NetIQ® Identity Manager

安装和升级指南 - Linux

2024 年 5 月

法律声明

版权所有 2009 - 2024 Open Text。保留所有权利。

Open Text 及其关联公司和许可方 （统称为 “Open Text”）对其产品与服务的担保，可能仅述于此类产品和服务随附的明确担保声明中。不可将此处所列任何内容解释为构成额外担保。 Open Text 不对本文档所含的技术、编辑错误或遗漏承担责任。此处包含的信息如有更改，恕不另行通知。如需其他信息 （如与证书相关的声明和商标），请访问 http://www.microfocus.com/about/legal/ (http://www.microfocus.com/about/legal/)。

目录

关于本文档和库 13

I Identity Manager 环境概述 15

1 Identity Manager 组件简介 17

Identity Manager 服务器组件 . . . 18
Identity Manager 服务器 . . . 19
Remote Loader . . . 19
扇出代理 . . . 20
Identity Console . . . 20
Identity Applications 组件 . . . 20
User Application . . . 21
鉴定服务 . . . 21
Self-Service Password Reset . . . 21
Web 应用程序服务器 . . . 21
Identity Applications 数据库 . . . 22
Identity Applications 的驱动程序 . . . 22
Identity Reporting 组件 . . . 22
Identity Reporting . . . 23
鉴定服务 . . . 23
Self-Service Password Reset . . . 23
Identity Reporting 数据库 . . . 23
Web 应用程序服务器 . . . 24
Identity Reporting 的驱动程序 . . . 24
Sentinel Log Management for Identity Governance and Administration . . . 25
Identity Manager 工具 . . . 25
Designer for Identity Manager . . . 25
Analyzer for Identity Manager . . . 25
功能体系结构 . . . 26
Identity Manager 的部署选项 . . . 27
Identity Manager 部署示例 . . . 28
高级版部署示例 . . . 29
标准版部署示例 . . . 31

II 规划 Identity Manager 安装 33

2 计划安装 35

实施核对清单 . . . 35
建议的安装方案和服务器设置 . . . 36
确定何时安装 SLM for IGA . . . 37
在分布式环境中安装的注意事项 . . . 37
确定硬件要求 . . . 39
系统要求工作表 . . . 39
在 SLES 服务器上安装 Identity Manager . . . 39

在 RHEL 服务器上安装 Identity Manager 41
先决条件 41
确保服务器上已安装依赖库 42
在 RHEL 9.x 上创建用于安装媒体的储存库 42
在 RHEL 8.x 上创建用于安装媒体的储存库 44
运行先决条件检查 45

3 安装 Identity Manager 组件的注意事项 47

安装顺序 47
了解安装和配置过程 47
安装 Identity Manager 引擎组件和 Remote Loader 的注意事项 49
安装 Identity Applications 组件的注意事项 50
安装注意事项 50
数据库注意事项 50
配置 Identity Applications 的数据库 51
安装 Identity Reporting 组件的注意事项 54
Identity Reporting 的先决条件 54
Identity Reporting 的身份审计事件 54
安装 Designer 的注意事项 55
安装 Analyzer 的注意事项 56
安装 SLM for IGA 的注意事项 56
查看 Identity Manager 组件使用的端口 57

III 安装和配置 Identity Manager 组件 59

4 安装 Identity Manager 61

执行交互式安装 61
以无提示模式安装 61
以非 root 用户身份安装 Identity Manager 引擎 62
安装 NICI 62
以非 root 用户身份安装身份库 63
以非 root 用户身份安装引擎 65
安装 SSPR 65
以交互模式安装 SSPR 66
以无提示模式安装 SSPR 66
安装 Remote Loader 66
交互式安装 66
无提示安装 67
安装 Designer 67
安装 Analyzer 67
使用向导安装 Analyzer 68
以无提示模式安装 Analyzer 68
将 XULRunner 添加到 Analyzer.ini 中 69
安装 Sentinel Log Management for Identity Governance and Administration 69
以 Root 用户身份安装 Sentinel Log Management 69
以非 Root 用户身份安装 Sentinel Log Management 70
安装 Java Remote Loader 71
了解目录结构 72

5 配置 Identity Manager 组件 75

在配置期间使用不可猜出的口令 . . . 75
了解配置参数 . . . 75
创建和配置驱动程序集 . . . 83
配置 Identity Manager 组件 . . . 84
执行交互式配置 . . . 85
执行无提示配置 . . . 85
配置 SSPR . . . 85
执行交互式配置 . . . 85
执行无提示配置 . . . 86
在 OSP 服务器上修改单点登录访问设置 . . . 86

6 完成安装的最后步骤 87

配置 Identity Vault . . . 87
创建身份库的值索引 . . . 87
手动将 Identity Applications 和 Identity Reporting 证书导入到身份库中 . . . 88
将非管理员用户配置为身份库管理员 . . . 88
配置 Remote Loader 和驱动程序 . . . 88
配置已连接系统 . . . 89
创建和配置驱动程序集 . . . 89
创建驱动程序 . . . 91
定义策略 . . . 92
配置忘记口令管理 . . . 92
使用 Self Service Password Reset 进行忘记口令管理 . . . 92
使用外部系统进行忘记口令管理 . . . 94
针对分布式环境或群集环境更新仪表板中的 SSPR 链接 . . . 96
配置 Identity Applications . . . 96
储存 Configupdate 实用程序口令 . . . 97
配置 Identity Applications 的设置 . . . 97
指定权限索引的位置 . . . 121
部署适用于 Identity Applications 的 REST API . . . 122
配置 Identity Applications 的 Oracle 数据库 . . . 122
使用 Oracle 服务名称访问 Oracle 数据库 . . . 123
手动创建数据库纲要 . . . 124
配置 Identity Applications 的单点登录设置 . . . 125
启动 Identity Applications . . . 125
Identity Applications 的配置和用法注意事项 . . . 126
配置数据收集的运行时环境 . . . 126
将数据收集服务驱动程序配置为从 Identity Applications 收集数据 . . . 127
迁移数据收集服务驱动程序 . . . 128
添加对自定义属性和对象的支持 . . . 130
添加多个驱动程序集支持 . . . 132
将驱动程序配置为使用 SSL 在远程模式下运行 . . . 133
配置 Identity Reporting . . . 135
配置受管系统网关驱动程序 . . . 135
在 “ 身份数据收集服务 ” 页面中手动添加数据源 . . . 135
对 Oracle 数据库运行报告 . . . 136
手动生成数据库纲要 . . . 136
部署 Identity Reporting 的 REST API . . . 141
连接远程 Remote PostgreSQL 数据库 . . . 141
在 OSP 中为采用分布式设置的 Identity Reporting 注册客户端 . . . 142
Identity Reporting 的安装后步骤 . . . 142

完成非 Root 用户安装 142
为口令策略创建容器 143
增加对电子邮件通知中的图形的支持 143
激活 Identity Manager 143
为分布式部署创建 SSL 证书 144

IV 在 FIPS 模式下配置 Identity Manager 147

7 为 FIPS 配置 JRE 149

8 在 FIPS 模式下配置 Identity Manager 引擎 151

操作步骤 151

9 在 FIPS 模式下配置扇出代理 153

操作步骤 153

10 在 FIPS 模式下配置 Identity Applications 和 Identity Reporting 155

操作步骤 155

11 在 FIPS 模式下配置 Remote Loader 159

V 将 Identity Manager 数据迁移到新安装 161

12 准备迁移 Identity Manager 163

执行迁移的核对清单 163

13 将 Identity Manager 迁移到新服务器 165

先决条件 165
准备要迁移的 Designer 项目 165
将 Identity Manager 引擎迁移到新服务器 166
复制驱动程序集的服务器特定信息 166
在 Designer 中复制服务器特定信息 167
在 Identity Console 中更改服务器特定的信息 167
更改 User Application 的服务器特定信息 168
迁移 Identity Applications 168
将数据库迁移到新服务器 168
在新服务器上安装 Identity Applications 170
迁移 Identity Reporting 171
更新 Identity Reporting 的驱动程序 171
部署 Identity Reporting 的驱动程序 171
将现有数据迁移到新数据库 172
设置新 Reporting 服务器 175
创建数据同步策略 175

VI 升级 Identity Manager **177**

14 准备升级 Identity Manager **179**

Identity Manager 的升级核对清单 . . . 179
了解升级过程 . . . 180
支持的升级路径 . . . 181
从 Identity Manager 4.7.5 版本升级 . . . 181
从 Identity Manager 4.8.x 版本升级 . . . 183
备份当前配置 . . . 184
导出 Designer 项目 . . . 184
导出驱动程序配置 . . . 185

15 升级 Identity Manager 组件 **187**

升级顺序 . . . 187
升级注意事项 . . . 188
升级 Designer . . . 189
升级 Identity Manager 引擎 . . . 190
安装前校验 Linux RPM . . . 190
升级身份库 . . . 190
升级 Identity Manager 引擎 . . . 191
以非 Root 用户身份升级 Identity Manager 引擎 . . . 193
升级 Remote Loader . . . 193
升级 Java Remote Loader . . . 194
停止和启动 Identity Manager 驱动程序 . . . 194
停止驱动程序 . . . 195
启动驱动程序 . . . 195
升级 Identity Manager 驱动程序 . . . 196
创建新驱动程序 . . . 197
用包的内容替换现有内容 . . . 197
保留当前内容并通过包添加新内容 . . . 197
升级 Identity Applications . . . 198
升级注意事项 . . . 199
系统要求 . . . 201
了解升级程序 . . . 201
升级 PostgreSQL . . . 201
升级 Identity Applications 组件 . . . 201
Identity Applications 组件的升级后任务 . . . 204
升级后校验版本号 . . . 207
升级 Identity Reporting . . . 207
升级注意事项 . . . 208
升级 Sentinel Log Management for IGA . . . 208
升级 Identity Reporting . . . 208
Reporting 的升级后步骤 . . . 209
校验 Identity Reporting 的升级 . . . 210
升级 Analyzer . . . 211
升级后任务 . . . 211
升级服务驱动程序 . . . 211
去除未使用的 Log4j JAR . . . 212
将新服务器添加到驱动程序集 . . . 212
从驱动程序集中去除旧服务器 . . . 212
将自定义策略和规则恢复到驱动程序 . . . 213

使用 Designer 将自定义策略和规则恢复为驱动程序 . . . 214
使用 Identity Console 将自定义策略和规则恢复到驱动程序 . . . 214

16 从高级版切换到标准版 215

VII 部署 Identity Manager 容器 217

17 规划容器部署 219

系统要求 . . . 219
获取 Docker 映像 . . . 219

18 Identity Manager 容器部署 221

最佳实践 . . . 221
管理容器卷数据 . . . 222
创建无提示属性文件 . . . 222
部署 Remote Loader 容器后自动启动 Remote Loader 实例 . . . 224
容器部署模式 . . . 225
在单台服务器上部署容器 . . . 225
先决条件 . . . 225
部署 Identity Manager 引擎容器 . . . 226
部署 Remote Loader 容器 . . . 226
部署扇出代理容器 . . . 227
通过身份库证书颁发机构生成证书 . . . 227
部署 OSP 容器 . . . 229
部署 PostgreSQL 容器 . . . 229
部署 Identity Applications 容器 . . . 230
部署表单渲染器容器 . . . 231
部署 ActiveMQ 容器 . . . 232
部署 Identity Reporting 容器 . . . 232
部署 SSPR 容器 . . . 233
部署 Identity Console 容器 . . . 234
在分布式服务器上部署容器 . . . 235
设置覆盖网络 . . . 235
先决条件 . . . 236
公开容器访问的端口 . . . 237
部署 Identity Manager 引擎容器 . . . 238
部署 Remote Loader 容器 . . . 239
部署扇出代理容器 . . . 239
通过身份库证书颁发机构生成证书 . . . 240
部署 OSP 容器 . . . 244
部署 PostgreSQL 容器 . . . 244
部署 Identity Applications 容器 . . . 245
部署表单渲染器容器 . . . 246
部署 ActiveMQ 容器 . . . 247
部署 Identity Reporting 容器 . . . 248
部署 SSPR 容器 . . . 248
部署 Identity Console 容器 . . . 250

19 升级 Identity Manager 容器 251

容器更新先决条件 . . . 251

更新分布式服务器上的容器 . . . 251
更新 Identity Manager 引擎容器 . . . 252
更新 Remote Loader 容器 . . . 252
更新扇出代理容器 . . . 253
更新 OSP 容器 . . . 253
更新 PostgreSQL 容器 . . . 254
更新 Identity Applications 容器 . . . 255
更新表单渲染器容器 . . . 255
更新 ActiveMQ 容器 . . . 255
更新 Identity Reporting 容器 . . . 256
更新 SSPR 容器 . . . 256
更新 Identity Console 容器 . . . 256
更新单台服务器上的容器 . . . 257
更新 Identity Manager 引擎容器 . . . 257
更新 Remote Loader 容器 . . . 257
更新扇出代理容器 . . . 258
更新 OSP 容器 . . . 258
更新 PostgreSQL 容器 . . . 259
更新 Identity Applications 容器 . . . 260
更新表单渲染器容器 . . . 260
更新 ActiveMQ 容器 . . . 260
更新 Identity Reporting 容器 . . . 261
更新 SSPR 容器 . . . 261
更新 Identity Console 容器 . . . 261

VIII 使用 Ansible 部署 Identity Manager 容器 263

20 规划部署 265

准备 Ansible 节点 . . . 265
准备控制节点 . . . 266
准备受管节点 . . . 267
创建 setup.csv 文件 . . . 268

21 部署容器 271

22 部署后任务 273

IX 在 Microsoft Azure Kubernetes 服务上部署 Identity Manager 容器 275

概述 . . . 276

23 规划部署 277

24 准备部署 281

25 部署过程 283

Azure 云上的基础结构部署 . . . 283
使用配置生成器进行部署 . . . 283
使用配置模板进行部署 . . . 287
Azure Kubernetes 服务上的 Identity Manager 容器部署 . . . 297

在 Azure Kubernetes 服务上设置 Remote Loader 服务 298
在 Azure Kubernetes 服务上设置扇出代理服务 300

26 部署后任务 303

访问 Identity Manager 应用程序 303
在 Azure 虚拟机上部署 Designer 303
在 Azure 虚拟机上部署 SLM for IGA 303
处理 AKS 的 RPM 更新和第三方文件 304

27 维护 Identity Manager 容器的部署 305

管理数据持久化层 305
重启动 Pod 306
访问 Pod 307
重启动 Azure Kubernetes 群集 307
缩放 Identity Manager 引擎复本 308
缩减 Identity Manager 引擎复本的用例 309
扩展 Identity Manager 引擎复本 309
缩放 OSP 和 Identity Applications 复本 310
销毁使用 Terraform 创建的整个资源 310

X 在 AWS EC2 上部署 Identity Manager 311

28 在 AWS EC2 上规划和实施 Identity Manager 313

先决条件 313
部署过程 313
准备 AWS Virtual Private Cloud 315
创建和部署实例 317
准备 EC2 实例 318
安装 Identity Manager 组件 320
安装 Identity Applications 和 Identity Reporting 的数据库 320
安装 Designer 322
创建 AWS EC2 负载平衡器 322
（可选）使用注册的托管区域创建别名 DNS 327
访问 Identity Manager 组件 328
安全考虑因素 328

29 混合 Identity Manager 方案示例 331

使用 Remote Loader 连接 331
使用多服务器驱动程序集连接 332
使用 eDirectory 驱动程序连接 333

XI 部署 Identity Manager 以实现高可用性 335

30 在群集环境中安装 Identity Manager 的准备工作 337

先决条件 337
身份库 337

Identity Applications 338
Identity Applications 的数据库 338
为 Identity Applications 准备群集 339
了解 Tomcat 环境中的群集组 339
设置工作流程引擎 ID 的系统属性 339

31 Identity Manager 群集部署解决方案示例 341

先决条件 341
安装过程 342
配置 iSCSI 服务器 342
在所有节点上配置 iSCSI 发起程序 343
对共享储存进行分区 343
安装 HA Extension 344
设置 Softdog 检查包 344
配置 HA 群集 344
在群集节点上安装并配置身份库和 Identity Manager 引擎 345
配置身份库资源 347
eDirectory 和共享储存子资源的原始值 347
更改位置约束分数 348

32 Tomcat 应用程序服务器上的 Identity Applications 群集部署解决方案示例 351

先决条件 352
准备群集 353
了解 Tomcat 环境中的群集组 353
设置工作流程引擎 ID 的系统属性 353
安装过程 353
为群集启用许可权限索引 358
为群集配置 User Application 驱动程序 358
为群集配置 OSP 和 SSPR 359
配置 SSPR 以支持群集 359
在群集节点上配置任务 359

33 卸装 Identity Manager 组件 361

从身份库中去除对象 361
卸装 Identity Manager 引擎 361
卸装 Identity Applications 362
卸装 Identity Reporting 组件 362
删除报告驱动程序 363
卸装 Identity Reporting 363
卸装 Sentinel Log Management for IGA 363
卸装 Designer 363
卸装 Analyzer 364

34 查错 365

查找日志文件 365
登录相关问题查错 365
安装和卸装相关问题查错 367
升级相关问题查错 370
Ansible 部署相关问题查错 374

AKS 部署相关问题查错 376
Identity Manager 引擎查错 382
Identity Applications 和 Identity Reporting 查错 384
其他问题查错 388

关于本文档和库

本 《*安装和升级指南*》提供了有关安装或更新 NetIQ Identity Manager （简称 Identity Manager）产品的说明。其中介绍了在分布式环境中安装和配置各个组件的过程。

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 (https://www.netiq.com/documentation/identity-manager-49/)。

Identity Manager 环境概述

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

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

- “Identity Manager 组件简介 ”
- “ 功能体系结构 ”

1 Identity Manager 组件简介

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

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

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

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

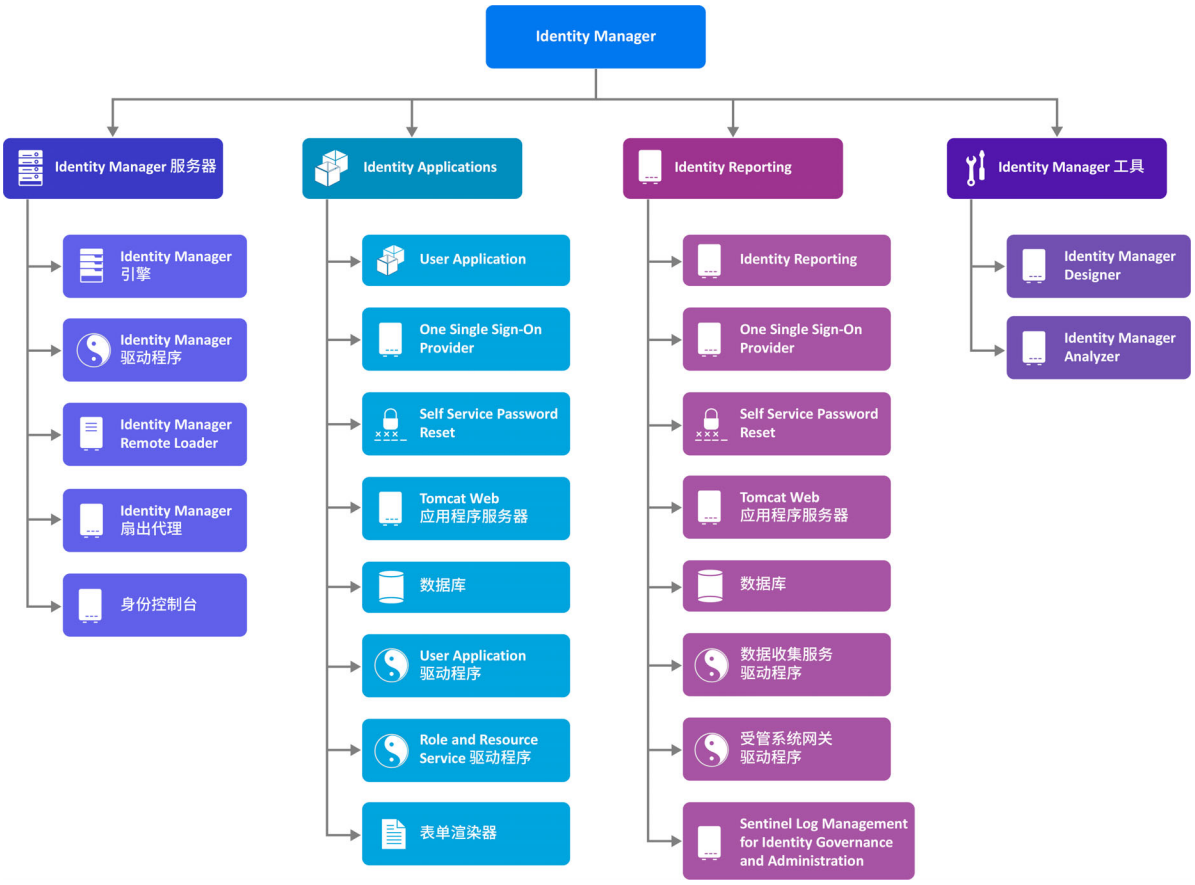
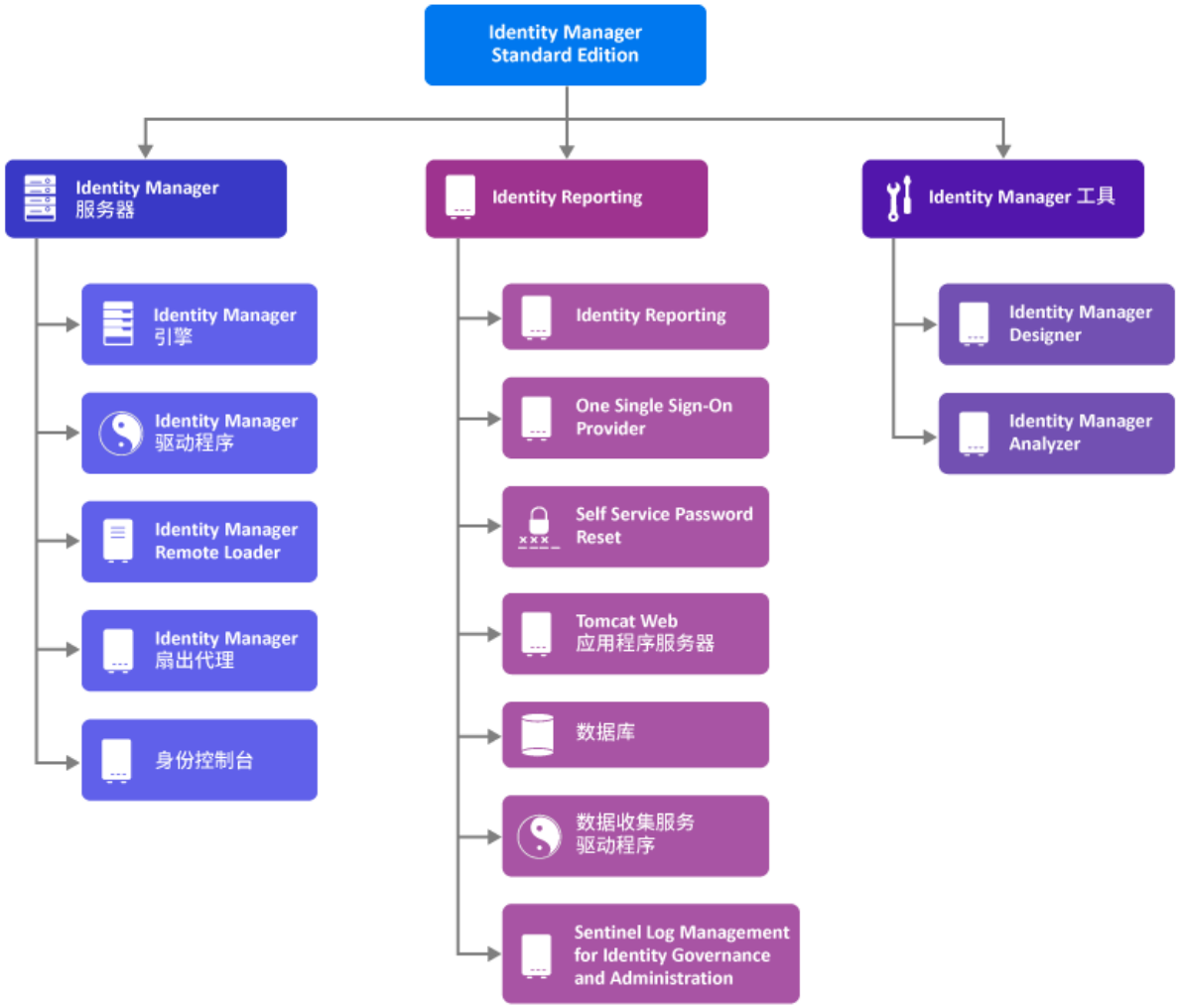


图 1-2 列出了 Identity Manager Standard Edition 环境中部署的组件。

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



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

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

Identity Manager 服务器组件

所有安装必需的组件

Identity Manager 服务器安装包含以下组件。

Identity Manager 服务器

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

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

身份库

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

Identity Manager 引擎

Identity Manager 引擎用于处理身份库或已连接应用程序中发生的所有数据更改。用来运行 Identity Manager 引擎的服务器称为 Identity Manager 服务器。

Identity Manager 驱动程序

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

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

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

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

Remote Loader

可以在 Identity Manager 服务器本地安装驱动程序，也可以使用 Remote Loader 来安装。Remote Loader 可装载驱动程序，并代表远程服务器上安装的驱动程序来与 Identity Manager 引擎通讯。如果应用程序与 Identity Manager 引擎在同一个服务器上运行，您便可以将驱动程序安装在该服务器上。但是，如果应用程序与 Identity Manager 引擎不在同一个服务器上运行，您必须将驱动程序安装在应用程序所在的服务器上。要改善环境的工作负载或配置，您

可以将 Remote Loader 安装在单独的服务器上，不要将其与 Tomcat 和 Identity Manager 服务器安装在同一个服务器上。有关 Remote Loader 的详细信息，请参见 《NetIQ Identity Manager Driver Administration Guide》（NetIQ Identity Manager 驱动程序管理指南）中的 “Determining When to Use the Remote Loader”（确定何时使用 Remote Loader）。

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

扇出代理

Identity Manager 扇出代理是 Java Database Connectivity (JDBC) 扇出驱动程序用来创建多个 JDBC 扇出驱动程序实例的安装组件。使用扇出驱动程序可以十分轻松地为多个数据库供应用户、组和口令。有了此驱动程序， Identity Manager 管理员就无需再使用相同的策略配置多个 JDBC 驱动程序来供应多个相同类型的数据库。您可以集中管理用户帐户，并在适当的情况下自动创建、配置、维护和去除这些帐户。有关详细信息，请参见 《NetIQ Identity Manager Driver for JDBC Fanout Implementation Guide》（NetIQ Identity Manager Driver for JDBC FanOut 实施指南）(https://www.netiq.com/documentation/identity-manager-49-drivers/jdbc_fanout/data/netiq-identity-manager-for-jdbc-fan-out-driver-implementation-guide.html)。

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

Identity Console

NetIQ Identity Console 是一款先进的 Web 管理控制台，借助它，用户可随时随地通过因特网和 Web 浏览器以虚拟、安全的自定义方式访问网络管理实用程序。 Identity Console 让管理任务权利下放更容易实现。 Identity Console 取代了 iManager。

使用 Identity Console，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 Identity Console 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 Identity Console 的详细信息，请参见 《Identity Console Administration Guide》（Identity Console 管理指南）(https://www.netiq.com/documentation/identity-console/identity_console-admin/data/bookinfo.html)

Identity Applications 组件

高级版安装必需的组件

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

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

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

Identity Applications 安装包括以下组件：

User Application

User Application 是基于浏览器的 Web 应用程序，可让用户执行各种身份自助服务和角色供应任务。在本产品的旧版本中使用 User Application 界面执行的部分任务已转移到新用户界面，新界面包括管理控制台和用户控制台。 User Application 将继续提供新用户界面中尚不存在的一些功能。有关详细信息，请参见 《NetIQ Identity Manager - Administrator's Guide to the Identity Applications》（NetIQ Identity Manager - Identity Applications 管理员指南）。

鉴定服务

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

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

Self-Service Password Reset

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

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

Web 应用程序服务器

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

- **IDMProv** （用于 User Application 的应用程序编程接口 (API)）
- **idmdash** （用于仪表板和 Identity Applications 管理界面）

当某个用户与 `idmdash` 应用程序交互时，此应用程序将查询底层 `IDMProv.war` 文件，并提取该用户的信息。`IDMProv.war` 会公开 REST 和 SOAP API，而 `idmdash` 则使用这些 API 来提供用户界面的信息。

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

Identity Applications 数据库

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

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

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

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

Identity Applications 的驱动程序

Identity Applications 组件需要以下驱动程序：

User Application 驱动程序

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

Role and Resource Service 驱动程序

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

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

Identity Reporting 组件

（可选）仅当您打算实施报告功能时，才需安装此组件

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

Reporting 还提供了一个报告打包工具，可简化自定义报告的创建过程。 Identity Reporting 的用户界面便于您将报告安排在非高峰时间运行，从而实现性能优化。有关 Identity Reporting 的详细信息，请参见 《Administrator Guide to NetIQ Identity Reporting》（NetIQ Identity Reporting 管理员指南）。

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

Identity Reporting 安装包括以下组件：

Identity Reporting

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

鉴定服务

鉴定服务由 OSP 组件提供。有关详细信息，请参见 “ 鉴定服务 ”（第 21 页）。

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

Self-Service Password Reset

自助式口令管理服务可让用户访问自助式口令管理功能。有关详细信息，请参见 “Self-Service Password Reset”（第 21 页）。

Identity Reporting 数据库

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

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

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

Web 应用程序服务器

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

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

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

有关 Web 应用程序服务器的详细信息，请参见 “Web 应用程序服务器 ”（第 21 页）。

Identity Reporting 的驱动程序

Identity Reporting 组件需要以下驱动程序：

受管系统网关驱动程序

可查询身份库以从受管系统收集下列类型的信息：

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

数据收集服务驱动程序

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

该服务包括三个子服务：

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

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

Sentinel Log Management for Identity Governance and Administration

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

Identity Manager 提供单独的 Sentinel Log Management for IGA 安装程序 (`SentinelLogManagementForIGA8.6.1.0.tar.gz`)。

Identity Manager 工具

所有安装必需的组件

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

Designer for Identity Manager

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

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

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

Identity Manager 提供单独的 Designer 安装程序。

Analyzer for Identity Manager

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

- Analyzer 的纲要映射可使应用程序的纲要属性与 Analyzer 基本纲要中的对应纲要属性相关联。这可让您确保您的数据分析和清理操作在不同系统之间正确关联类似的值。为此， Analyzer 利用了 Designer 中的纲要映射功能。

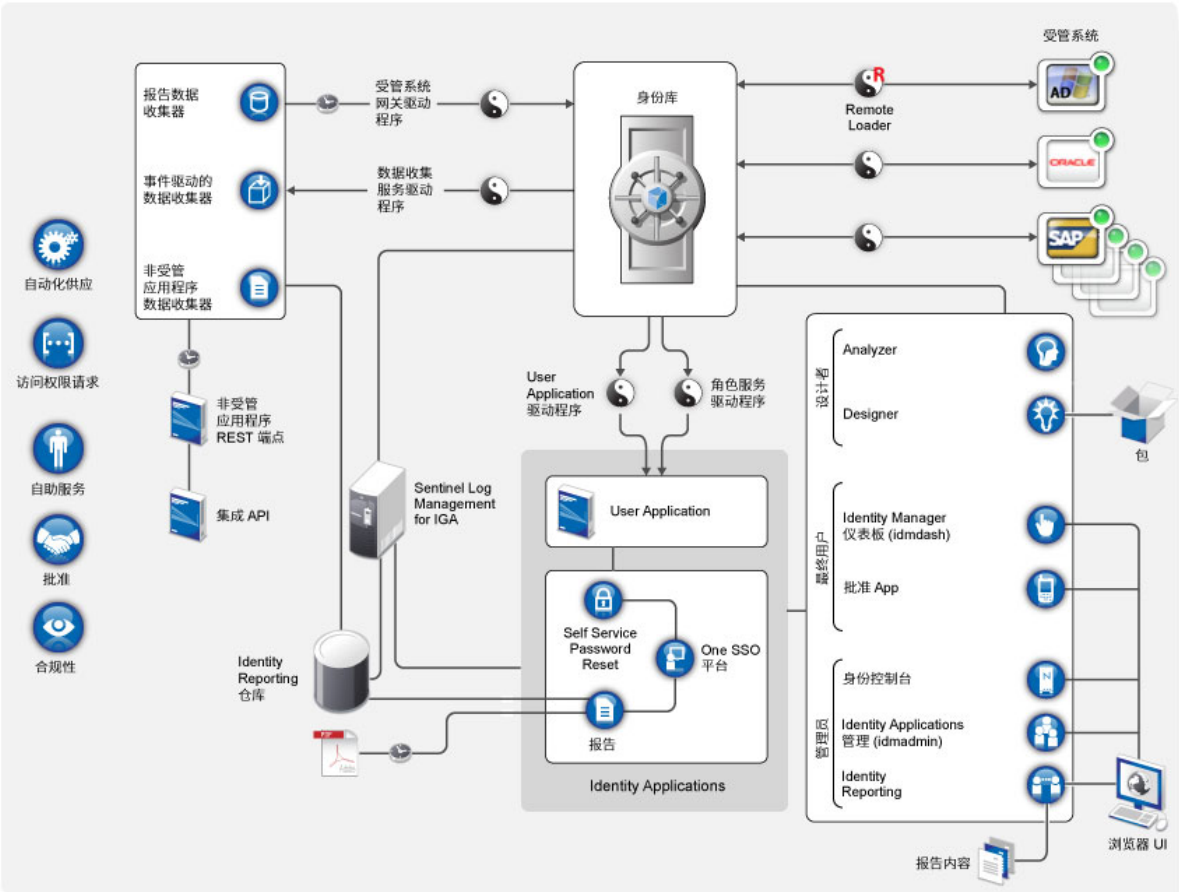
- 分析配置文件编辑器可让您配置用于分析一或多个数据集实例的配置文件。每个分析配置文件包含一或多个度量标准，您可以依据这些度量标准来评估属性值，以确定数据符合您所定义的数据格式标准的程度。
- 匹配配置文件编辑器可让您比较一或多个数据集中的值。您可以检查指定的数据集中是否有重复的值，以及两个数据集之间是否有匹配的值。

Identity Manager 提供单独的 Analyzer 安装程序。

重要：Identity Manager 4.9 ISO 中不包含 Analyzer 工具。如果已安装 Analyzer，请务必将其更新到版本 4.8.5 并与 Identity Manager 4.9 搭配使用。

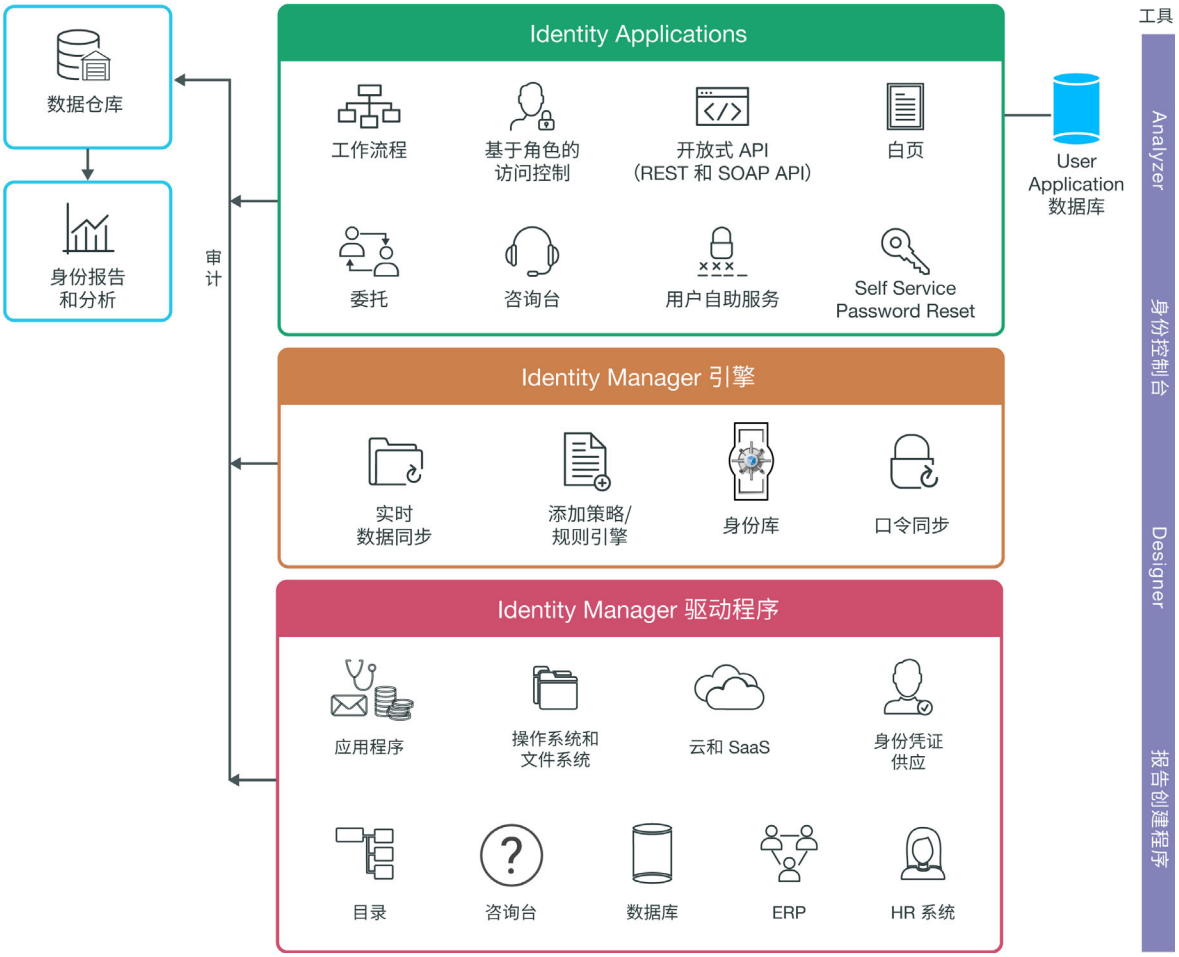
了解 Identity Manager 不同组件的用途及安装方式后，请参见图 1-3 了解组件之间的交互方式。

图 1-3 *Identity Manager 组件之间的交互*



功能体系结构

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



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

Identity Manager 的部署选项

请查阅下表来规划 Identity Manager 解决方案的物理环境。这些部署用例概括介绍了 Identity Management 物理体系结构，以及组件产品的连接方式、相互通讯及与其他产品通讯的方式。有关 Identity Management 功能体系结构和组件的简介概述，请参见 “ 功能体系结构 ”（第 26 页）。

部署选项	摘要
一台计算机上的单服务器配置	最基本的部署配置包括安装在一台计算机上的 Identity Manager 服务器以及其他必需的应用程序。必须确保该计算机具有所需的内存、速度和可用磁盘空间，以满足工作负载的要求。这是基本的部署用例，基本上只适合用于概念证明 (POC) 和演示目的，可能不适合用于生产环境。
分布式服务器配置	这种部署包括安装在一台计算机上的 Identity Manager 服务器，以及安装在其他一台或多台计算机上的所有其他必需的应用程序。例如，Identity Applications、 OSP 和 SSPR 等组件可在单独的计算机上运行。您可以提供一台额外的计算机来托管报告服务的组件，以满足运行 Sentinel Log Management for IGA 组件的系统要求。
高可用性部署	高可用性是一种冗余运行模式。当主服务器发生故障或者需要维护而暂时关闭时，高可用性功能可以自动切换到备用服务器。 Identity Manager 支持在高可用性环境中安装以下组件： ◆ 身份库 ◆ Identity Manager 引擎 ◆ Remote Loader ◆ Identity Applications，不包括 Identity Reporting 典型的群集配置包含托管 Identity Applications 以便实现负载平衡和容错的 Tomcat 应用程序服务器节点。所有通讯都通过负载平衡器路由。所有节点均与同一个身份库和 Identity Applications 数据库实例通讯。此配置可缩放。您可以轻松增加节点来处理负载。

Identity Manager 部署示例

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

特性	高级版	标准版	要安装的组件
基于规则的自动化用户供应	✓	✓	Identity Manager 引擎和 Designer
实时身份同步	✓	✓	Identity Manager 引擎和 Designer
口令管理和口令自助服务	✓	✓	Identity Manager 引擎和 SSPR
统一身份信息工具 (Analyzer)	✓	✓	Analyzer

特性	高级版	标准版	要安装的组件
REST API 和单点登录支持	✓	✓ （仅提供受限制的支持）	Identity Manager 引擎、 OSP 和 Identity Reporting
当前状态报告	✓	✓	Identity Manager 引擎和 Identity Reporting
基于角色的企业级供应	✓	✗	Identity Manager 引擎和 Identity Applications
业务策略执行的自动化批准工作流程	✓	✗	Identity Manager 引擎、 Designer 和 Identity Applications
Identity Applications 中的高级自助服务	✓	✗	Identity Manager 引擎和 Identity Applications
资源模型和编目方便资源供应	✓	✗	Identity Manager 引擎和 Identity Applications
历史状态报告	✓	✗	Identity Manager 引擎和 Identity Reporting
已连接系统报告	✓	✗	Identity Manager 引擎和 Identity Reporting
角色和资源管理	✓	✗	Identity Manager 引擎和 Identity Applications

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

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

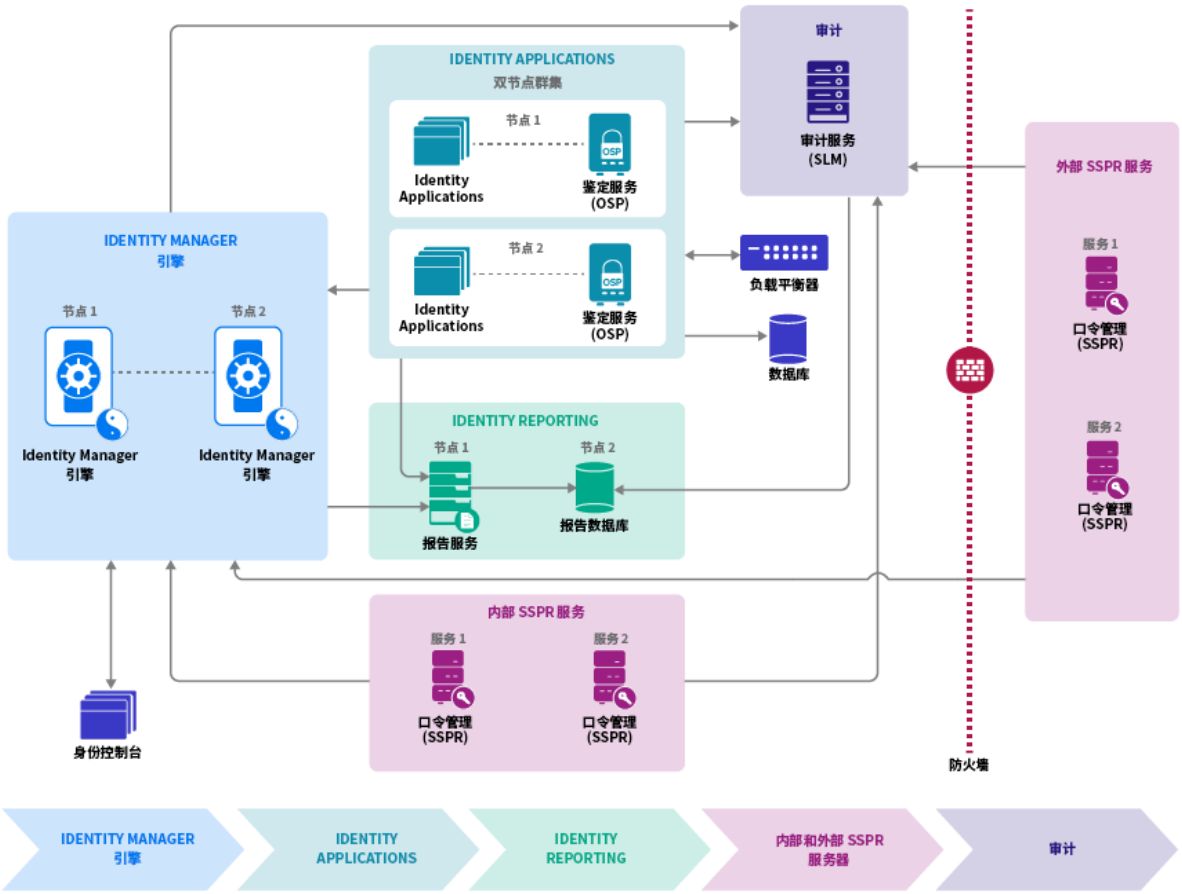
高可用性可确保关键网络资源 （包括数据、应用程序和服务）的高效可管理性。您可以通过减少任何单一故障点及使用冗余组件来实现高可用性。同样，将 Identity Management 组件的多个实例连接到负载平衡器也可以提供高度可用的环境。

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

高级版部署示例

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

图 1-4 高级版部署示例



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

发生故障，对该节点发出的请求将转移到群集中幸存的节点。由于此安装是一种站点内高可用性解决方案，因此可以在发生本地硬件和软件故障时提供保护，并使用基于双节点硬件的群集来实现 Identity Applications 组件的高可用性。

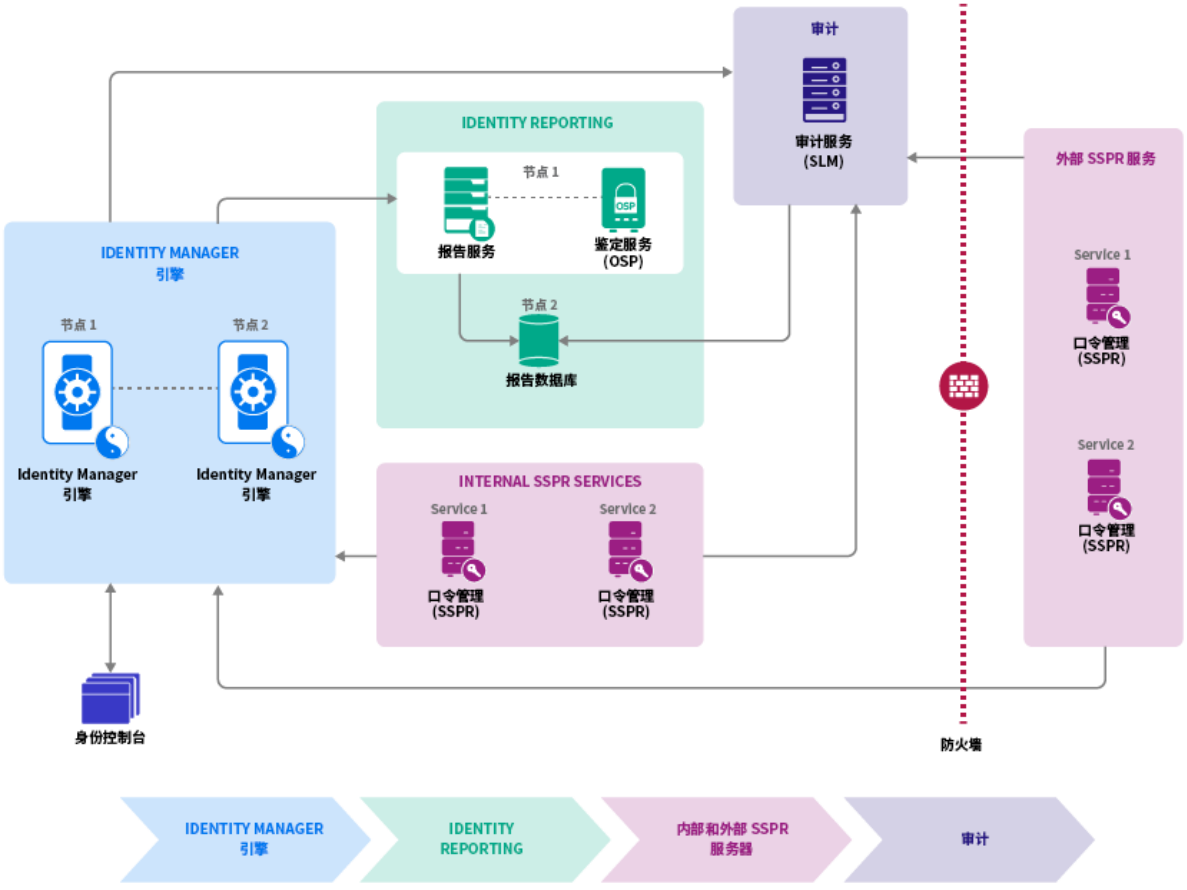
NetIQ 已对此配置进行测试，并建议使用此配置。

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

标准版部署示例

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

***图 1-5** 标准版部署示例*



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

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

NetIQ 已对此配置进行测试，并建议使用此配置。

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

规划 Identity Manager 安装

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

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

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

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

2 计划安装

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

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

实施核对清单

使用以下核对清单来规划、安装和配置 Identity Manager。

	核对清单项目
❑	1. 查看产品体系结构信息，以了解 Identity Manager 组件。有关详细信息，请参见《*NetIQ Identity Manager Overview and Planning Guide*》（NetIQ Identity Manager 概述和规划指南）中的 “How Identity Manager Works”（Identity Manager 的工作原理）。

	核对清单项目
❑	2. 查看 Identity Manager 许可信息，确定您需要使用 Identity Manager 的评估许可证还是企业许可证。有关详细信息，请参见《*NetIQ Identity Manager Overview and Planning Guide*》（NetIQ Identity Manager 概述和规划指南）中的 “Understanding Licensing and Activation”（了解许可和激活）。
❑	3. 根据您要实施的功能确定适合您环境的部署类型。有关详细信息，请参见《*NetIQ Identity Manager Overview and Planning Guide*》（NetIQ Identity Manager 概述和规划指南）中的 “Identity Manager Deployment Configurations”（Identity Manager 部署配置）。
❑	4. 确定是否可使用您的首选语言运行安装程序。有关详细信息，请参见《*NetIQ Identity Manager Overview and Planning Guide*》（NetIQ Identity Manager 概述和规划指南）中的 “Understanding Identity Manager Localization”（了解 Identity Manager 本地化）。
❑	5. 找到安装文件。有关详细信息，请参见《*NetIQ Identity Manager Overview and Planning Guide*》（NetIQ Identity Manager 概述和规划指南）中的 “Where to Get Identity Manager”（从何处获取 Identity Manager）。
❑	6. 安装 Identity Manager。有关更多信息，请参见第 III 部分 “ 安装和配置 Identity Manager 组件 ”（第 59 页）。
❑	7. 配置安装的组件。有关更多信息，请参见第 5 章 “ 配置 Identity Manager 组件 ”（第 75 页）。
❑	8. 执行一些额外的配置步骤，以使各个组件完全正常运行。有关详细信息，请参见第 6 章 “ 完成安装的最后步骤 ”（第 87 页）。

注释：对于群集和云部署，请务必查看建议的配置细节和要求。

- “ 部署 Identity Manager 以实现高可用性 ”（第 335 页）
- “ 在 AWS EC2 上部署 Identity Manager”（第 311 页）

建议的安装方案和服务器设置

本节内容可帮助您确定单服务器环境或分布式环境中的安装顺序和服务器设置。

- “ 确定何时安装 SLM for IGA”（第 37 页）
- “ 在分布式环境中安装的注意事项 ”（第 37 页）

确定何时安装 SLM for IGA

Sentinel 是 Identity Manager 的首选审计事件目标。 Identity Manager 可使用 Sentinel Event Source Management (ESM) 来配置 Sentinel Link，从而提供将事件转发到 Sentinel 的功能。如果您已在使用 Sentinel 进行审计，或者将其用作集成框架来跟踪身份，则可选择使用现有的 Sentinel 来审计事件，而无需安装 SLM for IGA。

无论您是选择重复利用现有的 Sentinel 服务器，还是全新安装 Identity Manager 随附的 SLM for IGA，都必须将 Sentinel 服务器配置为审计数据的源。为此，可以通过 “Identity Manager 数据收集服务 ” 页面在 Sentinel 服务器上创建一个数据同步策略，以用于审计事件。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）。

在分布式环境中安装的注意事项

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。 **重要：**Identity Manager 不支持远程安装的 OSP。如果您要升级到此版本，必须使用 Identity Applications 升级期间安装的 OSP，然后将现有 OSP 服务器中的 OSP 设置复制到安装了 OSP 的新服务器中。有关详细信息，请参见 “Identity Applications 组件的升级后任务 ”（第 204 页）。
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。必须将 OSP 和 Identity Applications 安装在同一台计算机上。 **重要：**如果您要升级到此版本，必须使用 Identity Applications 升级期间安装的 OSP，然后将现有 OSP 服务器中的 OSP 设置复制到安装了 OSP 的新服务器上。有关详细信息，请参见 “Identity Applications 组件的升级后任务 ”（第 204 页）。

组件	独立安装	注释
SSPR	是	安装程序支持独立安装和升级 SSPR。 如果您在标准版中安装或升级 SSPR，NetIQ 建议您在独立服务器上安装或升级 SSPR。换言之，SSPR 不得与 Identity Reporting 安装在同一台服务器上。 **重要：**如果您要在 Identity Applications 和 SSPR 部署到不同服务器的环境中升级到此版本，并希望将现有的 SSPR 设置还原到安装了 SSPR 的新服务器，请务必使用 ConfigUpdate 实用程序修改新 SSPR 服务器上的 SSPR 设置。有关详细信息，请参见 “Identity Applications 组件的升级后任务 ”（第 204 页）。
Identity Applications 数据库	是	
Reporting 数据库	是	
Sentinel Log Management for Identity Governance and Administration (Sentinel Log Management)	是	

服务器设置

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

计算机设置	组件设置
一体机 （建议仅用于演示 / POC 设置）	在一台计算机上安装并配置所有组件 （Identity Manager 引擎、 Identity Applications、 Identity Reporting、 OSP、 SSPR、 Identity Applications 数据库和 Reporting 数据库），在另一台计算机上安装并配置 Sentinel Log Management。
分布式设置	
服务器 1	◆ 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： ◆ Identity Applications ◆ Identity Reporting

计算机设置	组件设置
服务器 7	Sentinel Log Management

注释：从版本 4.7 开始，不再支持在包含多个身份库实例的服务器上安装 Identity Manager。

确定硬件要求

Identity Manager 安装所需的硬件取决于两个因素：

- 要实施的功能
- 部署规模

以下部署类型可帮助您预估部署的规模。

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

系统要求工作表

有关建议的硬件、支持的操作系统和虚拟环境的详细信息，请参见 System Requirements for Identity Manager 4.9 （Identity Manager 4.9 系统要求）。有关某个特定版本的系统要求信息，请参见 System Requirements for Identity Manager 4.9 （Identity Manager 4.9 系统要求）中该版本随附的发行说明。

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。

在 SLES 服务器上安装 Identity Manager

- 在安装 Identity Manager 之前，请务必安装以下依赖库或 RPM：
  - `libgcc*.x86_64`

- gettext.x86_64
- unzip
- bc
- lsof
- net-tools
- openssl
- pam-modules
- coreutils
- glibc-32bit-*.x86_64.rpm
- libnsl-*.x86_64.rpm
- libstdc++6-32bit
- libz1-32bit

其中 * 表示 RPM 的最新版本。

例如，要添加 libnsl-<version>.x86_64.rpm 文件，可以输入以下命令：

```
zypper in libsnl-<version>.x86_64.rpm
```

- （视情况而定）如果您在 SLES 15 或 SLES 15 SPx（x 表示 Identity Manager 支持的所有 SLES 15 版本）上安装 Identity Manager，请确保已安装 libncurses5*、libncurses6* 和 insserv-compat* RPM。 * 符号表示 RPM 的最新版本。
- （可选）要在 SLES 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

zypper refresh

PKGS=" libstdc*.x86_64 libgcc*.x86_64 unzip bc bash coreutils
gettext.x86_64 glibc.x86_64 lsof net-tools openssl sed insserv ss* pam-
modules"

for PKG in $PKGS ;
do
    zypper -n install "$PKG"

done
```

运行 install.sh 文件。

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。

在 RHEL 服务器上安装 Identity Manager

要在运行 Red Hat Enterprise Linux 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 41 页）
- “ 确保服务器上已安装依赖库 ”（第 42 页）
- “ 在 RHEL 9.x 上创建用于安装媒体的储存库 ”（第 42 页）
- “ 在 RHEL 8.x 上创建用于安装媒体的储存库 ”（第 44 页）
- “ 运行先决条件检查 ”（第 45 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
  <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。

- 如果您已在 RHEL 8.x 上配置安全增强式 Linux (SELinux)，则必须
  - 将值设置为 **permissive** 以安装 Identity Manager 引擎。否则，引擎安装将会失败，并显示以下错误：`身份库配置失败，退出代码为 10`

    例如，要将 SELinux 的值设置为 permissive，请执行以下步骤：

    1. 修改 `/etc/selinux/` 目录中的 `config` 文件。
    2. 在 **SELINUX** 字段中，将值设为 `permissive`。
    3. 保存更改并重启动系统。
  - 如果安装 Identity Reporting 的服务器不同于安装 Identity Manager 引擎和 Identity Applications 的服务器，请禁用 SELinux。否则， Tomcat 服务将不会启动，并且 Identity Reporting 数据库配置会报告 liquibase 错误。
- 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 42 页）。
- 务必在要安装 Remote Loader 的服务器上的环境变量 `$PATH` 或 `$JAVA_HOME` 中设置 Java 路径。您必须先执行此操作，然后再运行 `./RHEL-Prerequisite.sh` 脚本。要设置 Java 路径，请运行以下命令：

export PATH=<java 安装位置 >/bin:$PATH

例如：export PATH=/opt/netiq/common/jre/bin/:$PATH

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。请按以下顺序安装依赖库或 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
- libgcc-*.i686.rpm
- libXtst-*.i686.rpm
- libXrender-*.i686.rpm
- libXi-*.i686.rpm
- unzip
- bc
- lsof
- net-tools
- libncurses

注释：对于 Identity Manager，您可以编辑 ./RHEL-Prerequisite.sh 脚本，去除其中包含的所有 compat-libstdc++-33.x86_64.rpm 和 compat-libstdc++-33-*.i686.rpm。安装 Identity Manager 时不再需要这些包。

在 RHEL 9.x 上创建用于安装媒体的储存库

如果您的 RHEL 9.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 服务器必须装有适当的库。有关详细信息，请参见“ 确保服务器上已安装依赖库 ”（第 42 页）。

要设置用于安装的储存库，请执行以下操作：

1. 在本地服务器上创建安装点。

   例如：

   ```
   mkdir -p /mnt/rhel9
   ```

2. 装入 RHEL 9.x 安装 ISO：

   ```
   mount -o loop <RHEL9.x.iso> /mnt/rhel9
   ```

例如：

```
mount -o loop rhel-server-9.0-x86_64-dvd.iso mnt/rhel9
```

3 将装入目录中的 media.repo 文件复制到 /etc/yum.repos.d/，并设置所需的许可权限。

例如：

```
cp /mnt/rhel9/media.repo /etc/yum.repos.d/rhel9.repo


chmod 644 /etc/yum.repos.d/rhel9.repo
```

4 修改 rhel9.repo 文件并添加以下内容：

```
[InstallMedia]
name=Red Hat Enterprise Linux 9.0.0
mediaid=None
metadata_expire=-1
gpgcheck=0
cost=500
enabled=1
baseurl=file:///mnt/rhel9/BaseOS/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
```

5 如果您要安装 32 位包，请在 /etc/yum.conf 文件中将 exactarch 参数的值从 1 更改为 0。

6 运行以下命令：

```
yum clean all
```

7 （视情况而定）如果您要从 DVD 储存库检索包列表，请运行以下命令：

```
yum --noplugins list
```

8 安装 yum-utils 包。

```
yum install createrepo dnf-utils
```

9 要在 RHEL 9.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：

注释：如果您看到任何有关 RPM 重复的警告，则必须使用相应的 yum 命令手动处理该警告。

```
#!/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-*.i686.rpm
libstdc++.x86_64 libgcc-*.i686.rpm unzip bc lsof net-tools"

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

10 安装以下包：

```
yum install libgcc*.i686 libnsl* libnsl*.i686 libncurses*
```

11 运行 `install.sh` 文件。

12 要确认是否满足先决条件，请运行 “ 运行先决条件检查 ”（第 45 页）中所述的脚本。

13 安装 Identity Manager 4.9。

在 RHEL 8.x 上创建用于安装媒体的储存库

如果您的 RHEL 8.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 服务器必须装有适当的库。有关详细信息，请参见 “ 确保服务器上已安装依赖库 ”（第 42 页）。

要设置用于安装的储存库，请执行以下操作：

1 在本地服务器上创建安装点。

例如：

```
mkdir -p /mnt/rhel8
```

2 装入 RHEL 8 安装 ISO：

```
mount -o loop rhel-server-8.0-x86_64-dvd.iso mnt/rhel8
```

3 将装入目录中的 `media.repo` 文件复制到 `/etc/yum.repos.d/`，并设置所需的许可权限。

例如：

```
cp /mnt/rhel8/media.repo /etc/yum.repos.d/rhel8.repo


chmod 644 /etc/yum.repos.d/rhel8.repo
```

4 修改 `rhel8.repo` 文件并添加以下内容：

```
[dvd-BaseOS]
name=DVD for RHEL8 - BaseOS
baseurl=file:///RHEL8/BaseOS
enabled=1
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release

[dvd-AppStream]
name=DVD for RHEL8 - AppStream
baseurl=file:///RHEL8/AppStream
enabled=1
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
```

5 如果您要安装 32 位包，请在 `/etc/yum.conf` 文件中将 `exactarch` 参数的值从 1 更改为 0。

6 运行以下命令：

```
yum clean all
```

7 （视情况而定）如果您要从 DVD 储存库检索包列表，请运行以下命令：

```
yum --noplugins list
```

8 安装 `yum-utils` 包。

```
yum install createrepo yum-utils
```

9 要在 RHEL8 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：

注释：如果您看到任何有关 RPM 重复的警告，则必须使用相应的 `yum` 命令手动处理该警告。

```
#!/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-*.i686.rpm
libstdc++.x86_64 libgcc-*.i686.rpm unzip bc lsof net-tools"

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

10 安装以下包：

```
yum install libgcc*.i686 libnsl* libnsl*.i686 libncurses*
```

11 运行 `install.sh` 文件。

12 要确认是否满足先决条件，请运行 “ 运行先决条件检查 ”（第 45 页）中所述的脚本。

13 安装 Identity Manager 4.9。

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 `./RHEL-Prerequisite.sh` 脚本 （位于安装套件的装入目录中）。

3 安装 Identity Manager 组件的注意事项

本章提供有关安装 Identity Manager 组件的先决条件、注意事项以及所需的系统设置。

- “ 安装顺序 ”（第 47 页）
- “ 了解安装和配置过程 ”（第 47 页）
- “ 安装 Identity Manager 引擎组件和 Remote Loader 的注意事项 ”（第 49 页）
- “ 安装 Identity Applications 组件的注意事项 ”（第 50 页）
- “ 安装 Identity Reporting 组件的注意事项 ”（第 54 页）
- “ 安装 Designer 的注意事项 ”（第 55 页）
- “ 安装 Analyzer 的注意事项 ”（第 56 页）
- “ 安装 SLM for IGA 的注意事项 ”（第 56 页）
- “ 查看 Identity Manager 组件使用的端口 ”（第 57 页）

安装顺序

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

- Sentinel Log Management for Identity Governance and Administration
- Identity Manager 引擎组件
- Identity Applications 组件 （仅适用于高级版）
- Identity Reporting 组件
- Identity Console
- Designer for Identity Manager
- Analyzer for Identity Manager

重要：Identity Manager 4.9 ISO 中不包含 Analyzer 工具。如果已安装 Analyzer，请务必将其更新到版本 4.8.5 并与 Identity Manager 4.9 搭配使用。

在安装每个组件之前，必须查看该组件的安装先决条件和注意事项。

了解安装和配置过程

交互式安装：在交互式安装过程中，必须在交互模式下指定输入内容。 Identity Manager 提供脚本式安装程序，用于通过两个不同的阶段来安装和配置单个组件或一组组件。安装阶段将会安装组件。安装脚本 `install.sh` 位于 Identity Manager 安装包 `.iso` 映像文件的根目录中。有关配置的信息，请参见配置。

表 3-1 安装选项

安装选项	安装的组件
Identity Manager 引擎	安装身份库、Identity Manager 引擎和 Identity Manager 驱动程序。安装过程还会安装 Azul Zulu JDK。
Identity Manager Remote Loader 服务器	在 Remote Loader 中安装 Remote Loader 服务和驱动程序实例。
Identity Manager 扇出代理	安装 JDBC 扇出驱动程序的扇出代理。有关详细信息，请参见 Installing the Fanout Agent with Identity Manager 4.9 (https://www.netiq.com/documentation/identity-manager-49-drivers/jdbc_fanout/data/how-to-install-fan-out-agent-with-identity-manager-4-7.html) （随 Identity Manager 4.9 一起安装扇出代理）。
Identity Applications	安装用于提供 Identity Applications 底层框架的数个组件。 ◆ User Application ◆ OSP ◆ SSPR ◆ Tomcat ◆ PostgreSQL 数据库 为了支持 Tomcat 应用程序服务器，安装程序将安装受支持版本的 JRE 和 Apache ActiveMQ。 安装过程还会将 User Application 驱动程序和 Role and Resource Service 驱动程序部署到身份库。
Identity Reporting	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) ◆ OSP （与 Identity Applications 不安装在同一台服务器上时） ◆ Tomcat （与 Identity Applications 不安装在同一台服务器上时） ◆ PostgreSQL 数据库 （与 Identity Applications 不安装在同一台服务器上时） 为了支持 Tomcat 应用程序服务器，安装程序将安装受支持版本的 JRE。

注释：Identity Manager 为 Designer、 Analyzer 和 Sentinel Log Management 提供了不同的安装程序。

无提示安装：安装程序将提供以交互模式创建无提示属性文件的选项。您可以将安装选项记录在属性文件中，然后使用该文件在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。有关组件范围配置的细节，请参见“ 了解配置参数 ”（第 75 页）。

配置：Identity Manager 提供两种配置模式：

- 典型配置
- 自定义配置

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。

安装 Identity Manager 引擎组件和 Remote Loader 的注意事项

- Identity Manager 引擎安装过程要求至少具有以下数量的磁盘空间：

路径	组件	所需的最低安全空间
/opt	Identity Manager 引擎	3 GB
/var	Identity Manager 引擎	5 GB，用于包含 100,000 个对象的 dib
/etc	Identity Manager 引擎	5 MB

- 确保先安装 Identity Manager 引擎，再安装 Remote Loader。
- 您可以在装有 Identity Manager 引擎的同一台计算机上安装 Remote Loader。确保操作系统支持这两个组件。
- 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。
- （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 Linux 帐户驱动程序或 Remote Loader。您必须单独安装这些组件。
- NetIQ 建议您不要将 `changelog` 模块安装在 Identity Manager 引擎或 Remote Loader 所在的同一台服务器上。
- 如果您打算使用非默认部署环境 （即除 `o=system` 以外的任何环境）， NetIQ 建议您在安装 Identity Manager 引擎之前创建自定义 LDIF 文件。在配置过程中，系统会提示您输入该自定义 LDIF 文件的位置。

  注释：如果您在安装之前未创建 OU 结构，可以使用要在其下创建驱动程序集的所有容器的层次结构来定义所需 OU 结构。通过 LDIF 文件配置新的驱动程序集时，将使用此结构和层次结构。

- NetIQ 建议您在开始安装之前，针对所有语言运行下面的命令：

  `export LC_ALL=< 语言 >`

  例如：

  `export LC_ALL=zh_TW`

安装 Identity Applications 组件的注意事项

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。有关在安装应用程序组件后配置 Identity Applications 环境的详细信息，请参见《*NetIQ Identity Manager - Administrator's Guide to the Identity Applications*》（NetIQ Identity Manager - Identity Applications 管理员指南）。

- "安装注意事项"（第 50 页）
- "数据库注意事项"（第 50 页）
- "配置 Identity Applications 的数据库"（第 51 页）

安装注意事项

- Identity Applications 安装过程要求至少提供以下数量的磁盘空间来安装组件：
  - /opt - 5 GB
  - /var - 100 MB
- Identity Applications 要求已安装以下 Identity Manager 组件的受支持版本：
  - Identity Manager 引擎
  - Remote Loader
- （可选） NetIQ 在安装期间会启用安全套接字层 (SSL) 协议。要更改环境中 Identity Applications 组件之间的通讯设置，请参见《*NetIQ Identity Manager - Administrator's Guide to the Identity Applications*》（NetIQ Identity Manager - Identity Applications 管理员指南）中的 "Configuring 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。
- 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。
- 在分布式环境中， Identity Applications 服务器的密钥存储区 (`idm.jks`) 中必须存在 CN 为 Identity Applications 的证书。作为增强的 Java 安全措施的一部分， Identity Applications 现在需要可信证书才能与 OSP 通讯。

数据库注意事项

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 配合使用的数据库，必须确保该数据库包含所需的 JDBC jar 文件。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。
- 如果您使用受支持版本的 Oracle 或 Microsoft SQL Server 数据库，则必须配置以下两个数据库实例才能使 Identity Applications 正常工作：Identity Applications （例如：`idmuserappdb`）数据库和工作流程 （例如：`igaworkflowdb`）数据库。
- 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 认可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 52 页）或 “ 配置 Oracle 数据库 ”（第 52 页）。
- 如果您要连接到远程数据库，请确保在安装 Identity Applications 之前创建该数据库。有关连接到远程 PostgreSQL 数据库的信息，请参见 “ 连接远程 Remote PostgreSQL 数据库 ”（第 141 页）。
- 对数据库使用区分大小写的排序可能导致在迁移期间发生重复键错误。请检查排序并予以更正，然后重新安装 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。
- MS SQL 仅支持 SQL_Latin1_General_CP1_CI_AS 排序规则。

配置 Identity Applications 的数据库

Identity Applications 的数据库支持多种任务，例如，储存配置数据和工作流程活动的数据。在安装应用程序之前，必须先安装并配置数据库。

默认情况下，安装过程将为 Identity Applications 安装 PostgreSQL 数据库，并创建拥有该数据库的管理用户 `idmadmin`。但不会在 Identity Applications 的数据库中创建纲要。纲要信息是在您安装 Identity Applications 时添加的。

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。

- “检查数据库的兼容性级别”（第 52 页）
- “配置字符集”（第 52 页）
- “配置管理员用户帐户”（第 53 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';
   ```

