
NetIQ Identity Manager

安装指南 - Linux

2018 年 2 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、美国政府限制权限、专利政策以及 FIPS 合规性的信息，请访问 <http://www.netiq.com/company/legal/>。

Copyright (C) 2018 NetIQ Corporation. 保留所有权利。

目录

关于本书和库	11
关于 NetIQ Corporation	13
I 简介	15
1 Identity Manager 的组件概述	17
2 创建和维护 Identity Manager 环境	19
2.1 Designer for Identity Manager	19
2.2 Analyzer for Identity Manager	19
2.3 iManager	20
3 在 Identity Manager 环境中管理数据	21
3.1 了解数据同步	21
3.2 了解审计、报告和合规性	21
3.3 了解用于同步身份数据的组件	22
3.3.1 身份库	22
3.3.2 Identity Manager 引擎	22
3.3.3 Remote Loader	22
3.3.4 Identity Reporting	22
4 供应用户以进行安全的访问	25
4.1 了解 Identity Manager 中的证明过程	25
4.2 了解 Identity Manager 中的自助服务过程	26
4.3 了解管理用户供应的组件	26
4.3.1 User Application 和 Roles Based Provisioning Module	27
4.3.2 Identity Applications 管理	28
4.3.3 Identity Manager 仪表盘	28
II 规划安装 Identity Manager	31
5 规划概述	33
5.1 规划核对清单	33
5.2 了解 Identity Manager 通讯	34
5.3 了解安装文件	35
5.4 目录结构	36
5.5 默认安装位置	36
5.6 安装的组件版本	37
5.7 建议的安装方案和服务器设置	38
5.7.1 将事件发送到审计服务而不在 Identity Manager 中报告	38
5.7.2 将事件发送到 Identity Manager 并生成报告	38
5.7.3 将事件推送到 Identity Manager 之前先将事件发送到外部服务	39
5.7.4 建议的服务器设置	39
5.7.5 选择 Identity Manager 的操作系统平台	40

5.8	了解许可和激活	41
5.9	准备安装	41
5.9.1	确保 Identity Manager 的高可用性	42
5.9.2	Linux 服务器上的最低空间要求	42
5.9.3	在 SLES 12 SP2 或更高版本的服务器上安装 Identity Manager	43
5.9.4	在 RHEL 7.3 或更高版本的服务器上安装 Identity Manager	43
5.10	了解语言支持	46
5.10.1	已翻译的组件和安装程序	46
5.10.2	语言支持的特别注意事项	47
5.11	下载安装文件	47
III	安装 Sentinel Log Management for Identity Governance and Administration	49
6	计划安装 SLM for IGA	51
6.1	安装 SLM for IGA 的核对清单	51
6.2	系统要求	51
7	安装 SLM for IGA	53
7.1	标准安装	53
7.2	自定义安装	53
IV	安装和配置 Identity Manager 引擎、Identity Applications 及 Identity Reporting	55
8	计划安装 Identity Manager 引擎、Identity Applications 和 Identity Reporting	57
8.1	安装 Identity Manager 组件的核对清单	57
8.2	了解安装程序	58
8.2.1	Identity Manager 引擎	58
8.2.2	Identity Manager Remote Loader 服务器	58
8.2.3	Identity Manager 扇出代理	58
8.2.4	iManager Web 管理	59
8.2.5	Identity Applications	59
8.2.6	Identity Reporting	59
8.3	计划安装 Identity Manager 引擎	59
8.3.1	安装 Identity Manager 引擎的注意事项	59
8.3.2	随 Identity Manager 引擎一起安装驱动程序的注意事项	60
8.3.3	在群集环境中安装身份库的先决条件	60
8.3.4	Identity Manager 引擎、Remote Loader 和 iManager 的系统要求	61
8.4	规划安装 Remote Loader	62
8.4.1	Remote Loader 安装核对清单	63
8.4.2	了解 Remote Loader	64
8.4.3	了解安装程序	65
8.4.4	在同一台计算机上使用 32 位和 64 位 Remote Loader	65
8.4.5	安装 Remote Loader 的先决条件和注意事项	66
8.5	计划安装 Identity Applications	67
8.5.1	Identity Applications 安装核对清单	68
8.5.2	安装 Identity Applications 的先决条件和注意事项	69
8.5.3	Identity Applications 的系统要求	75
8.6	规划安装 Identity Reporting	77
8.6.1	Identity Reporting 的安装核对清单	77
8.6.2	安装 Identity Reporting 组件的先决条件	78
8.6.3	了解 Identity Reporting 组件的安装过程	79
8.6.4	Identity Reporting 的系统要求	80

9	安装 Identity Manager 引擎、Identity Applications 和 Identity Reporting	83
9.1	安装 Identity Manager 引擎	83
9.1.1	执行交互式安装	83
9.1.2	以无提示模式安装 Identity Manager 引擎	84
9.1.3	以非 root 用户身份安装 Identity Manager 引擎	84
9.2	安装 Java Remote Loader	87
9.3	安装 Identity Applications	88
9.3.1	执行交互式安装	88
9.3.2	以无提示模式安装	88
9.3.3	以交互模式安装 SSPR	89
9.3.4	以无提示模式安装 SSPR	89
9.4	安装 Identity Reporting	89
9.4.1	执行交互式安装	90
9.4.2	以无提示模式安装	90
10	配置安装的组件	91
10.1	了解配置参数	91
10.2	执行配置	95
10.2.1	执行交互式配置	95
10.2.2	执行无提示配置	96
11	完成安装的最后步骤	97
11.1	完成非 Root 用户安装	97
11.1.1	为口令策略创建容器	97
11.1.2	增加对电子邮件通知中的图形的支持	97
11.2	安装后配置身份库	98
11.2.1	使用 ndsconfig 实用程序修改 eDirectory 树和复本服务器	98
11.2.2	使用 ndsmanage 实用程序管理实例	103
11.3	配置 Remote Loader 和驱动程序	105
11.3.1	创建与 Identity Manager 引擎的安全连接	105
11.3.2	了解 Remote Loader 的配置参数	108
11.3.3	为驱动程序实例配置 Remote Loader	115
11.3.4	为驱动程序实例配置 Java Remote Loader	116
11.3.5	配置 Identity Manager 驱动程序以与 Remote Loader 配合使用	117
11.3.6	配置与 Identity Manager 引擎的相互鉴定	118
11.3.7	校验配置	124
11.3.8	启动 Remote Loader 中的驱动程序实例	124
11.3.9	停止 Remote Loader 中的驱动程序实例	125
11.4	配置 Identity Applications 的身份库	125
11.5	为群集配置 User Application 驱动程序	126
11.6	配置 Identity Applications 的设置	126
11.6.1	运行 Identity Applications 配置实用程序	126
11.6.2	用户应用程序参数	127
11.6.3	报告参数	136
11.6.4	鉴定参数	137
11.6.5	SSO 客户端参数	140
11.6.6	CEF 审计参数	144
11.7	启动 Identity Applications	144
11.8	为群集配置 OSP 和 SSPR	144
11.8.1	配置 SSPR 以支持群集	145
11.8.2	在群集节点上配置任务	145
11.9	配置运行时环境	146
11.9.1	将数据收集服务驱动程序配置为从 Identity Applications 收集数据	147
11.9.2	迁移数据收集服务驱动程序	147
11.9.3	添加对自定义属性和对象的支持	149

11.9.4	添加多个驱动程序集支持	152
11.9.5	将驱动程序配置为使用 SSL 在远程模式下运行.	153
11.10	配置 Identity Reporting	154
11.10.1	在“身份数据收集服务”页面中手动添加数据源	154
11.10.2	对 Oracle 数据库运行报告.	154
11.10.3	手动生成数据库纲要	155
11.10.4	清除数据库校验和	156
11.10.5	部署 Identity Reporting 的 REST API	156
11.10.6	连接远程 Remote PostgreSQL 数据库	156
V	安装 Designer	159
12	规划安装 Designer	161
12.1	Designer 安装核对清单	161
12.2	Designer 的安装先决条件	161
12.3	Designer 的系统要求	161
13	安装 Designer	163
VI	安装 Analyzer	165
14	计划安装 Analyzer	167
14.1	Analyzer 安装核对清单	167
14.2	Analyzer 安装先决条件	167
14.3	Analyzer 的系统要求	168
15	安装 Analyzer	169
15.1	使用向导安装 Analyzer	169
15.2	以无提示模式安装 Analyzer	170
15.3	将 XULrunner 添加到 Analyzer.ini 中	170
15.4	安装 Analyzer 的审计客户端.	171
VII	在 Identity Manager 中配置单点登录访问	173
16	准备单点登录访问	175
17	在 Identity Manager 中使用 One SSO Provider 进行单点登录访问	177
17.1	准备 eDirectory 进行单点登录访问	177
17.2	修改单点登录访问的基本设置	177
17.3	将 Self Service Password Reset 配置为信任 OSP	178
18	对 NetIQ Access Manager 使用 SAML 鉴定进行单点登录	179
18.1	了解第三方鉴定和单点登录	179
18.2	创建和安装 SSL 证书.	179
18.2.1	为 Access Manager 创建 SSL 证书.	180
18.2.2	在 Identity Manager 可信证书存储区中安装 Access Manager 证书	180
18.2.3	在 Access Manager 可信证书存储区中安装 SSL 服务器证书.	181
18.3	将 Identity Manager 配置为信任 Access Manager	181

18.4	将 Access Manager 配置为与 Identity Manager 配合工作	182
18.4.1	复制 Identity Manager 的元数据	182
18.4.2	创建 SAML 的属性集	182
18.4.3	将 Identity Manager 添加为可信的服务提供程序	183
18.5	更新 Access Manager 的登录页面	183
19	校验是否可对 Identity Applications 进行单点登录访问	185
20	使用 SSL 进行安全通讯	187
20.1	确保 SSL 连接的核对清单	187
20.2	创建密钥存储区和证书签名请求	188
20.3	使用外部 CA 签名的证书启用 SSL	189
20.4	使用自我签名证书启用 SSL	190
20.4.1	导出证书颁发机构	190
20.4.2	生成自我签名证书	191
20.5	在 Sentinel 与 Identity Manager 组件之间启用 SSL	192
20.5.1	在 Sentinel 与 Identity Manager 引擎 /Remote Loader 之间启用 SSL	193
20.5.2	在 Sentinel 与 User Application 之间启用 SSL	194
20.6	更新应用程序服务器的 SSL 设置	195
20.7	在配置实用程序中更新 SSL 设置	196
20.8	更新 Self Service Password Reset 的 SSL 设置	197
VIII	安装后任务	199
21	配置已连接系统	201
21.1	创建和配置驱动程序集	201
21.1.1	创建驱动程序集	201
21.1.2	将默认口令策略指派给驱动程序集	201
21.1.3	在身份库中创建口令策略对象	202
21.1.4	创建自定义口令策略	203
21.1.5	在身份库中创建默认通知集合对象	203
21.2	创建驱动程序	203
21.3	定义策略	204
22	配置忘记口令管理	205
22.1	使用 Self Service Password Reset 进行忘记口令管理	205
22.1.1	将 Identity Manager 配置为使用 Self Service Password Reset	205
22.1.2	为 Identity Manager 配置 Self Service Password Reset	206
22.1.3	锁定 SSPR 配置	206
22.2	使用外部系统进行忘记口令管理	207
22.2.1	指定外部忘记口令管理 WAR 文件	207
22.2.2	测试外部忘记口令配置	208
22.2.3	配置应用程序服务器之间的 SSL 通讯	208
22.3	针对分布式环境或群集环境更新仪表板中的 SSPR 链接	208
23	管理驱动程序活动	209
23.1	停止和启动 Identity Manager 驱动程序	209
23.1.1	停止驱动程序	209
23.1.2	启动驱动程序	210

24 激活 Identity Manager	213
24.1 安装产品激活身份凭证	213
24.2 查看 Identity Manager 和驱动程序的产品激活	214
24.3 激活 Identity Manager 驱动程序	214
24.4 激活特定的 Identity Manager 组件	214
24.4.1 激活 Designer	215
24.4.2 激活 Analyzer	215
24.4.3 激活 Sentinel Log Management for IGA	215
 IX 升级 Identity Manager	 217
25 准备升级 Identity Manager	219
25.1 Identity Manager 的升级核对清单	219
25.2 了解升级过程	220
25.3 支持的升级路径	221
25.3.1 从 Identity Manager 4.6.x 版本升级	221
25.3.2 从 Identity Manager 4.5.x 版本升级	222
25.4 备份当前配置	224
25.4.1 导出 Designer 项目	225
25.4.2 导出驱动程序的配置	226
 26 升级 Identity Manager 组件	 227
26.1 升级顺序	227
26.2 升级 Designer	227
26.3 升级 Identity Manager 引擎	228
26.3.1 升级身份库	228
26.3.2 升级 Identity Manager 引擎	228
26.3.3 升级 Remote Loader	229
26.3.4 升级 iManager	230
26.4 升级 Identity Manager 驱动程序	231
26.4.1 创建新驱动程序	232
26.4.2 用包的内容替换现有内容	232
26.4.3 保留当前内容并通过包添加新内容	232
26.5 升级 Identity Applications	233
26.5.1 了解升级程序	234
26.5.2 升级的先决条件和注意事项	234
26.5.3 系统要求	235
26.5.4 升级 PostgreSQL 数据库	235
26.5.5 升级 Identity Applications 的驱动程序包	238
26.5.6 升级 Identity Applications	238
26.5.7 升级后任务	239
26.6 升级 Identity Reporting	242
26.6.1 升级的先决条件和注意事项	243
26.6.2 升级 Identity Reporting 的驱动程序包	243
26.6.3 升级 Sentinel Log Management for IGA	243
26.6.4 升级操作系统	244
26.6.5 升级 Identity Reporting	244
26.6.6 Reporting 的升级后步骤	245
26.6.7 校验 Identity Reporting 的升级	245
26.7 升级 Analyzer	245
26.8 将新服务器添加到驱动程序集	246
26.8.1 将该新服务器添加到驱动程序集中	246
26.8.2 从驱动程序集中去除旧服务器	246
26.9 将自定义策略和规则恢复到驱动程序	247

26.9.1	使用 Designer 将自定义策略和规则恢复为驱动程序	247
26.9.2	使用 iManager 将自定义策略和规则恢复为驱动程序	248
27	从 Advanced Edition 切换到 Standard Edition	249
X	将 Identity Manager 数据迁移到新安装	251
28	准备迁移 Identity Manager	253
28.1	执行迁移的核对清单	253
28.2	在迁移期间停止和启动 Identity Manager 驱动程序	254
29	将 Identity Manager 迁移到新服务器	255
29.1	Identity Manager 的迁移核对清单	255
29.2	准备要迁移的 Designer 项目	256
29.3	复制驱动程序集的服务器特定信息	256
29.3.1	在 Designer 中复制服务器特定信息	257
29.3.2	在 iManager 中更改服务器特定信息	257
29.3.3	更改 User Application 的服务器特定信息	258
29.4	将 Identity Manager 引擎迁移到新服务器	258
29.5	迁移 User Application 驱动程序	258
29.5.1	导入新的基础包	258
29.5.2	升级现有的基础包	259
29.5.3	部署迁移的驱动程序	259
29.6	升级 Identity Applications	259
29.7	完成 Identity Applications 的迁移	260
29.7.1	准备 Oracle 数据库以运行 SQL 文件	260
29.7.2	清理浏览器超速缓存	261
29.7.3	更新 SharedPagePortlet 的最大超时设置	261
29.7.4	禁用组的自动查询设置	261
29.8	迁移 Identity Reporting	262
29.8.1	从事件审计服务迁移到 Sentinel Log Management for IGA	262
29.8.2	设置新 Reporting 服务器	265
29.8.3	创建数据同步策略	265
30	卸载 Identity Manager 组件	267
30.1	从身份库中去除对象	267
30.2	卸载 Identity Manager 引擎	267
30.3	卸载 Identity Applications	268
30.4	卸载 Identity Reporting 组件	268
30.4.1	删除报告驱动程序	268
30.4.2	卸载 Identity Reporting	269
30.4.3	卸载 Sentinel	269
30.5	卸载 Designer	269
30.6	卸载 Analyzer	269
31	查错	271
31.1	User Application 和 RBPM 安装查错	271
31.2	登录查错	272
31.3	卸载查错	273

A	使用身份库的多个实例	275
A.1	了解 eDirectory 中的 Identity Manager 对象	275
A.2	在服务器上复制 Identity Manager 需要的对象	275
A.3	使用“范围过滤”管理不同服务器上的用户	276
A.4	了解身份库安装套件中的 Linux 包	278
B	SLES 12 SP2 上简单的 Identity Manager 群集部署解决方案	281
B.1	先决条件	281
B.2	安装过程	282
B.2.1	配置 iSCSI 服务器	282
B.2.2	在所有节点上配置 iSCSI 发起程序	283
B.2.3	对共享储存进行分区	283
B.2.4	安装 HA Extension	283
B.2.5	设置 Softdog 检查包	284
B.2.6	配置 HA 群集	284
B.2.7	在群集节点上安装并配置 eDirectory 和 Identity Manager	285
B.2.8	配置 eDirectory 资源	285
B.2.9	eDirectory 和共享储存子资源的原始值	286
B.2.10	更改位置约束分数	287
C	Tomcat 应用程序服务器上的示例 Identity Applications 群集部署解决方案	289
C.1	先决条件	290
C.2	安装过程	290

关于本书和库

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

适用对象

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

库中的其他信息

有关 Identity Manager 库的详细信息，请参见 [Identity Manager 文档网站](#)。

关于 NetIQ Corporation

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

我们的观点

适应变化及管理复杂性和风险实乃老生常谈

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

提供更好、更快的关键业务服务

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

我们的理念

销售智能解决方案，而不只是软件

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

推动您走向成功是我们的追求

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

我们的解决方案

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

与销售支持联系

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

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

联系技术支持

有关具体的产品问题，请与我们的技术支持团队联系。

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

联系文档支持

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

联系在线用户社区

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

简介

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

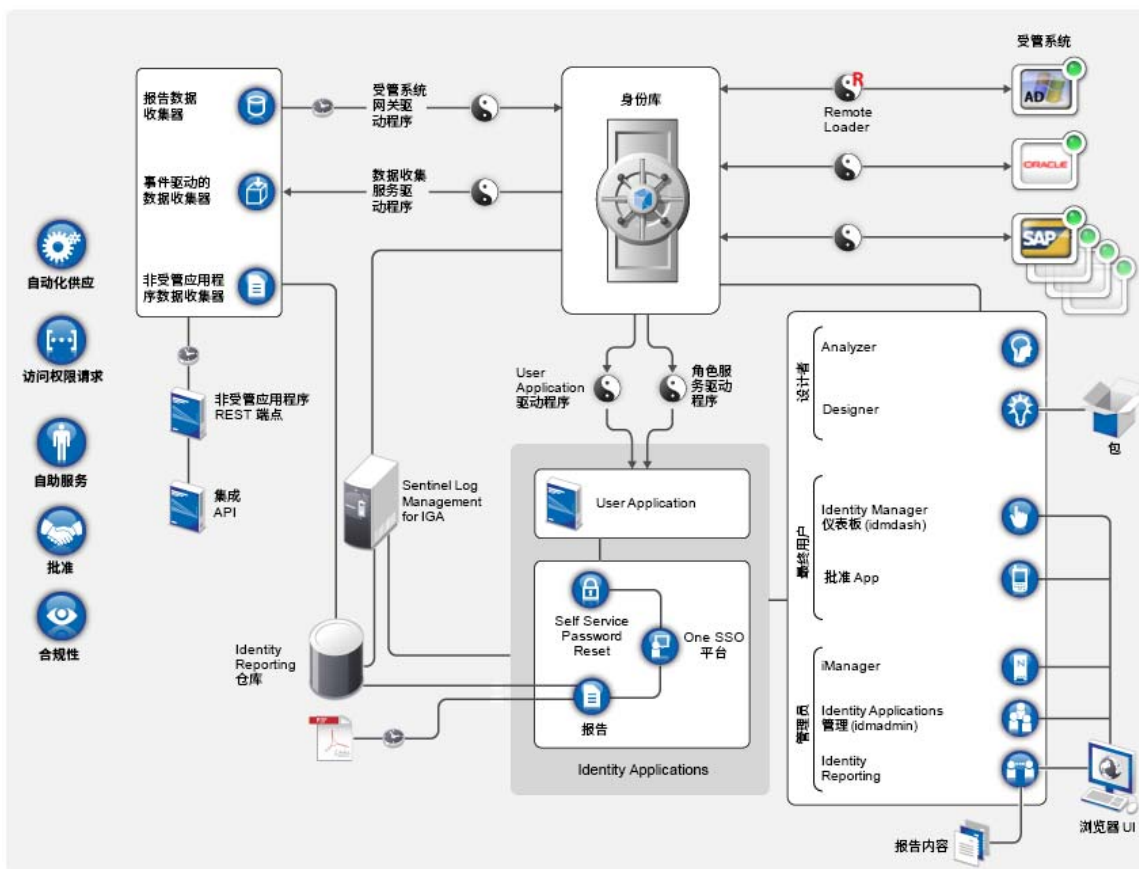
一般而言，您可以将构成 Identity Manager 的组件分成下列功能：

- ♦ 创建和维护 Identity Manager 环境。有关详细信息，请参见第 2 章“[创建和维护 Identity Manager 环境](#)”（第 19 页）。
- ♦ 监控 Identity Manager 环境，包括审计和报告用户供应活动的功能。如此，您便可以证明对业务、IT 及企业策略的合规性状况。有关详细信息，请参见第 3 章“[在 Identity Manager 环境中管理数据](#)”（第 21 页）。
- ♦ 管理用户供应活动，例如单个用户的角色、证明和自助服务。有关详细信息，请参见第 4 章“[供应用户以进行安全的访问](#)”（第 25 页）。

本部分介绍了可帮助您执行这些活动的各个 Identity Manager 组件。掌握这些知识之后，您便可以开始规划产品安装。要了解这些组件如何是互连的，请参见第 1 章“[Identity Manager 的组件概述](#)”（第 17 页）。

1 Identity Manager 的组件概述

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



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

2 创建和维护 Identity Manager 环境

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

- 第 2.1 节 “Designer for Identity Manager”（第 19 页）
- 第 2.2 节 “Analyzer for Identity Manager”（第 19 页）
- 第 2.3 节 “iManager”（第 20 页）

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

2.1 Designer for Identity Manager

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

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

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

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

2.2 Analyzer for Identity Manager

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

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

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

2.3 iManager

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

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

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

3 在 Identity Manager 环境中管理数据

Identity Manager 在物理、虚拟和云网络之间实施一致的访问控制，并使用可让您证明合规性的动态报告。实际上，Identity Manager 可同步储存在已连接应用程序或身份库中的任何类型的数据。

Identity Manager 解决方案的下列组件可提供数据同步，包括口令同步：

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

3.1 了解数据同步

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

- ◆ 控制已连接系统之间的数据流。
- ◆ 确定要共享的数据、数据块的权威来源系统以及对数据进行解释和转换以满足其他系统要求的方法。
- ◆ 在各系统之间同步口令。例如，如果用户更改了在 Active Directory 中的口令，Identity Manager 可将该口令同步到 Lotus Notes 和 Linux。
- ◆ 在各目录（例如 Active Directory）、系统（例如 PeopleSoft 和 Lotus Notes）及操作系统（例如 UNIX 与 Linux）中创建新用户帐户及去除现有账户。例如，向 SAP HR 系统中添加新员工时，Identity Manager 可自动在 Active Directory 中创建新用户帐户，在 Lotus Notes 中创建新帐户以及在 Linux NIS 帐户管理系统中创建新帐户。

3.2 了解审计、报告和合规性

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

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

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

3.3 了解用于同步身份数据的组件

- [第 3.3.1 节“身份库”（第 22 页）](#)
- [第 3.3.2 节“Identity Manager 引擎”（第 22 页）](#)
- [第 3.3.3 节“Remote Loader”（第 22 页）](#)
- [第 3.3.4 节“Identity Reporting”（第 22 页）](#)

3.3.1 身份库

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

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

3.3.2 Identity Manager 引擎

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

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

3.3.3 Remote Loader

Identity Manager Remote Loader 可装载驱动程序，并代表远程服务器上安装的驱动程序来与 Identity Manager 引擎通讯。如果应用程序与 Identity Manager 引擎在同一个服务器上运行，您便可以将驱动程序安装在该服务器上。但是，如果应用程序与 Identity Manager 引擎不在同一个服务器上运行，您必须将驱动程序安装在应用程序所在的服务器上。

有关 Remote Loader 的详细信息，请参见[第 8.4.2 节“了解 Remote Loader”（第 64 页）](#)。

3.3.4 Identity Reporting

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

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

身份信息仓库的基础结构需要使用下列组件：

- ◆ [Identity Manager 的 Identity Reporting](#)（第 23 页）
- ◆ [数据收集服务](#)（第 23 页）
- ◆ [受管系统网关驱动程序](#)（第 23 页）

Identity Manager 的 Identity Reporting

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

数据收集服务

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

该服务包括三个子服务：

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

受管系统网关驱动程序

受管系统网关驱动程序会查询身份库，以便从受管系统中收集下列类型的信息：

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

4 供应用户以进行安全的访问

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

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

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

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

Identity Manager 解决方案提供了下列组件用来供应用户：

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

仪表板为所有 Identity Manager 用户和管理员提供了单一访问点。它允许访问所有现有的 Catlog Administrator 和 User Application 功能。从 Identity Manager 4.6 版开始，仪表板取代了 Identity Manager 主页和供应仪表板。

4.1 了解 Identity Manager 中的证明过程

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

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

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

4.2 了解 Identity Manager 中的自助服务过程

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

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

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

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

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

4.3 了解管理用户供应的组件

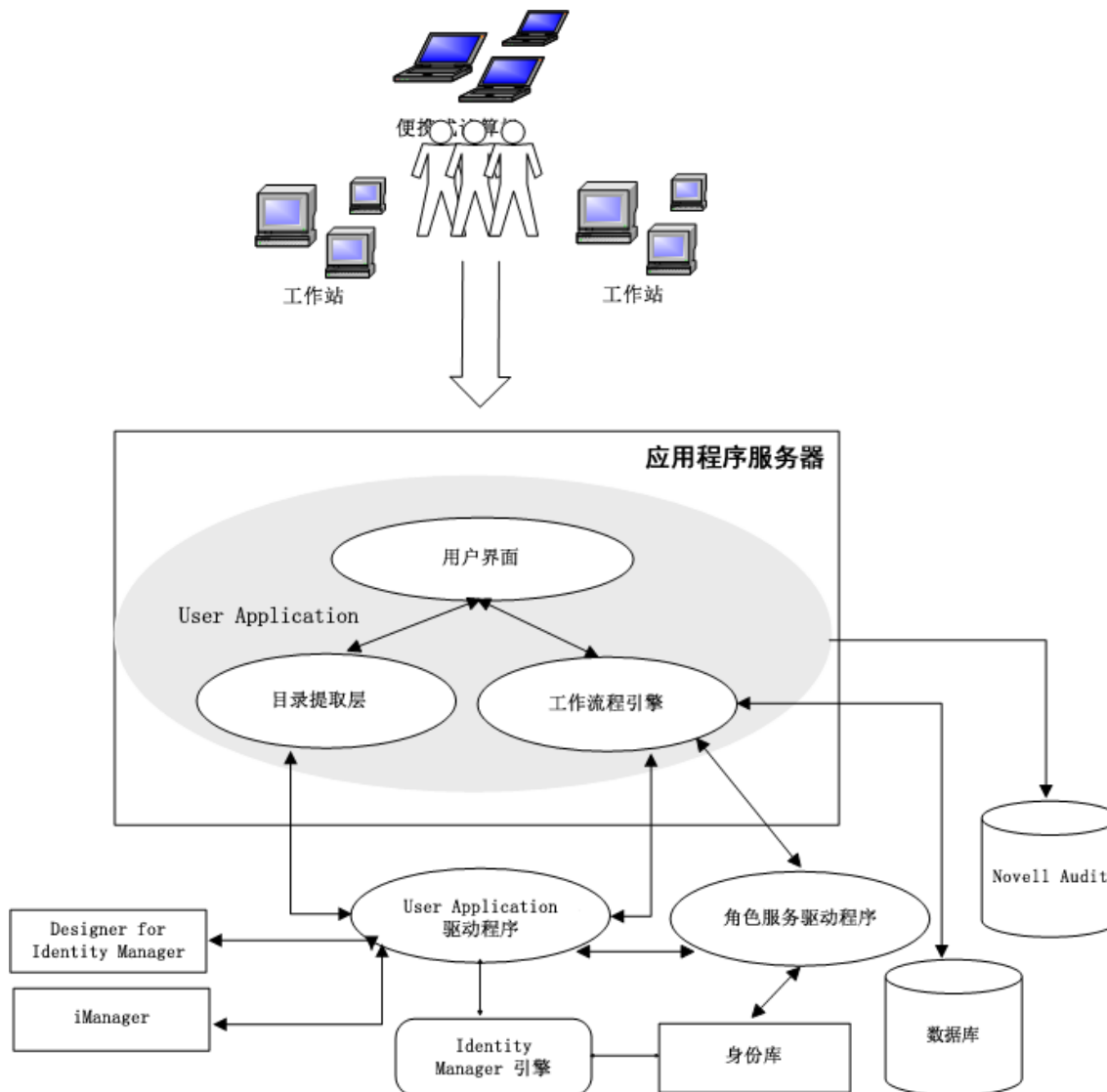
本节说明下列组件的用途：

- [第 4.3.1 节 “User Application 和 Roles Based Provisioning Module”（第 27 页）](#)
- [第 4.3.2 节 “Identity Applications 管理”（第 28 页）](#)
- [第 4.3.3 节 “Identity Manager 仪表板”（第 28 页）](#)

4.3.1 User Application 和 Roles Based Provisioning Module

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

User Application 依赖于许多共同运作的独立组件。



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

用户应用程序驱动程序

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

Role and Resource Service 驱动程序

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

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

4.3.2 Identity Applications 管理

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

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

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

4.3.3 Identity Manager 仪表板

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

我需要某些项目。

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

我需要执行某个动作。

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

我拥有哪些项目？

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

我是如何获取的？

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

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

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

- ♦ REST 端点
- ♦ 标记，例如用户可以访问的特定类型的项目数

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

规划安装 Identity Manager

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

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

- ◆ [第 5 章“规划概述”（第 33 页）](#)

5 规划概述

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

- 第 5.1 节“规划核对清单”（第 33 页）
- 第 5.2 节“了解 Identity Manager 通讯”（第 34 页）
- 第 5.3 节“了解安装文件”（第 35 页）
- 第 5.4 节“目录结构”（第 36 页）
- 第 5.5 节“默认安装位置”（第 36 页）
- 第 5.6 节“安装的组件版本”（第 37 页）
- 第 5.7 节“建议的安装方案和服务器设置”（第 38 页）
- 第 5.8 节“了解许可和激活”（第 41 页）
- 第 5.9 节“准备安装”（第 41 页）
- 第 5.10 节“了解语言支持”（第 46 页）
- 第 5.11 节“下载安装文件”（第 47 页）

5.1 规划核对清单

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

	核对清单项目
<input type="checkbox"/>	1. 查看产品体系结构信息，以了解 Identity Manager 组件。有关更多信息，请参见第 I 部分“简介”（第 15 页）。
<input type="checkbox"/>	2. （视情况而定）在 Red Hat Enterprise Linux 7.x 环境中安装组件时，请确保服务器装有正确的库。有关详细信息，请参见第 5.9.4 节“在 RHEL 7.3 或更高版本的服务器上安装 Identity Manager”（第 43 页）。
<input type="checkbox"/>	3. 确保已获取运行 Identity Manager 的许可证。有关更多信息，请参见第 5.8 节“了解许可和激活”（第 41 页）。
<input type="checkbox"/>	4. 查看每个 Identity Manager 组件的默认端口，以确定是否需要自定义安装设置。有关更多信息，请参见第 5.2 节“了解 Identity Manager 通讯”（第 34 页）。
<input type="checkbox"/>	5. 确定是否可使用您的首选语言运行安装程序。有关更多信息，请参见第 5.10 节“了解语言支持”（第 46 页）。
<input type="checkbox"/>	6. 确保已获取 Identity Manager 的安装文件。有关更多信息，请参见第 5.11 节“下载安装文件”（第 47 页）。
<input type="checkbox"/>	7. （视情况而定）要在群集中安装 Identity Manager，请确保您的环境符合要求。有关更多信息，请参见第 5.9.1 节“确保 Identity Manager 的高可用性”（第 42 页）。

	核对清单项目
<input type="checkbox"/>	8. 确保已获取在服务器上安装 Identity Manager 组件所需的适当身份凭证，以及可能在安装期间创建的帐户。
<input type="checkbox"/>	<p>9. 确保要安装 Identity Manager 组件的目标计算机符合指定的要求。有关详细信息，请参见每个组件的系统要求。</p> <ul style="list-style-type: none"> ◆ 第 8.3.4 节“Identity Manager 引擎、Remote Loader 和 iManager 的系统要求”（第 61 页） ◆ 第 8.5.3 节“Identity Applications 的系统要求”（第 75 页） ◆ 第 8.6.4 节“Identity Reporting 的系统要求”（第 80 页） ◆ 第 12.3 节“Designer 的系统要求”（第 161 页） ◆ 第 14.3 节“Analyzer 的系统要求”（第 168 页） <p>注释： NetIQ 建议您记下安装期间所创建的每个帐户。</p>
<input type="checkbox"/>	10. 激活 Identity Manager 组件。有关详细信息，请参见第 24 节“激活 Identity Manager”（第 213 页）。

5.2 了解 Identity Manager 通讯

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

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

端口号	组件计算机	端口用途
389	身份库	用于以明文方式与 Identity Manager 组件进行 LDAP 通讯
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

端口号	组件计算机	端口用途
8080	Identity Applications iManager	Tomcat 使用该端口进行 HTTP 明文通讯
8090	Remote Loader	Remote Loader 使用该端口侦听来自远程接口 shim 的 TCP/IP 连接 注释： 应为 Remote Loader 的每个实例指派唯一的端口。
8180	Identity Applications	运行 Identity Applications 的 Tomcat 应用程序服务器使用该端口进行 HTTP 通讯
8443	Identity Applications iManager	Tomcat 使用该端口进行 HTTPS (SSL) 通讯，或者重定向 SSL 通讯的请求
8543	Identity Applications	当您未使用 TLS/SSL 协议时，Tomcat 使用该端口来重定向需要 SSL 传输的请求
9009	iManager	Tomcat 为 MOD_JK 使用该端口
15432	Identity Reporting	用于 PostgreSQL 数据库
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

5.3 了解安装文件

下表列出了可用于该版本的文件：

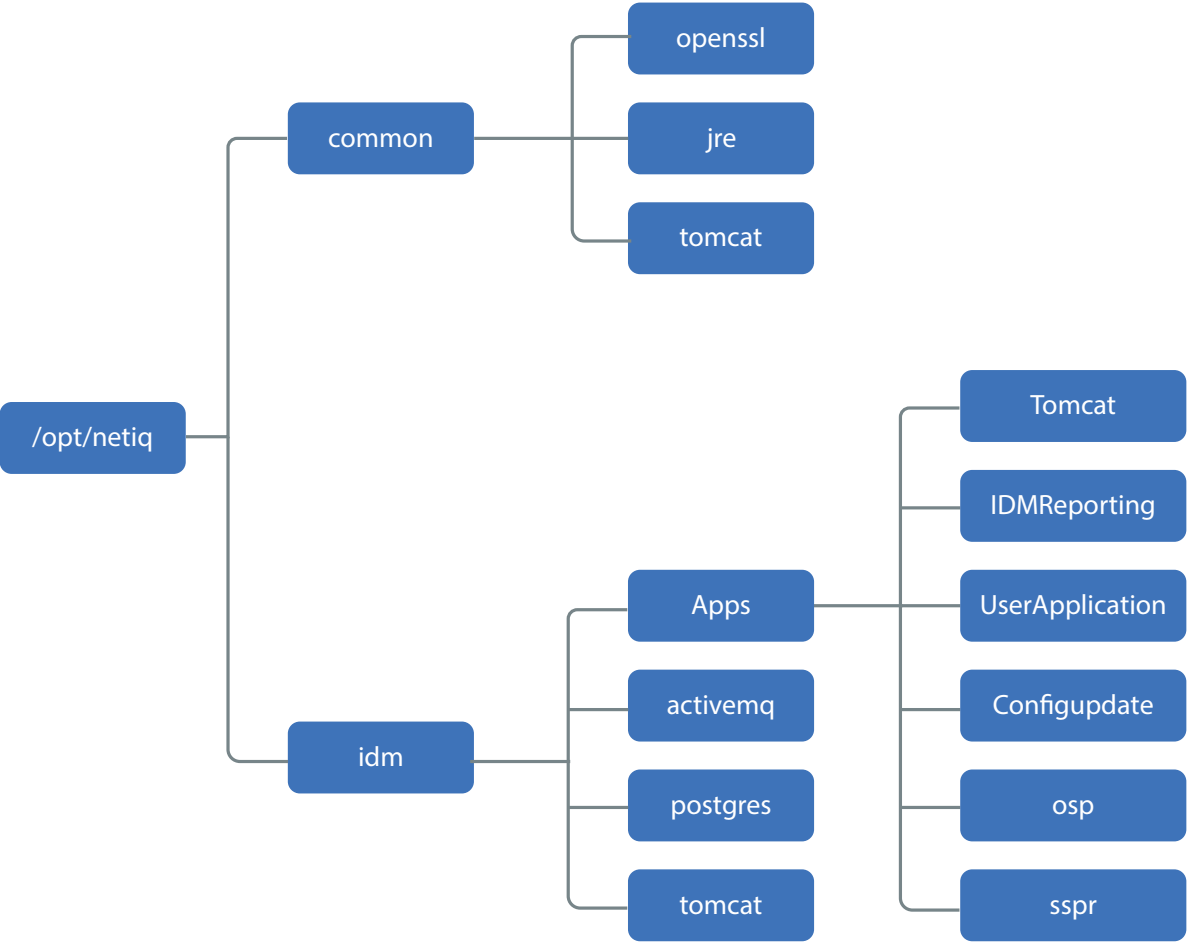
文件名	说明
Identity_Manager_4.7_Linux.iso	包含以下 Identity Manager 组件： <ul style="list-style-type: none"> ♦ Identity Manager 引擎 ♦ Remote Loader 服务 ♦ 扇出代理 ♦ Designer ♦ iManager Web 管理 ♦ Identity Reporting ♦ Identity Applications ♦ Analyzer
SentinelLogManagementForIGA8.1.1.0.tar.gz	包含 Sentinel Log Management for IGA。
Identity_Manager_4.7_Linux_Designer.tar.gz	包含 Designer for Identity Manager。
Identity_Manager_4.7_Linux_Analyzer.tar.gz	包含 Analyzer for Identity Manager。

注释：Identity_Manager_4.7_Linux.iso 文件还打包了运行 Identity Manager 所需的支持软件和组件，例如 Oracle JRE、PostgreSQL、ActiveMQ 和 Apache Tomcat。

5.4 目录结构

安装过程会创建以下目录结构：

- /opt/netiq 目录是目录结构的起点。其他每个文件和目录都在此目录下。
- common 目录包含支持软件。此软件会在需要它的组件之间共享。
- idm 目录包含组件特定的子目录，其中包括用于安装和配置组件的二进制文件。



5.5 默认安装位置

安装过程会将组件放置在以下预定义位置。

Identity Manager 组件	默认安装路径
Identity Manager 引擎	/opt/novell/eDirectory/lib/dirxml
Remote Loader	/opt/novell/dirxml/bin/x86_64
扇出代理	/opt/novell/dirxml/fanoutagent
Designer	/root/designer
iManager	/var/opt/novell/iManager

Identity Manager 组件	默认安装路径
User Application	/opt/netiq/idm/apps/UserApplication
Identity Applications	/opt/netiq/idm/apps
配置更新实用程序	/opt/netiq/idm/apps/configupdate
Identity Reporting	/opt/netiq/idm/apps/IDMReporting
SLM for IGA	/opt/novell/sentinel
Analyzer	/root/analyzer

支持组件	默认安装路径
Oracle JRE	/opt/netiq/common/jre
Apache Tomcat	/opt/netiq/idm/tomcat
PostgreSQL	/opt/netiq/idm/postgres
Apache ActiveMQ	/opt/netiq/idm/activemq

系统将在 /var/opt/netiq/idm/log 目录中生成安装日志文件。

5.6 安装的组件版本

此版本中提供以下版本的组件和支持软件：

Identity Manager 组件	版本
身份库	9.1
注释： 如果您要升级到 Identity Manager 4.7，请确保身份库已升级到 9.1 版本。	
Identity Manager 引擎、Remote Loader、扇出代理	4.7
Designer	4.7
iManager	3.1
One SSO Provider	6.2.1
Self-Service Password Reset	4.2.0.4
Identity Applications	4.7
Identity Reporting	6.0
SLM for IGA	8.1.1.0

支持组件	版本
Oracle Java Development Kit (JRE)	1.8.0_162
Apache Tomcat	8.5.27
PostgreSQL	9.6.6
Apache ActiveMQ	5.15.2

5.7 建议的安装方案和服务器设置

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

本节将帮助您根据特定的审计和报告方案，确定安装顺序和服务器类型。

- ◆ [第 5.7.1 节“将事件发送到审计服务而不在 Identity Manager 中报告”](#)（第 38 页）
- ◆ [第 5.7.2 节“将事件发送到 Identity Manager 并生成报告”](#)（第 38 页）
- ◆ [第 5.7.3 节“将事件推送到 Identity Manager 之前先将事件发送到外部服务”](#)（第 39 页）
- ◆ [第 5.7.4 节“建议的服务器设置”](#)（第 39 页）
- ◆ [第 5.7.5 节“选择 Identity Manager 的操作系统平台”](#)（第 40 页）

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

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

1. Sentinel Log Management for IGA
2. Identity Manager 引擎、驱动程序和 iManager 插件
3. （可选）iManager
4. Designer
5. SSPR
6. Identity Applications
7. （可选）Analyzer

5.7.2 将事件发送到 Identity Manager 并生成报告

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

1. Sentinel Log Management for IGA
2. Identity Manager 引擎、驱动程序和 iManager 插件
3. （可选）iManager
4. Designer

5. SSPR
6. Identity Applications
7. Identity Reporting
8. (可选) Analyzer

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

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

1. 外部审计服务，例如 Sentinel
2. Identity Manager 引擎、驱动程序和 iManager 插件
3. (可选) iManager
4. Designer
5. SSPR
6. Identity Applications
7. Identity Reporting
8. (可选) Analyzer

5.7.4 建议的服务器设置

查看以下注意事项以帮助您规划安装：

组件粘性

组件	独立安装	注释
Identity Manager 引擎	是	
Identity Applications	是	必须具有自己的 OSP。必须将 Identity Applications 和 OSP 安装在同一台计算机上。
Identity Reporting	是	可以具有自己的 OSP。安装或升级 Identity Reporting 时，安装程序支持本地或远程安装的 OSP。
OSP	否	对于 Identity Applications，安装程序不支持远程安装的 OSP 服务器。必须将 OSP 和 Identity Applications 安装在同一台计算机上。
SSPR	是	安装程序支持独立安装和升级 SSPR。
Identity Applications 数据库	是	
Reporting 数据库	是	
Sentinel Log Management for IGA	是	

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

计算机设置	组件设置
一体机（建议仅用于演示 /POC 设置）	在一台计算机上安装和配置所有组件（Identity Manager 引擎、Identity Applications、Identity Reporting、OSP、SSPR、Identity Applications 数据库和 Reporting 数据库），并在另一台计算机上安装和配置 Sentinel Log Management for IGA。
分布式设置	
服务器 1	<ul style="list-style-type: none">◆ 身份库◆ Identity Manager 引擎
服务器 2	Identity Applications 和 OSP（可以群集化）
服务器 3	Identity Reporting (OSP)
服务器 4	SSPR
服务器 5 和 6	Identity Manager 数据库，用于： <ul style="list-style-type: none">◆ Identity Applications◆ Identity Reporting
服务器 7	Sentinel Log Management for IGA

5.7.5 选择 Identity Manager 的操作系统平台

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

平台	组件
openSUSE	Analyzer Designer
Red Hat Linux Server (RHEL)	Identity Applications Identity Manager 引擎 Identity Reporting iManager Remote Loader Sentinel Log Management for IGA
SUSE Linux Enterprise Desktop (SLED)	Designer

平台	组件
SUSE Linux Enterprise Server (SLES)	Analyzer
	Designer
	Identity Applications
	Identity Manager 引擎
	Identity Reporting
	iManager
	Remote Loader
	Sentinel Log Management for IGA

有关系统要求与先决条件的详细信息，请参见以下各章节：

- [规划安装 Designer](#)（第 161 页）
- [计划安装 Identity Manager 引擎、Identity Applications 和 Identity Reporting](#)（第 57 页）

5.8 了解许可和激活

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

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

您可以安装 Identity Manager 的评估版，并免费使用 90 天。但是，必须在安装后的 90 天内激活 Identity Manager 组件，否则它们到期后会停止运行。您可以在 90 天评估期内或者评估期过后，购买产品许可证并激活 Identity Manager。有关详细信息，请参见第 24 节“[激活 Identity Manager](#)”（第 213 页）。

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

5.9 准备安装

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

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

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

- ◆ [第 5.9.1 节“确保 Identity Manager 的高可用性”](#)（第 42 页）
- ◆ [第 5.9.2 节“Linux 服务器上的最低空间要求”](#)（第 42 页）
- ◆ [第 5.9.3 节“在 SLES 12 SP2 或更高版本的服务器上安装 Identity Manager”](#)（第 43 页）
- ◆ [第 5.9.4 节“在 RHEL 7.3 或更高版本的服务器上安装 Identity Manager”](#)（第 43 页）

5.9.1 确保 Identity Manager 的高可用性

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

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

有关下列项的详细信息 ...	参见 ...
确定 Identity Manager 组件的服务器配置	第 5.7.4 节“建议的服务器设置” （第 39 页）
在群集中运行身份库	第 8.3.3 节“在群集环境中安装身份库的先决条件” （第 60 页） 《NetIQ eDirectory Installation Guide》 （NetIQ eDirectory 安装指南）中的“ Deploying eDirectory on High Availability Clusters ”（在高可用性群集上部署 eDirectory）。
在群集中运行 Identity Applications	为群集配置 OSP 和 SSPR （第 144 页） 在群集环境中安装 Identity Applications 的先决条件 （第 74 页） 为群集启用许可权限索引 （第 71 页） 为 Identity Applications 准备群集 （第 74 页） 为群集配置 User Application 驱动程序 （第 126 页） 第 22.3 节“针对分布式环境或群集环境更新仪表板中的 SSPR 链接” （第 208 页）

5.9.2 Linux 服务器上的最低空间要求

Identity Manager 组件有最低空间要求。

[表 5-1](#) 在 [第 43 页](#) 包含不同组件所需的最低安全空间：

表 5-1 最低安全空间要求

路径	组件	所需的最低安全空间
/opt	IDM	3 GB
/var	IDM	5 GB, 用于包含 100,000 个对象的 dib
/etc	IDM	5 MB
/opt	iManager	700 MB
/var	iManager	3 GB
/etc	iManager	10 MB
/opt	Identity Applications 服务器	5 GB
/var	Identity Applications 服务器	100 MB

在安装期间, 请确保 /temp 文件夹以执行权限装入, 有 5 GB 可用空间且具有写入许可权限。

5.9.3 在 SLES 12 SP2 或更高版本的服务器上安装 Identity Manager

- ♦ 要使用单独的组件安装程序或集成安装程序以引导模式来安装 Identity Manager 组件, 您的 SLES 12 SP2 或更高版本服务器上必须已安装特定的包。
 - ♦ libXtst6-32bit-1.2.1-4.4.1.x86_64
 - ♦ libXrender1-32bit
 - ♦ libXi6-32bit
- ♦ (视情况而定) 在 SLES 12 SP3 环境中安装 Identity Manager 组件时, 请确保已安装 glibc-32bit-*x86_64.rpm, 其中 * 表示 RPM 的最新版本。

注释: NetIQ 建议从您的操作系统订购服务获取相关的包, 以确保获得操作系统供应商的持续支持。如果您没有订购服务, 可以从相关网站 (例如 <http://rpmfind.net/linux>) 找到最新的包。

5.9.4 在 RHEL 7.3 或更高版本的服务器上安装 Identity Manager

要在运行 Red Hat Enterprise Linux 7.3 或更高版本操作系统的服务器上安装 Identity Manager, 请确保服务器满足一组特定的先决条件。

- ♦ [先决条件 \(第 44 页\)](#)
- ♦ [运行先决条件检查 \(第 44 页\)](#)
- ♦ [确保服务器上已安装依赖库 \(第 44 页\)](#)
- ♦ [创建用于安装媒体的储存库 \(第 44 页\)](#)

先决条件

NetIQ 建议您查看以下先决条件：

- ♦ 如果 /etc/hosts 条目中包含系统主机名的回写地址别名，则必须将其更改为主机名或 IP 地址。也就是说，如果 /etc/hosts 文件中包含类似下面第一个示例中的条目，则需将其更改为下面第二个示例中的正确条目。

当任何实用程序尝试解析到 ndsd 服务器时，下面的示例会出现问题：

```
<loopback IP address> test-system localhost.localdomain localhost
```

下面是 /etc/hosts 中正确条目的示例：

```
<loopback IP address> localhost.localdomain localhost
<loopback IP address> test-system
```

如果任何第三方工具或实用程序通过 localhost 解析，则需要将其更改为通过主机名或 IP 地址而非 localhost 地址解析。

- ♦ 在服务器上安装适当的库。有关更多信息，请参见[确保服务器上已安装依赖库](#)（第 44 页）。

运行先决条件检查

您可以为每个 Identity Manager 组件生成缺失先决条件报告。在终端中运行 ./ll-rhel-Prerequisite.sh 脚本，位于安装工具包的 <Identity Manager 版本提取位置>install/Utilities 目录中。

确保服务器上已安装依赖库

在 64 位平台上，RHEL 视所选安装方法需要的库也有所不同。请按列出的顺序安装依赖库或 rpm。

注释：要添加 ksh 文件，您可以输入以下命令：

```
yum -y install ksh
```

- ♦ glibc-*.i686.rpm
- ♦ libstdc++-*.i686.rpm
- ♦ libgcc-*.i686.rpm
- ♦ compat-libstdc++-33-*.x86_64.rpm
- ♦ compat-libstdc++-33-*.i686.rpm
- ♦ libXtst-*.i686.rpm
- ♦ libXrender-*.i686.rpm

创建用于安装媒体的储存库

如果您的 RHEL 7.x 服务器需要用于存放安装媒体的储存库，您可以手动创建一个储存库。

注释：

- RHEL 服务器还必须装有适当的库。有关更多信息，请参见[确保服务器上已安装依赖库](#)（第 44 页）。
 - 在安装 Identity Manager 之前，请确保已安装 unzip rpm。这适用于所有 Linux 平台。
-

要设置用于安装的储存库，请执行以下操作：

- 1 在本地服务器中创建安装点。

例如：/mnt/rhel (mkdir -p /mnt/rhel)

- 2 如果您使用安装媒体，则可以使用以下命令来装入：

```
# mount -o loop /dev/sr0 /mnt/rhel
```

或

使用以下命令将 RHEL 7 安装 ISO 装到 /mnt/rhel 这样的目录中：

```
# mount -o loop RHEL7.x.iso /mnt/rhel
```

下载并装入 RHEL 7.4 iso。

例如：mount -o loop <所下载 rhel*.iso 的路径> /mnt/rhel

- 3 将 media.repo 文件从所装入目录的根目录复制到 /etc/yum.repos.d/，并设置所需的许可权限。

例如：

```
# cp /mnt/rhel/media.repo /etc/yum.repos.d/rhel7dvd.repo
# chmod 644 /etc/yum.repos.d/rhel7dvd.repo
```

- 4 编辑新的 repo 文件，将 gpgcheck=0 设置更改为 1，并添加以下内容：

```
enabled=1
baseurl=file:///mnt/rhel/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
```

最后，新的 repo 文件内容将与下文类似（不过 mediaid 应该会因 RHEL 版本而异）：

```
[InstallMedia]
name=DVD for Red Hat Enterprise Linux 7.1 Server
mediaid=1359576196.686790
metadata_expire=-1
gpgcheck=1
cost=500
enabled=1
baseurl=file:///mnt/rhel
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
```

- 5 要安装 32 位包，请在 /etc/yum.conf 文件中将“exactarch=1”更改为“exactarch=0”。
- 6 要在 RHEL 7.x 上安装 Identity Manager 所需的包，请创建 install.sh 文件并在其中添加以下内容：

```
#!/bin/bash
yum clean all
yum repolist
yum makecache

PKGS="ksh gettext.x86_64 libXrender.i686 libXau.i686 libxcb.i686 libX11.i686
libXext.i686 libXi.i686 libXtst.i686 glibc.x86_64 libstdc++.i686
libstdc++.x86_64 libgcc.x86_64"

for PKG in $PKGS;
do
yum -y install "$PKG"
done
```

注释：由于安装媒体不包含 compat-libstdc++-33-*.i686.rpm 和 compat-libstdc++-33-*.x86_64.rpm，因此需要从 [Red Hat](#) 门户下载该 rpm。

例如：要安装 compat-libstdc++-33-*.x86_64.rpm，请运行以下命令：

```
yum -y install compat-libstdc++-33-*.x86_64.rpm
```

- 7 运行在步骤 8 或步骤 7（视 RHEL 版本而定）中创建的 install.sh 文件。
- 8 要确认是否满足先决条件，请运行第 6.3.2 节中所述的脚本。
- 9 安装 Identity Manager 4.7。

5.10 了解语言支持

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

要以特定语言运行安装程序，请在配置文件中或通过命令行设置 LANG 变量。

5.10.1 已翻译的组件和安装程序

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

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

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

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

5.10.2 语言支持的特别注意事项

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

- 一般而言，如果某个 Identity Manager 组件不支持操作系统的语言，则该组件的界面默认使用英语。例如，Identity Manager 驱动程序的语言与 Identity Manager 引擎的语言相同。如果 Identity Manager 不支持驱动程序的语言，则驱动程序配置默认使用英语。
- 以下 iManager 插件提供了西班牙语、俄语、意大利语、葡萄牙语以及上表中列出的语言版本。
- 安装 Designer 时，必须安装 gettext 实用程序。GNU gettext 实用程序提供了一个国际化和多语言讯息的框架。
- 在启动 Identity Manager 组件的安装程序时，需注意以下事项：
 - 如果操作系统使用安装程序支持的语言，则安装程序将默认使用该语言。但是，您也可以为安装过程指定其他语言。
 - 如果安装程序不支持操作系统的语言，则安装程序默认使用英语。
 - 如果操作系统使用某种拉丁语系的语言，则安装程序允许您指定任何一种拉丁语系的语言。
 - 如果操作系统使用支持的亚洲语言或俄语，则安装程序只允许您指定与操作系统匹配的语言或英语。

5.11 下载安装文件

要安装 Identity Manager 组件，请从 NetIQ 下载网站下载以下安装文件：

- Identity Manager 引擎、Identity Applications 和 Identity Reporting：**
Identity_Manager_4.7_Linux.iso
- Sentinel Log Management for Identity Governance and Administration：**
SentinelLogManagementForIGA8.1.1.0.tar.gz
- Designer：** Identity_Manager_4.7_Linux_Designer.tar.gz
- Analyzer：** Identity_Manager_4.7_Linux_Analyzer.tar.gz

