identity Synchronization for Windows 命令行实用程序共用相同的公用参数（请参阅 第 306 页的 “公用参数”）。唯一专用于 export10cnf 的选项为 -f *<filename>*。如果操作成功，则实用程序会将当前配置导出到 -f 选项的参数中所指定的文件。

插入明文密码

export10cnf 实用程序不从版本 1.0 配置导出明文密码（出于安全原因）。而是由实用程序在 cleartextPassword 字段的合适位置插入空字符串。例如，

```
<Credentials
        userName="cn=iswservice,cn=users,dc=example,dc=com"
        cleartextPassword=""/>
        <!-- INSERT PASSWORD BETWEEN THE DOUBLE QUOTES IN THE ABOVE FIELD
-->
```

必须为导出的配置文件的每个 cleartextPassword 字段（在双引号内）手动输入密码，然后才能将文件导入 *Identity Synchronization for Windows 1 2004Q3*。（importcnf 验证可避免导入有空密码值的配置文件。）

例如，

```
<Credentials
        userName="cn=iswservice,cn=users,dc=example,dc=com"
        cleartextPassword="mySecretPassword"/>
        <!-- INSERT PASSWORD BETWEEN THE DOUBLE QUOTES IN THE ABOVE
FIELD -->
```

导出配置文件示例

第 188 页的代码示例 7-1 包含一个示例导出配置文件。

在此文件中，

- ad-host.example.com 指 Active Directory 域控制器。
- ds-host.example.com 指运行 Sun Java System Directory Server 的主机。

代码示例 7-1 导出配置文件示例

```
<?xml version="1.0" encoding="UTF-8"?>

<ActiveConfiguration>
  <SunDirectorySource
    parent.attr="DirectorySource"
    onDemandSSLOption="true"
    maxConnections="5"
    displayName="dc=example,dc=com"
    resyncInterval="1000">
    <SynchronizationHost
      hostOrderOfSignificance="1"
      hostname="ds-host.example.com"
      port="389"
      portSSLOption="true"
      securePort="636">
      <Credentials
        userName="uid=PSWConnector,dc=example,dc=com"/>
    </SynchronizationHost>
<SyncScopeDefinitionSet
      index="0"
      location="ou=people,dc=example,dc=com"
      filter=""
      creationExpression="cn=%cn%,ou=people,dc=example,dc=com"
      sulid="SUL"/>
  </SunDirectorySource>
<ActiveDirectorySource
parent.attr="DirectorySource"
    displayName="example.com"
    resyncInterval="1000">
```

```
<SyncScopeDefinitionSet
      index="0"
      location="cn=users,dc=example,dc=com"
      filter=""
      creationExpression="cn=%cn%,cn=users,dc=example,dc=com"
      sulid="SUL"/>
</ActiveDirectorySource>
<ActiveDirectoryGlobals
    flowInboundCreates="true"
    flowInboundModifies="true"
    flowOutboundCreates="true"
flowOutboundModifies="true">
    <AttributeDescription
      parent.attr="CreationAttribute"
name="samaccountname"
syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
<AttributeMap>
      <AttributeDescription
        parent.attr="WindowsAttribute"
        name="samaccountname"
        syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
      <AttributeDescription
        parent.attr="SunAttribute"
        name="uid"
        syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
    </AttributeMap>
<AttributeDescription
      parent.attr="SignificantAttribute"
      name="description"
      syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
<AttributeMap>
      <AttributeDescription
        parent.attr="SunAttribute"
        name="sn"
        syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
<AttributeDescription
        parent.attr="WindowsAttribute"
        name="sn"
        syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
    </AttributeMap>
```

```
<SynchronizationHost
      hostOrderOfSignificance="1"
      hostname="ad-host.example.com"
      port="389"
      portSSLOption="true"
      securePort="636">
      <Credentials
        userName="cn=iswservice,cn=users,dc=example,dc=com"
        cleartextPassword=""/>
        <!-- INSERT PASSWORD BETWEEN THE DOUBLE QUOTES IN THE ABOVE FIELD -->
    </SynchronizationHost>
<AttributeDescription
      parent.attr="CreationAttribute"
      name="cn"
      syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
    <TopologyHost
      parent.attr="SchemaLocation"
hostname="ad-host.example.com"
      port="3268"
      portSSLOption="true"
      securePort="3269">
      <Credentials
        parent.attr="Credentials"
        userName="cn=iswservice,cn=users,dc=example,dc=com"
        cleartextPassword=""/>
        <!-- INSERT PASSWORD BETWEEN THE DOUBLE QUOTES IN THE ABOVE FIELD -->
    </TopologyHost>
    <TopologyHost
      parent.attr="HostsTopologyConfiguration"
      hostname="ad-host.example.com"
      port="3268"
      portSSLOption="true"
      securePort="3269">
<Credentials
        parent.attr="Credentials"
        userName="cn=iswservice,cn=users,dc=example,dc=com"
        cleartextPassword=""/>
        <!-- INSERT PASSWORD BETWEEN THE DOUBLE QUOTES IN THE ABOVE FIELD -->
    </TopologyHost>
<AttributeMap>
      <AttributeDescription
        parent.attr="SunAttribute"
        name="cn"
        syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
```

```
 <AttributeDescription
        parent.attr="WindowsAttribute"
        name="cn"
        syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
    </AttributeMap>
<AttributeMap>
      <AttributeDescription
        parent.attr="SunAttribute"
        name="description"
        syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
<AttributeDescription
        parent.attr="WindowsAttribute"
name="description"
        syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
    </AttributeMap>
</ActiveDirectoryGlobals>
<SunDirectoryGlobals
    userObjectClass="inetorgperson"
    flowInboundCreates="true"
    flowInboundModifies="true"
    flowOutboundCreates="true"
    flowOutboundModifies="true">
<TopologyHost
      parent.attr="SchemaLocation"
      hostname="ds-host.example.com"
      port="389"
      portSSLOption="false"
      securePort="636">
      <Credentials
        parent.attr="Credentials"
        userName="cn=directory manager"
        cleartextPassword=""/>
        <!-- INSERT PASSWORD BETWEEN THE DOUBLE QUOTES IN THE ABOVE FIELD -->
    </TopologyHost>
   <TopologyHost
      parent.attr="HostsTopologyConfiguration"
      hostname="ds-host.example.com"
      port="389"
      portSSLOption="false"
      securePort="636"><Credentials
        parent.attr="Credentials"
        userName="cn=directory manager"
        cleartextPassword=""/>
        <!-- INSERT PASSWORD BETWEEN THE DOUBLE QUOTES IN THE ABOVE FIELD -->
    </TopologyHost>
```

```
<AttributeDescription
      parent.attr="SignificantAttribute"
      name="description"
      syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
<AttributeDescription
      parent.attr="CreationAttribute"
      name="sn"
      syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
    <AttributeDescription
      parent.attr="CreationAttribute"
      name="cn"
      syntax="1.3.6.1.4.1.1466.115.121.1.15"/>
  </SunDirectoryGlobals>
</ActiveConfiguration>
```

配置导出完成后， `export10cnf` 会报告操作结果。如果操作失败，会显示带有错误标识符的相应错误消息。

检查未传送的消息

Identity Synchronization for Windows 1.0 到 1 2004Q3 的移植过程通过保留现有部署中的连接器状态而使系统停机时间最短。但是，这些状态仅反映 Message Queue 接收并确认的上一更改，所以无法获知消息是否已实际传送并应用到目标连接器。

只要 Message Queue 保持不变，此行为就不会出现问题；但在移植过程中 （即安装 Message Queue 3.5 SP1 时）会丢失 Message Queue 中的所有消息。

继续进行移植前，必须检验是否现有 Message Queue 的同步主题中没有任何未传送的消息。使用 Identity Synchronization for Windows `checktopics` 实用程序可以检验是否所有同步主题均为空 （且系统处于静止状态）。

使用 checktopics 实用程序

checktopics 实用程序位于 Solaris/SPARC 和 Windows Identity Synchronization for Windows 1 2004Q3 软件包的 migration 目录下。

注意 运行 checktopics 的唯一前提条件是有一台合适的 “Java 虚拟机”（版本 1.4.2_04 或更高）。

当运行 checktopics 实用程序时，它将连接到配置目录，该目录中包含有关同步用户列表 (SUL) 及 Message Queue 中使用的当前同步主题名的信息。另外，当运行 checktopics 时，它将查询 Message Queue，以确定每个活动同步主题有多少未解决的消息，然后为您显示此信息。

要执行 checktopics 命令行实用程序：

a. 打开 “终端”窗口，并使用 **cd** 进入 migration 目录。

b. 出现命令提示符后，键入以下子命令：

```
java -jar checktopics.jar -h <hostname> -p <port> -D <bind_DN> -w
<bind_password> -s <root_suffix> -q <configuration_password> -Z
```

例如：

```
java -jar checktopics.jar -D "cn=directory manager" -w - -s
"dc=example,dc=com" -q -
```

注意

- 有关 checktopics 参数的详细信息，请查看第 306 页的 “公用参数”。
- 有关使用 checktopics 的详细信息，请参阅第 192 页的 “检查未传送的消息”。

运行 checktopics 后，请查看终端上的消息：

- 如果操作成功，终端上会显示一条消息，说明日志中没有未解决的消息。
- 如果操作失败，会显示带有错误标识符的相应错误消息。

清除消息

如果任何一个活动同步主题有未解决的消息，可按以下步骤清除这些消息：

1. 重新启动同步。
2. 请等待，直到这些消息被应用到目标连接器。
3. 停止同步。
4. 重新运行 checktopics。

在 Windows NT 上强制执行密码更改

在 Windows NT 上，移植过程中不对密码更改进行监控且不捕获新密码值。因此，无法在完成移植后确定新密码值。

移植至 1 2004Q3 后，并不是要求所有用户都更改密码，而是可使用 forcepwchg 命令行实用程序要求所有在移植过程中更改了密码的用户更改密码。

注意 仅可从 Windows 软件包获取 forcepwchg 实用程序。

可在 Windows 的 migration 目录下找到 forcepwchg 实用程序。从该目录直接执行 forcepwchg，无需执行其它安装步骤。

必须在安装了 NT 组件 （连接器、 Change Detector DLL 及 Password Filter DLL）的 “主域控制器” (PDC) 主机上运行 forcepwchg - 不能远程运行 forcepwchg 。

forcepwchg 实用程序还将打印出它尝试移植的帐户名 （每行一个名称）。如果移植过程中出错，则该错误会在移植最后一个打印出来的用户帐户时出现。

移植系统

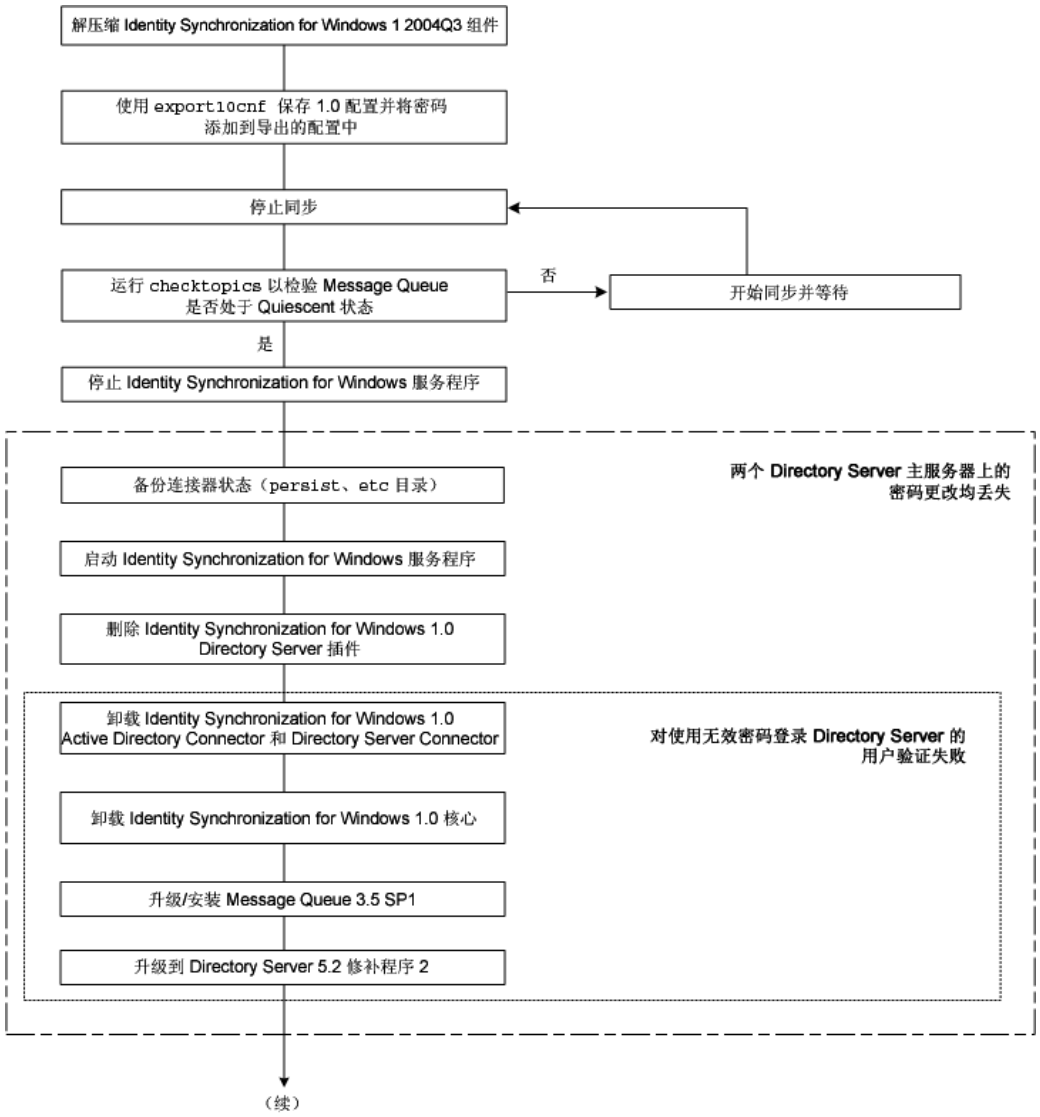
本节说明如何将单主机部署移植至版本 1 2004Q3。在单主机部署中，所有 Identity Synchronization for Windows 组件均安装在单个主机 （Windows 2000 Server、Solaris 版本 8 或 9 或 SPARC）上，具体如下：

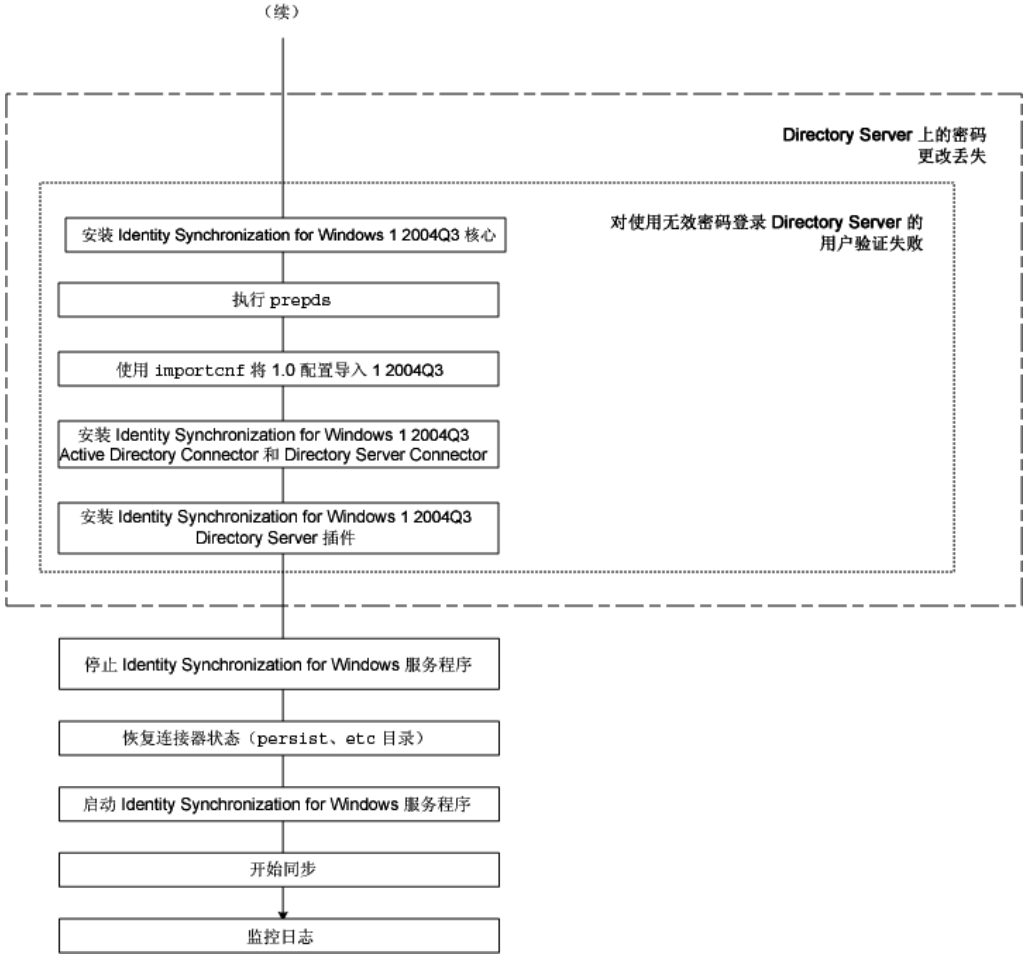
- Directory Server （一个实例）
- 核心 （Message Queue、中心记录器、系统管理器和控制台）
- Active Directory Connector
- Directory Server Connector
- Directory Server 插件

注意 如果使用 Solaris 作为安装主机，则仅在进行同步时才需要装有 Active Directory 的 Windows 2000 计算机。（将不在 Windows 2000 机器上安装任何组件。）

下图说明移植过程，并可充当随后移植说明的补充清单。

图 7-1 移植单主机部署




（续）
Directory Server 上的密码更改丢失
对使用无效密码登录 Directory Server 的用户验证失败
安装 Identity Synchronization for Windows 1 2004Q3 核心
执行 prepds
使用 importcnf 将 1.0 配置导入 1 2004Q3
安装 Identity Synchronization for Windows 1 2004Q3 Active Directory Connector 和 Directory Server Connector
安装 Identity Synchronization for Windows 1 2004Q3 Directory Server 插件
停止 Identity Synchronization for Windows 服务程序
恢复连接器状态（persist、etc 目录）
启动 Identity Synchronization for Windows 服务程序
开始同步
监控日志

准备移植

按以下步骤准备从 Identity Synchronization for Windows 版本 1.0 移植至版本 1 2004Q3：

1. 出现命令提示符后：
   - **在 Solaris 或 SPARC 中：**键入 **`uncompress -c <`*filename*`> | tar xf -`**
   - **在 Windows 中：**键入 **`%JAVA_HOME%\bin\jar -xf <`*filename*`>**（或使用任何用于 Windows 的压缩归档程序，如 WinZip®）。

   解压缩二进制文件后，可看到包含所需移植工具的以下子目录：
   - `installer/`
   - `lib/`
   - `migration/`

Solaris	Windows
export10cnf.jar	export10cnf.jar
—	forcepwchg.exe
checktopics.jar	checktopics.jar

2. 将版本 1.0 配置设置导出到 XML 文件。如第 186 页的 “使用 export10cnf 实用程序”所述，从 `migration` 目录执行 `export10cnf`。例如：

   ```
   java -jar export10cnf.jar -D "cn=directory manager" -w - -s
   "dc=example,dc=com" -q - -f export.cfg
   ```

3. 将密码添加到导出的 XML 文件。

   在导出的配置文件的每个 `cleartextPassword` 字段中的双引号内输入密码（请参阅第 187 页的 “插入明文密码”）。

4. 按第 180 页的 “启动和停止同步”中所述方法停止同步。

5. 检验系统是否处于静止状态。如第 193 页的 “使用 checktopics 实用程序”所述，从 `migration` 目录执行 `checktopics`。

   例如：

   ```
   java -jar checktopics.jar -D "cn=directory manager" -w - -s
   "dc=example,dc=com" -q -
   ```

6. 按第 181 页的 “启动和停止服务”中所述方法停止 Identity Synchronization for Windows 服务 （守护进程）。

注意	此时不要停止 Sun ONE Message Queue 服务。

7. *仅在 Windows NT 上* - 停止 Sun One NT ChangeDetector Service。
可从命令行键入以下内容停止服务

```
net stop "Sun One NT ChangeDetector Service"
```

8. *仅在 Windows NT 上* - 按如下步骤保存 NT ChangeDetector Service 计数器：
   a. 通过执行 `regedt32.exe` 打开 “注册表编辑器”。
   b. 选择 `HKEY_LOCAL_MACHINE` 窗口。
   c. 导航到 `SOFTWARE\Sun Microsystems\PSW\1.0` 节点。
   d. 保存以下注册表值：
      - `HighestChangeNumber`
      - `LastProcessedSecLogRecordNumber`
      - `LastProcessedSecLogTimeStamp`
      - `QueueSize`
9. 通过从现有 1.0 安装树备份 `persist` 和 `etc` 目录来保存连接器状态。
   - **在 Solaris 中**：键入 **`cd <`*serverroot*`>/isw-<`*hostname*`>`**
     `tar cf /var/tmp/connector-state.tar persist etc`
   - **在 Windows 中**：键入 **`cd <`*serverroot*`>\isw-<`*hostname*`>`**
     `zip -r C:\WINNT\Temp\connector-state.zip persist etc`
     `%JAVA_HOME%\bin\jar -cfM %TEMP%\connector-state.jar persist etc`
     （或使用任何用于 Windows 的压缩归档程序，如 WinZip）
10. 启动 Identity Synchronization for Windows 服务 （请参阅第 181 页）。

注意	因为并未停止 Sun ONE Message Queue 服务，所以无需启动它。

卸载 Identity Synchronization for Windows

注意 如果其它应用程序 （非 Identity Synchronization for Windows 1.0）未注册使用 `SUNWjss` 软件包， Identity Synchronization for Windows 1.0 卸载程序会将该软件包删除。特别是在 Solaris 机器上安装了压缩版的 Directory Server 5.2.2 时，更会出现这种情况，此时卸载程序会从 `/usr/share/lib/mps/secv1` 删除 `jss3.jar` 文件。

如果在移植到 Identity Synchronization for Windows 11 2004Q3 时遇到这种情况，安装程序会报告缺少必需文件，并将文件名记录到安装日志中。出现这种情况时，必须重新安装必需的补丁程序（请参阅第 54 页的 “Sun Java System 软件要求”）并重新启动安装程序。

完成准备步骤后，即可开始卸载 Identity Synchronization for Windows 版本 1.0（或 1.0 SP1），具体如下：

1. 手动卸载 Directory Server 插件，然后重新启动每个安装了 “插件”的 Directory Server。
2. 在每个安装有 “插件”的 Directory Server 上执行以下步骤：
   a. 从 Directory Server 中删除以下条目：

      ```
      cn=config,cn=pswsync,cn=plugins,cn=config
      cn=pswsync,cn=plugins,cn=config
      ```

      例如：

      `ldapdelete -D "cn=directory manager" -w - -p <port> -c cn=config, cn=pswsync,cn=plugins,cn=config cn=pswsync,cn=plugins,cn=config`

   b. 重新启动 Directory Server。
      - **在 Solaris 中**：键入 **`<serverroot>/slapd-<hostname>/restart-slapd`**
      - **在 Windows 中**：键入 **`<serverroot>\slapd-<hostname>\restart-slapd.bat`**

   c. 从系统中删除 “插件”二进制文件。
      - **在 Solaris 中**：键入 **`rm <serverroot>/lib/psw-plugin.so`** **`rm <serverroot>/lib/64/psw-plugin.so`**
      - **在 Windows 中**：键入 **`del <serverroot>\lib\psw-plugin.dll`**

3. 将目录更改 (**cd**) 为 **<***server_root***>\isw-<***hostname***>**，然后使用 Identity Synchronization for Windows 1.0 卸载程序卸载版本 1.0/1.0 SP1 “连接器”和“核心”组件。

   注意 卸载 “核心”组件前必须先卸载 “连接器”。

   - **在 Solaris 或 SPARC 中**：键入 **./runUninstaller.sh**
   - **在 Windows 中**：键入 **\runUninstaller.bat**

4. 按以下步骤从产品注册表文件中删除与 Identity Synchronization for Windows 相关的条目：

   a. 备份文件副本 （位于）：

      - **在 Solaris 中**：`/var/sadm/install/productregistry`
      - **在 Windows 中**：`C:\WINNT\System32\productregistry`

   b. 要从产品注册表文件中删除与 Identity Synchronization for Windows 相关的条目，请按 “从 Solaris 手动卸载 1.0 核心和实例”的步骤 6 中的说明操作。

5. *仅在 Windows 中* - 卸载 “核心”后，重新启动计算机。

   注意 如果卸载因某种原因失败，则必须手动卸载 Identity Synchronization for Windows 组件。第 205 页的 “如果 1.0 卸载失败应采取何种措施”中提供了说明。

6. *仅在 Windows 中* - 检验 Identity Synchronization for Windows 是否正在运行。如有必要，可从命令行键入以下内容停止服务

   ```
   net stop "Sun ONE Identity Synchronization for Windows"
   ```

   如果在完成卸载后此服务继续运行，会导致共享冲突，从而阻止您删除该实例目录。

7. 删除 Identity Synchronization for Windows 实例目录 (`isw-`*<hostname>*)。

安装或升级相关产品

按以下步骤升级 Java Runtime Environment、安装 Message Queue 和升级 Directory Server：

1. 在每台安装了 Identity Synchronization for Windows 组件的主机 （Windows NT 除外）上升级 Java 2 Runtime Environment （或 Java 2 SDK）。（所需的最低版本为 1.4.2_04。）

   - **Java 2 SDK**：http://java.sun.com/j2se/1.4.2/install.html
   - **Java 2 Runtime Environment**：
     http://java.sun.com/j2se/1.4.2/jre/install.html

2. 使用 《*Sun Java System Message Queue 3.5 SP1 Installation Guide*》中提供的说明安装 Message Queue 3.5 SP1。

3. 使用 《*Sun Java System Directory Server 5 2004Q2 Installation and Migration Guide*》中提供的说明，将 Directory Server 升级至版本 5.2 SP2，可从以下网址获得该指南：

   http://docs.sun.com/db/coll/DirectoryServer_04q2

   Directory Server 升级将保留当前的 Directory Server 配置和数据库。

安装 Identity Synchronization for Windows 1 2004Q3

按照以下步骤安装 Identity Synchronization for Windows 1 2004Q3 组件：

1. 安装 Identity Synchronization for Windows 1 2004Q3 核心。（请参阅第 85 页的 “安装核心”）
2. 按如下步骤对 Directory Server 执行 `idsync prepds`，以更新模式。
   - **在 Solaris 中**：键入 **`cd /opt/SUNWisw/bin`**
     然后键入：**`idsync prepds <`*arguments*`>`**
   - **在 Windows 中**：键入 **`cd \<`*serverroot*`>\isw-<`*hostname*`>\bin`**
     然后键入：**`idsync prepds <`*arguments*`>`**

   有关 `idsync prepds` 的详细信息，请参阅附录 A，“使用 Identity Synchronization for Windows 命令行实用程序”。
3. 通过键入以下内容导入版本 1.0 配置 XML 文件

   `idsync importcnf <`*arguments*`>`

   注意 如果该程序在输入配置文件中检测到错误，则会出现错误。Identity Synchronization for Windows 会中止 `importcnf` 进程，并提供必要的信息以更正错误。

   有关使用 `idsync importcnf` 的详细信息，请参阅附录 A 中的 “使用 importcnf”。
4. 安装 Identity Synchronization for Windows 1 2004Q3 连接器 （请参阅第 158 页的 “安装连接器”）。
5. 安装 “Identity Synchronization for Windows 1 2004Q3 Directory Server 插件”（第 169 页的 “安装 Directory Server 插件”）。
6. 按第 181 页的 “启动和停止服务”中所述方法停止 Identity Synchronization for Windows 服务 （守护进程）。
7. *仅在 Windows NT 上* — 停止 Sun Java™ System NT Change Detector 服务。可从命令行键入以下内容停止服务

   `net stop "Sun Java(TM) System NT Change Detector"`
8. *仅在 Windows NT 上* — 恢复 NT ChangeDetector Service 计数器：
   a. 通过执行 `regedt32.exe` 打开 “注册表编辑器”。

b. 选择 HKEY_LOCAL_MACHINE 窗口。

c. 导航到 SOFTWARE\Sun Microsystems\Sun Java(TM) System Identity Synchronization for Windows\1.1 节点。

d. 双击下面的每个条目以恢复其值 （在卸载版本 1.0 前已保存的值）：

- HighestChangeNumber
- LastProcessedSecLogRecordNumber
- LastProcessedSecLogTimeStamp
- QueueSize

9. *仅在 Windows NT 上* — 启动 Sun Java™ System NT Change Detector 服务。可从命令行键入以下内容启动该服务

```
net start "Sun Java(TM) System NT Change Detector"
```

10. 从实例目录删除 1 2004Q3 persist 和 etc 目录 （及其全部内容），并恢复在第 198 页的 “准备移植”中备份的版本 1.0 （或 1.0 SP1） persist 和 etc 目录。

- 在 **Solaris** 中：类型

```
cd /var/opt/SUNWisw
rm -rf etc persist
tar xf /var/tmp/connector-state.tar
```

- 在 **Windows** 中：类型

```
cd <serverroot>\isw-<hostname>
rd /s etc persist
%JAVA_HOME%\bin\jar -xf %TEMP%\connector-state.jar
```

