NetIQ® Identity Manager

安装指南 - Windows

2019 年 10 月

法律声明

有关 NetIQ 法律声明、免责声明、保证条款、出口和其他使用限制、美国政府限制性权限、专利政策以及 FIPS 合规性的信息，请访问 http://www.netiq.com/company/legal/。

版权所有 (C) 2019 NetIQ Corporation。保留所有权利。

目录

关于本书和库 9
关于 NetIQ Corporation 11

I Identity Manager 环境概述 13

1 Identity Manager 组件简介 15

Identity Manager 服务器组件 16
Identity Manager 服务器 17
Remote Loader 17
扇出代理 18
iManager 18
Identity Applications 组件 19
User Application 19
鉴定服务 19
Self-Service Password Reset 19
Web 应用程序服务器 20
Identity Applications 数据库 20
Identity Applications 的驱动程序 20
Identity Reporting 组件 21
Identity Reporting 21
鉴定服务 21
Self-Service Password Reset 21
Identity Reporting 数据库 22
Web 应用程序服务器 22
Identity Reporting 的驱动程序 22
Sentinel Log Management for Identity Governance and Administration 23
Identity Manager 工具 23
Designer for Identity Manager 23
Analyzer for Identity Manager 24
功能体系结构 25
Identity Manager 的部署选项 25
Identity Manager 部署示例 26
高级版部署示例 27
标准版部署示例 29

II 规划 Identity Manager 安装 31

2 计划安装 33

确定硬件要求 33
部署规划工作表 34
确定规模工作表 34
体系结构工作表 35
系统要求工作表 35
查看 Identity Manager 组件使用的端口 36

III 安装和配置 Identity Manager 组件 39

3 安装和配置流程概述 41

安装顺序 41
了解 Identity Manager 服务器、 Identity Applications 及 Identity Reporting 组件的安装和配置流程 41
安装方式类型 42
安装选项 42
配置模式类型 42
在配置期间使用不可猜出的口令 43
了解 Designer 和 Analyzer 的安装过程 43
安装过程 43
安装 Identity Manager 服务器、 Identity Applications 和 Identity Reporting 的先决条件 . . . 43
安装 Remote Loader 45
安装 Java Remote Loader 46
安装 SSPR 47
了解配置设置 48
Identity Manager 引擎的配置工作表 48
Identity Applications 的配置工作表 50
Identity Reporting 的配置工作表 52
Self-Service Password Reset 的配置工作表 53
安装后步骤 54
将 preferIPv4Stack 属性传递给 JVM 54
检查服务器的运行状况 55
监视运行状况统计数字 55
创建复合索引 56
配置 Identity Application 以拒绝客户端发起的 SSL 重新协商 57

4 完成安装的最后步骤 59

配置 Identity Vault 59
手动将 Identity Applications 和 Identity Reporting 证书导入到身份库中 59
配置 Remote Loader 和驱动程序 60
配置忘记口令管理 60
使用 Self Service Password Reset 进行忘记口令管理 60
使用外部系统进行忘记口令管理 62
针对分布式环境或群集环境更新仪表板中的 SSPR 链接 63
配置 Identity Applications 的数据库 64
配置 Oracle 数据库 64
配置 SQL Server 数据库 65
配置 Identity Applications 66
配置 Identity Applications 的设置 66
部署适用于 Identity Applications 的 REST API 87
使用 Oracle 服务名称访问 Oracle 数据库 87
手动创建数据库纲要 87
配置 Identity Applications 的单点登录设置 89
启动 Identity Applications 89
Identity Applications 的配置和用法注意事项 89
配置数据收集的运行时环境 90
将数据收集服务驱动程序配置为从 Identity Applications 收集数据 90
迁移数据收集服务驱动程序 91
添加对自定义属性和对象的支持 93

添加多个驱动程序集支持 96
将驱动程序配置为使用 SSL 在远程模式下运行 97
配置 Identity Reporting 98
在 " 身份数据收集服务 " 页面中手动添加数据源 98
对 Oracle 数据库运行报告 99
手动生成数据库纲要 99
部署 Identity Reporting 的 REST API 102
连接远程 Remote PostgreSQL 数据库 102
激活 Identity Manager 103
查看 Identity Manager 组件使用的端口 103

IV 安装 Designer **107**

5 规划 Designer 安装 **109**

Designer 安装核对清单 109

6 安装 Designer **111**

运行 Windows 可执行文件 111
使用无提示安装过程 111
修改包含空格字符的安装路径 112

V 安装 Analyzer **113**

7 计划 Analyzer 安装 **115**

Analyzer 安装核对清单 115

8 安装 Analyzer **117**

运行 Windows 可执行文件 117
使用无提示安装过程 117

9 安装后任务 **119**

配置已连接系统 119
创建和配置驱动程序集 119
创建驱动程序集 120
将默认口令策略指派给驱动程序集 120
在身份库中创建口令策略对象 120
创建自定义口令策略 121
在身份库中创建默认通知集合对象 121
创建驱动程序 122
定义策略 122
管理驱动程序活动 123
激活 Identity Manager 123

VI 升级 Identity Manager **125**

10 准备升级 Identity Manager **127**

Identity Manager 的升级核对清单 127
了解升级和迁移 129
升级顺序 130
支持的升级路径 130
从 Identity Manager 4.7.x 版本升级 130
从 Identity Manager 4.6.x 版本升级 132
备份当前配置 133
导出 Designer 项目 133
导出驱动程序的配置 134

11 升级 Identity Manager 组件 **137**

升级 Designer 137
升级 Identity Manager 引擎组件 138
升级身份库 138
升级 Identity Manager 引擎 139
升级 Remote Loader 141
升级 Java Remote Loader 142
升级 iManager 142
升级 Identity Applications 144
了解升级程序 145
升级先决条件 145
系统要求 145
升级 PostgreSQL 数据库 145
升级 Identity Applications 的驱动程序包 147
升级 Identity Applications 148
升级后任务 149
升级 Identity Reporting 152
升级先决条件 152
升级 Identity Reporting 152
Reporting 的升级后步骤 153
更改对数据库中的 reportRunner 的参照 153
校验 Identity Reporting 的升级 153
升级 Analyzer 154
停止和启动 Identity Manager 驱动程序 154
停止驱动程序 154
启动驱动程序 155
升级 Identity Manager 驱动程序 156
创建新驱动程序 157
用包的内容替换现有内容 157
保留当前内容并通过包添加新内容 157
将新服务器添加到驱动程序集 158
将该新服务器添加到驱动程序集中 158
从驱动程序集中去除旧服务器 158
将自定义策略和规则恢复到驱动程序 159
使用 Designer 将自定义策略和规则恢复为驱动程序 160
使用 iManager 将自定义策略和规则恢复为驱动程序 160

12 从高级版切换到标准版 161

VII 将 Identity Manager 数据迁移到新安装 163

13 准备迁移 Identity Manager 165

执行迁移的核对清单 165

14 将 Identity Manager 迁移到新服务器 167

Identity Manager 的迁移核对清单 167
准备要迁移的 Designer 项目 168
复制驱动程序集的服务器特定信息 168
在 Designer 中复制服务器特定信息 169
在 iManager 中更改服务器特定信息 170
更改 User Application 的服务器特定信息 170
将 Identity Manager 引擎迁移到新服务器 170
迁移 User Application 驱动程序 171
导入新的基础包 171
升级现有的基础包 171
部署迁移的驱动程序 171
升级 Identity Applications 172
迁移 Identity Applications 172
将数据库迁移到新服务器 172
在新服务器上安装 Identity Applications 173
完成 Identity Applications 的迁移 174
准备 Oracle 数据库以运行 SQL 文件 174
清理浏览器超速缓存 175
更新 SharedPagePortlet 的最大超时设置 175
禁用组的自动查询设置 175

VIII 在 Microsoft Azure 上部署 Identity Manager 177

15 在 Microsoft Azure 上规划和实施 Identity Manager 179

先决条件 179
部署过程 179
创建资源组 181
创建虚拟网络和子网 181
创建应用程序网关 182
创建虚拟机实例 183
更新 VM 中的主机项 184
安装 Designer 185
配置应用程序网关 186

16 混合 Identity Manager 方案示例 189

使用多服务器驱动程序集连接 189
使用 eDirectory 驱动程序连接 190

17 卸装 Identity Manager 组件 **191**

卸装身份库 191
从身份库中去除对象 192
卸装 Identity Manager 引擎 192
卸装 Remote Loader 192
卸装 Identity Applications 193
删除 Roles Based Provisioning Module 的驱动程序 193
卸装 Identity Applications 193
卸装 Identity Reporting 组件 194
删除报告驱动程序 194
卸装 Identity Reporting 194
卸装 Analyzer 195
卸装 iManager 195
在 Windows 上卸装 iManager 195
卸装 iManager Workstation 195
卸装 Designer 196

18 查错 **197**

Identity Manager 引擎查错 197
对 Identity Applications 和 RBPM 安装进行查错 198
安装和卸装查错 200
登录查错 204
排查 SSPR 页面请求错误 206
对 .NET Remote Loader 在 Windows 2016 上不启动的问题查错 207
对在 Azure 部署中装载表单时出现 “502 错误的网关 ” 进行查错 207

IX 部署 Identity Manager 以实现高可用性 **209**

19 在群集环境中安装 Identity Manager 的准备工作 **211**

先决条件 211
身份库 211
Identity Applications 212
Identity Applications 的数据库 212
为 Identity Applications 准备群集 213
了解 Tomcat 环境中的群集组 213
设置工作流程引擎 ID 的系统属性 213
为群集中的每个用户应用程序使用相同的主密钥 213

20 Identity Manager 群集部署解决方案示例 **215**

先决条件 215
在 eDirectory 群集上配置 NetIQ Identity Manager 215
Remote Loader 群集化 215

21 Identity Applications 群集部署解决方案示例 **217**

先决条件 218
安装过程 219
为群集启用许可权限索引 224

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 https://www.netiq.com/communities/。

Identity Manager 环境概述

本指南重点说明您要安装和配置 Identity Manager 所必须完成的任务。开始安装前

如果您是 NetIQ Identity Manager 的新用户，以下章节中的信息将帮助您熟悉该解决方案及其包括的组件。可下载和安装的组件取决于您的 Identity Manager 版本。

- Identity Manager 组件简介
- 功能体系结构

1 Identity Manager 组件简介

我们提供了高级版和标准版 Identity Manager 来满足客户的各种需求。每个版本包括一组特定的功能，而每项功能由多个组件处理。因此，您的 Identity Manager 实施可能包含下列一个或所有组件，具体取决于您的要求：

- Identity Manager 服务器
- Identity Applications
- Identity Reporting
- Identity Manager 工具

图 1-1 列出了 Identity Manager Advanced Edition 环境中部署的组件。

图 1-1 *Identity Manager Advanced Edition 的组件*

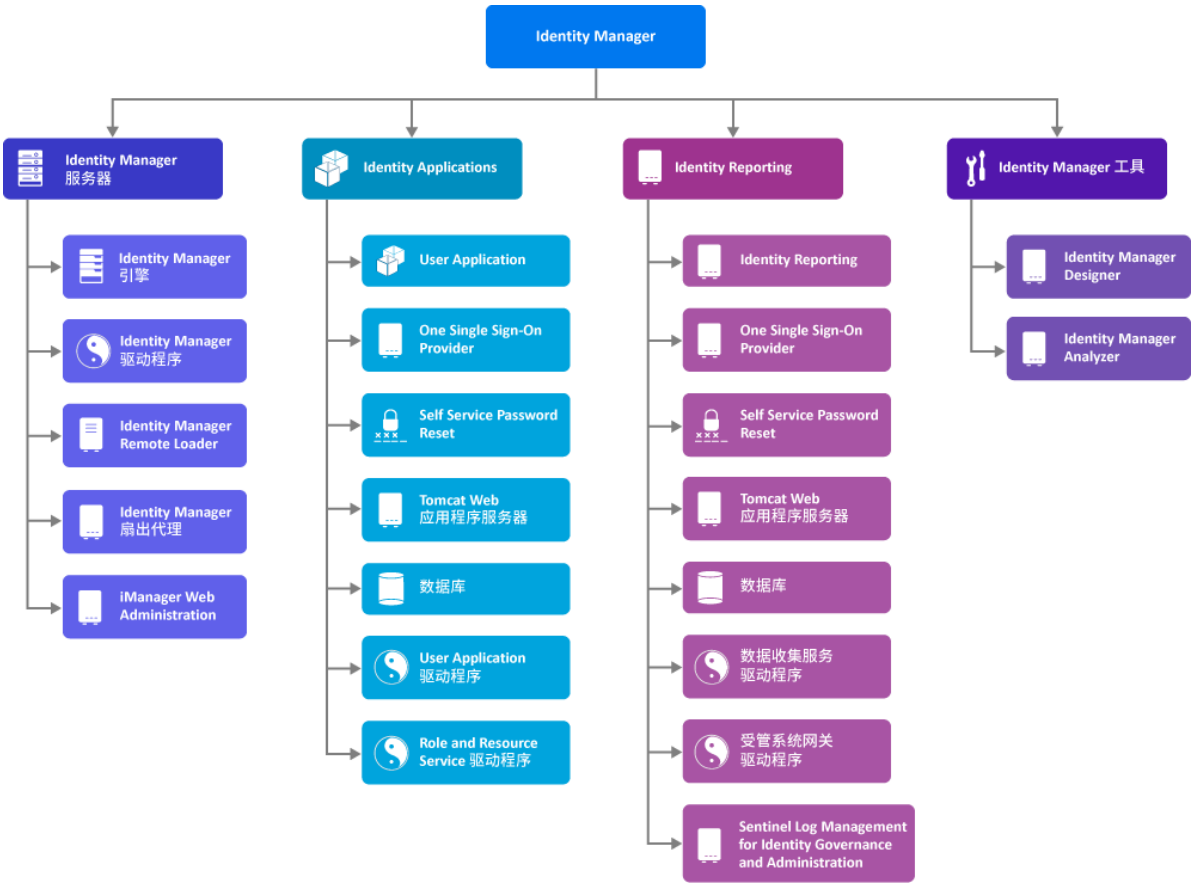
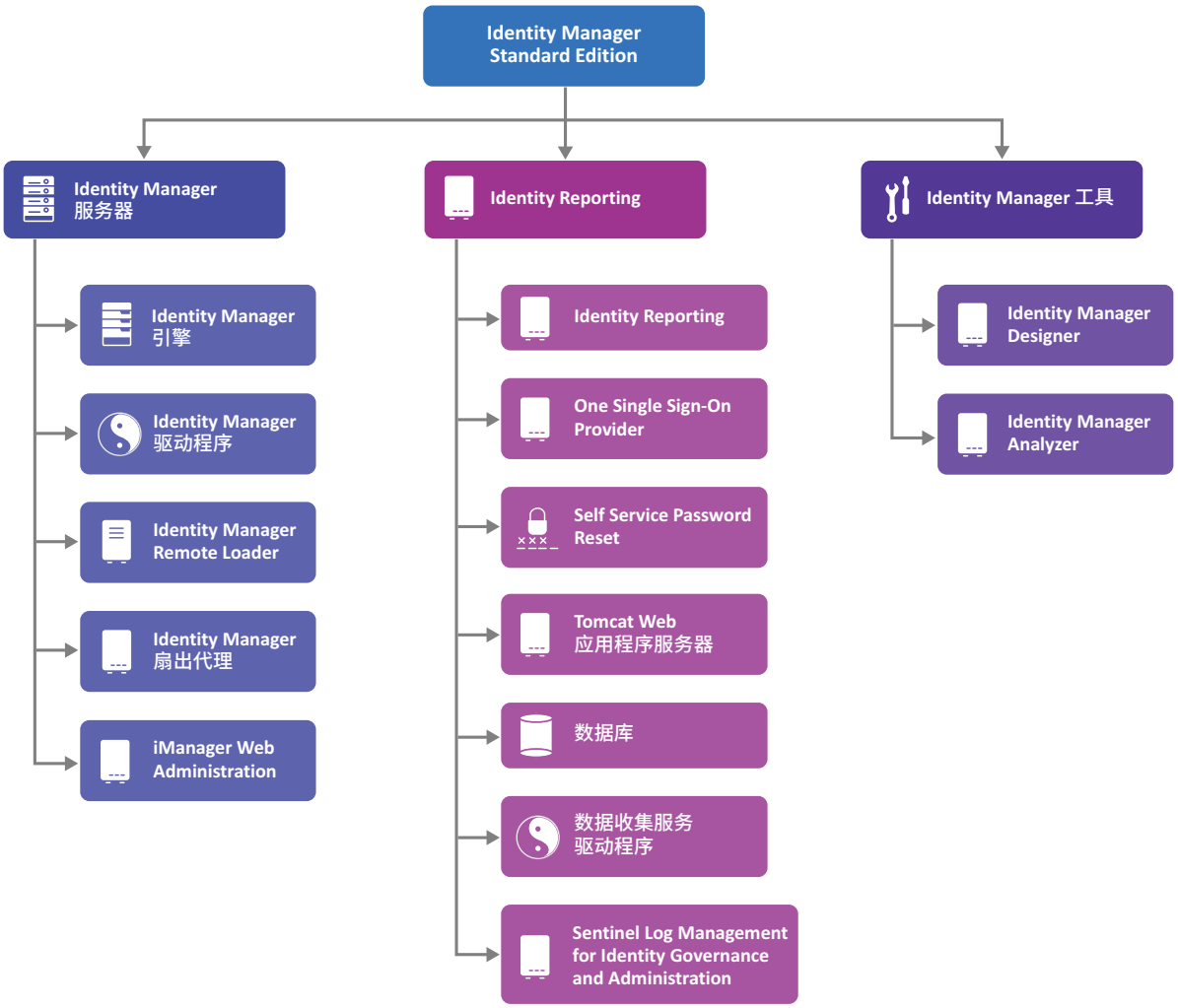


图 1-2 列出了 Identity Manager Standard Edition 环境中部署的组件。

图 1-2 *Identity Manager Standard Edition 的组件*



根据组件之间的交互方式，某些组件在逻辑上以一组组件的形式安装。为了简化安装体验，某些组件作为独立的组件安装。有关组件之间交互方式的信息，请参见 《NetIQ Identity Manager Overview and Planning Guide》（NetIQ Identity Manager 概述和规划指南）。

请查看后续章节中的信息，以了解组件的分组方式，以及每个组件或一组组件的安装方式。

Identity Manager 服务器组件

所有安装必需的组件

Identity Manager 服务器安装包含以下组件。

Identity Manager 服务器

Identity Manager 服务器负责执行 Identity Manager 内的任务。它由身份库、 Identity Manager 引擎和 Identity Manager 驱动程序构成。

为了支持 Identity Manager 服务器运行，安装程序将安装受支持版本的 Oracle Java Runtime Environment (JRE)。要安装 Identity Manager 服务器组件，请使用安装程序的 **Identity Manager 引擎**安装选项。

身份库

当您安装 Identity Manager 引擎时，安装过程将创建并配置与身份库的连接。Identity Manager 使用身份库作为所有身份数据的默认储存库。身份数据包括受管身份 （包括用户帐户和组织数据）的当前状态。

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。用来运行 Identity Manager 引擎的服务器称为 Identity Manager 服务器。

Identity Manager 驱动程序

Identity Manager 服务器处理用户的供应，并通过驱动程序管理已连接系统的帐户和组。驱动程序是已连接系统的软件接口。

Identity Manager 驱动程序作为 Identity Manager 服务器体系结构的一部分运行。驱动程序充当本机端点类型系统技术的网关。例如，仅当已在 Identity Manager 服务器或者可与 Identity Manager 服务器通讯的目标应用程序服务器上安装了 Active Directory 驱动程序时，才能管理运行 Active Directory 服务的计算机。驱动程序会管理驻留在已连接系统上的对象。受管对象包括帐户、组和特定于端点类型的对象 （可选）。

驱动程序会将 Identity Manager 引擎操作转译为已连接系统上的更改，例如 “ 在 Microsoft Exchange 已连接系统上创建新电子邮件帐户 ”。在 Identity Manager 中配置的每个驱动程序都有一个关联的事件超速缓存文件 （TAO 文件）。在驱动程序处理事件之前，这些事件会超速缓存在该超速缓存文件中。超速缓存文件默认存放在身份库的 DIB （数据信息库）目录中。

Identity Manager 提供多个内置驱动程序 （Java、本机、 .NET）来管理与不同类型的已连接系统之间的连接。 Identity Manager 还提供开发定制驱动程序的功能，以使数据能够同步到其他各种系统，例如，组织内部开发的应用程序，或者没有技术接口，因此无法利用现成驱动程序的储存库。

Remote Loader

可以在 Identity Manager 服务器本地安装驱动程序，也可以使用 Remote Loader 来安装。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 《NetIQ Identity Manager Driver Administration Guide》（NetIQ Identity Manager 驱动程序管理指南）中的 “Determining When to Use the Remote Loader”（确定何时使用 Remote Loader）。

使用 **Identity Manager Remote Loader 服务器**安装选项可在 Remote Loader 中安装 Remote Loader 服务和驱动程序实例。

扇出代理

Identity Manager 扇出代理是 Java Database Connectivity (JDBC) 扇出驱动程序用来创建多个 JDBC 扇出驱动程序实例的安装组件。使用扇出驱动程序可以十分轻松地为多个数据库供应用户、组和口令。有了此驱动程序， Identity Manager 管理员就无需再使用相同的策略配置多个 JDBC 驱动程序来供应多个相同类型的数据库。您可以集中管理用户帐户，并在适当的情况下自动创建、配置、维护和去除这些帐户。有关详细信息，请参见 《*NetIQ Identity Manager Driver for JDBC Fanout Implementation Guide*》（NetIQ Identity Manager Driver for JDBC FanOut 实施指南）。

要安装扇出代理，请使用安装程序的 **Identity Manager 扇出代理**安装选项。

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。您可以使用 iManager 来执行各种管理任务，例如，管理您无法在 Identity Manager Identity Applications 中管理的 Identity Manager 服务器选项或驱动程序属性。有关 iManager 的详细信息，请参见 *《NetIQ iManager Administration Guide》*（NetIQ iManager 管理指南）。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。

Identity Manager 要求将 Identity Manager 插件随 iManager 一起安装。 Identity Manager 提供单个安装程序来安装 iManager 客户端和 Identity Manager 插件。您可以在 Identity Manager 服务器或单独的计算机上安装 iManager。

要安装 iManager，请使用安装程序的 “iManager Web Administration” 安装选项。

提示：了解组件后，必须深入了解如何安装和配置组件以在生产环境中使用。

Identity Applications 组件

高级版安装必需的组件

Identity Applications 指一组基于浏览器的互联 Web 应用程序。它们可让您的组织管理用户帐户及与提供给用户的各种角色和资源关联的许可权限。您可以配置 Identity Applications，以便为您的用户提供自助服务支持，例如请求角色或更改他们的口令。您还可以设置工作流程，以提高管理和指派角色与资源的效率。 Identity Applications 由可帮助您执行这些任务的管理控制台 （用于执行管理任务）、用户控制台 （仪表板）和 REST 服务组成。

注释：只有在安装 Identity Manager 引擎之后，才能安装 Identity Applications。

要安装 Identity Applications 组件，请使用安装程序的 **Identity Applications** 安装选项。

Identity Applications 安装包括以下组件：

User Application

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。在本产品的旧版本中使用 User Application 界面执行的部分任务已转移到新用户界面，新界面包括管理控制台和用户控制台。 User Application 将继续提供新用户界面中尚不存在的一些功能。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）。

鉴定服务

鉴定服务提供了访问 Identity Applications 功能的通道。有关在 Identity Manager 中使用单点登录访问的详细信息，请参见 《NetIQ Identity Manager - Administrator's Guide to the Identity Applications》（NetIQ Identity Manager - Identity Applications 管理员指南）。

鉴定服务由 NetIQ One Single Sign-On Provider (OSP) 组件提供。Identity Applications 要求在本地安装 OSP。 OSP 将随 Identity Applications 一起自动安装。

Self-Service Password Reset

自助式口令管理服务可让用户访问自助式口令管理功能。 Identity Applications 中包含 NetIQ Self Service Password Reset (SSPR)，可帮助能够访问 Identity Applications 的用户重设置其口令，而无需管理人员干预。

Identity Applications 安装过程默认会启用 SSPR。但是，如果您的部署需要 SSPR，或者您要安装标准版，您可以选择在单独的计算机上安装 SSPR。如果在高级版中将 SSPR 安装在单独的计算机上，必须在完成这两个组件的安装之后，以手动方式或使用 ConfigUpdate 实用程序在 Identity Applications 配置文件 (ism-configuration.properties) 中定义口令管理设置。

Web 应用程序服务器

该应用程序服务器提供用于执行 Identity Applications 组件的运行时框架。 Identity Applications 将打包成 WAR （Web 应用程序资源或 Web 应用程序存档）文件。安装过程允许您将 WAR 文件部署到应用程序服务器。应用程序服务器运行 Java™ 虚拟机，用于为应用程序代码提供运行时环境。以下 WAR 文件适用于 Identity Applications 组件的 URL：

- **IDMProv** （用于 User Application 界面）
- **idmdash** （用于仪表板）
- **idmadmin** （用于 Identity Applications 管理界面）

当某个用户与 idmdash 或 idmadmin 应用程序交互时，这些应用程序将查询底层 IDMProv.war 文件，并提取该用户的信息。 IDMProv.war 会公开 REST 和 SOAP API，这些 API 的 idmdash 和 idmadmin 包含提供用户界面的信息。

Identity Applications 在安装套件中随附的 Apache Tomcat 应用程序服务器上运行。为了支持 Tomcat 应用程序服务器，安装程序将安装受支持版本的 JRE 和 Apache ActiveMQ。

Identity Applications 数据库

Identity Applications 数据库会维护 Identity Applications 的配置数据，例如本地化的标签、权利值和电子邮件服务器配置。它还会储存工作流程引擎所需的工作流程状态数据。 Identity Applications 支持的数据库包括 PostgreSQL、 Oracle 和 Microsoft SQL Server。

Identity Applications 安装程序会自动安装受支持版本的 PostgreSQL 数据库，该数据库作为 Identity Applications 的默认数据库。如果您不想使用 PostgreSQL 数据库，可以为 Identity Applications 配置受支持版本的 Oracle 或 MS SQL 数据库。 Identity Applications 需要使用 Java Database Connectivity 驱动程序 （JDBC 类型 4 驱动程序）来与数据库通讯。安装程序会提示您提供数据库 JDBC 驱动程序的位置和名称。因此，在开始安装 Identity Applications 之前，必须从数据库安装目录获取此 JDBC 驱动程序。

- 对于 PostgreSQL 数据库，该驱动程序已捆绑在 Identity Manager 安装程序中。
- 对于 Oracle 数据库，可以从 Oracle 网站下载该驱动程序。
- 对于 Microsoft SQL Server 数据库，可以从 Microsoft 网站下载该驱动程序。

数据库可以驻留在 Identity Applications 服务器本地，也可以驻留在远程计算机上。使用远程数据库时，必须配置与该数据库的连接。

Identity Applications 的驱动程序

Identity Applications 组件需要以下驱动程序：

User Application 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 Identity Applications。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