   预期的输出为 12.2.xx、 18.xx 或 19.xx。

注释：从 Identity Manager 4.8.1 开始支持 Oracle 19c。

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。

要确认支持的 Oracle 数据库是否设置为使用 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 CREATE SESSION TO idmuser;
GRANT CREATE CLUSTER TO idmuser;
GRANT CREATE PROCEDURE TO idmuser;
GRANT CREATE SEQUENCE TO idmuser;
GRANT CREATE TABLE TO idmuser;
GRANT CREATE TRIGGER TO idmuser;
ALTER USER idmuser quota 100M on USERS;
```

其中， *idmuser* 表示用户帐户。

注释：建议使用支持的第三方 JDBC jar。例如：`ojdbc8.jar`。

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。

- “配置字符集”（第 53 页）
- “配置管理员用户帐户”（第 53 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`
- `REFERENCES`

注释：建议使用支持的第三方 JDBC jar。例如 `mssql-jdbc-7.2.2.jre11.jar`。

安装 Identity Reporting 组件的注意事项

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。

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 54 页）
- “Identity Reporting 的身份审计事件 ”（第 54 页）

Identity Reporting 的先决条件

- 安装过程要求至少具有以下数量的磁盘空间：
  - /opt - 5 GB
  - /var - 2 GB
  - /etc - 2 GB
- 安装过程要求已安装且设定以下 Identity Manager 组件的受支持版本：
  - Identity Applications，包括 User Application 驱动程序 （仅适用于高级版）
  - 安装在单独的 Linux 计算机上的 Sentinel Log Management。
- 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。
- 请不要将 Identity Reporting 安装在群集环境中的服务器上。
- 如果您要连接到远程数据库，请确保在安装 Identity Reporting 之前创建该数据库。有关连接到远程 PostgreSQL 数据库的信息，请参见 “ 连接远程 Remote PostgreSQL 数据库 ”（第 141 页）。
- 要针对 Oracle 数据库运行报告，必须确保已复制支持的第三方 jar。有关更多信息，请参见 “ 对 Oracle 数据库运行报告 ”（第 136 页）。
- 为任何您要授予报告功能访问权限的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 引擎与托管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。
- 要配置报告，必须以小写形式指定主机名。 Identity Reporting 6.6.0 及更高版本不再允许您使用 IP 地址配置报告。

Identity Reporting 的身份审计事件

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

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

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

事件名称	审计标志
鉴定和口令更改	**选择使用 SSPR 的审计标志：**起动 **SSPR 配置编辑器** > **审计配置** > 选择以下审计标志之一： • 鉴定 • 更改口令 • 解除锁定口令 • 恢复口令 • 入侵者尝试 • 入侵者锁定 • 入侵者锁定用户 **使用 Identity Console 选择审计标志：**登录 Identity Console，前往**审计** > **NCP 服务器** > **安全事件**，从以下审计标志中选择： • 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**

安装 Designer 的注意事项

- 要在 RHEL 平台上安装 Designer，应创建 RHEL 储存库。有关详细信息，请参见“ 在 RHEL 服务器上安装 Identity Manager”（第 41 页）。
- 此版本不支持从早期版本升级 Designer，因此如果您安装了旧版本，则需要在安装 Designer 4.9 之前将其卸装。此外，内置的自动更新和脱机更新功能无法用于升级到 Designer 4.9。
- 在运行 SLES 或 RHEL 的计算机上，请先安装 GNU gettext 实用程序 (`gettext`)，再安装 Designer。这些实用程序为国际化和多语言讯息提供了一个框架。

注释：NetIQ 建议从您的操作系统订购服务获取依赖的包，以确保可持续从操作系统供应商网站获得支持。如果您没有订购服务，可以从相关网站 （例如 http://rpmfind.net/linux (http://rpmfind.net/linux)）找到最新的包。

安装 Analyzer 的注意事项

重要：Identity Manager 4.9 ISO 中不包含 Analyzer 工具。如果已安装 Analyzer，请务必将其更新到版本 4.8.5 并与 Identity Manager 4.9 搭配使用。

- 在运行 SLES 12 SP3 平台的计算机上安装 Analyzer 之前，请确保已安装以下库：
  - `libswt3-gtk2`
  - `libxcomposite`
  - `libgdk_pixbuf`
  - `libgtk+-x11`
  - `gettext` （GNU gettext 实用程序）
- 在运行 SLES 8 或更高版本平台的计算机上安装 Analyzer 之前，请确保已安装以下库：
  - `gtk2.i686.rpm`。例如，可以从操作系统供应商网站下载包。
  - `gettext` （GNU gettext 实用程序）

  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。如果您没有订阅服务，可以从相关网站 （例如 http://rpmfind.net/linux/）找到最新的包。
- 确保运行 Analyzer 的计算机的视频分辨率达到 1024x768 （建议 1280x1025）。

安装 SLM for IGA 的注意事项

SLM for IGA 服务器的操作系统必须至少包含 SLES 服务器或 RHEL 服务器的基础服务器组件。Sentinel 需要以下 RPM 的 64 位版本：

- `bash`
- `bc`
- `coreutils`
- `gettext`
- `glibc`
- `grep`
- `libgcc`
- `libstdc`
- `lsof`
- `net-tools`
- `openssl`
- `python-libs`

- sed
- zlib

有关详细信息，请访问 NetIQ Sentinel 技术信息网站 (https://www.microfocus.com/documentation/sentinel/8.5/)。

查看 Identity Manager 组件使用的端口

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

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

端口号	组件	端口用途
389	身份库	用于以明文方式与 Identity Manager 组件进行 LDAP 通讯
465	Identity Reporting	用于与 SMTP 邮件服务器进行通讯
524	身份库	用于 NetWare 核心协议 (NCP) 通讯
636	身份库	用于与 Identity Manager 组件进行 LDAP with TLS/SSL 通讯
5432	Identity Applications	用于与 Identity Applications 数据库进行通讯
7707	Identity Reporting	受管系统网关驱动程序使用该端口来与身份库进行通讯
8000	Remote Loader	驱动程序实例使用该端口进行 TCP/IP 通讯 **注释：**应为 Remote Loader 的每个实例指派唯一的端口。
8005	Identity Applications	Tomcat 使用该端口来侦听关闭命令
8009	Identity Applications	Tomcat 使用该端口通过 AJP 协议 （而不是 HTTP）来与 Web 连接器进行通讯
8028	身份库	用于 NCP 通讯的 HTTP 明文通讯
8030	身份库	用于 NCP 通讯的 HTTPS 通讯
3000	Identity Applications	由 NGINX 服务使用
8090	Remote Loader	Remote Loader 使用该端口侦听来自远程接口 shim 的 TCP/IP 连接 **注释：**应为 Remote Loader 的每个实例指派唯一的端口。
8109	Identity Applications	仅当使用集成安装过程时适用 Tomcat 使用该端口通过 AJP 协议 （而不是 HTTP）来与 Web 连接器进行通讯
8443	Identity Applications	Tomcat 使用该端口进行 HTTPS (SSL) 通讯，或者重定向 SSL 通讯的请求

端口号	组件	端口用途
8543	Identity Applications	*默认情况下不侦听* 当您未使用 TLS/SSL 协议时，Tomcat 使用该端口来重定向需要 SSL 传输的请求
8600	表单渲染器	由 NGINX 服务使用
9000	Identity Console	由 Identity Console 使用
5432	Identity Reporting	用于 PostgreSQL 数据库 Sentinel
45654	User Application	将 Tomcat 与群集组搭配运行时，安装了 Identity Applications 数据库的服务器使用该端口来侦听通讯

III 安装和配置 Identity Manager 组件

此部分将指导您完成安装和配置 Identity Manager 组件的过程。有关安装说明，请参阅第 4 章 “ 安装 Identity Manager”（第 61 页）。有关配置 Identity Manager 组件的指导，请参见第 5 章 “ 配置 Identity Manager 组件 ”（第 75 页）。

安装 Identity Manager 组件并完成基本配置后，必须执行一些额外的配置步骤，才能让组件完全正常运行。有关详细信息，请参见第 6 章 “ 完成安装的最后步骤 ”（第 87 页）。

4 安装 Identity Manager

本章提供有关可用于安装 Identity Manager 组件的各种方式的信息。您可以通过以下方式安装 Identity Manager 组件：

- 交互式安装
- 无提示安装

执行交互式安装

1. 从软件和许可页面 (https://sld.microfocus.com/) 下载 `Identity_Manager_4.9.0_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` 将安装高级版，输入 `n` 将安装标准版。
7. 在可供安装的组件列表中选择所需的组件：
   - 要安装引擎，请选择 **Identity Manager 引擎**。
   - 要安装 Remote Loader，请选择 **Identity Manager Remote Loader**。
   - 要安装扇出代理，请选择 **Identity Manager 扇出代理**。
   - 要安装 Identity Applications，请选择 **Identity Applications**。
   - 要安装 Identity Reporting，请选择 **Identity Reporting**。
   - 要安装 Identity Console，请选择 **Identity Console**。
8. （视情况而定）配置安装的组件。有关详细信息，请参见第 5 章 “ 配置 Identity Manager 组件 ”（第 75 页）。

以无提示模式安装

1. 从软件和许可页面 (https://sld.microfocus.com/) 下载 `Identity_Manager_4.9.0_Linux.iso`。
2. 装入下载的 `.iso`。
3. 从 `.iso` 的根目录运行 `create_silent_props.sh` 脚本。
4. 输入 `y` 以确认创建文件。

5 指定无提示属性文件的路径。

6 决定要安装的 Identity Manager 服务器版本。输入 `y` 将安装高级版，输入 `n` 将安装标准版。

7 决定您是要以典型模式还是自定义模式配置组件。

8 在可供安装的组件列表中选择所需的组件：

- 要安装引擎，请选择 **Identity Manager 引擎**。
- 要安装 Remote Loader，请选择 **Identity Manager Remote Loader**。
- 要安装扇出代理，请选择 **Identity Manager 扇出代理**。
- 要安装 Identity Applications，请选择 **Identity Applications**。
- 要安装 Identity Reporting，请选择 **Identity Reporting**。
- 要安装 Identity Console，请选择 **Identity Console**。

配置安装的组件。有关详细信息，请参见第 5 章 “ 配置 Identity Manager 组件 ”（第 75 页）。

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

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 NICI。有关详细信息，请参见“ 安装 NICI”（第 62 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 63 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 65 页）。

安装 NICI

必须先安装 NICI，然后再继续身份库安装。由于必需的 NICI 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 NICI 包。

1 从装入的 `iso` 中，导航到 `/IDVault/setup/` 目录。

2 运行以下命令：

```
rpm -qa|grep nici64-3.2.0.0500-0.x86_64
```

3 校验 NICI 是否设置为服务器模式。输入下面的命令：

```
/var/opt/novell/nici/set_server_mode64
```

必须执行此步骤，以确保身份库配置过程不会失败。

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 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/
ndsmodules:
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 要使用 ndspath 脚本导出环境变量的路径，必须将 ndspath 脚本置于实用程序之前。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 使用以下方法之一配置身份库：

- 使用 ndsconfig 实用程序

```
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>] [--configure-eba-now <yes/no>]
```

其中， -t 表示要将服务器添加到的树名。

-n 表示要在其中添加服务器对象的服务器环境。

-a 表示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整判别名。

-s 表示服务器名称。

-d 表示储存数据库文件的目录路径。

-m 表示模块名称。

必须指定在配置过程中所指定的相同值。

例如：

```
ndsconfig new -t novell-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/
inst1/var --config-file /home/inst1/nds.conf --configure-eba-now
yes
```

输入的端口号需在 1024 到 65535 的范围内。小于 1024 的端口号通常是为超级用户和标准应用程序预留的。因此，不能对任何 eDirectory 应用程序假定使用默认端口 524。

这可能会导致以下应用程序中断：

- 未提供用来指定目标服务器端口的选项的应用程序。
- 使用 NCP 并以 root 身份在 524 上运行的较旧应用程序。

- 使用 ndsmanage 实用程序配置一个新实例。有关详细信息，请参见 《NetIQ eDirectory Installation Guide》（NetIQ eDirectory 安装指南）中的 “The ndsmanage Utility” （ndsmanage 实用程序）。

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 71 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_4.9.0_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“ 完成非 Root 用户安装 ”（第 142 页）。

安装 SSPR

安装程序将提供用于单独安装 SSPR 的选项。如果您要将 Identity Applications 和 SSPR 安装到不同的计算机上，此选项非常有用。

注释：如果您安装的是标准版，则必须执行以下过程来安装 SSPR。安装标准版时默认不会安装 SSPR。

以交互模式安装 SSPR

1 从 NetIQ 下载网站下载 `Identity_Manager_4.9.0_Linux.iso`。

2 装入下载的 `.iso`。

3 从 `.iso` 文件的根目录导航到 `sspr` 目录。

4 要安装 SSPR，请运行以下命令：

```
./install.sh
```

5 通读许可协议。

6 输入 `y` 以接受许可协议。

7 （视情况而定）配置 SSPR。有关详细信息，请参见“配置 SSPR”（第 85 页）。

以无提示模式安装 SSPR

1 从 NetIQ 下载网站下载 `Identity_Manager_4.9.0_Linux.iso`。

2 装入下载的 `.iso`。

3 从 `.iso` 文件的根目录导航到 `sspr` 目录。

注释：根据您的要求编辑 `sspr_silentinstall.properties` 文件。

4 要执行无提示安装，请运行以下命令：

```
./install.sh -s -f sspr_silentinstall.properties
```

5 （视情况而定）配置 SSPR。有关详细信息，请参见“配置 SSPR”（第 85 页）。

安装 Remote Loader

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

交互式安装

1 从 NetIQ 下载网站下载 `Identity_Manager_4.9.0_RL_Linux.iso`。

2 装入下载的 `.iso`。

3 从装入位置运行以下命令：

```
./install.sh
```

4 通读许可协议。

5 输入 `y` 以接受许可协议。

无提示安装

1 从 NetIQ 下载网站下载 `Identity_Manager_4.9.0_RL_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 指定文件的位置。

6 对于**是否要为 Docker 容器配置无提示属性文件**参数，请指定 *n*。

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

安装 Designer

可以使用 GUI 模式或控制台模式来安装 Designer。

1 从软件许可和下载 (https://sld.microfocus.com/index) 门户下载 `Identity_Manager_4.9.0_Designer_Linux.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_4.9.0_Designer_Linux.tar.gz
```

4 运行以下命令之一安装 Designer。

控制台： `./install -i console`

GUI： `./install`

5 按照提示继续安装。

安装 Analyzer

重要：Identity Manager 4.9 ISO 中不包含 Analyzer 工具。如果已安装 Analyzer，请务必将其更新到版本 4.8.5 并与 Identity Manager 4.9 搭配使用。

本节提供有关安装 Analyzer 以及为其配置环境的各种方式的信息。

- “使用向导安装 Analyzer”
- “以无提示模式安装 Analyzer”
- “将 XULRunner 添加到 Analyzer.ini 中”

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 “ 以无提示模式安装 Analyzer”（第 68 页）。

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）如果您已下载 Analyzer 安装文件，请完成以下步骤：

2a 浏览到所下载映像的 .tgz 或 win.zip 文件。

2b 将该文件的内容解压缩到本地计算机上的某个文件夹中。

3 执行安装程序：

```
./install
```

4 遵循向导中的说明操作，直到完成安装 Analyzer。

5 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。

6 单击**完成**。

7 （视情况而定）完成 “ 将 XULRunner 添加到 Analyzer.ini 中 ”（第 69 页）中的步骤。

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

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。相反，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 root/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 如果您已从软件和许可页面 (https://sld.microfocus.com/) 下载 Analyzer 安装文件，请完成以下步骤：

2a 浏览到所下载映像的 .tgz 或 win.zip 文件。

2b 将该文件的内容解压缩到本地计算机上的某个文件夹中。

3 （可选）要指定非默认安装路径，请完成以下步骤：

3a 打开 analyzerInstaller.properties 文件 （默认位于 < 文件解压缩位置 >/analyzer_install/ 目录中）。

3b 在该 properties 文件中添加以下文本：

```
USER_INSTALL_DIR=installation_path
```

4 要运行无提示安装，请从属性文件所在的目录运行以下命令：

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

5 （视情况而定）在 Linux 计算机上，完成 “ 将 XULRunner 添加到 Analyzer.ini 中 ”（第 69 页）中的步骤。

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

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。

1 安装 XULRunner。

2 浏览到默认情况下位于以下位置的 `Analyzer` 安装目录：

```
root/analyzer
```

3 在 gedit 编辑器中打开 `Analyzer.ini` 文件。

4 在参数列表的末尾添加以下行：

```
-Djava.util.Arrays.useLegacyMergeSort=true
-Dorg.eclipse.swt.internal.gtk.disablePrinting
-Dorg.eclipse.swt.browser.XULRunnerPath=/opt/xulrunner
```

5 保存 `Analyzer.ini` 文件。

6 起动 Analyzer。

安装 Sentinel Log Management for Identity Governance and Administration

可以使用以下方法安装 Sentinel Log Management：

- 以 root 用户身份安装 Sentinel Log Management
- 以非 root 用户身份安装 Sentinel Log Management

注释：在安装之前，请校验是否正确指定了主机名；不应启用 IPV6 设置。

以 Root 用户身份安装 Sentinel Log Management

1 从 NetIQ 下载网站下载 `SentinelLogManagementForIGA8.6.1.0.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 SentinelLogManagementForIGA8.6.1.0.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 口令时重设置 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>/sentinel/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。

以非 Root 用户身份安装 Sentinel Log Management

必须以 novell 用户身份安装 Sentinel Log Management。 NetIQ 不支持 novell 用户以外的非 root 用户安装，尽管安装会顺利地进行。

1 创建名为 novell 的非 root 用户。

```
useradd novell
```

2 创建名为 novell 的非 root 组。

```
groupadd novell
```

3 创建用于安装 Sentinel 的目录。

```
mkdir /home/slmnonroot
```

4 为 novell 用户指派对非根目录的安装目录的许可权限。

```
chown novell:novell /home/slmnonroot
```

5 设置适当的口令。

```
sudo passwd < 口令 >
```

6 以 novell 用户身份登录。

7 从 NetIQ 下载网站下载 SentinelLogManagementForIGA8.6.1.0.tar.gz。

8 导航到要提取文件的目录。

9 运行以下命令来提取文件

```
tar -zxvf SentinelLogManagementForIGA8.6.1.0.tar.gz
```

10 导航到 SentinelLogManagementforIGA 目录。

11 运行以下命令：

```
./install.sh --location=/home/slmnonroot
```

12 按照 “ 以 Root 用户身份安装 Sentinel Log Management”（第 69 页）中的步骤 6 至 16 操作。

安装 Java Remote Loader

您需在操作系统与本机 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，请导航到包含 Java Remote Loader 安装文件的目录 （默认为 /IDM/packages/java_remoteloader）。

4b （视情况而定）如果您已从软件和许可页面 (https://sld.microfocus.com/) 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 tar -zxvf dirxml_jremote.tar.gz

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。

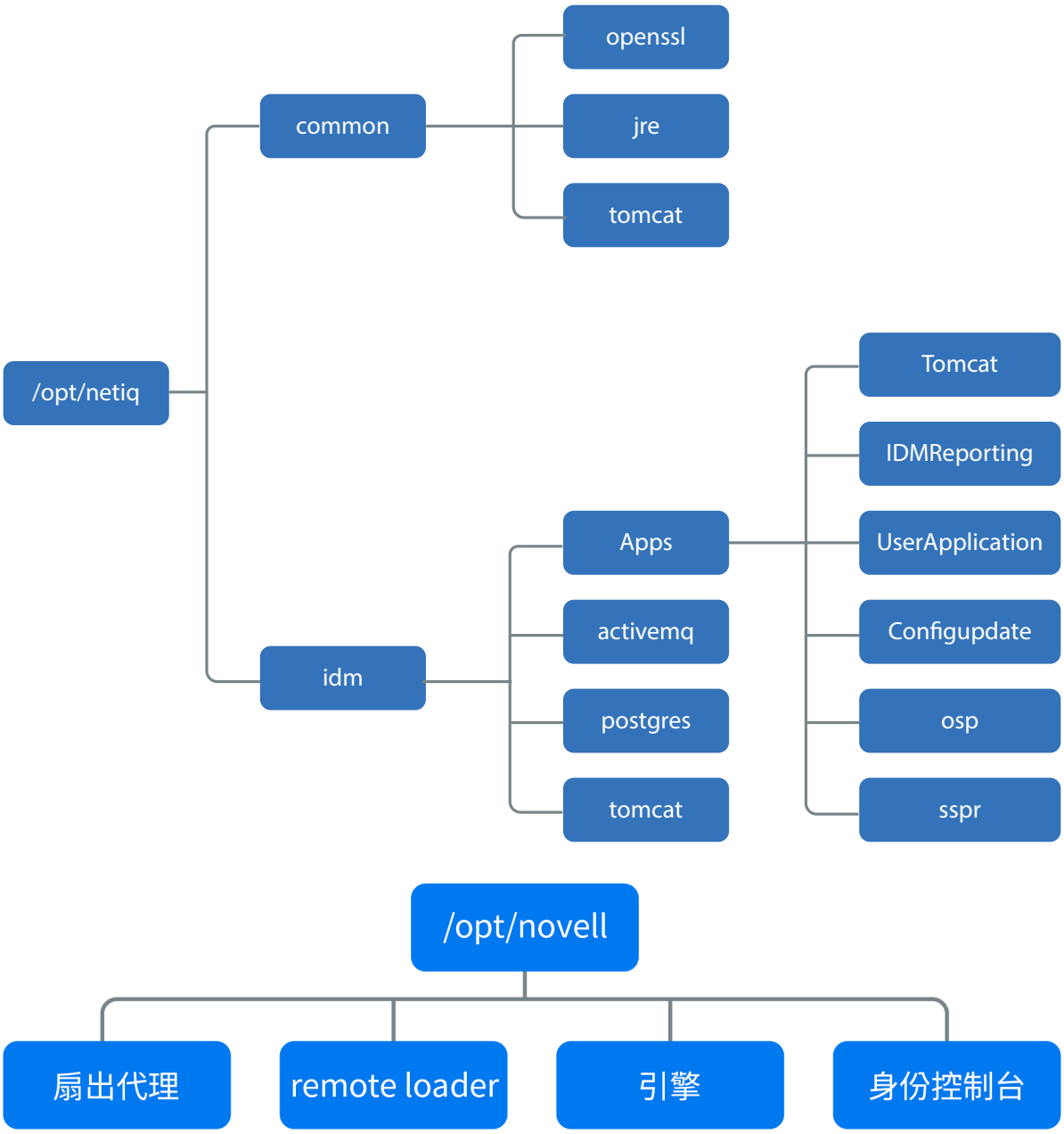
10 必须在 dirxml_jremote 脚本中指定 jar 文件的位置。这些文件位于解压缩 dirxml_jremote.tar.gz 目录的 lib 子目录中。例如， /lib/*.jar。

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“ 配置 Remote Loader 和驱动程序 ”（第 88 页）。

了解目录结构

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。
- 引擎、扇出代理、 Remote Loader 和 Identity Console 安装在 `/opt/novell` 目录下。

5 配置 Identity Manager 组件

本章将指导您完成配置 Identity Manager 组件的过程。在开始配置前，必须查看每个组件的配置选项。有关详细信息，请参见“ 了解配置参数 ”（第 75 页）。

某些组件 （例如 Designer、 Analyzer、 Remote Loader 和扇出代理）可能不需要配置。

在配置期间使用不可猜出的口令

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

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

了解配置参数

本节定义配置 Identity Manager 安装需要指定的参数。您可以使用安装程序在安装组件后立即对其进行配置，也可以稍后运行 `configure.sh` 脚本来配置。

注释：

- 在典型配置模式下配置的 Identity Applications 和 Identity Reporting 无法连接到另一台计算机上安装的数据库服务器。
- 安装过程不允许您为 Identity Manager 组件启用审计。必须在完成安装后为每个组件配置审计。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）。
- 身份库将随 OES 一起自动安装。要在 OES 平台上配置 Identity Manager 引擎，必须依次选择**自定义配置**和**添加到现有库**。
- 确保使用 FQDN 或 IP 地址以统一的方式配置 Identity Applications、 Identity Reporting 和数据库。换言之，不得使用 FQDN 和 IP 地址的组合来配置这些组件。
- 对于容器，建议指定 FQDN 值，而不要指定 IP 地址。

表 5-1 描述了在典型模式下配置 Identity Manager 组件所需的参数。

表 5-1 典型配置

参数	无提示属性文件中的参数	典型配置
Identity Manager 引擎		

参数	无提示属性文件中的参数	典型配置
通用口令	IS_COMMON_PASSWORD	指定是否要设置通用口令。
身份库主机名 /IP 地址	ID_VAULT_HOST	指定安装了身份库的服务器的 IP 地址。
身份库管理员名称	ID_VAULT_ADMIN_LDAP	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	IS_COMMON_PASSWORD	指定是否要设置通用口令。确保口令符合“在配置期间使用不可猜出的口令”（第 75 页）章节中指定的注意事项。
通用 One SSO 服务口令	SSO_SERVICE_PWD	指定 One SSO 服务器的鉴定服务的口令。
SSPR 配置口令		指定 SSPR 的鉴定服务的口令。
Identity Applications 管理员名称	UA_ADMIN	指定 Identity Applications 管理员帐户的名称。
Identity Applications 管理员口令		指定 Identity Applications 的管理员口令。
Identity Applications 和工作流程引擎数据库用户口令		指定 Identity Applications 和工作流程引擎数据库用户口令。
Identity Applications 和工作流程引擎数据库管理员口令		指定 Identity Applications 和工作流程引擎数据库管理员口令。
NGINX 端口	NGINX_HTTPS_PORT	指定 NGINX 端口。
Identity Reporting		
通用口令	IS_COMMON_PASSWORD	指定是否要设置通用口令。确保口令符合“在配置期间使用不可猜出的口令”（第 75 页）章节中指定的注意事项。
Identity Reporting 数据库帐户口令	RPT_DATABASE_SHARE_PASSWORD	指定 Identity Reporting 的数据库帐户口令。
Identity Reporting 管理员名称	RPT_ADMIN	指定 Identity Reporting 的管理员名称。默认值为 `cn=uaadmin,ou=sa,o=data`。
Identity Reporting 管理员口令		指定管理员对象的口令。例如， *password*。
Identity Console		
Identity Console 服务器名称	ID_CONSOLE_SERVER_HOST	指定用于托管 Identity Console 的服务器名称。

参数	无提示属性文件中的参数	典型配置
Identity Console 服务器端口	ID_CONSOLE_SERVER_SSL_PORT	指定用于托管 Identity Console 的端口。
用于通过 Identity Console 授权的 OSP	ID_CONSOLE_USE_OSP	指定您是否要选择使用 OSP 通过 Identity Console 进行授权 (y/n)。
One SSO 服务口令	SSO_SERVICE_PWD	*仅当您已选择使用 OSP 进行授权 （即前面选择了*是）时才适用。 指定 One SSO 服务口令。
可信根证书文件夹路径	ID_CONSOLE_CA_CERT_LOCATION	指定可信根证书 (SSCert.pem) 文件夹路径。
服务器证书路径，包括文件名	ID_CONSOLE_SERVER_CERT_LOCATION	指定服务器证书路径，包括文件名。
服务器证书口令	ID_CONSOLE_SERVER_CERT_PASSWD	指定服务器证书口令。

表 5-2 描述了在自定义模式下配置 Identity Manager 组件所需的参数。

***表 5-2** 自定义配置*

参数	无提示属性文件中的参数	自定义配置
Identity Manager 引擎		
创建新的身份库	TREE_CONFIG	指定要安装的身份库。
添加到本地计算机上的现有身份库		指定是否要连接到要安装 Identity Manager 引擎的同一台服务器上的现有身份库。
添加到远程计算机上的现有身份库		指定是否要连接到未与 Identity Manager 引擎安装到同一台服务器的身份库。
身份库树名	ID_VAULT_TREENAME	为身份库指定新的树。树名必须满足以下要求： ◆ 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。 **注释：**如果您要在 OES 上安装 Identity Manager，请指定现有的树名。
身份库服务器名称	ID_VAULT_SERVERNAME	指定身份库服务器名称。
身份库环境 DN	ID_VAULT_SERVER_CONTEXT	指定现有身份库服务器的环境 DN。默认值为 servers.system。
身份库管理员名称	ID_VAULT_ADMIN_LDAP	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	无提示属性文件中的参数	自定义配置
身份库管理员口令	ID_VAULT_PASSWORD	指定管理员对象的口令。例如， *password*。
RSA 密钥大小	ID_VAULT_RSA_KEYSIZE	指定 RSA 证书的密钥大小。允许的值为 2048、4096 和 8192 位。默认值为 4096。
EC 曲线	ID_VAULT_EC_CURVE	指定 EC 证书的椭圆曲线 (EC) 限制。允许的值为 P256、 P384 和 P521。默认值为 P384。
证书有效期	ID_VAULT_CA_LIFE	*仅当您选择了*创建新树*选项时才适用。* 以年为单位指定证书的有效期。
NDS var 文件夹位置	ID_VAULT_VARDIR	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	ID_VAULT_DIB	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	ID_VAULT_NCP_PORT	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	ID_VAULT_LDAP_PORT	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	ID_VAULT_LDAPS_PORT	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	ID_VAULT_HTTP_PORT	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	ID_VAULT_HTTPS_PORT	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	ID_VAULT_CONF	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	ID_VAULT_DRIVER_SET	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	ID_VAULT_DEPLOY_CTX	指定要在其中创建驱动程序集对象的容器的 LDAP DN。
Identity Applications		
通用口令	IS_COMMON_PASSWORD	指定是否要设置通用口令。确保口令符合“在配置期间使用不可猜出的口令”（第 75 页）章节中指定的注意事项。
主机名 （小写 FQDN）	UA_SERVER_HOST	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。

参数	无提示属性文件中的参数	自定义配置
身份库主机名 /IP 地址	ID_VAULT_HOST	指定安装了身份库的服务器的 IP 地址或主机名。
身份库管理员名称	ID_VAULT_ADMIN_LDAP	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	ID_VAULT_PASSWORD	指定管理员对象的口令。例如， *password*。
OSP 自定义登录屏幕名称	OSP_CUSTOM_NAME	指定将显示在 OSP 登录屏幕上的名称。
用户搜索容器 DN	USER_CONTAINER	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	ADMIN_CONTAINER	指定身份库中包含鉴定服务 (OSP) 必须鉴定的任何管理员用户对象的容器判别名。例如 o=data。
应用程序服务器 DNS/IP 地址	TOMCAT_SERVLET_HOSTNAME	指定 Tomcat 服务器的 IP 地址或主机名。
One SSO 服务器 SSL 端口	SSO_SERVER_SSL_PORT	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	SSO_SERVICE_PWD	*仅当将通用口令设置为*否时才适用。 指定 Identity Applications 使用的单点登录客户端的口令。
Identity Applications 管理员名称	UA_ADMIN	指定 Identity Applications 管理员帐户的名称。
SSPR 配置口令	CONFIGURATION_PWD	*仅当将通用口令设置为*否时才适用。 指定 Identity Applications 用于进行口令管理的口令。
OAuth 密钥存储区口令	OSP_KEYSTORE_PWD	*仅当将通用口令设置为*否时才适用。 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。
数据库平台	UA_DB_PLATFORM_OPTION	指定 Identity Applications 所需的数据库。
在当前服务器上配置 PostgreSQL	INSTALL_PG_DB	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	UA_DB_PORT	指定 Identity Applications 的数据库端口。
Identity Applications 数据库名称	UA_DATABASE_NAME	指定数据库的名称。默认值为 idmuserappdb。
Identity Applications 数据库和工作流程引擎用户名	UA_WFE_DATABASE_USER	指定 Identity Applications 数据库管理员的用户名。

参数	无提示属性文件中的参数	自定义配置
用户 postgres 的 Identity Applications 和工作流程引擎数据库管理员口令	UA_WFE_DATABASE_ADMIN_PWD	指定用户 postgres 的 Identity Applications 和工作流程引擎数据库管理员口令
使用自定义容器作为根容器	ENABLE_CUSTOM_CONTAINER_CREATION	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。 要创建自定义容器，请选择**是**。
创建 Identity Applications 的 User Application 和 Roles and Resources Services 驱动程序	UA_CREATE_DRIVERS	指定是否要安装 UA 和 RRSD 驱动程序。如果您选择 **N**，则必须指定现有 User Application 驱动程序的名称。
现有 User Application 驱动程序的名称	UA_DRIVER_NAME	仅当您已将用于创建 UA 和 RRSD 驱动程序的值设置为**否**时才适用。 指定现有 User Application 驱动程序 DN 细节。
User Application 工作流程引擎 ID	UA_WORKFLOW_ENGINE_ID	指定 Identity Applications 工作流程引擎 ID。
Identity Applications 和工作流程引擎数据库平台	UA_WFE_DB_PLATFORM_OPTION	指定 Identity Applications 和工作流程引擎数据库平台。支持的值为 Postgres、 Oracle 和 MsSQL。
Identity Applications 和工作流程引擎数据库端口	UA_WFE_DB_PORT	指定 Identity Applications 和工作流程引擎数据库端口。
工作流程引擎数据库名称	WFE_DATABASE_NAME	指定工作流程引擎数据库名称 . 默认数据库名称为 igaworkflowdb。
Identity Applications 和工作流程引擎数据库口令	UA_WFE_DATABASE_PWD	指定 Identity Applications 和工作流程引擎数据库口令。
Identity Applications 和工作流程引擎数据库 JDBC 驱动程序 jar 文件	UA_WFE_DB_JDBC_DRIVER_JAR	指定数据库平台的 JAR 文件。
创建纲要	UA_WFE_DB_CREATE_OPTION	当您要在安装过程中为 Identity Applications 和工作流程引擎创建数据库纲要时，请指定该参数。可用选项有**现在**、**启动**和**文件**。
创建新数据库，或从工作流程引擎的现有数据库升级 / 迁移	WFE_DB_NEW_OR_EXIST	指定是要在新数据库中创建表，还是从工作流程引擎的现有数据库更新 / 升级。支持的值为 new 和 exist。

参数	无提示属性文件中的参数	自定义配置
创建新数据库，或从 Identity Applications 的现有数据库升级 / 迁移	UA_DB_NEW_OR_EXIST	指定是要创建新数据库还是从现有数据库升级。
根容器	ROOT_CONTAINER	指定根容器。默认值为 o=data。
组搜索根容器 DN	GROUP_ROOT_CONTAINER	指定组搜索根容器的 DN。
Identity Applications 自定义证书	CUSTOM_UA_CERTIFICATE	指定是否要为 Identity Applications 使用自定义证书
自定义容器 LDIF 文件路径		*仅当将自定义容器设置为*是时适用。 为自定义容器指定 LDIF 文件的路径。
NGINX 端口	NGINX_HTTPS_PORT	指定 NGINX 端口。
Identity Reporting		
通用口令	IS_COMMON_PASSWORD	指定是否要设置通用口令。确保口令符合“在配置期间使用不可猜出的口令”（第 75 页）章节中指定的注意事项。
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	ID_VAULT_HOST	指定安装了身份库的服务器的 IP 地址或主机名。
身份库管理员名称	ID_VAULT_ADMIN_LDAP	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	ID_VAULT_PASSWORD	指定管理员对象的口令。例如， *password*。
应用程序服务器 HTTPS 端口	TOMCAT_HTTPS_PORT	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。
应用程序服务器 DNS/IP 地址	TOMCAT_SERVLET_HOSTNAME	指定 Tomcat 服务器的 IP 地址或主机名。
选择用于 Identity Reporting 的数据库平台	RPT_DATABASE_PLATFORM_OPTION	指定要用于 Identity Reporting 的数据库。
在当前服务器上配置 PostgreSQL	INSTALL_PG_DB_FOR_REPORTING	指定是否要在同一台服务器上配置 PostgreSQL 数据库。
Identity Reporting 数据库帐户口令	RPT_DATABASE_SHARE_PASSWORD	指定 Identity Reporting 的数据库帐户口令。
创建新数据库或从现有数据库升级 / 迁移	RPT_DATABASE_NEW_OR_EXIST	指定是要创建新数据库还是从现有数据库升级。

参数	无提示属性文件中的参数	自定义配置
Identity Reporting 管理员名称	RPT_ADMIN	指定 Identity Reporting 的管理员名称。默认值为 cn=uaadmin,ou=sa,o=data。
Identity Reporting 管理员口令	RPT_ADMIN_PWD	指定 Identity Reporting 的管理员口令。
Identity Reporting 数据库名称	RPT_DATABASE_NAME	指定 Identity Reporting 的数据库名称。默认值为 idmrptdb。
Identity Reporting 数据库用户	RPT_DATABASE_USER	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。
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	RPT_DATABASE_PORT	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	RPT_DATABASE_JDBC_DRIVER_JAR	指定数据库平台的 JAR 文件。
包含主题备用名称的 Identity Reporting Tomcat 密钥存储区文件	RPT_COMM_TOMCAT_KEYSTORE_FILE	指定 Tomcat 密钥存储区文件的位置。 **注释：**只支持 PKCS 类型的自定义证书。
创建纲要	RPT_DATABASE_CREATE_OPTION	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**。
为 Identity Reporting 创建 MSGW 和 DCS 驱动程序	RPT_CREATE_DRIVERS	指定是否要创建 MSGW 和 DCS 驱动程序。
NGINX HTTPS 端口	NGINX_HTTPS_PORT	指定 NGINX 的端口。
Identity Console		
Identity Console 服务器名称	ID_CONSOLE_SERVER_HOST	指定用于托管 Identity Console 的服务器名称。
Identity Console 服务器端口	ID_CONSOLE_SERVER_SSL_PORT	指定用于托管 Identity Console 的端口。
用于通过 Identity Console 授权的 OSP	ID_CONSOLE_USE_OSP	指定您是否要选择使用 OSP 通过 Identity Console 进行授权 (y/n)。
One SSO 服务口令	SSO_SERVICE_PWD	*仅当您已选择使用 OSP 进行授权 （即前面选择了**是**）时才适用。* 指定 One SSO 服务口令。
可信根证书文件夹路径	ID_CONSOLE_CA_CERT_LOCATION	指定可信根证书 (SSCert.pem) 文件夹路径。

参数	无提示属性文件中的参数	自定义配置
包含文件名的服务器证书路径	ID_CONSOLE_SERVER_CERT_LOCATION	指定服务器证书路径，包括文件名。
服务器证书口令	ID_CONSOLE_SERVER_CERT_PASSWD	指定服务器证书口令。
身份库树名称	ID_CONSOLE_TREENAME	输入用于托管 Identity Console 的身份库树名称。

创建和配置驱动程序集

使用 Identity Manager 安装套件的 IDM/LDIF/ 目录中的 sample-driverset.ldif 文件可帮助您创建驱动程序集。该文件包含以下内容：

```
dn: cn=driverset1,o=system
changetype: add
DirXML-LogLimit: 0
DirXML-ConfigValues::
PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz48Y29u

ZmlndXJhdGlvbi12YWx1ZXM+Cgk8ZGVmaW5pdGlvbnMvPgo8L2NvbmZpZ3VyYXRpb24tdmFsdW
VzPg==
objectClass: DirXML-DriverSet
objectClass: Top
objectClass: Partition
objectClass: nsimPasswordPolicyAux

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
description: This Password Policy is used by IDM Engine
nspmMaximumLength: 64
nspmConfigurationOptions: 596
passwordUniqueRequired: FALSE
passwordMinimumLength: 1
passwordAllowChange: TRUE
objectClass: nspmPasswordPolicy
objectClass: Top
cn: DirXML-PasswordPolicy
nsimAssignments: cn=driverset1,o=system
```

在全新安装过程中创建驱动程序集

在文本编辑器中打开 `sample-driverset.ldif` 文件，并进行以下更改。如果您提供了自定义 LDIF 文件路径，请指定该自定义路径：

1. 将驱动程序集 DN 指向新驱动程序集。例如，将 `dn: cn=driverset1,o=system` 更改为 `dn:cn=Driverset47,ou=drivers,o=acme`。
2. 将 `nsimAssignments` 属性值更改为新驱动程序集的 DN。例如，将 `nsimAssignments: cn=driverset1,o=system` 更改为 `nsimAssignments: cn=Driverset47,ou=drivers,o=acme`。

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。

在现有服务器上配置驱动程序集

如果 Identity Manager 已安装在 eDirectory 树中的某台服务器上，则该树中会存在 DirXML-PasswordPolicy。您有以下选择：

- **使用现有口令策略**

  仅在以下更改

  ```
  dn: cn=DirXML-PasswordPolicy,cn=Password Policies,cn=Security
  changetype: modify
  add: nsimAssignments
  nsimAssignments: cn=driverset1,o=system
  ```

- **使用其他口令策略**

  使用

  ```
  dn: cn=DirXML-PasswordPolicy,cn=Password Policies,cn=Security
  changetype: add
  ```

在文本编辑器中打开 `sample-driverset.ldif` 文件，并进行以下更改：

1. 将驱动程序集 DN 指向新驱动程序集。
2. 将 nsimAssignments 属性值更改为新驱动程序集的 DN。
3. 将 DirXML-PasswordPolicy 属性更改为指向现有 DirXML-PasswordPolicy 对象或其他口令策略。

配置 Identity Manager 组件

您可通过以下方式执行配置：

- 交互式配置
- 无提示配置

执行交互式配置

1 导航到装入 Identity_Manager_4.9.0_Linux.iso 文件的位置。

2 在命令行指定以下命令来运行 configure.sh 脚本：

```
./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“ 了解配置参数 ”（第 75 页）中的信息。

注释：在 Identity Manager 引擎配置过程中，简单绑定的 TLS 设置为 **Yes**。如果您要将简单绑定的 TLS 值更改为 **No**，请在安装 Identity Manager 引擎的服务器上运行以下命令：

```
ldapconfig set "Require TLS for Simple Binds with Password=no"
```

执行无提示配置

1 导航到装入 Identity_Manager_4.9.0_Linux.iso 文件的位置。

2 要运行无提示安装，请执行以下命令：

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

例如：

./configure.sh -s -f /home/silent.properties，其中， /home/silent.properties 是无提示属性文件的储存位置。

3 要配置组件，请参考“ 了解配置参数 ”（第 75 页）中的信息。

配置 SSPR

下列各节提供有关配置 SSPR 的信息。在配置组件之前，请查看“ 了解配置参数 ”（第 75 页）中的信息。

注释：在配置 SSPR 之前，请确保身份库中存在以下容器和用户对象：

- 用户搜索容器
- 管理员搜索容器
- Identity Applications 管理员用户

执行交互式配置

1 导航到装入 Identity_Manager_4.9.0_Linux.iso 的位置。

2 导航到 sspr 目录。

3 执行以下命令：

```
./configure.sh
```

4 配置设置。

执行无提示配置

在开始配置之前，请确保 `sspr_silentinstall.properties` (`<iso 装入路径 >/sspr/`) 文件已复制到某个可写的目录。例如，将该文件复制到 `/tmp` 目录。

1 导航到装入 `Identity_Manager_4.9.0_Linux.iso` 的位置。

2 导航到 `sspr` 目录。

3 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 /tmp/sspr_silentinstall.properties`，其中，`/tmp/sspr_silentinstall.properties` 是无提示属性文件的储存位置。

4 配置设置。

在 OSP 服务器上修改单点登录访问设置

如果 SSPR 和 OSP 安装在不同的服务器上 （安装 SSPR 的服务器不同于安装 Identity Applications 或 Identity Reporting 的服务器），则您必须在 OSP 服务器上配置单点登录访问设置。本节将帮助您确保这些设置适合您的环境。

1 在安装 OSP 的服务器上起动 RBPM 配置更新实用程序。

2 导航到 **SSO 客户端** > **Self Service Password Reset**。

3 在 **OSP OAuth 重定向 URL** 字段中指定 SSPR 服务器细节。例如 `https://<SSPR 主机名 IP>: 端口 /sspr/public/oauth`。

4 单击**确定**保存所做的更改，然后关闭配置实用程序。

5 重启动 Tomcat 以使更改生效。

6 完成安装的最后步骤

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

安装后的任务通常包括下列项目：

- “配置 Identity Vault”（第 87 页）
- “将非管理员用户配置为身份库管理员”（第 88 页）
- “配置 Remote Loader 和驱动程序”（第 88 页）
- “配置已连接系统”（第 89 页）
- “配置忘记口令管理”（第 92 页）
- “配置 Identity Applications”（第 96 页）
- “配置数据收集的运行时环境”（第 126 页）
- “配置 Identity Reporting”（第 135 页）
- “完成非 Root 用户安装”（第 142 页）
- “激活 Identity Manager”（第 143 页）
- “为分布式部署创建 SSL 证书”（第 144 页）

配置 Identity Vault

- “创建身份库的值索引”
- “手动将 Identity Applications 和 Identity Reporting 证书导入到身份库中”

创建身份库的值索引

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，身份库管理员应该为 manager、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问题，这在群集环境中尤为突出。

您可以在完成 Identity Applications 安装后使用以下方法之一创建这些值索引：

- Identity Console。使用索引管理器。有关详细信息，请参见《NetIQ eDirectory Administration Guide》（NetIQ eDirectory 管理指南）中的 “Creating an Index”（创建索引）。
- 配置实用程序。导航到“杂项”> **身份库索引**，然后在**服务器 DN** 中选择**创建**并指定 DN 值。单击**确定**，然后重启动身份库以保存更改。

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

- 如果您有 Identity Applications 和 Identity Reporting 组件的自定义证书，请将这些证书导入到身份库中的 cacerts (`/opt/netiq/common/jre/lib/security/cacerts`)。

  例如，您可以使用以下 keytool 命令将证书导入到身份库中：

  ```
  keytool -import -trustcacerts -alias <User Application certificate
  alias name> -keystore <cacerts file> -file <User Application
  certificate file>
  ```

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

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

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

将非管理员用户配置为身份库管理员

如果 Identity Applications 配置为使用某个非管理员用户作为身份库管理员，该非管理员用户必须对用户所在子树中的 oidpInstanceData 属性拥有 [写] 权限。否则， OSP 登录可能会失败。

要为非管理员用户设置对 oidpInstanceData 属性的写权限，请执行以下操作：

1. 登录到 Identity Console。
2. 在 **eDirectory** 视图中，单击**权限管理 > 修改受托者**。
3. 选择非管理员用户对象，然后单击**确定**。
4. “ 受托者 ” 即会显示，请单击**指派的权限**。
5. 对 oidpInstanceData 属性设置**比较**、**读**和**写**权限。
6. 单击**应用**以保存并应用您的更改。

配置 Remote Loader 和驱动程序

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

配置已连接系统

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 (https://www.netiq.com/documentation/identity-manager-49-drivers/)。

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。

- “ 创建驱动程序集 ”（第 89 页）
- “ 将默认口令策略指派给驱动程序集 ”（第 89 页）
- “ 在身份库中创建口令策略对象 ”（第 90 页）
- “ 创建自定义口令策略 ”（第 91 页）
- “ 在身份库中创建默认通知集合对象 ”（第 91 页）

创建驱动程序集

Designer for Identity Manager 提供了许多设置供您创建和配置驱动程序集。这些设置可让您指定全局配置值、驱动程序集包、驱动程序集已命名口令、日志级别、跟踪级别和 Java 环境参数。有关详细信息，请参见 《*NetIQ Designer for Identity Manager Administration Guide*》（NetIQ Designer for Identity Manager 管理指南）中的 “Configuring Driver Sets”（配置驱动程序集）。

将默认口令策略指派给驱动程序集

必须将 DirMXL-PasswordPolicy 对象指派给身份库中的每个驱动程序集。 Identity Manager 默认通用口令策略包包括此策略对象。默认策略会安装并指派通用口令策略，以控制 Identity Manager 引擎自动为驱动程序生成随机口令的方式。

或者，若要使用自定义口令策略，您必须创建口令策略对象和策略。有关详细信息，请参见 “ 在身份库中创建口令策略对象 ”（第 90 页）和 “ 创建自定义口令策略 ”（第 91 页）。

1. 在 Designer 中打开您的项目。
2. 在 “ 概要 ” 窗格中，展开您的项目。
3. 展开**包编目 > 通用**以校验默认通用口令策略包是否存在。
4. （视情况而定）如果口令策略包尚未在 Designer 中列出，请完成以下步骤：
   - **4a** 右键单击**包编目**。
   - **4b** 选择**导入包**。

4c 选择 **Identity Manager 默认通用口令策略**，然后单击**确定**。

为了确保表格中显示所有可用的包，您可能需要取消选择**只显示基础包**。

5 选择每个驱动程序集并指派口令策略。

在身份库中创建口令策略对象

如果身份库中不存在 `DirMXL-PasswordPolicy` 对象，您可以使用 Designer 或 ldapmodify 实用程序创建该对象。有关如何在 Designer 中创建此对象的详细信息，请参见《*NetIQ Designer for Identity Manager Administration Guide*》（NetIQ Designer for Identity Manager 管理指南）中的 "Configuring Driver Sets"（配置驱动程序集）。要使用 ldapmodify 实用程序，请执行以下过程：

1 在文本编辑器中创建具有以下属性的 LDAP 数据交换格式 (LDIF) 文件：

```
dn: cn=DirXML-PasswordPolicy,cn=Password Policies,cn=Security
changetype: add
nsimPwdRuleEnforcement: FALSE
nspmSpecialAsLastCharacter: TRUE
nspmSpecialAsFirstCharacter: TRUE
nspmSpecialCharactersAllowed: TRUE
nspmNumericAsLastCharacter: TRUE
nspmNumericAsFirstCharacter: TRUE
nspmNumericCharactersAllowed: TRUE
nspmMaximumLength: 64
nspmConfigurationOptions: 596
passwordUniqueRequired: FALSE
passwordMinimumLength: 1
passwordAllowChange: TRUE
objectClass: nspmPasswordPolicy

dn: cn=DirXML-PasswordPolicy,cn=Password Policies,cn=Security
changetype: modify
add: nsimAssignments
nsimAssignments: <driverset LDAP dn>
```

注释：按原样复制该内容可能会在该文件中插入隐藏的特殊字符。如果在将这些属性添加到身份库时收到 `ldif_record() = 17` 错误讯息，请在两个 DN 之间额外插入一个空格。

2 要在身份库中添加 DirMXL-PasswordPolicy 对象，请执行以下操作从文件导入属性：

从包含 ldapmodify 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， ldapmodify 实用程序位于 `/opt/novell/eDirectory/bin` 目录中。

创建自定义口令策略

您可以不使用 Identity Manager 中的默认口令策略，而是根据您组织的需要创建新的策略。口令策略可以指派给整个树结构、分区根容器、容器或特定的用户。为简化管理， NetIQ 建议在树中尽可能高的位置指派口令策略。有关详细信息，请参见 《*Password Management 3.3.2 Administration Guide*》（Password Management 3.3.2 管理指南）中的 “Creating Password Policies”（创建口令策略）。

注释：您还必须将 DirXML-PasswordPolicy 对象指派给驱动程序集。有关详细信息，请参见 “在身份库中创建口令策略对象”（第 90 页）。

在身份库中创建默认通知集合对象

默认通知集合是一个身份库对象，它包含一套电子邮件通知模板，以及一个用于发送基于模板生成的电子邮件的 SMTP 服务器。如果身份库中不存在默认通知集合对象，请使用 Designer 创建该对象。

1. 在 Designer 中打开您的项目。
2. 在“概要”窗格中，展开您的项目。
3. 右键单击身份库，然后单击身份库**属性**。
4. 单击**包**，然后单击**添加包**图标。
5. 选择所有通知模板包，然后单击**确定**。
6. 单击**应用**以通过**安装**操作来安装包。
7. 将通知模板部署到身份库。

创建驱动程序

要创建驱动程序，请使用 Designer 中提供的包管理功能。对于您打算使用的每个 Identity Manager 驱动程序，创建一个驱动程序对象，并导入驱动程序配置。驱动程序对象中包含该驱动程序的配置参数和策略。在创建驱动程序对象的过程中，安装驱动程序包，然后根据您环境的需求修改驱动程序配置。

驱动程序包包含默认策略集。在实施数据共享模型时，这些策略可以帮您顺利开始工作。在大多数时候，需要使用附带的默认配置文件设置驱动程序，然后根据环境要求修改驱动程序配置文件。创建并配置驱动程序后将其部署到身份库并加以启动。通常情况下，驱动程序创建过程涉及以下操作：

1. 导入驱动程序包
2. 安装驱动程序包
3. 配置驱动程序对象
4. 部署驱动程序对象
5. 启动驱动程序对象

有关其他信息和特定于驱动程序的信息，请参见 Identity Manager 驱动程序网站 (https://www.netiq.com/documentation/identity-manager-49-drivers/) 上的相关驱动程序实施指南。

定义策略

可以使用策略在特定环境中自定义流入、流出 Identity Vault 的信息流。例如，某个公司可能使用 inetorgperson 作为主用户类，而另一个公司则可能使用 User。为了处理这种情况，系统会创建策略以告知 Identity Manager 引擎一个用户在各个系统中的名称。只要在已连接系统间传递对用户产生影响的操作， Identity Manager 都将应用策略以进行上述更改。

也可利用策略创建新对象、更新特性值、执行纲要转换、定义匹配准则、维护 Identity Manager 关联以及执行其他许多操作。

NetIQ 建议使用 Designer 定义驱动程序策略，以满足您的业务需求。有关详细的策略指南，请参见 《*NetIQ Identity Manager - Using Designer to Create Policies*》（NetIQ Identity Manager - 使用 Designer 创建策略）指南和 《*NetIQ Identity Manager Understanding Policies Guide*》（NetIQ Identity Manager 了解策略指南）。有关 Identity Manager 使用的文档类型定义 (DTD) 的信息，请参见 《Identity Manager DTD Reference》（Identity Manager DTD 参考手册）。这些资源包含：

- 每种可用策略的详细说明。
- 关于策略构建器全面详尽的用户指南和参照，包括每个条件、操作、名词和动词的示例和语法。
- 讨论如何使用 XSLT 样式表创建策略。

配置忘记口令管理

Identity Manager 安装中包含 Self Service Password Reset，可帮助您管理忘记口令的重设置过程。此外，您也可以使用外部口令管理系统。

- “ 使用 Self Service Password Reset 进行忘记口令管理 ”（第 92 页）
- “ 使用外部系统进行忘记口令管理 ”（第 94 页）
- “ 针对分布式环境或群集环境更新仪表板中的 SSPR 链接 ”（第 96 页）

使用 Self Service Password Reset 进行忘记口令管理

在大多数情况下，您可以在安装 SSPR 和 Identity Applications 时启用忘记口令管理功能。但是，有时您可能没有指定当口令更改后， SSPR 要将用户定向到的 Identity Applications 登录页 URL。此时，您也需要启用忘记口令管理。本节提供以下信息：

- “ 将 Identity Manager 配置为使用 Self Service Password Reset”（第 93 页）
- “ 为 Identity Manager 配置 Self Service Password Reset”（第 93 页）
- “ 锁定 SSPR 配置 ”（第 94 页）

将 Identity Manager 配置为使用 Self Service Password Reset

本节提供了将 Identity Manager 配置为使用 SSPR 的相关信息。

1 登录到安装了 Identity Applications 的服务器。

2 运行 RBPM 配置实用程序。有关详细信息，请参见 “ 运行 Identity Applications 配置实用程序 ”（第 97 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 客户端密码**，请指定 SSPR 单点登录客户端的口令。

9 对于 **OSP 重定向 URL**，请指定在完成鉴定后，鉴定服务器要将浏览器客户端重定向到的绝对 URL。

使用以下格式：`protocol://server:port/path`。例如，`http://10.10.10.48:8180/sspr/public/oauth`。

10 保存更改并关闭实用程序。

为 Identity Manager 配置 Self Service Password Reset

本节提供了配置 SSPR 以与 Identity Manager 配合使用的相关信息。例如，您可能想要修改口令策略和询问应答问题。

如果您随 Identity Manager 一起安装了 SSPR，即已指定了管理员可用来配置应用程序的口令。NetIQ 建议您修改 SSPR 设置，然后指定可以配置 SSPR 的管理员帐户或组。

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* (https://www.netiq.com/documentation/self-service-password-reset-47/sspr-adminguide/data/bookinfo.html)》（NetIQ Self Service Password Reset 管理指南）中的 “Configuring Self Service Password Reset (https://wwwtest.netiq.com/documentation/self-service-password-reset-47/sspr-adminguide/data/b14gnrxl.html)”（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 94 页）。

4 （可选）要在锁定配置后修改 SSPR 设置，必须在 `SSPRConfiguration.xml` 文件中将 `configIsEditable` 设置设为 `true`。

5 从 SSPR 中注销。

6 要使更改生效，请重启动 Tomcat。

锁定 SSPR 配置

1 转到 **http://<IP/DNS name>:<port>/sspr**。此链接可将您转到 SSPR 门户。

2 使用管理员帐户登录到 Identity Manager，或使用现有的登录身份凭证登录。

3 单击页面顶部的**配置管理器**，然后指定您在安装期间指定的配置口令。

4 单击**配置编辑器**，然后浏览到**设置 > LDAP 设置**。

5 锁定 SSPR 配置 文件 (`SSPRConfiguration.xml`)。

5a 在 “ 管理员许可权限 ” 部分下，在身份库中以 LDAP 格式定义过滤器，以过滤对 SSPR 具有管理员权限的用户或组。默认情况下，该过滤器设置为 `groupMembership=cn=Admins,ou=Groups,o=example`。

例如，对于 User Application 管理员，请将它设置为 `uaadmin` (`cn=uaadmin`)。

这可以防止用户修改 SSPR 中的配置，但具有完全权限可修改设置的 SSPR 管理员用户除外。

5b 为确保 LDAP 查询返回结果，请单击**查看匹配项**。

如果设置中存在任何错误，则您无法继续设置下一个配置选项。 SSPR 会显示错误细节，以帮助您进行问题查错。

5c 单击**保存**。

5d 在弹出的确认窗口中，单击**确定**。

锁定 SSPR 后，管理员用户可以在 “ 管理 ” 用户界面中查看其他选项，例如 “ 仪表板 ”、“ 用户活动 ”、“ 数据分析 ” 等，而在锁定 SSPR 之前则不会显示这些选项。

6 （可选）要在锁定配置后修改 SSPR 设置，必须在 `SSPRConfiguration.xml` 文件中将 `configIsEditable` 设置设为 `true`。

7 从 SSPR 中注销。

8 以步骤 3 中定义的管理员用户身份再次登录到 SSPR。

9 单击**关闭配置**，然后单击**确定**以确认更改。

10 要使更改生效，请重启动 Tomcat。

使用外部系统进行忘记口令管理

要使用外部系统，必须指定包含 “ 忘记口令 ” 功能的 WAR 文件的位置。此过程包括以下活动：

- “ 指定外部忘记口令管理 WAR 文件 ”（第 95 页）
- “ 测试外部忘记口令配置 ”（第 95 页）
- “ 配置应用程序服务器之间的 SSL 通讯 ”（第 96 页）

指定外部忘记口令管理 WAR 文件

如果您在安装期间未指定这些值，现在想要修改设置，您可以使用 RBPM 配置实用程序，或者以管理员身份在 User Application 中进行更改。

1 （视情况而定）要在 RBPM 配置实用程序中修改设置，请完成以下步骤：

   1a 登录到安装了 Identity Applications 的服务器。

   1b 运行 RBPM 配置实用程序。有关详细信息，请参见“ 运行 Identity Applications 配置实用程序 ”（第 97 页）。

   1c 在实用程序中，浏览到**鉴定 > 口令管理**。

   1d 对于**口令管理提供程序**，请指定 **User Application （旧版）**。

2 （视情况而定）要在 User Application 中修改设置，请完成以下步骤：

   2a 以 User Application 管理员身份登录。

   2b 浏览到**管理 > 应用程序配置 > 口令模块设置 > 登录**。

3 对于**忘记口令**，请指定**外部**。

4 对于**忘记口令链接**，请指定当用户在登录页面上单击**忘记口令**时所显示的链接。当用户单击此链接时，应用程序会将其定向到外部口令管理系统。例如：

   ```
   http://localhost:8180/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsp
   ```

5 对于**忘记口令返回链接**，请指定用户执行完忘记口令过程后显示的链接。用户单击此链接，即可重定向到指定的链接。例如：

   ```
   http://localhost/IDMProv
   ```

6 对于**忘记口令 Web 服务 URL**，请指定外部转发口令 WAR 用来回调 Identity Applications 的 Web 服务 URL。使用以下格式：

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

   返回链接必须使用 SSL，以确保与 Identity Applications 进行安全的 Web 服务通讯。有关详细信息，请参见“ 配置应用程序服务器之间的 SSL 通讯 ”（第 96 页）。

7 手动将 `ExternalPwd.war` 复制到运行外部口令 WAR 功能的远程应用程序服务器部署目录。

测试外部忘记口令配置

如果您拥有外部口令 WAR 文件并想要通过访问 “ 忘记口令 ” 功能来测试该功能，可以在以下位置访问它：

- 直接在浏览器中访问。转到外部口令 WAR 文件中的 “ 忘记口令 ” 页面。例如：`http://localhost:8180/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsp`。
- 在 User Application 登录页面上，单击**忘记口令**链接。

配置应用程序服务器之间的 SSL 通讯

如果您使用的是外部口令管理系统，则必须在部署 Identity Applications 与外部忘记口令管理 WAR 文件的 Tomcat 实例之间配置 SSL 通讯。有关详细信息，请参见 Tomcat 文档。

针对分布式环境或群集环境更新仪表板中的 SSPR 链接

安装过程假设您要将 SSPR 部署在 Identity Applications 和 Identity Reporting 所在的同一个应用程序服务器上。默认情况下，仪表板中**应用程序**页面上的内置链接使用指向本地系统上 SSPR 的相对 URL 格式。例如 `\sspr\private\changepassword`。如果在分布式环境或群集环境中安装应用程序，则必须更新 SSPR 链接的 URL。

有关详细信息，请参见 *Identity Applications 的帮助*。

1. 以管理员身份登录仪表板。例如，以 `uaadmin` 身份登录。
2. 单击**编辑**。
3. 在“编辑主页项目”页面上，将鼠标悬停在要更新的项目上，然后单击编辑图标。例如，选择**更改我的口令**。
4. 对于**链接**，请指定绝对 URL。例如：`http://10.10.10.48:8180/sspr/changepassword`。
5. 单击**保存**。
6. 对要更新的每个 SSPR 链接重复上述步骤。
7. 完成后，单击**我已完成**。
8. 注销，然后以普通用户身份登录以测试更改。

配置 Identity Applications

- “储存 Configupdate 实用程序口令”（第 97 页）
- “配置 Identity Applications 的设置”（第 97 页）
- “指定权限索引的位置”（第 121 页）
- “部署适用于 Identity Applications 的 REST API”（第 122 页）
- “配置 Identity Applications 的 Oracle 数据库”（第 122 页）
- “使用 Oracle 服务名称访问 Oracle 数据库”（第 123 页）
- “手动创建数据库纲要”（第 124 页）
- “配置 Identity Applications 的单点登录设置”（第 125 页）
- “启动 Identity Applications”（第 125 页）
- “Identity Applications 的配置和用法注意事项”（第 126 页）

储存 Configupdate 实用程序口令

起动 configupdate 时，系统将提示用户输入主密钥储存区 (encrypt-keys.pkcs12) 口令。默认情况下，此口令是 changeit。此密钥储存区位于 /opt/netiq/idm/apps/tomcat/conf。

执行以下步骤，以更改并重新加密口令：

1. 运行以下命令，以更改您的 Configupdate 实用程序口令：

   ```
   keytool -storepasswd -new <new master keystore password> -keystore /
   opt/netiq/idm/apps/tomcat/conf/encrypt-keys.pkcs12 -storepass changeit
   -storetype PKCS12
   ```

2. 要加密新口令，请运行以下命令：

   ```
   /opt/netiq/common/jre/bin/java -cp /opt/netiq/idm/apps/tomcat/lib/
   obscurity-<version>-uber.jar
   com.netiq.ism.obfuscate.server.util.PasswordObfuscator <new master
   keystore password>
   ```

3. 请务必通过更改 /opt/netiq/idm/apps/tomcat/conf 下的 ism-sensitive.properties 文件中的 com.microfocus.ism.master-storepass 值，来储存已加密的口令

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 configudate.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。将主节点中的 ism-sensitive.properties、 ism-configuration.properties 和 encrypt-keys.pkcs12 复制到所有 User Application 节点。

本节说明了配置实用程序中的设置。这些设置按选项卡组织。如果您要安装 Identity Reporting，安装过程会将报告的参数添加到实用程序中。

运行 Identity Applications 配置实用程序

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.properties`。

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。

注释：由于 Identity Manager 不支持 NAM OAuth，因此请不要在配置实用程序的“鉴定服务器”选项卡中使用 **Access Manager 是 OAuth 提供程序**选项。

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 98 页）
- “身份库 DN”（第 99 页）
- “身份库用户身份”（第 102 页）
- “身份库用户组”（第 103 页）
- “身份库证书”（第 103 页）
- “电子邮件服务器配置”（第 104 页）
- “可信密钥储存区”（第 106 页）
- “NetIQ Sentinel 数字签名证书和密钥”（第 106 页）
- “杂项”（第 106 页）
- “容器对象”（第 108 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 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。

通知模板主机

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

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

通知模板端口

指定托管 Identity Applications 的 Tomcat 的端口号。

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

通知模板安全端口

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

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

通知模板协议

指定在发送用户电子邮件时要包含在 URL 中的非安全协议。例如：`http`。

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

通知模板安全协议

指定在发送用户电子邮件时要包含在 URL 中的安全协议。例如：`https`。

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

通知 SMTP 电子邮件发件人

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

SMTP 服务器名称

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

服务器需要鉴定

指定您是否希望服务器要求鉴定。

您还必须指定电子邮件服务器的身份凭证。

用户名

*仅当您启用了**服务器需要鉴定**时才适用。*

指定电子邮件服务器的登录帐户名。

口令

*仅当您启用了**服务器需要鉴定**时才适用。*

指定邮件服务器的登录帐户口令。

使用 SMTP TLS

指定在邮件服务器之间进行传输期间，是否要保护电子邮件内容的安全。

电子邮件通知图像位置

指定要在电子邮件通知中包含的图像的路径。

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

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

如果 Identity Applications 在使用 http 进行纯文本通讯的服务器上运行，请将映像路径中的 `https` 替换为 `http`。映像路径的示例：`http://localhost:8080/IDMProv/images`

对电子邮件签名

指定是否要在寄出的邮件中添加数字签名。

如果启用此选项，则还必须指定密钥存储区和签名密钥的设置。

密钥存储区路径

*仅当您启用了**对电子邮件签名**时才适用。*

指定要用于对电子邮件进行数字签名的密钥存储区 (`cacerts`) 文件的完整路径。您可以手动输入路径，也可以浏览到 `cacerts` 文件。

例如， `/opt/netiq/idm/apps/jre/lib/security/cacerts`。

密钥存储区口令

*仅当您启用了**对电子邮件签名**时才适用。*

提供密钥存储区文件的口令。例如， `changeit`。

签名密钥的别名

*仅当您启用了**对电子邮件签名**时才适用。*

指定签名密钥在密钥存储区中的别名。例如， `idmapptest`。

签名密钥口令

*仅当您启用了**对电子邮件签名**时才适用。*

指定用于保护包含签名密钥的文件的口令。例如， `changeit`。

可信密钥储存区

这组设置定义了 Identity Applications 的可信密钥存储区的值。仅当您选择了**显示高级选项**时，实用程序才显示这些设置。

可信储存区路径

指定包含所有可信签名者的证书的可信密钥存储区的路径。如果此路径为空， Identity Applications 将从系统属性 `javax.net.ssl.trustStore` 中获取路径。如果该系统属性无法提供路径，安装程序默认使用 `jre/lib/security/cacerts`。

可信储存口令

指定可信密钥存储区的口令。如果将此字段留空， Identity Applications 将从系统属性 `javax.net.ssl.trustStorePassword` 中获取口令。如果该系统属性无法提供口令，安装程序默认使用 `changeit`。

此口令已使用主密钥进行过加密。

可信证书存储区类型

指定可信证书存储区路径是使用 Java 密钥存储区 (JKS) 还是 PKCS12 进行数字签名。

NetIQ Sentinel 数字签名证书和密钥

本节定义可让 Identity Manager 与 Sentinel 通讯以进行事件审计的值。仅当您选择了**显示高级选项**时，实用程序才显示这些设置。

Sentinel 数字签名证书

列出您希望 OAuth 服务器用来鉴定发送到 Sentinel 的审计讯息的自定义公共密钥证书。

Sentinel 数字签名私用密钥

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

杂项

仅当您选择了**显示高级选项**时，实用程序才显示这些设置。

OCSP URI

指定当客户端安装使用联机证书状态协议 (OCSP) 时要使用的统一资源标识符 (URI)。例如：`http://host:port/ocspLocal`。

OCSP URI 在线更新可信证书的状态。

授权配置路径

指定授权配置文件的完全限定名。

身份库索引

要提高 Identity Applications 的性能，可以为 manager、 ismanager 和 srvprvUUID 属性创建值索引。

您可以在完成 Identity Applications 安装后，使用配置实用程序创建值索引。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 Identity Console 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。
- 要创建索引，请在**服务器 DN** 设置中选择**创建**，并指定**服务器 DN** 的值。单击**确定**，然后重启动身份库以使更改生效。
- 要删除索引，请在**服务器 DN** 设置中选择**删除**，并指定**服务器 DN** 的值。单击**确定**，然后重启动身份库以使更改生效。

服务器 DN

仅当您要创建或删除身份库索引时才适用。

指定要在其中创建或去除索引的 eDirectory 服务器。

一次只能指定一个服务器。要在多个 eDirectory 服务器上配置索引，必须多次运行 RBPM 配置实用程序。

重初始化 RBPM 安全性

指定是否要在完成安装过程时重设置 RBPM 安全性。您还必须重新部署 Identity Applications。

IDMReport URL

指定 Identity Manager Reporting Module 的 URL。例如：`http://hostname:port/IDMRPT`。

自定义主题环境名称

指定要用于在浏览器中显示 Identity Applications 的自定义主题的名称。

日志讯息标识符前缀

指定要在 `idmuserapp_logging.xml` 文件中 CONSOLE 和 FILE 追加器的布局模式内使用的值。默认值为 `RBPM`。

更改 RBPM 环境名称

指定是否要更改 RBPM 的环境名称。

您还必须指定 Roles and Resource 驱动程序的新名称和 DN。

RBPM 环境名称

*仅当您选择了**更改 RBPM 环境名称**时才适用。*

指定 RBPM 的新环境名称。

角色驱动程序 DN

*仅当您选择了**更改 RBPM 环境名称**时才适用。*

指定角色和资源驱动程序的 DN。

容器对象

这些参数只会在安装期间应用。

这组设置将帮助您定义容器对象的值或创建新的容器对象。

已选定

指定您要使用的容器对象类型。

容器对象类型

指定以下容器：位置、国家 / 地区、组织单位、组织或域。

您也可以在 Identity Console 中定义自己的容器，然后在**添加新容器对象**下面添加这些容器。

容器属性名称

指定与所指定容器对象类型关联的属性类型的名称。

添加新的容器对象：容器对象类型

指定可用作新容器的身份库中对象类的 LDAP 名称。

添加新的容器对象：容器属性名称

指定与新容器对象类型关联的属性类型的名称。

报告参数

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

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

- “ 电子邮件递送配置 ”（第 108 页）
- “ 报告保留值 ”（第 109 页）
- “ 修改区域设置 ”（第 109 页）
- “ 角色配置 ”（第 109 页）
- “ 出站代理 ”（第 110 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**

出站代理

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

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

使用代理

指定该选项会为报告功能使用反向代理服务器。

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

  仅当您要使用 TCP 作为网络协议时适用。

鉴定参数

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

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

- “ 鉴定服务器 ”（第 110 页）
- “ 鉴定配置 ”（第 111 页）
- “ 身份验证方法 ”（第 111 页）
- “ 口令管理 ”（第 113 页）
- “Sentinel 数字签名证书和密钥 ”（第 114 页）

鉴定服务器

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

OAuth 服务器主机标识符

必需

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

OAuth 服务器 TCP 端口

指定鉴定服务器的端口。

Access Manager 是 OAuth 提供程序

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

OAuth 服务器正在使用 TLS/SSL

指定鉴定服务器是否使用 TLS/SSL 协议进行通讯。

可选 TLS/SSL 可信证书存储区文件

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

可选 TLS/SSL 可信证书存储区口令

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

指定用于装载 TLS/SSL 鉴定服务器的密钥存储区文件的口令。

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

鉴定配置

这组设置定义了鉴定服务器的设置。

管理员容器的 LDAP DN

必需

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

解析命名属性重复

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

将鉴定源限制为环境

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

会话超时 （分钟）

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

访问令牌有效期 （秒）

指定 OSP 访问令牌保持有效的秒数。默认值为 60 秒。

刷新令牌有效期 （小时）

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

身份验证方法

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

方法

指定当用户登录时您希望 Identity Manager 使用的鉴定类型。

- **名称和口令：**OSP 使用身份库校验鉴定。
- **Kerberos：**OSP 接受来自 Kerberos 票据服务器和身份库的鉴定。
- **SAML 2.0：**OSP 接受来自 SAML 身份提供商和身份库的鉴定。

启用 reCAPTCHA

*仅当您指定了**名称和口令**时才适用。*

指定是否要在登录页面上启用 reCAPTCHA。

reCAPTCHA 会要求用户确认他们不是机器人，这提供了一层额外的安全防护。它会显示一些图像，用户必须根据匹配准则选择相应图像。如果选择正确， Access Manager 将鉴定用户的鉴定身份凭证。如果选择不正确， Access Manager 将不会鉴定用户身份凭证，而是重定向到登录页面。

启用双因素鉴定

*仅当您指定了**名称和口令**时才适用。*

指定是否要启用双因素鉴定。

这需要在**第二个因素**选项卡中完成一些配置。有关详细信息，请参见“ 第二个因素参数 ”（第 119 页）。

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。

启用回退 reCAPTCHA

*仅当您指定了 **Kerberos** 时才适用。*

指定在无法使用 Kerberos 时，是否要通过回退用户名和口令启用 reCAPTCHA。

需要启用 reCAPTCHA 前的尝试次数

*仅当您选中了**启用回退 reCAPTCHA** 复选框时才适用。*

指定登录尝试失败多少次后启用 reCAPTCHA。将值设置为零表示始终需要启用 reCAPTCHA。

站点密钥

*仅当您选中了**启用回退 reCAPTCHA** 复选框时才适用。*

指定从 Google reCAPTCHA 网站获取的 reCAPTCHA 站点密钥值。

私用密钥

*仅当您选中了**启用回退 reCAPTCHA** 复选框时才适用。*

指定从 Google reCAPTCHA 网站获取的 reCAPTCHA 私用密钥值。

启用回退双因素鉴定

*仅当您指定了 **Kerberos** 时才适用。*

指定在无法使用 Kerberos 时，是否要通过回退用户名和口令启用双因素鉴定。

这需要在**第二个因素**选项卡中完成一些配置。有关详细信息，请参见“ 第二个因素参数 ”（第 119 页）。

用户注销登陆页

*仅当您指定了 **Kerberos** 时才适用。*

指定是否要在成功注销后启用登陆页，而不是重定向到登录页。

登陆页

仅当您指定了SAML 时才适用。

- **无：**指定不使用登陆页。如果指定了 IDP URL，请选择此选项。
- **内部：**指定要使用内部 OSP 登陆页。
- **外部：**指定要将您重定向到外部 OSP 登陆页。

URL

仅当您在登陆页 字段中选择了外部时才适用。

指定外部登陆页的 URL。

元数据来源

仅当您指定了SAML 时才适用。

指定 IDP 元数据的来源。您可以从 URL 装载元数据，也可以复制以前获取的元数据。

元数据 URL

仅当您在元数据 URL 字段中指定了 URL 时才适用。

指定是否要从 URL 装载元数据，并在退出应用程序之前将元数据保存到配置中。

保存时装载

仅当您在元数据 URL 字段中指定了 URL 时才适用。

指定 OSP 用于将鉴定请求重定向到 SAML 的 URL。

IDP 元数据

仅当您在元数据 URL 字段中指定了复制 / 粘贴时才适用。

指定您要粘贴的数据 （该数据从 SAML IDP 获取）。

退出时配置 Access Manager

仅当您在元数据 URL 字段中指定了复制 / 粘贴时才适用。

指定是否要在 Access Manager 中自动配置 SAML 服务提供程序定义。

口令管理

这组设置定义了可让用户通过自助操作修改其口令的值。

口令管理提供程序

指定要使用的口令管理系统类型。

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

忘记口令

仅当您要使用 SSPR 时，此复选框参数才适用。

指定是否希望用户不联系帮助中心自行恢复忘记的口令。

您还必须为“忘记口令”功能配置询问应答策略。有关详细信息，请参见 *《NetIQ Self Service Password Reset Administration Guide》*(https://wwwtest.netiq.com/documentation/self-service-password-reset-47/sspr-adminguide/data/bookinfo.html)（NetIQ Self Service Password Reset 管理指南）。

忘记口令

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

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

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

忘记口令链接

仅当您要使用外部口令管理系统时才适用。

指定指向“忘记口令”功能页面的 URL。在外部或内部口令管理 WAR 中指定 `ForgotPassword.jsp` 文件。

忘记口令返回链接

仅当您要使用外部口令管理系统时才适用。

指定**忘记口令返回链接**的 URL，用户可在执行完忘记口令操作后单击该链接以返回。

忘记口令 Web 服务 URL

仅当您要使用外部口令管理系统时才适用。

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

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

Sentinel 数字签名证书和密钥

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

Sentinel 数字签名证书

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

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

Sentinel 数字签名私用密钥

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

SSO 客户端参数

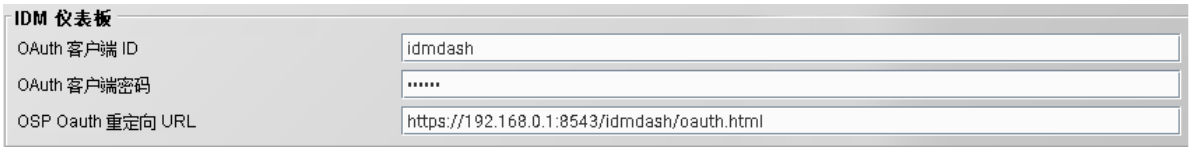
在配置 Identity Applications 时，此选项卡可定义用于管理对应用程序的单点登录访问的值。

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 115 页）
- “IDM 管理员 ”（第 116 页）
- “RBPM”（第 116 页）
- “ 报告 ”（第 117 页）
- “IDM 数据收集服务 ”（第 118 页）
- “DCS 驱动程序 ”（第 118 页）
- “Self Service Password Reset”（第 118 页）

IDM 仪表板

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



OAuth 客户端 ID

必需

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

OAuth 客户端密码

必需

指定仪表板的单点登录客户端的口令。

OSP OAuth 重定向 URL

必需

指定在完成鉴定后，鉴定服务器要将浏览器客户端重定向到的绝对 URL。

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

IDM 管理员

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

OAuth 客户端 ID

必需

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

OAuth 客户端密码

必需

指定 Identity Manager 管理员的单点登录客户端的口令。

OSP OAuth 重定向 URL

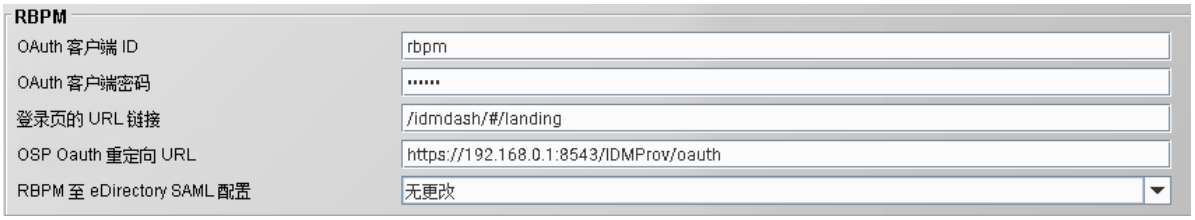
必需

指定在完成鉴定后，鉴定服务器要将浏览器客户端重定向到的绝对 URL。

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

RBPM

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



OAuth 客户端 ID

必需

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

OAuth 客户端密码

必需

指定 User Application 单点登录客户端的口令。

登录页的 URL 链接

必需

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

OSP OAuth 重定向 URL

必需

指定在完成鉴定后，鉴定服务器要将浏览器客户端重定向到的绝对 URL。

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

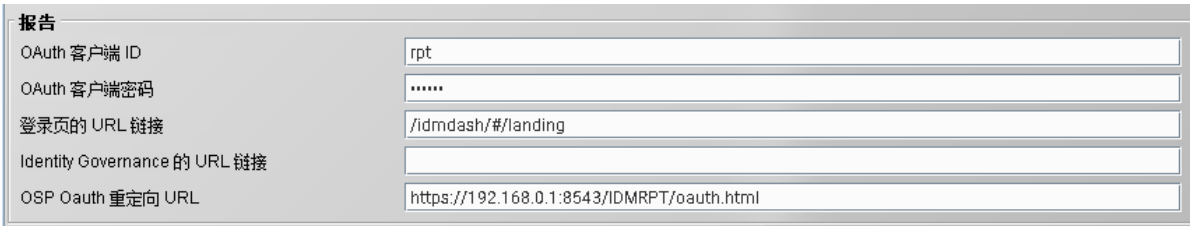
RBPM 至 eDirectory SAML 配置

必需

指定 SSO 鉴定所需的 RBPM 至身份库 SAML 设置。

报告

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



OAuth 客户端 ID

必需

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

OAuth 客户端密码

必需

指定 Identity Reporting 单点登录客户端的口令。

登录页的 URL 链接

必需

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

如果您将 Identity Reporting 和 Identity Applications 安装到不同的服务器中，请指定绝对 URL。使用以下格式：`protocol://server:port/path`。例如，`https://192.168.0.1:8543/IDMRPT/oauth`。

OSP OAuth 重定向 URL

必需

指定在完成鉴定后，鉴定服务器要将浏览器客户端重定向到的绝对 URL。

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

IDM 数据收集服务

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

OAuth 客户端 ID

必需

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

OAuth 客户端密码

必需

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

OSP OAuth 重定向 URL

必需

指定在完成鉴定后，鉴定服务器要将浏览器客户端重定向到的绝对 URL。

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

DCS 驱动程序

这组设置定义了用于管理数据收集服务驱动程序的值。



OAuth 客户端 ID

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

OAuth 客户端密码

指定数据收集服务驱动程序的单点登录客户端的口令。

Self Service Password Reset

本节定义用户访问 SSPR 所需 URL 的值。

OAuth 客户端 ID

必需

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

OAuth 客户端密码

必需

指定 SSPR 单点登录客户端的口令。

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`。

第二个因素参数

在继续后续操作之前，请确保已在高级鉴定中创建了方法、链和事件。您必须将 OSP 配置为接受来自高级鉴定的鉴定。

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：

AAF 管理员

此部分定义高级鉴定管理员的设置：

管理员名称 （储存库 \ 名称）

必需

指定 OSP 用来与高级鉴定进行交互的高级鉴定管理员帐户的储存库限定名称。通常，该帐户位于 LOCAL 储存库中。

默认的高级鉴定管理员帐户名为 admin。如果您已使用此帐户，则**管理员名称**值为：

LOCAL\admin （即储存库名称 \ 用户名）

管理员口令

必需

指定上面设置的高级鉴定管理用户的口令。

AAF 用户储存库

此部分定义高级鉴定用户储存库的设置：

用户储存库名称

必需

指定您在高级鉴定中创建的储存库的名称。此储存库对应于 Identity Manager 的身份库。

AAF 服务器

此部分定义高级鉴定服务器的设置：

允许测试 TLS 证书

必需

指定是否要忽略来自 AAF 服务器的无效测试证书主体。这仅适用于初始配置和测试。

单击**添加**，然后指定高级鉴定服务器的 DNS 名称或 IP 地址。如果您使用的端口不是 443，另请指定所用的端口。

（视情况而定）如果您已群集化高级鉴定服务器，请再次单击**添加**，然后指定群集中每台服务器的每个 DNS 名称或 IP 地址。

显示优化参数

必需

指定是否要启用优化参数。

注销会话清理（分钟）：*仅当您已选中**显示优化参数**复选框时才适用。*

指定经过多久后将活动的 AAF 登录会话视为发生超时和清理问题。

检测信号间隔（毫秒）：*仅当您已选中**显示优化参数**复选框时才适用。*

指定经过多久后向 AAF 服务器发送检测信号请求以检查可用性。

AAF 端点

此部分定义高级鉴定端点的设置：

创建新端点

必需

指定是否要创建用于双因素鉴定的新端点。

标识符：*仅当您未选中**创建新端点**复选框时才适用。*

指定 AAF 管理中配置的端点标识符。

机密：*仅当您未选中**创建新端点**复选框时才适用。*

指定 AAF 管理中配置的端点机密。

名称：*仅当您已选中**创建新端点**复选框时才适用。*

指定新端点的名称，用于在 AAF 管理页面中标识该端点。

说明：*仅当您已选中**创建新端点**复选框时才适用。*

指定上面设置的新端点的说明。

第二个因素条件

此部分定义第二个因素条件的设置。

所有用户，任何时间

必需

指定是否允许所有用户在任何时间提供第二个因素鉴定。

用户登录条件：*仅当您未选中**所有用户，任何时间**复选框时才适用。*

指定您可以定义要让 Identity Manager 使用第二个因素鉴定所需满足的特定表达式和条件。

第二个因素鉴定方法

此部分定义高级鉴定方法的设置。

指定是否要为不同的方法启用第二个因素鉴定。

要对某个方法禁用第二个因素鉴定，请取消选中该方法名称旁边的复选框。

如果用户已在多个方法中注册， Identity Manager 将使用第二个因素方法的相对优先级。

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。选择**使用 TLS** >“ 显示高级选项 ”，并提供 **Identity Manager 密钥存储区文件名**和 **Identity Manager 密钥存储区口令**。

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。如果您要提供自选的中间事件储存目录，必须先确保该目录的许可权限和所有权已更改为 `novlua`。要更改目录的许可权限，请运行以下命令：