（或使用任何用于 Windows 的压缩归档程序，如 WinZip）

11. 启动 Identity Synchronization for Windows 服务 （请参阅第 181 页）。

12. 按第 180 页的 “启动和停止同步”中所述方法启动同步。

13. 检查中心审计日志以验证没有警告消息。

注意 如果自定义了版本 1.0 日志设置，则必须手动将这些自定义设置应用到版本 1 2004Q3 安装。使用 Identity Synchronization for Windows 控制台来配置版本 1 2004Q3 日志设置。

如果 1.0 卸载失败应采取何种措施

如果 1 2004Q3 版本安装程序找到 1.0 版本的残存组件，则 1 2004Q3 安装将失败。因此，在安装版本 1 2004Q3 前，应检验是否从系统中彻底删除了所有 1.0 版本的组件。

如果卸载程序未卸载所有版本 1.0/1.0 SP1 组件，则必须手动清除 Identity Synchronization for Windows 产品注册表和 Solaris 软件包。

以下三个小节中提供了手动卸载 Identity Synchronization for Windows 版本 1.0 的详细说明：

- 第 206 页的 “从 Solaris 手动卸载 1.0 核心和实例”
- 第 212 页的 “从 Windows 2000 手动卸载 1.0 核心和实例”
- 第 218 页的 “从 Windows NT 手动卸载 1.0 实例”

注意 本节中提供的说明仅适用于 Identity Synchronization for Windows *版本 1.0* 的卸载。

除非 Identity Synchronization for Windows 卸载程序失败，否则*不要*使用以下各节中介绍的手动卸载过程。

从 Solaris 手动卸载 1.0 核心和实例

按照本节介绍的说明从 Solaris 机器手动卸载 “核心”。

注意 在本节中，将采用下列格式描述 Identity Synchronization for Windows 位置：

<serverroot>/isw-*<hostname>*

其中，*<serverroot>* 表示 Identity Synchronization for Windows 安装位置的父目录。

例如，如果在 /var/Sun/mps/isw-*<example>* 下安装 Identity Synchronization for Windows，*<serverroot>* 将是 /var/Sun/mps。

1. 通过在终端窗口中键入 **/etc/init.d/isw stop** 停止所有 Identity Synchronization for Windows Java 进程。

   如果上述命令不停止所有 Java 进程，请键入以下内容：

   /usr/ucb/ps -gauxwww | grep java

   kill -s SIGTERM <*上述命令的进程 ID*>

2. 按如下步骤停止 Message Queue：

   a. 在提示符后键入下列命令以停止 Message Queue 代理程序：

      /etc/init.d/imq stop

   b. 要停止任何仍在进行的 imq 进程，请键入：

      *** ps -ef | grep imqbroker**

      *** kill -s SIGTERM <*上述命令的进程 ID*>**

   c. 使用以下方法之一卸载代理程序软件包和目录：

      - 使用 Message Queue 代理程序卸载脚本 （位于安装 “核心”的主机的 Identity Synchronization for Windows 实例目录下）卸载代理程序。键入以下内容：

        /<*serverroot*>/isw-<*hostname*>/imq_uninstall

- 按如下步骤手动卸载软件包和目录：

  使用 pkgrm: 命令删除以下软件包：

SUNWaclg	SUNWiqum	SUNWiqjx
SUNWiqlen	SUNWxsrt	SUNWiqu
SUNWjaf	SUNWiqfs	SUNWjhrt
SUNWiqdoc	SUNWiquc	SUNWiqsup
SUNWiqr	SUNWjmail	

  使用 rm -rf 命令删除以下目录：

  ```
  rm -rf /etc/imq
  rm -rf /var/imq
  rm -rf /usr/bin/imq*
  ```

3. 要删除 Identity Synchronization for Windows 1.0 Solaris 软件包，请为表 7-1 中列出的每个软件包运行 pkgrm <*packageName*>。（例如，**pkgrm SUNWidscm SUNWidscn SUNWidscr SUNWidsct SUNWidsoc**）

表 7-1 要删除的 Solaris 软件包

软件包名称	说明
SUNWidscm	Sun ONE Directory Server Identity Synchronization 的“核心”组件和“连接器”软件包。
SUNWidscn	Sun ONE Directory Server Identity Synchronization 的“控制台”帮助文件软件包。
SUNWidscr	Sun ONE Directory Server Identity Synchronization 的核心组件软件包。
SUNWidsct	Sun ONE Directory Server Identity Synchronization 的连接器软件包。
SUNWidsoc	Sun ONE Directory Server Identity Synchronization 的对象高速缓存软件包。

要检验是否删除了所有软件包，请键入：

```
pkginfo | grep -i "Identity Synchronization"
```

注意 如果由于相关性而仍存在现有软件包，请再次运行 `pkgrm <packageName>` 命令。

4. 按如下步骤删除 Director Server 插件：
   a. 打开 “Directory Server 控制台”，然后选择 “配置”选项卡。
   b. 在左侧窗格中，展开 “插件”节点，然后选择 pswsync 节点。
   c. 在右侧窗格中，取消选中 “启用插件”复选框。
   d. 单击 “保存”保存所做更改。
   e. 在 “Directory Server 控制台”中，从 “配置目录”找到并删除以下条目：

      `cn=pswsync,cn=plugins,cn=config`

   f. 停止 Directory Server。
   g. 要删除 “插件”二进制文件，请键入

      `rm -f /<serverroot>/lib/psw-plugin.so`

   h. 重新启动 Directory Server。
5. 备份 （复制并重命名）位于 `/var/sadm/install/productregistry` 下的当前 `productregistry` 文件。
6. 手动编辑 `/var/sadm/install/` 下的 `productregistry` 文件，从中删除下列条目 （*如果存在*）：

注意
- 为获得最佳效果，请使用 XML 编辑器。或者，可使用标准文本编辑器。
- 以下组件中的某些组件可能不包括在文件中。
- 必须删除开始标记 (`<compid>`)、结束标记 (`<\compid>`) 及两个标记之间的所有内容。在以下列表中，用省略号表示这些标记中的内容，包括任何其它文本和 / 或标记。（请参阅第 209 页的示例。）

- `<compid>Identity Synchronization for Windows .. . </compid>`
- `<compid>Core .. . </compid>`
- `<compid>unistaller .. . </compid>`

- <compid>wpsyncwatchdog .. . </compid>
- <compid>setenv .. . </compid>
- <compid>Create DIT .. . </compid>
- <compid>Extend Schema .. . </compid>
- <compid>resources .. . </compid>
- <compid>CoreComponents .. . </compid>
- <compid>Connector .. . </compid>
- <compid>DSConnector .. . </compid>
- <compid>Directory Server Plugin .. . </compid>
- <compid>DSSubcomponents .. . </compid>
- <compid>ObjectCache .. . </compid>
- <compid>ObjectCacheDLLs .. . </compid>
- <compid>SUNWidscr .. . </compid>
- <compid>SUNWidscm .. . </compid>
- <compid>SUNWidsct .. . </compid>
- <compid>SUNWidscn .. . </compid>
- <compid>SUNWidsoc .. . </compid>
- <compid>ADConnector .. . </compid>

以下为 <compid> 标记示例。删除 <compid>、 </compid> 以及两者之间的所有文本和标记。

```
<compid>Identity Synchronization for Windows
    <compversion>1.0
          <uniquename>Identity Synchronization for Windows</uniquename>
           <compinstance>1
                    <children>
                        <compref>ADConnector
                            <instance>1
                                <version>1.0</version>
                            </instance>
                        </compref>
                        <compref>DSSubcomponents
                        . . .

        </compinstance>
    </compversion>
</compid>
```

7. 删除以下 Identity Synchronization for Windows 目录和文件：

   a. 从安装位置键入

      rm -rf /<*serverroot*>/isw-<*hostname*>

   b. 通过键入以下内容删除引导文件

      rm -rf /etc/init.d/isw

8. 按如下步骤清除配置目录：

   a. 对安装了 Identity Synchronization for Windows 核心的配置目录运行以下 `ldapsearch` 命令，以找到 Identity Synchronization for Windows 控制台子树：

      ```
      ldapsearch -D "cn=directory manager" -w <my_password> -b
      o=netscaperoot "(nsnickname=isw)" dn
      ```

注意	`ldapsearch` 位于 Directory Server 的 `<serverroot>/shared/bin/ldapsearch` 下 例如， `/var/Sun/mps/shared/bin/ldapsearch`

      产生的条目应类似于以下内容 （请注意条目始终以 *o=NetscapeRoot* 结束）：

      ```
      "cn=Sun ONE Identity Synchronization for Windows,cn=server
      group, cn=myhost.mydomain.com,ou=mydomain.com,o=NetscapeRoot"
      ```

   b. 使用 “Directory Server 控制台”删除 Identity Synchronization for Windows 控制台子树及其下面的所有子树。

9. 按如下步骤清除 Identity Synchronization for Windows 配置注册表：

   a. 运行以下 `ldapsearch` 命令，以在 Directory Server 中找到 Identity Synchronization for Windows 配置注册表：

      ```
      ldapsearch -D "cn=directory manager" -w <my_password> -b
      "dc=my,dc=domain"
      "(&(objectclass=iplanetservice)(ou=IdentitySynchronization))" dn
      ```

      产生的条目应类似于以下内容：

      ```
      "ou=IdentitySynchronization,ou=Services,dc=my,dc=domain"
      ```

   b. 使用 “Directory Server 控制台”删除 Identity Synchronization for Windows 配置注册表及其下面的所有子树。

10. 按如下步骤清除其它所有与控制台相关的文件：

    a. 键入以下内容删除所有控制台 jar 文件：

       rm -rf <*serverroot*>/java/jars/isw*
       例如， /var/Sun/mps/java/jars/isw*

    b. 键入以下内容删除所有控制台 servlet jar 文件：

       rm -rf <*serverroot*>/bin/isw/
       例如， /var/Sun/mps/bin/isw/

从 Windows 2000 手动卸载 1.0 核心和实例

使用本节中提供的说明可从 Windows 2000 计算机手动卸载 “核心”。

注意 在本节中，将采用下列格式描述 Identity Synchronization for Windows 位置：

<*serverroot*>\isw-<*hostname*>

其中， <*serverroot*> 表示 Identity Synchronization for Windows 安装位置的父目录。

例如，如果在 C:\Program Files\Sun\mps\isw-*example* 中安装了 Identity Synchronization for Windows，则 <*serverroot*> 应为 C:\Program Files\Sun\mps。

---

1. 使用以下方法之一停止所有 Identity Synchronization for Windows Java 进程：

   - 选择 “开始” > “设置” > “控制面板” > “管理工具” > “服务”，打开 “服务”窗口。在右侧窗格中，右键单击 Sun ONE Identity Synchronization for Windows，然后选择 “停止”。
   - 打开 “命令提示符”窗口，然后键入以下命令：

     net stop “Sun ONE Identity Synchronization for Windows”

- 如果上述方法不可行，可使用以下步骤手动停止 Java 进程：

  I. 打开 “服务”窗口，右键单击 Sun ONE Identity Synchronization for Windows，然后选择 “属性”。

  II. 在 “属性”窗口的 “常规”选项卡中，从 “启动类型”下拉列表中选择 “手动”。

  注意 虽然可从 “Windows 任务管理器”查看 Java 进程 （如 `pswwatchdog.exe`），但您无法确定哪个进程与 Identity Synchronization for Windows 密切相关。因此，请不要从 “Windows 任务管理器”停止进程。

2. 使用以下方法之一停止 Message Queue （仅限 “核心”卸载）：

   - 在 “服务”窗口中，右键单击右侧窗格中的 iMQ Broker，然后选择 “停止”。
   - 打开 “命令提示符”窗口，然后键入以下命令：

     ```
     net stop "iMQ Broker"
     ```

   - 如果上述方法不可行，可使用以下步骤手动停止 Message Queue：

     I. 打开 “服务”窗口，右键单击 iMQ Broker，然后选择 “属性”。

     II. 在 “属性”窗口的 “常规”选项卡中，从 “启动类型”下拉列表中选择 “手动”。

3. 按如下步骤删除 Director Server 插件：

   a. 打开 “Directory Server 控制台”，然后选择 “配置”选项卡。

   b. 在左侧窗格中，展开 “插件”节点，然后选择 pswsync 节点。

   c. 在右侧窗格中，取消选中 “启用插件”复选框。

   d. 单击 “保存”保存所做更改。

   e. 在 “控制台”中，从 “配置目录”找到并删除以下条目：

      ```
      cn=pswsync,cn=plugins,cn=config
      ```

   f. 使用以下方法之一停止 Directory Server：

      - 在 “服务”窗口中，右键单击右侧窗格中的 Sun ONE Directory Server 5.2，然后选择 “停止”。

- 打开 “命令提示符”窗口，然后键入以下命令：

  net stop slapd-<*myhostname*>

g. 打开 “Windows 资源管理器”查找并删除 “插件”二进制文件：

<*serverroot*>\lib\psw-plugin.so

h. 重新启动 Directory Server。

4. 打开 “命令提示符”窗口，然后键入 **regedit** 以打开 “注册表编辑器”窗口。

要点 – 继续进行步骤 5 前请备份当前注册表文件。

a. 在 “注册表编辑器”中，选择左侧窗格中的顶节点 （我的电脑）。

b. 从菜单条中选择 “注册表” > “导出注册表文件”。

c. 显示 “导出注册表文件”对话框后，请指定文件名，然后选择保存备份注册表的位置。

5. 在 “注册表编辑器”中，从菜单条中选择 “编辑” > “删除”，并从 “Windows 注册表”中删除以下 Identity Synchronization for Windows 注册表主键：

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Identity Synchronization for Windows 下的所有条目
- HKEY_LOCAL_MACHINE\SYSTEM* 下的所有 CurrentControlSet 和 ControlSet （如 ControlSet001、 ControlSet002 等）条目，其中包括以下条目 （如果存在）：
  - ...\Control\Session Manager\Environment\<*isw-installation directory*>
  - ...\Services\Eventlog\Application\Sun ONE Identity Synchronization for Windows
  - ...\Services\Sun ONE Identity Synchronization for Windows
  - ...\Services\iMQBroker

6. 备份 （复制并重命名）位于 C:\WINNT\system32 中的当前 productregistry 文件。

7. 编辑 C:\WINNT\system32 \productregistry 文件，从中删除下列标记：

注意

- 为获得最佳效果，请使用 XML 编辑器。或者，可使用标准文本编辑器。
- 以下组件中的某些组件可能不包括在文件中。
- 必须删除开始标记 (<compid>)、结束标记 (<\compid>) 及两个标记之间的所有内容。在以下列表中，用省略号表示这些标记中的内容，包括任何其它文本和 / 或标记。（请参阅第 216 页上的示例。）

- <compid>Identity Synchronization for Windows .. . </compid>
- <compid>Core .. . </compid>
- <compid>unistaller .. . </compid>
- <compid>wpsyncwatchdog .. . </compid>
- <compid>setenv .. . </compid>
- <compid>Create DIT .. . </compid>
- <compid>Extend Schema .. . </compid>
- <compid>resources .. . </compid>
- <compid>CoreComponents .. . </compid>
- <compid>Connector .. . </compid>
- <compid>DSConnector .. . </compid>
- <compid>Directory Server Plugin .. . </compid>
- <compid>DSSubcomponents .. . </compid>
- <compid>ObjectCache .. . </compid>
- <compid>ObjectCacheDLLs .. . </compid>
- <compid>ADConnector .. . </compid>

以下为 <compid> 标记示例。删除 <compid>、 </compid> 以及两者之间的所有文本和标记。

```
<compid>Identity Synchronization for Windows
    <compversion>1.0
          <uniquename>Identity Synchronization for Windows</uniquename>
           <compinstance>1
                    <children>
                        <compref>ADConnector
                            <instance>1
                                <version>1.0</version>
                            </instance>
                        </compref>
                        <compref>DSSubcomponents
                        . . .

        </compinstance>
    </compversion>
</compid>
```

8. 删除位于 <*serverroot*>\isw-<*hostname*> 下的 Identity Synchronization for Windows 安装文件夹。

   例如， C:\Program Files\Sun\mps\isw-example

9. 按如下步骤清除配置目录：

   a. 在 “命令提示符”窗口中，对安装了 Identity Synchronization for Windows 核心的配置目录运行 ldapsearch 命令，以找到 Identity Synchronization for Windows 控制台子树。

注意 ldapsearch 位于 <*serverroot*>\shared\bin\ldapsearch 下。

例如，
C:\Program Files\Sun\mps\shared\bin\ldapsearch

```
ldapsearch -D "cn=directory manager" -w <my_password> -b
o=netscaperoot "(nsnickname=isw)" dn
```

产生的条目应类似于以下内容 （请注意条目始终以 *o=NetscapeRoot* 结束）：

```
"cn=Sun ONE Identity Synchronization for Windows,cn=server
group, cn=myhost.mydomain.com,ou=mydomain.com,o=NetscapeRoot"
```

b. 使用 “Directory Server 控制台”删除查找到的 Identity Synchronization for Windows 控制台子树及其下面的所有子树。

10. 按以下步骤清除 Identity Synchronization for Windows 配置目录 （*也称作配置注册表*）：

a. 在 “命令提示符”窗口中，运行下列 ldapsearch 命令，以在 Directory Server 中找到 Identity Synchronization for Windows 配置目录：

```
ldapsearch -D "cn=directory manager" -w <my_password> -b
"dc=my,dc=domain"
"(&(objectclass=iplanetservice)(ou=IdentitySynchronization))" dn
```

产生的条目应类似于以下内容：

```
"ou=IdentitySynchronization,ou=Services,dc=my,dc=domain"
```

b. 使用 “Directory Server 控制台”删除查找到的配置目录子树及其下面的所有子树。

11. 按如下步骤清除其它所有与控制台相关的文件：

a. 删除 <*serverroot*>\java\jars\isw* 中的所有控制台 jar 文件
例如， C:\Program Files\Sun\mps\java\jars\isw*

b. 删除 \<*directory_server_install_root*>\bin\isw\ 中的所有控制台 servlet jar 文件
例如， C:\SunOne\Servers\bin\isw\

12. 重新启动机器以使所有更改生效。

从 Windows NT 手动卸载 1.0 实例

使用本节中提供的说明可从 Windows NT 机器手动卸载实例。

注意 在本节中，将采用下列格式描述 Identity Synchronization for Windows 位置：

<*serverroot*>\isw-<*hostname*>

其中，<*serverroot*> 表示 Identity Synchronization for Windows 安装位置的父目录。例如，如果在 C:\Program Files\Sun\mps\isw-*example* 下安装了 Identity Synchronization for Windows，则 <***serverroot***> 应为 C:\Program Files\Sun\mps。

1. 使用以下方法之一停止所有 Identity Synchronization for Windows Java 进程（“核心”和实例安装）：
   - 选择 “开始” > “设置” > “控制面板” > “管理工具” > “服务”，打开 “服务”窗口。在右侧窗格中，右键单击 Sun ONE Identity Synchronization for Windows，然后选择 “停止”。
   - 打开 “命令提示符”窗口，然后键入以下命令：

     net stop "Sun ONE Identity Synchronization for Windows"
   - 如果上述方法不可行，请使用以下步骤手动停止 Java 进程：

     I. 打开 “服务”窗口，右键单击 Sun ONE Identity Synchronization for Windows，然后选择 “属性”。

     II. 在 “属性”窗口的 “常规”选项卡中，从 “启动类型”下拉列表中选择 “手动”。

     注意 虽然可从 “Windows 任务管理器”查看 Java 进程 （如 pswwatchdog.exe），但您无法确定哪个进程与 Identity Synchronization for Windows 密切相关。因此，请不要从 “Windows 任务管理器”停止进程。

2. 使用以下方法之一停止 Change Detector Service：
   - 在 “服务”窗口中，右键单击右侧窗格中的 Sun ONE NT Change Detector Service，然后选择 “停止”。

- 打开 “命令提示符”窗口，然后键入以下命令：

  `net stop "Sun ONE NT Change Detector Service"`

- 如果上述方法不可行，请使用以下步骤手动停止 Change Detector Service：

  I. 打开 “服务”窗口，右键单击 Change Detector Service，然后选择 “属性”。

  II. 在 “属性”窗口的 “常规”选项卡中，从 “启动类型”下拉列表中选择 “手动”。

3. 重新启动 Windows NT 计算机。

4. 必须删除 Identity Synchronization for Windows 注册表主键。打开 “命令提示符”窗口，然后键入 **`regedt32`** 以打开 “注册表编辑器”窗口。

警告 *不要*使用 `regedit`，因为该程序不允许编辑多值字符串。

继续进行步骤 5 *之前*请务必备份当前 Windows 注册表文件。

---

a. 在 “注册表编辑器”中，选择左侧窗格中的顶节点 （我的电脑）。

b. 从菜单条中选择 “注册表” > “导出注册表文件”。

c. 显示 “导出注册表文件”对话框后，请指定文件名，然后选择保存备份注册表的位置。

5. 在 “注册表编辑器”中，从菜单条中选择 “编辑” > “删除”，并从 “注册表”中删除以下 Identity Synchronization for Windows 注册表主键：

   - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Identity Synchronization for Windows 下的所有条目
   - HKEY_LOCAL_MACHINE\SYSTEM* 下的所有 CurrentControlSet 和 ControlSet（如 ControlSet001、 ControlSet002 等）条目，其中包括以下条目 （如果存在）：
     - ...\Control\Session Manager\Environment\<*isw-installation directory*>
     - ...\Services\Eventlog\Application\Sun ONE Identity Synchronization for Windows
     - ...\Services\Sun ONE Identity Synchronization for Windows
     - ...\Services\iMQBroker
   - HKEY_LOCAL_MACHINE\SOFTWARE\Sun Microsystems\PSW

6. 使用 **regedt32** （*不要使用* regedit）修改 （***不要删除***）以下注册表主键：

   a. 在左侧窗格中选择注册表主键条目：

   HKEY_LOCAL_MACHINE\SYSTEM\\CurrentControlSet\\CONTROL\\LSA

   注册表值类型必须为 REG_MULTI_SZ。

   b. 在右侧窗格中，右键单击 “通知软件包”值，然后选择 “修改”。

   c. 将 PASSFLT 值更改为 FPNWCLNT。

7. 备份 （复制并重命名）位于 C:\WINNT\system32 中的当前 productregistry 文件。

8. 编辑 C:\WINNT\system32 productregistry 文件，从中删除下列标记：

注意

- 为获得最佳效果，请使用 XML 编辑器。或者，可使用标准文本编辑器。
- 以下组件中的某些组件可能不包括在文件中。
- 必须删除开始标记 (<compid>)、结束标记 (<\compid>) 及两个标记之间的所有内容。在以下列表中，用省略号表示这些标记中的内容，包括任何其它文本和 / 或标记。（请参阅第 216 页上的示例。）

- <compid>Identity Synchronization for Windows .. . </compid>
- <compid>Core .. . </compid>
- <compid>uninstaller .. . </compid>
- <compid>wpsyncwatchdog .. . </compid>
- <compid>setenv .. . </compid>
- <compid>Create DIT .. . </compid>
- <compid>Extend Schema .. . </compid>
- <compid>resources .. . </compid>
- <compid>CoreComponents .. . </compid>
- <compid>Connector .. . </compid>
- <compid>DSConnector .. . </compid>
- <compid>Directory Server Plugin .. . </compid>
- <compid>DSSubcomponents .. . </compid>
- <compid>ObjectCache .. . </compid>
- <compid>ObjectCacheDLLs .. . </compid>
- <compid>ADConnector .. . </compid>

以下为 <compid> 标记示例。删除 <compid>、 </compid> 以及两者之间的所有文本和标记。

```
<compid>Identity Synchronization for Windows
    <compversion>1.0
       <uniquename>Identity Synchronization for Windows</uniquename>
           <compinstance>1
                    <children>
                        <compref>ADConnector
                            <instance>1
                                <version>1.0</version>
                            </instance>
                        </compref>
                        <compref>DSSubcomponents
                        . . .

        </compinstance>
    </compversion>
</compid>
```

9. 删除位于 <***serverroot***>\isw-<*hostname*> 下的 Identity Synchronization for Windows 安装文件夹。

   例如， `C:\Program Files\Sun\mps\isw-example`

   注意 继续进行步骤 10 前，必须如步骤 8 中所述编辑 Windows 注册表。

10. 删除 Password Filter DLL。

    在 `C:\winnt\system32` 文件夹中找到 `passflt.dll` 文件，然后将该文件重命名为 **`passflt.dll.old`**。

11. 重新启动机器以使所有更改生效。

其它移植方案

因为可能存在其它部署拓扑，所以具体移植过程可能与所描述的单主机部署过程有所不同。

本节为您介绍两种备用部署方案，并介绍如何在每种方案中进行移植。示例部署方案包括：

- “多主复制部署”
- 第 226 页的 “使用 Windows NT 的多主机部署”

多主复制部署

在多主复制 (MMR) 部署中，两个 Directory Server 实例安装在不同的主机上。可以在不同的操作系统上运行主机，但在本方案中，两台主机均在同一操作系统中运行。

表 7-2 说明 Identity Synchronization for Windows 组件将如何在这两台主机之间分布。

表 7-2 多主复制部署中的组件分布

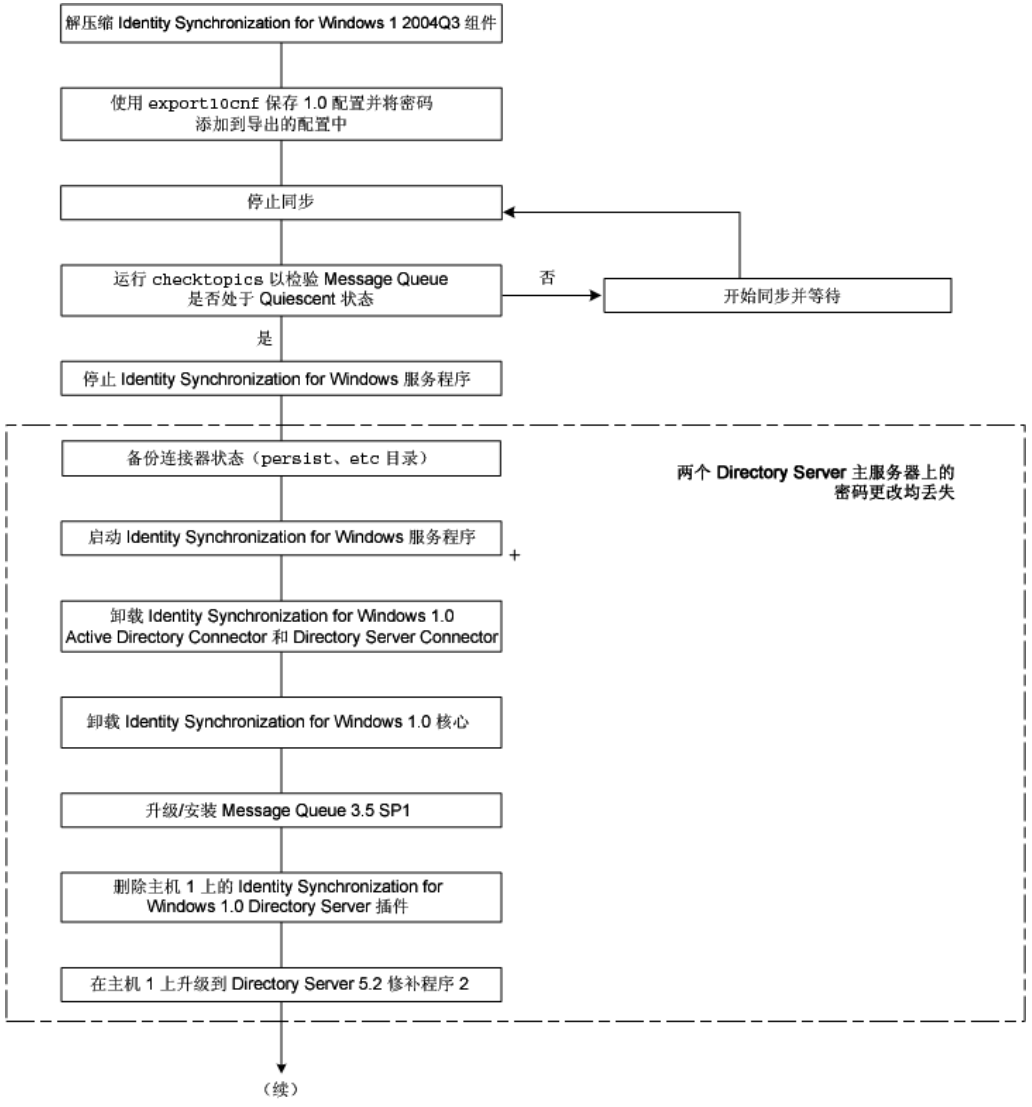
主机 1	主机 2
作为已同步用户的备用主服务器的 Directory Server （一个实例）	作为已同步用户的首选主服务器的 Directory Server （一个实例）
核心 （Message Queue、中心记录器、系统管理器和控制台）	Directory Server 插件
Active Directory Connector	
Directory Server Connector	
Directory Server 插件	

