



Informatica®
10.4.1

安全指南

Informatica 安全指南

10.4.1

2020 年 6 月

© 版权所有 Informatica LLC 2013, 2020

本软件和文档仅根据包含使用与披露限制的单独许可协议提供。未事先征得 Informatica LLC 同意，不得以任何形式、通过任何手段（电子、影印、录制或其他手段）复制或传播本文档的任何部分。

美国政府权利交付给美国政府客户的程序、软件、数据库及相关文档和技术数据是指适用的联邦采购条例和政府机构特定补充条例中定义的"商业计算机软件"或"商业技术数据"。因此，使用、复制、披露、修改和改编应遵循适用的政府合同中规定的限制和许可条款、政府合同条款的适用范围以及 FAR 52.227-19 商用计算机软件许可中规定的额外权利。

Informatica、Informatica 标志、Informatica Cloud、PowerCenter 和 PowerExchange 是 Informatica LLC 在美国和世界其他许多司法管辖区的商标或注册商标。欲获得 Informatica 商标的最新列表，请访问 <https://www.informatica.com/trademarks.html>。其他公司和产品名称可能是其各自所有者的商业名称或商标。

本软件和/或文档中的若干部分受第三方版权约束。所需的第三方声明随产品一起提供。

本文档中的信息如有更改，恕不另行通知。如发现本文档中有什么问题，请通过以下电子邮件地址向我们报告：infa_documentation@informatica.com。

Informatica 产品根据对应协议的条款和条件进行担保。INFORMATICA 按"原样"提供本文档中的信息，无任何明示或暗示的担保，包括但不限于任何适销性和特定用途适用性担保，也没有任何非侵权担保或条件。

发布日期: 2020-08-03

目录

前言	10
Informatica 资源	10
Informatica Network	10
Informatica 知识库	10
Informatica 文档	10
Informatica 产品可用性矩阵	11
Informatica Velocity	11
Informatica Marketplace	11
Informatica 全球客户支持部门	11
 第 1 章： Informatica 安全简介.....	12
Informatica 安全概览	12
基础结构安全	12
身份验证	13
安全域通信	13
安全数据存储	14
操作安全	14
域配置存储库	15
安全域	15
 第 2 章： 用户身份验证.....	16
用户身份验证概览	16
本地用户身份验证	17
LDAP 用户身份验证	17
Kerberos 身份验证	17
Informatica Web 应用程序的 SAML 身份验证	18
 第 3 章： LDAP 身份验证.....	19
概览	19
LDAP 安全域	19
用户帐户同步	20
LDAP 目录服务	20
安全 LDAP 身份验证的 Azure Active Directory	21
创建 LDAP 配置	22
创建 LDAP 配置并配置 LDAP 服务器连接	22
配置安全域	23
配置同步计划	24
在 LDAP 目录服务中使用嵌套组	25
使用自签名 SSL 证书	25
删除 LDAP 配置	26

第 4 章：Kerberos 身份验证.....	27
Kerberos 概览.....	27
Kerberos 在 Informatica 域中的工作原理.....	28
Kerberos 跨域身份验证.....	29
将域从 Kerberos 单个域身份验证转换为 Kerberos 跨域身份验证.....	29
准备启用 Kerberos 身份验证.....	30
确定 Kerberos 服务主体级别.....	30
配置 Kerberos 配置文件.....	31
在 Active Directory 中创建 Kerberos 主体帐户.....	33
生成服务主体名称和 Keytab 文件名格式.....	34
生成 Keytab 文件.....	39
为 Active Directory 中的 Kerberos 主体用户帐户启用委派.....	43
启用 Kerberos 身份验证.....	44
在域中启用 Kerberos 身份验证.....	45
更新域中的节点.....	47
在 Informatica 节点上启用 Kerberos.....	48
将 Keytab 文件复制到 Informatica 节点.....	49
为 Informatica 客户端启用 Kerberos 身份验证.....	50
启用用户帐户以使用 Kerberos 身份验证.....	51
将 Active Directory 中的用户帐户导入到 LDAP 安全域.....	51
将本地用户特权和权限迁移至 Kerberos 安全域.....	53
第 5 章：Informatica Web 应用程序的 SAML 身份验证.....	55
SAML 身份验证概览.....	55
SAML 身份验证流程.....	56
在域中启用 SAML 身份验证.....	56
为标识提供程序或 LDAP 存储创建 LDAP 配置.....	57
导出断言签名证书.....	57
将证书导入到用于 SAML 身份验证的信任库.....	57
配置标识提供程序.....	57
将 Informatica Web 应用程序 URL 添加到标识提供程序.....	58
在域中启用 SAML 身份验证.....	58
在网关节点上启用 SAML 身份验证.....	60
配置 Web 应用程序以使用其他标识提供程序.....	61
准备使用标识提供程序.....	61
配置 Informatica Administrator 以使用一个标识提供程序.....	62
配置 Informatica Web 应用程序.....	63
第 6 章：域安全性.....	65
域安全概览.....	65
域中的安全通信.....	66
服务和 Service Manager 的安全通信.....	66

安全域配置存储库数据库.	71
安全的 PowerCenter 存储库数据库.	73
安全模型存储库数据库.	73
工作流和会话的安全通信.	74
建立与 Web 应用程序服务的安全连接.	75
建立与 Web 应用程序服务的安全连接的要求.	75
启用与 Administrator 工具的安全连接.	75
Informatica Web 应用程序服务.	76
Informatica 域的密码套件.	78
创建密码套件列表.	79
为 Informatica 域配置新的密码套件有效列表.	80
安全源和目标.	81
数据集成服务源和目标.	81
PowerCenter 源和目标.	82
安全数据存储.	82
UNIX 上的安全目录.	82
从命令行更改加密密钥.	83
应用程序服务和端口.	85
 第 7 章： Informatica Administrator 中的安全管理.....	 88
使用 Informatica Administrator 概览.	88
用户安全.	89
加密.	89
身份验证.	90
授权.	90
安全选项卡.	91
使用搜索部分.	91
使用安全导航器.	92
组.	92
用户.	92
角色.	93
操作系统配置文件.	93
LDAP 配置.	93
帐户管理.	94
审计报告.	94
密码管理.	94
更改密码.	95
域安全性管理.	95
用户安全管理.	95
 第 8 章： 用户和组.....	 97
用户和组概览.	97
默认组.	98

管理员组.	98
“任何人”组.	98
操作员组.	98
了解用户帐户.	98
默认管理员.	99
域管理员.	99
应用程序客户端管理员.	99
用户.	100
管理用户.	100
创建本地用户.	100
编辑本地用户的常规属性.	101
向本地组分配本地用户.	101
向本地组分配 LDAP 用户.	102
启用和禁用用户帐户.	102
删除本地用户.	102
LDAP 用户.	103
解锁用户帐户.	103
为大量用户增加系统内存.	103
查看用户活动.	104
管理组.	107
添加本地组.	108
编辑本地组的属性.	108
将一个本地组移动到另一个本地组.	109
删除本地组.	109
LDAP 组.	109
管理操作系统配置文件.	109
PowerCenter 集成服务的操作系统配置文件属性.	109
数据集成服务的操作系统配置文件属性.	111
元数据访问服务的操作系统配置文件属性.	112
创建操作系统配置文件.	113
编辑操作系统配置文件.	114
向用户或组分配默认操作系统配置文件.	114
删除操作系统配置文件.	115
在安全域中使用操作系统配置文件.	115
在使用 Kerberos 身份验证的域中使用操作系统配置文件.	115
帐户锁定.	116
配置帐户锁定.	116
帐户锁定的规则和准则.	117
 第 9 章：特权和角色.	 118
特权.	118
特权组.	119
角色.	119

域特权.	120
安全管理特权组.	120
域管理特权组.	121
监视特权组.	125
工具特权组.	126
云管理特权组.	127
分析服务特权.	127
内容管理服务特权.	128
数据集成服务特权.	128
Mass Ingestion 服务特权.	129
Metadata Manager 服务特权.	129
目录特权组.	129
加载特权组.	131
模型特权组.	131
安全特权组.	131
模型存储库服务特权.	132
PowerCenter 存储库服务特权.	133
工具特权组.	134
文件夹特权组.	134
设计对象特权组.	136
源和目标特权组.	138
运行时对象特权组.	139
全局对象特权组.	143
PowerExchange 侦听器服务特权.	145
PowerExchange 日志记录器服务特权.	146
计划程序服务特权.	147
Test Data Manager 服务特权.	147
管理特权组.	148
连接特权组.	149
数据域特权组.	150
数据屏蔽特权组.	150
数据子集特权组.	151
策略特权组.	152
项目特权组.	152
规则特权组.	155
数据生成特权组.	156
管理角色.	156
系统定义的角色.	157
自定义角色.	158
将特权和角色分配给用户和组.	160
继承特权.	160
通过导航将特权和角色分配给用户或组.	160

查看对服务有特权的用户.	161
特权和角色故障排除.	161
第 10 章：权限.	164
权限概览.	164
权限类型.	165
权限搜索筛选器.	166
域对象权限.	166
域对象的权限.	167
用户或组的权限.	168
操作系统配置文件权限.	169
连接权限.	170
连接权限的类型.	171
默认连接权限.	171
分配对连接的权限.	171
查看连接的权限详细信息.	171
编辑对连接的权限.	172
群集配置权限.	172
应用程序和应用程序对象权限.	173
应用程序和应用程序对象权限的类型.	173
分配对应用程序或应用程序对象的权限.	173
查看对应用程序或应用程序对象的权限详细信息.	173
编辑对应用程序或应用程序对象的权限.	174
拒绝对应用程序或应用程序对象的权限.	174
SQL 数据服务权限.	174
SQL 数据服务权限类型.	175
分配对 SQL 数据服务的权限.	175
查看对 SQL 数据服务的权限详细信息.	175
编辑对 SQL 数据服务的权限.	176
拒绝对 SQL 数据服务的权限.	176
列级别安全.	177
Web 服务权限.	178
Web 服务权限的类型.	178
分配对 Web 服务的权限.	179
查看 Web 服务的权限详细信息.	179
编辑对 Web 服务的权限.	180
第 11 章：审计报告.	181
审计报告概览.	181
用户个人信息.	182
用户组关联.	182
特权.	183
角色关联.	184

域对象权限.	184
选择审计报表的用户.	184
选择审计报告的组.	185
选择审计报告的角色.	186

附录 A：命令行特权和权限..... 187

infacmd as 命令.	187
infacmd 群集命令.	188
infacmd dis 命令.	189
infacmd dp 命令.	190
infacmd es 命令.	190
infacmd ipc 命令.	191
infacmd isp 命令.	191
infacmd mas 命令.	199
infacmd mi 命令.	199
infacmd mrs 命令.	199
infacmd ms 命令.	201
infacmd tools 命令.	202
infacmd ps 命令.	202
infacmd pwx 命令.	203
infacmd rms 命令.	204
infacmd rtm 命令.	204
infacmd sch 命令.	205
infacmd sql 命令.	205
infacmd wfs 命令.	206
pmcmd 命令.	206
pmrep 命令.	209

附录 B：自定义角色..... 214

分析服务自定义角色.	214
Metadata Manager 服务自定义角色.	215
操作员自定义角色.	216
PowerCenter 存储库服务自定义角色.	217
Test Data Manager 自定义角色.	218

索引..... 223

前言

使用《Informatica 安全指南》了解如何在 Informatica 域中启用安全。了解如何配置和管理各种身份验证协议，包括轻量级目录访问协议、Kerberos 和安全断言标记语言。了解如何管理用户和组，以及如何使用权限、特权和角色管理用户安全。

Informatica 资源

Informatica 通过 Informatica Network 和其他在线门户为您提供一系列产品资源。使用这些资源，可以充分利用 Informatica 产品和解决方案，并向其他 Informatica 用户和主题专家学习。

Informatica Network

在 Informatica Network 中可以获得许多资源，包括 Informatica 知识库和 Informatica 全球客户支持。要进入 Informatica Network，请访问 <https://network.informatica.com>。

作为 Informatica Network 成员，您可以选择以下服务：

- 在知识库中搜索产品资源。
- 查看产品可用性信息。
- 创建并检查您的支持案例。
- 查找当地的 Informatica 用户组网络并与您的伙伴进行协作。

Informatica 知识库

使用 Informatica 知识库可查找产品资源，例如操作方法文章、最佳实践、视频教程以及常见问题的答案。

要搜索知识库，请访问 <https://search.informatica.com>。如果您对知识库有任何疑问、意见或建议，请与 Informatica 知识库团队联系，电子邮件地址为 KB_Feedback@informatica.com。

Informatica 文档

使用 Informatica 文档门户可浏览大量当前与最近产品版本的文档库。要浏览文档门户，请访问 <https://docs.informatica.com>。

如果您对产品文档有任何疑问、意见或建议，请与 Informatica 文档团队联系，电子邮件地址为 infa_documentation@informatica.com。

Informatica 产品可用性矩阵

产品可用性矩阵 (PAM) 指明了产品版本支持的操作系统版本、数据库以及数据源和目标的类型。您可以在以下网址中浏览 Informatica PAM:

<https://network.informatica.com/community/informatica-network/product-availability-matrices>。

Informatica Velocity

Informatica Velocity 是由 Informatica 专业服务根据数百个数据管理项目的实际经验所开发出来的，其中汇集了大量使用技巧和最佳实践。Informatica Velocity 代表了 Informatica 顾问的集体知识，这些顾问与世界各地的组织合作，共同计划、开发、部署和维护成功的数据管理解决方案。

您可以在以下网址中找到 Informatica Velocity 资源：<http://velocity.informatica.com>。如果您对 Informatica Velocity 有任何疑问、意见或建议，请通过 ips@informatica.com 与 Informatica 专业服务联系。

Informatica Marketplace

Informatica Marketplace 是一个论坛，该论坛中提供的解决方案可扩展和增强您的 Informatica 实施。利用 Informatica 开发人员和合作伙伴在 Marketplace 中提供的数以百计的解决方案，可提高您的工作效率并加快项目实施时间。您可以在以下网址中找到 Informatica Marketplace：<https://marketplace.informatica.com>。

Informatica 全球客户支持部门

您可以通过电话或 Informatica Network 与全球支持中心联系。

要查找您当地的 Informatica 全球客户支持部门电话号码，请访问 Informatica 网站，链接为：<https://www.informatica.com/services-and-training/customer-success-services/contact-us.html>。

要在 Informatica Network 上查找在线支持资源，请访问 <https://network.informatica.com>，然后选择 eSupport 选项。

第 1 章

Informatica 安全简介

本章包括以下主题：

- [Informatica 安全概览, 12](#)
- [基础结构安全, 12](#)
- [操作安全, 14](#)
- [域配置存储库, 15](#)
- [安全域, 15](#)

Informatica 安全概览

您可以保护 Informatica 域，使其免受来自运行该域的网络内部和外部的威胁。

Informatica 域的安全性包括以下安全类型：

基础结构安全

基础结构安全保护 Informatica 域不受对 Informatica 域中服务和资源的未经授权的访问或修改。基础结构安全包括以下几个方面：

- 保护在 Informatica 域中传输和存储的数据
- 对连接到 Informatica 域的用户和服务进行身份验证
- 确保外部组件连接（包括客户端应用程序以及存储库、源和目标的关系数据库）的安全。

操作安全

操作安全控制对 Informatica 域中的数据和服务的访问。操作安全包括以下几个方面：

- 根据用户在组织中的角色设置对数据和元数据的用户访问限制
- 根据用户在组织中的角色设置用户在 Informatica 域中执行操作的能力限制

Informatica 存储域配置信息和有权在域配置存储库中访问域的用户列表。域配置存储库还包含组、角色、特权和分配给 Informatica 域中的每个用户的权限。

Informatica 将按安全域组织用户列表。安全域包含用户帐户的集合。一个域可以有多个安全域。

基础结构安全

基础架构安全包括用户和服务身份验证、域内的安全通信以及安全的数据存储。

身份验证

服务管理器会对域中运行的服务及登录到 Informatica 客户端工具的用户进行身份验证。

您可以将 Informatica 域配置为使用以下类型的身份验证：

本地身份验证

本地身份验证是一种仅适用于 Informatica 域中用户帐户的身份验证模式。Informatica 域使用本地身份验证时，服务管理器会在域配置存储库中存储用户凭据和特权，并在 Informatica 域中执行所有用户身份验证。

如果 Informatica 域使用本地身份验证，默认情况下，此域具有一个本地安全域，且所有用户帐户都属于本地安全域。

Informatica 使用用户名和密码对 Informatica 域中的用户和服务进行身份验证。

轻量级目录访问协议 (LDAP) 身份验证

LDAP 是一种用于访问网络上的用户和资源的软件协议。如果 Informatica 域使用 LDAP 身份验证，则用户帐户和凭据将存储在 LDAP 目录服务中。用户特权和权限将存储在域配置存储库中。您必须定期将域配置存储库中的用户帐户与 LDAP 目录服务中的用户帐户同步。

Informatica 使用用户名和密码对 Informatica 域中的 Informatica 用户和服务进行身份验证。

Kerberos 身份验证

Kerberos 是一种网络身份验证协议，它使用票证对网络中的用户和服务进行身份验证。Informatica 域使用 Kerberos 身份验证时，用户帐户和凭据将存储在可以是 LDAP 目录服务的 Kerberos 主体数据库中。用户特权和权限将存储在域配置存储库中。您必须定期将域配置存储库中的用户帐户与 Kerberos 主体数据库中的用户帐户同步。

Informatica 使用 Kerberos 票证对 Informatica 域中的 Informatica 用户和服务进行身份验证。

基于 SAML 的单点登录

安全断言标记语言 (Security Assertion Markup Language, SAML) 是一种基于 XML 的数据格式，用于在服务提供程序和标识提供程序之间交换身份验证和授权信息。可为 Administrator 工具、Analyst 工具和 Monitoring 工具 Web 应用程序配置基于 SAML 的单点登录。

在 Informatica 域中，Informatica Web 应用程序是服务提供程序，Microsoft Active Directory 联合身份验证服务 (AD FS) 是标识提供程序。Informatica Web 应用程序用户的帐户和凭据存储在 Microsoft Active Directory 中。可以将帐户从 Active Directory 导入到 Informatica 域中的安全域。必须定期将安全域中的用户帐户与 Active Directory 目录服务中的用户帐户同步。

请注意，不能在配置为使用 Kerberos 身份验证的 Informatica 域中启用基于 SAML 的单点登录。

安全域通信

Informatica 域包含各种选项以保护在域和客户端应用程序中的服务管理器和服务之间传输的数据和元数据。Informatica 使用 TCP/IP 和 HTTP 协议在域中的组件之间进行通信，并使用 SSL 证书来保护域中服务与服务管理器之间的通信。

SSL/TLS 协议使用公钥加密法对网络流量进行加密和解密。用于对流量进行加密和解密的公钥存储在 SSL 证书中，该证书可以是自签名证书，也可以是签名证书。自签名证书由证书的创建者签名。由于签名方的身份未经经验证，因此自签名证书的安全性低于签名证书。签名证书是一种 SSL 证书，其请求者身份已由证书颁发机构 (CA) 进行验证。Informatica 建议使用 CA 签名证书来提高安全性。

密钥库包含私钥和证书，用于提供凭据。信任库包含信任的 SSL/TLS 服务器的证书，用于验证凭据。

要确保域中连接的安全，Informatica 需要使用 PEM 和 JKS 格式的密钥库和信任库。您可以使用以下程序创建所需文件：

keytool

可以使用 Java keytool 密钥和证书管理实用程序创建 SSL 证书或证书签名请求 (CSR) 以及 JKS 格式的密钥库和信任库。

keytool 实用程序位于域节点的以下目录中：

<Informatica installation directory>\java\bin

如果域节点在 AIX 上运行，则可以使用随 IBM JDK 一起提供的 keytool 创建一个 SSL 证书或证书签名请求 (CSR) 以及密钥库和信任库。

OpenSSL

您可以使用 OpenSSL 创建 SSL 证书或 CSR，以及将 JKS 格式的密钥库转换为 PEM 格式。

有关 OpenSSL 的详细信息，请参阅以下网站的文档：

<https://www.openssl.org/docs/>

要保护的连接的类型决定了所需的文件。

安全数据存储

在将数据存储在域配置存储库中之前，Informatica 会对敏感数据进行加密，如密码和安全连接参数。Informatica 还会将敏感文件（如配置文件）保存在一个安全目录中。

操作安全

可以为用户或用户组分配特权、角色和权限，以管理用户和组所拥有的访问级别以及用户和组可在域中执行的操作的范围。

可以使用以下方法来管理用户和组在域中的访问权限：

特权

特权决定了用户可以在 Informatica 客户端工具中执行的操作。可以为用户分配一组特权以限制对域中可用服务的访问权限。还可以为组分配特权以允许组中的所有用户拥有服务的相同访问权限。

角色

角色是指可以分配给用户或组的一组特权。可以使用角色来更轻松地管理对用户的特权分配。可以创建具有有限特权的角色，并将该角色分配给限制访问域服务的用户和组。或者，可以创建具有相关特权的角色，以分配给需要相同访问级别的用户和组。

权限

权限定义了用户对对象的访问级别。拥有执行特定操作特权的用户可能需要在特定对象上执行操作的权限。例如，要管理应用程序服务，用户必须拥有管理服务的特权以及特定应用程序服务的权限。

默认管理员组

Informatica 域拥有系统定义的管理员组，该组包含服务的所有特权和权限。您添加到管理员组的任何用户帐户都拥有域中所有服务和对象的特权和权限。安装 Informatica 服务时，安装程序会创建一个属于管理员组的用户帐户。您可以使用默认的管理员帐户首次登录到 Administrator 工具。

域配置存储库

域配置存储库中包含有关域配置以及用户特权和权限的信息。

如果 Informatica 域使用本地用户身份验证，域配置存储库还将包含用户凭据。如果该域使用 LDAP 或 Kerberos 身份验证，域配置存储库将不包含用户凭据。所有 LDAP 和 Kerberos 用户凭据都存储在 Informatica 域外部的 LDAP 目录服务或 Kerberos 主体数据库中。

当您在安装过程中创建 Informatica 域时，安装程序会在关系数据库中创建域配置存储库。必须指定要在其中创建域配置存储库的数据库。可以在通过 SSL 协议进行安全保护的数据库中创建存储库。

安全域

安全域是 Informatica 域中用户帐户和组的集合。

Informatica 域可以有以下类型的安全域：

本地安全域

本地安全域包含在 Administrator 工具中创建和管理的用户和组。Informatica 将本地安全域中用户帐户的所有凭据存储在域配置存储库中。默认情况下，在安装过程中创建本地安全域。安装完成后，无法创建其他本地安全域或删除该本地安全域。

如果 Informatica 域使用 Kerberos 身份验证，该域将不使用本地安全域。

LDAP 安全域

LDAP 安全域包含从 LDAP 目录服务导入的用户和组。如果 Informatica 域使用 LDAP 或 Kerberos 身份验证，您可以创建 LDAP 安全域并添加从 LDAP 目录服务导入的用户和组。

安装 Informatica 服务并创建使用本地或 LDAP 身份验证的域时，安装程序将创建本地安全域，但不创建 LDAP 安全域。您可以在安装完成后创建 LDAP 安全域。

安装 Informatica 服务并创建使用 Kerberos 身份验证的域时，安装程序将创建以下 LDAP 安全域：

- 内部安全域。安装程序创建名为 *_infalInternalNamespace* 的 LDAP 安全域。*_infalInternalNamespace* 安全域包含在安装过程中创建的默认管理员用户帐户。安装完成后，您无法将用户添加到 *_infalInternalNamespace* 安全域或删除该安全域。
- 用户域安全域。安装程序创建空的 LDAP 安全域，并且使用与在安装过程中指定的 Kerberos 用户域相同的名称进行命名。安装完成后，可以将用户从 Kerberos 主体数据库导入到用户域安全域。不能删除用户域安全域。
在使用 Kerberos 身份验证的域中运行命令行程序时，安全域选项默认为安装过程中创建的用户域安全域。

使用相同的方法创建和管理 LDAP 安全域，不管 Informatica 域使用 LDAP 身份验证还是 Kerberos 身份验证。

第 2 章

用户身份验证

本章包括以下主题：

- [用户身份验证概览, 16](#)
- [本地用户身份验证, 17](#)
- [LDAP 用户身份验证, 17](#)
- [Kerberos 身份验证, 17](#)
- [Informatica Web 应用程序的 SAML 身份验证, 18](#)

用户身份验证概览

Informatica 域中的用户身份验证取决于安装 Informatica 服务时配置的身份验证类型。

Informatica 域可以使用以下类型的身份验证对 Informatica 域中的用户进行身份验证：

- 本地用户身份验证
- LDAP 用户身份验证
- Kerberos 网络身份验证
- 基于安全断言标记语言 (SAML) 的单点登录

本地用户帐户存储在 Informatica 域中，并且只能在 Informatica 域中使用。

LDAP 和 Kerberos 用户帐户存储在 LDAP 目录服务中，由企业内部的应用程序共享。

基于 SAML 的单点登录根据存储在 Microsoft Active Directory 中的帐户凭据对用户进行身份验证。可以从 Active Directory 将帐户导入到 Informatica 域中的安全域。

可以在安装过程中选择要在 Informatica 域中使用的身份验证类型。如果在安装过程中启用 Kerberos 身份验证，则必须将 Informatica 域配置为使用 Kerberos 密钥分发中心 (KDC)。必须在 Kerberos 主体数据库中创建 Informatica 域所需的服务主体名称 (SPN)。Kerberos 主体数据库可以是 LDAP 目录服务。此外，还必须为 SPN 创建 keytab 文件，并将其存储在 Informatica 域所要求的 Informatica 目录中。

如果在安装过程中不启用 Kerberos 身份验证，安装程序会将 Informatica 域配置为使用本地身份验证。安装完成后，可以设置 LDAP 服务器连接，并将 Informatica 域配置为使用本地身份验证和 LDAP 身份验证。

可以在 Informatica 域中同时使用本地身份验证和 LDAP 身份验证。服务管理器基于安全域对用户进行身份验证。如果用户属于本地安全域，服务管理器将在域配置存储库中对该用户进行身份验证。如果用户属于 LDAP 安全域，服务管理器会将用户名和密码传递到 LDAP 服务器进行身份验证。

不能同时使用本地身份验证和 Kerberos 身份验证。如果 Informatica 域使用 Kerberos 身份验证，所有用户帐户都必须位于 LDAP 安全域中。用户登录到网络时，Kerberos 服务器会对用户帐户进行身份验证。Informatica 客户端应用程序使用网络登录凭据对 Informatica 域中的用户进行身份验证。仍然支持本地组和角色。

可以在安装期间为 Informatica Web 应用程序启用基于 SAML 的单点登录，也可以在安装之后启用。但是，必须先完成所有必需的设置任务，然后才能启用基于 SAML 的单点登录。不能在配置为使用 Kerberos 身份验证的 Informatica 域中启用基于 SAML 的单点登录。

本地用户身份验证

如果 Informatica 域使用本地身份验证，服务管理器在 Informatica 域中存储所有用户帐户信息并执行所有用户身份验证。当用户登录时，服务管理器使用本地安全域来对用户名和密码进行身份验证。

如果不将 Informatica 域配置为使用 Kerberos 网络身份验证，默认情况下，Informatica 域包含本地安全域。本地安全域在安装时创建且无法删除。一个 Informatica 域只有一个本地安全域。您可以在 Administrator 工具中创建或维护本地安全域中的用户帐户。服务管理器在域配置存储库中存储有关用户帐户的详细信息（包括用户凭据和特权）。

LDAP 用户身份验证

您可以配置 Informatica 域，以允许 LDAP 目录服务中的用户登录到 Informatica 客户端应用程序。可以为域创建多个 LDAP 配置，每个配置连接到不同的 LDAP 服务器。除本地用户身份验证外，域还可以使用 LDAP 用户身份验证。

要使 Informatica 域可以使用 LDAP 用户身份验证，则必须设置到 LDAP 服务器的连接，并通过可以访问 Informatica 域的 LDAP 目录服务指定用户和组。可以使用 Administrator 工具来设置到 LDAP 服务器的连接。

如果将 LDAP 安全域与 LDAP 目录服务同步，服务管理器将可以访问 Informatica 域的 LDAP 用户帐户列表导入到 LDAP 安全域。将特权和权限分配到 LDAP 安全域中的用户时，服务管理器在域配置存储库中存储该信息。服务管理器不在域配置存储库中存储用户凭据。

当用户登录时，服务管理器会将用户名和密码传递给 LDAP 服务器进行身份验证。

注意：服务管理器要求 LDAP 用户使用密码登录到客户端应用程序，即使 LDAP 目录服务可能允许在匿名登录模式下使用空白密码也是如此。

Kerberos 身份验证

您可以将 Informatica 域配置为使用 Kerberos 网络身份验证，以对网络中的用户和服务进行身份验证。

Kerberos 是一种网络身份验证协议，它使用票证对网络中服务和节点的访问进行身份验证。Kerberos 使用密钥分发中心 (KDC) 来验证用户和服务的身份，并向经过身份验证的用户帐户和服务帐户授予票证。在 Kerberos 协议中，用户和服务称为主体。KDC 具有一个数据库，其中包含主体以及用作身份证明的关联密钥。Kerberos 可以使用 LDAP 目录服务作为主体数据库。

要使用 Kerberos 身份验证，必须在使用 Kerberos 网络身份验证的网络上安装并运行 Informatica 域。Informatica 可以在使用 Kerberos 身份验证并将 Microsoft Active Directory 服务作为主体数据库的网络上运行。

可以将 Informatica 域配置为使用 Kerberos 跨域身份验证。通过 Kerberos 跨域身份验证，一个 Kerberos 域中的 Informatica 客户端可以在另一个 Kerberos 域中的节点和应用程序服务上完成身份验证。

Informatica 域需要 keytab 文件对域中的节点和服务进行身份验证，而无需通过网络传送密码。Keytab 文件包含服务主体名称 (SPN) 和关联的加密密钥。在 Informatica 域中创建节点和服务之前，请创建 keytab 文件。

Informatica Web 应用程序的 SAML 身份验证

可以对 Informatica 域进行配置，使其允许用户使用安全断言标记语言 (SAML) 身份验证登录到 Administrator 工具、Analyst 工具、Mass Ingestion 工具、Metadata Manager 和 Monitoring 工具 Web 应用程序。

安全断言标记语言是一种基于 XML 的数据格式，用于在服务提供程序和标识提供程序之间交换身份验证和授权信息。在 Informatica 域中，Informatica Web 应用程序是服务提供程序。Microsoft Active Directory 联合身份验证服务 (AD FS) 是标识提供程序，它将使用组织的 Active Directory 标识存储对 Web 应用程序用户进行身份验证。

要使 Informatica 域能够使用基于 SAML 的单点登录，您必须为 Informatica Web 应用程序用户帐户创建一个 LDAP 安全域，然后将 Active Directory 中的用户导入到该域。可以使用 Administrator 工具设置与 Active Directory 服务器的连接，然后将用户导入到安全域。

当用户登录到 Informatica Web 应用程序时，应用程序会向 AD FS 发送 SAML 身份验证请求。AD FS 将根据 Active Directory 中的用户帐户信息对用户的凭据进行身份验证，然后将包含有关该用户的安全相关信息的 SAML 断言令牌返回到 Web 应用程序。

请对 AD FS 进行配置，使其颁发用于对 Informatica Web 应用程序用户进行身份验证的 SAML 令牌。还必须从 AD FS 导出标识提供程序断言签名证书，然后将该证书导入到域中每个网关节点上的 Informatica 默认信任库文件。

第 3 章

LDAP 身份验证

本章包括以下主题：

- [概览, 19](#)
- [LDAP 安全域, 19](#)
- [用户帐户同步, 20](#)
- [LDAP 目录服务, 20](#)
- [安全 LDAP 身份验证的 Azure Active Directory, 21](#)
- [创建 LDAP 配置, 22](#)
- [删除 LDAP 配置, 26](#)

概览

您可以配置 Informatica 域，允许从一个或多个 LDAP 目录服务导入的用户登录到 Informatica 节点、服务和应用程序客户端（例如 Informatica Developer 和 Informatica Analyst）。

LDAP 目录服务可存储帐户用户名和密码。使用 LDAP 身份验证，可以将所有 Informatica 用户的凭据合并到一个标识存储中，从而简化帐户凭据的创建和更新任务。

可以在 Informatica 域中同时使用本地身份验证和 LDAP 身份验证。在域中的主网关节点上运行的服务管理器基于用户所属的安全域对用户进行身份验证。如果用户属于默认本地安全域，服务管理器将根据域配置存储库中的帐户信息对该用户进行身份验证。如果用户属于 LDAP 安全域，服务管理器会将用户凭据传递到 LDAP 服务器进行身份验证。

LDAP 安全域

LDAP 安全域包含从 LDAP 目录服务导入的用户和组。您可以在 Informatica 域中定义多个 LDAP 安全域。然后，可以将帐户从 LDAP 目录服务导入到安全域中。

如果将 Informatica 域配置为使用 Kerberos 身份验证，则必须创建 LDAP 安全域。安装 Informatica 服务并启用 Kerberos 身份验证后，Informatica 安装程序会使用安装期间指定的 Kerberos 域的名称创建 LDAP 安全域。

创建 LDAP 安全域时，可以配置搜索基础和筛选器以定义要包含在安全域中的 LDAP 用户帐户和组的集合。服务管理器使用安全域配置来导入安全域中的用户和组，或将这些用户和组与 LDAP 目录服务中的用户和组同步。

服务管理器在导入或同步 LDAP 安全域中的用户和组时使用以下条件：

- 服务管理器使用用户搜索基础和筛选器来导入用户帐户。
- 服务管理器使用组搜索基础和筛选器来导入组。
- 服务管理器导入组筛选器中包含的组以及用户筛选器中包含的用户帐户。

用户帐户同步

服务管理器按计划使用 LDAP 目录服务中的用户和组更新安全域。配置 LDAP 身份验证时，可以设置同步计划。

在同步期间，服务管理器执行以下步骤：

- 基于为安全域配置的搜索基础和筛选器，从 LDAP 目录服务中检索用户和组的更新列表。
- 更新安全域中 LDAP 用户和组的列表。如果已在 LDAP 目录服务中删除安全域中的 LDAP 用户，服务管理器会将该用户对象的所有权转移到域管理员帐户。

LDAP 目录服务

可以将用户帐户从 LDAP 目录服务导入 Informatica 安全域。

可以从以下 LDAP 目录服务导入用户：

- IBM Tivoli Directory Server
- Microsoft Active Directory
- Microsoft Azure Active Directory
- Novell eDirectory
- OpenLDAP
- Oracle Directory Server (ODSEE)
- Oracle Unified Directory (OUD)
- Sun Java System Directory Server

注意：如果使用 Kerberos 身份验证，则只能从 Microsoft Active Directory 中导入用户。

服务管理器需要特定唯一 ID (UID) 标识各个 LDAP 目录服务中的用户。下表列出了各个 LDAP 目录服务的默认 UID：

LDAP 目录服务	UID
IBM Tivoli Directory Server	uid
Microsoft Active Directory	sAMAccountName
Microsoft Azure Active Directory	UserPrincipalName
Novell eDirectory	uid

LDAP 目录服务	UID
OpenLDAP	uid
Oracle Directory Server (ODSEE)	uid
Oracle Unified Directory (OUD)	uid
Sun Java System Directory Server	uid

安全 LDAP 身份验证的 Azure Active Directory

您可以将用户从 Azure Active Directory (Azure AD) 导入到 LDAP 安全域中。

Azure Active Directory 域服务提供安全 LDAP 公共 IP 地址，用于将用户帐户从 Azure Active Directory 导入到 LDAP 安全域中。导入的用户可以使用其 LDAP 凭据登录到在 Azure Active Directory 托管域的虚拟机上运行的 Informatica 节点、服务和应用程序。

您必须在 Azure Active Directory 域服务中启用安全轻量级目录访问协议（安全 LDAP）身份验证，才能对 Informatica 用户进行身份验证。

完成以下步骤，准备将用户帐户从 Azure Active Directory 导入到 Informatica 域中：

1. 验证是否可通过防火墙访问端口 636（Azure Active Directory 安全 LDAP 端口）。
2. 在 Azure Active Directory 域服务中启用安全 LDAP 身份验证。

使用 Azure 门户在 Azure Active Directory 域服务中启用安全 LDAP。有关在 Azure Active Directory 域服务中配置安全 LDAP 的信息，请参阅以下链接：

<https://docs.microsoft.com/en-us/azure/active-directory-domain-services/active-directory-ds-admin-guide-configure-secure-ldap>

3. 在 Azure Active Directory 域服务中配置安全 LDAP 证书时，请确保证书上的主题名称为 Azure Active Directory 的完全限定域名(FQDN)。
4. 将安全 LDAP 证书从 PFX 格式转换为 PEM 格式。Java 要求证书采用 PEM 格式。
5. 将所有域节点使用的证书导入到域中单个网关节点的以下目录中的 Java cacerts 信任存储文件中：
<Informatica 安装目录>/java/jre/lib/security/
6. 将包含导入证书的 cacerts 文件复制到域中每个其他网关节点上的相同目录。
7. 将 Azure Active Directory 公共 IP 地址和 Azure Active Directory 的完全限定域名(FQDN)添加到域中每个网关节点的 /etc/hosts 文件中。使用以下格式：
<Azure Active Directory 主机 IP 地址> ldaps.<Azure Active Directory 的 FQDN>

创建 LDAP 配置

可以创建一个或多个 LDAP 配置以允许从 LDAP 目录服务导入的用户帐户和用户组使用 Informatica 域进行身份验证。

可在 LDAP 目录服务中创建和管理 LDAP 用户和组。设置与 LDAP 目录服务器的连接，并使用搜索筛选器指定要有权访问 Informatica 域的用户和组。随后将用户帐户导入 LDAP 安全域。如果 LDAP 服务器使用 SSL 协议，还必须指定 SSL 证书的位置。

将用户导入 LDAP 安全域后，可以为用户分配角色、特权和权限。可以将 LDAP 用户帐户分配到本地组，以基于这些帐户在 Informatica 域中的角色来组织这些帐户。

无法使用 Administrator 工具创建、编辑或删除 LDAP 安全域中的用户和组。必须对 LDAP 目录服务中的 LDAP 用户和组进行更改，然后将 LDAP 安全域与 LDAP 目录服务同步。

使用“LDAP 配置”对话框设置与 LDAP 目录服务的连接，并创建要向其中导入用户帐户的 LDAP 安全域。还可以使用“LDAP 配置”对话框设置同步计划。

要创建 LDAP 配置，请执行以下步骤：

1. 配置与 LDAP 服务器的连接，该服务器包含要用来导入用户帐户和组的目录服务。
2. 为要从 LDAP 目录服务导入的每个用户帐户和组的集合创建 LDAP 安全域。
3. 为服务管理器设置计划，以便使用 LDAP 目录服务中新的或已更改的用户和组更新所有 LDAP 安全域。

创建 LDAP 配置并配置 LDAP 服务器连接

创建 LDAP 配置并配置指向包含要从中导入用户帐户的目录服务的 LDAP 服务器的连接。

配置与 LDAP 服务器的连接时，应指出，如果服务管理器将用户分配给 Informatica 域中的组，则服务管理器必须忽略 LDAP 用户帐户的识别名属性的大小写。如果服务管理器不忽略大小写，可能无法分配属于某个组的所有用户。

如果 LDAP 服务器使用 SSL，则必须将每个域节点使用的证书导入到网关节点域上的 cacerts 信任库文件中。然后，将包含导入证书的 cacerts 文件复制到域中每个节点上的相同目录。有关详细信息，请参阅[“使用自签名 SSL 证书”](#) 页面上 25。

要设置与 LDAP 目录服务的连接，请执行以下任务：

1. 在 Administrator 工具中，单击**安全**选项卡。
2. 单击 **LDAP 配置**选项卡。
3. 单击**操作**菜单，然后选择**创建 LDAP 配置**。
4. 在**创建 LDAP 配置**对话框中，单击 **LDAP 连接**选项卡。
5. 配置 LDAP 服务器的连接属性。

您可能需要咨询 LDAP 管理员以获取连接到 LDAP 服务器所需的信息。

下表描述了 LDAP 服务器配置属性：

属性	说明
LDAP 配置名称	LDAP 配置名称。
服务器名称	托管 LDAP 目录服务的计算机的主机名或 IP 地址。

属性	说明
端口	LDAP 服务器的侦听端口。该端口号与 LDAP 目录服务通信。通常，LDAP 服务器的端口号为 389。如果 LDAP 服务器使用 SSL，则 LDAP 服务器端口号为 636。最大端口号为 65535。
LDAP 目录服务	LDAP 目录服务的类型。 注意: 如果使用 Kerberos 身份验证，必须选择 Microsoft Active Directory 服务。
名称	主要用户的识别名 (DN)。用户名通常由通用名称 (CN)、组织 (O) 和国家/地区 (C) 组成。主要用户名是能够访问目录的管理用户。指定具有读取 LDAP 目录服务中其他用户条目权限的用户。 要连接到 Azure Active Directory，请指定主体用户的用户主体名称 (UPN)。
密码	主要用户的密码。对于匿名登录则留空。
使用 SSL 证书	指出 LDAP 服务器使用安全套接字层 (SSL) 协议。
信任 LDAP 证书	决定服务管理器是否可以信任 LDAP 服务器的 SSL 证书。如果选中，服务管理器将不验证 SSL 证书即连接到 LDAP 服务器。如果未选中，服务管理器在连接至 LDAP 服务器之前将验证 SSL 证书是否由证书颁发机构签名。
不区分大小写	指出当将用户分配给组时，服务管理器必须忽略识别名属性的大小写。
组成员关系属性	包含用户的组成员关系信息的属性名称。该属性是 LDAP 组对象中的属性，其中包含属于某个组的用户或组的识别名。例如， <i>member</i> 或 <i>memberof</i> 。
最大大小	导入安全域的用户帐户数量上限。例如，如果该值设置为 100，则可以将最多 100 个用户帐户导入到安全域中。 如果要导入的用户数超出该属性的值，服务管理器将生成一条错误消息，并且不导入任何用户。如果要导入的用户数量很多，请将该属性设置为一个较高的值。默认值为 1000。

6. 单击**测试连接**以验证与 LDAP 服务器的连接是否有效。

7. 单击**确定保存 LDAP 配置**。

配置安全域

为要从 LDAP 目录服务导入的每个用户帐户和组的集合创建 LDAP 安全域。设置搜索基础和筛选器以定义要包含在安全域中的用户帐户和组的集合。

从 LDAP 目录服务导入的用户和组的名称必须符合本地用户和组的名称规则。如果名称不符合本地用户和组的名称规则，服务管理器将不导入 LDAP 用户或组。请注意，与本地用户名不同，LDAP 用户名可以区分大小写。

服务管理器使用用户搜索基础和筛选器导入用户帐户，使用组搜索基础和筛选器导入组。服务管理器使用筛选器导入组以及属于每个组的用户的列表。

如果修改 LDAP 连接属性以连接到其他 LDAP 服务器，服务管理器不会删除现有安全域。必须确保 LDAP 安全域对于新 LDAP 服务器是正确的。修改安全域中的用户和组筛选器或创建其他安全域，以便服务管理器能够正确导入要在 Informatica 域中使用的用户和组。

要配置 LDAP 安全域，请执行以下步骤：

1. 在 Administrator 工具中，单击**安全**选项卡。
2. 单击**操作**菜单，然后选择 **LDAP 配置**。
3. 在 **LDAP 配置**对话框中，单击**安全域**选项卡。

4. 单击**添加**。

下表介绍了可以为安全域设置的筛选器属性：

属性	说明
安全域	LDAP 安全域的名称。名称不区分大小写，但在域中必须唯一。字符串不能超过 128 个字符，也不能包含以下特殊字符： , + / < > @ ; \ % ? 名称可以包含 ASCII 空格字符，但不能将其用作第一个或最后一个字符。不允许使用所有其他空格字符。
用户搜索基础	条目的识别名 (DN)，该条目用作在 LDAP 目录服务中搜索用户名的起点。搜索可根据对象识别名中的路径在目录中找到对象。 例如，在 Microsoft Active Directory 中，用户对象的识别名可为 cn=UserName,ou=OrganizationalUnit,dc=DomainName，其中 dc=DomainName 所表示的一系列相关识别名标识了对象的 DNS 域。
用户筛选器	用于指定在目录服务中搜索用户的条件的 LDAP 查询字符串。筛选器可以指定属性类型、断言值和匹配条件。 例如：(objectclass=*) 搜索所有对象。(&(objectClass=user)(!(cn=susan))) 搜索除 “susan” 之外的所有用户对象。有关搜索筛选器的详细信息，请参阅 LDAP 目录服务文档。
组搜索基础	条目的识别名 (DN)，该条目用作在 LDAP 目录服务中搜索组名称的起点。
组筛选器	用于指定在目录服务中搜索组的条件的 LDAP 查询字符串。

5. 单击**预览**查看包含在筛选器参数中的用户和组的列表子集。

如果预览不显示正确的用户和组集，请修改用户和组筛选器和搜索基础以获取正确的用户和组。

6. 要立即同步安全域中的用户和组与 LDAP 目录服务中的用户和组，请单击**立即同步**。

服务管理器将 LDAP 安全域中的所有用户与 LDAP 目录服务中的用户同步。完成同步进程所需的时间取决于要导入的用户和组的数量。

7. 单击**确定**保存安全域。

配置同步计划

您可以为服务管理器设置每日计划，以便使用 LDAP 目录服务中新或已更改的用户和组更新 LDAP 安全域。

服务管理器将 LDAP 安全域与 LDAP 目录服务同步时，会将与用户筛选器设置匹配的所有用户从 LDAP 目录服务导入到安全域中。然后，服务管理器导入与组筛选器设置匹配的所有组，并将用户与其对应的组相关联。服务管理器还会从安全域中删除在 LDAP 目录服务中找不到的用户或组。

默认情况下，服务管理器未计划与 LDAP 目录服务同步的时间。为了确保 LDAP 安全域中用户和组的列表准确无误，请计划服务管理器将 LDAP 安全域与 LDAP 目录服务进行同步的时间。服务管理器每天在您设定的时间将 LDAP 安全域与 LDAP 目录服务同步。

要确保同步成功，请在设置同步计划之前考虑以下建议：

验证 /etc/hosts 文件是否包含 LDAP 服务器的条目。

验证域中每个节点网关上的 /etc/hosts 文件是否包含一个具有 LDAP 服务器主机名和 IP 地址的条目。如果服务管理器无法解析 LDAP 服务器的主机名，同步可能会失败。

如果要同步 100 个以上的用户或组，请在 LDAP 中启用分页。

在同步 100 个以上的用户或组之前，在 LDAP 目录服务上启用分页。如果未在 LDAP 目录服务中启用分页，同步可能会失败。

在大多数用户未登录 Informatica 应用程序的时间内同步安全域。

在同步期间，服务管理器将锁定其同步的每个用户帐户。在同步期间，用户可能无法登录到 Informatica 应用程序客户端。在同步开始时登录到应用程序客户端的用户可能无法执行某些任务。

要设置一个将 LDAP 安全域与 LDAP 目录服务进行同步的计划，请执行以下步骤：

1. 在 Administrator 工具中，单击**安全**选项卡。
2. 单击**操作**菜单，然后选择 **LDAP 配置**。
3. 在 **LDAP 配置**对话框中，单击**计划**选项卡。
4. 单击**添加**按钮 (+) 以添加时间。
同步计划使用 24 小时时间格式。
5. 要立即将 LDAP 安全域中的用户和组与 LDAP 目录服务中的用户和组同步，请单击**立即同步**。
6. 单击**确定**保存同步计划。

注意：请等到服务管理器与 LDAP 目录服务同步后再重新启动 Informatica 域，以免错过您在计划中设置的同步时间。

在 LDAP 目录服务中使用嵌套组

LDAP 安全域可以包含嵌套 LDAP 组。服务管理器可以导入通过以下方式创建的嵌套组：

- 在相同的组织单位 (OU) 下创建的组。
- 请在组之间设置关系。

例如，您想创建一个嵌套组，其中 GroupB 是 GroupA 的成员，GroupD 是 GroupC 的成员。

1. 请在相同的 OU 下创建 GroupA、GroupB、GroupC 和 GroupD。
2. 编辑 GroupA，然后将 GroupB 添加为成员。
3. 编辑 GroupC，然后将 GroupD 添加为成员。

不能将嵌套 LDAP 组导入到通过不同的方式创建的 LDAP 安全域中。

使用自签名 SSL 证书

可以连接到使用证书颁发机构 (CA) 签名的 SSL 证书的 LDAP 服务器。默认情况下，服务管理器不连接到使用自签名证书的 LDAP 服务器。

要连接到使用 SSL 证书的 LDAP 服务器，请使用 Java keytool 密钥和证书管理实用程序将所有域节点使用的证书导入域中单个网关节点上的 Java cacerts 信任库文件。然后，将包含导入证书的 cacerts 密钥库文件复制到域中的其他节点上。

cacerts 信任库文件位于每个节点上的以下目录中：

<Informatica 安装目录>\java\jre\lib\security

keytool 实用程序位于每个节点上的以下目录中：

<Informatica 安装目录>\java\bin

导入证书之后，重新启动节点。

删除 LDAP 配置

可以删除 LDAP 配置和相关安全域以永久禁止用户访问域。

删除 LDAP 配置时，必须先删除与 LDAP 配置相关的安全域。Service Manager 将从域配置数据库中删除每个已删除 LDAP 安全域中的所有用户帐户和组。

1. 在 Administrator 工具中，单击**安全**选项卡。
2. 单击 **LDAP 配置**选项卡。
3. 单击**安全域**选项卡，然后单击**编辑**按钮。
4. 在**编辑 LDAP 配置**对话框中选择安全域，然后单击**删除**。
5. 在 LDAP 配置导航器中选择要删除的 LDAP 配置。
6. 单击**操作**菜单，然后选择**删除 LDAP 配置**。
7. 单击**确定**以确认要删除 LDAP 配置。

第 4 章

Kerberos 身份验证

本章包括以下主题：

- [Kerberos 概览, 27](#)
- [Kerberos 在 Informatica 域中的工作原理, 28](#)
- [Kerberos 跨域身份验证, 29](#)
- [准备启用 Kerberos 身份验证, 30](#)
- [启用 Kerberos 身份验证, 44](#)
- [在 Informatica 节点上启用 Kerberos, 48](#)
- [启用用户帐户以使用 Kerberos 身份验证, 51](#)

Kerberos 概览

Kerberos 为计算机网络身份验证协议，可确保 Informatica 客户端、节点和服务通过网络进行通信时彼此间连接的安全性。

Kerberos 身份验证去除了 Informatica 本地帐户，而且无需针对域将用户凭据传递到 LDAP 服务器。当您在某个域中启用 Kerberos 身份验证后，Informatica 客户端将使用在 Windows 身份验证过程中创建的 Kerberos 票证登录到在该域中运行的 Informatica 服务。

您可以在运行于 Windows 网络上的域中启用 Kerberos 身份验证。该网络必须使用 Microsoft Active Directory 域服务 (AD DS) 作为 Kerberos 主体数据库。

要在 Informatica 域中启用 Kerberos 身份验证，请执行以下步骤：

准备启用 Kerberos 身份验证。

在启用 Kerberos 身份验证之前，必须完成多项任务。必须完成的任务如下所述：

- 创建 Kerberos 配置文件。
- 为 Active Directory 中的 Kerberos 主体用户创建帐户。
- 生成服务主体名称 (SPN) 和 keytab 格式。
- 创建用于对网络中的用户和服务进行身份验证的 keytab 文件。

在 Informatica 域中启用 Kerberos 身份验证。

您可以在安装 Informatica 服务时在 Informatica 域中启用 Kerberos 身份验证，也可以在安装完服务后启用 Kerberos 身份验证。如果不在安装过程中启用 Kerberos 身份验证，您可以使用 Informatica 命令程序将域配置为使用 Kerberos 身份验证。

在 Informatica 节点和客户端主机上启用 Kerberos 身份验证。

在域中启用 Kerberos 后，将 Kerberos 配置文件复制到域中的每个节点以及每个 Informatica 客户端主机。还需配置 Web 浏览器以访问 Informatica Web 应用程序。

启用 Informatica 用户以使用 Kerberos 身份验证。

启用 Kerberos 身份验证后，将 Active Directory 中的 Informatica 用户导入到包含 Kerberos 用户帐户的 LDAP 安全域。还必须将本地用户帐户的组、角色、特权和权限迁移到 LDAP 安全域中的用户帐户。

Kerberos 在 Informatica 域中的工作原理

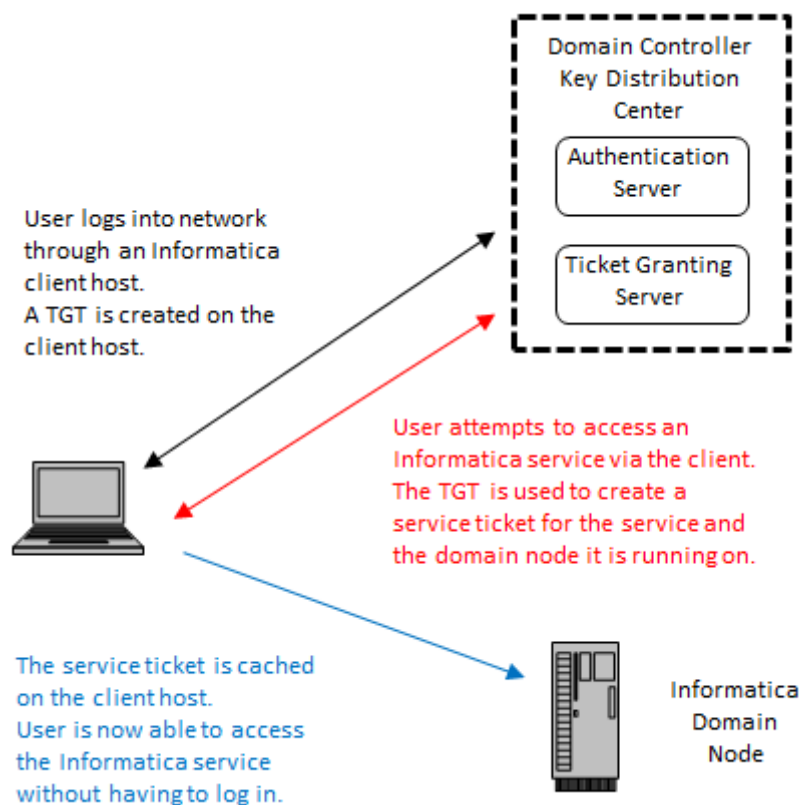
在配置为使用 Kerberos 身份验证的域中，Informatica 客户端借助域内的节点和应用程序服务进行身份验证，无需密码。

在使用 Kerberos 身份验证的域中，在域内运行的服务，包括节点进程、Web 应用程序进程和 Informatica 应用程序服务，都是 Kerberos 主体。在 Kerberos 域使用的 Active Directory 主体数据库中，每个主体都有一个用户帐户。

Kerberos 身份验证协议使用 *keytabs* 借助在域内运行的服务对 Informatica 客户端进行验证。主体的 keytab 储存在运行服务的节点中。keytab 包含在 Kerberos 域内标识服务的 *服务主体名称 (SPN)* 和在 Active Directory 内分配给 SPN 的密钥。

当 KDC 向客户端提供服务票证时，它会使用分配给 SPN 的密钥加密该票证。请求的服务使用该密钥对服务票证进行解密。

下图说明了基本 Kerberos 身份验证流程：



下面概括了基本 Kerberos 身份验证流程：

1. Informatica 客户端用户登录到托管 Informatica 客户端的网络计算机。
2. 登录请求被定向到 *身份验证服务器*，它是 *Kerberos 密钥分发中心 (KDC)* 的一个组件。KDC 是一种在 Active Directory 域内的每个域控制器上运行、有权访问用户帐户信息的网络服务。
3. 验证服务器验证用户是否存在于主体数据库中，然后在用户的计算机上创建名为 *票证授予票证 (TGT)* 的令牌。
4. 用户尝试通过 Informatica 客户端访问 Informatica 域内的进程或服务。
5. Informatica 和 Kerberos 库使用 TGT 从同在 KDC 内运行的 *票证授予服务器* 中请求一个 *服务票证* 和 *会话密钥*。

例如，如果用户从 Informatica Developer 客户端访问模型存储库服务，TGT 则会请求运行所请求服务的节点的服务票证。此外，TGT 还会请求模型存储库服务的服务票证。

6. Kerberos 使用该服务票证借助所请求的服务对客户端进行身份验证。
服务票证缓存在托管 Informatica 客户端的计算机上，因而客户端能够在票证仍有效的情况下使用该票证。
如果用户关闭然后重新启动 Informatica 客户端，客户端将重新使用同一票证来访问 Informatica 域内的进程和服务。

