NetIQ Identity Manager

安装指南 - Windows

2018 年 3 月

NetIQ

法律声明

目录

关于本书和库

本 *《安装指南》*中提供了安装 NetIQ Identity Manager (Identity Manager) 产品的相关说明。其中介绍了在分布式环境中安装各个组件的过程。

适用对象

本书提供的信息面向负责安装必要组件以为其组织构建身份管理解决方案的身份设计者和身份管理员。

库中的其他信息

有关 Identity Manager 库的详细信息，请参见 Identity Manager 文档网站。

关于 NetIQ Corporation

我们是一家全球性的企业软件公司，专注于您的环境中三大永恒挑战：变化、复杂性和风险，设法帮助您应对这些挑战。

我们的观点

适应变化及管理复杂性和风险实乃老生常谈

实际上在您面临的所有挑战中，这些也许是容易让您失控的最突出变数，从而无法安全地衡量、监视和管理您的物理环境、虚拟环境和云计算环境所需。

提供更好、更快的关键业务服务

我们相信，尽可能多地为 IT 组织提供控制，是更及时、经济有效地交付服务的唯一方法。只有在组织不断做出改变，并且管理这些变化所需的技术本身日益复杂时，持续存在的压力 （如变化和复杂性）才会继续增大。

我们的理念

销售智能解决方案，而不只是软件

为了提供可靠的控制，我们首先务必了解 IT 组织 （如贵组织）的实际日常运作情况。这才是我们可以开发出实用的智能型 IT 解决方案以成功取得公认的重大成果的唯一途径。并且，这比单纯销售软件要有价值得多。

推动您走向成功是我们的追求

我们将您的成功视为我们业务活动的核心。从产品启动到部署，我们深知：您需要与您当前购买的解决方案配合使用和完美集成的解决方案；您需要在部署后获得持续的支持并接受后续的培训；您还需要真正易于合作的伙伴一起应对变化。总之，只有您成功，才是我们都成功。

我们的解决方案

- 身份和访问管理
- 访问管理
- 安全管理
- 系统和应用程序管理
- 工作负载管理
- 服务管理

与销售支持联系

若对产品、定价和功能有疑问，请与本地合作伙伴联系。如果无法与合作伙伴联系，请与我们的销售支持团队联系。

全球：	www.netiq.com/about_netiq/officelocations.asp
美国和加拿大：	1-888-323-6768
电子邮件：	info@netiq.com
网站：	www.netiq.com

联系技术支持

有关具体的产品问题，请与我们的技术支持团队联系。

全球：	www.netiq.com/support/contactinfo.asp
北美和南美：	1-713-418-5555
欧洲、中东和非洲：	+353 (0) 91-782 677
电子邮件：	support@netiq.com
网站：	www.netiq.com/support

联系文档支持

我们的目标是提供满足您的需要的文档。 NetIQ 网站上提供了本产品 HTML 和 PDF 格式的文档，您无需登录即可访问该文档网页。如果您对文档改进有任何建议，请单击 www.netiq.com/documentation 上发布的 HTML 版本文档任一页面下方的**评论该主题**。您还可以发送电子邮件至 Documentation-Feedback@netiq.com。我们会重视您的意见，欢迎您提供建议。

联系在线用户社区

NetIQ 在线社区 NetIQ Communities 是让您可与同行及 NetIQ 专家沟通的协作网络。 NetIQ Communities 上提供了更多即时信息、实用资源的有用链接，以及联系 NetIQ 专家的途径，有助于确保您掌握必要的知识，以充分发挥所依赖的 IT 投资的潜力。有关详细信息，请访问 community.netiq.com。

简介

NetIQ Identity Manager 可帮助您构建智能身份管理框架 （无论是在防火墙内还是在云中），来为您的企业提供服务。 Identity Manager 会集中管理用户访问权，并确保从您的物理与虚拟网络到云，每个用户都具有一致的身份。

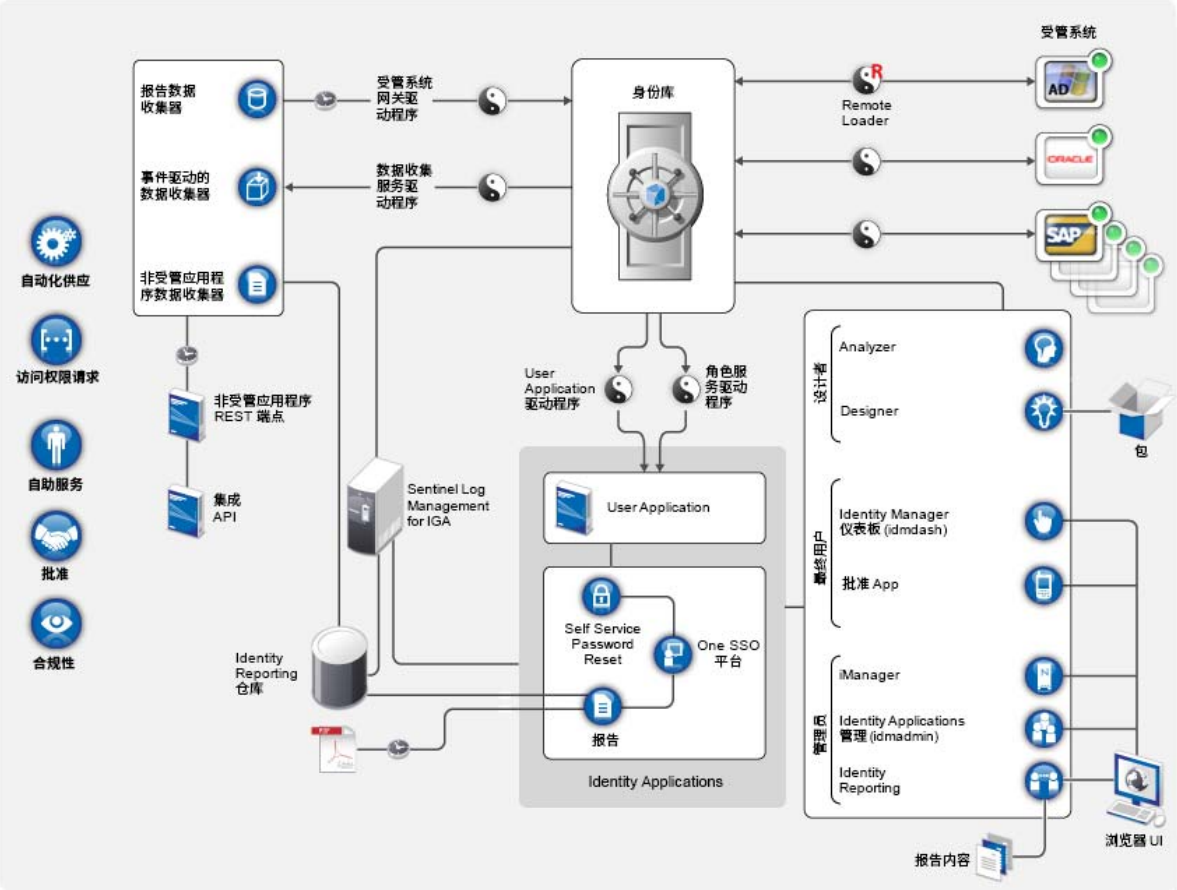
一般而言，您可以将构成 Identity Manager 的组件分成下列功能：

- 创建和维护 Identity Manager 环境。有关详细信息，请参见第 2 章 “ 创建和维护 Identity Manager 环境 ”（第 21 页）。
- 监控 Identity Manager 环境，包括审计和报告用户供应活动的功能。如此，您便可以证明对业务、 IT 及企业策略的合规性状况。有关详细信息，请参见第 3 章 “ 在 Identity Manager 环境中管理数据 ”（第 23 页）。
- 管理用户供应活动，例如单个用户的角色、证明和自助服务。有关详细信息，请参见第 4 章 “ 供应用户以进行安全的访问 ”（第 27 页）。

本部分介绍了可帮助您执行这些活动的各个 Identity Manager 组件。掌握这些知识之后，您便可以开始规划产品安装。要了解这些组件如何是互连的，请参见第 1 章 “Identity Manager 的组件概述 ”（第 19 页）。

1 Identity Manager 的组件概述

Identity Manager 可确保从您的物理与虚拟网络到云，每个用户都具有一致的身份。下图显示了支持 Identity Manager 功能的各组件的概要视图。其中的部分组件可安装在同一个服务器上，具体视您身份管理解决方案的大小而定。但是，某些组件 （例如 Identity Applications）提供基于浏览器的界面，供用户从工作站或移动平台访问。



在 Identity Manager 中，**受管系统** （也称为**已连接系统**或**应用程序**）指任何您要管理其身份信息的系统、目录、数据库或操作系统。例如，连接的系统可以是 PeopleSoft 应用程序或 LDAP 目录。由**驱动程序** （例如数据收集服务驱动程序）提供受管系统与身份库之间的连接。它还允许在系统间进行数据同步和共享。 Identity Manager 将驱动程序和库对象储存在称为**驱动程序集**的容器中。

2 创建和维护 Identity Manager 环境

大多数组织都使用单独的环境来开发并逐步完成 Identity Manager，然后将其部署到生产环境。要构建和维护 Identity Manager 环境，您可以使用下列 Identity Manager 组件：

- 第 2.1 节 “Designer for Identity Manager” （第 21 页）
- 第 2.2 节 “Analyzer for Identity Manager” （第 21 页）
- 第 2.3 节 “iManager” （第 22 页）

这些组件还可以帮助您调整 Identity Manager 以满足多变的业务需要，从而确保业务持续运作，并提高整个企业的用户生产力。

2.1 Designer for Identity Manager

Designer for Identity Manager (Designer) 可帮助您在网络或测试环境中设计、测试、记录和部署 Identity Manager 解决方案。您可以在脱机环境中配置 Identity Manager 项目，然后再将其部署到在线系统。从设计角度而言， Designer 可帮助执行下列工作：

- 以图形方式查看构成 Identity Manager 解决方案的所有组件，并观察它们是如何交互的。
- 修改并测试 Identity Manager 环境，确保它的表现符合预期，然后再将部分或整个测试解决方案部署到生产环境。

Designer 会跟踪设计及布局信息。您只需单击按钮，即可用选定的格式打印该信息。 Designer 还允许小组共享针对企业级项目执行的工作。

有关使用 Designer 的详细信息，请参见 *《NetIQ Designer for Identity Manager Administration Guide》*（NetIQ Designer for Identity Manager 管理指南）。

2.2 Analyzer for Identity Manager

Analyzer for Identity Manager (Analyzer) 提供数据分析、清理、调节和报告，以帮助您遵守内部数据质量策略。 Analyzer 允许您分析、增强和控制企业范围内储存的所有数据。 Analyzer 包含下列功能：

- Analyzer 的纲要映射可使应用程序的纲要属性与 Analyzer 基本纲要中的对应纲要属性相关联。这可让您确保您的数据分析和清理操作在不同系统之间正确关联类似的值。为此， Analyzer 利用了 Designer 中的纲要映射功能。
- 分析配置文件编辑器可让您配置用于分析一或多个数据集实例的配置文件。每个分析配置文件包含一或多个度量标准，您可以依据这些度量标准来评估属性值，以确定数据符合您所定义的数据格式标准的程度。
- 匹配配置文件编辑器可让您比较一或多个数据集中的值。您可以检查指定的数据集中是否有重复的值，以及两个数据集之间是否有匹配的值。

有关使用 Analyzer 的详细信息，请参见 *《NetIQ Analyzer for Identity Manager Administration Guide》*（NetIQ Analyzer for Identity Manager 管理指南）。

2.3 iManager

NetIQ iManager 是一款基于浏览器的工具，提供了对众多 Novell 及 NetIQ 产品 （包括 Identity Manager）的单点管理功能。通过安装用于 iManager 的 Identity Manager 插件，您可管理 Identity Manager 并接收有关 Identity Manager 系统的实时运行状态信息。

使用 iManager，您可以执行使用 Designer 可执行的类似任务，还可以监控系统的状态。 NetIQ 建议您使用 iManager 来执行管理任务。请使用 Designer 来执行需要在部署前进行包更改、建模和测试的配置任务。

有关 iManager 的详细信息，请参见 *《NetIQ iManager Administration Guide》*（NetIQ iManager 管理指南）。

3 在 Identity Manager 环境中管理数据

Identity Manager 在物理、虚拟和云网络之间实施一致的访问控制，并使用可让您证明合规性的动态报告。实际上， Identity Manager 可同步储存在已连接应用程序或身份库中的任何类型的数据。Identity Manager 解决方案的下列组件可提供数据同步，包括口令同步：

- 身份库
- Identity Manager 引擎
- Identity Manager Remote Loader
- Identity Reporting
- Identity Manager 驱动程序
- 已连接系统

3.1 了解数据同步

Identity Manager 允许您在多种连接的系统 （例如 SAP、 PeopleSoft、 Microsoft SharePoint、 Lotus Notes、 Microsoft Exchange、 Microsoft Active Directory、 NetIQ eDirectory 与 LDAP 目录）之间同步、转换和分布信息。 Identity Manager 可让您执行下列活动：

- 控制已连接系统之间的数据流。
- 确定要共享的数据、数据块的权威来源系统以及对数据进行解释和转换以满足其他系统要求的方法。
- 在各系统之间同步口令。例如，如果用户更改了在 Active Directory 中的口令， Identity Manager 可将该口令同步到 Lotus Notes 和 Linux。
- 在各目录 （例如 Active Directory）以及系统 （例如 PeopleSoft 和 Lotus Notes）中创建新用户帐户及去除现有账户。例如，在您将新员工添加到 SAP HR 系统时， Identity Manager 可在 Active Directory 中自动创建新用户帐户，并在 Lotus Notes 中自动创建新帐户。

3.2 了解审计、报告和合规性

如果没有 Identity Manager，供应用户可能是件单调乏味且耗时费财的事情。然后，您必须校验供应活动是否符合贵组织的策略、要求和规定。是否正确的人对正确的资源有访问权？您是否确定未经授权的人员无法访问这些资源？昨天开始上班的员工是否具有对网络、电子邮件以及工作所需的其他系统的访问权？是否取消了上周离职员工的访问权？

有了 Identity Manager 您会感到很轻松，因为无论是过去的还是现在的所有用户供应活动都会针对审计目的进行跟踪和记录。通过查询身份信息仓库，可检索确保贵组织完全符合相关业务法律和规定的所有所需信息。

Identity Manager 包含预定义报告，使您能够针对身份信息仓库执行查询以证明符合业务、 IT 和公司策略。如果预定义报告不能满足您的需求，您还可以创建自定义报告。

3.3 了解用于同步身份数据的组件

3.3.1 身份库

身份库包含 Identity Manager 需要的所有信息。身份库充当要在各个已连接系统之间同步的数据的元目录。例如，从 PeopleSoft 系统同步到 Lotus Notes 的数据将首先添加到身份库，然后再发送给 Lotus Notes 系统。身份库还会储存特定于 Identity Manager 的信息，例如驱动程序配置、参数和策略。

身份库使用 NetIQ eDirectory 数据库。有关使用 eDirectory 的详细信息，请参见 《NetIQ eDirectory 9.1 Administration Guide》（NetIQ eDirectory 8.8 管理指南）。

3.3.2 Identity Manager 引擎

Identity Manager 引擎用于处理身份库或已连接应用程序中发生的所有数据更改。对于身份库中发生的事件，引擎将处理更改并通过驱动程序向应用程序发出命令。对于应用程序中发生的事件，引擎将接收驱动程序中的更改、处理更改然后向身份库发出命令。**驱动程序**会将 Identity Manager 引擎连接到多个应用程序。驱动程序有两个基本责任：将应用程序中的数据更改 （事件）报告给 Identity Manager 引擎，以及执行由 Identity Manager 引擎提交给应用程序的数据更改 （命令）。驱动程序必须安装在已连接应用程序所在的服务器上。

Identity Manager 引擎也称为元目录引擎。用来运行 Identity Manager 引擎的服务器称为 **Identity Manager 服务器**。您的环境中可以有多个 Identity Manager 服务器，具体视服务器工作负载而定。

3.3.3 Remote Loader

Identity Manager Remote Loader 可装载驱动程序，并代表远程服务器上安装的驱动程序来与 Identity Manager 引擎通讯。如果应用程序与 Identity Manager 引擎在同一个服务器上运行，您便可以将驱动程序安装在该服务器上。但是，如果应用程序与 Identity Manager 引擎不在同一个服务器上运行，您必须将驱动程序安装在应用程序所在的服务器上。要改善环境的工作负载或配置，您可以将 Remote Loader 安装在单独的服务器上，不要将其与 Tomcat 和 Identity Manager 服务器安装在同一个服务器上。

有关 Remote Loader 的详细信息，请参见第 10.1.2 节 “ 了解 Remote Loader” （第 86 页）。

3.3.4 Identity Reporting

Identity Manager 中包含**身份信息仓库**，后者是用于储存组织中身份库与已连接系统的实际和预期状态相关信息的智能储存库。身份信息仓库使您能够全面了解业务权利，提供了解授予组织中用户身份的授权和许可权限的过去和当前状态的所需信息。

查询身份信息仓库时，您可以检索确保贵组织完全符合相关业务法律和规定的所有所需信息。掌握这些信息后，您甚至可以回答最复杂的管理风险和合规性 (GRC) 问题。

身份信息仓库的基础结构需要使用下列组件：

- Identity Manager 的 Identity Reporting （第 25 页）
- 数据收集服务 （第 25 页）
- 受管系统网关驱动程序 （第 25 页）

Identity Manager 的 Identity Reporting

身份信息仓库将其信息储存在 Sentinel Log Management for IGA 的 SIEM 数据库中。 **Identity Reporting** 组件可让您审计和创建有关 Identity Manager 解决方案的报告。您可以使用这些报告来帮助满足企业的合规性法规。您可以运行预定义的报告，以证明对业务、 IT 及企业策略的合规性状况。如果预定义报告不能满足您的需求，您还可以创建自定义报告。使用 Identity Reporting 可报告有关 Identity Manager 配置各方面的重要业务信息，包括从身份库和已连接系统收集而来的信息。 Identity Reporting 的用户界面便于您将报告安排在非高峰时间运行，从而实现性能优化。有关 Identity Reporting 的详细信息，请参见 《Administrator Guide to NetIQ Identity Reporting》（NetIQ Identity Reporting 管理员指南）。

数据收集服务

数据收集服务使用数据收集服务驱动程序来捕获对储存在身份库中的对象 （例如帐户、角色、资源、组和小组成员资格）所做的更改。驱动程序向该服务进行注册，并将更改事件 （例如数据同步、添加、修改和删除事件）推送到该服务。

该服务包括三个子服务：

- **报告数据收集器：**使用拉式设计模型从一个或多个身份库数据源中检索数据。它根据一组配置参数确定的周期定期运行收集。为了检索数据，收集器需调用受管系统网关驱动程序。
- **事件驱动的数据收集器：**使用推式设计模型收集由数据收集服务驱动程序捕获的事件数据。
- **非受管应用程序数据收集器：**通过调用专门为每个应用程序编写的 REST 端点，从一个或多个非受管应用程序中检索数据。非受管应用程序是指您企业中未连接到身份库的应用程序。

受管系统网关驱动程序

受管系统网关驱动程序会查询身份库，以便从受管系统中收集下列类型的信息：

- 所有受管系统列表
- 所有受管系统帐户列表
- 受管系统的权利类型、值和指派以及用户帐户配置文件

4 供应用户以进行安全的访问

Identity Manager 会集中管理访问权，并确保从您的物理与虚拟网络到云，每个用户都具有一致的身份。此外，用户通常根据其在组织中的角色来请求对资源的访问权。例如，某个法律公司的律师和该公司的律师助理可能需要访问不同的资源组。

Identity Manager 允许您根据其在组织中的角色来供应用户。您可根据组织需求定义角色并进行指派。将用户指派给角色后， Identity Manager 可向该用户供应与该角色关联的资源的访问权。具有多个角色的用户会得到与所有角色所关联的资源的访问权。

您可以让用户因组织中发生的事件而自动添加到某些角色。例如，您可以将职称为 " 律师 " 的新用户添加到 SAP HR 数据库。如果要求批准才能将某个用户添加到角色，您可以建立工作流程以将角色请求路由到相应批准者。也可手动将用户指派给角色。

在某些情况下，某些角色可能由于冲突而不应指派给同一个人。 Identity Manager 提供了 " 责任分离 " 功能，使用该功能可避免将用户指派给冲突角色，除非组织中有人将该冲突作为例外。

Identity Manager 解决方案提供了下列组件用来供应用户：

- Identity Manager 仪表板
- Identity Applications 管理
- User Application

仪表板为所有 Identity Manager 用户和管理员提供了单一访问点。在仪表板中可以访问所有现有的 User Application 功能。从 Identity Manager 4.7 版开始，仪表板取代了 Identity Manager 主页和供应仪表板。

4.1 了解 Identity Manager 中的证明过程

Identity Manager 可通过证明流程帮助您验证角色指派的正确性。错误的角色指派可能会危及与公司和政府规定的一致性。使用证明过程，贵组织中的负责人可认证与角色关联的数据：

- **用户简介证明：**所选用户证明其自身的简介信息 （姓、名、职位、部门、电子邮件等等）并纠正所有错误信息。准确的简介信息对于正确的角色指派非常重要。
- **责任分离违反证明：**负责人审阅 " 责任分离 " 违反报告并证明报告的准确性。该报告列出了允许将用户指派给冲突角色的所有例外。
- **角色指派证明：**负责人审阅列出了所选角色和指派给每个角色的用户、组以及角色的报告。然后负责人必须证明该信息的准确性。
- **用户指派证明：**负责人审阅列出了所选用户以及将其指派给的角色的报告。然后负责人必须证明该信息的准确性。

这些证明报告主要是为了帮助您确保角色指派准确，并确保存在允许冲突角色例外的有效原因。

4.2 了解 Identity Manager 中的自助服务过程

Identity Manager 以身份为基础来为用户授予对各系统、应用程序和数据库的访问权。每个用户的唯一标识符及角色定义了对身份数据的特定访问权限。例如，身份为主管的用户可以访问其下属的薪资信息，但不能访问组织中其他员工的薪资信息。使用 Identity Manager，您可将管理责任委托给应对上述人员负责的人。例如，您可让个别用户具有实现下列目标的能力：

- 在公司目录中管理各自的个人数据。他们可以先在某个位置更改手机号码，然后在您已通过 Identity Manager 同步的所有系统中更改该数据，从而不必由您来执行此类更改。
- 更改口令、设置忘记口令的提示以及设置忘记口令的提示问题和答案。在他们忘记口令的情况下，不必让您来重设置口令，他们可在收到提示或回答询问问题后自行进行该操作。
- 请求对诸如数据库、系统和目录等资源的访问权。不必致电给您来请求对某个应用程序的访问权，他们可从可用资源列表中选择该应用程序。

除了个人用户的自助服务， Identity Manager 还为负责辅助、监视和批准用户请求的各种职能 （管理层、咨询台等等）提供了自助管理。例如， John 使用 Identity Manager 自助服务功能来请求访问他需要的文档。 John 的经理和 CFO 通过自助服务功能收到了请求，并且可以批准该请求。已建立的批准工作流程使 John 可以启动并监视其请求的进度，并使 John 的经理和 CFO 可以响应其请求。John 的经理和 CFO 对请求的批准触发了 John 访问和查看财务单据所需的 Active Directory 权限的供应。

Identity Manager 还提供工作流程功能以确保供应过程包括了相应的资源批准者。例如，假设 John （已获得 Active Directory 帐户）需要通过 Active Directory 访问一些财务报告。这需要 John 的直属经理和 CFO 的批准。幸运的是，您已建立一个批准工作流程，可将 John 的请求路由到他的经理，待经理批准后，再将请求路由到 CFO。 CFO 的批准将触发 John 访问和查看财务单据所需的 Active Directory 权限的自动供应。

您可以让工作流程在某个特定事件发生时 （例如，向 HR 系统中添加新用户）自动启动，也可通过用户请求手动启动。要确保批准能够及时发生，可设置代理批准者和批准小组。

4.3 了解管理用户供应的组件

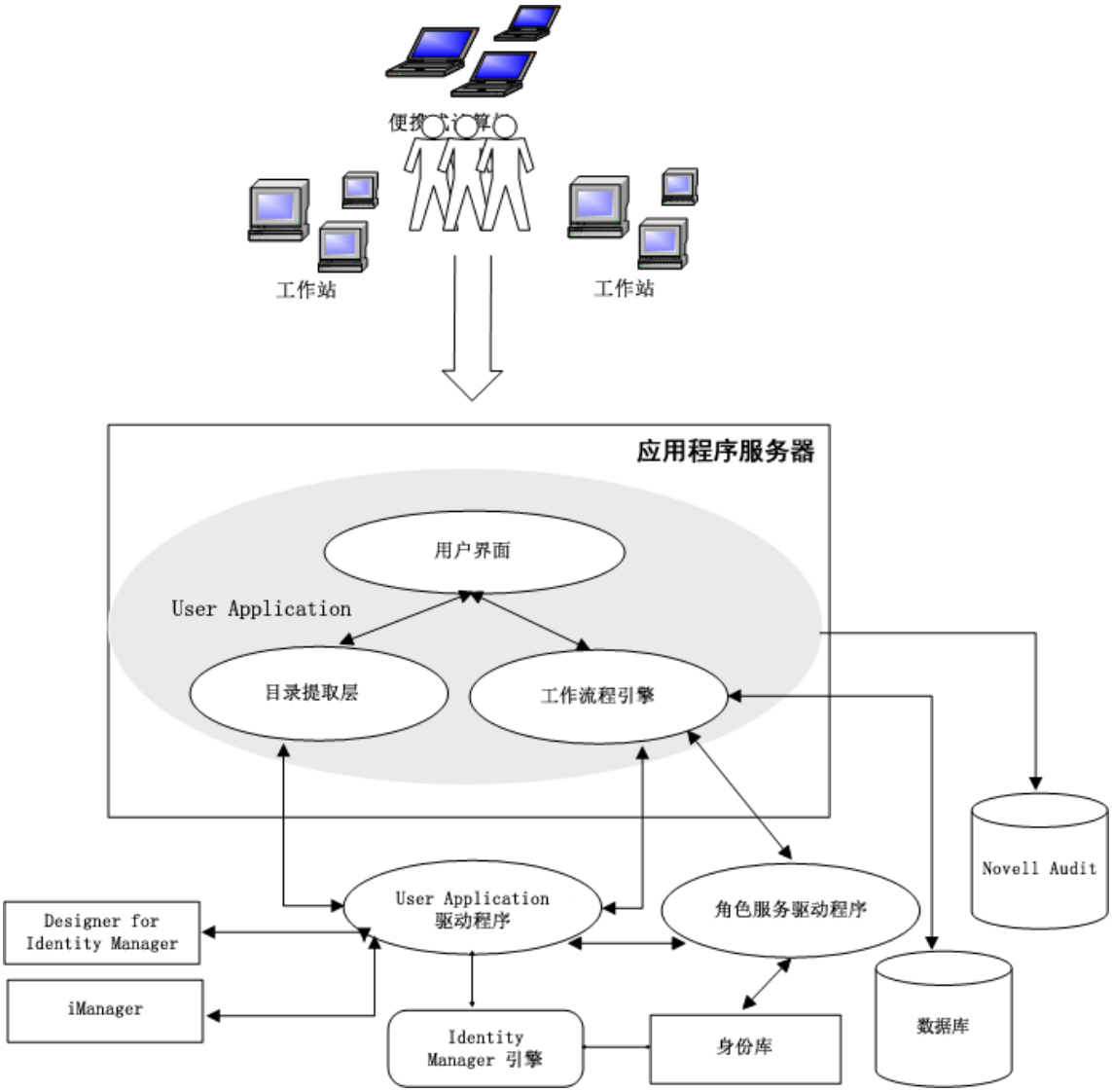
本节说明下列组件的用途：

- 第 4.3.1 节 “User Application 和 Roles Based Provisioning Module” （第 29 页）
- 第 4.3.2 节 “Identity Applications 管理 ” （第 30 页）
- 第 4.3.3 节 “Identity Manager 仪表板 ” （第 30 页）

4.3.1 User Application 和 Roles Based Provisioning Module

Identity Manager **User Application** 可让您的用户和业务管理员了解 Identity Manager 的信息、资源和功能。 User Application 是基于浏览器的 Web 应用程序，可让用户执行各种身份自助服务和角色供应任务。用户可以管理口令与身份数据、启动和监控供应与角色指派请求、管理供应请求的批准过程，以及校验证明报告。

User Application 依赖于许多共同运作的独立组件。



User Application 在 **Roles Based Provisioning Module** (RBPM) 框架上运行，该框架包括一个工作流程引擎，用于通过相应的批准过程控制请求的路由。这些组件需要下列驱动程序：

用户应用程序驱动程序

储存配置信息，并在身份库中发生更改时立即通知 User Application。您可以配置驱动程序，以允许身份库中的事件触发工作流程。该驱动程序还可以向 User Application 报告工作流程的供应活动是成功还是失败，以便用户可以查看其请求的最终状态。

Role and Resource Service 驱动程序

管理所有角色和资源指派。驱动程序可启动角色和资源指派请求 （要求批准）的工作流程，以及根据组和容器成员资格维护间接角色指派。该驱动程序还可根据用户的角色成员资格为其授予和撤消权利。它会对已完成的请求执行清理过程。

用户可以从任何支持的 Web 浏览器访问 User Application。有关 User Application 和 RBPM 的详细信息，请参见 《*NetIQ Identity Manager - Administrator's Guide to the Identity Applications*》（NetIQ Identity Manager - Identity Applications 管理员指南）。

4.3.2 Identity Applications 管理

在 **Identity Applications 管理**界面中可以使用相应的管理员角色管理以下任务：

- 创建和管理角色、资源及其指派
- 设置责任分离 (SoD) 限制，以免系统中的两个不同角色之间发生冲突
- 配置允许用户通过电子邮件批准许可权限请求的功能
- 配置 Identity Applications 组成部分 （例如角色、资源和委托）的默认设置。

管理员可以在计算机或平板电脑上使用任何支持的 Web 浏览器访问 " 管理 " 页面。有关详细信息，请参见 《*NetIQ Identity Manager - Administrator's Guide to the Identity Applications*》（NetIQ Identity Manager - Identity Applications 管理员指南）。

4.3.3 Identity Manager 仪表板

Identity Manager 仪表板 （简称 " 仪表板 "）是每个用户的许可权限、任务和请求的个性化视图。它有助于让用户着重关注以下几个基本方面的功能：

我需要某些项目。

如果您需要某个项目，无论该项目是便携式计算机之类的一件设备，还是对特定服务器或应用程序的访问权之类的无形项目，您都可以请求该项目。

我需要执行某个动作。

如果想要知道自己需要管理的任务，可以使用**我的任务**页面显示 Identity Manager 系统中您的所有待审批或供应任务。

我拥有哪些项目？

如果想要查看您当前的许可权限，可以使用**我的许可权限**页面显示您有权访问的角色和资源的列表。

我是如何获取的？

如果想要查看过往请求的列表，可以使用**请求历史记录**页面显示您最近请求的一切项目，以及您的待处理请求的状态。

如果您具有 Identity Applications 的管理角色，则可以在仪表板中针对所有用户自定义**应用程序**页面。您可以对页面进行配置，以显示您的用户需要看到的项目和链接，并将其组织成适合您企业的类别。您可以包括以下几种类型的项目：

- Identity Manager 功能，例如创建组或运行报告
- 大部分用户需要请求的许可权限
- 指向经常访问的网站或基于 Web 的应用程序的链接

- REST 端点
- 标记，例如用户可以访问的特定类型的项目数

用户可以从计算机或平板电脑上使用任何支持的 Web 浏览器访问仪表板。有关详细信息，请参见《*NetIQ Identity Manager - Administrator's Guide to the Identity Applications*》（NetIQ Identity Manager - Identity Applications 管理员指南）。

4.4 使用 Identity Manager 中的自助式口令管理

Identity Manager 提供 NetIQ Self Service Password Reset (SSPR) 来帮助可访问 Identity Applications 的用户重设置其口令，而无需管理用户的干预。当您安装或升级到 Identity Manager 的最新版本时，安装进程默认会启用 SSPR。在全新安装中， SSPR 将使用专有协议来管理鉴定方法。不过，在升级之后，您可以指示 SSPR 使用 NetIQ Modular Authentication Services (NMAS)，Identity Manager 一贯将 NMAS 用于其旧式口令管理程序。

根据您是否要使用复杂的口令管理，您可以配置下列其中一个提供程序：

SSPR

NetIQ Self Service Password Reset 是您安装或升级 Identity Manager 时的默认选项。有关详细信息，请参见第 4.4.1 节 " 了解默认自助服务过程 " （第 31 页）。

旧式口令管理提供程序

使用 Identity Manager 4.0.2 中的口令管理过程，它支持使用多个口令策略。有关详细信息，请参见第 4.4.2 节 " 了解旧式口令管理提供程序 " （第 32 页）。

第三方口令管理提供程序

您可以使用第三方程序来管理忘记的口令。您需要修改 Identity Manager 的某些配置设置。有关详细信息，请参见使用外部系统进行忘记口令管理 （第 202 页）。

4.4.1 了解默认自助服务过程

SSPR 自动与 Identity Applications 和 Identity Reporting 的单点登录过程集成。它是 Identity Manager 的默认口令管理程序，即使您未安装 SSPR 也是如此。当用户请求重设置口令时， SSPR 要求用户回答询问应答问题。如果答案正确， SSPR 会以下列其中一种方式响应：

- 允许用户创建新口令
- 创建新口令并将它发送给用户
- 创建新口令并将它发送给用户，同时将旧口令标记为已失效。

您可在 SSPR 配置编辑器中配置此响应。升级到 Identity Manager 的新版本之后，您可以将 SSPR 配置为使用 Identity Manager 一贯用来进行口令管理的 NMAS 方法。不过， SSPR 不能识别您用于管理忘记的口令的现有口令策略。要继续使用您的策略，请参见第 4.4.2 节 " 了解旧式口令管理提供程序 " （第 32 页）。

您也可以将 SSPR 配置为使用其专用协议而不是 NMAS。进行此更改后，要恢复为使用 NMAS，将只能通过重设置口令策略来实现。

有关下列项的详细信息 ...	参见 ...
安装 SSPR	第 14.2 章 " 为 Identity Manager 安装口令管理 "（第 157 页）
配置 Identity Applications 的口令管理	使用 Self Service Password Reset 进行忘记口令管理（第 199 页）
管理和配置 SSPR	*《NetIQ Self Service Password Reset Administration Guide》*（NetIQ Self Service Password Reset 管理指南）

4.4.2 了解旧式口令管理提供程序

注释：此版本弃用了 User Application 的旧式口令自助服务功能。 NetIQ 强烈建议您开始使用 SSPR 来执行所有口令特定的任务。安装进程默认会启用 SSPR。有关详细信息，请参见第 4.2 节 " 了解 Identity Manager 中的自助服务过程 "（第 28 页）。

如果您从 Identity Manager 的较旧版本升级， Identity Applications 默认使用 SSPR 做为口令管理程序。SSPR 可以使用 Identity Manager 一惯用来进行口令管理的 NMAS 方法。不过， SSPR 不能识别您用于管理忘记的口令的现有口令策略。您可以绕过 SSPR，使用旧式口令管理提供程序。

当用户请求重设置口令时，旧式提供程序会将用户的身份凭证与您设置的口令策略进行比较。例如，它可能要求用户回答询问应答问题。根据应用于该用户的策略，程序会以下列其中一种方式响应：

- 重设置口令
- 显示口令提示
- 通过电子邮件将口令提示发送给用户
- 通过电子邮件将新口令发送给用户

如果贵企业使用多个或复杂的口令策略，请使用旧式提供程序。例如，您的口令策略基于用户角色运作。实习员工可能只需要自动生成的口令，而不需要提供询问应答；而对于可以访问安全数据的经理，您可能有更严格的要求。此用户可能需要定期重设置口令。对于这两个案例，您希望用户自助完成口令请求。

要使用旧式提供程序，请在安装或升级 Identity Manager 之后修改 Identity Applications 的配置设置。升级之后，您将不需要重新配置口令策略。

有关下列项的详细信息 ...	参见 ...
配置 Identity Manager 以使用旧式提供程序	使用旧版提供程序进行忘记口令管理 （第 201 页）
使用旧式提供程序进行口令管理	*《NetIQ Identity Manager Password Management Guide》*（NetIQ Identity Manager 口令管理指南）

4.5 在 Identity Manager 中使用单点登录访问

为了提供单点登录访问 (SSO)， Identity Manager 使用了鉴定服务 NetIQ One SSO Provider (OSP)。您必须对下列组件使用 OSP：

- Identity Applications 管理
- Identity Manager 仪表板
- Identity Reporting
- Self-Service Password Reset
- User Application

Identity Manager 安装程序的 .iso 映像提供安装 OSP 的途径。有关安装 OSP 的详细信息，请参见第 14.2 章 " 为 Identity Manager 安装口令管理 "（第 157 页）。

4.5.1 了解使用 One SSO Provider 进行鉴定的方法

OSP 支持 OAuth2 规范，并需要使用 LDAP 鉴定服务器。默认情况下， Identity Manager 使用身份库 (eDirectory)。 OSP 可以与其他类型的**鉴定源**或**身份库**通讯，以处理鉴定请求。您可以配置希望 OSP 使用的鉴定类型：userID 和口令、 Kerberos 或 SAML。不过， OSP 不支持 MIT 样式的 Kerberos 或 SAP 登录票据。

OSP 和 SSO 如何运作？

如果您使用身份库作为鉴定服务，并且身份库中的指定容器具有 CN 和口令，则授权用户在 Identity Manager 安装好后便可立即登录其中。如果没有这些登录帐户，则只有安装期间指定的管理员可以立即登录。

当用户登录其中一个基于浏览器的组件时，此过程会将用户的名称 / 口令对重定向到 OSP 服务，该服务随即会查询鉴定服务器。服务器会验证用户身份凭证。随后， OSP 将 OAuth2 访问令牌发给该组件和浏览器。浏览器会在用户的会话期间使用该令牌来提供对任何基于浏览器的组件的 SSO 访问权。

如果您使用 Kerberos 或 SAML， OSP 会接受来自 Kerberos 票据服务器或 SAML IDP 的鉴定，然后将 OAuth2 访问令牌发给用户所登录的组件。

OSP 如何与 Kerberos 配合工作？

OSP 和 Kerberos 可确保用户能够登录系统一次，以便使用其中一个 Identity Applications 及 Identity Reporting 创建会话。如果用户的会话超时，授权会自动进行，而无需用户的干预。注销之后，用户应始终关闭浏览器以确保其会话结束。否则，应用程序会将用户重定向到登录窗口，并且 OSP 会重新对该用户会话进行授权。

如何设置鉴定和单点登录访问？

要让 OSP 与 SSO 正常运作，您必须安装 OSP。然后指定客户端用于访问每个组件的 URL、将验证请求重定向到 OSP 的 URL，以及鉴定服务器的设置。您可以在安装期间或安装之后使用 RBPM 配置实用程序来提供此信息。您还可以指定 Kerberos 票据服务器或 SAML IDP 的设置。

有关配置鉴定和单点登录访问的详细信息，请参见第 VIII 部分 " 在 Identity Manager 中配置单点登录访问 "（第 277 页）。

在群集中，所有群集成员的配置设置都必须相同。

4.5.2 了解 One SSO Provider 的密钥存储区

Identity Manager 使用支持在 OSP 服务与鉴定服务器之间进行 http 和 https 通讯的密钥存储区。密钥存储区是在您安装 OSP 时创建的。您也可以创建一个口令，供 OSP 服务用于与鉴定服务器进行授权交互。有关详细信息，请参见第 14.2 章 " 为 Identity Manager 安装口令管理 "（第 157 页）。

4.5.3 了解 One SSO Provider 的审计事件

OSP 会生成单个事件，来说明用户何时登录或注销 User Application 或 Identity Reporting：

- 003E0204 （登录）
- 003E0201 （注销）

然后，XDAS 分类法会将这些 OSP 事件解释为登录 / 注销或 SOAP 调用 User Application 成功，或者是 " 不成功 "。

规划安装 Identity Manager

本部分提供了有关规划 Identity Manager 环境的重要信息。要查看安装每个 Identity Manager 组件的计算机所要满足的先决条件和系统要求，请参见相关组件的安装章节。

您无需提供激活代码就能安装或初始运行 Identity Manager。但是，如果未提供激活代码， Identity Manager 将在安装完成 90 天后停止运行。在这 90 天内或者 90 天后，您随时可以激活 Identity Manager。

5 规划概述

本章将帮助您规划 Identity Manager 的安装过程。因为安装过程需要访问先前安装的组件，所以某些组件必须按特定的顺序安装。例如，应该先安装并配置身份库，然后再安装 Identity Manager 引擎。

5.1 规划核对清单

以下核对清单提供了在您的环境中规划 Identity Manager 安装的概要步骤。安装各 Identity Manager 组件的相关章节提供了更具体的核对清单。

	核对清单项目
❑	1. 查看产品体系结构信息，以了解 Identity Manager 组件。有关更多信息，请参见第 I 部分 " 简介 "（第 17 页）。
❑	2. 确定想要使用的安装程序类型。有关更多信息，请参见第 5.2 节 " 了解安装过程 "（第 38 页）。
❑	3. 确定最适合您的安装的操作系统平台。有关更多信息，请参见第 5.3.5 节 " 选择 Identity Manager 的操作系统平台 "（第 41 页）。 **注释：**Identity Manager 仅支持在 Linux 服务器上安装 Sentinel Log Management for Identity Governance and Administration (Sentinel Log Management for IGA)。如果要在您的环境中使用 Sentinel Log Management for IGA，请参见《*NetIQ Identity Manager 安装指南 - Linux*》中的 " 安装 Sentinel Log Management for Identity Governance and Administration"，了解此安装所需的先决条件和系统设置。但是，如果您的身份解决方案仅适用于 Windows，则可以使用其他审计服务。
❑	4. 确定组件的安装顺序以及要安装每个组件的具体位置。有关更多信息，请参见第 5.3 节 " 建议的安装方案和服务器设置 "（第 39 页）。
❑	5. 确保已获取运行 Identity Manager 的许可证。有关更多信息，请参见第 5.4 节 " 了解许可和激活 "（第 42 页）。
❑	6. 查看每个 Identity Manager 组件的默认端口，以确定是否需要自定义安装设置。有关更多信息，请参见第 6.1 节 " 了解 Identity Manager 通讯 "（第 45 页）。
❑	7. 确定是否可使用您的首选语言运行安装程序。有关更多信息，请参见第 6.2 节 " 了解语言支持 "（第 46 页）。

	核对清单项目
❑	8. 确保已获取 Identity Manager 的安装文件。有关更多信息，请参见第 5.5 节 " 下载安装文件 " （第 43 页）。 **重要：**为了顺利安装，请勿在安装 Identity Manager 组件时运行任何大量占用 CPU 资源的应用程序。您必须在开始 Identity Manager 安装前停止 Windows 模块安装程序和 Windows 更新等 Windows 服务，并且仅当完成安装后方可启动这些服务。
❑	9. （视情况而定）要在群集中安装 Identity Manager，请确保您的环境符合要求。有关更多信息，请参见第 6.3 节 " 确保 Identity Manager 的高可用性 " （第 47 页）。
❑	10. 确保已获取在服务器上安装 Identity Manager 组件所需的适当身份凭证，以及可能在安装期间创建的帐户。
❑	11. 确保要安装 Identity Manager 组件的目标计算机符合指定的要求。有关详细信息，请参见以下各节： ◆ **Designer**：规划安装 Designer （第 265 页） ◆ **适用于角色和资源管理的 Identity Applications**：规划安装 Identity Applications （第 165 页） ◆ **Identity Manager 引擎**：规划引擎、驱动程序和插件的安装 （第 73 页） ◆ **身份库**：安装身份库 （第 51 页） ◆ **iManager**：（可选）规划安装 iManager （第 125 页） ◆ **Password Reset (SSPR)**：为 Identity Manager 规划安装口令管理 （第 155 页） ◆ **PostgreSQL**：规划安装 PostgreSQL 和 Tomcat （第 141 页） ◆ **Remote Loader**：规划引擎、驱动程序和插件的安装 （第 73 页） ◆ **报告** : 规划安装 Identity Reporting （第 225 页） ◆ **单点登录访问 (OSP)**：为 Identity Manager 规划安装口令管理 （第 155 页） ◆ **Tomcat**：规划安装 PostgreSQL 和 Tomcat （第 141 页） **注释：**NetIQ 建议您记下安装期间所创建的每个帐户。
❑	12. 激活 Identity Manager 组件。有关更多信息，请参见第 30.6 节 " 激活 Identity Manager" （第 310 页）。

5.2 了解安装过程

NetIQ 提供了 Identity Manager 组件的独立安装程序，让您可以更灵活地设置环境。例如，许多 Identity Manager 组件都是数据密集型组件 （如身份库），应安装在独立的服务器上。

独立安装过程具有以下特点：

- 允许您自定义组件设置，包括身份库中的树型结构
- 允许您在分布式和群集环境中安装
- 允许您选择驱动程序，并创建想要添加到身份管理解决方案中的驱动程序集
- 允许您选择想要添加到身份管理解决方案中的 iManager 插件
- 允许您使用非管理员帐户安装某些组件
- 支持多个数据库平台

- 针对所有支持的操作系统使用 Apache Tomcat
- 创建支持的生产环境
- 可用于升级 Identity Manager 的先前版本

为获得最佳效果，请按身份管理解决方案所指定的顺序运行独立安装程序。有关更多信息，请参见第 5.3 节 " 建议的安装方案和服务器设置 "（第 39 页）。

5.3 建议的安装方案和服务器设置

执行独立安装时，应按特定的顺序在特定的服务器上安装组件。某些组件的安装程序需要使用先前安装的组件的相关信息。

本节将帮助您根据特定的审计和报告方案，确定安装顺序和服务器类型。

5.3.1 将事件发送到审计服务而不在 Identity Manager 中报告

在此方案中，您计划使用 Sentinel 来审计 Identity Manager 中发生的事件，但不打算在 Identity Manager 中生成报告。按以下顺序安装组件：

1. Sentinel Log Management for IGA （在 Windows 上不受支持）

   注释：NetIQ 仅支持在 Linux 服务器上安装此组件。有关安装指导，请参见 《*NetIQ Identity Manager Setup Guide for Linux*》（NetIQ Identity Manager 安装指南 - Linux）。但是，如果您的身份解决方案仅适用于 Windows，则可以使用其他审计服务。

2. 身份库
3. Identity Manager 引擎、驱动程序和 iManager 插件
4. （可选） iManager
5. Designer
6. Tomcat 和 PostgreSQL
7. OSP
8. SSPR
9. Identity Applications
10. （可选） Analyzer

5.3.2 将事件发送到 Identity Manager 并生成报告

在此方案中，您计划使用 Identity Manager 随附的 Sentinel Log Management for IGA 来审计 Identity Manager。您可能还想为这些事件生成报告。按以下顺序安装组件：

1. 身份库
2. Sentinel Log Management for IGA （在 Windows 上不受支持）

   注释：NetIQ 仅支持在 Linux 服务器上安装此组件。有关安装指导，请参见 《*NetIQ Identity Manager Setup Guide for Linux*》（NetIQ Identity Manager 安装指南 - Linux）。但是，如果您的身份解决方案仅适用于 Windows，则可以使用其他审计服务。

3. Identity Manager 引擎、驱动程序和 iManager 插件
4. （可选） iManager
5. Designer
6. Tomcat 和 PostgreSQL
7. OSP
8. SSPR
9. Identity Applications
10. Identity Reporting
11. （可选） Analyzer

5.3.3 将事件推送到 Identity Manager 之前先将事件发送到外部服务

在此方案中，您计划使用某个服务 （例如 Sentinel）来审计 Identity Manager。按以下顺序安装组件：

1. 外部审计服务，例如 Sentinel
2. 身份库
3. Identity Manager 引擎、驱动程序和 iManager 插件
4. （可选） iManager
5. Designer
6. Tomcat 和 PostgreSQL
7. OSP
8. SSPR
9. Identity Applications
10. Identity Reporting
11. （可选） Analyzer

5.3.4 建议的服务器设置

在典型的生产环境中，您可以将 Identity Manager 安装在七个或更多台服务器上以及客户端工作站上。例如：

计算机设置	组件设置
服务器 1 和 2 （双服务器目录复本）	◆ 身份库 ◆ Identity Manager 引擎
服务器 3 和 4 （双服务器群集）	◆ Identity Applications ◆ iManager ◆ One SSO Provider ◆ Remote Loader ◆ Self Service Password Reset **注释：**NetIQ 建议您将 Identity Applications 和 One SSO Provider 安装在同一台服务器上。
服务器 5 （或服务器群集）	Identity Manager 数据库： ◆ Identity Applications ◆ Identity Reporting
服务器 6	Identity Reporting
服务器 7	Sentinel Log Management for IGA
客户端工作站 （1 个以上）	◆ Designer ◆ iManager Workstation ◆ 访问 Identity Applications 和 Identity Reporting 的因特网浏览器

5.3.5 选择 Identity Manager 的操作系统平台

您可以在各种操作系统平台上安装 Identity Manager 组件。下表将帮助您确定要将哪些服务器用于身份管理解决方案。

平台	组件
Windows 台式机	Designer iManager Workstation(客户端) 访问 Identity Applications 和 Identity Reporting 的浏览器

平台	组件
Windows Server	Analyzer
	Designer
	Identity Applications
	Identity Manager 引擎
	Identity Reporting
	身份库
	iManager （服务器）
	.NET Remote Loader
	One SSO Provider
	PostgreSQL
	Remote Loader
	Self Service Password Reset
	Tomcat

有关系统要求与先决条件的详细信息，请参见以下各章节：

- 规划安装 Designer （第 265 页）
- 规划安装 iManager （第 125 页）
- 安装身份库 （第 51 页）
- 规划引擎、驱动程序和插件的安装 （第 73 页）
- 规划安装 Identity Applications （第 165 页）
- 为 Identity Manager 规划安装口令管理 （第 155 页）
- 规划安装 PostgreSQL 和 Tomcat （第 141 页）

5.4 了解许可和激活

Identity Manager 包含各种各样的功能。为了满足不同客户的需求， Identity Manager 功能以 Advanced Edition 和 Standard Edition 两种版本提供。 Identity Manager 的 Advanced Edition 包括全套功能。 Standard Edition 只提供 Advanced Edition 的一部分功能。有关 Advanced Edition 和 Standard Edition 中可用功能的比较，请参见 “Identity Manager Version Comparison” （Identity Manager 版本比较）。 NetIQ 为每个版本提供了不同的许可模式。

NetIQ 在一个 ISO 文件中提供 Advanced 和 Standard 两个版本，从而改进其递送新功能、增补程序、文档和支持的服务，同时可让客户选择最适合其需求的解决方案功能。

您可以安装 Identity Manager 的评估版，并免费使用 90 天。但是，必须在安装后的 90 天内激活 Identity Manager 组件，否则它们到期后会停止运行。您可以在 90 天评估期内或者评估期过后，购买产品许可证并激活 Identity Manager。有关详细信息，请参见第 30.6 节 “ 激活 Identity Manager” （第 310 页）。

根据您购买的版本， NetIQ 将为您提供相应的许可证密钥，以在 Identity Manager 中启用合适的功能。要购买 Identity Manager 产品许可证，请参见 NetIQ Identity Manager How to Buy （NetIQ Identity Manager 如何购买）网站。您购买产品许可证后， NetIQ 将会向您发送一个客户 ID。相应的电子邮件中还包含 NetIQ 网站的 URL，您可以通过该网站获取产品激活身份凭证。如果您忘记了自己的客户 ID 或者未收到该 ID，请与销售代表联系。

5.5 下载安装文件

NetIQ 提供有 ISO 文件，其中包含了构成 Identity Manager 完整安装的全部组件。每个文件都包含各种产品版本。 ISO 文件的名称指定了平台。例如 Identity_Manager_*版本*_Windows.iso。

注释：ISO 映像文件很大。请确保将其下载到能容纳该文件大小的卷或 DVD 中。

要下载 Identity Manager 安装文件，请执行以下操作：

1 转到 NetIQ 下载网站。
2 在**产品或技术**菜单中，选择 **Identity Manager**，然后单击**搜索**。
3 在 NetIQ Identity Manager 下载页上，单击要下载的 ISO 文件旁边的**下载**按钮。
4 遵循屏幕提示，将文件下载到计算机上的某个目录中。
5 将下载的 .iso 文件作为卷装入，或者使用 .iso 文件创建软件的 DVD。

5.6 查找可执行文件和默认安装路径

下表提供了有关产品 ISO 文件中可执行文件的位置，以及组件在文件系统中的默认安装路径的信息：

Identity Manager 组件	版本 (Advanced/ Standard)	ISO 中可执行文件的位置	默认安装路径
身份库	Advanced 和 Standard	Setup.exe，位于 \products\eDirectory\x64\ 中	C:\NetIQ
iManager	Advanced 和 Standard	◆ **服务器安装：** iManagerInstall.exe，位于 \extracted_directory\products\iManager\installs\win\ ◆ **工作站安装：**iManager.bat，位于 imanager\bin	C:\Program Files\Novell
Identity Manager 引擎、驱动程序和插件	Advanced 和 Standard	idm_install.exe，位于 \products\idm\windows\setup 中	C:\Novell
Remote Loader	Advanced 和 Standard	idm_install.exe，位于 \products\idm\windows\setup 中	C:\Novell
PostgreSQL 和 Tomcat （受支持的数据库和应用程序服务器）	Advanced 和 Standard	TomcatPostgreSQL.exe，位于 products\CommonApplication\postgre_tomcat_install\ 中	C:\NetIQ\idm\apps\tomcat

Identity Manager 组件	版本 (Advanced/ Standard)	ISO 中可执行文件的位置	默认安装路径
单点登录 (OSP)	Advanced 和 Standard	osp-install-win.exe，位于 \products\CommonApplication\osp_install 中	C:\NetIQ\idm\apps\osp
Self Service Password Reset (SSPR)	Advanced 和 Standard	sspr-install-win.exe，位于 \products\CommonApplication\sspr_install 中	C:\NetIQ\idm\apps\sspr
Identity Applications	仅限 Advanced Edition	IdmUserApp.exe，位于 products\UserApplication 中	C:\NetIQ\idm\apps\UserApplication
Designer for Identity Manager	Advanced 和 Standard	install.exe，位于 \products\Designer\	c:\NetIQ\idm\apps\Designer
Identity Reporting	Advanced Edition 中完全支持 Standard Edition 中提供有限支持。	rpt-install-win.exe，位于 \products\Reporting 中	C:\NetIQ\idm\apps\IdentityReporting
Analyzer for Identity Manager	Advanced 和 Standard	install.exe，位于 \products\Analyzer\	C:\NetIQ\idm\apps\Analyzer

6 安装注意事项

本节列出了要托管 Identity Manager 组件的计算机所要满足的一般性先决条件。一般而言，您应该安装所有组件，以使您的环境能够提供完整的身份管理。但是，您并不一定需要全部组件，例如 Analyzer 或 iManager。

Identity Manager 实现可能因 IT 环境需要而异，因此在最终确定环境的 Identity Manager 体系结构之前，您应该先咨询 NetIQ 咨询服务部门或任何 NetIQ Identity Manager 合作伙伴。

有关建议的硬件、支持的操作系统和浏览器信息，请访问 NetIQ Identity Manager 技术信息网站。

6.1 了解 Identity Manager 通讯

为使 Identity Manager 组件之间能够正常通讯， NetIQ 建议您打开下表中列出的默认端口。

注释：如果某个默认端口已被占用，请确保为 Identity Manager 组件指定另一个端口。

端口号	组件计算机	端口用途
389	身份库	用于以明文方式与 Identity Manager 组件进行 LDAP 通讯
435	Identity Reporting	用于与 SMTP 邮件服务器进行通讯
524	身份库	用于 NetWare 核心协议 (NCP) 通讯
636	身份库	用于与 Identity Manager 组件进行 LDAP with TLS/SSL 通讯
5432	Identity Applications	用于与 Identity Applications 数据库进行通讯
7707	Identity Reporting	受管系统网关驱动程序使用该端口来与身份库进行通讯
8000	Remote Loader	驱动程序实例使用该端口进行 TCP/IP 通讯 **注释：**应为 Remote Loader 的每个实例指派唯一的端口。
8005	Identity Applications	Tomcat 使用该端口来侦听关闭命令
8009	Identity Applications	Tomcat 使用该端口通过 AJP 协议 （而不是 HTTP）来与 Web 连接器进行通讯
8028	身份库	用于 NCP 通讯的 HTTP 明文通讯
8030	身份库	用于 NCP 通讯的 HTTPS 通讯

端口号	组件计算机	端口用途
8080	Identity Applications iManager	Tomcat 使用该端口进行 HTTP 明文通讯
8090	Remote Loader	Remote Loader 使用该端口侦听来自远程接口 shim 的 TCP/IP 连接 **注释：**应为 Remote Loader 的每个实例指派唯一的端口。
8180	Identity Applications	运行 Identity Applications 的 Tomcat 应用程序服务器使用该端口进行 HTTP 通讯
8443	Identity Applications iManager	Tomcat 使用该端口进行 HTTPS (SSL) 通讯，或者重定向 SSL 通讯的请求
8543	Identity Applications	*默认情况下不侦听* 当您未使用 TLS/SSL 协议时， Tomcat 使用该端口来重定向需要 SSL 传输的请求
9009	iManager	Tomcat 为 MOD_JK 使用该端口
15432	Identity Reporting	用于 PostgreSQL 数据库 Sentinel
45654	User Application	将 Tomcat 与群集组搭配运行时，安装了 Identity Applications 数据库的服务器使用该端口来侦听通讯

6.2 了解语言支持

NetIQ 翻译了 （本地化） Identity Manager 的界面及其安装程序，以支持您本地计算机上的操作系统语言。但是，我们无法支持所有语言。在安装期间，某些安装程序将会检查计算机的区域设置，以确定安装过程的语言。

要以特定的语言运行安装程序，请通过区域设置选项更改区域设置。

6.2.1 已翻译的组件和安装程序

下表列出了每个组件安装的可用翻译版本。表格中未列出的组件只提供英语版。如果组件未被翻译成操作系统的语言，则安装程序默认使用英语。此外，安装程序中的 “ 最终用户许可协议 ” 可能未提供所有支持的语言版本。

区域设置	Designer	Identity Manager 引擎	iManager	iManager 插件	Identity Applications
简体中文	是	是	是	是	是
繁体中文	是	是	是	是	是
丹麦语	–	–	–	–	是
荷兰语	是	–	–	–	是
英语	是	是	是	是	是
法语	是	是	是	是	是

区域设置	Designer	Identity Manager 引擎	iManager	iManager 插件	Identity Applications
德语	是	是	是	是	是
意大利语	是	–	是	–	是
日语	是	是	是	是	是
葡萄牙语 （巴西）	是	–	是	–	是
俄罗斯语	–	–	是	–	是
西班牙语	是	–	是	–	是
瑞典语	–	–	–	–	是

Identity Applications 指仪表板、 Identity Applications 管理、 Identity Reporting、身份批准和 User Application。

6.2.2 语言支持的特别注意事项

在确定是否使用 Identity Manager 的翻译版本时， NetIQ 建议您查看以下注意事项。

- 一般而言，如果某个 Identity Manager 组件不支持操作系统的语言，则该组件的界面默认使用英语。例如， Identity Manager 驱动程序的语言与 Identity Manager 引擎的语言相同。如果 Identity Manager 不支持驱动程序的语言，则驱动程序配置默认使用英语。
- 以下 iManager 插件提供了西班牙语、俄语、意大利语、葡萄牙语以及上表中列出的语言版本。
- 在起动 Identity Manager 组件的安装程序时，需注意以下事项：
  - 如果操作系统使用安装程序支持的语言，则安装程序将默认使用该语言。但是，您也可以为安装过程指定其他语言。
  - 如果安装程序不支持操作系统的语言，则安装程序默认使用英语。
  - 如果操作系统使用某种拉丁语系的语言，则安装程序允许您指定任何一种拉丁语系的语言。
  - 如果操作系统使用支持的亚洲语言或俄语，则安装程序只允许您指定与操作系统匹配的语言或英语。

6.3 确保 Identity Manager 的高可用性

高可用性可确保关键网络资源 （包括数据、应用程序和服务）的高效可管理性。 NetIQ 通过群集或超级管理程序群集 （例如 VMWare Vmotion）支持 Identity Manager 解决方案的高可用性。规划高可用性环境时，应注意以下事项：

- 您可以在高可用性环境中安装以下组件：
  - 身份库
  - Identity Manager 引擎
  - Remote Loader
  - Identity Applications，不包括 Identity Reporting
- 当您在群集环境中运行身份库 (eDirectory) 时， Identity Manager 引擎也会加入群集。

有关下列项的详细信息 ...	参见 ...
确定 Identity Manager 组件的服务器配置	第 5.3.4 节 “ 建议的服务器设置 ”（第 41 页）
在群集中运行身份库	安装身份库的先决条件 （第 52 页）
	第 A.2 节 “ 在 eDirectory 群集上配置 NetIQ Identity Manager”（第 373 页）
	《*NetIQ eDirectory Installation Guide*》（NetIQ eDirectory 安装指南）中的 “Deploying eDirectory on High Availability Clusters”（在高可用性群集上部署 eDirectory）
在群集中运行 Identity Applications	第 14.2.4 节 “ 为群集配置 OSP 和 SSPR”（第 162 页）
	第 15.1.3 节 “ 安装 Identity Applications 的先决条件和注意事项 ”（第 167 页）
	第 15.4.2 节 “ 为群集启用许可权限索引 ”（第 178 页）
	第 15.4.4 节 “ 为 Identity Applications 准备群集 ”（第 179 页）
	第 15.6.2 节 “ 为群集配置 User Application 驱动程序 ”（第 192 页）
	针对分布式环境或群集环境更新仪表板中的 SSPR 链接 （第 203 页）

安装 Identity Manager 引擎

本部分提供了有关安装 Identity Manager 服务器的某些基本框架的信息。此安装程序允许您安装以下组件：

- Identity Manager 驱动程序
- Identity Manager 引擎
- Identity Manager 的 iManager 插件

为了方便起见， NetIQ 将这些组件捆绑在同一个安装程序中。您可以选择在同一个服务器上安装这些组件，也可以分别安装在不同服务器上。安装文件位于 Identity Manager 安装包的 \products\idm 目录中。默认情况下，安装程序将在 C:\Netiq 中安装组件。

NetIQ 建议您在开始之前，先查看安装过程。有关详细信息，请参见第 8.1 节 “Identity Manager 引擎、驱动程序和插件安装核对清单 ”（第 73 页）。

注释：此安装程序还可以安装 Remote Loader。有关详细信息，请参见第 10 部分 “ 安装和管理 Remote Loader”（第 85 页）。

---

7 安装身份库

本章将指导您完成安装身份库所需组件的过程。身份库用于储存 Identity Manager 特定的信息，例如驱动程序配置、参数和策略。

安装文件位于 Identity Manager 安装包 .iso 映像文件中的 \products\eDirectory*processor_type*\ 目录内。默认情况下，安装程序将在 C:\NetIQ\eDirectory 中安装身份库。

NetIQ 建议您在开始之前，先查看安装过程。有关详细信息，请参见第 7.1 章 " 规划安装身份库 "（第 51 页）。

7.1 规划安装身份库

本节提供了安装身份库所需的先决条件、注意事项以及系统设置。首先，请查阅核对清单，以了解安装过程。

7.1.1 身份库安装核对清单

NetIQ 建议您执行以下核对清单中的步骤：

	核对清单项目
❑	1. 了解 Identity Manager 各组件之间的交互。有关详细信息，请参见第 I 部分 " 简介 "（第 17 页）。
❑	2. 确定要为 Identity Manager 组件使用哪些服务器。有关详细信息，请参见第 5.3.4 节 " 建议的服务器设置 "（第 41 页）。
❑	3. 查看安装身份库的注意事项，以确保计算机符合先决条件。有关详细信息，请参见第 7.1.2 节 " 安装身份库的先决条件和注意事项 "（第 52 页）。
❑	4. 查看将要托管身份库的计算机所要满足的硬件和软件要求。有关详细信息，请参见第 7.1.4 节 " 身份库的系统要求 "（第 54 页）。
❑	5. 了解当身份库中的容器名称包含句点 （".") 时该如何使用转义符。有关详细信息，请参见第 7.2.1 节 " 当容器名称包含句点 （".") 时使用转义符 "（第 55 页）。
❑	6. 了解如何在使用 IPv6 地址的环境中使用身份库。有关详细信息，请参见第 7.2.4 节 " 在身份库服务器上使用 IPv6 地址 "（第 60 页）。
❑	7. 了解要进行 LDAP 通讯所需的端口。有关详细信息，请参见第 7.2.5 节 " 使用 LDAP 来与身份库通讯 "（第 61 页）。

	核对清单项目
❑	8. 有关安装指导，请参见以下章节之一： ◆ 要执行引导式安装 （向导），请参见第 7.3.1 节 " 使用向导安装身份库 " （第 63 页）。 ◆ 要执行无提示安装 （无人照管），请参见第 7.3.2 节 " 以无提示方式安装和配置身份库 " （第 63 页）。
❑	9. （可选）从任何防病毒或备份软件进程中排除 eDirectory 服务器上的 DIB 目录。
❑	10. （可选）备份 DIB 目录。有关详细信息，请参见 《*NetIQ eDirectory Administration Guide*》（NetIQ eDirectory 管理指南）中的 "Backing Up and Restoring NetIQ eDirectory" （备份和恢复 NetIQ eDirectory）。
❑	11. 安装 Identity Manager 引擎。有关详细信息，请参见第 8 章 " 规划引擎、驱动程序和插件的安装 " （第 73 页）。

7.1.2 安装身份库的先决条件和注意事项

身份库使用某个目录来储存通过 Identity Manager 解决方案同步的对象。以下各节包含相关指导，可帮助您规划要用作身份库框架的 NetIQ eDirectory 的部署。

- 安装身份库的先决条件 （第 52 页）
- 在群集环境中安装身份库的先决条件 （第 53 页）

安装身份库的先决条件

NetIQ 建议您在安装用作身份库框架的 eDirectory 之前，先查看以下注意事项：

- 要使 eDirectory 基础结构有效执行，您必须在服务器上配置一个静态 IP 地址。如果在服务器上使用 DHCP 地址， eDirectory 可能会发生不可预知的结果。
- 同步所有网络服务器上的时间。 NetIQ 建议使用网络时间协议 (NTP) 的 ntp 选项。
- （视情况而定）要安装二级服务器，安装该产品的目标分区中的所有复本都应处于 " 开 " 状态。
- （视情况而定）要以非管理员用户身份在现有树中安装二级服务器，请创建一个容器，然后对它进行分区。确保您具有以下权限：
  - 对该服务器所要添加到的目标分区具有 " 主管 " 权限。
  - 对要添加该服务器的容器具有 " 主管 " 权限。
  - 所有属性权限：对 W0.KAP.Security 对象具有读取、比较和写入权限。
  - 属性权限：对安全性容器对象具有读取和比较权限。
  - 条目权限：对安全性容器对象具有浏览权限。

  当复本计数小于 3 时，如果您要添加复本，则需要具有这些权限。
- （视情况而定）要以非管理员用户身份在现有树中安装二级服务器，请确保树中至少有一个服务器的 eDirectory 版本等于或高于以容器管理员身份添加的二级服务器的 eDirectory 版本。如果所添加的二级服务器的版本更高，树管理员必须先扩展纲要，然后使用容器管理员添加二级服务器。

- 配置 eDirectory 时，您必须在防火墙中启用 NetWare 核心协议 (NCP) 端口 （默认为 524），以允许添加二级服务器。此外，您还可以根据需要启用以下默认服务端口：
  - LDAP 明文 - 389
  - LDAP 安全 - 636
  - HTTP 明文 - 8028
  - HTTP 安全 - 8030
- 您必须使用适用于 eDirectory 的管理实用程序 （例如 iManager）在每个工作站上安装 Novell International Cryptographic Infrastructure (NICI)。 NICI 和 eDirectory 支持最多 4096 位的密钥大小。有关详细信息，请参见 《*NetIQ eDirectory Installation Guide*》（NetIQ eDirectory 安装指南）中的 “Installing NICI” （安装 NICI）。
- （视情况而定）如果 eDirectory 树中的容器名称包含句点，则您在安装期间以及在向现有树中添加服务器时，必须使用转义符指定管理员名称、管理员环境和服务器环境参数。有关详细信息，请参见第 7.2.1 节 “ 当容器名称包含句点 （“.”）时使用转义符 ” （第 55 页）。
- 您必须对 服务器以及对 eDirectory 树中包含支持域功能的 “ 用户 ” 对象的所有部分具有管理权限。安装到现有的树中时，需要具有对树对象的管理权限以便扩展纲要和创建对象。
- 由于 NTFS 提供的事务进程较之 FAT 文件系统提供的事务进程更安全，所以您只能在 NTFS 分区上安装 eDirectory。因此，如果您只有 FAT 文件系统，请执行以下操作之一：
  - 使用磁盘管理程序。有关详细信息，请参见 Windows Server 文档。
  - 创建一个新的分区并将其格式化为 NTFS。
  - 使用 CONVERT 命令将现有 FAT 文件系统转换为 NTFS。
  - 有关详细信息，请参见 Windows Server 文档。

  如果服务器仅有 FAT 文件系统，而您忘记或疏忽了这一过程，安装程序将提示您提供 NTFS 分区。
- 您必须运行最新版本的 Windows SNMP 服务。
- 只有 Windows 操作系统运行的是最新的服务包，您才可以开始安装过程。
- 要在具有 DHCP 地址的虚拟机上安装，或者要在未广播 SLP 的物理机或虚拟机上安装，请确保网络中已配置目录代理。

在群集环境中安装身份库的先决条件

NetIQ 建议您在群集环境中安装身份库之前，先查看以下注意事项：

- 必须配备两个或更多个装有群集软件的 Windows 服务器。
- 必须配备群集软件支持的外部共享储存，且其磁盘空间足以储存所有身份库和 NICI 数据：
  - 身份库 DIB 必须位于群集共享储存中。身份库的状态数据必须位于共享储存中，以供当前运行服务的群集节点使用。
  - 必须将每个群集节点上的根身份库实例配置为使用共享储存中的 DIB。
  - 此外，您还必须共享 NICI (NetIQ International Cryptographic Infrastructure) 数据，以便在群集节点之间复制服务器特定的密钥。所有群集节点使用的 NICI 数据必须位于群集共享储存中。
  - NetIQ 建议在共享储存中储存所有其他 eDirectory 配置和日志数据。

- 您必须有一个虚拟 IP 地址。
- （视情况而定）如果您使用 eDirectory 作为身份库的支持结构， nds-cluster-config 实用程序仅支持配置根 eDirectory 实例。 eDirectory 不支持配置多个实例，也不支持以非 root 身份在群集环境中安装 eDirectory。

有关在群集环境中安装身份库的详细信息，请参见 《*NetIQ eDirectory Installation Guide*》（NetIQ eDirectory 安装指南）中的 “Deploying eDirectory on High Availability Clusters” （在高可用性群集上部署 eDirectory）。

7.1.3 了解 eDirectory 中的 Identity Manager 对象

以下列表指出 eDirectory 中存储的主要 Identity Manager 对象以及这些对象如何彼此互相关联。安装过程不会创建对象。您需要在配置 Identity Manager 解决方案时创建 Identity Manager 对象。

- **驱动程序集：**驱动程序集是保存 Identity Manager 驱动程序和库对象的容器。在任何时候，一台服务器上只能有一个驱动程序集处于活动状态。但可能有多台服务器与一个驱动程序集关联。且一个驱动程序也可以同时与多台服务器关联。但此驱动程序在任何时候只应在一台服务器上运行。此驱动程序在其他服务器上应处于禁用状态。与驱动程序集关联的任何服务器上都必须安装 Identity Manager 服务器。
- **库：**库对象是可从多个位置参照的常用策略的储存库。库存储在驱动程序集中。可将策略放置在库中，以便驱动程序集中的每个驱动程序均可参照它。
- **驱动程序：**驱动程序连接应用程序与身份库。它还允许在系统间进行数据同步和共享。驱动程序存储在驱动程序集中。
- **作业：**作业就是将重现的任务自动化。例如，某个作业可以将系统配置为在特定一天禁用帐户，或启动工作流程以请求延长某用户对公司资源的访问时限。作业存储在驱动程序集中。

7.1.4 身份库的系统要求

本节提供要安装身份库的服务器的最低要求。请务必查看安装的先决条件和注意事项，特别是与操作系统有关的内容。

注释：BTRFS 文件系统不支持身份库。

类别	要求
处理器	1 GHz
磁盘空间	◆ 身份库需要 300 MB ◆ 每 50,000 个用户需要 150 MB 的额外磁盘空间
内存	2 GB

类别	要求
操作系统 （经认可）	以下 64 位操作系统之一： ◆ Windows Server 2016 ◆ Windows Server 2012 R2 ◆ Windows Server 2012 NetIQ 建议您在安装 Identity Manager 之前，按照制造商的自动更新工具应用最新的操作系统增补程序。 **注释：***经认可*指操作系统已经过全面测试且受支持。
操作系统 （受支持）	经认可操作系统的最新版服务包 **注释：***受支持*指操作系统尚未经过测试，但预期可以正常工作。
虚拟化系统	◆ Hyper-V Server 2012 R2 ◆ VMWare ESX 5.0 及更高版本 ◆ 包含 Hyper-V 的 Windows Server 2012 R2 Virtualization （受支持） NetIQ 支持在为运行 NetIQ 产品的操作系统提供官方支持的企业级虚拟化系统上安装 Identity Manager。只要虚拟化系统的供应商为这些操作系统提供官方支持， NetIQ 就可支持这些系统上的整个 Identity Manager 堆栈。
目录服务	NetIQ eDirectory 9.1

7.2 准备安装身份库

必须恰当配置身份库的环境。例如，服务器必须能够通过某种方法 （服务或指定的文件）将身份库中的树名解析为服务器参照。本节将帮助您准备要安装身份库的环境。

7.2.1 当容器名称包含句点 （“.”）时使用转义符

您可以在目录树中添加服务器名称中包含句点的 Windows 服务器。例如， O=netiq.com 或 C=u.s.a。但是，如果树中的容器名称包含句点 （“.”），则必须使用转义符。请查看以下注意事项：

- 请勿在服务器名称的开头使用句点，例如：.netiq。
- 使用反斜杠 （“\”）来转义容器名称中的句点。例如：

  ```
  O=novell\.com
  ```

  或者

  ```
  C=a\.b\.c
  ```

为 iMonitor、iManager、DHost iConsole、DSRepair、Backup、DSMerge、DSLogin 和 ldapconfig 等实用程序输入带句点的管理员名称和环境时，请包含转义符。例如，在登录 iMonitor 时，如果树中 O 的名称为 netiq.com，请输入 'admin.netiq\.com' 或 admin.netiq\.com。

7.2.2 使用 OpenSLP 或 hosts.nds 解析树名

在安装身份库基础结构之前，服务器应该能够通过某种方法 （服务或指定的文件）将身份库中的树名解析为服务器参照。 NetIQ 建议使用服务定位协议 (SLP) 服务来解析树名。 eDirectory 先前版本的安装中包含 OpenSLP。但是，从 eDirectory 8.8 开始，安装中不再包含 OpenSLP。您必须单独安装 SLP 服务或使用 hosts.nds 文件。如果您使用 SLP 服务，该服务的目录代理 (SLPDA) 必须稳定。

本节提供以下信息：

- 使用 hosts.nds 文件解析树名 （第 56 页）
- 了解 OpenSLP （第 57 页）
- 为身份库配置 SLP （第 59 页）

使用 hosts.nds 文件解析树名

hosts.nds 文件是一个静态查找表，身份库应用程序使用它来搜索身份库分区和服务器。当网络中不存在 SLP DA 时，它可以帮助您避免 SLP 多路广播延迟。对于每个树或服务器，您必须在 hosts.nds 文件的一行中指定以下信息：

- **服务器名称或树名**：树名应以后随点 (.) 结尾。
- **因特网地址**：可以是 DNS 名称或 IP 地址。请不要使用 localhost。
- **服务器端口**：（可选）追加在因特网地址后面以冒号 (:) 分隔。

除非本地服务器在非默认 NCP 端口上侦听，否则不需要在该文件中包含本地服务器的对应项。

要配置 hosts.nds 文件，请执行以下操作：

1 创建新的或打开现有的 hosts.nds 文件。

2 添加以下信息：

```
partition_name.tree_name. host_name/ip-addr:port server_name dns-addr/ip-
addr:port
```

例如：

```
# This is an example of a hosts.nds file:
# Tree name Internet address/DNS Resolvable Name
  CORPORATE. myserver.mycompany.com
  novell.CORPORATE. 1.2.3.4:524

# Server name Internet address
  CORPSERVER myserver.mycompany.com:524
```

3 （可选）如果您随后决定使用 SLP 来解析树名并确保网络中提供身份库树，请在 hosts.nds 文件中添加以下文本：

```
/usr/bin/slptool findattrs services:ndap.novell///(svcname-ws==[treename or
*])"
```

例如，要搜索其 svcname-ws 属性与 SAMPLE_TREE 值匹配的服务，请输入以下命令：

```
/usr/bin/slptool findattrs services:ndap.novell///(svcname-ws==SAMPLE_TREE)"
```

注释：请在安装 SLP 和身份库之后执行此操作。

如果所注册服务的 svcname-ws 属性为 SAMPLE_TREE，则输出将与 service:ndap.novell:///SAMPLE_TREE 类似。否则，您将不会收到输出响应。

了解 OpenSLP

OpenSLP 指的是 IETF Request-For-Comments (RFC) 2608 中所述的 IETF 服务定位协议 2.0 版标准的开源实现。

由 OpenSLP 源代码提供的接口是 RFC 2614 中所述的、以编程方式访问 SLP 功能的另一种 IETF 标准的实现。

要完全了解 SLP 的工作原理，最好阅读这些文档并吃透其中的内容。它们未必通俗易懂，但要想在内部网中正确配置 SLP，您必须了解这些知识。

有关 OpenSLP 项目的详细信息，请参见 OpenSLP 和 SourceForge 网站。 OpenSLP 网站上提供了包含有用配置提示的数份文档。其中的许多文档在本文档发布时并不完善。

本节中包含了有个 SLP 的用途以及它与身份库关系的以下讨论：

- NetIQ 服务定位提供程序 （第 57 页）
- 用户代理 （第 58 页）
- 服务代理 （第 58 页）
- 目录代理 （第 58 页）

NetIQ 服务定位提供程序

为了提供更强大的服务播发环境， NetIQ 版本的 SLP 采用了某些具有 SLP 标准的库，但这样做的代价是降低了一定程度的可伸缩性。

例如，为了改善服务播发框架的可伸缩性，您可以对在子网上广播或进行多路广播的包数加以限制。SLP 规范通过对服务代理和用户代理上的目录代理查询施加限制，来实现此管理。发现的作用于所需范围的第一个目录代理，就是服务代理 （以及本地用户代理）要为该范围的所有未来请求使用的目录代理。

实际上， NetIQ SLP 实现会扫描它所知道的所有目录代理以获取查询信息。它认为 300 毫秒的一轮往返时间已经很长，因此它可以在 3 到 5 秒内扫描 10 个服务器。如果已在网络中正确配置了 SLP，则不需要设置此时间， OpenSLP 假定针对 SLP 流量正确配置了网络。 OpenSLP 的响应超时值大于 NetIQ SLP 服务提供程序的超时值，它会将目录代理的数目限制为响应的第一个代理，而不管该代理的信息是否正确和完整。

用户代理

用户代理 (UA) 采用与某个应用程序链接的静态或动态库的物理形式。它允许该应用程序查询 SLP 服务。用户代理的工作是提供一个编程接口，使客户端能够查询服务，并使服务能够自我播发。用户代理将联系目录代理以查询位于指定范围内的、具有指定服务类的已注册服务。

用户代理遵循某种算法来获取查询将要发送到的目录代理的地址。一旦获取指定范围的目录代理 (DA) 地址，它们便会针对该范围一直使用该地址，直到其不再做出响应，此时，用户代理将获取该范围的另一个 DA 地址。用户代理通过以下方式查找指定范围的目录代理地址：

1. 检查以确定当前请求中的套接字句柄是否已连接到指定范围的 DA。如果该请求正好是一个多部分请求，则表示该请求中可能已存在超速缓存的连接。
2. 检查它的本地已知 DA 超速缓存以查找与指定范围匹配的 DA。
3. 检查本地服务代理 (SA) 以查找具有指定范围的 DA （并将新地址添加到超速缓存）。
4. 查询 DHCP 以查找与指定范围匹配的、网络配置的 DA 地址 （并将新地址添加到超速缓存）。
5. 在已知的端口上多路广播 DA 发现请求 （并将新地址添加到超速缓存）。

指定的范围为 “default” （如果未指定）。也就是说，如果未在 SLP 配置文件中静态定义任何范围，并且未在查询中指定任何范围，那么，使用的范围将为 “default”。此外，还应注意，身份库永远不会在其注册中指定范围。如果存在静态配置的范围，则在缺少某个指定范围的情况下，该范围将成为所有本地 UA 请求和 SA 注册的默认范围。

服务代理

服务代理采用主机上单独进程的物理形式。 slpd.exe 作为本地计算机上的服务运行。用户代理通过向已知端口上的回写地址发送讯息来查询本地服务代理。

服务代理的工作是为已向 SLP 自行注册的本地服务提供持久的储存和维护地点，其本质上维护的是已注册本地服务的内存中数据库。事实上，除非存在本地 SA，否则服务无法向 SLP 注册。客户端能够发现仅包含 UA 库的服务，但注册却需要 SA，其主要原因是 SA 必须定期重新声明已注册服务的存在性，以维护在侦听目录代理中的注册。

服务代理通过执行以下操作并直接向可能的 DA 地址发送 DA 发现请求，来查找和超速缓存目录代理及其支持的范围列表：

1. 检查所有静态配置的 DA 地址 （并将新地址添加到 SA 的已知 DA 超速缓存）。
2. 请求 DHCP 中的 DA 和范围的列表 （并将新地址添加到 SA 的已知 DA 超速缓存）。
3. 在已知端口上多路广播 DA 发现请求 （并将新地址添加到 SA 的已知 DA 超速缓存）。
4. 接收 DA 定期广播的 DA 播发包 （并将新地址添加到 SA 的已知 DA 超速缓存）。

用户代理始终会先查询本地服务代理，这一点非常重要，因为本地服务代理的响应决定了用户代理是否要继续执行下一个发现阶段 （在本案例中为 DHCP - 请参见用户代理 （第 58 页）中的步骤 3 和步骤 4）。

目录代理

目录代理的工作是为播发的服务提供长期持久的超速缓存，以及为用户代理提供查找服务的访问点。作为超速缓存， DA 将侦听 SA 以播发新服务，并超速缓存这些通知。不久后， DA 的超速缓存就会变得更充实，或者说更完整。目录代理使用失效算法来令超速缓存项失效。某个目录代理启动时，将会

从持久存储 （通常是硬盘驱动器）中读取其超速缓存，然后开始根据算法令超速缓存项失效。当有新的 DA 启动或者当删除某个超速缓存时， DA 将检测此情况，并向所有侦听 SA 发送让其转储本地数据库的特殊通知，以使 DA 能够快速构建超速缓存。

在不存在任何目录代理的情况下，将由 UA 执行 SA 可以响应的常规多路广播查询，以 DA 构建超速缓存时所用的大致相同方式构建所请求服务的列表。此类查询返回的服务列表是不完整的，与 DA 提供的服务列表相比，该列表的本地化程度要高得多，特别是当存在多路广播过滤时尤其如此，为了将广播和多路广播局限于本地子网，许多网络管理员会执行此项过滤。

总而言之，所有这一切都取决于用户代理针对给定范围查找到的目录代理。

为身份库配置 SLP

%systemroot%/slp.conf 文件中的以下参数用于控制目录代理发现：

```
net.slp.useScopes = comma-delimited scope list
net.slp.DAAddresses = comma-delimited address list
net.slp.passiveDADetection = <"true" or "false">
net.slp.activeDADetection = <"true" or "false">
net.slp.DAActiveDiscoveryInterval = <0, 1, or a number of seconds>
```

useScopes

指定 SA 要播发到的范围，以及当服务或客户端应用程序执行的注册或查询不存在特定的范围时，执行查询时将采用的范围。由于身份库会始终播发到默认范围并在默认范围内执行查询，此列表将成为所有身份库注册和查询的默认范围列表。

DAAddresses

表示优先级最高的 DA 点分十进制 IP 地址的逗号分隔列表。如果此已配置 DA 列表不支持某个注册或查询的范围，才会由 SA 和 UA 执行多路广播 DA 发现，除非禁用了此类发现。

passiveDADetection

默认情况下为 True。目录代理将定期通过已知端口在子网上广播其存在性 （如果已进行了相应的配置）。这些包称为 DAAdvert 包。如果将此选项设置为 False， SA 将忽略所有广播 DAAdvert 包。

activeDADetection

默认情况下为 True。此参数允许 SA 定期广播请求，以使所有 DA 能够以定向的 DAAdvert 包作为响应。定向包不会以广播发出，而是应请求在响应中直接发送给 SA。如果将此选项设置为 False，则 SA 将不会定期广播 DA 发现请求。

DAActiveDirectoryInterval

表示一个 tri-state 参数。默认值为 1，该特殊值表示 SA 在初始化时只应发出一个 DA 发现请求。将此选项设置为 0 相当于将 activeDADetection 选项设置为 false。任何其他值是发现广播之间间隔的秒数。

正确使用这些选项可确保合理使用网络带宽来进行服务播发。事实上，所设计的默认设置本就优化了一般网络的可伸缩性。

7.2.3 改进身份库性能

身份库的底层基础结构 eDirectory 属于 I/O 密集型应用程序，而不是处理器密集型应用程序。以下两个因素可以提高身份库的性能：更多的超速缓存内存和更快的处理器。为了达到最佳效果，应在硬件允许的情况下尽可能多地超速缓存目录信息数据库 (DIB) 集。

尽管在单个处理器上 eDirectory 就能获得良好的伸缩性，但您还是可以考虑使用多个处理器。增加处理器会改进用户登录等方面的性能。此外，在多个处理器上激活多个线程也能提高性能。

下表提供了根据 eDirectory 中预期对象数进行服务器设置的一般指导。

对象	内存	硬盘
100.000	384 MB	144 MB
100 万	4 GB	1.5 GB
1000 万	2 GB 以上	15 GB

例如，对于带有标准纲要的 eDirectory 基本安装，每 50,000 位用户需要大约 74 MB 磁盘空间。但如果添加一组新特性或将每个现有特性完全填满，则对象将增大。进行这样的添加会影响所需的磁盘空间、处理器和内存。此外，对处理器的要求取决于计算机上可用的附加服务以及计算机要处理的鉴定、读和写的数量。加密和索引编制等进程可能会占用大量处理器时间。

7.2.4 在身份库服务器上使用 IPv6 地址

身份库同时支持 IPv4 和 IPv6 地址。您可以在安装身份库时启用 IPv6 地址。如果是从先前的版本升级，则必须手动启用 IPv6 地址。

身份库还支持双 IP 堆栈、隧道和纯 IPv6 转换方法。它仅支持全局 IP 地址。例如：

- [::]
- [::1]
- [2015::12]
- [2015::12]:524

指定 IPv6 地址时必须将其括在方括号 [ ] 中。要使用主机名而不是 IP 地址，您必须在 C:\Windows\System32\drivers\etc\hosts 文件中指定该名称，并将它与 IPv6 地址关联。