```
chown novlua:novlua <directory_path>
```

```
chmod 755 <directory_path>
```

其中， `<directory_path>` 是中间事件储存目录的路径。

有关配置 CEF 审计的完整文档，请参见 《*NetIQ Identity Manager - Configuring Auditing in Identity Manager*》（NetIQ Identity Manager - 在 Identity Manager 中配置审计）中的 “Configuring Identity Applications” （配置 Identity Applications）。

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/permindex`。

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

要指定索引的位置，请执行以下操作：

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

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

   例如：

   `com.netiq.idm.cis.indexdir = /opt/netiq/idm/apps/tomcat/temp/permindex`
4. 保存并关闭文件。
5. 删除临时目录中的现有 `permindex` 文件夹。
6. 启动 Tomcat。

要为群集启用许可权限索引，请参见第 32 章 “Tomcat 应用程序服务器上的 Identity Applications 群集部署解决方案示例 ”（第 351 页）。

部署适用于 Identity Applications 的 REST API

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

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

注释：要导出工作流程数据库表，请在 `ism-configuration.properties` 文件中添加下面一项：

```
com.microfocus.workflow.migration.tables = <list-of-tables-to-exported-comma-separated>
```

例如：

```
com.microfocus.workflow.migration.tables = afmodel,afform,
afprocess,afdocument,afactivity,afactivitytimertasks,afbranch,afcomment,af
provisioningstatus,afquorum,afworktask,configuration,email_approval_token,
localization,processed_eba_mails
```

配置 Identity Applications 的 Oracle 数据库

执行以下步骤来配置 Oracle 数据库：

1. 下载并安装最新版本的 Oracle 数据库。

   该数据库的默认 SID 为 `orcl`。

2 创建数据库实例：

2a 在命令行中运行以下命令，以起动数据库配置助手 (Database Configuration Assistor)。

```
dbca
```

2b 在**全局数据库名称**字段中指定数据库名称。例如 `idappsdb`。

3 创建数据库用户：

3a 登录到 Oracle SQL 开发人员工具。

3b 运行以下命令：

```
CREATE USER idmadmin IDENTIFIED BY <password>;
GRANT CONNECT, RESOURCE to idmadmin;
ALTER USER idmadmin quota 100M on USERS;
```

其中，

`idmadmin` 表示用户帐户，

`<password>` 表示用户口令。

4 重复步骤 2 和 3 以配置工作流程引擎数据库。

注释：为 Identity Applications 配置 Oracle 数据库时，请确保使用上述章节中指定的相同细节。

使用 Oracle 服务名称访问 Oracle 数据库

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

1 运行以下命令，在 Oracle 数据库中创建服务名称：

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

其中，`SERVICE 1` 是 Oracle 服务的名称。

注释：可以使用大写或小写指定服务名称。搜索不区分大小写。

---

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

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

3 重启动 Tomcat。

4 校验该服务名称是否已包含在 `catalina.out` 日志文件中。

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

手动创建数据库纲要

安装 Identity Applications 时，可以暂缓连接到数据库或者在数据库中创建表。如果您对数据库没有许可权限，则可能需要选择此选项。安装程序将创建一个 SQL 文件，您可以使用该文件来创建数据库纲要。您也可以在安装后重创建数据库表，而无需重新安装。为此，您要删除 Identity Applications 的数据库，并创建同名的新数据库。

使用 SQL 文件生成数据库纲要

本节假设安装程序已创建了您可执行以生成数据库纲要的 SQL 文件。如果您没有该 SQL 文件，请参见“ 手动创建 SQL 文件以生成数据库纲要 ”（第 124 页）。

注释：请不要使用 SQL*Plus 来执行该 SQL 文件。该文件中的行长度超过了 4000 个字符。

---

1. 停止 应用程序服务器。
2. 登录到数据库服务器。
3. 删除 Identity Applications 使用的数据库。
4. 创建与步骤 3 中所删除数据库同名的新数据库。
5. 浏览到安装过程创建的 SQL 脚本 （默认位于 `/installation_path/userapp/sql` 目录中）。
6. （视情况而定）对于 Oracle 数据库，请在函数 `CONCAT_BLOB` 的定义后面插入一个斜杠 (/)。例如：

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

7. 让数据库管理员运行该 SQL 脚本，以创建并配置 User Application 数据库。
8. 重启动 Tomcat。

手动创建 SQL 文件以生成数据库纲要

您可以在安装后重新创建数据库表，而无需重新安装，也无需具有 SQL 文件。本节将帮助您在没有 SQL 文件的情况下创建数据库纲要。

1. 停止 Tomcat。
2. 登录到托管 Identity Applications 数据库的服务器。
3. 删除现有的数据库。

4 创建与您在步骤 3 中删除的数据库同名的新数据库。

5 在文本编辑器中，打开 NetIQ-Custom-Install.log 文件 （默认位于 Identity Applications 的安装根目录中）。例如：

```
/opt/netiq/idm/apps/UserApplication
```

6 在 NetIQ-Custom-Install.log 文件中搜索并复制以下命令：

```
/opt/netiq/common/jre/bin/java -Xms256m -Xmx256m  -
Dwar.context.name=IDMProv -Ddriver.dn="cn=User Application
Driver,cn=driverset1,o=system" -Duser.container="o=data" -jar /opt/
netiq/idm/apps/UserApplication/liquibase.jar --
databaseClass=liquibase.database.core.PostgresDatabase --
driver=org.postgresql.Driver --classpath=/opt/netiq/idm/apps/
postgresql/postgresql-9.4.1212jdbc42.jar opt/netiq/idm/apps/
UserApplication/IDMProv.war --changeLogFile=DatabaseChangeLog.xml  --
url="jdbc:postgresql://localhost:5432/idmuserappdb" --
contexts="prov,newdb" --logLevel=info --logFile=/opt/netiq/idm/apps/
UserApplication/db.out --username******** --password******** update
```

7 登录到安装了 Identity Applications 数据库的服务器。

8 在终端中，粘贴您复制的命令字符串。

注释：该命令应是 updateSQL。如果命令是 update，请将它更改为 updateSQL。

9 在该命令中，将表示数据库用户名和口令的星号 (*) 替换为进行鉴定所需的实际值。此外，请确保 SQL 文件名是唯一的。

10 执行该命令。

11 （视情况而定）如果进程生成了一个 SQL 文件而没有填充数据库，请向数据库管理员提供该文件，以将它导入数据库服务器。有关详细信息，请参见 “ 使用 SQL 文件生成数据库纲要 ”（第 124 页）。

12 在数据库管理员导入该 SQL 文件后，启动 Tomcat。

配置 Identity Applications 的单点登录设置

安装过程会安装用于在 Identity Manager 中进行单点登录访问的鉴定服务 (OSP)。不过，您也可以将 OSP 鉴定服务器配置为接受来自 Kerberos 票据服务器或 SAML 的鉴定。要在安装后配置 Identity Applications 的单点登录设置，请参见 《*NetIQ Identity Manager - Administrator's Guide to the Identity Applications*》（NetIQ Identity Manager - Identity Applications 管理员指南）中的 “Configuring Single Sign-on Access in Identity Manager”（在 Identity Manager 中配置单点登录访问）。

启动 Identity Applications

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

```
systemctl restart netiq-tomcat.service

systemctl restart netiq-activemq.service
```

Identity Applications 的配置和用法注意事项

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

- 在安装过程中，安装程序会将日志文件写入安装目录。这些文件包含有关您的配置的信息。配置 Identity Applications 环境后，应考虑删除这些日志文件或将其储存在安全位置。在安装过程中，可以选择将数据库纲要写入到文件。由于此文件包含有关数据库的描述性信息，因此在安装过程完成后应将文件移至安全位置。
- （视情况而定）要审计 Identity Applications，必须在环境中安装 Identity Reporting 和审计服务，并将其配置为捕获事件。此外，还必须配置 Identity Applications，以便能够进行审计。
- 只有在您完成以下活动之后，用户才能访问 Identity Applications：
  - 确保已安装所有必要的 Identity Manager 驱动程序。
  - 确保身份库的索引处于联机模式。有关在安装期间或之后配置索引的详细信息，请参见“ 创建身份库的值索引 ”（第 87 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。
- 如果您将 Identity Applications 和 SSPR 安装在不同的服务器上，则必须将 SSPR 可信证书导入到 Identity Applications 服务器的 `idm.jks` 中。

配置数据收集的运行时环境

本节提供为确保运行时环境正常运行而应执行的额外配置步骤的相关信息。此外，本节还提供了查错方法，以及具有特定用途的数据库表的一些信息。

此过程包括以下活动：

- “ 将数据收集服务驱动程序配置为从 Identity Applications 收集数据 ”（第 127 页）
- “ 迁移数据收集服务驱动程序 ”（第 128 页）
- “ 添加对自定义属性和对象的支持 ”（第 130 页）
- “ 添加多个驱动程序集支持 ”（第 132 页）
- “ 将驱动程序配置为使用 SSL 在远程模式下运行 ”（第 133 页）

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

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

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

注释：

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

---

1. 登录 Designer。
2. 在 Designer 中打开您的项目。
3. （视情况而定）如果您尚未将 DCS 驱动程序升级到支持的增补程序版本，请完成以下步骤：
   - **3a** 下载最新的 DCS 驱动程序增补程序文件。
   - **3b** 将该增补程序文件提取到服务器上的某个位置。
   - **3c** 在终端中，浏览到适用于您环境的增补程序 RPM 的提取位置，然后运行以下命令：

     ```
     rpm -Uvh novell-DXMLdcs.rpm
     ```

   - **3d** 重启动身份库。
   - **3e** 在 Designer 中，确保已安装支持版本的数据收集服务基础包。如果需要，请安装最新版本，然后再继续。有关软件要求的详细信息，请参见“ 安装 Identity Reporting 组件的注意事项 ”（第 54 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 Identity Reporting 的 IP 地址和端口。
10. 指定 SSO 服务客户端的口令。默认口令为 `driver`。
11. 单击**应用**，然后单击**确定**。
12. 在**建模器**视图中，右键单击 DCS 驱动程序，然后选择**驱动程序 > 部署**。
13. 单击**部署**。
14. 出现是否重启动 DCS 驱动程序的提示时，单击**是**。
15. 单击**确定**。

迁移数据收集服务驱动程序

要将对象同步到身份信息仓库中，您必须迁移数据收集服务驱动程序。

1 登录到 Identity Console。

2 在 **IDM 管理**磁贴中，选择“数据收集服务驱动程序”并转到**数据转换和同步**。

3 在数据同步视图中，选择**从身份库迁移**。

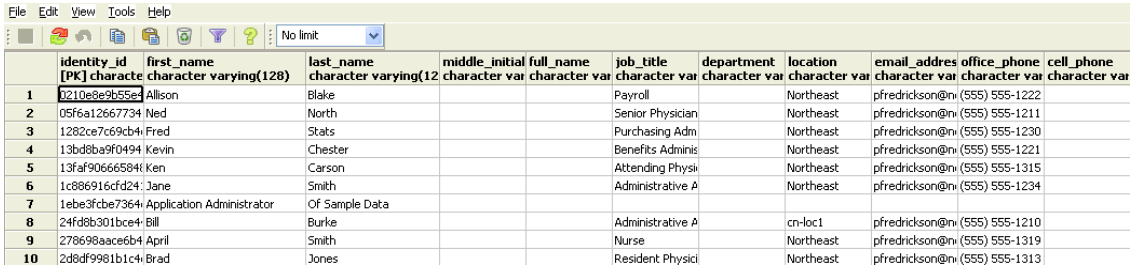
4 选择包含相关数据的组织，然后单击**启动**。

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。

---

5 等待迁移过程完成。

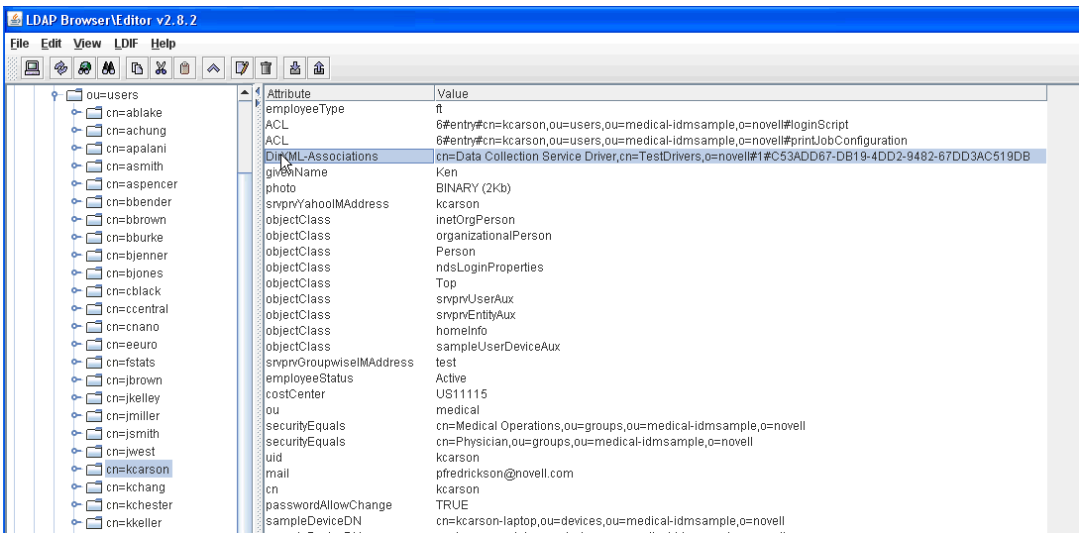
6 确保 **idmrpt_identity** 和 **idmrpt_acct** 表 （提供身份库中身份和帐户的相关信息）中包含以下类型的信息：



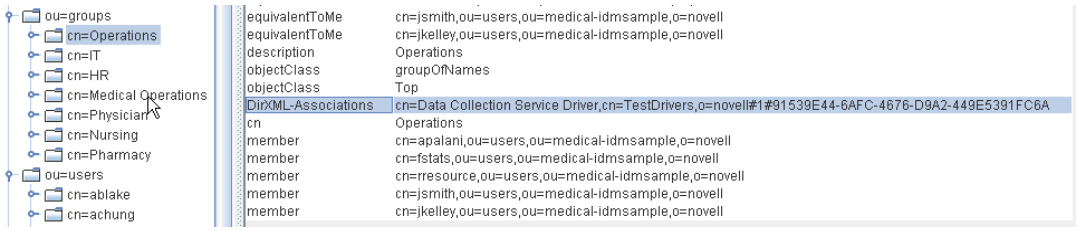
	identity_id [PK] characte	first_name character varying(128)	last_name character varying(12	middle_initial character var	full_name character var	job_title character var	department character var	location character var	email_addres character var	office_phone character var	cell_phone character var
1	0210e8e9b55e4	Allison	Blake			Payroll		Northeast	pfredrickson@n	(555) 555-1222	
2	05f6a12667734	Ned	North			Senior Physician		Northeast	pfredrickson@n	(555) 555-1211	
3	1282ce7c69cb4	Fred	Stats			Purchasing Adm		Northeast	pfredrickson@n	(555) 555-1230	
4	13bd8ba9f0494	Kevin	Chester			Benefits Adminis		Northeast	pfredrickson@n	(555) 555-1221	
5	13faf906665846	Ken	Carson			Attending Physi		Northeast	pfredrickson@n	(555) 555-1315	
6	1c886916cfd24	Jane	Smith			Administrative A		Northeast	pfredrickson@n	(555) 555-1234	
7	1ebe3fcbe7364	Application Administrator	Of Sample Data								
8	24fd8b301bce4	Bill	Burke			Administrative A		cn-loc1	pfredrickson@n	(555) 555-1210	
9	278698aace6b4	April	Smith			Nurse		Northeast	pfredrickson@n	(555) 555-1319	
10	2d8df9981b1c4	Brad	Jones			Resident Physici		Northeast	pfredrickson@n	(555) 555-1313	

7 在 LDAP 浏览器中，校验迁移过程是否添加了对 DirXML-Associations 的以下参照：

- 对于每个用户，校验是否包含以下类型的信息：



- 对于每个组，校验是否包含以下类型的信息：



8 确保 **idmrpt_group** 表中的数据看上去类似于以下信息：

group_name character var	group_desc character var	dynamic_gro boolean	dynamic_rule character var	nested_group boolean	idmrpt_valid_from timestamp without tin	idmrpt_deleted boolean	idmrpt_syn_state smallint
Pharmacy	Pharmacy	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
IT	Information Tec	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
HR	Human Resourc	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
Physician	Physician	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
Operations	Operations	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
Medical Operatic	Medical Operatic	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
Nursing	Nursing	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1

此表将显示每个组的名称，以及用于指出组是动态组还是嵌套组的标志。此外，它还会显示组是否已迁移。如果某个对象在 User Application 中已被修改但尚未迁移，则同步状态 (idmrpt_syn_state) 可能会设置为 0。例如，如果在组中添加了用户，并且尚未迁移驱动程序，那么，此值可能会设置为 0。

9 （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

10 （可选）校验 **idmrpt_ms_collect_state** 表现在是否包含行。该表显示有关受管系统网关驱动程序的数据收集状态信息。

此表包含有关为受管系统执行了哪些 REST 端点的数据。此时，该表不包含任何行，因为您尚未启动此驱动程序的收集过程。

添加对自定义属性和对象的支持

您可以对数据收集服务驱动程序进行配置，使其收集和保留不属于默认数据收集模式的自定义属性与对象的数据。为此，您需要修改数据收集服务驱动程序过滤器。修改过滤器不会立即触发对象同步，而是会在身份库中发生添加、修改或删除事件时，向数据收集服务发送新添加的属性和对象。

在添加对自定义属性和对象的支持时，您需要修改报告，以包括扩展的属性和对象信息。以下视图提供有关扩展对象和属性的当前数据与历史数据：

- idm_rpt_cfg.idmrpt_ext_idv_item_v
- idm_rpt_cfg.idmrpt_ext_item_attr_v

此过程包括以下活动：

- “ 将驱动程序配置为使用扩展对象 ”（第 130 页）
- “ 包含数据库中的名称和说明 ”（第 131 页）
- “ 向已知的对象类型添加扩展属性 ”（第 131 页）

将驱动程序配置为使用扩展对象

您可将任何对象或属性添加到数据收集服务过滤器策略中。在添加新对象或属性时，请务必按以下示例所示映射 GUID （subscriber 为 sync）和对象类 （subscriber 为 notify）：

```
<filter-class class-name="Device" publisher="ignore" publisher-create-
homedir="true" publisher-track-template-member="false" subscriber="sync">
<filter-attr attr-name="CN" merge-authority="default" publisher="ignore"
publisher-optimize-modify="true" subscriber="sync"/>
<filter-attr attr-name="Description" merge-authority="default"
publisher="ignore" publisher-optimize-modify="true" subscriber="sync"/>
<filter-attr attr-name="GUID" merge-authority="default" publisher="ignore"
publisher-optimize-modify="true" subscriber="sync"/>
<filter-attr attr-name="Object Class" merge-authority="default"
publisher="ignore" publisher-optimize-modify="true" subscriber="notify"/>
<filter-attr attr-name="Owner" merge-authority="default"
publisher="ignore" publisher-optimize-modify="true" subscriber="sync"/>
<filter-attr attr-name="Serial Number" merge-authority="default"
publisher="ignore" publisher-optimize-modify="true" subscriber="sync"/>
<filter-attr attr-name="sampleDeviceModel" from-all-classes="true" merge-
authority="default" publisher="ignore" publisher-optimize-modify="true"
subscriber="sync"/>
<filter-attr attr-name="sampleDeviceType" from-all-classes="true" merge-
authority="default" publisher="ignore" publisher-optimize-modify="true"
subscriber="sync"/>
</filter-class>
```

包含数据库中的名称和说明

如果您希望对象包含数据库中的名称和说明，则需要为 _dcsName 和 _dcsDescription 添加一个纲要映射策略。该纲要映射策略会将对象实例的相关属性值分别映射到 idmrpt_ext_idv_item.item_name 和 idmrpt_ext_idv_item.item_desc 列。如果您未添加纲要映射策略，属性将填充到子表 idmrpt_ext_item_attr 中。

例如：

```
<attr-name class-name="Device">
<nds-name>CN</nds-name>
<app-name>_dcsName</app-name>
</attr-name>
<attr-name class-name="Device">
<nds-name>Description</nds-name>
<app-name>_dcsDescription</app-name>
</attr-name>
```

下面是一个可显示数据库中这些对象和属性值的 SQL 示例：

```
SELECT
    item.item_dn,
    item.item_name,
    item.item_desc,
    attr.attribute_name,
    itemAttr.attribute_value,
    item.idmrpt_deleted as item_deleted,
    itemAttr.idmrpt_deleted as attr_deleted,
    item.item_desc,
    obj.object_class
FROM
    idm_rpt_data.idmrpt_ext_idv_item as item,
idm_rpt_data.idmrpt_ext_item_attr itemAttr, idm_rpt_data.idmrpt_ext_attr
as attr, idm_rpt_data.idmrpt_ext_obj as obj
WHERE
    item.object_id = obj.object_id and itemAttr.attribute_id =
attr.attribute_id and itemAttr.cat_item_id = item.item_id
ORDER BY
    item.item_dn, item.item_name
```

向已知的对象类型添加扩展属性

如果某个属性已添加到数据收集服务驱动程序的过滤器策略中，但未显式映射到 XML 参照文件 (`IdmrptIdentity.xml`) 中的报告数据库，则系统会在 idmrpt_ext_item_attr 表中填充并维护值，并在 idmrpt_ext_attr 表中添加一个属性参照。

下面的 SQL 示例显示了这些扩展属性：

```
SELECT
    acct.idv_acct_dn,
    attrDef.attribute_name,
    attribute_value,
    attrVal.idmrpt_valid_from,
    cat_item_attr_id,
    attrVal.idmrpt_deleted,
    attrVal.idmrpt_syn_state
FROM
    idm_rpt_data.idmrpt_ext_item_attr as attrVal,
idm_rpt_data.idmrpt_ext_attr as attrDef, idm_rpt_data.idmrpt_identity as
idd, idm_rpt_data.idmrpt_idv_acct as acct
WHERE attrVal.attribute_id = attrDef.attribute_id and idd.identity_id =
acct.identity_id and attrVal.cat_item_id = acct.identity_id and
cat_item_type_id = 'IDENTITY'
```

除了用户对象以外，您还可在以下对象的过滤器策略中添加扩展属性，并在数据库中填充这些属性：

- nrfRole
- nrfResource
- 容器

  注释：安装的产品将提供对 organizationUnit、 Organization 和 Domain 的支持。容器类型在 idmrpt_container_types 表中维护。

- 组
- nrfSod

您可以查看 idmrpt_cat_item_types.idmrpt_table_name 列，来了解扩展属性与父表或父对象之间的关联。此列描述如何将 idm_rpt_data.idmrpt_ext_item_attr.cat_item_id 列连接到父表的主键。

添加多个驱动程序集支持

数据收集服务范围包 (NOVLDCSSCPNG) 为包含多个驱动程序集和多组数据收集服务驱动程序及受管系统网关驱动程序的企业环境提供静态和动态范围功能。

在安装期间或安装之后，您需要确定要在其上安装该包的数据收集服务驱动程序的角色。您需要选择以下角色之一：

- **主要** 驱动程序将会同步所有信息，但其他驱动程序集的子树除外。主要数据收集服务驱动程序能够正常为整个身份库提供服务，或者可与一个或多个次要驱动程序配合工作。
- **次要** 驱动程序只同步自身的驱动程序集，而不同步其他任何信息。通常，次要数据收集服务驱动程序要求主要驱动程序在不同的驱动程序集中运行，否则，任何本地驱动程序集外部的数据都不会发送到数据收集服务。
- **自定义** 允许管理员自定义范围规则。唯一的隐式范围是本地驱动程序集，其他任何驱动程序如果未显式添加到自定义范围列表，都会被视为不在范围内。自定义范围是身份库中应该同步其从属或子树的容器的判别名 （采用斜杠格式）。

只有如下所述的某些配置情况才需要范围包：

- **单个服务器与具有单个驱动程序集的身份库：**对于此情况，您不需要定义范围，因此也就无需安装范围包。
- **多个服务器与具有单个驱动程序集的身份库：**对于此情况，您需要遵循以下指导原则：
  - 确保 Identity Manager 服务器存有要从中收集数据的所有分区的复本。
  - 对于此情况，您不需要定义范围，因此，请不要安装范围包
- **多个服务器与具有多个驱动程序集的身份库：**此情况有两种基本配置：
  - 所有服务器都存有要从中收集数据的所有分区的复本。

    对于此配置，您需要遵循以下指导原则：
    - 需要定义范围，以免有多个 DCS 驱动程序处理同一项更改。
    - 您需要在所有 DCS 驱动程序上安装范围包。
    - 您需要将一个 DCS 驱动程序选作主要驱动程序。
    - 您需要将其他所有 DCS 驱动程序配置为次要驱动程序。
  - 所有服务器都*未*存有要从中收集数据的所有分区的复本。

    此配置存在两种可能的情况：
    - 应从中收集数据的所有分区*仅由一个* Identity Manager 服务器存放

      在此情况下，您需要遵循以下指导原则：
      - 需要定义范围，以免有多个 DCS 驱动程序处理同一项更改。
      - 您需要在所有 DCS 驱动程序上安装范围包。
      - 您需要将所有 DCS 驱动程序都配置为主要驱动程序。
    - 应从中收集数据的所有分区*不是仅由一个* Identity Manager 服务器存放 （某些分区由多个 Identity Manager 服务器存放）。

      在此情况下，您需要遵循以下指导原则：
      - 需要定义范围，以免有多个 DCS 驱动程序处理同一项更改。
      - 您需要在所有 DCS 驱动程序上安装范围包。
      - 您需要将所有 DCS 驱动程序都配置为自定义驱动程序。

        您需要为每个驱动程序定义自定义范围规则，并务必不要创建任何重叠的范围。

将驱动程序配置为使用 SSL 在远程模式下运行

在以远程模式运行时，您可以将数据收集服务驱动程序和受管系统网关驱动程序配置为使用 SSL。本节提供有关将驱动程序配置为使用 SSL 在远程模式下运行的步骤。

要使用密钥存储区为受管系统网关驱动程序配置 SSL，请执行以下操作：

1 在 Identity Console 中创建服务器证书。

  1a 在 **eDirectory** 下，单击**证书管理 > 服务器证书管理**。

  1b 单击 **+** 图标，**创建服务器证书**选项卡随即出现

1c 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。

1d 指定证书昵称。

1e 选择**标准**创建方法，然后单击**下一步**。

1f 单击**完成**，然后单击**关闭**。

2 使用 Identity Console 导出服务器证书。

2a 在 **eDirectory** 下，单击**证书管理 > 服务器证书管理**。

2b 选择步骤 1 （第 133 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 134 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 Identity Console 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 **IDM 管理**中，单击包含受管系统网关驱动程序的驱动程序集。

4b 单击**受管系统网关驱动程序**图标并转到**配置**。

4c 单击**驱动程序参数**下拉菜单。

4d 在**驱动程序设置**选项卡下，设置要显示的**连接参数**，并将**驱动程序配置模式**设置为 “ 远程 ”。

4e 输入密钥存储区文件的完整路径和口令。

4f 保存并重启动驱动程序。

5 使用 Identity Console 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 **IDM 管理**中，单击包含数据收集服务驱动程序的驱动程序集。

5b 单击**数据收集服务驱动程序**图标并转到**驱动程序配置**。

5c 单击**驱动程序参数**下拉菜单，并设置要显示的**注册参数**。

5d 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 ”。

5e 输入密钥存储区的完整路径、口令以及在步骤 1d （第 134 页）中指定的别名。

5f 保存并重启动驱动程序。

配置 Identity Reporting

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

如果使用配置工具更改了 Identity Reporting 的任何设置，您必须重启动 Tomcat 才能使更改生效。但是，在 Identity Reporting 的 Web 用户界面中进行更改后，则不需要重启动服务器。

- “ 配置受管系统网关驱动程序 ”（第 135 页）
- “ 在 “ 身份数据收集服务 ” 页面中手动添加数据源 ”（第 135 页）
- “ 对 Oracle 数据库运行报告 ”（第 136 页）
- “ 手动生成数据库纲要 ”（第 136 页）
- “ 部署 Identity Reporting 的 REST API”（第 141 页）
- “ 连接远程 Remote PostgreSQL 数据库 ”（第 141 页）
- “ 在 OSP 中为采用分布式设置的 Identity Reporting 注册客户端 ”（第 142 页）
- “Identity Reporting 的安装后步骤 ”（第 142 页）

配置受管系统网关驱动程序

安装程序将为 Identity Reporting 创建并配置数据收集服务驱动程序和受管系统网关驱动程序。

配置受管系统网关驱动程序后， NetIQ 建议您将 KMO 修改为 **SSL EC 证书 DNS**。要修改 KMO，请执行以下步骤：

1. 登录到 Identity Console。
2. 在 **IDM 管理**中，单击包含受管系统网关驱动程序的驱动程序集。
3. 单击**受管系统网关驱动程序**图标并转到**驱动程序配置**。
4. 在**配置**选项卡中，单击**驱动程序参数**下拉菜单并执行以下步骤：
   - **4a** 从**显示连接参数**字段中选择显示。
   - **4b** 在 **KMO 名称**字段中，将值从 **SSL CertificateDNS** 更改为 **SSL EC 证书 DNS**。
   - **4c** 依次单击**应用**、**确定**。

在 “ 身份数据收集服务 ” 页面中手动添加数据源

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

对 Oracle 数据库运行报告

Identity Reporting 可让您针对远程 Oracle 数据库运行报告。确保运行 Oracle 数据库的服务器上存在 `ojbc8.jar` 文件。

手动生成数据库纲要

要在安装后手动生成数据库纲要，请对您的数据库执行下列过程之一：

- “ 针对 PostgreSQL 数据库配置 Create_rpt_roles_and_schemas.sql 纲要 ”（第 136 页）
- “ 针对 Oracle 数据库配置 Create_rpt_roles_and_schemas.sql 纲要 ”（第 137 页）
- “ 针对 MS SQL 数据库配置 Create_rpt_roles_and_schemas.sql 纲要 ”（第 139 页）
- “ 清除数据库校验和 ”（第 139 页）
- “ （可选）增加列数据大小 ”（第 140 页）

针对 PostgreSQL 数据库配置 Create_rpt_roles_and_schemas.sql 纲要

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

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

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

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

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

   Select CREATE_RPT_ROLES_AND_SCHEMAS('password2');
   ```

6. 将 `/opt/netiq/idm/apps/IDMReporting/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这些命令。

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

针对 Oracle 数据库配置 Create_rpt_roles_and_schemas.sql 纲要

1 以数据库管理员 (sysdba) 用户身份登录到 SQL Developer。

2 创建 Create_rpt_roles_and_schemas，方法是将以下 SQL 内容复制到 SQL Developer，并针对连接的数据库执行这些代码：

```
alter session set "_ORACLE_SCRIPT"=true;

CREATE OR REPLACE PROCEDURE create_rpt_roles_and_schemas(
   idm_rpt_cfg_password character varying)
AUTHID CURRENT_USER
AS
   cnt number;
BEGIN
   /* Create user IDM_RPT_CFG if it does not exist */
   select count(*) into cnt from ALL_USERS WHERE USERNAME =
'IDM_RPT_CFG';
   IF cnt = 0 THEN
       execute immediate 'CREATE USER idm_rpt_cfg IDENTIFIED BY ' ||
idm_rpt_cfg_password;
       DBMS_OUTPUT.put_line('Created user idm_rpt_cfg');
   END IF;

   /* Grant rights to the idm_rpt_cfg user */
   execute immediate 'GRANT CREATE SESSION, CREATE TABLE, CREATE VIEW,
CREATE PROCEDURE, CREATE SEQUENCE, CREATE TRIGGER, UNLIMITED TABLESPACE
to idm_rpt_cfg';
   DBMS_OUTPUT.put_line('Granted rights to user idm_rpt_cfg');
   execute immediate 'alter session set "_ORACLE_SCRIPT"=true';
   execute immediate 'alter session set "_ORACLE_SCRIPT"=false';
END;
/
exec CREATE_RPT_ROLES_AND_SCHEMAS('Novell123');
/
alter session set "_ORACLE_SCRIPT"=false;
/
```

3 以系统用户身份登录到 SQL Developer，然后创建 Create_dcs_roles 和纲要，方法是将以下 SQL 内容复制到 SQL Developer，并针对连接的数据库执行这些代码：

```
alter session set "_ORACLE_SCRIPT"=true;

CREATE OR REPLACE PROCEDURE create_dcs_roles_and_schemas(
   idm_rpt_data_password character varying,
   idmrptuser_password character varying)
AUTHID CURRENT_USER
AS
   cnt number;
BEGIN
/* Create user IDM_RPT_DATA if it does not exist already */
   select count(*) into cnt from ALL_USERS WHERE USERNAME =
'IDM_RPT_DATA';
   IF cnt = 0 THEN
       execute immediate 'CREATE USER idm_rpt_data IDENTIFIED BY ' ||
```

```
idm_rpt_data_password;
       DBMS_OUTPUT.put_line('Created user idm_rpt_data');
   END IF;

   /* Grant rights to the idm_rpt_data user */
   execute immediate 'GRANT CREATE SESSION, CREATE TABLE, CREATE VIEW,
CREATE PROCEDURE, CREATE SEQUENCE, CREATE TRIGGER, UNLIMITED TABLESPACE
to idm_rpt_data';
   execute immediate 'GRANT CREATE PUBLIC SYNONYM to IDM_RPT_DATA';
   execute immediate 'GRANT SELECT ON DBA_SEGMENTS TO IDM_RPT_DATA';
   DBMS_OUTPUT.put_line('Granted rights to user idm_rpt_data');
   /* Create user IDMRPTUSER if it does not exist */
   select count(*) into cnt from ALL_USERS WHERE USERNAME =
'IDMRPTUSER';
   IF cnt = 0 THEN
       execute immediate 'CREATE USER idmrptuser IDENTIFIED BY ' ||
idmrptuser_password;
       DBMS_OUTPUT.put_line('Created user idmrptuser');
   END IF;

   /* Grant rights to the idmrptuser user */
   execute immediate 'GRANT CREATE SESSION to idmrptuser';
   execute immediate 'GRANT SELECT ON sys.all_tables TO idmrptuser';
   DBMS_OUTPUT.put_line('Granted rights to user idmrptuser');
END;
/
```

4 要创建 IDM_RPT_CFG 角色，请执行以下命令：

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

例如，如果 IDM_RPT_CFG 的口令是 password，则您必须执行以下命令：

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

5 指派以下许可权限：

```
GRANT CREATE PUBLIC SYNONYM to IDM_RPT_CFG;
```

6 将 /opt/netiq/idm/apps/IDMReporting/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这些命令。

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

针对 MS SQL 数据库配置 Create_rpt_roles_and_schemas.sql 纲要

1 执行 delete_create_dcs_roles_and_schemas-mssql.sql 和 delete_get_formatted_user_dn-mssql.sql。

2 使用 /opt/netiq/idm/apps/IDMReporting/sql/ 中的 create_dcs_roles_and_schemas.mssql 和 create_rpt_roles_and_schemas.mssql，将所需的角色添加到数据库。

3 以数据库管理员用户身份登录 SQL Developer。

4 要创建 Create_rpt_roles_and_schemas 和 Create_dcs_roles_and_schemas 过程，请将 create_dcs_roles_and_schemas.mssql 和 create_rpt_roles_and_schemas.mssql 中的内容复制到 SQL Developer，然后对连接的数据库执行这些命令。

5 要创建 IDM_RPT_DATA、 IDM_RPT_CFG 和 IDMRPTUSER 角色，请按给定的顺序执行以下命令：

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

execute CREATE_RPT_ROLES_AND_SCHEMAS \'<Set pwd for IDM_RPT_CFG>\'
```

6 将 /opt/netiq/idm/apps/IDMReporting/sql/ 中 get_formatted_user_dn.sql 的内容复制到 SQL Developer，然后对连接的数据库执行这些命令。

清除数据库校验和

1 在 /opt/netiq/idm/apps/IDMReporting/sql 中找到以下 .sql 文件。

- DbUpdate-001-run-as-idm_rpt_data.sql
- 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
go
```

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:@192.168.0.1:1521/orcl
-- Liquibase version: 3.5.1
--
**********************************************************************
**
update databasechangelog set md5sum = null
go
```

2b 以相应的用户身份运行每个 `.sql`。

3 将更改提交到数据库。

（可选）增加列数据大小

在 Identity Manager 的先前版本中，因为字符数限制，长数据字段无法与 Identity Reporting 服务器进行数据同步。 Identity Manager 4.9 提供了一个选项，可提高 PostgreSQL、 Oracle 和 MS SQL 数据库中下列表及其相应列的字符数限制：

表名称	列名称
idm_rpt_data.idmrpt_idv_ent_bindings	ent_param_str
idm_rpt_data.idmrpt_idv_ent_bindings	ent_param_val
idm_rpt_data.idmrpt_idv_identity_trust	idv_ent_ref
idm_rpt_data.idmrpt_idv_identity_trust	trust_params
idm_rpt_data.idmrpt_idv_ent_bindings_hist	ent_param_str
idm_rpt_data.idmrpt_idv_ent_bindings_hist	ent_param_val
idm_rpt_data.idmrpt_idv_identity_trust_hist	idv_ent_ref
idm_rpt_data.idmrpt_idv_identity_trust_hist	trust_params

- 对于 PostgreSQL，Identity Manager 4.9 中已自动为上表中所述的所有字段提高了字符数限制。
- 对于 Oracle，您必须从 `/opt/netiq/idm/apps/IDMReporting/sql/` 目录运行 `alter_column_length-oracle.sql` 脚本，以提高上表中所述的所有列的字符数限制。
- 对于 MS SQL，您必须从 `/opt/netiq/idm/apps/IDMReporting/sql/` 目录运行 `alter_column_length-mssql.sql` 脚本，以仅提高已编入索引的列的字符数限制。在此例中， `ENT_PARAM_STR` 是表 `idmrpt_idv_ent_bindings` 中唯一编入索引的列。

部署 Identity Reporting 的 REST API

Identity Reporting 在报告功能中整合了多个用于实现不同功能的 REST API。这些 REST API 使用 OAuth2 协议进行鉴定。

在 Tomcat 上，系统会在安装 Identity Reporting 时自动部署 `rptdoc war` 和 `dcsdoc war`。

连接远程 Remote PostgreSQL 数据库

如果您的 PostgreSQL 数据库安装在单独的服务器上，则需要在该远程数据库的 `postgresql.conf` 和 `pg_hba.conf` 文件中更改默认设置。

1 在 `postgresql.conf` 文件中更改侦听地址。

默认情况下， PostgreSQL 允许侦听 localhost 连接，不允许远程 TCP/IP 连接。要允许远程 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 = '*'
```

如果服务器上有多个接口，可以指定要侦听的特定接口。

2 将客户端鉴定条目添加到 `pg_hba.conf` 文件中。

默认情况下， PostgreSQL 只接受来自 `localhost` 的连接。它会拒绝远程连接。这通过应用访问控制规则来控制，该规则允许用户在提供有效口令 （md5 关键字）后从某个 IP 地址登录。要接受远程连接，请将下面的条目添加到 `/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 重启动远程 PostgreSQL 服务器。

3b 使用用户名和口令远程登录服务器。

在 OSP 中为采用分布式设置的 Identity Reporting 注册客户端

1 导航到 OSP 的安装位置，编辑 `configupdate.sh.properties` 文件中的以下项：

```
app_versions="ua#<version>,rpt#<version>"
sso_apps=ua,rpt
```

示例：

```
app_versions="ua#4.9.0,rpt#7.2.0"
sso_apps=ua,rpt
```

2 起动 configupdate，在以下字段中更新 Identity Reporting 的客户端细节：

- 报告客户端
- 数据收集服务
- DCS 驱动程序

3 重启动 OSP 的 tomcat。

Identity Reporting 的安装后步骤

如果在安装期间针对 “ 创建 Identity Reporting 的纲要 ” 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。

另外，请在启动一次 Tomcat 后再重启动一次，以确保可用数据库正常运行。

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。

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 用户安装过程不会为口令策略创建容器。

1 登录到 Identity Console 并转到**树视图**。

2 导航到身份库中的安全性容器。

3 为口令策略创建容器。

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 重启动身份库。

激活 Identity Manager

您无需提供激活代码就能安装或初始运行 Identity Manager。但是，如果未提供激活代码，Identity Manager 将在安装完成 90 天后停止运行。在这 90 天内或者 90 天后，您随时可以激活 Identity Manager。有关详细信息，请参见《*NetIQ Identity Manager Overview and Planning Guide*》（NetIQ Identity Manager 概述和规划指南）中的“Activating Identity Manager”（激活 Identity Manager）。

为分布式部署创建 SSL 证书

以下过程说明如何为分布式部署创建 SSL 证书：

1 运行以下命令设置 Java 路径：

```
export PATH=/opt/netiq/common/jre/bin:$PATH
```

确保已在服务器上设置 Java 路径。例如：

```
export PATH=/opt/netiq/common/jre/bin/:$PATH
```

2 创建一个示例工作目录。

```
mkdir -p /opt/certs
```

3 生成 PKCS 密钥存储区：

```
keytool -genkey -alias < alias_name > -keyalg RSA -keystore <absolute
path of keystore > -validity 3650 -keysize 1024 -dname "CN=<Subject
Alternate Name>" -keypass <keypass> -storepass <storepass>
```

4 生成 CSR （证书签名请求）：

```
keytool -certreq -v -alias < alias_name >  -file < name of the csr file
> -keypass < keypass >  -keystore < absolute path of the keystore >  -
storepass < storepass >
```

5 生成自我签名证书：

5a 起动 Identity Console 并登录。

5b 导航到**证书管理** > **颁发证书**。

5c 浏览到在步骤 3 中创建的 `.csr` 文件。例如 `ua.csr`。

5d 单击**打开**。

5e 在**密钥使用规范**下拉列表中指定密钥类型。

5f 在**扩展密钥使用规范**下拉列表中指定扩展密钥类型。

5g 对于证书类型，请在**基本约束**下拉列表中选择**未指定**。

5h 在**证书参数**下拉列表中指定证书的有效期。

5i 在**证书格式**下拉列表中选择**采用二进制 DER 格式的文件**。

5j 单击**下一步**。

5k 单击**确定**。

5l 下载证书并将其复制到 `/data` 目录。

6 导出 `.der` 格式的根证书：

6a 起动 Identity Console 并登录。

6b 导航到**证书管理** > **服务器证书管理**。

6c 选中 **SSL 证书 DNS** 复选框并单击**导出**。

6d 在**证书**下拉列表中选择 “ 组织 CA”。

6e 在**导出格式**下拉列表中选择 `DER`。

6f 单击**确定**。

6g 下载证书并将其复制到 /data 目录。

7 将证书导入到前面所述的 PKCS 密钥存储区。

```
keytool -import -trustcacerts -alias root -keystore <name of the
keystore> -file <root certificate > -storepass <password> -noprompt
```

例如：

```
keytool -import -alias <alias name> -keystore <name of the keystore> -
file <self-signed certificate> -storepass <password> -noprompt
```

8 针对 osp，userapp 和 reporting （如果它们在不同的计算机中使用）重复上述过程。

IV 在 FIPS 模式下配置 Identity Manager

Identity Manager 利用符合联邦信息处理标准 (FIPS) 的功能来满足美国联邦机构与客户对高度安全环境的安全要求。FIPS 140-2 标准用于监管加密软件的实施和通讯。Bouncy Castle 使用一个通过了 FIPS 140-2 Level 1 认证的开源 JCA 提供程序。该提供程序是基于成熟且知名的 Bouncy Castle 开源加密提供程序构建的。

注释：

- SSPR 不支持 FIPS 模式。您必须将非 FIPS SSPR 设置迁移到另一台服务器。有关详细信息，请参见《*Self Service Password Reset 4.7 Administration Guide*》（Self Service Password Reset 4.7 管理指南）中的 “Backing Up Configuration Information”（备份配置信息）和 “Importing Configuration Information”（导入配置信息）。
- 确保主密钥储存区口令与 tomcat 密钥储存区口令相同。要更改口令，请查看 “ 储存 Configupdate 实用程序口令 ”（第 97 页）。

本部分介绍如何在 FIPS 模式下配置和操作 Identity Manager。

- 第 7 章 “ 为 FIPS 配置 JRE”（第 149 页）
- 第 8 章 “ 在 FIPS 模式下配置 Identity Manager 引擎 ”（第 151 页）
- 第 9 章 “ 在 FIPS 模式下配置扇出代理 ”（第 153 页）
- 第 10 章 “ 在 FIPS 模式下配置 Identity Applications 和 Identity Reporting”（第 155 页）
- 第 11 章 “ 在 FIPS 模式下配置 Remote Loader”（第 159 页）

7 为 FIPS 配置 JRE

要为 BCFIPS 仅批准模式配置 JRE，请执行以下操作：

1 将 BCFIPS.jar 文件添加到 Java 类路径。

所需的 BCFIPS 文件如下：

- bc-fips-1.0.2.4.jar
- bcpkix-fips-1.0.7.jar
- bctls-fips-1.0.18.jar

2 修改 <jre 根目录 >/conf/security 目录下的 java.security 文件，并设置 BCFIPS 定义的 Java 系统属性。

在文本编辑器中，从 <jre 根目录 >/conf/security/java.security 打开托管 Web 容器的 JRE 的上述文件。找到安全提供程序列表，注释掉所有现有提供程序，然后如下所示替换文件中的项：

- security.provider.1=BCFIPS
- security.provider.2=BCJSSE
- security.provider.3=SunJSSE
- security.provider.4=SUN
- security.provider.5=SunJCE

必须指定 SunJSSE 提供程序 (Java 11)，因为 OSP 在初始化其可信证书存储区时需要特定的 TrustManager 实现。除了对安全提供程序进行更改之外，还必须使用 BCFIPS JSSE KeyManager 实现。这种必要性主要是因为 Sun 实现中存在缺陷，导致无法在一定程度上做到 FIPS 在密钥方面要求的确定性。为此，请将 java.security 中的以下行：

```
ssl.KeyManagerFactory.algorithm=SunX509
```

替换成

```
ssl.KeyManagerFactory.algorithm=PKIX
```

另外，最好禁用较旧的 SSL 和 TLS 算法。这是因为， TLS v2.0 之前的 SSL/TLS 版本所需的算法在 BCFIPS 已批准模式下不可用。要禁用旧算法，请找到 jdk.tls.disabledAlgorithms 项。例如：

```
jdk.tls.disabledAlgorithms=SSLv3, RC4, MD5withRSA, DH keySize < 1024, \ EC
keySize < 224, DES40_CBC, RC4_40, 3DES_EDE_CBC
```

将 TLSv1 和 TLSv1.1 添加到列表中：

```
jdk.tls.disabledAlgorithms=SSLv3, TLSv1, TLSv1.1, RC4, MD5withRSA, DH
keySize < 1024, \ EC keySize < 224, DES40_CBC, RC4_40, 3DES_EDE_CBC
```

禁用 TLSv1 和 TLSv1.1 不是强制要求，但这样可以避免在 OSP 尝试安全连接到仅支持 TLS v1.1 或更低版本的服务 （例如 LDAP）时出现不明所以的错误讯息。禁用较低 TLS 版本后出现的错误讯息更容易理解，并且可以直接指明问题所在。

注释：eDirectory 8.8 （或更低版本）无法与安全 LDAP 一起使用，因为它仅支持 TLS v1.0。如果要使用安全 LDAP，则必须使用 eDirectory 9 或更高版本。另一种做法是修改默认的密钥存储区类型。找到 `keystore.type=jks` 或 `keystore.type=pkcs12` 行，将其更改为 `keystore.type=bcfks`。

---

8 在 FIPS 模式下配置 Identity Manager 引擎

在 Identity Manager 引擎上配置 FIPS 模式之前，应考虑先完成以下准备工作：

- 要启用安全性增强，请将以下 jar 文件放入 `/opt/netiq/common/jre/lib/` 目录：
  - `bc-fips-1.0.2.4.jar`
  - `bcpkix-fips-1.0.7.jar`
  - `bctls-fips-1.0.18.jar`

  注释：您可以从以下 maven 储存库下载上述 jar 文件：
  - bc-fips (https://mvnrepository.com/artifact/org.bouncycastle/bc-fips)
  - bcpkix-fips (https://mvnrepository.com/artifact/org.bouncycastle/bcpkix-fips)
  - bctls-fips (https://mvnrepository.com/artifact/org.bouncycastle/bctls-fips)
- 要启用对上述 `.jar` 文件的许可权限，请运行以下命令：

  ```
  chown novlua:novlua <jar-file>
  chmod 755 <jar-file>
  ```
- 要设置环境变量，请运行以下命令：

  ```
  export IS_FIPS_ENABLED=true
  export BC_FIPS_VERSION=1.0.2.4
  export JAVA_OPTS =" -Dorg.bouncycastle.fips.approved_only=true  -Dorg.bouncycastle.rsa.allow_multi_use=true"
  export CLASSPATH=/opt/netiq/common/jre/lib/bc-fips-1.0.2.4.jar
  ```

  设置完成后，可以使用 `echo` 命令校验所有环境变量。

注释：要通过端口 636 访问 `dxcmd`，请在 LDAP 设置中启用 SSL EC 证书。

操作步骤

1. 导航到 `/opt/netiq/common/jre/conf/security/` 目录。
2. 备份 `java.security` 文件。
3. 执行以下步骤来编辑 `java.security` 文件：

   3a 搜索字符串 `List of providers and their preference orders`，注释掉所有现有提供程序，然后添加以下项：

```
security.provider.1=BCFIPS
security.provider.2=BCJSSE
security.provider.3=SunJSSE
security.provider.4=SUN
security.provider.5=SunJCE
```

3b 搜索字符串 `ssl.KeyManagerFactory.algorithm=SunX509`，将其注释掉，然后添加以下项：

```
ssl.KeyManagerFactory.algorithm=PKIX
```

3c 搜索字符串 `keystore.type`，将其注释掉，然后添加以下项：

```
keystore.type=bcfks
```

4 导航到 `/opt/netiq/common/jre/lib/security/` 目录。

5 备份 `cacerts` 文件。

6 为了支持安全性增强，请使用以下命令将 `cacerts` 文件转换为 `bcfks` 格式：

```
keytool -importkeystore -srckeystore cacerts -srcstorepass changeit -
srcstoretype JKS -destkeystore cacerts -deststorepass changeit -
deststoretype BCFKS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
$CLASSPATH
```

生成 `cacerts_bcfks` 文件后，删除原来的 `cacerts`。将 `cacerts_bcfks` 重命名为 `cacerts`。

7 登录到 Identity Console。

8 转到 **IDM Administrator**，单击驱动程序集的 操作菜单。

9 导航到**驱动程序集属性 > 驱动程序集配置 > Java 环境参数**。

10 在 **JVM 选项**中输入以下内容：

```
Djavax.net.ssl.trustStore=/opt/netiq/common/jre/lib/security/cacerts -
Djavax.net.ssl.trustStorePassword=changeit -
Djavax.net.ssl.trustStoreType=BCFKS
```

11 单击 **保存**按钮。

12 重启动 eDirectory。

9 在 FIPS 模式下配置扇出代理

在 Identity Manager 扇出代理上配置 FIPS 模式之前，应考虑先完成以下准备工作：

- 在未启用安全性增强的情况下，启动扇出代理，并在 `config` 文件夹中生成密钥存储区文件。
- 将以下 jar 文件放入 `/opt/novell/dirxml/fanoutagent/lib/` 目录：
  - `bc-fips-1.0.2.4.jar`
  - `bcpkix-fips-1.0.7.jar`
  - `bctls-fips-1.0.18.jar`
- 要启用对上述 `.jar` 文件的许可权限，请运行以下命令：

  ```
  chown root:bin <jar-file>
  ```

  ```
  chmod 755 <jar-file>
  ```

- 要设置环境变量，请运行以下命令：

  ```
  export IS_FIPS_ENABLED=true
  ```

  ```
  export BC_FIPS_VERSION=1.0.2.4
  ```

  ```
  export JAVA_OPTS =" -Dorg.bouncycastle.fips.approved_only=true  -
  Dorg.bouncycastle.rsa.allow_multi_use=true"
  ```

  ```
  export CLASSPATH=/opt/novell/dirxml/fanoutagent/lib/bc-fips-1.0.2.4.jar
  ```

  设置完成后，可以使用 `echo` 命令校验所有环境变量。

操作步骤

1. 导航到 `/opt/netiq/common/jre/conf/security/` 目录。
2. 备份 `java.security` 文件。
3. 执行以下步骤来编辑 `java.security` 文件：

   3a 搜索字符串 `List of providers and their preference orders`，注释掉所有现有提供程序，然后添加以下项：

   ```
   security.provider.1=BCFIPS
   security.provider.2=BCJSSE
   security.provider.3=SunJSSE
   security.provider.4=SUN
   security.provider.5=SunJCE
   ```

   3b 搜索字符串 `ssl.KeyManagerFactory.algorithm=SunX509`，将其注释掉，然后添加以下项：

```
ssl.KeyManagerFactory.algorithm=PKIX
```

3c 搜索字符串 `keystore.type`，将其注释掉，然后添加以下项：

```
keystore.type=bcfks
```

4 导航到 `/opt/netiq/common/jre/lib/security/` 位置：

5 备份 `cacerts` 文件。

6 为了支持安全性增强，请使用以下命令将 `cacerts` 文件转换为 `bcfks` 格式：

```
keytool -importkeystore -srckeystore cacerts -srcstorepass changeit -
srcstoretype JKS -destkeystore cacerts -deststorepass changeit -
deststoretype BCFKS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
$CLASSPATH
```

7 要将密钥存储区文件从 `jks` 格式转换为 `bcfks` 格式，请运行以下命令：

```
keytool -importkeystore -srckeystore /opt/novell/dirxml/fanoutagent/
config/keystore.jks -srcstorepass changeit -srcstoretype PKCS12 -
destkeystore /opt/novell/dirxml/fanoutagent/config/keystore.jks -
deststorepass changeit -deststoretype BCFKS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
$CLASSPATH
```