要下载安装文件，请执行以下操作：

- 1 访问 NetIQ 下载网站。
- 2 单击要下载的文件旁边的**下载**按钮。
- 3 遵循屏幕提示，将文件下载到计算机上的某个目录中。



安装 Sentinel Log Management for Identity Governance and Administration

本部分引导您完成安装 Identity Manager 的默认审计服务 SLM for IGA 的过程。

SLM for IGA 的安装程序会执行以下功能：

- ♦ 安装并有选择性地配置服务
- ♦ 创建可对服务执行管理任务的用户帐户 (**admin**)
- ♦ 创建服务可用来与数据库交互的数据库管理员帐户 (**dbauser**)

6 计划安装 SLM for IGA

本章提供安装 Identity Manager 的默认审计服务 SLM for IGA 的准备指南。

- 第 6.1 节 “安装 SLM for IGA 的核对清单”（第 51 页）
- 第 6.2 节 “系统要求”（第 51 页）

6.1 安装 SLM for IGA 的核对清单

NetIQ 建议您完成以下核对清单中的步骤：

	核对清单项目
<input type="checkbox"/>	1. 安装前查看系统要求，以确保计算机满足要求。有关详细信息，请参见第 6.2 节 “系统要求”（第 51 页）。
<input type="checkbox"/>	2. （视情况而定）对于运行 RHEL 7.4 操作系统的计算机，请确保您已安装一组适当的库。
<input type="checkbox"/>	3. 决定是要执行 SLM for IGA 的标准安装还是典型安装。有关详细信息，请参见第 7 节 “安装 SLM for IGA”（第 53 页）。

6.2 系统要求

本节提供要安装的服务器的最低要求。有关详细信息，请访问 [NetIQ Sentinel 技术信息网站](#)。

此外，请务必查看安装的先决条件和注意事项，特别是与操作系统有关的内容。

类别	要求
处理器	4 - 8 个 CPU 内核
磁盘空间	200 GB
内存	24 GB
操作系统（经认可）	以下 64 位操作系统之一（最低版本）： <ul style="list-style-type: none">◆ SLES 12 SP2◆ RHEL 7.3 <p>注释：经认可指操作系统已经过全面测试且受支持。</p>
操作系统（受支持）	经认可操作系统的最新版服务包 <p>注释：受支持指操作系统尚未经过测试，但预期可以正常工作</p>

7 安装 SLM for IGA

可以使用标准或自定义安装来安装 Sentinel Log Management for Identity Governance and Administration (IGA)。

7.1 标准安装

1 从 NetIQ 下载网站下载 SentinelLogManagementForIGA8.1.1.0.tar.gz。

2 导航到要提取文件的目录。

3 运行以下命令来提取文件

```
tar -zxvf SentinelLogManagementForIGA8.1.1.0.tar.gz
```

4 导航到 SentinelLogManagementforIGA 目录。

5 要安装 SLM for IGA，请运行以下命令：

```
./install.sh
```

6 指定要用于安装的语言，然后按 Enter。

7 输入 y 以接受许可协议。

安装过程可能会花几分钟时间来加载安装程序包。

8 收到提示时，请指定 1 以继续标准安装。

安装将采用安装程序包含的默认评估许可证密钥继续进行。在评估期内或评估期结束后，您随时可以使用购买的许可证密钥替换评估许可证。

9 指定管理员用户 admin 的口令。

10 再次确认此口令。

此口令由 admin、dbauser 和 appuser 使用。

安装即告完成，服务器会随之启动。安装之后，因为系统要执行一次性初始化，所以可能需要花费几分钟时间来启动所有服务。等到安装完成后，再登录 Sentinel 服务器。

要访问 SLM for IGA 主界面，请在 Web 浏览器中指定如下 URL：

```
https://<IP_Address/DNS_SLM for IGA_server>:8443/SLM for IGA/views/main.html
```

其中，<IP_Address/DNS_SLM for IGA_server> 是 SLM for IGA 服务器的 IP 地址或 DNS 名称，8443 是 SLM for IGA 服务器的默认端口。

7.2 自定义安装

1 从 NetIQ 下载网站下载 SentinelLogManagementForIGA8.1.1.0.tar.gz。

2 导航到要提取文件的目录。

3 运行以下命令来提取文件

```
tar -zxvf SentinelLogManagementForIGA8.1.1.0.tar.gz
```

- 4 导航到 SentinelLogManagementforIGA 目录。
- 5 运行以下命令：
`./install.sh`
- 6 输入 y 以接受许可协议并继续安装。
安装过程可能会花几分钟时间来加载安装程序包。
- 7 指定 2 以执行 SLM for IGA 的自定义配置。
- 8 输入 1 以使用默认的评估许可证密钥。
或者
输入 2 以输入为 SLM for IGA 购买的许可证密钥。
- 9 指定管理员用户 admin 的口令并再次确认口令。
- 10 指定数据库用户 dbauser 的口令并再次确认口令。
dbauser 帐户是 SLM for IGA 用来与数据库交互的身份。在此处输入的口令可用于执行数据库维护任务，包括在忘记或丢失 admin 口令时重置 admin 口令。
- 11 指定应用程序用户 appuser 的口令并再次确认口令。
- 12 通过输入所需的端口号更改端口指派。
例如，Web 服务器的默认端口为 8443。要修改 Web 服务器的端口号，请指定 4。为 Web 服务器输入新的端口值，例如，8643。
- 13 更改端口之后，指定 8 以完成更改。
- 14 输入 1 以便仅使用内部数据库来鉴定用户。
或
如果已在域中配置了 LDAP 目录，请输入 2 以便使用 LDAP 目录鉴定来鉴定用户。
默认值为 1。
- 15 当系统提示您启用 FIPS 140-2 模式时，请输入 n。
- 16 当系统提示您启用可伸缩储存时，请输入 n。

安装即告完成，服务器会随之启动。安装之后，因为系统要执行一次性初始化，所以可能需要花费几分钟来启动所有服务。等到安装完成后，再登录 Sentinel 服务器。

要访问 SLM for IGA 主界面，请在 Web 浏览器中指定如下 URL：

`https://<IP_Address/DNS_SLM for IGA_server>:<port>/SLM for IGA/views/main.html`

其中，<IP_Address/DNS_SLM for IGA_server> 是 SLM for IGA 服务器的 IP 地址或 DNS 名称，<port> 是 SLM for IGA 服务器的端口。

IV

安装和配置 Identity Manager 引擎、Identity Applications 及 Identity Reporting

本部分引导您完成安装 Identity Manager 引擎、Identity Applications 和 Identity Reporting 组件的过程。开始安装前，请先评估您要实施 Identity Manager 的方式。您可以将各 Identity Manager 组件安装在同一台服务器上，也可以安装在不同的服务器上。有关详细信息，请参见[第 5.7.4 节“建议的服务器设置”](#)（第 39 页）。

可以采用交互模式或无提示模式安装和配置组件。安装程序提供了不同阶段来安装和配置组件。有关详细信息，请参见[第 8.2 节“了解安装程序”](#)（第 58 页）。安装及配置脚本 `install.sh` 和 `configure.sh` 均位于 Identity Manager 安装包 `.iso` 映像文件的根目录中。默认情况下，安装程序将在默认位置中安装组件。有关详细信息，请参见[第 5.5 节“默认安装位置”](#)（第 36 页）。

注释：您应该从装入 `.iso` 的位置运行 `install.sh`。从自定义位置运行 `install.sh` 将导致失败。

NetIQ 建议您在开始安装前先查看先决条件和系统要求。有关详细信息，请参见[第 8 章“计划安装 Identity Manager 引擎、Identity Applications 和 Identity Reporting”](#)（第 57 页）。

- ◆ [第 8 章“计划安装 Identity Manager 引擎、Identity Applications 和 Identity Reporting”](#)（第 57 页）
- ◆ [第 9 章“安装 Identity Manager 引擎、Identity Applications 和 Identity Reporting”](#)（第 83 页）
- ◆ [第 10 章“配置安装的组件”](#)（第 91 页）
- ◆ [第 11 章“完成安装的最后步骤”](#)（第 97 页）

8 计划安装 Identity Manager 引擎、Identity Applications 和 Identity Reporting

本章提供安装 Identity Manager 引擎、Identity Applications 和 Identity Reporting 组件的先决条件、注意事项及所需的系统设置。首先，请查阅核对清单，以了解安装过程。

- 第 8.1 节“安装 Identity Manager 组件的核对清单”（第 57 页）
- 第 8.2 节“了解安装程序”（第 58 页）
- 第 8.3 节“计划安装 Identity Manager 引擎”（第 59 页）
- 第 8.4 节“规划安装 Remote Loader”（第 62 页）
- 第 8.5 节“计划安装 Identity Applications”（第 67 页）
- 第 8.6 节“规划安装 Identity Reporting”（第 77 页）

8.1 安装 Identity Manager 组件的核对清单

在开始安装过程之前，NetIQ 建议您先查看以下步骤。

	核对清单项目
<input type="checkbox"/>	1. 了解 Identity Manager 各组件之间的交互。有关详细信息，请参见第 I 部分“简介”（第 15 页）。
<input type="checkbox"/>	2. 确定要为 Identity Manager 组件使用哪些服务器。有关详细信息，请参见第 5.7 节“建议的安装方案和服务器设置”（第 38 页）。
<input type="checkbox"/>	3. 查看有关安装 Identity Manager 引擎的注意事项，以确保计算机符合先决条件。有关详细信息，请参见第 8.3 节“计划安装 Identity Manager 引擎”（第 59 页）。
<input type="checkbox"/>	4. 查看将要托管 Identity Manager 引擎的计算机所要满足的硬件和软件要求。有关详细信息，请参见 Identity Manager 引擎、Remote Loader 和 iManager 的系统要求（第 61 页）。
<input type="checkbox"/>	5. 了解在安装 Identity Manager 引擎后，会自动激活哪些驱动程序。有关详细信息，请参见第 8.3.2 节“随 Identity Manager 引擎一起安装驱动程序的注意事项”（第 60 页）。
<input type="checkbox"/>	6. （视情况而定）对于运行 RHEL 7.3 或更高版本的计算机，请确保您已安装一组适当的库。
<input type="checkbox"/>	7. 要安装 Identity Manager 引擎，请参见以下章节之一： <ul style="list-style-type: none">• 第 9.1.1 节“执行交互式安装”（第 83 页）• 第 9.1.2 节“以无提示模式安装 Identity Manager 引擎”（第 84 页）
<input type="checkbox"/>	8. （视情况而定）要安装 Remote Loader，请参见第 8.4 节“规划安装 Remote Loader”（第 62 页）。

	核对清单项目
<input type="checkbox"/>	9. （视情况而定）如果您是以非 root 身份执行安装的，请更新驱动程序集，以在电子邮件通知中支持图形。有关详细信息，请参见第 11.1.2 节“增加对电子邮件通知中的图形的支持”（第 97 页）。
<input type="checkbox"/>	10. 启动 Remote Loader 中的驱动程序实例。有关详细信息，请参见第 11.3 章“配置 Remote Loader 和驱动程序”（第 105 页）。

8.2 了解安装程序

Identity Manager 安装程序分不同的阶段来进行 Identity Manager 组件的安装和配置。根据安装期间选择的是 Identity Manager Advanced Edition 还是 Standard Edition，安装的组件将会有所不同。例如，如果选择 Identity Manager Advanced Edition，将显示以下选项：

- ◆ Identity Manager 引擎
- ◆ Identity Manager Remote Loader 服务
- ◆ Identity Manager 扇出代理
- ◆ iManager Web 管理
- ◆ Identity Reporting
- ◆ Identity Applications

可以在安装 Identity Manager 组件之后立即配置它们，也可以稍后配置。Identity Manager 提供两个配置选项：典型和自定义。

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。您可以使用此选项来配置大部分设置。

有关组件范围配置的细节，请参见第 10.1 节“了解配置参数”（第 91 页）。

下列小节说明使用安装程序提供的每个安装选项可以安装的组件：

8.2.1 Identity Manager 引擎

安装身份库、Identity Manager 引擎和 Identity Manager 驱动程序。

8.2.2 Identity Manager Remote Loader 服务器

在 Remote Loader 中安装 Remote Loader 服务和驱动程序实例。使用 Remote Loader 可以在不托管身份库和 Identity Manager 引擎的已连接系统上运行 Identity Manager 驱动程序。

8.2.3 Identity Manager 扇出代理

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

8.2.4 iManager Web 管理

安装 iManager Web 管理控制台和 iManager 插件。

8.2.5 Identity Applications

此安装选项将安装用于提供 Identity Applications 底层框架的数个组件。

- ♦ Identity Manager 仪表板
- ♦ Identity Manager 管理控制台
- ♦ User Application
- ♦ User Application 驱动程序 (UAD)
- ♦ 角色和资源服务驱动程序 (RRSD)

安装程序会在内部安装鉴定服务，以支持通过单点登录访问 Identity Applications 和 Identity Reporting 的功能。安装程序还会安装口令管理服务来帮助您配置 Identity Manager，以允许用户重设置其口令。

安装过程会部署 User Application 驱动程序以及角色和资源服务驱动程序。

8.2.6 Identity Reporting

此安装选项将安装用于提供 Identity Reporting 底层框架的数个组件。

- ♦ Identity Reporting
- ♦ 受管系统网关 (MSGW) 驱动程序
- ♦ 数据收集服务驱动程序 (DCS)

Identity Reporting 会与 SLM for IGA 通讯来进行审计。为了记录事件，Identity Reporting 需要使用随 SLM for IGA 一同安装的 SIEM 数据库。

安装过程会部署 MSGW 和 DCS 驱动程序。

8.3 计划安装 Identity Manager 引擎

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

- ♦ [第 8.3.1 节“安装 Identity Manager 引擎的注意事项”（第 59 页）](#)
- ♦ [第 8.3.2 节“随 Identity Manager 引擎一起安装驱动程序的注意事项”（第 60 页）](#)
- ♦ [第 8.3.3 节“在群集环境中安装身份库的先决条件”（第 60 页）](#)
- ♦ [第 8.3.4 节“Identity Manager 引擎、Remote Loader 和 iManager 的系统要求”（第 61 页）](#)

8.3.1 安装 Identity Manager 引擎的注意事项

在安装 Identity Manager 引擎之前，请先查看以下注意事项：

- ♦ 安装程序将根据身份库的版本安装 64 位 Identity Manager。

- ♦ （视情况而定）要在 Identity Manager 引擎所在的同一台计算机上安装 Remote Loader，请确保选择同时支持这两个组件的操作系统。有关 Remote Loader 系统要求的详细信息，请参见第 8.4.5 节“安装 Remote Loader 的先决条件和注意事项”（第 66 页）。
- ♦ （视情况而定）如果您以非 root 用户身份安装 Identity Manager 引擎，安装过程将不会安装 NetIQ Sentinel 平台代理、Linux 帐户驱动程序或 Remote Loader。您必须单独安装这些组件。

注释：要支持通过非 root 用户身份安装的引擎执行审计，请安装 Novell Audit 平台代理的最新增补程序。有关详细信息，请与[技术支持](#)团队联系。

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

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

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

有关在安装后激活 Identity Manager 驱动程序的详细信息，请参见第 24 章“[激活 Identity Manager](#)”（第 213 页）。

8.3.3 在群集环境中安装身份库的先决条件

NetIQ 建议您在群集环境中安装身份库之前，先查看以下注意事项：

- ♦ 必须配备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）。

8.3.4 Identity Manager 引擎、Remote Loader 和 iManager 的系统要求

下表列出了执行安装的组件范围最低系统要求：

注释： BTRFS 文件系统不支持身份库。

类别	身份库	Identity Manager 引擎	Remote Loader (64 位)	iManager
处理器	1 GHz	1 GHz	1 GHz	1 GHz
磁盘空间	<ul style="list-style-type: none"> 身份库需要 300 MB 每 50,000 个用户需要 150 MB 的额外磁盘空间 	<ul style="list-style-type: none"> 1 GB 每 50,000 个用户需要 150 MB 的额外磁盘空间 		200 MB
内存	2 GB	<ul style="list-style-type: none"> Identity Manager 引擎需要 2 GB Identity Manager 驱动程序需要 2 MB 	512 MB	512 MB
操作系统（经认可） 注释： 经认可指操作系统已经过全面测试且受支持。	以下 64 位操作系统之一： <ul style="list-style-type: none"> SLES 12 SP3 SLES 12 SP2 RHEL 7.4 RHEL 7.3 	以下 64 位操作系统之一： <ul style="list-style-type: none"> SLES 12 SP3 SLES 12 SP2 RHEL 7.4 RHEL 7.3 	以下 64 位操作系统之一： <ul style="list-style-type: none"> SLES 12 SP3 SLES 12 SP2 RHEL 7.4 RHEL 7.3 	以下 64 位操作系统之一： <ul style="list-style-type: none"> SLES 12 SP3 SLES 12 SP2 RHEL 7.4 RHEL 7.3
NetIQ 建议您在安装 Identity Manager 之前，按照制造商的自动更新工具应用最新的操作系统增补程序。				
操作系统（受支持） 注释： 受支持指操作系统尚未经过测试，但预期可以正常工作。	经认可操作系统的最新版服务包	经认可操作系统的最新版服务包	经认可操作系统的最新版服务包	经认可操作系统的最新版服务包

类别	身份库	Identity Manager 引擎	Remote Loader (64 位)	iManager
虚拟化系统 NetIQ 支持在为运行 NetIQ 产品的操作系统提供官方支持的企业级虚拟化系统上安装 Identity Manager。只要虚拟化系统的供应商为这些操作系统提供官方支持，NetIQ 就可支持这些系统上的整个 Identity Manager 堆栈。	<ul style="list-style-type: none"> ◆ Hyper-V Server 2012 R2 ◆ VMWare ESX 5.0 及更高版本 ◆ 包含 Hyper-V 的 Windows Server 2012 R2 Virtualization (受支持) 	<ul style="list-style-type: none"> ◆ Hyper-V Server 2012 R2 ◆ VMWare ESX 5.0 及更高版本 ◆ 包含 Hyper-V 的 Windows Server 2012 R2 Virtualization (受支持) 	<ul style="list-style-type: none"> ◆ Hyper-V Server 2012 R2 ◆ VMWare ESX 5.0 及更高版本 ◆ 包含 Hyper-V 的 Windows Server 2012 R2 Virtualization (受支持) 	
软件	eDirectory 9.1	Identity Manager 引擎 4.7	Remote Loader 4.7	iManager 3.1
Java (Oracle 的 Java 运行时环境 (JRE))	JRE 1.8.0_162	JRE 1.8.0_162	JRE 1.8.0_162	JRE 1.8.0_162
Web 浏览器				以下任意浏览器 (最低版本): <ul style="list-style-type: none"> ◆ Google Chrome 61 ◆ Mozilla Firefox 51
应用程序服务器				iManager 随附的 Apache Tomcat 8.5.27
默认端口				8080、8443 和 9009

8.4 规划安装 Remote Loader

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

- ◆ [第 8.4.1 节 “Remote Loader 安装核对清单” \(第 63 页\)](#)
- ◆ [第 8.4.2 节 “了解 Remote Loader” \(第 64 页\)](#)
- ◆ [第 8.4.3 节 “了解安装程序” \(第 65 页\)](#)
- ◆ [第 8.4.4 节 “在同一台计算机上使用 32 位和 64 位 Remote Loader” \(第 65 页\)](#)
- ◆ [第 8.4.5 节 “安装 Remote Loader 的先决条件和注意事项” \(第 66 页\)](#)

8.4.1 Remote Loader 安装核对清单

NetIQ 建议您完成以下核对清单中的步骤：

	核对清单项目
<input type="checkbox"/>	1. 了解 Identity Manager 各组件之间的交互。有关详细信息，请参见第 3.3.3 节“Remote Loader”（第 22 页）。
<input type="checkbox"/>	2. 确定要为 Identity Manager 组件使用哪些服务器。有关详细信息，请参见第 5.7 节“建议的安装方案和服务器设置”（第 38 页）。
<input type="checkbox"/>	3. 确保已安装 Identity Manager 引擎。
<input type="checkbox"/>	4. 查看安装 Remote Loader 的注意事项，以确保计算机符合先决条件。有关详细信息，请参见第 8.4.5 节“安装 Remote Loader 的先决条件和注意事项”（第 66 页）。
<input type="checkbox"/>	5. 查看将要托管 Remote Loader 的计算机所要满足的硬件和软件要求。有关详细信息，请参见第 8.3.4 节“Identity Manager 引擎、Remote Loader 和 iManager 的系统要求”（第 61 页）。
<input type="checkbox"/>	6. （视情况而定）对于运行 RHEL 7.3 或更高版本操作系统的计算机，请确保您已安装一组适当的库。有关详细信息，请参见第 5.9.4 节“在 RHEL 7.3 或更高版本的服务器上安装 Identity Manager”（第 43 页）。
<input type="checkbox"/>	7. （视情况而定）要在未托管 Identity Manager 引擎的服务器上安装 Remote Loader，请确保您能够与该引擎建立安全连接。有关详细信息，请参见第 11.3.1 节“创建与 Identity Manager 引擎的安全连接”（第 105 页）。
<input type="checkbox"/>	8. 确定是要安装 32 位还是 64 位版本的 Remote Loader。有关详细信息，请参见第 8.4.4 节“在同一台计算机上使用 32 位和 64 位 Remote Loader”（第 65 页）。
<input type="checkbox"/>	9. 确定是要使用 Remote Loader 还是 Java Remote Loader。有关详细信息，请参见了解 Java Remote Loader（第 65 页）。
<input type="checkbox"/>	10. 安装远程装载程序。有关详细信息，请参见第 9 章“安装 Identity Manager 引擎、Identity Applications 和 Identity Reporting”（第 83 页）。
<input type="checkbox"/>	11. （视情况而定）要安装 Java Remote Loader，请参见第 9.2 节“安装 Java Remote Loader”（第 87 页）。
<input type="checkbox"/>	12. 查看用于配置驱动程序实例的参数。有关详细信息，请参见第 11.3.2 节“了解 Remote Loader 的配置参数”（第 108 页）。
<input type="checkbox"/>	13. 要配置 Remote Loader 中的驱动程序实例，请参见以下章节之一： <ul style="list-style-type: none">◆ 第 11.3.3 节“为驱动程序实例配置 Remote Loader”（第 115 页）◆ 第 11.3.4 节“为驱动程序实例配置 Java Remote Loader”（第 116 页）
<input type="checkbox"/>	14. 准备 Remote Loader 的驱动程序。有关详细信息，请参见第 11.3.5 节“配置 Identity Manager 驱动程序以与 Remote Loader 配合使用”（第 117 页）。
<input type="checkbox"/>	15. 启动 Remote Loader 中的驱动程序实例。有关详细信息，请参见第 11.3.8 节“启动 Remote Loader 中的驱动程序实例”（第 124 页）。
<input type="checkbox"/>	16. （视情况而定）要配置 Remote Loader 与 Identity Manager 引擎间的相互鉴定，请参见第 11.3.6 节“配置与 Identity Manager 引擎的相互鉴定”（第 118 页）。

	核对清单项目
<input type="checkbox"/>	17. 校验 Remote Loader 和驱动程序是否可与 Identity Manager 引擎和已连接系统通讯。有关详细信息，请参见第 11.3.7 节“校验配置”（第 124 页）。
<input type="checkbox"/>	18. 安装其余的 Identity Manager 组件，包括 Designer 和 Analyzer。

8.4.2 了解 Remote Loader

使用 Remote Loader 可以在不托管身份库和 Identity Manager 引擎的已连接系统上运行 Identity Manager 驱动程序。

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

了解 Shim

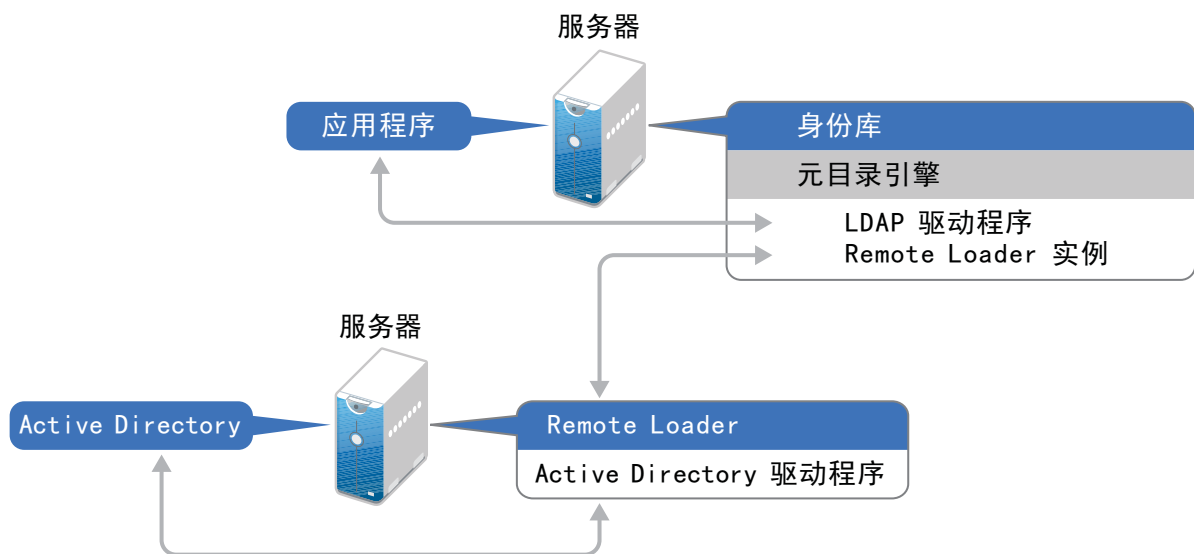
Remote Loader 使用 shim 来与受管系统上的应用程序通讯。*shim* 是一个或多个包含代码的文件，这些代码用于处理在身份库与应用程序之间同步的事件。在使用 Remote Loader 之前，必须将应用程序 shim 配置为安全连接到 Identity Manager 引擎。此外，还必须配置 Remote Loader 和 Identity Manager 驱动程序。有关详细信息，请参见第 11.3 章“配置 Remote Loader 和驱动程序”（第 105 页）。

确定何时使用 Remote Loader

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

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

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



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

了解 Java Remote Loader

在装有机 Remote Loader 不支持的 Linux 服务器的计算机上，Java Remote Loader 可提供装载驱动程序 Shim 的灵活性。Java Remote Loader 是一个 Java 应用程序。您可以将 Java Remote Loader 与任何公开支持的 Java 版本搭配使用。

要打开该应用程序，请运行名为 `dirxml_jremote` 的外壳脚本。有关详细信息，请参见第 11.3.4 节“为驱动程序实例配置 Java Remote Loader”（第 116 页）。

8.4.3 了解安装程序

Identity Manager 引擎安装程序可以安装 32 位和 / 或 64 位版本的 Remote Loader。除了 Remote Loader 以外，您还可以选择要在连接的系统上安装的驱动程序。

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

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

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

8.4.5 安装 Remote Loader 的先决条件和注意事项

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

- ◆ 确保先安装 Identity Manager 引擎，再安装 Remote Loader。

如果您未安装 Identity Manager 引擎就已安装 Remote Loader，则必须先安装 novell-openssl-9.1.0-0.x86_64.rpm，之后再开始配置 Identity Manager 引擎。

1. 导航到以下位置：

< 装入 Identity_Manager_4.7_Linux.iso 的位置 >/IDM/packages/OpenSSL/x86_64/

2. 使用以下命令安装 novell-openssl-9.1.0-0.x86_64.rpm：

```
rpm -ivh novell-openssl-9.1.0-0.x86_64.rpm
```

- ◆ 在可与受管系统通讯的服务器上安装 Remote Loader。必须能够通过相关的 API 访问每个受管系统的驱动程序。
- ◆ 您可以在装有 Identity Manager 引擎的同一台计算机上安装 Remote Loader。
- ◆ 您可以在同一台计算机上同时安装 32 位和 64 位 Remote Loader。
- ◆ 您可以在不支持本机 Remote Loader 的平台上安装 Java Remote Loader。有关受支持平台的详细信息，请参见第 8.3.4 节“Identity Manager 引擎、Remote Loader 和 iManager 的系统要求”（第 61 页）。
- ◆ NetIQ 建议您尽可能地对于驱动程序使用 Remote Loader 配置。即使是已连接系统位于 Identity Manager 服务器引擎所在的同一个服务器上，也要使用 Remote Loader。

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

- ◆ 在驱动程序 shim 之间实现内存与处理隔离，从而改善性能并能更好地监视 Identity Manager 解决方案。
- ◆ 增补和升级驱动程序 shim 不会影响身份库或其他驱动程序。
- ◆ 保护身份库免受驱动程序 shim 中可能发生的致命问题的影响。
- ◆ 将驱动程序 shim 的负载分散到其他服务器。
- ◆ 以下驱动程序支持 Remote Loader 功能：
 - ◆ Access Review
 - ◆ ACF2
 - ◆ Azure Active Directory
 - ◆ 标题页
 - ◆ Blackboard
 - ◆ 数据收集服务
 - ◆ Delimited Text
 - ◆ GoogleApps
 - ◆ REST
 - ◆ GroupWise 2014 （适用于 32 位 Remote Loader）
 - ◆ JDBC
 - ◆ JMS
 - ◆ LDAP
 - ◆ Linux 设置

- ◆ Lotus Notes
- ◆ 受管系统网关
- ◆ 手动任务服务
- ◆ Null and Loopback
- ◆ Office 365
- ◆ Oracle EBS HRMS
- ◆ Oracle EBS TCA
- ◆ Oracle EBS User Management
- ◆ PeopleSoft 5.2
- ◆ Privileged User Management
- ◆ Remedy
- ◆ Salesforce.com
- ◆ SAP 业务逻辑
- ◆ SAP 门户
- ◆ SAP HR （不受 Java Remote Loader 的支持）
- ◆ SAP User Management （不受 Java Remote Loader 的支持）
- ◆ ServiceNow
- ◆ Integration Module V2.0 for Sentinel
- ◆ SharePoint
- ◆ SOAP
- ◆ 绝密
- ◆ WorkOrder
- ◆ 以下驱动程序不支持 Remote Loader：
 - ◆ Bidirectional eDirectory
 - ◆ eDirectory
 - ◆ 权利服务
 - ◆ 角色服务
 - ◆ User Application

8.5 计划安装 Identity Applications

Identity Applications 安装包括以下组件：

- ◆ Identity Manager 仪表盘
- ◆ Identity Manager 管理界面
- ◆ User Application
- ◆ Role and Resource Service 驱动程序
- ◆ 用户应用程序驱动程序

本部分包含下列信息：

- ◆ 第 8.5.1 节 “Identity Applications 安装核对清单”（第 68 页）
- ◆ 第 8.5.2 节 “安装 Identity Applications 的先决条件和注意事项”（第 69 页）
- ◆ 第 8.5.3 节 “Identity Applications 的系统要求”（第 75 页）

8.5.1 Identity Applications 安装核对清单

NetIQ 建议您在开始安装过程之前先查看以下步骤：

	核对清单项目
<input type="checkbox"/>	1. 了解 Identity Manager 各组件之间的交互。有关详细信息，请参见第 4.3.1 节 “User Application 和 Roles Based Provisioning Module”（第 27 页）。
<input type="checkbox"/>	2. 确定要为 Identity Manager 组件使用哪些服务器。有关详细信息，请参见第 5.7.4 节 “建议的服务器设置”（第 39 页）。
<input type="checkbox"/>	3. 决定在安装 Identity Applications 之前是否应安装 Sentinel。有关详细信息，请参见第 5.7 节 “建议的安装方案和服务器设置”（第 38 页）。
<input type="checkbox"/>	4. 确保已安装 Identity Manager 引擎。有关安装引擎的详细信息，请参见第 8.3.4 节 “Identity Manager 引擎、Remote Loader 和 iManager 的系统要求”（第 61 页）。
<input type="checkbox"/>	5. 查看安装 Identity Applications 及其支持框架的注意事项，以确保您的服务器符合先决条件。有关详细信息，请参见第 8.5.2 节 “安装 Identity Applications 的先决条件和注意事项”（第 69 页）。
<input type="checkbox"/>	6. （视情况而定）对于运行 SLES 12 SP2 或更高版本操作系统的计算机，请确保您已安装引导式安装所需的一组适当的库。有关详细信息，请参见第 5.9.3 节 “在 SLES 12 SP2 或更高版本的服务器上安装 Identity Manager”（第 43 页）。
<input type="checkbox"/>	7. （视情况而定）对于运行 RHEL 7.3 或更高版本操作系统的计算机，请确保您已安装一组适当的库。有关详细信息，请参见第 5.9.4 节 “在 RHEL 7.3 或更高版本的服务器上安装 Identity Manager”（第 43 页）。
<input type="checkbox"/>	8. 查看将要托管 Identity Applications 及其框架的计算机所要满足的硬件和软件要求。有关详细信息，请参见第 8.5.3 节 “Identity Applications 的系统要求”（第 75 页）。
<input type="checkbox"/>	9. 在本地计算机或连接的服务器上为 Identity Applications 安装并配置一个数据库。 <ul style="list-style-type: none">◆ 要了解该数据库，请参见安装 Identity Applications 数据库的先决条件（第 71 页）。◆ 要安装该数据库，请参见第 4 章 “配置 Identity Applications 的数据库”（第 72 页）。
<input type="checkbox"/>	10. 安装 Identity Applications。有关详细信息，请参见以下章节之一： <ul style="list-style-type: none">◆ 第 9.1.1 节 “执行交互式安装”（第 83 页）◆ 第 9.1.2 节 “以无提示模式安装 Identity Manager 引擎”（第 84 页）
<input type="checkbox"/>	11. 要执行安装过程中的最后几个任务，请参见第 11 章 “完成安装的最后步骤”（第 97 页）。
<input type="checkbox"/>	12. 确保已正确配置 Identity Applications 和单点登录设置。有关详细信息，请参见第 19 章 “校验是否可对 Identity Applications 进行单点登录访问”（第 185 页）。

	核对清单项目
<input type="checkbox"/>	13. (可选) 要开始使用 Identity Applications, 请参见 《 NetIQ Identity Manager - Administrator's Guide to the Identity Applications 》 (NetIQ Identity Manager - Identity Applications 管理员指南)。

8.5.2 安装 Identity Applications 的先决条件和注意事项

NetIQ 建议您在开始执行安装过程之前, 先查看 Identity Applications 的先决条件和计算机要求。有关配置 User Application 环境的详细信息, 请参见 《[NetIQ Identity Manager - Identity Applications 用户指南](#)》。

- ◆ [Identity Applications 的安装注意事项 \(第 69 页\)](#)
- ◆ [Identity Applications 的配置和用法注意事项 \(第 70 页\)](#)
- ◆ [指定权限索引的位置 \(第 70 页\)](#)
- ◆ [为群集启用许可权限索引 \(第 71 页\)](#)
- ◆ [安装 Identity Applications 数据库的先决条件 \(第 71 页\)](#)
- ◆ [配置 Identity Applications 的数据库 \(第 72 页\)](#)
- ◆ [在群集环境中安装 Identity Applications 的先决条件 \(第 74 页\)](#)
- ◆ [为 Identity Applications 准备群集 \(第 74 页\)](#)

Identity Applications 的安装注意事项

在安装 Identity Applications 时, 请注意以下事项。

- ◆ 需要以下 Identity Manager 组件的受支持版本:
 - ◆ Identity Manager 引擎
 - ◆ Remote Loader
- ◆ (可选) NetIQ 建议为 Identity Manager 组件之间的通讯启用安全套接字层 (SSL) 协议。要使用 SSL 协议, 必须在您的环境中启用 SSL, 并在安装期间指定 **https**。有关启用 SSL 的信息, 请参见 《[NetIQ Analyzer for Identity Manager Administration Guide](#)》 (NetIQ Analyzer for Identity Manager 管理指南) 中的 “[Configuring Security in the Identity Applications](#)” (配置 Identity Applications 中的安全性)。
- ◆ 您不能将 Role and Resource Service 驱动程序与 Remote Loader 配合使用, 因为该驱动程序使用 jClient。
- ◆ 默认情况下, 安装过程会将程序文件放在 /opt/netiq/idm 目录中。如果您计划将 User Application 安装在非默认位置, 请在开始执行安装过程之前, 确保新目录符合以下要求:
 - ◆ 目录存在并且可写入。
 - ◆ 非 root 用户可对该目录进行写操作。
- ◆ 每个 User Application 实例只能为一个用户容器提供服务。例如, 您只能在与该实例关联的容器中添加用户、执行搜索和查询。此外, 用户容器与应用程序之间的关联是永久性的。

- ♦ （可选）要从受管系统检索授权，请安装一个或多个 Identity Manager 驱动程序。
 - ♦ 必须使用 Identity Manager 4.6 或更高版本支持的驱动程序。有关安装驱动程序的详细信息，请参见 [NetIQ Identity Manager 驱动程序文档网站](#) 中的相应驱动程序指南。
 - ♦ 要管理驱动程序，必须先安装 Designer 或适用的 iManager 插件。iManager 插件打包于 Identity Manager 引擎安装中。

Identity Applications 的配置和用法注意事项

在配置和初次使用 Identity Applications 时，请注意以下事项。

- ♦ 只有在您完成以下活动之后，用户才能访问 Identity Applications：
 - ♦ 确保已安装所有必要的 Identity Manager 驱动程序。
 - ♦ 确保身份库的索引处于联机模式。有关在安装期间配置索引的详细信息，请参见 [杂项（第 134 页）](#)。
 - ♦ 在所有浏览器上启用 Cookie。如果禁用了 Cookie，应用程序将不起作用。
- ♦ 在安装过程中，安装程序会将日志文件写入安装目录。这些文件包含有关您的配置的信息。配置 Identity Applications 环境后，应考虑删除这些日志文件或将其储存在安全位置。在安装过程中，可以选择将数据库纲要写入到文件。由于此文件包含有关数据库的描述性信息，因此在安装过程完成后应将文件移至安全位置。
- ♦ （视情况而定）要审计 Identity Applications，必须在环境中安装并配置 Identity Reporting 和审计服务，以捕获事件。此外，还必须配置 Identity Applications，以便能够进行审计。

指定权限索引的位置

当您安装 Identity Applications 时，安装进程将为 Tomcat 创建一个许可权限索引。如果您未指定该索引的位置，安装程序将在临时目录中创建文件夹。例如，Tomcat 上的 `/opt/netiq/idm/apps/tomcat/temp/perminindex`。

在测试环境中，该位置通常无关紧要。但是，在生产或过渡环境中，您可能不想将权限索引放置在临时目录中。

要指定索引的位置，请执行以下操作：

- 1 停止 Tomcat。
- 2 在文本编辑器中，打开 `ism-configuration.properties` 文件。
- 3 在该文件的末尾添加以下文本：

```
com.netiq.idm.cis.indexdir = path/perminindex
```

例如：

```
com.netiq.idm.cis.indexdir = /opt/netiq/idm/apps/tomcat/temp/perminindex
```

- 4 保存并关闭文件。
- 5 删除临时目录中的现有 `perminindex` 文件夹。
- 6 启动 Tomcat。

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**。

安装 Identity Applications 数据库的先决条件

该数据库储存 Identity Applications 数据和配置信息。

在安装数据库实例之前，请先查看以下先决条件：

- ◆ 要配置与 Tomcat 搭配使用的数据库，必须创建一个 JDBC 驱动程序。Identity Applications 使用标准 JDBC 调用来访问并更新该数据库。Identity Applications 使用绑定到 JNDI 树的 JDBC 数据源文件开启与数据库的连接。
- ◆ 必须有一个指向该数据库的现有数据源文件。User Application 安装程序将在 server.xml 和 context.xml 中创建一个指向数据库的 Tomcat 数据来源条目。
- ◆ 确保具备以下信息：
 - ◆ 数据库服务器的主机和端口。
 - ◆ 要创建的数据库的名称。Identity Applications 的默认数据库为 idmuserappdb。
 - ◆ 数据库用户名和口令。数据库用户名必须代表某个管理员帐户，或者必须具有在数据库服务器中创建表的足够许可权限。User Application 的默认管理员是 idmadmin。
 - ◆ 数据库供应商为您所使用的数据库提供的驱动程序 .jar 文件。NetIQ 不支持第三方供应商提供的驱动程序 JAR 文件。
- ◆ 数据库实例可以位于本地计算机上，也可以位于连接的服务器上。
- ◆ 数据库字符集必须使用 Unicode 编码。例如，UTF-8 就是一种使用 Unicode 编码的字符集，而 Latin1 则不使用 Unicode 编码。有关指定字符集的详细信息，请参见[配置字符集（第 73 页）](#)或[配置 Oracle 数据库（第 72 页）](#)。
- ◆ 为了避免在迁移期间发生重复键错误，请使用区分大小写的排序规则。如果发生重复键错误，请检查排序规则并更正它，然后重安装 Identity Applications。
- ◆ （视情况而定）要将同一个数据库实例用于审计和 Identity Applications，NetIQ 建议在一个独立的专用服务器（而非托管运行 Identity Applications 的 Tomcat 的服务器）上安装该数据库。
- ◆ （视情况而定）如果正要迁移到新版 Identity Applications，必须使用之前安装所用的同一个数据库。

- ◆ 数据库群集属于各相关数据库服务器的功能。NetIQ 不提供对任何群集数据库配置的官方测试，因为群集与产品功能不相关。因此，我们在支持群集数据库服务器的同时，作出以下声明：
 - ◆ 默认情况下，最大连接数设置为 100。此值可能太低，无法处理群集中的工作流程请求负载。您可能会看到以下异常：

```
(java.sql.SQLException: Data source rejected establishment of connection,
message from server: "Too many connections.")
```

要增加最大连接数，请在 my.cnf 文件中将 max_connections 变量设置为更高的值。

- ◆ 您可能需要禁用群集数据库服务器的某些功能或方面。例如，由于在尝试插入重复键时存在约束违规，所以必须对某些表禁用事务复制。
- ◆ 我们对于群集数据库服务器的安装、配置或优化不提供任何协助，包括将我们的产品安装到群集数据库服务器中。
- ◆ 我们会尽最大努力来解决在群集数据库环境中使用我们的产品时可能出现的任何问题。在复杂环境中采用的查错方法通常需要双方合作才能解决问题。NetIQ 提供了专业知识，便于您对 NetIQ 产品进行分析、规划及查错。客户必须具有对任何第三方产品进行分析、规划及查错的专业知识。我们将要求客户在非群集环境中再现问题或分析其组件的行为，以帮助从 NetIQ 产品问题中分离出潜在的群集设置问题。

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 workflows 活动的数据库。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 [Identity Applications 的系统要求（第 75 页）](#)。有关 User Application 数据库注意事项的详细信息，请参见 [安装 Identity Applications 数据库的先决条件（第 71 页）](#)。

- ◆ [配置 Oracle 数据库（第 72 页）](#)
- ◆ [配置 SQL Server 数据库（第 73 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 [Identity Applications 的系统要求（第 75 页）](#)。

检查数据库的兼容性级别

来自不同 Oracle 版本的数据库兼容的前提为，这些数据库支持相同的功能且这些功能以相同的方式执行。如果它们不兼容，则某些功能或操作可能不会按预期工作。例如，创建纲要会失败，导致您无法部署 Identity Applications。

要检查数据库的兼容性级别，请执行以下步骤：

1. 连接数据库引擎。
2. 连接到 SQL Server 数据库引擎的适当实例后，在 **对象资源管理器** 中单击服务器名称。
3. 展开 **数据库**，然后根据数据库选择用户数据库，或者展开 **系统数据库** 并选择一个系统数据库。
4. 右键单击数据库，然后单击 **属性**。
数据库属性对话框随即打开。
5. 在 **选择页面** 窗格中，单击 **选项**。
当前兼容性级别显示在 **兼容性级别** 列表框中。
6. 要检查兼容性级别，请在查询窗口中输入以下内容，然后单击 **执行**。


```
SQL> SELECT name, value FROM v$parameter
WHERE name = 'compatible';
```

预期输出为：12.1.0.2

配置字符集

User Application 数据库必须使用 Unicode 编码的字符集。在创建数据库时，请使用 AL32UTF8 指定此字符集。

要确认是否为 Oracle 12c 数据库设置 UTF-8，请发出以下命令：

```
select * from nls_database_parameters;
```

如果数据库未配置为 UTF-8，系统将使用以下信息进行响应：

```
NLS_CHARACTERSET
WE8MSWIN1252
```

否则，系统将使用以下信息进行响应，确认为数据库配置了 UTF-8：

```
NLS_CHARACTERSET
AL32UTF8
```

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 [Identity Applications 的系统要求](#)（第 75 页）。

配置字符集

SQL Server 不允许您为数据库指定字符集。User Application 以支持 UTF-8 的 NCHAR 列类型储存 SQL Server 字符数据。

配置管理员用户帐户

安装 Microsoft SQL Server 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：建议使用 JDBC JAR 版本 sqjjdbc42.jar。

在群集环境中安装 Identity Applications 的先决条件

您可以在 Tomcat 群集支持的环境中安装 Identity Applications 的数据库，不过需要注意以下事项：

- ♦ 群集必须具有唯一的群集分区名称、多路广播地址和多路广播端口。使用唯一的标识符可以区分多个群集，防止出现性能问题和异常行为。
 - ♦ 对于群集的每个成员，必须为 Identity Applications 数据库的侦听端口指定相同的端口号。
 - ♦ 对于群集的每个成员，必须为托管 Identity Applications 数据库的服务器指定相同的主机名或 IP 地址。
- ♦ 必须同步群集中服务器的时钟。如果服务器时钟不同步，会话可能会提前超时，导致 HTTP 会话故障转移无法正常工作。
- ♦ NetIQ 建议不要在同一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均衡解决方案安装在单独的计算机上。

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 74 页）
- ♦ [设置工作流程引擎 ID 的系统属性](#)（第 75 页）
- ♦ [为群集中的每个用户应用程序使用相同的主密钥](#)（第 75 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。只有在重新启动服务器节点后，对群集配置所做的更改才能在该节点上生效。

有关在群集环境中进行安装需要满足的先决条件的详细信息，请参见[第 8.5.2 节“安装 Identity Applications 的先决条件和注意事项”](#)（第 69 页）。

设置工作流程引擎 ID 的系统属性

在群集中托管 Identity Applications 的每个服务器都可以运行一个工作流程引擎。为确保群集和工作流程引擎的性能，群集中的每个服务器都应使用相同的分区名称和分区 UDP 组。此外，还必须使用工作流程引擎的唯一 ID 启动群集中的每个服务器，因为工作流程引擎的群集工作方式与 Identity Applications 的超速缓存框架无关。

为确保工作流程引擎正常运行，必须设置 Tomcat 的系统属性。

- 1 针对群集中的每个 Identity Applications 服务器创建一个新的 JVM 系统属性。
- 2 将系统属性命名为 `com.novell.afw.wf.engine-id`，其中的引擎 ID 是一个唯一值。

为群集中的每个用户应用程序使用相同的主密钥

Identity Applications 使用主密钥加密敏感数据。群集中的所有 Identity Applications 必须使用相同的主密钥。本节将帮助您确保群集中的所有 Identity Applications 使用相同的主密钥。

有关加密 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。

8.5.3 Identity Applications 的系统要求

本节提供要安装 Identity Applications 及其支持框架（包括 PostgreSQL、Tomcat、OSP 和 SSPR）的服务器的最低要求。

类别	要求
处理器	1 GHz
磁盘空间	1 GB
	注释： 为支持应用程序的内容（例如数据库和应用程序服务器日志）留出足够的空间。
内存	512 MB（建议 4 GB）

类别	要求
操作系统（经认可）	<p>以下 64 位操作系统之一：</p> <ul style="list-style-type: none"> ◆ SLES 12 SP3 ◆ SLES 12 SP2 ◆ RHEL 7.4 ◆ RHEL 7.3 <p>NetIQ 建议您在安装 Identity Manager 之前，按照制造商的自动更新工具应用最新的操作系统增补程序。</p> <p>注释：经认可指操作系统已经过全面测试且受支持。</p>
操作系统（受支持）	<p>经认可操作系统的最新版服务包</p> <p>注释：受支持指操作系统尚未经过测试，但预期可以正常工作。</p>
虚拟化系统	<ul style="list-style-type: none"> ◆ Hyper-V Server 2012 R2 ◆ VMWare ESX 5.5 及更高版本 <p>NetIQ 支持在为运行 NetIQ 产品的操作系统提供官方支持的企业级虚拟化系统上安装 Identity Manager。只要虚拟化系统的供应商为这些操作系统提供官方支持，NetIQ 就可支持这些系统上的整个 Identity Manager 堆栈。</p>
数据库	<ul style="list-style-type: none"> ◆ PostgreSQL 9.6.6 ◆ Oracle 12c ◆ MySQL 2016 <p>注释：请勿在 Tomcat 的类路径中包含 PostgreSQL 版本（例如 9.6.6）。如果指定这些版本，系统可能不会装载主页图像。</p>
应用程序服务器	Apache Tomcat 8.5.27
Java	<p>Java 开发工具包 (JDK)</p> <p>或者</p> <p>Sun (Oracle) 提供的 Java 运行时环境 (JRE) 1.8.0_162 或更高版本</p>
端口	8180
Web 浏览器	<p>以下任意浏览器（最低版本）：</p> <ul style="list-style-type: none"> ◆ Apple Safari 9 ◆ Google Chrome 61 或更高版本 ◆ Microsoft Edge 20.10240.17146.0 ◆ Microsoft Internet Explorer 11.0.10240.17443 <p>注释：此“兼容视图”选项在 Internet Explorer 浏览器中不受支持。</p> <ul style="list-style-type: none"> ◆ Mozilla FireFox 51 或更高版本 <p>注释：必须在浏览器中启用 Cookie。如果禁用了 Cookie，该产品将不会正常运行。</p>
Audit	Platform Agent 2011.1r6（最低版本）
目录服务	NetIQ eDirectory 9.1

8.6 规划安装 Identity Reporting

本节提供有关准备安装 Identity Reporting 组件的指导。您可以使用 Sentinel 来审计事件。

- ◆ 第 8.6.1 节 “Identity Reporting 的安装核对清单”（第 77 页）
- ◆ 第 8.6.2 节 “安装 Identity Reporting 组件的先决条件”（第 78 页）
- ◆ 第 8.6.3 节 “了解 Identity Reporting 组件的安装过程”（第 79 页）
- ◆ 第 8.6.4 节 “Identity Reporting 的系统要求”（第 80 页）

8.6.1 Identity Reporting 的安装核对清单

NetIQ 建议您完成以下核对清单中的步骤：

	核对清单项目
<input type="checkbox"/>	1. 了解 Identity Manager 各组件之间的交互。有关详细信息，请参见第 3.3.4 节 “Identity Reporting”（第 22 页）。
<input type="checkbox"/>	2. 确定要为 Identity Manager 组件使用哪些服务器。有关详细信息，请参见第 5.7 节 “建议的安装方案和服务器设置”（第 38 页）。
<input type="checkbox"/>	3. 查看有关安装 Identity Reporting 的注意事项。有关详细信息，请参见第 8.6.2 节 “安装 Identity Reporting 组件的先决条件”（第 78 页）。
<input type="checkbox"/>	4. 查看托管 Identity Reporting 的计算机所要满足的硬件和软件要求。有关详细信息，请参见第 8.6.4 节 “Identity Reporting 的系统要求”（第 80 页）。
<input type="checkbox"/>	5. （视情况而定）对于运行 RHEL 7.3 或更高版本操作系统的计算机，请确保您已安装一组适当的库。
<input type="checkbox"/>	6. （视情况而定）确保已安装 Identity Applications。如果已安装 Advanced Edition，则必须执行此步骤。有关详细信息，请参见第 8 章 “计划安装 Identity Manager 引擎、Identity Applications 和 Identity Reporting”（第 57 页）。
<input type="checkbox"/>	7. 安装 Sentinel。有关详细信息，请参见第 7 节 “安装 SLM for IGA”（第 53 页）
<input type="checkbox"/>	8. 安装 Identity Reporting。有关详细信息，请参见以下章节之一： <ul style="list-style-type: none">◆ 第 9.1.1 节 “执行交互式安装”（第 83 页）◆ 第 9.1.2 节 “以无提示模式安装 Identity Manager 引擎”（第 84 页）
<input type="checkbox"/>	9. 完成 Identity Reporting 的设置。有关详细信息，请参见第 11.10 章 “配置 Identity Reporting”（第 154 页）。
<input type="checkbox"/>	10. 配置驱动程序的环境。有关详细信息，请参见第 11.9 节 “配置运行时环境”（第 146 页）。

8.6.2 安装 Identity Reporting 组件的先决条件

NetIQ 建议您在开始安装前先查看以下信息。

- ◆ [Identity Reporting 的先决条件](#)（第 78 页）
- ◆ [Identity Reporting 的身份审计事件](#)（第 78 页）

Identity Reporting 的先决条件

在安装 Identity Reporting 时，请注意以下先决条件和事项：

- ◆ 需要以下 Identity Manager 组件的受支持且经过配置的版本：
 - ◆ Identity Applications，包括 User Application 驱动程序（仅适用于 Advanced Edition）
 - ◆ Sentinel 安装在单独的 Linux 计算机上。
- ◆ 请不要将 Identity Reporting 安装在群集环境中的服务器上。
- ◆ 要针对 Oracle 数据库运行报告，必须确保已复制 ojdbc8.jar。有关详细信息，请参见[第 11.10.2 节“对 Oracle 数据库运行报告”](#)（第 154 页）。
- ◆ 向您要授予报告功能访问权限的所有用户指派报告管理员角色。
- ◆ 确保 Identity Manager 环境中的所有服务器上都设置了相同的时间。如果您未同步服务器上的时间，有些报告在执行后可能是空的。例如，如果托管 Identity Manager 引擎的服务器和仓库的服务器的时戳不同，则此问题可能会影响与新用户相关的数据。如果您创建了一个用户，随后对其进行了修改，报告中会填充相应的数据。
- ◆ 安装进程会在 Tomcat 的 setenv.sh 文件中修改 JRE 映射的 JAVA_OPTS 或 CATALINA_OPTS 条目。

Identity Reporting 的身份审计事件

本节提供有关如何标识 Identity Manager 报告和自定义报告所需的不同审计事件的信息。您可以解压缩所有报告源并运行以下脚本来标识审计事件：

```
find . -name *.jrxml -print0 |xargs -0 grep -H "'000[B3]" | perl -ne '($file) = /  
^\.\.\/(.*)\/\//;@a = /000[3B].../g; foreach $a (@a) { print "$file;$a\n"}' |sort -u
```

本节提供有关如何标识和选择 Identity Manager 报告和自定义报告的不同审计事件的信息：

事件名称	审计标志
鉴定和口令更改	<p>选择使用 SSPR 的审计标志： 启动 SSPR 配置编辑器 > 审计配置 > 选择以下审计标志之一：</p> <ul style="list-style-type: none"> ♦ 鉴定 ♦ 更改口令 ♦ 解除锁定口令 ♦ 恢复口令 ♦ 入侵者尝试 ♦ 入侵者锁定 ♦ 入侵者锁定用户 <p>选择使用 iManager 的审计标志： 转到 iManager 角色和任务 > eDirectory 审计 > > 审计配置 > Novell Audit > 选择以下审计标志之一：</p> <ul style="list-style-type: none"> ♦ 更改口令 ♦ 校验口令 ♦ 登录 ♦ 注销
所有其他报告事件	转到 NetIQ Identity Manager UserApp > 管理 > 日志记录 > 启用审计服务

8.6.3 了解 Identity Reporting 组件的安装过程

NetIQ 建议将 Sentinel 和 Reporting 安装在不同的服务器上。

如果进行全新安装，安装程序将在该数据库中创建表并校验连接性。程序还会安装 PostgreSQL JDBC 驱动程序的 JAR 文件，并自动使用此文件建立数据库连接。

