Sun Identity Manager 8.1 业务管理员指南

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

文件号码 821–0065
2009 年 2 月

090729@22510

目录

前言

本指南介绍如何使用 Sun™Identity Manager (Identity Manager) 软件提供对企业信息系统和应用程序的安全用户访问。它提供了一些操作过程和方案，可以帮助您利用 Identity Manager 系统执行经常性和周期性管理任务。

目标读者

本 *Sun Identity Manager 8.1* **业务管理员指南**适用于通过 Identity Manager 服务器和软件实现集成的身份管理和 Web 访问平台的管理员、软件开发者以及 IT 服务提供者。

了解以下技术可帮助您应用本书中阐述的信息：

- 轻量目录访问协议 (Lightweight Directory Access Protocol, LDAP)
- Java 技术
- JavaServer Pages™ (JSP™) 技术
- 超文本传输协议 (Hypertext Transfer Protocol, HTTP)
- 超文本标记语言 (Hypertext Markup Language, HTML)
- 可扩展标记语言 (Extensible Markup Language, XML)

阅读本书之前

Identity Manager 是 Sun Java Enterprise System 的一个组件，后者是支持分布在网络或 Internet 环境中的企业应用程序的软件基础结构。 您应该熟悉 Sun Java Enterprise System 附带的文档，可以从 `http://docs.sun.com/coll/entsys_04q4` 联机访问该文档。

由于 Identity Manager Directory Server 用作 Identity Manager 部署中的数据存储库，因此您应熟悉该产品附带的文档。可以从 `http://docs.sun.com/coll/DirectoryServer_04q2` 联机访问 Directory Server 文档。

本书的结构

本指南由以下各章及附录组成。

第 1 章，Identity Manager 概述介绍 Identity Manager 和各个 Identity Manager 对象如何帮助您应对动态工作环境下的管理难题。

第 2 章，Identity Manager 用户界面入门介绍如何使用 Identity Manager 的图形用户界面。

第 3 章，用户和帐户管理介绍如何使用管理员界面创建和管理用户。

第 5 章，角色和资源包含用于帮助您了解 Identity Manager 角色和资源的信息。

第 4 章，配置业务管理对象包含用于帮助您设置和维护 Identity Manager 业务管理对象（如策略、电子邮件模板、审计组和审计事件等）的信息和过程。

第 6 章，管理介绍如何使用管理员界面执行各种管理员级别的任务。 此外，本章还包含有关使用角色、管理角色和权能的信息。

第 7 章，数据加载和同步介绍如何使用 Identity Manager 的数据加载和同步功能保持数据的最新状态。

第 8 章，报告介绍 Identity Manager 报告类型，并说明如何创建和管理报告。

第 9 章，任务模板介绍 Identity Manager 任务模板，以及如何使用这些模板配置工作流行为。

第 10 章，审计日志记录介绍 Identity Manager 的审计系统。

第 11 章，PasswordSync介绍如何安装、配置和使用 PasswordSync 功能检测和同步密码更改。

第 12 章，安全介绍如何使用 Identity Manager 管理系统安全。

第 13 章，身份审计：基本概念 介绍身份审计概念以及审计控制。

第 14 章，审计：审计策略介绍如何使用审计策略向导创建和管理审计策略。

第 15 章，审计：监视遵循性介绍如何执行审计查看以及管理对联邦委托法规的遵循性。

第 16 章，数据导出器介绍数据导出器功能，并说明如何使用此功能将有关用户、角色和其他对象类型的数据写入到外部数据仓库中。

第 17 章，服务提供者管理介绍如何配置和管理服务提供者功能。

附录 A，lh 参考消息介绍如何使用 Identity Manager 命令行界面。

附录 B，审计日志数据库模式包含有关支持的数据库类型的审计数据模式值和审计日志映射的信息。

附录 C，用户界面快速参考提供了一个快速参考，指示如何完成 Identity Manager 中经常执行的任务。

附录 D，权能定义提供了一个快速参考，说明可以分配给用户的基于任务的权能和功能性权能。

相关书籍

Sun 提供了其他文档和信息以帮助您安装、使用和配置 Identity Manager。Sun Identity Manager 8.1 库中包括以下发行文档：

主要读者	标题	描述
所有读者	《Sun Identity Manager 概述》	简要介绍 Identity Manager 功能。提供产品体系结构信息，并说明 Identity Manager 如何与其他 Sun 产品（如 Sun Open SSO Enterprise 和 Role Manager）集成在一起。
	《Sun Identity Manager 8.1 发行说明》	介绍在 Identity Manager 文档集中尚未提供的已知问题、已修复问题以及最新发布信息。
系统管理员	《Sun Identity Manager 8.1 Installation》	介绍如何安装 Identity Manager 以及可选组件，如 Sun Identity Manager Gateway 和 PasswordSync。
	《Sun Identity Manager 8.1 Upgrade》	提供有关如何从旧版 Identity Manager 升级到较新版本的说明。
	《Sun Identity Manager 8.1 System Administrator's Guide》	包含用于帮助系统管理员管理、微调其 Identity Manager 安装并排除该安装故障的信息及说明。
业务管理员	《Sun Identity Manager 8.1 业务管理员指南》	介绍如何使用 Identity Manager 的置备和审计功能。

主要读者	标题	描述
系统集成人员	《Sun Identity Manager Deployment Guide》	介绍如何在复杂的 IT 环境中部署 Identity Manager。 涉及到的主题包括：使用身份属性、数据加载和同步、配置用户操作、应用自定义品牌信息等。
	《Sun Identity Manager Deployment Reference》	包含有关工作流、表单、视图、规则以及 XPRESS 语言的信息。
	《Sun Identity Manager 8.1 Resources Reference》	提供有关安装、配置和使用资源适配器的信息。
	《Sun Identity Manager Service Provider 8.1 Deployment》	介绍如何部署 Sun Identity Manager Service Provider，以及视图、表单和资源与标准 Identity Manager 产品有何不同。
	《Sun Identity Manager 8.1 Web Services》	介绍如何配置 SPML 支持，支持的 SPML 功能（及原因），以及如何在字段中扩展支持。

此外，您可以从 `http://docs.sun.com` Web 站点联机访问 Sun 技术文档。

文档更新

有关本 Identity Manager 发行文档以及其他 Identity Manager 发行文档的修正及更新将发布到 Identity Manager 文档更新 Web 站点：

`http://blogs.sun.com/idmdocupdates/`

可以使用 RSS 订阅源读取器定期检查该网站，并在发布更新后通知您。要进行订阅，请下载订阅源读取器，并单击页面右侧“订阅源”下面的链接。从 8.0 版开始，将为每个主要发行版提供单独的订阅源。

相关的第三方 Web 站点引用

本文档引用了第三方 URL 以提供其他相关信息。

注 – Sun 对本文档中提到的第三方 Web 站点的可用性不承担任何责任。对于此类站点或资源中的（或通过它们获得的）任何内容、广告、产品或其他资料，Sun 并不表示认可，也不承担任何责任。对于因使用或依靠此类站点或资源中的（或通过它们获得的）任何内容、产品或服务而造成的、名义上造成的或连带产生的实际或名义损坏或损失，Sun 概不负责，也不承担任何责任。

文档、支持和培训

Sun Web 站点提供了有关以下附加资源的信息：

- 文档 (http://www.sun.com/documentation/)
- 支持 (http://www.sun.com/support/)
- 培训 (http://www.sun.com/training/)

Sun 欢迎您提出意见

Sun 致力于提高其文档的质量，并十分乐意收到您的意见和建议。要共享您的意见，请转至 http://docs.sun.com 并单击 "Feedback"（反馈）。

印刷约定

下表介绍了本文档中使用的印刷约定。

表 P–1 印刷约定

字样	含义	示例
AaBbCc123	命令、文件和目录的名称，以及计算机屏幕输出	编辑 .login 文件。 使用 ls -a 列出所有文件。 machine_name% you have mail.
AaBbCc123	您键入的内容，与计算机屏幕输出的显示不同	machine_name% **su** Password:
aabbcc123	占位符：将用实际名称或值替换	用于删除文件的命令为 rm *filename*。
AaBbCc123	书名、新术语和要强调的术语	请阅读用户指南中的第 6 章。 **高速缓存**是指在本地存储的副本。 请**勿**保存文件。 **注意**：某些强调项在联机查看时显示为粗体。

命令中的 Shell 提示符示例

下表显示了 C shell、Bourne shell 和 Korn shell 的默认 UNIX® 系统提示符和超级用户提示符。

表 P–2 Shell 提示符

Shell	提示符
C shell	`machine_name%`
用于超级用户的 C shell	`machine_name#`
Bourne shell 和 Korn shell	`$`
用于超级用户的 Bourne shell 和 Korn shell	`#`

◆ ◆ ◆ 第 1 章

1 Identity Manager 概述

Sun Identity Manager 系统使您可以管理和审计对帐户和资源的访问。通过为您提供快速处理周期性和日常用户置备及审计任务的权能和工具，Identity Manager 有助于为内部和外部客户提供优越的服务。

本章包含以下主题：

简介

当今的企业需要其 IT 服务不断提高灵活性和能力。以前，管理对业务信息和系统的访问需要直接与有限数量的帐户进行交互。现在，管理访问则日渐意味着不仅要处理数量不断增加的内部客户，还要处理企业外部的合作伙伴和客户。

访问需求的增加可产生庞大的管理开销。作为管理员，您必须安全有效地使人们（企业内部或外部人员）能够顺利工作。同时，在提供初始访问后，您还面临连续、复杂的问题，诸如忘记密码与更改角色以及业务关系等。

此外，当今的企业面临对关键业务信息的安全性和完整性进行控制的严格要求。在受与遵循性相关的法案（例如，Sarbanes-Oxley (SOX) Act（沙宾法案）、Health Insurance Portability and Accountability Act（HIPAA，健康保险流通与责任法案）和 Gramm-Leach-Bliley (GLB) Act（金融服务现代化法案））所控制的环境中，由监控和报告活动而产生的开销非常重要并且昂贵。您必须能够对访问控制的更改做出快速反应，还必须满足有助于保证业务安全的数据收集和报告的要求。

Identity Manager 专用于帮助您应对动态环境下的这些管理难题。通过使用 Identity Manager 来分散访问管理开销和处理遵循性负担，更易于解决您面临的主要复杂问题：如何定义访问？定义访问之后，如何维护灵活性和进行控制？

一种安全而灵活的设计允许您设置 Identity Manager 以适应您企业的结构并应对这些复杂问题。将 Identity Manager 对象映射到您管理的实体（用户和资源），可显著提高运行效率。

在服务提供者环境中，Identity Manager 还将这些权能扩展到管理外联网用户。

Identity Manager 系统的目标

Identity Manager 解决方案使您可以达到以下目标：

- 管理帐户对大量不同系统和资源的访问。
- 安全地管理每个用户的一组帐户的动态帐户信息。
- 设置委托权限以创建和管理用户帐户数据。
- 处理大量企业资源以及日益增加的大量外联网客户及合作伙伴。
- 安全地授权用户访问企业信息系统。利用 Identity Manager，您能具备授予、管理和撤销对内部和外部组织的访问权限的完全集成功能。
- 通过**不**保留数据来保持数据同步。Identity Manager 解决方案支持上级系统管理工具应当遵守的两条关键原则：
  - 产品应对其管理的系统产生最小的影响。
  - 产品不会因增加了其他要管理的资源而使企业管理更复杂。

  定义审计策略以使用用户访问权限管理遵循性以及通过自动修正操作和电子邮件警报管理违规。
- 执行周期性访问查看，并定义使验证用户权限的过程自动化的证明查看和批准过程。
- 通过面板监视关键信息并审计和查看统计信息。

定义用户访问资源的权限

更广泛意义的企业**用户**可以是与公司存在某种关系的任何人，包括雇员、客户、合作伙伴、供应商或采购人员。在 Identity Manager 系统中，用户以**用户帐户**表示。

根据他们与您的业务和其他实体的关系，用户需要访问不同的目标，诸如计算机系统、数据库中存储的数据或特定计算机应用程序。用 Identity Manager 的术语描述，这些目标称为**资源**。

因为用户针对其访问的每个资源通常具有一个或多个身份，所以 Identity Manager 会创建单个**虚拟身份**，此身份映射到各个不同的资源。这允许您将用户作为单个实体进行管理。请参见图 1–1。

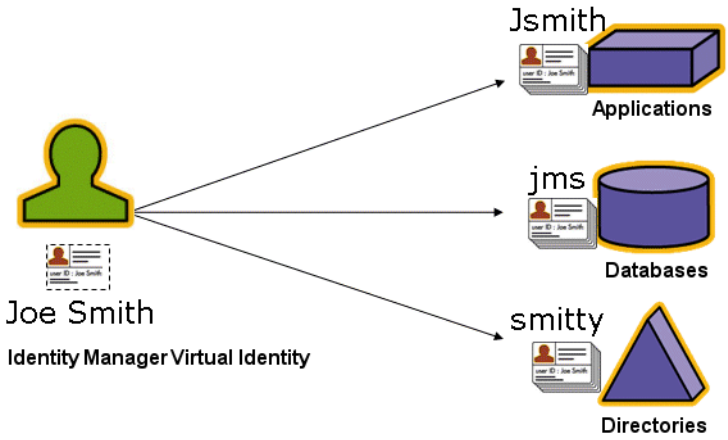


图 1–1 Identity Manager 用户帐户资源关系

为有效管理大量用户，您需要用逻辑方法将他们分组。在多数公司中，用户被分组到按职能或地理位置划分的各部门。这些部门中的每个部门通常都需要访问不同的资源。用 Identity Manager 的术语描述，此类型的组称为**组织**。

另一种对用户分组的方法是按照类似特征，如公司关系或工作职责。Identity Manager 将这些组称为**角色**。

在 Identity Manager 系统中，您可为用户帐户分配角色，以便有效地启用和禁用对资源的访问。为组织分配帐户可实现管理职责的有效委托。

Identity Manager 用户的直接或间接管理也可通过应用**策略**实现，这些策略设置了规则和密码及用户验证选项。

了解用户类型

Identity Manager 提供两种用户类型：*Identity Manager* **用户**和**服务提供者用户**（如果针对服务提供者实现配置了 Identity Manager 系统）。这两种类型允许您根据用户与公司的关系，来区分可能具有不同置备要求的用户，例如外联网用户与内联网用户。

服务提供者实现的一个典型方案是同时具有内部用户和外部用户（客户）的服务提供者公司，这些用户要使用 Identity Manager 进行管理。有关配置服务提供者实现的信息，请参见《Sun Identity Manager Service Provider 8.1 Deployment》。

可以在配置用户帐户时指定 Identity Manager 用户类型。有关服务提供者用户的详细信息，请参见第 17 章，服务提供者管理。

委托管理

要成功分布用户身份管理的职责，您需要在灵活性和控制之间寻求合适的平衡点。通过授予选择 Identity Manager 用户管理员权限并委托管理任务，您就能够将身份管理职责分配给最了解用户需求的那些人（如招聘部门的经理），从而可以减少开销并提高效率。具有此类扩展权限的用户称为 Identity Manager **管理员**。

但是，委托仅能够在安全模式下发挥作用。为维持适当的控制级别，Identity Manager 允许您为管理员分配不同级别的**权能**。权能会批准系统内各种级别的访问和操作。

Identity Manager 工作流模型还包括用来确保某些操作需要批准的方法。Identity Manager 管理员可以使用工作流保持对任务的控制并跟踪任务的进度。有关工作流的详细信息，请参见《Sun Identity Manager Deployment Reference》中的第 1 章 “Workflow”。

Identity Manager 对象

清楚地了解 Identity Manager 对象及它们交互的方式对成功管理和部署系统极为重要。这些对象包括：

注 – 在命名 Identity Manager 对象时，不要使用以下字符：

’（撇号）、.（句点）、|（管道符号）、[（左括号）、]（右括号）、,（逗号）、:（冒号）、$（美元符号）、"（双引号）、\（反斜杠）或 =（等号）。

还应该避免使用以下字符：_（下划线）、%（百分号）、^（插入符号）和 *（星号）。

Identity Manager 用户帐户

用户是指拥有 Identity Manager 系统帐户的任何人。Identity Manager 为每个用户存储一系列数据。这些信息共同构成每个用户的 Identity Manager 身份。

Identity Manager 用户帐户：

- 使用户能够访问一种或多种资源，并管理这些资源上的用户帐户数据。
- 作为分配的角色，以使用户能够访问多种资源。
- 是组织的一部分，组织决定了用户帐户由谁来管理及如何管理。

用户帐户设置过程是动态的过程。根据您在帐户设置期间选择的角色，您可以或多或少地提供一些特定于资源的信息，以创建帐户。与分配的角色相关的资源类型和数量决定了创建帐户所需的信息量。

管理员是指具有额外权限的用户，可通过这些权限管理用户帐户、资源和其他 Identity Manager 系统对象和任务。Identity Manager 管理员可以管理组织，并被分配了一定范围的权能，以应用于每个受管理组织中的对象。

有关用户帐户的详细信息，请参见第 3 章，用户和帐户管理。有关管理员帐户的详细信息，请参见第 6 章，管理。

Identity Manager 角色

角色是一个 Identity Manager 对象，通过该对象，可以将资源访问权限分组并有效地分配给用户。角色分为以下四种角色类型：

- 业务角色
- IT 角色
- 应用程序
- 资产

业务角色用于将组织中执行类似任务的人员工作时所需的访问权限划分到各个组中。通常，业务角色表示用户的工作职责。

IT **角色**、**应用程序**和**资产**将资源权利（或**访问权限**）划分到各个组中。要为用户提供资源访问权限，请将 IT 角色、应用程序和资产分配给业务角色，以使用户在工作时能够访问所需的资源。

IT 角色、应用程序和资产可以是**必需**、**条件**或**可选**角色。

- **必需角色**始终分配给用户。
- **条件角色**具有一定的条件，其计算值必须为 true 才能分配该角色。
- **可选角色**可以单独进行申请并会在经批准后分配给用户。

由于角色可以为条件或可选资源，因此，具有相同常规作业描述的用户可以具有相同的业务角色，但仍具有不同的访问权限。这种方法允许业务角色设计者定义粗粒度的角色访问，以使用户遵守相关的规定；同时仍为用户管理员提供了一定的灵活性，以微调用户的访问权限。通过采用这种方法，无需再为企业中的每种访问需求变化形式都定义新的业务角色（此问题称为**角色爆炸**）。

可以为用户分配一个或多个角色，也可以不分配角色。

注 – 有关角色的详细信息，请参见第 103 页中的 “了解和管理角色”。

资源和资源组

Identity Manager 存储了有关如何连接到资源或系统的信息。Identity Manager 可访问的资源包括：

- 数字资源，例如以下资源：
  - 主机安全管理器
  - 数据库
  - 目录服务（如 LDAP）
  - 应用程序
  - 操作系统
  - ERP 系统（如 SAP™）
- 非数字资源或 Identity Manager 的**外部**资源，例如以下资源：
  - 移动电话
  - 台式计算机
  - 便携式计算机
  - 安全徽章

每个 Identity Manager 资源都存储了以下类型的信息：

- 资源参数
- Identity Manager 参数
- 帐户信息（包括帐户属性和身份模板）

有两种方法可将资源分配给用户。可以将资源直接分配给用户（这称为单独或直接分配），也可以将资源分配给角色，然后再将角色分配给用户（这称为基于角色或间接分配）。

- **单独分配**。将各个资源直接分配给用户帐户。
- **基于角色的分配**。将一个或多个资源分配给角色（应用程序、资产或 IT 角色）。然后，将应用程序、资产或 IT 角色分配给业务角色。最后，将一个或多个业务角色分配给用户帐户。

相关的 Identity Manager 对象（即**资源组**），可用分配资源的方法将其分配给用户帐户。资源组与资源相关联，因此您可按特定顺序在各资源上创建帐户。同时，它们简化了将多个资源分配给用户帐户的过程。

有关资源组的详细信息，请参见第 145 页中的 “资源组”。

组织和虚拟组织

组织是 Identity Manager 容器，用于实现管理委托。它们定义 Identity Manager 管理员控制或管理的实体的范围。

组织也可表示指向基于目录的资源的直接链接。这些链接称为**虚拟组织**。虚拟组织允许直接管理资源数据而无需将信息载入 Identity Manager 信息库。利用虚拟组织镜像现有目录结构和成员资格，Identity Manager 去除了重复且费时的设置任务。

包含其他组织的组织称为**父组织**。可在平面结构中创建组织，也可在分层结构中排列组织。分层结构可代表您用来管理用户帐户的部门、地理区域或其他逻辑部门。

有关组织的详细信息，请参见第 178 页中的 “了解 Identity Manager 组织”。

目录连接

目录连接是与分层相关的一组组织，它镜像目录资源的实际层级容器集合。**目录资源**通过使用分层容器来使用分层名称空间。目录资源的示例包括 LDAP 服务器和 Windows Active Directory 资源。

目录连接中的每个组织都是**虚拟组织**。目录连接中的最顶层虚拟组织是代表资源中定义的基本上下文的容器的镜像。目录连接中的其余虚拟组织是顶层虚拟组织的**直接**或**间接**子组织，并且还镜像目录资源容器中的一个容器（已定义资源的基本环境容器的子容器）。

可以采用与组织一样的方法，使 Identity Manager 用户成为虚拟组织的成员，并且可用于虚拟组织。

有关目录连接的详细信息，请参见第 182 页中的 “了解目录连接和虚拟组织”。

Identity Manager 权能

可为每个用户分配权能或权限组，以使其能够通过 Identity Manager 执行管理操作。权能允许管理用户在系统内执行某些任务并对 Identity Manager 对象进行操作。

通常，您应根据特定工作职责（如密码重设或帐户批准）分配权能。通过为各个用户分配权能和权限，可创建一个分层管理结构，该结构在不危及数据保护安全的情况下提供具有针对性的访问和权限。

Identity Manager 提供一组用于常见管理功能的默认权能。满足您具体需求的权能也可被创建和分配。

有关权能的详细信息，请参见第 184 页中的 “了解和管理权能”。

管理员角色

Identity Manager 管理员角色使您能够为某个管理用户管理的每一个组织集合定义唯一的一组权能。管理员角色被分配了各种权能和受控组织，然后该角色可被分配给管理用户。

权能和受控组织可直接分配给管理员角色。这些权能和受控组织也可在管理用户每次登录到 Identity Manager 时间接地（动态）分配。Identity Manager 规则控制动态分配。

有关管理员角色的详细信息，请参见第 187 页中的 “了解和管理管理员角色”。

Identity Manager 策略

策略通过建立对帐户 ID、登录和密码特征的限制，对 Identity Manager 用户设置限制。*Identity System* **帐户策略**建立用户、密码以及验证策略选项和限制。**资源密码和帐户** *ID* **策略** 设置长度规则、字符类型规则以及允许的字词和属性值。**字典策略**使 Identity Auditor 可以对照字词数据库检查密码，以确保密码不会轻易受到字典攻击。

有关策略的详细信息，请参见第 88 页中的 “什么是策略？ ”。

审计策略

区别于其他系统策略，**审计策略**会为一组特定资源的用户定义策略违规。审计策略会建立一个或多个规则，用于判断用户是否违规。这些规则取决于以资源定义的一个或多个属性为基础的条件。当系统扫描用户时，它使用在分配给该用户的审计策略中定义的条件，以确定是否发生违规。

有关审计策略的详细信息，请参见第 377 页中的 “关于审计策略”。

对象关系

下表简要说明了 Identity Manager 对象以及它们之间的关系。

表 1–1 Identity Manager 对象关系

Identity Manager 对象	它是什么？	适用目标
用户帐户	Identity Manager 和一种或多种资源上的帐户。用户数据可从资源加载到 Identity Manager。 具有扩展权限的一类特殊用户（Identity Manager 管理员）	**角色**。通常，每个用户帐户都被分配了一个或多个角色。 **组织**。用户帐户作为组织的一部分安排在分层结构中。Identity Manager 管理员还额外管理组织。 **资源**。各资源均可被分配给用户帐户。 **权能**。管理员被分配了适用于其管理的组织的权能。
角色	业务角色用于将组织中执行类似任务的人员工作时所需的访问权限划分到各个组中。应用程序和 IT 角色用于将资源划分到各个组中，以便通过业务角色将资源分配给用户。在大型组织中，基于角色的资源分配可简化资源管理。	**资源和资源组**。可将资源和资源组分配给资产、应用程序和 IT 角色。 **用户帐户**。可将具有类似特征的用户帐户分配给业务角色。 **资产、应用程序和 IT 角色**。可将资产、应用程序和 IT 角色分配给业务角色。
资源	存储有关帐户受到管理的系统、应用程序或其他资源的信息。	**角色**。可将资源分配给应用程序和 IT 角色，然后再将这些角色分配给业务角色。用户帐户将从其业务角色分配不严格地“继承”资源访问权限。 **用户帐户**。资源可分别分配给用户帐户。
资源组	经排序的资源组。	**角色**。资源组被分配给角色；用户帐户通过分配业务角色“继承”资源的访问权限。 **用户帐户**。资源组可直接分配给用户帐户。
组织	定义由管理员管理的实体的范围；具有分层结构。	**资源**。给定组织中的管理员可访问某些资源或所有资源。 **管理员**。组织由具有管理权限的用户管理（控制）。管理员可管理一个或多个组织。给定组织中的管理权限可传递至其子组织。 **用户帐户**。每个用户帐户都可被分配到一个 Identity Manager 组织以及一个或多个目录组织。

表 1–1 Identity Manager 对象关系 （续）

Identity Manager 对象	它是什么？	适用目标
目录连接	分层相关的一组组织，这些组织镜像目录资源的实际层级容器集合。	**组织**。目录连接中的每个组织都是虚拟组织。
管理员角色	为分配给管理员的每一组组织定义唯一的一组权能。	**管理员**。管理员角色被分配给管理员。 **权能和组织**。权能和组织被直接或间接（动态）分配给管理员角色。
权能	定义一组系统权限。	**管理员**。权能被分配给管理员。
策略	设置密码和验证限制。	**用户帐户**。策略被分配给用户帐户。 **组织**。策略被分配给组织或由组织继承。
审计策略	设置用于判断用户是否违规的规则。	**用户帐户**。审计策略被分配给用户帐户。 **组织**。审计策略被分配给组织。

◆ ◆ ◆ 第 2 章

Identity Manager 用户界面入门

阅读本章内容可以了解 Identity Manager 图形用户界面 (User Interface, UI) 以及如何快速开始使用 Identity Manager。

包括下列主题：

Identity Manager 管理员界面

Identity Manager 系统包括两个主要图形界面，用户可通过它们执行任务。这两个界面是最终用户界面和管理员界面。本章后面的部分（第 36 页中的 “Identity Manager 最终用户界面”）介绍了最终用户界面（也称为用户界面）。此处介绍了管理员界面。

Identity Manager 管理员界面是本产品的主要管理视图。通过此界面，Identity Manager 管理员可管理用户、设置和分配资源、定义权限和访问级别以及审计 Identity Manager 系统中的遵循性。

界面通过以下元素进行组织：

- **导航栏选项卡**。这些选项卡位于每个界面页的顶部，通过它们可以导航主要功能区域。
- **子选项卡或菜单**。根据特定实现，您可能会看到每个导航栏选项卡下方的辅助选项卡或菜单。这些子选项卡或菜单选项允许您访问某一个功能区域内的任务。

在某些区域（例如“帐户”）中，**选项卡式的表单**将较长的表单分成一个或多个页，使您在导航这些表单时更加容易。图 2–1 中对其进行了展示。

注 – 附录 C，用户界面快速参考提供了在 UI 中执行管理任务的快速参考。

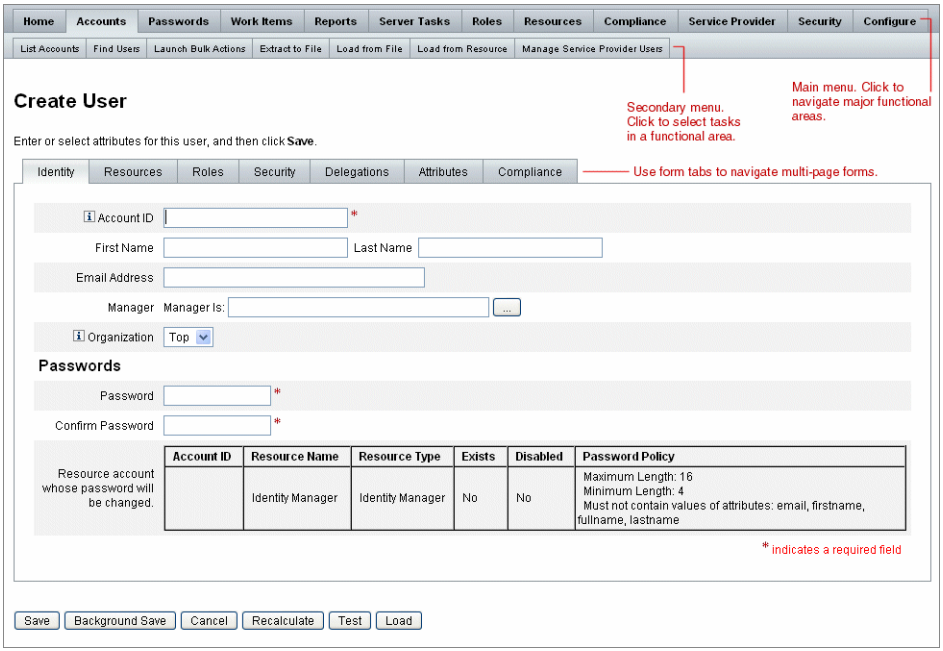


图 2–1 Identity Manager 管理员界面

登录到 Identity Manager 管理员界面

▼ 打开管理员界面

1. **打开 Web 浏览器，然后在地址栏中键入以下 URL：**

   `http://<AppServerHost>:<Port>/idm/login.jsp`

2. **输入用户 ID 和密码，然后单击登录。**

   如果用户 ID 具有分配的权能和受控组织，则会打开管理员界面。

会话限制和 Cookie

如果在管理员的 Web 浏览器中启用了 Cookie，在到达已配置的会话限制分配的时间之前，管理员在管理员界面上将一直保持登录状态。如果在浏览器中禁用了 Cookie，在执行某些操作时，将导致系统在会话期间提示管理员重新登录。

这些操作包括：

- 取消管理员、角色和组织重命名
- 取消组织删除
- 创建用户登录模块和管理员登录模块

为避免多次登录请求，应启用 Cookie。

忘记用户 ID

Identity Manager 允许管理员找回他或她忘记的用户 ID。当管理员在登录页面中单击“忘记用户 ID？”时，将显示一个查找页面，并请求与帐户关联的身份属性信息，例如，姓名、电子邮件地址或电话号码。

然后 Identity Manager 将创建一个查询，以查找与输入值相匹配的单个用户。如果未找到匹配项，或找到多个匹配项，则会在“查找用户 ID”页上显示一条错误消息。

默认情况下，将启用查找功能，但可以使用以下某个操作禁用此功能：

- 将 `login.jsp` 中的 `forgotUserIdMode` 值设置为 false。
- 编辑系统配置对象，并将 `admin` 和/或 `user` 属性的 `disableForgotUserId` 属性值设置为 true。

  有关编辑系统配置对象的说明，请参见第 102 页中的 “编辑 Identity Manager 配置对象”。

注 – 如果从早期的 Identity Manager 版本升级到 8.1 版，默认情况下，将**禁用**“忘记用户 ID？”功能。

要启用此功能，必须修改系统配置对象中的以下属性（第 102 页中的 “编辑 Identity Manager 配置对象”）：

```
ui.web.user.disableForgotUserId = false
ui.web.admin.disableForgotUserId = false
```

所显示的用户属性名称集是通过系统配置属性 `security.authn.lookupUserIdAttributes.<Administrator Interface | User Interface>` 配置的。可以指定的属性为 `IDM` **模式配置**配置对象中定义为可查询属性的属性。

恢复之后，Identity Manager 将使用“用户 ID 恢复”电子邮件模板向已恢复的用户的电子邮件地址发送邮件。

Identity Manager 最终用户界面

Identity Manager 最终用户界面（也称为“Identity Manager 用户界面”）只显示 Identity Manager 系统的一部分视图。此视图专为不具备管理权能的用户而设计。

注 – 有关如何登录到最终用户界面的说明，请参见第 38 页中的 “登录到 Identity Manager 最终用户界面”。

用户可以在用户界面中执行各种操作，例如更改用户密码、执行自置备任务以及管理工作项目和委托。

可以对 Identity Manager 进行配置，以使用户可通过单击最终用户界面登录页中的链接来请求帐户。有关详细信息，请参见第 84 页中的 “匿名注册”。

五个最终用户界面选项卡

最终用户界面分为以下五个部分：

“主页”选项卡

用户登录到 Identity Manager 用户界面时，“主页”选项卡上将显示用户的所有暂挂工作项目和委托，如下图中所示。

图 2–2 用户界面（“主页”选项卡）

可通过“主页”选项卡快速访问任何暂挂项目。用户可以单击列表中的项目，对工作项目请求进行响应或执行其他可用操作。

“工作项目”选项卡

“工作项目”选项卡又细分为单独的“批准”、“证明”、“修正”和“其他”选项卡。在用户界面的这一区域中，用户可以批准或拒绝拥有的或有权对其执行操作的所有暂挂工作项目。

“请求”选项卡

“请求”选项卡包含两个子选项卡：“启动请求”和“查看”。

在“启动请求”选项卡上，用户可以选择以下两个选项：“更新我的角色”和“更新我的资源”。

- 在“更新我的角色”页中，用户可以请求可能适用于该用户的可用角色列表中的角色。当最终用户提交角色请求时，将会生成一个工作项目，并向为该角色指定的批准者发送批准通知。最终用户也可以请求将其从一个或多个角色中删除或**取消分配**。

  有关如何创建最终用户可请求访问的可选角色的信息，请参见第 5 章，角色和资源一章。
- 在“更新我的资源”页中，用户可以请求可能适用于该用户的各资源列表中的资源。与角色请求一样，资源请求也会生成工作项目，需要在处理之前批准这些项目。

“查看”子选项卡显示用户提交的请求的状态详细信息。从该区域中，用户可以查看所提交的请求的进程状态和任务结果。

“委托”选项卡

在“委托”选项卡中，用户可以将工作项目委托给其他 Identity Manager 用户。例如，如果用户是为一个或多个角色分配的批准者，则可以委托在其休假的一段时间内将未来的批准工作项目发送给同事。通过使用“委托”页，用户可以创建和管理委托，而无需得到管理员的帮助。

“配置文件”选项卡

在“配置文件”选项卡中，最终用户可以管理其 Identity Manger 密码和帐户属性设置。此选项卡分为以下四个子选项卡：

- **更改密码**。最终用户可在选定资源或所有资源上更改其密码。
- **帐户属性**。最终用户可更改某些属性，如 Identity Manager 将帐户通知发送到的帐户电子邮件地址。
- **验证问题**。用于管理用户帐户的验证问题和答案。
- **访问权限**。列出用户当前分配的角色和资源分配。

登录到 Identity Manager 最终用户界面

可以使用以下说明登录到 Identity Manager 最终用户界面。

▼ 打开最终用户界面

1 **打开 Web 浏览器，然后在地址栏中键入以下 URL：**

`http://<AppServerHost>:<Port>/idm/user/login.jsp`

2 **输入用户 ID 和密码，然后单击“登录”。**

将打开最终用户界面。

找回忘记的用户 ID

Identity Manager 允许最终用户找回其忘记的用户 ID。有关详细信息，请参见第 34 页中的 “登录到 Identity Manager 管理员界面”一节中的第 35 页中的 “忘记用户 ID”。

帮助和指导

要成功完成某些任务，可能需要参考“帮助”和 Identity Manager **指导**（字段级别的信息和说明）。Identity Manager 的管理员界面和用户界面均提供帮助和指导。

Identity Manager 帮助

有关与任务相关的帮助和信息，请单击“帮助”按钮，该按钮位于每个管理员界面和用户界面页的顶部，如下图中所示。

图 2–3 Identity Manager 界面中的“帮助”按钮

在每个“帮助”窗口的底部有一个“内容”链接，通过该链接可转到其他“帮助”主题和 Identity Manager 术语表。

Identity Manager 指导

Identity Manager 指导是有针对性的简短帮助，显示在许多页面字段旁。其用途是当您在页内移动时帮助您输入信息或选择选项，以执行某项任务。

包含指导的字段旁会显示一个以字母 "i" 标记的符号。单击此符号可以打开窗口并显示与其关联的信息。

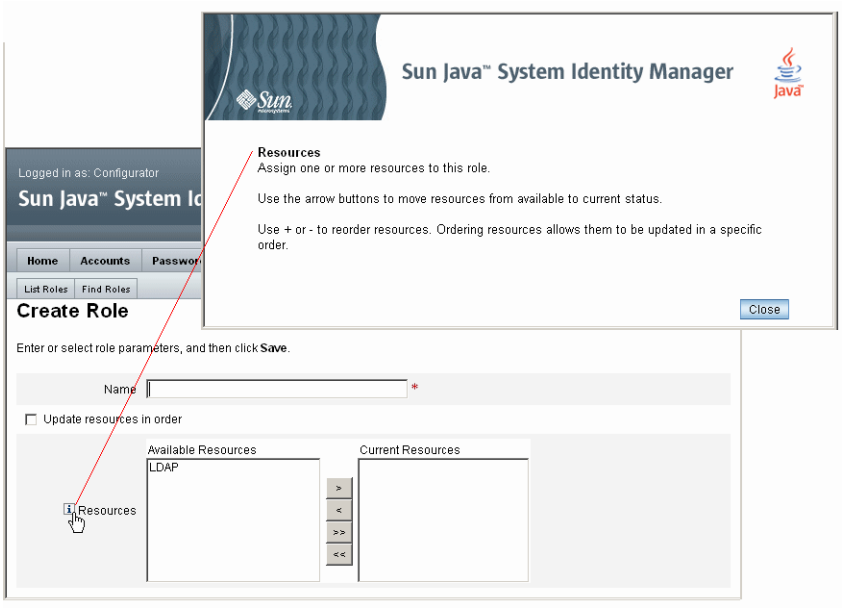


图 2–4 Identity Manager 指导

Identity Manager 的“调试”页

管理员界面包含一些页面，这些页面在需要优化 Identity Manager 或解决问题时非常有用。要访问这些页面，请打开 Identity Manager 的“调试”页（也称为“系统设置”页）。

要打开 Identity Manager 的“调试”页，请在浏览器中键入以下 URL。（根据您的平台和配置，URL 可能会区分大小写。）

```
http://<AppServerHost>:<Port>/idm/debug/session.jsp
```

用户必须具有“调试”权能才能查看 `/idm/debug/` 页。有关权能的信息，请参见第 187 页中的 “为用户分配权能”。

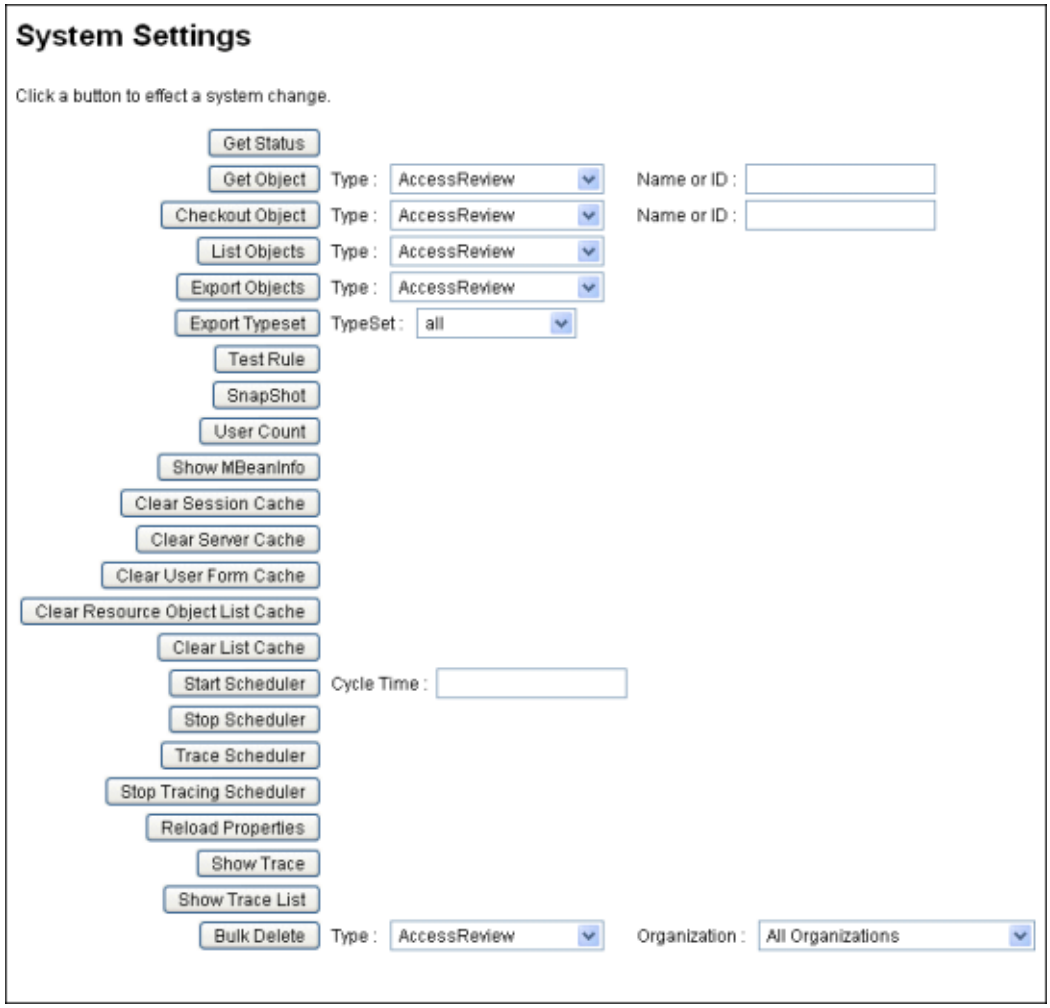


图 2–5 Identity Manager 的"调试"页（系统设置）

有关 Identity Manager 故障排除的信息，请参见《Sun Identity Manager 8.1 System Administrator's Guide》中的第 5 章 "Tracing and Troubleshooting"。

Identity Manager IDE

Sun Identity Manager 集成开发环境 (Identity Manager IDE) 提供 Identity Manager 表单、规则和工作流的图形视图。这是一个完全集成的 NetBeans 插件，它随 Identity Manager 分发软件包中的 Identity Manager 一起分发。

使用 Identity Manager IDE 可创建和编辑表单，这些表单确立了每个 Identity Manager 页上可用的功能。还可修改 Identity Manager **工作流**，这些工作流定义了使用 Identity Manager 用户帐户时遵循的操作顺序或执行任务的顺序。此外，您还可修改 Identity Manager 中定义的用于确定工作流行为的规则。

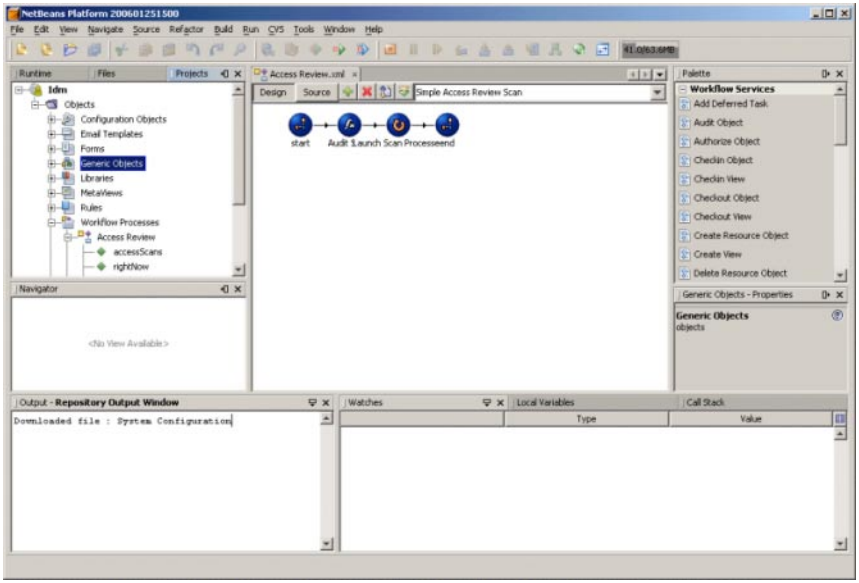


图 2–6 Identity Manager IDE 界面

要下载 Identity Manager IDE，请访问以下网站：

`https://identitymanageride.dev.java.net/`

如果早期版本的 Identity Manager 上已安装业务进程编辑器 (Business Process Editor, BPE)，您还可使用它来进行自定义。

后续内容

在熟悉 Identity Manager 界面以及查找信息的方法之后，可以使用以下参考来查找您要重点了解的主题：

章节主题	描述
第 3 章，用户和帐户管理	介绍界面的“帐户”区域并提供用于管理用户帐户的步骤。
第 5 章，角色和资源	介绍如何使用 Identity Manager 角色和资源。
第 4 章，配置业务管理对象	介绍配置任务以及如何设置 Identity Manager 对象。
第 6 章，管理	介绍如何创建和管理 Identity Manager 管理员和组织。
第 7 章，数据加载和同步	提供可用于维护 Identity Manager 中当前数据的功能和工具的指南。
第 8 章，报告	介绍报告以及如何生成报告。
第 9 章，任务模板	介绍可用于配置某些工作流行为的任务模板。
第 10 章，审计日志记录	介绍审计日志以及审计系统如何工作。
第 11 章，PasswordSync	介绍如何设置 PasswordSync 实用程序，以将 Windows Active Directory 域中的密码更改与 Identity Manager 的更改同步。
第 12 章，安全	介绍安全性功能以及如何使用这些功能。
第 13 章，身份审计：基本概念	介绍基本审计概念。
第 14 章，审计：审计策略	介绍如何创建审计策略。
第 15 章，审计：监视遵循性	介绍如何执行审计查看和实现实践，以帮助您管理对联邦委托法规的遵循性。
第 16 章，数据导出器	通过使用数据导出器功能，您可以将有关用户、角色和其他对象类型的信息写入到外部数据仓库中。
第 17 章，服务提供者管理	介绍用于管理服务提供商用户的功能。
附录 A，lh 参考消息	介绍 Identity Manager 命令行中可用的命令。
附录 B，审计日志数据库模式	支持的数据库类型的审计数据模式值以及审计日志数据库映射
附录 C，用户界面快速参考	这是一个在 UI 中执行管理任务的快速参考。它显示了开始每项任务时应转到的主要位置，并显示执行同一任务可以使用的替代位置或方法（如果可用）。

章节主题	描述
附录 D，权能定义	Identity Manager 的默认基于任务的权能和功能性权能（及定义）的列表。该附录还列出了可使用每种基于任务的权能访问的选项卡和子选项卡。

◆ ◆ ◆ 第 3 章

3 用户和帐户管理

本章提供了通过 Identity Manager 管理员界面创建和管理用户的信息和步骤。

该信息分为以下几个部分：

界面的“帐户”区域

用户是指拥有 Identity Manager 系统帐户的任何人。Identity Manager 为每个用户存储一系列数据。这些信息共同构成每个用户的 Identity Manager 身份。

通过使用 Identity Manager 的“帐户”/“用户列表”页，您可以管理 Identity Manager 用户。要访问此区域，请单击管理员界面菜单栏上的**帐户**。

帐户列表显示所有 Identity Manager 用户帐户。帐户按组织和虚拟组织进行分组，这些组织以文件夹的形式分层表示。

您可以按全名 ("Name")、用户的姓 ("Last Name") 或用户的名 ("First Name") 对帐户列表进行排序。单击标题栏可以按列进行排序。单击同一标题栏可以在升序和降序间切换。按全称（“名称”列）排序时，分层结构中所有级别的所有项都按字母顺序排序。

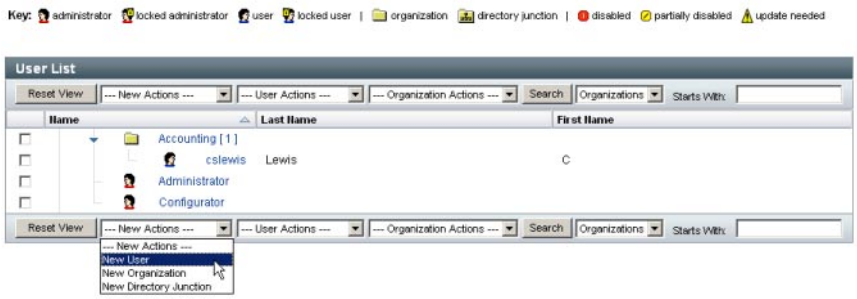
要展开分层结构视图，查看组织中的帐户，请单击文件夹旁的三角指示符。再次单击指示符可折叠视图。

帐户区域中的操作列表

可以使用操作列表（位于帐户区域的顶部和底部，如第 46 页中的 "帐户区域中的操作列表"中所示）执行一系列操作。

操作列表选项分为：

- **新建操作**。创建用户、组织和目录连接。
- **用户操作**。编辑、查看和更改用户状态；更改和重设密码；删除、启用、禁用、解除锁定、移动、更新和重命名用户；运行用户审计报告。
- **组织操作**。执行一系列组织和用户操作。



在"帐户列表"区域中搜索

使用帐户区域搜索功能查找用户和组织。从列表中选择"组织"或"用户"，在搜索区域中输入用户或组织名称开头的一个或多个字符，然后单击**搜索**。有关在帐户区域中搜索的详细信息，请参见第 54 页中的 "查找和查看用户帐户"。

用户帐户状态

每个用户帐户旁边显示的图标指示当前已分配帐户的状态。表 3–1 介绍了每个图标所表示的含义。

表 3–1 用户帐户状态图标描述

指示器	状态
	已锁定用户的 Identity Manager 帐户。请注意，此图标仅反映了 Identity Manager 帐户的锁定状态，而不反映用户的任何资源帐户的状态。 在超过 Identity Manager 帐户策略中定义的 Identity Manager 帐户登录尝试失败的最大次数后，将会锁定用户。在允许的最大次数中，仅计算 Identity Manager 帐户的密码或提问式登录失败次数。因此，如果 Identity Manager 登录应用程序（即，管理员界面、最终用户界面等）的登录模块组中不包含 Identity Manager 登录模块，则不会考虑 Identity Manager 失败的密码策略。不过，无论为给定 Identity Manager 登录应用程序配置了哪种登录模块栈，只要提问式登录失败次数超过在 Identity Manager 帐户策略中配置的最大次数，都可能会导致用户锁定并显示该图标。 有关如何解除帐户锁定的信息，请参见第 68 页中的 “解除锁定用户帐户”。
	已锁定管理员的 Identity Manager 帐户。请注意，此图标仅反映了 Identity Manager 帐户的锁定状态，而不反映管理员的任何资源帐户的状态。有关详细信息，请参见上面对用户锁定图标的描述。
	已在所有已分配资源和 Identity Manager 中禁用此帐户。（启用帐户时，不显示图标。） 有关如何启用已禁用的帐户的信息，请参见第 66 页中的 “禁用、启用和解除锁定用户帐户”。
	帐户被部分禁用，表示在一个或多个已分配资源上被禁用。
	系统尝试在一个或多个资源上创建或更新 Identity Manager 用户帐户，但未成功。（如果在所有已分配资源上更新了某一帐户，则不显示图标。）

注 – 在“管理员”列中，如果 Identity Manager 找不到与列出的名称匹配的 Identity Manager 帐户，则管理员的用户名将显示在括号内。

“用户”页（创建/编辑/查看）

本节介绍了管理员界面中提供的“创建用户”、“编辑用户”和“查看用户”页。本章后面介绍了如何使用这些页面。

注 – 本文档介绍了随 Identity Manager 提供的一组默认“创建用户”、“编辑用户”和“查看用户”页。不过，为了更好地反映业务流程或特定管理员权能，应创建针对您的环境的自定义用户表单。有关自定义用户表单的详细信息，请参见《Sun Identity Manager Deployment Reference》中的第 2 章 “Identity Manager Forms”。

- 第 48 页中的 ““身份”选项卡”

默认 Identity Manager 用户页面将划分到以下选项卡或部分中 :

- 身份
- 分配
- 安全
- 委托
- 属性
- 遵循性

"身份"选项卡

"身份"区域定义了用户的帐户 ID、名称、联系人信息、管理员、控制的组织和 Identity Manager 帐户密码。它还标识用户可以访问的资源以及控制每个资源帐户的密码策略。

注 – 有关设置帐户密码策略的信息，请参阅本章中标题为第 76 页中的 "管理帐户安全和权限"的一节。

下图展示了"创建用户"页的"身份"区域。

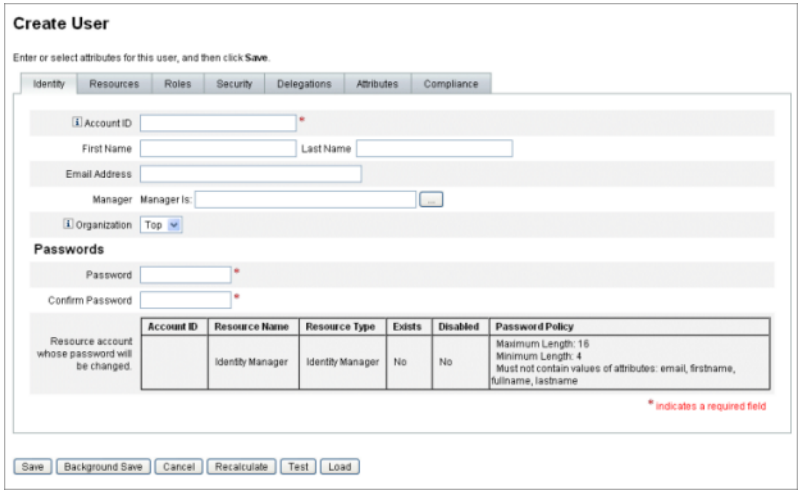


图 3–1 创建用户 - 身份

"资源"选项卡

"资源"区域可用于为用户直接分配资源和资源组。还可以分配资源排除。

直接分配的资源为通过**角色分配**间接分配给用户的资源提供补充。角色分配概要描述了一类用户。角色通过间接分配定义用户对资源的访问。

"角色"选项卡

"角色"选项卡用于将一个或多个角色分配给用户，以及管理这些角色分配。

有关此选项卡的信息，请参见第 124 页中的 "将角色分配给用户"。

"安全性"选项卡

在 Identity Manager 术语中，分配了扩展权能的用户称为 Identity Manager **管理员**。可以使用"安全性"选项卡为用户分配管理员权限。

有关使用"安全性"选项卡创建管理员的详细信息，请参见第 172 页中的 "创建和管理管理员"。

安全表单包含以下几个部分。

- **管理员角色**。为用户分配一个或多个管理角色。角色是一对特定的权能和受控组织，有助于以协调的方式为用户分配管理职责。
- **权能**。在 Identity Manager 系统中启用权限。通常根据工作职责向每个 Identity Manager 管理员分配一项或多项权能。

  第 184 页中的 "了解和管理权能"中介绍了权能。附录 D，权能定义包含基于任务的权能及其定义的列表。该附录还列出了可使用每种权能访问的选项卡和子选项卡。

- **受控组织**。分配该用户有权以管理员身份管理的组织。该管理员可管理已分配组织以及在分层结构中处于该组织之下的任何组织中的对象。

注 – 要拥有管理员权能，必须至少为用户分配一个管理员角色，或一个或多个权能，以及一个或多个受控组织。有关 Identity Manager 管理员的详细信息，请参见第 171 页中的 "了解 Identity Manager 管理"。

- **用户表单**。指定管理员在创建和编辑用户时将使用的用户表单。如果选择 **None**，管理员将继承分配给其组织的用户表单。
- **查看用户表单**。指定管理员在查看用户时将使用的用户表单。如果选择 **None**，管理员将继承分配给其组织的查看用户表单。
- **帐户策略**。设置密码和验证限制。

"委托"选项卡

"创建用户"页上的"委托"选项卡允许您在指定的时间内将工作项目委托给其他用户。有关委托工作项目的详细信息，请参阅第 199 页中的 "委托工作项目"。

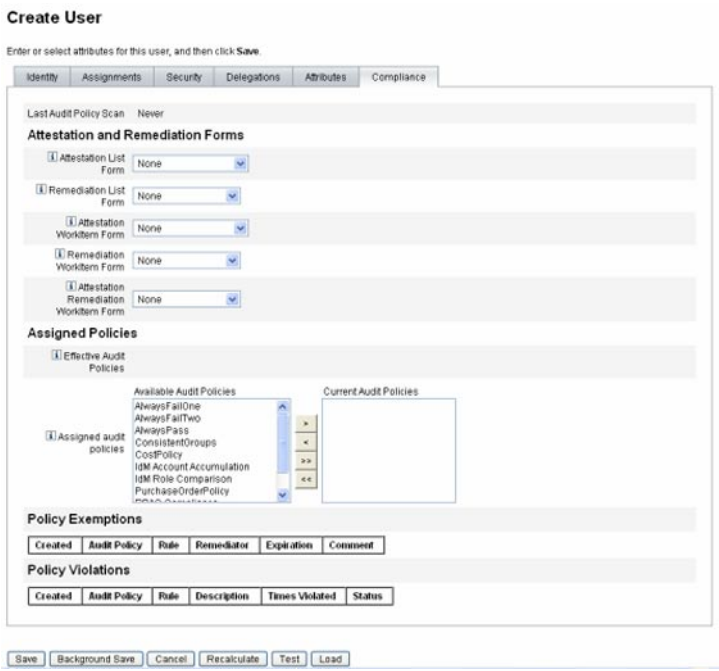
"属性"选项卡

"创建用户"页上的"属性"选项卡定义与分配的资源关联的帐户属性。列出的属性按分配的资源分类，具体情况根据分配资源的不同而不同。

"遵循性"选项卡

"遵循性"选项卡：

- 允许您为用户帐户选择证明和修正表单。
- 指定为用户帐户分配的审计策略，包括通过用户的组织分配生效的策略。仅可以通过编辑用户的当前组织或将用户移动到其他组织来更改这些策略分配。
- 指示策略扫描、违规和免除的当前状态，如下图所示（如果适用于用户帐户）。此信息包括选定用户上一次审计策略扫描的日期和时间。



要分配审计策略，请将选定策略从**可用审计策略**列表移动到**当前审计策略**列表中。

注 – 通过从**用户操作**列表中选择**查看遵循性违规日志**并指定要查看的条目范围，可以查看在特定时间段内为用户记录的遵循性违规。

创建用户和使用用户帐户

从管理员界面的“帐户/用户列表”页中，您可以对以下系统对象执行一系列操作：

- **管理员和用户**。查看、创建、编辑、移动、重命名、取消置备、启用、禁用、更新、解除锁定、删除、取消分配、解除链接以及审计。

  有关创建和编辑管理员帐户的详细信息，请参见第 171 页中的“了解 Identity Manager 管理”。

- **组织**。在组织的成员上创建、编辑、刷新和执行用户操作。

  有关组织的详细信息，请参见第 178 页中的“了解 Identity Manager 组织”。

- **目录连接**。创建与分层相关的一组组织以镜像目录资源的实际层级容器集合。

  有关目录连接的详细信息，请参见第 182 页中的“了解目录连接和虚拟组织”。

启用进程图

进程图描绘了 Identity Manager 在创建用户帐户或对其进行处理时遵循的工作流。如果启用进程图，它将显示在 Identity Manager 完成任务时创建的结果页或任务摘要页上。

在 Identity Manager 8.0 版中，为新安装和升级安装禁用了进程图。

▼ 在 Identity Manager 中启用进程图

1. **按照第 102 页中的“编辑 Identity Manager 配置对象”中的步骤，打开系统配置对象以进行编辑。**

2. **找到以下 XML 元素：**

```
<Attribute name='disableProcessDiagrams'>
  <Boolean>true</Boolean>
</Attribute>
```

3. **将 `true` 值更改为 `false`。**

4. **单击“保存”。**

5. **重新启动服务器以使更改生效。**

   也可以在最终用户界面中启用进程图，但前提是必须先按照上述步骤在管理员界面中将其启用。有关详细信息，请参见第 98 页中的 “在最终用户界面中启用进程图”。

▼ 在 Identity Manager 中创建用户

可以通过管理员界面菜单栏中的“帐户”选项卡创建和管理用户。

1. **在管理员界面中，单击“帐户”。**

2. **要在特定组织中创建用户，请选择该组织，然后从“新建操作”列表中选择“新建用户”。**

   或者，要在 Top 组织中创建用户帐户，请从“新建操作”列表中选择“新建用户”。

3. **在以下选项卡或部分中填写信息。**

   - **身份**。名称、组织、密码和其他详细信息。（请参见第 48 页中的 ““身份”选项卡”。）
   - **资源**。各个资源和资源组分配以及资源排除。（请参见第 49 页中的 ““资源”选项卡”。）
   - **角色**。角色分配。有关角色的信息，请参见第 103 页中的 “了解和管理角色”。有关填写“角色”选项卡的说明，请参见第 124 页中的 “将角色分配给用户”。

- **安全性**。管理员角色、受控组织和权能。以及用户表单设置和帐户策略。（请参见第 49 页中的 ““安全性”选项卡”。）
- **委托**。工作项目委托。（请参见第 50 页中的 ““委托”选项卡”。）
- **属性**。已分配的资源的特定属性。（请参见第 50 页中的 ““属性”选项卡”。）
- **遵循性**。为用户帐户选择证明和修正表单。在“遵循性”区域中，您还可以为用户帐户指定分配的审计策略，其中包括通过用户的组织分配生效的策略。表示策略扫描、违规和免除的当前状态，并包括用户上次审计策略扫描的相关信息。（请参见第 50 页中的 ““属性”选项卡”。）

  请注意，一个区域中的可用选项可能取决于在另一个区域中选择的内容。

为了更好地反映业务流程或特定管理员权能，应针对您的环境自定义用户表单。有关自定义用户表单的详细信息，请参见《Sun Identity Manager Deployment Reference》中的“Customizing Forms”。

4 **完成后，保存该帐户。**

可以使用以下两个选项来保存用户帐户：

- **保存**。保存用户帐户。如果您将大量资源分配给该帐户，则此过程可能需要一段时间。
- **后台保存**。此过程作为后台任务保存用户帐户，这样您可以继续使用 Identity Manager。每次正在进行保存时，都会在“帐户”页、“查找用户结果”页和主页中显示一个任务状态指示器。

  状态指示器（如下表所述）可以帮助您监视保存进程的进度。

状态指示器	状态
	正在进行保存。
	保存过程已暂停。这通常表示该过程正在等待批准。
	已顺利完成保存。这并不表示用户已被成功保存；只是表示保存的过程没有任何错误。
	尚未开始保存。
	已完成保存过程，但是出现一个或多个错误。

将鼠标移至状态指示器中显示的用户图标的上方，便可看到有关后台保存过程的详细信息。

注 – 如果已配置生效，则在创建用户时，将会创建一个可从“批准”选项卡中查看的工作项目。如果批准该项目，则会覆盖生效日期并创建帐户。如果拒绝该项目，则会取消帐户创建。有关配置生效的详细信息，请参见第 283 页中的 “配置“生效和失效”选项卡”。

为用户创建多个资源帐户

Identity Manager 提供了将多个资源帐户分配给单个用户的功能。它通过允许为每种资源定义多种资源帐户类型或**帐户类型**来实现此目的。应该根据需要创建资源帐户类型，以便与资源上的每种功能帐户类型相匹配。例如，AIX SuperUser 或 AIX BusinessAdmin。

为什么要针对每种资源为每个用户分配多个帐户？

在某些情况下，Identity Manager 用户可能需要在资源上设置多个帐户。用户可能具有多个与资源有关的不同作业功能。例如，用户可能同时是资源的用户和管理员。最好的做法是，建议对每个功能使用不同的帐户。这样，如果一个帐户受到破坏，其他帐户授予的访问权限仍然是安全的。

配置帐户类型

要使资源支持单个用户的多个帐户，必须先在 Identity Manager 中定义资源帐户类型。要为资源定义资源帐户类型，请使用资源向导。有关信息，请参见第 137 页中的 “管理资源列表”。

您必须先启用并配置资源帐户类型，然后才能将这些类型分配给用户。

分配帐户类型

在定义了帐户类型后，您可以将它们分配给资源。Identity Manager 将每次分配的帐户类型都视为单独的帐户。因此，每次在角色中的不同分配可能具有不同的属性集。

与每个资源具有单个帐户类似，所有特定类型的分配仅创建一个帐户，而与分配次数无关。

虽然可以将用户分配给资源上的任意数量的不同类型帐户，但只能为每个用户分配资源上的一个给定类型的帐户。该规则的例外情况是内置的“默认”类型。用户可以在资源上具有任意数量的默认类型帐户。不过，建议不要这样做，因为这可能导致在表单和视图中引用帐户时出现不确定性。

查找和查看用户帐户

使用 Identity Manager 查找功能可搜索用户帐户。输入和选择搜索参数以后，Identity Manager 将查找与您的选择匹配的所有帐户。

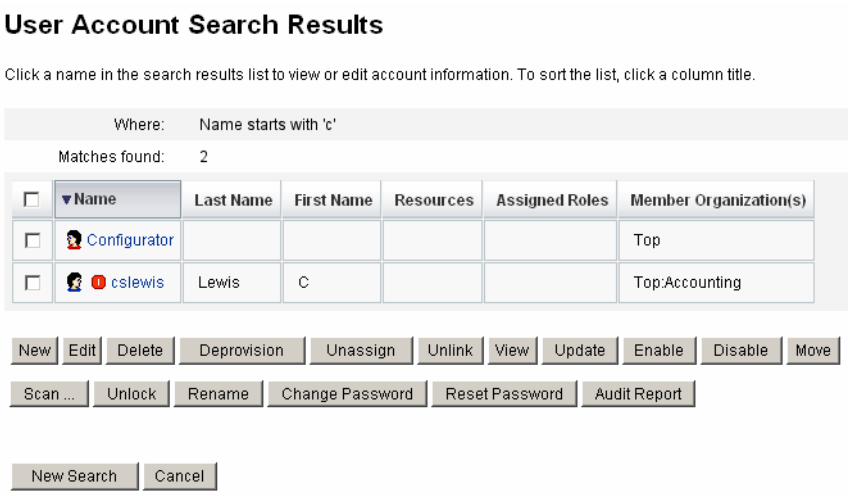
要搜索帐户，请从菜单栏中选择“帐户”→“查找用户”。可以使用下面的一种或多种搜索类型搜索帐户：

- **帐户详细信息**（如用户名、电子邮件地址、姓氏或名字）。这些选项取决于贵机构的具体 Identity Manager 实现。
- **用户的管理员**。如果管理员的用户名与 Identity Manager 中的现有帐户不匹配，则该用户名将显示在括号内。
- **资源帐户状态**。选项包括：
  - **已禁用**。用户不能访问任何 Identity Manager 帐户或已分配的资源帐户。
  - **部分禁用**。用户不能访问一个或多个已分配的资源帐户。
  - **已启用**。用户拥有对所有已分配的资源帐户的访问权限。
- **已分配的资源**。选项包括：
  - **角色**（请参见第 131 页中的“查找分配给特定角色的用户”）
  - **组织**
  - **组织控制权限**
  - **权能**
  - **管理员角色**
- **用户帐户状态**。选项包括：
  - **已锁定**。因为密码或提问式登录尝试失败的最大次数超过允许的最大次数，用户帐户被锁定。
  - **尚未锁定**。未限制用户帐户访问。
- **更新状态**。选项包括：
  - **否**。尚未在任何资源中更新的用户帐户。
  - **部分**。已在至少一个（但不是所有）已分配资源中更新的用户帐户。
  - **全部**。已在所有已分配资源中更新的用户帐户。

搜索结果列表显示与您的搜索条件相匹配的所有帐户。

在结果页中，您可以：

- 选择要编辑的用户帐户。要编辑帐户，请在搜索结果列表中单击此帐户；或在列表中选择此帐户，然后单击“编辑”。
- 对一个或多个帐户执行操作（例如启用、禁用、解除锁定、删除、更新或更改/重设密码）。要执行操作，请在搜索结果列表中选择一个或多个帐户，然后单击相应的操作。
- 创建用户帐户。



编辑用户

本节中的信息介绍了如何查看、编辑、重新分配以及重命名用户帐户。

▼ 查看用户帐户

可以使用“查看用户”页并执行以下步骤来查看帐户信息。

1. **在管理员界面中，单击菜单中的“帐户”。**
   将打开“用户列表”页。
2. **选中要查看帐户的用户旁边的框。**
3. **在“用户操作”下拉菜单中，选择“查看”。**
   “查看用户”页显示用户身份、分配、安全性、委托、属性和遵循性信息中的一部分信息。“查看用户”页上的信息只能查看，不能进行编辑。
4. **单击“取消”返回至“帐户”列表。**

▼ 编辑用户帐户

可以使用“编辑用户”页并执行以下步骤来编辑帐户信息。

1. **在管理员界面中，单击菜单中的“帐户”。**
2. **选中要编辑帐户的用户旁边的框。**
3. **在“用户操作”下拉菜单中，选择“编辑”。**

4 **进行更改并保存。**

Identity Manager 将显示“更新资源帐户”页。此页显示分配给用户的资源帐户以及将应用于帐户的更改。

5 **选择“更新所有资源帐户”将更改应用于所有分配的资源；或者单独选择与此用户关联的一个或多个资源帐户进行更新，或者不更新任何资源帐户。**

6 **再次单击“保存”完成编辑，或者单击“返回编辑”进行进一步更改。**

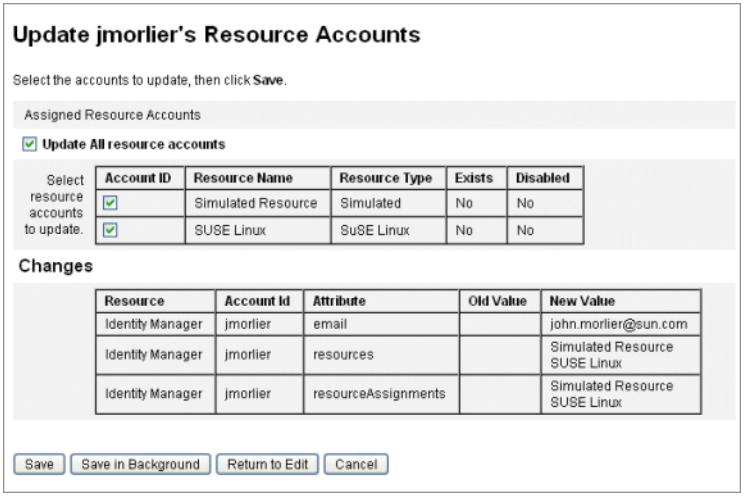


图 3–2 编辑用户（更新资源帐户）

将用户重新分配给其他组织

通过执行移动操作，您可以从某个组织中删除一个或多个用户，然后将其重新分配或移动到新组织中。

▼ 移动用户

1 **在管理员界面中，单击菜单中的“帐户”。**

将打开“用户列表”页。

2 **选中要移动的用户旁边的框。**

3 **在“用户操作”下拉菜单中，选择“移动”。**

将打开“更改用户组织”任务页。

4 **选择要将用户重新分配到的组织，然后单击“启动”。**

重命名用户

重命名资源上的帐户通常是个复杂的操作。因此，Identity Manager 提供一个单独的功能来重命名用户的 Identity Manager 帐户，或重命名与该用户相关的一个或多个资源帐户。