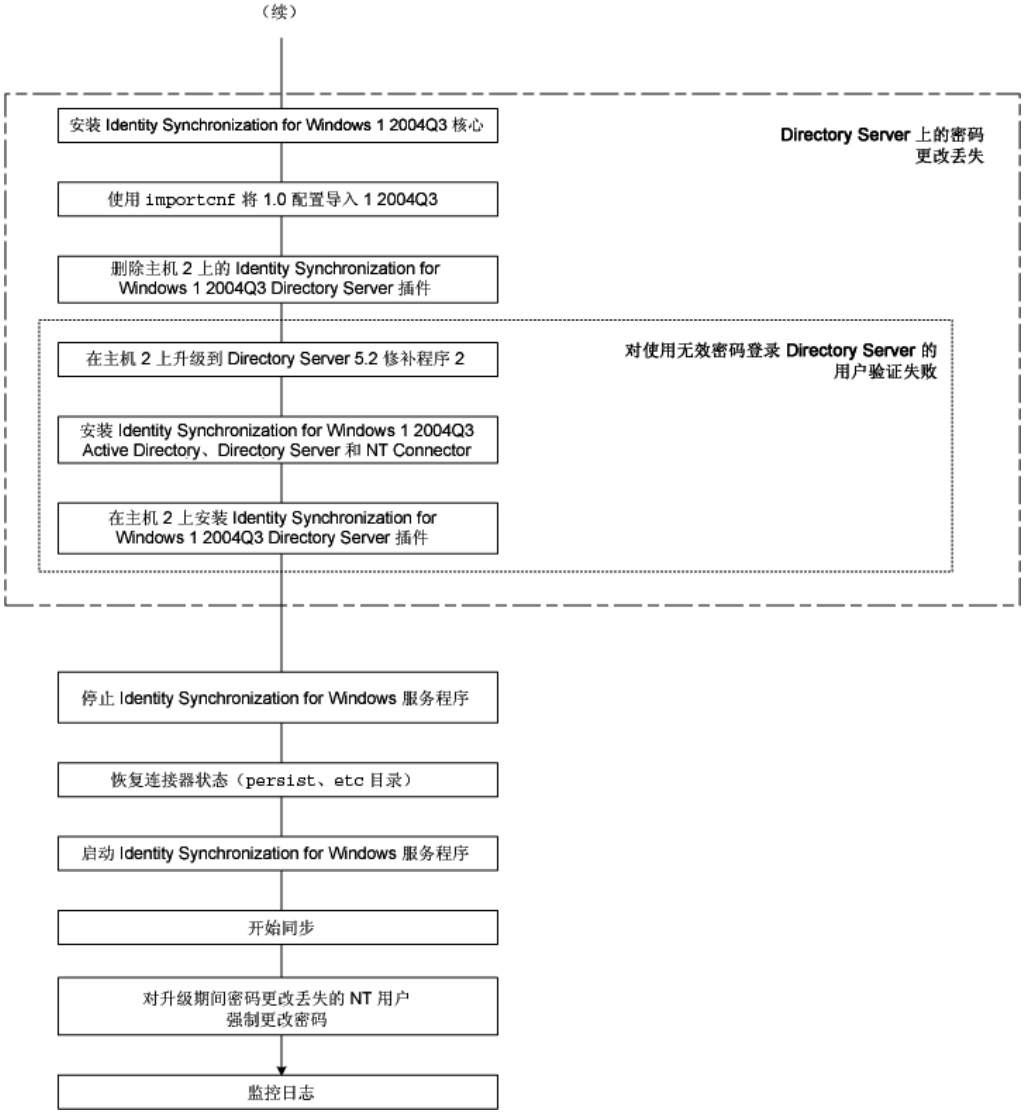
移植过程使即时请求密码同步在首选主服务器或备用主服务器上持续运行。

注意 如果两台主机均在 Solaris 操作系统中运行，则仅在进行同步时才需要使用第三台运行 Windows 2000 并装有 Active Directory 的主机。（第三台主机上不会安装任何组件。）

下图说明在 MMR 部署中移植 Identity Synchronization for Windows 的过程：

图 7-2 移植多主复制部署




（续）
安装 Identity Synchronization for Windows 1 2004Q3 核心
使用 importcnf 将 1.0 配置导入 1 2004Q3
删除主机 2 上的 Identity Synchronization for Windows 1 2004Q3 Directory Server 插件
在主机 2 上升级到 Directory Server 5.2 修补程序 2
安装 Identity Synchronization for Windows 1 2004Q3 Active Directory、Directory Server 和 NT Connector
在主机 2 上安装 Identity Synchronization for Windows 1 2004Q3 Directory Server 插件
Directory Server 上的密码更改丢失
对使用无效密码登录 Directory Server 的用户验证失败
停止 Identity Synchronization for Windows 服务程序
恢复连接器状态（persist、etc 目录）
启动 Identity Synchronization for Windows 服务程序
开始同步
对升级期间密码更改丢失的 NT 用户强制更改密码
监控日志

使用 Windows NT 的多主机部署

在本部署方案中将使用三台主机：

- Windows NT 系统
- 安装 Directory Server 的主机，包含已同步用户并安装了 Directory Server Connector
- 安装所有其它组件的主机

表 7-3 说明 Identity Synchronization for Windows 组件将如何在这三台主机之间分布。

表 7-3 多主机部署

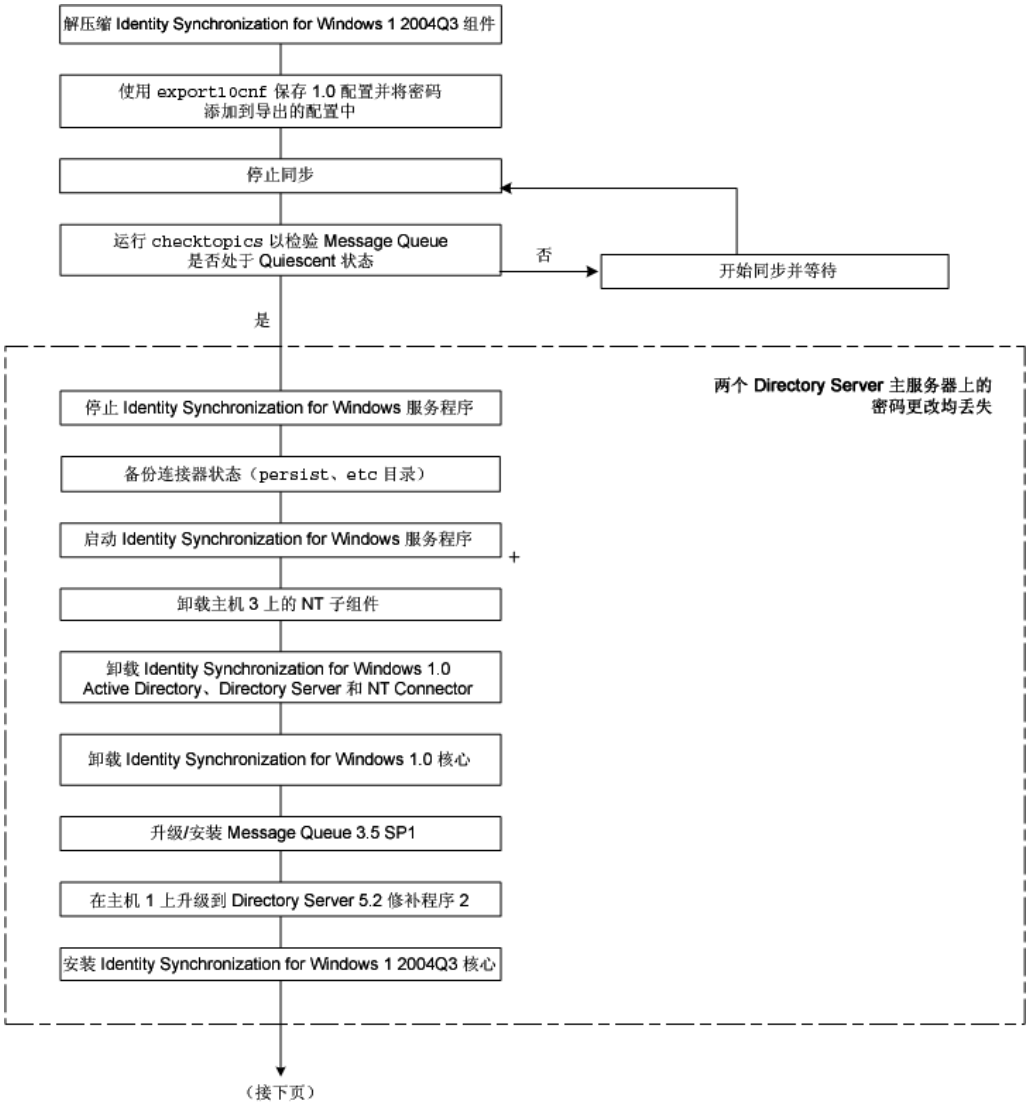
主机 1	主机 2	主机 3
带有配置信息库的 Directory Server	用于已同步用户的 Directory Server	Windows NT Connector
核心 （Message Queue、中心记录器、系统管理器和控制台）	Directory Server Connector	Windows NT 子组件（Password Filter DLL 和 Change Detector Service）
Active Directory Connector	Directory Server 插件	

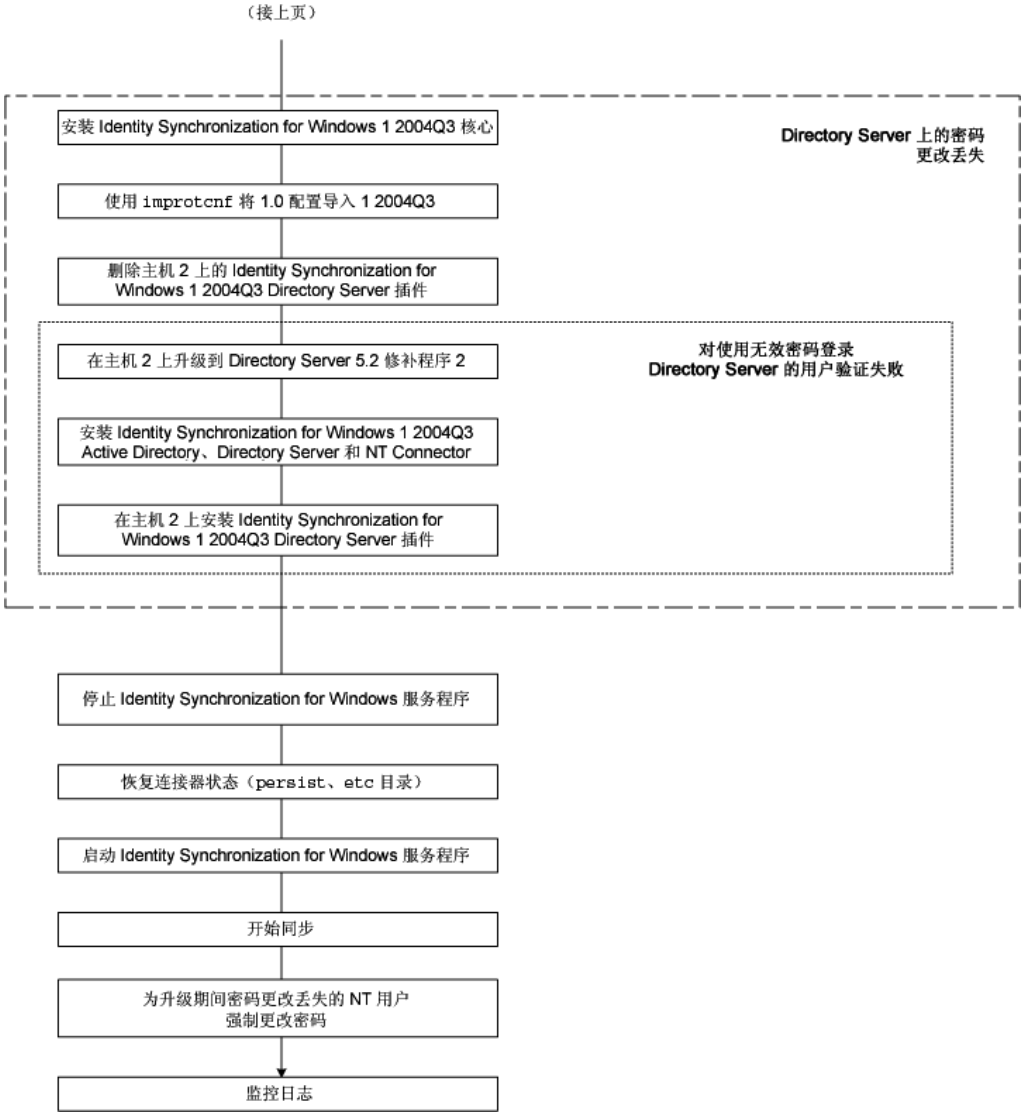
如同上一方案，主机 1 和主机 2 在相同的操作系统中运行。

注意 如果这两台主机均在 Solaris 操作系统中运行，则仅在进行同步时才需要使用第四台运行 Windows 2000 并装有 Active Directory 的主机。（第四台主机上不会安装任何组件。）

图 7-3 说明为多主机部署移植 Identity Synchronization for Windows 的过程：

图 7-3 使用 Windows NT 移植多主机部署




（接上页）
安装 Identity Synchronization for Windows 1 2004Q3 核心
使用 improtcnf 将 1.0 配置导入 1 2004Q3
删除主机 2 上的 Identity Synchronization for Windows 1 2004Q3 Directory Server 插件
在主机 2 上升级到 Directory Server 5.2 修补程序 2
安装 Identity Synchronization for Windows 1 2004Q3 Active Directory、Directory Server 和 NT Connector
在主机 2 上安装 Identity Synchronization for Windows 1 2004Q3 Directory Server 插件
Directory Server 上的密码更改丢失
对使用无效密码登录 Directory Server 的用户验证失败
停止 Identity Synchronization for Windows 服务程序
恢复连接器状态（persist、etc 目录）
启动 Identity Synchronization for Windows 服务程序
开始同步
为升级期间密码更改丢失的 NT 用户强制更改密码
监控日志

检查日志

移植到版本 1 2004Q3 后，请在中心审计日志中查找指示问题的消息，尤其是移植过程中密码更改可能已丢失的 Directory Server 用户，将产生类似于以下内容的消息：

```
[16/Apr/2004:14:23:41.029 -0500] WARNING    14  CNN101

ds-connector-host.example.com  "Unable to obtain password of user
cn=JohnSmith,ou=people,dc=example,dc=com, because the password was encoded
by a previous installation of Identity Synchronization for Windows
Directory Server Plugin.The password of this user cannot be synchronized at
this time.Update the password of this user again in the Directory Server."
```

在 Identity Synchronization for Windows 1 2004Q3 中启动同步后才能看到此日志消息，这便是在移植过程的最后一个步骤检查日志的原因所在。

第 8 章

删除软件

本节介绍删除 Identity Synchronization for Windows 1 2004Q3 的过程，具体包括以下几个部分：

卸载规划

在删除软件前，请牢记以下几点：

注意 必须按相关说明*明确地*卸载产品的组件和子组件，并检查所有组件是否均已成功卸载。

- 子组件和 Directory Server 插件必须在卸载其相关连接器之前卸载，而所有连接器必须在卸载 “核心”之前卸载。（Active Directory Connector 没有任何要卸载的子组件。）

  如果未按正确的顺序卸载上述某个组件，则将无法选择和卸载其它组件。例如，如果不先卸载连接器，则不能选择卸载 “核心”。

- 必须在卸载 “核心”之前卸载 Directory Server 插件

  先卸载 “核心”将导致在未从 Directory Server 取消注册的情况下卸载 “插件”组件，这样就无法启动 Directory Server，除非手动删除 `cn=pswsync,cn=plugins,cn=config`。

- 在带有副本的复制环境（除主服务器和备用服务器外）中，必须先卸载 Directory Server 插件，然后重新启动服务器。

- 连接器的卸载顺序无关紧要。
- 在卸载 Sun Java System Directory Server 或 Windows NT Connector 后，必须执行一些额外的步骤将 “连接器”重新安装到其它机器上，或使用不同的服务器端口。

  在这种情况下，必须卸载所有相应的子组件然后重新安装，并重新启动安装有 “核心”的 Identity Synchronization for Windows 服务 / 守护进程 （请参阅第 181 页的 “启动和停止服务”）。
- 在卸载所有系统上的所有连接器和子组件之前，不得卸载 “核心”。
- 必须在 Windows 2000 和 NT 平台上运行 `uninstall.cmd` 脚本 （位于 `isw-`*<hostname>* 目录中）。（必须以 “管理员”身份运行此批处理文件。）
- 必须在 Solaris 操作系统上运行 `runUninstall.sh` 脚本 （默认情况下位于 `/opt/SUNWisw` 安装目录中）。（必须以超级用户身份运行此脚本。）

卸载软件

您的系统中可能包含以下任何或全部 Identity Synchronization for Windows 组件：

- Active Directory Connector
- Directory Server 连接器和插件
- 核心

您的 Windows NT 系统可能包含 Windows NT Connector 和子组件。

使用 `runUninstaller.sh` (Solaris) 或 `uninstall.cmd` (Windows) 删除所有连接器和子组件，然后删除 “核心”（如果已安装）。

本节说明以下内容：

卸载 Directory Server 插件

注意

- 卸载程序仅删除 Identity Synchronization for Windows Directory Server 插件。不能使用此卸载程序删除任何其它 Directory Server 插件。

  在本书中， *Directory Server 插件*指 Identity Synchronization for Windows Directory Server 插件 （除非另有说明）。

- 要在基于文本的模式下运行卸载程序 （仅限 Solaris），请键入

  `./runUninstaller.sh -nodisplay`

  运行此程序时， Identity Synchronization for Windows 将自动屏蔽密码，从而密码不会以明文显示。

执行以下步骤卸载 Identity Synchronization for Windows Directory Server 插件。

1. 启动卸载程序 （Solaris 中为 `runUninstaller.sh`， Windows 中为 `uninstall.cmd`）。

   这些卸载程序位于安装目录 （默认情况下为 `/opt/SUNWisw` 目录）中。

2. 在 “欢迎”屏幕上单击 “下一步”。
3. 输入配置目录主机名和端口号。
   - 选择配置目录的根后缀。（如果需要，单击 “刷新”以查看后缀列表。）
   - 要实现卸载程序与配置目录服务器之间的安全通信，请启用 “安全端口”框，然后指定 Directory Server 的 SSL 端口号。
4. 为配置目录输入管理员的名称和密码。
5. 选择 “卸载 Directory Server 插件”选项。
6. 输入 Directory Server 主机名、端口和管理员的证书 （名称和密码）。
7. 单击 “下一步”继续执行与卸载相关的任务。
8. 出现系统提示时，重新启动安装了 “插件”的 Directory Server。
9. 会出现一个摘要窗口。请按此窗口中的说明操作。
   - **在 Solaris 系统中：**卸载日志被写入 `/var/sadm/install/logs/`

- **在 Windows 系统中**：卸载日志被写入 `%TEMP%` 目录，它是 `Local Settings` 文件夹的子目录，该文件夹在

  `C:\Documents and Settings\Administrator œ¬`

  注意 在某些 Windows 系统中 （如 Windows 2000 Advanced Server）， `Local Settings` 文件夹是隐藏文件夹。

  要查看此文件夹和 `Temp` 子目录：

  打开 “Windows 资源管理器”，然后从菜单条中选择 “工具” > “文件夹选项”。显示 “文件夹选项”对话框后，选择 “查看”选项卡，并启用 “显示隐藏的文件”选项。

单击 “关闭”退出该程序。

10. 如果该 Directory Server 插件是在目标主机上安装的*唯*一 Identity Synchronization for Windows 组件，则可以删除 isw-*hostname* 文件夹。
11. 对安装在网络中 Windows 2000 服务器上的每个 “Directory Server 插件”重复执行步骤 1 至步骤 9。

卸载连接器

要卸载连接器，请执行以下步骤：

1. 启动卸载程序 （Solaris 中为 runUninstaller.sh， Windows 中为 uninstall.cmd）。

   这些程序位于安装目录 （默认情况下为 /opt/SUNWisw 目录）中。

2. 在 “欢迎”屏幕上单击 “下一步”。

3. 输入配置目录主机名和端口号。

   - 选择配置目录的根后缀。（如果需要，单击 “刷新”以查看后缀列表。）
   - 要实现卸载程序与配置目录服务器之间的安全通信，请启用 “安全端口”框，然后指定 Directory Server 的 SSL 端口号。

4. 为配置目录输入管理员的名称和密码。

5. 选择要卸载的连接器。

   注意 选定的连接器*必须*存在于目标主机上。

6. 单击 “下一步”继续执行与卸载相关的任务。

7. 会出现一个摘要窗口。请按此窗口中的说明操作。

   - **在 Solaris 系统中**：卸载日志被写入 /var/sadm/install/logs/
   - **在 Windows 系统中**：卸载日志被写入 %TEMP% 目录，它是 Local Settings 文件夹的子目录，该文件夹在

     C:\Documents and Settings\Administrator œ¬

   注意 在某些 Windows 系统中 （如 Windows 2000 Advanced Server）， Local Settings 文件夹是隐藏文件夹。要查看此文件夹和 Temp 子目录：

   打开 “Windows 资源管理器”，然后从菜单条中选择 “工具” > “文件夹选项”。显示 “文件夹选项”对话框后，选择 “查看”选项卡，并启用 “显示隐藏的文件”选项。

8. 单击 “关闭”退出该程序。

9. 如果在目标主机上未安装其它连接器，则可以安全地删除 `isw-<hostname>` 文件夹。
10. 对安装了连接器的所有主机重复执行步骤 1 至步骤 7。

卸载核心

注意 必须在卸载 “核心” 之前卸载 Directory Server 插件

在卸载 “插件” 之前卸载 “核心” 将导致 “插件” 组件在未从 Directory Server 取消注册的情况下被卸载，这样就无法启动 Directory Server，除非手动删除 `cn=pswsync,cn=plugins,cn=config`。

请按下列说明卸载 “核心”：

1. 启动卸载程序：
   - 在 **Windows** 计算机中：
     I. 单击 “开始”，然后选择 “设置” > “控制面板”。
     II. 双击 “添加 / 删除程序”。
     III. 在 “添加 / 删除程序” 窗口中，选择 `Identity Synchronization for Windows`，然后单击 “删除”。
   - 在 **Solaris 或 Windows** 计算上，在 Solaris 中执行 `runUninstaller.sh`，在 Windows 中执行 `uninstall.cmd`。

     这些程序位于安装目录 （默认情况下为 `/opt/SUNWisw` 目录）中。
2. 在 “欢迎” 屏幕上单击 “下一步”。
3. 输入配置目录主机名和端口号。
   - 选择配置目录的根后缀。（如果需要，单击 “刷新” 以查看后缀列表。）
   - 要实现卸载程序与配置目录服务器之间的安全通信，请启用 “安全端口” 框，然后指定 Directory Server 的 SSL 端口号。
4. 为配置目录输入管理员的名称和密码。
5. 选择要卸载的 “核心”，然后单击 “下一步”。
6. 输入配置目录 URL，单击 “刷新”，然后从下拉列表中选择合适的根后缀。

7. 单击 “下一步”继续执行与卸载相关的任务。
8. 会出现一个摘要窗口。请按此窗口中的说明操作。
   - **在 Solaris 系统中**：卸载日志被写入 /var/sadm/install/logs/
   - **在 Windows 系统中**：卸载日志被写入 %TEMP% 目录，它是 Local Settings 文件夹的子目录，该文件夹在

     C:\Documents and Settings\Administrator 下

注意 在某些 Windows 系统中 （如 Windows 2000 Advanced Server）， Local Settings 文件夹是隐藏文件夹。

要查看此文件夹和 Temp 子目录：

打开 “Windows 资源管理器”，然后从菜单条中选择 “工具” > “文件夹选项” 。显示 “文件夹选项”对话框后，选择 “查看” 选项卡，并启用 “显示隐藏的文件”选项。

---

9. 单击 “关闭”退出该程序。

注意 如果因任何原因不能对特定连接器运行连接器卸载程序（例如，在硬盘发生故障时丢失了连接器文件），请使用 idsync resetconn 子命令（请参阅第 318 页的 “使用 resetconn”）。

此命令将配置目录中的连接器状态重置为*已卸载*，这样您就可将连接器重新安装到其它位置。 resetconn 子命令与访问配置目录的其它命令相似，具有两个选项：

- **-e <*dir-source*>**: 指定要重设的目录源名称。（在安装程序中，连接器通过它们的目录源名称识别。）
- **-n**（安全模式）：指示在不执行任何操作的情况下，为该命令指定的参数是否正确。

命令示例：

```
idsync resetconn -D "cn=Directory Manager" -w [-h CR-hostname]
[-p 389] [-s dc=example,dc=sun,dc=com] -q [-Z] [-P "cert8.db"]
[-m "secmod.db"] -e "dc=central,dc=example,dc=com" [-n]
```

resetconn 输出：

```
NOTICE:This program will reset the installation state to UNINSTALLED
for the Connector associated with the specified DirectorySource
'dc=central,dc=example,dc=com'.

Changing the Connector to an UNINSTALLED state is a last resort.This
is NOT meant to be used for uninstalling connectors.It is typically
used if you lost a machine with the connector on it and can not run
the uninstaller.Additionally, this program will rewrite the existing
configuration.This can be a lengthy process.Before proceeding, you
should stop the Console, any running installers, and all other
system processes.You may want to export the ou=Services tree in the
configuration directory to ldif as a backup.

Do you want to reset the installer settings for the connector (y/n)?
```

手动卸载控制台

在删除所有其它 Identity Synchronization for Windows 组件后，必须手动卸载“控制台”。

从 Solaris 系统

要从 Solaris 系统卸载控制台，请执行以下步骤：

1. 从配置目录中删除以下子树：

   cn=Sun Java (TM) System Identity Synchronization for Windows,cn=<*server_group*>,cn=<*hostname*>, ou=<*domain_name*>, o=netscaperoot

2. 对安装的所有控制台，从以下目录删除所有带 *isw* 前缀的 .jar 文件：

   <*serverroot*></*server*>/java/jars

从 Windows 系统

要从 Windows Active Directory 或 NT 系统卸载 “控制台”，请执行以下步骤：

1. 从配置目录中删除以下子树：

   cn=Sun Java (TM) System Identity Synchronization for Windows,cn=<*server_group*>,cn=<*hostname*>, ou=<*domain_name*>, o=netscaperoot

2. 对安装的所有控制台，从以下目录删除所有带 *isw* 前缀的 .jar 文件：

   <*serverroot*>/<*server*>/java/jars

第 9 章

故障排除

本章介绍的内容可帮助您解决在使用 Identity Synchronization for Windows 过程中可能会遇到的问题。内容具体安排如下：

故障排除清单

注意

管理员：排除故障时，请调整日志级别 （如第 272 页的 “配置日志文件”中所述），以确保日志反映出可能导致问题的所有事件。

直到您将日志级别调整为 “详细”或更高级别时，才会将某些事件（如因用户未包括在 SUL 中而致使程序未能同步用户更改）包括在日志文件中。在所有 `idsync resync` 操作期间，应将日志级别设为 “信息”。

在安装和配置 Identity Synchronization for Windows 时， `idsync printstat` 命令是一个很有用的工具。运行 `printstat` （请参阅第 317 页的 “使用 printstat”）后，将显示要完成安装和配置过程所必须执行的其余步骤的列表。

1. 中心 error.log 中是否报告有任何问题？

   `isw-`*<hostname>*`/logs/central/error.log`

   几乎所有错误都会在中心错误日志文件中报告。而且，通常还可在 `audit.log` 文件中获取有关任何错误的附加信息。为使相关日志条目易于关联，`audit.log` 文件还包括错误日志中的所有条目。

2. “发行说明”中提及了许多已知问题。是否对此问题进行了相应说明？

3. 安装是否是在已彻底卸载的机器上进行的？如果未彻底卸载先前的配置便重新安装本产品，则可能会出现问题。有关如何清除先前安装的详细说明，请参阅第 8 章，“删除软件”。

4. 是否正确安装了 “核心”？如果成功完成了 “核心”安装，那么日志文件会存在于 `isw-`*<hostname>*`/logs/central/` 目录中。

5. 资源配置期间是否运行了 Directory Server？

6. 当前是否在运行 “核心”（包括 Message Queue 和 “系统管理器”）？在 Windows 中，请检查相应的服务名称。在 Solaris 中，请检查相应的守护进程名称。使用 `idsync printstat` 命令检验 Message Queue 和 “系统管理器”是否处于活动状态。

7. 是否成功保存了配置？如果 `idsync printstat` 命令列出连接器，则表明成功保存了配置。

8. 是否安装了全部连接器？必须为要同步的每个目录源安装一个连接器。

9. 是否安装了全部子组件？ Directory Server Connector 和 Windows NT Connector 要求在安装 “连接器” 后安装子组件。必须在每个 Directory Server 副本上安装 “Directory Server 插件”。

10. 是否遵循了安装后步骤？安装 “Directory Server 插件” 后必须重新启动 Directory Server。安装 Windows NT 子组件后，必须重新启动 “Windows NT 主域控制器”。

11. 是从 “控制台” 还是命令行开始的同步？

12. 是否所有连接器都在运行？

13. 使用 “控制台” 或 `idsync printstat` 检验是否所有连接器均处于 “正在同步” 状态。

14. 所要同步的目录源是否正在运行？

15. 使用 “控制台” 检验是否按预期方向同步修改和 / 或创建。

16. 如果只同步存在于一个目录源中的用户，那么是否已使用 `idsync resync` 命令在另一个目录源中创建了这些用户？

    注意 只要存在现有用户，就必须运行 `idsync resync`。如果不重新同步现有用户，则重新同步行为仍处于未定义状态。

17. 如果同步存在于两个目录源中的用户，那么是否已使用 `idsync linkusers` 命令链接了这些用户？

18. 如果从 Active Directory 或 Windows NT 到 Sun Java System Directory Server 创建用户失败，请检验是否将 Directory Server 对象类中的所有强制属性均指定为创建属性，且相应属性的值显示在原始户条目中。

19. 如果从 Directory Server 到 Windows NT 同步创建并且用户创建成功，但是帐户不可用，请检验用户名是否违反了 Windows NT 的要求。

    例如，如果指定的名称超过 Windows NT 的最大允许长度限制，则虽然可在 NT 上创建用户，但须重命名该用户 （“用户” > “重命名”）后方可使用和编辑。

20. 为使 Windows NT SAM Change Detector 子组件有效，必须打开 NT 审计日志。选择 “开始” > “程序” > “管理工具” > “用户管理器”，然后选择 “策略” > “审核策略”。
    选择 “审核下列事件”，然后选中 “用户和组管理” 的 “成功” 和 “失败” 框。