管理所有角色指派、为需要批准的角色指派请求启动相应工作流程，以及根据组和容器成员资格维护间接角色指派。该驱动程序会根据用户的角色成员资格为其授予和撤消权利，以及执行已完成请求的清理过程。该驱动程序除了维护角色请求外，还可维护资源请求。

安装程序的 **Identity Applications** 安装选项会将 User Application 驱动程序以及 Role and Resource Service 驱动程序部署到身份库。

Identity Reporting 组件

（可选）仅当您打算实施报告功能时，才需安装此组件

Identity Reporting 可让您全面了解用户的权利，并会提供所需信息供您了解授予组织中各身份的授权和许可权限的过去和当前状态。 Identity Manager 提供了预定义报告，供您监视 Identity Manager 环境的状态，包括从身份库和已连接系统收集的信息。要将提供的报告与 Identity Manager 搭配使用，需安装 Identity Manager 随附的 Identity Reporting。 Identity Reporting 还提供了一个报告打包工具，可简化自定义报告的创建过程。 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）。

注释：在高级版中安装 Identity Reporting 之前，必须先安装 Identity Applications。

Identity Reporting 安装包括以下组件：

Identity Reporting

基于浏览器的应用程序，用于通过调用报告服务来生成报告。报告服务将从 Identity Reporting 储存库 （身份信息仓库）中检索生成报告所需的数据。 Identity Reporting 储存库中包含所有报告管理信息 （例如报告定义和日程安排）、数据库视图及报告所需的配置信息。

鉴定服务

鉴定服务由 OSP 组件提供。有关详细信息，请参见鉴定服务 （第 19 页）。

注释：OSP 将随 Identity Reporting 一起自动安装。但是，在高级版安装中， Identity Reporting 可以使用随 Identity Applications 一起安装的同一鉴定服务。使用同一鉴定服务时，必须在配置 Identity Reporting 期间指定鉴定设置。

Self-Service Password Reset

自助式口令管理服务可让用户访问自助式口令管理功能。有关详细信息，请参见 Self-Service Password Reset （第 19 页）。

Identity Reporting 数据库

Identity Reporting 数据库 （身份信息仓库）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。您可以基于这些信息生成报告，以查看用户和角色等对象之间的关系。该数据库可以驻留在 Identity Reporting 服务器本地，也可以驻留在远程计算机上。 Identity Manager 使用数据源连接到数据库。 Identity Reporting 需要使用 Java Database Connectivity 驱动程序（JDBC 类型 4 驱动程序）来与数据库通讯。 JDBC 驱动程序使 Identity Reporting 服务器能够与数据源通讯。 Identity Reporting 支持的数据库有 PostgreSQL、 Oracle 和 Microsoft SQL。

- 对于 PostgreSQL 数据库，此驱动程序已捆绑在 Identity Manager 安装程序中。
- 对于 Oracle 数据库，可以从 Oracle 网站下载该驱动程序。
- 对于 Microsoft SQL Server 数据库，可以从 Microsoft 网站下载该驱动程序。

注释：只有在安装 Identity Manager 服务器之后，才能安装 Identity Reporting 组件。

Web 应用程序服务器

该应用程序服务器提供用于执行 Identity Reporting 组件的运行时框架。以下 WAR 文件适用于 Identity Reporting 组件的 URL：

- **IDMRPT** （用于 Identity Reporting 应用程序 / 界面）
- **idmdcs** （用于 Identity Manager 数据收集服务）

当某个用户与 IDMRPT 或 idmdcs 应用程序交互时，这些应用程序将查询报告服务，并提取该用户的信息。报告服务会公开 REST API，这些 API 中的 IDMRPT 和 idmdcs 包含提供用户界面的信息。

有关 Web 应用程序服务器的详细信息，请参见 Web 应用程序服务器 （第 20 页）。

Identity Reporting 的驱动程序

Identity Reporting 组件需要以下驱动程序：

受管系统网关驱动程序

可查询身份库以从受管系统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

数据收集服务驱动程序

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：**使用拉式设计模型收集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。

安装过程的 **Identity Reporting** 安装选项会将受管系统网关驱动程序和数据收集服务驱动程序部署到身份库。

Sentinel Log Management for Identity Governance and Administration

Sentinel Log Management for Identity Governance and Administration (IGA) 是安全信息和事件管理 (SIEM) 系统，可接收来自整个企业中许多来源的信息，并将这些信息标准化、设置它们的优先顺序，然后将其提供给您以便制定与威胁、风险和策略相关的决策。 Sentinel Log Management for (IGA) 可捕获与数个 NetIQ 产品（包括 Identity Reporting、Identity Applications 和身份库）中执行的操作关联的日志事件。这些事件储存在 Identity Reporting 储存库 （身份信息仓库）内的公共纲要中。

Identity Manager 提供单独的 Sentinel Log Management for IGA 安装程序 (SentinelLogManagementForIGA8.2.2.0.tar.gz)。

Identity Manager 工具

所有安装必需的组件

Identity Manager 中包含一组用于简化解决方案实施、自定义和维护的管理工具。其中的一些工具将随 Identity Manager 一起安装，而有些则需要单独安装。

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。

Identity Manager 提供单独的 Designer 安装程序。

Analyzer for Identity Manager

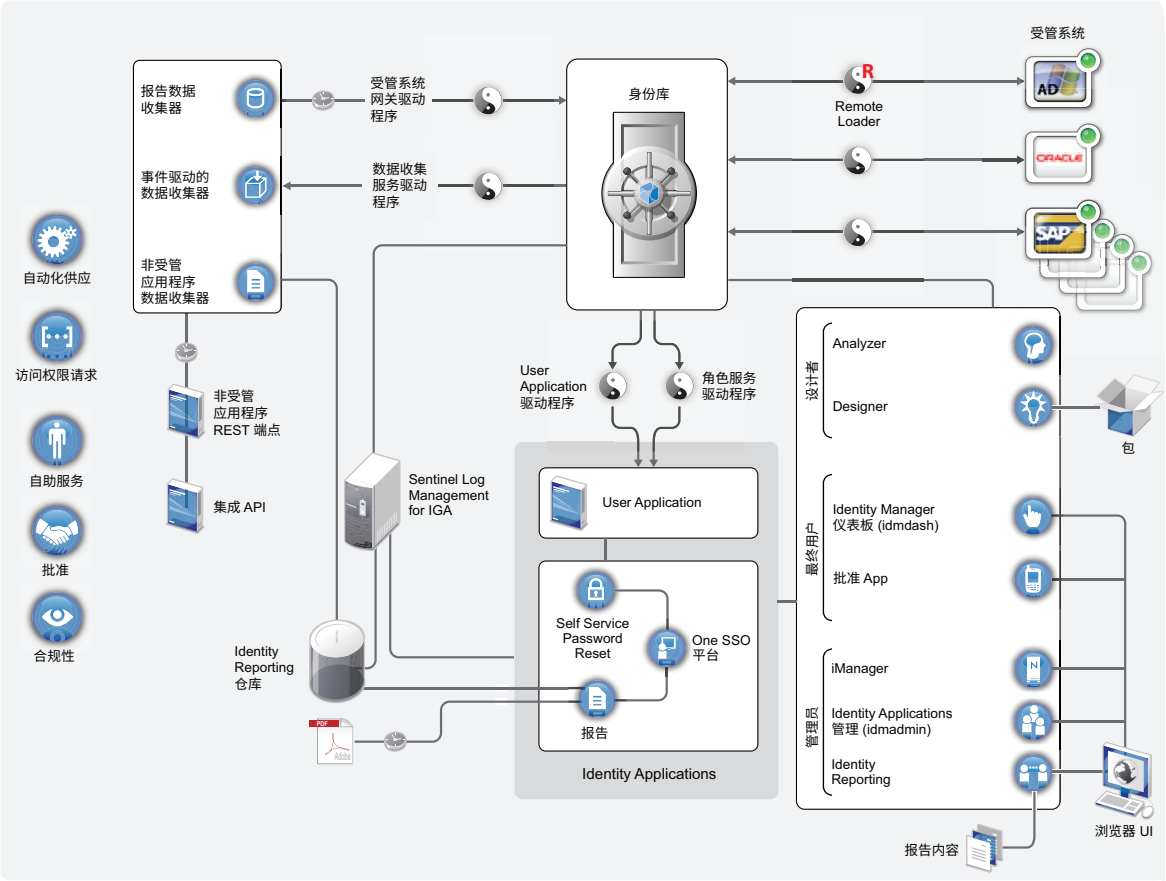
Analyzer for Identity Manager (Analyzer) 提供数据分析、清理、调节和报告，以帮助您遵守内部数据质量策略。Analyzer 允许您分析、增强和控制企业范围内储存的所有数据。Analyzer 包含下列功能：

- 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。

Identity Manager 提供单独的 Analyzer 安装程序。

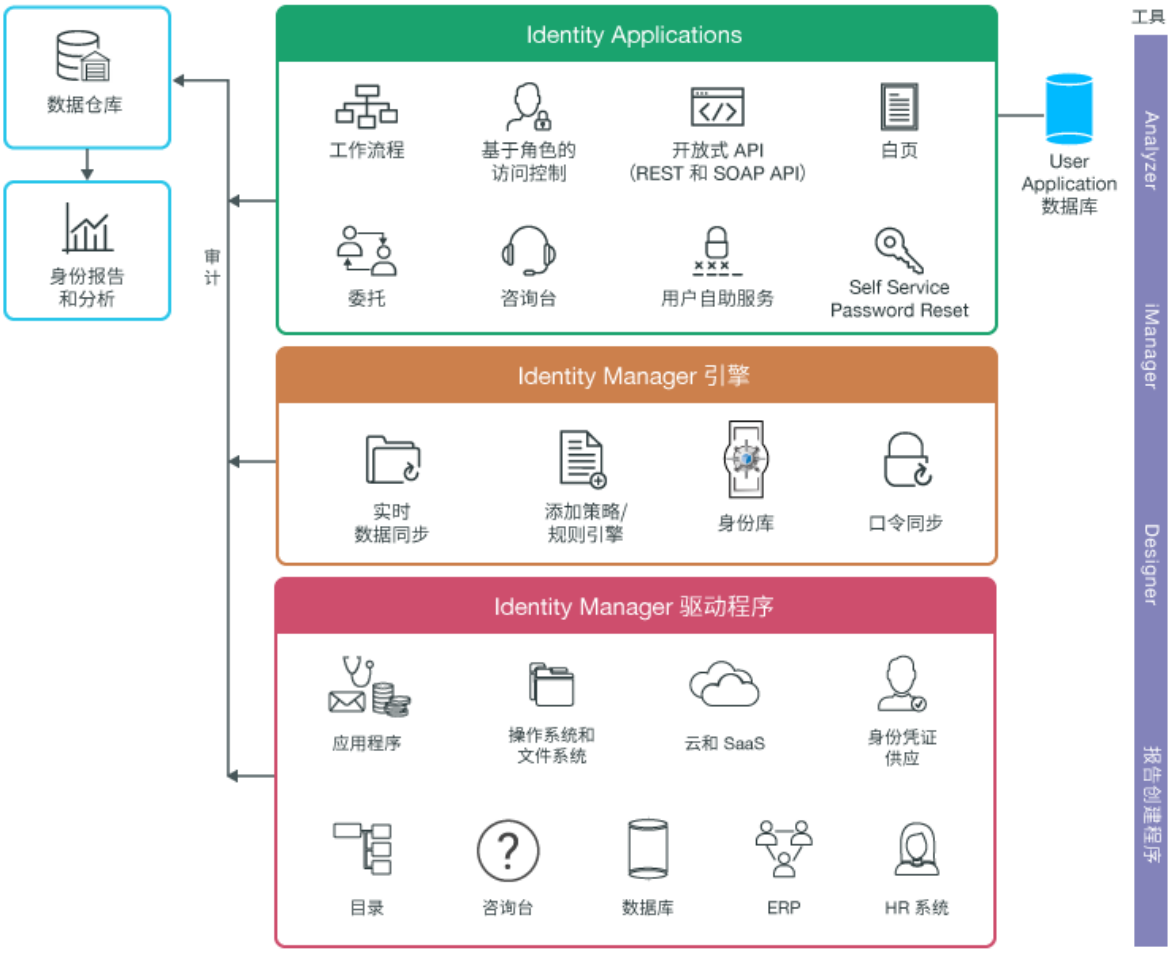
了解 Identity Manager 不同组件的用途及安装方式后，请参见图 1-3 了解组件之间的交互方式。

图 1-3 *Identity Manager 组件之间的交互*



功能体系结构

下图显示了 Identity Manager 组件的基本功能体系结构。此插图并未涵盖所有可能的集成。



有关可能的部署方案的信息，请参见 Identity Manager 的部署选项。

Identity Manager 的部署选项

请查阅下表来规划 Identity Manager 解决方案的物理环境。这些部署用例概括介绍了 Identity Management 物理体系结构，以及组件产品的连接方式、相互通讯及与其他产品通讯的方式。有关 Identity Management 功能体系结构和组件的简介概述，请参见功能体系结构 （第 25 页）。

部署选项	摘要
一台计算机上的单服务器配置	最基本的部署配置包括安装在一台计算机上的 Identity Manager 服务器以及其他必需的应用程序。必须确保该计算机具有所需的内存、速度和可用磁盘空间，以满足工作负载的要求。这是基本的部署用例，基本上只适合用于概念证明 (POC) 和演示目的，可能不适合用于生产环境。

部署选项	摘要
分布式服务器配置	这种部署包括安装在一台计算机上的 Identity Manager 服务器，以及安装在其他一台或多台计算机上的所有其他必需的应用程序。例如，Identity Applications、 iManager、 OSP 和 SSPR 等组件可在单独的计算机上运行。您可以提供一台额外的计算机来托管报告服务的组件，以满足运行 Sentinel Log Management for IGA 组件的系统要求。
高可用性部署	高可用性是一种冗余运行模式。当主服务器发生故障或者需要维护而暂时关闭时，高可用性功能可以自动切换到备用服务器。 Identity Manager 支持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 典型的群集配置包含托管 Identity Applications 以便实现负载平衡和容错的 Tomcat 应用程序服务器节点。所有通讯都通过负载平衡器路由。所有节点均与同一个身份库和 Identity Applications 数据库实例通讯。此配置可缩放。您可以轻松增加节点来处理负载。

Identity Manager 部署示例

Identity Manager 允许您控制用户身份以及他们对已连接系统上的应用程序和帐户的访问权限。请根据所需的功能，选择要安装的 Identity Manager 版本，而这又决定了要安装的组件。下表列出了 Identity Manager Advanced Edition 和 Identity Manager Standard Edition 提供的功能。

特性	高级版	标准版	要安装的组件
基于规则的自动化用户供应	✓	✓	Identity Manager 引擎和 Designer
实时身份同步	✓	✓	Identity Manager 引擎和 Designer
口令管理和口令自助服务	✓	✓	Identity Manager 引擎和 SSPR
统一身份信息工具 (Analyzer)	✓	✓	Analyzer
REST API 和单点登录支持	✓	✓ （仅提供受限制的支持）	Identity Manager 引擎、 OSP 和 Identity Reporting
当前状态报告	✓	✓	Identity Manager 引擎和 Identity Reporting

特性	高级版	标准版	要安装的组件
基于角色的企业级供应	✓	✗	Identity Manager 引擎和 Identity Applications
业务策略执行的自动化批准工作流程	✓	✗	Identity Manager 引擎、 Designer 和 Identity Applications
Identity Applications 中的高级自助服务	✓	✗	Identity Manager 引擎和 Identity Applications
资源模型和编目方便资源供应	✓	✗	Identity Manager 引擎和 Identity Applications
历史状态报告	✓	✗	Identity Manager 引擎和 Identity Reporting
已连接系统报告	✓	✗	Identity Manager 引擎和 Identity Reporting
角色和资源管理	✓	✗	Identity Manager 引擎和 Identity Applications

注释：在所有 Identity Manager 安装中， Identity Manager 服务器是一个中心组件。根据所选的 Identity Manager 版本，将会在 Tomcat 应用程序服务器上仅安装 Identity Reporting，或同时安装 Identity Reporting 和 Identity Applications。请根据需要使用 Identity Manager 组件的专用安装程序来安装其他组件。例如，安装 Designer、 Analyzer 或 Sentinel Log Management for Identity Governance and Administration。

此外，在安装 Identity Manager 之前，请查看实施的目标，并注意物理拓扑选项，例如高可用性和可伸缩性。这有助于确定与贵组织要求相符的配置。

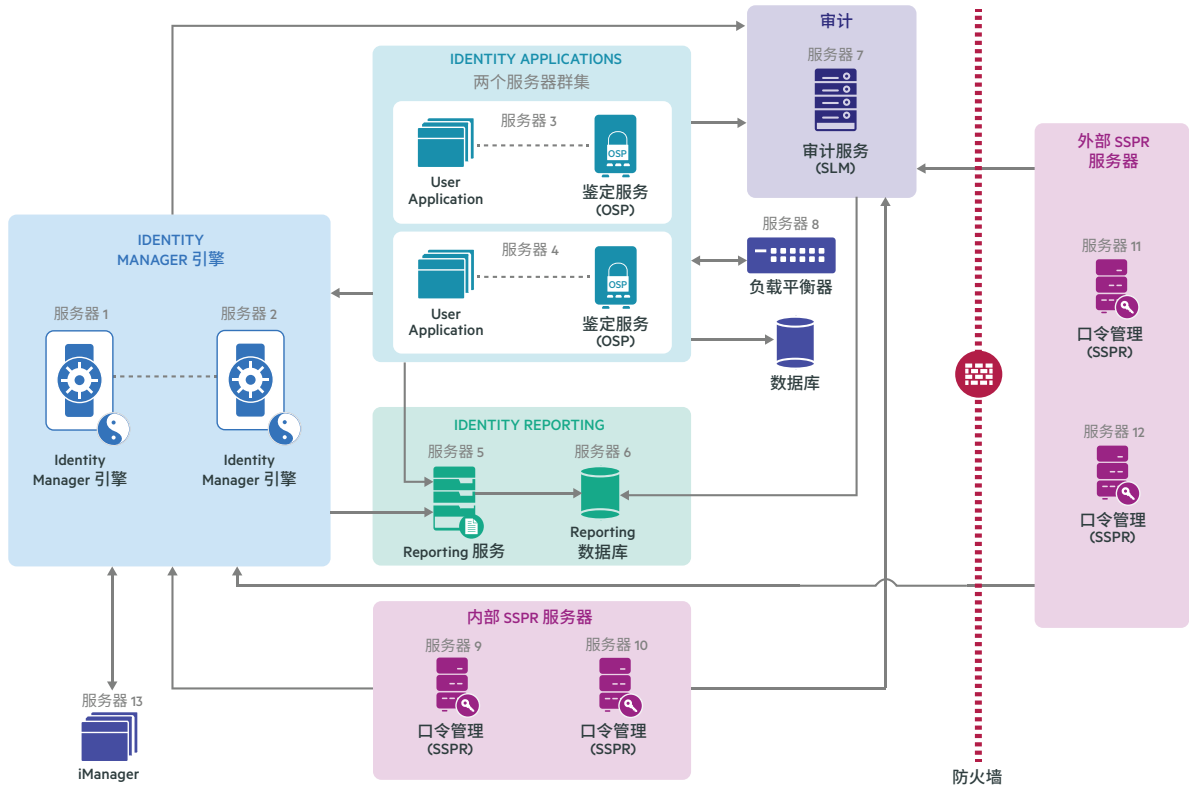
高可用性可确保关键网络资源 （包括数据、应用程序和服务）的高效可管理性。您可以通过减少任何单一故障点及使用冗余组件来实现高可用性。同样，将 Identity Management 组件的多个实例连接到负载平衡器也可以提供高度可用的环境。

本节通过两个示例概要说明高级版和标准版的实施。您可以参考这些示例来设计实施的部署图。

高级版部署示例

图 1-4 显示了 Identity Manager Advanced Edition 安装的概要性部署拓扑。

图 1-4 高级版部署示例



- Identity Manager 服务器组件及其底层储存库 （身份库）和支持 Web 的组件 （Identity Applications 和 Identity Reporting）安装在内部网区域中。负载平衡器将流量路由到 Identity Applications 组件。这种部署可提供增强的安全性，因为防火墙会将这些组件与因特网流量隔离。
- Identity Manager 服务器组件配置为使用双服务器 （主 / 次）配置。作为主节点 （活动）的主服务器上有一个活动的虚拟逻辑 IP 地址，另一台服务器作为次节点。如果主服务器发生故障，该逻辑 IP 地址将转移到次服务器。然后，所有进程都将在次服务器上启动。转移逻辑 IP 地址后，访问次服务器的应用程序进程可能会遇到暂时性的服务中断，而所有其他进程都会启动。在任意时间点，所有组件都使用同一台身份库服务器。
- 防火墙的内部和外部都会提供 SSPR 服务，用于解决组织的本地用户和移动用户的口令管理需求。在防火墙内部安装的服务可解决本地口令管理需求。如果忘记了口令，移动工作人员将无法访问 VPN，这可以防止他们访问在内部部署的 SSPR 服务。他们可以直接访问防火墙外部部署的 SSPR 服务来管理自己的口令。
- User Application 和鉴定服务 (OSP) 部署在群集中，用于处理负载和支持 Identity Applications 的故障转移过程。群集节点挂接到安装在单独计算机上的同一个 Identity Applications 数据库。这种部署允许您向群集添加更多节点，因而提供了更高的可伸缩性。群集配置会立即发送到新增的节点。负载平衡器通常是群集的一部分。它了解群集配置及故障转移策略。在此配置中，所有群集节点在任意时间点均处于活动状态。负载

平衡器会将负载分散到各个节点，以确保每个节点的工作负载大致相同。如果某个节点发生故障，对该节点发出的请求将转移到群集中幸存的节点。由于此安装是一种站点内高可用性解决方案，因此可以在发生本地硬件和软件故障时提供保护，并使用基于双节点硬件的群集来实现 Identity Applications 组件的高可用性。

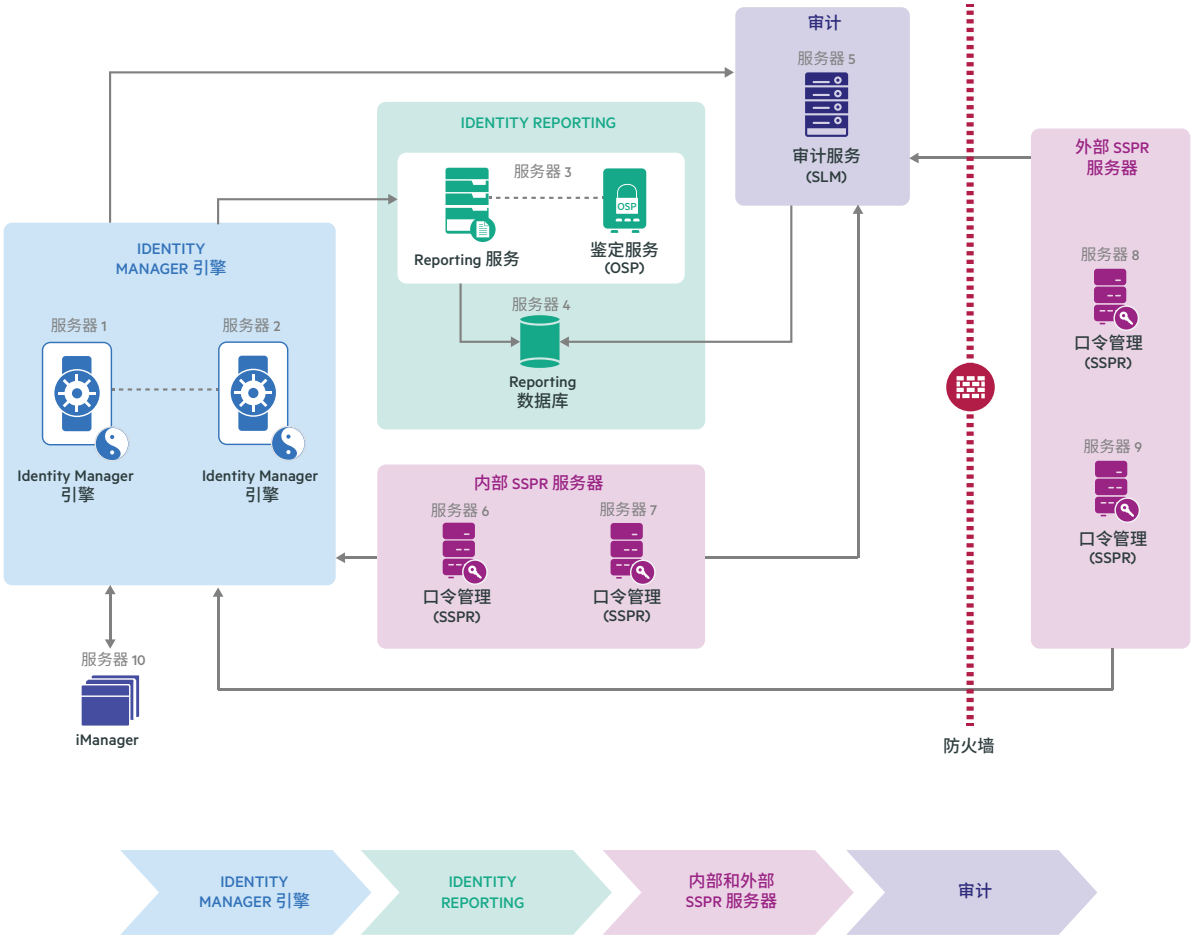
NetIQ 已对此配置进行测试，并建议使用此配置。

注释： Identity Manager 不支持将 Identity Manager 组件群集化。

标准版部署示例

在生产部署中，安全性策略可能会规定不能向公用网络公开用于为您的环境提供高级鉴定和保护的鉴定服务。图 1-5 显示了 Identity Manager Standard Edition 安装的概要性部署拓扑。

图 1-5 *标准版部署示例*



- Identity Manager 服务器组件及其底层储存库 （身份库）和 Identity Reporting 组件安装在内部网区域中。因特网 Web 流量通过安装在防火墙后面的 Web 服务器路由到 Identity Reporting 组件，以增强保护。这种部署可提供增强的安全性，因为防火墙会将这些组件与因特网流量隔离。

- Identity Manager 服务器组件配置为使用双服务器 （主 / 次）配置。作为活动节点的主服务器上有一个活动的虚拟逻辑 IP 地址，另一台服务器作为次节点。如果主服务器发生故障，该逻辑 IP 地址将转移到次服务器。然后，所有进程都将在次服务器上启动。转移逻辑 IP 地址后，访问次服务器的应用程序进程可能会遇到暂时性的服务中断，而所有其他进程都会启动。在任意时间点，所有组件都使用同一台身份库服务器。
- 防火墙的内部和外部都会提供 SSPR 服务，用于解决组织的本地用户和移动用户的口令管理需求。在防火墙内部安装的服务可解决本地口令管理需求。如果忘记了口令，移动工作人员将无法访问 VPN，这可以防止他们访问在内部部署的 SSPR 服务。他们可以直接访问防火墙外部部署的 SSPR 服务来管理自己的口令。

NetIQ 已对此配置进行测试，并建议使用此配置。

注释：Identity Manager 不支持将 Identity Manager 组件群集化。

规划 Identity Manager 安装

根据您希望 Identity Manager 如何管理用户，以及您需要使用哪些功能来实现业务目标，对您的 Identity Manager 实施进行规划。考虑以下要点可帮助您做出决策：

- 我要如何管理身份。
- 我是否需要自动供应。
- 我应使用工作流程实现哪些业务要求。

您做出的决策将会确定按您的要求实施 Identity Manager 的最佳方式。

在大型企业中部署 Identity Manager 之前，需要规划一些额外的任务。有关详细信息，请参见《NetIQ Identity Manager Overview and Planning Guide》（NetIQ Identity Manager 概述和规划指南）中的 “Planning”（规划）一节。

2 计划安装

下表列出了要支持您要实施的功能所需安装的组件。有关安装这些组件的指导，请参见“安装”一节。

功能	要安装的组件
管理公司目录中的用户身份	Identity Manager 服务器
供应已连接系统中的帐户	Identity Manager 服务器
	Identity Applications
	User Application 驱动程序
	Role and Resource Service 驱动程序
	Designer
	注释：有关安装 Identity Manager 驱动程序的指导，请参见 Identity Manager 驱动程序文档网站上适用于您要安装的驱动程序类型的驱动程序实施指南。
鉴定	Identity Manager 服务器
	One Single Sign-On Provider
口令管理	Identity Manager 服务器
	Self Service Password Management
生成有关 Identity Manager 活动的报告	Identity Manager 服务器
	Identity Reporting
	One Single Sign-On Provider

确定硬件要求

Identity Manager 安装所需的硬件取决于两个因素：

- 要实施的功能
- 部署规模

以下部署类型可帮助您预估部署的规模。

部署类型	硬件要求
概念证明 （演示）	单服务器部署，用于在开发环境中进行演示或基本测试。

部署类型	硬件要求
基本	适合中小规模实施的多服务器实施。 此类实施需要使用一台服务器来运行 Identity Manager 服务器及其组件，并使用另外两台服务器来运行 Identity Applications 和 Identity Reporting 组件。
中级	适合中等规模实施的高可用性实施。
大型企业	高可用性实施，包括用于提供故障转移功能的 Identity Manager 引擎群集，以及用于支持单点登录访问 （Windows 上的 OSP）、负载平衡和容错的另一个 Identity Applications 与鉴定服务群集。

部署规划工作表

使用本主题中的信息可了解新的 Identity Manager 实施的细节。

表 2-1 *规划工作表*

规划活动	工作单
根据用例确定实施类型以及决定部署规模	确定规模工作表
设计部署体系结构。列出支持环境所需的物理计算机 / 服务器和其他系统的数量	体系结构工作表
确保您的系统符合系统要求	系统要求工作表
检查网络端口，确定默认端口是否与使用中的端口相冲突	查看 Identity Manager 组件使用的端口

确定规模工作表

正确预估部署的规模非常重要，因为要遵循的步骤和设计要素将因部署规模而异。针对每个组件查看确定规模与可伸缩性注意事项，以了解容量要求。

表 2-2 确定规模工作表

特征	值
物理计算机 / 服务器的数量	
在 Identity Manager 主服务器上运行的驱动程序数量	
在 Identity Manager 次服务器上运行的驱动程序数量	
群集中 Identity Applications 节点的数量	
Identity Applications 数据库的数量	
防火墙内的 Self-Service Password Reset 实例数量	
更多注意事项 ...	