要在 Windows 服务器上使用 IPv6 地址，必须在安装期间选中 **IPv6 自选设置**下的**启用 IPv6** 复选框。此选项将为 IPv6 地址启用 NCP、 HTTP 和 HTTPS 协议。如果您在安装过程中未启用 IPv6 地址，后来又决定使用 IPv6 地址，则您必须重新运行安装程序。有关详细信息，请参见第 7.3 章 “ 安装身份库 ”（第 62 页）。

可以使用以下链接通过 IPv6 地址访问 iMontior：http://[2015::3]:8028/nds。

7.2.5 使用 LDAP 来与身份库通讯

当您安装身份库时，必须指定 LDAP 服务器监视的端口，以便其可通过该端口为 LDAP 请求提供服务。作为默认配置的一部分，明文和 SSL/TLS 的端口号分别设置为 389 和 636。

LDAP 简单绑定仅需要 DN 和口令。该口令采用明文格式。如果您使用端口 389，则整个包都采用明文格式。由于端口 389 允许明文， LDAP 服务器将通过此端口为目录的读请求和写请求提供服务。这种开放性适合不会发生欺骗且没有人会通过不当方式捕获包的信任环境。默认情况下，在安装期间会禁用此选项。

通过端口 636 的连接已加密。由 TLS （前称 SSL）管理此项加密。到端口 636 的连接会自动实例化一个握手。如果握手失败，则会拒绝连接。

注释：默认情况下，安装程序会选择端口 636 进行 TLS/SSL 通讯。此默认设置可能会给您的 LDAP 服务器带来问题。如果 （在安装 eDirectory 之前）主机服务器上已装载的服务使用了端口 636，则您必须指定另一个端口。在 eDirectory 8.7 版之前的安装中会将此冲突视为致命错误，并会卸载 nldap。而在 eDirectory 8.7.3 之后的版本中，安装程序会装载 nldap，然后在 dstrace.log 文件中添加一条错误讯息，并在不使用安全端口的情况下运行。

在安装过程中，您可以将身份库配置为禁止明文口令和其他数据。选择**对于带口令的简单绑定需要 TLS** 选项可以阻止用户发送可辨认的口令。如果您不选择此设置，用户将不知道其他人可以察觉到他的口令。这个不允许连接的选项仅适用于明文端口。如果与端口 636 建立安全连接并使用简单绑定，则连接已加密。没有人可以查看口令、数据包或绑定请求。

请考虑以下情况：

已启用 “ 对于带口令的简单绑定需要 TLS”

Olga 使用的客户端要求输入口令。 Olga 输入口令后，客户端才会连接到服务器。但是， LDAP 服务器不允许连接通过明文端口绑定到服务器。任何人都可以查看 Olga 的口令，但 Olga 无法获取绑定的连接。

已使用端口 636

您的服务器正在运行 Active Directory。 Active Directory 运行的 LDAP 程序使用了端口 636。安装 eDirectory。安装程序检测到端口 636 已被占用，并且未向 NetIQ LDAP 服务器指派端口号。LDAP 服务器已装载并看上去已运行。但是，由于 LDAP 服务器不会复制或使用已打开的端口，因此， LDAP 服务器不会在任何复制的端口上为请求提供服务。

要校验是否已将端口 389 或 636 指派给 NetIQ LDAP 服务器，请运行 ICE 实用程序。如果*供应商版本*字段中未指定 NetIQ，则您必须为 eDirectory 重配置 LDAP 服务器，并选择其他端口。有关详细信息，请参见 《*NetIQ eDirectory Administration Guide*》（NetIQ eDirectory 管理指南）中的 “Verifying That the LDAP Server is Running” （校验 LDAP 服务器是否正在运行）。

Active Directory 正在运行

如果 Active Directory 正在运行并且明文端口 389 已打开，则您可以对端口 389 运行 ICE 命令，并请求输入供应商版本。报告将显示 **Microsoft***。然后，您可以通过选择另一个端口来重配置 NetIQ LDAP 服务器，使 eDirectory LDAP 服务器能够为 LDAP 请求提供服务。

iMonitor 还可以报告端口 389 或 636 是否已打开。如果 LDAP 服务器不起作用，请使用 iMonitor 来查看细节。有关详细信息，请参见 《*NetIQ eDirectory Administration Guide*》（NetIQ eDirectory 管理指南）中的 “Verifying That the LDAP Server is Running” （校验 LDAP 服务器是否正在运行）。

7.2.6 在使用管理实用程序的工作站上手动安装 NICI

必须在使用 iManager 等管理实用程序的每个工作站上安装 NICI。有关将 NICI 与身份库配合使用的详细信息，请参见安装身份库的先决条件 （第 52 页）。

要安装 NICI，请使用默认位于 products\eDirectory*processor_type*\windows*processor_type*\nici 文件夹中的 NICI_wx64.msi 文件。您可以使用引导式过程 （向导）或无提示安装方式运行该文件。

7.2.7 安装 NMAS 客户端软件

必须在您想要使用 NetIQ Modular Authentication Service (NMAS) 登录方法的每个客户端工作站上安装 NMAS 客户端软件。登录方法是在安装身份库时指定的。

1. 使用管理员帐户登录到 客户端工作站。
2. 从安装目录 （默认为 Win:\products\eDirectory*processor_type*\nmas\）运行 nmasinstall.exe 程序。
3. 单击 **NMAS 客户端组件**。
4. （可选）选择 NICI 选项以安装 NICI 组件。
5. 单击**确定**。
6. 安装过程完成后，重启动客户端工作站。

7.3 安装身份库

安装程序将引导您完成身份库的配置设置。安装程序会自动默认为向导模式。但是，您也可以执行无提示安装。

本节假设您要将 eDirectory 用作身份库的基本结构。

当您启动安装程序时，它会检查 Novell International Cryptographic Infrastructure (NICI) 和 Novell Client for Windows。安装程序会根据需要安装或更新这些组件。如果在已包含 Novell Client 的计算机上安装身份库， eDirectory 将使用现有的 Novell Client。在没有 Novell Client 的情况下，您可以安装 Identity Vault

有关 NICI 的详细信息，请参见 《*Novell International Cryptographic Infrastructure Administration Guide*》（Novell International Cryptographic Infrastructure 管理指南）。有关 Client 的详细信息，请参见 Novell Client for Windows 文档。

安装程序可以安装 NetIQ Module Authentication Service (NMAS) 的服务器组件。在安装期间，您必须指定要与 NMAS 配合使用的登录方法。此外，还必须在您想要使用 NMAS 登录方法的每个客户端工作站上安装 NMAS 客户端软件。

注释：

- 从 eDirectory 8.8 开始，可以对所有实用程序使用区分大小写的口令。
- 容器名称可以包含句点。有关在容器名称中使用句点的信息，请参见第 7.1.2 节 “ 安装身份库的先决条件和注意事项 ” （第 52 页）。

7.3.1 使用向导安装身份库

1 以管理用户身份登录到要安装 eDirectory 的计算机。
2 导航到 \products\eDirectory\x64\ 目录。
3 运行 eDirectory_910_windows_x86_64.exe 文件。
4 在基本选项卡中指定以下细节：
   - 如果选择了新建树，请指定以下细节：
      - **树名：**指定身份库的树名。
      - **服务器 FDN：**指定服务器 FDN。

      注释：尽管身份库允许为 NCP 服务器对象设置最多包含 256 个字符的 FDN，但 NetIQ 建议将该变量限制为一个小得多的值，因为身份库会根据此对象的长度创建其他更长的对象。

      - **树管理员：**指定身份库的管理员名称。
      - **管理员口令：** 指定管理员口令。
   - 如果选择了现有树，请指定以下细节：
      - **IP 地址：**指定身份库现有树的 IP 地址。
      - **端口号：**指定现有树的端口号。默认值是 524。
      - **服务器 FDN：**指定服务器 FDN。
      - **树管理员：**指定身份库的现有管理员名称。
      - **管理员口令：**指定管理员口令。
5 （视情况而定）在高级选项卡中指定以下细节：
   - 要在身份库服务器上使用 IPv6 地址，请选择**启用 IPv6**。

      注释：NetIQ 建议您启用此选项。要在安装后启用 IPv6 地址，必须重新运行安装程序。

   - 要启用增强的后台鉴定 (EBA)，请选择**启用 EBA**。
   - 指定 HTTP 明文端口和安全端口。默认值分别为 8028 和 8030。
   - 指定 LDAP 明文端口和安全端口。默认值分别为 389 和 636。
6 在安装位置字段中，指定身份库的安装位置。
7 在 **DIB 位置**字段中，指定 DIB 文件所在的位置。
8 单击安装，然后继续安装。

7.3.2 以无提示方式安装和配置身份库

要支持以无提示 （或无人照管）方式安装或配置身份库，您可以使用一个包含相应部分和键的 response.ni 文件，该文件与 Windows.ini 文件类似。

注释：必须安装并配置 NetIQ SecreStore (ss)。有关详细信息，请参见第 7.4.1 节 “ 将 SecretStore 添加至身份库纲要 ”（第 70 页）。

编辑 response.ni 文件

您可以使用 ASCII 文本编辑器来创建和编辑 response.ni 文件。该 response 文件可帮助您：

- 使用所有必要的用户输入执行完全无人照管的安装。
- 定义组件的默认配置。
- 在安装期间绕过所有提示。

NetIQ 在安装套件的 products\eDirectory\x64\windows\x64\NDSonNT 文件夹中提供了 response.ni 文件。该文件包含必不可少的参数的默认设置。您必须编辑 NWI:NDS 部分中的 eDirectory 实例的值。

注释：当您编辑 response.ni 文件时，请不要在每个键 - 值对中的键、值和等号 （“=”）之间包含空格。

警告：在 response.ni 文件中为无人照管安装指定管理员用户身份凭证。为了防止管理员身份凭证泄露，应该在完成安装或配置后永久性删除该文件。

以下各部分描述了 response.ni 文件中所需的部分和键：

NWI:NDS

Upgrade Mode

指定是否要以升级模式运行安装程序。有效值为 False、 True 和 Copy。

Mode

指定要执行的安装类型：

- **full** 可让您同时安装和配置身份库。如果您想执行全新安装并配置身份库，或者只想升级并配置所需的文件，请指定此值。
- **install** 可让您安装全新版本的身份库，或升级所需的文件。
- **configure** 可让您修改身份库设置。如果您只执行所需文件的升级，则安装程序将只配置升级的文件。

注释：

- 如果指定 *configure*，请确保不要更改 [Initialization] 部分中的 ConfigurationMode 键的 RestrictNodeRemove 值。
- 如果指定 *full*，则在卸装身份库时，您无法单独选择取消配置和卸装选项。

New Tree

指定此次安装的是新树还是二级服务器。有效值为 Yes 和 No。例如，如果您要安装新树，请指定 Yes。有关指定现有树的值的详细信息，请参见 Novell:ExistingTree:1.0.0 （第 68 页）。

Tree Name

如果是全新安装，请指定想要安装的树的名称。要安装二级服务器，请指定要将该服务器添加到的树。

Server Name

指定要在身份库中安装的服务器的名称。

Server Container

指定树中要将服务器对象添加到的容器对象。服务器对象包含特定于身份库服务器的所有配置细节。如果您要安装全新版本的身份库，安装程序将使用服务器对象创建此容器。

Server Context

指定服务器对象 （服务器名称）的完整判别名 (DN) 以及容器对象。例如，如果身份库服务器为 EDIR-TEST-SERVER，容器为 Netiq，则指定 EDIR-TEST-SERVER.Netiq。

Admin Context

指定树中要将管理员对象添加到的容器对象。例如：Netiq。添加到树中的任何用户都有一个用户对象，其中包含该用户特定的所有细节。如果您要安装全新版本的身份库，安装程序将使用服务器对象创建此容器。

Admin Login Name

指定树中至少对此服务器所要添加到的环境具有完全权限的管理员对象的相对判别名 (RDN)。例如：Admin。安装程序将使用此帐户在树中执行所有操作。

Admin Password

指定管理员对象的口令。例如：netiq123。如果您要安装全新版本的身份库，安装程序将为管理员对象配置此口令。

NDS Location

指定要将身份库文件库和二进制文件安装到的本地系统中的路径。当您配置身份库组件时，这些组件将参照相关文件的此安装位置。默认情况下，安装程序会将文件放在 C:\Novell\NDS 中。

DataDir

指定要将 DIB 文件安装到的本地系统中的路径。默认情况下，安装程序会将文件放在 C:\Novell\NDS\DIBFiles 中。

如果您环境的 DIB 数据文件所需的空间超过了默认位置的可用空间，则可能需要指定其他路径。

Installation Location

（可选）指定安装程序在向 NDS 位置复制文件时使用的路径。例如：[Novell:DST:1.0.0_Location] 或 Path=file://C:\Novell\NDS。默认值为 C:\Novell\NDS，这与 “NDS Location” 的默认值相同。安装程序在向指定的 NDS 和 DataDir 位置复制文件时将使用此路径。

System Location

（可选）指定要将身份库服务器安装到的计算机上系统文件夹的路径。例如：[Novell:SYS32_DST:1.0.0_Location] 或 Path=file:/C:\Windows\system32。安装期间安装程序需要访问系统文件夹，以复制 DLL 并访问系统特定的文件。

Require TLS

（可选）指定身份库在接收明文格式的 LDAP 请求时是否需要传输层安全性 (TLS) 协议。

LDAP TLS Port

（可选）指定身份库要在其上侦听明文格式的 LDAP 请求的端口。

LDAP SSL Port

（可选）指定身份库应在其上使用安全套接字层 (SSL) 协议侦听 LDAP 请求的端口。

Install as Service

指示安装程序以服务形式安装 eDirectory。必须指定 Yes。

Prompt

指定是否要让安装程序提示您来决定诸如树名和服务器名称等项目。例如，在采用无提示或无人照管安装时，请指定 False。

NWI:NMAS （NMAS 方法）

在安装和升级期间，身份库支持多种 NMAS 方法。必须在 response.ni 文件中指定 NDS NMAS 方法。如果未指定任何 NMAS 方法，安装程序默认安装 NDS 方法。但是，如果您要创建一个明确的列表，则必须包含 NDS。

Choices

指定要安装的 NMAS 方法的数量。例如：5。

Methods

指定要安装的 NMAS 方法的类型。使用逗号分隔多个类型。例如：CertMutual,Challenge Response,DIGEST-MD5,NDS。

安装程序在选择要安装的 NMAS 方法时会比对确切的字符串 （包括大小写），因此，您必须完全按照列出的内容指定值：

- CertMutual
- Challenge Response - 表示 NetIQ 询问应答 NMAS 方法。
- DIGEST-MD5
- Enhanced Password
- Entrust
- GSSAPI - 表示 eDirectory 的 SASL GSSAPI 机制。使用 Kerberos 票据到身份库的鉴定贯穿整个 LDAP。
- NDS - 默认的登录方法。 REQUIRED.

- NDS Change Password
- Simple Password
- Universal Smart Card
- X509 Advanced Certificate
- X509 Certificate

当您在 response 文件中指定 NMAS 方法后，身份库将在安装时显示状态讯息，但不提示用户输入。

eDir:HTTP （端口）

身份库将在预配置的 HTTP 端口上侦听通过 Web 进行的访问。例如， iMonitor 通过 Web 界面访问身份库。需要指定特定的端口来访问相应的应用程序。以下选项可让您针对特定的端口配置身份库：

Clear Text HTTP Port

指定用于明文格式的 HTTP 操作的端口号。

SSL HTTP Port

指定用于使用 SSL 协议进行的 HTTP 操作的端口号。

Novell:Languages:1.0.0 （语言设置）

在安装期间，您可以指定身份库的区域设置和显示语言：英语、法语或日语。这些值是互斥的。

LangID4

表示英语。例如：LangID4=true。

LangID6

表示法语。

LangID9

表示日语。

注释：

- 请不要为一个以上的语言指定 true。
- 还可以指定安装程序在整个安装过程中用来显示讯息的语言。有关详细信息，请参见 Initialization（第 67 页）。

Initialization

response.ni 文件的 [Initialization] 部分指定安装过程的设置。

DisplayLanguage

指定安装过程中用于显示讯息的语言。例如：DisplayLanguage=en_US。

InstallationMode

指定要运行安装过程的方式。例如，要执行无提示或无人照管安装，请指定 silent。

SummaryPrompt

指定是否要让安装程序提示您复查安装设置的摘要。例如，在采用无提示或无人照管安装时，请指定 false。

prompt

指定是否要让安装程序提示您做出决定。例如，在采用无提示或无人照管安装时，请指定 false。

NWI:SNMP

大多数 Windows 服务器都配置并运行了 SNMP。在安装身份库时，您必须停止 SNMP 服务，并在完成安装过程后重启动这些服务。在手动安装期间，程序会提示您先停止 SNMP 服务然后再继续安装。

如果希望在无提示或无人照管安装期间停止 SNMP 服务且不收到提示，请在 response.ni 文件的 [NWI:SNMP] 部分中指定 Stop Service=yes。

EDIR:SLP

在安装或升级期间，身份库使用服务定位协议 (SLP) 服务识别子网中的其他服务器或树。如果您的服务器上已安装有 SLP 服务，可以将它们替换为当前身份库版本随附的服务版本，也可以使用您自己的 SLP 服务。

Need to uninstall service

指定是否要卸装服务器上已安装的所有 SLP 服务。默认值为 true。

Need to remove files

指定是否要去除服务器上已安装的所有 SLP 服务的文件。默认值为 true。

Novell:ExistingTree:1.0.0

安装程序提供了相应的选项让您可以选择以无人照管方式在网络中安装主服务器或二级服务器。安装程序使用三个不同的键来决定是要安装新树，还是在现有树中安装二级服务器。

注释：New Tree 键位于 NWI:NDS 部分中。有关详细信息，请参见 NWI:NDS （第 64 页）。

ExistingTreeYes

有效值为 True 和 False。例如，如果您要安装新树，请指定 False。

ExistingTreeNo

有效值为 True 和 False。例如，如果您要安装新树，请指定 True。

如果想要运行无提示或无人照管安装而不希望安装程序提示您决定是选择主服务器安装还是二级服务器安装，请在 response.ni 文件的 Existing Tree 部分中指定 prompt=false。

Selected Nodes

response.ni 文件的此部分列出了身份库中安装的组件，以及包含组件详细信息的配置文件数据库中的信息，包括源位置、目标复制位置和组件版本。配置文件数据库中的这些细节已被编译到身份库版本中随附的 .db 文件中。

如果想要运行无提示或无人照管安装而不希望安装程序提示您来决定目标复制位置或版本细节之类项目，请在 response.ni 文件的 [Selected Nodes] 部分中指定 prompt=false。

您的 response 文件必须包含此部分。请使用与示例 response.ni 文件中提供的完全相同的键和值。

Novell:NOVELL_ROOT:1.0.0

response.ni 文件的此部分包含安装过程中发生的图像和状态显示设置。例如，您可以指定安装程序对于文件写入冲突和文件复制决策等情况的响应方式设置。您还可以指定是否显示图像。大多数图像包含有关下列内容的信息：安装的身份库版本、安装的组件、欢迎屏幕、许可证文件、自定义选项、指示当前正在安装的组件的状态讯息、完成百分比等。要嵌入 eDirectory 的某些应用程序可能不希望 eDirectory 显示这些图像。

如果想要运行无提示或无人照管安装而不希望安装程序提示您来决定目标复制位置或版本细节之类项目，请在 response.ni 文件的此部分中指定 prompt=false。

您的 response 文件应包含此部分。请使用示例 response.ni 文件中提供的键和值。

执行无提示或无人照管安装

在开始之前，请查看有关执行无提示或无人照管安装的先决条件。有关详细信息，请参见第 7.1.2 节 " 安装身份库的先决条件和注意事项 " （第 52 页）。此外，请创建要用作安装模板的 response.ni 文件。有关详细信息，请参见编辑 response.ni 文件 （第 64 页）。

注释：为确保操作系统不会显示安装、升级或配置的状态窗口，请在命令中使用 nopleasewait 选项。

---

1. 创建新的 response.ni 文件或编辑现有的 response 文件。有关 response 文件中的值的详细信息，请参见编辑 response.ni 文件 （第 64 页）。
2. 使用管理员帐户登录到要安装身份库的计算机。
3. 在启用**以管理员身份运行**选项的情况下打开命令提示符。
4. 在命令行中输入以下命令：

   ```
   path_to_installation_files\windows\eDirectory\x64\NDSonNT>install.exe /silent
   /nopleasewait /template=Response file
   ```

   例如：

   ```
   D:\builds\eDirectory\windows\eDirectory\x64\NDSonNT>install.exe /silent /
   nopleasewait /template=D:\builds\eDirectory\windows\x64\NDSonNT\response.ni
   ```

执行无提示配置

1. 创建新的 response.ni 文件或编辑现有的 response 文件。有关 response 文件中的值的详细信息，请参见编辑 response.ni 文件 （第 64 页）。
2. 使用管理员帐户登录到要安装身份库的计算机。
3. 在启用**以管理员身份运行**选项的情况下打开命令提示符。
4. 在命令行中输入以下命令：

   ```
   Windows Drive\Program Files\Common Files\novell>install.exe /silent /
   restrictnoderemove /nopleasewait /template=Response file
   ```

   例如：

   ```
   c:\Program Files\Common Files\novell>install.exe /silent /restrictnoderemove /
   nopleasewait /template=D:\builds\eDirectory\windows\x64\NDSonNT\response.ni
   ```

执行附带配置的无提示安装

在开始之前，请查看有关执行无提示或无人照管安装的先决条件。有关详细信息，请参见第 7.1.2 节 “安装身份库的先决条件和注意事项 ”（第 52 页）。此外，请创建要用作安装模板的 response.ni 文件。

1 创建新的 response.ni 文件或编辑现有的 response 文件。有关 response 文件中的值的详细信息，请参见编辑 response.ni 文件 （第 64 页）。

2 使用管理员帐户登录到要安装身份库的计算机。

3 在启用**以管理员身份运行**选项的情况下打开命令提示符。

4 在命令行中输入以下命令：

```
Unzipped Location\windows\eDirectory\x64\NDSonNT>install.exe /silent /
nopleasewait /template=Response file
```

例如：

```
D:\builds\eDirectory\windows\eDirectory\x64\NDSonNT>install.exe /silent /
nopleasewait /template=D:\builds\eDirectory\windows\x64\NDSonNT\response.ni
```

7.4 安装后配置身份库

安装身份库后，您可能需要针对身份库执行某些配置任务。

7.4.1 将 SecretStore 添加至身份库纲要

必须扩展身份库纲要才能支持 SecretStore 功能。 Identity Applications 需要使用 SecretStore 来连接身份库。

1 要扩展身份库的纲要，请输入以下命令：

```
ice -S SCH -f C:\NetIQ\eDirectory\sssv3.sch -D LDAP -s serverIP -d adminDN
```

例如：

```
ice -S SCH -f C:\NetIQ\eDirectory\sssv3.sch -D LDAP -s 192.168.0.1 -d
cn=admin,o=administrators
```

2 要在 Windows 服务器上配置 SecretStore，请完成以下步骤：

2a 导航到 C:\NetIQ\eDirectory 目录。

2b 输入下面的命令：

```
ssscfg.exe -c
```

2c 指定 SecretStore 的配置设置，然后关闭该实用程序。

2d 运行 NDSCons.exe。

2e 在该实用程序中，为 ssncp.dlm 模块指定 auto。

2f 关闭该实用程序。

有关详细信息，请参见 《*NetIQ eDirectory Administration Guide* (https://www.netiq.com/documentation/edirectory-9/edir_admin/data/bookinfo.html)》（NetIQ eDirectory 管理指南）中的 “SecretStore Configuration for eDirectory Server” （适用于 eDirectory 服务器的 SecretStore 配置）。

7.4.2 在特定的区域设置中配置身份库

要在特定的区域设置中配置身份库，必须先将 LC_ALL 和 LANG 导出到该特定区域设置，然后再执行配置。例如，在 ndsconfig 实用程序中输入以下命令：

```
export LC_ALL=ja
export LANG=ja
```

7.4.3 管理 eDirectory 实例

您可以创建、启动和停止身份库中的服务器实例。还可以查看已配置实例的列表。

列出身份库实例

可以使用 DHost iConsole 来查看配置文件路径、服务器实例的完全判别名和端口，以及指定用户的实例状态 （活动或非活动）。

在身份库中创建新实例

可使用 DHost 实用程序在 eDirectory 中创建新实例。

在身份库中配置和取消配置实例

可使用 DHost 实用程序在身份库中配置和取消配置实例。

针对身份库中的实例调用实用程序

您可以针对某个实例运行 DSTrace 等实用程序。

1 导航到 C:\NetIQ\eDirectory 目录。
2 运行 NDCCons.exe。
3 在 **NetIQ eDirectory 服务**控制台中，导航到 dstrace.dlm。
4 单击**启动**。

在身份库中启动和停止实例

您可以启动或停止您所配置的一个或多个实例。

要启动某个实例，请执行以下操作：

1 导航到 C:\NetIQ\eDirectory 目录。
2 运行 NDCCons.exe。
3 导航到某个实例，然后单击**启动**。

要停止某个实例，请执行以下操作：

1 导航到 C:\NetIQ\eDirectory 目录。

2 运行 NDCCons.exe。

3 导航到某个实例，然后单击**停止**。

8 规划引擎、驱动程序和插件的安装

本章提供了安装身份库所需的先决条件、注意事项以及系统设置。首先，请查阅核对清单，以了解安装过程。

注释：此安装程序还可以安装 Remote Loader。有关详细信息，请参见第 10.2 节 “ 安装 Remote Loader”（第 92 页）。

8.1 Identity Manager 引擎、驱动程序和插件安装核对清单

在开始安装过程之前， NetIQ 建议您先查看以下步骤。

	核对清单项目
❑	1. 了解 Identity Manager 各组件之间的交互。有关详细信息，请参见第 1 章 “Identity Manager 的组件概述 ”（第 19 页）。
❑	2. 确定要为 Identity Manager 组件使用哪些服务器。有关详细信息，请参见第 5.3 节 “ 建议的安装方案和服务器设置 ”（第 39 页）。
❑	3. 查看有关安装 Identity Manager 引擎的注意事项，以确保计算机符合先决条件。有关详细信息，请参见第 8.3 节 “ 安装 Identity Manager 引擎的先决条件和注意事项 ”（第 74 页）。
❑	4. 查看将要托管 Identity Manager 引擎的计算机所要满足的硬件和软件要求。有关详细信息，请参见 iManager 服务器的系统要求 （第 128 页）。
❑	5. 了解在安装 Identity Manager 引擎后，会自动激活哪些驱动程序。有关详细信息，请参见第 8.3.2 节 “ 随 Identity Manager 引擎一起安装驱动程序的注意事项 ”（第 75 页）。
❑	6. 了解安装程序中的选项。有关详细信息，请参见第 8.2 节 “ 了解安装程序 ”（第 74 页）。
❑	7. （视情况而定）有关 Identity Manager 引擎的引导式安装过程 （向导），请参见第 9 节 “ 安装引擎、驱动程序和 iManager 插件 ”（第 77 页）。
❑	8. （视情况而定）要通过一条命令安装组件，请参见第 9.2 节 “ 执行无提示安装 ”（第 78 页）。
❑	9. （视情况而定）要安装 Remote Loader，请参见第 10.2 节 “ 安装 Remote Loader”（第 92 页）。
❑	10. 启动 Remote Loader 中的驱动程序实例。有关详细信息，请参见第 10.3 章 “ 配置 Remote Loader 和驱动程序 ”（第 96 页）。

	核对清单项目
❑	11. 安装其余的 Identity Manager 组件，包括 Identity Applications 和 Identity Reporting。

8.2 了解安装程序

为了方便起见，此安装程序捆绑了多个组件，这些组件提供了 Identity Manager 解决方案的底层框架。您可以选择在同一个服务器上安装所有组件，也可以选择安装在不同的服务器上。有关服务器要求的详细信息，请参见每个组件对应的规划引擎、驱动程序和插件的安装、各驱动程序的指南以及最新的 《发行说明》。

安装程序提供了以下组件安装选项：

Identity Manager 服务器

安装 Identity Manager 引擎、纲要、 NetIQ Audit 代理和 XDAS （分布式审计服务）。

已连接系统服务器 （32 位、 64 位、 .NET）

在加载程序中安装 Remote Loader 服务和驱动程序实例。使用 Remote Loader 可以在不托管身份库和 Identity Manager 引擎的已连接系统上运行 Identity Manager 驱动程序。在安装程序中，您可以选择要在已连接系统上随 Remote Loader 一起安装的驱动程序

扇出代理

安装 JDBC 扇出驱动程序的扇出代理。 JDBC 扇出驱动程序使用扇出代理来创建多个 JDBC 扇出驱动程序实例。扇出代理根据扇出驱动程序中连接对象的配置装载 JDBC 驱动程序实例。有关详细信息，请参见 《NetIQ Identity Manager Driver for JDBC Fan-Out Implementation Guide》（NetIQ Identity Manager Driver for JDBC Fan-Out 实施指南）。

Identity Manager 的 iManager 插件

安装 iManager 插件，这些插件可让您使用 iManager 来管理具有结构化全局配置值 (GCV) 的 Identity Manager 驱动程序。

驱动程序

Identity Manager 驱动程序可在多种目录、数据库和业务应用程序以及身份库之间同步身份信息。您可以将驱动程序配置为单向或双向同步数据。

在安装程序中，您可以选择要随其他组件一起安装的驱动程序。您可能需要在不托管 Identity Manager 引擎的服务器上安装一些驱动程序。在这种情况下，您还需要在该服务器上安装 Remote Loader 服务。

8.3 安装 Identity Manager 引擎的先决条件和注意事项

本节提供了有关安装 Identity Manager 引擎和驱动程序的信息。

- 第 8.3.1 节 “ 安装 Identity Manager 引擎的注意事项 ” （第 75 页）
- 第 8.3.2 节 “ 随 Identity Manager 引擎一起安装驱动程序的注意事项 ” （第 75 页）

8.3.1 安装 Identity Manager 引擎的注意事项

在安装 Identity Manager 引擎之前，请先查看以下注意事项：

- 在安装 Identity Manager 引擎之前，必须先安装身份库。此外，身份库还必须包含至少带有一个组织单位、一个用户和一个 iManager 服务器的树。
- 在托管身份库的同一个服务器上安装 Identity Manager 引擎。安装程序将会根据身份库的版本安装 32 位或 64 位 Identity Manager。
- （视情况而定）要在 Identity Manager 引擎所在的同一台计算机上安装 Remote Loader，请确保选择同时支持这两个组件的操作系统。有关 Remote Loader 系统要求的详细信息，请参见第 10.1.6 节 " 安装 Remote Loader 的先决条件和注意事项 "（第 88 页）。

8.3.2 随 Identity Manager 引擎一起安装驱动程序的注意事项

会影响安装了 Identity Manager 引擎的服务器的性能的变数有很多，其中就包括服务器上运行的驱动程序数目。在规划驱动程序的安装位置时， NetIQ 提供了以下建议供您参考：

- 一般而言，服务器上运行的驱动程序数目取决于驱动程序对服务器施加的负载。有些驱动程序需要处理大量的对象，而有些驱动程序则不然。
- 如果您计划使用每个驱动程序同步数百万个对象，请限制服务器上的驱动程序数目。例如，只部署不超过 10 个的 此类驱动程序。
- 如果您计划使用每个驱动程序同步 100 个或更少的对象，则也许能够在服务器上运行 10 个以上的驱动程序。
- 要创建服务器性能基准以帮助确定最佳驱动程序数目，可以使用 iManager 中的运行状况监视工具。有关运行状况监视工具的详细信息，请参见《*NetIQ Identity Manager Driver Administration Guide*》（NetIQ Identity Manager 驱动程序管理指南）中的 "Monitoring Driver Health"（监视驱动程序的运行状况）。

有关在安装后激活 Identity Manager 驱动程序的详细信息，请参见第 30.6 节 " 激活 Identity Manager"（第 310 页）。

8.4 Identity Manager 引擎的系统要求

本节提供要安装 Identity Manager 引擎的服务器的最低要求。请务必查看安装的先决条件和注意事项，特别是与操作系统有关的内容。

类别	要求
处理器	1 GHz
磁盘空间	◆ 300 MB ◆ 每 50,000 个用户需要 150 MB 的额外磁盘空间
内存	◆ Identity Manager 引擎需要 2 GB ◆ Identity Manager 驱动程序需要 2 MB

类别	要求
操作系统 （经认可）	以下 64 位操作系统之一： ◆ Windows Server 2016 ◆ Windows Server 2012 R2 ◆ Windows Server 2012 NetIQ 建议您在安装 Identity Manager 之前，按照制造商的自动更新工具应用最新的操作系统增补程序。 **注释：***经认可*指操作系统已经过全面测试且受支持。
操作系统 （受支持）	经认可操作系统的最新版服务包 **注释：***受支持*指操作系统尚未经过测试，但预期可以正常工作。
虚拟化系统	◆ Hyper-V Server 2012 R2 ◆ VMWare ESX 5.0 及更高版本 ◆ 包含 Hyper-V 的 Windows Server 2012 R2 Virtualization （受支持） NetIQ 支持在为运行 NetIQ 产品的操作系统提供官方支持的企业级虚拟化系统上安装 Identity Manager。只要虚拟化系统的供应商为这些操作系统提供官方支持， NetIQ 就可支持这些系统上的整个 Identity Manager 堆栈。
其他软件	◆ NetIQ eDirectory 9.1 ◆ iManager 3.1

9 安装引擎、驱动程序和 iManager 插件

本章介绍了 Identity Manager 引擎、驱动程序、 iManager 插件和 Remote Loader 的安装过程。您可以在同一个服务器上安装这些程序，也可以在不同的服务器上安装。例如，您可能要在某个已连接的系统上安装驱动程序，而不想在 Identity Manager 引擎所在的同一个服务器上安装该驱动程序。在此情况下，您还要在这个已连接的服务器上安装 Remote Loader。

NetIQ 提供了引导式安装过程和无提示安装两种安装模式。

9.1 使用向导安装组件

安装程序将引导您完成 Identity Manager 引擎的配置设置。安装程序会自动默认为向导模式。

要准备安装，请参见第 8.1 节 "Identity Manager 引擎、驱动程序和插件安装核对清单 "（第 73 页）。另请参见版本随附的 《发行说明》。要执行无人照管安装，请参见第 9.2 节 " 执行无提示安装 "（第 78 页）。

注释：是要以管理员还是非管理员用户身份执行安装，应根据您安装身份库时所用的方法而定。

9.1.1 以管理用户身份安装

本节介绍了以管理用户身份使用安装向导来安装 Identity Manager 引擎的引导式过程。安装程序的路径为 \products\idm\windows\setup\idm_install.exe。

要以管理用户身份安装 Identity Manager 引擎，请执行以下操作：

1. 在要安装 Identity Manager 引擎的计算机上以管理员身份登录。
2. 在包含安装文件的目录中，找到并运行 idm_install.exe。
3. 接受许可协议，然后单击**下一步**。
4. 在 " 选择组件 " 窗口中，指定要安装的组件。

   有关选项的详细信息，请参见第 8.2 节 " 了解安装程序 "（第 74 页）。
5. （可选）要为单个组件选择特定的驱动程序，请完成以下步骤：
   - **5a** 单击**自定义选择的组件**，然后单击**下一步**。
   - **5b** 展开要安装的组件下面的**驱动程序**。
   - **5c** 选择要安装的驱动程序。
6. 单击**下一步**。

7 在 " 激活通知 " 窗口中，单击**确定**。有关详细信息，请参见第 30.6 节 " 激活 Identity Manager"（第 310 页）。

8 对于 " 鉴定 "，请指定 eDirectory 中具有扩展纲要的足够权限的用户帐户及其口令。以 LDAP 格式指定用户名。例如：cn=admin,o=company。

9 在 " 预安装摘要 " 中检查设置。

10 单击**安装**。

11 激活 Identity Manager。有关详细信息，请参见第 30.6 节 " 激活 Identity Manager"（第 310 页）。

12 要创建和配置驱动程序对象，请查阅该驱动程序的特定指南。有关详细信息，请参见 Identity Manager 驱动程序文档网站。

13 （可选）有关默认安装位置，请参见安装日志。例如 C:\Users\Admin1\AppData\Local\Temp\1\idmInstall.log。

9.2 执行无提示安装

要运行 Identity Manager 的无提示安装，请创建包含完成安装所需参数的 properties 文件。 Identity Manager 媒体包含一个示例属性文件，其路径为 \products\idm\windows\setup\silent.properties。

要执行无提示安装，请执行以下操作：

1 在安装目录中，创建一个 properties 文件或编辑示例 silent.properties 文件。

2 使用文本编辑器在该文件中指定以下参数：

EDITION_INPUT_RESULTS

指定 Identity Manager 服务器的版本。例如， Advanced Edition 或 Standard Edition。安装程序会使用此信息配置指定的 Identity Manager 版本。

EDIR_USER_NAME

指定身份库的管理员帐户的 LDAP 判别名。例如：c=admin,o=netiq。安装程序使用此帐户将 Identity Manager 引擎连接到身份库。

您可能需要将此参数添加到示例 silent.properties 文件中。

EDIR_USER_PASSWORD

指定身份库的管理员帐户的口令。例如：netiq123。您可能需要将此参数添加到示例 silent.properties 文件中。

如果不想在文件中包含口令值，请将该字段留空。这样，安装程序就会从 EDIR_USER_PASSWORD 环境变量中读取该值。请确保指定了 EDIR_USER_PASSWORD 的环境变量。

METADIRECTORY_SERVER_SELECTED

指定是否要安装 Identity Manager 服务器和驱动程序。

CONNECTED_SYSTEM_SELECTED

指定是否要安装 32 位 Remote Loader 服务和驱动程序。可以在同一个服务器上同时安装 32 位和 64 位版本。

FANOUTAGENT_SELECTED

指定是否要安装 JDBC 驱动程序的扇出代理。

X64_CONNECTED_SYSTEM_SELECTED

指定是否要安装 64 位 Remote Loader 服务和驱动程序。可以在同一个服务器上同时安装 32 位和 64 位版本。

WEB_ADMIN_SELECTED

当您先前已安装 iManager 时适用。

指定是否要安装 iManager 插件。

UTLITIES_SELECTED

指定是否要安装实用程序和 Remote Loader 的系统组件。

DOT_NET_REMOTELOADER_SELECTED

指定是否要在 Windows 服务器上安装 .NET Remote Loader 服务和驱动程序。

EDIR_NDS_CONF

指定身份库配置文件的路径。

如果拥有多个身份库实例，请为每个实例指定相应值。

EDIR_IP_ADDRESS

指定身份库的 IP 地址。

如果拥有多个身份库实例，请为每个实例指定该地址。

EDIR_NCP_PORT

指定身份库的端口号。

如果拥有多个身份库实例，请为每个实例指定端口。

3 要运行无提示安装，请从 properties 文件所在的目录发出以下命令：install.exe -i silent -f *文件名*.properties

4 （可选）有关默认安装位置，请参见安装日志。例如 C:\Users\Admin1\AppData\Local\Temp\1\idmInstall.log。

9.3 在具有多个身份库实例的服务器上安装

Identity Manager 支持以管理用户身份在无提示模式下执行此安装。此过程需要您为要安装 Identity Manager 的每个身份库实例创建一个 silent.properties 文件。

要在无提示模式下安装 Identity Manager，请执行以下步骤：

1 查看第 8 章 " 规划引擎、驱动程序和插件的安装 "（第 73 页）中的先决条件和系统要求。

2 按照第 9.2 节 " 执行无提示安装 "（第 78 页）中的说明操作。

   2a 确保 silent.properties 文件包含以下设置：

```
EDITION_INPUT_RESULTS=Advanced Edition
EDIR_USER_NAME=cn=admin_name,o=organization_name
EDIR_USER_PASSWORD=identity_vault_password
METADIRECTORY_SERVER_SELECTED=true
CONNECTED_SYSTEM_SELECTED=false
X64_CONNECTED_SYSTEM_SELECTED=false
WEB_ADMIN_SELECTED=false
UTILITIES_SELECTED=false
FANOUTAGENT_SELECTED=false
EDIR_NCP_PORT=<ncp_port>
EDIR_NDS_CONF=</path/to/edir/conf>
EDIR_IP_ADDRESS=ip_address_for_identity_vault

# For Customization use the following properties
CUSTOM_SELECTED=true
# engine custom list engine and drivers jdbc and delim
CHOSEN_INSTALL_FEATURE_LIST_SERVER=ENGINE,JDBC,DELIM,additional_value
```

2b 您可以包括以下额外的值以自定义引擎列表：

- Server_DRIVERS
- AD
- EBSHR
- EBSTCA
- EBSUM
- DELIM
- EDIR
- BIEDIR
- JDBC
- JMS
- LDAP
- NXSET
- NOTES
- PS
- REMEDY
- SAPUMJ
- SAPHR
- SAPBL
- SAPPORTAL
- SOAP
- REST
- SFORCE
- SENTREST
- BLACK
- BANNER
- GOOGLE
- AR

- NPUM
- TSS
- RACF
- AFC2
- UAD
- RRSD

3 （视情况而定）要校验安装是否成功，请在安装日志文件中找到下面几行。例如 C:\Users\Admin1\AppData\Local\Temp\1\idmInstall.log 文件。

```
NDS schema extension complete.
exitValue=0
Schema extended
SCHEMA_EXTENDED=true
==== UpdateIDMConfigureStatus ==============================
stateFile: C:\IDM\Uninstall_Identity_Manager\idmconfigure_state.conf
INSTALL_SUCCESS: SUCCESS
enter loop:
==== Complete ==============================================
INSTALL_SUCCESS=SUCCESS
```

9.4 停止和启动 Identity Manager 驱动程序

您可能需要启动或停止 Identity Manager 驱动程序，以确保安装或升级过程能够修改或替换正确的文件。本节介绍了以下活动：

- 第 9.4.1 节 " 停止驱动程序 " （第 81 页）
- 第 9.4.2 节 " 启动驱动程序 " （第 82 页）

9.4.1 停止驱动程序

在修改驱动程序的任何文件之前，必须先停止驱动程序。

- 使用 Designer 停止驱动程序 （第 81 页）
- 使用 iManager 停止驱动程序 （第 82 页）

使用 Designer 停止驱动程序

1 在 Designer 中，在**大纲**选项卡中选择身份库 对象。

2 在建模器工具栏中，单击**停止所有驱动程序**图标 。

这将停止属于该项目的所有驱动程序。

3 将驱动程序设置为手动启动，以确保在升级过程完成前，驱动程序不会启动：

3a 双击**大纲**选项卡中的驱动程序图标 。

3b 选择**驱动程序配置 > 启动选项**。

3c 单击**手动**，然后单击**确定**。

3d 对每个驱动程序重复步骤 3a 到步骤 3c。

使用 iManager 停止驱动程序

1 在 iManager 中，选择 **Identity Manager > Identity Manager 概述**。
2 浏览到并选择树中要搜索驱动程序集对象的位置，然后单击搜索图标 ▶。
3 单击驱动程序集对象。
4 单击**驱动程序 > 停止所有驱动程序**。
5 对每个驱动程序集对象重复步骤 2 到步骤 4。
6 将驱动程序设置为手动启动，以确保在升级过程完成前，驱动程序不会启动：
   6a 在 iManager 中，选择 **Identity Manager > Identity Manager 概述**。
   6b 浏览到并选择树中要搜索驱动程序集对象的位置，然后单击搜索图标 ▶。
   6c 单击驱动程序集对象。
   6d 在驱动程序图标右上角，单击**编辑属性**。
   6e 在 " 驱动程序配置 " 页中的**启动选项**下选择**手动**，然后单击**确定**。
   6f 对树中的每个驱动程序重复步骤 6a 到步骤 6e。

9.4.2 启动驱动程序

更新所有 Identity Manager 组件后，重启动驱动程序。 NetIQ 建议在运行驱动程序后对其进行测试，以校验所有策略是否仍然有效。

- 使用 Designer 启动驱动程序 （第 82 页）
- 使用 iManager 启动驱动程序 （第 82 页）

使用 Designer 启动驱动程序

1 在 Designer 中，在**大纲**选项卡中选择身份库 对象。
2 在建模器工具栏中单击**启动所有驱动程序**图标 。这将启动项目中的所有驱动程序。
3 设置驱动程序启动选项：
   3a 双击**大纲**选项卡中的驱动程序图标 。
   3b 选择**驱动程序配置 > 启动选项**。
   3c 选择**自动启动**或选择启动驱动程序的首选方法，然后单击**确定**。
   3d 对每个驱动程序重复步骤 3a 到步骤 3c。
4 测试驱动程序以验证策略是否按照设计运行。有关如何测试您的策略的信息，请参见 《*NetIQ Identity Manager - Using Designer to Create Policies*》（NetIQ Identity Manager - 使用 Designer 创建策略）中的 "Testing Policies with the Policy Simulator" （使用策略模拟器测试策略）。

使用 iManager 启动驱动程序

1 在 iManager 中，选择 **Identity Manager > Identity Manager 概述**。
2 浏览到并选择树中要搜索驱动程序集对象的位置，然后单击搜索图标 ▶。
3 单击驱动程序集对象。
4 单击**驱动程序 > 启动所有驱动程序**可同时启动所有驱动程序。

或

在驱动程序图标的右上角，单击**启动驱动程序**可单独启动每个驱动程序。

5 如果有多个驱动程序，请重复步骤 2 到步骤 4。

6 设置驱动程序启动选项：

   6a 在 iManager 中，选择 **Identity Manager > Identity Manager 概述**。

   6b 浏览到并选择树中要搜索驱动程序集对象的位置，然后单击搜索图标 ▸。

   6c 单击驱动程序集对象。

   6d 在驱动程序图标右上角，单击**编辑属性**。

   6e 在 " 驱动程序配置 " 页中的**启动选项**下，选择**自动启动**，或选择启动驱动程序的首选方法，然后单击**确定**。

   6f 对每个驱动程序重复步骤 6b 到步骤 6e。

7 测试驱动程序以验证策略是否按照设计运行。

iManager 中没有任何策略模拟器。要测试策略，请触发使策略能够执行的事件。例如，创建用户、修改用户或删除用户。

10 安装和管理 Remote Loader

本章介绍了如何安装 Remote Loader、.NET Remote Loader 或 Java Remote Loader，以及在加载程序中配置驱动程序实例。

Identity Manager 引擎中捆绑提供了 Remote Loader 安装程序。这些文件位于 Identity Manager 安装包的 \products\idm 目录中。默认情况下，安装程序将在 C:\Netiq 中安装组件。

NetIQ 建议您在开始之前，先查看安装过程。有关详细信息，请参见第 10.1.1 节 “Remote Loader 安装核对清单 ”（第 85 页）。

10.1 规划安装 Remote Loader

本节提供的信息可帮助您为安装 .NET Remote Loader 做好准备。

10.1.1 Remote Loader 安装核对清单

NetIQ 建议您完成以下核对清单中的步骤：

	核对清单项目
❑	1. 了解 Identity Manager 各组件之间的交互。有关详细信息，请参见第 1 章 “Identity Manager 的组件概述 ”（第 19 页）。
❑	2. 确定要为 Identity Manager 组件使用哪些服务器。有关详细信息，请参见第 5.3 节 “ 建议的安装方案和服务器设置 ”（第 39 页）。
❑	3. 确保已安装 Identity Manager 引擎。有关详细信息，请参见第 9 章 “ 安装引擎、驱动程序和 iManager 插件 ”（第 77 页）
❑	4. 查看安装 Remote Loader 的注意事项，以确保计算机符合先决条件。有关详细信息，请参见第 10.1.6 节 “ 安装 Remote Loader 的先决条件和注意事项 ”（第 88 页）。
❑	5. 查看将要托管 Remote Loader 的计算机所要满足的硬件和软件要求。有关详细信息，请参见第 10.1.7 节 “Remote Loader 的系统要求 ”（第 90 页）。

	核对清单项目
❑	6. （视情况而定）要在未托管 Identity Manager 引擎的服务器上安装 Remote Loader，请确保您能够与该引擎建立安全连接。有关详细信息，请参见第 10.3.1 节 " 创建与 Identity Manager 引擎的安全连接 "（第 97 页）。
❑	7. 确定是要安装 32 位还是 64 位版本的 Remote Loader。有关详细信息，请参见第 10.1.5 节 " 在同一台计算机上使用 32 位和 64 位 Remote Loader"（第 88 页）。
❑	8. 要安装 Remote Loader，请执行以下操作： ◆ 要执行引导式安装，请参见第 10.2.1 节 " 使用向导安装 Remote Loader"（第 92 页）。 ◆ 要执行无提示安装，请参见第 10.2.5 节 " 执行 Remote Loader 的无提示安装 "（第 96 页）。
❑	9. （视情况而定）要安装 .NET Remote Loader，请参见第 10.2.4 节 " 安装 .NET Remote Loader"（第 95 页）。
❑	10. 查看用于配置驱动程序实例的参数。有关详细信息，请参见第 10.3.2 节 " 了解 Remote Loader 的配置参数 "（第 99 页）。
❑	11. 要配置 Remote Loader 中的驱动程序实例，请参见以下章节之一： ◆ 第 10.3.3 节 " 为驱动程序实例配置 Remote Loader"（第 107 页） ◆ 第 10.3.4 节 " 为驱动程序实例配置 Java Remote Loader"（第 110 页） ◆ 第 10.3.5 节 " 为驱动程序实例配置 .NET Remote Loader"（第 111 页）
❑	12. 准备 Remote Loader 的驱动程序。有关详细信息，请参见第 10.3.6 节 " 配置 Identity Manager 驱动程序以与 Remote Loader 配合使用 "（第 113 页）。
❑	13. 启动 Remote Loader 中的驱动程序实例。有关详细信息，请参见第 10.4.1 节 " 启动 Remote Loader 中的驱动程序实例 "（第 123 页）。
❑	14. （视情况而定）要配置 Remote Loader 与 Identity Manager 引擎间的相互鉴定，请参见第 10.3.7 节 " 配置与 Identity Manager 引擎的相互鉴定 "（第 114 页）。
❑	15. 校验 Remote Loader 和驱动程序是否可与 Identity Manager 引擎和已连接系统通讯。有关详细信息，请参见第 10.3.8 节 " 校验配置 "（第 122 页）。
❑	16. 安装其余的 Identity Manager 组件，包括 Identity Applications 和 Identity Reporting。

10.1.2 了解 Remote Loader

使用 Remote Loader 可以在不托管身份库和 Identity Manager 引擎的已连接系统上运行 Identity Manager 驱动程序。 .Net Remote Loader 只在基于 Windows 的系统上工作。

Remote Loader 可以通过 JNI 托管平台特定文件中包含的 Identity Manager 应用程序 shim，并且还可以托管与平台无关的 JAR 文件中包含的更常见 Identity Manager 应用程序 shim。 Remote Loader 可以在任何平台上运行。但是，特定于平台的 shim 必须在其本机平台上运行。

了解 Shim

Remote Loader 使用 shim 来与受管系统上的应用程序通讯。 *shim* 是一个或多个包含代码的文件，这些代码用于处理在身份库与应用程序之间同步的事件。在使用 Remote Loader 之前，必须将应用程序 shim 配置为安全连接到 Identity Manager 引擎。此外，还必须配置 Remote Loader 和 Identity Manager 驱动程序。

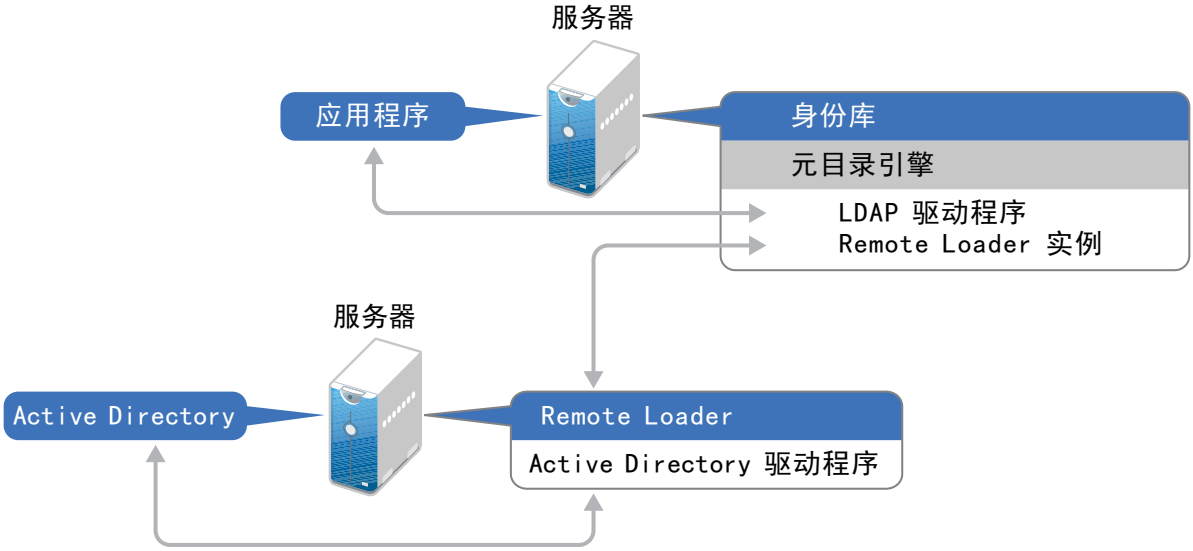
有关详细信息，请参见第 10.3 章 " 配置 Remote Loader 和驱动程序 " （第 96 页）。

确定何时使用 Remote Loader

可以在同一个服务器上安装 Identity Manager 引擎、身份库和驱动程序 shim。 Identity Manager 引擎作为 eDirectory 进程的一部分运行。 Identity Manager 驱动程序可以在装有 Identity Manager 的服务器上运行。它们也可以作为与 Identity Manager 引擎所属的同一进程的一部分运行。但是，对于以下情况，您可能希望 Identity Manager 驱动程序在托管 Identity Manager 引擎的服务器上作为单独的进程运行。

- 防止因驱动程序 shim 发生任何异常而使身份库受到影响。
- 通过将驱动程序命令卸载到远程应用程序或数据库，来提高运行 Identity Manager 引擎的服务器的性能。
- 在未托管 Identity Manager 引擎的服务器上运行更多的驱动程序。

针对这些情况， Remote Loader 在 Identity Manager 引擎与驱动程序之间提供了一个通讯通道。例如，您在 Identity Manager 引擎和身份库所在的同一个服务器上安装了 LDAP 驱动程序。然后，在装有 Remote Loader 的另一个服务器上安装了 Active Directory (AD) 驱动程序。要使这些驱动程序能够访问应用程序并与身份库通讯，请按下图中所示，在两个服务器上都安装 Remote Loader：



NetIQ 建议您尽可能地配合您的驱动程序使用 Remote Loader 配置。即使是应用程序位于 Identity Manager 引擎所在的同一个服务器上，也要使用 Remote Loader。

10.1.3 了解 Java Remote Loader

Java Remote Loader 是一个 Java 应用程序。您可以将 Java Remote Loader 与任何公开支持的 Java 版本搭配使用。

要配置驱动程序的 Java Remote Loader，请参见第 10.3.4 节 " 为驱动程序实例配置 Java Remote Loader"（第 110 页）。

10.1.4 了解安装程序

为了方便起见，此安装程序捆绑了多个组件，这些组件提供了 Identity Manager 解决方案的底层框架。您可以选择在同一个服务器上安装所有组件，也可以选择安装在不同的服务器上。除了 Remote Loader 以外，您还可以选择要在连接的系统上安装的驱动程序。此安装包提供适用于 Windows 操作系统的 .NET Remote Loader 选项。

10.1.5 在同一台计算机上使用 32 位和 64 位 Remote Loader

默认情况下，安装程序会检测操作系统的版本，然后安装相应版本的 Remote Loader。您可以在 64 位操作系统上同时安装 32 位和 64 位 Remote Loader：

- 如果要升级 64 位操作系统上安装的 32 位 Remote Loader，升级过程会将 32 位 Remote Loader 升级到最新版本，同时安装 64 位 Remote Loader。
- 如果选择在同一台计算机上同时安装 32 位和 64 位 Remote Loader，只会使用 64 位 Remote Loader 生成审计事件。如果在安装 32 位 Remote Loader 前已安装 64 位 Remote Loader，则事件将记录到 32 位超速缓存。

10.1.6 安装 Remote Loader 的先决条件和注意事项

在安装 Remote Loader 之前， NetIQ 建议您先查看以下注意事项：

- 在可与受管系统通讯的服务器上安装 Remote Loader。必须能够通过相关的 API 访问每个受管系统的驱动程序。
- 您可以在装有 Identity Manager 引擎的同一台计算机上安装 Remote Loader。
- 您可以在同一台计算机上同时安装 32 位和 64 位 Remote Loader。
- 您可以在不支持本机 Remote Loader 的平台上安装 Java Remote Loader。有关受支持平台的详细信息，请参见第 10.1.7 节 "Remote Loader 的系统要求 "（第 90 页）。
- （视情况而定）要将 Identity Manager 连接到 Active Directory，必须在充当成员服务器或域控制器的服务器上安装 Remote Loader 和 Active Directory 驱动程序。不需要在连接的系统所在的同一个服务器上安装 eDirectory 和 Identity Manager。Remote Loader 会将来自 Active Directory 的所有事件都发送到 Identity Manager 服务器。然后， Remote Loader 会接收来自 Identity Manager 服务器的任何信息，并将其传递给已连接的应用程序。
- NetIQ 建议您尽可能地对于驱动程序使用 Remote Loader 配置。即使是已连接系统位于 Identity Manager 服务器引擎所在的同一个服务器上，也要使用 Remote Loader。

  运行 Remote Loader 配置中的驱动程序 shim 具备以下优势：

  - 在驱动程序 shim 之间实现内存与处理隔离，从而改善性能并能更好地监视 Identity Manager 解决方案。

    - 增补和升级驱动程序 shim 时不会影响 eDirectory 或其他驱动程序。
    - 保护 eDirectory 使其免受驱动程序 shim 中可能发生的致命错误的影响。
    - 将驱动程序 shim 的负载分散到其他服务器。
- 以下驱动程序支持 Remote Loader 功能：
    - Active Directory
    - Access Review
    - ACF2
    - Azure Active Directory
    - 标题页
    - Blackboard
    - 数据收集服务
    - Delimited Text
    - GoogleApps
    - REST
    - GroupWise 2014 （适用于 32 位 Remote Loader）
    - JDBC
    - JMS
    - LDAP
    - Linux 设置
    - Lotus Notes
    - 受管系统网关
    - 手动任务服务
    - Null and Loopback
    - Office 365
    - Oracle EBS HRMS
    - Oracle EBS TCA
    - Oracle EBS User Management
    - PeopleSoft 5.2
    - Privileged User Management
    - Remedy
    - SalesForce.com
    - SAP 业务逻辑
    - SAP 门户
    - SAP HR （不受 Java Remote Loader 的支持）
    - SAP User Management （不受 Java Remote Loader 的支持）
    - ServiceNow
    - Integration Module V2.0 for Sentinel
    - SharePoint
    - SOAP

    - 绝密
    - WorkOrder
- 以下驱动程序不支持 Remote Loader：
    - Bidirectional eDirectory
    - eDirectory
    - 权利服务
    - 角色服务
    - User Application

有关 Identity Manager Remote Loader 的详细信息，请参见 "The Many Faces of Remote Loader in Identity Manager"（Identity Manager 中的 Remote Loader 面面观）。

10.1.7 Remote Loader 的系统要求

本节提供要安装 Remote Loader、 .NET Remote Loader 和 Java Remote Loader 的服务器的最低要求。

Remote Loader 32 位和 64 位

类别	要求
处理器	1 GHz 处理器
内存	512 MB
操作系统 （经认可）	以下 64 位操作系统之一： ◆ Windows Server 2016 ◆ Windows Server 2012 R2 ◆ Windows Server 2012 ◆ Windows Server 2008 R2 对于 32 位操作系统： ◆ Windows Server 2008 SP2 **重要：**Lotus Notes Client 仅受工作站平台的支持。在 Windows XP、 Windows 7 和 8 以及 SLED 32 位上运行的 Remote Loader 仅支持用于 Lotus Notes 驱动程序集成。在常规 Identity Manager 安装中，Remote Loader 仅受服务器平台的支持。 NetIQ 建议您在安装 Identity Manager 之前，按照制造商的自动更新工具应用最新的操作系统增补程序。 **注释：***经认可*指操作系统已经过全面测试且受支持。
操作系统 （受支持）	经认可操作系统的最新版服务包 **注释：***受支持*指操作系统尚未经过测试，但预期可以正常工作。

类别	要求
虚拟化系统	◆ Hyper-V Server 2012 R2 ◆ VMWare ESX 5.0 及更高版本 ◆ 包含 Hyper-V 的 Windows Server 2012 R2 Virtualization （受支持） NetIQ 支持在为运行 NetIQ 产品的操作系统提供官方支持的企业级虚拟化系统上安装 Identity Manager。只要虚拟化系统的供应商为这些操作系统提供官方支持， NetIQ 就可支持这些系统上的整个 Identity Manager 堆栈。

.NET Remote Loader

.NET Remote Loader 专用于与基于 Windows 的服务器搭配使用。

类别	要求
处理器	Pentium* III 600MHz 处理器
内存	512 MB
操作系统 （经认可）	以下 64 位操作系统之一： ◆ Windows Server 2016 ◆ Windows Server 2012 R2 ◆ Windows Server 2012 ◆ Windows Server 2008 R2 对于 32 位操作系统： ◆ Windows Server 2008 SP2 NetIQ 建议您在安装 Identity Manager 之前，按照制造商的自动更新工具应用最新的操作系统增补程序。 **注释：***经认可*指操作系统已经过全面测试且受支持。
操作系统 （受支持）	经认可操作系统的最新版服务包 **注释：***受支持*指操作系统尚未经过测试，但预期可以正常工作。
虚拟化系统	◆ Hyper-V Server 2012 R2 ◆ VMWare ESX 5.5 ◆ 包含 Hyper-V 的 Windows Server 2012 R2 Virtualization （受支持） NetIQ 支持在为运行 NetIQ 产品的操作系统提供官方支持的企业级虚拟化系统上安装 Identity Manager。只要虚拟化系统的供应商为这些操作系统提供官方支持， NetIQ 就可支持这些系统上的整个 Identity Manager 堆栈。
.NET Framework	4.x

Java Remote Loader

Java Remote Loader 可以在装有兼容 JRE 和 Java Sockets 的任何已连接系统上运行。

类别	要求
处理器	Pentium* III 600MHz （最低要求）
内存	Remote Loader 需要 512 MB
JRE	Java8u162 （最低要求） **注释：**您可以将 Java Remote Loader 与任何公开支持的 Java 版本搭配使用。
平台代理	PA v2011.1r6

10.2 安装 Remote Loader

Remote Loader 控制台使用 rlconsole.exe 与 dirxml_remote.exe 交互，后者是一个可执行文件，可让 Identity Manager 引擎服务器与运行的 Identity Manager 驱动程序通讯。

- 第 10.2.1 节 “ 使用向导安装 Remote Loader” （第 92 页）
- 第 10.2.2 节 “ 执行 Remote Loader 的无提示安装 ” （第 93 页）
- 第 10.2.3 节 “ 安装 Java Remote Loader” （第 94 页）
- 第 10.2.4 节 “ 安装 .NET Remote Loader” （第 95 页）
- 第 10.2.5 节 “ 执行 Remote Loader 的无提示安装 ” （第 96 页）

10.2.1 使用向导安装 Remote Loader

安装程序将引导您完成 Remote Loader 的配置设置。本节介绍了使用安装向导安装 Remote Loader 的引导式过程。安装程序位于 \products\idm\windows\setup\ 目录中。

要准备安装，请参见第 10.1.1 节 “Remote Loader 安装核对清单 ” （第 85 页）。另请参见版本随附的《发行说明》。要执行无人照管安装，请参见第 9.2 节 “ 执行无提示安装 ” （第 78 页）。

注释：是要以管理员还是非管理员用户身份执行安装，应根据您安装身份库时所用的方法而定。

安装 Remote Loader：

1. 登录要安装 Remote Loader 的计算机。

   注释：您可以使用非管理员用户身份安装 Java Remote Loader。

2. 导航到 \products\idm\windows\setup\ 目录。
3. 运行 idm_install.exe 程序。
4. 接受许可协议，然后单击下一步。
5. 在选择组件窗口中，指定要安装的 Remote Loader 组件。

   有关选项的详细信息，请参见第 8.2 节 “ 了解安装程序 ” （第 74 页）。

6 （可选）要为单个组件选择特定的驱动程序，请完成以下步骤：

   6a 单击自定义选择的组件，然后单击下一步。

   6b 展开要安装的组件下面的驱动程序。

   6c 选择要安装的驱动程序。

7 单击下一步。

8 在激活通知窗口中，单击确定。

9 对于 " 鉴定 "，请指定 eDirectory 中具有扩展纲要的足够权限的用户帐户及其口令。以 LDAP 格式指定用户名。例如：cn=admin,o=company。

10 在 " 预安装摘要 " 中检查设置。

11 单击安装。

12 激活 Identity Manager。有关更多信息，请参见第 30.6 节 " 激活 Identity Manager"（第 310 页）。

13 配置 Remote Loader 以便与驱动程序和 Identity Manager 连接。有关详细信息，请参见第 10.3 章 " 配置 Remote Loader 和驱动程序 "（第 96 页）。

14 要创建和配置驱动程序对象，请查阅该驱动程序的特定指南。有关详细信息，请参见 Identity Manager 驱动程序文档网站。

15 （可选）有关默认安装位置，请参见安装日志文件。例如 C:\Users\Admin1\AppData\Local\Temp\1\idmInstall.log。

10.2.2 执行 Remote Loader 的无提示安装

要运行 Remote Loader 的无提示安装，请创建包含完成安装所需参数的 properties 文件。 Identity Manager 媒体中包含一个示例 properties 文件。默认情况下，该示例属性文件位于 \products\idm\windows\setup\ 目录中。

要执行无提示安装，请执行以下操作：

1 登录要安装 Remote Loader 的计算机。

2 导航到 \products\idm\windows\setup\ 目录。

3 创建一个 properties 文件或编辑示例 silent.properties 文件。

4 在该文件中指定以下参数：

   CONNECTED_SYSTEM_SELECTED

   指定是否要安装 32 位 Remote Loader 服务和驱动程序。可以在同一个服务器上同时安装 32 位和 64 位版本。

   X64_CONNECTED_SYSTEM_SELECTED

   指定是否要安装 64 位 Remote Loader 服务和驱动程序。可以在同一个服务器上同时安装 32 位和 64 位版本。

   UTLITIES_SELECTED

   指定是否要安装实用程序和 Remote Loader 的系统组件。

   DOT_NET_REMOTELOADER_SELECTED

   指定是否要安装 .NET Remote Loader 服务和驱动程序。

5 要执行无提示安装，请从命令提示符运行以下命令：

   install.exe -i silent -f *文件名* .properties

10.2.3 安装 Java Remote Loader

Identity Manager 使用 Java Remote Loader 在运行于一台服务器上的 Identity Manager 引擎与运行于另一位置 （该位置未运行 rdxml）的 Identity Manager 驱动程序之间交换数据。您可以在装有兼容 JRE （最低为 1.8.0）和 Java 套接字的任何受支持 Windows 平台上安装 Java Remote Loader - dirxml_jremote。

1 在托管 Identity Manager 引擎的服务器上，复制位于默认位置的应用程序 Shim .iso 或 .jar 文件。例如， C:\NetIQ\idm\NDS\lib 目录。

2 登录到要安装 Java Remote Loader 的计算机 （目标计算机）。

3 校验目标计算机是否装有受支持版本的 JRE。

4 要访问安装程序，请完成以下步骤之一：

   4a （视情况而定）如果您已获取 Identity Manager 安装包的 .iso 映像文件，请导航到包含 Java Remote Loader 安装文件的目录 （默认为 products\idm\java_remoteloader）。

   4b （视情况而定）如果您已从 NetIQ 下载网站下载了 Java Remote Loader 安装文件，请完成以下步骤：

   4b1 浏览到所下载映像的 .tgz 文件。

   4b2 将该文件的内容解压缩到本地计算机上的某个文件夹中。

5 将 dirxml_jremote_dev.tar.gz 文件复制到目标计算机上的所需位置。例如，将该文件复制到 C:\NetIQ\idm。

6 将以下文件之一复制到目标计算机上的所需位置：

   - dirxml_jremote.tar.gz
   - dirxml_jremote_mvs.tar

   有关 mvs 的信息，请解压缩 dirxml_jremote_mvs.tar 文件，然后参见 usage.html 文档。

7 在目标计算机上，解压缩 .tar.gz 文件。

   例如，使用 7-Zip 或支持的软件解压缩 .tar.gz 文件。

8 将 CLASSPATH 环境变量设置到存在于 lib 文件夹中的所有 jar。如果您有特定于任何驱动程序的依赖 jar，请将这些 jar 文件复制到 lib 文件夹，然后也将 CLASSPATH 环境变量设置到这些 jar。

   例如，进行如下设置：

```
CLASSPATH=E:\RL\JAVARL\lib\activation.jar;E:\RL\JAVARL\lib\commondrivershim.ja
r;E:\RL\JAVARL\lib\delimitedtextshim.jar;E:\RL\JAVARL\lib\delimitedtextutil.ja
r;E:\RL\JAVARL\lib\dirxml.jar;E:\RL\JAVARL\lib\dirxml_misc.jar;E:\RL\JAVARL\li
b\dirxml_remote.jar;E:\RL\JAVARL\lib\jco3environment.jar;E:\RL\JAVARL\lib\mail
.jar;E:\RL\JAVARL\lib\mapdb.jar;E:\RL\JAVARL\lib\nxsl.jar;E:\RL\JAVARL\lib\shi
mwrapper.jar;E:\RL\JAVARL\lib\xds.jar;E:\RL\JAVARL\lib\xp.jar
```

9 将 PATH 环境变量设置为 Java.exe 的 JDK 或 JRE 对应的 bin 文件夹。

10 必须在 dirxml_jremote 脚本中指定 jar 文件的位置。这些文件位于解压缩 dirxml_jremote.tar.gz 目录的 lib 子目录中。例如 \lib*.jar。

11 配置示例配置文件 config8000.txt，使其可用于您的应用程序 shim。

   dirxml_jremote.tar.gz jar 文件包含此文件。有关详细信息，请参见第 10.3 章 “ 配置 Remote Loader 和驱动程序 ” （第 96 页）。

12 使用以下命令起动 Remote Loader：

   12a 要指定 Remote Loader 口令，请使用以下命令：

```
java.exe -classpath %CLASSPATH%
com.novell.nds.dirxml.remote.loader.RemoteLoader -config <config file name>
-sp <Remote Loader Password> <Object Driver Password>
```

例如：

```
java.exe -classpath %CLASSPATH%
com.novell.nds.dirxml.remote.loader.RemoteLoader -config
e:\RL\JAVARL\config8000.txt -sp novell novell
```

12b 要启动 Remote Loader，请使用以下命令：

```
java.exe -classpath %CLASSPATH%
com.novell.nds.dirxml.remote.loader.RemoteLoader -config <config file name>
```

例如：

```
java.exe -classpath %CLASSPATH%
com.novell.nds.dirxml.remote.loader.RemoteLoader -config
e:\RL\JAVARL\config8000.txt
```

12c 要停止 Remote Loader，请使用以下命令：

```
java.exe -classpath %CLASSPATH%
com.novell.nds.dirxml.remote.loader.RemoteLoader -config <config file name>
-unload
```

例如：

```
java.exe -classpath %CLASSPATH%
com.novell.nds.dirxml.remote.loader.RemoteLoader -config
e:\RL\JAVARL\config8000.txt -unload
```

10.2.4 安装 .NET Remote Loader

要以管理用户的身份安装 .NET Remote Loader，请执行以下操作：

1. 在要安装 .NET Remote Loader 的计算机上以管理员身份登录。
2. 要访问安装程序，请完成以下步骤之一：
   - **2a** （视情况而定）如果您已获取 Identity Manager 安装包的 .iso 映像文件，请导航到包含 .NET Remote Loader 安装文件的目录 （默认为 \products\idm\windows\setup\ 目录）。
   - **2b** （视情况而定）如果您已从 NetIQ 下载网站下载了 .NET Remote Loader 安装文件，请完成以下步骤：
     - 浏览到所下载映像的 .tgz 文件。
     - 将该文件的内容解压缩到本地计算机上的某个文件夹中。
3. 运行安装目录中的 idm_install.exe 程序。
4. 接受许可协议，然后单击下一步。
5. 在 “ 选择组件 ” 窗口中，指定 “.NET Remote Loader”。

   有关选项的详细信息，请参见第 8.2 节 “ 了解安装程序 ” （第 74 页）。
6. （可选）要为单个组件选择特定的驱动程序，请完成以下步骤：
   - **6a** 单击自定义选择的组件，然后单击下一步。
   - **6b** 展开要安装的组件下面的驱动程序。
   - **6c** 选择要安装的驱动程序。

7 单击下一步。

8 在激活通知窗口中，单击确定。

9 在计算机上选择 .NET Remote Loader 安装目录。

10 查看 " 摘要 " 页面，然后单击安装以完成安装。

10.2.5 执行 Remote Loader 的无提示安装

要运行 Remote Loader 的无提示安装，请创建包含完成安装所需参数的属性文件。 Identity Manager 媒体包含一个示例属性文件，其路径为 \products\idm\windows\setup\silent.properties。

要执行无提示安装，请执行以下操作：

1 在安装目录中，创建一个 properties 文件或编辑示例 silent.properties 文件。

2 使用文本编辑器在该文件中指定以下参数：

CONNECTED_SYSTEM_SELECTED

指定是否要安装 32 位 Remote Loader 服务和驱动程序。可以在同一个服务器上同时安装 32 位和 64 位版本。

X64_CONNECTED_SYSTEM_SELECTED

指定是否要安装 64 位 Remote Loader 服务和驱动程序。可以在同一个服务器上同时安装 32 位和 64 位版本。

UTLITIES_SELECTED

指定是否要安装实用程序和 Remote Loader 的系统组件。

DOT_NET_REMOTELOADER_SELECTED

指定是否要在 Windows 服务器上安装 .NET Remote Loader 服务和驱动程序。

3 要运行无提示安装，请发出以下命令：

install.exe -i silent -f *文件名* .properties

4 （可选）有关默认安装位置，请参见安装日志文件。例如 C:\Users\Admin1\AppData\Local\Temp\1\idmInstall.log。

10.3 配置 Remote Loader 和驱动程序

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

在使用 Remote Loader 之前，必须将应用程序 shim 配置为安全连接到 Identity Manager 引擎。您还必须配置 Remote Loader 和 Identity Manager 驱动程序。有关 shim 的详细信息，请参见了解 Shim（第 87 页）。

- 第 10.3.6 节 “ 配置 Identity Manager 驱动程序以与 Remote Loader 配合使用 ” （第 113 页）
- 第 10.3.7 节 “ 配置与 Identity Manager 引擎的相互鉴定 ” （第 114 页）
- 第 10.3.8 节 “ 校验配置 ” （第 122 页）

10.3.1 创建与 Identity Manager 引擎的安全连接

您必须确保在 Remote Loader 与 Identity Manager 引擎之间传输数据的安全。 NetIQ 建议使用传输层安全性 / 安全套接字层 (TLS/SSL) 协议进行通讯。要支持 TLS/SSL 连接，需要有密钥存储区文件或 KMO 中储存的相应自我签名证书。本节说明了如何创建、导出和储存该证书。

注释：在托管 Identity Manager 引擎和 Remote Loader 的服务器上使用相同 SSL 版本。如果该服务器与 Remote Loader 上的 SSL 版本不匹配，服务器将返回 SSL3_GET_RECORD：错误的版本号错误讯息。此讯息仅作警告之用，服务器与 Remote Loader 之间的通讯并不会中断。但是，该错误可能会让用户感到困惑。

了解通讯过程

Remote Loader 会打开客户端套接字，并监听来自远程接口 Shim 的连接。远程接口 shim 和 Remote Loader 会执行 SSL 握手，以建立安全通道。然后，远程接口 shim 将鉴定到 Remote Loader。如果远程接口 shim 的鉴定成功， Remote Loader 将鉴定到远程接口 shim。只有双向鉴定确认双方使用授权的实体进行通讯后，同步交通才能进行。

在驱动程序与 Identity Manager 引擎之间建立 SSL 连接的过程取决于驱动程序的类型：

- **对于本机驱动程序** （例如 Active Directory 驱动程序），请指向 base64 编码的证书。有关详细信息，请参见管理自我签名的服务器证书 （第 97 页）。
- **对于 Java 驱动程序**，您必须创建密钥存储区。有关详细信息，请参见使用 SSL 连接时创建密钥存储区文件 （第 99 页）。
- **对于 .NET 驱动程序**，指向 base64 编码的证书。有关详细信息，请参见管理自我签名的服务器证书 （第 97 页）。

注释：Remote Loader 允许在 Remote Loader 和 Identity Manager 服务器上托管的远程接口 shim 之间使用自定义连接方法。要配置自定义连接模块，请参见该模块随附文档中有关连接字符串中预期的和允许内容的信息。

管理自我签名的服务器证书

您可以创建和导出自我签名的服务器证书，以确保在 Remote Loader 与 Identity Manager 引擎之间进行安全通讯。如需额外的安全保障，您可以按照 Suite B 指定为 SSL 通讯配置较严密的密码。此通讯需要使用 ECDSA （Elliptic Curve Digital Signature Algorithm，椭圆曲线数字签名算法）证书来加密数据。启用 Suite B 时， Remote Loader 使用 TLS 1.2 作为通讯协议。有关 Suite B 的详细信息，请参见 “Suite B Cryptography” （Suite B 加密法）。

您可以导出新创建的证书，也可以使用现有证书。

注释：如果服务器加入树， eDirectory 将创建以下默认证书：

- SSL CertificateIP

- SSL CertificateDNS
- 符合 Suite B 要求的证书

---

1 登录到 NetIQ iManager。

2 要创建新证书，请完成以下步骤：

   2a 单击 **NetIQ 证书服务器 > 创建服务器证书**。

   2b 选择拥有该证书的服务器。

   2c 指定证书的绰号。例如：remotecert。

   注释：NetIQ 建议不要在证书绰号中使用空格。例如，使用 remotecert 而不要使用 remote cert。

   还需要记录证书绰号。此绰号将在驱动程序的远程连接参数中用作 KMO 名称。

   2d 选择证书创建方法，然后单击**下一步**。

   您可以选择以下选项：

   - **标准：** 该选项会使用可能的最大密钥大小创建服务器证书对象，并使用您的组织 CA 对公共密钥证书签名。
   - **自定义：**此选项会使用您指定的设置创建服务器证书对象。它可让您为服务器证书对象设置一些自定义设置。选择此选项可创建 ECDSA 证书以用于 Suite B 通讯。
   - **导入：**此选项会使用 PKCS12 (PFX) 文件中的密钥和证书创建服务器证书对象。您可以将该选项结合 " 导出 " 功能一起使用，以备份和恢复服务器证书或将服务器证书对象从一台服务器移至另一台服务器。

   2e 指定证书参数。

   2f 接受其余的证书默认值。

   2g 复查摘要，单击**完成**，然后单击**关闭**。

3 要导出证书，请完成以下步骤：

   3a 在 iManager 中，导航到**角色和任务** > **NetIQ 证书访问 > 服务器证书**。

   3b 浏览并选择已创建的证书或服务器创建的证书 （例如 SSL CertificateDNS）。

   3c 单击**导出**。

   3d 从下拉菜单中选择 **OU=organization CA.O=TREEANAME** 作为 **CA 证书**。

   3e 从下拉菜单中选择 **BASE64 > 导出格式**。

   注释：如果 Remote Loader 要在 Windows 2012 R2 64 位服务器上运行，证书必须采用 Base64 格式。如果您使用 DER 格式， Remote Loader 将无法连接到 Identity Manager 引擎。

   3f 单击**下一步**。

   3g 单击**保存**，然后单击**关闭**。

使用 SSL 连接时创建密钥存储区文件

要在 Java 驱动程序与 Identity Manager 引擎之间使用 SSL 连接，您必须创建一个密钥存储区。密钥存储区是一个 Java 文件，其中包含加密钥、可能还包含证书 （可选）。如果要在 Remote Loader 与 Identity Manager 引擎之间使用 SSL，并且要使用 Java shim，那么，您需创建一个密钥存储区文件。以下章节说明了如何创建密钥存储区文件：

- 在任何平台上创建密钥存储区 （第 99 页）
- 创建密钥存储区 （第 99 页）

在任何平台上创建密钥存储区

要在任意平台上创建密钥存储区，可以在命令行中输入以下内容：

keytool -import -alias trustedroot -file self-signed_certificate_name -keystore filename -storepass keystorepass

文件名可以是任意名称。例如：rdev_keystore。

创建密钥存储区

运行默认位于 c:\novell\remoteloader\jre\bin 目录中的 Keytool 实用程序。

10.3.2 了解 Remote Loader 的配置参数

要使 Remote Loader 能够与托管 Identity Manager 应用程序 shim 的驱动程序实例配合工作，您必须配置该驱动程序实例。例如，必须指定该实例的连接和端口设置。您可以通过命令行或 Remote Loader 控制台指定设置。实例运行后，您可以使用命令行修改配置参数，或者指示 Remote Loader 执行某个函数。例如，您可能需要打开跟踪窗口或卸载 Remote Loader。

本节提供了有关配置参数的信息。其中说明了当实例正在运行时，是否可以从命令行发送一个参数来更新 Remote Loader。

有关配置新驱动程序实例的详细信息，请参见第 10.3.3 节 “ 为驱动程序实例配置 Remote Loader” （第 107 页）。

Remote Loader 中驱动程序实例的配置参数

您可以在命令行或配置文件中配置驱动程序实例。 NetIQ 提供了 config8000.txt 示例文件，可帮助您配置要与应用程序 shim 配合使用的 Remote Loader 和驱动程序。该示例文件默认位于 C:\novell\remoteloader\<architecture(64bit/32bit>\ 或 C:\Novell\remoteloader.NET 目录中。例如，该配置文件可能包含以下行：

```
-commandport 8000
-connection "port=8090"
-trace 4
-tracefile ./trace8000.log
-class com.novell.nds.dirxml.driver.delimitedtext.DelimitedTextDriver
```

请使用以下参数：

-assembly

（视情况而定）使用 .NET Remote Loader 时，请指定驱动程序 .dll 所在的路径。请确保配置文件包含此参数。例如：

```
-assembly C:\Novell\remoteloader.NET\DXMLMADDriver.dll
```

-description *value* (-desc *value*)

（可选）以字符串格式指定简短说明 （例如 SAP），应用程序将在跟踪窗口的标题中使用该说明，并将其用于审计日志记录。例如：

```
-description SAP
```

```
-desc SAP
```

-class *name* (-cl *name*)

（视情况而定）使用 Java 驱动程序时，指定要托管的 Identity Manager 应用程序 shim 的 Java 类名。此选项将告知应用程序使用 Java 密钥存储区来读取证书。例如：

-class com.novell.nds.dirxml.driver.ldap.LDAPDriverShim -cl com.novell.nds.dirxml.driver.ldap.LDAPDriverShim

---

注释：

- 如果指定了 -module 选项，则不能使用上述选项。
- 如果使用制表符字符作为 -class 选项中的分隔符， Remote Loader 将不会自动启动，而必须由您手动启动。要让 Remote Loader 正常启动，您可以使用空格字符而不要使用制表符。
- 有关可为此选项指定的名称的详细信息，请参见了解 Java -class 参数的名称 （第 106 页）。

-commandport *port_number* (-cp *port_number*)

指定驱动程序实例用于控制用途的 TCP/IP 端口。例如：-commandport 8001 或 -cp 8001。默认值是 8000。

要在同一个服务器上将多个驱动程序实例与 Remote Loader 配合使用，请为每个实例指定不同的连接端口和命令端口。

如果驱动程序实例要托管应用程序 shim，则命令端口将是另一个实例与托管 shim 的实例进行通讯的端口。如果驱动程序实例要将命令发送到托管应用程序 shim 的实例，则命令端口将是托管实例所要侦听的端口。

如果要从命令行将此参数发送到托管应用程序 shim 的实例，则命令端口表示托管实例所要侦听的端口。您可以在 Remote Loader 运行时发送此命令。

-config *filename*

指定驱动程序实例的配置文件。例如：

```
-config config.txt
```

配置文件可以包含除 -config 以外的任意命令行选项。在命令行中指定的选项将覆盖配置文件中指定的选项。

您可以在 Remote Loader 运行时发送此命令。

-connection *“parameters”* (-conn *“parameters”*)

指定用于连接到托管 Identity Manager 引擎并运行 Identity Manager 远程接口 shim 的服务器的设置。默认连接方法为使用 SSL 的 TCP/IP。

要在同一个服务器上将多个驱动程序实例与 Remote Loader 配合使用，请为每个实例指定不同的连接端口和命令端口。

使用以下语法输入连接字符串：

```
-connection "parameter parameter parameter"
```

例如：

```
-connection "port=8091 fromaddress=198.51.100.0 rootfile=server1.pem
keystore=ca.pem localaddress=198.51.100.0 hostname=198.51.100.0 kmo=remote
driver cert"
```

使用以下参数指定 TCP/IP 连接的设置：

address=*IP_address*

（可选）指定 Remote Loader 是否侦听特定的本地 IP 地址。如果托管 Remote Loader 的服务器有多个 IP 地址，但 Remote Loader 只能监听其中一个地址时，这个参数将非常有用。以下值为有效值：

- address=address number
- address='localhost'

例如：

```
address=198.51.100.0
```

如果您未指定值， Remote Loader 将侦听所有本地 IP 地址。

fromaddress=*IP_address*

指定 Remote Loader 接受连接的来源服务器。应用程序将忽略来自其他地址的连接。指定服务器的 IP 地址或 DNS 名称。例如：

```
fromaddress=198.51.100.0
```

```
fromaddress=testserver1.company.com
```

handshaketimeout=*milliseconds*

（视情况而定）当来自 Identity Manager 引擎的其他有效连接发生握手超时适用。为 Remote Loader 与 Identity Manager 引擎之间的握手指定超时期限，以毫秒为单位。例如：

```
handshaketimeout=1000
```

您可以指定大于或等于零的整数。零表示连接永不超时。默认值为 1000 毫秒。

hostname=*server*

指定要在其上运行 Remote Loader 的服务器的 IP 地址或名称。例如：

```
hostname=198.51.100.0
```

secureprotocol=*TLS 版本*

指定 Remote Loader 用于连接 Identity Manager 引擎的 TLS 协议版本。例如：

```
secureprotocol=TLSv1_2
```

Identity Manager 支持 TLSv1 和 TLSv1_2。默认情况下， Remote Loader 使用 TLSv1_2。要使用 TLSv1，请在该参数中指定此版本。

enforceSuiteB=*true/false*

（视情况而定）仅当您希望 Remote Loader 使用 Suite B 加密算法与 Identity Manager 引擎通讯时才适用。

要将 Suite B 用于通讯，请指定 true。只有 TLS 1.2 协议支持此通讯。

如果您尝试将启用 Suite B 的引擎与不支持 TLSv1.2 的 Remote Loader 进行连接，握手将会失败，并且无法建立通讯。例如， Remote Loader 4.5.3 就不支持 TLS v1.2。

useMutualAuth=*true/false*

（视情况而定）仅当您希望 Remote Loader 与 Identity Manager 引擎通过校验可信证书颁发机构 (CA) 颁发的公共密钥证书或数字证书或者自我签名证书来相互鉴定时适用。例如：

```
useMutualAuth=true
```

keystore=*filename*

指定 Java 密钥存储区的文件名，该密钥存储区包含远程接口 shim 所用证书的颁发者的可信根证书。例如：

```
keystore=keystore filename
```