Kerberos 跨域身份验证

可以将 Informatica 域配置为使用 Kerberos 跨域身份验证。通过 Kerberos 跨域身份验证，一个 Kerberos 域中的 Informatica 客户端可以在另一个 Kerberos 域中的节点和应用程序服务上完成身份验证。

当将一个域配置为使用 Kerberos 跨域身份验证时，将每个 Kerberos 域的属性添加至 Kerberos 配置文件中。当运行 infasetup 命令以在域和域节点中启用 Kerberos 身份验证时，还要加上每个域的名称。

域用于进行 Kerberos 跨域身份验证的 Active Directory 服务器必须属于同一个 Active Directory 林。Active Directory 林是使用共同的全局目录、目录架构、逻辑结构和目录配置的一组 Active Directory 域。连接至全局目录以从 Active Directory 服务器将用户导入至 LDAP 安全域中。

要使用 Kerberos 跨域身份验证，林中的 Active Directory 服务器之间必须启用双向信任。

将域从 Kerberos 单个域身份验证转换为 Kerberos 跨域身份验证

您可以将 Informatica 域从使用单个 Kerberos 域身份验证转换为使用 Kerberos 跨域身份验证。

必须先将域升级至版本 10.2 HotFix 2，才能将域转换为使用 Kerberos 跨域身份验证。

您还必须将 Active Directory 全局目录中的用户和组帐户导入 LDAP 安全域中。导入帐户时，将删除 LDAP 安全域中使用 sam 帐户名属性的现有帐户并替换为使用用户主体名称属性的新帐户。

用户使用完全限定的用户主体名称登录 Informatica 客户端，其格式如下：

<用户名>@<KERBEROS 域名>

导入用户和组帐户后，为帐户分配特权、角色和权限。

1. 将域升级到版本 10.2 HotFix 2。
2. 在 Kerberos 配置文件中为每个 Kerberos 域添加必需属性。

在域中的每个节点的 krb5.conf 配置文件中为每个域设置属性。更新域中所有节点上的文件后，重新启动域。

有关为 Kerberos 跨域身份验证配置 krb5.conf 配置文件的更多信息，请参阅 [“配置 Kerberos 配置文件” 页面上 31](#)。

3. 将更新后的 krb5.conf 文件复制到每台托管 Informatica 客户端的计算机的以下目录中：
<Informatica 安装目录>\clients\shared\security
4. 在域节点上运行 infasetup UpdateGatewayNode 和 infasetup UpdateWorkerNode 命令。
将域用于对用户进行身份验证的每个 Kerberos 域的名称指定为 -srn 和 -urn 选项的值，以逗号分隔。
有关运行 infasetup 命令的更多信息，请参阅《Informatica 10.2 HotFix 2 命令引用》中的“infasetup 命令引用”章节。
5. 在域中的一个网关节点上运行 UpdateKerberosConfig 命令。
将域用于对用户进行身份验证的每个 Kerberos 域的名称指定为 -srn 和 -urn 选项的值，以逗号分隔。
6. 在域中的一个网关节点上运行 UpdateKerberosAdminUser 命令。
为域管理员用户帐户指定完全限定的用户主体名称。
7. 将用户和组帐户导入 LDAP 安全域中。
连接至 Active Directory 全局目录。连接至全局目录后，从由每个 Kerberos 域使用的 Active Directory 服务器中导入用户。
有关连接至全局目录和导入帐户的更多信息，请参见[“将 Active Directory 中的用户帐户导入到 LDAP 安全域”页面上 51](#)。
8. 向导入至 LDAP 安全域的用户和组帐户分配特权、角色和权限。
有关分配特权和角色的更多信息，请参阅[第 9 章，“特权和角色”页面上 118](#)。
有关分配权限的更多信息，请参阅[第 10 章，“权限”页面上 164](#)。

准备启用 Kerberos 身份验证

准备在 Informatica 域中启用 Kerberos 身份验证之前，必须先完成多项任务。每项任务所遵循的步骤取决于在哪个服务主体级别启用 Kerberos。

注意：在域中启用 Kerberos 身份验证后，不能将其禁用。此外，还不能在节点级别和进程级别之间切换服务主体级别。

确定 Kerberos 服务主体级别

当您准备启用 Kerberos 身份验证时，必须确定所需的服务主体级别。所需的服务主体级别确定您准备在域中启用 Kerberos 身份验证所必须遵循的程序。

可在下列某个级别启用 Kerberos 身份验证：

节点级别

如果您将域用于测试或开发，而且域不需要较高级别的安全性，则可在节点级别启用 Kerberos。您可以为节点和在节点上运行的所有进程和服务使用单个服务主体名称和单个 keytab 文件。还必须为在节点上运行的 HTTP 进程创建一个 SPN 和一个 keytab 文件。

进程级别

如果您将域用于生产，并且域需要较高级别的安全性，则可在进程级别设置服务主体。您可以对每个节点以及该节点上的每个进程创建唯一 SPN 和 keytab 文件。还必须为在节点上运行的 HTTP 进程创建一个 SPN 和一个 keytab 文件。

在进程级别启用的 Kerberos 提供最高级别的安全性，但在包含许多节点或具有许多服务的 Informatica 域中可能难以管理。这种情况下，您可能需要在节点级别启用 Kerberos。

配置 Kerberos 配置文件

在 Kerberos 配置文件中设置 Informatica 所需的属性，然后将文件复制到 Informatica 域中的每个节点。

Kerberos 将配置信息存储在一个名为 *krb5.conf* 的文件中。您必须在 *krb5.conf* 配置文件中设置属性，然后将文件复制到 Informatica 域中的每个节点。

如果域使用 Kerberos 跨域身份验证，请输入每个 Kerberos 域的必需属性。

- 1. 在文件的 *libdefaults* 部分中，配置以下 Kerberos 库属性。

下表介绍了要输入的属性：

属性	说明
default_realm	Informatica 域服务所属的 Kerberos 域的名称。域名称必须采用大写形式。 如果域使用单个 Kerberos 域进行身份验证，则服务域名称和用户域名称必须相同。
forwardable	允许服务将客户端用户凭据委派到其他服务。Informatica 域需要应用程序服务对其他服务的客户端用户凭据进行身份验证。 设置为 true。
default_tkt_enctypes	票证授予票证 (ticket-granting tickets, TGT) 中包含的会话密钥的加密类型。仅当会话密钥必须使用特定的加密类型时，才需要设置此属性。确保 Kerberos 密钥分发中心 (Key Distribution Center, KDC) 支持您指定的加密类型。 不设置此属性可允许 Kerberos 协议选择要使用的加密类型。 如果节点主机或 Informatica 客户端主机使用 256 位加密，请在所有节点主机和 Informatica 客户端主机上安装 Java 加密扩展 (Java Cryptography Extension, JCE) 无限强度策略文件以避免身份验证问题。
rdns	确定除正向名称查找外是否还使用反向名称查找，以规范主机名称在服务主体名称中的使用。 设置为 false。
renew_lifetime	初始票证请求的默认可续订有效期。
ticket_lifetime	初始票证请求的默认有效期。
udp_preference_limit	确定 Kerberos 将消息发送到 KDC 时使用的协议。 设置为 1 可在域遇到间歇性 Kerberos 身份验证故障时使用 TCP 协议。
dns_lookup_kdc	指示当域的 KDC 及其他服务器未在域的信息中列出时，Kerberos 客户端是否使用 DNS SRV 记录来定位它们。DNS 使用 SRV 记录来标识托管特定服务的计算机。当域启用 Kerberos 时，此属性为必需。 要求设置 admin_server 域属性。 设置为 true。
dns_lookup_realm	指示 Kerberos 客户端是否使用 DNS TXT 记录来确定主机的 Kerberos 域。DNS 使用文本或 TXT 记录将任意文本与主机名或其他名称（例如有关服务器、网络和数据中心的用户可读信息或其他会计信息）相关联。当域启用 Kerberos 时，此属性为必需。 设置为 true。

- 2. 在文件的 *realms* 部分中，定义每个 Kerberos 域。

以下示例显示了为名为 COMPANY.COM 的 Kerberos 域输入的内容：

```
[realms]
COMPANY.COM = {...}
```

3. 在文件的 *realms* 部分中，在每个 Kerberos 域的大括号内为其输入以下域属性。

下表介绍了要输入的属性：

属性	说明
admin_server	Kerberos 管理服务器主机的名称或 IP 地址。 您可以包括可选的端口号，用冒号将其与主机名隔开。默认值为 749。 如果在 <i>libdefaults</i> 部分中配置 <i>dns_lookup_kdc</i> ，则为必需。
kdc	为领域运行密钥分发中心 (KDC) 的主机的名称或 IP 地址。 您可以包括可选的端口号，用冒号将其与主机名隔开。默认值为 88。

以下示例显示了为 Kerberos 跨域配置中的每个 Kerberos 域输入的内容：

```
[realms]
COMPANY.COM = {
  admin_server = KDC01.COMPANY.COM:749
  kdc = KDC01.COMPANY.COM:88
}
EAST.COMPANY.COM = {
  kdc = 10.75.141.193
  admin_server = 10.75.141.193
}
WEST.COMPANY.COM = {
  kdc = 10.78.140.111
  admin_server = 10.78.140.111
}
```

4. 在 *domain_realms* 部分中，将域名或主机名映射到 Kerberos 域名称。域名以句点 (.) 为前缀。

以下示例显示了 Informatica 域不使用 Kerberos 身份验证时 Hadoop domain_realm 的参数：

```
[domain_realm]
.hadoop_realm.com = HADOOP-REALM
hadoop_realm.com = HADOOP-REALM
```

以下示例显示了 Informatica 域使用 Kerberos 身份验证时 Hadoop domain_realm 的参数：

```
[domain_realm]
.infa_ad_realm.com = INFA-AD-REALM
infa_ad_realm.com = INFA-AD-REALM
.hadoop_realm.com = HADOOP-REALM
hadoop_realm.com = HADOOP-REALM
```

5. 将 *krb5.conf* 文件复制到托管数据集成服务的计算机上的以下位置：

- <Informatica 安装目录>/services/shared/security
- <Informatica 安装目录>/java/jre/lib/security/

以下示例显示了具有单个 Kerberos 域配置必需属性的 Kerberos 配置文件的内容：

```
[libdefaults]
default_realm = COMPANY.COM
forwardable = true
rdns = false
renew_lifetime = 7d
ticket_lifetime = 24h
udp_preference_limit = 1
dns_lookup_kdc = true
dns_lookup_realm = true

[realms]
COMPANY.COM = {
```



```

admin_server = KDC01.COMPANY.COM:749
kdc = KDC01.COMPANY.COM:88
}

[domain_realm]
.company.com = COMPANY.COM
company.com = COMPANY.COM

```

以下示例显示了具有 Kerberos 跨域配置必需属性的 Kerberos 配置文件的内容：

```

[libdefaults]
default_realm = COMPANY.COM
forwardable = true
rdns = false
renew_lifetime = 7d
ticket_lifetime = 24h
udp_preference_limit = 1
dns_lookup_kdc = true
dns_lookup_realm = true

[realms]
COMPANY.COM = {
admin_server = KDC01.COMPANY.COM:749
kdc = KDC01.COMPANY.COM:88
}
EAST.COMPANY.COM = {
kdc = 10.75.141.193
admin_server = 10.75.141.193
}
WEST.COMPANY.COM = {
kdc = 10.78.140.111
admin_server = 10.78.140.111
}

[domain_realm]
.company.com = COMPANY.COM
company.com = COMPANY.COM
.east.company.com = EAST.COMPANY.COM
east.company.com = EAST.COMPANY.COM
.west.company.com = WEST.COMPANY.COM
west.company.com = WEST.COMPANY.COM

```

有关 Kerberos 配置文件的详细信息，请参阅 Kerberos 网络身份验证文档。

在 Active Directory 中创建 Kerberos 主体帐户

针对 Active Directory 中的 Kerberos 主体创建 LDAP 用户帐户。Kerberos 主体是 Kerberos 领域内的进程、服务或用户。

如果您将 krb5.conf 配置文件中的 default_tkt_enctypes 属性设置为 128 位或 256 位 AES 加密类型，请将每个帐户配置为使用 Active Directory 中的相应加密类型。

您创建的帐户取决于是在节点级别还是进程级别启用 Kerberos。

注意： 帐户名称长度不能超过 20 个字符。

节点级别所需的帐户

创建在 Active Directory 中的节点级别启用 Kerberos 身份验证所需的 LDAP 用户帐户。

如果您在节点级别启用 Kerberos，则在 Active Directory 中创建以下 Kerberos 主体帐户：

节点进程

为在域中运行的每个节点创建一个帐户。

HTTP 进程

为在域中的节点上运行的 Informatica Web 应用程序创建一个帐户。在节点上运行的 Web 应用程序可能包括 Administrator 工具、Informatica Analyst 和 Catalog Administrator。创建由节点上运行的所有 Web 应用程序共享的单个帐户。

绑定用户可辨别名称 (DN)

创建用于将包含 Kerberos 用户帐户的 LDAP 安全域与 Active Directory 同步的 LDAP 绑定用户帐户。

进程级别所需的帐户

创建在 Active Directory 中的进程级别启用 Kerberos 身份验证所需的 LDAP 用户帐户。

如果您在进程级别启用 Kerberos，则在 Active Directory 中创建以下 Kerberos 主体帐户：

节点进程

为在域中运行的每个节点创建一个帐户。

HTTP 进程

为在域中的节点上运行的 Informatica Web 应用程序创建一个帐户。在节点上运行的 Web 应用程序可能包括 Informatica Analyst 和 Catalog Administrator。创建由节点上运行的所有 Web 应用程序共享的单个帐户。

Informatica Administrator 服务

为域中每个网关节点上的 Administrator 工具创建一个帐户。

Informatica 应用程序服务

为在域中的每个节点上运行的每个 Informatica 应用程序服务创建一个帐户。

绑定用户可辨别名称 (DN)

创建用于将包含 Kerberos 用户帐户的 LDAP 安全域与 Active Directory 同步的 LDAP 用户帐户。

生成服务主体名称和 Keytab 文件名格式

使用 Informatica Kerberos SPN 格式生成器实用程序生成使用 Kerberos 身份验证所需的服务主体名称 (SPN) 和 keytab 文件名格式。Kerberos SPN 格式生成器实用程序生成名为 SPNKeytabFormat.txt 的文本文件，其中包含 SPN 和 keytab 文件名的正确格式。

您生成的 SPN 和 keytab 文件名格式取决于是在节点级别还是进程级别启用 Kerberos。

在节点级别生成服务主体名称和 Keytab 文件名格式

生成在节点级别启用 Kerberos 身份验证所需的 SPN 和 keytab 文件名的格式。

当您在节点级别启用 Kerberos 身份验证时，Informatica 域需要以下进程的 SPN 和 keytab 文件：

节点进程

对于域中的每个节点，Informatica 都需要一个 SPN 和 keytab 文件。Kerberos 使用相同的服务主体名称和 keytab 对在节点上运行的 Informatica 应用程序服务进行身份验证。

HTTP 进程

对于在域中的每个节点上运行的 Web 应用程序，Informatica 需要一个 SPN 和 keytab 文件。在节点上运行的 Web 应用程序可能包括 Administrator 工具、Informatica Analyst 和 Catalog Administrator。Kerberos 使用相同的服务主体名称对在节点上运行的所有 Web 应用程序进行身份验证。

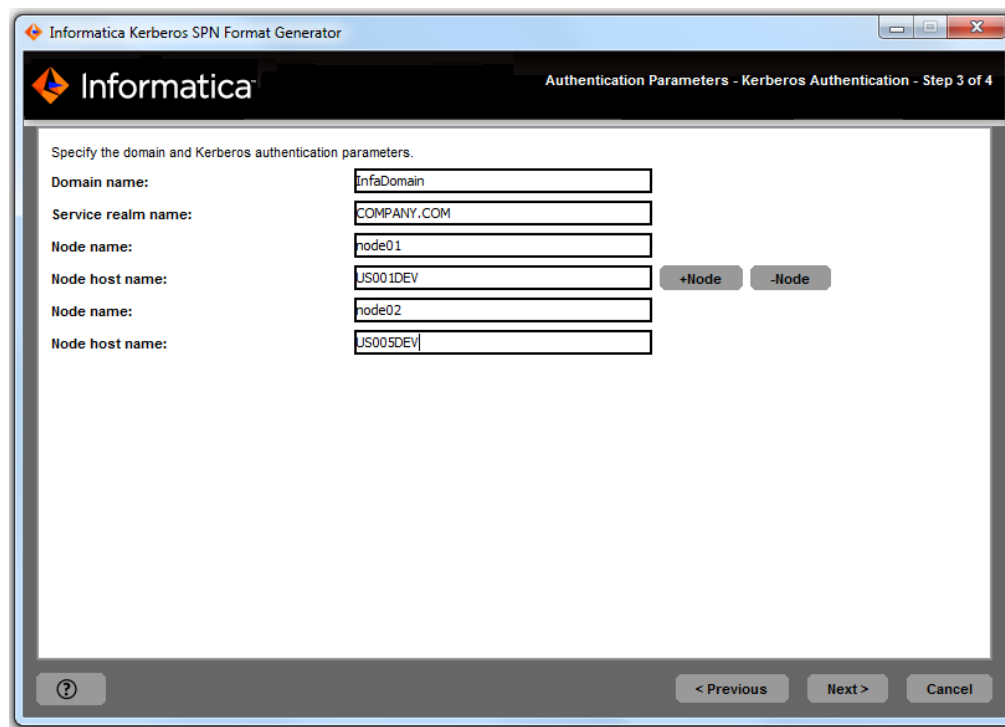
- 1. 在 Windows Informatica 节点主机上，转至包含 SPNFormatGenerator.bat 批处理文件的目录：
<Informatica 安装目录>\tools\Kerberos
在 UNIX Informatica 节点主机上，转至包含 SPNFormatGenerator.sh shell 文件的目录：
<Informatica 安装目录>/tools/Kerberos
- 2. 运行 SPNFormatGenerator.bat 或 SPNFormatGenerator.sh。
- 3. 单击**下一步**。
- 4. 选择**节点级别**。
- 5. 单击**下一步**。
- 6. 输入生成 SPN 和 keytab 文件格式所需的属性。

下表介绍了属性：

提示	说明
域名	Informatica 域的名称。域名的长度不得超过 128 个字符，并且必须为 7 位 ASCII。不能包含空格或以下任何字符：` % * + ; " ? , < > \ /
服务领域名	Kerberos 域的名称。领域名必须全部大写。
节点名称	Informatica 节点的名称。
节点主机名	节点主机的完全限定名称。节点主机名不能包含下划线 (_) 字符。 注意: 请勿使用 <i>localhost</i> 。主机名必须明确标识该主机。

7. 要为其节点生成 SPN 格式，请单击 **+节点**，然后指定节点名称和主机名。

下图显示了在 SPN 格式生成器实用程序中为 InfaDomain 域中的多个节点输入的内容：



8. 单击**下一步**。

SPN 格式生成器实用程序显示包含服务主体名称和 keytab 文件名列表的文件的路径和文件名。

9. 单击**完成**退出 SPN 格式生成器实用程序。

在进程级别生成服务主体名称和 Keytab 文件名格式

生成在进程级别启用 Kerberos 身份验证所需的 SPN 和 keytab 文件名的格式。

当您在进程级别启用 Kerberos 身份验证时，Informatica 域需要以下进程和服务的 SPN 和 keytab 文件：

节点进程

对于域中的每个节点，Informatica 都需要一个 SPN 和 keytab 文件。

Informatica Administrator

对于域中每个网关节点的 Administrator 工具，Informatica 需要一个 SPN 和 keytab 文件。

HTTP 进程

对于在域中的节点上运行的 Web 应用程序，Informatica 需要一个 SPN 和 keytab 文件。在节点上运行的 Web 应用程序可能包括 Informatica Analyst 和 Catalog Administrator。

Informatica 应用程序服务进程

对于在域中的每个节点上运行的每个 Informatica 应用程序服务，Informatica 都需要一个 SPN 和 keytab 文件。

- 1. 在 Windows Informatica 节点主机上，转至包含 SPNFormatGenerator.bat 批处理文件的目录：
<Informatica 安装目录>\tools\Kerberos
在 UNIX Informatica 节点主机上，转至包含 SPNFormatGenerator.sh shell 文件的目录：
<Informatica 安装目录>/tools/Kerberos
- 2. 运行 SPNFormatGenerator.bat 或 SPNFormatGenerator.sh。
- 3. 单击**下一步**。
- 4. 选择**进程级别**。
- 5. 单击**下一步**。
- 6. 输入生成 SPN 和 keytab 文件格式所需的属性。

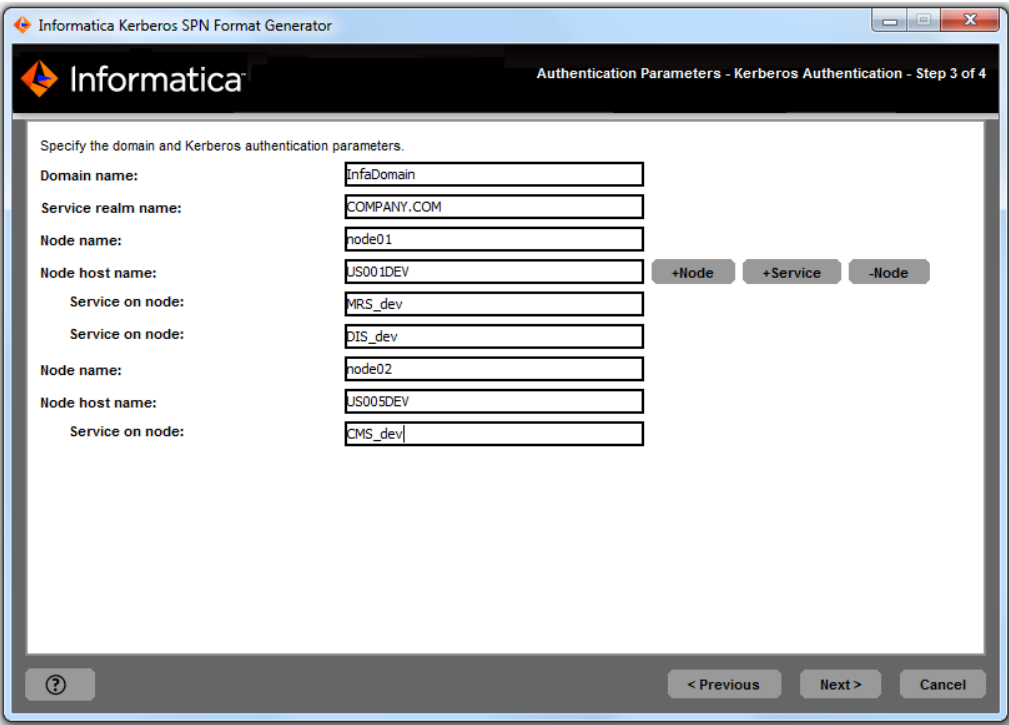
下表介绍了属性：

提示	说明
域名	Informatica 域的名称。域名的长度不得超过 128 个字符，并且必须为 7 位 ASCII。不能包含空格或以下任何字符：`%*+;"'?,<>\/
服务领域名	Kerberos 域的名称。领域名必须全部大写。
节点名称	Informatica 节点的名称。
节点主机名	节点主机的完全限定名称或 IP 地址。节点主机名不能包含下划线(_) 字符。 注意: 请勿使用 <i>localhost</i> 。主机名必须明确标识该主机。

- 7. 要为在节点上运行的 Informatica 应用程序服务生成 SPN 格式，请在输入节点详细信息后单击**服务**。
输入 Administrator 工具中显示的 Informatica 应用程序服务的名称。针对在域中的每个节点上运行的每个 Informatica 应用程序服务完成此步骤。

8. 要为其节点生成 SPN 格式，请单击 **+节点**，然后指定节点名称和主机名。

下图显示了在 SPN 格式生成器实用程序中为 InfaDomain 域中运行的多个节点和应用程序服务输入的内容：



9. 单击**下一步**。

SPN 格式生成器实用程序显示包含服务主体名称和 keytab 文件名列表的文件的路径和文件名。

10. 单击**完成**退出 SPN 格式生成器实用程序。

查看服务主体名称和 Keytab 文件名格式文本文件

生成 SPNKeytabFormat.txt 文件后，您可以查看该文件。

您可以使用该文件中的信息生成 keytab 文件，并将每个 SPN 与 Active Directory 中的相应主体用户帐户相关联。

SPNKeytabFormat.txt 文件包含以下信息：

实体名称

标识与该进程关联的节点或服务。

服务主体名称

SPN 的格式。SPN 区分大小写。

注意：如果输入包含多个 Kerberos 域名的字符串，或者在域名后缀前添加星号以将所有包含该后缀的域包含在内，则 SPN 格式不包括域名。

下表介绍了 SPN 格式：

Keytab 类型	SPN 格式
NODE_SPN	isp/<节点名称>/<域名>@<领域名>
NODE_AC_SPN	_AdminConsole/<节点名称>/<域名>@<领域名>
NODE_HTTP_SPN	HTTP/<节点主机名>@<领域名> 注意: Kerberos SPN 格式生成器验证节点主机名。如果节点主机名无效，该实用程序不会生成 SPN。而是会显示以下消息：无法解析主机名。
SERVICE_PROCESS_SPN	<应用程序服务名称>/<节点名称>/<域名>@<领域名>

密钥表文件名

为关联的 SPN 创建的 keytab 文件的名称格式。Keytab 文件名是区分大小写的。

下表介绍了 keytab 文件名格式：

Keytab 类型	Keytab 文件名
NODE_SPN	<节点名称>.keytab
NODE_AC_SPN	_AdminConsole.keytab
NODE_HTTP_SPN	webapp_http.keytab
SERVICE_PROCESS_SPN	<应用程序服务名称>.keytab

节点级别服务主体

下图显示了在节点级别为服务主体生成的 SPNKeytabFormat.txt 文件的内容：

ENTITY_NAME	SPN	KEY_TAB_NAME	KEY_TAB_TYPE
node01	isp/node01/Infadomain@COMPANY.COM	node01.keytab	NODE_SPN
node01	HTTP/US001DEV.company.com@COMPANY.COM	webapp_http.keytab	NODE_HTTP_SPN
node02	isp/node02/Infadomain@COMPANY.COM	node02.keytab	NODE_SPN
node02	HTTP/US005DEV.company.com@COMPANY.COM	webapp_http.keytab	NODE_HTTP_SPN

进程级别的服务主体

下图显示了在进程级别为服务主体生成的 SPNKeytabFormat.txt 文件的内容：

ENTITY_NAME	SPN	KEY_TAB_NAME	KEY_TAB_TYPE
node01	isp/node01/Infadomain@COMPANY.COM	node01.keytab	NODE_SPN
node01	_AdminConsole/node01/Infadomain@COMPANY.COM	_AdminConsole.keytab	NODE_AC_SPN
node01	HTTP/US001DEV.company.com@COMPANY.COM	webapp_http.keytab	NODE_HTTP_SPN
node02	isp/node02/Infadomain@COMPANY.COM	node02.keytab	NODE_SPN
node02	_AdminConsole/node02/Infadomain@COMPANY.COM	_AdminConsole.keytab	NODE_AC_SPN
node02	HTTP/US005DEV.company.com@COMPANY.COM	webapp_http.keytab	NODE_HTTP_SPN
MRS_dev:node01	MRS_dev/node01/Infadomain@COMPANY.COM	MRS_dev.keytab	SERVICE_PROCESS_SPN
DIS_dev:node01	DIS_dev/node01/Infadomain@COMPANY.COM	DIS_dev.keytab	SERVICE_PROCESS_SPN
CAT_dev:node02	CAT_dev/node02/Infadomain@COMPANY.COM	CAT_dev.keytab	SERVICE_PROCESS_SPN

生成 Keytab 文件

生成用于对 Informatica 用户和服务进行身份验证的 keytab 文件。

需使用 Microsoft Windows Server ktpass 实用程序为您在 Active Directory 中创建的每个用户帐户生成一个 keytab 文件。必须在成员服务器或在 Active Directory 域内的域控制器上生成 keytab 文件。不能在工作站操作系统（如 Microsoft Windows 7）上生成 keytab 文件。

要使用 ktpass 生成 keytab 文件，请运行以下命令：

```
ktpass.exe -out <keytab filename> -princ <service principal name> -mapuser <user account> [-pass <user account password>] -crypto <key types> -ptype <principal type> [-target <realm name>]
```

下表介绍了命令选项：

选项	说明
-out	要生成的 Kerberos keytab 文件的文件名，如 SPNKeytabFormat.txt 文件的 KEY_TAB_NAME 列所示。
-princ	在 SPNKeytabFormat.txt 文件的 SPN 列中显示的服务主体名称。 如果域使用 Kerberos 跨域身份验证，则在所有 Kerberos 域中，服务主体名称必须唯一。
-mapuser	要与 SPN 关联的 Active Directory 用户帐户。帐户名称不能超过 20 个字符。
-pass	在 Active Directory 中为 Active Directory 用户帐户设置的密码（若适用）。
-crypto	指定在 keytab 文件中生成的密钥类型。 设置为 all 可使用所有支持的加密类型。
-ptype	主体类型。设置为 KRB5_NT_PRINCIPAL。
-target	Active Directory 服务器所属域的名称。运行实用程序时如果出现以下错误，请加入此选项： DsCrackName 在名称中返回 0x2

您生成的 keytab 文件取决于是在节点级别还是进程级别启用 Kerberos。

在节点级别生成 Keytab 文件

运行 ktpass 以在节点级别生成 keytab 文件时，需将每个 Kerberos 主体用户帐户与 Active Directory 中的相应 SPN 相关联。

下表显示了 Kerberos 主体用户帐户与示例 SPNKeytabFormat.txt 文件中显示的 SPN 之间的关联：

用户帐户	Keytab 类型	服务主体名称
nodeuser01	NODE_SPN	isp/node01/InfaDomain/COMPANY.COM
httpuser01	NODE_HTTP_SPN	HTTP/US001DEV.company.com@COMPANY.COM
nodeuser02	NODE_SPN	isp/node02/InfaDomain/COMPANY.COM
httpuser02	NODE_HTTP_SPN	HTTP/US005DEV.company.com@COMPANY.COM

还需为 LDAP 同步期间用于访问和搜索 Active Directory 的 LDAP 绑定用户帐户创建一个 keytab。

1. 为您在 Active Directory 中针对每个节点创建的 Kerberos 主体用户帐户创建一个 keytab 文件。
从 SPNKeytabFormat.txt 文件中的 KEY_TAB_NAME 列复制 keytab 文件名。从 SPNKeytabFormat.txt 文件中的 SPN 列复制服务主体名称。

以下示例为名为 nodeuser0 的 Kerberos 主体用户帐户创建一个 keytab 文件：

```
ktpass.exe -out node01.keytab -princ isp/node01/Infadomain/COMPANY.COM -mapuser nodeuser01 -crypto all -ptype KRB5_NT_PRINCIPAL
```

2. 为您在 Active Directory 中创建的每个 HTTP 进程 Kerberos 主体用户帐户创建一个 keytab 文件。
如果域使用 Kerberos 跨域身份验证，主体用户帐户可以位于域使用的任何 Kerberos 域中。
从 SPNKeytabFormat.txt 文件中的 KEY_TAB_NAME 列复制 keytab 文件名。从 SPNKeytabFormat.txt 文件中的 SPN 列复制服务主体名称。

以下示例为名为 httpuser01 的 Kerberos 主体用户帐户创建一个 keytab 文件：

```
ktpass.exe -out webapp_http.keytab -princ HTTP/US001DEV.company.com@COMPANY.COM -mapuser httpuser01 -crypto all -ptype KRB5_NT_PRINCIPAL
```

3. 为 LDAP 同步期间用于访问和搜索 Active Directory 的 LDAP 绑定用户帐户创建一个 keytab。
将 -princ 选项的值结构化为 <主体名称>@<KERBEROS 域>。在 Keytab 文件名中包括 Active Directory 服务器的 LDAP 配置的名称。Keytab 文件名结构如下所示：<Active Directory LDAP 配置名称>.keytab。

以下示例为名为 ldapuser 的服务主体用户帐户创建一个 keytab 文件：

```
ktpass.exe -out ActiveDirectoryServer1.keytab -princ ldapuser@COMPANY.COM -mapuser ldapuser -crypto all -ptype KRB5_NT_PRINCIPAL
```

在进程级别生成 Keytab 文件

运行 ktpass 以在进程级别生成 keytab 文件时，需将每个 Kerberos 主体用户帐户与 Active Directory 中的相应 SPN 相关联。

下表显示了 Kerberos 主体用户帐户与示例 SPNKeytabFormat.txt 文件中显示的 SPN 之间的关联：

用户帐户	Keytab 类型	服务主体名称
nodeuser01	NODE_SPN	isp/node01/Infadomain/COMPANY.COM
admintooluser01	NODE_AC_SPN	_AdminConsole/node01/Infadomain@COMPANY.COM
httpuser01	NODE_HTTP_SPN	HTTP/US001DEV.company.com@COMPANY.COM
MRSdevuser01	SERVICE_PROCESS_SPN	MRS_dev/node01/Infadomain@COMPANY.COM
DISdevuser01	SERVICE_PROCESS_SPN	DIS_dev/node01/Infadomain@COMPANY.COM
nodeuser02	NODE_SPN	isp/node02/Infadomain/COMPANY.COM
admintooluser02	NODE_AC_SPN	_AdminConsole/node02/Infadomain@COMPANY.COM
httpuser02	NODE_HTTP_SPN	HTTP/US005DEV.company.com@COMPANY.COM
CATdevuser01	SERVICE_PROCESS_SPN	CAT_dev/node02/Infadomain@COMPANY.COM

还需为 LDAP 同步期间用于访问和搜索 Active Directory 的 LDAP 绑定用户帐户创建一个 keytab。

1. 为您在 Active Directory 中针对每个节点创建的 Kerberos 主体用户帐户创建一个 keytab 文件。

从 SPNKeytabFormat.txt 文件中的 KEY_TAB_NAME 列复制文件名。从 SPNKeytabFormat.txt 文件中的 SPN 列复制服务主体名称。

以下示例为名为 nodeuser01 的 Kerberos 主体用户帐户创建一个 keytab 文件：

```
ktpass.exe -out node01.keytab -princ isp/node01/Infadomain/COMPANY.COM -mapuser nodeuser01 -crypto all -  
ptype KRB5_NT_PRINCIPAL
```

2. 为您创建的每个 HTTP 进程 Kerberos 主体用户帐户创建一个 keytab 文件。

如果域使用 Kerberos 跨域身份验证，主体用户帐户可以位于域使用的任何 Kerberos 域中。

从 SPNKeytabFormat.txt 文件中的 KEY_TAB_NAME 列复制文件名。从 SPNKeytabFormat.txt 文件中的 SPN 列复制服务主体名称。

以下示例为名为 httpuser01 的 Kerberos 主体用户帐户创建一个 keytab 文件：

```
ktpass.exe -out webapp_http.keytab -princ HTTP/US001DEV.company.com@COMPANY.COM -mapuser httpuser01 -  
crypto all -ptype KRB5_NT_PRINCIPAL
```

3. 为您创建的每个 Administrator 工具 Kerberos 主体用户帐户创建一个 keytab 文件。

从 SPNKeytabFormat.txt 文件中的 KEY_TAB_NAME 列复制文件名。从 SPNKeytabFormat.txt 文件中的 SPN 列复制服务主体名称。

以下示例为名为 admintooluser01 的 Kerberos 主体用户帐户创建一个 keytab 文件：

```
ktpass.exe -out _AdminConsole.keytab -princ _AdminConsole/node01/Infadomain@COMPANY.COM -mapuser  
admintooluser01 -crypto all -ptype KRB5_NT_PRINCIPAL
```

4. 为您创建的每个 Informatica 应用程序服务 Kerberos 主体用户帐户创建一个 keytab 文件。

从 SPNKeytabFormat.txt 文件中的 KEY_TAB_NAME 列复制文件名。从 SPNKeytabFormat.txt 文件中的 SPN 列复制服务主体名称。

以下示例为名为 MRSdevuser01 的服务 Kerberos 主体用户帐户创建一个 keytab 文件：

```
ktpass.exe -out MRS_dev.keytab -princ HTTP/US001DEV.company.com@COMPANY.COM -mapuser MRSdevuser01 -crypto  
all -ptype KRB5_NT_PRINCIPAL
```

5. 为 LDAP 同步期间用于访问和搜索 Active Directory 的 LDAP 绑定用户帐户创建一个 keytab。

将 -princ 选项的值结构化为 <主体名称>@<KERBEROS 域>。在 Keytab 文件名中包括 Active Directory 服务器的 LDAP 配置的名称。Keytab 文件名结构如下所示：<Active Directory LDAP 配置名称>.keytab。

以下示例为名为 ldapuser 的服务主体用户帐户创建一个 keytab 文件：

```
ktpass.exe -out ActiveDirectoryServer1.keytab -princ ldapuser@COMPANY.COM -mapuser ldapuser -crypto all -  
ptype KRB5_NT_PRINCIPAL
```

验证服务主体名称和 Keytab 文件

您可以使用 Kerberos 实用程序验证 SPN 和 keytab 文件是否有效。还可以使用这些实用程序来确定 Kerberos 密钥分发中心 (KDC) 的状态。

您可以使用 Kerberos 实用程序（如 *kinit* 和 *klist*）来查看和验证 SPN 及 keytab 文件。要使用这些实用程序，请确保 KRB5_CONFIG 环境变量包含 Kerberos 配置文件的路径和文件名。有关运行 Kerberos 实用程序的详细信息，请参阅 Kerberos 文档。

使用以下实用程序验证 SPN 和 keytab 文件：

kinit

您可以使用 *kinit* 实用程序从 KDC 请求票证授予票证 (TGT)，并验证 keytab 文件是否可用于建立 Kerberos 连接。如果 keytab 和指定的 SPN 有效，命令则会获取一个票证，然后将该票证缓存在指定的缓存中。

kinit 实用程序位于 Informatica 节点上的以下目录中：

<Informatica 安装目录>\java\jre\bin

要为 SPN 请求票证授予票证，请运行以下命令：

```
kinit -c <缓存名称> -k -t <keytab 文件名> <服务主体名称>
```

以下输出示例显示了在默认缓存中为指定 keytab 文件和 SPN 创建的票证授予票证：

```
Cache: \temp\krb Using principal: isp/node01/Infadomain/COMPANY.COM Using keytab: node01.keytab
Authenticated to Kerberos v5
```

klist

您可以使用 *klist* 实用程序列出 keytab 文件中的 Kerberos 主体和密钥。要列出 keytab 文件中的密钥以及 keytab 条目的时间戳，请运行以下命令：

```
klist -k -t <keytab 文件名>
```

以下输出示例显示了 keytab 文件中的主体：

```
Keytab name: FILE:node01.keytab KVN0 Timestamp Principal ----
----- 3 12/31/16 19:00:00 MRS_dev/node01/
Infadomain@COMPANY.COM 3 12/31/16 19:00:00 MRS_dev/node01/Infadomain@COMPANY.COM 3 12/31/16 19:00:00
MRS_dev/node01/Infadomain@COMPANY.COM 3 12/31/16 19:00:00 MRS_dev/node01/Infadomain@COMPANY.COM
```

为 Active Directory 中的 Kerberos 主体用户帐户启用委派

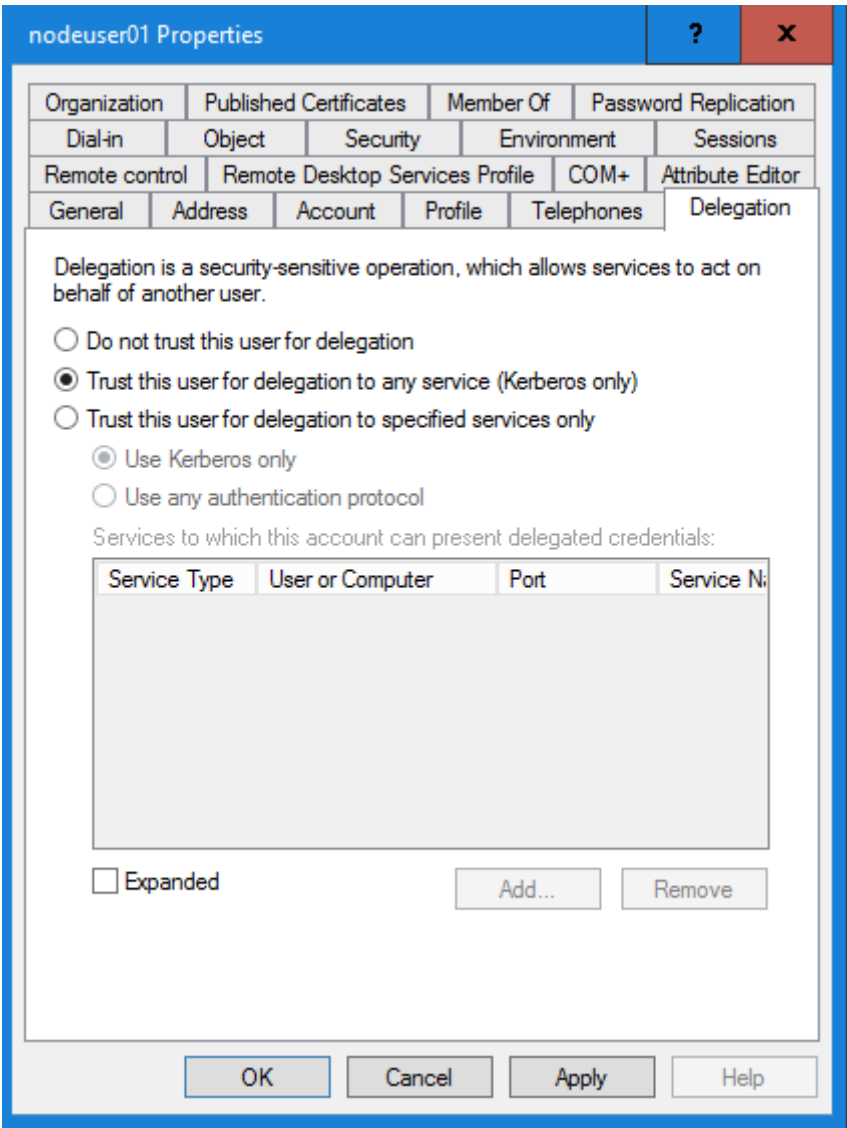
为在 Active Directory 中创建的每个 Kerberos 主体用户帐户启用委派。

如果使用某个服务对用户进行身份验证，且该服务使用经身份验证的用户的凭据连接到其他服务，将发生委派的身份验证。由于 Informatica 域中的服务需要连接到其他服务以完成某项操作，因此，Informatica 域要求在 Active Directory 中启用委派选项。

除了在 LDAP 同步期间用于访问和搜索 Active Directory 的 LDAP 绑定用户帐户外，必须为您创建的所有其他帐户启用委派。在每个用户帐户的属性对话框的“委派”选项卡中，将委派设置为**信任该用户以委派至任何服务（仅限 Kerberos）**。

注意: 在您运行 ktpass 创建 keytab 文件之前,“委派”选项卡在“属性”对话框中不可用。

下图显示了 nodeuser01 帐户属性对话框中的“委派”选项卡:



启用 Kerberos 身份验证

您可以在安装 Informatica 服务时在 Informatica 域中启用 Kerberos 身份验证,也可以在安装完服务后启用 Kerberos 身份验证。

有关如何在安装 Informatica 服务时启用 Kerberos 身份验证的信息,请参见《*Informatica 10.2 HotFix 2 安装和配置指南*》。

如果您在安装期间未启用 Kerberos 身份验证,可在安装完服务后,按照本节中的步骤使用 Informatica 命令行程序来启用 Kerberos 身份验证。

在域中启用 Kerberos 身份验证

在域内的网关节点上启用 Kerberos。

在域内的网关节点上运行 `infasetup switchToKerberosMode` 命令可将身份验证更改为 Kerberos 网络身份验证。

1. 关闭域和所有 Informatica 服务。按以下顺序关闭服务：

- Metadata Manager 服务
- PowerCenter® 集成服务
- PowerCenter® 存储库服务
- 内容管理服务
- 分析服务
- 数据集成服务
- 模型存储库服务

2. 在网关节点的命令提示符下，切换到 `infasetup` 可执行文件所在的目录：

<Informatica 安装目录>\isp\bin

3. 运行以下命令：

```
infasetup switchToKerberosMode -ad <administrator name> -srn <Kerberos realm names> -urn <Kerberos realm names> -spnSL <service principal level>
```

下表介绍了 infasetup switchToKerberosMode 命令的选项和参数：

选项	参数	说明
-administratorName -ad	user_name	<p>在配置 Kerberos 身份验证时创建的域管理员帐户的用户名。指定 Active Directory 中存在的帐户的名称。</p> <p>配置 Kerberos 身份验证后，此用户包含在该命令创建的 <i>_infalnternalNamespace</i> 安全域中。</p> <p>如果域使用单个 Kerberos 域对用户进行身份验证，指定要用作管理员帐户的那个帐户的 sam 帐户名。</p> <p>如果域使用 Kerberos 跨域身份验证，指定要用作管理员帐户的那个帐户的完全限定用户主体名称，其中包含域名。例如： sysadmin@COMPANY.COM</p>
-ServiceRealmName -srn	Kerberos_realm_name	<p>域在验证用户身份时使用的 Kerberos 域的名称。域名必须采用大写形式，且区分大小写。</p> <p>要配置 Kerberos 跨域身份验证，请指定域在验证用户身份时使用的每个 Kerberos 域的名称，用逗号分隔。例如： COMPANY.COM,EAST.COMPANY.COM, WEST.COMPANY.COM</p> <p>在域名称前使用星号作为通配符，将具有此名称的所有域包含在内。例如： *EAST.COMPANY.COM</p>
-UserRealmName -urn	Kerberos_realm_name	<p>域在验证用户身份时使用的 Kerberos 域的名称。域名必须采用大写形式，且区分大小写。</p> <p>要配置 Kerberos 跨域身份验证，请指定域在验证用户身份时使用的每个 Kerberos 域的名称，用逗号分隔。例如： COMPANY.COM,EAST.COMPANY.COM, WEST.COMPANY.COM</p> <p>在域名称前使用星号作为通配符，将具有此名称的所有域包含在内。例如： *EAST.COMPANY.COM</p>
-SPNShareLevel -spnSL	NODE PROCESS	<p>域的服务主体级别。</p> <p>设置为 NODE 可在节点级别启用 Kerberos。</p> <p>设置为 PROCESS 可在进程级别启用 Kerberos。</p>

以下示例将域的身份验证更改为 Kerberos，并将 sysadmin 用户帐户设置为使用单个 Kerberos 域进行用户身份验证的域的管理员帐户：

```
infasetup switchToKerberosMode -ad sysadmin -srn COMPANY.COM -urn COMPANY.COM -spnSL NODE
```

以下示例将域的身份验证更改为 Kerberos，并将 sysadmin 用户帐户设置为使用 Kerberos 跨域进行用户身份验证的域的管理员帐户：

```
infasetup switchToKerberosMode -ad sysadmin@COMPANY.COM -srn  
COMPANY.COM,COMPANY.EAST.COM,COMPANY.WEST.COM -urn COMPANY.COM,COMPANY.EAST.COM,COMPANY.WEST.COM -  
spnSL NODE
```

更新域中的节点

使用 Kerberos 身份验证服务器信息更新除运行 infasetup switchToKerberosMode 命令的网关节点外的所有网关和执行工作的节点。

使用以下命令更新网关和执行工作的节点：

infasetup UpdateGatewayNode

可使用 UpdateGatewayNode 命令在域中的网关节点上设置 Kerberos 身份验证参数。如果域有多个网关节点，请在各网关节点上运行 UpdateGatewayNode 命令。

infasetup UpdateWorkerNode

可使用 UpdateWorkerNode 命令在域中的执行工作的节点上设置 Kerberos 身份验证参数。如果域有多个执行工作的节点，请在各个执行工作的节点上运行 UpdateWorkerNode 命令。

1. 在节点的命令提示符下，切换到 infasetup 可执行文件所在的目录：

<Informatica 安装目录>\isp\bin

2. 要在网关节点上设置 Kerberos 身份验证参数，请运行以下命令：

```
infasetup UpdateGatewayNode -krb <true|false> -srn <Kerberos realm names> -urn <Kerberos realm names>
```

要在执行工作的节点上设置 Kerberos 身份验证参数，请运行以下命令：

```
infasetup UpdateWorkerNode -krb <true|false> -srn <Kerberos realm names> -urn <Kerberos realm names>
```

下表介绍了在节点上启用 Kerberos 身份验证所需的选项和参数：

选项	参数	说明
- EnableKerberos -krb	true false	将 Informatica 域配置为使用 Kerberos 身份验证。设置为 true 可启用 Kerberos 身份验证。默认值为 false。
- ServiceRealmName -srn	Kerberos_realm_name	域在验证用户身份时使用的 Kerberos 域的名称。域名必须采用大写形式，且区分大小写。 要配置 Kerberos 跨域身份验证，请指定域在验证用户身份时使用的每个 Kerberos 域的名称，用逗号分隔。例如： COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM 在域名称前使用星号作为通配符，将具有此名称的所有域包含在内。例如： *EAST.COMPANY.COM
- UserRealmName -urn	Kerberos_realm_name	域在验证用户身份时使用的 Kerberos 域的名称。域名必须采用大写形式，且区分大小写。 要配置 Kerberos 跨域身份验证，请指定域在验证用户身份时使用的每个 Kerberos 域的名称，用逗号分隔。例如： COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM 在域名称前使用星号作为通配符，将具有此名称的所有域包含在内。例如： *EAST.COMPANY.COM

以下示例将执行工作的节点更新为使用 Kerberos 身份验证：

```
infasetup updateWorkerNode -krb true -srn COMPANY.COM -urn COMPANY.COM
```

以下示例将执行工作的节点更新为使用 Kerberos 跨域身份验证：

```
infasetup updateWorkerNode -krb true -srn COMPANY.COM,COMPANY.EAST.COM,COMPANY.WEST.COM -urn  
COMPANY.COM,COMPANY.EAST.COM,COMPANY.WEST.COM
```

在 Informatica 节点上启用 Kerberos

在域中启用 Kerberos 后，必须将 Kerberos 配置文件复制到域中的每个节点。还必须配置 Web 浏览器以访问 Informatica Web 应用程序。

将 keytab 文件复制到每个节点上的以下目录：

```
<Informatica 安装目录>\isp\config\keys
```

您复制的 keytab 文件取决于是在节点级别还是进程级别启用 Kerberos 身份验证。

节点级别的 keytab 文件

将在节点级别生成的每个 keytab 文件复制到相应节点。

下表显示了每个 keytab 文件要复制到的节点：

Keytab 文件	在节点上的位置
<节点名称>.keytab	将每个文件复制到相应节点。
webapp_http.keytab	将每个文件复制到相应的网关节点。
ldapuser.keytab	将文件复制到每个网关节点。

进程级别的 keytab 文件

将在进程级别生成的每个 keytab 文件复制到相应节点。

下表显示了每个 keytab 文件要复制到的节点：

Keytab 文件	在节点上的位置
<节点名称>.keytab	将每个文件复制到相应节点。
webapp_http.keytab	将每个文件复制到相应的网关节点。
_AdminConsole.keytab	将每个文件复制到相应的网关节点。
<应用程序服务名称>.keytab	将每个文件复制到运行 Informatica 应用程序服务的相应节点。
ldapuser.keytab	将文件复制到每个网关节点。

配置 Web 浏览器以访问 Informatica Web 应用程序。

在 Microsoft Internet Explorer 和 Google Chrome 中，将 Informatica Web 应用程序（如 Analyst 工具）的 URL 添加到受信任站点列表。

如果使用 Chrome 版本 41 或更高版本，还必须设置 AuthServerWhitelist 和 AuthNegotiateDelegateWhitelist 策略。

将 Keytab 文件复制到 Informatica 节点

在创建 keytab 文件后，将每个 keytab 文件复制到相应节点。

将 keytab 文件复制到每个节点上的以下目录：

<Informatica 安装目录>\isp\config\keys

您复制的 keytab 文件取决于是在节点级别还是进程级别启用 Kerberos 身份验证。

节点级别的 keytab 文件

将在节点级别生成的每个 keytab 文件复制到相应节点。

下表显示了每个 keytab 文件要复制到的节点：

Keytab 文件	在节点上的位置
<节点名称>.keytab	将每个文件复制到相应节点。
webapp_http.keytab	将每个文件复制到相应节点。
ldapuser.keytab	将文件复制到每个网关节点。

进程级别的 keytab 文件

将在进程级别生成的每个 keytab 文件复制到相应节点。

下表显示了每个 keytab 文件要复制到的节点：

Keytab 文件	在节点上的位置
<节点名称>.keytab	将每个文件复制到相应节点。
webapp_http.keytab	将每个文件复制到相应节点。
_AdminConsole.keytab	将每个文件复制到相应节点。
<应用程序服务名称>.keytab	将每个文件复制到运行 Informatica 应用程序服务的相应节点。
ldapuser.keytab	将文件复制到每个节点。

为 Informatica 客户端启用 Kerberos 身份验证

将 Kerberos 配置文件复制到托管 Informatica 客户端的每台计算机，然后设置一个指向该配置文件的环境变量。还必须启用客户端浏览器以访问 Informatica Web 应用程序。

将 Informatica 域配置为使用 Kerberos 身份验证运行后，在 Informatica 客户端工具上执行以下任务：

将 Kerberos 配置文件复制到每个 Informatica 客户端主机。

将 krb5.conf 文件复制到托管 Informatica 客户端（如 PowerCenter 客户端或 Informatica Developer (Developer tool)）的每台计算机。将该文件复制到每个主机上的以下目录：

<Informatica 安装目录>\clients\shared\security

在每个 Informatica 客户端主机上设置 KRB5_CONFIG 环境变量。

将 KRB5_CONFIG 环境变量设置为托管 Informatica 客户端（如 PowerCenter 客户端和 Developer tool）的每台计算机上的 Kerberos 配置文件的路径和文件名。

配置 Web 浏览器以访问 Informatica Web 应用程序。

在 Microsoft Internet Explorer 和 Google Chrome 中，将 Informatica Web 应用程序（如 Analyst 工具）的 URL 添加到受信任站点列表。

如果使用 Chrome 版本 41 或更高版本，还必须设置 AuthServerWhitelist 和 AuthNegotiateDelegateWhitelist 策略。

启用用户帐户以使用 Kerberos 身份验证

在域中启用 Kerberos 身份验证后，将 Active Directory 中的 Informatica 用户帐户导入到包含 Kerberos 用户帐户的 LDAP 安全域。还必须将本地安全域中的组、角色、特权和权限迁移到包含 Kerberos 用户帐户的 LDAP 安全域中的相应 Active Directory 用户帐户。

将 Active Directory 中的用户帐户导入到 LDAP 安全域

将 Active Directory 中的用户帐户导入到 LDAP 安全域。

当您在域中启用 Kerberos 身份验证时，Informatica 会创建与 Kerberos 领域同名的空 LDAP 安全域。您可以将 Active Directory 中的用户帐户导入到此 LDAP 安全域，也可以将用户帐户导入到其他 LDAP 安全域。

可以使用 Administrator 工具将 Active Directory 中使用 Kerberos 身份验证的用户帐户导入到 LDAP 安全域。

要配置 Kerberos 跨域身份验证，请连接至 Active Directory 全局目录。连接至全局目录后，从由每个 Kerberos 域使用的 Active Directory 服务器中导入用户。

1. 启动该域和所有 Informatica 服务。
2. 使用您在域中启用 Kerberos 身份验证时指定的管理员帐户登录 Windows。
3. 登录 Administrator 工具。选择 _infalInternalNamespace 作为安全域。
4. 在 Administrator 工具中，单击**安全**选项卡。
5. 单击**操作**菜单，然后选择 **LDAP 配置**。
6. 在 **LDAP 配置**对话框中，单击 **LDAP 连接**选项卡。
7. 配置 Active Directory 的连接属性。

您可能需要咨询 LDAP 管理员以获取连接到 LDAP 服务器所需的信息。

下表描述了 LDAP 服务器配置属性：

属性	说明
服务器名称	Active Directory 服务器的主机名或 IP 地址。 要配置 Kerberos 跨域身份验证，请连接至 Active Directory 全局目录主机。指定完全限定的主机名。例如： host.company.local
端口	Active Directory 服务器的侦听端口。 默认为 389。默认 SSL 端口为 636。 要配置 Kerberos 跨域身份验证，请连接至 Active Directory 全局目录端口。默认为 3268。默认 SSL 端口为 3269。
LDAP 目录服务	选择 Microsoft Active Directory 服务 。
名称	指定您在 Active Directory 中创建的用于将 Active Directory 中的帐户与 LDAP 安全域同步的绑定用户帐户。 由于为 Kerberos 身份验证启用了域，因此您不能选择为该帐户提供密码。 如果域使用 Kerberos 跨域身份验证，则加上 Active Directory 主体数据库所属的域的名称。
使用 SSL 证书	指出 LDAP 服务器使用安全套接字层 (SSL) 协议。

属性	说明
信任 LDAP 证书	决定服务管理器是否可以信任 LDAP 服务器的 SSL 证书。如果选中，服务管理器将不验证 SSL 证书即连接到 LDAP 服务器。如果未选中，服务管理器在连接至 LDAP 服务器之前将验证 SSL 证书是否由证书颁发机构签名。
不区分大小写	指出当将用户分配给组时，服务管理器必须忽略识别名属性的大小写。
组成员关系属性	包含用户的组成员关系信息的属性名称。该属性是 LDAP 组对象中的属性，其中包含属于某个组的用户或组的识别名。例如， <i>member</i> 或 <i>memberof</i> 。
最大大小	导入安全域的用户帐户数量上限。例如，如果该值设置为 100，则可以将最多 100 个用户帐户导入到安全域中。 如果要导入的用户数超出该属性的值，服务管理器将生成一条错误消息，并且不导入任何用户。如果要导入的用户数量很多，请将该属性设置为一个较高的值。默认值为 1000。

8. 在 **LDAP 配置** 对话框中，单击**安全域**选项卡。

9. 单击**添加**。

下表介绍了可以为安全域设置的筛选器属性：

属性	说明
安全域	要将 Active Directory 中的用户帐户导入到的 LDAP 安全域的名称。
用户搜索基础	条目的识别名 (DN)，该条目用作在 Active Directory 中搜索用户名的起点。搜索可根据对象识别名中的路径在目录中找到对象。 例如，要在 example.com Windows 域中搜索包含 Informatica 用户帐户的 USERS 容器，请指定 CN=USERS,DC=EXAMPLE,DC=COM。
用户筛选器	用于指定在目录服务中搜索用户的条件的 LDAP 查询字符串。筛选器可以指定属性类型、断言值和匹配条件。 例如：(objectclass=*) 搜索所有对象。(&(objectClass=user)(!(cn=susan))) 搜索除 “susan” 之外的所有用户对象。有关搜索筛选器的详细信息，请参阅 LDAP 目录服务文档。

属性	说明
组搜索基础	条目的识别名 (DN)，该条目用作在 LDAP 目录服务中搜索组名称的起点。
组筛选器	用于指定在目录服务中搜索组的条件的 LDAP 查询字符串。

下图显示了将 Active Directory 中的 LDAP 用户导入到您在域中启用 Kerberos 时创建的 LDAP 安全域所需的信息：

LDAP Configuration

Fields marked with an asterisk (*) are required.