    在 “事件查看器” > “事件日志覆盖” 中选择 “事件日志设置”，然后选择 “视需要覆盖事件”。

21. 未能同步的用户是否在 “同步用户列表”中？例如，它们是否与 “同步用户列表”的基本 DN 及过滤器匹配？在包含 Active Directory 的部署中，如果 Sun Java System Directory Server 条目不在任何 “同步用户列表”中，则即时请求密码同步将失败且不显示任何提示信息。出现这种情况通常是因为 “同步用户列表”上的过滤器不正确。

22. 是否更改了同步设置？如果同步设置由仅将用户从 Active Directory 同步到 Sun Java System Directory Server 更改为从 Directory Server 同步到 Active Directory，则必须将 Active Directory SSL CA 证书添加到连接器的证书数据库。 `idsync certinfo` 命令根据当前 SSL 设置报告必须安装的 SSL 证书。

23. 是否正确指定了所有主机名且在 DNS 中可解析？ Active Directory 域控制器应能够从运行 Active Directory Connector 的机器和运行 “Sun Java System Directory Server 插件”的机器上进行 DNS 解析。

24. Active Directory 域控制器的 IP 地址是否解析为连接器用于与之建立连接的同一名称？

25. 源连接器是否检测对用户进行的更改？使用中心 `audit.log` 可确定添加或修改了用户的目录源的连接器是否检测修改。

26. 目标连接器是否处理此修改？

27. 是否配置了多个 “同步用户列表”？如果是，这些列表是否存在冲突？应使用 “控制台”将较为具体的 “同步用户列表”排列在不太具体的 “同步用户列表”前面。

28. 如果将流动设为双向或从 Sun 流动到 Windows，且部署中存在 Active Directory 数据源，那么是否将连接器配置为使用 SSL 通信？

29. 在 Solaris 环境中，如果疑有内存问题，请检查各个进程。要查看哪些组件正在作为不同的进程运行，请输入

    `/usr/ucb/ps -gauxwww | grep com.sun.directory.wps`

    输出结果将列出全部详细信息，包括连接器 ID、系统管理器和中心记录器。这非常有助于查看是否有任何进程正在占用过多内存。

30. 如果要创建或编辑 Sun Java System 目录源，而 Directory Server 未出现在 “选择已知服务器”下拉列表中，请检查 Directory Server 是否正在运行。只有正在运行的 Directory Server 才会出现在可用主机下拉列表中。

    如果所述服务器暂时处于关闭状态，请在 “通过提供主机名和端口指定服务器”字段中键入主机和端口。

注意 Identity Synchronization for Windows 默认情况下使用短主机名；但默认主机名可能不适用于您的配置。建议在系统要求您提供主机名时使用全限定名。

31. 运行卸载程序时是否接收到以下错误？

```
./runInstaller.sh
IOException while making /tmp/SolarisNativeToolkit_5.5.1_1
executable:java.io.IOException:Not enough space
java.io.IOException:Not enough space
```

增大安装在 /tmp 下的交换文件的容量。

排除连接器故障

利用本节提供的信息排除连接器故障。内容具体安排如下：

如何确定管理目录源的连接器的 ID

可使用以下方法之一确定连接器 ID：

使用中心日志

可通过搜索中心 `audit.log` 来确定要同步的目录源的连接器 ID。启动时，中心记录器会记录每个连接器的 ID 及其管理的目录源。查找启动标题的最后一个实例，以获取最新信息。

例如，在下列日志消息中有两个连接器：

- **CNN101** 是管理 `dc=airius,dc=com` 的 Sun Directory Connector
- **CNN100** 是管理 `airius.com` 域的 Active Directory Connector

```
[2003/03/19 00:00:00.722 -0600] INFO    16     "System Component
Information:SysMgr_100 is the system manager (CORE);  console is the Product
Console User Interface;  CNN101 is the connector that manages
[dc=airius,dc=com (ldap://host1.airius.com:389)];  CNN100 is the connector
that manages [airius.com (ldaps://host2.airius.com:636)];"
```

使用 idsync printstat

也可使用 idsync printstat 命令获取连接器 ID 和状态 （请参阅第 317 页的 “使用 printstat”）。

此命令的示例输出如下：

```
Connector ID: CNN100
   Type:     Active Directory
   Manages:  airius.com (ldaps://host2.airius.com:636)
   State:    READY

Connector ID: CNN101
   Type:     Sun Java System Directory
   Manages:  dc=airius,dc=com (ldap://host1.airius.com:389)
   State:    READY

Sun Java System Message Queue Status:  Started

Checking the System Manager status over the Sun Java System Message Queue.

System Manager Status:  Started

SUCCESS
```

如何确定连接器的当前状态

可使用以下方法确定同步所涉及的连接器的当前状态：使用 “控制台” 中的 “状态” 窗格，使用 idsync printstat 命令 （如前所述），或在中心 audit.log 中查找。

在 audit.log 中搜索报告连接器状态的最后一条消息。
例如，在下面的日志消息中，可看到连接器 CNN101 处于 “就绪” 状态。

```
[2003/03/19 10:20:16.889 -0600] INFO    13  SysMgr_100 host1  "Connector
[CNN101] is now in state "READY"."
```

表 9-1 对各种连接器状态进行了说明。

表 9-1 连接器状态含义

状态	含义
尚未安装	尚未安装连接器。
已安装	已安装连接器，但该连接器尚未接收到其配置。
就绪	已安装连接器且已接收到其配置，但尚未启动同步。
正在同步	已安装连接器并接收到其配置，且已尝试启动同步。

连接器处于 “尚未安装” 状态时应采取的操作

安装连接器。

连接器安装失败但无法重新安装时应采取的操作

如果连接器安装失败，但 Identity Synchronization for Windows 安装程序认为已安装该连接器，则安装程序将不允许您重新进行安装。

运行 `idsync resetconn`（如第 318 页的 “使用 resetconn”中所述），以将连接器状态重设为 “尚未安装”，然后重新安装该连接器。

连接器处于 “已安装” 状态时应采取的操作

如果连接器在较长一段时间内均处于已安装状态，则很可能未运行它，或者它无法与 Message Queue 通信。

在安装连接器的机器上，查看连接器的日志 （`audit.log` 和 `error.log`）以查找潜在错误。如果连接器无法连接至 Message Queue，则会在此报告错误。这种情况下，请参阅第 255 页的 “排除 Message Queue 故障”查找可能的原因。

如果审计日志中的最新消息已变得很陈旧，则可能未运行该连接器。请参阅第 250 页的 “排除组件故障”。

连接器处于 “就绪” 状态时应采取的操作

在启动同步、安装全部子组件并将它们连接至连接器前，连接器将保持 “就绪” 状态。如果尚未启动同步，请使用 “控制台” 或命令行实用程序进行启动。

如果已启动同步，但某个连接器未进入 “正在同步” 状态，则可能子组件有问题。请参阅第 253 页的 “排除子组件故障”。

连接器处于 “正在同步” 状态时应采取的操作

如果所有连接器均处于 “正在同步” 状态，但未同步修改，请检验同步设置是否正确：

- 使用 “控制台” 检验是否按预期方向（例如，从 Windows 到 Sun Java System Directory Server）同步修改和 / 或创建。
- 使用 “控制台” 检验要修改的属性是否是已同步的属性 （注意：密码始终会进行同步）。如果未同步已创建的用户条目，请检验是否在 “控制台” 中启用了用户创建流动。
- 源连接器是否检测对用户进行的更改？使用中心 `audit.log` 可确定添加或修改了用户的目录源的连接器是否检测修改。目标连接器是否处理此修改？

Active Directory Connector 无法通过 SSL 与 Active Directory 联系时应采取的操作

如果 Active Directory Connector 无法通过 SSL 与 Active Directory 联系，且随后显示以下错误消息，请重新启动 AD 域控制器。

```
Failed to open connection to ldaps://server.example.com:636,
error(91):Cannot connect to the LDAP server, reason:SSL_ForceHandshake
failed:(-5938) Encountered end of file.
```

排除组件故障

利用本节提供的信息排除组件故障。内容具体安排如下：

在 Solaris 中

命令 `/usr/ucb/ps -auxww | grep com.sun.directory.wps` 将列出运行的所有 Identity Synchronization for Windows 进程。下表列出了应该运行的进程。

表 9-2 Identity Synchronization for Windows 进程

Java 进程类名	组件	何时运行
`com.sun.directory.wps.watchdog.server.WatchDog`	系统监视器	始终
`com.sun.directory.wps.centrallogger.CentralLoggerManager`	中心记录器	仅当安装“核心”后
`com.sun.directory.wps.manager.SystemManager`	系统管理器	仅当安装“核心”后
`com.sun.directory.wps.controller.AgentHarness`	连接器	每个已安装的连接器对应一个

如果未运行预期数目的进程，则请发出以下命令重新启动所有 Identity Synchronization for Windows 进程。

```
# /etc/init.d/isw stop
# /etc/init.d/isw start
```

如果运行了 “监视器”进程，但未运行预期数目的 `java.exe` 进程，则请参阅 “检查 WatchList.properties”一节，以检验是否正确安装了所有组件。

与其它系统组件一样，“Sun Java System Directory Server 插件”通过总线发送由中心记录器管理的日志记录，以便最终用户查看。但是，该 “插件”还记录某些可能不通过总线显示的消息 （例如当子组件无法联系连接器时）。这种情况下，日志消息只显示在文件系统中类似如下所示的 “插件”的 `logs` 目录中：

<serverroot>`/isw-`*<hostname>*`/logs/SUBC`*<id>*。

因为该插件与 Directory Server 进程一起运行，所以有可能会出现插件无法向其 `logs` 目录进行写操作的问题。如果以 `logs` 目录属主之外的用户身份运行目录服务器，便会出现这种情况。此时，可能有必要使用本机操作系统命令通过更改目录权限或属主明确指定 “插件” 权限。

在 Windows 中

使用 “服务” 控制面板，检查是否已启动 Sun Java System Identity Synchronization for Windows 服务。如果未启动此服务，则表明该机器上未运行 Identity Synchronization for Windows，应将其启动。如果已启动此服务，则请使用 “任务管理器” 检验是否正在运行 `pswwatchdog.exe` （监视器进程）并且正在运行预期数目的 `java.exe` 进程：

- Message Queue 代理程序对应一个进程 （仅当安装了 “核心” 时）
- “系统管理器” 对应一个进程 （仅当安装了 “核心” 时）
- “中心记录器” 对应一个进程 （仅当安装了 “核心” 时）
- 该机器上安装的每个 “连接器” 对应一个进程

注意 可能会有其它处于活动状态的 java 进程，如 “Directory Server 控制台”。如果未运行 `pswwatchdog.exe`，则请重新启动 “Sun Java System Identity Synchronization for Windows” 服务。如果运行了它，但未运行预期数目的 `java.exe` 进程，则请参阅第 252 页的 “检查 WatchList.properties”，以检验是否正确安装了所有组件。

检查 WatchList.properties

在每台安装有 Identity Synchronization for Windows 组件的机器上，isw-<*machine_name*>/resources/WatchList.properties 文件将枚举应在该机上运行的组件。process.name[n] 属性用于命名应运行的组件。

在安装有 “核心”的机器上， WatchList.properties 将包括 “中心记录器”和 “系统管理器”的条目：

```
process.name[1]=Central Logger
…
process.name[2]=System Manager
…
```

在安装有连接器的机器上， WatchList.properties 将包括每个连接器的单独条目。process.name 属性为连接器 ID：

```
process.name[3]=CNN100
…
process.name[4]=CNN101
…
```

如果 WatchList.properties 中的条目和正在运行的进程不匹配，则请重新启动 Identity Synchronization for Windows 守护进程或服务。

如果 WatchList.properties 中的条目少于预期数目 （例如，虽然安装了两个连接器，但只有一个连接器条目），则请检查安装日志，看是否是因安装失败所致。

- **在 Solaris 系统中**：安装日志被写入 /var/sadm/install/logs/ 中
- **在 Windows 系统中**：安装日志被写入 %TEMP% 目录，它是 Local Settings 文件夹的子目录，该文件夹在下面的目录下：

  C:\Documents and Settings\Administrator

注意 在某些 Windows 系统中（如 Windows 2000 Advanced Server），`Local Settings` 文件夹是隐藏文件夹。

要查看此文件夹和 `Temp` 子目录：

1. 打开 “Windows 资源管理器”，然后从菜单条中选择 “工具” > “文件夹选项”。
2. 显示 “文件夹选项”对话框后，选择 “查看”选项卡，并启用 “显示隐藏的文件”选项。

排除子组件故障

使用以下清单排除部署中的子组件的故障：

1. 是否安装了所有子组件？

   安装连接器后必须完成子组件安装：

   - 对于 Active Directory Connector，不安装任何子组件。
   - 对于 Sun Java System Directory Connector，必须在要同步的 Sun Java System Directory Server 上安装 “Directory Server 插件”。
   - 对于 Windows NT Connector，必须在要同步的每个 Windows NT 域的主域控制器上安装 Windows Change Detector 和 Password Filter 子组件。安装 Windows NT Connector 后，将同时安装这两个子组件。

注意 为使 Windows NT SAM Change Detector 子组件有效，必须打开 NT 审计日志。选择 “开始” > “程序” > “管理工具” > “用户管理器”，然后选择 “策略” > “审核策略”。选择 “审核下列事件”，然后选中 “用户和组管理”的 “成功”和 “失败”框。

在 “事件查看器” > “事件日志覆盖”中选择 “事件日志设置”，然后选择 “视需要覆盖事件”。

2. 是否遵循了子组件安装后步骤？

   在 Sun Java System Directory Server 上安装 “Directory Server 插件”后，必须重新启动服务器。在主域控制器上安装 NT Change Detector 和 Password Filter 后，必须重新启动服务器。

3. 子组件是否正在运行？

   安装了 “插件”的 Directory Server 是否正在运行？安装了 Change Detector 和 Password Filter 的 “主域控制器”是否正在运行？

4. 子组件是否已与连接器建立了网络连接？

   在运行连接器的机器上，通过运行 `netstat -n -a` 来检验连接器是否在侦听子组件的连接。以下三个示例分别展示了此命令的三种不同结果。（将连接器配置为侦听端口 9999。）

   a. 连接器正在侦听收到的连接，且子组件已成功连接，这些都是预期的结果：

```
netstat -n -a | grep 9999
      *.9999               *.*    0   0 65536    0 LISTEN
12.13.1.2.44397 12.13.1.2.9999  73620 0 73620    0 ESTABLISHED
12.13.1.2.9999  12.13.1.2.44397 73620 0 73620    0 ESTABLISHED
```

   b. 连接器正在侦听收到的连接，但子组件未进行连接：

```
# netstat -n -a | grep 9999
     *.9999               *.*    0   0 65536    0 LISTEN
```

   确定子组件正在运行后，请在子组件的本地日志中查看是否存在潜在问题。

c. 连接器未侦听收到的连接：

```
# netstat -n -a | grep 9999
<no output>
```

检验是否指定了正确的端口号。检验连接器是否正在运行且处于 “就绪” 状态。在连接器的本地日志中查看是否存在潜在问题。

排除 Message Queue 故障

检验 Sun Java System Message Queue 代理程序是否正在运行。向运行 Message Queue 代理程序的机器和端口发出 `telnet` 命令将返回活动 Message Queue 服务列表：

```
# telnet localhost 7676
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
101 psw-broker 3.0.1
cluster tcp CLUSTER 32914
admin tcp ADMIN 32912
portmapper tcp PORTMAPPER 7676
ssljms tls NORMAL 32913
jms tcp NORMAL 32911
.
Connection closed by foreign host.
```

- 如果输出结果中未列出 “`ssljms tcp NORMAL`” 服务，则请在 Message Queue 日志中查看是否存在潜在问题。如果在 Solaris 中安装了 “核心”，则 Message Queue 代理程序的日志为：

  `/var/imq/instances/psw-broker/log/log.txt`

- 如果在 Windows 中安装了 “核心”，则代理程序的日志为：

  <*installation_root*>\isw-<*machine_name*>\imq\var\instances\isw-broker\log\log.txt

如果 telnet 命令失败，则未运行代理程序或指定了错误的端口。检查代理程序日志中的端口号。在下行中指定代理程序的端口

```
[13/Mar/2003:18:17:09 CST] [B1004]:"Starting the portmapper service using
tcp [ 7676, 50 ] with min threads 1 and max threads of 1"
```

如果未运行代理程序，则可通过运行 /etc/init.d/imq start 在 Solaris 中启动它，或通过启动 iMQ Broker Windows 服务在 Windows 中启动它。

如果要在 Solaris 8 中安装 Message Queue，且要运行 mquinstall 以安装所有软件包，则运行 mqinstall *前*务必设置 IMQ_JAVAHOME，以确保软件采用 Java 的正确版本。

如果尚未安装“核心”，则不必设置 IMQ_JAVAHOME，因为 Identity Synchronization for Windows 安装程序会通知 Message Queue 代理程序使用哪个 JVM。

排除代理程序配置目录通信故障

Message Queue 代理程序针对存储 Identity Synchronization for Windows 配置的 Directory Server 验证客户机。如果代理程序无法连接至此 Directory Server，则没有任何客户机可连接至 Message Queue，且代理程序日志会记录一些 javax.naming 异常，如 “javax.naming.CommunicationException”或 “javax.naming.NameNotFoundException”。

若出现 javax.naming 异常，请执行下列操作

- 检验 /var/imq/instances/isw-broker/props/config.properties 中的所有 imq.user_repository.ldap properties 的值是否都正确。如果存在任何不正确的值，请停止 Message Queue 代理程序，更改并保存文件，然后重新启动代理程序。必须能够从安装代理程序的机器上解析目录服务器主机名。
- 检验 /etc/imq/passfile 中的 imq.user_repository.ldap.password 属性是否正确。
- 在某些情况下，如果根后缀中包含空格，则代理程序无法搜索条目。

排除代理程序内存设置故障

正常运行时， Message Queue 代理程序会占用一定的内存。但在执行 idsync resync 操作期间，代理程序需要更多的内存。如果代理程序达到其内存极限，则未传送的消息便会积聚， idsync resync 操作的速度会明显降低 （或完全停止），而且此后 Identity Synchronization for Windows 可能会没有响应。

当代理程序进入低内存状态时，其日志中会出现以下消息：

```
[03/Nov/2003:14:07:51 CST] [B1089]:In low memory condition, Broker is
attempting to free up resources

[03/Nov/2003:14:07:51 CST] [B1088]:Entering Memory State [B0024]:RED  from
previous state [B0023]:ORANGE - current memory is 1829876K, 90% of total
memory
```

为避免出现这种情况，

- 请将代理程序的内存上限增加到 1 或 2 GB，如 《*Sun Java System 1 2004Q3 Identity Synchronization for Windows 发行说明*》中所述。
- 在执行 idsync resync 操作期间，应将日志级别设为 “信息”。将日志级别更改为 “详细”或更高级别会增加代理程序的负荷，因为这样就需要将更多的日志消息发送到中心记录器。
- 每次为一个 “同步用户列表”运行 idsync resync。

一旦代理程序内存不足，请按以下步骤恢复：

1. 通过检查相应目录中的持久消息存储器来验证代理程序是否积聚了大量未传送的消息。
   - **在 Solaris 中**：/var/imq/instances/psw-broker/filestore/message/
   - **在 Windows 中**：<*installation_root*>\isw-<*machine_name*>\imq\var\instances\isw-broker\filestore\message\

2. 此目录下的每个文件包含一个未传送的消息。如果此目录中的文件超过 10000 个，则表明代理程序积聚了大量的消息。[1] 不然，说明代理程序存在其它问题。
3. 积聚的消息可能只是与 `idsync resync` 操作有关的日志文件，可以安全地将这些文件删除。
4. 按第 181 页的 “启动和停止服务”中所述方法停止 Message Queue 代理程序。
5. 删除持久消息存储器中的所有文件。删除这些文件的最简便的方法就是递归删除 `message/` 目录，之后再重新创建它。
6. 重新启动 Message Queue 代理程序。

按本节中的说明进行操作，确保代理程序不再出现内存不足现象。

排除 SSL 故障

当诊断 SSL 问题时，另请参阅第 11 章，“配置安全性”，该章节介绍了如何在 Identity Synchronization for Windows 的组件间设置 SSL。本节包括：

- 核心组件间的 SSL
- “连接器”与 Directory Server 或 Active Directory 间的 SSL
- Directory Server 插件与 Active Directory 间的 SSL

1. 即使已经传送了所有消息，代理程序也可能会保留最多 10000 个消息文件，以避免创建和删除文件产生性能损失。

核心组件间的 SSL

Identity Synchronization for Windows 安装程序无法检验 “核心”安装期间所提供的 SSL 端口是否正确。如果在 “核心”安装期间键入了错误的 SSL 端口，那么 “核心”组件将无法正常通信。在第一次尝试保存配置之前您可能不会发现问题。“控制台”将显示下列警告：

```
配置已成功保存，但无法通知 “系统管理器”有关该新配置信息。
```

系统管理器日志将包括以下条目：

```
[10/Nov/2003:10:24:35.137 -0600] WARNING 14   example  "Failed to connect
to the configuration directory because "Unable to connect: (-5981)
Connection refused by peer.".Will retry shortly."
```

如果出现这种情况，请卸载 “核心”，然后使用正确的 SSL 端口号重新安装。

“连接器”与 Directory Server 或 Active Directory 间的 SSL

如果连接器无法通过 SSL 连接至 Directory Server 或 Active Directory，则下面的消息会出现在中心错误日志中：

```
[06/Oct/2003:14:02:48.911 -0600] WARNING 14  CNN100 host1  "failed to open
connection to ldaps://host2.airius.com:636."
```

打开 “控制台”并检查 “指定高级安全选项”面板 （参见第 119 页）。

不信任的证书

可从中心审计日志获取更多信息。例如，如果 LDAP 服务器的 SSL 证书不被信任，则会记录下列消息

```
[06/Oct/2003:14:02:48.951 -0600] INFO    14  CNN100 host1  "failed to open
connection to ldaps://host2.airius.com:636, error(91):Cannot connect to the
LDAP server, reason:SSL_ForceHandshake failed:(-8179) Peer's Certificate
issuer is not recognized."
```

大多数情况下， CA 证书未被添加到连接器的证书数据库中。这可通过运行 Directory Server 随附的 `certutil` 程序进行确认。[1]

注意

`SUNWtlsu` 软件包中提供了证书管理实用程序 （如 `certutil`），该软件包不是与 Directory Server 一并捆绑提供的。（可从 Sun Microsystems 免费下载此软件包。）

下载此软件包后，可在以下位置找到 `certutil`：

`/usr/sfw/bin/certutil`

1. 在 Solaris 中运行此命令前，必须将 *<installation_root>*`/lib` 目录添加到 `LD_LIBRARY_PATH` 环境变量中。

在本例中，证书数据库中不包含任何证书：[1]

```
# /usr/sunone/servers/shared/bin/certutil -L -d /usr/sunone/servers/
isw-host1/etc/CNN100
Certificate Name                                 Trust Attributes
p    Valid peer
P    Trusted peer (implies p)
c    Valid CA
T    Trusted CA to issue client certs (implies c)
C    Trusted CA to certs(only server certs for ssl) (implies c)
u    User cert
w    Send warning
```

在下例中，证书数据库中仅包含 Active Directory CA 证书：

```
# /usr/sunone/servers/shared/bin/certutil -L -d /usr/sunone/servers/
isw-host1/etc/CNN100
Certificate Name                                 Trust Attributes
airius.com CA                                    C,c,
p    Valid peer
P    Trusted peer (implies p)
c    Valid CA
T    Trusted CA to issue client certs (implies c)
C    Trusted CA to certs(only server certs for ssl) (implies c)
u    User cert
w    Send warning
```

1. Sun Java System Directory Server 和 Windows NT Connector 的默认证书数据库中包含两个证书，即 `saint-cert100` 和 `saintRootCA`。此版本中不使用这些证书。

如此处所显示， CA 证书的信任标志必须为 “C,,”。如果证书存在且正确设置了信任标志，但仍无法连接连接器，请首先检查添加证书后是否重新启动了连接器，然后借助 Sun Java System Directory 自带的 ldapsearch 命令诊断问题。如果 ldapsearch 不接受该证书，则连接器也不会接受。例如，如果证书不被信任，则会被 ldapsearch 拒绝。

```
# /usr/sunone/servers/shared/bin/ldapsearch -Z -P /usr/sunone/
servers/isw-host1/etc/CNN100 -h host2 -b "" -s base "(objectclass=*)"
ldap_search:Can't contact LDAP server
    SSL error -8179 (Peer's Certificate issuer is not recognized.)
```

-P 选项指示 ldapsearch 使用连接器 CNN100 的证书数据库进行 SSL 证书验证。将正确的证书添加到连接器的证书数据库后，检验 ldapsearch 是否接受该证书，然后重新启动连接器。

不匹配的主机名

当 Identity Synchronization for Windows 尝试建立 SSL 连接时 （禁用信任所有证书设置）， Identity Synchronization for Windows 的 “连接器”将检验服务器的主机名是否与服务器在 SSL 协商阶段所提供的证书中的主机名相匹配。若主机名不相匹配，则连接器将拒绝建立连接。

Identity Synchronization for Windows 配置中的目录源主机名必须始终与该目录源使用的证书中嵌入的主机名相符。

可使用 ldapsearch 来检验主机名是否匹配，如下所示：

```
/var/mps/serverroot/shared/bin/ldapsearch.exe -Z -P
/var/opt/SUNWisw/etc/CNN100 -3
-h host2.example.com -p 636 -s base -b "" "(objectclass=*)"
```

若命令行 (host2.example.com) 中的主机名与证书中所嵌入的主机名不匹配，则会显示以下错误消息：

```
ldap_search:Can't contact LDAP server
SSL error -12276 (Unable to communicate securely with peer: requested do
main name does not match the server's certificate.)
```

若主机名匹配，则将成功运行 ldapsearch 命令并显示根 DSE 的内容。

到期的证书

如果服务器的证书已到期，则会记录下列消息

```
[06/Oct/2003:14:06:47.130 -0600] INFO    20  CNN100 host1  "failed to open
connection to ldaps://host2.airius.com:636, error(91):Cannot connect to the
LDAP server, reason:SSL_ForceHandshake failed:(-8181) Peer's Certificate has
expired."
```

此时，必须为服务器发放新证书。

Directory Server 插件与 Active Directory 间的 SSL

默认情况下，在执行即时请求密码同步过程中， Directory Server 不通过 SSL 与 Active Directory 通信。如果改写默认值以保护此通过 SSL 进行的通信，则必须如第 11 章，“配置安全性”中所述，将 Active Directory CA 证书添加到每个主副本的 Directory Server 证书数据库中。如果不添加此证书，会出现 “执行 DSA 困难”错误而无法将用户绑定到 Directory Server，并且 “插件”的日志 （例如，isw-*<hostname>*/logs/SUBC100/pluginwps_log_0.txt）将报告下列信息：

```
[06/Nov/2003:15:56:16.310 -0600]  INFO    td=0x0376DD74 logCode=81
ADRepository.cpp:310    "unable to open connection to Active Directory
server at ldaps://host2.airius.com:636, reason: "
```

此时，必须将 Active Directory CA 证书添加到 Directory Server 的证书数据库中，然后重新启动 Directory Server。

排除控制器故障

从备份文件恢复 Active Directory 域控制器时，某些计数器不会被重置。

为确保正确重置所有计数器，请在恢复 Active Directory 域控制器后重新同步所有用户。

第 10 章

了解审计和错误文件

Identity Synchronization for Windows 提供有关安装和配置状态、日常系统操作以及与部署有关的任何错误状况的信息。

本章通过以下各节内容介绍如何获取和了解此信息：

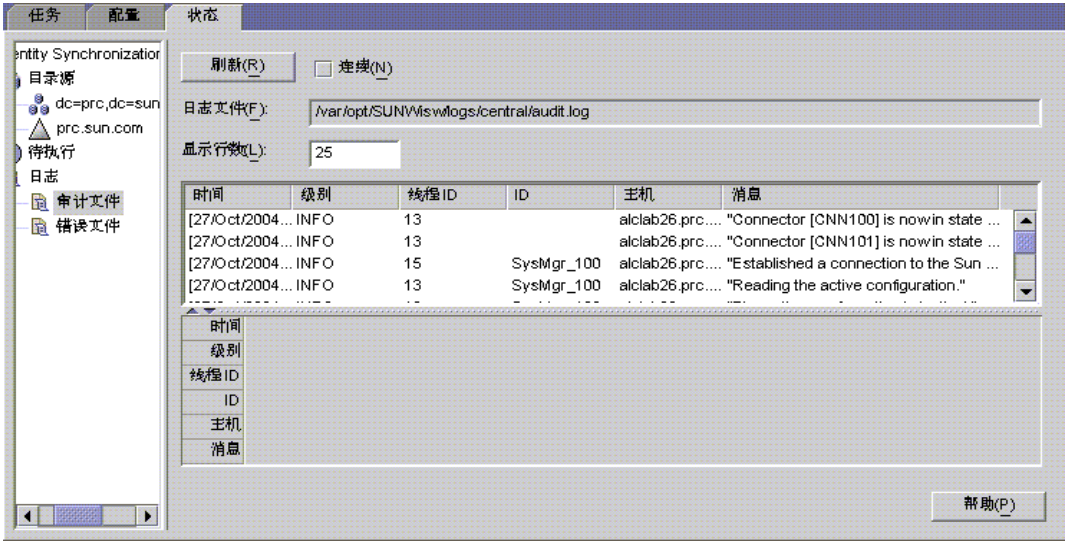
了解日志

可从 “Identity Synchronization for Windows 控制台” 的 “状态” 选项卡查看各类信息。

如果在导航树窗格 （位于左侧）中选择下列节点之一，“状态” 选项卡中显示的内容会发生变化，以提供特定于该项目的信息。

- **目录源**：选择一个目录源节点 （例如， dc=example,dc=com）查看该目录源的状态信息。
- **待执行**：选择此节点可显示一个步骤列表，要成功安装和配置 Identity Synchronization for Windows 必须完成这些步骤 （程序会以灰色显示所有已完成步骤）。
- **审计文件**：选择此节点可获取有关日常系统操作的信息 （包括错误状况）。
- **错误文件**：选择此节点可获取有关系统错误状况的信息。（“错误日志” 实际相当于一个过滤器，其中只显示错误条目。）