通常，您可指定托管远程接口 shim 的树的证书颁发机构。

kmo=*name*

指定包含用于 SSL 连接的密钥和证书的密钥材料对象的密钥名称。例如：

```
kmo=remote driver cert
```

localaddress=*IP_address*

指定要将客户端连接套接字绑定到的 IP 地址。例如：

```
localaddress=198.51.100.0
```

port=*port_number*

指定 Remote Loader 将用于监听来自远程接口 shim 的连接的 TCP/IP 端口。要指定默认端口，请输入 port=8090。

rootfile=*trusted certname*

指定包含远程接口 Shim 所用证书颁发者可信根证书的文件的文件名。该证书文件的格式必须是 Base 64 (PEM)。例如：

```
rootfile=trustedcert
```

通常，该文件是托管远程接口 shim 的树的证书颁发机构。

storepass=*password*

指定您为 keystore 参数输入的 Java 密钥存储区的口令。例如：

```
storepass=mypassword
```

若要让 Remote Loader 与 Java 驱动程序通讯，请使用以下语法指定键值对：

keystore=*keystorename* storepass=*password*

-datadir *directory* (-dd *directory*)

指定 Remote Loader 使用的数据文件所在的目录。例如：

```
-datadir C:\novell\remoteloader
```

当您使用此命令时， Remote Loader 会将其当前目录切换为指定的目录。将在此数据目录中创建不含明确的指定路径的跟踪文件和其他文件。

-help (-h)

指示应用程序显示帮助。

-java (-j)

（视情况而定）指定您想要为 Java 驱动程序 shim 实例设置口令。

注释：如果您未同时指定 -class 值，请将此选项与 -setpasswords 选项结合使用。

-javadebugport *port_number* (-jdp *port_number*)

指示实例在指定的端口上启用 Java 调试。例如：

```
-javadebugport 8080
```

在开发 Identity Manager 应用程序 shim 时请使用此命令。您可以在 Remote Loader 运行时发送此命令。

-javaparam *parameters* (-jp *parameters*)

指定 Java 环境的参数。使用以下语法输入 Java 环境参数：

```
-javaparam parameter
-jp parameter
-jp parameter
```

注释：不要对 Java Remote Loader 使用此参数。

要为单个参数指定多个值，请将该参数括在引号中。例如：

```
-javaparam DHOST_JVM_MAX_HEAP=512M
-jp DHOST_JVM_MAX_HEAP=512M
-jp "DHOST_JVM_OPTIONS=-Dfile.encoding=utf-8 -Duser.language=en"
```

使用以下参数设置 Java 环境：

DHOST_JVM_ADD_CLASSPATH

指定 JVM 要在其中搜索包 (.jar) 和类 (.class) 文件的其他路径。

DHOST_JVM_INITIAL_HEAP

以十进制字节数指定初始 （最小） JVM 堆大小。使用数字值后跟表示字节类型的 G、 M 或 K。例如：

```
100M
```

如果您未指定字节类型，大小默认以字节为单位。使用此参数的效果与使用 Java -Xms 命令相同。

此参数优先于驱动程序集属性选项。增加初始堆大小可以减少启动时间并提高吞吐量性能。

DHOST_JVM_MAX_HEAP

以十进制字节数指定最大 JVM 堆大小。使用数字值后跟表示字节类型的 G、M 或 K。例如：

```
100M
```

如果您未指定字节类型，大小默认以字节为单位。

此参数优先于驱动程序集属性选项。

DHOST_JVM_OPTIONS

指定在启动驱动程序的 JVM 实例时要使用的自变量。请使用空格来分隔各选项字符串。例如：

```
-Xnoagent -Xdebug -Xrunjdwp: transport=dt_socket,server=y, address=8000
```

驱动程序集属性选项优先于此参数。此环境变量附加在驱动程序集属性选项的末尾。有关有效选项的详细信息，请参见 JVM 文档。

-module "*name*" (-m "*name*")

（视情况而定）使用本机驱动器时，请指定包含要托管的 Identity Manager 应用程序 shim 的模块。此选项将告知应用程序使用 rootfile 证书。例如，对于本机驱动程序，请键入以下内容之一：

```
-module "c:\Novell\RemoteLoader\ADDriver.dll"
-m "c:\Novell\RemoteLoader\ADDriver.dll"
```

注释：

- 如果指定了 -class 选项，则不能使用上述选项。
- 如果使用制表符字符作为 -module 选项中的分隔符， Remote Loader 将不会自动启动，而必须由您手动启动。要让 Remote Loader 正常启动，您可以使用空格字符而不要使用制表符。

-password *value* (-p *value*)

当所发出命令会更改设置或影响实例操作时，请指定驱动程序实例的口令。您为所要发出命令的实例指定的口令必须与使用 setpasswords 指定的第一个口令相同。例如：

```
-password netiq4
```

如果您在发出命令时未发送该口令，驱动程序实例将提示您提供该口令。

您可以在 Remote Loader 运行时发送此命令。

-service *value* (-serv *value*)

指定是否要将某个实例配置为 Win32 服务。有效值为 install 和 uninstall，以及托管应用程序 shim 所需的其他参数。例如，您必须包含 -module，还可能需要包含 -commandport 和连接设置。

此命令只会安装或卸装用作服务的实例，而不会启动该服务。

您可以在 Remote Loader 运行时发送此命令。但是，您不能在 rdxml 或 Java Remote Loader 上使用此命令。

-setpasswords *Remote_Loader_pwd optional_pwd* (-sp *Remote_Loader_pwd optional_pwd*)

指定驱动程序实例的口令，以及与 Remote Loader 通讯的远程接口 shim 的 Identity Manager 驱动程序对象口令。

您不需要指定口令， Remote Loader 会提示您输入口令。但是，如果指定了 Remote Loader 的口令，则也必须指定与 Identity Manager 引擎服务器上远程接口 shim 关联的 Identity Manager 驱动程序对象的口令。要指定该口令，请使用以下语法：

```
-setpasswords Remote_Loader_password driver_object_password
```

例如：

```
-setpasswords netiq4 idmobject6
```

注释：使用此选项可为驱动程序实例配置指定的口令，但不会装载 Identity Manager 应用程序 shim 或与其他实例通讯。

跟踪文件设置

（视情况而定）在托管 Identity Manager 应用程序 shim 时，请为包含 Remote Loader 和此实例的驱动程序发来的信息讯息的跟踪文件指定设置。

在配置文件中添加以下参数：

-trace *integer* (-t *integer*)

指定要在跟踪窗口中显示的讯息级别。例如：

```
-trace 3
```

Remote Loader 的跟踪级别对应于托管 Identity Manager 引擎的服务器上使用的级别。

-tracefile *filepath* (-tf *filepath*)

指定要将跟踪讯息记录到的文件的路径。必须为特定计算机上运行的每个驱动程序实例指定唯一的跟踪文件。例如：

```
-tracefile c:\temp\trace.txt
```

如果 -trace 参数大于零，应用程序会将讯息写入该文件。无需打开跟踪窗口就能将讯息写入该文件。

-tracefilemax *size* (-tf *size*)

指定此实例的跟踪文件大小限制。请使用字节类型的缩写指定以 KB、 MB 或 GB 为单位的值。例如：

- -tracefilemax 1000K
- -tf 100M
- -tf 10G

注释：

- 如果启动远程装载程序时跟踪文件数据大于指定的最大值，则在所有 10 个文件都完成翻转之前，跟踪文件数据都将大于指定的最大值 .
- 将此选项添加到配置文件后，应用程序将为跟踪文件使用指定的名称，并最多包含 9 个 “ 滚动更新 ” 文件。滚动更新文件以其主跟踪文件的名称作为基本名，后跟 _n，其中 n 为从 1 到 9 的数字。

-tracechange *integer* (-tc *integer*)

（视情况而定）当某个现有驱动程序实例托管了应用程序 shim 时，指定新的信息讯息级别。跟踪级别与 Identity Manager 服务器上使用的级别相对应。例如：

```
-trace 3
```

您可以在 Remote Loader 运行时发送此命令。

-tracefilechange *filepath* (-tfc *filepath*)

（视情况而定）当某个现有驱动程序实例托管了应用程序 shim 时，指示该实例使用跟踪文件还是关闭已使用的文件而改用此新文件。例如：

```
-tracefilechange \temp\newtrace.txt
```

您可以在 Remote Loader 运行时发送此命令。

证书口令设置

（视情况而定）仅当配置文件中的 useMutualAuth 设置为 true 时。

-keystorepassword (-ksp)

仅指定对 Java Remote Loader 驱动程序启用相互鉴定所用的密钥存储区口令。

-keypassword (-kp)

指定对 Java 和本机 Remote Loader 驱动程序启用相互鉴定所用的密钥口令。

-unload (-u)

指示卸载驱动程序实例。如果远程装载程序运行为 Win32 服务，则此命令将停止该服务。

您可以在 Remote Loader 运行时发送此命令。

-window *value* (-w) *value*

指示应用程序打开或关闭某个驱动程序实例的跟踪窗口。有效值为 on 和 off。例如：

```
-window on
```

您可以在 Remote Loader 运行时发送此命令。您不能在 Java Remote Loader 上使用此命令。

-wizard (-wiz)

起动 Remote Loader 的配置向导。也可以通过运行不带命令行参数的 dirxml_remote.exe 来起动该向导。

如果您运行此命令并指定了配置文件 （-config 选项），向导将使用配置文件中的值启动。您可以使用该向导更改配置，而无需直接编辑配置文件。例如：

```
-wizard -config config.txt
```

您不能在 Java Remote Loader 上使用此命令。

了解 Java -class 参数的名称

当您使用 -class 参数配置 Remote Loader 和 Java Remote Loader 的驱动程序实例时，必须指定要托管的 Identity Manager 应用程序 shim 的 Java 类名。

Java 类名	驱动程序
com.novell.nds.dirxml.driver.dcsshim.DCSShim	Driver for Data Collection Service
com.novell.nds.dirxml.driver.delimitedtext.DelimitedTextDriver	Delimited Text Driver
be.opns.dirxml.driver.ars.arsremedydrivershim.ARSDriverShim	修复 ARS 的驱动程序
com.novell.nds.dirxml.driver.entitlement.EntitlementServiceDriver	Entitlements Service Driver
com.novell.gw.dirxml.driver.rest.shim.GWdriverShim	GroupWise 2014 驱动程序

Java 类名	驱动程序
com.novell.idm.drivers.idprovider.IDProviderShim	ID Provider Driver
com.novell.nds.dirxml.driver.jdbc.JDBCDriverShim	JDBC 驱动程序
com.novell.nds.dirxml.driver.jms.JMSDriverShim	JMS 驱动程序
com.novell.nds.dirxml.driver.ldap.LDAPDriverShim	LDAP Driver
com.novell.nds.dirxml.driver.loopback.LoopbackDriverShim	回送驱动程序
com.novell.nds.dirxml.driver.ebs.user.EBSUserDriver	Oracle User Management Driver
com.novell.nds.dirxml.driver.ebs.hr.EBSHRDriver	Oracle HR Driver
com.novell.nds.dirxml.driver.ebs.tca.EBSTCADriver	Oracle TCA Driver
com.novell.nds.dirxml.driver.msgateway.MSGatewayDriverShim	受管系统网关驱动程序
com.novell.nds.dirxml.driver.manualtask.driver.ManualTaskDriver	手动任务驱动程序
com.novell.nds.dirxml.driver.nisdriver.NISDriverShim	NIS 驱动程序
com.novell.nds.dirxml.driver.notes.NotesDriverShim	Notes 驱动程序
com.novell.nds.dirxml.driver.psoftshim.PSOFTDriverShim	PeopleSoft 驱动程序
com.netiq.nds.dirxml.driver.pum.PUMDriverShim	Privileged User Management Driver
com.novell.nds.dirxml.driver.salesforce.SFDriverShim	Salesforce Driver
com.novell.nds.dirxml.driver.SAPHRShim.SAPDriverShim	SAP HR Driver
com.novell.nds.dirxml.driver.sap.portal.SAPPortalShim	SAP Portal Driver
com.novell.nds.dirxml.driver.sapumshim.SAPDriverShim	SAP 用户管理驱动程序
com.novell.nds.dirxml.driver.soap.SOAPDriver	SOAP 驱动程序
com.novell.idm.driver.ComposerDriverShim	User Application
com.novell.nds.dirxml.driver.workorder.WorkOrderDriverShim	WorkOrder Driver

10.3.3 为驱动程序实例配置 Remote Loader

Remote Loader 可以托管 .dll、 .so 或 .jar 文件中包含的 Identity Manager 应用程序 shim。为使 Remote Loader 能够运行，应用程序需要一个配置文件 （例如 LDAPShim.txt）。 Remote Loader 控制台实用程序 （简称控制台）可帮助您管理 服务器上运行的所有 Identity Manager 驱动程序实例。您可以启动、停止、添加、去除和编辑 Remote Loader 的每个实例。 Remote Loader 的安装程序也会安装控制台。

如果您要升级，控制台将检测并导入现有的驱动程序实例。要自动导入某个驱动程序，必须将其配置文件储存在 Remote Loader 目录中 （默认为 c:\novell\remoteloader）。然后，就可以使用控制台管理远程驱动程序。

您可以使用命令行或 Remote Loader 控制台来配置 Remote Loader，以识别驱动程序。有关使用命令行的详细信息，请参见第 10.3.2 节 “ 了解 Remote Loader 的配置参数 ” （第 99 页）。

本节提供了以下活动的说明：

- 在 Remote Loader 中创建新驱动程序实例 （第 108 页）
- 在 Remote Loader 中修改现有驱动程序实例 （第 109 页）

在 Remote Loader 中创建新驱动程序实例

1 打开 Remote Loader 控制台。

注释：如果您在安装期间已选择创建控制台的快捷方式，请使用桌面上的 Identity Manager Remote Loader 控制台图标。否则，请运行默认位于 C:\novell\remoteloader*nn*bit 中的 rlconsole.exe。

---

2 要在此服务器上添加驱动程序的实例，请单击**添加**。

3 在**说明**中，提供一个简短名称用于描述该实例。

控制台将在**配置文件**的默认值中使用此信息。

4 对于**驱动程序**，请选择 Java 类名。

注释：要使用 Active Directory 驱动程序，请选择 **ADDriver.dll**。有关每个驱动程序的类名的详细信息，请参见了解 Java -class 参数的名称 （第 106 页）。

---

5 对于**配置文件**，请指定 Remote Loader 储存其配置参数的文件路径。默认值为 C:\novell\remoteloader*nn*bit*Description*-config.txt。

6 指定 Remote Loader 和驱动程序对象的口令。

7 （可选）要在 Remote Loader 与 Identity Manager 引擎服务器之间使用 TLS/SSL 连接，请完成以下步骤：

7a 选择**使用 SSL 连接**。

注释：NetIQ 建议在 Identity Manager 引擎服务器和 Remote Loader 上使用相同的 SSL 版本。如果服务器与 Remote Loader 上的 SSL 版本不匹配，服务器将返回 “SSL3_GET_RECORD：错误的版本号 ” 错误讯息。此讯息仅作警告之用，服务器与 Remote Loader 之间的通讯并不会中断。但是，该错误可能会让用户感到困惑。

7b 对于**可信根文件** （base64 格式文件），请指定从 eDirectory 树的组织证书颁发机构导出的自我签名证书。有关详细信息，请参见第 10.3.1 节 “ 创建与 Identity Manager 引擎的安全连接 ” （第 97 页）和第 10.3.2 节 “ 了解 Remote Loader 的配置参数 ” （第 99 页）。

8 （可选）要配置 Remote Loader 的跟踪文件，请完成以下步骤：

注释：NetIQ 建议仅将跟踪功能用于查错。启用跟踪会降低 Remote Loader 的性能。因此，请不要在生产环境中启用跟踪。

8a 对于**跟踪级别**，请指定一个大于零的值，该值定义了您希望在跟踪窗口中显示的 Remote Loader 和驱动程序所发信息讯息的级别。控制台预定义的值为 1 到 4。要创建您自己的讯息类型，请指定值 5 或更高。

最常用的设置是跟踪级别 3，它可以提供一般处理、 XML 文档和 Remote Loader 讯息。

8b 对于**跟踪文件**，请指定要将跟踪讯息记录到的文件路径。例如：C:\novell\remoteloader\64bit\Test-Delimited-Trace.log。

必须为特定计算机上运行的每个驱动程序实例指定唯一的跟踪文件。仅在跟踪级别大于零时才将跟踪讯息写入跟踪文件中。

8c 对于**所有跟踪日志可用的最大磁盘空间 (Mb)**，请指定此实例的跟踪文件可占用的最大磁盘空间的近似值。

9 （可选）要在启动计算机时自动启动 Remote Loader，请选择**为此驱动程序实例建立 Remote Loader 服务**。

注释：如果 Remote Loader 与 Identity Manager 引擎建立连接时因 handshaketimeout 导致 SSL 连接失败，请将默认 handshaketimeout 变量更新为 10000，并重启动驱动程序和 Remote Loader。

---

10 （视情况而定）要修改 Java 配置的参数，请完成以下步骤：

10a 选择**高级**。

10b 对于**类路径**，请指定 JVM 要在其中搜索包 (.jar) 和类 (.class) 文件的路径。

此参数的作用与 java -classpath 命令相同。

10c 对于 **JVM 选项**，请指定在启动驱动程序的 JVM 实例时要使用的选项。

10d 指定 JVM 实例的初始和最大堆大小 （以 MB 为单位）。

10e 对于 Suite B 通讯，指定 enforceSuiteB=true。只有 TLS 1.2 协议支持此通讯。

有关详细信息，请参见第 10.3.1 节 “ 创建与 Identity Manager 引擎的安全连接 ”（第 97 页）和第 10.3.2 节 “ 了解 Remote Loader 的配置参数 ”（第 99 页）。

10f 单击**确定**。

11 （可选）要允许 Remote Loader 在连接 Identity Manager 引擎时使用安全协议，请在 Remote Loader 配置文件中指定安全协议版本。例如：secureprotocol=TLSv1_2

有关详细信息，请参见第 10.3.2 节 “ 了解 Remote Loader 的配置参数 ”（第 99 页）。

注释：如果您已在驱动程序上配置安全协议版本，请跳过此步骤。

---

12 （可选）要允许 Remote Loader 使用 Suite B 指定的协议进行通讯，请在 Remote Loader 配置文件中指定 enforceSuiteB=true。只有 TLS 1.2 协议支持此通讯。

有关详细信息，请参见第 10.3.2 节 “ 了解 Remote Loader 的配置参数 ”（第 99 页）。

注释：如果您已在驱动程序上启用 Suite B 通讯，请跳过此步骤。

---

13 单击**确定**。

在 Remote Loader 中修改现有驱动程序实例

1 在 Remote Loader 控制台上，从**说明**列中选择驱动程序实例。

2 单击**停止**。

3 输入 Remote Loader 的口令，然后单击**确定**。

4 单击**编辑**。

5 修改配置信息。有关每个参数的详细信息，请参见在 Remote Loader 中创建新驱动程序实例（第 108 页）。

6 要保存更改，请单击**确定**。

10.3.4 为驱动程序实例配置 Java Remote Loader

Java 远程装载程序仅能托管 Java 驱动程序 Shim，但它不能装载或托管本机 (C++) 驱动程序 Shim。

1 在文本编辑器中创建一个新文件。

   NetIQ 提供了 config8000.txt 示例文件，可帮助您配置要与应用程序 shim 配合使用的 Remote Loader 和驱动程序。该示例文件默认位于 C:\novell\remoteloader\<architecture(64bit/32bit>\ 或 C:\Novell\remoteloader.NET 目录中。

2 在新配置文件中添加以下参数：
   - -description （可选）
   - -class 或 -module

     例如：-class com.novell.nds.dirxml.driver.ldap.LDAPDriverShim
   - -commandport
   - 连接参数：
     - port （必需）
     - address
     - fromaddress
     - handshaketimeout
     - rootfile
     - keystore
     - localaddress
     - hostname
     - kmo
     - secureprotocol
     - enforceSuiteB
     - useMutualAuth
   - -java （视情况而定）
   - -javadebugport
   - -password
   - -service
   - -setpasswords
   - 跟踪文件参数 （可选）：
     - -trace
     - -tracefile
     - -tracefilemax

   注释：有关参数的详细信息，请参见第 10.3.2 节 “ 了解 Remote Loader 的配置参数 ” （第 99 页）。

3 保存新的配置文件。

   要让 Remote Loader 在计算机启动时自动启动，请将该文件保存到 \jremote 目录。

4 打开命令提示符。

5 在提示符下，输入 -config *filename*，其中， *filename* 是新配置文件的名称。例如：

```
dirxml_jremote -config <configFile> -service
```

这会启动 Java Remote Loader 服务并打开跟踪窗口。

6 （可选）要停止驱动程序服务，请转到 " 服务 "，然后停止该服务。

10.3.5 为驱动程序实例配置 .NET Remote Loader

Remote Loader 可以托管 .dll 文件中包含的 Identity Manager 应用程序 shim。为使 Remote Loader 能够运行，应用程序需要一个配置文件 （例如 LDAPShim.txt）。 Remote Loader 控制台实用程序 （简称控制台）可帮助您管理 服务器上运行的所有 Identity Manager 驱动程序实例。您可以启动、停止、添加、去除和编辑 Remote Loader 的每个实例。 Remote Loader 的安装程序也会安装控制台。

如果您要升级，控制台将检测并导入现有的驱动程序实例。要自动导入某个驱动程序，必须将其配置文件储存在 Remote Loader 目录中 （默认为 c:\novell\remoteloader）。网络 . 然后，就可以使用控制台管理远程驱动程序。

您可以使用命令行或 Remote Loader 控制台来配置 Remote Loader，以识别驱动程序。有关使用命令行的详细信息，请参见第 10.3.2 节 " 了解 Remote Loader 的配置参数 " （第 99 页）。

本节提供了以下活动的说明：

- 在 .NET Remote Loader 中创建新驱动程序实例 （第 111 页）
- 在 .NET Remote Loader 中修改现有驱动程序实例 （第 112 页）

在 .NET Remote Loader 中创建新驱动程序实例

1 打开 Remote Loader 控制台。

注释：如果您在安装期间已选择创建控制台的快捷方式，请使用桌面上的 Identity Manager Remote Loader 控制台图标。否则，请运行默认位于 C:\novell\remoteloader.net 中的 rlconsole.exe。

---

2 要在此服务器上添加驱动程序的实例，请单击**添加**。

3 在**说明**中，提供一个简短名称用于描述该实例。

控制台将在**配置文件**的默认值中使用此信息。

4 对于**驱动程序**，请选择相应的 driver.dll。

5 对于**配置文件**，请指定 Remote Loader 储存其配置参数的文件路径。默认值为 C:\novell\remoteloader.net*Description*-config.txt。

6 指定 Remote Loader 和驱动程序对象的口令。

7 （可选）要在 Remote Loader 与 Identity Manager 引擎服务器之间使用 TLS/SSL 连接，请完成以下步骤：

7a 选择**使用 SSL 连接**。

注释：NetIQ 建议在 Identity Manager 引擎服务器和 Remote Loader 上使用相同的 SSL 版本。如果服务器与 Remote Loader 上的 SSL 版本不匹配，服务器将返回 “SSL3_GET_RECORD：错误的版本号 ” 错误讯息。此讯息仅作警告之用，服务器与 Remote Loader 之间的通讯并不会中断。但是，该错误可能会让用户感到困惑。

7b 对于**可信根文件** （base64 格式文件），请指定从 eDirectory 树的组织证书颁发机构导出的自我签名证书。有关详细信息，请参见第 10.3.1 节 “ 创建与 Identity Manager 引擎的安全连接 ”（第 97 页）和第 10.3.2 节 “ 了解 Remote Loader 的配置参数 ”（第 99 页）。

8 （可选）要配置 Remote Loader 的跟踪文件，请完成以下步骤：

注释：NetIQ 建议仅将跟踪功能用于查错。启用跟踪会降低 Remote Loader 的性能。因此，请不要在生产环境中启用跟踪。

8a 对于**跟踪级别**，请指定一个大于零的值，该值定义了您希望在跟踪窗口中显示的 Remote Loader 和驱动程序所发信息讯息的级别。控制台预定义的值为 1 到 4。要创建您自己的讯息类型，请指定值 5 或更高。

最常用的设置是跟踪级别 3，它可以提供一般处理、 XML 文档和 Remote Loader 讯息。

8b 对于**跟踪文件**，请指定要将跟踪讯息记录到的文件路径。例如 C:\novell\remoteloader.net\Test-Delimited-Trace.log。

必须为特定计算机上运行的每个驱动程序实例指定唯一的跟踪文件。仅在跟踪级别大于零时才将跟踪讯息写入跟踪文件中。

8c 对于**所有跟踪日志可用的最大磁盘空间 (Mb)**，请指定此实例的跟踪文件可占用的最大磁盘空间的近似值。

9 （可选）要在启动计算机时自动启动 Remote Loader，请选择**为此驱动程序实例建立 Remote Loader 服务**。

注释：如果 Remote Loader 与 Identity Manager 引擎建立连接时因 handshaketimeout 导致 SSL 连接失败，请将默认 handshaketimeout 变量更新为 10000，并重启动驱动程序和 Remote Loader。

10 （可选）要允许 Remote Loader 在连接 Identity Manager 引擎时使用安全协议，请在 Remote Loader 配置文件中指定安全协议版本。例如：secureprotocol=TLSv1_2

有关详细信息，请参见第 10.3.2 节 “ 了解 Remote Loader 的配置参数 ”（第 99 页）。

注释：如果您已在驱动程序上配置安全协议版本，请跳过此步骤。

11 （可选）要允许 Remote Loader 使用 Suite B 指定的协议进行通讯，请在 Remote Loader 配置文件中指定 enforceSuiteB=true。只有 TLS 1.2 协议支持此通讯。

有关详细信息，请参见第 10.3.2 节 “ 了解 Remote Loader 的配置参数 ”（第 99 页）。

注释：如果您已在驱动程序上启用 Suite B 通讯，请跳过此步骤。

12 单击**确定**。

在 .NET Remote Loader 中修改现有驱动程序实例

1 在 Remote Loader 控制台上，从**说明**列中选择驱动程序实例。

2 单击**停止**。

3 输入 Remote Loader 的口令，然后单击**确定**。

4 单击**编辑**。

5 修改配置信息。有关每个参数的详细信息，请参见在 .NET Remote Loader 中创建新驱动程序实例 （第 111 页）。

6 要保存更改，请单击**确定**。

10.3.6 配置 Identity Manager 驱动程序以与 Remote Loader 配合使用

可以配置新的驱动程序或启用现有的驱动程序，与远程装载程序进行通讯。您必须设置 Identity Manager 应用程序 shim 以与 Remote Loader 配合使用。

注释：本节提供配置驱动程序的一般信息，以实现驱动程序与远程装载程序的通讯。有关驱动程序特定的信息，请参见 Identity Manager 驱动程序文档网站上的相关驱动程序实施指南。

要在 Designer 或 iManager 中添加新驱动程序对象或修改现有驱动程序对象，必须配置用于启用 Remote Loader 驱动程序实例的设置。有关本节中所用参数的详细信息，请参见了解 Remote Loader 的配置参数 （第 99 页）。

1 在**概述**中，选择 Identity Manager 驱动程序对象。

2 在驱动程序对象的属性中，完成以下步骤：

   2a 对于**驱动程序模块**，请选择**连接到 Remote Loader**。

   2b 对于**驱动程序对象口令**，请指定 Remote Loader 用于对 Identity Manager 引擎服务器鉴定自身的口令。

   此口令必须与 Remote Loader 中定义的驱动程序对象口令相匹配。

   2c 对于 **Remote Loader 连接参数**，请指定连接到 Remote Loader 所需的信息。使用以下语法：

   ```
   hostname=xxx.xxx.xxx.xxx port=xxxx kmo=certificatename
   localaddress=xxx.xxx.xxx.xxx
   ```

   其中

   hostname

   指定托管 Remote Loader 的服务器的 IP 地址。例如：hostname=192.168.0.1。

   port

   指定 Remote Loader 侦听的端口。默认端口为 8090。

   kmo

   指定包含用于 SSL 连接的密钥和证书的密钥材料对象的密钥名称。例如：kmo=remotecert。

   localaddress

   如果在托管 Identity Manager 引擎的服务器上配置了多个 IP 地址，请指定源 IP 地址。

   2d 对于 **Remote Loader 口令**，请指定 Identity Manager 引擎 （或 Remote Loader shim）用于鉴定到 Remote Loader 所需的口令。

3 定义一个具有同等安全性的用户。

4 单击 “ 下一步 ”，然后单击 “ 完成 ”。

10.3.7 配置与 Identity Manager 引擎的相互鉴定

您可以配置相互鉴定，以确保在 Remote Loader 与 Identity Manager 引擎之间进行安全通讯。相互鉴定使用证书而非口令进行握手。 Remote Loader 与 Identity Manager 引擎通过交换并验证可信证书颁发机构 (CA) 颁发的公共密钥证书或数字证书或者自我签名证书来相互鉴定。如果相互鉴定成功，Remote Loader 会鉴定到引擎。当 Remote Loader 与 Identity Manager 引擎建立了信任关系，双方均确信它们是在与授权实体通讯后，才会进行同步通讯。

要配置相互鉴定，请执行以下任务：

- 导出 Identity Manager 引擎和 Remote Loader 的证书 （第 114 页）
- 启用驱动程序以进行相互鉴定 （第 116 页）

导出 Identity Manager 引擎和 Remote Loader 的证书

为了让相互鉴定正常工作，您需要有引擎的服务器证书和 Remote Loader 的客户端证书。您可以从 eDirectory 导出证书，也可以导入来自第三方供应商的证书。在大多数情况下，您会从 eDirectory 导出服务器证书，这样不需要花费额外的费用。在某些情况下，您可能想要导出 Remote Loader 的第三方客户端证书。

- 从 eDirectory 导出证书 （第 114 页）
- 为 Remote Loader 导出第三方证书 （第 116 页）

从 eDirectory 导出证书

身份库中的证书对象称为关键材料对象 (KMO)。此对象可安全地包含证书和数据，包括与用于 SSL 连接的证书关联的公共密钥和私用密钥。要使用相互鉴定，您需要两个 KMO，一个用于引擎，一个用于 Remote Loader。

您可以导出现有的 KMO，也可以创建新的 KMO，然后将其导出。创建客户端 KMO 与创建服务器 KMO 的过程不同。

创建 KMO

在创建客户端 KMO 之前，必须先创建服务器 KMO。要创建 KMO，请执行下列步骤：

1. 登录到 NetIQ iManager。
2. 在左侧窗格中，选择 **NetIQ 证书服务器 > 创建服务器证书**。
3. 选择拥有您所创建证书的服务器。
4. 指定证书的绰号。

   例如，为服务器证书指定 serverkmo，为客户端证书指定 clientkmo。
5. 在证书创建方法中选择**自定义**，然后单击**下一步**。
6. 保留默认的**组织证书颁发机构**选择，然后单击**下一步**。
7. （视情况而定）如果您要创建客户端 KMO。

   7a 选择**启用扩展密钥使用**。

   7b 选择**自定义**，然后选择**用户鉴定**。

   7c 单击**下一页**。

注释：对于服务器 KMO，请保留默认选择，然后单击下一步。

8 指定 KMO 的有效时段。

确保 iManager 系统时间与您的 Identity Manager 组件以及连接的应用程序保持同步。

9 复查摘要，单击完成，然后单击关闭。

10 重复以上步骤创建客户端 KMO。

导出 KMO

从 eDirectory 导出引擎和 Remote Loader 将用于相互鉴定的 KMO。

要为 Identity Manager 引擎导出 KMO，请运行 DirXML 命令行 (dxcmd) 实用程序：

```
dxcmd -user <admin DN> -password <password of admin> -exportcerts <kmoname>
<server|client> <java|native|dotnet> <output dir>
```

其中

- user 用于指定对驱动程序具有管理权限的用户名。
- password 用于指定对驱动程序具有管理权限的用户的口令。
- exportcerts 用于从 eDirectory 导出证书和私用密钥 / 公共密钥。您必须指定要导出服务器证书还是客户端证书、将使用证书的驱动程序类型以及命令将用于储存此信息的目标文件夹。

例如， dxcmd -user admin.sa.system -password novell -exportcerts serverkmo server java 'C:\certs'

此命令会在 C:\certs 目录中生成 serverkmo_server.ks 文件。默认密钥存储区口令和密钥口令是 dirxml。

运行用于为 Remote Loader 导出 KMO 的 dxcmd 命令时，请注意以下事项：

- dxcmd 实用程序在 LDAP 模式下运行。第一次使用该实用程序时，它会提示您指定信任来自 eDirectory 的证书的选项。根据您的环境，您可以选择仅针对当前会话或针对当前和将来会话信任该证书、信任所有证书，或者选择不信任证书。
- 如果 Remote Loader 要在 Identity Manager 服务器上运行，请以 LDAP 或点格式运行该命令。如果 Remote Loader 安装在单独的服务器上，请仅以 LDAP 格式运行命令。
- 在命令中指定 -host 参数可解析能够向 Identity Manager 服务器鉴定的服务器 IP 地址或主机名。

使用以下语法运行命令：

dxcmd -dnform ldap -host < 主机 IP 地址 > -user < 管理员 DN> -password < 管理员口令 > -exportcerts <KMO 名称 > <client> <java|native|dotnet> < 输出目录 >

表 10-1 不同类型驱动程序的示例

驱动程序类型	命令	输出
Java 驱动程序	`dxcmd -dnform ldap -host 194.99.90.218 -user cn=admin,ou=sa,o=system -password novell -exportcerts clientkmo client java 'C:\certs'`	C:\certs 目录中的 clientkmo_client.ks 文件 密钥存储区的默认口令为 dirxml。 默认私用密钥口令是 dirxml。

驱动程序类型	命令	输出
本机驱动程序	`dxcmd -dnform ldap -host 194.99.90.218 -user cn=admin,ou=sa,o=system -password novell -exportcerts clientkmo client native 'C:\certs'`	C:\certs 目录中的 clientkmo_clientcert.pem、clientkmo_clientkey.pem 和 trustedcert.b64 文件。 默认密钥口令是 dirxml。
.NET 驱动程序	`dxcmd -dnform ldap -host 194.99.90.218 -user cn=admin,ou=sa,o=system -password novell -exportcerts clientkmo client dotnet 'C:\certs'`	C:\certs 目录中的 clientkmo_clientcert.pfx 和 trustedcert.b64 文件。 clientkmo_clientcert.pfx 的默认密钥口令是 dirxml。

为 Remote Loader 导出第三方证书

要将第三方证书与 Remote Loader 搭配使用，您需要将证书导出到 .pfx 文件以及 Base 64 格式的可信根文件中，然后将 .pfx 证书转换为驱动程序使用的格式。例如，本机驱动程序需要 .pem 格式的私用密钥和证书密钥，而 Java 驱动程序需要 .jks 格式的密钥存储区。 .NET 驱动程序使用 .pfx 格式的文件。因此，您需要为 .NET 驱动程序转换文件。

本机驱动程序

完成下列步骤：

1. 从 .pfx 文件中检索 .pem 格式的私用密钥。

   输入一条命令，例如 openssl pkcs12 -in servercert.pfx -out serverkey.pem

2. 从 .pfx 文件中检索 .pem 格式的证书密钥。

   输入诸如 openssl pkcs12 -in servercert.pfx -out servercert.pem 的命令

Java 驱动程序

从 .pfx 文件创建 Java 密钥存储区。输入下面的命令：

```
keytool -importkeystore -srckeystore servercert.pfx -srcstoretype pkcs12 -
destkeystore servercert.jks -deststoretype JKS
```

此命令会提示您键入源密钥存储区口令 (srckeystore passwd) 和目标密钥存储区口令 (dest keystorepasswd)。请输入相应的口令。

最后一个步骤是根据驱动程序类型，在 Remote Loader 配置文件中指定信息。有关详细信息，请参见启用驱动程序以进行相互鉴定。

启用驱动程序以进行相互鉴定

要启用驱动程序通讯以进行相互鉴定，请执行以下任务：

- 使用 KMO 或密钥存储区配置驱动程序 （第 117 页）
- 添加新的 Remote Loader 驱动程序实例 （第 120 页）
- 为驱动程序实例配置 Remote Loader （第 122 页）

使用 KMO 或密钥存储区配置驱动程序

您可以在 Designer 或 iManager 中使用 KMO 或密钥存储区来配置驱动程序。

Designer

在 Designer 中使用 KMO 或密钥存储区配置驱动程序之前，务必按如下方式完成基本驱动程序配置：

1 在 Designer 中打开您的项目。
2 在建模器视图的面板中，选择您要创建的驱动程序。
3 将驱动程序的图标拖到建模器视图上。
4 遵循安装向导中的步骤操作。
5 在 “Remote Loader” 窗口中，选择是。
   5a **主机名：**指定用于运行驱动程序 Remote Loader 服务的服务器的主机名或 IP 地址。例如，输入 192.168.0.1 作为主机名。如果未指定此参数的值，则该值默认为 localhost。
   5b **端口：**指定用于为此驱动程序安装和运行 Remote Loader 的端口号。默认端口号是 8090。
6 单击下一步。
7 按照向导中的其余说明操作，直到完成驱动程序的安装。
8 复查为了创建驱动程序将要完成的任务摘要，然后单击完成。

使用 KMO 或密钥存储区修改驱动程序配置

1 在 Designer 的概要视图中，右键单击驱动程序。
2 选择属性。
3 在导航窗格中，选择驱动程序配置。
4 在鉴定中，选择启用相互鉴定并指定下列参数：

   KMO

   指定服务器 KMO 的名称。

   其他参数

   指定 rootfile 及其绝对路径。

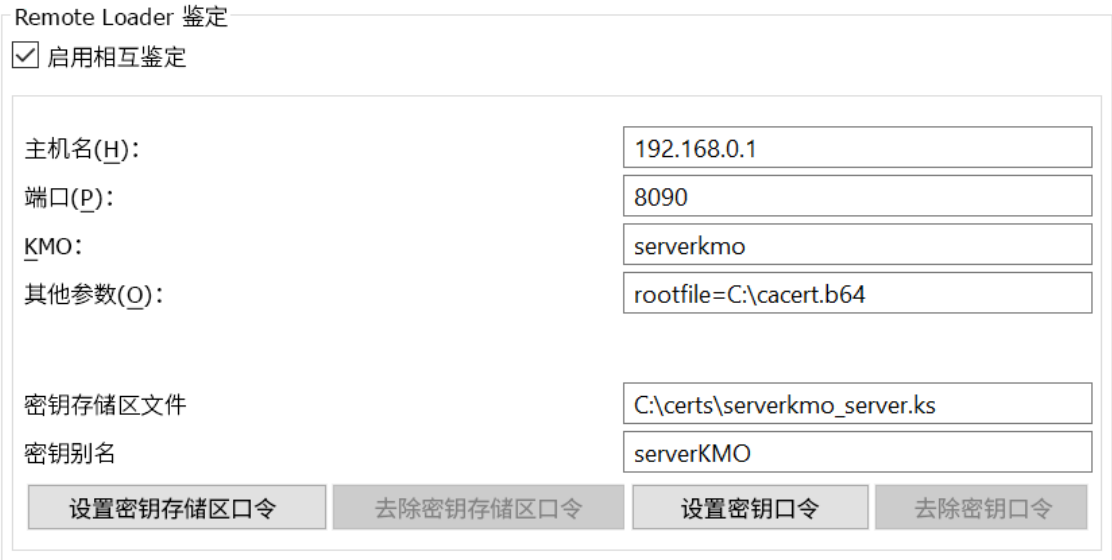
   密钥存储区文件

   指定密钥存储区文件的绝对路径。

   密钥别名

   指定服务器 KMO 的名称。

图 10-1 在 Designer 中启用相互鉴定的配置示例



5 设置密钥存储区口令。

6 设置密钥口令。

注释：默认情况下，密钥存储区口令和密钥口令均设为 dirxml。

您也可以使用 dxcmd 命令来设置密钥存储区和密钥口令。

```
dxcmd -user <administrative_user> -password <admin_password>
```

1. 选择驱动程序操作。
2. 选择要设置密钥存储区和密钥口令的驱动程序。
3. 选择口令操作。
4. 选择设置相互鉴定的密钥存储区口令，然后输入密钥存储区口令。
5. 选择设置相互鉴定的密钥口令，然后输入密钥口令。

---

iManager

要在 iManager 中修改配置，请执行以下操作：

1 起动 iManager。

2 在 Identity Manager 管理中，选择 Identity Manager 概述。

3 在概述中，选择 Identity Manager 驱动程序集。

4 针对要配置的驱动程序选择编辑属性。

5 在驱动程序配置中，指定下列参数：

5a 在驱动程序模块中，选择连接到 Remote Loader。

5b 在 Remote Loader 连接参数中，指定下列连接细节：

```
KMO=<server_KMO_name>
rootfile=<absolute path to the file>
```

例如：

```
KMO=serverkmo
rootfile=C:\cacert.b64
```

5c 设置应用程序口令。

5d 选择启用相互鉴定。

5e 要使用密钥存储区方法，请指定下列各项：

密钥别名

指定服务器 KMO 的名称，并设置密钥口令。

例如：serverKMO

密钥存储区文件

指定密钥存储区文件的绝对路径，并设置密钥存储区口令。

例如：C:\certs\serverkmo_server.ks

5f 单击应用，然后单击确定。

图 10-2 在 iManager 中启用相互鉴定的配置示例

注释：启用相互鉴定时，无需配置 Remote Loader 口令和驱动程序对象口令。

添加新的 Remote Loader 驱动程序实例

1 右键单击 **Identity Manager Remote Loader 控制台**应用程序，并选择**以管理员身份运行**。

2 单击**添加**以添加新的 Remote Loader 实例。

3 指定**说明**，并选择驱动程序类型。

4 指定用于连接 Remote Loader 和 Identity Manager 引擎的**连接端口**。

5 为您的 Remote Loader 实例指定**命令端口**。

6 选择**相互鉴定**并指定所需的驱动程序类型：

- **Java 驱动程序**：浏览包含证书的密钥存储区文件的路径。该密钥存储区文件必须至少包含一对公共 / 私用密钥对。

  密钥存储区文件

  指定要用于鉴定的 Java 密钥存储区文件的路径。密钥存储区文件包含加密密钥和证书。例如，从 eDirectory 导出证书 （第 114 页）中通过 dxcmd 在 C:\certs\ 目录下创建的 clientkmo_client.ks。

  密钥别名

  指定密钥存储区文件中要用于生成对称密钥的公共 / 私用密钥对的名称。例如，clientkmo。

  密钥存储区口令

  指定用于装载 密钥存储区文件的口令。

  私用密钥口令

  指定密钥存储区中储存的私用密钥的口令。Identity Manager 使用此密钥来加密 SSL 通讯。

  图 10-3 添加 Java Remote Loader 实例的示例

- **本机驱动程序**：浏览储存鉴定所用证书的密钥文件路径。该密钥文件的格式必须是 Base 64.

  密钥文件

  指定储存用于鉴定的密钥的文件路径。例如，通过 dxcmd 在 C:\certs\ 目录下创建的 clientkmo_clientkey.pem 文件。

  密钥口令

  指定用于鉴定的私用密钥的口令。

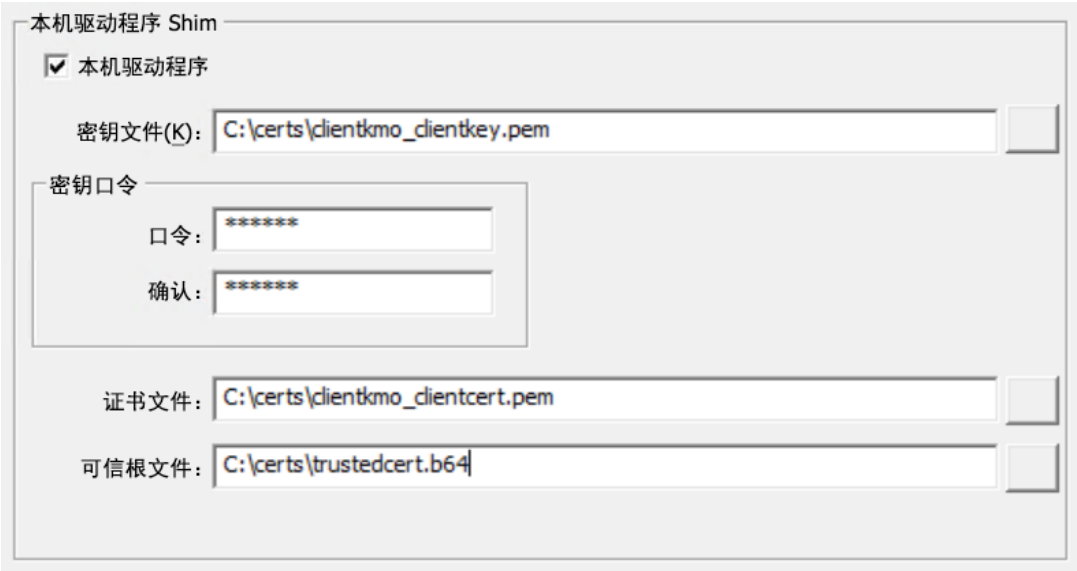
证书文件

指定储存证书的文件。该证书文件的格式必须是 Base 64. 例如，从 eDirectory 导出证书 （第 114 页）中通过 dxcmd 在 C:\certs\ 目录下创建的 clientkmo_clientcert.pem 文件。

可信根文件

指定包含远程接口 Shim 所用证书颁发者可信根证书的文件的文件名。该可信根文件的格式必须是 Base 64. 例如，从 eDirectory 导出证书 （第 114 页）中通过 dxcmd 在 C:\certs\ 目录下创建的 trustedcert.b64 文件。

图 10-4 添加本机 Remote Loader 实例的示例



- **.Net 驱动程序：**浏览储存鉴定所用证书的密钥文件路径。

密钥文件

指定储存用于鉴定的密钥的文件路径。例如，从 eDirectory 导出证书 （第 114 页）中通过 dxcmd 在 C:\certs\ 目录下创建的 clientkmo_clientcert.pfx。

密钥口令

指定用于鉴定的私用密钥的口令。

可信根文件

指定包含远程接口 Shim 所用证书颁发者可信根证书的文件的文件名。该可信根文件的格式必须是 Base 64. 例如，从 eDirectory 导出证书 （第 114 页）中通过 dxcmd 在 C:\certs\ 目录下创建的 trustedcert.b64 文件。

图 10-5 添加 .Net Remote Loader 实例的示例

有关使用 dxcmd 工具为此驱动程序生成的输出文件的详细信息，请参见表 10-1“ 不同类型驱动程序的示例 ”（第 115 页）。

为驱动程序实例配置 Remote Loader

您必须在 Remote Loader 配置文件中配置驱动程序实例。务必在驱动程序的 Remote Loader 配置文件中，指定储存密钥存储区文件、密钥文件、证书文件和根文件的目录的绝对路径。

1 在 Remote Loader 控制台上，从**说明**列中选择驱动程序实例。
2 单击**停止**。
3 输入 Remote Loader 的口令，然后单击**确定**。
4 单击**编辑**，并执行添加新的 Remote Loader 驱动程序实例 （第 120 页）中的步骤 6
5 单击**确定**。

10.3.8 校验配置

有关启动和停止 Remote Loader 的详细信息，请参见第 10.4 章 “ 启动和停止 Remote Loader” （第 123 页）。

1 使用 iManager 启动驱动程序。
2 使用以下任一方式管理 Remote Loader：

Remote Loader 用户界面

1. 右键单击 **Identity Manager Remote Loader** 控制台，并选择**以管理员身份运行**。
2. 您可以使用 Remote Loader 界面**启动**、**停止**、**添加**、**去除**，以及执行其他操作。

注释：要将 Remote Loader 作为服务运行，请选择**为此驱动程序实例建立 Remote Loader 服务**。如果取消选择此选项，会将 Remote Loader 作为应用程序运行。

Remote Loader 控制台

导航到 Remote Loader 安装位置，然后在命令提示符处运行以下命令：

1. 要启动或装载 Remote Loader 实例，请执行以下操作：

   对于 Java Remote Loader：

```
dirxml_jremote -config <configuration_filename> -ksp
<keystore_password> -kp <keypassword>
```

```
dirxml_jremote -config <configuration_filename>
```

对于本机 Remote Loader：

```
dirxml_remote -config <configuration_filename> -ksp <keystore_password>
-kp <keypassword>
```

```
dirxml_remote -config <configuration_filename>
```

对于 .Net Remote Loader：

```
RemoteLoader.exe  -config <configuration_filename> -ksp
<keystore_password> -kp <keypassword>
```

```
RemoteLoader.exe  -config <configuration_filename>
```

2. 要停止或卸载 Remote Loader 实例，请在上一条命令的末尾追加 -u。例如

   对于 Java Remote Loader：

```
dirxml_jremote -config <configuration_filename> -u
```

   对于本机 Remote Loader：

```
dirxml_remote -config <configuration_filename> -u
```

   对于 .Net Remote Loader：

```
RemoteLoader.exe  -config <configuration_filename> -u
```

注释：要将 Remote Loader 实例作为服务运行，请使用以下命令：

```
dirxml_remote -config config.txt -service install
```

10.4 启动和停止 Remote Loader

Remote Loader 可充当服务或守护程序，因此偶尔需要重启动。本节说明了如何停止和启动 Remote Loader。

- 第 10.4.1 节 " 启动 Remote Loader 中的驱动程序实例 " （第 123 页）
- 第 10.4.2 节 " 停止 Remote Loader 中的驱动程序实例 " （第 124 页）

10.4.1 启动 Remote Loader 中的驱动程序实例

您可以将每个平台配置为在启动主机计算机时自动启动一个驱动程序实例。也可以手动启动实例。

- 自动启动驱动程序实例 （第 124 页）
- 使用控制台启动驱动程序实例 （第 124 页）

自动启动驱动程序实例

您可以将 Remote Loader 的驱动程序实例配置为在启动主计算机时自动启动。

1 打开 Remote Loader 控制台。

   如果您在安装期间已创建了 Remote Loader 控制台的快捷方式，请使用桌面上的 Identity Manager Remote Loader 控制台图标。否则，请运行默认位于 C:\novell\remoteloader*nn*bit 中的 rlconsole.exe。

2 选择一个驱动程序实例，然后单击**编辑**。

3 选择**为此驱动程序实例建立 Remote Loader 服务**。

4 保存更改，然后关闭控制台。

使用控制台启动驱动程序实例

1 打开 Remote Loader 控制台。

   如果您在安装期间已创建了 Remote Loader 控制台的快捷方式，请使用桌面上的 Identity Manager Remote Loader 控制台图标。否则，请运行默认位于 C:\novell\remoteloader*nn*bit 中的 rlconsole.exe。

2 选择一个驱动程序实例，然后单击 **“ 启动 ”**。

10.4.2 停止 Remote Loader 中的驱动程序实例

每个平台提供了不同的方法用于停止 Remote Loader 中的驱动程序实例。有关本节中所用参数的详细信息，请参见了解 Remote Loader 的配置参数 （第 99 页）。

注释：要想停止驱动程序实例，您必须拥有足够的权限或指定 Remote Loader 口令。例如， Remote Loader 正在作为 Windows 服务运行。您拥有停止它的足够权限。您输入了一个口令，但意识到该口令并不正确。此时， Remote Loader 仍会停止，因为 Remote Loader 实际上并不 “ 接受 ” 口令，而是会忽略口令。原因是在这种情况下，口令是多余的。如果远程装载程序是作为应用程序运行，而不是作为服务运行的，则可以使用此口令。

要停止某个驱动程序实例，请执行以下操作：

Remote Loader

使用 Remote Loader 控制台。

如果您在安装期间已创建了 Remote Loader 控制台的快捷方式，请使用桌面上的 Identity Manager Remote Loader 控制台图标。否则，请运行默认位于 C:\novell\remoteloader*nn*bit 中的 rlconsole.exe。

Java Remote Loader

输入 dirxml_jremote -config *filename* -u 命令。例如：

```
dirxml_jremote -config config.txt -u
```

11 安装 iManager

本章将引导您完成 iManager 所需组件的安装过程。该安装程序可以安装以下组件：

- iManager （服务器版本）
- iManager Workstation （客户端版本）
- Java
- Novell 国际密码基础结构 (NICI)
- Tomcat

安装文件位于 Identity Manager 安装包 .iso 映像文件内的 \products\iManager\installs\ *服务器平台* \ 目录中。默认情况下，安装程序在 C:\Novell 中安装组件。

NetIQ 建议您在开始之前，先查看安装过程。有关更多信息，请参见第 11.1 章 “ 规划安装 iManager”（第 125 页）。

11.1 规划安装 iManager

本节提供了安装 iManager 所需的先决条件、注意事项以及系统设置。首先，请查阅核对清单，以了解安装过程。

11.1.1 iManager 安装核对清单

NetIQ 建议您在开始安装前先查看以下步骤：

	核对清单项目
❑	1. 了解 Identity Manager 各组件之间的交互。有关详细信息，请参见第 1 章 “Identity Manager 的组件概述 ”（第 19 页）。
❑	2. 确定要为 Identity Manager 组件使用哪些服务器。有关详细信息，请参见第 5.3 节 “ 建议的安装方案和服务器设置 ”（第 39 页）。
❑	3. 了解 iManager 和 iManager Workstation 之间的差别有关更多信息，请参见第 11.1.2 节 “ 了解 iManager 的服务器版本和客户端版本 ”（第 126 页）。

	核对清单项目
❑	4. 为确保计算机满足安装 iManager 服务器和 iManager Workstation 的先决条件，请查看以下注意事项： ◆ 对于 iManager 服务器，请参见安装 iManager 服务器的注意事项 （第 128 页） ◆ 对于 iManager Workstation，请参见安装 iManager Workstation 的注意事项 （第 128 页）
❑	5. 访问 iManager 的安装文件；默认情况下，这些文件位于 Identity Manager 安装包 .iso 映像文件内的 \products\iManager\installs\ *服务器平台* \ 目录中。 另外，您也可以从 NetIQ 下载网站下载这些安装文件。搜索 iManager 产品，选择所需的 iManager 版本，然后将 win.zip 文件下载到您服务器上的某个目录中。例如：iMan_31_win.zip。
❑	6. （可选）要进一步了解插件安装过程，请参见第 11.1.3 节 " 了解 iManager 插件的安装 " （第 127 页）。
❑	7. （可选）要查看安装 iManager 后可以执行的操作，请参见第 11.3 章 "iManager 的安装后任务 " （第 135 页）。
❑	8. 要安装 iManager 和 iManager Workstation，请参见以下章节： ◆ 有关 GUI 安装，请参见第 11.2.1 节 " 安装 iManager 和 iManager Workstation" （第 130 页） ◆ 对于无提示安装，请参见第 11.2.2 节 " 以无提示模式安装 iManager" （第 134 页）

11.1.2 了解 iManager 的服务器版本和客户端版本

您必须在可访问 eDirectory 树的服务器上安装 iManager。要在工作站而不是服务器上安装 iManager，需要基于客户端的 iManager 版本，即 **iManager Workstation**。请依据下列原则确定哪一个版本最适合于您的环境，或者确定同时安装这两个版本是否对您的 eDirectory 管理策略有益。

- 如果您只有一个管理员，并且该管理员始终从同一个客户机工作站管理 eDirectory，则可以使用 iManager Workstation。 iManager Workstation 为完全独立的，几乎不需要设置。在装载或卸载时，会自动启动和停止所需的资源。 iManager Workstation 可以在各种 Windows 客户端工作站上安装和运行，不依赖于基于服务器的 iManager，并且可以与安装在网络上的任何其他版本的 iManager 共存。

  iManager 插件不会自动在 iManager 实例之间进行同步。如果有多个管理员并使用自定义的插件，则必须在每个管理员的客户机工作站上都安装 iManager Workstation 和这些插件。
- 如果从多个客户机工作站管理 eDirectory 或者有多个管理员，则安装 iManager Server，以便任何相连的工作站都能使用。此外，自定义的插件只需在每个 iManager Server 上安装一次。

11.1.3 了解 iManager 插件的安装

默认情况下，插件模块无法在 iManager 服务器之间进行复制。您必须在每个 iManager 服务器上安装所需的插件模块。

在执行全新安装时，安装程序会预先选择 " 典型 " 插件。如果是升级，则只预选需要更新的插件。您可以覆盖默认选择，并添加要下载的新插件。但是，对于升级， NetIQ 建议您不要取消以前预选的任何插件。根据一般规则，您始终应升级随 iManager 先前版本一起安装的插件。此外，较新版本的插件可能与 iManager 的先前版本不兼容。

iManager 的基本插件仅作为完整 iManager 软件下载的一部分提供 （例如， eDirectory 管理插件）。除非这些插件有特定的更新，否则您只能随着整个 iManager 产品下载和安装插件。

安装程序使用 XML 描述符文件 iman_mod_desc.xml 来识别可供下载的插件。该文件的默认 URL 为 http://www.novell.com/products/consoles/imanager/iman_mod_desc.xml。但是，您可以将安装程序指向其他网络 URL。例如，您可能会将 iManager 安装在会阻止安装程序访问默认 URL 的代理或防火墙的后面。

重要：必须使用最新的 iManager SDK 来重新编译您想要在新装版本环境中使用的所有自定义插件。

有关下载和安装插件的说明，请参见以下章节之一中的步骤：

- **GUI 安装：**第 11.2.1 节 " 安装 iManager 和 iManager Workstation" （第 130 页）
- **无提示安装：**第 11.2.2 节 " 以无提示模式安装 iManager" （第 134 页）

有关自定义插件下载和安装过程的详细信息，请参见 《*NetIQ iManager Installation Guide*》（NetIQ iManager 安装指南）中的 "Downloading and Installing Plug-in Modules" （下载和安装插件模块）。

11.1.4 安装 iManager 的先决条件和注意事项

本节提供了有关安装 iManager 服务器版本和工作站版本的信息。

- 安装 iManager 的一般注意事项 （第 127 页）
- 安装 iManager 服务器的注意事项 （第 128 页）
- 安装 iManager Workstation 的注意事项 （第 128 页）

安装 iManager 的一般注意事项

在安装 iManager 之前，请先查看以下注意事项：

- Identity Manager 4.7 支持 eDirectory 9.1。请使用 iManager 3.1。有关详细信息，请参见 《iManager 3.1 Installation Guide》（iManager 3.1 安装指南）。
- 如果您计划要让 10 名以上的管理员同时在 iManager 中定期工作，请不要在其他 Identity Manager 组件所在的同一个服务器上安装 iManager。
- 如果您只计划分派一名管理员，则可以在 Identity Manager 引擎所在的同一个服务器上安装 iManager。
- 如果 iManager 服务器安装程序检测到以前安装的 iManager 版本，您可以停止安装过程，或者去除现有的 iManager、 JRE 和 Tomcat 安装。

- 由于 iManager Workstation 是一个独立的环境，您可以在同一工作站上安装多个版本 （包括 Mobile iManager 的旧版本）。但是，不能同时运行这些版本。如果需要使用不同的版本，可以运行一个版本，关闭该版本，然后再运行其他版本。
- 不能从包含空格的路径运行 iManager Workstation。例如：C:\NetIQ\iManager Workstation\working。
- 您必须对 Windows 服务器拥有管理员访问权限。
- 要在 eDirectory 树中创建基于角色的服务 (RBS) 集合，您必须具有等同于管理员的权限。
- 要运行 eDirectory RBS 配置向导，您必须具有等同于管理员的权限。
- 要使用多个 iManager 版本管理同一个 eDirectory 树，必须将 RBS 集合更新到最新的 iManager 版本。

安装 iManager 服务器的注意事项

如果您使用的是 Microsoft Internet Information Services (IIS) 或 Apache HTTP Server，必须手动将 iManager 与这些 Web 服务器基础结构集成。 iManager 默认使用 Tomcat。

安装 iManager Workstation 的注意事项

在 Windows 客户端上安装 iManager Workstation 之前， NetIQ 建议您先查看以下注意事项：

- 要让 Internet Explorer 为 LAN 使用代理服务器，必须在**工具** > **Internet 选项** > **连接** > **局域网设置**下指定**对于本地地址不使用代理服务器**。
- 要运行低于 4.91 的 Novell Client 版本，必须在起动 iManager Workstation 之前于工作站上安装 NetIQ Modular Authentication Service (NMAS) 客户端。
- 如果从名称中包含 temp 或 tmp 的任何目录 （例如 c:\programs\temp\imanager）所在的路径运行 iManager Workstation，将不会安装 iManager 插件。此时，您应该从 C:\imanager 或非临时目录运行 iManager Workstation。
- 首次在 Windows 工作站上运行 iManager Workstation 时，请使用工作站管理员组的成员帐户。

11.1.5 iManager 服务器的系统要求

本节提供要安装 iManager 的服务器的最低要求。有关 iManager 服务器版本的详细信息，请参见第 11.1.2 节 “ 了解 iManager 的服务器版本和客户端版本 ” （第 126 页）。

类别	要求
处理器	1 GHz
磁盘空间	200 MB
内存	512 MB （建议 1024 MB） iManager 插件需要 80 MB

类别	要求
操作系统 （经认可）	下列操作系统之一： ◆ Windows Server 2016 ◆ Windows Server 2012 R2 ◆ Windows Server 2012 NetIQ 建议您在安装 Identity Manager 之前，按照制造商的自动更新工具应用最新的操作系统增补程序。 **注释：***经认可*指操作系统已经过全面测试且受支持。 不能在 Solaris 平台上安装 iManager。但是， iManager 仍然可以管理并使用 Solaris 上运行的一些应用程序和资源，例如 eDirectory。
操作系统 （受支持）	经认可操作系统的最新版服务包 **注释：***受支持*指操作系统尚未经过测试，但预期可以正常工作。
操作系统热修复	NetIQ 建议您按照制造商的自动更新工具应用最新的操作系统增补程序。
Web 浏览器	以下任意浏览器 （最低版本）： ◆ Google Chrome 61 ◆ Mozilla Firefox 51
应用程序服务器	Tomcat 8.5.27 **注释：**您可以手动将现有的 IIS 或 Apache Web 服务器基础结构与 Windows 服务器上的 iManager 集成。
目录服务	NetIQ eDirectory 9.1 （最低版本）
默认端口	8080、 8443 和 9009

11.1.6 iManager Workstation （客户端版本）的系统要求

本节提供要安装 iManager Workstation 的服务器的最低要求。有关 iManager 客户端版本的详细信息，请参见第 11.1.2 节 “ 了解 iManager 的服务器版本和客户端版本 ” （第 126 页）。

类别	要求
处理器	1 GHz
磁盘空间	200 MB
内存	256 MB （建议 521 MB）

类别	要求
操作系统 （经认可）	下列操作系统之一： ◆ Windows Server 2016 ◆ Windows Server 2012 R2 ◆ Windows Server 2012 NetIQ 建议您在安装 Identity Manager 之前，按照制造商的自动更新工具应用最新的操作系统增补程序。 **注释：***经认可*指操作系统已经过全面测试且受支持。
操作系统 （受支持）	经认可操作系统的最新版服务包 **注释：***受支持*指操作系统尚未经过测试，但预期可以正常工作。
Web 浏览器	以下任意浏览器 （最低版本）： ◆ Google Chrome 61 ◆ Mozilla Firefox 51
操作系统热修复	NetIQ 建议您按照制造商的自动更新工具应用最新的操作系统增补程序。
应用程序服务器	Tomcat 8.5.27 （与 iManager Workstation 捆绑提供）
Java	JRE 1.8.0_162 （与 iManager Workstation 捆绑提供）
默认端口	8080、 8443 和 9009

11.2 安装 iManager 服务器和 iManager Workstation

本节介绍 iManager 的安装过程。要准备安装，请查看第 11.1.4 节 “ 安装 iManager 的先决条件和注意事项 ” （第 127 页）中提供的先决条件和系统要求。

要查看完整安装过程，请参见规划安装 iManager （第 125 页）。

- 第 11.2.1 节 “ 安装 iManager 和 iManager Workstation” （第 130 页）
- 第 11.2.2 节 “ 以无提示模式安装 iManager” （第 134 页）

11.2.1 安装 iManager 和 iManager Workstation

本节提供了在 Windows 服务器和客户端上安装 iManager 与 iManager Workstation 的步骤。要准备安装，请查看先决条件和系统要求：

- **iManager**：安装 iManager 服务器的注意事项 （第 128 页）。
- **iManager 工作站**：安装 iManager Workstation 的注意事项 （第 128 页）。
- 另请参见版本随附的 “ 发行说明 ”。

安装 iManager 服务器

以下过程描述了如何使用安装向导在 Windows 服务器上安装 iManager 的服务器版本。要执行无提示或无人照管安装，请参见第 11.2.2 节 “ 以无提示模式安装 iManager” （第 134 页）。

如果 iManager Server 的安装程序检测到以前安装的 iManager 版本，它可能会让您选择停止安装过程，或者去除现有 iManager、 JRE 和 Tomcat 安装。当安装程序去除以前安装的 iManager 版本时，它会将目录结构备份到旧的 *TOMCAT_HOME* 目录，以保留任何以前创建的自定义内容。

要安装 iManager 服务器，请执行以下操作：

1. 以具有管理员特权的用户身份登录到要安装 iManager 的计算机。
2. （视情况而定）如果您已获取 Identity Manager 安装包的 .iso 映像文件，请导航到包含 iManager 安装文件的目录 （默认为 \products\iManager\installs\win 目录）。
3. （视情况而定）如果您已从 NetIQ 下载网站下载了 iManager 安装文件，请完成以下步骤：
   - **3a** 找到 win.zip 文件。例如， iMan_310_win_x86_64.zip。
   - **3b** 将 win.zip 文件解压缩到本地计算机上的某个文件夹中。
4. 运行 iManagerInstall.exe。
5. （可选）要查看安装程序的调试输出，请在起动安装程序后立即按住 Ctrl 键，直到出现控制台窗口。有关调试的详细信息，请参见 《*NetIQ iManager Administration Guide*》（NetIQ iManager 管理指南）中的 “Troubleshooting” （查错）。
6. 在 iManager 欢迎窗口中选择一种语言，然后单击**确定**。
7. 在**简介**窗口中，单击**下一步**。
8. 接受许可协议，然后单击**下一步**。
9. （视情况而定）如果已在您的服务器上随 iManager 一起安装了某个版本的 JVM 或 Tomcat 或其他支持组件，请在**检测摘要**窗口中完成以下步骤：
   - **9a** 在**安装以下组件**的下面，检查为这些组件列出的版本是否与您要安装的版本匹配。
   - **9b** （可选）如果安装程序未列出您要安装的版本，请浏览到安装文件夹中的相应组件。
10. 单击**下一步**。
11. 在**获取端口输入**窗口中，指定必须在其上运行 Tomcat 服务器的端口号，然后单击**下一步**。

    默认情况下， HTTP 端口和 SSL 端口值分别为 8080 和 8443。但是，如果有其他服务或 Tomcat 服务器正在使用默认端口，则您可以指定其他端口。
12. 指定您希望 TLS 证书使用的证书公共密钥算法，然后单击**下一步**。默认情况下，公共密钥算法设置为 **RSA**。
    - **RSA:** 此证书使用 2048 位 RSA 密钥对。如果选择 **RSA**，则允许四个加密级别。默认情况下，加密法级别设置为**无**。
      - **NONE:** 允许使用任何类型的加密法。
      - **低：**允许使用 56 位或 64 位加密法。
      - **中：**允许使用 128 位加密法。
      - **高：**允许使用大于 128 位的加密法。
    - **ECDSA 256：**此证书使用包含曲线 secp256r1 的 ECDSA 密钥对。如果选择 **ECDSA 256**，则只允许一个加密级别：
      - **SUITEB 128 ONLY：**允许使用 128 位加密法。

有关加密法的详细信息，请参见 《NetIQ iManager Administration Guide》（NetIQ iManager 管理指南）。

13 （可选）要在 iManager 中使用 IPv6 地址，请在**启用 IPv6** 窗口中单击**是**。

您可以在安装 iManager 后启用 IPv6 地址。有关更多信息，请参见第 11.3.2 节 " 安装后为 iManager 配置 IPv6 地址 "（第 137 页）。

14 单击**下一步**。

15 在**选择安装文件夹**窗口中，指定用于储存安装文件的文件夹，然后单击**下一步**。

默认的安装位置为 C:\Program Files\Novell。

16 （可选）要在安装过程中下载并安装插件，请完成以下步骤：

16a 在**选择要下载并安装的插件**窗口中，选择所需的插件。

16b （可选）要从不同的网络位置下载插件，请指定另一个**网络 URL**。

使用其他 URL 下载插件时，您必须校验 URL 内容，并校验插件是否适合您使用。默认情况下，安装程序将从以下网址下载插件：http://www.novell.com/products/consoles/imanager/iman_mod_desc.xml。有关更多信息，请参见第 11.1.3 节 " 了解 iManager 插件的安装 "（第 127 页）。

16c 单击**下一步**。

16d （视情况而定）安装程序可能会显示以下讯息：

```
No new or updated plug-ins found. All plug-ins are downloaded or updated or
the iManager download server is unavailable.
```

如果出现此错误，则表明存在下列一种或多种情况：

- 下载站点中没有提供任何更新的插件。
- 因特网连接有问题。校验您的连接，然后重试。
- 到 描述符文件 (http://www.novell.com/products/consoles/imanager/iman_mod_desc.xml) 的连接没有成功。此 URL 参照了可用 iManager 插件的 XML 描述符文件。
- iManager 安装位于不允许连接到上述 URL 的代理之后。

16e （可选）要从本地目录安装插件，请在 " 从磁盘选择要安装的插件 " 窗口中，指定包含相应 .npm 插件文件的目录路径。

执行此步骤可以安装先前下载的插件或自定义插件。默认路径为 \ *提取位置* \products\iManager\plugins。不过，您也可以指定任何有效路径。

16f 单击**下一步**。

17 （可选）在**获取用户名和树名**窗口中，指定一个授权用户以及此用户将要管理的 eDirectory 树的名称。

注释：

- 如果 eDirectory 使用的端口不是默认端口 524，则您可以指定 eDirectory 服务器的 IP 地址或 DNS 名称再加上端口号。不要使用 localhost。例如，要指定 IPv6 地址，请输入 https://[2001:db8::6]:1080/nps/servlet/webacc?taskId=fw.Startup&forceMaster=true。
- NetIQ 不建议将这些设置保留为空白。如果将这些字段保留为空白，iManager 将允许任何用户安装插件以及更改 iManager 服务器设置。您可以在完成安装过程后指定授权用户。有关更多信息，请参见第 11.3.3 节 " 为 eDirectory 指定授权用户 "（第 138 页）。
- 安装程序不会在 eDirectory 上验证指定的用户身份凭证。

---

18 单击下一步。

19 阅读 " 预安装摘要 " 页，然后单击安装。

20 安装完成后，安装完成窗口将显示有关过程成功的讯息。

注释：尽管安装成功，但安装完成窗口也可能会显示以下错误讯息：

```
The installation of iManager version is complete, but some errors occurred
during the install.
Please see the installation log Log file path for details. Press "Done" to quit
the installer.
```

---

21 （视情况而定）如果安装程序显示了步骤 20 中所示的错误讯息，请完成以下步骤：

21a 记下错误讯息中显示的日志文件的路径。

21b 在安装完成窗口中单击完成。

21c 打开日志文件。

21d （视情况而定）如果在日志文件中发现以下错误，您可以忽略该错误讯息。安装成功，并且 iManager 正常运行。

```
Custom Action: com.novell.application.iManager.install.InstallDLLs
Status: ERROR
Additional Notes: ERROR - class
com.novell.application.iManager.install.InstallDLLs
NonfatalInstallException C:\WINDOWS\system32\msvcr71.dll (The process
cannot access the file because it is being used by another process)
```

21e （视情况而定）如果日志文件不包含步骤 21d 中所列的错误， NetIQ 建议您重试安装。

22 单击完成。

23 完成 iManager 初始化后，单击 " 入门 " 页中的第一个链接，然后登录。有关详细信息，请参见《*NetIQ iManager Administration Guide*》（NetIQ iManager 管理指南）中的 "Accessing iManager" （访问 iManager）。

安装 iManager Workstation

iManager Workstation 是一个独立的环境。您可以在同一个工作站上安装多个版本 （包括 Mobile iManager 的旧版本）。但是，请不要尝试同时运行这些版本。如果需要使用不同的版本，可以运行一个版本，关闭该版本，然后再运行其他版本。

注释：不能从包含空格的路径运行 iManager Workstation。例如：C:\NetIQ\iManager Workstation\working。

要安装 iManager Workstation，请执行以下操作：

1 （视情况而定）如果您已获取 Identity Manager 安装包的 .iso 映像文件，请导航到包含 iManager 安装文件的目录 （默认为 \products\iManager\installs\win\ 目录）。

2 （视情况而定）如果您已从 NetIQ 下载网站下载了 iManager 安装文件，请完成以下步骤：

2a 找到 win.zip 文件。例如：iMan_31_workstation_win.zip。

2b 将 win.zip 文件解压缩到本地计算机上的某个文件夹中。

3 从 imanager\bin 文件夹运行 iManager.bat 文件。

4 在 iManager 登录窗口中，指定某个授权用户的身份凭证以及此用户管理的 eDirectory 树。

有关访问 iManager 的详细信息，请参见 《*NetIQ iManager Administration Guide*》（NetIQ iManager 管理指南）中的 “Accessing iManager” （访问 iManager）。

5 （可选）要启用 IPv6 地址，请完成以下步骤：

1. 打开 *User_Install_Directory*\Tomcat\conf\catalina.properties 文件。
2. 在 catalina.properties 文件中设置以下配置项：

```
java.net.preferIPv4Stack=false
java.net.preferIPv4Addresses=true
```

3. 重启动 Tomcat 服务。

11.2.2 以无提示模式安装 iManager

无提示 （非交互式）安装不显示用户界面，也不向用户提出任何问题。此时， InstallAnywhere 将使用默认 install.properties 文件中的信息。您可以使用默认文件运行无提示安装，或者编辑该文件以自定义安装过程。

要准备安装，请查看先决条件和系统要求：

- **iManager 服务器**：安装 iManager 服务器的注意事项 （第 128 页） .
- **iManager 工作站**：安装 iManager Workstation 的注意事项 （第 128 页）。
- 另请参见版本随附的 “ 发行说明 ”。

编辑 Properties 文件以进行自定义的无提示安装

要更好地控制安装哪些模块，可以自定义无提示安装过程。

1 打开 install.properties 文件；默认情况下，该文件位于各操作系统环境的 Identity Manager 安装包 *.iso* 映像文件中的 products/iManager 目录内。

注释：如果您先前在服务器上安装了当前版本的 iManager，则可以使用安装程序生成的 installer.properties 文件。该文件 （默认位于 log 目录中）包含您在安装期间指定的值。

---

2 在该 properties 文件中，添加以下参数和值：

$PLUGIN_INSTALL MODE$

指定用于控制是否安装插件的属性。添加下面中一个值：

- DISK - （默认值）指示安装程序从本地磁盘安装插件。
- NET - 指示安装程序从网络安装插件。
- BOTH - 指示安装程序同时从磁盘和网络安装插件。
- SKIP - 不安装插件。

$PLUGIN_DIR$

指定位于本地磁盘中的插件的备选路径。默认路径为 *\installer_root_directory*\iManager\installs\ *平台路径* \plugin。

安装程序将安装插件目录中的所有模块，子目录除外。

$PLUGIN_INSTALL_URL$

指定安装程序可从中下载插件的网络 URL ；默认情况下，该 URL 为 http://www.novell.com/products/consoles/imanager/iman_mod_desc.xml。如果您指定了其他 URL，则必须校验 URL 内容，并校验插件是否适合您使用。有关更多信息，请参见第 11.1.3 节 " 了解 iManager 插件的安装 "（第 127 页）。

$LAUNCH_BROWSER$

指定完成安装过程后，安装程序是否会起动 gettingstarted.html 文件。

$USER_INSTALL_DIR$

指定要将 iManager 安装到的路径。

USER_INPUT_ENABLE_IPV6

指定是否要让 iManager 使用 IPv6 地址。默认情况下，安装程序会将此值设置为 yes。

3 对于要下载并安装的每个插件模块，请指定 MANIFEST.MF 文件中的模块 ID 和版本；该文件位于 .npm （插件模块）的 META-INF/ 文件夹中。例如：

```
$PLUGIN_MODULE_ID_1$=eDirectoryBackupAndRestore

$PLUGIN_VERSION_1$=2.7.20050517

$PLUGIN_MODULE_ID_2$=ldap

$PLUGIN_VERSION_2$=2.7.20050517
```

注释：

- 如果您未指定任何模块，程序将安装最常安装的模块，这些模块在下载网站上的 iman_mod_desc.xml 文件中标记为 "selected"。
- 如果您未定义模块版本，安装程序将安装与 .npm 名称匹配的任何模块。

运行 iManager 的无提示安装

您可以使用 install.properties 文件中的默认值以无提示模式安装 iManager。默认情况下，该文件位于各操作系统环境的 Identity Manager 安装包 .iso 映像文件中的 *\products*\iManager 目录内。*\products*\iManager 目录还应包含安装可执行文件。

1 在控制台窗口中，转到已下载的 install.properties 文件所在的目录。

2 在命令行上输入以下命令之一：

```
iManagerInstall.exe -i silent
```

11.3 iManager 的安装后任务

安装 iManager 后，您可以修改配置设置，例如，启用 IPv6 地址，或者更改 eDirectory 树的授权用户。此外， NetIQ 还建议您替换安装过程创建的自我签名证书。

- 第 11.3.1 节 " 替换临时的 iManager 自我签名证书 "（第 136 页）
- 第 11.3.2 节 " 安装后为 iManager 配置 IPv6 地址 "（第 137 页）
- 第 11.3.3 节 " 为 eDirectory 指定授权用户 "（第 138 页）

11.3.1 替换临时的 iManager 自我签名证书

独立的 iManager 安装包括 Tomcat 使用的自我签名临时证书。此证书有效期为一年。 NetIQ 提供此证书的目的是帮助您启动并运行系统，便于您在安装产品后可立即安全地使用 iManager。 NetIQ 和 OpenSSL 不建议将自我签名证书用于测试以外的用途。您应将临时证书替换为安全证书。

Tomcat 将自我签名证书储存在使用 Tomcat (JKS) 格式文件的密钥存储区中。通常，您可以导入私用密钥来替换该证书。但是，用于修改 Tomcat 密钥存储区的 keytool 无法导入私用密钥。该工具只能使用自我生成的密钥。

本节说明了如何使用 NetIQ 证书服务器在 eDirectory 中生成公共 / 私用密钥对，以及如何替换临时证书。如果使用的是 eDirectory，您可以使用 NetIQ 证书服务器安全地生成、跟踪、储存和撤消证书，而无需进一步投资。

替换 iManager 自我签名证书

本节介绍了如何在 eDirectory 中创建密钥对，以及如何通过 PKCS#12 文件导出公共密钥、私用密钥和根证书颁发机构 (CA) 密钥。其中包括修改 Tomcat 的 server.xml 配置文件，以使用 PKCS12 指令并使配置指向实际的 P12 文件，而不是使用默认的 JKS 密钥存储区。

此过程使用以下文件：

- C:\Program Files\Novell\Tomcat\conf\ssl\.keystore，用于保存临时密钥对
- C:\Program Files\Novell\jre\lib\security\cacerts，用于保存可信根证书
- C:\Program Files\Novell\Tomcat\conf\server.xml，用于配置 Tomcat 的证书用法

要替换自我签名证书，请执行以下操作：

1 要创建新证书，请完成以下步骤：
   - **1a** 登录到 iManager。
   - **1b** 单击 **NetIQ 证书服务器** > **创建服务器证书**。
   - **1c** 选择相应的服务器。
   - **1d** 指定服务器的绰号。
   - **1e** 接受其余的证书默认值。

2 要导出服务器证书，请完成以下步骤：
   - **2a** 在 iManager 中，选择**目录管理** > **修改对象**。
   - **2b** 浏览到关键材料对象 (KMO) 对象并选择该对象。
   - **2c** 单击**证书** > **导出**。
   - **2d** 指定口令。
   - **2e** 将服务器证书另存为 PKCS#12 (.pfx)。

3 要将 .pfx 文件转换为 .pem 文件，请完成以下步骤：

   注释：系统上默认不会安装 OpenSSL。但是，您可以从 OpenSSL 网站下载所需的版本。

   - **3a** 输入一条命令，例如 openssl pkcs12 -in newtomcert.pfx -out newtomcert.pem。
   - **3b** 为证书指定您在步骤 2 中指定的同一个口令。

3c 为新的 .pem 文件指定一个口令。

如果需要，可以使用相同的口令。

4 要将 .pem 文件转换为 .p12 文件，请完成以下步骤：

4a 输入一条命令，例如 openssl pkcs12 -export -in newtomcert.pem -out newtomcert.p12 -name "New Tomcat"。

4b 为证书指定您在步骤 3 中指定的同一个口令。

4c 为新的 .p12 文件指定一个口令。

如果需要，可以使用相同的口令。

5 将 .p12 文件复制到 Tomcat 证书位置 （默认为 C:\Program Files\Novell\Tomcat\conf\ssl\）。

6 使用 services.msc 启动脚本停止 Tomcat 服务。

7 为确保 Tomcat 使用新建的 .p12 证书文件，请将 keystoreType、 keystoreFile 和 keystorePass 变量添加到 Tomcat server.xml 文件。例如：

```
<Connector className="org.apache.coyote.http11.Http11AprProtocol"
 port="8443" minProcessors="5" maxProcessors="75" enableLookups="true"
 acceptCount="100" debug="0" scheme="https" secure="true"
 useURIValidationHack="false" disableUploadTimeout="true">
   <Factory className="org.apache.coyote.tomcat7.CoyoteServerSocketFactory"
 clientAuth="false" protocol="TLS" keystoreType="PKCS12"
 keystoreFile="C:\Program Files\Novell\Tomcat\conf\ssl\newtomcert.p12"
keystorePass="password" />
```

Or,

```
<Connector className="org.apache.coyote.http11.Http11NioProtocol"
 port="8443" minProcessors="5" maxProcessors="75" enableLookups="true"
 acceptCount="100" debug="0" scheme="https" secure="true"
 useURIValidationHack="false" disableUploadTimeout="true">
   <Factory className="org.apache.coyote.tomcat7.CoyoteServerSocketFactory"
 clientAuth="false" protocol="TLS" keystoreType="PKCS12"
 keystoreFile="C:\Program Files\Novell\Tomcat\conf\ssl\newtomcert.p12"
keystorePass="password" />
```

在将密钥存储区类型设置为 PKCS12 时，必须指定证书文件的完整路径，因为 Tomcat 不再默认使用 Tomcat 用户主路径。

8 使用 services.msc 启动脚本启动 Tomcat 服务。

11.3.2 安装后为 iManager 配置 IPv6 地址

安装 iManager 后，可以让 iManager 使用 IPv6 地址。

1. 打开安装目录中的 catalina.properties 文件。默认情况下，该文件位于 *installation_directory*\Tomcat\conf 中。
2. 在 properties 文件中设置以下配置项：

```
java.net.preferIPv4Stack=false

java.net.preferIPv4Addresses=true
```

3. 重启动 Tomcat。

11.3.3 为 eDirectory 指定授权用户

安装 iManager 后，您可以修改授权用户的身份凭证以及此用户管理的相应 eDirectory 树名。有关详细信息，请参见《*NetIQ iManager Administration Guide*》（NetIQ iManager 管理指南）中的 "iManager Authorized Users and Groups"（iManager 授权用户和组）。

1 登录到 iManager。
2 在 " 配置 " 视图中，选择 **iManager 服务器** > **配置 iManager** > **安全性**。
3 更新用户身份凭证和树名。

IV 安装 Identity Applications

本章将引导您完成安装 Identity Applications 所需组件和框架的过程：

- Identity Applications 管理
- Identity Applications 仪表板
- Role and Resource Service 驱动程序
- User Application
- 用户应用程序驱动程序

默认情况下，安装程序将在 C:\NetIQ\idm\apps 中安装这些组件。

在安装期间以及安装之后， Identity Applications 都需要访问其他 Identity Manager 组件。 NetIQ 建议您在开始之前，先查看安装过程。有关详细信息，请参见第 15.1 章 “ 规划安装 Identity Applications”（第 165 页）。

12 为 Identity Manager 安装 PostgreSQL 和 Tomcat

在本章中，您将要安装大多数 Identity Manager 组件所用的以下应用程序服务器和数据库程序：

- Apache Tomcat
- PostgreSQL

安装文件位于 Identity Manager 安装包的 \products\CommonApplication\ 目录中。默认情况下，安装程序将在 C:\NetIQ\idm\apps\ 中安装应用程序。

NetIQ 建议您在开始之前，先查看安装过程。有关详细信息，请参见第 12.1.1 节 “Tomcat 和 PostgreSQL 的安装核对清单 ”（第 141 页）。

12.1 规划安装 PostgreSQL 和 Tomcat

从 Identity Manager 4.6 起， NetIQ 仅支持使用 Apache Tomcat 作为应用程序服务器。如果您的公司提供支持版本的 Tomcat，您便可将其与 Identity Manager 搭配使用。

此外，为方便起见， NetIQ 将 Tomcat 和 PostgreSQL 捆绑在同一个安装程序中。借助此安装程序，您无需单独下载即可安装这些组件。除了 NetIQ Identity Manager 文档中概述的内容之外， NetIQ 不会另外提供这些组件的更新或其管理、配置或优化信息。

12.1.1 Tomcat 和 PostgreSQL 的安装核对清单

NetIQ 建议您完成以下核对清单中的步骤：

	核对清单项目
❑	1. 了解 Identity Manager 各组件之间的交互。有关详细信息，请参见以下各节： ◆ 第 4.4 节 “ 使用 Identity Manager 中的自助式口令管理 ”（第 31 页） ◆ 第 4.5 节 “ 在 Identity Manager 中使用单点登录访问 ”（第 33 页）
❑	2. 确定要为 Identity Manager 组件使用哪些服务器。有关详细信息，请参见第 5.3.4 节 “ 建议的服务器设置 ”（第 41 页）。

	核对清单项目
❑	3. 确定在安装 Tomcat 或 PostgreSQL 之前是否应安装 NetIQ Sentinel。有关详细信息，请参见第 5.3 节 " 建议的安装方案和服务器设置 " （第 39 页）。 **注释：**仅支持在 Linux 服务器上安装 Sentinel。要安装 Sentinel，您的环境中必须有一个 Linux 服务器。
❑	4. 查看安装应用程序的注意事项，以确保计算机符合要求： ◆ 第 12.1.4 节 "Tomcat 的安装先决条件 " （第 143 页） ◆ 第 12.1.3 节 "PostgreSQL 的安装先决条件 " （第 142 页）
❑	5. 安装应用程序： ◆ 要执行引导式安装，请参见第 12.2.1 节 " 使用向导安装 PostgreSQL 和 Tomcat"（第 144 页）。 ◆ 要执行无提示安装，请参见第 12.2.2 节 " 以无提示模式为 Identity Manager 安装 Tomcat 和 PostgreSQL" （第 146 页）。
❑	6. 安装其余的 Identity Manager 组件。