如果您已将您的数据（例如 SIEM）从 EAS 迁移到 PostgreSQL 数据库，则安装程序将连接到现有数据库。

Identity Reporting 的安装程序会执行以下功能：

- ♦ 配置 Identity Reporting 的鉴定服务
- ♦ 配置 Identity Reporting 的电子邮件递送系统
- ♦ 配置 Identity Reporting 的核心报告服务
- ♦ 部署 Identity Reporting 正常工作所需的驱动程序、受管系统网关和数据收集服务。
- ♦ 为 Identity Reporting 配置 PostgreSQL 数据库

8.6.4 Identity Reporting 的系统要求

本节提供要安装 Identity Reporting 的服务器的最低要求。

此外，请务必查看安装的先决条件和注意事项，特别是与操作系统有关的内容。

类别	要求
处理器	1 GHz
磁盘空间	1 GB 注释： 为支持应用程序的内容（例如数据库和应用程序服务器日志）留出足够的空间。
内存	512 MB（建议 4 GB）
操作系统（经认可）	以下 64 位操作系统之一： <ul style="list-style-type: none">◆ SLES 12 SP3◆ SLES 12 SP2◆ RHEL 7.4◆ RHEL 7.3 NetIQ 建议您在安装 Identity Manager 之前，按照制造商的自动更新工具应用最新的操作系统增补程序。 注释： 经认可指操作系统已经过全面测试且受支持。
操作系统（受支持）	经认可操作系统的最新版服务包 注释： 受支持指操作系统尚未经过测试，但预期可以正常工作。
虚拟化系统	<ul style="list-style-type: none">◆ Hyper-V Server 2012 R2◆ VMWare ESX 5.5 及更高版本 NetIQ 支持在为运行 NetIQ 产品的操作系统提供官方支持的企业级虚拟化系统上安装 Identity Manager。只要虚拟化系统的供应商为这些操作系统提供官方支持，NetIQ 就可支持这些系统上的整个 Identity Manager 堆栈。
数据库	<ul style="list-style-type: none">◆ PostgreSQL9.6.6◆ Oracle12.2.01
应用程序服务器	Apache Tomcat 8.5.27
Java	Java 开发工具包 (JDK) 或者 Sun (Oracle) 提供的 Java 运行时环境 (JRE) 1.8.0_162 或更高版本

类别	要求
Web 浏览器	<p>以下任意浏览器（最低版本）：</p> <p>Desktop</p> <ul style="list-style-type: none"> ◆ Apple Safari 9 ◆ Google Chrome 61 或更高版本 ◆ Microsoft Internet Explorer 11 ◆ Mozilla FireFox 51 或更高版本 <p>iPad</p> <ul style="list-style-type: none"> ◆ Apple Safari 9 ◆ Google Chrome 61 或更高版本 <p>注释：必须在浏览器中启用 Cookie。如果禁用了 Cookie，该产品将不会正常运行。</p>
Audit	Sentinel Log Management for IGA

9 安装 Identity Manager 引擎、Identity Applications 和 Identity Reporting

本章引导您完成安装 Identity Manager 引擎、Identity Applications 和 Identity Reporting 组件的必需组件的过程。

可以使用交互模式或无提示模式进行安装。安装程序将提供创建无提示属性文件的选项。您可以将多个组件的安装选项记录在属性文件中，然后使用该文件在您环境中的其他服务器上运行无提示安装。无提示安装程序会从该文件中读取相应的值来执行安装。

可以在安装 Identity Manager 组件之后立即配置它们，也可以稍后配置。

安装程序会将组件安装在第 5.5 节“默认安装位置”（第 36 页）中所述的预定义位置。

NetIQ 建议您在开始之前，先查看安装过程。有关详细信息，请参见第 8 章“计划安装 Identity Manager 引擎、Identity Applications 和 Identity Reporting”（第 57 页）。

9.1 安装 Identity Manager 引擎

可以使用以下方法来安装 Identity Manager 引擎：

- 第 9.1.1 节“执行交互式安装”（第 83 页）
- 第 9.1.2 节“以无提示模式安装 Identity Manager 引擎”（第 84 页）
- 第 9.1.3 节“以非 root 用户身份安装 Identity Manager 引擎”（第 84 页）

9.1.1 执行交互式安装

- 1 从 NetIQ 下载网站下载 Identity_Manager_4.7_Linux.iso。
- 2 装入下载的 .iso。
- 3 从 .iso 文件的根目录中，运行以下命令：

```
./install.sh
```
- 4 通读许可协议。
- 5 输入 y 以接受许可协议。
- 6 决定要安装的 Identity Manager 服务器版本。输入 y 将安装 Advanced Edition，输入 n 将安装 Standard Edition。
- 7 选择 Identity Manager 引擎并继续安装。
- 8 配置安装的组件。有关详细信息，请参见第 10 章“配置安装的组件”（第 91 页）。

9.1.2 以无提示模式安装 Identity Manager 引擎

- 1 从 NetIQ 下载网站下载 Identity_Manager_4.7_Linux.iso。
- 2 装入下载的 .iso。
- 3 从 .iso 的根目录中，运行以下命令：

```
./create_silent_props.sh
```
- 4 输入 y 以确认创建文件。
- 5 要安装 JRE，请输入 y。
- 6 要升级现有的 Identity Manager 组件，请输入 y。
- 7 决定要安装的 Identity Manager 服务器版本。输入 y 将安装 Advanced Edition，输入 n 将安装 Standard Edition。
- 8 选择组件的配置模式。有关详细信息，请参见第 10 章“配置安装的组件”（第 91 页）。
- 9 指定要安装的组件。
- 10 运行以下命令以执行无提示安装：

```
./install.sh -s -f <无提示属性文件的位置>
```

例如，

```
./install.sh -s -f /mnt/silent.properties
```

，其中， /mnt/silent.properties 是无提示属性文件的储存位置。

9.1.3 以非 root 用户身份安装 Identity Manager 引擎

您可以使用非 root 用户身份安装 Identity Manager 引擎，以增强 Linux 服务器的安全性。如果您是以 root 用户身份安装身份库的，则不能以非 root 用户身份安装 Identity Manager 引擎。如果要以非 root 用户身份安装引擎，则需执行以下步骤：

1. 确保已安装 NCI。有关详细信息，请参见[安装 NCI](#)（第 84 页）。
2. 以非 root 用户身份安装身份库。有关详细信息，请参见[以非 root 用户身份安装身份库](#)（第 85 页）。
3. 以非 root 用户身份安装 Identity Manager 引擎。有关详细信息，请参见[以非 root 用户身份安装引擎](#)（第 86 页）。

安装 NCI

必须先安装 NCI，然后再继续身份库安装。由于必需的 NCI 包将在系统范围内使用，因此建议您使用 root 用户身份安装必要的包。但是，如果需要，您也可以使用 sudo 将访问权委托给其他帐户，然后使用该帐户来安装 NCI 包。

- 1 从装入的 iso 中，导航到 /IDVault/setup/ 目录。
- 2 运行以下命令：

```
rpm -ivh nci64-3.1.0-0.00.x86_64.rpm
```
- 3 校验 NCI 是否设置为服务器模式。输入下面的命令：

```
/var/opt/novell/nci/set_server_mode
```

必须执行此步骤，以确保身份库配置不会失败。

以非 root 用户身份安装身份库

本节介绍如何使用 tarball 来安装身份库。当您提取文件时，系统将创建 etc、opt 和 var 目录。

- 1 使用对要安装身份库的计算机具有适当权限的 sudo 用户身份登录。

注释：如果您想要指定自定义安装路径，也可以使用 root 用户身份登录。

- 2 从装入的 iso 中，导航到 /IDVault/ 目录。
- 3 创建一个新目录，然后将 eDir_NonRoot.tar.gz 文件复制到该目录。例如：/home/user/install/eDirectory。
- 4 使用以下命令提取文件：

```
tar -zxvf eDir_NonRoot.tar.gz
```

- 5 （视情况而定）要手动导出环境变量的路径，请输入以下命令：

```
export LD_LIBRARY_PATH=custom_location/eDirectory/opt/novell/eDirectory/  
lib64:custom_location/eDirectory/opt/novell/eDirectory/lib64/ndsmodule:  
custom_location/eDirectory/opt/novell/lib64:$LD_LIBRARY_PATH
```

```
export PATH=custom_location/eDirectory/opt/novell/eDirectory/  
bin:custom_location/eDirectory/opt/novell/eDirectory/sbin:/opt/novell/  
eDirectory/bin:$PATH
```

```
export MANPATH=custom_location/eDirectory/opt/novell/man:custom_location/  
eDirectory/opt/novell/eDirectory/man:$MANPATH
```

```
export TEXTDOMAINDIR=custom_location/eDirectory/opt/novell/eDirectory/  
share/locale:$TEXTDOMAINDIR
```

- 6 （视情况而定）要使用 ndspath 脚本导出环境变量的路径，必须在实用程序的前面添加 ndspath 脚本。完成下列步骤：

- 6a 从 custom_location/eDirectory/opt directory 使用以下命令运行该实用程序：

```
custom_location/eDirectory/opt/novell/eDirectory/bin/ndspath  
utility_name_with_parameters
```

- 6b 使用以下命令导出当前外壳中的路径：

```
. custom_location/eDirectory/opt/novell/eDirectory/bin/ndspath
```

- 6c 像平时一样运行实用程序。

- 6d 在 /etc/profile、~/bashrc 或类似脚本的末尾添加用于导出路径的指令。

执行此步骤后，每当您登录或者打开新外壳时，都可以直接启动实用程序。

- 7 要配置身份库，请完成以下步骤之一：

- 7a 要运行 ndsconfig 实用程序，请在命令行中输入以下文本：

```
ndsconfig new [-t treename] [-n server_context] [-a admin_FDN] [-w  
admin_password] [-i] [-S server_name] [-d path_for_dib] [-m module] [e] [-L  
ldap_port] [-l SSL_port] [-o http_port] -O https_port] [-p IP  
address:[port]] [-c] [-b port_to_bind] [-B interface1@port1,  
interface2@port2,...] [-D custom_location] [--config-file  
configuration_file]
```

例如：

```
ndsconfig new -t mary-tree -n novell -a admin.novell -S linux1 -d /home/mary/inst1/data -b 1025 -L 1026 -l 1027 -o 1028 -O 1029 -D /home/mary/inst1/var --config-file /home/mary/inst1/nds.conf
```

注释：

- ♦ 必须指定介于 1024 到 65535 之间的端口号。不能对任何 eDirectory 应用程序假定默认端口 524。
- ♦ 端口规范中的这条限制可能会给以下类型的应用程序造成负面影响：
 - ♦ 无法使用选项来指定目标服务器端口的应用程序。
 - ♦ 使用 NCP 并针对 524 以 root 身份运行的旧式应用程序。
- ♦ 可以在 -B 和 -P 选项中指定 IPv6 地址。要指定 IPv6 地址，必须将地址包含在方括号 [] 中。例如：-B [2015::4]@636。

7b 使用 ndsmanage 实用程序配置一个新实例。有关详细信息，请参见[在身份库中创建新实例（第 104 页）](#)。

以非 root 用户身份安装引擎

当您使用此方法时，无法安装以下组件：

- ♦ **Remote Loader：** 要以非 root 用户身份安装 Remote Loader，请使用 Java Remote Loader。有关详细信息，请参见[安装 Java Remote Loader（第 87 页）](#)。
- ♦ **Linux 帐户驱动程序：** 需要根特权才能正常工作。

注释： 以非 root 用户身份安装 Identity Manager 引擎时，安装文件位于非 root 用户目录下。例如，/home/user（其中 user 为非 root 用户）。运行 Identity Manager 并不需要安装文件。您可在安装后删除安装文件。

要以非 root 用户身份安装 Identity Manager 引擎，请执行以下操作：

- 1 以安装身份库时使用的非 root 用户身份登录。
该用户帐户必须对非 root 身份库安装的目录和文件具有写访问权限。
- 2 导航到装入 Identity_Manager_4.7_Linux.iso 的位置。
- 3 从装入位置中，导航到 /IDM 目录。
- 4 执行以下命令：
./idm-nonroot-install.sh
- 5 使用以下信息完成安装：

非 root eDirectory 安装的基本目录

指定非根 eDirectory 安装的目录。例如：/home/user/install/eDirectory。

扩展 eDirectory 纲要

如果这是在此 eDirectory 实例中安装的第一个 Identity Manager 服务器，请输入 Y 以扩展纲要。如果纲要未扩展，则 Identity Manager 无法生效。

系统会提示您扩展由非根 eDirectory 安装托管的非根用户所拥有的每个 eDirectory 实例的纲要。

如果选择扩展纲要，请指定有权扩展该纲要的 eDirectory 用户的完整判别名 (DN)。用户必须具有对整个树的主管权限才能扩展纲要。有关以非根用户身份扩展纲要的更多信息，请参见位于各个 eDirectory 实例的 data 目录中的 schema.log 文件。

运行 /opt/novell/eDirectory/bin/idm-install-schema 程序以在安装完成后在其他 eDirectory 实例上扩展纲要。

- 6 要完成安装过程，请继续第 11.1 节“完成非 Root 用户安装”（第 97 页）。
- 7 激活 Identity Manager。有关详细信息，请参见第 24 章“激活 Identity Manager”（第 213 页）。
- 8 要创建和配置驱动程序对象，请查阅该驱动程序的特定指南。有关详细信息，请参见 [Identity Manager 驱动程序文档网站](#)。

9.2 安装 Java Remote Loader

一般来说，您会在操作系统与本机 Remote Loader 不兼容的计算机上安装 Java Remote Loader dirxml_jremote。不过，Java Remote Loader 也可以在您可能安装了本机 Remote Loader 的同一服务器上运行。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。您可以在装有任何公开支持的 Java 版本的任何受支持 Linux 计算机上安装 dirxml_jremote。

- 1 在托管 Identity Manager 引擎的服务器上，复制默认位于 /opt/novell/eDirectory/lib/dirxml/classes 目录中的应用程序 Shim .iso 或 .jar 文件。
- 2 登录到要安装 Java Remote Loader 的计算机（目标计算机）。
- 3 校验目标计算机是否装有受支持版本的 JRE。
- 4 要访问安装程序，请完成以下步骤之一：
 - 4a （视情况而定）如果您已获取 Identity Manager 安装包的 .iso 映像文件，请浏览到包含 Java Remote Loader 安装文件的目录（默认为 products/IDM/java_remoteloader）。
 - 4b （视情况而定）如果您已从 [NetIQ 下载网站](#) 下载了 Java Remote Loader 安装文件，请完成以下步骤：
 - 4b1 浏览到所下载映像的 .tgz 文件。
 - 4b2 将该文件的内容解压缩到本地计算机上的某个文件夹中。
- 5 将 dirxml_jremote_dev.tar.gz 文件复制到目标计算机上的所需位置。例如，将该文件复制到 /usr/idm。
- 6 将以下文件之一复制到目标计算机上的所需位置：
 - ♦ dirxml_jremote.tar.gz
 - ♦ dirxml_jremote_mvs.tar有关 mvs 的信息，请解压缩 dirxml_jremote_mvs.tar 文件，然后参见 usage.html 文档。
- 7 在目标计算机上，解压缩 .tar.gz 文件。
例如，输入 gunzip dirxml_jremote.tar.gz 或 tar -xvf dirxml_jremote_dev.tar。
- 8 将您在步骤 1 中从 dirxml/classes 目录复制的应用程序 shim 的 .iso 或 .jar 文件放置于 lib 目录下。

- 9 要自定义 dirxml_jremote 脚本以便能够通过 RDXML_PATH 环境变量访问 Java 可执行文件，请完成以下步骤之一：
 - 9a 输入以下命令之一，以设置环境变量 RDXML_PATH：
 - ♦ set RDXML_PATH=path
 - ♦ export RDXML_PATH
 - 9b 编辑 dirxml_jremote 脚本，并在脚本行中向执行 Java 的 Java 可执行文件预先添加路径。
- 10 必须在 dirxml_jremote 脚本中指定 jar 文件的位置。这些文件位于解压缩 dirxml_jremote.tar.gz 目录的 lib 子目录中。例如，/lib/*.jar。
- 11 配置示例配置文件 config8000.txt，使其可用于您的应用程序 shim。

默认情况下，该示例文件位于 /opt/novell/dirxml/doc 目录中。有关详细信息，请参见第 11.3 章“配置 Remote Loader 和驱动程序”（第 105 页）。

9.3 安装 Identity Applications

可以使用以下方法来安装 Identity Applications：

- ♦ 第 9.3.1 节“执行交互式安装”（第 88 页）
- ♦ 第 9.3.2 节“以无提示模式安装”（第 88 页）
- ♦ 第 9.3.3 节“以交互模式安装 SSPR”（第 89 页）
- ♦ 第 9.3.4 节“以无提示模式安装 SSPR”（第 89 页）

9.3.1 执行交互式安装

- 1 从 NetIQ 下载网站下载 Identity_Manager_4.7_Linux.iso。
- 2 装入下载的 .iso。
- 3 从 .iso 文件的根目录中，运行以下命令：

```
./install.sh
```
- 4 通读许可协议。
- 5 输入 y 以接受许可协议。
- 6 决定要安装的 Identity Manager 服务器版本。输入 y 将安装 Advanced Edition，输入 n 将安装 Standard Edition。
- 7 选择 Identity Applications 并继续安装。
- 8 配置安装的组件。有关详细信息，请参见第 10 章“配置安装的组件”（第 91 页）。

9.3.2 以无提示模式安装

- 1 从 NetIQ 下载网站下载 Identity_Manager_4.7_Linux.iso。
- 2 装入下载的 .iso。
- 3 从 .iso 的根目录中，运行以下命令：

```
./create_silent_props.sh
```
- 4 输入 y 以确认创建文件。

- 5 要安装 JRE，请输入 y。
- 6 决定要安装的 Identity Manager 服务器版本。输入 y 将安装 Advanced Edition，输入 n 将安装 Standard Edition。
- 7 选择组件的配置模式。有关详细信息，请参见第 10 章“配置安装的组件”（第 91 页）。
- 8 选择 Identity Applications 并继续安装。
- 9 运行以下命令以执行无提示安装：
`./install.sh -s -f <无提示属性文件的位置>`
例如，
`./install.sh -s -f /mnt/silent.properties`，其中，/mnt/silent.properties 是无提示属性文件的储存位置。

9.3.3 以交互模式安装 SSPR

如果要在分布式环境中安装 Identity Applications 和 SSPR，安装程序会为您提供单独安装 SSPR 的选项。

- 1 从 NetIQ 下载网站下载 Identity_Manager_4.7_Linux.iso。
- 2 装入下载的 .iso。
- 3 从 .iso 文件的根目录中，导航到 SSPR 目录。
- 4 运行以下命令：
`./install.sh`
- 5 通读许可协议。
- 6 输入 y 以接受许可协议。
- 7 配置安装的组件。有关详细信息，请参见第 10 章“配置安装的组件”（第 91 页）。

9.3.4 以无提示模式安装 SSPR

- 1 从 NetIQ 下载网站下载 Identity_Manager_4.7_Linux.iso。
- 2 装入下载的 .iso。
- 3 从 .iso 文件的根目录中，导航到 SSPR 目录。
- 4 运行以下命令：
`./install.sh -s sspr_silentinstall.properties`

9.4 安装 Identity Reporting

可以使用以下方法来安装 Identity Reporting：

- ♦ 第 9.4.1 节“执行交互式安装”（第 90 页）
- ♦ 第 9.4.2 节“以无提示模式安装”（第 90 页）

9.4.1 执行交互式安装

- 1 从 NetIQ 下载网站下载 Identity_Manager_4.7_Linux.iso。
- 2 装入下载的 .iso。
- 3 从 .iso 文件的根目录中，运行以下命令：
`./install.sh`
- 4 通读许可协议。
- 5 输入 y 以接受许可协议。
- 6 决定要安装的 Identity Manager 服务器版本。输入 y 将安装 Advanced Edition，输入 n 将安装 Standard Edition。
- 7 指定 Identity Reporting 并继续安装。
- 8 配置安装的组件。有关详细信息，请参见第 10 章“配置安装的组件”（第 91 页）。

9.4.2 以无提示模式安装

- 1 从 NetIQ 下载网站下载 Identity_Manager_4.7_Linux.iso。
- 2 装入下载的 .iso。
- 3 从 .iso 的根目录中，运行以下命令：
`./create_silent_props.sh`
- 4 输入 y 以确认创建文件。
- 5 要安装 JRE，请输入 y。
- 6 决定要安装的 Identity Manager 服务器版本。输入 y 将安装 Advanced Edition，输入 n 将安装 Standard Edition。
- 7 选择组件的配置模式。有关详细信息，请参见第 10 章“配置安装的组件”（第 91 页）。
- 8 指定 Identity Reporting 并继续安装。
- 9 运行以下命令以执行无提示安装：
`./install.sh -s -f <无提示属性文件的位置>`
例如，
`./install.sh -s -f /mnt/silent.properties`，其中，/mnt/silent.properties 是无提示属性文件的储存位置。

10 配置安装的组件

本章引导您完成配置第 9 章“安装 Identity Manager 引擎、Identity Applications 和 Identity Reporting”（第 83 页）中所安装 Identity Manager 组件的过程。您可以采用交互模式（控制台）或无提示模式执行配置。

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，请参见第 10.1 节“了解配置参数”（第 91 页）。

10.1 了解配置参数

本节定义配置 Identity Manager 安装需要指定的参数。您可以在安装组件后立即使用安装程序来配置组件，也可以稍后再配置。

注释：

- 如果采用典型配置模式配置 Identity Applications 和 Identity Reporting，则无法连接到安装在其他计算机上的数据库。
 - 安装过程不允许您启用审计。必须单独为 Identity Manager 组件启用审计。有关详细信息，请参见《NetIQ Identity Manager - Configuring Auditing in Identity Manager》（NetIQ Identity Manager - 在 Identity Manager 中配置审计）。
-

参数 典型配置

Identity Manager 引擎

通用口令	指定是否要设置通用口令。
身份库管理员名称	指定树中至少对要添加此服务器的环境具有完整权限的管理员对象的相对判别名 (RDN)。

Identity Applications

通用口令	指定是否要设置通用口令。
身份库管理员名称	指定树中至少对要添加此服务器的环境具有完整权限的管理员对象的相对判别名 (RDN)。
主机名（小写 FQDN）	指定服务器的完全限定判别名或默认 IP 地址。
应用程序服务器 DNS/IP 地址	指定 Tomcat 服务器的 IP 地址。
Identity Applications 管理员名称	指定 Identity Applications 管理员帐户的名称。

Identity Reporting

通用口令	指定是否要设置通用口令。
身份库管理员名称	指定树中至少对要添加此服务器的环境具有完整权限的管理员对象的相对判别名 (RDN)。

参数 典型配置

主机名（小写 FQDN）	指定服务器的完全限定判别名或默认 IP 地址。
连接到外部 One SSO 服务器	指定是否要连接到不同的 One SSO 服务器。
应用程序服务器 DNS/IP 地址	指定 Tomcat 服务器的 IP 地址。
One SSO 服务器 DNS/IP 地址	指定安装了单点登录服务的服务器的 IP 地址。
Identity Reporting 管理员名称	指定 Identity Reporting 的管理员名称。默认值为 cn=uaadmin,ou=sa,o=data。

参数 自定义配置

Identity Manager 引擎

身份库树名	为身份库指定新的树。树名必须满足以下要求： <ul style="list-style-type: none">♦ 树名在网络中必须是唯一的。♦ 树名的长度必须为 2 到 32 个字符。♦ 树名只能包含字母 (A-Z)、数字 (0-9)、连字符 (-) 和下划线 (_) 之类的字符。
身份库管理员名称	指定树中至少对要添加此服务器的环境具有完整权限的管理员对象的相对判别名 (RDN)。
身份库管理员口令	指定管理员对象的口令。例如， <i>password</i> 。
NDS var 文件夹位置	指定此身份库实例在此服务器上的路径。默认路径是 /var/opt/novell/eDirectory。
NDS 数据位置	指定本地系统中要安装目录信息数据库 (DIB) 文件的路径。DIB 文件是您的身份库数据库文件。默认位置是 /var/opt/novell/eDirectory/data/dib。
NCP 端口	指定身份库用来与 Identity Manager 各组件通讯的 NetWare 核心协议 (NCP) 端口。默认值为 524。
LDAP 非 SSL 端口	指定身份库要用来侦听明文格式 LDAP 请求的端口。默认值为 389。
LDAP SSL 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。
身份库 HTTP 端口	指定 HTTP 堆栈要以明文格式运行所需使用的端口。默认值为 8028。
身份库 HTTPS 端口	指定 HTTP 堆栈采用 TLS/SSL 协议运行所需使用的端口。默认值为 8030。
含路径的 NDS 配置文件	指定身份库配置文件的位置。默认值为 /etc/opt/novell/eDirectory/conf/nds.conf。
身份库驱动程序集名称	为新的 Identity Manager 驱动程序集对象指定名称。
身份库驱动程序集部署环境	指定要在其中创建驱动程序集对象的容器的 LDAP DN。

参数 自定义配置

Identity Applications

主机名（小写 FQDN）	指定服务器的完全限定判别名或默认 IP 地址。 注释： 确保以小写字符指定 FQDN。另外，必须将托管组件的服务器配置为使用小写 FQDN。
身份库主机名 /IP 地址	指定安装了身份库的服务器的 IP 地址。
身份库管理员名称	指定树中至少对要添加此服务器的环境具有完整权限的管理员对象的相对判别名 (RDN)。
身份库管理员口令	指定管理员对象的口令。例如， <i>password</i> 。
应用程序服务器 DNS/IP 地址	指定 Tomcat 服务器的 IP 地址。
OSP 自定义登录屏幕名称	指定将显示在 OSP 登录屏幕上的名称。
SSPR 配置口令	<i>仅当将通用口令设置为否时才适用。</i> 指定 Identity Applications 用于进行口令管理的口令。
OAuth 密钥存储区口令	<i>仅当将通用口令设置为否时才适用。</i> 指定您要创建以用于在 OAuth 服务器上装载新密钥存储区的口令。
用户搜索容器 DN	指定身份库中所有用户对象的默认容器。
管理员搜索容器 DN	指定数据组织中保存 Identity Manager 所有数据对象的位置。管理员应确保所有用户都有权访问此容器和所有子容器。
应用程序服务器 HTTPS 端口	指定 Tomcat 服务器在与客户端计算机通讯时要使用的 HTTPS 端口。默认值为 8543。
One SSO 服务器 SSL 端口	指定单点登录服务要使用的端口。默认值为 8543。
Identity Application One SSO 服务口令	<i>仅当将通用口令设置为否时才适用。</i> 指定 Identity Applications 使用的单点登录客户端的口令。
Identity Applications 管理员名称	指定 Identity Applications 管理员帐户的名称。
LDAP 非 SSL 端口	指定身份库要用来侦听明文格式 LDAP 请求的端口。默认值为 389。
身份库驱动程序集名称	指定身份库的驱动程序集名称。
身份库驱动程序集部署环境	指定要在其中创建驱动程序集对象的容器的 LDAP DN。
数据库平台	指定 Identity Applications 所需的数据库。
在当前服务器上配置 PostgreSQL	指定是否要在同一台服务器上配置 PostgreSQL 数据库。
Identity Applications 数据库端口	指定 Identity Applications 的数据库端口。
Identity Applications 数据库名称	指定数据库的名称。默认值为 <i>idmuserappdb</i> 。
Identity Applications 数据库用户名	指定 Identity Applications 数据库管理员的用户名

参数 自定义配置

Identity Application 数据库 JDBC jar 文件	指定数据库平台的 JAR 文件。
创建纲要	作为安装过程的一部分，指出要在何时创建数据库纲要。可用选项有 现在 、 启动 和 文件 。
创建新数据库或从现有数据库升级 / 迁移	指定是要创建新数据库还是从现有数据库升级。
使用自定义容器作为根容器	<p>指定是否要使用自定义容器作为根容器。默认情况下，安装程序会创建 o=data 并选择它作为用户容器，然后指派口令策略和所需的受托者权限。</p> <p>要创建自定义容器，请选择是。</p>
自定义容器 LDIF 文件路径	<p>仅当将自定义容器设置为是时适用。</p> <p>为自定义容器指定 LDIF 文件的路径。</p>
根容器	指定根容器。默认值为 o=data。
组搜索根容器 DN	指定组搜索根容器的 DN。

Identity Reporting

主机名（小写 FQDN）	<p>指定服务器的完全限定判别名或默认 IP 地址。</p> <p>注释：确保以小写字符指定 FQDN。另外，必须将托管组件的服务器配置为使用小写 FQDN。</p>
身份库主机名 /IP 地址	指定安装了身份库的服务器的 IP 地址。
LDAP SSL 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。
身份库管理员名称	指定树中至少对要添加此服务器的环境具有完整权限的管理员对象的相对判别名 (RDN)。
身份库管理员口令	指定管理员对象的口令。例如， <i>password</i> 。
应用程序服务器 DNS/IP 地址	指定 Tomcat 服务器的 IP 地址。
OSP 自定义登录屏幕名称	指定将显示在 OSP 登录屏幕上的名称。
用户搜索容器 DN	指定身份库中所有用户对象的默认容器。
管理员搜索容器 DN	指定数据组织中保存 Identity Manager 所有数据对象的位置。管理员应确保所有用户都有权访问此容器和所有子容器。
应用程序服务器 HTTPS 端口	指定 Tomcat 服务器在与客户端计算机通讯时要使用的 HTTPS 端口。默认值为 8543。
One SSO 服务器 DNS/IP 地址	指定安装了单点登录服务的服务器的 IP 地址。
One SSO 服务器 SSL 端口	指定单点登录服务要使用的端口。默认值是 8543。
Identity Reporting 数据库名称	指定 Identity Reporting 的数据库名称。默认值为 idmrptdb。
Identity Reporting 数据库用户	指定允许 Identity Reporting 访问和修改数据库中的数据的管理帐户。默认值为 rptadmin。

参数 自定义配置

Identity Reporting 数据库主机	指定需要在其中创建数据库的服务器的 DNS 名称或 IP 地址。
Identity Reporting 数据库端口	指定用于连接数据库的端口。默认端口为 5432。
Identity Application 数据库 JDBC jar 文件	指定数据库平台的 JAR 文件。
Identity Reporting 数据库帐户口令	指定 Identity Reporting 的数据库帐户口令。
创建纲要	<p>作为安装过程的一部分，指出要在何时创建数据库纲要。可用选项有现在、启动和文件。</p> <p>如果为数据库纲要创建选项选择启动或文件，则必须手动将数据源添加到“身份数据收集服务”页面。有关详细信息，请参见第 11.10.1 节“在“身份数据收集服务”页面中手动添加数据源”（第 154 页）。</p> <p>如果您的数据库在其他服务器上运行，则必须连接到该数据库。对于远程安装的 PostgreSQL 数据库，请校验该数据库是否正在运行。要连接到远程 PostgreSQL 数据库，请参见第 11.10.6 节“连接远程 Remote PostgreSQL 数据库”（第 156 页）。如果要连接到 Oracle 数据库，请确保已创建 Oracle 数据库实例。有关更多信息，请参见 Oracle 文档。</p> <p>如果为数据库纲要创建选项选择启动或文件，则必须在配置后手动创建表并连接到数据库。有关详细信息，请参见第 11.10.3 节“手动生成数据库纲要”（第 155 页）。</p>
默认电子邮件地址	指定您希望 Identity Reporting 用作电子邮件通知来源的电子邮件地址。
SMTP 服务器	指定 Identity Reporting 用于发送通知的 SMTP 电子邮件主机的 IP 地址或 DNS 名称。
SMTP 服务器端口	指定 SMTP 服务器的端口号。默认端口为 465。
为 Identity Reporting 创建 MSGW 和 DCS 驱动程序	指定是否要创建 MSGW 和 DCS 驱动程序。

10.2 执行配置

下列各节提供有关配置 Identity Manager 组件的信息。

10.2.1 执行交互式配置

- 1 导航到装入 Identity_Manager_4.7_Linux.iso 的位置。
- 2 执行以下命令：

```
./configure.sh
```
- 3 决定是要执行典型配置还是自定义配置。配置选项将因您选择要配置的组件而异。
- 4 要配置组件，请参考第 10.1 节“[了解配置参数](#)”（第 91 页）中的信息。

10.2.2 执行无提示配置

1 导航到装入 Identity_Manager_4.7_Linux.iso 的位置。

2 执行以下命令：

```
./configure.sh -s -f <无提示属性文件的位置>
```

例如，

```
./configure.sh -s -f /mnt/silent.properties
```

其中， /mnt/silent.properties 是无提示属性文件的储存位置。

3 要配置组件，请参考第 10.1 节“了解配置参数”（第 91 页）中的信息。

11

完成安装的最后步骤

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：

- 第 11.1 节“完成非 Root 用户安装”（第 97 页）
- 第 11.2 节“安装后配置身份库”（第 98 页）
- 第 11.3 节“配置 Remote Loader 和驱动程序”（第 105 页）
- 第 11.4 节“配置 Identity Applications 的身份库”（第 125 页）
- 第 11.5 节“为群集配置 User Application 驱动程序”（第 126 页）
- 第 11.6 节“配置 Identity Applications 的设置”（第 126 页）
- 第 11.7 节“启动 Identity Applications”（第 144 页）
- 第 11.8 节“为群集配置 OSP 和 SSPR”（第 144 页）
- 第 11.9 节“配置运行时环境”（第 146 页）
- 第 11.10 节“配置 Identity Reporting”（第 154 页）

11.1 完成非 Root 用户安装

以非 root 用户身份安装 Identity Manager 引擎和插件时，安装过程会执行所有预期的安装活动。本节将指导您执行完成安装所需的手动过程。

11.1.1 为口令策略创建容器

Identity Manager 需要身份库中的口令策略对象。但是，非 root 用户身份安装过程不会创建口令策略的容器。

- 1 在 iManager 中登录到 Identity Manager 树。
- 2 导航到 eDirectory 中的安全性容器。

11.1.2 增加对电子邮件通知中的图形的支持

如果您以非 root 用户身份安装身份库和 Identity Manager 引擎，电子邮件通知可能无法包含电子邮件模板中提供的图形或图像。例如，运行 do-send-email-from-template 操作时，Identity Manager 会发送电子邮件，但是包含的图像都是空白的。您必须更新驱动程序集以确保获得图形支持。

- 1 在 Designer 中登录到您的项目。
- 2 在“概要”窗格中，展开身份库。
- 3 右键单击驱动程序集。
- 4 选择属性 > Java。
- 5 对于 JVM 选项，输入以下内容：

```
-Dcom.novell.nds.dirxml.util.mail.templatepath=path_to_graphics_files
```

例如：

```
-Dcom.novell.nds.dirxml.util.mail.templatepath=/prod/eDirectory/opt/novell/  
eDirectory/lib/dirxml/rules/manualtask/mt_files
```

- 6 单击**确定**。
- 7 部署对驱动程序集的更改：
 - 7a 右键单击**驱动程序集**。
 - 7b 选择**在线 > 部署**。
 - 7c 选择**部署**。
- 8 重新启动身份库。

11.2 安装后配置身份库

在安装身份库后，您可以使用 `ndsconfig` 实用程序来配置目录，并使用 `ndsmanage` 实用程序来创建、启动和停止服务器实例。如果您的服务器已支持 IPv6 地址，则还可以将身份库配置为使用 IPv6 地址。

11.2.1 使用 `ndsconfig` 实用程序修改 eDirectory 树和复本服务器

安装身份库之后，您便可使用 `ndsconfig` 实用程序来配置身份库。要使用 `ndsconfig` 实用程序，您必须具有管理员权限。当您结合自变量使用此实用程序时，它会验证所有自变量，并提示输入具有管理员权限的用户的口令。如果您不结合自变量使用该实用程序，`ndsconfig` 将显示实用程序及可用选项的说明。

您还可以使用此实用程序去除 eDirectory 复本服务器以及更改 eDirectory 服务器的当前配置。有关详细信息，请参见第 11.2 章“安装后配置身份库”（第 98 页）。

在使用 `ndsconfig` 实用程序时，请注意以下事项：

- ◆ `treename`、`admin_FDN` 和 `server_FDN` 变量允许的最大字符数如下：
 - ◆ `treename`：32 个字符
 - ◆ `admin_FDN`：255 个字符
 - ◆ `server_FDN`：255 个字符
- ◆ 当您在现有树中添加服务器时，如果指定的环境在服务器对象中不存在，则 `ndsconfig` 实用程序将在添加该服务器时创建相应环境。
- ◆ 您可以在安装身份库后向现有树添加 LDAP 和安全服务。
- ◆ 要在服务器中启用加密复制，请在用于向现有树添加服务器的命令中包含 `-E` 选项。有关加密复制的详细信息，请参见《[NetIQ eDirectory Administration Guide](#)》（NetIQ eDirectory 管理指南）中的“[Encrypted Replication](#)”（加密复制）。

有关使用 `ndsconfig` 实用程序修改 eDirectory 的详细信息，请参见《[NetIQ eDirectory Administration Guide](#)》（NetIQ eDirectory 管理指南）。

了解 ndsconfig 实用程序参数

ndsconfig 实用程序支持以下参数：

new

创建新树。如果未在命令行中指定参数，该实用程序将提示您为每个缺少的参数输入值。

def

创建新树。如果未在命令行中指定参数，ndsconfig 将为每个缺少的参数应用默认值。

add

将服务器添加到现有树中。此外，在您配置现有树中的身份库后，还会添加 LDAP 和 SAS 服务。

rm

从树中去除服务器对象和目录服务。

注释：此选项不会去除密钥材料对象。您必须手动去除这些对象。

upgrade

将 eDirectory 升级到更高的版本。

-i

指示实用程序在您配置新树时忽略同名树检查。允许存在多个同名的树。

-t *treename*

指定要将服务器添加到的树的名称。该名称最多可包含 32 个字符。如果未指定树名，ndsconfig 将从 /etc/opt/novell/eDirectory/conf/nds.conf 文件中指定的 n4u.nds.treename 参数中获得该名称。默认树名为 \$LOGNAME-\$HOSTNAME-NDStree。

-n *server_context*

指定要在其中添加服务器对象的服务器环境。最多可包含 64 个字符。如果未指定环境，ndsconfig 将从 /etc/opt/novell/eDirectory/conf/nds.conf 文件中指定的 n4u.nds.server-context 配置参数中获得环境。应以键入的形式指定服务器环境。默认环境为 org。

-d *path_for_DIB*

指定要储存数据库文件的目录路径。

-r

不管已将多少个服务器添加到该服务器，都会强制添加该服务器的复本。

-L *ldap_port*

指定 LDAP 服务器上的 TCP 端口号。如果默认端口 389 已被占用，该实用程序会提示您指定一个新端口。

-l *ssl_port*

指定 LDAP 服务器上的 SSL 端口号。如果默认端口 636 已被占用，该实用程序会提示您指定一个新端口。

-a *admin_FDN*

指定对要在其中创建服务器对象和目录服务的环境具有主管权限的用户对象的完全判别名。应以键入的形式指定 admin 名称。最多可包含 64 个字符。默认值为 admin.org。

-e

为 LDAP 对象启用明文口令。

-m *module_name*

指定要安装或配置的模块的名称。如果您正在配置新树，则只能指定 ds 模块。在配置 ds 模块后，可以使用 add 命令添加 NMAS、LDAP、SAS、SNMP、HTTP 服务和 NetIQ SecretStore (ss)。如果未指定模块名称，则会安装所有模块。

注释：如果您不希望在通过 nds-install 命令升级 eDirectory 期间配置 SecretStore，请向此选项传递 no_ss 值。例如，输入 ndsinstall '-m no_ss'。

-o

指定 HTTP 明文端口号。

-O

指定 HTTP 安全端口号。

-p *IP_address:[port]*

指定远程主机的 IP 地址，该远程主机用于托管此服务器要添加到的分区的复本。在向树中添加二级服务器（使用 add 命令）时，请使用此选项。默认端口号是 524。这可以避免 SLP 查找，有助于加快树的查找速度。

-R

将服务器所要添加到的分区复制到本地服务器。此选项会禁止将复本添加到本地服务器。

-c

防止在执行 ndsconfig 操作期间出现提示，例如，提示是否要继续操作，或者在发生冲突时提示重新输入端口号，等等。如果未在命令行上传递强制参数，该实用程序会继续提示您输入这些参数。

-w *admin_password*

此选项允许以明文格式传递管理员用户口令。

注释：NetIQ 不建议在关注口令安全性的环境中使用此选项。

-E

对您在尝试添加的服务器启用加密复制。

-j

指示实用程序在安装身份库之前跳过或覆盖运行状况检查选项。

-b *port_to_bind*

指定特定实例要在其上侦听的默认端口号。这会设置 n4u.server.tcp-port 和 n4u.server.udp-port 上的默认端口号。如果您使用 -b 选项指定了 NCP 端口，则实用程序会假设该端口是默认端口，并相应地更新 TCP 和 UDP 参数。

注释：-b 和 -B 选项是互斥参数。

-B interface1@port1,interface2@port2,...

指定端口号以及 IP 地址或接口。例如：-B eth0@524、-B 100.1.1.2@524、-B[2015::3]@524。

注释：

- ◆ -b 和 -B 选项是互斥参数。
 - ◆ 要指定 IPv6 地址，必须将地址包含在方括号 ([]) 中。
-

--config-file configuration_file

指定用于储存 nds.conf 配置文件的绝对路径和文件名。例如，要在 /etc/opt/novell/eDirectory/directory 中储存配置文件，请输入以下命令：

```
--config-file /etc/opt/novell/eDirectory/nds.conf
```

-P LDAP_URL(s)

允许 LDAP URL 配置 LDAP 服务器对象上的 LDAP 接口。使用逗号分隔多个 URL。例如：

```
-P ldap://1.2.3.4:389,ldaps://1.2.3.4:636,ldap://[2015::3]:389
```

注释：

- ◆ 要指定 IPv6 地址，必须将地址包含在方括号 ([]) 中。例如：ldap://[2015::3]:389。
 - ◆ 如果在执行初始配置时未指定 LDAP URL，您可以在完成初始配置后使用 ldapconfig 命令或在 iManager 中将其添加到 ldapInterfaces 属性。
-

-D path_for_data

在指定的路径中创建 data、dib 和 log 目录。

set valuelist

设置您为身份库指定的可配置参数的值。在配置树之前，可以使用此选项设置引导参数。

更改配置参数后，必须重新启动 ndsd 才能使新值生效。对于以下配置参数，无需重新启动 ndsd：

- ◆ n4u.nds.inactivity-synchronization-interval
- ◆ n4u.nds.synchronization-restrictions
- ◆ n4u.nds.janitor-interval
- ◆ n4u.nds.backlink-interval
- ◆ n4u.nds.drl-interval
- ◆ n4u.nds.flatcleaning-interval
- ◆ n4u.nds.server-state-up-threshold
- ◆ n4u.nds.heartbeat-schema
- ◆ n4u.nds.heartbeat-data

get help paramlist

显示您为身份库指定的可配置参数的帮助字符串。如果您未指定参数列表，该实用程序将列出所有可配置参数的帮助字符串。

在特定的区域设置中配置身份库

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

```
export LC_ALL=ja
```

```
export LANG=ja
```

在身份库中添加新树

当您在身份库中创建新树时，ndsconfig 实用程序可以引导您完成配置，或者，您也可以输入一条命令来指定所有参数值。如果您的身份库服务器已支持 IPv6 地址，则可以为新树指定 IPv6 地址。

- 1 （视情况而定）要让 ndsconfig 实用程序提示您为身份库中的新树指定参数，请输入以下命令：

```
ndsconfig new [-t tree_name] [-n server_context] [-a admin_FDN]
```

例如：

```
ndsconfig new -t corp-tree -n o=company -a cn=admin.o=company
```

- 2 （视情况而定）要通过在命令行中指定所有参数的方式在身份库中创建新树，请输入以下文本：

```
ndsconfig new [-t treename] [-n server_context] [-a admin_FDN] [-i] [-S server_name] [-d path_for_dib] [-m module] [e] [-L ldap_port] [-l SSL_port] [-o http_port] [-O https_port] [-p IP_address:[port]] [-R] [-c] [-w admin_password] [-b port_to_bind] [-B interface1@port1,interface2@port2,...] [-D custom_location] [--config-file configuration_file]
```

或者

```
ndsconfig def [-t treename] [-n server_context] [-a admin_FDN] [-w admin_password] [-c] [-i] [-S server_name] [-d path_for_dib] [-m module] [-e] [-L ldap_port] [-l SSL_port] [-o http_port] [-O https_port] [-D custom_location] [--config-file configuration_file]
```

在现有树中添加服务器

要将服务器添加到现有树中，请输入以下命令：

```
ndsconfig add [-t treename] [-n server context] [-a admin_FDN] [-i] [-S server_name] [-d path_for_dib] [-m module] [e] [-L ldap_port] [-l SSL_port] [-o http_port] [-O https_port] [-p IP_address:[port]] [-R] [-c] [-w admin_password] [-b port_to_bind] [-B interface1@port1,interface2@port2,...] [-D custom_location] [--config-file configuration_file]
```

例如：

```
ndsconfig add -t corp-tree -n o=company -a cn=admin.o=company -S srv1
```

从服务器中去除身份库及其数据库

- 1 浏览到默认位于 /var/opt/novell/eDirectory/data/ 中的 dsreports 目录。
- 2 删除您先前使用 iMonitor 创建的 HTML 文件。
- 3 使用 ndsconfig 实用程序输入以下命令：

```
ndsconfig rm [-a admin_FDN] [-w admin_password] [-p IP_address:[port]] [-c]
```

从树中去除 eDirectory 服务器对象和目录服务

要从树中去除 服务器对象和目录服务，输入以下命令：

```
ndsconfig rm -a Admin_FDN
```

配置身份库的多个实例

您可以在一个主机上配置身份库的多个实例。使用 ndsconfig 实用程序配置多个实例的方法类似于数次配置单个实例。每个实例应具有唯一的实例符，如下所示：

- ◆ 不同的数据和日志文件位置。使用 --config-file、-d 和 -D 选项。
- ◆ 实例要侦听的唯一端口号。使用 -b 和 -B 选项。
- ◆ 实例的唯一服务器名称。使用 -S *server name* 选项。

有关详细信息，请参见《[NetIQ eDirectory Installation Guide](#)》（NetIQ eDirectory 安装指南）中的“[Using ndsconfig to Configure Multiple Instances of eDirectory](#)”（使用 ndsconfig 配置 eDirectory 的多个实例）。

注释：

- ◆ 在配置身份库期间，默认的 NCP 服务器名称将设置为主机服务器名称。在配置多个实例时，您必须更改 NCP 服务器名称。使用 ndsconfig 命令行选项 -S *server_name* 可以指定其他服务器名称。在相同或不同的树上配置多个实例时，NCP 服务器名称应是唯一的。
 - ◆ 所有实例共享同一个服务器密钥 (NICI)。
-

11.2.2 使用 ndsmanage 实用程序管理实例

使用 ndsmanage 实用程序可以创建、启动和停止身份库中的服务器实例。还可以查看已配置实例的列表。

列出身份库实例

您可以使用 ndsmanage 实用程序来查看配置文件路径、服务器实例的完全判别名和端口，以及指定用户的实例状态（活动或非活动）。该实用程序支持以下参数：

ndsmanage

列出您配置的所有实例。

ndsmanage -a|--all

列出使用身份库特定安装的所有用户的实例。

ndsmanage *username*

列出由指定用户配置的实例。

在身份库中创建新实例

- 1 在命令行中，输入 ndsmanage。
- 2 输入 c。
- 3 遵循命令提示符上的说明创建新实例。

在身份库中配置和取消配置实例

要配置实例，请输入以下命令：

```
ndsconfig new -t treename -n server_context -a admin_FDN -b port_to_bind -D  
path_for_data
```

例如：

```
ndsconfig new -t mytree -n o=netiq -a cn=admin.o=company -b 1524 -D  
/home/mary/inst1/var --config-file /home/mary/inst1/nds.conf
```

注释：Linux 操作系统限制在装入的文件系统上创建套接字。对于 eDirectory，NetIQ 建议将 var 目录放置在本地文件系统上（在 ndsconfig 中使用 -D 选项），而 DIB 目录可以是任何文件系统（在 ndsconfig 中使用 -d 选项）。

要取消配置某个实例，请执行以下操作：

- 1 在命令行中，输入 ndsmanage。
- 2 选择要取消配置的实例。
- 3 输入 d。

为身份库中的实例调用实用程序

您可以针对某个实例运行 DSTrace 等实用程序。例如，如果您希望对侦听端口 1524 且配置文件位于 /home/mary/inst1/nds.conf 目录、DIB 文件位于 /home/mary/inst1/var 目录的实例 1，运行 DSTrace 实用程序。则您可以输入以下命令之一：

```
ndstrace --config-file /home/mary/inst1/nds.conf
```

或者

```
ndstrace -h 192.168.0.1:1524
```

如果您未指定实例符，该实用程序将显示您的所有实例。然后，您可以选择其中一个实例。

在身份库中启动和停止实例

您可以启动或停止您所配置的一个或多个实例。

- 1（视情况而定）要通过引导式过程启动或停止单个实例，请完成以下步骤：
 - 1a 在命令行中，输入 ndsmanage。
 - 1b 选择要启动或停止的实例。
 - 1c 输入 s 或 k 可分别启动或停止该实例。
- 2（视情况而定）要启动或停止单个实例，请输入：


```
ndsmanage start --config-file configuration_file_of_the_instance
```

或者

```
ndsmanage stop --config-file configuration_file_of_the_instance
```

3（视情况而定）要启动或停止所有实例，请输入：

```
ndsmanage startall
```

或者

```
ndsmanage stopall
```

11.3 配置 Remote Loader 和驱动程序

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

在使用 Remote Loader 之前，必须将应用程序 shim 配置为安全连接到 Identity Manager 引擎。您还必须配置 Remote Loader 和 Identity Manager 驱动程序。有关 shim 的详细信息，请参见[了解 Shim](#)（第 64 页）。

- [第 11.3.1 节“创建与 Identity Manager 引擎的安全连接”](#)（第 105 页）
- [第 11.3.2 节“了解 Remote Loader 的配置参数”](#)（第 108 页）
- [第 11.3.3 节“为驱动程序实例配置 Remote Loader”](#)（第 115 页）
- [第 11.3.4 节“为驱动程序实例配置 Java Remote Loader”](#)（第 116 页）
- [第 11.3.5 节“配置 Identity Manager 驱动程序以与 Remote Loader 配合使用”](#)（第 117 页）
- [第 11.3.6 节“配置与 Identity Manager 引擎的相互鉴定”](#)（第 118 页）
- [第 11.3.7 节“校验配置”](#)（第 124 页）
- [第 11.3.8 节“启动 Remote Loader 中的驱动程序实例”](#)（第 124 页）
- [第 11.3.9 节“停止 Remote Loader 中的驱动程序实例”](#)（第 125 页）

11.3.1 创建与 Identity Manager 引擎的安全连接

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

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

了解通讯过程

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

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

- ◆ **对于本机驱动程序**（例如 Active Directory 驱动程序），请指向 base64 编码的证书。有关详细信息，请参见[管理自我签名的服务器证书](#)（第 106 页）。
- ◆ **对于 Java 驱动程序**，您必须创建密钥存储区。有关详细信息，请参见[使用 SSL 连接时创建密钥存储区文件](#)（第 107 页）。

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

管理自我签名的服务器证书

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

您可以导出新创建的证书，也可以使用现有证书。

注释：如果服务器加入树，eDirectory 将创建以下默认证书：

- ◆ SSL CertificateIP
 - ◆ SSL CertificateDNS
 - ◆ 符合 Suite B 要求的证书
-

- 1 登录到 NetIQ iManager。
- 2 要创建新证书，请完成以下步骤：
 - 2a 单击 **NetIQ 证书服务器 > 创建服务器证书**。
 - 2b 选择拥有该证书的服务器。
 - 2c 指定证书的绰号。例如：remotecert。

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

还需要记录证书绰号。此绰号将在驱动程序的远程连接参数中用作 KMO 名称。

- 2d 选择证书创建方法，然后单击**下一步**。

您可以选择以下选项：

- ◆ **标准：**该选项会使用可能的最大密钥大小创建服务器证书对象，并使用您的组织 CA 对公共密钥证书签名。

- ♦ **自定义：**此选项会使用您指定的设置创建服务器证书对象。它可让您为服务器证书对象设置一些自定义设置。选择此选项可创建 ECDSA 证书以用于 Suite B 通讯。
- ♦ **导入：**此选项会使用 PKCS12 (PFX) 文件中的密钥和证书创建服务器证书对象。您可以将该选项结合“导出”功能一起使用，以备份和恢复服务器证书或将服务器证书对象从一台服务器移至另一台服务器。

2e 指定证书参数。

2f 接受其余的证书默认值。

2g 复查摘要，单击**完成**，然后单击**关闭**。

3 要导出证书，请完成以下步骤：

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

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

3c 单击**导出**。

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

3e 从下拉菜单中选择 **BASE64 > 导出格式**。

3f 单击**下一步**。

3g 单击**保存**，然后单击**关闭**。

使用 SSL 连接时创建密钥存储区文件

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

- ♦ [在任何平台上创建密钥存储区（第 107 页）](#)
- ♦ [在 Linux 上创建密钥存储区（第 107 页）](#)

在任何平台上创建密钥存储区

要在任意平台上创建密钥存储区，可以在命令行中输入以下内容：

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

文件名可以是任意名称。例如：rdev_keystore。

在 Linux 上创建密钥存储区

在 Linux 环境中，请使用 create_keystore 文件，这是一个调用 Keytool 实用程序的外壳脚本。该文件已随 rdxml 一起安装，默认情况下位于 *install_directory/rdxml/bin* 目录中。\\dirxml\\java_remoteloader 目录下的 dirxml_jremote.tar.gz 文件中也包含了 create_keystore 文件。

在命令行中输入以下内容：

```
create_keystore self-signed_certificate_name keystorename
```

例如，键入以下任意一条内容

```
create_keystore tree-root.b64 mystore
create_keystore tree-root.der mystore
```

create_keystore 脚本指定密钥存储区口令的“dirxml”硬编码口令。由于密钥存储区中仅储存一个公共证书和一个公共密钥，因此不具有安全风险。

11.3.2 了解 Remote Loader 的配置参数

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

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

有关配置新驱动程序实例的详细信息，请参见第 11.3.3 节“为驱动程序实例配置 Remote Loader”（第 115 页）。

Remote Loader 中驱动程序实例的配置参数

您可以在命令行或配置文件中配置驱动程序实例。NetIQ 提供了 config8000.txt 示例文件，可帮助您配置要与应用程序 shim 配合使用的 Remote Loader 和驱动程序。默认情况下，该示例文件位于 /opt/novell/dirxml/doc 目录中。例如，该配置文件可能包含以下行：

```
-commandport 8000
-connection "port=8090 rootfile=/dirxmlremote/root.pem"
-module $DXML_HOME/dirxmlremote/libcskeldrv.so.0.0.0
-trace 3
```

请使用以下参数：

-description value (-desc value)

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

```
-description SAP
-desc SAP
```

-class name (-cl name)

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

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

注释：

- ◆ 如果指定了 -module 选项，则不能使用上述选项。
 - ◆ 如果使用制表符字符作为 -class 选项中的分隔符，Remote Loader 将不会自动启动，而必须由您手动启动。要让 Remote Loader 正常启动，您可以使用空格字符而不要使用制表符。
 - ◆ 有关可为此选项指定的名称的详细信息，请参见[了解 Java -class 参数的名称](#)（第 114 页）。
-

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

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

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

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

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

-config *filename*

指定驱动程序实例的配置文件。例如：

```
-config config.txt
```

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

您可以在 Remote Loader 运行时发送此命令。

-connection "*parameters*" (-conn "*parameters*")