LDAP Connectivity

Security Domains

Schedule

You can specify multiple security domains for LDAP users and groups.
Click Add to add a new security domain.

Add

▼ Add new Security Domain

Preview

Cancel

Security Domain *

COMPANY.COM

User search base

CN=USERS,DC=COMPANY,DC=COM

User filter

Group search base

Group filter

?

Synchronize Now

OK

Cancel

10. 单击**立即同步**。
- 服务管理器将 LDAP 安全域中的所有用户与 LDAP 目录服务中的用户同步。完成同步进程所需的时间取决于要导入的用户和组的数量。
11. 单击**确定**保存 LDAP 安全域。

将本地用户特权和权限迁移至 Kerberos 安全域

如果 Informatica 域在本地安全域中具有用户帐户，则 Kerberos 安全域中的对应 Active Directory 用户帐户必须具有相同的组、角色、特权和权限。将本地用户的组、角色、特权和权限迁移到 Kerberos LDAP 安全域中的相应用户帐户。

1. 查看本地用户帐户的列表并确定要迁移到 LDAP 安全域以执行 Kerberos 身份验证的帐户。
- 要列出 Informatica 域中的用户帐户，请运行以下命令：

```
infacmd isp ListAllUsers
```

要迁移到 Kerberos 安全域的每个本地用户帐户都必须在用于 Kerberos 身份验证的 Active Directory 服务中具有相应的帐户。

2. 创建用户迁移文件。

用户迁移文件为纯文本文件，包含本地用户列表及需要相同组、角色、特权和权限的相应 Kerberos 用户。

请使用以下格式在用户迁移文件中列出条目：

Native/<source user name>,<LDAP security domain>/<target user name>

以下示例显示了包含要迁移到 COMPANY.COM 安全域的以下用户列表的用户迁移文件：

Native/User1,COMPANY.COM/User1
Native/User2,COMPANY.COM/User2
Native/User3,COMPANY.COM/User3

3. 运行 infacmd isp migrateUsers 命令，将本地安全域中的帐户特权和权限迁移到 Kerberos 安全域中的帐户。

要迁移用户的组、角色、特权和权限，请运行以下命令：

infacmd isp migrateUsers -dn <domain name> -un <administrator user name> -pd <administrator password> -sdn <security domain> -umf <user migration file>

下表介绍了命令选项：

选项	说明
-DomainName -dn	Informatica 域的名称。
-UserName -un	连接到域的用户名。 指定您在 infasetup switchToKerberosMode 命令中指定的管理员帐户的用户名。
-Password -pd	管理员帐户的密码。
-SecurityDomain -sdn	用于连接到域的管理员帐户的 LDAP 安全域。 指定 _infaInternalNamespace。
-UserMigrationFile -umf	用户迁移文件的路径和文件名。 该命令会跳过含有重复源用户名或目标用户名的条目。

以下示例基于 Um_s.txt 用户迁移文件迁移用户的组、角色、特权和权限：

infacmd isp migrateUsers -dn InfaDomain -un nodeuser01 -pd password -sdn _infaInternalNamespace -umf C:\Infa\um_s.txt

该命令会使用本地用户的连接对象权限覆盖分配给 LDAP 用户的连接对象权限。该命令将合并本地用户和对应 LDAP 用户的组、角色、特权和域对象权限。

migrateUsers 命令在其运行目录中创建名为 Infacmd_uml_<date>_<time>.txt 的详细日志文件。

第 5 章

Informatica Web 应用程序的 SAML 身份验证

本章包括以下主题：

- [SAML 身份验证概览, 55](#)
- [SAML 身份验证流程, 56](#)
- [在域中启用 SAML 身份验证, 56](#)
- [配置 Web 应用程序以使用其他标识提供程序, 61](#)

SAML 身份验证概览

您可以为 Informatica Web 应用程序配置安全断言标记语言(SAML)身份验证。

安全断言标记语言是一种基于 XML 的数据格式，用于在服务提供程序和标识提供程序之间交换身份验证信息。在 Informatica 域中，Informatica Web 应用程序是服务提供程序。

可以配置以下 Informatica Web 应用程序以使用 SAML 身份验证：

- Informatica Administrator
- Informatica Analyst
- Mass Ingestion 工具
- Metadata Manager
- Enterprise Data Catalog
- Enterprise Data Preparation

Informatica 支持以下标识提供程序：

- Microsoft Active Directory 联合身份验证服务 (AD FS)
- PingFederate
- F5 Big-IP SAML
- NetScaler

有关这些标识提供程序受支持的版本的信息，请参阅 Informatica Network 上的“产品可用性矩阵”：
<https://network.informatica.com/community/informatica-network/product-availability-matrices>。

注意：不能在配置为使用 Kerberos 身份验证的 Informatica 域中使用 SAML 身份验证。

如果使域使用 SAML 身份验证，在域中运行的所有 Web 应用程序将使用在域中配置的默认标识提供程序。但是，可以在域中运行的 Web 应用程序配置为使用其他标识提供程序。例如，可以将 Informatica Administrator 配置为使用 AD FS 作为标识提供程序，并将 Informatica Analyst 配置为使用 PingFederate 作为标识提供程序。

有关配置 Web 应用程序以使用其他标识提供程序的详细信息，请参阅 [“配置 Web 应用程序以使用其他标识提供程序” 页面上 61。](#)

SAML 身份验证流程

Informatica Web 应用程序与标识提供程序交换身份验证信息以在 Informatica 域中启用 SAML 身份验证。

以下步骤描述了基本 SAML 身份验证流程：

1. 用户访问 Informatica Web 应用程序。
2. 用户选择包含用于在应用程序登录页面上进行 SAML 身份验证的 LDAP 用户帐户的安全域，然后单击“登录”按钮。
如果用户选择本机安全域，用户将提供用户名和密码并登录到应用程序。
3. 基于标识提供程序配置，系统将提示用户提供首次身份验证所需的凭据。
4. 标识提供程序验证用户凭据并为用户创建会话。
标识提供程序还验证目标 Web 应用程序 URL，然后使用包含用户身份信息的 SAML 令牌将用户重定向到 Web 应用程序。
5. 应用程序验证 SAML 令牌和用户身份信息，创建用户会话，然后完成用户登录过程。

浏览器中的现有用户会话用于后续身份验证。要访问其他 Informatica Web 应用程序配置以使用 SAML 身份验证，用户将在应用程序登录页面上选择 LDAP 安全域。用户不需要提供用户名或密码。

用户会保持登录到正在同一个浏览器会话中运行的所有 Informatica Web 应用程序。但是，如果用户从 Informatica Web 应用程序中注销，则该用户也会从正在同一个浏览器会话中运行的其他 Informatica Web 应用程序中注销。

在域中启用 SAML 身份验证

在域中配置标识提供程序、Informatica 域和网关节点以使用 SAML 身份验证。

要为在域中运行的受支持的 Informatica Web 应用程序配置 SAML 身份验证，请执行以下任务：

1. 创建 LDAP 配置以连接到包含 Informatica Web 应用程序用户帐户的 LDAP 标识存储：还创建 LDAP 安全域，然后将用户帐户导入安全域。
2. 从标识提供程序导出断言签名证书。
3. 将断言签名证书导入到域中每个网关节点上的信任库文件。可以将证书导入到 Informatica 默认信任库文件，也可以导入到自定义信任库文件。
4. 在标识提供程序中添加一个或多个依赖方信任或服务提供程序。
5. 将每个 Informatica Web 应用程序的 URL 添加到标识提供程序。
6. 在域中启用 SAML 身份验证。
7. 在域中的每个网关节点上启用 SAML 身份验证。

为标识提供程序或 LDAP 存储创建 LDAP 配置

使用 Administrator 工具为包含使用 SAML 身份验证的 Web 应用程序用户帐户的标识提供程序或 LDAP 存储创建 LDAP 配置。

创建 LDAP 配置时，为用户帐户创建安全域，然后将帐户导入安全域。将帐户导入到安全域中之后，为安全域中的帐户分配适当的 Informatica 域角色、特权和权限。

有关创建 LDAP 配置的详细信息，请参阅 [“创建 LDAP 配置” 页面上 22。](#)

导出断言签名证书

从标识提供程序导出断言签名证书。

该证书是一个标准 X.509 证书，用于为标识提供程序颁发给 Informatica Web 应用程序的 SAML 令牌中的断言签名。可生成自签名的安全套接字层 (Secure Sockets Layer, SSL) 证书，也可以从证书颁发机构获取证书并将其导入到标识提供程序。

将证书导入到用于 SAML 身份验证的信任库

将标识提供程序所用的断言签名证书导入用于在 Informatica 域中的每个网关节点上进行 SAML 身份验证的信任库文件。

可以将证书导入到 Informatica 默认信任库文件，也可以导入到自定义信任库文件。

默认 Informatica 信任库文件的文件名为 `infa_truststore.jks`。文件安装在每个节点的以下位置：

`<Informatica 安装目录>\services\shared\security\infa_truststore.jks`

注意：不要将默认 `infa_truststore.jks` 文件替换为自定义信任库文件。

如果将证书导入到自定义信任库文件中，则不得将信任库文件保存在包含默认 Informatica 信任库文件的目录中。信任库文件名称必须为 `infa_truststore.jks`。

可以使用 Java keytool 密钥和证书管理实用程序创建 SSL 证书或证书签名请求 (CSR) 以及 JKS 格式的密钥库和信任库。keytool 位于域节点的以下目录中：

`<Informatica installation directory>\java\bin`

如果域节点在 AIX 上运行，则可以使用随 IBM JDK 一起提供的 keytool 创建一个 SSL 证书或证书签名请求 (CSR) 以及密钥库和信任库。

1. 将证书文件复制到 Informatica 域中的网关节点上的本地文件夹。
2. 从命令行中，转到 keytool 实用程序在该节点上的位置。
3. 运行 keytool 实用程序导入证书。
4. 重新启动节点。

配置标识提供程序

配置标识提供程序以将 SAML 令牌颁发给 Informatica Web 应用程序。

执行以下任务以配置标识提供程序：

- 在标识提供程序中为域添加依赖方信任：依赖方信任定义使标识提供程序能够接受来自在域中运行的 Informatica Web 应用程序的身份验证请求。
- 编辑“以声明方式发送 LDAP 特性”规则，以将标识存储中的 LDAP 属性映射到标识提供程序颁发的 SAML 令牌中使用的相应类型。

在域中启用 SAML 身份验证时，提供依赖方信任的名称。根据您的安全要求，可以在标识提供程序中创建多个依赖方信任，使企业内不同组织所使用的域都能够使用 SAML 身份验证。

Informatica 将 “informatica” 识别为默认的依赖方信任名称。如果使用 “informatica” 作为依赖方信任名称创建单个依赖方信任，则在域中启用 SAML 身份验证时无需提供依赖方信任名称。

注意：标识提供程序中的所有字符串（包括 URL）区分大小写。

将 Informatica Web 应用程序 URL 添加到标识提供程序

将每个使用 SAML 身份验证的 Informatica Web 应用程序的 URL 添加到标识提供程序。

必须提供 Informatica Web 应用程序的 URL 才能使标识提供程序接受由应用程序发送的身份验证请求。提供该 URL 还能使标识提供程序在对用户进行身份验证之后将 SAML 令牌发送到应用程序。

在域中启用 SAML 身份验证

可以在现有的 Informatica 域中启用 SAML 身份验证，也可以在创建域时启用。

使域使用 SAML 身份验证时，在域中运行的所有 Web 应用程序将使用在域中启用 SAML 身份验证时指定的默认标识提供程序。例如，如果配置 AD FS 作为标识提供程序，所有 Web 应用程序将使用 AD FS 作为标识提供程序，除非将 Web 应用程序配置为使用其他标识提供程序。

选择以下选项之一：

运行 Informatica 安装程序时启用 SAML 身份验证

可以在安装过程中配置域时启用 SAML 身份验证并指定标识提供程序 URL。

在现有域中启用 SAML 身份验证。

使用 `infasetup updateDomainSamlConfig` 命令在现有的 Informatica 域中启用 SAML 身份验证。可以在域中的任何网关节点上运行此命令。

在创建域时启用 SAML 身份验证。

可以在创建域时使用 `infasetup defineDomain` 命令来启用 SAML 身份验证。

有关使用命令的说明，请参阅《*Informatica 命令参考*》。

infasetup updateDomainSamlConfig 命令选项

在 `infasetup updateDomainSamlConfig` 命令中设置 SAML 选项可在域中启用 SAML 身份验证。运行此命令之前，请关闭域。

指定标识提供程序 URL 作为 `-iu` 选项的值。以下示例显示了配置域以使用 AD FS 作为标识提供程序的命令用法：

```
infasetup updateDomainSamlConfig -saml true -iu https://server.company.com/adfs/ls/ -spid Prod_Domain -cst 240
```

下表介绍了选项和参数：

选项	参数	说明
-EnableSaml -saml	true false	必需。将此值设置为 true 可为 Informatica 域中受支持的 Informatica Web 应用程序启用 SAML 身份验证。 将此值设置为 false 可为 Informatica 域中受支持的 Informatica Web 应用程序禁用 SAML 身份验证。
-idpUrl -iu	identity_provider_url	如果 -saml 选项为 true，则为必需。指定域的标识提供程序 URL。必须指定完整的 URL 字符串。

选项	参数	说明
- ServiceProviderId -spid	service_provider_id	可选。如 Active Directory 联合身份验证服务(AD FS)中定义，域的依赖方信任名称或服务提供程序标识符。 如果已在 AD FS 中指定 “informatica” 作为依赖方信任名称，则无需指定值。
- ClockSkewTolerance -cst	clock_skew_tolerance_in_seconds	可选。AD FS 主机系统时钟与主网关节点系统时钟之间允许的时间差。 系统会根据 AD FS 主机系统时钟设置 AD FS 所颁发的 SAML 令牌的有效期。如果在令牌中设置的开始时间或结束时间与主网关节点系统时钟之间的时间差在指定的秒数内，则 AD FS 颁发的 SAML 令牌的有效期仍未到期。 值必须介于 0 到 600 秒之间。默认值为 120 秒。

有关使用 `infasetup updateDomainSamlConfig` 命令的说明，请参阅《*Informatica 命令参考*》。

infasetup DefineDomain 命令选项

可以在创建域时使用 `infasetup defineDomain` 命令来启用 SAML 身份验证。

以下示例显示了在命令提示符的最后 6 个选项中配置域以使用 AD FS 作为标识提供程序的选项。

```
infasetup defineDomain -cs "jdbc:informatica:oracle://host:1521;sid=DB2" -dt oracle -dn TestDomain -ad
test_admin -pd test_admin -ld $HOME/ISP/1011/source/logs -nn TestNode1 -na host1.company.com -saml true -iu
https://server.company.com/adfs/ls/ -spid Prod_Domain -cst 240 -asca adfs-cert -std \custom\security\ -stp
password -mi 10000 -ma 10200 -rf $HOME/ISP/BIN/nodeoptions.xml
```

下表介绍了 SAML 选项和参数：

选项	参数	说明
-EnableSaml -saml	true false	必需。将此值设置为 true 可为 Informatica 域中受支持的 Informatica Web 应用程序启用 SAML 身份验证。 将此值设置为 false 可为 Informatica 域中受支持的 Informatica Web 应用程序禁用 SAML 身份验证。
-idpUrl -iu	identity_provider_url	如果 -saml 选项为 true，则为必需。指定域的标识提供程序 URL。必须指定完整的 URL 字符串。
- ServiceProviderId -spid	service_provider_id	可选。如 Active Directory 联合身份验证服务(AD FS)中定义，域的依赖方信任名称或服务提供程序标识符。 如果已在 AD FS 中指定 “informatica” 作为依赖方信任名称，则无需指定值。
- ClockSkewTolerance -cst	clock_skew_tolerance_in_seconds	可选。AD FS 主机系统时钟与主网关节点系统时钟之间允许的时间差。 系统会根据 AD FS 主机系统时钟设置 AD FS 所颁发的 SAML 令牌的有效期。如果在令牌中设置的开始时间或结束时间与主网关节点系统时钟之间的时间差在指定的秒数内，则 AD FS 颁发的 SAML 令牌的有效期仍未到期。 值必须介于 0 到 600 秒之间。默认值为 120 秒。

选项	参数	说明
- AssertionSigning CertificateAlias -asca	idp_assertion_signing_certificate_alias	如果 -saml 选项为 true，则为必需项。在将标识提供程序断言签名证书导入到用于 SAML 身份验证的信任库文件时指定的别名。
- SamlTrustStoreDirectory -std	saml_truststore_directory	可选。一个目录，其中包含在域中的网关节点上使用 SAML 身份验证所需的自定义信任库文件。仅可指定文件的目录，而不能指定完整路径。 如果未指定任何信任库，SAML 身份验证将使用默认 Informatica 信任库。
- SamlTrustStorePassword -stp	saml_truststore_password	如果使用自定义信任库，则为必需。自定义信任库文件的密码。

有关使用 `infasetup defineDomain` 命令的说明，请参阅《*Informatica 命令参考*》。

在网关节点上启用 SAML 身份验证

必须在 Informatica 域中的每个网关节点上配置 SAML 身份验证。

选择以下选项之一在网关节点上配置 SAML 身份验证：

在计算机上定义网关节点时启用 SAML 身份验证。

使用 `infasetup DefineGatewayNode` 命令在网关节点上启用 SAML 身份验证。

在将网关节点配置为加入使用 SAML 身份验证的域时启用 SAML 身份验证。

使用 `infasetup UpdateGatewayNode` 命令在网关节点上启用 SAML 身份验证。

在将执行工作的节点转换为网关节点时启用 SAML 身份验证。

使用 `isp SwitchToGatewayNode` 命令在节点上启用 SAML 身份验证。

有关使用命令的说明，请参阅《*Informatica 命令参考*》。

网关节点命令选项

可以在创建网关节点时使用 `infasetup DefineGatewayNode` 命令来启用 SAML 身份验证。使用 `infasetup UpdateGatewayNode` 或 `infacmd isp SwitchToGatewayNode` 可在现有节点上启用 SAML 身份验证。

这些命令的 SAML 选项全部相同。以下示例显示了作为 `infasetup DefineGatewayNode` 命令行中最后四个选项的 SAML 选项：

```
infasetup defineGatewayNode -cs "jdbc:informatica:oracle://host:1521;sid=xxxx" -du test_user -dp test_user -dt
oracle -dn TestDomain -nn TestNode1 -na host2.company.com:1234 -ld $HOME/ISP/1011/source/logs -rf
$HOME/ISP/BIN/nodeoptions.xml -mi 10000 -ma 10200 -ad test_admin -pd test_admin -saml true -asca adfscert -std
\custom\security\ -stp password
```

下表介绍了选项和参数：

选项	参数	说明
-EnableSaml -saml	true false	必需。在 Informatica 域中启用 SAML 身份验证。 将此值设置为 true 可在域中启用 SAML 身份验证。 将此值设置为 false 可在域中禁用 SAML 身份验证。
-AssertionSigning CertificateAlias -asca	idp_assertion_ signing_certificate_ aliasAlias	如果为域启用了 SAML 身份验证，则为必需。在将标识提供程序断言 签名证书导入到用于 SAML 身份验证的信任库文件时指定的别名。
-SamlTrustStoreDir -std	saml_truststore_ directory	可选。一个目录，其中包含在域中的网关节点上使用 SAML 身份验证 所需的自定义信任库文件。仅可指定文件的目录，而不能指定完整路 径。 如果未指定任何信任库，将使用默认 Informatica 信任库。
-SamlTrustStorePassword -stp	saml_truststore_ password	如果使用自定义信任库，则为必需。自定义信任库文件的密码。

有关使用 `infasetup DefineGatewayNode`、`infasetup UpdateGatewayNode` 和 `infacmd isp SwitchToGatewayNode` 命令的说明，请参阅《*Informatica 命令参考*》。

配置 Web 应用程序以使用其他标识提供程序

可以在域中运行的 Informatica Web 应用程序配置为使用其他标识提供程序。例如，可以将 Informatica Administrator 配置为使用 AD FS 作为标识提供程序，并将 Informatica Analyst 配置为使用 PingFederate 作为标识提供程序。

使域使用 SAML 身份验证时，在域中运行的所有 Web 应用程序将使用在域中启用 SAML 身份验证时指定的默认标识提供程序。例如，如果配置 AD FS 作为标识提供程序，所有 Web 应用程序将使用 AD FS 作为标识提供程序，除非将 Web 应用程序配置为使用其他标识提供程序。

使用以下选项之一启用 SAML 身份验证时指定默认标识提供程序：

- 创建域并安装 Informatica 服务时。
- 运行 `infasetup defineDomain` 命令创建域时。
- 运行 `infasetup updateDomainSamlConfig` 命令在现有域中启用 SAML 身份验证时。

使用 Administrator 工具将 Web 应用程序配置为使用其他标识提供程序。要将 Administrator 工具或监视应用程序配置为使用其他标识提供程序，必须在应用程序运行的节点上修改 SAML 配置。要将其他 Web 应用程序配置为使用其他标识提供程序，请在应用程序进程中修改 SAML 配置。

准备使用标识提供程序

完成以下任务以准备 Informatica Web 应用程序以使用标识提供程序。

1. 为包含 Informatica Web 应用程序用户帐户的标识提供程序存储创建 LDAP 配置。还创建 LDAP 安全域，然后将用户帐户导入安全域。

2. 从标识提供程序导出标识提供程序断言签名证书。
3. 将标识提供程序断言签名证书导入到域中每个网关节点上的信任库文件。可以将证书导入到 Informatica 默认信任库文件，也可以导入到自定义信任库文件。
如果更改别名名称，请将相应证书导入每个网关节点上的信任库，然后重新启动节点。
4. 在标识提供程序中添加一个或多个依赖方信任，并将 LDAP 属性映射到标识提供程序颁发的安全令牌中使用的相应类型。
5. 将 Informatica Web 应用程序的 URL 添加到标识提供程序。

配置 Informatica Administrator 以使用一个标识提供程序

使用 Administrator 工具将 Administrator 工具或监视应用程序配置为使用 SAML 标识提供程序。配置 Administrator 工具或监视应用程序以在应用程序运行的节点上使用标识提供程序。

1. 在 Administrator 工具中，单击**服务和节点**选项卡。
2. 在域导航器中选择 Administrator 工具和监视应用程序在其中运行的网关节点。
3. 单击 SAML 配置旁边的编辑图标。
4. 输入使应用程序使用标识提供程序所需的属性。

下表介绍了输入的属性：

属性	说明
标识提供程序 URL	可选。标识提供程序服务器的 URL。必须指定完整的 URL 字符串。
服务提供程序 ID	可选。如标识提供程序中定义的域的依赖方信任名称或服务提供程序标识符。
断言签名证书别名	可选。在将标识提供程序断言签名证书导入到用于 SAML 身份验证的信任库文件时指定的别名。 如果更改别名名称，请将相应证书导入每个网关节点上的信任库，然后重新启动节点。
时钟偏差公差	可选。标识提供程序主机系统时钟与主网关节点上系统时钟之间允许的时间差。 可选。系统会根据标识提供程序主机系统时钟设置标识提供程序所颁发的 SAML 令牌的有效期。如果在令牌中设置的开始时间或结束时间与主网关节点系统时钟之间的时间差在指定的秒数内，则标识提供程序颁发的 SAML 令牌的有效期仍未到期。 值必须介于 0 到 600 秒之间。设置为 -1 以使用为域配置的值。默认值为 120 秒。

下图显示了使 Administrator 工具使用 AD FS 作为标识提供程序的配置：如果没有为属性指定值，域将使用在默认 SAML 配置中设置的值。

Edit SAML Configuration

Fields marked with an asterisk (*) are required.

Web Application ID *

monitoring

Identity Provider URL

Service Provider ID

Assertion Signing Certificate Alias

Clock Skew Tolerance

-1

Web Application ID *

AdministratorConsole

Identity Provider URL

https://server.company.com/adfs/ls/

Service Provider ID

ADFS_Prod

Assertion Signing Certificate Alias

adfs_cert

Clock Skew Tolerance

240

OKCancel

5. 单击**确定**。
6. 重新启动应用程序。

配置 Informatica Web 应用程序

使用 Administrator 工具将 Informatica Web 应用程序配置为使用 SAML 标识提供程序。

1. 在 Administrator 工具中，单击**服务和节点**选项卡。
2. 在域导航器中选择应用程序或应用程序服务。

• 要将 Analyst 工具应用程序配置为使用标识提供程序，请选择 Analyst 服务，然后单击**进程**选项卡。

• 要将 Mass Ingestion 工具应用程序配置为使用标识提供程序，请选择 Mass Ingestion 服务，然后单击**进程**选项卡。

• 要将 Metadata Manager 应用程序配置为使用标识提供程序，请选择 Metadata Manager 服务，然后单击**属性**选项卡。

• 要将 Enterprise Data Catalog 应用程序或 Catalog Administrator 应用程序配置为使用标识提供程序，请选择 Catalog 服务，然后单击**进程**选项卡。

• 要将 Enterprise Data Preparation 应用程序配置为使用标识提供程序，请选择 Enterprise Data Preparation 服务，然后单击**进程**选项卡。

3. 单击 **SAML 配置** 旁边的编辑图标。

4. 输入允许 Web 应用程序使用标识应用程序所需的属性。
- 配置 Web 应用程序以使用其他标识提供程序63

下表介绍了输入的属性：

属性	说明
标识提供程序 URL	可选。标识提供程序服务器的 URL。必须指定完整的 URL 字符串。
服务提供程序 ID	可选。如标识提供程序中定义的域的依赖方信任名称或服务提供程序标识符。
断言签名证书别名	可选。在将标识提供程序断言签名证书导入到用于 SAML 身份验证的信任库文件时指定的别名。 如果更改别名名称，请将相应证书导入每个网关节点上的信任库，然后重新启动节点。
时钟偏差公差	可选。标识提供程序主机系统时钟与主网关节点上系统时钟之间允许的时间差。 可选。系统会根据标识提供程序主机系统时钟设置标识提供程序所颁发的 SAML 令牌的有效期。如果在令牌中设置的开始时间或结束时间与主网关节点系统时钟之间的时间差在指定的秒数内，则标识提供程序颁发的 SAML 令牌的有效期仍未到期。 值必须介于 0 到 600 秒之间。默认值为 120 秒。

下图显示了使 Enterprise Data Catalog 使用 PingFederate 作为标识提供程序的配置：

Edit Ldadmin SAML Configuration

Fields marked with an asterisk (*) are required.

Web Application ID

catalog_service_ldadmin

IDP URL

https://10.70.140.70:9031/idp/startSSO.saml2

Service Provider ID

PingFed_Dev

Assertion Signing Certificate Alias

pingfed_cert

Clock Skew Tolerance

240

?

OK

Cancel

- 单击**确定**。
- 配置应用程序以使用 SAML 标识提供程序之后，重新启动应用程序或应用程序服务。

第 6 章

域安全性

本章包括以下主题：

- [域安全概览, 65](#)
- [域中的安全通信, 66](#)
- [建立与 Web 应用程序服务的安全连接, 75](#)
- [Informatica 域的密码套件, 78](#)
- [安全源和目标, 81](#)
- [安全数据存储, 82](#)
- [应用程序服务和端口, 85](#)

域安全概览

可以启用 Informatica 域中的选项配置域中组件之间以及域和客户端组件之间的安全通信。

可以启用不同选项以保护域中的特定组件。不需要保护域中的所有组件。例如，您可以保护域中的服务之间的通信，但不需要保护模型存储库服务和存储库数据库之间的连接。

Informatica 使用 TCP/IP 和 HTTP 协议在域中的组件之间进行通信。该域使用 SSL 证书来确保组件之间的通信安全。

安装 Informatica 服务时，可以为域中的服务以及 Administrator 工具启用安全通信。安装完成后，可以使用 Administrator 工具或命令行在域中配置安全通信。

在安装过程中，安装程序生成加密密钥来加密存储在域中的敏感数据，例如密码。可以提供安装程序用于生成加密密钥的关键字。安装完成后，可以更改敏感数据的加密密钥。必须升级存储库的内容才能更新加密的数据。

可以在以下几个区域启用安全通信：

域

在域中，您可以选择选项以启用以下组件的安全通信：

- 服务管理器、域中的服务以及 Informatica 客户端工具之间
- 域和域配置存储库之间
- 存储库服务和存储库数据库之间
- PowerCenter 集成服务和 DTM 进程之间

Web 应用程序服务

您可以在 Web 应用程序服务（例如分析服务或 REST 操作 Hub 服务）与浏览器之间建立安全连接。

源和目标

您可以在数据集成服务与 PowerCenter 集成服务之间以及源数据库与目标数据库之间启用安全通信。

数据存储

将数据存储域中时，Informatica 会对敏感数据进行加密，例如密码。Informatica 根据您在安装过程中提供的关键字生成加密密钥。Informatica 使用加密密钥来加密和解密存储在域中的敏感数据。

域中的安全通信

可以使用“安全通信”选项来保护服务之间以及服务与域中的服务管理器之间的连接。此外，您可以为工作流启用安全性，并为您在域中创建的存储库使用安全数据库。

实现安全域之后，配置 Informatica 客户端应用程序使用安全域。

服务和服管理器的安全通信

您可以在安装过程中配置域的安全通信。安装完成后，可以从 Administrator 工具或命令行配置域的安全通信。

Informatica 提供可用于保护域安全的 SSL 证书。但是，对于需要更高级别安全性的域，如生产环境中的域，应提供自定义的 SSL 证书。指定包含要使用的 SSL 证书的密钥库和信任库文件。

注意: Informatica 提供用于评估的 SSL 证书。如果未提供 SSL 证书，Informatica 将对所有 Informatica 安装使用同一默认私钥。域的安全性可能会受到威胁。提供 SSL 证书以确保实现高级别的域安全性。您提供的证书可以是自签名证书或来自证书颁发机构 (CA) 的证书。

配置域的安全通信时，需要保证以下组件之间连接的安全：

- 服务管理器与域中运行的所有服务之间的连接
- 数据集成服务与模型存储库服务之间的连接
- 数据集成服务与工作流进程之间的连接
- PowerCenter 集成服务与 PowerCenter 存储库服务之间的连接
- 域服务与 Informatica 客户端工具和命令行程序之间的连接

在域中实现安全通信的要求

在域中启用安全通信之前，请确保满足以下要求：

已创建了证书签名请求 (CSR) 和私钥。

可以使用 keytool 或 OpenSSL 创建 CSR 和私钥。

如果使用 RSA 加密，必须使用 512 位以上的加密。

具有已签名的 SSL 证书。

证书可以是自签名证书，也可以是 CA 签名证书。Informatica 建议使用 CA 签名证书。

已将证书导入密钥库。

必须具有一个名为 infa_keystore.pem 的 PEM 格式的密钥库和一个名为 infa_keystore.jks 的 JKS 格式的密钥库。

密钥库文件必须包含根和中间 SSL 证书。

注意: JKS 格式的密钥库的密码必须与用于生成 SSL 证书的私钥通行短语相同。

已将证书导入信任库。

必须具有一个名为 `infa_truststore.pem` 且采用 PEM 格式的信任库和一个名为 `infa_truststore.jks` 且采用 JKS 格式的信任库。

信任库文件必须包含根、中间和最终用户 SSL 证书。

密钥库和信任库位于正确的目录中。

如果您在安装过程中启用安全通信，密钥库和信任库必须位于安装程序可访问的目录中。

如果您在安装后启用安全通信，密钥库和信任库必须位于命令行程序可访问的目录中。

有关如何创建自定义密钥库和信任库的详细信息，请参阅 Informatica How-To Library 文章“如何为 Informatica 域中的安全通信创建密钥库和信任库”：

<https://kb.informatica.com/h2l/HowTo%20Library/1/0700-CreateKeystoresAndTruststores-H2L.pdf>

实现安全域之后，配置 Informatica 客户端应用程序使用安全域。

从命令行为域启用安全通信

使用 `infacmd` 和 `infasetup` 命令对域启用安全通信。启用安全通信之后，必须重新启动域以使更改生效。

要使用 SSL 证书文件，请在运行 `infasetup` 命令时指定密钥库文件和信任库文件。

要从命令行配置安全域通信，请使用以下命令：

`infacmd isp UpdateDomainOptions`

使用 `UpdateDomainOptions` 命令可设置域的安全通信模式。

`infasetup UpdateGatewayNode`

使用 `UpdateGatewayNode` 命令可为域中网关节点上的服务管理器启用安全通信。如果域有多个网关节点，请在各网关节点上运行 `UpdateGatewayNode` 命令。

`infasetup UpdateWorkerNode`

使用 `UpdateWorkerNode` 命令可为域中执行工作的节点上的服务管理器启用安全通信。如果域有多个执行工作的节点，请在各个执行工作的节点上运行 `UpdateWorkerNode` 命令。

1. 验证要保护的域是否正在运行。
2. 更新域。

使用所需的选项和参数运行以下命令：

- Windows: `infacmd isp UpdateDomainOptions`
- UNIX: `infacmd.sh isp UpdateDomainOptions`

要为域配置安全通信，请在运行 `infacmd` 命令时包括以下选项：

选项	参数	说明
<code>-DomainOptions</code> <code>-do</code>	<code>option_name=value</code>	设置以下选项来为域配置安全通信： <code>TLSTMode=True</code>

3. 关闭域。
运行 `infasetup` 命令前必须关闭域。
4. 使用所需选项和参数运行 `infasetup`。

输入以下命令：

- Windows：infasetup UpdateGatewayNode 或 infasetup UpdateWorkerNode
- UNIX：infasetup.sh UpdateGatewayNode 或 infasetup.sh UpdateWorkerNode

要在节点上配置安全通信，请运行包含以下选项的命令：

选项	参数	说明
-EnableTLS -tls	enable_tls	为 Informatica 域中的服务配置安全通信。
-NodeKeystore -nk	node_keystore_directory	如果使用 Informatica 提供的默认 SSL 证书，则为可选选项。如果使用自己的 SSL 证书，则为必需选项。包含密钥库文件的目录。Informatica 域需要 PEM 格式和 Java 密钥库 (JKS) 文件形式的 SSL 证书。目录必须包含 PEM 和 JKS 格式的密钥库文件。密钥库文件必须命名为 infa_keystore.jks 和 infa_keystore.pem 多个节点可使用同一密钥库文件。
-NodeKeystorePass -nkp	node_keystore_password	如果使用 Informatica 提供的默认 SSL 证书，则为可选选项。如果使用自己的 SSL 证书，则为必需选项。infa_keystore.jks 文件的密码。
-NodeTruststore -nt	node_truststore_directory	如果使用 Informatica 提供的默认 SSL 证书，则为可选选项。如果使用自己的 SSL 证书，则为必需选项。包含信任库文件的目录。Informatica 域需要 PEM 格式和 Java 密钥库 (JKS) 文件形式的 SSL 证书。目录必须包含 PEM 和 JKS 格式的信任库文件。信任库文件必须命名为 infa_truststore.jks 和 infa_truststore.pem。 多个节点可使用同一信任库文件。
-NodeTruststorePass -ntp	node_truststore_password	如果使用 Informatica 提供的默认 SSL 证书，则为可选选项。如果使用自己的 SSL 证书，则为必需选项。infa_truststore.jks 文件的密码。

5. 在域中的每个节点上运行 infasetup 命令。

如果您在域中有多个网关节点，请在每个网关节点上运行 infasetup UpdateGatewayNode。如果您有多个执行工作的节点，请在每个执行工作的节点上运行 infasetup UpdateWorkerNode。必须对域中的所有节点使用相同的密钥库和信任库文件。

6. 重新启动域。

域中所有节点更新完成后，必须更新托管 Informatica 客户端工具的计算机。在 Informatica 信任库环境变量中设置 SSL 证书的位置。

在 Administrator 工具中对域启用安全通信

您可以使用 Administrator 工具为该域启用安全通信。在 Administrator 工具中启用安全通信时，您还必须运行 infasetup 命令以更新节点。

在 Administrator 工具中启用“安全通信”选项时，您还需要运行 infasetup 命令来更新各个节点上的 Informatica 配置文件。要指定所用的 SSL 证书文件，请在运行 infasetup 命令时指定密钥库和信任库文件。

要更新各节点上的 Informatica 配置文件，请使用以下命令：

infasetup UpdateGatewayNode

使用 UpdateGatewayNode 命令可为域中网关节点上的服务管理器启用安全通信。如果域有多个网关节点，请在各网关节点上运行 UpdateGatewayNode 命令。

infasetup UpdateWorkerNode

使用 UpdateWorkerNode 命令可为域中执行工作的节点上的服务管理器启用安全通信。如果域有多个执行工作的节点，请在各个执行工作的节点上运行 UpdateWorkerNode 命令。

要通过 Administrator 工具启用安全域通信，请执行以下步骤：

1. 在 Administrator 工具中，选择域。
2. 在内容面板中，单击**属性**视图。
3. 转到**常规属性**部分，然后单击**编辑**。
4. 在**编辑常规属性**窗口中，选择**启用安全通信**。
5. 单击**确定**
6. 关闭域。

运行 infasetup 命令前必须关闭域。

7. 使用所需选项和参数运行 infasetup。

输入以下命令：

- Windows: infasetup UpdateGatewayNode 或 infasetup UpdateWorkerNode
- UNIX: infasetup.sh UpdateGatewayNode 或 infasetup.sh UpdateWorkerNode

要在节点上配置安全通信，请运行包含以下选项的命令：

选项	参数	说明
-EnableTLS -tls	enable_tls	为 Informatica 域中的服务配置安全通信。
-NodeKeystore -nk	node_keystore_directory	如果使用 Informatica 提供的默认 SSL 证书，则为可选选项。如果使用自己的 SSL 证书，则为必需选项。包含密钥库文件的目录。Informatica 域需要 PEM 格式和 Java 密钥库 (JKS) 文件形式的 SSL 证书。目录必须包含 PEM 和 JKS 格式的密钥库文件。密钥库文件必须命名为 infa_keystore.jks 和 infa_keystore.pem 多个节点可使用同一密钥库文件。
-NodeKeystorePass -nkp	node_keystore_password	如果使用 Informatica 提供的默认 SSL 证书，则为可选选项。如果使用自己的 SSL 证书，则为必需选项。infa_keystore.jks 文件的密码。

选项	参数	说明
-NodeTruststore -nt	node_truststore_directory	如果使用 Informatica 提供的默认 SSL 证书，则为可选选项。如果使用自己的 SSL 证书，则为必需选项。包含信任库文件的目录。Informatica 域需要 PEM 格式和 Java 密钥库 (JKS) 文件形式的 SSL 证书。目录必须包含 PEM 和 JKS 格式的信任库文件。信任库文件必须命名为 infa_truststore.jks 和 infa_truststore.pem。多个节点可使用同一信任库文件。
-NodeTruststorePass -ntp	node_truststore_password	如果使用 Informatica 提供的默认 SSL 证书，则为可选选项。如果使用自己的 SSL 证书，则为必需选项。infa_truststore.jks 文件的密码。

8. 在域中的每个节点上运行 infasetup 命令。

如果您在域中有多个网关节点，请在每个网关节点上运行 infasetup UpdateGatewayNode。如果您有多个执行工作的节点，请在每个执行工作的节点上运行 infasetup UpdateWorkerNode。必须对域中的所有节点使用相同的密钥库和信任库文件。

9. 重新启动域。

域中所有节点更新完成后，必须更新托管 Informatica 客户端工具的计算机。在 Informatica 信任库环境变量中设置 SSL 证书的位置。

配置 Informatica 客户端应用程序以使用安全域

在域中启用安全通信时，域和 Informatica 客户端应用程序（如 Developer tool）之间的连接也会得到保护。您可能需要在环境变量中指定用于保护域的信任库文件的位置和密码。可以在托管客户端应用程序（访问域中的服务）的计算机上设置环境变量。

用于保护 Informatica 域的 SSL 证书包含在名为 infa_truststore.jks 和 infa_truststore.pem 的信任库文件中。信任库文件必须在每个客户端主机上可用。

可能需要在每个客户端主机上设置以下环境变量：
INFA_TRUSTSTORE

将此变量设置为包含 infa_truststore.jks 和 infa_truststore.pem 信任库文件的目录。

INFA_TRUSTSTORE_PASSWORD

将此变量设置为信任库的密码。必须加密密码。使用命令程序 pmpasswd 加密密码。

Informatica 在默认信任库文件中提供 SSL 证书，您可以使用该证书来保护域。在安装 Informatica 客户端时，安装程序会设置环境变量并默认在以下目录中安装信任库文件：<Informatica 安装目录>\clients\shared\security

如果使用默认的 Informatica SSL 证书，并且 infa_truststore.jks 和 infa_truststore.pem 文件位于默认目录中，则不需要设置 INFA_TRUSTSTORE 或 INFA_TRUSTSTORE_PASSWORD 环境变量。

在以下情况下，必须在每个客户端主机上设置 INFA_TRUSTSTORE 和 INFA_TRUSTSTORE_PASSWORD 环境变量：

使用自定义 SSL 证书来保护域。

如果您提供 SSL 证书以用于保护域，请将证书导入到名为 infa_truststore.jks 和 infa_truststore.pem 的信任库文件，然后将信任库文件复制到每个客户端主机。必须指定文件位置和信任库密码。

重要说明：如果要将处理推送到一个计算群集且数据集成服务运行在网络上，请一次导入多个证书然后将它们复制到网络上的每个数据集成服务中。每次导入一个证书时，证书内容相同，但十六进制值不同。因此，在网络上运行的并发映射会因初始化错误而失败。

将默认目录中的默认 Informatica 信任库文件替换为自己的信任库文件。

如果将默认 Informatica 目录中的默认 `infa_truststore.jks` 和 `infa_truststore.pem` 信任库文件替换为自己的信任库文件，则必须指定信任库密码。信任库文件必须具有与默认信任库文件相同的文件名。

使用默认的 Informatica SSL 证书，但信任库文件不位于默认的 Informatica 目录中。

如果使用默认的 Informatica SSL 证书，但默认 `infa_truststore.jks` 和 `infa_truststore.pem` 信任库文件不位于默认目录中，则必须指定文件位置和信任库密码。

安全域配置存储库数据库

Informatica 域配置存储库存储配置信息以及用户帐户特权和权限。创建 Informatica 域时，必须创建域配置存储库。

可以在使用 SSL 协议进行安全保护的数据库上创建域配置存储库。SSL 协议使用信任库文件中存储的 SSL 证书。访问安全数据库需要使用包含数据库证书的信任库。

可以在安装 Informatica 服务并创建域时创建安全域配置存储库数据库。有关在安装过程中配置安全域配置存储库的详细信息，请参阅《Informatica 安装指南》。

安装后，可以从命令行配置安全域配置存储库数据库。

注意：在安装后配置安全域配置存储库数据库之前，必须为域启用安全通信。

可以在以下数据库上创建安全域配置存储库：

- Oracle
- Microsoft SQL Server
- IBM DB2

配置安全域配置存储库数据库

安装后，可以将域配置存储库更改为安全数据库。仅当为域启用安全通信时，才可以使用安全域配置存储库数据库。

在更改域配置存储库数据库之前，必须先关闭域。使用 `infasetup` 命令备份域配置存储库数据库并在安全数据库中进行还原。在安全数据库中还原域配置存储库时，为安全数据库指定安全参数。然后，使用域配置存储库信息更新网关节点。

要备份和还原存储库数据库及更新网关节点，请使用以下命令：

`infasetup BackupDomain`

使用 `BackupDomain` 选项可从域配置存储库数据库备份数据。

`infasetup RestoreDomain`

使用 `RestoreDomain` 选项可将域配置存储库数据还原到安全数据库。

`infasetup UpdateGatewayNode`

使用 `UpdateGatewayNode` 选项可在域的网关节点中更新域配置存储库设置。

要将域配置存储库更改为安全数据库，请完成以下步骤：

1. 验证是否已为域启用安全通信。
域必须是安全的，才能为域配置存储库使用安全数据库。
2. 关闭域。
3. 运行 `infasetup BackupDomain` 命令，并指定数据库连接信息。
运行 `BackupDomain` 命令时，`infasetup` 会将大多数域配置数据库表备份到您指定的文件名。

注意: 如果 infasetup 备份或还原命令因发生 Java 内存错误而失败, 请增加 infasetup 可用的系统内存。要增加系统内存, 请设置 INFA_JAVA_CMD_OPTS 环境变量中的 -Xmx 值。

4. 使用数据库备份实用程序手动备份 infasetup 命令未备份的其他存储库表。

备份下表的内容:

- ISP_RUN_LOG

5. 要在安全数据库中还原域配置存储库, 请运行 infasetup RestoreDomain 命令并指定数据库连接信息。

除连接信息之外, 还要指定安全数据库所需的以下选项:

选项	参数	说明
-DatabaseTlsEnabled -dbtls	database_tls_enabled	必需。指示域配置存储库将还原到的数据库是否是安全数据库。将此选项设置为 True。
-DatabaseTruststoreLocation -dbtl	database_truststore_location	必需。包含数据库 SSL 证书的信任库文件的路径和文件名。
-DatabaseTruststorePassword -dbtp	database_truststore_password	必需。安全数据库的数据库信任库文件的密码。

在连接字符串中, 包含以下安全参数:

EncryptionMethod

必需。指示数据在通过网络传送时是否进行了加密。该参数必须设置为 SSL。

ValidateServerCertificate

可选。指示 Informatica 是否验证数据库服务器发送的证书。

如果该参数设置为 True, 则 Informatica 将验证数据库服务器发送的证书。如果指定 HostNameInCertificate 参数, Informatica 还会验证证书中的主机名。

如果该参数设置为 False, 则 Informatica 不会验证数据库服务器发送的证书。Informatica 将忽略您指定的任何信任库信息。

默认值为 True。

HostNameInCertificate

可选。托管安全数据库的计算机的主机名。如果指定主机名, Informatica 将根据 SSL 证书中的主机名来验证连接字符串中包含的主机名。

cryptoProtocolVersion

必需。指定连接到安全数据库要使用的加密协议。可以根据数据库服务器所使用的加密协议将参数设置为 cryptoProtocolVersion=TLSv1.1 或 cryptoProtocolVersion=TLSv1.2。

6. 使用数据库还原实用程序还原已手动备份的存储库表。

还原下表:

- ISP_RUN_LOG

7. 要使用安全域配置存储库的相关信息更新域中的节点, 请运行 infasetup UpdateGatewayNode 命令并指定安全数据库连接信息。

除节点选项之外，还要指定安全数据库所需的以下选项：

选项	参数	说明
-DatabaseTlsEnabled -dbtls	database_tls_enabled	必需。指示用于域配置存储库的数据库是安全数据库。将此选项设置为 True。
- DatabaseConnectionString -cs	database_connection_string	必需。用于连接到安全数据库的连接字符串。连接字符串必须包含在步骤 5 中运行 infasetup RestoreDomain 命令时包含到连接字符串中的安全参数。
- DatabaseTruststorePassword -dbtp	database_truststore_password	必需。安全数据库的数据库信任库文件的密码。

如果您在域中有多个网关节点，请在每个网关节点上运行 infasetup UpdateGatewayNode。

8. 重新启动域。

安全的 PowerCenter 存储库数据库

当您创建 PowerCenter 存储库服务时，可以在通过 SSL 协议进行安全保护的数据库中创建创建关联的 PowerCenter 存储库。

PowerCenter 存储库服务通过本地连接连接到 PowerCenter 存储库数据库。

当您在安全数据库中创建 PowerCenter 存储库时，请验证数据库客户端文件是否包含数据库的安全连接信息。例如，如果您在安全的 Oracle 数据库中创建 PowerCenter 存储库，请使用安全连接信息配置 Oracle 数据库 tnsnames.ora 和 sqlnet.ora 客户端文件。

安全模型存储库数据库

当您创建模型存储库服务时，可以在通过 SSL 协议进行安全保护的数据库中创建创建关联的模型存储库。

模型存储库服务通过 JDBC 驱动程序连接到模型存储库数据库。

1. 设置通过 SSL 协议进行安全保护的数据库。
2. 在 Administrator 工具中，创建模型存储库服务。
3. 在 **新建模型存储库服务** 对话框中，输入模型存储库服务的常规属性并单击 **下一步**。
4. 输入模型存储库服务的数据库属性和 JDBC 连接字符串。

要连接到安全数据库，请在 **安全 JDBC 参数** 字段中输入安全数据库参数。Informatica 将 **安全 JDBC 参数** 字段的值视为敏感数据，并以加密的方式存储该参数字符串。

下表介绍了安全数据库参数：

EncryptionMethod

必需。指示数据在通过网络传送时是否进行了加密。该参数必须设置为 SSL。

ValidateServerCertificate

可选。指示 Informatica 是否验证数据库服务器发送的证书。

如果该参数设置为 True，则 Informatica 将验证数据库服务器发送的证书。如果指定 HostNameInCertificate 参数，Informatica 还会验证证书中的主机名。

如果该参数设置为 False，则 Informatica 不会验证数据库服务器发送的证书。Informatica 将忽略您指定的任何信任库信息。

默认值为 True。

HostNameInCertificate

可选。托管安全数据库的计算机的主机名。如果指定主机名，Informatica 将根据 SSL 证书中的主机名来验证连接字符串中包含的主机名。

cryptoProtocolVersion

必需。指定连接到安全数据库要使用的加密协议。可以根据数据库服务器所使用的加密协议将参数设置为 cryptoProtocolVersion=TLSv1.1 或 cryptoProtocolVersion=TLSv1.2。

TrustStore

必需。包含数据库 SSL 证书的信任库文件的路径和文件名。

如果不包括信任库文件的路径，Informatica 将在以下默认目录中查找文件：<Informatica 安装目录>/tomcat/bin

TrustStorePassword

必需。安全数据库的信任库文件的密码。

注意: Informatica 会将安全 JDBC 参数附加到 JDBC 连接字符串。如果将安全 JDBC 参数直接附加到该连接字符串，那么请勿在**安全 JDBC 参数**字段中输入任何参数。

5. 测试该连接以验证安全存储库数据库连接是否有效。
6. 完成该过程以创建模型存储库服务。

工作流和会话的安全通信

默认情况下，当您启用域的安全通信选项时，Informatica 将保护数据集成服务和 PowerCenter 集成服务与 DTM 进程之间的连接。

此外，如果在网络上运行 PowerCenter 会话，您可以启用选项来保护 DTM 进程之间的数据通信安全。

要启用 PowerCenter 会话中 DTM 进程之间的安全数据通信，请选择 PowerCenter 集成服务的**启用数据加密**选项。

注意: 当 DTM 进程在安全模式下运行时，PowerCenter 会话需要更多 CPU 和内存。在启用 PowerCenter 会话的 DTM 进程之间的安全数据通信之前，请确定域资源是否足以承担额外负载。

为 PowerCenter DTM 进程启用安全通信

要保护在网络上运行的 PowerCenter 会话中的 DTM 进程之间连接的安全，请将 PowerCenter 集成服务配置为对 DTM 进程启用数据加密。

1. 在 Administrator 工具的导航器中，选择“PowerCenter 集成服务”。
2. 在内容面板中，单击“属性”视图。
3. 转到“PowerCenter 集成服务属性”部分，然后单击“编辑”。
4. 在**编辑 PowerCenter 集成服务属性**窗口中，选择**启用数据加密**。
5. 单击**确定**。

如果在网络上运行 PowerCenter 会话，这些 DTM 进程将在与其他 DTM 进程通信时发送加密数据。

建立与 Web 应用程序服务的安全连接

为了保护 Web 应用程序服务与浏览器之间传输的数据，需要在 Web 应用程序服务与浏览器之间建立安全连接。

您可以为以下连接建立安全连接：

与 Administrator 工具的连接

您可以在 Administrator 工具与浏览器之间建立安全连接。

与 Web 应用程序服务的连接

您可以在以下 Web 应用程序服务与浏览器之间建立安全连接：

- 分析服务
- Metadata Manager 服务
- REST 操作 Hub 服务
- Test Data Manager 服务
- Web 服务中心控制台服务

建立与 Web 应用程序服务的安全连接的要求

在建立与 Web 应用程序服务的安全连接之前，请确保满足以下要求：

已创建了证书签名请求 (CSR) 和私钥。

可以使用 keytool 或 OpenSSL 创建 CSR 和私钥。

如果使用 RSA 加密，必须使用 512 位以上的加密。

具有已签名的 SSL 证书。

证书可以是自签名证书，也可以是 CA 签名证书。Informatica 建议使用 CA 签名证书。

已将证书导入 JKS 格式的密钥库。

一个密钥库只能包含一个证书。如果您为每个 Web 应用程序服务使用一个唯一证书，请为每个证书创建一个单独的密钥库。或者，也可以使用共享的证书和密钥库。

如果您为 Administrator 工具使用安装程序生成的 SSL 证书，则不需要将证书导入 JKS 格式的密钥库。

密钥库位于可访问的目录中。

密钥库必须位于 Administrator 工具和命令行程序可访问的目录中。

启用与 Administrator 工具的安全连接

安装完成后，您可以通过命令行配置与 Administrator 工具的安全连接。

必须使用浏览器与 Informatica Administrator 服务之间安全连接的属性更新域中的网关节点。

要使用安全连接属性更新网关节点，请运行以下命令：infasetup UpdateGatewayNode

包含以下选项：

选项	参数	说明
-HttpsPort -hs	AdminConsole_https_port	与 Informatica Administrator 服务安全连接要使用的端口号。
-KeystoreFile -kf	AdminConsole_Keystore_File	通过 HTTPS 连接到 Informatica Administrator 服务要使用的密钥库文件的路径和文件名。
-KeystorePass -kp	AdminConsole_Keystore_Password	密钥库文件的密码。