体系结构工作表

确定部署规模后，选择适当的部署，并记录支持该部署所需的物理计算机 / 服务器数量。

表 2-3 体系结构工作表

部署用例
包含所有驱动程序的 Identity Manager 服务器故障转移部署
运行的驱动程序数量
Identity Applications 高可用性部署

系统要求工作表

有关建议的硬件、支持的操作系统和虚拟环境的详细信息，请参见《System Requirements for Identity Manager 4.8》（Identity Manager 4.8 系统要求）。

有关某个特定版本的系统要求信息，请参见 Identity Manager 文档网站上提供的该版本的发行说明。 Identity Manager 实施可能会因您的 IT 环境需求而有所不同，因此您应在最终确定适用于您的环境的 Identity Manager 体系结构之前联系 NetIQ 咨询服务部门或任何 NetIQ Identity Manager 合作伙伴。

查看 Identity Manager 组件使用的端口

各 Identity Manager 组件使用不同的端口来保持相互之间的正常通讯。

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	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
465	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
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。
8109	Identity Applications	仅当使用集成安装过程时适用 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
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

端口号	组件	端口用途
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
5432	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

III 安装和配置 Identity Manager 组件

此部分将指导您完成安装和配置 Identity Manager 组件的过程。有关安装说明，请参阅安装过程 （第 43 页）。

安装 Identity Manager 组件并完成基本配置后，必须执行一些额外的配置步骤，才能让组件完全正常运行。有关详细信息，请参见第 4 章 “ 完成安装的最后步骤 ”（第 59 页）。

3 安装和配置流程概述

本章介绍安装和配置 Identity Manager 组件的流程。在开始配置前，必须查看每个组件的配置选项。有关详细信息，请参见了解配置设置。

某些组件 （例如 Designer 和 Analyzer）可能不需要配置。

安装顺序

必须按以下顺序安装组件，因为一些组件的安装程序需要之前安装的组件的相关信息：

- Sentinel Log Management for Identity Governance and Administration (IGA) （只能安装在 Linux 计算机上）
- Identity Manager 服务器组件
- Identity Applications 组件 （仅适用于高级版）
- Identity Reporting 组件
- Designer for Identity Manager
- Analyzer for Identity Manager

在安装每个组件之前，必须查看该组件的安装先决条件和注意事项。

了解 Identity Manager 服务器、 Identity Applications 及 Identity Reporting 组件的安装和配置流程

Identity Manager 提供基于向导的安装方式来安装和配置 Identity Manager 的下列组件：

- Identity Manager 服务器
- Identity Applications
- Identity Reporting

安装程序允许您以交互或无提示方式来安装和配置组件。安装过程允许您指定所安装组件的值。

安装过程还会在您的文件系统上创建 JRE、Apache Tomcat、PostgreSQL、ActiveMQ 和 OpenSSL 等依赖组件的储存库。如果您将多个 Identity Manager 组件安装在同一台计算机上，安装过程会参照此储存库，而不是为每个需要这些依赖组件的 Identity Manager 组件创建它们的多个副本。例如，如果 Identity Applications 和 Identity Reporting 安装在同一台计算机上，它们会使用同一个 Tomcat。

安装方式类型

Identity Manager 支持交互和无提示安装方式。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。

交互方式

您需要选择要安装的组件。安装程序会根据您的选择安装组件。

无提示方式

您需要在属性文件中指定要安装的组件的值。当您调用安装程序时，它会从属性文件中读取这些值。您可以使用同一个属性文件在环境中的不同计算机上运行无提示安装。

安装选项

下表说明了使用安装程序提供的安装选项将会安装的组件：

表 3-1 *安装选项*

安装选项	安装的组件
Identity Manager 引擎	安装身份库、 Identity Manager 引擎、 Remote Loader 服务、 iManager Web Administrator 和 Identity 插件、扇出代理以及驱动程序。
Identity Applications	安装 Identity Applications、 One SSO Provider (OSP)、 User Application 驱动程序、 Roles and Resource Service 驱动程序 (RRSD)、 PostgreSQL 和 Self Service Password Reset (SSPR)。 **注释：**如果您要在未安装 Identity Applications 的其他服务器上安装 SSPR，请使用 <iso 装入位置 >\common\sspr\ 目录中的 install.exe。
Identity Reporting	安装 Identity Reporting、 OSP、 PostgreSQL、数据收集服务驱动程序 (DCS) 和受管系统网关 (MSG) 驱动程序。

配置模式类型

您可以使用以下方式配置 Identity Manager 组件：

- 典型
- 自定义

典型配置对于大部分配置选项都采用默认设置。在自定义配置中，您可以根据自己的要求指定自定义值。可以使用此选项来配置大部分设置。

在配置期间使用不可猜出的口令

许多 Identity Manager 组件都要求您在配置阶段指定口令。为了更快地完成配置，您可以指示安装过程对所有配置参数应用相同的口令。

该口令必须至少包含六个字符。请不要使用字典中可以找到的单词。免费的口令破解工具使用附带的字典列表很容易就能猜出字典中的单词。如果您必须使用字典中的单词，请尝试将它们与数字和标点符号结合使用。

了解 Designer 和 Analyzer 的安装过程

对于 Designer 和 Analyzer， Identity Manager 提供了不同的 Windows 安装程序。您可在产品下载网站获取 Designer 和 Analyzer 的安装程序。

Designer

可以使用 Identity_Manager_4.8_Windows_Designer.tar.gz 文件安装 Designer。如果要进行无提示安装，请在 designerInstaller.properties 文件中为安装指定相应的值。否则，安装程序将假定使用默认参数值进行安装。

Designer 不需要任何配置。

Analyzer

您可以使用 Identity_Manager_4.8_Windows_Analyzer.tar.gz 文件安装 Analyzer。如果要进行无提示安装，请在 designerInstaller.properties 文件中为安装指定相应的值。否则，安装程序将假定使用默认参数值进行安装。

Analyzer 不需要任何配置。

安装过程

通过阅读此主题可了解 Identity Manager 组件的安装方式。

安装 Identity Manager 服务器、 Identity Applications 和 Identity Reporting 的先决条件

本节将引导您通过交互或无提示方式完成安装 Identity Manager 服务器、 Identity Applications 和 Identity Reporting 组件的整个过程。安装程序中的 **Identity Manager 服务器**选项允许您安装 32 位、 64 位和 .NET Remote Loader。

注释：安装 Identity Manager 引擎之前，请确保已使用最新的 Windows 增补程序更新您的 Windows 服务器，并已重启动 Windows 服务器。

交互式安装

1 从下载网站下载 Identity_Manager_4.8_Windows.iso。

2 装入下载的 iso。

3 根据要安装的组件，运行位于下列位置的 install.exe：

- **Identity Manager 服务器：**<iso 装入位置 >\IdentityManagerServer
- **Identity Applications：**<iso 装入位置 >\IdentityApplications
- **Identity Reporting：**<iso 装入位置 >\IdentityReporting

4 选择安装时要使用的语言，然后单击**确定**。

简介屏幕会显示可供安装的组件。

5 单击**下一步**。

6 阅读并接受许可协议。

7 选择要安装的组件，然后单击**下一步**。

8 指定安装文件夹，然后单击**下一步**。

注释：自定义安装文件夹不得包含特殊字符，例如 . 和 _

---

9 选择安装类型：

- 典型安装
- 自定义安装

10 安装参数将因您选择的安装模式而异。请指定所需细节。有关配置参数的信息，请参见下列表格：

- Identity Manager 引擎设置
- Identity Applications 设置
- Identity Reporting 设置

11 查看“安装前摘要”页面上的细节，然后单击**安装**。

无提示安装

要以无提示方式安装 Identity Manager 组件，请使用 .iso 中相应组件的属性文件。 Identity Manager 媒体中包含一个示例属性文件，位于 <iso 下载位置 >\<*Identity Manager 组件* >\response-files 位置。

要使用无提示方式安装组件，请执行以下操作：

1 从 NetIQ 下载网站下载 Identity_Manager_4.8_Windows.iso。

2 装入下载的 .iso。

3 根据要用来安装组件的安装模式，使用位于以下位置的 typical_install.properties 或 custom_install.properties 文件：

- **Identity Manager 服务器：**<iso 装入位置 >\IdentityManagerServer\response-files
- **Identity Applications：**<iso 装入位置 >\IdentityApplications\response-files

- **Identity Reporting：**<iso 装入位置 >\IdentityReporting\response-files

4 根据需要修改安装参数。有关配置参数的信息，请参见下列表格：

- Identity Manager 引擎设置
- Identity Applications 设置
- Identity Reporting 设置

5 要运行无提示安装，请从组件的目标安装目录运行以下命令：

.\install.exe -i silent -f < *典型或自定义安装属性文件的路径* >

例如：

.\install.exe -i silent -f *C:\Users\Administrator\Desktop typical_install_idmengine.properties*

6 （可选）有关默认安装位置，请参见安装日志。例如，可以查看以下文件：

C:\Program Files\NetIQ\IDM\Install\logs

安装 Remote Loader

Identity Manager 提供了在独立服务器上安装 Remote Loader 的选项。如果您要将 Identity Manager 引擎和 Remote Loader 安装到不同的计算机上，请使用此选项。

注释：可以使用此选项安装 64 位 Remote Loader 和 .NET Remote Loader。要安装 32 位 Remote Loader，请参见安装 Identity Manager 服务器、Identity Applications 和 Identity Reporting 的先决条件。

交互式安装

1 从 NetIQ 下载网站下载 Identity_Manager_4.8_RL_Windows.iso。

2 装入下载的 .iso。

3 从装入位置运行 install.exe 文件。

4 选择安装时要使用的语言，然后单击**确定**。

5 单击**下一步**。

6 阅读并接受许可协议。

7 单击**下一步**。

8 指定安装文件夹，然后单击**下一步**。

9 单击**安装**。

无提示安装

1 从 NetIQ 下载网站下载 Identity_Manager_4.8_RL_Windows.iso。

2 装入下载的 .iso。

3 导航到 <ISO 装入位置 >\response-files。

4 要进行无提示安装，请从属性文件所在的目录运行以下命令：

install.exe -i silent -f install.properties

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 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 从 NetIQ 下载网站下载 Identity_Manager_4.8_Windows.iso。

5 装入下载的 .iso。

6 导航到 <iso 装入位置 >\IdentityManagerServer\products\IDM\java_remoteloader 目录。

7 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。

8 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。

9 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。

10 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\commondrive
rshim.jar;E:\RL\JAVARL\lib\delimitedtextshim.jar;E:\RL\JAVARL\lib\deli
mitedtextutil.jar;E:\RL\JAVARL\lib\dirxml.jar;E:\RL\JAVARL\lib\dirxml_
misc.jar;E:\RL\JAVARL\lib\dirxml_remote.jar;E:\RL\JAVARL\lib\jco3envir
onment.jar;E:\RL\JAVARL\lib\mail.jar;E:\RL\JAVARL\lib\mapdb.jar;E:\RL\
JAVARL\lib\nxsl.jar;E:\RL\JAVARL\lib\shimwrapper.jar;E:\RL\JAVARL\lib\
xds.jar;E:\RL\JAVARL\lib\xp.jar
```

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

12 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。

13 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 《*NetIQ Identity Manager Driver Administration Guide*》（NetIQ Identity Manager 驱动程序管理指南）中的 “Configuring the Remote Loader and Drivers”（配置 Remote Loader 和驱动程序）。

14 使用以下命令起动 Remote Loader：

14a 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
```

14b 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
```

14c 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
```

安装 SSPR

安装程序将提供用于单独安装 SSPR 的选项。如果要将 Identity Applications 和 SSPR 安装在不同的计算机上，请使用此选项。这是唯一可在标准版中安装 SSPR 的选项。安装程序不会在标准版中自动安装 SSPR。

您可以采用交互或无提示方式安装 SSPR。

交互式安装

1. 从 NetIQ 下载网站下载 Identity_Manager_4.8_Windows.iso。
2. 装入下载的 .iso。

3 导航到 <ISO 装入位置 >\common\sspr 目录。

4 运行 install.exe 文件。

5 选择安装时要使用的语言，然后单击**确定**。

6 单击**下一步**。

7 阅读并接受许可协议。

8 单击**下一步**。

9 指定安装文件夹，然后单击**下一步**。

10 指定 SSPR 的配置设置。有关更多信息，请参见 Self-Service Password Reset 的配置工作表（第 53 页）。

11 单击**下一步**。

12 单击**安装**。

无提示安装

1 从 NetIQ 下载网站下载 Identity_Manager_4.8_Windows.iso。

2 装入下载的 .iso。

3 导航到 <ISO 装入位置 >\common\sspr 目录。

4 要进行无提示安装，请从属性文件所在的目录运行以下命令：

install.exe -i silent -f sspr_silentinstall.properties

了解配置设置

使用下面的工作表有助于收集配置 Identity Manager 组件时需要指定的信息。

Identity Manager 引擎的配置工作表

使用下面的工作表有助于收集配置 Identity Manager 引擎时需要指定的信息。

表 3-2 *Identity Manager 引擎设置*

参数	描述
身份库 IDB 位置	指定身份库 IDB 位置。
创建新树	如果要创建新身份库树，请选择此选项。
树名	*仅当您选择了**创建新树**选项时才适用。* 指定身份库树名。
添加到现有树	如果要连接到远程服务器上现有的身份库树，请选择此选项。必须指定 IP 地址，不支持主机名或 FQDN。

参数	描述
主机	*仅当您选择了**添加到现有树**时才适用。* 指定身份库的 IP 地址。
安全 LDAP 端口	*仅当您选择了**添加到现有树**时才适用。* 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。
管理员 DN	指定 Identity Manager 引擎的管理员名称。默认值为 cn=admin,ou=sa,o=system。
管理员口令	指定管理员对象的口令。例如， password。
身份库服务器环境 （使用 LDAP 格式）	指定服务器容器的 DN。默认值为 ou=servers, o=system
身份库驱动程序集 （LDAP 格式）	指定驱动程序集的环境 DN。默认值为 cn=DriverSet, o=system。
明文 LDAP 端口	指定身份库要用来侦听明文 LDAP 请求的端口。默认值为 389。
安全 LDAP 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。默认值为 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。
明文 HTTP 端口	指定 HTTP 堆栈要以明文格式运行的端口。默认值为 8028。
安全 HTTP 端口	指定 HTTP 堆栈采用 TLS/SSL 协议运行的端口。默认值为 8030。
RSA 密钥大小	*仅当您选择了**创建新树**选项时才适用。* 指定 RSA 证书的密钥大小。允许的值为 2048、 4096 和 8192 位。默认值为 4096。
EC 曲线	*仅当您选择了**创建新树**选项时才适用。* 指定 EC 证书的椭圆曲线 (EC) 限制。允许的值为 P256、 P384 和 P521。默认值为 P384。
证书有效期	*仅当您选择了**创建新树**选项时才适用。* 以年为单位指定证书的有效期。
iManager HTTP 端口	指定 Tomcat 应用程序服务器的 HTTP 端口。默认值为 8080。
iManager SSL 端口	指定 Tomcat 应用程序服务器的 HTTPS 端口。默认值为 8443。

Identity Applications 的配置工作表

使用下面的工作表有助于收集配置 Identity Applications 时需要指定的信息。

表 3-3 *Identity Applications 设置*

参数	描述
安装 Self-Service Password Reset	指定是否要安装 SSPR 组件。
主机	指定安装了身份库的服务器的 IP 地址。
安全 LDAP 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。默认值为 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。
管理员 DN	指定 Identity Manager 引擎的管理员名称。默认值为 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。
根容器 DN	指定根容器。默认值为 o=data。
用户容器 DN	*仅在安装新鉴定服务器时适用。* 指定 LDAP 鉴定服务器中用于储存可登录 Access Review 的用户帐户的容器。例如：o=data。
管理员容器 DN	*仅在安装新鉴定服务器时适用。* 指定 LDAP 鉴定服务器中用于储存管理员帐户的容器。
驱动程序集 DN	指定驱动程序集 DN。
部署 Identity Applications 驱动程序	如果要部署 User Application 驱动程序及 Roles and Resource Service 驱动程序，请选择此选项。
选择 Identity Applications 的数据库平台	选择要与 Identity Applications 搭配使用的数据库。选项有 PostgreSQL、 Oracle 和 Microsoft SQL Server。
新 PostgreSQL 服务器	如果要安装新的 PostgreSQL 数据库实例，请选择此选项。
现有 PostgreSQL 服务器	如果要连接到现有的 PostgreSQL 数据库服务器，请选择此选项。
数据库主机	指定服务器的名称或 IP 地址。
数据库端口	指定服务器要用于与 User Application 通讯的端口。该值默认设为 5432。
Identity Applications 数据库名称	指定 Identity Applications 的数据库名称。
工作流程引擎数据库名称	指定工作流程引擎的数据库名称。

参数	描述
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。
数据库用户口令	指定数据库 用户口令。
数据库驱动程序 JAR	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 不支持来自第三方供应商的驱动程序 JAR 文件。
要在何时创建纲要	在安装过程中，指定要在何时创建数据库纲要。可用选项有**现在**、**应用程序启动时**和**将 SQL 写入文件**。
应用程序服务器主机	指定安装了 Tomcat 的服务器的 IP 地址。
应用程序服务器 HTTPS 端口	指定安装了 Tomcat 的服务器的端口。该值默认设为 8543。
登录屏幕名称	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。 升级 Identity Applications 时，登录屏幕名称会自动更改为 NetIQ Access。
Identity Applications 管理员	指定 LDAP 鉴定服务器管理员帐户的 DN。例如，cn=uaadmin,ou=sa,o=data
管理员口令	指定 Identity Applications 管理员口令。
将此口令设为其他设置的通用口令	如果要设置通用口令，请选择此选项。 **注释：**Tomcat 密钥存储区的默认口令为 changeit。
OAuth 密钥存储区口令	*仅当您选中了**将此口令设为其他设置的通用口令**复选框时才适用。* 指定 OAuth 密钥存储区口令。
SSO 客户端口令	*仅当您选中了**将此口令设为其他设置的通用口令**复选框时才适用。* 指定 SSO 客户端口令。
SSPR 配置口令	*仅当您选中了**将此口令设为其他设置的通用口令**复选框时才适用。* 指定 SSPR 配置口令。
表单渲染器 HTTPS 端口	指定表单渲染器 HTTPS 端口。该值默认设为 8600。
工作流程引擎 ID	指定工作流程引擎 ID 的唯一值。

Identity Reporting 的配置工作表

使用下面的工作表有助于收集配置 Identity Reporting 时需要指定的信息。

表 3-4 *Identity Reporting 设置*

参数	描述
主机	指定安装了身份库的服务器的 IP 地址。
安全 LDAP 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。默认值为 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。
管理员 DN	指定 Identity Manager 引擎的管理员名称。默认值为 cn=admin,ou=sa,o=system。
管理员口令	指定 LDAP 鉴定服务器管理员帐户的口令。
用户容器 DN	*仅在安装新鉴定服务器时适用。* 指定 LDAP 鉴定服务器中用于储存可登录 Access Review 的用户帐户的容器。例如：o=data。
管理员容器 DN	*仅在安装新鉴定服务器时适用。* 指定 LDAP 鉴定服务器中用于储存管理员帐户的容器。
驱动程序集 DN	指定驱动程序集 DN。
部署 Identity Reporting 驱动程序	如果您要部署数据收集服务驱动程序和受管系统网关服务驱动程序，请选择此选项。
选择 Identity Reporting 的数据库平台	选择要与 Identity Reporting 搭配使用的数据库。选项有 PostgreSQL、 Oracle 和 Microsoft SQL Server。
新 PostgreSQL 服务器	如果要安装新的 PostgreSQL 数据库实例，请选择此选项。
现有 PostgreSQL 服务器	如果要连接到现有的 PostgreSQL 数据库服务器，请选择此选项。
数据库主机	指定服务器的名称或 IP 地址。
数据库端口	指定服务器要用于与 Identity Reporting 通讯的端口。该值默认设为 5432。
数据库名称	指定 Identity Reporting 的数据库名称。
数据库用户口令	指定数据库 用户口令。
数据库帐户口令	指定 Identity Reporting 的数据库帐户口令。
应用程序服务器主机	指定安装了 Tomcat 的服务器的 IP 地址。

参数	描述
应用程序服务器 HTTPS 端口	指定安装了 Tomcat 的服务器的端口。该值默认设为 8543。
外部 OSP 服务器	如果要连接到外部 OSP 服务器，请选择此选项。例如，如果要连接到 Identity Applications 使用的远程 OSP，请使用此选项。
OSP 服务器主机	*仅当您选择了**外部 OSP 服务器**选项时才适用。* 指定安装了 OSP 的服务器的 IP 地址。
OSP 服务器端口	*仅当您选择了**外部 OSP 服务器**选项时才适用。* 指定 OSP 服务器端口。
OSP 密钥存储区	*仅当您选择了**外部 OSP 服务器**选项时才适用。* 指定 OSP 密钥存储区文件的位置。
OSP 密钥存储区口令	*仅当您选择了**外部 OSP 服务器**选项时才适用。* 指定 OSP 密钥存储区口令。
OSP 客户端口令	*仅当您选择了**外部 OSP 服务器**选项时才适用。* 指定 OSP 客户端口令。
Identity Reporting 管理员	指定 Identity Reporting 的管理员名称。默认值为 cn=uaadmin,ou=sa,o=data。
Identity Reporting 管理员口令	指定 Identity Reporting 的管理员口令。
将此口令设为其他设置的通用口令	如果要设置通用口令，请选择此选项。

Self-Service Password Reset 的配置工作表

使用下面的工作表有助于收集配置 Self-Service Password Reset (SSPR) 时需要指定的信息。

仅当您要将 Identity Applications 和 SSPR 安装到不同的计算机上时，本节内容才适用。

***表 3-5** SSPR 设置*

参数	描述
主机	指定安装了身份库的服务器的 IP 地址。
安全 LDAP 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。默认值为 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。
管理员 DN	指定 Identity Manager 引擎的管理员名称。默认值为 cn=admin,ou=sa,o=system。

参数	描述
管理员口令	指定 LDAP 鉴定服务器管理员帐户的口令。
用户容器 DN	*仅在安装新鉴定服务器时适用。* 指定 LDAP 鉴定服务器中用于储存可登录 Access Review 的用户帐户的容器。例如：o=data。
管理员容器 DN	*仅在安装新鉴定服务器时适用。* 指定 LDAP 鉴定服务器中用于储存管理员帐户的容器。
应用程序服务器主机	指定安装了 Tomcat 的服务器的 IP 地址。
应用程序服务器 HTTPS 端口	指定安装了 Tomcat 的服务器的端口。该值默认设为 8543。
Identity Applications 管理员	指定 LDAP 鉴定服务器管理员帐户的 DN。例如，cn=uaadmin,ou=sa,o=data
管理员口令	指定 Identity Applications 管理员口令。
鉴定服务器主机	指定安装了 OSP 的服务器的 IP 地址。
鉴定服务器 HTTPS 端口	指定 OSP 服务器 HTTPS 端口。
鉴定服务器客户端口令	指定 OSP 客户端口令。

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。

- 将 preferIPv4Stack 属性传递给 JVM （第 54 页）
- 检查服务器的运行状况 （第 55 页）
- 监视运行状况统计数字 （第 55 页）
- 创建复合索引 （第 56 页）
- 配置 Identity Application 以拒绝客户端发起的 SSL 重新协商 （第 57 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"
```

4 完成安装的最后步骤

完成 Identity Manager 组件的安装和配置后，必须执行特定的任务，以使解决方案可在您的环境中正常工作。例如，根据业务流程定义的策略和要求配置安装的驱动程序，以及配置 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：

- 配置 Identity Vault （第 59 页）
- 配置 Remote Loader 和驱动程序 （第 60 页）
- 配置忘记口令管理 （第 60 页）
- 配置 Identity Applications 的数据库 （第 64 页）
- 配置 Identity Applications （第 66 页）
- 配置数据收集的运行时环境 （第 90 页）
- 配置 Identity Reporting （第 98 页）
- 激活 Identity Manager （第 103 页）
- 查看 Identity Manager 组件使用的端口 （第 103 页）

配置 Identity Vault

- 手动将 Identity Applications 和 Identity Reporting 证书导入到身份库中

手动将 Identity Applications 和 Identity Reporting 证书导入到身份库中

- 如果您有 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中的 cacerts (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 -import -trustcacerts -alias <User Application certificate
  alias name> -keystore <cacerts file> -file <User Application
  certificate file>
  ```