图 10-1 状态选项卡



日志类型

本节介绍 Identity Synchronization for Windows 可用的不同类型日志：

中心日志

只要各 Identity Synchronization for Windows 组件能访问 Message Queue，所有审计和错误消息就将被记录在 Identity Synchronization for Windows 中心记录器中。因此，这些中心日志 （其中包括来自所有组件的消息）是应监视的主要日志。

这些集中的日志位于安装了 “核心”的机器的以下目录中：

- **在 Solaris 中：** `/var/opt/SUNWisw/logs`
- **在 Windows 中：** *<installation_root>*`/isw-`*<machine_name>*`/logs/central/`

具体日志在表 10-1 中介绍。

表 10-1 Identity Synchronization for Windows 日志类型

日志名称	说明
`error.log`	用于报告 “警告”和 “严重”类消息。
`audit.log`	`error.log` 的超集，包含关于每个同步事件的消息。
`resync.log`	由 `resync` 命令生成的消息在此处报告。

每个中心日志还包含关于每个组件 ID 的信息。例如：

```
[2003/03/14 14:48:23.296 -0600] INFO 13 "System Component
Information:SysMgr_100 is the system manager (CORE);  console is the Product
Console User Interface;  CNN100 is the connector that manages [airius.com
(ldaps:// server1.airius.com:636)];  CNN101 is the connector that manages
[dc=airius,dc=com (ldap:// server2.airius.com:389)];"
```

除了中心记录器，每个组件还有自己的本地日志。如果连接器不能向中心记录器写入记录时，可使用这些本地日志来诊断连接器故障。

本地组件日志

每个连接器、系统管理器和中心记录器都含有以下本地日志：

表 10-2 本地日志

日志名称	说明
audit.log	error.log 的超集，包含关于每个同步事件的消息。这些消息也被写入到中心 audit.log。
error.log	用于报告 “警告”和 “严重”类消息。这些消息也被写入中心 error.log。

这些中心日志位于以下子目录中：

- **在 Solaris 中：**/var/opt/SUNWisw/logs
- **在 Windows 中：**<*installation_root*>/isw-<*machine_name*>/logs/central/

sysmgr 和 clogger100 （中心记录器）目录在安装了 “核心”的机器上。

Identity Synchronization for Windows 每天循环使用这些本地组件日志，这是通过将当前日志移动到包含日期的日志文件而实现的，形式如下：

audit_2004_08_06.log

注意 默认情况下， Identity Synchronization for Windows 会删除十天之前的连接器日志。编辑文件 Log.properties 中的 com.sun.directory.wps.logging.maxmiumDaysToKeepOldLogs 值然后重新启动服务守护进程，可延长此时间长度。

本地 Windows NT 子组件日志

以下 Windows NT 子组件也具有本地日志：

- Windows NT Change Detector DLL
- Password Filter DLL

这些子组件日志位于以下目录的 SUBC1XX （例如 SUBC100）子目录中：

<*installation_root*>/isw-<*machine_name*>/logs/

Identity Synchronization for Windows 将这些文件的大小限制为不能超过 1 MB，且只保留最后 10 个日志。

Directory Server 插件日志

Directory Server 插件通过 Directory Server 连接器将信息记录到中心日志，也通过 Directory Server 记录工具进行日志记录。因此，本地 Directory Server 插件日志消息也将被保存到 Directory Server 错误日志中。

Directory Server 将来自其它 Directory Server 插件和组件的信息保存到错误日志中。为了确定来自 Identity Synchronization for Windows Directory Server 插件的消息，可以筛选出包含字符串 `isw` 的行。

默认情况下，错误日志中只显示最小的 “插件”日志消息。
例如：

```
[14/Jun/2004:17:08:36 -0500] - ERROR<38747> - isw - conn=-1 op=-1 msgId=-1
- Plugins unable to establish connection to DS Connector at attila:1388,
will retry later
```

可从 “Directory Server 管理控制台”更改 Directory Server 错误日志的默认详细程度级别，具体步骤如下：

1. 打开 “Directory Server 控制台”。
2. 选择 “配置”选项卡。
3. 在导航窗格中单击 “日志”节点。
4. 选择 “错误”选项卡。
5. 单击 “日志级别”按钮。
6. 启用 “插件”框。为了达到更详细的程度，也可以启用 “详细模式”。
7. 单击 “确定”，然后单击 “保存”。

有关 Directory Server 日志记录的详细信息，请参阅 《*Sun Java System Directory 5 2004Q2 Server Administrator's Guide*》
(http://docs.sun.com/db/coll/DirectoryServer_04q2)。

读取日志

每条日志消息都包含以下信息：

- **时间**：指出日志条目在何时 （时间和日期）生成。例如：

  ```
  [13/Aug/2004:06:14:36:753 -0500]
  ```

- **级别**：指出日志消息的严重程度和详细程度。
  Identity Synchronization for Windows 使用以下日志级别：

表 10-3 日志级别

日志级别	说明
信息	这些消息提供关于每个操作的最少量的信息，因此系统可正常运行。例如，其中有何时检测到更改及何时发生同步的信息。这些消息始终记录到审计日志中。
详细	这些消息包含操作在系统中进行期间的较多有关信息。
更详细	这些消息包含操作在系统中进行期间的更多有关信息。将所有组件的日志级别设置为 “更详细”会对性能产生影响。
最详细	这些消息包含操作在系统中进行期间的最多有关信息。将所有组件的日志级别设置为 “最详细”会极大地影响性能。

- **线程 ID**：显示引发事件的函数的 Java 线程 ID。
- **ID**：表明引发事件的组件 （控制台、系统管理器等）。
- **主机**：显示引发事件的主机的名称。
- **消息**：显示与该事件相关的审计或错误信息。
  示例包括：

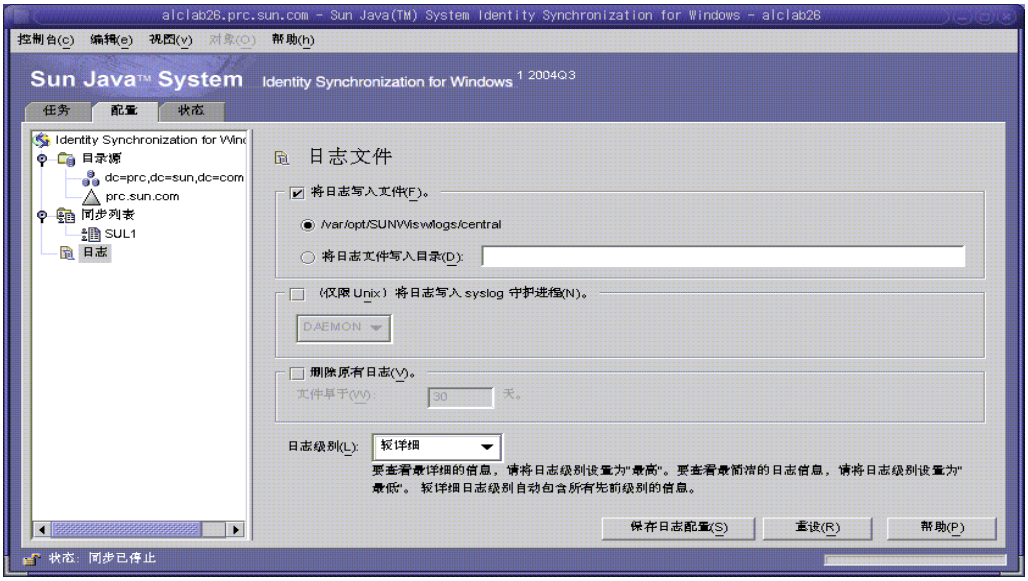
  ```
  "Resetting Central Logger configuration ..."
  "System manager is shutting down."
  "Processing request (ID=<ID_number> from the console to stop
  synchronization."
  ```

配置日志文件

可以使用 “Identity Synchronization for Windows 控制台”为您的部署配置日志记录，如下所示：

1. 打开 “控制台”，然后选择 “配置”选项卡。
2. 在导航树窗格中展开节点，直到出现 “日志”节点为止。
3. 选择该 “日志”节点，“配置”选项卡中显示 “日志文件”面板 （参见 图 10-2）。

图 10-2 配置日志文件



4. 使用 “日志文件”面板配置日志文件，方法如下：
   - **将日志写入文件。**启用此选项可将日志写入 “核心”主机上的文件。

     选择此选项后，您可以：

     - 启用默认日志目录和文件 （例如，`/var/opt/SUNWisw/logs/central`）。
     - 启用 “将日志文件写入目录”选项，然后指定日志文件的路径和文件名。

注意 控制台不会验证指定的日志文件位置是否真正存在。如果日志目录不存在，中心记录器将尝试创建日志目录。因此，在您尝试查看日志之前，不会有指示说明您指定并保存了不存在的日志位置。经过几次查看日志的尝试后，会出现一条消息，报告控制台在指定位置找不到日志。

- *仅限 Solaris* — **将日志写入 syslog 守护进程**：如果 Identity Synchronization for Windows 驻留在 Solaris 平台上，则启用此选项。
使用下拉列表可选择书写日志的类别。（*默认值为 DAEMON*。）

注意 如果选中此选项， Identity Synchronization for Windows 将全部信息都记录到 syslog 中；但是，默认情况下 syslog 被配置为只记录 “警告” 和 “严重” 消息。

要将 syslog 配置为记录 “信息” 类消息，请编辑 /etc/syslog.conf，并将以下行：

```
*.err;kern.debug;daemon.notice;mail.crit
/var/adm/messages
```

更改为：

```
*.err;kern.debug;daemon.notice;daemon.info;mail.crit
/var/adm/messages
```

做此更改后，必须重新启动 syslog 守护进程，如下所述：

```
/etc/init.d/syslog stop ; /etc/init.d/syslog start
```

要启用 “详细”、“更详细” 和 “最详细” 日志记录，请在分号分隔的列表中包含 daemon.debug。

- **删除原有日志**：日志文件的数量无限持续增长 （每天 1 个）。为了避免用尽磁盘空间，请启用此选项并指定程序可在何时从中心日志文件中删除原有日志。

  例如，如果指定 30 天， Identity Synchronization for Windows 将在文件生成 31 天后删除它们。

- **日志级别**。使用下拉列表可选择要在系统日志中查看的详细级别。（请查看第 271 页的 “日志级别”。）

5. 单击 “保存日志配置” 按钮，根据所选选项创建日志文件。

查看目录源状态

要查看目录源的状态：

1. 在 “Identity Synchronization for Windows 控制台”中，选择 “状态”选项卡。
2. 在导航树窗格中，展开 “目录源”节点，然后选择目录源节点 （例如，dc=example,dc=com）。

   “状态”选项卡的内容发生变化，提供与选定目录源有关的信息 （例如，参见图 10-3）。

图 10-3 目录源状态

注意 查看 “目录源”状态时，实际上是在查看与该 “目录源”关联的连接器的状态。

“状态”选项卡提供下列信息：

- **更新：**单击 “更新”可刷新此选项卡中的信息。
- **状态：**反映目录源的当前状态。有效状态包括：
  - **尚未安装：**未安装连接器。
  - **已安装：**已安装连接器，但因尚未接收到其运行时配置，所以未做好同步准备。如果连接器在此状态停留超过一分钟，则可能是某处出现了故障。
  - **就绪：**连接器已做好同步准备，但目前未同步任何对象。如果尚未启动同步，或者虽已启动同步但并非所有子组件都与连接器建立了连接，则连接器会保持 “就绪”状态。

- **正在同步：**连接器正在同步对象。可能仍有错误，因此若发现更改未同步，请参考错误日志。

- **活动的：**表明目录源是否处于活动状态。
- **上一次通信：**指出此目录源的连接器上次发出响应的时间。

查看安装和配置状态

要查看还必须完成 Identity Synchronization for Windows 安装和配置过程的哪些步骤，请按下列过程操作：

1. 在 “Identity Synchronization for Windows 控制台”中，选择 “状态”选项卡。
2. 在导航树窗格中，展开 “待执行”节点。

   “状态”选项卡的内容发生变化，提供安装和配置步骤的清单 （例如，参见图 10-3）。

图 10-4 查看 “待执行”列表

3. 单击 “更新”按钮 （右上角）刷新该列表。

   完成的步骤带有选中标记，并且以灰色显示。必须完成其余步骤才能成功完成安装和配置过程。

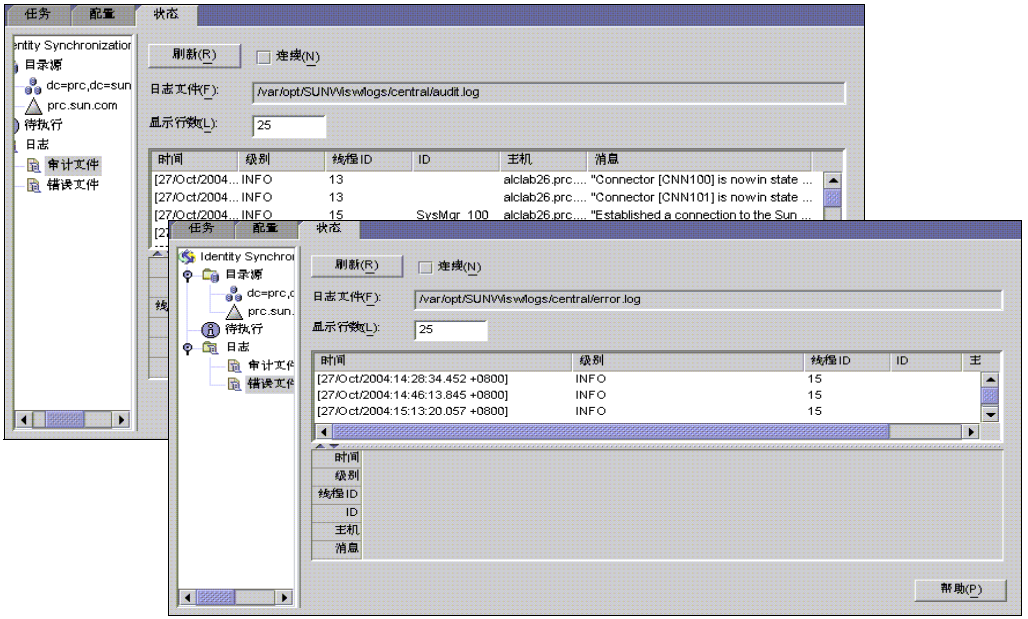
查看审计和错误日志

要查看错误日志：

1. 在 “Identity Synchronization for Windows 控制台”中，选择 “状态”选项卡。
2. 在导航树窗格中，展开 “审计文件”或 “错误文件”节点。

   “状态”选项卡的内容发生变化，显示当前日志 （图 10-5）。

图 10-5 查看日志



“状态”选项卡提供下列信息：

- **刷新**：加载最新的审计或错误信息。
- **连续**：连续更新和显示最新的审计或错误信息。
- **日志文件**：显示读取的审计或错误日志的完整路径名。例如：

  `C:\Program Files\Sun\MPS\isw-`*`hostname`*`>\logs\central\audit.log`
- **显示行数**：指定要显示的审计或错误条目数。（*默认值为 25*。）

在 Windows NT 机器上启用审计

如果您的部署中有一台 Windows NT 机器，请核实是否启用了审计，否则 Identity Synchronization for Windows 不能记录来自该机器的消息。

可按以下过程在 Windows NT 机器上启用审计日志记录：

1. 在 Windows NT 的“开始”菜单中，为“域”选择“程序”>“管理工具”>“用户管理器”。
2. 显示“用户管理器”对话框后，从菜单栏中选择“策略”>“审核”。

   将显示“审核策略”对话框。
3. 启用“审核下列事件”按钮，然后启用“成功”和“失败”框。
4. 单击“确定”关闭该对话框。

这些设置在再次更改之前始终有效。

第 11 章

配置安全性

本章提供有关为部署配置安全性的重要信息。内容具体安排如下：

注意 本章假设您熟悉公共密钥密码学和 “安全套接字层” (SSL) 协议的基本概念，并了解内联网、外联网和 Internet 安全的概念以及数字证书在企业中的作用。如果您不了解这些概念，请参阅手册 《*Managing Servers with iPlanet Console 5.0*》中与安全相关的附录。

安全性概述

密码是敏感信息；因此， Identity Synchronization for Windows 采取安全预防措施来确保用于访问要同步目录的用户和管理密码证书的安全。

本节涵盖了以下安全方法：

- 第 281 页的 “指定配置密码”
- 第 281 页的 “使用 SSL”
- 第 282 页的 “已生成的 3DES 密钥”
- 第 282 页的 “SSL 和 3DES 密钥保护概要”
- 第 284 页的 “Message Queue 访问控制”
- 第 284 页的 “目录证书”
- 第 285 页的 “持久存储保护概要”

此安全方法旨在防止下列事件发生：

- 窃听者通过网络截取明文密码
- 攻击者操纵连接器将用户密码更改为他们所选择的值，这等价于捕获用户的明文密码
- 攻击者获得对 Identity Synchronization for Windows 的特权组件的访问权
- 无特权的用户从磁盘上存储的文件恢复密码
- 入侵者从硬盘上恢复已从系统的某个组件删除的密码。这可能是被同步的密码，或者可能是用于访问某个目录的系统密码。

指定配置密码

为了在敏感信息存储在产品配置目录期间以及通过网络传输期间对其进行保护，Identity Synchronization for Windows 使用*配置密码*。管理员在安装 “核心”时指定配置密码，而且在打开 “控制台”或运行 Identity Synchronization for Windows 安装程序时必须提供此密码。

注意 系统管理器必须先访问配置密码，然后才能将其传递到连接器，这样系统管理器才会将此密码存储在其初始化文件中。

文件系统访问控制会防止无特权用户访问系统管理器的初始化文件。Identity Synchronization for Windows 安装程序不对此密码强制实施密码策略。

要在选择配置密码时提高安全性，请参阅第 286 页的 “加强安全性”。

使用 SSL

可将 Identity Synchronization for Windows 配置为在组件使用 LDAP 的任何位置使用基于 SSL 的 LDAP。所有对 Message Queue 的访问均通过 SSL 进行保护。

从 Directory Server 同步到 Active Directory 时，必须在 Active Directory Connector 和 Active Directory 之间使用 SSL。

需要信任 SSL 证书

默认情况下，配置为使用 SSL 的连接器将接受服务器 （即 Directory Server 或 Active Directory）返回的任何 SSL 证书 — 包括非信任证书、到期证书及无效证书。连接器和服务器之间的所有网络通信都将被加密，但是连接器检测不出模仿真实 Active Directory 或 Directory Server 的服务器。

要强制连接器只接受信任证书，请使用 “控制台”在 “目录源配置”向导的 “指定高级安全选项”面板中启用 “需要信任 SSL 证书”选项 （请参阅第 119 页）。启用此选项之后，必须将适当的 CA 证书添加到 `idsync certinfo` 报告的连接器证书数据库中。

已生成的 3DES 密钥

从配置密码生成的 3DES 密钥用于保护产品配置目录中的所有敏感信息。除日志消息外，传送至 Message Queue 的所有消息均采用了每主题 3DES 密钥加密方式。在连接器和子组件之间发送的消息会采用每会话 3DES 密钥加密方式。 Directory Server 插件采用 3DES 密钥方式对所有用户密码更改进行加密。

SSL 和 3DES 密钥保护概要

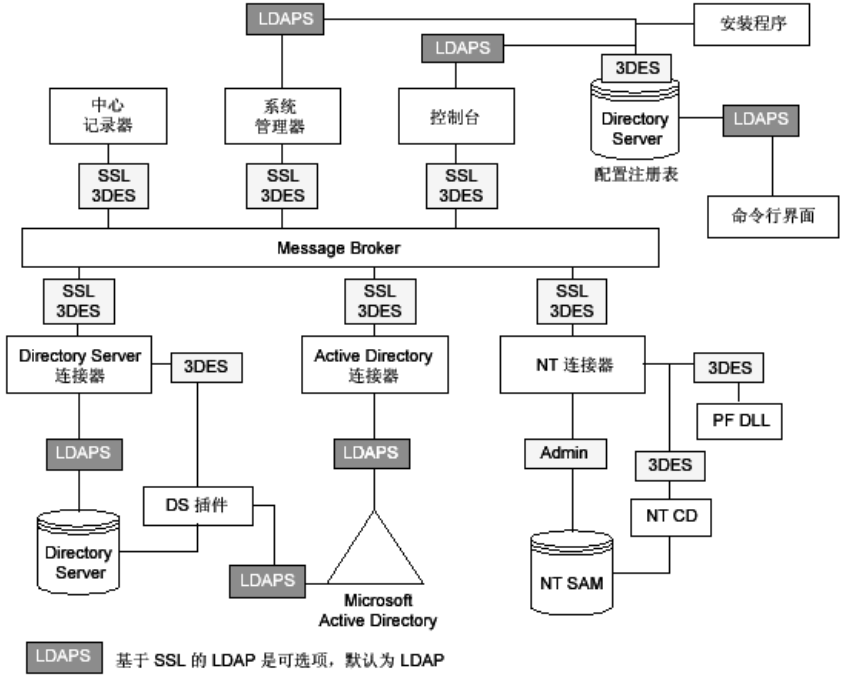
表 11-1 概述了 Identity Synchronization for Windows 如何保护通过网络发送的敏感信息。

表 11-1 利用网络安全保护敏感信息

使用此保护方法	在下列信息类型之间：
基于 SSL 的 LDAP （可选）	• Directory Server Connector 和 Directory Server、 Active Directory Connector 和 Active Directory • Directory Server 插件和 Active Directory • 命令行界面和产品的配置目录 • “控制台”和产品的配置目录 • “控制台”和 Active Directory 全局目录 • “控制台”和 Active Directory 域或要同步的 Directory Server • Message Queue 代理程序和产品的配置目录 • 连接器、系统管理器、中心记录器、命令行界面和 “控制台”可能会通过 LDAPS 验证 Message Queue • 安装程序和配置目录服务器 • 安装程序和 Active Directory • 安装程序和要同步的 Directory Server
利用 3DES 密钥加密 （默认值）	• Directory Server Connector 和 Directory Server 插件 （所有数据） • Windows NT Connector、 Windows NT Password Filter DLL 和 Windows NT Change Detector （所有数据） • 产品配置目录中的所有敏感信息 • 连接器和子组件之间发送的所有消息 （采用每会话 3DES 密钥进行加密） • 经由 Message Queue 发送的所有 （非日志）消息

图 11-1 概括说明了本节中所讨论的安全功能。

图 11-1 Identity Synchronization for Windows 安全性概述



Message Queue 访问控制

Identity Synchronization for Windows 使用 Message Queue 的访问控制来防止在未经授权的情况下对消息订阅和消息发布进行访问，从而允许各连接器信任收到的消息。

访问 Message Queue 代理程序时，将提供只有 Message Queue 和连接器识别的唯一用户名和密码。经由 Message Queue 发送的每条消息均采用每主题 3DES 密钥方式加密，从而保护消息内容，以防止不知道主题密钥的外来者发送有实际意义的消息。这些措施可防止 (a) 攻击者将虚假密码同步消息发送到连接器，以及 (b) 攻击者假冒连接器接收真实的密码更新。

注意 默认情况下， Message Queue 的客户机 （如连接器和系统管理器）将接受 Message Queue 代理程序返回的任何 SSL 证书。有关增强 Message Queue 证书验证功能及其它与 Message Queue 相关的安全问题的详细信息，请参阅第 286 页的 “加强安全性”。

目录证书

连接器必须具有特权证书，才能更改 Active Directory 和要同步的 Directory Server 中的密码。在将这些特权证书存储到产品配置目录中之前会对其进行加密。

持久存储保护概要

表 11-2 概述了 Identity Synchronization for Windows 如何保护存储在磁盘上的敏感信息。

表 11-2 持久存储保护

持久存储	机密信息	保护
存储在配置目录服务器中的产品配置	在产品的配置目录中存储用于访问各目录的证书和每个 Message Queue 主题的 3DES 密钥。	存储在产品配置目录中的所有敏感信息均采用了从配置密码生成的 3DES 密钥进行加密。有关进一步保护产品配置目录的建议，请参阅 “加强安全性”。
Directory Server Retro Changelog	Directory Server 插件捕获密码更改，并在写入 Directory Server Retro Changelog 之前对这些密码更改进行加密。	Directory Server 插件会采用每个部署所独有的 3DES 密钥对所有用户密码更改进行加密。
Message Queue 代理程序持久存储	Message Queue 代理程序将存储在所有连接器之间发送的密码同步消息。	除日志消息外，所有持久消息均以每主题 3DES 密钥方式加密。
Message Queue 代理程序目录证书	Message Queue 代理程序将根据产品的配置目录来验证用户。它使用在 “核心”安装期间提供的目录管理用户名和密码连接到配置目录。	目录密码被存储在利用文件系统访问控制进行保护的 passfile 中。
系统管理器引导文件	系统管理器的引导文件包含访问该配置的信息。其中包括 “核心”安装期间所提供的配置密码和目录管理用户名和密码。	该文件通过文件系统访问控制进行保护。
连接器和中心记录器引导文件	每个连接器及中心记录器均有一个初始配置文件，其中包含用于访问 Message Queue 的证书。	这些文件通过文件系统访问控制进行保护。
Directory Server 插件引导配置	该 “插件”的配置 （存储在 cn=config 中）包括用于连接到连接器的证书。	cn=config 子树通过 ACI 进行保护，而镜像此树的 `dse.ldif` 文件则通过文件系统访问控制进行保护。
NT Password Filter 和 NT Change Detector 引导配置	存储在 Windows 注册表中的 NT 子组件的配置包含了用于连接到相应连接器的证书。	如果对 PDC 注册表的访问未受到保护，则可通过访问控制保护这些注册表主键。
Windows Connector 的对象高速缓存	Windows 连接器将散列的用户密码存储在连接器的对象高速缓存中。	这些密码不以明文形式存储，而是采用 MD5 散列方法进行了加密。这些数据库文件通过文件系统访问控制进行保护。（请参阅 “加强安全性”。）

加强安全性

本节描述了本产品当前版本中存在的潜在安全缺陷以及有关如何在本产品默认配置之外扩展和加强安全性的建议。它包括以下内容：

配置密码

配置密码用于保护敏感的配置信息，但安装程序不会对此密码强制实施任何密码策略；请确保此密码遵循某些严格的指导方针，选择不易破解的复杂密码，并遵循重要密码的标准策略指导方针。

例如，其长度至少应为八个字符，其中包括大写字母、小写字母和非字母数字字符。它不应包括您的姓名、姓名首字母或日期。

创建配置目录证书

要访问产品配置目录所在的 Directory Server，您的证书必须处于 “配置管理员”组中。但是，如果出于某种原因需要创建 *admin* 证书之外的证书，请考虑下列事项：

安装程序会要求您为存储在 “控制台”管理子树中的用户提供证书。但是，“核心”安装程序不会将非 *admin* 用户扩展到 “`uid=admin,ou=Administrators, ou=TopologyManagement, o=NetscapeRoot`”。因此，必须在 “核心”安装期间指定整个 DN。

要创建新的非 *admin* 用户：

1. 在以下容器中创建用户

   ```
   ou=Administrators, ou=TopologyManagement, o=NetscapeRoot
   ```

2. 向 “配置管理员”组添加新证书

3. 对 ACI 进行设置，使其仅允许此用户或 “配置管理员”组中的所有用户访问存储产品的配置目录的 Directory Server。
4. 在 “核心”安装期间指定整个 DN

   有关在 Directory Server 中管理访问控制的详细信息，请参阅《*Sun Java System Directory Server 5 2004Q2 Administrator's Guide*》第 6 章：“管理访问控制”。

Message Queue 客户机证书验证

默认情况下，Message Queue 的客户机（如连接器和系统管理器）将接受 Message Queue 代理程序返回的任何 SSL 证书。

1. 要覆盖此设置并强制 Message Queue 客户机验证 Message Queue 代理程序的证书，请编辑：

   <*installation_root*>/resources/WatchList.properties

2. 将以下内容添加到 Watchlist.properties 的每个进程的 JVM 参数中：

   -Djavax.net.ssl.trustStore=<*keystore_path*> -DimqSSLIsHostTrusted=false

3. 重新启动 Identity Synchronization for Windows 守护进程或服务。

javax.net.ssl.trustStore 属性应指向信任代理程序证书的 JSEE keystore，例如，可在装有 “核心”的机器上使用 /etc/imq/keystore，因为这与代理程序所用的 keystore 相同。

Message Queue 自签名 SSL 证书

默认情况下， Message Queue 代理程序使用自签名 SSL 证书。要安装不同的证书，请使用随 Java 提供的 keytool 实用程序来修改该代理程序的 keystore （在 Solaris 上为 /var/imq/instances/isw-broker/etc/keystore，而在 Windows 2000 上为 <*mq_installation_root*>/var/instances/isw-broker/etc/keystore）。该证书的别名必须是 imq。

访问 Message Queue 代理程序

默认情况下， Message Queue 使用除了它的端口映射器之外的动态端口进行所有服务。要通过防火墙访问该代理程序或对可连接到该代理程序的主机集进行限制，该代理程序应使用固定端口进行所有服务。

这可以通过设置 `imq.<service_name>.<protocol_type>.port` 代理程序配置属性来实现。有关详细信息，请参阅 《*Sun Java System Message Queue Administrator's Guide*》。

配置目录证书验证

在通过 SSL 连接到产品配置目录时，系统管理器将接受任何证书；在通过 SSL 连接到产品配置目录时， Message Queue 代理程序将接受任何证书。当前，没有任何方法可以使系统管理器或 Message Queue 代理程序验证产品的配置目录 SSL 证书。