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

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

使用以下语法输入连接字符串：

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

例如：

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

使用以下参数指定 TCP/IP 连接的设置：

address=*IP_address*

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

以下值为有效值：

- ◆ address=address number
- ◆ address='localhost'

例如：

```
address=198.51.100.0
```

如果您未指定值，Remote Loader 将侦听所有本地 IP 地址。

fromaddress=*IP_address*

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

```
fromaddress=198.51.100.0  
fromaddress=testserver1.company.com
```

handshaketimeout=milliseconds

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

```
handshaketimeout=1000
```

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

hostname=server

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

```
hostname=198.51.100.0
```

secureprotocol=TLS 版本

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

```
secureprotocol=TLSv1_2
```

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

enforceSuiteB=true/false

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

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

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

useMutualAuth=true/false

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

```
useMutualAuth=true
```

keystore=filename

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

```
keystore=keystore filename
```

通常，您可指定托管远程接口 shim 的树的证书颁发机构。

kmo=name

指定包含用于 SSL 连接的密钥和证书的密钥材料对象的密钥名称。例如：

```
kmo=remote driver cert
```

localaddress=IP_address

指定要将客户端连接套接字绑定到的 IP 地址。例如：

```
localaddress=198.51.100.0
```

port=port_number

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

rootfile=trusted certname

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

```
rootfile=trustedcert
```

通常，该文件是托管远程接口 shim 的树的证书颁发机构。

storepass=password

指定您为 keystore 参数输入的 Java 密钥存储区的口令。例如：

```
storepass=mypassword
```

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

```
keystore=keystorename storepass=password
```

-datadir directory (-dd directory)

指定 Remote Loader 使用的数据文件所在的目录。例如：

```
-datadir /var/opt/novell/dirxml/rdxml/data
```

如果您使用此命令，rdxml 进程会将其当前目录更改为指定的目录。将在此数据目录中创建不含明确的指定路径的跟踪文件和其他文件。

-help (-h)

指示应用程序显示帮助。

-java (-j)

（视情况而定）指定您想要为 Java 驱动程序 shim 实例设置口令。

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

-javadebugport port_number (-jdp port_number)

指示实例在指定的端口上启用 Java 调试。例如：

```
-javadebugport 8080
```

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

-javaparam parameters (-jp parameters)

指定 Java 环境的参数。使用以下语法输入 Java 环境参数：

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

注释：不要对 Java Remote Loader 使用此参数。

要为单个参数指定多个值，请将该参数括在引号中。例如：

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

使用以下参数设置 Java 环境：

DHOST_JVM_ADD_CLASSPATH

指定 JVM 要在其中搜索包 (.jar) 和类 (.class) 文件的其他路径。要为 Linux JVM 指定多个类路径，请在各路径之间插入一个冒号。

DHOST_JVM_INITIAL_HEAP

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

```
100M
```

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

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

DHOST_JVM_MAX_HEAP

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

```
100M
```

如果您未指定字节类型，大小默认以字节为单位。

此参数优先于驱动程序集属性选项。

DHOST_JVM_OPTIONS

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

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

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

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

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

```
-password netiq4
```

如果您在发出命令时未发送该口令，驱动程序实例将提示您提供该口令。

您可以在 Remote Loader 运行时发送此命令。

-piddir *directory* (-pd *directory*)

指定 Remote Loader 进程使用的进程 ID 文件 (pidfile) 所在目录的路径。例如：

```
-piddir /var/opt/novell/dirxml/rdxml/data
```

pidfile 主要供 SysV-style init 脚本使用。默认值为 /var/run。另外，如果 Remote Loader 由权限不足的用户（无法打开 pidfile 以在 /var/run 中进行读取和写入）运行，那么，默认值将是当前目录。

此参数类似于 -datadir。

-setpasswords Remote_Loader_pwd optional_pwd (-sp Remote_Loader_pwd optional_pwd)

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

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

```
-setpasswords Remote_Loader_password driver_object_password
```

例如：

```
-setpasswords netiq4 idmobject6
```

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

跟踪文件设置

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

在配置文件中添加以下参数：

-trace integer (-t integer)

指定要在跟踪窗口中显示的讯息级别。例如：

```
-trace 3
```

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

-tracefile filepath (-tf filepath)

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

```
-tracefile /home/trace.txt
```

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

-tracefilemax size (-tf size)

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

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

注释：

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

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

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

```
-trace 3
```

您可以在 Remote Loader 运行时发送此命令。

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

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

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

您可以在 Remote Loader 运行时发送此命令。

证书口令设置

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

-keystorepassword (-ksp)

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

-keypassword (-kp)

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

-unload (-u)

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

您可以在 Remote Loader 运行时发送此命令。

了解 Java -class 参数的名称

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

Java 类名	驱动程序
com.novell.nds.dirxml.driver.dcsshim.DCSShim	Driver for Data Collection Service
com.novell.nds.dirxml.driver.delimitedtext.DelimitedTextDriver	Delimited Text Driver
be.opns.dirxml.driver.ars.arsremedydrivershim.ARSDriverShim	修复 ARS 的驱动程序
com.novell.nds.dirxml.driver.entitlement.EntitlementServiceDriver	Entitlements Service Driver
com.novell.gw.dirxml.driver.rest.shim.GWdriverShim	GroupWise 2014 驱动程序
com.novell.idm.drivers.idprovider.IDProviderShim	ID Provider Driver
com.novell.nds.dirxml.driver.jdbc.JDBCdriverShim	JDBC 驱动程序
com.novell.nds.dirxml.driver.jms.JMSDriverShim	JMS 驱动程序
com.novell.nds.dirxml.driver.ldap.LDAPDriverShim	LDAP Driver
com.novell.nds.dirxml.driver.loopback.LoopbackDriverShim	回送驱动程序
com.novell.nds.dirxml.driver.ebs.user.EBSUserDriver	Oracle User Management Driver

Java 类名	驱动程序
com.novell.nds.dirxml.driver.ebs.hr.EBSHRDriver	Oracle HR Driver
com.novell.nds.dirxml.driver.ebs.tca.EBSTCADriver	Oracle TCA Driver
com.novell.nds.dirxml.driver.msgateway.MSGatewayDriverShim	受管系统网关驱动程序
com.novell.nds.dirxml.driver.manualtask.driver.ManualTaskDriver	手动任务驱动程序
com.novell.nds.dirxml.driver.nisdriver.NISDriverShim	NIS 驱动程序
com.novell.nds.dirxml.driver.notes.NotesDriverShim	Notes 驱动程序
com.novell.nds.dirxml.driver.psoftshim.PSOFTDriverShim	PeopleSoft 驱动程序
com.netiq.nds.dirxml.driver.pum.PUMDriverShim	Privileged User Management Driver
com.novell.nds.dirxml.driver.salesforce.SFDriverShim	Salesforce Driver
com.novell.nds.dirxml.driver.SAPHRShim.SAPDriverShim	SAP HR Driver
com.novell.nds.dirxml.driver.sap.portal.SAPPortalShim	SAP Portal Driver
com.novell.nds.dirxml.driver.sapumshim.SAPDriverShim	SAP 用户管理驱动程序
com.novell.nds.dirxml.driver.soap.SOAPDriver	SOAP 驱动程序
com.novell.idm.driver.ComposerDriverShim	User Application
com.novell.nds.dirxml.driver.workorder.WorkOrderDriverShim	WorkOrder Driver

11.3.3 为驱动程序实例配置 Remote Loader

Remote Loader 可以托管 .dll、.so 或 .jar 文件中包含的 Identity Manager 应用程序 shim。为使 Remote Loader 能够在 Linux 计算机上运行，应用程序需要每个驱动程序实例都有相应的配置文件（例如 LDAPShim.txt）。您也可以使用命令行选项创建或编辑配置文件。

默认情况下，Remote Loader 会使用 TLS/SSL 协议通过 TCP/IP 连接到 Identity Manager 引擎。此连接的默认 TCP/IP 端口为 8090。您可以在同一个服务器上运行多个驱动程序实例以配合 Remote Loader 使用。每个实例托管一个单独的 Identity Manager 应用程序 shim 实例。要在同一个服务器上使用 Remote Loader 的多个实例，请为每个实例指定不同的连接端口和命令端口。

注释：

- 配置文件可以包含除 -config 以外的任意命令行选项。
- 向配置文件中添加参数时，可以使用参数的长格式或短格式。例如，可以使用 -description 或 -desc。
- 以下过程先列出长格式，后跟以括号括住的短格式。例如，-description 值 (-desc 值)。
- 有关本节中所用参数的详细信息，请参见[了解 Remote Loader 的配置参数（第 108 页）](#)。

要创建配置文件：

- 1 在文本编辑器中创建一个新文件。

NetIQ 提供了 config8000.txt 示例文件，可帮助您配置要与应用程序 shim 配合使用的 Remote Loader 和驱动程序。默认情况下，该示例文件位于 /opt/novell/dirxml/doc 目录中。

2 将以下配置参数添加到该文件中：

- ◆ -description （可选）
- ◆ -commandport
- ◆ 连接参数：
 - ◆ port （必需）
 - ◆ address
 - ◆ fromaddress
 - ◆ handshaketimeout
 - ◆ rootfile
 - ◆ keystore
 - ◆ localaddress
 - ◆ hostname
 - ◆ kmo
 - ◆ secureprotocol
 - ◆ enforceSuiteB
 - ◆ useMutualAuth
- ◆ 跟踪文件参数 （可选）：
 - ◆ -trace
 - ◆ -tracefile
 - ◆ -tracefilemax
- ◆ -javaparam
- ◆ -class 或 -module

有关为这些参数指定值的详细信息，请参见第 11.3.2 节“了解 Remote Loader 的配置参数”（第 108 页）。

3 保存文件。

要在启动计算机时自动启动 Remote Loader，请将该文件保存到 /etc/opt/novell/dirxml/rdxml 目录。

11.3.4 为驱动程序实例配置 Java Remote Loader

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

要在 Linux 平台上配置 Java Remote Loader 的新实例，请完成以下步骤。有关本节中所用参数的详细信息，请参见了解 Remote Loader 的配置参数（第 108 页）。

1 在文本编辑器中创建一个新文件。

NetIQ 提供了 config8000.txt 示例文件，可帮助您配置要与应用程序 shim 配合使用的 Remote Loader 和驱动程序。默认情况下，该示例文件位于 /opt/novell/dirxml/doc 目录中。

2 在新配置文件中添加以下参数：

- ◆ -description （可选）
- ◆ -class 或 -module
例如：-class com.novell.nds.dirxml.driver.Ldap.LDAPDriverShim
- ◆ -commandport

- ◆ 连接参数：
 - ◆ port（必需）
 - ◆ address
 - ◆ fromaddress
 - ◆ handshaketimeout
 - ◆ rootfile
 - ◆ keystore
 - ◆ localaddress
 - ◆ hostname
 - ◆ kmo
 - ◆ secureprotocol
 - ◆ enforceSuiteB
 - ◆ useMutualAuth
- ◆ -java（视情况而定）
- ◆ -javadebugport
- ◆ -password
- ◆ -service
- ◆ -keypassword
- ◆ -keystorepassword（仅适用于 Java 驱动程序）
- ◆ 跟踪文件参数（可选）：
 - ◆ -trace
 - ◆ -tracefile
 - ◆ -tracefilemax

3 保存新的配置文件。

要让 Remote Loader 在计算机启动时自动启动，请将该文件保存到 `/etc/opt/novell/dirxml/jremote` 目录。

4 打开命令提示符。

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

```
dirxml_jremote -config filename
```

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

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

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

要在 Designer 或 iManager 中添加新驱动程序对象或修改现有驱动程序对象，必须配置用于启用 Remote Loader 驱动程序实例的设置。有关本节中所用参数的详细信息，请参见[了解 Remote Loader 的配置参数（第 108 页）](#)。

- 1 在概述中，选择 Identity Manager 驱动程序对象。
- 2 在驱动程序对象的属性中，完成以下步骤：
 - 2a 对于驱动程序模块，请选择[连接到 Remote Loader](#)。
 - 2b 对于驱动程序对象口令，请指定 Remote Loader 用于对 Identity Manager 引擎服务器鉴定自身的口令。
此口令必须与 Remote Loader 中定义的驱动程序对象口令相匹配。
 - 2c 对于 [Remote Loader 连接参数](#)，请指定连接到 Remote Loader 所需的信息。使用以下语法：

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

其中

hostname

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

port

指定 Remote Loader 侦听的端口。默认端口为 8090。

kmo

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

localaddress

如果在托管 Identity Manager 引擎的服务器上配置了多个 IP 地址，请指定源 IP 地址。
 - 2d 对于 [Remote Loader 口令](#)，请指定 Identity Manager 引擎（或 Remote Loader shim）用于鉴定到 Remote Loader 所需的口令。
- 3 定义一个具有同等安全性的用户。
- 4 单击“下一步”，然后单击“完成”。

11.3.6 配置与 Identity Manager 引擎的相互鉴定

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

要配置相互鉴定，请执行以下任务：

- ◆ [导出 Identity Manager 引擎和 Remote Loader 的证书（第 119 页）](#)
- ◆ [启用驱动程序以进行相互鉴定（第 121 页）](#)

导出 Identity Manager 引擎和 Remote Loader 的证书

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

- ♦ [从 eDirectory 导出证书（第 119 页）](#)
- ♦ [为 Remote Loader 导出第三方证书（第 120 页）](#)

从 eDirectory 导出证书

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

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

创建 KMO

要创建服务器 KMO，请执行以下操作：

- 1 登录到 NetIQ iManager。
- 2 在左侧窗格中单击 **NetIQ 证书服务器**，然后选择服务器证书。
- 3 选择拥有您所创建证书的服务器。
- 4 指定证书的绰号。例如，serverkmo。
- 5 在证书创建方法中选择**标准**，然后单击**下一步**。
- 6 复查摘要，单击**完成**，然后单击**关闭**。

要创建客户端 KMO，请执行以下操作：

- 1 登录到 NetIQ iManager。
- 2 在左侧窗格中单击 **NetIQ 证书服务器**，然后选择服务器证书。
- 3 选择拥有您所创建证书的服务器。
- 4 指定证书的绰号。例如，clientkmo
- 5 在证书创建方法中选择**自定义**，然后单击**下一步**。
- 6 将默认的组织证书颁发机构保留不变，然后单击**下一步**。
- 7 取消选择**启用扩展密钥使用**，然后单击**下一步**。
- 8 接受其余的证书默认值。
- 9 复查摘要，单击**完成**，然后单击**关闭**。

导出 KMO

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

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

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

其中

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

例如， `dxcmd -user admin.sa.system -password novell -exportcerts serverkmo server java '/home/certs'`

此命令会在 `/home/certs/` 目录中生成 `serverkmo_server.ks` 文件。密钥存储区的默认口令为 `dirxml`。

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

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

使用以下语法运行命令：

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

表 11-1 不同类型驱动程序的示例

驱动程序类型	命令	输出
Java 驱动程序	<code>dxcmd -dnform ldap -host 192.168.0.1 -user cn=admin,ou=sa,o=system -password novell -exportcerts clientkmo client java '/home/certs'</code>	<code>/home/certs/</code> 目录中的 <code>clientkmo_client.ks</code> 文件 密钥存储区的默认口令为 <code>dirxml</code> 。

为 Remote Loader 导出第三方证书

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

Java 驱动程序

从 `.pfx` 文件创建 Java 密钥存储区。输入诸如 `keytool -importkeystore -srckeystore servercert.pfx -srcstoretype pkcs12 -destkeystore servercert.jks -deststoretype JKS` 的命令。

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

启用驱动程序以进行相互鉴定

要启用驱动程序通讯以进行相互鉴定，请执行以下任务：

- 使用 [KMO 或密钥存储区配置驱动程序](#)（第 121 页）
- [为驱动程序实例配置 Remote Loader](#)（第 123 页）

使用 KMO 或密钥存储区配置驱动程序

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

在 Designer 中，您可以在初始驱动程序创建过程中配置驱动程序，也可以在创建驱动程序之后再配置。

要在 Designer 中配置驱动程序，请执行以下操作：

- 1 在 Designer 中打开您的项目。
- 2 在“建模器”视图的面板中，选择您要创建的驱动程序。
- 3 将驱动程序的图标拖到“建模器”视图上。
- 4 遵循安装向导中的步骤操作。
- 5 在“Remote Loader”窗口中，选择是。
 - 5a **主机名**：指定用于运行驱动程序 Remote Loader 服务的服务器的主机名或 IP 地址。例如，输入 hostname=192.168.0.1。如果未为此参数指定值，则该值默认为 localhost。
 - 5b **端口**：指定用于为此驱动程序安装和运行 Remote Loader 的端口号。默认端口号为 8090。
 - 5c **KMO**：指定包含 Remote Loader 用于 SSL 连接的密钥和证书的 KMO 密钥名称。例如，输入 kmo=serverkmo。如果您要配置使用 KMO 进行的相互鉴定，则必须为此参数指定值。您还需要在“其他参数”部分指定根文件参数的值。
 - 5d **其他参数**：指定您要使用的 Remote Loader 的设置。可以在此参数中包括有关相互鉴定通讯的信息。指定的所有参数都必须使用键值对格式，如下所示：paraName1=paraValue1
paraName2=paraValue2
例如，对于密钥存储区，请使用以下语法：
UseMutualAuth=true keystore='/home/certs/serverkmo_server.ks' storepass='dirxml' keypass='dirxml'
key='serverkmo'
例如，对于 KMO，请使用以下语法：
useMutualAuth=true rootFile='/home/cacert.b64'
 - 5e **远程口令**：指定 Remote Loader 口令。
 - 5f **驱动程序口令**：指定驱动程序口令。
- 6 单击下一步。
- 7 按照向导中的其余说明操作，直到完成驱动程序的安装。
- 8 复查为了创建驱动程序将要完成的任务摘要，然后单击完成。

或者，您可以在创建驱动程序之后，通过执行以下步骤来配置驱动程序：

- 1 在 Designer 的“概要”视图中，右键单击驱动程序。
- 2 选择属性。
- 3 在导航窗格中，选择[驱动程序配置](#)。

4 选择鉴定。

5 在 **Remote Loader 鉴定** 部分下，指定配置 Remote Loader 与 Identity Manager 引擎间的相互鉴定所需的信息。

对于 KOM，请使用以下语法：

```
hostname=xxx.xxx.xxx.xxx port=xxxx useMutualAuth=true kmo=certificatename  
rootFile=<absolute path to the file>
```

例如：

```
hostname=192.168.0.1 port=8090 useMutualAuth=true kmo=serverkmo rootFile='/home/cacert.b64'
```

对于密钥存储区，请使用以下语法：

```
hostname=xxx.xxx.xxx.xxx port=xxxx useMutualAuth=true keystore=<absolute path to the keystore file> storepass=<keystore password> key=<alias name> keypass=<password for the key>
```

例如：

```
hostname=192.168.0.1 port=8097 useMutualAuth=true keystore='/home/certs/serverkmo_server.ks' storepass='dirxml' key='serverkmo' keypass='dirxml'
```

要在 iManager 中修改配置，请执行以下操作：

1 起动 iManager。

2 在概述中，选择 Identity Manager 驱动程序对象。

3 在驱动程序对象的属性中，完成以下步骤：

3a 对于驱动程序模块，请选择**连接到 Remote Loader**。

3b 对于驱动程序对象口令，请指定 Remote Loader 用于向引擎鉴定的口令。

此口令必须与 Remote Loader 中定义的驱动程序对象口令相匹配。

3c 对于 **Remote Loader 连接参数**，请指定连接到 Remote Loader 所需的信息。

对于 KOM，请使用以下语法：

```
hostname=xxx.xxx.xxx.xxx port=xxxx useMutualAuth=true kmo=certificatename  
rootFile=<absolute path to the file>
```

例如：

```
hostname=192.168.0.1 port=8090 useMutualAuth=true kmo=serverkmo rootFile='/home/cacert.b64'
```

对于密钥存储区，请使用以下语法：

```
hostname=xxx.xxx.xxx.xxx port=xxxx useMutualAuth=true keystore=<absolute path to the keystore file> storepass=<keystore password> key=<alias name> keypass=<password for the key>
```

例如：

```
hostname=192.168.0.1 port=8097 useMutualAuth=true keystore='/home/certs/serverkmo_server.ks' storepass='dirxml' key='serverkmo' keypass='dirxml'
```

3d (可选) 对于 **Remote Loader 口令**, 请指定 Identity Manager 引擎 (或 Remote Loader shim) 鉴定到 Remote Loader 所需的口令。

3e 单击**应用**, 然后单击**确定**。

为驱动程序实例配置 Remote Loader

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

修改驱动程序的 Remote Loader 配置文件, 以包括用于启用相互鉴定的内容。该文件位于 /opt/novell/dirxml/doc 目录中。

要修改配置, 请执行以下操作:

1 登录安装了驱动程序和 Remote Loader 的服务器。

2 停止 Remote Loader。

例如, 输入以下命令:

```
rdxml -config /home/drivershim.conf -u
```

3 根据 Remote Loader 类型提供密钥存储区或密钥口令:

Java Remote Loader:

使用以下语法指定密钥存储区口令和密钥口令的组合:

```
dirxml_jremote -config /home/drivershim.conf -ksp <keystorepassword> -kp  
<keypassword>
```

例如:

```
dirxml_jremote -config /home/drivershim.conf -ksp dirxml -kp dirxml
```

本机 Remote Loader:

使用以下语法指定密钥口令:

```
dirxml_jremote -config /home/drivershim.conf -kp <keypassword>
```

例如:

```
dirxml_jremote -config /home/drivershim.conf -kp dirxml
```

4 在文本编辑器中打开驱动程序的 Remote Loader 配置文件。

5 在该文件中添加启用相互鉴定所需的内容。

◆ 例如, 对于 Java 驱动程序, 请添加以下条目:

```
-connection "port=8090 useMutualAuth=true keystore='/home/certs/  
clientkmo_client.ks' key='clientkmo'
```

◆ 例如, 对于本机驱动程序, 请添加以下条目:

```
-connection "useMutualAuth=true port=8090 rootfile='/home/certs/  
trustedcert.b64' certfile='/home/certs/clientkmo_clientcert.pem'  
keyfile='/home/certs/clientkmo_clientkey.pem' certform=PEM keyform=PEM"
```

6 保存并关闭文件。

7 重新启动驱动程序。

11.3.7 校验配置

1. 启动 Remote Loader。例如：

```
dirxml_remote -config config.txt
```

2. 使用 iManager 启动远程接口 shim。
3. 确认 Remote Loader 可正常工作。
4. 停止 Remote Loader。例如：

```
dirxml_remote -config config.txt -u
```

11.3.8 启动 Remote Loader 中的驱动程序实例

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

NetIQ 可让您以两种方式启动 Remote Loader 的驱动程序实例：

- ♦ [自动启动驱动程序实例（第 124 页）](#)
- ♦ [使用命令行启动驱动程序实例（第 124 页）](#)

自动启动驱动程序实例

您可以将 Remote Loader 的驱动程序实例配置为在启动计算机时自动启动。请将您的配置文件放置在 `/etc/opt/novell/dirxml/rdxml` 目录中。

使用命令行启动驱动程序实例

对于 Remote Loader，二进制组件 `rdxml` 支持命令行功能。默认情况下，此组件位于 `/usr/bin/` 目录中。

- 1 打开命令提示符。
- 2 （视情况而定）要指定用于向 Identity Manager 引擎鉴定驱动程序实例的口令，请输入以下命令之一：
 - ♦ **Remote Loader:** `rdxml -config filename -keystorepassword <keystore pass> -keypassword <key pass>`
 - ♦ **Java Remote Loader:** `dirxml_jremote -config filename -keystorepassword <keystore pass> -keypassword <key pass>`
- 3 （视情况而定）如果在 Remote Loader 的驱动程序实例与 Identity Manager 引擎之间启用了相互鉴定，请输入以下命令之一来指定证书口令：
 - ♦ **Remote Loader:** `rdxml -config filename -keystorepassword <keystore pass> -keypassword <key pass>`
 - ♦ **Java Remote Loader:** `dirxml_jremote -config filename -keypassword <key pass>`
- 4 要启动驱动程序实例，请输入以下命令：

```
rdxml -config 文件名
```
- 5 登录到 iManager，然后启动驱动程序。
- 6 确认 Remote Loader 可正常工作。

使用 `ps` 命令或跟踪文件确定命令和连接端口是否正在侦听。

仅当 Remote Loader 正在与 Identity Manager 引擎服务器上的远程接口 shim 通讯时，Remote Loader 才会装载 Identity Manager 应用程序 shim。这意味着，如果 Remote Loader 与服务器的通讯断开，应用程序 shim 将会关闭。

11.3.9 停止 Remote Loader 中的驱动程序实例

每个平台提供了不同的方法用于停止 Remote Loader 中的驱动程序实例。

注释：

- 如果运行了 Remote Loader 的多个实例，请包含 `-cp command port` 选项，以确保 Remote Loader 能够停止相应的实例。
 - 要想停止驱动程序实例，您必须拥有足够的权限或指定 Remote Loader 口令。您拥有停止它的足够权限。您输入了一个口令，但意识到该口令并不正确。此时，Remote Loader 仍会停止，因为 Remote Loader 实际上并不“接受”口令，而是会忽略口令。原因是在这种情况下，口令是多余的。如果远程装载程序是作为应用程序运行，而不是作为服务运行的，则可以使用此口令。
-

要停止某个驱动程序实例，请执行以下操作：

Remote Loader

输入 `rdxml -config filename -u` 命令。例如：

```
rdxml -config config.txt -u
```

Java Remote Loader

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

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

11.4 配置 Identity Applications 的身份库

Identity Applications 必须能够与身份库中的对象交互。

为了提高 Identity Applications 的性能，eDirectory 管理员应为 `manager`、`ismanager` 和 `srvprvUUID` 属性创建值索引。如果这些属性没有值索引，Identity Applications 用户可能会遭遇性能不佳的状况，这在群集环境中尤为突出。

通过在 RBPM 配置实用程序中选择“高级”>“创建 eDirectory 索引”，即可在安装期间自动创建这些值索引。有关使用 Index Manager 创建值索引的详细信息，请参见《[NetIQ eDirectory Administration Guide](#)》（NetIQ eDirectory 管理指南）。

11.5 为群集配置 User Application 驱动程序

在群集环境中，可以将单个 User Application 驱动程序与多个 User Application 实例搭配使用。驱动程序存储特定于应用程序的各种信息（例如工作流程配置和群集信息）。必须将驱动程序配置为使用群集的发送程序或负载平衡器的主机名或 IP 地址。

- 1 登录管理身份库的 iManager 实例。
- 2 在导航框架中，选择 **Identity Manager**。
- 3 选择 **Identity Manager 概述**。
- 4 使用搜索页面显示“Identity Manager 概述”，以了解包含 User Application 驱动程序的驱动程序集。
- 5 单击驱动程序图标右上角的圆形状态指示器：
- 6 选择**编辑属性**。
- 7 对于**驱动程序参数**，请将**主机**更改为发送程序的主机名或 IP 地址。
- 8 单击**确定**。

11.6 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.sh) 的文件位于 /opt/netiq/idm/apps/configupdate 目录中：

注释：

- ◆ 您应该只从 configupdate 目录运行 configupdate.sh。从自定义位置运行 configupdate.sh 将导致失败。
 - ◆ 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。

- ◆ [第 11.6.1 节“运行 Identity Applications 配置实用程序”](#)（第 126 页）
- ◆ [第 11.6.2 节“用户应用程序参数”](#)（第 127 页）
- ◆ [第 11.6.3 节“报告参数”](#)（第 136 页）
- ◆ [第 11.6.4 节“鉴定参数”](#)（第 137 页）
- ◆ [第 11.6.5 节“SSO 客户端参数”](#)（第 140 页）
- ◆ [第 11.6.6 节“CEF 审计参数”](#)（第 144 页）

11.6.1 运行 Identity Applications 配置实用程序

- 1 在 configupdate.sh.properties 中，确保以下选项已正确配置：

```
edit_admin="true"
```

```
use_console="false"
```

注释： 仅当您要以控制台模式运行该实用程序时，才应将 `-use_console` 的值配置为 `true`。

2 保存并关闭 `configupdate.sh`。

3 在命令提示符处，执行以下命令运行配置实用程序：

```
./configupdate.sh
```

注释： 您可能需要等待几分钟，让实用程序启动。

11.6.2 用户应用程序参数

在配置 Identity Applications 时，此选项卡用于定义应用程序在与身份库通讯时所使用的值。某些设置对于完成安装过程必不可少。

默认情况下，该选项卡会显示基本选项。要查看所有设置，请单击[显示高级选项](#)。此选项卡包括以下设置组：

- ◆ [身份库设置](#)（第 127 页）
- ◆ [身份库 DN](#)（第 128 页）
- ◆ [身份库用户身份](#)（第 130 页）
- ◆ [身份库用户组](#)（第 131 页）
- ◆ [身份库证书](#)（第 132 页）
- ◆ [电子邮件服务器配置](#)（第 132 页）
- ◆ [可信密钥储存区](#)（第 134 页）
- ◆ [NetIQ Sentinel 数字签名证书和密钥](#)（第 134 页）
- ◆ [杂项](#)（第 134 页）
- ◆ [容器对象](#)（第 135 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.sh 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.sh 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.sh 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.sh 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.sh 文件更改此设置。

组容器范围

指定身份库用户在搜索组容器时可深入的范围。

组对象类

指定 LDAP 组的对象类。通常，该类为 groupofNames。

组成员资格属性

（可选）指定用户的组成员资格。不要在该名称中使用空格。

使用动态组

指定是否要使用动态组。

您还必须指定[动态组对象类](#)的值。

动态组对象类

仅当您选择了[使用动态组](#)时才适用。

指定 LDAP 动态组的对象类。通常，该类为 dynamicGroup。

身份库证书

这组设置定义了 JRE 密钥存储区的路径和口令。某些设置对于完成安装过程必不可少。

密钥储存区路径

必需

指定 Tomcat 在运行时要使用的 JRE 密钥存储区 (cacerts) 文件的完整路径。您可以手动输入路径，也可以浏览到 cacerts 文件。对于此设置，请注意以下事项：

- ♦ 在环境中，必须指定 RBPM 的安装目录。默认值设置的即为正确位置。
- ♦ Identity Applications 的安装程序将修改密钥存储区文件。在 Linux 上，用户必须有权写入此文件。

密钥储存区口令

必需

提供密钥存储区文件的口令。默认值为 changeit。

电子邮件服务器配置

本节定义用于启用电子邮件通知的值，您可以使用电子邮件通知来进行基于电子邮件的审批。有关详细信息，请参见《[NetIQ Identity Manager - Administrator's Guide to the Identity Applications](#)》（NetIQ Identity Manager - Identity Applications 管理员指南）中的“[Enabling Support for Digital Signatures](#)”（启用数字签名支持），及 *Identity Applications 帮助* 中的“管理通过电子邮件进行的审批”。

通知模板主机

指定托管 Identity Applications 的 Tomcat 的名称或 IP 地址。例如：myapplication serverServer。

此值将替换电子邮件模板中的 \$HOST\$ 令牌。安装程序将使用此信息来创建供应请求任务和批准通知的 URL。

通知模板端口

指定托管 Identity Applications 的 Tomcat 的端口号。

此值将替换供应请求任务和批准通知中使用的电子邮件模板内的 \$PORT\$ 标记。

通知模板安全端口

指定托管 Identity Applications 的 Tomcat 的安全端口号。

此值将替换供应请求任务和批准通知中使用的电子邮件模板内的 \$SECURE_PORT\$ 标记。

通知模板协议

指定在发送用户电子邮件时要包含在 URL 中的非安全协议。例如：http。

此值将替换供应请求任务和批准通知中使用的电子邮件模板内的 \$PROTOCOL\$ 标记。

通知模板安全协议

指定在发送用户电子邮件时要包含在 URL 中的安全协议。例如：https。

此值将替换供应请求任务和批准通知中使用的电子邮件模板内的 \$SECURE_PROTOCOL\$ 标记。

通知 SMTP 电子邮件发件人

指定 Identity Applications 用来发送电子邮件通知的电子邮件帐户。

SMTP 服务器名称

指定 Identity Applications 用于供应电子邮件的 SMTP 电子邮件主机的 IP 地址或 DNS 名称。请不要使用 localhost。

服务器需要鉴定

指定您是否希望服务器要求鉴定。

您还必须指定电子邮件服务器的身份凭证。

用户名

仅当您启用了服务器需要鉴定时才适用。

指定电子邮件服务器的登录帐户名。

口令

仅当您启用了服务器需要鉴定时才适用。

指定邮件服务器的登录帐户口令。

使用 SMTP TLS

指定在邮件服务器之间进行传输期间，是否要保护电子邮件内容的安全。

电子邮件通知图像位置

指定要在电子邮件通知中包含的图像的路径。例如：<http://localhost:8080/IDMProv/images>。

对电子邮件签名

指定是否要在寄出的邮件中添加数字签名。

如果启用此选项，则还必须指定密钥存储区和签名密钥的设置。

密钥存储区路径

仅当您启用了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，`/opt/netiq/idm/apps/jre/lib/security/cacerts`。

密钥存储区口令

仅当您启用了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

仅当您创建或删除身份库索引时才适用。

指定要在其中创建或删除索引的 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。

11.6.3 报告参数

在配置 Identity Applications 时，此选项卡定义用于管理 Identity Reporting 的值。当您安装 Identity Reporting 时，实用程序将添加此选项卡。

默认情况下，该选项卡会显示基本选项。要查看所有设置，请单击[显示高级选项](#)。此选项卡包括以下设置组：

- ♦ [电子邮件递送配置](#)（第 136 页）
- ♦ [报告保留值](#)（第 137 页）
- ♦ [修改区域设置](#)（第 137 页）
- ♦ [角色配置](#)（第 137 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: /opt/netiq/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

11.6.4 鉴定参数

在配置 Identity Applications 时, 此选项卡定义 Tomcat 用于将用户定向到 Identity Applications 和口令管理页面的值。

默认情况下, 该选项卡会显示基本选项。要查看所有设置, 请单击[显示高级选项](#)。此选项卡包括以下设置组:

- ◆ [鉴定服务器](#) (第 137 页)
- ◆ [鉴定配置](#) (第 138 页)
- ◆ [身份验证方法](#) (第 138 页)
- ◆ [口令管理](#) (第 139 页)
- ◆ [Sentinel 数字签名证书和密钥](#) (第 140 页)

鉴定服务器

这组设置定义了 Identity Applications 连接鉴定服务器时使用的设置。

OAuth 服务器主机标识符

必需

指定向 OSP 颁发令牌的鉴定服务器的相对 URL。例如, 192.168.0.1。

OAuth 服务器 TCP 端口

指定鉴定服务器的端口。

OAuth 服务器正在使用 TLS/SSL

指定鉴定服务器是否使用 TLS/SSL 协议进行通讯。

可选 TLS/SSL 可信证书存储区文件

仅当您选择了 OAuth 服务器正在使用 TLS/SSL，并且实用程序显示高级选项时才适用。

可选 TLS/SSL 可信证书存储区口令

仅当您选择了 OAuth 服务器正在使用 TLS/SSL，并且实用程序显示高级选项时才适用。

指定用于装载 TLS/SSL 鉴定服务器的密钥存储区文件的口令。

注释：如果您未指定密钥存储区路径和口令，并且鉴定服务器的信任证书不在 JRE 可信证书存储区 (cacerts) 中，则 Identity Applications 将无法连接到使用 TLS/SSL 协议的鉴定服务。

鉴定配置

这组设置定义了鉴定服务器的设置。

管理员容器的 LDAP DN

必需

指定身份库中包含 OSP 必须鉴定的任何管理员用户对象的容器判别名。例如：ou=sa,o=data。

解析命名属性重复

指定用于区分包含相同 cn 值的多个 eDirectory 用户对象的 LDAP 属性的名称。默认值为 mail。

将鉴定源限制为环境

指定是要将身份库中用户和管理员容器内进行的搜索限制为仅涵盖这些容器中的用户对象，还是应使搜索范围涵盖子容器。

会话超时（分钟）

指定当会话处于非活动状态多少分钟后，服务器会将用户会话置于超时状态。默认值为 20 分钟。

访问令牌有效期（秒）

指定 OSP 访问令牌保持有效的秒数。默认值为 60 秒。

刷新令牌有效期（小时）

指定 OSP 刷新令牌保持有效的秒数。OSP 在内部使用刷新令牌。默认值为 48 小时。

身份验证方法

这组设置定义了可让 OSP 对登录到 Identity Manager 基于浏览器组件的用户进行鉴定的值。

方法

指定当用户登录时您希望 Identity Manager 使用的鉴定类型。

- ◆ **名称和口令：**OSP 使用身份库校验鉴定。

- ♦ **Kerberos**: OSP 接受来自 Kerberos 票据服务器和身份库的鉴定。您还必须指定映射属性名称的值。
- ♦ **SAML 2.0**: OSP 接受来自 SAML 身份提供商和身份库的鉴定。您还必须指定映射属性名称和元数据 URL 的值。

映射属性名称

仅当您指定了 **Kerberos** 或 **SAML** 时才适用。

指定要映射到 Kerberos 票据服务器或身份提供程序中 SAML 表示的属性名称。

元数据 URL

仅当您指定了 **SAML** 时才适用。

指定 OSP 用于将鉴定请求重定向到 SAML 的 URL。

口令管理

这组设置定义了可让用户通过自助操作修改其口令的值。

口令管理提供程序

指定要使用的口令管理系统类型。

User Application (旧版): 使用 Identity Manager 惯常所用的口令管理程序。此选项还允许您使用外部口令管理程序。

忘记口令

仅当您使用 SSPR 时, 此复选框参数才适用。

指定是否希望用户不联系帮助中心自行恢复忘记的口令。

您还必须为“忘记口令”功能配置询问应答策略。有关详细信息, 请参见 [《NetIQ Self Service Password Reset Administration Guide》](#) (NetIQ Self Service Password Reset 管理指南)。

忘记口令

仅当您选择了 **User Application (旧版)** 时, 此菜单列表才适用。

指定是要使用 User Application 中集成的口令管理系统, 还是使用外部系统。

- ♦ **内部**: 使用默认的内部口令管理功能 /jsps/pwdmgt/ForgotPassword.jsp (开头没有 http(s) 协议)。这将用户重定向到内置于 User Application 的“忘记口令”功能, 而不是外部 WAR。
- ♦ **外部**: 使用外部忘记口令 WAR 通过 Web 服务回调 User Application。您还必须指定外部系统的设置。

忘记口令链接

仅当您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

仅当您使用外部口令管理系统时才适用。

指定外部忘记口令 WAR 用来回调 User Application 以执行核心忘记口令功能的 URL。使用以下格式：

```
https://<idmhost>:<sslport>/<idm>/  
pwdmgt/service
```

Sentinel 数字签名证书和密钥

本节定义可让 Identity Manager 与 Sentinel 通讯以进行事件审计的值。

Sentinel 数字签名证书

指定您希望 OSP 服务器用来鉴定发送到审计系统的审计讯息的自定义公共密钥证书。

有关配置 Novell Audit 证书的信息，请参见《[Novell Audit Administration Guide](#)》（Novell Audit 管理指南）中的“[Managing Certificates](#)”（管理证书）。

Sentinel 数字签名私用密钥

指定您希望 OSP 服务器用来鉴定发送到审计系统的审计讯息的自定义私用密钥文件的路径。

11.6.5 SSO 客户端参数

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

默认情况下，该选项卡会显示基本选项。要查看所有设置，请单击[显示高级选项](#)。此选项卡包括以下设置组：

- ◆ [IDM 仪表板](#)（第 140 页）
- ◆ [IDM 管理员](#)（第 141 页）
- ◆ [RBPM](#)（第 141 页）
- ◆ [报告](#)（第 142 页）
- ◆ [IDM 数据收集服务](#)（第 143 页）
- ◆ [DCS 驱动程序](#)（第 143 页）
- ◆ [Self Service Password Reset](#)（第 143 页）

IDM 仪表板

本节定义用户访问 Identity Manager 仪表板所需的 URL 的值，仪表板是 Identity Applications 的初始登录位置。

图 11-1 IDM 仪表板

IDM 仪表板	
OAuth 客户端 ID	<input type="text" value="idmdash"/>
OAuth 客户端密码	<input type="password" value="*****"/>
OSP OAuth 重定向 URL	<input type="text" value="https://192.168.0.1:8543/idmdash/oauth.html"/>

OAuth 客户端 ID

必需

指定用于供鉴定服务器识别仪表板的单点登录客户端的名称。默认值为 idmdash。

OAuth 客户端机密

必需

指定仪表板的单点登录客户端的口令。

OSP OAuth 重定向 URL

必需

指定在完成鉴定后，鉴定服务器要将浏览器客户端重定向到的绝对 URL。

使用以下格式：protocol://server:port/path。例如， https://192.168.0.1:8543/idmdash/oauth.html。

IDM 管理员

本节定义用户访问 Identity Manager 管理员页面所需 URL 的值。

OAuth 客户端 ID

必需

指定用于供鉴定服务器识别 Identity Manager 管理员的单点登录客户端的名称。默认值为 idmadmin。

OAuth 客户端机密

必需

指定 Identity Manager 管理员的单点登录客户端的口令。

OSP OAuth 重定向 URL

必需

指定在完成鉴定后，鉴定服务器要将浏览器客户端重定向到的绝对 URL。

使用以下格式：protocol://server:port/path。例如， https://192.168.0.1:8543/idmadmin/oauth.html。

RBPM

这组设置定义了用户访问 User Application 所需 URL 的值。

图 11-2 RBPM

RBPM	
OAuth 客户端 ID	<input type="text" value="rbpm"/>
OAuth 客户端密码	<input type="password" value="....."/>
登录页的 URL 链接	<input type="text" value="/idmdash/#/landing"/>
OSP OAuth 重定向 URL	<input type="text" value="https://192.168.0.1:8543/IDMProv/oauth"/>
RBPM 至 eDirectory SAML 配置	<input type="text" value="无更改"/>

OAuth 客户端 ID

必需

指定用来供鉴定服务器识别 User Application 单点登录客户端的名称。默认值为 rbpm。

OAuth 客户端机密

必需

指定 User Application 单点登录客户端的口令。

登录页的 URL 链接

必需

指定用于从 User Application 中访问仪表板的相对 URL。默认值为 /landing。

OSP OAuth 重定向 URL

必需

指定在完成鉴定后，鉴定服务器要将浏览器客户端重定向到的绝对 URL。

使用以下格式：protocol://server:port/path。例如，https://192.168.0.1:8543/IDMProv/oauth。

RBPM 至 eDirectory SAML 配置

必需

指定 SSO 鉴定所需的 RBPM 至 eDirectory SAML 设置。

报告

这组设置定义了用户访问 Identity Reporting 所需 URL 的值。仅当您将 Identity Reporting 添加到 Identity Manager 解决方案时，实用程序才会显示这些值。

图 11-3 报告

报告	
OAuth 客户端 ID	<input type="text" value="rpt"/>
OAuth 客户端密码	<input type="password" value="*****"/>
登录页的 URL 链接	<input type="text" value="/idmdash/#/landing"/>
Identity Governance 的 URL 链接	<input type="text"/>
OSP OAuth 重定向 URL	<input type="text" value="https://192.168.0.1:8543/IDMRPT/oauth.html"/>

OAuth 客户端 ID

必需

指定用来供鉴定服务器识别 Identity Reporting 单点登录客户端的名称。默认值为 rpt。

OAuth 客户端机密

必需

指定 Identity Reporting 单点登录客户端的口令。

登录页的 URL 链接

必需

指定用于从 Identity Reporting 中访问仪表板的相对 URL。默认值为 /idmdash/#/landing。

如果您将 Identity Reporting 和 Identity Applications 安装到不同的服务器中，请指定绝对 URL。

使用以下格式：protocol://server:port/path。例如，https://192.168.0.1:8543/IDMRPT/oauth。

OSP OAuth 重定向 URL

必需

指定在完成鉴定后，鉴定服务器要将浏览器客户端重定向到的绝对 URL。

使用以下格式：protocol://server:port/path。例如，https://192.168.0.1:8543/IDMRPT/oauth。

IDM 数据收集服务

本节定义用户访问 Identity Manager 数据收集服务所需 URL 的值。

OAuth 客户端 ID

必需

指定用于供鉴定服务器识别 Identity Manager 数据收集服务的单点登录客户端的名称。默认值为 idmdcs。

OAuth 客户端机密

必需

指定 Identity Manager 数据收集服务的单点登录客户端的口令。

OSP OAuth 重定向 URL

必需

指定在完成鉴定后，鉴定服务器要将浏览器客户端重定向到的绝对 URL。

使用以下格式：protocol://server:port/path。例如，https://192.168.0.1:8543/idmdcs/oauth.html。

DCS 驱动程序

这组设置定义了用于管理数据收集服务驱动程序的值。

图 11-4

DCS 驱动程序	
OAuth 客户端 ID	<input type="text" value="dcsdrv"/>
OAuth 客户端密码	<input type="password" value="*****"/>

OAuth 客户端 ID

指定用来供鉴定服务器识别数据收集服务驱动程序的单点登录客户端的名称。此参数的默认值为 dcsdrv。

OAuth 客户端机密

指定数据收集服务驱动程序的单点登录客户端的口令。

Self Service Password Reset

本节定义用户访问 SSPR 所需 URL 的值。

OAuth 客户端 ID

必需

指定用来供鉴定服务器识别 SSPR 单点登录客户端的名称。默认值为 sspr。

OAuth 客户端机密

必需

指定 SSPR 单点登录客户端的口令。

OSP OAuth 重定向 URL

必需

指定在完成鉴定后，鉴定服务器要将浏览器客户端重定向到的绝对 URL。

使用以下格式：protocol://server:port/path。例如，https://192.168.0.1:8543/sspr/public/oauth.html。

11.6.6 CEF 审计参数

本节定义用于管理单点登录客户端的 CEF 审计参数的值。

发送审计事件

指定是否要使用 CEF 来审计事件。

目标主机

指定审计服务器的 DNS 名称或 IP 地址。

目标端口

指定审计服务器的端口。

网络协议

指定审计服务器用来接收 CEF 事件的网络协议。

使用 TLS

仅当您要使用 TCP 作为网络协议时适用。

指定审计服务器是否配置为将 TLS 与 TCP 搭配使用。

中间事件储存目录

指定在将 CEF 事件发送到审计服务器之前超速缓存目录的位置。

注释：请确保对超速缓存目录设置了 novlua 许可权限。否则，您将不能访问 IDMDash 和 IDMProv 应用程序，并且系统也不会超速缓存目录中记录 OSP 事件。例如，您可以使用 `chown novlua:novlua /<directorypath>` 命令更改该目录的许可权限和所有权，其中，<directorypath> 是超速缓存文件目录路径。

11.7 启动 Identity Applications

配置 Identity Applications 之后，请务必重新启动 Tomcat 服务和 ActiveMQ 服务。

```
systemctl restart netiq-tomcat
```

```
systemctl restart netiq-activemq
```

11.8 为群集配置 OSP 和 SSPR

Identity Manager 在 Tomcat 群集环境中支持 SSPR 配置。

11.8.1 配置 SSPR 以支持群集

要在群集的第一个节点中更新 SSPR 信息，请启动 `/opt/netiq/idm/apps/configupdate/configupdate.sh` 中的配置实用程序。

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。

11.8.2 在群集节点上配置任务

在群集节点上执行以下配置任务：

- 1 要用 SSPR IP 地址更新“忘记口令”链接，请在第一个节点上登录 User Application，然后单击 **管理 > 忘记口令**。
有关 SSPR 配置的详细信息，请参见第 22 节“配置忘记口令管理”（第 205 页）。
- 2 要更改“更改我的口令”链接，请参见第 22.3 节“针对分布式环境或群集环境更新仪表板中的 SSPR 链接”（第 208 页）。
- 3 在群集中的其他节点上，校验“忘记口令”链接和“更改我的口令”链接是否已用 SSPR IP 地址更新。

注释：如果已用 SSPR IP 地址更新“更改口令”链接和“忘记口令”链接，则不需要执行其他更改。

- 4 在第一个节点中，停止 Tomcat，并使用以下命令指定负载均衡器服务器的 DNS 名称来生成新的 `osp.jks` 文件：

```
/opt/netiq/common/jre/bin/keytool -genkey -keyalg RSA -keysize 2048 -keystore osp.jks -storepass <password> -keypass <password> -alias osp -validity 1800 -dname "cn=<loadbalancer IP/DNS>"
```

例如：`/opt/netiq/common/jre/bin/keytool -genkey -keyalg RSA -keysize 2048 -keystore osp.jks -storepass changeit -keypass changeit -alias osp -validity 1800 -dname "cn=mydnsname"`

注释：确保密钥口令与在 OSP 安装期间提供的口令相同。或者，可以使用配置更新实用程序加入密钥存储区口令来更改该口令。

- 5 （视情况而定）要校验 `osp.jks` 文件是否已通过这些更改更新，请运行以下命令：

```
/opt/netiq/common/jre/bin/keytool -list -v -keystore osp.jks -storepass changeit
```
- 6 备份位于 `/opt/netiq/idm/apps/osp` 中的原始 `osp.jks` 文件，并将新 `osp.jks` 文件复制到此位置。新 `osp.jks` 文件是在步骤 3 中创建的。
- 7 将第一个节点上位于 `/opt/netiq/idm/apps/osp` 中的新 `osp.jks` 文件复制到群集中的所有其他 User Application 节点上。
- 8 在第一个节点中启动配置实用程序，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）更改为负载均衡器 DNS 名称。
 - 8a 保存配置实用程序中所做的更改。
 - 8b 要在群集的所有其他节点中反映此更改，请将第一个节点上位于 `TOMCAT_INSTALLED_HOME/conf` 中的 `ism-configuration.properties` 文件复制到所有其他 User Application 节点。

注释：您之前已将第一个节点上的 `ism.properties` 文件复制到群集中的其他节点上。如果您在 User Application 安装期间指定了自定义安装路径，请在群集节点中使用配置更新实用程序确保参照路径正确。

在此方案中，OSP 和 User Application 安装在同一台服务器上；因此，为重定向 URL 使用了相同的 DNS 名称。

如果 OSP 和 User Application 安装在不同的服务器上，请将 OSP URL 更改为指向负载均衡器的其他 DNS 名称。请对安装了 OSP 的所有服务器执行此操作。这可确保所有 OSP 请求均通过负载均衡器发送到 OSP 群集 DNS 名称。这涉及到为 OSP 节点建立一个单独的群集。

9 在 `/TOMCAT_INSTALLED_HOME/bin/` 目录下的 `setenv.sh` 文件中执行以下操作：

9a 为确保 `mcast_addr` 绑定成功，JGroups 要求 `preferIPv4Stack` 属性设置为 `true`。为此，请在所有节点上的 `setenv.sh` 文件中添加 JVM 属性 `-Djava.net.preferIPv4Stack=true`。

9b 在第一个节点上的 `setenv.sh` 文件中添加 `-Dcom.novell.afw.wf.Engine-id=Engine`。

引擎名称应该唯一。提供在安装第一个节点的过程中指定的名称。如果未指定名称，则默认名称为 `Engine`。

同样，为群集中的其他节点添加唯一的引擎名称。例如，对于第二个节点，引擎名称可以是 `Engine2`。

10 在 User Application 中启用群集。

11 为群集启用许可权限索引。有关更多信息，请参见[为群集启用许可权限索引](#)（第 71 页）。

12 在所有节点上重新启动 Tomcat。

13 为群集配置 User Application 驱动程序。有关更多信息，请参见[第 11.5 节“为群集配置 User Application 驱动程序”](#)（第 126 页）。

11.9 配置运行时环境

本节提供为确保运行时环境正常运行而应执行的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：

- ◆ [第 11.9.1 节“将数据收集服务驱动程序配置为从 Identity Applications 收集数据”](#)（第 147 页）
- ◆ [第 11.9.2 节“迁移数据收集服务驱动程序”](#)（第 147 页）
- ◆ [第 11.9.3 节“添加对自定义属性和对象的支持”](#)（第 149 页）
- ◆ [第 11.9.4 节“添加多个驱动程序集支持”](#)（第 152 页）
- ◆ [第 11.9.5 节“将驱动程序配置为使用 SSL 在远程模式下运行”](#)（第 153 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）。

11.9.1 将数据收集服务驱动程序配置为从 Identity Applications 收集数据

要使 Identity Applications 与 Identity Reporting 正常配合运行，必须将 DCS 驱动程序配置为支持 OAuth 协议。

注释：

- ◆ 仅当在环境中使用了 Identity Reporting 时，才需要安装并配置 DCS 驱动程序。
 - ◆ 如果在环境中配置了多个 DCS 驱动程序，则必须针对每个驱动程序完成以下步骤。
-

- 1 登录 Designer。
- 2 在 Designer 中打开您的项目。
- 3 （视情况而定）如果您尚未将 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 重新启动身份库。
 - 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。有关软件要求的详细信息，请参见第 8.6.2 节“安装 Identity Reporting 组件的先决条件”（第 78 页）。
 - 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 Reporting Module 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。

11.9.2 迁移数据收集服务驱动程序

要将对象同步到身份信息仓库中，您必须迁移数据收集服务驱动程序。

- 1 登录到 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] character varying(128)	first_name character varying(128)	last_name character varying(128)	middle_initial character varying(128)	full_name character varying(256)	job_title character varying(128)	department character varying(128)	location character varying(128)	email_address character varying(256)	office_phone character varying(128)	cell_phone character varying(128)
1	0210e2e3655e4	Allison	Blake			Payroll		Northeast	pfredrickson@novell.com (555) 555-1222		
2	05f6a12667734	Ned	North			Senior Physician		Northeast	pfredrickson@novell.com (555) 555-1211		
3	1282ce7c69cb4	Fred	Stats			Purchasing Admin		Northeast	pfredrickson@novell.com (555) 555-1230		
4	13bd8ba9f0494	Kevin	Chester			Benefits Admin		Northeast	pfredrickson@novell.com (555) 555-1221		
5	13faf90666584	Ken	Carson			Attending Physician		Northeast	pfredrickson@novell.com (555) 555-1315		
6	1c886916fd24	Jane	Smith			Administrative Assistant		Northeast	pfredrickson@novell.com (555) 555-1234		
7	1ebe3fcb7364	Application Administrator	Of Sample Data								
8	24fd8b301bce4	Bill	Burke			Administrative Assistant		cn=loc1	pfredrickson@novell.com (555) 555-1210		
9	278698aace6b4	April	Smith			Nurse		Northeast	pfredrickson@novell.com (555) 555-1319		
10	2d8df99b1b1c4	Brad	Jones			Resident Physician		Northeast	pfredrickson@novell.com (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：