- 如果您将 SSPR 安装在未安装 User Application 的其他服务器上，请将 SSPR 应用程序证书导入到 User Application 中的 idm.jks (C:\NetIQ\idm\apps\tomcat\conf\idm.jks)。

  例如，您可以使用以下 keytool 命令将证书导入到 User Application 中：

  ```
  keytool -import -trustcacerts -alias <SSPR certificate alias name> -
  keystore <idm.jks> -file <SSPR certificate file>
  ```

配置 Remote Loader 和驱动程序

利用 Remote Loader， Identity Manager 驱动程序可以访问连接的应用程序，而无需在该应用程序所在的同一台服务器上安装身份库和 Identity Manager 引擎。要使用 Remote Loader，需要配置应用程序 shim，使其能够安全连接到 Identity Manager 引擎。您还必须配置 Remote Loader 和 Identity Manager 驱动程序。《*NetIQ Identity Manager Driver Administration Guide*》（NetIQ Identity Manager 驱动程序管理指南）的 “Configuring the Remote Loader and Drivers”（配置 Remote Loader 和驱动程序）中提供了相关信息。

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 （第 60 页）
- 使用外部系统进行忘记口令管理 （第 62 页）
- 针对分布式环境或群集环境更新仪表板中的 SSPR 链接 （第 63 页）

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 （第 60 页）
- 为 Identity Manager 配置 Self Service Password Reset （第 61 页）
- 锁定 SSPR 配置 （第 61 页）

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. 运行配置更新实用程序。有关更多信息，请参见第 3 节 “ 安装和配置流程概述 ”（第 41 页）。
3. 在实用程序中，导航到**鉴定** > **口令管理**。
4. 对于**口令管理提供程序**，请指定 **Self Service Password Reset (SSPR)**。
5. （可选）要在 Identity Applications 登录页面上提供用于重设置用户名或口令或者激活新用户帐户的链接，请从**用户界面**下拉列表中选择**其他链接**，然后选中所需的复选框。或者，可以通过从**用户界面**下拉列表中选择 “ **无法登录？** ” 来提供通用链接。以下链接将显示在 Identity Applications 登录页面上：**如果您忘记了用户名或口令，或者需要注册，请单击此处。**
6. 导航到 **IDM SSO 客户端** > **Self Service Password Reset**。

7 对于 **OAuth 客户端 ID**，请指定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 **OAuth 客户端机密**，请指定 SSPR 单点登录客户端的口令。

9 对于 **OAuth 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。

注释：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。

---

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 61 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 62 页）
- 测试外部忘记口令配置 （第 63 页）
- 配置应用程序服务器之间的 SSL 通讯 （第 63 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这些值，现在想要修改设置，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 3 节“安装和配置流程概述”（第 41 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 63 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。

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“NetIQ Identity Manager System requirements”（NetIQ Identity Manager 系统要求）页面。

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。

- 配置 Oracle 数据库 （第 64 页）
- 配置 SQL Server 数据库 （第 65 页）

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 NetIQ Identity Manager 技术信息网站。

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：12.2.0.1

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。

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 NetIQ Identity Manager 技术信息网站。

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。

注释：SQL 仅支持 SQL_Latin1_General_CP1_CI_AS 排序规则。

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。

配置 Identity Applications

- 配置 Identity Applications 的设置 （第 66 页）
- 部署适用于 Identity Applications 的 REST API （第 87 页）
- 使用 Oracle 服务名称访问 Oracle 数据库 （第 87 页）
- 手动创建数据库纲要 （第 87 页）
- 配置 Identity Applications 的单点登录设置 （第 89 页）
- 启动 Identity Applications （第 89 页）
- Identity Applications 的配置和用法注意事项 （第 89 页）

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。

- 运行 Identity Applications 配置实用程序 （第 67 页）
- 用户应用程序参数 （第 67 页）
- 报告参数 （第 77 页）
- 鉴定参数 （第 79 页）

- SSO 客户端参数 （第 82 页）
- CEF 审计参数 （第 86 页）

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。

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 （第 67 页）
- 身份库 DN （第 68 页）
- 身份库用户身份 （第 71 页）
- 身份库用户组 （第 72 页）
- 身份库证书 （第 72 页）
- 电子邮件服务器配置 （第 73 页）
- 可信密钥储存区 （第 75 页）
- NetIQ Sentinel 数字签名证书和密钥 （第 75 页）
- 杂项 （第 75 页）
- 容器对象 （第 76 页）

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。

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）。

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。

当 Identity Applications 服务器和电子邮件服务器都设置为使用安全连接时，请确保满足以下条件：

- 用于在 Identity Applications 服务器与电子邮件服务器之间建立安全连接的证书是可信的 CA 证书
- 在映像路径中使用 https。例如 https://localhost:8543/IDMProv/images

如果 Identity Applications 在使用 http 进行纯文本通讯的服务器上运行，请将映像路径中的 https 替换为 http。映像路径的示例：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。

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 77 页）
- 报告保留值 （第 78 页）
- 修改区域设置 （第 78 页）
- 角色配置 （第 78 页）
- 出站代理 （第 78 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**

出站代理

仅当使用 Identity Manager 4.8.1 或更高版本时才适用。

本节定义了要使用供 Identity Reporting 用来下载报告的反向代理服务器所需指定的值。

使用代理

指定该选项会为报告功能使用反向代理服务器。

- **主机名或 IP 地址**
- **Port** （端口）
- **使用 TLS**

  仅当您要使用 TCP 作为网络协议时适用。

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 79 页）
- 鉴定配置 （第 80 页）
- 身份验证方法 （第 80 页）
- 口令管理 （第 81 页）
- Sentinel 数字签名证书和密钥 （第 82 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。

Access Manager 是 OAuth 提供程序

不支持通过配置更新实用程序的 “ 鉴定 ” 选项卡将 OAuth 从 OSP 转换为 NAM。要隐藏此选项，请在 configupdate.sh.properties 文件中将 no_nam_oauth 的值设置为 *"true"*。

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。

Self Service Password Reset (SSPR)： 使用 Identity Applications 随附的 NetIQ Self Service Password Reset 服务，该服务可帮助用户重设置其口令，而无需管理人员干预。您可以选择要在 Identity Applications 仪表板登录页面上显示的链接，使用户能够根据要求选择用于重设置登录访问方式的适当操作。有关更多信息，请参见用户界面 （第 81 页）。

SSPR 是口令管理提供程序字段中的默认选择。

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
```

用户界面

仅当您选择了 Self Service Password Reset (SSPR) 时，此菜单列表才适用。

指定要在 Identity Applications 仪表板的登录页面上显示的链接。默认选择 “ 无法登录？ ” 显示用于重设置用户名或口令，或者在登录页面上注册访问许可权限的通用链接。如果您选择无，则用户无法自行重设置口令。

选择“其他链接”时，以下选项可供选择：

- **忘记口令**：提供一个链接，当现有用户忘记其口令时，可以单击该链接重设置口令。
- **忘记用户名**：提供一个链接，当现有用户忘记其用户名时，可以单击该链接重设置用户名。
- **激活帐户**：提供一个链接，用户可以单击该链接创建用于访问 Identity Applications 的新用户帐户。

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。

SSO 客户端参数

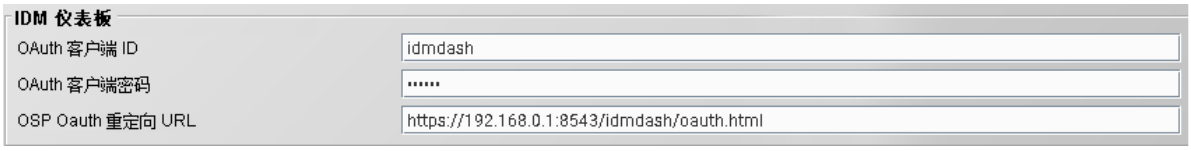
在配置 Identity Applications 时，此选项卡可定义用于管理对应用程序的单点登录访问的值。

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 82 页）
- IDM 管理员 （第 83 页）
- RBPM （第 83 页）
- 报告 （第 84 页）
- IDM 数据收集服务 （第 85 页）
- DCS 驱动程序 （第 85 页）
- Self Service Password Reset （第 86 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。



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 客户端密码

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 客户端密码

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

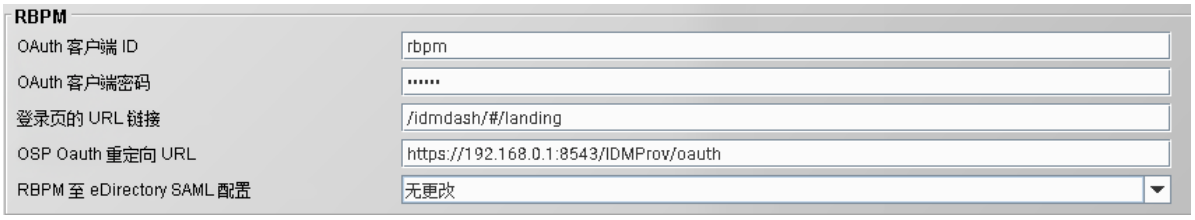
必需

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。



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 客户端密码

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。

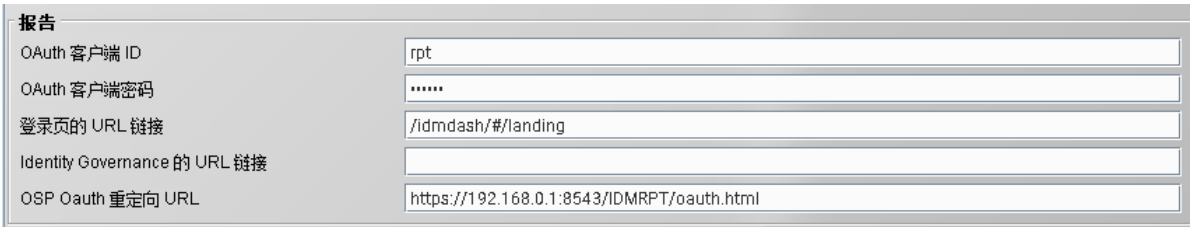
RBPM 至 eDirectory SAML 配置

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。



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 客户端密码

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 客户端密码

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 4-1

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 客户端密码

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 客户端密码

必需

指定 SSPR 单点登录客户端的口令。

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。

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：请确保针对中间事件储存目录设置了 novlua 许可权限。否则，您将不能访问 IDMDash 和 IDMProv 应用程序，并且系统也不会在中间事件储存目录中记录 OSP 事件。例如，您可以使用 chown novlua:novlua <directorypath> 命令更改对该目录的许可权限和所有权，其中， <directorypath> 是中间事件储存目录。

部署适用于 Identity Applications 的 REST API

Identity Applications 组件整合了可在 Identity Applications 中启用不同功能的多个 REST API。REST 服务使用 OAUTH2 协议来提供鉴定。您可以通过浏览器或使用脚本中的 curl 命令来调用这些 API，以实现管理任务自动化。 idmappsdoc.war 文件中提供了 REST API 和相应的文档。安装 Identity Applications 时会自动部署该 war 文件。有关详细信息，请参见 REST API 文档。

要访问安装了 Identity Applications 的服务器上的 REST API 文档，请在浏览器的地址栏中指定 https://<Identity Applications 服务器名称 >:< 端口 >/idmappsdoc。例如 https://192.168.0.1:8543/idmappsdoc。

使用 Oracle 服务名称访问 Oracle 数据库

您可以使用 Oracle 系统 ID (SID) 或 Oracle 服务名称连接到 Oracle 数据库。 Identity Applications 安装程序仅接受 SID。如果要使用服务名称访问数据库，请完成通过 SID 连接将 Identity Applications 安装到一个数据库实例的步骤。完成安装后，请执行以下操作：

1 运行以下命令，在 Oracle 数据库中创建服务名称：

```
alter system set service_names='SERVICE1' scope=both sid='*';
```

其中， SERVICE 1 是 Oracle 服务的名称。

注释：可以使用大写或小写指定服务名称。搜索不区分大小写。

2 在 Tomcat 的 server.xml 文件中修改 Oracle 数据源细节，以定义服务名称：

```
url="jdbc:oracle:thin:@IP:PORT/service1"
```

3 重启动 Tomcat。

4 校验该服务名称是否已包含在 catalina.out 日志文件中。

5 校验 Identity Applications 是否已正确连接到数据库。

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 88 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. （视情况而定）对于 Oracle 数据库，请在函数 CONCAT_BLOB 的定义后面插入一个斜杠 (/)。例如：

```
  -- Changeset icfg-data-load.xml::700::IDMRBPM
CREATE OR REPLACE FUNCTION CONCAT_BLOB(A IN BLOB, B IN BLOB) RETURN BLOB
AS
                C BLOB;
            BEGIN
                DBMS_LOB.CREATETEMPORARY(C, TRUE);
                DBMS_LOB.APPEND(C, A);
                DBMS_LOB.APPEND(C, B);
                RETURN c;
            END;
/
```

7. 让数据库管理员运行该 SQL 脚本，以创建并配置 User Application 数据库。
8. 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 88 页）。

12 在数据库管理员导入该 SQL 文件后，启动 Tomcat。

配置 Identity Applications 的单点登录设置

安装过程会安装用于在 Identity Manager 中进行单点登录访问的鉴定服务 (OSP)。不过，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 的鉴定。要在安装后配置 Identity Applications 的单点登录设置，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 "Configuring Single Sign-on Access in Identity Manager" （在 Identity Manager 中配置单点登录访问）。

启动 Identity Applications

配置 Identity Applications 之后，请务必重启动 Tomcat 和 ActiveMQ 服务。

systemctl restart netiq-tomcat

systemctl restart netiq-activemq

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。

- 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 Identity Reporting 和审计服务，并将其配置为捕获事件。此外，还必须配置 Identity Applications，以便能够进行审计。
- 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。
  - 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。
- 如果您将 Identity Applications 和 SSPR 安装在不同的服务器上，则必须将 CN 为 Identity Applications 的 SSPR 可信证书导入到 Identity Applications 服务器的 cacerts 中。

配置数据收集的运行时环境

本节提供为确保运行时环境正常运行而应执行的额外配置步骤的相关信息。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：

- 将数据收集服务驱动程序配置为从 Identity Applications 收集数据 （第 90 页）
- 迁移数据收集服务驱动程序 （第 91 页）
- 添加对自定义属性和对象的支持 （第 93 页）
- 添加多个驱动程序集支持 （第 96 页）
- 将驱动程序配置为使用 SSL 在远程模式下运行 （第 97 页）

如果一个或多个驱动程序出现了难以解释的问题，请参见 《NetIQ Identity Reporting Module Guide》（NetIQ Identity Reporting Module 指南）中的 *"Troubleshooting the Drivers"*（驱动程序查错）。

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：
   - **3a** 下载最新的 DCS 驱动程序增补程序文件。
   - **3b** 将该增补程序文件提取到服务器上的某个位置。

3c 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
```

3d 重启动身份库。

3e 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。

3f 在 Designer 中重部署并重启动 DCS 驱动程序。

4 在**大纲**视图中，右键单击 DCS 驱动程序，然后选择**属性**。

5 单击“驱动程序配置”。

6 单击**驱动程序参数**选项卡。

7 单击**显示连接参数**，然后选择**显示**。

8 单击 **SSO 服务支持**，然后选择**是**。

9 指定 Identity Reporting 的 IP 地址和端口。

10 指定 SSO 服务客户端的口令。默认口令为 driver。

11 单击**应用**，然后单击**确定**。

12 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**。

13 单击**部署**。

14 出现是否重启动 DCS 驱动程序的提示时，单击**是**。

15 单击**确定**。

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 登录到 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**。

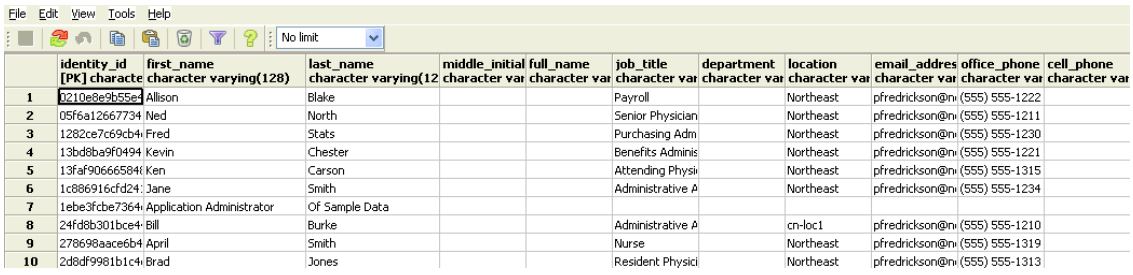
3 选择包含相关数据的组织，然后单击**启动**。

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。

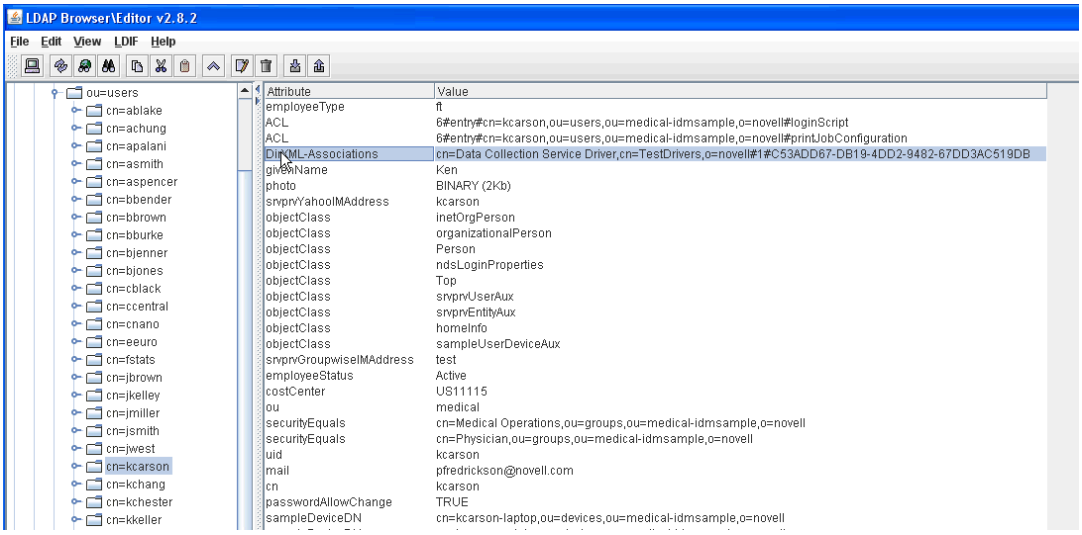
5 确保 **idmrpt_identity** 和 **idmrpt_acct** 表 （提供身份库中身份和帐户的相关信息）中包含以下类型的信息：



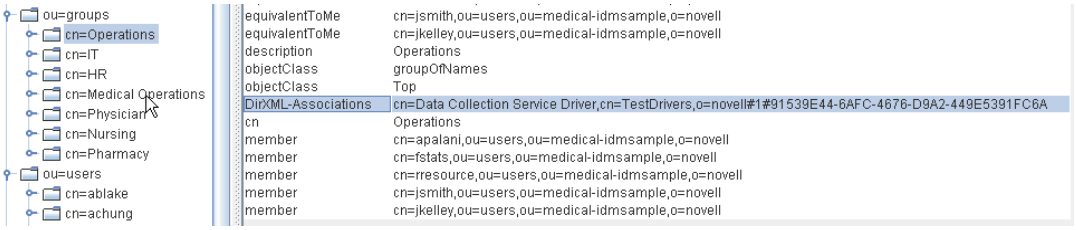
	identity_id [PK] characte	first_name character varying(128)	last_name character varying(12	middle_initial character var	full_name character var	job_title character var	department character var	location character var	email_addres character var	office_phone character var	cell_phone character var
1	0210e8e9b55e4	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	13faf906665846	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 Operatic	Medical Operatic	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。

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 93 页）
- 包含数据库中的名称和说明 （第 94 页）
- 向已知的对象类型添加扩展属性 （第 95 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。

添加多个驱动程序集支持

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：

- **主要** 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。主要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次要驱动程序配合工作。
- **次要** 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，次要数据收集服务驱动程序要求主要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。
- **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 驱动程序选作主要驱动程序。
    - 您需要将其他所有 DCS 驱动程序配置为次要驱动程序。
  - 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 驱动程序都配置为主要驱动程序。

- 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。

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 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 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 中指定的别名。

5e 保存并重启动驱动程序。

配置 Identity Reporting

安装 Identity Reporting 后，您仍可以修改许多安装属性。要进行更改，请运行配置更新实用程序 (configupdate.sh) 文件。

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。

- 在 “ 身份数据收集服务 ” 页面中手动添加数据源 （第 98 页）
- 对 Oracle 数据库运行报告 （第 99 页）
- 手动生成数据库纲要 （第 99 页）
- 部署 Identity Reporting 的 REST API （第 102 页）
- 连接远程 Remote PostgreSQL 数据库 （第 102 页）

在 “ 身份数据收集服务 ” 页面中手动添加数据源

1. 登录 Identity Reporting 应用程序。
2. 单击**数据源**。
3. 单击**添加**。
4. 在**添加数据源**对话框中，单击**从预定义列表中选择**单选按钮。
5. 选择 **IDMDCSDataSource**。
6. 单击**保存**。

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。确保运行 Oracle 数据库的服务器上存在 ojbc8.jar 文件。

手动生成数据库纲要

要在安装后手动生成数据库纲要，请对您的数据库执行下列过程之一：

- 针对 PostgreSQL 数据库配置 Create_rpt_roles_and_schemas.sql 纲要 （第 99 页）
- 针对 Oracle 数据库配置 Create_rpt_roles_and_schemas.sql 纲要 （第 100 页）
- 针对 MS SQL 数据库配置 Create_rpt_roles_and_schemas.sql 纲要 （第 100 页）
- 清除数据库校验和 （第 101 页）

针对 PostgreSQL 数据库配置 Create_rpt_roles_and_schemas.sql 纲要

1. 使用位于 C:\NetIQ\idm\apps\IdentityReporting\sql 中的 create_dcs_roles_and_schemas.sql 和 create_rpt_roles_and_schemas.sql SQL，将必需的角色添加到数据库中。
2. 以 postgres 用户身份登录 PGAdmin。
3. 运行查询工具。
4. 要创建 Create_rpt_roles_and_schemas 和 Create_dcs_roles_and_schemas 过程，请将这些 SQL 中的内容复制到查询工具，然后对连接的数据库执行命令。
5. 要创建 IDM_RPT_DATA、 IDM_RPT_CFG 和 IDMRPTUSER 角色，请按给定的顺序执行以下命令：

   ```
   Select CREATE_DCS_ROLES_AND_SCHEMAS('<Set pwd for IDM_RPT_DATA>', '<Set pwd for IDMRPTUSER>');

   Select CREATE_RPT_ROLES_AND_SCHEMAS('<Set pwd for IDM_RPT_CFG>');
   ```

   例如，如果 IDM_RPT_DATA、 IDMRPTUSER 和 IDM_RPT_CFG 的口令分别是 *password*、*password1* 和 *password2*，则您必须执行以下命令：

   ```
   Select CREATE_DCS_ROLES_AND_SCHEMAS('password', 'password1');

   Select CREATE_RPT_ROLES_AND_SCHEMAS('password2');
   ```

6. 将 C:\NetIQ\idm\apps\IdentityReporting\sql 中 get_formatted_user_dn.sql 的内容复制到查询工具中，然后对连接的数据库执行这些命令。

注释：如果针对数据库纲要创建选项选择文件，必须手动添加 get_formatted_user_dn.sql 函数。如果针对数据库纲要创建选项选择立即或启动，安装程序会将此函数添加到数据库。

针对 Oracle 数据库配置 Create_rpt_roles_and_schemas.sql 纲要

1. 使用 C:\NetIQ\idm\apps\IdentityReporting\sql 中的 create_dcs_roles_and_schemas-orcale.sql 和 create_rpt_roles_and_schemas-orcale.sql，将必需的角色添加到数据库中。
2. 以数据库管理员用户身份登录 SQL Developer。
3. 要创建 Create_rpt_roles_and_schemas 和 Create_dcs_roles_and_schemas 过程，请将这些 SQL 中的内容复制到 SQL Developer，然后对连接的数据库执行命令。
4. 要创建 IDM_RPT_DATA、 IDM_RPT_CFG 和 IDMRPTUSER 角色，请按给定的顺序执行以下命令：

   ```
   begin
   CREATE_DCS_ROLES_AND_SCHEMAS('<Set pwd for IDM_RPT_DATA>', '<Set pwd
   for IDMRPTUSER>');
   end;

   begin
   CREATE_RPT_ROLES_AND_SCHEMAS('<Set pwd for IDM_RPT_CFG>');
   end;
   ```

   例如，如果 IDM_RPT_DATA、 IDMRPTUSER 和 IDM_RPT_CFG 的口令分别是 *password*、*password1* 和 *password2*，则您必须执行以下命令：

   ```
   begin
   CREATE_DCS_ROLES_AND_SCHEMAS('password', 'password1');
   end;

   begin
   CREATE_RPT_ROLES_AND_SCHEMAS('password2');
   end;
   ```

5. 将 C:\NetIQ\idm\apps\IdentityReporting\sql 中 get_formatted_user_dn-oracle.sql 的内容复制到 SQL Developer 中，然后对连接的数据库执行这些命令。

注释：如果针对数据库纲要创建选项选择**文件**，必须手动将 get_formatted_user_dn-oracle.sql 函数添加到数据库。如果针对数据库纲要创建选项选择**立即**或**启动**，安装程序会将此函数添加到数据库。

针对 MS SQL 数据库配置 Create_rpt_roles_and_schemas.sql 纲要

1. 执行 delete_create_dcs_roles_and_schemas-mssql.sql 和 delete_get_formatted_user_dn-mssql.sql。
2. 使用 C:\NetIQ\idm\apps\IdentityReporting\sql 中的 create_dcs_roles_and_schemas.mssql 和 create_rpt_roles_and_schemas.mssql，将必需的角色添加到数据库中。
3. 以数据库管理员用户身份登录 SQL Developer。
4. 要创建 Create_rpt_roles_and_schemas 和 Create_dcs_roles_and_schemas 过程，请将 create_dcs_roles_and_schemas.mssql 和 create_rpt_roles_and_schemas.mssql 中的内容复制到 SQL Developer，然后对连接的数据库执行这些命令。
5. 要创建 IDM_RPT_DATA、 IDM_RPT_CFG 和 IDMRPTUSER 角色，请按给定的顺序执行以下命令：

execute CREATE_DCS_ROLES_AND_SCHEMAS '< 设置 IDM_RPT_DATA 的口令 >', '< 设置 IDMRPTUSER 的口令 >'

execute CREATE_DCS_ROLES_AND_SCHEMAS '< 设置 IDM_RPT_DATA 的口令 >', '< 设置 IDMRPTUSER 的口令 >'