8 导航到 `/opt/novell/dirxml/fanoutagent/bin/` 目录，在 `startAgent.sh` 文件中进行以下更改：

```
${JAVA} --add-opens=java.base/sun.security.internal.spec=ALL-UNNAMED -
Djavax.net.ssl.trustStore=/opt/netiq/common/jre/lib/security/cacerts -
Djavax.net.ssl.trustStorePassword=changeit -Dkeystore.type=BCFKS -
Dorg.bouncycastle.fips.approved_only=true -
Dorg.bouncycastle.rsa.allow_multi_use=true -cp ${CLASS_PATH}
com.netiq.idm.fanoutagent.FanoutAgent $filename $SERVERONLY &
```

9 使用以下命令启动扇出代理：

```
./startAgent
```

10 在 FIPS 模式下配置 Identity Applications 和 Identity Reporting

在 Identity Manager Reporting 和 Identity Applications 上配置 FIPS 模式之前，应考虑先完成以下准备工作：

- 在托管 Identity Applications 和 Identity Manager Reporting 组件的服务器上停止 Tomcat 服务。
- 校验管理员是否可以登录到 Identity Manager 引擎系统上的 `dxcmd` 工具。

操作步骤

1. 为 FIPS 创建一个新文件夹。例如 `/home/fips`
2. 在创建的文件夹中备份以下文件：

文件	现有文件路径
`idm.jks`	`/opt/netiq/idm/apps/tomcat/conf`
`tomcat.ks`	
`encrypt-keys.pkcs12`	
`server.xml`	
`ism-configuration.properties`	
`configupdate.sh`	`/opt/netiq/idm/apps/configupdate`
`configupdate.bat.properties`	

3. 导航到 `/mnt/osp/packages/misc/` 目录，并将 `osp-tomcat8-pwd-handler-<` 版本 `>.jar` 复制到 `/opt/netiq/idm/apps/tomcat/lib` 目录。
4. 导航到 `/opt/netiq/idm/apps/tomcat/bin/` 目录，并如下所示编辑 `setenv.sh` 文件：
   - `JAVA_OPTS= -Dorg.bouncycastle.fips.approved_only=true -Dinternal.osp.framework.fips-password=novell -Dorg.bouncycastle.rsa.allow_multi_use=true -Djavax.net.ssl.keyStoreType=BCFKS -Djavax.net.ssl.trustStoreType=BCFKS -Djavax.net.ssl.trustStore=/opt/netiq/idm/apps/tomcat/conf/idm.bcfks -Djavax.net.ssl.trustStorePassword=novell`
   - `BCFIPS_JARS=/opt/netiq/common/jre/lib/bc-fips-1.0.2.4.jar:/opt/netiq/common/jre/lib/bcpkix-fips-1.0.7.jar:/opt/netiq/common/jre/lib/bctls-fips-1.0.18.jar`

- export CLASSPATH="${BCFIPS_JARS}"
- 搜索 CATALINA_OPTS，将 encrypt-keys.pkcs12 更改为 encrypt-keys.bcfks，并将 storetype 更改为 bcfks

5 导航到 /opt/netiq/idm/apps/tomcat/conf/ 目录，并运行以下命令：

```
keytool -importkeystore -srckeystore idm.jks -srcstorepass novell -
srcstoretype PKCS12 -destkeystore idm.bcfks -deststorepass novell -
deststoretype BCFKS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
$CLASSPATH

keytool -importkeystore -srckeystore tomcat.ks -srcstorepass novell -
srcstoretype PKCS12 -destkeystore tomcat.bcfks -deststorepass novell -
deststoretype BCFKS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
$CLASSPATH

keytool -importkeystore -srckeystore idm.jks -srcstorepass novell -
srcstoretype PKCS12 -destkeystore /opt/netiq/idm/apps/osp/osp.bcfks -
deststorepass novell -deststoretype BCFKS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
$CLASSPATH

keytool -importkeystore -srckeystore tomcat.ks -srcstorepass novell -
srcstoretype PKCS12 -destkeystore /opt/netiq/idm/apps/osp/osp.bcfks -
deststorepass novell -deststoretype BCFKS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
$CLASSPATH --noprompt

java -jar <mount-location>/osp/packages/misc/osp-keymanager-6.7.1.jar -
genkeys -keystore /opt/netiq/idm/apps/osp/osp.bcfks -storepass novell -
storetype BCFKS -application idm -providerClass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerPath
$CLASSPATH -keypass novell -use Encrypting,Signing,TLS

keytool -importkeystore -srckeystore encrypt-keys.pkcs12 -srcstorepass
changeit -srcstoretype PKCS12 -destkeystore encrypt-keys.bcfks -
deststorepass changeit -deststoretype BCFKS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
$CLASSPATH
```

6 如下所示编辑 server.xml 文件：

```
<!--Connector port="8543"
protocol="org.apache.coyote.http11.Http11NioProtocol" maxThreads="150"
SSLEnabled="true" scheme="https" secure="true" clientAuth="false"
sslProtocol="TLSv1.2" keystoreFile="conf/tomcat.ks"
keystorePass="novell" maxHttpHeaderSize="65536"
sslEnabledProtocols="TLSv1.2" /-->

<Connector
protocol="com.microfocus.osp.tomcat.http.PasswordHttp11NioProtocol"
port="8543" maxThreads="150" maxHttpHeaderSize="65536"
SSLEnabled="true" scheme="https" secure="true">
<SSLHostConfig protocol="TLS" protocols="TLSv1.2"
ciphers="TLS_DHE_DSS_WITH_AES_128_GCM_SHA256,TLS_DHE_DSS_WITH_AES_256_
GCM_SHA384,TLS_DHE_DSS_WITH_AES_128_CBC_SHA256,TLS_DHE_DSS_WITH_AES_12
8_CBC_SHA,TLS_DHE_DSS_WITH_AES_256_CBC_SHA256,TLS_DHE_DSS_WITH_AES_256
_CBC_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_
GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_ECDSA_WIT
H_AES_128_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_EC
DSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECD
HE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_
ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA
_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_128_CCM,TLS_RSA_WITH_AES_256
_CCM,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_
RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA"
truststoreFile="/opt/netiq/idm/apps/osp/osp.bcfks"
truststorePassword="novell" truststoreType="BCFKS" > <Certificate
certificateKeystoreFile="/opt/netiq/idm/apps/tomcat/conf/tomcat.bcfks"
certificateKeystorePassword="novell" certificateKeyAlias="ssl
certificatedns" certificateKeystoreType="BCFKS" />
</Certificate>
</SSLHostConfig>
</Connector>
```

7 如下所示编辑 `ism-configuration.properties` 文件：

```
com.netiq.idm.osp.ssl-keystore.file = /opt/netiq/idm/apps/tomcat/conf/
tomcat.bcfks

com.netiq.idm.osp.ssl-keystore.type = BCFKS

com.netiq.idm.osp.oauth-keystore.file =/opt/netiq/idm/apps/tomcat/conf/
osp.bcfks

com.netiq.idm.osp.oauth-keystore.type = BCFKS

com.netiq.rpt.ssl-keystore.file = /opt/netiq/idm/apps/tomcat/conf/
idm.bcfks

com.netiq.rpt.ssl-keystore.type = BCFKS

DirectoryService/realms/jndi/params/KEYSTORE_PATH = /opt/netiq/idm/
apps/tomcat/conf/idm.bcfks

com.sssw.fw.security.sigcert.truststore.type = BCFKS

com.netiq.idm.osp.oauth-truststore.file = /opt/netiq/idm/apps/tomcat/
conf/idm.bcfks
```

```
com.netiq.idm.ua.ldap.keystore-type = BCFKS

com.netiq.idm.osp.oauth-key-alias = ssl certificatedns
```

8 导航到 /opt/netiq/idm/apps/tomcat/conf/ 目录，并运行以下命令：

```
keytool -storepasswd -new <new master keystore password> -keystore /
opt/netiq/idm/apps/tomcat/conf/encrypt-keys.bcfks -storepass changeit -
storetype BCFKS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
$CLASSPATH

keytool -keypasswd -alias ism.config.encrypt.0 -keypass changeit -new
<new master keystore password> -keystore /opt/netiq/idm/apps/tomcat/
conf/encrypt-keys.bcfks -storepass novell  -storetype BCFKS -
providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
$CLASSPATH
```

运行此命令会生成一个 keystorepass 值 :

```
java -cp ../lib/obscurity-0.13.2-uber.jar
com.netiq.ism.obfuscate.server.util.PasswordObfuscator novell
```

9 获取 keystorepass 值后，如下所示更新 ism-sensitive.properties 文件中的以下几行：

```
com.microfocus.ism.master-keypass = <keystorepass-value>
com.microfocus.ism.master-storepass = <keystorepass-value>
```

10 将以下 jar 文件复制到 configupdate/lib 目录：

- bc-fips-1.0.2.4.jar
- bcpkix-fips-1.0.7.jar
- bctls-fips-1.0.18.jar

11 如下所示编辑 configupdate.bat.properties 文件：

```
master_keystore=/opt/netiq/idm/apps/tomcat/conf/encrypt-keys.bcfks
master_keystore_type=bcfks
```

12 如下所示编辑 configupdate.sh 文件：

```
set "JAVA_OPTS= -Dorg.bouncycastle.fips.approved_only=true -
Dinternal.osp.framework.fips-password=novell -
Dorg.bouncycastle.rsa.allow_multi_use=true -
Djavax.net.ssl.keyStoreType=BCFKS -Djavax.net.ssl.trustStoreType=BCFKS
-Djavax.net.ssl.trustStore=/opt/netiq/idm/apps/tomcat/conf/idm.bcfks -
Djavax.net.ssl.trustStorePassword=novell  "

set CLASSPATH=/opt/netiq/common/jre/lib/bc-fips-1.0.2.4.jar:/opt/netiq/
common/jre/lib/bcpkix-fips-1.0.7.jar:/opt/netiq/common/jre/lib/bctls-
fips-1.0.18.jar:%CLASSPATH%
```

13 起动 configupdate.sh 实用程序。

14 启动 Tomcat。

11 在 FIPS 模式下配置 Remote Loader

要在 Remote Loader 上配置 FIPS 模式，请执行以下步骤：

1. 将以下 jar 文件放入 `/opt/novell/dirxml/remoteloader/lib/` 目录：
   - `bc-fips-1.0.2.4.jar`
   - `bcpkix-fips-1.0.7.jar`
   - `bctls-fips-1.0.18.jar`
2. 导航到 `/opt/novell/dirxml/doc/` 目录。
3. 配置 RL 实例时，在配置文件中添加 `is_fips_enabled=true` 标志。例如，可以在示例配置文件 `config8000.txt` 中添加该标志。
4. 保存该文件，并使用 `rdxml` 命令启动 Remote Loader 实例。

V 将 Identity Manager 数据迁移到新安装

本部分提供有关将 Identity Manager 组件中的现有数据迁移到新安装的信息。大多数迁移任务都适用于 Identity Applications。要升级 Identity Manager 组件，请参见第 VI 部分 “ 升级 Identity Manager”（第 177 页）。有关升级与迁移之间区别的详细信息，请参见“ 了解升级过程 ”（第 180 页）。

12 准备迁移 Identity Manager

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

执行迁移的核对清单

要执行迁移， NetIQ 建议您完成以下核对清单中的步骤。

	核对清单项目
❑	1. 确保拥有最新的安装包用于迁移 Identity Manager 数据。
❑	2. 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 “ 升级身份库 ”（第 190 页）。
❑	3. 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 “ 将 Identity Manager 引擎迁移到新服务器 ”（第 166 页）。
❑	4. 在新服务器上安装 Identity Manager。有关详细信息，请参见 “ 规划 Identity Manager 安装 ”（第 33 页）。
❑	5. （视情况而定）如果驱动程序集中有任何驱动程序是 Remote Loader 驱动程序，请升级每个驱动程序的 Remote Loader 服务器。有关详细信息，请参见 “ 升级 Remote Loader”（第 193 页）。
❑	6. （视情况而定）如果您要在旧服务器上运行 User Application，请更新该组件及其驱动程序。有关更多信息，请参见 “ 先决条件 ”（第 165 页）。
❑	7. 更改每个驱动程序的特定于服务器的信息。有关更多信息，请参见 “ 在 Designer 中复制服务器特定信息 ”（第 167 页）。
❑	8. （视情况而定）如果您正在运行 User Application，请将 User Application 的旧服务器中的服务器特定信息更新到新服务器。有关更多信息，请参见 “ 复制驱动程序集的服务器特定信息 ”（第 166 页）。
❑	9. 将驱动程序更新为包格式。有关详细信息，请参见 “ 升级 Identity Manager 驱动程序 ”（第 196 页）。
❑	10. （视情况而定）如果您有自定义的策略和规则，请恢复自定义设置。有关详细信息，请参见 “ 将自定义策略和规则恢复到驱动程序 ”（第 213 页）。
❑	11. 安装 Identity Reporting 和关联的驱动程序。有关更多信息，请参见 “ 迁移 Identity Reporting”（第 171 页）。
❑	12. 从驱动程序集中去除旧服务器。有关更多信息，请参见 “ 从驱动程序集中去除旧服务器 ”（第 212 页）。

	核对清单项目
❑	13. 激活已升级的 Identity Manager 解决方案。有关详细信息，请参见 《*NetIQ Identity Manager Overview and Planning Guide*》（NetIQ Identity Manager 概述和规划指南）中的 “Activating Identity Manager”（激活 Identity Manager）。

13 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：

- “ 先决条件 ”（第 165 页）
- “ 准备要迁移的 Designer 项目 ”（第 165 页）
- “ 将 Identity Manager 引擎迁移到新服务器 ”（第 166 页）
- “ 复制驱动程序集的服务器特定信息 ”（第 166 页）
- “ 迁移 Identity Applications”（第 168 页）
- “ 迁移 Identity Reporting”（第 171 页）

先决条件

- 备份 Identity Manager 解决方案的目录和数据库。
- 确保已安装最新版本的 Identity Manager 组件 （Identity Applications 除外）。

  注释：要继续使用当前的 User Application 数据库，请在安装程序中指定**现有数据库**。有关详细信息，请参见第 4 章 “ 安装 Identity Manager”（第 61 页）。
- 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。
- 将现有 User Application 驱动程序导入到 Designer 中。

准备要迁移的 Designer 项目

必须将 Designer 项目存档。它代表驱动程序的迁移前状态。

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。

将 Identity Manager 引擎迁移到新服务器

1 从软件和许可页面 (https://sld.microfocus.com/) 下载 `Identity_Manager_4.9.0_Linux.iso`。

2 装入下载的 `.iso`。

3 通过 `.iso` 安装 Identity Manager 引擎。

```
./install.sh
```

4 配置 Identity Manager 引擎。

```
configure.sh
```

5 为新服务器上的驱动程序集分区和数据分区创建读写复本。

6 将新服务器添加到 Designer 项目。

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 中执行此操作。如果使用 Designer，则这是一个自动过程。如果使用 Identity Console，则需要手动完成此过程。如果您要从版本低于 3.5 的 Identity Manager 服务器迁移到版本为 3.5 或更高的 Identity Manager 服务器，则应使用 Identity Console。对于所有其他支持的迁移路径，则可以使用 Designer。

- “ 在 Designer 中复制服务器特定信息 ”（第 167 页）
- “ 在 Identity Console 中更改服务器特定的信息 ”（第 167 页）
- “ 更改 User Application 的服务器特定信息 ”（第 168 页）

在 Designer 中复制服务器特定信息

此过程会影响驱动程序集中储存的所有驱动程序。

1 在 Designer 中，打开项目。

2 在**概要**选项卡中，右键单击服务器，然后选择**迁移**。

3 阅读概述以查看迁移到新服务器的项，然后单击**下一步**。

4 从可用服务器列表中选择目标服务器，然后单击**下一步**。

仅列出当前未与驱动程序集相关联且与源服务器的 Identity Manager 版本相同或更高的服务器。

5 选择以下选项之一：

- **激活目标服务器：**将源服务器中的设置复制到目标服务器并禁用源服务器上的驱动程序。 NetIQ 建议您使用此选项。
- **保持源服务器处于活动状态：**不要复制设置并禁用目标服务器上的所有驱动程序。
- **同时激活目标服务器和源服务器：**将源服务器中的设置复制到目标服务器，不禁用源服务器或目标服务器上的驱动程序。如果使用此选项，则必须禁用源服务器或目标服务器上的驱动程序，直到每个驱动程序在新服务器上成功运行。 NetIQ 建议不要同时在两台服务器上超速缓存驱动程序的事件。

注释：当驱动程序在服务器上处于活动状态时，它会超速缓存事件。禁用驱动程序会停止在服务器上超速缓存事件并删除超速缓存 (`.TAO`) 文件。

---

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 “ 启动驱动程序 ”（第 195 页）。

在 Identity Console 中更改服务器特定的信息

1 在 Identity Console 中，转到 **Identity Manager 管理**。

2 单击包含所需驱动程序的驱动程序集对象。

3 单击操作菜单图标 ，然后单击**停止驱动程序**。

4 单击驱动程序图标。

5 转到**配置**。选项卡。

6 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。

7 单击**保存**以保存所有更改并退出。

8 单击 操作菜单，然后单击**启动驱动程序**。

9 对驱动程序集中的每个驱动程序重复步骤 3 到步骤 8。

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，起动配置更新实用程序：

```
configupdate.sh
```

3 按 “ 配置 Identity Applications 的设置 ”（第 97 页）中所述指定值。

迁移 Identity Applications

不要对数据库使用区分大小写的排序。区分大小写的排序不受支持。使用区分大小写的排序可能会导致迁移期间出现重复键错误。如果遇到重复键错误，请检查排序规则并更正它，然后重安装 Identity Applications。唯一受支持的排序规则是 SQL_Latin1_General_CP1_CI_AS。

在迁移 Identity Applications 之前，必须从 `/opt/netiq/common/openssl/lib64/` 目录安装 `libssl.so.1.0.0` 和 `libcrypto.so.1.0.0` 库。

Identity Applications 迁移过程包括以下步骤：

- “ 将数据库迁移到新服务器 ”（第 168 页）
- “ 在新服务器上安装 Identity Applications”（第 170 页）

将数据库迁移到新服务器

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

1 以 `postgres` 用户身份登录装有 PostgreSQL 的服务器。

```
#su - postgres
```

2 将数据导出到 `.sql` 文件：确保 Postgres 用户对您要将文件导出到的目录具有完全访问权限：

```
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 5432 -U postgres -d idmuserappdb -f /tmp/idmuserappdb.sql
```

3 登录要安装 PostgreSQL 的新服务器。

4 安装 PostgreSQL。

4a 导航到装入 `Identity_Manager_4.9.0_Linux.iso` 的位置。

4b 导航到 `/common/packages/postgres/` 目录。

4c 使用以下命令安装 PostgreSQL：

```
rpm -ivh netiq-postgresql-9.6.6-0.noarch.rpm
```

4d 使用以下命令将组关联到 postgres 用户。

```
/usr/sbin/usermod -a -G postgres postgres
```

4e 在 `/etc/passwd` 文件中，将 postgres 用户的主目录路径更改为 `/opt/netiq/idm/postgres/`。

4e1 导航到 `/etc/` 目录。

4e2 编辑 `passwd` 文件。

```
vi /etc/passwd
```

4e3 将 postgres 用户的主目录更改为 `/opt/netiq/idm/postgres/`。

4f 以 `postgres` 用户身份登录。

例如：

```
su - postgres
```

4g 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
```

4h 导出 PostgreSQL `home` 目录 .

```
export PGHOME=<postgres home directory path>
```

例如：

```
export PGHOME=/opt/netiq/idm/postgres
```

4i 导出 PostgreSQL 口令：

```
export PGPASSWORD=< 输入数据库口令 >
```

4j 初始化数据库。

```
LANG=en_US.UTF-8 <POSTGRES 主目录 >/bin/initdb -D <POSTGRES 主目录 >/data
```

例如：

```
LANG=en_US.UTF-8 /opt/netiq/idm/postgres/bin/initdb -D /opt/netiq/idm/postgres/data
```

4k 导航到 /opt/netiq/idm/postgres/bin 目录。

4l 为以下组件创建数据库：

```
$ createdb idmuserappdb
$ psql -s idmuserappdb
# create user idmadmin password 'somepassword';
# GRANT ALL PRIVILEGES ON DATABASE idmuserappdb TO idmadmin;
# ALTER DATABASE idmuserappdb OWNER TO idmadmin;
```

5 将数据导入到新 PostgreSQL 数据库中。

5a 将步骤 2 中导出的文件复制到 postgres 用户具有完全访问权限的位置。

5b 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 > -W
```

例如：

```
psql -d idmuserappdb -U idmadmin -f /tmp/idmuserappdb.sql -W
```

在新服务器上安装 Identity Applications

1 从 NetIQ 下载网站下载 Identity_Manager_4.9.0_Linux.iso。

2 装入 .iso。

3 将 iso 的内容复制到您具有写访问权限的另一个目录。

例如：

```
cp /mnt/* /home
```

4 编辑配置文件的内容，以跳过 User Application 和 Roles and Resources Service 驱动程序的部署。

注释：默认情况下，Identity Applications 安装程序会创建并部署 Role and Resource Service 和 User Application 的驱动程序。

4a 导航到 /home/user_application 目录。

4b 编辑 configure.sh 文件。

```
vi configure.sh
```

4c 注释掉下行：

```
install_service_drivers "UA" "${ID_VAULT_ADMIN_LDAP}"
"${ID_VAULT_PASSWORD}" "${ID_VAULT_HOST}" ${ID_VAULT_LDAPS_PORT}
"cn=${ID_VAULT_DRIVER_SET},${ID_VAULT_DEPLOY_CTX}"
```

4d 保存 configure.sh 文件。

5 从 /mnt 目录安装 Identity Applications。

```
./install.sh
```

6 从 /mnt 目录配置 Identity Applications。

```
./configure.sh
```

7 选择**自定义配置**，出现以下提示时选择**否**：

是否要在当前服务器上配置 PostgreSQL 数据库？

8 导航到 /opt/netiq/idm/apps/configupdate 目录中的配置更新实用程序，并确保配置设置正确无误：

```
./configupdate.sh
```

迁移 Identity Reporting

Identity Reporting 迁移过程包括以下步骤：

- “ 更新 Identity Reporting 的驱动程序 ”（第 171 页）
- “ 部署 Identity Reporting 的驱动程序 ”（第 171 页）
- “ 将现有数据迁移到新数据库 ”（第 172 页）
- “ 设置新 Reporting 服务器 ”（第 175 页）
- “ 创建数据同步策略 ”（第 175 页）

更新 Identity Reporting 的驱动程序

1 升级数据收集服务和受管服务网关驱动程序包。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）。

注释：升级包时，请务必指定新 Identity Reporting 服务器的细节。

---

2 部署驱动程序。有关详细信息，请参见 “ 部署 Identity Reporting 的驱动程序 ”（第 171 页）。

3 （视情况而定）如果您是从 4.5.x 迁移且需要迁移 EAS 数据，请执行 “ 将现有数据迁移到新数据库 ”（第 172 页）中所述的步骤。

部署 Identity Reporting 的驱动程序

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，右键单击数据收集服务驱动程序。

3 选择**部署**。

4 对驱动程序集中的每个数据收集服务驱动程序重复此过程。部署数据收集服务驱动程序后，对受管服务网关驱动程序重复此过程。

将现有数据迁移到新数据库

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 Identity Console 停止 DCS 驱动程序：

2a 登录到 Identity Console。

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 （视情况而定）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 （视情况而定）如果您要迁移现有的 EAS 数据，NetIQ 建议运行以下命令来创建 SIEM 数据库：

```
CREATE DATABASE "SIEM"
  WITH OWNER = dbauser
       ENCODING = 'UTF8'
       TABLESPACE = sendata1
       CONNECTION LIMIT = -1;
```

3d 运行以下命令创建 Reporting 数据库：

```
CREATE DATABASE "idmrptdb"
  WITH OWNER = dbauser
       ENCODING = 'UTF8'
       CONNECTION LIMIT = -1;
```

导出 EAS 数据

请仅在您当前运行的是 Identity Manager 4.5.x 并想要将现有 EAS 数据迁移到 SIEM 数据库时，才执行以下操作：

- “导出 EAS 数据”（第 173 页）
- “将 EAS 数据导入新的 PostgreSQL 数据库”（第 174 页）

导出 EAS 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 Identity Console 停止 DCS 驱动程序：
   - **2a** 登录到 Identity Console。
   - **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 EAS 数据导入新的 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 Identity Console 停止 DCS 驱动程序：
   - **2a** 登录到 Identity Console。
   - **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 数据导入新的 PostgreSQL 数据库：
   - **3a** 将导出的 .sql 文件复制到 postgres 用户具有完全访问权限的位置。例如， /opt/netiq/idm/postgres
   - **3b** 执行以下命令将 EAS 数据导入 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。

导出报告数据

请仅在您当前运行的是 Identity Manager 4.7.x 并想要将现有报告数据迁移到新服务器时，才执行以下操作：

- “ 导出报告数据 ”（第 174 页）
- “ 将数据导入新的 Reporting 服务器 ”（第 175 页）

导出报告数据

1. 以 postgres 用户身份登录装有 PostgreSQL 的服务器。

   ```
   #su - postgres
   ```
2. 将数据导出到 .sql 文件：确保 Postgres 用户对您要将文件导出到的目录具有完全访问权限：

   ```
   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 5432 -U dbauser -W idmrptdb -f /tmp/idmrptdb.sql
```

将数据导入新的 Reporting 服务器

1 以 postgres 用户身份登录装有 PostgreSQL 的服务器。

```
#su - postgres
```

2 将数据导入到新 PostgreSQL 数据库中。

2a 将导出的 .sql 文件复制到 postgres 用户具有完全访问权限的位置。

2b 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 idmrptdb -U dbauser -f /tmp/idmrptdb.sql
```

3 检查是否存在任何迁移日志错误，如有则予以解决。

设置新 Reporting 服务器

1 从软件和许可页面 (https://sld.microfocus.com/) 下载 Identity_Manager_4.9.0_Linux.iso。

2 装入 .iso。

3 在 ISO 装入位置运行以下命令：

```
./install.sh
```

4 配置 Identity Reporting。

```
./configure.sh
```

5 选择**自定义配置**，并在出现以下提示时选择**否**：

是否要在当前服务器上配置 PostgreSQL 数据库？

是否要安装新驱动程序集？

注释：默认情况下，Identity Reporting 安装程序会创建并部署受管服务网关和数据收集服务的驱动程序。

---

6 导航到 /opt/netiq/idm/apps/configupdate 目录中的配置更新实用程序，并确保配置设置正确无误：

```
./configupdate.sh
```

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。

VI 升级 Identity Manager

本部分提供有关升级 Identity Manager 组件的信息。

- 第 14 章 “ 准备升级 Identity Manager”（第 179 页）
- 第 15 章 “ 升级 Identity Manager 组件 ”（第 187 页）
- 第 16 章 “ 从高级版切换到标准版 ”（第 215 页）

14 准备升级 Identity Manager

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

警告：您必须始终通过 Identity Manager 增补程序下载网站来更新随 Identity Manager 4.9 安装的组件。否则，您在进行日常的 Identity Manager 增补程序更新期间，可能会遇到严重的冲突。

- “Identity Manager 的升级核对清单 ”（第 179 页）
- “ 了解升级过程 ”（第 180 页）
- “ 支持的升级路径 ”（第 181 页）
- “ 备份当前配置 ”（第 184 页）

Identity Manager 的升级核对清单

要执行升级， NetIQ 建议您完成以下核对清单中的步骤：

	核对清单项目
❑	1. 了解升级过程。有关更多信息，请参见 “ 了解升级过程 ”（第 180 页）。
❑	2. 查看支持升级到 Identity Manager 4.9 的升级路径。有关支持的升级路径信息，请参见 “ 支持的升级路径 ”（第 181 页）。
❑	3. 确保您拥有升级 Identity Manager 的安装包。有关详细信息，请参见 《*NetIQ Identity Manager Overview and Planning Guide*》（NetIQ Identity Manager 概述和规划指南）中的 “Where to Get Identity Manager”（从何处获取 Identity Manager）。
❑	4. 备份当前的项目、驱动程序配置和数据库。有关详细信息，请参见 “ 备份当前配置 ”（第 184 页）。
❑	5. 安装最新版本的 Designer。
❑	6. 将 Sentinel Log Management for IGA 升级到最新版本。有关更多信息，请参见 “ 升级 Sentinel Log Management for IGA”（第 208 页）。
❑	7. 将身份库 (eDirectory) 升级到 9.2.9。有关详细信息，请参见 “ 升级身份库 ”（第 190 页）。
❑	8. 停止与安装了 Identity Manager 引擎的服务器关联的驱动程序。有关更多信息，请参见 “ 停止驱动程序 ”（第 195 页）。

	核对清单项目
❑	9. 升级 Identity Manager 引擎。有关详细信息，请参见 “ 升级 Identity Manager 引擎 ”（第 191 页）。 **注释：**如果要将 Identity Manager 引擎迁移到新服务器，您可以使用与当前 Identity Manager 服务器上相同的 eDirectory 复本。有关更多信息，请参见 “ 将 Identity Manager 引擎迁移到新服务器 ”（第 166 页）。
❑	10. （视情况而定）如果 Identity Manager 引擎的驱动程序集中有任何驱动程序是 Remote Loader 驱动程序，请升级每个驱动程序的 Remote Loader 服务器。有关详细信息，请参见 “ 升级 Remote Loader”（第 193 页）。
❑	11. （视情况而定）升级现有驱动程序的包 （如果有更新的包版本可用）。有关详细信息，请参见 “ 升级 Identity Manager 驱动程序 ”（第 196 页）。 仅当您要使用现有驱动程序的新包中的功能时，才需要进行升级。
❑	12. 升级 Identity Applications。有关更多信息，请参见 “ 升级 Identity Applications”（第 198 页）。
❑	13. 升级 Identity Reporting。有关更多信息，请参见 “ 升级 Identity Reporting”（第 207 页）。
❑	14. 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 “ 启动驱动程序 ”（第 195 页）。
❑	15. （视情况而定）如果已将 Identity Manager 引擎或 Identity Applications 迁移到某个新服务器，请将该新服务器添加到驱动程序集中。有关更多信息，请参见 “ 将新服务器添加到驱动程序集 ”（第 212 页）。
❑	16. （视情况而定）如果您有自定义策略和规则，请恢复自定义设置。有关更多信息，请参见 “ 将自定义策略和规则恢复到驱动程序 ”（第 213 页）。
❑	17. 升级 Analyzer。有关更多信息，请参见 “ 升级 Analyzer”（第 211 页）。
❑	18. 激活已升级的 Identity Manager 解决方案。有关详细信息，请参见 《*NetIQ Identity Manager Overview and Planning Guide*》（NetIQ Identity Manager 概述和规划指南）中的 “Activating Identity Manager”（激活 Identity Manager）。

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 不支持从现有版本直接升级的路径，则您必须先升级到可从其升级到 4.9 版的版本。或者，您可以迁移到新计算机。 NetIQ 将**迁移**定义为在新服务器上安装 Identity Manager，然后将现有数据迁移到该新服务器的过程。

升级

- **Identity Manager 4.8 Standard Edition：**如果您要从 Identity Manager 4.9 升级到 Identity Manager 4.9 Standard Edition，请执行 《Quick Start Guide for Installing NetIQ Identity Manager 4.9 Standard Edition》（NetIQ Identity Manager 4.8 Standard Edition 安

装和升级快速入门指南）中的 “Upgrading Identity Manager 4.8 Standard Edition to Identity Manager 4.8 Standard Edition”（将 Identity Manager 4.6 Standard Edition 升级到 Identity Manager 4.8 Standard Edition）部分所列的步骤。

- **Identity Manager 4.8 Advanced Edition：**如果您当前使用的是 Identity Manager 4.8 Advanced Edition，则可直接将其升级到 Identity Manager 4.9 Advanced Edition。有关详细信息，请参见 “Identity Manager 的升级核对清单 ”（第 179 页）。

迁移

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

如果有多个服务器与一个驱动程序集关联，则可以一次在一个服务器上执行升级或迁移。如果您无法同时升级这些服务器，驱动程序会继续与其他版本的 Identity Manager 配合工作，直到每台服务器都升级完毕。

重要：如果为驱动程序启用的功能仅在 Identity Manager 4.9 或更高版本上受支持，则驱动程序在混合版本的服务器上将停止工作。较旧的引擎无法处理新功能。这将使驱动程序暂停，直到所有服务器都升级到 Identity Manager 4.9 或更高版本后才可重新使用。

从高级版切换到标准版

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

重要：如果您已应用高级版激活码，则不需要切换到标准版，因为标准版的所有功能在高级版中都有提供。仅当您不想在环境中使用任何高级版功能，并且想要缩减 Identity Manager 部署时，才必须切换到标准版。有关详细信息，请参见第 16 章 “ 从高级版切换到标准版 ”（第 215 页）。

支持的升级路径

Identity Manager 4.9 支持从 4.7.5 和 4.8.x 版本升级。 NetIQ 建议您在开始升级前先查看当前版本的发行说明中的信息。

- “ 从 Identity Manager 4.7.5 版本升级 ”（第 181 页）
- “ 从 Identity Manager 4.8.x 版本升级 ”（第 183 页）

注释：Identity Manager 4.9 仅与 eDirectory 9.2.8 和 9.2.9 版本兼容。请务必先将 eDirectory 升级到 9.2.8 或 9.2.9，然后再升级 Identity Manager 引擎。

从 Identity Manager 4.7.5 版本升级

下表列出了 Identity Manager 4.7.5 的组件范围升级路径：

组件	基础版本	升级后的版本
Identity Manager 引擎	4.7.5	1. 将操作系统升级到支持的版本。 2. 将身份库升级到 9.2.9 3. 将 Identity Manager 引擎升级到 4.9。
Remote Loader/ 扇出代理	4.7.5	安装 4.7 版 Remote Loader/ 扇出代理。
Designer		安装 Designer 4.9。
Analyzer		安装 Analyzer 4.8.5。
Identity Applications	4.7.5	升级 Identity Applications 前，请确保身份库和 Identity Manager 引擎已分别升级到 9.2.9 和 4.9。 1. 将操作系统升级到支持的版本。 2. 将数据库升级到支持的版本。有关支持的数据库版本，请参见 NetIQ Identity Manager 技术信息网站。 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 4.9 版本。 4. 更新 User Application 驱动程序、Roles and Resources 驱动程序以及数据收集服务驱动程序包。更新包后，重启动驱动程序。 5. 将 Identity Applications 升级到 4.9。 6. 启动 Tomcat 和 NGINX 服务。
Identity Reporting	4.7.5	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 System Requirements for Identity Manager 4.9 （Identity Manager 4.9 系统要求）。 3. 将 SLM for IGA 升级到支持的版本。 4. 将 Identity Reporting 升级到 7.2.0。 5. （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 NetIQ 文档 (https://www.netiq.com/documentation/identity-manager-49/) 页面您所用版本的发行说明中查看相关信息。

从 Identity Manager 4.8.x 版本升级

下表列出了 Identity Manager 4.8.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	4.8.x	1. 将操作系统升级到支持的版本。 2. 将身份库升级到 9.2.9 3. 将 Identity Manager 引擎升级到 4.9。
Remote Loader/ 扇出代理	4.8.x	安装 4.7 版 Remote Loader/ 扇出代理。
Designer		安装 Designer 4.9。
Analyzer		安装 Analyzer 4.8.5。
Identity Applications	4.8.x	升级 Identity Applications 前，请确保身份库和 Identity Manager 引擎已分别升级到 9.2.9 和 4.9。 1. 将操作系统升级到支持的版本。 2. 将数据库升级到支持的版本。有关支持的数据库版本，请参见 NetIQ Identity Manager 技术信息网站。 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 4.9 版本。 4. 更新 User Application 驱动程序、Roles and Resources 驱动程序以及数据收集服务驱动程序包。更新包后，重启动驱动程序。 5. 将 Identity Applications 升级到 4.9。 6. 启动 Tomcat 和 NGINX 服务。
Identity Reporting	4.8.x	1. 将操作系统升级到支持的版本。 2. 将数据库升级到支持的版本。有关支持的数据库版本的详细信息，请参见 System Requirements for Identity Manager 4.9 （Identity Manager 4.9 系统要求）。 3. 将 SLM for IGA 升级到支持的版本。 4. 将 Identity Reporting 升级到 7.2.0。

NetIQ 建议开始升级前先在 NetIQ 文档 (https://www.netiq.com/documentation/identity-manager-49/) 页面您所用版本的发行说明中查看相关信息。

备份当前配置

在升级之前， NetIQ 建议您先备份 Identity Manager 解决方案的当前配置。您无需再执行其他步骤即可备份 User Application。所有 User Application 配置均储存在 User Application 驱动程序中。您可以通过以下方式创建备份：

- “ 导出 Designer 项目 ”（第 184 页）
- “ 导出驱动程序配置 ”（第 185 页）

导出 Designer 项目

Designer 项目包含纲要及所有驱动程序配置信息。通过创建 Identity Manager 解决方案项目，您可以一步导出所有驱动程序，而无需为每个驱动程序创建单独的导出文件。

- “ 导出当前项目 ”（第 184 页）
- “ 通过身份库创建新项目 ”（第 184 页）

导出当前项目

如果已具有 Designer 项目，请校验项目中的信息是否与身份库中的信息同步。

1. 在 Designer 中，打开项目。
2. 在建模器中，右键单击身份库，然后选择**在线 > 比较**。
3. 评估项目并协调所有差异，然后单击**确定**。

   有关详细信息，请参见 《*NetIQ Designer for Identity Manager Administration Guide*》（NetIQ Designer for Identity Manager 管理指南）中的 “Using the Compare Feature When Deploying”（部署时使用比较功能）。
4. 在工具栏上，选择**项目 > 导出**。
5. 单击**全选**以选择导出所有资源。
6. 选择保存项目的位置和格式，然后单击**完成**。

   将项目保存在当前工作空间以外的任何位置。升级到 Designer 时，必须创建一个新的工作空间位置。有关详细信息，请参见 《NetIQ Designer for Identity Manager Administration Guide》（NetIQ Designer for Identity Manager 管理指南）中的 “Exporting a Project”（导出项目）。

通过身份库创建新项目

如果当前 Identity Manager 解决方案没有 Designer 项目，则必须创建一个项目以备份当前解决方案。

1. 安装 Designer。
2. 起动 Designer，然后指定工作空间的位置。
3. 选择是否要查找联机更新，然后单击**确定**。
4. 在 “ 欢迎 ” 页面上，单击**运行 Designer**。

5 在工具栏上，选择**项目 > 导入项目 > 身份库**。

6 指定项目的名称，然后对项目使用默认位置或选择其他位置。

7 单击“下一步”。

8 指定以下用于连接身份库的值：

- **主机名**：表示身份库服务器的 IP 地址或 DNS 名称
- **用户名**：表示用于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。

导出驱动程序配置

创建驱动程序的导出文件可以备份当前配置。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 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。

15 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。

- “ 升级顺序 ”（第 187 页）
- “ 升级注意事项 ”（第 188 页）
- “ 升级 Designer”（第 189 页）
- “ 升级 Identity Manager 引擎 ”（第 190 页）
- “ 停止和启动 Identity Manager 驱动程序 ”（第 194 页）
- “ 升级 Identity Manager 驱动程序 ”（第 196 页）
- “ 升级 Identity Applications”（第 198 页）
- “ 升级 Identity Reporting”（第 207 页）
- “ 升级 Analyzer”（第 211 页）
- “ 升级后任务 ”（第 211 页）
- “ 将新服务器添加到驱动程序集 ”（第 212 页）
- “ 将自定义策略和规则恢复到驱动程序 ”（第 213 页）

升级顺序

一次只能升级一个 Identity Manager 组件。按以下顺序升级组件：

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. Identity Applications （适用于高级版）
8. Identity Reporting （同时安装标准版 OSP）
9. Analyzer
10. （视情况而定） SSPR
11. Identity Console

注释：

- 务必将 Analyzer 更新到 4.8.5，并将其与 Identity Manager 4.9 搭配使用。
- 如果 SSPR 安装在远程服务器上，则需要单独更新 SSPR。
- 如果所有 Identity Manager 组件都在同一台服务器上运行，请务必将它们都更新到最新版本。

升级注意事项

在开始升级 Identity Manager 组件之前，请查看以下注意事项：

- 只能以控制台模式升级组件。不支持无提示升级。
- 一次只能升级一个组件。
- 身份库必须单独升级。此版本支持 eDirectory 9.2.8 及更高版本。
- 如果在 BTRFS 文件系统上配置了身份库，则升级过程将不会成功。此版本仅支持 Ext3、Ext4 和 XFS 文件系统。
- 在开始升级 Identity Manager 引擎之前，请确保超速缓存文件中没有任何事件。如果驱动程序使用的是 MapDB，请确保升级后的驱动程序能正常与升级后的引擎配合工作。有关详细信息，请参见“使用 MapDB 3.0.9”（第 192 页）。
- 在升级组件之前，必须查看建议的服务器设置。 Identity Manager 要求 Identity Applications 和 OSP 必须安装在同一台计算机上。不过， Identity Reporting 支持本地或远程安装的 OSP。
- 确保使用 FQDN 以统一的方式配置 Identity Applications、 Identity Reporting 和数据库。
- 如果您使用受支持版本的 Oracle 或 Microsoft SQL Server 数据库，则必须配置以下两个数据库实例才能使 Identity Applications 正常工作：Identity Applications (`idmuserappdb`) 数据库和工作流程 (`igaworkflowdb`) 数据库。确保在同一服务器上配置这些数据库实例。
- 如果您使用 Identity Applications 的 NAM 反向代理配置来装载表单，则必须使用 NAM 5.x 版。
- 从 Identity Manager 4.9 开始，已弃用对 NetIQ SecretStore 的支持。升级到最新的 UAD 包并重启动 Tomcat 后， NetIQ SecretStore 储存库中的所有现有电子邮件帐户口令将自动迁移到 `notfSMTPMailPassword` 属性。此口令迁移过程由 `ism-configuration.properties` 文件中的 `com.netiq.idm.migrate.secretstore` 属性控制。此属性默认设置为 `true`。迁移完成后，该属性将自动设置回 false 并一直保持此状态。
- 升级 Self Service Password Reset (SSPR) 时，需注意以下事项：
  - 如果在 SSPR 服务器上启用了 Syslog 输出格式类型为 CEF 的审计功能，则必须从 Sentinel Syslog 服务器中卸装 NetIQ Self Service Password Reset Collector，否则 Syslog 服务器将无法分析 SSPR 审计事件。

- SSPR 支持对审计事件使用 CEF 和 JSON 两种输出格式类型。 SSPR 4.7.0.1 将继续支持 NetIQ Self Service Password Reset Collector 收集 JSON 输出格式类型的事件。如果有多台 SSPR 服务器连接到同一台 Sentinel Syslog 服务器，只能为所有服务器的审计事件选择一种格式类型。
- 如果 SSPR 安装在单独的服务器上，请将该组件升级到 Identity Manager 4.9 中捆绑的最新版本。

将 Identity Manager 更新到版本 4.9 后， SSPR 将升级到版本 4.7.0.1，这就需要使用 Universal CEF Collector 来收集 CEF 格式类型的审计事件。

注释：如果您是首次启用输出格式类型为 CEF 的 SSPR 审计功能，请确保未在 Sentinel Syslog 服务器上配置 NetIQ Self Service Password Reset Collector。

升级 Designer

注释：此版本不支持从早期版本升级 Designer，因此如果您安装了旧版本，则需要在安装 Designer 4.9 之前将其卸装。此外，内置的自动更新和脱机更新功能无法用于升级到 Designer 4.9。

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. 要卸装当前的 Designer 版本，请执行以下操作：

   3a 关闭 Designer

   3b 导航到包含卸装脚本的目录。默认情况下，该脚本的路径为 < 安装目录 >/designer/UninstallDesigner/Uninstall Designer for Identity Manager

   3c 要执行脚本，请输入 `./uninstall`
4. 可以使用 GUI 模式或控制台模式来安装 Designer。

   4a 从软件许可和下载 (https://sld.microfocus.com/index) 门户下载 `Identity_Manager_4.9.0_Designer_Linux.tar.gz`。

   4b 导航到要提取文件的目录。

   4c 运行以下命令：

   ```
   tar -zxvf Identity_Manager_4.9.0_Designer_Linux.tar.gz
   ```

   4d 运行以下命令之一安装 Designer。

   控制台： `./install`

GUI： `./install -i console`

4e 按照提示继续安装。

5 安装 Designer 4.9 后，必须导入旧版本中的所有 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）中的 “Converting Earlier Projects”（转换旧项目）。

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。

安装前校验 Linux RPM

请执行以下步骤来校验 RPM：

1 从软件和许可页面 (https://sld.microfocus.com/) 下载 `Identity_Manager_4.9.0_Linux.iso`。

2 装入下载的 `.iso`。

3 导航到存放公共密钥的以下位置：

```
<ISO-MOUNT-location>/common/license/
```

例如 `cd /mnt/common/license/`

4 运行以下命令导入密钥：

```
rpm --import MicroFocusGPGPackageSign.pub
```

```
rpm --import OT-package-sign.pub
```

5 （可选）运行以下命令校验签名：

```
rpm --checksig -v <mount-location>/IDVault/setup/<RPM Name>
```

例如：

```
rpm --checksig -v /mnt/IDVault/setup/novell-NDSbase-*.x86_64.rpm
```

升级身份库

1 按照《*NetIQ Identity Manager Overview and Planning Guide*》（NetIQ Identity Manager 概述和规划指南）的 “Where to Get Identity Manager”（从何处获取 Identity Manager）中的指导下载 `Identity_Manager_4.9.0_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 由于 iManager 即将弃用，请对以下警告提示输入您的回复：

```
This version of eDirectory installation will upgrade various packages
required by eDirectory and iManager.The updated packages may impact
iManager running on the same server.Do you want to continue
installation/upgrade (y/n)
```

5a （可选）如果要继续，请执行步骤 6。

5b （可选）如果不继续，更新将会终止。

6 接受许可协议并继续安装。

7 指定 **adminDN**。例如， `cn=admin.ou=sa.o=system`。

8 当系统提示停止 eDirectory 实例并升级 NICI 时，指定 `y`。

9 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` 命令提示运行 `ndsconfig upgrade`，请在运行 `nds-install` 后运行该命令。如果升级之后 eDirectory 服务未启动，请运行 `ndsconfig upgrade` 命令。有关详细信息，请参见 《NetIQ eDirectory Installation Guide》（NetIQ eDirectory 安装指南）。

升级 Identity Manager 引擎

验证驱动程序是否已停止。有关详细信息，请参见“ 停止驱动程序 ”（第 195 页）。

升级 Identity Manager 引擎需要执行的步骤如下：

1 从 NetIQ 下载网站下载 `Identity_Manager_4.9.0_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。

引擎升级过程会在身份库的 DIB 目录中保留某些现有的 MapDB 超速缓存文件 (`dx*`)。升级使用 MapDB 的驱动程序后，必须手动去除该驱动程序的这些文件。有关详细信息，请参见“ 使用 MapDB 3.0.9”（第 192 页）。

使用 MapDB 3.0.9

Identity Manager 支持 MapDB 3.0.9。除了 Identity Manager 引擎外，一些驱动程序 （例如 Office365 和 Azure Active Directory）也使用 MapDB。

如果您使用上述任何驱动程序，在升级驱动程序之前必须先查看以下章节：

- “ 了解各驱动程序版本对 Identity Manager 4.9 引擎的支持 ”（第 192 页）
- “ （可选）手动去除 MapDB 超速缓存文件 ”（第 192 页）

了解各驱动程序版本对 Identity Manager 4.9 引擎的支持

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

- Identity Manager 4.9 随附的驱动程序与 Identity Manager 4.9 引擎或 Remote Loader 兼容。必须遵循具体驱动程序实施指南中的驱动程序升级步骤。

（可选）手动去除 MapDB 超速缓存文件

Identity Manager 引擎升级过程会在身份库的 DIB 目录 (`/var/opt/novell/eDirectory/data/dib`) 中保留某些现有的 MapDB 超速缓存文件 (`dx*`)。升级驱动程序之后，必须手动去除该驱动程序的这些文件。此操作可确保您的驱动程序能正常与 Identity Manager 4.9 引擎配合工作。

下表列出了必须去除的 MapDB 超速缓存文件：

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

其中， * 表示 MapDB 状态超速缓存文件的版本。必须去除所有包含上述名称的 MapDB 状态超速缓存文件，无论其版本是什么。对于 Salesforce 驱动程序， MapDB 状态超速缓存文件也用驱动程序名称表示。下面是这些文件的一些示例。

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

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

以非 Root 用户身份升级 Identity Manager 引擎

仅当您以非 root 用户身份安装了 Identity Manager 引擎时，才能执行此操作。

1. 从软件和许可页面 (https://sld.microfocus.com/) 下载 Identity_Manager_4.9.0_Linux.iso。
2. 装入下载的 .iso。
3. 运行以下命令：

   ./install.sh
4. 选择 **Identity Manager 引擎**并按 Enter。
5. 指定 Identity Manager 引擎的非根目录安装位置。例如 /home/user/eDirectory/。
6. 指定 y 以完成升级。

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。有关详细信息，请参见“停止驱动程序”（第 195 页）。
3. 停止每个驱动程序的 Remote Loader 服务或守护程序。

   rdxml -config *path_to_configfile* -u
4. 从 NetIQ 下载网站下载 Identity_Manager_4.9.0_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。

    rdxml -config *path_to_config_file*

重要：如果您的驱动程序使用 MapDB，请在升级该驱动程序之后，手动去除其现有的 MapDB 状态超速缓存文件。之所以需要这样做，是因为 Identity Manager 引擎升级过程不会从身份库的 DIB 目录中去除所有这些文件。有关详细信息，请参见“使用 MapDB 3.0.9”（第 192 页）。

升级 Java Remote Loader

1. 创建 Java Remote Loader 配置文件的备份。
2. 验证驱动程序是否已停止。有关详细信息，请参见“停止驱动程序”（第 195 页）。
3. 停止每个驱动程序的 Remote Loader 服务或守护程序。

   `dirxml_jremote -config path_to_configfile -u`
4. 从 NetIQ 下载网站下载 `Identity_Manager_4.9.0_Linux.iso`。
5. 装入下载的 `.iso`。
6. 导航到 `/IDM/packages/java_remoteloader` 目录。
7. 复制并替换现有 Java Remote Loader 安装目录中的 `dirxml_jremote_dev.tar.gz` 文件。
8. 根据现有设置中的文件，复制并替换现有 Java Remote Loader 安装目录中的以下文件之一：
   - `dirxml_jremote.tar.gz`
   - `dirxml_jremote_mvs.tar`
9. 将步骤 7 和 8 中复制的文件解压缩。

   例如 `tar -zxvf dirxml_jremote.tar.gz`
10. （视情况而定）如果配置文件有问题，请复制您在第 1 步中创建的备份文件。否则，请继续下一步。

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

    `dirxml_jremote -config path_to_config_file`

停止和启动 Identity Manager 驱动程序

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

- “停止驱动程序”（第 195 页）
- “启动驱动程序”（第 195 页）

停止驱动程序

在修改驱动程序的任何文件之前，必须先停止驱动程序。

- “ 使用 Designer 停止驱动程序 ”（第 195 页）
- “ 使用 Identity Console 停止驱动程序 ”（第 195 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 Identity Console 停止驱动程序

1. 在 Identity Console 中，选择 **Identity Manager 管理**。
2. 单击驱动程序集对象对应的**操作菜单**。
3. 单击**停止所有驱动程序**。
4. 对每个驱动程序集对象重复步骤 1 至 3。
5. 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：
   - **5a** 在 Identity Console 中，选择 **Identity Manager 管理**。
   - **5b** 单击驱动程序集对象。
   - **5c** 在驱动程序图标的右上角，单击**操作菜单**并选择**启动选项**。
   - **5d** 单击**手动**，然后单击**确定**。
   - **5e** 对树中的每个驱动程序重复步骤 5a 到步骤 5d。

启动驱动程序

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

- “ 使用 Designer 启动驱动程序 ”（第 196 页）
- “ 使用 Identity Console 启动驱动程序 ”（第 196 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 Identity Console 启动驱动程序

1 在 Identity Console 中，选择 **Identity Manager 概述**。

2 单击驱动程序集对象对应的**操作菜单**图标 。

3 单击**启动所有驱动程序**。

4 如果您有多个驱动程序，请对每个驱动程序集对象重复步骤 1 至 3。

5 设置驱动程序启动选项：

5a 在 Identity Console 中，选择 **Identity Manager 管理**。

5b 单击驱动程序集对象。

5c 在驱动程序图标的右上角，单击**操作菜单**并选择**启动选项**。

5d 单击**手动**，然后单击**确定**。

5e 对每个驱动程序重复步骤 5c 和步骤 5d。

6 测试驱动程序以验证策略是否按照设计运行。

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。 Designer 不会保留您在 Identity Console 中对驱动程序内容所做的任何更改。有关管理包的详细信息，请参见 《*NetIQ Designer for Identity Manager Administration Guide*》（NetIQ Designer for Identity Manager 管理指南）中的 “Understanding Packages”（了解包）。

您可通过以下方式将驱动程序升级到包：

- “ 创建新驱动程序 ”（第 197 页）
- “ 用包的内容替换现有内容 ”（第 197 页）
- “ 保留当前内容并通过包添加新内容 ”（第 197 页）

创建新驱动程序

将驱动程序升级到包的最简单明了的方式是删除现有驱动程序并通过包创建新驱动程序。在新的驱动程序中添加所有需要的功能。每个驱动程序的步骤都不同。有关说明，请参见 Identity Manager 驱动程序文档网站 (https://www.netiq.com/documentation/identity-manager-49-drivers/) 上各个驱动程序的指南。现在驱动程序与之前一样工作，但其内容来自包而不是来自驱动程序配置文件。

用包的内容替换现有内容

如果需要保留驱动程序创建的关联，您无需删除然后重创建驱动程序。您可以保留关联，并用包替换现有的驱动程序内容。

要用包的内容替换现有内容：

1. 创建驱动程序及驱动程序中所有自定义内容的备份。

   有关说明，请参见“ 导出驱动程序配置 ”（第 185 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 (https://www.netiq.com/documentation/identity-manager-49-drivers/) 上每个驱动程序的指南。

4. 将所有自定义策略和规则恢复到驱动程序。有关说明，请参见“ 将自定义策略和规则恢复到驱动程序 ”（第 213 页）。

保留当前内容并通过包添加新内容

在安装包之前，请创建驱动程序配置文件的备份。安装某个包时，该包可能会重写现有策略，从而导致驱动程序停止工作。如果重写了某个策略，您可以导入备份驱动程序配置文件并重创建该策略。

在开始前，请确保任何自定义策略的名称均不同于默认策略。使用新驱动程序文件覆盖驱动程序配置时，会重写现有策略。如果自定义策略的名称不唯一，您将会丢失这些策略。

要通过包向驱动程序添加新内容：

1. 创建驱动程序及驱动程序中所有自定义内容的备份。

   有关说明，请参见“ 导出驱动程序配置 ”（第 185 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 (https://www.netiq.com/documentation/identity-manager-49-drivers/) 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 (https://www.netiq.com/documentation/identity-manager-49-drivers/)。

驱动程序现在包含通过包添加的新功能。

注释：升级 LDAP 驱动程序后，请确保从 temp 目录中删除 `ldap_*.zoomdb` 文件夹。为避免删除 `ldap_*.zoomdb` 文件夹时丢失数据，请执行以下操作：

1. 转到 Designer。
2. 导航到**属性 > 驱动程序配置 > 驱动程序参数 > 发布者选项**。
3. 将**首次启动时要同步的搜索结果**属性更改为**同步所有内容**。

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
- Self-Service Password Reset (SSPR)
- Tomcat、 JDK 和 ActiveMQ
- PostgreSQL 数据库
- One SSO Provider (OSP)

重要：Identity Manager 4.9 要求将 Identity Applications 和 OSP 安装在同一台计算机上。升级到此版本时，请使用升级 Identity Applications 时安装的 OSP，然后将现有 OSP 服务器中的 OSP 设置复制到新的 OSP 服务器。有关详细信息，请参见 “Identity Applications 组件的升级后任务 ”（第 204 页）。

本节提供有关以下主题的信息：

- “ 升级注意事项 ”（第 199 页）
- “ 系统要求 ”（第 201 页）
- “ 了解升级程序 ”（第 201 页）

- “ 升级 PostgreSQL”（第 201 页）
- “ 升级 Identity Applications 组件 ”（第 201 页）
- “Identity Applications 组件的升级后任务 ”（第 204 页）
- “ 升级后校验版本号 ”（第 207 页）

升级注意事项

Identity Applications 升级过程可能会因您升级 Identity Applications 组件的方式而异。在升级 Identity Applications 之前，请注意以下事项：

- 在开始执行 Identity Applications 的升级过程之前，如果您使用 Oracle 或 MS SQL 数据库，则必须创建 `igaworkflowdb`，并向拥有这些数据库的 `idmadmin` 用户指派所有特权。
- 在将 Identity Applications 组件从 Identity Manager 4.7.5 升级到 4.9 之前，请先使用工作流程迁移工具将数据从 Identity Applications 数据库 (`idmuserappdb`) 导出到工作流程引擎数据库 (`igaworkflowdb`)。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 “*Migrating Data from Identity Applications Database into Workflow Engine Database*”（将数据从 Identity Applications 数据库迁移到工作流程引擎数据库）。
- 如果 Identity Applications 和 SSPR 安装在不同的服务器上，则您可以选择单独升级 SSPR。
- 在升级过程中，请确保校验数据库名称和其他默认值，并根据需要进行修改。
- Identity Manager 支持在 Identity Applications 服务器本地安装 OSP。升级程序不支持将 OSP 独立升级到此版本，在升级 Identity Applications 时，它会安装 OSP 的新副本。要将现有 OSP 设置恢复到新安装的 OSP，请参见 “Identity Applications 组件的升级后任务 ”（第 204 页）中的 “One SSO Provider”。

表 15-1 Identity Applications 的升级过程

Identity Applications 部署	升级过程
Identity Applications、SSPR 和 OSP 安装在同一台服务器上	要升级所有组件，请按照 “ 升级 Identity Applications”（第 202 页）中的步骤操作。
Identity Applications 和 OSP 安装在同一台服务器上。 SSPR 安装在其他服务器上。	1. 要升级 Identity Applications 和 OSP，请按照 “ 升级 Identity Applications”（第 198 页）中的步骤操作。 2. 要升级其他服务器上的 SSPR，请按照 “ 升级 SSPR”（第 204 页）中的步骤操作。
Identity Applications 未与 SSPR 和 OSP 安装在同一台服务器上。在这种情况下， SSPR 可以安装在 Identity Applications 服务器或单独的服务器上。但是，OSP 必须安装在 Identity Applications 服务器上。	1. 要升级 Identity Applications 和 OSP，请按照 “ 升级 Identity Applications”（第 198 页）中的步骤操作。 2. 要升级其他服务器上的 SSPR，请按照 “ 升级 SSPR”（第 204 页）中的步骤操作。 3. 起动配置更新实用程序，并提供安装了 OSP 的新服务器的细节。在本例中，新服务器是安装了 Identity Applications 的服务器。有关更多信息，请参见 “SSO 客户端参数 ”（第 115 页）。

- 如果您要升级在 Open Enterprise Server (OES) 23.4 版本上运行的 Identity Applications，请确保 Identity Manager 引擎使用的 JRE 具有连接到 User Application 所需的证书。 Identity Manager 驱动程序使用 Identity Manager 引擎的密钥存储区来访问 User Application。如果 Role and Resource Service 驱动程序在目标位置无法找到所需证书，您可能会在该驱动程序的跟踪记录中看到一个错误。有关如何对此错误查错的详细信息，请参见 《NetIQ Identity Manager - Administrator’s Guide to the Identity Applications》（NetIQ Identity Manager - Identity Applications 管理员指南）。

系统要求

升级过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。有关详细信息，请访问 NetIQ Identity Manager 技术信息网站 (https://www.microfocus.com/en-us/products/netiq-identity-manager/specs)。

了解升级程序

升级进程会从现有组件中读取配置值。这些信息包括 `ism-configuration.properties`、`server.xml`、`SSPRConfiguration.xml` 和其他配置文件。当您使用这些配置文件时，升级过程会在内部调用指定组件的升级程序。此外，升级程序还会创建当前安装的备份。

升级 PostgreSQL

升级 PostgreSQL 需要执行的步骤如下：

1. 从 NetIQ 下载网站下载并解压缩 `Identity_Manager_4.9.0_Linux.iso`。
2. 导航到 `/common/scripts` 目录。
3. 运行以下命令：

   ```
   ./pg-upgrade.sh
   ```
4. 指定以下细节以完成安装：

   现有 Postgres 的安装位置：指定 PostgreSQL 的安装位置。默认位置为 `/opt/netiq/idm/postgres/`。

   注释：确保 Postgres 用户对 `/opt/netiq/idm/postgres` 目录具有相应的许可权限。

   现有的 Postgres 数据目录：指定 PostgreSQL 数据目录所在的位置。默认位置为 `/opt/netiq/idm/postgres/data`。

   现有的 Postgres 数据库口令：指定 PostgreSQL 口令。

   新的 Postgres 数据目录：指定新的 PostgreSQL 数据目录。例如 `/opt/netiq/idm/postgres_new/data`。

升级 Identity Applications 组件

- “ 升级 Identity Applications 的驱动程序包 ”
- “ 升级 Identity Applications”
- “ 升级 SSPR”

升级 Identity Applications 的驱动程序包

您必须停止 Tomcat，并将 User Application 驱动程序、 Role and Resource Service 驱动程序，以及数据收集服务驱动程序的包更新到最新版本。有关将包升级到最新版本的信息，请参见《*NetIQ Designer for Identity Manager Administration Guide*》（NetIQ Designer for Identity Manager 管理指南）中的 “Upgrading Installed Packages” （升级安装的包）。

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

1 在 Designer 中，导航到 User Application 驱动程序并选择 “ 属性 ”。
2 依次单击 “ 包 ”、  。
3 选中**仅显示适用的包版本**复选框。
4 选择**创建工作流程模板**。
5 单击**确定**，然后单击**完成**以完成安装。
6 部署 User Application 驱动程序。

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

升级 Identity Applications

下面的过程介绍如何升级 Identity Applications。

1 从 NetIQ 下载网站下载 `Identity_Manager_4.9.0_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 Applications。可用选项有 **y** 和 **n**。
7 如果您要继续升级，请指定以下细节：

用于备份的 OSP 安装文件夹

仅当 OSP 和 Identity Applications 安装在同一台服务器上时才适用。

指定用于储存 OSP 备份数据的 OSP 备份文件夹。

SSPR 安装文件夹

仅当 SSPR 和 Identity Applications 安装在同一台服务器上时才适用。

指定 SSPR 安装文件夹。

在系统中未找到 SSPR。是否要安装并配置？

仅当 Identity Applications 和 SSPR 安装在不同的服务器上时才适用。

如果您选择 y，则 SSPR 将安装在安装了 Identity Applications 的服务器上。您需要将现有的自定义设置复制到安装 SSPR 的新服务器上。

- **SSPR 配置口令**：指定 SSPR 配置口令。
- **One SSO 服务器 DNS/IP 地址**：指定安装了 OSP 的服务器的 IP 地址。
- **One SSO 服务器 SSL 端口**：指定 OSP SSL 端口。

如果您选择 n，将不会安装 SSPR，但会升级 Identity Applications。

User Application 安装文件夹

指定 User Application 安装文件夹。

Identity Applications One SSO 服务口令

指定 One SSO 口令。指定的口令将更新您在配置更新实用程序中为所有客户端配置的客户端机密。如果需要，您可以从配置更新实用程序重设置相应客户端的口令。有关更多信息，请参见“SSO 客户端参数 ”（第 115 页）。

Identity Applications 数据库 JDBC jar 文件

指定数据库 JAR 文件。例如，如果您要使用安装在同一台服务器上的 PostgresQL 数据库，则现有数据库 jar 文件的默认位置为 `/opt/netiq/idm/postgres/postgresql-42.6.1.jar`。

创建 Identity Applications 的纲要

指定何时创建数据库纲要。可用选项有现在、启动和文件。默认选项为现在。

注释：如果您要使用 MsSQL 或 Oracle，并向 idmadmin 用户指派对此数据库的所有特权，则必须创建 `igaworkflowdb`。

Identity Applications 数据库用户口令

指定数据库 用户口令。

Identity Applications 数据库管理员口令

指定数据库管理员口令。

8 启动 Tomcat。如果您选择立即创建数据库纲要，请选择现在。

```
systemctl start netiq-tomcat.service
```

（可选）在升级过程中，如果您选择启动或写入文件选项来创建数据库纲要，则必须将数据导入到工作流程数据库。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 “*Migrating Data from Identity Applications Database into Workflow Engine Database*” （将数据从 Identity Applications 数据库迁移到工作流程引擎数据库）。

9 重启动 NGINX 服务。

```
systemctl restart netiq-nginx.service
```

升级 SSPR

在高级版中，如果 SSPR 未与 Identity Applications 安装在同一台服务器上，请使用此方法。

在标准版中，只能通过此方法升级 SSPR。

要升级 SSPR，请执行以下操作：

1. 从 NetIQ 下载网站下载 `Identity_Manager_4.9.0_Linux.iso`。
2. 装入下载的 `.iso`。
3. 从 `.iso` 文件的根目录导航到 `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. 指定 **y** 以升级 SSPR。
8. 指定**身份库管理员口令**并完成升级。

Identity Applications 组件的升级后任务

在开始使用 Identity Applications 之前，请执行以下任务：

- 手动删除先前版本的 Tomcat 和 ActiveMQ 服务。例如，运行以下命令：

  ```
  /etc/init.d/idmapps_tomcat_init
  ```

  ```
  /etc/init.d/idmapps_activemq_init
  ```
- 必须手动恢复 Tomcat、 SSPR、 OSP 和 Kerberos 的自定义设置。
- Identity Applications 服务器的密钥存储区 (`idm.jks`) 中应存在 CN 为 Identity Applications 的证书。作为增强的 Java 安全措施的一部分， Identity Applications 现在需要可信证书才能与 OSP 通讯。
- 使用现有的 Identity Applications 密钥存储区文件将已签名证书导入到 idm.jks 中。例如：

  ```
  ./keytool -import -alias mycerts -keystore /opt/netiq/idm/apps/tomcat/
  conf/idm.jks -file /opt/certs/chap8.der
  ```

  注释：从版本 4.7.5 升级到 4.9 时需要执行此步骤。
- 如果您是在群集环境中升级 Identity Applications，则必须在升级 Identity Applications 之后执行以下步骤：
  - 导航到 `/opt/netiq/idm/apps/tomcat/conf` 目录，然后在 `context.xml` 文件的 `Context` 标记中添加下面一行：

    ```
    <Manager notifyListenersOnReplication="true"
    expireSessionsOnShutdown="false"
    className="org.apache.catalina.ha.session.DeltaManager"/>
    ```

- 导航到 /opt/netiq/idm/apps/tomcat/conf 目录，然后在 server.xml 文件的 Cluster 标记中添加下面一行：

```
<Channel className="org.apache.catalina.tribes.group.GroupChannel">
            <Membership
className="org.apache.catalina.tribes.membership.McastService"
                        address="228.0.0.4"
                        port="45564"
                        frequency="500"
                        dropTime="3000"/>
            <Receiver
className="org.apache.catalina.tribes.transport.nio.NioReceiver"
                      address="auto"
                      port="5000"
                      selectorTimeout="100"
                      maxThreads="6"/>

            <Sender
className="org.apache.catalina.tribes.transport.ReplicationTransmit
ter">
              <Transport
className="org.apache.catalina.tribes.transport.nio.PooledParallelS
ender"/>
            </Sender>
            <Interceptor
className="org.apache.catalina.tribes.group.interceptors.TcpFailure
Detector"/>
            <Interceptor
className="org.apache.catalina.tribes.group.interceptors.MessageDis
patchInterceptor"/>
            <Interceptor
className="org.apache.catalina.tribes.group.interceptors.Throughput
Interceptor"/>
          </Channel>

          <Valve
className="org.apache.catalina.ha.tcp.ReplicationValve"

filter=".*\.gif|.*\.js|.*\.jpeg|.*\.jpg|.*\.png|.*\.htm|.*\.html|.*
\.css|.*\.txt"/>

          <Deployer
className="org.apache.catalina.ha.deploy.FarmWarDeployer"
                    tempDir="/tmp/war-temp/"
                    deployDir="/tmp/war-deploy/"
                    watchDir="/tmp/war-listen/"
                    watchEnabled="false"/>

          <ClusterListener
className="org.apache.catalina.ha.session.ClusterSessionListener"/>
```

- 将主节点中的以下文件复制到所有 User Application 节点：
  - ism-sensitive.properties

- ism-configuration.properties
- encrypt-keys.pkcs12

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

  例如，将

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

  更改为

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

Tomcat

- 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 /opt/netiq/idm/apps/osp_backup_< 日期 > 中的 osp.jks 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。

SSPR

如果 Identity Applications 和 SSPR 部署在不同的服务器上，而您选择将现有的 SSPR 自定义设置恢复到安装了 SSPR 的新服务器，请务必使用 ConfigUpdate 实用程序修改新 SSPR 服务器上的 SSPR 设置。有关详细信息，请参见 “SSO 客户端参数 ”（第 115 页）。

One SSO Provider

如果在升级前的设置中，Identity Applications 和 OSP 部署在不同的服务器上，请将现有的 OSP 设置复制到安装了 OSP 的新服务器 （Identity Applications 服务器），然后在此服务器上运行安装套件中的 merge_jars 方法来恢复设置。

1 在升级了 Identity Applications 的服务器上停止 Tomcat （升级 Identity Applications 时会安装 OSP）。

2 恢复自定义设置。

  2a 导航到现有 OSP 服务器中的 OSP 安装目录，找到 osp-custom-resource.jar 文件。

  例如 /opt/netiq/backup_idm/osp/osp-extras/l10n-resources/osp-custom-resource.jar。

  2b 将 osp-custom-resource.jar 文件复制到升级了 Identity Applications 的服务器上的某个位置。

  2c 导航到 <Identity_Manager_4.9.0_Linux.iso 装入位置 >/osp/scripts/merge_cust_loc.sh。

  此脚本包含用于将现有自定义设置合并到新安装的 OSP 的 merge_jars 方法。

  2d 打开命令提示符并运行以下命令：