12.1.2 了解 PostgreSQL 和 Tomcat 的安装过程

您可以选择安装其中一个应用程序，或者两个都安装。例如，由于服务器上已装有受支持版本的 PostgreSQL，因此您可能就不需要安装该应用程序。在进行单独安装时，请注意以下事项：

PostgreSQL

安装进程会安装 Identity Applications 的数据库，并创建拥有该数据库的管理用户 idmadmin，但不会在 Identity Applications 的数据库中创建纲要。纲要信息是在您安装 Identity Applications 时添加的。

如果您已在服务器上运行受支持版本的 PostgreSQL，安装程序会提示您提供默认 postgres 用户的口令。然后，该程序会创建 idmadmin 用户，并为其指派与 postgres 相同的口令。

安装过程结束后，安装程序会启动数据库实例。当您安装使用该数据库的其他 Identity Manager 组件 （例如 User Application）时，该实例必须处于运行中状态。

您不需要使用 PostgreSQL 作为 Identity Applications 的数据库。

Tomcat

安装过程会创建 IDM Apps Tomcat Service。为了支持 Tomcat 应用程序服务器，安装程序还会安装 Apache ActiveMQ 和 Oracle JRE。这些项目可帮助 Tomcat 发送电子邮件通知。

安装程序不会在完成后启动 Tomcat。在您安装其他 Identity Manager 组件 （例如 Identity Reporting）之前， Tomcat 必须处于停止状态。

12.1.3 PostgreSQL 的安装先决条件

在规划安装 PostgreSQL 之前，请先查看以下注意事项：

- 您可以在运行旧版数据库程序的环境中安装与 Identity Manager 捆绑的 PostgreSQL 版本。为确保新安装不会重写以前的版本，请为安装文件指定一个不同的目录。

- Identity Applications 要求其使用的数据库 （例如 PostgreSQL）满足一些先决条件。有关详细信息，请参见安装 Identity Applications 数据库的先决条件 （第 170 页）。
- 您不能安装多个版本的 PostgreSQL，因为 PostgreSQL 的服务帐户无法处理两个实例。请在安装此版 PostgreSQL 之前先卸装旧版本。

12.1.4 Tomcat 的安装先决条件

在规划安装 Tomcat 之前，请先查看以下注意事项：

- 您可以在同一台服务器上安装 Tomcat 和 PostgreSQL，也可以在不同的服务器上安装。
- 安装过程会安装受支持版本的 Oracle JRE 和 Apache ActiveMQ。
- 安装过程还会安装 Apache Log4j 服务在审计 Tomcat 事件时所需的文件。
- 您可以使用自己的 Tomcat 安装程序，而不使用 Identity Manager 安装包中提供的安装程序。但是，要将 Apache Log4j 服务与您的 Tomcat 版本配合使用，请确保安装了相应的文件。有关详细信息，请参见第 13.1.4 节 " 使用 Apache Log4j 服务记录登录 "（第 150 页）。为 OSP、 Identity Applications 和 Identity Reporting 使用 Tomcat 时，需要满足此项要求。
- 为了使用 ActiveMQ 保证电子邮件通知的递送，请安装 MQServer。
- Identity Applications 要求运行它们的 Tomcat 应用程序服务器满足一些先决条件。有关详细信息，请参见应用程序服务器的先决条件和注意事项 （第 169 页）。
- 安装过程会在 setenv.bat 文件 （默认位于 c:\NetIQ\idm\apps\tomcat\bin 目录）中设置 JRE 位置。当您在 Tomcat 上安装 Identity Applications 和 Identity Reporting 时，安装过程会更新 setenv.bat 文件中的 JAVA_OPTs 或 CATALINA_OPTS 项。

12.1.5 PostgreSQL 的系统要求

PostgreSQL 对计算机的要求与 Identity Applications 的要求相同。有关详细信息，请参见 Identity Applications 的系统要求 （第 171 页）。另请参见最新版 Identity Manager 的 《发行说明》，以及 PostgreSQL 文档。

12.1.6 Tomcat 的系统要求

Tomcat 对计算机的要求与 Identity Applications 的要求相同。有关详细信息，请参见第 15.1.4 节 "Identity Applications 的系统要求 "（第 171 页）。另请参见最新版 Identity Manager 的 《发行说明》，以及 Apache 文档。

12.2 安装 PostgreSQL 和 Tomcat

本节将指导您完成安装 Tomcat 和 PostgreSQL 的过程。

- 第 12.2.1 节 " 使用向导安装 PostgreSQL 和 Tomcat"（第 144 页）
- 第 12.2.2 节 " 以无提示模式为 Identity Manager 安装 Tomcat 和 PostgreSQL"（第 146 页）

12.2.1 使用向导安装 PostgreSQL 和 Tomcat

以下过程介绍了如何使用引导式过程在 Windows 平台上安装 Tomcat 和 PostgreSQL。要执行无提示或无人照管安装，请参见第 12.2.2 节 “ 以无提示模式为 Identity Manager 安装 Tomcat 和 PostgreSQL” （第 146 页）。

要准备安装，请查看以下章节中列出的注意事项和系统要求：

- 第 12.1.4 节 “Tomcat 的安装先决条件 ” （第 143 页）
- 第 12.1.3 节 “PostgreSQL 的安装先决条件 ” （第 142 页）
- 该版本随附的 《发行说明》

注释：无论您要安装 PostgreSQL 还是要使用 PostgreSQL 的现有版本，都必须指定数据库的口令。但是，此安装程序不支持含有 " 或 $ 字符的口令。要使用这些特殊字符，请在完成安装过程之后更改口令。

要执行引导式安装，请执行以下操作：

1 以管理员身份登录要安装这些应用程序的计算机。

2 确保规划的安装路径不包含使用以下任一名称的目录：
   - tomcat
   - postgres
   - activemq
   - jre

   注释：安装 Standard Edition 时，必须安装 ActiveMQ。否则，当您登录 Identity Reporting 后，Reporting 页面不会装载。您也可以在完成 PostgreSQL 安装后将 activemq-all-5.15.2 jar 文件复制到 C:\NetIQ\idm\apps\tomcat\lib 目录，然后重启动 Tomcat。

   ---

3 （视情况而定）如果您已获取 Identity Manager 安装包的 .iso 映像文件，请导航到包含安装文件的 \products\CommonApplication\postgre_tomcat_install 目录。

4 （视情况而定）如果您已从 NetIQ 下载网站下载了安装文件，请完成以下步骤：

   4a 导航到所下载映像的 win.zip 文件。

   4b 将该文件的内容解压缩到本地计算机上的某个目录中。

5 从包含安装文件的目录中运行 TomcatPostgreSQL.exe。

6 在安装程序中，指定要用于安装的语言，然后单击**确定**。

7 查看简介信息，然后单击**下一步**。

8 接受许可协议，然后单击**下一步**。

9 指定是要安装 Tomcat、 PostgreSQL，还是这两者。

10 要完成引导式过程，请指定以下参数的值：
   - **Tomcat 父文件夹**

     仅当安装 Tomcat 时适用。

     指定要安装 Tomcat 文件的具体目录。
   - **Tomcat 细节**

仅当安装 Tomcat 时适用。

表示 Tomcat 所需的端口。

Tomcat 关闭端口

指定用于彻底关闭所有 Web 应用程序和 Tomcat 的端口。默认端口为 8005。

Tomcat http 端口

指定您希望 Tomcat 服务器在与客户端计算机通讯时使用的端口。默认端口为 8080。SSL 通讯的默认端口为 8443。

Tomcat 重定向端口

（视情况而定）如果您未使用 TLS/SSL 协议，请指定应用程序服务器用来重定向需要 SSL 传输的请求的端口。默认值是 8443。

Tomcat ajp 端口

（可选）指定应用程序服务器在通过 AJP 协议 （而不是 http）来与 Web 连接器进行通讯时要使用的端口。默认值是 8009。

当您希望应用程序服务器管理 Web 应用程序中包含的静态内容，并且 / 或者想要利用应用程序服务器的 SSL 处理时，请使用此参数。

- **PostgreSQL 父文件夹**

  仅当安装 PostgreSQL 时适用。

  表示要安装 PostgreSQL 文件的具体目录。

- **PostgreSQL 细节**

  仅当安装 PostgreSQL 时适用。

  表示 Identity Applications 的 PostgreSQL 数据库设置。

注释：如果您已在服务器上运行受支持版本的 PostgreSQL，安装程序会提示您提供默认 postgres 用户的口令。然后，该程序会创建 idmadmin 用户，并为其指派与 postgres 相同的口令。

此安装程序不支持含有 " 或 $ 字符的口令。

数据库名称

指定数据库的名称。默认值为 idmuserappdb。

数据库管理员

指定 idmadmin 帐户，这是一个可以创建数据库表、视图和其他项目的数据库管理员。

此帐户与默认的 postgres 用户不同。

管理员用户的口令

指定数据库管理员和默认 postgres 用户的口令。

此安装程序不支持含有 " 或 $ 字符的口令。

PostgreSQL 端口

指定托管 Postgres 数据库的服务器的端口。默认值是 5432。

11 查看安装前摘要。

12 启动安装过程。

13 安装过程完成后，单击*完成*。

12.2.2 以无提示模式为 Identity Manager 安装 Tomcat 和 PostgreSQL

无提示 （非交互式）安装不显示用户界面，也不向用户提出任何问题。此时， InstallAnywhere 将使用默认 silent.properties 文件中的信息。您可以使用默认文件运行无提示安装，或者编辑该文件以自定义安装过程。要执行引导式安装，请参见第 12.2.1 节 “ 使用向导安装 PostgreSQL 和 Tomcat” （第 144 页）。

要准备安装，请查看以下章节中列出的注意事项和系统要求：

- 第 12.1.4 节 “Tomcat 的安装先决条件 ” （第 143 页）
- 第 12.1.3 节 “PostgreSQL 的安装先决条件 ” （第 142 页）
- 保护无提示安装所用的口令 （第 146 页）
- 该版本随附的 《发行说明》

保护无提示安装所用的口令

如果您不想在 postgresq_tomcat-silent.properties 文件中指定用于安装的口令，可以改为在环境中设置口令。在这种情况下，无提示安装程序将从环境中读取口令，而不是从 postgresq_tomcat-silent.properties 文件中读取。这可以补充一些安全性。

必须为安装指定以下口令：

- NETIQ_DB_PASSWORD
- NETIQ_DB_PASSWORD_CONFIRM

使用 set 命令。例如：

```
set NETIQ_DB_PASSWORD_CONFIRM=myPassWord
```

该安装程序不支持含有 " 或 $ 字符的口令。要使用这些特殊字符，请在安装 PostgreSQL 之后更改口令。

以无提示模式安装 Tomcat 和 PostgreSQL

1 登录到要安装应用程序的计算机。
2 （视情况而定）如果您已获取 Identity Manager 安装包的 .iso 映像文件，请导航到包含安装文件的 \products\CommonApplication\postgre_tomcat_install 目录。
3 （视情况而定）如果您已从 NetIQ 下载网站下载了安装文件，请完成以下步骤：
   - **3a** 导航到所下载映像的 win.zip 文件。
   - **3b** 将该文件的内容解压缩到本地计算机上的某个目录中。
4 要指定安装参数，请完成以下步骤：
   - **4a** 确保 postgresq_tomcat-silent.properties 文件与安装的可执行文件位于同一目录中。
   - **4b** 在文本编辑器中，打开 postgresq_tomcat-silent.properties 文件。
   - **4c** 指定参数值。有关参数的说明，请参见步骤 10 （第 144 页）。
   - **4d** 保存并关闭文件。

5 要起动安装过程，请输入以下命令：

```
install -i silent -f postgresq_tomcat-silent.properties
```

注释：如果 postgresq_tomcat-silent.properties 文件不在安装脚本所在的目录中，您必须指定该文件的完整路径。该脚本会将必要的文件解压缩到一个临时目录，然后起动无提示安装。

13 安装单点登录组件

本章将介绍如何安装 One SSO Provider (OSP)，以支持通过单点登录来访问 Identity Applications 和 Identity Reporting。

安装文件位于 Identity Manager 安装包的 products\CommonApplication\osp_install 目录中。默认情况下，安装程序将在 C:\NetIQ\idm\apps\osp 中安装组件。

NetIQ 建议您在开始之前，先查看安装过程。

13.1 为 Identity Manager 规划安装单点登录

本节提供安装 One SSO Provider (OSP) 所需的先决条件、注意事项和系统设置信息。

- 第 13.1.1 节 " 单点登录组件的核对清单 " （第 149 页）
- 第 13.1.2 节 "One SSO Provider 安装先决条件 " （第 150 页）
- 第 13.1.3 节 "One SSO Provider 的系统要求 " （第 150 页）
- 第 13.1.4 节 " 使用 Apache Log4j 服务记录登录 " （第 150 页）

13.1.1 单点登录组件的核对清单

NetIQ 建议您完成以下核对清单中的步骤：

	核对清单项目
❑	1. 了解 Identity Manager 各组件之间的交互。有关详细信息，请参见第 4.5 节 " 在 Identity Manager 中使用单点登录访问 " （第 33 页）。
❑	2. 确定要为 Identity Manager 组件使用哪些服务器。有关详细信息，请参见第 5.3 节 " 建议的安装方案和服务器设置 " （第 39 页）。
❑	3. 确保已安装 Tomcat。有关详细信息，请参见第 12.2 章 " 安装 PostgreSQL 和 Tomcat" （第 143 页）。
❑	4. （视情况而定）要使用 Apache Log4j 服务来记录 Tomcat 中的事件，请确保您有相应的文件。有关详细信息，请参见第 13.1.4 节 " 使用 Apache Log4j 服务记录登录 " （第 150 页）。
❑	5. 安装 OSP： ◆ 要执行引导式安装，请参见第 13.2.1 节 " 使用向导安装 One SSO Provider" （第 151 页）。 ◆ 要执行无提示安装，请参见第 13.2.2 节 " 以无提示模式安装 One SSO Provider"（第 153 页）。
❑	6. 安装 Self Service Password Reset (SSPR) 以管理 Identity Applications 的用户口令。有关详细信息，请参见第 14.2 节 " 为 Identity Manager 安装口令管理 " （第 157 页）。

	核对清单项目
❑	7. 安装 Identity Applications 并将其配置为使用单点登录访问。有关详细信息，请参见第 15.5 节 “ 安装 Identity Applications”（第 180 页）。

13.1.2 One SSO Provider 安装先决条件

以下 Identity Manager 组件需要使用 OSP 进行用户鉴定：

- Identity Applications
- Identity Reporting

NetIQ 建议您在安装 OSP 之前，先查看以下注意事项：

- 要运行 OSP，您可以使用自己的 Tomcat 安装程序，而不使用 Identity Manager 安装套件中提供的安装程序。但是，要将 Apache Log4j 服务与您的 Tomcat 版本配合使用，请确保安装了相应的文件。有关详细信息，请参见第 13.1.4 节 “ 使用 Apache Log4j 服务记录登录 ”（第 150 页）。
- OSP 需要使用可信证书来确保 Identity Applications 和报告组件能够与鉴定服务器通讯。安装过程将自动在 osp.jks 文件中创建 TLS/SSL 的证书。您还可以让安装过程为 eDirectory 的 SAML 声明创建可信根证书。

  注释：这些证书将于其创建之日起的两年后失效。原来的证书失效后，您必须创建新证书。有关详细信息，请参见鉴定服务器 （第 215 页）和第 VIII 部分 “ 在 Identity Manager 中配置单点登录访问 ”（第 277 页）。

13.1.3 One SSO Provider 的系统要求

OSP 需要 Apache Tomcat 应用程序服务器。Tomcat 的版本必须为 Identity Applications 所需的版本。

所有其他服务器要求与 Identity Applications 的服务器要求一致。有关详细信息，请参见第 15.1.3 节 “ 安装 Identity Applications 的先决条件和注意事项 ”（第 167 页）和此版本的最新 《发行说明》。

13.1.4 使用 Apache Log4j 服务记录登录

您可以使用 Apache Log4j 或 java.util.logging 服务来记录 Tomcat 中发生的事件。Identity Manager 安装套件中的 Tomcat 安装程序包含 Log4j 所需的文件。但是，如果您安装自己的 Tomcat 版本，则需要借助以下文件来使用 Apache 日志记录服务：

- log4j-1.2.16.jar
- tomcat-juli-adapters.jar
- tomcat-juli.jar

要将这些文件添加到 Tomcat 安装中，请完成以下步骤：

1 从 Apache 网站下载 Tomcat 8.5.x 的 “JULI” 文件：
   - tomcat-juli.jar
   - tomcat-juli-adapters.jar
2 从 Apache 网站下载 log4j-1.2.16.jar 文件。

3 将以下文件放在 $TOMCAT_HOME\lib 目录中：

- log4j-1.2.16.jar
- tomcat-juli-adapters.jar

4 将 tomcat-juli.jar 文件放置在 $TOMCAT_HOME\bin 目录中。

5 为 CATALINA_OPTS 中的 -Dlog4j.configuration 指定值，或者在 $TOMCAT_HOME\lib 目录中创建 log4j.properties 文件。

13.2 为 Identity Manager 安装单点登录

13.2.1 使用向导安装 One SSO Provider

以下过程介绍了如何使用安装向导在 Windows 平台上安装 OSP。要执行无提示或无人照管安装，请参见第 13.2.2 节 " 以无提示模式安装 One SSO Provider" （第 153 页）。要准备安装，请查看第 13.1.1 节 " 单点登录组件的核对清单 " （第 149 页）中列出的先决条件和系统要求。

1 以管理员身份登录到要安装 OSP 的服务器。

2 停止 Tomcat 服务器。

3 （视情况而定）如果您已获取 Identity Manager 安装包的 .iso 映像文件，请导航到包含 OSP 安装文件的目录 （默认为 products\CommonApplication\osp_install 目录）。

4 （视情况而定）如果您已下载 OSP 安装文件，请完成以下步骤：

   4a 导航到所下载映像的 win.zip 文件。

   4b 将该文件的内容解压缩到本地计算机上的某个目录中。

5 从包含安装文件的目录中运行 osp-install-win.exe 文件。

6 阅读并接受许可协议，然后单击下一步。

7 指定安装文件的路径。

8 使用以下参数完成引导式过程：

- **Tomcat 细节**

  表示 Tomcat 服务器的用户主目录。例如 C:\NetIQ\idm\apps\tomcat\。安装过程会将 OSP 的一些文件添加到此文件夹中。

- **Tomcat Java 主目录**

  表示 Java 在 Tomcat 服务器上的主目录。例如， C:\NetIQ\idm\jre。安装过程会将 OSP 的一些文件添加到此目录中。

- **应用程序地址**

  表示用户连接 Tomcat 服务器上的 OSP 时所需的 URL 的设置。例如， https://myserver.mycompany.com:8543。

  协议

  指定是要使用 *http* 还是 *https*。要使用安全套接字层 (SSL) 进行通讯，请指定 https。

主机名

指定要安装 OSP 的服务器的 DNS 名称或 IP 地址。请不要使用 localhost。

端口

指定您希望服务器在与客户端计算机通讯时所使用的端口。

- **登录屏幕自定义**

指定要在用户登录屏幕上显示的自定义名称。默认值为 **Identity Access**。

注释：仅支持 Latin1 标准字符集。

- **鉴定细节**

表示与包含可登录应用程序的用户列表的鉴定服务器连接时需要满足的要求。有关鉴定服务器的详细信息，请参见第 4.5.1 节 " 了解使用 One SSO Provider 进行鉴定的方法 "（第 33 页）。

LDAP 主机

指定 LDAP 鉴定服务器的 DNS 名称或 IP 地址。请不要使用 localhost。

LDAP 端口

指定您希望 LDAP 鉴定服务器在与 Identity Manager 通讯时所使用的端口。例如，指定 389 作为非安全端口，或者为 SSL 连接指定 636。

使用 SSL

指定是否要为身份库与鉴定服务器之间的连接使用安全套接字层协议。

JRE 可信证书存储区 (cacerts) 文件

仅当您要为 LDAP 连接使用 SSL 时才适用。

指定证书的路径。例如， C:\NetIQ\idm\apps\jre\lib\security\cacerts。

JRE 可信证书存储区口令

仅当您要为 LDAP 连接使用 SSL 时才适用。

指定 cacerts 文件的口令。

管理员 DN

仅在安装新鉴定服务器时适用。

指定 LDAP 鉴定服务器管理员帐户的 DN。例如：cn=admin,ou=sa,o=system。

管理员口令

仅在安装新鉴定服务器时适用。

指定 LDAP 鉴定服务器管理员帐户的口令。

用户容器

仅在安装新鉴定服务器时适用。

指定 LDAP 鉴定服务器中要储存可登录 Access Review 的用户帐户的容器。例如：o=data。

管理员容器

仅在安装新鉴定服务器时适用。

指定 LDAP 鉴定服务器中要储存管理员帐户的容器。例如：ou=sa,o=system。

身份库

指定您的身份库。

密钥储存区口令

仅在安装新鉴定服务器时适用。

指定要为 LDAP 鉴定服务器的新密钥存储区创建的口令。

该口令必须至少包含六个字符。

- **审计细节 (OSP)**

表示用于审计鉴定服务器中发生的 OSP 事件的设置。

（视情况而定）*对 OSP 启用审计*

指定是否要将 OSP 事件发送到审计服务器。

如果选择此设置，则还需指定审计日志超速缓存的位置。

审计日志超速缓存文件夹

仅当为 OSP 启用了审计时才适用。

指定要用于审计的超速缓存目录的位置。例如 C:\NetIQ\idm\naudit\jcache。

指定现有证书 / 生成证书

指定是要使用 NAudit 服务器的现有证书，还是创建新的证书。

输入公共密钥

仅当您要使用现有证书时才适用。

列出您希望 NAudit 服务用来鉴定审计讯息的自定义公共密钥证书。

输入 RSA 密钥

仅当您要使用现有证书时才适用。

指定您希望 NAudit 服务用来鉴定审计讯息的自定义私用密钥文件的路径。

9 要安装 SSPR，请继续第 14 部分 " 安装口令管理组件 " （第 155 页）。

有关配置忘记口令管理的详细信息，请参见第 15.7.8 节 " 配置忘记口令管理 " （第 199 页）。

13.2.2 以无提示模式安装 One SSO Provider

无提示 （非交互式）安装不显示用户界面，也不向用户提出任何问题。

1 以管理员身份登录到要安装这些组件的计算机。

2 停止 Tomcat。

3 （视情况而定）如果您已获取 Identity Manager 安装包的 .iso 映像文件，请导航到包含 OSP 安装文件的目录 （默认为 osp 目录）。

4 （视情况而定）如果您已从 NetIQ 下载网站下载了安装文件，请完成以下步骤：

   4a 导航到所下载映像的 .zip 文件。

   4b 将该文件的内容解压缩到本地计算机上的某个文件夹中。

5 将 osp.configure.properties 文件复制到您有权写入的位置，然后编辑此文件。

有关安装设置的详细信息，请参见步骤 7 和步骤 8 （第 151 页）。

6 要运行无提示安装，请发出以下命令：

osp-install-win.exe -i silent -f *path_to_silent.properties_file*

在此命令中，请指定文件的绝对路径。例如：

osp-install-win.exe -i silent -f *c:\NetIQ\idm\apps\osp\osp.silent.properties*

7 安装 SSPR。有关详细信息，请参见第 14 部分 " 安装口令管理组件 " （第 155 页）。

13.2.3 配置单点登录访问

在安装 OSP 后，需要立即执行一些操作来配置单点登录访问。但是，最终的配置过程需要您先安装 Identity Applications。有关详细信息，请参见第 VIII 部分 " 在 Identity Manager 中配置单点登录访问 " （第 277 页）。

注释：在无提示模式下配置 One SSO Provider 时，请务必在 osp.silent.properties 文件中指定正确的安装、 Java、 Tomcat 和 SSL 密钥存储区文件夹路径。例如：

安装文件夹：USER_INSTALL_DIR=C:\NetIQ\idm\apps\osp

Tomcat 文件夹：NETIQ_TOMCAT_HOME=C:\NetIQ\idm\apps\tomcat

Windows：NETIQ_TOMCAT_HOME=C:\NetIQ\idm\apps\tomcat

Java 文件夹：NETIQ_JAVA_HOME=C:\NetIQ\idm\apps\jre

SSL 密钥存储区文件夹：USER_INSTALL_DIR=C:\NetIQ\idm\apps\jre\lib\security\cacerts

---

14 安装口令管理组件

本章将介绍如何安装 Self Service Password Reset (SSPR)，该工具可帮助您将 Identity Manager 配置为允许用户重设置其口令。

SSPR 与 Identity Applications、 Identity Reporting 和 OSP 相集成，可确保需要修改口令的用户无需执行任何额外操作，就能定向到相应的网页。在用户完成其自助活动后， SSPR 会将用户重定向到他们最初尝试访问的应用程序。

注释：Identity Manager 4.6 及以上版本使用 SSPR 作为主要的口令管理工具。

Identity Manager 不要求安装 SSPR。您可以使用其他方法来重设置用户口令，但可能需要修改 Identity Manager 的一些配置设置。有关详细信息，请参见第 15.7.8 节 " 配置忘记口令管理 " （第 199 页）。

安装文件位于 \products\CoomonApplication\sspr_install 目录中。默认情况下，安装程序将在 C:\NetIQ\idm\apps\sspr 中安装 SSPR 组件。

NetIQ 建议您在开始之前，先查看安装过程。

14.1 为 Identity Manager 规划安装口令管理

本节提供安装 Self Service Password Reset (SSPR) 所需的先决条件、注意事项和系统设置信息。

14.1.1 安装口令管理组件的核对清单

NetIQ 建议您完成以下核对清单中的步骤：

	核对清单项目
❑	1. 了解 Identity Manager 各组件之间的交互。有关详细信息，请参见第 4.4 节 " 使用 Identity Manager 中的自助式口令管理 " （第 31 页）。
❑	2. 确定要为 Identity Manager 组件使用哪些服务器。有关详细信息，请参见第 5.3 节 " 建议的安装方案和服务器设置 " （第 39 页）。
❑	3. 确保已安装 Tomcat。有关详细信息，请参见第 12.2 章 " 安装 PostgreSQL 和 Tomcat" （第 143 页）。

	核对清单项目
❑	4. （视情况而定）要使用 Apache Log4j 服务来记录 Tomcat 中的事件，请确保您有相应的文件。有关详细信息，请参见第 13.1.4 节 “ 使用 Apache Log4j 服务记录登录 ” （第 150 页）。
❑	5. 安装 SSPR： ◆ 要执行引导式安装，请参见第 14.2.1 节 “ 使用向导安装 Self Service Password Reset” （第 157 页）。 ◆ 要执行无提示安装，请参见第 14.2.2 节 “ 以无提示模式安装 Self Service Password Reset” （第 160 页）。
❑	6. 安装 Identity Applications 并将其配置为使用单点登录访问和口令管理。有关详细信息，请参见第 15.5 章 “ 安装 Identity Applications” （第 180 页）。

14.1.2 Self Service Password Reset 的安装先决条件

NetIQ Self Service Password Reset (SSPR) 的安装应符合 Identity Applications 的服务器要求，同时请注意以下事项：

- SSPR 要求使用 TSL/SSL 协议进行通讯。
- SSPR 要求使用受支持版本的 Tomcat 应用程序服务器。有关详细信息，请参见第 12.1.4 节 “Tomcat 的安装先决条件 ” （第 143 页）和此版本的最新 《发行说明》。
- NetIQ 建议您查看 *《NetIQ Self Service Password Reset Administration Guide》*（NetIQ Self Service Password Reset 管理指南）中列出的先决条件和要求。

14.1.3 Self Service Password Reset 的系统要求

SSPR 需要 Apache Tomcat 应用程序服务器。 Tomcat 的版本必须为 Identity Applications 所需的版本。

所有其他服务器要求与 Identity Applications 的服务器要求一致。有关详细信息，请参见第 15.1.3 节 “ 安装 Identity Applications 的先决条件和注意事项 ” （第 167 页）和此版本的最新 《发行说明》。

14.1.4 针对口令事件使用 Apache Log4j 服务

您可以使用 Apache Log4j 或 java.util.logging 服务来记录 Tomcat 中发生的事件。Identity Manager 安装套件中的 Tomcat 安装程序包含 Log4j 所需的文件。但是，如果您安装自己的 Tomcat 版本，则需要借助以下文件来使用 Apache 日志记录服务：

- log4j-1.2.16.jar
- tomcat-juli-adapters.jar
- tomcat-juli.jar

要将这些文件添加到 Tomcat 安装中，请完成以下步骤：

1 从 Apache 网站下载 Tomcat 8.5.x 的 “JULI” 文件：
   - tomcat-juli.jar
   - tomcat-juli-adapters.jar

2 从 Apache 网站下载 log4j-1.2.16.jar 文件。

3 将以下文件放在 $TOMCAT_HOME\lib 目录中：

- log4j-1.2.16.jar
- tomcat-juli-adapters.jar

4 将 tomcat-juli.jar 文件放置在 $TOMCAT_HOME/bin 目录中。

5 为 CATALINA_OPTS 中的 -Dlog4j.configuration 指定值，或者在 $TOMCAT_HOME\lib 目录中创建 log4j.properties 文件。

14.2 为 Identity Manager 安装口令管理

本节介绍 SSPR 的安装过程。您可以将这些程序安装在安装了 OSP 组件的同一台服务器上，也可以安装在单独的服务器上。

注释：如果您使用传统的忘记口令方法，则不需要安装 SSPR。有关详细信息，请参见第 4.4.2 节 " 了解旧式口令管理提供程序 " （第 32 页）。

14.2.1 使用向导安装 Self Service Password Reset

以下过程介绍了如何使用安装向导在 Windows 平台上安装 SSPR。要执行无提示或无人照管安装，请参见第 14.2.2 节 " 以无提示模式安装 Self Service Password Reset" （第 160 页）。要准备安装，请查看第 14.1.1 节 " 安装口令管理组件的核对清单 " （第 155 页）中列出的先决条件和系统要求。

1 以管理员用户身份登录要安装 SSPR 的服务器。

2 停止 Tomcat 服务器。

3 （视情况而定）如果您已获取 Identity Manager 安装包的 .iso 映像文件，请导航到包含 SSPR 安装文件的目录 （默认为 products\CommonApplication\sspr_install 目录）。

4 （视情况而定）如果您已下载 SSPR 安装文件，请完成以下步骤：

   4a 导航到所下载映像的 win.zip 文件。

   4b 将该文件的内容解压缩到本地计算机上的某个目录中。

5 从包含安装文件的目录中运行 sspr-install-win.exe 文件。

6 阅读并接受许可协议，然后单击下一步。

7 指定安装文件的路径。

8 使用以下参数完成引导式过程：

- **Tomcat 细节**

  表示 Tomcat 服务器的用户主目录。例如 C:\NetIQ\idm\apps\tomcat。安装进程会将 SSPR 的一些文件添加到此文件夹中。

- **Tomcat 连接**

  表示用户连接 Tomcat 服务器上的 SSPR 时所需的 URL 的设置。例如， https://myserver.mycompany.com:8080。

注释：如果存在以下注意事项，则您还必须选择连接外部鉴定服务器并指定外部服务器的值：

- 您正在安装 SSPR。
- OSP 与 SSPR 在不同的受支持应用程序服务器实例上运行。

协议

指定是要使用 *http* 还是 *https*。要使用安全套接字层 (SSL) 进行通讯，请指定 https。

主机名

指定要安装 SSPR 的服务器的 DNS 名称或 IP 地址。请不要使用 localhost。

端口

指定您希望服务器在与客户端计算机通讯时所使用的端口。

连接外部鉴定服务器

指定是否要用不同的 Tomcat 实例来托管鉴定服务器 (OSP)。鉴定服务器包含可登录 SSPR 的用户的列表。

如果选择此设置，则还要指定鉴定服务器的协议、主机名和端口值。

- **Tomcat Java 主目录**

  表示 Java 在 Tomcat 服务器上的主目录。例如， C:\NetIQ\idm\jre。安装过程会将 OSP 的一些文件添加到此目录中。

- **鉴定细节**

  表示与包含可登录应用程序的用户列表的鉴定服务器连接时需要满足的要求。有关鉴定服务器的详细信息，请参见第 4.5.1 节 “ 了解使用 One SSO Provider 进行鉴定的方法 ”（第 33 页）。

LDAP 主机

指定 LDAP 鉴定服务器的 DNS 名称或 IP 地址。请不要使用 localhost。

LDAP 端口

指定您希望 LDAP 鉴定服务器在与 Identity Manager 通讯时所使用的端口。例如，指定 389 作为非安全端口，或者为 SSL 连接指定 636。

使用 SSL

指定是否要为身份库与鉴定服务器之间的连接使用安全套接字层协议。

JRE 可信证书存储区 (cacerts) 文件

仅当您要为 LDAP 连接使用 SSL 时才适用。

指定证书的路径。例如， C:\NetIQ\idm\apps\jre\lib\security\cacerts。

JRE 可信证书存储区口令

仅当您要为 LDAP 连接使用 SSL 时才适用。

指定 cacerts 文件的口令。

管理员 DN

仅在安装新鉴定服务器时适用。

指定 LDAP 鉴定服务器管理员帐户的 DN。例如：cn=admin,ou=sa,o=system。

管理员口令

仅在安装新鉴定服务器时适用。

指定 LDAP 鉴定服务器管理员帐户的口令。

用户容器

仅在安装新鉴定服务器时适用。

指定 LDAP 鉴定服务器中要储存可登录 Access Review 的用户帐户的容器。例如：o=data。

管理员容器

仅在安装新鉴定服务器时适用。

指定 LDAP 鉴定服务器中要储存 Access Review 管理员帐户的容器。例如：ou=sa,o=system。

密钥储存区口令

仅在安装新鉴定服务器时适用。

指定要为 LDAP 鉴定服务器的新密钥存储区创建的口令。

该口令必须至少包含六个字符。

- **SSPR 细节**

表示配置 SSPR 所需的设置。

配置口令

指定要为管理员创建的、用于配置 SSPR 的口令。

默认情况下，SSPR 没有配置口令。如果不指定口令，任何能够登录 SSPR 的用户都可以修改配置设置。

SSPR 重定向 URL

指定在 SSPR 中完成口令更改或询问问题等操作后，客户端要重定向到的绝对 URL。例如，转到仪表板。

使用以下格式：protocol://server:port/path。例如， http://*IDM_userapp_ 服务器 _IP: 端口号* /idmdash/#/landing。

- **鉴定服务器细节**

表示您要创建的供 SSPR 服务在连接到服务器上的 OSP 客户端时使用的口令。该口令又称为客户端机密。

要在安装后修改此口令，请使用 RBPM 配置实用程序。

- **审计细节 (SSPR)**

表示用于审计鉴定服务器中发生的 SSPR 事件的设置。

（视情况而定）*对 SSPR 启用审计*

指定是否要将 SSPR 事件发送到审计服务器。

如果选择此设置，则还要指定系统日志服务器的设置。

系统日志主机名

仅当为 SSPR 启用了审计时才适用。

指定托管系统日志服务器的服务器的 DNS 或 IP 地址。请不要使用 localhost。

系统日志端口

仅当为 SSPR 启用了审计时才适用。

指定托管系统日志服务器的服务器的端口。

9 要将 Identity Applications 和 Identity Reporting 配置为使用 SSPR，请继续第 15 章 " 安装 Identity Applications" （第 165 页）。

10 在配置更新实用程序中，更新 SSO 客户端参数。有关更多信息，请参见 Self Service Password Reset （第 221 页）。

有关配置忘记口令管理的详细信息，请参见第 15.7.8 节 " 配置忘记口令管理 " （第 199 页）。

14.2.2 以无提示模式安装 Self Service Password Reset

无提示 （非交互式）安装不显示用户界面，也不向用户提出任何问题。

1 以管理员身份登录到要安装这些组件的计算机。

2 停止 Tomcat。

3 （视情况而定）如果您已获取 Identity Manager 安装包的 .iso 映像文件，请导航到包含 SSPR 安装文件的目录 （默认为 sspr 目录）。

4 （视情况而定）如果您已从 NetIQ 下载网站下载了安装文件，请完成以下步骤：

   4a 导航到所下载映像的 .zip 文件。

   4b 将该文件的内容解压缩到本地计算机上的某个文件夹中。

5 针对 SSPR 安装编辑 sspr-silent.properties 文件。默认情况下，该文件与安装脚本位于同一目录中。

   有关安装设置的详细信息，请参见步骤 7 （第 157 页）和步骤 8 （第 157 页）。

6 要运行无提示安装，请发出以下命令：

```
sspr-install-win.exe -i silent -f path_to_silent.properties_file
```

7 在配置更新实用程序中，更新 SSO 客户端参数。有关更多信息，请参见 Self Service Password Reset （第 221 页）。

14.2.3 安装后任务

确保无错安装

安装 SSPR 后，您便可修改配置设置，例如更改默认配置文件的 LDAP 组 DN 的管理员许可权限，或更改转发 URL。此外， NetIQ 还建议您校验安装进程创建的 URL，并视需要进行更改。

1 要打开 SSPR 登录页面，请在浏览器中输入以下 URL：

   protocol://server:port/web-context

   例如：

   http://192.168.0.1:8080/sspr/

2 在 SSPR 登录页面的右上角，从列表中选择**配置编辑器**。

3 指定配置口令并单击**登录**。

4 在树视图中选择**默认设置**，并确保在 **LDAP 供应商默认设置**列表中选择了 **NetIQ IDM/OAuth 集成**。

5 在树视图中，单击 **LDAP > LDAP 目录 > 默认 > 连接 > LDAP 证书**，然后单击**从服务器导入**以导入证书。

   （视情况而定）在同一页面上单击**测试 LDAP 配置文件**，确保可以访问所有已配置的 LDAP 服务器。

6 在树视图中，单击**模块 > 已鉴定 > 管理**，并确保已将管理员许可权限指派给默认配置文件的 LDAP 组 DN。

   如果执行的是 SSPR 全新安装，则该列表将为空。需要在 iManager 中创建一个新组，并将 admin 用户添加到该组。

7 在树视图中，单击**设置 > 应用程序 > 应用程序**，并确保**转发 URL** 设置为 http://*<Server:Port>*/idmdash/#/landing。

   例如 http:/192.168.0.1:8080/idmdash/#/landing。

8 在树视图中，单击**设置 > 用户界面 > 外观**，然后将**界面主题**更改为 **Micro Focus (mdefault)**（如果尚未指定）。

9 在树视图中，单击**设置 > 单点登录 (SSO) 客户端 > OAuth**，然后校验是否为以下参数指定了正确的值：

   OAuth 登录 URL

   指定 OAuth 服务器登录的 URL。当用户登录时，此 URL 会将用户重定向以向 OSP 进行鉴定。

   例如 http://192.168.0.1:8080/osp/a/idm/auth/oauth2/grant

   OAuth 代码解析服务 URL

   指定 OAuth 代码解析服务的 URL。SSPR 使用此 Web 服务 URL 来解析 OAuth 身份服务器返回的项目。

   例如 http://192.168.0.1:8080/osp/a/idm/auth/oauth2/authcoderesolve

   OAuth 配置文件服务 URL

   指定 Identity Manager 提供的用于返回用户属性数据的 Web 服务 URL。

   例如 http://192.168.0.1:8080/osp/a/idm/auth/oauth2/getattributes

   OAUTH Web 服务服务器证书

   （视情况而定）如果已启用 HTTPS，请导入 OAuth Web 服务服务器的证书。

   OAuth 客户端 ID

   指定 OAuth 客户端的客户端 ID。例如， sspr.

   OAuth 共享机密

   指定 OAuth 共享机密的口令。此口令在 OSP 和 SSPR 应用程序间共享。

   OAuth 用户名 //DN 登录属性

   指定 SSPR 用来请求 OAuth 服务器在本地鉴定用户的用户属性。例如 name。

10 在页面右上角单击 以保存配置。

11 在 SSPR 登录页面的右上角，从列表中选择**配置管理器**。

12 单击**限制配置**。

将通用口令策略指派给用户容器

要将通用口令策略指派给用户容器，请执行以下操作：

1 登录到 iManager。
2 选择角色和任务 > 口令策略，然后选择口令策略。
3 要选择具有管理权限的用户，请执行以下操作：
   3a 单击通用口令 > 配置选项 > 通用口令检索。
   3b 选择允许管理员检索口令或允许以下用户检索口令，然后单击确定。
   例如， cn=uaadmin,ou=sa,o=data
4 单击策略指派，然后将容器指派给该用户所在的容器。
   例如， o=data 或管理用户。

授予对 pwmResponseSet 属性的权限

权限经过鉴定的用户可以根据与用户连接相关联的许可权限执行操作。经过鉴定的用户需要对其自己的用户项拥有以下权限：

- [项权限] 的浏览权限
- pwmResponseSet 的读取、比较和写入权限

要授予对 pwmResponseSet 属性的权限，请执行以下步骤：

1 登录到 iManager。
2 单击 。
3 单击 iManager 服务器 > 配置 iManager。
4 单击杂项 > 启用 [this]。
5 单击 。
6 在树视图中，选择目录中所有用户的顶级容器。
7 单击当前级别复选框，然后单击操作 > 修改受托者。
8 在列表中单击 [This]，然后单击添加受托者。
9 单击应用。
10 对 [This] 受托者单击指派的权限。
11 单击添加属性，然后选中在纲要中显示所有属性复选框。
12 从列表中选择 pwmResponseSet。
   确保已选择 “ 写入 ”、“ 比较 ”、“ 读取 ” 和 “ 继承 ” 选项。
13 单击完成。

14.2.4 为群集配置 OSP 和 SSPR

Identity Manager 在 Tomcat 群集环境中支持 SSPR 配置。

配置 SSPR 以支持群集

执行以下步骤配置已安装在单独计算机上的 SSPR：

1 查看第 14.1.1 节 " 安装口令管理组件的核对清单 "（第 155 页）中的先决条件和系统要求。

2 按照第 14.2.1 节 " 使用向导安装 Self Service Password Reset"（第 157 页）中的说明操作，并确保在安装过程中考虑以下步骤。

   a. 在应用程序服务器连接页面中，选择**连接到外部鉴定服务器**，并提供安装了负载平衡器的服务器的 DNS 名称。

   b. 在鉴定细节页面中，提供 Identity Manager 引擎服务器的 IP 地址和端口。CA 证书的口令为 "changeit"。

   c. 完成 SSPR 安装后，更新 SSL 设置。有关详细信息，请参见第 29.8 节 " 更新 Self Service Password Reset 的 SSL 设置 "（第 306 页）。

3 要在群集的第一个节点中更新 SSPR 信息，请从 C:\NetIQ\idm\apps\UserApplication\configupdate.bat 起动配置实用程序。

   在随即打开的窗口中，单击 **SSO 客户端** > **Self Service Password Reset**，并为**客户端 ID**、**口令**和 **OSP OAuth 重定向 URL** 参数输入值。

在群集节点上配置任务

在群集节点上执行以下配置任务：

1 要用 SSPR IP 地址更新 " 忘记口令 " 链接，请在第一个节点上登录 User Application，然后单击**管理** > **忘记口令**。

   有关 SSPR 配置的详细信息，请参见第 15.7.8 节 " 配置忘记口令管理 "（第 199 页）。

2 要更改 " 更改我的口令 " 链接，请参见针对分布式环境或群集环境更新仪表板中的 SSPR 链接（第 203 页）。

3 在群集中的其他节点上，校验 " 忘记口令 " 链接和 " 更改我的口令 " 链接是否已用 SSPR IP 地址更新。

   注释：如果已用 SSPR IP 地址更新 " 更改口令 " 链接和 " 忘记口令 " 链接，则不需要执行其他更改。

4 在第一个节点中，停止 Tomcat，并使用以下命令指定负载平衡器服务器的 DNS 名称来生成新的 osp.jks 文件：

   C:NetIQ\idm\apps\jre\bin\keytool -genkey -keyalg RSA -keysize 2048 -keystore osp.jks -storepass < 口令 > -keypass < 口令 > -alias osp -validity 1800 -dname "cn=< 负载平衡器 IP/DNS>"

   例如：C:NetIQ\idm\apps\jre\bin\keytool -genkey -keyalg RSA -keysize 2048 -keystore osp.jks -storepass changeit -keypass changeit -alias osp -validity 1800 -dname "cn=mydnsname"

   注释：确保密钥口令与在 OSP 安装期间提供的口令相同。或者，可以使用配置更新实用程序加入密钥存储区口令来更改该口令。

5 （视情况而定）要校验 osp.jks 文件是否已通过这些更改更新，请运行以下命令：

   C:NetIQ\idm\apps\jre\bin\keytool -list -v -keystore osp.jks -storepass changeit

6 备份位于 C:\NetIQ\idm\apps\osp 中的原始 osp.jks 文件，并将新的 osp.jks 文件复制到此位置。新 osp.jks 文件是在步骤 3 中创建的。

7 将第一个节点上位于 C:\NetIQ\idm\apps\osp\ 中的新 osp.jks 文件复制到群集中的所有其他 User Application 节点。

8 在第一个节点中起动配置实用程序，并在 “SSO 客户端 ” 选项卡下将所有 URL 设置 （例如登录页的 URL 链接和 OAuth 重定向 URL）更改为负载平衡器 DNS 名称。

8a 保存配置实用程序中所做的更改。

8b 要在群集的所有其他节点中反映此更改，请将第一个节点上位于 \TOMCAT_INSTALLED_HOME\conf 中的 ism-configuration properties 文件复制到所有其他 User Application 节点。

注释：您之前已将第一个节点上的 ism.properties 文件复制到群集中的其他节点上。如果您在 User Application 安装期间指定了自定义安装路径，请在群集节点中使用配置更新实用程序确保参照路径正确。

在此方案中， OSP 和 User Application 安装在同一台服务器上；因此，为重定向 URL 使用了相同的 DNS 名称。

如果 OSP 和 User Application 安装在不同的服务器上，请将 OSP URL 更改为指向负载平衡器的其他 DNS 名称。请对安装了 OSP 的所有服务器执行此操作。这可确保所有 OSP 请求均通过负载平衡器发送到 OSP 群集 DNS 名称。这涉及到为 OSP 节点建立一个单独的群集。

---

9 在 \TOMCAT_INSTALLED_HOME\bin\ 目录下的 setenv.bat 文件中执行以下操作：

9a 为确保 mcast_addr 绑定成功， JGroups 要求 preferIPv4Stack 属性设置为 **true**。为此，请在所有节点上的 setenv.bat 文件中添加 JVM 属性 “-Djava.net.preferIPv4Stack=true”。

9b 在第一个节点上的 setenv.bat 文件中添加 “-Dcom.novell.afw.wf.Engine-id=Engine”。

引擎名称应该唯一。提供在安装第一个节点的过程中指定的名称。如果未指定名称，则默认名称为 “Engine”。

同样，为群集中的其他节点添加唯一的引擎名称。例如，对于第二个节点，引擎名称可以是 Engine2。

10 在 User Application 中启用群集。有关更多信息，请参见步骤 10 （第 191 页）。

11 为群集启用许可权限索引。有关更多信息，请参见第 15.4.2 节 “ 为群集启用许可权限索引 ” （第 178 页）。

12 启用 Tomcat 群集。有关详细信息，请参见第 15.4.3 节 “ 为 Identity Applications 准备应用程序服务器 ” （第 178 页）中的 “ 步骤 9”。

13 在所有节点上重启动 Tomcat。

14 为群集配置 User Application 驱动程序。有关更多信息，请参见第 15.6.2 节 “ 为群集配置 User Application 驱动程序 ” （第 192 页）。

15 安装 Identity Applications

本部分将引导您完成安装 Identity Applications 所需组件和框架的过程：

- Identity Applications 管理
- Identity Applications 仪表板
- Role and Resource Service 驱动程序
- User Application
- 用户应用程序驱动程序

默认情况下，安装程序将在 C:\NetIQ\idm\apps 中安装这些组件。

在安装期间以及安装之后， Identity Applications 都需要访问其他 Identity Manager 组件。 NetIQ 建议您在开始之前，先查看安装过程。有关详细信息，请参见第 15.1 章 “ 规划安装 Identity Applications”（第 165 页）。

15.1 规划安装 Identity Applications

Identity Applications 安装包括以下组件：

- Identity Manager 仪表板
- Identity Manager 管理控制台
- User Application
- 角色和资源服务驱动程序 (RRSD)
- User Application 驱动程序 (UAD)

安装不包含 Identity Applications 所需的以下两个驱动程序：User Application 驱动程序和 Roles and Resource Services 驱动程序。

注释：从技术上讲，Identity Reporting 可被视为一种 Identity Applications，因为该组件也使用 SSPR 和 OSP，并且您可以使用 RBPM 配置实用程序修改其设置。但是， Identity Reporting 具有自己的安装程序，可安装在单独的服务器上，并使用不同的数据库。有关详细信息，请参见第 16.5 节 “Identity Reporting 的系统要求 ”（第 228 页）。

15.1.1 Identity Applications 安装核对清单

NetIQ 建议您在开始安装过程之前先查看以下步骤：

	核对清单项目
❑	1. 了解 Identity Manager 各组件之间的交互。有关详细信息，请参见第 4.3.1 节 “User Application 和 Roles Based Provisioning Module” （第 29 页）。
❑	2. 确定要为 Identity Manager 组件使用哪些服务器。有关详细信息，请参见第 5.3.4 节 “ 建议的服务器设置 ” （第 41 页）。
❑	3. 决定在安装 Identity Applications 之前是否应安装 Sentinel。有关详细信息，请参见第 5.3 节 “ 建议的安装方案和服务器设置 ” （第 39 页）。
❑	4. 确保已安装 Identity Manager 引擎。有关安装引擎的详细信息，请参见第 8 章 “ 规划引擎、驱动程序和插件的安装 ” （第 73 页）。
❑	5. 查看安装 Identity Applications 及其支持框架的注意事项，以确保您的服务器符合先决条件。有关详细信息，请参见第 15.1.3 节 “ 安装 Identity Applications 的先决条件和注意事项 ” （第 167 页）。
❑	6. 查看将要托管 Identity Applications 及其框架的计算机所要满足的硬件和软件要求。有关详细信息，请参见 Identity Applications 的系统要求 （第 171 页）。
❑	7. 确保 eDirectory 在默认 LDAP 端口 389 和 636 上运行，以避免收到有关纲要无效的错误讯息。您可以在安装后手动扩展 eDirectory 纲要。有关详细信息，请参见第 15.2.1 节 “ 将 User Application 纲要作为日志应用程序添加到审计服务器中 ” （第 173 页）。
❑	8. 在 eDirectory 身份库中创建一个 User Application 管理员帐户。有关详细信息，请参见第 15.2.2 节 “ 向身份库管理员和 User Application 管理员帐户指派权限 ” （第 173 页）。
❑	9. 在本地计算机或连接的服务器上为 Identity Applications 安装并配置一个数据库。 ◆ 要了解该数据库，请参见安装 Identity Applications 数据库的先决条件 （第 170 页）。 ◆ 要安装该数据库，请参见第 15.3 章 “ 配置 Identity Applications 的数据库 ”（第 175 页）。
❑	10. 在本地计算机上或在群集中准备好应用程序服务器。 ◆ 要了解相关要求，请参见应用程序服务器的先决条件和注意事项 （第 169 页）。 ◆ 要准备群集，请参见第 15.4 章 “ 为 Identity Applications 准备环境 ” （第 177 页）。 ◆ 要安装应用程序服务器，请参见第 15.4.3 节 “ 为 Identity Applications 准备应用程序服务器 ” （第 178 页）。
❑	11. （视情况而定）要使用 Apache Log4j 服务来记录 Tomcat 中的事件，请确保您有相应的文件。有关详细信息，请参见第 13.1.4 节 “ 使用 Apache Log4j 服务记录登录 ” （第 150 页）。
❑	12. 查看 Identity Applications 安装套件的内容，以确定您的环境需要哪些文件。有关详细信息，请参见第 15.1.2 节 “ 了解 Identity Applications 的安装程序 ” （第 167 页）。
❑	13. 创建并部署 User Application 驱动程序和 Roles and Resource Service 驱动程序。有关详细信息，请参见第 15.6 章 “ 创建和部署 Identity Applications 的驱动程序 ” （第 191 页）。
❑	14. 安装 Identity Applications。有关详细信息，请参见第 15.5 章 “ 安装 Identity Applications”（第 180 页）。

	核对清单项目
❑	15. 要执行安装过程中的最后几个任务，请参见第 15.7 章 " 完成 Identity Applications 的安装 " （第 194 页）。
❑	16. 确保已正确配置 Identity Applications 和单点登录设置。有关详细信息，请参见第 28 章 " 校验是否可对 Identity Applications 进行单点登录访问 " （第 293 页）。
❑	17. （可选）要开始使用 Identity Applications，请参见 《*NetIQ Identity Manager - Administrator's Guide to the Identity Applications*》（NetIQ Identity Manager - Identity Applications 管理员指南）。

15.1.2 了解 Identity Applications 的安装程序

Identity Applications 的安装文件位于安装包的 \products\UserApplication\ 目录中。

安装程序 (IdmUserApp.exe) 会执行以下操作：

- 指定要使用的现有应用程序服务器版本。
- 指定要使用的数据库现有版本。数据库用于储存 Identity Applications 的数据和配置信息。
- 配置 JDK 的证书文件，以便 Tomcat 上运行的 Identity Applications 能够安全地与身份库和 User Application 驱动程序通讯。
- 配置 User Application 的 Java Web 应用程序存档 (WAR) 文件，并将其部署到 Tomcat。
- 启用通过 Sentinel 审计客户端进行日志记录的功能 （如果您选择如此）。
- 允许导入现有主密钥，以恢复特定的 Identity Applications 安装，并为群集提供支持。

15.1.3 安装 Identity Applications 的先决条件和注意事项

NetIQ 建议您在开始执行安装过程之前，先查看 Identity Applications 的先决条件和计算机要求。有关配置 User Application 环境的详细信息，请参见 《*NetIQ Identity Manager - Identity Applications 用户指南*》。

- Identity Applications 的安装注意事项 （第 167 页）
- Identity Applications 的配置和用法注意事项 （第 169 页）
- 应用程序服务器的先决条件和注意事项 （第 169 页）
- 在群集环境中安装 Identity Applications 的先决条件 （第 170 页）
- 安装 Identity Applications 数据库的先决条件 （第 170 页）

Identity Applications 的安装注意事项

在安装 Identity Applications 时，请注意以下事项。

- 需要以下 Identity Manager 组件的受支持版本：
  - Designer
  - 身份库
  - Identity Manager 引擎

- Remote Loader
- 一个 SSO 提供程序

有关这些组件的所需版本和增补程序的详细信息，请参见最新的 《发行说明》。

- 确保身份库包括已创建且已部署的 User Application 以及 Roles and Resources Service 驱动程序。有关详细信息，请参见第 15.6 章 " 创建和部署 Identity Applications 的驱动程序 " （第 191 页）。
- 在安装 Identity Applications 之前，请安装以下框架项目：
  - 在本地计算机上安装一个应用程序服务器。有关详细信息，请参见应用程序服务器的先决条件和注意事项 （第 169 页）。
  - 在本地计算机或连接的服务器上安装一个数据库。有关详细信息，请参见安装 Identity Applications 数据库的先决条件 （第 170 页）。
- （可选） NetIQ 建议为 Identity Manager 组件之间的通讯启用安全套接字层 (SSL) 协议。要使用 SSL 协议，必须在您的环境中启用 SSL，并在安装期间指定 **https**。有关启用 SSL 的信息，请参见 《*NetIQ Analyzer for Identity Manager Administration Guide*》（NetIQ Analyzer for Identity Manager 管理指南）中的 "Configuring Security in the Identity Applications" （配置 Identity Applications 中的安全性）。
- 在创建角色和资源驱动程序之前创建 User Application 驱动程序。角色和资源驱动程序会参照 User Application 驱动程序中的角色库容器 (RoleConfig.AppConfig)。
- 您不能将 Role and Resource Service 驱动程序与 Remote Loader 配合使用，因为该驱动程序使用 jClient。
- 将 JAVA_HOME 环境变量设置为指向您想要与 Identity Applications 配合使用的 JDK。要覆盖 JAVA_HOME，请在安装期间手动指定路径。
- 默认情况下，安装过程会将程序文件放在 C:\NetIQ\idm 目录中。

  如果您打算在非默认位置安装 User Application，则新目录必须存在且可写。
- 每个 User Application 实例只能为一个用户容器提供服务。例如，您只能在与该实例关联的容器中添加用户、执行搜索和查询。此外，用户容器与应用程序之间的关联是永久性的。
- （视情况而定）如果您计划使用外部口令管理，您的环境必须符合以下要求：
  - 为要部署 Identity Applications 和 IDMPwdMgt.war 文件的 Tomcat 启用安全套接字层 (SSL) 协议。
  - 确保防火墙上打开了 SSL 端口。

  有关为 Tomcat 启用 SSL 的详细信息，请参见第 29.8 节 " 更新 Self Service Password Reset 的 SSL 设置 " （第 306 页）。

  有关 IDMPwdMgt.war 文件的详细信息，请参见第 15.7.8 节 " 配置忘记口令管理 " （第 199 页）。
- （可选）要从受管系统检索授权，请安装一个或多个 Identity Manager 驱动程序。
  - 必须使用 Identity Manager 3.6.1、 4.0 或更高版本所支持的驱动程序。有关安装驱动程序的详细信息，请参见 NetIQ Identity Manager 驱动程序文档网站中的相应驱动程序指南。
  - 要管理驱动程序，必须先安装 Designer 或适用的 iManager 插件。有关详细信息，请参见第 11.1.3 节 " 了解 iManager 插件的安装 " （第 127 页）。

Identity Applications 的配置和用法注意事项

在配置和初次使用 Identity Applications 时，请注意以下事项。

- 只有在您完成以下活动之后，用户才能访问 Identity Applications：
  - 确保已安装所有必要的 Identity Manager 驱动程序。
  - 确保身份库的索引处于联机模式。有关在安装期间配置索引的详细信息，请参见杂项 （第 212 页）。
  - 在所有浏览器上启用 Cookie。如果禁用了 Cookie，应用程序将不起作用。
- 在未登录到 Identity Applications 的情况下，用户无法以 guest 或匿名用户的身份访问 Identity Applications。系统将提示用户登录到用户界面。有关详细信息，请参见 第 VIII 部分 " 在 Identity Manager 中配置单点登录访问 " （第 277 页）。
- 为确保 Identity Manager 强制实施通用口令功能，请将身份库配置为在用户首次登录时使用 "NMAS 登录 "。将 NDSD_TRY_NMASLOGIN_FIRST 连带字符串值 true 添加到 HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\Environment 注册表项。
- （视情况而定）要运行报告，必须在环境中安装 Identity Reporting 的组件。有关详细信息，请参见 《Administrator Guide to NetIQ Identity Reporting》（NetIQ Identity Reporting 管理员指南）。
- 在安装过程中，安装程序会将日志文件写入安装目录。这些文件包含有关您的配置的信息。配置 Identity Applications 环境后，应考虑删除这些日志文件或将其储存在安全位置。在安装过程中，可以选择将数据库纲要写入到文件。由于此文件包含有关数据库的描述性信息，因此在安装过程完成后应将文件移至安全位置。
- （视情况而定）要审计 Identity Applications，必须在环境中安装并配置 Identity Reporting 和审计服务，以捕获事件。此外，还必须配置 Identity Applications，以便能够进行审计。有关详细信息，请参见 《NetIQ Identity Manager - Configuring Auditing in Identity Manager》（NetIQ Identity Manager - 在 Identity Manager 中配置审计）。

应用程序服务器的先决条件和注意事项

要使用 Identity Applications，需要安装 Tomcat，同时需注意以下事项：

- Tomcat 必须与 Java 开发包 (JDK) 或 Java 运行时环境 (JRE) 搭配运行。有关支持的版本的详细信息，请参见 Identity Applications 的系统要求 （第 171 页）。
- 将 JAVA_HOME 环境变量设置为指向您打算与 User Application 配合使用的 JDK。要覆盖 JAVA_HOME，请在安装期间手动指定路径。
- （视情况而定）您可以使用自己的 Tomcat 安装程序，而不使用 Identity Manager 安装套件中提供的安装程序。但是，要将 Apache Log4j 服务与您的 Tomcat 版本配合使用，请确保安装了相应的文件。有关详细信息，请参见第 13.1.4 节 " 使用 Apache Log4j 服务记录登录 " （第 150 页）。
- （视情况而定）要保留您数字签名的文档，必须在 Tomcat 应用程序服务器上安装 Identity Applications，并使用 Novell Identity Audit。数字签名文档不是随工作流程数据储存在 User Application 数据库中，而是储存在日志记录数据库中。此外，还必须启用日志记录才能保留这些文档。有关详细信息，请参见 《*NetIQ Identity Manager - Administrator's Guide to the Identity Applications*》（NetIQ Identity Manager - Identity Applications 管理员指南）中的 "Setting Up Logging in the Identity Applications"（在 Identity Applications 中设置日志记录）。

- （视情况而定）在要记录大量用户数据或您的目录服务器包含大量对象的环境中，您可能需要使用多个部署有 Identity Applications 的应用程序服务器。有关进行性能优化配置的详细信息，请参见《*NetIQ Identity Manager - Administrator's Guide to the Identity Applications*》（NetIQ Identity Manager - Identity Applications 管理员指南）中的 "Tuning the Performance of the Applications"（优化应用程序的性能）。
- （视情况而定）如果您使用 Tomcat 应用程序服务器，在完成安装过程之前，请勿启动该服务器。
- （视情况而定）要使用外部口令管理，必须执行以下操作来启用安全套接字层 (SSL) 协议：
  - 为要部署 Identity Applications 和 IDMPwdMgt.war 文件的 Tomcat 启用 SSL。
  - 确保防火墙上打开了 SSL 端口。

  有关 IDMPwdMgt.war 文件的详细信息，请参见配置忘记口令管理和《*NetIQ Identity Manager - Administrator's Guide to the Identity Applications*》（NetIQ Identity Manager - Identity Applications 管理员指南）。
- 安装进程不会修改 Tomcat 服务器上的 JAVA_HOME 或 JRE_HOME 条目。默认情况下， Tomcat 的便捷安装程序会将 setenv.bat 文件放在 C:\NetIQ\idm\apps\tomcat\bin\ 目录中。安装还会在该文件中配置 JRE 位置。

在群集环境中安装 Identity Applications 的先决条件

您可以在 Tomcat 群集支持的环境中安装 Identity Applications 的数据库，不过需要注意以下事项：

- 群集必须具有唯一的群集分区名称、多路广播地址和多路广播端口。使用唯一的标识符可以区分多个群集，防止出现性能问题和异常行为。
  - 对于群集的每个成员，必须为 Identity Applications 数据库的侦听端口指定相同的端口号。
  - 对于群集的每个成员，必须为托管 Identity Applications 数据库的服务器指定相同的主机名或 IP 地址。
- 必须同步群集中服务器的时钟。如果服务器时钟不同步，会话可能会提前超时，导致 HTTP 会话故障转移无法正常工作。
- NetIQ 建议不要在同一个主机上的浏览器选项卡或浏览器会话之间使用多个登录。某些浏览器在选项卡和进程之间共享 Cookie，因此，允许多个登录可能会导致 HTTP 会话故障转移出现问题（此外，如果多个用户共享一台计算机，还可能会给鉴定功能带来意外的风险）。
- 群集节点位于在同一个子网中。
- 故障转移代理或负载平衡解决方案安装在单独的计算机上。

有关在群集环境中配置 Identity Applications 的详细信息，请参见第 15.4 章 " 为 Identity Applications 准备环境 "（第 177 页）。

安装 Identity Applications 数据库的先决条件

该数据库储存 Identity Applications 数据和配置信息。

在安装数据库实例之前，请先查看以下先决条件：

- 要配置与 Tomcat 搭配使用的数据库，必须创建一个 JDBC 驱动程序。 Identity Applications 使用标准 JDBC 调用来访问并更新该数据库。 Identity Applications 使用绑定到 JNDI 树的 JDBC 数据源文件开启与数据库的连接。

- 必须有一个指向该数据库的现有数据源文件。 User Application 安装程序将在 server.xml 和 context.xml 中创建一个指向数据库的 Tomcat 数据来源条目。
- 确保具备以下信息：
  - 数据库服务器的主机和端口。
  - 要创建的数据库的名称。 Identity Applications 的默认数据库为 idmuserappdb。
  - 数据库用户名和口令。数据库用户名必须代表某个管理员帐户，或者必须具有在数据库服务器中创建表的足够许可权限。 User Application 的默认管理员是 idmadmin。
  - 数据库供应商为您所使用的数据库提供的驱动程序 .jar 文件。 NetIQ 不支持第三方供应商提供的驱动程序 JAR 文件。
- 数据库实例可以位于本地计算机上，也可以位于连接的服务器上。
- 数据库字符集必须使用 Unicode 编码。例如， UTF-8 就是一种使用 Unicode 编码的字符集，而 Latin1 则不使用 Unicode 编码。有关指定字符集的详细信息，请参见配置字符集 （第 177 页）或第 15.3.1 节 “ 配置 Oracle 数据库 ” （第 175 页）。
- 为了避免在迁移期间发生重复键错误，请使用区分大小写的排序规则。如果发生重复键错误，请检查排序规则并更正它，然后重安装 Identity Applications。
- （视情况而定）要将同一个数据库实例用于审计和 Identity Applications， NetIQ 建议在一个独立的专用服务器 （而非托管运行 Identity Applications 的 Tomcat 的服务器）上安装该数据库。
- （视情况而定）如果正要迁移到新版 Identity Applications，必须使用之前安装所用的同一个数据库。
- 数据库群集属于各相关数据库服务器的功能。 NetIQ 不提供对任何群集数据库配置的官方测试，因为群集与产品功能不相关。因此，我们在支持群集数据库服务器的同时，作出以下声明：
  - 默认情况下，最大连接数设置为 100。此值可能太低，无法处理群集中的工作流程请求负载。您可能会看到以下异常：

    ```
    (java.sql.SQLException: Data source rejected establishment of connection,
    message from server: "Too many connections."
    ```

    要增加最大连接数，请在 my.cnf 文件中将 max_connections 变量设置为更高的值。
  - 您可能需要禁用群集数据库服务器的某些功能或方面。例如，由于在尝试插入重复键时存在约束违规，所以必须对某些表禁用事务复制。
  - 我们对于群集数据库服务器的安装、配置或优化不提供任何协助，包括将我们的产品安装到群集数据库服务器中。
  - 我们会尽最大努力来解决在群集数据库环境中使用我们的产品时可能出现的任何问题。在复杂环境中采用的查错方法通常需要双方合作才能解决问题。 NetIQ 提供了专业知识，便于您对 NetIQ 产品进行分析、规划及查错。客户必须具有对任何第三方产品进行分析、规划及查错的专业知识。我们将要求客户在非群集环境中再现问题或分析其组件的行为，以帮助从 NetIQ 产品问题中分离出潜在的群集设置问题。

15.1.4 Identity Applications 的系统要求

本节介绍安装 Identity Applications 的最低要求。

类别	要求
处理器	1 GHz

类别	要求
磁盘空间	1 GB **注释：**为支持应用程序的内容 （例如数据库和应用程序服务器日志）留出足够的空间 .
内存	4 GB
操作系统 （经认可）	以下 64 位操作系统之一： ◆ Windows Server 2016 ◆ Windows Server 2012 R2 ◆ Windows Server 2012 ◆ Windows Server 2008 R2 对于 32 位操作系统： ◆ Windows Server 2008 SP2 NetIQ 建议您在安装 Identity Manager 之前，按照制造商的自动更新工具应用最新的操作系统增补程序。 **注释：***经认可*指操作系统已经过全面测试且受支持。
操作系统 （受支持）	经认可操作系统的最新版服务包 **注释：***受支持*指操作系统尚未经过测试，但预期可以正常工作。
虚拟化系统	◆ VMWare ESX 5.5 及更高版本 NetIQ 支持在为运行 NetIQ 产品的操作系统提供官方支持的企业级虚拟化系统上安装 Identity Manager。只要虚拟化系统的供应商为这些操作系统提供官方支持， NetIQ 就可支持这些系统上的整个 Identity Manager 堆栈。
数据库	◆ PostgreSQL 9.6.6 ◆ Orcale 12c ◆ MsSQL 2016、 2014 **注释：**请勿在 Tomcat 的类路径中包含 PostgreSQL 版本 （例如 9.6.6）。如果指定这些版本，系统可能不会装载主页图像。
Web 浏览器	以下任意浏览器 （最低版本）： ◆ Google Chrome 61 ◆ Mozilla Firefox 51 **注释：**必须在浏览器中启用 Cookie。
应用程序服务器	Apache Tomcat 8.5.27
Java	JRE 1.8.0_162
端口	8180

15.2 为 Identity Applications 准备身份库

本节将帮助您为安装 Identity Applications 做好准备。该应用程序在名为 Roles Based Provisioning Module (RBPM) 的框架上运行。当您安装 Identity Manager 引擎时，安装过程会自动安装 netiq-DXMLuad-4.7.0-0.noarch，而该程序会安装 User Application 驱动程序以及角色和资源驱动程序，并扩展 eDirectory 纲要以便与 RBPM 交互。

安装文件位于 Identity Manager 安装包的 .iso 映像文件中的 products\UserApplication\ 目录下。

- 第 15.2.1 节 " 将 User Application 纲要作为日志应用程序添加到审计服务器中 "（第 173 页）
- 第 15.2.2 节 " 向身份库管理员和 User Application 管理员帐户指派权限 "（第 173 页）

15.2.1 将 User Application 纲要作为日志应用程序添加到审计服务器中

如果审计服务器要将 User Application 用作日志应用程序，则您必须将 dirxml.lsc 文件复制到该服务器。本节仅适用于 Novell Identity Audit。

1. 找到 dirxml.lsc 文件。

   安装后，此文件位于 Identity Manager User Application 安装目录中，例如 C:\NetIQ\idm\apps\UserApplication。
2. 使用 Web 浏览器访问装有 Novell Identity Audit 插件的 iManager，然后以管理员身份登录。
3. 浏览到**角色和任务 > 审计和日志记录**，然后选择**日志服务器选项**。
4. 浏览到树中的 " 日志记录服务 " 容器，选择相应的审计安全日志服务器，然后单击**确定**。
5. 在**日志应用程序**选项卡中，选择相应的容器名称，然后单击**新建日志应用程序**链接。
6. 在 " 新建日志应用程序 " 对话框中完成以下步骤：

   6a 对于 " 日志应用程序名称 "，请根据您的环境指定有意义的任何名称。

   6b 对于 " 导入 LSC 文件 "，请浏览到 dirxml.lsc 文件。

   6c 单击**确定**。
7. 单击 " 确定 " **完成 Audit 服务器配置。**
8. 确保将 " 日志应用程序 " 中的状态设置为**开**。（状态下方的圆圈应为绿色。）
9. 重启动 Audit 服务器以激活新的日志应用程序设置。

15.2.2 向身份库管理员和 User Application 管理员帐户指派权限

身份库管理员是有权配置身份库的用户。这是可与其他管理用户类型共享的逻辑角色。

身份库管理员需要以下权限：

- 对 User Application 驱动程序及其包含的所有对象的 " 主管 " 权限。要实现此目的，可在驱动程序容器级别设置权限，并将这些权限设为可继承。
- 对通过目录抽象层用户实体定义所定义的任何用户的"主管输入"权限。这应该包括对 objectClass 以及与 DirXML-EntitlementRecipient、 srvprvEntityAux 和 srvprvUserAux 辅助类关联的任何属性的 " 写入属性 " 权限。

- 对容器对象 cn=DefaultNotificationCollection, cn=Security 的“主管”权限。此对象保存用于自动供应电子邮件的电子邮件服务器设置。它可以包含对电子邮件服务器本身进行鉴定所用的 SecretStore 身份凭证。
- 对容器对象 cn=Authorized Login Methods, cn=Security 的 “ 主管 ” 权限。在安装 User Application 期间，系统会在此容器中创建 SAML 声明对象。
- 在安装 User Application 之前，请确保您对 cn=Security 容器拥有主管权限。在安装 User Application 期间，系统会在 cn=Security 容器下创建 cn=RBPMTrustedRootContainer 容器。

  或者，您可以手动创建 cn=RBPMTrustedRootContainer,cn=Security 容器 （创建名为可信根容器的对象，并在其 Security 容器中包含 NDSPKI:Trusted Root 对象类），然后指派对该容器的主管权限。

必须在 身份库中手动创建 User Application 管理员帐户，才能正确安装 Roles Based Provisioning Module。 User Application 管理员帐户必须是顶层容器的受托者，并且必须对该容器具有主管权限。

在创建 User Application 管理员帐户时，必须为此新用户帐户指派口令策略。有关详细信息，请参见《*Password Management Administration Guide*》（口令管理管理指南）中的 “Creating Password Policies” （创建口令策略）。

要为 User Application 管理员帐户创建许可权限，请在 LDAP 数据交换格式 (LDIF) 文件中运行以下命令：

```
dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 1#subtree#[Root]#[Entry Rights]
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#description
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#directReports
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#mail
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#manager
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#photo
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#srvprvQueryList
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#srvprvUserPrefs
```

```
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#telephoneNumber
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#title

dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 17#subtree#%%RBPM_USER_APP_ADMIN_DN%%#[Entry Rights]
ACL: 35#subtree#%%RBPM_USER_APP_ADMIN_DN%%#[All Attributes Rights]
```

15.3 配置 Identity Applications 的数据库

Identity Applications 的数据库支持多种任务，例如，储存配置数据和工作流程活动的数据。在安装应用程序之前，必须先安装并配置数据库。有关支持的数据库的详细信息，请参见第 15.1.4 节 “Identity Applications 的系统要求 ”（第 171 页）。有关 User Application 数据库注意事项的详细信息，请参见安装 Identity Applications 数据库的先决条件 （第 170 页）。

注释：如果要迁移到新版 RBPM 和 Identity Applications，必须使用之前安装所用的同一个数据库。“之前安装 ” 是指您要迁移的安装。

15.3.1 配置 Oracle 数据库

本节为 User Application 使用 Oracle 数据库提供了所需的配置选项。有关支持的 Oracle 版本的信息，请参见Identity Applications 的系统要求 （第 171 页）。

检查数据库的兼容性级别

来自不同 Oracle 版本的数据库兼容的前提为，这些数据库支持相同的功能且这些功能以相同的方式执行。如果它们不兼容，则某些功能或操作可能不会按预期工作。例如，创建纲要会失败，导致您无法部署 Identity Applications。

要检查数据库的兼容性级别，请执行以下步骤：

1. 连接数据库引擎。
2. 连接到 SQL Server 数据库引擎的适当实例后，在**对象资源管理器**中单击服务器名称。
3. 展开**数据库**，然后根据数据库选择用户数据库，或者展开**系统数据库**并选择一个系统数据库。
4. 右键单击数据库，然后单击**属性**。

   数据库属性对话框随即打开。
5. 在**选择页面**窗格中，单击**选项**。

   当前兼容性级别显示在**兼容性级别**列表框中。

6. 要检查兼容性级别，请在查询窗口中输入以下内容，然后单击执行。

   SQL> SELECT name, value FROM v$parameter

   WHERE name = 'compatible';

预期输出为：12.1.0.2

配置字符集

User Application 数据库必须使用 Unicode 编码的字符集。在创建数据库时，请使用 AL32UTF8 指定此字符集。

要确认是否为 Oracle 12c 数据库设置 UTF-8，请发出以下命令：

```
select * from nls_database_parameters;
```

如果数据库未配置为 UTF-8，系统将使用以下信息进行响应：

```
NLS_CHARACTERSET
WE8MSWIN1252
```

否则，系统将使用以下信息进行响应，确认为数据库配置了 UTF-8：

```
NLS_CHARACTERSET
AL32UTF8
```

注释：建议使用 JDBC JAR 版本 ojdbc6.jar。

有关配置字符集的详细信息，请参见 “Choosing an Oracle Database Character Set” （选择 Oracle 数据库字符集）。

配置管理员用户帐户

User Application 要求 Oracle 数据库用户帐户具有特定的特权。在 SQL Plus 实用程序中输入以下命令：

```
CREATE USER idmuser IDENTIFIED BY password
GRANT CONNECT, RESOURCE to idmuser
ALTER USER idmuser quota 100M on USERS;
```

其中， *idmuser* 表示用户帐户。

15.3.2 配置 PostgreSQL 数据库

方便起见， NetIQ 为 PostgreSQL 提供了一个安装程序，该程序完全支持 Identity Manager 中的框架服务和应用程序。该安装程序可引导您完成配置过程。有关详细信息，请参见第 12.2 章 “ 安装 PostgreSQL 和 Tomcat” （第 143 页）。

15.3.3 配置 SQL Server 数据库

本节为 User Application 使用 SQL Server 数据库提供了所需的配置选项。有关支持的 SQL Server 版本的信息，请参见Identity Applications 的系统要求 （第 171 页）。

配置字符集

SQL Server 不允许您为数据库指定字符集。User Application 以支持 UTF-8 的 NCHAR 列类型储存 SQL Server 字符数据。

配置管理员用户帐户

安装支持的 Microsoft SQL Server 版本之后，请使用 SQL Server Management Studio 之类的应用程序创建数据库和数据库用户。该数据库用户帐户必须具有以下特权：

- CREATE TABLE
- DELETE
- INSERT
- SELECT
- UPDATE

注释：建议对 Microsoft SQL Server 2014 使用 JDBC JAR 版本 sqljdbc4.jar，对 Microsoft SQL Server 2016 使用 sqljdbc42.jar。

15.4 为 Identity Applications 准备环境

在群集中运行 Identity Applications 时，将获得较高的可用性。此外，它们还支持 HTTP 会话复制和会话故障转移。这意味着，如果某个会话所在的节点发生故障，无需用户干预就能在群集中的另一个服务器上恢复该会话。

本节提供了有关准备环境 （包括群集环境）以便 Identity Applications 能够正常运行的说明。必须结合第 15.5.2 节 “ 使用引导式过程安装 Identity Applications”（第 181 页）中的指导来完成本节中的步骤。

有关群集环境要求的详细信息，请参见第 15.1.3 节 “ 安装 Identity Applications 的先决条件和注意事项 ”（第 167 页）和第 15.1.4 节 “Identity Applications 的系统要求 ”（第 171 页）。

15.4.1 指定权限索引的位置

当您安装 Identity Applications 时，安装进程将为 Tomcat 创建一个许可权限索引。如果您未指定该索引的位置，安装程序将在临时目录中创建文件夹。例如：Tomcat 上的 C:\NetIQ\idm\apps\tomcat\temp\permindex。

在测试环境中，该位置通常无关紧要。但是，在生产或过渡环境中，您可能不想将权限索引放置在临时目录中。

要指定索引的位置，请执行以下操作：

1 停止 Tomcat。
2 在文本编辑器中，打开 ism-configuration.properties 文件。
3 在该文件的末尾添加以下文本：

```
com.netiq.idm.cis.indexdir = path\permindex
```

例如：

```
com.netiq.idm.cis.indexdir = C:\NetIQ\idm\apps\tomcat\temp\permindex
```

4 保存并关闭文件。
5 删除临时目录中的现有 permindex 文件夹。
6 启动 Tomcat。

15.4.2 为群集启用许可权限索引

本节提供为群集启用许可权限索引的说明。

1. 在群集的第一个节点中登录 iManager，然后导航到**查看对象**。
2. 在**系统**下，导航到包含 **User Application 驱动程序**的驱动程序集。
3. 选择 **AppConfig** > **AppDefs** > **配置**。
4. 选择 XMLData 属性，并将 com.netiq.idm.cis.clustered 属性设置为 **true**。

   例如：

   <property>

   <key>com.netiq.idm.cis.clustered</key>

   <value>true</value>

   </property>
5. 单击**确定**。

15.4.3 为 Identity Applications 准备应用程序服务器

您应准备好将要运行 Identity Applications 的 Tomcat。方便起见，NetIQ 在安装套件中提供了 Apache Tomcat。另请参见第 15.4.4 节 " 为 Identity Applications 准备群集 "（第 179 页），以了解有关在群集环境中使用该应用程序的详细信息。

Identity Manager 的 .iso 安装文件中包含安装 Tomcat （PostgreSQL 可选）的程序。有关详细信息，请参见第 12.2 章 " 安装 PostgreSQL 和 Tomcat"（第 143 页）。

您可以使用自己的 Tomcat 安装程序，而不使用安装包中提供的便捷安装程序。但是，如果您要使用其他安装程序，则必须执行一些额外的步骤才能使 Tomcat 与 Identity Applications 正常配合运行。

在启动安装过程之前，请确保此版本的 Identity Applications 支持您要安装的组件版本。有关详细信息，请参见第 15.1.3 节 " 安装 Identity Applications 的先决条件和注意事项 "（第 167 页）。

1 在您的服务器上，作为服务安装 Apache Tomcat。

   有关详细信息，请参见 Tomcat Setup （Tomcat 安装）。

2 在装有 Tomcat 的同一个服务器上安装以下组件。

- **Java 运行时环境 (JRE)**：有关详细信息，请参见 《Java Platform Installation Guide》（Java 平台安装指南）。
- **Apache ActiveMQ**：有关详细信息，请参见 ActiveMQ。
- **PostgreSQL**：有关详细信息，请参见 PostgreSQL 手册。

3 将 activemq-all-5.15.2 jar 文件复制到 *C:\NetIQ\idm\apps\activemq* 文件夹。

4 将以下文件复制到 *C:\NetIQ\idm\apps\tomcat\bin* 文件夹，以用于日志记录。

- log4j.jar
- log4j.properties
- tomcat-juli-adapters.jar

5 在 setenv.bat 文件中设置以下属性。

```
JAVA_HOME
JRE_HOME
PATH (set Java path)
JAVA_OPTS="-Xms1024m -Xmx1024m"
```

6 将 postgresql-9.4.1212jdbc42.jar 文件复制到 C:\NetIQ\idm\apps\tomcat\bin 文件夹。

7 （视情况而定）在群集环境中，打开群集第一个节点上的 server.xml 文件 （默认位于 \TOMCAT_INSTALLED_HOME\conf\ 目录中），并取消注释下面一行：

<Cluster className="org.apache.catalina.ha.tcp.SimpleTcpCluster"/>

对群集中的所有节点执行此操作。

对于高级 Tomcat 群集配置，请按照 Apache Tomcat 相关文档中的步骤操作。

15.4.4 为 Identity Applications 准备群集

Identity Applications 支持 HTTP 会话复制和会话故障转移。如果某个执行中的会话所在的节点发生故障，则无需用户干预，该会话就能在群集中的另一个服务器上继续进行。在群集中安装 Identity Applications 之前，应先准备好环境。

- 了解 Tomcat 环境中的群集组 （第 179 页）
- 设置工作流程引擎 ID 的系统属性 （第 180 页）
- 为群集中的每个用户应用程序使用相同的主密钥 （第 180 页）

了解 Tomcat 环境中的群集组

User Application 群集组使用 UUID 名称，以尽量减少与用户可能添加到其服务器中的其他群集组之间产生冲突的风险。您可以使用 User Application 管理功能修改 User Application 群集组的配置设置。只有在重启动服务器节点后，对群集配置所做的更改才能在该节点上生效。

有关在群集环境中进行安装需要满足的先决条件的详细信息，请参见第 15.1.3 节 “ 安装 Identity Applications 的先决条件和注意事项 ” （第 167 页）。

设置工作流程引擎 ID 的系统属性

在群集中托管 Identity Applications 的每个服务器都可以运行一个工作流程引擎。为确保群集和工作流程引擎的性能，群集中的每个服务器都应使用相同的分区名称和分区 UDP 组。此外，还必须使用工作流程引擎的唯一 ID 启动群集中的每个服务器，因为工作流程引擎的群集工作方式与 Identity Applications 的超速缓存框架无关。

为确保工作流程引擎正常运行，必须设置 Tomcat 的系统属性。

1 针对群集中的每个 Identity Applications 服务器创建一个新的 JVM 系统属性。
2 将系统属性命名为 com.novell.afw.wf.*engine-id*，其中的引擎 ID 是一个唯一值。

为群集中的每个用户应用程序使用相同的主密钥

Identity Applications 使用主密钥加密敏感数据。群集中的所有 Identity Applications 必须使用相同的主密钥。本节将帮助您确保群集中的所有 Identity Applications 使用相同的主密钥。

有关创建主密钥的详细信息，请参见步骤 6 （第 182 页）中的 “ **安全 - 主密钥** ”。有关加密 Identity Applications 中的敏感数据的详细信息，请参见 《*NetIQ Identity Manager - Administrator's Guide to the Identity Applications*》（NetIQ Identity Manager - Identity Applications 管理员指南）中的 “Encrypting Sensitive Identity Applications Data” （加密 Identity Applications 敏感数据）。

1 在群集中的第一个节点上安装 User Application。
2 在安装程序的 “ 安全 - 主密钥 ” 窗口中，记下将要包含 Identity Applications 新主密钥的 master-key.txt 文件所在的位置。默认情况下，该文件在安装目录中。
3 在群集中的其他节点上安装 Identity Applications。
4 在 “ 安全 - 主密钥 ” 窗口中，单击**是**，然后单击**下一步**。
5 在 “ 导入主密钥 ” 窗口中，复制在步骤 2 中创建的文本文件的主密钥。

15.5 安装 Identity Applications

本节提供了为 User Application 和 RBPM 安装及配置应用程序服务器的相关说明。您必须拥有应用程序服务器适用的正确的 Java 环境版本。

有关 Tomcat 和 Java 的要求的详细信息，请参见第 15.1.4 节 “Identity Applications 的系统要求 ” （第 171 页）。

15.5.1 Identity Applications 安装核对清单

使用以下核对清单来逐步完成 Identity Applications 的安装过程。

	核对清单项目
❑	1. （视情况而定）查看在群集环境中的 Tomcat 上安装 Identity Applications 的注意事项。有关详细信息，请参见了解 Tomcat 环境中的群集组 （第 179 页）。
❑	2. 安装受支持版本的应用程序服务器和 Java 开发包或运行时环境。有关详细信息，请参见第 15.1.4 节 “Identity Applications 的系统要求 ” （第 171 页）。
❑	3. 确保 Tomcat 的设置正确。有关详细信息，请参见第 15.4.3 节 “ 为 Identity Applications 准备应用程序服务器 ” （第 178 页）。
❑	4. 配置数据库的数据源文件和 JDBC 提供程序。
❑	5. 安装 Identity Applications。有关详细信息，请参见第 15.5.2 节 “ 使用引导式过程安装 Identity Applications” （第 181 页）。
❑	6. 为 Identity Applications 配置 Tomcat。有关详细信息，请参见第 15.5.3 节 “ 安装后步骤 ” （第 186 页）。
❑	7. 部署并启动 Identity Applications。有关详细信息，请参见启动 Identity Applications （第 190 页）。

15.5.2 使用引导式过程安装 Identity Applications

以下过程介绍了如何使用安装向导安装 Identity Applications。

要准备安装，请查看第 15.5.1 节 “Identity Applications 安装核对清单 ” （第 181 页）中所列的活动。另请参见版本随附的 《发行说明》。

注释：

- 安装程序不会保存您在向导的各个窗口中输入的值。如果单击上一步返回到前一个窗口，则必须重新输入配置值。
- 安装程序将创建 *novlua* 用户帐户，并为此用户设置 Tomcat 中的许可权限。例如， services.msc 脚本将使用此用户帐户来运行 Tomcat。