如果您的域中包含多个网关节点，请在每个网关节点上运行此命令。

Informatica Web 应用程序服务

创建或配置 Web 应用程序服务时，为其配置一个安全连接。每种应用程序服务都具有特定的安全 HTTPS 连接属性。

Analyst 工具的安全

当您创建分析服务时，可以为 Analyst 工具配置安全 HTTPS 属性。

为了保护浏览器和分析服务之间的连接，请配置以下分析服务属性：

属性	说明
启用安全通信	选择此项可启用 Analyst 工具和分析服务之间的安全连接。
HTTPS 端口	启用传输层安全 (TLS) 协议时，运行 Informatica Analyst Web 应用程序的端口号。请使用与 HTTP 端口号不同的端口号。
密钥库文件	包含数字证书的密钥库文件存储的目录。
密钥库密码	密钥库文件的纯文本密码。如果未设置此属性，分析服务将使用默认密码 <i>changeit</i> 。
SSL 协议	Informatica 建议将此字段留空。启用的 TLS 的版本取决于该值。空字段将启用可用的最高版本的 TLS。如果您输入了值，则可能启用早期版本的 TLS。具体行为取决于环境的 Java 版本。 有关详细信息，请参阅 Java 版本对应的文档。

REST 操作 Hub 服务的安全

使用 REST 操作 Hub 服务时，可以为 REST 操作 Hub 配置安全 HTTPS 属性。

要在浏览器与 REST 操作 Hub 服务之间建立安全连接，请配置以下 REST 操作 Hub 服务属性：

属性	说明
HTTP 端口	REST 操作 Hub 服务使用 HTTP 协议时，该服务进程的唯一 HTTP 端口号。默认值为 6555。
HTTPS 端口	启用传输层安全 (TLS) 协议时，运行 REST 操作 Hub 服务的端口号。请使用与 HTTP 端口号不同的端口号。
启用传输层安全	选择以启用 REST 操作 Hub 服务和 REST 客户端之间的安全连接。
密钥库文件	包含数字证书的密钥库文件存储的目录。
密钥库密码	密钥库文件的纯文本密码。如果未设置该属性，则 REST 操作 Hub 服务使用默认密码。
SSL 协议	空白字段可启用 TLS 的最高版本。启用的 TLS 的版本取决于该值。如果您输入了值，则可能启用早期版本的 TLS。具体行为取决于环境的 Java 版本。有关详细信息，请参阅 Java 版本对应的文档。

Web 服务中心控制台的安全

创建 Web 服务中心服务时，可以配置 Web 服务中心控制台的安全 HTTPS 属性。

要保护浏览器与 Web 服务中心服务之间连接的安全，请配置以下 Web 服务中心服务属性：

属性	说明
URLScheme	指示为 Web 服务中心配置的安全协议： <ul style="list-style-type: none">- HTTP。仅在 HTTP 上运行 Web 服务中心。- HTTPS。仅在 HTTPS 上运行 Web 服务中心。- HTTP 和 HTTPS。在 HTTP 和 HTTPS 模式下运行 Web 服务中心。
HubPortNumber (https)	HTTPS 上的 Web 服务中心的端口号。当选择的 URL 架构包括 HTTPS 时显示。如果选择在 HTTPS 上运行 Web 服务中心，则需要。默认值为 7343。
密钥库文件	包含 HTTPS 连接所需的密钥和证书的密钥库文件的路径和文件名。
密钥库密码	密钥库文件的密码。如果未设置此属性，Web 服务中心将使用默认密码 <i>changeit</i> 。

Metadata Manager 的安全

创建 Metadata Manager 服务时，您可以为 Metadata Manager Web 应用程序配置安全 HTTPS 属性。

要提高浏览器和 Metadata Manager 服务间连接的安全性，请配置以下 Metadata Manager 服务属性：

属性	说明
启用安全套接字层	表示您要为 Metadata Manager Web 应用程序配置安全连接。 注意: 创建 Metadata Manager 服务时，会显示此属性。要为现有 Metadata Manager 服务建立安全连接，请将 URL 架构 配置属性设置为 HTTPS。
端口号	Metadata Manager 应用程序运行时使用的端口号。默认值为 10250。
密钥库文件	包含为 Metadata Manager Web 应用程序配置安全连接时所需的密钥和证书的密钥库文件。 注意: Metadata Manager 服务使用 RSA 加密。因此，Informatica 建议使用通过 RSA 算法生成的安全证书。
密钥库密码	密钥库文件的密码。

Informatica 域的密码套件

您可以配置 Informatica 域在加密域中连接时所使用的密码套件。密码套件配置不会影响从 Informatica 域到该域外部资源的连接。

当为 Informatica 域启用安全通信或与 Web 应用程序服务的安全连接时，Informatica 域会使用密码套件对流量进行加密。

Informatica 根据以下列表创建要使用的密码套件有效列表：

黑名单

希望 Informatica 域阻止的密码套件列表。在将某个密码套件加入黑名单后，Informatica 域会将该密码套件从有效列表中删除。您可将默认列表中的密码套件添加到黑名单。

默认列表

默认情况下 Informatica 域支持的密码套件列表。如果未配置白名单或黑名单，Informatica 域会使用默认列表作为有效列表。

有关详细信息，请参阅 [“密码套件默认列表” 页面上 79](#)。

白名单

希望 Informatica 域支持的密码套件列表。在将某个密码套件加入白名单后，Informatica 域会将该密码套件添加到有效列表。您无需将默认列表中的密码套件添加到白名单。

Informatica 创建有效列表的方法是，将白名单中的密码套件添加到默认列表，并从默认列表中删除黑名单中的密码套件。

对于有效列表，请考虑以下准则：

- 要使用自定义有效列表安全连接到 Web 客户端，Informatica 域必须在域中使用安全通信。如果域未使用安全通信，则 Informatica 使用默认列表作为有效列表。
- 有效列表只管理 Informatica 域中的连接。数据源连接不使用有效列表。
- 有效列表必须至少包含一个 TLS v1.1 或 1.2 支持的密码套件。
- 有效列表必须是对 Windows、Java 运行时环境和 OpenSSL 有效的密码套件。

创建密码套件列表

要将 Informatica 域配置为使用特定密码套件，请创建一个白名单以指定要支持的其他密码套件。还可以创建一个黑名单以指定要阻止的密码套件。

请与网络安全管理员一起确定适用于 Informatica 域的密码套件。

密码套件列表必须是以逗号分隔的列表。为列表中密码套件使用 Internet 编号分配机构 (IANA) 名称。或者，您也可以使用 Java 正则表达式。

可以使用 `infasetup` 命令配置白名单和黑名单。可以直接在命令参数中提供列表，也可指定包含逗号分隔列表的纯文本文件。

以下示例文本显示了包含两个密码套件的列表：

```
TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

可在创建 Informatica 域时为其配置密码套件白名单和黑名单。使用 `infasetup` 命令可创建 Informatica 域、网关节点和执行工作的节点。有关 `infasetup` 命令的详细信息，请参阅《*Informatica 命令参考*》。

或者，您也可以为现有 Informatica 域配置白名单和黑名单。

密码套件默认列表

默认情况下，Informatica 域对域中的安全通信和安全客户端连接使用以下密码套件：

- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA256

为 Informatica 域配置新的密码套件有效列表

要配置 Informatica 域使用的密码套件，您必须使用相同的白名单和黑名单更新 Informatica 域、所有网关节点和所有执行工作的节点。

注意: 对黑名单、白名单和有效列表所做的更改不会累积。运行命令时，Informatica 会根据黑名单、默认列表和白名单创建一个新的有效列表。该新的有效列表会覆盖先前的列表。

要为现有 Informatica 域配置新的密码套件有效列表，请执行以下步骤：

1. 关闭 Informatica 域。
2. （可选）运行 `infasetup listDomainCiphers` 命令，以查看域/节点支持或阻止的密码套件列表。

例如，运行以下命令以查看所有密码套件列表：

```
infasetup listDomainCiphers -l ALL -dc true
```

3. 在网关节点上运行 `infasetup updateDomainCiphers` 命令，并指定白名单、黑名单或二者。

例如，运行以下命令，以在有效列表中添加一个密码套件并删除两个密码套件：

```
infasetup updateDomainCiphers -cwl TLS_DHE_DSS_WITH_AES_128_CBC_SHA -cbl  
TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

4. 在每个网关节点上运行 `infasetup updateGatewayNode` 命令，并指定白名单、黑名单或二者。

使用与域相同的白名单和黑名单。

例如，运行以下命令：

```
infasetup updateGatewayNode -cwl TLS_DHE_DSS_WITH_AES_128_CBC_SHA -cbl  
TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

5. 使用与 Informatica 域相同的密码套件集更新每个执行工作的节点。

使用与域相同的白名单和黑名单。

例如，运行以下命令：

```
infasetup updateWorkerNode -cwl TLS_DHE_DSS_WITH_AES_128_CBC_SHA -cbl  
TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

6. 启动 Informatica 域。
7. （可选）运行 `infacmd isp listDomainCiphers` 命令，以查看域或节点使用的密码套件列表。

例如，运行以下命令以查看域使用的密码套件有效列表：

```
infacmd isp listDomainCiphers -l EFFECTIVE
```


安全源和目标

Informatica 使用连接对象连接到关系数据库作为源或目标。您可以创建到通过 SSL 证书进行安全保护的关系数据库的连接对象。

您在 Workflow Manager 中创建 PowerCenter 连接对象。在 Developer tool 或 Administrator 工具中创建 Data Service、Data Quality 或剖析连接。

可以在以下数据库中创建与安全的源或目标的连接：

- Oracle
- Microsoft SQL Server
- IBM DB2

数据集成服务源和目标

创建连接对象以供数据集成服务来处理映射、数据配置文件、结果卡或 SQL 数据服务时，您可以定义与通过 SSL 协议进行安全保护的数据库的连接。

数据集成服务通过 JDBC 驱动程序连接到源数据库或目标数据库。当您配置到安全存储库数据库的连接时，必须在 JDBC 连接字符串中包含安全连接参数。

1. 设置通过 SSL 协议进行安全保护的数据库来用作源或目标。
2. 在 Administrator 工具中创建连接。
3. 在 **新建连接** 对话框中，选择连接类型，然后单击 **确定**。
您可以创建与安全 DB2、Microsoft SQL Server 或 Oracle 数据库的连接。
4. 在 **新建连接 - 第 1 步(共 3 步)** 对话框中，输入该连接的属性，然后单击 **下一步**。
5. 在 **新建连接 - 第 2 步(共 3 步)** 页面中，输入数据库的连接字符串。

要连接到安全数据库，请在 **高级 JDBC 安全选项** 字段中输入安全数据库参数。Informatica 将 **高级 JDBC 安全选项** 字段的值视为敏感数据，并以加密的方式存储该参数字符串。

下表介绍了安全数据库参数：

EncryptionMethod

必需。指示数据在通过网络传送时是否进行了加密。该参数必须设置为 SSL。

ValidateServerCertificate

可选。指示 Informatica 是否验证数据库服务器发送的证书。

如果该参数设置为 True，则 Informatica 将验证数据库服务器发送的证书。如果指定 HostNameInCertificate 参数，Informatica 还会验证证书中的主机名。

如果该参数设置为 False，则 Informatica 不会验证数据库服务器发送的证书。Informatica 将忽略您指定的任何信任库信息。

默认值为 True。

HostNameInCertificate

可选。托管安全数据库的计算机的主机名。如果指定主机名，Informatica 将根据 SSL 证书中的主机名来验证连接字符串中包含的主机名。

TrustStore

必需。包含数据库 SSL 证书的信任库文件的路径和文件名。

TrustStorePassword

必需。安全数据库的信任库文件的密码。

注意: Informatica 会将安全的 JDBC 参数附加到该连接字符串。如果将安全的 JDBC 参数直接附加到该连接字符串, 那么请勿在**高级 JDBC 安全选项**字段中输入任何参数。

6. 测试该连接以验证安全数据库连接是否有效。
7. 完成该过程以创建关系连接。

PowerCenter 源和目标

创建 PowerCenter 会话的连接对象时, 您可以使用 SSL 协议定义与安全数据库的连接。

可通过本地连接或 ODBC 驱动程序连接到关系 PowerCenter 源和目标。

如果通过本地连接连接到安全关系源或目标, 请验证数据库客户端是否包含安全数据库的连接信息。例如, 如果连接到安全 Oracle 数据库上的 PowerCenter 目标, 请使用安全数据库的连接信息配置 Oracle 数据库客户端文件 *tnsnames.ora*。

如果通过 ODBC 驱动程序连接到安全关系源或目标, 请验证数据库客户端是否包含安全数据库的连接信息, 并验证 ODBC 数据源是否正确定义了与安全数据库的连接。

安全数据存储

在将数据存储在域配置存储库中之前, Informatica 会对敏感数据进行加密, 如密码和安全连接参数。Informatica 使用您提供的关键字来创建用于加密敏感数据的加密密钥。

在安装期间, 您必须提供关键字, 以便安装程序使用该关键字来生成域的加密密钥。一个域中的所有节点必须使用相同的加密密钥。如果您在多个节点上安装, 安装程序将为域中的所有节点使用相同的加密密钥。有关在安装期间生成域的加密密钥的详细信息, 请参阅 Informatica 安装指南。

安装完成后, 您可以更改域的加密密钥。运行 `infasetup` 命令可生成加密密钥并更改域的加密密钥。更改域的加密密钥后, 必须升级域中存储库的内容才能更新加密的数据。

注意: 必须将域的名称、加密密钥的关键字以及加密密钥文件保存在一个安全位置。更改域的加密密钥或将存储库移动到另一个域时, 需要提供域名、关键字和加密密钥。如果丢失了加密密钥文件, 则需要关键字来重新生成加密密钥。如果丢失了关键字和加密密钥, 则无法更改域的加密密钥或将存储库移动到另一个域。

UNIX 上的安全目录

当您安装 Informatica 时, 安装程序会创建目录来存储需要限制访问的 Informatica 文件, 如域加密密钥文件。在 UNIX 上, 安装程序将为目录和目录中的文件分配不同的权限。

默认情况下, 安装程序会在 Informatica 安装目录内创建以下目录来存储加密密钥: `<INFA_HOME>/isp/config/keys`
`/keys` 目录中包含节点的加密密钥文件。如果将域域配置为使用 Kerberos 身份验证, 该目录还包含 Kerberos keytab 文件。

在安装期间, 您可以指定其他目录来存储加密文件。安装程序会为指定目录分配与默认目录相同的权限。

`/keys` 目录和目录中的文件具有以下权限:

目录权限

目录所有者具有针对该目录的 `-wx` 权限, 但没有 `r` 权限。目录所有者是用于运行安装程序的用户帐户。所有者所属的组也具有针对该目录的 `-wx` 权限, 但没有 `r` 权限。

例如，用户帐户 *ediqa* 拥有该目录并属于 *infaadmin* 组。*ediqa* 用户帐户和 *infaadmin* 组具有以下权限：-
WX-WX---

ediqa 用户帐户和 *infaadmin* 组可以写入和运行目录中的文件。它们不能在目录中显示文件列表，但可以按名称列出特定文件。

如果您知道目录中文件的名称，则可以将该文件从目录中复制到其他位置。如果您不知道文件的名称，则必须更改目录的权限以包含读取权限，然后才能复制该文件。可以使用 `chmod 730` 命令向目录和子目录的所有者授予读取权限。

例如，您需要将名为 *siteKey* 的加密密钥文件复制到临时目录，以使域中的其他节点可以访问该文件。运行 `<Informatica 安装目录>/isp/config` 目录上的 `chmod 730` 命令可分配以下权限：`rwX-wX---`。然后可以将加密密钥文件从 `/keys` 子目录复制到其他目录中。

完成复制文件后，将目录的权限改回写入和执行权限。可以使用 `chmod 330` 命令删除读取权限。

注意：请勿使用 `-R` 选项以递归方式更改目录和文件的权限。目录和目录中的文件具有不同的权限。

文件权限

目录中文件的所有者具有对文件的 `rwX` 权限。目录中文件的所有者是用于运行安装程序的用户帐户。所有者所属的组也具有对目录中文件的 `rwX` 权限。

所有者和组具有对文件的完全访问权限，并且可以显示或编辑目录中的文件。

注意：必须知道文件的名称才能列出或编辑文件。

从命令行更改加密密钥

安装后，可以从命令行更改域的加密密钥。必须先关闭该域，然后再更改加密密钥。

使用 `infasetup` 命令生成加密密钥，并将域配置为使用新加密密钥。

以下 `infasetup` 命令可生成并更改加密密钥：

`generateEncryptionKey`

在名为 *sitekey* 的文件中生成加密密钥。如果为加密密钥指定的目录中包含名为 *sitekey* 的文件，则 Informatica 会将此文件重命名为 *siteKey_old*。

`migrateEncryptionKey`

更改用于将敏感数据存储在 Informatica 域中的加密密钥。

要更改域的加密密钥，请完成以下步骤：

1. 关闭域。
2. 请先备份该域，然后再更改加密密钥。
要确保可以在更改加密密钥的过程中遇到问题时恢复域，请先备份该域，然后再运行 `infasetup` 命令。
3. 要为域生成加密密钥，请运行 `infasetup generateEncryptionKey` 命令。

指定生成加密密钥所需的以下选项：

选项	参数	说明
-keyword -kw	关键字	用作生成加密密钥的基础字的文本字符串。 关键字必须满足以下条件： - 长度为 8 到 20 个字符 - 至少包含一个大写字母 - 至少包含一个小写字母 - 至少包含一个数字 - 不包含空格
-domainName -dn	domain_name	Informatica 域名。
-encryptionKeyLocation -kl	encryption_key_location	包含当前加密密钥的目录。加密文件的名称为 <i>sitekey</i> 。 Informatica 将当前的 <i>sitekey</i> 文件重命名为 <i>sitekey_old</i> ，并在同一目录下名为 <i>sitekey</i> 的新文件中生成加密密钥。

- 要更改域的加密密钥，请运行 `infasetup migrateEncryptionKey` 命令并指定旧加密密钥和新加密密钥的位置。

指定更改域的加密密钥所需的以下选项：

选项	参数	说明
-LocationOfEncryptionKeys -loc	location_of_encryption_keys	存储旧加密密钥文件（名为 <i>siteKey_old</i> ）和新加密密钥文件（名为 <i>siteKey</i> ）的目录。 该目录必须同时包含旧加密密钥文件和新加密密钥文件。如果旧加密密钥文件和新加密密钥文件存储在不同的目录中，请将两个加密密钥文件复制到同一目录中。 如果域包含多个节点，此目录必须对运行 <code>migrateEncryptionKey</code> 命令的域中的任何节点均可访问。 注意： 在 UNIX 上，文件名 <i>siteKey_old</i> 区分大小写。如果手动重命名先前的加密密钥文件，请验证文件名的字母大小写是否正确。
-IsDomainMigrated -mig	is_domain_migrated	指示是否已更新域以使用最新的加密密钥。 当首次运行 <code>migrateEncryptionKey</code> 命令时，请将此选项设置为 <code>False</code> 以指示该域使用旧加密密钥。 首次运行之后，当运行 <code>migrateEncryptionKey</code> 命令更新域中的其他节点时，请将此选项设置为 <code>True</code> 以指示该域已更新，可以使用最新的加密密钥。或者，也可以运行不带此选项的 <code>migrateEncryptionKey</code> 命令。 默认值为 <code>True</code> 。

5. 在域中的每个节点上运行 `infasetup` 命令。
如果域具有多个节点，请在每个节点上运行 `infasetup migrateEncryptionKey`。请先对网关节点运行此命令，然后再对执行工作的节点运行此命令。在首次运行此命令后，可以忽略 `IsDomainMigrated` 选项。
6. 重新启动域。
必须升级域中的所有存储库服务，以使用新加密密钥更新和加密存储库中的敏感数据。
7. 升级所有模型存储库服务、PowerCenter 存储库服务和 Metadata Manager 服务。
可以在 Administrator 工具中或在命令提示符下升级模型存储库服务和 PowerCenter 存储库服务。可以在 Administrator 工具中升级 Metadata Manager 服务。
注意: 必须先禁用 Metadata Manager 服务，然后才能进行升级。
要在 Administrator 工具中升级服务，请在表头区域选择 **管理 > 升级**。如果选择多个服务，Administrator 工具将按正确顺序升级这些服务。
要在命令提示符下升级服务，请使用以下命令：

存储库服务类型	命令
模型存储库服务	<code>infacmd mrs UpgradeContents</code>
PowerCenter 存储库服务	<code>pmrep Upgrade</code>

应用程序服务和端口

Informatica 域服务和 Informatica 域中的应用程序服务具有唯一端口。

Informatica 域

下表介绍了可以设置的端口：

端口	说明
服务管理器端口	服务管理器在节点上使用的端口号。服务管理器将侦听此端口上的传入连接请求。客户端应用程序使用该端口与域中的服务通信。Informatica 命令行程序使用此端口与域进行通信。这也是用于 SQL 数据服务 JDBC/ODBC 驱动程序端口。默认值为 6006。
服务管理器关闭端口	为域服务管理器控制服务器关闭的端口号。服务管理器将侦听此端口上的关闭命令。默认值为 6007。
Informatica Administrator 端口	Informatica Administrator 使用的端口号。默认值为 6008。
Informatica Administrator HTTPS 端口	无默认端口。创建服务时请输入所需端口号。将此端口设置为 0 将禁用与 Administrator 工具的 HTTPS 连接。
Informatica Administrator 关闭端口	控制 Informatica Administrator 关闭服务器的端口号。Informatica Administrator 将侦听此端口上的关闭命令。默认值为 6009。

端口	说明
端口号下限	可分配给此节点上运行的应用程序服务进程的动态端口号范围内的最小端口号。默认值为 6014。
端口号上限	可分配给此节点上运行的应用程序服务进程的动态端口号范围内的最大端口号。默认值为 6114。

分析服务

下表列出了与分析服务关联的默认端口：

类型	默认端口
分析服务 (HTTP)	8085
分析服务 (HTTPS)	无默认端口。创建服务时请输入所需端口号。

内容管理服务

下表列出了与内容管理服务关联的默认端口：

类型	默认端口
内容管理服务 (HTTP)	8105
内容管理服务 (HTTPS)	无默认端口。创建服务时请输入所需端口号。

数据集成服务

下表列出了与数据集成服务关联的默认端口：

类型	默认端口
数据集成服务 (HTTP 代理)	8080
数据集成服务 (HTTP)	8095
数据集成服务 (HTTPS)	无默认端口。创建服务时请输入所需端口号。
剖析仓库数据库	无默认端口。输入数据库端口号。

元数据访问服务

下表列出了与元数据访问服务关联的默认端口：

类型	默认端口
元数据访问服务(HTTP)	7080 元数据访问服务使用连续的端口号连接到多个 Hadoop 发行版。
元数据访问服务(HTTPS)	无默认端口。创建服务时请输入所需端口号。元数据访问服务使用连续的端口号连接到多个 Hadoop 发行版。

Metadata Manager 服务

下表列出了与 Metadata Manager 服务关联的默认端口：

类型	默认端口
Metadata Manager 服务 (HTTP)	10250
Metadata Manager 服务 (HTTPS)	无默认端口。创建服务时请输入所需端口号。

PowerExchange® 侦听器服务

使用 DBMOVER 文件的 SVCNODE 语句中指定的端口号。

如果在一个节点上定义运行多个侦听器服务，则必须为每个服务定义唯一 SVCNODE 端口号。

PowerExchange 日志记录器服务

使用 DBMOVER 文件的 SVCNODE 语句中指定的端口号。

如果在一个节点上定义运行多个侦听器服务，则必须为每个服务定义唯一 SVCNODE 端口号。

Web 服务中心服务

下表列出了与 Web 服务中心服务关联的默认端口：

类型	默认端口
Web 服务中心服务 (HTTP)	7333
Web 服务中心服务 (HTTPS)	7343

第 7 章

Informatica Administrator 中的安全管理

本章包括以下主题：

- [使用 Informatica Administrator 概览, 88](#)
- [用户安全, 89](#)
- [安全选项卡, 91](#)
- [密码管理, 94](#)
- [域安全性管理, 95](#)
- [用户安全管理, 95](#)

使用 Informatica Administrator 概览

Informatica Administrator 是用于管理 Informatica 域和 Informatica 安全的工具。

使用 Administrator 工具可完成以下类型的任务：

- **域管理任务。**管理日志、域对象、用户权限和域报告。生成和上载节点诊断。监视数据集成服务作业和应用程序。域对象包括应用程序服务、节点、网格、文件夹、数据库连接、操作系统配置文件和许可证。
- **域管理任务。**管理日志、域对象和用户权限。
- **安全管理任务。**管理用户、组、角色和特权。

Administrator 工具具有以下选项卡：

- **管理。**查看和编辑域及域中对象的属性。
- **监视。**查看每个数据集成服务的配置文件作业、结果卡作业、预览作业、映射作业、SQL 数据服务、Web 服务和工作流的状态。
- **监视。**查看每个数据集成服务的配置文件作业、预览作业、映射作业、SQL 数据服务和 Web 服务的状态。
- **监视。**查看和监视 Ultra Messaging 部署。
- **日志。**查看域及域中服务的日志事件。
- **报告。**运行 Web 服务报告或许可证管理报告。
- **安全。**管理用户、组、角色和特权。
- **云。**查看 Informatica Cloud® 组织的相关信息。

Administrator 工具具有以下表头项：

- **注销。**从 Administrator 工具注销。
- **管理。**管理帐户。
- **帮助。**访问当前选项卡的帮助并确定 Informatica 的版本。
- **帮助。**访问当前选项卡的帮助、确定 Informatica 的版本，以及配置数据用法策略。

用户安全

服务管理器和一些应用程序服务控制应用程序客户端中的用户安全。应用程序客户端包括 Informatica Administrator、Informatica Analyst、Informatica Developer、Metadata Manager 和 PowerCenter 客户端。服务管理器和一些应用程序服务控制应用程序客户端中的用户安全。应用程序客户端包括 Informatica Administrator 和 Informatica Developer。服务管理器和一些应用程序服务控制应用程序客户端中的用户安全。应用程序客户端包括 Informatica Administrator。

服务管理器和应用程序服务通过执行以下功能控制用户安全：

加密

登录应用程序客户端时，服务管理器将加密密码。

身份验证

登录应用程序客户端时，服务管理器会根据您的用户名和密码或用户身份验证令牌对用户帐户进行身份验证。

授权

在应用程序客户端中请求对象时，服务管理器和一些应用程序服务会根据您的特权、角色和权限授权请求。

还可使用 HTTPS 实现与域和应用程序服务的安全连接。以下应用程序服务提供 Informatica 域随附的 HTTPS 连接：

- 数据集成服务
- 分析服务
- 内容管理服务
- 元数据访问服务
- Metadata Manager 服务
- Web Service Hub 服务

还可使用 HTTPS 实现与域和应用程序服务的安全连接。以下应用程序服务支持 Informatica 域随附的 HTTPS 连接：

- 数据集成服务
- 分析服务

还可使用 HTTPS 实现与域和应用程序服务的安全连接。

加密

Informatica 对从应用程序客户端发送至服务管理器的密码进行加密。Informatica 将 AES 加密与多个 128 位密钥结合使用以加密密码并将已加密的密码存储到域配置数据库中。配置 HTTPS 对从应用程序客户端发送至服务管理器的密码进行加密。

身份验证

服务管理器将对登录应用程序客户端的用户进行身份验证。

首次登录应用程序客户端时，请输入用户名、密码和安全域。安全域是 Informatica 域中用户帐户和组的集合。

您选择的安全域将确定服务管理器对您的用户帐户进行身份验证的方法：

- 本地。以本地用户身份登录应用程序客户端时，服务管理器将根据域配置数据库中的用户帐户对您的用户名和密码进行身份验证。
- 轻型目录访问协议 (LDAP)。以 LDAP 用户身份登录应用程序客户端时，服务管理器会将您的用户名和密码传递给外部 LDAP 目录服务进行身份验证。

以本地用户身份登录应用程序客户端时，服务管理器将根据域配置数据库中的用户帐户对您的用户名和密码进行身份验证。

以本地用户身份登录应用程序客户端时，服务管理器将根据域配置数据库中的用户帐户对您的用户名和密码进行身份验证。

单点登录

在您登录到应用程序客户端后，服务管理器允许您启动另一个应用程序客户端或访问该应用程序客户端中的多个存储库。您不需要登录到其他应用程序客户端或存储库。

服务管理器首次对您的用户帐户进行身份验证时，它会为您的帐户创建加密的身份验证标志并将该身份验证标志返回应用程序客户端。身份验证标志包含您的用户名、安全域和到期时间。服务管理器会在到期时间之前定期续订身份验证标志。

当您访问某个应用程序客户端中的多个存储库时，该应用程序客户端会将身份验证标志发送到服务管理器，以进行用户身份验证。

当您从另一个 Web 应用程序客户端启动一个 Web 应用程序客户端时，应用程序客户端会将身份验证标志传递到下一个应用程序客户端。下一个 Web 应用程序客户端会将身份验证标志发送到服务管理器，以进行用户身份验证。您必须分别从每个 Web 应用程序客户端注销。例如，如果从 Administrator 工具打开 Analyst 工具，必须分别从 Analyst 工具和 Administrator 工具注销。

注意：要在 Administrator 工具、Analyst 工具和 Monitoring 工具之间使用单点登录，必须向每个节点的主机文件添加它们的完全限定的域名。

您无法使用单点登录从客户端工具连接到 Web 应用程序客户端。例如，如果从 Developer tool 启动 Administrator 工具，必须登录到 Administrator 工具。

授权

服务管理器授权用户对域对象的请求。通过 Administrator 工具可获得请求。以下应用程序服务将授权用户对其对象的请求：

- 数据集成服务
- Metadata Manager 服务
- 模型存储库服务
- PowerCenter 存储库服务

服务管理器授权用户对域对象的请求。通过 Administrator 工具可获得请求。以下应用程序服务将授权用户对其对象的请求：

- 数据集成服务
- 模型存储库服务

创建本地用户和组或导入 LDAP 用户和组时，服务管理器会将域配置数据库中的信息存储到以下存储库中：

- 模型存储库
- PowerCenter 存储库
- Metadata Manager 的 PowerCenter 存储库

以下事件发生后，服务管理器会将存储库和域配置数据库之间的用户和组信息进行同步：

- 重新启动 Metadata Manager 服务、模型存储库服务或 PowerCenter 存储库服务。
- 添加或删除本地用户或组。
- 服务管理器将域配置数据库中的 LDAP 用户和组列表与 LDAP 目录服务中的用户和组列表同步。

以下事件发生后，服务管理器会将存储库和域配置数据库之间的用户和组信息进行同步：

- 重新启动模型存储库服务。
- 添加或删除本地用户或组。

向应用程序客户端中的用户和组分配权限时，应用程序服务会将具有用户和组信息的权限分配存储到相应的存储库中。

在应用程序客户端中请求对象时，相应的应用程序服务将授权您的请求。例如，如果尝试编辑 Informatica Developer 中的项目，则模型存储库服务将根据您的特权、角色和权限分配授权请求。

安全选项卡

可以在 Administrator 工具的“安全”选项卡中管理 Informatica 安全。

“安全”选项卡包含以下组件：

- “搜索”部分。按名称搜索用户、组或角色。
- 导航器。导航器将出现在左侧窗格中，显示组、用户和角色。
- 内容面板。内容面板根据在导航器中选择对象和在内容面板中选择的选项卡来显示属性和选项。
- “安全操作”菜单。包含用于创建或删除组、用户或角色的选项。可以管理 LDAP 配置和操作系统配置文件。还可以查看对服务有特权的用户。

注意：如果已安装 PowerCenter Express Personal Edition，则无法访问“安全”选项卡

使用搜索部分

使用“搜索”部分可按名称搜索用户、组和角色。搜索不区分大小写。

1. 在“搜索”部分，选择是要搜索用户、组还是角色。
2. 输入要搜索的名称或部分名称。

名称中可以包含星号 (*) 以便在搜索中使用通配符。例如，输入“ad*”可搜索以“ad”开头的对象。输入“*ad”可搜索以“ad”结尾的对象。

3. 单击“执行”。

此时将显示“搜索结果”部分，其中最多显示 100 个对象。如果搜索返回的对象超过 100 个，则缩小搜索条件范围可细化搜索结果。

4. 选择“搜索结果”部分的对象可在内容面板中显示该对象的相关信息。

使用安全导航器

导航器显示在“安全”选项卡的内容面板中。在导航器中选择对象后，内容面板将显示该对象的相关信息。

“安全”选项卡上的导航器根据您要查看的内容显示以下的一个部分：

- “组”部分。选择组可查看该组的属性、向该组分配的用户，以及向该组分配的角色和特权。
- “用户”部分。选择用户可查看该用户的属性、该用户所属的组，以及向该用户分配的角色和特权。
- “角色”部分。选择角色可查看该角色的属性、将该角色分配到的用户和组，以及向该角色分配的特权。
- “操作配置文件”部分。选择一个操作配置文件，以查看操作系统配置文件的属性以及为使用该操作系统配置文件的用户和组分配的权限。
- “LDAP 配置”部分。选择一个配置，以查看 LDAP 服务器连接详细信息、包含从 LDAP 目录服务导入的用户和组的 LDAP 安全域以及 LDAP 同步计划。

导航器提供了完成任务的不同方法。可以使用以下任意方法来管理组、用户和角色：

- 单击**操作**菜单。导航器的每个部分都包含“操作”菜单，用于管理组、用户、角色、操作系统配置文件或 LDAP 配置。
- 右键单击对象。右键单击导航器中的对象可显示“操作”菜单中的可用选项。
- 使用键盘快捷方式。使用键盘快捷方式可移动到导航器的不同部分。

组

组是用户和组的集合，可以具有相同的特权、角色和权限。

导航器中的“组”部分可将组组织到安全域文件夹中。安全域是 Informatica 域中用户帐户和组的集合。本地身份验证使用本地安全域，该域包含在 Administrator 工具中创建和管理的用户和组。LDAP 身份验证使用 LDAP 安全域，该域包含从 LDAP 目录服务中导入的用户和组。

在导航器的“组”部分选择安全域文件夹后，内容面板将显示属于该安全域的所有组。

在导航器中选择组后，内容面板将显示以下选项卡：

- 概览。显示分配给组的组和用户的常规属性。
- 特权。显示向域和域中应用程序服务的组分配的特权和角色。
- 权限。显示组中的用户拥有的用于对域对象（包括节点、网格和应用程序服务）执行任务的访问权限级别。还显示组中的用户拥有的用于对连接对象和操作系统配置文件执行任务的访问权限级别。

用户

在 Informatica 域中具有帐户的用户可以登录到以下应用程序客户端：

- Informatica Administrator
- PowerCenter 客户端
- Informatica Developer
- Informatica Analyst
- Metadata Manager

导航器中的“用户”部分可将用户组织到安全域文件夹中。安全域是 Informatica 域中用户帐户和组的集合。本地身份验证使用本地安全域，该域包含在 Administrator 工具中创建和管理的用户和组。LDAP 身份验证使用 LDAP 安全域，该域包含从 LDAP 目录服务中导入的用户和组。

在导航器的“用户”部分选择安全域文件夹后，内容面板将显示属于该安全域的所有用户。

在导航器中选择用户后，内容面板将显示以下选项卡：

- 概览。显示用户以及该用户所属的所有组的常规属性。
- 特权。显示向域和域中应用程序服务的用户分配的特权和角色。
- 权限。显示用户拥有的用于对域对象（包括节点、网格和应用程序服务）执行任务的访问权限级别。还显示用户拥有的用于对连接对象和操作系统配置文件执行任务的访问权限级别。

角色

角色是指向用户或组分配的一组特权。特权决定了用户可执行的操作。可以向域或域中应用程序服务的用户和组分配角色。

导航器的“角色”部分可将角色组织到以下文件夹中：

- 系统定义角色。包含无法编辑或删除的角色。管理员角色是系统定义角色。
- 自定义角色。包含可以创建、编辑和删除的角色。Administrator 工具中包含一些可以编辑并向其分配用户和组的自定义角色。

在导航器的“角色”部分选择文件夹后，内容面板将显示属于该文件夹的所有角色。

在导航器中选择角色后，内容面板将显示以下选项卡：

- 概览。显示为域和应用程序服务分配角色的角色、用户和组的常规属性。
- 特权。显示分配给域和应用程序服务的角色的特权。

操作系统配置文件

操作系统配置文件是数据集成服务和 PowerCenter 集成服务用于运行映射、工作流和剖析作业的安全机制。

导航器的“操作系统配置文件”部分列出了在域中配置的操作系统配置文件。

在导航器中选择操作系统配置文件后，内容面板将显示以下选项卡：

- 属性。显示为数据集成服务和/或 PowerCenter 集成服务配置的操作系统配置文件的常规属性。
- 权限。显示分配给使用操作系统配置文件的用户和组的权限。此外，还指示操作系统配置文件是否为分配给用户或组的默认配置文件。

LDAP 配置

您可以配置 Informatica 域，以允许从一个或多个 LDAP 目录服务导入的用户和组登录到 Informatica 节点、服务和应用程序客户端。

导航器的“LDAP 配置”部分会列出域使用的 LDAP 配置。

选择 LDAP 配置时，以下选项卡将显示在“LDAP 配置”选项卡下：

- 概览。列出包含要从中导入用户和组的目录服务的 LDAP 服务器的连接详细信息。
- 安全域。列出包含从 LDAP 目录服务导入的用户和组的 LDAP 安全域的详细信息。
- 计划。列出同步计划的详细信息，同步计划指定了服务管理器何时使用 LDAP 目录服务中的用户和组更新安全域。

帐户管理

要提高 Informatica 域的安全性，可以在指定次数的登录尝试失败后强制锁定用户和管理员帐户。

“帐户管理”页面的“帐户锁定配置”部分显示是否为用户帐户和管理员帐户启用了帐户锁定。该部分还指示允许的登录失败的最大尝试次数。

该页面的“已锁定本地用户”部分列出了本地安全域中已锁定的用户帐户。您可以解锁本地安全域中的用户帐户。

该页面的“已锁定 LDAP 用户”部分列出了 LDAP 安全域中已锁定的用户帐户。您可以解锁 Informatica 域中的用户帐户。但是，LDAP 管理员必须在 LDAP 服务器中解锁用户帐户。在 LDAP 管理员解锁用户帐户之前，用户无法登录 Informatica 域。

审计报告

审计报告提供有关 Informatica 域中的用户和组的信息，以及有关分配给每个用户或组的特权、角色和权限的信息。

从“选择报告类型”菜单中选择要生成的审计报告。您可以生成以下审计报告：

用户个人信息

显示域中用户帐户的联系人信息和状态详细信息。可以选择要为其生成报告的用户或组。

用户组关联

显示有关用户及这些用户所属组的信息。可以选择要为其生成报告的用户或组。

特权

显示分配给域中用户和组的特权的相关信息。可以选择要为其生成报告的用户或组。

角色

显示分配给域中用户和组的角色的相关信息。可以选择要为其生成报告的角色。

域对象权限

显示用户和组对其拥有权限的域对象的相关信息。可以选择要为其生成报告的用户或组。

密码管理

通过更改密码应用程序可以更改密码。

通过 Administrator 工具或以下 URL 可以打开更改密码应用程序：<http://<完全限定的主机名>:<端口>/passwordchange/>

服务管理器使用执行工作节点关联的用户密码可对域用户进行身份验证。如果更改与一个或多个执行工作节点关联的用户密码，则服务管理器将更新每个执行工作节点的密码。服务管理器无法更新不运行的节点。对于不运行的节点，服务管理器会在节点重新启动时更新密码。

注意：对于 LDAP 用户帐户，更改 LDAP 目录服务中的密码。

对于本地用户帐户，如果启用了密码复杂度，请在创建或更改密码时遵循以下准则：

- 密码长度必须至少为 8 个字符。
- 密码必须包括字母字符、数字字符和非字母数字字符，例如：
! \ " # \$ % & ' () * + , - . / : ; < = > ? @ [] ^ _ { | } ~

在密码中使用特殊字符时，shell 有时会对这些字符做出不同的解释。例如，将 \$ 解释为一个变量。在这种情况下，请使用转义符对特殊字符进行转义。

更改密码

随时可更改本地用户帐户的密码。对于其他用户创建的用户帐户，请在首次登录 Administrator 工具时更改密码。

1. 在 Administrator 工具表头区域，单击**管理 > 更改密码**。
更改密码应用程序将在新的浏览器窗口中打开。
2. 在**密码**框中输入当前密码，在**新密码**和**确认密码**框中输入新密码。
3. 单击**更新**。

域安全性管理

您可以将 Informatica 域组件配置为使用安全传输层 (SSL) 协议或传输层安全 (TLS) 协议来加密与其他组件的连接。您为域组件启用 SSL 或 TLS 后，可以确保通信安全。

您可以采用以下方法配置安全通信：

在域中的多个服务之间

您可以在域中的多个服务之间配置安全通信。

在域组件和外部组件之间

您可以在 Informatica 域组件与 Web 浏览器或 Web 服务客户端之间配置安全通信。

每种安全通信配置方法都独立于其他方法。您为一组组件配置安全通信后，便不需要再为任何其他组组件配置安全通信。

注意：如果将安全域更改为非安全域，或者将非安全域更改为安全域，则必须在 Developer 工具和 PowerCenter 客户端工具中删除域配置，然后在客户端中重新配置域。

用户安全管理

您管理具有特权和权限的域中的用户安全性。

特权决定用户可以在域对象上完成的操作。权限定义用户对域对象的访问级别。域对象包括域、文件夹、节点、网络、许可证、数据库连接、操作系统配置文件和应用程序服务。

特权决定用户可以在域对象上完成的操作。权限定义用户对域对象的访问级别。域对象包括域、节点、许可证、数据库连接和应用程序服务。

即使用户具有完成某些操作的域特权，该用户仍可能需要权限才能完成对某个特定对象的操作。例如，某个用户具有管理服务域特权，因此该用户可以编辑应用程序服务。但是，该用户还必须具有该应用程序服务的权限。如果某个用户具有开发存储库服务上的管理服务域特权和权限，但不具有生产存储库服务上的相应特权和权限，则该用户可以编辑开发存储库服务，但不能编辑生产存储库服务。

即使用户具有完成某些操作的域特权，该用户仍可能需要权限才能完成对某个特定对象的操作。

要登录到 Administrator 工具，用户必须具有 Informatica Administrator 域访问特权。如果某个用户具有某个对象的 Informatica Administrator 访问特权和权限，但不具有可授予对象类型修改能力的域特权，则该用户可以查看该对象。例如，如果某个用户具有某个节点的权限，但不具有管理节点和网格特权，该用户可以查看节点属性，但不能配置、关闭或删除该节点。

要登录到 Administrator 工具，用户必须具有 Informatica Administrator 域访问特权。如果某个用户具有某个对象的 Informatica Administrator 访问特权和权限，但不具有可授予对象类型修改能力的域特权，则该用户可以查看该对象。

如果用户不具有导航器中选定对象的权限，内容面板将显示一条消息，指示该对象的权限被拒绝。

第 8 章

用户和组

本章包括以下主题：

- [用户和组概览, 97](#)
- [默认组, 98](#)
- [了解用户帐户, 98](#)
- [管理用户, 100](#)
- [管理组, 107](#)
- [管理操作系统配置文件, 109](#)
- [帐户锁定, 116](#)

用户和组概览

要访问 Informatica 域中的应用程序服务和对象并使用应用程序客户端，必须具有用户帐户。

安装期间，会创建默认的管理员用户帐户。使用默认的管理员帐户登录 Informatica 域并管理应用程序服务、域对象以及其他用户帐户。安装后登录到 Informatica 域时，请更改密码以确保 Informatica 域和应用程序的安全性。

注意: 如果安装 PowerCenter Express Personal Edition，对于所有操作您必须使用默认的管理员帐户。不能创建用户或组以及管理权限。

Informatica 中的用户帐户管理涉及以下关键组件：

- 用户。您可以在 Informatica 域中设置不同类型的用户帐户。用户可以基于分配给他们的角色、特权和权限执行任务。
- 身份验证。用户登录应用程序客户端时，服务管理器必须对 Informatica 域中的用户帐户进行身份验证，并验证用户是否可以使用应用程序客户端。Informatica 域可以使用本地或 LDAP 身份验证对用户进行身份验证。服务管理器按安全域组织用户帐户和组。它基于用户所属的安全域对用户进行身份验证。
- 组。您可以设置用户组，并为每个组分配不同的角色、特权和权限。分配给组的角色、特权和权限确定了组中的用户可以在 Informatica 域内执行的任务。
- 特权和角色。特权确定了用户可以在应用程序客户端中执行的操作。角色是您可以分配给用户和组的特权集合。您可以向域的用户和组以及域中的应用程序服务的用户和组分配角色或特权。
- 操作系统配置文件。如果您在 UNIX 或 Linux 上运行集成服务，可以将集成服务配置为使用操作系统配置文件。使用操作系统配置文件可以为用户提高安全性并隔离运行时环境。您可以在 Administrator 工具的“安全”选项卡上创建和管理操作系统配置文件。
- 帐户锁定。您可以将帐户锁定配置为当用户在 Administrator 工具或任何应用程序客户端（例如 Developer tool 和 Analyst 工具）中指定不正确的登录名时锁定用户帐户。您还可以解锁用户帐户。

默认组

Informatica 域包含一系列在安装过程中创建的用户组。

默认情况下，Informatica 域在安装后包含以下用户组：

- 管理员
- 任何人
- 操作员

管理员组

Informatica 域包括一个名为“管理员”的默认组。在安装过程中创建的默认管理员帐户属于此组。

管理员组对域及所有应用程序服务具有管理员权限和特权。可以在管理员组中添加或删除用户。管理员组中的所有用户与安装过程中创建的默认管理员具有相同的权限和特权。

无法从管理员组中删除默认管理员帐户，也无法删除管理员组。

“任何人”组

Informatica 域包括一个名为“任何人”的组。域中的所有用户都属于该组。

默认情况下，“任何人”组不具有任何特权。您可以向“任何人”组分配特权、角色和权限以授予所有用户相同的访问权限。

无法对“任何人”组执行以下任务：

- 编辑或删除“任何人”组。
- 向“任何人”组添加或者从中删除用户。
- 将一个组移动到“任何人”组。

操作员组

Informatica 域包括一个名为“操作员”的默认组。

默认情况下，操作员组具有域中所有对象的权限。您可以将操作员角色分配给操作员组，并使用它来管理域中的操作员用户。

您可以对操作员组执行以下任务：

- 向组分配特权和角色。
- 向组添加用户或者从中删除用户。
- 将某个组移动到此组。
- 编辑或删除此组。

了解用户帐户

一个 Informatica 域可以具有以下类型的帐户：

- 默认管理员

- 域管理员
- 应用程序客户端管理员
- 用户

默认管理员

安装 Informatica 服务时，安装程序将使用您提供的用户名和密码创建默认的管理员。您可以使用默认的管理员帐户首次登录到 Administrator 工具。

默认的管理员对域及所有应用程序服务具有管理员权限和特权。

默认的管理员可以执行以下任务：

- 在域中创建、配置和管理所有对象，包括节点、应用程序服务以及管理员和用户帐户。
- 配置和管理其他域管理员和应用程序客户端管理员创建的所有对象和用户帐户。
- 登录任意应用程序客户端。

您不能禁用或修改默认管理员的用户名或特权。您可以更改默认管理员密码。

域管理员

域管理员可以在域中创建和管理对象。

域管理员可以登录 Administrator 工具并在域中创建和配置应用程序服务。但是，默认情况下，域管理员无法登录应用程序客户端。默认管理员必须明确授予域管理员应用程序服务的全部权限和特权，以便他们可以登录并在应用程序客户端中执行管理任务。

域管理员可以登录 Administrator 工具并在域中配置应用程序服务。但是，默认情况下，域管理员无法登录应用程序客户端。默认管理员必须明确授予域管理员应用程序服务的全部权限和特权，以便他们可以登录并在应用程序客户端中执行管理任务。

要创建域管理员，必须为用户分配域的管理员角色。

应用程序客户端管理员

应用程序客户端管理员可以在应用程序客户端中创建和管理对象。您必须为应用程序客户端创建管理员帐户。要限制管理员特权并确保应用程序客户端的安全性，请为每个应用程序客户端创建一个单独的管理员帐户。

默认情况下，应用程序客户端管理员对域没有权限或特权。如果对域没有权限或特权，应用程序客户端管理员将无法登录到 Administrator 工具来管理应用程序服务。

您可以设置以下应用程序客户端管理员：

Informatica Analyst 管理员

在 Informatica Analyst 中具有完全权限和特权。Informatica Analyst 管理员可以登录到 Informatica Analyst 来创建和管理项目及项目中的对象，并在应用程序客户端中执行所有任务。

要创建 Informatica Analyst 管理员，必须为用户分配分析服务及相关模型存储库服务的管理员角色。

Informatica Developer 管理员

在 Informatica Developer 中具有完全权限和特权。Informatica Developer 管理员可以登录到 Informatica Developer 来创建和管理项目及项目中的对象，并在应用程序客户端中执行所有任务。

要创建 Informatica Developer 管理员，必须为用户分配模型存储库服务的管理员角色。

Metadata Manager 管理员

在 Metadata Manager 中具有完全权限和特权。Metadata Manager 管理员可以登录到 Metadata Manager 来创建和管理 Metadata Manager 对象，并在应用程序客户端中执行所有任务。

要创建 Metadata Manager 管理员，必须为用户分配 Metadata Manager 服务的管理员角色。

测试数据管理员

在 Test Data Manager 中具有完全权限和特权。Test Data Manager 管理员可以登录到 Test Data Manager 来创建和管理 Test Data Manager 对象，并在应用程序客户端中执行所有任务。

要创建测试数据管理员，请为用户分配 Test Data Manager 服务的管理员角色。

PowerCenter 客户端管理员

在 PowerCenter 客户端中具有对所有对象的完全权限和特权。PowerCenter 客户端管理员可以登录到 PowerCenter 客户端来管理 PowerCenter 存储库对象，并在 PowerCenter 客户端中执行所有任务。PowerCenter 客户端管理员还可以在 pmrep 和 pmcmd 命令行程序中执行所有任务。

要创建 PowerCenter 客户端管理员，必须为用户分配 PowerCenter 存储库服务的管理员角色。

用户

在 Informatica 域中具有帐户的用户可以在应用程序客户端中执行任务。

通常，默认管理员或域管理员在 Informatica 域中创建和管理用户帐户并分配角色、权限和特权。但是，具有所需域特权和权限的任何用户都可以创建用户帐户并分配角色、权限及特权。

用户可以基于分配给他们的特权和权限在应用程序客户端中执行任务。

管理用户

您可以在本地安全域中创建、编辑和删除用户。不能删除或修改 LDAP 安全域中的用户帐户的属性。不能修改 LDAP 组的用户分配。

可以基于 PowerCenter Express 许可证的类型创建、编辑和删除用户。可以向用户帐户分配角色、权限和特权。分配给用户的角色、权限和特权确定了用户可以在 Informatica 域内执行的任务。如果具有 PowerCenter Express Personal Edition，则无法创建用户或组。必须使用默认的管理员用户执行所有任务。

可以基于许可证的类型创建、编辑和删除用户。可以向用户帐户分配角色、权限和特权。分配给用户的角色、权限和特权确定了用户可以在 Informatica 域内执行的任务。

可以将角色、权限和特权分配给本地安全域或 LDAP 安全域中的用户帐户。分配给用户的角色、权限和特权确定了用户可以在 Informatica 域内执行的任务。

您还可以解锁用户帐户。

创建本地用户

在“安全”选项卡上添加、编辑或删除本地用户。

1. 在 Administrator 工具中，单击“安全”选项卡。
2. 在“安全操作”菜单上，单击“创建用户”。

3. 输入用户的以下详细信息：

属性	说明
登录名称	用户帐户的登录名。在用户帐户所属的安全域中，其登录名必须唯一。 用户名不区分大小写，且长度不能超过 128 个字符。名称不能包含制表符、换行符或下列特殊字符： , + " \ < > ; / * % ? & 名称可以包含 ASCII 空格字符，但不能将其用作第一个和最后一个字符。不允许使用所有其他空格字符。
密码	用户帐户的密码。密码长度可以是 1 到 80 个字符。
确认密码	请再次输入密码进行确认。必须重新键入密码。不要复制和粘贴密码。
全名	用户帐户的全名。全名不能包含以下特殊字符： < > “
说明	用户帐户的说明。说明不能超过 765 个字符，且不能包括以下特殊字符： < > “
电子邮件	用户的电子邮件地址。电子邮件地址不能包含以下特殊字符： < > “ 按 UserName@Domain 格式输入电子邮件地址。
电话	用户的电话号码。电话号码不能包含以下特殊字符： < > “

4. 单击“确定”保存用户帐户。

创建用户帐户后，详细信息面板会显示用户帐户以及用户所分配到的组的属性。

编辑本地用户的常规属性

不能更改本地用户的登录名。可以更改本地用户帐户的密码和其他详细信息。

1. 在 Administrator 工具中，单击“安全”选项卡。
2. 在导航器的“用户”部分中，选择一个本地用户帐户并单击“编辑”。
3. 要更改密码，请选择“更改密码”。
“安全”选项卡清除了“密码”和“确认密码”字段。
4. 输入新密码并确认。
5. 根据需要修改全名、描述、电子邮件以及电话。
6. 单击“确定”保存更改。

向本地组分配本地用户

在“安全”选项卡上向本地组分配本地用户。

1. 在 Administrator 工具中，单击“安全”选项卡。
2. 在导航器的“用户”部分中，选择一个本地用户帐户并单击**编辑**。
3. 单击“组”选项卡。

4. 要将本地用户分配给组，请在“所有组”列选择一个组名，然后单击**添加**。
如果嵌套组未在“所有组”列显示，请展开每个组显示所有嵌套组。
您可以将一个本地用户分配给多个组。使用 Ctrl 或 Shift 键同时选择多个组。
5. 要将本地用户从组中删除，请在“分配的组”列中选择一个组，然后单击**删除**。
6. 单击**确定**保存组分配。

向本地组分配 LDAP 用户

您可以向本地组分配 LDAP 用户帐户。您无法更改对 LDAP 组的 LDAP 用户帐户分配。

1. 在 Administrator 工具中，单击**安全**选项卡。
2. 在导航器的“组”部分中，选择一个本地组，然后单击**编辑**。
3. 单击**用户**选项卡。
4. 要将 LDAP 用户分配到组，请在“所有用户”列中选择 LDAP 用户，然后单击**添加**。
5. 要从组中删除 LDAP 用户，请在“分配的用户”列中选择 LDAP 用户，然后单击**删除**。
6. 单击**确定**以保存用户分配。

启用和禁用用户帐户

具有活动帐户的用户可以登录应用程序客户端并基于他们的权限和特权执行任务。如果暂时不希望用户访问应用程序客户端，可以禁用其帐户。可以启用或禁用本地或 LDAP 安全域中的用户帐户。禁用某个用户帐户时，该用户将无法登录到应用程序客户端。

具有活动帐户的用户可以登录应用程序客户端并基于他们的权限和特权执行任务。如果暂时不希望用户访问应用程序客户端，可以禁用其帐户。禁用某个用户帐户时，该用户将无法登录到应用程序客户端。

要禁用用户帐户，请在导航器的“用户”部分选择用户帐户并单击“禁用”。选择已禁用的用户帐户时，“安全”选项卡会显示用户帐户已禁用的消息。禁用用户帐户时，“启用”按钮可用。要启用用户帐户，请单击“启用”。

不能禁用默认的管理员帐户。

注意：当服务管理器从 LDAP 目录服务导入用户帐户时，不会导入指示用户帐户已启用或已禁用的 LDAP 属性。服务管理器会将所有用户帐户导入为已启用用户帐户。如果您不希望用户访问应用程序客户端，则必须在 Administrator 工具中禁用 LDAP 用户帐户。在与 LDAP 服务器的后续同步期间，用户帐户会保留在 Administrator 工具中设置的已启用或已禁用状态。

删除本地用户

要删除本地用户帐户，请右键单击导航器的“用户”部分中的用户帐户名并选择“删除用户”。确认是否要删除该用户帐户。

不能删除默认的管理员帐户。登录 Administrator 工具时，不能删除用户帐户。

删除 PowerCenter 的用户

删除拥有 PowerCenter 存储库中对象的用户时，可以删除该用户对文件夹、连接对象、部署组、标签或查询的任何所有权。删除用户后，默认管理员会成为已删除用户拥有的所有对象的所有者。

查看已删除用户之前拥有的受版本控制对象的历史记录时，将显示以单词“deleted”为前缀的已删除用户的名称。

删除 Metadata Manager 的用户

当您删除拥有快捷方式和文件夹的用户时，Metadata Manager 会将用户的个人文件夹移至默认管理员所拥有的名为“已删除用户”的文件夹。已删除用户的个人文件夹包含该用户创建的所有快捷方式和文件夹。删除用户后，任何共享文件夹仍保持共享。