6 将 C:\NetIQ\idm\apps\IdentityReporting\sql 中 get_formatted_user_dn.sql 的内容复制到 SQL Developer 中，然后对连接的数据库执行这些命令。

清除数据库校验和

1 在 C:\NetIQ\idm\apps\IdentityReporting\sql 中找到下列 .sql 文件。

- 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

2 清除数据库校验和

2a 要使用每个 .sql 运行 clearchsum 命令，请将下面一行附加到每个文件的开头：

```
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;
```

2b 以相应的用户身份运行每个 .sql。

3 将更改提交到数据库。

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 和 dcsdoc war。

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。要允许进行远程 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。

激活 Identity Manager

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。有关详细信息，请参见 《*NetIQ Identity Manager Overview and Planning Guide*》（NetIQ Identity Manager 概述和规划指南）中的 “Activating Identity Manager”（激活 Identity Manager）。

查看 Identity Manager 组件使用的端口

Identity Manager 组件使用多个端口来相互通讯。这些端口默认已在防火墙中打开。要查看 Identity Manager 组件使用的端口，请参见 《*NetIQ Identity Manager Security Guide*》（NetIQ Identity Manager 安全性指南）中的 “Understanding Identity Manager Communication”（了解 Identity Manager 通讯）。

```
kind: PersistentVolume
apiVersion: v1
metadata:
  name: task-pv-volume
  labels:
    type: nfs
spec:
  storageClassName: manual
  capacity:
    storage: 3Gi
  accessModes:
    - ReadWriteMany
  hostPath:
    path: '/mnt'
---
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: task-pv-claim1
spec:
  storageClassName: manual
  accessModes:
    - ReadWriteMany
  resources:
    requests:
      storage: 1Gi
---
apiVersion: v1
kind: Pod
metadata:
```

```
  labels:
    name: identity-engine
  name: identity-engine
spec:
  nodeSelector:
    kubernetes.io/hostname:
  hostNetwork: true
  containers:
    -
      image: <image name>
      name: identity-engine-container
      resources:
        limits:
            cpu: "2"
            memory: 4Gi
        requests:
            cpu: "1"
            memory: 1Gi
      volumeMounts:
        - name: data
          mountPath: /config
      env:
      - name: UPGRADE_IDM
        value:
      - name: IS_ADVANCED_EDITION
        value:
      - name: INSTALL_ENGINE
        value:
      - name: INSTALL_IDVAULT
        value:
      - name: IS_COMMON_PASSWORD
        value:
      - name: COMMON_PASSWORD
        value:
      - name: TREE_CONFIG
        value:
      - name: ID_VAULT_PASSWORD
        value:
      - name: ID_VAULT_EXISTING_SERVER
        value:
      - name: ID_VAULT_EXISTING_NCP_PORT
        value:
      - name: ID_VAULT_EXISTING_LDAPS_PORT
        value:
      - name: ID_VAULT_EXISTING_CONTEXTDN
        value:
      - name: ID_VAULT_TREENAME
        value:
      - name: ID_VAULT_ADMIN_LDAP
        value:
      - name: ID_VAULT_ADMIN
        value:
      - name: ID_VAULT_PASSWORD
        value:
      - name: ID_VAULT_VARDIR
```

```
      value:
    - name: ID_VAULT_DIB
      value: '
    - name: ID_VAULT_NCP_PORT
      value:
    - name: ID_VAULT_LDAP_PORT
      value:
    - name: ID_VAULT_LDAPS_PORT
      value:
    - name: ID_VAULT_HTTP_PORT
      value:
    - name: ID_VAULT_HTTPS_PORT
      value:
    - name: ID_VAULT_CONF
      value:
    - name: ID_VAULT_DRIVER_SET
      value:
    - name: ID_VAULT_DEPLOY_CTX
      value:
    - name: ID_VAULT_SERVER_CONTEXT
      value:
volumes:
  - name: data
    persistentVolumeClaim:
      claimName: task-pv-claim1
```

IV 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。例如，不要将其命名为 Designer Install，但可以命名为 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 5 章 “ 规划 Designer 安装 ”（第 109 页）。

5 规划 Designer 安装

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。

- Designer 安装核对清单 （第 109 页）

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. 查看规划信息。有关更多信息，请参见第 II 部分 “ 规划 Identity Manager 安装 ” （第 31 页）。
❑	2. 查看安装 Designer 的注意事项，以确保计算机符合先决条件。
❑	3. 要安装 Designer，请参见以下章节之一： • 运行 Windows 可执行文件 （第 111 页） • 使用无提示安装过程 （第 111 页）
❑	4. 安装其余的 Identity Manager 组件。
❑	5. （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）。

6 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。

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。

- 运行 Windows 可执行文件 （第 111 页）
- 使用无提示安装过程 （第 111 页）
- 修改包含空格字符的安装路径 （第 112 页）

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_4.8_Designer_Windows.zip。
3. 解压缩 Identity_Manager_4.8_Designer_Windows.zip 文件。
4. 导航到 designer_install 文件夹。
5. 运行 install.exe 文件。
6. 遵循向导中的步骤操作，直到完成安装过程。

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 打开默认位于 *Path_to_unzipped_Designer_file*\designer_install 目录中的 designerInstaller.properties 文件。

   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 从属性文件所在目录运行以下命令：

install -i silent -f designerInstaller.properties

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
```

V 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。

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 Analyzer 安装核对清单（第 115 页）。

7 计划 Analyzer 安装

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。

- Analyzer 安装核对清单 （第 115 页）

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. 查看规划信息。有关更多信息，请参见第 II 部分 “ 规划 Identity Manager 安装 ” （第 31 页）。
❑	2. 查看安装 Analyzer 的注意事项，以确保计算机符合先决条件。
❑	3. 要安装 Analyzer，请参见以下章节： ◆ 要使用安装向导，请参见运行 Windows 可执行文件 （第 117 页）。 ◆ 对于无提示安装，请参见使用无提示安装过程 （第 117 页）
❑	4. 要激活 Analyzer，请参见 《*NetIQ Identity Manager Overview and Planning Guide*》（NetIQ Identity Manager 概述和规划指南）中的 “Activating Analyzer” （激活 Analyzer）。

8 安装 Analyzer

本章将指导您完成安装 Analyzer 并为 Analyzer 配置环境的过程。

- 运行 Windows 可执行文件 （第 117 页）
- 使用无提示安装过程 （第 117 页）

运行 Windows 可执行文件

1. 使用管理员帐户登录到要安装 Analyzer 的计算机。
2. 从 NetIQ 下载网站下载 Identity_Manager_4.8_Analyzer_Windows.zip。
3. 解压缩 Identity_Manager_4.8_Analyzer_Windows.zip 文件。
4. 导航到 analyzer_install 文件夹。
5. 运行 install.exe 文件。
6. 遵循向导中的步骤操作，直到完成安装过程。

使用无提示安装过程

您可以使用脚本以无提示方式安装 Analyzer，此过程无需用户交互。除非您编辑了 analyzerInstaller.properties 文件，否则指定 -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 Analyzer 的计算机。
2. 浏览到包含安装程序的目录。
3. （可选）要配置 Analyzer 的安装目录和语言，请完成以下步骤。

   3a 打开默认位于 *Path_to_unzipped_Analyzer_file*\analyzerInstall 目录中的 analyzerInstaller.properties 文件。

   3b 在该属性文件中，修改以下参数的值：

   USER_INSTALL_DIR

   指定要安装 Analyzer 的位置的路径。例如：

   ```
   USER_INSTALL_DIR=C:\analyzer
   ```

   如果指定的路径不是以 analyzer 目录结尾，Analyzer 安装程序会自动追加 analyzer 目录。

   SELECTED_ANALYZER_LOCALE

   指定以下语言之一，作为 Analyzer 安装完成后起动时使用的语言：

   - 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 从属性文件所在目录运行以下命令：

```
install -i silent -f analyzerInstaller.properties
```

9 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：

- 配置已连接系统 （第 119 页）
- 创建和配置驱动程序集 （第 119 页）
- 创建驱动程序 （第 122 页）
- 定义策略 （第 122 页）
- 管理驱动程序活动 （第 123 页）
- 激活 Identity Manager （第 123 页）

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。

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。每次只能将一个驱动程序集关联到任一服务器。您可以使用 Designer 工具来创建驱动程序集。如果已将某个服务器关联到某个驱动程序集，然后将该服务器指派到新的驱动程序集，则会从原始驱动程序集中去除该服务器。

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。

- 创建驱动程序集 （第 120 页）
- 将默认口令策略指派给驱动程序集 （第 120 页）
- 在身份库中创建口令策略对象 （第 120 页）
- 创建自定义口令策略 （第 121 页）
- 在身份库中创建默认通知集合对象 （第 121 页）

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）。

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，请参见在身份库中创建口令策略对象 （第 120 页）和创建自定义口令策略 （第 121 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。

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。

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，请参见在身份库中创建口令策略对象 （第 120 页）。

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。

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。

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。

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。

激活 Identity Manager

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。有关详细信息，请参见 《*NetIQ Identity Manager Overview and Planning Guide*》（NetIQ Identity Manager 概述和规划指南）中的 “Understanding Licensing and Activation”（了解许可和激活）。

VI 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 VII 部分“ 将 Identity Manager 数据迁移到新安装 ”（第 163 页）。有关升级与迁移之间区别的详细信息，请参见了解升级和迁移（第 129 页）。

10 准备升级 Identity Manager

本章提供的信息可帮助您做好将 Identity Manager 解决方案升级到最新版本的准备工作。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。

警告：您必须始终通过 Identity Manager 增补程序渠道来更新随 Identity Manager 4.8 安装的组件。否则，您在进行日常的 Identity Manager 增补程序更新期间，可能会遇到严重的冲突。

- Identity Manager 的升级核对清单 （第 127 页）
- 了解升级和迁移 （第 129 页）
- 升级顺序 （第 130 页）
- 支持的升级路径 （第 130 页）
- 备份当前配置 （第 133 页）

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，请参见了解升级和迁移 （第 129 页）。
❑	2. 升级到 Identity Manager 4.6.4。您无法将低于 4.6.4 的版本升级或迁移到 4.8 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。有关详细信息，请参见 《*NetIQ Identity Manager Overview and Planning Guide*》（NetIQ Identity Manager 概述和规划指南）中的 “Where to Get Identity Manager” （从何处获取 Identity Manager）。
❑	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。
❑	5. 备份当前的项目、驱动程序配置和数据库。有关详细信息，请参见备份当前配置 （第 133 页）。
❑	6. 将 Designer 升级到最新版本。有关详细信息，请参见升级 Designer （第 137 页）。
❑	7. 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：**安装过程 （第 43 页） • **升级：**升级 iManager （第 142 页）

	核对清单项目
❑	8. 在运行 Identity Manager 的服务器上，将 eDirectory 升级到最新版本和增补程序。
❑	9. 更新 iManager 插件，使之与 iManager 的版本匹配。有关更多信息，请参见在升级或重安装后更新 iManager 插件 （第 144 页）。
❑	10. 停止与安装了 Identity Manager 引擎的服务器关联的驱动程序。有关更多信息，请参见停止和启动 Identity Manager 驱动程序 （第 154 页）。
❑	11. 升级 Identity Manager 引擎。有关详细信息，请参见升级 Identity Manager 引擎 （第 139 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，请参见将 Identity Manager 引擎迁移到新服务器 （第 170 页）。
❑	12. （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，请参见升级 Remote Loader （第 141 页）。
❑	13. （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，请参见升级 Identity Manager 驱动程序 （第 156 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。
❑	14. （视情况而定）如果未安装 SSPR，请加以安装。有关更多信息，请参见安装 SSPR （第 47 页）。
❑	15. 升级 Identity Applications。有关更多信息，请参见升级 Identity Applications （第 144 页）。
❑	16. 升级 Identity Reporting。有关更多信息，请参见升级 Identity Reporting （第 152 页）。
❑	17. 启动与 Identity Applications 和 Identity Manager 引擎关联的驱动程序。有关详细信息，请参见停止和启动 Identity Manager 驱动程序 （第 154 页）。
❑	18. （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。有关更多信息，请参见将新服务器添加到驱动程序集 （第 158 页）。
❑	19. （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。有关更多信息，请参见将自定义策略和规则恢复到驱动程序 （第 159 页）。
❑	20. 激活已升级的 Identity Manager 解决方案。有关详细信息，请参见激活 Identity Manager （第 123 页）。

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，新版 Identity Manager 不提供从现有版本升级的路径，您需要先升级到可从其升级到 4.8 版的版本。或者，您也可以迁移到新计算机。 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高级版之后，如果您不想在环境中使用高级版功能，可以**切换**到标准版。 Identity Manager 可让您通过一个简单的过程从高级版切换到标准版。

升级

通常情况下，您可以升级 Identity Manager 4.7 Standard Edition 和 Advanced Edition。

- **Identity Manager 4.7 Standard Edition：**如果您当前使用的是 Identity Manager 4.7 Standard Edition，则可直接将其升级到 Identity Manager 4.8 Standard Edition。有关详细信息，请参见《*Quick Start Guide for Installing and Upgrading NetIQ Identity Manager 4.8 Standard Edition*》（NetIQ Identity Manager 4.8 Standard Edition 安装和升级快速入门指南）。

  要将 Identity Manager 4.7 Standard Edition 升级到 Identity Manager 4.8 Advanced Edition，请选择以下其中一种方法来完成升级：

  - 将 Identity Manager 4.7 Standard Edition 升级到 Identity Manager 4.8 Standard Edition，然后再升级到 Identity Manager 4.8 Advanced Edition。
  - 将 Identity Manager 4.7 Standard Edition 升级到 Identity Manager 4.7 Advanced Edition，然后再升级到 Identity Manager 4.8 Advanced Edition。
- **Identity Manager 4.7 Advanced Edition：**如果您当前使用的是 Identity Manager 4.7 Advanced Edition，则可直接将其升级到 Identity Manager 4.8 Advanced Edition。有关详细信息，请参见 Identity Manager 的升级核对清单 （第 127 页）。

将包含最新版 NICI 的 Identity Manager 4.7.4 升级到 4.8 时， Upgrade.log 会显示退出代码 1603，因为已安装最新版 NICI。可以忽略此代码。

迁移

在某些情况下，您无法进行直接升级。此时最好采用迁移方式。例如，如果以前装有 Identity Manager 的服务器所运行的操作系统不再受支持，则您必须执行迁移，而不是升级。

如果有多个服务器与一个驱动程序集关联，则可以一次在一个服务器上执行升级或迁移。如果您没有时间同时升级这些服务器，则驱动程序会继续与其他版本的 Identity Manager 协作，直到完成每个服务器的升级。

重要：如果为驱动程序启用的功能仅在 Identity Manager 4.8 或更高版本上受支持，则驱动程序在混合版本的服务器上将停止工作。较旧的引擎无法处理新功能。这将使驱动程序暂停，直到所有服务器都升级到 Identity Manager 4.8 或更高版本后才可重新使用。

从高级版切换到标准版

Identity Manager 允许您在产品评估期内或激活高级版后从高级版切换到标准版。

重要：如果您已应用高级版激活码，则不需要切换到标准版，因为标准版的所有功能在高级版中都有提供。仅当您不想在环境中使用任何高级版功能，并且想要缩减 Identity Manager 部署时，才必须切换到标准版。有关详细信息，请参见第 12 章“从高级版切换到标准版”（第 161 页）。

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 （只能安装在 Linux 计算机上）
4. 身份库
5. Identity Manager 引擎
6. Remote Loader
7. iManager 插件
8. Identity Applications （适用于高级版）
9. Identity Reporting
10. Analyzer
11. Self Service Password Reset

支持的升级路径

Identity Manager 4.8 支持从 4.7.x 和 4.6.x 版本升级。 NetIQ 建议您在开始升级前先查看当前版本的发行说明中的信息。

注释：将 Identity Manager 升级到版本 4.8 需要应用 Identity Manager 4.8 Upgrade Enablement 增补程序。应用此增补程序的条件取决于当前的 Identity Manager 版本。有关详细信息，请参见 《NetIQ Identity Manager 4.8 Upgrade Enablement Patch Release Notes》（NetIQ Identity Manager 4.8 Upgrade Enablement 增补程序发行说明）。

- 从 Identity Manager 4.7.x 版本升级 （第 130 页）
- 从 Identity Manager 4.6.x 版本升级 （第 132 页）

从 Identity Manager 4.7.x 版本升级

下表列出了 Identity Manager 4.7.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	4.7.x	1. 将操作系统升级到支持的版本。 2. 将身份库升级到 9.2。 3. 将 Identity Manager 引擎升级到 4.8。
Remote Loader/ 扇出代理	4.7.x	安装 4.8 版 Remote Loader/ 扇出代理
Designer	4.7.x	安装 Designer 4.8。
Identity Applications	4.7.x	升级 Identity Applications 前，请确保身份库和 Identity Manager 引擎已分别升级到 9.2 和 4.8。 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。有关支持的数据库版本，请参见 NetIQ Identity Manager 技术信息网站 (https://www.netiq.com/products/identity-manager/advanced/technical-information/)。 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 4.8 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 4.8。 6. 停止 Tomcat。
Identity Reporting	4.7.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。有关支持的数据库版本的详细信息，请参见 NetIQ Identity Manager 技术信息网站。 3. 将 SLM for IGA 升级到支持的版本（只能安装在 Linux 计算机上） 4. 更新数据收集服务和受管理服务网关驱动程序包。 5. 升级 Identity Reporting 4.8。 6. （视情况而定）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 Identity Manager 文档页面您所用版本的发行说明中查看相关信息。

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	中间步骤	升级后的版本
Identity Manager 引擎	4.6.x（其中 x 为 0 至 3）	应用 4.6.4 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 9.2。 3. 将 Identity Manager 引擎升级到 4.8。
Remote Loader/ 扇出代理	4.6.x（其中 x 为 0 至 3）	应用 4.6.4 增补程序	安装 4.8 版 Remote Loader/ 扇出代理。
Designer	4.6.x（其中 x 为 0 至 3）		安装 Designer 4.8。
Identity Applications	4.6.x（其中 x 为 0 至 3）	应用 4.6.4 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 9.2 和 4.8 版本。 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。有关支持的数据库版本，请参见 NetIQ Identity Manager 技术信息网站。 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 4.8 版本。 5. 将 Identity Applications 升级到 4.8。 6. 停止 Tomcat。
Identity Reporting	4.6.x（其中 x 为 0 至 3）	应用 4.6.4 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。有关支持的数据库版本的详细信息，请参见 NetIQ Identity Manager 技术信息网站。 3. 将 SLM for IGA 升级到支持的版本（只能安装在 Linux 计算机上） 4. 更新数据收集服务和受管理服务网关驱动程序包。 5. 将 Identity Reporting 迁移到 4.8。 6. （视情况而定）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 Identity Manager 文档页面您所用版本的发行说明中查看相关信息。

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：

- 导出 Designer 项目 （第 133 页）
- 导出驱动程序的配置 （第 134 页）

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 133 页）
- 通过身份库创建新项目 （第 134 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。

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 135 页）
- 使用 iManager 创建驱动程序的导出 （第 135 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。

11 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。

- 升级 Designer （第 137 页）
- 升级 Identity Manager 引擎组件 （第 138 页）
- 升级 Identity Applications （第 144 页）
- 升级 Identity Reporting （第 152 页）
- 升级 Analyzer （第 154 页）
- 停止和启动 Identity Manager 驱动程序 （第 154 页）
- 升级 Identity Manager 驱动程序 （第 156 页）
- 将新服务器添加到驱动程序集 （第 158 页）
- 将自定义策略和规则恢复到驱动程序 （第 159 页）

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. 起动 Identity_Manager_4.8_Designer_Windows.zip 文件中的 Designer 安装程序。 (<Designer zip 文件解压缩位置 >\designer_install\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）。

升级 Identity Manager 引擎组件

在升级 Identity Manager 引擎前，请务必先升级身份库。 Identity Manager 引擎升级过程会更新主机计算机文件系统中储存的驱动程序 shim 文件。

升级身份库

1 按 《*NetIQ Identity Manager Overview and Planning Guide*》（NetIQ Identity Manager 概述和规划指南）中的 “Where to Get Identity Manager” （从何处获取 Identity Manager）所述下载 Identity_Manager_4.8_Windows.iso。

2 装入下载的 .iso。

3 导航到 <iso 装入位置 >\IdentityManagerServer\products\eDirectory\x64 目录。

4 运行 eDirectory_920_Windows_x86_x64.exe 文件。

5 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。

6 （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。

7 在**安装位置**字段中，指定身份库的安装位置。

8 在 **DIB 位置**字段中，指定 DIB 文件所在的位置。

9 单击**升级**并继续进行升级过程。

升级 Identity Manager 引擎

验证驱动程序是否已停止。有关详细信息，请参见停止驱动程序 （第 154 页）。

升级 Identity Manager 引擎需要执行的步骤如下：

1 从 NetIQ 下载网站下载 Identity_Manager_4.8_Windows.iso。

2 装入下载的 .iso。

3 导航到 <ISO 安装位置 >\IdentityManagerServer 文件夹，然后运行 install.exe。

4 选择安装时要使用的语言，然后单击**确定**。

5 在 “ 简介 ” 页面中单击**下一步**。

6 阅读并接受许可协议，然后单击**下一步**。
安装的组件及其版本即会显示。

7 选择 **Identity Manager 引擎**，然后单击**下一步**。

8 指定 Identity Manager 引擎的配置设置。有关详细信息，请参见 Identity Manager 引擎的配置工作表 （第 48 页）。

9 在 “ 升级前摘要 ” 页面中查看设置，然后单击**升级**。

使用 MapDB 3.0.5

MapDB 是 Identity Manager 引擎的附加组件，以下 Identity Manager 驱动程序会使用该组件：

- 数据收集服务
- JDBC
- LDAP
- 受管系统网关
- Office 365 和 Azure Active Directory
- Salesforce

如果您使用上述任何驱动程序，在升级驱动程序之前必须先查看以下章节：

- 了解各驱动程序版本对 Identity Manager 4.8 引擎的支持 （第 140 页）
- 手动去除 MapDB 超速缓存文件 （第 140 页）

了解各驱动程序版本对 Identity Manager 4.8 引擎的支持

在升级使用 MapDB 的 Identity Manager 驱动程序之前，请先查看以下注意事项：

- Identity Manager 4.8 随附的驱动程序与 Identity Manager 4.8 引擎或 Remote Loader 兼容。必须遵循具体驱动程序实施指南中的驱动程序升级步骤。
- 低于 Identity Manager 4.8 的版本随附的驱动程序与 Identity Manager 4.8 引擎或 Remote Loader 不兼容。
- Identity Manager 4.8 随附的驱动程序与 Identity Manager 4.7.x 引擎或 Remote Loader 不向后兼容。
- Identity Manager 4.8 随附的驱动程序与 Identity Manager 4.6.x 引擎或 Remote Loader 不向后兼容。

手动去除 MapDB 超速缓存文件

Identity Manager 引擎升级流程会在身份库的 DIB 目录中保留一些现有的 MapDB 超速缓存文件 (dx*)。升级驱动程序之后，必须手动去除该驱动程序的这些文件。此操作可确保您的驱动程序能正常与 Identity Manager 4.8 引擎配合工作。

下表列出了必须去除的 MapDB 超速缓存文件：

Identity Manager 驱动程序	要去除的 MapDB 状态超速缓存文件
数据收集服务	DCSDriver_< 驱动程序实例 GUID>-*
	< 驱动程序实例 GUID>-*
JDBC	jdbc_< 驱动程序实例 GUID>_*
LDAP	ldap_< 驱动程序实例 GUID>*
受管系统网关	MSGW-< 驱动程序实例 GUID>.*
Office 365 和 Azure Active Directory	<Azure 驱动程序名称 >_obj.db.*
Salesforce	<Salesforce 驱动程序名称 >.*
	<Salesforce 驱动程序名称 >

其中， * 表示 MapDB 状态超速缓存文件的名称。对于 Salesforce 驱动程序， MapDB 状态超速缓存文件也用驱动程序名称表示。下面是这些文件的一些示例。

- DCSDriver_< 驱动程序实例 GUID>-0.t、 < 驱动程序实例 GUID>-1.p
- jdbc_< 驱动程序实例 GUID>_0.t、 jdbc_< 驱动程序实例 GUID>_1
- ldap_< 驱动程序实例 GUID>b、 ldap_< 驱动程序实例 GUID>b.p

- MSGW-< 驱动程序实例 GUID>.p、 MSGW-< 驱动程序实例 GUID>.t
- <Azure 驱动程序名称 >_obj.db.t、 <Azure 驱动程序名称 >_obj.db.p
- <Salesforce 驱动程序名称 >.p、<Salesforce 驱动程序名称 >.t、 Salesforce driver1

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。有关说明，请参见 《*NetIQ Identity Manager Driver Administration Guide*》（NetIQ Identity Manager 驱动程序管理指南）中的 “Stopping, Starting, or Restarting a Driver in Designer” （在 Designer 中停止、启动或重启动驱动程序）。
3. 停止每个驱动程序的 Remote Loader 服务或守护程序。

   在 Remote Loader 控制台中，选择 Remote Loader 实例，然后单击**停止**。
4. 使用 Windows 任务管理器停止 lcache 进程。
5. 从 NetIQ 下载网站下载 Identity_Manager_4.8_Windows.iso。
6. 装入下载的 .iso。
7. 导航到 <ISO 安装位置 >\IdentityManagerServer 文件夹，然后运行 install.exe。
8. 选择安装时要使用的语言，然后单击**确定**。
9. 在 “ 简介 ” 页面中单击**下一步**。
10. 阅读并接受许可协议，然后单击**下一步**。

    安装的组件及其版本即会显示。
11. 选择 **Remote Loader 服务**并单击**下一步**。
12. 在 “ 升级前摘要 ” 页面中单击**下一步**。
13. 升级完成后，校验配置文件是否包含您的环境的信息。
14. （视情况而定）如果配置文件有问题，请复制您在第 1 步中创建的备份文件。否则，请继续下一步。
15. 启动每个驱动程序的 Remote Loader 服务或守护程序。

重要：如果您的驱动程序使用 MapDB，请在升级该驱动程序之后，手动去除其现有的 MapDB 状态超速缓存文件。之所以需要这样做，是因为 Identity Manager 引擎升级过程不会从身份库的 DIB 目录中去除所有这些文件。有关详细信息，请参见使用 MapDB 3.0.5 （第 139 页）。

升级 Java Remote Loader

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。有关说明，请参见 《*NetIQ Identity Manager Driver Administration Guide*》（NetIQ Identity Manager 驱动程序管理指南）中的 "Stopping, Starting, or Restarting a Driver in Designer" （在 Designer 中停止、启动或重启动驱动程序）。
3. 停止每个驱动程序的 Remote Loader 服务或守护程序。

   在 Remote Loader 控制台中，选择 Remote Loader 实例，然后单击停止。
4. 使用 Windows 任务管理器停止 lcache 进程。
5. 从 NetIQ 下载网站下载 Identity_Manager_4.8_Windows.iso。
6. 装入下载的 .iso。
7. 导航到 <ISO 安装位置 >\IdentityManagerServer\products\IDM\java_remoteloader 文件夹。
8. 复制并替换现有 Java Remote Loader 安装目录中的 dirxml_jremote_dev.tar.gz 文件。
9. 根据现有设置中的文件，复制并替换现有 Java Remote Loader 安装目录中的以下文件之一：
   - dirxml_jremote.tar.gz
   - dirxml_jremote_mvs.tar
10. 将步骤 8 和 9 中复制的文件解压缩。

    使用 7-zip 或支持的软件解压缩 .tar.gz 文件。
11. （视情况而定）如果配置文件有问题，请复制您在第 1 步中创建的备份文件。否则，请继续下一步。

    注释：请使用 version.txt 文件来确保 Java Remote Loader 版本是最新的。
12. 启动每个驱动程序的 Remote Loader 服务或守护程序。

升级 iManager

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。 NetIQ 建议您在将 iManager 升级到 3.2 版本之前执行以下操作：

- 将 eDirectory 升级到 9.2 版本。
- 备份 server.xml 和 context.xml 配置文件。

升级过程包括以下活动：

- 升级 iManager （第 143 页）
- 更新基于角色的服务 （第 143 页）
- 重安装或迁移 Plug-in Studio 的插件 （第 144 页）
- 在升级或重安装后更新 iManager 插件 （第 144 页）

升级 iManager

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。

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。

1. 从 NetIQ 下载网站下载 Identity_Manager_4.8_Windows.iso。
2. 装入下载的 .iso。
3. 导航到 <ISO 安装位置 >\IdentityManagerServer 文件夹，然后运行 install.exe。
4. 选择安装时要使用的语言，然后单击**确定**。
5. 在“简介”页面中单击**下一步**。
6. 阅读并接受许可协议，然后单击**下一步**。

   安装的组件及其版本即会显示。
7. 选择 **iManager Web Administration**，然后单击**下一步**。
8. 指定 iManager 的设置。有关详细信息，请参见 Identity Manager 引擎的配置工作表 （第 48 页）。
9. 在“升级前摘要”页面中查看设置，然后单击**升级**。

更新基于角色的服务

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。

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**。
- 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. 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**。

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。

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。

注释：只能通过此方法从 Open Enterprise Server 2018 上的 iManager 更新 Identity Manager 插件。

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。

升级 Identity Applications

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

升级后，组件将升级到以下版本：

- Tomcat - 8.5.40
- ActiveMQ - 5.15.9
- Java 8 Update 222
- One SSO Provider - 6.3.4
- Self-Service Password Reset - 4.4.0.3

- Identity Applications - 4.8
- Identity Reporting - 6.5

本节提供有关以下主题的信息：

- 了解升级程序 （第 145 页）
- 升级先决条件 （第 145 页）
- 系统要求 （第 145 页）
- 升级 PostgreSQL 数据库 （第 145 页）
- 升级 Identity Applications 的驱动程序包 （第 147 页）
- 升级 Identity Applications （第 148 页）
- 升级后任务 （第 149 页）

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。

升级先决条件

如果您的数据库是通过 SSL 配置的，请在位于 C:\NetIQ\idm\apps\tomcat\conf 路径下的 server.xml 文件中，将 ssl=true 替换为 sslmode=require。

例如，将