限制对配置目录的访问

安装 “核心”后，在将信息添加到存储产品的配置目录的 Directory Server 的过程中，不包括添加任何访问控制信息。要将访问权限仅限于配置管理员，可使用以下 ACI：

```
(targetattr = "*") (target =
"ldap:///ou=IdentitySynchronization,ou=Services,dc=example,dc=com")
(version 3.0;acl "Test";deny (all)(groupdn != "ldap:///cn=Configuration
Administrators, ou=Groups, ou=TopologyManagement, o=NetscapeRoot");)
```

有关在 Directory Server 中管理访问控制的详细信息，请参阅 《*Sun Java System Directory Server 5 2004Q2 Administrator's Guide*》第 6 章：“管理访问控制”。

保护复制配置

使用复制连接到 Directory Server 的部署将遵循在安全性概述中确定的相同规则。本节给出一个复制配置的示例，并说明如何在此配置中启用 SSL。

注意 有关规划、部署和保护复制配置的概述，请参阅附录 E，“复制环境的安装注意事项”。

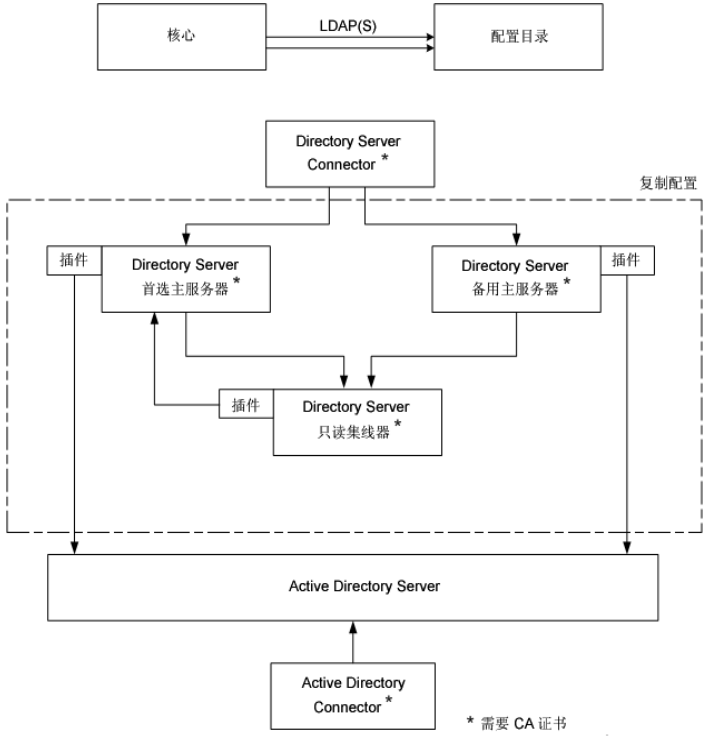
表 11-3 列出需要 CA 证书的配置组件并确定何处需要何种证书。

表 11-3 需要 CA 证书的 MMR 配置组件

组件	需要 CA 证书
首选 Directory Server 复制主服务器	Active Directory 系统
备用 Directory Server 复制主服务器	Active Directory 系统
只读 Directory Server 集线器	首选 Directory Server 复制主服务器 备用 Directory Server 复制主服务器
Directory Server Connector	首选 Directory Server 复制主服务器 备用 Directory Server 复制主服务器
Active Directory Connector	Active Directory 系统

图 11-2 显示在 MMR 配置中安装的 Identity Synchronization for Windows，其中有两台复制 Directory Server 主服务器和多个 Directory Server 只读集线器或用户服务器。每个 Directory Server 有一个 “插件”，而且只有一个 Directory Server Connector、一个 Active Directory 系统和一个 Active Directory Connector。

图 11-2 复制配置



注意 在配置 Directory Server 源以使用 SSL 时，必须确保副本 Directory Server 同时信任首选和备用 Directory Server 的证书。对于安装在具有 Directory Server 集线器或只读副本的系统上的 `other` 类型的每个 Directory Server 插件亦是如此。

Directory Server 插件有权访问与相关的 Directory Server 相同的 CA 证书。

使用 idsync certinfo

使用 `idsync certinfo` 实用程序根据当前的 Identity Synchronization for Windows SSL 设置确定需要什么证书。执行 `idsync certinfo` 以检索有关每个证书数据库需要哪些证书的信息。

注意 您必须确保当配置 Directory Server 源以使用 SSL 时，所有 “目录” 子组件或 “插件” 的副本 Directory Server 同时信任首选和备用 Directory Server 源证书。

如果 Identity Synchronization for Windows 尝试建立 SSL 连接 （启用信任所有证书设置），而服务器的主机名与服务器在 SSL 协商阶段提供的证书中的主机名不符，则 Identity Synchronization for Windows Connector 将拒绝建立连接。

Identity Synchronization for Windows 配置中的目录源主机名必须始终与该目录源使用的证书中嵌入的主机名相符。

参数

表 11-4 描述了可与 `idsync certinfo` 子命令一同使用的参数：

表 11-4 certinfo 参数

参数	说明
`-h` <*CR-hostname*>	指定配置目录主机名。此参数的默认值为 “核心” 安装期间指定的值。
`-p` <*CR-port-no*>	指定配置目录 LDAP 端口号。（*默认值为 389*。）
`-D` <*bind-DN*>	指定配置目录绑定识别名 (DN)。此参数的默认值为 “核心” 安装期间指定的值。
`-w` <*bind-password* | `->`	指定配置目录绑定密码。 - 值从标准输入 (`STDIN`) 中读取密码。
-s <*rootsuffix*>	指定配置目录根后缀。根后缀是识别名，如 `dc=example,dc=com`。此参数的默认值为 “核心” 安装期间指定的值。
`-q` <*configuration_password*>	指定配置密码。 - 值从标准输入 (`STDIN`) 读取密码。

用法

以下示例使用 idsync certinfo 来搜索被指定在 SSL 通信下运行的系统组件。此示例的结果确定了两个连接器 （CNN101 和 CNN100），并提供有关在何处导入相应 CA 证书的说明。

```
:\Program Files\Sun\MPS\isw-hostname\bin> idsync certinfo -h CR-hostname
-p 389 -D "cn=Directory Manager" -w dirmanager -s dc=example,dc=com
-q <password>
Connector:CNN101
Certificate Database Location:C:\Program
Files\Sun\MPS\isw-hostname\etc\CNN101
Get 'Active Directory CA' certificate from Active Directory and import into
Active Directory Connector certificate db for server
ldaps::/hostname.example.com:636
Connector:CNN100
Certificate Database Location:C:\Program
Files\Sun\MPS\isw-hostname\etc\CNN100
Export 'Directory Server CA' certificate from Directory Server certificate
db and import into Directory Server Connector certificate db
ldaps://hostname.example.com:636
Export 'Active Directory CA' certificate from Active Directory Server
hostname.example.sun.com:389 and import into Directory Server Server
certificate db for server ldaps://hostname.example.com:638
SUCCESS
```

在 Directory Server 中启用 SSL

请按照以下步骤使用自签名证书在 Directory Server 中启用 SSL。

注意 以下简化过程可方便您的使用。有关详细信息，请参阅 《*Directory Server 5 2004Q2 Administrator's Guide*》。

注意

- 在 Windows 上，请使用随 Directory Server 5 2004Q2 （或更高版本）捆绑的 `certutil` 版本。

  *请勿*使用随 5 2004Q2 版本之前的 Directory Server 提供的 `certutil`。更早期版本的 `certutil` 与 Identity Synchronization for Windows 不兼容。

- 在 Solaris 上， `certutil` 默认安装在 `/usr/sfw/bin` 中。

1. 通过输入以下内容为 Directory Server 创建新的密钥证书数据库：

```
C:\Program Files\Sun\MPS\shared\bin\certutil.exe -d . -P slapd-hostname-

In order to finish creating your database, you
must enter a password which will be used to
encrypt this key and any future keys.
The password must be at least 8 characters long,
and must contain at least one non-alphabetic character.
Enter new password:
Re-enter password:
```

注意 这些示例将在直接位于服务器根下面的 `alias` 目录中运行。否则， Directory Server 将无法找到证书数据库。

2. 生成一个自签名证书，它将是 Directory Server 使用的服务器证书。请确保根据当前运行 Directory Server 的服务器的主机名来选择主题 DN。

注意 默认情况下，自签名证书的有效期为三个月。如果您要延长或缩短该期限，请使用 `-v <months-valid>` 选项。例如，要将期限延长到 24 个月，请输入 **`-v 21`**；或者，要将期限缩短为一个月，请输入 **`-v -2`**。

```
C:\Program Files\Sun\MPS\shared\bin\certutil.exe -d . -P slapd-hostname-
-S -n server-cert -s "cn=hostname.example.com,c=us" -x -t CTu,,
A random seed must be generated that will be used in the
creation of your key.One of the easiest ways to create a
random seed is to use the timing of keystrokes on a keyboard.
To begin, type keys on the keyboard until this progress meter
is full.DO NOT USE THE AUTOREPEAT FUNCTION ON YOUR KEYBOARD!
Continue typing until the progress meter is full:
|************************************************************|
Finished.Press enter to continue:
Enter Password or Pin for "NSS Certificate DB":
Generating key.This may take a few moments...
```

3. 显示用于检查用途的证书。

```
C:\Program Files\Sun\MPS\shared\bin\certutil.exe -L -d . -P
slapd-hostname-
Certificate Name            Trust Attributes
server-cert                CTu,,
p    Valid peer
P    Trusted peer (implies p)
c    Valid CA
T    Trusted CA to issue client certs (implies c)
C    Trusted CA to certs(only server certs for ssl) (implies c)
u    User cert
w    Send warning
```

4. 创建一个 PIN 文件，从而不必在每次重新启动 Directory Server 时输入证书数据库密码。

   ```
   C:\Program Files\Sun\MPS\alias > echo Internal (Software) Token:<secret12>
   slapd-hostname-pin.txt
   ```

5. 在 Directory Server 中启用 SSL，如下所述：

   a. 打开控制台。

   b. 选择 “配置” 选项卡。

   c. 选择 “加密” 选项卡 （在右侧窗格上）。

   d. 为该服务器选择 “启用 SSL”。

   e. 选择 “使用此密码系列：RSA”。

   f. 单击 “保存”，然后单击 “确定” 两次。

   g. 选择 “网络” 选项卡。

   h. 更新 “安全端口” 字段。如果在与 Active Directory 相同的机器上运行，则必须将端口从 636 更改为未使用的端口，否则 Directory Server 将不会启动。

   i. 依次单击 “保存”、“是”，然后单击 “确定”。

   j. 选择 “任务” 选项卡 （位于顶部）。

   k. 单击 “重新启动 Directory Server”，然后单击 “是”。

从 “Directory Server 证书数据库” 检索 “CA 证书”

请确保已在 Directory Server 中启用了 SSL。要将 Directory Server 证书导出到临时文件，以便您可将其导入到 Directory Server Connector 的证书数据库，请发出以下命令：

```
C:\Program Files\Sun\MPS\shared\bin\certutil.exe -L -d . -P slapd-hostname-
-n server-cert -a > C:\s-cert.txt
```

这些示例将在直接位于服务器根下面的 alias 目录中运行。否则，Directory Server 会找不到证书数据库。

在 Active Directory Connector 中启用 SSL

Identity Synchronization for Windows *自动*通过 SSL 检索 Active Directory SSL 证书，并使用您为 “连接器” 提供的证书将它们导入到 “连接器” 的证书数据库中。

但是，如果出现错误 （例如，找到的证书无效或者找不到 SSL 证书），则可检索出一个 Active Directory CA 证书并将其添加到 “连接器” 证书数据库。有关说明请参阅以下各节：

- 第 296 页的 “检索 Active Directory 证书”
- 第 299 页的 “将 Active Directory 证书添加到连接器的证书数据库中”

检索 Active Directory 证书

如果出错，可如下列各节所述使用 `certutil` （随 Windows 2000/2003 提供的一个程序）或 LDAP 检索 Active Directory 证书。

注意 本节讨论的 `certutil` 命令与随 Directory Server 提供且已在本书前面讨论的 `certutil` 命令*不*同。

使用 Windows 的 certutil

要使用 `certutil` 程序检索 “Active Directory 证书”：

1. 从 Active Directory 机器运行下列命令以导出证书。

   ```
   C:\>certutil -ca.cert cacert.bin
   ```

2. 然后，便可将 `cacert.bin` 文件导入到证书数据库中。

使用 LDAP

要使用 LDAP 检索 “Active Directory 证书”：

1. 对 Active Directory 执行以下搜索：

   ```
   ldapsearch -h <CR-hostname> -D <administrator_DN> -w <administrator_password> -b
   "cn=configuration,dc=put,dc=your,dc=domain,dc=here" "cacertificate=*"
   ```

   其中， *<administrator_DN>* 可能类似于：

   ```
   cn=administrator,cn=users,dc=put,dc=your,dc=domain,dc=here
   ```

   在本例中，域名为：*<put.your.domain.name.here>*。

   有若干条目与搜索过滤器相符。您或许需要 DN 中使用 `cn=Certification Authorities, cn=Public Key Services` 的条目。

2. 打开文本编辑器并剪切第一个 CA 证书属性的第一个值 （它应是一个 base64 编码的文本块）。请将该值 （文本块）粘贴到文本编辑器中 （仅限该值）。编辑其内容，以使这些行不会以空白开始。

3. 在第一行之前添加 `-----BEGIN CERTIFICATE-----`，在最后一行之后添加 `-----END CERTIFICATE-----`。请参阅下列示例：

```
-----BEGIN CERTIFICATE-----

MIIDvjCCA2igAwIBAgIQDgoyk+Tu14NGoQnxhmNHLjANBgkqhkiG9w0BAQUFA
DCBjjEeMBwGCSqGSIb3DQEJARYPYmVydG9sZEBzdW4uY29tMQswCQYDVQQGEwJVUzELMAkG
A1UECBMCVFgxDzANBgNVBAcTBkF1c3RpbjEZMBcGA1UEChMQU3VuIE1pY3Jvc3lzdGVtczE
QMA4GA1UECxMHaVBsYW5ldDEUMBIGA1UEAxMLUmVzdGF1cmFudHMwHhcNMDIwMTExMDA1ND
A5WhcNMTIwMTExMDA1OTQ2WjCBjjEeMBwGCSqGSIb3DQEJARYPYmVydG9sZEBzdW4uY29tM
QswCQYDVQQGEwJVUELMAkGA1UECBMCVFgxDzANBgNVBAcTBkF1c3RpbjEZMBcGA1UEChMQU
3VuIE1pY3Jvc3lzdGVtczEQMA4GA1UECxMHaVBsYW5ldDEUMBIGA1UEAxMLUmVzdGF1cmFu
dHMwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAyekZa8gwwhw3rLK3eV/12St1DVUsg31LOu3
CnB8cMHQZXlgiUgtQ0hm2kpZ4nEhwCAHhFLD3iIhIP4BGWQFjcwIDAQABo4IBnjCCAZowEw
YJKwYBBAGCNxQCBAYeBABDAEEwCwYDVR0PBAQDAgFGMA8GA1UdEwEB/wQFMAMBAf8wHQYDV
R0OBBYEFJ5Bgt6Oypq7T8Oykw4LH6ws2d/IMIIBMgYDVR0fBIIBKTCCASUwgdOggdCggc2G
gcpsZGFwOi8vL0NOPVJlc3RhdXJhbnRzLENOPWRvd2l0Y2hlcixDTj1DRFAsQ049UHVibGl
jJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049Q29uZmlndXJhdGlvbixEQz1yZX
N0YXVyYW50cyxEQz1jZW50cmFsLERDPXN1bixEQz1jb20/Y2VydGlmaWNhdGVSZXZvY2F0a
W9uTGlzdD9iYXNlP29iamVjdGNsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50ME2gS6BJhkdo
dHRwOi8vZG93aXRjaGVyLnJlc3RhdXJhbnRzLmNlbnRyYWwuc3VuLmNvbS9DZXJ0RW5yb2x
sL1Jlc3RhdXJhbnRzLmNybDAQBgkrBgEEAYI3FQEEAwIBADANBgkqhkiG9w0BAQUFAANBAL
5R9R+ONDdVHWu/5Sd9Tn9dpxN8oegjS88ztv1HD6XSTDzGTuaaVebSZV3I+ghSInsgQbH0g
W4fGRwaI BvePI4=

-----END CERTIFICATE-----
```

4. 将该证书保存到文件 （如 ad-cert.txt）中。
5. 然后，便可将该文件 （例如， ad-cert.txt）导入到证书数据库中。有关说明，请继续阅读下一节 “将 Active Directory 证书添加到连接器的证书数据库中”。

将 Active Directory 证书添加到连接器的证书数据库中

只有在安装 Active Directory Connector 后为该 “连接器” 启用了 SSL，或者在安装过程中提供了无效证书时，才能使用此过程。

1. 在安装 Active Directory Connector 的机器上，停止 Identity Synchronization for Windows 服务 / 守护进程。
2. 使用下列方法之一检索 Active Directory CA 证书：
   - 第 296 页的 “使用 Windows 的 certutil”
   - 第 297 页的 “使用 LDAP”
3. 假设 Active Directory Connector 的连接器 ID 为 CNN101（有关从连接器 ID 到其管理的目录源之间的映射，请参阅 `logs/central/error.log`），转至其证书数据库目录 （在安装它的机器上），并导入证书文件：
   - 如果使用 `certutil` 检索证书，请键入：

     ```
     C:\\Program Files\Sun\MPS\shared\bin\certutil.exe -A -d . -n
     ad-ca-cert -t C,, -i \cacert.bin
     ```

   - 如果使用 LDAP 检索证书，请键入：

     ```
     C:\\Program Files\Sun\MPS\shared\bin\certutil.exe -A -d . -n
     ad-ca-cert -t C,, -a -i \ad-cert.txt
     ```

4. 重新启动 Identity Synchronization for Windows 服务 / 守护进程。

注意 因为 Directory Server `certutil.exe` 在安装 Directory Server 5 2004Q2 时自动安装，您无法将 CA 证书添加到安装在无 Directory Server 的机器上的连接器中。

至少，您必须将 Directory Server 5 2004Q2 软件包的 Sun Java System Server Basic Libraries 和 Sun Java System Server Basic System Libraries 安装在安装了 Active Directory Connector 的服务器上。（您不必安装 Administration Server 或 Directory Server 组件。）

此外，请务必从 “控制台” 选择 JRE 子组件 （以确保您能够进行卸载）。

将 Active Directory 证书添加到 Directory Server

请按照以下步骤将 Active Directory CA 证书添加到 Directory Server 证书数据库中。

注意 请确保已在 Directory Server 中启用了 SSL。

1. 使用下列方法之一检索 Active Directory CA 证书：
   - 第 296 页的 “使用 Windows 的 certutil”
   - 第 297 页的 “使用 LDAP”
2. 停止 Directory Server。
3. 在安装 Directory Server 的机器上，按如下方式导入 Active Directory CA 证书：
   - 如果使用 `certutil` 检索证书，请键入：

     ```
     C:\\Program Files\Sun\MPS\shared\bin\certutil.exe -A -d . -P
     slapd-hostname- -n ad-ca-cert -t C,, -i \cacert.bin
     ```

   - 如果使用 LDAP 检索证书，请键入：

     ```
     C:\\Program Files\Sun\MPS\shared\bin\certutil.exe -A -d . -P
     slapd-hostname- -n ad-ca-cert -t C,, -a -i \ad-cert.txt
     ```

4. 启动 Directory Server。

将 Directory Server 证书添加到 Directory Server Connector

如果在 Directory Server 插件和 Active Directory 之间启用 SSL 通信，则必须将 Active Directory CA 证书添加到每个 Directory Server 主服务器的证书数据库中。请按下列步骤操作：

1. 在安装了 Directory Server Connector 的机器上，停止 Identity Synchronization for Windows 服务 / 守护进程。
2. 检索 Directory Server CA 证书。
3. 假定该 Directory Server Connector 的连接器 ID 为 CNN100（有关从连接器 ID 到其管理的目录源之间的映射，请参阅 `logs/example/error.log`），转至其证书数据库目录 （在安装它的机器上），并导入 `cacert.bin` 文件：

```
C:\Program Files\Sun\MPS\shared\bin\certutil.exe -A -d .-n ds-cert -t
C,, -i C:\s-cert.txt
```

注意 如果该证书是以 ASCII 形式获得的证书，请将 “`-a`”参数添加到 `certutil` 命令行，以指出该证书是 ASCII 形式而不是二进制形式。

4. 重新启动 Identity Synchronization for Windows 服务 / 守护进程。

第 II 部分

附录

使用 Identity Synchronization for Windows 命令行实用程序

Identity Synchronization for Windows 允许您使用命令行执行各种任务。本附录介绍如何执行 Identity Synchronization for Windows 命令行实用程序以完成各种任务。这些信息被编排在以下各节中：

一般特性

Identity Synchronization for Windows 命令行实用程序具有以下特性：

公用参数

本节介绍多数命令行实用程序的公用参数 （选项）。这些信息被编排在下表中：

- 表 A-1 所有子命令的公用参数：介绍以下参数，它们是所有 `idsync` 子命令（*除 `prepds`* 外）和移植工具的公用参数。

```
-D <bind-DN> -w <bind-password | -> [-h <Configuration Directory-hostname>]
[-p <Configuration Directory-port-no>] [-s <rootsuffix>] [-Z] [-P <cert-db-path>]
[-m <secmod-db-path>]
```

注意 括号 `[ ]` 表示可选参数。

Identity Synchronization for Windows 安装程序将根据您在安装过程中提供的信息自动将默认值写入 `-h`、 `-p`、 `-D` 和 `-s` 参数中。不过，您可在命令行中指定不同的值来覆盖默认值。

为了对多字节字符提供支持，在命令行接口 (CLI) 环境文件中，Identity Synchronization for Windows 对 `-s` *<rootsuffix>* 和 `-D` *<bind-DN>* 默认值进行 base64 编码。不能对根后缀的默认值进行更改。可在命令行中覆盖绑定 DN 的默认值，或者在 CLI 环境文件中使用合适的 base64 编码值对其进行更新。

- 表 A-2 所有子命令的公用 SSL- 相关参数：介绍可选参数，这些参数提供有关使用 “安全套接字层” (SSL) 安全访问 “配置目录服务器” 的信息。这些参数也是所有 `idsync` 子命令和移植工具的公用参数。

- 表 A-3 配置目录参数：介绍与配置目录有关的参数。这些参数为两个或更多 idsync 子命令和移植工具的公用参数。

注意 特定子命令的独有参数将在相关子命令部分介绍。

表 A-1 所有子命令的公用参数

参数	说明
-h <*Configuration Directory-hostname*>	指定配置目录主机名。此参数的默认值为 “核心”安装期间指定的值。
-p <*Configuration Directory-port-no*>	指定配置目录 LDAP 端口号。
-D <*bind-DN*>	指定配置目录绑定识别名 (DN)。此参数的默认值为 “核心”安装期间指定的值。
-w <*bind-password* | ->	指定配置目录绑定密码。 值 - 从标准输入 (STDIN) 中读取密码。
-s <*rootsuffix*>	指定配置目录根后缀。根后缀是识别名，如 dc=example,dc=com。 此参数的默认值为 “核心”安装期间指定的值。
-q <*configuration_password* | ->	指定配置密码。值 - 代表将从标准输入 (STDIN) 中读取密码。 除了 prepds 之外，此参数对所有子命令都是*强制项*。

表 A-2 所有子命令的公用 SSL- 相关参数

参数	说明
-Z	指定使用 SSL 提供安全通信。当连接至配置目录访问命令行界面或首选 / 备用 Directory Server 时，使用 SSL 提供基于证书的客户机验证。
-P <*cert-db-path*>	指定客户机的证书数据库的路径和文件名。 此证书数据库必须包含用于 Directory Server 的证书数据库签名的 CA 证书。 如果指定 -Z，但不使用 -P，则 <*cert-db-path*> 将采用默认值 <*current-working-directory*>/cert8.db。 **注意**：如果 Identity Synchronization for Windows 未在指定目录中找到证书数据库文件，程序将在该目录下创建一个 *empty* 数据库，其中包含以下三个文件：cert8.db、key3.db 和 secmod.db。
-m <*secmod-db-path*>	指定安全模块数据库的路径。例如： /var/Sun/MPS/slapd-<*serverID*>/secmod.db 仅当安全模块数据库与证书数据库本身处于不同的目录下时，才指定此参数。

表 A-3 配置目录参数

参数	说明
`-a` <*ldap_filter*> 与 `forcepwchg` 和 `resync` 子命令一起使用	指定从源 SUL 检索用户时将使用的 LDAP 过滤器，并且在确定用户是否在指定 SUL 范围内之前，允许操作从目录源检索侧重的用户子集。
`-f` <*filename*> 与 `export10cnf`、`importcnf` 和 `resync` 子命令一起使用	指定 “配置 XML 文档”文件的名称。
`-n` 与 `forcepwchg`、`importcnf` 和 `resetconn` 子命令一起使用	在安全模式下运行，这样您便可以预览某个操作的效果而不进行实际更改。

输入密码

需要密码参数时 （如 `-w` <*bind-password*> 或 `-q` <*configuration_password*>），可使用 “`-`”参数告知密码程序从 `STDIN` 读取密码。

如果对多个密码选项使用值 “`-`”， `idsync` 会基于参数的顺序提示您输入密码。

此时，程序将首先需要输入 <*bind-password*>，然后输入 <*configuration-password*>。

获取帮助

可使用以下命令之一在命令控制台中显示有关 `idsync` 或其任何子命令的用法信息：

- **`-help`**
- **`--help`**
- **`-?`**

用法信息

- 对于 `idsync` （包括一列有效子命令），请在命令提示符处键入上述帮助选项中的一个，然后按回车键。
- 对于某个子命令，请在命令提示符处键入该子命令，后接帮助选项，然后按回车键。

使用 idsync 命令

您可使用 idsync 命令和子命令执行 Identity Synchronization for Windows 命令行实用程序。

注意 idsync 命令可在将参数发送至 Directory Server 之前，将所有 DN 值参数（如绑定 DN 或后缀名）从该窗口的指定字符集转换为 UTF-8。

在后缀名中不要使用反斜线作为换码符。

要在 Solaris 上指定 UTF-8 字符，终端窗口中必须有基于 UTF-8 的语言环境。确保环境变量的 LC_CTYPE 和 LANG 设置正确。

除非另行说明，否则可使用以下方法之一运行带有子命令的 idsync 命令：

- **Solaris：**
  a. 打开终端窗口，并使用 **cd** 进入 /opt/SUNWisw/bin 目录。
  b. 键入带有一个子命令的 idsync 命令，如下所示

     idsync <*subcommand*>

- **Windows：**
  a. 打开“命令窗口”，并使用 **cd** 进入 <*install_path*>\isw-<*hostname*>\bin 目录。
  b. 键入带有一个子命令的 idsync 命令，如下所示

     idsync <*subcommand*>

表 A-4 列出了所有 idsync 实用程序子命令及其用途：

表 A-4 idsync 子命令快速参考

子命令	用途
certinfo	基于配置和 SSL 设置显示证书信息 （请参阅第 310 页的 “使用 certinfo”）
changepw	更改 Identity Synchronization for Windows 配置密码 （请参阅第 311 页的 “使用 changepw”）
importcnf	导入已导出的 Identity Synchronization for Windows 版本 1.0 配置 XML 文档 （请参阅第 312 页的 “使用 importcnf”）
prepds	准备供 Identity Synchronization for Windows 使用的 Sun Java System Directory Server 源 （请参阅第 313 页的 “使用 prepds”）
printstat	显示要完成安装 / 配置过程必须执行的步骤的列表。还提供已安装连接器、系统管理器和 Message Queue 的状态 （请参阅第 317 页的 “使用 printstat”）
resetconn	将配置目录中的连接器状态重设为 *尚未安装* （请参阅第 318 页的 “使用 resetconn”）
resync	作为安装过程的一部分，链接和重新同步现有用户并预先填充目录 （请参阅第 319 页的 “使用 resync”）
startsync	启动同步 （请参阅第 321 页的 “使用 startsync”）
stopsync	停止同步 （请参阅第 322 页的 “使用 stopsync”）

使用 certinfo

可使用 certinfo 子命令基于配置和 SSL 设置显示证书信息。此信息有助于确定必须为每个连接器和 / 或 Directory Server 插件证书数据库添加哪些证书。

要显示证书信息，请打开终端窗口 （或 “命令窗口”），然后键入 **idsync certinfo** 命令，如下所示：

```
idsync certinfo [<bind-DN>] -w <bind-password | -> [-h <Configuration
Directory-hostname>] [-p <Configuration Directory-port-no>] [-s <rootsuffix>] -q
<configuration_password> [-Z] [-P <cert-db-path>] [-m <secmod-db-path>]
```

注意 因为 certinfo 子命令不能访问连接器和 Directory Server 的证书数据库，所以它列出的所需步骤中，有一些可能已经执行。

例如：

idsync certinfo -w <*admin-password*> -q <*configuration-password*>

注意 有关 certinfo 参数的详细信息，请查看第 306 页的 “公用参数”。

使用 changepw

您可使用 changepw 子命令更改 Identity Synchronization for Windows 配置密码。

更改 Identity Synchronization for Windows 的配置密码：

1. 停止所有 Identity Synchronization for Windows 进程 （例如，系统管理器、中心记录器、连接器、控制台、安装程序 / 卸载程序）。
2. 停止所有进程后，通过将配置目录导出到 ldif 备份 ou=Services 树。
3. 键入 **idsync changepw** 命令，如下所示：

```
idsync changepw [-D <bind-DN>] -w <bind-password | -> [-h <Configuration
Directory-hostname>] [-p <Configuration Directory-port-no>] [-s <rootsuffix>]
-q <configuration_password> [-Z] [-P <cert-db-path>] [-m <secmod-db-path>]
-b <new password | - > [-y]
```