```
merge_jars ${IDM_BACKUP_FOLDER in the remote OSP server}/tomcat/lib/
osp-custom-resource.jar ${IDM 4.9_OSP_INSTALLED_HOME}/osp-extras/
l10n-resources/osp-custom-resource.jar)
```

例如：

```
merge_jars /opt/netiq/backup_idm/osp/osp-extras/l10n-resources/osp-
custom-resource.jar /opt/netiq/idm/apps/osp/osp-extras/l10n-
resources/osp-custom-resource.jar
```

其中， `backup_idm` 目录包含现有 OSP 服务器中的 OSP 设置。

3 在安装了 OSP 的新服务器上启动 Tomcat。

要更新其他设置，请参见 “SSO 客户端参数 ”（第 115 页）。

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 Tomcat 文件夹中，请从备份文件夹中将这些文件复制到新 Tomcat 文件夹。

升级后校验版本号

升级到 Identity Manager 4.9 后，请校验组件是否已升级到以下版本：

- Tomcat - `9.0.85`
- ActiveMQ - `5.18.3`
- Java – `1.8.0_222`
- One SSO Provider - `6.7.0`
- Self-Service Password Reset - `4.7.0.1`

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 “ 升级 PostgreSQL”（第 201 页）。
2. 升级 Sentinel Log Management for IGA。有关详细信息，请参见 “ 升级 Sentinel Log Management for IGA”（第 208 页）。
3. 升级 Identity Reporting。有关详细信息，请参见 “ 升级 Identity Reporting”（第 208 页）。

4. 配置受管系统网关驱动程序。有关更多信息，请参见 “ 配置受管系统网关驱动程序 ”（第 135 页）。
5. 配置数据收集。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 “Configuring Settings and Data Collection” （配置设置和数据收集）。

升级注意事项

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

升级 Sentinel Log Management for IGA

1 从 NetIQ 下载网站下载 `SentinelLogManagementForIGA8.6.1.0.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 SentinelLogManagementForIGA8.6.1.0.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` 以接受许可协议并完成升级。

注释：升级 SLM for IGA 后，请手动导入最新的收集器。

1. 导航到 `SentinelLogManagementForIGA8.6.1.0.tar.gz` 文件的解压缩目录。
2. 导航到 `/content/` 目录。
3. 导入并配置收集器。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）中的 “Installing and Configuring the Sentinel Collectors” （安装和配置 Sentinel 收集器）。

升级 Identity Reporting

1 从 NetIQ 下载网站下载 `Identity_Manager_4.9.0_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。

OSP 安装文件夹：指定 OSP 的备份安装文件夹。

用于备份的 Reporting 安装文件夹：指定 Reporting 安装文件夹。

您希望何时创建 Identity Reporting 的纲要：指定是要现在还是以后创建数据库的纲要。可用选项有**现在**、**启动**和**文件**。

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。

注释：将 Identity Manager 升级到 4.9 后，

- IDMDCS UI 中将不会显示数据同步策略。如果您打算创建新策略，则必须去除 Sentinel 服务器中现有的数据同步策略，然后在配置 Identity Reporting 之后使用 IDMDCS UI 创建新的数据同步策略。
- `ism-configuration.properties` 文件中的 `com.netiq.rpt.ssl-keystore.type` 属性将保留升级之前设置的值 (JKS/PKCS12)。

注释：如果您将 Identity Reporting 从 4.8.7 升级到 4.9，将在 `/opt/netiq/idm/apps/deprecate-tomcat-jre8` 位置备份基于 Java 8 的 tomcat。

Reporting 的升级后步骤

- 在分布式设置中，将 Identity Applications 和 Identity Reporting 从 4.8.x 升级到 4.9 之后，请执行以下步骤：

  1. 运行以下命令从 Identity Applications 的 `idm.jks` 文件导入 OSP 证书，并将其置于新的 Java 密钥存储区文件中：

     ```
     /opt/netiq/common/jre/bin/keytool -importkeystore -srckeystore /opt/netiq/idm/apps/tomcat/conf/idm.jks -srcstorepass novell-destkeystore ./idm.jks -deststorepass novell -srcalias "cn=<用户名>, o=< 组织名称 >" -destalias "cn=< 用户名 >" -noprompt
     ```

     例如：

```
/opt/netiq/common/jre/bin/keytool -importkeystore -srckeystore /
opt/netiq/idm/apps/tomcat/conf/idm.jks -srcstorepass novell-
destkeystore ./idm.jks -deststorepass novell -srcalias "cn=sean,
o=novell" -destalias "cn=sean" -noprompt
```

2. 将 Identity Reporting 服务器中现有的 Java 密钥存储区文件替换为这个新创建的密钥存储区文件，然后重启动 Identity Reporting 服务器。

- 如果在升级期间针对“创建 Identity Reporting 的纲要”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。

另外，请在启动一次 Tomcat 后再重启动一次，以确保可用数据库正常运行。

- 将 Identity Reporting 升级到 4.9 之后，导航到 `/opt/netiq/idm/apps/tomcat/conf/` 目录中的 `ism-configuration.properties` 文件，并执行以下操作：
  - 按如下所示更改 `com.netiq.rpt.landing.url` 属性的值：

    ```
    com.netiq.rpt.landing.url = ${com.netiq.idm.osp.url.host}/idmdash/
    #/landing
    ```

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

    ```
    com.netiq.idmdcs.landing.url = ${com.netiq.idm.osp.url.host}/
    idmdash/#/landing
    ```

  - 采用以下格式指定 `com.netiq.rpt.redirect.url` 属性的值：`https:<`主机名`>:<`端口`>/`路径

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

  完成所需的更改后，保存文件并重启动 Tomcat。

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

  例如，将

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

  更改为

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

校验 Identity Reporting 的升级

1. 起动 Identity Reporting。
2. 校验工具中是否显示了旧报告和新报告。
3. 查看**日历**以确定是否显示了安排的报告。
4. 确保**设置**页面显示了受管和非受管应用程序的先前设置。

5 校验所有其他设置是否正确。

6 校验应用程序是否列出已完成的报告。

升级 Analyzer

重要：Identity Manager 4.9 ISO 中不包含 Analyzer 工具。如果已安装 Analyzer，请务必将其更新到版本 4.8.5 并与 Identity Manager 4.9 搭配使用。

1 从软件和许可页面 (https://sld.microfocus.com/) 下载 `Identity_Manager_4.8.5_Linux_Analyzer.tar.gz`。

2 将该 `.zip` 文件抽取到包含 Analyzer 安装文件 （例如插件、卸装脚本和其他 Analyzer 文件）的目录。

3 重启动 Analyzer。

4 要校验是否已成功应用新的增补程序，请完成以下步骤：

4a 起动 Analyzer。

4b 单击**帮助 > 关于 Analyzer**。

4c 检查程序显示的是否为新版本。

升级后任务

升级后，请执行以下操作：

升级服务驱动程序

注释：更新驱动程序包之前，请确保已将 Identity Applications 更新到最新版本。

将 Identity Applications 更新到最新版本后，您可以将 User Application 驱动程序包更新到 4.8.8.20240401125038，将 Role and Resource Service 驱动程序包更新到 4.8.8.20231216023752，将数据收集服务驱动程序包更新到 2.4.2.20230627174512。

请执行以下步骤来更新驱动程序包：

1 打开包含所需服务驱动程序的项目。

2 右键单击服务驱动程序，然后单击**驱动程序** > **属性**。

3 单击**包**。

“ 可用升级 ” 列中的对勾表示相应包有新版本。

4 （视情况而定）如果是 UAD 包，请对 `NOVLUABASE_4.8.8.20240401125038.jar` 包单击**选择**操作。

5 （视情况而定）如果是 RRSD 包，请对 `NOVLRSERVB_4.8.8.20231216023752.jar` 包单击**选择**操作。

6 （视情况而定）如果是 DCS 包，请对 NOVLRSERVB_2.4.2.20230627174512.jar 包单击**选择**操作。

7 在下拉列表中，单击**升级**。

8 选择要升级到的版本，然后单击**确定**。

注释：Designer 会列出可用于升级的所有版本。

9 单击**应用**。

10 （视情况而定）在字段中填写适当的信息以升级该包，然后单击**下一步**。

根据您选择升级的包，您必须相应地填写升级该包所需的信息。

11 查看将安装的包的摘要，然后单击**完成**。

12 查看升级的包，然后单击**确定**关闭“包维护”页面。

13 部署更改，然后重启动驱动程序。

14 重启动 eDirectory 服务。

去除未使用的 Log4j JAR

安装 Identity Manager 4.9 时，会在 /opt/netiq/idm/lightWeightDesigner/plugins/com.novell.soa.eai.integrationActivity_4.0.0.201910221801/lib 目录中安装 log4j-1.2.13.jar。 Identity Manager 不再使用此 jar 文件。请在该目录中找到并删除 log4j-1.2.13.jar。

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 Identity Console 更新驱动程序集。

例如，如果您使用 Identity Console，请执行以下步骤：

1 在 Identity Console 中，单击 **IDM 管理**。

2 选择驱动程序集。

3 单击 。

4 单击**添加 服务器**。

5 浏览并选择新 Identity Manager 服务器，然后单击**确定**。

从驱动程序集中去除旧服务器

当新服务器运行所有驱动程序后，您可以从驱动程序集中去除旧服务器。

- “使用 Designer 从驱动程序集中去除旧服务器”（第 213 页）
- “使用 Identity Console 从驱动程序集中去除旧服务器”（第 213 页）
- “弃用旧服务器”（第 213 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 Identity Console 从驱动程序集中去除旧服务器

1. 在 Identity Console 中，单击 **IDM 管理**。
2. 选择驱动程序集。
3. 单击  。
4. 单击**去除服务器**。
5. 浏览并选择新 Identity Manager 服务器，然后单击**确定**。

弃用旧服务器

此时，旧服务器不再托管任何驱动程序。如果不再需要该服务器，则必须完成其他步骤以将其弃用：

1. 从此服务器中去除 eDirectory 复本。

   有关详细信息，请参见 《*NetIQ eDirectory Administration Guide*》（NetIQ eDirectory 管理指南）。
2. 从此服务器中去除 eDirectory。

将自定义策略和规则恢复到驱动程序

安装或升级到驱动程序的新包之后，您必须将所有自定义策略或规则恢复到驱动程序，然后再重写新的驱动程序配置文件。如果这些策略具有不同名称，则它们仍存储在驱动程序中，但是链接会损坏并需要重新建立。

- “ 使用 Designer 将自定义策略和规则恢复为驱动程序 ”（第 214 页）
- “ 使用 Identity Console 将自定义策略和规则恢复到驱动程序 ”（第 214 页）

使用 Designer 将自定义策略和规则恢复为驱动程序

您可以将策略添加到策略集中。在将升级后的驱动程序移到生产环境中之前，您应该在测试环境中执行以下步骤。

1. 在**大纲**视图中，选择已升级的驱动程序，然后单击**显示策略流**图标 。
2. 右键单击需要将自定义策略恢复为驱动程序的策略集，然后选择**添加策略 > 复制现有策略**。
3. 浏览到并选择自定义策略，然后单击**确定**。
4. 指定自定义策略的名称，然后单击**确定**。
5. 在文件冲突讯息中单击**是**以保存项目。
6. 策略构建器打开策略后，验证复制的策略中信息是否正确。
7. 对需要恢复为驱动程序的每个自定义策略，重复步骤 2 到步骤 6。
8. 启动并测试驱动程序。

   有关启动驱动程序的详细信息，请参见 <TBD - provide a link to the book where you will have the Starting the Drivers section>。有关测试驱动程序的详细信息，请参见 《*NetIQ Identity Manager - Using Designer to Create Policies*》（NetIQ Identity Manager - 使用 Designer 创建策略）中的 “Testing Policies with the Policy Simulator” （使用策略模拟器测试策略）。
9. 验证策略工作正常后，将驱动程序移动到生产环境中。

使用 Identity Console 将自定义策略和规则恢复到驱动程序

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 Identity Console 中，转到 **Identity Manager 管理**。
2. 单击包含已升级的驱动程序的驱动程序集对象。
3. 单击驱动程序图标。
4. 转到**数据转换和同步 > 策略**，然后选择您需要在其中恢复自定义策略的策略集。
5. 单击**插入策略**。
6. 在**使用现有策略**弹出窗口中，浏览并选择自定义策略。
7. 单击**保存**。
8. 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 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 “ 启动驱动程序 ”（第 195 页）。 Identity Console 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。

16 从高级版切换到标准版

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

1 （视情况而定）如果您已应用高级版激活，请去除激活。

2 （视情况而定）要切换到标准版评估模式，请执行以下操作：

2a 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 重启动身份库。

2d 继续步骤 4。

3 （视情况而定）如果您已购买标准版激活，请应用激活。

4 停止 Tomcat。

5 从 `/opt/netiq/idm/apps/tomcat/webapps` 目录中去除以下 WAR 文件和 Webapps 文件夹：

- `IDMProv*`
- `IDMRPT*`
- `dash*`
- `idmdash*`
- `landing*`
- `rra*`
- `rptdoc*`

6 将以下现有文件夹移到备份目录：

- `IDMReporting`
- `UserApplication`

7 将 `<安装文件夹>/tomcat/conf` 目录中的 `ism-configuration.properties` 文件复制到备份目录。

8 安装 Identity Reporting。有关更多信息，请参见第 4 章 “ 安装 Identity Manager”（第 61 页）。

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 客户端密码。例如， *<sspr 客户端密码 >*
  - **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 97 页）。

10 保存更改并退出配置实用程序。

11 启动 Tomcat。

VII 部署 Identity Manager 容器

Identity Manager 提供了通过容器化机制来部署 Identity Manager 组件的灵活选择。 Identity Manager 使用 Docker 来管理容器。支持容器化的 Identity Manager 组件以 Docker 映像的形式提供。 Docker 映像是自足性的，能够独立运行。

此 Docker 映像可用于以下 Identity Manager 组件：

- Identity Manager 引擎
- Remote Loader
- One SSO Provider (OSP)
- 扇出代理
- ActiveMQ
- PostgreSQL (Redistribution)
- Identity Applications
- Self Service Password Reset (SSPR)
- 表单渲染器
- Identity Reporting
- Identity Console

注释：Identity Configuration Generator 映像用于生成无提示属性文件。

可通过企业安装模式实现的所有功能和操作也可以通过容器化机制来实现。

17 规划容器部署

下列各节介绍 Docker 环境中基于容器的部署所需的高层级规划：

- “ 系统要求 ”（第 219 页）
- “ 获取 Docker 映像 ”（第 219 页）

系统要求

必须确保符合部署容器的下列要求：

软件	认证的版本
Docker	24.0.7-ce 或更高版本

获取 Docker 映像

获取 Docker 映像需要执行的步骤如下：

1. 从软件许可和下载 (https://sld.microfocus.com) 门户下载 `Identity_Manager_4.9.0_Containers.tar.gz`。
2. 运行以下命令解压缩 `.tar` 文件：

   ```
   tar -zxvf Identity_Manager_4.9.0_Containers.tar.gz
   ```

18 Identity Manager 容器部署

Identity Manager 容器部署过程包括安装前、安装期间以及安装后工作。本章中使用的示例提供有关在高级版中部署容器的信息，但您也可以在标准版中部署容器。

有些容器依赖于其他容器。下表提供了这些依赖于其他容器的容器的相关细节。

***表 18-1** 依赖的容器*

容器	依赖的容器
OSP	◆ Identity Engine
Identity Applications	◆ OSP ◆ Identity Applications 的数据库
表单渲染器	Identity Applications
Identity Reporting	◆ Identity Applications ◆ Identity Reporting 的数据库
SSPR	Identity Applications

最佳实践

本节包含部署 Docker 容器的一些提示和最佳实践：

- NetIQ 建议您为容器设置 CPU 使用量限制。可通过在 docker run 命令中使用 `--cpuset-cpus` 标志来指定此设置。
- 要设置容器的重启动策略，请在 docker run 命令中使用 `--restart` 标志。建议选择故障时重启动策略，并将重启动尝试次数限制为 5 次。
- 要设置容器可使用的内存量限制，请在 docker run 命令中使用 `--memory` 标志。
- 如果您要备份已部署驱动程序的跟踪文件，可将跟踪文件放到 `/config/idm/` 下，或将跟踪文件手动复制到卷文件夹中。
- 要设置在任意时间点允许运行的进程数限制，请在 docker run 命令中使用 --pids-limit 标志。建议将 PID 值限制为 300。
- 对于 Identity Manager 引擎容器，如果您要查看位于 `/proc` 文件系统 /process 目录下的 `environ` 文件，请在 docker run 命令中使用 `--cap-add=SYS_PTRACE` 标志。系统默认会限制大部分特权，只会启用必需的特权。有关详细信息，请参见 Docker 文档。
- 确保第三方 jar 文件为已装入的卷，这样每次启动容器时这些文件才可用。例如，如果容器的 `/opt/netiq/idm/apps/tomcat/lib` 目录中存在 `ojdbc.jar`，则您必须使用以下命令对 jar 文件进行卷装入操作：

  ```
  -v /host/ojdbc.jar:/opt/netiq/idm/apps/tomcat/lib/ojdbc.jar
  ```

例如，可运行包含上述所有自变量的以下示例命令来部署容器：

```
docker run -itd --cap-add=SYS_PTRACE --pids-limit< 调整容器 pid 限制 > --
memory=< 容器可使用的最大内存量 > --restart=on-failure:5 --cpuset-cpus=< 允许在其
中执行的 CPU> --network=< 将容器连接到网络 > -v < 绑定装入卷 > --name=< 指派容器的名
称 > < 映像名称 >
```

管理容器卷数据

Docker 支持使用多种机制来进行数据储存和持久化。实现容器数据持久化的其中一个机制是使用容器中的共享卷。

本指南中使用的示例假设您创建和使用的是共享卷。例如，在 Docker 主机上创建名为 `/data` 的共享卷。

```
mkdir /data
```

创建的共享卷需要许可权限。使用以下命令提供许可权限：

```
chmod -R 777 /data
```

不过，您也可以使用 Docker 支持的其他卷。有关详细信息，请参见 Docker 文档。

注释：确保您对共享卷拥有读写许可权限。

创建无提示属性文件

大多数 Identity Manager 容器都提供交互安装模式。不过， NetIQ 建议使用无提示属性文件来部署不同的容器。

注释：生成 `silent.properties` 文件后，会在 Docker 主机的 `/data` 中提供该文件。

1. 在解压缩 `Identity_Manager_4.9.0_Containers.tar.gz` 文件的位置，导航到 `Identity_Manager_4.9.0_Containers/docker-images` 目录。
2. 运行以下命令装载映像：

   ```
   docker load --input IDM_490_idm_conf_generator.tar.gz
   ```

3. 使用以下示例命令部署容器：

   注释：务必将主机名的值指定为计算机 FQDN。

   ```
   docker run -it --name=idm_conf_generator --
   hostname=identitymanager.example.com -v /data:/config
   idm_conf_generator:idm-4.9.0-580
   ```

4. 导航到 `idm` 目录。
5. 运行 `create_silent_props.sh` 文件：

```
./create_silent_props.sh
```

6 输入 y 继续安装并配置组件。

7 要安装 JRE，请输入 y。

8 指定属性文件的路径。

注释：务必在共享卷的位置 （例如 /config）创建 silent.properties 文件。

9 指定以下设置以创建无提示属性文件：

参数	描述
包含绝对路径的无提示属性文件名	指定无提示属性文件的路径。
配置 Docker 容器的无提示属性	指定是否要为 Docker 容器配置属性文件。
生成用于 Kubernetes 编制的输入	*仅当您已在为 Docker 容器配置无提示属性选项中选择了 y 时才适用。* 指定是否要生成 Kubernetes 的 YAML 文件。
包含用于创建 kube yaml 文件的绝对路径的目录名称	*仅当您已在生成用于 Kubernetes Orchestration 的输入选项中选择了 y 时才适用。* 指定用于创建 Kubernetes YAML 文件的路径。 **注释：**建议为 Identity Applications 和 Identity Reporting YAML 文件提供不同的路径。
Kubernetes 卷装入路径	*仅当您已在“生成用于 Kubernetes Orchestration 的输入”选项中选择了“y”时才适用。* 指定 Kubernetes 卷的路径。
Kubernetes 部署的 Identity Manager 引擎主机名	*仅当您已在生成用于 Kubernetes Orchestration 的输入选项中选择了 y 时才适用。* 指定 Identity Manager 引擎的主机名。

10 决定要安装的 Identity Manager 服务器版本。输入 y 将安装高级版，输入 n 将安装标准版。

11 决定您是要以典型模式还是自定义模式配置组件。

12 在可供安装的组件列表中选择所需的组件：

- 要安装引擎，请选择 **Identity Manager 引擎**。
- 要安装 Identity Reporting，请选择 **Identity Reporting**。
- 要安装 Identity Applications，请选择 **Identity Applications**。

有关配置参数的信息，请参见“了解配置参数”（第 75 页）。

注释：

- 必须一次性为所有组件生成 silent.properties 文件。

- 针对所有与 IP 相关的配置提示使用 FQDN。
- SSO_SERVER_SSL_PORT、 TOMCAT_HTTPS_PORT、 UA_SERVER_SSL_PORT 和 RPT_TOMCAT_HTTPS_PORT 必须是唯一端口。例如，分别将 SSO_SERVER_SSL_PORT 修改为 8543，将 TOMCAT_HTTPS_PORT 和 UA_SERVER_SSL_PORT 修改为 18543，将 RPT_TOMCAT_HTTPS_PORT 修改为 28543。
- （视情况而定）如果您要使用主机网络模式在单台服务器上部署容器，那么针对特定于 OSP、 Identity Applications 和 Identity Reporting 的证书相关提示，必须将 tomcat.ks 路径指定为 /opt/netiq/idm/apps/tomcat/conf/tomcat.ks。

13 （视情况而定）如果您要使用主机网络模式在单台服务器上部署容器，则必须在生成无提示属性文件后执行以下步骤：

- 确保 CUSTOM_OSP_CERTIFICATE 的值设置为 n。
- 将以下条目添加到 Designer.ini 文件的末尾：

```
SKIP_PORT_CHECK=1
CUSTOM_UA_CERTIFICATE="n"
TOMCAT_SSL_KEYSTORE_PASS="< 口令 >"
CUSTOM_RPT_CERTIFICATE="n"
```

部署 Remote Loader 容器后自动启动 Remote Loader 实例

如果您想要在部署 Remote Loader 容器后自动启动 Remote Loader 实例，请执行以下步骤：

1 在 Docker 主机上，导航到共享目录。例如 data。

2 创建 rdxml 目录。

注释：此步骤仅在首次部署容器时适用。换句话说，如果您正在更新容器并且以前已经创建了 rdxml 目录，请跳过此步骤。

3 导航到 rdxml 目录。

4 在 rdxml 目录中创建 driverconf 目录。

注释：如果您对不同的 Remote Loader 实例运行了多个配置文件，请复制所有文件。

5 将所有必需的配置文件复制到 driverconf 目录。例如 config8000.txt。

6 在 rdxml 目录中创建 keystore 目录。

7 将所有必需的密钥储存区文件和证书复制到 keystore 目录。

8 在 rdxml 目录中，创建一个新的 .txt 文件。例如 StartupRL.txt。

9 在 StartupRL.txt 文件中，用以下格式指定所需内容：

```
<Remote Loader 配置文件 > -sp < 驱动程序口令 > <Remote Loader 口令 >
```

例如：

```
config8000.txt -sp dirxml dirxml
```

或者，也可以用以下格式指定项：

```
<Remote Loader 配置文件 > -ksp < 密钥储存区口令 > -kp < 密钥口令 >
```

例如：

```
config8000.txt -ksp dirxml -kp dirxml
```

10 通过在 docker run 命令中传递 `RL_DRIVER_STARTUP` 环境变量来部署 Remote Loader 容器。例如 `-e RL_DRIVER_STARTUP="StartupRL.txt"`。

容器部署模式

NetIQ 建议使用以下模式来部署容器：

- 在单台服务器上部署容器
- 在分布式服务器上部署容器

在单台服务器上部署容器

此示例使用主机网络模式将所有 Identity Manager 容器部署在单个 Docker 主机上。

先决条件

- 确保主机名采用如下所示的 FQDN 格式：

  ```
  < 主机 IP> <FQDN> < 短名称 >
  ```

  例如：

  ```
  172.120.0.1     identitymanager.example.com      identitymanager
  ```

- 必须在部署容器之前生成无提示属性文件。有关生成无提示属性文件的详细信息，请参见 “ 创建无提示属性文件 ”（第 222 页）。

必须按以下顺序部署容器：

- “ 部署 Identity Manager 引擎容器 ”（第 226 页）
- “ 部署 Remote Loader 容器 ”（第 226 页）
- “ 部署扇出代理容器 ”（第 227 页）
- “ 通过身份库证书颁发机构生成证书 ”（第 227 页）
- “ 部署 OSP 容器 ”（第 229 页）
- “ 部署 PostgreSQL 容器 ”（第 229 页）
- “ 部署 Identity Applications 容器 ”（第 230 页）
- “ 部署表单渲染器容器 ”（第 231 页）

- “ 部署 ActiveMQ 容器 ”（第 232 页）
- “ 部署 Identity Reporting 容器 ”（第 232 页）
- “ 部署 SSPR 容器 ”（第 233 页）

部署 Identity Manager 引擎容器

1 生成无提示属性文件。有关详细信息，请参见 “ 创建无提示属性文件 ”。

2 在解压缩 Identity_Manager_4.9.0_Containers.tar.gz 文件的位置，导航到 Identity_Manager_4.9.0_Containers 目录。

3 运行以下命令装载映像：

```
docker load --input IDM_490_identityengine.tar.gz
```

4 使用以下命令部署容器：

```
docker run --restart unless-stopped -d --network=host --name=engine-
container -v /data:/config -e SILENT_INSTALL_FILE=/config/
silent.properties --stop-timeout 100 identityengine:idm-4.9.0-580
```

5 要校验是否已成功部署容器，请运行以下命令检查日志文件：

```
tail -f /data/idm/log/idmconfigure.log
```

6 要登录容器，请运行以下命令：

```
docker exec -it < 容器 > < 命令 >
```

例如：

```
docker exec -it engine-container bash
```

注释：要运行 ndstrace 或 ndsrepair 等身份库实用程序，请以非 root 用户 nds 的身份登录到容器。如果您以 root 用户身份登录，则无法运行这些实用程序。要以 nds 用户身份登录到容器，请运行 docker exec -it engine-container sudo nds 命令。

部署 Remote Loader 容器

1 在解压缩 Identity_Manager_4.9.0_Containers.tar.gz 文件的位置，导航到 Identity_Manager_4.9.0_Containers 目录。

2 运行以下命令装载映像：

```
docker load --input IDM_490_remoteloader.tar.gz
```

3 使用以下命令部署容器：

```
docker run -d --network=host --name=rl-container -v /data:/config
remoteloader:idm-4.9.0-580
```

此命令会部署 64 位和 32 位版本的 Remote Loader。容器的 /opt/novell/eDirectory/lib/dirxml/classes/ 目录中提供了驱动程序文件。

4 （视情况而定）如果您不想在部署容器时使用配置文件，请使用以下命令部署容器：

```
docker run --restart unless-stopped -d --network=host --name=rl-
container -v /data:/config --stop-timeout 100 remoteloader:idm-4.9.0-
580
```

5 要登录容器，请运行以下命令：

```
docker exec -it < 容器 > < 命令 >
```

例如：

```
docker exec -it rl-container bash
```

6 配置 Remote Loader。有关详细信息，请参见 《*NetIQ Identity Manager Driver Administration Guide*》（NetIQ Identity Manager 驱动程序管理指南）中的 “Configuring the Remote Loader and Drivers”（配置 Remote Loader 和驱动程序）。

7 确保配置文件在共享卷中可用。

部署扇出代理容器

1 在解压缩 `Identity_Manager_4.9.0_Containers.tar.gz` 文件的位置，导航到 `Identity_Manager_4.9.0_Containers` 目录。

2 运行以下命令装载映像：

```
docker load --input IDM_490_fanoutagent.tar.gz
```

3 使用以下命令部署容器：

```
docker run --restart unless-stopped -d --network=host --name=foa-
container -v /data:/config --stop-timeout 100 fanoutagent:idm-4.9.0-580
```

4 要登录容器，请运行以下命令：

```
docker exec -it < 容器 > < 命令 >
```

例如：

```
docker exec -it foa-container bash
```

5 配置扇出代理。有关详细信息，请参见 *《NetIQ Identity Manager Driver for JDBC Fanout Implementation Guide》（NetIQ Identity Manager Driver for JDBC Fanout 实施指南）(https://www.netiq.com/documentation/identity-manager-49-drivers/jdbc_fanout/data/netiq-identity-manager-for-jdbc-fan-out-driver-implementation-guide.html)* 中的 “Configuring the Fanout Agent”（配置扇出代理）(https://www.netiq.com/documentation/identity-manager-49-drivers/jdbc_fanout/data/how-to-configure-fan-out-agent.html)。

通过身份库证书颁发机构生成证书

（视情况而定）仅当您使用身份库作为证书颁发机构时，本节内容才适用。

在部署以下组件之前，需要先生成证书。在为以下组件生成证书之前，请务必先部署 Identity Manager 引擎和 Identity Console 容器。

- OSP
- Identity Applications
- Identity Reporting

执行以下步骤来生成证书：

1 确保安装的 Java 版本为 Azul Zulu 1.8.0_392 或更高。

2 请务必设置 Java 路径。例如，运行以下命令：

```
export PATH=<java 安装位置 >/bin:$PATH
```

例如：

```
export PATH=/opt/netiq/common/jre/bin/:$PATH
```

3 生成 PKCS 密钥存储区：

```
keytool -genkey -alias idm -keyalg RSA -storetype pkcs12 -keystore /
data/tomcat.ks -validity 3650 -keysize 2048 -dname
"CN=identitymanager.example.com" -keypass <password> -storepass
<password>
```

4 生成证书签名请求：

```
keytool -certreq -v -alias idm -file /config/idm.csr -keypass
<password> -keystore /config/tomcat.ks -storepass <password>
```

5 生成自我签名证书：

5a 起动 Identity Console 并登录。

5b 导航到**证书管理** > **颁发证书**。

5c 浏览到在步骤 3 中创建的 `.csr` 文件。例如 `idm.csr`。

5d 单击**打开**。

5e 在**密钥使用规范**下拉列表中指定密钥类型。

5f 在**扩展密钥使用规范**下拉列表中指定扩展密钥类型。

5g 对于证书类型，请在**基本约束**下拉列表中选择**未指定**。

5h 在**证书参数**下拉列表中指定证书的有效期。

5i 在**证书格式**下拉列表中选择**采用二进制 DER 格式的文件**。

5j 单击**下一步**。

5k 单击**确定**。

5l 下载证书并将其复制到 `/data` 目录。

6 导出 `.der` 格式的根证书：

6a 起动 Identity Console 并登录。

6b 导航到**证书管理** > **服务器证书管理**。

6c 选中 **SSL 证书 DNS** 复选框并单击**导出**。

6d 在**证书**下拉列表中选择 “ 组织 CA”。

6e 在**导出格式**下拉列表中选择 `DER`。

6f 单击**确定**。

6g 下载证书并将其复制到 `/data` 目录。

7 将证书导入到您在步骤 2 中创建的 PKCS 密钥存储区中：

```
keytool -import -trustcacerts -alias root -keystore /config/tomcat.ks -
file /config/cert.der -storepass <password> -noprompt

keytool -import -alias idm -keystore /config/tomcat.ks -file /config/
idm.der -storepass <password> -noprompt
```

注释：请确保指定为部署输入的路径中有密钥存储区。

部署 OSP 容器

1. 生成无提示属性文件。有关详细信息，请参见“创建无提示属性文件”。
2. 确保 SSO_SERVER_SSL_PORT 属性设置为某个唯一端口。
3. 在解压缩 Identity_Manager_4.9.0_Containers.tar.gz 文件的位置，导航到 Identity_Manager_4.9.0_Containers 目录。
4. 运行以下命令装载映像：

   ```
   docker load --input IDM_490_osp.tar.gz
   ```

5. 使用以下命令部署容器：

   ```
   docker run --restart unless-stopped -d --network=host --name=osp-
   container -v /data:/config -e SILENT_INSTALL_FILE=/config/
   silent.properties --stop-timeout 100 osp:idm-4.9.0-580
   ```

6. 要校验是否已成功部署容器，请运行以下命令检查日志文件：

   ```
   tail -f /data/osp/log/idmconfigure.log
   ```

7. 使用以下命令停止容器：

   ```
   docker stop osp-container
   ```

8. 运行以下命令修改 server.xml 文件中的 Tomcat 关闭端口。在下面的示例中，端口 8005 将更改为 18005：

   ```
   sed -i "s~8005~18005~g" /data/osp/tomcat/conf/server.xml
   ```

9. 使用以下命令启动 容器：

   ```
   docker start osp-container
   ```

10. 要登录容器，请运行以下命令：

    ```
    docker exec -it < 容器 > < 命令 >
    ```

    例如：

    ```
    docker exec -it osp-container bash
    ```

部署 PostgreSQL 容器

1. 在解压缩 Identity_Manager_4.9.0_Containers.tar.gz 文件的位置，导航到 Identity_Manager_4.9.0_Containers 目录。
2. 运行以下命令装载映像：

```
docker load --input IDM_490_postgres.tar.gz
```

3 在共享卷 data 下创建一个子目录，例如 postgres。

```
mkdir postgres
```

4 使用以下命令部署容器：

```
docker run --restart unless-stopped -d --network=host --
name=postgresql-container -e POSTGRES_PASSWORD=<password> -v /data/
postgres:/var/lib/postgresql/data --stop-timeout 100 postgres:12.18
```

例如：

```
docker run --restart unless-stopped -d --network=host --
name=postgresql-container -e POSTGRES_PASSWORD=novell -v /data/
postgres:/var/lib/postgresql/data --stop-timeout 100 postgres:12.18
```

5 创建 Identity Applications 的 idmdamin 用户。

```
docker exec -it postgresql-container psql -U postgres -c "CREATE USER
idmadmin WITH ENCRYPTED PASSWORD '<password>'"
```

6 创建 Identity Applications、工作流程和 Identity Reporting 数据库。

```
docker exec -it postgresql-container psql -U postgres -c "CREATE
DATABASE idmuserappdb"

docker exec -it postgresql-container psql -U postgres -c "CREATE
DATABASE igaworkflowdb"

docker exec -it postgresql-container psql -U postgres -c "CREATE
DATABASE idmrptdb"
```

注释：当您配置 Identity Applications 和 Identity Reporting 容器时，会用到这些数据库。

7 为 idmadmin 用户授予对数据库的所有特权：

```
docker exec -it postgresql-container psql -U postgres -c "GRANT ALL
PRIVILEGES ON DATABASE idmuserappdb TO idmadmin"

docker exec -it postgresql-container psql -U postgres -c "GRANT ALL
PRIVILEGES ON DATABASE igaworkflowdb TO idmadmin"
```

8 要登录容器，请运行以下命令：

```
docker exec -it < 容器 > < 命令 >
```

例如：

```
docker exec -it postgresql-container bash
```

部署 Identity Applications 容器

1 在解压缩 Identity_Manager_4.9.0_Containers.tar.gz 文件的位置，导航到 Identity_Manager_4.9.0_Containers 目录。

2 运行以下命令装载映像：

```
docker load --input IDM_490_identityapplication.tar.gz
```

3 使用以下命令部署容器：

```
docker run --restart unless-stopped -d --network=host --name=idapps-
container -v /data:/config -e SILENT_INSTALL_FILE=/config/
silent.properties --stop-timeout 100 identityapplication:idm-4.9.0-580
```

4 要校验是否已成功部署容器，请运行以下命令检查日志文件：

```
tail -f /data/userapp/log/idmconfigure.log
```

5 运行以下命令导入密钥存储区：

注释：在执行此步骤之前，请确保容器已成功部署。

```
/opt/netiq/common/jre/bin/keytool -importkeystore -srckeystore /config/
tomcat.ks -srcstorepass <password> -destkeystore /opt/netiq/idm/apps/
tomcat/conf/idm.jks -deststorepass <password>
```

6 系统会提示您将重写 alias idm 的现有项。要重写，请输入 `yes`。

7 系统会提示您将重写 alias root 的现有项。要重写，请输入 `yes`。

8 使用以下命令停止容器：

```
docker stop idapps-container
```

9 运行以下命令修改 `server.xml` 文件中的 Tomcat 关闭端口。在下面的示例中，端口 8005 将更改为 28005：

```
sed -i "s~8005~28005~g" /data/userapp/tomcat/conf/server.xml
```

10 使用以下命令启动 Docker 容器：

```
docker start idapps-container
```

11 要登录容器，请运行以下命令：

```
docker exec -it < 容器 > < 命令 >
```

例如：

```
docker exec -it idapps-container bash
```

注释：要在配置更新实用程序中修改任何设置，请从 Identity Applications 容器的 `/opt/netiq/idm/apps/configupdate/` 目录起动 `configupdate.sh`。配置更新实用程序只能在控制台模式下起动。

部署表单渲染器容器

1 生成无提示属性文件。在生成无提示属性文件时选择 **Identity Applications**。有关详细信息，请参见 “ 创建无提示属性文件 ”。

2 在解压缩 `Identity_Manager_4.9.0_Containers.tar.gz` 文件的位置，导航到 `Identity_Manager_4.9.0_Containers` 目录。

3 运行以下命令装载映像：

```
docker load --input IDM_490_formrenderer.tar.gz
```

4 使用以下命令部署容器：

```
docker run --restart unless-stopped -d --network=host --name=fr-container -v /data:/config -e SILENT_INSTALL_FILE=/config/silent.properties --stop-timeout 100 formrenderer:idm-4.9.0-580
```

5 要登录容器，请运行以下命令：

```
docker exec -it < 容器 > < 命令 >
```

例如：

```
docker exec -it fr-container bash
```

部署 ActiveMQ 容器

1 在解压缩 Identity_Manager_4.9.0_Containers.tar.gz 文件的位置，导航到 Identity_Manager_4.9.0_Containers 目录。

2 运行以下命令装载映像：

```
docker load --input IDM_490_activemq.tar.gz
```

3 使用以下命令部署容器：

```
docker run --restart unless-stopped -d --network=host --name=amq-container -v /data:/config --env-file /data/silent.properties --stop-timeout 100 activemq:idm-4.9.0-580
```

4 要登录容器，请运行以下命令：

```
docker exec -it < 容器 > < 命令 >
```

例如：

```
docker exec -it amq-container bash
```

5 配置 ActiveMQ。有关详细信息，请参见 《NetIQ Identity Manager Driver for JDBC Fanout Implementation Guide》（NetIQ Identity Manager Driver for JDBC Fanout 实施指南）(https://www.netiq.com/documentation/identity-manager-49-drivers/jdbc_fanout/data/how-to-setup-activemq-startup-service.html) 中的 *"Setting Up ActiveMQ Startup Service"（设置 ActiveMQ 启动服务）(https://www.netiq.com/documentation/identity-manager-49-drivers/jdbc_fanout/data/netiq-identity-manager-for-jdbc-fan-out-driver-implementation-guide.html)*。

部署 Identity Reporting 容器

1 在解压缩 Identity_Manager_4.9.0_Containers.tar.gz 文件的位置，导航到 Identity_Manager_4.9.0_Containers 目录。

2 运行以下命令装载映像：

```
docker load --input IDM_490_identityreporting.tar.gz
```

3 使用以下命令部署容器：

```
docker run --restart unless-stopped -d --network=host --name=rpt-
container -v /data:/config -e SILENT_INSTALL_FILE=/config/
silent.properties --stop-timeout 100 identityreporting:idm-4.9.0-580
```

4 要校验是否已成功部署容器，请运行以下命令检查日志文件：

```
tail -f /data/reporting/log/idmconfigure.log
```

5 运行以下命令导入密钥存储区：

注释：在执行此步骤之前，请确保容器已成功部署。

```
/opt/netiq/common/jre/bin/keytool -importkeystore -srckeystore /config/
tomcat.ks -srcstorepass <password> -destkeystore /opt/netiq/idm/apps/
tomcat/conf/idm.jks -deststorepass <password>
```

6 系统会提示您将重写 alias idm 的现有项。要重写，请输入 `yes`。

7 系统会提示您将重写 alias root 的现有项。要重写，请输入 `yes`。

8 使用以下命令停止容器：

```
docker stop rpt-container
```

9 运行以下命令修改 `server.xml` 文件中的 Tomcat 关闭端口。在下面的示例中，端口 8005 将更改为 38005：

```
sed -i "s~8005~38005~g" /data/reporting/tomcat/conf/server.xml
```

10 *（视情况而定）仅当您使用身份库作为证书颁发机构时才适用。*

在 `setenv.sh` 文件的 `export CATALINA_OPTS` 条目中添加 `-Dcom.sun.net.ssl.checkRevocation=false` 参数。在此示例中， `setenv.sh` 文件位于 `/data/reporting/tomcat/bin/` 目录下。

11 使用以下命令启动 Docker 容器：

```
docker start rpt-container
```

12 要登录容器，请运行以下命令：

```
docker exec -it < 容器 > < 命令 >
```

例如：

```
docker exec -it rpt-container bash
```

部署 SSPR 容器

部署 SSPR 容器需要执行的任务如下：

1 生成 SSPR 的无提示属性文件。有关更多信息，请参见 “ 创建无提示属性文件 ”。

2 在共享卷 `data` 下创建一个子目录，例如 `sspr`。

```
mkdir sspr
```

3 在解压缩 `Identity_Manager_4.9.0_Containers.tar.gz` 文件的位置，导航到 `Identity_Manager_4.9.0_Containers` 目录。

4 运行以下命令装载映像：

```
docker load --input IDM_490_sspr.tar.gz
```

5 使用以下示例命令部署容器：

```
docker run --restart unless-stopped -d --network=host --name=sspr-
container -v /data/sspr:/config --stop-timeout 100 sspr/sspr-
webapp:4.7.0.1-580
```

6 在 Docker 主机上运行以下命令，以将 Docker 主机中的 `silent.properties` 文件复制到 SSPR 容器：

```
docker cp /data/silent.properties sspr-container:/tmp
```

7 将无提示属性文件装载到 SSPR 容器。

```
docker exec -it sspr-container /app/command.sh ImportPropertyConfig /
tmp/silent.properties
```

注释：检查是否在 SSPR 容器的 `/config` 目录下创建了 `SSPRConfiguration.xml`，并校验该文件的内容。

---

8 将 OAuth 证书导入 SSPR：

8a 在 Docker 主机上编辑 `/data/sspr/` 目录中的 `SSPRConfiguration.xml` 文件，将 `configIsEditable` 标志的值设置为 **true** 并保存更改。

8b 起动浏览器并输入 `https://identitymanager.example.com:8443/sspr` URL。

8c 使用管理员身份凭证 （例如 `uaadmin`）登录。

8d 单击右上角的用户 （例如 `uaadmin`），然后单击**配置编辑器**。

8e 指定配置口令并单击**登录**。

8f 单击**设置** > **单点登录 (SSO) 客户端** > **OAuth**，确保所有 URL 都使用 HTTPS 协议和正确的端口。

8g 在 **OAuth 服务器证书**下，单击**从服务器导入**以导入新证书，然后单击**确定**。

8h 单击右上角的 保存证书。

8i 查看更改并单击**确定**。

8j SSPR 应用程序重启动之后，编辑 `SSPRConfiguration.xml` 文件，将 `configIsEditable` 标志的值设置为 **true** 并保存更改。

部署 Identity Console 容器

有关部署 Identity Console 容器的详细信息，请参见 Deploying Identity Console as Docker Container （将 Identity Console 部署为 Docker 容器）。

在分布式服务器上部署容器

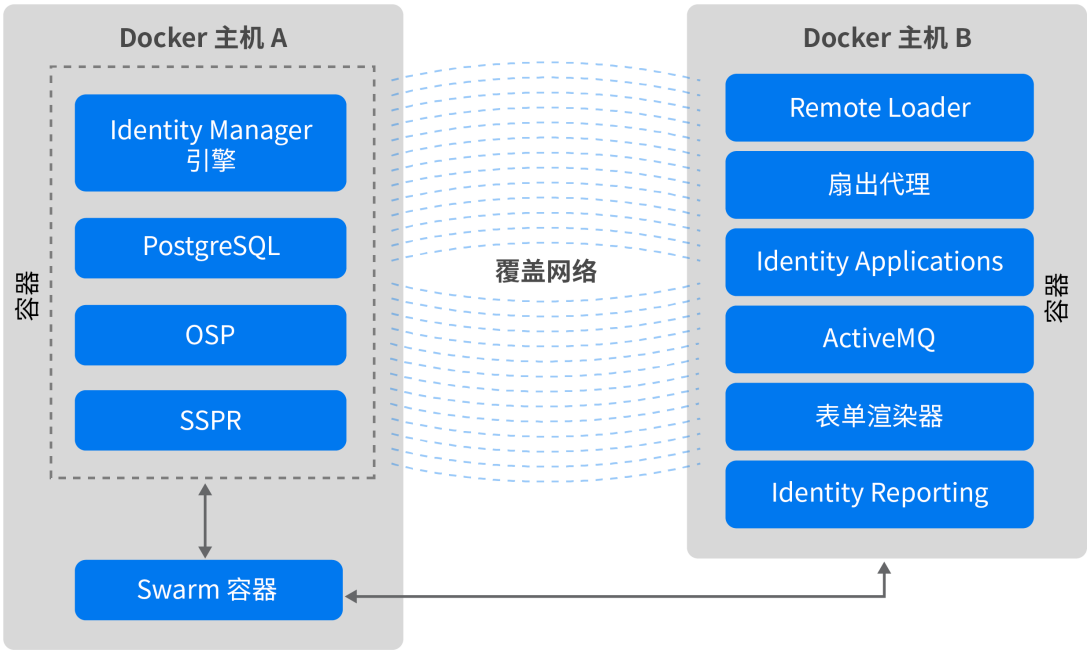
设置覆盖网络

NetIQ 建议您使用覆盖网络或桥接网络模式在分布式设置中部署所有 Identity Manager 容器。本指南中所述的方案特定于覆盖网络中的容器部署。但是，您也可以使用桥接网络来部署容器。在以下分布式服务器方案中， Identity Manager 引擎、 PostgreSQL、 OSP 和 SSPR 容器将部署在 Docker 主机 A 上。 Remote Loader、扇出代理、 Identity Applications、 ActiveMQ、表单渲染器和 Identity Reporting 容器将部署在 Docker 主机 B 上。

下图演示了部署在覆盖网络中两台 Docker 主机上的 Identity Manager 容器。

注释：由于不再支持群集储存，我们可以使用 Docker swarm 来设置覆盖网络。要详细了解弃用了哪些功能，请查看 “cluster store” （群集储存）(https://docs.docker.com/engine/deprecated/#classic-swarm-and-overlay-networks-using-cluster-store)。

图 18-1 *覆盖网络中的容器部署体系结构*



设置覆盖网络需要执行的步骤如下：

1 在 Docker 主机 A 上运行以下命令：

```
docker swarm init
```

2 记下基于步骤 1 的输出生成的 join 命令，然后在 Docker 主机 B 上运行此 join 命令，以便在这两台主机之间创建 swarm 网络。

例如：

```
docker swarm join --token SWMTKN-1-
24vozonapa4anwszd3ykthgomo84e9y3p3vbcrtibz6jzo94k2-
148g7yrnepmz963x3z5udnae4 10.71.142.191:2377
```

注释：如果您前面来不及记下用于连接工作节点的命令，请运行以下命令来获取该 join 命令：

```
docker swarm join-token worker
```

3 运行以下命令查看所有主机的状态：

```
docker node ls
```

4 使用以下命令在 Docker 主机 B 上创建覆盖网络：

```
docker network create --driver overlay --subnet=<subnet-cidr> --
gateway=<gateway-ip> --attachable <network-name>
```

例如：

```
docker network create --driver overlay --subnet=192.168.0.0/24 --
gateway=192.168.0.1 --attachable idmoverlaynetwork
```

5 运行以下命令校验是否已创建覆盖网络：

```
docker network ls
```

注释：由于 swarm 会动态指派 IP，因此在容器部署期间，请确保 swarm 负载平衡器使用尚未由任何 Identity Manager 组件占用的新 IP 地址，否则您可能会遇到以下错误：

来自守护程序的错误响应：挂接网络失败，请确保您的网络选项正确，并检查管理器日志：已超过环境期限

运行以下命令检查 swarm 负载平衡器的 IP：

```
docker inspect idmoverlaynetwork | grep lb-idmoverlaynetwork -A 7
```

先决条件

- 对于 Docker 部署中的所有 Docker 主机，必须使用主机上运行的所有容器的细节来更新该主机的 /etc/hosts 文件。确保所有容器的主机名仅采用完全限定的域名 (FQDN) 格式。

  所有组件的主机文件项可采用以下格式：

  < 容器的 IP> <FQDN> < 简称 >

  在本指南使用的示例部署中，于 /etc/hosts 文件中添加以下几项：

```
192.168.0.12     identityengine.example.com       identityengine
192.168.0.2      remoteloader.example.com         remoteloader
192.168.0.3      fanoutagent.example.com          fanoutagent
192.168.0.5      osp.example.com                  osp
192.168.0.6      postgresql.example.com           postgresql
192.168.0.7      identityapps.example.com         identityapps
192.168.0.8      formrenderer.example.com         formrenderer
192.168.0.9      activemq.example.com             activemq
192.168.0.10     identityreporting.example.com    identityreporting
192.168.0.11     sspr.example.com                 sspr
```

- 确保第三方 jar 文件为已装入的卷，这样每次启动容器时这些文件才可用。例如，如果容器的 `/opt/netiq/idm/apps/tomcat/lib` 目录中存在 `ojdbc.jar`，则您必须使用如下示例命令对 jar 文件进行卷装入操作：

  ```
  -v /host/ojdbc.jar:/opt/netiq/idm/apps/tomcat/lib/ojdbc.jar
  ```

- 必须在部署容器之前生成无提示属性文件。有关生成无提示属性文件的详细信息，请参见“创建无提示属性文件”（第 222 页）。

公开容器访问的端口

作为先决条件，您必须知道要用于容器的端口。您必须公开所需的端口，并将容器端口映射到 Docker 主机上的端口。下表根据指南中的示例提供了您必须在 Docker 主机上公开的端口的信息。

表 18-2 *根据示例部署公开的默认端口*

容器	根据示例部署假定使用的默认端口
Remote Loader	8090
扇出代理	不适用
OSP	8543
Identity Applications	18543
Identity Reporting	28543
表单渲染器	8600
ActiveMQ	• 8161 • 61616
PostgreSQL	5432
SSPR	8443 **注释：**SSRP 容器仅可在 8443 端口上运行。

不过，您可以根据自己的需要自定义端口。在公开端口时，请遵循以下注意事项：

- 确保您要公开的并非使用中的端口。
- 必须将容器端口映射到 Docker 主机上的相同端口。例如，必须将容器上的 8543 端口映射到 Docker 主机上的 8543 端口。

必须按以下顺序部署容器：

- “ 部署 Identity Manager 引擎容器 ”（第 238 页）
- “ 部署 Remote Loader 容器 ”（第 239 页）
- “ 部署扇出代理容器 ”（第 239 页）
- “ 部署 OSP 容器 ”（第 244 页）
- “ 部署 PostgreSQL 容器 ”（第 244 页）
- “ 部署 Identity Applications 容器 ”（第 245 页）
- “ 部署表单渲染器容器 ”（第 246 页）
- “ 部署 ActiveMQ 容器 ”（第 247 页）
- “ 部署 Identity Reporting 容器 ”（第 248 页）
- “ 部署 SSPR 容器 ”（第 248 页）

部署 Identity Manager 引擎容器

1. 生成无提示属性文件。有关详细信息，请参见 “ 创建无提示属性文件 ”。
2. 在解压缩 `Identity_Manager_4.9.0_Containers.tar.gz` 文件的位置，导航到 `Identity_Manager_4.9.0_Containers` 目录。
3. 运行以下命令装载映像：

   ```
   docker load --input IDM_490_identityengine.tar.gz
   ```

4. 使用以下命令部署容器：

   ```
   docker run --restart unless-stopped -d --ip=192.168.0.12 --
   network=idmoverlaynetwork --hostname=identityengine.example.com --
   name=engine-container -v /etc/hosts:/etc/hosts -v /data:/config -p
   8028:8028 -p 524:524 -p 389:389 -p 8030:8030 -p 636:636 -e
   SILENT_INSTALL_FILE=/config/silent.properties --stop-timeout 100
   identityengine:idm-4.9.0-580
   ```

5. 要校验是否已成功部署容器，请运行以下命令检查日志文件：

   ```
   tail -f /data/idm/log/idmconfigure.log
   ```

6. 要登录容器，请运行以下命令：

   ```
   docker exec -it < 容器 > < 命令 >
   ```

   例如：

   ```
   docker exec -it engine-container bash
   ```

注释：要运行 ndstrace 或 ndsrepair 等身份库实用程序，请以非 root 用户 nds 的身份登录到容器。如果您以 root 用户身份登录，则无法运行这些实用程序。要以 nds 用户身份登录到容器，请运行 docker exec -it engine-container sudo nds 命令。

部署 Remote Loader 容器

1 在解压缩 Identity_Manager_4.9.0_Containers.tar.gz 文件的位置，导航到 Identity_Manager_4.9.0_Containers 目录。

2 运行以下命令装载映像：

```
docker load --input IDM_490_remoteloader.tar.gz
```

3 使用以下命令部署容器：

```
docker run -d --ip=192.168.0.2 --network=idmoverlaynetwork --
hostname=remoteloader.example.com -p 8090:8090 --name=rl-container -v /
etc/hosts:/etc/hosts -v /data:/config remoteloader:idm-4.9.0-580
```

此命令会部署 64 位和 32 位版本的 Remote Loader。容器的 /opt/novell/eDirectory/lib/dirxml/classes/ 目录中提供了驱动程序文件。

4 （视情况而定）如果您不想在部署容器时使用配置文件，请使用以下命令部署容器：

```
docker run --restart unless-stopped -d --ip=192.168.0.2 --
network=idmoverlaynetwork --hostname=remoteloader.example.com -p
8090:8090 --name=rl-container -v /etc/hosts:/etc/hosts -v /data:/config
--stop-timeout 100 remoteloader:idm-4.9.0-580
```

5 要登录容器，请运行以下命令：

```
docker exec -it < 容器 > < 命令 >
```

例如：

```
docker exec -it rl-container bash
```

6 配置 Remote Loader。有关详细信息，请参见《*NetIQ Identity Manager Driver Administration Guide*》（NetIQ Identity Manager 驱动程序管理指南）中的 “Configuring the Remote Loader and Drivers”（配置 Remote Loader 和驱动程序）。

部署扇出代理容器

1 在解压缩 Identity_Manager_4.9.0_Containers.tar.gz 文件的位置，导航到 Identity_Manager_4.9.0_Containers 目录。

2 运行以下命令装载映像：

```
docker load --input IDM_490_fanoutagent.tar.gz
```

3 使用以下命令部署容器：

```
docker run --restart unless-stopped -d --ip=192.168.0.3 --
network=idmoverlaynetwork --hostname=fanoutagent.example.com --
name=foa-container -v /etc/hosts:/etc/hosts -v /data:/config --stop-
timeout 100 fanoutagent:idm-4.9.0-580
```

4 要登录容器，请运行以下命令：

```
docker exec -it < 容器 > < 命令 >
```

例如：

```
docker exec -it foa-container bash
```

5 配置扇出代理。有关详细信息，请参见《NetIQ Identity Manager Driver for JDBC Fanout Implementation Guide》（NetIQ Identity Manager Driver for JDBC Fanout 实施指南）(https://www.netiq.com/documentation/identity-manager-49-drivers/jdbc_fanout/data/netiq-identity-manager-for-jdbc-fan-out-driver-implementation-guide.html) 中的 “Configuring the Fanout Agent”（配置扇出代理）(https://www.netiq.com/documentation/identity-manager-49-drivers/jdbc_fanout/data/how-to-configure-fan-out-agent.html)。

通过身份库证书颁发机构生成证书

（视情况而定）仅当您使用身份库作为证书颁发机构时，本节内容才适用。

下列组件需要您先生成证书才能部署。在为以下组件生成证书之前，请务必先部署 Identity Manager 引擎容器。

- OSP
- Identity Applications
- Identity Reporting

生成 OSP 的证书

生成证书需要执行的步骤如下：

1 确保安装的 Java 版本为 Azul Zulu 1.8.0_392 或更高。

2 确保在 Docker 主机中设置 Java 路径。例如，运行以下命令：

```
export PATH=<java installed location>/bin:$PATH
```

例如：

```
export PATH=/opt/netiq/common/jre/bin/:$PATH
```

3 生成 PKCS 密钥存储区：

```
keytool -genkey -alias osp -keyalg RSA -storetype pkcs12 -keystore /
data/tomcat-osp.ks -validity 3650 -keysize 2048 -dname
"CN=osp.example.com" -keypass <password> -storepass <password>
```

4 生成证书签名请求：

```
keytool -certreq -v -alias osp -file /config/osp.csr -keypass
<password> -keystore /config/tomcat-osp.ks -storepass <password>
```

5 生成自我签名证书：

5a 起动 Identity Console 并登录。

5b 导航到**证书管理** > **颁发证书**。

5c 浏览到在步骤 3 中创建的 .csr 文件。例如 osp.csr。

5d 单击**打开**。

5e 在**密钥使用规范**下拉列表中指定密钥类型。

5f 在**扩展密钥使用规范**下拉列表中指定扩展密钥类型。

5g 对于证书类型，请在**基本约束**下拉列表中选择**未指定**。

5h 在**证书参数**下拉列表中指定证书的有效期。

5i 在**证书格式**下拉列表中选择**采用二进制 DER 格式的文件**。

5j 单击**下一步**。

5k 单击**确定**。

5l 下载证书并将其复制到 /data 目录。

6 导出 .der 格式的根证书：

6a 起动 Identity Console 并登录。

6b 导航到**证书管理** > **服务器证书管理**。

6c 选中 **SSL 证书 DNS** 复选框并单击**导出**。

6d 在**证书**下拉列表中选择 “ 组织 CA”。

6e 在**导出格式**下拉列表中选择 DER。

6f 单击**确定**。

6g 下载证书并将其复制到 /data 目录。

7 将证书导入到您在步骤 2 中创建的 PKCS 密钥存储区中：

```
keytool -import -trustcacerts -alias root -keystore /config/tomcat-osp.ks -file /config/cert.der -storepass < 口令 > -noprompt
```

```
keytool -import -alias osp -keystore /config/tomcat-osp.ks -file /config/osp.der -storepass < 口令 > -noprompt
```

注释：请确保指定为部署输入的路径中有密钥存储区。

生成 Identity Applications 的证书

生成证书需要执行的步骤如下：

1 确保安装的 Java 版本为 Azul Zulu 1.8.0_392 或更高。

2 请务必设置 Java 路径。例如，运行以下命令：

```
export PATH=<java installed location>/bin:$PATH
```

例如：

```
export PATH=/opt/netiq/common/jre/bin/:$PATH
```

3 生成 PKCS 密钥存储区：

```
keytool -genkey -alias ua -keyalg RSA -storetype pkcs12 -keystore /
config/tomcat-ua.ks -validity 3650 -keysize 2048 -dname
"CN=identityapps.example.com" -keypass <password> -storepass <password>
```

4 生成证书签名请求：

```
keytool -certreq -v -alias ua -file /config/ua.csr -keypass <password>
-keystore /config/tomcat-ua.ks -storepass <password>
```

5 生成自我签名证书：

5a 起动 Identity Console 并登录。

5b 导航到**证书管理** > **颁发证书**。

5c 浏览到在步骤 3 中创建的 `.csr` 文件。例如 `ua.csr`。

5d 单击**打开**。

5e 在**密钥使用规范**下拉列表中指定密钥类型。

5f 在**扩展密钥使用规范**下拉列表中指定扩展密钥类型。

5g 对于证书类型，请在**基本约束**下拉列表中选择**未指定**。

5h 在**证书参数**下拉列表中指定证书的有效期。

5i 在**证书格式**下拉列表中选择**采用二进制 DER 格式的文件**。

5j 单击**下一步**。

5k 单击**确定**。

5l 下载证书并将其复制到 `/data` 目录。

6 导出 `.der` 格式的根证书：

6a 起动 Identity Console 并登录。

6b 导航到**证书管理** > **服务器证书管理**。

6c 选中 **SSL 证书 DNS** 复选框并单击**导出**。

6d 在**证书**下拉列表中选择 “ 组织 CA”。

6e 在**导出格式**下拉列表中选择 `DER`。

6f 单击**确定**。

6g 下载证书并将其复制到 `/data` 目录。

7 将证书导入到步骤 2 中的 PKCS 密钥存储区：

```
keytool -import -trustcacerts -alias root -keystore /config/tomcat-
ua.ks -file /config/cert.der -storepass < 口令 > -noprompt
```

```
keytool -import -alias ua -keystore /config/tomcat-ua.ks -file /config/
ua.der -storepass < 口令 > -noprompt
```

注释：请确保指定为部署输入的路径中有证书。

生成 Identity Reporting 的证书

生成证书需要执行的步骤如下：

1 确保安装的 Java 版本为 Azul Zulu 1.8.0_392 或更高。

2 请务必设置 Java 路径。例如，运行以下命令：

```
export PATH=<java installed location>/bin:$PATH
```

例如：

```
export PATH=/opt/netiq/common/jre/bin/:$PATH
```

3 生成 PKCS 密钥存储区：

```
keytool -genkey -alias rpt -keyalg RSA -storetype pkcs12 -keystore /
config/tomcat-rpt.ks -validity 3650 -keysize 2048 -dname
"CN=identityreporting.example.com" -keypass <password> -storepass
<password>
```

4 生成证书签名请求：

```
keytool -certreq -v -alias rpt -file /config/rpt.csr -keypass
<password> -keystore /config/tomcat-rpt.ks -storepass <password>
```

5 生成自我签名证书：

5a 起动 Identity Console 并登录。

5b 导航到**证书管理** > **颁发证书**。

5c 浏览到在步骤 3 中创建的 `.csr` 文件。例如 `rpt.csr`。

5d 单击**打开**。

5e 在**密钥使用规范**下拉列表中指定密钥类型。

5f 在**扩展密钥使用规范**下拉列表中指定扩展密钥类型。

5g 对于证书类型，请在**基本约束**下拉列表中选择**未指定**。

5h 在**证书参数**下拉列表中指定证书的有效期。

5i 在**证书格式**下拉列表中选择**采用二进制 DER 格式的文件**。

5j 单击**下一步**。

5k 单击**确定**。

5l 下载证书并将其复制到 `/data` 目录。

6 导出 `.der` 格式的根证书：

6a 起动 Identity Console 并登录。

6b 导航到**证书管理** > **服务器证书管理**。

6c 选中 **SSL 证书 DNS** 复选框并单击**导出**。

6d 在**证书**下拉列表中选择 “ 组织 CA”。

6e 在**导出格式**下拉列表中选择 `DER`。

6f 单击**确定**。

6g 下载证书并将其复制到 `/data` 目录。

7 将证书导入到您在步骤 2 中创建的 PKCS 密钥存储区中：

```
keytool -import -trustcacerts -alias root -keystore /config/tomcat-rpt.ks -file /config/cert.der -storepass < 口令 > -noprompt
```

```
keytool -import -alias rpt -keystore /config/tomcat-rpt.ks -file /config/rpt.der -storepass < 口令 > -noprompt
```

注释：请确保指定为部署输入的路径中有证书。

部署 OSP 容器

注释：在部署 OSP 容器之前，请务必生成所需的证书。有关详细信息，请参见 “ 生成 OSP 的证书 ”。

1 生成无提示属性文件。有关详细信息，请参见 “ 创建无提示属性文件 ”。

2 在解压缩 Identity_Manager_4.9.0_Containers.tar.gz 文件的位置，导航到 Identity_Manager_4.9.0_Containers 目录。

3 运行以下命令装载映像：

```
docker load --input IDM_490_osp.tar.gz
```

4 使用以下命令部署容器：

```
docker run --restart unless-stopped -d --ip=192.168.0.5 --network=idmoverlaynetwork --hostname=osp.example.com -p 8543:8543 --name=osp-container -v /etc/hosts:/etc/hosts -v /data:/config -e SILENT_INSTALL_FILE=/config/silent.properties --stop-timeout 100 osp:idm-4.9.0-580
```

5 要校验是否已成功部署容器，请运行以下命令检查日志文件：

```
tail -f /data/osp/log/idmconfigure.log
```

6 要登录容器，请运行以下命令：

```
docker exec -it < 容器 > < 命令 >
```

例如：

```
docker exec -it osp-container bash
```

部署 PostgreSQL 容器

1 在解压缩 Identity_Manager_4.9.0_Containers.tar.gz 文件的位置，导航到 Identity_Manager_4.9.0_Containers 目录。

2 运行以下命令装载映像：

```
docker load --input IDM_490_postgres.tar.gz
```

3 在共享卷 data 下创建一个子目录，例如 postgres。

```
mkdir postgres
```

4 使用以下示例命令部署容器：

```
docker run --restart unless-stopped -d --ip=192.168.0.6 --
network=idmoverlaynetwork --hostname=postgresql.example.com --
name=postgresql-container -p 5432:5432 -e POSTGRES_PASSWORD=<password>
-v /data/postgres:/var/lib/postgresql/data -v /etc/hosts:/etc/hosts -v
/data:/config --stop-timeout 100 postgres:12.18
```

例如：

```
docker run --restart unless-stopped -d --ip=192.168.0.6 --
network=idmoverlaynetwork --hostname=postgresql.example.com --
name=postgresql-container -p 5432:5432 -e POSTGRES_PASSWORD=novell -v /
data/postgres:/var/lib/postgresql/data -v /etc/hosts:/etc/hosts -v /
data:/config --stop-timeout 100 postgres:12.18
```

5 创建 Identity Applications 的 idmdamin 用户。

```
docker exec -it postgresql-container psql -U postgres -c "CREATE USER
idmadmin WITH ENCRYPTED PASSWORD '<password>'"
```

6 创建 Identity Applications、工作流程和 Identity Reporting 数据库。

```
docker exec -it postgresql-container psql -U postgres -c "CREATE
DATABASE idmuserappdb"

docker exec -it postgresql-container psql -U postgres -c "CREATE
DATABASE igaworkflowdb"

docker exec -it postgresql-container psql -U postgres -c "CREATE
DATABASE idmrptdb"
```

注释：当您配置 Identity Applications 和 Identity Reporting 容器时，会用到这些数据库。

7 为 idmadmin 用户授予对数据库的所有特权：

```
docker exec -it postgresql-container psql -U postgres -c "GRANT ALL
PRIVILEGES ON DATABASE idmuserappdb TO idmadmin"

docker exec -it postgresql-container psql -U postgres -c "GRANT ALL
PRIVILEGES ON DATABASE igaworkflowdb TO idmadmin"
```

8 要登录容器，请运行以下命令：

```
docker exec -it < 容器 > < 命令 >
```

例如：

```
docker exec -it postgresql-container bash
```

部署 Identity Applications 容器

注释：在部署 Identity Applications 容器之前，请务必生成所需的证书。有关详细信息，请参见 “ 生成 Identity Applications 的证书 ”。

1 生成无提示属性文件。有关详细信息，请参见 “ 创建无提示属性文件 ”。

注释：将应用程序服务器端口的值指定为公开的端口 18543。

2 在解压缩 Identity_Manager_4.9.0_Containers.tar.gz 文件的位置，导航到 Identity_Manager_4.9.0_Containers 目录。

3 运行以下命令装载映像：

```
docker load --input IDM_490_identityapplication.tar.gz
```

4 使用以下命令部署容器：

```
docker run --restart unless-stopped -d --ip=192.168.0.7 --
network=idmoverlaynetwork --hostname=identityapps.example.com -p
18543:18543 --name=idapps-container -v /etc/hosts:/etc/hosts -v /data:/
config -e SILENT_INSTALL_FILE=/config/silent.properties --stop-timeout
100 identityapplication:idm-4.9.0-580
```

5 要校验是否已成功部署容器，请运行以下命令检查日志文件：

```
tail -f /data/userapp/log/idmconfigure.log
```

6 要登录容器，请运行以下命令：

```
docker exec -it < 容器 > < 命令 >
```

例如：

```
docker exec -it idapps-container bash
```

7 运行以下命令：

注释：在执行此步骤之前，请确保容器已成功部署。

```
/opt/netiq/common/jre/bin/keytool -importkeystore -srckeystore /config/
tomcat-osp.ks -srcstorepass <password> -destkeystore /opt/netiq/idm/
apps/tomcat/conf/idm.jks -deststorepass <password>
```

8 键入 yes 以覆盖 root 别名的项。

9 重启动 Identity Applications 容器。

```
docker restart idapps-container
```

注释：要在配置更新实用程序中修改任何设置，请从 Identity Applications 容器的 /opt/netiq/idm/apps/configupdate/ 目录起动 configupdate.sh。配置更新实用程序只能在控制台模式下起动。

部署表单渲染器容器

1 生成无提示属性文件。有关详细信息，请参见 “ 创建无提示属性文件 ”。

2 在解压缩 Identity_Manager_4.9.0_Containers.tar.gz 文件的位置，导航到 Identity_Manager_4.9.0_Containers 目录。

3 运行以下命令装载映像：

```
docker load --input IDM_490_formrenderer.tar.gz
```

4 使用以下命令部署容器：

```
docker run --restart unless-stopped -d --ip=192.168.0.8 --
network=idmoverlaynetwork --hostname=formrenderer.example.com -p
8600:8600 --name=fr-container -v /etc/hosts:/etc/hosts -v /data:/config
-e SILENT_INSTALL_FILE=/config/silent.properties --stop-timeout 100
formrenderer:idm-4.9.0-580
```

5 要登录容器，请运行以下命令：