要使用重命名功能，请在列表中选择用户帐户，然后在 "User Actions" 列表中选择 "Rename" 选项。

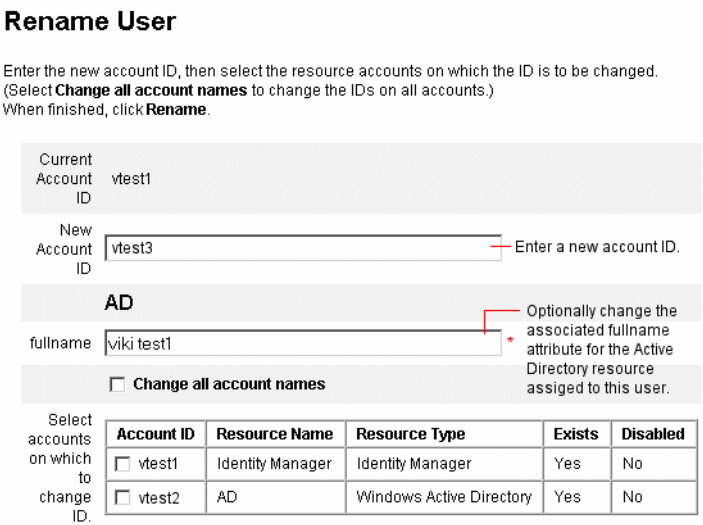
使用“重命名用户”页可更改用户帐户名、相关资源帐户名和与用户的 Identity Manager 帐户相关的资源帐户属性。

注 – 某些资源类型不支持帐户重命名功能。

如下图所示，此用户拥有已分配的 Active Directory 资源。

在重命名过程中，您可以更改：

- Identity Manager 用户帐户名称
- Active Directory 资源帐户名
- Active Directory 资源属性（全称）



更新与帐户关联的资源

在更新操作中，Identity Manager 更新与用户帐户相关的资源。从帐户区域执行的更新操作会将先前对用户进行的任何暂挂更改发送到选定的资源。

可能出现这种情况的条件是：

- 进行更新时资源不可用。
- 需要将对角色或资源组进行的更改发送到分配给该角色或资源组的所有用户。在这种情况下，您应使用 "Find User" 页搜索用户，然后选择一个或多个要对其执行更新操作的用户。

更新用户帐户时，有以下选项可供选择：

- 选择已分配的资源帐户是否接收更新的信息。
- 更新所有资源帐户或者从列表中单独选择帐户。

更新单个用户帐户上的资源

要更新用户帐户，请在列表中选择此帐户，然后在 "User Actions" 列表中选择 "Update"。

在 "Update Resource Accounts" 页中，选择一个或多个要更新的资源帐户，或者选择 "Update All resource accounts" 更新所有已分配的资源帐户。完成选择后，单击“确定”开始更新过程。或者，单击“后台保存”在后台执行操作。

使用确认页确认将数据发送到每个资源。

图 3–3 展示了“更新资源帐户”页。

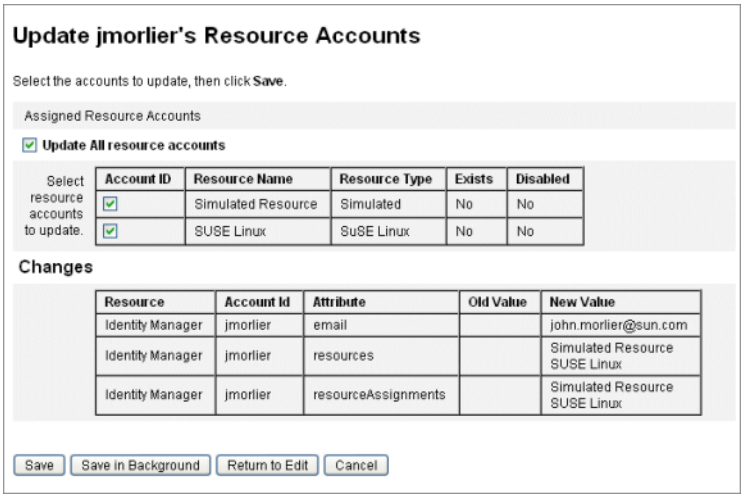


图 3–3 更新资源帐户

更新多个用户帐户上的资源

可以同时更新两个或更多 Identity Manager 用户帐户。在列表中选择多个用户帐户，然后在 "User Actions" 列表中选择 "Update"。

注 – 如果选择更新多个用户帐户，则无法从每个用户帐户单独选择已分配的资源帐户。此过程会更新所有选定用户帐户上的所有资源。

删除 Identity Manager 用户帐户

在 Identity Manager 中，将按照与删除远程资源帐户相同的方式删除 Identity Manager 用户帐户。请按照删除资源帐户的步骤进行操作，但要选择删除 Identity Manager 帐户，而不是选择远程资源帐户。

注 – 如果用户具有未完成的工作项目，或者用户将未完成的工作项目委托给另一个用户，Identity Manager 将禁止删除该用户的 Identity Manager 帐户。需要先解决委托的工作项目或将其转发给另一个用户，然后才能删除用户的 Identity Manager 帐户。

有关详细信息，请参见第 61 页中的 “从单个用户帐户中删除资源”和第 62 页中的 “从多个用户帐户中删除资源”。

从用户帐户中删除资源

Identity Manager 提供了一些删除操作，可用于从资源中删除 Identity Manager 用户帐户访问权限：

- **删除**。对于每个选定的资源，Identity Manager 将删除远程资源上的用户帐户。（要从 Identity Manager 中删除用户，请选择 Identity Manager 作为资源。）
  - 已删除的资源帐户将从 Identity Manager 用户中自动**解除链接**。
  - 删除的资源帐户不会从用户中**取消分配**。除非还选择了取消分配操作，否则，仍会将资源分配给用户。
- **取消分配**。对于每个选定的资源，Identity Manager 将从用户的已分配资源列表中删除该资源。
  - 已取消分配的资源帐户将从 Identity Manager 用户中自动**解除链接**。
  - **不会**删除远程资源上的用户帐户。除非还选择了删除操作，否则，该帐户将保持不变。
- **解除链接**。对于每个选定的资源，将从 Identity Manager 中删除用户的资源帐户信息。
  - 除非还选择了删除操作，否则，远程资源上的用户帐户将保持不变。
  - 除非还选择了取消分配操作，否则，用户的已分配资源列表上的资源将保持不变。
  - 如果取消通过角色或资源组间接分配给用户的帐户的链接，则该链接会在更新用户时恢复。

虽然取消置备作为用户操作显示在“用户列表”页菜单上，但 Identity Manager 中实际只有三个删除操作：删除、取消分配和解除链接。

要取消置备远程资源，请对该资源执行删除和取消分配操作。

从单个用户帐户中删除资源

可以使用以下过程，对单个 Identity Manager 用户执行删除操作。通过每次处理一个用户帐户，您可以为各个资源帐户指定不同的删除、取消分配和/或解除链接操作。

▼ 为单个用户帐户启动删除、取消分配或解除链接操作

1. **在管理员界面中，单击主菜单中的“帐户”。**
   将在“列出帐户”选项卡中显示“用户列表”页。
2. **选择一个用户，然后单击“用户操作”下拉菜单。**
3. **从列表中选择任何删除操作（删除、取消置备、取消分配或解除链接）。**
   Identity Manager 将显示“删除资源帐户”页（图 3–4）。

4 **填写表单。有关删除、取消分配和解除链接操作的详细信息，请参见第 61 页中的“从用户帐户中删除资源”。**

5 **单击“确定”。**

图 3–4 显示了“删除资源帐户”页。在该屏幕捕获中，用户 jrenfro 在远程资源（模拟资源）上具有一个活动帐户。选择了删除操作，这意味着，在提交表单时，将删除该资源上的 jrenfro 帐户。由于已删除的帐户将自动解除链接，因此，将从 Identity Manager 中删除该资源的帐户信息。由于未选择取消分配操作，因此，仍会将模拟资源分配给 jrenfro。

要删除 jrenfro 的 Identity Manager 帐户，应为 Identity Manager 选择删除操作。

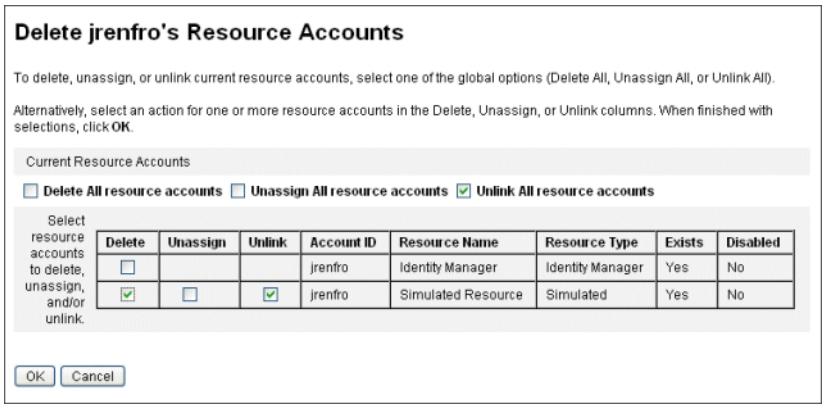


图 3–4 “删除资源帐户”页

从多个用户帐户中删除资源

您可以一次对多个 Identity Manager 用户帐户执行删除操作，但只能对用户的**所有**资源帐户执行选定的删除操作。

还可以使用 Identity Manager 的批量帐户操作功能执行删除操作。请参见第 71 页中的“Delete、DeleteAndUnlink、Disable、Enable、Unassign 和 Unlink 命令”。

▼ 为多个用户启动删除、取消分配或解除链接操作

1 **在管理员界面中，单击主菜单中的“帐户”。**

将在“列出帐户”选项卡中显示“用户列表”页。

2 **选择一个或多个用户，然后单击“用户操作”下拉菜单。**

3 **从列表中选择任何删除操作（删除、取消置备、取消分配或解除链接）。**

Identity Manager 将显示“确认删除、取消分配或解除链接”页（图 3–5）。

4 **指定要执行的操作。**

这些选项包括：

- **仅删除用户**。删除用户的 Identity Manager 帐户。此选项不会删除或取消分配用户的资源帐户。
- **删除用户和资源帐户**。删除用户的 Identity Manager 帐户以及用户的所有资源帐户。
- **仅删除资源帐户**。删除用户的所有资源帐户。此选项既不会取消分配资源帐户，也不会删除用户的 Identity Manager 帐户。
- **删除资源帐户并为用户取消分配直接分配的资源**。删除并取消分配用户的所有资源帐户，但不删除用户的 Identity Manager 帐户。
- **为用户取消分配直接分配的资源帐户**。取消分配直接分配的资源帐户。此选项不会删除远程资源上的用户帐户；不会影响通过角色或资源组分配的资源帐户。
- **解除资源帐户与用户的链接**。将用户的资源帐户信息从 Identity Manager 中删除。不会删除或取消分配远程资源上的用户帐户。在更新用户时，可以恢复通过角色或资源组间接分配给用户的帐户。

5 **单击“确定”。**

图 3–5 显示了“确认删除、取消分配或解除链接”页。页面顶部显示了六个可以为多个用户执行的操作。页面底部将显示受选定操作影响的用户。

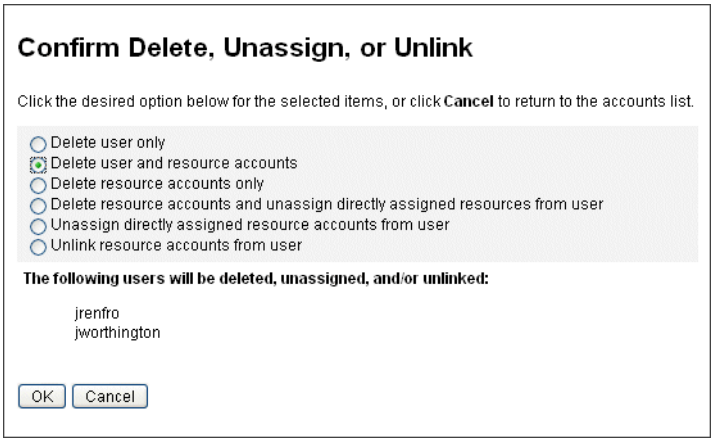


图 3–5 “确认删除、取消分配或解除链接”页

更改用户密码

所有 Identity Manager 用户都被分配了一个密码。设置 Identity Manager 用户密码后，该密码将用于同步用户的资源帐户密码。如果不能同步一个或多个资源帐户密码（例如，为了遵守必需的密码策略），则可单独进行设置。

注 – 有关帐户密码策略的信息以及有关用户验证的一般信息，请参见第 76 页中的 “管理帐户安全和权限”。

▼ 从“用户列表”页中更改密码

可以使用“用户列表”（“帐户”→“列出帐户”）页中的“更改密码”用户操作，从“用户列表”页中更改用户帐户密码。请按照以下步骤操作：

1. **在管理员界面中，单击主菜单中的“帐户”。**
   将在“列出帐户”选项卡中显示“用户列表”页。
2. **选择一个用户，然后单击“用户操作”下拉菜单。**
3. **要更改密码，请选择“更改密码”。**
   将打开“更改用户密码”页。
4. **键入新密码，然后单击“更改密码”按钮。**

▼ 从主菜单中更改密码

要从主菜单中更改用户帐户密码，请执行以下步骤：

1. **在管理员界面中，单击主菜单中的“密码”。**
   默认情况下，将显示“更改用户密码”页。

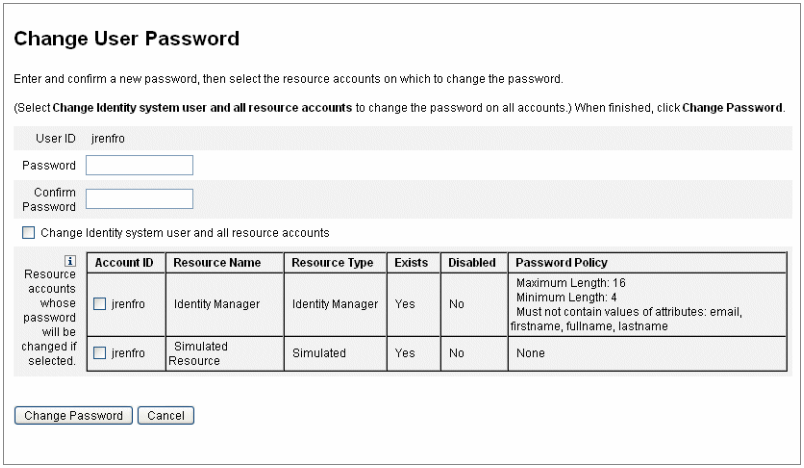


图 3–6 更改用户密码

2. **选择搜索项目（例如帐户名称、电子邮件地址、姓或名），然后选择搜索类型（开头为、包含或是）。**

3. **在输入字段中键入搜索项目的一个或多个字母，然后单击“查找”。Identity Manager 将返回 ID 中包含输入的字符的所有用户的列表。单击以选择某个用户并返回到 "Change User Password" 页。**

4. **输入并确认新的密码信息，然后单击“更改密码”以更改所列资源帐户的用户密码。Identity Manager 将显示工作流程图，该图显示了执行密码更改操作的顺序。**

重设用户密码

重设 Identity Manager 用户帐户密码的过程与更改过程类似。重设过程与密码更改过程的不同之处为重设过程不需要您指定新密码。而是由 Identity Manager 为用户帐户、资源帐户或这些帐户的组合随机生成新密码（根据您的选择和密码策略）。

分配给用户的策略（无论是直接分配还是通过用户的组织分配）控制多个重设选项，其中包括：

- 禁用重设前允许的密码重设频率
- 新密码的显示或发送位置

  根据为角色选择的“重设通知选项”，Identity Manager 以电子邮件方式将新密码发送给相应用户，或（在“结果”页中）将新密码显示给请求重设密码的 Identity Manager 管理员。

▼ 从“用户列表”页中重设密码

“用户列表”页（“帐户”>“列出帐户”）中提供了“重设密码”用户操作。

要从“用户列表”页中重设密码，请执行以下步骤：

1. **在管理员界面中，单击主菜单中的“帐户”。将在“列出帐户”选项卡中显示“用户列表”页。**
2. **选择一个用户，然后单击“用户操作”下拉菜单。**
3. **要重设密码，请选择“重设密码”。**
   将打开“重设用户密码”页。
4. **单击“重设密码”按钮。**

▼ 使用 Identity Manager 帐户策略使密码到期

默认情况下，重设用户密码时，它便会立即到期。因此，用户在重设密码后首次登录时，必须选择新密码才能进行访问。可以编辑“重设用户密码”表单覆盖此默认值，以使用户密码的到期日期取决于与该用户关联的 Identity Manager 帐户策略中设置的密码到期策略。

可以使用以下过程覆盖默认密码更改要求：

1. **编辑“重设用户密码”表单，并将以下值设置为** `false`。

   ```
   resourceAccounts.currentResourceAccounts[Lighthouse].expirePassword
   ```

2. **使用 Identity Manager 帐户策略中的“重设选项”指定密码的到期时间。**
   这些设置包括：

   - **永久**。重设密码时，Identity Manager 使用在 `passwordExpiry` 策略属性中指定的时间段计算当前日期的相对日期，然后将此日期设置为用户的密码到期日期。如果没有指定值，则更改或重设的密码将永不到期。
   - **临时**。重设密码时，Identity Manager 使用在 `tempPasswordExpiry` 策略属性中指定的时间段计算当前日期的相对日期，然后将此日期设置为用户的密码到期日期。如果没有指定值，则更改或重设的密码将永不到期。如果将 `tempPasswordExpiry` 的值设置为 0，则密码立即到期。

     `tempPasswordExpiry` 属性仅适用于重设密码（随机更改）的情况。它不适用于密码更改。

禁用、启用和解除锁定用户帐户

本节介绍了如何禁用和启用 Identity Manager 用户帐户。还介绍了如何帮助已锁定 Identity Manager 帐户的用户解除锁定。

▼ 禁用用户帐户

在禁用用户帐户时，将会更改该帐户，以使用户无法再登录到 Identity Manager 或为其分配的资源帐户。

请注意，管理员可以从管理员界面中禁用用户帐户，但无法锁定用户帐户。仅当用户超过了 Identity Manager 帐户策略定义的允许的失败登录尝试次数时，才会将帐户锁定。

注 – 如果分配的资源没有为帐户禁用提供本机支持，但支持密码更改，则可以将 Identity Manager 配置为通过分配随机生成的新密码来禁用该资源上的用户帐户。

可以使用以下步骤确保此功能正常工作：

1. **在编辑资源向导中打开“Identity System 参数”页。（有关如何打开该向导的说明，请参见第 143 页中的“管理资源”。）**

2. **在“帐户功能配置”表中，确保“密码”功能和“禁用”功能的“是否禁用？”列中没有复选标记。（要显示“禁用”功能，请选择“显示全部功能”。）**

   如果“禁用”功能的“是否禁用？”列中带有复选标记，则无法禁用资源中的帐户。

更多信息

禁用单个用户帐户

要禁用用户帐户，请在“用户列表”中选择该帐户，然后从“用户操作”下拉菜单中选择“禁用”。

在显示的“禁用”页中，选择要禁用的资源帐户，然后单击“确定”。Identity Manager 将显示禁用 Identity Manager 用户帐户以及所有关联资源帐户的结果。此帐户列表指示用户帐户已禁用。

禁用多个用户帐户

可以同时禁用两个或更多 Identity Manager 用户帐户。在列表中选择多个用户帐户，然后从“用户操作”列表中选择“禁用”。

注 – 如果选择禁用多个用户帐户，则无法从每个用户帐户单独选择已分配的资源帐户。此过程会禁用所有选定用户帐户上的所有资源。

▼ 通过密码重设启用资源上的用户帐户

用户帐户的启用过程与禁用过程相反。

根据选定的通知选项，Identity Manager 还会在管理员的结果页中显示密码。

然后用户可以重设自己的密码（通过验证进程），具有管理员权限的用户也可以重设该密码。

注 – 如果分配的资源没有为帐户启用提供本机支持，但支持密码更改，则可以将 Identity Manager 配置为通过密码重设启用该资源上的用户帐户。

要确保此功能正常工作，请执行以下操作：

---

1. **在编辑资源向导中打开“Identity System 参数”页。（有关如何打开该向导的说明，请参见第 143 页中的“管理资源”。）**

2. **在“帐户功能配置”表中，确保“密码”功能和“启用”功能的“是否禁用？”列中没有复选标记。（要显示“启用”功能，请选择“显示全部功能”。）**

   如果“启用”功能的“是否禁用？”列中带有复选标记，则无法启用资源中的帐户。

更多信息

启用单个用户帐户

要启用用户帐户，请在列表中选择此帐户，然后在 "User Actions" 列表中选择 "Enable"。

在显示的“启用”页中，选择要启用的资源，然后单击“确定”。Identity Manager 将显示启用 Identity Manager 帐户以及所有关联资源帐户的结果。

启用多个用户帐户

可以同时启用两个或更多 Identity Manager 用户帐户。在列表中选择多个用户帐户，然后在 "User Actions" 列表中选择 "Enable"。

注 – 如果选择启用多个用户帐户，则无法从每个用户帐户单独选择已分配的资源帐户。此过程会启用所有选定用户帐户上的所有资源。

解除锁定用户帐户

如果用户无法登录到 Identity Manager，则将被锁定。要将用户锁定，用户必须超过 Identity Manager 帐户策略定义的允许的失败登录尝试次数。

注 – 在 Identity Manager 锁定次数中，仅计算 Identity Manager 用户界面上的登录尝试次数（即，管理员界面、最终用户界面、命令行界面或 SPML API 界面）。不会计入资源帐户上的登录失败尝试，这些尝试不会导致用户锁定其 Identity Manager 帐户。

Identity Manager 帐户策略可设定所允许的密码或提问式登录失败尝试的最大次数。

- 如果用户超过了密码登录失败尝试的最大次数，则系统会在所有 Identity Manager 应用程序界面中将其锁定，其中包括“忘记密码”界面。

- 如果用户超过了提问式登录失败尝试的最大次数，仍可以在任何 Identity Manager 应用程序界面中进行验证，但“忘记密码”界面除外。

密码登录尝试失败

如果用户由于失败的密码登录尝试次数过多而在 Identity Manager 中锁定，则在管理员解除锁定该帐户或者锁定到期之前，用户将无法进行登录。

- 如果管理员具有用户的成员组织的管理控制权以及**解除锁定用户**权能，则可以解除锁定帐户。
- 如果在 Identity Manager 帐户策略中设置了**锁定超时**值，则对帐户的锁定最终会到期。密码登录失败尝试的**锁定超时**值是“由失败的密码登录创建的帐户锁定到期时间”值设置的。

提问式登录尝试失败

如果用户由于失败的提问式登录尝试次数过多而在“忘记密码”界面中锁定，则在管理员解除锁定该帐户，锁定的用户（或具有相同权能的用户）更改或重设其密码或者锁定到期之前，用户将无法登录到该界面。

- 如果管理员具有用户的成员组织的管理控制权以及**解除锁定用户**权能，则可以解除锁定帐户。
- 如果在 Identity Manager 帐户策略中设置了**锁定超时**值，则对帐户的锁定最终会到期。提问式登录失败尝试的**锁定超时**值是“由失败的提问式登录创建的帐户锁定到期时间”值设置的。

具有相应权能的管理员可以对处于锁定状态的用户执行以下操作：

- 更新（包括资源重新置备）
- 更改或重设密码
- 禁用或启用
- 重命名
- 解除锁定

要解除锁定帐户，请在列表中选择一个或多个用户帐户，然后在“用户操作”或“组织操作”列表中选择“解除锁定用户”。

批量帐户操作

可以对 Identity Manager 帐户执行若干**批量**操作，这样您便可以同时对多个帐户进行操作。

可以启动以下批量操作：

- **删除**。删除、取消分配选定的资源帐户和解除这些帐户的链接。选择“以 Identity Manager 帐户为目标”选项还会删除每个用户的 Identity Manager 帐户。
- **删除和解除链接**。删除任意选定的资源帐户并解除这些帐户与用户的链接。
- **禁用**。禁用任意选定的资源帐户。选择“以 Identity Manager 帐户为目标”选项还会禁用每个用户的 Identity Manager 帐户。
- **启用**。启用任意选定的资源帐户。选择“以 Identity Manager 帐户为目标”选项将启用每个用户的 Identity Manager 帐户。
- **取消分配，解除链接**。解除任意选定的资源帐户的链接，并删除为这些资源分配的 Identity Manager 用户帐户。取消分配并不从资源删除帐户。不能取消分配已通过角色或资源组间接分配给 Identity Manager 用户的帐户。
- **解除链接**。删除资源帐户与 Identity Manager 用户帐户的关联（链接）。取消链接并不从资源中删除帐户。如果将通过角色或资源组间接分配给 Identity Manager 用户的帐户取消链接，则该链接会在更新用户时恢复。

如果在文件或应用程序（如电子邮件客户机或电子表格程序）中有一个用户列表，则批量操作将发挥最佳功能。可将上述列表复制并粘贴到此界面页的一个字段中，也可从文件加载这个用户列表。

这些操作中的许多操作都可对某个用户搜索的结果执行。可以使用“查找用户”页（“帐户”→“查找用户”）来搜索用户。

当任务完成后显示任务结果时，可通过单击“下载 CSV”将批量帐户操作的结果保存为 CSV 文件。

启动批量帐户操作

▼ 启动批量帐户操作

1. **在管理员界面中，单击主菜单中的“帐户”。**
2. **单击次级菜单中的“启动批量操作”。**
3. **填写表单，然后单击“启动”。**

   Identity Manager 将启动后台任务以执行批量操作。

   要监视批量操作任务的状态，请单击主菜单中的“服务器任务”，然后单击“所有任务”。

使用操作列表

可使用逗号分隔值 (CSV) 格式指定批量操作列表。这样您便可在单个操作列表中混合各种不同的操作类型。此外，可指定更复杂的创建和更新操作。

CSV 格式由两个或多个输入行组成。每一行由逗号分隔的值列表组成。第一行包含字段名称。其余的每一行都对应于要对 Identity Manager 用户和/或该用户的资源帐户执行的操作。每一行都应包含相同个数的值。空值将保持相应字段值不变。

任何批量操作 CSV 输入中都必需有这两个字段：

- **user**。包含 Identity Manager 用户的名称。
- **command**。包含对 Identity Manager 用户执行的操作。有效命令有：
  - **Delete**。对资源帐户和/或 Identity Manager 帐户执行删除、取消分配和解除链接操作。
  - **DeleteAndUnlink**。删除资源帐户并将其解除链接。
  - **Disable**。禁用资源帐户和/或 Identity Manager 帐户。
  - **Enable**。启用资源帐户和/或 Identity Manager 帐户。
  - **Unassign**。取消分配资源帐户并解除其链接。
  - **Unlink**。将资源帐户解除链接。
  - **Create**。创建 Identity Manager 帐户。（可选）创建资源帐户。
  - **Update**。更新 Identity Manager 帐户。（可选）创建、更新或删除资源帐户。
  - **CreateOrUpdate**。如果 Identity Manager 帐户尚不存在，则执行创建操作。否则执行更新操作。

Delete、DeleteAndUnlink、Disable、Enable、Unassign 和 Unlink 命令

如果您要执行 Delete、DeleteAndUnlink、Disable、Enable、Unassign 或 Unlink 操作，则需要指定的唯一附加字段是 resources。使用 resources 字段指定哪些资源上的哪些帐户将受到影响。

“资源”字段可能具有以下值：

- **all**。处理所有资源帐户，其中包括 Identity Manager 帐户。
- **resonly**。处理除 Identity Manager 帐户之外的所有资源帐户。
- *resource_name* [| *resource_name* ...]. 处理指定的资源帐户。指定 Identity Manager 以处理 Identity Manager 帐户。

下面是这些操作中几个操作的 CSV 格式的示例：

```
command,user,resources
Delete,John Doe,all
Disable,Jane Doe,resonly
Enable,Henry Smith,Identity Manager
Unlink,Jill Smith,Windows Active Directory|Solaris Server
```

Create、Update 和 CreateOrUpdate 命令

如果您要执行 Create、Update 或 CreateOrUpdate 命令，则除了 user 和 command 字段之外，还可指定“用户视图”中的字段。使用的字段名称是视图中属性的路径表达式。有关“用户视图”中提供的属性的信息，请参见《Sun Identity Manager Deployment Reference》中的“User View Attributes”。如果您正使用自定义“用户表单”，则该表单中的字段名称包含您可使用的一些路径表达式。

在批量操作中使用的一些较常见的路径表达式有：

- **waveset.roles**。要分配给 Identity Manager 帐户的一个或多个角色名称的列表。
- **waveset.resources**。要分配给 Identity Manager 帐户的一个或多个资源名称的列表。
- **waveset.applications**。要分配给 Identity Manager 帐户的一个或多个角色名称的列表。
- **waveset.organization**。用来放置 Identity Manager 帐户的组织的名称。
- **accounts**[*resource_name*].*attribute_name*。资源帐户属性。属性的名称在资源的模式中列出。

以下示例展示了创建和更新操作的 CSV 格式：

```
command,user,waveset.resources,password.password,
password.confirmPassword,accounts[Windows Active Directory].description,
accounts[Corporate Directory].location Create,John Doe,
Windows Active Directory|Solaris Server,changeit,changeit,John Doe - 888-555-5555,
Create,Jane Smith,Corporate Directory,changeit,changeit,,New York
CreateOrUpdate,Bill Jones,,,,,California
```

通过使用 `CreateOrUpdate` 命令，您可以在支持多种帐户类型的资源上指定特定的帐户类型。因此，如果某个用户在特定资源上拥有多个帐户，并且每个帐户的帐户类型各不相同，则可按照以下示例进行操作，该示例显示了如何更新 `userAye` 用户的**管理员**帐户类型：

```
command,user,accounts[Sim1|admin].emailAddress
CreateOrUpdate,userAye,bbye8@example.com
```

注 –

尽管可使用 `CreateOrUpdate` 命令为用户的各个帐户设置特定于帐户的属性，但请注意，用户视图全局部分中的以下值将会应用于**所有**指定的帐户：

- `accountId`
- `email`
- `password`
- `disable`
- 所有扩展属性

因此，以下形式的 BulkOps 命令**可能**不会执行预期的操作。

```
command,user,accounts[Sim1].email
CreateOrUpdate,userAye,bbye8@example.com
```

如果 userAye 已具有一个 email 值，则会将该值应用于 Sim1 资源上的 email 属性。没有任何方法可以改变此行为。

有多个值的字段

某些字段可以有多个值。这些字段称为多值字段。例如，waveset.resources 字段可用于为一个用户分配多个资源。可以使用竖线 (|) 字符（也称为“管道”字符）分隔字段中的多个值。可以按如下方法指定多值的语法：

```
value0 | value1 [ | value2 ... ]
```

更新现有用户的多值字段时，您可能并不希望使用一个或多个新值替换当前字段值。您可能要删除一些值或添加一些值至当前值。可以使用字段指令指定如何处理现有字段的值。字段指令在字段值之前，并且由竖线字符包围，如下所示：

```
|directive [ ; directive ] | field values
```

您可选择下列指令：

- **Replace**。用指定值替换当前值。如果没有指定指令（或只指定 List 指令），则此指令为默认指令。
- **Merge**。将指定值添加到当前值中。重复的值将被过滤掉。
- **Remove**。从当前值中删除指定值。
- **List**。即使字段只有一个值，也强制按照有多个值的方式处理它的值。因为对多数字段而言，无论有多少个字段值，都能正确处理这些值，因此该指令并不常用。此指令是唯一可用另一个指令指定的指令。

注 – 字段值区分大小写。指定 Merge 和 Remove 指令时，这一点很重要。进行合并时，值必须完全匹配才能正确将其删除或避免有多个相似的值。

字段值中的特殊字符

如果字段值中包含逗号 (,) 或双引号 (") 字符，或者要保留前导或结尾空格，则必须将字段值用一对双引号引起来 ("field_value")。这样就需要将字段值中的双引号替换为两个双引号 (") 字符。例如，"John ""Johnny"" Smith" 的字段值为 John "Johnny" Smith。

如果字段值中包含竖线 (|) 或反斜杠 (\) 字符，则必须前置一个反斜杠（\| **或** \\）。

批量操作视图属性

执行 Create、Update 或 CreateOrUpdate 操作时，"User View" 中有一些只在批量操作处理过程中使用或可用的附加属性。可在“用户表单”中引用这些属性，以提供批量操作的特定性能。

这些属性如下所列：

- `waveset.bulk.fields.`*field_name* 属性；这些属性包含从 CSV 输入中读入的字段值，其中 *field_name* 是字段名称。例如，command 和 user 字段分别在带有路径表达式 `waveset.bulk.fields.command` 和 `waveset.bulk.fields.user` 的属性中。
- `waveset.bulk.fieldDirectives.`*field_name* 属性；只对那些指定了指令的字段定义这些属性。值为指令字符串。
- `waveset.bulk.abort` 布尔型属性；将该属性设置为 true 可中止当前操作。
- `waveset.bulk.abortMessage` 属性；将该属性设置为消息字符串，当 `waveset.bulk.abort` 设置为 true 时，将显示该消息字符串。如果未设置此属性，将显示一条普通中止消息。

关联和确认规则

当没有可用的 Identity Manager 用户名放在操作的 user 字段时，请使用关联和确认规则。如果没有为用户字段指定值，则必须在启动批量操作时指定关联规则。如果确实为用户字段指定了值，则不会针对该操作评估关联和确认规则。

关联规则查找匹配操作字段的 Identity Manager 用户。确认规则根据操作字段测试 Identity Manager 用户，以确定用户是否匹配。此两阶段式方法允许 Identity Manager 通过快速查找可能的用户（基于名称或属性）并仅针对可能的用户执行繁琐的检查，以优化关联过程。

分别创建子类型为 `SUBTYPE_ACCOUNT_CORRELATION_RULE` 或 `SUBTYPE_ACCOUNT_CONFIRMATION_RULE` 的规则对象，以创建关联或确认规则。

有关关联规则和确认规则的详细信息，请参见《Sun Identity Manager Deployment Guide》中的第 3 章 “Data Loading and Synchronization”。

关联规则

为任意关联规则输入的内容是操作字段的映射。输出必须是下列内容之一：

- 字符串（包含用户名或用户 ID）
- 字符串元素列表（每个元素为用户名或用户 ID）
- `WSAttribute` 元素列表
- `AttributeCondition` 元素列表

常用关联规则会根据操作字段中的值生成用户名列表。关联规则还会生成用于选择用户的属性条件（参考 `Type.USER` 的可查询属性）的列表。

关联规则的处理过程应相对简便，但应尽可能缩小范围。如有可能，将繁琐的处理过程转给确认规则。

属性条件必须参考 Type.USER 的可查询属性。这些属性是在名为 IDM **模式配置**的 Identity Manager 配置对象中配置的。

关联扩展属性需要特殊配置：

必须将扩展属性指定为可查询属性。

▼ 将扩展属性设置为可查询属性

1. **打开 IDM 模式配置。您必须具有 IDM 模式配置权能才能查看或编辑 IDM 模式配置。**
2. **找到 <IDMObjectClassConfiguration name='User'> 元素。**
3. **找到 <IDMObjectClassAttributeConfiguration name=' xyz '> 元素，其中 xyz 是要设置为可查询属性的属性名称。**
4. **设置 queryable='true'**
   在第 74 页中的 "关联规则"中，将 email 扩展属性定义为可查询属性。

示例 3–1 将 Email 扩展属性定义为可查询属性的 XML 代码摘录

```
<IDMSchemaConfiguration>
  <IDMAttributeConfigurations>
    <IDMAttributeConfiguration name='email' syntax='STRING'/>
    </IDMAttributeConfiguration>
  </IDMAttributeConfigurations>
  <IDMObjectClassConfigurations>
    <IDMObjectClassConfiguration name='User' extends='Principal' description='User description'>
      <IDMObjectClassAttributeConfiguration name='email' queryable='true'/>
    </IDMObjectClassConfiguration>
  </IDMObjectClassConfigurations>
 </IDMSchemaConfiguration>
```

您必须重新启动 Identity Manager 应用程序（或应用服务器）以使 IDM **模式配置**更改生效。

确认规则

任意确认规则的输入如下：

- 使用 userview 以获取 Identity Manager 用户的完整视图。
- 使用 account 以获取操作字段的映射。

如果用户与操作字段匹配，则确认规则会返回字符串形式的布尔值 true；否则，它会返回值 false。

典型的确认规则会将用户视图的内部值与操作字段的值比较。作为关联进程的可选第二阶段，确认规则执行不能在关联规则中表达的检查（或关联规则中因太昂贵而不能评估的检查）。

总之，只有在下列情况下才需要确认规则：

- 关联规则可能返回多个匹配用户。
- 必须比较的用户值不可查询。

为关联规则返回的每个匹配用户运行一次确认规则。

管理帐户安全和权限

本节讨论了您可以执行哪些操作来提供用户帐户的安全访问并管理 Identity Manager 中的用户权限。

- 第 76 页中的 “设置密码策略”
- 第 79 页中的 “用户验证”
- 第 83 页中的 “分配管理权限”

设置密码策略

资源密码策略建立对密码的限制。强大的密码策略可提供增强的安全性，从而有助于保护资源不会遭受未经授权的登录尝试。可以编辑密码策略来设置或选择一定范围的特征值。

要开始使用密码策略，请单击主菜单中的“安全性”，然后单击“策略”。

要编辑密码策略，请在“策略”列表中单击该策略。要创建密码策略，请在 "New" 选项列表中选择 "String Quality Policy"。

注 – 有关策略的详细信息，请参见第 87 页中的 “配置 Identity Manager 策略”。

创建策略

密码策略是字符串质量策略的默认类型。在命名新策略并提供可选描述后，请为定义新策略的规则选择选项和参数。

长度规则

长度规则设置密码所需字符长度的最小值和最大值。选择此选项以启用规则，然后为规则输入限制值。

策略类型

选择策略类型按钮之一。如果选择“其他”选项，则必须在提供的文本字段中输入该类型。

字符类型规则

字符类型规则确定密码中可以包括的某些类型字符和数字的最少数量和最多数量。

其中包括：

- 字母、数字、大写、小写和特殊字符的最少数量和最多数量
- 嵌入的数字字符的最少数量和最多数量
- 重复字符和顺序字符的最多数量
- 开始字母和数字字符的最少数量

为每个字符类型规则输入一个数字限制值；或者输入 "All" 指示所有字符必须都是该类型字符。

字符类型规则的最小数目

还可以设置必须通过验证的字符类型规则的最小数目，如图 3–7 中所示。必须通过的最小数量是 1。最大数量不能超过您启用的字符类型规则数。

注 – 要将必须通过的最小数量设置为最高值，请输入 "All"。

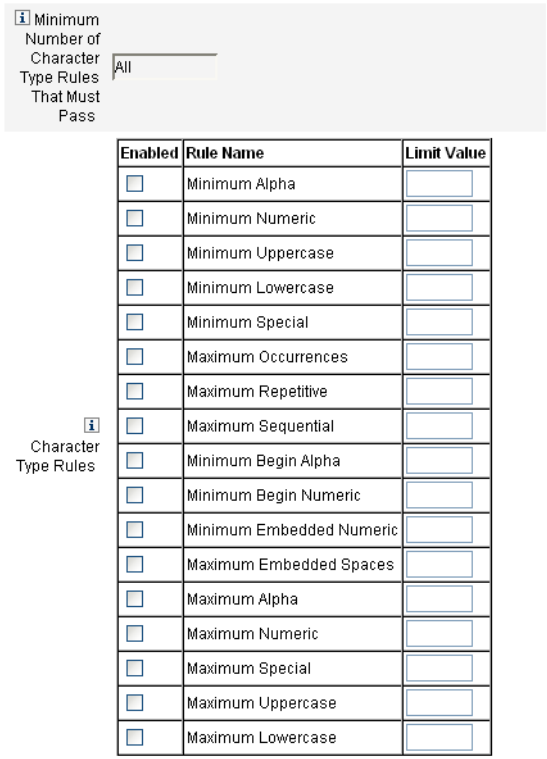


图 3–7 密码策略（字符类型）规则

字典策略选项

可以选择根据字典中的词语检查密码，以防范简单的字典攻击。

在能够使用此选项之前，您必须：

- 配置字典
- 加载字典的词

从 "Policies" 页配置字典。有关如何设置字典的详细信息，请参见第 90 页中的 “什么是字典策略？ ”。

密码历史记录策略

可以禁止再次使用直接在新选密码之前使用的密码。

在 "Number of Previous Passwords that Cannot be Reused" 字段中，输入一个大于 1 的数字，以禁止再次使用当前和先前密码。例如，如果输入数值 3，新密码就不能与当前密码或直接在当前密码之前使用的两个密码相同。

您也可禁止再次使用先前密码中使用过的类似字符。在 "Maximum Number of Similar Characters from Previous Passwords that Cannot be Reused" 字段中，输入不能在新密码中重复使用的一个或多个先前密码中的连续字符数。例如，如果输入了值 7，且先前密码为 password1，则新密码不能为 password2 或 password3。

如果输入了值 0，则无论顺序如何，所有字符都不得相同。例如，如果先前密码为 abcd，则新密码不能包含字符 a、b、c 或 d。

此规则可应用于一个或多个先前密码。检查的先前密码的数量是“不能再次使用的先前密码数”字段中指定的数量。

不得包含词

可输入一个或多个密码不能包含的词。在输入框中，每行输入一个词。

还可以通过配置和实现字典策略排除词。有关详细信息，请参见第 90 页中的 “什么是字典策略？ ”。

不得包含属性

可以输入一个或多个密码不能包含的属性。

您可以指定以下属性：

- `accountID`
- `email`
- `firstname`
- `fullname`
- `lastname`

可在 `UserUIConfig` 配置对象中更改密码“不得包含”属性允许的设置。有关详细信息，请参见第 90 页中的 “策略中不得包含属性”。

实现密码策略

密码策略是为每个资源建立的。要将某个密码策略应用于指定资源，请从“密码策略”选项列表中选择它，“密码策略”选项列表位于“创建/编辑资源向导：Identity Manager 参数”页的“策略配置”区域中。

用户验证

如果用户忘记了密码或重设了密码，该用户可通过回答一个或多个帐户验证问题来获得访问 Identity Manager 的权限。这些问题以及管理这些问题的规则是 Identity Manager 帐户策略的一部分，由您来设定。与密码策略不同，Identity Manager 帐户策略直接分配给用户或者通过分配给用户的组织分配给用户（在“创建用户”页和“编辑用户”页中）。

▼ 在帐户策略中设置验证

1 **单击主菜单中的“安全性”，然后单击“策略”。**

2 **从策略列表中选择“默认 Identity Manager 帐户策略”。**

验证选项位于该页的 "Secondary Authentication Policy Options" 区域中。

要点！首次设置时，用户应登录到“用户界面”并提供对验证问题的初始答案。如果不设置这些问题，用户必须使用密码才能成功登录。

验证问题策略决定了用户执行以下操作时所发生的情况：在登录页上单击“忘记密码？”按钮或访问“更改我的回答”页。第 79 页中的 “用户验证”介绍了其中的每个选项。

选项	描述
所有	要求用户回答所有策略定义的问题以及个性化问题。
任何	Identity Manager 将显示所有策略定义的问题以及个性化问题。必须指定用户必须回答的问题数量。
下一步	要求用户在首次登录时回答所有可能的策略定义问题。 如果用户在登录期间单击“忘记密码？”按钮，Identity Manager 将显示第一个问题。如果用户的回答不正确，Identity Manager 将显示下一个问题，直至用户正确回答了验证问题并登录，否则根据指定的失败尝试次数限制将其锁定。此策略不支持用户生成的问题。
随机	允许管理员指定用户必须回答的问题数。Identity Manager 将从策略中定义的问题以及用户定义的问题列表中随机选择并显示指定数量的问题。用户必须回答所有显示的问题。
循环	Identity Manager 从配置的问题列表中选择下一个问题，并将此问题分配给用户。为第一个用户分配验证问题列表中的第一个问题，为第二个用户分配第二个问题。此模式会一直持续下去，直至用户数超出问题数。此时，会按顺序依次将问题分配给用户。例如，如果共有 10 个问题，则将为第 11 个和第 21 个用户分配第一个问题。 仅显示选定的问题。如果您希望用户每次回答不同的问题，则需要使用“随机”策略，并将问题数设置为 1。 用户无法定义自己的验证问题。有关此功能的详细信息，请参见第 81 页中的 “个性化验证问题”。

可以检验您的验证选择，方法是：登录到 Identity Manager 用户界面，单击“忘记密码？”按钮，并回答显示的一个或多个问题。

图 3–8 显示了“用户帐户验证”屏幕的示例。

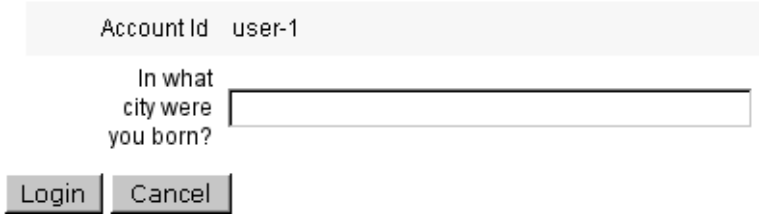


图 3–8 User Account Authentication

个性化验证问题

在 Identity Manager 帐户策略中，您可以选择一个选项，以允许用户在用户界面和管理员界面中提供自己的验证问题。此外，可以设置用户必须提供并回答的最小问题数以便使用个性化的验证问题成功登录。

然后用户可以在 "Change Answers to Authentication Questions" 页添加和更改问题。图 3–9 显示了此页的示例。

图 3–9 更改答案：个性化验证问题

验证后忽略更改密码质询

用户回答一个或多个问题成功通过验证后，默认情况下，系统会要求该用户提供一个新密码。但是，可以通过为一个或多个 Identity Manager 应用程序设置 `bypassChangePassword` 系统配置属性，来配置 Identity Manager 忽略更改密码质询。

有关编辑系统配置对象的说明，请参见第 102 页中的 “编辑 Identity Manager 配置对象”。

要在成功验证后忽略所有应用程序的更改密码质询，请在系统配置对象中将 bypassChangePassword 属性设置如下：

示例 3–2 设置属性以忽略更改密码质询

```
<Attribute name="ui"
 <Object>
   <Attribute name="web">
     <Object>
       <Attribute name='questionLogin'>
         <Object>
           <Attribute name='bypassChangePassword'>
             <Boolean>true</Boolean>
           </Attribute>
         </Object>
       </Attribute>
   ...
 </Object>
...
```

要对特定应用程序禁用此密码质询，请将其设置如下：

示例 3–3 设置属性以禁用更改密码质询

```
<Attribute name="ui">
  <Object>
    <Attribute name="web">
      <Object>
        <Attribute name='user'>
          <Object>
            <Attribute name='questionLogin'>
              <Object>
                <Attribute name='bypassChangePassword'>
                  <Boolean>true</Boolean>
                </Attribute>
              </Object>
            </Attribute>
          </Object>
        </Attribute>
      ...
  </Object>
...
```

分配管理权限

可以将 Identity Manager 管理权限或权能分配给用户，如下所述：

- 管理员角色。分配了管理员角色的用户继承由角色定义的权能和受控组织。默认情况下，所有 Identity Manager 用户帐户在创建后都将分配**用户管理员角色**。有关管理员角色和创建管理员角色的详细信息，请参见第 5 章，角色和资源中的第 136 页中的“了解和管理 Identity Manager 资源”。
- 权能。权能是由规则定义的。Identity Manager 提供了一系列权能，这些权能按照功能分为几个组，您可以从中进行选择。分配权能可以更为细化地分配管理权限。有关权能和创建权能的信息，请参见第 6 章，管理中的第 184 页中的“了解和管理权能”。
- 受控组织。受控组织授予对指定组织的管理控制权限。有关详细信息，请参见第 6 章，管理中的第 178 页中的“了解 Identity Manager 组织”。

有关 Identity Manager 管理员和管理职责的详细信息，请参见第 6 章，管理。

用户自行搜索

最终用户可以使用 Identity Manager 最终用户界面**搜索**资源帐户。这意味着拥有 Identity Manager 身份的用户可以与现有的但未关联的资源帐户相关联。

启用自行搜索

要启用自行搜索，必须编辑特殊配置对象（最终用户资源），然后将允许用户在其中搜索帐户的每个资源的名称添加到该对象中。

▼ 启用自行搜索

1. **编辑“最终用户资源”配置对象。**

   有关编辑 Identity Manager 配置对象的说明，请参见第 102 页中的“编辑 Identity Manager 配置对象”。

2. **添加 `<String>`*Resource*`</String>`，其中 *Resource* 与系统信息库中的资源对象的名称相匹配，如图 3–10 中所示。**

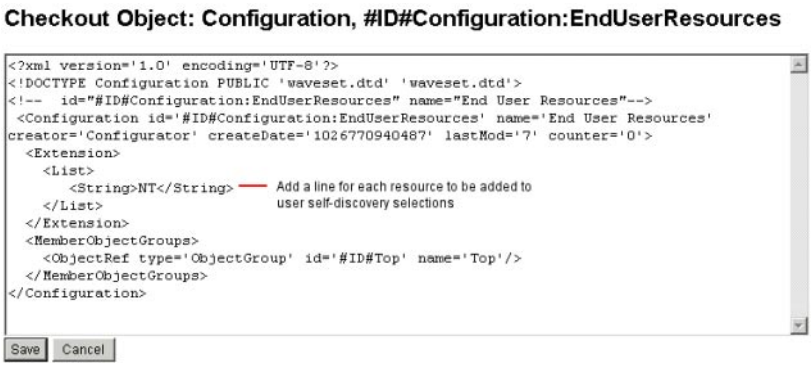


图 3–10 最终用户资源配置对象

3 **单击“保存”。**

启用自行搜索后，将在 Identity Manager 用户界面的“配置文件”菜单选项卡下向用户显示一个新的选择区域（自行搜索）。用户可以使用该区域从可用列表中选择资源，然后输入资源帐户 ID 和密码，将此帐户与其 Identity Manager 身份链接。

注 – 要为最终用户授予 Identity Manager 配置对象的访问权限，管理员还可以使用“最终用户”组织。有关详细信息，请参见第 197 页中的 “最终用户组织”。

匿名注册

匿名注册功能允许无 Identity Manager 帐户的用户通过请求获得此帐户。

启用匿名注册

默认情况下将禁用匿名注册功能。

▼ 启用匿名注册功能

1 **在管理员界面中，单击“配置”，然后单击“用户界面”。**

2 **在“匿名注册”区域中选择“启用”选项，然后单击“保存”。**

当用户登录到用户界面时，登录页将显示“初次登录的用户？”文本，然后显示“请求帐户”链接。

注 – 可以对“初次登录的用户？请求帐户”文本进行自定义。有关详细信息，请参见《Sun Identity Manager Deployment Guide》。

图 3–11 启用了“请求帐户”链接的用户界面页

配置匿名注册

在“用户界面”页的“匿名注册”区域中，可以为匿名注册过程配置以下选项：

- **通知模板**。指定电子邮件模板的 ID，此模板用于将通知发送给请求帐户的用户。
- **要求隐私政策**。如果选择了该选项，则用户必须接受隐私政策，然后才能请求帐户。默认情况下将启用此选项。
- **启用验证**。如果选择了该选项，则用户必须验证其人事任用情况，然后才能请求帐户。默认情况下将启用此选项。
- **进程启动 URL**。输入 URL 以指定用于匿名注册进程的工作流。
- **启用通知**。如果选择了该选项，则会在创建用户的帐户后将通知电子邮件发送给用户。
- **电子邮件域**。输入用于构建用户电子邮件地址的电子邮件域的名称。

完成后请单击“保存”。

用户注册过程

当用户登录到用户界面时，可通过单击登录页上的“请求帐户”来请求帐户。

Identity Manager 将显示第一个注册页面（共两页），该页面要求提供姓名和雇员 ID。如果将“启用验证”属性设置为 yes（默认值），则必须先验证此信息，用户才能进入下一页。

`EndUserLibrary` 中的 `verifyFirstname`、`verifyLastname`、`verifyEmployeeId` 和 `verifyEligibility` 规则可验证每个属性的信息。

注 – 您可能需要修改上述一个或多个规则。尤其是，您应该修改验证雇员 ID 的规则，以使用 Web 服务调用或 Java 类验证此信息。

如果禁用“启用验证”属性，则不会显示初始注册页面。在这种情况下，您必须修改“最终用户匿名注册完成”表单，以允许用户输入通常被初始验证表单捕获的信息。

使用注册页面上提供的信息，Identity Manager 可以生成以下内容：

- 帐户 ID（遵循名字首大写字母、姓氏首大写字母和雇员 ID 的约定）。
- 使用以下格式的电子邮件地址：

  FirstName. *LastName*@*EmailDomain*

  其中 *EmailDomain* 是由匿名注册配置中的“电子邮件域”属性所设置的域。
- 管理员属性 (`idmManager`)。可以通过修改 `EndUserRuleLibrary:getIdmManager` 规则设置此属性。默认情况下将管理员设置为配置器。指定为管理员的管理者必须先批准用户请求，然后才能置备其帐户。
- 组织属性。可以通过自定义 `EndUserRuleLibrary:getOrganization` 规则设置此属性。默认情况下，会将用户分配到组织分层结构的顶层 ("Top")。

如果用户在注册页面上所提供的信息经验证是正确的，Identity Manager 将向用户显示第二个注册页面。用户必须在此处输入密码和密码确认。如果将“需要隐私策略”属性设置为 yes，用户还必须选择相应选项以接受隐私策略的条款。

当用户单击“注册”时，Identity Manager 将显示确认页面。如果将“启用通知”属性设置为 yes，则页面会指出用户将在创建帐户后收到电子邮件通知。

标准的创建用户过程（包括 `idmManager` 属性和策略设置所需的批准）完成之后，将创建帐户。

◆ ◆ ◆ 第 4 章

配置业务管理对象

本章提供了使用管理员界面设置和维护 Identity Manager 对象的信息和过程。有关 Identity Manager 对象的详细信息，请参见“概述”一章中的第 26 页中的 “Identity Manager 对象”。

注 – 有关为服务提供者实现配置 Identity Manager 的信息，请参见第 17 章，服务提供者管理。

本章按以下主题进行组织：

配置 Identity Manager 策略

阅读本节可以了解有关配置用户策略的信息。

本节包含以下主题：

什么是策略？

Identity Manager 策略通过建立 Identity Manager 帐户 ID、登录和密码特征的约束，对 Identity Manager 用户设置限制。

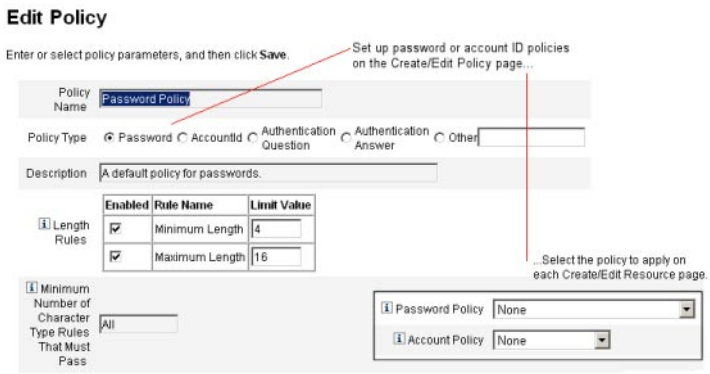
注 – Identity Manager 还提供专用于审计用户遵循性的审计策略。第 13 章，身份审计：基本概念中对审计策略进行了论述。

策略按以下类型分类：

- **Identity System 帐户策略**。建立用户、密码以及验证策略选项和约束。通过“创建组织”和“编辑组织”页以及“创建用户”和“编辑用户”页，可以将 Identity System 帐户策略分配给组织或用户。

  您可以设置或选择以下选项：

  - **用户帐户策略选项**。指定 Identity Manager 在用户不能正确回答验证问题时如何处理用户帐户。
  - **密码策略选项**。设置密码到期日期、到期前的警告时间以及重设选项。
  - **辅助验证策略选项**。确定以何种方式向用户显示验证问题、用户是否可以提供自己的验证问题、是否在登录时强制验证，以及是否建立可以向用户显示的问题库。
- **服务提供者系统帐户策略**。可以在服务提供者实现中使用此策略类型，为服务提供者用户建立用户、密码和验证策略选项和约束。通过“创建组织”和“编辑组织”页以及“创建服务提供者用户”和“编辑服务提供者用户”页，可以将策略分配给组织或用户。
- **字符串质量策略**。包括密码、帐户 ID 和验证等策略类型。可用于设置长度规则、字符类型规则、允许的字词以及属性值。此策略类型绑定到每个 Identity Manager 资源，并在每个资源页上进行设置。下图提供了一个示例。



您可以为密码和帐户 ID 设置以下选项和规则：

- **长度规则**。确定最小和最大长度。
- **字符类型规则**。设置字母、数字、大写、小写、重复和顺序字符的最小和最大允许值。
- **密码重新使用限制**。指定在当前密码之前使用的、不能重新使用的密码的数量。当用户试图更改其密码时，新密码将与密码历史记录进行比较，以确保该密码是唯一密码。出于安全原因，以前密码的数字签名将被保存；而新密码将与此进行比较。
- **禁用的字词和属性值**。指定不能作为 ID 或密码的组成部分使用的字词和属性。

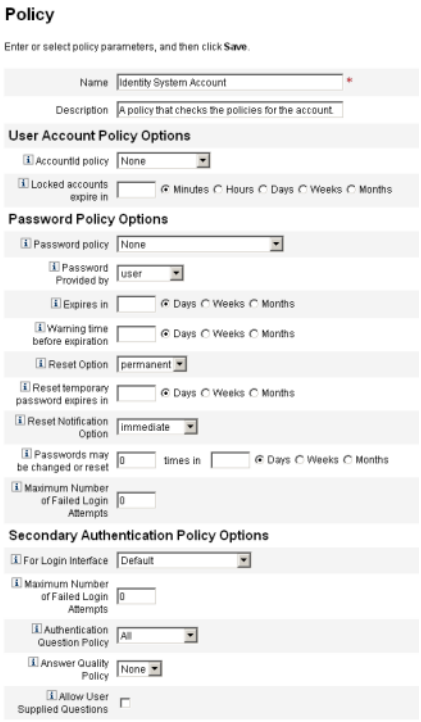
▼ 打开“策略”页

可在“策略”页中创建和编辑 Identity Manager 用户策略。要打开该页，请执行以下步骤：

1 **登录到管理员界面。**

2 **单击“安全性”选项卡，然后单击“策略”子选项卡。**

将打开“策略”页，如下图中所示。



策略中不得包含属性

可在 `UserUIConfig` 配置对象中更改“不得包含”属性允许的设置。

`UserUIConfig` 中列出的属性如下：

- `<PolicyPasswordAttributeNames>` 属性。策略类型“密码”
- `<PolicyAccountAttributeNames>` 属性。策略类型“帐户 ID”
- `<PolicyOtherAttributeNames>` 属性。策略类型“其他”

什么是字典策略？

通过使用字典策略，Identity Manager 可以对照字词数据库检查密码，以确保密码不会受到简单的字典攻击。Identity Manager 通过将此策略与其他策略设置结合使用的方式来强制设定密码的长度和组成，从而使利用字典也很难猜出在系统中生成或更改的密码。

字典策略扩展了能够用该策略进行设置的密码排除列表。（此列表是使用 "Administrator Interface" 密码 "Edit Policy" 页中的 "Must Not Contain Words" 选项实现的。）

▼ 配置字典策略

要设置字典策略，必须：

- 配置字典服务器支持
- 加载字典

1. 按第 89 页中的“打开“策略”页”中所述打开“策略”页。
2. 单击“配置字典”显示“字典配置”页。
3. 选择并输入数据库信息。

   数据库信息包括：

   - **数据库类型**。选择要用于存储字典的数据库类型（Oracle、DB2、SQLServer 或 MySQL）。
   - **主机**。输入正在运行数据库的主机的名称。
   - **用户**。输入要在连接数据库时使用的用户名。
   - **密码**。输入要在连接数据库时使用的密码。
   - **端口**。输入数据库当前侦听的端口。
   - **连接 URL**。输入要在连接时使用的 URL。可使用以下模板变量：
     - %h主机
     - %p端口
     - %d数据库名称

     驱动程序类。输入要在与数据库交互时使用的 JDBC 驱动程序类。
   - **数据库名称**。输入要加载字典的数据库名称。
   - **字典文件名**。输入要在加载字典时使用的文件名。
4. 单击“测试”以测试数据库连接。
5. 如果连接测试成功，请单击“加载词”以加载字典。加载任务可能需要几分钟才能完成。
6. 单击“测试”以确保正确加载字典。

▼ 实现字典策略

可以使用以下步骤来实现字典策略：

1. 按第 89 页中的“打开“策略”页”中所述打开“策略”页。
2. 单击“密码策略”链接以编辑密码策略。
3. 在“编辑策略”页中，选择“根据字典的词检查密码”选项。

4 **单击"保存"以保存更改。**

字典策略实现后，系统会根据字典来检查所有更改的或生成的密码。

自定义电子邮件模板

Identity Manager 使用电子邮件模板将信息和操作请求提交给用户和批准者。本系统包括以下用途的模板：

- **访问查看通知**。发送需要查看用户访问权限的通知。当必须修正或缓解访问策略的违规时，系统发送此通知。
- **帐户创建批准**。向批准者发送通知，告知有新帐户等待其批准。当相关角色的 "Provisioning Notification Option" 设置为批准时，系统发送此通知。
- **帐户创建通知**。发送通知，告知已经用特定角色分配创建了一个帐户。当在"创建角色"或"编辑角色"页的"通知收件人"字段中选择了一个或多个管理员时，系统会发送此通知。
- **帐户删除批准**。向批准者发送通知，告知有用户帐户删除操作等待其批准。当在"创建角色"或"编辑角色"页的"通知收件人"字段中选择了一个或多个管理员时，系统会发送此通知。
- **帐户删除通知**。发送通知，告知已删除帐户。
- **帐户更新通知**。向指定电子邮件地址或用户帐户发送通知，告知已更新帐户。
- **外部资源**。通知外部资源置备程序必须执行置备任务。
- **密码重设**。发送 Identity Manager 密码重设通知。根据为相关 Identity Manager 策略选择的"重设通知选项"值，系统会立即（在 Web 浏览器中）为重设密码的管理员显示通知，或者向密码将被重设的相应用户发送电子邮件。
- **密码同步通知**。通知用户已成功完成对所有资源的密码更改。该通知列出已成功更新哪些资源并指出密码更改请求的来源。
- **密码同步失败通知**。通知用户未成功完成对所有资源的密码更改。该通知提供一个错误列表并指出密码更改请求的来源。
- **策略违规通知**。发送帐户已发生策略违规的通知。
- **协调帐户事件**。协调资源事件、协调摘要。分别从"通知协调响应"、"通知协调启动"和"通知协调完成"默认工作流中调用。通知按照在每个工作流中的配置发送。
- **报告**。向指定的一列收件人发送生成的报告。
- **请求资源**。向资源管理员发送通知，告知某个资源已被请求。当管理员从"资源"区请求资源时，系统会发送此通知。

注 – 自 Identity Manager 8.1 发行版起，不再使用请求资源，而改为使用外部资源。您无法再使用请求适配器来创建新的连接。请改用外部资源适配器。有关详细信息，请参见第 148 页中的“了解和管理外部资源”。

- **重试通知**。向管理员发送通知，告知已对某个资源尝试了指定次数的特定操作，但未成功。
- **风险分析**。发送风险分析报告。当一个或多个电子邮件收件人被指定为资源扫描的组成部分时，系统会发送此报告。
- **临时密码重设**。向用户或角色批准者发送通知，告知已经为帐户提供了临时密码。根据为相关 Identity Manager 策略选择的“密码重设通知选项”值，系统会立即（在 Web 浏览器中）为用户显示通知，发送电子邮件给用户，或者发送电子邮件给角色批准者。
- **用户 ID 恢复**。将已恢复的用户 ID 发送到指定的电子邮件地址。

编辑电子邮件模板

可以通过自定义电子邮件模板为收件人提供具体指导，告诉他如何完成一项任务或如何查看结果。例如，您可能想要通过添加以下消息自定义 "Account Creation Approval" 模板以将批准者引导到帐户批准页：

请转至 `http://host.example.com:8080/idm/approval/approval.jsp` **，以批准** `$(fullname)` **的帐户创建。**

可以使用以下步骤自定义电子邮件模板，这些步骤使用“帐户创建批准”模板作为示例：

▼ 自定义电子邮件模板

1. **在管理员界面中，单击“配置”选项卡，然后单击“电子邮件模板”子选项卡。**
   将打开“电子邮件模板”页。
2. **单击以选择 "Account Creation Approval" 模板。**

图 4–1 编辑电子邮件模板

3 输入模板的详细信息。

您可以输入以下信息：

- 在 "SMTP Host" 字段中，输入 SMTP 服务器名称以便发送电子邮件通知。
- 在 "From" 字段中，自定义发件地址。
- 在“收件人”和“抄送”字段中，输入一个或多个将收到电子邮件通知的电子邮件地址或 Identity Manager 帐户。
- 在“电子邮件正文”字段中，自定义内容以提供指向 Identity Manager 位置的指针。

4 **单击“保存”。**

也可以使用 Sun Identity Manager 集成开发环境 (Identity Manager IDE) 修改电子邮件模板。有关 Identity Manager IDE 的信息，请访问以下网站：`https://identitymanageride.dev.java.net/`。

注 – 您必须注册并登录到此站点。

电子邮件模板中的 HTML 和链接

可以在电子邮件模板中插入 HTML 格式的内容，使之在电子邮件消息正文中显示。内容可以包括文本、图形以及信息的 Web 链接。要启用 HTML 格式的内容，请选择 "HTML Enabled" 选项。

电子邮件正文中允许使用的变量

还可以在电子邮件模板正文中包括变量的引用，格式为 `$(`*Name*`)`；例如：**您的密码 `$(password)` 已恢复。**

下表定义了每个模板允许使用的变量。

.