例如：

idsync changepw -w <*admin password*> -q <*old config password*> -b -q <*new config password*>

以下参数是 changepw 的独有参数：

表 A-5 idsync changepw 参数

参数	说明
-b <*password*>	指定新的配置密码。值 - 从标准输入 (STDIN) 读取密码。
[-y]	不提示命令确认。

注意 有关其它 changepw 参数的详细信息，请查看第 306 页的 “公用参数”。

4. 对终端窗口中显示的信息进行应答。例如，

```
Are you sure that want to change the configuration password (y/n)? yes
Before restarting the system - you must edit the
$PSWHOME/resources/SystemManagerBootParams.cfg file and change the
'deploymentPassword' to the new value.

SUCCESS
```

5. 重新启动系统前必须修改 SystemManagerBootParams.cfg 文件。

   $PSWHOME\resources（其中 $PSWHOME 为 *<isw-installation directory>*）中的文件 SystemManagerBootParams.cfg 包含了系统管理器用于连接配置目录的配置密码。

   例如，您可更改密码值，如下所示：

   从：*<Parameter name="manager.configReg.deploymentPassword" value="***oldpassword***"/>*

   更改为：*<Parameter name="manager.configReg.deploymentPassword" value="***newpassword***"/>*

6. 如果程序报告任何错误，请使用 ldif 从步骤 2 恢复配置目录，然后再试。出现错误的最可能原因是密码更改期间托管配置目录的 Directory Server 变为不可用。

使用 importcnf

警告 *仅*当从 Identity Synchronization for Windows 1.0 或 1.0 SP1 移植到版本 1 2004Q3 时才使用 idsync importcnf。

安装核心（第 3 章，“安装核心”）后，使用 idsync importcnf 子命令导入您导出的包含 “核心”配置信息的 Identity Synchronization for Windows 版本 1.0 (SP1) 配置 XML 文件。

要导入版本 1.0 配置 XML 文档”，请打开终端窗口 （或 “命令窗口”），然后键入 **idsync importcnf** 命令，如下所示：

```
idsync importcnf [-D <bind-DN>] -w <bind-password | -> [-h <Configuration
Directory-hostname>] [-p <Configuration Directory-port-no>] [-s <rootsuffix>] -q
<configuration_password> [-Z] [-P <cert-db-path>] [-m <secmod-db-path>] -f <filename>
[-n]
```

例如：

```
idsync importcnf -w <admin_password> -q <configuration_password> -f "MyConfig.cfg"
```

以下参数是 importcnf 的独有参数：

表 A-6 idsync importcnf 参数

参数	说明
-f <*filename*>	指定配置 XML 文档的名称。
-n	在安全模式下运行，这样您便可以预览某个操作的效果而不进行实际更改。

注意 有关其它 importcnf 参数的详细信息，请查看第 306 页的 “公用参数”。

导入 1.0 版本的配置 XML 文档后，必须在为进行同步而配置的所有 Directory Server 源上运行 prepds （请参阅第 313 页的 “使用 prepds”），然后便可安装 Identity Synchronization for Windows 连接器和子组件。

使用 prepds

可使用控制台或 prepds 子命令准备 Sun Java System Directory Server 源，供 Identity Synchronization for Windows 使用。安装 Directory Server Connector 之前必须运行 prepds。

运行 idsync prepds 子命令可将相应的 ACI 应用到 cn=changelog 条目，它是 Retro-Changelog 数据库的根节点。

- 如果要准备将由 Identity Synchronization for Windows 使用的 *首选 主* Directory Server，必须提供 *Directory Manager* 证书。

“目录管理员”用户是 Directory Server 上的特殊用户，他们对 Directory Server 实例具有全部权限。（ACI 不适用于 “目录管理员”用户。）

例如，只有 “目录管理员”才可设置 Retro-Changelog 数据库的访问控制，这是 Identity Synchronization for Windows 需要首选主服务器的 “目录管理员”证书的原因之一。

注意 无论出于何种原因为首选 Sun 目录源重建 Retro-Changelog 数据库，默认的访问控制设置都将不允许 Directory Server Connector 读取数据库内容。

要为 Retro-Changelog 数据库恢复访问控制设置，需要运行 `idsync prepds`，或在控制台中选择合适的 Sun 目录源后单击 “准备 Directory Server”按钮。

注意 可将系统配置为在指定时间段后自动删除 （或*整理*） Change-log 条目。从命令行修改 `cn=Retro Changelog Plugin, cn=plugins, cn=config` 中的 `nsslapd-changelogmaxage` 配置属性：

`nsslapd-changelogmaxage:` *IntegerTimeunit*

其中：

- ***Integer*** 是一个数字
- ***Timeunit*** 为时间单位， s 代表秒， m 代表分钟， h 代表小时， d 代表天数， w 代表周数。（在 Integer 和 Timeunit 变量之间不应有空格。）

例如， `nsslapd-changelogmaxage: 2d`

有关详细信息，请参阅 《Sun Java™ System Directory Server 5 2004Q2 管理指南》中的 “管理复制”一章。

- 可使用*管理*证书准备*备用*服务器。

注意 运行 idsync prepds *之前*，请务必计划 Identity Synchronization for Windows 配置，因为您必须清楚要使用哪些主机和后缀。

如果在已经安装、配置和同步了 Directory Server Connector 和插件的 Directory Server 后缀上运行 idsync prepds，将出现一条消息，要求您安装 Directory Server Connector。忽略此消息。

要准备 Sun Java System Directory Server 源，请打开终端窗口 （或 “命令窗口”），然后键入 **idsync prepds** 命令，如下所示：

```
idsync prepds [-D <bind-DN>] -w <bind-password | -> [-h <preferred host>]
[-p <preferred-port>] [-s <database-suffix>] [-Z] [-P <cert-db-path>]
[-m <secmod-db-path>] [-j <secondary_host>] [-r <secondary-port>] [-E <admin DN of
secondary host>] [-u <password for secondary host | ->] [-x]
```

例如：

```
idsync prepds -D "cn=Directory Manager" -w <preferred master password> -h
<preferred-host> -p 389 -s dc=example,dc=com -j "secondary host" -r 389 -E
"cn=Administrator" -u <secondary master password> -s dc=example,dc=com
```

注意 -h、 -p、 -D、 -w 和 -s 参数仅为 prepds 子命令重新定义 （如下表所述）。此外，不使用 -q 参数。

表 A-7 描述了 idsync prepds 所独有的参数：

表 A-7 prepds 参数

参数	说明
-h <*name*>	指定作为首选主机的 Directory Server 实例的 DNS 名称。
-p <*port*>	指定作为首选主机的 Directory Server 实例的端口号。（*默认值为 389*。）
-j <*name*> (*optional*)	指定作为备用主机的 Directory Server 实例的 DNS 名 （适用于 Sun Java System Directory Server 5 2004Q2 多主复制 (MMR) 环境）。
-r <*port*> （*可选*）	指定作为备用主机的 Directory Server 实例的端口 （适用于 Sun Java System Directory Server 5 2004Q2 多主复制 (MMR) 环境）。（*默认值为 389*。）
-D <*dn*>	为首选主机的目录管理员用户指定识别名。

表 A-7 prepds 参数 *（续）*

参数	说明
-w <*password*>	为首选主机的目录管理员用户指定密码。值 - 从标准输入 (STDIN) 中读取密码。
-E <*admin-DN*>	为备用主机的目录管理员用户指定识别名。
-u <*password*>	为备用主机的目录管理员用户指定密码。值 - 从标准输入 (STDIN) 中读取密码。
-s <*rootsuffix*>	指定根后缀，用于添加索引 （同步用户的根后缀）。 **注意**：“首选”主机和 “备用”主机的数据库名可能不同，但后缀则相同。因此，程序便可以找到每个主机的数据库名并用它添加索引。
-x	对于 dspswuserlink 属性，不向数据库中添加等同索引和当前索引。

如果要在复制环境 （例如，具有首选主服务器、备用主服务器和两个用户的环境中）中运行 idsync prepds，则只需为首选主服务器和备用主服务器运行一次 idsync prepds。

要运行 idsync prepds

1. 确保 Directory Server 复制环境正常并正在运行 （如果适用。）
2. 从控制台或命令行运行 idsync prepds，例如：

```
idsync prepds -h M1.example.com -p 389 -j M2.example.com -r 389 . . .
```

运行 idsync prepds 命令将实现：

- 在 M1 上：
  - 启用和扩展 RCL，以捕获更多属性 （dspswuserlink 等）

    仅在 M1 上需要 RCL。
  - 扩展模式
  - 使用 ACI 添加 uid=pswconnector,<*suffix*> user
  - 将索引添加到 dspswuserlink 属性，此操作会在完成索引创建前将 Directory Server 临时置于只读模式。

    可稍后再添加索引，以避开停机时间，但必须在安装 Directory Server Connector *之前*添加索引。
- 在 M2 上添加索引。

注意

- 复制环境可确保 Identity Synchronization for Windows 将模式信息和 uid=pswconnector 从首选主服务器复制到备用主服务器及两个用户。
- 必须安装一次 Directory Server Connector。必须在*所有*目录下安装 Directory Server 插件。
- 只需在首选主服务器和备用主服务器上创建索引。（复制不会将创建索引配置从首选主服务器传播至备用主服务器。）

使用 printstat

可使用 printstat 子命令实现：

- 显示其余完成安装和配置过程所必须执行的步骤列表
- 打印已安装连接器、系统管理器和 Message Queue 的状态。

  可能的状态设置包括：

  - **尚未安装。**未安装连接器。
  - **已安装。**已安装连接器，但因尚未接收到其运行时配置，所以同步未就绪。
  - **就绪。**连接器同步就绪，但尚未同步任何对象。
  - **正在同步。**连接器正在同步对象。

要打印已安装连接器、系统管理器及 Message Queue 的状态，请打开终端窗口（或“命令窗口”），然后输入 **idsync printstat** 命令，如下所示：

```
idsync printstat [-D <bind-DN>] -w <bind-password | -> [-h <Configuration
Directory-hostname>] [-p <Configuration Directory-port-no>] [-s <rootsuffix>]
-q <configuration_password> [-Z] [-P <cert-db-path>] [-m <secmod-db-path>]
```

例如：

```
idsync printstat -w <admin password> -q <configuration password>
```

注意 有关 printstat 参数的详细信息，请查看第 306 页的 “公用参数”。

使用 resetconn

可使用 resetconn 子命令将配置目录中的连接器状态重设为*尚未安装*。例如，如果硬件故障使您无法卸载连接器，可使用 resetconn 将连接器的状态更改为 “尚未安装”，这样便可重新安装该连接器。

警告 仅在硬件或卸载程序出现故障的情况下才使用 resetconn 子命令。

要从命令行重设连接器的状态，请打开终端窗口 （或 “命令窗口”），然后键入 **idsync resetconn** 命令，如下所示：

```
idsync resetconn [-D <bind-DN>] -w <bind-password> | -> [-h <Configuration
Directory-hostname>] [-p <Configuration Directory-port-no>] [-s <rootsuffix>] -q
<configuration_password> [-Z] [-P <cert-db-path>] [-m <secmod-db-path>] -e
<directory-source-name> [-n]
```

例如：

```
idsync resetconn -w <admin password> -q <configuration_password> -e
"dc=example,dc=com"
```

表 A-8 描述了 resetconn 所独有的参数：

表 A-8 idsync resetconn 参数

参数	说明
-e <*dir-source*>	指定要重设的目录源名称。
-n	在安全模式下运行，这样您便可以预览某个操作的效果而不进行实际更改。

注意 idsync printstat 可用于查找目录源名称。

有关其它 resetconn 参数的详细信息，请查看第 306 页的 “公用参数”。

使用 resync

可使用 resync 子命令引导现有用户的部署。此命令使用管理员指定的匹配规则实现

- 链接现有条目
- 用远程目录的内容填充空白目录
- 在两个现有用户群体之间批量同步属性值

注意 有关链接和同步用户的更详细信息，请参阅第 173 页的 “同步现有用户”。

要重新同步现有用户和预先填充目录，请打开终端窗口 （或 “命令窗口”），然后键入 **idsync resync** 命令，如下所示：

```
idsync resync [-D <bind-DN>] -w <bind-password> | -> [-h <Configuration
Directory-hostname>] [-p <Configuration Directory-port-no>] [-s <rootsuffix>] -q
<configuration_password> [-Z] [-P <cert-db-path>] [-m <secmod-db-path>] [-n] [-f <xml
filename for linking>] [-k] [-a <ldap-filter>] [-l <sul-to-sync>] [-o Sun | Windows]
[-c] [-x] [-u] [-i ALL_USERS | NEW_USERS | NEW_LINKED_USERS]
```

例如：

```
idsync resync -w <admin password> -q <configuration_password>
```

表 A-9 描述了 resync 所独有的参数：

表 A-9 idsync resync 用法

参数	含义
-f <*filename*>	使用 Identity Synchronization for Windows 提供的指定 XML 配置 文件之一在两个未链接用户条目间创建链接。（请参阅附录 B，“LinkUsers XML 文档范例”）
-k	只在未链接用户间创建链接 （不创建用户或修改现有用户）
-a <*ldap-filter*>	指定 LDAP 过滤器来限制要同步的条目 此过滤器将被用作重新同步操作的源。 例如，如果指定 idsync resync -o Sun -a "uid=*"，则所有具有 uid 属性的 Directory Server 用户将被同步到 Active Directory。
-l <*sul-to-sync*>	指定要重新同步的各个 “同步用户列表” (SUL)。 **注意**：可指定多个 SUL ID 以重新同步多个 SUL，如果不指定任何 SUL ID，程序将重新同步您的所有 SUL。
-o (Sun | Windows)	指定重新同步操作的源 • **Sun**：将 Windows 条目的属性值设置为 Sun Java System Directory Server 目录源条目中的相应属性值。 • **Windows**：将 Sun Java System Directory Server 条目的属性值设置为 Windows 目录源条目中的相应属性值。 （*默认为 Windows*。）
-c	如果在目标处未找到相应用户，则自动创建用户条目 • 随机为在 Active Directory 或 Windows NT 中创建的用户生成密码 • 为在 Directory Server 中创建的用户自动创建指定的密码值 ((PSWSYNC)***INVALID PASSWORD***)（除非指定了 -i 选项）
-i (ALL_USERS | NEW_USERS | NEW_LINKED_USERS)	为在 Sun 目录源中同步的用户条目重设密码，下次需要提供用户密码时对这些用户强制执行当前域内的密码同步。 • **ALL_USERS**：对所有已同步的用户强制执行即时请求密码同步 • **NEW_USERS**：仅对新创建的用户强制执行即时请求密码同步 • **NEW_LINKED_USERS**：对所有新创建和新链接的用户强制执行即时请求密码同步
-u	仅更新对象高速缓存。无条目被修改。 该参数仅为 Windows 目录源更新用户条目的本地高速缓存，这将防止在 Directory Server 中创建已经存在的 Windows 用户。如果使用此参数，则不会将 Windows 用户条目与 Directory Server 用户条目同步。仅当同步源为 Windows 时，此参数才有效。
-x	删除所有与源条目不匹配的目标用户条目。
-n	在安全模式下运行，这样您便可以预览某个操作的效果而不进行实际更改。

注意

- 运行不带任何参数的 idsync resync 可查看用法说明。
- 有关 resync 参数的详细信息，请查看第 306 页的 “公用参数”。
- 有关重新同步现有用户的详细信息，请查看第 173 页的 “同步现有用户”。

在运行 resync 之后，查看中心 audit.log 中的 resync.log 文件。如果出现错误，请参考第 9 章，“故障排除”。

使用 startsync

可使用 startsync 子命令从命令行启动同步。

要启动同步，请打开终端窗口 （或 “命令窗口”），然后键入 **idsync startsync** 命令，如下所示：

```
idsync startsync [-D <bind-DN>] -w <bind-password | -> [-h <Configuration
Directory-hostname>] [-p <Configuration Directory-port-no>] [-s <rootsuffix>] -q
<configuration_password> [-Z] [-P <cert-db-path>] [-m <secmod-db-path>]
```

例如：

```
idsync startsync -w <admin password> -q <configuration_password>
```

表 A-10 描述了 startsync 所独有的参数：

表 A-10 idsync startsync 参数

参数	说明
[-y]	不提示命令确认。

注意 有关其它 startsync 参数的详细信息，请查看第 306 页的 “公用参数”。

使用 stopsync

可使用 stopsync 子命令从命令行停止同步。

要停止同步，请打开终端窗口 （或 “命令窗口”），然后键入 **idsync stopsync** 命令，如下所示：

```
idsync stopsync [-D <bind-DN>] -w <bind-password | -> [-h <Configuration
Directory-hostname>] [-p <Configuration Directory-port-no>] [-s <rootsuffix>] -q
<configuration_password> [-Z] [-P <cert-db-path>] [-m <secmod-db-path>]
```

例如：

```
idsync stopsync -w <admin password> -q <configuration_password>
```

注意 有关 stopsync 参数的详细信息，请查看第 306 页的 “公用参数”。

使用 forcepwchg 移植实用程序

在移植过程中更改了密码的用户将会在 Windows NT 和 Directory Server 中有不同的密码。可使用 `forcepwchg` 实用程序为那些在从 Identity Synchronization for Windows 版本 1.0 到版本 1 2004Q3 的移植过程中更改了密码的用户请求密码更改。

注意 `forcepwchg` 实用程序仅与 Windows 软件包一并提供。

使用 `forcepwchg` 之前必须验证以下内容：

- 确保未将 Directory Server 中的 7 位校验插件配置为对 `userpassword` 属性强制使用 7 位值。使用 Directory Server 控制台执行此操作。
- 确保用于验证的客户机将您使用的语言环境编码值正确转换为 UTF-8。（例如，Directory Server 附带的 `ldapsearch` 的 `-i` 选项。）

要执行 `forcepwchg` 命令行实用程序，

1. 打开 “命令提示”窗口，并使用 cd 进入要在其中执行移植的主机的 Windows `migration` 目录。（必须在 PDC 主机上安装 Identity Synchronization for Windows 1.0 NT 组件 （连接器、更改检测器 DLL、密码过滤器 DLL）。）
2. 在 `migration` 目录中，键入

```
java -jar forcepwchg.jar [-n] [-a] [-t <time_specification>]
```

例如：

```
forcepwchg.jar -n -a
forcepwchg.jar -t 33m
```

表 A-11 描述了 forcepwchg 所独有的参数：

表 A-11 forcepwchg 参数

选项	说明
-n	指定*预览模式*。 在预览模式中，实用程序将打印出所有常规用户的名称，但不打印以下用户： • 如果指定 -a 参数，则不打印内置帐户 （管理员和临时用户）。 • 在使用 -t 参数指定的时间内更改了密码的用户。 在预览模式中，任何用户都可以执行 forcepwchg。 在非预览模式中，只有管理员才能执行 forcepwchg。
-a	要求所有用户 （管理员和临时用户除外）更改其密码。 如果使用 -t 参数，则不能使用此参数。
-t <*time_specification*>	强制在过去的 < *时间定义* > 中更改了密码的所有用户更改其密码。其中， < *时间定义* > 可采用以下形式： • **<** *数值* **>**：秒数 （例如， -t 30） • **<** *数值* **>m**：分钟数 （例如， -t 25m） • **<** *数值* **>h**：小时数 （例如， -t 6h） 例如，如果指定 forcepwchg -t 6h，则会要求在最近六小时内更改了密码的所有用户再次更改其密码。
-?	打印出用法信息。

注意 有关使用 forcepwchg 的详细信息，请参阅第 194 页的 “在 Windows NT 上强制执行密码更改”。

LinkUsers XML 文档范例

本附录提供两个 XML 配置文档范例，它们可与 `idsync resync` 子命令共用，以链接部署中的现有用户。

下列两个文件都可以在安装 “核心”的子目录 `samples1` 中获得：

- 第 326 页的 “范例 1：linkusers-simple.cfg”（普通简单配置示例）
- 第 327 页的 “范例 2：linkusers.cfg”（较复杂的配置示例，说明指定链接条件的全部功能）

您可以修改这些示例，使其适合您的环境。这两个文件均包含解释如何修改示例以链接用户的注释 — 包括如何链接多个 SUL 中的用户。

范例 1：linkusers-simple.cfg

```
<!--

    Copyright 2004 Sun Microsystems, Inc. All rights reserved

    Use is subject to license terms.

-->

<!--

    This xml file is used to link Windows and Sun Directory Server users from the command
    line.It is passed to the 'idsync resync' script as the -f option.

    This is a simple file that links users in the SUL1 synchronization user list that have
    the same login name, that is the Directory Server uid attribute matches the Active
    Directory samaccountname attribute.

    For more complex matching rules, see the linkusers.cfg sample.

-->

<UserLinkingOperationList>

    <UserLinkingOperation parent.attr="UserLinkingOperation" sulid="SUL1">

        <UserMatchingCriteria parent.attr="UserMatchingCriteria">

            <AttributeMap parent.attr="AttributeMap">

                <AttributeDescription parent.attr="SunAttribute" name="uid"/>

                <AttributeDescription parent.attr="WindowsAttribute" name="samaccountname"/>

            </AttributeMap>

        </UserMatchingCriteria>

    </UserLinkingOperation>

</UserLinkingOperationList>
```

范例 2：linkusers.cfg

```
<?xml version =”1.0” encoding=”UTF-8”?>
<!--
    Copyright 2004 Sun Microsystems, Inc. All rights reserved
    Use is subject to license terms.
-->
<!--
    This xml file is used to link Windows and Sun Directory Server users from
    the command line.  It is passed to the 'idsync resync' script as the -f option.
-->
<!--
    The following parameters allowLinkingOutOfScope: if true, then Windows users can be
    linked to Sun Directory Server users that are outside of the users' Synchronization
    User List. Default is false.
-->
<UserLinkingOperationList allowLinkingOutOfScope="false">
<!--
    UserLinkingOperation encapsulates the configuration of a single SUL to link.
    It includes the SUL ID and a list of attributes to match.
    A separate UserLinkingOperation must be specified for each SUL being linked.
-->
<UserLinkingOperation parent.attr="UserLinkingOperation" sulid="SUL1">
<!--
    UserMatchingCriteria encapsulates a list of attributes that must match for a user
    to be linked. -->
<!--
    For two users to match using this UserMatchingCriteria, they must have the same
    givenName and the same sn. -->
<UserMatchingCriteria parent.attr="UserMatchingCriteria">
    <AttributeMap parent.attr="AttributeMap">
        <AttributeDescription parent.attr="SunAttribute" name="sn"/>
        <AttributeDescription parent.attr="WindowsAttribute" name="sn"/>
    </AttributeMap>
    <AttributeMap parent.attr="AttributeMap">
        <AttributeDescription parent.attr="SunAttribute" name="givenName"/>
        <AttributeDescription parent.attr="WindowsAttribute"
        name="givenName"/>
    </AttributeMap>
</UserMatchingCriteria>
```

```
<!--
    Multiple UserMatchingCriteria can be specified for a single SUL.  They are treated as
    a logical OR.  In this example, (the givenName's and sn's must match (see above)) OR
    (the employee(Number|ID) must match), for the user to be linked.  Notice that attribute
    that is specified, employeeNumber, is the name of the DS attribute. -->

<!--
    This UserMatchingCriteria is commented out because employeeNumber is not an indexed
    attribute in DS.  All attributes used in a UserMatchingCriteria should be indexed.

    <UserMatchingCriteria parent.attr="UserMatchingCriteria">
        <AttributeMap parent.attr="AttributeMap">
            <AttributeDescription parent.attr="SunAttribute" name="employeeNumber"/>
            <AttributeDescription parent.attr="WindowsAttribute" name="employeeID"/>
        </AttributeMap>
    </UserMatchingCriteria>

-->
```

</UserLinkingOperation>

```
<!--
    When multiple SULs are linked, a separate UserLinkingOperation is specified
    for each.  As shown here, each UserLinkingOperation can use different
    UserMatchingCriteria: in this example, users in SUL2 are only linked if their
    sn and employeeNumber match.

    Note: this UserLinkingOperation is currently commented out because
    the example configuration only has a single SUL.

<UserLinkingOperation parent.attr="UserLinkingOperation" sulid="SUL2">
    <UserMatchingCriteria parent.attr="UserMatchingCriteria">
        <AttributeMap parent.attr="AttributeMap">
            <AttributeDescription parent.attr="SunAttribute" name="sn"/>
            <AttributeDescription parent.attr="WindowsAttribute" name="sn"/>
        </AttributeMap>
            <AttributeMap parent.attr="AttributeMap">
                <AttributeDescription parent.attr="SunAttribute" name="employeeNumber"/>
                <AttributeDescription parent.attr="WindowsAttribute" name="employeeID"/>
        </AttributeMap>
    </UserMatchingCriteria>
</UserLinkingOperation>
-->
```

</UserLinkingOperationList>

在 Solaris 上以非超级用户身份运行服务

必须具有超级用户权限才能安装和运行 Identity Synchronization for Windows 服务。但在安装产品之后，可将软件配置为以非超级用户身份运行程序服务。

注意 如果要以非超级用户身份运行服务，必须更改 Identity Synchronization for Windows 实例目录下所有目录的权限。（*默认*目录为 `/var/opt/SUNWisw`。）

要在 Solaris 上以非超级用户身份运行服务，请执行下列步骤：

1. 使用 UNIX `useradd` 命令为 Identity Synchronization for Windows 创建一个用户帐户 （*此步骤为可选步骤*）。

   还可以用 `nobody` 用户身份运行服务。
   此过程中的其余示例假定您创建了一个称为 *`iswuser`* 的用户。

2. 要在 Solaris 上安装 Sun Java System Directory Server Connector，安装过程中必须为 “连接器”选择一个无权限的端口。
   （例如，可以使用大于 1024 的端口。）

   注意 必须以 `root` 身份执行其余步骤中的所有命令。

3. 安装所有组件之后，请执行下列命令停止 Identity Synchronization for Windows：

   `/etc/init.d/isw stop`

4. 必须更新实例目录的拥有权。
   例如，如果您是在 /var/opt/SUNWisw 中安装的产品。

   ```
   chown -R iswuser /var/opt/SUNWisw
   chown -R iswuser /opt/SUNWisw
   ```

5. 在文本编辑器中，打开 /etc/init.d/isw 文件并将以下行：

   ```
   "$EXEC_START_WATCHDOG" "$JAVA_PATH" "$INSTALL_DIR" "CONFIG_DIR"
   ```

   替换为：

   ```
   su iswuser -c "$EXEC_START_WATCHDOG '$JAVA_PATH' '$INSTALL_DIR'
   'CONFIG_DIR'"
   ```

6. 执行以下命令重新启动服务：

   ```
   /etc/init.d/isw start
   ```

7. 执行以下命令检验各组件是否用指定用户的用户 ID 运行：

   ```
   ps -ef | grep iswuser
   ```

定义和配置同步用户列表

本附录提供有关“同步用户列表” (SUL) 各个定义的补充信息，并说明如何配置多个域。内容具体安排如下：

了解同步用户列表定义

每个“同步用户列表” (SUL) 都包含两个定义 — 一个用于确定要同步的 Directory Server 用户，另一个用于确定要同步的 Windows 用户。

每个定义确定要同步目录中的哪些用户、哪些用户不在同步范围内以及在何处创建新用户。

注意 使用 “Identity Synchronization for Windows 控制台”选择的对象类还确定将同步哪些用户。程序只同步具有选定对象类的那些用户，包括具有选定对象类的子类的任何用户。

例如，如果选择 `organizationalPerson` 对象类，则 Identity Synchronization for Windows 将同步具有 `inetorgperson` 对象类的用户，因为它是 `organizationalPerson` 对象类的子类。

表 D-1 说明了 SUL 定义的要素：

表 D-1 SUL 定义要素

要素	定义	适用范围		
		Sun	AD	NT
基本 DN	定义要同步的所有用户的父 LDAP 节点。 “同步用户列表”基本 DN 包括该 DN 中的所有用户 — 除非用户被“同步用户列表”过滤器排除在外，或者该用户的 DN 符合更具体的“同步用户列表”。例如， `ou=sales,dc=example,dc=com`。	是	是	否
过滤器	定义一个类似于 LDAP 的过滤器，用于将用户包括在“同步用户列表”之内或排除在外。该过滤器可包括 `&`、 `|`、 `!`、 `=` 和 `*` 运算符。不支持 `>=` 和 `<=` 运算符。所有比较都不区分大小写。 例如， `(&(employeeType=manager)(st=CA))` 将仅包括加利福尼亚的经理。	是	是	是
创建表达式	定义新创建用户的父 DN 和命名属性（仅当启用创建时才适用）。 创建表达式必须含有“同步用户列表”的基本 DN。例如， `cn=%cn%,ou=sales,dc=example,dc=com`。（其中的 `%cn%` 标记用创建的用户条目的值代替。）	是	是	否

注意 如果要同步 Sun Java System Directory Server 中有多个 Active Directory 域的用户，必须为每个 Active Directory 域定义至少一个 SUL。

如果定义了多个 SUL，Identity Synchronization for Windows 会通过反复匹配每个 SUL 定义来确定 SUL 中的成员关系。程序首先检查基本 DN 较具体的 SUL 定义。例如，程序首先测试是否与 `ou=sales,dc=example,dc=com` 匹配，然后再测试是否与 `dc=example,dc=com` 匹配。

如果两个 SUL 定义有相同的基本 DN 而过滤器不同，则 Identity Synchronization for Windows 就无法自动确定应先测试哪个过滤器。此时，必须用“解决域交叉”功能为两个 SUL 定义排序。如果用户符合某个 SUL 定义的基本 DN，但不符合该基本 DN 的任何过滤器，程序会将该用户排除在同步之外 — 即使该用户与具体程度稍差一些的基本 DN 的过滤器相符。