要使用引导式过程安装，请执行以下操作：

1. 以管理用户身份登录到要安装 Identity Applications 的计算机。
2. 停止 Tomcat。
3. （视情况而定）如果您已获取 Identity Manager 安装包的 .iso 映像文件，请导航到包含安装文件的目录 （默认为 products\UserApplication\ 目录）。
4. （视情况而定）如果您已下载安装文件，请完成以下步骤：
   - **4a** 导航到所下载映像的 win.zip 文件。
   - **4b** 将该文件的内容解压缩到本地计算机上的某个目录中。
5. 从包含安装文件的目录中运行 IdmUserApp.exe 文件。

6 使用以下参数完成引导式过程：

- **应用程序服务器平台**

  表示用于运行 Identity Applications 的 Tomcat。必须已安装 Tomcat。

- **安装文件夹**

  表示安装程序要在其中创建应用程序文件的目录路径。

- **数据库平台**

  表示 User Application 数据库的平台。必须已安装数据库软件。但是，在安装期间，您无需创建数据库纲要。

  为方便起见， NetIQ 提供了 PostgreSQL。

- **数据库主机和端口**

  表示托管 User Application 数据库的服务器的设置。

  注释：在群集环境中，必须为群集中的每个成员指定相同的数据库设置。

  主机

  指定服务器的名称或 IP 地址。

  端口

  指定您希望服务器在与 User Application 通讯时所使用的端口。

- **数据库用户名和口令**

  表示运行 User Application 数据库的设置。

  注释：

  - 如果您在安装此版 Identity Manager 的过程中安装了 PostgreSQL，则安装过程已创建了数据库和数据库管理员。默认情况下，安装的数据库为 idmuserappdb，数据库用户为 idmadmin。指定您在安装 PostgreSQL 时使用的相同值。
  - 在群集环境中，必须为群集中的每个成员指定相同的数据库名称、用户名和口令。

  数据库名称或 SID

  根据数据库平台指定数据库的名称。默认情况下，数据库名称为 idmuserappdb。

  - 对于 PostgreSQL 或 SQL Server 数据库，请指定名称。
  - 对于 Oracle 数据库，请指定您为数据库实例创建的安全标识符 (SID)。

  数据库用户名

  指定允许 User Application 访问和修改数据库中数据的帐户名。

  数据库口令

  为指定用户名指定口令。

  数据库驱动程序 JAR 文件

  指定数据库平台的 JAR 文件。

  数据库供应商将提供驱动程序 JAR 文件，该文件即为数据库服务器的瘦客户端 JAR。例如，对于 PostgreSQL，可以指定默认位于 C:\NetIQ\idm\apps\Postgres 文件夹中的 postgresql-9.4-1212.jdbc42.jar。

  NetIQ 不支持第三方供应商提供的驱动程序 JAR 文件。

- **数据库管理员**

可选

表示数据库管理员的名称和口令。

此字段会自动列出您为 " 数据库用户名和口令 " 指定的同一用户帐户和口令。要使用该帐户，请不要做任何更改。

数据库管理员

（可选）指定可创建数据库表、视图和其他项目的数据库管理员的帐户。

口令

（可选）指定数据库管理员的口令。

- **创建数据库表**

指定是否要在安装过程中或安装后配置新的或现有的数据库。

立即创建表

安装程序将在安装过程中创建数据库表。

应用程序启动时创建表

安装程序将下达指令，以在首次启动 User Application 时创建表。

将 SQL 写入文件

生成一个 SQL 脚本，数据库管理员可以运行该脚本来创建数据库。如果选择此选项，则还必须为**纲要文件**指定名称。该设置在 **SQL 输出文件**配置中指定。

如果您无权在环境中创建或修改某个数据库，则可以选择此选项。有关使用该文件生成表的详细信息，请参见第 15.7.2 节 " 手动创建数据库纲要 " （第 194 页）。

- **新数据库或现有数据库**

指定您要使用现有的空数据库还是在现有数据库中创建新表。请注意以下事项：

  - 新建数据库

  如果使用新的数据库，请单击**新数据库**。在选择此选项之前，请确保数据库已存在。

  - 现有数据库

  如果数据库是现有的且具有来自先前安装的 User Application 表，请选择**现有数据库**。

  如果现有数据库在 Oracle 平台上运行，则您必须在更新纲要之前准备好 Oracle。

选择数据库类型之后，需要指定应在何时创建数据库表。" 创建数据库表 " 屏幕允许您选择是在安装时还是在应用程序启动时创建表。或者，可以在安装时创建纲要文件，之后数据库管理员将使用该文件创建表。

如果要生成纲要文件，请选择 " 将 SQL 写入文件 " 按钮，并在 " 纲要输出文件 " 字段中提供文件名。

- **测试数据库连接**

指定您是希望安装程序连接到数据库后直接创建表，还是在连接后创建 .sql 文件。

在您单击**下一步**或按 **Enter** 后，安装程序即会尝试建立连接。

注释：如果数据库连接失败，您可以继续安装。但是，必须在安装后手动创建表并连接到数据库。有关详细信息，请参见手动创建 SQL 文件以生成数据库纲要 （第 195 页）。

- **Java 安装**

表示用于起动安装程序的 JRE 文件的路径。例如， C:\NetIQ\idm\jre。

- ***Application_Server* 配置**

表示 Tomcat 的安装文件路径。例如， C:\NetIQ\idm\jre。安装过程会将一些文件添加到此文件夹中。

- **IDM 配置**

  表示 URL 中使用的 Identity Applications 环境的设置以及工作流程引擎的设置。

  应用程序环境

  指定表示 Tomcat 配置的名称、应用程序 WAR 文件以及 URL 环境中的名称。

  安装脚本将创建服务器配置，然后根据您在安装 Tomcat 时创建的名称命名该配置。例如：IDMProv。

  重要说明：NetIQ 建议您记下指定的应用程序环境。当您从浏览器启动 Identity Applications 时，将会在 URL 中用到此应用程序名称。

- **选择审计日志记录类型**

  指出要启用 CEF 还是 Sentinel Log Management for IGA。指定是或否。

- **Audit 日志记录**

  仅当您为“选择审计日志记录类型”指定了“是”时才适用。

  指定要启用的日志记录类型。

  有关设置日志记录的详细信息，请参见 *《User Application Administration Guide》*（User Application 管理指南）。

  Sentinel Log Management for IGA

  通过适用于 User Application 的 Novell 或 NetIQ 客户端启用日志记录。

  注释：如果您选择此选项，则还必须指定客户端服务器的主机名或 IP 地址，以及日志超速缓存的路径。

  CEF

  让 User Application 通过 CEF 来记录事件。

  注释：如果您选择此选项，则还必须指定系统日志服务器的主机名或 IP 地址，以及系统日志端口。

- **安全 — 主密钥**

  指定是否要导入现有的主密钥。 User Application 使用主密钥来访问加密的数据。指定是或否。

  在以下情况下，可能会想要导入主密钥：

  - 在群集中安装 Identity Applications 的第一个实例后。群集中 User Application 的每个实例必须使用相同的主密钥。有关详细信息，请参见为群集中的每个用户应用程序使用相同的主密钥 （第 180 页）。
  - 您要将安装从过渡系统迁移到生产系统，并希望依然能够访问您在过渡系统中使用的数据库。
  - 您要恢复 User Application，并想要访问先前版本的 User Application 所储存的加密数据。

  是

  指定您想要导入现有的主密钥。

否

指定您要让安装程序创建该密钥。

默认情况下，安装过程会将加密的主密钥写入安装目录中的 master-key.txt 文件。

- **导入主密钥**

  仅当您为 " 安全 - 主密钥 " 指定了 " 是 " 时才适用。

  指定您要使用的主密钥。可以从 master-key.txt 文件中复制主密钥。

- **应用程序服务器连接**

  表示用户连接 Tomcat 上的 Identity Applications 时所需的 URL 设置。例如：https：myserver.mycompany.com：8080。

注释：如果 OSP 在不同的 Tomcat 应用程序服务器实例上运行，则还必须选择**连接外部鉴定服务器**并指定 OSP 服务器的值。

协议

指定是要使用 *http* 还是 *https*。要使用安全套接字层 (SSL) 进行通讯，请指定 https。

主机名

指定托管 OSP 的服务器的 DNS 名称或 IP 地址。请不要使用 localhost。

端口

指定您希望服务器在与客户端计算机通讯时所使用的端口。

连接外部鉴定服务器

指定是否要用不同的 Tomcat 实例来托管鉴定服务器 (OSP)。鉴定服务器包含可登录 SSPR 的用户的列表。

如果选择此设置，则还要指定鉴定服务器的**协议**、**主机名**和**端口**值。

- **鉴定服务器细节**

  指定您希望 Identity Applications 在连接鉴定服务器时所使用的口令。该口令又称为客户端机密。安装过程将创建此口令。

7 在 " 配置更新 " 窗口中配置 Identity Applications 的设置。

7a 浏览**身份库 DN**。

7b 单击**确定**。

注释：

- 确保 User Application 和 Roles and Resources Service 驱动程序已创建且已部署到身份库。有关详细信息，请参见 Identity Applications 的安装注意事项 （第 167 页）。
- 如果您单击**取消**，安装程序会让您返回到 " 应用程序服务器连接 " 窗口。
- 安装 User Application 后，您可以修改 configureupdate.bat 文件中的大部分设置。有关指定设置值的详细信息，请参见第 15.8 章 " 配置 Identity Applications 的设置 " （第 204 页）。

---

8 （视情况而定）在 GUI 安装中，如果要立即配置 Identity Applications，请在 “ 配置 IDM” 窗口中完成以下步骤：

8a 单击**是**，然后单击**下一步**。

8b 在 “Roles Based Provisioning Module 配置 ” 中，单击**显示高级选项**。

8c 根据需要修改设置。

注释：

- 有关指定值的详细信息，请参见第 15.8 章 “ 配置 Identity Applications 的设置 ”（第 204 页）。
- 在生产环境中，所有管理员指派都受到许可限制。 NetIQ 会收集审计数据库中的监视数据，以确保生产环境符合要求。此外， NetIQ 还建议仅向一个用户授予安全管理员的许可权限。

8d 单击**确定**。

9 单击**下一步**。

10 在 “ 安装前摘要 ” 窗口中单击**安装**。

11 （可选）查看安装日志文件。要了解基本安装的结果，请参见 C:\NetIQ\idm\apps\UserApplication\logs\ 目录中的 user_application_install_log.log 文件。

有关 Identity Applications 配置的信息，请参见 C:\NetIQ\idm\apps\UserApplication 目录中的 NetIQ-Custom-Install.log 文件。

12 （可选）如果使用的是外部口令管理 WAR，请手动将 WAR 复制到安装目录和运行外部口令 WAR 功能的远程应用程序服务器部署目录。

13 根据第 15.7 章 “ 完成 Identity Applications 的安装 ”（第 194 页）中所述继续执行安装后任务。

15.5.3 安装后步骤

本节提供有关在安装 Identity Applications 后更新 Tomcat 环境的信息。

- 为群集配置 User Application 驱动程序 （第 187 页）
- 将 preferIPv4Stack 属性传递给 JVM （第 187 页）
- 检查服务器的运行状况 （第 187 页）
- 监视运行状况统计数字 （第 187 页）
- 创建复合索引 （第 188 页）
- 配置 Identity Application 以拒绝客户端发起的 SSL 重新协商 （第 189 页）

如果您使用了 Tomcat 的便捷安装程序， Identity Manager 的安装程序将为您配置 Tomcat。如果您安装了自己的 Tomcat 程序，请注意以下问题：

- 您可以修改 Tomcat 服务，以提高其执行效率。有关详细信息，请参见 *《So You Want High Performance》*（如何提高性能）。
- 您可能想要添加对日志记录事件的支持。有关详细信息，请参见第 13.1.4 节 “ 使用 Apache Log4j 服务记录登录 ”（第 150 页）。

为群集配置 User Application 驱动程序

有关更多信息，请参见第 15.6.2 节 " 为群集配置 User Application 驱动程序 "（第 192 页）。

将 preferIPv4Stack 属性传递给 JVM

Identity Applications 使用 JGroups 实现超速缓存。在某些配置中， JGroups 需要将 preferIPv4Stack 属性设置为 true，以确保 mcast_addr 绑定成功。

如果不使用此选项，可能会发生以下错误：

```
[10/1/09 16:11:22:147 EDT] 0000000d UDP           W org.jgroups.util.Util
createMulticastSocket could not bind to /228.8.8.8 (IPv4 address); make sure
your mcast_addr is of the same type as the IP stack (IPv4 or IPv6).
```

您还可能会看到此错误：

```
[3/21/12 10:04:32:470 EDT] 00000024 UDP      E org.jgroups.protocols.TP down
failed sending message to null (131 bytes)
        java.lang.Exception: dest=/228.8.8.8:45654 (134 bytes)
    at org.jgroups.protocols.UDP._send(UDP.java:353)
```

参数 java.net.preferIPv4Stack=true 是一项系统属性，与其他系统属性 （例如 extend.local.config.dir）的设置方式相同。

检查服务器的运行状况

大多数负载平衡器都提供运行状况检查功能，以确定 HTTP 服务器是否已启动且正在监听。 User Application 包含一个 URL，可用于配置负载平衡器上的 HTTP 运行状况检查。该 URL 为：

http://< 节点 IP>: 端口 /IDMProv/jsps/healthcheck.jsp

监视运行状况统计数字

REST API 可让您检索有关 User Application 运行状态的信息。API 可以访问系统以了解当前正在运行的线程、内存占用、超速缓存和群集信息，并使用 GET 操作返回信息。

- **内存信息 （JVM 和系统内存）：**读取与内存相关的信息，例如系统内存和 JVM 占用的内存。

  例如，

  `http://<ip_addr:port>/IDMProv/rest/monitoring/statistics/memoryinfo`

- **线程信息：** 读取大量占用 CPU 的线程的相关信息，并返回导致高 CPU 利用率的排名靠前的线程列表。

  例如，

  `http://<ip_addr:port>/IDMProv/rest/monitoring/statistics/threadinfo`

  要访问 JVM 中线程的堆栈跟踪，请将堆栈参数设置为 **True**。

  例如，

  `http://<ip_addr:port>/IDMProv/rest/monitoring/statistics/threadinfo?stack=true`

  要指定 JVM 中的线程数，请为 **thread-count** 参数指定值。

  例如，

```
http://<ip_addr:port>/IDMProv/rest/monitoring/statistics/threadinfo?thread-count=1
```

- **超速缓存信息：**读取 User Application 的超速缓存信息。

  例如，

  ```
  http://<ip_addr:port>/IDMProv/rest/monitoring/statistics/cacheinfo
  ```

- **群集信息：**读取与群集相关的信息。

  例如，

  ```
  http://<ip_addr:port>/IDMProv/rest/monitoring/statistics/clusterinfo
  ```

注释：您必须是安全管理员才能使用 REST API 查看 User Application 运行状况统计数字。

创建复合索引

安装或升级 Identity Applications 后，为您要用于在 Identity Manager 仪表板中对用户排序的每个属性手动创建复合索引。您可以使用位于 eDirectory 安装路径中的 ndsindex 实用程序来创建复合索引。可以指定多个属性并以 $ 符号分隔来创建复合索引。下面是需要创建复合索引的基本属性：

- Surname,Given Name
- Given Name,Surname
- cn,Surname
- Title,Surname
- Telephone Number,Surname
- Internet Email Address,Surname
- L,Surname
- OU,Surname

以下命令可帮助您使用 ndsindex 实用程序创建复合索引：

```
ndsindex add [-h <hostname>] [-p <port>] -D <admin DN> -W|[-w <password>] -s
<eDirectory Server DN> [<indexName1>, <indexName2>.....]
```

例如，要根据**职位**对用户排序，请执行以下命令：

```
ndsindex add -h <hostname> -p <ldap port> -D <admin DN> -w <admin passwd> -s
<eDirectory Server DN> Title-SN;Title$Surname;value
```

您也可以使用转换导出实用程序创建复合索引。

必须使用 LDIF 文件来创建索引。导入 LDIF 文件后，请通过触发 Limber 来启动索引编制活动。否则，索引编制会在 Limber 自动触发时才执行。

用于创建复合索引以根据 **Title** 属性对用户排序的示例 LDIF 文件：

```
dn: cn=osg-nw5-7, o=Novell

changetype: modify

add: indexDefinition

indexDefinition: 0$sntitleindex$0$0$0$1$Title$surname
```

有关 LDIF 文件的详细信息，请参见 《*NetIQ eDirectory Administration Guide*》（NetIQ eDirectory 管理指南）中的 “LDIF Files” （LDIF 文件）。

配置 Identity Application 以拒绝客户端发起的 SSL 重新协商

默认情况下， Identity Applications 安装程序会配置一个非安全连接 (http)。在某些情况下，非安全连接会使 Identity Manager 容易受到因客户端所发起与 Identity Applications 服务器的 SSL 重新协商而导致的拒绝服务攻击。为防止发生此问题，请将以下标志添加到 <tomcat-install-directory>\bin\setenv.bat 文件中的 CATALINA_OPTS 条目。

```
"-Djdk.tls.rejectClientInitiatedRenegotiation=true"
```

15.5.4 禁用阻止 HTML 成帧设置以将 Identity Manager 与 SSPR 集成

本节介绍了将 Identity Manager 集成到 Identity Manager 4.5 未部署的现有 SSPR 4.2 环境所需的配置。 SSPR 提供了一个可配置选项**阻止 HTML 成帧**，使用该选项，用户可以查看包含 iframe html 源代码的任何应用程序的内嵌帧中的 SSPR。如果您选择此选项， SSPR 将不会包含在应用程序的指定 iFrame 中。要为 Identity Manager 禁用此选项，请执行以下步骤：

1. 转到 http://*<IP/DNS name>:<port>/sspr*。此链接可将您导向到 SSPR 门户。
2. 以 SSPR 管理员身份登录。
3. 单击页顶部的**配置编辑器**，然后指定 OSP 配置口令。
4. 单击**设置 > 安全性 > 始终显示高级设置**，然后执行以下操作：
   - **4a** 浏览到**阻止 HTML 成帧**，取消选择**已启用**，然后单击**保存**以保存设置。
   - **4b** 在确认窗口中，单击**确定**。

15.5.5 校验用户属性

要让用户能够使用 Identity Applications，必须确保具有必要权限的用户属性已添加到包含您所有系统用户的容器中。您可以使用 iManager 校验这些属性。在 iManager 中执行下列步骤来校验这些设置：

1. 使用身份库 IP 地址作为树，以管理员身份登录 iManager。
2. 在**树**面板中，选择配置了 Identity Applications 的树。
3. 针对包含所有系统用户的容器单击**指派的权限**。
4. 校验下列属性是否具有列表中的必要权限：
   - 说明
   - Internet EMail Address
   - 登录脚本
   - 打印作业配置
   - 电话号码
   - 标题
   - 直属下属
   - 管理者
   - 照片

- srvprvQueryList
- srvprvUserPrefs

如果缺少任何属性，请单击**添加属性**。

4a 从列表中选择所需的属性，然后单击**完成**。

4b 选择属性的必要权限，然后单击**完成**。

图 15-1 将属性添加到用户容器中

15.5.6 启动 Identity Applications

本节提供了启动 Identity Applications 以及在应用程序服务器上首次登录的说明。在群集环境中，请在主节点上开始该过程。 Identity Applications 应已安装，并且已可进行部署。有关安装后任务的详细信息，请参见第 15.7 章 " 完成 Identity Applications 的安装 " （第 194 页）。

可以使用 services.msc 启动脚本来启动 Tomcat 服务。此文件也可用于停止和重启动 Tomcat 服务。

完成这些步骤之后，如果浏览器未显示 User Application 页面，请检查终端控制台上是否有错误讯息，并参见第 37 章 " 查错 " （第 369 页）。

要启动 Identity Applications，请执行以下操作：

1 启动 Identity Applications 的数据库。有关详细信息，请参见数据库文档。

2 要使 User Application 运行报告，请在 Tomcat 的启动脚本中添加 Djava.awt.headless=true 标志。例如：

```
JAVA_OPTS="-Djava.awt.headless=true -Dfile.encoding=UTF-8 -Dsun.jnu.encoding=UTF-8 -server -Xms1024m -Xmx1024m -XX:MaxPermSize=512m
```

注释：如果是在 X11 Windows 系统上运行，则不需要执行此步骤。

---

3 启动 Identity Applications 安装到的 Tomcat。

注释：在群集中，请只启动主节点。

---

4 在命令行中，将安装目录设置为工作目录。

5 执行启动脚本。

6 要启用与 User Application 驱动程序的通讯，请完成以下步骤：

6a 登录到 iManager。

6b 在左侧导航框架中的**角色和任务 > Identity Manager** 下，单击 **Identity Manager 概述**。

6c 在内容视图中，指定包含 User Application 驱动程序的驱动程序集，然后单击**搜索**。

6d 在显示驱动程序集及其关联驱动程序的示意图中，单击 User Application 驱动程序对应的红白图标。

6e 单击**启动驱动程序**。

启动后，驱动程序将尝试与 User Application“ 握手 ”。如果应用程序服务器未运行，或者 WAR 未成功部署，驱动程序将返回错误。否则，驱动程序状态将更改为阴阳符号，指示驱动程序现已启动。

7 要启动 Role and Resource Service 驱动程序，请重复步骤 6 中的过程。

8 要起动并登录到 User Application，请在 Web 浏览器中输入以下 URL：

`http://hostname:port/ApplicationName`

hostname

表示应用程序服务器的名称 (Tomcat)。例如：myserver.domain.com

port

表示应用程序服务器的端口号。例如：8180。

ApplicationName

表示您在安装应用程序期间提供应用程序服务器配置信息时所指定的名称。例如：IDMProv。

9 在 User Application 登录页的右上角，单击**登录**。

10 （视情况而定）要在群集组中启用 User Application，请完成以下步骤：

10a 单击**管理**。

10b 在 “ 应用程序配置 ” 门户中，单击**超速缓存**。

10c 在 “ 超速缓存管理 ” 窗口中，为**群集已启用**选择 **True**。

10d 单击**保存**。

10e 重启动服务器。

10f （视情况而定）要使用本地设置，请针对群集中的每个服务器重复此过程。

15.6 创建和部署 Identity Applications 的驱动程序

安装 RBPM 时会添加用于创建 Identity Applications 的驱动程序的文件。该驱动程序配置支持允许您执行以下操作：

- 将一个 User Application 驱动程序与一个角色和资源服务驱动程序相关联。
- 将一个 User Application 与一个 User Application 驱动程序相关联。

在尝试配置驱动程序之前，请确保已拥有 Designer“ 包编目 ” 中的所有必要包。当您创建新 Identity Manager 项目时，用户界面会自动提示您将若干包导入该新项目。

15.6.1 创建 User Application 驱动程序

User Application 驱动程序不仅是一个运行时组件，也是一个目录对象 （构成 User Application 的运行时项目）的储存封装程序。它负责储存应用程序特定的环境配置数据。当身份库中的重要数据值发生更改时，该驱动程序还会通知目录提取层。收到此通知后，目录提取层将更新其超速缓存。

1 在 Designer 中打开您的项目。
2 在**建模器 > 供应**视图上的调色板中，选择 **User Application**。
3 将 **User Application** 的图标拖到**建模器**视图上。
4 在驱动程序配置向导中，选择 **User Application 基本**，然后单击**下一步**。
5 在出现安装多个附加包的提示时，单击**确定**。
6 （可选）指定驱动程序的名称。

   单击**下一步**。
7 在连接参数窗口中，指定 User Application 管理员的 ID 和口令。
8 指定 User Application 服务器的主机和端口。
9 指定 User Application 服务器的应用程序环境。
10 （可选）要允许供应管理员以其他人 （供应管理员被指定为其代理）的名义启动工作流程，请为**允许覆盖初始程序**选择**是**。
11 在**确认安装任务**窗口中，单击**完成**。

15.6.2 为群集配置 User Application 驱动程序

在群集环境中，可以将单个 User Application 驱动程序与多个 User Application 实例搭配使用。驱动程序存储特定于应用程序的各种信息 （例如工作流程配置和群集信息）。必须将驱动程序配置为使用群集的发送程序或负载平衡器的主机名或 IP 地址。

1 登录管理身份库的 iManager 实例。
2 在导航框架中，选择 **Identity Manager**。
3 选择 **Identity Manager 概述**。
4 使用搜索页面显示 “Identity Manager 概述 ”，以了解包含 User Application 驱动程序的驱动程序集。
5 单击驱动程序图标右上角的圆形状态指示器：
6 选择**编辑属性**。
7 对于**驱动程序参数**，请将**主机**更改为发送程序的主机名或 IP 地址。
8 单击**确定**。

15.6.3 创建 Role and Resource Service 驱动程序

User Application 使用 Role and Resource Service 驱动程序来管理资源的后端处理。例如，它管理所有资源请求、启动资源请求的工作流程，以及启动资源请求的供应处理。

1 在 Designer 中打开您的项目。
2 在建模器 > 供应视图上的调色板中，选择角色服务。
3 将角色服务的图标拖到建模器视图上。
4 在驱动程序配置向导中，选择 Role and Resource Service 基本，然后单击下一步。
5 （视情况而定）如果这是 Designer 中安装的第一个驱动程序，请单击确定以安装 Common Settings Advanced Edition 包。
   5a 指定 User Application 服务器的 URL。
   5b 指定 User Application 管理员的 eDirectory DN。
   5c 指定 User Application 供应服务帐户的 LDAP DN。该帐户可与 User Application 管理员帐户相同，也可以不同。

      如果此服务帐户发出了角色或资源供应请求，则会绕过与此角色或资源关联的所有批准或供应工作流程。
6 （可选）指定驱动程序的名称。
7 单击下一步。
8 在 “User Application/ 工作流程连接 ” 窗口中，指定用户组基本容器 DN 和您刚刚创建的 User Application 驱动程序。

   由于该驱动程序尚未部署，浏览功能将不会显示您刚刚配置的 User Application 驱动程序。您可能需要键入该驱动程序的 DN。
9 指定 User Application 的 URL。
10 指定 User Application 管理员帐户的 LDAP DN

   User Application 管理员帐户将鉴定到 User Application，以启动批准工作流程。有关详细信息，请参见第 15.2.2 节 “ 向身份库管理员和 User Application 管理员帐户指派权限 ” （第 173 页）。
11 指定 User Application 管理员帐户的口令。
12 单击下一步。
13 在 “ 确认安装任务 ” 窗口中，单击完成。

15.6.4 部署 User Application 的驱动程序

只有在部署 User Application 和 Role and Resource Service 驱动程序后，它们才可用。

注释：复制 eDirectory 环境时，必须确保复本包含 Identity Manager 的 NCP 服务器对象。 Identity Manager 仅限于服务器的本地复本。因此，如果二级服务器不包含服务器对象， Role and Resource Service 驱动程序可能无法正常启动。

要部署驱动程序，请执行以下操作：

1 在 Designer 中打开您的项目。

2 在建模器或大纲视图中，选择 “ 驱动程序集 ”。

3 单击在线 > 部署。

15.7 完成 Identity Applications 的安装

本节提供了在安装 Identity Applications 及其框架后可能要执行的活动的说明：

15.7.1 在群集环境中检查服务器的运行状况

有关详细信息，请参见检查服务器的运行状况 （第 187 页）

15.7.2 手动创建数据库纲要

安装 Identity Applications 时，可以暂缓连接到数据库或者在数据库中创建表。如果您对数据库没有许可权限，则可能需要选择此选项。安装程序将创建一个 SQL 文件，您可以使用该文件来创建数据库纲要。您也可以在安装后重创建数据库表，而无需重新安装。为此，您要删除 Identity Applications 的数据库，并创建同名的新数据库。

使用 SQL 文件生成数据库纲要

本节假设安装程序已创建了您可执行以生成数据库纲要的 SQL 文件。如果您没有该 SQL 文件，请参见手动创建 SQL 文件以生成数据库纲要 （第 195 页）。

注释：请不要使用 SQL*Plus 来执行该 SQL 文件。该文件中的行长度超过了 4000 个字符。

---

1 停止 应用程序服务器。

2 登录到数据库服务器。

3 删除 Identity Applications 使用的数据库。

4 创建与步骤 3 中所删除数据库同名的新数据库。

5 浏览到安装过程创建的 SQL 脚本 （默认位于 */installation_path*/userapp/sql 目录中）。

6 让数据库管理员运行该 SQL 脚本，以创建并配置 User Application 数据库。

7 重启动 Tomcat。

手动创建 SQL 文件以生成数据库纲要

您可以在安装后重新创建数据库表，而无需重新安装，也无需具有 SQL 文件。本节将帮助您在没有 SQL 文件的情况下创建数据库纲要。

1 停止 Tomcat。

2 登录到托管 Identity Applications 数据库的服务器。

3 删除现有的数据库。

4 创建与您在步骤 3 中删除的数据库同名的新数据库。

5 在文本编辑器中，打开 NetIQ-Custom-Install.log 文件 （默认位于 Identity Applications 的安装根目录中）。例如：

```
C:\NetIQ\idm\apps\UserApplication
```

6 在 NetIQ-Custom-Install.log 文件中搜索并复制以下命令：

```
C:\NetIQ\idm\jre\bin\java -Xms256m -Xmx256m  -Dwar.context.name=IDMProv -
Ddriver.dn="cn=User Application Driver,cn=driverset1,o=system" -
Duser.container="o=data" -jar C:\NetIQ\idm\jre\liquibase.jar --
databaseClass=liquibase.database.core.PostgresDatabase --
driver=org.postgresql.Driver --
classpath=C:\NetIQ\idm\apps\postgresql\postgresql-9.4.1212jdbc42.jar
C:\NetIQ\idm\apps\UserApplication\IDMProv.war --
changeLogFile=DatabaseChangeLog.xml  --url="jdbc:postgresql://localhost:5432/
idmuserappdb" --contexts="prov,newdb" --logLevel=info --
logFile=C:\NetIQ\idm\apps\UserApplication\db.out --username=******** --
password=******** update
```

7 登录到安装了 Identity Applications 数据库的服务器。

8 在终端中，粘贴您复制的命令字符串。

注释：该命令应是 updateSQL。如果命令是 update，请将它更改为 updateSQL。

---

9 在该命令中，将表示数据库用户名和口令的星号 (*) 替换为进行鉴定所需的实际值。此外，请确保 SQL 文件名是唯一的。

10 执行该命令。

11 （视情况而定）如果进程生成了一个 SQL 文件而没有填充数据库，请向数据库管理员提供该文件，以将它导入数据库服务器。有关详细信息，请参见使用 SQL 文件生成数据库纲要 （第 194 页）。

12 在数据库管理员导入该 SQL 文件后，启动 Tomcat。

15.7.3 手动将 Identity Applications 和 Identity Reporting 证书导入到身份库中

- 如果您拥有 Identity Applications 和 Identity Reporting 组件的自定义证书，请将这些证书导入到身份库 （位于 C:\NetIQ\eDirectory\jre\lib\security\cacerts 中)。

  例如，您可以使用以下 keytool 命令将证书导入到身份库中：

```
keytool -importkeystore -alias <User Application certificate alias> -
srckeystore  <backup cacert> -srcstorepass changeit -destkeystore
C:\NetIQ\eDirectory\jre\lib\security\cacerts
```

- 如果您将 SSPR 安装在不同于 User Application 服务器的另一服务器上，请确保将 SSPR 应用程序证书添加到 User Application cacerts。

15.7.4 记录主密钥

NetIQ 建议在安装后，立即复制加密的主密钥并将其记录在安全的位置。如果此项安装是在群集的第一个成员上进行的，当您在群集的其他成员上安装 Identity Applications 时，将要用到这个加密的主密钥。

警告：要始终保留加密主密钥的复本。如果丢失了主密钥，您需要使用加密的主密钥重新获取加密数据的访问权。例如，在发生设备故障后，您可能需要该密钥。

15.7.5 配置 Identity Applications 的身份库

Identity Applications 必须能够与身份库中的对象交互。

为了提高 Identity Applications 的性能， eDirectory 管理员应为 manager、 ismanager 和 srvprvUUID 属性创建值索引。如果这些属性没有值索引， Identity Applications 用户可能会遭遇性能不佳的状况，这在群集环境中尤为突出。

通过在 RBPM 配置实用程序中选择 “ 高级 ”>“ 创建 eDirectory 索引 ”，即可在安装期间自动创建这些值索引。有关使用 Index Manager 创建值索引的详细信息，请参见《*NetIQ eDirectory Administration Guide*》（NetIQ eDirectory 管理指南）。

15.7.6 更改 User Application 的默认环境名称

如果不使用默认环境名称，您可以根据组织的要求创建新环境。您可以通过执行下列操作来更改环境名称：

1. 使用 services.msc 文件停止 Tomcat 服务。
2. 导航到 C:\NetIQ\idm\apps\UserApplication 中的 User Application 目录。
3. 在 GUI 模式下起动 configupdate 实用程序。

   确保 configupdate.bat.properties 文件中的 use_console 选项设置为 false。
4. 在 **User Application** 选项卡中单击**显示高级选项**，然后执行以下步骤：

   4a 选择**更改 RBPM 环境名称**。

   4b 在 **RBPM 环境名称**中指定自定义环境名称。例如 IDMProvCustom。

   4c 浏览到并选择 “ 角色驱动程序 DN”。例如 cn=Role and Resource Service Driver,cn=Driver Set,o=system。

4d 单击确定。

5 校验 war 文件是否已重命名。

- 导航到 Tomcat webapps 文件夹，检查 IDMProvCustom.war 项是否已更新。
- 导航到 \TOMCAT_INSTALLED_HOME\conf 中的 ism-configuration properties 文件，并检查 portal.context 项是否指定了新的环境名称。

6 使用 C:\NetIQ\idm\apps\UserApplication 中的 update-context.bat 文件将数据库更新为采用新的环境名称。

执行以下命令以运行 update-context.bat 文件。

```
ua:C:\NetIQ\idm\apps\UserApplication # vi update-context.bat
```

屏幕上应该会显示以下项：

```
# copy and paste or execute this script before changing context name

# Substitute your new context where indicated

#
```

```
C:\NetIQ\idm\jre\bin\java -Xms256m -Xmx256m  -Dwar.context.name=[New Context
Here] -Ddriver.dn=[UA Driver DN] -jar
C:\NetIQ\idm\apps\UserApplication\liquibase.jar --
databaseClass=liquibase.database.core.PostgresDatabase  --
driver=org.postgresql.Driver  --classpath=
C:\NetIQ\idm\apps\postgres\postgresql-9.4.1212.jdbc42.jar:
C:\NetIQ\idm\apps\tomcat\webapps\IDMProv.war --
changeLogFile=UpdateProducerId.xml   --url="jdbc:postgresql://localhost:5432/
idmuserappdb?compatible=true" --contexts="prov,updatedb" --logLevel=debug --
username=******** --password=******** update
```

例如，如果您使用的是 PostgreSQL 数据库，请运行以下脚本：

```
C:\NetIQ\idm\apps\jre\bin\java -Xms256m -Xmx256m  -
Dwar.context.name=IDMProvCustom  -Ddriver.dn= cn=Role and Resource Service
Driver,cn=driverset1,o=system -jar
C:\NetIQ\idm\apps\UserApplication\liquibase.jar --
databaseClass=liquibase.database.core.PostgresDatabase  --
driver=org.postgresql.Driver  --classpath=
C:\NetIQ\idm\apps\postgres\postgresql-9.4.1212.jdbc42.jar:
C:\NetIQ\idm\apps\tomcat\webapps\IDMProv.war --
changeLogFile=UpdateProducerId.xml   --url="jdbc:postgresql://<Database
Server:5432/idmuserappdb?compatible=true" --contexts="prov,updatedb" --
logLevel=debug --username=dbadmin --password=******** update
```

其中

-Dwar.context.name=IDMProvCustom 指定新环境。

-Ddriver.dn ="cn=User Application Driver,cn=driverset1,o=system" 指定 User Application 驱动程序 DN。

--username=dbadmin 指定可创建数据库表、视图和其他项目的数据库管理员用户名。

重要：对于其他支持的数据库，请不要更改脚本中的数据库驱动程序细节。

---

7 校验数据库表是否使用了新的环境名称。

表名	要检查的列
PORTALPRODUCERS	producerid
PORTALPRODUCERREGISTRY	producerid
PORTALREGISTRY	producerid
PORTALPORTLETSETTINGS	producerid
PORTALPORTLETHANDLES	producerid
PROFILEGROUPPREFERENCES	elementid

例如，运行以下 SQL 命令可在 PORTALPRODUCERS 表中校验新环境名称：

```
Select * from PORTALPRODUCERS;
```

该命令应该只返回新环境名称。

8 使用 services.msc 文件启动 Tomcat 服务。

15.7.7 重新配置 Identity Applications 的 WAR 文件

要更新 Identity Applications 的 WAR 文件，请运行 RBPM 配置实用程序。

1 通过执行 configupdate.bat 来运行安装目录中的实用程序。

   有关实用程序参数的详细信息，请参见第 15.8 章 " 配置 Identity Applications 的设置 " （第 204 页）。

2 将新的 WAR 文件部署到应用程序服务器。

   对于 Tomcat 单一服务器，这些更改将应用于所部署的 WAR。

15.7.8 配置忘记口令管理

Identity Manager 安装中包含 Self Service Password Reset，可帮助您管理忘记口令的重设置过程。此外，您也可以使用外部口令管理系统。

使用 Self Service Password Reset 进行忘记口令管理

在大多数情况下，您可以在安装 SSPR 和 Identity Applications 时启用忘记口令管理功能。但是，有时您可能没有指定当口令更改后，SSPR 要将用户定向到的 Identity Applications 登录页 URL。此时，您也需要启用忘记口令管理。本节提供以下信息：

将 Identity Manager 配置为使用 Self Service Password Reset

本节提供了将 Identity Manager 配置为使用 SSPR 的相关信息。

1 登录到安装了 Identity Applications 的服务器。

2 运行 RBPM 配置实用程序。有关详细信息，请参见第 15.8.1 节 " 运行 Identity Applications 配置实用程序 " （第 204 页）。

3 在实用程序中，浏览到**鉴定 > 口令管理**。

4 对于**口令管理提供程序**，请指定 **SSPR**。

5 选择**忘记口令**。

6 浏览到 **SSO 客户端 > Self Service Password Reset**。

7 对于 **OSP 客户端 ID**，请指定要用于供鉴定服务器识别 SSPR 单点登录客户端的名称。默认值为 sspr。

8 对于 **OSP 客户端机密**，请指定 SSPR 单点登录客户端的口令。

9 对于 **OSP 重定向 URL**，请指定在完成鉴定后，鉴定服务器要将浏览器客户端重定向到的绝对 URL。

使用以下格式：protocol://server:port/path。例如， http://10.10.10.48:8180/sspr/public/oauth。

10 保存更改并关闭实用程序。

为 Identity Manager 配置 Self Service Password Reset

本节提供了配置 SSPR 以与 Identity Manager 配合使用的相关信息。例如，您可能想要修改口令策略和询问应答问题。

如果您随 Identity Manager 一起安装了 SSPR，即已指定了管理员可用来配置应用程序的口令。NetIQ 建议您修改 SSPR 设置，然后指定可以配置 SSPR 的管理员帐户或组。有关配置口令的详细信息，请参见第 14.2 章 " 为 Identity Manager 安装口令管理 "（第 157 页）。

1 使用您在安装期间指定的配置口令登录到 SSPR。

2 在 " 设置 " 页面中，修改口令策略和询问应答问题的设置。有关配置 SSPR 设置默认值的详细信息，请参见 《*NetIQ Self Service Password Reset Administration Guide*》（NetIQ Self Service Password Reset 管理指南）中的 "Configuring Self Service Password Reset"（配置 Self Service Password Reset）。

3 锁定 SSPR 配置 文件 (SSPRConfiguration.xml)。有关锁定配置文件的详细信息，请参见锁定 SSPR 配置 （第 200 页）。

4 （可选）要在锁定配置后修改 SSPR 设置，必须在 SSPRConfiguration.xml 文件中将 configIsEditable 设置设为 true。

5 从 SSPR 中注销。

6 要使更改生效，请重启动 Tomcat。

锁定 SSPR 配置

1 转到 **http://<IP/DNS name>:<port>/sspr**。此链接可将您转到 SSPR 门户。

2 使用管理员帐户登录到 Identity Manager，或使用现有的登录身份凭证登录。

3 单击页面顶部的**配置管理器**，然后指定您在安装期间指定的配置口令。

4 单击**配置编辑器**，然后浏览到**设置 > LDAP 设置**。

5 锁定 SSPR 配置 文件 (SSPRConfiguration.xml)。

   5a 在 " 管理员许可权限 " 部分下，在身份库中以 LDAP 格式定义过滤器，以过滤对 SSPR 具有管理员权限的用户或组。默认情况下，该过滤器设置为 groupMembership=cn=Admins,ou=Groups,o=example。

   例如，对于 User Application 管理员，请将它设置为 uaadmin (cn=uaadmin)。

   这可以防止用户修改 SSPR 中的配置，但具有完全权限可修改设置的 SSPR 管理员用户除外。

   5b 为确保 LDAP 查询返回结果，请单击**查看匹配项**。

   如果设置中存在任何错误，则您无法继续设置下一个配置选项。 SSPR 会显示错误细节，以帮助您进行问题查错。

   5c 单击**保存**。

5d 在弹出的确认窗口中，单击确定。

锁定 SSPR 后，管理员用户可以在 “ 管理 ” 用户界面中查看其他选项，例如 “ 仪表板 ”、“ 用户活动 ”、“ 数据分析 ” 等，而在锁定 SSPR 之前则不会显示这些选项。

6 （可选）要在锁定配置后修改 SSPR 设置，必须在 SSPRConfiguration.xml 文件中将 configIsEditable 设置设为 true。

7 从 SSPR 中注销。

8 以步骤 3 中定义的管理员用户身份再次登录到 SSPR。

9 单击关闭配置，然后单击确定以确认更改。

10 要使更改生效，请重启动 Tomcat。

使用旧版提供程序进行忘记口令管理

您也可以不使用 SSPR，而是使用 Identity Manager 中的旧版提供程序实现忘记口令管理功能。如果选择了旧版提供程序，则不需要安装 SSPR。但是，您需要为用户重指派许可权限，使其能够访问共享页面以进行口令管理。本节提供执行以下活动的步骤：

- 配置旧版提供程序以进行忘记口令管理 （第 201 页）
- 重指派对口令管理页面的许可权限 （第 201 页）

有关旧版提供程序的详细信息，请参见第 4.4.2 节 “ 了解旧式口令管理提供程序 ” （第 32 页）。有关共享页面和许可权限的详细信息，请参见 《*NetIQ Identity Manager - Administrator's Guide to the Identity Applications*》（NetIQ Identity Manager - Identity Applications 管理员指南）中的 “Page Administration” （页面管理）。

配置旧版提供程序以进行忘记口令管理

1 登录到安装了 Identity Applications 的服务器。

2 运行 RBPM 配置实用程序。有关详细信息，请参见第 15.8.1 节 “ 运行 Identity Applications 配置实用程序 ” （第 204 页）。

3 在实用程序中，浏览到**鉴定 > 口令管理**。

4 对于**口令管理提供程序**，请指定 **User Application （旧版）**。

5 对于**忘记口令**，请指定**内部**。

6 浏览到 **SSO 客户端 > Self Service Password Reset**。

7 **OSP 重定向 URL** 设置应该是空的。

8 保存更改并关闭实用程序。

重指派对口令管理页面的许可权限

在安装期间， Identity Applications 的设置默认为 SSPR。必须为允许访问用于管理口令的共享页面的用户、组或容器指派或重指派许可权限。向用户指派对某个容器页面或共享页面的查看许可权限后，用户便可以访问该页面，并能在可用页列表中看到该页。

1 确保 Identity Manager 使用的是旧版提供程序。有关详细信息，请参见配置旧版提供程序以进行忘记口令管理 （第 201 页）。

2 以应用程序管理员身份登录到 User Application。例如，以 uaadmin 身份登录。

3 浏览到**管理 > 页面管理**。

4 在共享页面面板中，浏览到口令管理。

5 选择要对其指定许可权限的页面。例如 “ 更改口令 ” 或 “ 口令询问应答 ”。

6 在右侧面板中，单击指派许可权限。

7 在查看中，选择要指派到该页面的用户、组或容器。

8 （可选）要确保只有应用程序管理员才能访问指定的页面，请选择仅为管理员设置的查看许可权限。

9 单击保存。

10 针对想要配置的每个页面，执行步骤 5 至步骤 9。

11 选择主页图标返回仪表板。

12 导航到应用程序，然后选择 ⚙。

13 在管理应用程序页面上，使用 UserApp PwdMgt 的链接替换指向 SSPR 的链接。

有关详细信息，请参见针对分布式环境或群集环境更新仪表板中的 SSPR 链接 （第 203 页）和 *Identity Applications 的帮助*。

14 注销，然后重启动 Tomcat。

使用外部系统进行忘记口令管理

要使用外部系统，必须指定包含 “ 忘记口令 ” 功能的 WAR 文件的位置。此过程包括以下活动：

- 指定外部忘记口令管理 WAR 文件 （第 202 页）
- 测试外部忘记口令 配置 （第 203 页）
- 配置应用程序服务器之间的 SSL 通讯 （第 203 页）

指定外部忘记口令管理 WAR 文件

如果您在安装期间未指定此值，并想要修改设置，则您可以使用 RBPM 配置实用程序，或者以管理员身份在 User Application 中进行更改。

1 （视情况而定）要在 RBPM 配置实用程序中修改设置，请完成以下步骤：

1a 登录到安装了 Identity Applications 的服务器。

1b 运行 RBPM 配置实用程序。有关详细信息，请参见第 15.8.1 节 “ 运行 Identity Applications 配置实用程序 ” （第 204 页）。

1c 在实用程序中，浏览到鉴定 > 口令管理。

1d 对于口令管理提供程序，请指定 User Application （旧版）。

2 （视情况而定）要在 User Application 中修改设置，请完成以下步骤：

2a 以 User Application 管理员身份登录。

2b 浏览到管理 > 应用程序配置 > 口令模块设置 > 登录。

3 对于**忘记口令**，请指定外部。

4 对于忘记口令链接，请指定当用户在登录页面上单击**忘记口令**时所显示的链接。当用户单击此链接时，应用程序会将其定向到外部口令管理系统。例如：

```
http://localhost:8180/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsp
```

5 对于忘记口令返回链接，请指定用户执行完忘记口令过程后显示的链接。用户单击此链接，即可重定向到指定的链接。例如：

```
http://localhost/IDMProv
```

6 对于**忘记口令 Web 服务 URL**，请指定外部转发口令 WAR 用来回调 Identity Applications 的 Web 服务 URL。使用以下格式：

```
https://idmhost:sslport/idm/pwdmgt/service
```

返回链接必须使用 SSL，以确保与 Identity Applications 进行安全的 Web 服务通讯。有关详细信息，请参见配置应用程序服务器之间的 SSL 通讯 （第 203 页）。

7 手动将 ExternalPwd.war 复制到运行外部口令 WAR 功能的远程应用程序服务器部署目录。

测试外部忘记口令 配置

如果您拥有外部口令 WAR 文件并想要通过访问 " 忘记口令 " 功能来测试该功能，可以在以下位置访问它：

- 直接在浏览器中访问。转到外部口令 WAR 文件中的 " 忘记口令 " 页面。例如：http://localhost:8180/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsp。
- 在 User Application 登录页面上，单击**忘记口令**链接。

配置应用程序服务器之间的 SSL 通讯

如果您使用的是外部口令管理系统，则必须在部署 Identity Applications 与外部忘记口令管理 WAR 文件的 Tomcat 实例之间配置 SSL 通讯。有关详细信息，请参见 Tomcat 文档。

针对分布式环境或群集环境更新仪表板中的 SSPR 链接

安装过程假设您要将 SSPR 部署在 Identity Applications 和 Identity Reporting 所在的同一个应用程序服务器上。默认情况下，仪表板中**应用程序**页面上的内置链接使用指向本地系统上 SSPR 的相对 URL 格式。例如 \sspr\private\changepassword。如果在分布式环境或群集环境中安装应用程序，则必须更新 SSPR 链接的 URL。

有关详细信息，请参见 *Identity Applications 的帮助*。

1 以管理员身份登录仪表板。例如，以 uaadmin 身份登录。
2 单击**编辑**。
3 在 " 编辑主页项目 " 页面上，将鼠标悬停在要更新的项目上，然后单击编辑图标。例如，选择**更改我的口令**。
4 对于**链接**，请指定绝对 URL。例如：http://10.10.10.48:8180/sspr/changepassword。
5 单击**保存**。
6 对要更新的每个 SSPR 链接重复上述步骤。
7 完成后，单击**我已完成**。
8 注销，然后以普通用户身份登录以测试更改。

15.8 配置 Identity Applications 的设置

Identity Applications 配置实用程序可帮助您管理 User Application 驱动程序和 Identity Applications 的设置。 Identity Applications 安装程序将调用此实用程序的某个版本，使您能够更快地配置应用程序。您也可以在安装后修改其中的大部分设置。

默认情况下，用于运行配置实用程序 (configupdate.bat) 的文件位于 Identity Applications 的某个安装子目录 (C:\NetIQ\idm\apps\UserApplication) 中。

注释：在群集中，所有群集成员的配置设置都必须相同。

本节说明了配置实用程序中的设置。这些设置按选项卡组织。如果您要安装 Identity Reporting，安装过程会将报告的参数添加到实用程序中。

15.8.1 运行 Identity Applications 配置实用程序

1 在文本编辑器中打开 configupdate.properties 文件，并校验是否已配置以下选项：

```
edit_admin="true"

use_console="false"
```

2 在命令提示符下，运行配置实用程序 (configupdate.bat)。

注释：您可能需要等待几分钟，让实用程序启动。

15.8.2 用户应用程序参数

在配置 Identity Applications 时，此选项卡用于定义应用程序在与身份库通讯时所使用的值。某些设置对于完成安装过程必不可少。

默认情况下，该选项卡会显示基本选项。要查看所有设置，请单击**显示高级选项**。此选项卡包括以下设置组：

身份库设置

这组设置定义了可让 Identity Applications 访问身份库中用户身份和角色的设置。某些设置对于完成安装过程必不可少。

身份库服务器

必需

为 LDAP 服务器指定主机名或 IP 地址。例如：myLDAPhost。

LDAP 端口

指定身份库要用来侦听明文格式 LDAP 请求的端口。默认值是 389。

LDAP 安全端口

指定身份库要用来侦听使用安全套接字层 (SSL) 协议的 LDAP 请求的端口。默认值是 636。

如果 （在安装 eDirectory 之前）服务器上已装载的服务使用了默认端口，您必须指定其他端口。

身份库管理员

必需

指定 LDAP 管理员的身份凭证。例如， cn=admin. 身份库中必须已存在此用户。

Identity Applications 将使用此帐户来建立与身份库的管理连接。此值已使用主密钥进行过加密。

身份库管理员口令

必需

指定与 LDAP 管理员关联的口令。此口令已使用主密钥进行过加密。

使用公开匿名帐户

指定未登录的用户是否能够访问 LDAP 公共匿名帐户。

安全管理员连接

指定 RBPM 是否使用 SSL 协议来进行与管理员帐户相关的所有通讯。如果指定此设置，则无需 SSL 的其他操作便可在不使用 SSL 的情况下执行。

注释：此选项可能会对性能产生不良影响。

安全用户连接

指定 RBPM 是否使用 TLS/SSL 协议来进行与已登录用户帐户相关的所有通讯。如果指定此设置，则无需 TLS/SSL 的其他操作便可在不使用该协议的情况下执行。

注释：此选项可能会对性能产生不良影响。

身份库 DN

这组设置定义了可在 Identity Applications 和其他 Identity Manager 组件之间启用通讯的容器和用户帐户的判别名。某些设置对于完成安装过程必不可少。

根容器 DN

必需

指定根容器的 LDAP 判别名。如果没有在目录抽象层中指定搜索根，则将该判别名用作默认的实体定义搜索根。例如：o=mycompany。

用户容器 DN

必需

显示高级选项时，实用程序将在“身份库用户身份”下显示此参数。

指定用户容器的 LDAP 判别名 (DN) 或完全限定的 LDAP 名称。对于此设置，请注意以下事项：

- 允许此容器 （及其下）中的用户登录到 Identity Applications。
- 如果您已启动托管 Identity Applications 的 Tomcat，则无法使用 configupdate.bat 文件更改此设置。
- 此容器必须包含您在设置 User Application 驱动程序时指定的 User Application 管理员。否则，指定的帐户无法执行工作流程。

组容器 DN

必需

显示高级选项时，实用程序将在“身份库用户组”下显示此参数。

指定组容器的 LDAP 判别名 (DN) 或完全限定的 LDAP 名称。对于此设置，请注意以下事项：

- 目录提取层中的实体定义会使用此 DN。
- 如果您已启动托管 Identity Applications 的 Tomcat，则无法使用 configupdate.bat 文件更改此设置。

User Application 驱动程序

必需

指定 User Application 驱动程序的判别名。

例如，如果驱动程序为 UserApplicationDriver，驱动程序集为 MyDriverSet，并且驱动程序集位于 o=myCompany 环境中，则请指定 cn=UserApplicationDriver,cn=myDriverSet,o=myCompany。

用户应用程序管理员

必需

指定身份库中有权对指定的 User Application 用户容器执行管理任务的现有用户帐户。对于此设置，请注意以下事项：

- 如果您已启动托管 User Application 的 Tomcat，则无法使用 configupdate.bat 文件更改此设置。
- 要在部署 User Application 后更改此指派，请使用 User Application 中的管理 > 安全性页面。

- 此用户帐户有权使用 User Application 的管理选项卡来管理门户。
- 如果 User Application 管理员参与 iManager、 Designer 或 User Application （请求和批准选项卡）中公开的工作流程管理任务，您必须为此管理员授予相应的受托者权限，使其能够访问 User Application 驱动程序中包含的对象实例。有关详细信息，请参见《*User Application Administration Guide*》（User Application 管理指南）。

供应管理员

指定身份库中的一个现有用户帐户，该帐户将管理可在整个 User Application 中使用的 " 供应工作流程 " 功能。

要在部署 User Application 后更改此指派，请使用 User Application 中的管理 > 管理员指派页面。

合规性管理员

指定身份库中的一个现有帐户，该帐户将执行某个系统角色，以允许成员执行合规性选项卡上的所有功能。对于此设置，请注意以下事项：

- 要在部署 Identity Applications 后更改此指派，请使用 User Application 中的管理 > 管理员指派页面。
- 在配置更新期间，只有在未指派有效的合规性管理员时，对此值的更改才会生效。如果存在有效的合规性管理员，则将不保存更改。

角色管理员

指定一个角色，该角色允许成员创建、去除或修改所有角色，以及授予或撤消对任何用户、组或容器的任何角色指派。它还允许其角色成员运行任何用户的任何报告。对于此设置，请注意以下事项：

- 默认情况下，会对 User Application Admin 指派此角色。
- 要在部署 Identity Applications 后更改此指派，请使用 User Application 中的管理 > 管理员指派页面。
- 在配置更新期间，只有在未指派有效的角色管理员时，对此值的更改才会生效。如果存在有效的角色管理员，则将不保存更改。

安全管理员

指定一个角色，该角色为成员提供安全域内的所有功能。对于此设置，请注意以下事项：

- 安全管理员可以对安全域内的所有对象执行所有可能的操作。安全域允许安全管理员配置对 RBPM 内所有域中的所有对象的访问权限。安全管理员可以配置小组，还可以指派域管理员、委托管理员及其他安全管理员。
- 要在部署 Identity Applications 后更改此指派，请使用 User Application 中的管理 > 管理员指派页面。

资源管理员

指定一个角色，该角色为成员提供资源域内的所有功能。对于此设置，请注意以下事项：

- 资源管理员可以对资源域内的所有对象执行所有可能的操作。
- 要在部署 Identity Applications 后更改此指派，请使用 User Application 中的管理 > 管理员指派页面。

RBPM 配置管理员

指定一个角色，该角色为成员提供配置域内的所有功能。对于此设置，请注意以下事项：

- RBPM 配置管理员可以对配置域内的所有对象执行所有可能的操作。RBPM 配置管理员负责控制对 RBPM 内导航项目的访问权。此外， RBPM 配置管理员还配置委托和代理服务、供应用户界面及工作流程引擎。
- 要在部署 Identity Applications 后更改此指派，请使用 User Application 中的管理 > 管理员指派页面。

RBPM 报告管理员

指定报告管理员。默认情况下，安装程序列出的此值与其他安全性字段中的用户相同。

身份库用户身份

这组设置定义了可让 Identity Applications 与身份库中的用户容器通讯的值。某些设置对于完成安装过程必不可少。

仅当您选择了显示高级选项时，实用程序才显示这些设置。

用户容器 DN

必需

在不显示高级选项时，实用程序将在“身份库 DN”下显示此参数。

指定用户容器的 LDAP 判别名 (DN) 或完全限定的 LDAP 名称。对于此设置，请注意以下事项：

- 允许此容器 （及其下）中的用户登录到 Identity Applications。
- 如果您已启动托管 Identity Applications 的 Tomcat，则无法使用 configupdate.bat 文件更改此设置。
- 此容器必须包含您在设置 User Application 驱动程序时指定的 User Application 管理员。否则，指定的帐户无法执行工作流程。

用户搜索范围

指定身份库用户在搜索容器时可深入的范围。

用户对象类

指定 LDAP 用户的对象类。通常，该类为 inetOrgPerson。

登录属性

指定表示用户登录名的 LDAP 属性。例如：cn。

命名属性

指定在查找用户或组时用作标识符的 LDAP 属性。这不同于登录属性，登录属性仅在登录期间使用。例如：cn。

用户成员资格属性

（可选）指定表示用户的组成员资格的 LDAP 属性。指定名称时请不要使用空格。

身份库用户组

这组设置定义了可让 Identity Applications 与身份库中的组容器通讯的值。某些设置对于完成安装过程必不可少。

仅当您选择了显示高级选项时，实用程序才显示这些设置。

组容器 DN

必需

在不显示高级选项时，实用程序将在“身份库 DN”下显示此参数。

指定组容器的 LDAP 判别名 (DN) 或完全限定的 LDAP 名称。对于此设置，请注意以下事项：

- 目录提取层中的实体定义会使用此 DN。
- 如果您已启动托管 Identity Applications 的 Tomcat，则无法使用 configupdate.bat 文件更改此设置。

组容器范围

指定身份库用户在搜索组容器时可深入的范围。

组对象类

指定 LDAP 组的对象类。通常，该类为 groupofNames。

组成员资格属性

（可选）指定用户的组成员资格。不要在该名称中使用空格。

使用动态组

指定是否要使用动态组。

您还必须指定动态组对象类的值。

动态组对象类

仅当您选择了使用动态组时才适用。

指定 LDAP 动态组的对象类。通常，该类为 dynamicGroup。

身份库证书

这组设置定义了 JRE 密钥存储区的路径和口令。某些设置对于完成安装过程必不可少。

密钥储存区路径

必需

指定 Tomcat 在运行时要使用的 JRE 密钥存储区 (cacerts) 文件的完整路径。您可以手动输入路径，也可以浏览到 cacerts 文件。对于此设置，请注意以下事项：

- 在环境中，必须指定 RBPM 的安装目录。默认值设置的即为正确位置。
- Identity Applications 的安装程序将修改密钥存储区文件。在 Linux 上，用户必须有权写入此文件。

密钥储存区口令

必需

提供密钥存储区文件的口令。默认值为 changeit。

电子邮件服务器配置

本节定义用于启用电子邮件通知的值，您可以使用电子邮件通知来进行基于电子邮件的审批。有关详细信息，请参见《*NetIQ Identity Manager - Administrator's Guide to the Identity Applications*》（NetIQ Identity Manager - Identity Applications 管理员指南）中的 "Enabling Support for Digital Signatures"（启用数字签名支持），及 *Identity Applications 帮助*中的 " 管理通过电子邮件进行的审批 "。

通知模板主机

指定托管 Identity Applications 的 Tomcat 的名称或 IP 地址。例如：myapplication serverServer。

此值将替换电子邮件模板中的 $HOST$ 令牌。安装程序将使用此信息来创建供应请求任务和批准通知的 URL。

通知模板端口

指定托管 Identity Applications 的 Tomcat 的端口号。

此值将替换供应请求任务和批准通知中使用的电子邮件模板内的 $PORT$ 标记。

通知模板安全端口

指定托管 Identity Applications 的 Tomcat 的安全端口号。

此值将替换供应请求任务和批准通知中使用的电子邮件模板内的 $SECURE_PORT$ 标记。

通知模板协议

指定在发送用户电子邮件时要包含在 URL 中的非安全协议。例如：http。

此值将替换供应请求任务和批准通知中使用的电子邮件模板内的 $PROTOCOL$ 标记。

通知模板安全协议

指定在发送用户电子邮件时要包含在 URL 中的安全协议。例如：https。

此值将替换供应请求任务和批准通知中使用的电子邮件模板内的 $SECURE_PROTOCOL$ 标记。

通知 SMTP 电子邮件发件人

指定 Identity Applications 用来发送电子邮件通知的电子邮件帐户。

SMTP 服务器名称

指定 Identity Applications 用于供应电子邮件的 SMTP 电子邮件主机的 IP 地址或 DNS 名称。请不要使用 localhost。

服务器需要鉴定

指定您是否希望服务器要求鉴定。

您还必须指定电子邮件服务器的身份凭证。

用户名

*仅当您启用了**服务器需要鉴定**时才适用。*

指定电子邮件服务器的登录帐户名。

口令

*仅当您启用了**服务器需要鉴定**时才适用。*

指定邮件服务器的登录帐户口令。

使用 SMTP TLS

指定在邮件服务器之间进行传输期间，是否要保护电子邮件内容的安全。

电子邮件通知图像位置

指定要在电子邮件通知中包含的图像的路径。例如：http://localhost:8080/IDMProv/images。

对电子邮件签名

指定是否要在寄出的邮件中添加数字签名。

如果启用此选项，则还必须指定密钥存储区和签名密钥的设置。

密钥存储区路径

仅当您启用了对电子邮件签名时才适用。

指定要用于对电子邮件进行数字签名的密钥存储区 (cacerts) 文件的完整路径。您可以手动输入路径，也可以浏览到 cacerts 文件。

例如， C:\NetIQ\idm\apps\jre\lib\security\cacerts。

密钥存储区口令

仅当您启用了对电子邮件签名时才适用。

提供密钥存储区文件的口令。例如， changeit。

签名密钥的别名

仅当您启用了对电子邮件签名时才适用。

指定签名密钥在密钥存储区中的别名。例如， idmapptest。

签名密钥口令

仅当您启用了对电子邮件签名时才适用。

指定用于保护包含签名密钥的文件的口令。例如， changeit。

可信密钥储存区

这组设置定义了 Identity Applications 的可信密钥存储区的值。仅当您选择了显示高级选项时，实用程序才显示这些设置。

可信储存区路径

指定包含所有可信签名者的证书的可信密钥存储区的路径。如果此路径为空， Identity Applications 将从系统属性 javax.net.ssl.trustStore 中获取路径。如果该系统属性无法提供路径，安装程序默认使用 jre/lib/security/cacerts。

可信储存口令

指定可信密钥存储区的口令。如果将此字段留空， Identity Applications 将从系统属性 javax.net.ssl.trustStorePassword 中获取口令。如果该系统属性无法提供口令，安装程序默认使用 changeit。

此口令已使用主密钥进行过加密。

可信证书存储区类型

指定可信证书存储区路径是使用 Java 密钥存储区 (JKS) 还是 PKCS12 进行数字签名。

NetIQ Sentinel 数字签名证书和密钥

本节定义可让 Identity Manager 与 Sentinel 通讯以进行事件审计的值。仅当您选择了显示高级选项时，实用程序才显示这些设置。

Sentinel 数字签名证书

列出您希望 OAuth 服务器用来鉴定发送到 Sentinel 的审计讯息的自定义公共密钥证书。

Sentinel 数字签名私用密钥

指定您希望 OAuth 服务器用来鉴定发送到 Sentinel 的审计讯息的自定义私用密钥文件的路径。

杂项

仅当您选择了显示高级选项时，实用程序才显示这些设置。

OCSP URI

指定当客户端安装使用联机证书状态协议 (OCSP) 时要使用的统一资源标识符 (URI)。例如：http://host:port/ocspLocal。

OCSP URI 在线更新可信证书的状态。

授权配置路径

指定授权配置文件的完全限定名。

身份库索引

在安装期间，指定是否希望安装程序创建 manager、 ismanager 和 srvprvUUID 属性的索引。安装后，您可以修改设置，以指向索引的新位置。对于此设置，请注意以下事项：

- 如果这些属性没有索引， Identity Applications 用户可能会遭遇 Identity Applications 性能不佳的状况。
- 您可以在安装 Identity Applications 后使用 iManager 手动创建这些索引。
- 为获最佳性能，您应在安装期间创建索引。
- 索引必须处于联机模式，用户才可以使用 Identity Applications。
- 要创建或删除索引，还必须指定服务器 DN 的值。

服务器 DN

仅当您要创建或删除身份库索引时才适用。

指定要在其中创建或去除索引的 eDirectory 服务器。

一次只能指定一个服务器。要在多个 eDirectory 服务器上配置索引，必须多次运行 RBPM 配置实用程序。

重初始化 RBPM 安全性

指定是否要在完成安装过程时重设置 RBPM 安全性。您还必须重新部署 Identity Applications。

IDMReport URL

指定 Identity Manager Reporting Module 的 URL。例如：http://hostname:port/IDMRPT。

自定义主题环境名称

指定要用于在浏览器中显示 Identity Applications 的自定义主题的名称。

日志讯息标识符前缀

指定要在 idmuserapp_logging.xml 文件中 CONSOLE 和 FILE 追加器的布局模式内使用的值。默认值为 RBPM。

更改 RBPM 环境名称

指定是否要更改 RBPM 的环境名称。

您还必须指定 Roles and Resource 驱动程序的新名称和 DN。

RBPM 环境名称

仅当您选择了更改 RBPM 环境名称时才适用。

指定 RBPM 的新环境名称。

角色驱动程序 DN

仅当您选择了更改 RBPM 环境名称时才适用。

指定角色和资源驱动程序的 DN。

容器对象

这些参数只会在安装期间应用。

这组设置将帮助您定义容器对象的值或创建新的容器对象。

已选定

指定您要使用的容器对象类型。

容器对象类型

指定以下容器：位置、国家 / 地区、组织单位、组织或域。

也可以在 iManager 中自己定义容器，然后在添加新容器对象下面添加这些容器。

容器属性名称

指定与所指定容器对象类型关联的属性类型的名称。

添加新的容器对象：容器对象类型

指定可用作新容器的身份库中对象类的 LDAP 名称。

添加新的容器对象：容器属性名称

指定与新容器对象类型关联的属性类型的名称。

15.8.3 报告参数

在配置 Identity Applications 时，此选项卡定义用于管理 Identity Reporting 的值。当您安装 Identity Reporting 时，实用程序将添加此选项卡。

默认情况下，该选项卡会显示基本选项。要查看所有设置，请单击显示高级选项。此选项卡包括以下设置组：

- 电子邮件递送配置 （第 214 页）
- 报告保留值 （第 214 页）

- 修改区域设置 （第 215 页）
- 角色配置 （第 215 页）

电子邮件递送配置

这组设置定义了用于发送通知的值。

SMTP 服务器主机名

指定您希望 Identity Reporting 在发送通知时使用的电子邮件服务器的 DNS 名称或 IP 地址。请不要使用 localhost。

SMTP 服务器端口

指定 SMTP 服务器的端口号。

SMTP 使用 SSL

指定是否要使用 TLS/SSL 协议来与电子邮件服务器通讯。

服务器需要鉴定

指定是否要对与电子邮件服务器的通讯使用鉴定。

SMTP 用户名

指定要用于鉴定的电子邮件地址。

您必须指定一个值。如果服务器不需要鉴定，您可以指定无效的地址。

SMTP 用户口令

仅当您指定了服务器需要鉴定时才适用。

指定 SMTP 用户帐户的口令。

默认电子邮件地址

指定您希望 Identity Reporting 用作电子邮件通知来源的电子邮件地址。

报告保留值

这组设置定义了用于储存已完成报告的值。

报告单位 , 报告有效期

指定 Identity Reporting 在删除已完成报告之前保留这些报告的时间。例如，要指定六个月，请在**报告有效期**字段中输入 6，然后在**报告单位**字段中选择**月**。

报告位置

指定要将报告定义储存到的路径。例如， C:\NetIQ\idm\apps\IdentityReporting。

修改区域设置

这组设置定义了您希望 Identity Reporting 使用的语言的值。Identity Reporting 在搜索中使用特定的区域设置。有关详细信息，请参见 《Administrator Guide to NetIQ Identity Reporting》（NetIQ Identity Reporting 管理员指南）。

角色配置

这组设置定义了 Identity Reporting 用来生成报告的鉴定源的值。

添加鉴定源

指定您要为报告功能添加的鉴定源的类型。鉴定源可以是

- **默认值**
- **LDAP 目录**
- **文件**

15.8.4 鉴定参数

在配置 Identity Applications 时，此选项卡定义 Tomcat 用于将用户定向到 Identity Applications 和口令管理页面的值。

默认情况下，该选项卡会显示基本选项。要查看所有设置，请单击**显示高级选项**。此选项卡包括以下设置组：

- 鉴定服务器 （第 215 页）
- 鉴定配置 （第 216 页）
- 身份验证方法 （第 216 页）
- 口令管理 （第 217 页）
- Sentinel 数字签名证书和密钥 （第 218 页）

鉴定服务器

这组设置定义了 Identity Applications 连接鉴定服务器时使用的设置。

OAuth 服务器主机标识符

必需

指定向 OSP 颁发令牌的鉴定服务器的相对 URL。例如， 192.168.0.1.

OAuth 服务器 TCP 端口

指定鉴定服务器的端口。

OAuth 服务器正在使用 TLS/SSL

指定鉴定服务器是否使用 TLS/SSL 协议进行通讯。

可选 TLS/SSL 可信证书存储区文件

仅当您选择了 **OAuth 服务器正在使用 TLS/SSL**，*并且实用程序显示高级选项时才适用。*

可选 TLS/SSL 可信证书存储区口令

*仅当您选择了 **OAuth 服务器正在使用 TLS/SSL**，并且实用程序显示高级选项时才适用。*

指定用于装载 TLS/SSL 鉴定服务器的密钥存储区文件的口令。

注释：如果您未指定密钥存储区路径和口令，并且鉴定服务器的信任证书不在 JRE 可信证书存储区 (cacerts) 中，则 Identity Applications 将无法连接到使用 TLS/SSL 协议的鉴定服务。

鉴定配置

这组设置定义了鉴定服务器的设置。

管理员容器的 LDAP DN

必需

指定身份库中包含 OSP 必须鉴定的任何管理员用户对象的容器判别名。例如：ou=sa,o=data。

解析命名属性重复

指定用于区分包含相同 cn 值的多个 eDirectory 用户对象的 LDAP 属性的名称。默认值为 mail。

将鉴定源限制为环境

指定是要将身份库中用户和管理员容器内进行的搜索限制为仅涵盖这些容器中的用户对象，还是应使搜索范围涵盖子容器。

会话超时 （分钟）

指定当会话处于非活动状态多少分钟后，服务器会将用户会话置于超时状态。默认值为 20 分钟。

访问令牌有效期 （秒）

指定 OSP 访问令牌保持有效的秒数。默认值为 60 秒。

刷新令牌有效期 （小时）

指定 OSP 刷新令牌保持有效的秒数。 OSP 在内部使用刷新令牌。默认值为 48 小时。

身份验证方法

这组设置定义了可让 OSP 对登录到 Identity Manager 基于浏览器组件的用户进行鉴定的值。

方法 ：

指定当用户登录时您希望 Identity Manager 使用的鉴定类型。

- **名称和口令**：OSP 使用身份库校验鉴定。
- **Kerberos**：OSP 接受来自 Kerberos 票据服务器和身份库的鉴定。您还必须指定**映射属性名称**的值。
- **SAML 2.0**：OSP 接受来自 SAML 身份提供商和身份库的鉴定。您还必须指定**映射属性名称**和**元数据 URL** 的值。

映射属性名称

*仅当您指定了 **Kerberos** 或 **SAML** 时才适用。*

指定要映射到 Kerberos 票据服务器或身份提供程序中 SAML 表示的属性名称。

元数据 URL

*仅当您指定了 **SAML** 时才适用。*

指定 OSP 用于将鉴定请求重定向到 SAML 的 URL。

口令管理

这组设置定义了可让用户通过自助操作修改其口令的值。

口令管理提供程序

指定要使用的口令管理系统类型。

User Application （旧版）：使用 Identity Manager 惯常所用的口令管理程序。此选项还允许您使用外部口令管理程序。

忘记口令

仅当您要使用 SSPR 时，此复选框参数才适用。

指定是否希望用户不联系帮助中心自行恢复忘记的口令。

您还必须为 " 忘记口令 " 功能配置询问应答策略。有关详细信息，请参见 *《NetIQ Self Service Password Reset Administration Guide》*（NetIQ Self Service Password Reset 管理指南）。

忘记口令

*仅当您选择了 **User Application （旧版）** 时，此菜单列表才适用。*

指定是要使用 User Application 中集成的口令管理系统，还是使用外部系统。

- **内部**：使用默认的内部口令管理功能 ./jsps/pwdmgt/ForgotPassword.jsp （开头没有 http(s) 协议）。这将用户重定向到内置于 User Application 的 " 忘记口令 " 功能，而不是外部 WAR。
- **外部**：使用外部忘记口令 WAR 通过 Web 服务回调 User Application。您还必须指定外部系统的设置。

忘记口令链接

仅当您要使用外部口令管理系统时才适用。

指定指向 " 忘记口令 " 功能页面的 URL。在外部或内部口令管理 WAR 中指定 ForgotPassword.jsp 文件。

忘记口令返回链接

仅当您要使用外部口令管理系统时才适用。

指定**忘记口令返回链接**的 URL，用户可在执行完忘记口令操作后单击该链接以返回。

忘记口令 Web 服务 URL

仅当您要使用外部口令管理系统时才适用。

指定外部忘记口令 WAR 用来回调 User Application 以执行核心忘记口令功能的 URL。使用以下格式：

```
https://<idmhost>:<sslport>/<idm>/
pwdmgt/service
```

Sentinel 数字签名证书和密钥

本节定义可让 Identity Manager 与 Sentinel 通讯以进行事件审计的值。

Sentinel 数字签名证书

指定您希望 OSP 服务器用来鉴定发送到审计系统的审计讯息的自定义公共密钥证书。

有关配置 Novell Audit 证书的信息，请参见《*Novell Audit Administration Guide*》（Novell Audit 管理指南）中的 "Managing Certificates"（管理证书）。

Sentinel 数字签名私用密钥

指定您希望 OSP 服务器用来鉴定发送到审计系统的审计讯息的自定义私用密钥文件的路径。

15.8.5 SSO 客户端参数

在配置 Identity Applications 时，此选项卡可定义用于管理对应用程序的单点登录访问的值。

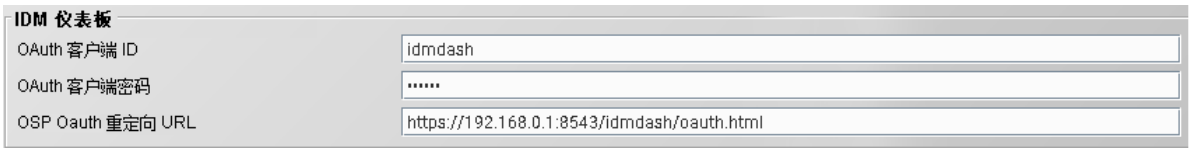
默认情况下，该选项卡会显示基本选项。要查看所有设置，请单击显示高级选项。此选项卡包括以下设置组：

- IDM 仪表板 （第 218 页）
- IDM 管理员 （第 219 页）
- RBPM （第 219 页）
- 报告 （第 220 页）
- IDM 数据收集服务 （第 221 页）
- DCS 驱动程序 （第 221 页）
- Self Service Password Reset （第 221 页）

IDM 仪表板

本节定义用户访问 Identity Manager 仪表板所需的 URL 的值，仪表板是 Identity Applications 的初始登录位置。

图 15-2 IDM 仪表板



OAuth 客户端 ID

必需

指定用于供鉴定服务器识别仪表板的单点登录客户端的名称。默认值为 idmdash。

OAuth 客户端机密

必需

指定仪表板的单点登录客户端的口令。

OSP OAuth 重定向 URL

必需

指定在完成鉴定后，鉴定服务器要将浏览器客户端重定向到的绝对 URL。

使用以下格式：protocol://server:port/path。例如， https://192.168.0.1:8543/idmdash/oauth.html。

IDM 管理员

本节定义用户访问 Identity Manager 管理员页面所需 URL 的值。

OAuth 客户端 ID

必需

指定用于供鉴定服务器识别 Identity Manager 管理员的单点登录客户端的名称。默认值为 idmadmin。

OAuth 客户端机密

必需

指定 Identity Manager 管理员的单点登录客户端的口令。

OSP OAuth 重定向 URL

必需

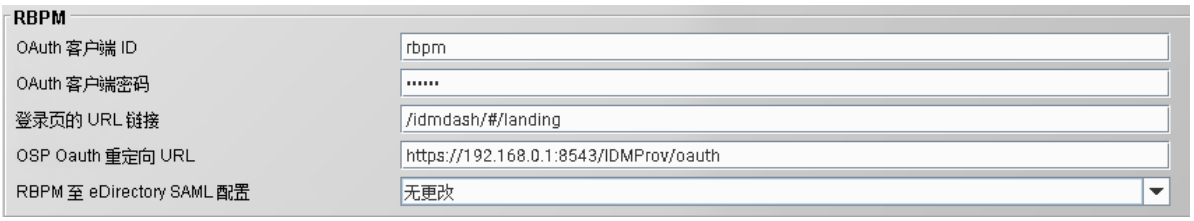
指定在完成鉴定后，鉴定服务器要将浏览器客户端重定向到的绝对 URL。

使用以下格式：protocol://server:port/path。例如， https://192.168.0.1:8543/idmadmin/oauth.html。

RBPM

这组设置定义了用户访问 User Application 所需 URL 的值。

图 15-3 *RBPM*



OAuth 客户端 ID

必需

指定用来供鉴定服务器识别 User Application 单点登录客户端的名称。默认值为 rbpm。

OAuth 客户端机密

必需

指定 User Application 单点登录客户端的口令。

登录页的 URL 链接

必需

指定用于从 User Application 中访问仪表板的相对 URL。默认值为 /landing。

OSP OAuth 重定向 URL

必需

指定在完成鉴定后，鉴定服务器要将浏览器客户端重定向到的绝对 URL。

使用以下格式：protocol://server:port/path。例如， https://192.168.0.1:8543/IDMProv/oauth。

RBPM 至 eDirectory SAML 配置

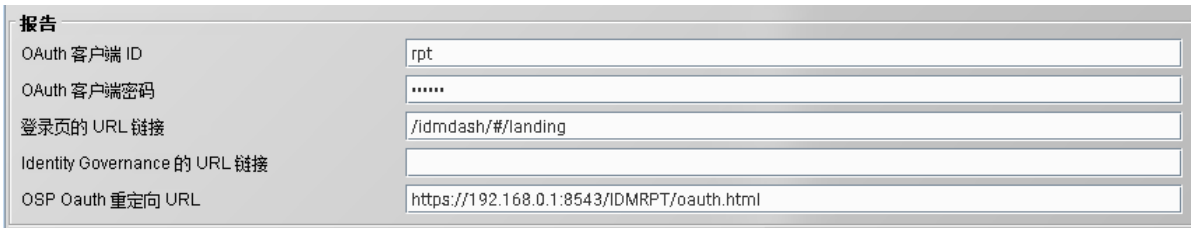
必需

指定 SSO 鉴定所需的 RBPM 至 eDirectory SAML 设置。

报告

这组设置定义了用户访问 Identity Reporting 所需 URL 的值。仅当您将 Identity Reporting 添加到 Identity Manager 解决方案时，实用程序才会显示这些值。

图 15-4 报告



OAuth 客户端 ID

必需

指定用来供鉴定服务器识别 Identity Reporting 单点登录客户端的名称。默认值为 rpt。

OAuth 客户端机密

必需

指定 Identity Reporting 单点登录客户端的口令。

登录页的 URL 链接

必需

指定用于从 Identity Reporting 中访问仪表板的相对 URL。默认值为 /idmdash/#/landing。

如果您将 Identity Reporting 和 Identity Applications 安装到不同的服务器中，请指定绝对 URL。使用以下格式：protocol://server:port/path。例如， https://192.168.0.1:8543/IDMRPT/oauth。

OSP OAuth 重定向 URL

必需

指定在完成鉴定后，鉴定服务器要将浏览器客户端重定向到的绝对 URL。

使用以下格式：protocol://server:port/path。例如， https://192.168.0.1:8543/IDMRPT/oauth。

IDM 数据收集服务

本节定义用户访问 Identity Manager 数据收集服务所需 URL 的值。

OAuth 客户端 ID

必需

指定用于供鉴定服务器识别 Identity Manager 数据收集服务的单点登录客户端的名称。默认值为 idmdcs。

OAuth 客户端机密

必需

指定 Identity Manager 数据收集服务的单点登录客户端的口令。

OSP OAuth 重定向 URL

必需

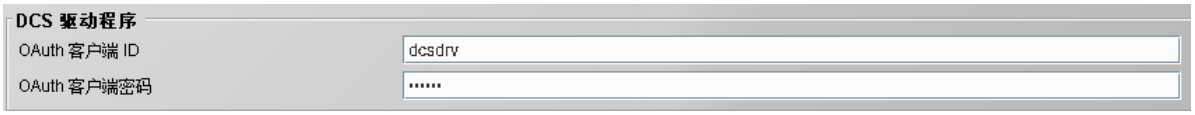
指定在完成鉴定后，鉴定服务器要将浏览器客户端重定向到的绝对 URL。

使用以下格式：protocol://server:port/path。例如， https://192.168.0.1:8543/idmdcs/oauth.html。

DCS 驱动程序

这组设置定义了用于管理数据收集服务驱动程序的值。

图 15-5



OAuth 客户端 ID

指定用来供鉴定服务器识别数据收集服务驱动程序的单点登录客户端的名称。此参数的默认值为 dcsdrv。

OAuth 客户端机密

指定数据收集服务驱动程序的单点登录客户端的口令。

Self Service Password Reset

本节定义用户访问 SSPR 所需 URL 的值。

OAuth 客户端 ID

必需

指定用来供鉴定服务器识别 SSPR 单点登录客户端的名称。默认值为 sspr。

OAuth 客户端机密

必需

指定 SSPR 单点登录客户端的口令。

OSP OAuth 重定向 URL

必需

指定在完成鉴定后，鉴定服务器要将浏览器客户端重定向到的绝对 URL。

使用以下格式：protocol://server:port/path。例如， https://192.168.0.1:8543/sspr/public/oauth.html。

15.8.6 CEF 审计参数

本节定义用于管理 CEF 审计参数的值。

发送审计事件

指定是否要使用 CEF 在 Identity Applications 中审计事件。

目标主机

指定审计服务器的 DNS 名称或 IP 地址。

目标端口

指定审计服务器的端口。

网络协议

指定审计服务器用来接收 CEF 事件的网络协议。

使用 TLS

仅当您要使用 TCP 作为网络协议时适用。

指定审计服务器是否配置为将 TLS 与 TCP 搭配使用。

中间事件储存目录

指定在将 CEF 事件发送到审计服务器之前超速缓存目录的位置。

注释：请确保对超速缓存目录设置了 novlua 许可权限。否则，您将不能访问 IDMDash 和 IDMProv 应用程序，并且系统也不会在超速缓存目录中记录 OSP 事件。例如，您可以使用 chown novlua:novlua /<directorypath> 命令更改该目录的许可权限和所有权，其中， <directorypath> 是超速缓存文件目录路径。

V 安装 Identity Reporting

本部分将引导您完成安装运行报告所需组件的过程。安装过程包括应用程序所需的全部组件：

- NetIQ Identity Reporting
- Identity Manager Managed System Gateway Driver （MSGW 驱动程序）
- Identity Manager Driver for Data Collection Service （DCS 驱动程序）

安装文件位于 Identity Manager 安装包的 .iso 映像文件中的 \products\Reporting 目录下。默认情况下，安装程序将在 C:\NetIQ\idm\apps\IDMReporting 中安装组件。

为方便起见， Identity Manager 安装包中包含了 Sentinel Log Management for IGA (Sentinel) 作为内置审计服务。有关详细信息，请参见 《NetIQ Identity Manager Setup Guide for Linux》（NetIQ Identity Manager 安装指南 - Linux）中的 “Installing Sentinel Log Management for Identity Governance and Administration” （安装 Sentinel Log Management for Identity Governance and Administration）。

NetIQ 建议您在开始之前，先查看安装过程。有关详细信息，请参见第 16 章 “ 规划安装 Identity Reporting” （第 225 页）。

16 规划安装 Identity Reporting

本章提供有关准备安装 Identity Reporting 组件的指导。您可以使用 Sentinel 来审计事件。

16.1 Identity Reporting 的安装核对清单

NetIQ 建议您完成以下核对清单中的步骤：

	核对清单项目
❑	1. 了解 Identity Manager 各组件之间的交互。有关详细信息，请参见第 3.3.4 节 “Identity Reporting”（第 24 页）。
❑	2. 确定要为 Identity Manager 组件使用哪些服务器。有关详细信息，请参见第 5.3 节 “ 建议的安装方案和服务器设置 ”（第 39 页）。
❑	3. 查看有关安装 Identity Reporting 的注意事项。有关详细信息，请参见第 16.3 节 “ 安装 Identity Reporting 组件的先决条件 ”（第 226 页）。
❑	4. 查看托管 Identity Reporting 的计算机所要满足的硬件和软件要求。有关详细信息，请参见第 16.5 节 “Identity Reporting 的系统要求 ”（第 228 页）。
❑	5. 确保已安装 Identity Applications。有关详细信息，请参见第 15.1 章 “ 规划安装 Identity Applications”（第 165 页）。
❑	6. 要审计事件，请在 Linux 服务器上安装 Sentinel。有关详细信息，请参见 《NetIQ Identity Manager Setup Guide for Linux》（NetIQ Identity Manager 安装指南 - Linux）中的 “Installing Sentinel Log Management for Identity Governance and Administration”（安装 Sentinel Log Management for Identity Governance and Administration）。
❑	7. 确保要安装 Identity Reporting 的服务器上已装有 Tomcat 之类的应用程序服务器。有关详细信息，请参见第 12.2 章 “ 安装 PostgreSQL 和 Tomcat”（第 143 页）。
❑	8. （视情况而定）要使用 Apache Log4j 服务来记录 Tomcat 中的事件，请确保您有相应的文件。有关详细信息，请参见第 13.1.4 节 “ 使用 Apache Log4j 服务记录登录 ”（第 150 页）。
❑	9. 安装 Identity Reporting： ◆ 要执行引导式安装，请参见第 17.1 节 “ 使用引导式过程安装 Identity Reporting”（第 231 页）。 ◆ 要以无提示模式安装 Reporting，请参见第 17.2 节 “ 以无提示模式安装 Identity Reporting”（第 235 页）。

	核对清单项目
❑	10. 完成 Identity Reporting 的设置。有关详细信息，请参见第 18 章 " 配置 Identity Reporting" （第 239 页）。
❑	11. 配置受管系统网关驱动程序和数据收集服务驱动程序。有关详细信息，请参见第 19.1 节 " 配置 Identity Reporting 的驱动程序 " （第 241 页）。
❑	12. 部署并启动驱动程序。有关详细信息，请参见第 19.2 节 " 部署并启动 Identity Reporting 的驱动程序 " （第 246 页）。
❑	13. 配置驱动程序的环境。有关详细信息，请参见第 19.3 节 " 配置运行时环境 " （第 251 页）。
❑	14. 配置 Identity Manager 和 eDirectory，以向驱动程序发送数据。有关详细信息，请参见第 19.4 节 " 设置驱动程序的审计标志 " （第 258 页）。