表 4–1 电子邮件模板变量

模板	允许的变量
密码重设	`$(password)` – 新生成的密码
更新批准	`$(fullname)` – 用户的全称
	`$(role)` – 用户的角色
更新通知	`$(fullname)` – 用户的全称
	`$(role)` – 用户的角色
报告	`$(report)` – 生成的报告
	`$(id)` – 任务实例的编码 ID
	`$(timestamp)` – 电子邮件发送的时间
请求资源	`$(fullname)` – 用户的全称
	`$(resource)` – 资源类型
风险分析	`$(report)` – 风险分析报告

表 4–1 电子邮件模板变量 （续）

模板	允许的变量
临时密码重设	`$(password)` – 新生成的密码 `$(expiry)` – 密码到期日期

配置审计组和审计事件

设置审计配置组允许您记录和报告您选择的系统事件。通过设置审计组，您还可以随后运行审计日志报告。

▼ 打开“审计配置”页

可以使用“审计配置”页来设置审计组。要打开“审计配置”页，请执行以下步骤：

1. **打开管理员界面。**
2. **单击“配置”选项卡，然后单击“审计”子选项卡。**
   将打开“审计配置”页。

▼ 配置审计组

配置审计组和事件需要配置审计管理权能。

1. **按照上一节中所述打开“审计配置”页。**
   "Audit Configuration" 页将显示审计组的列表，每个组可包含一个或多个事件。对于每个组，您可记录成功事件、失败事件或两者都记录。
2. **单击列表中的审计组以显示 "Edit Audit Configuration Group" 页。此页允许您选择审计事件的类型，将在系统审计日志的审计配置组中记录这些类型。**
3. **检查是否选中了“启用审计”复选框。清除复选框以禁用审计系统。**

注 – 有关审计组的详细信息，请参见第 10 章，审计日志记录中的第 295 页中的 “审计配置”。

▼ 为审计配置组添加事件

可以使用以下步骤在组中添加事件：

1. **单击“新建”。**
   Identity Manager 将事件添加到页底部。
2. **从列表的“对象类型”列中选择一个对象类型，然后将“操作”列中的一个或多个项目从新对象类型的“可用”区域移动到“选定”区域。**
3. **单击“确定”以将事件添加到组中。**

▼ 编辑审计配置组中的事件

可通过为对象类型添加或删除操作来编辑组中的事件，如下所示：

1. **将“操作”列中的项目从该对象类型的“可用”区域移到“已选定”区域。**
2. **单击“确定”。**

Remedy 集成

可以将 Identity Manager 与 Remedy 服务器集成，从而使之能够根据指定的模板发送 Remedy 票证。

在 "Administrator Interface" 界面的两个区域设置 Remedy 集成：

- **Remedy 服务器设置**。通过在“资源”区域创建 Remedy 资源来设置 Remedy 配置。（请参见第 137 页中的 “管理资源列表”。）资源设置完成后，请测试连接以确保集成可用。
- **Remedy 模板**。Remedy 资源设置完成后，定义 Remedy 模板。为此，请打开管理员界面，单击“配置”选项卡，然后单击“Remedy 集成”。然后选择 Remedy 模式和资源。

Remedy 票证的创建是通过 Identity Manager 工作流配置的。根据您的偏好，可以在使用已定义模板的合适时间执行调用，以打开 Remedy 票证。有关配置工作流的详细信息，请参见《Sun Identity Manager Deployment Reference》中的第 1 章 “Workflow”。

配置最终用户界面

管理员可以修改管理员界面中的表单，以配置最终用户界面中的某些内容。

▼ 设置用于在最终用户界面中显示信息的选项

1. **在管理员界面中，单击主菜单中的“配置”。**
2. **单击次级菜单中的“用户界面”。**
   将打开“用户界面”页。
3. **填写并保存表单中的最终用户面板部分。如果需要该表单的帮助，请单击“帮助”。**
   有关填写表单中的“匿名注册”部分的信息，请参见第 84 页中的 “匿名注册”。

▼ 在最终用户界面中启用进程图

进程图说明了在最终用户启动请求或更新其配置文件时 Identity Manager 遵循的工作流。如果启用了进程图，在最终用户提交表单后，它们将显示在结果页中。

必须先在管理员界面中启用进程图，然后才能在最终用户界面中启用这些进程图。有关详细信息，请参见第 52 页中的 “启用进程图”。

1. **执行第 98 页中的“配置最终用户界面”中的步骤以打开“用户界面”配置页。**
2. **选择“启用最终用户进程图”选项，该选项位于表单的“结果页”部分中。**
   如果“启用最终用户进程图”选项不可用，则必须先在管理员界面中启用进程图。请参见第 52 页中的 “启用进程图”。
3. **单击“保存”。**

注册 Identity Manager

建议管理员注册其 Identity Manager 安装。

您必须具有 Sun 联机帐户和密码才能进行注册。如果没有 Sun 联机帐户，您可以在以下地址填写表单以注册一个帐户：

`https://reg.sun.com/register`

可以通过控制台或管理员界面来注册 Identity Manager。

通过从控制台中进行注册，您还可以创建一个本地服务标记，可以在 Sun 服务标记软件中使用此标记来跟踪 Sun 系统、软件和服务清单。在创建本地服务标记之前，应该先安装服务标记客户机包。可通过在以下地址中单击 "Download Service Tags"（下载服务标记）按钮来下载该包：

```
http://inventory.sun.com/inventory
```

要注册 Identity Manager，您必须使用允许配置 Identity Manager 对象的管理员帐户进行登录。此帐户必须具有产品注册权能。有关权能的信息，请参见第 187 页中的 “为用户分配权能”。

注 – 要使产品注册功能正常工作，必须为 SSL 正确配置 Identity Manager 应用服务器上的 Java。`java.security` 文件（或等效文件）中引用的所有 JAR 文件必须存在。

本节其余部分提供了帮助您注册 Identity Manager 的信息和说明。该信息分为以下几个主题：

- 第 99 页中的 “从控制台中注册 Identity Manager”
- 第 101 页中的 “从管理员界面中注册 Identity Manager”

从控制台中注册 Identity Manager

本节包含从控制台中注册 Identity Manager 所需的信息。

使用 `register` 命令

可以使用 `register` 命令从控制台中注册 Identity Manager。本节提供了有关使用该命令的信息。

`register` 命令用法

```
register -local
register -remote [-u <userid> [-p <password>]] [-prompt] -userSOA <userid>
-passSOA <password> [-proxy <proxyHost> [-port <proxyPortNumber>]]
register [-help | -?]
```

`register` 命令选项

下表介绍了可与 `register` 命令一起使用的选项。

表 4–2 命令选项

选项	描述
`-local`	在此主机上创建服务标记。
`-remote`	通过网络直接向 Sun 注册此 Identity Manager 安装。
`-u <userid>`	经授权进行注册的 Identity Manager 管理员的 Identity Manager 用户 ID。
`-p <password>`	经授权进行注册的 Identity Manager 管理员的 Identity Manager 密码。
`-prompt`	如果缺少密码，则会以交互方式提示输入密码。
`-userSOA <userid>`	用于注册的 Sun 联机帐户的用户 ID。如果使用 `-remote` 选项进行注册，则需要使用此选项。
`-passSOA <password>`	用于注册的 Sun 联机帐户的密码。如果使用 `-remote` 选项进行注册，则需要使用此选项。
`-proxy <proxyHost>`	用于访问 Sun 联机注册服务的网络代理。在使用 `-remote` 选项进行注册并将网络配置为使用代理到达外部 Internet 地址时，需要使用此选项。
`-port <proxyPortNumber>`	用于访问 Sun 联机注册服务的网络代理上的端口。在使用 `-remote` 选项进行注册并将网络配置为使用代理到达外部 Internet 地址时，需要使用此选项。
`-help | -?`	将此命令的帮助输出到控制台。

▼ 从控制台中注册 Identity Manager

要从控制台中注册 Identity Manager，必须创建本地服务标记或通过 Internet 向 Sun 注册。请按以下说明进行操作：

1 启动 Identity Manager 控制台（命令行）界面。

- 从 Windows 命令行中键入

  `%WSHOME%\bin\lh`

- 从 UNIX 命令行中键入

  `$WSHOME/bin/lh`

2 按如下方式使用 `register` 命令：

- 创建本地服务标记：

  `register -local`

- 要通过 Internet 注册 Identity Manager，请使用以下命令：

  `register -remote -u <`*userid*`> -p <`*password*`> -userSOA <`*soaUserid*`> -passSOA <`*soaPassword* `> -proxy <`*proxyHost*`> -port <` *proxyPortNumber*`>`

其中：

- **userid** 是经授权进行注册的 Identity Manager 管理员的 Identity Manager 用户 ID。
- **password** 是经授权进行注册的 Identity Manager 管理员的 Identity Manager 密码。
- **soaUserid** 是用于注册的 Sun 联机帐户的用户 ID。
- **soaPassword** 是用于注册的 Sun 联机帐户的密码。
- **proxyHost** 是用于访问 Sun 联机注册服务的网络代理。只有在将网络配置为使用代理到达外部 Internet 地址时，才需要使用此参数。
- **proxyPortNumber** 是用于访问 Sun 联机注册服务的网络代理上的端口。只有在将网络配置为使用代理到达外部 Internet 地址时，才需要使用此参数。

▼ 从管理员界面中注册 Identity Manager

如果不需要创建本地服务标记，可从管理员界面中注册 Identity Manager。

1 **在管理员界面中，单击“配置”。**

2 **在次级菜单中，单击“产品注册”。**
将打开“产品注册”页。

3 **填写表单，然后单击“立即注册”。有关各个表单字段的信息，请单击 i-Helps。**

注 –

- 如果未将应用服务器配置为允许传出 SSL 连接，则可能会看到以下错误消息：

```
Failed to register on Sun Connection server
due to invalid Sun Online Account user/password.
```

  要解决此问题，请将相应的可信根证书添加到应用服务器的密钥库中。有关详细信息，请查阅应用服务器文档。
- 如果应用服务器的类路径中包含旧版本的 `xml-apis.jar` 和 `xercesImpl.jar`，则可能会看到以下错误消息：

```
java.lang.NoSuchMethodError:org.w3c.dom.Node.getTextContent()Ljava/lang/String;
```

  要解决此问题，请修改类路径，使其只包含最新版本的 `xml-apis.jar` 和 `xercesImpl.jar`。

编辑 Identity Manager 配置对象

在管理 Identity Manager 过程中，偶尔可能需要编辑 Identity Manager 系统配置对象（也称为系统配置文件）或其他类似的对象。

1. **在浏览器中键入以下 URL 以打开 Identity Manager 调试页：**

   `http://<`*AppServerHost*`>:<`*Port*`>/idm/debug/session.jsp`

   将打开“系统设置”页。

   注 – 必须具有“调试”权能才能查看 `/idm/debug/` 页。

2. **找到“列出对象”按钮，然后从旁边的“类型”下拉列表中选择“配置”。**
3. **单击“列出对象”按钮。**

   将打开“列出以下类型的对象：配置”页。
4. **在对象列表中找到所需的对象，然后单击“编辑”。**

   例如，要编辑系统配置对象，请找到“系统配置”，然后单击“编辑”。
5. **按照说明编辑该对象，然后单击“保存”。**
6. **如果要求重新启动服务器，请将其重新启动。**

◆ ◆ ◆ 第 5 章

5 角色和资源

本章介绍了 Identity Manager 角色和资源。

本章中的信息分为以下主题：

了解和管理角色

阅读本节可以了解有关在 Identity Manager 中设置角色的信息。在大型组织中，基于角色的资源分配可大大简化资源管理。

注 – 不要将**角色**和**管理员角色**相混淆。角色用于管理最终用户对外部资源的访问。而管理员角色主要用于管理管理员对内部 Identity Manager 对象（如用户、组织和权能）的访问。

本节中的信息讨论的是角色。有关管理员角色的信息，请参见第 187 页中的“了解和管理管理员角色”。

什么是角色？

角色是一个 Identity Manager 对象，通过该对象，可以将资源访问权限分组并有效地分配给用户。

角色分为以下四种角色类型：

- 业务角色
- IT 角色

- 应用程序
- 资产

业务角色用于将组织中执行类似任务的人员工作时所需的访问权限划分到各个组中。通常，业务角色表示用户的工作职责。例如，在一个金融机构中，业务角色可能对应于各个工作职责，如银行出纳员、信贷员、分行经理、办事员、会计或管理助理。

IT **角色**、**应用程序**和**资产**将资源权利划分为不同的组。要为最终用户提供资源访问权限，请将 IT 角色、应用程序和资产分配给业务角色，以使用户在工作时能够访问所需的资源。IT 角色包含一组特定的应用程序、资产和/或资源，其中包括这些分配的资源的特定权利。IT 角色也可以包含其他 IT 角色。

注 – 角色类型的概念是在 Identity Manager 8.0 版中引入的。如果组织从早期版本的 Identity Manager 升级到 8.0 版，则会将传统角色作为 IT 角色导入。有关详细信息，请参见第 104 页中的 “管理在 8.0 之前的版本中创建的角色”。

IT 角色、应用程序和资产可以是**必需**、**条件**或**可选**角色。

- 必需角色将始终分配给最终用户。
- 条件角色具有一定的条件，其计算值必须为 true 才能分配该角色。
- 可以单独请求可选角色；在得到批准后，便会将其分配给最终用户。

通过使用必需、条件和可选角色，业务角色设计者可以针对包含的角色定义粗粒度的访问以使用户遵守相关的规定；同时仍为最终用户管理员提供了一定的灵活性，以微调最终用户的访问权限。对于分配了条件或可选角色的用户，仍然可以为其分配相同的业务角色，但为其分配的访问权限是不同的。通过采用这种方法，无需为组织中的每种访问要求变化形式都定义新的业务角色（此问题称为**角色爆炸**）。

运用角色类型

下面介绍了如何有效地使用角色类型。有关角色类型描述，请参见上一节。

管理在 8.0 之前的版本中创建的角色

从早期版本的 Identity Manager 升级到 8.0 版的组织会自动将其传统角色转换为 IT 角色。这些 IT 角色仍将直接分配给用户。在升级过程中，不会为传统角色分配角色所有者。不过，以后可以分配角色所有者。（有关角色所有者的信息，请参见第 114 页中的 “指定角色所有者和角色批准者”。）

默认情况下，升级到 8.0 版的组织可以直接将 IT 角色和业务角色分配给用户（请参见图 5–2）。

如果组织具有传统角色，则应该考虑按照下一节中简要介绍的原则创建新角色。

使用角色类型设计灵活的角色

IT 角色、应用程序和资产是角色设计者的基本构件。可以结合使用这三种角色类型来设置用户权利（即，**访问权限**）。然后可将 IT 角色、应用程序和资产分配给业务角色。

设计业务角色

在 Identity Manager 中，可以为用户分配一个或多个角色，也可以不分配角色。随着在 Identity Manager 8.0 中引入角色类型概念，建议您仅将业务角色直接分配给用户。事实上，默认情况下，无法将任何其他角色类型直接分配给用户，除非组织安装了 8.0 之前版本的 Identity Manager 并将其至少升级到 8.0 版。可通过修改角色配置对象来更改这种默认限制（第 132 页中的 “配置角色类型”）。

为了降低复杂性，不能对业务角色进行嵌套。即，一个业务角色不能包含另一个业务角色。另外，业务角色不能直接包含资源和资源组。而应将资源和资源组分配给 IT 角色或应用程序，然后再将这些角色分配给一个或多个业务角色。

设计 IT 角色

IT 角色可以包含应用程序和资产以及其他 IT 角色。IT 角色还可以包含资源和资源组。

IT 角色一般是由组织的 IT 人员或资源所有者（了解启用资源中特定权限所需的权利）创建和管理的。

设计应用程序和资产

应用程序和资产角色类型用于表示常用业务术语，以描述最终用户工作时需要具备的条件。例如，可以将应用程序角色命名为“客户支持工具”或“内部网 HR 工具管理”。

- 应用程序不能包含角色，但可以包含资源和资源组。应用程序还可以定义特定的权利，以仅限访问包含的资源上的特定应用程序。
- 资产（通常）是需要手动置备的非连接资源或非数字资源，例如移动电话和便携式计算机。因此，资产不能包含角色、资源或资源组。

应用程序和资产用于分配给业务角色和 IT 角色。

注 –

应该为角色管理员分配下面的一种或多种权能：

- 资产管理员
- 应用程序管理员
- 业务角色管理员
- IT 角色管理员

有关详细信息，请参见第 187 页中的 “为用户分配权能”。

角色类型总览

下图显示了可以为四种角色类型中的每种角色类型分配的角色类型、资源和资源组。该图还显示了可以为所有四种角色类型分配的角色类型排除。（有关角色排除的说明，请参见第 110 页中的 “分配资源和资源组”。）

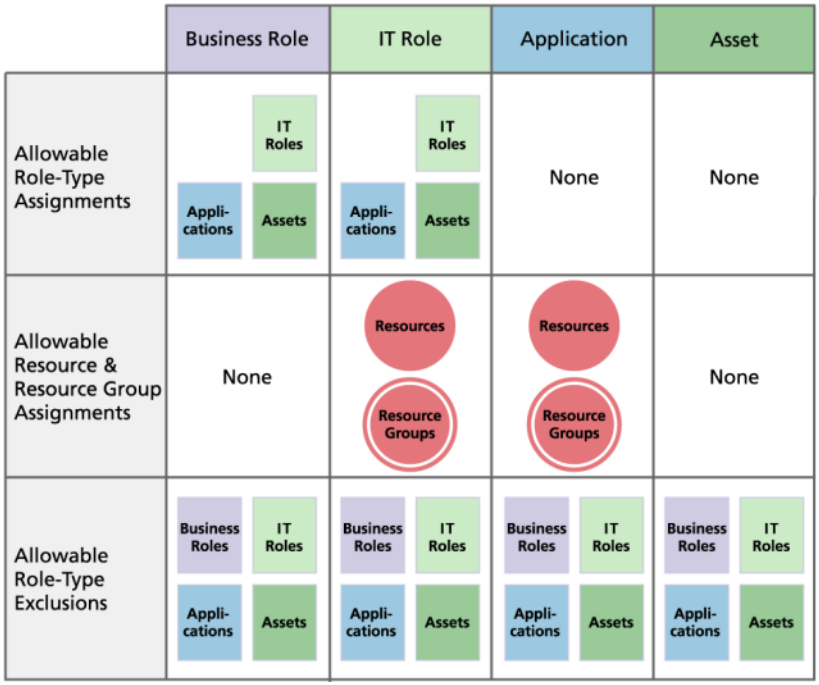


图 5–1 业务角色、IT 角色、应用程序和资产角色类型。

可选、条件和必需包含角色（第 103 页中的 “什么是角色？ ”）提供了额外的灵活性。灵活的角色定义可以减少组织需要管理的角色总数。

图 5–2 显示了从 8.0 之前版本的 Identity Manager 至少升级到 8.0 版时可以将业务角色和 IT 角色直接分配给用户。在升级时，传统角色将转换为 IT 角色，并将 IT 角色直接分配给用户以保持向后兼容性。如果 Identity Manager 不是从 8.0 之前版本升级的，则只能将业务角色直接分配给用户。

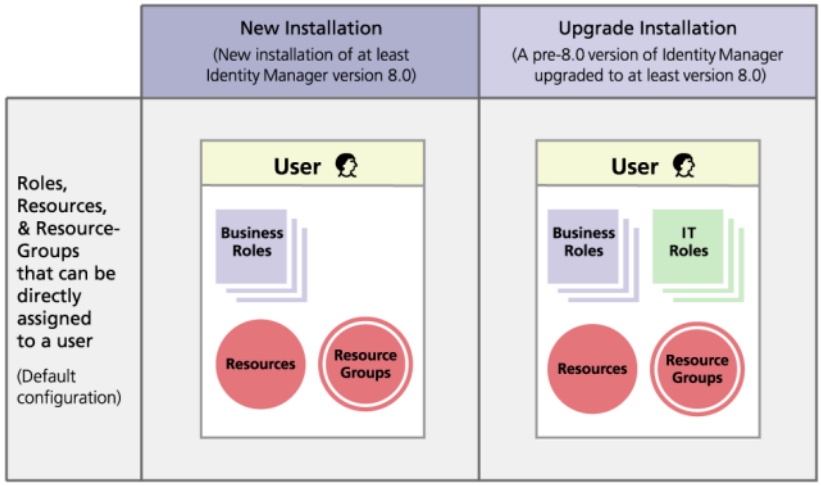


图 5–2 可直接分配给用户的角色和资源。

创建角色

本节介绍了如何创建角色，该信息分为以下几个部分：

- 第 107 页中的“使用创建角色表单创建角色”
- 第 110 页中的“分配资源和资源组”
- 第 111 页中的“编辑分配的资源属性值”
- 第 113 页中的“分配角色和角色排除”
- 第 114 页中的“指定角色所有者和角色批准者”
- 第 116 页中的“指定通知”
- 第 117 页中的“启动更改批准工作项目和批准工作项目”

注 – 有关设计角色的提示，请参见第 105 页中的“使用角色类型设计灵活的角色”。

当您创建或编辑角色时，Identity Manager 会启动 `ManageRole` 工作流。此工作流将新建角色或更新的角色保存在信息库中，并允许您在创建或保存该角色前插入批准或其他操作。

▼ 使用创建角色表单创建角色

1 **在管理员界面中，单击主菜单中的“角色”。**
将打开“角色”页（“列出角色”选项卡）。

2 **单击页面底部的“新建”。**
将打开“创建 IT 角色”页。要创建另一种类型的角色，请使用“类型”下拉菜单。

3 **填写“标识”选项卡上的表单字段。**

下图显示了“标识”选项卡。

图 5–3 “创建 IT 角色”页中的“标识”选项卡

4 **填写“资源”选项卡上的表单字段（如果适用）。有关填写此选项卡上的字段的帮助，请参阅联机帮助以及第 110 页中的“分配资源和资源组”。**

有关在角色上设置扩展属性值的帮助，请参见第 144 页中的“查看或编辑资源帐户属性”。

下图显示了“资源”选项卡。

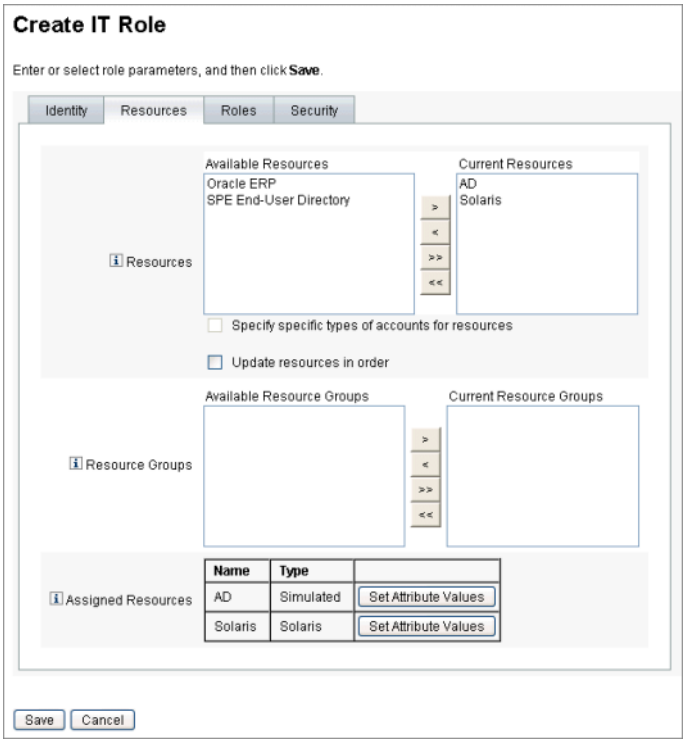


图 5–4 “创建 IT 角色”页中的“资源”选项卡

5 **填写“角色”选项卡上的表单字段（如果适用）。有关填写此选项卡上的字段的帮助，请参阅联机帮助以及第 113 页中的“分配角色和角色排除”。**

图 5–6 显示了“角色”选项卡。

6 **填写“安全性”选项卡上的表单字段。有关填写此选项卡上的字段的帮助，请参阅联机帮助以及第 114 页中的“指定角色所有者和角色批准者”和第 116 页中的“指定通知”。**

第 114 页中的 “指定角色所有者和角色批准者”显示了“安全性”选项卡。

7 **单击页面底部的“保存”。**

8 **在“创建角色”表单的“标识”选项卡中，可以输入角色的名称和描述。如果要创建新角色，请使用“类型”下拉菜单选择要创建的角色类型。**

图 5–4 显示了“创建角色”表单的“标识”选项卡的“标识”部分。有关使用此表单的帮助，请参见联机帮助。

▼ 分配资源和资源组

可以使用“创建角色”表单的“资源”选项卡，将资源和资源组直接分配给 IT 角色和应用程序角色。后面的第 136 页中的 “了解和管理 Identity Manager 资源”一节中介绍了资源。第 145 页中的 “资源组”一节中介绍了资源组。

- 无法将资源和资源组直接分配给业务角色，因为只能将角色分配给业务角色。
- 无法将资源和资源组分配给资产角色，因为资产角色是为需要手动置备的非连接资源或非数字资源保留的。

此过程介绍了在填写“创建角色”表单时如何将资源和资源组分配给角色。要了解入门知识，请参见第 107 页中的 “使用创建角色表单创建角色”。

1. **在“创建角色”页中单击“资源”选项卡。**
2. **要分配某个资源，请在“可用资源”列中选中该资源，然后单击箭头按钮将其移到“当前资源”列中。**
3. **如果要分配多个资源，则可以指定更新这些资源的顺序：选中“按顺序更新资源”复选框，然后使用 + 和 - 按钮更改“当前资源”列中的资源顺序。**
4. **要将资源组分配给此角色，请在“可用资源组”列中将其选中，然后单击箭头按钮以将其移到“当前资源组”列中。资源组是一个资源集合，它提供了另外一种方法来指定创建和更新资源帐户的顺序。**
5. **要针对每个资源为此角色指定帐户属性，请在分配的资源部分中单击“设置属性值”。有关详细信息，请参见第 144 页中的“查看或编辑资源帐户属性”。**
6. **单击“保存”以保存角色，或者单击“标识”、“角色”或“安全性”选项卡以继续执行角色创建过程。**

   下图显示了“创建角色”表单的“资源”选项卡。

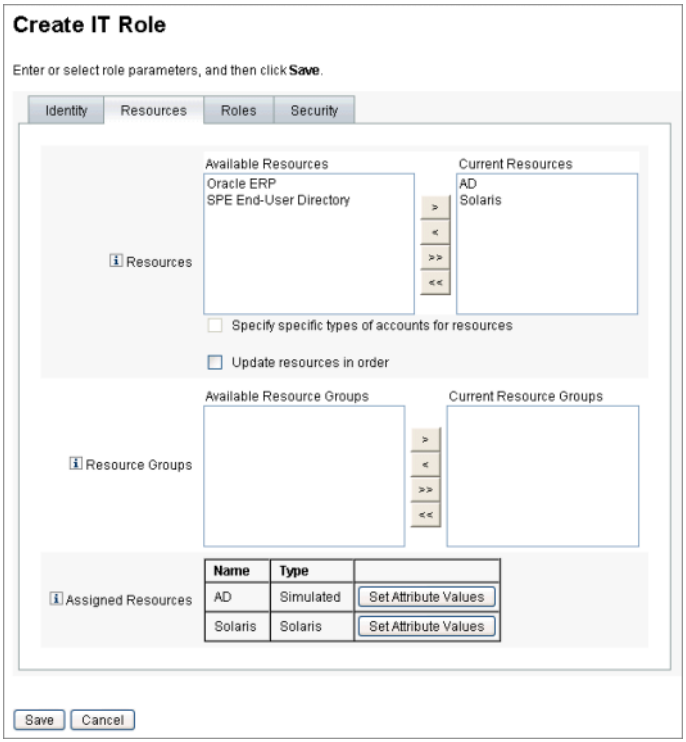
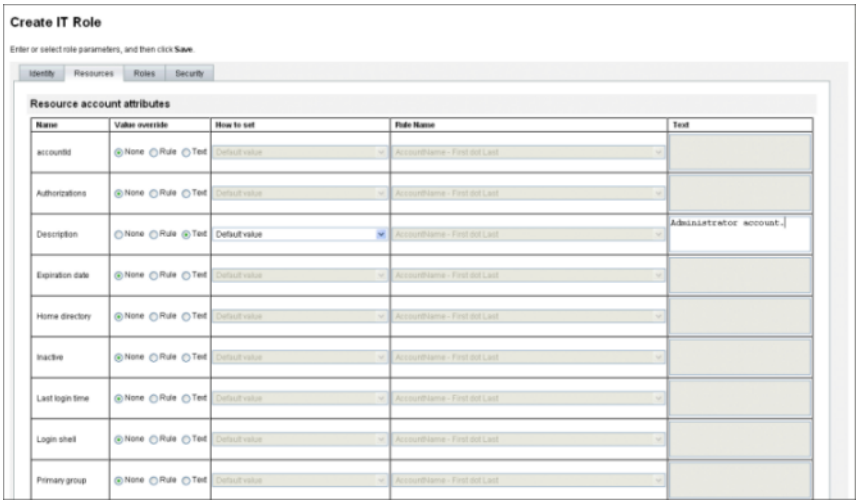


图 5–5 “创建角色”选项卡式表单的“资源”部分

▼ 编辑分配的资源属性值

可以使用“分配的资源”表来设置或修改分配给角色的资源上的资源属性值。资源可以针对每个角色定义不同的属性值。单击“设置属性值”按钮将打开“资源帐户属性”页。

下图显示了“资源帐户属性”页，它用于在分配给角色的资源上设置扩展资源属性值。



1 **从"资源帐户属性"页中，为每个属性指定新值，并确定如何设置属性值。**

Identity Manager 允许直接设置值，或使用一个规则来设置值；它还提供一些用于覆盖或合并现有值的选项。有关资源属性值的一般信息，请参见第 144 页中的 "查看或编辑资源帐户属性"。

可以使用以下选项设置每个资源帐户属性的值：

- **值覆盖**。请选择以下任一选项：
  - **无（默认）**。不设置任何值。
  - **规则**。使用规则设置值。

    如果选择此选项，必须从列表中选择规则名称。
  - **文本**。使用指定的文本设置值。

    如果选择此选项，则必须在旁边的文本字段中输入文本。
- **设置方法**。请选择以下任一选项：
  - **默认值**。使规则或文本作为默认属性值。

    用户可更改或覆盖此值。
  - **设置成值**。将属性值设置为规则或文本指定的值。

    设置该值将覆盖所有用户更改。
  - **与值合并**。合并当前属性值与规则或文本指定的值。
  - **与值合并，清除现有值**。删除当前属性值；将值设置为此分配角色与其他分配角色所指定值的合并值。
  - **从值中删除**。从属性值中删除规则或文本指定的值。
  - **授权设置值**。将属性值设置为规则或文本指定的值。

设置该值将覆盖所有用户更改。如果删除角色，则即使该属性先前具有相应值，新属性值仍会是空值。

- **授权与值合并**。合并当前属性值与规则或文本指定的值。

  删除角色将删除在分配角色时分配的值，原始属性值将保持不变。

- **授权与值合并，清除现有**。删除当前属性值；将值设置为此分配角色与其他分配角色所指定值的合并值。

  如果删除角色，则即使该属性先前具有相应值，仍会清除此角色指定的属性值。

- **规则名称**。如果在“值覆盖”区域选择“规则”，则需要从列表中选择规则。
- **文本**。如果在“值覆盖”区域选择“文本”，则需要输入要添加至属性值、从属性值删除或用作属性值的文本。

2 **单击“确定”可保存所做的更改并返回“创建角色”或“编辑角色”页。**

▼ 分配角色和角色排除

可以使用“创建角色”表单的“角色”选项卡，将角色分配给业务角色和 IT 角色。应该将分配的角色添加到包含的角色表中。

- 无法将角色分配给应用程序角色和资产角色。
- 无法将业务角色分配给任何角色类型。

可以使用“创建角色”表单的“角色”选项卡，将角色排除分配给所有四种角色类型。如果将具有角色排除的角色分配给用户，则无法将排除的角色分配给用户。应该将角色排除添加到角色排除表中。

此过程介绍了在填写“创建角色”表单时如何将一个或多个角色分配给某个角色。要了解入门知识，请参见第 107 页中的 “使用创建角色表单创建角色”。

填写“角色”选项卡

1 **在“创建角色”页中单击“角色”选项卡。**

2 **在“包含的角色”部分中单击“添加”。**

将刷新该选项卡并显示查找要包含的角色表单。

3 **搜索将要分配给此角色的角色。请先从任何必需角色入手。（将随后添加条件和可选角色。）**

有关使用搜索表单的帮助，请参见第 118 页中的 “搜索角色”。无法将业务角色嵌套在其他角色类型中，也无法将其分配给其他角色类型。

4 **使用复选框选择一个或多个要分配的角色，然后单击“添加”。**

将刷新该选项卡并显示添加包含的角色表单。

5 **根据需要，从“关联类型”下拉菜单中选择“必需”、“条件”或“可选”。**

单击“确定”。

6 **重复前面的四个步骤，以添加条件角色（如果需要）。再次重复前面的四个步骤，以添加可选角色（如果需要）。**

7 **单击“保存”以保存角色，或者单击“标识”、“资源”或“安全性”选项卡以继续执行角色创建过程。**

图 5–6 显示了“创建角色”表单的“角色”选项卡。有关使用此表单的帮助，请参见联机帮助。

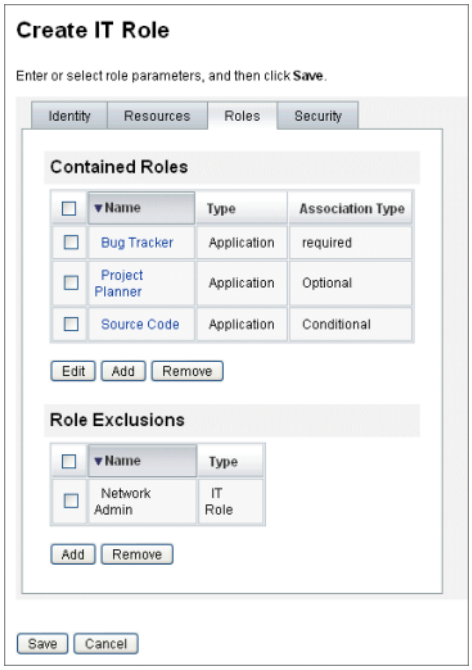


图 5–6 “创建角色”选项卡式表单的“角色”部分

指定角色所有者和角色批准者

角色具有指定的**所有者**和**批准者**。仅角色所有者能够授权对定义角色的参数进行更改，仅角色批准者能够授权将角色分配给最终用户。

注 – 如果将 Identity Manager 与 Sun™ Role Manager 集成在一起，应通过手动禁用 Identity Manager 处理角色更改批准和通知的功能以允许 Role Manager 执行所有这些操作。

必须按如下方式在 Identity Manager 中编辑 RoleConfiguration 配置对象：

- 查找 changeApproval 的所有实例，并将值设置为 **false**。
- 查找 changeNotificaiton 的所有实例，并将值设置为 **false**。

成为角色所有者就是成为负责通过角色分配的基本资源帐户权限的业务所有者。如果管理员对角色进行更改，则必须经角色所有者批准后才能执行这些更改。此功能可防止管理员在业务所有者不知情或未批准的情况下更改角色。然而，如果在角色配置对象中禁用了更改批准，则不需要得到角色所有者的批准即可执行更改。

除了批准角色更改以外，未经角色所有者批准也无法启用、禁用或删除角色。

可以将所有者和批准者直接添加到角色中，也可以使用角色分配规则动态地进行添加。在 Identity Manager 中，可以创建没有所有者和批准者的角色（但不建议这样做）。

注 – 角色分配规则的 authType 为 RoleUserRule。

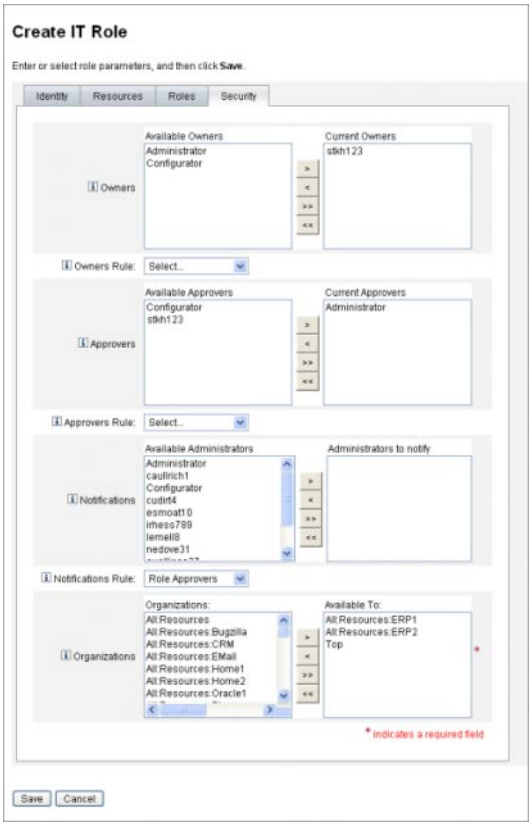
如果需要创建自定义角色分配规则，请参考三个默认角色分配规则对象并将它们用作示例：

- 角色批准者
- 角色通知
- 角色所有者

如果工作项目需要得到所有者和批准者批准，则会通过电子邮件通知他们。第 117 页中的 “启动更改批准工作项目和批准工作项目”一节中介绍了更改批准工作项目和批准工作项目。

所有者和批准者将添加到“创建角色”表单的“安全性”选项卡上的角色中。

第 114 页中的 “指定角色所有者和角色批准者” 显示了“创建角色”表单的“安全性”选项卡。有关使用此表单的帮助，请参见联机帮助。



指定通知

在将角色分配给用户时，可以向一个或多个管理员发送通知。

可以选择是否指定通知收件人。如果决定在将角色分配给用户时不需要批准，您可以选择通知管理员。或者，您可以指定一个管理员作为批准者，并指定另一个管理员作为进行批准时的通知收件人。

与所有者和批准者一样，可以将通知直接添加到角色中，也可以使用角色分配规则动态地进行添加。在将角色分配给用户时，可以通过电子邮件向通知收件人发出通知。但不会创建工作项目，因为不需要进行批准。

通知将分配给“创建角色”表单的“安全性”选项卡上的角色。第 114 页中的 “指定角色所有者和角色批准者” 显示了“创建角色”表单的“安全性”选项卡。

启动更改批准工作项目和批准工作项目

在对角色进行更改时，角色所有者可能会收到**更改批准**或**更改通知**电子邮件，也可能没有收到任何电子邮件。在将角色分配给用户时，角色批准者将会收到角色**批准**电子邮件。

默认情况下，只要更改了角色所有者拥有的角色，就会向其发送更改批准电子邮件。不过，可以针对每种角色类型对这种行为进行配置。例如，您可以选择为业务角色和 IT 角色启用更改批准，而为应用程序和资产角色启用更改通知。

有关启用和禁用更改批准和更改通知电子邮件的说明，请参见第 132 页中的 “配置角色类型”。

下面是更改批准和更改通知的工作方式：

- 如果启用了**更改批准**，在管理员更改角色时，将会生成一个工作项目并向角色所有者发送批准电子邮件。角色所有者必须批准该工作项目才能进行更改。可以委托更改批准工作项目。有关详细信息，请参见第 202 页中的 “批准用户帐户”。

  如果禁用了更改批准，则不会生成工作项目，也不会向角色所有者发送更改批准电子邮件。
- 如果启用了**更改通知**，则在管理员更改角色时，将会立即进行更改并向角色所有者发送通知电子邮件。

  如果禁用了更改通知，则不会向角色所有者发送任何通知。

在将角色分配给用户时，角色批准者将会收到角色**批准**电子邮件。无法在 Identity Manager 中禁用角色批准电子邮件。

对于角色批准，在为用户分配角色时，将会生成一个工作项目并向角色批准者发送批准电子邮件。角色批准者必须批准该工作项目才能将角色分配给用户。

可以委托更改批准工作项目和批准工作项目。有关委托工作项目的详细信息，请参见第 199 页中的 “委托工作项目”。

编辑和管理角色

可以使用“查找角色”和“列出角色”选项卡执行大多数角色编辑和角色管理任务，这些选项卡位于主菜单的“角色”选项卡下面。

本节包含以下主题：

▼ 搜索角色

可以使用“查找角色”选项卡搜索符合指定搜索条件的角色。

通过使用“查找角色”选项卡，您可以基于各种不同的条件（如角色所有者和批准者、分配的帐户类型以及包含的角色等）搜索角色。

有关查找分配给角色的用户的信息，请参见第 131 页中的 “查找分配给特定角色的用户”。

1 **在管理员界面中，单击“角色”选项卡。**

将打开“列出角色”选项卡。

2 **单击“查找角色”次级选项卡。**

图 5–7 显示了“查找角色”选项卡。有关使用此表单的帮助，请参见联机帮助。

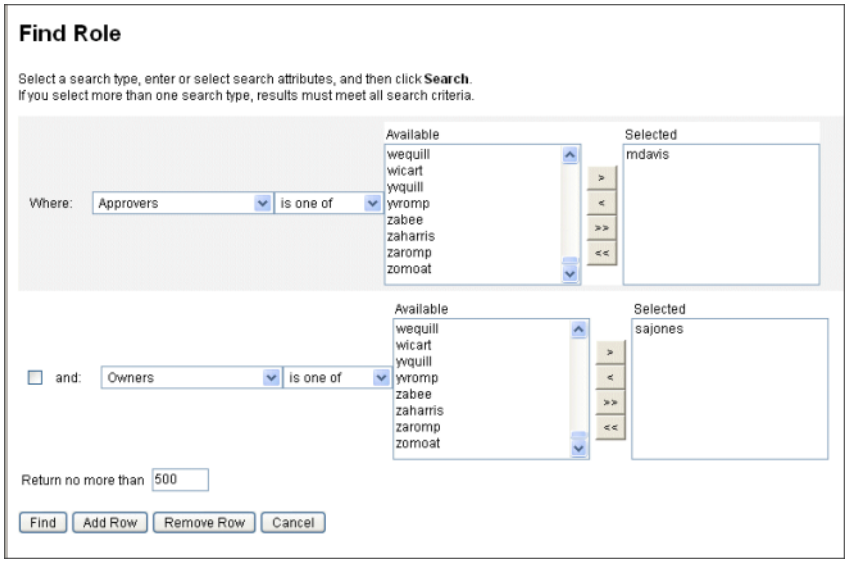


图 5–7 “查找角色”选项卡

可以使用下拉菜单来定义搜索参数。单击“添加行”按钮可添加其他参数。

▼ 查看角色

可以使用“列出角色”选项卡来查看角色。可以使用“列出角色”页顶部的过滤器字段按名称或角色类型查找角色。过滤不区分大小写。

- **在管理员界面中，单击“角色”选项卡。**

  将打开“列出角色”选项卡。

  图 5–8 显示了“列出角色”选项卡。有关使用此表单的帮助，请参见联机帮助。

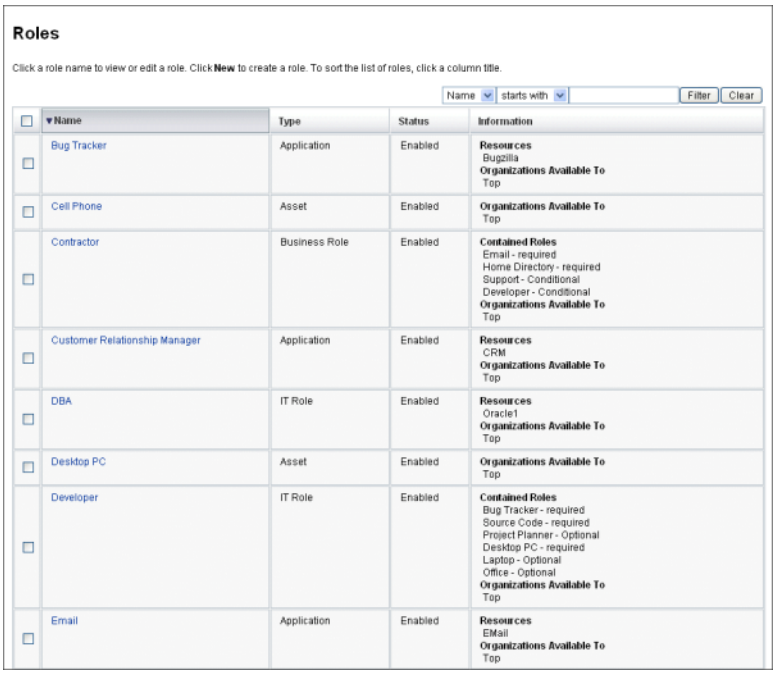


图 5–8 “列出角色”选项卡

▼ 编辑角色

可以使用“列出角色”或“查找角色”选项卡搜索要编辑的角色。如果对角色进行更改并将更改批准设置为 true，则必须在角色所有者批准更改之后才能执行更改。

有关使用角色更改更新用户的信息，请参见第 127 页中的“更新分配给用户的角色”。

1. **按照第 118 页中的“搜索角色”或第 119 页中的“查看角色”中的说明，搜索要编辑的角色。**

2. **单击要编辑的角色的名称。**
   将打开“编辑角色”页。

3. **根据需要，编辑该角色。有关填写“标识”、“资源”、“角色”和“安全性”选项卡的帮助，请参阅第 107 页中的“使用创建角色表单创建角色”一节中的步骤。**
   单击“保存”。将打开“确认角色更改”页。

4. **如果将此角色分配给用户，则可以选择何时使用角色更改更新用户。有关详细信息，请参见第 127 页中的“更新分配给用户的角色”。**

5. **单击“保存”以保存更改。**

▼ 克隆角色

1. **按照第 118 页中的“搜索角色”或第 119 页中的“查看角色”中的说明，搜索要编辑的角色。**

2. **单击要克隆的角色的名称。**
   将打开“编辑角色”页。

3. **在“名称”字段中输入新名称，然后单击“保存”。**
   将打开“角色：创建还是重命名？”页。

4. **单击“创建”以复制角色。**

▼ 将角色分配给其他角色

第 103 页中的“什么是角色？”和第 104 页中的“运用角色类型”中介绍了 Identity Manager 的角色分配要求。在分配角色之前，您应该了解此信息。

如果父角色的角色所有者批准，Identity Manager 将更改角色的角色分配。

1. **搜索将向其分配一个或多个包含的角色的业务角色或 IT 角色。（只能将角色分配给业务角色和 IT 角色。）请按照第 118 页中的“搜索角色”或第 119 页中的“查看角色”中的说明搜索角色。**

2. **单击以打开业务角色或 IT 角色。**
   将打开“编辑角色”页。

3. **在“编辑角色”页中单击“角色”选项卡。**

4. **在“包含的角色”部分中单击“添加”。**
   将刷新该选项卡并显示查找要包含的角色表单。

5 **搜索将要分配给此角色的角色。请先从任何必需角色入手。（将随后添加条件和可选角色。）**

有关使用搜索表单的帮助，请参见第 118 页中的“搜索角色”。无法将业务角色嵌套在其他角色类型中，也无法将其分配给其他角色类型。

6 **使用复选框选择一个或多个要分配的角色，然后单击“添加”。**

将刷新该选项卡并显示添加包含的角色表单。

7 **根据需要，从“关联类型”下拉菜单中选择“必需”、“条件”或“可选”。**

单击“确定”。

8 **重复前面的四个步骤，以添加条件角色（如果需要）。再次重复前面的四个步骤，以添加可选角色（如果需要）。**

9 **单击“保存”以打开“确认角色更改”页。**

将打开“确认角色更改”页。

10 **在“更新分配的用户”部分中，选择一个“更新分配的用户”菜单选项，然后单击“保存”以保存角色分配。**

有关详细信息，请参见第 127 页中的“更新分配给用户的角色”。

▼ 删除分配给其他角色的角色

如果得到父角色的角色所有者批准，Identity Manager 将从另一个角色中删除包含的角色。当用户收到角色更新时，将从用户中删除已删除的角色。（有关详细信息，请参见第 127 页中的“更新分配给用户的角色”。）删除角色后，用户将失去该角色所赋予的权利。

- 有关删除分配给一个或多个用户的角色的信息，请参见第 131 页中的“从用户中删除一个或多个角色”。
- 有关禁用角色的信息，请参见第 122 页中的“启用或禁用角色”。
- 有关从 Identity Manager 中删除角色的信息，请参见第 122 页中的“删除角色”。

1 **搜索要从中删除角色的业务角色或 IT 角色。请按照第 118 页中的“搜索角色”或第 119 页中的“查看角色”中的说明搜索角色。**

2 **单击以打开该角色。**

将打开“编辑角色”页。

3 **在“编辑角色”页中单击“角色”选项卡。**

4 **在“包含的角色”部分中，选中要删除的角色旁边的复选框，然后单击“删除”。选中多个复选框可删除多个角色。**
将更新该表以显示其余的包含角色。

5 **单击“保存”。**
将打开“确认角色更改”页。

6 **在“更新分配的用户”部分中，选择一个“更新分配的用户”菜单选项。有关详细信息，请参见第 127 页中的“更新分配给用户的角色”。**

7 **单击“保存”以完成更改。**

▼ 启用或禁用角色

可以在“列出角色”选项卡上启用和禁用角色。角色状态将显示在状态列中。单击“状态”列标题可按角色状态对该表进行排序。

禁用的角色不会显示在“创建/编辑用户”表单的“角色”选项卡中，并且无法直接分配给用户。可以将包含已禁用角色的角色分配给用户，但无法分配已禁用的角色。

如果以后禁用了为用户分配的角色，用户并不会失去其权利。角色禁用仅阻止**未来的角色分配**。

角色禁用和重新启用需要具有角色所有者权限。

在启用或禁用分配了用户的角色时，Identity Manager 将提示您更新这些用户。有关详细信息，请参见第 127 页中的“更新分配给用户的角色”。

1 **按照第 118 页中的“搜索角色”或第 119 页中的“查看角色”中的说明，搜索要删除的角色。**

2 **单击需要启用或禁用的角色旁边的复选框。**

3 **单击“角色”表底部的“启用”或“禁用”。**
将打开“启用角色”或“禁用角色”确认页。

4 **单击“确定”以启用或禁用该角色。**

▼ 删除角色

本节介绍了从 Identity Manager 中删除角色的过程。

- 有关删除分配给其他角色的角色的信息，请参见第 121 页中的“删除分配给其他角色的角色”。
- 有关删除分配给一个或多个用户的角色的信息，请参见第 131 页中的“从用户中删除一个或多个角色”。

如果删除当前分配给用户的角色，当您尝试保存该角色时，Identity Manager 将阻止删除操作。您必须取消分配（或重新分配）分配给角色的所有用户，然后 Identity Manager 才能删除该角色。您还必须从任何其他角色中删除该角色。

Identity Manager 需要得到角色所有者的批准，然后才能删除角色。

1. **按照第 118 页中的“搜索角色”或第 119 页中的“查看角色”中的说明，搜索要删除的角色。**
2. **选中要删除的每个角色旁边的复选框。**
3. **单击“删除”。**
   将显示“删除角色”确认页。
4. **单击“确定”以删除一个或多个角色。**

▼ 将资源或资源组分配给角色

第 103 页中的“什么是角色？”和第 104 页中的“运用角色类型”中介绍了 Identity Manager 的资源和资源组分配要求。在将资源分配给角色之前，您应该了解此信息。

如果得到角色所有者批准，Identity Manager 将更改角色的资源和资源组分配。

1. **搜索要向其添加资源或资源组的 IT 角色或应用程序。有关如何搜索角色的说明，请参见第 118 页中的“搜索角色”或第 119 页中的“查看角色”。**
2. **单击以打开该角色。**
3. **在“编辑角色”页中单击“资源”选项卡。**
4. **要分配某个资源，请在“可用资源”列中选中该资源，然后单击箭头按钮将其移到“当前资源”列中。**
5. **如果要分配多个资源，则可以指定更新这些资源的顺序：选中“按顺序更新资源”复选框，然后使用 + 和 - 按钮更改“当前资源”列中的资源顺序。**
6. **要将资源组分配给此角色，请在“可用资源组”列中将其选中，然后单击箭头按钮以将其移到“当前资源组”列中。资源组是一个资源集合，它提供了另外一种方法来指定创建和更新资源帐户的顺序。**
7. **要针对每个资源为此角色指定帐户属性，请在分配的资源部分中单击“设置属性值”。有关详细信息，请参见第 144 页中的“查看或编辑资源帐户属性”。**
8. **单击“保存”以打开“确认角色更改”页。**
   将打开“确认角色更改”页。

9 **在“更新分配的用户”部分中，选择一个“更新分配的用户”菜单选项。有关详细信息，请参见第 127 页中的“更新分配给用户的角色”。**

10 **单击“保存”以保存资源分配。**

▼ 删除分配给角色的资源或资源组

如果得到角色所有者批准，Identity Manager 将从角色中删除资源或资源组。当用户收到角色更新时，将从用户中删除已删除的资源。（有关详细信息，请参见第 127 页中的“更新分配给用户的角色”。）在删除资源时，用户将失去该资源的权利，除非还将该资源直接分配给用户。

1 **搜索要从中删除资源或资源组的 IT 角色或应用程序。请按照第 118 页中的“搜索角色”或第 119 页中的“查看角色”中的说明搜索角色。**

2 **单击以打开该角色。**

将打开“编辑角色”页。

3 **在“编辑角色”页中单击“资源”选项卡。**

4 **要删除资源，请在当前资源列中将其选中，然后单击箭头按钮以将其移到可用资源列中。**

要删除资源组，请在当前资源组列中将其选中，然后单击箭头按钮以将其移到可用资源组列中。

5 **单击“保存”。**

将打开“确认角色更改”页。

6 **在“更新分配的用户”部分中，选择一个“更新分配的用户”菜单选项。有关详细信息，请参见第 127 页中的“更新分配给用户的角色”。**

7 **单击“保存”以完成更改。**

管理用户角色分配

角色是在 Identity Manager 的“帐户”区域中分配给用户的。

▼ 将角色分配给用户

可以使用以下过程将一个或多个角色分配给用户。

最终用户也可以为其自己请求分配角色。（只能请求已将父角色分配给用户的可选角色。）有关最终用户如何请求可用角色的信息，请参见第 36 页中的 “Identity Manager 最终用户界面”一节中的第 37 页中的 ““请求”选项卡”。

1. **在管理员界面中，单击“帐户”选项卡。**
   将打开“列出帐户”子选项卡。

2. **要将角色分配给现有用户，请执行以下步骤：**

   a. **单击“用户列表”中的用户名称。**

   b. **单击“角色”选项卡。**

   c. **单击“添加”，将一个或多个角色添加到用户帐户中。**
      默认情况下，只能将业务角色直接分配给用户。（如果 Identity Manager 安装是从 8.0 之前版本升级的，则可以将业务角色和 IT 角色直接分配给用户。）

   d. **在角色表中，选择要分配给用户的角色，然后单击“确定”。**
      要按名称、类型或描述的字母顺序对该表进行排序，请单击列标题。再次单击可按相反的顺序进行排序。要按角色类型过滤该列表，请从“当前”下拉菜单中进行选择。

      将更新该表以显示选定的角色分配以及与父角色分配有关的任何必需角色分配。

   e. **单击“添加”，以查看也可以分配给用户的可选角色分配。**
      选择要分配给用户的可选角色，然后单击“确定”。

   f. **（可选）在“激活日期”列中，选择使角色变为活动状态的日期。如果没有指定日期，在指定的角色所有者批准角色分配时，角色分配将立即变为活动状态。**
      要使角色分配转变为临时状态，请在“取消激活日期”列中选择使角色变为非活动状态的日期。角色取消激活将在选定日期开始生效。

      有关详细信息，请参见第 125 页中的 “在特定日期激活和取消激活角色”。

   g. **单击“保存”。**

在特定日期激活和取消激活角色

在将角色分配给用户时，您可以指定激活日期和取消激活日期。在进行分配时，将创建角色分配工作项目请求。不过，如果在预定激活日期之前没有批准角色分配，则不会分配该角色。角色激活和取消激活将在预定日期午夜稍后的时间（凌晨 0:01）进行。

默认情况下，仅业务角色可以具有激活和取消激活日期。所有其他角色类型继承直接分配给用户的业务角色的激活日期和取消激活日期。可以将 Identity Manager 配置为允许其他角色类型具有可直接分配的激活和取消激活日期。有关说明，请参见第 132 页中的 “配置角色类型”。

▼ 编辑延迟任务扫描程序进度表

延迟任务扫描程序扫描用户角色分配，并根据需要激活和取消激活角色。默认情况下，延迟任务扫描程序任务每小时运行一次。

1. **在管理员界面中，单击“服务器任务”。**
2. **单击次级菜单中的“管理进度表”。**
3. **在“可调度的任务”部分中，单击“延迟任务扫描程序 TaskDefinition”。**

   将打开“创建新的延迟任务扫描程序任务进度表”页。
4. **填写表单。有关帮助，请参阅 i-Helps 和联机帮助。**

   要指定应运行任务的日期和时间，请在开始日期中使用 `mm/dd/yyyy hh:mm:ss` 格式。例如，要计划在 2008 年 9 月 29 日晚上 7:00 开始运行任务，请键入 `09/29/2008 19:00:00`。

   在“结果选项”下拉菜单中，选择“重命名”。如果选择等待，直到删除以前的结果时，才会运行该任务的以后实例。有关各种结果选项设置的详细信息，请参见联机帮助。
5. **单击“保存”以保存该任务。**

   图 5–9 显示了延迟任务扫描程序任务的预定任务表单。

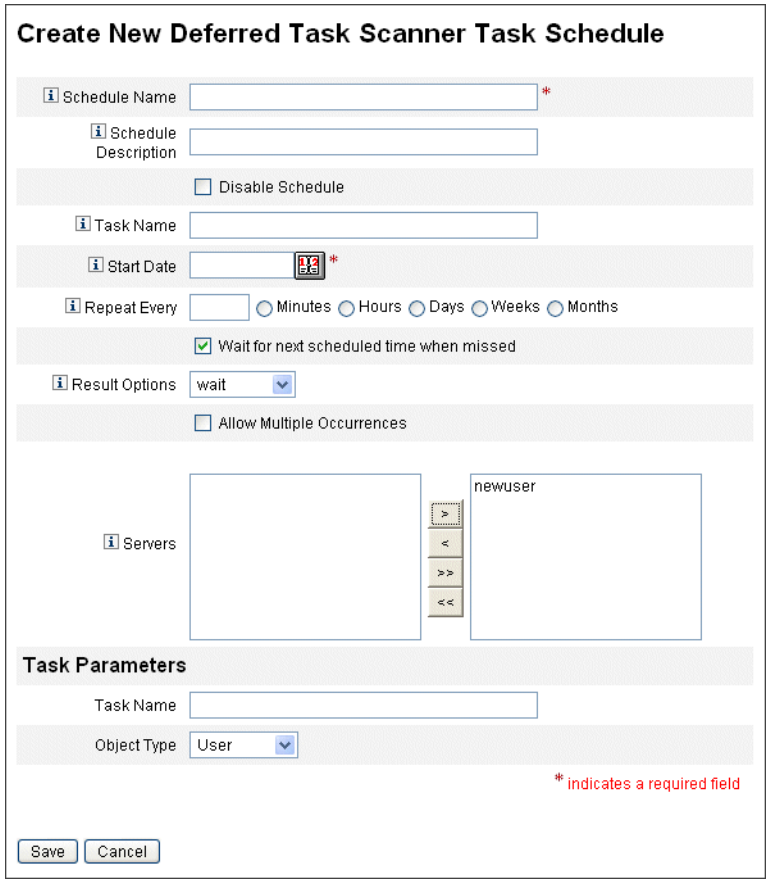


图 5–9 延迟任务扫描程序的预定任务表单

更新分配给用户的角色

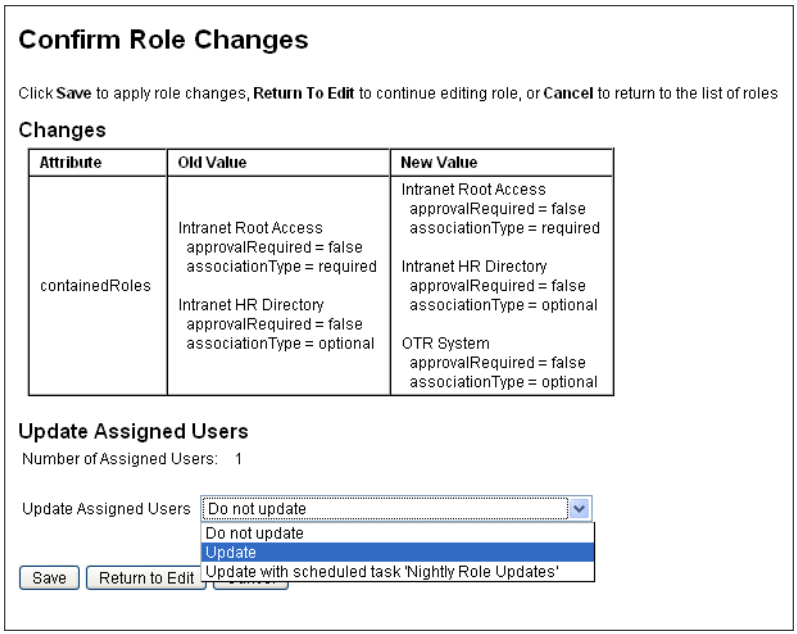
在编辑分配给用户的角色时，您可以选择使用新角色更改立即更新用户，或者将更新推迟到在预定维护时段运行。

在对角色进行更改时，将打开“确认角色更改”页。第 127 页中的“更新分配给用户的角色”中显示了“确认角色更改”页。

- 该页的“更新分配的用户”部分显示了当前分配了该角色的用户数。
- 使用“更新分配的用户”菜单可选择是使用新角色更改立即更新用户（更新），将用户更新推迟到以后的某个时间进行（不更新），还是选择自定义的预定更新任务。
  - 由于更新会立即更新用户，如果这会影响到很多用户，则应该避免选择该选项。用户更新可能需要花费很多时间并占用大量资源。如果需要更新很多用户，最好将更新安排在非峰值时间进行。

- 如果为角色选择了“不更新”，则在管理员查看用户的用户配置文件或者通过“更新角色用户”任务更新用户后，分配给该角色的用户才会收到角色更新。有关计划更新角色用户任务的信息，请参见下一节。
- 如果创建了“更新角色用户”任务进度表，则可以从菜单中选择该进度表。选定的“更新角色用户”任务将根据为该任务定义的进度表更新分配给该角色的用户。有关详细信息，请参见下一节。

  第 127 页中的“更新分配给用户的角色”显示了“确认角色更改”页。“更新分配的用户”部分显示了当前分配了该角色的用户数。“更新分配的用户”下拉菜单包含两个默认选项：“不更新”和“更新”。也可以从预定更新角色用户任务列表中进行选择。有关创建预定更新角色用户任务的说明，请参见第 129 页中的“计划更新角色用户任务”。



▼ 手动更新分配的用户

可通过选择一个或多个角色并单击“更新分配的用户”按钮，更新分配给角色的用户。此过程为指定角色运行更新角色用户任务实例。

1. **按照第 118 页中的“搜索角色”或第 119 页中的“查看角色”中的说明，搜索一个或多个应更新为其分配的用户的角色。**
2. **使用复选框选择角色。**

3 **单击“更新分配的用户”。**
将显示“更新为角色分配的用户”页（图 5–10）。

4 **单击“启动”以开始进行更新。**

5 **单击主菜单中的“服务器任务”，然后单击次级菜单中的“所有任务”以检查更新角色用户任务的状态。**

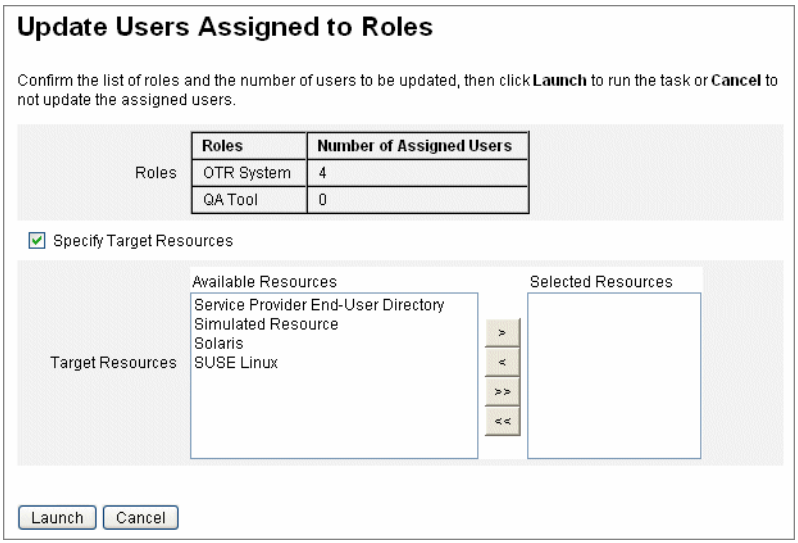


图 5–10 “更新为角色分配的用户”页

▼ 计划更新角色用户任务

注 – 应计划定期运行更新角色用户任务。

请按如下方式计划更新角色用户任务，以使用未完成的角色更改更新用户：

1 **在管理员界面中，单击“服务器任务”。**

2 **单击次级菜单中的“管理进度表”。**

3 **在“可调度的任务”部分中，单击“更新角色用户 TaskDefinition”。**
将打开“创建新的更新角色用户任务进度表”页；如果编辑现有任务，则会打开“编辑任务进度表”页（图 5–11）。

4 **填写表单。有关帮助，请参阅 i-Helps 和联机帮助。**

要指定应运行任务的日期和时间，请在开始日期中使用 `mm/dd/yyyy hh:mm:ss` 格式。例如，要计划在 2008 年 9 月 29 日晚上 7:00 开始运行任务，请键入 `09/29/2008 19:00:00`。

在“结果选项”下拉菜单中，选择“重命名”。如果选择等待，直到删除以前的结果时，才会运行该任务的以后实例。有关各种结果选项设置的详细信息，请参见联机帮助。

5 **单击“保存”以保存该任务。**

图 5–11 显示了更新角色用户任务的预定任务表单。可以将特定角色分配给特定的更新角色用户任务（如“任务参数”一节中所示）。有关详细信息，请参见第 127 页中的“更新分配给用户的角色”。

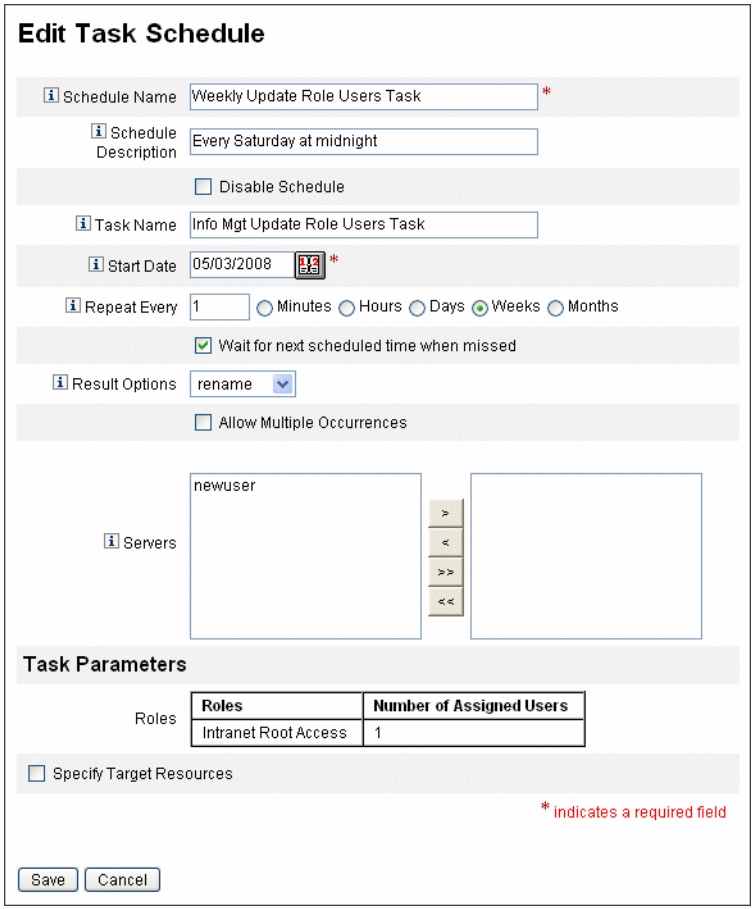


图 5–11 “更新角色用户”的预定任务表单

▼ 查找分配给特定角色的用户

您可以搜索分配了特定角色的用户。

1. **在管理员界面中，单击“帐户”。**
2. **单击次级菜单中的“查找用户”。将打开“查找用户”页。**
3. **找到分配了[选择角色类型]角色的搜索类型用户。**
4. **选择选项框，然后使用“选择角色类型”下拉菜单过滤可用角色列表。**
   将打开第二个角色菜单。
5. **选择一个角色。**
6. **清除其他搜索类型复选框，除非您要进一步缩小搜索范围。**
7. **单击“搜索”。**

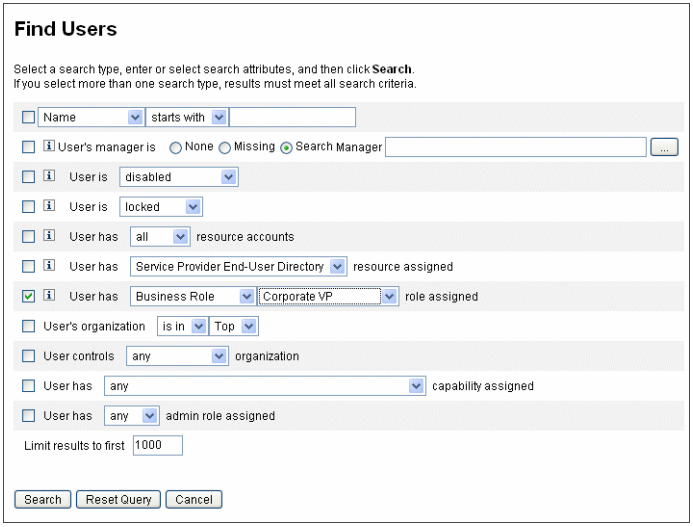


图 5–12 使用“查找用户”页搜索分配了角色的用户

▼ 从用户中删除一个或多个角色

通过使用“编辑用户”页，可以从用户帐户中删除一个或多个角色。只能删除直接分配的角色。在删除父角色时，将会删除间接分配的角色（即条件和/或必需**包含角色**）。另一种从用户中删除间接分配的角色的方法是，从父角色中删除角色（请参见第 121 页中的“删除分配给其他角色的角色”）。

最终用户也可以请求从其用户帐户中删除分配的角色。请参见第 36 页中的 “Identity Manager 最终用户界面”一节中的第 37 页中的 ““请求”选项卡”。

有关使用预定取消激活日期删除角色的信息，请参见第 125 页中的 “在特定日期激活和取消激活角色”。

1. **在管理员界面中，单击“帐户”选项卡。**
   将打开“列出帐户”子选项卡。
2. **单击要从中删除角色的用户。**
   将打开“编辑用户”页。
3. **单击“角色”选项卡。**
4. **在“角色”表中，选择要从用户中删除的角色，然后单击“确定”。**
   要按名称、类型、激活日期、取消激活日期、分配者或状态的字母顺序对该表进行排序，请单击列标题。再次单击可按相反的顺序进行排序。要按角色类型过滤该列表，请从“当前”下拉菜单中进行选择。

   该表将显示父角色分配（可以选择这些角色）以及与父角色分配有关的任何角色分配（无法选择这些角色）。
5. **单击“删除”。**
   将更新分配的角色表以显示其余的分配角色。
6. **单击“保存”。**
   将打开“更新资源帐户”页。取消选择不希望删除的任何资源帐户。
7. **单击“保存”以保存更改。**

配置角色类型

可通过编辑角色配置对象来修改角色类型功能。

▼ 将角色类型配置为可直接分配给用户

默认情况下，只能将某些角色类型直接分配给用户。要更改这些设置，请执行以下步骤。

注 – 建议的最佳做法是仅将业务角色直接分配给用户。有关详细信息，请参见第 105 页中的 “使用角色类型设计灵活的角色”。

要更改可直接分配给用户的角色类型，请执行以下步骤：

1. 按照第 102 页中的“编辑 Identity Manager 配置对象”中的步骤，打开要编辑的角色配置对象。

2. 找到与要编辑的角色类型对应的角色对象。

   - 要编辑 IT 角色，请找到 `Object name='ITRole'`
   - 要编辑应用程序角色，请找到 `Object name='ApplicationRole'`
   - 要编辑资产角色，请找到 `Object name='AssetRole'`

3. 指定一组指令以更新配置。

   根据所需的配置更新方式，选择以下选项之一：

   - 要修改角色类型以使其能直接分配给用户，请在角色对象中找到以下 `userAssignment` 属性：

     ```
     <Attribute name='userAssignment'>
             <Object/>
         </Attribute>
     ```

     将其替换为以下内容：

     ```
     <Attribute name='userAssignment'>
             <Object>
                 <Attribute name='manual' value='true'/>
              </Object>
         </Attribute>
     ```

   - 要修改角色类型以使其不能直接分配给用户，请在角色对象中找到 `userAssignment` 属性并删除 `manual` 属性，如下所示：

     ```
     <Attribute name='userAssignment'>
             <Object>
             </Object>
         </Attribute>
     ```

4. 保存角色配置对象。无需重新启动应用服务器即可使更改生效。

▼ 使角色类型具有可分配的激活日期和取消激活日期

默认情况下，仅业务角色可以具有激活日期和取消激活日期，可以在分配角色时指定这些日期。所有其他角色继承直接分配给用户的业务角色的激活日期或取消激活日期。

注 – 建议的最佳做法是仅将业务角色直接分配给用户。有关详细信息，请参见第 105 页中的 “使用角色类型设计灵活的角色”。

如果选择允许将其他角色类型直接分配给用户（例如，IT 角色类型），您可能还希望能够为该角色类型分配激活和取消激活日期。

可以使用以下步骤更改具有可分配的激活日期和取消激活日期的角色类型：

1. **按照第 102 页中的 “编辑 Identity Manager 配置对象”中的步骤，打开要编辑的角色配置对象。**

2. **找到与要编辑的角色类型对应的角色对象。**

   - 要编辑业务角色，请找到 `Object name='BusinessRole'`
   - 要编辑 IT 角色，请找到 `Object name='ITRole'`
   - 要编辑应用程序角色，请找到 `Object name='ApplicationRole'`
   - 要编辑资产角色，请找到 `Object name='AssetRole'`

3. **指定一组指令以更新配置。**

   根据所需的配置更新方式，选择以下选项之一：

   - 要修改角色类型以使其具有可直接分配的激活日期和取消激活日期，请在角色对象中找到以下 `userAssignment` 属性：

     ```
     <Attribute name='userAssignment'>
             <Attribute name='manual' value='true'/>
          </Attribute>
     ```

     将其替换为以下内容：

     ```
     <Attribute name='userAssignment'>
             <Object>
                 <Attribute name='activateDate' value='true'/>
                  <Attribute name='deactivateDate' value='true'/>
                  <Attribute name='manual' value='true'/>
             </Object>
         </Attribute>
     ```

   - 要修改角色类型以使其不能具有可直接分配的激活日期和取消激活日期，请在角色对象中找到 `userAssignment` 属性并删除 `activateDate` 和 `deactivateDate` 属性，如下所示：

     ```
     <Attribute name='userAssignment'>
             <Object>
             </Object>
         </Attribute>
     ```

4 保存角色配置对象。无需重新启动应用服务器即可使更改生效。

▼ 启用或禁用更改批准和更改通知工作项目

默认情况下，将为所有角色类型启用更改批准工作项目。这意味着，每次更改角色（无论是业务角色、IT 角色、应用程序还是资产）时，如果角色具有所有者，则必须得到所有者批准才能进行更改。