LDAP Browser/Editor v2.8.2

File Edit View LDIF Help

ou=users

cn=ablake

cn=achung

cn=apalani

cn=asmith

cn=aspencer

cn=bbender

cn=bbrown

cn=bburke

cn=bjenner

cn=bjones

cn=cblack

cn=ccentral

cn=cnano

cn=eeuro

cn=fstats

cn=jbrown

cn=jkelly

cn=jmiller

cn=jsmith

cn=jwest

cn=karson

cn=kchang

cn=kchester

cn=kkeller

Attribute

Value

employeeType

ft

ACL

6#entry#cn=karson,ou=users,ou=medical-idmsample,o=novell#loginScript

ACL

6#entry#cn=karson,ou=users,ou=medical-idmsample,o=novell#printJobConfiguration

DirXML-Associations

cn=Data Collection Service Driver,cn=TestDrivers,o=novell#1#C53ADD67-DB19-4DD2-9482-67DD3AC519DB

givenName

Ken

photo

BINARY (2Kb)

snrprVahoolMAddress

karson

objectClass

inetOrgPerson

objectClass

organizationalPerson

objectClass

Person

objectClass

ndsLoginProperties

objectClass

Top

objectClass

snrprVuserAux

objectClass

snrprVentityAux

objectClass

homeInfo

objectClass

sampleUserDeviceAux

snrprVgroupwisellMAddress

test

employeeStatus

Active

costCenter

US11115

ou

medical

securityEquals

cn=Medical Operations,ou=groups,ou=medical-idmsample,o=novell

securityEquals

cn=Physician,ou=groups,ou=medical-idmsample,o=novell

uid

karson

mail

pfredrickson@novell.com

cn

karson

passwordAllowChange

TRUE

sampleDeviceDN

cn=karson-laptop,ou=devices,ou=medical-idmsample,o=novell

- 对于每个组，校验是否包含以下类型的信息：

ou=groups	cn=Operations	cn=IT	cn=HR	cn=Medical Operations	cn=Physician	cn=Nursing	cn=Pharmacy	ou=users	cn=ablake	cn=achung
equivalentToMe	cn=jsmith,ou=users,ou=medical-idmsample,o=novell									
equivalentToMe	cn=jkelly,ou=users,ou=medical-idmsample,o=novell									
description	Operations									
objectClass	groupOfNames									
objectClass	Top									
DirXML-Associations	cn=Data Collection Service Driver,cn=TestDrivers,o=novell#1#91539E44-6AFC-4676-D9A2-449E5391FC6A									
cn	Operations									
member	cn=apalani,ou=users,ou=medical-idmsample,o=novell									
member	cn=fstats,ou=users,ou=medical-idmsample,o=novell									
member	cn=rresource,ou=users,ou=medical-idmsample,o=novell									
member	cn=jsmith,ou=users,ou=medical-idmsample,o=novell									
member	cn=jkelly,ou=users,ou=medical-idmsample,o=novell									

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_group boolean	dynamic_rule character var	nested_group boolean	idmrpt_valid_from timestamp without time zone	idmrpt_deleted boolean	idmrpt_syn_state smallint
Pharmacy	Pharmacy	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
IT	Information Technology	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
HR	Human Resources	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 Operations	Medical Operations	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。

11.9.3 添加对自定义属性和对象的支持

您可以对数据收集服务驱动程序进行配置，使其收集和保留不属于默认数据收集模式的自定义属性与对象的数据。为此，您需要修改数据收集服务驱动程序过滤器。修改过滤器不会立即触发对象同步，而是会在身份库中发生添加、修改或删除事件时，向数据收集服务发送新添加的属性和对象。

在添加对自定义属性和对象的支持时，您需要修改报告，以包括扩展的属性和对象信息。以下视图提供有关扩展对象和属性的当前数据与历史数据：

- ◆ idm_rpt_cfg.idmrpt_ext_idv_item_v
- ◆ idm_rpt_cfg.idmrpt_ext_item_attr_v

此过程包括以下活动：

- ◆ 将驱动程序配置为使用扩展对象（第 150 页）
- ◆ 包含数据库中的名称和说明（第 150 页）
- ◆ 向已知的对象类型添加扩展属性（第 151 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。

11.9.4 添加多个驱动程序集支持

新的数据收集服务范围包 (NOVLDCSSCPNG) 为包含多个驱动程序集和多组数据收集服务驱动程序及受管系统网关驱动程序的企业环境提供静态和动态范围功能。

在安装期间或安装之后，您需要确定要在其上安装该包的数据收集服务驱动程序的角色。您需要选择以下角色之一：

- ♦ **Primary** 驱动程序将会同步所有信息，但其他驱动程序集的子树除外。一级数据收集服务驱动程序能够正常为整个身份库提供服务，或者可与一个或多个二级驱动程序配合工作。
- ♦ **次要的** 驱动程序只同步自身的驱动程序集，而不同步其他任何信息。通常，二级数据收集服务驱动程序要求一级驱动程序在不同的驱动程序集中运行，否则，任何本地驱动程序集外部的数据都不会发送到数据收集服务。

如果您使用集成安装过程向树中添加另一个服务器，则服务器只会接收根及其自身驱动程序集分区的副本。如果您还将数据收集服务驱动程序用作此二级服务器上的主驱动程序，则该驱动程序无法发现需要报告的对象更改。

- ♦ **自定义** 允许管理员自定义范围规则。唯一的隐式范围是本地驱动程序集，其他任何驱动程序如果未显式添加到自定义范围列表，都会被视为不在范围内。自定义范围是身份库中应该同步其从属或子树的容器的判别名（采用斜杠格式）。

只有如下所述的某些配置情况才需要范围包：

- ♦ **单个服务器与具有单个驱动程序集的身份库：**对于此情况，您不需要定义范围，因此也就无需安装范围包。
- ♦ **多个服务器与具有单个驱动程序集的身份库：**对于此情况，您需要遵循以下指导原则：
 - ♦ 确保 Identity Manager 服务器存有要从中收集数据的所有分区的复本。
 - ♦ 对于此情况，您不需要定义范围，因此，请不要安装范围包
- ♦ **多个服务器与具有多个驱动程序集的身份库：**此情况有两种基本配置：
 - ♦ 所有服务器都存有要从中收集数据的所有分区的复本。

对于此配置，您需要遵循以下指导原则：

- ♦ 需要定义范围，以免有多个 DCS 驱动程序处理同一项更改。
 - ♦ 您需要在所有 DCS 驱动程序上安装范围包。
 - ♦ 您需要将一个 DCS 驱动程序选作一级驱动程序。
 - ♦ 您需要将所有其他 DCS 驱动程序配置为二级驱动程序。
- ♦ 所有服务器都未存有要从中收集数据的所有分区的复本。

此配置存在两种可能的情况：

- ♦ 应从中收集数据的所有分区 *仅由* 一个 Identity Manager 服务器存放

在此情况下，您需要遵循以下指导原则：

- ♦ 需要定义范围，以免有多个 DCS 驱动程序处理同一项更改。
- ♦ 您需要在所有 DCS 驱动程序上安装范围包。
- ♦ 您需要将所有 DCS 驱动程序都配置为一级驱动程序。

- ♦ 应从中收集数据的所有分区 *不是仅由* 一个 Identity Manager 服务器存放（某些分区由多个 Identity Manager 服务器存放）。

在此情况下，您需要遵循以下指导原则：

- ♦ 需要定义范围，以免有多个 DCS 驱动程序处理同一项更改。

- ◆ 您需要在所有 DCS 驱动程序上安装范围包。
- ◆ 您需要将所有 DCS 驱动程序都配置为自定义驱动程序。

您需要为每个驱动程序定义自定义范围规则，并务必不要创建任何重叠的范围。

11.9.5 将驱动程序配置为使用 SSL 在远程模式下运行

在以远程模式运行时，您可以将数据收集服务驱动程序和受管系统网关驱动程序配置为使用 SSL。本节提供有关将驱动程序配置为使用 SSL 在远程模式下运行的步骤。

要使用密钥存储区为受管系统网关驱动程序配置 SSL，请执行以下操作：

- 1 在 iManager 中创建服务器证书。
 - 1a 在角色和任务视图中，单击 **NetIQ 证书服务器 > 创建服务器证书**。
 - 1b 浏览到安装了受管系统网关驱动程序的服务器对象，并将其选中。
 - 1c 指定证书昵称。
 - 1d 选择“标准”创建方法，然后单击“下一步”。
 - 1e 单击“完成”，然后单击“关闭”。
- 2 使用 iManager 导出服务器证书。
 - 2a 在角色和任务视图中，单击 **NetIQ 证书访问 > 服务器证书**。
 - 2b 选择步骤 1（第 153 页）中创建的证书，然后单击导出。
 - 2c 在证书菜单中，选择该证书的名称。
 - 2d 确保导出私用密钥已选中。
 - 2e 输入口令，然后单击下一步。
 - 2f 单击保存导出的证书，并保存导出的 pfx 证书。
- 3 将步骤 2（第 153 页）中导出的 pfx 证书导入 Java 密钥存储区。
 - 3a 使用 Java 随附的 keytool。您必须使用 JDK 6 或更高版本。
 - 3b 在命令提示符处输入以下命令：


```
keytool -importkeystore -srckeystore pfx certificate -srcstoretype PKCS12 -destkeystore Keystore Name
```

例如：

```
keytool -importkeystore -srckeystore cert.pfx -srcstoretype PKCS12 -destkeystore msgw.jks
```
 - 3c 在系统提示时输入口令。
- 4 使用 iManager 将受管系统网关驱动程序配置修改为使用密钥存储区。
 - 4a 在 **Identity Manager 概述** 中，单击包含受管系统网关驱动程序的驱动程序集。
 - 4b 单击驱动程序状态图标，然后选择编辑属性 > 驱动程序配置。
 - 4c 将显示连接参数设置为 true，并将驱动程序配置模式设置为“远程”。
 - 4d 输入密钥存储区文件的完整路径和口令。
 - 4e 保存并重启动驱动程序。

- 5 使用 iManager 将数据收集服务驱动程序配置修改为使用密钥存储区。
 - 5a 在 **Identity Manager 概述** 中，单击包含受管系统网关驱动程序的驱动程序集。
 - 5b 单击驱动程序状态图标，然后选择编辑属性 > 驱动程序配置。
 - 5c 在受管系统网关注册标题下，将受管系统网关驱动程序配置模式设置为“远程”。
 - 5d 输入密钥存储区的完整路径、口令以及在步骤 1c（第 153 页）中指定的别名。
 - 5e 保存并重启动驱动程序。

11.10 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，您必须重新启动 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，则不需要重新启动服务器。

- [第 11.10.1 节“在“身份数据收集服务”页面中手动添加数据源”（第 154 页）](#)
- [第 11.10.2 节“对 Oracle 数据库运行报告”（第 154 页）](#)
- [第 11.10.3 节“手动生成数据库纲要”（第 155 页）](#)
- [第 11.10.4 节“清除数据库校验和”（第 156 页）](#)
- [第 11.10.5 节“部署 Identity Reporting 的 REST API”（第 156 页）](#)
- [第 11.10.6 节“连接远程 Remote PostgreSQL 数据库”（第 156 页）](#)

11.10.1 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。

11.10.2 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 数据库的服务器上有 ojbc.jar 文件。

有关支持的 Oracle 数据库的详细信息，请参见[第 8.6.4 节“Identity Reporting 的系统要求”（第 80 页）](#)。

11.10.3 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 155 页）
- ♦ 针对 Oracle 数据库配置 `Create_rpt_roles_and_schemas.sql` 纲要（第 155 页）

针对 PostgreSQL 数据库配置 `Create_rpt_roles_and_schemas.sql` 纲要

- 1 使用位于 `/mnt/reporting/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。
 1. 以 postgres 用户身份登录 PGAdmin。
 2. 运行查询工具。
 3. 要创建 `Create_rpt_roles_and_schemas` 和 `Create_dcs_roles_and_schemas` 过程，请将这些 SQL 中的内容复制到查询工具，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：

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

Select CREATE_RPT_ROLES_AND_SCHEMAS('<Set pwd for IDM_RPT_CFG>', '<Set pwd for IDMRPTUSER>');
```
 5. 要创建 `IDM_RPT_DATA` 纲要，请将 `/mnt/Reporting/sql` 中 `get_formatted_user_dn.sql` 的内容复制到查询工具，然后对连接的数据库执行命令。

针对 Oracle 数据库配置 `Create_rpt_roles_and_schemas.sql` 纲要

- 1 使用 `/mnt/Reporting/sql` 中的 `create_dcs_roles_and_schemas-oracle.sql` 和 `create_rpt_roles_and_schemas-oracle.sql`，将必需的角色添加到数据库。
 1. 以数据库管理员用户身份登录 SQL Developer。
 2. 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。
 3. 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>');
end;

begin
CREATE_RPT_ROLES_AND_SCHEMAS('<Set pwd for IDM_RPT_CFG>', '<Set pwd for IDMRPTUSER>');
end;
```
 4. 要创建 `IDM_RPT_DATA` 纲要，请将 `/mnt/Reporting/sql` 中 `get_formatted_user_dn-oracle.sql` 的内容复制到 SQL Developer，然后对连接的数据库执行命令。

11.10.4 清除数据库校验和

1 在 /opt/netiq/idm/apps/IDMReporting/sql 中找到以下 .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。

11.10.5 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。

11.10.6 连接远程 Remote PostgreSQL 数据库

如果您的 PostgreSQL 数据库安装在单独的服务器上，则需要在该远程数据库的 postgresql.conf 和 pg_hba.conf 文件中更改默认设置。

1 在 postgresql.conf 文件中更改侦听地址。

默认情况下，PostgreSQL 允许侦听 localhost 连接，不允许远程 TCP/IP 连接。要允许远程 TCP/IP 连接，请将下面的条目添加到 /opt/netiq/idm/postgres/data/postgresql.conf 文件中：

```
listen_addresses = '*'
```

如果服务器上有多接口，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，请将下面的条目添加到 /opt/netiq/idm/postgres/data/pg_hba.conf 文件中。

```
host all all 0.0.0.0/0 md5
```

例如，192.168.104.24/26 trust

这仅适用于 IPv4 地址。对于 IPv6 地址，请添加以下条目：

```
host all all ::0/0 md5
```

如果您要允许来自特定网络上多台客户端计算机的连接，请采用 CIDR 地址格式在此条目中指定网络地址。

pg_hba.conf 文件支持以下客户端鉴定格式。

- ◆ local database user authentication-method [authentication-option]
- ◆ host database user CIDR-address authentication-method [authentication-option]
- ◆ hostssl database user CIDR-address authentication-method [authentication-option]
- ◆ hostnossl database user CIDR-address authentication-method [authentication-option]

您可以使用以下格式在单独的字段中指定 IP 地址和网络掩码，而不使用 CIDR 地址格式：

- ◆ host database user IP-address IP-mask authentication-method [authentication-option]
- ◆ hostssl database user IP-address IP-mask authentication-method [authentication-option]
- ◆ hostnossl database user IP-address IP-mask authentication-method [authentication-option]

3 测试远程连接。

3a 重新启动远程 PostgreSQL 服务器。

3b 使用用户名和口令远程登录服务器。

安装 Designer

本部分将指导您完成 Designer for Identity Manager 的安装过程。

12 规划安装 Designer

本章提供了安装 Designer 所需的先决条件、注意事项以及系统设置。

- ◆ 第 12.1 节 “Designer 安装核对清单”（第 161 页）
- ◆ 第 12.2 节 “Designer 的安装先决条件”（第 161 页）
- ◆ 第 12.3 节 “Designer 的系统要求”（第 161 页）

12.1 Designer 安装核对清单

在开始安装之前，NetIQ 建议您先查看以下步骤。

	核对清单项目
<input type="checkbox"/>	1. 查看安装 Designer 的注意事项，以确保计算机符合先决条件。有关详细信息，请参见第 12.2 节 “Designer 的安装先决条件”（第 161 页）。
<input type="checkbox"/>	2. 确保安装 Designer 的目标计算机符合指定的软件和硬件要求。有关详细信息，请参见第 12.3 节 “Designer 的系统要求”（第 161 页）。
<input type="checkbox"/>	3. 安装 Designer。有关详细信息，请参见第 13 节 “安装 Designer”（第 163 页）。
<input type="checkbox"/>	4. （可选）要启动 Identity Manager 解决方案的项目，请参见《Understanding Designer for Identity Manager》（了解 Designer for Identity Manager）。

12.2 Designer 的安装先决条件

本节提供安装 Designer 的先决条件和注意事项。

- ◆ 在运行 Linux 操作系统的计算机上安装 Designer 之前，必须先安装 GNU gettext 实用程序。这些实用程序为国际化和多语言讯息提供了一个框架。有关语言支持的详细信息，请参见第 5.10 节 “了解语言支持”（第 46 页）。
- ◆ 在运行 RHEL 7.4 操作系统的计算机上安装 Designer 之前，必须先安装 gtk2-2.24.31-1.el7.x86_64.rpm。例如，可以从[操作系统供应商网站](#)下载包。

12.3 Designer 的系统要求

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

类别	要求
处理器	1 GHz

类别	要求
磁盘空间	1 GB
内存	1 GB
操作系统（经认可）	<p>以下 64 位操作系统之一：</p> <p>服务器</p> <ul style="list-style-type: none"> ◆ SLES 12 SP3 ◆ SLES 12 SP2 ◆ RHEL 7.4 ◆ RHEL 7.3 ◆ openSUSE Leap 42.1 <p>Desktops</p> <ul style="list-style-type: none"> ◆ SLED 12 SP3 ◆ SLED 12 SP2 <p>注释：经认可指操作系统已经过全面测试且受支持。</p>
操作系统（受支持）	<p>经认可操作系统的最新版服务包</p> <p>注释：受支持指操作系统尚未经过测试，但预期可以正常工作</p>
虚拟化系统	<ul style="list-style-type: none"> ◆ Hyper-V Server 2012 R2 ◆ VMWare ESX 5.5 或更高版本 <p>NetIQ 支持在为运行 NetIQ 产品的操作系统提供官方支持的企业级虚拟化系统上安装 Identity Manager。只要虚拟化系统的供应商为这些操作系统提供官方支持，NetIQ 就可支持这些系统上的整个 Identity Manager 堆栈。</p>

13 安装 Designer

本章介绍 Designer 的安装过程。可以采用 GUI 模式或控制台模式执行安装。

要安装 Designer，请执行以下操作：

1 从 NetIQ 下载网站下载 Identity_Manager_Linux_LDAP_Designer.tar.gz。

2 导航到要提取文件的目录。

3 运行以下命令：

```
tar -zxvf Identity_Manager_Linux_LDAP_Designer.tar.gz
```

4 运行以下命令之一安装 Designer。

控制台： ./install

GUI： ./install -i console

5 按照提示继续安装。



安装 Analyzer

本节将指导您完成安装 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。

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 14.1 节 “Analyzer 安装核对清单”](#)（第 167 页）。

14 计划安装 Analyzer

本章提供有关准备安装 Analyzer for Identity Manager 的指导。NetIQ 建议您在开始之前，先查看安装过程。

- ◆ 第 14.1 节 “Analyzer 安装核对清单”（第 167 页）
- ◆ 第 14.2 节 “Analyzer 安装先决条件”（第 167 页）
- ◆ 第 14.3 节 “Analyzer 的系统要求”（第 168 页）

14.1 Analyzer 安装核对清单

在开始安装过程之前，NetIQ 建议您先查看以下步骤。

	核对清单项目
<input type="checkbox"/>	1. 了解 Identity Manager 各组件之间的交互。有关详细信息，请参见第 1 章 “Identity Manager 的组件概述”（第 17 页）。
<input type="checkbox"/>	2. 确定要为 Identity Manager 组件使用哪些服务器。有关详细信息，请参见第 5.7 节 “建议的安装方案和服务器设置”（第 38 页）。
<input type="checkbox"/>	3. 确保您的环境符合有关托管 Analyzer 的注意事项和要求。有关详细信息，请参见以下各节： <ul style="list-style-type: none">◆ 第 14.2 节 “Analyzer 安装先决条件”（第 167 页）◆ 第 14.3 节 “Analyzer 的系统要求”（第 168 页）
<input type="checkbox"/>	4. 要安装 Analyzer，请参见以下章节： <ul style="list-style-type: none">◆ 要使用安装向导，请参见第 15.1 节 “使用向导安装 Analyzer”（第 169 页）。◆ 对于无提示安装，请参见第 15.2 节 “以无提示模式安装 Analyzer”（第 170 页）
<input type="checkbox"/>	5. （可选）要自动接收和显示来自 Analyzer 的审计事件，请安装 XDAS 客户端。有关详细信息，请参见第 15.4 节 “安装 Analyzer 的审计客户端”（第 171 页）。
<input type="checkbox"/>	6. 要激活 Analyzer，请参见第 24.4.2 节 “激活 Analyzer”（第 215 页）。
<input type="checkbox"/>	7. （可选）要升级 Analyzer，请参见第 26.7 节 “升级 Analyzer”（第 245 页）。

14.2 Analyzer 安装先决条件

本节提供安装 Analyzer 的先决条件和注意事项。

- ◆ 在运行 SLES 12 SP3 操作系统的计算机上安装 Analyzer 之前，请确保已安装以下库：
 - ◆ libswt3-gtk2-3.3.0-0.20.8.9mdv2008.0.i586.rpm
 - ◆ libxcomposite1-0.4.1-1mdv2010.1.i586.rpm

- ♦ libgdk_pixbuf2.0_0-2.20.1-1mdv2010.1.i586.rpm
- ♦ libgtk+-x11-2.0_0-2.12.1-2.1mdv2008.0.i586.rpm
- ♦ 在运行 RHEL 7.3 或更高版本平台的计算机上安装 Analyzer 之前，必须先安装 gtk2.i686.rpm。例如，可以从[操作系统供应商网站](#)下载包。

14.3 Analyzer 的系统要求

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

类别	要求
处理器	1 GHz
内存	2 GB
视频分辨率	1024*768（建议 1280*1025）
操作系统（经认可）	<p>下列操作系统之一：</p> <ul style="list-style-type: none"> ♦ SLES 12 SP3 ♦ SLES 12 SP2 ♦ RHEL 7.4 ♦ RHEL 7.3 ♦ openSUSE Leap 42.1 <p>注释：经认可指操作系统已经过全面测试且受支持。</p>
操作系统（受支持）	<p>经认可操作系统的最新版服务包</p> <p>注释：受支持指操作系统尚未经过测试，但预期可以正常工作</p>
虚拟化系统	<ul style="list-style-type: none"> ♦ Hyper-V Server 2012 R2 ♦ VMWare ESX 5.0 及更高版本 <p>NetIQ 支持在为运行 NetIQ 产品的操作系统提供官方支持的企业级虚拟化系统上安装 Identity Manager。只要虚拟化系统的供应商为这些操作系统提供官方支持，NetIQ 就可支持这些系统上的整个 Identity Manager 堆栈。</p>
其他软件	<ul style="list-style-type: none"> ♦ Gettext 实用程序

15 安装 Analyzer

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

- 第 15.1 节 “使用向导安装 Analyzer” (第 169 页)
- 第 15.2 节 “以无提示模式安装 Analyzer” (第 170 页)
- 第 15.3 节 “将 XULrunner 添加到 Analyzer.ini 中” (第 170 页)
- 第 15.4 节 “安装 Analyzer 的审计客户端” (第 171 页)

15.1 使用向导安装 Analyzer

以下过程描述如何通过 GUI 或控制台使用安装向导在 Linux 或 Windows 平台上安装 Analyzer。要执行无提示或无人照管安装，请参见第 15.2 节 “以无提示模式安装 Analyzer” (第 170 页)。

要准备安装，请查看第 14.1 节 “Analyzer 安装核对清单” (第 167 页) 中列出的先决条件和系统要求。

- 1 以 root 或管理员身份登录到要安装 Analyzer 的计算机。
- 2 (视情况而定) 如果您已获取 Identity Manager 安装包的 .iso 映像文件，请浏览到包含 Analyzer 安装文件的目录 (默认位于 /Analyzer/packages 目录中)。
- 3 (视情况而定) 如果您已下载 Analyzer 安装文件，请完成以下步骤：
 - 3a 浏览到所下载映像的 .tgz 或 win.zip 文件。
 - 3b 将该文件的内容解压缩到本地计算机上的某个文件夹中。
- 4 执行安装程序：

```
./install
```
- 5 遵循向导中的说明操作，直到完成安装 Analyzer。
- 6 安装过程完成后，复查安装后摘要，以检查 Analyzer 的安装状态及其日志文件的位置。
- 7 单击**完成**。
- 8 (视情况而定) 完成第 15.3 节 “将 XULrunner 添加到 Analyzer.ini 中” (第 170 页) 中的步骤。
- 9 (可选) 要在 Windows 计算机上为 Analyzer 配置基于角色的服务，请打开默认情况下位于 C:\Program Files (x86)\NetIQ\Tomcat\webapp\help\en\install 目录中的 gettingstarted.html 网站的链接。
请使用 iManager 来配置基于角色的服务。
- 10 要激活 Analyzer，请参见[激活 Analyzer](#) (第 215 页)。

15.2 以无提示模式安装 Analyzer

无提示（非交互式）安装不显示用户界面，也不向用户提出任何问题。此时，InstallAnywhere 将使用默认 `analyzerInstaller.properties` 文件中的信息。您可以使用默认文件运行无提示安装，或者编辑该文件以自定义安装过程。

默认情况下，安装程序将在 `Program Files (x86)\NetIQ\Analyzer` 目录中安装 Analyzer。

- 1 以 root 或管理员身份登录到要安装 Analyzer 的计算机。
- 2（视情况而定）如果您已获取 Identity Manager 安装包的 .iso 映像文件，请浏览到包含 Analyzer 安装文件的目录（默认情况下在 `products/Analyzer/` 目录中）。
- 3（视情况而定）如果您已从 [NetIQ 下载网站](#) 下载了 Analyzer 安装文件，请完成以下步骤：
 - 3a 浏览到所下载映像的 .tgz 或 win.zip 文件。
 - 3b 将该文件的内容解压缩到本地计算机上的某个文件夹中。
- 4（可选）要指定非默认安装路径，请完成以下步骤：
 - 4a 打开默认位于 `products/Analyzer/` 目录中的 `analyzerInstaller.properties` 文件。
 - 4b 在该 properties 文件中添加以下文本：

```
USER_INSTALL_DIR=installation_path
```
- 5 要运行无提示安装，请发出以下命令之一：
 - ◆ **Linux:** `install -i silent -f analyzerInstaller.properties`
 - ◆ **Windows:** `install.exe -i silent -f analyzerInstaller.properties`
- 6（视情况而定）在 Linux 计算机上，完成第 15.3 节“[将 XULrunner 添加到 Analyzer.ini 中](#)”（第 170 页）中的步骤。
- 7 要激活 Analyzer，请参见[激活 Analyzer](#)（第 215 页）。

15.3 将 XULrunner 添加到 Analyzer.ini 中

在 Linux 平台上运行 Analyzer 之前，必须更改 XULRunner 映射。

注释：在 SLED 11 上，建议的 XULrunner 版本是 1.9.0.19。在 OpenSUSE 11.4 上，建议版本是 1.9.0.2。这些版本随操作系统提供。

- 1 浏览到默认情况下位于以下位置的 Analyzer 安装目录：

```
home/admin/analyzer
```
- 2 在 gedit 编辑器中打开 `Analyzer.ini` 文件。
- 3 在参数列表的末尾添加以下行：

```
-Dorg.eclipse.swt.browser.XULRunnerPath=/usr/lib/xulrunner-1.9/
```

例如，`Analyzer.ini` 文件应如下所示：

```
-vmargs
-Xms256m
-Xmx1024m
-XX:MaxPermSize=128m
-XX:+UseParallelGC
-XX:ParallelGCThreads=20
-XX:+UseParallelOldGC
-Dorg.eclipse.swt.browser.XULRunnerPath=/usr/lib/xulrunner-1.9/
```

4 保存 Analyzer.ini 文件。

5 起动 Analyzer。

15.4 安装 Analyzer 的审计客户端

Analyzer 包含一个 XDAS 库，当您向应用程序发回数据更新时，该库将从“数据浏览器”编辑器自动生成审计事件。有关在源应用程序中使用“数据浏览器”编辑器更新数据的详细信息，请参见《*NetIQ Analyzer for Identity Manager Administration Guide*》（NetIQ Analyzer for Identity Manager 管理指南）中的“*Modifying Data*”（修改数据）。

要查看这些审计事件，请安装可从 Analyzer 接收审计事件的 XDAS 客户端。[OpenXDAS Project \(http://openxdas.sourceforge.net\)](http://openxdas.sourceforge.net)（OpenXDAS 项目）中提供了有关 XDAS 的详细信息。

Analyzer 的下载包中包含 XDAS 客户端。但是，Analyzer 的安装程序不会安装 XDAS 客户端。

- 1 安装 Analyzer。
- 2 浏览到 OpenXDAS 安装文件；默认情况下，这些文件位于 .iso 映像文件的 products/Analyzer/openxdas/Operating_system 目录中。
- 3 使用 rpm 命令起动 XDAS 客户端的安装程序。
- 4 遵循提示安装 XDAS 客户端。
- 5 安装过程完成后，起动 XDAS 客户端，以自动接收和显示来自 Analyzer 的审计事件。

VII

在 Identity Manager 中配置单点登录访问

默认情况下，Identity Manager 使用 OSP 进行单点登录访问。安装 Identity Reporting 和 Identity Applications 时，您可以指定用户鉴定的基本设置。但是，您也可以将 OSP 鉴定服务器配置为接受来自 Kerberos 票据服务器或 SAML IDP 的鉴定。例如，您可以使用 SAML 支持来自 NetIQ Access Manager 的鉴定。

16 准备单点登录访问

默认情况下，Identity Manager 使用 OSP 进行单点登录访问。安装 Identity Reporting 和 Identity Applications 时，您可以指定用户鉴定的基本设置。但是，您也可以将 OSP 鉴定服务器配置为接受来自 Kerberos 票据服务器或 SAML IDP 的鉴定。例如，您可以使用 SAML 支持来自 NetIQ Access Manager 的鉴定。

NetIQ 建议您完成以下核对清单中的步骤。

	核对清单项目
<input type="checkbox"/>	1. 安装 Identity Applications。有关详细信息，请参见第 9 章“安装 Identity Manager 引擎、Identity Applications 和 Identity Reporting”（第 83 页）。
<input type="checkbox"/>	2. （可选）安装 Identity Reporting。有关详细信息，请参见第 9 章“安装 Identity Manager 引擎、Identity Applications 和 Identity Reporting”（第 83 页）。
<input type="checkbox"/>	3. 将 Identity Applications 配置为使用 OSP 进行单点登录访问。有关详细信息，请参见第 17 章“在 Identity Manager 中使用 One SSO Provider 进行单点登录访问”（第 177 页）。
<input type="checkbox"/>	4. 安装要用于 Identity Manager 的鉴定系统。例如：Access Manager 或 Kerberos。
<input type="checkbox"/>	5. （视情况而定）配置 Access Manager 和 OSP。有关详细信息，请参见第 18 章“对 NetIQ Access Manager 使用 SAML 鉴定进行单点登录”（第 179 页）。
<input type="checkbox"/>	6. 校验单点登录设置。有关详细信息，请参见第 19 章“校验是否可对 Identity Applications 进行单点登录访问”（第 185 页）。

17 在 Identity Manager 中使用 One SSO Provider 进行单点登录访问

要提供对 Identity Applications 的单点登录访问，您必须配置 RBPM 配置实用程序中的一些设置。您应该已具备必要的证书和密钥，以便在安装 OSP 后进行单点登录。

此过程假设您的环境将为 eDirectory、SSO 控制器和 OAuth 提供程序使用一个证书。如果您的组织需要更多分离层，请为 OAuth 提供程序单独创建一个证书。

17.1 准备 eDirectory 进行单点登录访问

在安装 eDirectory 的过程中，您必须配置身份库以支持对 Identity Applications 和 Identity Reporting 进行单点登录访问。

执行中所述的步骤。如果您先前已将 eDirectory 概要扩展为包含 SAML 概要，并安装了所需的 NMAS 方法，则不需要再次执行这些步骤，而是可以直接跳转到有关创建可信根容器的小节。

17.2 修改单点登录访问的基本设置

在安装 Identity Applications 时，您通常需要配置单点登录访问的基本设置。本节将帮助您确保这些设置适合您的环境。

- 1 运行 RBPM 配置实用程序。有关详细信息，请参见第 11.6.1 节“运行 Identity Applications 配置实用程序”（第 126 页）。
- 2 要修改鉴定设置，请完成以下步骤：
 - 2a 单击**鉴定**。
 - 2b （视情况而定）要指定实际的服务器 DNS 名称或 IP 地址，请更改 localhost 的所有实例。
 - ◆ 指定的地址必须可从所有客户端解析。仅当对 Identity Manager 的所有访问（包括通过浏览器访问）都是从本地进行时，才应使用 localhost。
 - ◆ 此“公共”主机名或 IP 地址应与您在安装 OSP 时指定的 *PublicServerName* 值相同。
 - ◆ 在分布式或群集环境中，所有 OAuth URL 都应该使用相同的值。该 URL 应该通过 L4 交换机或负载均衡器实现客户端访问。此外，osp.war 和配置文件必须安装到环境中的每个部署上。
 - 2c 对于**管理员容器的 LDAP DN**，请单击**浏览**按钮，然后选择身份库中包含 Identity Applications 管理员的容器。
 - 2d 指定您在安装 OSP 时创建的 OAuth 密钥存储区文件。

请包含密钥存储区文件路径、密钥存储区文件口令、密钥别名和密钥口令。默认的密钥存储区文件为 osp.jks，默认的密钥别名为 osp。

3 要修改单点登录设置，请完成以下步骤：

3a 单击 **SSO 客户端**。

3b （视情况而定）要指定实际的服务器 DNS 名称或 IP 地址，请更改 localhost 的所有实例。

- ♦ 指定的地址必须可从所有客户端解析。仅当对仪表板的所有访问（包括通过浏览器访问）都将在本地进行时，才应使用 localhost。
- ♦ 此“公共”主机名或 IP 地址应与您在安装 OSP 时指定的 *PublicServerName* 值相同。
- ♦ 在分布式或群集环境中，所有 OAuth 重定向 URL 都应该使用相同的值。该 URL 应该通过 L4 交换机或负载均衡器实现客户端访问。

3c （视情况而定）如果使用非默认端口，请更新以下 Identity Manager 组件的端口号：

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

4 单击**确定**保存所做的更改，然后关闭配置实用程序。

5 启动 Tomcat。

17.3 将 Self Service Password Reset 配置为信任 OSP

为了使单点登录正常工作，您必须使用证书在 OSP 与 Self Service Password Reset (SSPR) 之间配置信任关系。您必须从 OSP 的密钥存储区文件 *osp.jks* 中导出证书。

导出证书后，必须将它导入 SSPR 的密钥存储区文件。

有关设置安全通道的详细信息，请参见《[Self Service Password Reset Administration Guide](#)》（Self Service Password Reset 管理指南）中的“[Setting Up a Secure Channel Between the Application Server and the LDAP Server](#)”（在应用程序服务器与 LDAP 服务器之间设置安全通道）。

18 对 NetIQ Access Manager 使用 SAML 鉴定进行单点登录

本章将帮助您配置 NetIQ Access Manager 和 OSP，以支持在 Identity Manager 中使用 SAML 2.0 鉴定进行单点登录访问。在开始之前，请先查看操作说明所基于的以下假设：

- 您已装有新的受支持 Access Manager 版本。
- 您已装有新版 Identity Manager。
- 这两项安装的主机名配置都使用了 DNS 名称。
- 这两项安装都使用 SSL 协议进行通讯。
- 您必须为 Access Manager 设置一个使用身份库作为 LDAP 用户存储区的群集环境。有关详细信息，请参见《[NetIQ Access Manager Administration Guide](#)》（NetIQ Access Manager 管理指南）。

18.1 了解第三方鉴定和单点登录

您可以将 Identity Manager 配置为使用 SAML 2.0 鉴定来与 NetIQ Access Manager 相互协作。借助此项功能，您可以使用一项非基于口令的技术通过 Access Manager 登录到 Identity Applications。例如，用户可以通过用户（客户端）证书进行登录，例如从智能卡登录。

Access Manager 将与 OSP 交互，以将用户映射到身份库中的 DN。当用户通过 Access Manager 登录 Identity Applications 时，Access Manager 可在 HTTP 标题中插入一个 SAML 声明（使用用户的 DN 作为标识符），并将该请求转发到 Identity Applications。Identity Applications 使用该 SAML 声明与身份库建立 LDAP 连接。

如果将 SAML 声明用于 Identity Applications 鉴定，则允许基于口令的单点登录鉴定的附属 Portlet 将不支持单点登录。

18.2 创建和安装 SSL 证书

为确保完成鉴定，Access Manager 和 OSP 必须共享其 SSL 证书的可信根。本节将帮助您为 Access Manager 创建新证书，并确保可信证书存储区包含正确的证书。

- [第 18.2.1 节“为 Access Manager 创建 SSL 证书”](#)（第 180 页）
- [第 18.2.2 节“在 Identity Manager 可信证书存储区中安装 Access Manager 证书”](#)（第 180 页）
- [第 18.2.3 节“在 Access Manager 可信证书存储区中安装 SSL 服务器证书”](#)（第 181 页）

18.2.1 为 Access Manager 创建 SSL 证书

Access Manager 无法使用其默认的 SSL 证书 test-connector 来与 Identity Manager 进行通讯。您必须创建一个证书主题字段中包含主机名的证书，然后将它指派给 Access Manager。

有关详细信息，请参见《[NetIQ Access Manager Administration Console Guide](#)》（NetIQ Access Manager 管理控制台指南）中的“[Security and Certificate Management](#)”（安全性和证书管理）。

- 1 打开 Access Manager 的管理控制台。
- 2 单击[安全性 > 证书](#)。
- 3 单击[新建](#)。
- 4 指定新证书的名称。例如：`hostname_ssl`。
- 5 单击窗口右侧的编辑按钮。
- 6 对于[常用名](#)，请指定托管 Access Manager 的服务器的 DNS 名称，然后单击[确定](#)。
- 7 对于[有效月数](#)，请指定一个不超过 99 的值。
- 8 对于[密钥大小](#)，请指定 2048。
- 9 选择新建的证书，然后单击[操作 > 将证书添加到密钥存储区 ...](#)。
- 10 单击[密钥存储区](#)右侧的编辑按钮。
- 11 选择 **SSL 连接器**，然后单击[确定](#)。
- 12 单击[确定](#)。
- 13 在 OSP 可信证书存储区中安装新证书。有关详细信息，请参见第 18.2.2 节“[在 Identity Manager 可信证书存储区中安装 Access Manager 证书](#)”（第 180 页）。

18.2.2 在 Identity Manager 可信证书存储区中安装 Access Manager 证书

OSP 可信证书存储区必须包含 Access Manager 的安全性证书。

- 1 要导出新的 SSL 证书，请完成以下操作：
 - ♦ 在 Access Manager 管理控制台的安全性 > 可信根下，导出 SSL 证书的根证书。将根证书命名为 **configCA**。
 - ♦ 导出 SSL 服务器证书。

有关详细信息，请参见《[NetIQ Access Manager Administration Console Guide](#)》（NetIQ Access Manager 管理控制台指南）中的“[Managing Trusted Roots and Trust Stores](#)”（管理可信根和可信证书存储区）。
- 2 将导出的证书复制到运行 OSP 的服务器上。
- 3 使用随 Java 提供的 keytool 将该文件导入到 JRE 的 cacerts 密钥存储区中。

例如，`/opt/netiq/common/jre/bin/keytool -importcert -trustcacerts -alias <NAM-cert> -keystore /opt/netiq/common/jre/lib/security-storepass <password> -file custom_location/<exported_file>`
- 4 在 Access Manager 可信证书存储区中安装 OSP 证书。

有关详细信息，请参见第 18.2.3 节“[在 Access Manager 可信证书存储区中安装 SSL 服务器证书](#)”（第 181 页）。

18.2.3 在 Access Manager 可信证书存储区中安装 SSL 服务器证书

Access Manager 可信证书存储区必须包含 OSP 的安全性证书。有关详细信息，请参见《[NetIQ Access Manager Administration Console Guide](#)》（NetIQ Access Manager 管理控制台指南）中的“[Managing Trusted Roots and Trust Stores](#)”（管理可信根和可信证书存储区）。

获取运行 OSP 的 Tomcat 实例要用于 SSL 的服务器证书。

- 1 将托管 OSP 的 Tomcat 实例的 SSL 服务器证书复制到装有 Access Manager 的服务器。
- 2 打开 Access Manager 的管理控制台。
- 3 要导入证书，请单击[安全性 > NIDP 可信证书存储区](#)。
- 4 单击[添加](#)。
- 5 从[添加对话框 > 导入](#)中选择“可信根”。
- 6 选择要导入的根证书，然后单击[确定](#)。
- 7 确保 OSP 能够识别来自 SAML 的鉴定声明。

有关详细信息，请参见第 18.4.2 节“[创建 SAML 的属性集](#)”（第 182 页）。

18.3 将 Identity Manager 配置为信任 Access Manager

对于鉴定请求，Identity Manager 需要使用 SAML 元数据的 URL 来重定向用户。默认情况下，Access Manager 使用以下 URL 来储存 SAML 元数据：

`https://server:port/nidp/saml2/metadata`

其中，`server:port` 表示 Access Manager 身份服务器。

- 1 （可选）要查看 SAML 元数据的 .xml 文档，请在浏览器中打开该 URL。
如果该 URL 未生成文档，请确保链接正确无误。
- 2 在 OSP 服务器上，运行 RBPM 配置实用程序。有关详细信息，请参见第 11.6.1 节“[运行 Identity Applications 配置实用程序](#)”（第 126 页）。
- 3 在实用程序中选择[鉴定](#)。
- 4 对于[鉴定方法](#)，请指定 **SAML 2.0**。
- 5 对于[元数据 URL](#)，请指定 OSP 用于将鉴定请求重定向到 Access Manager 的 SAML 元数据的 URL。
例如：`https://server:port/nidp/saml2/metadata`
- 6 在[鉴定服务器](#)部分的 **OAuth 服务器主机标识符**设置中，指定托管 OSP 的服务器的 DNS 名称。
- 7 单击[确定](#)保存更改。
- 8 重新启动托管 OSP 的 Tomcat 实例。

18.4 将 Access Manager 配置为与 Identity Manager 配合工作

为确保 Access Manager 将 Identity Manager 识别为可信的服务提供程序，请将 OSP 的元数据文本添加到身份服务器，并配置一个属性集。此过程包括以下活动：

- [第 18.4.1 节“复制 Identity Manager 的元数据”](#)（第 182 页）
- [第 18.4.2 节“创建 SAML 的属性集”](#)（第 182 页）
- [第 18.4.3 节“将 Identity Manager 添加为可信的服务提供程序”](#)（第 183 页）

18.4.1 复制 Identity Manager 的元数据

Access Manager 需要 OSP 的元数据文本。您应该将元数据 .xml 文件的内容复制到可通过 Access Manager 身份服务器打开的文档。

- 1 在浏览器中，浏览到 OSP 元数据的 URL。默认情况下，Identity Manager 使用以下 URL：

```
https://server:port/osp/a/idm/auth/saml2/spmetadata
```

其中，`server:port` 表示托管 OSP 的 Tomcat 服务器。

- 2 查看 `spmetadata.xml` 文件的页面来源。
- 3 将该文件的内容复制到可在[将 Identity Manager 添加为可信的服务提供程序](#)（第 183 页）中访问的文档。

18.4.2 创建 SAML 的属性集

为确保 SAML 能够在 Access Manager 与 OSP 之间执行声明交换，请在 Access Manager 中创建一个属性集。属性集为交换提供了一个通用命名方案。OSP 会查找用于标识声明主题的属性值。默认情况下，该属性为 `mail`。

有关详细信息，请参见《[NetIQ Access Manager Administration Guide](#)》（NetIQ Access Manager 管理指南）中的“[Configuring Attribute Sets](#)”（配置属性集）。

- 1 打开 Access Manager 的管理控制台。
- 2 单击设备 > 身份服务器 > 共享设置 > 属性集 > 新建。
- 3 指定属性集的名称。例如：IDM SAML Attributes。
- 4 单击下一步，然后单击新建。
- 5 对于本地属性，请选择 **Ldap 属性：mail [LDAP 属性配置文件]**。
- 6 对于远程属性，请指定 `mail`。
- 7 单击确定，然后单击完成。

18.4.3 将 Identity Manager 添加为可信的服务提供程序

配置 Access Manager 以将 Identity Manager 识别为可信的服务提供程序。有关详细信息，请参见《[NetIQ Access Manager Administration Guide](#)》（NetIQ Access Manager 管理指南）中的“[Creating a Trusted Service Provider for SAML 2.0](#)”（为 SAML 2.0 创建可信的服务提供程序）。

- 1 打开 Access Manager 的管理控制台。
- 2 单击设备 > 身份服务器 > 编辑 > SAML 2.0。
- 3 单击新建 > 服务提供程序。
- 4 对于提供程序类型，请指定一般。
- 5 对于源，请指定元数据文本。
- 6 在文本字段中，粘贴您在[复制 Identity Manager 的元数据](#)（第 182 页）中复制的 spmetadata.xml 文件内容。
- 7 指定新 OSP 服务提供程序的名称。
- 8 单击“下一步”，然后单击“完成”。
- 9 在 SAML 2.0 选项卡上，选择您在步骤 7 中创建的 OSP 服务提供程序。
- 10 单击属性。
- 11 选择您在[创建 SAML 的属性集](#)（第 182 页）中创建的属性集。例如：IDM SAML Attributes。
- 12 将可用于 OSP 服务提供程序集的属性移至页面左侧的[鉴定时发送](#)面板中。
移至[鉴定时发送](#)面板中的属性就是您在鉴定期间要获取的属性。
- 13 单击确定两次。
- 14 要更新身份服务器，请单击设备 > 身份服务器 > 更新 > 更新所有配置。

18.5 更新 Access Manager 的登录页面

Access Manager 的默认登录页面使用 HTML iFrame 元素，这些元素与 Identity Applications 所用的元素相冲突。本节说明了如何通过创建 Access Manager 的新登录方法和协定来消除该冲突。本节提到的 .jsp 文件默认位于 /opt/novell/idm/apps 目录中。

有关详细信息，请参见《[NetIQ Access Manager Administration Guide](#)》（NetIQ Access Manager 管理指南）中的“[Customizing the Identity Server Login Page](#)”（自定义身份服务器登录页面）。

- 1 根据 [TID 7004020](#) 和 [TID 7018468](#) 的内容修改 top.jsp 文件。
- 2 （可选）为进行备份，请复制 login.jsp 文件并进行重命名。例如，将其重命名为 idm_login.jsp。
- 3 打开 Access Manager 的管理控制台。
- 4 要创建新的登录方法，请完成以下步骤：
 - 4a 单击设备 > 身份服务器 > 编辑 > 本地 > 方法。
 - 4b 单击新建，然后指定新方法的显示名称。例如：IDM Name/Password。
 - 4c 对于类，请指定 Name/Password-Form。
 - 4d 对于用户存储区，请指定身份库作为 LDAP 用户存储区。

4e 在属性部分中，单击**新建**，然后指定以下属性：

名称	值
JSP	idm_login
MainJSP	true

4f 单击**确定**。

5 要创建使用新登录方法的协定，请完成以下步骤：

5a 单击**协定 > 新建**。

5b 在**配置**选项卡中，指定新协定的**显示名称**。例如：IDM Name/Password。

5c 对于 **URI**，指定 name/password/uri/idm。

5d 在**方法**下，添加您在**步骤 4**中创建的方法。例如：IDM Name/Password。

5e 在**鉴定卡**选项卡中，指定卡的 **ID**。例如：IDM_NamePassword。

5f 指定卡的图像。

5g 单击**确定**。

6 要指定系统处理新鉴定协定方式的默认值，请完成以下步骤：

6a 在**本地**选项卡上，单击**默认值**。

6b 对于“用户存储区”，指定“身份库”作为 LDAP 用户存储区。

6c 对于**鉴定协定**，指定您在**步骤 5**中创建的协定。例如：IDM Name/Password-Form。

6d 单击**确定**。

7 要更新身份服务器，请单击**设备 > 身份服务器 > 更新 > 更新所有配置**。

19 校验是否可对 Identity Applications 进行单点登录访问

在安装 Identity Applications 并配置单点登录设置后，您应校验是否能够登录各个应用程序，并在不注销的情况下切换不同的应用程序。默认情况下，应用程序会在 URL 链接中使用以下后缀：

- ♦ Identity Applications 管理：/idmadmin
- ♦ Identity Manager 仪表板：/idmdash
- ♦ User Application：/IDMProv
- ♦ Identity Reporting：/IDMRPT

要自定义后缀，请使用 RBPM 配置实用程序。有关详细信息，请参见[第 11.6 章“配置 Identity Applications 的设置”](#)（第 126 页）。

要校验单点登录功能，请执行以下操作：

- 1 在 Identity Applications 服务器上的新浏览器窗口中，输入仪表板的 URL：

```
https://server:port/idmdash
```

请不要登录到仪表板。

- 2 在浏览器中，浏览到 User Application：

```
https://server:port/IDM-context
```

- 3 校验 User Application 是否显示[步骤 1](#)中所示的同一个登录页面。
- 4 登录 User Application。
- 5 单击右上角的[主页](#)图标，然后校验您是否不必再次登录即可访问仪表板。

20 使用 SSL 进行安全通讯

Identity Applications 和 Identity Reporting 使用 HTML 表单进行鉴定。因此，登录过程可能会暴露用户身份凭证。NetIQ 建议您启用 SSL 协议来保护敏感信息。SSL 协议可确保在 Identity Manager 各组件之间处理的通讯是安全的。

您必须拥有证书才能将 Tomcat 服务器配置为使用 SSL 进行通讯。可通过两种方法获取证书：

- 外部可信的证书颁发机构 (CA) 颁发的证书
- 自我签名证书

安装程序会使用身份库颁发的证书，自动为 Identity Applications 与 Identity Reporting 组件配置安全连接 (HTTPS)。对于生产环境，建议您使用外部证书颁发机构颁发的证书。

20.1 确保 SSL 连接的核对清单

为确保在 Identity Applications、Identity Reporting、SSPR 和 OSP 之间进行安全连接，NetIQ 建议您执行以下核对清单中的步骤：

	核对清单项目
<input type="checkbox"/>	1. 使用密钥存储区来储存鉴定证书。有关详细信息，请参见第 20.2 节“创建密钥存储区和证书签名请求”（第 188 页）。
<input type="checkbox"/>	2. （视情况而定）可以在您的环境中使用自我签名证书或外部 CA 颁发的证书。有关详细信息，请参见第 20.4 节“使用自我签名证书启用 SSL”（第 190 页）。对于生产环境，则建议使用外部 CA 颁发的证书。
<input type="checkbox"/>	3. （视情况而定）在生产环境中导入签名的证书。有关详细信息，请参见第 20.3 节“使用外部 CA 签名的证书启用 SSL”（第 189 页）。
<input type="checkbox"/>	4. 配置鉴定服务器、Identity Applications 和 Identity Reporting，以支持 SSL 通讯。有关详细信息，请参见第 20.6 节“更新应用程序服务器的 SSL 设置”（第 195 页）和第 20.7 节“在配置实用程序中更新 SSL 设置”（第 196 页）。

20.2 创建密钥存储区和证书签名请求

密钥存储区是一个 Java 文件，其中包含加密密钥，有时还包含安全性证书。要创建密钥存储区，可以使用 JRE 中提供的 Java Keytool 实用程序。您可以创建 .jks 文件，将证书生成到密钥存储区中。每个证书都与一个唯一的别名关联。将密钥存储区放置在支持 Identity Applications 和 Identity Reporting 的应用程序服务器的 conf 目录中。

默认情况下，安装程序会在 /opt/netiq/idm/apps/tomcat/conf 中创建名为 tomcat.ks 的密钥存储区，然后使用此密钥存储区来配置 https 连接。如果您创建了同名的密钥存储区文件，请替换此目录中的此密钥存储区文件。

- 1 在命令提示符中，导航到部署了 Identity Applications 的应用程序服务器安装的 conf 目录。例如，
/opt/netiq/idm/apps/tomcat/conf。

tomcat/conf 路径是安装于 Tomcat 上的 Identity Applications 的默认路径。该路径可能会有所不同，具体取决于应用程序和 Tomcat 的安装方式。

- 2 使用以下命令设置用于创建密钥存储区的环境路径：

```
cd /opt/netiq/idm/apps/tomcat/conf
export PATH=/opt/netiq/common/jre/bin:$PATH
```

- 3 使用以下命令创建密钥存储区：

```
keytool -genkey -alias keystore_name -keyalg RSA -keystore
keystore_name.keystore -validity 3650 -keysize 2048
```

例如：

```
keytool -genkey -alias IDMkey -keyalg RSA -keystore IDMkey.keystore -validity
3650 -keysize 2048
```

- 4 出现提示时，根据以下注意事项指定参数值：

- ◆ 对于名字和姓氏，请指定服务器的完全限定名称。例如：

```
MyTomcatServer.NetIQ.com
```

- ◆ 使用正确的拼写。如果拼错了任何单词，则从签名机构生成签名的证书时，您将会看到错误。

- 5（可选）创建一个简单的文本文件，用于保存您为参数值提供的信息副本。

保存此信息可帮助确保在向签名机构提出申请以及导入证书时提供相同的信息。

- 6 将密钥存储区文件复制到已部署 Identity Manager 组件和 SSPR 的每个应用程序服务器实例的 /tomcat/conf 目录。

- 7 要生成 CA 证书请求，请完成以下步骤：

7a 在 conf 目录中，创建名为 your_request.csr 的简单文本文件。例如：IDMcertrequest.csr。

7b 运行以下命令：

```
keytool -certreq -v -alias keystore_name -file your_request.csr -keypass
keystore_password -keystore your.keystore -storepass your_password
```

例如：

```
keytool -certreq -v -alias IDMkey.keystore -file IDMcertrequest.csr -
keypass IDMkeypass -keystore IDMkey.keystore -storepass IDMpass
```

当您运行该命令时，Keytool 实用程序将在 .csr 文件中填入用于请求证书的相应数据。

- 8 (视情况而定) 要获取签名的证书, 请将 .csr 文件提交给有效的证书颁发机构。
- 9 将证书复制到应用程序服务器的配置目录中。
例如, /opt/netiq/idm/apps/tomcat/conf。
- 10 停止 Tomcat。

创建密钥存储区并生成 CA 证书请求后, 请遵循以下过程将证书导入密钥存储区:

- 对于外部 CA 签名的证书, 请参见第 20.3 节“使用外部 CA 签名的证书启用 SSL”(第 189 页)。
- 对于自我签名证书, 请参见第 20.4 节“使用自我签名证书启用 SSL”(第 190 页)。

20.3 使用外部 CA 签名的证书启用 SSL

对于生产环境, 请使用有效证书颁发机构颁发的签名证书。本节介绍了如何将签名的证书导入 Identity Applications 的默认 Tomcat 应用程序服务器。

此过程假设您已从有效的证书颁发机构获取了一个签名证书。有关详细信息, 请参见第 20.2 节“创建密钥存储区和证书签名请求”(第 188 页)。

要使用签名的证书和 SSL, 请执行以下操作:

- 1 将证书复制到应用程序服务器的配置目录中。例如, /opt/netiq/idm/apps/tomcat/conf。
- 2 要将根证书转换为 DER 格式, 请完成以下步骤:
 - 2a 双击 conf 目录中储存的证书。
 - 2b 在“证书”对话框中, 单击**证书路径**。
 - 2c 选择您从签名机构收到的根证书。
 - 2d 单击**查看证书**。
 - 2e 单击**细节 > 复制到文件**。
 - 2f 在导出证书向导中, 单击**下一步**。
 - 2g 选择**适用于 X.509 的 DER 编码二进制文件 (.CER)**, 然后单击**下一步**。
 - 2h 创建一个新文件用于储存设置了新格式的证书, 并将该文件储存在应用程序服务器的 conf 目录中。
例如, /opt/netiq/idm/apps/tomcat/conf。
 - 2i 单击**完成**。
- 3 要导入转换的证书, 请完成以下步骤:
 - 3a 在命令提示符中, 浏览到应用程序服务器的 conf 目录。
 - 3b 输入下面的命令:

```
keytool -import -trustcacerts -alias root -keystore your.keystore -file  
yourRootCA.der
```

例如:

```
keytool -import -trustcacerts -alias root -keystore IDMkey.keystore -file  
IDMTESTREE.der
```

注释: 您必须指定 **root** 作为您的别名。

导入证书后，服务器会显示证书已添加到密钥存储区。

3c 使用以下命令校验是否已将签名的证书正确导入到 conf 目录中：

```
keytool -list -v -alias root -keystore your.keystore
```