```
docker exec -it < 容器 > < 命令 >
```

例如：

```
docker exec -it fr-container bash
```

部署 ActiveMQ 容器

1 生成无提示属性文件。有关详细信息，请参见“ 创建无提示属性文件 ”。

2 在解压缩 Identity_Manager_4.9.0_Containers.tar.gz 文件的位置，导航到 Identity_Manager_4.9.0_Containers 目录。

3 运行以下命令装载映像：

```
docker load --input IDM_490_activemq.tar.gz
```

4 使用以下命令部署容器：

```
docker run --restart unless-stopped -d --ip=192.168.0.9 --
network=idmoverlaynetwork --hostname=activemq.example.com -p
61616:61616 --name=amq-container -v /etc/hosts:/etc/hosts -v /data:/
config --env-file /data/silent.properties --stop-timeout 100
activemq:idm-4.9.0-580
```

5 要登录容器，请运行以下命令：

```
docker exec -it < 容器 > < 命令 >
```

例如：

```
docker exec -it amq-container bash
```

6 配置 ActiveMQ。有关详细信息，请参见《NetIQ Identity Manager Driver for JDBC Fanout Implementation Guide》（NetIQ Identity Manager Driver for JDBC Fanout 实施指南）(https://www.netiq.com/documentation/identity-manager-49-drivers/jdbc_fanout/data/how-to-setup-activemq-startup-service.html) 中的 *“Setting Up ActiveMQ Startup Service”（设置 ActiveMQ 启动服务）(https://www.netiq.com/documentation/identity-manager-49-drivers/jdbc_fanout/data/netiq-identity-manager-for-jdbc-fan-out-driver-implementation-guide.html)*。

部署 Identity Reporting 容器

注释：在部署 Identity Reporting 容器之前，请务必生成所需的证书。有关详细信息，请参见“生成 Identity Reporting 的证书”。

1 生成无提示属性文件。有关详细信息，请参见“创建无提示属性文件”。

注释：将应用程序服务器端口的值指定为公开的端口 28543。

2 在解压缩 `Identity_Manager_4.9.0_Containers.tar.gz` 文件的位置，导航到 `Identity_Manager_4.9_Containers` 目录。

3 运行以下命令装载映像：

```
docker load --input IDM_490_identityreporting.tar.gz
```

4 使用以下命令部署容器：

```
docker run --restart unless-stopped -d --ip=192.168.0.10 --
network=idmoverlaynetwork --hostname=identityreporting.example.com -p
28543:28543 --name=rpt-container -v /etc/hosts:/etc/hosts -v /data:/
config -e SILENT_INSTALL_FILE=/config/silent.properties --stop-timeout
100 identityreporting:idm-4.9.0-580
```

5 要校验是否已成功部署容器，请运行以下命令检查日志文件：

```
tail -f /data/reporting/log/idmconfigure.log
```

6 要登录容器，请运行以下命令：

```
docker exec -it < 容器 > < 命令 >
```

例如：

```
docker exec -it rpt-container bash
```

7 运行以下命令：

注释：在执行此步骤之前，请确保容器已成功部署。

```
/opt/netiq/common/jre/bin/keytool -importkeystore -srckeystore /config/
tomcat-osp.ks -srcstorepass <password> -destkeystore /opt/netiq/idm/
apps/tomcat/conf/idm.jks -deststorepass <password>
```

8 键入 `yes` 以覆盖 `root` 别名的项。

9 重启动 Identity Reporting 容器。

```
docker restart rpt-container
```

部署 SSPR 容器

部署 SSPR 容器需要执行的任务如下：

1 生成 SSPR 的无提示属性文件。在生成无提示属性文件时选择 **Identity Applications**。有关更多信息，请参见“创建无提示属性文件”。

2 在共享卷 data 下创建一个子目录，例如 sspr。

```
mkdir sspr
```

3 在解压缩 Identity_Manager_4.9.0_Containers.tar.gz 文件的位置，导航到 Identity_Manager_4.9.0_Containers 目录。

4 运行以下命令装载映像：

```
docker load --input IDM_490_sspr.tar.gz
```

5 使用以下示例命令部署容器：

```
docker run --restart unless-stopped -d --ip=192.168.0.11 --
network=idmoverlaynetwork --hostname=sspr.example.com --name=sspr-
container -v /etc/hosts:/etc/hosts -v /data/sspr:/config -p 8443:8443 -
-stop-timeout 100 sspr/sspr-webapp:4.7.0.1-580
```

6 在 Docker 主机上运行以下命令，以将 Docker 主机中的 silent.properties 文件复制到 SSPR 容器：

```
docker cp /data/silent.properties sspr-container:/tmp
```

7 将无提示属性文件装载到 SSPR 容器。

```
docker exec -it sspr-container /app/command.sh ImportPropertyConfig /
tmp/silent.properties
```

注释：检查是否在 SSPR 容器的 /config 目录下创建了 SSPRConfiguration.xml，并校验该文件的内容。

---

8 将 OAuth 证书导入 SSPR：

8a 在 Docker 主机上编辑 /data/sspr 目录中的 SSPRConfiguration.xml 文件，将 configIsEditable 标志的值设置为 **true** 并保存更改。

8b 起动浏览器并输入 https://sspr.example.com:8443/sspr URL。

8c 使用管理员身份凭证 （例如 uaadmin）登录。

8d 单击右上角的用户 （例如 uaadmin），然后单击**配置编辑器**。

8e 指定配置口令并单击**登录**。

8f 单击**设置** > **单点登录 (SSO) 客户端** > **OAuth**，确保所有 URL 都使用 HTTPS 协议和正确的端口。

8g 在 **OAuth 服务器证书**下，单击**从服务器导入**以导入新证书，然后单击**确定**。

8h 单击右上角的 保存证书。

8i 查看更改并单击**确定**。

8j SSPR 应用程序重启动之后，编辑 SSPRConfiguration.xml 文件，将 configIsEditable 标志的值设置为 **true** 并保存更改。

部署 Identity Console 容器

有关部署 Identity Console 容器的详细信息，请参见 Deploying Identity Console as Docker Container （将 Identity Console 部署为 Docker 容器）。

19 升级 Identity Manager 容器

本章提供有关更新 Identity Manager 各个容器的信息。

后续章节将会介绍容器更新过程。

- “ 容器更新先决条件 ”（第 251 页）
- “ 更新分布式服务器上的容器 ”（第 251 页）
- “ 更新单台服务器上的容器 ”（第 257 页）

容器更新先决条件

在更新每个 Identity Manager 容器之前，请执行以下步骤。

重要：本节不适用于 PostgreSQL 容器。有关更新 PostgreSQL 容器的信息，请参见 *“ 更新分布式服务器上的容器 ”（第 251 页）*一节中的 “ 更新 PostgreSQL 容器 ”，或 *“ 更新单台服务器上的容器 ”（第 257 页）*一节中的 “ 更新 PostgreSQL 容器 ”。

---

1 停止所有 Identity Manager 容器。

```
docker stop < 容器名称 >
```

例如：

```
docker stop engine-container
```

2 备份共享目录。本指南中的示例假设共享目录为 `/data`。

3 删除所有 Identity Manager 容器。

```
docker rm < 容器名称 >
```

例如：

```
docker rm engine-container
```

4 （视情况而定）删除所有已过时的 Docker 映像。

```
docker rmi < 映像 ID>
```

更新分布式服务器上的容器

必须按以下顺序更新容器：

- “ 更新 Identity Manager 引擎容器 ”（第 252 页）
- “ 更新 Remote Loader 容器 ”（第 252 页）
- “ 更新扇出代理容器 ”（第 253 页）
- “ 更新 OSP 容器 ”（第 253 页）

- “更新 PostgreSQL 容器”（第 254 页）
- “更新 Identity Applications 容器”（第 255 页）
- “更新表单渲染器容器”（第 255 页）
- “更新 ActiveMQ 容器”（第 255 页）
- “更新 Identity Reporting 容器”（第 256 页）
- “更新 SSPR 容器”（第 256 页）
- “更新 Identity Console 容器”（第 256 页）

更新 Identity Manager 引擎容器

1 在共享目录 /data 下创建包含以下内容的 credentials.properties 文件。

```
ID_VAULT_ADMIN_LDAP="<ID_VAULT_ADMIN_LDAP>"
ID_VAULT_PASSWORD="<ID_VAULT_PASSWORD>"
```

其中， ID_VAULT_ADMIN_LDAP 必须采用逗号分隔格式。

例如：

```
ID_VAULT_ADMIN_LDAP="cn=admin,ou=sa,o=system"

ID_VAULT_PASSWORD="novell"
```

2 导航到 Identity_Manager_4.9.0_Containers.tar.gz 文件的解压缩位置。

3 导航到 docker-images 目录。

4 运行以下命令装载映像：

```
docker load --input IDM_490_identityengine.tar.gz
```

5 如果您要使用覆盖网络部署 Identity Manager 引擎，请使用以下命令更新容器：

```
docker run --restart unless-stopped -d --ip=192.168.0.12 --
network=idmoverlaynetwork --hostname=identityengine.example.com --
name=engine-container -v /etc/hosts:/etc/hosts -v /data:/config -p
8028:8028 -p 524:524 -p 389:389 -p 8030:8030 -p 636:636 -e
SILENT_INSTALL_FILE=/config/credentials.properties --stop-timeout 100
identityengine:idm-4.9.0-580
```

如果您要使用主机网络部署 Identity Manager 引擎，请使用以下命令更新容器：

```
docker run --restart unless-stopped -d --network=host --name=engine-
container -v /etc/hosts:/etc/hosts -v /data:/config -e
SILENT_INSTALL_FILE=/config/credentials.properties --stop-timeout 100
identityengine:idm-4.9.0-580
```

更新 Remote Loader 容器

1 导航到 Identity_Manager_4.9.0_Containers.tar.gz 文件的解压缩位置。

2 导航到 docker-images 目录。

3 运行以下命令装载映像：

```
docker load --input IDM_490_remoteloader.tar.gz
```

4 运行以下命令部署容器：

```
docker run --restart unless-stopped -d --ip=192.168.0.2 --
network=idmoverlaynetwork --hostname=remoteloader.example.com -p
8090:8090 --name=rl-container -v /etc/hosts:/etc/hosts -v /data:/config
--stop-timeout 100 remoteloader:idm-4.9.0-580
```

容器的 /opt/novell/eDirectory/lib/dirxml/classes/ 目录中提供了驱动程序文件。

5 （视情况而定）如果 Remote Loader 实例未运行，请启动 Remote Loader 实例。

更新扇出代理容器

1 导航到 Identity_Manager_4.9.0_Containers.tar.gz 文件的解压缩位置。

2 导航到 docker-images 目录。

3 运行以下命令装载映像：

```
docker load --input IDM_490_fanoutagent.tar.gz
```

4 使用以下命令更新容器：

```
docker run --restart unless-stopped -d --ip=192.168.0.3 --
network=idmoverlaynetwork --hostname=fanoutagent.example.com --
name=foa-container -v /etc/hosts:/etc/hosts -v /data:/config --stop-
timeout 100 fanoutagent:idm-4.9.0-580
```

5 启动扇出代理。

更新 OSP 容器

1 导航到 Identity_Manager_4.9.0_Containers.tar.gz 文件的解压缩位置。

2 导航到 docker-images 目录。

3 运行以下命令装载映像：

```
docker load --input IDM_490_osp.tar.gz
```

4 使用以下命令更新容器：

```
docker run --restart unless-stopped -d --ip=192.168.0.5 --
network=idmoverlaynetwork --hostname=osp.example.com -p 8543:8543 --
name=osp-container -v /etc/hosts:/etc/hosts -v /data:/config --stop-
timeout 100 osp:idm-4.9.0-580
```

5 运行以下命令以登录容器：

```
docker exec -it <container> <command>
```

例如：

```
docker exec -it osp-container bash
```

更新 PostgreSQL 容器

注释：在更新 PostgreSQL 容器之前，请务必停止 Identity Applications 和 / 或 Identity Reporting 等依赖容器。

1. 在 Docker 主机上，导航到任意位置。例如：

   ```
   cd /tmp
   ```

2. 运行以下命令备份现有的 PostgreSQL 容器数据。

   ```
   docker exec postgresql-container pg_dumpall -U postgres > dump.sql
   ```

3. 停止 PostgreSQL 容器。

   ```
   docker stop <container name>
   ```

   例如：

   ```
   docker stop postgresql-container
   ```

4. 删除 PostgreSQL 容器。

   ```
   docker rm < 容器名称 >
   ```

5. 删除现有的 PostgreSQL 数据目录。

   ```
   rm -rf /data/postgres
   ```

6. （视情况而定）删除 PostgreSQL Docker 映像。

   ```
   docker rmi < 映像 ID>
   ```

7. 在共享目录 `/data` 下创建一个子目录，例如 `postgres`。

   ```
   mkdir postgres
   ```

8. 导航到 `Identity_Manager_4.9.0_Containers.tar.gz` 文件的解压缩位置。

9. 导航到 `docker-images` 目录。

10. 运行以下命令装载映像：

    ```
    docker load --input IDM_490_postgres.tar.gz
    ```

11. 使用以下命令更新容器：

    ```
    docker run --restart unless-stopped -d --ip=192.168.0.6 --
    network=idmoverlaynetwork --hostname=postgresql.example.com --
    name=postgresql-container -p 5432:5432 -e POSTGRES_PASSWORD=<password>
    -v /data/postgres:/var/lib/postgresql/data -v /etc/hosts:/etc/hosts -v
    /data:/config --stop-timeout 100 postgres:12.18
    ```

    例如：

    ```
    docker run --restart unless-stopped -d --ip=192.168.0.6 --
    network=idmoverlaynetwork --hostname=postgresql.example.com --
    name=postgresql-container -p 5432:5432 -e POSTGRES_PASSWORD=novell -v /
    data/postgres:/var/lib/postgresql/data -v /etc/hosts:/etc/hosts -v /
    data:/config --stop-timeout 100 postgres:12.18
    ```

12. 将您在 Docker 主机上备份的数据文件 （步骤 2）复制到新的 PostgreSQL `data` 目录。

```
cp /tmp/dump.sql /data/postgres
```

13 运行以下命令以登录容器：

```
docker exec -it <container> <command>
```

例如：

```
docker exec -it postgresql-container bash
```

14 导航到 /var/lib/postgresql/data/ 目录。

15 将在步骤 2 中备份的数据恢复到新的 PostgreSQL 容器。

```
psql -U postgres < dump.sql >
```

16 运行以下命令退出容器。

```
exit
```

更新 Identity Applications 容器

1 导航到 Identity_Manager_4.9.0_Containers.tar.gz 文件的解压缩位置。

2 导航到 docker-images 目录。

3 运行以下命令装载映像：

```
docker load --input IDM_490_identityapplication.tar.gz
```

4 使用以下命令更新容器：

```
docker run --restart unless-stopped -d --ip=192.168.0.7 --
network=idmoverlaynetwork --hostname=identityapps.example.com -p
18543:18543 --name=idapps-container -v /etc/hosts:/etc/hosts -v /data:/
config --stop-timeout 100 identityapplication:idm-4.9.0-580
```

更新表单渲染器容器

1 导航到 Identity_Manager_4.9.0_Containers.tar.gz 文件的解压缩位置。

2 导航到 docker-images 目录。

3 运行以下命令装载映像：

```
docker load --input IDM_490_formrenderer.tar.gz
```

4 使用以下命令更新容器：

```
docker run --restart unless-stopped -d --ip=192.168.0.8 --
network=idmoverlaynetwork --hostname=formrenderer.example.com -p
8600:8600 --name=fr-container -v /etc/hosts:/etc/hosts -v /data:/config
--stop-timeout 100 formrenderer:idm-4.9.0-580
```

更新 ActiveMQ 容器

1 导航到 Identity_Manager_4.9.0_Containers.tar.gz 文件的解压缩位置。

2 导航到 docker-images 目录。

3 运行以下命令装载映像：

```
docker load --input IDM_490_activemq.tar.gz
```

4 使用以下命令更新容器：

```
docker run --restart unless-stopped -d --ip=192.168.0.9 --
network=idmoverlaynetwork --hostname=activemq.example.com -p
61616:61616 --name=amq-container -v /etc/hosts:/etc/hosts -v /data:/
config --stop-timeout 100 activemq:idm-4.9.0-580
```

更新 Identity Reporting 容器

1 导航到 Identity_Manager_4.9.0_Containers.tar.gz 文件的解压缩位置。

2 导航到 docker-images 目录。

3 运行以下命令装载映像：

```
docker load --input IDM_490_identityreporting.tar.gz
```

4 使用以下命令更新容器：

```
docker run --restart unless-stopped -d --ip=192.168.0.10 --
network=idmoverlaynetwork --hostname=identityreporting.example.com -p
28543:28543 --name=rpt-container -v /etc/hosts:/etc/hosts -v /data:/
config --stop-timeout 100 identityreporting:idm-4.9.0-580
```

更新 SSPR 容器

1 导航到 Identity_Manager_4.9.0_Containers.tar.gz 文件的解压缩位置。

2 导航到 docker-images 目录。

3 运行以下命令装载映像：

```
docker load --input IDM_490_sspr.tar.gz
```

4 使用以下命令更新容器：

```
docker run --restart unless-stopped -d --ip=192.168.0.11 --
network=idmoverlaynetwork --hostname=sspr.example.com --name=sspr-
container -v /etc/hosts:/etc/hosts -v /data/sspr:/config -p 8443:8443 -
-stop-timeout 100 sspr/sspr-webapp:4.7.0.1-580
```

更新 Identity Console 容器

有关更新 Identity Console 容器的详细信息，请参见 Upgrading Identity Console As Docker Container （将 Identity Console 升级为 Docker 容器）。

更新单台服务器上的容器

必须按以下顺序更新容器：

- “ 更新 Identity Manager 引擎容器 ”（第 257 页）
- “ 更新 Remote Loader 容器 ”（第 257 页）
- “ 更新扇出代理容器 ”（第 258 页）
- “ 更新 OSP 容器 ”（第 258 页）
- “ 更新 PostgreSQL 容器 ”（第 259 页）
- “ 更新 Identity Applications 容器 ”（第 260 页）
- “ 更新表单渲染器容器 ”（第 260 页）
- “ 更新 ActiveMQ 容器 ”（第 260 页）
- “ 更新 Identity Reporting 容器 ”（第 261 页）
- “ 更新 SSPR 容器 ”（第 261 页）
- “ 更新 Identity Console 容器 ”（第 261 页）

更新 Identity Manager 引擎容器

1 在共享目录 `/data` 下创建包含以下内容的 `credentials.properties` 文件。

```
ID_VAULT_ADMIN_LDAP="<ID_VAULT_ADMIN_LDAP>"
ID_VAULT_PASSWORD="<ID_VAULT_PASSWORD>"
```

其中， `ID_VAULT_ADMIN_LDAP` 必须采用逗号分隔格式。

例如：

```
ID_VAULT_ADMIN_LDAP="cn=admin,ou=sa,o=system"

ID_VAULT_PASSWORD="novell"
```

2 导航到 `Identity_Manager_4.9.0_Containers.tar.gz` 文件的解压缩位置。

3 导航到 `docker-images` 目录。

4 运行以下命令装载映像：

```
docker load --input IDM_490_identityengine.tar.gz
```

5 使用以下命令更新容器：

```
docker run --restart unless-stopped -d --network=host --name=engine-
container -v /etc/hosts:/etc/hosts -v /data:/config -e
SILENT_INSTALL_FILE=/config/credentials.properties --stop-timeout 100
identityengine:idm-4.9.0-580
```

更新 Remote Loader 容器

1 导航到 `Identity_Manager_4.9.0_Containers.tar.gz` 文件的解压缩位置。

2 导航到 `docker-images` 目录。

3 运行以下命令装载映像：

```
docker load --input IDM_490_remoteloader.tar.gz
```

4 使用以下命令更新容器：

```
docker run --restart unless-stopped -d --network=host --name=<container
name> -v /data:/config --stop-timeout 100 remoteloader:idm-4.9.0-580
```

例如：

```
docker run --restart unless-stopped -d --network=host --name=rl-
container -v /data:/config --stop-timeout 100 remoteloader:idm-4.9.0-
580
```

容器的 /opt/novell/eDirectory/lib/dirxml/classes/ 目录中提供了驱动程序文件。

5 （视情况而定）如果 Remote Loader 实例未运行，请启动 Remote Loader 实例。

更新扇出代理容器

1 导航到 Identity_Manager_4.9.0_Containers.tar.gz 文件的解压缩位置。

2 导航到 docker-images 目录。

3 运行以下命令装载映像：

```
docker load --input IDM_490_fanoutagent.tar.gz
```

4 使用以下命令更新容器：

```
docker run --restart unless-stopped -d --network=host --name=foa-
container -v /data:/config --stop-timeout 100 fanoutagent:idm-4.9.0-580
```

5 启动扇出代理。

更新 OSP 容器

1 导航到 Identity_Manager_4.9.0_Containers.tar.gz 文件的解压缩位置。

2 导航到 docker-images 目录。

3 运行以下命令装载映像：

```
docker load --input IDM_490_osp.tar.gz
```

4 使用以下命令更新容器：

```
docker run --restart unless-stopped -d --network=host --name=osp-
container -v /data:/config --stop-timeout 100 osp:idm-4.9.0-580
```

5 运行以下命令以登录容器：

```
docker exec -it <container> <command>
```

例如：

```
docker exec -it osp-container bash
```

更新 PostgreSQL 容器

注释：在更新 PostgreSQL 容器之前，请务必停止 Identity Applications 和 / 或 Identity Reporting 等依赖容器。

1 在 Docker 主机上，导航到任意位置。例如：

```
cd /tmp
```

2 运行以下命令备份现有的 PostgreSQL 容器数据。

```
docker exec postgresql-container pg_dumpall -U postgres > dump.sql
```

3 停止 PostgreSQL 容器。

```
docker stop < 容器名称 >
```

例如：

```
docker stop postgresql-container
```

4 删除 PostgreSQL 容器。

```
docker rm < 容器名称 >
```

5 删除现有的 PostgreSQL 数据目录。

```
rm -rf /data/postgres
```

6 （视情况而定）删除 PostgreSQL Docker 映像。

```
docker rmi < 映像 ID>
```

7 在共享目录 `/data` 下创建一个子目录，例如 `postgres`。

```
mkdir postgres
```

8 导航到 `Identity_Manager_4.9.0_Containers.tar.gz` 文件的解压缩位置。

9 导航到 `docker-images` 目录。

10 运行以下命令装载映像：

```
docker load --input IDM_490_postgres.tar.gz
```

11 使用以下命令更新容器：

```
docker run --restart unless-stopped -d --network=host --
name=postgresql-container -e POSTGRES_PASSWORD=<password> -v /data/
postgres:/var/lib/postgresql/data --stop-timeout 100 postgres:12.18
```

例如：

```
docker run --restart unless-stopped -d --network=host --
name=postgresql-container -e POSTGRES_PASSWORD=novell -v /data/
postgres:/var/lib/postgresql/data --stop-timeout 100 postgres:12.18
```

12 将您在 Docker 主机上备份的数据文件 （步骤 2）复制到新的 PostgreSQL `data` 目录。

```
cp /tmp/dump.sql /data/postgres
```

13 运行以下命令以登录容器：

```
docker exec -it <container> <command>
```

例如：

```
docker exec -it postgresql-container bash
```

14 导航到 /var/lib/postgresql/data/ 目录。

15 将在步骤 2 中备份的数据恢复到新的 PostgreSQL 容器。

```
psql -U postgres < dump.sql
```

16 运行以下命令退出容器。

```
exit
```

更新 Identity Applications 容器

1 导航到 Identity_Manager_4.9.0_Containers.tar.gz 文件的解压缩位置。

2 导航到 docker-images 目录。

3 运行以下命令装载映像：

```
docker load --input IDM_490_identityapplication.tar.gz
```

4 使用以下命令更新容器：

```
docker run --restart unless-stopped -d --network=host --name=idapps-
container -v /data:/config --stop-timeout 100 identityapplication:idm-
4.9.0-580
```

更新表单渲染器容器

1 导航到 Identity_Manager_4.9.0_Containers.tar.gz 文件的解压缩位置。

2 导航到 docker-images 目录。

3 运行以下命令装载映像：

```
docker load --input IDM_490_formrenderer.tar.gz
```

4 使用以下命令更新容器：

```
docker run --restart unless-stopped -d --network=host --name=fr-
container -v /data:/config --stop-timeout 100 formrenderer:idm-4.9.0-
580
```

更新 ActiveMQ 容器

1 导航到 Identity_Manager_4.9.0_Containers.tar.gz 文件的解压缩位置。

2 导航到 docker-images 目录。

3 运行以下命令装载映像：

```
docker load --input IDM_490_activemq.tar.gz
```

4 使用以下命令更新容器：

```
docker run --restart unless-stopped -d --network=host --name=amq-
container -v /data:/config --stop-timeout 100 activemq:idm-4.9.0-580
```

更新 Identity Reporting 容器

1. 导航到 `Identity_Manager_4.9.0_Containers.tar.gz` 文件的解压缩位置。
2. 导航到 `docker-images` 目录。
3. 运行以下命令装载映像：

   ```
   docker load --input IDM_490_identityreporting.tar.gz
   ```

4. 使用以下命令更新容器：

   ```
   docker run --restart unless-stopped -d --network=host --name=rpt-container -v /data:/config --stop-timeout 100 identityreporting:idm-4.9.0-580
   ```

更新 SSPR 容器

1. 导航到 `Identity_Manager_4.9.0_Containers.tar.gz` 文件的解压缩位置。
2. 导航到 `docker-images` 目录。
3. 运行以下命令装载映像：

   ```
   docker load --input IDM_490_sspr.tar.gz
   ```

4. 使用以下命令更新容器：

   ```
   docker run --restart unless-stopped -d --network=host --name=sspr-container -v /data/sspr:/config --stop-timeout 100 sspr/sspr-webapp:4.7.0.1-580
   ```

更新 Identity Console 容器

有关更新 Identity Console 容器的详细信息，请参见 Upgrading Identity Console As Docker Container （将 Identity Console 升级为 Docker 容器）。

VIII 使用 Ansible 部署 Identity Manager 容器

此 Identity Manager 版本支持使用 Ansible 部署 Identity Manager 容器。使用 Ansible 部署方法可以通过自动化过程轻松部署容器。部署过程更简单且更省时。 Identity Manager 随附了用于自动完成容器部署的 Ansible 战略规划书。

本章提供有关通过 Ansible 部署容器的说明。

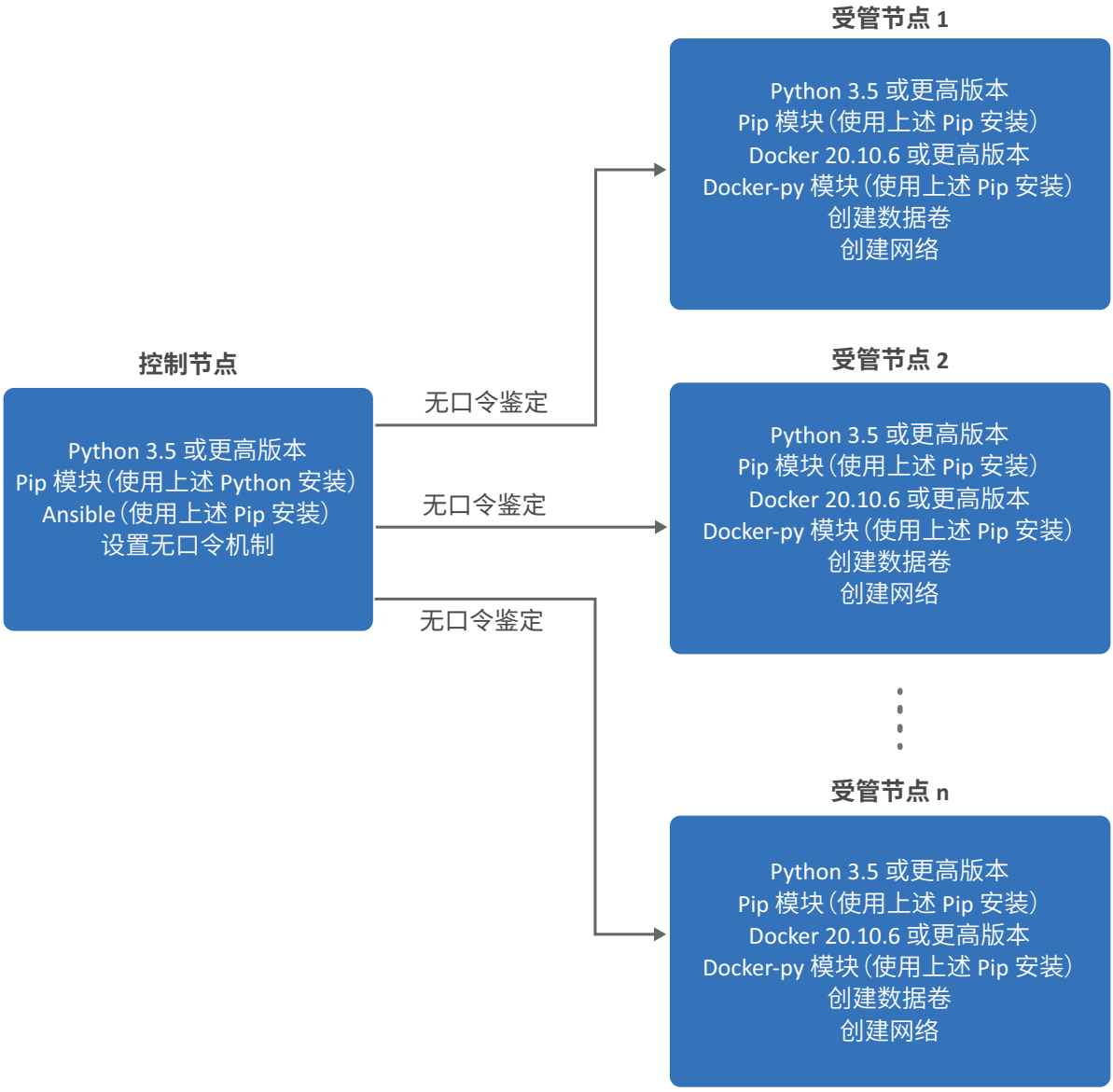
20 规划部署

在部署容器之前，需要做出一些规划并满足先决条件。本节提供有关规划部署的细节。

确定两台或更多服务器用于基于 Ansible 的容器部署。其中一台服务器称为 Ansible 控制节点，其余服务器称为受管节点。有关控制节点和受管节点的更多细节，请参见 Ansible (https://docs.ansible.com/ansible/latest/network/getting_started/basic_concepts.html#basic-concepts) 文档。

准备 Ansible 节点

在开始部署之前，必须确保已适当设置 Ansible 节点。控制节点和受管节点的先决条件各不相同。下图概括性地说明了如何准备控制节点和受管节点。



准备控制节点

确保在控制节点上执行以下任务：

- 确保已安装 Python3 或更高版本。要检查 Python 版本，请导航到 `/usr/bin/` 目录并运行以下命令：

  例如：

  ```
  python3 --version
  ```

  有关详细信息，请参见 Python 文档。
- 确保已安装 pip。要检查 pip 版本，请运行以下命令：

  例如：

  ```
  pip --version
  ```

确保已通过先前安装的 Python3 或更高版本安装了 `pip`。

有关详细信息，请参见 Python 文档。

- 运行以下命令，以使用 pip 安装 Docker 模块：

  例如：

  ```
  pip install docker
  ```

  确保 Docker 版本为 20.10.6 或更高。有关详细信息，请参见 Docker 文档。

- 使用先前安装的 pip 安装 Ansible。确保安装 Ansible 2.10.5 或更高版本。

  例如：

  ```
  pip install ansible
  ```

  有关详细信息，请参见 Ansible (https://docs.ansible.com/ansible/latest/installation_guide/intro_installation.html#installing-ansible-with-pip) 文档。

- 确保可从控制节点访问受管节点。例如，可以使用 `ping` 或任何相关机制来确保可访问这些节点。
- 确保在部署中的控制节点与所有受管节点之间建立无口令鉴定。请执行下列步骤：
  1. 生成 SSH 密钥。

     例如：

     ```
     ssh-keygen
     ```

  2. 不要输入任何口令，而是继续生成密钥。
  3. 运行以下命令启用对受管节点的无口令鉴定：

     ```
     ssh-copy-id root@< 受管节点的 FQDN 或 IP 地址 >
     ```

     例如：

     ```
     ssh-copy-id root@192.168.0.25
     ```

  4. 指定受管节点的口令。

     例如， `password`。

  5. 测试与受管节点的连接：

     ```
     ssh 'root@< 受管节点的 FQDN 或 IP 地址 >'
     ```

     例如：

     ```
     ssh 'root@<192.168.0.25>'
     ```

准备受管节点

确保在所有受管节点上执行以下任务：

- 确保已安装 Python3 或更高版本。要检查 Python 版本，请导航到 `/usr/bin/` 目录并运行以下命令：

  例如：

  ```
  python3 --version
  ```

  有关详细信息，请参见 Python 文档。

- 确保已安装 pip。要检查 pip 版本，请运行以下命令：

  例如：

  ```
  pip --version
  ```

  确保已通过先前安装的 Python3 或更高版本安装了 `pip`。

  有关详细信息，请参见 Python 文档。
- 安装 Docker。确保 Docker 版本为 20.10.6 或更高。有关详细信息，请参见 Docker 文档。
- 使用 pip 安装 Docker python 模块：

  例如：

  ```
  pip install docker-py
  ```
- 创建共享目录。有关更多信息，请参见“管理容器卷数据”（第 222 页）。

创建 setup.csv 文件

`setup.csv` 文件是部署容器时 Ansible 将要使用的输入文件。 Identity Manager 将 `setup.csv` 文件的默认模板捆绑在 Identity Manager 容器 tar 文件中。

`setup.csv` 文件的默认模板位于 `/< 容器 tar 文件解压缩到的位置 >/ansible/input/` 目录。您可以根据要求编辑 setup.csv 文件。

以下章节介绍了 `setup.csv` 文件包含的参数，以及每个参数的用途：

- **组件：**指示您要部署的容器。例如 `engine`。
- **部署：**指示您是否要部署容器。支持的值为 **yes** 和 **no**。
- **DockerHost：**指示容器要部署到的 Docker 主机。换言之，它可以是您为部署确定的任何受管节点。例如 `DockerHostA`
- **IP 地址：**指示容器要部署到的 Docker 主机的 IP 地址。例如 `192.168.0.15`
- **ContainerName：**指示容器的名称。例如 `engine-container`。
- **ContainerHostname：**指示容器要部署到的 Docker 主机或服务器的主机名。 NetIQ 建议您以 FQDN 格式指定主机名。例如 `identityengine.example.com`。
- **ExposedPorts：**指示您要为容器公开的侦听端口。例如， 636.

  注释：确保为每个容器公开唯一端口，并指定您在创建 `silent.properties` 文件时提供的相同端口。例如，您可以参考表 18-2 （第 237 页）中提供的示例端口来规划要公开的端口。

- **FileMounting：**指示任何自定义文件 （例如 `ojdbc.jar`）的路径。例如 `/opt/novell/eDirectory/lib/dirxml/classes/ojdbc.jar`。

  注释：
  - 如果有多个值，请以空格分隔的变量列表形式指定这些值。例如 `/opt/novell/eDirectory/lib/dirxml/classes/ojdbc.jar /opt/novell/eDirectory/lib/dirxml/classes/mssql.jar`

- （视情况而定）仅当您已在 `Deploy` 列中将 Core DNS 容器的值设置为 **no** 时，此参数才适用。

  确保已在 FileMounting 字段中映射 `hosts` 文件。例如 `/etc/hosts`。

- **SharedVolume**：指示您要让容器用来保存数据的共享目录。例如， `/data`。需要跨 Docker 主机创建此目录。

21 部署容器

执行以下步骤部署容器：

1 在控制节点上执行以下步骤：

1a 下载并解压缩 Identity Manager 容器 tar 文件。有关更多信息，请参见 “ 获取 Docker 映像 ”（第 219 页）。

1b 导航到 /<tar 文件解压缩到的位置 >/docker-images/ 目录。

1c 复制 IDM_490_idm_conf_generator.tar.gz 文件并将其放在任一受管节点上。

2 在任一受管节点上执行以下步骤：

2a 将在步骤 1c 中复制的 IDM_490_idm_conf_generator.tar.gz 文件放在任意位置。例如 /home。

2b 创建 silent.properties 文件。有关更多信息，请参见 “ 创建无提示属性文件 ”（第 222 页）。

3 在控制节点上执行以下步骤：

3a 导航到 /<tar 文件解压缩到的位置 >/ansible/input/ 目录并在其中放置以下文件：

- 在步骤 2b 中创建的 silent.properties 文件
- 在 “ 创建 setup.csv 文件 ”（第 268 页）一节中创建的 setup.csv 文件
- 从外部证书颁发机构获取的任何自定义证书

注释：如果您使用身份库作为生成证书的证书颁发机构，请执行 “ 通过身份库证书颁发机构生成证书 ”（第 240 页）中所述的步骤。

- 任何自定义文件，例如 ojdbc.jar 或自定义 LDIF 文件

注释：确保在 setup.csv 文件的 FileMounting 列中指定这些文件的目标路径。有关更多信息，请参见 “ 创建 setup.csv 文件 ”（第 268 页）。

3b 导航到 /<tar 文件解压缩到的位置 >/ansible/ 目录。

3c （可选）此步骤适用于高级用户。查看用于部署的 ansible.cfg 文件。

3d 运行以下命令来部署 setup.yml 战略规划书：

```
ansible-playbook setup.yml
```

3e （可选）此步骤适用于高级用户。查看用于部署的 idminventory.ini 文件。

3f 运行以下命令来部署 deploy.yml 战略规划书：

```
ansible-playbook deploy.yml -e 'network_set=<Docker 网络名称 >'
```

例如：

```
ansible-playbook deploy.yml -e 'network_set=idmoverlaynetwork'
```

22 部署后任务

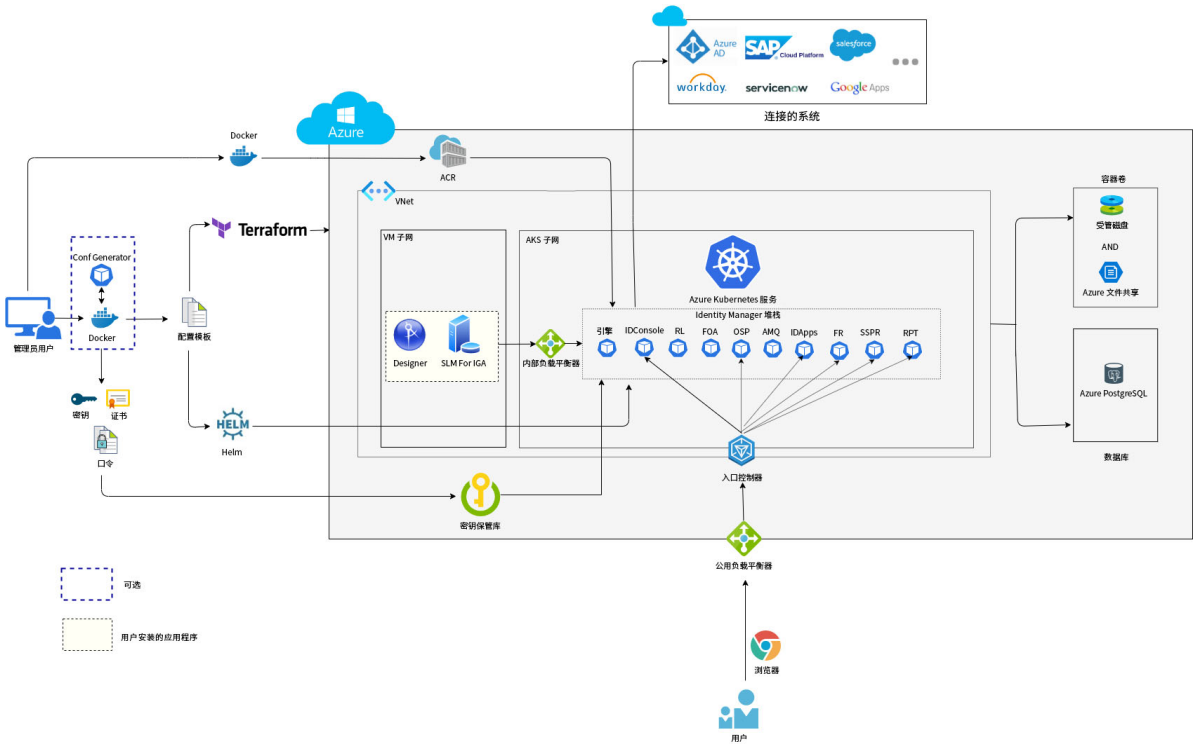
完成 Identity Manager 容器的部署后，必须执行某些任务才能确保 Identity Manager 解决方案在您的环境中正常运行。

必须将 OAuth 证书导入 SSPR。有关详细信息，请参见 “ 部署 SSPR 容器 ”（第 248 页）一节的步骤 8。

IX 在 Microsoft Azure Kubernetes 服务上部署 Identity Manager 容器

此版本允许您在 Microsoft Azure Kubernetes 服务上部署 Identity Manager 容器。可以借助 Terraform 和 Helm 图表来自动完成 Identity Manager 容器部署。

下图提供了在 Azure 上部署容器的体系结构视图。



- `ACRcreate.sh` 文件创建新的 Azure 容器注册表，并允许用户在 Azure 门户中上载 / 储存 Docker 映像。
- Identity Manager 配置生成器映像用于完成下列任务：
  - 生成配置文件 （Terraform 文件和 Helm 图表）。
  - 创建 Azure 资源组。
  - 在 Azure 资源组下创建密钥保管库。
  - 将所有敏感信息推送到密钥保管库。
- 用户可以使用 Terraform 脚本设置基础结构，例如：
  - 网络创建。

    - Azure PostgreSQL （可选）。
    - Azure Kubernetes 服务 (AKS)。
- 用户可以使用 Helm 图表在 Azure Kubernetes 群集内部署 Identity Manager 容器。
- NGINX 入口控制器充当反向代理，用于访问 AKS 群集内运行的 Identity Manager Web 应用程序 （包括 Identity Applications、 Identity Reporting 和 Identity Console 等）。
    - 需要购买单个域 （例如 `identitymanager.eastus.cloudapp.azure.com`）。
    - 该域将指派到 Nginx 入口控制器。
- 内部负载平衡器用于引擎 Docker 主机与 Kubernetes 群集之间的内部通讯。
- 持久储存是动态创建的，将会装入到整个基础结构。
- 可将 Identity Applications 和 Identity Reporting 配置为使用 Azure 提供的 Azure PostgreSQL 数据库。
- 用于 Identity Governance 管理的 Designer 和 Sentinel Log Management (SLM) 应在 Terraform 执行完成后由用户手动部署。

概述

要规划 Azure Kubernetes 群集上的 Identity Manager 容器部署，请参见以下章节：

- 第 23 章 “ 规划部署 ”（第 277 页）
- 第 24 章 “ 准备部署 ”（第 281 页）
- 第 25 章 “ 部署过程 ”（第 283 页）
- 第 26 章 “ 部署后任务 ”（第 303 页）
- 第 27 章 “ 维护 Identity Manager 容器的部署 ”（第 305 页）

23 规划部署

本章将指导您完成部署规划过程，并提供在 Azure 上部署容器所要满足的先决条件列表。

Identity Manager 容器部署过程需要以下 Azure 资源：

1 确保您的 Azure 帐户拥有创建基础结构所需的读写许可权限。

1a Azure Kubernetes 服务 (AKS)。

1b 网络创建。

1c （可选） Azure PostgreSQL。

注释：这些元素由 Terraform 部署脚本创建。

注释：在部署之前，请确保资源各有差异，并且尚未为您的 Azure 帐户创建 Identity Manager 配置文件。

2 购买一个域以访问 Identity Manager 中的不同应用程序。

您可以在相应的资源组中使用自己的域。例如 `identitymanager.eastus.cloudapp.azure.com`。

注释：对于上面的示例， **eastus** 表示位置， **cloudapp.azure.com** 表示一般的 Azure 后缀域。

3 从任一证书颁发机构 (CA) 获取域的 SSL 证书 （`.crt` 和 `.key` 文件）。

4 （可选）在命令行界面中运行以下命令，生成您自己的自我签名证书：

```
openssl req -new -newkey rsa:2048 -nodes -keyout domain.key -out
domain.csr
```

4a 为以下提示指定输入：

表 23-1

Prompt	说明
国家 / 地区名称 （双字母代码）	使用双字母代码指定国家 / 地区名称。
州或省名称	指定州或省 / 自治区 / 直辖市的全名。
地区名称	指定市名。
组织名称	指定组织名称。例如 Internet Widgits Pty Ltd。
组织单元名	指定组织单位名称。例如 section。
通用名称	指定服务器完全限定的域名 (FQDN)。例如 `identitymanager.eastus.cloudapp.azure.com`。
电子邮件地址	指定您的电子邮件地址。
询问口令	指定唯一口令。
可选的公司名称	指定可选的公司名称。

4b 运行以下命令将私用密钥转换为 RSA 格式：

```
openssl rsa -in domain.key -out tls.key
```

4c 执行以下步骤获取根证书。

4c1 登录到 `https://<IP 地址或主机名 >:9000/identityconsole/#/`。

4c2 导航到**证书管理** > **服务器证书管理**。

4c3 单击**导出**。

4c4 在 “ 证书 ” 下拉列表中选择**组织 CA**。

4c5 在 “ 导出格式 ” 下拉列表中选择 **BASE64**。

4c6 单击**确定**。

4c7 单击**保存导出的证书**。

4d 执行以下步骤，将您的 CSR 提交到证书颁发机构 (CA) 并获取签名的服务器证书。

4d1 登录到 `https://<IP 地址或主机名 >:9000/identityconsole/#/`。

4d2 导航到**证书管理** > **颁发证书**。

4d3 单击**选择文件**，上载在**步骤 4b （第 278 页）**中生成的 < 域 >.csr 文件。

4d4 在**证书参数**下拉列表中选择有效期。例如 “ 最大 ”。

4d5 在**证书格式**下拉列表中选择**采用 Base64 格式的文件**。

4d6 单击**下一步**。

4d7 检查提供的输入，然后单击**确定**。

4d8 单击**下载颁发的证书**。

4e 运行以下命令以连接服务器证书和根证书。

```
cat domain.b64 <(echo) cert.b64 <(echo) > tls.crt
```

5 要生成服务主体身份凭证，请执行以下步骤。

重要：必须拥有服务主体身份凭证才能生成配置并将所有敏感信息推送到 Azure 密钥保管库。

5a 登录到 Azure 门户。

5b 单击  。

5c 在终端窗口中运行以下命令：

```
az ad sp create-for-rbac --skip-assignment
```

注释：请记下命令输出中的 appid、口令和租户 ID。

24 准备部署

本章提供有关在部署 Identity Manager 容器之前所要完成的任务的说明。

1 从软件和许可页面 (https://sld.microfocus.com/) 下载 `Identity_Manager_4.9.0_Containers.tar.gz`。

2 运行以下命令以解压缩 `Identity_Manager_4.9.0_Containers.tar.gz` 文件：

```
tar -zxvf Identity_Manager_4.9.0_Containers.tar.gz
```

3 导航到 `Identity_Manager_4.9.0_Containers` 目录并运行以下命令：

```
./ACRCreate.sh
```

注释：当前目录中至少需要有 6 GB 空间才能执行脚本。

3a 执行以下步骤登录到 Microsoft Azure CLI。

3a1 登录到 https://microsoft.com/devicelogin。

3a2 输入列显的代码。

3a3 单击**下一步**。

3a4 单击**继续**。

3b 为以下提示指定输入：

Prompt	说明
按原样输入上面列显的相应 Azure 帐户 ID （不包括双引号）。	指定在上述步骤中生成的 Azure 帐户 ID。
是否要创建 Azure 容器注册表？	指定您是否要创建 Azure 容器注册表。 ◆ （视情况而定）如果选择 “ 是 ”： 1. 指定您是否要创建新的资源组。 ◆ （视情况而定）如果您选择 “ 是 ”，请指定 Azure 资源组名称。 ◆ （视情况而定）如果您选择 “ 否 ”，请指定现有的 Azure 资源组名称。 **注释：**资源组名称中只能包含字母数字字符。 2. 输入 Azure 资源组位置。例如 `eastus`。 ◆ （视情况而定）如果您选择 “ 否 ”，请输入现有的 Azure 容器注册表 URL。例如 `azureregname.azurecr.io`。

3c （视情况而定）要获取 Azure 容器注册表细节，请执行以下步骤：

3c1 登录到 Azure 门户。

3c2 转到您的资源组。

3c3 在“ 资源 ”下，单击**容器注册表**。

3c4 转到**设置** > **访问密钥**并启用**管理员用户**切换开关。

3c5 记下注册表细节以备后用。

25 部署过程

本章介绍在 Azure 上部署 Identity Manager 容器所涉及的部署过程。部署过程分为两个阶段：

- “Azure 云上的基础结构部署 ”（第 283 页）
- “Azure Kubernetes 服务上的 Identity Manager 容器部署 ”（第 297 页）
- “ 在 Azure Kubernetes 服务上设置 Remote Loader 服务 ”（第 298 页）
- “ 在 Azure Kubernetes 服务上设置扇出代理服务 ”（第 300 页）

Azure 云上的基础结构部署

Azure 云上的基础结构部署是使用 terraform 配置定义的。可通过两种不同的方法在 Azure 上部署基础结构。您可以根据自己的要求，选择使用配置生成器或配置模板来部署基础结构。

- “ 使用配置生成器进行部署 ”（第 283 页）
- “ 使用配置模板进行部署 ”（第 287 页）

使用配置生成器进行部署

执行以下步骤，以使用 Identity Manager 配置生成器生成配置文件。

重要：必须有一台已安装并运行 Docker 的计算机才能执行以下步骤。

1. 创建共享卷。有关更多信息，请参见 “ 管理容器卷数据 ”（第 222 页）。
2. 将您的域的证书复制到共享卷。
3. 运行以下命令装载 Docker 映像：

   ```
   docker load --input docker-images/IDM_490_idm_conf_generator.tar.gz
   ```

4. 导航到解压缩位置，并运行以下命令来部署配置生成器容器：

   ```
   docker run --rm -it --name=idm_conf_generator -v /data:/config
   idm_conf_generator:idm-4.9.0-580
   ```

5. 下表提供了有关新提示的信息：

   注释：有关所有现有提示，请参见 “ 了解配置参数 ”（第 75 页）一节。

Prompt	说明
是否要在 Azure 上部署 Identity Manager 容器？对于次要服务器部署，请选择 “n” 并继续进行无提示属性生成 (y/n)？	指定您是否要部署 Identity Manager 容器。 ◆ （视情况而定）如果您选择 “ 是 ”，请继续回答下一条提示。 ◆ （视情况而定）如果您选择 “ 否 ”，请输入包含绝对路径的无提示属性文件名。例如 `/config/silent.properties`。 **注释：**对于次要服务器部署，请输入 **n** 并继续 “ 创建无提示属性文件 ”。
指定 Kubernetes 部署的名称空间。	输入 Kubernetes 部署的名称空间。例如 idm。
是否要创建新的 Azure PostgreSQL 服务器实例？	指定您是否要创建新的 Azure PostgreSQL 服务器实例。 ◆ （视情况而定）如果您选择 “ 是 ”，请指定 Azure PostgreSQL 服务器名称的前缀。例如 idmpgserver。 **注释：**输入的前缀中将追加一个连字符和一个随机生成的 14 位数字。 ◆ （视情况而定）如果您选择 “ 否 ”，请继续回答下一条提示。
输入用于访问 Identity Manager Web 应用程序的完全限定域名 (FQDN)。	指定 FQDN 以访问 Identity Manager Web 应用程序。例如 `identitymanager.eastus.cloudapp.azure.com`。 **注释：**Identity Manager Web 应用程序包括 Identity Applications、Identity Reporting、SSPR、OSP 以及 Identity Console。
输入 TLS 证书文件。	指定 PEM 格式的 TLS 证书文件，其中包含上面指定的域的主题备用名称和常用名。例如 `/config/tls.crt`。
输入 TLS 证书的私用密钥文件。	指定 TLS 证书的私用密钥文件。例如 `/config/tls.key`。
输入要在 Azure 上为 Identity Manager 引擎部署的实例 （Pod 复本）数量？	指定要在 Azure 上为 Identity Manager 引擎部署的实例 （Pod 复本）数量。例如， 5 位。
输入要在 Azure 上为 OSP 部署的实例 （Pod 复本）数量？	指定要在 Azure 上为 OSP 部署的实例 （Pod 复本）数量。例如， 5 位。
输入要在 Azure 上为 Identity Applications 部署的实例 （Pod 复本）数量？	指定要在 Azure 上为 Identity Applications 部署的实例 （Pod 复本）数量。例如， 5 位。
输入 Azure 服务主体 ID。	指定在 “ 规划部署 ” 一章的 “ 步骤 5” 中生成的 Azure 服务主体 ID。

Prompt	说明
输入 Azure 服务口令。	指定在 “ 规划部署 ” 一章的 “ 步骤 5” 中生成的 Azure 服务口令。
输入您的服务主体的租户 ID。	指定在 “ 规划部署 ” 一章的 “ 步骤 5” 中生成的租户 ID。
输入现有的 Azure 容器注册表服务器名称。	指定 Azure 容器注册表服务器名称。请参考步骤 3c。
输入 Azure 容器注册表用户名。	指定 Azure 容器注册表用户名。请参考步骤 3c。
输入 Azure 容器注册表用户口令。	指定 Azure 容器注册表口令。请参考步骤 3c。
按原样输入上面列显的相应 Azure 帐户 ID （不包括双引号）。	指定在上述步骤中生成的 Azure 帐户 ID。
输入 Azure 资源组名称。	指定 Azure 资源组名称。例如 `idvault-rg`。
输入 Azure 资源组位置。	指定资源组位置。例如 `eastus`。

回答所有提示后， Identity Manager 配置生成器将执行以下操作：

- 如果 Azure 中没有可用的资源组，则会创建一个资源组。
- 将在资源组下创建一个密钥保管库和储存帐户。
- 所有敏感信息将推送到密钥保管库。

  注释：要访问 Azure 密钥保管库中的敏感信息，请参见 《Quickstart: Azure Key Vault》（快速入门：Azure 密钥保管库）。

- 将在共享卷下创建 `IDM_4.9.0_Cloud_Deployment_files.zip` 文件，其中包括 Terraform 文件和 Helm 图表。

6 登录到 Azure 门户。

注释：将使用初始登录帐户自动对 Azure Cloud Shell 进行鉴定。如果您需要使用其他帐户，请运行 `az login` 命令并登录到 Azure-CLI。

7 执行以下步骤，将 `IDM_4.9.0_Cloud_Deployment_files.zip` 文件上载到 Azure Cloud Shell。

7a 单击  。

7b 在终端窗口中单击  。

7c 选择要上载到 Azure 的 zip 文件。

8 运行以下命令以解压缩 zip 文件的内容：

```
unzip IDM_4.9.0_Cloud_Deployment_files.zip
```

9 导航到 `IDM_4.9.0_Cloud_Deployment_files` 目录。

10 在 `values.yaml` 文件中进行以下更改：

部分	字段	说明
Identity Manager Web 应用程序的 TLS 配置	kubernetesSecret	将值指定为 `false`。
	azurekeyVault	将值指定为 `true`。 入口 TLS 证书将作为 kubernetes 机密进行管理。
敏感数据的机密管理器	kubernetesSecret	将值指定为 `false`。
	azurekeyVault	将值指定为 `true`。 Azure 密钥保管库用作机密管理器。
AWS Secret Manager 用作机密管理器	awsSecretManager	将值指定为 `false`。

11 （可选）查看 `terraform.tfvars` 和 `values.yaml`。

12 （可选）运行以下命令创建储存帐户密钥：

```
ACCOUNT_KEY=$(az storage account keys list --resource-group
$AZURE_RESOURCE_GROUP_NAME --account-name
$AZURE_STORAGE_ACCOUNT_FOR_TFSTATE --query '[0].value' -o tsv)
```

例如：

```
ACCOUNT_KEY=$(az storage account keys list --resource-group idvault-rg
--account-name stract10226600913781 --query '[0].value' -o tsv)
```

13 （可选）运行以下命令：

```
export ARM_ACCESS_KEY=$ACCOUNT_KEY
```

14 运行以下命令，以下载基础结构部署所需的所有必要插件。

```
terraform init
```

15 运行以下命令以根据输入规划和了解部署。

```
terraform plan
```

16 运行以下命令以创建输入中定义的基础结构。

```
terraform apply --auto-approve
```

17 （可选）运行以下命令以识别 Azure 帐户特定的信息，例如储存帐户名称、密钥保管库名称和数据库管理员细节。

```
terraform output
```

成功执行 Terraform 命令后，执行 “Azure Kubernetes 服务上的 Identity Manager 容器部署 ”（第 297 页）中所述的步骤以完成 Azure 上的 Identity Manager 容器部署。

使用配置模板进行部署

执行以下步骤以更新虚拟机中的配置模板。

1 导航到 `Identity_Manager_4.9.0_Containers.tar.gz` 文件的解压缩目录。

2 导航到 `Identity_Manager_4.9.0_Containers/terraform/` 目录，并运行以下命令来解压缩 zip 文件的内容。

```
unzip IDM_4.9.0_Azure_Terraform_Configuration.zip
```

3 转到 `IDM_Azure_Terraform_Configuration` 文件夹，并更新 `terraform.tfvars` 文件中的以下字段。

表 25-1

字段	说明
resource_group_name	指定 Azure 资源组名称。例如 idvault-rg。
resource_group_location	指定资源组位置。例如 eastus。
resource_group_exists	指定您是否想要知道是否存在现有的资源组。例如 true。
keyvault_name	指定唯一的密钥保管库名称。
keyvault_exists	指定您是否想要知道是否存在现有的密钥保管库。例如 true。
image_registry_server	指定 Azure 容器注册表服务器名称。
image_registry_server_username	指定 Azure 容器注册表用户名。
image_registry_server_password	指定 Azure 容器注册表口令。
aks_kubernetes_namespace	输入 Kubernetes 部署的名称空间。例如 idm。
azure_postgres_server_name	指定 Azure PostgreSQL 服务器名称。例如 idmpgserver。

注释：生成 `terraform.tfvars` 文件时会预填充所有剩余字段。

4 运行以下命令并登录到 Azure-CLI。

```
az login
```

5 执行以下步骤，以将 terraform 状态文件储存在 Azure 储存帐户中：

5a 运行以下命令以在 Azure 中创建储存帐户。

```
az storage account create --name
"${AZURE_STORAGE_ACCOUNT_FOR_TFSTATE}" --resource-group
"${AZURE_RESOURCE_GROUP_NAME}" --location
"${AZURE_RESOURCE_GROUP_LOCATION}" --sku Standard_LRS --encryption-
services blob
```

例如：

```
az storage account create --name stract10226600913781 --resource-group idvault-rg --location eastus --sku Standard_LRS --encryption-services blob
```

5b 运行以下命令创建 Azure 储存容器：

```
az storage container create -n terraform-state --account-name "${AZURE_STORAGE_ACCOUNT_FOR_TFSTATE}"
```

例如：

```
az storage container create -n terraform-state --account-name stract10226600913781
```

5c 导航到 `Identity_Manager_4.8.7_Containers/terraform/IDM_Azure_Terraform_Configuration/` 目录，转到 `main.tf` 文件，并更新 `backend "azurerm"` 字段下的以下细节。

字段	说明
resource_group_name	指定 Azure 资源组名称。例如 idvault-rg。
storage_account_name	指定 Azure 储存帐户名称。例如 stract89671501132193。
container_name	指示 Azure 容器名称。此字段是自动生成的。
key	指示 Azure 密钥名称。此字段是自动生成的。

6 查看 `terraform.tfvars` 和 `main.tf` 文件中已修改的细节，然后将已更新的 `IDM_4.9.0_Azure_Terraform_Configuration.zip` 文件上载到 Azure Cloud Shell。

7 运行以下命令，以下载基础结构部署所需的所有必要插件。

```
terraform init
```

8 运行以下命令以根据输入规划和了解部署。

```
terraform plan
```

9 运行以下命令以创建输入中定义的基础结构。

```
terraform apply --auto-approve
```

10 （可选）运行以下命令以识别 Azure 帐户特定的信息，例如储存帐户名称、密钥保管库名称和数据库管理员细节。

```
terraform output
```

11 运行以下命令，以在密钥保管库中创建机密值。

```
az keyvault secret set --name idm-common-password --vault-name <key vault name> --value "novell@123"
```

注释：您可以根据自己的要求使用 Values.yaml 文件指定多个机密值。

12 导航到在其中生成了 TLS 证书的目录，运行以下命令以将证书和密钥导出为 .pfx 格式。

```
openssl pkcs12 -export -out tls.pfx -inkey tls.key -in tls.crt -passout pass:''
```

注释：`tls.pfx` 文件将在密钥保管库中用于验证机密值和密钥。

13 在 Azure Cloud Shell 中上载 `tls.pfx` 文件，并运行以下命令以将该文件导入密钥保管库。

```
az keyvault certificate import --vault-name <key vault name> -n "ingress-tls-cert" -f tls.pfx
```

例如：

```
az keyvault certificate import --vault-name idmkv20220712 -n "ingress-tls-cert" -f tls.pfx
```

14 导航到 `Identity_Manager_4.9.0_Containers/helm_charts/` 目录并更新 `value.yaml` 文件中的以下字段。

表 25-2

部分	字段	说明
Identity Manager Advanced Edition	IS_ADVANCED_EDITION	指定您是否要部署 Identity Manager Advanced Edition。(true/false)
Azure PostgreSQL 服务器实例	AZURE_POSTGRESQL_REQUIRED	指定您是否要使用 Azure PostgreSQL 服务器实例作为 Identity Applications 和 Identity Reporting 的数据库服务器。(y/n)
Identity Manager Docker 映像的注册表身份凭证	注册表	指定 Azure 容器注册表服务器名称。
	name	指定包含注册表登录身份凭证的 Kubernetes 机密的名称。
数据持久化	**Identity Engine 的持久储存** volumeClaimTemplate： ◆ storageClassName ◆ storageSize	指定 Identity Engine 使用的卷声明模板的储存类名和储存大小。
	共享持久储存 ◆ existingClaim	如果您想要使用现有的持久卷声明 (PVC)，请输入现有声明的名称。
	dynamicClaim： ◆ storageClassName ◆ storageSize	否则，请指定储存类名和储存大小进行 PVC 动态供应。

部分	字段	说明
口令、密钥和证书等敏感数据的机密管理器	azureKeyVaultName：	指定 Azure 密钥保管库的名称。
	azureKeyVaultTenantId	指定 Azure 密钥保管库租户 ID。请参考步骤 10 的 terraform 输出。
	azureUserAssignedIdentityID	指定 Azure 密钥保管库机密提供程序使用的用户定义受管身份的客户端 ID。可以运行以下 az cli 命令来检索身份的客户端 ID： `az aks show -g <资源组> -n <AKS 群集名称> --query addonProfiles.azureKeyvaultSecretsProvider.identity.clientId -o tsv`
入口配置	host	指定用于访问 Identity Manager Web 应用程序的域名。
	azureKeyVaultCertificateName	指定包含 TLS 证书和私用密钥的 Azure 密钥保管库证书的名称。

部分	字段	说明
Identity Engine 配置	部署	指定您是否要部署 Identity Engine。 (true/false)
	replicaCount	指定 Identity Engine 复本 Pod 的数量。例如：“2”。
	ID_VAULT_TREENAME	指定身份库树名称。
	ID_VAULT_SERVER_CONTEXT	指定身份库服务器环境。
	ID_VAULT_DRIVER_SET	指定身份库默认驱动程序集名称。
	ID_VAULT_DEPLOY_CTX	指定身份库默认驱动程序集部署环境。
	ID_VAULT_ADMIN_LDAP	指定身份库管理员 DN。
	ID_VAULT_PASSWORD: secret	指定包含身份库管理员口令的 Azure 密钥保管库机密。
	ID_VAULT_RSA_KEYSIZE	指定用于创建 RSA 证书颁发机构密钥和服务器密钥的密钥大小。
	ID_VAULT_EC_CURVE	指定用于创建 EC 证书颁发机构密钥和服务器密钥的椭圆曲线算法。
	ID_VAULT_CA_LIFE	指定用于创建默认服务器证书的证书寿命。
	资源请求和限制 ◆ cpu ◆ 内存	指定 Identity Engine 的资源请求和限制的 CPU 和内存值。有关更多细节，请参见 Resource Management for Pods and Containers (https://kubernetes.io/docs/concepts/configuration/manage-resources-containers/)（Pod 和容器的资源管理）

部分	字段	说明
One SSO Provider (OSP) 配置	部署	指定您是否要部署 OSP。 (true/false)
	replicaCount	指定 Identity Engine 复本 Pod 的数量。例如：“2”。
	OSP_CUSTOM_NAME	指定 OSP 自定义登录屏幕名称。
	SSO_SERVICE_PWD: secret	指定包含 OSP 客户端口令的 Azure 密钥保管库机密。
	资源请求和限制 ◆ cpu ◆ 内存	指定 OSP 的资源请求和限制的 CPU 和内存值。有关更多细节，请参见 Resource Management for Pods and Containers (https://kubernetes.io/docs/concepts/configuration/manage-resources-containers/) （Pod 和容器的资源管理）

部分	字段	说明
Identity Applications 配置	部署	指定您是否要部署 Identity Applications。 (true/false)
	replicaCount	指定 Identity Engine 复本 Pod 的数量。例如：“2”。
	UA_ADMIN	指定 Identity Applications 管理员 DN
	UA_ADMIN_PWD: secret	指定包含 Identity Applications 管理员口令的 Azure 密钥保管库机密。
	UA_WFE_DB_PLATFORM_OPTION	指定 Identity Applications 和工作流程引擎数据库平台。支持的值为：postgres、 oracle 和 mssql
	UA_ORACLE_DATABASE_TYPE	如果数据库平台为 Oracle， 请指定数据库的配置。（sid/ 服务）
	UA_WFE_DB_HOST	指定 Identity Applications 和工作流程引擎数据库服务器主机。
	UA_WFE_DB_PORT	指定 Identity Applications 和工作流程引擎数据库服务器端口号。
	UA_DATABASE_NAME	指定 Identity Applications 数据库名称。
	WFE_DATABASE_NAME	指定工作流程引擎数据库名称。
	UA_WFE_DATABASE_USER	指定 Identity Applications 数据库用户名。
	UA_WFE_DATABASE_PWD: secret	指定包含 Identity Applications 数据库用户口令的 Azure 密钥保管库机密。
	资源请求和限制 ◆ cpu ◆ 内存	指定 Identity Application 的资源请求和限制的 CPU 和内存值。有关更多细节，请参见 Resource Management for Pods and Containers (https://kubernetes.io/docs/concepts/configuration/manage-resources-containers/)（Pod 和容器的资源管理）

部分	字段	说明
表单渲染器配置	部署	指定您是否要部署表单渲染器。(true/false)
	资源请求和限制 ◆ cpu ◆ 内存	指定表单渲染器的资源请求和限制的 CPU 和内存值。有关更多细节，请参见 Resource Management for Pods and Containers (https://kubernetes.io/docs/concepts/configuration/manage-resources-containers/)（Pod 和容器的资源管理）
ActiveMQ 配置	部署	指定您是否要部署 ActiveMQ。(true/false)
	资源请求和限制 ◆ cpu ◆ 内存	指定表单渲染器的资源请求和限制的 CPU 和内存值。有关更多细节，请参见 Resource Management for Pods and Containers (https://kubernetes.io/docs/concepts/configuration/manage-resources-containers/)（Pod 和容器的资源管理）

部分	字段	说明
Identity Reporting 配置	部署	指定您是否要部署 Identity Reporting。 (true/false)
	RPT_ADMIN	指定 Identity Reporting 管理员 DN
	RPT_ADMIN_PWD: secret	指定包含 Identity Reporting 管理员口令的 Azure 密钥保管库机密。
	RPT_DATABASE_PLATFORM_OPTION	指定 Identity Reporting 数据库平台。支持的值为：postgres、oracle 和 mssql
	RPT_ORACLE_DATABASE_TYPE	如果数据库平台为 Oracle， 请指定数据库的配置。（sid/ 服务）
	RPT_DATABASE_HOST	指定 Identity Reporting 数据库主机。
	RPT_DATABASE_PORT	指定 Identity Reporting 数据库端口号。
	RPT_DATABASE_NAME	指定 Identity Reporting 数据库名称。
	RPT_DATABASE_USER	指定 Identity Reporting 数据库用户。
	RPT_DATABASE_SHARE_PASSWORD: secret	指定包含 Identity Reporting 数据库帐户口令的 Azure 密钥保管库机密
	资源请求和限制 ◆ cpu ◆ 内存	指定表单渲染器的资源请求和限制的 CPU 和内存值。有关更多细节，请参见 Resource Management for Pods and Containers (https://kubernetes.io/docs/concepts/configuration/manage-resources-containers/)（Pod 和容器的资源管理）

部分	字段	说明
Self Service Password Reset (SSPR) 配置	部署	指定您是否要部署 SSPR。 (true/false)
	CONFIGURATION_PWD:	指定要为管理员创建的、用于配置 SSPR 的口令。
	secret:	
	资源请求和限制 ◆ cpu ◆ 内存	指定 SSPR 的资源请求和限制的 CPU 和内存值。有关更多细节，请参见 Resource Management for Pods and Containers (https://kubernetes.io/docs/concepts/configuration/manage-resources-containers/) （Pod 和容器的资源管理）
Identity Console 配置	部署	指定您是否要部署 Identity Console。 (true/false)
	ID_CONSOLE_USE_OSP	不支持使用 One SSO Provider (OSP) 作为 Identity Console 的登录方法，因此默认值应为 “n”。
	资源请求和限制 ◆ cpu ◆ 内存	指定 Identity Console 的资源请求和限制的 CPU 和内存值。有关更多细节，请参见 Resource Management for Pods and Containers (https://kubernetes.io/docs/concepts/configuration/manage-resources-containers/) （Pod 和容器的资源管理）
高级配置	**DATA_CONTAINERS：**	
	DATA_CONTAINERS_LDIF	指定用于创建数据容器的 LDIF 配置。
	ROOT_CONTAINER GROUP_ROOT_CONTAINER USER_CONTAINER ADMIN_CONTAINER	指定根容器、组根容器、用户容器和管理员容器的 DN
	Kubernetes 群集域：	指定 Kubernetes 群集域
	KUBE_SUB_DOMAIN	
Identity Manager Web 应用程序的 TLS 配置	kubernetesSecret	将值指定为 `false`。
	azurekeyVault	将值指定为 `true`。 入口 TLS 证书将作为 kubernetes 机密进行管理。

部分	字段	说明
敏感数据的机密管理器	kubernetesSecret	将值指定为 `false`。
	azurekeyVault	将值指定为 `true`。 Azure 密钥保管库用作机密管理器。
AWS Secret Manager 用作机密管理器	awsSecretManager	将值指定为 `false`。

更新 `terraform.tfvars` 和 `values.yaml` 文件后，按照 “Azure Kubernetes 服务上的 Identity Manager 容器部署 ”（第 297 页）中所述的步骤完成 Azure 上的 Identity Manager 容器部署。

Azure Kubernetes 服务上的 Identity Manager 容器部署

本节提供有关在 Azure kubernetes 服务上部署 Identity Manager 容器的信息。

1 运行以下命令连接到 Kubernetes 群集并储存所需的配置：