有关更改批准和更改通知工作项目的详细信息，请参见第 117 页中的 “启动更改批准工作项目和批准工作项目”。

可以使用以下步骤为角色类型启用或禁用更改批准工作项目和更改通知工作项目：

1 **按照第 102 页中的 “编辑 Identity Manager 配置对象”中的步骤，打开要编辑的角色配置对象。**

2 **找到与要编辑的角色类型对应的角色对象。**

- 要编辑业务角色，请找到 `Object name='BusinessRole'`
- 要编辑 IT 角色，请找到 `Object name='ITRole'`
- 要编辑应用程序角色，请找到 `Object name='ApplicationRole'`
- 要编辑资产角色，请找到 `Object name='AssetRole'`

3 **找到位于 `<Object>` 元素（位于 `<Attribute name='features'>` 元素中）中的以下属性：**

```
<Attribute name='changeApproval' value='true'/>
 <Attribute name='changeNotification' value='true'/>
```

4 **根据需要，将属性值设置为 true 或 false。**

5 **根据需要重复步骤 2-4 以配置其他角色类型。**

6 **保存角色配置对象。无需重新启动应用服务器即可使更改生效。**

▼ 配置“列出角色”页可加载的最大行数

管理员界面中的“列出角色”页可以显示一定数量的行，您可以配置显示的最大行数。默认数目为 500。可以使用本节中的步骤更改该数字。

可以使用以下步骤更改“列出角色”页可显示的最大行数：

1 **按照第 102 页中的 “编辑 Identity Manager 配置对象”中的步骤，打开要编辑的角色配置对象。**

2 **找到以下属性并更改属性值：**

```
<Attribute name='roleListMaxRows' value='500'/>
```

3 保存角色配置对象。无需重新启动应用服务器即可使更改生效。

同步 Identity Manager 角色和资源角色

可以将 Identity Manager 角色与某资源上本地创建的角色同步。默认情况下，同步时资源被分配给角色。这适用于使用同步任务创建的角色以及与某个资源角色名匹配的现有 Identity Manager 角色。

▼ 将 Identity Manager 角色与资源角色同步

1 在管理员界面中，单击主菜单中的“服务器任务”。

2 单击“运行任务”。将打开“可用任务”页。

3 单击“使 Identity System 角色与资源角色同步”任务。

4 填写表单。有关详细信息，请单击“帮助”。

5 单击“启动”。

了解和管理 Identity Manager 资源

阅读本节的信息和过程可以帮助您设置 Identity Manager 资源。

什么是资源？

Identity Manager 资源存储了关于如何与要在其中创建帐户的某个资源或系统相连接的信息。Identity Manager 资源定义有关某个资源的相关属性，并帮助指定如何在 Identity Manager 中显示资源信息。

Identity Manager 提供类型广泛的资源，包括：

- 主机安全管理器
- 数据库
- 目录服务
- 操作系统
- 企业资源计划 (ERP) 系统
- 消息平台

界面中的资源区域

Identity Manager 在“资源”页上显示关于现有资源的信息。

要访问资源，请选择菜单栏上的“资源”。

资源列表中的资源是按类型进行分组的。每种资源类型由一个文件夹图标表示。要查看当前定义的资源，请单击文件夹旁边的指示符。再次单击指示符可折叠视图。

当展开资源类型文件夹后，它会动态更新并显示包含的资源对象数量（如果它是支持多个组的资源类型）。

有些资源含有可以管理的附加对象，包括以下对象：

- 组织
- 组织单位
- 组
- 角色

从资源列表中选择一个对象，然后从以下某个选项列表中进行选择，以启动一个管理任务：

- **资源操作**。用于对资源执行一系列操作，包括编辑、活动同步、重命名和删除；还可以使用资源对象和管理资源连接。
- **资源对象操作**。编辑、创建、删除、重命名、另存为和查找资源对象。
- **资源类型操作**。编辑资源策略、使用帐户索引和配置受管理的资源。

当您创建或编辑资源时，Identity Manager 会启动 `ManageResource` 工作流。此工作流将新建资源或更新的资源保存在信息库中，并允许您在创建或保存该资源前插入批准或其他操作。

管理资源列表

在创建新的资源之前，必须指示 Identity Manager 您希望能够管理哪些资源类型。要启用资源并创建自定义资源，请使用“配置受管理的资源”页。

▼ 打开“配置受管理的资源”页

可以使用以下步骤打开“配置受管理的资源”页：

1. **登录到管理员界面。**
2. **单击“资源”选项卡。**

可以使用下面的某种方法打开“配置受管理的资源”页：

- 找到“资源类型操作”下拉列表，然后选择“配置受管理的资源”。
- 单击“配置类型”选项卡。

将打开“配置受管理的资源”页。

该页包含三个部分：

- **资源连接器**。此部分列出了资源连接器类型、连接器版本以及连接器服务器。
- **资源适配器**。此部分列出了大型企业环境中的常见资源类型。“版本”列中列出了连接到资源的 Identity Manager 适配器版本。
- **自定义资源适配器**。此部分用于将自定义资源添加到资源列表中。

▼ 启用资源类型

可以使用以下步骤从“配置受管理的资源”页中启用资源类型：

1. **如果尚未打开“配置受管理的资源”页（第 137 页中的“管理资源列表”），请将其打开。**
2. **在“资源”部分中，在“受管理？”列选中要启用的资源类型的框。**
   要启用所有列出的资源类型，请选择“管理所有资源”。
3. **单击页面底部的“保存”。**
   该资源将添加到资源列表中。

▼ 添加自定义资源

可以使用以下步骤从“配置受管理的资源”页中添加自定义资源：

1. **如果尚未打开“配置受管理的资源”页（第 137 页中的“管理资源列表”），请将其打开。**
2. **在“自定义资源”部分中单击“添加自定义资源”，以便在表中添加一行。**
3. **输入资源的资源类路径或输入您自定义创建的资源。有关随 Identity Manager 提供的适配器，请参见《 Sun Identity Manager 8.1 Resources Reference 》以了解完整的类路径。**
4. **单击“保存”将资源添加到“资源”列表。**

▼ 创建资源

在启用资源类型后，您可以随后在 Identity Manager 中创建该资源的实例。要创建资源，请使用**资源向导**。

资源向导将指导您完成设置以下项的过程：

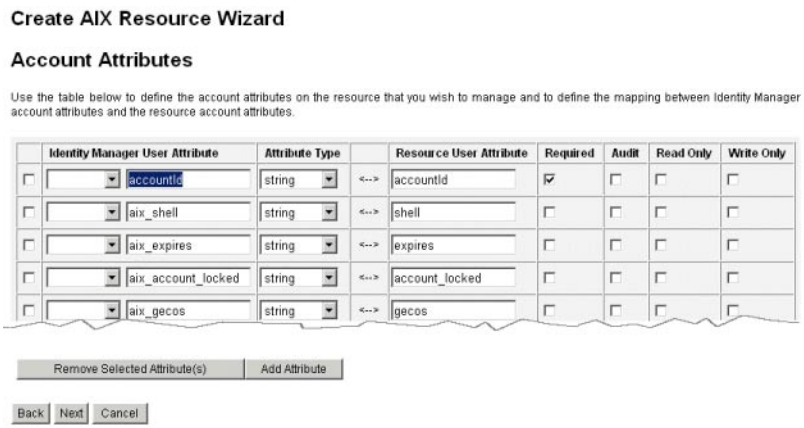
- **资源特定的参数**。创建此资源类型的具体实例时，可以从 Identity Manager 界面修改这些值。
- **帐户属性**。在资源的模式映射中定义。这些值确定 Identity Manager 用户属性如何与资源上的属性映射。
- **帐户 DN 或身份模板**。包括用户的帐户名语法，它对分层名称空间尤其重要。
- **资源的 Identity Manager 参数**。设置策略、建立资源批准者，并设置组织对资源的访问权限。

1. **登录到管理员界面。**
2. **单击“资源”选项卡。确保选中了“列出资源”子选项卡。**
3. **找到“资源类型操作”下拉列表，然后选择“新建资源”。**
   将打开“新建资源”页。
4. **从下拉列表中选择一种资源类型。（如果没有列出要查找的资源类型，您需要将其启用。请参见第 137 页中的“管理资源列表”。）**
5. **单击“新建”以显示“资源向导”欢迎页。**
6. **单击“下一步”开始定义资源。**
   “资源向导”步骤和页面按以下顺序显示：
   - **资源参数**。设置控制验证和资源适配器行为的资源特定参数。输入参数，然后单击“测试连接”，以确保连接有效。在确认连接有效后，单击“下一步”设置帐户属性。

     下图显示了 Solaris 资源的“资源参数”页。对于不同的资源，该页上的表单字段也不相同。

- **帐户属性（模式映射）**。将 Identity Manager 帐户属性映射到资源帐户属性。有关资源帐户属性的详细信息，请参见第 144 页中的“查看或编辑资源帐户属性”。
  - 要添加属性，请单击“添加属性”。
  - 要删除一个或多个属性，请选中属性旁边的框，然后单击“删除选定的属性”。

  下图显示了“资源向导”中的“帐户属性”页。



注 – 如果要将属性导出到 EXT_RESOURCEACCOUNT_ACCTATTR 表中，必须选中要导出的每个属性的“审计”框。

完成后，单击“下一步”以设置身份模板。

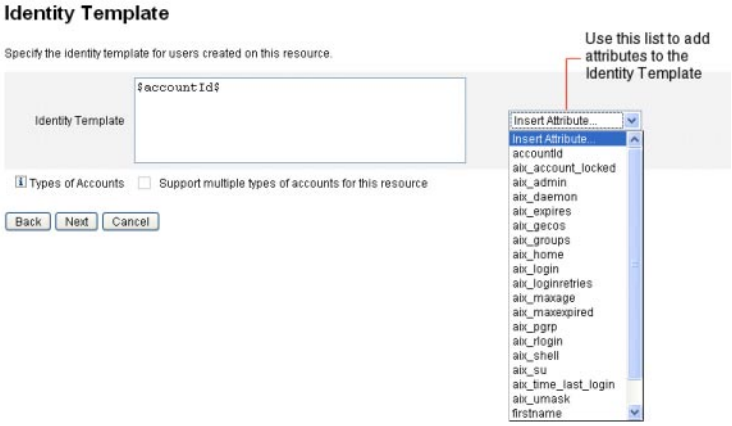
- **身份模板**。定义用户的帐户名称语法。此功能对分层结构的名称空间尤其重要。
  - 要在模板中添加属性，请从“插入属性”列表中选择该属性。
  - 要删除属性，请在字符串中突出显示该属性，然后按键盘上的 Delete 键。删除属性名称以及前导和后续的 $（美元符号）字符。
  - **帐户类型**。Identity Manager 提供了将多个资源帐户分配给单个用户的功能。例如，用户可能需要特定资源上的管理员级别帐户以及普通用户帐户。要在该资源上支持多种帐户类型，请选中“帐户类型”复选框。

    注 – 如果尚未创建由子类型 IdentityRule 标识的一个或多个身份生成规则，则无法选中“帐户类型”复选框。由于 accountId 各不相同，因此，不同类型的帐户必须为给定用户生成不同的 accountId。身份生成规则指定了应如何创建这些唯一的 accountId。

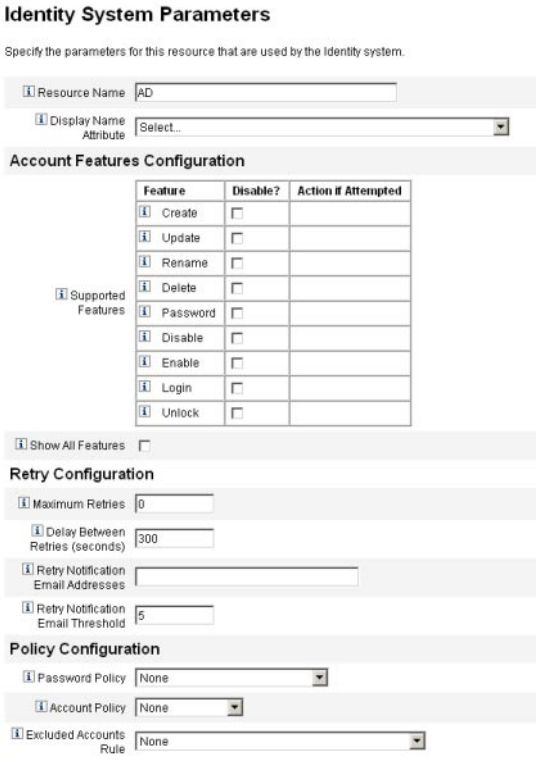
    sample/identityRules.xml 中提供了样例身份规则。

    直到 Identity Manager 中的其他对象不再引用某种帐户类型时，才能删除该帐户类型。另外，也无法重命名帐户类型。

    有关填写“帐户类型”表单的详细信息，请参见 Identity Manager 联机帮助。有关为用户创建多个资源帐户的详细信息，请参见第 54 页中的 “为用户创建多个资源帐户”。



- **Identity System 参数**。为资源设置 Identity Manager 参数，包括重试和策略配置，如第 138 页中的 “创建资源”中所示。



7 **使用“下一步”和“上一步”在页间移动。完成所有选择后，单击“保存”以保存该资源，并返回到列表页。**

管理资源

本节介绍了如何管理现有资源。

这些主题分为以下几个部分：

▼ 查看资源列表

您可以从“资源列表”中查看现有资源。

1 **登录到管理员界面。**

2 **在主菜单中单击“资源”。**
将在“列出资源”子选项卡上显示资源列表。

▼ 使用资源向导编辑资源

可以使用资源向导来编辑资源参数、帐户属性以及 Identity System 参数。也可以指定在此资源上创建的用户应使用的身份模板。

1 **在 Identity Manager 管理员界面中，单击主菜单中的“资源”。**
将在“列出资源”子选项卡上显示资源列表。

2 **选择要编辑的资源。**

3 **在“资源操作”下拉菜单中，选择“资源向导”（在“编辑”下面）。**
将在编辑模式下打开选定资源的资源向导。

▼ 使用资源列表命令编辑资源

除了编辑资源向导外，您还可以使用资源列表命令对资源执行一系列编辑操作。

1 **从资源列表中选择一个或多个选项。**

这些选项包括：

- **删除资源**。选择一个或多个资源，然后从“资源操作”列表中选择“删除”。可以同时选择几种类型的资源。不能删除与任何角色或资源组相关的资源。
- **搜索资源对象**。选择某个资源，然后从“资源对象操作”列表中选择“查找资源对象”，以便按对象特征查找资源对象（如组织、组织单位、组或个人）。
- **管理资源对象**。对于某些资源类型，可以创建新的对象。选择资源，然后从 "Resource Object Actions" 列表中选择 "Create Resource Object"。
- **重命名资源**。选择某个资源，然后从“资源操作”列表中选择“重命名”。在出现的输入框中输入新的名称，然后单击“重命名”。
- **克隆资源**。选择某个资源，然后从“资源操作”列表中选择“另存为”。在出现的输入框中输入新名称。克隆的资源以选择的名称显示在资源列表中。
- **对资源执行批量操作**。指定一个资源列表和应用（从 CSV 格式的输入）到列表中所有资源的操作。然后启动批量操作以启动批量操作后台任务。

2 **保存所做的更改。**

▼ 查看或编辑资源帐户属性

资源帐户属性（或模式映射）提供了一种抽象方法，以引用受管理资源上的属性。通过使用模式映射，您可以指定如何在 Identity Manager 中引用属性（在模式映射左侧）以及如何将该名称映射到实际资源上的属性名称（在模式映射右侧）。可随后在表单或工作流定义中引用 Identity Manager 属性名称，并有效地引用资源本身上的属性。

下面显示了 Identity Manager 中的属性与 LDAP 资源属性之间的映射示例：

Identity Manager 属性		LDAP 资源属性
`firstname`	`<-->`	`givenName`
`lastname`	`<-->`	`sn`

在对该资源执行操作时，对 Identity Manager 属性 `firstname` 的任何引用实际上是引用 LDAP 属性 `givenName`。

在 Identity Manager 中管理多个资源时，通过将通用 Identity Manager 帐户属性映射到多个资源属性，可以大大简化资源管理。例如，可以将 Identity Manager `fullname` 属性映射到 Active Directory 资源属性 `displayName`。同时，在 LDAP 资源上，可以将相同的 Identity Manager `fullname` 属性映射到 LDAP 属性 `cn`。这样，管理员只需要提供一次 `fullname` 值。在保存用户时，`fullname` 值将传递给具有不同属性名称的资源。

通过在资源向导的“帐户属性”页上建立模式映射，您可以执行以下操作：

- 为来自受管理的资源的属性定义属性名称和数据类型
- 将资源属性限制在公司或组织需要的范围内
- 创建与多个资源共用的公共 Identity Manager 属性名称
- 确定所需用户属性和属性类型

要查看或编辑资源帐户属性，请执行以下步骤：

1 **在管理员界面中，单击“资源”。**

2 **选择要查看或编辑帐户属性的资源。**

3 **在“资源操作”列表中，单击“编辑资源模式”。**

将打开“编辑资源帐户属性”页。

模式映射左侧的列（标题为 Identity System 用户属性）包含 Identity Manager 帐户属性的名称，Identity Manager 管理员界面和用户界面中使用的表单将引用这些名称。模式映射的右列（标题为 "Resource User Attribute"）包含来自外部源的属性名称。

资源组

可以使用资源区域来管理资源组，以使您能够对资源进行分组，以便按特定顺序更新这些资源。通过在组中加入资源并对资源排序，然后将组分配给用户，可确定创建、更新和删除该用户资源的顺序。

活动依次在每个资源上执行。如果某个操作在一个资源上失败，则其余资源不会被更新。这种关系类型对相关资源很重要。

例如，Exchange Server 2007 资源依赖于现有的 Windows Active Directory 帐户。该帐户必须存在，然后才能成功创建 Exchange 帐户。通过使用 Windows Active Directory 资源和 Exchange Server 2007 资源（按顺序）创建资源组，可以确保用户的创建顺序正确无误。反过来，此顺序可以确保删除用户时资源按正确顺序删除。

选择“资源”，然后选择“列出资源组”以显示当前定义的资源组列表。在该页单击“新建”以定义资源组。定义资源组时，有一个选项区域允许您在选择资源后对所选资源排序，并可以选择可以使用该资源组的组织。

全局资源策略

本节介绍了如何编辑全局资源策略以及为资源设置超时值。

▼ 编辑策略属性

可以从“编辑全局资源策略属性”页中编辑资源策略属性。

1 **打开“编辑全局资源策略属性”页，然后根据需要编辑这些属性。**

这些属性包括：

- **默认捕获超时**。输入一个值（以毫秒为单位），以指定在命令行提示之后适配器超时之前，适配器应等待的最长时间。该值仅适用于 GenericScriptResourceAdapter 或 ShellScriptSourceBase 适配器。当命令或脚本的结果很重要且将由适配器解析时，将使用此设置。

  此设置的默认值为 30000（30 秒）。
- **默认等待超时**。输入一个值（以毫秒为单位），以指定在执行检查以查看命令是否具有就绪字符（或结果）之前，脚本化适配器在两次轮询之间应等待的最长时间。该值仅适用于 GenericScriptResourceAdapter 或 ShellScriptSourceBase 适配器。当适配器不检查命令或脚本的结果时，将使用此设置。
- **等待忽略大小写**。输入一个值（以毫秒为单位），以指定适配器在超时之前应等待命令行提示的最长时间。该值仅适用于 GenericScriptResourceAdapter 或 ShellScriptSourceBase 适配器。不区分大小写（大写或小写）时，将使用此设置。
- **资源帐户密码策略**。（如果适用）选择要应用于选定资源的资源帐户密码策略。“无”是默认选项。
- **排除资源帐户规则**。（如果适用）选择管理排除资源帐户的规则。“无”是默认选项。

2 **必须单击“保存”才能保存对策略所做的更改。**

▼ 设置其他超时值

可以通过编辑 `Waveset.properties` 文件来修改 `maxWaitMilliseconds` 属性。`maxWaitMilliseconds` 属性将控制监视操作超时的频率。如果未指定该值，系统将使用默认值 50。

1 **在 `Waveset.properties` 文件中添加以下行：**

```
com.waveset.adapter.ScriptedConnection.ScriptedConnection.maxwaitMilliseconds.
```

2 **保存该文件。**

批量资源操作

通过使用 CSV 格式的文件或通过创建或指定应用于操作的数据可以对资源执行批量操作。

图 5–13 显示了使用创建操作的批量操作的启动页。

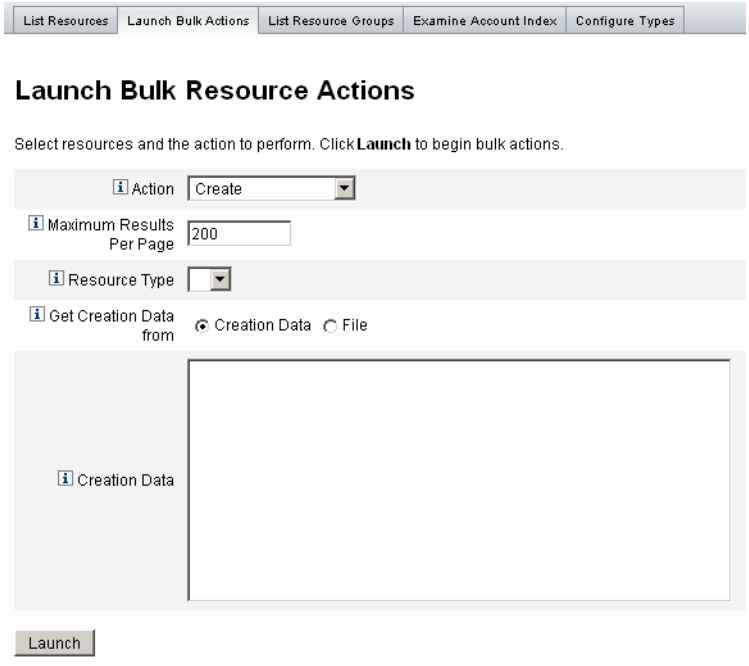


图 5–13 “启动批量资源操作”页

用于批量资源操作的选项取决于为此操作选择的操作。可以指定应用于此操作的单个操作或选择“从操作列表”以指定多个操作。

- **操作**。要指定单个操作，请选择以下选项之一：创建、克隆、更新、删除、更改密码、重设密码。

  对于单个操作选项，系统将显示选项，可以使用这些选项指定与该操作有关的资源。对于创建操作，您需要指定资源类型。

  如果指定“从操作列表”，请使用“操作列表来源”区域指定要使用的包含操作的文件或在“输入”区域中指定的操作。

  注 – 在输入区域列表中或在文件中输入的操作必须为以逗号分隔值 (Comma-separated Value, CSV) 格式。

- **每页最多结果数**。使用此选项可指定在每个任务结果页上显示的批量操作结果的最大数目。默认值为 200。

单击“启动”以启动操作，该操作将作为后台任务运行。

了解和管理外部资源

您还可以使用 Identity Manager 为企业创建、置备和集中管理**外部资源**。

本节介绍了如何使用外部资源，该信息分为以下主题：

什么是外部资源？

外部资源是唯一不能直接存储用户帐户信息的资源类型。该资源在 Identity Manager 工作区之外。这些资源可能是台式计算机、便携式计算机、移动电话和安全徽章等。

置备外部资源几乎始终需要一个或多个手动过程。例如，在提出初始请求并获得为新雇员置备便携式计算机所需的批准后，您可能需要向公司的订购请求系统提交购买请求。在填写订单后，另一个人可能需要使用公司应用程序预配置便携式计算机以完成置备请求，然后才会亲自将便携式计算机交给新雇员。

为什么使用外部资源？

通过使用 Identity Manager 置备外部资源，您可以向一个或多个置备程序通知暂挂请求，其中包括所置备的资源的详细信息。

例如，外部资源置备程序可能是 IT 管理员，他需要为用户手动订购并预配置便携式计算机。

Identity Manager 还可以维护为给定用户置备的外部资源的相关信息，并在完成置备请求后更新该信息。然后，Identity Manager 提供该信息以进行查看、报告、审计遵循性验证以及导出。

注 – 要配置外部资源，您必须具有外部资源管理员权能。要创建新的外部资源，您必须具有资源管理员权能。

配置外部资源

本节介绍了配置外部资源数据存储库以及外部资源置备程序通知的过程。

配置外部资源数据存储库

Identity Manager 的外部资源数据存储库是单个数据存储库，用于保存有关外部资源和外部资源分配的信息。此数据存储库可以是数据库，也可以是目录。

- 如果外部资源数据存储库是**数据库**，则该数据存储库由 ScriptedJdbcResourceAdapter 进行管理。
- 如果外部资源数据存储库是**目录**，则该数据存储库由 LDAPResourceAdapter 进行管理。

注 – 您必须具有外部资源管理员权能才能配置外部资源数据存储库。

通过使用外部资源数据存储库，您可以将数据存储在所需的任意属性值中，并且可以将这些值存储在一个或多个表中。

例如，如果使用的是 MySQL 数据库，则 Identity Manager 将外部资源信息存储在以下表中：

- `extres.accounts` 表包含 accountID 和 resourceID。由于外部资源数据存储库是单个数据存储库，Identity Manager 提供了唯一 ID 关键字 `<accountId>@<resourceId>`，它按 resourceID 唯一地标识了帐户。
- `extres.attributes` 表包含名称/值对属性的集合。在创建外部资源时，您可以在模式映射中定义这些属性。

用于创建数据库表的示例脚本与 Identity Manager 封装在一起，这些脚本位于以下位置：

wshome`/sample/ScriptedJdbc/External`

Identity Manager 支持多种数据库类型，并为每种类型提供了示例脚本。对于特定环境，您可以根据需要修改这些脚本。

外部资源数据存储库还通过使用 LDAPResourceAdapter 来支持 LDAP，这样您便可以将数据存储在现有类或自定义类中。示例 LDIF 脚本也与 Identity Manager 封装在一起，该脚本位于以下位置：

wshome`/sample/other/externalResourcePerson.ldif`

您可以在配置外部资源目录数据存储库过程中修改该脚本。

▼ 配置数据库类型数据存储库

虽然您可以方便地进行更改，但通常仅配置一次外部资源数据存储库。如果您修改了配置，Identity Manager 会自动更新所有现有外部资源以使用新配置的数据存储库。

可以使用以下步骤配置数据库类型数据存储库：

1 从 Identity Manager 管理员界面的菜单栏中选择“配置”→“外部资源”。

2 在显示“数据存储库配置”页时，从“数据存储库类型”菜单中选择“数据库”。将显示其他选项。

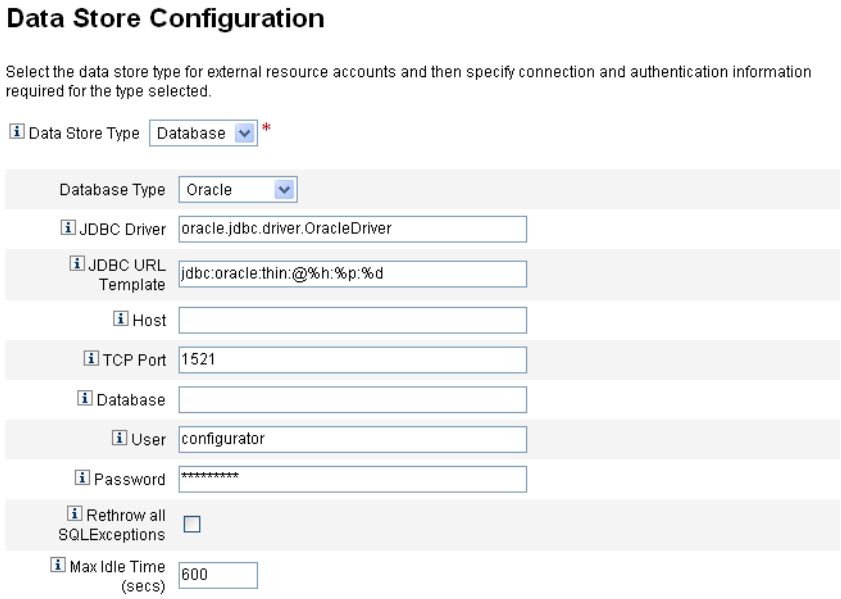


图 5–14 “数据存储库配置”页：数据库

3 指定以下连接和验证信息：

注 – Identity Manager 自动使用默认值填充“JDBC 驱动程序”、“JDBC URL 模板”、“端口”和“最长空闲时间（秒）”字段。如有必要，您可以更改这些默认值。

- **JDBC 驱动程序**。指定 JDBC 驱动程序类名。
- **JDBC URL 模板**。指定 JDBC 驱动程序 URL 模板。
- **主机**。输入运行数据库的主机的名称。
- **TCP 端口**。输入数据库侦听的端口号。
- **数据库**。输入数据库服务器上包含数据存储库表的数据库的名称。
- **用户**。输入有足够权限读取、更新和删除数据存储库表行的数据库用户的 ID。例如，超级用户。
- **密码**。输入数据库用户的密码。

- **重新抛出所有 SQLException**。选中此框可在异常错误代码为 0 时重新抛出 SQL 语句的 SQL 异常。

  如果未启用此选项，Identity Manager 将捕获并禁止这些异常。
- **最长空闲时间**。指定希望 JDBC 连接在池中保持未使用状态的最长时间（秒）。

  如果在指定时间内未使用该连接，Identity Manager 将关闭该连接并将其从池中删除。
  - 默认值为 600 秒。
  - -1 值可防止连接到期

4 **在成功连接到数据存储库后，您必须为每个受支持的资源操作指定一个或多个要执行的脚本。有关说明，请参见第 151 页中的“配置操作脚本”。**

▼ 配置操作脚本

必须指定一组 BeanShell (bsh) 脚本，Identity Manager 可使用这些脚本跟踪和执行给定请求的获取、创建、更新、删除、启用、禁用以及测试状态。

以下位置提供了示例操作脚本：

wshome/sample/ScriptedJdbc/External/beanshell

注 – 可以修改这些示例以创建您自己的自定义操作脚本。自定义脚本将添加到“操作脚本”选择工具中，并显示在“可用”和“已选定”列表中的水平线以下。

对于外部资源支持的任何数据库类型的资源操作，Identity Manager 提供了一些示例脚本。要访问这些脚本，请使用以下位置中提供的 ResourceAction 脚本：

wshome/sample/ScriptedJdbc/External/beanshell

默认数据库名称、用户名和密码均为 extres。

- 如果选择任何其他数据库选项，或者要使用不同的用户名或数据库名称，则必须使用不同的值修改示例数据库创建脚本和 ResourceAction 脚本。

  例如，如果选择 MySQL 数据库，但要更改现有的数据库名称、用户名和密码，则必须进行以下更改：必须通过将默认数据库名称、用户名和密码由 extres 分别更改为 externalresources、externaladmin 和 externalpassword 来更新 create_external_tables.mysql 脚本。
- 接下来，必须将 ResourceAction 脚本的默认 extres.accounts 和 extres.attributes 值分别更改为 externalresources.accounts 和 externalresources.attributes。

可以使用以下步骤配置操作脚本：

1 使用“数据存储库配置”页中的“操作脚本”选择工具为每个资源操作指定一个或多个操作脚本。必须至少为每个资源操作选择一个脚本。

图 5–15 “操作脚本”区域

必须选择与资源操作匹配的默认操作脚本。例如，必须使用

- `External-getUser-bsh` 执行获取用户资源操作

注 – 获取用户资源操作用于执行搜索操作。

- External-createUser-bsh 执行创建用户资源操作
- External-deleteUser-bsh 执行删除用户资源操作
- External-updateUser-bsh 执行更新用户资源操作
- External-disableUser-bsh 执行禁用用户资源操作
- External-enableUser-bsh 执行启用用户资源操作
- External-test-bsh 执行测试资源操作

注 – 测试资源操作用于启用“测试连接”按钮的全部功能。

无法从列表的示例脚本中选择任何其他 bsh 脚本。

2 **从菜单中选择一种操作上下文模式，以指定将属性值传递到操作脚本的方式。**

- **字符串**。将属性值作为字符串值进行传递。
- **直接**。将属性值作为 com.waveset.object.AttributeValues 对象进行传递。

3 **现在是测试数据存储库连接配置的最佳时机。请单击位于页面底部的“测试连接”按钮。**
将显示一条消息，以确认连接成功或报告配置错误。

4 **完成后，单击“下一步”以转至“置备程序通知配置”页。**

▼ 配置目录类型数据存储库

可以使用以下步骤配置目录类型数据存储库。

1 **从“数据存储库类型”菜单中选择“目录”。将显示其他选项。**

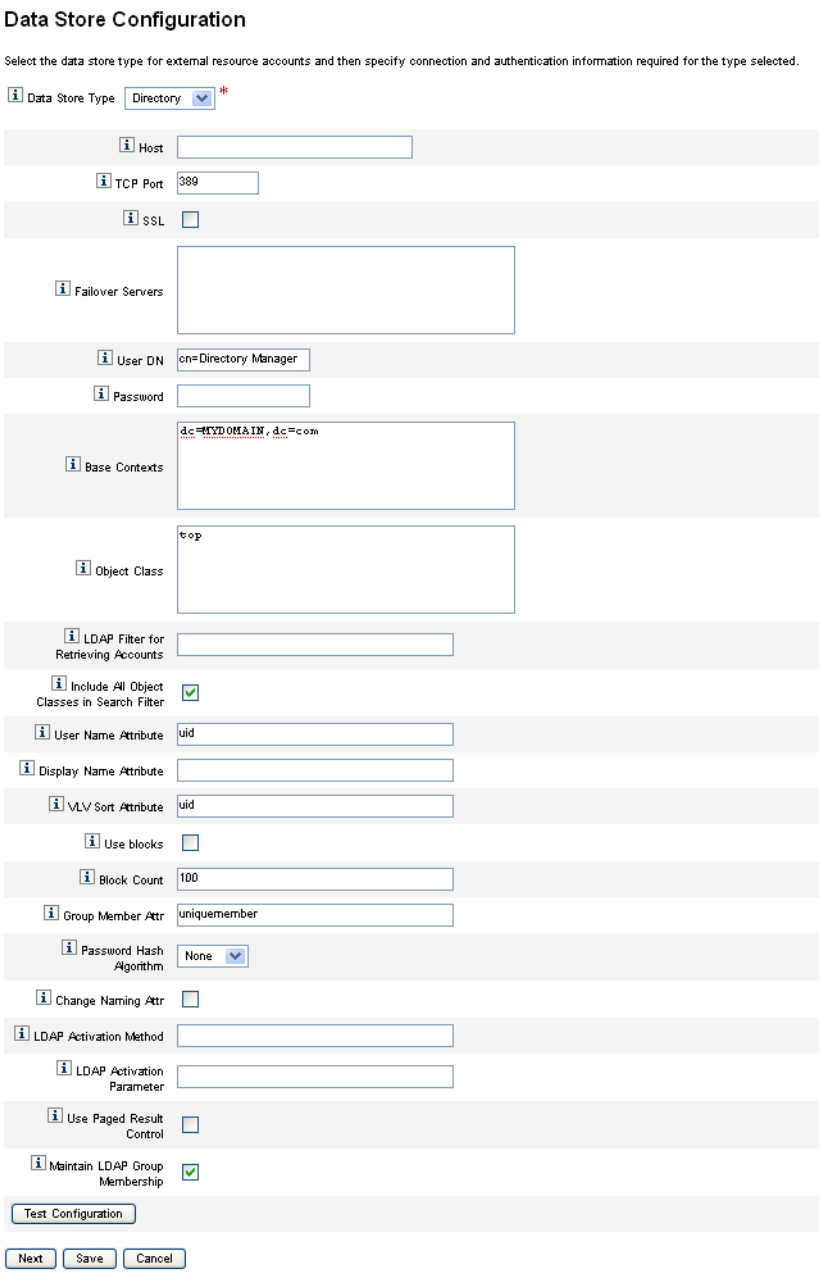


图 5–16 “数据存储库配置”页：目录

2 您必须为目录类型数据存储库指定连接和验证信息。

请配置以下选项：

- **主机**。输入运行 LDAP 服务器的主机的 IP 地址或名称。
- **TCP 端口**。输入用于与 LDAP 服务器通信的 TCP/IP 端口。
  - 如果使用的是 SSL，该端口通常为 636。
  - 如果使用的不是 SSL，该端口通常为 389。
- **SSL**。选中此选项可使用 SSL 连接到 LDAP 服务器。
- **故障转移服务器**。列出首选服务器发生故障时所使用的所有故障转移服务器。请使用以下格式（遵循 RFC 2255 中介绍的标准 LDAP 版本 3 URL）输入该信息：

  ```
  ldap://ldap.example.com:389/o=LdapFailover
  ```

  只有 URL 的主机、端口和标识名 (distinguished name, DN) 部分在此设置中是相关的。

  如果首选服务器发生故障，JNDI 将自动连接到此列表中的下一个服务器。
- **用户 DN**。输入在更新时用于进行 LDAP 服务器验证的 DN。（默认为 `cn=Directory Manager`）
- **密码**。输入主体的密码。
- **基本上下文**。指定在 LDAP 树中搜索用户时 Identity Manager 可以使用的一个或多个起始点。（默认为 `dc=MYDOMAIN,dc=com`）

  在尝试从 LDAP 服务器中查找用户或查找用户所属的组时，Identity Manager 将执行搜索。
- **对象类**。输入在 LDAP 树中创建新用户对象时使用的一个或多个对象类。（默认为 top）

  每个条目必须位于单独一行中。不要使用逗号或空格分隔条目。

  某些 LDAP 服务器要求您指定类分层结构中的所有对象类。例如，您可能需要指定 `top`、`person`、`organizationalperson` 和 `inetorgperson`，而不是只使用 `inetorgperson`。
- **用于检索帐户的 LDAP 过滤器**。输入 LDAP 过滤器以控制从 LDAP 资源返回的帐户。如果未指定过滤器，Identity Manager 将返回包含所有指定对象类的所有帐户。
- **在搜索过滤器中包括所有对象类**。选中此框可要求所有帐户都包含每个指定的对象类，并且与“用于检索帐户的 LDAP 过滤器”字段中指定的过滤器相匹配。

注 – 如果未指定任何搜索过滤器，则必须启用此选项。如果禁用此选项，可通过使用“协调”或“从资源加载”功能将不包含所有指定对象类的帐户加载到 Identity Manager 中。

在加载后，不会自动更新帐户的 objectclass 属性。如果通过管理员界面公开缺少对象类的属性，将无法在不修改 objectclass 属性的情况下提供此属性的值。要避免此问题，请覆盖“协调”或“从资源加载”表单中的 objectclass 值。

- **用户名属性**。输入 LDAP 属性的名称，从目录中搜索用户时，该名称会映射到 Identity Manager 用户名称。该名称通常为 uid 或 cn。
- **显示名称属性**。输入资源帐户属性名称，其值将在显示此帐户名称时使用。
- **VLV 排序属性**。输入用于资源上 VLV 索引的排序属性的名称。
- **使用块**。选中此框可采用分块方式检索并处理用户。

  在对大量用户执行操作时，采用分块方式处理用户可减少该操作使用的内存量。
- **块计数**。输入可组合到块中以进行处理的最大用户数目。
- **组成员属性**。输入在组中添加用户时使用用户标识名 (Distinguished Name, DN) 更新的组成员属性名称。

  属性名称取决于组的对象类。例如，Sun Java™ System Enterprise Edition Directory Server 和一些 LDAP 服务器使用包含 groupOfUniqueNames 对象类和 uniqueMember 属性的组。其他 LDAP 服务器使用包含 groupOfUniqueNames 对象类和 member 属性的组。
- **密码散列算法**。输入 Identity Manager 可用于散列密码的算法。支持的值包括：
  - SSHA
  - SHA
  - SMD5
  - MD5

  如果指定 0 或将此字段保留空白，Identity Manager 将不散列密码，并在 LDAP 中存储明文密码，除非 LDAP 服务器执行散列。例如，Sun Java System Enterprise Edition Directory Server 散列密码。
- **更改命名属性**。选中此框可允许修改操作更改代表最左侧相关标识名 (distinguished name, DN) 的用户属性。修改通常会将命名属性更改为 uid 或 cn。
- **LDAP 激活方法**。
  - 如果希望资源使用密码分配执行启用或禁用操作，则将此字段保留空白。
  - 输入对此资源的用户执行激活操作时使用的 nsmanageddisabledrole 关键字、nsaccountlock 关键字或类名。
- **LDAP 激活参数**。根据在“LDAP 激活方法”字段中填写的内容，输入一个值：
  - 如果指定 nsmanageddisabledrole 关键字，则必须使用以下格式输入一个值：

    IDMAttribute=CN=nsmanageddisabledrole,*baseContext*
  - 如果指定 nsaccountlock 关键字，则必须使用以下格式输入一个值：

    IDMAttribute=true
  - 如果指定类名，则必须使用以下格式输入一个值：

IDMAttribute

注 – 有关“LDAP 激活方法”和“LDAP 激活参数”的详细信息，请参见《Sun Identity Manager 8.1 Resources Reference》 。

- **使用分页结果控制**。选中此框可使用 LDAP 分页结果控制在协调期间迭代处理帐户，而不是使用 VLV 控制。

注 – 资源必须支持简单分页控制。

- **保留 LDAP 组成员资格**。选中此框可在重命名或删除用户时让适配器保留 LDAP 组成员资格。

  如果未启用此选项，则 LDAP 资源保留组成员资格。

3 **单击“测试连接”按钮以测试数据存储库连接配置。**

将显示一条消息，以确认连接成功或报告配置错误。

4 **完成后，单击“保存”，然后单击“下一步”以转至“置备程序通知配置”页。**

注 – 您必须先设置有效的帐户属性和身份模板，然后才能在 LDAP 资源上创建用户。

配置置备程序通知

在为外部资源配置数据存储库后，您必须配置置备程序通知。您还可以配置请求程序通知。本节介绍了使用电子邮件或 Remedy 配置通知的过程。

▼ 配置电子邮件通知

注 – 有关电子邮件模板的详细信息，请参见“配置任务模板”。

可以按照以下说明配置电子邮件通知并将其发送到一个或多个置备程序：

1 **在“置备程序通知配置”页中，从“置备程序通知类型”菜单中选择“电子邮件”。将显示其他选项，如下图中所示。**

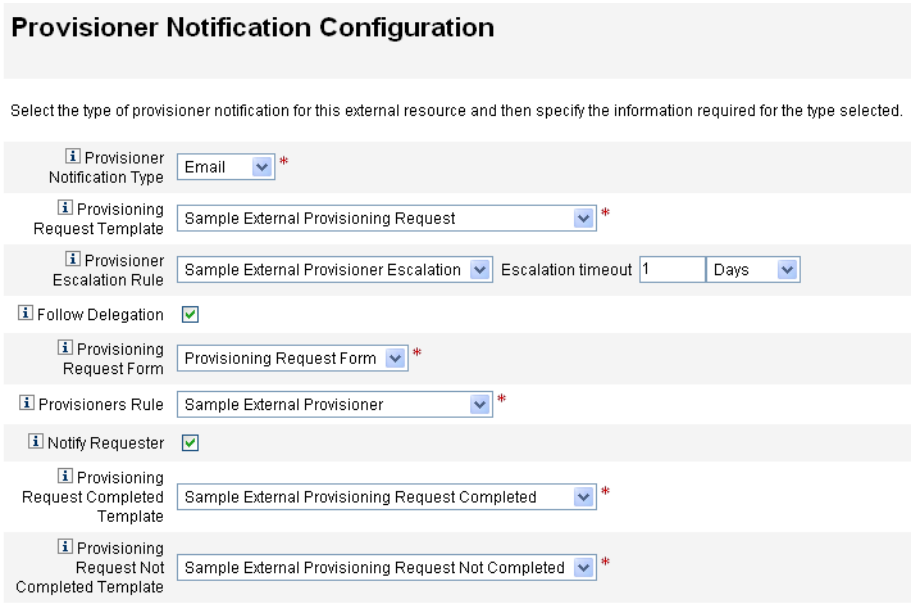


图 5–17 置备程序通知配置页：电子邮件通知类型

2 配置以下选项：

- **置备请求模板**。从菜单中选择“样例外部置备请求”。可以使用此电子邮件模板配置用于向置备程序通知外部资源请求的电子邮件。
- **按照委托**。如果希望 Identity Manager 遵循为置备程序定义的委托，请选中此框。
- **置备程序提升规则（可选）**。选择一个规则以确定在下列情况下将请求提升到的置备程序：当前置备程序在指定的超时时间段内未响应请求。

注 – 虽然此菜单中提供了一些示例规则，但您必须选择**样例外部置备程序提升**规则或使用您自己的自定义规则。样例外部置备程序提升规则使用外部置备程序提升规则确定提升到的置备程序。

- **提升超时**。指定将置备请求提升到下一个置备程序之前等待的最长时间。

注 –

- 如果将此字段保留空白或输入零，则从不提升请求。
- 如果指定超时但未选择“置备程序提升规则”，Identity Manager 将在请求超过指定超时后将请求提升到配置器。如果配置器不存在，则在超时到期后将请求归类为“未完成”。

- **置备请求表单**。选择一个表单，外部资源置备程序可使用该表单将置备请求标记为“已完成”或“未完成”。
- **置备程序规则**。您必须选择一个规则，以定义在为用户分配外部资源时将置备请求发送到的置备程序。

注 –

- 您可以编写自己的规则以达到此目的。您还可以定义多个置备程序。当任何置备程序完成任务时，会将该任务从所有置备程序的队列中删除。有关编写自定义规则的详细信息，请参见《Sun Identity Manager Deployment Reference》中的第 4 章 “Working with Rules”。
- 虽然此菜单中提供了一些示例规则，但您必须选择**样例外部置备程序**规则或使用您自己的自定义规则。样例外部置备程序规则将配置器指定为置备程序。

- **通知请求程序**。选中此框可向原始请求程序回复电子邮件，其中包含对请求执行的操作的相关信息。例如，置备请求是否完成以及是否需要其他信息等。

  在启用此选项时，将显示以下附加字段：

注 –

- **置备请求完成模板**。选择在完成请求时用于通知请求程序的样例外部置备请求完成模板。
- **置备请求未完成模板**。选择在未完成请求时用于通知请求程序的样例外部置备请求未完成模板。

3 **单击“保存”。**

将显示“配置”页，指示您可以继续执行其他配置任务。

4 **转到“资源”→“列出资源”选项卡。您现在可以基于此配置创建各个外部资源。有关说明，请参见第 138 页中的“创建资源”。**

▼ 配置 Remedy 通知

可以按照以下说明创建 Remedy 票证并将其发送到置备程序：

1 从“置备程序通知类型”菜单中选择 "Remedy"。将显示其他选项，如下图中所示。

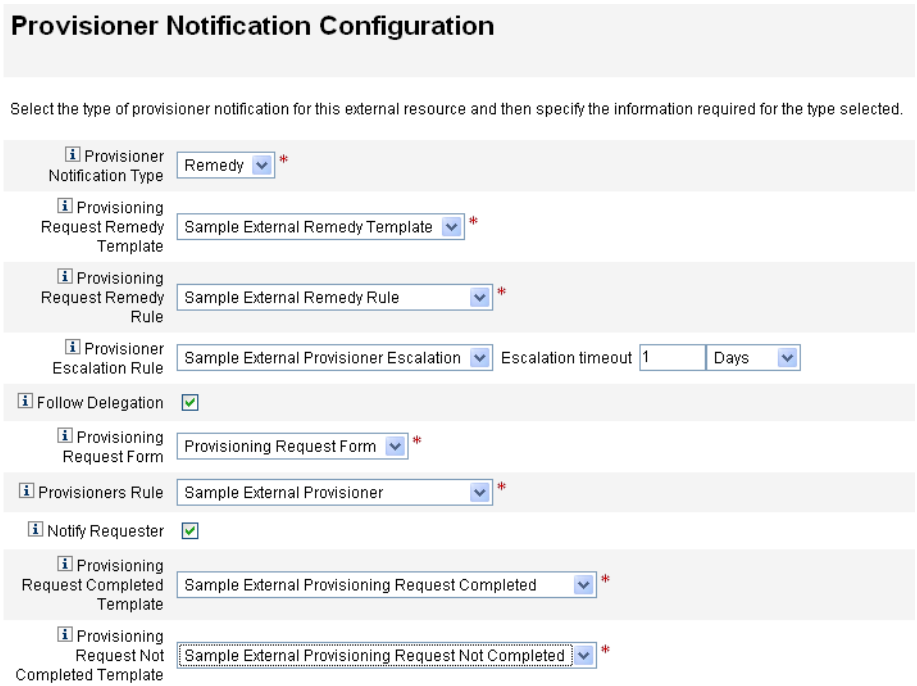


图 5–18 置备程序通知配置页：Remedy 通知类型

2 配置以下选项：

- **置备请求 Remedy 模板**。从菜单中选择“样例外部 Remedy 模板”。

  注 – Identity Manager 提供了一个样例 Remedy 模板，您可以直接使用该模板，也可以根据需要对其进行修改。

  Remedy 模板包含一组用于创建 Remedy 票证的字段。Identity Manager 还使用此模板查询 Remedy 的票证状态，以查看任务是否完成。

- **置备请求 Remedy 规则**。您必须从此菜单中选择一个规则以定义 Remedy 配置设置。

注 – 虽然此菜单中提供了一些示例规则，但您必须选择**样例外部** *Remedy* **规则**或使用您自己的自定义规则。样例外部 Remedy 规则使用 Remedy 规则来确定 Remedy 票证的当前状态是“已完成”还是“未完成”。

Remedy 模板包含一组用于创建 Remedy 票证的字段。Identity Manager 还使用此模板查询 Remedy 的票证状态，以查看任务是否完成。

Identity Manager 使用此规则查询 Remedy 票证以了解状态信息。如果票证状态为“已完成”或“未完成”，则 Identity Manager 将工作项目分别标记为“已完成”或“未完成”。

注 – 您可以编写自己的规则以达到此目的。系统提供了一个样例规则（名为“样例外部 Remedy 规则”），您可以直接使用该规则，也可以根据需要对其进行修改。有关编写自定义规则的详细信息，请参见《Sun Identity Manager Deployment Reference》中的第 4 章 “Working with Rules”。

- **按照委托**。如果希望 Identity Manager 遵循为置备程序定义的委托，请选中此框。
- **置备程序提升规则**（**可选**）。选择一个规则以确定在下列情况下将请求提升到的置备程序：当前置备程序在指定的超时时间段内未响应请求。

注 – 虽然此菜单中提供了一些示例规则，但您必须选择**样例外部置备程序提升**规则或使用您自己的自定义规则。样例外部置备程序提升规则使用外部置备程序提升规则确定提升到的置备程序。

- **提升超时**。指定将置备请求提升到下一个置备程序之前等待的最长时间。

注 –

- 如果将此字段保留空白或输入零，则从不提升请求。
- 如果指定超时但未选择“置备程序提升规则”，Identity Manager 将在请求超过指定超时后将请求提升到配置器。如果配置器不存在，则在超时到期后将请求归类为“未完成”。

- **置备请求表单**。选择一个表单，外部资源置备程序可使用该表单将置备请求标记为“已完成”或“未完成”。
- **置备程序规则**。选择一个规则，以便为此外部资源请求确定一个或多个置备程序。

注 – 您可以编写自己的规则以达到此目的。您还可以定义多个置备程序。当任何置备程序完成任务时，会将该任务从所有置备程序的队列中删除。有关编写自定义规则的详细信息，请参见《Sun Identity Manager Deployment Reference》中的第 4 章 “Working with Rules”。

- **样例外部置备程序**。将配置器指定为置备程序。
- **样例外部置备程序提升**。使用外部置备程序提升规则来确定提升到的置备程序。
- **样例外部 Remedy 规则**。定义 Remedy 配置器设置。

- **通知请求程序**。如果要在完成或未完成请求时向请求程序发送电子邮件，请选中此框。在启用此选项时，将显示以下附加字段：
  - **置备请求完成模板**。选择在完成请求时使用的电子邮件模板。
  - **置备请求未完成模板**。选择在未完成请求时使用的电子邮件模板。

注 – 有关电子邮件模板的详细信息，请参见第 261 页中的 “配置任务模板”。

3 **单击“保存”。**

将显示“配置”页，指示您可以继续执行其他配置任务。

4 **转到“资源”→“列出资源”选项卡。您现在可以基于此配置创建各个外部资源。有关说明，请参见第 162 页中的 “创建外部资源”。**

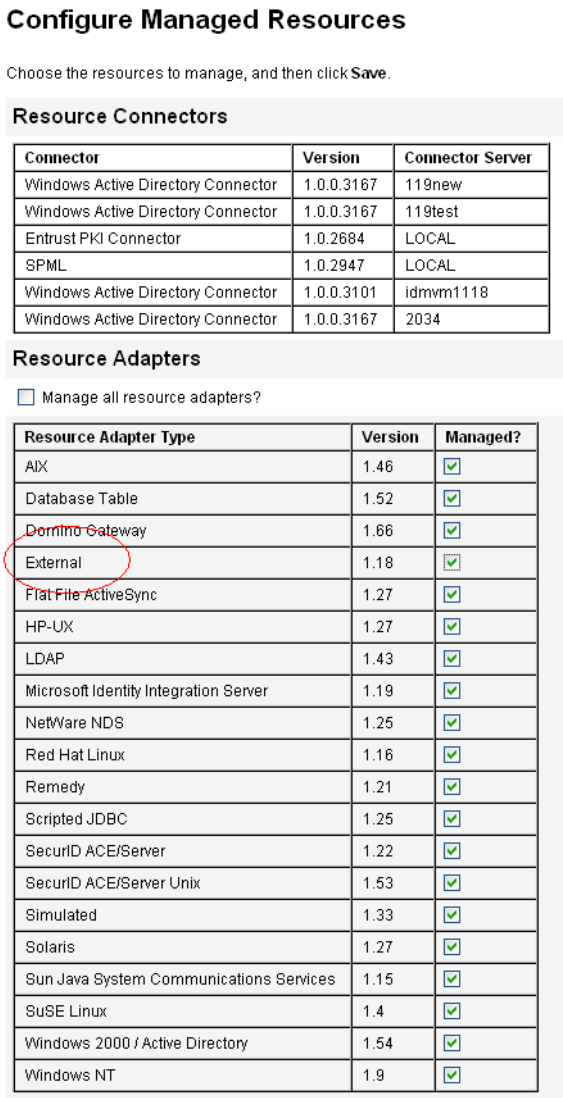
创建外部资源

在配置外部资源数据存储库和置备程序通知后，您可以创建新的外部资源。

注 – 您必须具有资源管理员权能才能创建新的外部资源。

要创建新的外部资源，请使用以下步骤：

1. 从主菜单栏中选择“资源”选项卡。默认情况下，将显示“列出资源”选项卡。
2. 单击“配置类型”选项卡以打开“配置受管理的资源”页。



Configure Managed Resources

Choose the resources to manage, and then click **Save**.

Resource Connectors

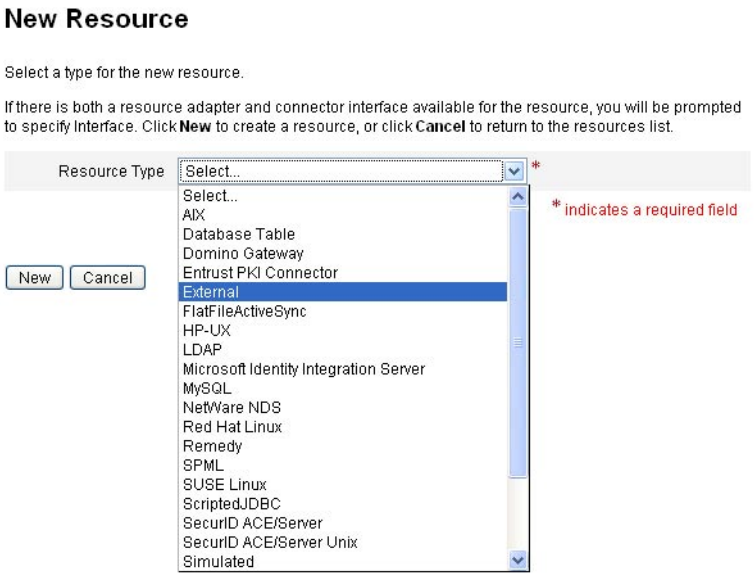
Connector	Version	Connector Server
Windows Active Directory Connector	1.0.0.3167	119new
Windows Active Directory Connector	1.0.0.3167	119test
Entrust PKI Connector	1.0.2684	LOCAL
SPML	1.0.2947	LOCAL
Windows Active Directory Connector	1.0.0.3101	idmvm1118
Windows Active Directory Connector	1.0.0.3167	2034

Resource Adapters

☐ Manage all resource adapters?

Resource Adapter Type	Version	Managed?
AIX	1.46	☑
Database Table	1.52	☑
Domino Gateway	1.66	☑
External	1.18	☑
Flat File ActiveSync	1.27	☑
HP-UX	1.27	☑
LDAP	1.43	☑
Microsoft Identity Integration Server	1.19	☑
NetWare NDS	1.25	☑
Red Hat Linux	1.16	☑
Remedy	1.21	☑
Scripted JDBC	1.25	☑
SecurID ACE/Server	1.22	☑
SecurID ACE/Server Unix	1.53	☑
Simulated	1.33	☑
Solaris	1.27	☑
Sun Java System Communications Services	1.15	☑
SuSE Linux	1.4	☑
Windows 2000 / Active Directory	1.54	☑
Windows NT	1.9	☑

3. 查看资源适配器表以检查外部资源类型是否可用。
4. 返回到“列出资源”选项卡，然后从“资源类型操作”菜单中选择“新建资源”。
5. 在显示“新建资源”页时，从“资源类型”菜单中选择“外部”，然后单击“新建”。



6. 将显示“创建外部资源向导”欢迎页。单击“下一步”。

   将显示“数据存储库配置”页的只读视图，其中显示了以前定义的连接和验证信息。

   正如前面所述，您通常仅配置一次此数据存储库，因为该配置适用于所有外部资源。如果要更改任何此类信息，您必须返回到“配置”→“外部资源”选项卡。

注 – 如果要在继续之前重新测试当前数据存储库配置，您可以单击位于页面底部的“测试配置”。

---

7. 单击“下一步”以打开“置备程序通知配置”页，该页与在“配置”→“外部资源”选项卡上配置的页面完全相同。
8. 查看当前置备程序通知设置，并对新资源进行任何必要的更改。

注 – 如有必要，请参阅前文第 157 页中的 “配置置备程序通知”中的配置说明。对此页进行的任何更改只影响此资源。

---

9. 单击“下一步”。

从这个角度讲，创建外部资源的过程与用于创建任何其他资源的过程是相同的。该向导将指导您完成几个其他页面的配置工作：

- **“帐户属性”页**。可以使用该页为资源定义可选帐户属性，并将 Identity System 属性映射到新资源帐户属性。例如，如果要创建一个名为 "laptop" 的外部资源，您可能需要添加属性以表示型号和大小。

  注 – 没有为该页指定任何默认值。

- **“身份模板”页**。可以使用该页为在此外部资源上创建的用户定义帐户名称语法。您可以使用默认身份模板 `$accountId$`，也可以指定不同的模板。
- **“Identity System 参数”页**。可以使用该页为外部资源配置 Identity System 参数。例如，您可以禁用策略，配置重试次数或指定批准者。

有关这些页面的详细信息以及完成配置此资源所需的说明，请参见第 138 页中的 “创建资源”。

10. 在配置完“Identity System 参数”页后，单击“保存”。现在，您可以将此资源分配给用户，就像分配任何其他资源一样。

置备外部资源

本节介绍了实际置备过程，其中包括：

▼ 为用户分配外部资源

可以使用以下步骤为用户分配外部资源：

注 – 要分配外部资源，您必须具有资源管理员权能。

1. **单击“帐户”→“列出帐户”，然后从该页中单击用户的名称。**
2. **在显示“编辑用户”页时，单击“资源”选项卡。**
3. **在“单独资源分配”的“可用资源”列表中找到外部资源，将该资源移到“当前资源”列表中，然后单击“保存”。**

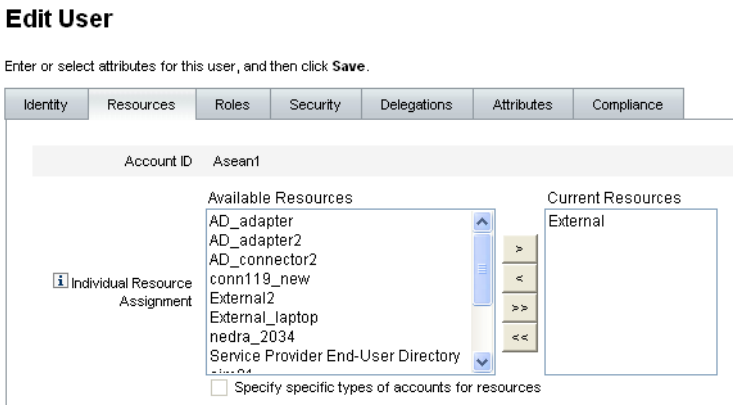


图 5–19 “编辑用户”页

Identity Manager 将创建一个置备任务，并向您发送邮件以指示拥有该置备任务的用户。请记住，在为此资源配置“置备程序通知”页时，使用置备程序规则定义了一个或多个置备程序。

Identity Manager 还会通过电子邮件或 Remedy 票证通知置备程序，它们具有暂挂请求。

注 – 与其他资源一样，您可以定义批准者，他们可以批准或拒绝请求。您必须定义置备程序，但他们不能批准或拒绝请求。置备程序可以完成或未完成任务。

---

4 **单击“确定”以返回至“帐户”→“列出帐户”页。请注意，将在工作项目图标中的用户名旁边显示沙漏，以指示请求处于暂挂状态。**

▼ 响应外部资源置备请求

在生成置备请求后，该请求将暂停置备过程，直至某个定义的置备程序完成手动置备，或将该请求标记为未完成或者该请求超时。Identity Manager 将审计这些置备响应。

与任何其他工作项目一样，可以从“工作项目”→“置备请求”选项卡中查看所有暂挂外部资源置备请求。

可以按如下方式响应置备请求：

1 **单击“工作项目”>“置备请求”选项卡以打开“等待置备”页。**

图 5–20 “等待置备”页

2 **查找并选择暂挂置备请求。**

3 **（可选）您可以打开置备请求电子邮件，单击置备请求模板中定义的链接，然后登录以查看包含置备请求详细信息的页面。**

您可以从该页中更新任何请求的属性，以便准确地反映为用户置备的资源。例如，如果用户请求置备 Sony 便携式计算机，但该型号不可用，您可以使用实际置备的型号更新该页面。

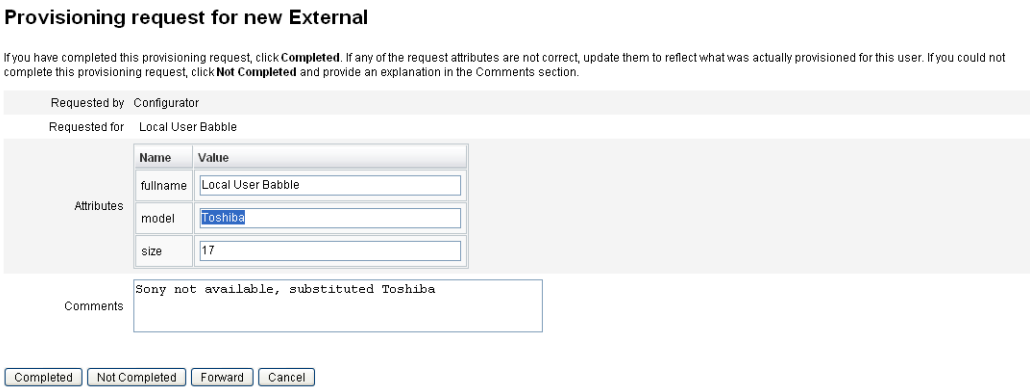


图 5–21 置备新便携式计算机的请求

4 **单击下面的某个按钮以处理该请求：**

- 如果您可以置备该资源，请单击“已完成”。

  Identity Manager 将更新该用户的外部资源帐户属性以显示实际置备的资源，删除暂挂置备状态标记，并完成所更新的置备请求工作项目。

如果已配置，Identity Manager 还会通知请求程序，置备请求已完成（使用为此目的配置的电子邮件模板）。

- 如果无法置备该资源，请指定原因，然后单击“未完成”。

  在将请求标记为“未完成”时，

  - 不会为该用户置备外部资源。
  - 但仍会将外部资源分配给用户。
  - 将在该用户的名称旁边显示黄色图标，指示该用户需要更新。

    如果编辑此用户，则会显示一条错误消息，指出在外部资源中找不到该用户。
  - 如果已配置，Identity Manager 还会向请求程序发送通知（使用为此目的配置的电子邮件模板）。
- 如果无法置备资源，您也可以单击“转发”，将该请求转发给其他人。

在完成或未完成置备请求工作项目时，Identity Manager 将清除用户的分配外部资源暂挂状态，并且不会对外部资源数据存储库进行任何更新。

将在用户的分配资源列表和当前资源帐户列表中显示该资源，其中包括该资源的用户 accountId。

注 – 如果分配的置备程序在指定的超时时间段内未响应置备请求，Identity Manager 将取消关联的置备请求工作项目。

更多信息

提升置备请求

- 如果在配置“置备程序通知”页时指定了超时时间段，并且置备请求超过了超时时间段，Identity Manager 将执行以下操作之一：
  - 如果指定了置备程序提升规则，Identity Manager 将使用该规则确定下一个置备程序，然后将请求提升到该置备程序。
  - 如果未选择置备程序提升规则，Identity Manager 则会将请求提升到配置器。如果配置器不存在，则在超时到期后将请求归类为“未完成”。
- 如果将“升级超时时间”字段保留空白或输入零，Identity Manager 将从不提升请求。

委托置备请求

您可以像委托任何其他置备请求一样委托外部资源置备工作项目。有关详细信息和说明，请参见第 199 页中的 “委托工作项目”。

取消分配外部资源和解除其链接

与任何其他资源一样，您可以从“常规”选项卡中为用户取消分配外部资源或解除其链接。有关说明，请参见第 51 页中的 “创建用户和使用用户帐户”。

注 – 为用户取消分配外部资源或解除其链接并不会创建置备请求或工作项目。在取消分配外部资源或解除其链接时，Identity Manager 不会取消置备或删除资源帐户，因此，您无需执行任何操作。

外部资源故障排除

无法删除仍分配了外部资源的用户。您必须首先取消置备或删除这些外部资源，然后才能删除用户。

Identity Manager 允许您使用以下方法调试和跟踪外部资源：

- 您可以跟踪外部资源适配器。
  - 如果使用的数据存储库是数据库，请跟踪 `com.waveset.adapter.ScriptedJdbcResourceAdapter` 和 `com.waveset.adapter.JdbcResourceAdapter` 跟踪类名。
  - 如果使用的数据存储库是目录，请跟踪 `com.waveset.adapter.LDAPResourceAdapter` 跟踪类名。
- 您可以使用工作流跟踪来跟踪其他数据流和工作流，然后使用 NetBeans 或 Eclipse Identity Manager IDE 插件进行调试。
- 由于数据存储库是由您配置和控制的，因此，可以使用数据存储库检查来确保该数据存储库中的信息正确无误。
- Identity Manager 将为所有发生的活动写入审计记录。

有关跟踪和故障排除的详细信息，请参见《Sun Identity Manager 8.1 System Administrator's Guide》。

◆ ◆ ◆ 第 6 章

管理

本章介绍在 Identity Manager 系统中执行一系列管理级任务的信息和过程，例如创建和管理 Identity Manager 管理员和组织。此外，本章还介绍了在 Identity Manager 中如何使用角色、权能和管理角色。

按以下主题对信息进行分组：

了解 Identity Manager 管理

Identity Manager 管理员是具有扩展 Identity Manager 权限的用户。

Identity Manager 管理员管理：

- 用户帐户
- 系统对象，例如角色和资源
- 组织

与用户不同，为 Identity Manager 中的管理员分配了权能和受控组织，其定义如下所示：

- **权能**。授予对 Identity Manager 用户、组织、角色及资源访问权限的一组权限。
- **受控组织**。分配了控制组织的权限后，该管理员就可以管理该组织中以及分层结构中该组织之下的任何组织中的对象。

委托管理

在多数公司内，执行管理任务的雇员具有特定职责。因此，这些管理员可以执行的帐户管理任务范围是非常有限的。

例如，管理员可能只负责创建 Identity Manager 用户帐户。由于该职责的范围有限，管理员可能不需要有关用于创建用户帐户的资源或者系统中存在的角色或组织的特定信息。

Identity Manager 还可以将管理员限制为仅执行已定义的特定范围内的特定任务。

Identity Manager 支持如下所示的职责划分和委托管理模型：

- 分配的**权能**将管理员限制为仅履行特定工作职责
- 分配的**受控组织**将管理员限制为仅控制特定组织（以及这些组织中的对象）
- “创建用户”和“编辑用户”页的过滤视图可防止管理员查看与其工作职责无关的信息

设置新用户帐户或编辑用户帐户时，您可以在“创建用户”页中为用户指定委托。

您也可以从“工作项目”选项卡委托工作项目，例如批准请求。有关委托的详细信息，请参见第 199 页中的 “委托工作项目”。

创建和管理管理员

本节分为以下几个主题：

▼ 创建管理员

要创建管理员，请将一项或多项权能分配给用户，并指定将应用这些权能的组织。

1 **在管理员界面中，单击菜单栏中的“帐户”。**

将打开“用户列表”页。

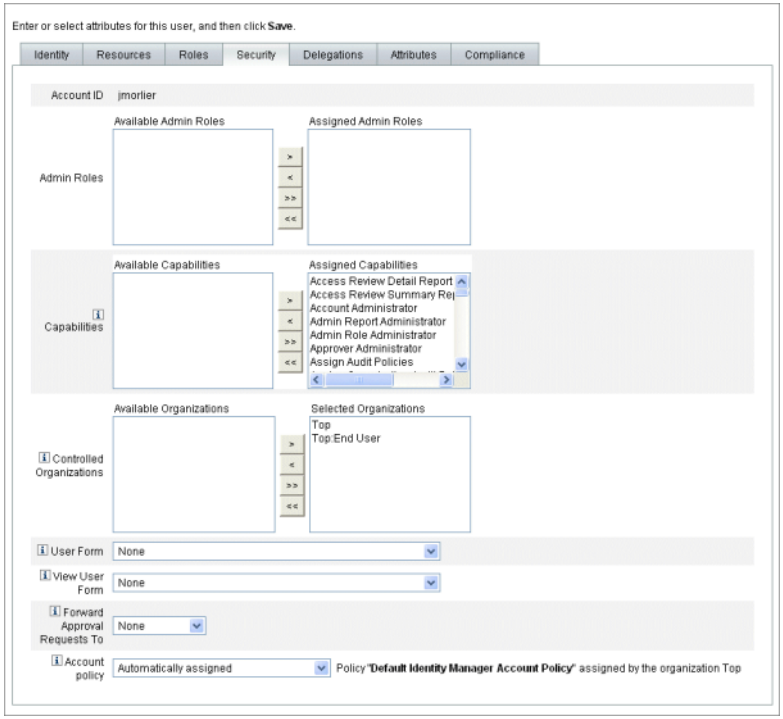
2 **要为现有用户分配管理权限，请单击用户名（将打开“编辑用户”页），然后单击“安全性”选项卡。**