例如：

```
keytool -list -v -alias root -keystore IDMkey.keystore
```

服务器会列出您的证书。

- 4 建议您将签名的证书导入到 idm.jks。这是一个集中式密钥存储区，用于储存供 Identity Applications 和 Identity Reporting 使用的所有证书。例如：

```
keytool -import -trustcacerts -alias root -keystore /opt/netiq/idm/apps/tomcat/  
conf/idm.jks -file IDMTTESTTREE.der
```

- 5 更新应用程序服务器的 SSL 设置，请参见第 20.6 节“更新应用程序服务器的 SSL 设置”（第 195 页）。
- 6 在配置实用程序中更新 SSL 设置。有关详细信息，请参见第 20.7 节“在配置实用程序中更新 SSL 设置”（第 196 页）。
- 7 更新 Self Service Password Reset 的 SSL 设置。有关详细信息，请参见第 20.8 节“更新 Self Service Password Reset 的 SSL 设置”（第 197 页）
- 8 重新启动 Tomcat。

20.4 使用自我签名证书启用 SSL

如果您想要在测试环境中使用自我签名证书（因为与从有效机构获取签名证书相比，这种类型的证书更容易获得），请参阅本节。

- 第 20.4.1 节“导出证书颁发机构”（第 190 页）
- 第 20.4.2 节“生成自我签名证书”（第 191 页）

20.4.1 导出证书颁发机构

您可以使用 iManager 从 eDirectory 服务器导出证书颁发机构 (CA)，以生成自我签名证书。

- 1 使用 eDirectory 管理员的用户名和口令登录 iManager。
- 2 单击“管理”>“修改对象”。
- 3 在安全性容器中，浏览到名为 *TreeName* CA.Security 的 CA 对象。例如：IDMTTESTTREE CA.Security。
- 4 单击**确定**。
- 5 单击**证书 > 自我签名证书**。
- 6 选择要使用的自我签名证书。
示例：**自我签名证书 RSA**
 - 6a 选中**自我签名证书 RSA**。
 - 6b 单击**验证**。
- 7 单击**导出**。

- 8 清除导出私用密钥。
- 9 单击**导出格式 > DER**。
- 10 单击**下一步**。
- 11 单击**保存导出的证书**。
- 12 单击**保存文件**。

iManager 会将该文件保存为 *TreeName* cert.der。例如：IDMTESTREE cert.der。

- 13 单击**关闭**。
- 14 将证书复制到应用程序服务器的配置目录中 (cert.der)。

例如， /opt/netiq/idm/apps/tomcat/conf。

- 15 要导入根证书，请完成以下步骤：

- 15a 在命令提示符中，使用以下命令导航到应用程序服务器的 conf 目录：

```
keytool -import -trustcacerts -alias root -keystore <keystore  
file>.keystore -file exported_certificate_filename.der
```

示例：

```
keytool -import -trustcacerts -alias root -keystore IDMkey.keystore -file  
cert.der
```

注释：您必须指定 **root** 作为您的别名。

导入证书后，服务器会显示**证书已添加到密钥存储区**。

- 15b 建议您将根证书也导入到 Java cacerts 位置。

例如：

```
keytool -import -trustcacerts -alias root -keystore /opt/netiq/common/jre/  
lib/security/cacerts -file cert.der
```

- 15c 使用以下命令校验是否已将签名的证书正确导入到 conf 目录中：

```
keytool -list -v -alias root -keystore your.keystore
```

例如：

```
keytool -list -v -alias root -keystore IDMkey.keystore
```

服务器会列出证书。

20.4.2 生成自我签名证书

在生成自我签名证书之前，请确保您有一个密钥存储区和证书请求文件。有关详细信息，请参见第 20.2 节“创建密钥存储区和证书签名请求”（第 188 页）

- 1 登录到 iManager。
- 2 浏览到**证书服务器 > 颁发证书**。
- 3 浏览到第 20.2 节“创建密钥存储区和证书签名请求”（第 188 页）的步骤 7 中创建的 .csr 文件。
示例：IDMcertrequest.csr
- 4 单击**下一步两次**。
- 5 对于证书类型，请单击**未指定**。

6 单击**下一步**两次。

iManager 会将文件保存为 `csr_request_name.der`。示例：`IDMcertrequest.der`

7 将证书复制到应用程序服务器的配置目录中 (`IDMcertrequest.der`)。

例如，`/opt/netiq/idm/apps/tomcat/conf`。

8 要导入生成的自我签名证书，请完成以下步骤：

8a 在命令提示符中，使用以下命令导航到应用程序服务器的 `conf` 目录：

```
keytool -import -alias keystore_name -keystore <keystore_file> -file  
<signed_certificate_filename>.der
```

示例：

```
keytool -import -alias IDMkey -keystore IDMkey.keystore -file  
IDMcertrequest.der
```

注释：必须指定密钥存储区名称作为别名。

导入证书后，服务器会显示**证书已添加到密钥存储区**。

8b 建议您将自我签名证书也导入到 Java cacerts 位置。

例如：

```
keytool -import -alias IDMkey -keystore  
/opt/netiq/common/jre/lib/security/cacerts -file IDMcertrequest.der
```

8c 使用以下命令校验是否已将签名的证书正确导入到 `conf` 目录中：

```
keytool -list -v -alias keystore_name -keystore your.jks
```

例如：

```
keytool -list -v -alias IDMkey -keystore IDMkey.jks
```

服务器会列出证书。

9 更新应用程序服务器的 SSL 设置。有关详细信息，请参见 [第 20.6 节“更新应用程序服务器的 SSL 设置”](#)（第 195 页）。

10 在配置实用程序中更新 SSL 设置。有关详细信息，请参见 [第 20.7 节“在配置实用程序中更新 SSL 设置”](#)（第 196 页）。

11 更新 Self Service Password Reset 的 SSL 设置。有关详细信息，请参见 [第 20.8 节“更新 Self Service Password Reset 的 SSL 设置”](#)（第 197 页）

12 重新启动 Tomcat。

20.5 在 Sentinel 与 Identity Manager 组件之间启用 SSL

您可以创建并导出自我签名的服务器证书，以确保在 Sentinel 与 Identity Manager 组件之间进行安全通讯。请使用有效证书颁发机构颁发的签名证书。

- [第 20.5.1 节“在 Sentinel 与 Identity Manager 引擎 /Remote Loader 之间启用 SSL”](#)（第 193 页）
- [第 20.5.2 节“在 Sentinel 与 User Application 之间启用 SSL”](#)（第 194 页）

20.5.1 在 Sentinel 与 Identity Manager 引擎 /Remote Loader 之间启用 SSL

- 1 要创建新证书，请完成以下步骤：
 - 1a 登录到 iManager。
 - 1b 单击 **NetIQ 证书服务器 > 创建服务器证书**。
 - 1c 选择相应的服务器。
 - 1d 指定服务器的绰号。
 - 1e 接受其余的证书默认值。
- 2 要将服务器证书导出为 .pfx 格式，请完成以下步骤：
 - 2a 在 iManager 中，选择**目录管理 > 修改对象**。
 - 2b 浏览到关键材料对象 (KMO) 对象并选择该对象。
 - 2c 单击**证书 > 导出**。
 - 2d 指定口令。
 - 2e 将服务器证书另存为 PKCS#12。例如，certificate.pfx。
- 3 使用以下命令将导出的证书中的私用密钥提取到 dxipkey.pem。

```
openssl pkcs12 -in certificate.pfx -nocerts -out dxipkey.pem -nodes
```
- 4 将证书提取到 dxicert.pem 文件。

```
openssl pkcs12 -in certificate.pfx -nokeys -out dxicert.pem
```
- 5 要将**步骤 1** 中创建的 eDirectory 服务器 CA 证书导出为 Base64 格式，请完成以下步骤：
 - 5a 在 iManager 中，浏览到**角色和任务 > NetIQ 证书访问 > 用户证书**。
 - 5b 浏览并选择创建的证书。
 - 5c 单击**导出**。
 - 5d 从下拉菜单中选择 **OU=organizationCA.O=TREENAME** 作为 **CA 证书**。
 - 5e 从下拉菜单中选择 **BASE64 > 导出格式**。
 - 5f 单击**下一步**，然后保存该证书。例如，cacert.b64。
- 6 使用以下命令将 CA 证书导出到密钥存储区：

```
keytool -import -alias < 别名 > -file <b64 文件> -keystore < 密钥存储区文件 > -noprompt
```

例如：

```
keytool -import -alias trustedroot -file cacert.b64 -keystore idmKeystore.ks -noprompt
```
- 7 要将证书导入到审计连接器的可信证书存储区，请完成以下步骤：
 - 7a 以管理员身份登录到 Sentinel 主界面。
 - 7b 在主 ESM 显示屏幕中，找到审计服务器。
 - 7c 右键单击**审计服务器**，然后单击**编辑**。
 - 7d 在“安全性”选项卡中，选择**严格**。

注释：该选项默认配置为使用**开放**（不安全）模式，以允许初始连接。但是，当您在生产环境中使用它时，请务必将模式设置为**严格**。

- 7e 单击**导入**，然后浏览到您在**步骤 6** 中创建的证书。例如，idmkeystore.ks。

- 7f 依次单击**打开**和**保存**。
- 7g 重新启动审计服务器。
- 8 重新启动 Identity Manager 服务。

20.5.2 在 Sentinel 与 User Application 之间启用 SSL

- 1 要创建新证书，请完成以下步骤：
 - 1a 登录到 iManager。
 - 1b 单击 **NetIQ 证书服务器** > **创建用户证书**。
 - 1c 选择相应的用户。
 - 1d 为用户指定绰号。
 - 1e 在**创建方法**中选择**自定义**。
 - 1f 接受其余的证书默认值。
 - 1g 单击**下一步**。
 - 1h 在**自定义扩展**中选择**新建 DER 编码的扩展**。
 - 1i 浏览到 \products\RBPM\ext.der 自定义扩展。
 - 1j （可选）指定电子邮件地址。
 - 1k 查看证书参数，然后单击**完成**。
- 2 要导出用户证书，请完成以下步骤：
 - 2a 单击 **NetIQ 证书访问** > **用户证书**。
 - 2b 选择在**步骤 1**中导入的用户证书。
 - 2c 选择有效的用户证书，然后单击**导出**。
 - 2d 指定口令。
 - 2e 将用户证书另存为 PKCS12。例如， certificate.pfx。
- 3 使用以下命令将导出的证书中的私用密钥提取到 key.pem 文件。

```
openssl pkcs12 -in certificate.pfx -nocerts -out key.pem -nodes
```
- 4 将证书提取到 cert.pem 文件。

```
openssl pkcs12 -in certificate.pfx -nokeys -out cert.pem
```
- 5 停止 User Application。
- 6 将私用密钥和证书添加到 configupdate 实用程序。
 - 6a 打开 configupdate 实用程序。
 - 6b 单击**显示高级选项**。
 - 6c 在 **NetIQ Sentinel 数字签名证书**字段中，复制 cert.pem。
 - 6d 在 **NetIQ Sentinel 数字签名私用密钥**字段中，浏览到私用密钥 (key.pem) 的提取位置，然后导入密钥。
 - 6e 保存在 configupdate 实用程序中所作的更改。
- 7 重新启动 User Application。

8 要将步骤 1 中创建的 eDirectory 服务器 CA 证书导出为 Base64 格式，请完成以下步骤：

8a 在 iManager 中，浏览到角色和任务 > NetIQ 证书访问 > 用户证书。

8b 选择创建的证书。

8c 单击导出并清除“导出私用密钥”复选框。

8d 从下拉菜单中选择 **BASE64 > 导出格式**。

8e 单击下一步，然后保存该证书。例如，cacert.b64。

9 使用以下命令将 CA 证书导出到密钥存储区：

```
keytool -import -alias <alias name> -file cacert.b64 -keystore <keystore file> -noprompt
```

例如：

```
keytool -import -alias trustedroot -file cacert.b64 -keystore idmKeystore.ks -noprompt
```

10 要将证书导入到审计连接器的可信证书存储区，请完成以下步骤：

10a 以管理员身份登录到 Sentinel 主界面。

10b 在主 ESM 显示屏幕中，找到审计服务器。

10c 右键单击**审计服务器**，然后单击**编辑**。

10d 在**安全性**选项卡中，选择**严格**。

注释：该选项默认配置为使用**开放**（不安全）模式，以允许初始连接。但是，当您在生产环境中使用它时，请务必将模式设置为**严格**。

10e 单击**导入**，然后浏览到您在步骤 9 中创建的证书。例如，idmKeystore.ks。

10f 依次单击**打开**和**保存**。

10g 重新启动审计服务器。

11 重新启动 User Application。

20.6 更新应用程序服务器的 SSL 设置

安装程序会自动配置托管 Identity Applications 和 Identity Reporting 的应用程序服务器，以支持 SSL 通讯。它默认会在位于 /opt/netiq/idm/apps/tomcat/conf/ 目录中的 server.xml 文件中创建连接器。

```
<Connector port="https_port" protocol="org.apache.coyote.http11.Http11NioProtocol"
maxThreads="150" SSLEnabled="true" scheme="https" secure="true" clientAuth="false"
sslProtocol="TLSv1.2" keystoreFile="path_to_keystore_file"
keystorePass="keystore_password" sslEnabledProtocols="TLSv1.2" />
```

其中：

keystoreFile

指定密钥存储区文件（例如，idmaps.keystore 文件）的路径。将该文件放置在 /opt/netiq/idm/apps/tomcat/conf/ 目录中。

keystorePass

指定 tomcat.ks 文件的口令。

您必须校验 server.xml 文件中的密钥存储区口令和密钥存储区文件路径是否正确。

要修改安装提供的值，请执行以下操作：

- 1 如果 Tomcat 正在运行，请将它停止。
- 2 导航到 Tomcat 的 conf 目录（默认为 /opt/netiq/idm/apps/tomcat/conf/）。
- 3 确保 conf 目录中包含密钥存储区文件。例如，tomcat.ks。

如果您要在执行此过程之后再创建密钥存储区文件，请务必使用在此过程中提供的相同文件名。有关详细信息，请参见第 20.2 节“创建密钥存储区和证书签名请求”（第 188 页）。

- 4 在文本编辑器中打开 conf 目录中的 server.xml 文件。
- 5 配置 Tomcat 服务器的 SSL 端口。

例如，SSL 的连接器端口为 8543。

另外，请将 redirectPort 属性更新为 8543 并保存 server.xml。

例如：

```
<Connector port="8543" protocol="HTTP/1.1" maxThreads="150" SSLEnabled="true"
scheme="https" secure="true" clientAuth="false" sslProtocol="TLS"
keystoreFile="/opt/netiq/idm/apps/tomcat/conf/idmapps.keystore"
keystorePass="encrypted_password"
```

- 6 启动 Tomcat。

例如，systemctl start netiq-tomcat.service

20.7 在配置实用程序中更新 SSL 设置

安装程序会自动配置 SSL 设置。要修改安装提供的值，请执行以下操作：

- 1 如果 Tomcat 正在运行，请使用 services.msc 文件将它停止。
例如，systemctl status netiq-tomcat.service。
- 2 导航到默认位于 Identity Applications 安装目录中的 RBPM 配置实用程序。
- 3 在命令提示符处，运行配置实用程序 (configupdate.sh)：

注释：您可能需要等待几分钟，让实用程序启动。

- 4（视情况而定）如果您在 configupdate 实用程序中配置了 SSL，请导航到**鉴定**选项卡，并替换 **SSO 客户端**选项卡中提到的所有引用。

https://<IP address>:<SSL Port number>

例如：

https://192.168.0.1:8543

- 5 单击**鉴定**，然后修改以下设置：

OAuth 服务器 TCP 端口

指定鉴定服务器的端口。

例如：8543

OAuth 服务器正在使用 TLS/SSL

指定您希望鉴定服务器使用 TLS/SSL 协议进行通讯。

可选 TLS/SSL 密钥存储区文件

指定包含鉴定服务器可信证书的 Java JKS 密钥存储区文件的路径和文件名。当鉴定服务器使用 TLS/SSL 协议，并且鉴定服务器的可信证书不在 JRE 可信证书存储区 (cacerts) 中时，将应用此参数。

可选 TLS/SSL 密钥存储区口令

指定用于装载 TLS/SSL 鉴定服务器的密钥存储区文件的口令。

OAuth 密钥存储区文件

指定要用于鉴定的 Java JKS 密钥存储区文件的路径。该密钥存储区文件必须至少包含一个公共 / 私用密钥对。

OAuth 密钥存储区文件口令

指定用于装载 OAuth 密钥存储区文件的口令。

OAuth 使用的密钥的密钥别名

指定要用于生成对称密钥的 OSP 密钥存储区文件中的公共 / 私用密钥对名称。

OAuth 使用的密钥口令密钥

指定鉴定服务器使用的私用密钥的口令。

6 单击 **SSO 客户端**。

7 更新所有 URL 设置，例如**登录页的 URL 链接**和 **OAuth 重定向 URL**。

这些设置指定鉴定服务器完成鉴定后要将浏览器客户端重定向到的绝对 URL。

使用以下格式：https://DNS_name:sslport/path。例如，https://nqserver.testsite:8543/landing/com.netiq.test。

8 保存在配置实用程序中所作的更改。

9 启动 Tomcat。

20.8 更新 Self Service Password Reset 的 SSL 设置

要修改 SSPR 的 SSL 设置，您必须登录该应用程序。

1 在浏览器中，输入您在配置实用程序中为登录页指定的 https URL。例如：https://myserver.host:8543/landing。

2 使用 Identity Applications 的管理员身份凭证进行登录。

应用程序会显示一条警告，指出您需要更改重定向白名单 URL。

3 要更改重定向白名单 URL，请遵循页面上的说明操作。

4 浏览到**设置 > OAuth SSO**。

5 对于所有三个 URL，指定 https 协议和端口。

6 浏览到**设置 > 应用程序**。

7 对于所有三个 URL，指定 https 协议和端口。

8 单击**保存**，然后单击**确定**。

9 校验 Identity Applications 的所有 URL 现在是否都使用了 https 协议。

查错提示

更新 SSPR 的 SSL 设置后，如果您无法访问 SSPR 登录页，请遵循以下步骤在 SSPRConfiguration.xml 文件中更新所需的 URL。

- 1 导航到位于以下路径的 SSPRConfiguration.xml 文件：

```
/opt/netiq/idm/apps/sspr/sspr_data
```

- 2 使用相应的 IP 地址和端口号更新所有 URL。

```
https://<IP address>:<SSL Port number>
```

示例：

```
https://192.168.0.1:8543
```



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：

21 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](#)。

21.1 创建和配置驱动程序集

驱动程序集是一个可容纳多个 Identity Manager 驱动程序的容器。在任何时候，一台服务器上只能有一个驱动程序集处于活动状态。您可以使用 Designer 工具来创建驱动程序集。

要支持将口令同步到身份库的功能，Identity Manager 需要驱动程序集具有口令策略。您可以使用 Identity Manager 中的默认通用口令策略包，也可以根据现有的组织要求创建口令策略。不过，口令策略必须包括 DirMXL-PasswordPolicy 对象。如果身份库中不存在该策略对象，您可以创建该对象。

- ◆ [第 21.1.1 节“创建驱动程序集”](#)（第 201 页）
- ◆ [第 21.1.2 节“将默认口令策略指派给驱动程序集”](#)（第 201 页）
- ◆ [第 21.1.3 节“在身份库中创建口令策略对象”](#)（第 202 页）
- ◆ [第 21.1.4 节“创建自定义口令策略”](#)（第 203 页）
- ◆ [第 21.1.5 节“在身份库中创建默认通知集合对象”](#)（第 203 页）

21.1.1 创建驱动程序集

Designer for Identity Manager 提供了许多设置供您创建和配置驱动程序集。这些设置可让您指定全局配置值、驱动程序集包、驱动程序集已命名口令、日志级别、跟踪级别和 Java 环境参数。有关详细信息，请参见《[NetIQ Designer for Identity Manager Administration Guide](#)》（NetIQ Designer for Identity Manager 管理指南）中的“[Configuring Driver Sets](#)”（配置驱动程序集）。

21.1.2 将默认口令策略指派给驱动程序集

必须将 DirMXL-PasswordPolicy 对象指派给身份库中的每个驱动程序集。Identity Manager 默认通用口令策略包包括此策略对象。默认策略会安装并指派通用口令策略，以控制 Identity Manager 引擎自动为驱动程序生成随机口令的方式。

或者，若要使用自定义口令策略，您必须创建口令策略对象和策略。有关详细信息，请参见[第 21.1.3 节“在身份库中创建口令策略对象”](#)（第 202 页）和[第 21.1.4 节“创建自定义口令策略”](#)（第 203 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。

21.1.3 在身份库中创建口令策略对象

如果身份库中不存在 DirXML-PasswordPolicy 对象，您可以使用 Designer 或 Idapmodify 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 Idapmodify 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 DirXML-PasswordPolicy 对象，请执行以下操作从文件导入属性：

从包含 Idapmodify 实用程序的目录中，输入以下命令：

```
ldapmodify -x -c -h hostname_or_IP_address -p 389 -D "cn=admin,ou=sa,o=system"
-w password -f path_to_ldif_file
```

例如：

```
ldapmodify -x -ZZ -c -h server1.test.com -p 389 -D "cn=admin,ou=sa,o=system" -
w test123 -f /root/dirxmlpasswordpolicy.ldif
```

默认情况下，Idapmodify 实用程序位于 `/opt/novell/eDirectory/bin` 目录中。

21.1.4 创建自定义口令策略

您可以不使用 Identity Manager 中的默认口令策略，而是根据您的组织的需要创建新的策略。口令策略可以指派给整个树结构、分区根容器、容器或特定的用户。为简化管理，NetIQ 建议在树中尽可能高的位置指派口令策略。有关详细信息，请参见《[Password Management 3.3.2 Administration Guide](#)》（Password Management 3.3.2 管理指南）中的“[Creating Password Policies](#)”（创建口令策略）。

注释：您还必须将 DirXML-PasswordPolicy 对象指派给驱动程序集。有关详细信息，请参见第 21.1.3 节“[在身份库中创建口令策略对象](#)”（第 202 页）。

21.1.5 在身份库中创建默认通知集合对象

默认通知集合是一个身份库对象，它包含一套电子邮件通知模板，以及一个用于发送基于模板生成的电子邮件的 SMTP 服务器。如果身份库中不存在默认通知集合对象，请使用 Designer 创建该对象。

- 1 在 Designer 中打开您的项目。
- 2 在“概要”窗格中，展开您的项目。
- 3 右键单击身份库，然后单击身份库属性。
- 4 单击包，然后单击添加包图标。
- 5 选择所有通知模板包，然后单击确定。
- 6 单击应用以通过安装操作来安装包。
- 7 将通知模板部署到身份库。

21.2 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。

21.3 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。

22 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。

- 第 22.1 节 “使用 Self Service Password Reset 进行忘记口令管理”（第 205 页）
- 第 22.2 节 “使用外部系统进行忘记口令管理”（第 207 页）
- 第 22.3 节 “针对分布式环境或群集环境更新仪表板中的 SSPR 链接”（第 208 页）

22.1 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：

- 第 22.1.1 节 “将 Identity Manager 配置为使用 Self Service Password Reset”（第 205 页）
- 第 22.1.2 节 “为 Identity Manager 配置 Self Service Password Reset”（第 206 页）
- 第 22.1.3 节 “锁定 SSPR 配置”（第 206 页）

22.1.1 将 Identity Manager 配置为使用 Self Service Password Reset

本节提供了将 Identity Manager 配置为使用 SSPR 的相关信息。

- 1 登录到安装了 Identity Applications 的服务器。
- 2 运行 RBPM 配置实用程序。有关详细信息，请参见第 11.6.1 节 “运行 Identity Applications 配置实用程序”（第 126 页）。
- 3 在实用程序中，浏览到**鉴定 > 口令管理**。
- 4 对于**口令管理提供程序**，请指定 **SSPR**。
- 5 选择**忘记口令**。
- 6 浏览到 **SSO 客户端 > Self Service Password Reset**。
- 7 对于 **OSP 客户端 ID**，请指定要用于供鉴定服务器识别 SSPR 单点登录客户端的名称。默认值为 **sspr**。
- 8 对于 **OSP 客户端机密**，请指定 SSPR 单点登录客户端的口令。
- 9 对于 **OSP 重定向 URL**，请指定在完成鉴定后，鉴定服务器要将浏览器客户端重定向到的绝对 URL。

使用以下格式：protocol://server:port/path。例如，http://10.10.10.48:8180/sspr/public/oauth。

- 10 保存更改并关闭实用程序。

22.1.2 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 206 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 设置为 true。
- 5 从 SSPR 中注销。
- 6 要使更改生效，请重新启动 Tomcat。

22.1.3 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, 请重新启动 Tomcat。

22.2 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:

- 第 22.2.1 节“指定外部忘记口令管理 WAR 文件”(第 207 页)
- 第 22.2.2 节“测试外部忘记口令配置”(第 208 页)
- 第 22.2.3 节“配置应用程序服务器之间的 SSL 通讯”(第 208 页)

22.2.1 指定外部忘记口令管理 WAR 文件

如果您在安装期间未指定此值, 并想要修改设置, 则您可以使用 RBPM 配置实用程序, 或者以管理员身份在 User Application 中进行更改。

- 1 (视情况而定) 要在 RBPM 配置实用程序中修改设置, 请完成以下步骤:
 - 1a 登录到安装了 Identity Applications 的服务器。
 - 1b 运行 RBPM 配置实用程序。有关详细信息, 请参见第 11.6.1 节“运行 Identity Applications 配置实用程序”(第 126 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, 即可重新定向到指定的链接。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 208 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。

22.2.2 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。

22.2.3 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。

22.3 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。

23 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。

23.1 停止和启动 Identity Manager 驱动程序

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




- ◆ [第 23.1.1 节“停止驱动程序”](#)（第 209 页）
- ◆ [第 23.1.2 节“启动驱动程序”](#)（第 210 页）

23.1.1 停止驱动程序


在修改驱动程序的任何文件之前，必须先停止驱动程序。


- ◆ [使用 Designer 停止驱动程序](#)（第 209 页）
- ◆ [使用 iManager 停止驱动程序](#)（第 209 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**。

23.1.2 启动驱动程序


更新所有 Identity Manager 组件后，重新启动驱动程序。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 210 页）
- 使用 [iManager 启动驱动程序](#)（第 210 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。

24 激活 Identity Manager

当您首次登录时，有些 Identity Manager 组件会自动激活。其他组件则需要通过执行某个过程才能激活。

- 第 24.1 节“安装产品激活身份凭证”（第 213 页）
- 第 24.2 节“查看 Identity Manager 和驱动程序的产品激活”（第 214 页）
- 第 24.3 节“激活 Identity Manager 驱动程序”（第 214 页）
- 第 24.4 节“激活特定的 Identity Manager 组件”（第 214 页）

24.1 安装产品激活身份凭证

NetIQ 建议您使用 iManager 来安装产品激活身份凭证。

注释：对于要激活的每个驱动程序，激活包含驱动程序的集成模块。

- 1 在您购买许可证之后，NetIQ 会向您发送一封电子邮件，其中包含您的客户 ID。在该电子邮件的“订单细节”部分下方，还包含一个链接，指向可获得您的身份凭证的站点。单击该链接可转至该站点。
- 2 单击许可证下载链接，然后完成以下操作之一：
 - ♦ 打开产品激活身份凭证文件，然后将其内容复制到剪贴板。
 - ♦ 保存产品激活身份凭证文件。
 - ♦ 如果选择复制内容，请不要包含任何多余的行或空格。您应从身份凭证的第一个破折号 (-) 开始复制 (----BEGIN PRODUCT ACTIVATION CREDENTIAL)，一直复制到身份凭证的最后一个破折号 (-) (END PRODUCT ACTIVATION CREDENTIAL-----)。
- 3 登录到 iManager。
- 4 选择 **Identity Manager > Identity Manager 概述**。
- 5 要在树型结构中选择一个驱动程序集，请单击浏览图标 (🔍)。
- 6 在 **Identity Manager 概述**页面上，单击包含要激活的驱动程序的驱动程序集。
- 7 在 **驱动程序集概述**页面上，单击**激活 > 安装**。
- 8 选择要激活 Identity Manager 组件的驱动程序集，然后单击**下一步**。
- 9 （视情况而定）如果您之前保存了产品激活身份凭证文件，请指定保存的位置。
- 10 （视情况而定）如果您之前复制了产品激活身份凭证文件的内容，请将这些内容粘贴到文本区域中。
- 11 单击**下一步**。
- 12 单击**完成**。

24.2 查看 Identity Manager 和驱动程序的产品激活

对于每个驱动程序集，您都可以查看为 Identity Manager 引擎服务器和 Identity Manager 驱动程序安装的产品激活身份凭证。您还可以去除激活身份凭证。

注释：为驱动程序集安装了有效的产品激活身份凭证后，驱动程序名称的旁边可能仍然会显示“要求激活”。如果出现这种情况，请重新启动驱动程序。该讯息应该即会消失。

- 1 登录到 iManager。
- 2 单击 **Identity Manager > Identity Manager 概述**。
- 3 要在树型结构中选择一个驱动程序集，请使用浏览图标 (🔍) 和搜索图标 (🔍)。
- 4 在 **Identity Manager 概述** 页面上，单击要查看其激活信息的驱动程序集。
- 5 在 **驱动程序集概述** 页面上，单击 **激活 > 信息**。

可以查看激活身份凭证的文本，或者，如果报告了错误，则可以去除激活身份凭证。

24.3 激活 Identity Manager 驱动程序

激活 Identity Manager 引擎时，同时会激活以下驱动程序：

服务驱动程序	通用驱动程序
数据收集服务	Active Directory
ID 提供程序	eDirectory 的双向驱动程序
受管系统网关	eDirectory
Role and Resource Service	GroupWise 2014
User Application	LDAP
	Lotus Notes

要激活其他 Identity Manager 驱动程序，您必须另外购买 Identity Manager 集成模块，其中可能包含一或多个驱动程序。您每购买一个 Identity Manager 集成模块，就会收到一个产品激活身份凭证。在收到身份凭证后，请执行第 24.1 节“安装产品激活身份凭证”（第 213 页）中所列的过程。有关驱动程序的详细信息，请参见 [Identity Manager 驱动程序文档网站](#)。

24.4 激活特定的 Identity Manager 组件

本节提供有关激活 Identity Manager 特定组件的信息。

- [第 24.4.1 节“激活 Designer”（第 215 页）](#)
- [第 24.4.2 节“激活 Analyzer”（第 215 页）](#)
- [第 24.4.3 节“激活 Sentinel Log Management for IGA”（第 215 页）](#)

24.4.1 激活 Designer

激活 Identity Manager 引擎或 Identity Manager 驱动程序的同时，还会激活 Designer 和 Catalog Administrator。

24.4.2 激活 Analyzer

当您启动未获许可的 Analyzer 透视功能时，Analyzer 会打开激活页面，您可以从中管理 Analyzer 许可证。

注释：如果关闭“激活”对话框，Analyzer 将一直保持锁定状态，直到您提供许可证将它激活。当您准备好添加许可证时，请在项目视图中单击**激活 Analyzer** 打开“激活”对话框。

- 1 启动 Analyzer。
- 2 在 **Analyzer 激活** 窗口中，可以**添加新许可证**，或访问 [Customer Center](#) 以获得许可证。
- 3 （视情况而定）要添加新许可证，请执行以下操作：
 - 3a 单击**添加新许可证**。
 - 3b 在**许可证**窗口中，键入您从 NetIQ 客户关怀入口下载的激活代码，然后单击**确定**。
- 4 （视情况而定）要访问 Customer Center 以获得许可证，请执行以下操作：
 - 4a 单击访问 [Customer Center](#) 以获得许可证。
 - 4b 在 [Micro Focus Customer Center](#) 页面中单击**访问 NetIQ Customer Center**。
 - 4c 浏览到 Analyzer 许可证并加以选择。
 - 4d 复制激活代码，然后关闭客户关怀入口。
 - 4e 在**许可证**窗口中键入激活代码，然后单击**确定**。
- 5 在 **Analyzer 激活** 窗口中，查看您刚刚安装的许可证的细节。
- 6 单击**确定**开始使用 Analyzer。

24.4.3 激活 Sentinel Log Management for IGA

您可在安装 Sentinel 时添加许可证。本节提供有关在安装 Sentinel 后添加许可证密钥的信息。

如果您使用的是默认安装的评估许可证密钥，则必须在评估密钥失效前激活 Sentinel，以免 Sentinel 功能中断。有关如何购买许可证的信息，请访问 [Identity Manager 产品网站](#)。

您可以使用 Sentinel 主界面或通过命令行添加许可证密钥。

- 使用 [Sentinel 主界面添加许可证密钥](#)（第 215 页）
- [通过命令行添加许可证密钥](#)（第 216 页）

使用 Sentinel 主界面添加许可证密钥

- 1 以管理员身份登录到 Sentinel 主界面。
- 2 单击**关于 > 许可证**。
- 3 在许可证部分中，单击**添加许可证**。

4 在**密钥**字段中指定许可证密钥。

指定许可证后，会在预览部分显示以下信息：

- ◆ **功能**：可通过该许可证获得的功能。
- ◆ **主机名**：此字段仅供 NetIQ 内部使用。
- ◆ **序列**：此字段仅供 NetIQ 内部使用。
- ◆ **EPS**：许可证密钥中内置的事件速率。超出此速率，Sentinel 会生成警告，但会继续收集数据。
- ◆ **失效日期**：许可证的过期日期。您必须在失效日期之前指定一个有效的许可证密钥，以避免功能中断。

5 单击**保存**。

通过命令行添加许可证密钥

如果您使用的是 Sentinel 传统安装，则可以使用 softwarekey.sh 脚本通过命令行来添加许可证。

1 以 root 用户身份登录到 Sentinel 服务器。

2 切换到 /opt/novell/sentinel/bin 目录。

3 输入以下命令来更改为 novell 用户：

```
su novell
```

4 指定以下命令来运行 softwarekey.sh 脚本。

```
./softwarekey.sh
```

5 输入 **1** 以插入许可证密钥。

6 指定许可证密钥，然后按 **Enter**。

升级 Identity Manager

本部分提供有关升级 Identity Manager 组件的信息。

25 准备升级 Identity Manager

本章提供的信息可帮助您准备好将 Identity Manager 解决方案升级到最新版本。您可以根据目标计算机，使用可执行文件、二进制文件或文本模式升级 Identity Manager 的大部分组件。要执行升级，您必须下载并解压缩或解包 Identity Manager 安装包。

- 第 25.1 节“Identity Manager 的升级核对清单”（第 219 页）
- 第 25.2 节“了解升级过程”（第 220 页）
- 第 25.3 节“支持的升级路径”（第 221 页）
- 第 25.4 节“备份当前配置”（第 224 页）

25.1 Identity Manager 的升级核对清单

要执行升级，NetIQ 建议您完成以下核对清单中的步骤。

	核对清单项目
<input type="checkbox"/>	1. 了解升级过程。有关详细信息，请参见第 25.2 节“了解升级过程”（第 220 页）。
<input type="checkbox"/>	2. 查看将 Identity Manager 升级到 4.7 的支持路径。有关支持的升级路径信息，请参见第 25.3 节“支持的升级路径”（第 221 页）。
<input type="checkbox"/>	3. 确保您拥有升级 Identity Manager 的安装包。
<input type="checkbox"/>	4. 了解 Identity Manager 各组件之间的交互。有关详细信息，请参见第 I 部分“简介”（第 15 页）。
<input type="checkbox"/>	5. 确保您的计算机符合较新版 Identity Manager 的硬件和软件先决条件。有关详细信息，请参见第 5.9 章“准备安装”（第 41 页）和要升级的目标版本的《发行说明》。
<input type="checkbox"/>	6. 备份当前的项目、驱动程序配置和数据库。有关详细信息，请参见第 25.4 节“备份当前配置”（第 224 页）。
<input type="checkbox"/>	7. 将 Designer 升级到最新版本。有关详细信息，请参见第 26.2 节“升级 Designer”（第 227 页）。
<input type="checkbox"/>	8. 将 Sentinel Log Management for IGA 升级到最新版本。有关详细信息，请参见第 26.6.3 节“升级 Sentinel Log Management for IGA”（第 243 页）。
<input type="checkbox"/>	9. 在运行 Identity Manager 的服务器上，将身份库 (eDirectory) 升级到 9.1。这是 Identity Manager 引擎升级过程的第一步。有关详细信息，请参见第 26.3.1 节“升级身份库”（第 228 页）。 升级 eDirectory 会停止 ndsd，而后者又会停止所有驱动程序。有关详细信息，请参见《NetIQ eDirectory Installation Guide》（NetIQ eDirectory 安装指南）。
<input type="checkbox"/>	10. 停止与安装了 Identity Manager 引擎的服务器关联的驱动程序。有关详细信息，请参见第 23.1.1 节“停止驱动程序”（第 209 页）。

	核对清单项目
<input type="checkbox"/>	11. 升级 Identity Manager 引擎。有关详细信息，请参见第 26.3 节“升级 Identity Manager 引擎”（第 228 页）。 注释： 如果要将 Identity Manager 引擎迁移到新服务器，可以使用与当前 Identity Manager 服务器上相同的 eDirectory 复本。有关详细信息，请参见第 29.4 节“将 Identity Manager 引擎迁移到新服务器”（第 258 页）。
<input type="checkbox"/>	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，请参见第 26.3.3 节“升级 Remote Loader”（第 229 页）。
<input type="checkbox"/>	13. 将 iManager 升级到 3.1。有关详细信息，请参见第 26.3.4 节“升级 iManager”（第 230 页）。
<input type="checkbox"/>	14. 更新 iManager 插件，使之与 iManager 的版本匹配。有关详细信息，请参见在升级或重安装后更新 iManager 插件（第 231 页）。
<input type="checkbox"/>	15. （视情况而定）如果您使用的是包，请在现有驱动程序上升级包以获取新策略。有关详细信息，请参见第 26.4 节“升级 Identity Manager 驱动程序”（第 231 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。
<input type="checkbox"/>	16. 升级 Identity Applications。有关详细信息，请参见第 26.5 节“升级 Identity Applications”（第 233 页）。
<input type="checkbox"/>	17. 升级 Identity Reporting。有关详细信息，请参见第 26.6 节“升级 Identity Reporting”（第 242 页）。
<input type="checkbox"/>	18. 启动与 Identity Applications 和 Identity Manager 引擎关联的驱动程序。有关详细信息，请参见第 23.1.2 节“启动驱动程序”（第 210 页）。
<input type="checkbox"/>	19. （视情况而定）如果已将 Identity Manager 引擎或 Identity Applications 迁移到某个新服务器，请将该新服务器添加到驱动程序集中。有关详细信息，请参见第 26.8 节“将新服务器添加到驱动程序集”（第 246 页）。
<input type="checkbox"/>	20. （视情况而定）如果您有自定义策略和规则，请恢复自定义设置。有关详细信息，请参见第 26.9 节“将自定义策略和规则恢复到驱动程序”（第 247 页）。
<input type="checkbox"/>	21. 升级 Analyzer。有关详细信息，请参见第 26.7 节“升级 Analyzer”（第 245 页）。
<input type="checkbox"/>	22. 激活已升级的 Identity Manager 解决方案。有关详细信息，请参见第 24 节“激活 Identity Manager”（第 213 页）。

25.2 了解升级过程

当您想要安装现有 Identity Manager 安装的较新版本时，通常可以执行**升级**。但是，如果新版 Identity Manager 不提供现有数据的升级路径，则您必须执行**迁移**。NetIQ 将**迁移**定义为在新服务器上安装 Identity Manager，然后将现有数据迁移到这个新服务器的过程。

在产品评估期或者在激活 Advanced Edition 之后，如果您不想在环境中使用 Advanced Edition 功能，可以**切换**到 Standard Edition。Identity Manager 可让您通过一个简单的过程从 Advanced Edition 切换到 Standard Edition。

从 Advanced Edition 切换到 Standard Edition

Identity Manager 允许您在产品评估期内或激活 Advanced Edition 后从 Advanced Edition 切换到 Standard Edition。

重要：如果您已应用 Advanced Edition 激活码，则不需要切换到 Standard Edition，因为 Standard Edition 的所有功能在 Advanced Edition 中都有提供。仅当您不想在环境中使用任何 Advanced Edition 功能，并且想要缩减 Identity Manager 部署时，才必须切换到 Standard Edition。有关详细信息，请参见 [从 Advanced Edition 切换到 Standard Edition](#)（第 249 页）。

25.3 支持的升级路径

Identity Manager 4.7 支持从 4.6.x 和 4.5.6 版本升级。NetIQ 建议开始升级前先在您当前版本相应的发行说明中查看该信息。

- [第 25.3.1 节“从 Identity Manager 4.6.x 版本升级”](#)（第 221 页）
- [第 25.3.2 节“从 Identity Manager 4.5.x 版本升级”](#)（第 222 页）

25.3.1 从 Identity Manager 4.6.x 版本升级

下表列出了 Identity Manager 4.6.x 版本的组件范围升级路径：

组件	基础版本	升级后的版本
Identity Manager 引擎	4.6.x	<ol style="list-style-type: none">1. 将操作系统升级到支持的版本。2. 将身份库升级到 9.1。3. 将 Identity Manager 引擎升级到 4.7。
Remote Loader/ 扇出代理	4.6.x	安装 4.7 版 Remote Loader/ 扇出代理
Designer	4.6.x	<ol style="list-style-type: none">1. 安装 Designer 4.7。2. 将工作空间从 NCP 转换为 LDAP。 <p>Designer 4.7 基于 LDAP 运行。使用此版本之前，请参见 《NetIQ Identity Manager LDAP Designer 发行说明》。</p>

组件	基础版本	升级后的版本
Identity Applications	4.6.x	<p>升级 Identity Applications 前，请确保身份库和 Identity Manager 引擎已分别升级到 9.1 和 4.7。</p> <ol style="list-style-type: none"> 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，请参见第 8.5.3 节“Identity Applications 的系统要求”（第 75 页）。 3. （视情况而定）如果 SSPR 安装在单独的计算机上，请将该组件升级到 4.7 版本。 4. 更新 User Application 驱动程序以及角色和资源驱动程序包。 5. 将 Identity Applications 升级到 4.7。 6. 停止 Tomcat。
Identity Reporting	4.6.x	<ol style="list-style-type: none"> 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，请参见第 8.6.4 节“Identity Reporting 的系统要求”（第 80 页）。 3. 将 SLM for IGA 升级到支持的版本。 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 4.7。 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您所用版本的发行说明中查看该信息：

- 《[NetIQ Identity Manager 4.6 Service Pack 2 Release Notes](#)》（NetIQ Identity Manager 4.5 SP4 发行说明）
- 《[NetIQ Identity Manager 4.6 Service Pack 1 Release Notes](#)》（NetIQ Identity Manager 4.5 SP4 发行说明）
- 《[NetIQ Identity Manager 4.6 发行说明](#)》

25.3.2 从 Identity Manager 4.5.x 版本升级

下表列出了 Identity Manager 4.5.x 版本的组件范围升级路径：

组件	基础版本	中间步骤	升级后的版本
Identity Manager 引擎	装有 eDirectory 8.8.8.x（其中 x 为 3 至 9）的 Identity Manager 4.5.x（其中 x 为 0 至 5）	应用 4.5.6 增补程序	<ol style="list-style-type: none"> 1. 将操作系统升级到支持的版本。 2. 将身份库升级到 9.1。 3. 将 Identity Manager 引擎升级到 4.7。
Remote Loader/ 扇出代理	4.5.x（其中 x 为 0 至 5）	应用 4.5.6 增补程序	安装 4.7 版 Remote Loader/ 扇出代理。
Designer	4.5.x（其中 x 为 0 至 5）	应用 4.5.6 增补程序	<ol style="list-style-type: none"> 1. 安装 Designer 4.7。 2. 将工作空间从 NCP 转换为 LDAP。 <p>Designer 4.7 基于 LDAP 运行。使用此版本之前，请参见 《NetIQ Identity Manager LDAP Designer 发行说明》。</p>
Identity Applications	4.5.x（其中 x 为 0 至 5）	<ul style="list-style-type: none"> ◆ 如果您使用的是 JBoss 或 Websphere，请迁移到 Tomcat 应用程序服务器。 ◆ 应用 4.5.6 增补程序。 	<p>升级 Identity Applications 前，请确保身份库和 Identity Manager 引擎已分别升级到 9.1 和 4.7。</p> <ol style="list-style-type: none"> 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，请参见第 8.5.3 节“Identity Applications 的系统要求”（第 75 页）。 4. （视情况而定）如果 SSPR 安装在单独的计算机上，请将该组件升级到 4.7 版本。 5. 将 Identity Applications 升级到 4.7。 6. 停止 Tomcat。

组件	基础版本	中间步骤	升级后的版本
Identity Reporting	4.5.x（其中 x 为 0 至 5）	<ul style="list-style-type: none"> 如果您使用的是 JBoss 或 Websphere，请迁移到 Tomcat 应用程序服务器。 应用 4.5.6 增补程序。 	<ol style="list-style-type: none"> 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，请参见第 8.6.4 节“Identity Reporting 的系统要求”（第 80 页）。 3. 将事件审计服务数据迁移到支持版本的 PostgreSQL 或 Oracle 数据库。 4. 安装 SLM for IGA。 5. 更新数据收集服务和受管理服务网关驱动程序包。 6. 将 Identity Reporting 迁移到 4.7。有关详细信息，请参见第 29.8 节“迁移 Identity Reporting”（第 262 页）。 7. （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您所用版本的发行说明中查看该信息：

- 《[NetIQ Identity Manager 4.5 Service Pack 6 Release Notes](#)》（NetIQ Identity Manager 4.5 SP4 发行说明）
- 《[NetIQ Identity Manager 4.5 Service Pack 5 Release Notes](#)》（NetIQ Identity Manager 4.5 SP5 发行说明）
- 《[NetIQ Identity Manager 4.5 Service Pack 4 Release Notes](#)》（NetIQ Identity Manager 4.5 SP4 发行说明）
- 《[NetIQ Identity Manager 4.5 Service Pack 3 Release Notes](#)》（NetIQ Identity Manager 4.5 SP4 发行说明）
- 《[NetIQ Identity Manager 4.5 Service Pack 2 Release Notes](#)》（NetIQ Identity Manager 4.5 SP4 发行说明）
- 《[NetIQ Identity Manager 4.5 Service Pack 1 Release Notes](#)》（NetIQ Identity Manager 4.5 SP4 发行说明）
- 《[NetIQ Identity Manager 4.5 发行说明](#)》

25.4 备份当前配置

在升级之前，NetIQ 建议您先备份 Identity Manager 解决方案的当前配置。您无需再执行其他步骤即可备份 User Application。所有 User Application 配置均储存在 User Application 驱动程序中。您可以通过以下方式创建备份：

- 第 25.4.1 节“导出 Designer 项目”（第 225 页）
- 第 25.4.2 节“导出驱动程序的配置”（第 226 页）

25.4.1 导出 Designer 项目

Designer 项目包含纲要及所有驱动程序配置信息。通过创建 Identity Manager 解决方案项目，您可以一步导出所有驱动程序，而无需为每个驱动程序创建单独的导出文件。

- ◆ [导出当前项目](#)（第 225 页）
- ◆ [通过身份库创建新项目](#)（第 225 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 启动 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**：表示用于向身份库鉴定的用户的 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**。

25.4.2 导出驱动程序的配置


通过创建驱动程序的导出，可备份当前配置。但是，Designer 当前不会创建基于角色的权利驱动程序和策略的备份。使用 iManager 以校验是否具有基于角色的权利驱动程序的导出。

- 使用 Designer 导出驱动程序配置（第 226 页）
- 使用 iManager 创建驱动程序的导出（第 226 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**。

26 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。本章还提供了在执行升级后可能需要执行的步骤。

- [第 26.1 节“升级顺序”](#)（第 227 页）
- [第 26.2 节“升级 Designer”](#)（第 227 页）
- [第 26.3 节“升级 Identity Manager 引擎”](#)（第 228 页）
- [第 26.4 节“升级 Identity Manager 驱动程序”](#)（第 231 页）
- [第 26.5 节“升级 Identity Applications”](#)（第 233 页）
- [第 26.6 节“升级 Identity Reporting”](#)（第 242 页）
- [第 26.7 节“升级 Analyzer”](#)（第 245 页）
- [第 26.8 节“将新服务器添加到驱动程序集”](#)（第 246 页）
- [第 26.9 节“将自定义策略和规则恢复到驱动程序”](#)（第 247 页）

26.1 升级顺序

必须按以下顺序升级 Identity Manager 组件：

1. Designer
2. Sentinel Log Management for IGA
3. 身份库
4. Identity Manager 引擎
5. Remote Loader
6. 扇出代理
7. iManager
8. Identity Applications（适用于 Advanced Edition）
9. Identity Reporting
10. Analyzer

注释：一次只能升级一个组件。

26.2 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 启动 Designer 安装程序。有关详细信息，请参见第 13 章“安装 Designer”（第 163 页）。

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）。

26.3 升级 Identity Manager 引擎

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。

26.3.1 升级身份库

- 1 如第 5.11 节“下载安装文件”（第 47 页）中所述下载 Identity_Manager_4.7_Linux.iso。
- 2 装入下载的 .iso。
- 3 从 .iso 文件的根目录中，导航到 IDVault/setup 目录。
- 4 运行以下命令：

```
./nds-install
```
- 5 接受许可协议并继续安装。
- 6 指定 **adminDN**。例如，cn=admin.ou=sa.o=system。
- 7 当系统提示停止 eDirectory 实例并升级 NICI 时，指定 y。
- 8 指定是否要配置增强型后台鉴定。

注释：如果升级 DIB 失败并且 nds-install 提示运行 ndsconfig 升级，请在运行 nds-install 后运行该升级命令。如果升级后 eDirectory 服务未启动，请运行 ndsconfig 升级命令。有关详细信息，请参见《[NetIQ eDirectory Installation Guide](#)》（NetIQ eDirectory 安装指南）。

26.3.2 升级 Identity Manager 引擎

验证驱动程序是否已停止。有关详细信息，请参见第 23.1.1 节“停止驱动程序”（第 209 页）。

在开始升级过程前，请确保超速缓存文件中没有事件。当您 Identity Manager 引擎升级到 4.7 版本时，引擎安装程序会清理现有 MapDB 驱动程序工作超速缓存文件 (dx*)。不过，您必须在升级驱动程序后，手动去除现有的 MapDB 状态超速缓存文件。否则，驱动程序可能无法启动。以下 Identity Manager 驱动程序使用 MapDB 3.0.5：

- MS Azure
- JDBC
- DCS
- MSGW
- LDAP

- ◆ Salesforce
- ◆ ServiceNow

执行以下步骤来升级 Identity Manager 引擎：

- 1 从 NetIQ 下载网站下载 Identity_Manager_4.7_Linux.iso。
- 2 装入下载的 .iso。
- 3 运行以下命令：
./install.sh
- 4 通读许可协议。
- 5 输入 y 以接受许可协议。
- 6 指定是否要升级 Identity Manager 组件。可用选项有 **y** 和 **n**。
- 7 选择 Identity Manager 引擎。
- 8 指定以下细节：
身份库管理员：指定身份库管理员名称。
身份库管理员口令：指定身份库管理员口令。

26.3.3 升级 Remote Loader

如果您在运行 Remote Loader，则需要升级 Remote Loader 文件。

- 1 创建 Remote Loader 配置文件的备份。
- 2 验证驱动程序是否已停止。有关指导，请参见第 23.1.1 节“停止驱动程序”（第 209 页）。
- 3 停止每个驱动程序的 Remote Loader 服务或守护程序。
 - ◆ **Remote Loader:** `rdxml -config path_to_configfile -u`
 - ◆ **Java Remote Loader:** `dirxml_jremote -config path_to_configfile -u`
- 4 从 NetIQ 下载网站下载 Identity_Manager_4.7_Linux.iso。
- 5 装入下载的 .iso。
- 6 运行以下命令：
./install.sh
- 7 通读许可协议。
- 8 输入 y 以接受许可协议。
- 9 指定是否要升级 Identity Manager 组件。可用选项有 **y** 和 **n**。
- 10 选择 Remote Loader。
- 11 安装完成后，校验配置文件是否包含环境的信息。
- 12 （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。
- 13 启动每个驱动程序的 Remote Loader 服务或守护程序。
 - ◆ **Remote Loader:** `rdxml -config path_to_config_file`
 - ◆ **Java Remote Loader:** `dirxml_jremote -config path_to_config_file`

26.3.4 升级 iManager

通常情况下，iManager 的升级过程会使用 configiman.properties 文件中的现有配置值，例如端口值和授权用户。如果您先前修改了 server.xml 和 context.xml 配置文件，NetIQ 建议您在升级之前先备份这些文件。

在将 iManager 升级到 3.1 之前，请确保您的 eDirectory 版本已升级到 9.1。

升级过程包括以下活动：

- ◆ [升级 iManager](#)（第 230 页）
- ◆ [更新基于角色的服务](#)（第 230 页）
- ◆ [重安装或迁移 Plug-in Studio 的插件](#)（第 231 页）
- ◆ [在升级或重安装后更新 iManager 插件](#)（第 231 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 如[第 5.11 节“下载安装文件”](#)（第 47 页）中所述下载 Identity_Manager_4.7_Linux.iso。
- 2 装入下载的 .iso。
- 3 运行以下命令：

```
./install.sh
```
- 4 通读许可协议。
- 5 输入 y 以接受许可协议。
- 6 指定 iManager 以继续升级。

更新基于角色的服务

第一次使用 iManager 登录到已包含基于角色的服务 (RBS) 集合的 eDirectory 树时，您可能只能看到部分角色信息。此现象是正常的，因为您必须更新一些插件才能让其最新版本在 iManager 上正常运行。NetIQ 建议您将 RBS 模块更新到最新版本，以便您可以查看和使用 iManager 中提供的所有功能。“RBS 配置”表列出了需要更新的 RBS 模块。

请注意，您可能会遇到多个同名的角色。从 iManager 2.5 开始，一些插件开发人员会更改任务 ID 或模块名称，但保留其显示名称不变。此问题导致有些角色可能出现重复，但实际上，两个实例中一个来自旧版本，另一个来自较新的版本。

注释：

- ◆ 在更新或重安装 iManager 时，安装程序不会更新现有的插件。要手动更新插件，请启动 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是否有过期的模块。
- 3（可选）要更新某个模块，请完成以下步骤：
 - 3a 对于要更新的集合，请在[已过期](#)列中选择它的编号。
iManager 会显示已过期模块的列表。
 - 3b 选择要更新的模块。
 - 3c 单击表格顶部的[更新](#)。

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。

- 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。

26.4 升级 Identity Manager 驱动程序

NetIQ 通过包提供新驱动程序内容。您可以在 Designer 中管理、维护和创建包。尽管 iManager 可以识别包，但 Designer 不会保留您在 iManager 中对驱动程序内容所做的任何更改。有关管理包的详细信息，请参见《[NetIQ Designer for Identity Manager Administration Guide](#)》（NetIQ Designer for Identity Manager 管理指南）中的“[Managing Packages](#)”（管理包）。

您可通过以下方式将驱动程序升级到包：

- [第 26.4.1 节“创建新驱动程序”](#)（第 232 页）
- [第 26.4.2 节“用包的内容替换现有内容”](#)（第 232 页）
- [第 26.4.3 节“保留当前内容并通过包添加新内容”](#)（第 232 页）

26.4.1 创建新驱动程序

将驱动程序升级到包的最简单明了的方式是删除现有驱动程序并通过包创建新驱动程序。在新的驱动程序中添加所有需要的功能。每个驱动程序的步骤都不同。有关说明，请参见 [Identity Manager 驱动程序文档网站](#) 上各个驱动程序的指南。现在驱动程序与之前一样工作，但其内容来自包而不是来自驱动程序配置文件。