```
az aks get-credentials --resource-group <resource group> --name
<cluster name> --overwrite-existing
```

例如：

```
az aks get-credentials --resource-group idvault-rg --name cluster-name
--overwrite-existing
```

2 运行以下命令创建用于运行负载平衡器的 Nginx 实例：

```
helm repo add ingress-nginx https://kubernetes.github.io/ingress-nginx
```

3 执行以下步骤，从 Azure 门户获取 Kubernetes 服务的公共 IP 地址。

3a 转到 Azure 主页并单击**所有资源**。

3b 在搜索框中，键入 “ 负载平衡器 ” 并按 Enter。

3c 在 Azure Cloud Shell 中运行以下命令创建新的公共 IP：

```
az network public-ip create     --resource-group <aks-cluster-
resource-group-name> --name <name-public-ip> --sku Standard  --
version IPv4 --zone 1 2 3 --ip-tags 'RoutingPreference=Internet' --
dns-name <Domain Name>   --query publicIp.ipAddress -o tsv
```

3d 单击与您的资源组和 AKS 群集关联的负载平衡器。

3e 转到**设置 > 前端 IP 配置**并提供步骤 3c （第 297 页）创建的公共 IP。

3f 单击**保存**。

4 导航到 IDM_4.9.0_Cloud_Deployment_files 目录，运行以下命令安装 Nginx-ingress 控制器：

```
helm install ingress-nginx ingress-nginx/ingress-nginx --namespace
<your namespace> --set controller.replicaCount=1 --set
controller.nodeSelector."kubernetes\.io/os"=linux --set
defaultBackend.nodeSelector."kubernetes\.io/os"=linux --set
controller.service.loadBalancerIP=<Kubernetes public IP address
obtained from the Azure portal> --set
controller.service.externalTrafficPolicy=Local --set
controller.service.annotations."service\.beta\.kubernetes\.io/azure-
dns-label-name"=<Domain Name>
```

使用您在步骤 3c （第 297 页）中创建的公共 IP 地址。

例如：

```
helm install ingress-nginx ingress-nginx/ingress-nginx --namespace idm
--set controller.replicaCount=1 --set
controller.nodeSelector."kubernetes\.io/os"=linux --set
defaultBackend.nodeSelector."kubernetes\.io/os"=linux --set
controller.service.loadBalancerIP="20.33.59.34" --set
controller.service.externalTrafficPolicy=Local --set
controller.service.annotations."service\.beta\.kubernetes\.io/azure-
dns-label-name"=identitymanager
```

5 要运行 Helm 图表，请运行以下命令：

```
helm install identity-manager helm_charts/identity-manager-1.4.0.tgz --
namespace <namespace> -f values.yaml
```

例如：

```
helm install identity-manager helm_charts/identity-manager-1.4.0.tgz --
namespace idm -f values.yaml
```

6 运行以下命令查看 Azure Kubernetes 服务中运行的 Pod 列表：

```
kubectl get pods --watch -n <namespace>
```

例如：

```
kubectl get pods --watch -n idm
```

在 Azure Kubernetes 服务上设置 Remote Loader 服务

执行以下步骤在 Azure Kubernetes 服务上设置 Remote Loader 服务：

1 创建持久卷 (PV) 和持久卷声明 (PVC) 以持久保存 Remote Loader 数据。

2 在 PV 内创建 `rdxml` 目录。

3 在 `rdxml` 目录中创建 `driverconf` 目录。

4 在 `rdxml` 目录中创建 `keystore` 目录。

5 将所有必需的密钥储存区文件和证书复制到 keystore 目录。

6 在 `rdxml` 目录中，创建一个新的 `.txt` 文件。例如 `StartupRL.txt`。

7 在 `StartupRL.txt` 文件中，用以下格式指定所需内容：

```
<Remote Loader 配置文件 > -sp < 驱动程序口令 > <Remote Loader 口令 >
```

例如：

```
config8000.txt -sp dirxml dirxml
```

或者，也可以用以下格式指定项：

```
<Remote Loader 配置文件 > -ksp < 密钥储存区口令 > -kp < 密钥口令 >
```

例如：

```
config8000.txt -ksp dirxml -kp dirxml
```

8 从容器 tarball 中复制 `helm-charts/rl-values.yaml` 并更新该文件中的以下字段：

表 25-3

部分	字段	说明
Remote Loader Docker 映像的注册表身份凭证	注册表	指定 Azure 容器注册表服务器名称。
	name	指定包含注册表登录身份凭证的 Kubernetes 机密的名称。
数据持久化	**共享持久储存** ◆ existingClaim dynamicClaim： ◆ storageClassName ◆ storageSize	如果您想要使用现有的持久卷声明 (PVC)，请输入现有声明的名称。 否则，请指定储存类名和储存大小进行 PVC 动态供应。
驱动程序启动文件	driverStartupFileName	指定驱动程序启动文件的名称。例如 `StartupRL.txt`
Remote Loader 服务	ports	指定 Remote Loader 服务侦听的端口列表。
资源请求和限制	资源请求 ◆ cpu ◆ 内存	指定资源请求的 CPU 和内存值。有关更多细节，请参见 Resource Management for Pods and Containers (https://kubernetes.io/docs/concepts/configuration/manage-resources-containers/)（Pod 和容器的资源管理）
	限制 ◆ cpu ◆ 内存	指定限制的 CPU 和内存值。有关更多细节，请参见 Resource Management for Pods and Containers (https://kubernetes.io/docs/concepts/configuration/manage-resources-containers/)（Pod 和容器的资源管理）

9 从容器 tarball 中复制 `helm-charts/remote-loader-1.4.0.tgz`，然后运行以下 helm 命令安装 Remote Loader：

```
helm install remote-loader helm_charts/remote-loader-1.4.0.tgz --
namespace idm -f rl-values.yaml
```

10 （可选）如果您要安装多个 Remote Loader，请从容器 tarball 中复制 `helm-charts/remote-loader-1.4.0.tgz`，然后运行以下 helm 命令：

```
helm install <remote-loader-n> helm_charts/remote-loader-1.4.0.tgz --
namespace idm -f rl-values.yaml
```

`remote-loader-n` 中的 n 表示安装的第 n 个 Remote Loader。

例如：

如果您要安装两个 Remote Loader，那么用于安装第二个 Remote Loader 的命令是

```
helm install remote-loader-2 helm_charts/remote-loader-1.4.0.tgz --
namespace idm -f rl-values.yaml
```

在 Azure Kubernetes 服务上设置扇出代理服务

执行以下步骤在 Azure Kubernetes 服务上进行设置：

1 从容器 tarball 中复制 `helm-charts/fa-values.yaml` 并更新该文件中的以下字段：

表 25-4

部分	字段	说明
Remote Loader Docker 映像的注册表身份凭证	注册表	指定 Azure 容器注册表服务器名称。
	name	指定包含注册表登录身份凭证的 Kubernetes 机密的名称。
数据持久化	**共享持久储存** ◆ existingClaim	如果您想要使用现有的持久卷声明 (PVC)，请输入现有声明的名称。
	dynamicClaim： ◆ storageClassName ◆ storageSize	否则，请指定储存类名和储存大小进行 PVC 动态供应。
扇出代理服务	ports	指定 Remote Loader 服务侦听端口的值。

部分	字段	说明
资源请求和限制	资源请求 ◆ cpu ◆ 内存	指定资源请求的 CPU 和内存值。有关更多细节，请参见 “Resource Management for Pods and Containers”（Pod 和容器的资源管理）(https://kubernetes.io/docs/concepts/configuration/manage-resources-containers/)
	限制 ◆ cpu ◆ 内存	指定限制的 CPU 和内存值。有关更多细节，请参见 “Resource Management for Pods and Containers”（Pod 和容器的资源管理）(https://kubernetes.io/docs/concepts/configuration/manage-resources-containers/)
ActiveMQ 服务	install	指定您是否要为扇出代理部署 ActiveMQ 服务 (true/false)
	资源请求 ◆ cpu ◆ 内存	指定 ActiveMQ 服务的资源请求的 CPU 和内存值。有关更多细节，请参见 Resource Management for Pods and Containers (https://kubernetes.io/docs/concepts/configuration/manage-resources-containers/)（Pod 和容器的资源管理）
	限制 ◆ cpu ◆ 内存	指定 ActiveMQ 服务的限制的 CPU 和内存值。有关更多细节，请参见 Resource Management for Pods and Containers (https://kubernetes.io/docs/concepts/configuration/manage-resources-containers/)（Pod 和容器的资源管理）

2 从容器 tarball 中复制 `helm-charts/fanout-agent-1.4.0.tgz`，然后运行以下 helm 命令安装扇出代理：

```
helm install fanout-agent helm_charts/fanout-agent-1.4.0.tgz --
namespace idm -f rl-values.yaml
```

3 （可选）如果您要安装多个扇出代理，请从容器 tarball 中复制 `helm-charts/fanout-agent-1.4.0.tgz`，然后运行以下 helm 命令：

```
helm install <fanout-agent-n> helm_charts/fanout-agent-1.4.0.tgz --
namespace idm -f rl-values.yaml
```

`fanout-agent-n` 中的 n 表示安装的第 n 个扇出代理。

例如：

如果您要安装两个扇出代理，那么用于安装第二个扇出代理的命令是

```
helm install fanout-agent-2 helm_charts/fanout-agent-1.4.0.tgz --
namespace idm -f rl-values.yaml
```

26 部署后任务

本章提供有关在部署 Identity Manager 容器之后所要完成的任务的说明。

访问 Identity Manager 应用程序

要访问任何 Identity Manager 应用程序，请在浏览器中输入以下 URL。

`https://< 域名 >/< 应用程序名称 >`

例如：

`https://identitymanager.eastus.cloudapp.azure.com/idmdash`

在 Azure 虚拟机上部署 Designer

执行以下步骤在 VM 子网下的 Azure 虚拟机上部署 Designer。

1. 请参见 《Quickstart:Linux VMs》（快速入门：Linux VM）创建 Linux 计算机，或参见 《Quickstart:Windows VMs》（快速入门：Windows VM）创建 Windows VM。
2. 指派一个公共 IP 地址用于连接 Designer。
3. 在创建的虚拟机中下载并安装 Designer。有关详细信息，请参见 “ 安装 Designer”（第 67 页）或 Installing Designer （安装 Designer）（适用于 Windows）。

在 Azure 虚拟机上部署 SLM for IGA

执行以下步骤，在 VM 子网下的 Azure 虚拟机上部署 Sentinel Log Management (SLM) for Identity Governance and Administration (IGA)。

1. 创建 Linux 计算机，具体请参见 《Quickstart:Linux VMs》（快速入门：Linux VM）。
2. 指派公共 IP 地址用于连接 SLM for IGA 安装程序。
3. 在创建的虚拟机中下载并安装 SLM for IGA。有关更多信息，请参见 “ 安装 Sentinel Log Management for Identity Governance and Administration”（第 69 页）。

处理 AKS 的 RPM 更新和第三方文件

此服务包提供了一种处理容器中 RPM 更新和第三方文件的有效方式。可以通过将所需的 RPM 文件、库 (.so) 文件和第三方 .jar 文件放入 mountfiles 目录来实现这种处理。将强制更新 mountfiles 目录中的 RPM 文件。重启动容器时， .so 和 .jar 文件将分别自动软链接到 /opt/novell/eDirectory/lib64/nds-modules/ 和 /opt/novell/eDirectory/lib/dirxml/classes/ 目录。这种做法旨在更新 Docker 容器中的驱动程序。

注释：目前，此增强功能适用于 Identity Manager 引擎和 Remote Loader 容器。

1 登录到 Azure 门户并单击 。

2 运行以下命令登录到您的持久卷：

```
kubectl exec –it -n idm <container name> bash
```

例如

```
kubectl exec –it -n idm identityengine-0 bash
```

3 将所需的文件复制到容器特定的相应 mountfiles 目录。

3a （视情况而定）对于 Identity Manager 引擎容器，请运行以下命令将文件复制到 /config/idm/mountfiles：

```
kubectl cp -n < 名称空间 > < 要复制的文件 > < 容器名称 >:/config/idm/mountfiles
```

3b （视情况而定）对于 Identity Remote Loader 容器，请运行以下命令将文件复制到 /config/rdxml/mountfiles：

```
kubectl cp -n < 名称空间 > < 要复制的文件 > < 容器名称 >:/config/rdxml/mountfiles
```

注释：支持的文件格式为 .so、 .jar 和 .rpm。

4 运行以下命令重启动容器：

```
helm upgrade identity-manager helm_charts/identity-manager-1.4.0.tgz --namespace <namespace> -f values.yaml
```

重要：无论装入文件中的哪个 rpm 优先级最高，将来更新时，您都需要小心去除现有的 rpm 并更新最新的 rpm。

27 维护 Identity Manager 容器的部署

本章介绍如何维护 Azure Kubernetes 群集上的 Pod （包含一个或多个容器的组）部署。

重要：如果您需要在部署中添加更多图表、重新创建部署或者增加 （或减少）部署中的 Pod 数量，请执行以下步骤：

1 登录到 Azure 门户。

2 单击  ，然后运行以下命令。

```
helm upgrade identity-manager helmcharts/identity-manager-1.4.0.tgz --
namespace < 名称空间 > -f values.yaml
```

管理数据持久化层

在 Visual Studio Code 应用程序中执行以下步骤来修改 Pod 的数据层：

1 下载并安装 Visual Studio Code。请参见 code.visualstudio.com/download。

2 打开 Visual Studio Code 应用程序，单击  。

3 在 “ 搜索 ” 中键入 **Azure**，然后按 Enter。

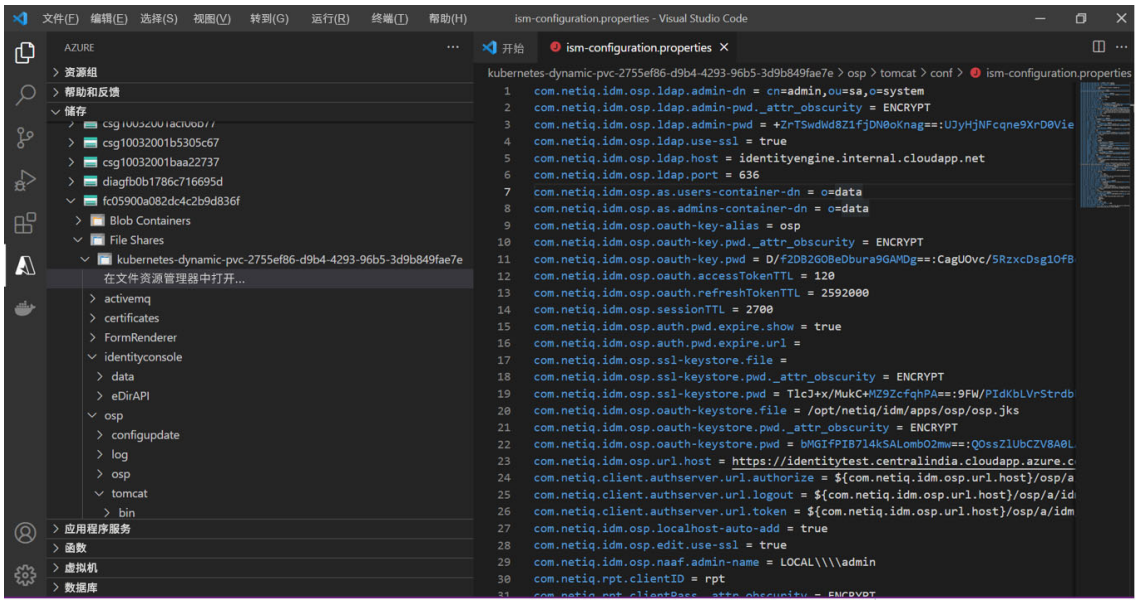
4 在 “Azure 工具 ” 中单击**安装**。

5 单击  。

6 转到**储存** > **Security-IdentityMgmtAZ-NonProd** > **fc05900a082dc4c2b9d836f** > **文件共享** > **Kubernetes 动态 PVC** （有关详细信息，请参见图 27-1 （第 306 页））。

注释：上面导航路径中提到的 **Security-IdentityMgmtAZ-NonProd** 和 **fc05900a082dc4c2b9d836f** 密钥仅供参考，请根据您的登录身份凭证予以更改。

图 27-1 Visual Studio 储存



7 选择文件并更改所需属性。

8 转到**文件**菜单，单击**保存**。

9 保存所有更改后，重启动 Pod （请参见 “ 重启动 Pod”（第 306 页））。

重启动 Pod

执行以下步骤重启动 Azure 中的 Pod。

例如，如果您对数据层进行了任何更改，则需要重启动容器。

1 登录到 Azure 门户。

2 在 “ 搜索 ” 中键入 “ 所有资源 ”，然后按 Enter。

3 在 “ 服务 ” 下，选择**所有资源**。

4 转到您的 Kubernetes 群集。

5 在 “Kubernetes 资源 ” 下，单击**工作负载**。

6 转到 **Pod** 选项卡，单击**按名称空间过滤**下拉列表，然后选择 **idm**。

7 选择要重启动的 Pod。

8 单击 **“ 删除 ”**。有关更多信息，请参见 图 27-2 （第 307 页）。

注释：系统将识别已删除的 Pod，并自动触发部署到新 Pod 的操作。

图 27-2 Kubernetes 群集



访问 Pod

执行以下步骤访问 Azure 中的 Pod：

1 登录到 Azure 门户。

2 单击 。

3 运行以下命令识别 Pod 的名称：

```
kubectl get pods --watch -n <namespace>
```

例如：

```
kubectl get pods --watch -n idm
```

4 运行以下命令：

```
kubectl exec -it -n idm <pod-name> bash
```

例如：

```
kubectl exec -it -n idm userapp-d54f98b58-qcpmz bash
```

重启动 Azure Kubernetes 群集

执行以下步骤以确保所有 IDM 组件正常关闭：

1 登录到 Azure 门户。

2 转到您的 Kubernetes 群集。

3 在 “Kubernetes 资源 ” 下，单击**工作负载**。

4 转到**部署**选项卡，单击**按名称空间过滤**下拉列表，然后选择您的名称空间。

5 选择部署并单击**删除**。

6 转到 Pod 选项卡，单击按名称空间过滤下拉列表，然后选择您的名称空间。

7 单击刷新，检查是否已完全去除组件 Pod。

8 转到有状态集选项卡，单击按名称空间过滤下拉列表，然后选择您的名称空间。

9 选择有状态集并单击删除。

10 同样，请转到 Pod 选项卡，单击按名称空间过滤下拉列表，然后选择您的名称空间。

11 单击刷新，检查是否已完全去除组件。

12 转到 “Kubernetes 资源 ” 下的 “ 概述 ”，单击停止并等待一段时间。

13 群集完全停止后，单击启动。

14 在 Azure CLI 中，运行以下命令重启动 Nginx-ingress 控制器：

```
helm upgrade nginx-ingress ingress-nginx/ingress-nginx --namespace
<your namespace> --set controller.replicaCount=1 --set
controller.service.loadBalancerIP=<Public IP address assigned to load
balancer> --set
controller.service.annotations."service\.beta\.kubernetes\.io/azure-
dns-label-name"=<LoadBalancerName>
```

例如

```
helm upgrade nginx-ingress ingress-nginx/ingress-nginx --namespace idm
--set controller.replicaCount=1 --set
controller.service.loadBalancerIP=192.168.0.1 --set
controller.service.annotations."service\.beta\.kubernetes\.io/azure-
dns-label-name"=identitymanager
```

15 运行以下命令重启动剩余组件：

```
helm upgrade identity-manager helm_charts/identity-manager-1.4.0.tgz --
namespace <namespace> -f values.yaml
```

例如

```
helm upgrade identity-manager helm_charts/identity-manager-1.4.0.tgz --
namespace idm -f values.yaml
```

16 等待所有 Pod 进入就绪状态。

要检查 Pod 的当前状态，请运行以下命令：

```
kubectl get pods --watch -n <namespace>
```

17 运行以下命令重启动引擎服务：

```
kubectl rollout restart -n <namespace> statefulset/identityengine
```

例如

```
kubectl rollout restart -n idm statefulset/identityengine
```

18 重复 步骤 16.

缩放 Identity Manager 引擎复本

缩放 Identity Manager 引擎复本的过程由两个部分组成：

缩减 Identity Manager 引擎复本的用例

本主题将介绍一个基本用例，您可以参考该用例来缩减 Identity Manager 引擎复本。

开始之前

- 在缩减 Identity Manager 引擎复本之前，请仔细了解该过程。
- 一次只能缩减一个 Pod。

用例

假设有 3 个 Identity Manager 引擎实例，其 Pod 名称为：

- identityengine-0
- identityengine-1
- identityengine-2

当您缩减为两个 Identity Manager 引擎实例时， identityengine-2 将会关闭。

在缩减之前，需要在 Identityengine-2 上执行以下操作：

1 将实例 Identityengine-2 上运行的驱动程序迁移到另一个实例，或者在另一实例上重创建。

2 从树中删除服务器。

3 运行以下命令列出持久卷声明 (PVC)：

```
kubectl get pvc -n < 名称空间 >
```

例如：

```
kubectl get pvc -n idm
```

4 运行以下命令删除 identityengine-2 的 PVC：

```
kubectl delete pvc -n < 名称空间 > <identityengine 复本名称 >
```

例如：

```
kubectl delete pvc -n idm identityenginedata-identityengine-2
```

5 在 `values.yaml` 文件中将引擎复本计数设置为 2。

6 使用以下命令进行缩减：

```
helm upgrade identity-manager helm_charts/identity-manager-1.4.0.tgz --
namespace < 名称空间 > -f values.yaml
```

扩展 Identity Manager 引擎复本

执行以下步骤来扩展 Identity Manager 引擎复本：

1 登录到 Azure 门户。

2 单击 。

3 在 values.yaml 文件中增大 Identity Manager 引擎复本计数。

4 使用以下命令进行扩展：

```
helm upgrade identity-manager helm_charts/identity-manager-1.4.0.tgz --
namespace < 名称空间 > -f values.yaml
```

缩放 OSP 和 Identity Applications 复本

执行以下步骤来扩展或缩减 OSP 和 Identity Applications 复本：

1 登录到 Azure 门户。

2 单击  。

3 在 values.yaml 文件中增大或减小 OSP/Identity Applications 复本计数。

4 使用以下命令进行扩展或缩减：

```
helm upgrade identity-manager helm_charts/identity-manager-1.4.0.tgz --
namespace < 名称空间 > -f values.yaml
```

销毁使用 Terraform 创建的整个资源

执行以下步骤来销毁使用 Terraform 创建的资源：

注释：请在经过慎重考虑之后再继续执行此过程。

1 导航到您在其中使用 terraform 创建了资源的目录。

2 运行以下命令以删除资源：

```
terraform destroy --auto-approve
```

3 （可选）如果在运行上述命令期间出现任何错误，请重运行该命令。

X 在 AWS EC2 上部署 Identity Manager

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

- 第 28 章 “ 在 AWS EC2 上规划和实施 Identity Manager”（第 313 页）
- 第 29 章 “ 混合 Identity Manager 方案示例 ”（第 331 页）

28 在 AWS EC2 上规划和实施 Identity Manager

Identity Manager 现在支持在 Amazon Web Services (AWS) EC2 上以服务的形式部署以下 Identity Manager 组件：

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

有关 AWS EC2 支持的操作系统的更多细节，请参见 System Requirements for Identity Manager 4.9 （Identity Manager 4.9 系统要求）

先决条件

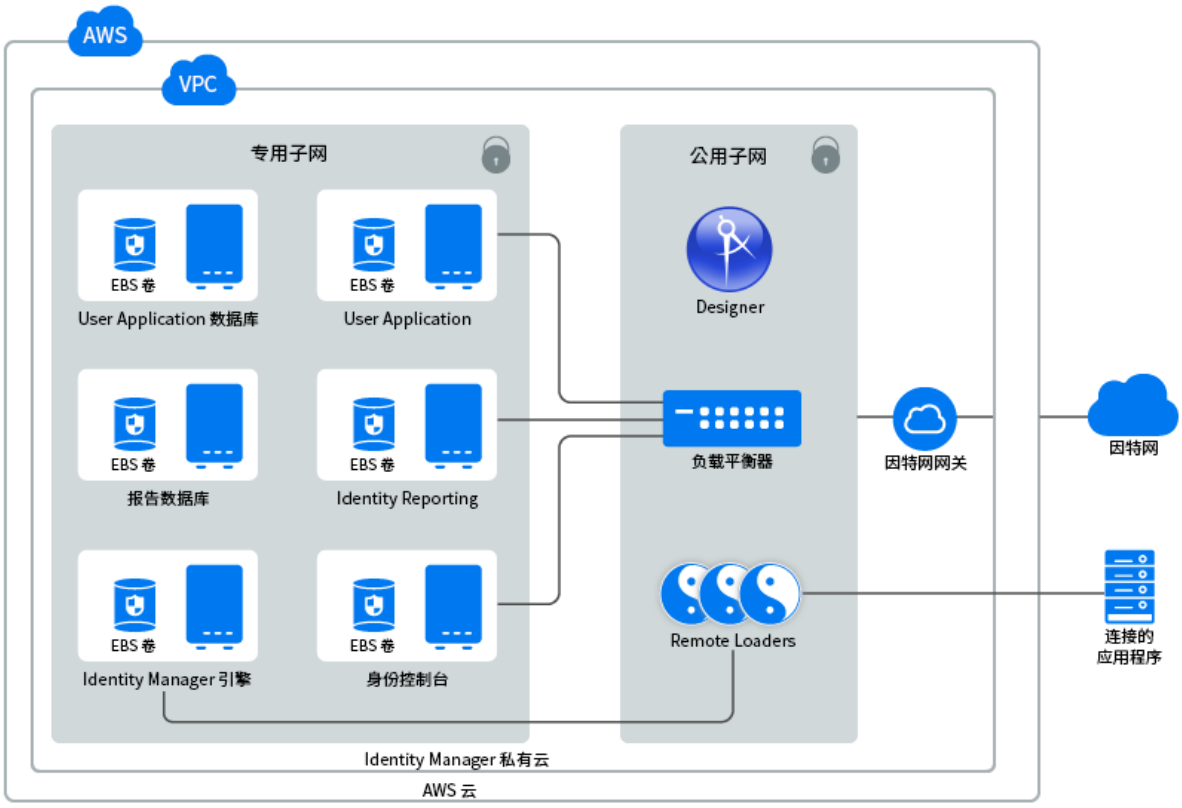
除了 Identity Manager 组件的系统要求以外，另请确保符合以下先决条件：

- 在 AWS EC2 上有管理帐户。
- `Identity_Manager_4.9.0_Linux.iso` 和 Designer 已下载、解压缩并可在 Identity Manager 组件实例上使用。
- 用于从本地客户端计算机连接到 AWS EC2 实例的 SSH 客户端。

部署过程

您可以根据相应要求在专用或公用网络中部署 Identity Manager 组件。图 28-1“AWS EC2 上的 Identity Manager 部署 ”（第 314 页）演示了一个示例部署，后续章节中将用到该部署。

图 28-1 AWS EC2 上的 Identity Manager 部署



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

部署过程包括以下步骤：

- “准备 AWS Virtual Private Cloud”（第 315 页）
- “创建和部署实例”（第 317 页）
- “准备 EC2 实例”（第 318 页）
- “安装 Identity Manager 组件”（第 320 页）
- “安装 Identity Applications 和 Identity Reporting 的数据库”（第 320 页）
- “安装 Designer”（第 322 页）
- “创建 AWS EC2 负载平衡器”（第 322 页）
- “（可选）使用注册的托管区域创建别名 DNS”（第 327 页）
- “访问 Identity Manager 组件”（第 328 页）

准备 AWS Virtual Private Cloud

本节概述将 AWS VPC 设置为与 Identity Manager 搭配使用的一般性步骤。有关详细信息，请参见 Amazon Elastic Compute Cloud 文档。

创建 AWS VPC 服务需要执行的步骤如下：

1 登录 AWS Management Console （AWS 管理控制台）。

2 单击 Services （服务）并创建以下服务：

服务	步骤
VPC	1. 单击 Networking & Content Delivery （网络和内容交付）下的 Services > VPC （服务 > VPC）。 2. 单击 Start VPC Wizard （启动 VPC 向导）。 3. 选择 VPC 配置类型，然后单击 Select （选择）。 4. 在表单中指定细节，然后单击 Create VPC （创建 VPC）。 如此即会创建指定大小的专用网络。 VPC 和子网创建过程使用 CIDR 表示法来表示地址范围。最大的 VPC 大小为 /16 网络。 有关详细信息，请参见 Amazon Virtual Private Cloud 文档 (https://docs.aws.amazon.com/vpc/index.html)。
重要：使用 Start VPC Wizard （启动 VPC 向导）创建 VPC 会创建该 VPC 的子网、因特网网关和路由表。您可以按如下所述查看或编辑这些项目：	
子网	要按图 28-1 中所示部署 Identity Manager 组件，请在 VPC 中创建三个子网。例如 privateSN、 publicSN1 和 publicSN2。 创建子网需要执行的步骤如下。 1. 在左侧菜单中，单击 Subnets （子网）。 2. 单击 Create Subnet （创建子网）。 3. 指定用于标识子网的名称标记。 4. 指定 VPC 中的 IPv4 CIDR 块。 例如：`10.0.0.0/24` 必须在不同的可用性区域中创建公用子网。 5. 依次单击 Yes （是）、 “Create” （创建）。 6. （视情况而定）对于公用子网，启用自动指派公用 IP 地址： a. 选择 Subnet Actions > Modify auto-assign IP settings （子网操作 > 修改自动指派 IP 设置）。 b. 选择 Enable auto-assign public IPv4 address （启用自动指派公用 IPv4 地址）。 c. 单击 Save （保存）。 重复上述步骤创建更多子网。

服务	步骤
因特网网关	1. 在左侧菜单中，单击 Internet Gateways （因特网网关）。 2. 单击 Create Internet Gateway （创建因特网网关）。 3. 指定名称标记，然后单击 Create （创建）。 4. 选择新建的因特网网关，并将其挂接到 VPC： a. 选择 Actions > Attach to VPC （操作 > 挂接到 VPC）。 b. 从列表中选择该 VPC，然后单击 Attach （挂接）。
路由表	1. 在左侧菜单中，单击 Route Tables （路由表）。 2. 选择系统自动为此 VPC 创建的路由表。 3. 在 Routes （路由）选项卡中： a. 单击编辑。 b. 单击 Add another route （添加另一个路由）。 c. 在 Destination （目的地）中，指定 0.0.0.0/0。 d. 在 Target （目标）中，选择与此 VPC 关联的因特网网关表。请参见 “因特网网关 ”。 e. 单击 Save （保存）。 4. 在 Subnet Association （子网关联）选项卡中： a. 单击 Edit （编辑）。 b. 找到要与此 VPC 关联的子网，然后单击 Save （保存）。
（可选）托管区域	如果您有已注册的域，可以执行以下操作以使用该域来托管 Identity Manager 组件： 1. 单击 Services > Route 53 > Hosted Zones （服务 > Route 53 > 托管区域）。 2. 单击 Create Hosted Zone （创建托管区域）并指定如下所述的细节： ◆ **域名：**指定域名。 ◆ **注释：**添加注释。 ◆ **类型：**指定托管区域的类型。 3. 单击 Create （创建）。
弹性 IP 地址	1. 单击 Services > EC2 （服务 > EC2）。 2. 在左侧菜单中，选择 Elastic IPs （弹性 IP）。 3. 单击 Allocate New address （分配新地址）。 4. 单击 Allocate （分配）。 系统即会分配一个其他任何资源均未使用的静态 IPv4 地址。 5. 单击 Close （关闭）。

创建和部署实例

本节概述创建和部署 Identity Manager 基本设置 （包含 Identity Manager 引擎、 Identity Applications、 Reporting、 User Application 数据库和 Reporting 数据库）实例的步骤。

创建 Identity Manager 组件实例需要执行的步骤如下。

1 单击 **Services** （服务） > **EC2**。

2 单击 **Launch Instance** （起动实例）。

3 选择 `SLES 15 SPx` 或映像。

4 选择符合基础操作系统及 Identity Manager 组件部署要求的实例类型。请参见 System Requirements for Identity Manager 4.9 （Identity Manager 4.9 系统要求）。

5 单击 **Next: Configure Instance Details** （下一步：配置实例细节）。

确保该实例使用的是正确的 VPC 和子网。此页面中会自动填充子网设置。

字段	操作
Auto-assign Public IP （自动指派公用 IP）	对于公用子网，请设置为 `Enable` （启用）。使用此设置会自动填充子网设置。对于专用子网，请将值设置为 `Disable` （禁用）。

6 单击 **Next: Add Storage** （下一步：添加储存）。

默认储存大小为 10 GB。请根据要求更改储存大小。请参见 System Requirements for Identity Manager 4.9 （Identity Manager 4.9 系统要求）。

7 单击 **Next: Add Tags** （下一步：添加标记）。

请根据需要添加标记。使用标记可以组织实例。例如，可将以下两个标记添加到每个实例：

- 一个标记指示该实例的用途
- 一个标记指示此计算机的拥有者

8 单击 **Next: Configure Security Group** （下一步：配置安全组）。

安全组是实例组的虚拟防火墙规则。建议对防火墙要求相同的每组实例单独创建一个安全组。

例如，可对 Identity Manager 引擎的所有节点、 Identity Applications 的所有节点以及 Identity Reporting 的所有节点分别配置一个安全组。默认情况下，新安全组仅允许端口 22 上的传入流量，因此，您只能使用 SSH 连接到实例。

有关详细信息，请参见 “Amazon EC2 Security Groups for Linux Instances” （Linux 实例的 Amazon EC2 安全组）(https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-security-groups.html)。

9 创建新的安全组；指定该组的名称和说明。

在安装以下 Identity Manager 组件之前，请添加额外的端口规则：

组件	端口	说明
身份库的 LDAP	TCP 636	需要使用它来进行 LDAP 安全通讯。
Identity Applications	TCP 8543	需要使用它来进行 HTTPS 通讯，以便访问 Identity Applications。
Identity Reporting	TCP 8643	需要使用它来进行 HTTPS 通讯，以便访问 Identity Reporting。
PostgreSQL 数据库	TCP 5432	需要使用它来进行安全数据库通讯，以便访问 PostgreSQL。

10 单击 **Review and Launch** （查看并起动）。

11 查看细节后，单击 **Launch** （起动）。

12 选择现有的密钥对或创建新的密钥对。

此密钥对用于通过 SSH 访问实例。您可在多台计算机上使用相同密钥对。

13 单击 **Download Key Pair** （下载密钥对）。

重要：您只能使用私用密钥来连接和管理实例。因此，在下载密钥对后，请勿丢失私用密钥。

14 挂接初始化实例时创建的弹性 IP 地址。

15 重复步骤 1 至步骤 13 创建其他实例。

准备 EC2 实例

起动某个实例，并校验软件储存库。要校验配置的软件储存库，请执行以下操作：

1 使用密钥对登录某个实例。

2 切换到 `root` 用户。

3 校验您的操作系统中是否存在以下更新：

SLES 上的 SLES12-SP3-Pool 和 SLES12-SP3-Updates：要进行校验，请运行 `zypper lr -n` 命令。

RHEL 上的 rhui-REGION-rhel-server-releases/7Server/x86_64：要进行校验，请运行 `yum repolist` 命令。

注释：如果您的操作系统中没有储存库，请校验配置的弹性 IP 地址是否已挂接到该实例，然后重启动该实例。

4 为操作系统安装以下先决组件：

SLES

使用 `zypper` 命令安装 `glibc-32bit` 库。

Red Hat

使用 `yum install` 命令安装以下先决组件：

- `unzip`
- `ksh`
- `bc`
- `glibc-*.i686`
- `libXau-1.0.8-2.1.el7.i686`
- `libxcb.i686`
- `libX11.i686`
- `libXtst.i686`
- `libXrender.i686`
- `libgcc.i686`
- `lsof`

对于 Identity Manager 引擎，您可以编辑 `prerequisite.sh` 脚本，去除其中包含的 `compat-libstdc++-33.x86_64`。 Identity Manager 安装不再需要此包。

5 设置 `/etc/hosts` 和 `hostname`：

5a 使用实例的专用 IP 地址在防火墙中保护 Identity Manager 服务器。

5b 为实例指派 DNS 名称并更新 `hosts` 文件。

例如：

```
# 10.0.0.1 identityEngine.example.com identityEngine
```

5c 设置主机名和域名。

SLES

```
yast lan
```

RHEL

```
hostnamectl set-hostname idmengine.example.com
```

6 （视情况而定）创建加密的弹性块储存 (EBS) 卷，以加密云中的数据。

6a 单击 **Services > EC2** （服务 > EC2）。

6b 在 **Elastic Block Store** （弹性块储存）中，选择 **Volumes** （卷）并单击 **Create Volume** （创建卷）。

6c 指定所需的卷大小。

6d 选择 **Encrypt this volume** （加密此卷）并单击 **Create Volume** （创建卷）。

6e 在列表中选择新建的卷。

6f 在 **Actions** （操作）中单击 **Attach Volume** （挂接卷），将该卷挂接到 EC2 实例。

6g 对每个实例重复上述步骤。

有关 EBS 的详细信息，请参见 “Amazon EBS”。

7 使用操作系统工具格式化该卷并装入分区：

SLES

运行 `yast disk` 命令格式化该卷。

RHEL

运行 `mkfs` 进行格式化，并添加到 `/etc/fstab`。有关详细信息，请参见 《Red Hat Enterprise Linux Deployment Guide》（Red Hat Enterprise Linux 部署指南）。

注释：

- 装入 Identity Manager 引擎数据分区。数据分区默认为 `/var/opt/novell/`。
- 在 `/opt/netiq/` 中装入其他 Identity Manager 组件。

---

8 在所有实例上的 `/etc/hosts` 文件中，更新所有计算机的 DNS 或 IP 地址。

安装 Identity Manager 组件

在安装 Identity Manager 组件之前，请执行以下步骤：

1 在要安装 Identity Manager 组件的实例上下载 `Identity_Manager_4.9.0_Linux.iso`。

2 装入下载的 `.iso` 文件。

3 （视情况而定）创建 Identity Applications 和 Identity Reporting 的数据库。有关详细信息，请参见 “ 安装 Identity Applications 和 Identity Reporting 的数据库 ”（第 320 页）。

4 从 `.iso` 文件的根目录运行 `./install.sh` 命令。

5 通读许可协议，然后键入 `y` 接受许可协议。

6 选择自定义安装选项，然后选择要在实例上安装的组件。配置该组件。有关详细信息，请参见表 5-2 “ 自定义配置 ”（第 77 页）。

7 在 Identity Reporting 和 Identity Applications 上运行 `configupdate.sh` 以设置所有客户端。

安装 Identity Applications 和 Identity Reporting 的数据库

如果您要在外部服务器上安装 Identity Applications 和 Identity Reporting 的 PostgreSQL 数据库，应在安装前执行以下步骤：

1 导航到装入 `Identity_Manager_4.9.0_Linux.iso` 的位置。

2 找到 `/common/packages/postgres/` 目录并安装 PostgreSQL。

```
rpm -ivh netiq-postgresql-9.6.6-0.noarch.rpm
```

3 运行以下命令将组关联到 `postgres` 用户：

```
/usr/sbin/usermod -a -G postgres postgres
```

4 在 `/etc/passwd` 文件中，将 `postgres` 用户的主目录路径更改为 `/opt/netiq/idm/postgres/`。

4a 导航到 `/etc/` 目录。

4b 编辑 `passwd` 文件。

```
vi /etc/passwd
```

4c 将 postgres 用户的主目录更改为 /opt/netiq/idm/postgres/。

5 以 postgres 用户身份登录。

例如：

```
su - postgres
```

6 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
```

7 导出 PostgreSQL home 目录

```
export PGHOME=<postgres home directory path>
```

例如：

```
export PG_HOME=/opt/netiq/idm/postgres
```

8 导出 PostgreSQL 口令：

```
export PGPASSWORD=< 输入数据库口令 >
```

9 初始化数据库。

```
"LANG=en_US.UTF-8 <POSTGRES 主目录 >/bin/initdb -D <POSTGRES 主目录 >/
data"
```

例如：

```
"LANG=en_US.UTF-8 /opt/netiq/idm/postgres/bin/initdb -D /opt/netiq/idm/
postgres/data"
```

10 在 /opt/netiq/idm/postgres/ 目录中创建以下组件的数据库。

Identity Applications

```
$ createdb idmuserappdb
$ psql -s idmuserappdb
# create user idmadmin password 'somepassword';
# GRANT ALL PRIVILEGES ON DATABASE idmuserappdb TO idmadmin;
# ALTER DATABASE idmuserappdb OWNER TO idmadmin;
```

Identity Reporting

```
$ createdb idmrptdb
```

11 以 postgres 用户身份注销。

12 修改 postgresql.conf 文件，以允许 PostgreSQL 实例侦听除 localhost 以外的网络实例。

12a 导航到 /opt/netiq/idm/postgres/data/ 目录。

12b 编辑 postgresql.conf 文件：

```
vi postgresql.conf
```

12c 在文件中添加下列行：

```
listen_addresses = '*'
```

13 在 `<postgres home directory path>/data` 下创建 `pg_log` 目录。

例如：

```
mkdir -p /opt/netiq/idm/postgres/data/pg_log
```

14 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
```

15 启动 PostgreSQL 服务。

```
systemctl start netiq-postgresql
```

此命令将启动新的 PostgreSQL 服务。

安装 Designer

要使用 Designer，必须在 Windows 计算机上安装 Designer。

1 在公用子网中，起动支持的 Windows 实例。

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

2 在 Windows 实例上安装 Designer。有关详细信息，请参见 《*NetIQ Identity Manager 安装和升级指南 - Windows*》中的 “ 安装 Designer”。

创建 AWS EC2 负载平衡器

您可以创建负载平衡器在各个 Identity Manager 组件之间平衡传入请求的负载。负载平衡器可用于保护 Identity Manager 服务器免遭公共访问。

以下过程说明了为示例部署方案设置负载平衡器所需的配置细节：

为负载平衡器创建证书以使用安全通讯

负载平衡器使用此证书在各 Identity Manager 组件之间建立安全通讯。可通过三种方式为负载平衡器创建证书：

- “ 使用 AWS Certificate Manager (ACM)” （第 322 页）
- “ 将外部证书上载到 ACM” （第 323 页）
- “ 将外部证书上载到 IAM” （第 323 页）

使用 AWS Certificate Manager (ACM)

1 单击 **Services > Certificates Manager** （服务 > Certificates Manager）。

2 单击 **Request Certificate** （请求证书）。

3 指定要为其创建证书的 DNS 名称。

4 校验 DNS 机构。

将外部证书上载到 ACM

1 单击 **Services > Certificates Manager** （服务 > Certificates Manager）。

2 单击 **Import Certificate** （导入证书）。

3 指定证书细节。

将外部证书上载到 IAM

1 单击 **Services** （服务）。

2 在 **Security, Identity & Compliance** （安全性、身份与合规性）中，单击 **IAM**。

3 使用 IAM API 指定证书细节。有关详细信息，请参见 “Uploading Server Certificate Using IAM API” （使用 IAM API 上载服务器证书）。

创建目标组

使用目标组可将负载平衡器关联至负载将分散到的各个实例 （目标）的 IP 地址。

创建目标组需要执行的步骤如下：

1 在 EC2 仪表板中，单击 **LOAD BALANCING** （负载平衡）下的 **Target Groups** （目标组）。

2 单击 **Create target group** （创建目标组）。

3 指定以下细节：

字段	说明
Target group name （目标组名称）	指定目标组的名称。 您可以指定要配置此目标组的组件的名称。例如 Identity Applications、Identity Reporting。
协议	选择 **HTTPS**。
Port （端口）	指定服务器配置为要侦听的端口。 下面是不同 Identity Manager 组件使用的示例端口值： ◆ **Identity Applications：** 8543 ◆ **Identity Reporting：** 8643
Target type （目标类型）	选择 **Instance** （实例）。
VPC	选择您为 Identity Manager 组件实例所选的同一个 VPC。
Health Check Settings （运行状况检查设置）	

字段	说明
Protocol （协议）	选择 HTTPS。 负载平衡器在执行运行状况检查时将使用此协议。
Path （路径）	指定运行状况检查的目标路径。 要执行运行状况检查的 Identity Manager 组件的默认路径如下： ◆ **Identity Applications：** `/idmdash/index.html` ◆ **Identity Reporting：** `/IDMRPT/index.html`
Advanced health check settings （高级运行状况检查设置）	保留默认值。

4 单击 Create （创建）。

5 启用会话粘性。

5a 选择您创建的目标组。

5b 在 Description （说明）选项卡中，单击 Edit attributes （编辑属性）。

5c 对 Stickiness （粘性）选择 Enable （启用）。

6 重复上述步骤，为每个应用程序创建目标组。

注释：如果 SSPR 安装在其他服务器上，请为此组件单独创建一个目标组。

创建负载平衡器

创建负载平衡器需要执行的步骤如下：

1 在左侧菜单中，单击 Load Balancers （负载平衡器）。

2 单击 Create Load Balancers （创建负载平衡器）。

3 单击 Application Load Balancer （应用程序负载平衡器）下的 Create （创建）。

4 指定以下细节：

字段	说明
Name （名称）	指定负载平衡器的名称。
Scheme （纲要）	选择 internet-facing （面向因特网）。

字段	说明
Listeners（侦听器）	要为负载平衡器添加更多侦听器，请单击 Add Listener （添加侦听器）。 按如下所述指定侦听器端口： **对于 Identity Applications：** ◆ Load Balancer Protocol （负载平衡器协议）：HTTPS ◆ Load Balancer Port （负载平衡器端口）：8543 **对于 Identity Reporting：** ◆ Load Balancer Protocol （负载平衡器协议）：HTTPS ◆ Load Balancer Port （负载平衡器端口）：8643
Availability Zones （可用性区域）	1. 选择您之前为 Identity Manager 组件创建的同一个 VPC。 2. 选择可在其中使用公用子网的可用性区域。 **注释：**必须至少选择两个子网。
Tags （标记）	（可选）您可以添加一个标记来标识您的负载平衡器。

5 单击 Next: Configure Security Settings （下一步：配置安全性设置）。

6 指定证书细节以使用 HTTPS 协议。可执行以下操作之一：

- 选择您在 “ 为负载平衡器创建证书以使用安全通讯 ”（第 322 页）中创建的证书类型。
- 将证书上载到 IAM 或 ACM - 指定证书细节。

7 单击 Next: Configure Security Groups （下一步：配置安全组）。

8 在 Assign a security group （指派安全组）中，选择 Create a new security group （创建新的安全组）。

9 （可选）指定负载平衡器的名称和说明。

10 在安全组中添加规则，以便将流量路由到配置的侦听器：

字段	说明
Type （类型）	选择 Custom TCP Rule （自定义 TCP 规则）。
Protocol（协议）	如此会显示用于规则的协议类型。
Port Range（端口范围）	选择 Identity Manager 组件的端口范围： ◆ **Identity Applications：**8543 ◆ **Identity Reporting：**8643
Source（源）	选择 Anywhere （任意位置），以连接到部署了 Identity Manager 组件的实例。

11 单击 Next: Configure Routing （下一步：配置路由）。

12 在 Target group （目标组）中指定以下细节：

字段	说明
Target group （目标组）	选择 Existing target group （现有目标组）。此列表显示在 “ 创建目标组 ” （第 323 页）中为 Identity Manager 组件创建的目标组。
Name （名称）	从该列表中选择一个目标组。 在此处只能选择一个目标组。例如，选择您为 Identity Applications 创建的目标组。 创建负载平衡器后，您需要修改侦听器端口 8443，以使用针对 HTTPS 协议配置的目标组。请参见本节中的步骤 18 （第 326 页）。
Protocol （协议）	此字段中将填充您在指定的目标组中配置的值。请查看列出的值以确保其正确无误。
Port （端口）	此字段中将填充您在指定的目标组中配置的值。请查看列出的值以确保其正确无误。
Target type （目标类型）	此字段中将填充您在指定的目标组中配置的值。请查看列出的值以确保其正确无误。

13 查看 Health Checks （运行状况检查）下的以下细节：

字段	说明
Protocol （协议）	根据您在步骤 12 中选择的目标组配置，此字段中将填充 HTTPS 或 HTTP。 请参见 “ 创建目标组 ” （第 323 页）。
Path （路径）	此字段中将填充您在步骤 12 中选择的目标组内配置的运行状况 URL。 请参见 “ 创建目标组 ” （第 323 页）。
Advanced health check settings （高级运行状况检查设置）	保留默认值。

14 单击 Next: Register Targets （下一步：注册目标）。

注册到所选目标组的所有目标都会列出。您只能在创建负载平衡器之后修改此列表。

15 单击 Next: Review （下一步：检查）。

16 校验负载平衡器细节是否正确。

17 依次单击 Create （创建）、 Close （关闭）。

18 （视情况而定）如果您跳转到为 Identity Manager 组件创建侦听器端口的步骤，或者想要添加新的侦听器端口，请更新侦听器端口以使用相应的目标组：

18a 选择您创建的负载平衡器。

18b 选择 Listeners （侦听器）选项卡。

18c 单击 Add Listener （添加侦听器）并为每个侦听器指定所需的细节。详情请参见步骤 4。

18d 选择用于负载平衡器的证书。详情请参见“为负载平衡器创建证书以使用安全通讯”（第 322 页）。

18e 单击 Create （创建）。

如果将 SSPR 配置在单独的计算机上，则您可能需要添加一个侦听器。

重要：要在分布式设置中使用单个负载平衡器，请单独创建一条 DNS 别名记录来区分该设置中的服务器。否则，请为每个 Web 应用程序单独创建一个负载平衡器。

（可选）使用注册的托管区域创建别名 DNS

如果您已注册了某个站点，可以使用它为每个 Identity Manager 组件创建单个记录集。

1 单击 Services > Route 53 （服务 > Route 53）。

2 在左侧菜单中，单击 Hosted Zones （托管区域）并选择设置 AWS EC2 服务时创建的托管区域。请参见“准备 AWS Virtual Private Cloud”（第 315 页）。

3 单击 Go to Record Sets （转到记录集）。

4 单击 Create Record Set （创建记录集）：

字段	说明
Name （名称）	为记录集指定有意义的名称。 例如：将 Identity Applications 记录集命名为 `rbpm`。
Type （类型）	选择 A – IPv4 address （A – IPv4 地址）。
Alias （别名）	选择 Yes （是）。
Alias Target （别名目标）	选择配置为连接 Identity Manager 组件的负载平衡器
Routing Policy （路由策略）	选择 Simple （简单）

5 单击 Create （创建）。

6 重复步骤 4 和步骤 5，为每个 Identity Manager 实例创建一个记录集。

7 在 Identity Applications、Identity Reporting 和 OSP 实例上运行 `configupdate.sh`，并使用公用 DNS 名称更新 SSO 配置。

8 重启动 Tomcat。

9 通过使用公用 DNS 访问应用程序来校验配置。

`https://< 公用 DNS 名称 >:< 端口 >/< 应用程序环境名称 >`

访问 Identity Manager 组件

可以使用负载平衡器的公用 DNS 名称或使用别名 DNS 记录集来访问 Identity Manager 实例。要使 Identity Manager 实例能够互相通讯，请编辑每个实例上的 `/etc/hosts` 文件，并添加一项，以将此实例的主机名解析为其专用 IP 地址。

更新以下实例以在内部访问其他实例

实例	说明

OSP	OSP 实例需要访问 SSPR 实例才能重设置口令。
	主机文件位置：`/etc/hosts`
	修改 hosts 文件，在其中包含以下项：
	`<IP_address>  <Private_DNS_Name> <Public_DNS_Name>`
	例如：
	`10.0.1.5  sspr.privatedns.local sspr.publicdns.com`

Identity Applications	Identity Applications 实例需要访问 OSP 实例才能完成登录。
	主机文件位置：`/etc/hosts`
	修改 hosts 文件，在其中包含以下项：
	`<IP_address>  <Private_DNS_Name> <Public_DNS_Name>`
	例如：
	`10.0.1.6  osp.privatedns.local osp.publicdns.com`

Identity Reporting	Identity Reporting 实例需要访问 OSP 实例才能完成登录。
	主机文件位置：`/etc/hosts`
	修改 hosts 文件，在其中包含以下项：
	`<IP_address>  <Private_DNS_Name> <Public_DNS_Name>`
	例如：
	`10.0.1.6  osp.privatedns.local  osp.publicdns.comm`

安全考虑因素

NetIQ 建议您查看有关在 AWS 云中部署 Identity Manager 组件的以下注意事项：

- Identity Manager 组件是在不提供公共访问权限或者已挂接到弹性 IP 地址的专用网络中配置的。
- 通过负载平衡器来访问 Identity Applications、 Identity Reporting 等 Web 应用程序。
- Identity Manager 组件配置为使用安全通讯通道。
- 每个组件的数据是在单独的加密 EBS 卷上配置的。

- Identity Manager 服务器上的以下端口可以在子网中使用。

端口	应用程序
636	LDAP
8543	Identity Applications
8643	Identity Reporting
5432	PostgreSQL

29 混合 Identity Manager 方案示例

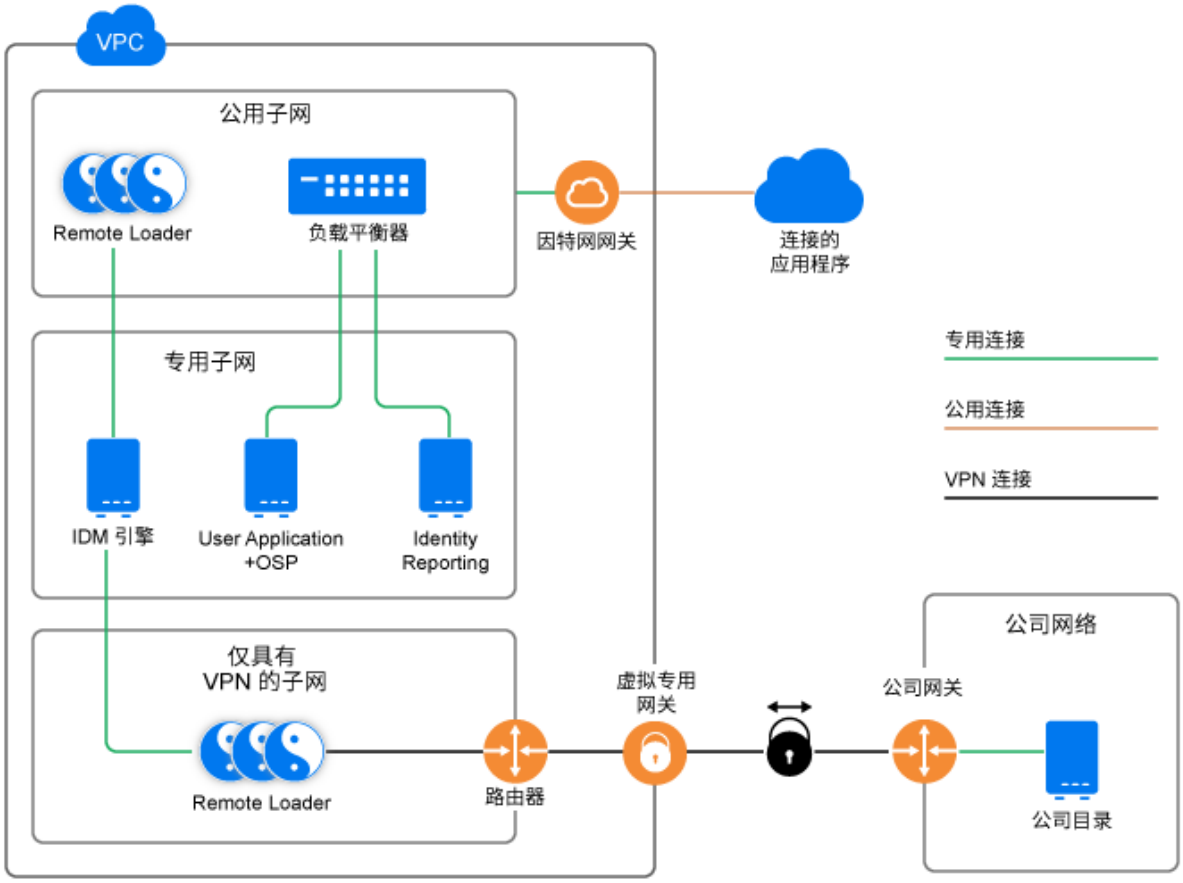
您可以对 Identity Manager 组件进行配置，使其中的身份在企业本地与 AWS 云之间无缝同步。实施此类混合方案需要您在 AWS 子网与企业网络之间配置 VPN 连接。本章将会对下面的混合 Identity Manager 方案进行说明：

- “使用 Remote Loader 连接”（第 331 页）
- “使用多服务器驱动程序集连接”（第 332 页）
- “使用 eDirectory 驱动程序连接”（第 333 页）

使用 Remote Loader 连接

Remote Loader 安装在配置了 VPN 的子网中。启用同步后， Remote Loader 驱动程序 shim 将连接到企业网络中运行的应用程序，并在 AWS 云中的 Identity Manager 与应用程序之间同步身份。

图 29-1 *使用 Remote Loader 连接的混合方案*



此方案适合用于连接的应用程序较少的系统，需要为 Remote Loader 打开一个侦听器端口。该连接仅允许在同步期间传递配置的属性。

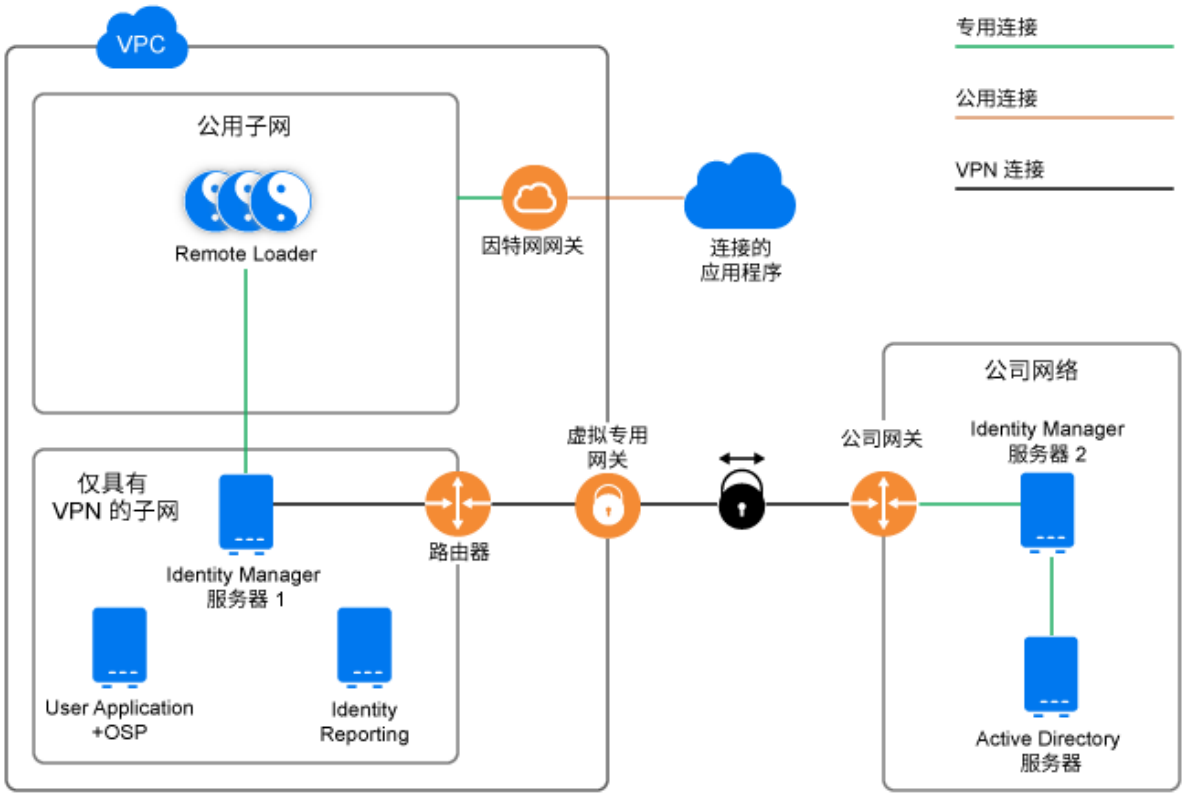
限制：

- 此方案适用于为 Remote Loader 的使用提供支持的驱动程序。
- 如果有大量连接的应用程序，传输至 Remote Loader 的流量将会增大。

使用多服务器驱动程序集连接

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

图 29-2 使用多服务器驱动程序集连接的混合方案

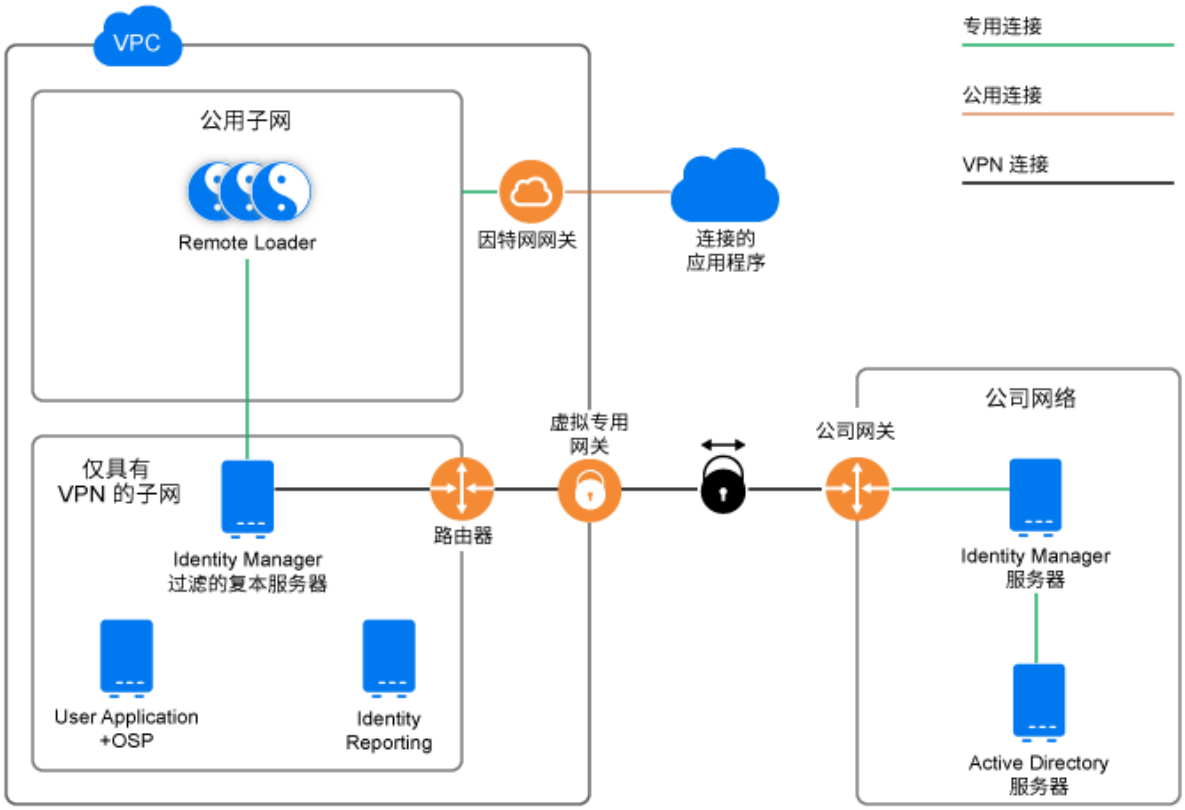


此配置仅将 VPN 连接用于同步任何一端的 Identity Manager 服务器之间的增量更改。

使用过滤复制

这是多服务器驱动程序集方案的一种变体，包含 AWS 云中服务器上的数据分区的已过滤读写复本。对于驱动程序集分区，应始终使用任何一端的完整复本分区。

图 29-3 使用受控复制的混合方案

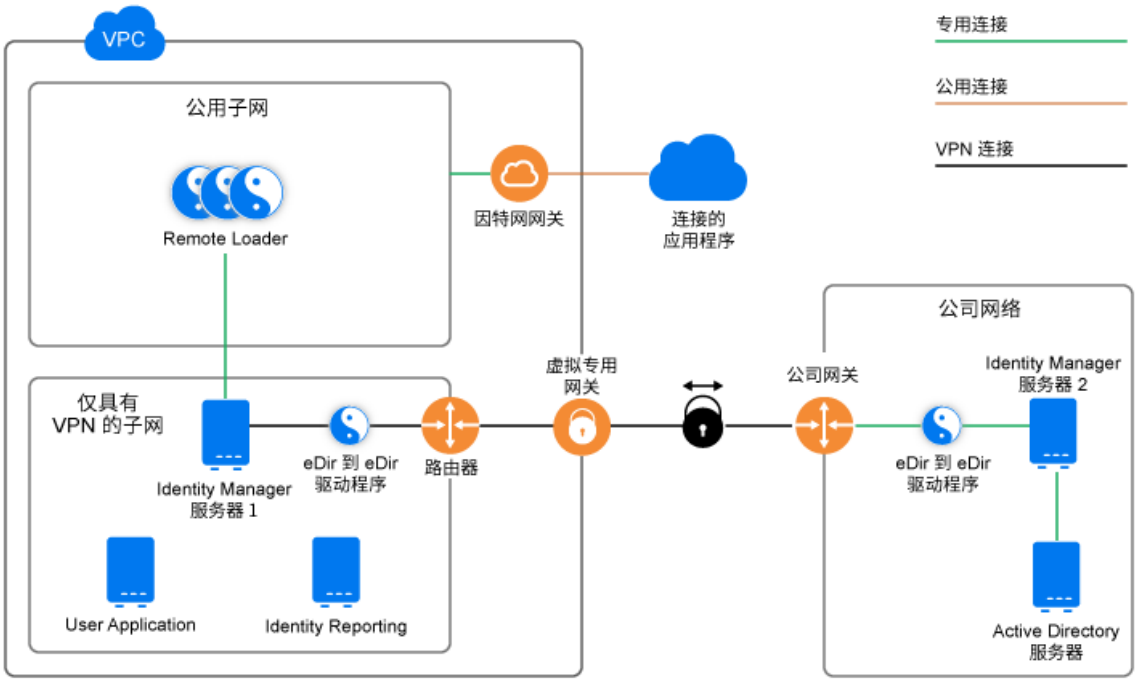


此方案增强了对要同步的属性的控制能力。例如，您可以防止与 AWS 云中的 Identity Manager 服务器同步敏感属性。

使用 eDirectory 驱动程序连接

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

图 29-4 使用 eDirectory 驱动程序连接的混合方案



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

XI 部署 Identity Manager 以实现高可用性

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

- 您可以在高可用性环境中安装以下组件：
  - 身份库
  - Identity Manager 引擎
  - Remote Loader
  - Identity Applications，不包括 Identity Reporting
- 要管理 Identity Manager 环境的网络资源可用性，请将 SUSE Linux Enterprise High Availability Extension 与已安装最新增补程序的 SUSE Linux Enterprise Server (SLES) 12 SP3 或更高版本搭配使用。
- 当您在群集环境中运行身份库时， Identity Manager 引擎也会群集化。

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

有关更多详细信息 ...	请参见 ...
确定 Identity Manager 组件的服务器配置	请参见 《NetIQ Identity Manager Overview and Planning Guide》（NetIQ Identity Manager 概述和规划指南）中的 “*High Availability Configuration*” （高可用性配置）。
在群集中运行身份库	“Identity Manager 群集部署解决方案示例 ” 《*NetIQ eDirectory Installation Guide*》（NetIQ eDirectory 安装指南）中的 “Deploying eDirectory on High Availability Clusters” （在高可用性群集上部署 eDirectory）
在群集中运行 Identity Applications	“Tomcat 应用程序服务器上的 Identity Applications 群集部署解决方案示例 ”

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

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

- 第 30 章 “ 在群集环境中安装 Identity Manager 的准备工作 ”（第 337 页）
- 第 31 章 “Identity Manager 群集部署解决方案示例 ”（第 341 页）
- 第 32 章 “Tomcat 应用程序服务器上的 Identity Applications 群集部署解决方案示例 ”（第 351 页）

30 在群集环境中安装 Identity Manager 的准备工作

- “ 先决条件 ”
- “ 为 Identity Applications 准备群集 ”

先决条件

- “ 身份库 ”（第 337 页）
- “Identity Applications”（第 338 页）
- “Identity Applications 的数据库 ”（第 338 页）

身份库

NetIQ 建议您在群集环境中安装身份库之前，先查看以下注意事项：

- 必须配备群集软件支持的外部共享储存，且其磁盘空间足以储存所有身份库和 NICI 数据：
  - 身份库 DIB 必须位于群集共享储存中。身份库的状态数据必须位于共享储存中，以供当前运行服务的群集节点使用。
  - 必须将每个群集节点上的根身份库实例配置为使用共享储存中的 DIB。
  - 此外，您还必须共享 NICI (NetIQ International Cryptographic Infrastructure) 数据，以便在群集节点之间复制服务器特定的密钥。所有群集节点使用的 NICI 数据必须位于群集共享储存中。
  - NetIQ 建议在共享储存中储存所有其他 eDirectory 配置和日志数据。
- 您必须有一个虚拟 IP 地址。
- （视情况而定）如果您使用 eDirectory 作为身份库的支持结构，`nds-cluster-config` 实用程序仅支持配置根 eDirectory 实例。 eDirectory 不支持配置多个实例，也不支持以非 root 身份在群集环境中安装 eDirectory。

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

Identity Applications

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

- 群集必须具有唯一的群集分区名称、多路广播地址和多路广播端口。使用唯一的标识符可以区分多个群集，防止出现性能问题和异常行为。
  - 对于群集的每个成员，必须为 Identity Applications 数据库的侦听端口指定相同的端口号。
  - 对于群集的每个成员，必须为托管 Identity Applications 数据库的服务器指定相同的主机名或 IP 地址。
- 必须同步群集中服务器的时钟。如果服务器时钟不同步，会话可能会提前超时，导致 HTTP 会话故障转移无法正常工作。
- NetIQ 建议不要在同一个主机上的浏览器选项卡或浏览器会话之间使用多个登录。某些浏览器在选项卡和进程之间共享 Cookie，因此，允许多个登录可能会导致 HTTP 会话故障转移出现问题 （此外，如果多个用户共享一台计算机，还可能会给鉴定功能带来意外的风险）。
- 群集节点位于在同一个子网中。
- 故障转移代理或负载平衡解决方案安装在单独的计算机上。

Identity Applications 的数据库

数据库群集属于各相关数据库服务器的功能。 NetIQ 不提供对任何群集数据库配置的官方测试，因为群集与产品功能不相关。因此，我们在支持群集数据库服务器的同时，作出以下声明：

- 默认情况下，最大连接数设置为 100。此值可能太低，无法处理群集中的工作流程请求负载。您可能会看到以下异常：

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

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

为 Identity Applications 准备群集

Identity Applications 支持 HTTP 会话复制和会话故障转移。如果某个执行中的会话所在的节点发生故障，则无需用户干预，该会话就能在群集中的另一个服务器上继续进行。在群集中安装 Identity Applications 之前，应先准备好环境。

- “ 了解 Tomcat 环境中的群集组 ”（第 339 页）
- “ 设置工作流程引擎 ID 的系统属性 ”（第 339 页）

了解 Tomcat 环境中的群集组

User Application 群集组使用 UUID 名称，以尽量减少与用户可能添加到其服务器中的其他群集组之间产生冲突的风险。您可以使用 User Application 管理功能修改 User Application 群集组的配置设置。只有在重启动服务器节点后，对群集配置所做的更改才能在该节点上生效。

设置工作流程引擎 ID 的系统属性

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

为确保工作流程引擎正常运行，必须设置 Tomcat 的系统属性。

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

31 Identity Manager 群集部署解决方案示例

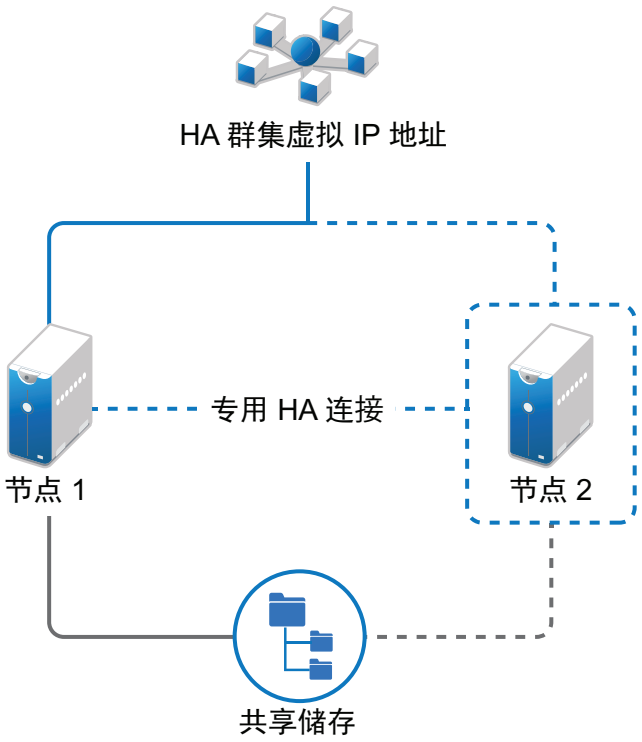
本章通过分步说明介绍如何在使用共享储存的受支持 SUSE Linux Enterprise Server (SLES) 群集环境中配置 eDirectory 和 Identity Manager，并提供了一个 Identity Manager 群集部署示例。

- “先决条件”（第 341 页）
- “安装过程”（第 342 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 31-1 （第 341 页）显示了一个群集部署解决方案示例。

图 31-1 *群集部署解决方案示例*



先决条件

- 两台运行 SLES 12 SP3 64 位的服务器作为节点
- 一台运行 SLES 12 SP3 64 位的服务器作为 iSCSI 服务器
- SLES12 SP3 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。

安装过程

本节说明在群集环境中安装 Identity Manager 的步骤。有关配置 SLES High Availability Extension 的详细信息，请参见《SUSE Linux Enterprise High Availability Extension 指南》。

- “ 配置 iSCSI 服务器 ”
- “ 在所有节点上配置 iSCSI 发起程序 ”
- “ 对共享储存进行分区 ”
- “ 安装 HA Extension”
- “ 设置 Softdog 检查包 ”
- “ 配置 HA 群集 ”
- “ 在群集节点上安装并配置身份库和 Identity Manager 引擎 ”
- “ 配置身份库资源 ”
- “eDirectory 和共享储存子资源的原始值 ”
- “ 更改位置约束分数 ”

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 SP3 后，在其他两个节点上安装 iSCSI 发起程序包。

在安装 SLES 12 SP3 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.sles12sp3node3.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。

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。

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**。

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**。

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个不同内核模块。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
```