如果需要创建新的用户帐户，请参见第 51 页中的 “创建用户和使用用户帐户”。

3 **指定属性以建立管理控制。**

可用属性包括：

- **权能**。选择一个或多个应分配给此管理员的权能。此信息是必填信息。有关详细信息，请参见第 184 页中的 “了解和管理权能”。
- **受控组织**。选择一个或多个应分配给此管理员的组织。该管理员将控制其分得的组织中以及在分层结构中处于该组织之下的任何组织中的对象。此信息是必填信息。有关详细信息，请参见第 178 页中的 “了解 Identity Manager 组织”。
- **用户表单**。选择此管理员在创建和编辑 Identity Manager 用户（如果分配了该权能）时将使用的用户表单。如果不直接分配用户表单，管理员将继承已分配给其所属组织的用户表单。此处选定的表单会取代在此管理员组织内选定的任何表单。
- **转发批准请求至**。选择一个用户，以将所有当前暂挂批准请求转发至该用户。还可以从“批准”页进行此管理员设置。
- **将工作项目委托给**。使用此选项指定该用户帐户的委托（如果可用）。您可以指定该管理员的管理者、一个或多个选定的用户，或使用委托批准者规则。



过滤管理员视图

将用户表单分配给组织和管理员，即可建立用户信息的特定管理员视图。

在两个级别设置对用户信息的访问：

- **组织**。创建组织时，您可以分配该组织内的所有管理员在创建和编辑 Identity Manager 用户时将使用的用户表单。任何在管理员级设置的表单都会覆盖在此设置的表单。如果没有为管理员或组织选择表单，Identity Manager 会继承为父组织选择的表单。如果未在父组织设置表单，Identity Manager 会使用在系统配置中设置的默认表单。
- **管理员**。分配用户管理权能时，可以将用户表单直接分配给管理员。如果未分配表单，管理员会继承分配给其组织的表单（或者，在没有为该组织设置表单时继承在系统配置中设置的默认表单）。

第 184 页中的“了解和管理权能”介绍了您可以分配的内置 Identity Manager 权能。

更改管理员密码

管理员密码可以由分配了管理密码更改权能的管理员进行更改，或由管理员拥有者更改。

管理员可以使用下列表单更改其他管理员的密码：

- **更改用户密码表单**。可以使用两种方法打开该表单：
  - 在菜单中单击“帐户”。将打开“用户列表”。选择一个管理员，然后在“用户操作”列表中选择“更改密码”。将打开“更改用户密码”页。
  - 在菜单中单击“密码”。将打开“更改用户密码”页。
- **选项卡式用户表单**。在菜单中单击“帐户”。将打开“用户列表”。选择一个管理员，然后在“用户操作”菜单中选择“编辑”。将打开“编辑用户”页（选项卡式用户表单）。在“身份”表单选项卡上，在“密码”和“确认密码”字段中键入新密码。

管理员可从“密码”区域更改自己的密码。在菜单中单击“密码”，然后单击“更改我的密码”。

注 – 应用于帐户的 Identity Manager 帐户策略决定密码限制条件，例如密码到期日期、重设选项和通知选择。其他密码限制条件可以按照在管理员的资源中设置的密码策略设置。

验明管理员操作

可以对 Identity Manager 进行配置，以便在处理某些帐户更改前提示管理员输入密码。如果验证失败，则会取消帐户更改。

管理员可以使用三个表单来更改用户密码。它们分别是：选项卡式用户表单、更改用户密码表单以及重设用户密码表单。要确保管理员必须在 Identity Manager 处理用户帐户更改之前输入其密码，请务必更新所有三个表单。

▼ 为选项卡式用户表单启用质询选项

要在选项卡式用户表单上要求使用密码质询，请执行以下步骤：

1. **在管理员界面中，通过在浏览器中键入以下 URL 打开 Identity Manager 调试页（第 40 页中的“Identity Manager 的“调试”页”）。（您必须具有“调试”权能才能打开此页面。）**

   `http://<AppServerHost>:<Port>/idm/debug/session.jsp`

   将打开“系统设置”页（Identity Manager 调试页）。

2. **找到“列出对象”按钮，从下拉菜单中选择“用户表单”，然后单击“列出对象”按钮。**

   将打开“列出以下类型的对象：用户表单”页。

3 找到在生产中使用的选项卡式用户表单的副本，然后单击“编辑”。（随 Identity Manager 一起分发的选项卡式用户表单是一个模板，不应对其进行修改。）

4 在 <Form> 元素中添加以下代码片段：

```
<Properties>
  <Property name='RequiresChallenge'>
    <List>
      <String>password</String>
      <String>email</String>
      <String>fullname</String>
    </List>
  </Property>
</Properties>
```

此属性值是一个列表，可以包含一个或多个以下用户视图属性名称：

- applications
- adminRoles
- assignedLhPolicy
- capabilities
- controlledOrganizations
- email
- firstname
- fullname
- lastname
- organization
- password
- resources
- roles

5 保存所做的更改。

▼ 为更改用户密码表单和重设用户密码表单启用质询选项

要在更改用户密码表单和重设用户密码表单上要求使用密码质询，请执行以下步骤：

1 在管理员界面中，通过在浏览器中键入以下 URL 打开 Identity Manager 调试页（第 40 页中的“Identity Manager 的“调试”页”）。（您必须具有“调试”权能才能打开此页面。）

`http://<AppServerHost>:<Port>/idm/debug/session.jsp`

将打开“系统设置”页（Identity Manager 调试页）。

2 找到“列出对象”按钮，从下拉菜单中选择“用户表单”，然后单击“列出对象”按钮。

将打开“列出以下类型的对象：用户表单”页。

3. **找到在生产中使用的更改密码用户表单的副本，然后单击“编辑”。（随 Identity Manager 一起分发的更改密码用户表单是一个模板，不应对其进行修改。）**

4. **找到 `<Form>` 元素，然后转到 `<Properties>` 元素。**

5. **在 `<Properties>` 元素中添加以下行，然后保存更改。**

   ```
   <Property name='RequiresChallenge' value='true'/>
   ```

6. **重复执行步骤 3 至步骤 5，但不要编辑在生产中使用的“重设用户密码表单”的副本。**

更改验证问题回答

使用“密码”区域更改已经为帐户验证问题设置的回答。在菜单栏中选择“密码”，然后选择“更改我的回答”。

有关验证的详细信息，请参见第 3 章，用户和帐户管理中的第 79 页中的 “用户验证”一节。

自定义在“管理员界面”中显示的管理员名称

可以在某些 Identity Manager 管理员界面页和区域中按属性（例如，`email` 或 `fullname`）而不是按帐户 ID 来显示 Identity Manager 管理员。

例如，可以在以下区域中按属性显示 Identity Manager 管理员：

- 编辑用户（转发批准选项列表）
- 角色表
- 创建/编辑角色
- 创建/编辑资源
- 创建/编辑组织/目录连接
- 批准

要配置 Identity Manager 以使用显示名称，可将以下内容添加到 `UserUIConfig` 对象：

```
<AdminDisplayAttribute>
  <String>attribute_name</String>
</AdminDisplayAttribute>
```

例如，要使用电子邮件属性作为显示名称，可将以下属性名称添加到 `UserUIconfig`：

```
<AdminDisplayAttribute>
  <String>email</String>
</AdminDisplayAttribute>
```

了解 Identity Manager 组织

组织允许您：

- 合乎逻辑并安全地管理用户帐户和管理员
- 限制对资源、应用程序、角色和其他 Identity Manager 对象的访问

通过创建组织并将用户分配到组织分层结构中的不同位置，可以设置委托管理的阶段。包含一个或多个其他组织的组织称为**父组织**。

所有 Identity Manager 用户（包括管理员）都被**静态分配给**一个组织。用户还可以被**动态地分配**到其他组织。

将额外分配 Identity Manager 管理员以**控制**组织。

创建组织

▼ 创建组织

在 Identity Manager 的“帐户”区域中创建组织。

1 **在管理员界面中，单击菜单栏中的“帐户”。**
将打开“用户列表”页。

2 **在“新建操作”菜单中，选择“新建组织”。**

提示 – 要在组织分层结构中的特定位置上创建组织，请在列表中选择一个组织，然后在“新建操作”菜单中选择“新建组织”。

图 6–1 展示了“创建组织”页。

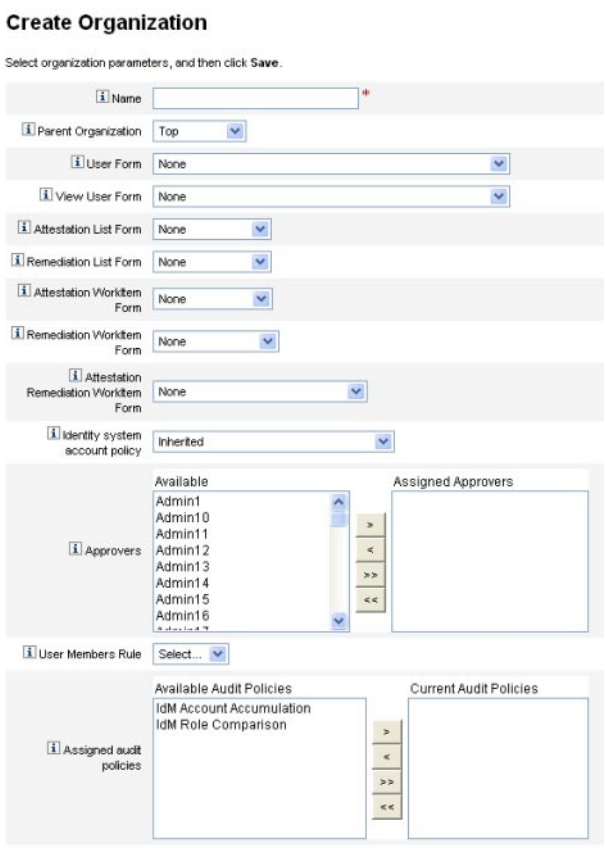


图 6–1 “创建组织”页

将用户分配给组织

每个用户都是一个组织的静态成员，并且可以是多个组织的动态成员。

可以使用以下任一方法定义组织成员资格：

- **直接（静态）分配**。在“创建用户”或“编辑用户”页中选择“身份”表单选项卡，以将用户直接分配给组织。用户必须被直接分配给一个组织。
- **规则驱动（动态）分配**。使用分配给组织的用户成员规则将用户分配给该组织。在评估该规则时，将返回一组成员用户。

  Identity Manager 将在以下情况下评估用户成员规则：

  - 列出组织中的用户
  - 查找用户（通过“查找用户”页），包括搜索具有某个用户成员规则的组织中的用户
  - 请求访问用户，但前提是当前管理员控制具有用户成员规则的组织

注 – 有关在 Identity Manager 中创建和使用规则的详细信息，请参见《Sun Identity Manager Deployment Reference》中的第 4 章 “Working with Rules”。

在“创建组织”页的“用户成员规则”菜单中选择一个用户成员规则。下图显示了一个用户成员规则示例。

以下示例展示了用于动态控制组织用户成员资格的用户成员规则示例的语法。

注 –

在创建用户成员规则之前，您应该注意以下事项：

- 要在“用户成员规则”选项框中显示某个规则，必须将其 `authType` 设置为 `authType='UserMembersRule'`。
- 该上下文是目前已验证的 Identity Manager 用户的会话。
- 已定义的变量 `(defvar) Team players` 为属于 Windows Active Directory 组织单位 (Organization Unit, ou) `Pro Ball Team` 成员的每位用户获取标识名 (Distinguished Name, dn)。
- 对于找到的每位用户，附加逻辑会将 `Pro Ball Team` ou 中每位成员用户的 dn 与前缀为冒号的 Identity Manager 资源的名称（例如 `:smith-AD`）连接在一起。
- 返回的结果将是与 Identity Manager 资源名称连接的 dn 的列表，格式为 *dn* `:smith-AD`。

示例 6–1 用户成员规则示例

```
<Rule name='Get Team Players' authType='UserMembersRule'>
  <defvar name='Team players'>
    <block>
```

示例 6–1 用户成员规则示例 （续）

```
      <defvar name='player names'>
        <list/>
      </defvar>
  <dolist name='users'>
    <invoke class='com.waveset.ui.FormUtil' name='getResourceObjects'>
      <ref>context</ref>
      <s>User</s>
      <s>singleton-AD</s>
      <map>
        <s>searchContext</s>
        <s>OU=Pro Ball Team,DC=dev-ad,DC=waveset,DC=com</s>
        <s>searchScope</s>
        <s>subtree</s>
        <s>searchAttrsToGet</s>
        <list>
          <s>distinguishedName</s>
        </list>
      </map>
    </invoke>
    <append name='player names'>
    <concat>
      <get>
        <ref>users</ref>
        <s>distinguishedName</s>
      </get>
        <s>:sampson-AD</s>
    </concat>
    </append>
  </dolist>
    <ref>player names</ref>
  </block>
   </defvar>
    <ref>Team players</ref>
</Rule>
```

注 – 您可以在 `Waveset.properties` 中配置一些属性，以控制规则驱动用户成员列表高速缓存，它可能会影响内存和性能。有关信息，请参见《Sun Identity Manager 8.1 System Administrator's Guide》中的"Tracing Rule-Driven Members Caches"。

分配组织控制

从"创建用户"或"编辑用户"页中分配一个或多个组织的管理控制。选择"安全性"表单选项卡以显示"受控组织"字段。

您还可以从“管理员角色”字段分配一个或多个管理员角色，从而分配组织的管理控制。

了解目录连接和虚拟组织

目录连接是与分层相关的一组组织，它镜像目录资源的实际层级容器集合。**目录资源**通过使用分层容器来使用分层名称空间。目录资源的示例包括 LDAP 服务器和 Windows Active Directory 资源。

目录连接中的每个组织都是**虚拟组织**。目录连接中的最顶层虚拟组织是代表资源中定义的基本上下文的容器的镜像。目录连接中的其余虚拟组织是顶层虚拟组织的**直接**或**间接**子组织，并且还镜像目录资源容器中的一个容器（已定义资源的基本环境容器的子容器）。图 6–2 展示了此结构。

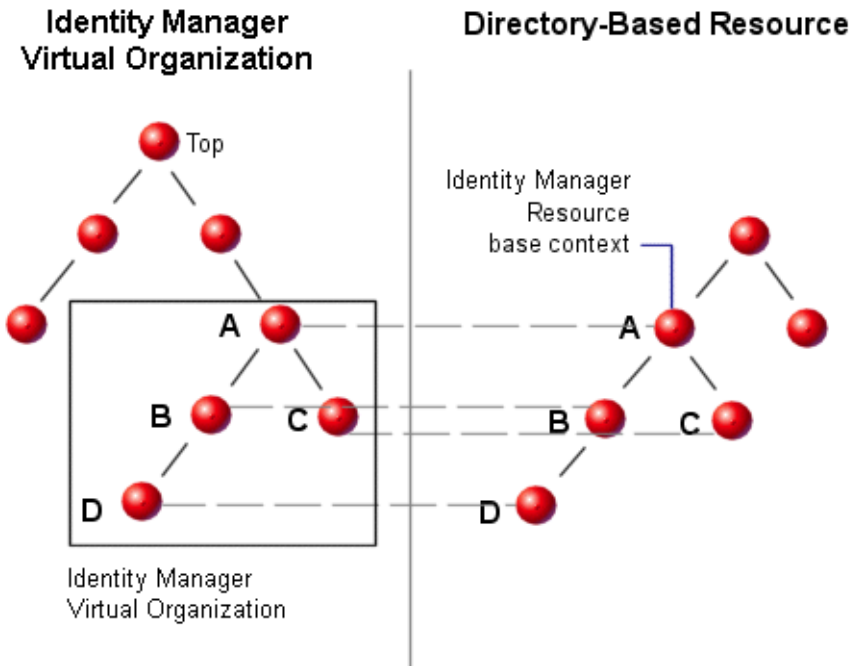


图 6–2 Identity Manager 虚拟组织

目录连接可以在任一点被连接到现有 Identity Manager 组织结构中。但是，目录连接不能连接到现有目录连接之内或之下。

如果已将目录连接添加到 Identity Manager 组织树中，就可以在该目录连接的上下文中创建或删除虚拟组织。此外，您可以随时刷新由目录连接组成的虚拟组织集，以确保虚拟组织集与目录资源容器保持同步。不能在目录连接内创建非虚拟组织。

可以采用与 Identity Manager 组织一样的方法，使 Identity Manager 对象（例如用户、资源和角色）成为虚拟组织的成员，并且可用于虚拟组织。

设置目录连接

本节介绍了如何设置目录连接。

▼ 设置目录连接

1. **在管理员界面中，选择菜单栏中的“帐户”。**
   将打开“用户列表”页。

2. **在“帐户”列表中选择一个 Identity Manager 组织。**
   您选择的组织将是所设置的虚拟组织的父组织。

3. **在“新建操作”菜单中，选择“新建目录连接”。**
   Identity Manager 将打开“创建目录连接”页。

4. **使用“创建目录连接”页中的选项设置虚拟组织。**
   这些选项包括：
   - **父组织**。此字段包含从“帐户”列表中选择的组织；但是您也可以从该列表中选择不同的父组织。
   - **目录资源**。选择目录资源，该目录资源管理您要在虚拟组织中镜像其目录结构的现有目录。
   - **用户表单**。选择要应用于该组织内的管理员的用户表单。
   - **Identity Manager 帐户策略**。选择一个策略，或者选择默认选项（继承），以继承父组织的策略。
   - **批准者**。选择可以批准与此组织相关的请求的管理员。

刷新虚拟组织

此过程从所选组织向下刷新虚拟组织并使之与相关目录资源重新同步。在列表中选择虚拟组织，然后在“组织操作”列表中选择“刷新组织”。

删除虚拟组织

删除虚拟组织时，可以从两个删除选项中选择：

- **仅删除 Identity Manager 组织**。仅删除 Identity Manager 目录连接。
- **删除 Identity Manager 组织和资源容器**。删除 Identity Manager 目录连接和本机资源上的相应组织。

选择其中一个选项，然后单击“删除”。

了解和管理权能

权能是 Identity Manager 系统中的权限组。权能代表管理作业职责（如重设密码或管理用户帐户）。每个 Identity Manager 管理用户都分配有一个或多个权能，这些权能提供了一组权限而不会损害数据保护。

并非所有 Identity Manager 用户都需要分配权能。只有那些要通过 Identity Manager 执行一项或多项管理操作的用户才需要权能。例如，使用户可以更改自己的密码并不需要为用户分配权能，但要更改其他用户的密码就需要分配权能。

分配的权能决定了您可以访问 Identity Manager 管理员界面的哪些区域。

所有 Identity Manager 管理用户都可以访问 Identity Manager 的某些区域，其中包括：

- **主页**和**帮助**选项卡
- **密码**选项卡（仅限“更改我的密码”和“更改我的回答”子选项卡）
- **报告**（仅限于与管理员的特定职责有关的类型）

注 – 附录 D，权能定义中包含 Identity Manager 的默认基于任务的权能和功能性权能（及定义）的列表。该附录还列出了可使用每种基于任务的权能访问的选项卡和子选项卡。

权能类别

Identity Manager 将权能定义为：

- **基于任务**。这些是处于最简单的任务级别的权能。
- **功能性**。功能性权能包含一项或多项其他功能性或基于任务的权能。

内置权能（随 Identity Manager 系统提供的权能）是**受保护的**权能，即，不能对它们进行编辑。但是，可以在创建的权能中使用它们。

受保护的（内置）权能在列表中以红色钥匙（或红色钥匙和文件夹）图标指示。创建和可编辑的权能在权能列表中以绿色钥匙（或绿色钥匙和文件夹）图标指示。

使用权能

本节介绍如何创建、编辑、分配和重命名权能。这些任务是使用“权能”页执行的。

查看“权能”页

“权能”页位于“安全性”选项卡下面。

▼ 打开“权能”页

1. **在管理员界面中，单击顶部菜单中的“安全性”。**
2. **单击次级菜单中的“权能”。**
   将打开“权能”页并显示 Identity Manager 权能列表。

创建权能

可以使用以下步骤来创建权能。要**克隆**权能，请参见第 186 页中的 “保存和重命名权能”。

▼ 创建权能

1. **在管理员界面中，单击顶部菜单中的“安全性”。**
2. **单击次级菜单中的“权能”。**
   将打开“权能”页并显示 Identity Manager 权能列表。
3. **单击“新建”。**
   将打开“创建权能”页。
4. **按如下方式填写表单：**

   a. **命名新权能。**

   b. **在“权能”部分中，使用箭头按钮将应分配给用户的权能移动到“已分配的权能”框中。**

   c. **在“分配者”框中，选择一个或多个用户，允许这些用户将此权能分配给其他用户。**

   - 如果未选择任何用户，则只有可以分配此权能的用户才能创建权能。
   - 如果尚未将“分配用户权能”权能分配给创建权能的用户，则必须选择一个或多个用户，以确保至少一个用户能够将权能分配给其他用户。

   d. **在“组织”框中，选择一个或多个可使用此权能的组织。**

e. **单击“保存”。**

注 – 可供您选择分配者的一组用户是已经分配了“分配权能”权限的用户。

编辑权能

您可以编辑未受保护的权能。

▼ 编辑未受保护的权能

1 **在管理员界面中，单击顶部菜单中的“安全性”。**

2 **单击次级菜单中的“权能”。**
将打开“权能”页并显示 Identity Manager 权能列表。

3 **右键单击列表中的一个权能，然后选择“编辑”。将打开“编辑权能”页。**

4 **进行相应的更改，然后单击“保存”。**
您无法编辑内置权能。不过，可以将这些权能保存为不同的名称，以创建您自己的权能。也可以在您创建的权能中使用内置权能。

保存和重命名权能

可通过将现有权能保存为新名称创建新的权能。此过程称为**克隆**权能。

▼ 克隆权能

1 **在管理员界面中，单击顶部菜单中的“安全性”。**

2 **单击次级菜单中的“权能”。**
将打开“权能”页并显示 Identity Manager 权能列表。

3 **右键单击列表中的一个权能，然后选择“另存为”。**
将打开一个对话框，并要求您键入新权能的名称。

4 **键入一个名称，然后单击“确定”。**
您可以立即编辑新权能。

为用户分配权能

可以使用“创建用户”页（第 51 页中的 “创建用户和使用用户帐户”）或“编辑用户”页（第 56 页中的 “编辑用户”）为用户分配权能。还可以通过分配管理员角色（通过界面中的“安全性”区域设置），将权能分配给用户。有关详细信息，请参见第 187 页中的 “了解和管理管理员角色”。

注 – 附录 D，权能定义中包含 Identity Manager 的默认基于任务的权能和功能性权能（及定义）的列表。该附录还列出了可使用每种基于任务的权能访问的选项卡和子选项卡。

了解和管理管理员角色

管理员角色定义了以下两项内容：一组权能和一个控制范围。（术语控制范围是指一个或多个受管理的组织。）在定义管理员角色后，即可将其分配给一个或多个管理员。

注 – 不要将**角色**和**管理员角色**相混淆。角色用于管理最终用户对外部资源的访问权限，而管理员角色主要用于管理 Identity Manager 管理员对 Identity Manager 对象的访问权限。

本节中介绍的信息仅限于管理员角色。有关角色的信息，请参见第 103 页中的 “了解和管理角色”。

可以将多个管理员角色分配给单个管理员。这可使管理员在一个控制范围内具有一组权能，而在另一个控制范围内具有另外一组权能。例如，某个管理员角色可能会向管理员授予为该管理员角色中指定的受控组织创建和编辑用户的权限。不过，分配给同一管理员的第二个管理员角色可能仅授予以下权限：在该管理员角色定义的另一组受控组织中更改用户密码。

通过使用管理员角色，可以重复使用权能和控制范围对。管理员角色还简化了包含大量用户的环境中的管理员权限管理工作。应使用管理员角色授予管理员权限，而不是直接将权能和受控组织分配给各个用户。

可以直接或动态（间接）地将权能和/或组织分配给管理员角色。

- **直接**。使用此方法可以将权能和/或受控组织明确分配给管理员角色。例如，可以将用户报告管理员权能和受控组织 Top 分配给某个管理员角色。
- **动态（间接）**。此方法使用规则来分配权能和受控组织。每次分配了管理员角色的管理员登录时，都会评估这些规则。在管理员通过验证后，这些规则将动态地确定分配哪些权能和/或受控组织。

  例如，当用户登录时：

  - 如果其 Active Directory (Active Directory, AD) 用户角色为**管理员**，则权能规则可能返回“帐户管理员”作为要分配的权能。
  - 如果其 Active Directory (Active Directory, AD) 用户部门为**营销部**，则受控组织规则可能返回“营销部”作为要分配的受控组织。

可以为每个登录界面（例如用户界面或管理员界面）启用或禁用将管理员角色动态分配给用户的操作。要执行此操作，请将以下系统配置属性设置为 `true` 或 `false`：

```
security.authz.checkDynamicallyAssignedAdminRolesAtLoginTo.logininterface
```

所有界面的默认值为 `false`。

有关编辑系统配置对象的说明，请参见第 102 页中的 “编辑 Identity Manager 配置对象”。

管理员角色规则

Identity Manager 提供了可用于为管理员角色创建规则的示例规则。您可以在 Identity Manager 安装目录的 `sample/adminRoleRules.xml` 中找到这些规则。

表 6–1 提供了这些规则名称以及必须为每个规则指定的 `authType`。

表 6–1 管理员角色示例规则

规则名称	authType
受控组织规则	`ControlledOrganizationsRule`
权能规则	`CapabilitiesRule`
向用户分配管理员角色规则	`UserIsAssignedAdminRoleRule`

注 – 有关为服务提供者用户管理员角色提供的示例规则的信息，请参见第 17 章，服务提供者管理中的第 467 页中的 “服务提供者用户的委托管理”。

用户管理员角色

Identity Manager 中包括名为“用户管理员角色”的内置管理员角色。默认情况下，该管理员角色不具有任何分配的权能或受控组织分配。无法将其删除。在登录时，此管理员角色将被隐含分配给所有用户（最终用户和管理员），而不管用户登录到何种界面（例如用户界面、管理员界面、控制台或 Identity Manager IDE）。

注 – 有关为服务提供者用户创建管理员角色的信息，请参见第 17 章，服务提供者管理 中的第 467 页中的 “服务提供者用户的委托管理”。

可以通过管理员界面编辑用户管理员角色（选择“安全性”，然后再选择“管理员角色”）。

因为通过这种管理员角色静态分配的所有权能或受控组织都将分配给所有用户，所以建议通过规则来分配权能和受控组织。这会使不同的用户能够拥有不同的权能或没有权能，分配范围将取决于用户身份、所属部门或是否为管理人员，可以在规则的上下文中查询这些信息。

用户管理员角色不会使工作流中使用的 `authorized=true` 标志过时，也不会取而代之。对于工作流（正在执行的工作流除外）所访问的对象，如果用户不拥有访问权限，这种标志将仍然适用。这本质上是使用户可以进入**以超级用户身份运行**模式。

不过，在某些情况下，用户应对工作流外的一个或多个对象拥有特定访问权限（并且可能对工作流内的一个或多个对象拥有这种权限）。在这些情况下，通过使用规则动态分配权能和受控组织可以实现对这些对象进行细化授权。

创建和编辑管理员角色

要创建或编辑管理员角色，您必须分配有“管理员角色管理员”权能。

要在管理员界面中访问管理员角色，请单击“安全性”，然后单击“管理员角色”选项卡。“管理员角色”列表页允许您为 Identity Manager 用户和服务提供者用户创建、编辑和删除管理员角色。

要编辑现有管理员角色，请单击列表中的名称。单击“新建”以创建管理员角色。Identity Manager 将显示“创建管理员角色”的各个选项（如图 6–3 中所示）。“创建管理员角色”视图显示了四个选项卡，您可以使用这些选项卡指定常规属性、权能和新管理员角色的范围以及向用户的角色分配。

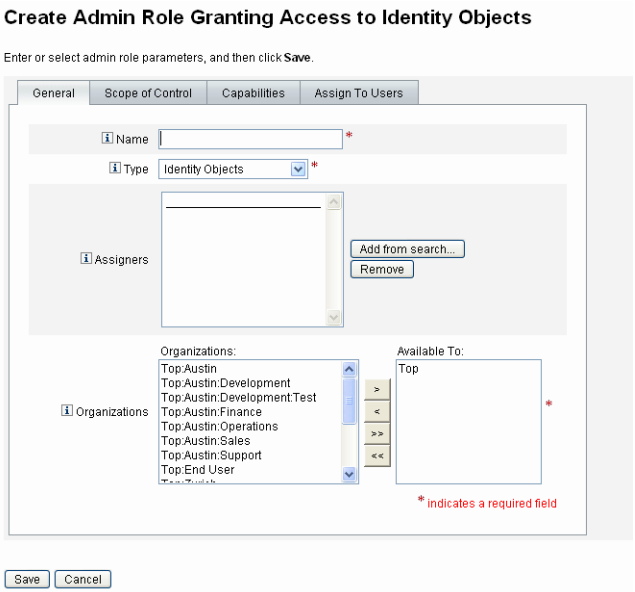


图 6–3 管理员角色创建页：“常规”选项卡

“常规”选项卡

使用创建管理员角色或编辑管理员角色视图中的“常规”选项卡可指定管理员角色的以下基本特性：

- **名称**。此管理员角色的唯一名称。

  例如，您可能要为对财务部（或组织）中的用户具有管理权能的用户创建财务管理员角色。

- **类型**。选择“身份对象”或“服务提供者用户”作为类型。此字段为必填字段。

  如果为 Identity Manager 用户（或对象）创建管理员角色，请选择“身份对象”。如果创建管理员角色以向服务提供商用户授予访问权限，请选择“服务提供者用户”。

注 – 有关创建管理员角色以向服务提供者用户授予访问权限的信息，请参见第 17 章，服务提供者管理中的第 467 页中的 “服务提供者用户的委托管理”。

- **分配者**。选择或搜索允许其将此管理员角色分配给其他用户的用户。可供您选择的一组用户包括已经分配了“分配权能”权限的用户。

  如果未选择任何用户，则唯一可以分配此管理员角色的用户为该管理员角色的创建者。如果尚未将“分配用户权能”权能分配给创建管理员角色的用户，请选择一个或多个用户作为分配者，以确保至少一个用户能够将管理员角色分配给其他用户。

- **组织**。选择可使用此管理员角色的一个或多个组织。此字段为必填字段。

该管理员可管理已分配组织以及在分层结构中处于该组织之下的任何组织中的对象。

控制范围

Identity Manager 允许您控制哪些用户在最终用户的控制范围之内。

使用“控制范围”选项卡（如图 6–4 中所示）可指定此组织的成员可管理的组织，也可以指定用于确定由管理员角色用户管理的组织的规则，以及选择管理员角色的用户表单。

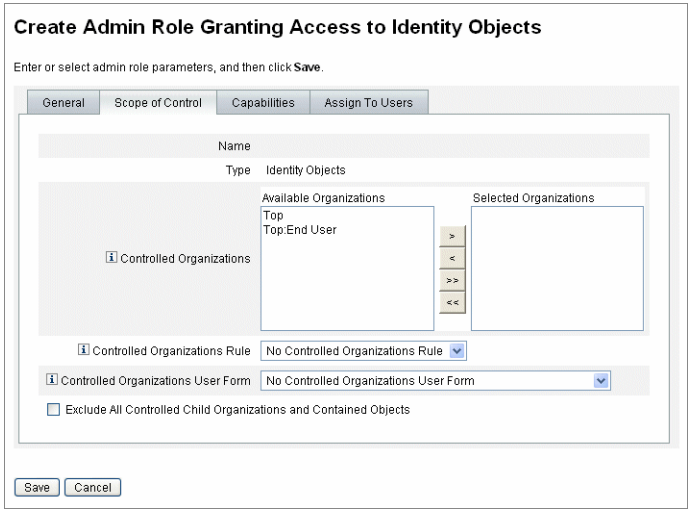


图 6–4 创建管理员角色：控制范围

- **受控组织**。从“可用组织”列表中选择此管理员角色有权管理的组织。
- **受控组织规则**。选择在用户登录时评估的规则，以确定由分配了此管理员角色的用户所控制的组织的个数（零个或多个）。选定的规则必须具有 `ControlledOrganizationsRule` authType。默认情况下，将选择 "No Controlled Organization Rule"。

  可以根据组织需要，使用 `EndUserControlledOrganizations` 规则来定义所需的逻辑，以确保为委托提供正确的用户集。

  如果希望管理员的用户范围列表始终相同（无论他们登录到管理员界面还是最终用户界面），则必须更改 `EndUserControlledOrganizations` 规则。

修改此规则，使其首先检查验证用户是否为管理员，然后再配置以下内容：

- 如果该用户不是管理员，则返回应由最终用户控制的组织集，如用户自己的组织（如 `waveset.organization`）。
- 如果该用户是管理员，则不返回任何组织，这样用户将只控制已分配的组织（因为用户是管理员）。

  例如：

```
<Rule protectedFromDelete='true'
      authType='EndUserControlledOrganizationsRule'
      id='#ID#End User Controlled Organizations'
      name='End User Controlled Organizations'>
  <Comments>
    If the user logging in is not an Idm administrator,
    then return the organization that they are a member of.
    Otherwise, return null.
  </Comments>
  <cond>
    <and>
      <isnull><ref>waveset.adminRoles</ref></isnull>
      <isnull><ref>waveset.capabilities</ref></isnull>
      <isnull><ref>waveset.controlledOrganizations</ref></isnull>
    </and>
    <ref>waveset.organization</ref>
  </cond>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' id='#ID#Top' name='Top'/>
  </MemberObjectGroups>
</Rule>
```

- 如果用户或管理员属于动态组织，则不会在搜索结果中返回他们。

  不过，您可以创建规则以返回动态组织中的用户。通过在 `Idm` **模式配置**对象中定义的 Identity Manager 用户模式定义中添加新属性来更改以下示例规则，导入该对象，然后重新启动 Identity Manager 服务器。

```
<IDMAttributeConfigurations>
    ...
    <IDMAttributeConfiguration name='region'
                               syntax='STRING'
                               description='region of the country'/>
</IDMAttributeConfigurations>

<IDMObjectClassConfigurations>
    ...
    <IDMObjectClassConfiguration name='User'
                                 extends='Principal'
                                   description='User description'>
```

```
                ...
                <IDMObjectClassAttributeConfiguration name='region'
                                                      queryable='true'/>
            </IDMObjectClassConfiguration>
        </IDMObjectClassConfigurations>
```

Next, import the following Identity Manager objects:

```
<!-- User member rule that will include all users whose region attribute
matches the region organization display name -->

<Rule name="Region User Member Rule" authType="UserMembersRule">
  <Description>User Member Rule</Description>
  <list>
    <new class='com.waveset.object.AttributeCondition'>
      <s>region</s>
      <s>equals</s>
      <ref>userMemberRuleOrganizationDisplayName</ref>
    </new>
  </list>
  <MemberObjectGroups>
    <ObjectRef type="ObjectGroup" id="#ID#All" name="All"/>
  </MemberObjectGroups>
</Rule>

<!-- North & South Region organizations with user member rule assigned -->

<ObjectGroup id='#ID#North Region' name='North Region'
displayName='North Region'> <UserMembersRule cacheTimeout='3600000'>
    <ObjectRef type='Rule' name='Region User Member Rule'/>
  </UserMembersRule>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' name='Top' id='#ID#Top'/>
  </MemberObjectGroups>
</ObjectGroup>

<ObjectGroup id='#ID#South Region' name='South Region'
displayName='South Region'>  <UserMembersRule cacheTimeout='3600000'>
    <ObjectRef type='Rule' name='Region User Member Rule'/>
  </UserMembersRule>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' name='Top' id='#ID#Top'/>
  </MemberObjectGroups>
</ObjectGroup>

<!-- Organization containing all employees -->

<ObjectGroup id='#ID#Employees' name='Employees' displayName='Employees'>
```

```
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' name='Top' id='#ID#Top'/>
  </MemberObjectGroups>
</ObjectGroup>

<!-- End user controlled organization rule that give each user control
of the regional organization they are a member of -->

<Rule protectedFromDelete='true'
      authType='EndUserControlledOrganizationsRule'
      id='#ID#End User Controlled Organizations'
      name='End User Controlled Organizations'
      primaryObjectClass='Rule'>
  <switch>
    <ref>waveset.attributes.region</ref>
    <case>
      <s>North Region</s>
      <s>North Region</s>
    </case>
    <case>
      <s>South Region</s>
      <s>South Region</s>
    </case>
    <case>
      <s>East Region</s>
      <s>East Region</s>
    </case>
    <case>
      <s>West Region</s>
      <s>West Region</s>
    </case>
  </switch>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' id='#ID#Top' name='Top'/>
  </MemberObjectGroups>
</Rule>

<!-- 4 employees (2 in North and 2 in South region) -->

<User name='emp1' primaryObjectClass='User' asciipassword='1111'>
  <Attribute name='firstname' type='string' value='Employee'/>
  <Attribute name='fullname' type='string' value='Employee One'/>
  <Attribute name='lastname' type='string' value='One'/>
  <Attribute name='region' type='string' value='North Region'/>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' id='#ID#Employees' name='Employees'
     displayName='Employees'/>
  </MemberObjectGroups>
```

```
</User>

<User name='emp2' primaryObjectClass='User' asciipassword='1111'>
  <Attribute name='firstname' type='string' value='Employee'/>
  <Attribute name='fullname' type='string' value='Employee Two'/>
  <Attribute name='lastname' type='string' value='Two'/>
  <Attribute name='region' type='string' value='North Region'/>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' id='#ID#Employees' name='Employees'
     displayName='Employees'/>
  </MemberObjectGroups>
</User>

<User name='emp4' primaryObjectClass='User' asciipassword='1111'>
  <Attribute name='firstname' type='string' value='Employee'/>
  <Attribute name='fullname' type='string' value='Employee Four'/>
  <Attribute name='lastname' type='string' value='Four'/>
  <Attribute name='region' type='string' value='South Region'/>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' id='#ID#Employees' name='Employees'
     displayName='Employees'/>
  </MemberObjectGroups>
</User>

<User name='emp5' primaryObjectClass='User' asciipassword='1111'>
  <Attribute name='firstname' type='string' value='Employee'/>
  <Attribute name='fullname' type='string' value='Employee Five'/>
  <Attribute name='lastname' type='string' value='Five'/>
  <Attribute name='region' type='string' value='South Region'/>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' id='#ID#Employees' name='Employees'
     displayName='Employees'/>
  </MemberObjectGroups>
</User>
```

接下来，通过 Identity Manager 最终用户界面以 `emp1`（位于北部地区）身份登录。选择“委托”→“新建”。将搜索→提供条件更改为**开头为**，将该值更改为 **emp**，然后选择“查找”。进行此选择将会在可用用户列表中返回 `emp2`。

- **受控组织用户表单**。选择分配了此管理员角色的用户在创建或编辑属于此管理员角色受控组织的用户时使用的用户表单。默认情况下，不会选择任何“受控组织用户表单”。

  通过管理员角色分配的用户表单将覆盖从该管理员所在组织继承的任何用户表单。不会覆盖直接分配给该管理员的用户表单。

为管理员角色分配权能

分配给管理员角色的权能将确定已分配管理员角色的用户所具有的管理权限。例如，此管理员角色可能被限制为仅为管理员角色的受控组织创建用户。这种情况下，可以分配创建用户权能。

在“权能”选项卡中，请选择以下选项：

- **权能**。这些为管理员角色的用户对其受控组织所具有的特定权能（管理权限）。从可用权能列表中选择一个或多个权能，并将其移动到“已分配的权能”列表。
- **权能规则**。选择在用户登录时评估的规则，以确定向分配了管理员角色的用户授予的权能（零个或多个）的列表。选定的规则必须具有 `CapabilitiesRule` authType。

将用户表单分配给管理员角色

您可为某个管理员角色的成员指定用户表单。使用创建管理员角色或编辑管理员角色视图中的 "Assign To Users" 选项卡可指定分配。

分配了管理员角色的管理员在该管理员角色所控制的组织中创建或编辑用户时，将会使用此用户表单。通过管理员角色分配的用户表单将覆盖从该管理员所在组织继承的任何用户表单。该用户表单不会覆盖直接分配给该管理员的用户表单。

将按以下优先级顺序来决定编辑用户时使用的用户表单：

- 如果用户表单是直接分配给该管理员的，则使用该表单。
- 如果没有直接为管理员分配用户表单，但为管理员分配了管理员角色，且该管理员角色控制管理员创建或编辑的用户所属的组织并指定了一个用户表单，则使用该用户表单。
- 如果没有直接为管理员分配用户表单，也没有通过管理员角色间接为其分配用户表单，则使用分配给该管理员的成员组织的用户表单（优先顺序从管理员的成员组织开始，直到 `Top` 的下一级）。
- 如果管理员的成员组织没有分配用户表单，则使用默认用户表单。

如果为该管理员分配了多个管理员角色，这些角色控制相同的组织，但指定不同的用户表单，则在管理员尝试创建或编辑这些组织中的用户时会显示错误消息。如果管理员尝试分配两个或多个管理员角色，这些角色控制相同的组织，但指定不同的用户表单，则会显示错误消息。如果未解决此冲突，则不能保存变更。

最终用户组织

“最终用户”组织为管理员提供了一种简便方法，以便将某些对象（如资源和角色）提供给最终用户。最终用户可以使用最终用户界面（第 38 页中的“登录到 Identity Manager 最终用户界面”）查看指定的对象，并且还可能会将这些对象分配给自己（暂挂批准进程）。

注 – 最终用户组织是在 Identity Manager 7.1.1 版中引入的。

以前，要为最终用户授予对 Identity Manager 配置对象（如角色、资源和任务等）的访问权限，管理员必须编辑配置对象并使用最终用户任务、最终用户资源和最终用户 authType。

今后，Sun 建议使用“最终用户”组织为最终用户提供 Identity Manager 配置对象的访问权限。

“最终用户”组织是由所有用户隐式控制的，使用户能够查看几种对象类型，包括任务、规则、角色和资源。不过，该组织最初没有成员对象。

“最终用户”组织是 `Top` 的成员，其中不能包含子组织。此外，“最终用户”组织不会显示在“帐户”页列表中。但是，在编辑对象（如角色、管理员角色、资源、策略和任务等）时，您可以使用管理员用户界面为“最终用户”组织提供任何对象。

当最终用户登录到最终用户界面时，将会出现以下情况：

- 最终用户将被授予对**最终用户**组织 (`ObjectGroup`) 的控制权限。
- Identity Manager 评估内置的最终用户受控组织规则，该规则自动为用户授予对规则所返回的任何组织名称的控制权限。（此规则是在 Identity Manager 7.1.1 版中添加的。有关详细信息，请参见第 197 页中的“最终用户受控组织规则”一节。）
- 最终用户将被授予在**最终用户**权能中指定的对象类型的权限。

最终用户受控组织规则

最终用户受控组织规则的输入参数是验证用户的视图。Identity Manager 希望该规则返回一个或多个组织，登录到最终用户界面的用户将控制这些组织。Identity Manager 希望该规则返回字符串（对于单个组织）或列表（对于多个组织）。

要管理这些对象，用户需要“最终用户管理员”权能。分配了“最终用户管理员”权能的用户可以查看和修改最终用户受控组织规则的内容。这些用户还可以查看和修改在“最终用户”权能中指定的对象类型。

默认情况下，“最终用户管理员”权能将分配给配置器用户。对于最终用户受控组织规则评估返回的列表或组织，所做的任何更改不会动态反映给已登录的用户。这些用户必须先登出，然后再重新登录才能看到这些更改。

如果最终用户受控组织规则返回一个无效的组织（例如，在 Identity Manager 中不存在的组织），则会在系统日志中记录该问题。要更正此问题，请登录到管理员用户界面并修复此规则。

管理工作项目

某些在 Identity Manager 中由任务生成的工作流进程可以创建操作项目或**工作项目**。这些工作项目可能是分配给 Identity Manager 帐户的批准请求或某些其他操作请求。

Identity Manager 将对界面“工作项目”区域中的所有工作项目进行分组，使您可以查看一个位置的所有暂挂请求并对其做出响应。

工作项目类型

工作项目可能属于以下类型之一：

- **批准**。新帐户或对帐户进行更改的批准请求。
- **证明**。查看和批准用户权利的请求。
- **修正**。修正或缓解用户帐户策略违规的请求。
- **其他**。除任何一种标准类型之外的操作项目请求。这可能是从自定义的工作流生成的操作请求。

要查看每种工作项目类型的暂挂工作项目，请在菜单中单击“工作项目”。

注 – 如果您是暂挂工作项目（或委托工作项目）的工作项目所有者，则在您登录 Identity Manager 用户界面时将显示“工作项目”列表。

使用工作项目请求

要对工作项目请求做出响应，请在界面的“工作项目”区域中单击工作项目类型之一。从请求列表中选择项目，然后单击用于指示您要执行操作的按钮之一。这些工作项目选项因工作项目类型而异。

有关对请求做出响应的详细信息，请参见以下主题：

- 第 202 页中的 “批准用户帐户”
- 第 424 页中的 “管理证明责任”
- 第 404 页中的 “遵循性违规修正和缓解”

查看工作项目历史

可以使用“工作项目”区域中的“历史”选项卡查看以前的工作项目操作的结果。

图 6–5 显示了工作项目历史的示例视图。

图 6–5 工作项目历史视图

委托工作项目

工作项目拥有者可以通过将工作项目委托给其他用户一段指定的时间来管理工作负荷。从主菜单中，您可以使用“工作项目”→“委托我的工作项目”页将未来的工作项目（如批准请求）委托给一个或多个用户（受托者）。用户无需批准者权能即可成为受托者。

注 – 委托功能仅适用于未来的工作项目。必须通过转发功能选择性地转发现有项目（列于“我的工作项目”之下）。

您可以从其他页中委托工作项目：

- 在管理员界面中，您可以在“创建用户”和“编辑用户”页（第 47 页中的 ““用户”页（创建/编辑/查看）”）中委托工作项目。单击“委托”表单选项卡。
- 在最终用户用户界面（第 36 页中的 “Identity Manager 最终用户界面”）中，用户可以单击“委托”菜单项。

在有效委托期内，受托者可以代表工作项目所有者批准工作项目。委托的工作项目包括受托者的姓名。

任何用户都可以为其将来的工作项目创建一个或多个委托。可编辑用户的管理员也可以代表该用户创建委托。不过，如果该用户无法委托给某个人，则管理员也无法委托给该人员。（就委托而言，管理员的控制范围与其进行委托时所代表的用户相同。）

审计日志条目

在批准或拒绝委托的工作项目时，审计日志条目将列出委托者的姓名。当创建或修改用户时，对用户委托批准者信息的更改将记录到审计日志条目的详细更改区域中。

查看当前委托

可以在“当前委托”页上查看委托。

▼ 查看当前委托

1. **在管理员界面中，单击主菜单中的“工作项目”。**
2. **单击次级菜单中的“委托我的工作项目”。**
   Identity Manager 将显示“当前委托”页，可以在其中查看和编辑当前有效的委托。

查看以前的委托

可以在“先前的委托”页上查看先前的委托。

▼ 查看先前的委托

1. **在管理员界面中，单击主菜单中的“工作项目”。**
2. **单击次级菜单中的“委托我的工作项目”。**
   将打开“当前委托”页。
3. **单击“前一个”。**
   将打开“先前的委托”页。可以使用先前委托的工作项目来设置新的委托。

创建委托

可以使用“新建委托”页来创建委托。

▼ 创建委托

1. **在管理员界面中，单击主菜单中的“工作项目”。**
2. **单击“委托我的工作项目”。**
   将打开“当前委托”页。

3 **单击“新建”。**

将打开“新建委托”页。

4 **按如下方式填写表单：**

a. **从“选择要委托的工作项目类型”选择列表中，选择一种工作项目类型。要委托所有工作项目，请选择“所有工作项目类型”。**

如果要委托角色类型、组织或资源工作项目，请使用箭头将选择内容从可用列移动到已选定列，以指定用于定义此委托的特定角色、组织或资源。

b. **将工作项目委托给。**

请选择以下任一选项：

- **选定用户**。选择此选项可以搜索您的控制范围内要成为受托者的用户（按姓名）。如果任一选定的受托者已委托其工作项目，则您将来的工作项目请求将委托给该受托者的受托者。
- **在“已选定用户”区域中选择一个或多个用户**。或者，单击“从搜索中添加”以打开搜索功能并搜索用户。单击“添加”将找到的用户添加到列表中。要从此列表中删除受托者，请选择该受托者，然后单击“删除”。
  - **我的管理员**。选择此选项可以将工作项目委托给您的管理员（如果已分配）。
  - **委托工作项目规则**。选择可返回 Identity Manager 用户名列表的规则，您可以将选定的工作项目类型委托给这些用户。

c. **开始日期。选择工作项目委托开始的日期。默认情况下，选定的日期从 12:01 a.m. 开始。**

d. **结束日期。选择工作项目委托结束的日期。默认情况下，选定的日期在 11:59 p.m. 结束。**

注 – 如果将工作项目委托一天，则可以将开始日期和结束日期选在同一天。

---

e. **单击“确定”可保存所做的选择，并返回到等待批准的工作项目列表。**

注 – 在设置委托后，在有效委托期内创建的所有工作项目都会添加到受托者列表中。如果结束委托或委托时间段到期，则会将委托的工作项目重新添加到您的列表中。这可能会导致您的列表中包含重复的工作项目。不过，在批准或拒绝某个工作项目时，将会自动从您的列表中删除重复的项目。

委托给删除的用户

在删除拥有任何暂挂工作项目的用户时，Identity Manager 的工作方式如下所示：

- 如果委托了暂挂工作项目并且尚未删除委托者，则将暂挂工作项目返回给委托者。
- 如果没有委托暂挂工作项目，或者委托了暂挂工作项目并删除了委托者，删除尝试将会失败，直至解决了用户的暂挂工作项目或将其转发给另一个用户。

结束委托

可以从“当前委托”页中结束一个或多个委托。

▼ 结束一个或多个委托

1. **在管理员界面中，单击主菜单中的“工作项目”。**
2. **单击次级菜单中的“委托我的工作项目”。**
   将打开“当前委托”页。
3. **选择一个或多个要结束的委托，然后单击“结束”。**
   Identity Manager 删除选定的委托配置，然后向您的暂挂工作项目列表返回任何选定类型的委托工作项目。

批准用户帐户

在将用户添加到 Identity Manager 系统后，指定为新帐户**批准者**的管理员必须对帐户创建进行验证。

Identity Manager 支持三种类别的批准：

- **组织**。需要批准要添加到组织的用户帐户。
- **角色**。需要批准要分配给角色的用户帐户。
- **资源**。需要批准要授权访问资源的用户帐户。

此外，如果启用了更改批准，并且对角色进行了更改，则会将更改批准工作项目发送至指定的角色所有者。

Identity Manager 支持通过**角色定义**进行更改批准。如果管理员更改了角色定义，则需要指定的角色所有者进行更改批准。角色所有者必须批准该工作项目才能进行更改。

注 –

- 您可以配置 Identity Manager 以获得数字签名的批准。有关说明，请参见第 204 页中的 “配置数字签名的批准和操作”。
- 不熟悉 Identity Manager 的管理员有时会将批准概念与听起来类似的证明概念混淆。虽然名称听起来类似，但批准和证明出现在不同的上下文中。

  批准关注的是验证新用户帐户。在将用户添加到 Identity Manager 后，可能需要进行一次或多次批准以确保新帐户获得了授权。

  证明关注的是验证现有用户是否在相应资源上仅具有相应权限。在周期性访问查看的过程中，可能会要求 Identity Manager 用户（证明者）证明其他用户的帐户详细信息（即，为该用户分配的资源）是否有效且正确无误。此过程称为证明。

设置帐户批准者

为组织、角色和资源批准设置帐户批准者是可选的，但建议进行此类设置。对于在其中设置批准者的每个类别，帐户创建至少都需要一个批准。如果一个批准者拒绝批准请求，则不会创建帐户。

可以将多个批准者分配给各个类别。因为一个类别内只需要一个批准，所以可设置多个批准者，以帮助确保不会延迟或停止工作流。如果一个批准者不可用，则其他批准者可用于处理请求。批准仅适用于帐户创建。默认情况下，帐户的更新和删除不需要批准。不过，您可以自定义此过程以要求进行批准。

可以通过使用 Identity Manager IDE 自定义工作流，以更改批准、捕获帐户删除以及捕获更新的流程。

有关 Identity Manager IDE 的信息，请访问 `https://identitymanager.dev.java.net`。有关工作流的信息以及更改批准工作流的说明示例，请参见《Sun Identity Manager Deployment Reference》中的第 1 章 “Workflow”。

Identity Manager 批准者可以批准或拒绝批准请求。

管理员可以在 Identity Manager 界面的“工作项目”区域中查看和管理暂挂批准。在“工作项目”页中，单击**我的工作项目**以查看暂挂批准。单击**批准**选项卡以管理批准。

对批准签名

要使用数字签名批准工作项目，您必须先按第 204 页中的 “配置数字签名的批准和操作”中所述设置数字签名。

▼ 对批准进行签名

1. 在 Identity Manager 管理员界面中，选择工作项目。
2. 单击批准选项卡。
3. 从列表中选择一个或多个批准。
4. 输入批准的注释，然后单击 Approve。
   Identity Manager 会给出提示，并询问您是否信任该 applet。
5. 单击 Always。
   Identity Manager 将显示一个含有日期的批准摘要。
6. 输入密钥库位置，或者单击浏览以找到密钥库位置。（在配置签名的批准期间设置此位置，如第 207 页中的“使用 PKCS12 为签名的批准启用服务器端配置”过程中的步骤 10m 所述。）
7. 输入密钥库密码（在配置签名的批准期间设置此密码，如第 207 页中的“使用 PKCS12 为签名的批准启用服务器端配置”过程中的步骤 10l 所述）。
8. 单击签名以批准请求。

更多信息 **对后续批准签名**

对某个批准签名之后，只需输入密钥库密码，然后单击 **Sign**，即可执行后续批准操作。（Identity Manager 将通过先前的批准记忆密钥库的位置。）

配置数字签名的批准和操作

可以使用以下信息和过程来设置数字签名。可以对以下项目进行数字签名：

- 批准（包括更改批准）
- 访问查看操作
- 遵从性违规的修正

本节讨论的主题说明了将证书和 CRL 添加到 Identity Manager 以获得签名批准所需的服务器端和客户端配置。

▼ 为签名的批准启用服务器端配置

1 **打开系统配置对象以进行编辑并设置**
`security.nonrepudiation.signedApprovals=true`。

有关编辑系统配置对象的说明，请参见第 102 页中的 “编辑 Identity Manager 配置对象”。

如果使用的是 PKCS11，您还必须设置
`security.nonrepudiation.defaultKeystoreType=PKCS11`。

如果使用的是自定义 PKCS11 密钥提供程序，您还必须设置
`security.nonrepudiation.defaultPKCS11KeyProvider=`**您的提供程序名称**。

注 – 有关何时需要编写自定义提供程序的详细信息，请参阅 REF（Resource Extension Facility，资源扩充工具）工具包中的以下项目：

```
com.sun.idm.ui.web.applet.transactionsigner.DefaultPKCS11KeyProvider (Javadoc)
REF/transactionsigner/SamplePKCS11KeyProvider
```

REF（Resource Extension Facility，资源扩充工具）工具包是在产品 CD 上的 `/REF` 目录中提供的，或者是随安装映像提供的。

---

2 **将证书颁发机构 (Certificate Authority, CA) 的证书添加为信任证书。为此，必须首先获得证书的副本。**
例如，如果要使用 Microsoft CA，请按类似以下的步骤操作：

   a. **转至** `http://`*IPAddress*`/certsrv`，**然后通过管理权限登录。**

   b. **选择 Retrieve the CA certificate or certificate revocation list，然后单击 Next。**

   c. **下载并保存 CA 证书。**

3 **将证书作为信任证书添加到 Identity Manager 中：**

   a. **从管理员界面中选择安全性，然后选择证书。Identity Manager 将显示“证书”页。**

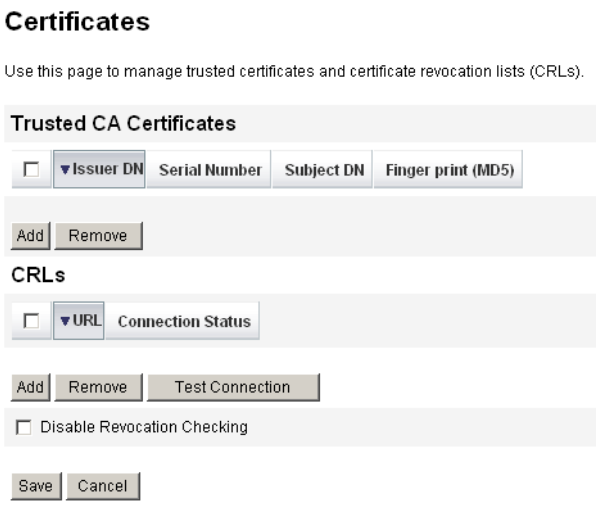


图 6–6 “证书”页

b. **在“信任 CA 证书”区域中，单击添加。Identity Manager 将显示“导入证书”页。**

c. **浏览到信任证书后将其选中，然后单击 Import。**
证书将立即显示在信任证书列表中。

4 **添加 CA 的证书撤销列表 (Certificate Revocation List, CRL)：**

a. **在 Certificates 页的 CRLs 区域中单击 Add。**

b. **输入 CA CRL 的 URL。**

注 –

- 证书撤销列表 (Certificate Revocation List, CRL) 是已被撤销或无效的证书序列号的列表。
- CA CRL 的 URL 可以是 http 或 LDAP。
- 对于每个 CA，从中分发 CRL 的 URL 都各不相同，可以通过浏览 CA 证书的 CRL 分发点扩展部分来确定其 URL。

---

5 **单击测试连接验证 URL。**

6 **单击保存。**

7 **使用 jarsigner 对 applets/`ts2.jar` 签名。**

注 – 有关详细信息，请访问 http://java.sun.com/j2se/1.5.0/docs/tooldocs/windows/jarsigner.html。Identity Manager 附带的 ts2.jar 文件使用自签名证书来签名，不应将其用于生产系统。在生产中，应使用由信任 CA 颁发的代码签名证书重新对此文件签名。

▼ 使用 PKCS12 为签名的批准启用服务器端配置

以下配置信息适用于使用 PKCS12 获得的签名批准。先获取证书和专用密钥，然后将其导出到 PKCS#12 密钥库中。例如，如果要使用 Microsoft CA，请按类似以下的步骤操作：

开始之前 Identity Manager 现在至少需要使用 JRE 1.5。

1. **使用 Internet Explorer 浏览到** http://*IPAddress*/certsrv，**然后通过管理权限登录。**
2. **选择“请求证书”，然后单击“下一步”。**
3. **选择“高级请求”，然后单击“下一步”。**
4. **单击“下一步”。**
5. **选择 "User for Certificate Template"。**
6. **选择以下选项：**
   a. **编辑密钥为可导出。**
   b. **启用强密钥保护。**
   c. **使用本地机器存储。**
7. **单击“提交”，然后单击“确定”。**
8. **单击“安装此证书”。**
9. **选择“运行”→ "mmc" 以启动 mmc。**
10. **添加证书插件：**
    a. **选择“控制台”→“添加/删除插件”。**
    b. **单击“添加”。**

c. 选择计算机帐户。

d. 单击“下一步”，然后单击“完成”。

e. 单击“关闭”。

f. 单击“确定”。

g. 转至“证书”→“个人”→“证书”。

h. 右键单击“管理员所有任务”→“导出”。

i. 单击“下一步”。

j. 单击“下一步”确认导出专用密钥。

k. 单击“下一步”。

l. 输入密码，然后单击“下一步”。

m. 文件 *CertificateLocation*。

n. 单击“下一步”，然后单击“完成”。单击“确定”进行确认。

注 – 请注意在客户端配置的步骤 10l（密码）和步骤 10m（证书位置）中使用的信息。您将需要此信息来对批准签名。

▼ 使用 PKCS11 为签名的批准启用客户端配置

如果将 PKCS11 用于签名的批准

- **请参阅 REF 工具包中的以下资源以了解配置信息：**

  `com.sun.idm.ui.web.applet.transactionsigner.DefaultPKCS11KeyProvider (Javadoc)`
  `REF/transactionsigner/SamplePKCS11KeyProvider`

  REF（Resource Extension Facility，资源扩充工具）工具包是在产品 CD 上的 `/REF` 目录中提供的，或者是随安装映像提供的。

查看事务签名

本节介绍了用于查看 Identity Manager 审计日志报告中的事务签名的过程。

▼ 查看事务签名

1. **在 Identity Manager 管理员界面中，选择报告。**
2. **在“运行报告”页中，从新建选项列表中选择审计日志报告。**
3. **在报告标题字段中输入标题（如“批准”）。**
4. **在组织选择区域中，选择所有组织。**
5. **选择操作选项，然后选择批准。**
6. **单击 Save 保存报告并返回至 Run Reports 页。**
7. **单击 Run 运行批准报告。**
8. **单击详细信息链接查看事务签名信息。**
   事务签名信息可以包含以下内容：
   - 颁发者
   - 主题
   - 证书序列号
   - 已签名的消息
   - 签名
   - 签名算法

配置 XMLDSIG 格式的签名批准

Identity Manager 允许将 XMLDSIG 格式的签名批准（包括 RFC 3161 兼容的数字时间戳）添加到 Identity Manager 批准进程中。在将 Identity Manager 配置为使用 XMLDSIG 签名批准时，不会向批准者显示任何更改，除非他们在审计日志中查看该批准。仅更改了审计日志记录中存储的签名批准的格式。

与 Identity Manager 中以前的签名批准一样，将在客户端计算机上启动一个 applet，并向批准者显示要签名的批准信息。然后，批准者选择用于对批准进行签名的密钥库和密钥。

在批准者对批准进行签名后，将创建一个包含该批准数据的 XMLDSIG 文档。此文档将返回到服务器，该服务器会验证 XMLDSIG 签名文档。如果验证成功，并且配置了 RFC 3161 数字时间戳，则还会为此文档生成数字时间戳。将检查从时间戳服务中心 (Timestamp Authority, TSA) 检索的时间戳是否有错误，并验证其证书。最后，如果验证成功，Identity Manager 将生成一个审计日志记录，它在 XML 二进制大对象列中包含 XMLDSIG 格式的签名批准对象。

批准数据格式

XMLDSIG 格式的批准对象的格式如下所示：

```
<XMLSignedData signedContent="...base64 transaction text ...">
   <XMLSignature>
      <TSATimestamp>
         ...The base64 encoded PKCS7 timestamp token returned by the TSA...
      </TSATimestamp
      <Signature>
        <SignedInfo>...XMLDSIG stuff...</SignedInfo>
        <SignatureValue>...base64 signature value</SignatureValue>
        <KeyInfo>...cert info for signer</KeyInfo>
      </Signature>
   </XMLSignature>
</XMLSignedData>
```

其中：

- `base64` 批准数据包含在 applet 中向批准者显示的实际批准数据文本（以 `base64` 格式编码）。
- `<TSATimestamp>` 元素包含来自时间戳服务中心 (Timestamp Authority, TSA) 的 `base64` 编码的 PKCS7 时间戳响应。
- 整个 `<Signature>` 由 XMLDSIG 签名数据组成。

该 XMLDSIG 文件存储在审计日志批准记录的 XML 列中。

安装和设置

使用 XMLDSIG 签名批准的安装和设置要求与 第 205 页中的 “为签名的批准启用服务器端配置”中介绍的要求相同，但还增加了一个步骤。除了对 `ts2.jar` 文件进行签名以外，还必须对 `xmlsec-1.4.2.jar` 文件进行签名。

批准配置

可以使用系统配置属性执行以下操作：

- 选择 `SignedData` 格式或 `XMLSignedData` 格式。请注意，每次只能配置一种格式，但管理员可以根据需要更改此设置。
- 包括从配置的 RFC 3161 时间戳服务中心 (Timestamp Authority, TSA) 检索的数字时间戳。
- 指定从中提取该时间戳的 URL（只能采用 HTTP 格式）。

要编辑这些属性，请使用 Identity Manager 调试页编辑系统配置对象。这些属性以及其他签名批准属性均位于 `security.nonrepudiation` 下面。

XMLDSIG 属性包括：

- `security.nonrepudiation.useXmlDigitalSignatures` 是一个布尔值，用于启用 XMLDSIG 签名。
- `security.nonrepudiation.timestampXmlDigitalSignatures` 是一个布尔值，其中包含 XMLDSIG 签名中的 RFC 3161 数字时间戳。
- `security.nonrepudiation.timestampServerURL` 是一个字符串值，其中的 URL 指向从中提取时间戳的基于 HTTP 的 TSA。

注 –

- 您必须先将现有的 `useSignedApprovals` 属性设置为 **`true`**，才能使任何以前的属性生效。
- Identity Manager 不支持对一个批准进行多次签名，也不支持为更一般性的置备请求提供签名批准。

◆ ◆ ◆ 第 7 章

7 数据加载和同步

本章提供了使用 Identity Manager 数据加载和同步功能的信息和过程。您将了解如何使用 Identity Manager的数据同步工具（搜索、协调和同步）将数据保持最新状态。

本章中的信息分为以下几个部分：

有关数据加载和同步在 Identity Manager 中的工作方式的详细说明，请参见《Sun Identity Manager Deployment Guide》中的第 3 章 “Data Loading and Synchronization”。

数据同步工具：使用哪一个？

Identity Manager 提供了几种可用于导入和同步帐户数据的工具。有关为给定任务选择正确工具的帮助，请参阅表 7–1。

注 – 有关数据加载和同步在 Identity Manager 中的工作方式的详细说明，请参见《Sun Identity Manager Deployment Guide》中的第 3 章 “Data Loading and Synchronization”。

表 7–1 使用数据同步工具执行的任务

如果要	请选择此功能
初次将资源帐户**引入** Identity Manager，在加载之前没有查看	从资源加载
初次将资源帐户**引入** Identity Manager，加载之前可以选择性地查看和编辑数据	提取到文件，从文件加载

表 7–1 使用数据同步工具执行的任务 （续）

如果要	请选择此功能
定期将资源帐户**引入** Identity Manager，根据配置的策略对每个帐户执行操作	协调资源
将资源帐户更改**推入**或**引入** Identity Manager	使用活动同步适配器进行同步（多个资源实现）

帐户搜索功能

Identity Manager 帐户搜索功能有助于加快部署和帐户创建任务的速度。

这些功能包括：

- **提取到文件**。将资源适配器返回的资源帐户提取到一个文件（采用 CSV 或 XML 格式）。在将数据导入 Identity Manager 之前，可以对此文件进行操作。
- **从文件加载**。读取文件（采用 CSV 或 XML 格式）中的帐户并将它们加载到 Identity Manager 中。
- **从资源加载**。结合其他两个搜索功能，从资源提取帐户并将它们直接加载到 Identity Manager 中。

使用这些工具可以创建新的 Identity Manager 用户，或者将某个资源上的帐户与现有 Identity Manager 用户帐户关联。

注 – 本节中的页面重点介绍如何使用 Identity Manager 的搜索功能。要了解数据加载和同步的详细信息，请参见《Sun Identity Manager Deployment Guide》中的第 3 章 “Data Loading and Synchronization”。

提取到文件

使用此功能将资源帐户从资源提取到一个 XML 或 CSV 文本文件中这样做可以在将提取数据导入 Identity Manager 之前查看和更改该数据。

▼ 提取帐户

1. **在菜单栏中选择“帐户”，然后选择“提取到文件”。**
2. **选择要从中提取帐户的资源。**
3. **为输出帐户信息选择文件格式。可以将数据提取到 XML 文件，或提取到以逗号分隔值 (CSV) 格式编排帐户属性的文本文件中。**

4 **单击“下载”。Identity Manager 将显示“文件下载”对话框，您可以在该对话框中选择保存或查看提取的文件。**

如果选择打开该文件，则可能需要选择查看程序。

从文件加载

可以使用此功能将资源帐户（通过 Identity Manager 从资源提取的帐户或从另一文件源提取的帐户）加载到 Identity Manager 中。由 Identity Manager 的“提取到文件”功能创建的文件为 XML 格式的文件。如果加载一列新用户，则数据文件通常采用 CSV 格式。

关于 CSV 文件格式

通常，要加载的帐户在一个电子表格中列出并以逗号分隔值 (Comma-separated Value, CSV) 格式保存，以便加载到 Identity Manager 中。

CSV 文件内容必须遵循以下格式准则：

- **第 1 行**。以逗号分隔的形式列出每个字段的列标题或模式属性。
- **第 2 行到最后**。以逗号分隔的形式列出在第 1 行中定义的每个属性的值。如果某个字段值没有数据，则该字段必须用相邻的逗号表示。

  例如，CVS 文件的前三行可能类似于下面的示例文件条目：

```
firstname,middleinitial,lastname,accountId,asciipassword,EmployeeID,Department,Phone
John,Q,Example,E1234,E1234,1234,Operations,555-222-1111
Jane,B,Doe,E1111,E1111,1111,,555-222-4444
```

  在此例中，请注意第二个用户 Jane Doe 没有部门。缺少的值用相邻的逗号 (,,) 表示。

▼ 加载帐户

1 **在管理员界面中，单击菜单中的“帐户”，然后单击从文件加载。**

Identity Manager 将显示“从文件加载帐户”页。

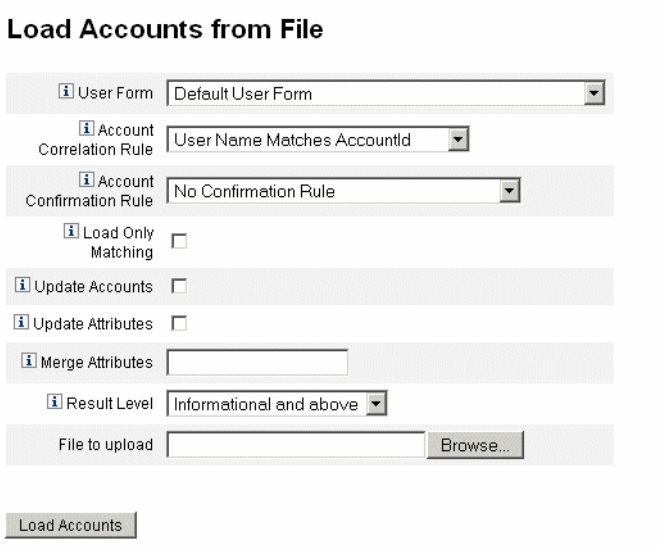


图 7–1 从文件加载

2 **可以使用该页指定所需的帐户加载选项。**

这些选项包括：

- **用户表单**。当加载过程创建了 Identity Manager 用户时，用户表单会分配组织以及角色、资源和其他属性。选择要应用于每个资源帐户的用户表单。
- **帐户关联规则**。帐户关联规则选择可能拥有每个无拥有者资源帐户的 Identity Manager 用户。如果给定无拥有者资源帐户的属性，关联规则会返回一个名称列表或属性条件列表，用于选择潜在拥有者。选择一个规则，以查找可能拥有每个无拥有者资源帐户的 Identity Manager 用户。
- **帐户确认规则**。帐户确认规则可将任何非拥有者从关联规则选择的潜在拥有者列表中清除。在给定某个 Identity Manager 用户和某个无拥有者的资源帐户的属性这些详细资料后，若用户拥有该帐户，则确认规则返回 true，否则返回 false。选择一个规则以测试资源帐户的每个潜在拥有者。如果选择“无确认规则”，Identity Manager 将接受所有潜在拥有者，而不进行确认。