26.4.2 用包的内容替换现有内容

如果需要保留驱动程序创建的关联，您无需删除然后重创建驱动程序。您可以保留关联，并用包替换现有的驱动程序内容。

要用包的内容替换现有内容：

- 1 创建驱动程序及驱动程序中所有自定义内容的备份。
有关说明，请参见第 25.4.2 节“导出驱动程序的配置”（第 226 页）。
- 2 在 Designer 中，删除储存在驱动程序内的所有对象。删除储存在驱动程序内的策略、过滤器、权利及所有其他项目。

注释： Designer 提供了自动导入工具用于导入最新的包。您不需要手动将驱动程序包导入到包编目中。

有关详细信息，请参见《*NetIQ Designer for Identity Manager Administration Guide*》（NetIQ Designer for Identity Manager 管理指南）中的“[Importing Packages into the Package Catalog](#)”（将包导入包编目）。

- 3 将最新的包安装到驱动程序中。
这些步骤对每个驱动程序都是特定的。有关说明，请参见 [Identity Manager 驱动程序文档网站](#) 上每个驱动程序的指南。
- 4 将所有自定义策略和规则恢复到驱动程序。有关说明，请参见第 26.9 节“[将自定义策略和规则恢复到驱动程序](#)”（第 247 页）。

26.4.3 保留当前内容并通过包添加新内容

只要包中的功能不与驱动程序的当前功能重叠，就可以保留当前的驱动程序不变，而通过包向驱动程序添加新功能。

在安装包之前，请创建驱动程序配置文件的备份。安装某个包时，该包可能会重写现有策略，从而导致驱动程序停止工作。如果重写了某个策略，您可以导入备份驱动程序配置文件并重创建该策略。

在开始前，请确保任何自定义策略的名称均不同于默认策略。使用新驱动程序文件覆盖驱动程序配置时，会重写现有策略。如果自定义策略的名称不唯一，您将会丢失这些策略。

要通过包向驱动程序添加新内容：

- 1 创建驱动程序及驱动程序中所有自定义内容的备份。
有关说明，请参见第 25.4.2 节“导出驱动程序的配置”（第 226 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。

26.5 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
- ♦ PostgreSQL 数据库

升级后，组件将升级到以下版本：

- ♦ Tomcat – 8.5.27
- ♦ ActiveMQ – 5.15.2
- ♦ Java – 1.8.0_162
- ♦ One SSO Provider – 6.2.1
- ♦ Self-Service Password Reset – 4.2.0.4

本节提供有关以下主题的信息：

- ♦ [第 26.5.1 节“了解升级程序”](#)（第 234 页）
- ♦ [第 26.5.2 节“升级的先决条件和注意事项”](#)（第 234 页）
- ♦ [第 26.5.3 节“系统要求”](#)（第 235 页）
- ♦ [第 26.5.4 节“升级 PostgreSQL 数据库”](#)（第 235 页）
- ♦ [第 26.5.5 节“升级 Identity Applications 的驱动程序包”](#)（第 238 页）
- ♦ [第 26.5.6 节“升级 Identity Applications”](#)（第 238 页）
- ♦ [第 26.5.7 节“升级后任务”](#)（第 239 页）

26.5.1 了解升级程序

升级进程会从现有组件中读取配置值。这些信息包括 ism-configuration.properties、server.xml、SSPRConfiguration 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。

26.5.2 升级的先决条件和注意事项

在执行升级之前，请先查看以下注意事项：

- ♦ **Identity Manager 已升级到版本 4.5.6：**您不能从低于 4.5.6 的版本升级或迁移到版本 4.7。有关如何升级到 Identity Manager 4.7 的详细信息，请参见第 25.3 节“支持的升级路径”（第 221 页）。
- ♦ **系统要求：**升级过程至少需要 3 GB 可用磁盘空间，用于存储当前配置以及升级过程中创建的临时文件。确保服务器具有足够储存备份的空间，另外还有可供升级的可用空间。

如果您已将 Identity Applications 安装在非根分区的其他分区中，请确保该分区具有足够的空间用来储存备份配置。另外，请确保 /tmp 目录具有足够的空间用来储存日志和临时文件。如果此目录不能提供所需的空間，请将 IATEMPDIR 环境变量设置为分区上具有足够可用空间的某个目录。这会重新指示升级程序将文件储存到该目录。

要将 IATEMPDIR 设置为某个目录，请执行以下操作：

1. 打开一个终端，并输入以下命令：

```
export IATEMPDIR=/opt/custom_tmp
```

其中，/opt/custom_tmp 是具有足够可用磁盘空间的目录的路径。

注释：备份 Identity Applications 证书 (cacerts)。

2. 从命令行启动升级程序。

- ♦ **使用 Tomcat 作为应用程序服务器：**此版本的 Identity Manager 仅支持使用 Tomcat 作为应用程序服务器。
如果用于运行 Identity Applications 的应用程序服务器不是 Tomcat，请在执行升级前将该应用程序服务器迁移到 Tomcat。有关详细信息，请参见“从 Websphere 或 JBoss 迁移到 Tomcat”。
- ♦ **数据库平台已升级：**此程序不会升级 Identity Applications 的数据库平台。请手动将当前的数据库版本升级到支持的版本。要升级 PostgreSQL 数据库，请参见第 26.5.4 节“升级 PostgreSQL 数据库”（第 235 页）。
- ♦ **Role and Resource Service 驱动程序包已升级：**有关详细信息，请参见《NetIQ Designer for Identity Manager Administration Guide》（NetIQ Designer for Identity Manager 管理指南）中的“Upgrading Installed Packages”（升级安装的包）。
- ♦ **Self Service Password Reset：**如果要从 SSPR 4.0 升级，请确保您已更新 CATALINA_OPTS 属性，并且 -Dsspr.application.Path 设置为储存 SSPR 配置的文件夹。

例如：

```
export CATALINA_OPTS="-Dsspr.applicationPath=/home/sspr_data"
```

在升级前备份 SSPR LocalDB。要导出或下载 LocalDB，请执行以下步骤：

1. 以管理员身份登录 SSPR 门户。
2. 在页面右上角的下拉菜单中单击配置管理器。

3. 单击 **LocalDB**。
4. 单击 **下载 LocalDB**。

26.5.3 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。

26.5.4 升级 PostgreSQL 数据库

需要执行以下升级前步骤以升级 PostgreSQL 数据库。

- 1 停止 PostgreSQL 服务。

```
su -s /bin/sh - postgres -c "/opt/netiq/idm/apps/postgres/bin/pg_ctl stop -w -D /opt/netiq/idm/apps/postgres/data"
```

- 2 禁用 PostgreSQL 服务的现有单元文件。

```
systemctl disable postgresql-9.6.service
```

- 3 清理 PostgreSQL 服务的现有单元文件。

```
rm /usr/lib/systemd/system/postgresql-9.6.service  
systemctl daemon-reload  
systemctl reset-failed
```

- 4 创建备份目录并备份现有的 PostgreSQL 目录。

例如：

```
mkdir -p /home/backup  
cp -rvf /opt/netiq/idm/apps/postgres/ /home/backup/
```

- 5 导航到装入 Identity_Manager_4.7_Linux.iso 的位置。

- 6 导航到 /common/packages/postgres/ 目录。

- 7 安装新版 PostgreSQL。

```
rpm -ivh netiq-postgresql-9.6.6-0.noarch.rpm
```

注释： PostgreSQL 主目录会从先前安装的自定义位置更改为 /opt/netiq/idm/postgres/。

- 8 在 PostgreSQL 安装位置中创建 data 目录。

```
mkdir -p <POSTGRES_HOME>/data, 其中, <POSTGRES_HOME> 是 /opt/netiq/idm/postgres  
例如：
```

```
mkdir -p /opt/netiq/idm/postgres/data
```

- 9 更改新安装的 PostgreSQL 目录的许可权限。

```
chown -R postgres:postgres <postgres directory path>
```

例如：

```
chown -R postgres:postgres /opt/netiq/idm/postgres
```

- 10 创建 postgres 用户主目录。

例如， mkdir -p /home/users/postgres

- 11** 更改新创建的 PostgreSQL 用户主目录的许可权限。

```
chown -R postgres:postgres <postgres home directory path>
```

例如：

```
chown -R postgres:postgres /home/users/postgres
```

- 12** 导出 PostgreSQL home 目录

```
export PGHOME=<postgres home directory path>
```

例如：

```
export PG_HOME=/opt/netiq/idm/postgres
```

- 13** 导出 PostgreSQL 口令：

```
export PGPASSWORD=< 输入数据库口令 >
```

- 14** 初始化数据库。

```
su -s /bin/sh - postgres -c "LANG=en_US.UTF-8 <POSTGRES_HOME>/bin/initdb -D  
<POSTGRES_HOME>/data"
```

例如：

```
su -s /bin/sh - postgres -c "LANG=en_US.UTF-8 /opt/netiq/idm/postgres/bin/initdb -D /opt/netiq/idm/  
postgres/data"
```

- 15** 在 /etc/passwd 文件中，将 postgres 用户的主目录路径更改为 /opt/netiq/idm/postgres/。

15a 导航到 /etc/ 目录。

15b 编辑 passwd 文件。

```
vi /etc/passwd
```

15c 将 postgres 用户的主目录更改为 /opt/netiq/idm/postgres/。

- 16** 导航到 /opt/netiq/idm/postgres/ 目录。

- 17** 以 postgres 用户身份登录。

例如：

```
su postgres
```

- 18** 迁移现有数据。

例如：

```
/opt/netiq/idm/postgres/bin/pg_upgrade --old-datadir /opt/netiq/idm/apps/postgres/data/ --new-datadir /opt/  
netiq/idm/postgres/data/ --old-bindir /opt/netiq/idm/apps/postgres/bin --new-bindir /opt/netiq/idm/postgres/  
bin/
```

- 19** 以 postgres 用户身份注销。

- 20** 更新 pg_hba.conf 文件以信任服务器网络：

20a 导航到 /opt/netiq/idm/postgres/data/ 目录。

20b 编辑 pg_hba.conf 文件：

```
vi pg_hba.conf
```

20c 在 pg_hba.conf 文件中添加下面一行：

```
host all all 0.0.0.0/0 trust
```

21 为了确保 PostgreSQL 实例会侦听 localhost 以外的其他网络实例，请更新配置文件：

21a 导航到 /opt/netiq/idm/postgres/data/ 目录。

21b 编辑 postgresql.conf 文件：

```
vi postgresql.conf
```

21c 在 postgresql.conf 文件中添加下面一行：

```
listen_addresses = '*'
```

注释：要侦听受限的网络接口，请指定 IP 地址的逗号分隔列表。

22 在 <postgres home directory path>/data 下创建 pg_log 目录。

例如：

```
mkdir -p /opt/netiq/idm/postgres/data/pg_log
```

23 更改 pg_log 目录的许可权限。

```
chown -R postgres:postgres <postgres directory path>/data/pg_log
```

例如：

```
chown -R postgres:postgres /opt/netiq/idm/postgres/data/pg_log
```

24 启动 PostgreSQL 服务。

```
systemctl start netiq-postgresql
```

此命令将启动新的 PostgreSQL 服务。

25 （可选）通过 GUI 启动新的 pgAdmin：

25a 将 scripts 目录从旧的 postgres 主目录复制到新的 postgres 主目录。

例如：

```
cp -rvf /opt/netiq/idm/apps/postgres/scripts /opt/netiq/idm/postgres
```

25b 导航到 /opt/netiq/idm/postgres/scripts 目录。

25c 编辑 launchpgadmin.sh，使用新的 PostgreSQL 路径替换旧路径。

使用 /opt/netiq/idm/postgres 替换 /opt/netiq/idm/apps/postgres/。

25d 导航到 /usr/share/application 目录，然后编辑 .desktop 应用程序以提供 launchpgadmin.sh 的新路径。

SLES：编辑 pg-pgadmin-9_6.desktop 应用程序，使用新的 launchpgadmin.sh 路径替换 EXEC 值

例如：

将 "Exec=/opt/netiq/idm/apps/postgres/scripts/launchpgadmin.sh" 的值更改为 : "Exec=/opt/netiq/idm/postgres/scripts/launchpgadmin.sh"

RHEL：导航到 /usr/share/application，然后创建含有以下细节的 pg-pgadmin-9_6.desktop 文件：

例如：

```
[Desktop Entry]
Version=1.0
Encoding=UTF-8
Name=pgAdmin 4
Exec=/opt/netiq/idm/postgres/scripts/launchpgadmin.sh
Icon=pg-pgadmin-9_6.png
Terminal=false
Type=Application
```

25e 从系统中去除旧的 postgres 主目录。

```
rm -rf /opt/netiq/idm/apps/postgres/
```

25f 为使更改生效，请重新启动您的系统。

26.5.5 升级 Identity Applications 的驱动程序包

本节介绍如何将 User Application 驱动程序以及角色和资源服务驱动程序的包更新到最新版本。升级 Identity Applications 前必须先执行此任务。

- 1 在 Designer 中打开当前项目。
- 2 右键单击**包编目 > 导入包**。
- 3 选择相应的包。例如，**User Application 驱动程序基础包**。
- 4 单击**确定**。
- 5 在开发人员视图中，右键单击该驱动程序，然后单击**属性**。
- 6 浏览到**属性**页面中的**包**选项卡。
- 7 单击右上角的**添加包 (+)** 符号。
- 8 选择该包，然后单击**确定**。
- 9 重复相同过程升级角色和资源服务驱动程序的包。

注释： 确保 User Application 驱动程序以及角色和资源服务驱动程序连接到升级后的 Identity Manager。

26.5.6 升级 Identity Applications

注释： 如果 Identity Applications 和 SSPR 安装在不同的服务器上，您需要手动升级 SSPR。有关详细信息，请参见[升级 SSPR（第 239 页）](#)。

- ♦ [升级 Identity Applications（第 238 页）](#)
- ♦ [升级 SSPR（第 239 页）](#)

升级 Identity Applications

下面的过程介绍如何升级 Identity Applications。

- 1 从 NetIQ 下载网站下载 Identity_Manager_4.7_Linux.iso。
- 2 装入下载的 .iso。
- 3 运行以下命令：

./install.sh

- 4 通读许可协议。
- 5 输入 y 以接受许可协议。
- 6 指定是否要升级 Identity Manager 组件。可用选项有 **y** 和 **n**。
- 7 选择 Identity Applications 以继续升级。
- 8 指定以下细节：

SSPR 安装文件夹：指定 SSPR 安装文件夹。

User Application 文件夹：指定 User Application 文件夹。

Identity Applications One SSO 服务口令：指定 One SSO 口令。

Identity Applications 数据库 JDBC jar 文件：指定数据库 JAR 文件。现有数据库 jar 文件的默认位置是 /opt/netiq/idm/apps/postgres/postgresql-9.4.1212.jar。

创建 Identity Applications 的纲要：指定要在何时创建数据库纲要。可用选项有**现在**、**启动**和**文件**。

升级 SSPR

注释：如果 SSPR 安装在不同于安装 Identity Applications 和 OSP 的服务器上，则必须单独升级 SSPR。

- 1 如第 5.11 节“下载安装文件”（第 47 页）中所述下载 Identity_Manager_4.7_Linux.iso。
- 2 装入下载的 .iso。
- 3 从 .iso 文件的根目录中，导航到 SSPR 目录。
- 4 运行以下命令：
./install.sh
- 5 通读许可协议。
- 6 输入 y 以接受许可协议。

26.5.7 升级后任务

- ◆ 校验 configupdate 实用程序中的 **RBPM 至 eDirectory SAML 配置** 参数是否设置为**自动**。
 1. 起动 configupdate 实用程序。
 2. 导航到 **SSO 客户端 > RBPM**，并将 **RBPM 至 eDirectory SAML 配置** 设置为**自动**。
 3. 保存更改。
 4. 启动 Tomcat。
- ◆ 更改 OSP 目录的许可权限和所有权：
chmod +x novlua:novlua /opt/netiq/idm/apps/osp
- ◆ 手动删除先前版本的 Tomcat 和 ActiveMQ 服务。
/etc/init.d/idmapps_tomcat_init
/etc/init.d/idmapps_activemq_init

您还必须手动恢复 Tomcat、SSPR、OSP 或 Identity Applications 的自定义设置。

- ♦ [Java](#) (第 240 页)
- ♦ [Tomcat](#) (第 240 页)
- ♦ [Identity Applications](#) (第 241 页)
- ♦ [One SSO Provider](#) (第 242 页)
- ♦ [Kerberos](#) (第 242 页)

Java

校验升级后的 JRE 位置 (jre/lib/security/cacerts) 是否包含较旧 JRE 位置中的所有证书。如果某个证书缺失，请手动将该证书导入到升级后的 JRE 的 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：/opt/netiq/idm/apps/jre。

- 2 校验 JRE 主目录位置。

```
tomcat/bin/setenv.sh
```

- 3 启动[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 文件是否包含以下项：

```
<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 /opt/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 （位于 /opt/novell/eDirectory/lib64/nds-modules/jre/lib/security/cacerts 中）。

例如，您可以使用以下 keytool 命令将证书导入到身份库中：

```
keytool -importkeystore -alias <keyalias> -srckeystore <backup cacert> -
srcstorepass changeit -destkeystore /opt/novell/eDirectory/lib64/nds-
modules/jre/lib/security/cacerts
-deststorepass changeit
```

- 2 （视情况而定）导航到 User Application，然后通过读取备份的配置手动恢复自定义设置。

Identity Applications

从升级过程中创建的备份恢复 Identity Applications 自定义配置。

如果您在运行升级程序前已将自定义环境文件夹重命名为 IDMProv，则应使用 configupdate 实用程序将该环境文件夹名称更改为原来的环境名称。例如，原来的自定义环境名称为 IDMDev，现在它被重命名为 IDMProv。

请完成以下步骤将环境名称改回为原来的环境名称：

- 1 导航到 User Application 目录 （位于 /opt/netiq/idm/apps/UserApplication 中）。
- 2 （可选）要以 GUI 模式起动 configupdate 实用程序，请确保 configupdate.sh.properties 文件中的 use_console 选项设置为 false。

之所以需要执行此步骤，是因为升级实用程序会将此选项的值更改为 true。

或者，在 Linux 上起动 configupdate 实用程序，并传递额外的命令行自变量。

```
./configupdate.sh use_console=false
```

- 3 起动 configupdate 实用程序。
configupdate.sh
- 4 在 **User Application** 选项卡中单击**高级选项**，然后执行以下步骤：
 - 4a 选中**更改 RBPM 环境名称**复选框。
 - 4b 将 RBPM 环境名称更改为原来的环境名称。
 - 4c 浏览并选择相应的**角色驱动程序 DN**，然后单击**确定**。
 - 4d 使用以下命令更改 WAR 文件的许可权限和所有权。

```
chmod 755 <Original_Context_Name>.war; chown -R novlua:novlua  
<Original_Context_Name>.war
```

例如，如果原来的自定义环境名称为 IDMDDev：

```
chmod 755 IDMDDev.war; chown -R novlua:novlua IDMDDev.war
```

5（视情况而定）如果您已完成所有升级后任务，则请启动 Identity Applications 的 Tomcat 服务。

One SSO Provider

如果 OSP 和 User Application 部署在不同的服务器上，请使用配置更新实用程序更新 SSO 客户端参数。有关更多信息，请参见第 11.6.5 节“SSO 客户端参数”（第 140 页）中的 IDM 仪表板（第 140 页）。

位于 /etc/logevent.conf 文件中的 LogHost 条目默认设置为 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。

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。

26.6 升级 Identity Reporting

Identity Reporting 中包含两个驱动程序。按以下顺序执行升级：

注释：确保数据库已升级到支持的版本。

1. 将数据库升级到支持的版本。有关升级 PostgreSQL 数据库的信息，请参见第 26.5.4 节“升级 PostgreSQL 数据库”（第 235 页）。
2. 升级驱动程序包。有关详细信息，请参见第 26.6.2 节“升级 Identity Reporting 的驱动程序包”（第 243 页）。
3. 升级 / 迁移到 Sentinel Log Management for IGA。

如果您要从 Identity Reporting 4.6.x 升级，请将 Sentinel Log Management for IGA 升级到 4.7 版本。有关详细信息，请参见第 26.6.3 节“升级 Sentinel Log Management for IGA”（第 243 页）。

如果您要从 Identity Reporting 4.5.x 迁移，请从 EAS 迁移到 Sentinel Log Management for IGA。有关详细信息，请参见第 29.8.1 节“从事件审计服务迁移到 Sentinel Log Management for IGA”（第 262 页）。

4. 升级 Identity Reporting。有关详细信息，请参见第 26.6.5 节“升级 Identity Reporting”（第 244 页）。

26.6.1 升级的先决条件和注意事项

执行升级前，请注意以下事项：

- ♦ 在升级期间，请务必指定 postgresql-9.4.1212.jar 文件的正确位置。默认位置为 /opt/netiq/idm/postgres/。在下列情况下，数据库连接将失败：
 - ♦ 如果提供的路径不正确
 - ♦ 如果提供的 jar 文件不正确
 - ♦ 如果启用了防火墙
 - ♦ 如果数据库不接受来自远程计算机的连接
- ♦ 如果您的数据库配置在 SSL 上，请从 server.xml 文件的 PATH 中去除 ssl=true，该文件位于以下位置：

```
/opt/netiq/idm/apps/tomcat/conf/
```

例如，更改

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

更改为

```
jdbc:postgresql://<postgres db>:5432/idmuserappdb
```

26.6.2 升级 Identity Reporting 的驱动程序包

本节介绍了如何将受管系统网关驱动程序包和数据收集服务驱动程序包更新到最新版本。升级 Identity Reporting 前必须先执行此任务。

- 1 在 Designer 中打开当前项目。
- 2 右键单击**包编目 > 导入包**。
- 3 选择相应的包。例如，**受管系统网关基础包**。
- 4 单击**确定**。
- 5 在开发人员视图中，右键单击该驱动程序，然后单击**属性**。
- 6 浏览到**属性**页面中的**包**选项卡。
- 7 单击右上角的**添加包 (+)** 符号。
- 8 选择该包，然后单击**确定**。
- 9 重复相同过程升级数据收集服务驱动程序的包。

注释：确保受管系统网关驱动程序和数据收集服务驱动程序已连接到升级后的 Identity Manager。

26.6.3 升级 Sentinel Log Management for IGA

- 1 从 NetIQ 下载网站下载 SentinelLogManagementForIGA8.1.1.0.tar.gz。
 - 2 导航到要提取文件的目录。
 - 3 运行以下命令来提取文件
- ```
tar -zxvf SentinelLogManagementForIGA8.1.1.0.tar.gz
```

- 4 导航到 SentinelLogManagementforIGA 目录。
- 5 要安装 SLM for IGA，请运行以下命令：  
`./install.sh`
- 6 指定要用于安装的语言，然后按 Enter。
- 7 输入 y 以接受许可协议。

---

**注释：**升级 SLM for IGA 后，您需要手动导入最新的收集器。

1. 导航到 NetIQ 下载网站。
  2. 下载 SentinelLogManagementForIGA8.1.1.0.tar.gz 文件。
  3. 提取文件并导航到 /content/ 目录。
  4. 导入 Identity Manager 收集器。
- 

## 26.6.4 升级操作系统

将操作系统从 SLES 11 升级到 SLES 12 时，操作系统的升级过程会删除一些 SLM for IGA RPM。

以下命令可确保 SLM for IGA 在您升级操作系统后能正常工作。

---

**注释：**升级操作系统前，必须先升级 SLM for IGA。

---

使用以下步骤来升级您的操作系统：

- 1 导航到提取 Sentinel 安装文件的目录。
- 2 停止 Sentinel 服务：  
`rcsentinel stop`
- 3 运行以下命令：  
`./install.sh --preosupgrade`
- 4 升级您的操作系统。
- 5 运行以下命令：  
`./install.sh --postosupgrade`
- 6 重新启动 Sentinel 服务：  
`rcsentinel 重启动`

## 26.6.5 升级 Identity Reporting

- 1 从 NetIQ 下载网站下载 Identity\_Manager\_4.7\_Linux.iso。
- 2 装入下载的 .iso。
- 3 运行以下命令：  
`./install.sh`
- 4 通读许可协议。
- 5 输入 y 以接受许可协议。

- 6 指定是否要升级 Identity Manager 组件。可用选项有 **y** 和 **n**。
- 7 选择 Identity Reporting 以继续升级。
- 8 指定以下细节：
  - 已安装 OSP**：指定是否已安装 OSP。
  - 用于备份的 Reporting 安装文件夹**：指定 Reporting 安装文件夹。
  - 创建 Identity Reporting 的纲要**：指定要在何时创建数据库纲要。
  - Identity Reporting 数据库 JDBC jar 文件**：指定 Identity Reporting 的数据库 JAR 文件。现有数据库 jar 文件的默认位置是 /opt/netiq/idm/apps/postgres/postgresql-9.4.1212.jar。
  - Identity Reporting 数据库用户**：指定 Reporting 数据库用户的名称。
  - Identity Reporting 数据库帐户口令**：指定 Reporting 数据库口令。

## 26.6.6 Reporting 的升级后步骤

---

**注释：**执行升级后，Identity Manager 4.6.1 将报告不能正常工作。您只能使用 Identity Manager 4.7 报告。

---

如果在升级期间为**数据库纲要**创建选择了**启动**或**文件**，请务必执行以下操作：

1. 登录 Identity Reporting。
2. 从 Identity Reporting 储存库中删除现有数据源和报告定义。
3. 添加新的 Identity Manager 数据收集服务数据源。

## 26.6.7 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。

## 26.7 升级 Analyzer

NetIQ 提供了 .zip 格式的增补程序文件用于升级 Analyzer。在升级 Analyzer 之前，请确保计算机满足各项先决条件和系统要求。有关详细信息，请参见更新随附的《发行说明》。

- 1 从 NetIQ 下载网站下载 Identity\_Manager\_4.7\_Linux\_Analyzer.tar.gz。
- 2 将该 .zip 文件抽取到包含 Analyzer 安装文件（例如插件、卸载脚本和其他 Analyzer 文件）的目录。
- 3 重新启动 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 检查程序显示的是否为新版本。

## 26.8 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。

### 26.8.1 将该新服务器添加到驱动程序集中

如果正在使用 iManager，则必须将该新服务器添加到驱动程序集中。Designer 包含一个用于服务器的迁移向导，可为您完成此步骤。如果正在使用 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](#)。

### 26.8.2 从驱动程序集中去除旧服务器。

当新服务器运行所有驱动程序后，您可以从驱动程序集中去除旧服务器。


- [使用 Designer 从驱动程序集中去除旧服务器](#)（第 246 页）
- [使用 iManager 从驱动程序集中去除旧服务器](#)（第 247 页）
- [弃用旧服务器](#)（第 247 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 副本。  
有关详细信息，请参见《[NetIQ eDirectory Administration Guide](#)》（NetIQ eDirectory 管理指南）中的“[Deleting Replicas](#)”（删除副本）。
- 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](#)”。


## 26.9 将自定义策略和规则恢复到驱动程序

安装或升级到驱动程序的新包之后，您必须将所有自定义策略或规则恢复到驱动程序，然后再重写新的驱动程序配置文件。如果这些策略具有不同名称，则它们仍存储在驱动程序中，但是链接会损坏并需要重新建立。

- [第 26.9.1 节“使用 Designer 将自定义策略和规则恢复为驱动程序”](#)（第 247 页）
- [第 26.9.2 节“使用 iManager 将自定义策略和规则恢复为驱动程序”](#)（第 248 页）

### 26.9.1 使用 Designer 将自定义策略和规则恢复为驱动程序

您可以将策略添加到策略集中。在将升级后的驱动程序移到生产环境中之前，您应该在测试环境中执行以下步骤。


- 1 在大纲视图中，选择已升级的驱动程序，然后单击 **显示策略流图** .
- 2 右键单击需要将自定义策略恢复为驱动程序的策略集，然后选择 **添加策略 > 复制现有策略**。
- 3 浏览到并选择自定义策略，然后单击 **确定**。
- 4 指定自定义策略的名称，然后单击 **确定**。
- 5 在文件冲突讯息中单击 **是** 以保存项目。
- 6 策略构建器打开策略后，验证复制的策略中信息是否正确。
- 7 对需要恢复为驱动程序的每个自定义策略，重复 [步骤 2](#) 到 [步骤 6](#)。
- 8 启动并测试驱动程序。

有关启动驱动程序的更多信息，请参见第 23.1.2 节“启动驱动程序”（第 210 页）。有关测试驱动程序的详细信息，请参见《*NetIQ Identity Manager - Using Designer to Create Policies*》（NetIQ Identity Manager - 使用 Designer 创建策略）中的“*Testing Policies with the Policy Simulator*”（使用策略模拟器测试策略）。

- 9 验证策略工作正常后，将驱动程序移动到生产环境中。

## 26.9.2 使用 iManager 将自定义策略和规则恢复为驱动程序

在将升级的驱动程序移到生产环境中前，请在测试环境中执行这些步骤。

- 1 在 iManager 中，选择 **Identity Manager > Identity Manager 概述**。
- 2 浏览到并选择树中要搜索驱动程序集对象的位置，然后单击搜索图标 。
- 3 单击包含已升级的驱动程序的驱动程序集对象。
- 4 单击驱动程序图标，然后选择需要恢复自定义策略的策略集。
- 5 单击**插入**。
- 6 选择**使用现有策略**，然后浏览到并选择自定义策略。
- 7 单击**确定**，然后单击**关闭**。
- 8 对需要恢复为驱动程序的每个自定义策略，重复步骤 3 到步骤 7。
- 9 启动并测试驱动程序。

有关启动驱动程序的信息，请参见第 23.1.2 节“启动驱动程序”（第 210 页）。iManager 中没有任何策略模拟器。要测试策略，请触发使策略能够执行的事件。例如，创建用户、修改用户或删除用户。

- 10 验证策略工作正常后，将驱动程序移动到生产环境中。



# 27 从 Advanced Edition 切换到 Standard Edition

仅当您不想在环境中使用任何 Advanced Edition 功能，并且想要缩减 Identity Manager 部署时，才应切换到 Standard Edition。

- 1 （视情况而定）如果您已应用 Advanced Edition 激活，请去除激活。
- 2 （视情况而定）要切换到 Standard Edition 评估模式，请执行以下操作：
  - 2a 浏览到身份库 dib 目录。  
`/var/opt/novell/eDirectory/data/dib`
  - 2b 创建一个新文件，将其命名为 `.idme`，并在其中添加 2 （数值）。
  - 2c 重新启动 eDirectory。
  - 2d 继续步骤 4。
- 3 （视情况而定）如果您已购买 Standard Edition 激活，请应用激活。
- 4 停止 Tomcat。
- 5 从 `/opt/netiq/idm/apps/tomcat/webapps` 目录中去除以下 WAR 文件和 Webapps 文件夹：
  - ◆ IDMPProv\*
  - ◆ IDMRPT\*
  - ◆ dash\*
  - ◆ idmdash\*
  - ◆ landing\*
  - ◆ rra\*
  - ◆ rptdoc\*
- 6 将以下现有文件夹移到备份目录：
  - ◆ IDMReporting
  - ◆ UserApplication
- 7 将 `<安装文件夹>/tomcat/conf` 目录中的 `ism-configuration.properties` 文件复制到备份目录。
- 8 从 Identity Manager 4.6 媒体安装 Identity Reporting。
- 9 从 `<Reporting 安装文件夹>/bin` 目录启动 `configupdate.sh`，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 192.168.0.1）
  - ◆ **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， /opt/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 客户端机密**。例如， <*sspr 客户端机密*>
  - ◆ **OSP OAuth 重定向 URL**. 例如， http://192.168.0.1:8180/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 126 页）](#)。

**10** 保存更改并退出配置实用程序。

**11** 启动 Tomcat。



# 将 Identity Manager 数据迁移到新安装

本部分提供有关将 Identity Manager 组件中的现有数据迁移到新安装的信息。大多数迁移任务都适用于 Identity Applications。要升级 Identity Manager 组件，请参见第 IX 部分“[升级 Identity Manager](#)”（第 217 页）。有关升级与迁移之间区别的详细信息，请参见第 25.2 节“[了解升级过程](#)”（第 220 页）。



# 28 准备迁移 Identity Manager

本章提供的信息可帮助您准备好将 Identity Manager 解决方案迁移到新安装。

## 28.1 执行迁移的核对清单

要执行迁移，NetIQ 建议您完成以下核对清单中的步骤。

|                          | 核对清单项目                                                                                                                      |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> | 1. 确定应执行升级还是迁移。有关详细信息，请参见第 25.2 节“了解升级过程”（第 220 页）。                                                                         |
| <input type="checkbox"/> | 2. 确保拥有最新的安装包用于迁移 Identity Manager 数据。                                                                                      |
| <input type="checkbox"/> | 3. 了解 Identity Manager 各组件之间的交互。有关详细信息，请参见第 I 部分“简介”（第 15 页）。                                                               |
| <input type="checkbox"/> | 4. 确保您的计算机符合较新版 Identity Manager 的硬件和软件先决条件。有关详细信息，请参见第 5.9 节“准备安装”（第 41 页）和要升级的目标版本的《发行说明》。                                |
| <input type="checkbox"/> | 5. 将 eDirectory 升级到身份库的最新受支持版本。有关详细信息，请参见第 26.3.1 节“升级身份库”（第 228 页）。                                                        |
| <input type="checkbox"/> | 6. 将位于当前 Identity Manager 服务器上的 eDirectory 复本添加到新服务器。有关详细信息，请参见第 29.4 节“将 Identity Manager 引擎迁移到新服务器”（第 258 页）。             |
| <input type="checkbox"/> | 7. 在新服务器上安装 Identity Manager。有关详细信息，请参见规划安装 Identity Manager（第 31 页）。                                                       |
| <input type="checkbox"/> | 8. （视情况而定）如果驱动程序集中有任何驱动程序是 Remote Loader 驱动程序，请升级每个驱动程序的 Remote Loader 服务器。有关详细信息，请参见第 26.3.3 节“升级 Remote Loader”（第 229 页）。 |
| <input type="checkbox"/> | 9. （视情况而定）如果在旧服务器上运行 User Application，请更新该组件及其驱动程序。有关详细信息，请参见第 29.1 节“Identity Manager 的迁移核对清单”（第 255 页）。                   |
| <input type="checkbox"/> | 10. 更改每个驱动程序的特定于服务器的信息。有关详细信息，请参见第 29.3.1 节“在 Designer 中复制服务器特定信息”（第 257 页）。                                                |
| <input type="checkbox"/> | 11. （视情况而定）如果您在使用 RBPM，请将 User Application 的服务器特定信息从旧服务器更新为新服务器。有关详细信息，请参见第 29.3 节“复制驱动程序集的服务器特定信息”（第 256 页）。               |
| <input type="checkbox"/> | 12. 将驱动程序更新为包格式。有关详细信息，请参见第 26.4 节“升级 Identity Manager 驱动程序”（第 231 页）。                                                      |
| <input type="checkbox"/> | 13. （视情况而定）如果您有自定义的策略和规则，请恢复自定义设置。有关详细信息，请参见第 26.9 节“将自定义策略和规则恢复到驱动程序”（第 247 页）。                                            |
| <input type="checkbox"/> | 14. 安装 Identity Reporting 和关联的驱动程序。有关详细信息，请参见第 29.8 节“迁移 Identity Reporting”（第 262 页）。                                      |

|                          | 核对清单项目                                                                                             |
|--------------------------|----------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> | 15. 从驱动程序集中去除旧服务器。有关详细信息，请参见 <a href="#">第 26.8.2 节“从驱动程序集中去除旧服务器。”</a> （第 246 页）。                 |
| <input type="checkbox"/> | 16. 激活已升级的 Identity Manager 解决方案。有关详细信息，请参见 <a href="#">第 24 节“激活 Identity Manager”</a> （第 213 页）。 |

## 28.2 在迁移期间停止和启动 Identity Manager 驱动程序

在升级或迁移 Identity Manager 时，您需要启动和停止驱动程序，以确保升级或迁移过程能够修改或替换正确的文件。本节包含以下活动。有关详细信息，请参见以下各节：

- [第 23.1.1 节“停止驱动程序”](#)（第 209 页）
- [第 23.1.2 节“启动驱动程序”](#)（第 210 页）

# 29 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：

- 第 29.1 节 “Identity Manager 的迁移核对清单”（第 255 页）
- 第 29.2 节 “准备要迁移的 Designer 项目”（第 256 页）
- 第 29.3 节 “复制驱动程序集的服务器特定信息”（第 256 页）
- 第 29.4 节 “将 Identity Manager 引擎迁移到新服务器”（第 258 页）
- 第 29.5 节 “迁移 User Application 驱动程序”（第 258 页）
- 第 29.6 节 “升级 Identity Applications”（第 259 页）
- 第 29.7 节 “完成 Identity Applications 的迁移”（第 260 页）
- 第 29.8 节 “迁移 Identity Reporting”（第 262 页）

## 29.1 Identity Manager 的迁移核对清单

NetIQ 建议您完成以下核对清单中的步骤。

|                          | 核对清单项目                                                                                                                                                                                                                                                                      |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> | 1. 备份 Identity Manager 解决方案的目录和数据库。                                                                                                                                                                                                                                         |
| <input type="checkbox"/> | 2. 确保已安装最新版本的 Identity Manager 组件（Identity Applications 除外）。有关详细信息，请参见第 5.7.4 节 “建议的服务器设置”（第 39 页）和组件的最新《发行说明》。<br><br><b>注释：</b> 要继续使用当前的 User Application 数据库，请在安装程序中指定现有数据库。有关详细信息，请参见第 9 章 “安装 Identity Manager 引擎、Identity Applications 和 Identity Reporting”（第 83 页）。 |
| <input type="checkbox"/> | 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。                                                                                                                                                                                                                           |
| <input type="checkbox"/> | 4. 将现有 User Application 驱动程序导入到 Designer 中。                                                                                                                                                                                                                                 |
| <input type="checkbox"/> | 5. 对 Designer 项目存档。它代表驱动程序的迁移前状态。有关详细信息，请参见第 29.2 节 “准备要迁移的 Designer 项目”（第 256 页）。                                                                                                                                                                                          |
| <input type="checkbox"/> | 6. （视情况而定）要将 Identity Manager 引擎迁移到某个新服务器，请将 eDirectory 副本复制到该新服务器。有关详细信息，请参见第 29.4 节 “将 Identity Manager 引擎迁移到新服务器”（第 258 页）。                                                                                                                                              |
| <input type="checkbox"/> | 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。                                                                                                                                                                                                    |
| <input type="checkbox"/> | 8. 迁移 User Application 驱动程序。有关详细信息，请参见第 29.5 节 “迁移 User Application 驱动程序”（第 258 页）。                                                                                                                                                                                         |

|                          | 核对清单项目                                                                                                           |
|--------------------------|------------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> | 9. 升级 Identity Applications。有关详细信息，请参见第 26.5 节“升级 Identity Applications”（第 233 页）。                               |
| <input type="checkbox"/> | 10. （视情况而定）要使用安装过程创建的 SQL 文件升级 Oracle 数据库，请准备好 Oracle 环境。有关详细信息，请参见第 29.7.1 节“准备 Oracle 数据库以运行 SQL 文件”（第 260 页）。 |
| <input type="checkbox"/> | 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，请参见第 29.7.2 节“清理浏览器超速缓存”（第 261 页）。                                |
| <input type="checkbox"/> | 12. （视情况而定）恢复 SharedPagePortlet 的自定义设置。有关详细信息，请参见第 29.7.3 节“更新 SharedPagePortlet 的最大超时设置”（第 261 页）。              |
| <input type="checkbox"/> | 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，请参见第 29.7.4 节“禁用组的自动查询设置”（第 261 页）。                                      |

## 29.2 准备要迁移的 Designer 项目

在迁移驱动程序之前，您需要执行一些设置步骤，以准备要迁移的 Designer 项目。

**注释：**如果没有要迁移的现有 Designer 项目，请使用文件 > 导入 > 项目（从身份库）创建一个新项目。

- 1 起动 Designer。
- 2 （视情况而定）如果您的某个现有 Designer 项目包含要迁移的 User Application，请备份该项目：
  - 2a 在“项目”视图中右键单击该项目的名称，然后选择复制项目。
  - 2b 指定项目的名称，然后单击确定。
- 3 要更新现有项目的纲要，请完成以下步骤：
  - 3a 在“建模器”视图中，选择“身份库”。
  - 3b 选择在线 > 纲要 > 导入。
- 4 （可选）要校验项目中 Identity Manager 的版本号是否正确，请完成以下步骤：
  - 4a 在“建模器”视图中，选择“身份库”，然后单击属性。
  - 4b 在左侧导航菜单中，选择服务器列表。
  - 4c 选择一个服务器，然后单击编辑。

Identity Manager 版本字段应显示最新版本。

## 29.3 复制驱动程序集的服务器特定信息

您必须将储存在每个驱动程序和驱动程序集中的所有服务器特定信息复制到新服务器的信息中。这还包括新服务器中原本没有但需从驱动程序集复制的 GCV 和其他数据。特定于服务器的信息包含于：

- 全局配置值
- 引擎控制值
- 命名口令



- 驱动程序鉴定信息
- 驱动程序启动选项
- 驱动程序参数
- 驱动程序集数据

可以在 Designer 或 iManager 中进行此操作。如果使用 Designer，则这是一个自动过程。如果使用 iManager，则这是手动过程。如果要从版本低于 3.5 的 Identity Manager 服务器迁移到高于或等于版本 3.5 的 Identity Manager 服务器，则应使用 iManager。对于所有其他支持的迁移路径，则可以使用 Designer。


- [第 29.3.1 节“在 Designer 中复制服务器特定信息”](#)（第 257 页）
- [第 29.3.2 节“在 iManager 中更改服务器特定信息”](#)（第 257 页）
- [第 29.3.3 节“更改 User Application 的服务器特定信息”](#)（第 258 页）

## 29.3.1 在 Designer 中复制服务器特定信息

此过程会影响驱动程序集中储存的所有驱动程序。

- 1 在 Designer 中，打开项目。
- 2 在概要选项卡中，右键单击服务器，然后选择**迁移**。
- 3 阅读概述以查看迁移到新服务器的项，然后单击**下一步**。
- 4 从可用服务器列表中选择目标服务器，然后单击**下一步**。  
仅列出当前未与驱动程序集相关联且与源服务器的 Identity Manager 版本相同或更高的服务器。
- 5 选择以下选项之一：
  - ♦ **激活目标服务器**：将源服务器中的设置复制到目标服务器并禁用源服务器上的驱动程序。NetIQ 建议您使用此选项。
  - ♦ **保持源服务器处于活动状态**：不要复制设置并禁用目标服务器上的所有驱动程序。
  - ♦ **同时激活目标服务器和源服务器**：将源服务器中的设置复制到目标服务器，不禁用源服务器或目标服务器上的驱动程序。不建议使用此选项。如果同时启动了两个驱动程序，则相同信息会写入两个不同队列，这样可能导致损坏。
- 6 单击**迁移**。
- 7 将更改的驱动程序部署到身份库。  
有关详细信息，请参见《[NetIQ Designer for Identity Manager Administration Guide](#)》（NetIQ Designer for Identity Manager 管理指南）中的“[Deploying a Driver to an Identity Vault](#)”（将驱动程序部署到身份库）。
- 8 启动驱动程序。  
有关详细信息，请参见[第 23.1.2 节“启动驱动程序”](#)（第 210 页）。

## 29.3.2 在 iManager 中更改服务器特定信息

- 1 在 iManager 中，单击  以显示“Identity Manager 管理”页面。
- 2 单击 **Identity Manager 概述**。
- 3 浏览到并选择保存驱动程序集的容器。
- 4 单击驱动程序集名称以访问“驱动程序集概述”页。

- 5 单击驱动程序的右上角，然后单击**停止驱动程序**。
- 6 单击驱动程序的右上角，然后单击**编辑属性**。
- 7 将所有包含旧服务器信息的特定于服务器的驱动程序参数、全局配置值、引擎控制值、命名口令、驱动程序鉴定数据及驱动程序启动选项复制或迁移到新服务器的信息中。驱动程序集的全局配置值及其他参数（比如最大堆大小、Java 设置等）必须与旧服务器的值相同。
- 8 单击**确定**保存所有更改。
- 9 单击驱动程序的右上角以启动驱动程序。
- 10 对驱动程序集中的每个驱动程序重复**步骤 5** 到**步骤 9**。

### 29.3.3 更改 User Application 的服务器特定信息

您必须重配置 User Application，以便识别新服务器。运行 configupdate.sh。

- 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 在命令提示符中，启动配置更新实用程序：  
configupdate.sh
- 3 按第 11.6 章“配置 Identity Applications 的设置”（第 126 页）中所述指定值。

## 29.4 将 Identity Manager 引擎迁移到新服务器

将 Identity Manager 引擎迁移到新服务器时，您可以保留当前在旧服务器上使用的 eDirectory 复本。

- 1 在新服务器上安装受支持版本的 eDirectory。
- 2 将位于当前 Identity Manager 服务器上的 eDirectory 复本复制到新服务器。  
有关详细信息，请参见《[NetIQ eDirectory Administration Guide](#)》（NetIQ eDirectory 管理指南）中的“[Administering Replicas](#)”（管理复本）。
- 3 在新服务器上安装 Identity Manager 引擎。  
有关详细信息，请参见第 9 章“安装 Identity Manager 引擎、Identity Applications 和 Identity Reporting”（第 83 页）。

## 29.5 迁移 User Application 驱动程序

在升级到新版 Identity Manager 或迁移到另一台服务器时，您可能需要导入 User Application 驱动程序的新基础包，或升级现有包。例如：**User Application 基础包版本 2.2.0.20120516011608**。

当您开始处理某个 Identity Manager 项目时，Designer 会自动提示您将新包导入该项目。到时您也可以手动导入包。

### 29.5.1 导入新的基础包

- 1 在 Designer 中打开您的项目。
- 2 右键单击**包编目 > 导入包**，然后选择相应的包。

- 3 （视情况而定）如果“导入包”对话框未列出 User Application 基础包，请完成以下步骤：
  - 3a 单击“浏览”按钮。
  - 3b 浏览到 `designer_root/packages/eclipse/plugins/NOVLUABASE_version_of_latest_package.jar`。
  - 3c 单击**确定**。
- 4 单击**确定**。

## 29.5.2 升级现有的基础包

- 1 在 Designer 中打开您的项目。
- 2 右键单击 User Application 驱动程序。
- 3 单击**驱动程序 > 属性 > 包**。

如果基础包可以升级，应用程序将在**升级**列中显示一个选中标记。
- 4 对指出有可用升级的包单击**选择操作**。
- 5 在下拉列表中，单击**升级**。
- 6 选择要升级的目标版本。然后单击“确定”。
- 7 单击**应用**。
- 8 在字段中填写适当的信息以升级该包。然后单击**下一步**。
- 9 阅读安装摘要。然后单击**完成**。
- 10 关闭“包管理”页面。
- 11 取消选择**仅显示适用的包版本**。

## 29.5.3 部署迁移的驱动程序

只有将 User Application 驱动程序部署到身份库后，驱动程序迁移才算完成。迁移后，项目所处的状态只允许部署整个迁移的配置。您无法将任何定义导入迁移的配置。在部署整个迁移配置后，此限制即会消除，您便可以部署各个对象并导入定义。

- 1 在 Designer 中打开项目，然后对迁移的对象运行 Project Checker。

有关详细信息，请参见《[NetIQ Identity Manager - Administrator's Guide to Designing the Identity Applications](#)》（NetIQ Identity Manager - Identity Applications 管理员设计指南）中的“[Validating Provisioning Objectss](#)”（验证供应对象）。如果配置存在验证错误，系统会告知您具体错误。只有更正了这些错误，才能部署驱动程序。
- 2 在大纲视图中，右键单击 User Application 驱动程序。
- 3 选择**部署**。
- 4 对驱动程序集中的每个 User Application 驱动程序重复此过程。

## 29.6 升级 Identity Applications

在运行 Identity Applications 的升级程序时，请务必注意以下事项：

- ◆ 使用以前的 User Application 所用的同一个数据库。“之前安装”是指您要迁移的安装。在安装程序中，指定**现有数据库**作为数据库类型。

- （视情况而定）如果现有数据库在 Oracle 上运行，并且您要指示安装程序编写一个 SQL 文件来更新纲要，则必须执行附加的步骤。有关详细信息，请参见第 29.7.1 节“准备 Oracle 数据库以运行 SQL 文件”（第 260 页）。
- 您可为 User Application 环境指定一个不同的名称。
- 指定不同于先前安装的安装位置。
- 指向支持版本的 Tomcat。
- 不要对数据库使用不区分大小写的排序规则。不区分大小写的排序规则不受支持。如果使用不区分大小写的排序规则，则在迁移过程中可能会遇到重复项错误。如果遇到重复键错误，请检查排序规则并更正它，然后重安装 Identity Applications。
- 了解各口令管理提供程序之间的区别。SSPR 是默认的提供程序。要使用 Identity Manager 的旧式提供程序或使用外部提供程序，您必须在升级后更新 Identity Applications 的配置。

有关升级 Identity Applications 的详细信息，请参见第 26.5 节“升级 Identity Applications”（第 233 页）。

## 29.7 完成 Identity Applications 的迁移

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

### 29.7.1 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：

```
/opt/novell/idm/jre/bin/java -Xms256m -Xmx256m -Dwar.context.name=IDMProv
-jar /opt/novell/idm/liquibase.jar
--databaseClass=com.novell.soa.persist.liquibase.OracleUnicodeDatabase
--driver=oracle.jdbc.driver.OracleDriver
--classpath=/root/ojdbc8.jar:/opt/novell/idm/tomcat/server/IDMProv/deploy/
IDMProv.war
--changeLogFile=DatabaseChangeLog.xml
--url="jdbcURL" --logLevel=debug
--logFile=/opt/novell/idm/db.out --contexts="prov,updatedb" --username=xxxx
--password=xxxx updateSQL > /opt/novell/idm/db.sql
```

- 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。

---

**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。

---

## 29.7.2 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。

## 29.7.3 更新 SharedPagePortlet 的最大超时设置

如果您已自定义 SharedPagePortlet 的任何默认设置或首选项，则这些自定义已保存到数据库，并且此设置将被重写。因此，浏览到“身份自助服务”选项卡并不总是高亮显示正确的共享页面。为确保不遇到此问题，请完成以下步骤：

- 1 以 User Application 管理员身份登录。
- 2 浏览到**管理 > Portlet 管理**。
- 3 展开**共享页面导航**。
- 4 在左侧的 Portlet 树中，单击**共享页面导航**。
- 5 在页面的右侧，单击**设置**。
- 6 确保**最大超时**设置为 0。
- 7 单击“保存设置”。

## 29.7.4 禁用组的自动查询设置

默认情况下，目录提取层中“组”实体的“DNLookup 显示”处于启用状态。这意味着，每当为组指派打开对象选择器时，无需搜索就会按默认显示所有组。您应该更改此设置，因为用于搜索组的窗口在用户输入搜索内容之前不应显示任何结果。

您可以在 Designer 中取消选中**执行自动查询**来更改此设置，如下所示：



## 29.8 迁移 Identity Reporting

迁移先前版本的 Identity Manager 涉及到迁移 Identity Reporting。请务必注意以下事项：

- 手动将事件审计服务数据迁移到 PostgreSQL 数据库。
- 清理现有 Reporting 安装。
- 在新服务器上执行 Identity Reporting 4.7 的全新安装。
- 为新安装的 Identity Reporting 指定现有鉴定服务和身份库的安装位置。

### 29.8.1 从事件审计服务迁移到 Sentinel Log Management for IGA

本节提供有关将 EAS 数据库中的 SIEM 数据迁移到支持的 PostgreSQL 数据库的信息。

您必须创建必要的角色和表空间，以确保迁移期间不会出现故障。

#### 准备新 PostgreSQL 数据库

- 1 停止 EAS 以确保不会有任何事件发送到 EAS 服务器。
- 2 使用 iManager 停止 DCS 驱动程序：
  - 2a 登录到 iManager。
  - 2b 停止 DCS 驱动程序。

**2c** 编辑驱动程序属性，将启动选项设置为**手动**。

此步骤可确保驱动程序不会自动启动。

**3** 使用 PGAdmin 运行以下 SQL 命令，创建必要的角色、表空间和数据库。

此步骤可确保迁移期间不会出现故障。

**3a** 运行以下命令创建必要角色：

```
CREATE ROLE esec_app
 NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE;

CREATE ROLE esec_user
 NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE;

CREATE ROLE admin LOGIN
 ENCRYPTED PASSWORD '<specify the password for admin>'
 NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE;
GRANT esec_user TO admin;

CREATE ROLE appuser LOGIN
 ENCRYPTED PASSWORD '<specify the password for appuser>'
 NOSUPERUSER INHERIT NOCREATEDB CREATEROLE;
GRANT esec_app TO appuser;

CREATE ROLE dbauser LOGIN
 ENCRYPTED PASSWORD '<specify the password for dbauser>'
 SUPERUSER INHERIT CREATEDB CREATEROLE;

CREATE ROLE idmrptsrv LOGIN
 ENCRYPTED PASSWORD '<specify the password for idmrptsrv>'
 NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE;
GRANT esec_user TO idmrptsrv;

CREATE ROLE idmrptuser LOGIN
 ENCRYPTED PASSWORD '<specify the password for idmrptuser>'
 NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE;

CREATE ROLE rptuser LOGIN
 ENCRYPTED PASSWORD '<specify the password for rptuser>'
 NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE;
GRANT esec_user TO rptuser;
```

**3b** 运行以下命令创建表空间：

```
CREATE TABLESPACE sendata1
 OWNER dbauser
 LOCATION '<provide the location where table space has to be created>';
```

例如：

```
CREATE TABLESPACE sendata1
 OWNER dbauser
 LOCATION '</opt/netiq/idm/apps/postgres/data>';
```

**3c** 运行以下命令创建 SIEM 数据库：

```
CREATE DATABASE "SIEM"
 WITH OWNER = dbauser
 ENCODING = 'UTF8'
 TABLESPACE = sendata1
 CONNECTION LIMIT = -1;
```



## 导出 EAS 中的数据

- 1 停止 EAS 以确保不会有任何事件发送到 EAS 服务器。
- 2 使用 iManager 停止 DCS 驱动程序：
  - 2a 登录到 iManager。
  - 2b 停止 DCS 驱动程序。
  - 2c 编辑驱动程序属性，将启动选项设置为**手动**。  
此步骤可确保驱动程序不会自动启动。
- 3 将 EAS 数据库中的数据导出到文件：
  - 3a 登录 EAS 用户帐户：  

```
su - novleas
```
  - 3b 指定 EAS 用户具有完全访问权限的位置，例如 /home/novleas。
  - 3c 浏览到 PostgreSQL 安装目录并执行以下命令：  
例如：  

```
export PATH=/opt/novell/sentinel_eas/3rdparty/postgresql/bin/:$PATH
export LD_LIBRARY_PATH=/opt/novell/sentinel_eas/3rdparty/postgresql/lib/:$LD_LIBRARY_PATH
```
  - 3d 使用以下命令将数据导出到 .sql 文件：  