如果“已删除用户”文件夹包含具有相同用户名的文件夹，Metadata Manager 会将该附加文件夹命名为“<用户名> 的副本 (n)”。

LDAP 用户

无法在 Administrator 工具中添加、编辑或删除 LDAP 用户。必须在 LDAP 目录服务中管理 LDAP 用户帐户。

解锁用户帐户

域管理员可以解锁域中已锁定的用户帐户。如果用户是本地用户，管理员可以请求用户在登录回域之前重置其密码。

用户必须在域中配置有效的电子邮件，以在其帐户密码重置时接收通知。

如果锁定 LDAP 验证服务器的用户，则 LDAP 管理员必须解除 LDAP 服务器中的用户帐户锁定。

1. 在 Administrator 工具中，单击**安全**选项卡。
2. 单击**帐户管理**。
“帐户管理”页面会显示下列已锁定用户列表：
已锁定本地用户
包括已锁定的本地安全域中的用户帐户。
已锁定 LDAP 用户
包括已锁定的 LDAP 安全域中的用户帐户。
3. 选择要解锁的用户。
4. 选择**解除用户锁定并重置密码**，以在解锁帐户锁定后为用户生成新密码。
用户将在电子邮件中收到新密码。
5. 单击**解除所选用户的锁定**按钮。

为大量用户增加系统内存

重新启动 Informatica 域、同步 LDAP 用户及部分 infacmd 和 infasetup 命令的处理时间与 Informatica 域中的用户数量成比例增加。

用户数量会影响以下命令的处理时间：

- infasetup BackupDomain、DeleteDomain 和 RestoreDomain
- infacmd isp ExportDomainObjects、ExportUsersandGroups、ImportDomainObjects 和 ImportUsersandGroups
- infacmd tools ExportObjects 和 ImportObjects

当域中有大量的用户时，您可能需要增加 Informatica 服务、infasetup 和 infacmd 所用的系统内存。要增加最大堆大小，请配置以下环境变量并以兆字节为单位指定值：

- INFA_JAVA_OPTS。确定 Informatica 服务使用的最大堆大小。在安装 Informatica 服务的各个节点上配置。
- ICMD_JAVA_OPTS。确定 infacmd 使用的最大堆大小。在运行 infacmd 的各台计算机上配置。

- INFA_JAVA_CMD_OPTS。确定 infasetup 使用的最大堆大小。在运行 infasetup 的各台计算机上配置。

例如，要在 UNIX 上为 INFA_JAVA_OPTS 环境变量配置 2048 MB 的系统内存，请使用以下命令：

```
setenv INFA_JAVA_OPTS "-Xmx2048m"
```

在 Windows 上，作为系统变量配置这些变量。

下表基于域中的用户和服务数量列出了堆大小上限设置的最低要求：

域用户数量	堆大小上限 (1-5 个服务)	堆大小上限 (6-10 个服务)
1000 或更少	512 MB（默认）	1,024 MB
5,000	2,048 MB	3,072 MB
10,000	3,072 MB	5,120 MB
20,000	5,120 MB	6,144 MB
30,000	5,120 MB	6,144 MB

注意：表中的堆大小上限设置基于域中的应用程序服务数量。

配置这些环境变量之后，请重新启动节点以使更改生效。

查看用户活动

可以使用 Administrator 工具的“日志”选项卡查看用户活动日志。查看用户活动日志可检查从 Informatica 客户端应用程序进行的登录尝试。还可以查看日志来确定用户何时创建、更新或删除服务、节点、用户、组或角色。

有关用户活动日志和 Administrator 工具的“日志”选项卡的详细信息，请参阅《Informatica 管理员指南》。

也可以使用 infacmd isp getUserActivityLog 命令查看用户活动日志数据。infacmd isp getUserActivityLog 命令使用以下语法：

```
infacmd isp getUserActivityLog -dn domain_name -un user_name -pd password
```

infacmd isp getUserActivityLog 命令需要管理员角色或管理员组中的成员身份。有关 isp getUserActivityLog 命令的详细信息，请参阅《Informatica 命令参考》。

用户活动日志数据包含用户从 Informatica 客户端进行的已成功和未成功的登录尝试。如果客户端对登录请求设置了自定义属性，则日志数据包含自定义属性。

注意：用户活动日志不包含配置为使用 Kerberos 身份验证的域中的用户登录尝试。

对于从 Informatica 客户端进行的每次登录尝试，用户活动数据包含以下属性：

- 应用程序名称
- 应用程序版本
- 应用程序主机的主机名或 IP 地址

您可以基于以下可选筛选器查看日志事件：

- 用户名
- 安全域

- 日期和时间
- 时间顺序
- 活动代码
- 活动文本

可以在命令提示符中显示日志事件，或者也可以将事件写入到以下格式之一的文件：

- 二进制
- 文本
- XML

如果要以二进制格式打印日志，可以使用 `infacmd isp convertUserActivityLog` 命令将其转换为文本或 XML 格式。有关使用 `infacmd isp convertUserActivityLog` 命令的详细信息，请参阅《*Informatica 命令参考*》。

用户活动代码

用户活动日志包含一些代码，这些代码指示每个活动的成功或失败。

有效的活动代码包括：

- CCM_10437。指示活动成功。
- CCM_10438。指示活动失败。
- CCM_10778。指示使用自定义属性的登录尝试已成功。
- CCM_10779。指示使用自定义属性的登录尝试已失败。
- CCM_10786。指示不使用自定义属性的登录尝试已成功。
- CCM_10787。指示不使用自定义属性的登录尝试已失败。

用户活动日志筛选器

使用一个或多个筛选器可检索特定用户、日期或事件的日志事件。

对 `infacmd isp getUserActivityLog` 命令使用下面的一个或多个参数可筛选日志事件：

用户和安全域

可选。要获取其日志事件的用户列表。请用空格分隔多个用户。使用通配符 (*) 可查看单个安全域或所有安全域上多个用户的日志。例如，以下字符串是此选项的有效值：

```
user:Native
"user:*"
"user*"
"*_users_*"
"*:Native"
```

将以下参数添加到 `getUserActivityLog` 命令可基于用户或安全域筛选日志事件：

```
-usrs <UserName>:<SecurityDomain>
```

例如，添加以下参数可检索所有安全域中用户 User1 的用户活动：

```
-usrs "User1:*
```

日期和时间

可选。要查看日志事件的日期范围。

如果输入的结束日期在开始日期之前，该命令将不会返回任何日志事件。

按以下格式之一输入日期和时间：

- yyyy/MM/dd
- yyyy/MM/dd HH:mm:ss
- yyyy-MM-dd
- yyyy-MM-dd HH:mm:ss

将以下参数添加到 `getUserActivityLog` 命令可按开始日期或结束日期筛选日志：

```
-sd <start_date> -ed <end_date>
```

例如，添加以下参数可检索 2014 年 1 月 1 日到 2014 年 2 月 3 日的用户活动：

```
-sd 01/01/2014 -ed 02/03/2014
```

活动代码

可选。根据活动代码返回日志事件。

使用通配符 (*) 可针对多个活动代码检索日志事件。有效的活动代码包括：

- CCM_10437。指示活动成功。
- CCM_10438。指示活动失败。
- CCM_10778。指示使用自定义属性的登录尝试已成功。
- CCM_10779。指示使用自定义属性的登录尝试已失败。
- CCM_10786。指示不使用自定义属性的登录尝试已成功。
- CCM_10787。指示不使用自定义属性的登录尝试已失败。

将以下参数添加到 `getUserActivityLog` 命令可按活动代码进行筛选：

```
-ac <activity_code>
```

例如，添加以下参数可检索成功的日志事件：

```
-ac CCM_10437
```

如果使用通配符，请用引号将参数引起来。

活动文本

可选。根据在活动文本中找到的字符串返回日志事件。

将以下参数添加到 `getUserActivityLog` 命令可按活动文本进行筛选：

```
-atxt <activity_text>
```

使用通配符 (*) 可针对多个事件检索日志。例如，以下参数将返回在其说明中包含短语 “Enabling service” 的所有日志事件。

```
-atxt "*Enabling service*"
```

如果使用通配符，请用引号将参数引起来。

时间顺序

可选。按倒序输出日志事件。如果您不指定此参数，该命令将按时间顺序显示日志事件。

将以下参数添加到 `getUserActivityLog` 命令可首先打印最新事件：

```
-ro true
```

写入和查看用户活动日志事件

可以将用户活动日志事件写入到某个文件，或者在使用 `infacmd isp getUserActivityLog` 命令时在命令行中显示。根据计划使用导出的日志事件文件的方式将用户活动日志写为某种格式。

写入和查看日志文件

要将用户活动日志事件写入到文件中，可使用输出文件参数 `-lo` 运行命令：

```
-lo output_file_name
```

如果不指定输出格式，该命令将日志事件写入到文本文件中。例如，运行以下命令将日志事件写入到名为 `log.txt` 的文件中：

```
infacmd isp getUserActivityLog -dn TestDomain -un Administrator -pd Administrator -lo log.txt
```

要指定输出格式，可使用格式参数 `-fm` 运行该命令：

```
-fm output_format_BIN_TEXT_XML
```

有效格式包括：

- Bin（二进制）。使用二进制格式备份二进制格式的日志事件。您可能需要使用此格式将日志事件发送给 Informatica 全球客户支持部门
- 文本。如果要在文本编辑器中分析日志事件，请使用文本格式。
- XML。如果要在使用 XML 的外部工具中分析日志事件，或者如果要使用 XSLT 等 XML 工具，请使用 XML 格式。

如果指定文本或 XML 作为输出格式，但未指定输出文件，则该命令将在命令行显示文本或 XML 日志。

如果指定二进制作为输出格式，必须提供输出文件名。

例如，运行以下命令将日志事件打印到名为 `log.xml` 的文件：

```
infacmd isp getUserActivityLog -dn TestDomain -un Administrator -pd Administrator -fm xml -lo log.xml
```

转换日志文件

如果使用 `getUserActivity` 命令将日志事件写入二进制文件，则可以将该文件转换为文本或 XML 格式。

运行以下命令将检索的二进制日志转换为文本或 XML 格式：

```
infacmd isp convertUserActivityLogFile -in BIN_input_file_name -fm output_format_TEXT_XML -lo output_file_name
```

例如，运行以下命令将二进制输入文件 `log.bin` 转换为 XML 格式，并将其输出到名为 `convertedLog.xml` 的文件中：

```
infacmd isp convertUserActivityLogFile -in log.bin -fm XML -lo convertedLog.xml
```

要在命令行显示日志，可忽略输出文件名。

如果忽略格式，该命令将使用文本格式。

管理组

您可以在本地安全域中创建、编辑和删除组。

可以将角色、权限和特权分配给本地安全域或 LDAP 安全域中的组。不能删除或修改 LDAP 安全域中的组帐户的属性。分配给组的角色、权限和特权确定了组中的用户可以在 Informatica 域内执行的任务。

可以向组分配角色、权限和特权。分配给组的角色、权限和特权确定了组中的用户可以在 Informatica 域内执行的任务。

可以向组分配角色、权限和特权。分配给组的角色、权限和特权确定了组中的用户可以在 Informatica 域内执行的任务。

添加本地组

在“安全”选项卡上添加、编辑或删除本地组。

本地组可以包含本地用户帐户或 LDAP 用户帐户或其他本地组。可以创建多个级别的本地组。例如，“财务”组包含“应付款项”组，而“应付款项”组又包含“办公用品”组。“财务”组是“应付款项”组的父组，“应付款项”是“办公用品”组的父组。每个组可以包含其他本地组。

本地组可以包含用户帐户或其他本地组。可以创建多个级别的本地组。例如，“财务”组包含“应付款项”组，而“应付款项”组又包含“办公用品”组。“财务”组是“应付款项”组的父组，“应付款项”是“办公用品”组的父组。每个组可以包含其他本地组。

本地组可以包含用户帐户或其他本地组。可以创建多个级别的本地组。例如，“财务”组包含“应付款项”组，而“应付款项”组又包含“办公用品”组。“财务”组是“应付款项”组的父组，“应付款项”是“办公用品”组的父组。每个组可以包含其他本地组。

1. 在 Administrator 工具中，单击“安全”选项卡。
2. 在“安全操作”菜单上，单击“创建组”。
3. 输入组的以下信息：

属性	说明
名称	组的名称。用户名不区分大小写，且长度不能超过 128 个字符。组名称不能包含制表符、换行符或下列特殊字符： , + " \ < > ; / * % ? 名称可以包含 ASCII 空格字符，但不能将其用作第一个或最后一个字符。不允许使用所有其他空格字符。
父组	新组所属的组。如果在单击“创建组”之前选择本地组，则选择的组即是父组。否则，“父组”字段将显示“本地”，表示新组不属于某个组。
说明	组的说明。组说明不能超过 765 个字符，且不能包括以下特殊字符： < > “

4. 单击“浏览”选择其他父组。
您可以创建多个级别的组和子组。
5. 单击“确定”保存组。

编辑本地组的属性

创建组之后，您可以更改组的说明和组中的用户列表。不能更改组名称或者组的父组。要更改组的父组，必须将组移动到其他组。

1. 在 Administrator 工具中，单击“安全”选项卡。
2. 在导航器的“组”部分中，选择本地组并单击“编辑”。
3. 更改组的说明。
4. 要更改组中的用户列表，请单击“用户”选项卡。
“用户”选项卡将显示域中的用户列表以及分配给组的用户列表。
5. 要向组分配用户，请在“所有用户”列中选择用户帐户并单击“添加”。

6. 要从组中删除用户，请在“分配的用户”列中选择一个用户帐户，然后单击“删除”。
7. 单击“确定”保存更改。

将一个本地组移动到另一个本地组

要在本地安全域中组织用户组，可以设置嵌套组并将一个组移动到另一个组中。

要将本地组移动到另一个本地组，请右键单击导航器“组”部分中的本地组的名称，然后选择“移动组”。

删除本地组

要删除本地组，请右键单击导航器的“组”部分中的组名并选择“删除组”。

删除组时，组中的用户将失去其在组中的成员身份以及从组中继承的所有权限和特权。

删除组时，服务管理器将删除所有组以及属于该组的子组。

LDAP 组

不能在 Administrator 工具中添加、编辑或删除 LDAP 组或修改 LDAP 组的用户分配。必须在 LDAP 目录服务中管理组 and 用户分配。

管理操作系统配置文件

在 Administrator 工具的“安全”选项卡上或者从命令行创建并管理操作系统配置文件。您可以创建、编辑和删除操作系统配置文件。可以为用户和组分配或更改默认操作系统配置文件。

如果数据集成服务配置为使用操作系统配置文件，它将使用操作系统配置文件运行映射、配置文件和工作流。如果 PowerCenter 集成服务配置为使用操作系统配置文件，它将使用操作系统配置文件运行工作流。

在**安全**选项卡的**操作系统配置文件**视图中创建、编辑和删除操作系统配置文件。

完成以下步骤以创建操作系统配置文件：

1. 输入操作系统配置文件名称和系统用户名。
2. 选择集成服务并配置操作系统配置文件属性。
3. 或者，分配对操作系统配置文件的权限。

在创建操作系统配置文件后，可以为操作系统配置文件分配用户和组，并将默认配置文件分配给用户和组。

PowerCenter 集成服务的操作系统配置文件属性

在会话属性和参数文件中设置的服务进程变量将覆盖操作系统配置文件设置。

下表介绍了 PowerCenter 集成服务的操作系统配置文件属性：

属性	说明
名称	操作系统配置文件的只读名称。名称不得超过 128 个字符。不得包含空格或以下特殊字符：\ / : * ? " < > [] = + ; ,
系统用户名	存在于运行 PowerCenter 集成服务的计算机上的操作系统用户的只读名称。PowerCenter 集成服务会使用为操作系统配置文件定义的系统用户的系统访问权限运行工作流。
\$PMRootDir	该节点可访问的根目录。这是其他服务进程变量的根目录。它不能包含以下特殊字符： * ? < > “ ,
\$PMSessionLogDir	会话日志的目录。它不能包含以下特殊字符： * ? < > “ , 默认值为 \$PMRootDir/SessLogs。
\$PMBadFileDir	拒绝文件的目录。它不能包含以下特殊字符： * ? < > “ , 默认值为 \$PMRootDir/BadFiles。
\$PMCacheDir	索引和数据缓存文件的目录。 当缓存目录是 PowerCenter 集成服务进程本地的驱动器时，可以提高性能。请勿对缓存文件使用映射或装入的驱动器。它不能包含以下特殊字符： * ? < > “ , 默认值为 \$PMRootDir/Cache。
\$PMTargetFileDir	目标文件的目录。它不能包含以下特殊字符： * ? < > “ , 默认值为 \$PMRootDir/TgtFiles。
\$PMSourceFileDir	源文件的目录。它不能包含以下特殊字符： * ? < > “ , 默认值为 \$PMRootDir/SrcFiles。
\$PmExtProcDir	外部过程的目录。它不能包含以下特殊字符： * ? < > “ , 默认值为 \$PMRootDir/ExtProc。
\$PMTempDir	临时文件的目录。它不能包含以下特殊字符： * ? < > “ , 默认值为 \$PMRootDir/Temp。
\$PMLookupFileDir	查找文件的目录。它不能包含以下特殊字符： * ? < > “ , 默认值为 \$PMRootDir/LkpFiles。

属性	说明
\$PMStorageDir	运行时文件的目录。 workflow 恢复文件保存到现在 PowerCenter 集成服务属性中配置的 \$PMStorageDir 中。会话恢复文件保存到现在操作系统配置文件中配置的 \$PMStorageDir 中。它不能包含以下特殊字符： * ? < > “ , 默认值为 \$PMRootDir/Storage。
环境变量	集成服务在运行时使用的环境变量的名称和值。 如果在操作系统配置文件属性中指定 LD_LIBRARY_PATH 环境变量，则集成服务会将该变量的值追加到其 LD_LIBRARY_PATH 环境变量中。集成服务使用其 LD_LIBRARY_PATH 环境变量的值来设置为操作系统配置文件生成的子进程的环境变量。 如果未在操作系统配置文件属性中指定 LD_LIBRARY_PATH 环境变量，则集成服务会使用其 LD_LIBRARY_PATH 环境变量。

数据集成服务的操作系统配置文件属性

下表介绍了数据集成服务的操作系统配置文件属性：

属性	说明
名称	操作系统配置文件的只读名称。名称不得超过 128 个字符。并且不能包含空格或以下特殊字符： % * + \ / ? ; < >
系统用户名	运行数据集成服务的系统上存在的操作系统用户的只读名称。数据集成服务使用操作系统用户的系统访问权限运行映射、工作流和剖析作业。
\$DISRootDir	该节点可访问的根目录。这是其他服务进程变量的根目录。它不能包含以下特殊字符： * ? < > " , []
\$DISTempDir	运行作业时创建的临时文件目录。它不能包含以下特殊字符： * ? < > " , [] 默认为 <根目录>/disTemp。
\$DISCacheDir	转换的索引和数据缓存文件的目录。它不能包含以下特殊字符： * ? < > " , [] 默认为 <根目录>/cache。
\$DISSourceDir	映射中使用的源平面文件的目录。它不能包含以下特殊字符： * ? < > " , [] 默认为 <根目录>/source。
\$DISTargetDir	映射中使用的目标平面文件的目录。它不能包含以下特殊字符： * ? < > " , [] 默认为 <根目录>/target。

属性	说明
\$DISRejectedFilesDir	拒绝文件的目录。拒绝文件包含运行映射时所拒绝的行。它不能包含以下特殊字符： * ? < > " , [] 默认为 <根目录>/reject。
\$DISLogDir	日志的目录。它不能包含以下特殊字符： * ? < > " , [] 默认为 <根目录>/disLogs。
启用 Hadoop 模拟属性	表示数据集成服务使用 Hadoop 模拟用户在 Hadoop 环境中运行映射、工作流和剖析作业。 默认 Hadoop 模拟用户为登录用户。要指定不同的 Hadoop 模拟用户，请选择 使用指定用户作为 Hadoop 模拟用户 并输入用户名。
环境变量	集成服务在运行时使用的环境变量的名称和值。 如果在操作系统配置文件属性中指定 LD_LIBRARY_PATH 环境变量，则集成服务会将该变量的值追加到其 LD_LIBRARY_PATH 环境变量中。集成服务使用其 LD_LIBRARY_PATH 环境变量的值来设置为操作系统配置文件生成的子进程的环境变量。 如果未在操作系统配置文件属性中指定 LD_LIBRARY_PATH 环境变量，则集成服务会使用其 LD_LIBRARY_PATH 环境变量。 注意: 在 AIX 上，您必须将环境变量 LD_LIBRARY_PATH 设置为 INFA_HOME/services/shared/bin 以确保数据集成服务成功使用操作系统配置文件运行映射、配置文件和工作流。
平面文件缓存目录	Analyst 工具用于存储已上载平面文件的平面文件缓存目录。 如果分析服务连接到使用操作系统配置文件的数据集成服务，在操作系统配置文件中指定的操作系统用户必须能够访问该平面文件缓存目录。导入引用表或平面文件源时，Analyst 工具使用此目录中的文件创建引用表或平面文件数据对象。如更改平面文件位置，请重新启动分析服务。

元数据访问服务的操作系统配置文件属性

下表介绍了元数据访问服务的操作系统配置文件属性：

属性	说明
名称	操作系统配置文件的只读名称。名称不得超过 128 个字符。并且不能包含空格或以下特殊字符： % * + \ / ? ; < >
系统用户名	运行元数据访问服务的系统上存在的操作系统用户的只读名称。元数据访问服务允许 Developer tool 访问 Hadoop 连接信息，以使用操作系统用户的系统访问权限导入和预览元数据。
启用 Hadoop 模拟属性	指示元数据访问服务使用 Hadoop 模拟用户导入和预览元数据。 默认 Hadoop 模拟用户为登录用户。要指定不同的 Hadoop 模拟用户，请选择 使用指定用户作为 Hadoop 模拟用户 并输入用户名。

创建操作系统配置文件

创建操作系统配置文件并将其分配给用户和组，以提高安全性并隔离运行时用户环境。您可以创建一个或多个操作系统配置文件。PowerCenter 集成服务使用操作系统配置文件运行工作流。数据集成服务使用操作系统配置文件运行映射、配置文件和工作流。元数据访问服务使用操作系统配置文件访问 Hadoop 连接信息以导入和预览元数据。

- 1. 在 Administrator 工具中，单击**安全**选项卡。
- 2. 在“安全操作”菜单上，单击**创建操作系统配置文件**。
此时将显示**创建操作系统配置文件 - 第 1 步(共 3 步)**对话框。
- 3. 为操作系统配置文件输入以下常规属性：

属性	说明
名称	操作系统配置文件的名称。名称不区分大小写，但在域中必须唯一。名称长度不能超过 128 个字符，且不能以 @ 开头。名称也不能包含以下特殊字符： % * + \ / ? ; < > 名称可以包含 ASCII 空格字符，但不能将其用作第一个或最后一个字符。不允许使用所有其他空格字符。
系统用户名	运行集成服务的计算机上存在的操作系统用户的名称。集成服务会使用为操作系统配置文件定义的系统用户的系统访问权限来运行工作流或作业。 注意: 创建操作系统配置文件时，不能将系统用户名指定为 root，也不能使用 uid=0 的非 root 用户。

- 4. 单击**下一步**。
此时将显示**配置操作系统配置文件 - 第 2 步(共 3 步)**对话框。
- 5. 选择将要使用操作系统配置文件的服务。
 - PowerCenter 集成服务
 - 数据集成服务
 - 元数据访问服务
- 6. 为选定服务配置操作系统配置文件属性。要为元数据访问服务创建操作系统配置文件，还必须选择数据集成服务以及元数据访问服务，并为数据集成服务指定 \$DISRootDir 变量。
- 7. 如果这些服务在设计时或运行时访问 Hadoop 环境，请配置 Hadoop 模拟属性，具体如下所述：
 - a. 选择**启用 Hadoop 模拟属性**。
 - b. 选择使用登录的用户或指定一个 Hadoop 模拟用户运行 Hadoop 作业。
- 8. 或者，配置环境变量。
- 9. 如果分析服务连接到使用操作系统配置文件的数据集成服务，配置分析服务属性。
- 10. 单击**下一步**。
此时将显示**向操作系统配置文件分配组 and 用户 - 第 3 步(共 3 步)**对话框。
- 11. 在**组**选项卡上，将组分配给操作系统配置文件，如下所示：
 - a. 要将特定组分配给操作系统配置文件，选择一个或多个组，然后单击**添加**。
 - b. 要将所有可用组分配给操作系统配置文件，单击**全部添加**。
- 12. 或者，将操作系统配置文件作为默认配置文件分配给一个或多个组。要分配默认配置文件，为“已选组”列表中的组选择**默认配置文件**。

13. 在**用户**选项卡上，将用户分配给操作系统配置文件，如下所示：
 - a. 要将特定用户分配给操作系统配置文件，选择一个或多个用户，然后单击**添加**。
 - b. 要将所有可用用户分配给操作系统配置文件，单击**全部添加**。
14. 或者，将操作系统配置文件作为默认配置文件分配给一个或多个用户。要分配默认配置文件，为“已选用户”列表中的用户选择**默认配置文件**。
15. 单击**完成**。

在您创建操作系统配置文件后，详细信息面板将显示操作系统配置文件的属性以及分配了配置文件的组和用户。

编辑操作系统配置文件

您可以编辑操作系统配置文件，以更改操作系统配置文件的属性。

创建操作系统配置文件之后，您无法编辑名称或系统用户名。如果不希望使用操作系统配置文件中指定的操作系统用户，请删除操作系统配置文件。

1. 在 Administrator 工具中，单击**安全**选项卡。
2. 选择**操作系统配置文件**视图。
3. 选择操作系统配置文件。
4. 在**属性**选项卡中，单击**编辑**。

此时将显示**编辑属性**对话框。
5. 选择要配置的数据集成服务、PowerCenter 集成服务或元数据访问服务。
6. 编辑服务属性。
7. 单击**确定**。

向用户或组分配默认操作系统配置文件

当用户或组有权访问多个操作系统配置文件时，分配集成服务用于运行作业和工作流的默认操作系统配置文件。您可以通过直接权限将任何操作系统配置文件作为默认配置文件分配给用户或组。一个用户或组只能有一个默认的操作系统配置文件。然而，您可以将同一个操作系统配置文件作为默认配置文件分配给多个用户或组。

1. 在“安全”选项卡上，选择**用户或组**视图。
2. 在导航器中，选择用户或组。
3. 在内容面板中，选择**权限**视图。
4. 单击**操作系统配置文件**选项卡。
5. 单击**分配或更改默认操作系统配置文件**按钮。

此时将显示**分配或更改默认操作系统配置文件**对话框。
6. 从**默认操作系统配置文件**列表中选择配置文件。或者从列表中选择**不分配默认操作系统配置文件**以删除分配给用户或组的默认配置文件。
7. 单击**确定**。

在详细信息面板中，**默认配置文件**列显示操作系统配置文件为**是(直接)**。

删除操作系统配置文件

要删除操作系统配置文件，在导航器的“操作系统配置文件”部分中，右键单击操作系统配置文件名称，然后选择**删除配置文件**。

删除操作系统配置文件后，将另一个操作系统配置文件分配给之前分配了操作系统配置文件（作为默认配置文件）的用户和组。如果 PowerCenter 集成服务使用操作系统配置文件，将另一个操作系统配置文件分配给之前分配了操作系统配置文件的存储库文件夹和工作流。

在安全域中使用操作系统配置文件

您可以在已启用安全通信的 Informatica 域中使用操作系统配置文件。

如果在已启用安全通信的域中使用操作系统配置文件，请考虑以下规则和准则：

- 您必须为操作系统配置文件设置以下环境变量：

INFA_TRUSTSTORE

将该值设置为包含安全域 SSL 证书的信任库文件的目录。该目录必须包含一个名为 infa_truststore.pem 的信任库文件。

INFA_TRUSTSTORE_PASSWORD

如果使用自定义信任存储，请为包含安全域的 SSL 证书的 infa_truststore.pem 设置密码值。必须加密密码。使用命令程序 `pmpasswd` 加密密码。

- 此外，如果 PowerCenter 集成服务使用“网格上的会话”选项，您必须为操作系统配置文件设置以下环境变量：

INFA_KEYSTORE

将该值设置为包含安全域 SSL 证书的存储库文件的目录。该目录必须包含一个名为 infa_keystore.pem 的密钥库文件。

可以在 Administrator 工具中设置操作系统配置文件的环境变量。要为操作系统配置文件设置环境变量，请单击 **安全 > 操作系统配置文件**。编辑操作系统配置文件的属性，并设置环境变量。

在使用 Kerberos 身份验证的域中使用操作系统配置文件

您可以在 Informatica 域（在使用 Kerberos 身份验证的网络中运行）中使用操作系统配置文件。

当您使用的操作系统配置文件所在的域在使用 Kerberos 身份验证的网络中运行时，请考虑以下规则和准则：

- 操作系统配置文件的用户帐户必须是用于 Kerberos 身份验证的 Active Directory 服务中的主体，并且必须导入到 Informatica 域中的 LDAP 安全域。
- 用户帐户必须具有操作系统配置文件用户帐户可以访问的 Kerberos 凭据缓存文件。每个操作系统配置文件用户帐户都必须有单独的凭据缓存文件。
- 操作系统配置文件用户帐户的凭据缓存文件必须是可转发文件。例如，如果使用 *kinit* 实用程序创建凭据缓存文件，则必须包括 `-f` 选项。
- 当您运行使用操作系统配置文件的工作流时，操作系统配置文件用户帐户的凭据缓存文件必须可用。
- 操作系统配置文件用户帐户的凭据缓存文件必须始终包含最新凭据。您可以运行作业计划程序实用程序（如 *cron*），以定期更新凭据缓存文件中的用户凭据。

- 您必须设置操作系统配置文件的以下环境变量：

INFA_OSPI_SECURITY_DOMAIN

将值设置为包含操作系统配置文件用户帐户的安全域的名称。如果用户帐户位于 Kerberos 的用户域安全域中，则无需设置此变量。Kerberos 的用户域安全域是在安装过程中创建的安全域，具有与 Kerberos 用户域相同的名称。

KRB5_CONFIG

将值设置为 Kerberos 配置文件的路径和文件名。Kerberos 配置文件的名称为 *krb5.conf*。

KRB5CCNAME

将值设置为操作系统配置文件用户帐户的 Kerberos 凭据缓存文件的路径和文件名。

可以在 Administrator 工具中设置操作系统配置文件的环境变量。要为操作系统配置文件设置环境变量，请单击**安全 > 操作系统配置文件**。编辑操作系统配置文件的属性，并设置环境变量。

帐户锁定

为了提高 Informatica 域的安全性，管理员可以在用户多次登录失败后强制锁定包括其他管理员用户在内的域用户帐户。

管理员可以指定用户帐户被锁定前用户可以进行的失败登录尝试次数。如果帐户被锁定，管理员可以在 Informatica 域解除帐户锁定。

解除用户帐户锁定时，管理员可以选择“解除用户锁定并重置密码”选项以重置用户密码。管理员可以向用户发送电子邮件，要求用户在再次登录域之前先更改密码。要使域在用户的密码重置时向用户发送电子邮件，请配置该域的电子邮件服务器设置。

如果用户被锁定而无法登录 Informatica 域和 LDAP 服务器，Informatica 管理员可以在 Informatica 域中解除用户帐户锁定。除非 LDAP 管理员同时在 LDAP 服务器中解除用户帐户锁定，否则用户无法登录 Informatica 域。

注意：如果 Informatica 域使用 Kerberos 网络身份验证，则无法为用户帐户配置锁定。Administrator 工具的**安全**选项卡中不提供**帐户管理**视图。

配置帐户锁定

选择帐户锁定选项，以在多次登录失败之后锁定 Informatica 域中的用户帐户。

1. 在 Administrator 工具中，单击**安全 > 帐户管理**。
2. 在**帐户锁定配置**部分中，单击**编辑**。

3. 设置以下属性：

属性	说明
启用帐户锁定	登录失败超过指定次数后，强制锁定 Informatica 域用户帐户。默认情况下，此选项不强制锁定管理员用户帐户。必须选择 启用管理帐户锁定 选项，才能强制锁定管理员用户帐户。
启用管理帐户锁定	登录失败超过指定次数后，强制锁定 Informatica 域管理员用户帐户。必须选择 启用帐户锁定 选项，才能强制锁定管理员用户帐户。
最多登录尝试次数	指定锁定 Informatica 域的用户帐户之前允许的连续登录失败的最多次数。

帐户锁定的规则和准则

为 Informatica 用户实施帐户锁定时，请考虑以下规则和准则：

- 如果某一应用程序服务在某个用户帐户下运行，而为应用程序服务提供了错误的密码，如果应用程序服务尝试启动，该用户帐户可以被锁定。数据集成服务、Web 服务中心服务和 PowerCenter 集成服务是弹性应用程序服务，它们使用一个用户名和密码进行模型存储库服务或 PowerCenter 存储库服务身份验证。如果数据集成服务、Web 服务中心服务或 PowerCenter 集成服务在登录失败后不断尝试重新启动，域最终会锁定相关的用户帐户。
- 如果 LDAP 用户帐户被锁定而无法登录 Informatica 域和 LDAP 身份验证服务器，Informatica 域管理员可以在 Informatica 域中解除帐户锁定。LDAP 管理员可以在 LDAP 服务器中解除锁定用户帐户。
- 如果在 Informatica 域和 LDAP 服务器中启用帐户锁定，请在 Informatica 域和 LDAP 服务器中为登录失败配置相同的阈值，以避免混淆帐户锁定策略。
- 如果没有在 Informatica 域中启用帐户锁定，但用户被锁定，请验证该用户没有在 LDAP 服务器中锁定。

第 9 章

特权和角色

本章包括以下主题：

- [特权, 118](#)
- [角色, 119](#)
- [域特权, 120](#)
- [分析服务特权, 127](#)
- [内容管理服务特权, 128](#)
- [数据集成服务特权, 128](#)
- [Mass Ingestion 服务特权, 129](#)
- [Metadata Manager 服务特权, 129](#)
- [模型存储库服务特权, 132](#)
- [PowerCenter 存储库服务特权, 133](#)
- [PowerExchange 侦听器服务特权, 145](#)
- [PowerExchange 日志记录器服务特权, 146](#)
- [计划程序服务特权, 147](#)
- [Test Data Manager 服务特权, 147](#)
- [管理角色, 156](#)
- [将特权和角色分配给用户和组, 160](#)
- [查看对服务有特权的用户, 161](#)
- [特权和角色故障排除, 161](#)

特权

特权确定了用户可以在应用程序客户端中执行的操作。Informatica 包括以下特权：

- 域特权。决定了用户可以使用 Administrator 工具以及 infacmd 和 pmrep 命令行程序对 Informatica 域执行的操作。
- 分析服务特权。决定用户可以使用 Informatica Analyst 执行的操作。
- 内容管理服务特权。决定用户可以使用 Informatica Developer tool 和 Informatica Analyst 工具中的引用表执行的操作。
- 数据集成服务特权。决定用户可以使用 Administrator 工具和 infacmd 命令行程序对应用程序执行的操作。此特权还决定用户是否能够向下钻取和导出配置文件结果。

- Mass Ingestion 服务特权。决定了用户可以使用 Mass Ingestion 工具执行的操作。
- Metadata Manager 服务特权。决定用户可以使用 Metadata Manager 执行的操作。
- 模型存储库服务特权。决定用户可以使用 Informatica Analyst 和 Informatica Developer 对项目执行的操作。
- PowerCenter 存储库服务特权。决定用户可以使用 Repository Manager、Designer、Workflow Manager、Workflow Monitor 以及 pmrep 和 pmcmd 命令执行程序执行的 PowerCenter 存储库操作。
- PowerExchange 应用程序服务特权。决定用户可以使用 infacmd pwx 命令对 PowerExchange 侦听器服务和 PowerExchange 日志记录器服务执行的操作。
- 计划程序服务特权。决定了用户可以使用计划程序服务执行的操作。
- Test Data Manager 服务特权。决定用户可以使用 Test Data Manager 执行的数据发现、数据屏蔽、数据子集和测试数据生成任务。

特权确定了用户可以在应用程序客户端中执行的操作。Informatica 提供了域特权，这些特权决定用户可以使用 Administrator 工具执行的操作。

您针对应用程序服务将特权分配给用户和组。可以针对服务类型相同的每项应用程序服务将不同的特权分配给用户。

您可以在 Administrator 工具的**安全**选项卡中为用户和组分配特权。

Administrator 工具将特权组织到级别中。特权在其包含的特权下列出。某些特权包括其他特权。将特权分配给用户和组时，Administrator 工具还分配包含的所有特权。

特权组

域和应用程序服务特权组织到特权组中。特权组是一组特权，用于定义常见用户操作。例如，域特权包括以下特权组：

- 工具。包括登录 Administrator 工具的特权。
- 安全管理。包括管理用户、组、角色和特权的特权。
- 域管理。包括管理域、文件夹、节点、网格、许可证和应用程序服务的特权。
- 安全管理。包括管理用户、组、角色和特权的特权。
- 域管理。包括管理域、文件夹、节点、网格、许可证和应用程序服务的特权。
- 工具。包括登录 Administrator 工具的特权。
- 监视。包括监视 Ultra Messaging 部署和查看统计信息的特权。

提示: 将特权分配给用户和用户组时，可以选择一个特权组以分配该组中的所有特权。

角色

角色是指向用户或组分配的一组特权。组织中的每个用户都具有特定角色，而无论该用户属于开发人员、管理员、基本用户还是高级用户。

例如，PowerCenter 开发人员角色包括开发人员执行的所有 PowerCenter 存储库服务特权或操作。

可以向域或域中应用程序服务的用户和组分配角色。

提示: 如果您将用户组织到组中，然后将角色和权限分配给组，则可以简化用户管理任务的过程。例如，如果某个用户在组织中的职位发生变化，则可以将其移至其他组。如果某个新用户加入了组织，请将其添加到某个组中。

这些用户将继承分配给组的角色和权限。您不需要重新分配特权、角色和权限。有关详细信息，请参阅以下 Informatica 入门知识库文章：

<https://kb.informatica.com/h2l/HowTo%20Library/1/0236-GroupsAndRolesToManageAccessControl.pdf>。

提示: 如果您将用户组织到组中，然后将角色和权限分配给组，则可以简化用户管理任务的过程。例如，如果某个用户在组织中的职位发生变化，则可以将其移至其他组。如果某个新用户加入了组织，请将其添加到某个组中。这些用户将继承分配给组的角色和权限。您不需要重新分配特权、角色和权限。

域特权

域特权决定用户可以使用 Administrator 工具以及 infacmd 和 pmrep 命令执行程序执行的操作。

下表介绍了每个域特权组：

特权组	说明
安全管理	包括管理用户、组、角色和特权的特权。
域管理	包括管理域、文件夹、节点、网格、许可证、应用程序服务、连接和群集配置的特权。
监视	包括配置监视统计信息和报告、查看集成对象的监视以及访问监视的特权。
工具	包括登录 Administrator 工具的特权。
云管理	包括在 Administrator 工具中添加 Informatica Cloud 组织以及查看它们的特权。

特权组	说明
安全管理	包括管理用户、组、角色和特权的特权。
域管理	包括管理域、应用程序服务、连接和群集配置的特权。
监视	包括监视 UM 部署和查看统计信息的特权。
工具	包括登录 Administrator 工具的特权。

安全管理特权组

安全管理特权组中的特权和域对象权限决定用户可以执行的安全管理操作。

某些安全管理任务由管理员角色决定，而不是由特权或权限决定。

某些安全管理任务由管理员角色决定，而不是由特权或权限决定。分配了域的管理员角色的用户可以完成以下任务：

- 创建、编辑和删除操作系统配置文件。
- 授予对操作系统配置文件的权限。

注意: 要在 Administrator 工具中完成安全管理任务，用户还必须具有访问 Informatica Administrator 特权。

授予特权和角色特权

分配了授予特权和角色特权的用户可以将特权和角色分配给用户和组。

下表列出了所需的权限以及用户可以使用授予特权和角色特权执行的操作：

权限对象	说明
域或应用程序服务	用户能够执行以下操作： <ul style="list-style-type: none">- 针对域或应用程序服务将特权和角色分配给用户和组。- 编辑和删除分配给用户和组的特权和角色。

管理用户、组和角色特权

分配了管理用户、组和角色特权的用户可以配置 LDAP 身份验证并管理用户、组和角色。

管理用户、组和角色特权包括授予特权和角色特权。

下表列出了所需的权限以及用户可以使用管理用户、组和角色特权执行的操作：

权限对象	说明
-	用户能够执行以下操作： <ul style="list-style-type: none">- 配置该域的 LDAP 身份验证。- 创建、编辑和删除用户、组和角色。- 导入 LDAP 用户和组。
操作系统配置文件	用户能够编辑操作系统配置文件属性。

域管理特权组

用户可以执行的域管理操作取决于域管理组中的特权以及对域对象的权限。

某些域管理任务由管理员角色决定，而不是由特权或权限决定。分配了域的管理员角色的用户可以完成以下任务：

- 配置域属性。
- 配置群集配置。
- 授予对域的权限。
- 管理和清除日志事件。
- 接收域警告。
- 运行许可证报告。
- 查看用户活动日志事件。
- 关闭域。
- 访问服务升级向导。

分配了域对象权限但未分配任何特权的用户可以完成部分域管理任务。下表列出了仅将域对象权限分配给用户时这些用户可以执行的操作：

权限对象	说明
域	用户可以执行以下操作： <ul style="list-style-type: none">- 查看域属性和日志事件。- 配置监视设置。
文件夹	用户可以查看文件夹属性。
应用程序服务	用户可以查看应用程序服务属性和日志事件。
许可证对象	用户可以查看许可证对象属性。
网格	用户可以查看网格属性。
节点	用户可以查看节点属性。
Web 服务中心	用户可以运行 Web 服务报告。

注意: 要在 Administrator 工具中完成域管理任务，用户还必须具有访问 Informatica Administrator 特权。

管理服务执行特权

分配了管理服务执行特权的用户可以启用和禁用应用程序服务以及接收应用程序服务警告。

下表列出了所需的权限以及用户可以使用管理服务执行特权执行的操作：

权限对象	说明
应用程序服务	用户能够执行以下操作： <ul style="list-style-type: none">- 启用和禁用应用程序服务以及服务进程。要启用和禁用 Metadata Manager 服务，用户还必须对关联的 PowerCenter 集成服务和 PowerCenter 存储库服务具有权限。- 接收应用程序服务警告。

权限对象	说明
应用程序服务	用户能够执行以下操作： <ul style="list-style-type: none">- 启用和禁用应用程序服务以及服务进程。- 接收应用程序服务警告。

管理服务特权

分配了管理服务特权的用户可以创建、配置、移动、删除以及授予对应用程序服务和许可证对象的权限。

管理服务特权包括管理服务执行特权。

下表列出了所需的权限以及用户可以使用管理服务特权执行的操作：

权限对象	说明
域或父文件夹	用户能够创建许可证对象。
域或父文件夹、运行应用程序服务的节点或网格、许可证对象以及任何关联的应用程序服务	用户能够创建应用程序服务。
应用程序服务	用户能够执行以下操作： <ul style="list-style-type: none"> - 配置应用程序服务。 - 授予对应用程序服务的权限。
原始和目标文件夹	用户能够将应用程序服务或许可证对象从一个文件夹移至另一个文件夹。
域或父文件夹和应用程序服务	用户能够删除应用程序服务。
分析服务	用户能够创建和删除审计跟踪表。
Metadata Manager 服务	用户能够执行以下操作： <ul style="list-style-type: none"> - 备份 Metadata Manager 存储库内容。 - 删除 Metadata Manager 存储库内容。 - 升级 Metadata Manager 服务的内容。 注意: 用户必须属于默认管理员组，才能创建或还原 Metadata Manager 存储库内容。
Metadata Manager 服务 PowerCenter 存储库服务	用户能够为 Metadata Manager 还原 PowerCenter 存储库。
模型存储库服务	用户能够执行以下操作： <ul style="list-style-type: none"> - 创建和删除模型存储库内容。 - 创建、删除和重新编制搜索索引。 - 通过操作菜单或命令行升级模型存储库服务的内容。用户还必须具有模型存储库服务的创建、编辑和删除项目的特权，以及对项目的写入权限。
PowerCenter 集成服务	用户能够在安全模式下运行 PowerCenter 集成服务。
PowerCenter 存储库服务	用户能够执行以下操作： <ul style="list-style-type: none"> - 备份、还原和升级 PowerCenter 存储库。 - 配置 PowerCenter 存储库的数据沿袭。 - 复制其他 PowerCenter 存储库中的内容。 - 关闭用户连接和释放 PowerCenter 存储库锁定。 - 创建和删除 PowerCenter 存储库内容。 - 创建、编辑和删除 PowerCenter Repository Manager 中的可重用元数据扩展。 - 为 PowerCenter 存储库启用版本控制。 - 管理 PowerCenter 存储库域。 - 在 PowerCenter Repository Manager 中的存储库级别执行对象版本的高级清除。 - 注册和取消注册 PowerCenter 存储库插件。 - 以独占模式运行 PowerCenter 存储库。 - 向用户发送 PowerCenter 存储库通知。 - 更新 PowerCenter 存储库统计信息。 - 升级 PowerCenter 存储库服务的内容。

权限对象	说明
Test Data Manager 服务	用户能够执行以下操作： - 创建并删除 Test Data Manager 存储库内容。 - 升级 Test Data Manager 服务的内容。
许可证对象	用户能够执行以下操作： - 编辑许可证对象。 - 授予对许可证对象的权限。
许可证对象和应用程序服务	用户无法将许可证分配给应用程序服务。
域或父文件夹和许可证对象	用户能够删除许可证对象。

权限对象	说明
运行应用程序服务的域以及任何关联的应用程序服务	用户能够创建应用程序服务。
应用程序服务	用户能够执行以下操作： - 配置应用程序服务。 - 授予对应用程序服务的权限。
模型存储库服务	用户能够执行以下操作： - 创建和删除模型存储库内容。 - 创建、删除和重新编制搜索索引。

管理节点和网格特权

分配了管理节点和网格特权的用户可以创建、配置、移动、删除、关闭和授予对节点和网格的权限。

下表列出了所需的权限以及用户在拥有管理节点和网格特权时可以执行的操作：

权限对象	说明
域或父文件夹	用户能够创建节点。
分配给网格的域或父文件夹和节点	用户能够创建网格。
节点或网格	用户能够执行以下操作： - 配置和关闭节点和网格。 - 授予对节点和网格的权限。
原始和目标文件夹	用户能够将节点和网格从一个文件夹移到另一个文件夹。
域或父文件夹和节点或网格	用户能够删除节点和网格。

管理域文件夹特权

分配了管理域文件夹特权的用户可以创建、编辑、移动、删除和授予对域文件夹的权限。

下表列出了所需的权限以及用户可以使用管理域文件夹特权执行的操作：

权限对象	说明
域或父文件夹	用户能够创建文件夹。
文件夹	用户能够执行以下操作： <ul style="list-style-type: none">- 编辑文件夹。- 授予对文件夹的权限。
原始和目标文件夹	用户能够将文件夹从一个父文件夹移动到另一个父文件夹。
域或父文件夹和正在删除的文件夹	用户能够删除文件夹。

管理连接特权

分配了管理连接特权的用户可以在 Administrator 工具、Analyst 工具、Developer 工具以及 infacmd 命令行程序中创建、编辑和删除连接。用户还可以在 Developer 工具中复制连接，并且能够在 Administrator 工具和 infacmd 命令行程序中授予对连接的权限。

分配了“管理连接”特权的用户还可以在 Administrator 工具和 infacmd 命令行程序中创建、刷新和删除群集配置，以及设置和清除配置属性。

分配了连接权限但未分配管理连接特权的用户可以执行以下连接管理操作：

- 查看所有连接元数据（密码除外）。需要对连接具有读取权限。
- 预览数据或者运行映射、结果卡或配置文件。需要对连接具有执行权限。

下表列出了所需的权限以及用户可以使用管理连接特权执行的操作：

权限	说明
-	用户能够创建连接和群集配置。
对连接的写入权限	用户能够复制、编辑和删除连接。
对连接的授予权限	用户能够授予和撤消对连接的权限。
对群集配置的写入权限	用户能够创建、刷新和删除群集配置。用户能够设置和清除群集配置属性。

监视特权组

监视特权组中的特权决定哪些用户可以查看和配置监视。

下表列出了所需的权限以及用户可以使用管理监视组中的特权执行的操作：

父特权	特权	权限对象	说明
管理监视	监视配置	域	用户可以配置监视设置。
管理监视	报告和统计信息设置	域	用户可以配置监视统计信息和报告。
视图	查看用户所属的组中所有用户的作业	域	组中用户可以监视组中其他用户运行的作业。如果用户属于多个组，则该用户能够从所有组中查看作业。
查看用户所属的组中所有用户的作业	查看其他用户的作业	域	用户可以查看其他用户的作业。
视图	查看统计信息	域	用户可以查看摘要统计信息视图和域对象的统计信息。 注意: 在使用 Kerberos 身份验证的域中，用户还必须对监视模型存储库服务具有管理员角色，才能查看摘要统计信息以及域对象的统计信息。
视图	查看报告	域	用户可以查看域对象的报告。
访问监视	从 Analyst 工具进行访问	域	用户可以访问 Analyst 工具中的作业状态工作区。
访问监视	从 Developer tool 进行访问	域	用户可以从 Developer tool 访问监视工具。
访问监视	从 Administrator 工具进行访问	域	用户可以访问 Administrator 工具中的“监视”选项卡。
不适用	对作业执行操作	域	用户可以执行以下操作： <ul style="list-style-type: none"> - 中止作业。 - 重新发出映射作业。 - 查看作业日志。

用户访问 Monitoring 工具不需要“访问 Informatica Administrator”特权。

工具特权组

域工具组中的特权决定哪些用户能够访问 Administrator 工具。

下表列出了所需的权限以及用户可以使用工具组中的特权执行的操作：

特权	说明
访问 Informatica Administrator	用户可以执行以下操作： <ul style="list-style-type: none"> - 登录 Administrator 工具。 - 在 Administrator 工具中管理自己的用户帐户。 - 导出日志事件。

用户必须拥有“访问 Informatica Administrator”特权才能在 Administrator 工具中完成任务。运行 infacmd 命令或访问 Monitoring 工具不需要“访问 Informatica Administrator”特权。

云管理特权组

云管理组中的特权决定哪些用户可以查看和配置 Informatica Cloud 组织。

下表列出了所需的权限以及用户可以使用 Cloud 云管理组中的特权执行的操作：

特权	权限对象	说明
查看组织	域	用户可以查看 Informatica Cloud 组织及关联的安全代理和云连接。
管理组织	域	用户可以在 Administrator 工具中添加 Informatica Cloud 组织。

分析服务特权

分析服务特权决定许可用户使用 Analyst 工具可以对项目执行的操作。

下表列出了管理项目和项目中的对象所需的特权和权限：

特权	权限	说明
运行配置文件和结果卡	对项目执行读取操作。 针对关系数据源连接的执行操作。	用户能够在 Analyst 工具中运行许可用户的配置文件和结果卡。
访问映射规范	对项目执行读取操作。	用户能够在 Analyst 工具中访问许可用户的映射规范。
加载映射规范结果	对项目执行写入操作。	用户能够将许可用户的映射规范的结果加载到表或平面文件。 注意: 默认情况下，选择此特权后还会授予访问映射规范特权。
管理词汇表	-	用户能够管理业务词汇表。
查看词汇表	-	用户可以在库工作区查看已发布的 Business Glossary 资产。这等于在词汇表安全工作区提供词汇表和 Glossary 资产的读取权限。
工作区访问	-	用户能够在 Analyst 工具中访问以下工作区： - 设计工作区。 - 发现工作区。 - 词汇表工作区。 - 结果卡工作区。 注意: 选择此特权后，还会授予在 Analyst 工具中访问项目的特权。如果用户没有此特权，则必须拥有设计工作区、发现工作区、词汇表工作区或结果卡工作区特权以访问项目。
设计工作区	-	用户能够访问设计工作区。
发现工作区	-	用户能够访问发现工作区。
词汇表工作区	-	用户能够访问词汇表工作区。
结果卡工作区	-	用户能够访问结果卡工作区。

内容管理服务特权

内容管理服务特权确定授权用户可以对引用表执行的操作。

下表列出了管理引用表所需的特权和权限：

特权	权限	说明
创建引用表	对项目执行写入操作	<ul style="list-style-type: none">- 在 Analyst 和 Developer 工具中创建一个引用表。- 通过 infacmd rtm 导入创建一个引用表。- 将引用表对象导入模型存储库。- 在 Analyst 和 Developer 工具中复制一个引用表。- 通过配置文件数据创建一个引用表。 注意： “创建”特权在默认情况下授予“编辑”特权。
编辑引用表数据和元数据	对项目执行读取操作	<ul style="list-style-type: none">- 在 Developer 工具和 Analyst 工具中编辑引用表数据值。- 将配置文件数据添加到引用表。- 添加或删除引用表中的列。更改引用表元数据（如列名、说明和默认值）。

数据集成服务特权

数据集成服务特权决定用户可以使用 Administrator 工具以及 infacmd 命令行程序对应用程序执行的操作。这些特权还决定用户是否能够使用 Analyst 工具和 Developer tool 向下钻取和导出配置文件结果。

数据集成服务特权决定用户可以使用 Administrator 工具以及 infacmd 命令行程序对应用程序执行的操作。这些特权还决定用户是否能够使用 Developer tool 向下钻取和导出配置文件结果。

下表列出了在应用程序管理特权组中具有特权的用户可以执行的操作：

特权名称	说明
管理应用程序	用户可以执行以下操作： <ul style="list-style-type: none">- 备份应用程序以及将其还原到文件。- 将应用程序部署到数据集成服务以及解析名称冲突。- 在部署后启动应用程序。- 查找应用程序。- 启动或停止应用程序中的对象。- 配置应用程序属性。

下表列出了所需的权限以及用户可以使用剖析管理特权组中的特权执行的操作：

特权名称	权限对象	说明
向下钻取和导出结果	对项目执行读取操作 向下钻取实时数据时还需要针对关系数据源连接的执行操作	用户可以执行以下操作： <ul style="list-style-type: none">- 向下钻取剖析结果。- 导出剖析结果。

Mass Ingestion 服务特权

Mass Ingestion 服务特权决定了用户可以使用 Mass Ingestion 工具执行的操作。

下表列出了具有 Mass Ingestion 服务特权的用户可执行的操作：

特权	说明
Mass Ingestion 规范访问	用户可以执行以下操作： <ul style="list-style-type: none">- 浏览所有 Mass Ingestion 规范- 编辑 Mass Ingestion 规范- 运行 Mass Ingestion 规范- 删除 Mass Ingestion 规范

注意：如果用户不具有“Mass Ingestion 规范访问”特权或域的管理员角色，则只能对自己创建的 Mass Ingestion 规范执行这些操作。

Metadata Manager 服务特权

Metadata Manager 服务特权确定了用户可以使用 Metadata Manager 执行的 Metadata Manager 操作。

下表介绍了每个 Metadata Manager 特权组：

特权组	说明
目录	包括用于管理 Metadata Manager 界面的“浏览”页中对象的特权。
加载	包括用于管理 Metadata Manager 界面的“加载”页中对象的特权。
模型	包括用于管理 Metadata Manager 界面的“模型”页中对象的特权。
安全	包括用于管理 Metadata Manager 界面的“安全”页中对象的特权。

目录特权组

“目录”特权组中的特权决定用户在 Metadata Manager 应用程序的浏览选项卡上可以执行的任务。具有执行某项操作的特权的用户还需要具有相应的权限才能对某个特定对象执行该操作。可在 Metadata Manager 应用程序的安全选项卡上配置这些权限。

下表列出了“目录”特权组中的特权和对某一对象执行某项任务所需的权限：

特权	包括特权	权限	说明
共享快捷方式	不适用	写入	用户能够与其他用户和组共享包含快捷方式的文件夹。
查看沿袭	不适用	读取	用户能够执行以下操作： <ul style="list-style-type: none">- 对元数据对象、类别和业务术语运行数据沿袭分析。- 通过 PowerCenter Designer 运行数据沿袭分析。用户还必须拥有对 PowerCenter 存储库文件夹的读取权限。