16.2 了解 Identity Reporting 组件的安装过程

您可以将 Sentinel、 Identity Reporting 和 Reporting 驱动程序安装在同一台服务器上。但是，由于工作负载的原因， NetIQ 建议将 Sentinel 和 Reporting 安装在不同的服务器上。

如果进行全新安装，安装程序将在该数据库中创建表并校验连接性。程序还会安装 PostgreSQL JDBC 驱动程序的 JAR 文件，并自动使用此文件建立数据库连接。

如果您已将您的数据 （例如 SIEM）从 EAS 迁移到 PostgreSQL 数据库，则安装程序将连接到现有数据库。

Identity Reporting 的安装程序会执行以下功能：

- 允许您选择应用程序服务器平台
- 将客户端 WAR 文件 （DCS 和 Reporting）部署到 Tomcat，该文件中包含用于运行报告的用户界面组件
- 部署核心 WAR 文件 （DCS 和 Reporting），其中包含运行报告所需的核心 REST 服务
- 部署 API WAR 文件，其中包含运行报告所需的 REST 服务的文档
- 部署 API WAR 文件，其中包含运行报告所需的 Identity Manager 数据收集服务
- 配置 Identity Reporting 的鉴定服务
- 配置 Identity Reporting 的电子邮件递送系统
- 配置 Identity Reporting 的核心报告服务
- 为 Identity Reporting 创建用户帐户 （**idmrptsrv** 和 **idmrptuser**）
- 创建用来与 Sentinel 交互的用户帐户 （**appuser** 和 **rptuser**）

16.3 安装 Identity Reporting 组件的先决条件

在安装 Identity Reporting 时，请注意以下先决条件和事项：

- 需要以下 Identity Manager 组件的受支持且经过配置的版本：
  - Identity Applications，包括 User Application 驱动程序

- Sentinel 安装在单独的 Linux 计算机上。
- Driver for Data Collection Service
- 受管系统网关服务的驱动程序

有关这些组件的所需版本和增补程序的详细信息，请参见最新的 《发行说明》。有关安装驱动程序的详细信息，请参见第 19 章 " 管理运行报告所需的驱动程序 "（第 241 页）。

- 请不要将 Identity Reporting 安装在群集环境中的服务器上。
- 如果您要使用本地数据库以外的数据库，则应在 Identity Reporting 安装期间在其他服务器上创建数据库，并指定细节。
- （视情况而定）要针对 Oracle 12c 数据库运行报告，必须安装相应的 JDBC 文件。有关详细信息，请参见第 18.1 节 " 对 Oracle 数据库运行报告 "（第 239 页）。
- （视情况而定）您可以使用自己的 Tomcat 安装程序，而不使用 Identity Manager 安装套件中提供的安装程序。但是，要将 Apache Log4j 服务与您的 Tomcat 版本配合使用，请确保安装了相应的文件。有关详细信息，请参见第 13.1.4 节 " 使用 Apache Log4j 服务记录登录 "（第 150 页）。
- 向您要授予报告功能访问权限的所有用户指派报告管理员角色。
- 确保 Identity Manager 环境中的所有服务器上都设置了相同的时间。如果您未同步服务器上的时间，有些报告在执行后可能是空的。例如，如果托管 Identity Manager 引擎的服务器和仓库的服务器的时戳不同，则此问题可能会影响与新用户相关的数据。如果您创建了一个用户，随后对其进行了修改，报告中会填充相应的数据。
- 安装过程会在 Tomcat 的 setenv.bat 文件中修改 JRE 映射的 JAVA_OPTs 或 CATALINA_OPTS 项。

  默认情况下， Tomcat 的便捷安装程序会将 setenv.bat 文件放在 C:\NetIQ\idm\apps\tomcat\bin 目录中。安装程序还会在该文件中配置 JRE 位置。

16.4 Identity Reporting 的身份审计事件

本节提供有关如何标识 Identity Manager 报告和自定义报告所需的不同审计事件的信息。您可以解压缩所有报告源并运行以下脚本来标识审计事件：

```
find . -name *.jrxml -print0 |xargs -0 grep -H "'000[B3]" | perl -ne '($file) = /
^\.\/(.*?)\//;@a = /000[3B]..../g; foreach $a (@a) { print "$file;$a\n"}' |sort -u
```

本节提供有关如何标识和选择 Identity Manager 报告和自定义报告的不同审计事件的信息：

事件名称	审计标志
鉴定和口令更改	**选择使用 SSPR 的审计标志：**起动 **SSPR 配置编辑器** > **审计配置** > 选择以下审计标志之一： ◆ 鉴定 ◆ 更改口令 ◆ 解除锁定口令 ◆ 恢复口令 ◆ 入侵者尝试 ◆ 入侵者锁定 ◆ 入侵者锁定用户 **选择使用 iManager 的审计标志：**转到 **iManager 角色和任务** > **eDirectory 审计** > **审计配置** > **Novell Audit** 选择以下审计标志之一： ◆ 更改口令 ◆ 校验口令 ◆ 登录 ◆ 注销
所有其他报告事件	转到 **NetIQ Identity Manager UserApp** > **管理** > **日志记录** > **启用审计服务**

16.5 Identity Reporting 的系统要求

本节提供要安装 Identity Reporting 组件的服务器的最低要求。

类别	要求
处理器	1 GHz 处理器
磁盘空间	1 GB **注释：**为支持应用程序的内容 （例如数据库和应用程序服务器日志）留出足够的空间 .
内存	512 MB （建议 4 GB）
操作系统 （经认可）	以下 64 位操作系统之一： ◆ Windows Server 2016 ◆ Windows Server 2012 R2 ◆ Windows Server 2012 NetIQ 建议您在安装 Identity Manager 之前，按照制造商的自动更新工具应用最新的操作系统增补程序。

类别	要求
操作系统 （受支持）	经认可操作系统的最新版服务包 **注释：***受支持*指操作系统尚未经过测试，但预期可以正常工作。
虚拟化系统	◆ Hyper-V Server 2012 R2 ◆ VMWare ESX 5.5 及更高版本 ◆ 包含 Hyper-V 的 Windows Server 2012 R2 Virtualization （受支持） NetIQ 支持在为运行 NetIQ 产品的操作系统提供官方支持的企业级虚拟化系统上安装 Identity Manager。只要虚拟化系统的供应商为这些操作系统提供官方支持， NetIQ 就可支持这些系统上的整个 Identity Manager 堆栈。
数据库	◆ PostgreSQL 9.6.6 ◆ Oracle 12c ◆ MsSQL 2014、 2016
应用程序服务器	Apache Tomcat 8.5.27
Java	Java 开发工具包 (JDK) 或者 Sun (Oracle) 提供的 Java 运行时环境 (JRE) 1.8.0_162 或更高版本
Web 浏览器	以下任意浏览器 （最低版本）： **桌面** ◆ Apple Safari 9 ◆ Apple Safari 5.1.7 for Windows ◆ Google Chrome 61 ◆ Microsoft Internet Explorer 11 ◆ Mozilla Firefox 51 **iPad** ◆ Apple Safari 9 ◆ Google Chrome 61 **注释：**必须在浏览器中启用 Cookie。如果禁用了 Cookie，该产品将不会正常运行。
Audit	Sentinel Log Management for IGA

17 安装 Identity Reporting

本章介绍 Identity Reporting 的安装过程。

17.1 使用引导式过程安装 Identity Reporting

以下过程介绍了如何使用安装向导安装 Identity Reporting。要执行无提示或无人照管安装，请参见第 17.2 节 “ 以无提示模式安装 Identity Reporting” （第 235 页）。

要准备安装，请查看第 16.5 节 “Identity Reporting 的系统要求 ” （第 228 页）中列出的先决条件和系统要求。另请参见版本随附的 《发行说明》。

1. 登录要安装 Identity Reporting 的计算机。
2. 停止 Tomcat。
3. （视情况而定）如果您已获取 Identity Manager 安装包的 .iso 映像文件，请导航到包含 Identity Reporting 安装文件的目录 （默认位于 \products\Reporting 目录中）。
4. （视情况而定）如果您已从 NetIQ 下载网站下载了 Identity Reporting 安装文件，请完成以下步骤：
   - **4a** 浏览到所下载映像的 .tgz 文件。
   - **4b** 将该文件的内容解压缩到本地计算机上的某个文件夹中。
5. 从包含安装文件的目录中运行 rpt-install-win.exe 文件。
6. 在安装程序中，指定要用于安装的语言，然后单击**确定**。
7. 查看 “ 简介 ” 文本，然后单击**下一步**。
8. 接受许可协议，然后单击**下一步**。
9. 使用以下参数完成引导式过程：
   - **安装文件夹**

     指定安装程序要在其中创建应用程序文件 （包括安装日志文件、助手脚本和配置脚本）的目录路径。
   - **Reporting 安装**

     表示要将 Identity Reporting 添加到的环境及其设置。为 **Identity Manager** 指定以下值：

     身份库服务器

     指定 eDirectory 服务器的主机名。

安全 LDAP 端口

指定您要用于通过 SSL 与 eDirectory 服务器建立 LDAP 连接的端口。默认端口为 636。

供应主目录

指定 Identity Manager 供应主目录位置。这可以是完整的应用程序服务器 URL，也可以是 URL 的相对路径。

- **应用程序服务器细节**

表示要运行 Identity Reporting 的 Tomcat。必须已安装该应用程序服务器。

次要

指定当前安装是否位于群集的次要节点上。

Tomcat 根文件夹

指定 Tomcat 实例的路径。例如 C:\NetIQ\idm\apps\tomcat。

Java JRE 基本文件夹

指定 Java JRE 基本文件夹位置。

该路径包含配置更新实用程序文件，用于在安装 Identity Reporting 后起动此实用程序。

- **应用程序地址**

表示托管 Identity Reporting 的服务器的设置。

协议

指定是要使用 *http* 还是 *https*。要使用 SSL 进行通讯，请指定 https。

主机名

指定 Tomcat 的 DNS 名称或 IP 地址。请不要使用 localhost。

端口

指定您希望 Tomcat 在与 Identity Reporting 应用程序通讯时使用的端口。

连接外部鉴定服务器

指定是否要用不同的 Tomcat 实例来托管鉴定服务器 (OSP)。鉴定服务器包含可登录 Identity Reporting 的用户的列表。

如果选择此设置，请指定鉴定服务器的**协议**、**主机名**和**端口**值。

- **鉴定服务器细节**

指定 Identity Reporting 服务的口令。

Identity Manager 使用此口令来连接鉴定服务器上的 OSP 客户端。

- **数据库细节**

表示 Reporting 数据库的设置，包括您是要让安装进程创建数据库还是生成一个 SQL 文件以便稍后再创建数据库。

数据库名称

根据您的要求指定数据库名称：

- 在执行全新安装时，请指定 Reporting 数据库的名称。例如， idmrptdb 或 SIEM。
- 如果您要从 EAS 迁移，请指定 EAS 数据库的名称，例如 SIEM。

数据库主机

根据您的要求指定数据库主机：

- 在执行全新安装时，请指定需要在其中创建数据库的服务器的 DNS 名称或 IP 地址。
- 如果您要从 EAS 迁移，请指定托管 SIEM 数据库的服务器的 DNS 名称或 IP 地址。

数据库类型

选择要使用的数据库。

如果选择了 **Oracle**，请指定以下细节：

- **JDBC 驱动程序 jar**

  指定 Oracle JDBC 驱动程序 jar 文件的路径。例如 C:\oracle\ojdbc7.jar。

  有关详细信息，请参见第 18.1 节 " 对 Oracle 数据库运行报告 "（第 239 页）。

- **JDBC 驱动程序类名**

  指定 JDBC 驱动程序的类。

- **JDBC 驱动程序类型**

  指定 JDBC 驱动程序的类型。

如果选择了 **PostgresSQL**，请单击**下一步**。

共享口令

可让您为所有 Reporting 用户指定一个用于连接数据库的口令。

指定每个用户的口令

可让您为每个 Reporting 用户指定用于连接数据库的唯一口令。需要为 idm_rpt_data_password、 idm_rpt_cfg_password 和 idmrptuserpassword 指定口令。

数据库端口

指定用于连接数据库的端口。默认端口为 5432。

立即配置数据库或在启动时配置

指出您可以选择以下数据库登录设置：让安装程序立即创建数据库，或在启动 Reporting 期间创建。此外，您还必须指定以下值：

- **DBA 用户 ID**

  指定 SIEM 数据库服务器管理帐户的名称。例如， *postgres.*

- **DBA 口令**

  指定数据库管理帐户的口令。

- **测试数据库连接：**指定是否要让安装程序测试您为数据库指定的值。

  当您单击**下一步**或按 **Enter** 后，安装程序即会尝试建立连接。

注释：如果数据库连接失败，您可以继续安装。但是，必须在安装后手动创建表并连接到数据库。有关详细信息，请参见第 17.3 节 " 手动生成数据库纲要 "（第 236 页）。

生成 SQL 供日后使用

指示安装程序生成数据库管理员将用于在您完成安装过程后创建数据库的 SQL 文件。要在安装后创建数据库，请参见第 17.3 节 " 手动生成数据库纲要 "（第 236 页）。

- **默认语言**

指定您希望 Identity Reporting 在搜索时使用的语言。

- **身份库身份凭证**

  表示 Identity Reporting 用于连接身份库的设置。

  身份库管理员

  指定 LDAP 管理员的判别名。例如， cn=admin. 身份库中必须已存在此用户。

  身份库管理员口令

  指定身份库管理员的口令。

  密钥存储区路径

  指定 Tomcat 在运行时要使用的 JRE 密钥存储区 (cacerts) 文件的完整路径。

  密钥储存区口令

  提供密钥存储区文件的口令。

  报告管理员角色容器 DN

  指定储存报告管理员角色的容器的 DN。

  报告管理员用户 DN

  指定身份库中有权执行 Identity Reporting 管理任务的现有用户帐户。

- **用户应用程序驱动程序**

  表示应用程序驱动程序、驱动程序集和驱动程序集容器的名称。

  User Application 驱动程序

  指定 User Application 驱动程序的名称。

  驱动程序集名称

  指定驱动程序集的名称。

  驱动程序集容器

  指定驱动程序集容器的名称。

- **电子邮件递送**

  表示发送报告通知的 SMTP 服务器的设置。要在安装后修改这些设置，请使用 RBPM 配置实用程序。

  默认电子邮件地址

  指定您希望 Identity Reporting 用作电子邮件通知来源的电子邮件地址。

  SMTP 服务器

  指定 Identity Reporting 用于发送通知的 SMTP 电子邮件主机的 IP 地址或 DNS 名称。请不要使用 localhost。

  SMTP 服务器端口

  指定 SMTP 服务器的端口号。默认端口为 465。

  对 SMTP 使用 SSL

  指定是否要使用 SSL 协议来与 SMTP 服务器通讯。

  需要服务器鉴定

  指定是否要对与 SMTP 服务器之间的通讯使用鉴定。此外，您还必须指定以下值：

  - ***SMTP 用户名***

    指定 SMTP 服务器登录帐户的名称。

- ***SMTP 口令***

  指定 SMTP 服务器登录帐户的口令。

- **报告细节**

  表示报告定义及已完成报告的设置。

  将完成的报告保留

  指定 Identity Reporting 在删除已完成报告之前应保留这些报告的时间。

  例如，要指定六个月，请输入 6 然后选择月。

  报告定义的位置

  指定要将报告定义储存到的路径。

  例如， C:\NetIQ\idm\apps\IdentityReporting。

10 在 " 安装前摘要 " 窗口中单击安装。

17.2 以无提示模式安装 Identity Reporting

无提示 （非交互式）安装不显示用户界面，也不向用户提出任何问题。相反，系统会使用 .properties 文件中的信息。您可以使用默认文件运行无提示安装，或者编辑该文件以自定义安装过程。要执行引导式安装，请参见使用引导式过程安装 Identity Reporting （第 231 页）。

要准备安装，请查看第 16.5 节 "Identity Reporting 的系统要求 " （第 228 页）中列出的先决条件和系统要求。另请参见版本随附的 《发行说明》。

1 （视情况而定）如果不想在 .properties 文件中为无提示安装指定用于安装的管理员口令，请使用 export 或 set 命令。例如：set NOVL_ADMIN_PWD=*myPassWord*

无提示安装过程将从环境中读取口令，而不是从 .properties 文件中读取。

指定以下口令：

NOVL_DB_RPT_USER_PASSWORD

指定 SIEM 数据库管理员的口令。

NOVL_IDM_SRV_PWD

指定用于报告的数据库纲要和对象拥有者的口令。

NOVL_IDM_USER_PWD

指定对报告数据具有只读访问权的 idmrptuser 的口令。

NOVL_ADMIN_PWD

（视情况而定）要在登录时启用子容器搜索，请指定 LDAP 管理员的口令。

NOVL_SMTP_PASSWORD

（视情况而定）要对电子邮件通讯使用鉴定，请指定默认 SMTP 电子邮件用户的口令。

2 要指定安装参数，请完成以下步骤：

2a 确保 .properties 文件位于安装可执行文件所在的目录中。

为方便起见， NetIQ 提供了两个 .properties 文件 （这些文件默认位于 .iso 映像的 products\Reporting 目录中）：

- rpt_installonly.properties，使用默认安装设置
- rpt_configonly.properties，用于自定义安装设置

2b 在文本编辑器中打开 .properties 文件。

2c 指定参数值。有关参数的说明，请参见步骤 9 （第 231 页）。

注释：用于安装 Standard Edition 的 .properties 文件中只包含该版本所需的参数。

2d 保存并关闭文件。

3 要起动安装过程，请输入以下命令：

rpt-install.exe -i silent -f *path_to_properties_file*

注释：如果 .properties 文件不在安装脚本所在的目录中，则您必须指定该文件的完整路径。该脚本会将必要的文件解压缩到一个临时目录，然后起动无提示安装。

17.3 手动生成数据库纲要

您可以在安装后重创建数据库表，而无需重新安装。本节将会帮助您创建数据库纲要。

1 使用 services.msc 文件停止 Tomcat。

2 （视情况而定）创建一个新数据库。

如果您的数据库不是在同一服务器上运行，则必须连接到该数据库服务器。对于远程安装的 PostgreSQL 数据库，请校验该数据库服务器是否正在运行。要连接到远程 PostgreSQL 数据库，请参见第 17.4 节 " 连接远程 Remote PostgreSQL 数据库 " （第 237 页）。如果您要连接到 Oracle 数据库，请确保已在该数据库服务器中创建 Oracle 数据库实例。有关更多信息，请参见 Oracle 文档。

3 使用 C:\NetIQ\idm\apps\IdentityReporting\sql 中的下列 SQL 将所需角色添加到数据库中。

- **PostgreSQL：**create_dcs_roles_and_schemas.sql 和 create_rpt_roles_and_schemas.sql
- **Oracle：**create_dcs_roles_and_schemas-orcale.sql 和 create_rpt_roles_and_schemas-orcale.sql

4 要创建 IDM_RPT_DATA、 IDM_RPT_CFG 和 IDMRPTUSER 角色，请执行以下操作：

- **PostgreSQL：**按给定顺序运行以下命令：

```
Select CREATE_DCS_ROLES_AND_SCHEMAS('<Set pwd for IDM_RPT_DATA>');

Select CREATE_RPT_ROLES_AND_SCHEMAS('<Set pwd for IDM_RPT_CFG>', '<Set pwd
for IDMRPTUSER>');
```

- **Oracle：**按给定顺序运行以下命令：

```
begin
CREATE_DCS_ROLES_AND_SCHEMAS('<Set pwd for IDM_RPT_DATA>');
end;

begin
CREATE_RPT_ROLES_AND_SCHEMAS('<Set pwd for IDM_RPT_CFG>', '<Set pwd for
IDMRPTUSER>');
end;
```

5 将 get_formatted_user_dn 函数添加到 IDM_RPT_DATA 纲要中。

5a 以数据库管理员用户的身份登录数据库。

5b 从 C:\NetIQ\idm\apps\IdentityReporting\sql 中添加 get_formatted dn 函数。

对于 PostgreSQL，请查找 get_formatted_user_dn.sql ；对于 Oracle，请查找 get_formatted_user_dn-oracle.sql。

6 清除位于 C:\NetIQ\idm\apps\IdentityReporting\sql 中的下列 .sql 文件的数据库校验和：

- DbUpdate-01-run-as-idm_rpt_cfg.sql
- DbUpdate-02-run-as-idm_rpt_cfg.sql
- DbUpdate-03-run-as-idm_rpt_data.sql
- DbUpdate-04-run-as-idm_rpt_data.sql
- DbUpdate-05-run-as-idm_rpt_data.sql
- DbUpdate-06-run-as-idm_rpt_cfg.sql

6a 在每个 SQL 的开头追加下面一行：

```
update DATABASECHANGELOG set MD5SUM = NULL;
```

修改后的内容应该类似如下：

```
-- *********************************************************************
-- Update Database Script
-- *********************************************************************
-- Change Log: IdmDcsDataDropViews.xml
-- Ran at: 2/23/18 5:17 PM
-- Against: IDM_RPT_CFG@jdbc:oracle:thin:@192.99.170.20:1521/orcl
-- Liquibase version: 3.5.1
-- *********************************************************************
update databasechangelog set md5sum = null;
```

6b 运行相应用户的每个 SQL。

7 将更改提交到数据库。

8 使用 services.msc 文件启动 Tomcat。

17.4 连接远程 Remote PostgreSQL 数据库

如果您的 PostgreSQL 数据库安装在单独的服务器上，则需要在该远程数据库的 postgresql.conf 和 pg_hba.conf 文件中更改默认设置。

1 在 postgresql.conf 文件中更改侦听地址。

默认情况下，PostgreSQL 允许侦听 localhost 连接，不允许远程 TCP/IP 连接。要允许远程 TCP/IP 连接，请将以下条目添加到 C:\NetIQ\idm\postgres\data\postgresql.conf 文件中：

```
listen_addresses = '*'
```

如果服务器上有多个接口，可以指定要侦听的特定接口。

2 将客户端鉴定条目添加到 pg_hba.conf 文件中。

默认情况下， PostgreSQL 只接受来自 localhost 的连接。它会拒绝远程连接。这通过应用访问控制规则来控制，该规则允许用户在提供有效口令 （md5 关键字）后从某个 IP 地址登录。要接受远程连接，请将以下条目添加到 C:\NetIQ\idm\postgres\data\pg_hba.conf 文件中。

```
host all all 0.0.0.0/0 md5
```

例如， 192.168.104.24/26 trust

这仅适用于 IPv4 地址。对于 IPv6 地址，请添加以下条目：

```
host all all ::0/0 md5
```

如果您要允许来自特定网络上多台客户端计算机的连接，请采用 CIDR 地址格式在此条目中指定网络地址。

pg_hba.conf 文件支持以下客户端鉴定格式。

- local database user authentication-method [authentication-option]
- host database user CIDR-address authentication-method [authentication-option]
- hostssl database user CIDR-address authentication-method [authentication-option]
- hostnossl database user CIDR-address authentication-method [authentication-option]

您可以使用以下格式在单独的字段中指定 IP 地址和网络掩码，而不使用 CIDR 地址格式：

- host database user IP-address IP-mask authentication-method [authentication-option]
- hostssl database user IP-address IP-mask authentication-method [authentication-option]
- hostnossl database user IP-address IP-mask authentication-method [authentication-option]

3 测试远程连接。

3a 重启动远程 PostgreSQL 服务器。

3b 使用用户名和口令远程登录服务器。

18 配置 Identity Reporting

安装 Identity Reporting 后，您仍可以通过运行 configupdate.bat 文件来修改许多安装属性。

如果使用配置工具更改了 Identity Reporting 的任何设置，您必须重启动 Tomcat 才能使更改生效。但是，在 Identity Reporting 的 Web 用户界面中进行更改后，则不需要重启动服务器。

18.1 对 Oracle 数据库运行报告

Identity Reporting 可让您针对远程 Oracle 数据库运行报告。但是，您必须将一个 Oracle JDBC 文件添加到应用程序服务器的库中。

1 从 Oracle 网站下载 ojdbc7.jar 文件。
2 将该文件复制到 Tomcat 服务器的相应位置 （*tomcat_lib* 中的 common/lib 目录）。

有关支持的 Oracle 数据库的详细信息，请参见第 16.5 节 "Identity Reporting 的系统要求 "（第 228 页）。

18.2 部署 Identity Reporting 的 REST API

Identity Reporting 在报告功能中整合了多个用于实现不同功能的 REST API。这些 REST API 使用 OAuth2 协议进行鉴定。

在 Tomcat 上，系统会在安装 Identity Reporting 时自动部署 rptdoc war。

在临时环境或生产环境中运行时，请从 Tomcat 上的环境中手动删除 rptdoc war 文件和文件夹。

18.3 连接远程 Remote PostgreSQL 数据库

如果您的 PostgreSQL 数据库安装在单独的服务器上，则需要在该远程数据库的 postgresql.conf 和 pg_hba.conf 文件中更改默认设置。

1 在 postgresql.conf 文件中更改侦听地址。

   默认情况下，PostgreSQL 允许侦听 localhost 连接，不允许远程 TCP/IP 连接。要允许远程 TCP/IP 连接，请将以下条目添加到 C:\NetIQ\idm\apps\postgres\data\postgresql.conf 文件中：

   ```
   listen_addresses = '*'
   ```

   如果服务器上有多个接口，可以指定要侦听的特定接口。
2 将客户端鉴定条目添加到 pg_hba.conf 文件中。

默认情况下， PostgreSQL 只接受来自 localhost 的连接。它会拒绝远程连接。这通过应用访问控制规则来控制，该规则允许用户在提供有效口令 （md5 关键字）后从某个 IP 地址登录。要接受远程连接，请将以下条目添加到 C:\NetIQ\idm\apps\postgres\data\pg_hba.conf 文件中。

```
host all all 0.0.0.0/0 md5
```

例如， 192.168.104.24/26 trust

这仅适用于 IPv4 地址。对于 IPv6 地址，请添加以下条目：

```
host all all ::0/0 md5
```

如果您要允许来自特定网络上多台客户端计算机的连接，请采用 CIDR 地址格式在此条目中指定网络地址。

pg_hba.conf 文件支持以下客户端鉴定格式。

- local database user authentication-method [authentication-option]
- host database user CIDR-address authentication-method [authentication-option]
- hostssl database user CIDR-address authentication-method [authentication-option]
- hostnossl database user CIDR-address authentication-method [authentication-option]

您可以使用以下格式在单独的字段中指定 IP 地址和网络掩码，而不使用 CIDR 地址格式：

- host database user IP-address IP-mask authentication-method [authentication-option]
- hostssl database user IP-address IP-mask authentication-method [authentication-option]
- hostnossl database user IP-address IP-mask authentication-method [authentication-option]

3 测试远程连接。

3a 重启动远程 PostgreSQL 服务器。

3b 使用用户名和口令远程登录服务器。

19 管理运行报告所需的驱动程序

Identity Reporting 需要以下驱动程序：

- Identity Manager Managed System Gateway Driver
- Identity Manager Driver for Data Collection Service

您可以使用 Designer 随附的包管理工具来安装和配置这些驱动程序。此过程包括以下活动：

19.1 配置 Identity Reporting 的驱动程序

本节将会帮助您安装和配置 Identity Reporting 的受管系统网关驱动程序和数据收集服务驱动程序。

注释：本节假设您已安装并配置 RBPM 的 User Application 驱动程序及角色和资源驱动程序。有关详细信息，请参见第 15.6 章 " 创建和部署 Identity Applications 的驱动程序 "（第 191 页）。

19.1.1 安装 Identity Reporting 的驱动程序包

在尝试配置驱动程序之前，必须先安装 " 包编目 " 中所有必要的驱动程序包。当您在 Designer 中创建新的 Identity Manager 项目时，用户界面会自动提示您将若干个包导入到该新项目。您不需要在安装期间导入这些包，但为了使 Identity Reporting 正常运行，您必须在某个时间点安装这些包。

1. 在 Designer 中打开您的项目。
2. 选择**包编目 > 导入包**。
3. 在 " 选择包 " 对话框中，单击**全选**，然后单击**确定**。

   Designer 在**包编目**下添加若干新的包文件夹。这些包文件夹对应于 Designer 中建模器视图右侧选用板中的对象。
4. 单击**保存**。

19.1.2 配置受管系统网关驱动程序

1 在 Designer 中打开您的项目。

2 在建模器视图上的调色板中，选择服务 > 受管系统网关。

3 将受管系统网关的图标拖到建模器视图上。

4 在驱动程序配置向导中，选择受管系统网关基础，然后单击下一步。

5 在 " 选择强制功能 " 窗口中选择强制功能，然后单击下一步。

6 （视情况而定）如果应用程序提示您选择一个名为高级 Java 类的附加包，请选择该包，然后单击确定。

7 （可选）指定要为驱动程序使用的名称。

8 单击下一步。

9 对于 " 连接参数 "，请指定 Identity Reporting 用于从驱动程序请求数据的值。

如果指定了多个 IP 地址，您仍然是使用同一个端口号来侦听所有接口。例如，如果您指定了 192.168.0.1,127.0.0.1 地址和 9000 端口，驱动程序将使用以下设置：

```
192.168.0.1:9000
127.0.0.1:9000
```

10 （可选）要启用端点跟踪，请选择 true，然后指定跟踪文件的位置。

11 单击下一步。

12 （可选）要将驱动程序连接到 Remote Loader，请完成以下步骤：

12a 在 "Remote Loader" 窗口中，选择是。

12b 指定您要使用的 Remote Loader 的设置。

13 单击下一步。

14 查看 " 确认安装任务 " 窗口中的信息，然后单击完成。

15 （可选）要配置驱动程序的其他设置，请在 " 建模器 " 视图中完成以下步骤：

15a 右键单击用于将受管系统网关驱动程序连接到驱动程序集的行，然后单击属性。

15b 在 " 属性 " 对话框中，选择驱动程序配置 > 启动选项。

15c 选择手动作为启动选项，然后单击应用。

15d 选择驱动程序参数选项卡。

15e （可选）在驱动程序选项选项卡中，修改驱动程序、连接和端点跟踪的设置。

您可能需要在连接参数和驱动程序参数下选择显示才能显示这些设置。

15f （可选）要使驱动程序定期在发布者通道上发送状态讯息，请单击发布者选项选项卡，然后为发布者检测信号间隔指定一个值 （以分钟为单位）。

如果在指定的间隔内，发布者通道上未发生通讯，则驱动程序会发送新的检测信号。

15g 单击应用。

16 （可选）要指定服务器的全局配置值，请完成以下步骤：

16a 在导航窗格中，选择 GCV。

16b 指定全局配置值，例如：

查询各驱动程序集的受管系统

定义受管系统网关驱动程序的操作范围。如果设置为 true，驱动程序将返回各驱动程序集的受管系统的信息。否则，范围限制为本地驱动程序集。

将端点请求数据添加到查询中

指定是否将端点请求数据添加到驱动程序发送的查询中。这些数据将添加为操作数据节点。

端点请求数据节点名称

指定要添加到查询操作数据的节点名称。节点属性将包含有关请求的细节。

16c 单击应用。

17 （可选）要查看已安装的包，请在导航窗格中单击包。

除非您要卸装特定的包，否则不需要更改操作设置。

18 单击确定。

19 启用订购者通道，以使 Identity Reporting 能够正常运行。

19.1.3 配置数据收集服务的驱动程序

1 在 Designer 中打开您的项目。

2 在建模器视图上的调色板中，选择服务 > 数据收集服务。

3 将数据收集服务的图标拖到建模器视图上。

4 在驱动程序配置向导中，选择数据收集服务基础，然后单击下一步。

5 在 " 选择强制功能 " 窗口中选择强制功能，然后单击下一步。

6 选择要应用的可选功能，然后单击下一步。

7 （视情况而定）如果应用程序提示您选择一个名为 LDAP 库的附加包，请完成以下步骤：

7a 选择该包，然后单击确定。

7b （可选）要在 " 安装 LDAP 库 " 页面上配置所有驱动程序的全局连接配置文件，请选择是。

8 单击下一步。

9 （可选）指定要为驱动程序使用的名称。

10 单击下一步。

11 对于 " 连接参数 "，请指定 Identity Reporting 用于从驱动程序请求数据的值。

例如，指定用于鉴定的报告管理员用户和口令。

如果指定了多个 IP 地址，您仍然是使用同一个端口号来侦听所有接口。例如，如果您指定了 192.168.0.1,127.0.0.1 地址和 9000 端口，驱动程序将使用以下设置：

```
192.168.0.1:9000
127.0.0.1:9000
```

12 单击下一步。

13 对于身份库注册，请指定身份库的设置。

必须指定一个 IP 地址。请不要指定用于身份库注册的 localhost 地址。

14 （可选）要注册受管系统网关驱动程序，请完成以下步骤：

14a 对于受管系统网关注册，请单击是。

14b 指定驱动程序的 DN，以及 LDAP 管理员的用户和口令。

注释：由于您刚才配置的受管系统网关驱动程序尚未部署，浏览功能将不显示该驱动程序，因此，您可能需要键入该驱动程序的 DN。

---

15 单击下一步。

16 （可选）要将驱动程序连接到 Remote Loader，请完成以下步骤：

16a 在 “Remote Loader” 窗口中，选择是。

16b 指定您要使用的 Remote Loader 的设置。

17 单击下一步。

18 对于范围配置，请指定数据收集服务驱动程序的角色。

19 查看 “ 确认安装任务 ” 窗口中的信息，然后单击完成。

20 （可选）要配置驱动程序的其他设置，请在 “ 建模器 ” 视图中完成以下步骤：

20a 右键单击用于将数据收集服务驱动程序连接到驱动程序集的行，然后单击属性。

20b 在 “ 属性 ” 对话框中，选择驱动程序配置 > 启动选项。

20c 选择手动作为启动选项，然后单击应用。

20d 选择驱动程序参数选项卡。

在驱动程序会接收到大量事件的环境中， NetIQ 建议将每个文件的批次数设置为不超过 5 的数值。如果将此参数设置为大于 5 的值，驱动程序将无法有效率地处理事件。

20e （可选）在驱动程序选项选项卡中，修改驱动程序、连接和注册的设置。

在测试环境中，您可能需要使用较小的数字，以确保事件得到正确处理。但是，在生产环境中，您可能要使用较大的数字，以免系统不必要地处理事件。

IP 地址

指定托管 Identity Reporting 的服务器的 IP 地址。

端口

指定 Identity Reporting 用来建立 REST 连接的端口号。

协议

指定用于访问 Identity Reporting 的协议。如果选择 HTTPS，则还必须指定是否要信任服务器的证书。

名称

指定用于在 Identity Reporting 中参照您的身份库的名称。

描述

指定身份库的简短说明。

地址

指定身份库的 IP 地址。

例如 192.168.0.1

注释：必须指定一个 IP 地址。请不要指定用于身份库注册的 “localhost” 地址。

注册受管系统网关

指定是否要注册受管系统网关驱动程序。

受管系统网关驱动程序 DN (LDAP)

以斜杠格式指定受管系统网关驱动程序的 DN。

受管系统网关驱动程序配置模式

指定是要在本地还是远程配置驱动程序。

用户 DN (LDAP)

指定驱动程序鉴定到受管系统网关驱动程序时应使用的用户的 LDAP DN。身份库中必须存在此 DN。

口令

指定该用户的口令。

提交事件的时间间隔

在将某个事件提交到 DCS （以及 Identity Reporting 的数据库）之前，该事件可在持久性层中保留的最长时间，以分钟为单位。

20f （视情况而定）要从 Identity Applications 收集数据，请指定 **SSO 服务支持**的值。有关详细信息，请参见第 19.1.4 节 " 配置 Identity Reporting 以从 Identity Applications 收集数据 " （第 245 页）。

20g 单击 " **应用** "。

21 要配置 DN，请完成以下步骤：

21a 在导航菜单中，选择**引擎控制值**。

21b 对于 **DN 语法特性值的限定格式**设置，请选择 **True**。

21c 单击**应用**。

22 （可选）要指定服务器的全局配置值，请完成以下步骤：

22a 在导航窗格中，选择 **GCV**。

22b 对于**显示覆盖选项**，请选择**显示**。

22c 修改用于覆盖全局配置值的设置。

22d 单击**应用**。

23 单击**确定**。

19.1.4 配置 Identity Reporting 以从 Identity Applications 收集数据

要让 Identity Reporting 从 Identity Applications 收集数据，必须将 DCS 驱动程序配置为支持单点登录过程。

1 在 Designer 中打开您的项目。

2 在**大纲**视图中，右键单击数据收集服务驱动程序，然后单击**属性**。

3 单击**驱动程序配置 > 驱动程序参数**。

4 单击**显示连接参数 > 显示**。

5 单击 **SSO 服务支持 > 是**。

6 指定单点登录功能的参数：

SSO 服务地址

必需

指定向 OSP 颁发令牌的鉴定服务器的相对 URL。例如， 10.10.10.48。

此值必须与您在 RBPM 配置实用程序中为 **OSP 服务器主机标识符**指定的值匹配。有关详细信息，请参见鉴定服务器 （第 215 页）。

SSO 服务端口

必需

指定鉴定服务器的端口。默认值是 8180。

此值必须与您在 RBPM 配置实用程序中为 **OSP 服务器 TCP 端口**指定的值匹配。有关详细信息，请参见鉴定服务器 （第 215 页）。

SSO 服务客户端 ID

必需

指定用于供鉴定服务器识别 DCS 驱动程序单点登录客户端的名称。默认值为 dcsdrv。

此值必须与您在 RBPM 配置实用程序中为 **OSP 客户端 ID** 指定的值匹配。有关详细信息，请参见报告 （第 220 页）。

SSO 服务客户端密码

必需

指定 DCS 驱动程序单点登录客户端的口令。

此值必须与您在 RBPM 配置实用程序中为 **OSP 客户端密码**指定的值匹配。有关详细信息，请参见报告 （第 220 页）。

协议

指定服务客户端在与鉴定服务器通讯时，应使用 http （非安全）协议还是 https （安全）协议。

7 单击**应用**，然后单击**确定**。

8 （视情况而定）如果您在部署驱动程序后更改了这些设置，则必须部署并重启动驱动程序。有关详细信息，请参见第 19.2 节 " 部署并启动 Identity Reporting 的驱动程序 " （第 246 页）。

9 对环境中的每个 DCS 驱动程序重复此过程。

19.2 部署并启动 Identity Reporting 的驱动程序

Identity Reporting 需要以下驱动程序：

- Identity Manager Managed System Gateway Driver
- Identity Manager Driver for Data Collection Service

此过程包括以下活动：

有关安装和配置这些驱动程序的详细信息，请参见第 19.1 节 " 配置 Identity Reporting 的驱动程序 " （第 241 页）。

19.2.1 部署驱动程序

您必须为 Identity Reporting 部署两个驱动程序。

1 在 Designer 中打开您的项目。

2 在**建模器**或**大纲**视图中，右键单击您要部署的驱动程序集。

3 选择在线 > 部署。

4 指定所选驱动程序的身份库身份凭证。

19.2.2 校验受管系统是否正在工作

在启动受管系统网关驱动程序和数据收集服务驱动程序之前，您应该确认是否已正确配置了底层受管系统。此过程将会帮助您排除环境中与报告驱动程序配置无关的问题。

例如，要对 Active Directory 环境中的问题进行查错，您可能需要通过在 User Application 中指派资源来测试某个 Active Directory 权利。

注释：有关 Active Directory 驱动程序的详细信息，请参见《*NetIQ Identity Manager Driver for Active Directory Implementation Guide*》（NetIQ Identity Manager Driver for Active Directory 实施指南）。

以下步骤演示了一种用于确认 Active Directory 是否已正确配置的方法：

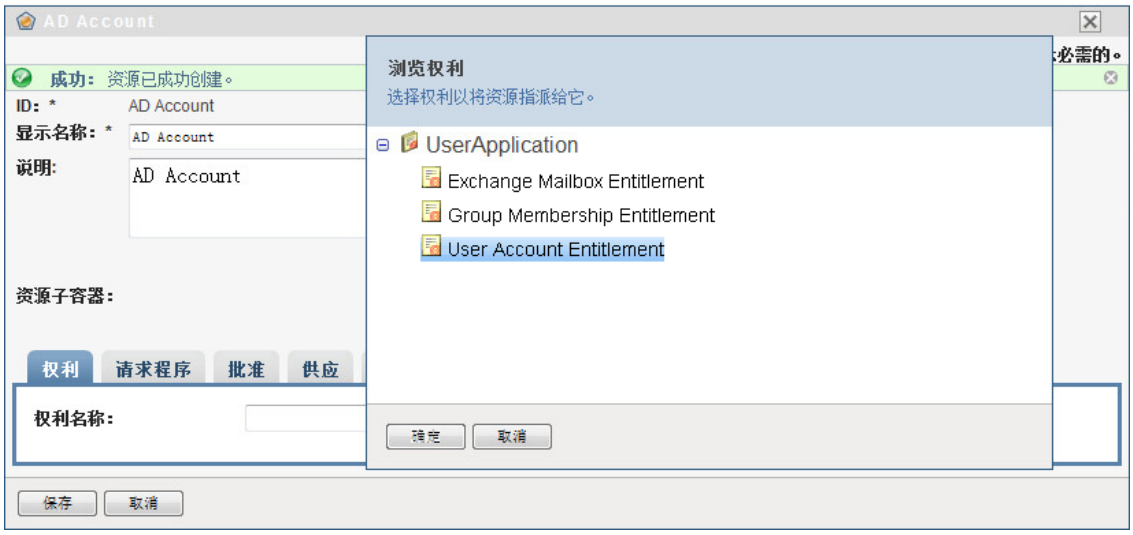
1 确保 User Application 和 Identity Reporting 在同一台服务器上运行。

2 在 iManager 中，校验 User Application 驱动程序和 Role and Resource Service 驱动程序是否正在运行，然后确保受管系统的驱动程序正在运行。

3 要校验 User Application 是否能够从 Active Directory 检索信息，请以 User Application 管理员身份登录 User Application。

4 在 " 资源编目 " 中，为 Active Directory 帐户创建一个新资源：

5 将该资源与 Active Directory 驱动程序中的某个权利绑定，例如用户帐户权利。



User Application 可以从驱动程序检索该权利。

6 由于这个特定的资源隶属于帐户，因此，请对该资源进行配置，以指派一个帐户值。

7 选择该帐户值，然后单击添加。

8 创建另一个要指派组的资源。

9 将该资源与适用于组的权利绑定。将这个特定的资源映射到组成员资格权利。

10 配置此资源，让用户能够在请求时指派权利值，并允许用户为单个指派请求选择多个值。

11 校验是否已成功创建权利。

此时，您可以看到，受管系统 （在本例中为 Active Directory）的底层体系结构在正常运行。这可以帮助您对以后可能出现的任何问题进行查错。

19.2.3 启动 Identity Reporting 的驱动程序

本节提供有关启动受管系统网关驱动程序和数据收集服务驱动程序的指导。

1 打开 iManager。

2 右键单击受管系统网关驱动程序，然后单击启动驱动程序。

3 右键单击数据收集服务驱动程序，然后单击启动驱动程序。

4 启动驱动程序后，检查控制台是否显示了服务器控制台中的附加信息。例如：

```
21:22:56,399 INFO  [LogEvent] [DCS_Driver_Registration_Add] DCS Driver DN
TREE\novell\TestDrivers\Data Collection Service Driver; DCS-Report Driver
d44571a5708446bad65832481bb401d
```

5 以报告管理员身份登录 Identity Reporting。

6 在左侧的导航窗格中，单击概述。

7 检查配置部分是否指出身份库已配置。

8 在导航窗格中，单击身份库。

9 检查 “ 身份库 ” 页面是否提供了有关数据收集驱动程序和受管系统网关驱动程序的细节。受管系统网关驱动程序状态应指出该驱动程序已初始化。

此时，您可以查看身份信息仓库的内容，以详细了解所储存的有关身份库的丰富数据，以及企业中的受管系统。

10 要查看身份信息仓库中的数据，请使用 PGAdmin for PostgreSQL 等数据库管理工具来查看 SIEM 数据库的内容。当您查看 SIEM 数据库时，应该会看到以下纲要：

idm_rpt_cfg

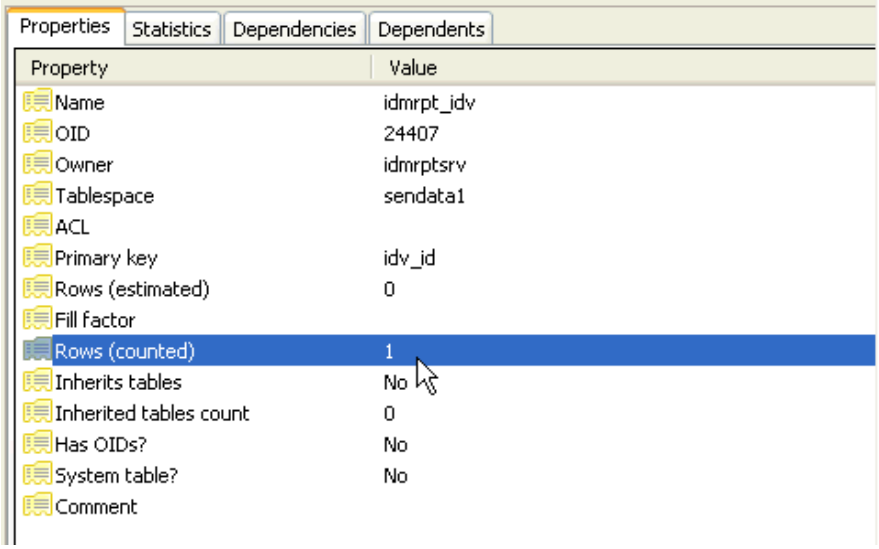
包含报告配置数据，例如报告定义和日程表。 Identity Reporting 的安装程序会将此纲要添加到数据库。

idm_rpt_data

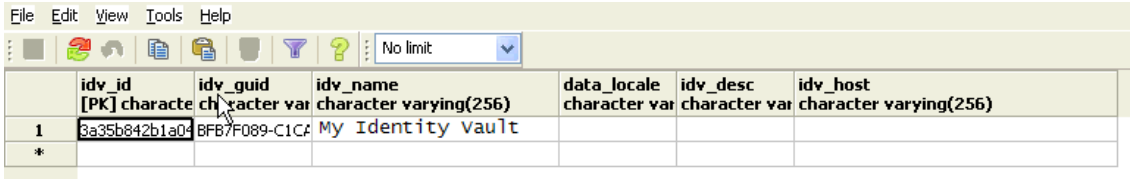
包含受管系统网关驱动程序和数据收集服务驱动程序收集的信息。 Identity Reporting 的安装程序会将此纲要添加到数据库。

11 要查看驱动程序收集的数据，请展开 **idm_rpt_data > 表 > idmrpt_idv**。

12 校验新数据收集服务驱动程序的此表中是否已添加了一行：



13 校验此表的数据是否显示了身份库名称：



如果您在此表中看到了这个新行，则表示驱动程序注册过程成功。

19.3 配置运行时环境

本节提供为确保运行时环境正常运行而应执行的一些额外配置步骤。此外，本节还提供了查错方法，以及具有特定用途的数据库表的一些信息。

此过程包括以下活动：

- 第 19.3.1 节 " 将数据收集服务驱动程序配置为从 Identity Applications 收集数据 "（第 251 页）
- 第 19.3.2 节 " 迁移数据收集服务驱动程序 "（第 252 页）
- 第 19.3.3 节 " 添加对自定义属性和对象的支持 "（第 254 页）
- 第 19.3.4 节 " 添加多个驱动程序集支持 "（第 256 页）
- 第 19.3.5 节 " 将驱动程序配置为使用 SSL 在远程模式下运行 "（第 257 页）

如果一个或多个驱动程序出现了难以理解的问题，请参见《Administrator Guide to NetIQ Identity Reporting》（NetIQ Identity Reporting 管理员指南）中的 "Troubleshooting"（查错）。

19.3.1 将数据收集服务驱动程序配置为从 Identity Applications 收集数据

要使 Identity Applications 与 Identity Reporting 正常配合运行，必须将 DCS 驱动程序配置为支持 OAuth 协议。

注释：

- 仅当在环境中使用了 Identity Reporting 时，才需要安装并配置 DCS 驱动程序。
- 如果在环境中配置了多个 DCS 驱动程序，则必须针对每个驱动程序完成以下步骤。

---

1. 登录 Designer。
2. 在 Designer 中打开您的项目。
3. （视情况而定）如果您的项目尚不包含数据收集服务驱动程序，请将该驱动程序导入您的项目。有关详细信息，请参见第 15.6 章 " 创建和部署 Identity Applications 的驱动程序 "（第 191 页）。
4. （视情况而定）如果您尚未将 DCS 驱动程序升级到支持的增补程序版本，请完成以下步骤：
   - **4a** 下载最新的 DCS 驱动程序增补程序文件。
   - **4b** 将该增补程序文件提取到服务器上的某个位置。
   - **4c** 在终端中，浏览到适用于您环境的增补程序 RPM 的提取位置，然后运行以下命令：

     ```
     rpm -Uvh novell-DXMLdcs.rpm
     change this
     ```

   - **4d** 重启动 eDirectory。
   - **4e** 在 Designer 中，确保已安装支持版本的数据收集服务基础包。如果需要，请安装最新版本，然后再继续。有关软件要求的详细信息，请参见第 16.3 节 " 安装 Identity Reporting 组件的先决条件 "（第 226 页）。
   - **4f** 在 Designer 中重部署并重启动 DCS 驱动程序。
5. 在**大纲**视图中，右键单击 DCS 驱动程序，然后选择**属性**。
6. 单击 " 驱动程序配置 "。

7 单击**驱动程序参数**选项卡。

8 单击**显示连接参数**，然后选择**显示**。

9 单击 **SSO 服务支持**，然后选择**是**。

10 指定 Reporting Module 的 IP 地址和端口。

11 指定 SSO 服务客户端的口令。默认口令为 driver。

12 单击**应用**，然后单击**确定**。

13 在**建模器**视图中，右键单击 DCS 驱动程序，然后选择**驱动程序 > 部署**。

14 单击**部署**。

15 出现是否重启动 DCS 驱动程序的提示时，单击**是**。

16 单击**确定**。

19.3.2 迁移数据收集服务驱动程序

要将对象同步到身份信息仓库中，您必须迁移数据收集服务驱动程序。

1 登录 iManager。

2 在数据收集服务驱动程序的**概述**面板中，选择**从身份库迁移**。

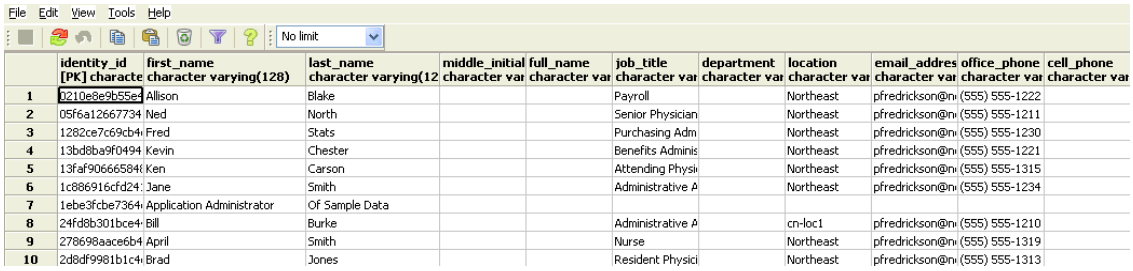
3 选择包含相关数据的组织，然后单击**启动**。

注释：迁移过程可能需要几分钟时间，具体取决于您的数据量。请务必等到迁移过程完成后再继续下一步。

---

4 等待迁移过程完成。

5 确保 **idmrpt_identity** 和 **idmrpt_acct** 表 （提供身份库中身份和帐户的相关信息）中包含以下类型的信息：



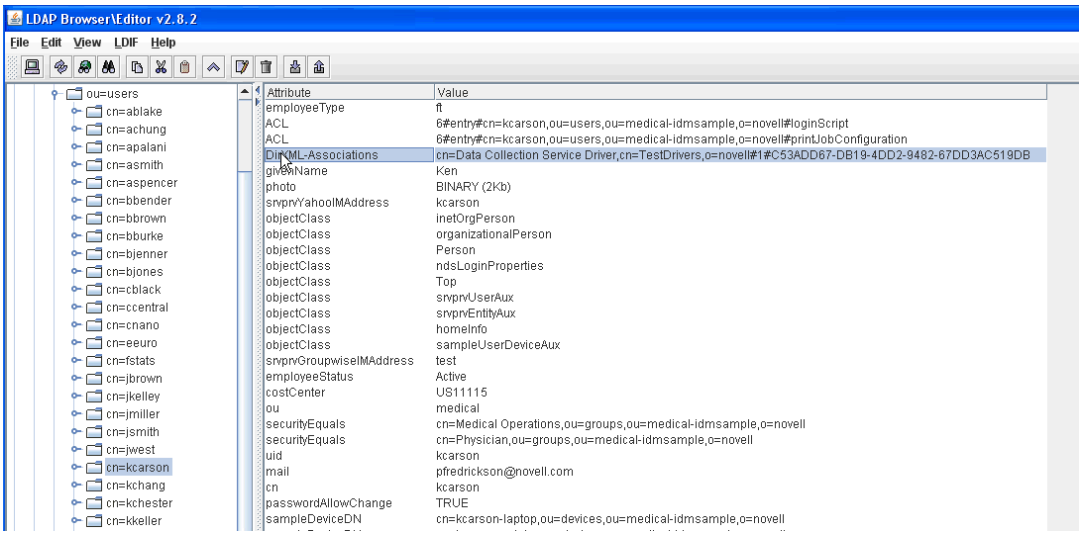
File Edit View Tools Help

No limit

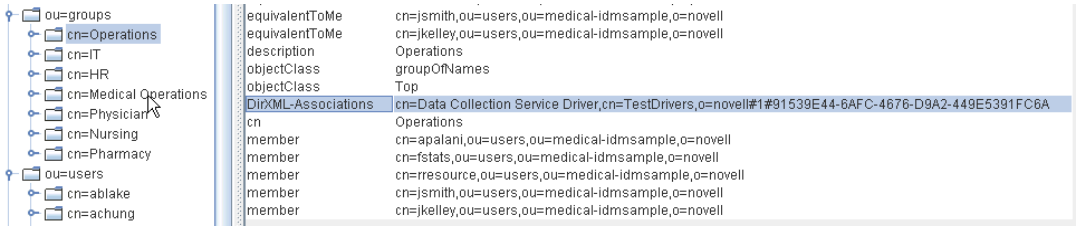
	identity_id [PK] characte	first_name character varying(128)	last_name character varying(12	middle_initial character var	full_name character var	job_title character var	department character var	location character var	email_addres character var	office_phone character var	cell_phone character var
1	0210e8e9b55e4	Allison	Blake			Payroll		Northeast	pfredrickson@n	(555) 555-1222	
2	05f6a12667734	Ned	North			Senior Physician		Northeast	pfredrickson@n	(555) 555-1211	
3	1282ce7c69cb4	Fred	Stats			Purchasing Adm		Northeast	pfredrickson@n	(555) 555-1230	
4	13bd8ba9f0494	Kevin	Chester			Benefits Adminis		Northeast	pfredrickson@n	(555) 555-1221	
5	13faf90666584	Ken	Carson			Attending Physi		Northeast	pfredrickson@n	(555) 555-1315	
6	1c886916cfd24	Jane	Smith			Administrative A		Northeast	pfredrickson@n	(555) 555-1234	
7	1ebe3fcbe7364	Application Administrator	Of Sample Data								
8	24fd8b301bce4	Bill	Burke			Administrative A		cn-loc1	pfredrickson@n	(555) 555-1210	
9	278698aace6b4	April	Smith			Nurse		Northeast	pfredrickson@n	(555) 555-1319	
10	2d8df9981b1c4	Brad	Jones			Resident Physici		Northeast	pfredrickson@n	(555) 555-1313	

6 在 LDAP 浏览器中，校验迁移过程是否添加了对 DirXML-Associations 的以下参照：

- 对于每个用户，校验是否包含以下类型的信息：



- 对于每个组，校验是否包含以下类型的信息：



7 确保 **idmrpt_group** 表中的数据看上去类似于以下信息：

group_name character var	group_desc character var	dynamic_gro boolean	dynamic_rule character var	nested_grou boolean	idmrpt_valid_from timestamp without tin	idmrpt_deleted boolean	idmrpt_syn_state smallint
Pharmacy	Pharmacy	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
IT	Information Tec	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
HR	Human Resourc	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
Physician	Physician	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
Operations	Operations	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
Medical Operati	Medical Operati	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
Nursing	Nursing	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1

此表将显示每个组的名称，以及用于指出组是动态组还是嵌套组的标志。此外，它还会显示组是否已迁移。如果某个对象在 User Application 中已被修改但尚未迁移，则同步状态 (idmrpt_syn_state) 可能会设置为 0。例如，如果在组中添加了用户，并且尚未迁移驱动程序，那么，此值可能会设置为 0。

8 （可选）校验下列表中的数据：

- idmrpt_approver
- idmrpt_association
- idmrpt_category
- idmrpt_container
- idmrpt_idv_drivers
- idmrpt_idv_prd
- idmrpt_role

- idmrpt_resource
- idmrpt_sod

9 （可选）校验 **idmrpt_ms_collect_state** 表现在是否包含行。该表显示有关受管系统网关驱动程序的数据收集状态信息。

此表包含有关为受管系统执行了哪些 REST 端点的数据。此时，该表不包含任何行，因为您尚未启动此驱动程序的收集过程。

19.3.3 添加对自定义属性和对象的支持

您可以对数据收集服务驱动程序进行配置，使其收集和保留不属于默认数据收集模式的自定义属性与对象的数据。为此，您需要修改数据收集服务驱动程序过滤器。修改过滤器不会立即触发对象同步，而是会在身份库中发生添加、修改或删除事件时，向数据收集服务发送新添加的属性和对象。

在添加对自定义属性和对象的支持时，您需要修改报告，以包括扩展的属性和对象信息。以下视图提供有关扩展对象和属性的当前数据与历史数据：

- idm_rpt_cfg.idmrpt_ext_idv_item_v
- idm_rpt_cfg.idmrpt_ext_item_attr_v

此过程包括以下活动：

- 将驱动程序配置为使用扩展对象 （第 254 页）
- 包含数据库中的名称和说明 （第 255 页）
- 向已知的对象类型添加扩展属性 （第 255 页）

将驱动程序配置为使用扩展对象

您可将任何对象或属性添加到数据收集服务过滤器策略中。在添加新对象或属性时，请务必按以下示例所示映射 GUID （subscriber 为 sync）和对象类 （subscriber 为 notify）：

```
<filter-class class-name="Device" publisher="ignore" publisher-create-
homedir="true" publisher-track-template-member="false" subscriber="sync">
<filter-attr attr-name="CN" merge-authority="default" publisher="ignore"
publisher-optimize-modify="true" subscriber="sync"/>
<filter-attr attr-name="Description" merge-authority="default" publisher="ignore"
publisher-optimize-modify="true" subscriber="sync"/>
<filter-attr attr-name="GUID" merge-authority="default" publisher="ignore"
publisher-optimize-modify="true" subscriber="sync"/>
<filter-attr attr-name="Object Class" merge-authority="default" publisher="ignore"
publisher-optimize-modify="true" subscriber="notify"/>
<filter-attr attr-name="Owner" merge-authority="default" publisher="ignore"
publisher-optimize-modify="true" subscriber="sync"/>
<filter-attr attr-name="Serial Number" merge-authority="default"
publisher="ignore" publisher-optimize-modify="true" subscriber="sync"/>
<filter-attr attr-name="sampleDeviceModel" from-all-classes="true" merge-
authority="default" publisher="ignore" publisher-optimize-modify="true"
subscriber="sync"/>
<filter-attr attr-name="sampleDeviceType" from-all-classes="true" merge-
authority="default" publisher="ignore" publisher-optimize-modify="true"
subscriber="sync"/>
</filter-class>
```

包含数据库中的名称和说明

如果您希望对象包含数据库中的名称和说明，则需要为 _dcsName 和 _dcsDescription 添加一个纲要映射策略。该纲要映射策略会将对象实例的相关属性值分别映射到 idmrpt_ext_idv_item.item_name 和 idmrpt_ext_idv_item.item_desc 列。如果您未添加纲要映射策略，属性将填充到子表 idmrpt_ext_item_attr 中。

例如：

```
<attr-name class-name="Device">
<nds-name>CN</nds-name>
<app-name>_dcsName</app-name>
</attr-name>
<attr-name class-name="Device">
<nds-name>Description</nds-name>
<app-name>_dcsDescription</app-name>
</attr-name>
```

下面是一个可显示数据库中这些对象和属性值的 SQL 示例：

```
SELECT
    item.item_dn,
    item.item_name,
    item.item_desc,
    attr.attribute_name,
    itemAttr.attribute_value,
    item.idmrpt_deleted as item_deleted,
    itemAttr.idmrpt_deleted as attr_deleted,
    item.item_desc,
    obj.object_class
FROM
    idm_rpt_data.idmrpt_ext_idv_item as item, idm_rpt_data.idmrpt_ext_item_attr
itemAttr, idm_rpt_data.idmrpt_ext_attr as attr, idm_rpt_data.idmrpt_ext_obj as obj
WHERE
    item.object_id = obj.object_id and itemAttr.attribute_id = attr.attribute_id
and itemAttr.cat_item_id = item.item_id
ORDER BY
    item.item_dn, item.item_name
```

向已知的对象类型添加扩展属性

如果某个属性已添加到数据收集服务驱动程序的过滤器策略中，但未显式映射到 XML 参照文件 (IdmrptIdentity.xml) 中的报告数据库，则系统会在 idmrpt_ext_item_attr 表中填充并维护值，并在 idmrpt_ext_attr 表中添加一个属性参照。

下面的 SQL 示例显示了这些扩展属性：

```
SELECT
    acct.idv_acct_dn,
    attrDef.attribute_name,
    attribute_value,
    attrVal.idmrpt_valid_from,
    cat_item_attr_id,
    attrVal.idmrpt_deleted,
    attrVal.idmrpt_syn_state
FROM
    idm_rpt_data.idmrpt_ext_item_attr as attrVal, idm_rpt_data.idmrpt_ext_attr as
attrDef, idm_rpt_data.idmrpt_identity as idd, idm_rpt_data.idmrpt_idv_acct as acct
WHERE attrVal.attribute_id = attrDef.attribute_id and idd.identity_id =
acct.identity_id and attrVal.cat_item_id = acct.identity_id and cat_item_type_id =
'IDENTITY'
```

除了用户对象以外，您还可在以下对象的过滤器策略中添加扩展属性，并在数据库中填充这些属性：

- nrfRole
- nrfResource
- 容器

注释：安装的产品将提供对 organizationUnit、 Organization 和 Domain 的支持。容器类型在 idmrpt_container_types 表中维护。

- 组
- nrfSod

您可以查看 idmrpt_cat_item_types.idmrpt_table_name 列，来了解扩展属性与父表或父对象之间的关联。此列描述如何将 idm_rpt_data.idmrpt_ext_item_attr.cat_item_id 列连接到父表的主键。

19.3.4 添加多个驱动程序集支持

新的数据收集服务范围包 (NOVLDCSSCPNG) 为包含多个驱动程序集和多组数据收集服务驱动程序及受管系统网关驱动程序的企业环境提供静态和动态范围功能。

在安装期间或安装之后，您需要确定要在其上安装该包的数据收集服务驱动程序的角色。您需要选择以下角色之一：

- **Primary** 驱动程序将会同步所有信息，但其他驱动程序集的子树除外。一级数据收集服务驱动程序能够正常为整个身份库提供服务，或者可与一个或多个二级驱动程序配合工作。
- **次要的** 驱动程序只同步自身的驱动程序集，而不同步其他任何信息。通常，二级数据收集服务驱动程序要求一级驱动程序在不同的驱动程序集中运行，否则，任何本地驱动程序集外部的数据都不会发送到数据收集服务。

  如果您还将数据收集服务驱动程序用作此二级服务器上的主驱动程序，则该驱动程序无法发现需要报告的对象更改。要在此服务器上配置数据收集服务驱动程序，请参见第 19.1.3 节 “ 配置数据收集服务的驱动程序 ”（第 243 页）。
- **自定义** 允许管理员自定义范围规则。唯一的隐式范围是本地驱动程序集，其他任何驱动程序如果未显式添加到自定义范围列表，都会被视为不在范围内。自定义范围是身份库中应该同步其从属或子树的容器的判别名 （采用斜杠格式）。

只有如下所述的某些配置情况才需要范围包：

- **单个服务器与具有单个驱动程序集的身份库** 对于此情况，您不需要定义范围，因此也就无需安装范围包。

- **多个服务器与具有单个驱动程序集的身份库** 对于此情况，您需要遵循以下指导原则：
  - 确保 Identity Manager 服务器存有要从中收集数据的所有分区的复本。
  - 对于此情况，您不需要定义范围，因此，请不要安装范围包
- **多个服务器与具有多个驱动程序集的身份库** 此情况有两种基本配置：
  - 所有服务器都存有要从中收集数据的所有分区的复本。

    对于此配置，您需要遵循以下指导原则：
    - 需要定义范围，以免有多个 DCS 驱动程序处理同一项更改。
    - 您需要在所有 DCS 驱动程序上安装范围包。
    - 您需要将一个 DCS 驱动程序选作一级驱动程序。
    - 您需要将其他所有 DCS 驱动程序配置为二级驱动程序。
  - 所有服务器都*未*存有要从中收集数据的所有分区的复本。

    此配置存在两种可能的情况：
    - 应从中收集数据的所有分区*仅由一个* Identity Manager 服务器存放

      在此情况下，您需要遵循以下指导原则：
      - 需要定义范围，以免有多个 DCS 驱动程序处理同一项更改。
      - 您需要在所有 DCS 驱动程序上安装范围包。
      - 您需要将所有 DCS 驱动程序都配置为一级驱动程序。
    - 应从中收集数据的所有分区*不是仅由一个* Identity Manager 服务器存放 （某些分区由多个 Identity Manager 服务器存放）。

      在此情况下，您需要遵循以下指导原则：
      - 需要定义范围，以免有多个 DCS 驱动程序处理同一项更改。
      - 您需要在所有 DCS 驱动程序上安装范围包。
      - 您需要将所有 DCS 驱动程序都配置为自定义驱动程序。

        您需要为每个驱动程序定义自定义范围规则，并务必不要创建任何重叠的范围。

19.3.5 将驱动程序配置为使用 SSL 在远程模式下运行

在以远程模式运行时，您可以将数据收集服务驱动程序和受管系统网关驱动程序配置为使用 SSL。本节提供有关将驱动程序配置为使用 SSL 在远程模式下运行的步骤。

要使用密钥存储区为受管系统网关驱动程序配置 SSL，请执行以下操作：

1. 在 iManager 中创建服务器证书。
   - **1a** 在**角色和任务**视图中，单击 **NetIQ 证书服务器 > 创建服务器证书**。
   - **1b** 浏览到安装了受管系统网关驱动程序的服务器对象，并将其选中。
   - **1c** 指定证书昵称。
   - **1d** 选择 “ 标准 ” **创建方法，然后单击 “ 下一步 ”**。
   - **1e** 单击 “ 完成 ”，**然后单击 “ 关闭 ”**。
2. 使用 iManager 导出服务器证书。
   - **2a** 在**角色和任务**视图中，单击 **NetIQ 证书访问 > 服务器证书**。
   - **2b** 选择步骤 1 （第 257 页）中创建的证书，然后单击**导出**。

2c 在证书菜单中，选择该证书的名称。

2d 确保导出私用密钥已选中。

2e 输入口令，然后单击下一步。

2f 单击保存导出的证书，并保存导出的 pfx 证书。

3 将步骤 2 （第 257 页）中导出的 pfx 证书导入 Java 密钥存储区。

3a 使用 Java 随附的 keytool。您必须使用 JDK 6 或更高版本。

3b 在命令提示符处输入以下命令：

```
keytool -importkeystore -srckeystore pfx certificate -srcstoretype
PKCS12 -destkeystore Keystore Name
```

例如：

```
keytool -importkeystore -srckeystore cert.pfx -srcstoretype PKCS12
-destkeystore msgw.jks
```

3c 在系统提示时输入口令。

4 使用 iManager 将受管系统网关驱动程序配置修改为使用密钥存储区。

4a 在 Identity Manager 概述中，单击包含受管系统网关驱动程序的驱动程序集。

4b 单击驱动程序状态图标，然后选择编辑属性 > 驱动程序配置。

4c 将显示连接参数设置为 true，并将驱动程序配置模式设置为 “ 远程 ”。

4d 输入密钥存储区文件的完整路径和口令。

4e 保存并重启动驱动程序。

5 使用 iManager 将数据收集服务驱动程序配置修改为使用密钥存储区。

5a 在 Identity Manager 概述中，单击包含受管系统网关驱动程序的驱动程序集。

5b 单击驱动程序状态图标，然后选择编辑属性 > 驱动程序配置。

5c 在受管系统网关注册标题下，将受管系统网关驱动程序配置模式设置为 “ 远程 ”。

5d 输入密钥存储区的完整路径、口令以及在步骤 1c （第 257 页）中指定的别名。

5e 保存并重启动驱动程序。

19.4 设置驱动程序的审计标志

本节概述了受管系统网关驱动程序和数据收集服务驱动程序的建议审计设置。

19.4.1 在 Identity Manager 中设置审计标志

NetIQ 建议您在 Identity Manager 中设置驱动程序的审计标志。这些标志适用于 Novell 审计 （不适用于 XDAS）。

要在 iManager 中设置标志，请转到驱动程序集属性 > 日志级别 > 记录特定事件。

类别	建议的标志
元目录引擎事件	◆ 元目录引擎警告
状态事件	◆ 成功 **注释：** 按用户关联的资源指派事件报告需要 " 成功 " 标志。如果您希望能够运行此报告或它的自定义版本，则需要启用 " 成功 " 标志。 ◆ 错误 ◆ 致命错误
操作事件	◆ 修改 ◆ 添加关联 ◆ 检查口令 ◆ 添加值 ◆ 添加 ◆ 重命名 ◆ 去除关联 ◆ 检查对象口令 ◆ 清除特性 ◆ 去除值 ◆ 获取命名口令 ◆ 去除 ◆ 移动 ◆ 更改口令 ◆ 添加值 （修改时） ◆ 重设置特性
转换事件	◆ 口令重设置 ◆ 用户代理请求 ◆ 口令同步
身份凭证供应事件	◆ 设置 SSO 身份凭证 ◆ 清除 SSO 身份凭证 ◆ 设置 SSO 通行口令

19.4.2 在 eDirectory 中设置审计标志

NetIQ 建议您在 eDirectory 中设置驱动程序的审计标志。这些标志适用于 Novell 审计 （不适用于 XDAS）。

要在 iManager 中设置标志，请转到 **eDirectory 审计 > 审计配置 > Novell 审计**。

类别	建议的标志
全局	◆ 不发送复制的事件
元数据	◆ *（选择所有标志）*
对象	◆ 添加属性 ◆ 允许登录 ◆ 更改口令 ◆ 更改安全性等于 ◆ 创建 ◆ 删除 ◆ 删除属性 ◆ 登录 ◆ 注销 ◆ 修改 RDN ◆ 移动 （源） ◆ 移动 （目标） ◆ 去除 ◆ 重命名 ◆ 恢复 ◆ 搜索 ◆ 校验口令
属性	◆ *（选择所有标志）*
代理	◆ DS 已重装载 ◆ 本地代理已打开 ◆ 本地代理已关闭 ◆ NLM 已装载
杂项	◆ 生成 CA 密钥 ◆ 已重新认证公共密钥

类别	建议的标志
LDAP	◆ LDAP 绑定 ◆ LDAP 绑定响应 ◆ LDAP 修改 ◆ LDAP 修改响应 ◆ LDAP 口令修改 ◆ LDAP 取消绑定 ◆ LDAP 删除 ◆ LDAP 删除响应 ◆ LDAP 修改 DN ◆ LDAP 修改 DN 响应 ◆ LDAP 搜索 ◆ LDAP 搜索响应 ◆ LDAP 添加 ◆ LDAP 添加响应

VI 安装 Designer

本部分将指导您完成 Designer for Identity Manager 的安装过程。默认情况下，安装程序将在 C:\Netiq 中安装组件。

重要：请确保包含 Designer 安装程序的目录名称不带空格。如果目录名称包含空格，则安装 Designer 期间不会安装 NICI。例如，目录名称不能是 Designer Install，但可以是 DesignerInstall。

NetIQ 建议您在开始之前，先查看安装过程。有关详细信息，请参见第 20 章 “ 规划安装 Designer”（第 265 页）。

20 规划安装 Designer

本章提供了安装 Designer 所需的先决条件、注意事项以及系统设置。首先，请查阅核对清单，以了解安装过程。

20.1 Designer 安装核对清单

NetIQ 建议您在开始安装前先查看以下步骤：

	核对清单项目
❑	1. 查看产品体系结构信息，以了解 Identity Manager 组件之间的交互。有关详细信息，请参见第 1 章 “Identity Manager 的组件概述 ”（第 19 页）。
❑	2. 确定要为 Identity Manager 组件使用哪些服务器。有关详细信息，请参见第 5.3 节 “ 建议的安装方案和服务器设置 ”（第 39 页）。
❑	3. 查看安装 Designer 的注意事项，以确保计算机符合先决条件。有关详细信息，请参见第 20.2 节 “Designer 的安装先决条件 ”（第 266 页）。
❑	4. 确保安装 Designer 的目标计算机符合指定的软件和硬件要求。有关详细信息，请参见第 20.3 节 “Designer 的系统要求 ”（第 266 页）。
❑	5. 要安装 Designer，请参见以下章节之一： ◆ 运行 Windows 可执行文件 （第 269 页） ◆ 使用无提示安装过程 （第 269 页）
❑	6. 安装其余的 Identity Manager 组件。
❑	7. （可选）要启动 Identity Manager 解决方案的项目，请参见 *《NetIQ Designer for Identity Manager Administration Guide》*（NetIQ Designer for Identity Manager 管理指南）。

20.2 Designer 的安装先决条件

本节提供了安装 Designer 的注意事项和系统要求。

在安装或升级 Designer 之前，请先查看以下注意事项：

- 在安装 Designer 之前，必须先安装 32 位 Novell International Cryptographic Infrastructure (NICI) 包。
- 您不能为 Designer 3.0 或更高版本使用 Designer 2.1*x* 工作空间，因为旧版工作空间与较新版本的 Designer 不兼容。Designer 将在**工作空间**中储存项目和配置信息。例如，在 **Windows 10 和 Windows 7** 上， Designer 4.x 工作空间默认将安装在 %UserProfile%\designer_workspace 目录中。

20.3 Designer 的系统要求

本节提供要安装 Designer 的服务器的最低要求。请务必查看安装的先决条件和注意事项，特别是与操作系统有关的内容。

类别	要求
处理器	1 GHz
磁盘空间	1 GB
内存	1 GB
操作系统 （经认可）	以下 64 位操作系统之一 （最低版本）： **服务器** ◆ Windows Server 2016 ◆ Windows Server 2012 R2 **Desktops** ◆ Windows 10 ◆ Windows 8
操作系统 （受支持）	经认可操作系统的最新版服务包 **注释：***受支持*指操作系统尚未经过测试，但预期可以正常工作。
虚拟化系统	◆ Hyper-V Server 2012 R2 ◆ VMWare ESX 5.0 及更高版本 ◆ 包含 Hyper-V 的 Windows Server 2012 R2 Virtualization （受支持） NetIQ 支持在为运行 NetIQ 产品的操作系统提供官方支持的企业级虚拟化系统上安装 Identity Manager。只要虚拟化系统的供应商为这些操作系统提供官方支持， NetIQ 就可支持这些系统上的整个 Identity Manager 堆栈。

类别	要求
Web 浏览器	以下任意浏览器 （最低版本）： ◆ Internet Explorer 11 ◆ Chrome 61 ◆ Firefox 51

21 安装 Designer

您可以根据目标计算机，使用可执行文件、二进制文件或文本模式安装 Identity Manager Designer。您还可以执行无提示安装。使用默认位于 \products\Designer\ 目录中的安装程序：

Identity Manager 的多个组件都需要 Designer 中的包。当您安装 Designer 时，安装程序将自动向新项目中添加数个包。

21.1 运行 Windows 可执行文件

1 使用管理员帐户登录到要安装 Designer 的计算机。

2 从 NetIQ 下载网站下载 Identity_Manager_4.7_Windows_Designer.zip。

3 解压缩 Identity_Manager_4.7_Windows_Designer.zip 文件。

4 运行 install.exe 文件。

5 遵循向导中的步骤操作，直到完成安装过程。

21.2 使用无提示安装过程

您可以使用脚本来执行无提示的 Designer 安装，此过程无需用户交互。除非您编辑了 designerInstaller.properties 文件，否则 -i silent 选项将使用默认的参数值进行安装。

1 使用管理员帐户登录到要安装 Designer 的目标计算机。

2 浏览到包含安装程序的目录。

3 （可选）要配置 Designer 的安装目录和语言，请完成以下步骤。

   3a 打开 designerInstaller.properties 文件 （默认位于 *Path_to_unzipped_Designer_file*\products\Designer 目录中）。

   3b 在该属性文件中，修改以下参数的值：

   USER_INSTALL_DIR

   指定要将 Designer 安装到的位置路径。例如：

   ```
   USER_INSTALL_DIR=C:\designer
   ```

   如果指定的路径不是以 designer 目录结尾， Designer 安装程序会自动追加 designer 目录。

   SELECTED_DESIGNER_LOCALE

   指定以下语言之一，作为安装后起动 Designer 所使用的语言：

   - zh_CN - 简体中文

- zh_TW - 繁体中文
- nl - 荷兰语
- en - 英语
- fr - 法语
- de - 德语
- it - 意大利语
- ja - 日语
- pt_BR - 巴西葡萄牙语
- es - 西班牙语

3c 保存并关闭属性文件。

4 运行以下命令之一：

```
install -i silent -f Path\designerInstaller.properties
```

21.3 修改包含空格字符的安装路径

您可以将 Designer 安装到目录名称中包含空格的位置。但是，在安装 Designer 后，必须修改 StartDesigner.bat 和 Designer.ini 文件，才能确保 Designer 正常运行。手动将空格替换为转义符（“\”）。例如：

将

```
C:\designer installation
```

更改为

```
C:\designer\ installation
```

VII 安装 Analyzer

本部分将指导您完成安装 Analyzer for Identity Manager 的过程。 Analyzer 是安装在工作站上的富客户端组件。可以使用 Analyzer 来检查和清理您要添加到 Identity Manager 解决方案的已连接系统中的数据。在规划阶段使用 Analyzer 可以了解需要进行的更改及这些更改的效果。

安装文件位于 Identity Manager 安装包的 .iso 映像文件中的 \products\Analyzer 目录内。默认情况下，安装程序将在 C:\NetIQ\Analyzer 中安装组件。

NetIQ 建议您在开始之前，先查看安装过程。有关详细信息，请参见第 22.1 节 “Analyzer 安装核对清单 ”（第 273 页）。

22 计划安装 Analyzer

本章提供有关准备安装 Analyzer for Identity Manager 的指导。NetIQ 建议您在开始之前，先查看安装过程。

22.1 Analyzer 安装核对清单

NetIQ 建议您在开始安装过程之前先查看以下步骤：

	核对清单项目
❑	1. 了解 Identity Manager 各组件之间的交互。有关详细信息，请参见第 1 章 “Identity Manager 的组件概述 ” （第 19 页）。
❑	2. 确定要为 Identity Manager 组件使用哪些服务器。有关详细信息，请参见第 5.3 节 “ 建议的安装方案和服务器设置 ” （第 39 页）。
❑	3. 确保您的环境符合有关托管 Analyzer 的注意事项和要求。有关详细信息，请参见第 22.2 节 “ 安装 Analyzer 需要满足的系统要求 ” （第 273 页）。
❑	4. 要安装 Analyzer，请参见以下章节： ◆ 要使用安装向导，请参见第 23.1 节 “ 使用向导安装 Analyzer” （第 275 页）。 ◆ 对于无提示安装，请参见第 23.2 节 “ 以无提示模式安装 Analyzer” （第 276 页）
❑	5. （可选）要自动接收和显示来自 Analyzer 的审计事件，请安装 XDAS 客户端。有关详细信息，请参见第 23.3 节 “ 安装 Analyzer 的审计客户端 ” （第 276 页）。
❑	6. 要激活 Analyzer，请参见激活 Analyzer （第 312 页）。
❑	7. （可选）要升级 Analyzer，请参见第 32.7 节 “ 升级 Analyzer” （第 343 页）。

22.2 安装 Analyzer 需要满足的系统要求

本节提供要安装 Analyzer 的服务器的最低要求。请务必查看安装的先决条件和注意事项，特别是与操作系统有关的内容。

类别	要求
处理器	1 GHz
内存	512 MB （建议 4 GB）
视频分辨率	1024*768 （建议 1280*1025）

类别	要求
操作系统 （经认可）	以下 64 位操作系统之一： ◆ Windows Server 2016 ◆ Windows Server 2012 R2 ◆ Windows Server 2012 NetIQ 建议您在安装 Identity Manager 之前，按照制造商的自动更新工具应用最新的操作系统增补程序。 **注释：***经认可*指操作系统已经过全面测试且受支持。
操作系统 （受支持）	经认可操作系统的最新版服务包 **注释：***受支持*指操作系统尚未经过测试，但预期可以正常工作。
虚拟化系统	◆ Hyper-V Server 2012 R2 ◆ VMWare ESX 5.0 及更高版本 NetIQ 支持在为运行 NetIQ 产品的操作系统提供官方支持的企业级虚拟化系统上安装 Identity Manager。只要虚拟化系统的供应商为这些操作系统提供官方支持， NetIQ 就可支持这些系统上的整个 Identity Manager 堆栈。

23 安装 Analyzer

本章将指导您完成安装 Analyzer 并为 Analyzer 配置环境的过程。

23.1 使用向导安装 Analyzer

以下过程介绍了如何使用安装向导安装 Analyzer。要执行无提示或无人照管安装，请参见第 23.2 节 “ 以无提示模式安装 Analyzer” （第 276 页）。

要准备安装，请查看第 22.1 节 “Analyzer 安装核对清单 ” （第 273 页）中列出的先决条件和系统要求。

1 登录要安装 Analyzer 的计算机。

2 （视情况而定）如果您已获取 Identity Manager 安装包的 .iso 映像文件，请导航到包含 Analyzer 安装文件的目录 （默认情况下在 \products\Analyzer 目录中）。

3 （视情况而定）如果您已下载 Analyzer 安装文件，请完成以下步骤：

   3a 导航到所下载映像的 win.zip 文件。

   3b 将该文件的内容解压缩到本地计算机上的某个文件夹中。

4 从 \products\Analyzer 目录执行 install.exe 安装程序：

5 遵循向导中的说明操作，直到完成安装 Analyzer。

6 安装过程完成后，复查安装后摘要，以检查 Analyzer 的安装状态及其日志文件的位置。

7 单击**完成**。

8 （可选）要在 Windows 计算机上为 Analyzer 配置基于角色的服务，请打开默认情况下位于 C:\Program Files (x86)\NetIQ\Tomcat\webapp\nps\help\en\install 目录中的 gettingstarted.html 网站的链接。

   请使用 iManager 来配置基于角色的服务。

9 要激活 Analyzer，请参见激活 Analyzer （第 312 页）。

23.2 以无提示模式安装 Analyzer

无提示 （非交互式）安装不显示用户界面，也不向用户提出任何问题。此时， InstallAnywhere 将使用默认 analzerInstaller.properties 文件中的信息。您可以使用默认文件运行无提示安装，或者编辑该文件以自定义安装过程。

默认情况下，安装程序将在 Program Files (x86)\NetIQ\Analyzer 目录中安装 Analyzer。

1 登录到要安装 Analyzer 的计算机。
2 （视情况而定）如果您已获取 Identity Manager 安装包的 .iso 映像文件，请导航到包含 Analyzer 安装文件的目录 （默认情况下在 \products\Analyzer 目录中）。
3 （视情况而定）如果您已从 NetIQ 下载网站下载了 Analyzer 安装文件，请完成以下步骤：
   - **3a** 导航到所下载映像的 win.zip 文件。
   - **3b** 将该文件的内容解压缩到本地计算机上的某个文件夹中。
4 （可选）要指定非默认安装路径，请完成以下步骤：
   - **4a** 打开默认位于 \products\Analyzer 目录中的 analzerInstaller.properties 文件。
   - **4b** 在该 properties 文件中添加以下文本：

     ```
     USER_INSTALL_DIR=installation_path
     ```
5 要运行无提示安装，请发出以下命令：

   install.exe -i silent -f analyzerInstaller.properties
6 要激活 Analyzer，请参见激活 Analyzer （第 312 页）。

23.3 安装 Analyzer 的审计客户端

Analyzer 包含一个 XDAS 库，当您向应用程序发回数据更新时，该库将从 “ 数据浏览器 ” 编辑器自动生成审计事件。有关在源应用程序中使用 “ 数据浏览器 ” 编辑器更新数据的详细信息，请参见《*NetIQ Analyzer for Identity Manager Administration Guide*》（NetIQ Analyzer for Identity Manager 管理指南）中的 “Modifying Data” （修改数据）。

要查看这些审计事件，请安装可从 Analyzer 接收审计事件的 XDAS 客户端。 OpenXDAS Project (http://openxdas.sourceforge.net) （OpenXDAS 项目）中提供了有关 XDAS 的详细信息。

Analyzer 的下载包中包含 Windows 版 XDAS 客户端。但是，Analyzer 的安装程序不会安装 XDAS 客户端。

1 安装 Analyzer。
2 导航到 OpenXDAS 安装文件；这些文件默认位于 .iso 映像文件的 \products\Analyzer\openxdas\ *操作系统*目录中。
3 起动 XDAS 客户端的安装程序 （.msi 文件）：
4 遵循提示安装 XDAS 客户端。
5 安装过程完成后，起动 XDAS 客户端，以自动接收和显示来自 Analyzer 的审计事件。

VIII 在 Identity Manager 中配置单点登录访问

默认情况下， Identity Manager 使用 OSP 进行单点登录访问。安装 Identity Reporting 和 Identity Applications 时，您可以指定用户鉴定的基本设置。但是，您也可以将 OSP 鉴定服务器配置为接受来自 Kerberos 票据服务器或 SAML IDP 的鉴定。例如，您可以使用 SAML 支持来自 NetIQ Access Manager 的鉴定。有关 OSP 的详细信息，请参见第 4.5 节 “ 在 Identity Manager 中使用单点登录访问 ”（第 33 页）。

24 准备单点登录访问

默认情况下， Identity Manager 使用 OSP 进行单点登录访问。安装 Identity Reporting 和 Identity Applications 时，您可以指定用户鉴定的基本设置。但是，您也可以将 OSP 鉴定服务器配置为接受来自 Kerberos 票据服务器或 SAML IDP 的鉴定。例如，您可以使用 SAML 支持来自 NetIQ Access Manager 的鉴定。