```
./pg_dump -p < 端口号 > -U < 用户名 > -d < 数据库名称 > -f < 导出位置 >
```

  
例如，  

```
./pg_dump -p 15432 -U dbauser SIEM -f /home/novleas/SIEM.sql
```

## 将数据导入到新 PostgreSQL 数据库中

- 1 停止 EAS 以确保不会有任何事件发送到 EAS 服务器。
- 2 使用 iManager 停止 DCS 驱动程序：
  - 2a 登录到 iManager。
  - 2b 停止 DCS 驱动程序。
  - 2c 编辑驱动程序属性，将启动选项设置为**手动**。  
此步骤可确保驱动程序不会自动启动。
- 3 将数据导入到新的 PostgreSQL 数据库：
  - 3a （视情况而定）创建一个 postgres 用户。  
此步骤仅针对 Windows。Linux 上会自动创建用户。
  - 3b 将**步骤 3d** 中导出的文件复制到该 postgres 用户具有完全访问权限的位置。例如：/opt/netiq/idm/postgres
  - 3c 执行以下命令将数据导入到 PostgreSQL 数据库。  

```
psql -d < 数据库名称 > -U < 用户名 > -f < 导出文件所在位置的完整路径 >
```

  
例如：  

```
psql -d SIEM -U postgres -f /opt/netiq/idm/apps/postgres/SIEM.sql
```
- 4 检查是否存在任何迁移日志错误，如有则予以解决。



---

**注释：** Identity Manager 4.7 报告将不使用从 EAS 迁移到 SLM for IGA 的审计数据，而是使用直接从 SLM for IGA 同步的审计数据。

---

## 29.8.2 设置新 Reporting 服务器

将 EAS 数据导入到新 PostgreSQL 数据库后，在另一台服务器上安装新的 Reporting 应用程序，并让它指向身份库和现有鉴定服务。

- 1 停止运行现有 Reporting 应用程序的现有 Tomcat 服务。
- 2 在 Tomcat 安装路径外部，为 /opt/netiq/idm/apps/ 下 tomcat/webapps 目录和 Reporting 主目录中的现有 Identity Reporting WAR 文件创建备份
- 3 从现有 server.xml 文件中去除 EAS 条目。
- 4 在迁移 EAS 数据的同一个 PostgreSQL 数据库中创建新数据库。
- 5 在新服务器上安装和配置 Identity Reporting，并让它指向现有单点登录服务和身份库。有关详细信息，请参见第 10 章“配置安装的组件”（第 91 页）。
- 6 要让现有单点登录服务指向新安装的 Identity Reporting，请使用配置更新实用程序修改 Identity Reporting 配置条目。
- 7 重启动运行现有单点登录服务的 Tomcat 服务器。

## 29.8.3 创建数据同步策略

配置 Reporting 服务器之后，需要创建数据同步策略以将事件从 SLM for IGA 转发到 Reporting 数据库。升级到 Identity Reporting 4.7 时，请注意以下事项。

---

**注释：**

- ♦ 如果您要从 Identity Reporting 4.5.6 升级到 Identity Reporting 4.7，则需要在 Identity Manager 的“数据收集服务”页面中创建新策略。有关详细信息，请参见《[Administrator Guide to NetIQ Identity Reporting](#)》（NetIQ Identity Reporting 管理员指南）中的“[About the Data Sync Policies tab](#)”（关于“数据同步策略”选项卡）。
  - ♦ 如果您要从 Identity Reporting 4.6.x 升级到 Identity Reporting 4.7，请按照《[NetIQ Identity Manager 4.7 发行说明](#)》的“[Identity Manager 升级问题](#)”中的步骤操作。
-



# 30 卸载 Identity Manager 组件

本章介绍卸载 Identity Manager 各组件的过程。卸载某些组件需要满足一些先决条件。在开始执行卸载过程之前，请务必查看每个组件的相关完整章节。

---

**注释：**在卸载 Identity Manager 组件之前，必须先停止所有服务，例如 Tomcat、PostgreSQL 和 ActiveMQ。

---

## 30.1 从身份库中去除对象

卸载 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。

## 30.2 卸载 Identity Manager 引擎

安装程序提供了 Identity Manager 的卸载脚本。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：**在卸载 Identity Manager 引擎之前，请准备好身份库。有关详细信息，请参见第 30.1 节“[从身份库中去除对象](#)”（第 267 页）。

---

**要卸载 Identity Manager 引擎，请执行以下操作：**

- 1 导航到安装时装入 iso 的位置。
- 2 从 .iso 文件的根目录中，运行以下命令：

```
./uninstall.sh
```

3 指定要卸装的组件。

例如，指定 1 会卸装 Identity Manager 引擎。您还可以同时卸装多个组件。例如，指定 1,2,3 会卸装 Identity Manager 引擎、Remote Loader 和扇出代理。

## 30.3 卸装 Identity Applications

1 导航到安装时装入 .iso 的位置。

2 从 .iso 文件的根目录中，运行以下命令：

```
./uninstall.sh
```

3 指定要卸装的组件。

例如，指定 1 会卸装 Identity Applications。

## 30.4 卸装 Identity Reporting 组件

您必须按以下顺序卸装 Identity Reporting 组件：

1. 删除驱动程序。有关详细信息，请参见第 30.4.1 节“删除报告驱动程序”（第 268 页）。
2. 删除 Identity Reporting。有关详细信息，请参见第 30.4.2 节“卸装 Identity Reporting”（第 269 页）。
3. 删除 Sentinel。有关详细信息，请参见第 30.4.3 节“卸装 Sentinel”（第 269 页）。

---

**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。

---

### 30.4.1 删除报告驱动程序

您可以使用 Designer 或 iManager 删除数据收集驱动程序和受管系统网关驱动程序。

- 1 停止驱动程序。根据所用的组件完成以下操作之一：
  - ◆ **Designer：**对于每个驱动程序，请右键单击驱动程序行，然后单击**在线 > 停止驱动程序**。
  - ◆ **iManager：**在“驱动程序集概述”页面上，单击每个驱动程序图像的右上角，然后单击**停止驱动程序**。
- 2 删除驱动程序。根据所用的组件完成以下操作之一：
  - ◆ **Designer：**对于每个驱动程序，请右键单击驱动程序行，然后单击**删除**。
  - ◆ **iManager：**在“驱动程序集概述”页面上，单击**驱动程序 > 删除驱动程序**，然后单击要删除的驱动程序。

## 30.4.2 卸载 Identity Reporting

在删除 Identity Reporting 之前，请确保您已删除数据收集驱动程序和受管系统网关驱动程序。有关详细信息，请参见第 30.4.1 节“删除报告驱动程序”（第 268 页）。

- 1 导航到安装时装入 .iso 的位置。
- 2 从 .iso 文件的根目录中，运行以下命令：  
`./uninstall.sh`
- 3 指定要卸载的组件。  
例如，指定 1 会卸载 Identity Reporting。

## 30.4.3 卸载 Sentinel

- 1 登录到 Sentinel 服务器。
- 2 导航到包含卸载脚本的目录：  
`/opt/novell/sentinel/setup/`
- 3 执行以下命令：  
`./uninstall.sh`
- 4 当系统提示您重新确认要继续卸载时，请按 y。  
该脚本首先停止服务，然后完全去除它。

## 30.5 卸载 Designer

- 1 关闭 Designer。
- 2 要卸载 Designer  
浏览到包含卸载脚本的目录，默认为 `<installation_directory>/designer/UninstallDesigner/Uninstall Designer for Identity Manager`。  
要执行脚本，请输入 `./uninstall`

## 30.6 卸载 Analyzer

- 1 关闭 Analyzer。
- 2 根据操作系统卸载 Analyzer：  
浏览到默认位于 `<installation_directory>/analyzer/UninstallAnalyzer` 目录中的 Uninstall Analyzer for Identity Manager 脚本。  
要执行脚本，请输入 `./Uninstall`



# 31 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。

## 31.1 User Application 和 RBPM 安装查错

下表列出了您可能会遇到的问题，以及解决这些问题的建议操作。如果问题仍然存在，请联系 NetIQ 代表。

| 问题                                                                                                                                                                                               | 建议的操作                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 从 configupdate 实用程序 (configupdate.sh) 中对 OSP 启用 CEF 审计时，尝试登录 IDMRPT 会失败。                                                                                                                         | <p>请执行以下步骤来解决此问题：</p> <ol style="list-style-type: none"><li>1. 导航到 /opt/netiq/idm/apps/tomcat/conf 目录中的 ism-configuration.properties 和 idmrptcore_logging.xml 文件。</li><li>2. 分别编辑 ism-configuration.properties 和 idmrptcore_logging.xml 文件。</li><li>3. 在 ism-configuration.properties 和 idmrptcore_logging.xml 文件中，分别将 <b>com.netiq.ism.audit.cef.protocol</b> 和 <b>&lt;protocol&gt;</b> 的值从 <b>tcp</b> 更改为 <b>TCP</b>。</li><li>4. 重新启动 Tomcat。</li></ol> |
| 如果 Identity Applications 和 Identity Reporting 安装在同一台服务器上，并且您为数据库创建选项选择了启动，将会在日志中看到一些异常。                                                                                                          | 要清除这些异常，请手动重新启动 Tomcat。                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 您要修改安装过程中创建的以下一或多个 User Application 配置设置： <ul style="list-style-type: none"><li>◆ 身份库连接和证书</li><li>◆ 电子邮件设置</li><li>◆ Identity Manager 引擎用户身份和用户组</li><li>◆ Access Manager 或 iChain 设置</li></ul> | <p>在独立于安装程序的情况下运行配置实用程序。</p> <p><b>Linux：</b>从安装目录（默认为 /opt/netiq/idm/apps/configupdate/）中运行以下命令：</p> <pre>./configupdate.sh</pre>                                                                                                                                                                                                                                                                                                                        |
| 启动 Tomcat 会导致以下异常：<br><br>port 8180 already in use                                                                                                                                               | 关闭 Tomcat（或其他服务器软件）的可能已在运行的任何实例。如果将 Tomcat 重新配置为使用 8180 以外的其他端口，请编辑 User Application 驱动程序的 config 设置。                                                                                                                                                                                                                                                                                                                                                     |
| 当 Tomcat 启动时，应用程序报告称找不到可信证书。                                                                                                                                                                     | 请务必使用安装 User Application 期间指定的 JDK 来启动 Tomcat。                                                                                                                                                                                                                                                                                                                                                                                                            |
| 无法登录门户管理页面。                                                                                                                                                                                      | 确保存在 User Application 管理员帐户。此帐户与 iManager 管理员帐户不同。                                                                                                                                                                                                                                                                                                                                                                                                        |

| 问题                   | 建议的操作                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 即使使用管理员帐户也无法创建新用户。   | User Application 管理员必须是顶层容器的受托者，并且应有主管权限。您可以尝试将 User Application 管理员的权限设置为等效于 LDAP 管理员的权限（使用 iManager）。                                                                                                                                                                                                                                                                                     |
| 启动应用程序服务器时发生密钥存储区错误。 | <p>应用程序服务器未使用安装 User Application 期间指定的 JDK。</p> <p>使用 keytool 命令导入证书文件：</p> <pre>keytool -import -trustcacerts -alias aliasName -file certFile -keystore ..\lib\security\cacerts -storepass changeit</pre> <ul style="list-style-type: none"> <li>◆ 使用为该证书选择的唯一名称替换 <i>aliasName</i>。</li> <li>◆ 使用证书文件的完整路径和名称替换 <i>certFile</i>。</li> <li>◆ 默认的密钥储存区口令为 changeit（如果有其他口令，请指定）。</li> </ul> |
| 无法发送电子邮件通知。          | <p>运行 configupdate 实用程序以检查是否提供了以下 User Application 配置参数的值：<b>Email From</b> 和 <b>Email Host</b>。</p> <p><b>Linux：</b>从安装目录（默认为 /opt/netiq/idm/apps/UserApplication/）运行以下命令：</p> <pre>./configupdate.sh</pre>                                                                                                                                                                                |

## 31.2 登录查错

下表列出了您可能会遇到的问题，以及解决这些问题的建议操作。如果问题仍然存在，请联系 NetIQ 代表。

| 问题                                                                    | 建议的操作                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 在大型环境（超过两百万个对象）中，用户无法登录                                               | 在 eDirectory 主服务器和复本服务器中均为 mail(Internet Mail Address) 属性添加索引，并将规则集设置为 Value。                                                                                                                                                                                                                                                                                        |
| 当您从 Identity Applications 页面注销时，SSPR 显示错误 5053 ERROR_APP_UNAVAILABLE。 | 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                                 | <ol style="list-style-type: none"> <li>1. 确保 SSPR 服务器具有使用 FQDN 创建的证书。</li> <li>2. 登录 User Application 服务器，并启动 ConfigUpdate (/opt/netiq/idm/apps/configupdate/) 实用程序。</li> <li>3. 导航到 <b>SSO 客户端 &gt; Self Service Password Reset</b>，并确保设置正确。</li> </ol> <p>如果 SSPR 安装在单独的服务器上，请确保 SSPR 证书已导入到 User Application 服务器上 /opt/netiq/idm/apps/tomcat/conf 中的 idm.jks。</p> |



| 问题                              | 建议的操作                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 访问 SSPR URL 时浏览器显示空白页           | <p>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：</p> <pre>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 &lt;IP&gt; doesn't match any of the subject alternative names: [IP]))</pre> <ol style="list-style-type: none"> <li>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 User Application 服务器，并起动 ConfigUpdate 实用程序。导航到 <b>SSO 客户端 &gt; Self Service Password Reset</b>，并确保设置正确。</li> <li>2. 通过覆盖 OSP 登录方法登录 SSPR（例如，<code>https://&lt;sspr sserver ip&gt;:&lt;port&gt;/sspr/private/Login?sso=false</code>）。</li> <li>3. 导航到页面右上角的<b>配置编辑器</b>。</li> <li>4. 指定<b>配置口令</b>，然后单击<b>登录</b>。</li> <li>5. 导航到 <b>LDAP &gt; LDAP 目录 &gt; 默认 &gt; 连接</b>。</li> <li>6. 如果 LDAP 证书不正确，请单击<b>清除</b>。</li> <li>7. 要重新导入证书，请单击<b>从服务器导入</b>。</li> <li>8. 导航到<b>设置 &gt; 单点登录 (SSO) 客户端 &gt; OAuth</b>，并在 <b>OAUTH Web 服务服务器证书</b> 下校验证书是否正确。</li> <li>9. 如果证书不正确，请单击<b>清除</b>。</li> <li>10. 要重新导入证书，请单击<b>从服务器导入</b>。</li> </ol> |
| 从不同的目录起动 ConfigUpdate 实用程序时发生错误 | <p>ConfigUpdate 实用程序会报告错误。它将不保存任何更改。例如，如果您使用 <code>/opt/netiq/idm/apps/configupdate/configupdate.sh</code> 命令起动 configupdate 实用程序，它不会起动。</p> <p>您应导航到 <code>/opt/netiq/idm/apps/configupdate/</code> 目录，然后运行 <code>./configupdate.sh</code> 命令。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

## 31.3 卸装查错

下表列出了您可能会遇到的问题，以及解决这些问题的建议操作。如果问题仍然存在，请联系 NetIQ 代表。

| 问题                      | 建议的操作                                                           |
|-------------------------|-----------------------------------------------------------------|
| 卸装过程报告未完成，但日志文件未显示失败信息。 | 默认情况下，卸装过程无法删除包含安装文件的 netiq 目录。如果已从计算机中去除所有 NetIQ 软件，则您可以删除该目录。 |



# A

## 使用身份库的多个实例

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

- [第 A.1 节“了解 eDirectory 中的 Identity Manager 对象”（第 275 页）](#)
- [第 A.2 节“在服务器上复制 Identity Manager 需要的对象”（第 275 页）](#)
- [第 A.3 节“使用“范围过滤”管理不同服务器上的用户”（第 276 页）](#)
- [第 A.4 节“了解身份库安装套件中的 Linux 包”（第 278 页）](#)

### A.1 了解 eDirectory 中的 Identity Manager 对象

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

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

### A.2 在服务器上复制 Identity Manager 需要的对象

如果 Identity Manager 环境需要多个服务器以运行多个 Identity Manager 驱动程序，则计划应确保在运行这些 Identity Manager 驱动程序的服务器上复制了某些 eDirectory 对象。

只要已过滤复本中包括驱动程序需要读取或同步的所有对象和特性，就可以使用这些复本。

请记住，必须为 Identity Manager 驱动程序对象授予对任何要同步的对象的足够 eDirectory 权限，方法是通过显式授权，或者使驱动程序对象的安全性等效于具有所需权限的对象。

运行 Identity Manager 驱动程序的 eDirectory 服务器（如果使用 Remote Loader，则是驱动程序参照的 eDirectory 服务器）必须保存下列主复本或读 / 写复本：

- 该服务器的驱动程序集对象。

运行 Identity Manager 的每个服务器都应该具有一个驱动程序集对象。除非有特定的需求，否则不要将多个服务器与同一个驱动程序集对象关联。

---

**注释：**创建驱动程序集对象时，默认设置是创建独立的分区。NetIQ 建议在驱动程序集对象上创建独立的分区。要使 Identity Manager 正常运行，服务器需要保存驱动程序集对象的完整复本。如果服务器具有驱动程序集对象的安装位置的完整复本，则不需要分区。

---

- ◆ 该服务器的服务器对象。

服务器对象是必需的，因为驱动程序使用它为对象生成密钥对。对于 Remote Loader 鉴定来说，它也至关重要。

- ◆ 需要同步驱动程序的该实例的对象。

除非这些对象的复本与驱动程序位于同一台服务器上，否则驱动程序不能同步对象。事实上，Identity Manager 驱动程序将同步在服务器上复制的 *所有* 容器中的对象，除非您创建用于范围过滤的规则以另行指定。

例如，如果需要驱动程序同步所有用户对象，最简单的方法是使用驱动程序的一个实例，该驱动程序位于保存所有用户的主复本或读 / 写复本的服务器上。

但是，许多环境都没有包含所有用户复本的单台服务器。相反，完整用户集分布在多台服务器上。在这种情况下，有三种选择：

- ◆ **将用户聚合到单台服务器。** 可通过向现有服务器添加复本来创建保存所有用户的单台服务器。如果需要，只要必需的用户对象和特性是已过滤复本的一部分，就可以使用已过滤复本减少 eDirectory 数据库的大小。
- ◆ **在启用范围过滤的情况下，使用多台服务器上的驱动程序的多个实例。** 如果不希望将用户聚合到单台服务器，则需要确定由哪个服务器集保存所有用户，同时在其中的每个服务器上设置 Identity Manager 驱动程序的一个实例。  
  
为防止驱动程序的不同实例尝试同步相同的用户，您将需要使用范围过滤来定义每个驱动程序实例应该同步的用户。范围过滤表示向每个驱动程序添加规则，以将驱动程序的管理范围限制到特定的容器。请参见[使用“范围过滤”管理不同服务器上的用户（第 276 页）](#)。
- ◆ **在没有范围过滤的情况下，使用多台服务器上的驱动程序的多个实例。** 如果要在不同服务器上运行驱动程序的多个实例且不使用已过滤复本，则需要对不同的驱动程序实例定义策略，以使驱动程序能够处理同一 Identity Vault 中的不同对象集。
- ◆ 创建用户时需要驱动程序使用的模板对象（如果选择使用模板）。

Identity Manager 驱动程序不要求指定用于创建用户的 eDirectory 模板对象。但是，如果指定在 eDirectory 中创建用户时驱动程序应使用模板，则必须在运行驱动程序的服务器上复制模板对象。

- ◆ Identity Manager 驱动程序管理用户时需要使用的任何容器。

例如，如果创建了一个名称为“非活动用户”的容器以保存禁用的用户帐户，则必须使运行驱动程序的服务器上具有该容器的主复本或读 / 写复本（最好是主复本）。

- ◆ 驱动程序需要参照的其他任何对象（例如，驱动程序的工作指令对象）。

如果驱动程序只是读取而不是更改其他对象，则服务器上的这些对象的复本可以是只读复本。

## A.3 使用“范围过滤”管理不同服务器上的用户

“范围过滤”表示向每个驱动程序添加规则，以将驱动程序的操作范围限制到特定的容器。在以下两种情况下，可能需要使用范围过滤：

- ◆ 希望驱动程序只同步特定容器中的用户。

默认情况下，Identity Manager 驱动程序将同步运行该驱动程序的服务器上复制的所有容器中的对象。要缩小该范围，必须创建范围过滤规则。

- ◆ 希望 Identity Manager 驱动程序同步所有用户，但不希望在同一服务器上复制所有用户。

要同步所有用户且不将其复制到单台服务器上，则需要确定由哪个服务器集保存所有用户，然后在其中的每台服务器上创建 Identity Manager 驱动程序的实例。为防止驱动程序的两个实例尝试与相同的用户同步，您将需要使用“范围过滤”来定义驱动程序的每个实例应该同步的用户。

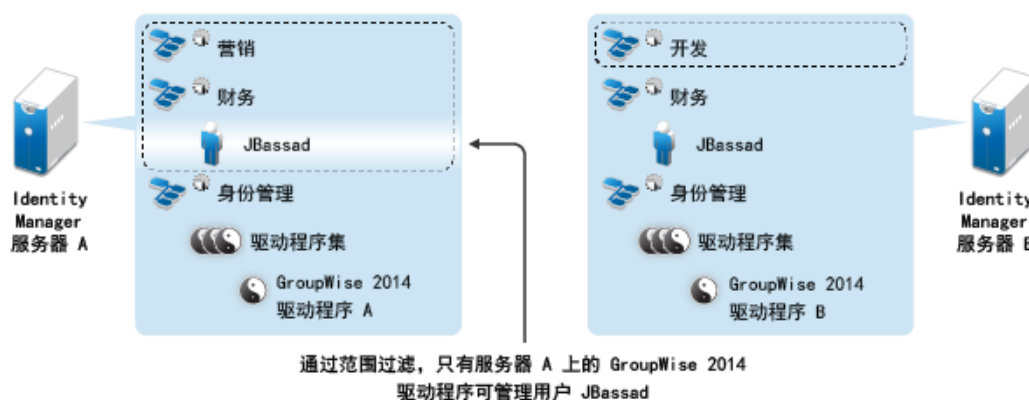
---

**注释：**即使服务器的复本当前未重叠，也应该使用范围过滤。以后，服务器上可能会添加复本，因而可能无意中产生重叠。如果实施了范围过滤，Identity Manager 驱动程序就不会尝试同步相同的用户，即使以后向服务器添加复本，也是如此。

---

图 A-1 在第 277 页中显示了一个示例身份库，它带有三个用于储存用户的容器：“营销”、“财务”和“开发”。同时它还显示保存驱动程序集的身份管理容器。其中每个容器都是一个独立的分区。在此示例中，Identity Manager 管理员有两个身份库服务器：服务器 A 和服务器 B。这两个服务器都不包含所有用户的副本。每个服务器包含三个分区中的两个，因此服务器保存项目的范围重叠。

图 A-1 范围过滤定义同步每个容器的驱动程序



管理员希望通过 GroupWise 2014 驱动程序同步树中的所有用户，但是不希望将这些用户的复本聚合到单台服务器。他选择使用两个 GroupWise 2014 驱动程序实例，每台服务器上安装一个。他在每台 Identity Manager 服务器上安装了 Identity Manager，并设置了 GroupWise 2014 驱动程序。

服务器 A 保存“市场营销”和“财务”容器的复本。另外，该服务器上还有一个“身份管理”容器的复本，该容器存放服务器 A 的驱动程序集以及服务器 A 的 GroupWise 2014 驱动程序对象。

服务器 B 保存“开发”容器、“财务”容器和“身份管理”容器的复本，最后一个容器存放服务器 B 的驱动程序集和服务器 B 的 GroupWise 2014 驱动程序对象。

由于服务器 A 和服务器 B 均保存了“财务”容器的复本，因此这两个服务器均保存了“财务”容器中的用户 JBassad。如果不使用范围过滤，GroupWise 2014 驱动程序 A 和 GroupWise 2014 驱动程序 B 都会同步 JBassad。由于范围过滤定义了同步每个容器的驱动程序，因此可以避免驱动程序的两个实例管理同一用户。

Identity Manager 附带一些预定义的规则。有两个规则可帮助执行范围过滤：**事件转换 — 范围过滤** — 包括子树和**事件转换 — 范围过滤** — 排除子树。有关详细信息，请参见《[NetIQ Identity Manager Understanding Policies Guide](#)》（NetIQ Identity Manager 了解策略指南）。

对于此示例，可以对服务器 A 和服务器 B 使用“包括子树”预定义规则。可为每个驱动程序定义不同的范围，以便它们只同步指定容器中的用户。服务器 A 将同步“市场营销”和“财务”。服务器 B 将同步开发容器。

## A.4 了解身份库安装套件中的 Linux 包

NetIQ eDirectory 包括 Linux 包系统，它们是一组工具，可用于简化各种 eDirectory 组件的安装和卸载。包中的 makefile 文件说明构建特定 eDirectory 组件的要求。包中还包含配置文件、实用程序、库、守护程序和使用随操作系统一起安装的标准 Linux 工具的手册页。

某些包依赖于其他包或 Identity Manager 组件（例如 NCI）。只有安装了所有依赖包才能让功能正常运作。

下表提供了 eDirectory 随附的 Linux 包的相关信息。所有包均带有 *novell-* 前缀。例如，*novell-NDSserv* 表示 NDSserv 包。

| 包         | 描述                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NOVLice   | 包含 NetIQ Import Convert Export 实用程序。此包依赖于 NOVLmgnt、NOVLxis 和 NLDAPbase 包。                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| NOVbase   | 代表目录用户代理。此包依赖于 NCI 包。<br><br>此包包含以下项目： <ul style="list-style-type: none"><li>◆ 包含 eDirectory 所需的 RSA 鉴定的鉴定工具箱。</li><li>◆ 与平台无关的系统抽象库、包含所有已定义目录用户代理功能的库，以及纲要扩展库。</li><li>◆ 组合的配置实用程序和目录用户代理测试实用程序。</li><li>◆ eDirectory 配置文件和手册页。</li></ul>                                                                                                                                                                                                                                                                         |
| NDScommon | 包含 eDirectory 配置文件、安装和卸载实用程序的手册页。此包依赖于 NDSbase 包。                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| NDSmasv   | 包含强制访问控制 (MASV) 所需的库。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| NDSserv   | 包含 eDirectory 服务器所需的所有二进制文件和库。它还包含用于管理系统上的 eDirectory 服务器的实用程序。此包依赖于 NDSbase、NDScommon、NDSmasv、NLDAPsdk、NOVLpkia 和 NOVLpkit 包。它还包含以下项目： <ul style="list-style-type: none"><li>◆ NDS 安装库、FLAIM 库、跟踪库、NDS 库、LDAP 服务器库、LDAP 安装库、索引编辑器库、DNS 库、合并库以及用于 LDAP SDK 的 LDAP 扩展库。</li><li>◆ eDirectory 服务器守护程序。</li><li>◆ DNS 的二进制文件，以及用于装载和卸载 LDAP 的二进制文件。</li><li>◆ 创建 MAC 地址所需的实用程序、用于跟踪服务器和更改服务器的某些全局变量的实用程序、用于备份和恢复 eDirectory 的实用程序，以及用于合并 eDirectory 树的实用程序。</li><li>◆ DNS、NDS 和 NLDAP 的启动脚本。</li><li>◆ 手册页。</li></ul> |

| 包         | 描述                                                                                                                                                                                                |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NDSrepair | 包含运行时库，以及用于更正 eDirectory 数据库中的问题的实用程序。此包依赖于 NDSbase 包。                                                                                                                                            |
| NLDAPbase | <p>包含 LDAP 库、LDAP 库的扩展以及以下 LDAP 工具：</p> <ul style="list-style-type: none"> <li>◆ ldapdelete</li> <li>◆ ldapmodify</li> <li>◆ ldapmodrdn</li> <li>◆ ldapsearch</li> </ul> <p>此包依赖于 NLDAPsdk 包。</p> |
| NOVLnmas  | 包含所有 NMAS 库，以及 NMAS 服务器所需的 nmasinst 二进制文件。此包依赖于 NICI 和 NDSmasv 包。                                                                                                                                 |
| NLDAPsdk  | 包含 LDAP 运行时的 NetIQ 扩展以及安全库（客户端 NICI）。                                                                                                                                                             |
| NOVLsubag | 包含运行时库，以及用于 eDirectory SNMP 子代理的实用程序。此包依赖于 NICI、NDSbase 和 NLDAPbase 包。                                                                                                                            |
| NOVLpklt  | 提供不需要 eDirectory 的 PKI 服务。此包依赖于 NICI 和 NLDAPsdk 包。                                                                                                                                                |
| NOVLpkis  | 提供 PKI 服务器服务。此包依赖于 NICI、NDSbase 和 NLDAPsdk 包。                                                                                                                                                     |
| NOVLsnmp  | 运行时库和用于 SNMP 的实用程序。此包依赖于 NICI 包。                                                                                                                                                                  |
| NDSdexvnt | 包含用于管理在 NetIQ eDirectory 中生成的针对其他数据库的事件的库。                                                                                                                                                        |
| NOVLpkia  | 提供 PKI 服务。此包依赖于 NICI、NDSbase 和 NLDAPsdk 包。                                                                                                                                                        |
| NOVLembox | 提供 eMBox 基础结构和 eMTools。                                                                                                                                                                           |
| NOVLimgnt | 包含用于 NetIQ 语言管理的运行时库。                                                                                                                                                                             |
| NOVLxis   | 包含用于 NetIQ XIS 的运行时库。                                                                                                                                                                             |
| NOVLsas   | 包含 NetIQ SAS 库。                                                                                                                                                                                   |
| NOVLntls  | 包含 NetIQ TLS 库。此包也写作 ntls。                                                                                                                                                                        |
| NOVLdif2  | 包含 NetIQ Offline Bulkload 实用程序，此包依赖于 NDSbase、NDSserv、NOVLntls、NOVLimgnt 和 NICI 包。                                                                                                                 |
| NOVLncp   | 包含 NetIQ Encrypted NCP Services for Linux。此包依赖于 NDScommon 包。                                                                                                                                      |





# B SLES 12 SP2 上简单的 Identity Manager 群集部署解决方案

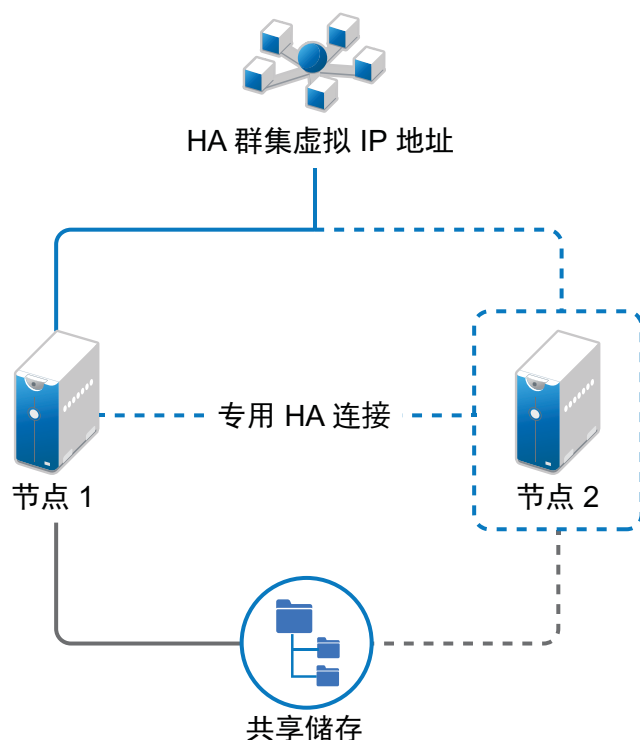
本附录逐步说明了如何在使用共享储存的受支持 SUSE Linux Enterprise Server (SLES) 群集环境中配置 eDirectory 和 Identity Manager，并提供了一个 Identity Manager 群集部署的示例。

- ◆ 第 B.1 节“先决条件”（第 281 页）
- ◆ 第 B.2 节“安装过程”（第 282 页）

对于使用共享储存的生产级 Linux 高可用性 (HA) 解决方案，建议在群集中实施屏蔽机制。尽管在群集中实施屏蔽机制的方法有多种，但在本示例中，我们采用的是使用节点分裂检测器 (SBD) 的 STONITH 资源。

图 B-1 在第 281 页显示了一个群集部署解决方案示例。

图 B-1 群集部署解决方案示例



## B.1 先决条件

- ◆ 两台运行 SLES 12 SP2 64 位的服务器作为节点
- ◆ 一台运行 SLES 12 SP2 64 位的服务器作为 iSCSI 服务器
- ◆ SLES12 SP2 64 位 HA Extension ISO 映像文件

- ◆ 六个静态 IP：
  - ◆ 每个节点有两个静态 IP 地址。
  - ◆ 一个静态 IP 地址用于群集。此 IP 地址将动态指派给当前运行 eDirectory 的节点。
  - ◆ 一个 IP 地址用于 iSCSI 服务器。

## B.2 安装过程

本节介绍安装和配置以下项目以设置群集环境的过程。有关配置 SLES High Availability Extension 的详细信息，请参见 [SUSE Linux Enterprise High Availability Extension](#) 指南。

### B.2.1 配置 iSCSI 服务器

iSCSI 目标是指配置为群集中所有节点的公用储存的设备。它是 Linux 服务器上创建的虚拟磁盘，可以让 iSCSI 发起程序通过以太网连接进行远程访问。iSCSI 发起程序是指群集中配置为与服务目标 (iSCSI) 连接的任一节点。iSCSI 目标应始终处于已启动且正在运行状态，以便任何作为发起程序的主机都能连接该目标。在 iSCSI 服务器上安装 iSCSI 目标之前，请确保 iSCSI 目标有足够的空间用于配置公用储存。安装 SLES 12 SP2 后，在其他两个节点上安装 iSCSI 发起程序包。

在安装 SLES 12 SP2 期间：

- 1 创建一个独立的分区，然后将分区路径指定为 iSCSI 共享储存分区。
- 2 安装 iSCSI 目标包。

要配置 iSCSI 服务器，请执行以下操作：

- 1 在目标服务器上创建一个块设备。
- 2 在终端中键入 `yast2 disk` 命令。
- 3 创建一个新的 Linux 分区并选择**不格式化**。
- 4 选择**不装入分区**。
- 5 指定分区大小。
- 6 在终端中键入 `yast2 iscsi-server` 或 `yast2 iscsi-lio-server` 命令。
- 7 单击**服务选项卡**，然后在**服务启动选项**中选择**引导时**。
- 8 在**目标选项卡**中，单击**添加**以输入分区路径（在安装 SLES 期间创建的路径）。
- 9 在**修改 iSCSI 目标启动程序设置**页面中，指定目标服务器的 iSCSI 客户端启动程序主机名，然后单击**下一步**。

例如，`iqn.sles12sp2node2.com` 和 `iqn.sles12sp2node3.com`。

- 10 单击**完成**。
- 11 在终端中运行 `cat /proc/net/iet/volume` 命令，以校验是否已安装 iSCSI 目标。

## B.2.2 在所有节点上配置 iSCSI 发起程序

要连接到 iSCSI 目标，您必须在所有群集节点上配置 iSCSI 发起程序。

要配置 iSCSI 发起程序，请执行以下操作：

- 1 安装 iSCSI 发起程序包。
- 2 在终端中运行 `yast2 iscsi-client`。
- 3 单击**服务选项卡**，然后在**服务启动选项**中选择**引导时**。
- 4 单击**已连接目标选项卡**，然后单击**添加**以输入 iSCSI 目标服务器的 IP 地址。
- 5 选择**无鉴定**。
- 6 单击**下一步**，然后单击**连接**。
- 7 单击**切换启动方式**将启动选项从手动更改为自动，然后单击**下一步**。
- 8 单击**下一步**，然后单击**确定**。
- 9 要检查目标服务器上已连接发起程序的状态，请在目标服务器上运行 `cat /proc/net/iet/session` 命令。随即会显示已连接到 iSCSI 服务器的发起程序列表。

## B.2.3 对共享储存进行分区

创建两个共享储存分区：一个用于 SBD，另一个用于 Cluster File System。

要对共享储存进行分区，请执行以下操作：

- 1 在终端中运行 `yast2 disk` 命令。
- 2 在**专家分区程序**对话框中选择共享卷。在本示例中，请从**专家分区程序**对话框中选择 **sdb**。
- 3 单击**添加**，选择**主分区**选项，然后单击**下一步**。
- 4 选择**自定义大小**，然后单击**下一步**。在本示例中，自定义大小为 100 MB。
- 5 在**格式化选项**下，选择**不格式化分区**。在本示例中，文件系统 ID 为 0x83 Linux。
- 6 在**装入选项**下，选择**不装入分区**，然后单击**完成**。
- 7 单击**添加**，然后选择**主分区**。
- 8 单击**下一步**，选择**最大大小**，然后单击**下一步**。
- 9 在**格式化选项**中，选择**不格式化分区**。在本示例中，指定了 0x83 Linux 作为文件系统 ID。
- 10 在**装入选项**中，选择**不装入分区**，然后单击**完成**。

## B.2.4 安装 HA Extension

要安装 HA Extension，请执行以下操作：

- 1 访问 [SUSE 下载网站](#)。  
对于每个可用平台，SUSE Linux Enterprise High Availability Extension (SLE HA) 提供了两个 ISO 映像供您下载。媒体 1 包含二进制包，媒体 2 包含源代码。

---

**注释：**根据您的系统体系结构选择并安装相应的 HA Extension ISO 文件。

---

- 2 将媒体 1 ISO 文件下载到每台服务器上。

- 3 打开 **YaST 控制中心**对话框，然后单击**附加产品 > 添加**。
- 4 单击**浏览**并选择 DVD 或本地 ISO 映像，然后单击**下一步**。
- 5 在**模式**选项卡中的**主要功能**下，选择**高可用性**。  
确保已安装高可用性下的所有组件。
- 6 单击**接受**。

## B.2.5 设置 Softdog 检查包

在 SLES HA Extension 中，默认启用内核中的检查包支持。它随附了提供硬件特定的检查包驱动程序的多不同内核模块。在系统引导过程中，会自动装载适用于您硬件的检查包驱动程序。

- 1 启用 softdog 检查包：  

```
echo softdog > /etc/modules-load.d/watchdog.conf
```

```
systemctl restart systemd-modules-load
```
- 2 测试 softdog 模块是否已正确装载：  

```
lsmod | grep dog
```

## B.2.6 配置 HA 群集

此示例假设您要在群集中配置两个节点。

**设置第一个节点：**

- 1 以 root 用户身份登录到要用作群集节点的物理机或虚拟机。
- 2 运行以下命令：  

```
ha-cluster-init
```

该命令会检查是否存在 NTP 配置和硬件检查包服务。此操作会生成用于 SSH 存取和 Csync2 同步的公共和私有 SSH 密钥，并启动相应的服务。
- 3 配置群集通讯层：
  - 3a 输入要绑定的网络地址。
  - 3b 输入多路广播地址。脚本将建议使用可用作默认值的随机地址。
  - 3c 输入多路广播端口。默认端口号为 5405。
- 4 将 SBD 设置为节点屏蔽机制：
  - 4a 按 **y** 以使用 SBD。
  - 4b 输入要为 SBD 使用的块设备分区的持久路径。该路径对于群集中的两个节点必须一致。
- 5 配置用于群集管理的虚拟 IP 地址：
  - 5a 按 **y** 以配置虚拟 IP 地址。
  - 5b 输入一个未使用的 IP 地址，作为 SUSE Hawk GUI 的管理 IP。例如， **192.168.1.3**。  
您可以连接到该虚拟 IP 地址，而无需登录单个群集节点。

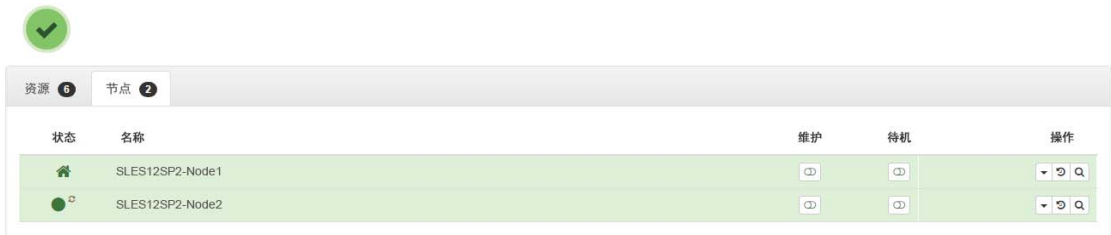
第一个节点启动并运行后，使用 **ha-cluster-join** 命令添加第二个群集节点。

### 设置第二个节点：

- 1 以 root 用户身份登录要用于连接群集的物理机或虚拟机。
- 2 运行以下命令：  

```
ha-cluster-join
```

如果未配置 NTP，则会显示一条讯息。该命令会检查是否存在硬件检查包设备，如果不存在，将发出通知。
- 3 输入第一个节点的 IP 地址。
- 4 输入第一个节点的 root 口令。
- 5 登录 SUSE Hawk GUI，然后单击**状态** > **节点**。例如， <https://192.168.1.3:7630/cib/live>。



## B.2.7 在群集节点上安装并配置 eDirectory 和 Identity Manager

- 1 在群集节点上安装 eDirectory：  
安装受支持版本的 有关在高可用性群集上配置 eDirectory 的逐步说明，请参见 《[eDirectory Installation Guide](#)》（eDirectory 安装指南）中的 “[Deploying eDirectory on High Availability Clusters](#)” （在高可用性群集上部署 eDirectory）。

---


**重要：**在节点 1 上安装 eDirectory 之前，请确保已在该节点上配置虚拟 IP。

---

- 2 使用 “元目录服务器” 选项在节点 1 上安装 Identity Manager。
- 3 使用 DCLUSTER\_INSTALL 选项在节点 2 服务器上安装 Identity Manager 引擎。  
在终端中运行 `./install.bin -DCLUSTER_INSTALL="true"` 命令。  
安装程序将直接安装 Identity Manager 文件，而不与 eDirectory 发生任何交互。

## B.2.8 配置 eDirectory 资源

- 1 登录 SUSE Hawk GUI。
- 2 单击**添加资源**，然后创建新组。
  - 2a 单击**组**旁边的
  - 2b 指定组 ID。例如，`组 1`。  
创建组时，确保选择了以下子资源：
    - ♦ `stonith-sbd`
    - ♦ `admin_addr` （群集 IP 地址）
- 3 在**元数据属性**选项卡中，将 **target-role** 字段设置为 `Started`，并将 **is-managed** 字段设置为 `Yes`。

- 4 单击**编辑配置**，然后单击在第 2 步中创建的组旁边的 。
- 5 在子项字段中，添加以下子资源：

- ◆ `shared-storage`
- ◆ `eDirectory-resource`

例如，在该组中，应该按以下顺序添加资源：

- ◆ `stonith-sbd`
- ◆ `admin_addr`（群集 IP 地址）
- ◆ `shared-storage`
- ◆ `eDirectory-resource`

如果需要，可以更改资源名称。每个资源都有一组参数需要定义。有关 `shared-storage` 和 `eDirectory` 资源示例的信息，请参见 [eDirectory](#) 和 [共享储存子资源的原始值](#)。

## B.2.9 eDirectory 和共享储存子资源的原始值

默认情况下，`stonith-sbd` 和 `admin_addr` 资源是在初始化群集节点时通过高可用性群集命令配置的。

**表 B-1** `shared-storage` 的示例

|                     |                                                                                                                   |
|---------------------|-------------------------------------------------------------------------------------------------------------------|
| 资源 ID               | 共享储存资源的名称                                                                                                         |
| Class               | ocf                                                                                                               |
| Provider            | heartbeat                                                                                                         |
| Type                | Filesystem                                                                                                        |
| device              | /dev/sdc1                                                                                                         |
| directory           | /shared                                                                                                           |
| fstype              | xfs                                                                                                               |
| operations          | <ul style="list-style-type: none"><li>◆ start (60, 0)</li><li>◆ stop (60, 0)</li><li>◆ monitor (40, 20)</li></ul> |
| is-managed          | Yes                                                                                                               |
| resource-stickiness | 100                                                                                                               |
| target-role         | Started                                                                                                           |

**表 B-2** `eDirectory-resource` 的示例

|       |                                                |
|-------|------------------------------------------------|
| 资源 ID | eDirectory 资源的名称                               |
| Class | systemd                                        |
| Type  | ndsdtmpl-shared-conf-nds.conf@-shared-conf-env |


---

|                     |                                                                                                                          |
|---------------------|--------------------------------------------------------------------------------------------------------------------------|
| operations          | <ul style="list-style-type: none"> <li>♦ start (100, 0)</li> <li>♦ stop (100, 0)</li> <li>♦ monitor (100, 60)</li> </ul> |
| target-role         | Started                                                                                                                  |
| is-managed          | Yes                                                                                                                      |
| resource-stickiness | 100                                                                                                                      |
| failure-timeout     | 125                                                                                                                      |
| migration-threshold | 0                                                                                                                        |

---

## B.2.10 更改位置约束分数

将位置约束分数更改为 0。

- 1 登录 SUSE Hawk GUI。
- 2 单击**编辑配置**。
- 3 在**约束**选项卡中，单击群集节点 1 旁边的 。
- 4 在**简单**选项卡中，将分数设置为 0。
- 5 单击**应用**。

务必将群集中所有节点的分数设置为 0。

---

**注释：**当从 SUSE Hawk GUI 中使用**状态 > 资源 > 迁移**选项将资源从一个节点迁移到另一个节点时，位置约束分数将更改为 *Infinity* 或 *-Infinity*。如此只会将自选设置提供给群集中的一个节点，并且将导致 eDirectory 操作延迟。

---





# C Tomcat 应用程序服务器上的示例 Identity Applications 群集部署解决方案

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

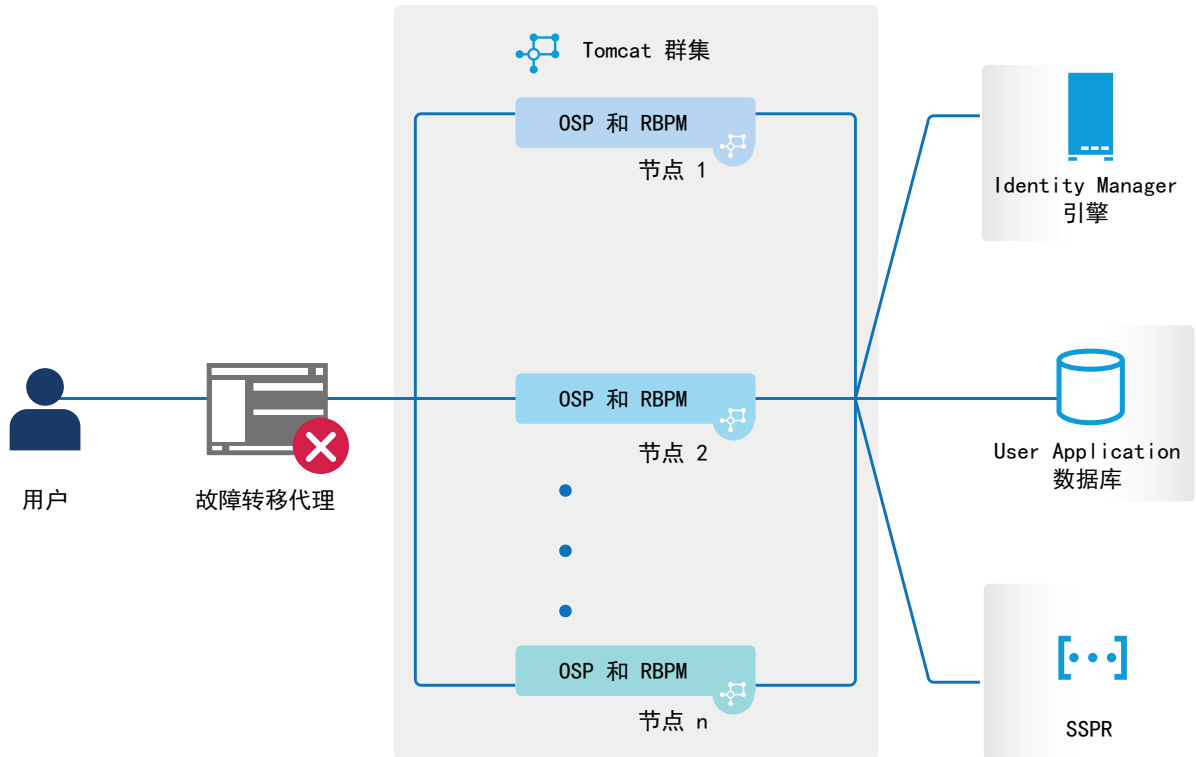
使用群集，您可以在多个并行服务器（群集节点）上运行 Identity Applications，从而实现高可用性。要构建群集，您需要将几个 Tomcat 实例（节点）组合在一起。负载将分布在不同的服务器之间，即使有服务器发生故障，您仍可通过其他群集节点来访问 Identity Applications。若要实现故障转移，您可以创建一个 Identity Applications 群集，然后将这些 Identity Applications 配置为充当单个服务器。不过，此配置不包括 Identity Reporting。

建议使用负载均衡器软件，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。负载均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 C-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均衡器路由。
- 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使用此方法。
- 您熟悉 eDirectory、Identity Manager 引擎、Identity Applications、Tomcat 应用程序服务器和 User Application 数据库的安装过程。
- 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，您可以使用支持的任何数据库，例如 Oracle 或 MsSQL。
- 所有 User Application 节点均与 eDirectory 和 User Application 数据库的同一个实例通讯。您可以根据需要增加 User Application 实例数量。

图 C-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。

## C.1 先决条件

- 两台运行 SUSE Linux Enterprise Server (SLES) 12 SP2 64 位或 RedHat Enterprise Linux (RHEL) 7.3 64 位的服务器作为安装了所有相关库的节点。有关详细信息，请参见有关 RHEL 的章节。
- 已安装 Identity Manager 4.7 组件。
- 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均衡解决方案安装在单独的计算机上。

## C.2 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 4.7 引擎。有关逐步指导，请参见第 9.1 节“安装 Identity Manager 引擎”（第 83 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 安装数据库。可以使用随 Identity Applications 一起安装的 PostgreSQL 数据库。不过，建议将数据库安装在单独的服务器上。
3. 在节点 1 上，安装并配置 Identity Applications。

在安装期间，请确保：

- ◆ 选择新数据库选项
- ◆ 提供唯一的工作流程引擎 ID。例如，节点 1。
- ◆ 群集中的所有 User Application 节点上均有可用的数据库 jar 文件。对于 PostgreSQL，postgresql-9.4.1212.jar 位于 /opt/netiq/idm/postgres。

Identity Applications 使用主密钥加密敏感数据。在 Identity Applications 配置期间，安装程序将创建新的主密钥。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。主密钥储存在 /opt/netiq/idm/apps/tomcat/conf/ 目录中 ism-configuration.properties 文件内的属性 com.novell.idm.masterkey 下。

有关详细指导，请参见第 9.3 节“安装 Identity Applications”（第 88 页）。

4. 在节点 2 上，安装并配置 Identity Applications。

在安装期间，请确保：

- ◆ 选择现有数据库选项
- ◆ 提供唯一的工作流程引擎 ID。例如，节点 2。
- ◆ 群集中的所有 User Application 节点上均有可用的数据库 jar 文件。对于 PostgreSQL，postgresql-9.4.1212.jar 位于 /opt/netiq/idm/postgres。

完成节点 2 上的 User Application 配置后，复制节点 1 的 ism-configuration.properties 中的主密钥值，并替换节点 2 的 ism-configuration.properties 中储存的相应主密钥值。主密钥储存在 ism-configuration.properties (/opt/netiq/idm/apps/tomcat/conf/) 中的属性 "com.novell.idm.masterkey" 下。

5. 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：

完成 SSPR 安装后，启动 Tomcat 并启动 SSPR（http://<IP>:<端口>/sspr/private/config/ConfigEditor），然后登录其中。单击配置编辑器 > 设置 > 安全性 > 重定向白名单。

- a. 单击添加值并指定以下 URL：

OSP: http://<dns of the failover>:<port>/osp

- b. 保存更改。

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

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

- e. 要在节点 1 上更新 SSPR 信息，请启动位于 /opt/netiq/idm/apps/UserApplication/configupdate.sh 的配置实用程序。

- f. 单击 SSO 客户端 > Self Service Password Reset，输入客户端 ID、口令和 OSP Auth 重定向 URL 参数的值。有关详细信息，请参见第 22.3 节“针对分布式环境或群集环境更新仪表板中的 SSPR 链接”（第 208 页）。

---

**注释：**校验节点 2 中是否更新了这些参数的值。

---

6. 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：

```
/opt/netiq/idm/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：/opt/netiq/idm/jre/bin/keytool -genkey -keyalg RSA -keysize 2048 -keystore osp.jks -storepass  
changeit -keypass changeit -alias osp -validity 1800 -dname "cn=mydnsname"

---

**注释：**确保密钥口令与在 OSP 安装期间提供的口令相同。或者，可以使用配置更新实用程序加入密钥存储区口令来更改该口令。

---

7. （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：  

```
/opt/netiq/idm/jre/bin/keytool -list -v -keystore osp.jks -storepass changeit
```
8. 备份位于 /opt/netiq/idm/apps/osp\_sspr/osp/ 中的原始 osp.jks 文件，并将新 osp.jks 文件复制到此位置。
9. 将节点 1 上位于 /opt/netiq/idm/apps/osp\_sspr/osp/ 中的新 osp.jks 文件复制到群集中的其他 User Application 节点上。
10. 在节点 1 中启动配置实用程序，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。
  - 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 /TOMCAT\_INSTALLED\_HOME/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。

---

11. 在位于 /TOMCAT\_INSTALLED\_HOME/bin/ 目录下的 setenv.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。
12. 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“管理”选项卡。  
User Application 将显示应用程序配置门户。
  - d. 单击[超速缓存](#)。

User Application 将显示“超速缓存管理”页面。

- e. 为支持群集属性选择 **True**。
- f. 单击**保存**。
- g. 重新启动 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。如果您要将此协议更改为使用 TCP，请参见《[NetIQ Analyzer for Identity Manager Administration Guide](#)》（NetIQ Analyzer for Identity Manager 管理指南）中的“[Portal Configuration Tasks](#)”（门户配置任务）。

---

13. 为群集启用许可权限索引。

- a. 在节点 1 中登录 iManager，然后导航到**查看对象**。
- b. 在**系统**下，导航到包含 User Application 驱动程序的驱动程序集。
- c. 选择 **AppConfig > AppDefs > > 配置**
- d. 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>
```

- e. 单击**确定**。

14. 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 <https://tomcat.apache.org/tomcat-8.5-doc/cluster-howto.html> 中的步骤操作。

15. 在所有节点上重新启动 Tomcat。

16. 为群集配置 User Application 驱动程序。

在群集中，必须将 User Application 驱动程序配置为使用群集负载均衡器的 DNS 名称。可使用 iManager 来配置 User Application 驱动程序。

- a. 登录用于管理 Identity Manager 引擎的 iManager。
- b. 在 iManager 导航框架中，单击 **Identity Manager 节点**。
- c. 单击 **Identity Manager 概述**。
- d. 使用搜索页面显示“Identity Manager 概述”，以查找包含 User Application 驱动程序和 Roles and Resource Service 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：  
一个菜单即会显示，其中列出了用于启动和停止驱动程序以及编辑驱动程序属性的命令。
- f. 选择**编辑属性**。
- g. 在“驱动程序参数”部分，将**主机**更改为发送程序的主机名或 IP 地址。

- h. 单击**确定**。
  - i. 重新启动驱动程序。
- 17. 要更改 Roles and Resource Service 驱动程序的 URL，请重复步骤 18a 到 18f，然后单击**驱动程序配置**，用负载均衡器 DNS 名称更新 **User Application URL**。
- 18. 确保针对 User Application 节点的负载均衡器软件中创建的群集启用了会话粘性。
- 19. 在 Identity Manager 仪表板上配置客户端设置。有关详细信息，请参见《[NetIQ Identity Manager - Administrator's Guide to the Identity Applications](#)》（NetIQ Identity Manager - Identity Applications 管理员指南）中的“[Configuring Client Settings Mode](#)”（配置客户端设置模式）。