特权	包括特权	权限	说明
查看相关目录	不适用	读取	用户能够查看相关目录。
查看配置文件结果	不适用	读取	用户能够查看来自关系源的目录中的元数据对象的剖析信息。
查看目录	不适用	读取	用户能够执行以下操作： <ul style="list-style-type: none"> - 查看元数据目录中的资源和元数据对象。 - 搜索元数据目录。
查看关系	不适用	读取	用户能够查看元数据对象、类别和业务术语的关系。
管理关系	查看关系	写入	用户能够创建、编辑和删除自定义元数据对象、类别和业务术语的关系。
查看注释	不适用	读取	用户能够查看元数据对象、类别和业务术语的注释。
发布注释	查看注释	写入	用户能够添加元数据对象、类别和业务术语的注释。
删除注释	<ul style="list-style-type: none"> - 发布注释 - 查看注释 	写入	用户能够删除元数据对象、类别和业务术语的注释。
查看链接	不适用	读取	用户能够查看元数据对象、类别和业务术语的链接。
管理链接	查看链接	写入	用户能够创建、编辑和删除元数据对象、类别和业务术语的链接。
查看词汇表	不适用	读取	用户能够执行以下操作： <ul style="list-style-type: none"> - 在词汇表视图中查看业务词汇表。 - 搜索业务词汇表。
管理对象	不适用	写入	用户能够执行以下操作： <ul style="list-style-type: none"> - 编辑目录中的元数据对象。 - 创建、编辑和删除自定义元数据对象。用户还必须拥有“查看模型”特权。 - 创建、编辑和删除自定义元数据资源。用户还必须拥有“管理资源”特权。

加载特权组

“加载”特权组中的特权决定用户在 Metadata Manager 应用程序的**加载**选项卡上可以执行的任务。具有执行某项操作的特权的用户还需要具有相应的权限才能对某个特定对象执行该操作。可在 Metadata Manager 应用程序的**安全**选项卡上配置这些权限。

下表列出了管理 Metadata Manager 仓库中的资源实例所需的特权：

特权	包括特权	权限	说明
查看资源	-	读取	用户能够执行以下操作： <ul style="list-style-type: none">- 在 Metadata Manager 仓库中查看资源和资源属性。- 导出资源配置。- 下载 Metadata Manager Agent 安装程序。
加载资源	查看资源	写入	用户能够执行以下操作： <ul style="list-style-type: none">- 将资源的元数据加载到 Metadata Manager 仓库中。*- 创建已连接资源中对象之间的链接以供数据沿袭。- 配置资源的搜索索引编制设置。- 导入资源配置。
管理计划	查看资源	写入	用户能够执行以下操作： <ul style="list-style-type: none">- 创建和编辑计划。- 将计划添加到资源。
清除元数据	查看资源	写入	用户能够从 Metadata Manager 仓库中删除资源的元数据。
管理资源	<ul style="list-style-type: none">- 清除元数据- 查看资源	写入	用户能够创建、编辑和删除资源。
* 要加载 Business Glossary 资源的元数据，需要“加载资源”、“管理资源”和“查看模型”特权。			

模型特权组

“模型”特权组中的特权决定用户在 Metadata Manager 应用程序的**模型**选项卡上可以执行的任务。您不能配置对模型的权限。

下表列出了管理模型所需的特权：

特权	包括特权	权限	说明
查看模型	-	-	用户能够打开模型和类，并查看模型和类属性。查看类的关系和属性。
管理模型	查看模型	-	用户能够创建、编辑和删除自定义模型。向封装式通用模型添加属性。
导出/导入模型	查看模型	-	用户能够导入和导出自定义模型。导入和导出修改的封装式通用模型。

安全特权组

“安全”特权组中的特权决定用户在 Metadata Manager 应用程序的**安全**选项卡上可以执行的任务。

默认情况下，安全特权组中的“管理目录权限”特权分配给管理员，或者分配给具有 Metadata Manager 服务的管理员角色的用户。可以为其他用户分配“管理目录权限”特权。

下表列出了管理 Metadata Manager 的安全所需的特权和权限：

特权	包括特权	权限	说明
管理目录权限	-	完全控制	用户能够执行以下操作： <ul style="list-style-type: none"> - 为用户和组分配针对资源、元数据对象、类别和业务术语的权限。 - 编辑针对资源、元数据对象、类别和业务术语的权限。

模型存储库服务特权

模型存储库服务特权决定用户可以使用 Informatica Analyst 和 Informatica Developer 对项目执行的操作。

模型存储库服务特权决定用户可以使用 Informatica Developer 对项目执行的操作。

模型存储库对象权限确定用户可以对项目中的对象完成的任务。

下表列出了所需的权限以及用户可以使用模型存储库服务特权执行的操作：

特权	权限	说明
N/A	对项目执行读取操作	用户可以查看项目和项目中的对象。
N/A	对项目执行写入操作	用户可以创建、编辑和删除项目中的对象。
N/A	对项目执行授予操作	用户可以授予和撤消用户和组对项目的权限。
访问 Analyst	N/A	用户可以通过 Analyst 工具访问模型存储库。
访问 Developer	N/A	用户可以从 Developer tool 访问模型存储库。
创建、编辑和删除项目	N/A	用户可以创建项目。
创建、编辑和删除项目	对项目执行写入操作	用户可以执行以下操作： <ul style="list-style-type: none"> - 编辑项目。 - 删除项目（如果用户创建了项目）。 - 升级模型存储库服务的内容。要通过操作菜单或通过命令行升级服务，用户还必须拥有域的“管理服务”特权和针对模型存储库服务的权限。要使用服务升级向导升级服务，用户还必须拥有域的管理员角色。
管理数据域	N/A	用户可以在数据域词汇表中创建、编辑和删除数据域。此特权是 数据域管理 特权组的一部分。
管理通知	N/A	用户可以配置结果卡通知。此特权是 剖析管理 特权组的一部分。

特权	权限	说明
管理基于团队的开发	N/A	用户可以管理模型存储库对象的锁定或未锁定状态。如果模型存储库与版本控制系统集成，用户可以管理对象的签出或签入状态。用户还可以管理已签出对象的所有权。
显示安全详细信息	N/A	用户可以查看以下详细信息： <ul style="list-style-type: none"> - 用户对其没有读取权限的对象的名称。 - 错误和警告消息的详细信息。

特权	权限	说明
N/A	对项目执行读取操作	用户可以查看项目和项目中的对象。
N/A	对项目执行写入操作	用户可以创建、编辑和删除项目中的对象。
N/A	对项目执行授予操作	用户可以授予和撤消用户和组对项目的权限。
访问 Developer	N/A	用户可以从 Developer tool 访问模型存储库。
创建、编辑和删除项目	N/A	用户可以执行以下操作： <ul style="list-style-type: none"> - 创建项目。 - 升级模型存储库服务。
创建、编辑和删除项目	对项目执行写入操作	用户可以执行以下操作： <ul style="list-style-type: none"> - 编辑项目。 - 删除项目（如果用户创建了项目）。
显示安全详细信息	N/A	用户可以查看以下详细信息： <ul style="list-style-type: none"> - 用户对其没有读取权限的对象的名称。 - 错误和警告消息的详细信息。

PowerCenter 存储库服务特权

PowerCenter 存储库服务特权决定了用户可以使用 PowerCenter Repository Manager、Designer、Workflow Manager、Workflow Monitor 以及 pmrep 和 pmcmd 命令行程序执行的 PowerCenter 存储库操作。

下表介绍了 PowerCenter 存储库服务的每个特权组：

特权组	说明
工具	包括访问 PowerCenter 客户端工具和命令行程序的特权。
文件夹	包括管理存储库文件夹的特权。
设计对象	包括管理业务组件、映射参数和变量、映射、Mapplet、转换和用户定义的函数的特权。
源和目标	包括管理多维数据集、维度、源定义和目标定义的特权。

特权组	说明
运行时对象	包括管理会话配置对象、任务、工作流和工作集的特权。
全局对象	包括管理连接对象、部署组、标签和查询的特权。

用户必须拥有对 PowerCenter 存储库服务的管理服务域特权和权限才能在 Repository Manager 中执行以下操作：

- 在 PowerCenter 存储库级别执行对象版本的高级清除。
- 创建、编辑和删除可重用元数据扩展。

工具特权组

PowerCenter 存储库服务工具特权组中的特权决定用户可以访问的 PowerCenter 客户端工具和命令行程序。

下表列出了针对工具组中的特权用户可以执行的操作：

特权	权限	说明
访问 Designer	-	用户能够使用 Designer 连接到 PowerCenter 存储库。
访问 Repository Manager	-	用户能够执行以下操作： <ul style="list-style-type: none"> - 使用 Repository Manager 连接到 PowerCenter 存储库。 - 运行 <i>pmrep</i> 命令。
访问 Workflow Manager	-	用户能够执行以下操作： <ul style="list-style-type: none"> - 使用 Workflow Manager 连接到 PowerCenter 存储库。 - 从 Workflow Manager 中移除 PowerCenter 集成服务。
访问 Workflow Monitor	-	用户能够执行以下操作： <ul style="list-style-type: none"> - 使用 Workflow Monitor 连接到 PowerCenter 存储库。 - 在 Workflow Monitor 中连接到 PowerCenter 集成服务。

注意：如果 PowerCenter 集成服务在安全模式下运行，用户必须具备关联的 PowerCenter 存储库服务的管理员角色。

所有用户均需要“工具”特权组中的相应特权，以完成 PowerCenter 客户端工具和命令行程序中的任务。例如，要在 Repository Manager 中创建文件夹，用户必须具有“创建文件夹”和“访问 Repository Manager”特权。

如果用户有“工具”特权组中的特权，以及 PowerCenter 存储库对象的权限，但没有修改对象类型的特权，则他们仍可以在对象上执行部分操作。例如，用户具有“访问 Repository Manager”特权和部分文件夹的读取权限。用户不具有“文件夹”特权组中的任何特权。用户可以查看文件夹中的对象以及比较文件夹。

文件夹特权组

文件夹管理操作由文件夹特权组、PowerCenter 存储库对象权限和域对象权限中的特权决定。用户在 Repository Manager 中使用 *pmrep* 命令行程序执行文件夹管理操作。

某些文件夹管理任务由文件夹所有权和管理员角色决定，而不是由特权或权限决定。文件夹所有者或分配了 PowerCenter 存储库服务管理员角色的用户可以完成以下文件夹管理任务：

- 如果 PowerCenter 集成服务使用操作系统配置文件，则会将操作系统配置文件分配给文件夹。需要对操作系统配置文件具有权限。

- 更改文件夹所有者。
- 配置文件夹权限。
- 删除文件夹。
- 指定要共享的文件夹。
- 编辑文件夹名称和说明。

分配了文件夹权限但未分配任何特权的用户可以执行部分文件夹管理操作。下表列出了仅将文件夹权限分配给用户时这些用户可以执行的操作：

权限	说明
对文件夹执行读取操作	用户能够执行以下操作： <ul style="list-style-type: none">- 比较文件夹。- 在文件夹中查看对象。

注意：要对文件夹执行操作，用户还必须具有访问 Repository Manager 的特权。

创建文件夹特权

分配了创建文件夹特权的用户可以创建 PowerCenter 存储库文件夹。

下表列出了所需的权限以及用户可以使用创建文件夹特权执行的操作：

权限	说明
-	用户能够创建文件夹。

复制文件夹特权

分配有“复制文件夹”特权的用户能够复制 PowerCenter 存储库中的文件夹或将文件夹复制到其他 PowerCenter 存储库。

下表列出了所需权限以及用户可以使用“复制文件夹”特权执行的操作：

权限	说明
对文件夹执行读取操作	用户能够在同一 PowerCenter 存储库中复制文件夹或将文件夹复制到其他 PowerCenter 存储库。用户还必须拥有目标存储库中的“创建文件夹”特权。

管理文件夹版本

如果您有基于团队的开发选项，请在受版本控制的 PowerCenter 存储库中为用户分配管理文件夹版本特权。用户可以更改文件夹的状态，并在文件夹级别执行对象版本的高级清除。

下表列出了所需的权限以及用户可以使用管理文件夹版本特权执行的操作：

权限	说明
对文件夹执行读取和写入操作	用户能够执行以下操作： <ul style="list-style-type: none">- 更改文件夹的状态。- 在文件夹级别执行对象版本的高级清除。

设计对象特权组

“设计对象”特权组中的特权和 PowerCenter 存储库对象权限确定用户可以在以下设计对象上执行的操作：

- 业务组件
- 映射参数和变量
- 映射
- Mapplet
- 转换
- 用户定义的函数

用户分配了权限，但没有特权可以为设计对象执行某些操作。下表列出了仅将权限分配给用户时这些用户可以执行的操作：

权限	说明
对文件夹执行读取操作	用户能够执行以下操作： <ul style="list-style-type: none">- 比较设计对象。- 作为图像复制设计对象。- 导出设计对象。- 为自定义转换和外部程序生成代码。- 接收 PowerCenter 存储库通知消息。- 在设计对象上运行数据沿袭。用户还必须具有 Metadata Manager 服务的查看沿袭特权，以及对 Metadata Manager 目录中元数据对象的读取权限。- 搜索设计对象。- 查看设计对象、设计对象相关性和设计对象历史记录。
对共享文件夹执行读取操作 对目标文件夹执行读取和写入操作	用户能够创建快捷方式。

注意: 要在设计对象上执行操作，用户必须具有“工具”特权组中的适当权限。

创建、编辑和删除设计对象特权

分配有创建、编辑和删除设计对象特权的用户可以创建、编辑和删除业务组件、映射参数、映射变量、映射、Mapplet、转换以及用户定义的函数。

下表列出了所需的权限以及用户可以使用创建、编辑和删除设计对象特权执行的操作：

权限	说明
对原始文件夹执行读取操作 对目标文件夹执行读取和写入操作	用户能够执行以下操作： <ul style="list-style-type: none">- 将设计对象从一个文件夹复制到另一个文件夹。- 将设计对象复制到其他 PowerCenter 存储库。用户还必须具有目标存储库的创建、编辑和删除设计对象特权。
对文件夹执行读取和写入操作	用户能够执行以下操作： <ul style="list-style-type: none">- 更改有版本控制的设计对象的注释。- 签入和撤消签出通过其自己的用户帐户签出的设计对象。- 签出设计对象。- 复制并粘贴同一文件夹中的设计对象。- 创建、编辑和删除数据配置文件并启动 Profile Manager。用户还必须具有创建、编辑和删除运行时对象的特权。- 创建、编辑和删除设计对象。- 生成和清除 SAP ABAP 程序。- 生成业务内容集成映射。用户还必须具有创建、编辑和删除源和目标的特权。- 使用 Designer 导入设计对象。用户还必须具有创建、编辑和删除源和目标的特权。- 使用 Repository Manager 导入设计对象。用户还必须具有创建、编辑和删除运行时对象以及创建、编辑和删除源和目标的特权。- 还原到以前的设计对象版本。- 验证映射、Mapplet 以及用户定义的函数。

管理设计对象版本

如果拥有基于团队的开发选项，则可以为用户分配有版本控制的 PowerCenter 存储库中的“管理设计对象版本”特权。用户可以更改状态、恢复和清除设计对象版本。用户还可以签入和撤消其他用户所做的签出。

“管理设计对象版本”特权包括“创建、编辑和删除设计对象”特权。

下表列出了所需的权限以及用户可以使用“管理设计对象版本”特权执行的操作：

权限	说明
对文件夹执行读取和写入操作	用户能够执行以下操作： <ul style="list-style-type: none">- 更改设计对象的状态。- 签入和撤消由其他用户签出的设计对象的签出。- 清除设计对象的版本。- 恢复已删除的设计对象。

源和目标特权组

源和目标特权组中的特权以及 PowerCenter 存储库对象权限确定了用户可以对以下源和目标对象执行的操作：

- 多维数据集
- 维度
- 源定义
- 目标定义

分配了权限但未分配任何特权的用户可以执行部分源和目标对象操作。下表列出了仅将权限分配给用户时这些用户可以执行的操作：

权限	说明
对文件夹执行读取操作	用户能够执行以下操作： <ul style="list-style-type: none">- 比较源和目标对象。- 导出源和目标对象。- 预览源数据和目标数据。- 接收 PowerCenter 存储库通知消息。- 在源和目标对象上运行数据沿袭。用户还必须具有 Metadata Manager 服务的查看沿袭特权，以及对 Metadata Manager 目录中元数据对象的读取权限。- 搜索源和目标对象。- 查看源和目标对象、源和目标对象相关性以及源和目标对象历史记录。
对共享文件夹执行读取操作 对目标文件夹执行读取和写入操作	创建快捷方式。

注意: 要对源和目标对象执行操作，用户还必须在工具特权组中具有相应特权。

创建、编辑和删除源和目标特权

分配了创建、编辑和删除源和目标特权的用户可以创建、编辑和删除多维数据集、维度、源定义和目标定义。

下表列出了所需的权限以及用户可以使用创建、编辑和删除源和目标特权执行的操作：

权限	说明
对原始文件夹执行读取操作 对目标文件夹执行读取和写入操作	用户能够执行以下操作： <ul style="list-style-type: none">- 将源和目标对象复制到其他文件夹。- 将源和目标对象复制到其他 PowerCenter 存储库。用户还必须在目标存储库中具有创建、编辑和删除源和目标特权。
对文件夹执行读取和写入操作	用户能够执行以下操作： <ul style="list-style-type: none">- 更改受版本控制的源或目标对象的注释。- 签入和撤消签出通过其自己的用户帐户签出的源和目标对象。- 签出源和目标对象。- 复制并粘贴同一文件夹中的源和目标对象。- 创建、编辑和删除源和目标对象。- 导入 SAP 函数。- 使用 Designer 导入源和目标对象。用户还必须具有创建、编辑和删除设计对象特权。- 使用 Repository Manager 导入源和目标对象。用户还必须有创建、编辑和删除设计对象以及创建、编辑和删除运行时对象的特权。- 生成和执行 SQL 以在关系数据库中创建目标。- 还原为以前的源或目标对象版本。

管理源和目标版本特权

如果拥有基于团队的开发选项，则可以为用户分配有版本控制的 PowerCenter 存储库中的管理源和目标版本特权。用户可以更改状态、恢复和清除源和目标对象的版本。用户还可以签入和撤消其他用户所做的签出。

管理源和目标版本特权包括创建、编辑和删除源和目标特权。

下表列出了所需的权限以及用户可以使用管理源和目标版本特权执行的操作：

权限	说明
对文件夹执行读取和写入操作	用户能够执行以下操作： <ul style="list-style-type: none">- 更改源和目标对象的状态。- 签入和撤消由其他用户签出的源和目标对象的签出。- 清除源和目标对象的版本。- 恢复已删除的源和目标对象。

运行时对象特权组

运行时对象特权组中的特权、PowerCenter 存储库对象权限和域对象权限决定用户可以对以下运行时对象所执行的操作：

- 会话配置对象
- 任务

- 工作流
- 工作集

某些运行时对象任务由管理员角色决定，而不是由特权或权限决定。分配了 PowerCenter 存储库服务的管理员角色的用户可以通过 Workflow Manager 的导航器删除 PowerCenter 集成服务。

分配了权限但未分配特权的用户可以执行部分运行时对象操作。下表列出了仅将权限分配给用户时这些用户可以执行的操作：

权限	说明
对文件夹执行读取操作	用户能够执行以下操作： <ul style="list-style-type: none">- 比较运行时对象。- 导出运行时对象。- 接收 PowerCenter 存储库通知消息。- 搜索运行时对象。- 在会话中使用映射参数和变量。- 查看运行时对象、运行时对象相关项和运行时对象历史记录。
对文件夹的读取和执行权限	停止及中止由自有用户帐户所启动的任务和工作流。 如果 PowerCenter 集成服务在安全模式下运行，用户必须具备关联的 PowerCenter 存储库服务的管理员角色。

注意: 要对运行时对象执行操作，用户还必须在工具特权组中具有相应特权。

创建、编辑和删除运行时对象特权

分配了创建、编辑和删除运行时对象特权的用户可以创建、编辑和删除会话配置对象、任务、工作流和工作集。

下表列出了所需的权限以及用户可以使用创建、编辑和删除运行时对象特权执行的操作：

权限	说明
对原始文件夹执行读取操作 对目标文件夹执行读取和写入操作	用户能够执行以下操作： <ul style="list-style-type: none">- 将任务、工作流或工作集从一个文件夹复制到另一个文件夹。- 将任务、工作流或工作集复制到另一个 PowerCenter 存储库。用户还必须在目标存储库中具有创建、编辑和删除运行时对象特权。
对文件夹执行读取和写入操作	用户能够执行以下操作： <ul style="list-style-type: none">- 在工作流属性中将 PowerCenter 集成服务分配给工作流。- 将服务级别分配给工作流。- 更改有版本控制的运行时对象的注释。- 签入和撤消签出通过其自己的用户帐户签出的运行时对象。- 签出运行时对象。- 在同一文件夹中复制和粘贴任务、工作流和工作集。- 创建、编辑和删除数据配置文件并启动 Profile Manager。用户还必须具有创建、编辑和删除设计对象特权。- 创建、编辑和删除会话配置对象。- 删除和验证任务、工作流和工作集。- 使用 Repository Manager 导入运行时对象。用户还必须具有创建、编辑和删除设计对象以及创建、编辑和删除源和目标的特权。- 使用 Workflow Manager 导入运行时对象。- 还原到以前的对象版本。
对文件夹执行读取和写入操作 对连接对象执行读取操作	用户能够执行以下操作： <ul style="list-style-type: none">- 创建和编辑任务、工作流和工作集。- 替换使用关系数据库连接的所有会话的此连接。

管理运行时对象版本特权

如果拥有基于团队的开发选项，则可以为用户分配有版本控制的 PowerCenter 存储库中的管理运行时对象版本特权。用户可以更改状态、恢复和清除运行时对象版本。用户还可以签入和撤消其他用户所做的签出。

管理运行时对象版本特权包括创建、编辑和删除运行时对象特权。

下表列出了所需的权限以及用户可以使用管理运行时对象版本特权执行的操作：

权限	说明
对文件夹执行读取和写入操作	用户能够执行以下操作： <ul style="list-style-type: none">- 更改运行时对象的状态。- 签入和撤消由其他用户签出的运行时对象的签出。- 清除运行时对象的版本。- 恢复已删除的运行时对象。

监视运行时对象特权

分配了监视运行时对象特权的用户可以在 Workflow Monitor 中监视工作流和任务。

下表列出了所需的权限以及用户可以使用监视运行时对象特权执行的操作：

权限	授予用于以下权限
对文件夹执行读取操作	用户能够执行以下操作： <ul style="list-style-type: none">- 查看 Workflow Monitor 中的运行时对象的属性。- 查看 Workflow Monitor 中的会话和工作流日志。- 查看 Workflow Monitor 中的运行时对象和性能详细信息。 如果 PowerCenter 集成服务在安全模式下运行，用户必须具备关联的 PowerCenter 存储库服务的管理员角色。

执行运行时对象特权

分配了执行运行时对象特权的用户可以启动、冷启动和恢复任务及工作流。

执行运行时对象特权包括监视运行时对象特权。

下表列出了所需的权限以及用户可以使用执行运行时对象特权执行的操作：

权限	说明
对文件夹的读取和执行权限	用户能够使用导航器的“服务”菜单将 PowerCenter 集成服务分配给工作流。
对文件夹的读取、写入和执行权限 对连接对象的读取和执行权限	用户能够通过创建调试会话实例或使用现有可重用会话来调试映射。用户还必须具有创建、编辑和删除运行时对象的特权。 如果 PowerCenter 集成服务在安全模式下运行，用户必须具备关联的 PowerCenter 存储库服务的管理员角色。
对文件夹的读取和执行权限 对连接对象的读取和执行权限	用户能够通过使用现有不可重用会话来调试映射。 如果 PowerCenter 集成服务在安全模式下运行，用户必须具备关联的 PowerCenter 存储库服务的管理员角色。
对文件夹的读取和执行权限 对连接对象的读取和执行权限	用户能够执行以下操作： <ul style="list-style-type: none">- 启动、冷启动和重新启动任务及工作流。- 恢复通过其自己的用户帐户启动的任务及工作流。 如果 PowerCenter 集成服务使用操作系统配置文件，用户还必须拥有对该操作系统配置文件的权限。 如果 PowerCenter 集成服务在安全模式下运行，用户必须具备关联的 PowerCenter 存储库服务的管理员角色。

管理运行时对象执行特权

分配了管理运行时对象执行特权的用户可以计划工作流和取消工作流的计划。用户还可以停止、中止和恢复由其他用户启动的任务和工作流。

管理运行时对象执行特权包括执行运行时对象特权和监视运行时对象特权。

下表列出了所需的权限以及用户在具有管理运行时对象特权时可以执行的操作：

权限	说明
对文件夹的读取和执行权限	用户能够截断工作流和会话日志条目。
对文件夹的读取和执行权限	<p>用户能够执行以下操作：</p> <ul style="list-style-type: none"> - 停止和中止由其他用户启动的任务和工作流。 - 停止和中止已自动恢复的任务。 - 取消工作流的计划。 <p>如果 PowerCenter 集成服务在安全模式下运行，用户必须具备关联的 PowerCenter 存储库服务的管理员角色。</p>
对文件夹的读取和执行权限 对连接对象的读取和执行权限	<p>用户能够执行以下操作：</p> <ul style="list-style-type: none"> - 恢复由其他用户启动的任务和工作流。 - 恢复已自动恢复的任务。 <p>如果 PowerCenter 集成服务使用操作系统配置文件，用户还必须拥有对该操作系统配置文件的权限。</p> <p>如果 PowerCenter 集成服务在安全模式下运行，用户必须具备关联的 PowerCenter 存储库服务的管理员角色。</p>
对文件夹的读取、写入和执行权限 对连接对象的读取和执行权限	<p>用户能够执行以下操作：</p> <ul style="list-style-type: none"> - 从“工作流 > 计划程序”菜单中创建和编辑可重用的计划程序。 - 在工作流属性中编辑不可重用计划程序。 - 在工作流属性中编辑可重用计划程序。用户还必须具有创建、编辑和删除运行时对象的特权。 <p>如果 PowerCenter 集成服务使用操作系统配置文件，用户还必须拥有对该操作系统配置文件的权限。</p> <p>如果 PowerCenter 集成服务在安全模式下运行，用户必须具备关联的 PowerCenter 存储库服务的管理员角色。</p>

全局对象特权组

全局对象特权组中的特权和 PowerCenter 存储库对象权限确定了用户可以对以下全局对象执行的操作：

- 连接对象
- 部署组
- 标签
- 查询

某些全局对象任务由全局对象所有权和管理员角色决定，而不是由特权或权限决定。全局对象所有者或分配了 PowerCenter 存储库服务管理员角色的用户可以完成以下全局对象任务：

- 配置全局对象权限。
- 更改全局对象所有者。
- 删除全局对象。

分配了权限但未分配任何特权的用户可以执行部分全局对象操作。下表列出了仅将权限分配给用户时这些用户可以执行的操作：

权限	说明
对连接对象执行读取操作	用户能够查看连接对象。
对部署组执行读取操作	用户能够查看部署组。
对标签执行读取操作	用户能够查看标签。
对查询执行读取操作	用户能够查看对象查询。
对连接对象执行读取和写入操作	用户能够编辑连接对象。
对标签执行读取和写入操作	用户能够编辑和锁定标签。
对查询执行读取和写入操作	用户能够编辑和验证对象查询。
对查询执行读取和执行操作	用户能够运行对象查询。
对文件夹执行读取操作 对标签执行读取和执行操作	用户能够应用标签和删除标签引用。

注意: 要对全局对象执行操作，用户还必须在工具特权组中具有相应特权。

创建连接特权

分配了创建连接特权的用户可以创建连接对象。

下表列出了所需的权限以及用户可以使用创建连接特权执行的操作：

权限	说明
-	用户能够创建和复制连接对象。

管理部署组特权

如果您有基于团队的开发选项，则在受版本控制的 PowerCenter 存储库中分配了管理部署组特权的用户可以创建、编辑、复制和回滚部署组。在无版本控制的存储库中，用户可以创建、编辑和复制部署组。

下表列出了所需的权限以及用户可以使用管理部署组特权执行的操作：

权限	说明
-	用户能够创建部署组。
对部署组执行读取和写入操作	用户能够执行以下操作： - 编辑部署组。 - 从部署组中删除对象。
对原始文件夹执行读取操作 对部署组执行读取和写入操作	用户能够向部署组添加对象。

权限	说明
对原始文件夹执行读取操作 对目标文件夹执行读取和写入操作 对部署组执行读取和执行操作	用户能够复制部署组。
对目标文件夹执行读取和写入操作	用户能够回滚部署组。

执行部署组特权

分配了执行部署组特权的用户可以复制对目标文件夹没有写入权限的部署组。

下表列出了所需的权限以及用户可以使用执行部署组特权执行的操作：

权限	说明
对原始文件夹执行读取操作 对部署组执行操作	用户能够复制部署组。

创建标签特权

如果您有基于团队的开发选项，则在受版本控制的 PowerCenter 存储库中分配了创建标签特权的用户可以创建标签。

下表列出了所需的权限以及用户可以使用创建标签特权执行的操作：

权限	说明
-	用户能够创建标签。

创建查询特权

分配了创建查询特权的用户可以创建对象查询。

下表列出了所需的权限以及用户可以使用创建查询特权执行的操作：

权限	说明
-	用户能够创建对象查询。

PowerExchange 侦听器服务特权

PowerExchange 侦听器服务特权决定了用户可以运行的 infacmd pwx 命令。

下表介绍了信息命令特权组中的 PowerExchange 侦听器服务特权：

特权名称	说明
listtask	运行 infacmd pwx ListTaskListener 命令。

下表介绍了管理命令特权组中的每个 PowerExchange 侦听器服务特权：

特权名称	说明
关闭	运行 infacmd pwx CloseListener 命令。
closeforce	运行 infacmd pwx CloseForceListener 命令。
stoptask	运行 infacmd pwx StopTaskListener 命令。

PowerExchange 日志记录器服务特权

PowerExchange 日志记录器服务特权确定了用户可以运行的 infacmd pwx 命令。

下表介绍了信息命令特权组中的每个 PowerExchange 日志记录器服务特权：

特权名称	说明
displayall	运行 infacmd pwx DisplayAllLogger 命令。
displaycpu	运行 infacmd pwx DisplayCPULogger 命令。
displaycheckpoints	运行 infacmd pwx DisplayCheckpointsLogger 命令。
displayevents	运行 infacmd pwx DisplayEventsLogger 命令。
displaymemory	运行 infacmd pwx DisplayMemoryLogger 命令。
displayrecords	运行 infacmd pwx DisplayRecordsLogger 命令。
displaystatus	运行 infacmd pwx DisplayStatusLogger 命令。

下表介绍了管理命令特权组中的每个 PowerExchange 日志记录器服务特权：

特权名称	说明
condense	运行 infacmd pwx CondenseLogger 命令。
fileswitch	运行 infacmd pwx FileSwitchLogger 命令。
shutdown	运行 infacmd pwx ShutDownLogger 命令。

计划程序服务特权

计划程序服务特权确定用户可以对计划和已计划的作业执行的操作。

下表介绍了计划程序服务特权和所需权限：

特权	说明	需要对以下对象的权限
创建计划	用户可以创建计划。要创建计划，用户还必须具有对数据集成服务的应用程序管理特权。	<ul style="list-style-type: none">- 计划程序服务- 运行用户要计划的作业的数据集成服务
编辑计划	用户可以编辑、暂停和恢复计划。要编辑计划，用户还必须具有对数据集成服务的应用程序管理特权。	<ul style="list-style-type: none">- 计划程序服务- 运行用户要计划的作业的数据集成服务
删除计划	用户可以删除计划。	计划程序服务
查看计划	用户可以查看计划视图和计划。	计划程序服务

Test Data Manager 服务特权

Test Data Manager 服务特权决定了用户可以使用 Test Data Manager 执行的操作。可以在 Administrator 工具的安全选项卡上配置特权。

下表介绍了每个 Test Data Manager 特权组：

特权组	说明
管理	包括创建和管理连接、密码、角色以及向 Informatica Administrator 中的用户和用户组分配特权、管理存储库、添加许可证和设置工作流和项目属性的特权。 注意: 在您创建用户和用户组之前，默认 Informatica 管理员用户必须将安全管理特权分配给测试数据管理员用户。
数据域	包括在 Test Data Manager 中查看和管理数据域的特权。
数据屏蔽	包括在 Test Data Manager 中查看和管理屏蔽规则和策略分配的特权。
数据子集	包括在 Test Data Manager 中查看和管理子集对象（包括实体、组和模板）的特权。
数据子集	包括在 Test Data Manager 中查看和管理子集对象（包括组）的特权。
策略	包括在 Test Data Manager 中查看和管理策略的特权。
项目	包括在 Test Data Manager 中查看和管理项目、审计和导入元数据，以及执行计划和工作流的特权。
规则	包括在 Test Data Manager 中查看和管理屏蔽和生成规则的特权。
规则	包括在 Test Data Manager 中查看和管理屏蔽规则的特权。
数据生成	包括在 Test Data Manager 中查看和管理测试数据生成的特权。

管理特权组

管理特权组中的特权决定测试数据管理员可以执行的管理任务。

下表列出了管理特权组中的特权和对某个对象执行某项任务所需的权限：

特权	包括特权	权限	说明
管理首选项	-	写入	用户可以在 Informatica Administrator 和 Test Data Manager 中执行以下操作： <ul style="list-style-type: none"> - 创建角色。 - 编辑角色。 - 删除角色。 - 查看角色。 - 将角色与用户关联。 - 将特权与用户关联。 - 将角色与用户组关联。 - 将特权与用户组关联。 - 创建密码。 - 编辑密码。 - 删除密码。 - 编辑密码权限。 - 创建全局参数。 - 编辑全局参数。 - 删除全局参数。 - 导入全局参数文件。 - 添加许可证。 - 设置 TDM 存储库。 - 设置 PowerCenter 存储库。 - 设置数据域敏感度级别。 - 配置 Test Data Warehouse 存储库。 - 配置 Test Data Warehouse。 - 设置项目自定义属性。 - 设置工作流生成属性。 - 启用数据发现。 - 设置剖析服务。 - 查看管理对象。 - 配置关键字搜索索引选项。
查看连接	-	读取	用户可以在 Test Data Manager 中的“连接”页面上执行以下操作： <ul style="list-style-type: none"> - 查看连接。 - 测试连接。
管理连接	查看连接	写入	用户可以在 Test Data Manager 中的“连接”页面上执行以下操作： <ul style="list-style-type: none"> - 创建连接。 - 编辑连接。 - 删除连接。 - 查看连接。 - 测试连接。 - 配置 Test Data Warehouse 存储库。 - 配置 Test Data Warehouse。

特权	包括特权	权限	说明
管理首选项	-	写入	用户可以在 Informatica Administrator 和 Test Data Manager 中执行以下操作： <ul style="list-style-type: none"> - 创建角色。 - 编辑角色。 - 删除角色。

特权	包括特权	权限	说明
			<ul style="list-style-type: none"> - 查看角色。 - 将角色与用户关联。 - 将特权与用户关联。 - 将角色与用户组关联。 - 将特权与用户组关联。 - 创建密码。 - 编辑密码。 - 删除密码。 - 编辑密码权限。 - 添加许可证。 - 设置 TDM 存储库。 - 设置数据域敏感度级别。 - 设置项目自定义属性。 - 设置 workflow 生成属性。 - 启用数据发现。 - 设置剖析服务。 - 查看管理对象。 - 配置关键字搜索索引选项。
查看连接	-	读取	用户可以在 Test Data Manager 中的“连接”页面上执行以下操作： <ul style="list-style-type: none"> - 查看连接。 - 测试连接。
管理连接	查看连接	写入	用户可以在 Test Data Manager 中的“连接”页面上执行以下操作： <ul style="list-style-type: none"> - 创建连接。 - 编辑连接。 - 删除连接。 - 查看连接。 - 测试连接。

连接特权组

连接特权组中的特权决定用户可以在 TDM 工作台的“连接”页面中执行的任务。下表列出了连接特权组中的特权和对某一对象执行某项任务所需的权限：

特权	包括特权	权限	说明
查看连接	-	读取	用户可以在 TDM 工作台查看并测试连接。
管理连接	查看连接	写入	用户可以在 TDM 工作台的“连接”页面中执行以下操作： <ul style="list-style-type: none"> - 创建连接。 - 编辑连接。 - 删除连接。 - 查看连接。 - 测试连接。

数据域特权组

数据域特权组中的特权决定用户可以在 Test Data Manager 的“策略”页面中对数据域执行的任务。

下表列出了数据域特权组中的特权以及对某个对象执行任务所需的权限：

特权	包括特权	权限	说明
查看数据域	-	读取	用户可以在 Test Data Manager 中查看数据域。
管理数据域	查看数据域	写入	用户可以在 Test Data Manager 中对数据域执行以下操作： <ul style="list-style-type: none">- 创建数据域。- 编辑数据域。- 删除数据域。- 查看数据域。

数据屏蔽特权组

数据屏蔽特权组中的特权决定用户可以在 Test Data Manager 的“项目”|“定义”|“数据屏蔽”视图中执行的任务。可以在此视图将规则和策略分配给表列。

下表列出了“数据屏蔽”特权组中的特权和对某一对象执行某项任务所需的权限：

特权	包括特权	权限	说明
查看数据屏蔽	-	读取	用户可以在 Test Data Manager 中查看数据屏蔽分配。
管理数据屏蔽	查看数据屏蔽	写入	用户可以在 Test Data Manager 中执行以下数据屏蔽分配操作： <ul style="list-style-type: none">- 添加规则和策略分配。- 删除规则和策略分配。- 替代规则属性。- 查看数据屏蔽分配。

数据子集特权组

“数据子集”特权组中的权限决定了用户在 Test Data Manager 中可以对数据子集对象执行的任务。

下表列出了“数据子集”特权组中的权限和对某一对象执行某项任务所需的权限：

特权	包括特权	权限	说明
查看数据子集	-	读取	用户可以在 Test Data Manager 中执行以下数据子集操作： <ul style="list-style-type: none">- 查看组。- 查看模板。- 查看实体。- 查看最近的项目对象。
管理数据子集	查看数据子集	写入	用户可以在 Test Data Manager 中执行以下数据子集操作： <ul style="list-style-type: none">- 创建组。- 编辑组。- 删除组。- 添加组参数。- 创建模板。- 编辑模板。- 删除模板。- 添加模板参数。- 创建实体。- 编辑实体。- 删除实体。- 添加实体条件。- 启用关系。- 禁用关系。- 编辑关系。- 对更改的审查和操作。- 将更改审查标记为已完成。

特权	包括特权	权限	说明
查看数据子集	-	读取	用户可以在 Test Data Manager 中执行以下数据子集操作： <ul style="list-style-type: none">- 查看组。- 查看最近的项目对象。
管理数据子集	查看数据子集	写入	用户可以在 Test Data Manager 中执行以下数据子集操作： <ul style="list-style-type: none">- 创建组。- 编辑组。- 删除组。- 启用关系。- 禁用关系。- 编辑关系。- 对更改的审查和操作。- 将更改审查标记为已完成。

策略特权组

策略特权组中的特权决定了用户可以在 Test Data Manager 中对策略执行的任务。

下表列出了策略特权组中的特权和对某一对象执行某项任务所需的权限：

特权	包括特权	权限	说明
查看策略	-	读取	用户可以在 Test Data Manager 中查看策略。
管理策略	查看策略	写入	用户可以在 Test Data Manager 中执行以下策略操作： <ul style="list-style-type: none">- 创建策略。- 编辑策略。- 删除策略。- 查看策略。

项目特权组

项目特权组中的特权确定用户可以在 Test Data Manager 中对项目执行的任务。

下表列出了项目特权组中的特权和对某一对象执行某项任务所需的权限：

特权	包括特权	权限	说明
查看项目	-	读取	用户可以在 Test Data Manager 中对项目执行以下操作： <ul style="list-style-type: none">- 查看项目。- 查看计划。- 查看计划详细报表。- 查看计划审计报表。- 查看最近的项目。- 创建测试数据仓库计划- 管理测试数据仓库计划- 生成测试数据仓库计划- 执行测试数据仓库计划
管理项目	查看项目	写入	用户可以在 Test Data Manager 中对项目执行以下操作： <ul style="list-style-type: none">- 创建项目。- 编辑项目。- 删除项目。- 查看项目。- 创建参数- 编辑参数- 删除参数- 将用户与项目相关联。- 将用户组与项目相关联。- 关联或移除项目的规则。- 关联或移除项目的策略。- 创建计划。- 编辑计划。- 删除计划。- 生成计划。

特权	包括特权	权限	说明
发现项目	-	写入	用户可以在 Test Data Manager 中对项目执行以下发现操作： <ul style="list-style-type: none"> - 对表进行分类。 - 将发现标记为完成。 - 将数据域与列相关联。 - 将列标记为受限制。 - 将列标记为区分大小写。 - 设置类似值列。 - 删除类似值列。 - 添加主键。 - 删除主键。 - 创建逻辑约束。 - 查看逻辑约束。 - 编辑逻辑约束。 - 删除逻辑约束。 - 查看项目。 - 查看剖析的数据域。 - 批准或拒绝配置文件数据域。 - 将数据域分类标记为已完成。 - 查看剖析的主键。 - 批准或拒绝剖析的主键。 - 将主键发现标记为已完成。 - 查看剖析的实体。 - 批准或拒绝剖析的实体。 - 将实体发现标记为已完成。 - 查看项目风险分析。 - 查看最近项目敏感数据分布。 - 删除表。
生成项目	-	写入	用户可以在 Test Data Manager 中生成工作流。
执行项目	-	写入	用户可以在 Test Data Manager 中对项目执行以下执行操作： <ul style="list-style-type: none"> - 执行计划。 - 执行工作流。 - 停止工作流。 - 中止工作流。 - 恢复工作流。 - 查看计划执行。
监视项目	-	读取	用户可以在 Test Data Manager 中对项目执行以下监视操作： <ul style="list-style-type: none"> - 监视项目作业。 - 查看项目作业日志。 - 跨项目监视作业。 - 跨项目查看作业日志。
审计项目	-	读取	用户可以在 Test Data Manager 中查看项目和计划的最近活动。
导入元数据	-	写入	用户可以在 Test Data Manager 中对项目执行以下操作： <ul style="list-style-type: none"> - 导入源。 - 删除源。 - 删除表。

特权	包括特权	权限	说明
查看项目	-	读取	用户可以在 Test Data Manager 中对项目执行以下操作： <ul style="list-style-type: none"> - 查看项目。

特权	包括特权	权限	说明
			<ul style="list-style-type: none"> - 查看计划。 - 查看计划详细报表。 - 查看计划审计报表。 - 查看最近的项目。
管理项目	查看项目	写入	<p>用户可以在 Test Data Manager 中对项目执行以下操作：</p> <ul style="list-style-type: none"> - 创建项目。 - 编辑项目。 - 删除项目。 - 查看项目。 - 将用户与项目相关联。 - 将用户组与项目相关联。 - 关联或移除项目的规则。 - 关联或移除项目的策略。 - 创建计划。 - 编辑计划。 - 删除计划。 - 生成计划。
发现项目	-	写入	<p>用户可以在 Test Data Manager 中对项目执行以下发现操作：</p> <ul style="list-style-type: none"> - 对表进行分类。 - 将发现标记为完成。 - 将数据域与列相关联。 - 将列标记为受限制。 - 将列标记为区分大小写。 - 设置类似值列。 - 删除类似值列。 - 添加主键。 - 删除主键。 - 创建逻辑约束。 - 查看逻辑约束。 - 编辑逻辑约束。 - 删除逻辑约束。 - 查看项目。 - 查看剖析的数据域。 - 批准或拒绝配置文件数据域。 - 将数据域分类标记为已完成。 - 查看项目风险分析。 - 查看最近项目敏感数据分布。 - 删除表。
生成项目	-	写入	用户可以在 Test Data Manager 中生成工作流。
执行项目	-	写入	<p>用户可以在 Test Data Manager 中对项目执行以下执行操作：</p> <ul style="list-style-type: none"> - 执行计划。 - 执行工作流。 - 停止工作流。 - 中止工作流。 - 查看计划执行。
监视项目	-	读取	<p>用户可以在 Test Data Manager 中对项目执行以下监视操作：</p> <ul style="list-style-type: none"> - 监视项目作业。 - 查看项目作业日志。 - 跨项目监视作业。 - 跨项目查看作业日志。

特权	包括特权	权限	说明
审计项目	-	读取	用户可以在 Test Data Manager 中查看项目和计划的最近活动。
导入元数据	-	写入	用户可以在 Test Data Manager 中对项目执行以下操作： <ul style="list-style-type: none"> - 导入源。 - 删除源。 - 删除表。

注意: 具有管理项目特权的用户必须至少具有以下级别的特权，才能使用每个组件创建一个计划。

- 查看管理特权组的连接。创建一个计划。
- 查看 Data Subset 特权组的数据子集。使用子集组件创建一个计划。
- 查看规则特权组的屏蔽规则。使用屏蔽组件创建一个计划。
- 查看规则特权组的生成规则。使用生成组件创建一个计划。

规则特权组

“规则”特权组中的特权决定用户可在 Test Data Manager 中对数据屏蔽和数据生成规则执行的任务。

“规则”特权组中的特权决定用户可在 Test Data Manager 中对数据屏蔽规则执行的任务。

下表列出了“数据屏蔽”特权组中的特权和对某一对象执行某项任务所需的权限：

特权	包括特权	权限	说明
查看屏蔽规则	-	读取	用户能够在 Test Data Manager 中查看屏蔽规则。
管理屏蔽规则	查看屏蔽规则	写入	用户能够在 Test Data Manager 中对数据屏蔽规则执行以下操作： <ul style="list-style-type: none"> - 创建屏蔽规则。 - 编辑屏蔽规则。 - 删除屏蔽规则。 - 查看屏蔽规则。

特权	包括特权	权限	说明
查看生成规则	-	读取	用户能够在 Test Data Manager 中查看生成规则。
管理生成规则	查看生成规则	写入	用户能够在 Test Data Manager 中对数据生成规则执行以下操作： <ul style="list-style-type: none"> - 创建生成规则。 - 编辑生成规则。 - 删除生成规则。 - 查看生成规则。

特权	包括特权	权限	说明
查看屏蔽规则	-	读取	用户能够在 Test Data Manager 中查看屏蔽规则。
管理屏蔽规则	查看屏蔽规则	写入	用户能够在 Test Data Manager 中对数据屏蔽规则执行以下操作： <ul style="list-style-type: none"> - 创建屏蔽规则。 - 编辑屏蔽规则。 - 删除屏蔽规则。 - 查看屏蔽规则。

数据生成特权组

数据生成特权组中的特权确定了用户可以在 Test Data Manager 中执行的测试数据生成任务。

下表列出了数据生成特权组中的特权以及对某个对象执行任务所需的权限：

特权	包括特权	权限	说明
查看数据生成	-	读取	用户可以在 Test Data Manager 中查看数据生成规则分配。
管理数据生成	查看数据生成	写入	用户可以在 Test Data Manager 中对数据生成执行以下操作： <ul style="list-style-type: none"> - 查看数据生成规则分配。 - 添加数据生成规则分配。 - 删除数据生成规则分配。 - 替代数据生成规则分配。

管理角色

角色是您可以分配给用户和组的特权集合。可以分配以下类型的角色：

- 系统定义。无法编辑或删除的角色。
- 自定义。可以创建、编辑和删除的角色。

角色包括针对域或应用程序服务类型的特权。您针对域或域中的每项应用程序服务将角色分配给用户或组。例如，您可以创建一个包括 PowerCenter 存储库服务的特权的开发人员角色。一个域可以包含多个 PowerCenter 存储库服务。您可以针对开发 PowerCenter 存储库服务将开发人员角色分配给用户。您可以针对生产 PowerCenter 存储库服务将不同的角色分配给该用户。

角色包括针对域或应用程序服务类型的特权。您针对域或域中的每项应用程序服务将角色分配给用户或组。

角色包括针对域或应用程序服务类型的特权。您针对域或域中的每项应用程序服务将角色分配给用户或组。

UMSM 包含以下角色类型：

- 管理员。这是系统定义的角色，具有管理 Administrator 工具的特权。分配此角色后，可以创建和管理用户帐户、创建 Ultra Messaging 服务并对其进行配置、配置 UMSM 组件以及 UM 部署。
- 操作员。这是自定义角色，具有监视 UM 部署的特权。

在导航器的“角色”部分中选择角色时，可以查看已针对域和应用程序服务直接分配了角色的所有用户和组。可以按用户和组或者按服务查看角色分配。要导航到“分配”部分中列出的某个用户或组，请右键单击该用户或组，然后选择“导航到项目”。

可以搜索系统定义的角色和自定义角色。

系统定义的角色

系统定义的角色是您无法编辑或删除的角色。管理员角色是系统定义角色。

为用户或组分配域、分析服务、数据集成服务、Mass Ingestion 服务、Metadata Manager 服务、模型存储库服务或 PowerCenter 存储库服务的管理员角色时，将向该用户或组授予服务的所有特权。管理员角色将跳过权限检查。具有管理员角色的用户可以访问服务管理的所有对象。

为用户或组分配域、数据集成服务或模型存储库服务的管理员角色时，将向该用户或组授予服务的所有特权。管理员角色将跳过权限检查。具有管理员角色的用户可以访问服务管理的所有对象。

针对域或 Ultra Messaging 服务将管理员角色分配给用户或组时，会将服务的所有特权授予该用户或组。管理员角色将跳过权限检查。具有管理员角色的用户可以访问服务管理的所有对象。

管理员角色

针对域、数据集成服务或 PowerCenter 存储库服务将管理员角色分配给用户或组时，该用户或组能够完成由管理员角色（而非特权或权限）决定的某些任务。

针对域或 Ultra Messaging 服务将管理员角色分配给用户或组时，该用户或组能够完成由管理员角色（而非特权或权限）决定的某些任务。

可以针对域、数据集成服务或 PowerCenter 存储库服务将所有特权分配给用户或组，然后向该用户或组授予对所有域或 PowerCenter 存储库对象的完全权限。但是，该用户或组无法完成由管理员角色决定的任务。

可以针对域或 Ultra Messaging 服务将所有特权分配给用户或组，然后向该用户或组授予对所有域对象的完全权限。但是，该用户或组无法完成由管理员角色决定的任务。

例如，分配了域的管理员角色的用户可以在 Administrator 工具中配置域属性。分配了对域的所有域特权和权限的用户不能配置域属性。

下表列出了由域、数据集成服务、Mass Ingestion 服务和 PowerCenter 存储库服务的管理员角色决定的任务：

下表列出了由域或 Ultra Messaging 服务的管理员角色决定的任务：

服务	任务
域	<ul style="list-style-type: none">- 配置域属性。- 配置群集配置。- 创建操作系统配置文件。- 删除操作系统配置文件。- 授予对域和操作系统配置文件的权限。- 管理和清除日志事件。- 接收域警告。- 运行许可证报告。- 查看用户活动日志事件。- 关闭域。- 访问服务升级向导。
数据集成服务	<ul style="list-style-type: none">- 使用“操作”菜单升级数据集成服务。
Mass Ingestion 服务	<ul style="list-style-type: none">- 浏览所有 Mass Ingestion 规范。- 编辑 Mass Ingestion 规范。- 运行 Mass Ingestion 规范。- 删除 Mass Ingestion 规范。
PowerCenter 存储库服务	<ul style="list-style-type: none">- 如果 PowerCenter 集成服务使用操作系统配置文件，则会将操作系统配置文件分配给存储库文件夹。*- 更改文件夹和全局对象的所有者。*- 配置文件夹权限和全局对象权限。*- 在安全模式下运行 PowerCenter 集成服务时，从 PowerCenter 客户端连接到 PowerCenter 集成服务。- 从 Workflow Manager 的导航器中删除 PowerCenter 集成服务。- 删除文件夹和全局对象。*- 指定要共享的文件夹。*- 编辑文件夹的名称和说明。* <p>*PowerCenter 存储库文件夹所有者或全局对象所有者也能完成这些任务。</p>

服务	任务
域	<ul style="list-style-type: none">- 配置域属性。- 授予对域的权限- 管理和清除日志事件。- 接收域警告。- 查看用户活动日志事件。

自定义角色

自定义角色是指您可以编辑或删除的角色。

默认情况下，Administrator 工具包括以下自定义角色：

- 分析服务自定义角色
- Metadata Manager 服务自定义角色
- 操作员自定义角色
- PowerCenter 存储库服务自定义角色
- Test Data Manager 服务自定义角色

您可以编辑这些角色的特权或删除这些角色。还可以创建自己的自定义角色。

创建自定义角色

创建自定义角色时，您针对域或应用程序服务类型将特权分配给角色。一个角色可以包括一项或多项服务的特权。

1. 在 Administrator 工具中，单击“安全”选项卡。
2. 在“安全操作”菜单中，单击“创建角色”。
此时将显示“创建角色”对话框。
3. 输入角色的以下属性：

属性	说明
名称	角色的名称。角色名称不区分大小写，且长度不能超过 128 个字符。组名称不能包含制表符、换行符或下列特殊字符：, + \ < > ; / * % ? 名称可以包含 ASCII 空格字符，但不能将其用作第一个或最后一个字符。不允许使用所有其他空格字符。
说明	角色的说明。说明不能超过 765 个字符或包含制表符、换行符或以下特殊字符：< > "

4. 单击“特权”选项卡。
5. 展开域或应用程序服务类型。
6. 选择要针对域或应用程序服务类型分配给角色的特权。
7. 单击“确定”。

编辑自定义角色的属性

编辑自定义角色时，可以更改角色的说明。您不能更改角色的名称。

1. 在 Administrator 工具中，单击“安全”选项卡。
2. 在导航器的“角色”部分中，选择一个角色。
3. 单击“编辑”。
4. 更改该角色的说明，然后单击“确定”。

编辑分配给自定义角色的特权

可以针对域和每种应用程序服务类型更改分配给自定义角色的特权。

1. 在 Administrator 工具中，单击“安全”选项卡。
2. 在导航器的“角色”部分中，选择一个角色。
3. 单击“特权”选项卡。
4. 单击“编辑”。
此时将显示“编辑角色和特权”对话框。
5. 展开域或应用程序服务类型。
6. 要将特权分配给角色，请针对域或应用程序服务类型选择特权。
7. 要从角色中删除特权，请针对域或应用程序服务类型清除特权。
8. 重复上述步骤以针对每种服务类型更改特权。
9. 单击“确定”。

删除自定义角色

删除自定义角色时，自定义角色及其包含的所有特权都将从已分配该角色的任何用户或组中删除。

要删除自定义角色，请右键单击导航器的“角色”部分中的角色，然后选择“删除角色”。确认要删除角色。

将特权和角色分配给用户和组

您通过将以下项目分配给用户和组来决定用户可以执行的操作：

- 特权。特权决定用户可以在应用程序客户端中执行的操作。
- 角色。角色是特权的集合。将角色分配给用户或组时，您分配的是属于该角色的特权的集合。

将特权分配给用户和组时，请遵循以下规则和准则：

- 您针对域以及该域中运行的每项应用程序服务将特权和角色分配给用户和组。
在以下情况下，无法为用户和组分配 Metadata Manager 服务或 PowerCenter 存储库服务的特权和角色：
 - 应用程序服务已禁用。
 - PowerCenter 存储库服务正以独占模式运行。
- 可以针对服务类型相同的每项应用程序服务将不同的特权和角色分配给用户或组。
- 角色可以包括针对域以及多种应用程序服务类型的特权。针对一项应用程序服务将角色分配给用户或组时，会将该应用程序服务类型的特权分配给该用户或组。

如果您更改了分配给用户的特权或角色，更改的特权或角色将在用户下次登录时生效。

注意：您无法编辑分配给默认管理员用户帐户的特权或角色。

继承特权

用户或组可以从以下对象继承特权：

- 组。将特权分配给组时，属于该组的所有子组 and 用户将继承这些特权。
- 角色。将角色分配给用户时，用户将继承属于该角色的特权。将角色分配给组时，组以及属于该组的所有子组 and 用户将继承属于该角色的特权。子组 and 用户不继承该角色。

您无法撤销继承自组或角色的特权。您可以将非继承自组或角色的其他特权分配给用户或组。

用户或组的“特权”选项卡显示针对域和每项应用程序服务分配给该用户或组的所有角色和特权。展开域或应用程序服务可查看针对域或服务分配的角色和特权。单击以下项目可显示与已分配的角色和特权有关的更多信息：

- 已分配角色的名称。在详细信息面板中显示角色详细信息。
- 已分配角色的信息图标。突出显示随该角色继承的所有特权。

继承自角色或组的特权显示一个继承图标。继承特权的工具提示显示用户从哪个角色或组继承了该特权。

通过导航将特权和角色分配给用户或组

1. 在 Administrator 工具中，单击“安全”选项卡。
2. 在导航器中，选择一个用户或组。
3. 单击“特权”选项卡。
4. 单击“编辑”。

此时将显示“编辑角色和特权”对话框。

5. 要分配角色，请展开“角色”选项卡中的域或应用程序服务。
6. 要授予角色，请选择要针对域或应用程序服务分配给用户或组的角色。
您可以针对选定的域或应用程序服务类型选择包括特权的任何角色。
7. 要撤消角色，请清除分配给用户或组的角色。
8. 重复步骤 5 到 7，以针对其他服务分配角色。
9. 要分配特权，请单击“特权”选项卡。
10. 展开域或应用程序服务。
11. 要授予特权，请选择要针对域或应用程序服务分配给用户或组的特权。
12. 要撤消特权，请清除分配给用户或组的特权。
您无法撤消继承自角色或组的特权。
13. 重复步骤 10 到 12，以针对其他服务分配特权。
14. 单击“确定”。