```
jdbc:postgresql://<postgres db>:5432/idmuserappdb?ssl=true
```

更改为

```
jdbc:postgresql://<postgres db>:5432/idmuserappdb?sslmode=require
```

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。

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_old。

3 执行以下命令去除旧服务：

sc delete <postgres 服务名称 >

4 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。

4a 装入 Identity_Manager_4.8_Windows.iso 映像文件，然后导航到 \common\postgres_tomcat 目录。

4b 运行 TomcatPostgreSQL.exe 文件。

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**。
- 确保您拥有新旧 PostgreSQL 安装目录的管理员特权。

---

5 停止新安装的 PostgreSQL 服务。转到**服务**，搜索 *<PostgreSQL 版本号>* 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。

---

6 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**。

7 以 postgres 用户的身份访问 PostgreSQL 目录。

1. 以 postgres 用户身份登录服务器。

   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. 删除新 postgres 安装位置中的数据目录。例如， C:\NetIQ\idm\apps\postgres\data
3. 打开命令提示符，并使用以下命令设置 PGPASSWORD：

   ```
   set PGPASSWORD=<your pg password>
   ```
4. 切换到新安装的 PostgreSQL 目录。
5. 以 postgres 数据库用户身份执行 initdb。

   initdb.exe -D < 新数据目录 > -E UTF8 -U postgres

例如，

initdb.exe -D C:\NetIQ\idm\apps\postgres\data -E UTF8 -U postgres

8 从新 PostgreSQL 的 bin 目录升级 PostgreSQL。运行以下命令，然后单击 **Enter**。

注释：确保已在 C:\NetIQ\idm\apps\postgres\data\ 目录下的 pg_hba.conf 中，将方法类型由 md5 设置为 trust。

```
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"
```

9 成功升级后，用旧 postgres 数据目录中的文件替换新 postgres 目录 (C:\NetIQ\idm\apps\postgres\data) 中的 pg_hba.conf 和 postgresql.conf 文件。

10 启动升级后的 PostgreSQL 数据库服务。

转到服务，搜索 *<PostgreSQL 版本号>* 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。

11 禁用旧的 PostgreSQL 服务，以确保该服务不会自动启动。

12 （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\apps\postgresql\bin

注释：仅当您想要删除旧数据文件时，才需要运行此步骤。

升级 Identity Applications 的驱动程序包

您必须停止 Tomcat，并将 User Application 及 Role and Resource Service 驱动程序的包更新到最新版本。有关将包升级到最新版本的信息，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）。

升级 User Application 驱动程序包后，必须手动添加工作流程模板包：

1 在 Designer 中，导航到 **User Application 驱动程序** > **属性**。

2 依次单击 “ 包 ”、 。

3 选择**创建工作流程模板**。

4 单击**确定**，然后单击**完成**以完成安装。

5 部署 User Application 驱动程序。

重要：如果在升级 User Application 驱动程序的过程中安装或升级了任何电子邮件通知模板，则需要部署**默认通知集合**对象。

升级 Identity Applications

下面的过程说明了如何升级以下组件：

- Identity Applications
- OSP
- Tomcat
- PostgreSQL
- SSPR （如果与 Identity Applications 安装在同一台计算机上）
- ActiveMQ

升级 Identity Applications 需要执行的步骤如下：

1. 从 NetIQ 下载网站下载 Identity_Manager_4.8_Windows.iso。
2. 装入下载的 .iso。
3. 导航到 <ISO 安装位置 >\IdentityApplications 文件夹，然后运行 install.exe。
4. 选择安装时要使用的语言，然后单击**确定**。
5. 在 “ 简介 ” 页面中单击**下一步**。
6. 阅读并接受许可协议，然后单击**下一步**。
   安装的组件及其版本即会显示。
7. 选择 **Identity Applications**，然后单击**下一步**。
8. 指定 Identity Applications 的配置设置。有关详细信息，请参见 Identity Applications 的配置工作表 （第 50 页）。

   注释：
   - 如果您将 PostgreSQL 数据库安装到了 Identity Applications 所在的同一台服务器上，NetIQ 建议使用 Identity Manager 安装程序来创建工作流程数据库。
   - 升级时，您必须手动指定数据库 JDBC JAR 文件。例如，如果您使用的是 PostgresQL 数据库，则需要指定位于 tomcat\lib 文件夹外部的数据库 JAR 文件的位置。
9. 在 “ 升级前摘要 ” 页面中查看设置，然后单击**升级**。

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

升级后任务

如果您将 Identity Applications 和 SSPR 安装在不同的服务器上，则必须将 CN 为 Identity Applications 的 SSPR 可信证书导入到 Identity Applications 服务器的 cacerts 中。

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 149 页）
- Tomcat （第 149 页）
- Identity Applications （第 150 页）
- One SSO Provider （第 151 页）
- Self-Service Password Reset （第 151 页）
- Kerberos （第 151 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 Certificate_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 重启动身份库。

3 校验 JRE 主目录位置是否为 tomcat\bin\setenv.bat。

4 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

将 Identity Applications 从 4.6 SP4 升级到 4.8 时，必须确保 tomcat/bin 文件夹内的 setenv 文件中存在 Dcom.novell.afw.wf.engine-id=IDMProv 参数。如果升级 Identity Applications 后此参数缺失，则必须在 setenv 文件中手动添加该参数，并重启动 Tomcat 服务器。

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。有关详细信息，请参见 SSO 客户端参数 （第 82 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，请参见安装后步骤 （第 54 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 **4.8.0**。

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。

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 Sentinel Log Management for IGA。有关详细信息，请参见 《NetIQ Identity Manager 安装指南 - Linux》中的 “ 升级 Sentinel Log Management for IGA”。
2. 升级 Identity Reporting。

升级先决条件

如果您的数据库是通过 SSL 配置的，请在位于 C:\NetIQ\idm\apps\tomcat\conf 路径下的 server.xml 文件中，将 ssl=true 替换为 sslmode=require。

例如，将

```
jdbc:postgresql://<postgres db>:5432/idmrptdb?ssl=true
```

更改为

```
jdbc:postgresql://<postgres db>:5432/idmrptdb?sslmode=require
```

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，请在旧版本的基础上安装新版本。

升级 Identity Reporting 需要执行的步骤如下：

1. 从 NetIQ 下载网站下载 Identity_Manager_4.8_Windows.iso。
2. 装入下载的 .iso。
3. 导航到 <ISO 安装位置 >\IdentityReporting 文件夹，然后运行 install.exe。
4. 选择安装时要使用的语言，然后单击**确定**。
5. 在 “ 简介 ” 页面中单击**下一步**。
6. 阅读并接受许可协议，然后单击**下一步**。
   安装的组件及其版本即会显示。
7. 选择 **Identity Reporting**，然后单击**下一步**。
8. 指定 Identity Reporting 的配置设置。有关详细信息，请参见 Identity Reporting 的配置工作表 （第 52 页）。
9. 在 “ 升级前摘要 ” 页面中查看设置，然后单击**升级**。

注释： ism-configuration.properties 文件中的 com.netiq.rpt.ssl-keystore.type 属性将保留升级之前设置的值 (JKS/PKCS12)。

Reporting 的升级后步骤

将 Identity Reporting 升级到 4.8 之后，导航到 /opt/netiq/idm/apps/tomcat/conf/ 目录中的 ism-configuration.properties 文件，并执行以下操作：

- 按如下所示更改 com.netiq.rpt.landing.url 属性的值：

  com.netiq.rpt.landing.url = ${com.netiq.idm.osp.url.host}/idmdash/#/landing
- 按如下所示更改 com.netiq.idmdcs.landing.url 属性的值：

  com.netiq.idmdcs.landing.url = ${com.netiq.idm.osp.url.host}/idmdash/#/landing
- 采用以下格式指定 com.netiq.rpt.redirect.url 属性的值：https:< 主机名 >:< 端口 >/ 路径

  例如 com.netiq.rpt.redirect.url = https://192.168.0.1:8543/IDMRPT/oauth.html

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。

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。

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 Identity_Manager_4.8_Analyzer_Windows。

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。

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，以确保升级或安装过程能够修改或替换正确的文件。本节介绍了以下活动：

- 停止驱动程序 （第 154 页）
- 启动驱动程序 （第 155 页）

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 154 页）
- 使用 iManager 停止驱动程序 （第 155 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。

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 155 页）
- 使用 iManager 启动驱动程序 （第 156 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。

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“Understanding Packages”（了解包）。

您可通过以下方式将驱动程序升级到包：

- 创建新驱动程序 （第 157 页）
- 用包的内容替换现有内容 （第 157 页）
- 保留当前内容并通过包添加新内容 （第 157 页）

重要：如果您的驱动程序使用 MapDB，请在升级该驱动程序之后，手动去除其现有的 MapDB 状态超速缓存文件。之所以需要执行此操作，是因为 Identity Manager 引擎升级流程不会将这些文件全部清理掉。有关详细信息，请参见使用 MapDB 3.0.5 （第 139 页）。

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。

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，请参见导出驱动程序的配置 （第 134 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，请参见将自定义策略和规则恢复到驱动程序 （第 159 页）。

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，请参见导出驱动程序的配置 （第 134 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。

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。

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，请跳至在 Designer 中复制服务器特定信息 （第 169 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**。

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 （第 158 页）
- 使用 iManager 从驱动程序集中去除旧服务器 （第 159 页）
- 弃用旧服务器 （第 159 页）

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 ”。

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。

- 使用 Designer 将自定义策略和规则恢复为驱动程序 （第 160 页）
- 使用 iManager 将自定义策略和规则恢复为驱动程序 （第 160 页）

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 “Stopping, Starting, or Restarting a Driver in Designer” （在 Designer 中停止、启动或重启动驱动程序）。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。

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 《*NetIQ Identity Manager Driver Administration Guide*》（NetIQ Identity Manager 驱动程序管理指南）中的 “Stopping, Starting, or Restarting a Driver in Designer” （在 Designer 中停止、启动或重启动驱动程序）。 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。

12 从高级版切换到标准版

仅当您不想在环境中使用任何高级版功能，并且想要缩减 Identity Manager 部署时，才应切换到标准版。

1 （视情况而定）如果您已应用高级版激活，请去除激活。

2 （视情况而定）要切换到标准版评估模式，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）如果您已购买标准版激活，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 C:\NetIQ\IDM\apps\tomcat\conf 目录中的 ism-configuration.properties 文件复制到备份目录。

8 从 Identity Manager 4.8 iso 文件安装 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://192.168.0.1:8180/IDMRPT
- Self Service Password Reset
  - **OAuth 客户端 ID**。例如， *sspr*
  - OAuth 客户端密码。例如， *<sspr 客户端密码 >*
  - **OSP OAuth 重定向 URL**。例如， http://192.168.0.2:8180/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 67 页）。

10 保存更改并退出配置实用程序。

11 启动 Tomcat。

VII 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 VI 部分 “ 升级 Identity Manager” （第 125 页）。有关升级与迁移之间区别的详细信息，请参见了解升级和迁移（第 129 页）。

13 准备迁移 Identity Manager

本章提供的信息可帮助您做好将 Identity Manager 解决方案迁移到新安装的准备工作。

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. 确保拥有最新的安装包用于迁移 Identity Manager 数据。
❑	2. 确保您的计算机符合较新版 Identity Manager 的硬件和软件先决条件。
❑	3. 将身份库升级到支持的最新版本。
❑	4. 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 14 节 “ 将 Identity Manager 迁移到新服务器 ”（第 167 页）。
❑	5. 在新服务器上安装 Identity Manager。有关详细信息，请参见规划 Identity Manager 安装 （第 31 页）。
❑	6. （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，请参见升级 Remote Loader （第 141 页）。
❑	7. （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 Identity Manager 的迁移核对清单 （第 167 页）。
❑	8. 将该新服务器添加到驱动程序集中。有关更多信息，请参见将该新服务器添加到驱动程序集中 （第 158 页）。
❑	9. 更改每个驱动程序的特定于服务器的信息。有关更多信息，请参见在 Designer 中复制服务器特定信息 （第 169 页）。
❑	10. （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。有关更多信息，请参见复制驱动程序集的服务器特定信息 （第 168 页）
❑	11. 将驱动程序更新为包格式。有关详细信息，请参见升级 Identity Manager 驱动程序 （第 156 页）。
❑	12. （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，请参见将自定义策略和规则恢复到驱动程序 （第 159 页）。
❑	13. 从驱动程序集中去除旧服务器。有关更多信息，请参见从驱动程序集中去除旧服务器 （第 158 页）。

	核对清单项目
❑	14. 激活已升级的 Identity Manager 解决方案。有关详细信息，请参见激活 Identity Manager （第 123 页）。

14 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：

- Identity Manager 的迁移核对清单 （第 167 页）
- 准备要迁移的 Designer 项目 （第 168 页）
- 复制驱动程序集的服务器特定信息 （第 168 页）
- 将 Identity Manager 引擎迁移到新服务器 （第 170 页）
- 迁移 User Application 驱动程序 （第 171 页）
- 升级 Identity Applications （第 172 页）
- 迁移 Identity Applications （第 172 页）
- 完成 Identity Applications 的迁移 （第 174 页）

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）。 **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**。
❑	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，请参见准备要迁移的 Designer 项目 （第 168 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，请参见将 Identity Manager 引擎迁移到新服务器 （第 170 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。有关更多信息，请参见迁移 User Application 驱动程序 （第 171 页）。

	核对清单项目
❑	9. 将两个驱动程序部署到身份库。
❑	10. 升级 Identity Applications。有关更多信息，请参见升级 Identity Applications （第 144 页）。
❑	11. 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，请参见清理浏览器超速缓存 （第 175 页）。
❑	12. （视情况而定）恢复 SharedPagePortlet 的自定义设置。有关详细信息，请参见更新 SharedPagePortlet 的最大超时设置 （第 175 页）。
❑	13. 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，请参见禁用组的自动查询设置 （第 175 页）。

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。

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。

- 在 Designer 中复制服务器特定信息 （第 169 页）
- 在 iManager 中更改服务器特定信息 （第 170 页）
- 更改 User Application 的服务器特定信息 （第 170 页）

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 《*NetIQ Identity Manager Driver Administration Guide*》（NetIQ Identity Manager 驱动程序管理指南）中的 “Stopping, Starting, or Restarting a Driver in Designer”（在 Designer 中停止、启动或重启动驱动程序）。

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。

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. 按配置 Identity Applications 的设置 （第 66 页）中所述指定值。

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。

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。

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**。

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**。

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。

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。
- 不要对数据库使用区分大小写的排序。区分大小写的排序不受支持。使用区分大小写的排序可能会导致迁移期间出现重复键错误。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。唯一受支持的排序规则是 SQL_Latin1_General_CP1_CI_AS。

有关升级 Identity Applications 的详细信息，请参见升级 Identity Applications （第 144 页）。

迁移 Identity Applications

不要对数据库使用区分大小写的排序。区分大小写的排序不受支持。使用区分大小写的排序可能会导致迁移期间出现重复键错误。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。唯一受支持的排序规则是 SQL_Latin1_General_CP1_CI_AS。

在迁移 Identity Applications 之前，必须安装 /opt/netiq/common/openssl/lib64/ 目录中的 libssl.so.1.0.0 和 libcrypto.so.1.0.0 库。

Identity Applications 迁移过程包括以下步骤：

- 将数据库迁移到新服务器 （第 172 页）
- 在新服务器上安装 Identity Applications （第 173 页）

将数据库迁移到新服务器

如果您的 User Application 数据库位于 PostgreSQL 中，请执行以下步骤：

1 登录到安装了 PostgreSQL 的服务器。

2 打开命令提示符，导航到 postgres bin 目录并将数据导出到 .sql 文件。

示例：pg_dumpall -U postgres > dump.sql

3 登录到要安装 PostgreSQL 的新服务器。

4 如下所述安装 PostgreSQL：

4a 从软件许可和下载 (https://sldlogin.microfocus.com/) 门户下载并装入 Identity_Manager_4.8.x_Windows.iso。

4b 导航到装入 Identity_Manager_4.8.x_Windows.iso 的位置。

4c 导航到：< 装入位置 >\common\packages\postgres\ 目录。

4d 运行 PostgreSQL 安装程序。

5 导航到 C:\NetIQ\IDM\postgres 并删除 Data 目录。

6 在 PostgreSQL 安装位置创建一个 data 目录，并确保 postgres 用户有权访问该目录。

7 打开命令提示符，导航到 postgres bin 目录并如下所示初始化数据库：

示例：initdb.exe -D C:\NetIQ\IDM\postgres\data -E WIN1252 -U postgres。

8 确保 C:\NetIQ\IDM\postgres\data 下的 pg_hba.conf 文件中存在以下项。

IPv6 local connections:

host all all ::1/128 trust

host all all 0.0.0.0/0 trust

9 确保已在 postgresql.conf 文件中取消注释以下项：

listen_addresses = '*'

port = 5432

10 从运行菜单运行 services.msc，重启动 postgres 服务。

11 打开命令提示符，导航到 postgres bin 目录，将数据导入新的 PostgreSQL 数据库，然后按照步骤 2 中所述使用收集的转储。

示例：psql -U postgres < dump.sql。

在新服务器上安装 Identity Applications

以下过程说明如何在新服务器上安装 Identity Application：

1 从 NetIQ 下载网站 (https://dl.netiq.com/) 下载 Identity_Manager_4.8.x_Windows.iso。

2 装入 .iso 文件。

3 导航到 Identity apps 目录，安装 Identity Applications，并跳过 User Application 和 Roles and Resources Service 驱动程序的部署。

3a 选择 “ 自定义安装 ” 模式。

3b 输入身份库细节。

3c 取消选中部署 Identity Applications 驱动程序。

4 选择现有 PostgreSQL 服务器，提供所需的细节，然后继续安装。

完成 Identity Applications 的迁移

在升级或迁移 Identity Applications 后，请完成迁移过程。

准备 Oracle 数据库以运行 SQL 文件

在安装过程中，您可能已选择编写一个 SQL 文件来更新 Identity Applications 数据库。如果数据库在 Oracle 平台上运行，则您必须先执行一些步骤，然后才能运行该 SQL 文件。

1 在数据库中运行以下 SQL 语句：

```
ALTER TABLE DATABASECHANGELOG ADD ORDEREXECUTED INT;
UPDATE DATABASECHANGELOG SET ORDEREXECUTED = -1;
ALTER TABLE DATABASECHANGELOG MODIFY ORDEREXECUTED INT NOT NULL;
ALTER TABLE DATABASECHANGELOG ADD EXECTYPE VARCHAR(10);
UPDATE DATABASECHANGELOG SET EXECTYPE = 'EXECUTED';
ALTER TABLE DATABASECHANGELOG MODIFY EXECTYPE VARCHAR(10) NOT NULL;
```

2 运行以下 updateSQL 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
```

3 在文本编辑器中，打开默认位于 */installation_path*/userapp/sql 目录中的 SQL 文件。

4 在函数 CONCAT_BLOB 的定义后面插入一个反斜杠 (/)。例如

```
  -- Changeset icfg-data-load.xml::700::IDMRBPM
CREATE OR REPLACE FUNCTION CONCAT_BLOB(A IN BLOB, B IN BLOB) RETURN BLOB
AS
                C BLOB;
            BEGIN
                DBMS_LOB.CREATETEMPORARY(C, TRUE);
                DBMS_LOB.APPEND(C, A);
                DBMS_LOB.APPEND(C, B);
                RETURN c;
            END;
/
```

5 执行 SQL 文件。

有关运行 SQL 文件的详细信息，请参见手动创建数据库纲要 （第 87 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。

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。

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”。

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：

用户
部门
查询列表
地区
电话号码
电子邮件
管理者
名
首选通知
姓
隐藏属性列表
用户照片
用户自选设置
用户自选设置
职务
直属上司
组
用户查找
组
列表
使用文字字符串或表达式提供属性的默认值:
文字字符串:
表达式:
UI 控件
指定用于显示属性的任何格式设置或特殊控件:
数据类型:
DN
格式类型:
<无>
控件类型:
DNLookup
DNLookup 显示
选择"查找"操作显示的实体和属性:
查找实体:
组
查找属性
说明
执行自动查询
如果您不希望自动执行查询，请取消选中此复选框

VIII 在 Microsoft Azure 上部署 Identity Manager

本部分介绍如何在 Microsoft Azure 云中规划和实施 Identity Manager。

- 第 15 章 “ 在 Microsoft Azure 上规划和实施 Identity Manager”（第 179 页）
- 第 16 章 “ 混合 Identity Manager 方案示例 ”（第 189 页）

15 在 Microsoft Azure 上规划和实施 Identity Manager

Identity Manager 现支持在 Microsoft Azure 上部署以下 Identity Manager 组件。

- Identity Manager 引擎
- Identity Manager 驱动程序和 Remote Loader
- iManager
- Designer
- Identity Applications
- Identity Reporting

注释：不支持在 Microsoft Azure 上部署 Sentinel Log Management。

先决条件

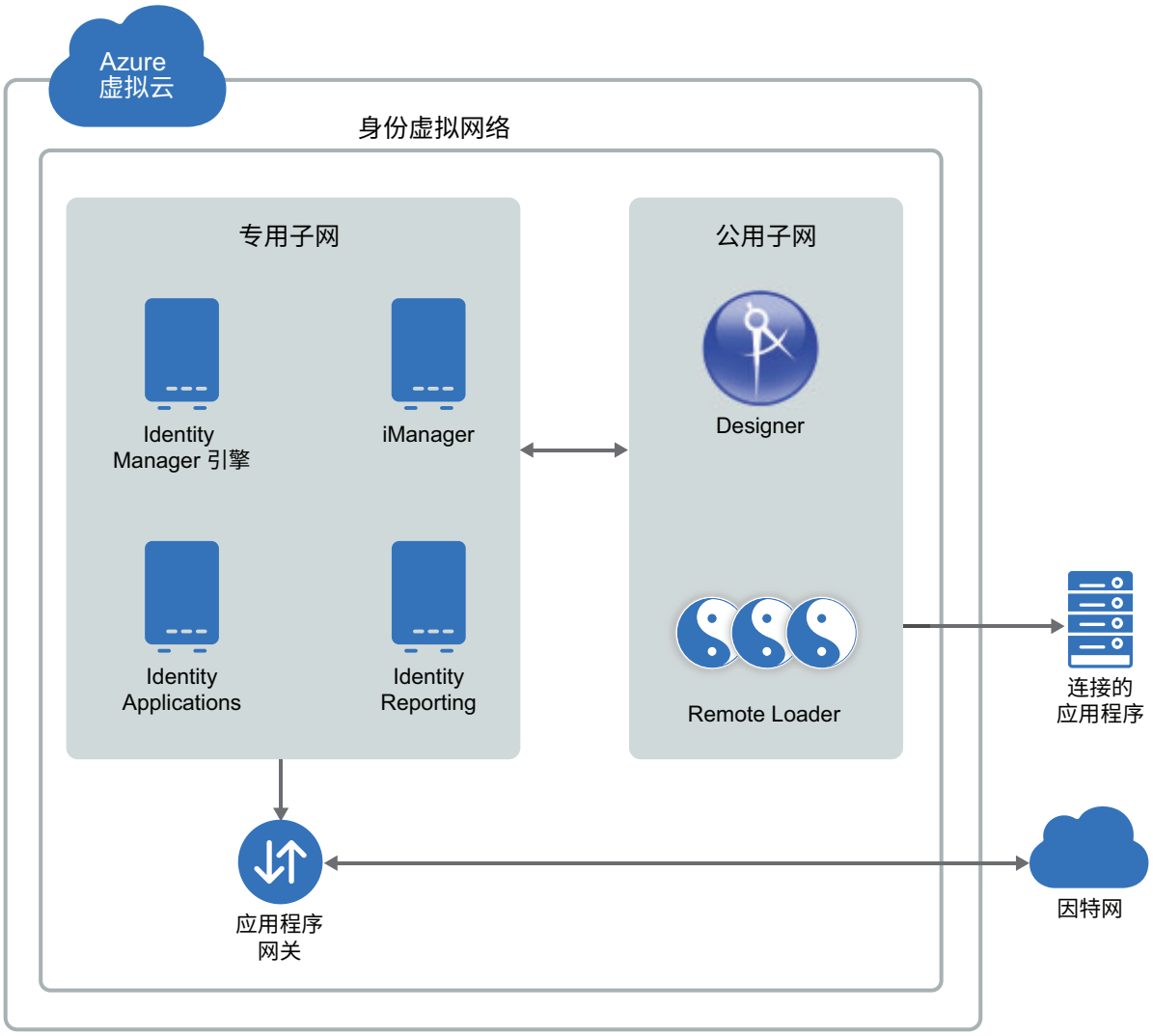
除了 Identity Manager 组件的系统要求以外，另请确保符合以下先决条件：