配置多个 Windows 域

为支持将多个 Windows 域同步到同一个 Directory Server 容器 （例如 `ou=people,dc=example,dc=com`）， Identity Synchronization for Windows 使用含有域信息的 “综合” Windows 属性。

- 对于 Active Directory 域， Identity Synchronization for Windows 会先将 `activedirectorydomainname` 属性设置为 Active Directory 域名 （如 *east.example.com*），然后再将该条目同步到 Directory Server。
- 对于 Windows NT 域， Identity Synchronization for Windows 会先将 `user_nt_domain_name` 属性设置为 Windows NT 域名 （如 *NTEXAMPLE*），然后再将该条目同步到 Directory Server。

虽然这些属性不实际出现在 Windows 用户条目中，却可在 “Identity Synchronization for Windows 控制台”中同步，并可映射到 Directory Server 用户属性。 Identity Synchronization for Windows 映射域属性后，它们将在同步期间被置入 Directory Server 条目，并可在 “同步用户列表” (SUL) 过滤器中使用。

下例说明了 Identity Synchronization for Windows 如何使用这些属性。此例假设三个 Windows 域 （两个 Active Directory 域和一个 Windows NT 域）与一个 Directory Server 实例同步。

1. Active Directory 的 east.example.com 域中的用户将以 `ou=people,dc=example,dc=com` 同步到 Directory Server 中。
2. Active Directory 的 west.example.com 域中的用户将以 `ou=people,dc=example,dc=com` 同步到 Directory Server 中。
3. Windows NT 的 NTEXAMPLE 域中的用户将以 `ou=people,dc=example,dc=com` 同步到 Directory Server 中。

创建或修改 Directory Server 用户时，程序用 SUL 过滤器确定要在哪个 Windows 域中同步用户 （因为每个 Directory Server SUL 都有相同的基本 DN，`ou=people,dc=example,dc=com`）。使用 `activedirectorydomainname` 和 `user_nt_domain_name` 属性可以很方便地构建这些过滤器。

要从 “控制台”的 “属性”选项卡构建过滤器：

1. 将 Directory Server `destinationindicator` 属性映射到 Active Directory `activedirectorydomainname` 属性和 Windows NT `user_nt_domain_name` 属性。
2. 按以下方式为每个 Windows 域配置一个 SUL：

```
EAST_SUL
  Sun Java System Directory Server definition
    Base DN:  ou=people,dc=example,dc=com
    Filter:  destinationindicator=east.example.com
    Creation Expression:  cn=%cn%,ou=people,dc=example,dc=com
Active Directory definition (east.example.com)
    Base DN:  cn=users,dc=east,dc=example,dc=com
    Filter:<none>
    Creation Expression:  cn=%cn%,cn=users,dc=east,dc=example,dc=com
WEST_SUL
  Sun Java System Directory Server definition
    Base DN:  ou=people,dc=example,dc=com
    Filter:  destinationindicator=west.example.com
    Creation Expression:  cn=%cn%,ou=people,dc=example,dc=com
Active Directory definition (west.example.com)
    Base DN:  cn=users,dc=west,dc=example,dc=com
    Filter:<none>
    Creation Expression:  cn=%cn%,cn=users,dc=west,dc=example,dc=com
NT_SUL
  Sun Java System Directory Server definition
    Base DN:  ou=people,dc=example,dc=com
    Filter:  destinationindicator=NTEXAMPLE
    Creation Expression:  cn=%cn%,ou=people,dc=example,dc=com
Windows NT definition (NTEXAMPLE)
    Base DN:  NA
    Filter:<none>
    Creation Expression:  NA
```

注意：每个 Directory Server SUL 定义都有相同的基本 DN 和创建表达式，但过滤器指示相应 Windows 用户条目的域。

为进一步说明这些设置如何允许 Directory Server 用户条目与单独的 Windows 域同步，请参考以下测试条件：

1. 在 Active Directory 的 east.example.com 域中创建 `cn=Jane Test,cn=users,dc=east,dc=example,dc=com`。
2. Identity Synchronization for Windows 在 Directory Server 中创建用户条目 `cn=Jane Test,ou=people,dc=example,dc=com`，该 Directory Server 含有 `destinationindicator=east.example.com` 条目。
3. 修改 Directory Server 中的 `cn=Jane Test,ou=people,dc=example,dc=com` 条目。
4. 因为 Jane Test 的 `destinationindicator` 属性为 east.example.com，其条目符合 `EAST_SUL` “同步用户列表”过滤器，修改内容将同步到 east.example.com Active Directory 域。

本例假设 Identity Synchronization for Windows 将用户创建从 Windows 同步到 Directory Server。如果情况与此不同，可以运行 `idsync resync` 命令设置 `destinationindicator` 属性。

注意 在具有多个 SUL 的部署中使用 `idsync resync -f` 时，可能必须在链接配置文件中将 `allowLinkingOutOfScope` 选项设置为 `true`。有关详细信息，请参阅附录 B，“LinkUsers XML 文档范例”。

示例中使用了 `inetorgperson`, `destinationIndicator` 的已有属性，此属性还可能另有所用。如果此属性已在使用或者您选择了不同的对象类，则必须将用户的 Directory Server 条目中的某些属性映射到 `user_nt_domain_name` 和 / 或 `activedirectorydomainname` 属性。选择用于保存此值的 Directory Server 属性必须在其余属性映射配置使用的对象类中。

如果没有未使用的属性来保存此域信息，则必须创建一个新的对象类，将新的域属性和 Identity Synchronization for Windows 要使用的所有其它属性包括在内。

复制环境的安装注意事项

Identity Synchronization for Windows 1 2004Q3 支持对单个复制后缀中的用户进行同步。

注意 本附录总结了用于配置和保护多主复制 (MMR) 部署的过程。信息直接取自 《*Sun Java System Directory Server 5 2004Q2 Administrator's Guide*》 — 并非 Identity Synchronization for Windows 特有。

MMR 部署的设计和实施非常*复杂*。设计部署请参阅 《*Sun Java System Directory Server 5 2004Q2 Deployment Guide*》，实施部署请参阅 《*Sun Java System Directory Server 5 2004Q2 Administrator's Guide*》。

本附录被编排为以下各节：

配置复制

注意 在多主复制 (MMR) 环境中，Identity Synchronization for Windows 允许为任何给定的 Sun 目录源指定首选主服务器和备用主服务器。

Directory Server 版本 5 2004Q2 现在支持四路 MMR （您可以在四台主服务器中的任何一台上更改复制的数据库）。在第三或第四台主服务器上安装 “插件”时，在 “插件”安装过程中必须选择*其它*主机类型并手动输入 Directory Server 实例的参数。

下列步骤假设您要复制单个后缀。如果要复制多个后缀，可以同时在每台服务器上配置它们。换言之，可通过在多个后缀上重复每个步骤配置复制。

要配置任意复制拓扑，请按以下顺序进行：

1. 除了单独主服务器外，在所有其它服务器上定义复制管理器条目 （或者在所有服务器上使用默认复制管理器）。
2. 在含有专门用户副本的所有服务器上：
   a. 为用户副本创建一个空后缀。
   b. 通过复制向导启用后缀上的用户副本。
   c. 配置高级副本设置，此为可选步骤。
3. 如果适用，在含有集线器副本的所有服务器上：
   a. 为集线器副本创建一个空后缀。
   b. 通过复制向导在后缀上启用集线器副本。
   c. 配置高级副本设置，此为可选步骤。
4. 在含有主副本的所有服务器上：
   a. 在其中一台主服务器上选择或创建一个将作为主副本的后缀。
   b. 通过复制向导在后缀上启用主副本。
   c. 配置高级副本设置，此为可选步骤。
5. 按以下顺序在所有提供者副本上配置复制协议：
   a. 在多主服务器集合中的各主服务器之间。
   b. 在各主服务器及其专门用户之间。

c. 在各主服务器和集线器副本之间。

   或者，可在此阶段配置部分复制。

6. 配置集线器副本及其用户间的复制协议。
7. 对于多主复制，从含有数据原始副本的同一主副本初始化所有主服务器。初始化集线器和用户副本。

对通过 SSL 复制进行配置

注意 在本步骤中，所有引用都是《*Sun Java System Directory Server 5 2004Q2 管理指南*》中的章节。

要将复制过程中涉及的 Directory Server 配置为所有复制操作都通过 SSL 连接完成，请完成以下步骤：

1. 将提供者和用户服务器配置为使用 SSL。

   详细信息，请参阅第 11 章 “管理验证和加密”。

   注意
   - 如果提供者服务器证书是仅限 SSL 服务器的证书，无法在 SSL 信号交换期间充当客户机，则通过 SSL 复制将会失败。
   - 当前，自签名证书不支持通过 SSL 复制。

2. 如果没有为用户服务器上的后缀配置复制，请按第 8 章中 “启用用户副本”的说明启用复制。
3. 遵循第 8 章中 “高级用户配置”的步骤，将用户的证书条目的 DN 定义为另一个复制管理器。
4. 如果没有为提供者服务器上的后缀配置复制，请按第 8 章中 “启用集线器副本”或 “启用主副本”的说明启用复制。
5. 在提供者服务器上创建一个新的复制协议，将更新信息发送到安全 SSL 端口上的用户。有关详细说明，请按第 8 章中 “创建复制协议”的步骤操作。在用户服务器上指定一个安全端口，选择使用密码或证书的 SSL 选项。为选择的 SSL 选项输入一个 DN，可以是复制管理器或者证书。

完成复制协议的配置后，提供者会通过 SSL 将所有复制更新信息发送给用户，如果选择了证书选项，还会使用证书。如果通过控制台使用为 SSL 配置的协议执行客户初始化，则客户初始化也会使用安全连接。

在 MMR 环境中配置 Identity Synchronization for Windows

下列过程总结在 MMR 环境中配置 Identity Synchronization for Windows 的步骤 — 详细说明在本书的其它章节提供。

1. 从 “Identity Synchronization for Windows 控制台” 为要同步的后缀指定首选和备用 Directory Server 主服务器。（请查看第 102 页的 “创建 Sun Java System Directory 源”。）

   不必在拓扑中提供有关其它 Directory Server 的信息。

2. 通过 “控制台” 或者使用 `idsync prepds` 命令行实用程序准备首选和备用服务器。（请查看第 109 页的 “准备 Directory Server”或第 313 页的 “使用 prepds”。）

   如使用命令行实用程序，应通过为首选服务器和备用服务器指定参数来同时在单个调用中准备这两台服务器。

3. 为在这些目录之间复制的后缀安装 Directory Server Connector。（请查看第 159 页的 “安装 Directory Server Connector”。）

4. 在首选主服务器、备用主服务器和管理复制后缀中的用户的所有其它 Directory Server 实例上安装 Directory Server 插件。（请查看第 169 页的 “安装 Directory Server 插件”。）

术语

下面是 Identity Synchronization for Windows 产品和本套文档中使用的术语。

安全套接字层　请参阅 SSL。

绑定 DN　执行某项操作时，用于对 LDAP 目录（如 Active Directory 或 Directory Server）进行验证的识别名。

绑定识别名　请参阅绑定 DN。

备用目录服务器　在 MMR 环境中的目录服务器主机实例，当首选目录服务器不可用时， Identity Synchronization for Windows 可以使用备用目录服务器。当首选目录服务器不可用时， Identity Synchronization for Windows 可以将 Active Directory 或 Windows NT 中的更改同步到备用目录服务器，但是在备用服务器或任何其它目录服务器主机上的更改则只有在首选目录服务器可用时才能同步。

CA　请参阅证书授权机构。

CLI　请参阅命令行界面

操作　单个同步事件的封装。 Identity Synchronization for Windows 连接器使用操作传达用户更改事件。每个操作包括一个类型 （如 `CREATE`、 `MODIFY` 或 `DELETE`）以及来自用户条目的充足属性，以使目标连接器可以同步更改。所有操作都是最基本的处理。

层叠复制　在层叠复制方案中，对于特定副本，一台服务器 （通常称为*集线器提供者*）既充当用户又充当提供者。该服务器保存只读副本，并保留更改日志。它从存储数据主副本的提供者服务器接收更新，然后将这些更新提供给用户。

插件 一个可以被加载并用作整个系统的一部分的辅助程序。

例如， Identity Synchronization for Windows 使用 Directory Server 插件来增强 Directory Server Connector 的更改检测功能，并对 Active Directory 与 Directory Server 之间的密码同步提供双向支持。

超级用户 请参阅根用户。

出站 在连接器内，从 Message Queue 向目录源流动的操作方向。由连接器应用的更改按出站方向流动到同步的目录源。关于操作的日志信息经常涉及发生在连接器出站端的事件。

创建属性 仅当创建对象时才同步的属性。所有重要属性都在创建对象时自动同步。可以为在远程目录中没有对应属性值的创建属性配置默认值。

存取程序 一个通过诸如 LDAP 等协议与目录源直接接口的连接器层。 Identity Synchronization for Windows 对 Directory Server、 Active Directory 和 Windows NT 执行相互独立的存取程序。关于操作的日志消息经常涉及存取程序。

DIT 请参阅目录信息树。

DM 请参阅目录管理员。

DNS 域名系统。网络中的计算机用来将标准 IP 地址 （如 198.93.93.10）与主机名（如 `www.example.com`）相关联的系统。计算机通常从 DNS 服务器上获得主机名的 IP 地址，或从所在系统维护的表格中查找该地址。

代理 一种连接器组件，它与 Message Queue 连接，并在属性的 Directory Server 名称和 Windows 名称间转换属性。关于操作的日志消息经常涉及代理。

代理程序 请参阅 Sun Java System Message Queue 代理程序。

对象高速缓存 Windows 连接器用来检测用户条目更改的处理中的数据库。对象高速缓存存储每个用户条目的散列摘要，该摘要使 Windows 连接器可以确定用户条目中被修改的具体属性。

对象类 一种模板，用于指定条目描述的对象种类及条目包含的有效和强制属性集合。例如， Directory Server 指定一个含有诸如 `cn` 和 `userpassword` 属性的 `inetorgperson` 对象类。即时请求密码同步：一种机制，在该机制下，用户在 Directory Server 中的密码直到该用户尝试进行 Directory Server 登录验证时才被更新。仅当提供的密码与存储在 Active Directory 中的密码匹配时才同步用户密码。此机制简化了 Active Directory 环境中的密码同步。

多主复制 一种目录服务器复制模型，在该模型中，条目无需在执行写入或更新前与其它主机副本通信，就可以对多个主机副本中的任何副本执行写入或更新操作。在一台服务器上进行的更改会自动复制到其它服务器上。 Identity Synchronization for Windows 可以安装到含有多个目录服务器主机的部署中。但是，当将更改同步到 Windows 时，首选目录服务器必须是可用的，而当从 Windows 同步更改时，首选或备用服务器之一必须是可用的。

FSMO 角色 “灵活单主机操作”角色。Active Directory 用来防止在多主机部署中发生更新冲突的机制。即使是多主服务器部署，有些对象也以单主服务器模式更新。这与过去 Windows NT 域中的 “主域控制器” (PDC) 概念很相似。在 Active Directory 部署中有五个 FSMO 角色，但只有 PDC 仿真器角色影响 Identity Synchronization for Windows。因为密码更新仅会立即复制到带有 PDC 仿真器角色的 Active Directory 域控制器，所以 Identity Synchronization for Windows 使用此域控制器进行同步。否则，与 Sun Java System Directory Server 的同步可能会延迟数分钟。

服务 Windows 计算机上负责特定系统任务的后台进程。服务进程可连续运行而无需人为干预。在 Windows 上，连接器、系统管理器和中心记录器作为由 Identity Synchronization for Windows 监视器服务启动和监视的进程而运行。

服务器根 服务器上专用于存储服务器程序配置、维护和信息文件的目录。

辅助对象类 对选定结构类进行扩充的对象类，它提供了同步的附加属性。请参阅结构对象类。

根后缀 一个或多个 LDAP 子后缀的父项。一个目录树可包含多个根后缀。

根用户 UNIX 计算机上可用的具有最高权限的用户 （也称为超级用户）。根用户拥有对计算机上所有文件的完全访问权限。在 Solaris 系统上， Identity Synchronization for Windows 必须作为根用户安装。

核心 安装的第一个 Identity Synchronization for Windows 组件。“核心”包括存储在配置目录中的初始配置、系统管理器、中心记录器、控制台和命令行界面。

后缀 位于目录树顶端的条目的名称，数据即存储在该条目下。同一目录中可能有多个后缀。每个数据库仅有一个后缀。

Identity Synchronization for Windows 控制台 用于配置和监视 Identity Synchronization for Windows 的图形用户界面。

IP 地址 “Internet 协议”地址。一组由句点分隔的数字，用于指定 Internet 上的计算机的实际位置 （例如， 192.168.2.1）。

ISO 国际标准化组织。

Java 消息服务 一种标准 API 消息，允许基于 Java 2 平台企业版 (J2EE) 的应用程序组件创建、发送、接收和读取消息。它可以实现松散耦合、可靠和异步的分布式通信。

JMS 请参阅 Java 消息服务。

基本 DN 基本识别名。搜索操作在基本 DN、条目的 DN 和目录树中所有在其下的条目上执行。对于 Active Directory 和 Directory Server，“同步用户列表”基于特定的基本 DN 而确立。除非使用某个过滤器将用户明确排除，否则将同步此基本 DN 下的所有用户。

基本识别名 请参阅基本 DN。

监视器 独立的 Java 进程，它安装在每个安装了“核心”或连接器的计算机上。“监视器”启动所有 Identity Synchronization for Windows Java 进程，包括系统管理器、中心记录器和连接器。如果上述任何组件发生故障，则“监视器”会重新启动它们。在 Solaris 上，“监视器”是通过 `/etc/init.d/isw` 守护进程脚本控制的，在 Windows 上，它是通过“Sun Java™ System Identity Synchronization for Windows”服务控制的。

结构对象类 条目的主对象类，用于定义 Identity Synchronization for Windows 同步的用户条目上的有效和强制属性集合。例如，默认的 Active Directory 对象类是 `user`，默认的 Directory Server 对象类是 `inetorgperson`。请参阅辅助对象类。

客户机 请参阅 LDAP 客户机。

控制器 与代理和存取程序组件连接的连接器组件。控制器执行与同步有关的关键任务，如确定用户在“同步用户列表”中的成员关系、搜索并链接等效用户条目、通过将当前用户条目与存储在对象高速缓存中的以前版本进行比较来检测对用户进行的更改等。关于操作的日志消息经常涉及控制器。

控制台 用于配置和监视服务器应用程序的图形用户界面。 Sun Java System Directory Server 和 Identity Synchronization for Windows 具有相互独立的控制台。

LDAP 轻量级目录访问协议。专用于通过 TCP/IP 并跨多个平台运行的目录服务协议。 Identity Synchronization for Windows 使用 LDAP 与 Active Directory 域控制器和 Sun Java System Directory Server 通信。

LDAP URL 提供使用 DNS 定位目录服务器，然后通过 LDAP 完成查询的方法。LDAP URL 的一个示例为 `ldap://ldap.example.com`

LDAP 客户机 用于从 LDAP Directory Server 请求和查看 LDAP 条目的软件。Identity Synchronization for Windows 连接器在连接到 LDAP 服务器时作为 LDAP 客户机使用。

连接器 管理 Identity Synchronization for Windows 与单独数据源 （如 Directory Server、 Active Directory 域或 Windows NT 域）交互的 Java 进程。连接器负责检测数据源中的用户更改，并通过 Message Queue 将这些更改发布到远程连接器，还负责订阅用户更改主题以及将来自这些主题的更新应用到数据源。

Message Queue 请参阅 Sun Java System Message Queue。

MMR 请参阅多主复制。

MQ 请参阅 Sun Java System Message Queue。

密码文件 UNIX 计算机上的一个文件，用于存储 UNIX 用户登录名称、密码和用户 ID。因其所处位置，它又称为 `/etc/passwd`。

密码策略 用于控制在给定目录下密码使用方式的一组规则。

命令行界面 程序和用户之间的通信方式，它的输入输出完全基于文本。命令通过键盘或类似设备输入，然后由程序解释和执行。 Identity Synchronization for Windows 命令行界面称为 `idsync`，可以从安装了 “核心”的 `bin/` 目录获得。

命名上下文 （也称为根后缀）目录信息树 (DIT) 的特定后缀，由其识别名 (DN)（例如 dc=example、 dc=com）标识。在 Identity Synchronization for Windows 中， Sun Java System Directory Server 的目录源由包含要同步的数据的后缀定义。

模式 用于描述哪些类型的信息可作为条目存储在目录中的定义。当与模式不匹配的信息存储在目录中时，试图访问该目录的客户机可能不能显示正确的结果。

模式检查 确保目录中添加或修改的条目与定义的模式相符。默认情况下模式检查为开启状态，如果用户试图保存与模式不相符的条目，将会出错。

目录管理员 获得授权的目录服务器管理员，相当于 UNIX 中的超级用户。Identity Synchronization for Windows 需要 “目录管理员”证书才能执行某些配置操作，但是连接器进行同步不需要 “目录管理员”证书。

目录信息树 存储在目录中的信息的逻辑表示。它镜像大多数文件系统采用的树模式，在这种模式中树根位于层次结构的顶部。

目录源 Sun Java System Directory Server、 Windows Active Directory 域或 Windows NT 域。目录源含有要同步的用户。

配置密码 在安装 “核心”过程中选择的密码，用于保护保存在配置目录中的所有 Identity Synchronization for Windows 敏感信息。在使用安装程序、控制台或命令行界面时必须提供配置密码。

配置目录 Directory Server 的特殊安装，作为配置和状态信息的信息库使用。Identity Synchronization for Windows 存储安装 “核心”时选择的配置目录实例内的所有配置。

配置注册表 Identity Synchronization for Windows 用来表示配置目录的另一个术语。

轻量级目录访问协议 请参阅 LDAP。

全局目录 存储 Active Directory 目录拓扑和 Active Directory 目录模式信息的 Windows 信息库。

权限 在访问控制的上下文中，权限表明对目录信息进行的访问是被获准还是被拒绝，以及被获准或拒绝的访问的级别。

确认 确认从其它组件收到消息的专用消息。 Identity Synchronization for Windows 在连接器和 Message Queue 之间以及各种连接器组件 （代理、控制器和存取程序）之间使用确认，以确保所有更改都已可靠同步。

RCL 请参阅 retro changelog。

retro changelog Directory Server 数据库 (cn=changelog)，用于存储对 Directory Server 进行的所有更改的记录。Identity Synchronization for Windows 使用 retro changelog 检测对 Directory Server 进行的更改。在 MMR 环境中，必须在 “首选目录服务器”上启用 retro changelog。

入站 在连接器内，从目录源流向 Message Queue 的操作方向。连接器检测到的更改按入站方向流入系统。关于操作的日志信息经常涉及发生在连接器入站端的事件。

Server Console 基于 Java 的应用程序，允许通过 GUI 对 Directory Server 进行管理。

SSL 安全套接字层。用于在客户机和服务器双方之间建立安全连接的软件库。用于执行 HTTPS （HTTP 的安全版本）和 LDAPS （LFAP 的安全版本）。

SUL 请参阅同步用户列表。

Sun Java System Message Queue 执行 Java Message Service (JMS) 开放标准的企业消息系统。 Message Queue 的基本体系结构由使用一般服务交换消息的发布者和订阅者组成。 Sun Java System Message Queue 由专用的消息代理程序管理，该代理程序负责控制对 Message Queue 的访问、维护活动的发布者和订阅者信息以及确保消息的交付。 Identity Synchronization for Windows 使用 Message Queue 安全地同步用户更改事件、分配配置信息和监视远程组件的运行状况。

Sun Java System Message Queue 代理程序 独立的 Java 服务器，为客户机提供对 Sun Java System Message Queue 的访问权限。在 Solaris 上，此“代理程序”通过 `/etc/init.d/imq daemon` 脚本控制，在 Windows 上，它通过“iMQ Broker”服务控制。 Identity Synchronization for Windows 在安装“核心”时配置和启动此代理程序。

审计日志 包含日常事件条目（如要同步的用户密码）的中心日志文件。管理员可以使用“Identity Synchronization for Windows 控制台”控制此日志中显示的条目数量及详细程度。

每个连接器均生成一个由该连接器处理的用户的审计日志，同时，还有一个集中的审计日志，含有由部署中的所有连接器生成的审计日志的集合。

识别名 表示条目名称及其在 LDAP 目录中位置的字符串。

守护进程 UNIX 计算机上负责特殊系统任务的一个后台进程。守护进程可连续运行而无需人为干预。连接器、系统管理器和中心记录器作为由 Identity Synchronization for Windows 监视器启动和监视的守护进程而运行。

首选目录服务器 Identity Synchronization for Windows 用来检测和应用用户条目更改的目录服务器主机实例。当此服务器可用时， Identity Synchronization for Windows 不与任何其它目录服务器主机通信。

属性 保存条目的描述性信息。属性具有一个标签和一个值。对于可存储为属性值的信息类型，每个属性还遵循一个标准语法。

属性列表 对于给定条目类型或对象类的必需的以及可选的属性的列表。

同步用户列表 定义 Sun 和 Windows 目录中要同步的用户。“同步用户列表”可以基于 LDAP 基本 DN 或过滤器限制要同步的用户范围。

同步主机 依照“同步用户列表” (SUL) 中定义的规则存储同步数据的服务器。

拓扑 在物理服务器间划分目录树以及这些服务器间相互链接的方式。

uid 与 UNIX 系统上每一用户相关的唯一编号。

URL 统一资源定位器。服务器和客户机用于请求文档的寻址系统。它通常称为位置。 URL 的格式为 `[protocol]://[machine:port]/[document]`。端口号仅在选定服务器上是必需的，并且它通常由服务器指定，用户无需将其置于 URL 中。

文件扩展名 文件名中句点或点 (.) 后面的部分，通常定义文件类型（例如， .GIF 和 .HTML）。例如，在名为 `index.html` 的文件中，文件扩展名为 *`html`*。

文件类型 给定文件的格式。例如，图形文件通常保存为 `GIF` 格式，而文本文件通常保存为 `ASCII` 文本格式。文件类型通常由文件扩展名标识（例如， .GIF 或 .HTML）。

系统管理器 独立的 Java 进程，由安装了“核心”的“监视器”守护进程 / 服务启动。系统管理器将配置信息分配给连接器和中心记录器，监视系统的运行状况并协调 `idsync resync` 操作。

协议 描述网络上设备间信息交换方式的一组规则。

验证 验证登录到 Directory Server 的客户机用户身份的进程。为了获准访问该目录，用户必须提供绑定 DN 及相应密码。根据目录管理员授予用户的许可，Directory Server 允许用户执行功能或访问文件和目录。

验证证书 由第三方发放的、不能转让和伪造的数字文件。验证证书从服务器发送到客户机（或从客户机发送到服务器），用以核实和验证对方的身份。

已同步的属性 请参阅重要属性。

语言环境 标识特定地区、文化和 / 或习俗的用户用于表示数据的整理序列、字符类型、货币格式以及时间 / 日期格式。还包括关于如何解释、存储或整理给定语言数据的信息。语言环境还用于指示对于给定语言应当使用的代码页。

域 (1) (n.) 全限定域名的最后部分，标识拥有该域名的公司或组织（例如，example.com、 host.example.com）。

(2) (n.) 在单个计算机系统控制下的资源。

域控制器 存储用户帐户信息、验证用户身份和强制执行 Windows 域安全策略的 Windows 服务器。 Identity Synchronization for Windows 连接器直接与域控制器通信，以检测对用户帐户进行的更改并同步在 Directory Server 用户条目中进行的更改。

再同步间隔 连接器检查目录源更改的频率。此周期性检查是高效的，并且只需读取自上次检查以来发生更改的用户条目。控制台以毫秒为单位表示此值，默认值为 1000 （1 秒）。

证书　将公共密钥与网络身份关联的数据集合。此信息可以使电子消息接收者验证消息和消息发送者的真实性。当您将 Identity Synchronization for Windows 连接器配置为使用 SSL 通信时，必须将证书添加到连接器的证书数据库后，才能进行信任 SSL 通信。另请参阅证书授权机构。

证书授权机构　销售和发放验证证书的公司或组织。可以从您信任的证书授权机构（又称为 *CA*）购买验证证书。超级用户证书授权机构证书用于签署其它证书。当您将 Identity Synchronization for Windows 连接器配置为使用 SSL 通信时，必须将合适的超级用户证书授权机构证书添加到 “连接器”的证书数据库中。

证书数据库　安全的证书信息库，它包括以下三个文件：`cert8.db`、`key3.db` 和 `secmod.db`。在 Identity Synchronization for Windows 中，每个连接器都有自己的证书数据库目录 （例如，`<`*install-root*`>/etc/CNN100`）。另请参阅证书。

中心记录器　管理所有中心日志的 “核心”组件，它是每个连接器的审计和错误日志的集合。管理员可以通过监视这些日志监视整个 Identity Synchronization for Windows 安装的运行状况。可以直接或从 “Identity Synchronization for Windows 控制台”查看中心日志。默认情况下，在安装了 “核心”的机器的 `<`*install-root*`>/logs/central/` 子目录下可获得中心日志。

重要属性　在创建或修改条目时同步的属性。

主对象类　请参阅结构对象类。

主机名　machine.domain.com 形式的计算机名，该名称被转换成 IP 地址。例如，`www.example.com` 为计算机 *www*，该计算机处于子域 *example* 和域 *com* 中。

子组件　子组件是一个独立于连接器运行的轻量级进程或库。子组件在连接器管理的目录源附近运行，实现在连接器中无法从远程计算机或单独进程获得的功能。子组件通过自定义加密频道与连接器通信，以接收配置信息、报告更改事件并记录到中心记录器。 Identity Synchronization for Windows 包括以下三个子组件：Directory Server 插件、 Windows NT Password Filter DLL 和 Windows NT Change Detector。

字符类型　使字母字符与数字 （或其它）字符区别开来，并包括大小写字母转换。

索引

数字

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

W

X

Y

Z