查看对服务有特权的用户

您可以针对域或应用程序服务查看具有特权的所有用户。

1. 在 Administrator 工具中，单击“安全”选项卡。
2. 在“安全操作”菜单中，单击“服务用户特权”。
此时将显示“服务”对话框。
3. 选择域或应用程序服务。
详细信息面板针对域或应用程序服务显示具有特权的所有用户。
4. 右键单击某个用户名，然后单击“导航到项目”以导航到该用户。

特权和角色故障排除

我无法为用户分配现有 Metadata Manager 服务或 PowerCenter 存储库服务的特权和角色。

在以下情况下，无法为用户和组分配现有 Metadata Manager 服务或 PowerCenter 存储库服务的特权和角色：

- 应用程序服务已禁用。
- PowerCenter 存储库服务正以独占模式运行。

我从某个组中删除了某项特权。为什么该组中的部分用户仍具有该特权？

您可以通过以下任意方法将特权分配给用户：

- 将特权直接分配给用户。
- 将角色分配给用户。

- 将特权或角色分配给用户所属的组。

如果您从某个组中删除了某项特权，则可以直接向属于该组的用户分配该项特权，或者这些用户可以从已分配的角色继承该特权。

我被分配了针对所有域对象的所有域特权和权限，但是我无法在 Administrator 工具中完成所有任务。

某些 Administrator 工具任务由管理员角色决定，而不是由特权或权限决定。可以向您分配域的所有特权以及授予对所有域对象的完全权限。但是，您无法完成由管理员角色决定的任务。

我被分配了某项应用程序服务的管理员角色，但是我无法在 Administrator 工具中配置应用程序服务。

如果您具有某项应用程序服务的管理员角色，您即是应用程序客户端管理员。应用程序客户端管理员在应用程序客户端中具有完全权限和特权。

但是，应用程序客户端管理员在 Informatica 域中没有权限或特权。应用程序客户端管理员无法登录 Administrator 工具，因此无法管理其具有管理员特权的应用程序客户端的服务。

要在 Administrator 工具中管理应用程序服务，您必须具有恰当的域特权和权限。

我被分配了 PowerCenter 存储库服务的管理员角色，但是我无法使用 Repository Manager 来执行对象的高级清除或创建可重用元数据扩展。

您必须在 Administrator 工具中对 PowerCenter 存储库服务具有“管理服务”域特权和权限，才能在 Repository Manager 中执行以下操作：

- 在 PowerCenter 存储库级别执行对象版本的高级清除。
- 创建、编辑和删除可重用元数据扩展。

我的特权指示我应能够在应用程序客户端中编辑对象，但我无法编辑任何元数据。

您在应用程序客户端中可能没有必需的对象权限。即使具有执行某些操作的特权，您仍可能需要权限才能对某个特定对象执行操作。

我无法使用 pmrep 连接到正以独占模式运行的新 PowerCenter 存储库服务。

服务管理器可能尚未将 PowerCenter 存储库中的用户和组列表与域配置数据库中的列表同步。要同步用户和组列表，请重新启动 PowerCenter 存储库服务。

我在文件夹特权组中被分配了针对 PowerCenter 存储库服务的所有特权，并且对文件夹具有读取、写入和执行权限。但是，我无法配置文件夹的权限。

只有文件夹所有者或被分配了 PowerCenter 存储库服务管理员角色的用户可以完成以下文件夹管理任务：

- 如果 PowerCenter 集成服务使用操作系统配置文件，则会将操作系统配置文件分配给文件夹。需要对操作系统配置文件具有权限。
- 更改文件夹所有者。
- 配置文件夹权限。
- 删除文件夹。
- 指定要共享的文件夹。
- 编辑文件夹名称和说明。

我被分配了 Metadata Manager 服务的管理员角色，但是无法创建或还原 Metadata Manager 存储库。

要创建或还原 Metadata Manager 存储库，您必须属于默认的管理员组。默认管理员组中的用户比分配了应用程序服务管理员角色的用户拥有更多特权。

我分配有 Metadata Manager 服务的“加载资源”特权，但是在尝试加载 Business Glossary 资源时，出现“特权不足 (insufficient privileges)”错误。

要加载 Business Glossary 资源，需要具有“加载资源”、“管理资源”和“查看模型”特权。对于要加载的任何业务词汇表资源，您还需要对其具有写入权限。

第 10 章

权限

本章包括以下主题：

- [权限概览, 164](#)
- [域对象权限, 166](#)
- [连接权限, 170](#)
- [群集配置权限, 172](#)
- [应用程序和应用程序对象权限, 173](#)
- [SQL 数据服务权限, 174](#)
- [Web 服务权限, 178](#)

权限概览

使用特权和权限管理用户安全。权限定义了用户和组对对象的访问级别。

即使用户具有执行某些操作的特权，该用户仍可能需要具有对某个特定对象执行操作的权限。

例如，某个用户拥有对开发 PowerCenter 存储库服务的管理服务域特权和权限，但没有对生产 PowerCenter 存储库服务的管理服务域特权和权限。该用户可以编辑或删除开发 PowerCenter 存储库服务，但不能编辑或删除生产 PowerCenter 存储库服务。要管理应用程序服务，用户必须拥有对该应用程序服务的管理服务域特权和权限。

可以使用不同的工具配置对以下对象的权限：

可以使用不同的工具配置对以下对象的权限：

对象类型	工具	说明
应用程序和应用程序对象	Administrator 工具	您可以分配对应用程序和应用程序对象（如映射和工作流）的权限。
连接对象	Administrator 工具 Analyst 工具 Developer tool	您可以分配对 Administrator 工具、Analyst 工具或 Developer tool 中定义的连接的权限。这些工具共享连接权限。
域对象	Administrator 工具	您可以分配对以下域对象的权限：域、文件夹、节点、网格、许可证、应用程序服务和操作系统配置文件。

对象类型	工具	说明
Metadata Manager 目录对象	Metadata Manager	您可以分配对 Metadata Manager 文件夹和目录对象的权限。
模型存储库项目	Analyst 工具 Developer tool	您可以分配对 Analyst 工具和 Developer tool 中定义的项目的权限。这些工具共享项目权限。
PowerCenter 存储库对象	PowerCenter 客户端	您可以分配对 PowerCenter 文件夹、部署组、标签、查询和连接对象的权限。
SQL 数据服务对象	Administrator 工具	您可以分配对 SQL 数据服务、虚拟架构、虚拟表和虚拟存储过程等 SQL 数据对象的权限。
Web 服务对象	Administrator 工具	您可以分配对 Web 服务或 Web 服务操作的权限。

对象类型	工具	说明
连接对象	Administrator 工具 Developer tool	您可以分配对 Administrator 工具或 Developer tool 中定义的连接对象的权限。这些工具共享连接权限。
域对象	Administrator 工具	您可以分配对以下域对象的权限：域、文件夹、节点和应用程序服务。
模型存储库项目	Developer tool	您可以分配对 Developer tool 中定义的项目的权限。

您可以使用 Administrator 工具配置对域对象的权限。您可以分配对以下域对象的权限：

- 域
- 节点
- 应用程序服务

权限类型

用户和组在域中可以拥有以下类型的权限：

直接权限

直接分配给用户或组的权限。用户和组拥有对对象的权限后，如果还拥有相应的特权，则可以对该对象执行管理任务。您可以编辑直接权限。

继承权限

用户继承的权限。如果用户拥有对域或文件夹的权限，则可以继承域或文件夹中所有对象的权限。如果组拥有对域对象的权限，属于该组的所有子组 and 用户都可以继承对该域对象的权限。例如，域中具有一个名为“节点”的文件夹，其中包含多个节点。如果分配对该文件夹的组权限，则属于该组的所有子组 and 用户都可以继承对该文件夹及文件夹中所有节点的权限。

用户继承的权限。如果用户拥有对域的权限，则可以继承对域中所有对象的权限。如果组拥有对域对象的权限，属于该组的所有子组 and 用户都可以继承对该域对象的权限。

用户继承的权限。如果用户拥有对域的权限，则可以继承对域中所有对象的权限。如果组拥有对域对象的权限，属于该组的所有子组 and 用户都可以继承对该域对象的权限。

无法撤销继承权限。也无法撤销分配有管理员角色的用户或组的权限。管理员角色将跳过权限检查。具有管理员角色的用户可以访问所有对象。

您可以拒绝对某些对象类型的继承权限。拒绝权限后，您可以配置用户和组可能已经拥有的权限以外的权限。

有效权限

用户或组的所有权限的超集。包括直接权限和继承权限。

当您查看权限详细信息时，可以查看有效权限的来源。权限详细信息显示分配给用户或组的直接权限、分配给父组的直接权限，以及从父对象继承的权限。此外，权限详细信息还显示用户或组是否已分配可绕过权限检查的管理员角色。

权限搜索筛选器

为用户或组分配权限、查看权限详细信息或编辑权限时，可以使用搜索筛选器搜索用户或组。

管理用户或组的权限时，可以使用以下搜索筛选器：

安全域

输入安全域可以搜索用户或组。

模式字符串

输入字符串可以搜索用户或组。Administrator 工具将返回包含搜索字符串的所有名称。该字符串不区分大小写。例如，字符串“DA”可以返回“iasdaemon”、“daphne”和“DA_AdminGroup”。

您还可以对用户或组列表进行排序。右键单击列名称可按升序或降序对列进行排序。

域对象权限

您可以配置特权和权限来管理域中的用户安全。权限定义用户对域对象的访问级别。要登录到 Administrator 工具，用户必须至少对一个域对象拥有权限。如果用户拥有对对象的权限，但没有授予可修改对象类型的域权限，则用户将只能查看该对象。

例如，如果某个用户拥有对节点的权限，但没有管理节点和网格特权，则该用户可以查看节点属性，但不能配置、关闭或删除节点。

您可以配置对以下类型的域对象的权限：

域对象类型	权限的说明
域	使 Administrator 工具用户可以访问域中的所有对象。如果用户拥有域的权限，则可以继承域中所有对象的权限。
文件夹	使 Administrator 工具用户可以在 Administrator 工具中访问文件夹内的所有对象。如果用户拥有文件夹的权限，则可以继承文件夹中所有对象的权限。
节点	使 Administrator 工具用户可以查看和编辑节点属性。如果没有权限，用户在定义应用程序服务或创建网格时则无法使用节点。
网格	使 Administrator 工具用户可以查看和编辑网格属性。如果没有权限，用户则无法将网格分配给数据集成服务或 PowerCenter 集成服务。

域对象类型	权限的说明
许可证	使 Administrator 工具用户可以查看和编辑许可证属性。如果没有权限，用户则无法在创建应用程序服务时使用许可证。
应用程序服务	使 Administrator 工具用户可以查看和编辑应用程序服务属性。
操作系统配置文件	使相关 Informatica 开发人员、分析人员和操作员能够使用操作系统配置文件运行映射、配置文件和工作流。使 PowerCenter 用户可以运行与操作系统配置文件关联的工作流。如果运行工作流的用户没有分配给工作流的操作系统配置文件的权限，工作流将失败。

域对象类型	权限的说明
域	使 Administrator 工具用户可以访问域中的所有对象。如果用户拥有域的权限，则可以继承域中所有对象的权限。
节点	使 Administrator 工具用户可以查看和编辑节点属性。
应用程序服务	使 Administrator 工具用户可以查看和编辑应用程序服务属性。
许可证	使 Administrator 工具用户可以查看和编辑许可证属性。

域对象类型	权限的说明
域	使 Administrator 工具用户可以访问域中的所有对象。如果用户拥有域的权限，则可以继承域中所有对象的权限。
节点	使 Administrator 工具用户可以查看和编辑节点属性。
应用程序服务	使 Administrator 工具用户可以查看和编辑应用程序服务属性。
许可证	使 Administrator 工具用户可以查看和编辑许可证属性。

可以使用以下方法管理域对象权限：

- 管理域对象的权限。使用域对象的“权限”视图可分配和编辑对多个用户或组的对象的权限。
- 管理用户或组的权限。使用“管理权限”对话框可分配和编辑对特定用户或组的域对象的权限。

注意：配置对操作系统配置文件的权限不同于配置对其他域对象的权限。

域对象的权限

使用域对象的**权限**视图可分配、查看和编辑对多个用户或组的域对象的权限。

分配对域对象的权限

当您分配对域对象的权限时，将授予用户和组对该对象的访问权限。

1. 在管理选项卡上，选择**服务和节点**视图。

2. 在导航器中，选择域对象。
3. 在内容面板中，选择**权限**视图。
4. 单击**组**或**用户**选项卡。
5. 单击**操作 > 分配权限**。
分配权限对话框将显示没有该对象权限的所有用户或组。
6. 输入筛选条件搜索用户和组，然后单击**筛选**按钮。
7. 选择某个用户或组，然后单击**下一步**。
8. 选择**允许**，然后单击**完成**。

查看域对象的权限详细信息

当您查看权限详细信息时，可以查看有效权限的来源。

1. 在管理选项卡上，选择**服务和节点**视图。
2. 在导航器中，选择域对象。
3. 在内容面板中，选择**权限**视图。
4. 单击**组**或**用户**选项卡。
5. 输入筛选条件搜索用户和组，然后单击**筛选**按钮。
6. 选择某个用户或组，然后单击**操作 > 查看权限详细信息**。
此时将显示**权限详细信息**对话框。该对话框显示分配给用户或组的直接权限、分配给父组的直接权限，以及从父对象继承的权限。此外，权限详细信息还显示用户或组是否已分配可绕过权限检查的管理员角色。
7. 单击**关闭**。
8. 或者单击**编辑权限**以编辑直接权限。

编辑对域对象的权限

您可以为用户或组编辑对域对象的直接权限。但无法撤销继承权限或您自己的权限。

注意: 如果撤销了对对象的直接权限，用户或组可能仍然会从父组或对象继承权限。

1. 在管理选项卡上，选择**服务和节点**视图。
2. 在导航器中，选择域对象。
3. 在内容面板中，选择**权限**视图。
4. 单击**组**或**用户**选项卡。
5. 输入筛选条件搜索用户和组，然后单击**筛选**按钮。
6. 选择某个用户或组，然后单击**操作 > 编辑直接权限**。
此时将显示**编辑直接权限**对话框。
7. 要分配对对象的权限，请选择**允许**。
8. 要撤销对对象的权限，请选择**撤销**。
您可以单击**查看权限详细信息**查看是否已直接分配或继承该权限。
9. 单击**确定**。

用户或组的权限

使用**管理权限**对话框可查看、分配和编辑对特定用户或组的域对象权限。

查看用户或组的权限详细信息

当您查看权限详细信息时，可以查看有效权限的来源。

1. 在 Administrator 工具中，单击**安全**选项卡。
2. 单击**组**选项卡或**用户**选项卡。
3. 选择某个用户或组。
4. 单击**权限**选项卡。

分配和编辑用户或组的权限

为用户或组编辑域对象权限时，可以分配权限并编辑现有直接权限。但无法撤销继承权限或您自己的权限。

您可以单击**查看权限详细信息**查看是否已直接分配或继承该权限。如果撤消了对对象的权限，用户或组可能仍然会从父组或对象继承权限。

1. 在 Administrator 工具中，单击**安全**选项卡。
2. 单击**组**选项卡或**用户**选项卡。
3. 选择某个用户或组。
4. 单击**权限**选项卡。
5. 选择一个域对象，然后单击**编辑直接权限**。
6. 要分配对对象的权限，请选择**允许**。
7. 要撤销对对象的权限，请选择**撤销**。
8. 单击**确定**。

操作系统配置文件权限

在 Administrator 工具的“安全”页面上，分配、查看和编辑对操作系统配置文件的权限。

管理员组具有所有操作系统配置文件的权限。

分配操作系统配置文件权限

当您分配对操作系统配置文件的权限时，Informatica 用户使用操作系统配置文件运行映射、配置文件和工作流。PowerCenter 用户运行分配给操作系统配置文件的工作流。

1. 在 Administrator 工具中，单击**安全**选项卡。
2. 单击**操作系统配置文件**选项卡。
3. 选择操作系统配置文件，然后单击**权限**选项卡。
4. 单击**组**选项卡或**用户**选项卡，然后选择**编辑直接权限**。
5. 选择一个域对象，然后单击**编辑直接权限**。
6. 要分配对对象的权限，请选择**允许**。
7. 要撤销对对象的权限，请选择**撤销**。
8. 单击**确定**。

查看操作系统配置文件的权限详细信息

当您查看权限详细信息时，可以查看有效权限的来源。

1. 在**安全**选项卡上，选择**操作系统配置文件**视图。

2. 选择操作系统配置文件，然后单击**权限**选项卡。
3. 选择**组**或**用户**视图。
4. 输入筛选条件搜索用户和组，然后单击**筛选**按钮。
5. 选择用户或组，然后单击**查看权限详细信息**。
此时将显示**权限详细信息**对话框。该对话框显示分配给用户或组的直接权限、分配给父组的直接权限，以及从父对象继承的权限。此外，权限详细信息还显示用户或组是否已分配可绕过权限检查的管理员角色。
6. 单击**关闭**。
7. 或者单击**编辑权限**以编辑直接权限。

编辑对操作系统配置文件的权限

您可以为用户和组编辑对操作系统配置文件的直接权限。但无法撤销继承权限或您自己的权限。

注意: 如果撤销了对对象的直接权限，用户或组可能仍然会从父组或对象继承权限。

1. 在**安全**选项卡上，选择**操作系统配置文件**视图。
2. 选择操作系统配置文件，然后单击**权限**选项卡。
3. 选择**组**或**用户**视图。
4. 输入筛选条件搜索用户和组，然后单击**筛选**按钮。
5. 选择用户或组，然后单击**编辑直接权限**。
此时将显示**编辑直接权限**对话框。
6. 要分配对操作系统配置文件的权限，请选择**允许**。
7. 要撤销对操作系统配置文件的权限，请选择**撤销**。
您可以单击**查看权限详细信息**查看是否已直接分配或继承该权限。
8. 单击**确定**。

连接权限

权限可控制用户或组对连接拥有的访问级别。

您可以配置对 Analyst 工具、Developer 工具或 Administrator 工具中的连接的权限。

在一个工具中分配给用户或组的所有连接权限也适用于其他工具。例如，在 Developer 工具中授予 GroupA 对 ConnectionA 的权限。GroupA 在 Analyst 工具和 Administrator 工具中也拥有对 ConnectionA 的权限。

在一个工具中分配给用户或组的所有连接权限也适用于其他工具。例如，在 Developer 工具中授予 GroupA 对 ConnectionA 的权限。GroupA 在 Administrator 工具中也拥有对 ConnectionA 的权限。

以下 Informatica 组件使用连接权限：

- Administrator 工具。对连接强制执行读取、写入和执行权限。
- Analyst 工具。对连接强制执行读取、写入和执行权限。
- Informatica 命令行界面。对连接强制执行读取、写入和授予权限。
- Developer 工具。对连接强制执行读取、写入和执行权限。
对于 SQL 数据服务，Developer 工具不会强制执行连接权限。而是强制实施列级别和传递安全以限制对数据的访问。
- 数据集成服务。在用户尝试预览数据或运行映射、结果卡或配置文件时，强制执行执行权限。

注意: 您无法分配对以下连接的权限：剖析仓库、数据对象缓存数据库或模型存储库。

连接权限的类型

您可以向用户分配不同权限类型以执行以下操作：

操作	权限类型
查看除密码以外的所有连接元数据，如连接名称、类型、说明、连接字符串和用户名。	读取
编辑所有连接元数据，包括密码。删除连接。具有写入权限的用户可继承读取权限。	写入
访问由连接定义的基本数据源中的物理数据。用户可以预览数据、运行映射、运行工作流映射任务中的映射、运行结果卡或运行使用连接的配置文件。 访问由连接定义的基本数据源中的物理数据。用户可以预览数据、运行映射、运行工作流映射任务中的映射或运行使用连接的配置文件。	执行
授予和撤销对连接的权限。	授予

默认连接权限

域管理员拥有对所有连接的所有权限。创建连接的用户拥有对连接的读取、写入、执行和授予权限。默认情况下，所有用户都有权对连接执行以下操作：

- 查看基本连接元数据，如连接名称、类型和说明。
- 在 Developer 工具中使用映射中的连接。
- 在 Analyst 工具中对连接中的对象创建配置文件。

分配对连接的权限

分配对连接的权限时，可以定义用户或组对连接的访问级别。

1. 在“管理”选项卡中，选择**连接**视图。
2. 在导航器中，选择连接。
3. 在内容面板中，选择**权限**视图。
4. 单击**组**或**用户**选项卡。
5. 单击**操作 > 分配权限**。
分配权限对话框将显示没有该连接权限的所有用户或组。
6. 输入筛选条件搜索用户和组，然后单击**筛选**按钮。
7. 选择某个用户或组，然后单击**下一步**。
8. 为要分配的每个权限类型选择**允许**。
9. 单击**完成**。

查看连接的权限详细信息

当您查看权限详细信息时，可以查看有效权限的来源。

1. 在“管理”选项卡中，选择**连接**视图。

2. 在导航器中，选择连接。
3. 在内容面板中，选择**权限**视图。
4. 单击**组**或**用户**选项卡。
5. 选择某个用户或组，然后单击**操作 > 查看权限详细信息**。
此时将显示**查看权限详细信息**对话框。该对话框显示了分配给用户或组的直接权限和分配给父组的直接权限。此外，权限详细信息还显示用户或组是否已分配可绕过权限检查的管理员角色。
6. 单击**关闭**。
7. 或者单击**编辑权限**以编辑直接权限。

编辑对连接的权限

您可以为用户或组编辑对连接的直接权限。但无法撤销继承权限或您自己的权限。

注意: 如果撤销了对对象的直接权限，用户或组可能仍然会从父组或对象继承权限。

1. 在“管理”选项卡中，选择**连接**视图。
2. 在导航器中，选择连接。
3. 在内容面板中，选择**权限**视图。
4. 单击**组**或**用户**选项卡。
5. 输入筛选条件搜索用户和组，然后单击**筛选**按钮。
6. 选择某个用户或组，然后单击**操作 > 编辑直接权限**。

此时将显示**编辑直接权限**对话框。

7. 选择允许或撤销权限。
 - 选择**允许**分配权限。
 - 清除**允许**撤销单个权限。
 - 选择**撤销**撤销所有权限。

您可以单击**查看权限详细信息**查看是否已直接分配或继承该权限。

8. 单击**确定**。

群集配置权限

权限可控制用户或组对群集配置拥有的访问级别。

可以在 Administrator 工具和 Informatica 命令行界面中配置群集配置权限。

用户或组对群集配置可以拥有以下权限：

- 读取。用户或组成员可以查看群集配置。
- 写入。用户或组成员可以编辑群集配置。包括读取权限。
- 执行。用户或组成员可以在 Hadoop 环境中运行映射。
- 授予。用户或组成员可以向其他用户和组授予对群集配置的权限。包括读取权限。
- 全部。用户将继承所有允许的权限。

默认情况下，所有用户都具有查看群集配置名称的权限。

应用程序和应用程序对象权限

权限用于控制用户或组对应用程序和应用程序对象（如映射和工作流）的访问级别。

您可以在 Administrator 工具中或者从命令行配置应用程序和应用程序对象权限。

应用程序和应用程序对象权限的类型

您可以向用户和组分配查看、授予和执行权限。

您可以向用户和组分配以下权限：

查看权限

查看应用程序和应用程序对象。

授予权限

授予和撤销对应用程序和应用程序对象的权限。

执行权限

运行应用程序和应用程序对象。

注意：要通过 Administrator 工具或命令行执行诸如启动、停止或备份等应用程序操作，用户必须具有应用程序的执行权限和“管理应用程序”特权。

分配对应用程序或应用程序对象的权限

当您分配对应用程序或应用程序对象的权限时，您可以定义用户或组对应用程序或应用程序对象的访问级别。

1. 在“管理”选项卡上，选择**服务和节点**视图。
2. 在导航器中，选择数据集成服务。
3. 在内容面板中，选择**应用程序**视图。
4. 选择应用程序、映射或工作流。
5. 在详细信息面板中，选择**组权限**或**用户权限**视图。
6. 单击**分配权限**按钮。
7. 输入筛选条件搜索用户和组，然后单击**筛选**按钮。
8. 选择某个用户或组，然后单击**下一步**。
9. 为要分配的每个权限类型选择**允许**。
10. 单击**完成**。

分配权限对话框显示对应用程序或应用程序对象没有权限的所有用户或组。

查看对应用程序或应用程序对象的权限详细信息

当您查看权限详细信息时，可以查看有效权限的来源。

1. 在“管理”选项卡上，选择**服务和节点**视图。
2. 在导航器中，选择数据集成服务。
3. 在内容面板中，选择**应用程序**视图。
4. 选择应用程序、映射或工作流。
5. 在详细信息面板中，选择**组权限**或**用户权限**视图。

6. 输入筛选条件搜索用户和组，然后单击**筛选**按钮。
7. 选择用户或组并单击**查看权限详细信息**按钮。
此时将显示**权限详细信息**对话框。该对话框显示分配给用户或组的直接权限、分配给父组的直接权限，以及从父对象继承的权限。此外，权限详细信息还显示用户或组是否已分配可绕过权限检查的管理员角色。
8. 单击**关闭**。
9. 或者单击**编辑权限**以编辑直接权限。

编辑对应用程序或应用程序对象的权限

您可以为用户或组编辑对应用程序或应用程序对象的直接权限。但无法撤销继承权限或您自己的权限。

注意: 如果撤销了对对象的直接权限，用户或组可能仍然会从父组或对象继承权限。

1. 在“管理”选项卡上，选择**服务和节点**视图。
2. 在导航器中，选择数据集成服务。
3. 在内容面板中，选择**应用程序**视图。
4. 选择应用程序或应用程序对象。
5. 在详细信息面板中，选择**组权限**或**用户权限**视图。
6. 输入筛选条件搜索用户和组，然后单击**筛选**按钮。
7. 选择用户或组并单击**编辑直接权限**按钮。

此时将显示**编辑直接权限**对话框。

8. 选择允许或撤销权限。
 - 选择**允许**分配权限。
 - 清除**允许**撤销单个权限。
 - 选择**撤销**撤销所有权限。

您可以单击**查看权限详细信息**查看是否已直接分配或继承该权限。

9. 单击**确定**。

拒绝对应用程序或应用程序对象的权限

您可以明确拒绝对应用程序和应用程序对象的权限。当您拒绝权限时，您正将例外应用于有效权限。

SQL 数据服务权限

最终用户可以通过 JDBC 或 ODBC 客户端工具连接到 SQL 数据服务。连接后，用户可以针对 SQL 数据服务中的虚拟表运行 SQL 查询，或者用户也可以运行 SQL 数据服务中的虚拟存储过程。权限可控制用户对 SQL 数据服务拥有的访问级别。

可以向用户和组分配对以下 SQL 数据服务对象的权限：

- SQL 数据服务
- 虚拟表
- 虚拟存储过程

当您分配对 SQL 数据服务对象的权限时，用户或组将继承属于 SQL 数据服务对象的所有对象的相同权限。例如，您可以分配对 SQL 数据服务的用户选择权限。该用户将继承对 SQL 数据服务中所有虚拟表的选择权限。

您可以拒绝用户和组对部分 SQL 数据服务对象的权限。拒绝权限后，您可以配置用户和组可能已经拥有的权限以外的权限。例如，您不能将权限分配给虚拟表中的列，但可以拒绝用户运行包含该列的 SQL SELECT 语句。

SQL 数据服务权限类型

可以向用户和组分配以下权限：

- 授予权限。用户可以使用 Administrator 工具或使用 *infacmd* 命令行程序授予和撤销对 SQL 数据服务对象的权限。
- 执行权限。用户可以使用 JDBC 或 ODBC 客户端工具运行 SQL 数据服务中的虚拟存储过程。
- 选择权限。用户可以使用 JDBC 或 ODBC 客户端工具对 SQL 数据服务中的虚拟表运行 SQL SELECT 语句。

部分权限不适用于所有 SQL 数据服务对象。

下表介绍了各个 SQL 数据服务对象的权限：

对象	授予权限	执行权限	选择权限
SQL 数据服务	授予和撤销对 SQL 数据服务和 SQL 数据服务中的所有对象的权限。	运行 SQL 数据服务中的所有虚拟存储过程。	对 SQL 数据服务中的所有虚拟表运行 SQL SELECT 语句。
虚拟表	授予和撤销对虚拟表的权限。	-	对虚拟表运行 SQL SELECT 语句。
虚拟存储过程	授予和撤销对虚拟存储过程的权限。	运行虚拟存储过程。	-

分配对 SQL 数据服务的权限

分配对 SQL 数据服务对象的权限时，您可以定义用户或组对对象的访问级别。

1. 在管理选项卡上，选择**服务和节点**视图。
2. 在导航器中，选择数据集成服务。
3. 在内容面板中，选择**应用程序**视图。
4. 选择 SQL 数据服务对象。
5. 在详细信息面板中，选择**组权限**或**用户权限**视图。
6. 单击**分配权限**按钮。
分配权限对话框将显示对 SQL 数据服务对象没有权限的所有用户或组。
7. 输入筛选条件搜索用户和组，然后单击**筛选**按钮。
8. 选择某个用户或组，然后单击**下一步**。
9. 为要分配的每个权限类型选择**允许**。
10. 单击**完成**。

查看对 SQL 数据服务的权限详细信息

当您查看权限详细信息时，可以查看有效权限的来源。

1. 在管理选项卡上，选择**服务和节点**视图。

2. 在导航器中，选择数据集成服务。
3. 在内容面板中，选择**应用程序**视图。
4. 选择 SQL 数据服务对象。
5. 在详细信息面板中，选择**组权限**或**用户权限**视图。
6. 输入筛选条件搜索用户和组，然后单击**筛选**按钮。
7. 选择用户或组并单击**查看权限详细信息**按钮。

此时将显示**权限详细信息**对话框。该对话框显示分配给用户或组的直接权限、分配给父组的直接权限，以及从父对象继承的权限。此外，权限详细信息还显示用户或组是否已分配可绕过权限检查的管理员角色。

8. 单击**关闭**。
9. 或者单击**编辑权限**以编辑直接权限。

编辑对 SQL 数据服务的权限

您可以编辑对用户或组的 SQL 数据服务的直接权限。但无法撤销继承权限或您自己的权限。

注意: 如果撤销了对对象的直接权限，用户或组可能仍然会从父组或对象继承权限。

1. 在管理选项卡上，选择**服务和节点**视图。
2. 在导航器中，选择数据集成服务。
3. 在内容面板中，选择**应用程序**视图。
4. 选择 SQL 数据服务对象。
5. 在详细信息面板中，选择**组权限**或**用户权限**视图。
6. 输入筛选条件搜索用户和组，然后单击**筛选**按钮。
7. 选择用户或组并单击**编辑直接权限**按钮。

此时将显示**编辑直接权限**对话框。

8. 选择允许或撤销权限。
 - 选择**允许**分配权限。
 - 清除**允许**撤销单个权限。
 - 选择**撤销**撤销所有权限。

您可以单击**查看权限详细信息**查看是否已直接分配或继承该权限。

9. 单击**确定**。

拒绝对 SQL 数据服务的权限

您可以显式拒绝对某些 SQL 数据服务对象的权限。当您拒绝对 SQL 数据服务中某个对象的权限时，您将对有效权限应用例外。

要拒绝权限，请使用以下 `infacmd` 命令之一：

- `infacmd sql SetStoredProcedurePermissions`。拒绝存储过程级别的执行或授予权限。
- `infacmd sql SetTablePermissions`。拒绝虚拟表级别的选择和授予权限。
- `infacmd sql SetColumnPermissions`。拒绝列级别的选择权限。

每个命令都包含应用权限的选项 (`-ap`) 和拒绝权限的选项 (`-dp`)。 `SetColumnPermissions` 命令不包括应用权限选项。

注意: 您无法通过 Administrator 工具拒绝权限。

数据集成服务在针对虚拟数据库运行 SQL 查询和存储过程之前验证权限。数据集成服务从 SQL 数据服务级别开始验证用户或组的权限。当权限应用于 SQL 数据服务中的父对象时，子对象会继承该权限。数据集成服务将检查被拒绝的列级别权限。

列级别安全

管理员可以拒绝对 SQL 数据对象的虚拟表中的列的访问。管理员可以为针对限制列执行的查询配置数据集成服务行为。

如果用户查询没有权限的列时，可能会发生以下结果：

- 查询返回一个替代值，而不是数据。查询在返回的每一行中返回一个替代值。替代值通过查询替换列值。如果查询中包含筛选器或联接，结果替代出现在结果中。
- 查询失败，显示没有足够的权限错误。

有关配置 SQL 数据服务安全的详细信息，请参阅 Informatica 入门知识库中的“如何配置 SQL 数据服务的安全”章节：

https://kb.informatica.com/h2l/HowTo%20Library/1/0266_ConfiguringSecurityForSQLDataServices.pdf。

受限制列

在配置列级别安全时，您可以设置列选项来确定用户在查询中选择限制列时发生的行为。您可以使用默认值替代受限制数据。或者，可以在用户选择限制列时使查询失败。

例如，管理员拒绝用户访问“员工”表中的工资列。管理员可以将工资列的替代值配置为 100,000。当用户在 SQL 查询中选择工资列时，数据集成服务为每一行中的工资返回 100,000。

请运行 `infacmd sql UpdateColumnOptions` 命令配置列选项。您无法在 Administrator 工具中设置列选项。

运行 `infacmd sql UpdateColumnOptions` 时，您可以输入以下选项：

`ColumnOptions.DenyWith=option`

确定替代限制列值还是使查询失败。如果替代列值，则可以选择将值替换为空值或常量值。输入以下选项之一：

- 错误。当 SQL 查询选择限制列时，使查询失败并返回错误。
- 空。对每一行中的限制列返回空值。
- 值。返回常量值以代替每一行中的限制列。可在 `ColumnOptions.InsufficientPermissionValue` 选项中配置常量值。

`ColumnOptions.InsufficientPermissionValue=value`

将限制列值替换为常量。默认值为空字符串。如果数据集成服务将列替换为空字符串，但列为数字或日期，则查询返回错误。如果未配置 `DenyWith` 选项的值，数据集成服务会忽略 `InsufficientPermissionValue` 选项。

要配置列的替代值，请使用以下语法输入命令：

```
infacmd sql UpdateColumnOptions -dn empDomain -sn DISService -un Administrator -pd Adminpass -sql ds
employee_APP.employees_SQL -t Employee -c Salary -o ColumnOptions.DenyWith=VALUE
ColumnOptions.InsufficientPermissionValue=100000
```

如果未配置受限制列的任一选项，默认为不使查询失败。查询运行，数据集成服务将列值替换为“无”。

添加列级别安全

使用 `infacmd sql SetColumnPermissions` 命令配置列级别安全。您无法通过 Administrator 工具设置列级别安全。

Employee 表包含 FirstName、LastName、Dept 和 Salary 列。您希望允许用户访问员工表，但限制用户访问工资列。

要限制用户访问工资列，请禁用数据集成服务，然后输入类似于以下命令的 `infacmd`：

```
infacmd sql SetColumnPermissions -dn empDomain -sn DISService -un Administrator -pd Adminpass -sqlds employee_APP.employees -t Employee -c Salary gun -Tom -dp SQL_Select
```

以下 SQL 语句在工资列返回“空”：

```
Select * from Employee
Select LastName, Salary from Employee
```

默认行为是返回空值。

Web 服务权限

最终用户能够通过 Web 服务客户端发送 Web 服务请求和接收 Web 服务响应。权限控制用户对 Web 服务的访问级别。

可以向用户和组分配针对以下 Web 服务对象的权限：

- Web 服务
- REST Web 服务资源
- SOAP Web 服务操作

分配 Web 服务对象的权限时，用户和组继承属于 Web 服务对象的所有对象上的相同权限。例如，为用户分配针对 Web 服务的执行权限。该用户将继承 Web 服务中的 Web 服务操作的执行权限。

您可以拒绝用户和组执行 Web 服务操作的权限。拒绝权限后，您可以配置用户和组可能已经拥有的权限以外的权限。例如，用户拥有对包含三项操作的 Web 服务的执行权限。您可以拒绝用户运行属于 Web 服务的一项 Web 服务操作。

Web 服务权限的类型

管理员可将 Web 服务权限分配给以下类型的用户和组：

- Web 服务使用者。向 Web 服务发送请求并接收来自 Web 服务的响应的本地域用户。该用户必须具有对 Web 服务的执行权限。
- Web 服务管理员。可以执行以下操作的用户：登录到 Administrator，编辑 Web 服务属性以及向其他用户授予权限。
- Web 服务操作员。可以执行以下操作的用户：登录到 Administrator，监视 Web 服务以及启动或停止 Web 服务。

管理员可以将以下权限分配给用户和组：

- 授予权限。用户可以使用 Administrator 工具或使用 `infacmd` 命令行程序管理对 Web 服务对象的权限。
- 执行权限。用户可以发送 Web 服务请求并接收 Web 服务响应。

下表介绍了每个 SOAP Web 服务对象的权限：

对象	授予权限	执行权限
SOAP Web 服务	授予和撤消对 Web 服务以及 Web 服务内的所有 Web 服务操作的权限。	发送 Web 服务请求以及接收来自 Web 服务内的所有 Web 服务操作的 Web 服务响应。
SOAP Web 服务操作	授予、撤消和拒绝对 Web 服务操作的权限。	发送 Web 服务请求以及接收来自 Web 服务操作的 Web 服务响应。

下表介绍了每个 REST Web 服务对象的权限：

对象	授予权限	执行权限
REST Web 服务	授予和撤消对 REST Web 服务以及 Web 服务内的所有 Web 服务资源的权限。	发送 Web 服务请求以及接收来自 REST Web 服务中所有 Web 服务资源的 Web 服务响应。
REST 资源	授予、撤消和拒绝对 REST Web 服务资源的权限。	发送 Web 服务请求以及接收来自 REST Web 服务资源的 Web 服务响应。

分配对 Web 服务的权限

分配对 Web 服务对象的权限时，可以定义用户或组对该对象的访问级别。

1. 在管理选项卡上，选择**服务和节点**视图。
2. 在导航器中，选择数据集成服务。
3. 在内容面板中，选择**应用程序**视图。
4. 选择 Web 服务对象。
5. 在详细信息面板中，选择**组权限**或**用户权限**视图。
6. 单击**分配权限**按钮。
分配权限对话框将显示对 SQL 数据服务对象没有权限的所有用户或组。
7. 输入筛选条件搜索用户和组，然后单击**筛选**按钮。
8. 选择某个用户或组，然后单击**下一步**。
9. 为要分配的每个权限类型选择**允许**。
10. 单击**完成**。

查看 Web 服务的权限详细信息

当您查看权限详细信息时，可以查看有效权限的来源。

1. 在管理选项卡上，选择**服务和节点**视图。
2. 在导航器中，选择数据集成服务。
3. 在内容面板中，选择**应用程序**视图。
4. 选择 Web 服务对象。
5. 在详细信息面板中，选择**组权限**或**用户权限**视图。
6. 输入筛选条件搜索用户和组，然后单击**筛选**按钮。
7. 选择用户或组并单击**查看权限详细信息**按钮。

此时将显示**权限详细信息**对话框。该对话框显示分配给用户或组的直接权限、分配给父组的直接权限，以及从父对象继承的权限。此外，权限详细信息还显示用户或组是否已分配可绕过权限检查的管理员角色。

8. 单击**关闭**。
9. 或者单击**编辑权限**以编辑直接权限。

编辑对 Web 服务的权限

您可以为用户或组编辑对 Web 服务的直接权限。编辑对 Web 服务对象的权限时，可以拒绝对该对象的权限。但无法撤销继承权限或您自己的权限。

注意: 如果撤销了对对象的直接权限，用户或组可能仍然会从父组或对象继承权限。

1. 在管理选项卡上，选择**服务和节点**视图。
2. 在导航器中，选择数据集成服务。
3. 在内容面板中，选择**应用程序**视图。
4. 选择 Web 服务对象。
5. 在详细信息面板中，选择**组权限**或**用户权限**视图。
6. 输入筛选条件搜索用户和组，然后单击**筛选**按钮。
7. 选择用户或组并单击**编辑直接权限**按钮。

此时将显示**编辑直接权限**对话框。

8. 选择允许或撤销权限。
 - 选择**允许**分配权限。
 - 选择**拒绝**拒绝对 Web 服务对象的权限。
 - 清除**允许**撤销单个权限。
 - 选择**撤销**撤销所有权限。

您可以单击**查看权限详细信息**查看是否已直接分配或继承该权限。

9. 单击**确定**。

第 11 章

审计报告

本章包括以下主题：

- [审计报告概览, 181](#)
- [用户个人信息, 182](#)
- [用户组关联, 182](#)
- [特权, 183](#)
- [角色关联, 184](#)
- [域对象权限, 184](#)
- [选择审计报表的用户, 184](#)
- [选择审计报告的组, 185](#)
- [选择审计报告的角色, 186](#)

审计报告概览

使用审计报告可查看 Informatica 域中用户和组及向其分配的特权和权限的相关信息。

您可以生成以下审计报告：

用户个人信息

显示域中用户帐户的相关信息，包括用户状态。可以选择要为其生成报告的用户或组。

用户组关联

显示有关用户及这些用户所属组的信息。可以选择要为其生成报告的用户或组。

特权

显示分配给域中用户和组的特权的相关信息。可以选择要为其生成报告的用户或组。

角色

显示分配给域中用户和组的角色的相关信息。可以选择要为其生成报告的角色。

域对象权限

显示用户和组对其拥有权限的域对象的相关信息。可以选择要为其生成报告的用户或组。

可以生成不同格式（包括 CSV、文本或 PDF 文件）的审计报告。还可以在屏幕上查看报告。

可以从 Administrator 工具或命令行中生成审计报告。要从命令行中运行审计报告，请运行 `infacmd aud` 命令行程序。

用户个人信息

- 用户个人信息报表显示域中的联系人信息和用户帐户状态。
- 如果运行组的报表，报表将按组来组织用户列表，并显示每个组的组名称和安全域。报表单独显示嵌套组。
- 用户个人信息报表显示以下信息：
- 登录名称
 - 用户帐户的登录名。
 - 全名
 - 用户帐户的全名。
 - 安全域
 - 用户所属的安全域。
 - 说明
 - 用户帐户的说明。
 - 电子邮件 ID
 - 用户帐户的电子邮件地址。
 - 电话
 - 用户帐户的电话号码。
 - 帐户已锁定
 - 指示帐户是否被锁定。如果帐户被锁定，报表将显示“是”，如果帐户未锁定，报表将显示“否”。
 - 帐户已禁用
 - 指示帐户是否被禁用。如果帐户被禁用，报表将显示“是”，如果帐户未禁用，报表将显示“否”。

用户组关联

- “用户组关联”报告显示有关用户及其关联的组的信息。
- 如果为用户运行报告，该报告会显示用户及其所属组的列表。
- “用户组关联”报告显示以下信息：
- 登录名称
 - 用户帐户的登录名。
 - 全名
 - 用户帐户的全名。
 - 安全域
 - 用户帐户所属的安全域。
 - 组名称
 - 用户所属的组的名称。
 - 组路径
 - 如果组是单个组，则组路径显示组名称。如果组是嵌套组，则组路径显示组在嵌套组的层次结构中的位置。

组安全域

用户所属的组的安全域。

如果为组运行报告，报告将按组整理用户列表，并显示每个组的组名称和安全域。报告单独显示嵌套组。对于每个组，该报告显示用户及属于该组的子组的列表。

对于属于该组的用户，“用户组关联”报告显示以下信息：

登录名称

用户帐户的登录名。

全名

用户帐户的全名。

安全域

用户帐户所属的安全域。

对于属于该组的子组，“用户组关联”报告显示以下信息：

组名称

组的名称。

安全域

组所属的安全域。

组路径

如果组是单个组，则组路径显示组名称。如果组是嵌套组，则组路径显示组在嵌套组的层次结构中的位置。

特权

“特权”报告显示用户和组以及分配给这些用户和组的特权。

如果为用户运行报告，该报告会显示用户以及分配给每个用户的特权的列表。如果为组运行报告，该报告会显示组以及分配给每个组的特权的列表。

特权报告显示以下信息：

特权名称

特权的名称。

特权路径

包含特权的特权组的层次结构。

对象名称

允许特权的对象的名称。

对象类型

允许特权的对象的类型。

角色关联

角色关联报告显示角色列表以及分配角色的用户和组。

角色关联报告显示以下信息：

登录名称

分配角色的用户帐户的登录名。针对用户列表显示。

全名

分配角色的用户帐户的全名。针对用户列表显示。

组名称

分配角色的组的名称。针对组列表显示。

安全域

用户或组所属的安全域。

对象名称

允许对其拥有角色中的特权集的对象名称。

对象类型

允许对其拥有角色中的特权集的对象类型。

域对象权限

“域对象权限”报告显示用户和组以及用户和组具有权限的对象。

如果为用户运行报告，该报告会显示用户以及用户具有权限的对象的列表。如果为组运行报告，该报告会显示组以及组具有权限的对象的列表。

“域对象权限”报告显示以下信息：

对象名称

用户或组具有权限的对象名称。

对象类型

用户或组具有权限的对象类型。

对象路径

存储库中对象的位置。

选择审计报表的用户

您可以为多个用户生成一份审计报表。

1. 在 Administrator 工具中，单击**安全 > 审计报表**。
2. 从**选择报表类型**列表中，选择要运行的审计报表的类型。
3. 从**为以下对象生成报表**列表中，选择**用户**并单击**执行**。

此时将显示**选择用户**对话框。默认情况下，将选择**用户**图标并显示所有可用用户的列表。该列表显示用户和用户所属安全域的完整名称。

4. 从**可用用户**列表中，选择要为其运行报表的用户。

使用 Shift 键或 Ctrl 键选择多个用户。

5. 要按组选择用户，请单击**组**图标。

可用组列表将显示域中的所有组，**成员**列表将显示属于组成员的用户。从**成员**列表中，选择要为其运行报表的用户。可以从多个组中选择用户。

6. 单击**添加**。

要为所有用户运行报表，请单击**用户**图标，然后在没有选择任何用户的情况下单击**全部添加**。

要为组中的所有用户运行报表，请单击**组**图标。选择一个组，然后在没有从**成员**列表中选择任何用户的情况下单击**全部添加**。

所选用户将移至**选定用户**列表。

7. 从**报表输出格式**列表中，选择要查看报表的格式。

默认情况下，报表将显示在屏幕上。

您还可以使用下列格式之一查看审计报告：

- 文本。生成文本文件格式的审计报告，并在列中列出值。
- CSV。生成文本文件格式的审计报告，并以逗号分隔值。
- PDF。生成 .pdf 格式的审计报告。必须安装 Acrobat Reader 才能查看报表。

8. 单击**生成报表**。

选择审计报告的组

可以为多个组运行审计报告

1. 在 Administrator 工具中，单击**安全 > 审计报告**。

2. 从**选择报表类型**列表中，选择要运行的审计报告的类型。

3. 从**为以下对象生成报告**列表中，选择**组**并单击**执行**。

此时将显示**选择组**对话框。组列表按照安全域排列。

4. 从**可用组**列表中，选择要为其运行报告的组。

使用 Shift 键或 Ctrl 键选择多个组。

5. 单击**添加**。

要为所有组运行报告，不选择组，而是单击**全部添加**。

所选组将移至**已选组**列表。

6. 从**报告输出格式**列表中，选择要用来查看报告的格式。

默认情况下，报告显示在屏幕上。

还可以使用下列格式之一运行审计报告：

- 文本。生成文本文件格式的审计报告，并在列中列出值。
- CSV。生成文本文件格式的审计报告，并以逗号分隔值。
- PDF。生成 .pdf 格式的审计报告。必须安装 Acrobat Reader 才能查看报表。

7. 单击**生成报表**。

选择审计报告的角色

运行角色关联报告时，必须选择要为其运行报告的角色。

1. 在 Administrator 工具中，单击**安全 > 审计报告**。
2. 从**选择报告类型**列表中，选择**角色关联报告**。
3. 从**为以下对象生成报告**列表中，选择**角色**，然后单击**执行**。
此时将显示**选择角色**对话框。系统定义的角色列表与自定义角色列表分别显示。
4. 从**可用角色**列表中，选择要为其运行报告的角色。
使用 Shift 键或 Ctrl 键选择多个角色。
5. 单击**添加**。
要为所有角色运行报告，不选择角色，而是单击**全部添加**。
所选组将移至**已选角色**列表。
6. 从**报告输出格式**列表中，选择要用来查看报告的格式。
默认情况下，报告显示在屏幕上。
还可以使用下列格式之一运行审计报告：
 - 文本。生成文本文件格式的审计报告，并在列中列出值。
 - CSV。生成文本文件格式的审计报告，并以逗号分隔值。
 - PDF。生成 .pdf 格式的审计报告。必须安装 Acrobat Reader 才能查看报表。
7. 单击**生成报表**。