注 – 如果在您的环境中，关联规则为每个帐户选择最多一个拥有者，则您不需要确认规则。

- **仅加载匹配项**。选择此选项可仅将与现有 Identity Manager 用户匹配的帐户加载到 Identity Manager 中。如果选择此选项，则加载将放弃任何不匹配的资源帐户。
- **更新属性**。选择此选项可使用所加载帐户的属性值替换当前 Identity Manager 用户的属性值。

- **合并属性**。输入一个或多个用逗号分隔的属性名，这些属性的值应被合并（去掉重复部分）而不被覆盖。此选项仅用于列表类型的属性，例如组和邮递列表。还必须选择“更新属性”选项。
- **结果级别**。选择一个阈值，加载进程将在达到该阈值时为帐户记录单独的结果：
  - **仅限错误**。仅在加载帐户的过程中产生错误消息时才记录单独结果。
  - **警告和错误**。在加载帐户过程中生成警告或错误消息时记录单独的结果。
  - **信息性及更高级别**。为每个帐户记录单独的结果。这会导致加载进程运行得更慢。

3 **在“要上载的文件”字段中，指定要加载的文件，然后单击“加载帐户”。**

注 –

- 如果输入文件不包含用户列，则必须选择确认规则以使加载正确进行。
- 与加载过程相关的任务实例名称基于输入文件名；因此，如果重复使用某文件名，则与最近的加载过程相关的任务实例将覆盖以前所有任务实例。

  第 215 页中的 “关于 CSV 文件格式”展示了“从文件加载”屏幕中的可用字段和选项。

如果帐户与现有用户匹配（或关联），则加载进程会将帐户合并到用户中。该进程也将通过任何不相关的输入帐户创建新的 Identity Manager 用户（除非指定“必需相关”）。

`bulkAction.maxParseErrors` 配置变量会设置加载文件时可发现的错误数的限制。默认情况下，限制为 10 个错误。如果发现的错误数达到了 `maxParseErrors` 的值，则会停止解析。

从资源加载

使用此功能可根据您指定的加载选项直接提取帐户并将其导入 Identity Manager。

▼ 导入帐户

1 **在管理员界面中，单击菜单中的“帐户”，然后单击“从资源加载”。**

将打开“从资源加载帐户”页。

2 **在“从资源加载帐户”页上指定加载选项。**

此页面的加载选项与“从文件加载”页（请参见第 215 页中的 “从文件加载”）上的加载选项相同。

帐户协调

可以使用协调功能，定期将 Identity Manager 中的资源帐户与资源上实际存在的帐户进行比较。协调将关联帐户数据并突出显示存在的差异。

注 – 本节中的页面重点介绍如何使用管理员界面执行协调任务。要了解协调的详细信息，请参见《Sun Identity Manager Deployment Guide》中的第 3 章 “Data Loading and Synchronization”。

协调简介

因为协调专用于进行中的比较，因此其具有以下特征：

- 比搜索过程更明确地诊断帐户情况，支持的响应也更广泛
- 被预定（搜索不能）
- 提供增量模式（搜索始终为完全模式）
- 检测本机更改（搜索不能）

也可以将协调配置为在处理资源过程中的下列每一点处启动任意工作流：

- 协调任何帐户之前
- 每个帐户
- 协调所有帐户之后

从“资源”区域访问 Identity Manager 协调功能。“资源”列表显示每个资源上次协调的时间及其当前协调状态。

注 – 协调是由 Identity Manager 的协调程序组件执行的。有关协调程序配置设置的信息，请参见相关参考手册。

关于协调策略

协调策略允许您按资源为每个协调任务建立一组响应。您可在策略中选择运行协调的服务器、确定协调发生的频率和时间，以及设置对协调期间遇到的每种情况作出响应。还可将协调配置为检测对帐户属性进行的本机更改（即，不是通过 Identity Manager 进行的更改）。

编辑协调策略

▼ 编辑协调策略

1. **在管理员界面中，单击菜单中的“资源”。**
2. **在“资源列表”中选择一种资源。**
3. **在“资源操作”列表中，选择“编辑协调策略”。**

   Identity Manager 将显示“编辑协调策略”页面，可在其中进行下列策略选择：

   - **协调服务器**。在群集环境中，每个服务器都可以运行协调。请在策略中指定哪个 Identity Manager 服务器将运行针对资源的协调。
   - **协调模式**。可以在不同模式下执行协调，这样能够将不同质量的结果最优化：
     - **完全协调**。协调最彻底（以速度为代价）。
     - **增量式协调**。协调速度最快（以彻底性为代价）。

       在策略中选择 Identity Manager 对资源运行协调应该采用的模式。选择“不协调”禁用针对目标资源的协调。
   - **完全协调进度表**。如果启用完全模式协调，则按固定的进度表自动执行协调。在策略中指定针对资源运行完全式协调的频率。
     - 选择“继承默认策略”选项可从更高级策略中继承指定的进度表。
     - 清除“继承默认策略”选项可指定一个进度表。使用提供的字段建立一个循环进度表，或使用“任务进度表重复”规则对协调进度表进行自定义调整。有关创建任务进度表重复规则的信息，请参见第 225 页中的 “使用任务进度表重复规则”。
   - **增量式协调进度表**。如果启用增量模式协调，则按固定的进度表自动执行协调。
     - 选择“继承默认策略”选项可从更高级策略继承进度表。
     - 清除“继承默认策略”选项可指定一个进度表。使用提供的字段建立一个循环进度表，或使用“任务进度表重复”规则对协调进度表进行自定义调整。有关创建任务进度表重复规则的信息，请参见第 225 页中的 “使用任务进度表重复规则”。

     注 – 并非所有资源都支持增量式协调。

   - **属性级协调**。可以将协调配置为检测对帐户属性进行的本机更改（即，不是通过 Identity Manager 进行的更改）。指定协调是否应检测对协调的帐户属性中指定的属性进行的本机更改。
   - **帐户关联规则**。帐户关联规则选择可能拥有每个无拥有者资源帐户的 Identity Manager 用户。如果给定无拥有者资源帐户的属性，关联规则会返回一个名称列表或属性条件列表，用于选择潜在拥有者。选择一个规则，以查找可能拥有每个无拥有者资源帐户的 Identity Manager 用户。

- **帐户确认规则**。帐户确认规则可将任何非拥有者从关联规则选择的潜在拥有者列表中清除。在给定某个 Identity Manager 用户和某个无拥有者的资源帐户的属性这些详细资料后，若用户拥有该帐户，则确认规则返回 true，否则返回 false。选择一个规则以测试资源帐户的每个潜在拥有者。如果选择“无确认规则”，Identity Manager 将接受所有潜在拥有者，而不进行确认。

  注 – 如果在您的环境中，关联规则为每个帐户选择最多一个拥有者，则您不需要确认规则。

- **代理管理员**。指定执行协调响应时使用的管理员。协调只能执行允许指定代理管理员执行的那些操作。响应将使用与该管理员关联的用户表单（如果需要）。

  还可以选择“无代理管理员”选项。选择后，可以查看协调结果，但不会运行响应操作或工作流。

- **情况选项**（和“响应”）。协调会识别多种类型的情况。下面介绍了这些情况。请在“响应”列中指定协调应执行的任何操作。
  - **已确认**。所需帐户存在。

    要标记为“已确认”，必须满足以下条件：
    - Identity Manager 要求帐户必须存在。
    - 帐户在资源上存在。
  - **冲突**。为两个或多个 Identity Manager 用户分配了资源上的同一帐户。
  - **已删除**。所需帐户不存在。

    要标记为“已删除”，必须满足以下条件：
    - Identity Manager 要求帐户必须存在。
    - 帐户在资源上不存在。
  - **找到**。协调进程在分配的资源上找到匹配帐户。

    要标记为“找到”，必须满足以下条件：
    - Identity Manager 不要求帐户必须存在。（如果已将资源分配给用户，但尚未进行置备，则帐户可以在资源上存在，也可以不存在。）
    - 帐户在资源上存在。
  - **缺少**。分配给用户的资源上不存在匹配的帐户。

    要标记为“缺少”，必须满足以下条件：
    - Identity Manager 不要求帐户必须存在。（如果已将资源分配给用户，但尚未进行置备，则帐户可以在资源上存在，也可以不存在。）
    - 帐户在资源上不存在。
  - **已取消分配**。协调进程在未分配给用户的资源上找到匹配帐户。

    要标记为“取消分配”，必须满足以下条件：

- Identity Manager 不要求帐户必须存在。（如果没有将资源分配给用户，则 Identity Manager 不要求帐户必须存在。）
- 帐户在资源上存在。

- **不匹配**。资源帐户不匹配任何用户。
- **有争议**。资源帐户匹配多个用户。

  从这些响应选项（可用选项因情况而异）中选择一个：

  - **基于资源帐户创建新的 Identity Manager 用户**。运行资源帐户属性的用户表单以创建新用户。该资源帐户不会因任何更改而被更新。
  - **为 Identity Manager 用户创建资源帐户**。使用用户表单重新生成资源帐户属性，以重新创建缺少的资源帐户。
  - **“删除资源帐户”和“禁用资源帐户”**。删除/禁用资源上的帐户。
  - **“将资源帐户与 Identity Manager 用户链接”和“解除资源帐户与 Identity Manager 用户的链接”**。向用户添加资源帐户分配或从用户中删除资源帐户分配。未执行任何表单处理。
  - **不执行任何操作**。如果不希望协调执行修复，请选择此选项。

    您可以手动修复协调发现的任何帐户情况。在菜单中单击“资源”→“检查帐户索引”。可以从中浏览为所有已协调的帐户记录的情况。右键单击某个帐户，将会看到一个有效修复选项的列表。有关详细信息，请参见第 224 页中的 “检查帐户索引”。

- **协调前工作流**。可以将协调配置为在对资源进行协调之前运行用户指定的工作流。指定协调应运行的工作流。如果没有要运行的工作流，请选择 "Do not run workflow"。
- **每一帐户工作流**。可以将协调配置为在对资源帐户情况作出响应后运行用户指定的工作流。指定协调应运行的工作流。如果没有要运行的工作流，请选择 "Do not run workflow"。
- **协调后工作流**。可以将协调配置为在完成资源协调后运行用户指定的工作流。指定协调应运行的工作流。如果没有要运行的工作流，请选择 **Do not run workflow**。
- **说明情况**。如果启用，协调将会记录其他信息，以说明如何对帐户情况进行分类。默认情况下禁用此选项。记录解释会使协调进程运行时间增加。
- **错误限制**。如果启用，在处理过程中发生指定数量的错误后，将自动终止协调。值 0 表示对错误数没有限制。取消选择“继承默认策略”选项，将显示“允许的最多错误数”字段，在其中输入值。
- **最大本机删除帐户数**。此选项是一项安全保护功能，用于计算资源上缺少的帐户数；如果超过某一阈值，则禁止协调程序解除这些帐户的链接。

  要启用此功能，请清除“继承默认策略”复选框，然后在“允许的最大本机删除帐户数”字段中指定一个百分比。必须将阈值设置为从 0 到 100 的整数百分比。（0 表示禁用此功能。）

  如果删除的帐户百分比超过该阈值，协调将继续执行与缺少的帐户无关的所有处理并完成此过程，但会出现一个错误。

单击“保存”以保存策略更改。

启动协调

本节介绍了两个用于启动协调任务的选项：

- 按调度间隔运行协调
- 立即协调

▼ 定期运行协调

1. **按第 219 页中的“编辑协调策略”中所述打开“编辑协调策略”页。**
2. **指定协调进度表参数。**
   协调将按照您在策略中设置的参数运行。

▼ 立即运行协调

1. **在管理员界面中，单击菜单中的“资源”。**
2. **在“资源列表”中选择一种资源。**
3. **从“资源操作”列表中选择一个选项。**
   这些选项包括：
   - 立即进行完全式协调
   - 立即进行增量式协调
     协调将按照您在策略中设置的参数运行。如果在策略中针对协调设置了定期进度表，则协调将继续按指定方式运行。

▼ 取消协调

1. **在管理员界面中，单击菜单中的“资源”。**
2. **在“资源列表”中，选择要取消协调的资源。**
3. **找到“资源操作”列表，然后选择“取消协调”。**

查看协调状态

可以使用两种主要方法来查看协调状态。要查看详细的协调状态，请打开特定资源的“协调摘要结果”页。资源列表中也会直接提供有限的协调状态。

▼ 查看详细的协调状态

可以使用“协调摘要结果”页来查看详细的协调状态。

1. **在管理员界面中，单击菜单中的“资源”。**
2. **在“资源列表”中，选择要查看协调状态的资源。**
3. **找到“资源操作”列表，然后选择“查看协调状态”。**
   将打开该资源的“协调摘要结果”页。

▼ 在“资源列表”中查看协调状态

您也可以从“资源列表”中查看协调状态。

1. **打开管理员界面。**
2. **在主菜单中单击“资源”。**
   状态列可报告以下协调状态情况：
   - **未知**。状态未知。最新协调任务的结果不可用。
   - **已禁用**。协调已禁用。
   - **失败**。未能完成最新的协调。
   - **成功**。已成功完成最新的协调。
   - **完成但有错误**。最新协调已完成，但出现错误。

注 – 必须刷新此页才能查看状态变化。（这些信息不会自动刷新。）

使用帐户索引

帐户索引会记录 Identity Manager 已知的每个资源帐户的最新已知状态。它主要由协调来维护，但是需要时其他 Identity Manager 功能也会更新帐户索引。

搜索工具不更新帐户索引。

▼ 搜索帐户索引

可以搜索帐户索引以查看给定资源帐户的最新已知状态。

1. **在管理员界面中，单击菜单中的“资源”。**
2. **在“资源列表”中，选择要搜索帐户索引的资源。**

3 **找到“资源操作”列表，然后选择“搜索帐户索引”。**
将打开“搜索帐户索引”页。

4 **选择一种搜索类型，然后输入或选择搜索属性。**

- **资源帐户名**。选择此选项，再选择其中一个修改符号（开头为、包含或是），然后输入部分帐户名称或完整的帐户名称。
- **资源为其中之一**。选择此选项，然后从列表中选择一个或多个资源，以查找位于指定资源上的已协调帐户。
- **拥有者**。选择此选项，选择一个修改符号（开头为、包含或是），然后输入拥有者的完整或部分名称。要搜索无所有者帐户，请在 UNMATCHED 或 DISPUTED 情况下进行搜索。
- **情况为其中之一**。选择此选项，然后从列表中选择一种或多种情况，以查找处于指定情况下的已协调帐户。

5 **单击“搜索”以根据搜索参数来搜索帐户。要限制搜索结果，也可将“限制”结果中的数量指定为第一个字段。默认限制为找到的前 1000 个帐户。**
单击“重设查询”以清除该页并进行新的选择。

检查帐户索引

也可以查看所有 Identity Manager 用户帐户，并可选择对每个用户分别协调帐户。

▼ 检查帐户索引

1 **在管理员界面中，单击菜单中的“资源”。**

2 **单击次级菜单中的“检查帐户索引”。**
将打开“检查帐户索引”页。

表格会显示 Identity Manager 已知的所有资源帐户（无论 Identity Manager 用户是否拥有该帐户）。此信息按资源或 Identity Manager 组织分组。要更改此视图，请从 "Change index view" 列表中进行选择。

使用帐户

要使用资源上的帐户，请选择“按资源分组”索引视图。Identity Manager 会针对每种类型的资源显示文件夹。通过展开文件夹导航到特定资源。单击资源旁边的 + 或 - 以显示 Identity Manager 已知的所有资源帐户。

自上次对资源进行协调以来直接添加到该资源的帐户不会显示出来。

根据给定帐户的当前情况，可以执行几种操作。右键单击某个帐户，将会看到一个有效修复选项的列表。也可以查看帐户详细信息或选择协调该帐户。

使用用户

要使用 Identity Manager 用户，请选择“按用户分组”索引视图。在此视图中，Identity Manager 用户和组织显示为类似“帐户列表”页的分层结构。要查看当前分配给 Identity Manager 中某个用户的帐户，请导航到该用户并单击用户名旁边的指示符。在该用户名的下方将显示该用户的所有帐户和 Identity Manager 已知的这些帐户的当前状态。

根据给定帐户的当前情况，可以执行几种操作。也可以查看帐户详细信息或选择协调该帐户。

使用任务进度表重复规则

可以使用任务进度表重复规则来调整协调进度表。例如，如果要将预定在星期六进行的协调推迟到下星期一，可使用任务进度表重复规则。

可以使用任务进度表重复规则来调整完全和增量式协调的进度表。

有关如何选择任务进度表重复规则的信息，请参见第 219 页中的 “编辑协调策略”。

如何安排协调运行时间

在完成协调作业后，协调程序组件将检查其下次的预定运行时间。

首先，协调程序查看默认进度表以获取其下次运行时间。接下来，协调程序运行所有适用的任务进度表重复规则，以确定是否需要进行进度表调整。如果需要调整，规则进度表将覆盖该协调的默认进度表。

注 – 任务进度表重复规则无法覆写默认进度表。它们只能针对每个作业覆盖预定的开始时间。

▼ 查看“接受所有日期”示例规则

本节介绍了内置的“接受所有日期”示例规则。

1. **在文本编辑器中，打开位于 Identity Manager 的 `sample` 目录中的 `ReconRules.xml`。**

2. **搜索名为 `SCHEDULING_RULE_ACCEPT_ALL_DATES` 的规则。**

   要在“任务进度表重复规则”下拉菜单（在“编辑协调策略”页上）中列出规则，必须将规则的 `subtype` 属性设置为 `SUBTYPE_TASKSCHEDULE_REPETITION_RULE`：

   ```
   <Rule subtype='SUBTYPE_TASKSCHEDULE_REPETITION_RULE'
   name='SCHEDULING_RULE_ACCEPT_ALL_DATES'>
   ```

   正如前面所述，任务进度表重复规则可以修改默认协调进度表。

calculatedNextDate 变量可以接受按默认方式计算的下一个日期，也可以返回一个不同的日期。正如该示例规则所编写的，calculatedNextDate 无条件地接受默认日期，如以下摘录中所示：

```
<RuleArgument name='calculatedNextDate'/>
<block>
  <ref>calculatedNextDate</ref>
</block>
```

要创建自定义进度表，请替换 <block> 元素之间的规则逻辑。例如，要将协调开始时间更改为星期六上午 10:00，<block> 元素之间应包含以下 JavaScript：

```
<block>
  <script>
     var calculatedNextDate = env.get('calculatedNextDate');

    // Test to see if this task is scheduled for a Saturday
    // (Note that 6 is used to denote Saturday in JavaScript)
    if(calculatedNextDate.getDay() == 6) {
      // If so, set the time to 10:00:00
      calculatedNextDate.setHours(10);
      calculatedNextDate.setMinutes(0);
      calculatedNextDate.setSeconds(0);
    }
    // Return the modified date
    calculatedNextDate;
  </script>
</block>
```

在第 225 页中的 “查看“接受所有日期”示例规则”中，最初将 calculatedNextDate 设置为默认预定时间。如果下次的预定运行日期为星期六，则规则将协调安排在 10:00 开始运行。如果下次的预定运行日期不是星期六，则第 225 页中的 “查看“接受所有日期”示例规则”将返回 calculatedNextDate（而未进行任何时间调整）并使用默认进度表。

有关创建用于 Identity Manager 的自定义规则的详细信息，请参见《Sun Identity Manager Deployment Reference》中的第 4 章 “Working with Rules”。

活动同步适配器

Identity Manager 活动同步功能允许存储在**授权外部资源**（如应用程序或数据库）中的信息与 Identity Manager 用户数据同步。为 Identity Manager 资源配置同步可使其能够**侦听**或轮询对授权资源的更改。

可通过在资源同步策略中指定输入表单（针对相应目标对象类型），配置资源属性更改流向 Identity Manager 的方式。

注 – 本章中的页面重点介绍如何使用管理员界面执行活动同步任务。要了解活动同步的详细信息，请参见《Sun Identity Manager Deployment Guide》中的第 3 章 “Data Loading and Synchronization”。

配置同步

Identity Manager 使用同步策略为资源启用同步。

▼ 编辑或配置同步

每个资源均具有自己的同步策略。可以使用以下步骤配置或编辑同步策略：

1. **在管理员界面中，单击菜单中的“资源”。**
2. **在“资源列表”中，选择要配置同步的资源。**
3. **找到“资源操作”列表，然后选择“编辑同步策略”。**

   将打开该资源的“编辑同步”页。

   在 "Edit Synchronization Policy" 页中指定以下选项以配置同步：

   - **目标对象类型**。选择要应用策略的用户类型：Identity Manager 用户或服务提供者用户。

     注 – 在 服务提供者 实现中，必须配置一个同步策略（将“服务提供者用户”指定为对象类型），以便为这些用户启用数据同步。有关服务提供者用户的详细信息，请参见第 17 章，服务提供者管理。

   - **调度设置**。使用此部分可指定启动方法以及轮询进度表。

     您可以指定以下启动类型：

     - **“自动”或“以故障转移方式自动启动”**。启动 Identity System 时启动授权源。
     - **手动**。要求管理员启动授权源。
     - **已禁用**。禁用资源。

       可以使用“开始日期”和“开始时间”选项指定何时开始轮询。通过选择间隔并输入间隔值（秒、分钟、小时、天、周、月）可指定轮询周期。

       注 – 如果更改了启动方法或轮询进度表，则必须重新启动服务器以使更改生效。

如果您设置的轮询开始日期和时间还未到达，则轮询将按指定的时间开始。如果您设置的轮询开始日期和时间已经过去，Identity Manager 将根据此信息和轮询间隔确定轮询开始的时间。

例如：

- 为资源配置活动同步的时间为 2005 年 7 月 18 日（星期二）。
- 将资源设置为每周轮询，开始日期为 2005 年 7 月 4 日（星期一）的上午 9:00。

在这种情况下，资源将于 2005 年 7 月 25 日（下一个星期一）开始轮询。

如果未指定开始日期或时间，则资源将立即开始轮询。如果采用此方法，则每次应用服务器重新启动时，为活动同步配置的所有资源均将立即开始轮询。典型的方法是设置开始日期和时间。

- **同步服务器**。在群集环境中，每个服务器都可以运行同步。选择某个选项可指定将用于运行资源同步的服务器。
  - 如果同步运行的位置并不重要，请选择“使用任何可用服务器”。同步启动时，将从一组可用的服务器中选择一个服务器。
  - 选择“使用 `waveset.properties` 中的设置”可使用其中指定的服务器来运行同步。（此功能已过时。）
  - 选择“使用指定服务器”，然后从“同步服务器”列表中选择一个或多个可用服务器，可选择特定服务器来运行同步。
- **特定于资源的设置**。使用此部分可指定同步以何种方式确定要为资源处理的数据。
- **通用设置**。为数据同步活动指定常规设置。

  这些设置包括：
  - **代理管理员**。选择将处理更新的管理员。所有操作将通过分配给此管理员的权能进行授权。您应选择具有空用户表单的代理管理员。
  - **输入表单**。选择将处理数据更新的输入表单。此可选配置项目使属性可以在保存到帐户上之前被转换。
  - **规则（可选）**。选择在数据同步过程中使用的规则。

    您可以指定以下内容：
    - **进程规则**。选择此规则可指定要为每个传入帐户运行的进程规则。此选择将覆盖所有其他选项。如果指定了进程规则，则会为每一行运行该进程，而不管资源上的其他设置如何。既可以是进程名称，也可以是进程名称的评估规则。
    - **关联规则**。选择关联规则可以覆盖在资源的协调策略中指定的关联规则。关联规则使资源帐户与 Identity System 帐户相关联。
    - **确认规则**。选择确认规则可以覆盖在资源的协调策略中指定的确认规则。

- **解决进程规则**。选择此规则可指定在数据供应的记录中存在多个匹配项时将运行的任务定义的名称。这应该是提示管理员进行手动操作的进程。既可以是进程名称，也可以是进程名称的评估规则。
- **删除规则**。选择将针对每个传入的用户更新进行评估并返回 true 或 false 的规则，以确定是否应进行删除操作。

- **创建不匹配帐户**。启用此选项 (true) 后，适配器将尝试创建在 Identity Manager 系统中未找到的帐户。如果未启用此选项，则适配器将通过由 "Resolve Process Rule" 返回的进程来运行帐户。
- **日志设置**。为日志记录选项指定值。

  日志记录选项包含以下内容：

  - **最大日志归档数**。如果大于零，则保留最新的 `N` 个日志文件。如果等于零，则重复使用单个日志文件。如果为 `-1`，则保留日志文件。
  - **最长活动日志使用期限**。在此时间段过后，将对活动日志进行归档。如果时间为零，则不发生基于时间的归档。如果“最大日志归档数”为零，则在指定时间段之后，活动日志将被截断并重新使用。此使用期限条件将独立于“最大日志文件大小”指定的时间条件进行评估。

    输入数字，然后选择时间单位（天、小时、分钟、月、秒或周）。默认单位是天。
  - **日志文件路径**。输入要创建活动和归档日志文件的目录的路径。日志文件名将以资源名称开头。
  - **最大日志文件大小**。输入活动日志文件的最大大小（以字节为单位）。当活动日志文件大小达到最大值时，该文件将被归档。如果“最大日志归档数”为零，则在指定时间段之后，活动日志将被截断并重新使用。此大小条件将独立于“最长活动日志使用期限”指定的使用期限条件进行评估。
  - **日志级别**。指定日志记录级别。

    可以使用以下日志记录级别：

    - **0**. 不记录
    - **1**. 错误
    - **2**. 信息
    - **3**. 详细
    - **4**. 调试

4 **单击“保存”以保存资源的策略设置。**

编辑活动同步适配器

在编辑活动同步适配器之前，请停止同步。

▼ 停止同步

1 **打开“编辑同步”页。（有关说明，请参见第 227 页中的“编辑或配置同步”。）**

2 **在“调度设置”下面，找到“启动类型”，然后选择“已禁用”。**
对于服务提供者用户，请取消选择“启用同步”选项。

将显示警告消息，指示已禁用活动同步。

3 **单击“保存”。**
为资源禁用同步将导致在保存更改时停止同步任务。

调节活动同步适配器性能

由于同步是后台任务，因此活动同步适配器配置可能会影响服务器性能。

调节活动同步适配器性能涉及以下任务：

通过资源列表管理活动同步适配器。选择活动同步适配器，然后从“资源操作”列表的**同步**部分中选择启动、停止和状态刷新控制操作。

更改轮询时间间隔

轮询时间间隔决定活动同步适配器何时开始处理新信息。应根据正在执行的活动类型确定轮询时间间隔。例如，如果适配器每次从数据库读入相当长的用户列表并在 Identity Manager 中更新所有用户，则可以考虑在每天早晨运行此进程。某些适配器可能需要快速搜索要处理的新项目，可以设置为每分钟运行一次。

指定运行适配器的主机

要指定运行适配器的主机，请编辑 `waveset.properties` 文件中的 `sources.hosts` 属性。

指定以下设置之一：

- 设置 `sources.hosts=`*hostname1,hostname2,hostname3*。此设置列出了要运行活动同步适配器的计算机的主机名。适配器将在此字段中列出的第一个可用主机上运行。

注 – 输入的 *hostname* 必须与 Identity Manager 服务器列表中的条目匹配。可以通过 "Configure" 选项卡查看服务器列表。

- 设置 `sources.hosts=localhost`。通过该设置，适配器将在尝试为资源启动活动同步的第一个 Identity Manager 服务器上运行。

  注 – 在群集环境中，如需指定特定服务器，应使用第一个选项。

  此属性设置仅适用于 Identity Manager 用户同步。服务提供商用户同步的主机配置将由同步策略来确定。

可将需要更多内存和 CPU 循环的活动同步适配器配置为在专用服务器上运行，以帮助平衡系统负载。

启动和停止

可禁用、手动启动或自动启动活动同步适配器。要启动或停止活动同步适配器，您必须具有相应的管理员权能以更改活动同步资源。有关管理员权能的信息，请参见第 184 页中的 “权能类别”。

如果将适配器设置为自动启动，则当应用服务器重新启动时，该适配器也将重新启动。启动适配器后，它将立即运行并按指定的轮询时间间隔执行。如果您停止某一适配器，则它将在下次检查停止标志时停止。

适配器日志记录

适配器日志捕获有关适配器当前处理情况的信息。日志捕获的详细信息量取决于您为该日志设置的日志级别。适配器日志对调试问题和查看适配器处理进度都很有用。

每个适配器都有自己的日志文件、路径和日志级别。可以在“同步策略”的“日志”部分中为相应的用户类型（Identity Manager 用户或服务提供者用户）指定这些值。

只能在适配器已经停止时删除适配器日志。大多数情况下，最好在删除适配器日志之前对其进行复制，以便归档。

◆ ◆ ◆ 第 8 章

报告

Identity Manager 可以报告自动和手动系统活动。强健的报告功能组可以随时捕获和查看有关 Identity Manager 用户的重要访问信息和统计信息。

在本章中，您将了解 Identity Manager 报告类型，如何创建、运行和通过电子邮件发送报告，以及如何下载报告信息。

本章分为以下几个主题：

使用报告

在 Identity Manager 中，报告被视为一类特殊任务。因此，可以在 Identity Manager 管理员界面的两个区域使用报告：

- **报告（运行报告）**。可以使用“运行报告”区域定义、运行、删除和下载报告。只有具有足够权能的管理员才可以定义、运行、删除和下载报告。有关详细信息，请参见附录 D，权能定义。
- **服务器任务**。在定义报告后，可以转到“预定任务”区域（“服务器任务”→“管理进度表”）以调度和修改报告任务。要进行调度，TaskDefinition 对象必须包含 `visibility=schedule`。请使用调试页进行此更改。有关详细信息，请参见第 102 页中的 “编辑 Identity Manager 配置对象”。

报告类型

报告分为以下两种类别：

- **Identity Manager 报告**。包含多种报告类型，其中包括实时、摘要、审计日志、系统日志以及使用情况报告。
- **审计者报告**。提供有助于您根据审计策略中定义的条件来管理用户遵循性的信息。

在这两种类别中，可以进一步将报告划分为各种报告类型。本章后续部分详细介绍了这些报告类型。从第 239 页中的 “Identity Manager 报告”开始介绍 Identity Manager 报告，从第 246 页中的 “Auditor 报告”开始介绍了审计者报告。

有关如何查看 Identity Manager 报告和审计者报告的说明，请参见第 235 页中的 “查看报告”。

运行报告

▼ 运行报告

1 **在管理员界面中，单击主菜单中的“报告”。**

将打开“运行报告”页。

2 **要查看可用 Identity Manager 报告列表，请在“报告类型”下拉菜单中选择“Identity Manager 报告”。（默认情况下，将选择此选项。）**

要查看可用审计者报告列表，请在“报告类型”下拉菜单中选择“审计者报告”。有关详细信息，请参见第 15 章，审计：监视遵循性中的第 401 页中的 “使用审计者报告”。

图 8–1 显示“运行报告”页的示例。在“报告类型”下拉菜单中选择了“审计者报告”。

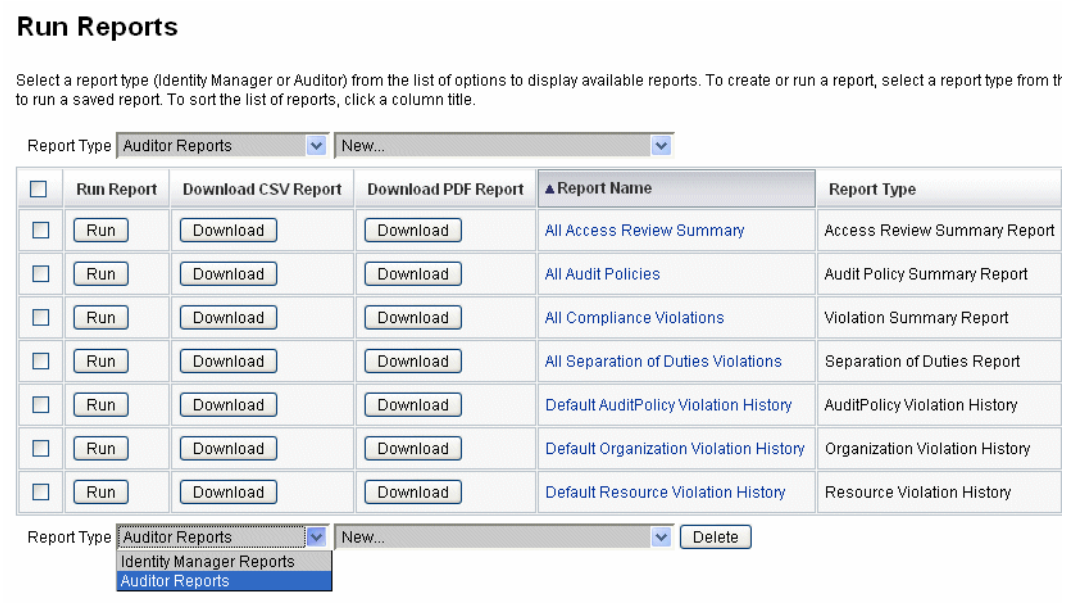


图 8–1 运行报告选项

3 **单击“运行”以运行报告。**

注 – 要允许同时运行同一个报告的多个实例，请编辑该报告并选择“允许同时执行报告”选项。通过启用此选项，多个管理员可以同时运行同一个报告。

如果同时运行同一个报告的两个或更多实例，将在每个报告名称后面附加管理员 ID 和时间戳。

查看报告

在从“运行报告”页中运行报告后，您可以立即查看输出或稍后查看输出。

▼ 查看报告

1 **在管理员界面中，单击主菜单中的“报告”。**
将打开“运行报告”页。

2 **单击“查看报告”选项卡。**
将打开“查看报告”页。

3 **单击一个报告以进行查看。**

创建报告

本节介绍如何创建不基于现有报告的新 Identity Manager 报告或 Identity Auditor 报告。

注 – 要修改现有报告并使用新名称进行保存，请参见下一节中的第 236 页中的 “编辑和克隆报告”。

▼ 创建新报告

1. **在管理员界面中，单击主菜单中的“报告”。**
   将打开“运行报告”页。

2. **使用“报告类型”下拉菜单选择一种报告类别。**
   共有两种报告类别：
   - Identity Manager 报告
   - Identity Auditor 报告

3. **使用下一个下拉菜单选择要创建的特定报告类型。（此菜单顶部显示“新建”。）**
   Identity Manager 将显示“定义报告”页，您可以在其中选择创建、运行或保存报告的选项。
   输入并选择了报告条件后，您可以执行以下操作：
   - 运行报告而不保存。单击“运行”以运行报告。Identity Manager 不保存报告（如果定义新报告）或更改的报告条件（如果编辑现有报告）。
   - 保存报告。单击“保存”以保存报告。保存后，您可从“运行报告”页（报告的列表）运行报告。

   有关运行报告的详细信息，请参见第 234 页中的 “运行报告”。

编辑和克隆报告

本节介绍如何修改或克隆现有报告，并使用新名称进行保存。

▼ 编辑或克隆报告

1. **在管理员界面中，单击主菜单中的“报告”。**
   将打开“运行报告”页。

2. **使用“报告类型”下拉菜单选择一种报告类别。**

共有两种报告类别：

- Identity Manager 报告
- Auditor 报告

  报告表将显示属于选定类别中的现有报告。

3 **单击一个报告名称以进行编辑。**

4 **要编辑报告，请根据需要调整报告参数，然后单击“保存”。**

要克隆报告，请输入新的报告名称。根据需要调整报告参数，然后单击“保存”以使用新名称进行保存。

发送电子邮件报告

创建或编辑报告时，可以选择选项，通过电子邮件将报告结果发送给一个或多个电子邮件收件人。选择此选项时，页面将刷新并提示输入电子邮件收件人的地址。输入一个或多个地址，中间用逗号分隔。

还可以为要附加到电子邮件的报告选择以下格式之一：

- **附加 CSV 格式**。以逗号分隔值 (Comma-separated Value, CVS) 格式附加报告结果。
- **附加 PDF 格式**。以可移植文档格式 (Portable Document Format, PDF) 附加报告结果。

调度报告

可通过选择以下选项之一，立即运行报告或安排定期运行报告：

- 选择**“报告”→“运行报告”**以立即运行保存的报告。在报告列表中，单击“运行”。Identity Manager 将运行报告，然后以摘要和明细格式显示结果。
- 选择**“服务器任务”→“管理进度表”**以安排报告任务运行时间。选择报告任务后，可以设置报告的频率和选项。还可以调整报告的具体细节（就如同在“定义报告”页的“报告”区域中一样）。

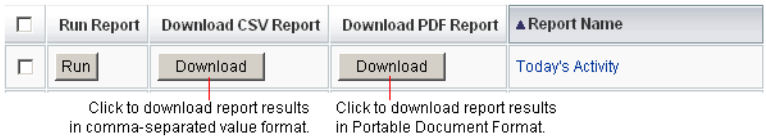
  要在此列表中显示报告 TaskDefinition，必须将 TaskDefinition 对象中的 `visibility` 属性设置为 `schedule`。

下载报告数据

在“运行报告”页中，您可以下载报告信息以便在其他应用程序（如 Acrobat Reader 或 StarOffice）中使用。

打开“运行报告”页，然后在以下任一列中单击“下载”：

- **下载 CSV 报告**。下载 CSV 格式的报告输出。保存报告后，可以在其他应用程序（如 StarOffice）中打开和使用该报告。
- **下载 PDF 报告**。下载可移植文档格式的报告输出，该报告可使用 Adobe Reader 查看。



配置报告输出

要配置报告输出，请单击“报告”，然后选择“配置报告”。

“配置报告”页中提供了以下选项：

- **PDF 报告选项**

  对于以可移植文档格式 (Portable Document Format, PDF) 生成的报告，可以做出选择以确定要在报告中使用的字体、页面大小和页面方向。

  - **PDF 字体名称**。选择生成 PDF 报告时使用的字体。默认情况下，仅显示所有 PDF 查看器均可使用的字体。但是，通过将字体定义文件复制到产品的 `fonts/` 目录中并重新启动服务器可以将其他字体（如支持亚洲语言所需的字体）添加到系统。

    可接受的字体定义格式包括 `.ttf`、`.ttc`、`.otf` 和 `.afm`。如果您选择了其中一种字体，则这种字体必须在查看报告的计算机系统中可用。也可选择“PDF 文档中的嵌入字体”选项。

  - **PDF 文档中的嵌入字体**。选择该选项可以将字体定义嵌入到生成的 PDF 报告中。这将确保可以在任何 PDF 查看器中查看报告。

    注 – 嵌入字体会极大地增加文档的大小。

  - **页面大小**。从菜单中选择 PDF 页面大小：Letter（8 ½ x 11 英寸）或 Legal（8 ½ x 14 英寸）。（默认值为 *letter*。）

    注 – 可通过使用“报告配置库”表单上的 pdfPageSize 字段，在此菜单中添加其它大小。pdfPageSize 值必须是 `itext` 包中的 `com.lowagie.text.Rectangle` 类已知的值。

- **方向**。从菜单中选择 PDF 页面方向：纵向或横向。（默认值为**纵向**。）

- **CSV 报告选项**。选择“字符集名称”选项可指定生成 CSV 报告时使用的字符集。并非所有导入 CSV 文件的应用程序都支持默认的 UTF-8 编码。请根据需要选择其他字符集。
- **跟踪的事件配置**。选择“启用事件收集”选项可配置系统监视报告，它不适用于自定义报告格式。有关详细信息，请参见第 254 页中的 “跟踪的事件配置”。

单击“保存”保存报告配置选项。

Identity Manager 报告

Identity Manager 报告类型可分为以下报告类型类别：

审计日志报告

审计日志报告基于在系统审计日志中捕获的事件。这些报告提供有关生成的帐户、批准的请求、失败的访问尝试、密码更改和重设、自置备活动、策略违规、服务提供商（外联网）用户及其他方面的信息。

注 – 在运行审计日志前，必须指定要捕获的 Identity Manager 事件类型。要执行此操作，请在菜单栏中选择“配置”，然后选择“审计”。选择一个或多个审计组名称，以记录每个组的成功和失败事件。有关设置审计配置组的详细信息，请参见第 96 页中的 “配置审计组和审计事件”。

▼ 定义审计日志报告

1 **按照第 236 页中的 “创建报告”上的报告创建说明进行操作。**

从第一个报告类型菜单中选择“Identity Manager 报告”，然后从第二个菜单中选择“审计日志报告”。

将打开“定义报告”页。

2 **填写表单，然后单击“保存”。**

如果有关于表单的问题，请单击“帮助”。

设置并保存报告参数后，便可以从“运行报告”页运行该报告。单击“运行”，以生成一个包含所有符合保存条件的结果的报告。报告内容包括事件发生的日期、执行的操作和操作结果。

单个用户审计日志报告

与审计日志报告一样，单个用户审计日志报告基于在系统审计日志中捕获的事件。不过，此报告提示输入要报告的用户，并返回对该用户执行的各种活动的列表。为了获得最详尽的结果，此报告将在审计日志的 `AccountId` 和 `ObjectDesc` 字段中搜索匹配的用户名。

此报告可以返回一组固定的列，您也可以选择一组自定义的列。这些列是在 `reporttasks.xml` 和 `defaultreports.xml` 中定义的。这两个文件位于 `sample` 目录中，该目录位于 Identity Manager 安装目录中。

▼ 定义单个用户审计日志报告

1 **按照第 236 页中的“创建报告”上的报告创建说明进行操作。**

从第一个报告类型菜单中选择“Identity Manager 报告”，然后从第二个菜单中选择“单个用户审计日志报告”。

将打开“定义报告”页。

2 **填写表单，然后单击“保存”。**

如果有关于表单的问题，请单击“帮助”。

实时报告

实时报告直接轮询资源以报告实时信息。

实时报告包括：

- **资源组报告**。概述组属性，包括用户成员资格。
- **资源状态报告**。通过对每项资源执行 `testConnection` 方法来测试一项或多项指定资源的连接状态。
- **资源用户报告**。列出用户资源帐户和帐户属性。

▼ 定义实时报告

1 **按照第 236 页中的“创建报告”上的报告创建说明进行操作。**

从第一个报告类型菜单中选择“Identity Manager 报告”，然后从第二个菜单中选择“资源组报告”、“资源状态报告”或“资源用户报告”。

将打开“定义报告”页。

2 **填写表单，然后单击“保存”。**

如果有关于表单的问题，请单击“帮助”。

设置并保存报告参数后，便可以从“运行报告”列表页运行该报告。单击“运行”，以生成一个包含所有符合保存条件的结果的报告。

摘要报告

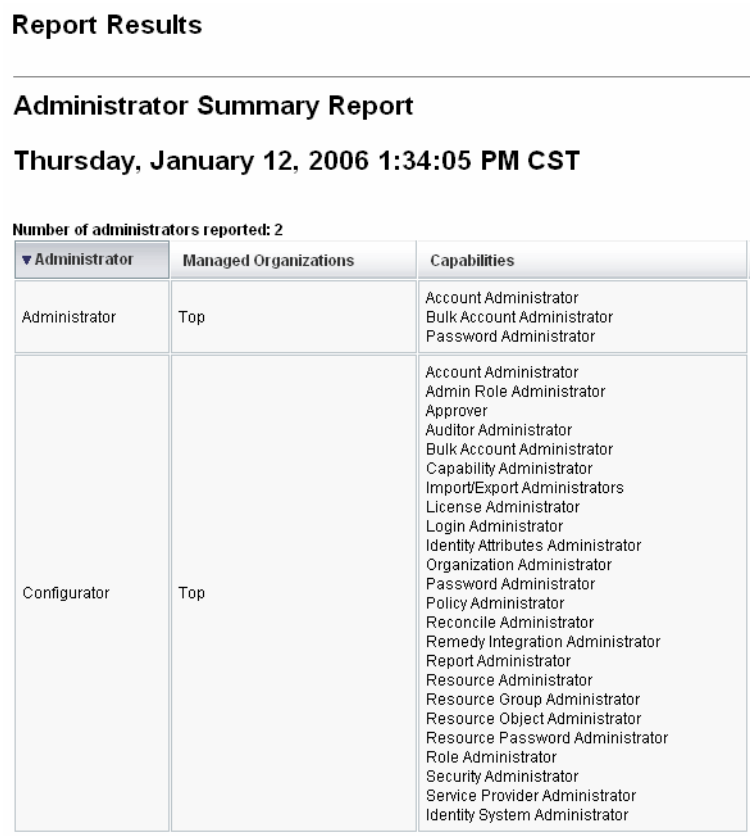
摘要报告类型包括 Identity Manager 报告列表中的以下报告：

- **帐户索引报告**。根据协调情况报告选定的资源帐户。
- **管理员报告**。查看 Identity Manager 管理员、管理员管理的组织以及分配的权能。定义管理员报告时，可以按组织选择要包含的管理员。
- **管理员角色报告**。列出分配了管理员角色的用户。
- **角色报告**。报告角色的所有方面和关联的资源。
- **任务报告**。报告暂挂和已完成的任务。通过从属性列表中进行选择来确定要包括的信息的深度，例如批准者、描述、到期日期、拥有者、开始日期和状态。
- **用户报告**。查看用户、分配给用户的角色以及用户可访问的资源。定义用户报告时，可以按名称、分配的管理员、角色、组织或资源分配选择要包括的用户。
- **用户问题报告**。允许管理员查找未回答其帐户策略要求指定的最小数量验证问题的用户。结果显示用户名、帐户策略、与策略关联的界面及要求回答问题的最小数量。

注 – 默认情况下，除非通过选择针对其运行报告的一个或多个组织来覆盖以下报告，否则将在登录管理员控制的组织集上运行这些报告。

- 管理员角色摘要
- 管理员摘要
- 角色摘要
- 用户问题摘要
- 用户摘要

如下图中所示，管理员报告列出了 Identity Manager 管理员、管理员管理的组织以及其分配的权能和管理员角色。



Report Results

Administrator Summary Report

Thursday, January 12, 2006 1:34:05 PM CST

Number of administrators reported: 2

▼Administrator	Managed Organizations	Capabilities
Administrator	Top	Account Administrator Bulk Account Administrator Password Administrator
Configurator	Top	Account Administrator Admin Role Administrator Approver Auditor Administrator Bulk Account Administrator Capability Administrator Import/Export Administrators License Administrator Login Administrator Identity Attributes Administrator Organization Administrator Password Administrator Policy Administrator Reconcile Administrator Remedy Integration Administrator Report Administrator Resource Administrator Resource Group Administrator Resource Object Administrator Resource Password Administrator Role Administrator Security Administrator Service Provider Administrator Identity System Administrator

▼ 定义摘要报告

1 **按照第 236 页中的“创建报告”上的报告创建说明进行操作。**

从第二个菜单中选择摘要报告类型（上面列出的类型）之一。

将打开“定义报告”页。

2 **填写表单，然后单击“保存”。**

如果有关于表单的问题，请单击“帮助”。

系统日志报告

系统日志报告可显示记录在系统信息库中的系统消息和错误。

设置此报告时，可以指定包含或排除以下项目：

- 系统组件（如置备程序、调度程序或服务器）
- 错误代码
- 严重级别（错误、致命或警告）

也可设置要显示的最大记录数（默认值为 3000），以及可用记录超过指定的最大数时要显示最旧的记录还是最新的记录。

运行系统日志报告时，通过指定目标条目的 syslog ID 可检索特定的 Syslog 条目。例如，要查看近期系统消息报告中的特定条目，请编辑该报告，然后选择“事件”字段。接下来，输入请求的系统日志 ID，然后单击“运行”。

注 – 也可运行 `lh syslog` 命令从系统日志中提取记录。有关详细的命令选项，请参阅附录 A，`lh` 参考消息中的第 487 页中的 “`syslog` 命令”。

▼ 定义系统日志报告

1 **按照第 236 页中的“创建报告”上的报告创建说明进行操作。**

从第一个报告类型菜单中选择“Identity Manager 报告”，然后从第二个菜单中选择“系统日志报告”。

将打开“定义报告”页。

2 **填写表单，然后单击“保存”。**

如果有关于表单的问题，请单击“帮助”。

设置并保存报告参数后，便可以从“运行报告”列表页运行该报告。

使用情况报告

创建和运行使用情况报告可以查看与 Identity Manager 对象（如管理员、用户、角色或资源）相关的系统事件的图形和/或表格摘要。可以以表格、条形图、饼图或折线图格式显示使用情况报告显示数据。

▼ 定义使用情况报告

1 **按照第 236 页中的“创建报告”上的报告创建说明进行操作。**

2 **从第一个报告类型菜单中选择“Identity Manager 报告”，然后从第二个菜单中选择“使用情况报告”。**

将打开“定义报告”页。

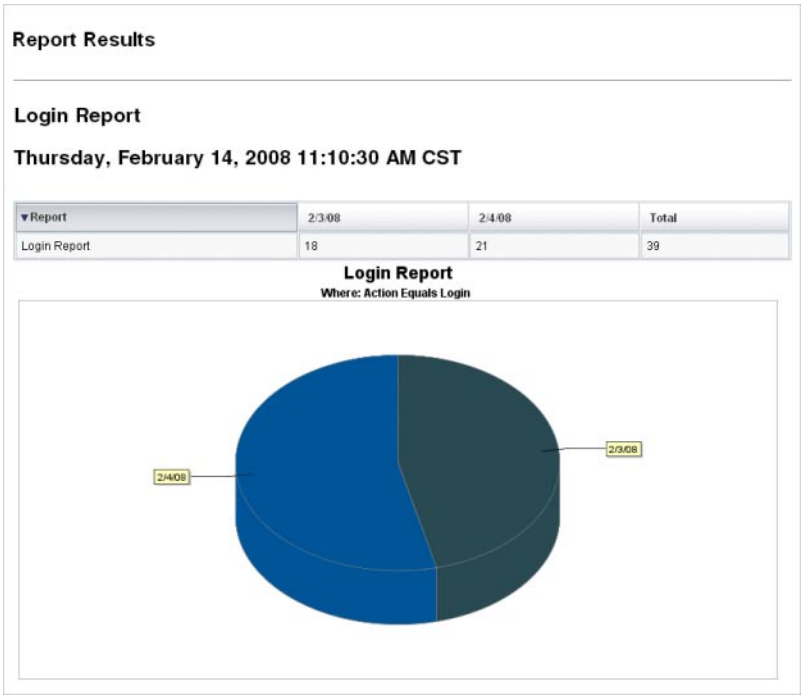
3 **填写表单，然后单击“保存”。**

如果有关于表单的问题，请单击“帮助”。

设置并保存报告参数后，便可以从“运行报告”列表页运行该报告。

示例 8–1 使用情况报告图表（生成的用户帐户）

下图显示了示例使用情况报告。报告上方的表格显示报告包含的事件，下方的图表以图形格式显示相同的信息。



工作流报告

此报告按名称列出工作流，并提供以下信息：

- 工作流的平均完成时间
- 请求工作流的次数

- 完成的工作流请求数

此外，单击工作流名称将打开工作流的详细视图，它将显示在工作流中执行的每个活动及其平均完成时间。

工作流报告对捕获性能度量特别有用，这些度量可帮助确定是否达到了服务品质协议 (Service Level Agreement, SLA) 目标。

必须对 Identity Manager 进行配置，以便将工作流计时度量作为运行工作流报告的先决条件进行捕获。有关详细信息，请参见下一节。

配置工作流以捕获审计计时事件

必须先为要报告的每种工作流类型启用工作流审计，然后才能运行工作流报告。

注 – 审计工作流将会使性能下降。因此，只应为计划在工作流报告中使用的那些工作流启用工作流审计。

请按如下方式启用工作流审计：

- 对于可以在管理员界面中使用任务模板配置的工作流，请在任务模板配置表单的“审计”选项卡上选中“审计整个工作流”复选框。有关说明，请参见第 280 页中的 “配置“审计”选项卡”。
- 对于没有任务模板的工作流，请参阅第 293 页中的 “修改工作流以记录计时审计事件”。

为工作流报告指定要存储的属性

虽然定义属性并非一项必需的操作，但如果要充分利用工作流报告，则存储一些属性是很重要的，因为您可以稍后将这些属性作为过滤报告的依据。

要为每种工作流类型定义一个要存储的属性组，请使用管理员界面的选项卡式任务模板配置表单。“审计”选项卡包含“审计属性”部分，该部分位于“审计整个工作流”复选框下面。有关说明，请参见第 280 页中的 “配置“审计”选项卡”。

▼ 定义工作流报告

1 **按照第 236 页中的“创建报告”上的报告创建说明进行操作。**

从第一个报告类型菜单中选择“Identity Manager 报告”，然后从第二个菜单中选择“工作流报告”。

将打开“定义报告”页。

2 **填写表单，然后单击“保存”。您可以定义时间参数，以及添加选择审计的任何属性。（请参见上一节中的第 245 页中的“为工作流报告指定要存储的属性”。）**

要缩小结果范围，请指定属性名称（例如，`user.global.state`），选择条件，然后输入属性值。您可以根据需要输入任意数量的属性。

如果有关于表单的问题，请单击“帮助”。

设置并保存报告参数后，便可以从“运行报告”页运行该报告。单击“运行”，以生成一个包含所有符合保存条件的结果的报告。

报告将按名称返回工作流，并显示工作流的平均完成时间、请求工作流的次数以及完成的请求数。

单击工作流名称可打开工作流的详细视图，它将显示在工作流中执行的每个活动。由于进程可以具有相同名称的活动，因此，这些活动是按进程限定范围的。

Auditor 报告

Auditor 报告提供有助于您根据审计策略中定义的条件来管理用户遵循性的信息。

Identity Manager 提供了以下审计者报告：

- 访问查看覆盖报告
- 访问查看详细信息报告
- 访问查看摘要报告
- 访问扫描用户范围覆盖报告
- 审计策略摘要报告
- 审计的属性报告
- 审计策略违规历史
- 用户访问报告
- 组织违规历史
- 资源违规历史
- 任务划分报告
- 违规摘要报告

要定义审计者报告，请按照第 236 页中的 “创建报告”中的步骤进行操作。

有关审计者报告的详细信息，请参见第 15 章，审计：监视遵循性中的第 401 页中的 “使用审计者报告”。

使用图形

您可以执行以下与图形有关的活动：

查看定义的图形

Identity Manager 提供了一些示例图形。一些使用样例数据，而一些不使用样例数据。建议您创建适用于您部署的其他图形。

您应该在将部署移入生产系统前删除样例图形和样例面板。如果尚未收集任何适用数据，则某些没有使用样例数据的样例图形可能会显示为空白。

▼ 查看定义的图形

1. **在管理员界面中，单击主菜单中的“报告”。**
2. **单击次级菜单中的“面板图形”。**
3. **从“选择面板图形类型”选项列表中选择一类面板图形。**
   选定类别中的所有图形都显示在图形列表中。
4. **单击某个图形名称。**
5. **如果需要，单击“暂停刷新”以暂停面板刷新。单击“恢复”以更新视图。**

注 – 对于包含多个图形的面板，有时在初始载入所有图形前暂停刷新很有用。

---

6. **如果需要，单击“立即刷新”以立即强制执行刷新。**
7. **单击“完成”以返回到“面板图形”列表页。**

注 – 如果任何图形显示了错误消息，请打开系统配置对象以进行编辑（第 102 页中的“编辑 Identity Manager 配置对象”），并设置 `dashboard.debug=true`。设置了该属性后，请返回到生成错误的图形，并使用“报告问题时，请附带该文本脚本”链接检索图形脚本。报告问题时应包括该图形脚本。

▼ 创建面板图形

1 **在管理员界面中，选择“报告”→“面板图形”。**

2 **从“选择面板图形类型”选项列表中选择一类面板图形。**
选定类别中的所有图形都显示在图形列表中。

3 **单击“新建”以显示“创建面板图形”页，然后输入“图形名称”。**
由于图形将按名称添加到面板中，请选择唯一的有意义的名称。

4 **选择“注册表”：IDM 或 SAMPLE。**
样例数据选项供您熟悉系统之用。由于并非所有跟踪事件都能获得样例数据，因此，在演示和试验各种图形选项时该选项非常有用。在转至生产环境之前删除样例数据。

注 – 使用样例数据的跟踪事件集不同于实际跟踪的事件。

---

5 **从列表中选择一种“跟踪事件”类型。**
事件是一种系统特征（例如内存使用率）或事件的聚集（例如资源操作），它们的历史值将被跟踪并可以直观地显示为图形或图表。
IDM 注册表的跟踪事件包括：

- **置备程序执行计数**。跟踪置备程序执行的操作数（根据操作类型）。
- **置备程序执行的持续时间**。跟踪每个置备程序操作的持续时间（根据操作类型）。
- **资源操作计数**。跟踪资源操作的数量。
- **资源操作持续时间**。跟踪某个资源操作的持续时间。
- **工作流持续时间**。跟踪执行一个工作流所需的时间。
- **工作流执行计数**。跟踪执行每个工作流的次数。

6 **从列表中选择“时间范围”。**
该选项控制数据聚集的频率（例如，一小时）及其保留的频率（例如，一个月）。系统可以存储不断增大的时间范围内的跟踪事件数据，以获得系统当前的详细视图，并了解历史趋势。

7 **从列表中选择度量。**
根据选定的跟踪事件，将选择一个默认度量（计数或平均值）。每个图形显示一种度量。可用的度量取决于选定的跟踪事件。
可能的度量包括：

- **计数**。时间间隔内事件发生的总次数
- **平均值**。时间间隔内事件值的算术平均值
- **最大值**。时间间隔内的最大事件值

- **最小值**。时间间隔内的最小事件值
- **直方图**。分别计数时间间隔内各个离散区域的事件值

8 **从列表中选择"计数显示为"。**

图形计数显示为原始总数或按不同的时间范围进行划分。

9 **从列表中选择一种图形类型。**

这用于控制如何显示跟踪事件的数据。可用的图形类型取决于选择的跟踪事件，可能包括折线图、条形图和饼形图。

10 **指定基本尺寸（可选）。**

请从以下列表中进行选择：

- **资源名称**。如果选择了该选项，尺寸的所有值均将包括在图形中。取消选定该选项可以选择将尺寸的单个值包含在图形中。
- **服务器实例**。如果选择了该选项，尺寸的所有值均将包括在图形中。取消选定该选项可以选择将尺寸的单个值包含在图形中。
- **操作类型**。如果选择了该选项，尺寸的所有值均将包括在图形中。取消选定该选项可以选择将尺寸的单个值包含在图形中。

  选择了尺寸后，页面将刷新以显示图形。

11 **在"图形选项"字段中输入文本，以便在图形主标题下面生成一个副标题（可选）。**

12 **选择"高级图形选项"（可选）。**

如果要指定以下内容，请使用此选项：

- **网格线**
- **字体**
- **颜色调色板**

13 **单击"保存"以创建图形。**

▼ 编辑面板图形

1 **在管理员界面中，单击主菜单中的"报告"。**

2 **单击次级菜单中的"面板图形"。**

将打开"面板图形"页。

3 **从"选择面板图形类型"下拉菜单中，选择一个类别。**

将打开一个列出面板图形的表。

4 **单击一个图形名称以进行编辑。**

您可编辑的图形属性因选择的图形而异。

以下一个或多个特征可用于编辑：

- **图形名称**。按名称将图形添加到面板。
- **注册表**。指定注册表中定义的**跟踪的事件描述**。当前选项包括：SAMPLE、服务提供者和 IDM。
- **跟踪的事件**。一种系统特征（例如内存使用率）或事件的聚集（例如资源操作），它们的历史值将被跟踪并可以直观地显示为图形或图表。
- **时间范围**。控制数据聚集的频率及其保留的频率。
- **度量**。每个图形显示一种度量。可用的度量取决于选定的跟踪事件。对于所选度量，可能还有其他可用选项。
- **图形类型**。控制如何显示跟踪事件的数据（例如折线图或条形图）。
- **包括的尺寸值**。如果选择了该选项，所有尺寸值均将包括在图形中。
- **图形副标题**。如果需要，请在图形主标题下输入副标题。
- **高级图形选项**。如果要设置以下内容，请选择此选项：
  - **网格线**
  - **字体**
  - **颜色调色板**

5 **单击“保存”。**

▼ 删除定义的图形

1 **在管理员界面中，单击主菜单中的“报告”。**

2 **单击次级菜单中的“面板图形”。**

3 **从“选择面板图形类型”选项列表中选择一类面板图形。**

选定类别中的所有图形都显示在图形列表中。

4 **使用复选框选择要删除的图形，然后单击“删除”。**

注 – 将从所有包含图形的面板中删除该图形，并且不会发出警告。

使用面板

面板是在单个页面上查看的相关图形的集合。和图形一样，Identity Manager 提供了一组示例面板，建议管理员使用这些示例面板自定义他们自己的部署。有关说明，请参见第 251 页中的 “创建面板”。

▼ 查看面板

1. **在管理员界面中，单击主菜单中的“报告”。**
2. **单击次级菜单中的“查看面板”以查看当前定义的面板。**
   将打开“面板”页。
3. **单击要查看的面板旁边的“显示”。**

注 – 对于包含多个图形的面板，有时在初始载入所有图形前暂停刷新很有用。

单击“暂停”以暂停面板刷新，或单击“刷新”以更新视图。

以下各节提供了使用面板的步骤：

- 第 251 页中的 “创建面板”
- 第 252 页中的 “编辑面板”
- 第 253 页中的 “删除面板”

▼ 创建面板

1. **在管理员界面中，单击主菜单中的“报告”。**
2. **单击次级菜单中的“查看面板”。**
3. **单击“新建”。**
4. **输入新面板的名称。**
5. **输入描述新面板的摘要。**
6. **选择刷新速率，单位为列表中的秒、分钟或小时。**

注 – 将刷新速率设置为小于 30 秒会导致包含多个图形的面板出现问题。

7 **要使图形样式与面板关联，请从列表中选择相应的条目。**

注 – 单个图形可以用在多个面板中。

8 **要删除面板图形，请从列表中选择相应的条目并单击“删除图形”。**

9 **单击“保存”。**

编辑面板

使用第 251 页中的 “创建面板”中描述的步骤编辑面板（除选择“新建”外），选择要修改的面板并编辑以下属性：

- 面板的名称。
- 描述新面板的摘要。
- 刷新速率，单位为列表中的秒、分钟或小时。
- 添加或删除与面板关联的图形。

注 – 从面板删除图形并不会删除图形本身。该图形仍可用于其他面板。

单个图形可以用在多个面板中。

图 8–2 展示了示例面板编辑页。

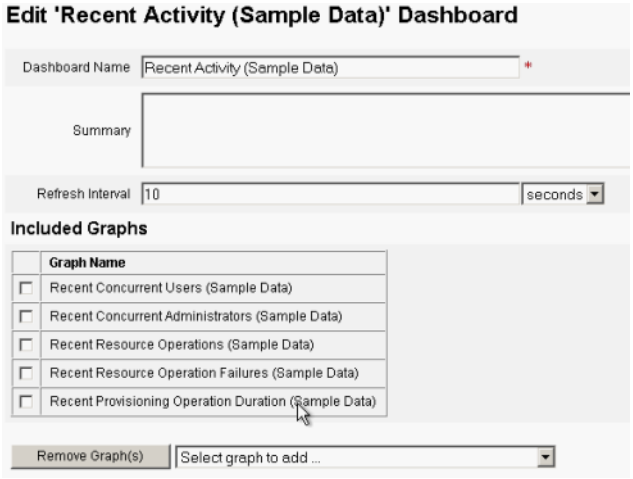


图 8–2 编辑面板

删除面板

要删除服务提供者面板，请在“服务提供者”区域中单击“管理面板”，然后选择所需的面板并单击“删除”。

注 – 使用上述步骤不会删除包含在面板中的图形。可以使用“管理面板图形”页删除图形（请参见第 250 页中的 “删除定义的图形”）。

系统监视

您可以设置 Identity Manager 实时跟踪事件并通过在面板图形中查看事件以进行监视。使用面板，您可以快速评估系统资源和点异常性，了解历史性能趋势（基于当天时间、周几等）以及在查看审计日志前交互隔离问题。它们不会提供像审计日志那样详细的信息，但是它们可提供给您一些提示，告诉您在哪可以查找日志中问题。

您可以创建图形面板显示以跟踪高级别的自动和手动活动。Identity Manager 提供了示例**资源操作**面板图形。**资源操作**面板图形使您可以快速监视系统资源，以维持可接受的服务级别。

您可以在资源操作面板中查看这些图形的样例数据。有关使用面板的详细信息，请参见第 251 页中的 “使用面板”。

以不同的级别收集和聚集统计信息，以根据您的规范显示实时视图。

跟踪的事件配置

在“配置报告”页的“跟踪的事件配置”区域中，您可以决定当前是否启用跟踪事件的统计信息收集，并将其启用。单击“启用事件收集”可启用跟踪的事件配置。

为事件收集指定以下选项：

- **时区**。该选项设置用于记录跟踪的事件的时区。这主要用于确定日期的前后界限。您也可以将时区设置为服务器上设置的默认时区。
- **用于收集的时间范围**。该选项指定数据聚集的时间间隔（即数据收集和保留的频率）。例如，如果选择 1 分钟的时间间隔，则每隔 1 分钟收集并保留数据。

系统可以存储长时间的跟踪事件数据，不但能查看系统当前的详细信息，也可了解历史趋势。

以下时间范围可用，并且默认情况下将全部选定。清除不需要的收集间隔选项。

- 10 秒钟间隔
- 1 分钟间隔
- 1 小时间隔
- 1 天间隔
- 1 周间隔
- 1 个月间隔

配置了跟踪的事件后，使用面板监视跟踪的事件。请使用滑块（如果有）放大图表的某一部分。

风险分析

Identity Manager 风险分析功能允许对配置文件超出一定安全限制的用户帐户进行报告。风险分析报告扫描物理资源，以收集数据，并按资源显示有关禁用的帐户、锁定的帐户和无拥有者帐户的详细信息。此类报告还提供有关到期密码的详细信息。报告细节因资源类型而异。

注 – 标准报告可用于 AIX、HP、Solaris、NetWare NDS 和 Windows Active Directory 资源。

风险分析页由表单控制，并可以针对您的环境进行配置。可以在 `idm\debug` 页（第 40 页中的 “Identity Manager 的“调试”页”）的 RiskReportTask 对象下找到一个表单列表，然后使用 Identity Manager IDE 修改这些对象。有关配置表单的详细信息，请参见《Sun Identity Manager Deployment Reference》中的第 2 章 “Identity Manager Forms”。

▼ 创建风险分析报告

1 **在管理员界面中，单击主菜单中的“报告”。**

2 **单击次级菜单中的“运行风险分析”。**

3 **在“新建”下拉菜单中，选择要创建的报告。**
将打开“风险分析报告设置”页。

4 **填写表单。**
可以将报告限制为仅扫描选定的资源；根据资源的类型，可以扫描描符合以下条件的帐户：

- 已禁用、已到期、非活动或已锁定的帐户
- 从未使用过的帐户
- 没有全称或密码的帐户
- 不需要密码的帐户
- 密码已到期或未在指定天数内更改的帐户

5 **单击“保存”。**

▼ 计划风险分析报告

定义完成后，可以使用以下步骤将风险分析报告调度为按指定间隔运行。

1 **在管理员界面中，单击主菜单中的“服务器任务”。**

2 **单击次级菜单中的“管理进度表”。**
将打开“预定任务”页。

3 **选择要调度的风险分析报告。**
将打开“创建新的风险分析任务进度表”页。

4 **输入名称和进度表信息，然后调整其他风险分析选项（可选）。**

5 **单击“保存”以保存该进度表。**

◆ ◆ ◆ 第 9 章

9 任务模板

通过使用 Identity Manager 的任务模板，您可以使用管理员界面配置某些工作流行为，以此作为编写自定义工作流的替代方法。

本章分为以下几节：

- 第 257 页中的 “启用任务模板”。介绍如何将任务模板用于您的系统。
- 第 261 页中的 “配置任务模板”。介绍如何使用任务模板配置工作流行为。

启用任务模板

Identity Manager 提供了以下可以配置的任务模板：

- **创建用户模板**。配置属性以创建用户任务。
- **删除用户模板**。配置属性以删除用户任务。
- **更新用户模板**。配置属性以更新用户任务。

在使用任务模板之前，必须映射任务模板的进程。

▼ 映射进程类型

1 **在管理员界面中，选择菜单中的“服务器任务”，然后选择“配置任务”。**

图 9–1 展示了“配置任务”页。

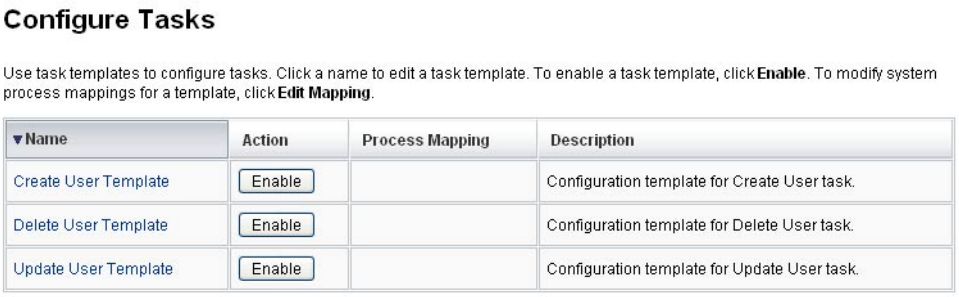


图 9–1 初始“配置任务”页

“配置任务”页包含具有以下各列的表：

- **名称**。提供创建用户模板、删除用户模板和更新用户模板的链接。
- **操作**。包含以下按钮之一：
  - **启用**。如果尚未启用模板，则显示此按钮。
  - **编辑映射**。启用模板后显示此按钮。

    启用和编辑进程映射的过程是相同的。
- **进程映射**。列出针对每个模板映射的进程类型。
- **描述**。提供每个模板的简短描述。

2 单击“启用”打开模板的“编辑进程映射”页。

例如，针对创建用户模板将显示以下页面（图 9–2）。

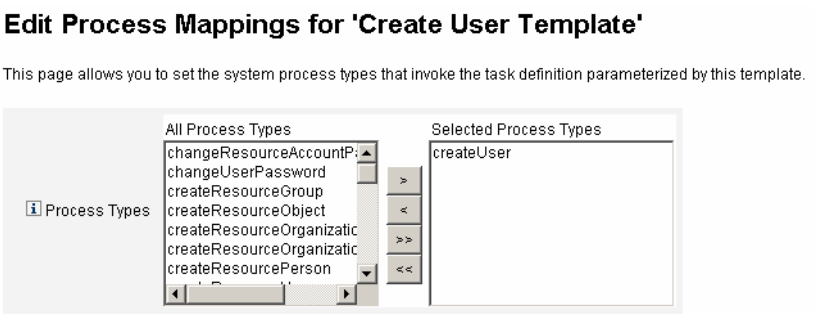
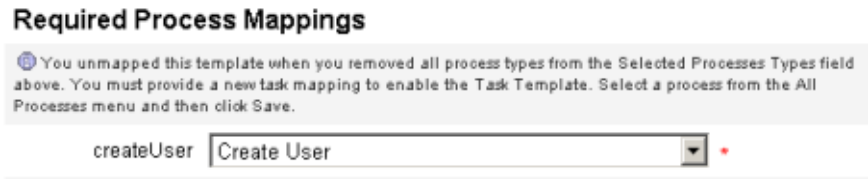