- Microsoft Azure 上的管理帐户。
- Identity_Manager_4.8_Windows.iso 和 Designer 已下载、解压缩并可在 Identity Manager 组件实例上使用。
- 用于从本地客户端计算机连接到 Azure VM 实例的远程桌面。

部署过程

您可以根据相应要求在专用或公用网络中部署 Identity Manager 组件。图 15-1 演示了一个示例部署，后续章节中将用到该部署。

图 15-1 在 Microsoft Azure 上部署 Identity Manager



您可以根据 Identity Manager 组件在不同服务器上的分布方式，以不同的组合在 Microsoft Azure 上部署这些组件。不过，所有方案的部署过程都是相同的。

部署过程包括以下步骤：

- 创建资源组 （第 181 页）
- 创建虚拟网络和子网 （第 181 页）
- 创建应用程序网关 （第 182 页）
- 创建虚拟机实例 （第 183 页）
- 更新 VM 中的主机项 （第 184 页）
- 安装 Designer （第 185 页）
- 配置应用程序网关 （第 186 页）

创建资源组

NetIQ 建议您创建一个资源组并将所需资源添加到该组，以与 Identity Manager 搭配使用。执行以下步骤来创建新的资源组：

1 登录到 Azure 门户。

2 单击**资源组**。

3 单击**创建**。

4 在**基本信息**选项卡中：

4a 从下拉列表中选择您的**订阅**。

4b 输入新的资源组名称。

4c 从**区域**下拉列表中选择位置。例如印度中部。

4d 单击**下一步：标记 >**。

5 在**标记**选项卡中，单击**下一步：查看 + 创建 >**。

6 在**查看 + 创建**选项卡中，单击**创建**。

创建虚拟网络和子网

1 登录到 Azure 门户。

2 在搜索中键入**虚拟网络**。

3 在 “ 服务 ” 下，选择**虚拟网络**。

4 单击**创建**。

5 在**基本信息**选项卡中指定以下细节：

字段	说明
订购	从下拉列表中选择您的订阅。
资源组	从下拉列表中选择现有的资源组。
名称	指定虚拟网络的名称。
区域	从下拉列表中选择位置。例如印度中部。

5a 单击**下一步：IP 地址 >**。

6 在 “IP 地址 ” 选项卡中，单击**添加子网**。

6a 单击**添加子网**。

6a1 指定子网名称。例如 default。

6a2 指定子网地址范围。例如 10.1.0.0/24。

6a3 单击**添加**。

6b 单击**下一步：安全性 >**。

7 在**安全性**选项卡中，保留所有字段的默认值，然后单击**下一步：标记 >**。

8 在标记选项卡中，单击下一步：查看 + 创建 >。

9 在查看 + 创建选项卡中查看您的设置，然后单击创建。

创建应用程序网关

1 登录到 Azure 门户。

2 单击创建资源。

3 转到类别 > 网络 > 应用程序网关。

4 在基本信息选项卡中指定以下细节：

字段	说明
订购	从下拉列表中选择您的订阅。
资源组	从下拉列表中选择现有的资源组。
应用程序网关名称	指定应用程序网关名称。
区域	从下拉列表中选择位置。例如印度中部。
层	选择所需的层。例如标准 V2。
最小实例计数	指定值 **0**。
最大实例计数	指定值 **10**。
虚拟网络	选择虚拟网络和已创建的对应子网。请参见创建虚拟网络和子网 （第 181 页）。

4a 保留其余字段的默认值，然后单击下一步：前端 >。

5 在前端选项卡中：

5a 选择公共。

5b 在公共 IP 地址下，单击新增。

5b1 指定公共 IP 地址名称。例如 idmgateway.centralindia.cloudapp.azure.com。

5b2 单击确定。

5c 单击下一步：后端 >

6 在后端选项卡中：

6a 单击添加后端池。

6a1 指定后端池名称。

6a2 选择是添加一个没有目标的后端池。

6a3 单击添加。

6b 单击下一步：配置 >。

7 在配置选项卡中：

7a 在路由规则下，单击添加路由规则。

7b 指定规则名称。

7c 在侦听器选项卡中指定以下细节：

字段	说明
侦听器名称	指定侦听器名称。
前端 IP	从下拉列表中选择**公共**。
协议	选择 **HTTP**。
端口	指定值 **80**。

7d 保留其余字段的默认值。

7e 在后端目标选项卡中指定以下细节：

字段	说明
后端目标	从下拉列表中选择后端目标。
HTTP 设置	单击**新增**，指定 HTTP 设置名称。保留所有字段的默认值，然后单击**添加**。

7e1 单击添加。

7f 单击下一步：标记 >。

8 在标记选项卡中，单击下一步：查看 + 创建 >。

9 在查看 + 创建 > 选项卡中查看您的设置，然后单击创建。

注释：有关配置应用程序网关的详细信息，请参见配置应用程序网关 （第 186 页）。

创建虚拟机实例

创建单独的虚拟机以托管 Identity Manager 组件。

1 登录到 Azure 门户。

2 在搜索中键入**虚拟机**。

3 在“服务”下，选择虚拟机。

4 单击创建，然后选择虚拟机。

5 在基本信息选项卡中：

5a 从下拉列表中选择您的订阅。

5b 从下拉列表中选择现有的资源组 （参见创建资源组 （第 181 页））。

5c 指定虚拟机名称。

5d 从区域下拉列表中选择位置。例如印度中部。

5e 从映像下拉列表中选择所需的 **Windows Server**。例如 Windows Server 2019。

5f 从大小下拉列表中选择虚拟机大小。

5g 指定用户名、密码并确认密码。

5h 在“许可”下，选择 **Windows Server 许可证**，然后选择符合条件的**附带软件保障的 Windows Server 许可证**以确认。

5i 保留其余字段的默认值。

5j 单击**下一步：磁盘 >**。

6 在**磁盘**选项卡中：

6a 从 **OS 磁盘类型**下拉列表中选择磁盘类型。例如高级 SSD。

6b 从下拉列表中选择所需的加密类型。

6c 单击**下一步：网络 >**。

7 在**网络**选项卡中：

7a 选择虚拟网络和已创建的对应子网。请参见创建虚拟网络和子网 （第 181 页）。

7b 在网络安全组下，选择**高级**。

7c 从下拉列表中选择现有的网络安全组。

7c1 （视情况而定）如果没有可用的网络安全组，请单击**新建**。

7c2 指定网络安全组名称。

7c3 单击**添加入站角色**，指定所需的细节。

7c4 单击**添加出站角色**，指定所需的细节。

7c5 单击**确定**。

7d 保留其余字段的默认值。

7e 单击**下一步：管理 >**。

8 在**管理**选项卡中，保留所有字段的默认值，然后单击**下一步：高级 >**。

9 在**高级**选项卡中，保留所有字段的默认值，然后单击**下一步：标记 >**。

10 在**标记**选项卡中，保留所有字段的默认值，然后单击**下一步：查看 + 创建 >**。

11 在**查看 + 创建**选项卡中查看您的设置，然后单击**创建**。

更新 VM 中的主机项

可以使用应用程序网关的公共 DNS 名称或使用别名 DNS 记录集来访问 Identity Manager 组件。要使 Identity Manager 组件能够互相通讯，请编辑每个 VM 上的 hosts 文件，并添加一项来解析此 VM 的主机名。

表 15-1 更新主机项

组件	说明
Identity Engine	导航到 Identity Engine VM 中的 **hosts** 文件。例如， C:\Windows\System32\drivers\etc\hosts **修改 hosts 文件，在其中包含以下项：** <Identity Engine VM 的 IP 地址 > <Identity Engine VM 的专用 DNS 名称 > 例如： 10.0.1.1 identityengine.example.com <Identity Applications VM 的 IP 地址 > < 应用程序网关的公共 DNS 名称 > 例如： 10.0.1.2 idmgateway.centralindia.cloudapp.azure.com
Identity Applications	导航到 Identity Engine VM 中的 **hosts** 文件。例如， C:\Windows\System32\drivers\etc\hosts **修改 hosts 文件，在其中包含以下项：** <Identity Engine VM 的 IP 地址 > <Identity Engine VM 的专用 DNS 名称 > 例如： 10.0.1.1 identityengine.example.com <Identity Applications VM 的 IP 地址 > < 应用程序网关的公共 DNS 名称 > 例如： 10.0.1.2 idmgateway.centralindia.cloudapp.azure.com

要更新 Identity Reporting 和 iManager 的主机项，请参见表 15-1 （第 185 页）中的 **Identity Applications**。

注释：有关 Identity Manager 组件的安装，请参见安装过程 （第 43 页）。

安装 Designer

1 在公用子网中，起动虚拟机实例。请参见创建虚拟机实例 （第 183 页）。

对于 Windows 安全组，请仅使用 rdesktop 端口。例如 3389。 .

2 安装 Designer。请参考第 IV 部分 “ 安装 Designer” （第 107 页）。

配置应用程序网关

配置应用程序网关后，外部网络便可使用虚拟机上托管的 Identity Manager 组件。

1 为 iManager、Identity Applications、表单和 Identity Reporting 等 Identity Manager 组件配置单独的后端池。

1a 在**后端池**中，单击**添加**。

1b 指定以下细节：

字段	说明
名称	指定用于识别 Identity Manager 组件的后端池名称。
类型	以下列方式之一指定类型： ◆ **IP 地址或 FQDN**：指定所需 Identity Manager 组件的 IP 地址或 FQDN。 ◆ **虚拟机**：选择托管所需 Identity Manager 组件的虚拟机。

1c 单击**确定**。

重复此步骤以配置更多后端池。

2 为 iManager、Identity Applications、表单和 Identity Reporting 等 Identity Manager 组件配置单独的 HTTP 设置。

注释：确保您已导出所需 Identity Manager 组件的公共证书。

2a 在 **HTTP 设置**中单击**添加**。

2b 指定以下细节：

字段	说明
名称	指定用于识别 Identity Manager 组件的 HTTP 设置名称。
协议	选择 HTTPS。
端口	指定 Identity Manager 组件的端口。 例如： ◆ **iManager**：8443 ◆ **Identity Applications**：8543 ◆ **Forms**：8600 ◆ **Identity Reporting**：8643
后端鉴定证书	1. 选择“新建”。 2. 指定证书的名称。 3. 浏览并上载为对应 Identity Manager 组件导出的公共证书。 4. 单击“添加证书”。

2c 单击**确定**。

重复此步骤以配置更多 HTTP 设置。

3 为每个 Identity Manager 组件（例如 iManager、 Identity Applications、表单和 Identity Reporting）配置单独的侦听程序。

注释：确保已从身份库导出 .PFX 证书。

3a 在**侦听程序**中单击**基本**。

3b 指定以下细节：

字段	说明
名称	指定用于识别 Identity Manager 组件的侦听程序名称。
前端 IP 配置	1. 选择之前创建的虚拟网络和子网。请参见创建虚拟网络和子网 （第 181 页）。 2. 指定应用程序的名称和端口号。例如： **iManager：** 8443 **Identity Applications：** 8543 **Forms：** 8600 **Identity Reporting：** 8643
协议	选择 HTTPS。
证书	1. 浏览并上载 PFX 证书。 2. 指定证书的名称和口令。

3c 单击确定。

重复此步骤以配置更多侦听程序。

4 为 iManager、Identity Applications、表单和 Identity Reporting 等 Identity Manager 组件创建基本规则，并将此规则与相应的后端池、侦听程序和 HTTP 设置关联。

4a 在规则中单击添加。

4b 指定以下细节：

字段	说明
名称	指定有助于识别 Identity Manager 组件的规则名称。
侦听程序	选择在步骤 3 中创建的相应侦听程序。
后端池	选择在步骤 1 中创建的相应后端池。
HTTP 设置	选择在步骤 2 中创建的相应 HTTP 设置。

4c 单击确定。

重复此步骤以配置更多规则。

16 混合 Identity Manager 方案示例

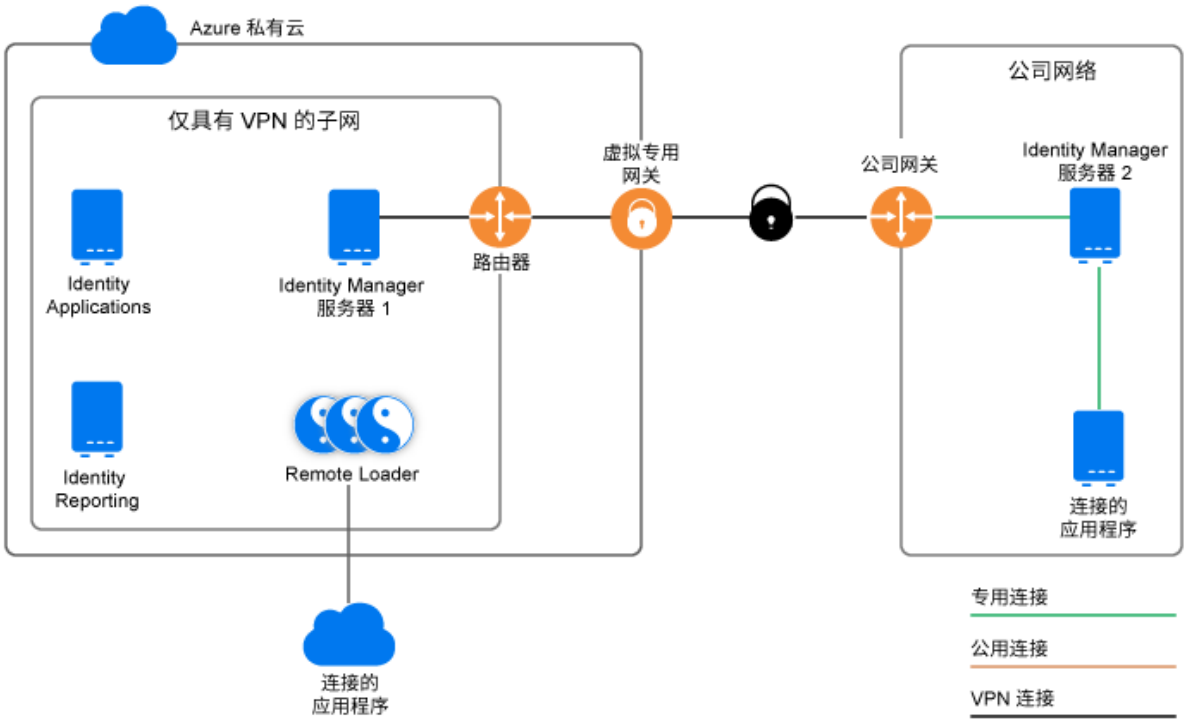
您可以对 Identity Manager 组件进行配置，使其中的身份在企业本地与 MS Azure 云之间无缝同步。要实施此类混合方案，您需要在 Azure 子网与企业网络之间配置 VPN 连接。本章将会对下面的混合方案进行说明：

- 使用多服务器驱动程序集连接 （第 189 页）
- 使用 eDirectory 驱动程序连接 （第 190 页）

使用多服务器驱动程序集连接

在此方案中，至少有两台 Identity Manager 服务器使用相同的 eDirectory 树和驱动程序集，其中的一台服务器安装在 AWS 云中，另一台服务器安装在企业本地。其中包括通过 VPN 连接使用身份库复制通道同步身份的完整复本服务器。在企业网络中或 Azure 云中运行的 Identity Manager 服务器会分别在各自的已连接应用程序之间同步身份。

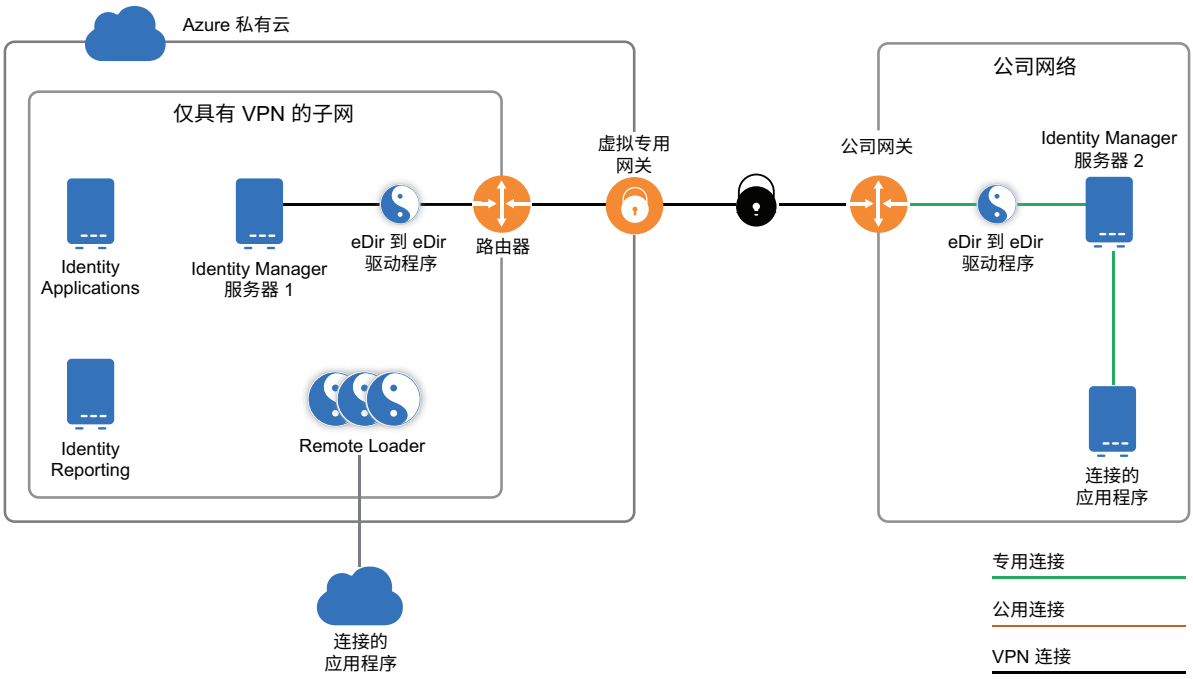
图 16-1 *使用多服务器驱动程序集连接的混合方案*



使用 eDirectory 驱动程序连接

如果您的 Identity Manager 服务器安装在两个不同的 eDirectory 树中，其中一个树属于 Azure 云，另一个树属于企业网络，则适合使用此方案。此配置使用 eDirectory 驱动程序通过 VPN 连接在 Azure 云与企业网络之间同步身份。在企业网络中或 Azure 云中运行的 Identity Manager 服务器会分别在各自的已连接应用程序之间同步身份。

图 16-2 *使用 eDirectory 驱动程序连接的混合方案*



Azure 云与企业网络之间的通讯会受到限制。此方案只能同步增量更改。您可以通过配置驱动程序过滤器来控制要同步的属性。您还可以利用策略引擎来定义有关同步属性的更多控制措施。例如，限制同步口令属性，并允许用户在 Azure 云和企业网络中使用不同的口令访问 Identity Manager 服务器。

17 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。

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）。

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。

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，请参见从身份库中去除对象 （第 192 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**。

卸装 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。

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，请参见卸装 Identity Manager 引擎 （第 192 页）。

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。

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**。

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，请参见删除报告驱动程序 （第 194 页）。
2. 删除 Identity Reporting。有关详细信息，请参见卸装 Identity Reporting （第 194 页）。
3. 删除 Sentinel。有关详细信息，请参见 《NetIQ Identity Manager 安装指南 - Linux》中的 “卸装 Sentinel Log Management for IGA”。

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。

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。

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，请参见删除报告驱动程序 （第 194 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**。

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**。

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。

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。

卸装 iManager Workstation

要卸装 iManager Workstation，请删除将文件解压缩到的目录。

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**。

18 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。

Identity Manager 引擎查错

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
当 eDirectory 初始化过程正在进行时， Identity Manager 引擎无法启动。如果 eDirectory DIB 极大，则很有可能会出现此问题。	请执行以下步骤来解决此问题： 1. 创建名为 **SLEEP_BEFORE_ENGINE_STARTUP** 的系统环境变量，并将该变量的值设置为 0 到 600。该值以秒为单位。 **注释：**如果提供的值无效或大于 600，将使用默认值 600。 2. 重启动 eDirectory。 3. （视情况而定）检查 dhost.log 以查看讯息和日志。
在多服务器环境中显示了一个无法识别的扩展异常。	确保主服务器具有次服务器的读写分区： 1. 登录到 iManager。 2. 单击**角色和任务** > **分区和复本** > **复本视图**。 3. 选择次服务器。 4. 指派对该服务器的读写许可权限。 **注释：**确保已在驱动程序集中添加了次服务器。

对 Identity Applications 和 RBPM 安装进行查错

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
“仪表板”页面上的角色和自己的任务控件不显示任何数据。如果您签入浏览器的控制台，将会显示 404 错误。将默认 IDMProv 部署环境更改为自定义环境后会出现此问题。	要解决此问题，必须更改受影响控件上的 REST API URL。请执行下列步骤： 1. 以管理员身份登录到 Identity Manager 仪表板。 2. 导航到“仪表板”页面，然后单击“管理仪表板”。 3. 要编辑角色控件中的控件配置，请执行以下操作： a. 单击 ⚙。 b. 在 **URL** 字段中，如下所示将默认 IDMProv 环境更改为自定义环境：/<custom-context>/rest/access/assignments/advanced?nextIndex=1&sortBy=name&sortOrder=ASC&forceRefresh=true&searchScope=role&size=20 其中， <custom-context> 是您在 Identity Manager 部署中使用的环境。 c. 单击应用。 4. 要编辑自己的任务控件中的控件配置，请执行以下操作： a. 单击 ⚙。 b. 在 **URL** 字段中，如下所示将默认 IDMProv 环境更改为自定义环境：/<custom-context>/rest/access/tasks/list?fromIndex=1&size=10&q=*&sortOrder=asc&sortBy=createTime&assignedTo=assignedTo&recipient=recipientAsMe&expireUnit=weeks&expireWithin=&proxyUser=&assignStatus=&delegatedTasks=false&status= c. 单击应用。 5. 单击完成编辑。

问题	建议的操作
升级群集中安装的 Identity Applications 并重启动 Tomcat 后，群集未按预期工作。	在群集的所有节点上执行以下操作： 1. 导航到 C:\NetIQ\IDM\apps\tomcat\conf 文件夹中的 server.xml 文件。 2. 在 server.xml 中取消注释下面一行。 <Cluster className="org.apache.catalina.ha.tcp.SimpleTcpCluster"/> 3. 从 Tomcat 备份目录恢复所有自定义配置。 4. 重启动 Tomcat。
升级过程不会将默认的 Identity Applications 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。
您需要修改安装过程中创建的以下一个或多个 Identity Applications 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。

问题	建议的操作
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 Identity Applications 期间指定的 JDK 来启动 Tomcat。
无法登录门户管理页面。	确保存在 Identity Applications 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。	Identity Applications 管理员必须是顶层容器的受托者，并且应该具有主管权限。您可以尝试将 Identity Applications 管理员的权限设置为与 LDAP 管理员等同的权限 （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 Identity Applications 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 实用程序检查是否提供了以下 Identity Applications 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`

安装和卸装查错

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
运行 ConfigUpdate 实用程序后，您无法登录到 Identity Applications。 catalina.out 日志文件中显示了以下错误讯息： javax.net.ssl.SSLHandshakeException: PKIX path validation failed: java.security.cert.CertPathValidatorException: Could not determine revocation status. 如果在 LDAP 服务器上将**加密的绑定限制**设置为使用 SuiteB 加密 （128 位）， Identity Manager 4.8.4（包含 eDirectory 9.2.5）中会出现此问题。Identity Manager 使用数字证书来授权并与其组件安全通讯。通过检查 CRL 分发点 (CDP) 字段指定的证书撤消列表 (CRL) 来验证证书，这项检查可以确定证书是否已撤消。根证书以及密钥存储区文件 tomcat.ks 和 idm.jks 中的中间证书都会提供 CRLDP。但是，默认已禁用证书撤消检查。因此，PKIX 信任管理器无法确定证书的撤消状态。	要解决此问题，请通过将 -Dcom.sun.security.enableCRLDP 属性设置为 true 来启用 CRL 分发点检查。 要设置该属性，请执行以下操作： 1. 停止 Tomcat。 2. 转到位于 Tomcat 的 bin 文件夹中的 setenv.sh 文件。例如 C:\NetIQ\idm\apps\tomcat\bin\setenv.bat。 3. 如下所示在 CATALINA_OPTS 中添加属性 -Dcom.sun.security.enableCRLDP=true： `export CATALINA_OPTS="-Dcom.sun.security.enableCRLDP=true"` 4. 启动 Tomcat。
升级 Identity Manager 后，非管理员用户在 Identity Manager 仪表板中的登录速度非常缓慢。装载 “ 应用程序 ” 和 “ 仪表板 ” 页面时存在很高的延迟。 此问题是由默认启用的嵌套组搜索造成的。不管环境中是否存在任何嵌套组，应用程序都会通过嵌套组成员资格查找已登录用户继承的许可权限。	（视情况而定）以下步骤适用于 Identity Manager 4.8.5 和更高版本。 1. 登录到其中的 Identity Applications 已升级到版本 4.8.5 的服务器。 2. 导航到 C:\NetIQ\IDM\apps\tomcat\conf 位置。 3. 在文本编辑器中打开 ism-configuration.properties 文件。 4. 在该文件的末尾添加以下属性： DirectoryService/realms/jndi/params/USE_NESTED_GROUPS=false 5. 保存该文件并重启动 Tomcat。