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 同步的公共和私用 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：

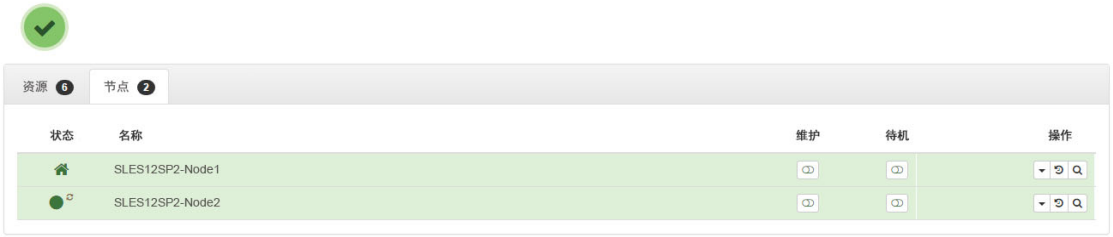
```
ha-cluster-join
```

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`。



在群集节点上安装并配置身份库和 Identity Manager 引擎

1 在群集节点上安装 Identity Manager 引擎：

1a 从 NetIQ 下载网站下载 `Identity_Manager_4.9.0_Linux.iso`。

1b 装入下载的 `.iso`。

1c 在 ISO 装入位置运行以下命令：

```
./install.sh
```

1d 通读许可协议。

1e 输入 `y` 以接受许可协议。

1f 决定要安装的 Identity Manager 服务器版本。输入 `y` 将安装高级版，输入 `n` 将安装标准版。

1g 从列表中选择 **Identity Manager 引擎**并继续安装。

此步骤将安装受支持的身份库版本。

2 在所有节点上配置 Identity Manager 引擎。

2a 导航到装入 `Identity_Manager_4.9.0_Linux.iso` 的位置。

2b 在 ISO 装入位置运行以下命令：

```
./configure.sh
```

2c 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。

2d 从列表中选择 **Identity Manager 引擎**组件。

2e 如果您是第一次配置身份库，请选择**创建新身份库**选项。如果您之前已安装身份库并想要连接到该身份库实例，请选择**添加到本地计算机上现有的身份库**或**添加到本地计算机上现有的身份库**选项。

3 导航到 `/etc/opt/novell/eDirectory/conf` 目录。

4 编辑 `nds.conf` 文件，并在 `n4u.nds.preferred-server` 字段中指定群集的虚拟 IP 地址。

5 停止身份库服务。

```
ndsmanage stopall
```

6 备份 `/var/opt/novell/nici`、`/etc/opt/novell/eDirectory/conf` 和 `/var/opt/novell/eDirectory/` 目录中的所有文件夹与文件。

7 导航到 `/opt/novell/eDirectory/bin` 目录。

8 运行以下命令：

```
nds-cluster-config -s /<shared cluster path>
```

其中，`<shared cluster path>` 表示您要用于身份库共享群集数据的位置。

9 启动身份库服务。

```
ndsmanage startall
```

有关在群集设置中配置身份库的详细信息，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）。

配置身份库资源

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**创建**。

5 单击**编辑配置**，然后单击在第 2 步中创建的组旁边的 ✎。

6 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 ”。

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 31-1 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	◆ start (60, 0) ◆ stop (60, 0) ◆ monitor (40, 20)
is-managed	Yes
resource-stickiness	100
target-role	Started

表 31-2 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	◆ start (100, 0) ◆ stop (100, 0) ◆ monitor (100, 60)
target-role	Started
is-managed	Yes
resource-stickiness	100
failure-timeout	125
migration-threshold	0

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 *-Infintity*。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。

---

32 Tomcat 应用程序服务器上的 Identity Applications 群集部署解决方案示例

本章通过示例部署来说明如何在 Tomcat 上的群集环境中配置 Identity Applications。

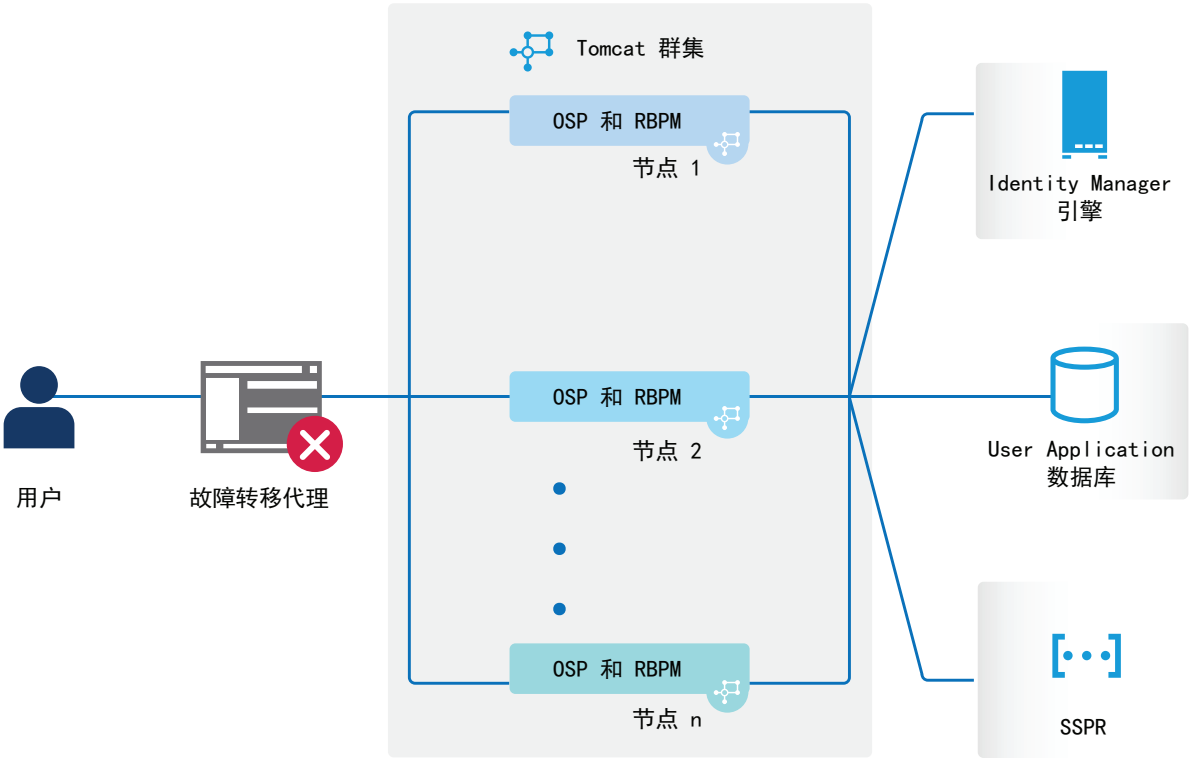
使用群集，您可以在多个并行服务器 （群集节点）上运行 Identity Applications，从而实现高可用性。要构建群集，您需要将几个 Tomcat 实例 （节点）组合在一起。负载将分布在不同的服务器之间，即使有服务器发生故障，您仍可通过其他群集节点来访问 Identity Applications。若要实现故障转移，您可以创建一个 Identity Applications 群集，然后将这些 Identity Applications 配置为充当单个服务器。不过，此配置不包括 Identity Reporting。

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

图 32-1 显示了一个包含双节点群集的示例部署，并做出如下假设：

- 所有通讯都通过负载平衡器路由。
- Identity Manager 引擎和 User Application 等组件安装在单独的服务器上。建议对生产级别部署使用此方法。
- 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。您可以根据自己的需要增加 User Application 实例数量。

图 32-1 群集部署解决方案示例



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

为了帮助您了解逐步配置，本文后续小节中通篇都会参照此示例部署。

先决条件

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。
- 群集中的服务器之间已同步时钟时间。否则，会话可能会提前超时，导致 HTTP 会话故障转移无法正常工作。
- NetIQ 建议不要在同一个主机上的浏览器选项卡或浏览器会话之间使用多个登录。某些浏览器在选项卡和进程之间共享 Cookie，因此，允许多个登录可能会导致 HTTP 会话故障转移出现问题 （此外，如果多个用户共享一台计算机，还可能会给鉴定功能带来意外的风险）。

- 群集节点位于在同一个子网中。
- 故障转移代理或负载平衡解决方案安装在单独的计算机上。
- 要实现表单群集化，请在服务器上启动两个负载平衡器实例，一个用于 Identity Applications，另一个用于表单渲染器。

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 353 页）
- “ 设置工作流程引擎 ID 的系统属性 ”（第 353 页）

了解 Tomcat 环境中的群集组

User Application 群集组使用 UUID 名称，以尽量减少与用户可能添加到其服务器中的其他群集组之间产生冲突的风险。您可以使用 User Application 管理功能修改 User Application 群集组的配置设置。只有在重启动服务器节点后，对群集配置所做的更改才能在该节点上生效。

设置工作流程引擎 ID 的系统属性

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

为确保工作流程引擎正常运行，必须设置 Tomcat 的系统属性。

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

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。

注释：在群集中，所有群集成员的配置设置都必须相同。将主节点中的 ism-sensitive.properties、 ism-configuration.properties 和 encrypt-keys.pkcs12 复制到所有 User Application 节点。

---

1. 安装 Identity Manager 引擎。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。

   在配置期间，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-42.6.1.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。
4. 在节点 2 上，安装并配置 Identity Applications。

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

   - `./balance 8543 apps1-au.edu.in:8543 ! apps2-au.edu.in:8543`
   - `./balance 8600 apps1-au.edu.in:8600 ! apps2-au.edu.in:8600`
6. 在单独的计算机上安装 SSPR。

   完成 SSPR 安装后，起动 SSPR (`https://<IP>:< 端口 >/sspr/private/config/editor`) 并登录其中。单击**配置编辑器** > **设置** > **安全性** > **Web 安全性** > **重定向白名单**。

   a. 单击**添加值**并指定以下 URL：

      `https://< 故障转移的 DNS>/osp`

   b. 保存更改。

   c. 在 SSPR 配置页面中，单击**设置** > **单点登录 (SSO) 客户端** > **OAuth**，然后修改 **OAuth 登录 URL**、 **OAuth 代码解析服务 URL** 和 **OAuth 配置文件服务 URL** 链接，具体做法是将 IP 地址替换为装有负载平衡器软件的服务器的 DNS 名称。

   d. 单击**设置** > **应用程序** > **应用程序**，然后更新**转发 URL** 和**注销 URL**，具体做法是将 IP 地址替换为装有负载平衡器软件的服务器的 DNS 名称。通过提供装有 SSPR 的服务器 / 系统的 IP 地址或主机名来更新**站点 URL**。

e. 要在节点 1 上更新 SSPR 信息，请起动位于 /opt/netiq/idm/apps/configupdate/ 中的配置实用程序。

```
./configupdate.sh
```

注释：您应只从 configupdate 目录运行 configudate.sh 文件。从自定义位置运行 configupdate.sh 将导致失败。

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 “Self Service Password Reset”（第 118 页）。

注释：校验节点 2 中是否更新了这些参数的值。

7. 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/common/jre/bin/keytool -genkey -storetype PKCS12 -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/common/jre/bin/keytool -genkey -storetype PKCS12 -
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。

8. （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
```

9. 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。
10. 将节点 1 上位于 /opt/netiq/idm/apps/osp/ 中的新 osp.jks 文件复制到群集中的其他 User Application 节点上。
11. 在每个群集节点上：
    a. 导航到 /opt/netiq/idm/apps/sites 目录，然后编辑 ServiceRegistry.json 文件以添加负载平衡器细节。

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

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

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

12. 在节点 1 中起动配置实用程序，并在 “SSO 客户端 ” 选项卡下将所有 URL 设置 （例如登录页的 URL 链接和 OAuth 重定向 URL）更改为负载平衡器 DNS 名称。

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

    b. 要在群集的所有其他节点中反映此更改，请将节点 1 上位于 `/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-configuration.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。
    - 将 `ism-configuration.properties` 文件从一个节点复制到另一个节点后，请确保对该文件具有 `novlua:novlua` 许可权限。
    - 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。

13. 指派对 `osp.jks` 文件的 `novlua` 许可权限：

    ```
    chown novlua:novlua osp.jks
    ```

14. 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`*。

15. 在 User Application 中启用群集。

    a. 在节点 1 上启动 Tomcat。

    不要启动任何其他服务器。

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

    c. 单击**配置** > **超速缓存和群集**选项。

    User Application 将显示 “ 超速缓存管理 ” 页面。

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

    e. 单击**保存**。

    f. 重启动 Tomcat。

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

User Application 群集使用 JGroups 在采用默认 UDP 的节点间进行超速缓存同步。如果您要更改此协议以使用 TCP，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 User Application Caching to use TCP"（将 User Application 超速缓存配置为使用 TCP）(https://www.netiq.com/documentation/identity-manager-47/identity_apps_admin/data/b6iiw3v.html)。

16. 为群集启用许可权限索引。
    a. 在 IDVault 中登录到 Identity Console，然后导航到**树视图**。
    b. 在树视图的左侧窗格中，选择**系统** > 包含 User Application 驱动程序的**驱动程序集**。
    c. 然后选择 **AppConfig** > **AppDefs**。
    d. 在右侧窗格中选择**配置**。
    e. 在**值属性**下选择 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>
       ```
    f. 单击**保存**。
17. 启用 Tomcat 群集。

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

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

    对于高级 Tomcat 群集配置，请按照 https://tomcat.apache.org/tomcat-8.5-doc/cluster-howto.html 中的步骤操作。
18. 在所有节点上重启动 Tomcat。
19. 为群集配置 User Application 驱动程序。

    在群集中，必须将 User Application 驱动程序配置为使用群集负载平衡器的 DNS 名称。可以使用 Identity Console 来配置 User Application 驱动程序。
    a. 登录到用于管理 Identity Manager 引擎的 Identity Console。
    b. 单击 **Identity Manager 管理**。
    c. 选择包含您的 User Application 驱动程序、 Role and Resource Service 驱动程序，以及数据收集服务驱动程序的驱动程序集。
    d. 单击 **User Application 驱动程序**图标。
    e. 转到**配置**选项卡。
    f. 在**驱动程序参数**下拉列表中，将**主机**更改为负载平衡器的主机名或 IP 地址。
    g. 单击**保存**。
    h. 重启动驱动程序。

20. 要更改 Roles and Resource Service 驱动程序的 URL，请重复步骤 19a 到 19e，然后单击**驱动程序参数**下拉列表，用负载平衡器 DNS 名称更新 **User Application URL**。
21. 确保针对 User Application 节点的负载平衡器软件中创建的群集启用了会话粘性。
22. 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）。

为群集启用许可权限索引

1 在节点 1 中登录到 Identity Console，然后导航到**树视图**。
2 在树视图的左侧窗格中，选择**系统** > 包含 User Application 驱动程序的**驱动程序集**。
3 然后选择 **AppConfig** > **AppDefs**。
4 在右侧窗格中选择**配置**。
5 在**值属性**下选择 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>
```

6 单击**保存**。

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 登录到用于管理身份库的 Identity Console 实例。
2 单击 **Identity Manager 管理**。
3 选择包含您的 User Application 驱动程序的驱动程序集。
4 单击 **User Application 驱动程序**图标。
5 转到**配置**选项卡。
6 在**驱动程序参数**下拉列表中，将**主机**更改为发送程序的主机名或 IP 地址。
7 单击**保存**。
8 重启动驱动程序。

为群集配置 OSP 和 SSPR

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

配置 SSPR 以支持群集

要在群集的第一个节点中更新 SSPR 信息，请起动 `/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。

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 " 配置忘记口令管理 "（第 92 页）。

2. 要更改 " 更改我的口令 " 链接，请参见 " 针对分布式环境或群集环境更新仪表板中的 SSPR 链接 "（第 96 页）。

3. 在群集中的其他节点上，校验 " 忘记口令 " 链接和 " 更改我的口令 " 链接是否已用 SSPR IP 地址更新。

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

   ---

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

   ```
   /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 4 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 在第一个节点中起动配置实用程序，并在 “SSO 客户端 ” 选项卡下将所有 URL 设置 （例如登录页的 URL 链接和 OAuth 重定向 URL）更改为负载平衡器 DNS 名称。

8a 保存配置实用程序中所做的更改。

8b 要在群集的所有其他节点中反映此更改，请将第一个节点上位于 /TOMCAT_INSTALLED_HOME/conf 中的 ism-configuration properties 文件复制到所有其他 User Application 节点。

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

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

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

---

9 在 /TOMCAT_INSTALLED_HOME/bin/ 目录下的 setenv.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。

33 卸装 Identity Manager 组件

本章介绍卸装 Identity Manager 各组件的过程。卸装某些组件需要满足一些先决条件。在开始执行卸装过程之前，请务必查看每个组件的相关完整章节。

注释：在开始卸装 Identity Manager 组件之前，请务必执行以下操作：

- 停止 Tomcat、 PostgreSQL 和 ActiveMQ 服务。
- 备份 `/var/opt/netiq/idm/log/` 目录中的安装日志文件。

从身份库中去除对象

卸装 Identity Manager 的第一步是删除身份库中的所有 Identity Manager 对象。创建驱动程序集时，向导将提示您将该驱动程序集作为分区。如果有任何驱动程序集对象也是 eDirectory 中的分区根对象，则您必须将该分区合并到父分区，然后才能删除驱动程序集对象。

要从身份库中去除对象，请执行以下操作：

1. 在继续操作之前，请对 eDirectory 数据库执行运行状况检查，然后修复出现的所有错误。

   有关详细信息，请参见 《*NetIQ eDirectory Administration Guide*》（NetIQ eDirectory 管理指南）中的 “Keeping eDirectory Healthy” （保持 eDirectory 稳定运行）。
2. 以对 eDirectory 树拥有完全权限的管理员身份登录到 Identity Console。
3. 选择**分区管理**。
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 。
5. 等待合并过程完成，然后单击**确定**。
6. 删除驱动程序集对象。

   当您删除驱动程序集对象时，删除过程将删除与该驱动程序集关联的所有驱动程序对象。
7. 对 eDirectory 数据库中的每个驱动程序集对象重复步骤 3 到步骤 6，直到将它们全部删除。
8. 重复步骤 1 以确保所有合并均已完成，且所有对象均已删除。

卸装 Identity Manager 引擎

安装程序提供了 Identity Manager 的卸装脚本。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：在卸装 Identity Manager 引擎之前，请准备好身份库。有关详细信息，请参见 “ 从身份库中去除对象 ”（第 361 页）。

要卸装 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 **Identity Manager 引擎**的值。

4 如果您要将身份库随 Identity Manager 引擎一起卸装，请对**是否要取消配置并卸装 IDVault** 参数指定 **y**，并指定以下细节：

- **身份库树名：**指定身份库树名。
- **身份库管理员名称：**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。

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 **Identity Applications** 的值。

卸装 Identity Reporting 组件

您必须按以下顺序卸装 Identity Reporting 组件：

1. 删除驱动程序。有关详细信息，请参见 “ 删除报告驱动程序 ”（第 363 页）。
2. 删除 Identity Reporting。有关详细信息，请参见 “ 卸装 Identity Reporting”（第 363 页）。
3. 删除 Sentinel。有关详细信息，请参见 “ 卸装 Sentinel Log Management for IGA”（第 363 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。

删除报告驱动程序

您可以使用 Designer 或 Identity Console 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**。
- **Identity Console**：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**。
- **Identity Console**：在“驱动程序集概述”页面上，单击**驱动程序 > 删除驱动程序**，然后单击要删除的驱动程序。

卸装 Identity Reporting

在删除 Identity Reporting 之前，请确保您已删除数据收集驱动程序和受管系统网关驱动程序。有关详细信息，请参见“删除报告驱动程序”（第 363 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 **Identity Reporting** 的值。

卸装 Sentinel Log Management for IGA

1 登录到 Sentinel 服务器。

2 导航到包含卸装脚本的目录：

```
/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装时，请按 `y`。

该脚本首先停止服务，然后完全去除它。

卸装 Designer

1 关闭 Designer。

2 要卸装 Designer

浏览到包含卸装脚本的目录，默认为 *<installation_directory>*`/designer/UninstallDesigner/Uninstall Designer for Identity Manager`。

要执行脚本，请输入 `./uninstall`

卸装 Analyzer

重要：Identity Manager 4.9 ISO 中不包含 Analyzer 工具。如果已安装 Analyzer，请务必将其更新到版本 4.8.5 并与 Identity Manager 4.9 搭配使用。

1. 关闭 Analyzer。
2. 根据操作系统卸装 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`

34 查错

本章提供有关对 Identity Manager 安装和升级问题进行查错的有用信息。有关其他查错提示，请参见特定组件的指南。

查找日志文件

Identity Manager 将维护日志以帮助用户调试任何问题。日志文件位于以下位置：

- 所有 Identity Manager 组件的安装日志文件：`/var/opt/netiq/idm/log/idminstall.log`
- 所有 Identity Manager 组件的配置日志文件：`/var/opt/netiq/idm/log/idmconfigure.log`
- User Application：`/opt/netiq/idm/apps/tomcat/logs/catalina.out` 和 `/opt/netiq/idm/apps/tomcat/logs/idapps.out`
- Identity Reporting：`/opt/netiq/idm/apps/tomcat/logs/localhost.<日期>.log`
- DCS：`/opt/netiq/idm/apps/tomcat/logs/catalina.out`
- eDirectory：`/var/opt/novell/eDirectory/log/ndsd.log`
- Tomcat：`/opt/netiq/idm/apps/tomcat/logs/catalina.out`
- OSP：`/opt/netiq/idm/apps/tomcat/logs/osp-idm.log`
- SSPR：`/opt/netiq/idm/apps/tomcat/logs/catalina.out`
- Sentinel Log Management for IGA：`/var/opt/novell/sentinel/log/server0.0log`
- 表单渲染器：`opt/netiq/common/nginix/logs`

登录相关问题查错

下表列出了您可能会遇到的问题，以及为解决这些问题建议执行的操作。如果问题仍然存在，请联系 NetIQ 代表。

问题	建议执行的操作
起动 Designer 时显示以下错误，并且 Designer 自述文件不显示： 异常 ..." 更新清单中缺少必需的 addons 属性。 "	忽略该错误并启动 Designer。功能不会受到任何影响。
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`。

问题	建议执行的操作
当您从 Identity Applications 页面注销时， SSPR 显示错误 `5053 ERROR_APP_UNAVALIABLE`。	忽略此错误，它不会导致功能受损。
在第一次登录 Identity Applications 时不提示询问应答	1. 确保 SSPR 服务器具有使用 FQDN 创建的证书。 2. 登录 User Application 服务器，并起动 ConfigUpdate (`/opt/netiq/idm/apps/configupdate/`) 实用程序。 3. 导航到 **SSO 客户端 > Self Service Password Reset**，并确保设置正确。 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`。
访问 SSPR URL 时浏览器显示空白页	未使用 OSP 正确配置 SSPR 时，会出现这种情况。 SSPR 日志会显示以下信息： `2018-01-24T22:24:02Z, ERROR, oauth.OAuthConsumerServlet, 5071 ERROR_OAUTH_ERROR (unexpected error communicating with oauth server: password.pwm.error.PwmUnrecoverableException: 5071 ERROR_OAUTH_ERROR (io error during oauth code resolver http request to oauth server: Certificate for <IP> doesn't match any of the subject alternative names: [IP]))`  1. 校验运行 OSP 的 Tomcat 服务器是否具有使用 FQDN 创建的有效证书。登录 User Application 服务器，并起动 ConfigUpdate 实用程序。导航到 **SSO 客户端 > Self Service Password Reset**，并确保设置正确。 2. 通过覆盖 OSP 登录方法登录 SSPR （例如，`https://<sspr sserver ip>:<port>/sspr/private/Login?sso=false`）。 3. 导航到页面右上角的**配置编辑器**。 4. 指定**配置口令**，然后单击**登录**。 5. 导航到 **LDAP > LDAP 目录 > 默认 > 连接**。 6. 如果 LDAP 证书不正确，请单击**清除**。 7. 要重新导入证书，请单击**从服务器导入**。 8. 导航到**设置 > 单点登录 (SSO) 客户端 > OAuth**，并在 **OAUTH Web 服务服务器证书**下校验证书是否正确。 9. 如果证书不正确，请单击**清除**。 10. 要重新导入证书，请单击**从服务器导入**。

问题	建议执行的操作
从不同的目录起动 ConfigUpdate 实用程序时发生错误	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 `/opt/netiq/idm/apps/configupdate/configupdate.sh` 命令起动 configupdate 实用程序，它不会起动。 您应导航到 `/opt/netiq/idm/apps/configupdate/` 目录，然后运行 `./configupdate.sh` 命令。

以管理员身份登录到分布式设置中部署的 SSPR 容器时，无法跳过系统提出的安全问题。	在 `ssprconfiguration.xml` 中，确保去除以下行中 `objectclass` 周围的任何多余空格：
	
	`<setting key="pwmAdmin.queryMatch" syntax="USER_PERMISSION" syntaxVersion="2">`
	
	`<label>Administrator Permission</label>`
	
	`<value>{"ldapProfileID":"default","ldapQuery":"(objectClass=*)","ldapBase":"cn=admin,ou=sa,o=system"}</value>`
	
	`<value>{"ldapProfileID":"default","ldapQuery":"(objectClass=*)","ldapBase":"cn=uaadmin,ou=sa,o=data"}</value>`
	
	`</setting>`

安装和卸装相关问题查错

下表列出了您可能会遇到的问题，以及为解决这些问题建议执行的操作。如果问题仍然存在，请联系 NetIQ 代表。

问题	建议执行的操作
在 Open Enterprise Server (OES) 24.2 上安装 Identity Manager 4.9 会导致依赖关系无法满足错误 （未安装 `glibc-32bit*.rpm`）。当升级到 Identity Manager 4.9 时，也会发生此错误。	在安装 Identity Manager 之前，请务必安装以下依赖库或 RPM： ◆ glibc-32bit-*.x86_64.rpm ◆ libz1-32bit 如果系统中已安装 `glibc-32bit-*.x86_64.rpm`，则可忽略此错误。
在 SLES 15 SP5 一体化配置中安装 Identity Manager 4.9 时，无法装载 SSPR 页面，并显示 SSPR 5203 CONFIG_FORMAT_ERROR。	重启动 Tomcat 服务。

问题	建议执行的操作
重启动系统 （其中的 Identity Manager 4.9 安装在 RHEL 8 操作系统上）后，您无法访问 Identity Manager 仪表板。`catalina.log` 文件包含以下警告讯息： `WARN [com.novell.soa.af.impl.core.WorkflowEngineImpl] (main) [WORKFLOW] Duplicate engine id detected.This engine may not have been shutdown cleanly or another engine is running with engine-id: ENGINE.Waiting 60000 ms for heartbeat to timeout.` 如果重启动系统之前未停止 Tomcat 服务，则会出现此问题。当工作流程引擎启动时，它会遇到群集中的另一个节点，而该节点的引擎 ID 已被使用，因此工作流程引擎会记录警告。	始终建议在重启动系统之前停止 Tomcat 服务。如果您确实看到了该警告，可以通过更改 `igaworkflowdb` 数据库中 afenginestate 表内的引擎状态来解决问题。登录到 pgAdmin 之类的数据库管理工具，并手动将引擎状态更新为关闭状态。
在 RHEL 8.3 上安装 Identity Manager 4.9 时，PostgreSQL 服务无法正常启动。	请执行下列步骤： 1. 在 RHEL 8 上安装 Identity Manager 4.9。 2. 将 RHEL OS 版本升级到 8.3。

当您在 SLES 15 或 SLES 15 SPx （x 表示 Identity Manager 支持的所有 SLES 15 版本）上安装 Identity Manager 时， Tomcat 和 ActiveMQ 服务处于禁用状态。	请执行下列步骤：
	
	1. 登录到禁用了 Tomcat 和 ActiveMQ 服务的服务器。
	2. 安装 `insserv-compat*` RPM。 * 符号表示 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。
	
	3. 运行以下命令以启用 Tomcat 和 ActiveMQ 服务：
	
	`systemctl enable netiq-tomcat.service`
	
	`systemctl enable netiq-activemq.service`

问题	建议执行的操作

如果您是在 RHEL 8.1 上安装 Identity Manager 4.9，执行以下操作时会显示如下错误讯息：
• 运行 `RHEL-Prerequisite.sh` 脚本：
`dnf-utils rpm required but not found`
`RHEL 8.1 iso does not contain dnf-utils packages, its replaced by yum-utils`
• 安装 Identity Manager 引擎组件：
`Some of the dependencies required for installation of Identity Vault are not found`
	请忽略错误讯息并继续安装。

将 Identity Applications 升级到版本 4.9 后，工作流程表单无法在 Identity Applications 上呈现。在某些情况下，`/opt/netiq/idm/apps/sites/config.ini` 中的客户端口令 (CientPass) 会保留空白。	要解决此问题，请执行以下步骤： 1. 导航到 `/opt/netiq/idm/apps/sites/` 目录。 2. 编辑 config.ini 文件，为 `ClientPass` 参数提供 base64 编码的口令。 **注释：**指定您在配置更新实用程序中为 **forms client** 所指定的相同口令。 3. 重启动 NGINX 服务。 `systemctl restart netiq-nginx.service` 有关详细信息，请参见 TID 7024492。
在容器环境中，如果超过了针对 Identity Manager 仪表板设置的空闲时间并且会话超时，**延长**按钮不会按预期工作。	在 OSP 容器的 `ism-configuration.properties` 文件中添加 `com.netiq.idm.session-timeout` 属性。
在多服务器环境中，尝试将驱动程序部署到次要服务器时显示 LDAP 异常。	安装次要服务器并在身份库中为次要服务器添加分区之后，必须在两台服务器上重启动 `ndsd`。如果您要在容器部署过程中安装 Identity Manager 引擎，此规则同样适用。
在群集环境中，如果您断开某个节点 （例如节点 2）与网络的连接，然后在主动节点 （例如节点 1）上创建角色，当节点 2 重新连接到网络后，新添加的角色不会同步到节点 2 上。	在节点 2 上执行以下步骤： 1. 删除 `.../temp/permindex` 文件。 2. 重启动 Tomcat。
在配置 Identity Applications 期间，如果您要连接到远程服务器上安装的 SSPR，将会跳过 SSPR 配置。但是，当您重启动 Tomcat 时，系统将会部署在安装过程中安装的 `sspr.war`。	如果您要连接到远程服务器上安装的 SSPR，请在配置 Identity Applications 之前，先从 `/opt/netiq/idm/apps/tomcat/webapps` 目录中去除 `sspr.war`。

问题	建议执行的操作
在配置 Identity Applications 期间，如果您为 Identity Applications 管理员使用自定义子容器（例如 cn=uaadmin,ou=univ,o=data），则会在默认容器 (ou=sa,o=data) 下创建 uaadmin。	如果您要为 Identity Applications 管理员使用自定义子容器，请执行以下步骤之一： ◆ 在配置 Identity Applications 之前，创建 ou=univ,o=data 自定义子容器。 ◆ 在配置过程中，请在出现**是否要使用自定义容器作为根容器**提示时指定**否**。要导入的自定义 LDIF 文件应包含自定义根容器和子容器细节。
创建无提示属性文件时，无提示安装过程不检查系统要求。在无提示安装期间，日志文件显示一条错误讯息，指出不符合系统要求。	如果遇到此错误，请在 silent.properties 文件中手动添加 IS_SYSTEM_CHECK_DONE 参数。要跳过系统要求检查，请将 IS_SYSTEM_CHECK_DONE 参数的值设置为 1。
卸装和重新安装 Identity Applications 或 Identity Reporting 时，配置过程在设置数据库用户与纲要时失败。如果在重新安装组件期间进行典型配置，则会出现此问题。	重新安装 Identity Applications 或 Identity Reporting 组件时，必须进行自定义配置。
卸装过程报告未完成，但日志文件未显示失败信息。	默认情况下，卸装过程无法删除包含安装文件的 netiq 目录。如果已从计算机中去除所有 NetIQ 软件，则您可以删除该目录。

升级相关问题查错

下表列出了您可能会遇到的问题，以及为解决这些问题建议执行的操作。如果问题仍然存在，请联系 NetIQ 代表。

问题	建议执行的操作
在 Open Enterprise Server (OES) 24.2 上升级 Identity Manager 引擎时， idmupgrade.log 日志中报告了以下错误： [SEVERE]: Could not connect to the server Exception: Connect ErrorLDAPException: I/O Exception on host <IP_address>, port <port_number> Connect Error java.net.SocketException: Connection or outbound has closed	忽略此错误，它不会导致功能受损。

问题	建议执行的操作
Identity Manager 使用数字证书进行授权并与其组件安全通讯。必须将身份库证书导入 `idm.jks` 和 `tomcat.ks` 密钥储存区文件。但是，导入证书后尝试访问 Identity Applications 时，您可能会遇到以下错误： `javax.net.ssl.SSLHandshakeException: PKIX path validation failed: java.security.cert.CertPathValidatorException: Could not determine revocation status.` 通过检查 CRL 分发点 (CDP) 字段指定的证书撤消列表 (CRL) 来验证证书，以确定证书是否已撤消。根证书以及密钥存储区文件 `tomcat.ks` 和 `idm.jks` 中的中间证书都会提供 CRLDP。但是，默认已禁用证书撤消检查。因此， PKIX 信任管理器无法确定证书的撤消状态。	要解决此问题，请通过将 `-Dcom.sun.security.enableCRLDP` 属性设置为 `true` 来启用 CRL 分发点检查。 要设置该属性，请执行以下操作： 1. 停止 Tomcat。 2. 转到位于 Tomcat 的 `bin` 目录中的 `setenv.sh` 文件。例如 `/opt/netiq/idm/apps/tomcat/bin/setenv.sh`。 3. 如下所示在 CATALINA_OPTS 中添加属性 `-Dcom.sun.security.enableCRLDP=true`： `export CATALINA_OPTS="-Dcom.sun.security.enableCRLDP=true"` 4. 启动 Tomcat。
升级 Identity Manager 后，非管理员用户在 Identity Manager 仪表板中的登录速度非常缓慢。装载 “ 应用程序 ” 和 “ 仪表板 ” 页面时存在很高的延迟。 此问题是由默认启用的嵌套组搜索造成的。不管环境中是否存在任何嵌套组，应用程序都会通过嵌套组成员资格查找已登录用户继承的许可权限。	（视情况而定）以下步骤适用于 Identity Manager 4.9： 1. 登录到其中的 Identity Applications 已升级到版本 4.9 的服务器。 2. 导航到 `/opt/etiq/idm/apps/tomcat/conf/` 位置。 3. 在文本编辑器中打开 `ism-configuration.properties` 文件。 4. 在该文件的末尾添加以下属性： `DirectoryService/realms/jndi/params/USE_NESTED_GROUPS=false` 5. 保存该文件并重启动 Tomcat。

问题	建议执行的操作
将 Identity Applications 从旧版升级到版本 4.9 后，表单渲染器不按预期工作。将默认 IDMProv 部署环境修改为自定义环境后会出现此问题。	要解决此问题，请执行以下步骤： 1. 登录到其中的 Identity Applications 已升级到版本 4.9 的服务器。 2. 导航到 `/opt/netiq/idm/apps/sites` 目录。 3. 编辑 `ServiceRegistry.json` 文件。 4. 将部署环境从 `IDMProv` 修改为在升级之前指定的自定义环境。 5. 保存 `ServiceRegistry.json` 文件。 6. 导航到 `/opt/netiq/idm/apps/sites/forms/` 目录。 7. 编辑 `main.<version>.js` 文件，其中 *<version>* 是随机生成的字母数字值。 8. 将部署环境从 `IDMProv` 修改为在升级之前指定的自定义环境。 9. 保存 `main.<version>.js` 文件。 10. 重启动 Tomcat。
将分布式环境中的 Identity Manager 升级到版本 4.9 后，登录 Identity Applications 失败。显示以下错误讯息： 您的登录过程未成功完成。 登录 Identity Applications 需要提供信任锚证书，以便在 Identity Applications 与 OSP 之间建立安全连接。信任锚证书必须包含 “ 主题类型 ” 设置为 “CA” 的 “ 基本限制 ” 扩展。 Identity Manager 利用属性 `jdk.security.allowNonCaAnchor` 来验证证书中的信任锚。此属性默认设置为 `false`。因此，如果在证书中找不到信任锚，则无法在 Identity Applications 与 OSP 之间建立连接，登录也会失败。您将在 `idm-osp.log` 文件中看到以下异常： `sun.security.validator.ValidatorException: TrustAnchor with subject "CN=***, L=***, O=***" is not a CA certificate`	要解决此问题，必须满足下列任一条件： ◆ 确保用于在 Identity Applications 与 OSP 之间建立安全连接的证书是包含正确 “ 基本限制 ” 扩展的可信 CA 证书。 ◆ 如果使用的是客户端信任的自我签名证书和自定义证书，您可以更改属性 `jdk.security.allowNonCaAnchor`，以允许使用不包含 “ 基本限制 ” 扩展的非 CA 证书。请执行以下操作来修改 Java 安全性设置： 1. 导航到 `/opt/netiq/common/jre/lib/security/java.security` 目录。 2. 设置属性值 `jdk.security.allowNonCaAnchor=true`。 3. 保存文件。

问题	建议执行的操作
升级到 Identity Applications 4.9 版本后，在 Identity Applications 仪表板中请求许可权限时无法打开表单。	要解决此问题，请使用以下命令手动重启动 NGNIX 和 Golang 服务： ◆ **NGNIX：** `/opt/netiq/common/ngnix/ngnix` ◆ **Golang：** `/etc/init.d/netiq-golang.sh` Identity Applications 使用 NGNIX 服务在 Identity Applications 仪表板中呈现表单。
在标准版中升级 Identity Reporting 后，`configupdate.sh.properties` 中的 **is_prov** 参数设置为 `true`。因为 Identity Applications 在标准版中不可用，所以此参数的值必须设置为 `false`。	在 `configupdate.sh.properties` 文件中手动将 **is_prov** 参数设置为 `false`。
如果先前的 Identity Manager 引擎升级失败，将无法重新运行 Identity Manager 引擎安装程序。例如，如果第一次尝试将 Identity Manager 引擎升级到 4.9 失败，然后再次尝试升级 Identity Manager 引擎，则无法触发升级过程。	请执行下列步骤： 1. 使用 `novell-DXMLengnx` RPM 将 Identity Manager 引擎降级到旧版本。 2. 升级 Identity Manager 引擎。
升级 Identity Manager 后，以下属性会添加到 `ism-configuration.properties` 文件中： `com.netiq.idm.osp.ldap.admin-dn = cn=admin,ou=sa,o=system`	请在 `ism-configuration.properties` 文件中注释掉该属性，然后重启动 Tomcat。它不会导致功能受损。
升级 Identity Manager 后，即使您的部署中不包含 SSPR，系统也会将以下 SSPR 属性添加到 `ism-configuration.properties` 文件中： `com.netiq.sspr.redirect.url = https://___SSPR_IP___:___SSPR_TOMCAT_HTTPS_PORT___/sspr/public/oauth`	请在 `ism-configuration.properties` 文件中注释掉该属性，然后重启动 Tomcat。它不会导致功能受损。
升级 Identity Manager 后， `ism-configuration.properties` 文件中会填充 `java.protocol.handler.pkgs` 属性的某些重复值。	不会出现功能受损的情况。要解决此问题，请执行以下操作： 1. 导航到 `/opt/netiq/idm/apps/tomcat/conf` 目录中的 `ism-configuration.properties` 文件。 2. 修改 `ism-configuration.properties` 文件，去除 `java.protocol.handler.pkgs` 属性的重复值。 3. 保存该文件并重启动 Tomcat。

问题	建议执行的操作
升级 Identity Manager 后无法启动 Tomcat。在 Tomcat 日志中，您会发现几项异常以及工作流程引擎与身份库之间的通讯失败事件。	1. 登录到 Identity Console。 2. 导航到**证书管理** > **服务器证书管理**。 3. 选中 **SSL 证书 DNS** 复选框并单击**导出**。 4. 在**证书**下拉列表中，选择 *SSL CertificateDNS*。 5. 清除**导出私用密钥**复选框。确保**导出格式**设置为 *DER*。 6. 单击**确定** > **保存导出的证书**将证书下载到您的系统中。 7. 登录到 Identity Applications 服务器。 8. 停止 Tomcat。 9. 导航到 `opt/netiq/common/jre/bin` 目录，并使用以下命令将证书导入到 `idm.jks` 文件： `opt/netiq/common/jre/bin/keytool -import -trustcacerts -alias <证书别名> -keystore /opt/netiq/idm/apps/tomcat/conf/idm.jks -file <下载的证书文件>` 10. 重启动 Tomcat。

Ansible 部署相关问题查错

下表列出了您可能会遇到的问题，以及为解决这些问题建议执行的操作。如果问题仍然存在，请联系 NetIQ 代表。

问题	建议的操作
在部署中首次运行 `deploy.yml` 时，您会看到以下讯息，指出目标节点上不存在 Docker 映像。例如，如果您正在部署 Core DNS 容器，您将看到以下错误： `fatal: [<ip address/DNS>]: FAILED! => {"changed": true, "cmd": "docker images | grep coredns | grep 1.8.0", "delta": "0:00:00.914078", "end": "msg": "non-zero return code", "rc": 1, "start": "stderr": "", "stderr_lines": [], "stdout": "", "stdout_lines": []}`	目前没有任何解决方法。但是，您可以忽略该讯息并继续部署。这不会造成任何功能性损失。
如果 IP 地址已被网络中的其他容器使用，容器部署将会失败。控制台会报告以下异常。 `fatal: [<ip address/DNS>]: FAILED! => {"changed": false, "msg": "Error starting container b1eb07f42cf6bd63787ae6167f5e3a0f7cbee0f8be80a5764bcc7c7f9d6b96b1 : 403 Client Error for http+docker://localhost/v1.40/containers/b1eb07f42cf6bd63787ae6167f5e3a0f7cbee0f8be80a5764bcc7c7f9d6b96b1 /start: Forbidden (\"Address already in use\")"}`	为容器指派不同的 IP 地址。

问题	建议的操作

部署 Identity Applications 容器后，当您登录到 Identity Manager 仪表板并导航到任务页面时，仪表板不按预期提取任务列表。 `catalina.out` 文件中报告了以下错误。
 	
`SEVERE [main] org.apache.catalina.startup.ContextConfig.processAnnotationsWebResource Unable to process web resource [/WEB-INF/classes/com/microfocus/idm/nrf/resources/NRFRsrc_fr.class] for annotations`
`java.io.EOFException`
`at java.io.DataInputStream.readFully(DataInputStream.java:197)`
`at java.io.DataInputStream.readUTF(DataInputStream.java:609)`
`at java.io.DataInputStream.readUTF(DataInputStream.java:564)`
`at org.apache.tomcat.util.bcel.classfile.ConstantUtf8.getInstance(ConstantUtf8.java:36)`
`at org.apache.tomcat.util.bcel.classfile.Constant.readConstant(Constant.java:79)`
`at org.apache.tomcat.util.bcel.classfile.ConstantPool.<init>(ConstantPool.java:53)`
`at org.apache.tomcat.util.bcel.classfile.ClassParser.readConstantPool(ClassParser.java:174)`
`at org.apache.tomcat.util.bcel.classfile.ClassParser.parse(ClassParser.java:83)`
`at org.apache.catalina.startup.ContextConfig.processAnnotationsStream(ContextConfig.java:2351)`
`at org.apache.catalina.startup.ContextConfig.processAnnotationsWebResource(ContextConfig.java:2250)`
`at org.apache.catalina.startup.ContextConfig.processAnnotationsWebResource(ContextConfig.java:2244)`
`at org.apache.catalina.startup.ContextConfig.processAnnotationsWebResource(ContextConfig.java:2244)`
`at org.apache.catalina.startup.ContextConfig.processAnnotationsWebResource(ContextConfig.java:2244)`
`at org.apache.catalina.startup.ContextConfig.processAnnotationsWebResource(ContextConfig.java:2244)`
`at org.apache.catalina.startup.ContextConfig.processAnnotationsWebResource(ContextConfig.java:2244)`
`at org.apache.catalina.startup.ContextConfig.processClasses(ContextConfig.java:1397)`
`at org.apache.catalina.startup.ContextConfig.webConfig(ContextConfig.java:1302)`
`at org.apache.catalina.startup.ContextConfig.configureStart(ContextConfig.java:985)`
	要解决此问题，请执行以下步骤：
	
	1. 导航到 `/opt/netiq/idm/apps/tomcat/webapps/` 目录。
	2. 删除 `workflow` 文件夹。
	3. （可选）重启动 Tomcat。

AKS 部署相关问题查错

下表列出了您可能会遇到的问题，以及为解决这些问题建议执行的操作。如果问题仍然存在，请联系 NetIQ 代表。

问题	建议的操作

在 Azure 门户中运行 Terraform 命令时，您可能会遇到阻碍基础结构部署的错误。下面列出了一些可能的错误。
 	
`Error: making Read request on Azure KeyVault Secret slesvmpwd: azure.BearerAuthorizer#WithAuthorization: Failed to refresh the Token for request to https://idmkv88211894240361.vault.azure.net/secrets/slesvmpwd/?api-version=7.1: StatusCode=401 -- Original Error: adal: Refresh request failed.Status Code = '401'.Response body: {"error":{"code":"invalid_request","message":"Required audience parameter not specified"}} Endpoint http://localhost:50342/oauth2/token | | with module.server.data.azurerm_key_vault_secret.slesvmpwd, | on sles15sp2-server/main.tf line 42, in data "azurerm_key_vault_secret" "slesvmpwd": | 42: data "azurerm_key_vault_secret" "slesvmpwd" { kubernetes_secret.example3: Creation complete after 1s [id=idm/ingress-tls] ? | Error: error detecting capabilities: error PostgreSQL version: dial tcp 52.186.162.130:5432: connect: connection timed out | | with module.dbserver.postgresql_database.igaworkflowdb, | on Azure-PG-Server/main.tf line 217, in resource "postgresql_database" "igaworkflowdb": | 217: resource "postgresql_database" "igaworkflowdb" { | az aks get-credentials --resource-group rajj_rg --name cluster-name --overwrite-existing | Error: making Read request on Azure KeyVault Secret uawfedbuser: azure.BearerAuthorizer#WithAuthorization: Failed to refresh the Token for request to https://idmkv80357639695488.vault.azure.net/secrets/uawfedbuser/?api-version=7.1: StatusCode=401 -- Original Error: adal: Refresh request failed.Status Code = '401'.Response body: {"error":{"code":"invalid_request","message":"Required audience parameter not specified"}} Endpoint http://localhost:50342/oauth2/token | | with module.dbserver.data.azurerm_key_vault_secret.uawfedbuser, | on Azure-PG-Server/main.tf line 28, in data "azurerm_key_vault_secret" "uawfedbuser": | 28: data "azurerm_key_vault_secret" "uawfedbuser" { module.dbserver.null_resource.delay: Creation complete after 5m0s [id=5961346882319865424] ?| Error: waiting for creation of Managed Kubernetes Cluster "test-akscluster" (Resource Group "idmtest_rg"): Code="ReconcileStandardLoadBalancerError" Message="Reconcile standard load balancer failed.Details: outboundReconciler retry failed: Category: ClientError; SubCode: PublicIPCountLimitReached; Dependency: Microsoft.Network/PublicIPAddresses; OrginalError: Code=\"PublicIPCountLimitReached\" Message=\"Cannot create more than 10 public IP addresses for this subscription in this region.\" Details=[]; AKSTeam: Networking, Retriable: false." | | with module.aks.azurerm_kubernetes_cluster.main, | on .terraform/modules/aks/main.tf line 10, in resource "azurerm_kubernetes_cluster" "main": | 10: resource "azurerm_kubernetes_cluster" "main" {`
	要解决此问题，请执行以下步骤：
	
	1. 登录到 Azure 门户。
	2. （可选）找到 Azure Kubernetes 群集配置文件路径。
	3. 运行以下命令重写默认配置文件 ~/.kube/config。
	
	`aks get-credentials --resource-group <资源组名称> --name <kube 群集名称> --overwrite-existing`
	
	`export KUBE_CONFIG_PATH=~/.kube/config`
	
	4. 重运行 Terraform 命令。有关详细信息，请参见“使用配置生成器进行部署”中的步骤 14、步骤 15、步骤 16。

问题	建议的操作
当您尝试在 Azure 上创建公共 IP 地址时，可能会出现以下错误。 `| Error: waiting for creation of Managed Kubernetes Cluster "cluster-name" (Resource Group "raj_rg"): Code="ReconcileStandardLoadBalancerError" Message="Reconcile standardload balancer failed.Details: outboundReconciler retry failed: Category: ClientError; SubCode: PublicIPCountLimitReached; Dependency: Microsoft.Network/PublicIPAddresses;OrginalError: Code=\"PublicIPCountLimitReached\" Message=\"Cannot create more than 10 public IP addresses for this subscription in this region.\" Details=[]; AKSTeam: Networking, Retriable: false." | | with module.aks.azurerm_kubernetes_cluster.main, | on .terraform/modules/aks/main.tf line 10, in resource "azurerm_kubernetes_cluster" "main": | 10: resource "azurerm_kubernetes_cluster" "main" {`	请联系 Azure 小组来提高订阅配额，或尝试去除已指派的但未使用的公共 IP 地址。

问题	建议的操作

在 Azure 门户中运行 `terraform apply` 命令时，可能会出现以下异常：
 	
`(AgentPoolK8sVersionNotSupported) 版本 < 版本 > 在此区域中不受支持。请使用 [az aks get-versions] 命令获取此区域中支持的版本列表。有关详细信息，请查看 https://aka.ms/supported-version-list`
	要解决此问题，请执行以下步骤：
	
	1. 登录到 Azure 门户。
	2. 单击  。
	3. 运行以下命令来确定您所在位置支持的版本：
	
	`az aks get-versions -l <location>`
	
	例如：
	
	`az aks get-versions -l eastus`
	
	4. 导航到 `IDM_4.9_Cloud_Deployment_files` 目录，转到 `main.tf` 文件并编辑以下值：
	
	`kubernetes_version = "< 版本 >"`
	
	`orchestrator_version = "< 版本 >"`
	
	例如：
	
	`kubernetes_version = "1.20.15"`
	
	`orchestrator_version = "1.20.15"`
	
	注释：版本 `1.20.x` 已经过认证，在 AKS Kubernetes 上受支持。
	
	5. 重运行以下命令：
	
	`terraform apply --auto-approve`

问题	建议的操作
在 Azure Kubernetes 服务上部署多实例容器时，您可能会发现有几个 Pod 处于等待中状态。	要解决该问题，请执行以下步骤： 1. 登录到 Azure 门户。 2. 在 “ 搜索 ” 中键入 “kubernetes 服务 ”，然后按 Enter。 3. 选择您的 kubernetes 群集。 4. 单击**诊断并解决问题** > **故障排除**。 5. （视情况而定）如果使用查错方法未能解决问题，请检查您的 Azure 帐户的使用配额。 a. 转到 “ 主页 ”，在 “ 搜索 ” 中键入 “ 配额 ”，然后按 Enter。 b. 单击**计算**。 c. （视情况而定）如果 “ 当前使用率 ” 列显示 100% 并带有红线，请单击**请求提高配额**。 d. 在**新限制**文本框中输入新限制。 e. 单击**提交**。
当您重启动引擎实例 Pod 时，现有身份库的驱动程序部署将会失败。Designer 应用程序中可能会出现以下错误： `"cn=Azure AD Driver,cn=Driver Set,o=system"` 部署失败并出现错误和 / 或警告。	转到 Designer 应用程序，并将身份库重新导入 Designer。
当您重启动主服务器时，将为它指派新 IP 地址，此 IP 地址与次要服务器的 SSL 证书中的 IP 地址不匹配。	重启动次要服务器会导致它使用新 IP 地址重新颁发 SSL 证书。

问题	建议的操作
在 Identity Manager Reporting 中，当您尝试导入总大小超过 1MB 的多个报告时，会显示错误 413。发生此错误的原因是 nginx-ingress 控制器允许的默认请求正文大小为 1MB。 调用 URL (/IDMRPT-CORE/rpt/definitions/import?uploadid=<id>&content=text/html&format=application/json&overwrite=true) 时发生错误。服务器返回状态代码 413 及以下不可分析的 JSON 数据：	要解决此问题，可以允许指定更大的请求正文大小，为此，请在入口配置部分下的 values.yaml 文件中添加以下批注： nginx.ingress.kubernetes.io/proxy-body-size: 3m

Identity Manager 引擎查错

下表列出了您可能会遇到的问题，以及为解决这些问题而建议执行的操作。如果问题仍然存在，请联系 NetIQ 代表。

问题	建议执行的操作
在 OES 上安装 Identity Manager 引擎时，控制台以及 /var/opt/netiq/idm/log/ 目录下的 idminstall.log 文件中报告了以下讯息。	请确保 OES 服务器上存在 /etc/OES-brand 文件。如果该文件不存在，请创建一个新文件并再次尝试安装 Identity Manager 引擎。
当 eDirectory 初始化过程正在进行时， Identity Manager 引擎无法启动。如果 eDirectory DIB 极大，则很有可能会出现此问题。	请执行以下步骤来解决此问题： 1. 导航到 /etc/opt/novell/eDirectory/conf/ 目录。 2. 在 env_idm 文件中，添加 SLEEP_BEFORE_ENGINE_STARTUP 环境变量并将该变量的值设置为 0 到 600。该值以秒为单位。 **注释：**如果提供的值无效或大于 600，将使用默认值 600。 3. 重启动 eDirectory。 4. （视情况而定）检查 ndsd.log 以查看讯息和日志。

问题	建议执行的操作
在 Linux 系统上运行 Identity Manager 引擎时，虽然有可用的空间，但仍出现 /tmp 目录磁盘空间不足的错误。您可以使用 df (disk free) 和 du (disk used) 命令来检查此状态。 df 命令指出没有任何可用空间，而 du 命令则指出并未用完分配给 /tmp 的所有空间。之所以出现此问题，是因为每个实例化 Identity Manager 驱动程序都会在内存中装载多个库。 JVM 会将这些驱动程序暂时复制到 /tmp 目录，事后会将其删除。已删除的文件会继续占用内存，直到创建这些文件的 JVM 进程终止为止。您可以使用 lsof 命令来查出此行为。处于此状态的文件标记为已删除。消耗的总磁盘空间取决于服务器上运行的驱动程序数。	消耗的空间是相对静态的。因此，请确保在 /tmp 目录中提供足够的额外空间。如果该问题持续出现，请重启动 eDirectory。
在多服务器环境中显示了一个无法识别的扩展异常。	确保主服务器具有次服务器的读写分区： 1. 登录到 iManager。 2. 单击**角色和任务** > **分区和复本** > **复本视图**。 3. 选择次服务器。 4. 指派对该服务器的读写许可权限。 **注释：**确保已在驱动程序集中添加了次服务器。
通过 dxcmd 执行大规模查询时， dxcmd 会退出并显示 625 ERR_TRANSPORT_FAILURE 错误，而且不会生成任何结果文件。 Identity Manager 引擎使用环境变量 NCPCLIENT_REQ_TIMEOUT 的值作为执行 dxcmd 查询的默认时间。默认情况下， NCP 连接的超时为 115 秒。如果执行查询和返回结果所需的时间超过此值，将会显示错误。	通过将环境变量 NCPCLIENT_REQ_TIMEOUT 的值设置为大于查询所需总时间的秒数来提高超时值。可通过在 dxcmd 脚本 /opt/novell/eDirectory/bin/dxcmd 中添加 export NCPCLIENT_REQ_TIMEOUT=value 来永久设置 dxcmd 的环境变量。也可在执行 dxcmd 之前从执行该脚本的终端中运行 export NCPCLIENT_REQ_TIMEOUT=value 来手动设置变量。
将 Identity Manager 引擎升级到 4.9 时，日志中可能会出现有关 OES 从服务器断开连接的错误。	此问题的原因是未定义参数 ${IDM_KEYSTORE_PWD}。 可以忽略此问题，但如果您想要避免其发生，请在无提示属性或环境中定义参数 ${IDM_KEYSTORE_PWD}。

Identity Applications 和 Identity Reporting 查错

下表列出了您可能会遇到的问题，以及为解决这些问题建议执行的操作。如果问题仍然存在，请联系 NetIQ 代表。

问题	建议执行的操作
如果在“证书主体”和“应用程序配置”中指定的 LDAP 服务器名称不同，则在升级 Identity Manager 后， Identity Applications 将无法连接到身份库。	Java 对 LDAPS 连接启用端点识别，因此，在连接到 Identity Manager 服务器时指定的服务器名称必须与证书中返回的服务器名称相同。如果服务器名称不同，请执行以下步骤： 1. 导航到 `/opt/netiq/idm/apps/configupdate` 目录。 2. 运行以下命令起动配置更新实用程序。 `./configupdate.sh` 3. 导航到 **User Application** 选项卡，单击**身份库服务器**，然后将服务器名称更改为 LDAP 服务器证书主体中指定的名称。 此操作将更新 `ism-configuration.properties` 文件中的 `DirectoryService/realms/jndi/params/AUTHORITY` 属性。 4. 单击**确定**。
如果 Identity Applications 和 Identity Reporting 安装在同一台服务器上，而您使用 `<Reporting 安装文件夹 >/bin` 目录中的配置更新实用程序来更改配置， Identity Manager 仪表板将无法起动。`catalina.out` 日志文件中会报告以下错误： `EboPortalBootServlet [RBPM] +++++WARNING!!!! : This portal application context, IDMProv, does not match the portal.context property set in the PortalService-conf/config.xml file.Only one portal per database is allowed.Data has been loaded using the previous portal context.To correct this you must revert back to the previous portal name of, NoCacheFilter, please consult the documentation.`	要进行任何配置更改，请使用 `/opt/netiq/idm/apps/configupdate/` 目录中的配置更新实用程序。

问题	建议执行的操作
无法使用配置更新实用程序更改某个属性的口令。	您可以执行以下步骤从命令行更改某个属性（例如 com.netiq.rpt.ssl-keystore）的口令： 1. 使用以下实用程序加密您的口令： `/opt/netiq/common/jre/bin/java -jar tomcat/lib/obscurity-0.13.2-uber.jar com.netiq.ism.obfuscate.server.util.PasswordObfuscator << 口令 >>` 2. 导航到 /opt/netiq/idm/apps/tomcat/conf 目录中的 ism-configuration.properties 文件。 3. 修改 ism-configuration.properties 文件，添加在步骤 2 中为 com.netiq.rpt.ssl-keystore.pwd 参数指定的加密口令。 4. 保存该文件并重启动 Tomcat。
如果 Identity Reporting 安装在独立的服务器上，并且您通过仪表板起动 Identity Reporting 或 IDM DCS URL， URL 将无法起动。	起动 Identity Reporting 或 IDM DCS URL 之后，请执行以下步骤： 1. 导航到地址栏。 2. 修改 URL，并手动提供安装了 Identity Reporting 的服务器的主机名和端口细节。 此外，导航到安装了 Identity Applications 的服务器上的 configupdate.sh.properties 文件，并在 sso_apps 参数中添加 rpt 项，然后保存更改。例如 **sso_apps=ua,rpt**
如果 Identity Applications 和 Identity Reporting 安装在同一台服务器上，并针对 OSP 和 Identity Applications 启用了 CEF 审计，则 Reporting 组件将无法起动。	请执行以下步骤来解决此问题： 1. 导航到 /opt/netiq/idm/apps/tomcat/conf 目录中的 idmrptcore_logging.xml 文件。 2. 在 idmrptcore_logging.xml 文件中添加 <keystore file> 参数，并指定密钥存储区文件路径。例如，添加下行： `<keystore-file>/opt/netiq/idm/app/tomcat/conf/idm.jks</keystore-file>` 3. 重启动 Tomcat。
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，请手动重启动 Tomcat。

问题	建议执行的操作
如果现有的 Identity Applications 或 Identity Reporting 配置中未配置端口，而您尝试对 Identity Manager 进行升级，配置更新实用程序中**鉴定**和 **SSO 客户端**选项卡下列出的 IP 地址与端口将显示错误的值。	升级 Identity Applications 和 Identity Reporting 后，请执行以下步骤： 1. 导航到 `/opt/netiq/idm/apps/configupdate` 目录。 2. 运行以下命令： `./configupdate.sh` 3. 在**鉴定**选项卡上的 **OAuth 服务器主机标识符**和 **OAuth 服务器 TCP 端口**字段中，分别指定正确的 IP 地址和端口。 4. 在 **SSO 客户端**选项卡中，确保 IDM Administrator、Reporting 和 IDM 数据收集服务的 URL 格式正确。 5. 重启动 Tomcat。
您要修改安装过程中创建的以下一或多个 User Application 配置设置： ◆ 身份库连接和证书 ◆ 电子邮件设置 ◆ Identity Manager 引擎用户身份和用户组 ◆ Access Manager 或 iChain 设置	在独立于安装程序的情况下运行配置实用程序。 **Linux**：从安装目录 （默认为 `/opt/netiq/idm/apps/configupdate/`）中运行以下命令： `./configupdate.sh`
启动 Tomcat 会导致以下异常： `port 8180 already in use`	关闭 Tomcat （或其他服务器软件）的可能已在运行的任何实例。如果将 Tomcat 重新配置为使用 8180 以外的其他端口，请编辑 User Application 驱动程序的 `config` 设置。
当 Tomcat 启动时，应用程序报告称找不到可信证书。	请务必使用安装 User Application 期间指定的 JDK 来启动 Tomcat。
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 Identity Console 管理员帐户不同。
即使使用管理员帐户也无法创建新用户。	User Application 管理员必须是顶层容器的受托者，并且应有主管权限。您可以尝试将 User Application 管理员的权限设置为等效于 LDAP 管理员的权限 （使用 Identity Console）。

问题	建议执行的操作
启动应用程序服务器时发生密钥存储区错误。	应用程序服务器未使用安装 User Application 期间指定的 JDK。 使用 `keytool` 命令导入证书文件： `keytool -import -trustcacerts -alias aliasName -file certFile -keystore ..\lib\security\cacerts -storepass changeit` • 使用为该证书选择的唯一名称替换 *aliasName*。 • 使用证书文件的完整路径和名称替换 *certFile*。 • 默认的密钥储存区口令为 `changeit` （如果有其他口令，请指定）。
无法发送电子邮件通知。	运行 `configupdate` 实用程序以检查是否提供了以下 User Application 配置参数的值：**Email From** 和 **Email Host**。 **Linux**：从安装目录 （默认为 `/opt/netiq/idm/apps/configupdate/`）中运行以下命令： `./configupdate.sh`
配置更新实用程序中未显示 **IG SSO 客户端**选项卡	在 `configupdate.sh.properties` 文件中的 `sso_apps` 参数内添加 `ig` 项，然后保存更改。如果 `sso_apps` 参数已包含 Identity Applications 和 Identity Reporting 项，请将 Identity Governance 项添加到列表中。例如 **sso_apps=ua,rpt,ig**
部署 Identity Applications 容器时显示以下异常： `错误 [com.novell.afw.portlet.consumer.core.EboPortletProducerChangeListener] (main) [RBPM] portletID 为 "HeaderPortlet" 的 Portlet 注册不存在。 com.novell.afw.portlet.exception.EboPortletRegistrationException: portletID 为"HeaderPortlet"的 Portlet 注册不存在。`	重启动 Identity Applications 容器。

问题	建议执行的操作

部署 Identity Applications 容器后，当您尝试请求与新表单关联的许可权限时，该表单不按预期装载。此问题是随机出现的。	确保已在 nginx.conf 文件中指定表单渲染器服务器和端口细节。要更新 nginx.conf 文件，请执行以下步骤：
	1. 登录到表单渲染器容器。
	`docker exec -it < 容器 > < 命令 >`
	例如：
	`docker exec -it fr-container bash`
	2. 导航到 /opt/netiq/common/nginx/ 目录。
	3. 编辑 nginx.conf 文件。
	4. 指定表单渲染器服务器和端口细节。例如：
	`server {`
	`listen 8600 ssl;`
	`server_name formrenderer.example.com;`

其他问题查错

下面列出了您可能会遇到的问题，以及为解决这些问题而建议执行的操作。如果问题仍然存在，请联系 NetIQ 代表。

问题	建议执行的操作
如果在 Identity Manager 引擎中启用了 FIPS，尝试连接到 Identity Console 时，启用了 FIPS 的身份库 /eDirectory 的口令验证会失败。	导航到 Identity Console 目录并运行以下文件： `./identityconsole_install` 然后进一步按照《*Identity Console Installation Guide*》（Identity Console 安装指南）中 “Performing an Interactive Installation”（执行交互式安装）过程的步骤 5 及后续步骤进行操作。