图 9–2 “编辑进程映射”页

注 – 默认进程类型（在本例中，为 `createUser`）自动显示在“选定的进程类型”列表中。如果需要，可从菜单中选择其他进程类型。

- 通常，针对每个模板只映射一种进程类型。
- 如果从“选定的进程类型”列表中删除进程类型而不选择替换的进程类型，则将显示“必需的进程映射”部分，指示您选择新任务映射。



3 **单击“保存”以映射选定的进程类型，并返回“配置任务”页。**

注 – 重新显示“配置任务”页后，“编辑映射”按钮将替换“启用”按钮，而进程名称将列在“进程映射”列中。

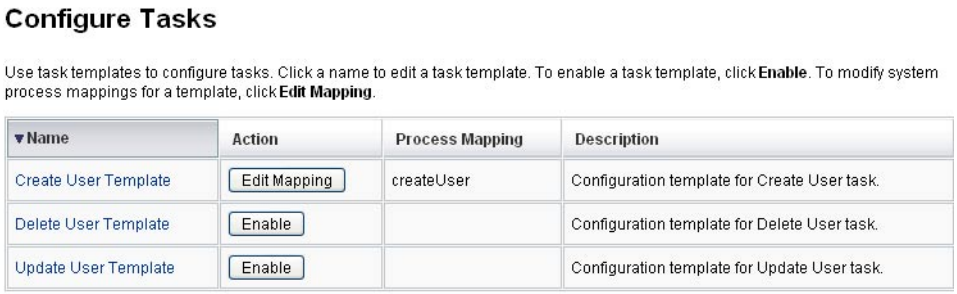


图 9–3 更新后的“配置任务”表

4 **为其余每个模板重复映射进程。**

更多信息 验证映射

- 可以通过选择“配置”→“表单和进程映射”来验证映射。显示“配置表单和进程映射”页后，向下滚动到“进程映射”表，验证以下进程类型已映射至表中显示的“进程名称，映射到”条目。

进程类型	Process Name Mapped To
createUser	**创建用户模板**
deleteUser	**删除用户模板**
updateUser	**更新用户模板**

如果成功启用模板，则“进程名称，映射到”条目应该全部包含词**模板**。

- 如果按上表所示在“进程名称，映射到”列中键入**模板**，则还可以直接通过“表单和进程映射”页映射这些进程类型。

▼ 配置任务模板

在映射模板进程类型（第 257 页中的 “启用任务模板”）后，您可以配置任务模板。

1 **在管理员界面中，单击主菜单中的“服务器任务”，然后单击“配置任务”。**

将打开“配置任务”页。

2 **在“名称”列中选择一个链接。**

将显示以下页面之一：

- **编辑任务模板“创建用户模板”**。打开此页可编辑用于创建新用户帐户的模板。
- **编辑任务模板“删除用户模板”**。打开此页可编辑用于删除或取消置备用户帐户的模板。
- **编辑任务模板“更新用户模板”**。打开此页可编辑用于更新现有用户信息的模板。

每个"Edit Task Template" 页都包含一组选项卡，作为用户工作流的主要配置区域。下表介绍了每个选项卡及其用途，以及每个选项卡都由哪些模板使用。

选项卡名称	用途	模板
常规（**默认选项卡**）	用于定义在“主页”和“帐户”页上的任务栏中以及“任务”页的任务实例表中如何显示任务名称。	仅适用于创建用户和更新用户任务模板
	用于指定如何删除或取消置备用户帐户	仅适用于删除用户模板
通知	用于配置 Identity Manager 调用进程时发送给管理员和用户的电子邮件通知。	所有模板
批准	用于按类型启用或禁用批准、指定附加批准者以及在 Identity Manager 执行某些任务之前指定帐户数据的属性。	所有模板

选项卡名称	用途	模板
Audit	用于启用和配置工作流的审计。可以使用此选项卡配置工作流以捕获工作流报告的信息。	所有模板
置备	用于在后台运行任务并允许 Identity Manager 在任务失败时重试该任务。	仅适用于创建用户任务模板和更新用户任务模板
Sunrise and Sunset	用于将创建任务延迟到指定日期/时间执行（生效），或者将删除任务延迟到指定日期/时间执行（失效）。	创建用户任务模板
Data Transformations	用于配置在置备期间如何变换用户数据。	仅适用于创建用户和更新用户任务模板

3 **选择一个选项卡以配置模板的工作流功能。**

以下各节提供了配置这些选项卡的说明：

- 第 257 页中的 “映射进程类型”
- 第 260 页中的 “配置任务模板”

4 **配置完模板后，单击“保存”按钮以保存所做的更改。**

配置任务模板

本节包含有关配置任务模板的信息和说明。这些主题包括：

- 第 261 页中的 “配置“常规”选项卡”
- 第 264 页中的 “配置“通知”选项卡”
- 第 268 页中的 “配置“批准”选项卡”
- 第 280 页中的 “配置“审计”选项卡”
- 第 282 页中的 “配置“置备”选项卡”
- 第 283 页中的 “配置“生效和失效”选项卡”
- 第 287 页中的 “配置“数据转换”选项卡”

配置“常规”选项卡

本节提供了配置“常规”选项卡的说明，它可作为任务模板配置进程的一部分。有关如何启动配置进程的说明，请参见第 261 页中的 “配置任务模板”。

注 – 在管理员界面中，用于编辑“创建用户模板”和“更新用户模板”的页面完全相同，因此我们在同一节中提供它们的配置说明。

对于创建用户模板或更新用户模板

默认情况下，在打开“编辑任务模板‘创建用户模板”’表单或“编辑任务模板‘更新用户模板”’表单时，将显示“常规”选项卡页。该页包含“任务名称”文本字段以及“插入属性”菜单，如图 9–4 中所示。有关如何启动配置进程的说明，请参见第 261 页中的 “配置任务模板”一节。

图 9–4 “常规”选项卡：创建用户模板

任务名称可以包含文字文本和/或属性引用，在任务执行期间解析该名称。

▼ 更改默认任务名称

1. **在“任务名称”字段中键入名称。**
   可以编辑或完全替换默认的任务名称。

2. **“任务名称”菜单提供当前为视图（与此模板配置的任务关联）定义的属性列表。从菜单中选择一个属性（可选）。**
   Identity Manager 将在“任务名称”字段的条目中附加该属性名称。例如：

   ```
   Create user $(accountId) $(user.global.email)
   ```

3. **完成后，可以**
   - 选择其他选项卡以继续编辑模板。
   - 单击“保存”以保存更改并返回到“配置任务”页。
     在“主页”和“帐户”选项卡底部的 Identity Manager 任务栏中，将显示新的任务名称。
   - 单击“取消”以放弃更改并返回到“配置任务”页。

对于删除用户模板

默认情况下，在打开“编辑任务模板‘删除用户模板”’页时，将显示“常规”选项卡页。（有关如何启动配置进程的说明，请参见第 261 页中的 “配置任务模板”。）

▼ 指定如何删除/取消置备用户帐户

1 使用“删除 Identity Manager 帐户”按钮指定是否可以在删除操作期间删除 Identity Manager 帐户。

这些按钮包括：

- **永不**。选择此按钮可以禁止删除帐户。
- **仅当用户在取消置备后没有链接帐户时**。如果选择此按钮，则仅当在取消置备后没有链接的资源帐户时才允许删除用户帐户。
- **始终**。选择此按钮可以始终允许删除用户帐户，即使仍分配了资源帐户。

2 使用“取消置备资源帐户”框控制所有资源帐户的取消置备操作。

注 – 为用户取消分配**外部**资源或解除外部资源的链接不会生成置备请求或工作项目。在取消分配外部资源或解除外部资源的链接时，Identity Manager 不会取消置备或删除该资源帐户，因此，您无需执行任何操作。

这些框包括：

- **删除全部**。启用此框可以删除所有已分配的资源中的全部用户帐户。
- **取消分配全部**。启用此框可以取消分配用户的所有资源帐户。但不删除资源帐户。
- **取消链接全部**。启用此框可以断开 Identity Manager 系统与资源帐户的所有链接。拥有已分配但未链接帐户的用户将以带有徽章的形式显示，以表明需要更新。

这些控制选项将覆盖在 "Individual Resource Accounts Deprovisioning" 表中的选择。

3 使用“单独资源帐户取消置备”框以对用户取消置备进行更为细化的操作（与“取消置备资源帐户”相比）。

这些框包括：

- **删除**。启用此框可以删除资源中的用户帐户。
- **取消分配**。如果启用此框，将不再直接把用户分配给资源，但不删除资源帐户。
- **解除链接**。启用此框可以断开 Identity Manager 系统与资源帐户的链接。拥有已分配但未链接帐户的用户将以带有徽章的形式显示，以表明需要更新。

如果要为不同的资源分别指定取消配置策略，则 **Individual Resource Accounts Deprovisioning** 选项将很有用。例如，大部分客户都不会删除 Active Directory 用户，因为每个 Active Directory 用户都有一个全局标识符，该标识符无法在删除后重新创建。不过，在添加新资源的环境中，可能不希望使用此选项，因为每次添加新资源时都必须更新取消置备配置。

配置“通知”选项卡

本节提供了配置“通知”选项卡的说明，它可作为任务模板配置进程的一部分。有关如何启动配置进程的说明，请参见第 261 页中的 “配置任务模板”。

所有任务模板都支持在 Identity Manager 调用进程后（通常在该进程完成后）发送电子邮件通知给管理员和用户。可以使用“通知”选项卡配置这些通知。

注 – Identity Manager 使用电子邮件模板将信息和操作请求传送给管理员、批准者和用户。有关 Identity Manager 电子邮件模板的详细信息，请参见本指南中标题为第 92 页中的 “自定义电子邮件模板”的一节。

图 9–5 显示了创建用户模板的“通知”页。

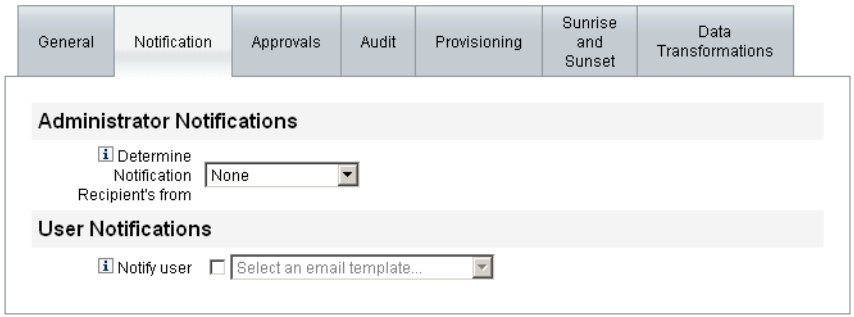


图 9–5 “通知”选项卡：创建用户模板

配置用户通知

指定要通知的用户后，还必须指定用于生成电子邮件通知的电子邮件模板的名称。

要在创建、更新或删除用户时通知用户，请启用“通知用户”复选框（如图 9–6 中所示），然后从列表中选择一个电子邮件模板。

图 9–6 指定电子邮件模板

配置管理员通知

要指定 Identity Manager 如何决定管理员通知收件人，请从“决定通知收件人来源”菜单中选择一个选项。

可用选项包括：

- **无**（默认）。不通知任何管理员。
- **属性**。选择此选项可以根据用户视图中指定的属性来获取通知收件人的帐户 ID。有关详细信息，请参见第 265 页中的“通过属性指定管理员通知收件人”。
- **规则**。选择此选项可以通过评估指定规则来获取通知收件人的帐户 ID。有关详细信息，请参见第 266 页中的“通过规则指定管理员通知收件人”。
- **查询**。选择此选项可以通过查询特定资源来获取通知收件人的帐户 ID。有关详细信息，请参见第 267 页中的“通过查询指定管理员通知收件人”。
- **管理员列表**。选择此选项可以直接从列表中选择通知收件人。有关详细信息，请参见第 265 页中的“通过属性指定管理员通知收件人”。

通过属性指定管理员通知收件人

注 – 该属性必须解析为代表单个帐户 ID 的字符串或其元素为帐户 ID 的列表。

▼ 通过指定属性获取通知收件人的帐户 ID

1 **从“决定通知收件人来源”菜单中选择“属性”，将显示一些新选项，如下图中所示。**

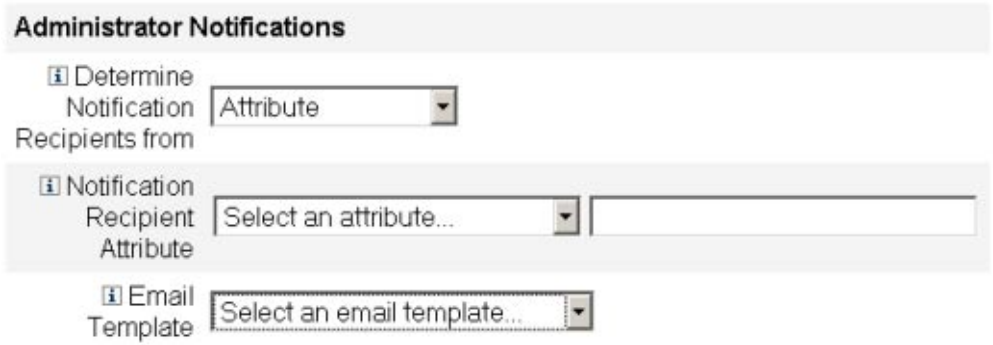


图 9–7 管理员通知：属性

这些选项包括：

- **通知收件人属性**。提供用于决定收件人帐户 ID 的属性（当前为视图定义的属性，其中的视图是与此模板配置的任务相关的视图）列表。
- **电子邮件模板**。提供电子邮件模板的列表。

2 **从"通知收件人属性"菜单中选择属性。**
属性名称将显示在菜单旁的文本字段中。

3 **从"电子邮件模板"菜单中选择模板，以指定管理员通知电子邮件的格式。**

通过规则指定管理员通知收件人

注 – 评估后，此规则必须返回代表单个帐户 ID 的字符串或其元素为帐户 ID 的列表。

▼ 通过指定规则获取通知收件人的帐户 ID

1 **从"决定通知收件人来源"菜单中选择"规则"，"通知"表单中将显示以下新选项。**

图 9–8 管理员通知：规则

- **通知收件人规则**。提供评估后会返回收件人帐户 ID 的规则（当前为系统定义）列表。
- **电子邮件模板**。提供电子邮件模板的列表。

2 **从"通知收件人规则"菜单中选择规则。**

3 **从"电子邮件模板"菜单中选择模板，以指定管理员通知电子邮件的格式。**

通过查询指定管理员通知收件人

注 – 目前只支持 LDAP 和 Active Directory 资源查询。

▼ 通过查询指定资源获取通知收件人的帐户 ID

1 从“决定通知收件人来源”菜单中选择“查询”，“通知”表单中将显示一些新选项，如图 9–9 中所示。

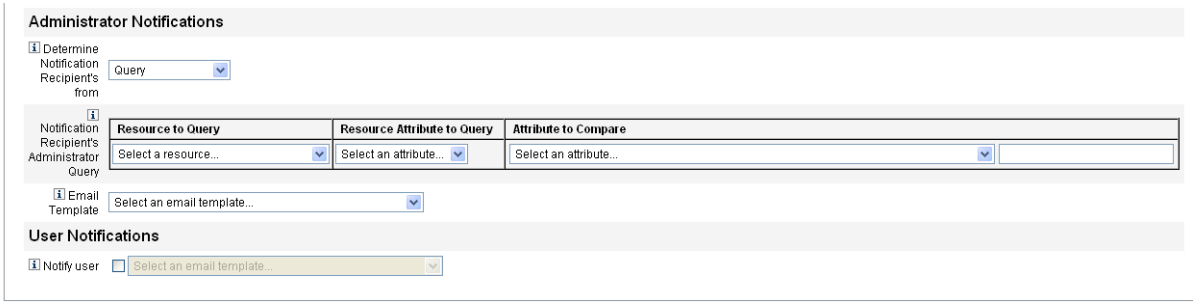


图 9–9 管理员通知：查询

“通知收件人管理员查询”表包括以下菜单，可以使用这些菜单来构建查询：

- **要查询的资源**。提供当前为系统定义的资源列表。
- **要查询的资源属性**。提供当前为系统定义的资源属性列表。
- **要比较的属性**。提供当前为系统定义的属性列表。
- **电子邮件模板**。提供电子邮件模板的列表。

2 从这些菜单中选择资源、资源属性和要比较的属性以构建查询。

3 从“电子邮件模板”菜单中选择模板，以指定管理员通知电子邮件的格式。

▼ 通过管理员列表指定管理员通知收件人

1 从“决定通知收件人来源”菜单中选择“管理员列表”，“通知”表单中将显示一些新选项，如下图中所示。

图 9–10 管理员通知：管理员列表

这些选项包括：

- **要通知的管理员**。提供带有可用管理员列表的选择工具。
- **电子邮件模板**。提供电子邮件模板的列表。

2 **在“可用管理员”列表中选择一个或多个管理员，然后将其移至“选定的管理员”列表中。**

3 **从“电子邮件模板”菜单中选择模板，以指定管理员通知电子邮件的格式。**

配置“批准”选项卡

本节提供了配置“批准”选项卡的说明，它可作为任务模板配置进程的一部分。有关如何启动配置进程的说明，请参见第 261 页中的 “配置任务模板”一节。

可以使用“批准”选项卡指定附加批准者，并在 Identity Manager 执行创建、删除或更新用户任务之前指定任务批准表单的属性。

通常，在执行某些任务之前，需要与特定组织、资源或角色关联的管理员来批准这些任务。Identity Manager 还允许您指定**附加批准者**，即，需要批准任务的其他管理员。

注 – 如果在工作流中配置了 Additional Approvers，则需要原有批准者**和在**模板中指定的所有其他批准者的共同批准。

图 9–11 展示了初始“批准”页的管理员用户界面。

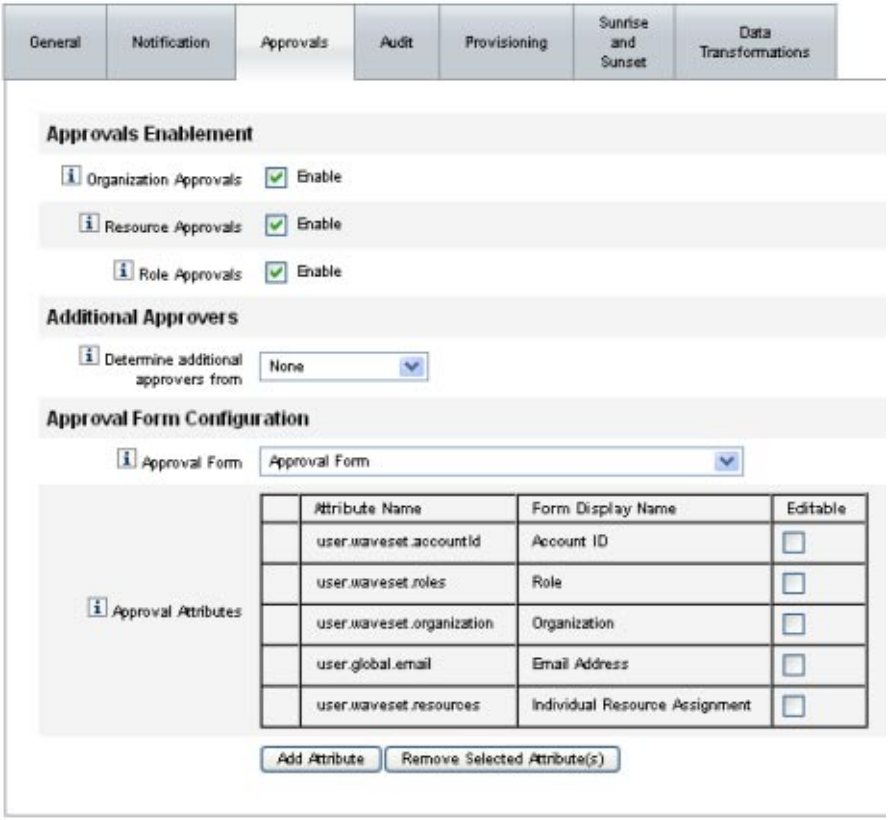


图 9–11 “批准”选项卡：创建用户模板

▼ 配置批准

1 完成“批准启用”部分（请参见第 270 页中的“启用批准（“批准”选项卡的“启用批准”部分）”）。

2 完成“附加批准者”部分（请参见第 270 页中的“指定附加批准者（“批准”选项卡的“附加批准者”部分）”）。

3 完成“批准表单配置”部分（仅适用于“创建用户模板”和“更新用户模板”）（请参见第 277 页中的“配置批准表单（“批准”选项卡的“批准表单配置”部分）”）。

4 配置完“批准”选项卡后，可以

- 选择其他选项卡以继续编辑模板。
- 单击“保存”以保存更改并返回到“配置任务”页。

- 单击“取消”以放弃更改并返回到“配置任务”页。

启用批准（“批准”选项卡的“启用批准”部分）

如果使用以下“批准启用”复选框，则只有通过批准才能继续执行创建用户、删除用户或更新用户任务。

注 – 默认情况下，将针对“创建用户模板”和“更新用户模板”启用这些复选框，但针对“删除用户模板”**禁用**这些复选框。

- **组织批准**。如果启用此复选框，则需要所有配置的组织批准者进行批准。
- **资源批准**。如果启用此复选框，则需要所有配置的资源批准者进行批准。
- **角色批准**。如果启用此复选框，则需要所有配置的角色批准者进行批准。

指定附加批准者（“批准”选项卡的“附加批准者”部分）

使用“决定附加批准者来源”菜单，可以指定 Identity Manager 将为创建用户、删除用户或更新用户任务决定附加批准者的方式。

表 9–1 列出了此菜单中的选项。

表 9–1 “决定附加批准者来源”菜单选项

选项	描述
无（**默认**）。	执行任务不需要附加批准者。
属性	批准者的帐户 ID 是从用户视图中指定的属性内获取的。
规则	批准者的帐户 ID 是通过评估指定规则获取的。
Query	批准者的帐户 ID 是通过查询特定资源获取的。
Administrator List	直接从列表中选择批准者。

如果选择其中的任何选项（除**无**以外），则会在管理员用户界面中显示附加选项。

使用以下各节提供的说明，可以指定决定附加批准者的方法。

▼ 通过属性决定附加批准者

可以使用以下步骤通过属性决定附加批准者。

1. **从“决定附加批准者来源”菜单中选择“属性”。**

注 – 该属性必须解析为代表单个帐户 ID 的字符串或其元素为帐户 ID 的列表。

将显示一些新选项，如下图中所示。

图 9–12 附加批准者：属性

- **批准者属性**。提供用于决定批准者帐户 ID 的属性（当前为视图定义的属性，其中的视图是与此模板配置的任务相关的视图）列表。
- **批准超时期限**。提供一种方法以指定批准超时时间。

  “批准超时期限”设置对原始批准和提升批准都起作用。

2 **通过“批准者属性”菜单选择属性。**

所选属性将显示在旁边的文本字段中。

3 **决定是否要为批准请求指定超时值。**

- 如果要指定超时时间段，请继续阅读第 274 页中的 “配置批准超时”以获取有关说明。
- 如果不想指定超时时间段，则可以继续阅读第 277 页中的 “配置批准表单（“批准”选项卡的“批准表单配置”部分）”，或者保存更改，然后配置其他选项卡。

▼ 通过规则决定附加批准者

可以使用以下步骤通过指定规则获取批准者的帐户 ID。

1 **从“决定附加批准者来源”菜单中选择“规则”。**

注 – 评估后，此规则必须返回代表单个帐户 ID 的字符串或其元素为帐户 ID 的列表。

将显示一些新选项，如下图中所示。

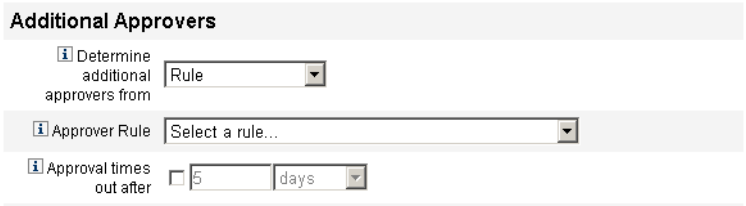


图 9–13 附加批准者：规则

- **批准者规则**。提供评估后会返回收件人帐户 ID 的规则（当前为系统定义）列表。
- **批准超时期限**。提供一种方法以指定批准超时时间。

  “批准超时期限”设置对原始批准和提升批准都起作用。

2 **从“批准者规则”菜单中选择规则。**

3 **决定是否要为批准请求指定超时值。**

- 如果要指定超时时间段，请继续阅读第 274 页中的 “配置批准超时”以获取有关说明。
- 如果不想指定超时时间段，则可以继续阅读第 277 页中的 “配置批准表单（“批准”选项卡的“批准表单配置”部分）”，或者保存更改，然后配置其他选项卡。

▼ 通过查询决定附加批准者

可以使用以下步骤通过查询指定资源获取批准者帐户 ID。

注 – 目前只支持 LDAP 和 Active Directory 资源查询。

---

1 **从“决定附加批准者来源”菜单中选择“查询”，将显示一些新选项，如下图中所示。**

图 9–14 附加批准者：查询

- **批准管理员查询**。提供由以下菜单组成的表格，以用于构建查询：

- **要查询的资源**。提供当前为系统定义的资源列表。
- **要查询的资源属性**。提供当前为系统定义的资源属性列表。
- **要比较的属性**。提供当前为系统定义的属性列表。

- **批准超时期限**。提供一种方法以指定批准超时时间。

注 – “批准超时期限”设置对原始批准和提升批准都起作用。

---

2 按如下步骤构建一个查询：

a. 从“要查询的资源”菜单中选择资源。

b. 从“要查询的资源属性”和“要比较的属性”菜单中选择属性。

3 决定是否要为批准请求指定超时值。

- 如果要指定超时时间段，请继续阅读第 274 页中的 “配置批准超时”以获取有关说明。
- 如果不想指定超时时间段，则可以继续阅读第 277 页中的 “配置批准表单（“批准”选项卡的“批准表单配置”部分）”，或者保存更改，然后配置其他选项卡。

▼ 通过管理员列表决定附加批准者

可以使用以下步骤从管理员列表中明确选择附加批准者。

1 从“决定附加批准者来源”菜单中选择“管理员列表”，将显示一些新选项，如下图中所示。

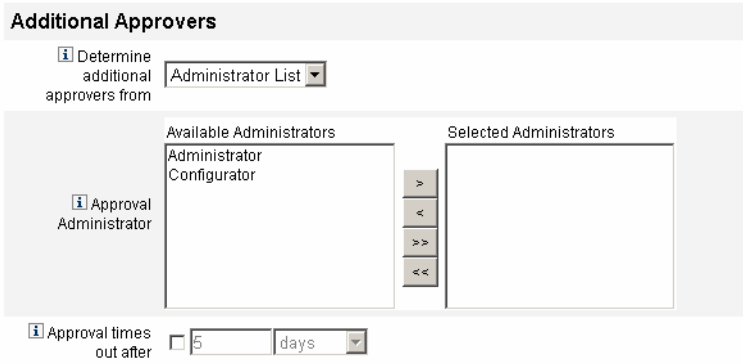


图 9–15 附加批准者：管理员列表

- **要通知的管理员**。提供带有可用管理员列表的选择工具。
- **批准表单**。提供用户表单列表，附加批准者可以使用该列表批准或拒绝批准请求。

- **批准超时期限**。提供一种方法以指定批准超时时间。

批准超时期限。同时影响原始批准和提升批准。

2 **在“可用管理员”列表中选择一个或多个管理员，然后将所选名称移至“选定的管理员”列表中。**

3 **决定是否要为批准请求指定超时值。**

- 如果要指定超时时间段，请继续阅读第 274 页中的 “配置批准超时”以获取有关说明。
- 如果不想指定超时时间段，则可以继续阅读第 277 页中的 “配置批准表单（“批准”选项卡的“批准表单配置”部分）”。

▼ 配置批准超时

可以使用以下步骤在“批准超时期限”部分中配置批准超时。

1 **选中“批准超时期限”复选框。**

旁边的文本字段和菜单将变为活动状态，并显示“超时操作”选项，如下图中所示。

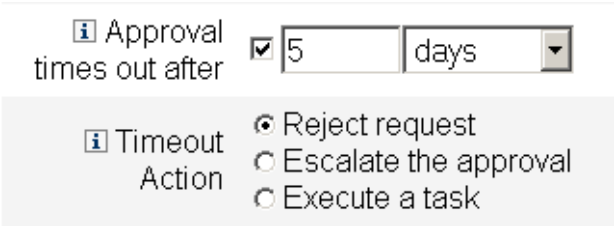


图 9–16 批准超时选项

2 **可以使用“批准超时期限”文本字段和菜单指定超时时间段，步骤如下：**

a. **从菜单中选择以秒、分钟、小时或天为单位。**

b. **在文本字段中输入数字，以表示要指定的超时秒数、分钟数、小时数或天数。**

注 – “批准超时期限”设置对原始批准和提升批准都起作用。

---

3 **使用“超时操作”按钮指定批准请求超时后执行的操作。**

单击以下选项之一：

- **拒绝请求**。如果在指定的超时时间段之前没有批准请求，Identity Manager 将自动拒绝该请求。
- **提升批准**。如果在指定的超时时间段之前没有批准请求，Identity Manager 将自动把该请求提升至另一批准者。

  启用此按钮后，将显示新选项；必须通过这些选项指定 Identity Manager 决定提升批准的批准者的方式。请继续阅读第 275 页中的 “配置“决定提升批准者来源”部分”以获取有关说明。
- **执行任务**。如果在指定的超时时间段之前批准请求未获批准，则 Identity Manager 将自动执行备用任务。

  启用此按钮，将显示“批准超时任务”菜单，可以通过该菜单指定批准请求超时后执行的任务。请继续阅读第 277 页中的 “配置“批准超时任务”部分”以获取有关说明。

▼ 配置“决定提升批准者来源”部分

在“超时操作”部分中选择“提升批准”（第 274 页中的 “配置批准超时”）时，将显示“决定提升批准者来源”菜单，如下图中所示。

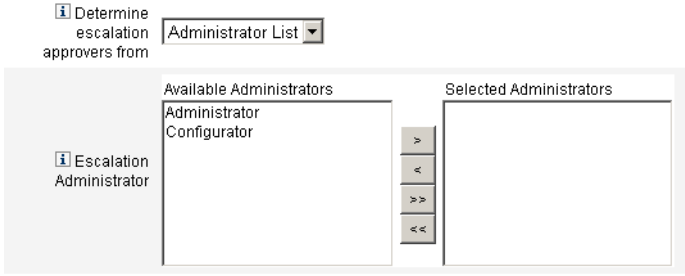
- **从此菜单选择一个选项，以指定如何决定提升批准的批准者。**

  这些选项包括：

  - **属性**。根据新用户视图中指定的属性来决定批准者帐户 ID。

    注 – 该属性必须解析为代表单个帐户 ID 的字符串或其元素为帐户 ID 的列表。

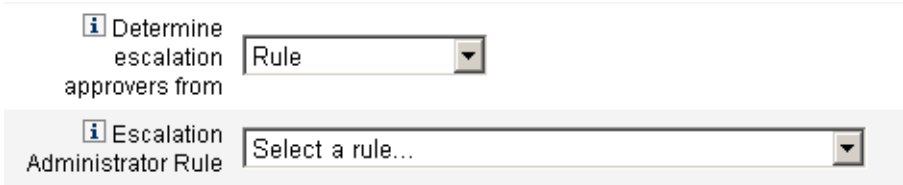
    在选择此选项时，将显示“提升管理员属性”菜单。从列表中选择一个属性，将在旁边的文本字段中显示选定的属性，如下图中所示。



- **规则**。通过评估指定规则来决定批准者帐户 ID。

  注 – 评估后，此规则必须返回代表单个帐户 ID 的字符串或其元素为帐户 ID 的列表。

  在选择此选项时，将显示“提升管理员规则”菜单，如下图中所示。从列表中选择一个规则。



- **查询**。通过查询特定资源决定批准者帐户 ID。

  将显示“提升管理员查询”菜单，如下图中所示。

  按如下方式构建查询：

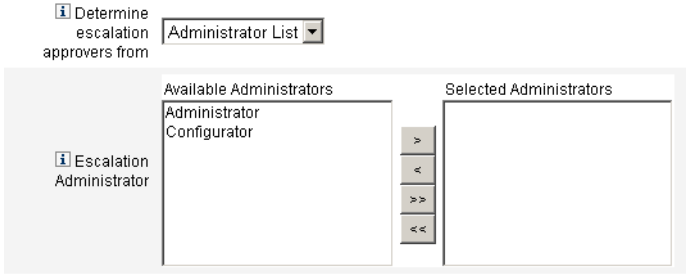
  a. 从“要查询的资源”菜单中选择资源。

  b. 从“要查询的资源属性”菜单中选择属性。

  c. 从“要比较的属性”菜单中选择属性。

- **管理员列表（默认）**。从列表中明确选择批准者。

将显示“提升管理员”选择工具，如下图中所示。

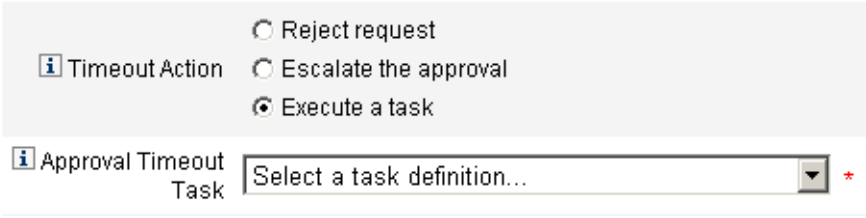


按如下方式选择批准者：

a. 从“可用管理员”列表中选择一个或多个管理员名称。
b. 将选定名称移至“选定的管理员”列表中。

▼ 配置“批准超时任务”部分

在“超时操作”部分中选择“执行任务”选项（第 274 页中的 “配置批准超时”）时，将显示“批准超时任务”菜单，如下图中所示。



- **选择在批准请求超时后执行的任务定义。**
  例如，可以允许请求者提交帮助台请求或发送报告给管理员。

配置批准表单（ “批准”选项卡的“批准表单配置”部分 ）

注 – 删除用户模板不包含 "Approval Form Configuration" 部分。只能针对创建用户模板和更新用户模板配置此部分。

可以使用“批准表单配置”部分的功能选择批准表单，然后将属性添加到批准表单中（或从中删除属性）。

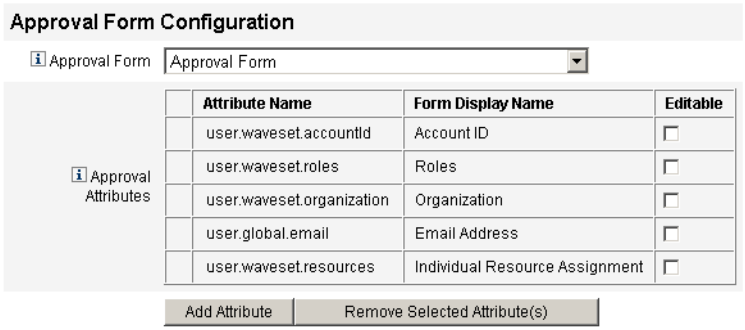


图 9–17 Approval Form Configuration

默认情况下，“批准属性”表包含以下标准属性：

- `user.waveset.accountId`
- `user.waveset.roles`
- `user.waveset.organization`
- `user.global.email`
- `user.waveset.resources`

注 – 默认批准表单经程序校验可以显示批准属性。如果使用的是批准表单而不是默认表单，则必须对表单进行程序校验以显示在“批准属性”表中指定的批准属性。

▼ 为附加批准者配置批准表单

1. **从“批准表单”菜单中选择表单。**
   批准者将使用此表单来批准或拒绝批准请求。

2. **启用“批准属性”表的“可编辑”列中的复选框，以使批准者可以编辑属性值。**
   例如，如果启用 `user.waveset.accountId` 复选框，则批准者可以更改用户的帐户 ID。

注 – 如果修改了批准表单中特定于帐户的任何属性，则在实际置备用户时，具有相同名称的所有全局属性值也将被覆盖。例如，如果资源 `R1` 存在于带有 `description` 模式属性的系统中，而您将 `user.accounts[R1].description` 属性作为可编辑的属性添加到批准表单中，则任何对批准表单中 `description` 属性值的更改都将覆盖仅从资源 `R1` 的 `global.description` 传播来的值。

---

3. **单击“添加属性”或删除选定属性按钮，从新用户的帐户数据中指定要在批准表单中显示的属性。**

- 要将属性添加到表单中，请参见第 279 页中的 “将属性添加到批准表单中”。
- 要从表单中删除属性，请参见第 279 页中的 “删除属性”。

除非修改 XML 文件，否则不能从批准表单中删除默认属性。

▼ 将属性添加到批准表单中

1 单击“批准属性”表下面的“添加属性”按钮。

“批准属性”表中的“属性名称”菜单将变为活动状态，如下图中所示。

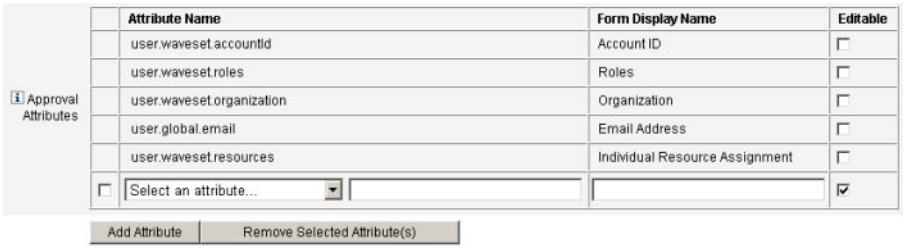


图 9–18 添加批准属性

2 从菜单中选择一个属性。

选定属性的名称将显示在旁边的文本字段中，而属性的默认显示名称则显示在“表单显示名称”列中。

例如，如果选择 `user.waveset.organization` 属性，则可以：

- 在必要时更改默认属性名称或默认表单显示名称，方法是在相应文本字段中键入新名称。
- 启用“可编辑”复选框以允许批准者更改属性值。

  例如，批准者可能要覆盖诸如用户电子邮件地址之类的信息。

3 重复以上步骤以指定其他属性。

删除属性

注 – 除非修改 XML 文件，否则不能从批准表单中删除默认属性。

▼ 从批准表单中删除属性

1 **启用“批准属性”表的最左列中的一个或多个复选框。**

2 **单击“删除选定属性”按钮，立即从“批准属性”表中删除选定的属性。**

例如，单击“删除选定属性”按钮后，将从下表中删除 `user.global.firstname` 和 `user.waveset.organization`。

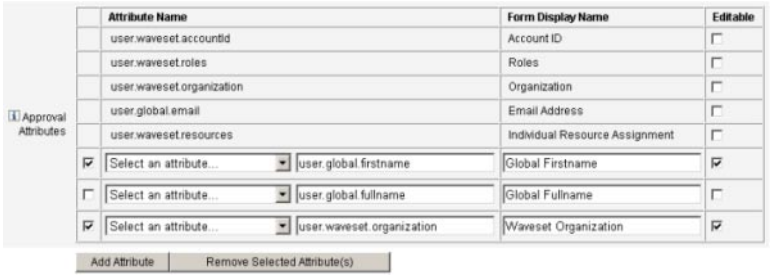


图 9–19 删除批准属性

配置“审计”选项卡

本节提供了配置“审计”选项卡的说明，它可作为任务模板配置进程的一部分。有关如何启动配置进程的说明，请参见第 261 页中的 “配置任务模板”。

所有可配置的任务模板都支持配置工作流以审计某些任务。具体来说，您可以配置“审计”选项卡以控制是否审计工作流事件，以及指定将存储哪些属性以供报告。

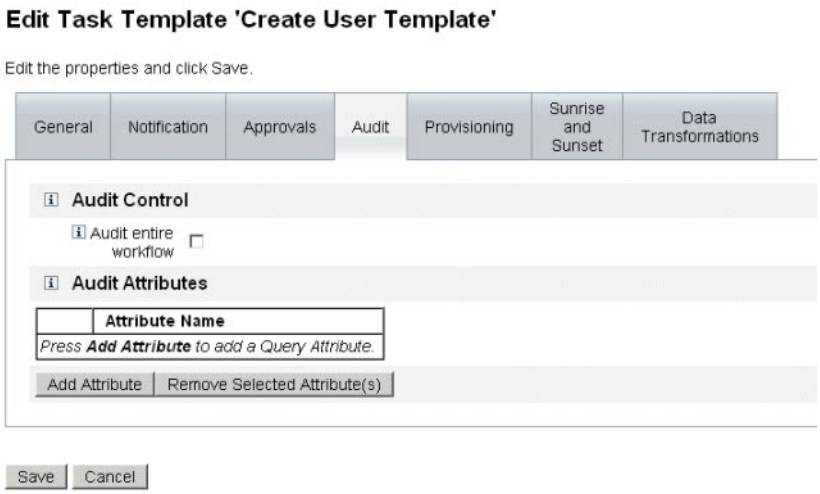


图 9–20 审计创建用户模板

▼ 配置审计

1 **选中“审计整个工作流”复选框以激活工作流审计功能。**

有关工作流审计的信息，请参见第 290 页中的 “通过工作流创建审计事件”。请注意，审计工作流将使性能下降。

2 **单击位于“审计属性”部分中的“添加属性”按钮，以选择要为生成报告而审计的属性。**

3 **当“选择属性”菜单显示在“审计属性”表中时，请从列表中选择一个属性。**

所选属性名称将显示在旁边的文本字段中。

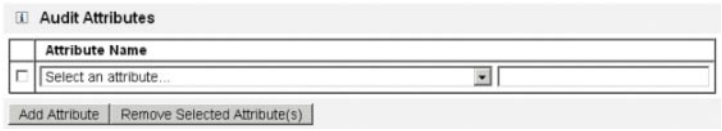


图 9–21 添加属性

▼ 删除属性

1 **启用要删除的属性旁边的复选框。**

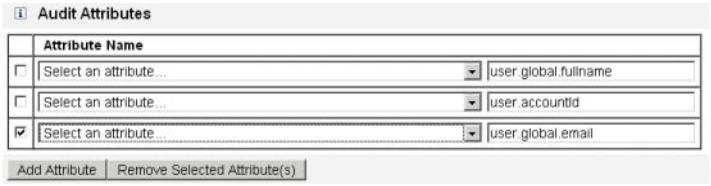


图 9–22 删除 user.global.email 属性

2 **单击“删除选定属性”按钮。**

配置“置备”选项卡

本节提供了配置“置备”选项卡的说明，它可作为任务模板配置进程的一部分。有关如何启动配置进程的说明，请参见第 261 页中的 “配置任务模板”。

注 – 此选项卡仅适用于“创建用户模板”和“更新用户模板”。

图 9–23 “置备”选项卡：创建用户模板

可以使用“置备”选项卡配置以下与置备有关的选项：

- **后台置备**。启用此复选框可以在后台运行创建、删除或更新任务，而不是同步运行任务。

  后台置备允许您在执行任务时继续在 Identity Manager 中工作。
- **向任务结果中添加“重试”链接**。启用此复选框可以在执行任务发生置备错误时，将“重试”链接添加到用户界面。“重试”链接可让用户在第一次尝试失败后再次尝试执行该任务。

配置“生效和失效”选项卡

本节提供了配置“生效和失效”选项卡的说明，它可作为任务模板配置进程的一部分。有关如何启动配置进程的说明，请参见第 261 页中的“配置任务模板”。

注 – 此选项卡仅适用于创建用户任务模板。

使用“生效和失效”选项卡，可以选择一种方法来决定以下操作发生的时间和日期。

- 针对新用户进行置备（**生效**）。
- 取消针对新用户的置备（**失效**）。

例如，可以为六个月后合同到期的临时工指定失效日期。

图 9–24 展示了“生效和失效”选项卡的设置。

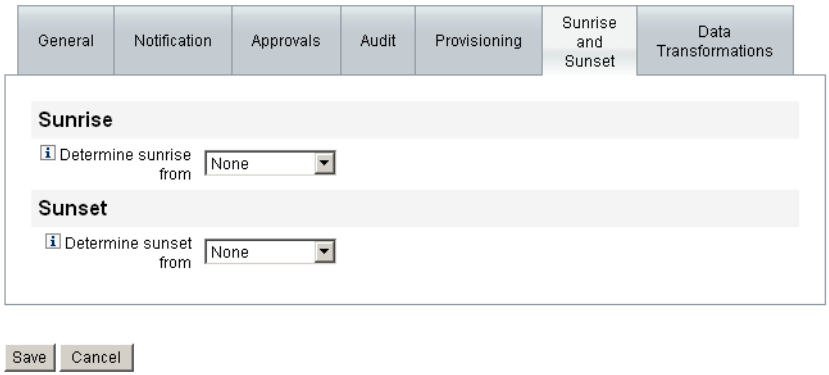


图 9–24 “生效和失效”选项卡：创建用户模板

以下主题介绍了有关配置 "Sunrise and Sunset" 选项卡的说明。

配置生效

配置生效设置可以指定对新用户进行置备的时间和日期，以及用于指定将拥有生效工作项目的用户。

▼ 配置生效

1 **从“决定生效时间”菜单中选择以下选项之一，以指定 Identity Manager 如何决定置备的时间和日期。**

- **指定时间**。将置备延迟到未来的指定时间。请继续阅读第 284 页中的 “将置备延迟到指定时间”以获取有关说明。
- **指定日期**。将置备延迟到未来的指定日历日期。请继续阅读第 285 页中的 “将置备延迟到指定日历日期”以获取有关说明。
- **指定属性**。根据用户视图中的属性值，将置备延迟到指定的日期和时间。此属性必须包含日期/时间字符串。指定包含日期/时间字符串的属性后，可以指定数据必须符合的数据格式。

  请继续阅读第 285 页中的 “通过指定属性决定置备日期和时间”以获取有关说明。
- **指定规则**。根据评估后产生日期/时间字符串的规则延迟置备。与指定属性一样，可以指定数据必须符合的数据格式。

  请继续阅读第 286 页中的 “通过评估规则来决定置备日期和时间”以获取有关说明。

“决定生效时间”菜单的默认选项为“无”，即允许立即进行置备。

2 **从“工作项目拥有者”菜单中选择一个用户，以指定拥有生效工作项目的用户。**

注 – 可在“批准”选项卡中找到生效工作项目。

指定时间

本节提供了帮助您将置备延迟到特定时间的说明。

▼ 将置备延迟到指定时间

1 **从“决定生效时间”菜单中选择“指定时间”。**

2 **当新的文本字段和菜单显示在“决定生效时间”菜单右侧后，在空白的文本字段中键入数字并从旁边的菜单中选择时间单位。**

例如，要在两小时后置备新用户，请指定下图中显示的信息。

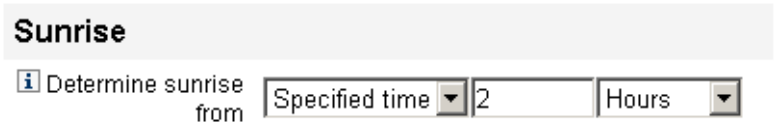


图 9–25 在两个小时后置备新用户

▼ 将置备延迟到指定日历日期

本节提供了帮助您将置备延迟到特定日期的说明。

1 **从“决定生效时间”菜单中选择“指定日”。**

2 **使用这些菜单选项来指定在哪个月的哪一周、哪一周的哪一天以及哪个月进行置备。**
例如，要在九月的第二个星期一置备新用户，请指定以下信息。

图 9–26 按照日期置备新用户

▼ 通过指定属性决定置备日期和时间

本节提供了帮助您根据用户帐户数据中的属性值决定置备日期和时间的说明。

1 **从“决定生效时间”菜单中选择“属性”。**

以下选项将变为活动状态：

- **“生效属性”菜单**。提供当前为视图（与此模板配置的任务相关）定义的属性列表。
- **“特定日期格式”复选框和菜单**。用于指定属性值的日期格式字符串（如果需要）。

如果未启用“特定日期格式”复选框，则日期字符串必须符合 `FormUtil` 方法的 `convertDateToString` 可接受的格式。请查阅产品文档，以了解支持的日期格式的完整列表。

2 **从“生效属性”菜单中选择属性。**

3 **如果需要，启用“特定日期格式”复选框，并在“特定日期格式”字段变为活动状态后输入日期格式字符串。**

例如，要根据 `waveset.accountId` 属性值使用日、月和年格式置备新用户，请指定下图中显示的信息。

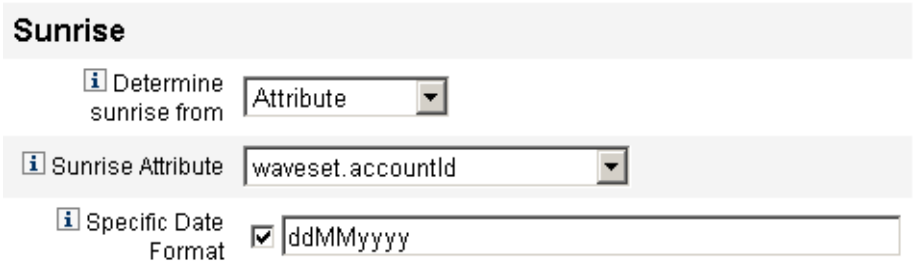


图 9–27 通过属性置备新用户

▼ 通过评估规则来决定置备日期和时间

本节提供了帮助您通过评估特定规则来决定置备日期和时间的说明。

1 **从"决定生效时间"菜单中选择"规则"。**

以下选项将变为活动状态：

- **生效规则**菜单。提供当前为系统定义的规则列表。
- **特定日期格式**复选框和菜单。用于为规则的返回值指定日期格式字符串（如果需要）。

如果未启用"特定日期格式"复选框，则日期字符串必须符合 `FormUtil` 方法的 `convertDateToString` 可接受的格式。请查阅产品文档，以了解支持的日期格式的完整列表。

2 **从"生效规则"菜单中选择规则。**

3 **如果需要，启用"特定日期格式"复选框，并在"特定日期格式"字段变为活动状态后输入日期格式字符串。**

例如，要根据电子邮件规则使用年、月、日、小时、分钟和秒格式置备新用户，请指定下图中显示的信息。

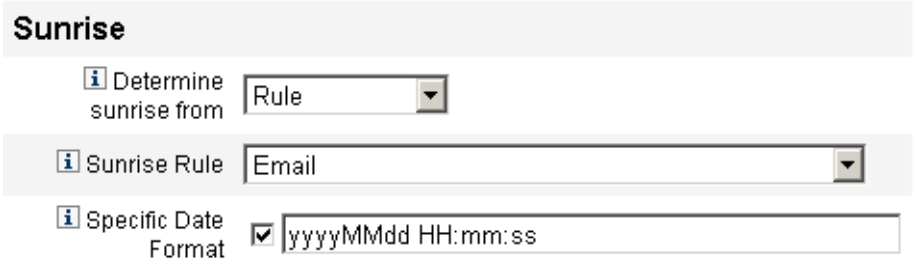


图 9–28 使用规则置备新用户

配置失效

配置失效（取消置备）部分的选项和过程与“配置生效”部分针对生效（置备）提供的选项和过程相同。

唯一的不同之处是“失效”部分还提供了“失效任务”菜单，这是因为您还必须指定任务以在特定日期和时间取消对用户的置备。

▼ 配置失效

1 **使用“决定失效时间”菜单指定方法来决定取消置备的时间：**

注 – “决定失效时间”菜单的默认选项为“无”，即允许立即取消置备。

- **指定时间**。将取消置备延迟到未来的指定时间。有关说明，请参见第 284 页中的 “将置备延迟到指定时间”。
- **指定日期**。将取消置备延迟到未来的指定日历日期。有关说明，请参见第 285 页中的 “将置备延迟到指定日历日期”。
- **属性**。根据用户帐户数据中的属性值，将取消置备延迟到指定的日期和时间。此属性必须包含日期/时间字符串。指定包含日期/时间字符串的属性后，可以指定数据必须符合的数据格式。有关说明，请参阅第 285 页中的 “通过指定属性决定置备日期和时间”。
- **规则**。根据评估后产生日期/时间字符串的规则延迟取消置备。与指定属性一样，可以指定数据必须符合的日期格式。

  有关说明，请参见第 286 页中的 “通过评估规则来决定置备日期和时间”。

2 **使用“失效任务”菜单指定一个任务，以在指定日期和时间取消置备该用户。**

配置“数据转换”选项卡

本节提供了配置“数据转换”选项卡的说明，它可作为任务模板配置进程的一部分。有关如何启动配置进程的说明，请参见第 261 页中的 “配置任务模板”。

注 – 此选项卡仅适用于“创建用户模板”和“更新用户模板”。

如果要在执行工作流的过程中更改用户帐户数据，则可以使用“数据转换”选项卡指定在置备期间 Identity Manager 如何转换数据。

例如，如果要使表单或规则生成遵守公司策略的电子邮件地址，或如果要生成生效或失效日期。

选择“数据转换”选项卡后，将显示以下页面。

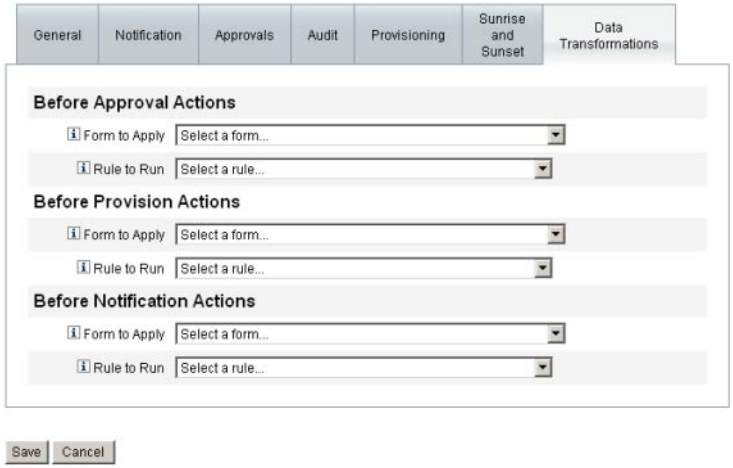


图 9–29 “数据转换”选项卡：创建用户模板

此页由以下部分组成：

- **批准前操作**。如果要在将批准请求发送到指定的批准者之前转换用户帐户数据，请配置此部分的选项。
- **置备前操作**。如果要在置备操作之前转换用户帐户数据，请配置此部分的选项。
- **通知前操作**。如果要在将通知发送到指定收件人之前转换用户帐户数据，请配置此部分的选项。

在每个部分均可以配置以下选项：

- **要应用的表单**菜单。提供当前为系统配置的表单列表。使用该菜单可以指定将用于转换用户帐户数据的表单。
- **要运行的规则**菜单。提供当前为系统配置的规则列表。使用该菜单可以指定将用于转换用户帐户数据的规则。

◆ ◆ ◆ 第 10 章

10 审计日志记录

本章介绍审计系统如何记录事件。

该信息分为以下几个主题：

审计日志记录概述

Identity Manager 审计的目的是记录操作人员、操作内容、操作的 Identity Manager 对象以及操作时间。

审计事件由一个或多个发布器处理。默认情况下，Identity Manager 使用系统信息库发布器将审计事件记录在系统信息库中。借助审计组，过滤可允许管理员选择审计事件的子集进行记录。您可为每个发布器分配最初已启用的一个或多个审计组。

注 – 有关监视和管理用户违规的信息，请参见第 13 章，身份审计：基本概念

Identity Manager 对哪些内容进行审计？

大多数默认审计是通过内部 Identity Manager 组件执行的。但是，有些接口允许通过工作流或 Java 代码生成事件。

默认的 Identity Manager 审计方法主要针对以下四个领域：

- **置备程序**。称为置备程序的内部组件可以生成审计事件。
- **视图处理程序**。在视图体系结构中，视图处理程序生成审计记录。视图处理程序应始终在创建或修改对象时审计。
- **会话**。会话方法（例如 `checkinObject`、`createObject`、`runTask`、`login` 和 `logout`）将在完成可审计操作后创建审计记录。该方法的大部分将被推送到视图处理程序中。
- **工作流**。默认情况下，仅对批准工作流进行程序校验以生成审计记录。当批准或拒绝请求时，这些工作流将生成审计事件。审计记录程序的工作流功能的接口通过 `com.waveset.session.WorkflowServices` 应用程序实现。有关详细信息，请参见下一节。

通过工作流创建审计事件

默认情况下，仅对批准工作流进行程序校验以生成审计记录。本节介绍了如何使用 `com.waveset.session.WorkflowServices` 应用程序通过任何工作流进程生成额外的审计事件。

如果需要报告自定义工作流，则可能需要其他审计事件。有关将审计事件添加到工作流中的信息，请参见第 291 页中的“修改工作流以记录标准审计事件”。

也可以在工作流中添加特殊审计事件以支持工作流报告（第 244 页中的“工作流报告”）。工作流报告将报告完成工作流所需的时间。需要使用特殊审计事件来存储时间计算所需的数据。有关将计时审计事件添加到工作流中的信息，请参见第 293 页中的“修改工作流以记录计时审计事件”。

`com.waveset.session.WorkflowServices` 应用程序

`com.waveset.session.WorkflowServices` 应用程序可通过任何工作流进程生成审计事件。表 10–1 介绍了可用于此应用程序的参数。

表 10–1 com.waveset.session.WorkflowServices 的参数

参数	类型	描述
op	字符串	对 WorkflowServices 执行的操作。必须设置为 audit 或 auditWorkflow。audit 用于标准工作流审计。auditWorkflow 用于存储时间计算所需的计时审计事件。该参数是必需的。
type	字符串	正在进行审计的对象类型名称。表 B–5 中列出了可审计的对象类型。这是记录标准审计事件所需的参数。
action	字符串	执行的操作的名称。表 B–6 中列出了可审计的操作。该参数是必需的。
status	字符串	指定操作的状态名称。表 B–7 中列出了状态（在“结果”列中）。这是记录标准审计事件所需的参数。
name	字符串	受指定操作影响的对象的名称。这是记录标准审计事件所需的参数。
resource	字符串	（**可选**）进行更改的对象所在资源的名称。
accountId	字符串	（**可选**）正在修改的帐户 ID。它应是本机资源帐户名称。
error	字符串	（**可选**）伴随任何故障的本地化错误字符串。
reason	字符串	（**可选**）ReasonDenied 对象的名称，此名称将映射到描述一般故障原因的国际化消息。
attributes	映射	（**可选**）已添加或已修改的属性名称和值的映射。
parameters	映射	（**可选**）最多映射五个与事件相关的附加名称或值。
organizations	列表	（**可选**）放置该事件的组织名称或 ID 列表。它用于审计日志的组织范围限定。如果不存在，则处理程序将尝试根据类型和名称来解析组织。如果无法解析组织，则将事件置于“顶级”（组织分层结构的最高级别）。
originalAttributes	映射	（**可选**）旧属性值的映射。名称应与属性参数中列出的名称相匹配。这些值是您要在审计日志中保存的任何先前的值。

修改工作流以记录标准审计事件

要在工作流中创建标准审计事件，请将以下 <Activity> 元素添加到工作流中：

```
<Activity name='createEvent'>
```

然后，将引用 com.waveset.session.WorkflowServices 应用程序的 <Action> 元素嵌套在 <Activity> 元素中：

```
<Action class='com.waveset.session.WorkflowServices'>
```

将必需和可选的 <Argument> 元素嵌套在 <Action> 元素中。有关这些参数的列表，请参见表 10–1。

要记录标准审计事件，必须将 op 参数设置为 audit。

第 292 页中的 “工作流示例”显示了创建标准审计事件所需的最少代码。

工作流示例

以下示例展示了简单的工作流活动，并显示了事件的生成，该事件将记录由 ResourceAdministrator 执行的名为 ADSIResource1 的资源删除活动。

示例 10–1 简单的工作流活动

```
<Activity name='createEvent'> <Action class='com.waveset.session.WorkflowServices'>
<Argument name='op' value='audit'/> <Argument name='type' value='Resource'/>
<Argument name='action' value='Delete'/> <Argument name='status' value='Success'/>
<Argument name='subject' value='ResourceAdministrator'/>
<Argument name='name' value='ADSIResource1'/> </Action> <Transition to='end'/> </Activity>
```

下一个示例展示了如何将特定属性添加到工作流，该工作流将跟踪由每个用户在批准进程中根据细化级别应用的更改。通常，此添加将遵循从用户请求输入的 ManualAction。

ACTUAL_APPROVER 是根据实际执行批准的人员，在表单和工作流中（如果从批准表中批准）设置的。APPROVER 将标识分配了 APPROVER 的人员。

示例 10–2 在批准进程中跟踪更改的已添加属性

```
<Action name='Audit the Approval' application='com.waveset.session.WorkflowServices'>
<Argument name='op' value='audit'/> <Argument name='type' value='User'/>
<Argument name='name' value='$(CUSTOM_DESCRIPTION)'/> <Argument name='action' value='approve'/>
<Argument name='accountId' value='$(accountId)'/> <Argument name='status' value='success'/>
<Argument name='resource' value='$(RESOURCE_IF_APPLICABLE)'/>
<Argument name='loginApplication' value='$(loginApplication)'/>
<Argument name='attributes'> <map>
<s>fullname</s><ref>user.accounts[Lighthouse].fullname</ref>
<s>jobTitle</s><ref>user.accounts[Lighthouse].jobTitle</ref>
<s>location</s><ref>user.accounts[Lighthouse].location</ref>
<s>team</s><ref>user.waveset.organization</ref> <s>agency</s>
<ref>user.accounts[Lighthouse].agency</ref> </map> </Argument>
<Argument name='originalAttributes'> <map> <s>fullname</s> <s>User's previous fullname</s>
<s>jobTitle</s> <s>User's previous job title</s> <s>location</s> <s>User's previous location</s>
<s>team</s> <s>User's previous team</s> <s>agency</s> <s>User's previous agency</s> </map>
</Argument> <Argument name='attributes'> <map> <s>firstname</s> <s>Joe</s> <s>lastname</s>
<s>New</s> </map> </Argument> <Argument name='subject'> <or> <ref>ACTUAL_APPROVER</ref>
```

示例 10–2 在批准进程中跟踪更改的已添加属性 （续）

```
<ref>APPROVER</ref> </or>
</Argument> <Argument name='approver' value='$(APPROVER)'/> </Action>
```

修改工作流以记录计时审计事件

可以修改工作流以记录计时事件来支持工作流报告（第 244 页中的“工作流报告”）。标准审计事件仅记录已发生的事件；而计时审计事件记录事件的开始和停止时间，以便可以执行时间计算。除了计时事件数据以外，还会存储标准审计事件所记录的大部分信息。有关详细信息，请参见第 294 页中的“计时审计事件存储哪些信息？”。

注 – 要记录计时审计事件，必须先为要审计的每种工作流类型激活工作流审计。

- 对于可以在管理员界面中使用任务模板配置的工作流，请先启用与要审计的工作流对应的任务模板。有关说明，请参见第 257 页中的“启用任务模板”。

  然后，选中“审计整个工作流”复选框以启用工作流审计。有关说明，请参见第 280 页中的“配置“审计”选项卡”。
- 对于没有任务模板的工作流，应定义一个名为 `auditWorkflow` 的变量，并将其值设置为 `true`。

请注意，审计工作流将使性能下降。

示例 10–3 显示了创建计时审计事件所需的代码。要记录计时审计事件，必须将 `op` 参数设置为 `auditWorkflow`。

还需要 `action` 参数，并且必须将其设置为以下值之一：

- `StartWorkflow`
- `EndWorkflow`
- `StartProcess`
- `EndProcess`
- `StartActivity`
- `EndActivity`

可以在 `auditconfig.xml` 中定义其他 action 参数。

示例：在工作流中启动和停止审计事件

示例 10–3 展示了如何在工作流中启用计时审计事件。要对工作流进行程序校验，应在工作流、进程和活动的开头和结尾添加 `auditWorkflow` 事件。

`auditWorkflow` 操作是在 `com.waveset.session.WorkflowServices` 中定义的。有关详细信息，请参见第 290 页中的“`com.waveset.session.WorkflowServices` 应用程序”。

示例 10–3 在工作流中启动计时审计事件

```
<Action application='com.waveset.session.WorkflowServices'>
<Argument name='op' value='auditWorkflow'/>
<Argument name='action' value='StartWorkflow'/>
</Action>
```

要在工作流中停止记录计时审计事件，请将示例 10–4 中的代码添加到工作流末尾附近的 pre-end 活动中。请注意，在对工作流或进程进行程序校验时，不允许在 end 活动中添加任何内容。必须创建 pre-end 活动以执行最终 auditWorkflow 事件，然后无条件地转换到 end 事件。

示例 10–4 在工作流中停止计时审计事件

```
<Action application='com.waveset.session.WorkflowServices'>
<Argument name='op' value='auditWorkflow'/> <Argument name='action' value='EndWorkflow'/>
</Action>
```

计时审计事件存储哪些信息？

默认情况下，计时审计事件记录常规审计事件存储的大部分信息，其中包括以下属性：

属性	描述
WORKFLOW	所执行的工作流的名称
PROCESS	所执行的当前进程的名称
INSTANCEID	所执行的工作流的唯一实例 ID
ACTIVITY	记录事件的活动
MATCH	工作流实例中的唯一标识符

上面的属性存储在 logattr 表中，它们来自于 auditableAttributesList。Identity Manager 还会检查是否定义了 workflowAuditAttrConds 属性。

可以在进程或工作流的单个实例中调用某些活动若干次。为了匹配特定活动实例的审计事件，Identity Manager 将工作流实例中的唯一标识符存储在 logattr 表中。

要在 logattr 表中为工作流存储其他属性，必须定义 workflowAuditAttrConds 列表，该列表被视为 GenericObjects 列表。如果在 workflowAuditAttrConds 列表中定义 attrName 属性，Identity Manager 将通过以下方法从代码内的对象中提取 attrName：先将 attrName 作为键，然后存储 attrName 值。所有键和值都是以大写值形式存储的。

审计配置

审计配置由一个或多个发布器和若干预定义的组构成。

审计组根据对象类型、操作和操作结果定义所有审计事件的子集。每个发布器都被分配了一个或多个审计组。默认情况下，系统信息库发布器将分配给所有审计组。

审计发布器会将审计事件传送给特定审计目的地。默认系统信息库发布器会将审计记录写入系统信息库。每个审计发布器均可以具有特定于实现的选项。可以为审计发布器分配文本格式化程序。（文本格式化程序提供审计事件的文本表示。）

审计配置 (`#ID#Configuration:AuditConfiguration`) 对象是在 `sample/auditconfig.xml` 文件中定义的。此配置对象具有一个扩展，该扩展是一个通用对象。

在顶层，此配置对象具有以下属性：

- 第 295 页中的 “`filterConfiguration` 属性”
- 第 300 页中的 “`extendedTypes` 属性”
- 第 301 页中的 “`extendedActions` 属性”
- 第 302 页中的 “`extendedResults` 属性”
- 第 302 页中的 “`publishers` 属性”

`filterConfiguration` 属性

`filterConfiguration` 属性列出了事件组，这些组用于使一个或多个事件通过事件过滤器。`filterConfiguration` 属性中列出的每个组都包含表 10–2 中列出的属性。

表 10–2 `filterConfiguration` 属性

属性	类型	描述
`groupName`	字符串	事件组名称
`displayName`	字符串	表示组名称的消息目录关键字
`enabled`	字符串	指示是否已启用或禁用整个组的布尔值标志。此属性是对过滤对象的优化。
`enabledEvents`	列表	描述组启用哪些事件的通用对象列表。必须列出事件以启用其日志记录。列出的每个对象都必须具有以下属性： ■ `objectType`（字符串）– `objectType` 名称。 ■ `actions`（列表）– 一个或多个操作的列表。 ■ `results`（列表）– 一个或多个结果的列表。

示例 10–5 展示了默认资源管理组。

示例 10–5 默认资源管理组

```
<Object name='Resource Management'> <Attribute name='enabled' value='true'/>
<Attribute name='displayName' value='UI_RESOURCE_MGMT_GROUP_DISPLAYNAME'/>
<Attribute name='enabledEvents'> <List> <Object> <Attribute name='objectType' value='Resource'/>
<Attribute name='actions' value='ALL'/> <Attribute name='results' value='ALL'/> </Object> <Object>
<Attribute name='objectType' value='ResourceObject'/> <Attribute name='actions' value='ALL'/>
<Attribute name='results' value='ALL'/> </Object> </List> </Attribute> </Object>
```

Identity Manager 提供了默认审计事件组。以下部分介绍了这些组及其启用的事件：

- 第 296 页中的 “帐户管理组”
- 第 297 页中的 “Identity System 之外的更改组”
- 第 297 页中的 “遵循性管理组”
- 第 297 页中的 “配置管理组”
- 第 298 页中的 “事件管理组”
- 第 298 页中的 “登录/注销组”
- 第 298 页中的 “密码管理组”
- 第 298 页中的 “资源管理组”
- 第 299 页中的 “角色管理组”
- 第 299 页中的 “安全管理组”
- 第 299 页中的 “服务提供者 组”
- 第 300 页中的 “任务管理组”

您可以在 Identity Manager 管理员界面的“审计配置”页中配置审计事件组（“配置”>“审计”）。有关说明，请参见第 96 页中的 “配置审计组和审计事件”。

还可以在“审计配置”页中为每个组配置成功或失败的事件。此界面不支持添加或修改为组启用的事件，但可通过 Identity Manager 调试页（第 40 页中的 “Identity Manager 的“调试”页”）来执行此操作。

注 – 并非可以为审计事件组选择的每个操作都会生成日志记录。另外，选择“所有操作”选项并不表示所有列出的操作均可用于所有审计事件组。

帐户管理组

默认情况下将启用此组。

表 10–3 默认帐户管理事件组

类型	操作
加密密钥	所有操作
`Identity System` **帐户**	所有操作

表 10–3 默认帐户管理事件组 （续）

类型	操作
资源帐户	批准、创建、删除、禁用、启用、修改、拒绝、重命名、解除锁定
工作流案例	结束活动、结束进程、结束工作流、启动活动、启动进程、启动工作流
用户	批准、创建、删除、禁用、启用、修改、拒绝、重命名

Identity System 之外的更改组

默认情况下将禁用此组。

表 10–4 Identity Manager 之外的更改事件组和事件

类型	操作
资源帐户	**本机更改**

遵循性管理组

默认情况下将启用此组。

表 10–5 默认遵循性管理组事件

类型	操作
审计策略	所有操作
访问扫描	所有操作
遵循性违规	所有操作
数据导出器	所有操作
用户权利	已批准证明者、已拒绝证明者、已请求修正、已请求重新扫描、终止
访问查看工作流	所有操作
修正工作流?	所有操作