附录 A

命令行特权和权限

本附录包括以下主题：

- [infacmd as 命令, 187](#)
- [infacmd 群集命令, 188](#)
- [infacmd dis 命令, 189](#)
- [infacmd dp 命令, 190](#)
- [infacmd es 命令, 190](#)
- [infacmd ipc 命令, 191](#)
- [infacmd isp 命令, 191](#)
- [infacmd mas 命令, 199](#)
- [infacmd mi 命令, 199](#)
- [infacmd mrs 命令, 199](#)
- [infacmd ms 命令, 201](#)
- [infacmd tools 命令, 202](#)
- [infacmd ps 命令, 202](#)
- [infacmd pwx 命令, 203](#)
- [infacmd rms 命令, 204](#)
- [infacmd rtm 命令, 204](#)
- [infacmd sch 命令, 205](#)
- [infacmd sql 命令, 205](#)
- [infacmd wfs 命令, 206](#)
- [pmcmd 命令, 206](#)
- [pmrep 命令, 209](#)

infacmd as 命令

要运行 *infacmd as* 命令，用户必须具有列出的域特权、分析服务特权和域对象权限集之一。

下表列出了 *infacmd as* 命令所需的特权和权限：

infacmd as 命令	特权组	特权名称	权限对象...
CreateAuditTables	域管理	管理服务	分析服务运行所在的域或节点
CreateService	域管理	管理服务	分析服务运行所在的域或节点
DeleteAuditTables	域管理	管理服务	分析服务运行所在的域或节点
ListServiceOptions	-	-	分析服务
ListServiceProcessOptions	-	-	分析服务
UpdateServiceOptions	域管理	管理服务	分析服务运行所在的域或节点
UpdateServiceProcessOptions	域管理	管理服务	分析服务运行所在的域或节点

infacmd 群集命令

要运行 *infacmd cluster* 命令，用户必须具有列出的域特权和群集配置权限集之一。

下表列出了 *infacmd cluster* 命令所需的特权和权限：

infacmd 群集命令	特权组	特权名称	权限对象...
clearConfigurationProperties	域管理	管理连接	对群集配置的写入权限
createConfiguration	域管理	管理连接	对群集配置的写入权限
deleteConfiguration	域管理	管理连接	对群集配置的写入权限
exportConfiguration（使用敏感属性）	-	-	对群集配置的写入权限
exportConfiguration（不使用敏感属性）	-	-	对群集配置的读取权限
listAssociatedConnections	-	-	-
listConfigurations	-	-	-
listConfigurationGroupPermissions	-	-	-

infacmd 群集命令	特权组	特权名称	权限对象...
listConfigurationProperties	-	-	对群集配置的读取权限
listConfigurationSets	-	-	对群集配置的读取权限
listConfigurationUserPermissions	-	-	-
refreshConfiguration	域管理	管理连接	对群集配置的写入权限
setConfigurationPermissions	-	-	对群集配置的授予权限
setConfigurationProperties	域管理	管理连接	对群集配置的写入权限

infacmd dis 命令

要运行 *infacmd dis* 命令，用户必须具有所列的域特权、数据集成服务特权和域对象权限集之一。

下表列出了 *infacmd dis* 命令所需的特权和权限：

infacmd dis 命令	特权组	特权名称	权限对象...
BackupApplication	应用程序管理	管理应用程序	应用程序
CancelDataObjectCacheRefresh	-	-	-
CreateService	域管理	管理服务	数据集成服务运行所在的域或节点
DeployApplication	应用程序管理	管理应用程序	应用程序
ListApplicationObjects	-	-	-
ListApplications	-	-	-
ListComputeOptions	域管理	管理服务	数据集成服务
ListDataObjectOptions	-	-	-
ListServiceOptions	域管理	管理服务	数据集成服务
ListServiceProcessOptions	域管理	管理服务	数据集成服务
PurgeDataObjectCache	-	-	-

infacmd dis 命令	特权组	特权名称	权限对象...
RefreshDataObjectCache	-	-	-
RenameApplication	应用程序管理	管理应用程序	应用程序
RestoreApplication	应用程序管理	管理应用程序	应用程序
StartApplication	应用程序管理	管理应用程序	应用程序
StopApplication	应用程序管理	管理应用程序	应用程序
stopBlazeService	应用程序管理	管理应用程序	应用程序
UndeployApplication	应用程序管理	管理应用程序	应用程序
UpdateApplication	应用程序管理	管理应用程序	应用程序
UpdateApplicationOptions	应用程序管理	管理应用程序	应用程序
UpdateDataObjectOptions	应用程序管理	管理应用程序	-
UpdateComputeOptions	域管理	管理服务	数据集成服务
UpdateServiceOptions	域管理	管理服务	数据集成服务
UpdateServiceProcessOptions	域管理	管理服务	数据集成服务

infacmd dp 命令

用户必须为本机用户或分配有管理员角色，才能运行以下 infacmd dp 命令：

- startSparkJobServer
- stopSparkJobServer

infacmd es 命令

必须为用户分配域的管理员角色，用户才能运行以下 infacmd es 命令：

- ListServiceOptions
- UpdateServiceOptions
- UpdateSMTPOptions

infacmd ipc 命令

要运行 *infacmd ipc* 命令，用户必须具有列出的模型存储库对象权限之一。

下表列出了 *infacmd ipc* 命令所需的权限和特权：

infacmd ipc 命令	特权组	特权名称	权限对象...
ExportToPC	-	-	对创建要导出的引用表的文件夹的读取权限
genReuseReportFromPC	工具	访问 Repository Manager	-

infacmd isp 命令

要运行 *infacmd isp* 命令，用户必须具有列出的域特权、服务特权、域对象权限和连接权限集之一。

下表列出了 *infacmd isp* 命令所需的特权和权限：

infacmd isp 命令	特权组	特权名称	权限对象
AddAlertUser（针对其他用户）	安全管理	管理用户、组和角色	-
AddAlertUser（针对用户帐户）	-	-	-
AddConnectionPermissions	-	-	对连接的授予权限
AddDomainLink*	-	-	-
AddDomainNode	域管理	管理节点和网格	域和节点
AddGroupPrivilege	安全管理	授予特权和角色	域、Metadata Manager 服务、模型存储库服务或 PowerCenter 存储库服务。
AddLicense	域管理	管理服务	域或父文件夹
AddNodeResource	域管理	管理节点和网格	节点
AddRolePrivilege	安全管理	管理用户、组和角色	-
AddServiceLevel*	-	-	-
AddUserToGroup	安全管理	管理用户、组和角色	-

infacmd isp 命令	特权组	特权名称	权限对象
AssignGroupPermission (对应用程序服务或许可证对象)	域管理	管理服务	应用程序服务或许可证对象
AssignGroupPermission (对域) *	-	-	-
AssignGroupPermission (对文件夹)	域管理	管理域文件夹	文件夹
AssignGroupPermission (对节点和网格)	域管理	管理节点和网格	节点或网格
AssignGroupPermission (对操作系统配置文件) *	-	-	-
AssignISTOMMService	域管理	管理服务	Metadata Manager 服务
AssignLicense	域管理	管理服务	许可证对象和应用程序服务
AssignRSToWSHubService	域管理	管理服务	PowerCenter 存储库服务和 Web 服务中心
AssignRoleToGroup	安全管理	授予特权和角色	域、Metadata Manager 服务、模型存储库服务或 PowerCenter 存储库服务。
AssignRoleToUser	安全管理	授予特权和角色	域、Metadata Manager 服务、模型存储库服务或 PowerCenter 存储库服务。
AssignUserPermission (对应用程序服务或许可证对象)	域管理	管理服务	应用程序服务或许可证对象
AssignUserPermission (对域) *	-	-	-
AssignUserPermission (对文件夹)	域管理	管理域文件夹	文件夹
AssignUserPermission (对节点或网格)	域管理	管理节点和网格	节点或网格
AssignUserPermission (对操作系统配置文件) *	-	-	-
AssignUserPrivilege	安全管理	授予特权和角色	域、Metadata Manager 服务、模型存储库服务或 PowerCenter 存储库服务。
AssignedToLicense	域管理	管理服务	许可证对象和应用程序服务
ConvertLogFile	-	-	域或应用程序服务
CreateConnection*	-	-	-
CreateFolder	域管理	管理域文件夹	域或父文件夹
CreateGrid	域管理	管理节点和网格	分配给网格的域或父文件夹和节点

infacmd isp 命令	特权组	特权名称	权限对象
CreateGroup	安全管理	管理用户、组和角色	-
CreateIntegrationService	域管理	管理服务	域或父文件夹、PowerCenter 集成服务运行所在的节点或网格、许可证对象和关联的 PowerCenter 存储库服务
CreateMMService	域管理	管理服务	域或父文件夹、Metadata Manager 服务运行所在的节点、许可证对象和关联的 PowerCenter 集成服务和 PowerCenter 存储库服务
CreateOSProfile*	-	-	-
CreateRepositoryService	域管理	管理服务	域或父文件夹、PowerCenter 存储库服务运行所在的节点以及许可证对象
CreateRole	安全管理	管理用户、组和角色	-
CreateSAPBWService	域管理	管理服务	域或父文件夹、SAP BW 服务运行所在的节点或网格、许可证对象和关联的 PowerCenter 集成服务
CreateUser	安全管理	管理用户、组和角色	-
CreateWSHubService	域管理	管理服务	域或父文件夹、Web 服务中心运行所在的节点或网格、许可证对象和关联的 PowerCenter 存储库服务
DisableNodeResource	域管理	管理节点和网格	节点
DisableService（针对 Metadata Manager 服务）	域管理	管理服务执行	Metadata Manager 服务和关联的 PowerCenter 集成服务以及 PowerCenter 存储库服务
DisableService（针对所有其他应用程序服务）	域管理	管理服务执行	应用程序服务
DisableServiceProcess	域管理	管理服务执行	应用程序服务
DisableUser	安全管理	管理用户、组和角色	-
EditUser	安全管理	管理用户、组和角色	-
EnableNodeResource	域管理	管理节点和网格	节点

infacmd isp 命令	特权组	特权名称	权限对象
EnableService (针对 Metadata Manager 服务)	域管理	管理服务执行	Metadata Manager 服务和关联的 PowerCenter 集成服务以及 PowerCenter 存储库服务
EnableService (针对所有其他应用程序服务)	域管理	管理服务执行	应用程序服务
EnableServiceProcess	域管理	管理服务执行	应用程序服务
EnableUser	安全管理	管理用户、组和角色	-
ExportDomainObjects (针对连接)	域管理	管理连接	对连接的读取权限
ExportDomainObjects (针对用户、组和角色)	安全管理	管理用户、组和角色	-
ExportUsersAndGroups	安全管理	管理用户、组和角色	-
GetFolderInfo	-	-	文件夹
GetLastError	-	-	应用程序服务
GetLog	-	-	域或应用程序服务
GetNodeName	-	-	节点
GetServiceOption	-	-	应用程序服务
GetServiceProcessOption	-	-	应用程序服务
GetServiceProcessStatus	-	-	应用程序服务
GetServiceStatus	-	-	应用程序服务
GetSessionLog	运行时对象	监视	对存储库文件夹的读取权限
GetWorkflowLog	运行时对象	监视	对存储库文件夹的读取权限
帮助	-	-	-
ImportDomainObjects (针对连接)	域管理	管理连接	对连接的写入权限
ImportDomainObjects (针对用户、组和角色)	安全管理	管理用户、组和角色	-
ImportUsersAndGroups	安全管理	管理用户、组和角色	-
ListAlertUsers	-	-	域
ListAllGroups	-	-	-

infacmd isp 命令	特权组	特权名称	权限对象
ListAllRoles	-	-	-
ListAllUsers	-	-	-
ListConnectionOptions	-	-	对连接的读取权限
ListConnectionPermissions	-	-	-
ListConnectionPermissions by Group	-	-	-
ListConnectionPermissions by User	-	-	-
ListConnections	-	-	-
ListDomainLinks	-	-	域
ListDomainOptions	-	-	域
ListFolders	-	-	文件夹
ListGridNodes	-	-	-
ListGroupPermissions	-	-	-
ListGroupPrivilege	安全管理	授予特权和角色	域、Metadata Manager 服务、模型存储库服务或 PowerCenter 存储库服务。
ListGroupsForUser	-	-	域
ListLDAPConnectivity	安全管理	管理用户、组和角色	-
ListLicenses	-	-	许可证对象
ListNodeOptions	-	-	节点
ListNodeResources	-	-	节点
ListNodes	-	-	-
ListPlugins	-	-	-
ListRepositoryLDAPConfiguration	-	-	域
ListRolePrivileges	-	-	-
ListSMTPOptions	-	-	域
ListSecurityDomains	安全管理	管理用户、组和角色	-
ListServiceLevels	-	-	域

infacmd isp 命令	特权组	特权名称	权限对象
ListServiceNodes	-	-	应用程序服务
ListServicePrivileges	-	-	-
ListServices	-	-	-
ListUserPermissions	-	-	-
ListUserPrivilege	安全管理	授予特权和角色	域、Metadata Manager 服务、模型存储库服务或 PowerCenter 存储库服务。
MoveFolder	域管理	管理域文件夹	原始和目标文件夹
MoveObject（针对应用程序服务或许可证对象）	域管理	管理服务	原始和目标文件夹
MoveObject（针对节点或网格）	域管理	管理节点和网格	原始和目标文件夹
Ping	-	-	-
PurgeLog*	-	-	-
RemoveAlertUser（针对其他用户）	安全管理	管理用户、组和角色	-
RemoveAlertUser（针对您的用户帐户）	-	-	-
RemoveConnection	-	-	对连接的写入权限
RemoveConnectionPermissions	-	-	对连接的授予权限
RemoveDomainLink*	-	-	-
RemoveFolder	域管理	管理域文件夹	域或父文件夹和正在删除的文件夹
RemoveGrid	域管理	管理节点和网格	域或父文件夹和网格
RemoveGroup	安全管理	管理用户、组和角色	-
RemoveGroupPrivilege	安全管理	授予特权和角色	域、Metadata Manager 服务、模型存储库服务或 PowerCenter 存储库服务。
RemoveLicense	域管理	管理服务	域或父文件夹和许可证对象
RemoveNode	域管理	管理节点和网格	域或父文件夹和节点
RemoveNodeResource	域管理	管理节点和网格	节点

infacmd isp 命令	特权组	特权名称	权限对象
RemoveOSProfile*	-	-	-
RemoveRole	安全管理	管理用户、组和角色	-
RemoveRolePrivilege	安全管理	管理用户、组和角色	-
RemoveService	域管理	管理服务	域或父文件夹和应用程序服务
RemoveServiceLevel*	-	-	-
RemoveUser	安全管理	管理用户、组和角色	-
RemoveUserFromGroup	安全管理	管理用户、组和角色	-
RemoveUserPrivilege	安全管理	授予特权和角色	域、Metadata Manager 服务、模型存储库服务或 PowerCenter 存储库服务。
RenameConnection	-	-	对连接的写入权限
ResetPassword（针对其他用户）	安全管理	管理用户、组和角色	-
ResetPassword（针对您的用户帐户）	-	-	-
RunCPUProfile	域管理	管理节点和网格	节点
SetConnectionPermission	-	-	对连接的授予权限
SetLDAPConnectivity	安全管理	管理用户、组和角色	-
SetRepositoryLDAPConfiguration	-	-	域
ShowLicense	-	-	许可证对象
ShutdownNode	域管理	管理节点和网格	节点
SwitchToGatewayNode*	-	-	-
SwitchToWorkerNode*	-	-	-
UnAssignISMMSERVICE	域管理	管理服务	PowerCenter 集成服务和 Metadata Manager 服务
UnAssignRoleFromGroup	安全管理	授予特权和角色	域、Metadata Manager 服务、模型存储库服务或 PowerCenter 存储库服务。

infacmd isp 命令	特权组	特权名称	权限对象
UnAssignRoleFromUser	安全管理	授予特权和角色	域、Metadata Manager 服务、模型存储库服务或 PowerCenter 存储库服务。
UnassignLicense	域管理	管理服务	许可证对象和应用程序服务
UnassignRSWSHubService	域管理	管理服务	PowerCenter 存储库服务和 Web 服务中心
UnassociateDomainNode	域管理	管理节点和网格	节点
UpdateConnection	-	-	对连接的写入权限
UpdateDomainOptions*	-	-	-
UpdateFolder	域管理	管理域文件夹	文件夹
UpdateGatewayInfo*	-	-	-
UpdateGrid	域管理	管理节点和网格	网格和节点
UpdateIntegrationService	域管理	管理服务	PowerCenter 集成服务
UpdateLicense	域管理	管理服务	许可证对象
UpdateMMService	域管理	管理服务	Metadata Manager 服务
UpdateNodeOptions	域管理	管理节点和网格	节点
UpdateNodeRole	域管理	管理节点和网格	节点
UpdateOSProfile	安全管理	管理用户、组和角色	操作系统配置文件
UpdateRepositoryService	域管理	管理服务	PowerCenter 存储库服务
UpdateSAPBWService	域管理	管理服务	SAP BW 服务
UpdateSMTPOptions*	-	-	-
UpdateServiceLevel*	-	-	-
UpdateServiceProcess	域管理	管理服务	PowerCenter 集成服务 添加到 PowerCenter 集成服务中的每个节点
UpdateWSHubService	域管理	管理服务	Web 服务中心
generateHadoopConnectionFromHiveConnection	-	-	-

infacmd isp 命令	特权组	特权名称	权限对象
listMonitoringOptions	监视	监视配置	域
purgeMonitoringData	监视	监视配置	域
updateMonitoringOptions	监视	监视配置	域
*要运行这些命令，必须为用户分配该域的管理员角色。			

infacmd mas 命令

要运行 *infacmd dis* 命令，用户必须具有所列的域特权、元数据访问服务特权和域对象权限集之一。

下表列出了 *infacmd mas* 命令所需的特权和权限：

infacmd dis 命令	特权组	特权名称	权限对象...
CreateService	域管理	管理服务	运行元数据访问服务的域或节点
ListServiceOptions	域管理	管理服务	元数据访问服务
ListServiceProcessOptions	域管理	管理服务	元数据访问服务
UpdateServiceOptions	域管理	管理服务	元数据访问服务
UpdateServiceProcessOptions	域管理	管理服务	元数据访问服务

infacmd mi 命令

用户必须具有 Mass Ingestion 服务的管理员角色才能运行以下 *infacmd mi* 命令：

- clearSamlConfig
- updateSamlConfig

infacmd mrs 命令

要运行 *infacmd mrs* 命令，用户必须具有列出的域特权、模型存储库服务特权和模型存储库对象权限集之一。

用户可以对自己拥有的对象运行以下命令，这些命令与锁定和版本控制操作相关。在其他用户拥有的对象上运行命令需要“管理基于团队的开发”特权：

- CheckInObject
- ListCheckedOutObjects
- ListLockedObjects
- UndoCheckout
- UnlockObject

下表列出了 *infacmd mrs* 命令所需的特权和权限：

infacmd mrs 命令	特权组	特权名称	权限对象...
BackupContents	域管理	管理服务	模型存储库服务运行所在的域或节点
CheckInObject	域管理	管理基于团队的开发	模型存储库服务
CreateContents	域管理	管理服务	模型存储库服务运行所在的域或节点
CreateFolder	域管理	对于·Developer tool： - 访问 Developer 对于 Analyst 工具： - 访问 Analyst - 发现工作区访问	模型存储库服务
CreateProject	域管理	创建、编辑和删除项目	模型存储库服务
CreateService	域管理	管理服务	模型存储库服务运行所在的域或节点
DeleteContents	域管理	管理服务	模型存储库服务运行所在的域或节点
DeleteFolder	域管理	对于·Developer tool： - 访问 Developer 对于 Analyst 工具： - 访问 Analyst - 发现工作区访问	模型存储库服务
DeleteProject	域管理	创建、编辑和删除项目	模型存储库服务
ListBackupFiles	域管理	管理服务	模型存储库服务运行所在的域或节点
ListCheckedOutObjects	域管理	管理基于团队的开发	模型存储库服务
ListFolders	域管理	管理服务	模型存储库服务运行所在的域或节点
ListLockedObjects	域管理	管理基于团队的开发	模型存储库服务

infacmd mrs 命令	特权组	特权名称	权限对象...
ListProjects	域管理	对于·Developer tool: - 访问 Developer 对于 Analyst 工具: - 访问 Analyst - 发现工作区访问	模型存储库服务运行所在的域或节点
ListServiceOptions	-	-	模型存储库服务
ListServiceProcessOptions	-	-	模型存储库服务
PopulateVCS	域管理	管理基于团队的开发	模型存储库服务
ReassignCheckedOutObject	域管理	管理基于团队的开发	模型存储库服务
RebuildDependencyGraph	-	-	模型存储库服务
RenameFolder	域管理	对于·Developer tool: - 访问 Developer 对于 Analyst 工具: - 访问 Analyst - 发现工作区访问	模型存储库服务
RestoreContents	域管理	管理服务	模型存储库服务运行所在的域或节点
UndoCheckout	域管理	管理基于团队的开发	模型存储库服务
UnlockObject	域管理	管理基于团队的开发	模型存储库服务
UpdateServiceOptions	域管理	管理服务	模型存储库服务
UpdateServiceProcessOptions	域管理	管理服务	模型存储库服务
UpgradeContents	模型存储库服务管理	管理服务	模型存储库服务

infacmd ms 命令

要运行 *infacmd ms* 命令，用户必须具有列出的域对象权限集之一。

下表列出了 *infacmd ms* 命令所需的特权和权限：

infacmd ms 命令	特权组	特权名称	权限对象...
deleteMappingPersistedOutputs	-	-	在应用程序上执行
getRequestLog	-	-	-

infacmd ms 命令	特权组	特权名称	权限对象...
listMappingParams	-	-	-
listMappingPersistedOutputs	-	-	在应用程序上查看
listMappings	-	-	-
runMapping	-	-	对映射所使用的连接对象的执行权限

infacmd tools 命令

要运行 *infacmd tools* 命令，用户必须具有列出的模型存储库对象权限之一。

下表列出了 *infacmd tools* 命令所需的权限：

infacmd tools 命令	特权组	特权名称	权限对象...
ExportObjects	-	-	对项目执行读取操作
ImportObjects	-	-	对项目执行写入操作

infacmd ps 命令

要运行 *infacmd ps* 命令，用户必须具有列出的剖析特权和域对象权限集之一。

下表列出了 *infacmd ps* 命令所需的特权和权限：

infacmd ps 命令	特权组	特权名称	权限对象...
CreateWH	-	-	-
DropWH	-	-	-
执行	-	-	对项目执行读取操作 对源连接对象的执行权限

infacmd ps 命令	特权组	特权名称	权限对象...
列表	-	-	对项目执行读取操作
清除	-	-	对项目的读写和写入权限

infacmd ps 命令	特权组	特权名称	权限对象...
CreateWH	-	-	-
DropWH	-	-	-

infacmd pwx 命令

要运行 *infacmd pwx* 命令，用户必须具有列出的 PowerExchange 应用程序服务权限和特权集之一。

下表列出了 *infacmd pwx* 命令所需的特权和权限：

infacmd pwx 命令	特权组	特权名称	权限对象...
CloseForceListener	管理命令	closeforce	-
CloseListener	管理命令	关闭	-
CondenseLogger	管理命令	condense	-
CreateListenerService	域管理	管理服务	PowerExchange 应用程序服务运行所在的域或节点
CreateLoggerService	域管理	管理服务	PowerExchange 应用程序服务运行所在的域或节点
DisplayAllLogger	信息性命令	displayall	-
DisplayCPULogger	信息性命令	displaycpu	-
DisplayEventsLogger	信息性命令	displayevents	-
DisplayMemoryLogger	信息性命令	displaymemory	-
DisplayRecordsLogger	信息性命令	displayrecords	-
DisplayStatusLogger	信息性命令	displaystatus	-
FileSwitchLogger	管理命令	fileswitch	-
ListTaskListener	信息性命令	listtask	-

infacmd pwx 命令	特权组	特权名称	权限对象...
ShutDownLogger	管理命令	shutdown	-
StopTaskListener	管理命令	stoptask	-
UpdateListenerService	域管理	管理服务	PowerExchange 应用程序服务运行所在的域或节点
UpdateLoggerService	域管理	管理服务	PowerExchange 应用程序服务运行所在的域或节点

infacmd rms 命令

要运行 *infacmd rms* 命令，用户必须具有列出的域特权和权限集之一。

下表列出了 *infacmd rms* 命令所需的特权和权限：

infacmd rms 命令	特权组	特权名称	权限对象
ListComputeNodeAttributes	域管理	-	资源管理器服务
ListServiceOptions	域管理	-	资源管理器服务
SetComputeNodeAttributes	域管理	管理服务	资源管理器服务
UpdateServiceOptions	域管理	管理服务	资源管理器服务

infacmd rtm 命令

要运行 *infacmd rtm* 命令，用户必须具有列出的模型存储库服务特权和域对象权限集之一。

下表列出了 *infacmd rtm* 命令所需的特权和权限：

infacmd rtm 命令	特权组	特权名称	权限对象...
Deployimport	-	-	-
导出	-	-	对包含要导出的引用表的项目的读取权限
导入	-	-	对导入了引用表的项目的读取和写入权限

infacmd sch 命令

要运行 `infacmd sch` 命令，用户必须具有列出的特权和权限集之一。

下表列出了 `infacmd sch` 命令所需的特权和权限：

infacmd sch 命令	特权组	特权名称	权限对象
CreateSchedule	计划程序特权	创建计划	计划程序服务
DeleteSchedule	计划程序特权	删除计划	计划程序服务
ListSchedule	计划程序特权	查看计划	计划程序服务
ListServiceOptions	域特权	管理服务	计划程序服务
ListServiceProcessOptions	域特权	管理服务	计划程序服务
PauseAll	计划程序特权	编辑计划	计划程序服务
PauseSchedule	计划程序特权	编辑计划	计划程序服务
ResumeAll	计划程序特权	编辑计划	计划程序服务
ResumeSchedule	计划程序特权	编辑计划	计划程序服务
UpdateSchedule	计划程序特权	编辑计划	计划程序服务
UpdateService	域特权	管理服务	计划程序服务
UpdateServiceProcess	域特权	管理服务	计划程序服务
升级	域特权	管理服务	计划程序服务

infacmd sql 命令

要运行 `infacmd sql` 命令，用户必须具有列出的域特权、数据集成服务特权和域对象权限集之一。

下表列出了 `infacmd sql` 命令所需的特权和权限：

infacmd sql 命令	特权组	特权名称	权限对象...
ExecuteSQL	-	-	基于 SQL 语句中要访问的对象
ListColumnPermissions	-	-	-
ListSQLDataServiceOptions	-	-	-
ListSQLDataServicePermissions	-	-	-

infacmd sql 命令	特权组	特权名称	权限对象...
ListSQLDataServices	-	-	-
ListStoredProcedurePermissions	-	-	-
ListTableOptions	-	-	-
ListTablePermissions	-	-	-
PurgeTableCache	-	-	-
RefreshTableCache	-	-	-
RenameSQLDataService	应用程序管理	管理应用程序	-
SetColumnPermissions	-	-	对对象的授予权限
SetSQLDataServicePermissions	-	-	对对象的授予权限
SetStoredProcedurePermissions	-	-	对对象的授予权限
SetTablePermissions	-	-	对对象的授予权限
StartSQLDataService	应用程序管理	管理应用程序	-
StopSQLDataService	应用程序管理	管理应用程序	-
UpdateColumnOptions	应用程序管理	管理应用程序	-
UpdateSQLDataServiceOptions	应用程序管理	管理应用程序	-
UpdateTableOptions	应用程序管理	管理应用程序	-

infacmd wfs 命令

要运行 `infacmd wfs` 命令，用户不需要任何特权或权限。

pmcmd 命令

要运行 `pmcmd` 命令，用户必须具有列出的 PowerCenter 存储库服务特权和 PowerCenter 存储库对象权限集。

如果 PowerCenter 集成服务在安全模式下运行，用户必须具备关联的 PowerCenter 存储库服务的管理员角色才能运行以下命令：

- `aborttask`
- `abortworkflow`
- `getrunningssessionsdetails`

- getservicedetails
- getsessionstatistics
- gettaskdetails
- getworkflowdetails
- recoverworkflow
- scheduleworkflow
- starttask
- startworkflow
- stoptask
- stopworkflow
- unscheduleworkflow

下表列出了 *pmcmd* 命令所需的特权和权限：

pmcmd 命令	特权组	特权名称	权限
aborttask (由自有用户帐户启动)	-	-	对文件夹的读取和执行权限
aborttask (由其他用户启动)	运行时对象	管理执行	对文件夹的读取和执行权限
abortworkflow (由自有用户帐户启动)	-	-	对文件夹的读取和执行权限
abortworkflow (由其他用户启动)	运行时对象	管理执行	对文件夹的读取和执行权限
connect	-	-	-
disconnect	-	-	-
exit	-	-	-
getrunningsessionsdetails	运行时对象	监视	-
getservicedetails	运行时对象	监视	对文件夹执行读取操作
getserviceproperties	-	-	-
getsessionstatistics	运行时对象	监视	对文件夹执行读取操作
gettaskdetails	运行时对象	监视	对文件夹执行读取操作
getworkflowdetails	运行时对象	监视	对文件夹执行读取操作
帮助	-	-	-
pingservice	-	-	-

pmcmd 命令	特权组	特权名称	权限
recoverworkflow (由自有用户帐户启动)	运行时对象	执行	对文件夹的读取和执行权限 对连接对象的读取和执行权限 对操作系统配置文件的权限 (如果适用)
recoverworkflow (由其他用户启动)	运行时对象	管理执行	对文件夹的读取和执行权限 对连接对象的读取和执行权限 对操作系统配置文件的权限 (如果适用)
scheduleworkflow	运行时对象	管理执行	对文件夹的读取和执行权限 对连接对象的读取和执行权限 对操作系统配置文件的权限 (如果适用)
setfolder	-	-	对文件夹执行读取操作
setnowait	-	-	-
setwait	-	-	-
showsettings	-	-	-
starttask	运行时对象	执行	对文件夹的读取和执行权限 对连接对象的读取和执行权限 对操作系统配置文件的权限 (如果适用)
startworkflow	运行时对象	执行	对文件夹的读取和执行权限 对连接对象的读取和执行权限 对操作系统配置文件的权限 (如果适用)
stoptask (由自有用户帐户启动)	-	-	对文件夹的读取和执行权限
stoptask (由其他用户启动)	运行时对象	管理执行	对文件夹的读取和执行权限
stopworkflow (由自有用户帐户启动)	-	-	对文件夹的读取和执行权限
stopworkflow (由其他用户启动)	运行时对象	管理执行	对文件夹的读取和执行权限
unscheduleworkflow	运行时对象	管理执行	对文件夹的读取和执行权限
unsetfolder	-	-	对文件夹执行读取操作
版本	-	-	-

pmcmd 命令	特权组	特权名称	权限
waittask	运行时对象	监视	对文件夹执行读取操作
waitworkflow	运行时对象	监视	对文件夹执行读取操作

pmrep 命令

用户必须具有访问 Repository Manager 特权才能运行除以下命令之外的所有 *pmrep* 命令：

- 运行
- 创建
- 还原
- 升级
- 版本
- 帮助

要运行 *pmrep* 命令，用户必须具有列出的域特权、PowerCenter 存储库服务特权、域对象权限和 PowerCenter 存储库对象权限集之一。

用户必须是对象所有者或者具有 PowerCenter 存储库服务的管理员角色才能运行以下命令：

- AssignPermission
- ChangeOwner
- CreateQuery
- DeleteConnection
- DeleteDeploymentGroup
- DeleteFolder
- DeleteLabel
- DeleteQuery
- ModifyFolder（更改所有者、配置权限、将文件夹指定为共享或者编辑文件夹名称或说明）

下表列出了 *pmrep* 命令所需的特权和权限：

pmrep 命令	特权组	特权名称	权限
AddToDeploymentGroup	全局对象	管理部署组	对原始文件夹执行读取操作 对部署组执行读取和写入操作
ApplyLabel	-	-	对文件夹执行读取操作 对标签执行读取和执行操作
AssignPermission	-	-	-
BackUp	域管理	管理服务	对 PowerCenter 存储库服务的权限

pmrep 命令	特权组	特权名称	权限
ChangeOwner	-	-	-
CheckIn (针对自己的签出)	设计对象	创建、编辑和删除	对文件夹执行读取和写入操作
CheckIn (针对自己的签出)	源和目标	创建、编辑和删除	对文件夹执行读取和写入操作
CheckIn (针对自己的签出)	运行时对象	创建、编辑和删除	对文件夹执行读取和写入操作
签入 (针对其他人的签出)	设计对象	管理版本	对文件夹执行读取和写入操作
签入 (针对其他人的签出)	源和目标	管理版本	对文件夹执行读取和写入操作
签入 (针对其他人的签出)	运行时对象	管理版本	对文件夹执行读取和写入操作
CleanUp	-	-	-
ClearDeploymentGroup	全局对象	管理部署组	对部署组执行读取和写入操作
连接	-	-	-
创建	域管理	管理服务	对 PowerCenter 存储库服务的权限
CreateConnection	全局对象	创建连接	-
CreateDeploymentGroup	全局对象	管理部署组	-
CreateFolder	文件夹	创建	-
CreateLabel	全局对象	创建标签	-
CreateQuery	全局对象	创建查询	-
删除	域管理	管理服务	对 PowerCenter 存储库服务的权限
DeleteConnection	-	-	-
DeleteDeploymentGroup	-	-	-
DeleteFolder	-	-	-
DeleteLabel	-	-	-
DeleteObject	设计对象	创建、编辑和删除	对文件夹执行读取和写入操作
DeleteObject	源和目标	创建、编辑和删除	对文件夹执行读取和写入操作

pmrep 命令	特权组	特权名称	权限
DeleteObject	运行时对象	创建、编辑和删除	对文件夹执行读取和写入操作
DeleteQuery	-	-	-
DeployDeploymentGroup	全局对象	管理部署组	对原始文件夹执行读取操作 对目标文件夹执行读取和写入操作 对部署组执行读取和执行操作
DeployFolder	文件夹	对初始存储库的复制权限 对目标存储库的创建权限	对文件夹执行读取操作
ExecuteQuery	-	-	对查询执行读取和执行操作
退出	-	-	-
FindCheckout	-	-	对文件夹执行读取操作
GetConnectionDetails	-	-	对连接对象的读取权限
帮助	-	-	-
KillUserConnection	域管理	管理服务	对 PowerCenter 存储库服务的权限
ListConnections	-	-	对连接对象的读取权限
ListObjectDependencies	-	-	对文件夹执行读取操作
ListObjects	-	-	对文件夹执行读取操作
ListTablesBySess	-	-	对文件夹执行读取操作
ListUserConnections	域管理	管理服务	对 PowerCenter 存储库服务的权限
ModifyFolder（更改所有者、配置权限、将文件夹指定为共享或者编辑文件夹名称或说明）	-	-	-
ModifyFolder（更改状态）	文件夹	管理版本	对文件夹执行读取和写入操作
Notify	域管理	管理服务	对 PowerCenter 存储库服务的权限
ObjectExport	-	-	对文件夹执行读取操作
ObjectImport	设计对象	创建、编辑和删除	对文件夹执行读取和写入操作
ObjectImport	源和目标	创建、编辑和删除	对文件夹执行读取和写入操作

pmrep 命令	特权组	特权名称	权限
ObjectImport	运行时对象	创建、编辑和删除	对文件夹执行读取和写入操作
PurgeVersion	设计对象	管理版本	对文件夹执行读取和写入操作 对查询的读取、写入和执行权限（如果指定查询名称）
PurgeVersion	源和目标	管理版本	对文件夹执行读取和写入操作 对查询的读取、写入和执行权限（如果指定查询名称）
PurgeVersion	运行时对象	管理版本	对文件夹执行读取和写入操作 对查询的读取、写入和执行权限（如果指定查询名称）
PurgeVersion（在文件夹级别清除对象）	文件夹	管理版本	对文件夹执行读取和写入操作
PurgeVersion（在存储库级别清除对象）	域管理	管理服务	对 PowerCenter 存储库服务的权限
注册	域管理	管理服务	对 PowerCenter 存储库服务的权限
RegisterPlugin	域管理	管理服务	对 PowerCenter 存储库服务的权限
还原	域管理	管理服务	对 PowerCenter 存储库服务的权限
RollbackDeployment	全局对象	管理部署组	对目标文件夹执行读取和写入操作
运行	-	-	-
ShowConnectionInfo	-	-	-
SwitchConnection	运行时对象	创建、编辑和删除	对文件夹执行读取和写入操作 对连接对象的读取权限
TruncateLog	运行时对象	管理执行	对文件夹的读取和执行权限
UndoCheckout（针对自己的签出）	设计对象	创建、编辑和删除	对文件夹执行读取和写入操作
UndoCheckout（针对自己的签出）	源和目标	创建、编辑和删除	对文件夹执行读取和写入操作
UndoCheckout（针对自己的签出）	运行时对象	创建、编辑和删除	对文件夹执行读取和写入操作
UndoCheckout（针对其他人的签出）	设计对象	管理版本	对文件夹执行读取和写入操作

pmrep 命令	特权组	特权名称	权限
UndoCheckout (针对其他人的签出)	源和目标	管理版本	对文件夹执行读取和写入操作
UndoCheckout (针对其他人的签出)	运行时对象	管理版本	对文件夹执行读取和写入操作
取消注册	域管理	管理服务	对 PowerCenter 存储库服务的权限
UnregisterPlugin	域管理	管理服务	对 PowerCenter 存储库服务的权限
UpdateConnection	-	-	对连接对象执行读取和写入操作
UpdateEmailAddr	运行时对象	创建、编辑和删除	对文件夹执行读取和写入操作
UpdateSeqGenVals	设计对象	创建、编辑和删除	对文件夹执行读取和写入操作
UpdateSrcPrefix	运行时对象	创建、编辑和删除	对文件夹执行读取和写入操作
UpdateStatistics	域管理	管理服务	对 PowerCenter 存储库服务的权限
UpdateTargPrefix	运行时对象	创建、编辑和删除	对文件夹执行读取和写入操作
升级	域管理	管理服务	对 PowerCenter 存储库服务的权限
验证	设计对象	创建、编辑和删除	对文件夹执行读取和写入操作
验证	运行时对象	创建、编辑和删除	对文件夹执行读取和写入操作
版本	-	-	-

附录 B

自定义角色

本附录包括以下主题：

- [分析服务自定义角色, 214](#)
- [Metadata Manager 服务自定义角色, 215](#)
- [操作员自定义角色, 216](#)
- [PowerCenter 存储库服务自定义角色, 217](#)
- [Test Data Manager 自定义角色, 218](#)

分析服务自定义角色

分析服务 Business Glossary 使用者是一个自定义分析服务角色。

下表列出了向“分析服务 Business Glossary 使用者”自定义角色分配的默认特权：

特权组	特权名称
工作区访问	词汇表工作区

Metadata Manager 服务自定义角色

Metadata Manager 服务自定义角色包括 Metadata Manager 高级用户、Metadata Manager 基本用户和 Metadata Manager 中级用户角色。

Metadata Manager 高级用户

下表列出了向 Metadata Manager 高级用户自定义角色分配的默认特权：

特权组	特权名称
目录	<ul style="list-style-type: none">- 共享快捷方式- 查看沿袭- 查看相关目录- 查看报表- 查看配置文件结果- 查看目录- 查看关系- 管理关系- 查看注释- 发布注释- 删除注释- 查看链接- 管理链接- 查看词汇表- 管理对象
加载	<ul style="list-style-type: none">- 查看资源- 加载资源- 管理计划- 清除元数据- 管理资源
模型	<ul style="list-style-type: none">- 查看模型- 管理模型- 导出/导入模型
安全	管理目录权限

Metadata Manager 基本用户

下表列出了向 Metadata Manager 基本用户自定义角色分配的默认特权：

特权组	特权名称
目录	<ul style="list-style-type: none">- 查看沿袭- 查看相关目录- 查看目录- 查看关系- 查看注释- 查看链接
模型	查看模型

Metadata Manager 中级用户

下表列出了向 Metadata Manager 中级用户自定义角色分配的默认特权：

特权组	特权名称
目录	<ul style="list-style-type: none">- 查看沿袭- 查看相关目录- 查看报表- 查看配置文件结果- 查看目录- 查看关系- 查看注释- 发布注释- 删除注释- 查看链接- 管理链接- 查看词汇表
加载	<ul style="list-style-type: none">- 查看资源- 加载资源
模型	查看模型

操作员自定义角色

操作员自定义角色包括用于管理、计划和监视应用程序服务的特权。

下表列出了向操作员自定义角色分配的默认特权：

特权组	特权名称
应用程序管理	管理应用程序
域管理	管理服务执行
模型存储库服务管理	管理基于团队的开发
监视	<p>监视特权组包括以下特权：</p> <ul style="list-style-type: none">- 查看：查看其他用户的作业- 查看：查看统计信息- 查看：查看报告- 访问监视：从 Analyst 工具进行访问- 访问监视：从 Developer tool 进行访问- 访问监视：从 Administrator 工具进行访问- 对作业执行操作 <p>注意: 在使用 Kerberos 身份验证的域中，用户还必须具有配置为用于监视的模型存储库服务的管理员角色。</p>

特权组	特权名称
计划程序	计划程序特权组包括以下特权： - 管理计划作业：创建计划 - 管理计划作业：删除计划 - 管理计划作业：编辑计划 - 管理计划作业：查看计划
工具	访问 Informatica Administrator

PowerCenter 存储库服务自定义角色

PowerCenter 存储库服务自定义角色包括 PowerCenter 连接管理员、PowerCenter 开发人员、PowerCenter 操作员和 PowerCenter 存储库文件夹管理员。

PowerCenter 连接管理员

下表列出了向 PowerCenter 连接管理员自定义角色分配的默认特权：

特权组	特权名称
工具	访问 Workflow Manager
全局对象	创建连接

PowerCenter 开发人员

下表列出了向 PowerCenter Developer 自定义角色分配的默认特权：

特权组	特权名称
工具	- 访问 Designer - 访问 Workflow Manager - 访问 Workflow Monitor
设计对象	- 创建、编辑和删除 - 管理版本
源和目标	- 创建、编辑和删除 - 管理版本
运行时对象	- 创建、编辑和删除 - 执行 - 管理版本 - 监视

PowerCenter 操作员

下表列出了向 PowerCenter 操作员自定义角色分配的默认特权：

特权组	特权名称
工具	访问 Workflow Monitor
运行时对象	<ul style="list-style-type: none">- 执行- 管理执行- 监视

PowerCenter 存储库文件夹管理员

下表列出了向 PowerCenter 存储库文件夹管理员自定义角色分配的默认特权：

特权组	特权名称
工具	访问 Repository Manager
文件夹	<ul style="list-style-type: none">- 复制- 创建- 管理版本
全局对象	<ul style="list-style-type: none">- 管理部署组- 执行部署组- 创建标签- 创建查询

Test Data Manager 自定义角色

Test Data Manager 自定义角色包括测试数据管理员、测试数据开发人员、测试数据项目 DBA、测试数据项目开发人员、测试数据项目所有者、测试数据风险经理、测试数据专家和测试工程师。

测试数据管理员

下表列出了分配给“测试数据管理员”自定义角色的默认特权：

特权组	特权名称
项目	审计项目
管理	<ul style="list-style-type: none">- 查看连接- 管理连接- 管理首选项

测试数据开发人员

下表列出了分配给“测试数据开发人员”自定义角色的默认特权：

特权组	特权名称
策略	<ul style="list-style-type: none">- 查看策略- 管理策略
数据域	<ul style="list-style-type: none">- 查看数据域- 管理数据域
规则	<ul style="list-style-type: none">- 查看屏蔽规则- 管理屏蔽规则- 查看生成规则- 管理生成规则
规则	<ul style="list-style-type: none">- 查看屏蔽规则- 管理屏蔽规则
项目	审计项目

测试数据项目 DBA

下表列出了分配给“测试数据项目 DBA”自定义角色的默认特权：

特权组	特权名称
项目	<ul style="list-style-type: none">- 查看项目- 执行项目- 监视项目- 审计项目
管理	<ul style="list-style-type: none">- 查看连接- 管理连接
数据集	<ul style="list-style-type: none">- 查看数据集- 查看数据集中的数据。

测试数据项目开发人员

下表列出了分配给“测试数据项目开发人员”自定义角色的默认特权：

特权组	特权名称
策略	查看策略
规则	<ul style="list-style-type: none">- 查看屏蔽规则- 查看生成规则- 管理生成规则
规则	<ul style="list-style-type: none">- 查看屏蔽规则
数据域	查看数据域

特权组	特权名称
项目	<ul style="list-style-type: none"> - 查看项目 - 发现项目 - 执行项目 - 监视项目 - 审计项目 - 导入元数据
数据屏蔽	<ul style="list-style-type: none"> - 查看数据屏蔽 - 管理数据屏蔽
数据子集	<ul style="list-style-type: none"> - 查看数据子集 - 管理数据子集
数据生成	<ul style="list-style-type: none"> - 查看数据生成 - 管理数据生成
管理	<ul style="list-style-type: none"> - 查看连接 - 管理连接
数据集	<ul style="list-style-type: none"> - 查看数据集 - 查看数据集中的数据

测试数据项目所有者

下表列出了分配给“测试数据项目所有者”自定义角色的默认特权：

特权组	特权名称
策略	查看策略
规则	<ul style="list-style-type: none"> - 查看屏蔽规则 - 查看生成规则 - 管理生成规则
规则	<ul style="list-style-type: none"> - 查看屏蔽规则
数据域	查看数据域
项目	<ul style="list-style-type: none"> - 查看项目 - 管理项目 - 发现项目 - 执行项目 - 监视项目 - 审计项目 - 导入元数据
数据屏蔽	<ul style="list-style-type: none"> - 查看数据屏蔽 - 管理数据屏蔽
数据子集	<ul style="list-style-type: none"> - 查看数据子集 - 管理数据子集
数据生成	<ul style="list-style-type: none"> - 查看数据生成 - 管理数据生成

特权组	特权名称
管理	<ul style="list-style-type: none"> - 查看连接 - 管理连接
数据集	<ul style="list-style-type: none"> - 查看数据集 - 查看数据集中的数据 - 管理数据集 - 管理数据集中的数据 - 重置数据集

测试数据风险经理

下表列出了分配给“测试数据风险经理”自定义角色的默认特权：

特权组	特权名称
策略	查看策略
规则	<ul style="list-style-type: none"> - 查看屏蔽规则 - 查看生成规则
规则	<ul style="list-style-type: none"> - 查看屏蔽规则
数据域	查看数据域
项目	审计项目

测试数据专家

下表列出了分配给“测试数据专家”自定义角色的默认特权：

特权组	特权名称
策略	查看策略
规则	<ul style="list-style-type: none"> - 查看屏蔽规则 - 管理屏蔽规则 - 查看生成规则 - 管理生成规则
规则	<ul style="list-style-type: none"> - 查看屏蔽规则 - 管理屏蔽规则
数据域	<ul style="list-style-type: none"> - 查看数据域 - 管理数据域
项目	<ul style="list-style-type: none"> - 查看项目 - 管理项目 - 发现项目 - 执行项目 - 监视项目 - 审计项目 - 导入元数据

特权组	特权名称
数据屏蔽	<ul style="list-style-type: none"> - 查看数据屏蔽 - 管理数据屏蔽
数据子集	<ul style="list-style-type: none"> - 查看数据子集 - 管理数据子集
数据生成	<ul style="list-style-type: none"> - 查看数据生成 - 管理数据生成
管理	<ul style="list-style-type: none"> - 查看连接 - 管理连接
数据集	<ul style="list-style-type: none"> - 查看数据集 - 查看数据集中的数据 - 管理数据集 - 管理数据集中的数据 - 重置数据集

测试工程师

下表列出了分配给“测试工程师”自定义角色的默认特权：

特权组	特权名称
项目	<ul style="list-style-type: none"> - 查看项目 - 监视项目
数据集	<ul style="list-style-type: none"> - 查看数据集 - 管理数据集 - 重置数据集 - 查看数据集中的数据 - 管理数据集中的数据

索引

A

- 安全
 - 角色 [119](#)
 - 权限 [95](#)
 - 特权 [95](#), [118](#), [120](#)
 - 密码 [100](#)
- 安全管理特权组
 - 说明 [120](#)
- 安全特权组
 - 说明 [131](#)
- 安全域
 - 本地 [17](#)
 - LDAP [17](#)
 - 客户端配置 [70](#)
 - 删除 LDAP [26](#)
- as
 - 权限（按命令） [187](#)
 - 特权（按命令） [187](#)
- 安全断言标记语言 (SAML)
 - 支持 [55](#)
- 安全页
 - Informatica Administrator [91](#)
 - 导航器 [92](#)

B

- 本地安全域
 - 说明 [17](#)
- 本地身份验证
 - 说明 [17](#), [90](#)
- 本地用户
 - 编辑 [101](#)
 - 分配给组 [101](#)
 - 管理 [100](#)
 - 启用 [102](#)
 - 删除 [102](#)
 - 密码 [100](#)
 - 添加 [100](#)
- 本地组
 - 编辑 [108](#)
 - 管理 [107](#)
 - 删除 [109](#)
 - 添加 [108](#)
 - 移至其他组 [109](#)
 - 用户, 分配 [101](#)
- 编辑引用表元数据
 - 特权 [128](#)
- 标签
 - PowerCenter 特权 [143](#)
- 部署组
 - PowerCenter 特权 [143](#)
- 标识提供程序
 - 配置单点登录 [57](#)

C

- cacerts 信任库文件 [25](#)
- 创建引用表
 - 特权 [128](#)
- convertUserActivityLog
 - 用户活动日志 [104](#)
- 操作系统配置文件
 - 编辑 [109](#)
 - 管理 [109](#)
 - 默认值 [114](#)
 - 权限 [166](#), [169](#)
 - 删除 [115](#)
 - 属性, PowerCenter 集成服务 [109](#)
 - 属性, 数据集成服务 [109](#), [111](#)
 - 创建 [113](#)
 - 概览 [93](#)
 - 属性, 元数据访问服务 [112](#)

D

- 登录活动
 - 查看 [104](#)
- dis
 - 权限（按命令） [189](#)
 - 特权（按命令） [189](#)
- 对象查询
 - PowerCenter 特权 [143](#)
- 单点登录
 - 说明 [90](#)
 - 概览 [55](#)
 - 配置 [56](#)
- 导航器
 - 安全页 [92](#)

E

- es
 - 权限（按命令） [190](#)
 - 特权（按命令） [190](#)

F

- 分析服务
 - 特权 [127](#)
 - 自定义角色 [214](#)
- 服务管理器
 - 单点登录 [90](#)
 - 身份验证 [90](#)
 - 授权 [90](#)
- 父组
 - 说明 [108](#)

G

- getUserActivityLog
 - 筛选器 [105](#)
 - 用户活动日志 [104](#)
- 工具特权组
 - PowerCenter 存储库服务 [134](#)
 - 域 [126](#)
- 工作流
 - 继承权限 [173](#)
 - 权限 [173](#)
- 更改
 - 用户帐户的密码 [95](#)
- 管理员
 - 域 [99](#)
 - 角色 [157](#)
 - 默认 [99](#)
 - 应用程序客户端 [99](#)

H

- 环境变量
 - INFA_TRUSTSTORE [70](#)
 - INFA_TRUSTSTORE_PASSWORD [70](#)

I

- Informatica Administrator
 - 搜索 [91](#)
 - 安全页 [91](#)
 - 导航器 [92](#)
 - 概览 [88](#)
 - 选项卡, 查看 [88](#)
- Informatica Analyst
 - 管理员 [99](#)
- Informatica Developer
 - 管理员 [99](#)
- Informatica 域
 - 权限 [95](#)
 - 特权 [95](#)
 - 用户, 管理 [100](#)
 - 用户安全 [95](#)
- ipc
 - 权限 (按命令) [191](#)
 - 特权 (按命令) [191](#)
- isp
 - 权限 (按命令) [191](#)
 - 特权 (按命令) [191](#)

J

- 加载特权组
 - 说明 [131](#)
- 继承权限
 - 说明 [165](#)
- 继承特权
 - 说明 [160](#)
- 节点
 - 权限 [166](#)
- 计划程序服务
 - 特权 [147](#)
- 监视特权组
 - 域 [125](#)
- 角色
 - 说明 [119](#)

- 角色 (续)
 - 分配 [160](#)
 - 概览 [93](#)
 - 故障排除 [161](#)
 - 管理 [156](#)
 - 管理员 [157](#)
 - 自定义 [158](#)

K

- Kerberos 身份验证
 - 服务主体名称 [34](#)
 - keytab [34](#)
 - LDAP 同步 [51](#)
 - SPN keytab 格式文件 [38](#)
 - 服务主体帐户 [33](#)
 - 概览 [27, 28](#)
 - 节点级别 [30](#)
 - 进程级别 [30](#)
 - 跨域身份验证 [29](#)
 - 说明 [17](#)
- keytool 实用程序 [25](#)
- 客户端配置
 - 安全域 [70](#)

L

- LDAP 目录服务
 - 嵌套组 [25](#)
- LDAP 安全域
 - 说明 [17](#)
- LDAP 配置
 - 删除 [26](#)
- LDAP 身份验证
 - Azure Active Directory [21](#)
 - 嵌套组 [25](#)
 - 说明 [17, 90](#)
 - 目录服务 [22](#)
 - 设置 [22](#)
 - 受支持的目录服务 [20](#)
 - 自签名 SSL 证书 [25](#)
- LDAP 用户
 - 管理 [100](#)
 - 启用 [102](#)
 - 导入 [22](#)
 - 分配给组 [102](#)
- LDAP 组
 - 管理 [107](#)
 - 导入 [22](#)
- 连接
 - 默认权限 [171](#)
 - 权限 [170](#)
 - 权限类型 [171](#)
- 连接对象
 - PowerCenter 特权 [143](#)
- 列级别安全
 - 限制列 [177](#)
- 浏览特权组
 - 说明 [129](#)

M

- mas
 - 权限 (按命令) [199](#)
 - 特权 (按命令) [199](#)

Metadata Manager
 管理员 [99](#)
Metadata Manager 服务
 特权 [129](#)
 自定义角色 [215](#)
 具有特权的用户 [161](#)
 授权 [90](#)
 用户同步 [90](#)
Metadata Manager 服务特权
 安全特权组 [131](#)
 加载特权组 [131](#)
 模型特权组 [131](#)
 浏览特权组 [129](#)
命令行程序
 特权 [187](#)
模型特权组
 说明 [131](#)
mrs
 权限 (按命令) [199](#)
 特权 (按命令) [199](#)
ms
 权限 (按命令) [201](#)
 特权 (按命令) [201](#)
目标
 特权 [138](#)
密码
 本地用户 [100](#)
 为默认管理员进行更改 [99](#)
 为用户帐户进行更改 [95](#)
 要求 [100](#)
密码套件
 配置 [78](#)
模型存储库服务
 特权 [132](#)
 具有特权的用户 [161](#)
 授权 [90](#)
 用户同步 [90](#)
默认管理员
 密码, 更改 [99](#)
 说明 [99](#)
 修改 [99](#)

N

内容管理服务
 特权 [128](#)

P

pmcmd
 权限 (按命令) [206](#)
 特权 (按命令) [206](#)
pmrep
 权限 (按命令) [209](#)
 特权 (按命令) [209](#)
PowerCenter 安全
 管理 [91](#)
PowerCenter 存储库服务
 特权 [133](#)
 自定义角色 [217](#)
 管理员角色 [157](#)
 具有特权的用户 [161](#)
 授权 [90](#)
 用户同步 [90](#)
PowerCenter 客户端
 管理员 [99](#)

PowerExchange 日志记录器服务
 特权 [146](#)
PowerExchange 侦听器服务
 特权 [145](#)
ps
 权限 (按命令) [202](#)
 特权 (按命令) [202](#)
pwx
 权限 (按命令) [203](#)
 特权 (按命令) [203](#)

Q

嵌套组
 LDAP 目录服务 [25](#)
 LDAP 身份验证 [25](#)
全局对象
 PowerCenter 特权 [143](#)
全局对象特权组
 说明 [143](#)
群集
 权限 (按命令) [188](#)
 特权 (按命令) [188](#)
权限
 连接 [170](#)
 as 命令 [187](#)
 操作系统配置文件 [166](#), [169](#)
 dis 命令 [189](#)
 es 命令 [190](#)
 工作流 [173](#)
 ipc 命令 [191](#)
 isp 命令 [191](#)
 继承 [165](#)
 节点 [166](#)
 类型 [165](#)
 mas 命令 [199](#)
 mrs 命令 [199](#)
 ms 命令 [201](#)
 pmcmd 命令 [206](#)
 pmrep 命令 [209](#)
 ps 命令 [202](#)
 pwx 命令 [203](#)
 群集命令 [188](#)
 rms 命令 [204](#)
 rtm 命令 [204](#)
 sch 命令 [205](#)
 搜索筛选器 [166](#)
 sql 命令 [205](#)
 SQL 数据服务 [174](#)
 tools 命令 [202](#)
 网格 [166](#)
 Web 服务 [178](#)
 Web 服务操作 [178](#)
 文件夹 [166](#)
 wfs 命令 [206](#)
 许可证 [166](#)
 虚拟表 [174](#)
 虚拟存储过程 [174](#)
 虚拟架构 [174](#)
 映射 [173](#)
 应用程序 [173](#)
 应用程序服务 [166](#)
 有效 [165](#)
 域对象 [166](#)
 直接 [165](#)
 使用特权 [164](#)
 说明 [164](#)

R

“任何人”组
说明 [98](#)

rms

权限 (按命令) [204](#)
特权 (按命令) [204](#)

rtm

权限 (按命令) [204](#)
特权 (按命令) [204](#)

S

sch

权限 (按命令) [205](#)
特权 (按命令) [205](#)

筛选器

getUserActivityLog [105](#)

设计对象

说明 [136](#)
特权 [136](#)

设计对象特权组

说明 [136](#)

身份验证

本地 [17](#), [90](#)
服务管理器 [90](#)
Kerberos [17](#)
LDAP [17](#), [22](#), [90](#)

审计报表

用户 [184](#)

搜索部分

Informatica Administrator [91](#)

搜索筛选器

权限 [166](#)

sql

权限 (按命令) [205](#)
特权 (按命令) [205](#)

SQL 数据服务

继承权限 [174](#)
权限 [174](#)
权限类型 [175](#)

SSL 证书

LDAP 身份验证 [25](#)

审计报告

说明 [181](#)
用户 [186](#)
组 [185](#)
概览 [94](#)

授权

Metadata Manager 服务 [90](#)
PowerCenter 存储库服务 [90](#)
服务管理器 [90](#)
模型存储库服务 [90](#)
数据集成服务 [90](#)
应用程序服务 [90](#)

数据集成服务

特权 [128](#)
授权 [90](#)

T

Test Data Manager

管理员 [99](#)

tools

权限 (按命令) [202](#)
特权 (按命令) [202](#)

特权

安全管理 [120](#)
as 命令 [187](#)
dis 命令 [189](#)
es 命令 [190](#)
分析服务 [127](#)
Informatica Cloud 管理 [127](#)
ipc 命令 [191](#)
isp 命令 [191](#)
继承 [160](#)
计划程序服务 [147](#)
mas 命令 [199](#)
Metadata Manager 服务 [129](#)
命令行程序 [187](#)
模型存储库服务 [132](#)
mrs 命令 [199](#)
ms 命令 [201](#)
目标 [138](#)
内容管理服务 [128](#)
pmcmd 命令 [206](#)
pmrep 命令 [209](#)
PowerCenter 存储库服务 [133](#)
PowerCenter 存储库服务工具 [134](#)
PowerCenter 全局对象 [143](#)
PowerExchange 日志记录器服务 [146](#)
PowerExchange 侦听器服务 [145](#)
ps 命令 [202](#)
pwx 命令 [203](#)
群集命令 [188](#)
rms 命令 [204](#)
rtm 命令 [204](#)
sch 命令 [205](#)
设计对象 [136](#)
数据集成服务 [128](#)
sql 命令 [205](#)
tools 命令 [202](#)
文件夹 [134](#)
wfs 命令 [206](#)
域 [120](#)
源 [138](#)
域工具 [126](#)
域管理 [121](#)
运行时对象 [139](#)
分配 [160](#)
故障排除 [161](#)
监视 [125](#)
使用权限 [164](#)
说明 [118](#)

特权组

安全 [131](#)
安全管理 [120](#)
工具 [126](#), [134](#)
Informatica Cloud 管理 [127](#)
加载 [131](#)
模型 [131](#)
全局对象 [143](#)
设计对象 [136](#)
文件夹 [134](#)
源和目标 [138](#)
域管理 [121](#)
运行时对象 [139](#)
监视 [125](#)
浏览 [129](#)
说明 [119](#)

同步

LDAP 用户 [22](#)
用户 [90](#)

U

UpdateColumnOptions
替换列值 [177](#)

W

网格
权限 [166](#)
Web 服务
权限 [178](#)
权限类型 [178](#)
Web 服务操作
权限 [178](#)
Web 服务资源
权限 [178](#)
文件夹
权限 [166](#)
特权 [134](#)
文件夹特权组
说明 [134](#)
wfs
权限（按命令） [206](#)
特权（按命令） [206](#)

X

许可证
权限 [166](#)
虚拟表
继承权限 [174](#)
权限 [174](#)
虚拟存储过程
继承权限 [174](#)
权限 [174](#)
虚拟架构
继承权限 [174](#)
权限 [174](#)
系统定义的角色
分配给用户和组 [160](#)
管理员 [157](#)
说明 [156](#)
系统内存
增加 [103](#)

Y

映射
继承权限 [173](#)
权限 [173](#)
应用程序
权限 [173](#)
用户活动日志
convertUserActivityLog [104](#)
getUserActivityLog [104](#)
活动代码 [105](#)
输出格式 [104](#)
有效权限
说明 [165](#)
源
特权 [138](#)
源和目标特权组
说明 [138](#)
域对象
权限 [166](#)

域管理特权组
说明 [121](#)
域管理员
说明 [99](#)
云管理特权组
域 [127](#)
运算符
自定义角色 [216](#)
运行时对象
说明 [139](#)
特权 [139](#)
运行时对象特权组
说明 [139](#)
域权限
继承 [165](#)
有效 [165](#)
直接 [165](#)
应用程序服务
权限 [166](#)
授权 [90](#)
用户同步 [90](#)
用户
分配给组 [101](#)
管理 [100](#)
大量 [103](#)
概览 [92](#)
角色, 分配 [160](#)
特权, 分配 [160](#)
同步 [90](#)
无效字符 [100](#)
系统内存 [103](#)
有效名称 [100](#)
用户安全
说明 [89](#)
用户说明
无效字符 [100](#)
用户帐户
启用 [102](#)
概览 [98](#)
更改密码 [95](#)
默认 [99](#)
在安装期间创建 [99](#)
有效名称
组 [108](#)
用户帐户 [100](#)
域
安全管理特权 [120](#)
管理特权 [121](#)
管理员 [99](#)
特权 [120](#)
用户安全 [95](#)
管理员角色 [157](#)
具有特权的用户 [161](#)
用户同步 [90](#)

Z

直接权限
说明 [165](#)
组说明
无效字符 [108](#)
帐户
更改密码 [95](#)
帐户管理
概览 [94](#)
自定义角色
编辑 [159](#)

自定义角色 (续)

操作员 [216](#)

创建 [159](#)

Metadata Manager 服务 [215](#)

PowerCenter 存储库服务 [217](#)

删除 [160](#)

特权, 分配 [159](#)

分配给用户和组 [160](#)

分析服务 [214](#)

说明 [156](#), [158](#)

组

父组 [108](#)

组 (续)

管理 [107](#)

默认的任何人 [98](#)

无效字符 [108](#)

有效名称 [108](#)

概览 [92](#)

角色, 分配 [160](#)

特权, 分配 [160](#)

同步 [90](#)