NetIQ 建议您完成以下核对清单中的步骤。

	核对清单项目
❑	1. 了解 Identity Manager 如何使用 OSP 进行单点登录访问。有关详细信息，请参见第 4.5 节 " 在 Identity Manager 中使用单点登录访问 " （第 33 页）。
❑	2. 安装 OSP。有关详细信息，请参见第 14 部分 " 安装口令管理组件 " （第 155 页）。
❑	3. 安装 Identity Applications。有关详细信息，请参见第 IV 部分 " 安装 Identity Applications" （第 139 页）。
❑	4. （可选）安装 Identity Reporting。有关详细信息，请参见第 V 部分 " 安装 Identity Reporting" （第 223 页）。
❑	5. 将 Identity Applications 配置为使用 OSP 进行单点登录访问。有关详细信息，请参见第 25 章 " 在 Identity Manager 中使用 One SSO Provider 进行单点登录访问 " （第 281 页）。
❑	6. 安装要用于 Identity Manager 的鉴定系统。例如：Access Manager 或 Kerberos。
❑	7. （视情况而定）配置 Access Manager 和 OSP。有关详细信息，请参见第 26 章 " 对 NetIQ Access Manager 使用 SAML 鉴定进行单点登录 " （第 283 页）。
❑	8. 校验单点登录设置。有关详细信息，请参见第 28 章 " 校验是否可对 Identity Applications 进行单点登录访问 " （第 293 页）。

25 在 Identity Manager 中使用 One SSO Provider 进行单点登录访问

要提供对 Identity Applications 的单点登录访问，您必须配置 RBPM 配置实用程序中的一些设置。您应该已具备必要的证书和密钥，以便在安装 OSP 后进行单点登录。

此过程假设您的环境将为 eDirectory、SSO 控制器和 OAuth 提供程序使用一个证书。如果您的组织需要更多分离层，请为 OAuth 提供程序单独创建一个证书。

25.1 准备 eDirectory 进行单点登录访问

在安装 eDirectory 的过程中，您必须配置身份库以支持对 Identity Applications 和 Identity Reporting 进行单点登录访问。

执行第 15.7.5 节 " 配置 Identity Applications 的身份库 "（第 196 页）中所述的步骤。如果您先前已将 eDirectory 纲要扩展为包含 SAML 纲要，并安装了所需的 NMAS 方法，则不需要再次执行这些步骤，而是可以直接跳转到有关创建可信根容器的小节。

25.2 修改单点登录访问的基本设置

在安装 Identity Applications 时，您通常需要配置单点登录访问的基本设置。本节将帮助您确保这些设置适合您的环境。

1 运行 RBPM 配置实用程序。有关详细信息，请参见第 15.8.1 节 " 运行 Identity Applications 配置实用程序 "（第 204 页）。

2 要修改鉴定设置，请完成以下步骤：

   2a 单击**鉴定**。

   2b （视情况而定）要指定实际的服务器 DNS 名称或 IP 地址，请更改 localhost 的所有实例。

   - 指定的地址必须可从所有客户端解析。仅当对 Identity Manager 的所有访问 （包括通过浏览器访问）都是从本地进行时，才应使用 localhost。
   - 此 " 公共 " 主机名或 IP 地址应与您在安装 OSP 时指定的 *PublicServerName* 值相同。有关详细信息，请参见第 14.2 章 " 为 Identity Manager 安装口令管理 "（第 157 页）。
   - 在分布式或群集环境中，所有 OAuth URL 都应该使用相同的值。该 URL 应该通过 L4 交换机或负载平衡器实现客户端访问。此外， osp.war 和配置文件必须安装到环境中的每个部署上。

   2c 对于**管理员容器的 LDAP DN**，请单击**浏览**按钮，然后选择身份库中包含 Identity Applications 管理员的容器。

   2d 指定您在安装 OSP 时创建的 OAuth 密钥存储区文件。有关详细信息，请参见第 14.2 章 " 为 Identity Manager 安装口令管理 "（第 157 页）。

   请包含密钥存储区文件路径、密钥存储区文件口令、密钥别名和密钥口令。默认的密钥存储区文件为 osp.jks，默认的密钥别名为 osp。

3 要修改单点登录设置，请完成以下步骤：

3a 单击 **SSO 客户端**。

3b （视情况而定）要指定实际的服务器 DNS 名称或 IP 地址，请更改 localhost 的所有实例。

- 指定的地址必须可从所有客户端解析。仅当对仪表板的所有访问 （包括通过浏览器访问）都将在本地进行时，才应使用 localhost。
- 此 " 公共 " 主机名或 IP 地址应与您在安装 OSP 时指定的 *PublicServerName* 值相同。有关详细信息，请参见第 14.2 章 " 为 Identity Manager 安装口令管理 " （第 157 页）。
- 在分布式或群集环境中，所有 OAuth 重定向 URL 都应该使用相同的值。该 URL 应该通过 L4 交换机或负载平衡器实现客户端访问。

3c （视情况而定）如果使用非默认端口，请更新以下 Identity Manager 组件的端口号：

- Identity Applications 管理
- Identity Manager 仪表板
- Identity Reporting
- User Application

4 单击**确定**保存所做的更改，然后关闭配置实用程序。

5 启动 Tomcat。

25.3 将 Self Service Password Reset 配置为信任 OSP

要正常使用单点登录，您必须使用证书在 OSP 与 Self Service Password Reset (SSPR) 之间配置信任关系。您必须从 OSP 的密钥存储区文件 osp.jks 中导出证书。

导出证书后，必须将它导入 SSPR 的密钥存储区文件。 SSPR 的默认密钥存储区文件路径为 C:\[Java_Home]\lib\security\cacerts。

有关设置安全通道的详细信息，请参见 《Self Service Password Reset Administration Guide》（Self Service Password Reset 管理指南）中的 "Setting Up a Secure Channel Between the Application Server and the LDAP Server" （在应用程序服务器与 LDAP 服务器之间设置安全通道）。

26 对 NetIQ Access Manager 使用 SAML 鉴定进行单点登录

本章将帮助您配置 NetIQ Access Manager 和 OSP，以支持在 Identity Manager 中使用 SAML 2.0 鉴定进行单点登录访问。在开始之前，请先查看操作说明所基于的以下假设：

- 您已装有新的受支持 Access Manager 版本。
- 您已装有新版 Identity Manager。
- 这两项安装的主机名配置都使用了 DNS 名称。
- 这两项安装都使用 SSL 协议进行通讯。
- 您必须为 Access Manager 设置一个使用身份库作为 LDAP 用户存储区的群集环境。有关详细信息，请参见《*NetIQ Access Manager Administration Guide*》（NetIQ Access Manager 管理指南）。

26.1 了解第三方鉴定和单点登录

您可以将 Identity Manager 配置为使用 SAML 2.0 鉴定来与 NetIQ Access Manager 相互协作。借助此项功能，您可以使用一项非基于口令的技术通过 Access Manager 登录到 Identity Applications。例如，用户可以通过用户 （客户端）证书进行登录，例如从智能卡登录。

Access Manager 将与 OSP 交互，以将用户映射到身份库中的 DN。当用户通过 Access Manager 登录 Identity Applications 时， Access Manager 可在 HTTP 标题中插入一个 SAML 声明 （使用用户的 DN 作为标识符），并将该请求转发到 Identity Applications。 Identity Applications 使用该 SAML 声明与身份库建立 LDAP 连接。

如果将 SAML 声明用于 Identity Applications 鉴定，则允许基于口令的单点登录鉴定的附属 Portlet 将不支持单点登录。

26.2 创建和安装 SSL 证书

为确保完成鉴定，Access Manager 和 OSP 必须共享其 SSL 证书的可信根。本节将帮助您为 Access Manager 创建新证书，并确保可信证书存储区包含正确的证书。

26.2.1 为 Access Manager 创建 SSL 证书

Access Manager 无法使用其默认的 SSL 证书 test-connector 来与 Identity Manager 进行通讯。您必须创建一个证书主题字段中包含主机名的证书，然后将它指派给 Access Manager。

有关详细信息，请参见《*NetIQ Access Manager Administration Console Guide*》（NetIQ Access Manager 管理控制台指南）中的 "Security and Certificate Management"（安全性和证书管理）。

1 打开 Access Manager 的管理控制台。
2 单击**安全性 > 证书**。
3 单击**新建**。
4 指定新证书的名称。例如：*hostname*_ssl。
5 单击窗口右侧的编辑按钮。
6 对于**常用名**，请指定托管 Access Manager 的服务器的 DNS 名称，然后单击**确定**。
7 对于**有效月数**，请指定一个不超过 99 的值。
8 对于**密钥大小**，请指定 2048。
9 选择新建的证书，然后单击**操作 > 将证书添加到密钥存储区 ...**。
10 单击**密钥存储区**右侧的编辑按钮。
11 选择 **SSL 连接器**，然后单击**确定**。
12 单击**确定**。
13 在 OSP 可信证书存储区中安装新证书。有关详细信息，请参见第 26.2.2 节 " 在 Identity Manager 可信证书存储区中安装 Access Manager 证书 "（第 284 页）。

26.2.2 在 Identity Manager 可信证书存储区中安装 Access Manager 证书

OSP 可信证书存储区必须包含 Access Manager 的安全性证书。

1 要导出新的 SSL 证书，请完成以下操作：
   - 在 Access Manager 管理控制台的**安全性** > **可信根**下，导出 SSL 证书的根证书。将根证书命名为 **configCA**。
   - 导出 SSL 服务器证书。

     有关详细信息，请参见《*NetIQ Access Manager Administration Console Guide*》（NetIQ Access Manager 管理控制台指南）中的 "Managing Trusted Roots and Trust Stores"（管理可信根和可信证书存储区）。
2 将导出的证书复制到运行 OSP 的服务器上。
3 使用随 Java 提供的 keytool 将该文件导入到 JRE 的 cacerts 密钥存储区中。

   例如， C:\NetIQ\idm\apps\jre\bin\keytool -importcert -trustcacerts -alias <NAM-cert> -keystore C:\NetIQ\idm\apps\jre\bin\security\cacerts -storepass <password> -file custom_location\<exported_file>
4 在 Access Manager 可信证书存储区中安装 OSP 证书。

   有关详细信息，请参见第 26.2.3 节 " 在 Access Manager 可信证书存储区中安装 SSL 服务器证书 "（第 285 页）。

26.2.3 在 Access Manager 可信证书存储区中安装 SSL 服务器证书

Access Manager 可信证书存储区必须包含 OSP 的安全性证书。有关详细信息，请参见《*NetIQ Access Manager Administration Console Guide*》（NetIQ Access Manager 管理控制台指南）中的 "Managing Trusted Roots and Trust Stores"（管理可信根和可信证书存储区）。

获取运行 OSP 的 Tomcat 实例要用于 SSL 的服务器证书。

1 将托管 OSP 的 Tomcat 实例的 SSL 服务器证书复制到装有 Access Manager 的服务器。
2 打开 Access Manager 的管理控制台。
3 要导入证书，请单击**安全性 > NIDP 可信证书存储区**。
4 单击**添加**。
5 从**添加**对话框 > **导入**中选择 " 可信根 "。
6 选择要导入的根证书，然后单击**确定**。
7 确保 OSP 能够识别来自 SAML 的鉴定声明。

   有关详细信息，请参见第 26.4.2 节 " 创建 SAML 的属性集 "（第 286 页）。

26.3 将 Identity Manager 配置为信任 Access Manager

对于鉴定请求， Identity Manager 需要使用 SAML 元数据的 URL 来重定向用户。默认情况下，Access Manager 使用以下 URL 来储存 SAML 元数据：

`https://server:port/nidp/saml2/metadata`

其中， *server*:*port* 表示 Access Manager 身份服务器。

1 （可选）要查看 SAML 元数据的 .xml 文档，请在浏览器中打开该 URL。

   如果该 URL 未生成文档，请确保链接正确无误。
2 在 OSP 服务器上，运行 RBPM 配置实用程序。有关详细信息，请参见第 15.8.1 节 " 运行 Identity Applications 配置实用程序 "（第 204 页）。
3 在实用程序中选择**鉴定**。
4 对于**鉴定方法**，请指定 **SAML 2.0**。
5 对于**元数据 URL**，请指定 OSP 用于将鉴定请求重定向到 Access Manager 的 SAML 元数据的 URL。

   例如：https://*server:port*/nidp/saml2/metadata
6 在**鉴定服务器**部分的 **OAuth 服务器主机标识符**设置中，指定托管 OSP 的服务器的 DNS 名称。
7 单击**确定**保存更改。
8 重启动托管 OSP 的 Tomcat 实例。

26.4 将 Access Manager 配置为与 Identity Manager 配合工作

为确保 Access Manager 将 Identity Manager 识别为可信的服务提供程序，请将 OSP 的元数据文本添加到身份服务器，并配置一个属性集。此过程包括以下活动：

- 第 26.4.1 节 " 复制 Identity Manager 的元数据 "（第 286 页）
- 第 26.4.2 节 " 创建 SAML 的属性集 "（第 286 页）
- 第 26.4.3 节 " 将 Identity Manager 添加为可信的服务提供程序 "（第 287 页）

26.4.1 复制 Identity Manager 的元数据

Access Manager 需要 OSP 的元数据文本。您应该将元数据 .xml 文件的内容复制到可通过 Access Manager 身份服务器打开的文档。

1 在浏览器中，浏览到 OSP 元数据的 URL。默认情况下， Identity Manager 使用以下 URL：

   `https://server:port/osp/a/idm/auth/saml2/spmetadata`

   其中， *server*:*port* 表示托管 OSP 的 Tomcat 服务器。

2 查看 spmetadata.xml 文件的页面来源。

3 将该文件的内容复制到可在将 Identity Manager 添加为可信的服务提供程序 （第 287 页）中访问的文档

26.4.2 创建 SAML 的属性集

为确保 SAML 能够在 Access Manager 与 OSP 之间执行声明交换，请在 Access Manager 中创建一个属性集。属性集为交换提供了一个通用命名方案。 OSP 会查找用于标识声明主题的属性值。默认情况下，该属性为 mail。

有关详细信息，请参见 《*NetIQ Access Manager Administration Guide*》（NetIQ Access Manager 管理指南）中的 "Configuring Attribute Sets"（配置属性集）。

1 打开 Access Manager 的管理控制台。

2 单击**设备 > 身份服务器 > 共享设置 > 属性集 > 新建**。

3 指定属性集的名称。例如：IDM SAML Attributes。

4 单击**下一步**，然后单击**新建**。

5 对于**本地属性**，请选择 **Ldap 属性：mail [LDAP 属性配置文件]**。

6 对于**远程属性**，请指定 mail。

7 单击**确定**，然后单击**完成**。

26.4.3 将 Identity Manager 添加为可信的服务提供程序

配置 Access Manager 以将 Identity Manager 识别为可信的服务提供程序。有关详细信息，请参见《*NetIQ Access Manager Administration Guide*》（NetIQ Access Manager 管理指南）中的 "Creating a Trusted Service Provider for SAML 2.0" （为 SAML 2.0 创建可信的服务提供程序）。

1 打开 Access Manager 的管理控制台。
2 单击**设备 > 身份服务器 > 编辑 > SAML 2.0**。
3 单击**新建 > 服务提供程序**。
4 对于**提供程序类型**，请指定**一般**。
5 对于**源**，请指定**元数据文本**。
6 在**文本**字段中，粘贴您在复制 Identity Manager 的元数据 （第 286 页）中复制的 spmetadata.xml 文件内容。
7 指定新 OSP 服务提供程序的名称。
8 单击 " 下一步 "，然后单击 " 完成 "。
9 在 **SAML 2.0** 选项卡上，选择您在步骤 7 中创建的 OSP 服务提供程序。
10 单击**属性**。
11 选择您在创建 SAML 的属性集 （第 286 页）中创建的属性集。例如：IDM SAML Attributes。
12 将可用于 OSP 服务提供程序集的属性移至页面左侧的**鉴定时发送**面板中。

   移至**鉴定时发送**面板中的属性就是您在鉴定期间要获取的属性。
13 单击**确定**两次。
14 要更新身份服务器，请单击**设备 > 身份服务器 > 更新 > 更新所有配置**。

26.5 更新 Access Manager 的登录页面

Access Manager 的默认登录页面使用 HTML iFrame 元素，这些元素与 Identity Applications 所用的元素相冲突。本节说明了如何通过创建 Access Manager 的新登录方法和协定来消除该冲突。本节所述的 .jsp 文件默认位于 C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\jsp 目录中。

有关详细信息，请参见《*NetIQ Access Manager Administration Guide*》（NetIQ Access Manager 管理指南）中的 "Customizing the Identity Server Login Page" （自定义身份服务器登录页面）。

1 根据 TID 7004020 和 TID 7018468 的内容修改 top.jsp 文件。
2 （可选）为进行备份，请复制 login.jsp 文件并进行重命名。例如，将其重命名为 idm_login.jsp。
3 打开 Access Manager 的管理控制台。
4 要创建新的登录方法，请完成以下步骤：
   - **4a** 单击**设备 > 身份服务器 > 编辑 > 本地 > 方法**。
   - **4b** 单击**新建**，然后指定新方法的**显示名称**。例如：IDM Name/Password。
   - **4c** 对于**类**，请指定 **Name/Password-Form**。
   - **4d** 对于**用户存储区**，请指定身份库作为 LDAP 用户存储区。

4e 在属性部分中，单击新建，然后指定以下属性：

名称	值
JSP	idm_login
MainJSP	true

4f 单击确定。

5 要创建使用新登录方法的协定，请完成以下步骤：

5a 单击协定 > 新建。

5b 在配置选项卡中，指定新协定的显示名称。例如：IDM Name/Password。

5c 对于 URI，指定 name/password/uri/idm。

5d 在方法下，添加您在步骤 4 中创建的方法。例如：IDM Name/Password。

5e 在鉴定卡选项卡中，指定卡的 ID。例如：IDM_NamePassword。

5f 指定卡的图像。

5g 单击确定。

6 要指定系统处理新鉴定协定方式的默认值，请完成以下步骤：

6a 在本地选项卡上，单击默认值。

6b 对于 " 用户存储区 "，指定 " 身份库 " 作为 LDAP 用户存储区。

6c 对于鉴定协定，指定您在步骤 5 中创建的协定。例如：IDM Name/Password-Form。

6d 单击确定。

7 要更新身份服务器，请单击设备 > 身份服务器 > 更新 > 更新所有配置。

27 使用 Kerberos 进行单点登录

对于允许单点登录 (SSO) 的 Identity Applications，您可以使用 Kerberos 作为鉴定方法。此方法还允许用户使用集成 Windows 鉴定登录应用程序。本章提供了配置 Active Directory 以使用 Kerberos 连接 Identity Applications 的说明：

27.1 在 Active Directory 中配置 Kerberos 用户帐户

请使用 Active Directory 管理工具来对 Kerberos 鉴定配置 Active Directory。您需要为 Identity Applications 和 Identity Reporting 创建新的 Active Directory 用户帐户。该用户帐户名称必须使用托管 Identity Applications 和 Identity Reporting 的服务器的 DNS 名称。

注释：对于域或领域参照，请使用大写格式。例如 @MYCOMPANY.COM。

---

1 以 Active Director 中的管理员身份，使用 Microsoft 管理控制台 (MMC) 创建一个包含 Identity Applications 所在服务器 DNS 名称的新用户帐户。

   例如，如果 Identity Applications 服务器的 DNS 名称为 rbpm.mycompany.com，则可以使用以下信息来创建用户：

   名：rbpm

   用户登录名：HTTP/rbpm.mycompany.com

   Windows 以前版本的登录名：rbpm

   设置口令：指定相应的口令。例如：Passw0rd。

   密码永不过期：选择此选项。

   用户下次登录时须更改密码：不要选择此选项。

2 将新用户与服务主体名称 (SPN) 相关联。

   2a 在 Active Directory 服务器中打开一个 cmd 外壳。

   2b 在命令提示时输入以下命令：

   ```
   setspn -A HTTP/DNS_Identity_Applications_server@WINDOWS-DOMAIN userID
   ```

   例如：

   ```
   setspn -A HTTP/rbpm.mycompany.com@MYCOMPANY.COM rbpm
   ```

   2c 输入 setspn -L *userID* 以校验 setspn。

3 要生成 keytab 文件，请使用 ktpass 实用程序：

   3a 在命令行提示符处输入以下命令：

```
ktpass /out filename.keytab /princ servicePrincipalName /mapuser
userPrincipalName /mapop set /pass password /crypto ALL /ptype
KRB5_NT_PRINCIPAL
```

例如：

```
ktpass /out rbpm.keytab /princ HTTP/rbpm.mycompany.com@MYCOMPANY.COM /mapuser
rbpm  /mapop set /pass Passw0rd /crypto All /ptype KRB5_NT_PRINCIPAL
```

重要：对于域或领域参照，请使用大写格式。例如， @MYCOMPANY.COM。

3b 将 rbpm.keytab 文件复制到 Identity Applications 服务器中。

4 以 Active Directory 中的管理员身份使用 MCC 创建一个最终用户帐户，以便为 SSO 做好准备。

为支持单点登录，该最终用户帐户名必须与 eDirectory 用户的某个属性值匹配。创建名称类似于 cnano 的用户，记住口令并确保用户下次登录时须更改密码处于未选中状态。

5 （可选）如果您已将报告组件安装在单独的服务器上，请对 Identity Reporting 重复这些步骤。

6 将 Identity Applications 的服务器配置为接受 Kerberos 配置。有关详细信息，请参见第 27.2 节 " 配置 Identity Applications 服务器 "（第 290 页）。

27.2 配置 Identity Applications 服务器

您必须将 Identity Applications 服务器配置为使用您在 Active Directory 中创建的 Kerberos Keytab 文件和用户帐户。在继续操作之前，请确保已完成第 27.1 节 " 在 Active Directory 中配置 Kerberos 用户帐户 "（第 289 页）中的步骤。

注释：对于域或领域参照，请使用大写格式。例如 @MYCOMPANY.COM。

1 要定义 Kerberos 配置的操作系统设置，请完成以下步骤：

1a 在托管 Identity Applications 的服务器上的文本编辑器中打开 C:\Windows\krb5.ini 中的 krb5 文件。

1b 在 krb5 文件中添加以下信息：

```
[libdefaults]
    default_realm = WINDOWS-DOMAIN
    kdc_timesync = 0
    forwardable = true
    proxiable = false
[realms]
    WINDOWS-DOMAIN = {
         kdc = FQDN Active Directory Server
         admin_server = FQDN Active  Directory Server
    }
[domain_realm]
    .your.domain = WINDOWS-DOMAIN
    your.domain = WINDOWS-DOMAIN
```

例如：

```
[libdefaults]
    default_realm = MYCOMPANY.COM
    kdc_timesync = 0
    forwardable = true
    proxiable = false
[realms]
    MYCOMPANY.COM = {
         kdc = myadserver.mycompany.com
         admin_server = myadserver.mycompany.com
    }
[domain_realm]
    .mycompany.com = MYCOMPANY.COM
    mycompany.com = MYCOMPANY.COM
```

1c 保存更改并关闭 krb5 文件。

2 （视情况而定）要定义 Tomcat 的 Kerberos 配置信息，请完成以下步骤：

2a 在 Tomcat 应用程序服务器上，创建包含以下内容的示例 Kerberos_login.config 文件：

注释：novlua 用户需要相应的许可权限才能创建 Kerberos_login.config 文件。

```
com.sun.security.jgss.krb5.accept {
    com.sun.security.auth.module.Krb5LoginModule required
    debug="true"
    refreshKrb5Config="true"
    useTicketCache="true"
ticketCache="c:\NetIQ\idm\apps\tomcat\kerberos\spnegoTicket.cache"
    doNotPrompt="true"
        principal="HTTP/DNS_Identity_Applications_server@WINDOWS-DOMAIN
"
    useKeyTab="true"
        keyTab="/absolute_path/filename.keytab"
    storeKey="true";
    };
```

Windows 服务器上的示例如下所示：

```
keyTab="c:\\NetIQ\\idm\\apps\\tomcat\kerberos\\rbpm.keytab"
```

2b 在该文件中为 principal 和 keyTab 指定值。例如：

```
principal="HTTP/rbpm.mycompany.com@MYCOMPANY.COM"
keyTab="/home/usr/rbpm.keytab"
```

- principal 的值必须与您为 Kerberos 指定的值相匹配。有关详细信息，请参见步骤 3（第 289 页）。
- 提供 Identity Applications 服务器上 keytab 文件的绝对路径。该文件不一定位于 Identity Applications 的默认目录中。

2c 使用以下命令行在 JVM java.security 文件中参照 Kerberos_login.config 文件：

```
login.config.url.1=file:c:\NetIQ\idm\apps\tomcat\kerberos\Kerberos_login.c
onfig
```

3 要在 RBPM 配置实用程序中指定鉴定方法，请完成以下步骤：

3a 打开 Configupdate 实用程序。

3b 单击**鉴定**选项卡。

3c 向下滚动到**鉴定方法**部分。

3d 在方法字段中，选择 Kerberos。

3e 在映射属性名称字段中，指定 cn。

注释：有关 RBPM 配置实用程序的详细信息，请参见第 15.8 章 " 配置 Identity Applications 的设置 "（第 204 页）。

---

4 （可选）如果您已将报告组件安装在单独的服务器上，请对 Identity Reporting 重复这些步骤。

5 配置最终用户用于访问 Identity Applications 的浏览器。有关详细信息，请参见第 27.3 节 " 将最终用户浏览器配置为使用集成 Windows 鉴定 "（第 292 页）。

27.3 将最终用户浏览器配置为使用集成 Windows 鉴定

最终用户用于访问 Identity Applications 和 Identity Reporting 的浏览器也需要配置为使用集成 Windows 鉴定。本节提供将最终用户计算机配置为通过使用集成 Windows 鉴定来支持单点登录访问的说明。

注释：必须对您要允许通过单点登录来访问 Identity Applications 和 Identity Reporting 的每台最终用户计算机都重复此过程。

---

1 登录用户将需要单点登录访问的计算机。

2 打开 "Internet 选项 " 控制面板。

3 单击安全。

4 单击受信任的站点 > 站点。

5 添加 Identity Applications 服务器的 DNS 名称。

例如：rbpm.mycompany.com

6 单击添加，然后单击关闭。

7 单击自定义级别 ...。

8 在用户验证下，选择自动使用当前用户名和密码登录。

9 单击确定。

10 在 "Internet 选项 " 中，单击高级。

11 在 " 安全 " 下，选择启用集成 Windows 验证。

12 对您要允许通过单点登录来访问 Identity Applications 和 Identity Reporting 的每台最终用户计算机重复此过程。

28 校验是否可对 Identity Applications 进行单点登录访问

在安装 Identity Applications 并配置单点登录设置后，您应校验是否能够登录各个应用程序，并在不注销的情况下切换不同的应用程序。默认情况下，应用程序会在 URL 链接中使用以下后缀：

- Identity Applications 管理：/idmadmin
- Identity Manager 仪表板：/idmdash
- User Application：/IDMProv
- Identity Reporting：/IDMRPT

要自定义后缀，请使用 RBPM 配置实用程序。有关详细信息，请参见第 15.8 章 " 配置 Identity Applications 的设置 "（第 204 页）。

要校验单点登录功能，请执行以下操作：

1. 在 Identity Applications 服务器上的新浏览器窗口中，输入仪表板的 URL：

   `https://server:port/idmdash`

   请不要登录到仪表板。

2. 在浏览器中，浏览到 User Application：

   `https://server:port/IDM-context`

3. 校验 User Application 是否显示步骤 1 中所示的同一个登录页面。
4. 登录 User Application。
5. 单击右上角的**主页**图标，然后校验您是否不必再次登录即可访问仪表板。

29 使用 SSL 进行安全通讯

Identity Applications 和 Identity Reporting 使用 HTML 表单进行鉴定。因此，登录过程可能会暴露用户身份凭证。NetIQ 建议您启用 SSL 协议来保护敏感信息。SSL 协议可确保在 Identity Manager 各组件之间处理的通讯是安全的。

您应该准备好证书，以便将 Tomcat 服务器配置为使用 SSL 进行通讯。可通过两种方式获取证书：

- 外部可信的证书颁发机构 (CA) 颁发的证书
- 自我签名证书

29.1 确保 SSL 连接的核对清单

为确保在 Identity Applications、Identity Reporting、SSPR 和 OSP 之间进行安全连接，NetIQ 建议您执行以下核对清单中的步骤：

	核对清单项目
❑	1. 使用密钥存储区来储存鉴定证书。有关详细信息，请参见第 29.2 节 " 创建密钥存储区和证书签名请求 " （第 295 页）。
❑	2. （视情况而定）可以在您的环境中使用自我签名证书或外部 CA 颁发的证书。有关详细信息，请参见第 29.4 节 " 使用自我签名证书启用 SSL" （第 298 页）。对于生产环境，则建议使用外部 CA 颁发的证书。
❑	3. （视情况而定）在生产环境中导入签名的证书。有关详细信息，请参见第 29.3 节 " 使用外部 CA 签名的证书启用 SSL" （第 296 页）。
❑	4. 配置鉴定服务器、 Identity Applications 和 Identity Reporting，以支持 SSL 通讯。有关详细信息，请参见第 29.6 节 " 更新应用程序服务器的 SSL 设置 " （第 303 页）和第 29.7 节 " 在配置实用程序中更新 SSL 设置 " （第 304 页）。

29.2 创建密钥存储区和证书签名请求

密钥存储区是一个 Java 文件，其中包含加密密钥，有时还包含安全性证书。要创建密钥存储区，可以使用 JRE 中提供的 Java Keytool 实用程序。您可以创建 .jks 文件，将证书生成到密钥存储区中。每个证书都与一个唯一的别名关联。将密钥存储区放置在支持 Identity Applications 和 Identity Reporting 的应用程序服务器的 conf 目录中。

1 在命令提示符中，导航到部署了 Identity Applications 的应用程序服务器安装的 conf 目录。例如，C:\NetIQ\idm\apps\tomcat\conf。

   tomcat/conf 路径是安装于 Tomcat 上的 Identity Applications 的默认路径。该路径可能会有所不同，具体取决于应用程序和 Tomcat 的安装方式。

2 使用以下命令设置用于创建密钥存储区的环境路径：

```
cd C:\NetIQ\idm\apps\tomcat\conf
export PATH=C:\NetIQ\idm\apps\jre\bin:$PATH
```

3 使用以下命令创建密钥存储区：

```
keytool -genkey -alias keystore_name -keyalg RSA -keystore
keystore_name.keystore -validity 3650 -keysize 2048
```

例如：

```
keytool -genkey -alias IDMkey -keyalg RSA -keystore IDMkey.keystore -validity
3650 -keysize 2048
```

4 出现提示时，根据以下注意事项指定参数值：

- 对于名字和姓氏，请指定服务器的完全限定名称。例如：

  ```
  MyTomcatServer.NetIQ.com
  ```

- 使用正确的拼写。如果拼错了任何单词，则从签名机构生成签名的证书时，您将会看到错误。

5 （可选）创建一个简单的文本文件，用于保存您为参数值提供的信息副本。

保存此信息可帮助确保在向签名机构提出申请以及导入证书时提供相同的信息。

6 将密钥存储区文件复制到已部署 Identity Manager 组件和 SSPR 的每个应用程序服务器实例的 tomcat/conf 目录。

7 要生成 CA 证书请求，请完成以下步骤：

7a 在 conf 目录中，创建名为 your_request.csr 的简单文本文件。例如：IDMcertrequest.csr。

7b 运行以下命令：

```
keytool -certreq -v -alias keystore_name -file your_request.csr -keypass
keystore_password -keystore your.keystore -storepass your_password
```

例如：

```
keytool -certreq -v -alias IDMkey.keystore -file IDMcertrequest.csr -
keypass IDMkeypass -keystore IDMkey.keystore -storepass IDMpass
```

当您运行该命令时， Keytool 实用程序将在 .csr 文件中填入用于请求证书的相应数据。

8 （视情况而定）要获取签名的证书，请将 .csr 文件提交给有效的证书颁发机构。

9 将证书复制到应用程序服务器的配置目录中。

例如， C:\NetIQ\idm\apps\tomcat\conf。

10 停止 Tomcat。

创建密钥存储区并生成 CA 证书请求后，请遵循以下过程将证书导入密钥存储区：

- 对于外部 CA 签名的证书，请参见第 29.3 节 “ 使用外部 CA 签名的证书启用 SSL”（第 296 页）。
- 对于自我签名证书，请参见第 29.4 节 “ 使用自我签名证书启用 SSL” （第 298 页）。

29.3 使用外部 CA 签名的证书启用 SSL

对于生产环境，请使用有效证书颁发机构颁发的签名证书。本节介绍了如何将签名的证书导入 Identity Applications 的默认 Tomcat 应用程序服务器。

此过程假设您已从有效的证书颁发机构获取了一个签名证书。有关详细信息，请参见第 29.2 节 “ 创建密钥存储区和证书签名请求 ” （第 295 页）。

要使用签名的证书和 SSL，请执行以下操作：

1 将证书复制到应用程序服务器的配置目录中。例如， C:\NetIQ\idm\apps\tomcat\conf。

2 要将根证书转换为 DER 格式，请完成以下步骤：

   2a 双击 conf 目录中储存的证书。

   2b 在 " 证书 " 对话框中，单击**证书路径**。

   2c 选择您从签名机构收到的根证书。

   2d 单击**查看证书**。

   2e 单击**细节 > 复制到文件**。

   2f 在导出证书向导中，单击**下一步**。

   2g 选择**适用于 X.509 的 DER 编码二进制文件 (.CER)**，然后单击**下一步**。

   2h 创建一个新文件用于储存设置了新格式的证书，并将该文件储存在应用程序服务器的 conf 目录中。

   例如， C:\NetIQ\idm\apps\tomcat\conf。

   2i 单击**完成**。

3 要导入转换的证书，请完成以下步骤：

   3a 在命令提示符中，浏览到应用程序服务器的 conf 目录。

   3b 输入下面的命令：

```
keytool -import -trustcacerts -alias root -keystore your.keystore -file
yourRootCA.der
```

   例如：

```
keytool -import -trustcacerts -alias root -keystore IDMkey.keystore -file
IDMTESTREE.der
```

   注释：您必须指定 **root** 作为您的别名。

   导入证书后，服务器会显示**证书已添加到密钥存储区**。

   3c 使用以下命令校验是否已将签名的证书正确导入到 conf 目录中：

```
keytool -list -v -alias root -keystore your.keystore
```

   例如：

```
keytool -list -v -alias root -keystore IDMkey.keystore
```

   服务器会列出您的证书。

4 建议您将签名的证书也导入到 Java cacerts 位置。例如：

```
keytool -import -trustcacerts -alias root -keystore
C:\NetIQ\idm\jre\lib\security\cacerts -file IDMTESTREE.der
```

5 更新应用程序服务器的 SSL 设置，请参见第 29.6 节 " 更新应用程序服务器的 SSL 设置 " （第 303 页）。

6 在配置实用程序中更新 SSL 设置。有关详细信息，请参见第 29.7 节 " 在配置实用程序中更新 SSL 设置 " （第 304 页）。

7 更新 Self Service Password Reset 的 SSL 设置。有关详细信息，请参见第 29.8 节 " 更新 Self Service Password Reset 的 SSL 设置 "（第 306 页）

8 重启动 Tomcat。

29.4 使用自我签名证书启用 SSL

如果您想要在测试环境中使用自我签名证书 （因为与从有效机构获取签名证书相比，这种类型的证书更容易获得），请参阅本节。

29.4.1 导出证书颁发机构

您可以使用 iManager 从 eDirectory 服务器导出证书颁发机构 (CA)，以生成自我签名证书。

1 使用 eDirectory 管理员的用户名和口令登录 iManager。

2 单击 " 管理 ">" 修改对象 "。

3 在安全性容器中，浏览到名为 *TreeName* CA.Security 的 CA 对象。例如：IDMTESTTREE CA.Security。

4 单击**确定**。

5 单击**证书 > 自我签名证书**。

6 选择要使用的自我签名证书。

示例：**自我签名证书 RSA**

6a 选中**自我签名证书 RSA**。

6b 单击**验证**。

7 单击**导出**。

8 清除**导出私用密钥**。

9 单击**导出格式 > DER**。

10 单击**下一步**。

11 单击**保存导出的证书**。

12 单击**保存文件**。

iManager 会将该文件保存为 *TreeName* cert.der。例如：IDMTESTREE cert.der。

13 单击**关闭**。

14 将证书复制到应用程序服务器的配置目录中 (cert.der)。

例如， C:\NetIQ\idm\apps\tomcat\conf。

15 要导入根证书，请完成以下步骤：

15a 在命令提示符中，使用以下命令导航到应用程序服务器的 conf 目录：

```
keytool -import -trustcacerts -alias root -keystore <keystore
file>.keystore -file exported_certificate_filename.der
```

示例：

```
keytool -import -trustcacerts -alias root -keystore IDMkey.keystore -file
cert.der
```

注释：您必须指定 **root** 作为您的别名。

导入证书后，服务器会显示**证书已添加到密钥存储区**。

15b 建议您将根证书也导入到 Java cacerts 位置。

例如：

```
keytool -import -trustcacerts -alias root -keystore
C:\NetIQ\idm\jre\lib\security\cacerts -file cert.der
```

15c 使用以下命令校验是否已将签名的证书正确导入到 conf 目录中：

```
keytool -list -v -alias root -keystore your.jks
```

例如：

```
keytool -list -v -alias root -keystore IDMkey.jks
```

服务器会列出证书。

29.4.2 生成自我签名证书

在生成自我签名证书之前，请确保您有一个密钥存储区和证书请求文件。有关详细信息，请参见第 29.2 节 " 创建密钥存储区和证书签名请求 "（第 295 页）

1. 登录到 iManager。
2. 浏览到**证书服务器 > 颁发证书**。
3. 浏览到第 29.2 节 " 创建密钥存储区和证书签名请求 "（第 295 页）的步骤 7 中创建的 .csr 文件。

   示例：IDMcertrequest.csr
4. 单击**下一步**两次。
5. 对于证书类型，请单击**未指定**。
6. 单击**下一步**两次。

   iManager 会将文件保存为 csr_request_name.der。示例：IDMcertrequest.der
7. 将证书复制到应用程序服务器的配置目录中 (IDMcertrequest.der)。

   例如， C:\NetIQ\idm\apps\tomcat\conf。
8. 要导入生成的自我签名证书，请完成以下步骤：

   8a 在命令提示符中，使用以下命令导航到应用程序服务器的 conf 目录：

   ```
   keytool -import -alias keystore_name -keystore <keystore_file> -file
   <signed_certificate_filename>.der
   ```

   示例：

   ```
   keytool -import -alias IDMkey -keystore IDMkey.keystore -file
   IDMcertrequest.der
   ```

   注释：必须指定密钥存储区名称作为别名。

   导入证书后，服务器会显示**证书已添加到密钥存储区**。

8b 建议您将自我签名证书也导入到 Java cacerts 位置。

例如：

```
keytool -import -alias IDMkey -keystore
C:\NetIQ\idm\jre\lib\security\cacerts -file IDMcertrequest.der
```

8c 使用以下命令校验是否已将签名的证书正确导入到 conf 目录中：

```
keytool -list -v -alias keystore_name -keystore your.jks
```

例如：

```
keytool -list -v -alias IDMkey -keystore IDMkey.jks
```

服务器会列出证书。

9 更新应用程序服务器的 SSL 设置。有关详细信息，请参见 第 29.6 节 " 更新应用程序服务器的 SSL 设置 "（第 303 页）。

10 在配置实用程序中更新 SSL 设置。有关详细信息，请参见第 29.7 节 " 在配置实用程序中更新 SSL 设置 "（第 304 页）。

11 更新 Self Service Password Reset 的 SSL 设置。有关详细信息，请参见第 29.8 节 " 更新 Self Service Password Reset 的 SSL 设置 "（第 306 页）

12 重启动 Tomcat。

29.5 在 Sentinel 与 Identity Manager 组件之间启用 SSL

您可以创建并导出自我签名的服务器证书，以确保在 Sentinel 与 Identity Manager 组件之间进行安全通讯。请使用有效证书颁发机构颁发的签名证书。

29.5.1 在 Sentinel 与 Identity Manager 引擎 /Remote Loader 之间启用 SSL

1 要创建新证书，请完成以下步骤：

1a 登录到 iManager。

1b 单击 **NetIQ 证书服务器** > **创建服务器证书**。

1c 选择相应的服务器。

1d 指定服务器的绰号。

1e 接受其余的证书默认值。

2 要将服务器证书导出为 .pfx 格式，请完成以下步骤：

2a 在 iManager 中，选择**目录管理** > **修改对象**。

2b 浏览到关键材料对象 (KMO) 对象并选择该对象。

2c 单击**证书** > **导出**。

2d 指定口令。

2e 将服务器证书另存为 PKCS#12。例如， certificate.pfx。

3 使用以下命令将导出的证书中的私用密钥提取到 dxipkey.pem。

openssl pkcs12 -in certificate.pfx -nocerts -out dxipkey.pem –nodes

4 将证书提取到 dxicert.pem 文件。

openssl pkcs12 -in certificate.pfx -nokeys -out dxicert.pem

5 要将步骤 1 中创建的 eDirectory 服务器 CA 证书导出为 Base64 格式，请完成以下步骤：

5a 在 iManager 中，浏览到**角色和任务** > **NetIQ 证书访问** > **用户证书**。

5b 浏览并选择创建的证书。

5c 单击**导出**。

5d 从下拉菜单中选择 **OU=organizationCA.O=TREENAME** 作为 **CA 证书**。

5e 从下拉菜单中选择 **BASE64 > 导出格式**。

5f 单击**下一步**，然后保存该证书。例如， cacert.b64。

6 使用以下命令将 CA 证书导出到密钥存储区：

keytool -import -alias < 别名 > -file <b64 文件 > -keystore < 密钥存储区文件 > –noprompt

例如：

keytool -import -alias trustedroot -file cacert.b64 -keystore idmKeystore.ks –noprompt

7 要将证书导入到审计连接器的可信证书存储区，请完成以下步骤：

7a 以管理员身份登录到 Sentinel 主界面。

7b 在主 ESM 显示屏幕中，找到审计服务器。

7c 右键单击**审计服务器**，然后单击**编辑**。

7d 在 “ 安全性 ” 选项卡中，选择**严格**。

注释：该选项默认配置为使用**开放** （不安全）模式，以允许初始连接。但是，当您在生产环境中使用它时，请务必将模式设置为**严格**。

7e 单击**导入**，然后浏览到您在步骤 6 中创建的证书。例如， idmkeystore.ks。

7f 依次单击**打开**和**保存**。

7g 重启动审计服务器。

8 根据您的组件，将步骤 3 和步骤 4 中创建的私用密钥和证书分别复制到以下位置：

组件	Windows 路径
Identity Manager 引擎	C:\NetIQ\idm\NDS\DIBFiles
Remote Loader	Remote Loader 安装目录： C:\NetIQ\idm\RemoteLoader 或 C:\NetIQ\idm\RemoteLoader\64bit 或 C:\NetIQ\idm\RemoteLoader\32bit
.NET Remote Loader	C:\NetIQ\idm\RemoteLoader.NET
扇出代理	C:\NetIQ\idm\FanoutAgent

9 重启动 Identity Manager 服务。

29.5.2 在 Sentinel 与 User Application 之间启用 SSL

1 要创建新证书，请完成以下步骤：
   - 1a 登录到 iManager。
   - 1b 单击 **NetIQ 证书服务器** > **创建用户证书**。
   - 1c 选择相应的用户。
   - 1d 为用户指定绰号。
   - 1e 在**创建方法**中选择**自定义**。
   - 1f 接受其余的证书默认值。
   - 1g 单击**下一步**。
   - 1h 在**自定义扩展**中选择**新建 DER 编码的扩展**。
   - 1i 浏览到 \products\UserApplication\ext.der 自定义扩展。
   - 1j （可选）指定电子邮件地址。
   - 1k 查看证书参数，然后单击**完成**。
2 要导出用户证书，请完成以下步骤：
   - 2a 单击 **NetIQ 证书访问** > **用户证书**。
   - 2b 选择在步骤 1 中导入的用户证书。
   - 2c 选择有效的用户证书，然后单击**导出**。
   - 2d 指定口令。
   - 2e 将用户证书另存为 PKCS12。例如， certificate.pfx。
3 使用以下命令将导出的证书中的私用密钥提取到 key.pem 文件。

   openssl pkcs12 -in certificate.pfx -nocerts -out key.pem –nodes
4 将证书提取到 cert.pem 文件。

   openssl pkcs12 -in certificate.pfx -nokeys -out cert.pem

5 停止 User Application。

6 将私用密钥和证书添加到 configupdate 实用程序。

6a 打开 configupdate 实用程序。

6b 单击**显示高级选项**。

6c 在 **NetIQ Sentinel 数字签名证书**字段中，复制 cert.pem。

6d 在 **NetIQ Sentinel 数字签名私用密钥**字段中，浏览到私用密钥 (key.pem) 的提取位置，然后导入密钥。

6e 保存在 configupdate 实用程序中所作的更改。

7 重启动 User Application。

8 要将步骤 1 中创建的 eDirectory 服务器 CA 证书导出为 Base64 格式，请完成以下步骤：

8a 在 iManager 中，浏览到**角色和任务** > **NetIQ 证书访问** > **用户证书**。

8b 选择创建的证书。

8c 单击**导出**并清除 " 导出私用密钥 " 复选框。

8d 从下拉菜单中选择 **BASE64 > 导出格式**。

8e 单击**下一步**，然后保存该证书。例如， cacert.b64。

9 使用以下命令将 CA 证书导出到密钥存储区：

```
keytool -import -alias <alias name> -file cacert.b64 -keystore <keystore file> –noprompt
```

例如：

```
keytool -import -alias trustedroot -file cacert.b64 -keystore idmKeystore.ks –noprompt
```

10 要将证书导入到审计连接器的可信证书存储区，请完成以下步骤：

10a 以管理员身份登录到 Sentinel 主界面。

10b 在主 ESM 显示屏幕中，找到审计服务器。

10c 右键单击**审计服务器**，然后单击**编辑**。

10d 在**安全性**选项卡中，选择**严格**。

注释：该选项默认配置为使用**开放** （不安全）模式，以允许初始连接。但是，当您在生产环境中使用它时，请务必将模式设置为**严格**。

10e 单击**导入**，然后浏览到您在步骤 9 中创建的证书。例如， idmKeystore.ks。

10f 依次单击**打开**和**保存**。

10g 重启动审计服务器。

11 重启动 User Application。

29.6 更新应用程序服务器的 SSL 设置

需要将托管 Identity Applications 和 Identity Reporting 的应用程序服务器配置为支持 SSL 通讯。本节提供更新 Tomcat 应用程序服务器 （即默认的应用程序服务器）的说明。

1 如果 Tomcat 正在运行，请将它停止。

2 配置 Tomcat 服务器的 SSL 端口。

例如， SSL 的连接器端口为 8543。编辑位于 C:\NetIQ\idm\apps\tomcat\conf 目录中的 server.xml 文件。

```
<Connector port="8543" protocol="HTTP/1.1"
maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS"
keystoreFile="path_to_keystore_file"
keystorePass="keystore_password" />
```

其中：

keystoreFile

指定默认位于 C:\NetIQ\idm\apps\tomcat\conf\userapp.keystore 目录中的 userapp.keystore 文件的路径。

keystorePass

指定 userapp.keystore 文件的口令。

另外，请将 redirectPort 属性更新为 8543 并保存 server.xml。

3 导航到 Tomcat 的 conf 目录 （默认为 C:\NetIQ\idm\apps\tomcat\conf）。

4 确保 conf 目录中包含密钥存储区文件。例如， idmapps.keystore。

如果您要在执行此过程之后再创建密钥存储区文件，请务必使用在此过程中提供的相同文件名。有关详细信息，请参见第 29.2 节 “ 创建密钥存储区和证书签名请求 ” （第 295 页）。

5 在文本编辑器中打开 conf 目录中的 server.xml 文件。

6 在 server.xml 文件中添加以下内容：

```
<Connector port="port_number" protocol="HTTP/1.1" maxThreads="150"
SSLEnabled="true" scheme="https" secure="true" clientAuth="false"
sslProtocol="TLS" keystoreFile="path_to_file/filename.keystore"
keystorePass="password"
```

例如：

```
<Connector port="8543" protocol="HTTP/1.1" maxThreads="150" SSLEnabled="true"
scheme="https" secure="true" clientAuth="false" sslProtocol="TLS"
keystoreFile="C:\NetIQ\idm\apps\tomcat\conf\idmapps.keystore"
keystorePass="encrypted_password"
```

NetIQ 建议您在 keystorePass 中指定加密口令，而不要提供明文口令。有关在 SSL 通讯中使用明文口令和加密口令的详细信息，请参见 “Securing Tomcat” （保护 Tomcat）。

7 启动 Tomcat。

29.7 在配置实用程序中更新 SSL 设置

安装 Identity Applications 和 Identity Reporting 时，您应该指定 *https* 作为通讯方法。例如，*协议（第 185 页）*。但在安装后，您可以使用 RBPM 配置实用程序来确保应用程序使用 SSL 进行通讯。有关这些参数的详细信息，请参见第 15.8 章 “ 配置 Identity Applications 的设置 ” （第 204 页）。

1 使用 services.msc 文件停止 Tomcat。

2 导航到默认位于 Identity Applications 安装目录中的 RBPM 配置实用程序。例如 C:\NetIQ\idm\apps\UserApplication。

3 在命令提示符下，运行配置实用程序 (configupdate.bat)：

注释：您可能需要等待几分钟，让实用程序启动。

4 （视情况而定）如果您在 configupdate 实用程序中配置了 SSL，请导航到**鉴定**选项卡，并替换 **SSO 客户端**选项卡中提到的所有引用。

```
https://<IP address>:<SSL Port number>
```

例如：

```
https://192.168.0.1:8543
```

5 单击**鉴定**，然后修改以下设置：

OAuth 服务器 TCP 端口

指定鉴定服务器的端口。

例如：8543

OAuth 服务器正在使用 TLS/SSL

指定您希望鉴定服务器使用 TLS/SSL 协议进行通讯。

可选 TLS/SSL 密钥存储区文件

指定包含鉴定服务器可信证书的 Java JKS 密钥存储区文件的路径和文件名。当鉴定服务器使用 TLS/SSL 协议，并且鉴定服务器的可信证书不在 JRE 可信证书存储区 (cacerts) 中时，将应用此参数。

可选 TLS/SSL 密钥存储区口令

指定用于装载 TLS/SSL 鉴定服务器的密钥存储区文件的口令。

OAuth 密钥存储区文件

指定要用于鉴定的 Java JKS 密钥存储区文件的路径。该密钥存储区文件必须至少包含一个公共 / 私用密钥对。

OAuth 密钥存储区文件口令

指定用于装载 OAuth 密钥存储区文件的口令。

OAuth 使用的密钥的密钥别名

指定要用于生成对称密钥的 OSP 密钥存储区文件中的公共 / 私用密钥对名称。

OAuth 使用的密钥口令密钥

指定鉴定服务器使用的私用密钥的口令。

6 单击 **SSO 客户端**。

7 更新所有 URL 设置，例如**登录页的 URL 链接**和 **OAuth 重定向 URL**。

这些设置指定鉴定服务器完成鉴定后要将浏览器客户端重定向到的绝对 URL。

使用以下格式：https://DNS_name:sslport/path。例如， https:/nqserver.testsite:8543/landing/com.netiq.test。

8 保存在配置实用程序中所作的更改。

9 使用 services.msc 文件启动 Tomcat。

29.8 更新 Self Service Password Reset 的 SSL 设置

要修改 SSPR 的 SSL 设置，您必须登录该应用程序。

1 在浏览器中，输入您在配置实用程序中为登录页指定的 https URL。例如：https://myserver.host:8543/landing。

2 使用 Identity Applications 的管理员身份凭证进行登录。

   应用程序会显示一条警告，指出您需要更改重定向白名单 URL。

3 要更改重定向白名单 URL，请遵循页面上的说明操作。

4 浏览到**设置 > OAuth SSO**。

5 对于所有三个 URL，指定 https 协议和端口。

6 浏览到**设置 > 应用程序**。

7 对于所有三个 URL，指定 https 协议和端口。

8 单击**保存**，然后单击**确定**。

9 校验 Identity Applications 的所有 URL 现在是否都使用了 https 协议。

查错提示

更新 SSPR 的 SSL 设置后，如果您无法访问 SSPR 登录页，请遵循以下步骤在 SSPRConfiguration.xml 文件中更新所需的 URL。

1 导航到位于以下路径的 SSPRConfiguration.xml 文件：

```
C:\NetIQ\idm\apps\sspr\sspr_data
```

2 使用相应的 IP 地址和端口号更新所有 URL。

```
https://<IP address>:<SSL Port number>
```

   示例：

```
https://192.168.0.1:8543
```

30 安装后任务

安装 Identity Manager 之后，应配置所安装的驱动程序，以符合业务过程定义的策略和要求。您还需要配置 Sentinel Log Management for IGA 以收集审计事件。安装后的任务通常包括下列项目：

30.1 配置已连接系统

Identity Manager 支持应用程序、目录和数据库共享信息。有关特定于驱动程序的配置说明，请参见 Identity Manager 驱动程序文档。

30.2 创建和配置驱动程序集

驱动程序集是一个可容纳多个 Identity Manager 驱动程序的容器。在任何时候，一台服务器上只能有一个驱动程序集处于活动状态。您可以使用 Designer 工具来创建驱动程序集。

要支持将口令同步到身份库的功能， Identity Manager 需要驱动程序集具有口令策略。您可以使用 Identity Manager 中的默认通用口令策略包，也可以根据现有的组织要求创建口令策略。不过，口令策略必须包括 DirMXL-PasswordPolicy 对象。如果身份库中不存在该策略对象，您可以创建该对象。

30.2.1 创建驱动程序集

Designer for Identity Manager 提供了许多设置供您创建和配置驱动程序集。这些设置可让您指定全局配置值、驱动程序集包、驱动程序集已命名口令、日志级别、跟踪级别和 Java 环境参数。有关详细信息，请参见《*NetIQ Designer for Identity Manager Administration Guide*》（NetIQ Designer for Identity Manager 管理指南）中的 "Configuring Driver Sets"（配置驱动程序集）。

30.2.2 将默认口令策略指派给驱动程序集

必须将 DirMXL-PasswordPolicy 对象指派给身份库中的每个驱动程序集。 Identity Manager 默认通用口令策略包包括此策略对象。默认策略会安装并指派通用口令策略，以控制 Identity Manager 引擎自动为驱动程序生成随机口令的方式。

或者，若要使用自定义口令策略，您必须创建口令策略对象和策略。有关详细信息，请参见第 30.2.3 节 " 在身份库中创建口令策略对象 "（第 308 页）和第 30.2.4 节 " 创建自定义口令策略 "（第 309 页）。

1 在 Designer 中打开您的项目。
2 在 " 概要 " 窗格中，展开您的项目。
3 展开**包编目 > 通用**以校验默认通用口令策略包是否存在。
4 （视情况而定）如果口令策略包尚未在 Designer 中列出，请完成以下步骤：
   - **4a** 右键单击**包编目**。
   - **4b** 选择**导入包**。
   - **4c** 选择 **Identity Manager 默认通用口令策略**，然后单击**确定**。

     为了确保表格中显示所有可用的包，您可能需要取消选择**只显示基础包**。
5 选择每个驱动程序集并指派口令策略。

30.2.3 在身份库中创建口令策略对象

如果身份库中不存在 DirMXL-PasswordPolicy 对象，您可以使用 Designer 或 ldapmodify 实用程序创建该对象。有关如何在 Designer 中创建此对象的详细信息，请参见 《*NetIQ Designer for Identity Manager Administration Guide*》（NetIQ Designer for Identity Manager 管理指南）中的 "Configuring Driver Sets"（配置驱动程序集）。要使用 ldapmodify 实用程序，请执行以下过程：

1 在文本编辑器中创建具有以下属性的 LDAP 数据交换格式 (LDIF) 文件：

```
dn: cn=DirXML-PasswordPolicy,cn=Password Policies,cn=Security
changetype: add
nsimPwdRuleEnforcement: FALSE
nspmSpecialAsLastCharacter: TRUE
nspmSpecialAsFirstCharacter: TRUE
nspmSpecialCharactersAllowed: TRUE
nspmNumericAsLastCharacter: TRUE
nspmNumericAsFirstCharacter: TRUE
nspmNumericCharactersAllowed: TRUE
nspmMaximumLength: 64
nspmConfigurationOptions: 596
passwordUniqueRequired: FALSE
passwordMinimumLength: 1
passwordAllowChange: TRUE
objectClass: nspmPasswordPolicy

dn: cn=DirXML-PasswordPolicy,cn=Password Policies,cn=Security
changetype: modify
add: nsimAssignments
nsimAssignments: <driverset LDAP dn>
```

注释：按原样复制该内容可能会在该文件中插入隐藏的特殊字符。如果在将这些属性添加到身份库时收到 ldif_record() = 17 错误讯息，请在两个 DN 之间额外插入一个空格。

2 要在身份库中添加 DirMXL-PasswordPolicy 对象，请从 Identity Manager 安装包的 install/utilities 目录运行 ldapmodify.exe，从文件中导入属性。

30.2.4 创建自定义口令策略

您可以不使用 Identity Manager 中的默认口令策略，而是根据您组织的需要创建新的策略。口令策略可以指派给整个树结构、分区根容器、容器或特定的用户。为简化管理， NetIQ 建议在树中尽可能高的位置指派口令策略。有关详细信息，请参见《*Password Management 3.3.2 Administration Guide*》（Password Management 3.3.2 管理指南）中的 "Creating Password Policies"（创建口令策略）。

注释：您还必须将 DirXML-PasswordPolicy 对象指派给驱动程序集。有关详细信息，请参见第 30.2.3 节 " 在身份库中创建口令策略对象 "（第 308 页）。

30.2.5 在身份库中创建默认通知集合对象

默认通知集合是一个身份库对象，它包含一套电子邮件通知模板，以及一个用于发送基于模板生成的电子邮件的 SMTP 服务器。如果身份库中不存在默认通知集合对象，请使用 Designer 创建该对象。

1 在 Designer 中打开您的项目。
2 在 " 概要 " 窗格中，展开您的项目。
3 右键单击身份库，然后单击身份库**属性**。
4 单击**包**，然后单击**添加包**图标。
5 选择所有通知模板包，然后单击**确定**。
6 单击**应用**以通过**安装**操作来安装包。
7 将通知模板部署到身份库。

30.3 创建驱动程序

要创建驱动程序，请使用 Designer 中提供的包管理功能。对于您打算使用的每个 Identity Manager 驱动程序，创建一个驱动程序对象，并导入驱动程序配置。驱动程序对象中包含该驱动程序的配置参数和策略。在创建驱动程序对象的过程中，安装驱动程序包，然后根据您环境的需求修改驱动程序配置。

驱动程序包包含默认策略集。在实施数据共享模型时，这些策略可以帮您顺利开始工作。在大多数时候，需要使用附带的默认配置文件设置驱动程序，然后根据环境要求修改驱动程序配置文件。创建并配置驱动程序后将其部署到身份库并加以启动。通常情况下，驱动程序创建过程涉及以下操作：

1. 导入驱动程序包
2. 安装驱动程序包
3. 配置驱动程序对象
4. 部署驱动程序对象
5. 启动驱动程序对象

有关其他信息和特定于驱动程序的信息，请参见 Identity Manager 驱动程序网站上的相关驱动程序实施指南。

30.4 定义策略

可以使用策略在特定环境中自定义流入、流出 Identity Vault 的信息流。例如，某个公司可能使用 inetorgperson 作为主用户类，而另一个公司则可能使用 User。为了处理这种情况，系统会创建策略以告知 Identity Manager 引擎一个用户在各个系统中的名称。只要在已连接系统间传递对用户产生影响的操作， Identity Manager 都将应用策略以进行上述更改。

也可利用策略创建新对象、更新特性值、执行纲要转换、定义匹配准则、维护 Identity Manager 关联以及执行其他许多操作。

NetIQ 建议使用 Designer 定义驱动程序策略，以满足您的业务需求。有关详细的策略指南，请参见《*NetIQ Identity Manager - Using Designer to Create Policies*》（NetIQ Identity Manager - 使用 Designer 创建策略）指南和 《*NetIQ Identity Manager Understanding Policies Guide*》（NetIQ Identity Manager 了解策略指南）。有关 Identity Manager 使用的文档类型定义 (DTD) 的信息，请参见 《Identity Manager DTD Reference》（Identity Manager DTD 参考手册）。这些资源包含：

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

30.5 管理驱动程序活动

要执行 Identity Manager 驱动程序的管理和配置功能，请使用 Designer 或 iManager。《*NetIQ Identity Manager Driver Administration Guide*》（NetIQ Identity Manager 驱动程序管理指南）中对这些功能进行了详细说明。

30.6 激活 Identity Manager

当您首次登录时，有些 Identity Manager 组件会自动激活。其他组件则需要通过执行某个过程才能激活。

30.6.1 安装产品激活身份凭证

NetIQ 建议您使用 iManager 来安装产品激活身份凭证。

注释：对于要使用的每个驱动程序，请激活包含驱动程序的驱动程序集。可以使用身份凭证激活所有树。

1 在您购买许可证之后， NetIQ 会向您发送一封电子邮件，其中包含您的客户 ID。在该电子邮件的 " 订单细节 " 部分下方，还包含一个链接，指向可获得您的身份凭证的站点。单击该链接可转至该站点。

2 单击许可证下载链接，然后完成以下操作之一：
   - 打开产品激活身份凭证文件，然后将其内容复制到剪贴板。
   - 保存产品激活身份凭证文件。
   - 如果选择复制内容，请不要包含任何多余的行或空格。您应从身份凭证的第一个破折号 (-) 开始复制 (----BEGIN PRODUCT ACTIVATION CREDENTIAL)，一直复制到身份凭证的最后一个破折号 (-) (END PRODUCT ACTIVATION CREDENTIAL-----)。

3 登录到 iManager。

4 选择 **Identity Manager > Identity Manager 概述**。

5 要在树型结构中选择一个驱动程序集，请单击浏览图标 ()。

6 在 **Identity Manager 概述**页面上，单击包含要激活的驱动程序的驱动程序集。

7 在**驱动程序集概述**页面上，单击**激活** > **安装**。

8 选择要激活 Identity Manager 组件的驱动程序集，然后单击**下一步**。

9 （视情况而定）如果您之前保存了产品激活身份凭证文件，请指定保存的位置。

10 （视情况而定）如果您之前复制了产品激活身份凭证文件的内容，请将这些内容粘贴到文本区域中。

11 单击**下一步**。

12 单击**完成**。

注释：应用包版本激活码后， Identity Manager 不显示正确的 Identity Manager 版本。

30.6.2 查看 Identity Manager 和驱动程序的产品激活

对于每个驱动程序集，您都可以查看为 Identity Manager 引擎服务器和 Identity Manager 驱动程序安装的产品激活身份凭证。您还可以去除激活身份凭证。

注释：为驱动程序集安装了有效的产品激活身份凭证后，驱动程序名称的旁边可能仍然会显示 " 要求激活 "。如果出现这种情况，请重启动驱动程序。该讯息应该即会消失。

1 登录到 iManager。

2 单击 **Identity Manager** > **Identity Manager 概述**。

3 要在树型结构中选择一个驱动程序集，请使用浏览图标 () 和搜索图标 ()。

4 在 **Identity Manager 概述**页面上，单击要查看其激活信息的驱动程序集。

5 在**驱动程序集概述**页面上，单击**激活 > 信息**。

   可以查看激活身份凭证的文本，或者，如果报告了错误，则可以去除激活身份凭证。

30.6.3 激活 Identity Manager 驱动程序

激活 Identity Manager 引擎时，同时会激活以下驱动程序：

服务驱动程序	通用驱动程序
数据收集服务	Active Directory
ID 提供程序	eDirectory 的双向驱动程序
受管系统网关	eDirectory
Role and Resource Service	GroupWise 2014
User Application	LDAP
	Lotus Notes

要激活其他 Identity Manager 驱动程序，您必须另外购买 Identity Manager 集成模块，其中可能包含一或多个驱动程序。您每购买一个 Identity Manager 集成模块，就会收到一个产品激活身份凭证。在收到身份凭证后，请执行第 30.6.1 节 " 安装产品激活身份凭证 "（第 310 页）中所列的过程。有关驱动程序的详细信息，请参见 Identity Manager 驱动程序文档网站。

30.6.4 激活特定的 Identity Manager 组件

本节提供有关激活 Identity Manager 特定组件的信息。

- 激活 Designer （第 312 页）
- 激活 Analyzer （第 312 页）

激活 Designer

激活 Identity Manager 引擎或 Identity Manager 驱动程序的同时，还会激活 Designer。

激活 Analyzer

当您起动未获许可的 Analyzer 透视功能时， Analyzer 会打开激活页面，您可以从中管理 Analyzer 许可证。

注释：如果关闭 " 激活 " 对话框， Analyzer 将一直保持锁定状态，直到您提供许可证将它激活。当您准备好添加许可证时，请在项目视图中单击**激活 Analyzer** 打开 " 激活 " 对话框。

1 起动 Analyzer。
2 在 **Analyzer 激活**窗口中，您可以添加新许可证，或访问 Customer Center 以获得许可证。
3 （视情况而定）要添加新许可证，请执行以下操作：
   3a 单击**添加新许可证**。
   3b 在**许可证**窗口中，键入您从 NetIQ 客户关怀入口下载的激活代码，然后单击**确定**。

4 （视情况而定）要访问 Customer Center 以获得许可证，请执行以下操作：

   4a 单击**访问 Customer Center 以获得许可证**。

   4b 单击**访问 Micro Focus Customer Center**。

   4c 浏览到 Analyzer 许可证并加以选择。

   4d 复制激活代码，然后关闭客户关怀入口。

   4e 在**许可证**窗口中键入激活代码，然后单击**确定**。

5 在 **Analyzer 激活**窗口中，查看您刚刚安装的许可证的细节。

6 单击**确定**开始使用 Analyzer。

IX 升级 Identity Manager

本部分提供有关升级 Identity Manager 组件的信息。要将现有数据迁移到新服务器，请参见第 X 部分 “ 将 Identity Manager 数据迁移到新安装 ”（第 351 页）。有关升级与迁移之间区别的详细信息，请参见第 31.2 节 “ 了解升级和迁移 ”（第 319 页）。

31 准备升级 Identity Manager

本章提供的信息可帮助您准备好将 Identity Manager 解决方案升级到最新版本。您可以根据目标计算机，使用可执行文件、二进制文件或文本模式升级 Identity Manager 的大部分组件。要执行升级，您必须下载并解压缩或解包 Identity Manager 安装包。

31.1 Identity Manager 的升级核对清单

要执行升级， NetIQ 建议您完成以下核对清单中的步骤。

	核对清单项目
❑	1. 查看升级与迁移之间的区别。有关详细信息，请参见第 31.2 节 “ 了解升级和迁移 ”（第 319 页）。
❑	2. 升级到 Identity Manager 4.5.6。您无法将低于 4.5.6 的版本升级或迁移到 4.7 版本。有关详细信息，请参见 《NetIQ Identity Manager 4.5 安装指南》。
❑	3. 确保拥有最新的安装包用于升级 Identity Manager。请参见 第 5.5 节 “ 下载安装文件 ”（第 43 页）。
❑	4. 了解 Identity Manager 各组件之间的交互。有关详细信息，请参见第 I 部分 “ 简介 ” （第 17 页）。
❑	5. 确保您的计算机符合较新版 Identity Manager 的硬件和软件先决条件。有关详细信息，请参见第 6 章 “ 安装注意事项 ”（第 45 页）和要升级的目标版本的 《发行说明》。
❑	6. 备份当前的项目、驱动程序配置和数据库。有关详细信息，请参见第 31.5 节 “ 备份当前配置 ”（第 323 页）。
❑	7. 将 Designer 升级到最新版本。有关详细信息，请参见第 32.1 节 “ 升级 Designer” （第 327 页）。
❑	8. 安装最新版本的 iManager，或将 iManager 升级到最新版本的 Identity Manager。有关详细信息，请参见以下章节之一： ◆ **安装**：安装 iManager （第 125 页） ◆ **升级**：升级 iManager （第 328 页）

	核对清单项目
❑	9. 在运行 Identity Manager 的服务器上，将 eDirectory 升级到最新版本和增补程序。 如果在已升级最新的 64 位 Remote Loader 的环境中升级 eDirectory 9.0 或更高版本，eDirectory 安装会失败，并且 Remote Loader 会停止工作。为了确保 Remote Loader 正常工作，请先执行以下步骤再升级 eDirectory： 1. 停止 Remote Loader 及其实例。 2. 卸装 novell-DXMLopensslx RPM。 3. 安装 eDirectory 9.1 或更高版本。 升级 eDirectory 会停止 ndsd，而后者又会停止所有驱动程序。有关详细信息，请参见《*NetIQ eDirectory Installation Guide*》（NetIQ eDirectory 安装指南）。
❑	10. 更新 iManager 插件，使之与 iManager 的版本匹配。有关详细信息，请参见第 32.2.4 节 " 在升级或重安装后更新 iManager 插件 "（第 331 页）。
❑	11. 停止与安装了 Identity Manager 引擎的服务器关联的驱动程序。有关详细信息，请参见第 9.4.1 节 " 停止驱动程序 "（第 81 页）。
❑	12. 升级 Identity Manager 引擎。有关详细信息，请参见第 32.4 节 " 升级 Identity Manager 引擎 "（第 332 页）。 **注释：**如果要将 Identity Manager 引擎迁移到新服务器，可以使用与当前 Identity Manager 服务器上相同的 eDirectory 复本。有关详细信息，请参见第 35.4 节 " 将 Identity Manager 引擎迁移到新服务器 "（第 358 页）。
❑	13. （视情况而定）如果 Identity Manager 引擎的驱动程序集中有任何驱动程序是 Remote Loader 驱动程序，请升级每个驱动程序的 Remote Loader 服务器。有关详细信息，请参见第 32.3 节 " 升级 Remote Loader"（第 331 页）。
❑	14. （视情况而定）如果您使用的是包，请在现有驱动程序上升级包以获取新策略。有关详细信息，请参见第 32.8 节 " 升级 Identity Manager 驱动程序 "（第 343 页）。 只有在以下情况下才需要升级该驱动程序：有较新版本的包可用，且要添加到现有驱动程序的驱动程序策略中包括新功能。
❑	15. （视情况而定）如果未安装 OSP，请加以安装。有关详细信息，请参见第 13 部分 " 安装单点登录组件 "（第 149 页）。
❑	16. （视情况而定）如果未安装 SSPR，请加以安装。有关详细信息，请参见第 14 部分 " 安装口令管理组件 "（第 155 页）。 **注释：**如果您当前使用的是旧式口令管理提供程序，请安装 SSPR。有关详细信息，请参见第 4.4.2 节 " 了解旧式口令管理提供程序 "（第 32 页）。
❑	17. 使用升级程序升级 User Application、 Identity Manager 仪表板、 OSP、 SSPR 和 Identity Reporting。有关详细信息，请参见第 32.5 节 " 升级 Identity Applications 和 Identity Reporting"（第 332 页）。 或者，您也可手动升级这些组件。有关详细信息，请参见第 X 部分 " 将 Identity Manager 数据迁移到新安装 "（第 351 页）。
❑	18. 升级 Identity Reporting 和关联的驱动程序。有关详细信息，请参见第 32.6 节 " 升级 Identity Reporting"（第 341 页）。
❑	19. 启动与 Identity Applications 和 Identity Manager 引擎关联的驱动程序。有关详细信息，请参见第 9.4.2 节 " 启动驱动程序 "（第 82 页）。

	核对清单项目
❑	20. （视情况而定）如果已将 Identity Manager 引擎或 Identity Applications 迁移到某个新服务器，请将该新服务器添加到驱动程序集中。有关详细信息，请参见第 32.9 节 " 将新服务器添加到驱动程序集 " （第 345 页）。
❑	21. （视情况而定）如果您有自定义策略和规则，请恢复自定义设置。有关详细信息，请参见第 32.10 节 " 将自定义策略和规则恢复到驱动程序 " （第 346 页）。
❑	22. 激活已升级的 Identity Manager 解决方案。有关详细信息，请参见第 30.6 节 " 激活 Identity Manager" （第 310 页）。

31.2 了解升级和迁移

当您想要安装现有 Identity Manager 安装的较新版本时，通常可以执行**升级**。但是，如果新版 Identity Manager 不提供现有数据的升级路径，则您必须执行迁移。 NetIQ 将**迁移**定义为在新服务器上安装 Identity Manager，然后将现有数据迁移到这个新服务器的过程。

在产品评估期或者在激活 Advanced Edition 之后，如果您不想在环境中使用 Advanced Edition 功能，可以**切换**到 Standard Edition。Identity Manager 可让您通过一个简单的过程从 Advanced Edition 切换到 Standard Edition。

从 Advanced Edition 切换到 Standard Edition

Identity Manager 允许您在产品评估期内或激活 Advanced Edition 后从 Advanced Edition 切换到 Standard Edition。

重要：如果您已应用 Advanced Edition 激活码，则不需要切换到 Standard Edition，因为 Standard Edition 的所有功能在 Advanced Edition 中都有提供。仅当您不想在环境中使用任何 Advanced Edition 功能，并且想要缩减 Identity Manager 部署时，才必须切换到 Standard Edition。有关详细信息，请参见 从 Advanced Edition 切换到 Standard Edition （第 349 页）。

31.3 升级顺序

必须按以下顺序升级 Identity Manager 组件：

1. Designer
2. iManager
3. Sentinel Log Management for IGA
4. 身份库
5. Identity Manager 引擎 /Remote Loader
6. iManager 插件
7. Tomcat 和 PostgreSQL 组件
8. 单点登录 (One SSO Provider)
9. Self Service Password Reset
10. Identity Applications （适用于 Advanced Edition）

11. Identity Reporting
12. Analyzer

有关最新的受支持升级路径的信息，请参见 Identity Manager 4.6 文档网站中适用于您版本的发行说明。

31.4 支持的升级路径

Identity Manager 4.7 支持从 4.6.x 和 4.5.x 版本升级。NetIQ 建议开始升级前先在您当前版本相应的发行说明中查看该信息。

- 第 31.4.1 节 " 从 Identity Manager 4.6.x 版本升级 " （第 320 页）
- 第 31.4.2 节 " 从 Identity Manager 4.5.x 版本升级 " （第 321 页）

31.4.1 从 Identity Manager 4.6.x 版本升级

下表列出了 Identity Manager 4.6.x 版本的组件范围升级路径：

组件	基础版本	升级后的版本
Identity Manager 引擎	4.6.x	1. 将操作系统升级到支持的版本。 2. 将身份库升级到 9.1。 3. 将 Identity Manager 引擎升级到 4.7。
Remote Loader/ 扇出代理	4.6.x	安装 4.7 版 Remote Loader/ 扇出代理
Designer	4.6.x	1. 安装 Designer 4.7。 2. 将工作空间从 NCP 转换为 LDAP。 Designer 4.7 基于 LDAP 运行。使用此版本之前，请参见 《*NetIQ Identity Manager LDAP Designer 发行说明*》。
Identity Applications	4.6.x	升级 Identity Applications 前，请确保身份库和 Identity Manager 引擎已分别升级到 9.1 和 4.7。 1. 将操作系统升级到支持的版本。 2. 将数据库升级到支持的版本。 3. （视情况而定）如果 SSPR 安装在单独的计算机上，请将该组件升级到 4.7 版本。 4. 更新 User Application 驱动程序以及角色和资源驱动程序包。 5. 将 Identity Applications 升级到 4.7。 6. 停止 Tomcat。

组件	基础版本	升级后的版本
Identity Reporting	4.6.x	1. 将操作系统升级到支持的版本。 2. 将数据库升级到支持的版本。 3. 升级 SLM for IGA。 4. 更新数据收集服务和受管理服务网关驱动程序包。 5. 安装 Identity Reporting 4.7。 6. 从 Identity Manager 的 " 数据收集服务 " 页面创建数据同步策略。

NetIQ 建议开始升级前先在您所用版本的发行说明中查看该信息：

- 《NetIQ Identity Manager 4.6 Service Pack 2 Release Notes》（NetIQ Identity Manager 4.5 SP4 发行说明）
- 《NetIQ Identity Manager 4.6 Service Pack 1 Release Notes》（NetIQ Identity Manager 4.5 SP4 发行说明）
- 《NetIQ Identity Manager 4.6 发行说明》

31.4.2 从 Identity Manager 4.5.x 版本升级

下表列出了 Identity Manager 4.5.x 版本的组件范围升级路径：

组件	基础版本	中间步骤	升级后的版本
Identity Manager 引擎	装有 eDirectory 8.8.8.x （其中 x 为 3 至 9）的 Identity Manager 4.5.x （其中 x 为 0 至 5）	应用 4.5.6 增补程序	1. 将操作系统升级到支持的版本。 2. 将身份库升级到 9.1。 3. 将 Identity Manager 引擎升级到 4.7。
Remote Loader/ 扇出代理	4.5.x （其中 x 为 0 至 5）	应用 4.5.6 增补程序	安装 4.7 版 Remote Loader/ 扇出代理。
Designer	4.5.x （其中 x 为 0 至 5）	应用 4.5.6 增补程序	1. 安装 Designer 4.7。 2. 将工作空间从 NCP 转换为 LDAP。 Designer 4.7 基于 LDAP 运行。使用此版本之前，请参见 《*NetIQ Identity Manager LDAP Designer 发行说明*》。

组件	基础版本	中间步骤	升级后的版本
Identity Applications	4.5.x （其中 x 为 0 至 5）	◆ 如果您使用的是 JBoss 或 Websphere，请迁移到 Tomcat 应用程序服务器。 ◆ 应用 4.5.6 增补程序。	升级 Identity Applications 前，请确保身份库和 Identity Manager 引擎已分别升级到 9.1 和 4.7。 1. 将操作系统升级到支持的版本。 2. 更新 User Application 驱动程序以及角色和资源驱动程序包。 3. 将数据库升级到支持的版本。 4. （视情况而定）如果 SSPR 安装在单独的计算机上，请将该组件升级到 4.7 版本。 5. 将 Identity Applications 升级到 4.7。 6. 停止 Tomcat。
Identity Reporting	4.5.x （其中 x 为 0 至 5）	◆ 如果您使用的是 JBoss 或 Websphere，请迁移到 Tomcat 应用程序服务器。 ◆ 应用 4.5.6 增补程序。	1. 将操作系统升级到支持的版本。 2. 将数据库升级到支持的版本。 3. 将事件审计服务数据迁移到支持版本的 PostgreSQL 或 Oracle 数据库。 4. 安装 SLM for IGA。 5. 更新数据收集服务和受管理服务网关驱动程序包。 6. 安装 Identity Reporting 4.7。 7. 从 IDMDCS 页面创建数据同步策略。

NetIQ 建议开始升级前先在您所用版本的发行说明中查看该信息：

- 《NetIQ Identity Manager 4.5 Service Pack 6 Release Notes》（NetIQ Identity Manager 4.5 SP4 发行说明）
- 《NetIQ Identity Manager 4.5 Service Pack 5 Release Notes》（NetIQ Identity Manager 4.5 SP5 发行说明）
- 《NetIQ Identity Manager 4.5 Service Pack 4 Release Notes》（NetIQ Identity Manager 4.5 SP4 发行说明）
- 《NetIQ Identity Manager 4.5 Service Pack 3 Release Notes》（NetIQ Identity Manager 4.5 SP4 发行说明）
- 《NetIQ Identity Manager 4.5 Service Pack 2 Release Notes》（NetIQ Identity Manager 4.5 SP4 发行说明）
- 《NetIQ Identity Manager 4.5 Service Pack 1 Release Notes》（NetIQ Identity Manager 4.5 SP4 发行说明）
- NetIQ Identity Manager 4.5 发行说明

31.5 备份当前配置

在升级之前， NetIQ 建议您先备份 Identity Manager 解决方案的当前配置。您无需再执行其他步骤即可备份 User Application。所有 User Application 配置均储存在 User Application 驱动程序中。您可以通过以下方式创建备份：

- 第 31.5.1 节 " 导出 Designer 项目 " （第 323 页）
- 第 31.5.2 节 " 导出驱动程序的配置 " （第 324 页）

31.5.1 导出 Designer 项目

Designer 项目包含纲要及所有驱动程序配置信息。通过创建 Identity Manager 解决方案项目，您可以一步导出所有驱动程序，而无需为每个驱动程序创建单独的导出文件。

- 导出当前项目 （第 323 页）
- 通过身份库创建新项目 （第 323 页）

导出当前项目

如果已具有 Designer 项目，请校验项目中的信息是否与身份库中的信息同步。

1. 在 Designer 中，打开项目。
2. 在建模器中，右键单击身份库，然后选择**在线 > 比较**。
3. 评估项目并协调所有差异，然后单击**确定**。

   有关详细信息，请参见 《*NetIQ Designer for Identity Manager Administration Guide*》（NetIQ Designer for Identity Manager 管理指南）中的 "Using the Compare Feature When Deploying" （部署时使用比较功能）。
4. 在工具栏上，选择**项目 > 导出**。
5. 单击**全选**以选择导出所有资源。
6. 选择保存项目的位置和格式，然后单击**完成**。

   将项目保存在当前工作空间以外的任何位置。升级到 Designer 时，必须创建一个新的工作空间位置。有关详细信息，请参见 《*NetIQ Designer for Identity Manager Administration Guide*》（NetIQ Designer for Identity Manager 管理指南）中的 "Exporting a Project" （导出项目）。

通过身份库创建新项目

如果当前 Identity Manager 解决方案没有 Designer 项目，则必须创建一个项目以备份当前解决方案。

1. 安装 Designer。
2. 起动 Designer，然后指定工作空间的位置。
3. 选择是否要查找联机更新，然后单击**确定**。
4. 在 " 欢迎 " 页面上，单击**运行 Designer**。
5. 在工具栏上，选择**项目 > 导入项目 > 身份库**。
6. 指定项目的名称，然后对项目使用默认位置或选择其他位置。
7. 单击 " 下一步 "。

8 指定以下用于连接身份库的值：
   - **主机名**：表示身份库服务器的 IP 地址或 DNS 名称
   - **用户名**：表示用于鉴定到身份库的用户的 DN
   - **口令**：表示鉴定用户的口令
9 单击 " 下一步 "。
10 使 " 身份库纲要 " 和 " 默认通知集合 " 保留选中状态。
11 展开 " 默认通知集合 "，然后取消选择不需要的语言。

   " 默认通知集合 " 已翻译为许多种不同语言。可导入所有语言，或仅选择您使用的语言。
12 单击浏览，然后浏览到并选择要导入的驱动程序集。
13 对此身份库中的每个驱动程序集重复步骤 12，然后单击完成。
14 在导入项目后单击确定。
15 如果您仅有一个身份库，则已完成。如果您有多个身份库，请继续步骤 16。
16 在工具栏上单击在线 > 导入。
17 对每个附加身份库重复步骤 8 到步骤 14。

31.5.2 导出驱动程序的配置

通过创建驱动程序的导出，可备份当前配置。但是， Designer 当前不会创建基于角色的权利驱动程序和策略的备份。使用 iManager 以校验是否具有基于角色的权利驱动程序的导出。

- 使用 Designer 导出驱动程序配置 （第 324 页）
- 使用 iManager 创建驱动程序的导出 （第 324 页）

使用 Designer 导出驱动程序配置

1 确认 Designer 中的项目具有最新版本的驱动程序。有关详细信息，请参见 《*NetIQ Designer for Identity Manager Administration Guide*》（NetIQ Designer for Identity Manager 管理指南）中的 "Importing a Library, a Driver Set, or a Driver from the Identity Vault" （从身份库导入库、驱动程序集或驱动程序）
2 在建模器中，右键单击要升级的驱动程序所对应的行。
3 选择导出到配置文件。
4 浏览到保存配置文件的位置，然后单击保存。
5 在结果页面上单击确定。
6 对每个驱动程序重复步骤 1 到步骤 5。

使用 iManager 创建驱动程序的导出

1 在 iManager 中，选择 **Identity Manager > Identity Manager 概述**。
2 浏览到并选择树中要搜索驱动程序集对象的位置，然后单击搜索图标 ▶。
3 单击保存要升级的驱动程序的驱动程序集对象。
4 单击要升级的驱动程序，然后单击导出。
5 单击下一步，然后选择导出所有包含的策略，无论是否链接到配置。

6 单击下一步，然后单击另存为。

7 选择保存到磁盘，然后单击确定。

8 单击完成。

9 对每个驱动程序重复步骤 1 到步骤 8。

32 升级 Identity Manager 组件

本章提供有关升级 Identity Manager 各个组件的具体信息。例如，您可能只想将 Designer 升级到最新版本，而不升级 iManager。本章还提供了在执行升级后可能需要执行的步骤。

32.1 升级 Designer

1. 以管理员身份登录到装有 Designer 的服务器。
2. 要创建项目的备份副本，请导出您的项目。

   有关导出的详细信息，请参见 《*NetIQ Designer for Identity Manager Administration Guide*》（NetIQ Designer for Identity Manager 管理指南）中的 “Exporting a Project” （导出项目）。
3. 从 Identity Manager 媒体起动 Designer 安装程序 (\products\Designer\install.exe)
4. 选择安装 Designer 所用的语言，然后阅读并接受许可协议。
5. 指定 Designer 的安装目录，然后在提示已安装 Designer 的讯息中单击**是**。
6. 选择是否在桌面和桌面菜单中放置快捷方式。
7. 查看摘要，然后单击**安装**。
8. 查看 《发行说明》，然后单击**下一步**。
9. 选择起动 Designer，然后单击**完成**。
10. 指定 Designer 工作空间的位置，然后单击**确定**。
11. 在提示需要关闭和转换项目的警告讯息中单击**确定**。
12. 在**项目**视图中，展开项目，然后双击**项目需要转换**。
13. 查看项目转换程序向导执行的步骤，然后单击**下一步**。
14. 指定项目备份的名称，然后单击**下一步**。
15. 查看转换过程的摘要，然后单击**转换**。
16. 转换完成后查看摘要，然后单击**打开**。

升级到最新版本的 Designer 后，您必须从较旧版本导入所有 Designer 项目。当您启动导入过程时，Designer 将运行项目转换程序向导，它会将较早的项目转换为最新版本。在向导中，选择**将项目复制到工作空间中**。有关项目转换程序的详细信息，请参见 *《NetIQ Designer for Identity Manager Administration Guide》*（NetIQ Designer for Identity Manager 管理指南）。

32.2 升级 iManager

通常情况下， iManager 的升级过程会使用 configiman.properties 文件中的现有配置值，例如端口值和授权用户。如果您先前修改了 server.xml 和 context.xml 配置文件， NetIQ 建议您在升级之前先备份这些文件。

如果您使用的是 eDirectory 9.1，请将 iManager 版本升级到 3.1。 iManager 3.1 安装文件位于 <iso_extracted_directory>\products\iManager277\installs\win 目录中。

升级过程包括以下活动：

- 第 32.2.1 节 " 在 Windows 上升级 iManager" （第 328 页）
- 第 32.2.2 节 " 更新基于角色的服务 " （第 330 页）
- 第 32.2.3 节 " 重安装或迁移 Plug-in Studio 的插件 " （第 330 页）
- 第 32.2.4 节 " 在升级或重安装后更新 iManager 插件 " （第 331 页）

32.2.1 在 Windows 上升级 iManager

如果 iManager 服务器的安装程序检测到以前安装的 iManager 版本，可能会提示您升级已安装的版本。如果您选择升级，该程序会将现有的 JRE 和 Tomcat 版本替换为最新版本。此过程还会将 iManager 升级至最新版本。