问题	建议的操作
将 Identity Applications 升级到版本 4.8.x 后，您无法登录到 Identity Applications 仪表板。如果在 Identity Applications 升级期间未将身份库可信证书存储区路径更新为正确的密钥存储区 (cacerts) 文件位置，则会出现此问题。 catalina.out 文件中记录了以下异常： com.netiq.idm.auth.oauth.AuthenticationCommunicationException: javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX path validation failed: sun.security.validator.ValidatorException: TrustAnchor with subject "CN=***, OU=idm, O=***, L=***, ST=***, C=**" is not a CA certificate" Identity Applications 使用设置为 < 安装路径 >\Common\JRE 的 JAVA_HOME 环境变量。如果未在 JAVA_HOME 中将可信证书存储区路径设置为 cacerts 文件所在位置，则 SSL 通讯会失败，导致出现与 “TrustAnchor” 相关的 SSL 错误 （信任锚用作 SSL 证书的增强式 Java 安全检查措施）。	要解决此问题，请执行以下操作： 1. 停止 Tomcat 服务。 2. 登录到 Identity Applications 服务器，并起动位于 < 安装路径 >\idm\apps\configupdate 中的 configupdate 实用程序。 3. 在 “User Application” 选项卡中，转到**身份库证书**，并确保**可信证书存储区路径**设置为 < 安装路径 >\Common\JRE\lib\security\cacerts。 4. 启动 Tomcat 服务。
将分布式环境中的 Identity Manager 升级到版本 4.8.1 后，登录 Identity Applications 失败。显示以下错误讯息： 您的登录过程未成功完成。 登录 Identity Applications 需要提供信任锚证书，以便在 Identity Applications 与 OSP 之间建立安全连接。信任锚证书必须包含 “ 主题类型 ” 设置为 “CA” 的 “ 基本限制 ” 扩展。 Identity Manager 利用属性 jdk.security.allowNonCaAnchor 来验证证书中的信任锚。此属性默认设置为 false。因此，如果在证书中找不到信任锚，则无法在 Identity Applications 与 OSP 之间建立连接，登录也会失败。您还会在 idm-osp.log 文件中看到以下异常： sun.security.validator.ValidatorException: TrustAnchor with subject "CN=***, L=***, O=***" is not a CA certificate	要解决此问题，必须满足下列任一条件： ◆ 确保用于在 Identity Applications 与 OSP 之间建立安全连接的证书是包含正确 “ 基本限制 ” 扩展的可信 CA 证书。 ◆ 如果使用的是客户端信任的自我签名证书和自定义证书，您可以更改属性 jdk.security.allowNonCaAnchor，以允许使用不包含 “ 基本限制 ” 扩展的非 CA 证书。请执行以下操作来修改 Java 安全性设置： 1. 导航到 C:\NetIQ\idm\apps\jre\lib\security\java.security 目录。 2. 设置属性值 jdk.security.allowNonCaAnchor=true。 3. 保存文件。

问题	建议的操作
升级到 Identity Applications 4.8.1 版本后，在 Identity Applications 仪表板中请求许可权限时无法打开表单。	要解决此问题，请执行以下步骤： 1. 在键盘上按 Windows + R，键入 services.msc，然后选择**确定**打开 Windows 的“服务”界面。 2. 搜索服务名称 **NetIQ Nginx Service** 和 **NetIQ IGA Form Renderer Service**。右键单击相应服务并选择**重新启动**选项。 Identity Applications 使用 NGNIX 服务在 Identity Applications 仪表板中呈现表单。
将 Identity Applications 或 Identity Reporting 升级到版本 4.8 后，控制面板中会显示多个 PostgreSQL 条目。	在控制面板中卸装以前的 PostgreSQL 版本。
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。
升级 Identity Manager 后，以下属性会添加到 ism-configuration.properties 文件中： com.netiq.idm.osp.ldap.admin-dn = cn=admin,ou=sa,o=system	请在 ism-configuration.properties 文件中注释掉该属性，然后重启动 Tomcat。它不会导致功能受损。
升级 Identity Manager 后，即使您的部署中不包含 SSPR，系统也会将以下 SSPR 属性添加到 ism-configuration.properties 文件中： com.netiq.sspr.redirect.url = https://___SSPR_IP___:___SSPR_TOMCAT_HTTPS_PORT___/sspr/public/oauth	请在 ism-configuration.properties 文件中注释掉该属性，然后重启动 Tomcat。它不会导致功能受损。

问题	建议的操作
升级 Identity Manager 后无法启动 Tomcat。在 Tomcat 日志中，您会发现几项异常以及工作流程引擎与身份库之间的通讯失败事件。	1. 登录到 iManager。 2. 导航到**角色和任务** > **NetIQ 证书访问** > **服务器证书**。 3. 选中 **SSL 证书 DNS** 复选框并单击**导出**。 4. 在**证书**下拉列表中，选择 *SSL CertificateDNS*。 5. 清除**导出私用密钥**复选框。确保**导出格式**设置为 *DER*。 6. 单击**下一步** > **保存导出的证书**将证书下载到您的系统中。 7. 登录到 Identity Applications 服务器。 8. 停止 Tomcat。 9. 导航到 C:\NetIQ\Common\JRE\bin\ 目录，并使用以下命令将证书导入到 idm.jks 文件： < 安装路径 >\NetIQ\Common\JRE\bin\keytool -import -trustcacerts -alias < 证书别名 > -keystore <idm.jks> -file < 下载的证书文件 > 10. 重启动 Tomcat。
将 Identity Manager 从 4.7.4 升级到 4.8 后，Tomcat 服务不会启动，并且日志文件中未报告任何错误。如果未在 igaworkflow 数据库的 afenginestate 表中正确更新检测信号计时器，便会出现此问题。	要解决此问题，请登录 pgAdmin 等数据库管理工具。运行以下查询，以手动更新 igaworkflow 数据库的 afenginestate 表中的检测信号计时器。 update afenginestate set heartbeat=now()::timestamp;

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
如果 Identity Applications 和 Identity Reporting 安装在同一台服务器上，而您使用 <Reporting 安装文件夹 >\bin 目录中的配置更新实用程序来更改配置，Identity Manager 仪表板将无法起动。 catalina.out 日志文件中会报告以下错误： EboPortalBootServlet [RBPM] +++++WARNING!!!! : This portal application context, IDMProv, does not match the portal.context property set in the PortalService-conf/config.xml file.Only one portal per database is allowed.Data has been loaded using the previous portal context.To correct this you must revert back to the previous portal name of, NoCacheFilter, please consult the documentation.	要进行任何配置更改，请使用 C:\NetIQ\idm\apps\UserApplication 目录中的配置更新实用程序。

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。
在第一次登录 Identity Applications 时不提示询问应答 .	1. 确保 SSPR 服务器具有使用 FQDN 创建的证书。 2. 登录 Identity Application 服务器并起动 ConfigUpdate 实用程序 （< 安装路径 >\apps\UserApplication）。 3. 导航到 **SSO 客户端** > **Self Service Password Reset**，确保设置正确无误。 如果 SSPR 安装在单独的服务器上，请确保 SSPR 证书已导入到 Identity Applications 服务器上 / netiq/idm/apps/tomcat/conf 中的 idm.jks。

问题	建议的操作
访问 SSPR URL 时浏览器显示空白页 .	未使用 OSP 正确配置 SSPR 时，会出现这种情况。SSPR 日志会显示以下信息： `2018-01-24T22:24:02Z, ERROR, oauth.OAuthConsumerServlet, 5071 ERROR_OAUTH_ERROR (unexpected error communicating with oauth server: password.pwm.error.PwmUnrecoverableException: 5071 ERROR_OAUTH_ERROR (io error during oauth code resolver http request to oauth server: Certificate for <IP> doesn't match any of the subject alternative names: [IP]))` 1. 校验运行 OSP 的 Tomcat 服务器是否具有使用 FQDN 创建的有效证书。登录 Identity Applications 服务器，并起动 ConfigUpdate 实用程序。导航到 **SSO 客户端 > Self Service Password Reset**，并确保设置正确。 2. 通过覆盖 OSP 登录方法登录 SSPR （例如，https://<sspr sserver ip>:<port>/sspr/private/Login?sso=false）。 3. 导航到页面右上角的**配置编辑器**。 4. 指定**配置口令**，然后单击**登录**。 5. 导航到 **LDAP** > **LDAP 目录** > **默认** > **连接**。 6. 如果 LDAP 证书不正确，请单击**清除**。 7. 要重新导入证书，请单击**从服务器导入**。 8. 导航到**设置 > 单点登录 (SSO) 客户端 > OAuth**，并在 **OAUTH Web 服务服务器证书**下校验证书是否正确。 9. 如果证书不正确，请单击**清除**。 10. 要重新导入证书，请单击**从服务器导入**。

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）。

对 .NET Remote Loader 在 Windows 2016 上不启动的问题查错

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
此问题随机出现。如果 .NET Remote Loader 的命令提示符的前端设置与主机操作系统的默认设置不同，此问题便可能出现。	通过删除 HKEY_CURRENT_USER\Console 注册表项将命令提示符设置更改为与系统默认设置一致，然后重启动服务器。

对在 Azure 部署中装载表单时出现 “502 错误的网关 ” 进行查错

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 Azure 环境中部署 IDM 4.8 组件之后。在 IDM 仪表板中，当您单击咨询台凭单或尝试审批任何任务时，您可能会看到以下错误。 `502 - Web server received an invalid response while acting as a gateway or proxy server.`	请执行以下步骤来解决此问题： 1. 导航到系统中的 Nginx\conf 位置。 例如 C:\NetIQ\Common\Nginx\conf 2. 在 nginx.conf 文件中： a. 在 error_page 502 /502.html; 行下面添加 **error_page 404 =200 /404.html**。 b. 将 **proxy_intercept_errors off;** 设置为 proxy_intercept_errors on;。 3. 在 Services.msc 中重启动 NetIQ Nginx Service。

IX 部署 Identity Manager 以实现高可用性

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时， Identity Manager 引擎也会群集化。

注释：Identity Manager 不支持在身份库与 Identity Applications 之间进行负载平衡 LDAP 或 LDAPS 通讯。

有关更多详细信息 ...	请参见 ...
确定 Identity Manager 组件的服务器配置	请参见 《NetIQ Identity Manager Overview and Planning Guide》（NetIQ Identity Manager 概述和规划指南）中的 “*High Availability Configuration*” （高可用性配置）。
在群集中运行身份库	Identity Manager 群集部署解决方案示例 《*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	Identity Applications 群集部署解决方案示例

有关在 Identity Manager 环境中实现高可用性和灾难恢复的详细信息，请联系 NetIQ 技术支持 (https://www.netiq.com/support/)。

以下几章提供了有关在高可用性环境中安装和配置 Identity Manager 组件的步骤：

- 第 19 章 “ 在群集环境中安装 Identity Manager 的准备工作 ” （第 211 页）
- 第 20 章 “Identity Manager 群集部署解决方案示例 ” （第 215 页）
- 第 21 章 “Identity Applications 群集部署解决方案示例 ” （第 217 页）

19 在群集环境中安装 Identity Manager 的准备工作

- 先决条件
- 为 Identity Applications 准备群集

先决条件

- 身份库
- Identity Applications
- Identity Applications 的数据库

身份库

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）。

Identity Applications

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。

Identity Applications 的数据库

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。

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 213 页）
- 设置工作流程引擎 ID 的系统属性 （第 213 页）
- 为群集中的每个用户应用程序使用相同的主密钥 （第 213 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。

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。

20 Identity Manager 群集部署解决方案示例

本章通过逐步说明介绍如何在 Windows 2016 平台上的群集环境中配置 Identity Manager。

- 先决条件 （第 215 页）
- 在 eDirectory 群集上配置 NetIQ Identity Manager （第 215 页）
- Remote Loader 群集化 （第 215 页）

先决条件

在 Windows 2016 上的群集环境中运行的 Identity Vault 9.2。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：身份库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。

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"

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：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。

21 Identity Applications 群集部署解决方案示例

本章通过一个示例部署说明如何在 Tomcat 应用程序服务器上的群集环境中配置 Identity Applications。

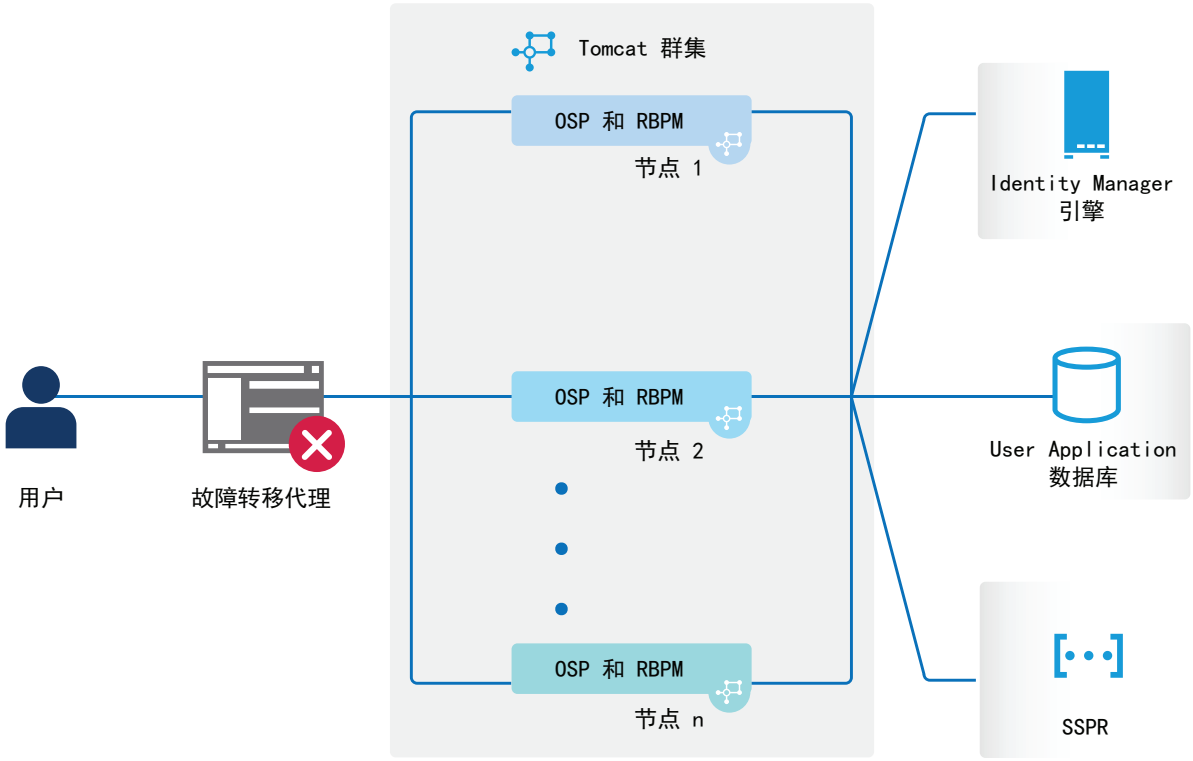
使用群集，您可以在多个并行服务器 （群集节点）上运行 Identity Applications，同时实现高可用性。要构建群集，您需要将几个 Tomcat 实例 （节点）组合在一起。负载将分布在不同的服务器之间，即使有服务器发生故障，您仍可通过其他群集节点来访问 Identity Applications。若要实现故障转移，您可以创建一个 Identity Applications 群集，然后将它们配置为充当单个服务器。不过，此配置不包括 Identity Reporting。

建议使用负载平衡器软件，它会处理所有用户请求并将它们发送给群集中的服务器节点。负载平衡器通常是群集的一部分。它了解群集配置及故障转移策略。您可以选择最适合您的解决方案。

图 21-1 显示了一个包含双节点群集的示例部署，并做出如下假设：

- 所有通讯都通过负载平衡器路由。
- Identity Manager 引擎和 User Application 等组件安装在单独的服务器上。建议对生产级别部署采用此方法。
- 您熟悉 eDirectory、Identity Manager 引擎、Identity Applications、Apache Tomcat 应用程序服务器和 User Application 数据库的安装过程。
- OSP (One Single-Sign On Provider) 和 User Application 安装在同一个群集节点上。但在生产环境中，您可以将 OSP 安装其他服务器上。在此情况下，您需要执行安装过程 （第 219 页）中所述的一些配置更改。
- SSPR (Single Sign-On Password Reset) 安装在单独的计算机上。建议对生产级别部署采用此方法。
- 使用 PostgreSQL 作为 User Application 的数据库。不过，您可以使用 Identity Manager 4.8 支持的任何数据库，例如 Oracle、 SQL Server 或 PostgreSQL。
- 所有 User Application 节点均与 eDirectory 和 User Application 数据库的同一个实例通讯。您可以根据自己的需要增加 User Application 实例数量。

图 21-1 群集部署解决方案示例



注释：双节点群集是实现高可用性的最低配置。但是，您可以轻松地将本章中的概念扩展到具有多个节点的群集。

为了帮助您了解逐步配置，本文后续小节中通篇都会参照此示例部署。

先决条件

- 两台运行 Windows Server 2012、 Windows Server 2012 R2 或 Windows Server 2016 的服务器作为节点。
- 已安装不低于 4.8 版的 Identity Manager 组件。要升级到 Identity Manager 4.8，请参见第 11 章 “ 升级 Identity Manager 组件 ” （第 137 页）。
- 所有节点的应用程序服务器时钟都相同。确保这一点最简单的方法就是将节点配置为使用同一个网络时间服务器来通过 NTP 同步时间。
- 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。
- 要实现表单群集化，请在服务器上启动两个负载平衡器实例，一个用于 Identity Applications，另一个用于表单渲染器。

安装过程

本节提供在 Tomcat 上安装新 Identity Applications 实例，然后针对群集配置该实例的逐步说明。

1. 安装 Identity Manager 引擎。有关逐步指导，请参见安装过程 （第 43 页）。对于生产级别部署，建议将 Identity Manager 引擎安装在单独的服务器上。
2. 为 Identity Applications 创建并部署以下驱动程序：
   - 用户应用程序驱动程序
   - Roles and Resource Service 驱动程序
3. 在节点 1 上安装以下 Identity Manager 组件：
   a. User Application

      在安装过程中配置以下设置：

      i. 选择 **Tomcat** 作为应用程序服务器。

      ii. 选择 **PostgreSQL** 作为数据库平台。

      注释：您可以使用 Identity Manager 4.8 支持的任何数据库。

      ---

      iii. 在后续页面中提供必需的数据库细节。

      iv. 将 PostgreSQL 服务器上的数据库驱动程序 jar 文件 postgresql-9.4.1212.jar 复制到群集中的所有 User Application 节点上。

      注释：如果您使用的是 Identity Manager 4.8 支持的其他数据库 （例如 Oracle 或 SQL Server），请务必将安装了数据库的服务器上的相应驱动程序 jar 文件复制到群集中的所有 User Application 节点上。有关详细信息，请参见配置 Identity Applications 的数据库 （第 64 页）。

      ---

      v. 浏览并选择所复制的数据库驱动程序 jar 文件。

      vi. 在新数据库或现有数据库的细节页面中，选择**新数据库**选项。

      vii. 在 Identity Manager“ 配置 ” 页面的**工作流程引擎 ID** 字段中提供唯一的名称。例如，您可以为节点 1 使用唯一的名称 Engine1。

      viii. 要创建新的主密钥，请在 “ 安全性 – 主密钥 ” 页面中选择**否**。

      Identity Applications 使用主密钥加密敏感数据。由于这是群集中的第一个 Identity Applications 实例，因此必须选择**否**来指示安装程序创建新的主密钥。在群集中， User Application 群集要求每个 User Application 实例都使用相同的主密钥。为确保使用相同的主密钥，请在配置这些实例时选择**是**以导入现有密钥。
4. 在节点 2 上执行以下操作：
   a. 使用便捷安装程序安装 Tomcat （在安装过程中只选择 Tomcat）。
   b. 安装 OSP。

      安装期间，请在鉴定细节页面中提供 Identity Manager 引擎 (eDirectory) 服务器的 IP 地址和端口号。
   c. 安装 User Application。

在安装过程中配置以下设置：

i. 选择 **Tomcat** 作为应用程序服务器。

ii. 选择 **PostgreSQL** 作为数据库平台。

注释：您可以使用 Identity Manager 4.8 支持的任何数据库。

---

iii. 在安装过程的后续页面中提供必需的数据库细节。

iv. 将 PostgreSQL 服务器上的数据库驱动程序 jar 文件 postgresql-9.4.1212.jar 复制到节点 2 上。

注释：如果您使用的是 Identity Manager 4.8 支持的任何其他数据库 （例如 Oracle 或 SQL Server），请务必将安装了数据库的服务器上的相应驱动程序 jar 文件复制到群集中的所有 User Application 节点上。

---

v. 浏览并选择所复制的数据库驱动程序 jar 文件。

vi. 在新数据库或现有数据库的细节页面中，选择**现有数据库**选项。

vii. 在 Identity Manager“ 配置 ” 页面的**工作流程引擎 ID** 字段中提供唯一的名称。例如，您可以为节点 2 使用唯一的名称 Engine2。

viii. 要在 “ 安全性 – 主密钥 ” 页面中创建新的主密钥，请选择**是**。

User Application 群集要求每个 User Application 实例都使用相同的主密钥。为确保使用相同的主密钥，请选择**是**以导入现有密钥。此密钥是您在节点 1 中安装第一个 User Application 实例时创建的。

您可以从节点 1 上位于 C:\NetIQ\IDM\apps\tomcat\conf 中的 ism-configuration 属性文件获取主密钥。包含主密钥的参数是 com.novell.idm.masterkey。

ix. 单击**安装**以完成安装。

注释：有关安装 Identity Applications 的详细信息，请参见安装过程 （第 43 页）。

---

5. 在负载平衡器服务器中，针对所有群集节点使用 Identity Applications 端口号启动一个负载平衡器实例，使用表单渲染器端口号启动另一个负载平衡器实例。例如，

   - ./balance 8543 apps1-au.edu.in:8543 ! apps2-au.edu.in:8543
   - ./balance 8600 apps1-au.edu.in:8600 ! apps2-au.edu.in:8600

6. 在单独的计算机上安装 SSPR。

   安装前请记下以下设置并在安装过程中指定这些设置：

   a. 安装 **Tomcat**。有关安装说明，请参见步骤 4a。

   b. 安装 **SSPR**。

      在 SSPR 安装期间，请执行以下操作：

      i. 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。

      ii. 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，起动 SSPR (https://<IP>:< 端口 >/sspr/private/config/ConfigEditor) 并登录其中。单击**配置编辑器** > **设置** > **安全性** > **重定向白名单**。

   i. 单击**添加值**并指定以下 URL：

      https:< 故障转移的 DNS>< 端口 >/osp

   ii. 保存更改。

   iii. 在 SSPR 配置页面中，单击**设置** > **OAuth SSO**，然后修改 OSP 链接 - 用安装了负载平衡器软件的服务器的 DNS 名称替换 IP 地址。

   iv. 单击**设置** > **应用程序**，然后更新转发和注销 URL - 用安装了负载平衡器软件的服务器的 DNS 名称替换 IP 地址。

d. 要在节点 1 上更新 SSPR 信息，请起动位于 C:\NetIQ\idm\apps\UserApplication\configupdate.bat 的配置实用程序。

   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。

注释：校验节点 2 中是否更新了这些参数的值。

---

7. 在群集节点上执行以下配置任务：

   a. 在所有群集节点上重启动 Tomcat。

   b. 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 63 页）。

   c. 在节点 2 上，校验是否已用 SSPR IP 地址更新 “ 忘记口令 ” 链接和 “ 更改我的口令 ” 链接。

      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。

8. 在节点 1 中，停止 Tomcat，并使用以下命令指定负载平衡器服务器的 DNS 名称以生成新的 osp.jks 文件：

   C:\NetIQ\Common\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\ -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。

---

9. （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\Common\JRE\bin\keytool -list -v -keystore osp.jks -storepass changeit

10. 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 8 中创建的。

11. 将节点 1 上的新 osp.jks 文件复制到群集中的其他 User Application 节点上。

12. 在每个群集节点上：

    a. 导航到 C:\netiq\idm\apps\sites 目录，然后编辑 ServiceRegistry.json 文件以添加负载平衡器细节。

    ```
    {"serviceRegisteries":[{"serviceID":"IDM","restUrl":"https://<DNS
    of the load balancer>:8543/IDMProv"}]}
    ```

    b. 导航到 C:\netiq\idm\apps\sites\ 目录，然后编辑 config.ini 文件以添加负载平衡器 DNS 和端口号。

    ```
    OSPIssuerUrl=https://<DNS of the load balancer>:8543/osp/a/idm/
    auth/oauth2
    OSPRedirectUrl=https://<DNS of the load balancer>:8600/forms/
    oauth.html
    ClientID=forms
    OSPLogoutUrl=https://<DNS of the load balancer>:8543/osp/a/idm/
    auth/app/logout
    ```

13. 在节点 1 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。

    a. 保存配置实用程序中所做的更改。检查 ism-configuration properties 文件是否体现了相应更改，如果有任何 URL 仍指向节点 1 DNS 和端口，请予以修改。

    b. 要在群集的所有其他节点中反映此更改，请将节点 1 上位于 C:\NetIQ\IDM\apps\tomcat\conf 中的 ism-configuration properties 文件复制到群集中的其他 User Application 节点上。

    注释：您之前已将节点 1 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不同 DNS 名称。请对安装了 OSP 的所有服务器执行此操作。执行此操作可确保所有 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。

    ---

14. 在位于 /TOMCAT_INSTALLED_HOME/bin/ 目录下的 setevn.sh 文件中执行以下操作：

    a. 为确保 mcast_addr 绑定成功， JGroups 要求将 preferIPv4Stack 属性设置为 **true**。为此，请在所有节点上的 setenv.sh 文件中添加 JVM 属性 “-Djava.net.preferIPv4Stack=true”。

    b. 在节点 1 上的 setenv.sh 文件中添加 “-Dcom.novell.afw.wf.Engine-id=Engine1”。同样，为群集中的每个节点添加唯一的引擎名称。例如，对于节点 2，您可以添加引擎名称 Engine2。

15. 在 User Application 中启用群集。

    a. 在节点 1 上启动 Tomcat。

    不要启动任何其他服务器。

    b. 以 User Application 管理员身份登录 User Application。

c. 单击**配置** > **超速缓存和群集**选项。

User Application 将显示 “ 超速缓存管理 ” 页面。

d. 单击**群集超速缓存配置**，然后为**群集已启用**属性选择 **True**。

e. 单击**保存**。

f. 重启动 Tomcat。

注释：如果您已选择 “ 启用本地 ” 设置，请针对群集中的每个服务器重复此过程。

User Application 群集使用 JGroups 在采用默认 UDP 的节点间进行超速缓存同步。如果您想将此协议更改为使用 TCP，请参见 “Configuring User Application to use TCP” （将 User Application 配置为使用 TCP）。

---

16. 为群集启用许可权限索引。有关详细信息，请参见为群集启用许可权限索引 （第 224 页）。

17. 启用 Tomcat 群集。

    在所有群集节点上打开 /TOMCAT_INSTALLED_HOME/conf/ 中的 Tomcat server.xml 文件，并取消注释此文件中的下面一行：

    <Cluster className="org.apache.catalina.ha.tcp.SimpleTcpCluster"/>

    对于高级 Tomcat 群集配置，请按照 Apache 文档网站中的步骤操作。

18. 在所有节点上重启动 Tomcat。

19. 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。

    a. 登录管理身份库的 iManager 实例。

    b. 在导航框架中，选择 **Identity Manager**。

    c. 选择 **Identity Manager 概述**。

    d. 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。

    e. 单击驱动程序图标右上角的圆形状态指示器：

    f. 选择**编辑属性**。

    g. 对于**驱动程序参数**，请将**主机**更改为负载平衡器的主机名或 IP 地址。

    h. 单击**确定**。

    i. 重启动驱动程序。

20. 要更改 Roles and Resource Service 驱动程序的 URL，请重复步骤 19a 到 19f，然后单击**驱动程序配置**，用负载平衡器 DNS 名称更新 **User Application URL**。

21. 确保针对 User Application 节点的负载平衡器软件中创建的群集启用了会话粘性。

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

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**。