在升级 iManager 之前，请确保计算机满足各项先决条件和系统要求。有关详细信息，请参见以下资料：

- 更新随附的 《发行说明》。
- 对于 iManager，请参见安装 iManager 服务器的注意事项 （第 128 页）。
- 对于 iManager Workstation，请参见安装 iManager Workstation 的注意事项 （第 128 页）。

注释：升级过程会使用 iManager 先前版本中配置的 HTTP 端口值和 SSL 端口值。

要在 Windows 上安装 iManager 服务器，请执行以下操作：

1. 以具有管理员特权的用户身份登录到要升级 iManager 的计算机。
2. （视情况而定）如果您修改了 server.xml 和 context.xml 配置文件，请在执行升级之前，在其他位置保存这些文件的备份副本。

   升级过程将替换这些配置文件。
3. 在 NetIQ 下载网站上，选择所需的 iManager 版本，然后将 win.zip 文件下载到服务器上的某个目录中。例如：iMan_277_win.zip。
4. 将该 win.zip 文件抽取到 iManager 文件夹中。
5. 运行默认位于 extracted_directory\iManager\installs\win *文件夹中的* iManagerInstall.exe。
6. 在 iManager 欢迎窗口中选择一种语言，然后单击**确定**。

7 在简介窗口中，单击下一步。

8 接受许可协议，然后单击下一步。

9 （可选）要在 iManager 中使用 IPv6 地址，请在启用 IPv6 窗口中单击是。

您可以在升级 iManager 后启用 IPv6 地址。有关详细信息，请参见第 11.3.2 节 " 安装后为 iManager 配置 IPv6 地址 "（第 137 页）。

10 单击下一步。

11 在升级提示符处，选择 " 升级 "。

12 （视情况而定）查看检测摘要窗口中的内容。

检测摘要窗口列出了 iManager 在升级后将使用的最新版 Servlet 容器和 JVM 软件。

13 单击下一步。

14 阅读安装前摘要页面，然后单击安装。

升级过程可能需要几分钟。该过程可能会为 iManager 组件添加新文件或更改 iManager 配置。有关详细信息，请参见升级的 《发行说明》。

15 （视情况而定）如果安装完成窗口显示了以下错误讯息，请完成以下步骤：

```
The installation of iManager version is complete, but some errors occurred
during the install.
Please see the installation log Log file path for details. Press "Done" to quit
the installer.
```

15a 记下错误讯息中显示的日志文件的路径。

15b 在安装完成窗口中单击完成。

15c 打开日志文件。

15d （视情况而定）如果在日志文件中发现以下错误，您可以忽略该错误讯息。安装成功，并且 iManager 正常运行。

```
Custom Action: com.novell.application.iManager.install.InstallDLLs
Status: ERROR
Additional Notes: ERROR - class
com.novell.application.iManager.install.InstallDLLs
NonfatalInstallException C:\WINDOWS\system32\msvcr71.dll (The process
cannot access the file because it is being used by another process)
```

15e （视情况而定）如果日志文件不包含步骤 21d 中所列的错误， NetIQ 建议您重试安装。

16 单击完成。

17 iManager 初始化完成后，单击 " 入门 " 页面中的第一个链接，然后登录。有关详细信息，请参见《*NetIQ iManager Administration Guide*》（NetIQ iManager 管理指南）中的 "Accessing iManager"（访问 iManager）。

18 （视情况而定）如果在启动升级过程之前已生成 server.xml 和 context.xml 配置文件的备份副本，请将新的配置文件替换为备份副本。

32.2.2 更新基于角色的服务

第一次使用 iManager 登录到已包含基于角色的服务 (RBS) 集合的 eDirectory 树时，您可能只能看到部分角色信息。此现象是正常的，因为您必须更新一些插件才能让其在最新版本的 iManager 上正常运行。 NetIQ 建议您将 RBS 模块更新到最新版本，以便您可以查看和使用 iManager 中提供的所有功能。 “RBS 配置 ” 表列出了需要更新的 RBS 模块。

请注意，您可能会遇到多个同名的角色。从 iManager 2.5 开始，一些插件开发人员会更改任务 ID 或模块名称，但保留其显示名称不变。此问题导致有些角色可能出现重复，但实际上，两个实例中一个来自旧版本，另一个来自较新的版本。

注释：

- 在更新或重安装 iManager 时，安装程序不会更新现有的插件。要手动更新插件，请起动 iManager 并浏览到**配置** > **插件安装** > **可用的 Novell 插件模块**。有关详细信息，请参见第 11.1.3 节 “ 了解 iManager 插件的安装 ” （第 127 页）。
- 不同的 iManager 安装程序可能会在本地安装不同数量的插件。因此，在**基于角色的服务** > **RBS 配置**页面中，您可能会发现任一给定集合的模块报告都有所不同。为了使每次安装 iManager 时插件数目都保持一致，请确保树中每个 iManager 实例上都安装了相同子集的插件。

要检查并更新过期的 RBS 对象，请执行以下操作：

1. 登录到 iManager。
2. 在 “ 配置 ” 视图中，选择 “ **基于角色的服务** ” > “**RBS 配置** ”。

   查看 “2.*x* 集合 ” 标签页面中的表格中有无过期的模块。
3. （可选）要更新某个模块，请完成以下步骤：
   - **3a** 对于要更新的集合，请在**已过期**列中选择它的编号。

     iManager 会显示已过期模块的列表。
   - **3b** 选择要更新的模块。
   - **3c** 单击表格顶部的**更新**。

32.2.3 重安装或迁移 Plug-in Studio 的插件

您可以将 Plug-in Studio 插件迁移或复制到其他 iManager 实例，以及新的或更新的 iManager 版本。

1. 登录到 iManager。
2. 在 iManager 的 “ 配置 ” 视图中，选择**基于角色的服务 > Plug-in Studio**。

   内容框架将显示 “ 已安装的自定义插件 ” 列表，包括插件所属的 RBS 集合的位置。
3. 选择要重安装或迁移的插件，然后单击**编辑**。

   注释：一次只能编辑一个插件。

   ---
4. 单击**安装**。
5. 针对每个需要重安装或迁移的插件重复上述步骤。

32.2.4 在升级或重安装后更新 iManager 插件

升级或重新安装 iManager 时，安装进程不会更新现有插件。确保插件与正确的 iManager 版本相匹配。有关详细信息，请参见第 11.1.3 节 " 了解 iManager 插件的安装 "（第 127 页）。

1 打开 iManager。
2 浏览到**配置 > 插件安装 > 可用的 Novell 插件模块**。
3 更新插件。

32.3 升级 Remote Loader

如果您在运行 Remote Loader，则需要升级 Remote Loader 文件。

注释：在升级 .Net Remote Loader 之前，请确保已在系统上成功安装所有 Windows 更新。

---

1 创建 Remote Loader 配置文件的备份。文件的默认位置为 C:\...\RemoteLoader*remoteloadername*-config.txt。
2 验证驱动程序是否已停止。有关指导，请参见第 9.4.1 节 " 停止驱动程序 "（第 81 页）。
3 停止每个驱动程序的 Remote Loader 服务或守护程序。
   - **Windows：**在 Remote Loader 控制台中，选择 Remote Loader 实例，然后单击**停止**。
   - **Java Remote Loader：**dirxml_jremote -config *path_to_configfile* -u
4 使用 Windows 任务管理器停止 lcache 进程。
5 （视情况而定）要在 Windows 服务器上运行无提示安装，请确保 silent.properties 文件包含安装的 Remote Loader 文件所在目录的路径。例如：

   ```
   X64_CONNECTED_SYSTEM_LOCATION=c:\novell\remoteloader\64bit
   ```

   安装程序不会检测先前安装的默认路径。
6 运行 Remote Loader 的安装程序。

   安装过程将文件和二进制数据更新为最新版本。有关详细信息，请参见第 III 部分 " 安装 Identity Manager 引擎 "（第 49 页）。
7 安装完成后，校验配置文件是否包含环境的信息。
8 （视情况而定）如果配置文件有问题，请复制您在步骤 1 中创建的备份文件。否则，继续步骤 9（第 331 页）。
9 启动每个驱动程序的 Remote Loader 服务或守护程序。
   - **Java Remote Loader：**dirxml_jremote -config *path_to_config_file*
   - **Windows：**在 Remote Loader 控制台中，选择 Remote Loader 实例，然后单击**启动**。

32.4 升级 Identity Manager 引擎

当您升级 Identity Manager 引擎或单独更新 SAML 方法时， iMonitor 会显示 SAML 方法的存在和不存在状态标志。您可以忽略不存在状态标志，因为 eDirectory 会正确使用更新后的方法。升级引擎时，升级进程会重启动 eDirectory，它会在内部负责使用更新后的 SAML 方法。如果您单独更新 SAML 方法，请手动重启动 eDirectory 服务器以使用更新后的 SAML 方法。

开始升级前，请确保超速缓存文件中没有任何事件。将 Identity Manager 引擎升级到 4.7 版本时，引擎安装程序会清理现有的 MapDB 驱动程序工作超速缓存文件 (dx*)。不过，您必须在升级驱动程序后，手动去除现有的 MapDB 状态超速缓存文件。否则，驱动程序可能无法启动。以下 Identity Manager 驱动程序使用 MapDB 3.0.5：

- MS Azure
- JDBC
- DCS
- MSGW
- LDAP
- Salesforce
- ServiceNow

升级 Remote Loader 和基于角色的服务后，您可以升级 Identity Manager 引擎。升级过程会更新主计算机的文件系统中所储存的驱动程序 shim 文件。

1. 验证驱动程序是否已停止。有关详细信息，请参见第 9.4.1 节 “ 停止驱动程序 ” （第 81 页）。
2. 从 IDM *version*_Win:\products\idm\Windows\setup\idm_install.exe 中起动 Identity Manager 引擎的安装程序。
3. 选择要用于安装的语言。
4. 阅读并接受许可协议。
5. 要更新 Identity Manager 引擎和驱动程序 shim 文件，请选择以下选项：
   - **Identity Manager 服务器**
   - **用于 Identity Manager 的 iManager 插件**
   - **驱动程序**
6. 以 LDAP 格式指定对 eDirectory 具有管理权限的用户及用户口令。
7. 查看摘要，然后单击**安装**。
8. 阅读安装摘要，然后单击**完成**。

32.5 升级 Identity Applications 和 Identity Reporting

本节提供有关升级 Identity Applications 和支持软件的信息，其中包括更新以下组件的内容：

- Identity Manager User Application
- One SSO Provider (OSP)
- Self-Service Password Reset (SSPR)
- Tomcat、 JDK 和 ActiveMQ
- Identity Reporting

NetIQ 提供了一个升级程序来升级这些组件。此程序位于 Identity Manager 安装包的 products\CommonApplication\ 目录中。导航到包含 ApplicationUpgrade.exe 文件的目录。

升级后，组件将升级到以下版本：

- Tomcat – 8.5.27
- ActiveMQ – 5.15.2
- Java – 1.80_162
- One SSO Provider – 6.2.1
- Self-Service Password Reset – 4.2.0.4
- Identity Applications – 4.7.0
- Identity Reporting – 6.0.0

本节提供有关以下主题的信息：

32.5.1 了解升级程序

升级进程会从现有组件中读取配置值。这些信息包括 ism-configuration.properties、 server.xml、SSPRConfiguration.xml 和其他配置文件。升级进程会使用这些配置文件在内部调用各组件的升级程序。此外，此程序还会创建当前安装的备份。

32.5.2 升级的先决条件和注意事项

在执行升级之前，请先查看以下注意事项：

- **Identity Manager 已升级到版本 4.5.6：**您不能从低于 4.5.6 的版本升级或迁移到版本 4.7。有关如何升级到 Identity Manager 4.5 的详细信息，请参见《*NetIQ Identity Manager 安装指南*》中的 " 升级 Identity Manager"。
- **系统要求：**升级过程至少需要 3 GB 可用磁盘空间，用于存储当前配置以及升级过程中创建的临时文件。确保服务器具有足够储存备份的空间，另外还有可供升级的可用空间。

  在 Windows 服务器上，升级程序会将临时文件储存在 %TEMP% 环境变量指定的目录中。如果此目录不能提供所需的空间，请将 TEMP 和 TMP 环境变量设置为文件系统中具有足够可用空间的某个目录。这会重新指示升级程序将文件储存到该目录。

  要将这些环境变量设置为不同的目录，请在开始升级之前完成以下步骤：

  1. 打开命令提示符并输入以下命令：

     ```
     SET TMP=D:\custom_tmp
     SET TEMP=D:\custom_tmp
     ```

其中， D:\custom_tmp 是具有足够可用磁盘空间的目录的路径。

注释：对于群集环境，请备份 Identity Applications 证书 (cacerts)。

---

2. 从命令行启动升级程序。

- **使用 Tomcat 作为应用程序服务器：**此版本的 Identity Manager 仅支持使用 Tomcat 作为应用程序服务器。

注释：确保您已在之前的安装期间使用便捷安装程序安装了 Tomcat 应用程序服务器。升级过程只允许您升级使用便捷安装程序安装的 Tomcat。

- **数据库平台已升级：**此程序不会升级 Identity Applications 的数据库平台。请手动将当前的数据库版本升级到支持的版本。要升级 PostgreSQL 数据库，请参见升级 PostgreSQL 数据库 （第 334 页）。
- **Identity Applications 和 Identity Reporting 驱动程序已升级：**确保您已升级 Identity Applications 和 Identity Reporting 的下列驱动程序。
  - User Application 驱动程序
  - 角色和资源驱动程序
  - 管理系统网关驱动程序
  - 数据收集服务驱动程序

  有关详细信息，请参见 《*NetIQ Designer for Identity Manager Administration Guide*》（NetIQ Designer for Identity Manager 管理指南）中的 “Upgrading Installed Packages” （升级安装的包）。
- **管理员用户拥有最高的访问特权：**向管理员用户提供最高访问特权。
- **用户帐户控制设置已更改为 “ 从不通知 ”：**转到**控制面板 > 用户帐户**，然后将**用户帐户控制设置**更改为**从不通知**。
- **Self Service Password Reset:** 如果要从 SSPR 4.0 升级，请确保您已更新 CATALINA_OPTS 属性，并且 -Dsspr.application.Path 设置为储存 SSPR 配置的文件夹。

  例如：set CATALINA_OPTS="-Dsspr.applicationPath=C:\sspr_data

  在升级前备份 SSPR LocalDB。要导出或下载 LocalDB，请执行以下步骤：

  1. 以管理员身份登录 SSPR 门户。
  2. 从下拉菜单中导航到**您的 ID > 配置管理器**。
  3. 单击 **LocalDB**。
  4. 单击**下载 LocalDB**。

32.5.3 升级 PostgreSQL 数据库

重要：升级过程可能需要一段时间，时间长短取决于数据库大小。因此，请相应规划您的升级。

---

1 停止服务器上正在运行的 PostgreSQL 服务。

2 重命名 C:\Netiq\idm\apps 中的 postgres 目录。

  例如，将 postgres 重命名为 postgresql_9_3。

3 安装您的操作系统支持的 PostgreSQL 版本。

选择的位置必须与 PostgreSQL 的当前安装位置不同。

3a 装入 Identity_Manager_4.7_Windows.iso 映像文件，并导航到包含 PostgreSQL 安装文件的 products\CommonApplication\postgre_tomcat_install 目录。

3b 运行 TomcatPostgreSQL.exe 文件来安装 PostgreSQL 应用程序。

安装期间，请只选择 **PostgreSQL** 选项。

注释：不要在 **PostgreSQL 细节**页面中提供任何数据库细节。确保取消选择**创建数据库登录帐户**和**创建空数据库**。

---

4 停止新安装的 PostgreSQL 服务。转到**服务**，搜索 PostgreSQL 9.6 服务，然后停止该服务。

注释：相应的用户在提供有效的鉴定信息后，可以执行停止操作。

---

5 通过执行以下操作更改新安装的 PostgreSQL 目录的许可权限：

创建一个 postgres 用户：

1. 转到**控制面板 > 用户帐户 > 用户帐户 > 管理帐户**。
2. 单击**添加用户帐户**。
3. 在 " 添加用户 " 页面中，指定 postgres 作为用户名，并提供该用户的口令。

为 postgres 用户提供对现有和新安装的 PostgreSQL 目录的许可权限：

1. 右键单击 PostgreSQL 目录，然后转到**属性 > 安全性 > 编辑**。
2. 为该用户选择**完全控制**，以提供完全许可权限。
3. 单击**应用**。

6 以 postgres 用户的身份访问 PostgreSQL 目录。

1. 以 postgres 用户的身份登录到服务器。

   在登录之前，请校验是否允许 postgres 用户建立远程连接，以确保此用户可连接到 Windows 服务器。

2. 打开命令提示符，并使用以下命令设置 PGPASSWORD：

   ```
   set PGPASSWORD=<your pg password>
   ```

3. 切换到新安装的 PostgreSQL 目录。

   例如：C:\Users\postgres>cd C:\NetIQ\idm\apps1\postgresql962\bin。

7 从新 PostgreSQL 的 bin 目录升级 PostgreSQL。运行以下命令，然后单击 **Enter**。

```
pg_upgrade.exe --old-datadir "C:\NetIQ\idm\apps1\postgres\data" --new-datadir
"C:\NetIQ\idm\apps1\postgresql962\data" --old-bindir
"C:\NetIQ\idm\apps1\postgres\bin" --new-bindir
"C:\NetIQ\idm\apps1\postgresql962\bin"
```

8 启动升级后的 PostgreSQL 数据库服务。

转到**服务**，搜索 PostgreSQL 9.6 服务，然后启动该服务。

注释：相应的用户在提供有效的鉴定信息后，可以执行启动操作。

---

9 禁用旧的 PostgreSQL 服务，以确保该服务不会自动启动。

10 （可选）从新安装的 PostgreSQL 服务的 bin 目录中删除旧数据文件。

1. 以 postgres 用户的身份登录。
2. 导航到 bin 目录，并运行 analyze_new_cluster.bat 和 delete_old_cluster.bat 文件。

   例如：C:\NetIQ\idm\apps1\postgresql961\bin

注释：仅当您想要删除旧数据文件时，才需要运行此步骤。

32.5.4 系统要求

升级进程会为所安装组件的当前配置创建备份。确保服务器具有足够储存备份的空间，另外还有可供升级的可用空间。

32.5.5 升级 Identity Applications 的驱动程序包

本节介绍如何将 User Application 驱动程序以及角色和资源服务驱动程序的包更新到最新版本。升级 Identity Applications 前必须先执行此任务。

1 在 Designer 中打开当前项目。
2 右键单击**包编目 > 导入包**。
3 选择相应的包。例如， **User Application 驱动程序基础包**。
4 单击**确定**。
5 在开发人员视图中，右键单击该驱动程序，然后单击**属性**。
6 浏览到**属性**页面中的**包**选项卡。
7 单击右上角的**添加包 (+)** 符号。
8 选择该包，然后单击**确定**。
9 部署并重启动驱动程序。
10 重复相同过程升级角色和资源服务驱动程序的包。

注释：

- 确保 User Application 驱动程序以及角色和资源服务驱动程序连接到升级后的 Identity Manager。
- 如果您在升级 User Application 驱动程序包时安装了任何通知模板，请将**默认通知集合**对象部署到您的 Identity Manager 服务器。

32.5.6 使用指导式过程进行升级

以下过程介绍了如何使用向导升级 Identity Applications、 OSP、 SSPR、 Tomcat、 ActiveMQ 和 Identity Reporting。

1 登录到要运行升级过程的服务器。
2 装入 .iso 映像文件，导航到包含升级可执行文件的目录 （默认位于 products\CommonApplication\ 目录中）。
3 起动升级程序。右键单击 ApplicationUpgrade.exe 并选择**以管理员身份运行**。
4 在**简介**页面上，您可以查看可升级的 Identity Manager 组件，然后单击**下一步**。

5 阅读并接受许可协议，然后单击下一步。

6 查看已部署的应用程序页面，然后单击下一步。

此页面会列出当前安装的组件及其版本。如果在该服务器上部署了其他应用程序，则升级进程会显示警告，指出升级后这些应用程序可能会无法正常工作。

您必须手动从升级进程创建的备份恢复它们。

7 要继续升级，请单击下一步。

8 使用以下参数完成引导式过程。此程序会自动填充现有组件的值。确保为参数指定了正确的值。

- **One SSO Provider 安装文件夹**

  表示升级程序要在其中创建 OSP 应用程序文件的目录路径。如果该路径不正确，请浏览到 OSP 的安装路径。

- **SSPR 安装文件夹**

  表示升级程序要在其中创建 SSPR 应用程序文件的目录路径。如果该路径不正确，请浏览到 SSPR 的安装路径。

- **User Application 安装文件夹**

  表示升级程序要在其中创建 User Application 应用程序文件的目录路径。如果该路径不正确，请浏览到 User Application 的安装路径。

- **数据库连接**

  表示用于连接 User Application 数据库的设置， Identity Applications 也会连接到此数据库。升级程序会将这些细节包含在 User Application 配置文件中。

  数据库平台

  表示 User Application 数据库的平台。

  数据库主机

  指定托管 User Application 的服务器的名称或 IP 地址。

  数据库端口

  指定数据库服务器用于与 User Application 通讯的端口。

  数据库驱动程序 JAR 文件

  指定数据库平台的 jar 文件。

  数据库供应商将提供驱动程序 JAR 文件，即数据库服务器的 JAR。例如，对于 PostgreSQL，可以指定默认位于 C:\NetIQ\idm\apps\postgres 中的 postgresql-9.4-1212.jdbc42.jar。同样，指定您数据库平台的相应 jar 文件。

- **（视情况而定） Reporting 数据库连接**

  表示用于连接 Identity Reporting 数据库的设置。

  数据库主机

  指定托管 User Application 的服务器的名称或 IP 地址。

  数据库端口

  指定数据库服务器用于与 User Application 通讯的端口。

  数据库名称

  指定数据库的名称。数据库名称默认为 idmrptdb。

- **（视情况而定） Reporting 数据库身份凭证**

  Reporting 数据库用户

  指定允许 User Application 访问和修改数据库中数据的帐户名。数据库用户名默认为 postgres。

  Reporting 数据库口令

  为指定用户名指定口令。

  升级 Reporting 数据库

  立即升级数据库：升级程序会在升级过程中更新 Reporting 数据库表的纲要。

  在应用程序启动时升级数据库：升级程序会下达在升级后 User Application 首次启动时为数据库表更新纲要的指令。

  将 SQL 写入文件：生成一个 SQL 脚本，数据库管理员可以运行该脚本来更新数据库。如果选择此选项，则还必须为**纲要文件**指定名称。设置位于 **SQL 输出**文件配置中。如果您无权在您的环境中创建或修改数据库，可以选择此选项。有关使用该文件生成表的详细信息，请参见第 15.7.2 节 " 手动创建数据库纲要 "（第 194 页）。

  数据库驱动程序 JAR 文件

  指定数据库平台的 jar 文件。

  数据库供应商将提供驱动程序 JAR 文件，即数据库服务器的 JAR。例如，对于 PostgreSQL，可以指定默认位于 C:\NetIQ\idm\apps\postgres 中的 postgresql-9.4-1212.jdbc42.jar。同样，指定您数据库平台的相应 jar 文件。

- **升级数据库**

  立即升级数据库

  升级程序会在升级过程中为数据库表更新纲要。

  在应用程序启动时升级数据库

  升级程序会下达在升级后 User Application 首次启动时为数据库表更新纲要的指令。

  将 SQL 写入文件

  生成一个 SQL 脚本，数据库管理员可以运行该脚本来更新数据库。如果选择此选项，则还必须为**纲要文件**指定名称。设置位于 **SQL 输出**文件配置中。如果您无权在您的环境中创建或修改数据库，可以选择此选项。有关使用该文件生成表的详细信息，请参见第 15.7.2 节 " 手动创建数据库纲要 "（第 194 页）。

- **数据库管理员**

  表示数据库管理员的名称和口令。

  数据库用户名

  指定可创建数据库表、视图和其他项目的数据库管理员帐户。

  口令

  指定数据库管理员的口令。

- **Reporting 数据库连接**

  表示数据库管理员的主机名和口令。

  数据库用户名

  指定可创建数据库表、视图和其他项目的数据库管理员帐户。

  口令

  指定数据库管理员的口令。

9 复查升级前摘要页面，然后单击安装。

升级进程会停止 Tomcat 服务并开始升级，完成此过程可能需要一段时间。

10 当升级过程完成时，查看 /tmp/rbpm_upgrade/ 中的升级日志文件，您需要手动更新数个配置，请参见第 32.5.7 节 " 升级后任务 " （第 339 页）。

根据组件的安装位置，安装进程会在该位置创建备份目录，并在备份目录中追加时戳 （指示备份时间）。

例如，

- Tomcat – C:\NetIQ\idm\apps\tomcat_backup_02262018_033634
- OSP 和 SSPR - C:\NetIQ\idm\apps\osp_sspr_backup_02262018_033634
- ActiveMQ - C:\NetIQ\idm\apps\activemq_backup_02262018_033634
- User Application - C:\NetIQ\idm\apps\UserApplication_backup_02262018_033634
- Identity Reporting - C:\NetIQ\idm\apps\IdentityReporting_backup_02262018_033634

32.5.7 升级后任务

升级 Identity Applications 后，请务必执行下列操作：

您还必须手动恢复 Tomcat、 SSPR、 OSP 或 Identity Applications 的自定义设置。

针对所需组件执行升级后步骤：

- Java （第 339 页）
- Tomcat （第 340 页）
- Identity Applications （第 340 页）
- One SSO Provider （第 341 页）
- Self-Service Password Reset （第 341 页）
- Kerberos （第 341 页）

Java

对照旧版 JRE 位置，校验新升级的 JRE 位置中的证书：jre\lib\security\cacerts。手动将缺少的证书导入到 cacerts 中。

1 使用 keytool 命令导入 java cacerts：

```
keytool -import -trustcacerts -file Cerificate_Path -alias ALIAS_NAME -keystore
cacerts
```

注释：升级后， JRE 储存在 Identity Applications 安装位置。例如：C:\NetIQ\idm\apps\jre

2 校验 JRE 主目录位置是否为 tomcat\bin\setenv.bat。

3 起动配置更新实用程序，并校验您的 cacerts 路径。

Tomcat

1 （视情况而定）要从升级过程先前创建的备份恢复自定义文件，请执行以下任务：

- 恢复自定义的 https 证书。要恢复这些证书，请将备份的 server.xml 中的 Java Secure Socket Extension (JSSE) 内容复制到 \tomcat\conf 目录下的新 server.xml 文件中。
- 不要将备份的 Tomcat 目录中的配置文件复制到新 Tomcat 目录中。应根据需要在新版本默认配置的基础上进行更改。有关详细信息，请参见此 Apache 网站。

  校验新的 server.xml 文件是否包含以下条目

  ```
  <Connector port="8543" protocol="HTTP/1.1"
         maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
         clientAuth="false" sslProtocol="TLS"
         keystoreFile="path_to_keystore_file"
         keystorePass="keystore_password" />
  <!--
        <Cluster className="org.apache.catalina.ha.tcp.SimpleTcpCluster"/>
   -->
  ```

  或者

  ```
  <Connector port="8543"
  protocol="org.apache.coyote.http11.Http11NioProtocol"
         maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
         clientAuth="false" sslProtocol="TLS"
         keystoreFile="path_to_keystore_file"
         keystorePass="keystore_password" />
  <!--
        <Cluster className="org.apache.catalina.ha.tcp.SimpleTcpCluster"/>
   -->
  ```

  注释：在群集环境中，手动取消注释 server.xml 中的 Cluster 标记，然后将第一个节点上的 osp.jks （位于 C:\netiq\idm\apps\osp_backup_<date> 中）复制到所有节点上。

- 如果您自定义了密钥存储区文件，请在新 server.xml 文件中包括正确的路径。
- 将 Identity Applications 证书导入到身份库中 （位于 C:\NetIQ\eDirectory\jre\lib\security\cacerts）。

  例如，您可以使用以下 keytool 命令将证书导入到身份库中：

  ```
  keytool -importkeystore -alias <User Application certificate alias> -
  srckeystore  <backup cacert> -srcstorepass changeit -destkeystore
  C:\NetIQ\eDirectory\jre\lib\security\cacerts
  ```

2 （视情况而定）导航到 User Application，然后通过读取备份的配置手动恢复自定义设置。

Identity Applications

从升级过程中创建的备份恢复 Identity Applications 自定义配置。

如果您要从 4.5.6 版本升级 Identity Manager，则必须为要用于在 Identity Manager 仪表板中对用户排序的每个属性手动创建复合索引，请参见创建复合索引 （第 188 页）。

1 起动 configupdate 实用程序 (configupdate.bat) 文件。

  在 configupdate.bat.properties 文件中，确保 use_console 的值设置为 false。

2 连接身份库服务器，并接受 eDirectory 证书。

3 在 SSO 客户端选项卡中，导航到 RBPM，然后单击显示高级选项。

4 将 RBPM 至 eDirectory SAML 配置设置为 “ 自动 ”。

One SSO Provider

logevent.conf 文件中的 LogHost 项默认设置为 localhost。

要修改 LogHost 条目，请手动从升级过程中创建的备份恢复 OSP 自定义配置。

Self-Service Password Reset

升级 SSPR 后，使用配置更新实用程序更新 SSO 客户端参数。有关更多信息，请参见第 15.8.5 节 “SSO 客户端参数 ” （第 218 页）中的 Self Service Password Reset （第 221 页）。

要更新 SSPR 配置细节，请执行以下步骤：

1 以管理员身份登录 SSPR 门户。

2 更新审计服务器细节：

   2a 导航到您的 ID > 配置编辑器，指定配置口令。

   2b 选择设置 > 审计 > 审计转发 > Syslog 审计服务器证书。

   2c 从服务器导入这些证书，然后单击保存。

3 将 LocalDB 导入 SSPR：

   3a 从下拉菜单导航到您的 ID > 配置管理器。

   3b 单击 LocalDB。

   3c 单击导入 （上载） LocalDB 存档文件。

4 （视情况而定）要限制 SSPR 的配置，请执行以下操作：

   4a 从列表中导航到您的 ID > 配置管理器。

   4b 单击限制配置。

5 配置 SSPR 的管理员许可权限，请参见第 14.2.3 节 “ 安装后任务 ” （第 160 页）。

要校验升级是否成功，请起动升级的组件。

例如，起动 Identity Manager 仪表板，单击关于。检查应用程序显示的是否为新版本，例如 4.7.0。

Kerberos

升级实用程序会在计算机上创建新的 Tomcat 文件夹。如果任何 Kerberos 文件 （例如 keytab 和 Kerberos_login.config）驻留在旧的 Tomcat 文件夹中，请从备份文件夹中将这些文件复制到新的 Tomcat 文件夹。

32.6 升级 Identity Reporting

Identity Reporting 中包含两个驱动程序。此外，您需要将 NetIQ Event Auditing Service 中的内容迁移到 Sentinel Log Management for IGA。按以下顺序执行升级：

1. 升级数据收集服务的驱动程序包。

2. 升级受管系统网关服务的驱动程序包。
3. 迁移到 Sentinel Log Management for IGA
4. 升级 Identity Reporting

32.6.1 升级 Identity Reporting 的驱动程序包

本节介绍了如何将受管系统网关驱动程序包和数据收集服务驱动程序包更新到最新版本。升级 Identity Reporting 前必须先执行此任务。

1 在 Designer 中打开当前项目。
2 右键单击**包编目 > 导入包**。
3 选择相应的包。例如，**受管系统网关基础包 2.0.0.20120509205929**。
4 单击**确定**。
5 在开发人员视图中，右键单击该驱动程序，然后单击**属性**。
6 浏览到**属性**页面中的**包**选项卡。
7 单击右上角的**添加包 (+)** 符号。
8 选择该包，然后单击**确定**。
9 完成驱动程序的配置过程。有关详细信息，请参见以下各节：
   - 第 19.1.2 节 " 配置受管系统网关驱动程序 " （第 242 页）
   - 第 19.1.3 节 " 配置数据收集服务的驱动程序 " （第 243 页）
10 重复步骤 2 至步骤 9 以升级数据收集服务驱动程序包。
11 确保受管系统网关驱动程序和数据收集服务驱动程序已连接到升级后的 Identity Manager。

32.6.2 升级 Identity Reporting

升级 Identity Reporting 之前，必须先升级 Identity Applications 和 SLM for IGA。要升级 Identity Reporting 4.0.2 或更高版本，请安装新版本并覆盖旧版本。有关详细信息，请参见安装 Identity Reporting （第 231 页）。

32.6.3 更改对数据库中的 reportRunner 的参照

升级 Identity Reporting 后，请务必在第一次启动 Tomcat 之前更新对数据库中 reportRunner 的参照。

1 停止 Tomcat。
2 导航到 Identity Reporting 安装目录，并将 reportContent 文件夹重命名为 ORG-reportContent。

   例如：C:\NetIQ\idm\apps\IdentityReporting
3 清理 Tomcat 文件夹下的临时目录和工作目录。
4 登录 PostgreSQL 数据库。

   4a 在下面的表中找到 reportRunner 参照：
   - idm_rpt_cfg.idmrpt_rpt_params
   - idm_rpt_cfg.idmrpt_definition

   4b 发出以下 delete 语句：

```
DELETE FROM idm_rpt_cfg.idmrpt_rpt_params WHERE
rpt_def_id='com.novell.content.reportRunner';

DELETE FROM idm_rpt_cfg.idmrpt_definition WHERE
def_id='com.novell.content.reportRunner';
```

5 启动 Tomcat。

检查日志以确定使用正确的 reportRunner 是否可重新生成报告。

6 登录 Identity Reporting 并运行报告。

32.6.4 校验 Identity Reporting 的升级

1 起动 Identity Reporting。
2 校验工具中是否显示了旧报告和新报告。
3 查看**日历**以确定是否显示了安排的报告。
4 确保**设置**页面显示了受管和非受管应用程序的先前设置。
5 校验所有其他设置是否正确。
6 校验应用程序是否列出已完成的报告。

32.7 升级 Analyzer

NetIQ 提供了 .zip 格式的增补程序文件用于升级 Analyzer。在升级 Analyzer 之前，请确保计算机满足各项先决条件和系统要求。有关详细信息，请参见更新随附的 《发行说明》。

1 从 NetIQ 下载网站下载增补程序文件，例如 analyzer_4.6_patch1_20121128.zip。
2 将该 .zip 文件抽取到包含 Analyzer 安装文件 （例如插件、卸装脚本和其他 Analyzer 文件）的目录。
3 重启动 Analyzer。
4 要校验是否已成功应用新的增补程序，请完成以下步骤：
   - **4a** 起动 Analyzer。
   - **4b** 单击**帮助 > 关于 Analyzer**。
   - **4c** 检查程序是否显示了新版本，例如 **4.6 Update 1** 和版本 ID **20121128**。

32.8 升级 Identity Manager 驱动程序

NetIQ 通过**包**而不是驱动程序配置文件递送新的驱动程序内容。您可以在 Designer 中管理、维护和创建包。尽管 iManager 可以识别包，但 Designer 不会保留您在 iManager 中对驱动程序内容所做的任何更改。有关管理包的详细信息，请参见 《*NetIQ Designer for Identity Manager Administration Guide*》（NetIQ Designer for Identity Manager 管理指南）中的 “Managing Packages” （管理包）。

注释：如果要将 3.*x* 版本的 User Application 驱动程序升级到 User Application 版本 4.0.2 包，Designer 会同时安装相同驱动程序策略的 3.*x* 和 4.0 版本。包目录中同时具有 3.*x* 和 4.0 策略可能会导致 Designer 无法正常运行。删除版本 3.*x* 策略并保留版本 4.0 策略。

您可通过以下方式将驱动程序升级到包：

- 第 32.8.1 节 " 创建新驱动程序 "（第 344 页）
- 第 32.8.2 节 " 用包的内容替换现有内容 "（第 344 页）
- 第 32.8.3 节 " 保留当前内容并通过包添加新内容 "（第 344 页）

32.8.1 创建新驱动程序

将驱动程序升级到包的最简单明了的方式是删除现有驱动程序并通过包创建新驱动程序。在新的驱动程序中添加所有需要的功能。每个驱动程序的步骤都不同。有关说明，请参见 Identity Manager 驱动程序文档网站上各个驱动程序的指南。现在驱动程序与之前一样工作，但其内容来自包而不是来自驱动程序配置文件。

32.8.2 用包的内容替换现有内容

如果需要保留驱动程序创建的关联，您无需删除然后重创建驱动程序。您可以保留关联，并用包替换现有的驱动程序内容。

要用包的内容替换现有内容：

1. 创建驱动程序及驱动程序中所有自定义内容的备份。

   有关说明，请参见第 31.5.2 节 " 导出驱动程序的配置 "（第 324 页）。

2. 在 Designer 中，删除储存在驱动程序内的所有对象。删除储存在驱动程序内的策略、过滤器、权利及所有其他项目。

   注释：Designer 提供了自动导入工具用于导入最新的包。您不需要手动将驱动程序包导入到包编目中。

   有关详细信息，请参见《*NetIQ Designer for Identity Manager Administration Guide*》（NetIQ Designer for Identity Manager 管理指南）中的 "Importing Packages into the Package Catalog"（将包导入包编目）。

3. 将最新的包安装到驱动程序中。

   这些步骤对每个驱动程序都是特定的。有关说明，请参见 Identity Manager 驱动程序文档网站上每个驱动程序的指南。

4. 将所有自定义策略和规则恢复到驱动程序。有关说明，请参见第 32.10 节 " 将自定义策略和规则恢复到驱动程序 "（第 346 页）。

32.8.3 保留当前内容并通过包添加新内容

只要包中的功能不与驱动程序的当前功能重叠，就可以保留当前的驱动程序不变，而通过包向驱动程序添加新功能。

在安装包之前，请创建驱动程序配置文件的备份。安装某个包时，该包可能会重写现有策略，从而导致驱动程序停止工作。如果重写了某个策略，您可以导入备份驱动程序配置文件并重创建该策略。

在开始前，请确保任何自定义策略的名称均不同于默认策略。使用新驱动程序文件覆盖驱动程序配置时，会重写现有策略。如果自定义策略的名称不唯一，您将会丢失这些策略。

要通过包向驱动程序添加新内容：

1. 创建驱动程序及驱动程序中所有自定义内容的备份。

有关说明，请参见第 31.5.2 节 " 导出驱动程序的配置 " （第 324 页）。

注释：Designer 提供了自动导入工具用于导入最新的包。您不需要手动将驱动程序包导入到包编目中。

有关详细信息，请参见 《*NetIQ Designer for Identity Manager Administration Guide*》（NetIQ Designer for Identity Manager 管理指南）中的 "Importing Packages into the Package Catalog"（将包导入包编目）。

---

2 将包安装到驱动程序上。

有关说明，请参见 Identity Manager 驱动程序文档网站上每个驱动程序的指南。

3 将所需包添加到驱动程序中。这些步骤对每个驱动程序都是特定的。

有关详细信息，请参见 Identity Manager 驱动程序文档网站。

驱动程序现在包含通过包添加的新功能。

32.9 将新服务器添加到驱动程序集

将 Identity Manager 升级或迁移到新服务器时，您必须更新驱动程序集信息。本节将指导您完成该过程。您可以使用 Designer 或 iManager 更新驱动程序集。

32.9.1 将该新服务器添加到驱动程序集中

如果正在使用 iManager，则必须将该新服务器添加到驱动程序集中。 Designer 包含一个用于服务器的迁移向导，可为您完成此步骤。如果正在使用 Designer，请跳至第 35.3.1 节 " 在 Designer 中复制服务器特定信息 " （第 357 页）。如果正在使用 iManager，请完成以下过程：

1 在 iManager 中，单击 以显示 "Identity Manager 管理 " 页面。

2 单击 **Identity Manager 概述**。

3 浏览到并选择保存驱动程序集的容器。

4 单击驱动程序集名称以访问 " 驱动程序集概述 " 页。

5 单击**服务器 > 添加服务器**。

6 浏览并选择新 Identity Manager 服务器，然后单击**确定**。

32.9.2 从驱动程序集中去除旧服务器

当新服务器运行所有驱动程序后，您可以从驱动程序集中去除旧服务器。

使用 Designer 从驱动程序集中去除旧服务器

1 在 Designer 中，打开项目。

2 在建模器中，右键单击驱动程序集，然后选择**属性**。

3 选择服务器列表。

4 在选定服务器列表中选择旧 Identity Manager 服务器，然后单击 < 从选定服务器列表中去除该服务器。

5 单击确定保存更改。

6 将更改部署到身份库中。

有关详细信息，请参见《*NetIQ Designer for Identity Manager Administration Guide*》（NetIQ Designer for Identity Manager 管理指南）中的 "Deploying a Driver Set to an Identity Vault"（将驱动程序集部署到身份库）。

使用 iManager 从驱动程序集中去除旧服务器

1 在 iManager 中，单击 以显示 "Identity Manager 管理 " 页面。

2 单击 **Identity Manager 概述**。

3 浏览到并选择保存驱动程序集的容器。

4 单击驱动程序集名称以访问 " 驱动程序集概述 " 页。

5 单击**服务器 > 去除服务器**。

6 选择旧 Identity Manager 服务器，然后单击确定。

弃用旧服务器

此时，旧服务器不再托管任何驱动程序。如果不再需要该服务器，则必须完成其他步骤以将其弃用：

1 从此服务器中去除 eDirectory 复本。

有关详细信息，请参见《*NetIQ eDirectory Administration Guide*》（NetIQ eDirectory 管理指南）中的 "Deleting Replicas"（删除复本）。

2 从此服务器中去除 eDirectory。

有关更多信息，请参见 TID 10056593，" 从 NDS 树中永久去除服务器 "。

32.10 将自定义策略和规则恢复到驱动程序

安装或升级到驱动程序的新包之后，您必须将所有自定义策略或规则恢复到驱动程序，然后再重写新的驱动程序配置文件。如果这些策略具有不同名称，则它们仍存储在驱动程序中，但是链接会损坏并需要重新建立。

- 第 32.10.1 节 " 使用 Designer 将自定义策略和规则恢复为驱动程序 "（第 346 页）
- 第 32.10.2 节 " 使用 iManager 将自定义策略和规则恢复为驱动程序 "（第 347 页）

32.10.1 使用 Designer 将自定义策略和规则恢复为驱动程序

您可以将策略添加到策略集中。在将升级后的驱动程序移到生产环境中之前，您应该在测试环境中执行以下步骤。

1 在大纲视图中，选择已升级的驱动程序，然后单击显示策略流图标 。

2 右键单击需要将自定义策略恢复为驱动程序的策略集，然后选择**添加策略 > 复制现有策略**。

3 浏览到并选择自定义策略，然后单击确定。

4 指定自定义策略的名称，然后单击**确定**。

5 在文件冲突讯息中单击**是**以保存项目。

6 策略构建器打开策略后，验证复制的策略中信息是否正确。

7 对需要恢复为驱动程序的每个自定义策略，重复步骤 2 到步骤 6。

8 启动并测试驱动程序。

有关启动驱动程序的更多信息，请参见第 9.4.2 节 " 启动驱动程序 " （第 82 页）。有关测试驱动程序的详细信息，请参见 《*NetIQ Identity Manager - Using Designer to Create Policies*》（NetIQ Identity Manager - 使用 Designer 创建策略）中的 "Testing Policies with the Policy Simulator" （使用策略模拟器测试策略）。

9 验证策略工作正常后，将驱动程序移动到生产环境中。

32.10.2 使用 iManager 将自定义策略和规则恢复为驱动程序

在将升级的驱动程序移到生产环境中前，请在测试环境中执行这些步骤。

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

2 浏览到并选择树中要搜索驱动程序集对象的位置，然后单击搜索图标 ▶。

3 单击包含已升级的驱动程序的驱动程序集对象。

4 单击驱动程序图标，然后选择需要恢复自定义策略的策略集。

5 单击**插入**。

6 选择**使用现有策略**，然后浏览到并选择自定义策略。

7 单击**确定**，然后单击**关闭**。

8 对需要恢复为驱动程序的每个自定义策略，重复步骤 3 到步骤 7。

9 启动并测试驱动程序。

有关启动驱动程序的信息，请参见第 9.4.2 节 " 启动驱动程序 " （第 82 页）。 iManager 中没有任何策略模拟器。要测试策略，请触发使策略能够执行的事件。例如，创建用户、修改用户或删除用户。

10 验证策略工作正常后，将驱动程序移动到生产环境中。

33 从 Advanced Edition 切换到 Standard Edition

仅当您不想在环境中使用任何 Advanced Edition 功能，并且想要缩减 Identity Manager 部署时，才应切换到 Standard Edition。

1 （视情况而定）如果您已应用 Advanced Edition 激活，请去除激活。

2 （视情况而定）要切换到 Standard Edition 评估模式，请执行以下操作：

   2a 导航到 C:\Novell\NDS\DIBFiles 中的身份库 dib 目录。

   2b 创建一个新文件，将其命名为 .idme，并在其中添加 2 （数值）。

   2c 重启动 eDirectory。

   2d 继续步骤 4。

3 （视情况而定）如果您已购买 Standard Edition 激活，请应用激活。

4 停止 Tomcat。

5 从 C:\NetIQ\idm\apps\tomcat\webapps 目录中去除以下 WAR 文件和 Webapps 文件夹：

   - IDMProv*
   - IDMRPT*
   - dash*
   - idmdash*
   - landing*
   - rra*
   - rptdoc*

6 将以下现有文件夹移到备份目录：

   - IDMReporting
   - UserApplication

7 将 < 安装文件夹 >/tomcat/conf 目录中的 ism-configuration.properties 文件复制到备份目录。

8 从 Identity Manager 4.6 媒体安装 Identity Reporting。

9 从 *<Reporting 安装文件夹 >*/bin 目录启动 configupdate.bat，然后指定以下参数的值：

   “ 报告 ” 选项卡：指定以下部分中的设置：

   - ID 库
   - 身份库用户身份
   - 报告管理员
     - **报告管理员角色容器 DN**. 例如， ou=sa,o=data
     - **报告管理员**。例如， cn=uaadmin,ou=sa,o=data

“ 鉴定 ” 选项卡：指定以下部分中的设置：

- 鉴定服务器
  - **OAuth 服务器主机标识符** . 例如，鉴定服务器的 IP 地址或 DNS 名称 （如 192.99.17.22）
  - **OAuth 服务器 TCP 端口**
  - **OAuth 服务器正在使用 TLS/SSL**
- 鉴定配置
  - **OAuth 密钥存储区文件** . 例如， C:\NetIQ\idm\apps\osp\osp.jks
  - **OAuth 使用的密钥的密钥别名**
  - **OAuth 所用密钥的密钥口令**
  - **会话超时 （分钟）**。例如， 60 分钟。

“SSO 客户端 ” 选项卡：指定以下部分中的设置：

- 报告
  - **登录页的 URL 链接** . 例如， http://192.99.17.22:8180/IDMRPT
- Self Service Password Reset
  - **OAuth 客户端 ID**. 例如， *sspr*
  - OAuth 客户端机密。例如， *<sspr 客户端机密 >*
  - **OSP OAuth 重定向 URL**. 例如， http://192.99.179.202:8180/sspr/public/oauth

有关配置实用程序的详细信息，请参见运行 Identity Applications 配置实用程序 （第 204 页）。

10 保存更改并退出配置实用程序。

11 启动 Tomcat。

X 将 Identity Manager 数据迁移到新安装

本部分提供有关将 Identity Manager 组件中的现有数据迁移到新安装的信息。大多数迁移任务都适用于 Identity Applications。要升级 Identity Manager 组件，请参见第 IX 部分 “ 升级 Identity Manager”（第 315 页）。有关升级与迁移之间区别的详细信息，请参见第 31.2 节 “ 了解升级和迁移 ”（第 319 页）。

34 准备迁移 Identity Manager

本章提供的信息可帮助您准备好将 Identity Manager 解决方案迁移到新安装。

34.1 执行迁移的核对清单

要执行迁移， NetIQ 建议您完成以下核对清单中的步骤。

	核对清单项目
❑	1. 确定应执行升级还是迁移。有关详细信息，请参见第 31.2 节 " 了解升级和迁移 " （第 319 页）。
❑	2. 确保拥有最新的安装包用于迁移 Identity Manager 数据。
❑	3. 了解 Identity Manager 各组件之间的交互。有关详细信息，请参见第 I 部分 " 简介 " （第 17 页）。
❑	4. 确保您的计算机符合较新版 Identity Manager 的硬件和软件先决条件。有关详细信息，请参见第 6 章 " 安装注意事项 " （第 45 页）和要升级的目标版本的 《发行说明》。
❑	5. 将 eDirectory 升级到身份库的最新受支持版本。有关详细信息，请参见第 7.1.2 节 " 安装身份库的先决条件和注意事项 " （第 52 页）。
❑	6. 将位于当前 Identity Manager 服务器上的 eDirectory 复本添加到新服务器。有关详细信息，请参见第 35.4 节 " 将 Identity Manager 引擎迁移到新服务器 " （第 358 页）。
❑	7. 在新服务器上安装 Identity Manager。有关详细信息，请参见规划安装 Identity Manager （第 35 页）。
❑	8. （视情况而定）如果驱动程序集中有任何驱动程序是 Remote Loader 驱动程序，请升级每个驱动程序的 Remote Loader 服务器。有关详细信息，请参见第 32.3 节 " 升级 Remote Loader" （第 331 页）。
❑	9. （视情况而定）如果在旧服务器上运行 User Application，请更新该组件及其驱动程序。有关详细信息，请参见第 35.1 节 "Identity Manager 的迁移核对清单 " （第 355 页）。
❑	10. 将该新服务器添加到驱动程序集中。有关详细信息，请参见第 32.9.1 节 " 将该新服务器添加到驱动程序集中 " （第 345 页）。
❑	11. 更改每个驱动程序的特定于服务器的信息。有关详细信息，请参见第 35.3.1 节 " 在 Designer 中复制服务器特定信息 " （第 357 页）。
❑	12. （视情况而定）如果您在使用 RBPM，请将 User Application 的服务器特定信息从旧服务器更新为新服务器。有关详细信息，请参见第 35.3 节 " 复制驱动程序集的服务器特定信息 " （第 357 页）
❑	13. 将驱动程序更新为包格式。有关详细信息，请参见第 32.8 节 " 升级 Identity Manager 驱动程序 " （第 343 页）。
❑	14. （视情况而定）如果您有自定义的策略和规则，请恢复自定义设置。有关详细信息，请参见第 32.10 节 " 将自定义策略和规则恢复到驱动程序 " （第 346 页）。

	核对清单项目
❑	15. 从驱动程序集中去除旧服务器。有关详细信息，请参见第 32.9.2 节 " 从驱动程序集中去除旧服务器 "（第 345 页）。
❑	16. 激活已升级的 Identity Manager 解决方案。有关详细信息，请参见第 30.6 节 " 激活 Identity Manager"（第 310 页）。

34.2 在迁移期间停止和启动 Identity Manager 驱动程序

在升级或迁移 Identity Manager 时，您需要启动和停止驱动程序，以确保升级或迁移过程能够修改或替换正确的文件。本节包含以下活动。有关详细信息，请参见以下各节：

- 第 9.4.1 节 " 停止驱动程序 "（第 81 页）
- 第 9.4.2 节 " 启动驱动程序 "（第 82 页）

35 将 Identity Manager 迁移到新服务器

本章提供有关从 User Application 迁移到新服务器上的 Identity Applications 的信息。当您无法升级现有安装时，可能还需要执行迁移操作。本章包含以下活动：

35.1 Identity Manager 的迁移核对清单

NetIQ 建议您完成以下核对清单中的步骤。

	核对清单项目
❑	1. 备份 Identity Manager 解决方案的目录和数据库。
❑	2. 确保已安装最新版本的 Identity Manager 组件 （Identity Applications 除外）。有关详细信息，请参见第 5.3.4 节 “ 建议的服务器设置 ”（第 41 页）和组件的最新 《发行说明》。 **注释：**要继续使用当前的 User Application 数据库，请在安装程序中指定现有数据库。有关详细信息，请参见第 15 章 “ 安装 Identity Applications”（第 165 页）。
❑	3. 运行身份库的运行状况检查，以确保纲要可正常扩展。使用 TID 3564075 完成状态检查。
❑	4. 将现有 User Application 驱动程序导入到 Designer 中。
❑	5. 对 Designer 项目存档。它代表驱动程序的迁移前状态。有关详细信息，请参见第 35.2 节 “ 准备要迁移的 Designer 项目 ”（第 356 页）。
❑	6. （视情况而定）要将 Identity Manager 引擎迁移到某个新服务器，请将 eDirectory 复本复制到该新服务器。有关详细信息，请参见第 35.4 节 “ 将 Identity Manager 引擎迁移到新服务器 ”（第 358 页）。
❑	7. 在最新版本的 Designer 中创建一个新 Designer 项目，然后导入 User Application 驱动程序以准备进行迁移。
❑	8. 迁移 User Application 驱动程序。有关详细信息，请参见第 35.5 节 “ 迁移 User Application 驱动程序 ”（第 358 页）。

	核对清单项目
❑	9. 创建新的 Role and Resource Service 驱动程序。 您无法迁移现有的 Role and Resource Service 驱动程序。有关详细信息，请参见第 15.6.3 节 " 创建 Role and Resource Service 驱动程序 " （第 193 页）。
❑	10. 将两个驱动程序部署到身份库。有关详细信息，请参见第 15.6.4 节 " 部署 User Application 的驱动程序 " （第 193 页）。
❑	11. 升级 Identity Applications。有关详细信息，请参见第 32.5 节 " 升级 Identity Applications 和 Identity Reporting" （第 332 页）。
❑	12. 确保您的浏览器不包含先前版本 Identity Manager 的内容。有关详细信息，请参见第 35.7.1 节 " 清理浏览器超速缓存 " （第 360 页）。
❑	13. （视情况而定）恢复 SharedPagePortlet 的自定义设置。有关详细信息，请参见第 35.7.3 节 " 更新 SharedPagePortlet 的最大超时设置 " （第 360 页）。
❑	14. 确保在用户未提供过滤器参数时，搜索组选项不会显示任何信息。有关详细信息，请参见第 35.7.4 节 " 禁用组的自动查询设置 " （第 361 页）。

35.2 准备要迁移的 Designer 项目

在迁移驱动程序之前，您需要执行一些设置步骤，以准备要迁移的 Designer 项目。

注释：如果没有要迁移的现有 Designer 项目，请使用**文件 > 导入 > 项目 （从身份库）**创建一个新项目。

1 起动 Designer。

2 （视情况而定）如果您的某个现有 Designer 项目包含要迁移的 User Application，请备份该项目：

   2a 在 " 项目 " 视图中右键单击该项目的名称，然后选择**复制项目**。

   2b 指定项目的名称，然后单击**确定**。

3 要更新现有项目的纲要，请完成以下步骤：

   3a 在 " 建模器 " 视图中，选择 " 身份库 "。

   3b 选择**在线 > 纲要 > 导入**。

4 （可选）要校验项目中 Identity Manager 的版本号是否正确，请完成以下步骤：

   4a 在 " 建模器 " 视图中，选择 " 身份库 "，然后单击**属性**。

   4b 在左侧导航菜单中，选择**服务器列表**。

   4c 选择一个服务器，然后单击**编辑**。

   Identity Manager 版本字段应显示最新版本。

35.3 复制驱动程序集的服务器特定信息

您必须将储存在每个驱动程序和驱动程序集中的所有服务器特定信息复制到新服务器的信息中。这还包括新服务器中原本没有但需从驱动程序集复制的 GCV 和其他数据。特定于服务器的信息包含于：

- 全局配置值
- 引擎控制值
- 命名口令
- 驱动程序鉴定信息
- 驱动程序启动选项
- 驱动程序参数
- 驱动程序集数据

可以在 Designer 或 iManager 中进行此操作。如果使用 Designer，则这是一个自动过程。如果使用 iManager，则这是手动过程。如果要从版本低于 3.5 的 Identity Manager 服务器迁移到高于或等于版本 3.5 的 Identity Manager 服务器，则应使用 iManager。对于所有其他支持的迁移路径，则可以使用 Designer。

- 第 35.3.1 节 " 在 Designer 中复制服务器特定信息 "（第 357 页）
- 第 35.3.2 节 " 在 iManager 中更改服务器特定信息 "（第 358 页）
- 第 35.3.3 节 " 更改 User Application 的服务器特定信息 "（第 358 页）

35.3.1 在 Designer 中复制服务器特定信息

此过程会影响驱动程序集中储存的所有驱动程序。

1. 在 Designer 中，打开项目。
2. 在**概要**选项卡中，右键单击服务器，然后选择**迁移**。
3. 阅读概述以查看迁移到新服务器的项，然后单击**下一步**。
4. 从可用服务器列表中选择目标服务器，然后单击**下一步**。

   仅列出当前未与驱动程序集相关联且与源服务器的 Identity Manager 版本相同或更高的服务器。
5. 选择以下选项之一：
   - **激活目标服务器：**将源服务器中的设置复制到目标服务器并禁用源服务器上的驱动程序。NetIQ 建议您使用此选项。
   - **保持源服务器处于活动状态：**不要复制设置并禁用目标服务器上的所有驱动程序。
   - **同时激活目标服务器和源服务器：**将源服务器中的设置复制到目标服务器，不禁用源服务器或目标服务器上的驱动程序。不建议使用此选项。如果同时启动了两个驱动程序，则相同信息会写入两个不同队列，这样可能导致损坏。
6. 单击**迁移**。
7. 将更改的驱动程序部署到身份库。

   有关详细信息，请参见《*NetIQ Designer for Identity Manager Administration Guide*》（NetIQ Designer for Identity Manager 管理指南）中的 "Deploying a Driver to an Identity Vault"（将驱动程序部署到身份库）。
8. 启动驱动程序。

   有关详细信息，请参见第 9.4.2 节 " 启动驱动程序 "（第 82 页）。

35.3.2 在 iManager 中更改服务器特定信息

1 在 iManager 中，单击 以显示 “Identity Manager 管理 ” 页面。
2 单击 **Identity Manager 概述**。
3 浏览到并选择保存驱动程序集的容器。
4 单击驱动程序集名称以访问 “ 驱动程序集概述 ” 页。
5 单击驱动程序的右上角，然后单击**停止驱动程序**。
6 单击驱动程序的右上角，然后单击**编辑属性**。
7 将所有包含旧服务器信息的特定于服务器的驱动程序参数、全局配置值、引擎控制值、命名口令、驱动程序鉴定数据及驱动程序启动选项复制或迁移到新服务器的信息中。驱动程序集的全局配置值及其他参数 （比如最大堆大小、 Java 设置等）必须与旧服务器的值相同。
8 单击**确定**保存所有更改。
9 单击驱动程序的右上角以启动驱动程序。
10 对驱动程序集中的每个驱动程序重复步骤 5 到步骤 9。

35.3.3 更改 User Application 的服务器特定信息

您必须重配置 User Application，以便识别新服务器。运行 configupdate.bat。

1 浏览到默认位于 User Application 安装子目录中的配置更新实用程序。
2 在命令提示符下，起动配置更新实用程序 (configupdate.bat)。
3 按第 15.8 章 “ 配置 Identity Applications 的设置 ” （第 204 页）中所述指定值。

35.4 将 Identity Manager 引擎迁移到新服务器

将 Identity Manager 引擎迁移到新服务器时，您可以保留当前在旧服务器上使用的 eDirectory 复本。

1 在新服务器上安装受支持版本的 eDirectory。
2 将位于当前 Identity Manager 服务器上的 eDirectory 复本复制到新服务器。

   有关详细信息，请参见 《*NetIQ eDirectory Administration Guide*》（NetIQ eDirectory 管理指南）中的 “Administering Replicas” （管理复本）。
3 在新服务器上安装 Identity Manager 引擎。

   有关详细信息，请参见第 III 部分 “ 安装 Identity Manager 引擎 ” （第 49 页）。

35.5 迁移 User Application 驱动程序

在升级到新版 Identity Manager 或迁移到另一台服务器时，您可能需要导入 User Application 驱动程序的新基础包，或升级现有包。例如：**User Application 基础包版本 2.2.0.20120516011608**。

当您开始处理某个 Identity Manager 项目时， Designer 会自动提示您将新包导入该项目。到时您也可以手动导入包。

35.5.1 导入新的基础包

1 在 Designer 中打开您的项目。
2 右键单击包编目 > 导入包，然后选择相应的包。
3 （视情况而定）如果 “ 导入包 ” 对话框未列出 User Application 基础包，请完成以下步骤：
   3a 单击 “ 浏览 ” 按钮。
   3b 浏览到 *designer_root*/packages/eclipse/plugins/NOVLUABASE_*version_of_latest_package*.jar。
   3c 单击确定。
4 单击确定。

35.5.2 升级现有的基础包

1 在 Designer 中打开您的项目。
2 右键单击 User Application 驱动程序。
3 单击驱动程序 > 属性 > 包。

   如果基础包可以升级，应用程序将在升级列中显示一个选中标记。
4 对指出有可用升级的包单击选择操作。
5 在下拉列表中，单击升级。
6 选择要升级的目标版本。然后单击 “ 确定 ”。
7 单击应用。
8 在字段中填写适当的信息以升级该包。然后单击下一步。
9 阅读安装摘要。然后单击完成。
10 关闭 “ 包管理 ” 页面。
11 取消选择仅显示适用的包版本。

35.5.3 部署迁移的驱动程序

只有将 User Application 驱动程序部署到身份库后，驱动程序迁移才算完成。迁移后，项目所处的状态只允许部署整个迁移的配置。您无法将任何定义导入迁移的配置。在部署整个迁移配置后，此限制即会消除，您便可以部署各个对象并导入定义。

1 在 Designer 中打开项目，然后对迁移的对象运行 Project Checker。

   有关详细信息，请参见 《*NetIQ Identity Manager - Administrator’s Guide to Designing the Identity Applications*》（NetIQ Identity Manager - Identity Applications 管理员设计指南）中的 “Validating Provisioning Objectss” （验证供应对象）。如果配置存在验证错误，系统会告知您具体错误。只有更正了这些错误，才能部署驱动程序。
2 在大纲视图中，右键单击 User Application 驱动程序。
3 选择部署。
4 对驱动程序集中的每个 User Application 驱动程序重复此过程。

35.6 升级 Identity Applications

在运行 Identity Applications 的升级程序时，请务必注意以下事项：

- 使用以前的 User Application 所用的同一个数据库。“ 之前安装 ” 是指您要迁移的安装。在安装程序中，指定**现有数据库**作为数据库类型。
- 您可为 User Application 环境指定一个不同的名称。
- 指定不同于先前安装的安装位置。
- 指向支持版本的 Tomcat。
- 不要对数据库使用不区分大小写的排序规则。不区分大小写的排序规则不受支持。如果使用不区分大小写的排序规则，则在迁移过程中可能会遇到重复项错误。如果遇到重复键错误，请检查排序规则并更正它，然后重安装 Identity Applications。
- 了解各口令管理提供程序之间的区别。 SSPR 是默认的提供程序。要使用 Identity Manager 的旧式提供程序或使用外部提供程序，您必须在升级后更新 Identity Applications 的配置。有关详细信息，请参见第 4.4 节 “ 使用 Identity Manager 中的自助式口令管理 ” （第 31 页）。

有关升级 Identity Applications 的详细信息，请参见第 32.5 节 “ 升级 Identity Applications 和 Identity Reporting” （第 332 页）。

35.7 完成 Identity Applications 的迁移

在升级或迁移 Identity Applications 后，请完成迁移过程。

35.7.1 清理浏览器超速缓存

登录到 Identity Applications 之前，您应先清理浏览器上的超速缓存。如果不清理超速缓存，您可能会遇到一些运行时错误。

35.7.2 使用旧式提供程序或外部提供程序来管理口令

默认情况下， Identity Manager 会使用 SSPR 进行口令管理。但是，要使用现有的口令策略，您可能需要使用 Identity Manager 内部的旧式提供程序。或者，您也可以使用外部提供程序。有关为这些提供程序配置 Identity Manager 的详细信息，请参见以下其中一节：

- 使用旧版提供程序进行忘记口令管理 （第 201 页）
- 使用外部系统进行忘记口令管理 （第 202 页）

35.7.3 更新 SharedPagePortlet 的最大超时设置

如果您已自定义 SharedPagePortlet 的任何默认设置或首选项，则这些自定义已保存到数据库，并且此设置将被重写。因此，浏览到 “ 身份自助服务 ” 选项卡并不总是高亮显示正确的共享页面。为确保不遇到此问题，请完成以下步骤：

1. 以 User Application 管理员身份登录。
2. 浏览到**管理 > Portlet 管理**。
3. 展开**共享页面导航**。

4 在左侧的 Portlet 树中，单击共享页面导航。

5 在页面的右侧，单击设置。

6 确保最大超时设置为 0。

7 单击 “ 保存设置 ”。

35.7.4 禁用组的自动查询设置

默认情况下，目录提取层中 “ 组 ” 实体的 “DNLookup 显示 ” 处于启用状态。这意味着，每当为组指派打开对象选择器时，无需搜索就会按默认显示所有组。您应该更改此设置，因为用于搜索组的窗口在用户输入搜索内容之前不应显示任何结果。

您可以在 Designer 中取消选中执行自动查询来更改此设置，如下所示：

36 卸装 Identity Manager 组件

本章介绍卸装 Identity Manager 各组件的过程。卸装某些组件需要满足一些先决条件。在开始执行卸装过程之前，请务必查看每个组件的相关完整章节。

注释：在卸装 Identity Manager 组件之前，必须先停止所有服务，例如 Tomcat、 PostgreSQL 和 ActiveMQ。

36.1 卸装身份库

在卸装身份库之前，您必须了解 eDirectory 树型结构和复本布局。例如，您应该了解树中是否包含多个服务器。

1 （视情况而定）如果 eDirectory 树中有多个服务器，请完成以下步骤：

   1a （视情况而定）如果装有 eDirectory 的服务器保存了任何主复本，请在去除 eDirectory 之前，先将复本环中的另一个服务器提升为主服务器。

   有关详细信息，请参见 《*NetIQ eDirectory Administration Guide*》（NetIQ eDirectory 管理指南）中的 "Managing Partitions and Replicas" （管理分区和复本）。

   1b （视情况而定）如果装有 eDirectory 的服务器上的树仅保存了某分区的副本，请将此分区合并到父分区中，或者将此分区的复本添加到其他服务器中并使其成为主复本保存者。

   有关详细信息，请参见 《*NetIQ eDirectory Administration Guide*》（NetIQ eDirectory 管理指南）中的 "Managing Partitions and Replicas" （管理分区和复本）。

   1c 对 eDirectory 数据库执行状态检查。在继续操作之前，请先修复出现的所有错误。

   有关详细信息，请参见 《*NetIQ eDirectory Administration Guide*》（NetIQ eDirectory 管理指南）中的 "Keeping eDirectory Healthy" （保持 eDirectory 稳定运行）。

2 卸装身份库：

   使用用于添加和去除程序的控制面板实用程序。例如，在 Windows Server 2012 R2 上，单击**程序和功能**。右键单击 **NetIQ eDirectory**，然后单击**卸载**。

3 （视情况而定）如果 eDirectory 树中有多个服务器，请完成以下步骤：

   3a 删除树中左侧的所有服务器特定对象。

   3b 再次执行运行状况检查，以校验服务器是否已从树中正确去除。

   有关详细信息，请参见 《*NetIQ eDirectory Administration Guide*》（NetIQ eDirectory 管理指南）中的 "Keeping eDirectory Healthy" （保持 eDirectory 稳定运行）。

36.2 从身份库中去除对象

卸装 Identity Manager 的第一步是删除身份库中的所有 Identity Manager 对象。创建驱动程序集时，向导将提示您将该驱动程序集作为分区。如果有任何驱动程序集对象也是 eDirectory 中的分区根对象，则您必须将该分区合并到父分区，然后才能删除驱动程序集对象。

要从身份库中去除对象，请执行以下操作：

1 在继续操作之前，请对 eDirectory 数据库执行运行状况检查，然后修复出现的所有错误。

   有关详细信息，请参见《*NetIQ eDirectory Administration Guide*》（NetIQ eDirectory 管理指南）中的 "Keeping eDirectory Healthy"（保持 eDirectory 稳定运行）。

2 以对 eDirectory 树具有完全权限的管理员身份登录到 iManager。

3 选择**分区和复本 > 合并分区**。

4 浏览到并选择作为分区根对象的驱动程序集对象，然后单击**确定**。

5 等待合并过程完成，然后单击**确定**。

6 删除驱动程序集对象。

   当您删除驱动程序集对象时，删除过程将删除与该驱动程序集关联的所有驱动程序对象。

7 对 eDirectory 数据库中的每个驱动程序集对象重复步骤 3 到步骤 6，直到将它们全部删除。

8 重复步骤 1 以确保所有合并均已完成，且所有对象均已删除。

36.3 卸装 Identity Manager 引擎

当您安装 Identity Manager 引擎时，安装过程会将一个卸装脚本放到 Identity Manager 服务器上。使用此脚本可以去除安装期间创建的所有服务、包和目录。

注释：在卸装 Identity Manager 引擎之前，请准备好身份库。有关详细信息，请参见第 36.2 节 " 从身份库中去除对象 "（第 363 页）。

要在 Windows 服务器上卸装 Identity Manager 引擎，请使用用于添加和去除程序的控制面板实用程序。例如，在 Windows 2012 R2 上，单击**程序和功能**。右键单击 **Identity Manager**，然后单击**卸载**。

36.4 卸载 Remote Loader

当您安装 Remote Loader 时，安装过程会将一个卸装脚本放到服务器上。使用此脚本可以去除安装期间创建的所有服务、包和目录。

要在 Windows 服务器上卸装 Remote Loader，请使用用于添加和去除程序的控制面板实用程序。

36.5 卸装 Identity Applications

您必须卸装 Roles Based Provisioning Module (RBPM) 的每个组件，例如驱动程序和数据库。

如果您需要卸装与 RBPM 关联的运行时组件，卸装程序将自动重引导服务器，除非您是在 Windows 上以无提示模式运行卸装程序。您必须手动重引导 Windows 服务器。

注释：在卸装 RBPM 之前，请先卸装 Identity Manager 引擎。有关详细信息，请参见第 36.3 节 " 卸装 Identity Manager 引擎 "（第 364 页）。

36.5.1 删除 Roles Based Provisioning Module 的驱动程序

您可以使用 Designer 或 iManager 删除 User Application 驱动程序和 Role and Resource Service 驱动程序。

1 停止 User Application 驱动程序及 Role and Resource Service 驱动程序。根据所用的组件完成以下操作之一：
   - **Designer**：右键单击驱动程序行，然后单击在线 > 停止驱动程序。
   - **iManager**：在 " 驱动程序集概述 " 页面上，单击驱动程序图像的右上角，然后单击停止驱动程序。
2 删除 User Application 驱动程序及 Role and Resource Service 驱动程序。根据所用的组件完成以下操作之一：
   - **Designer**：右键单击驱动程序行，然后单击删除。
   - **iManager**：在 " 驱动程序集概述 " 页面上，单击驱动程序 > 删除驱动程序，然后单击要删除的驱动程序。

36.5.2 卸装 Identity Applications

必须从 Tomcat 中卸装 User Application 及其数据库。本过程介绍了如何从 Tomcat 和 PostgreSQL 中去除 User Application 及其数据库。如果您使用的是其他应用程序服务器和数据库，请参见该产品的文档以获取相关说明。

重要：去除 User Application 时请务必小心，因为该过程会从装有 User Application 脚本和支持文件的文件夹中去除所有文件夹和文件。去除这些文件后，您可能会无意中卸装 Tomcat 或 PostgreSQL。例如，安装文件夹通常为 C:\NetIQ\idm\apps\UserApplication。此文件夹中还包含 Tomcat 和 PostgreSQL 的文件夹。

---

1 登录到安装了 User Application 的服务器。
2 打开用于添加和去除程序的控制面板实用程序。例如，在 Windows Server 2012 R2 上，单击程序和功能。
3 右键单击 **Identity Manager User Application**，然后单击卸载。

36.6 卸装 Identity Reporting 组件

您必须按以下顺序卸装 Identity Reporting 组件：

1. 删除驱动程序。有关详细信息，请参见第 36.6.1 节 " 删除报告驱动程序 "（第 366 页）。
2. 删除 Identity Reporting。有关详细信息，请参见第 36.6.2 节 " 卸装 Identity Reporting"（第 366 页）。
3. 删除 Sentinel。有关详细信息，请参见《NetIQ Identity Manager Setup Guide for Linux》（NetIQ Identity Manager 安装指南 - Linux）中的 "Uninstalling Sentinel"（卸装 Sentinel）。

注释：为了节省磁盘空间， Identity Reporting 的安装程序不会安装 Java 虚拟机 (JVM)。因此，要卸装一或多个组件，请确保您有一个 JVM，同时确保该 JVM 位于 PATH 中。如果在卸装期间遇到错误，请将 JVM 的位置添加到本地 PATH 环境变量中，然后再次运行卸装程序。

36.6.1 删除报告驱动程序

您可以使用 Designer 或 iManager 删除数据收集驱动程序和受管系统网关驱动程序。

1 停止驱动程序。根据所用的组件完成以下操作之一：
   - **Designer**：对于每个驱动程序，请右键单击驱动程序行，然后单击在线 > 停止驱动程序。
   - **iManager**：在 " 驱动程序集概述 " 页面上，单击每个驱动程序图像的右上角，然后单击停止驱动程序。
2 删除驱动程序。根据所用的组件完成以下操作之一：
   - **Designer**：对于每个驱动程序，请右键单击驱动程序行，然后单击删除。
   - **iManager**：在 " 驱动程序集概述 " 页面上，单击驱动程序 > 删除驱动程序，然后单击要删除的驱动程序。

36.6.2 卸装 Identity Reporting

在删除 Identity Reporting 之前，请确保您已删除数据收集驱动程序和受管系统网关驱动程序。有关详细信息，请参见第 36.6.1 节 " 删除报告驱动程序 "（第 366 页）。

重要：在运行 Identity Reporting 卸装程序之前，请确保您已将生成的报告从 Reporting 安装目录复制到计算机上的其他位置，因为卸装过程会从装有 Reporting 的目录中去除所有文件和文件夹。例如，Reporting 安装文件夹 C:\NetIQ\idm\apps\IDMReporting。

要卸装 Identity Reporting，请使用用于添加和去除程序的控制面板实用程序。例如，在 Windows Server 2012 R2 上，单击程序和功能。右键单击 **Identity Reporting**，然后单击卸载。

36.7 卸装 Analyzer

1 关闭 Analyzer。
2 卸装 Analyzer。

   使用用于添加和去除程序的控制面板实用程序。例如，在 Windows Server 2008 上，请单击程序和功能。右键单击 **Analyzer for Identity Manager**，然后单击卸载。

36.8 卸装 iManager

本节介绍了如何卸装 iManager 和 iManager Workstation。您无需遵循特定的顺序来卸装 iManager 或关联的第三方组件。 NetIQ 建议您查看有关卸装其中任一组件的注意事项：

- 如果卸装 Web 服务器或 servlet 容器，就无法运行 iManager。
- 在所有平台上，卸装过程都只会去除最初安装的文件，而不会去除应用程序在运行时所创建的任何文件。例如， Tomcat 运行时创建的日志文件和自动生成的配置文件。
- 卸装过程不会去除创建的任何文件，或者安装期间在目录结构中最初添加而之后被修改的文件。这一操作确保了卸装过程不会无意中删除数据。
- 卸装 iManager 不会影响您在树中已经设置的任何 RBS 配置。卸装过程不会去除日志文件或自定义内容。

重要：在卸装 iManager 之前，请备份所有自定义内容或您要保留的其他特殊 iManager 文件，例如自定义的插件。

36.8.1 在 Windows 上卸装 iManager

要卸装 iManager 组件，请使用用于添加和去除程序的控制面板实用程序。在卸装过程中请注意以下情况：

- 控制面板实用程序会将 Tomcat 和 NICI 与 iManager 分开列出。如果您不再使用这些程序，请将它们卸装。
- 如果 eDirectory 和 iManager 安装在同一台服务器上，请不要卸装 NICI。 eDirectory 需要使用 NICI 来运行。
- 在卸装 iManager 时，程序会询问您是否要去除所有 iManager 文件。如果选择**是**，程序将去除这些文件，包括所有自定义内容。但是，程序不会从 eDirectory 树中去除 2.7 RBS 对象，并且纲要将保持相同的状态。

36.8.2 卸装 iManager Workstation

要卸装 iManager Workstation，请删除将文件解压缩到的目录。

36.9 卸装 Designer

1. 关闭 Designer。
2. 根据操作系统卸装 Designer：

   使用用于添加和去除程序的控制面板实用程序。例如，在 Windows Server 2008 上，请单击**程序和功能**。右键单击 **Designer for Identity Manager**，然后单击**卸载**。

37 查错

本章提供 Identity Manager 安装问题查错的有用信息。有关 Identity Manager 查错的详细信息，请参见具体组件的指南。

37.1 User Application 和 RBPM 安装查错

下表列出了您可能会遇到的问题，以及解决这些问题的建议操作。如果问题仍然存在，请联系 NetIQ 代表。

问题	建议的操作
升级过程不会将默认的 User Application 管理帐户设置为 cn=uaadmin.ou=sa.o=data。 catalina.out 文件中记录了以下错误。 `AuthorizationManagerService [RBPM] Error occured calculating effective rights for attribute: nrfAccessMgrRevokeRole on object: cn=complianceAdmin,cn=System,cn=Level20,cn=RoleDefs,cn=RoleConfig,cn=AppConfig,cn=UserApplication,cn=Driver Set,o=system for trustee: cn=uaadmin,ou=sa,o=data.com.novell.srvprv.spi.security.IDMAuthorizationException: Error occured calculating effective rights for attribute: nrfAccessMgrRevokeRole on object: cn=complianceAdmin,cn=System,cn=Level20,cn=RoleDefs,cn=RoleConfig,cn=AppConfig,cn=UserApplication,cn=Driver Set,o=system for trustee: cn=uaadmin,ou=sa,o=data.at com.novell.idm.security.authorization.ldap.LdapRightsUtil.getPropertyRights(LdapRightsUtil.java:152)` `Unable to fetch roles from edirectory in the predefined time set.`	1. 导航到 setenv.bat 文件，然后在 CATALINA_OPTS 项中将 -Dncpclient_req_timeout 属性的值更改为 *1150*。 2. 重启动 Tomcat。
您要修改安装过程中创建的以下一或多个 User Application 配置设置： ◆ 身份库连接和证书 ◆ 电子邮件设置 ◆ Identity Manager 引擎用户身份和用户组 ◆ Access Manager 或 iChain 设置	在独立于安装程序的情况下运行配置实用程序。 从安装目录 （默认为 C:\NetIQ\idm\apps\UserApplication\）运行以下命令： `configupdate.bat`
启动 Tomcat 会导致以下异常： `port 8180 already in use`	关闭 Tomcat （或其他服务器软件）的可能已在运行的任何实例。如果将 Tomcat 重新配置为使用 8180 以外的其他端口，请编辑 User Application 驱动程序的 config 设置。
当 Tomcat 启动时，应用程序报告称找不到可信证书。	请务必使用安装 User Application 期间指定的 JDK 来启动 Tomcat。

问题	建议的操作
无法登录门户管理页面。	确保存在 User Application 管理员帐户。此帐户与 iManager 管理员帐户不同。
即使使用管理员帐户也无法创建新用户。	User Application 管理员必须是顶层容器的受托者，并且应有主管权限。您可以尝试将 User Application 管理员的权限设置为等效于 LDAP 管理员的权限 （使用 iManager）。
启动应用程序服务器时发生密钥存储区错误。	应用程序服务器未使用安装 User Application 期间指定的 JDK。 使用 keytool 命令导入证书文件： `keytool -import -trustcacerts -alias aliasName -file certFile -keystore ..\lib\security\cacerts -storepass changeit` ◆ 使用为该证书选择的唯一名称替换 *aliasName*。 ◆ 使用证书文件的完整路径和名称替换 *certFile*。 ◆ 默认的密钥储存区口令为 changeit （如果有其他口令，请指定）。
无法发送电子邮件通知。	运行 configupdate 实用程序以检查是否提供了以下 User Application 配置参数的值：**Email From** 和 **Email Host**。 从安装目录 （默认为 C:\NetIQ\idm\apps\UserApplication\）运行以下命令： `configupdate.bat`

37.2 卸装查错

下表列出了您可能会遇到的问题，以及解决这些问题的建议操作。如果问题仍然存在，请联系 NetIQ 代表。

问题	建议的操作
卸装过程报告未完成，但日志文件未显示失败信息。	默认情况下，卸装过程无法删除包含安装文件的 netiq 目录。如果已从计算机中去除所有 NetIQ 软件，则您可以删除该目录。

37.3 登录查错

下表列出了您可能会遇到的问题，以及解决这些问题的建议操作。如果问题仍然存在，请联系 NetIQ 代表。

问题	建议的操作
在大型环境 （超过两百万个对象）中，用户无法登录	在 eDirectory 主服务器和复本服务器中均为 mail(Internet Mail Address) 属性添加索引，并将规则集设置为 Value。
当您从 Identity Applications 页面注销时， SSPR 显示错误 5053 ERROR_APP_UNAVALIABLE。	忽略此错误，它不会导致功能受损。

37.4 排查 SSPR 页面请求错误

下表列出了您可能会遇到的问题，以及解决这些问题的建议操作。如果问题仍然存在，请联系 NetIQ 代表。

问题	建议的操作
SSPR 报告页面请求无序错误 如果在 SSPR 页面中单击**后退**按钮，则会出现此问题。SSPR 在 SSPR 错误日志中显示如下所示的错误顺序讯息： `ERROR, password.pwm.servlet.TopServlet, 5035 ERROR_INCORRECT_REQUEST_SEQUENCE (expectedPageID=3, submittedPageID=4, url=<some sspr url>`	通过 **SSPR 配置管理器 > 设置 > 安全性 > Web 安全性** 禁用 “ 后退 ” 按钮。 **注释：**更改此设置不会对最终用户造成影响。

有关鉴定到或登录 Identity Applications 期间遇到的一般问题，请参见 《*NetIQ Identity Manager - Administrator’s Guide to the Identity Applications*》（NetIQ Identity Manager - Identity Applications 管理员指南）。

A Windows 上的示例 Identity Manager 群集部署解决方案

本附录提供如何在 Windows 2012 R2 平台上的群集环境中配置 Identity Manager 的逐步说明。

A.1 先决条件

Windows 2012 R2 平台上的群集环境中正在运行 eDirectory 8.8.8 SP9 或 9.0.2 或更高版本的服务。有关设置 eDirectory 群集的详细信息，请参见 《*NetIQ eDirectory Installation Guide*》（NetIQ eDirectory 安装指南）中的 "Clustering eDirectory Services on Windows" （在 Windows 上将 eDirectory 服务群集化）。

注释：eDirectory 不支持使用多个群集节点进行负载平衡。eDirectory 群集只用于实现故障转移功能。

A.2 在 eDirectory 群集上配置 NetIQ Identity Manager

本节假设您已设置 eDirectory 群集。

请按照以下过程在 eDirectory 群集环境中配置 Identity Manager。

1. 在主节点上的**群集管理器**中，将 eDirectory 群集角色优先级设置为**不自动启动**。
2. 停止次要节点。
3. 在主节点上，通过在 Identity Manager 安装向导中选择**元目录服务器**选项来安装 Identity Manager 引擎。

   重要：确保您是在本地储存设备上安装 Identity Manager 引擎。

   ---

4. Identity Manager 安装向导会在安装期间停止 eDirectory 群集角色。当此角色停止时，此角色的状态可能会显示为失败。安装后，请从**群集管理器**中启动 eDirectory 群集角色。
5. 为 eDirectory 群集角色设置必要的优先级，并将次要节点设为主动节点。
6. 使用 DCLUSTER_INSTALL 命令在次要节点上安装 Identity Manager 引擎。

   例如 idm_install.exe -DCLUSTER_INSTALL="true"

A.3 Remote Loader 群集化

1. 在主要和次要群集节点上安装 Remote Loader。

注释：对于主要和次要节点，请确保 Remote Loader 安装在相同的共享储存路径上。

2 （视情况而定）如果您与 Remote Loader 之间使用的是安全通讯，请将所有 SSL 证书都储存在共享储存中。

3 在创建 Remote Loader 群集角色前，打开 Remote Loader 控制台并选择 **Remote Loader 作为 Windows 服务**。

4 在**群集管理器 > 角色**中，创建一个新的 Remote Loader 群集角色。

指定该角色的以下信息：

角色类型：一般性服务

选择服务：Remote Loader 实例会注册为 Windows 服务。

名称：群集角色名称

地址：指定唯一的 IP 地址

选择储存：共享群集储存

复制注册表设置：

1. HKEY_LOCAL_MACHINE\SOFTWARE\Novell\RLConsole
2. HKEY_LOCAL_MACHINE\SOFTWARE\Novell\DirXML Remote Loader\Command port 8000

   指定您要群集化的 Remote Loader 实例的注册表路径。
3. HKEY_LOCAL_MACHINE\SOFTWARE\Novell\PassSync

注释：

- 每个群集角色默认只接受一项 Windows 服务。因此，请指定对每个 Remote Loader 实例而言唯一的命令端口和相应的注册表路径。
- Windows 群集不支持 Active Directory 驱动程序的口令过滤器。

B 配置多服务器环境

安装身份库后，您可以配置目录，并使用 DHost 实用程序来创建、启动和停止服务器实例。如果您的服务器已支持 IPv6 地址，则还可以将身份库配置为使用 IPv6 地址。

B.1 修改 eDirectory 树和复本服务器

安装身份库后，您可以使用 DHost 实用程序来配置身份库。要使用 DHost 实用程序，您必须具有管理员权限。当您结合自变量使用此实用程序时，它会验证所有自变量，并提示输入具有管理员权限的用户的口令。如果您不结合自变量使用该实用程序， ndsconfig 将显示实用程序及可用选项的说明。

您还可以使用此实用程序去除 eDirectory 复本服务器以及更改 eDirectory 服务器的当前配置。有关详细信息，请参见第 7.4 章 " 安装后配置身份库 "（第 70 页）。

使用 DHost 实用程序时，请注意以下事项：

- *treename*、 *admin_FDN* 和 *server_FDN* 变量允许的最大字符数如下：
  - *treename*：32 个字符
  - *admin_FDN*：255 个字符
  - *server_FDN*：255 个字符
- 当您在现有树中添加服务器时，如果指定的环境在服务器对象中不存在，则 DHost 实用程序将在添加该服务器时创建相应环境。
- 您可以在安装身份库后向现有树添加 LDAP 和安全服务。
- 要在服务器中启用加密复制，请在用于向现有树添加服务器的命令中包含 -E 选项。有关加密复制的详细信息，请参见 《*NetIQ eDirectory Administration Guide*》（NetIQ eDirectory 管理指南）中的 "Encrypted Replication"（加密复制）。

有关使用 DHost 实用程序修改 eDirectory 的详细信息，请参见 《*NetIQ eDirectory Administration Guide*》（NetIQ eDirectory 管理指南）。

B.2 在身份库中添加新树

在身份库中创建新树时，如果您的身份库服务器原本就支持 IPv6 地址，则可以为新树指定 IPv6 地址。

B.3 在现有树中添加服务器

可以通过运行 eDirectory 安装程序，将服务器添加到现有树中。

B.4 从服务器中去除身份库及其数据库

1 导航到 dsreports 目录。

2 删除您先前使用 iMonitor 创建的 HTML 文件。

B.5 从树中去除 eDirectory 服务器对象和目录服务

使用 DHost 实用程序从树中去除服务器对象和目录服务。有关详细信息，请参见 《*NetIQ eDirectory Administration Guide*》（NetIQ eDirectory 管理指南）。