配置管理组

默认情况下将启用此组。

表 10–6 默认配置管理事件组

类型	操作
配置	所有操作

表 10–6 默认配置管理事件组 （续）

类型	操作
用户表单	所有操作
规则	所有操作
电子邮件模板	所有操作
登录配置	所有操作
策略	所有操作
`Xml` **数据**	导入
日志	所有操作

事件管理组

默认情况下将启用此组。

表 10–7 默认事件管理事件组

类型	操作
电子邮件	通知
测试通知	通知

登录/注销组

默认情况下将启用此组。

表 10–8 默认 Identity Manager 登录/注销事件组

类型	操作
用户	证书到期、锁定、登录、注销、解除锁定、用户名恢复

密码管理组

默认情况下将启用此组。

表 10–9 默认密码管理事件组和事件

类型	操作
资源帐户	更改密码、重设密码

资源管理组

默认情况下将启用此组。

表 10–10 默认资源管理事件组和事件

类型	操作
资源	所有操作
资源对象	所有操作
资源表单	所有操作
资源操作	所有操作
属性解析	所有操作
工作流案例	结束活动、结束进程、结束工作流、启动活动、启动进程、启动工作流

角色管理组

默认情况下将禁用此组。

表 10–11 默认角色管理事件组和事件

类型	操作
角色	所有操作

安全管理组

默认情况下将启用此组。

表 10–12 默认安全管理事件组和事件

类型	操作
权能	所有操作
加密密钥	所有操作
组织	所有操作
管理员角色	所有操作

服务提供者 组

默认情况下将启用此组。

表 10–13 服务提供者 事件组和事件

类型	操作
目录用户	质询响应、创建、删除、修改、操作后的标注、操作前的标注、更新验证答案、用户名恢复

任务管理组

默认情况下将禁用此组。

表 10–14 任务管理事件组和事件

类型	操作
任务实例	所有操作
任务定义	所有操作
任务进度	所有操作
任务结果	所有操作
置备任务	所有操作

extendedTypes 属性

可以审计添加到 com.waveset.object.Type 类的每种新类型。必须为新类型分配唯一的双字符数据库键，该键将存储在数据库中。所有新类型将添加到不同的审计报告界面。必须将要记录到数据库而无需过滤的每种新类型添加到审计事件组 enabledEvents 属性（如有关 enabledEvents 属性的内容所述）中。

在某些情况下，您可能要审计不具有关联 com.waveset.object.Type 的项目，或者您要更为细化地表示现有类型。

例如，WSUser 对象在系统信息库中存储用户的所有帐户信息。审计进程并未将每个事件都标记为 USER 类型，而是将 WSUser 对象分割为两种不同的审计类型（资源帐户和 Identity Manager 帐户）。以这种方式分割对象可以更容易地在审计日志中查找特定帐户信息。

通过添加到 extendedObjects 属性来添加扩展审计类型。每个扩展对象必须具有下表中列出的属性。

表 10–15 扩展对象属性

参数	类型	描述
name	字符串	类型的名称，在构建 AuditEvents 时和事件过滤期间使用。
displayName	字符串	表示类型名称的消息目录关键字。
logDbKey	字符串	在日志表中存储此对象时要使用的双字符数据库键。有关保留的值，请参见第 496 页中的 “审计日志数据库映射”。
supportedActions	列表	对象类型支持的操作。在用户界面中创建审计查询时将使用此属性。如果此值为 null，则所有操作将显示为针对此对象类型查询的可能值。
mapsToType	字符串	（可选）映射到此类型的 com.waveset.object.Type 的名称（如果适用）。尝试解析对象组织成员资格（如果尚未在事件上指定）时使用此属性。
organizationalMembership	列表	（可选）组织 ID 的默认列表，如果此类型的事件尚不具有已分配的组织成员资格，则应将这些事件置于此列表中。

所有客户特定的键应以 # 符号开头，以防止添加新的内部键时出现重复的键。

示例 10–6 展示了扩展类型的 Identity Manager 帐户。

示例 10–6 扩展类型的 Identity Manager 帐户

```
<Object name='LighthouseAccount'> <Attribute name='displayName' value='LG_LIGHTHOUSE_ACCOUNT'/>
<Attribute name='logDbKey' value='LA'/> <Attribute name='mapsToType' value='User'/>
<Attribute name='supportedActions'> <List> <String>Disable</String> <String>Enable</String>
<String>Create</String> <String>Modify</String> <String>Delete</String> <String>Rename</String>
</List> </Attribute> </Object>
```

extendedActions 属性

通常，审计操作会映射到 com.waveset.security.Right 对象。当添加新 Right 对象时，必须指定唯一的双字符 logDbKey，它将存储在数据库中。您可能会遇到没有权限符合必须审计的特定操作的情况。这时，可以通过将操作添加到 extendedActions 属性中的对象列表来扩展操作。

每个 extendedActions 对象必须包括表 10–16 中列出的属性。

表 10–16 extendedAction 属性

属性	类型	描述
name	字符串	操作的名称，在构建 AuditEvents 时和事件过滤期间使用。
displayName	字符串	表示操作名称的消息目录关键字。
logDbKey	字符串	在日志表中存储此操作时要使用的双字符数据库键。 有关保留的值，请参见第 496 页中的 “审计日志数据库映射”。

所有客户特定的键应以 # 符号开头，以防止添加新的内部键时出现重复的键。

表 10–16 展示了如何添加注销操作。

示例 10–7 添加注销操作

```
<Object name='Logout'> <Attribute name='displayName' value='LG_LOGOUT'/>
<Attribute name='logDbKey' value='LO'/> </Object>
```

extendedResults 属性

除可以扩展审计类型和操作外，还可以添加结果。默认情况下，有两种结果：**成功**和**失败**。可以通过将它们添加到 extendedResults 属性中的对象列表来扩展结果。

每个 extendedResults 对象必须包括表 10–17 中描述的属性。

表 10–17 extendedResults 属性

属性	类型	描述
name	字符串	结果的名称，在设置 AuditEvents 的状态时和事件过滤期间使用。
displayName	字符串	表示结果名称的消息目录关键字。
logDbKey	字符串	在日志表中存储此结果时要使用的单字符数据库键。有关保留的值，请参见标题为数据库键的部分。

所有客户特定的键都应使用 0–9 范围内的数字，以防止添加新的内部键时出现重复的键。

publishers 属性

publishers 列表中的每个项目均为通用对象。每个 publishers 对象都具有以下属性。

表 10–18 publishers 属性

属性	类型	描述
class	字符串	发布器类的名称。
displayName	字符串	表示发布器名称的消息目录关键字。
description	字符串	发布器的描述。
filters	列表	分配给此发布器的审计组列表。
formatter	字符串	文本格式化程序（如果有）的名称。
options	列表	发布器选项列表。这些选项是特定于发布器的；列表中的每个项目均为 PublisherOption 的映射表示。请参见 sample/auditconfig.xml 获得示例。

数据库模式

Identity Manager 系统信息库中有两个用于存储审计数据的表：

- waveset.log – 存储大多数事件详细信息。
- waveset.logattr – 存储每个事件所属组织的 ID。

本节中将首先讨论这些表。

当审计日志数据超过为上述表指定的列长度限制时，Identity Manager 将截断数据以使该数据适合列长度。第 305 页中的 “审计日志截断”中介绍了审计日志截断。

审计日志中的少数几列具有可配置的列长度限制。要了解有关这些列的信息以及如何更改其长度限制，请参见第 306 页中的 “审计日志配置”。

waveset.log 表

本节介绍了 waveset.log 表中的列名称和数据类型。数据类型是根据 Oracle 数据库定义获得的，在其他数据库中可能略微有所变化。有关所有受支持数据库的数据模式值列表，请参见附录 B，审计日志数据库模式。

一些列值在数据库中存储为键，以便优化空间。有关键的定义，请参见标题为第 496 页中的 “审计日志数据库映射”的一节。

- objectType CHAR(2) – 表示正在进行审计的对象类型的双字符键。
- action CHAR(2) – 表示已执行的操作的双字符键。
- actionStatus CHAR(1) – 表示已执行操作的结果的单字符键。
- reason CHAR(2) – 用于在出现故障时描述 ReasonDenied 对象的双字符数据库键。ReasonDenied 是一个封装了消息目录条目的类，用于一般的故障（例如证书无效和权限不足）。

- actionDateTimeVARCHAR(21) – 执行上述操作的日期和时间。以 GMT 时间存储此值。
- objectName VARCHAR(128) – 操作期间对其执行操作的对象的名称。
- resourceName VARCHAR(128) – 操作期间使用的资源名称（如果适用）。一些事件不会引用资源；但是，在许多情况下，将会提供更详细的信息来记录已在其中执行操作的资源。
- accountName VARCHAR(255) – 对其执行操作的帐户 ID（如果适用）。
- server VARCHAR(128) – 在其中执行操作的服务器（由事件记录程序自动分配）。
- message VARCHAR(255*) 或 CLOB – 任何与操作相关的本地化消息，包括诸如错误消息的消息。文本将进行本地化存储，因此不会被国际化。可以配置该列的列长度限制。默认数据类型为 VARCHAR，默认大小限制为 255。有关如何调整大小限制的信息，请参见第 306 页中的 “审计日志配置”。
- interface VARCHAR(50) – 从中执行操作的 Identity Manager 界面（例如管理员、用户、IVR 或 SOAP 界面）。
- acctAttrChanges VARCHAR(4000) **到** CLOB – 存储在创建和更新期间已更改的帐户属性。在创建或更新资源帐户或 Identity Manager 帐户对象期间将始终填充的属性更改字段。操作期间所有更改的属性都将作为字符串存储在此字段中。数据的格式为 NAME=VALUE NAME2=VALUE2。通过执行针对名称或值的 "contains" SQL 语句可以查询此字段。

  以下代码示例展示了 acctAttrChanges 列中的值。

```
COMPANY="COMPANY" DEPARTMENT="DEPT" DESCRIPTION="DSMITH DESCRIPTION"
FAX NUMBER="5122222222" HOME ADDRESS="12282 MOCKINGBIRD LANE" HOME CITY="AUSTIN"
HOME PHONE="5122495555" HOME STATE="TX" HOME ZIP="78729" JOB TITLE="DEVELOPER"
MOBILE PHONE="5125551212" WORK PHONE="5126855555" EMAIL="someone@somecompany.COM"
EXPIREPASSWORD="TRUE" FIRSTNAME="DANIEL" FULLNAME="DANIEL SMITH" LASTNAME="SMITH"
```

注 – 如果 Identity Manager 安装使用 Oracle 系统信息库，并且发现审计日志中出现截断错误，则可以将审计日志表中的 accountAttrChanges 字段由 VARCHAR(4000) 转换为 CLOB。Identity Manager 在 /web/sample 目录中提供了一个示例 DDL 脚本，用于将 log.acctAttrChanges 从 VARCHAR(4000) 转换为 CLOB。convert_log_acctAttrChangesCHAR2CLOB.oracle.sql 脚本保留了现有数据，并允许 accountAttrChanges 字段中包含的字符超过 4000 个。

这种转换是可选的，只应在发现截断错误时执行。另外，还要确保先备份受影响的表，然后再运行转换脚本。

在运行转换脚本后，请停止并重新启动 Web 应用服务器。在运行新报告时，它应该会正确进行显示。

- acctAttr01label-acctAttr05label VARCHAR(50) – 这五个附加 NAME 槽是最多可以提升五个属性名称的列，这些属性名称将存储在各自的列中，而不是存储在大的二进制大对象中。可以使用 "audit?" 设置从“资源模式配置”页中提升属性，此属性可用于数据挖掘。
- acctAttr01value-acctAttr05value VARCHAR(128) – 5 个附加 VALUE 槽，最多可以提升 5 个属性值，这些属性值将存储在单独的列中，而不是存储在二进制大对象列中。
- parm01label-parm05label VARCHAR(50) – 用于存储与事件相关的参数的 5 个槽。示例如客户机 IP 和会话 ID 名称。
- parm01value-parm05value VARCHAR(128*) 或 CLOB – 用于存储与事件相关的参数的 5 个槽。示例如客户机 IP 和会话 ID 值。可以配置这些列的列长度限制。默认数据类型为 VARCHAR，默认大小限制为 128。有关如何调整大小限制的信息，请参见第 306 页中的 “审计日志配置”。
- id VARCHAR(50) – 由 waveset.logattr 表中引用的系统信息库分配给每个记录的唯一 ID。
- name VARCHAR(128) – 生成的分配给每个记录的名称。
- xml BLOB – 由 Identity Manager 内部使用。

waveset.logattr 表

waveset.logattr 表用于存储每个事件的组织成员资格的 ID，这可以按组织限定审计日志的范围。

- id VARCHAR(50) – waveset.log 记录的 ID。
- attrname VARCHAR(50) – 当前始终为 MEMBEROBJECTGROUPS。
- attrval VARCHAR(255) – 事件所属的 MemberObject 组的 ID。

审计日志截断

当审计日志数据的一个或多个列超过指定的列长度限制时，将截断列数据以使该数据适合列长度。具体来说，将数据截断为指定限制，减去三个字符。然后，在列数据末尾附加省略号 (...) 以表示发生截断。

此外，还会在该审计记录的 NAME 列前面添加字符串 #TRUNCATED#，以便于查询截断的记录。

注 – 在计算消息的截断位置时，Identity Manager 将使用 UTF–8 编码。如果配置使用 UTF–8 以外的编码，截断的数据仍可能会超过数据库中的实际列大小。如果发生这种情况，审计日志中将不会显示截断的消息，并且系统日志中将写入错误。

审计日志配置

可以配置审计日志中的某些列以在系统信息库中存储大量数据。

调整列长度限制

审计日志中的一些列具有可配置的列长度限制。这些列包括：

- `message` 列
- `parmNNvalue` 列（其中 `NN` = `01`、`02`、`03`、`04` 或 `05`）
- `xml` 列

注 – 有关审计日志列的描述，请参见第 303 页中的 “数据库模式”。

可通过编辑 `RepositoryConfiguration` 对象来更改列长度限制。有关编辑 `RepositoryConfiguration` 对象的说明，请参见第 102 页中的 “编辑 Identity Manager 配置对象”。

- 要更改 `message` 列的列长度限制，请修改 `maxLogMessageLength` 值。
- 要更改 `parmNNvalue` 列的列长度限制，请修改 `maxLogParmValueLength` 值。同一限制值适用于所有 5 个列。（无法定义单个列长度值。）
- 要更改 `xml` 列的列长度限制，请修改 `maxLogXmlLength` 值。

需要重新启动服务器以使新值生效。

`RepositoryConfiguration` 对象中的列长度限制设置决定了可以在列中存储的最大数据量。如果要存储的数据超过这些设置，Identity Manager 将会截断数据。有关详细信息，请参见第 305 页中的 “审计日志截断”。

如果增加 `RepositoryConfiguration` 对象中的列长度设置，还要确保数据库中的列大小设置至少与 `RepositoryConfiguration` 对象中配置的大小一样。

从审计日志中删除记录

应定期截断审计日志，以使其不致变得太大。可以使用审计日志维护任务调度从审计日志中删除旧记录的任务。

1. **在管理员界面中，单击“服务器任务”→“管理进度表”。**
2. **在“可调度的任务”部分中，单击“审计日志维护任务”。**

   将打开“创建新的审计日志维护任务任务进度表”页。
3. **填写表单，然后单击“保存”。**

使用自定义审计发布器

Identity Manager 可以将审计事件提交给自定义审计发布器。

提供了以下自定义发布器：

- **控制台**。将审计事件打印到标准输出或标准错误。
- **文件**。将审计事件写入平面文件。
- **JDBC**。在 JDBC 数据存储中记录审计事件。
- **JMS**。在 JMS 队列或主题中记录审计事件。
- **JMX**。发布审计事件，以使 JMX (Java Management Extensions) 客户机可以监视 Identity Manager 审计日志活动。
- **脚本化**。允许使用自定义脚本存储审计事件。

如果要创建您自己的发布器，请参见第 314 页中的 “开发自定义审计发布器”。

本节中的信息包含以下主题：

▼ 启用自定义审计发布器

自定义审计发布器是从“审计配置”页中启用的。

1 **在管理员界面中，单击主菜单中的“配置”，然后单击次级菜单中的“审计”。**
将打开“审计配置”页。

2 **选择页面底部的“使用自定义发布器”选项。**
将打开一个表，其中列出了当前配置的审计发布器。

3 **要配置新的审计发布器，请从“新建发布器”下拉菜单中选择自定义发布器类型。**
填写“配置新审计发布器”表单。单击“确定”。

4 **要点！请单击“保存”以保存新的审计发布器！**

控制台、文件、JDBC 和执行脚本的发布器类型

要启用控制台、文件、JDBC 或执行脚本的审计发布器，请按照第 307 页中的 “启用自定义审计发布器”中的步骤进行操作。从“新建发布器”下拉菜单中选择相应的发布器类型。

填写“配置新审计发布器”表单。如果存在表单方面的问题，请参阅 i-Helps 和联机帮助。

- 控制台审计发布器用于将审计事件打印到标准输出或标准错误。
- 文件审计发布器用于将审计事件写入平面文件。
- JDBC 审计发布器用于在 JDBC 数据存储中记录审计事件。
- 执行脚本的审计发布器允许使用 JavaScript 或 BeanShell 编写自定义脚本以存储审计事件。

JMS 发布器类型

可以使用 JMS 审计日志自定义发布器将审计事件记录发布到 JMS（Java Message Service，Java 消息服务）队列或主题中。

为什么使用 JMS？

通过发布到 JMS，可以在具有多个 Identity Manager 服务器的环境中提供更大的关联灵活性。此外，还可以在限制使用文件审计日志发布器的环境中使用 JMS，例如，在服务器运行时客户机报告工具无法访问日志的 Windows 环境中。

JMS 为具有多个服务器的环境提供了很多好处：

- JMS 消息存储集中处理（并简化）消息存储和检索。
- JMS 体系结构不限制可访问服务的客户机数。
- 可通过防火墙和其他网络基础结构方便地发送 JMS 协议。

点对点或者发布和订阅？

Java Message System 提供了两种消息传送模型：点对点或队列模型，以及发布和订阅或主题模型。Identity Manager 支持这两种模型。

在点对点模型中，生成方将消息发布到特定队列，而使用方从队列中读取消息。此处，生成方知道该消息的目的地，并将该消息直接发布到使用方的队列。

点对点模型具有以下特征：

- 只有一个使用方将获得消息。
- 不必在接收者使用消息时运行生成方，也不需要在发送消息时运行接收者。
- 接收者将确认成功处理的每条消息。

另一方面，发布和订阅模型支持将消息发布到特定消息主题。零个或多个订阅者可以登记对接收特定消息主题的消息的意向。在此模型中，发布者和订阅者均不了解对方。一个贴切的比喻是，此模型就像一个匿名布告栏。

发布和订阅模型具有以下特征：

- 多个使用方可以接收消息。
- 发布者和订阅者之间存在计时依赖关系。发布者必须先创建一个订阅，然后客户机才能进行订阅。在订阅后，除非已建立持久订阅，否则订阅者必须持续处于活动状态才能接收消息。对于持久订阅，在订阅者未连接时发布的消息将在订阅者重新连接时重新分发。

注 – 有关 JMS 的详细信息，请访问 `http://www.sun.com/software/products/message_queue/index.xml`

配置 JMS 发布器类型

JMS 发布器将审计事件设置为 JMS TextMessage 格式。然后，根据配置情况将这些 TextMessage 发送到队列或主题。可以根据配置情况将文本消息的格式设置为 XML 或通用日志记录格式 (Universal Logging Format, ULF)。

要启用 JMS 发布器类型，请按照第 307 页中的 “启用自定义审计发布器”中的步骤进行操作，然后从“新建发布器”下拉菜单中选择 "JMS"。

要配置 JMS 发布器类型，请填写“配置新审计发布器”表单。如果存在表单方面的问题，请参阅 i-Helps 和联机帮助。

JMX 发布器类型

JMX 审计日志发布器发布审计事件，以使 JMX (Java Management Extensions) 客户机能够监视 Identity Manager 审计日志活动。

什么是 JMX？

Java Management Extensions (JMX) 是一项 Java 技术，用于管理和/或监视应用程序、系统对象、设备和面向服务的网络。管理/监视的实体由称为 MBean（受管 Bean）的对象表示。

Identity Manager 的 JMX 发布器实现

Identity Manager 的 JMX 审计日志发布器监视审计日志中的事件。在检测到事件时，JMX 发布器将使用 MBean 封装审计事件记录，并且还会更新临时历史记录（保留在内存中）。对于每个事件，将向 JMX 客户机发送单独的较小通知。如果对该事件感兴趣，JMX 客户机可以向封装审计事件的 MBean 查询其他信息。

注 – 有关审计事件记录的信息，请参见 `com.waveset.object.AuditEvent` Javadoc。第 314 页中的 “开发自定义审计发布器”中介绍的 REF 工具包中提供了该 Javadoc。

要从正确的 MBean 中检索信息，需要历史记录序列号。此号码包含在事件通知中。

每个事件通知包含以下信息：

- **类型**。描述事件类型的字符串。该字符串采用 `AuditEvent.<ObjectType>.<Action>` 格式，其中 `ObjectType` 和 `Action` 是从 `com.waveset.AuditEvent` 返回的。例如，如果发送解除锁定事件，则类型为 `AuditEvent.LighthouseAccount.Unlock`。
- **序列号**。用于从 MBean 查询信息的历史记录缓冲区键。

▼ 配置 JMX 发布器类型

1. **要启用 JMX 发布器类型，请按照第 307 页中的“启用自定义审计发布器”中的步骤进行操作，然后从“新建发布器”下拉菜单中选择 "JMX"。**
2. **要配置 JMX 发布器类型，请填写“配置新审计发布器”表单。如果存在表单方面的问题，请参阅 i-Helps 和联机帮助。**
   - **发布器名称**。为 JMX 审计事件发布器键入唯一名称。
   - **历史记录限制**。根据需要，更改默认值以指定发布器应在内存中保留的事件项目数。（默认值为 100。）
3. **单击“测试”以验证发布器名称是否为可接受的名称。**
4. **单击“确定”。将关闭“配置新审计发布器”表单。**
5. **要点！单击“保存”。**

使用 JMX 客户机查看审计事件

可以使用 JMX 客户机来查看 JMX 发布器。JDK 1.5 中包含的 JConsole 用于创建以下屏幕捕获。

如果使用 JConsole，请选择连接到进程以查看 `IDM:type=AuditLog` MBean。有关配置 JConsole 以用作 JMX 客户机的信息，请参见《Sun Identity Manager 8.1 System Administrator's Guide》中的“Viewing JMX Data”。

在 JConsole 中，单击“通知”选项卡可查看审计事件。记下通知中的序列号。在 MBean 中查询其他信息时需要使用序列号。

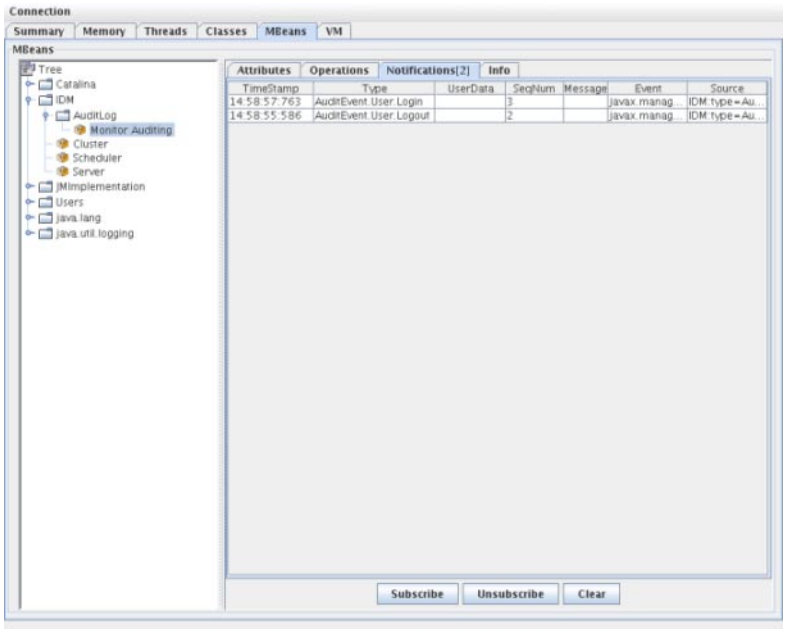


图 10–1 在 JConsole 中查看 JMX 审计事件通知

在 MBean 中查询其他信息

在 JConsole 中，单击“操作”选项卡。使用通知中的序列号从 MBean 中查询事件详细信息。每个操作都带有 'get' 前缀，并且唯一的参数是“序列”号。

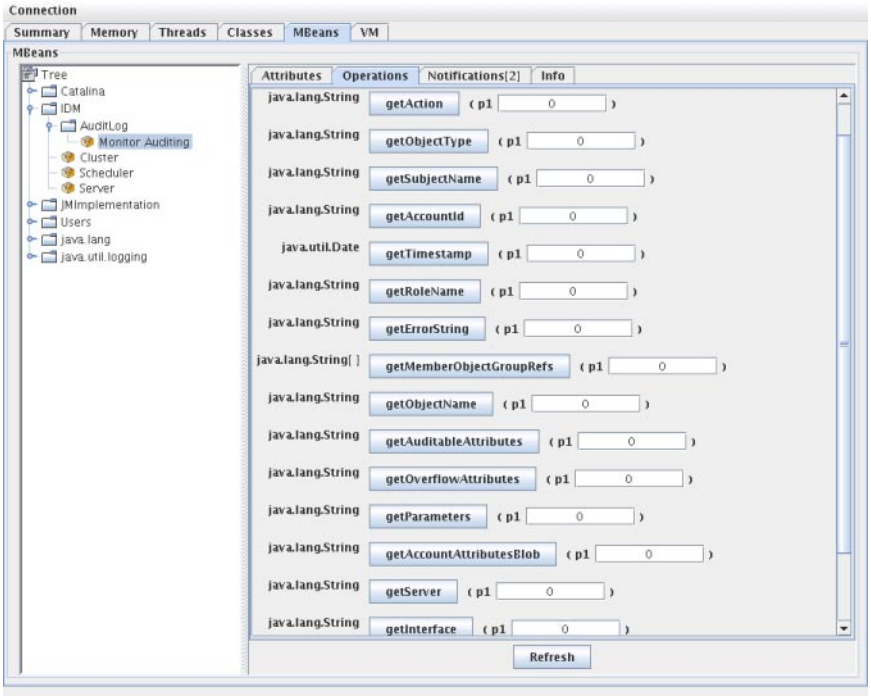


图 10–2 在 JConsole 中从 MBean 查询其他信息

实际上，MBean 是到 `com.waveset.object.AuditEvent` 类的一一映射。表 10–19 为 MBean 提供的每个属性/操作提供了说明。

表 10–19 MBeanInfo 属性/操作描述

属性/操作	描述
`AccountAttributesBlob`	已更改的属性的列表
`AccountId`	与事件关联的帐户 ID
`Action`	在事件期间执行的操作
`AuditableAttributes`	可审计属性
`ErrorString`	任何错误字符串
`Interface`	审计界面
`MemberObjectGroupRefs`	成员对象组引用
`ObjectName`	对象名
`ObjectType`	对象类型

表 10–19 MBeanInfo 属性/操作描述 （续）

属性/操作	描述
`OverflowAttributes`	所有溢出属性
`Parameters`	所有参数
`Reason`	事件原因
`ResourceName`	与事件关联的资源
`RoleName`	与事件关联的角色
`SubjectName`	与事件关联的用户或服务
`Server`	从中触发事件的服务器名称。
`Status`	审计事件的状态。
`Timestamp`	审计事件的日期/时间

在 JConsole 中，单击“属性”选项卡。属性带有 `Current` 前缀，表示属性包含发送到系统的最新审计事件。

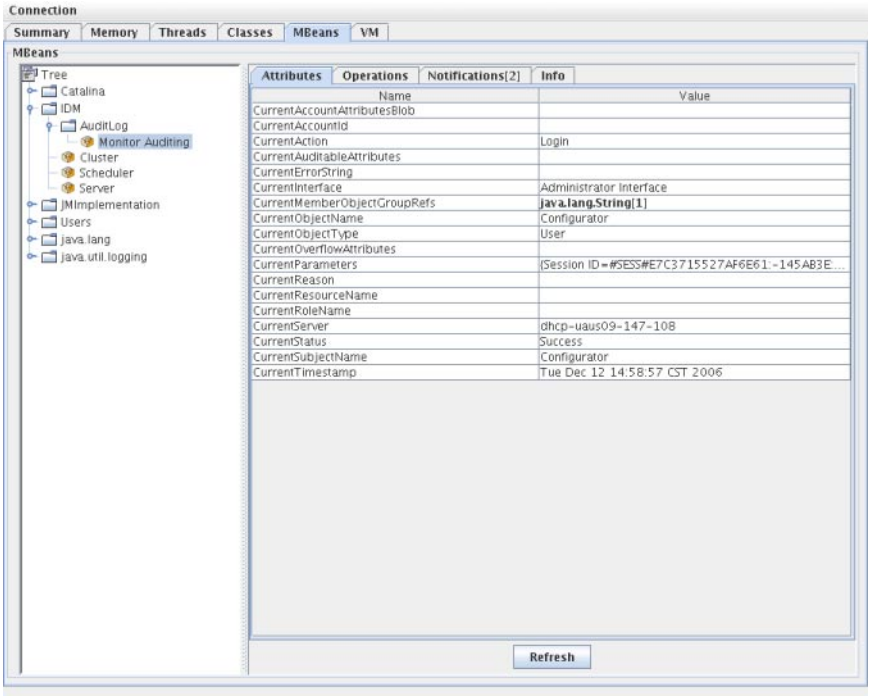


图 10–3 在 JConsole 中查看 MBean 属性

开发自定义审计发布器

本节说明了如何使用 Java 创建新的自定义审计发布器。

随 Identity Manager 提供的控制台、文件和 JDBC 自定义发布器实现了 `AuditLogPublisher` 接口。可以在 REF 工具包中找到这些发布器的源代码。也可以在 REF 工具包中找到 Javadoc 格式的接口文档。（有关接口的详细信息，请参阅 Javadoc。）

注 – REF（Resource Extension Facility，资源扩充工具）工具包是在产品 CD 上的 `/REF` 目录中提供的，或者是随安装映像提供的。

建议开发者扩展 `AbstractAuditLogPublisher` 类。此类可以解析配置并确保已将所有必需选项提供给发布器。（请参见 REF 工具包中的发布器示例。）

发布器必须具有一个**无参数**的构造函数。

发布器生命周期

以下步骤介绍发布器的生命周期：

1. 实例化对象。
2. 使用 `setFormatter()` 方法设置格式化程序（如果有）。
3. 使用 `configure(` *Map*`)` 方法提供选项。
4. 使用 `publish(` *Map*, *LoggingErrorHandler*`)` 方法发布事件。
5. 使用 `shutdown()` 方法终止发布器。

Identity Manager 启动以及更新审计配置时都执行步骤 1-3。如果调用关闭之前没有生成审计事件，则不会执行步骤 4。

在同一发布器对象上仅调用一次 `configure(`*Map*`)`。（发布器无需准备运行中的配置更改）。更新审计配置后，将先关闭当前发布器，然后再创建新发布器。

步骤 3 中的 `configure()` 方法可能会抛出 `WavesetException`。在这种情况下，将忽略发布器，并且对于此发布器不再会执行其他调用。

发布器配置

发布器可以没有选项，也可以具有多个选项。`getConfigurationOptions()` 方法将返回发布器支持的选项列表。这些选项可以使用 `PublisherOption` 类（有关此类的详细信息，请参见 Javadoc）进行封装。审计配置查看器在构建发布器的配置接口时将调用此方法。

Identity Manager 将在服务器启动时以及审计配置更改之后使用 `configure(` *Map*`)` 方法配置发布器。

开发格式化程序

REF 工具包包括以下格式化程序的源代码：

- `XmlFormatter`。将审计事件格式化为 XML 字符串。
- `UlfFormatter`。根据通用日志记录格式 (Universal Logging Format, ULF) 格式化审计事件。Sun Application Server 使用此格式。

格式化程序必须实现 `AuditRecordFormatter` 接口。此外，格式化程序必须具有一个**无参数**的构造函数。有关详细信息，请参阅 REF 工具包中的 Javadoc。

注册发布器/格式化程序

`#ID#Configuration:SystemConfiguration` 对象的审计属性列出了所有已注册的发布器和格式化程序。仅这些发布器和格式化程序可在审计配置用户界面中使用。

◆ ◆ ◆ 第 11 章

11 PasswordSync

PasswordSync 检测起始于 Windows 域上的用户密码更改，并将这些更改转发给 Identity Manager。然后，Identity Manager 与 Identity Manager 中定义的其他资源之间同步密码更改。

本章采用以下组织形式：

什么是 PasswordSync？

PasswordSync 功能可以使在 Windows Active Directory 域上进行的用户密码更改与 Identity Manager 中定义的其他资源保持同步。PasswordSync 必须安装在将与 Identity Manager 同步的域中的每个域控制器上。PasswordSync 必须与 Identity Manager 分开安装。

PasswordSync 由位于每个域控制器上的 DLL (`lhpwic.dll`) 组成。此 DLL 从 Windows 接收密码更新通知，对其进行加密，然后通过 HTTPS 将其发送到 PasswordSync Servlet。PasswordSync Servlet 位于运行 Identity Manager 的应用服务器上。

注 – 首选使用 HTTPS，但也支持 HTTP。

PasswordSync Servlet 将通知转换为 Identity Manager 可以理解的格式。然后，该 Servlet 使用以下方法之一将密码更改（仍处于加密状态）发送到 Identity Manager：

- **直接方法**。Servlet 使用本机 Identity Manager 类将密码更改直接传送到 Identity Manager。（请参见第 317 页中的“什么是 PasswordSync？”。）

  建议将直接连接方法仅用于不太复杂的较小环境，这种环境只要求将消息传送到一个系统，并且不要求确保传送消息。（如果由于某种原因无法直接传送消息，该消息将会丢失。无法进行备份传送。）

- **JMS 方法**。Servlet 使用 JMS（Java Message Service，Java 消息服务）将密码信息发送到 Identity Manager。借助于 JMS，Servlet 将密码更改提交到 JMS 消息队列。Identity Manager 的 JMS 侦听器资源适配器将单独检查队列中的新消息。如果找到在队列中等待的密码更改消息，JMS 侦听器适配器将从队列中提取该消息，并将其导入到 Identity Manager 中。（请参见图 11–2。）

  建议将 JMS 方法用于较复杂的环境，这种环境具有较高的数据传送量要求，需要将消息传送到多个系统，并且要确保将消息传送到目标位置。可以将 JMS 消息队列设置为具有较高的可用性。只要消息位于队列中，如果到 Identity Manager 的消息传送失败，该队列将保留更改，直到将消息传送到 Identity Manager。

  您必须单独安装和配置 JMS。

图 11–1 以图表形式显示了直接连接。在此配置中，PasswordSync Servlet 将更新消息直接发送到 Identity Manager。

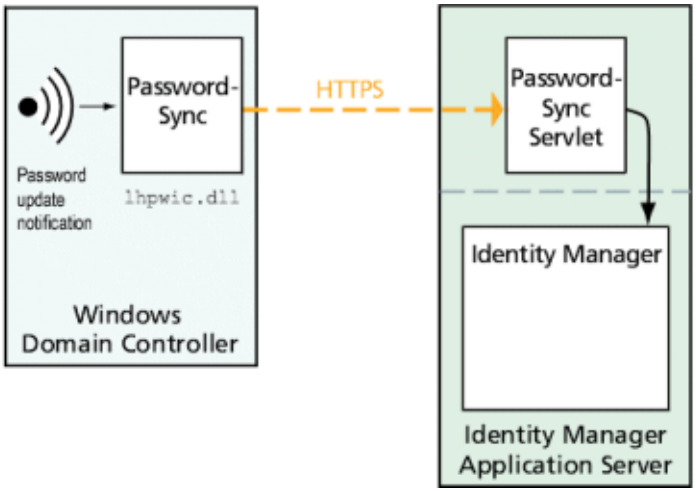


图 11–1 PasswordSync 逻辑图表（直接连接）。

图 11–2 以图表形式显示了 JMS 连接。在此配置中，PasswordSync Servlet 将更新消息发送到 JMS 消息队列。Identity Manager 的 JMS 侦听器资源适配器定期检查队列（图中用浅蓝色箭头表示）中的新消息。队列将消息发送到 Identity Manager（用深蓝色箭头表示）以进行响应。

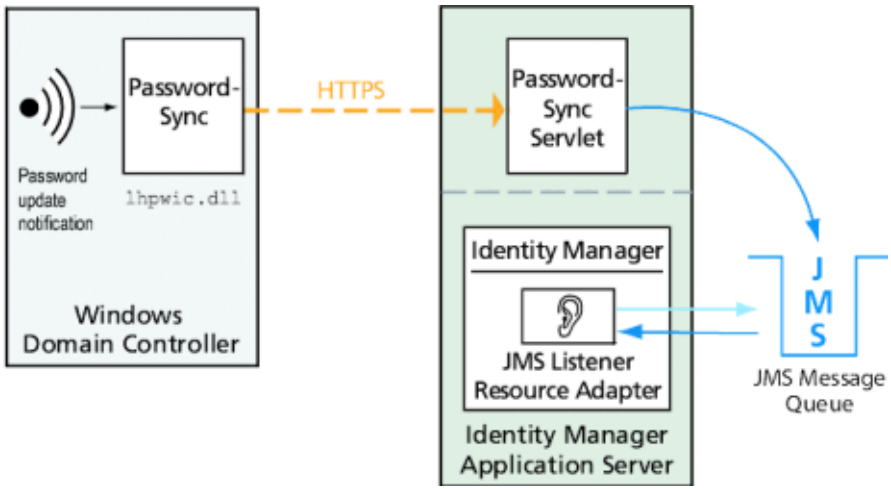


图 11–2 PasswordSync 逻辑图表（JMS 连接）。

当 Identity Manager 收到密码更改通知时，将对其进行解密，然后使用工作流任务处理该更改。密码将在用户所有的分配资源中得到更新，并且 SMTP 服务器发送电子邮件通知用户密码更改的状态。

注 – 只有在成功更改密码时，Windows 才会发出更新通知。如果密码更改请求不符合域的密码策略，Windows 将拒绝该请求，并且不会将同步数据发送到 Identity Manager。

图 11–3 显示了 Identity Manager 在收到密码更新通知后启动工作流并向用户发送电子邮件的过程。

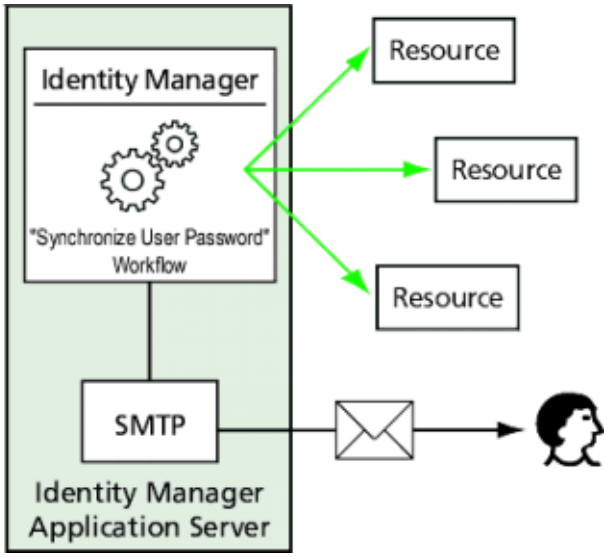


图 11–3 PasswordSync 触发了一个工作流。

注 – PasswordSync 放弃以 $（美元符号）结尾的帐户名称的所有帐户更改通知。名称以 $ 结尾的帐户被视为 Windows 计算机帐户。不会将以美元符号结尾的任何用户帐户名称转发到 Identity Manager。

安装之前

只能在 Windows 2008、Windows 2003 和 Windows 2000 域控制器上设置 PasswordSync 功能。（Identity Manager 8.0 版中不再提供对 Windows NT 域控制器的支持。）必须在与 Identity Manager 同步的域中的每个主域控制器和备份域控制器上安装 PasswordSync。强烈建议将 PasswordSync 配置为使用 HTTPS。

注 – 在所有域控制器上，应该将早于 PasswordSync 7.1.1 的版本至少更新到版本 7.1.1。

rpcrouter2 servlet 支持在 8.0 版中已过时，将来的发行版中将删除该支持。PasswordSync 7.1.1 和更高版本支持新协议。

如果使用的是 JMS，PasswordSync 需要与 JMS 服务器连接。有关 JMS 系统要求的详细信息，请参见《Sun Identity Manager 8.1 Resources Reference》中的 "JMS Listener resource adapter" 一节。

此外，PasswordSync 还要求您

- 在每个域控制器上至少安装 Microsoft .NET 1.1。
- 删除 PasswordSync 的任何先前版本。

以下各节将详细讨论这些要求。

安装 Microsoft .NET 1.1

要使用 PasswordSync，必须至少安装 Microsoft .NET 1.1 Framework。如果您使用 Windows 2003 域控制器，则默认安装此 Framework。默认情况下，在 Windows 2008 域控制器上安装 Microsoft .NET 2.0 Framework。如果使用的是 Windows 2000 域控制器，则默认不安装该框架。可以从 Microsoft 下载中心下载此工具包：

`http://www.microsoft.com/downloads`

注 –

- 在“关键字”搜索字段中输入 **`.NET Framework Redistributable`** 以快速找到该框架工具包。
- 该工具包将安装 .NET Framework。

将 PasswordSync 配置为使用 SSL

虽然在将敏感数据发送到 Identity Manager 服务器之前已对其进行加密，Sun Microsystems 仍建议对 PasswordSync 进行配置以使用安全 SSL 连接（即 HTTPS 连接）。

有关如何安装导入的 SSL 证书的信息，请参见以下 Microsoft 知识库 How-To 文章：

`http://support.microsoft.com/kb/816794`

在安装 PasswordSync 后，可通过在 PasswordSync 的“配置”对话框中指定 HTTPS URL 来测试是否正确配置了 SSL 连接。有关说明，请参见第 344 页中的 “测试配置”。

卸载 PasswordSync 的先前版本

安装更高版本之前，**必须**先删除任何先前安装的 PasswordSync 实例。

- 如果先前安装的 PasswordSync 版本支持 `IdmPwSync.msi` 安装程序，可以使用标准的 Windows“添加/删除程序”实用程序来删除此程序。
- 如果先前安装的 PasswordSync 版本**不**支持 `IdmPwSync.msi` 安装程序，则可以使用 InstallAnywhere 卸载程序来删除此程序。

在 Windows 上安装和配置 PasswordSync

本节包含有关安装和配置 PasswordSync 的信息和说明。

此信息分为以下几个部分：

▼ 安装 PasswordSync 配置应用程序

以下过程介绍了如何安装 PasswordSync 配置应用程序。

注 – 必须在与 Identity Manager 同步的域中的每个域控制器上安装 PasswordSync。

在继续操作之前，请确保卸载以前安装的任何版本的 PasswordSync。

---

1. **从 Identity Manager 安装介质中，**

   - 双击 `pwsync\IdmPwSync_x86.msi`（如果安装到 32 位版本的 Windows）。
   - 双击 `pwsync\IdmPwSync_x64.msi`（如果安装到 64 位版本的 Windows）。

   将打开安装向导，并且“欢迎”窗口显示以下导航按钮：

   - **取消**。随时可以单击以退出向导，而不保存任何更改。
   - **上一步**。单击以返回上一个对话框。
   - **下一步**。单击以前进到下一个对话框。

2. **阅读“欢迎”屏幕上提供的信息，然后单击“下一步”以显示“选择安装类型”窗口。**

3. **单击“典型”或“完全”安装完整的 PasswordSync 软件包，或者单击“自定义”控制安装哪些软件包组件。单击“下一步”继续。**

4. **在显示“准备安装”窗口时，单击“安装”以安装该产品。**

5. **将显示最终窗口。启用“启动配置应用程序”框，以便开始配置 Password Sync，然后单击“完成”以完成安装过程。**

   第 11 章，PasswordSync 中提供了有关配置 PasswordSync 的说明。

注 – 将显示一个对话框，提示必须重新启动系统才能使更改生效。在完成 PasswordSync 配置之前不需要重新启动系统，但在实现 PasswordSync 之前必须重新启动域控制器。

第 322 页中的 “在 Windows 上安装和配置 PasswordSync”介绍了在每个域控制器上安装的文件。

安装的组件	描述
`%$INSTALL_DIR$%\configure.exe`	PasswordSync 配置程序
`%$INSTALL_DIR$%\configure.exe.manifest`	用于配置程序的数据文件
`%$INSTALL_DIR$%\passwordsyncmsgs.dll`	处理 PasswordSync 消息的 DLL
`%SYSTEMROOT%\SYSTEM32\lhpwic.dll`	密码通知 DLL，该 DLL 实现 Windows `PasswordChangeNotify()` 功能。

▼ 配置 PasswordSync

如果从安装程序运行配置应用程序，则该应用程序会将配置屏幕显示为向导。完成向导后，以后每次运行 PasswordSync 配置应用程序时，都可以通过选择选项卡在屏幕间导航。

1 **如果尚未运行 PasswordSync 配置应用程序，请启动该应用程序。**

默认情况下，此配置应用程序安装在 "Program Files" → "Sun Identity Manager PasswordSync" → "Configuration" 中。

注 – 如果不打算使用 JMS，请从命令行中启动该配置应用程序并确保包含 `-direct` 标志，如下所示：

```
C:\InstallDir\Configure.exe -direct
```

将显示 PasswordSync 配置向导对话框（请参见图 11–4）。

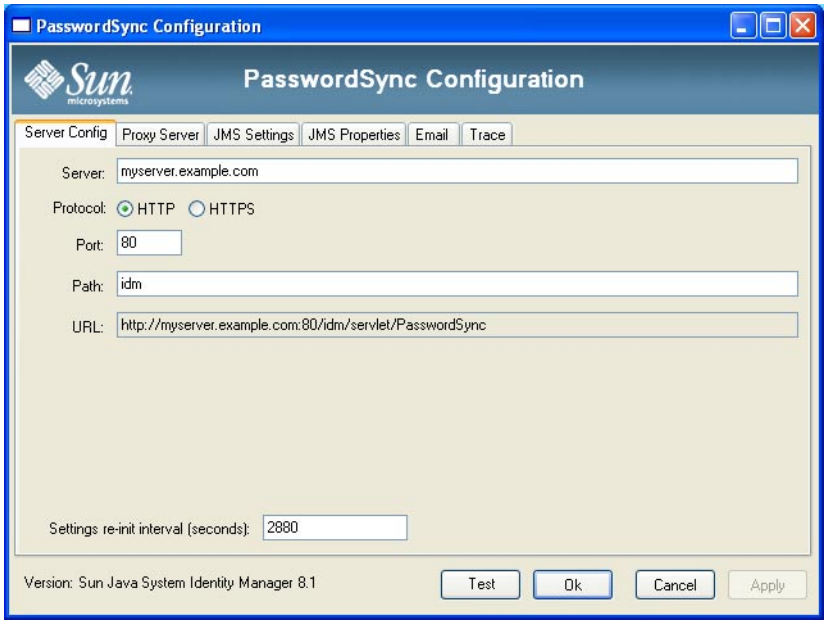


图 11–4 PasswordSync 配置向导

2 **根据需要，编辑该对话框中的字段。**

这些字段包括：

- **服务器**必须用安装 Identity Manager 的全限定主机名或 IP 地址替换。
- **协议**指示是否与 Identity Manager 进行安全连接。

  PasswordSync 支持配置 HTTPS 连接的证书检查行为。在启用 HTTPS 时，将显示以下选项：

  - **允许使用撤销的证书**。此设置映射到连接上的 `securityIgnoreCertRevoke` 注册表值。默认情况下，PasswordSync 不会忽略撤销问题，并将 `securityIgnoreCertRevoke` 注册表值设置为 0。

    如果希望 PasswordSync 忽略撤销的证书消息，请选中该框（或将 `SECURITY_FLAG_IGNORE_REVOCATION` 注册表值设置为 1）。

  - **允许使用无效的证书**。此设置影响连接上的 `SECURITY_FLAG_IGNORE_CERT_CN_INVALID`、`SECURITY_FLAG_IGNORE_CERT_DATE_INVALID` 和 `SECURITY_FLAG_IGNORE_UNKNOWN_CA` 选项。默认情况下，PasswordSync 不允许使用无效的证书，并将这些注册表值设置为 0。

    如果选中该框或将 `securityAllowInvalidCert` 注册表值设置为 1，则允许 PasswordSync 使用未通过一些安全检查的证书。对于生产环境，**不建议**启用此选项。

注 – 不会为 HTTP 协议类型显示这些设置，这些设置也不会影响 HTTP 设置。

- **端口**指定服务器的可用端口。对于 HTTP，默认端口为 80。对于 HTTPS，默认端口为 443。
- **路径**指定应用服务器上的 Identity Manager 的路径。
- **URL** 是通过将其他字段连接在一起生成的。不可在 URL 字段编辑该值。
- **设置重新初始化时间间隔（秒）**指定 PasswordSync `dll` 应从注册表中重新读取配置设置的频率。默认值为 2880 秒或 8 小时。

注 – 此 PasswordSync 配置向导以秒为单位显示该值，但注册表值实际是以毫秒存储的。

在 PasswordSync `dll` 处于活动状态时，该 `dll` 将从注册表中读取配置设置。此时间间隔值存储在 `reinitIntervalMilli` 注册表值中。

在更新这些设置时，无法同步密码，这可能会导致在处理密码更改时出现很短的延迟。通常，此延迟不到 1 秒。在更新完成后，PasswordSync 将直接处理在更新期间收到的任何密码更改。另外，PasswordSync 不会在进行密码同步时处理设置更新。将重新安排更新并在稍后执行。

3 单击“下一步”以显示“代理服务器配置”页（图 11–5），然后根据需要编辑这些字段。

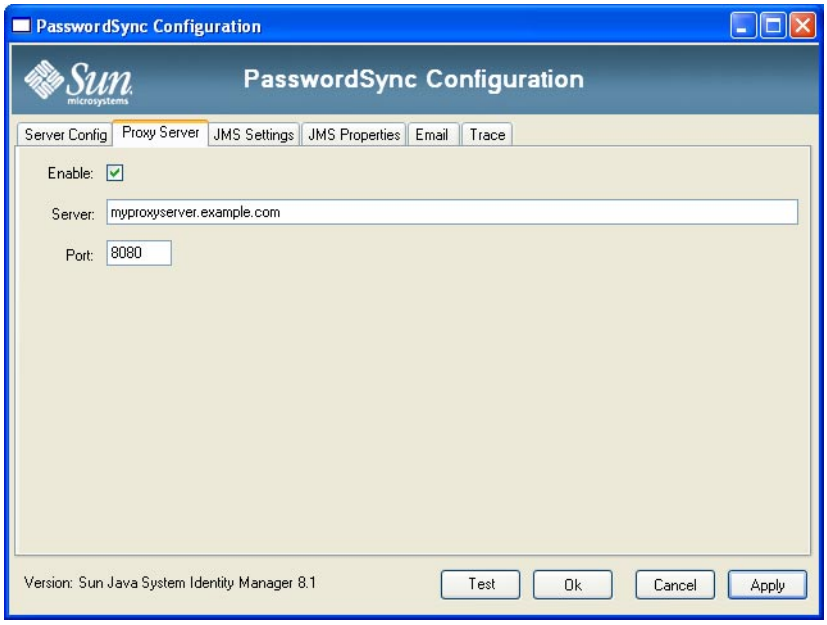


图 11–5 PasswordSync 向导“代理服务器”对话框

这些字段包括：

- **启用**。选择是否需要使用代理服务器。
- **服务器**。您必须输入代理服务器的全限定主机名或 IP 地址。
- **端口**。指定服务器的可用端口号。（默认代理端口为 8080，默认 HTTPS 端口为 443。）

4 单击“下一步”。

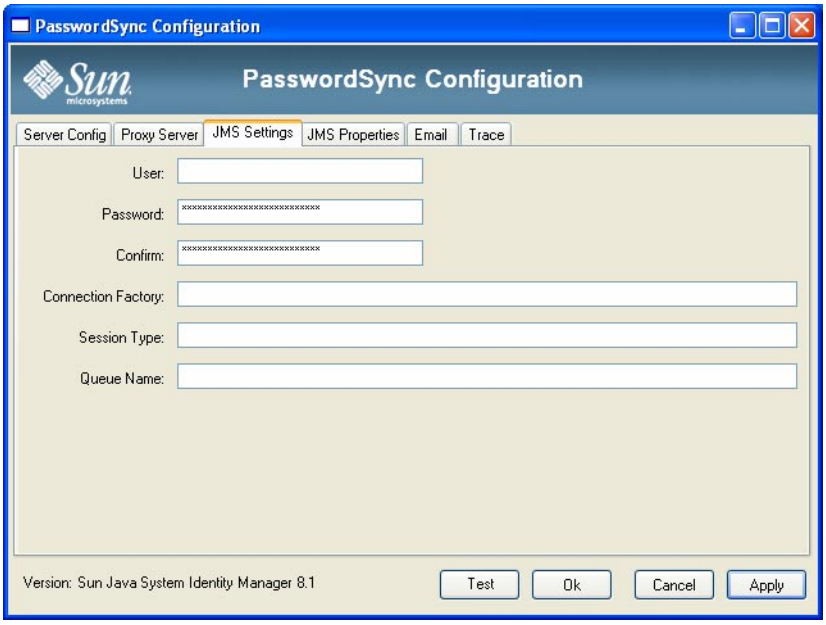


图 11–6 PasswordSync 向导“JMS 设置”对话框

在显示“JMS 设置”对话框（图 11–6）时，执行以下操作之一：

- 根据需要，编辑以下字段：
  - **用户**指定在队列中加入新消息的 JMS 用户名称。
  - **密码**和**确认密码**指定 JMS 用户的密码。
  - **连接工厂**指定要使用的 JMS 连接工厂的名称。该工厂必须已存在于 JMS 系统中。
  - 大多数情况下，应将**会话类型**设置为 `LOCAL`，这表示将使用本地会话事务。系统收到每条消息后，将提交会话。其他可能的值包括 `AUTO`、`CLIENT` 和 `DUPS_OK`。
  - **队列名称**指定密码同步事件的目的地查找名称。
- 如果不打算使用 JMS，并且使用 `-direct` 标志启动配置向导，请单击“下一步”以显示“用户”对话框。跳过此步骤并转到下一步（图 11–7）。

5 单击“下一步”以显示“JMS 属性”对话框（图 11–7）。

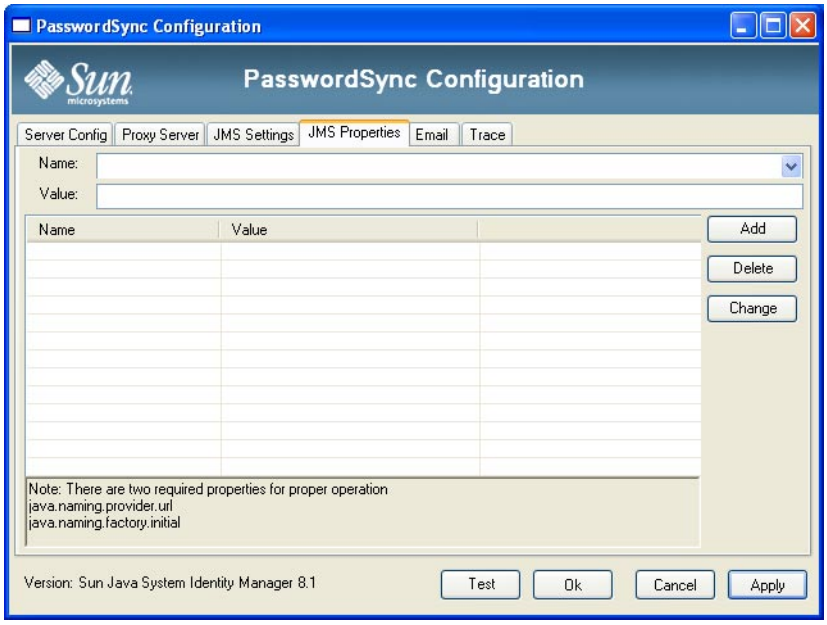


图 11–7 PasswordSync 向导“JMS 属性”对话框

JMS 属性对话框允许您定义用于构建初始 JNDI 上下文的属性集。您必须定义以下名称/值对：

- `java.naming.provider.url` - 指定运行 JNDI 服务的计算机的 URL。
- `java.naming.factory.initial` - 指定 JNDI 服务提供者的初始上下文工厂的类名（包括包）。

  “名称”下拉菜单包含 `java.naming` 软件包中的类的列表。在类名称中选择一个类或类型，然后在“值”字段中输入其相应的值。

6 **如果不打算使用 JMS，并且使用 `-direct` 标志启动配置向导，请配置“用户”选项卡。否则，跳过此步骤并转到下一步。**

要配置“用户”选项卡，请根据需要编辑这些字段。

- **帐户 ID**。指定将用于连接到 Identity Manager 的用户名。
- **密码**。指定将用于连接到 Identity Manager 的密码。

7 **单击“下一步”以显示“电子邮件”对话框（图 11–8），并根据需要编辑这些字段。**

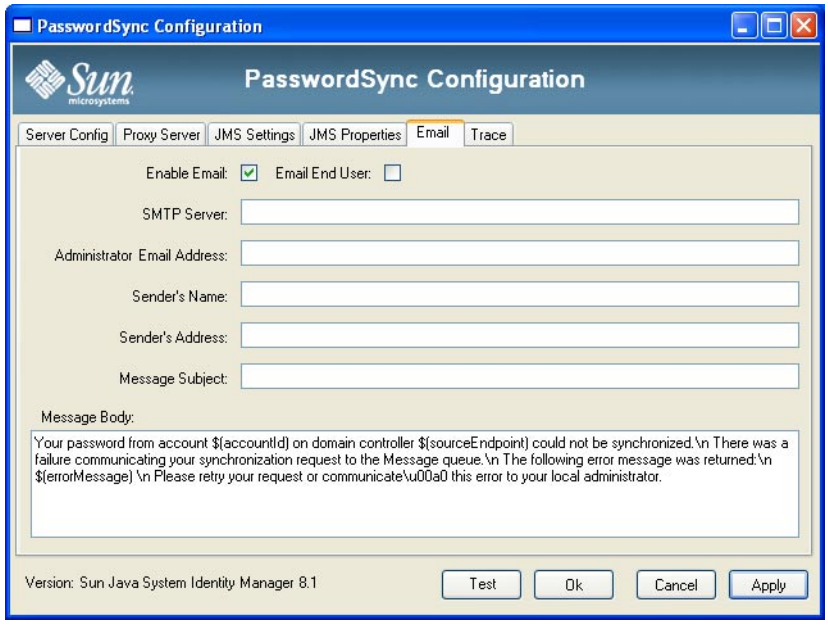


图 11–8 PasswordSync 向导“电子邮件”对话框

要在用户的密码更改没有成功同步（由于通信错误或 Identity Manager 之外的其他错误）时发送电子邮件通知，请使用“电子邮件”对话框中的以下选项设置通知和配置电子邮件。

- **启用电子邮件**。选择此选项可以启用该功能。
- **电子邮件最终用户**。如果用户要接收通知，请选择此选项。否则，将仅通知管理员。
- **SMTP 服务器**。输入发送故障通知时使用的 SMTP 服务器的全限定名称或 IP 地址。
- **管理员电子邮件地址**。输入要将通知发送到的电子邮件地址。
- **发件人名称**。输入发件人的“友好名称”。
- **发件人地址**。输入发件人的电子邮件地址。
- **邮件主题**。输入所有通知的主题行。
- **邮件正文**。输入通知的文本。

  邮件正文可能包含以下变量：

  - `$(accountId)` - 尝试更改密码的用户的帐户 ID。
  - `$(sourceEndpoint)` - 安装密码通知程序的域控制器的主机名，该主机名有助于找到出现故障的计算机。
  - `$(errorMessage)` - 用于描述所出现的错误的错误消息。

8 单击“跟踪”选项卡（图 11–9）。

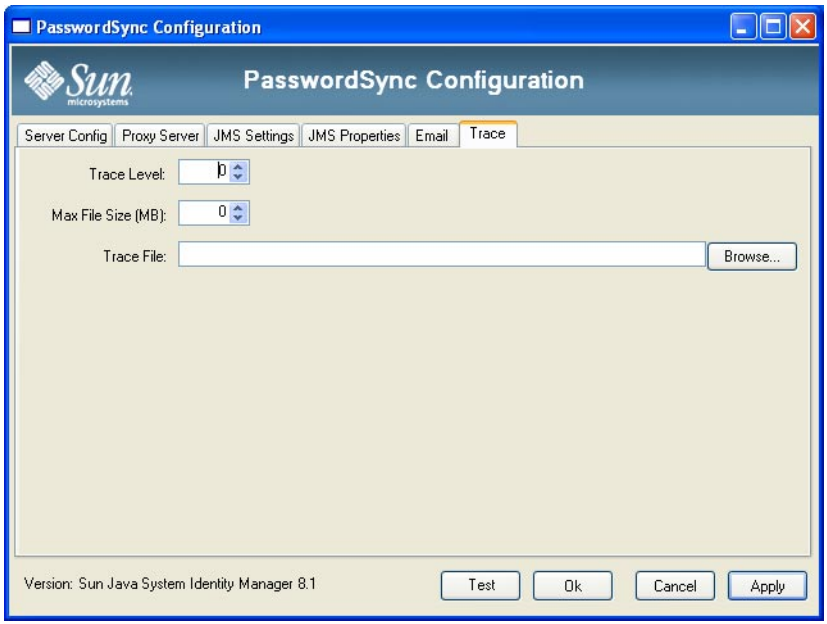


图 11–9 “跟踪”选项卡

设置以下字段。

- **跟踪级别**。
- **最大文件大小 (MB)**。
- **跟踪文件**。

9 **单击“完成”保存更改。**

如果再次运行配置应用程序，将显示一组选项卡而不是向导。如果要将应用程序显示为向导，请从命令行中键入以下命令：

```
C:\InstallDir\Configure.exe -wizard
```

要测试 PasswordSync 配置，请参见第 344 页中的 “测试配置”。

无提示安装 PasswordSync

可以将 PasswordSync 安装程序配置为无提示安装。要使用此功能，必须在安装 PasswordSync 时首先将配置参数记录到文件中。将来的安装将引用该文件并重新应用这些配置设置。

注 – 如果要使用无提示安装过程，则必须在将要使用该产品的每个服务器上安装完整产品。记录并重新应用配置设置取决于要在系统上安装的配置应用程序。

无提示安装过程利用一个名为 `msiexec` 的 Windows 实用程序，它将从命令行安装 `.msi` 文件。

在命令提示符下键入 `msiexec /?` 可查看该实用程序的用法信息。

Microsoft 网站上也提供了相关文档。例如，有关在 Windows Server 2003 上使用 `msiexec` 的文档，请参见 `http://technet.microsoft.com/en-us/library/cc759262.aspx`。

▼ 捕获安装参数将其写入到配置文件中

可以按照以下说明使用安装向导安装 PasswordSync。该配置实用程序将捕获配置参数并将其写入到 XML 文件中。

开始之前 在安装之前，请删除旧版本的 PasswordSync。

1. **转到包含 PasswordSync 安装 (`.msi`) 文件的目录。**
   有关信息，请参见第 322 页中的 “安装 PasswordSync 配置应用程序”。

2. **在命令提示符下键入以下命令。参数和值区分大小写。**

   ```
   msiexec /i pwSyncInstallFile CONFIGARGS="-writexml fullPathToFile"
   ```

   其中：

   - **pwSyncInstallFile** 是 PasswordSync 安装文件（`IdmPwSync_86.msi` 或 `IdmPwSync_x64.msi`）。
   - **fullPathToFile** 指定写入 XML 文件的位置。

   例如：

   ```
   msiexec /i IdmPwSync_x86.msi CONFIGARGS="-writexml c:\tmp\myconfig.xml"
   ```

3. **安装该产品。**

▼ 无提示安装 PasswordSync

开始之前

- 应创建安装配置 XML 文件。有关说明，请参见第 331 页中的 “捕获安装参数将其写入到配置文件中”。
- 在安装之前，请删除旧版本的 PasswordSync。

1. **将安装配置 XML 文件复制到安装程序可读取的位置。**

2 **在命令提示符下键入以下命令。参数和值区分大小写。**

```
msiexec /i pwSyncInstallFile ADDLOCAL="installFeature" CONFIGARGS="-readxml fullPathToFile"
 INSTALLDIR="installDir" /q
```

其中：

- **pwSyncInstallFile** 是 PasswordSync 安装文件（`IdmPwSync_86.msi` 或 `IdmPwSync_x64.msi`）。
- **installFeature** 指定要安装的 PasswordSync 功能。选择以下参数之一：
  - `MainProgram` - 仅安装拦截器 `.dll` 文件
  - `Configuration` - 仅安装配置应用程序
  - `ALL` - 安装完整产品

  如果未指定任何参数，则默认使用 `MainProgram`（如果提供了 `/q` 选项）。
- **fullPathToFile** 指定配置 XML 文件的路径。
- **installDir** 指定自定义安装目录的完整路径。可选。
- **/q** 指定一个非 GUI 安装，将在完成后自动重新启动服务器。如果不包含该选项，将显示安装向导，但使用预定义设置运行配置。可选。

示例：

```
msiexec /i IdmPwSync_x86.msi CONFIGARGS="-readxml c:\tmp\myconfig.xml"

msiexec /i IdmPwSync_x86.msi ADDLOCAL="MainProgram"
CONFIGARGS="-readxml c:\tmp\myconfig.xml" /q

msiexec /i IdmPwSync_x64.msi ADDLOCAL="Complete"
CONFIGARGS="-readxml c:\tmp\myconfig.xml"
INSTALLDIR="C:\Program Files\Sun Microsystems\MyCustomInstallDirectory" /q
```

在应用服务器上部署 PasswordSync

在 Windows 域控制器上安装 PasswordSync 后，您必须在运行 Identity Manager 的应用服务器上执行其他步骤。

无需在应用服务器上安装 PasswordSync Servlet。在安装 Identity Manager 时，将自动安装该 Servlet。

不过，要完成 PasswordSync 部署，您需要在 Identity Manager 中执行以下操作：

- 添加并配置 JMS 侦听器适配器（如果使用的是 JMS）
- 实现“同步用户密码”工作流
- 设置通知

添加和配置 JMS 侦听器适配器

如果 PasswordSync Servlet 使用 JMS 将消息发送到 Identity Manager，则需要添加 Identity Manager 的 JMS 侦听器资源适配器。JMS 侦听器资源适配器定期检查 PasswordSync Servlet 放在 JMS 消息队列中的消息。如果队列中包含新消息，则会将其发送到 Identity Manager 以进行处理。

▼ 添加 JMS 侦听器资源适配器

1 **登录到 Identity Manager 管理员界面（第 33 页中的“Identity Manager 管理员界面”）。**

2 **从主菜单中选择“资源”→“配置类型”。**
将打开“配置受管理的资源”页，如图 11–10 中所示。

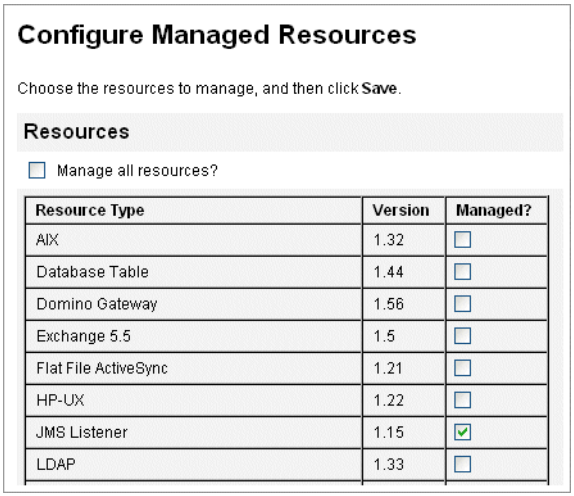


图 11–10 “配置受管理的资源”页。

3 **确保选中“受管理？”列中的“JMS 侦听器”复选框，如图 11–10 中所示。**
如果未选中该框，请将其选中，然后单击“保存”。

4 **单击次级菜单中的“列出资源”。**

5 **找到“资源类型操作”下拉菜单，然后选择“新建资源”。**
将显示“新建资源”页。

6 **要添加 JMS 侦听器适配器，请从下拉菜单中选择“JMS 侦听器”（如图 11–11 中所示），然后单击“新建”。**

图 11–11 新建资源向导

7 **在“资源参数”页上配置以下设置，然后单击“下一步”。**

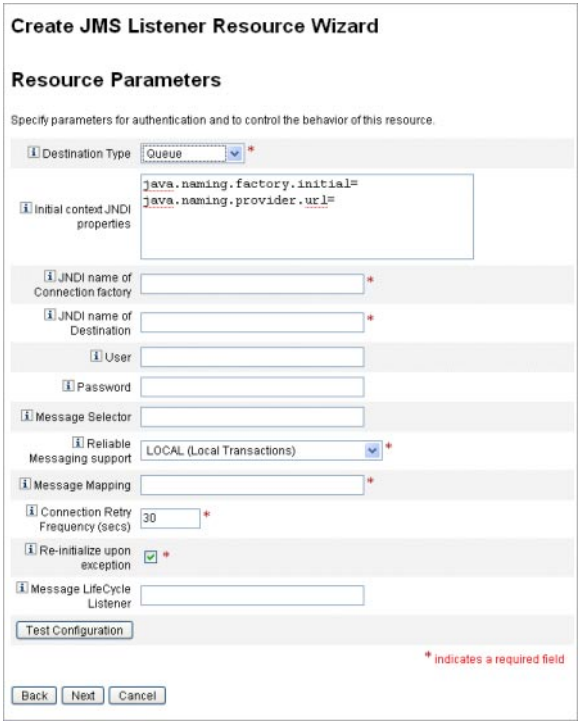
- **目的地类型**。通常将该值指定为“队列”。（因为有一个订阅者而可能有多个发布者，所以各主题通常不相关。）
- **初始上下文 JNDI 属性**。定义一组用于构建初始 JNDI 上下文的属性。

  您必须定义以下名称/值对：

  - `java.naming.factory.initial`。指定 JNDI 服务提供者的初始上下文工厂的类名（包括包）。
  - `java.naming.provider.url`。指定运行 JNDI 服务的计算机的 URL。

    您可能需要定义其他属性。属性和值的列表应该与 JMS 服务器上的 JMS 设置页中指定的属性和值相匹配。例如，要提供凭证和绑定方法，您可能需要指定以下示例属性：

    - `java.naming.security.principal` - 绑定 DN（例如，cn=Directory manager）
    - `java.naming.security.authentication` - 绑定方法（例如，简单绑定）
    - `java.naming.security.credentials` - 密码
- **连接工厂的 JNDI 名称**。输入在 JMS 服务器中定义的连接工厂的名称。
- **目的地的 JNDI 名称**。输入在 JMS 服务器中定义的目的地的名称。
- **用户**和**密码**。输入从队列中请求新事件的管理员的帐户名称和密码。
- **可靠的邮件传送支持**。选择 `LOCAL`（**本地事务**）。其他选项不适用于密码同步。
- **邮件映射**。输入 `java:com.waveset.adapter.jms.PasswordSyncMessageMapper`。该类将来自 JMS 服务器的消息转换为同步用户密码工作流可以使用的格式。



8 **在“帐户属性”向导页（图 11–12）上，单击“添加属性”并映射以下属性（由 `PasswordSyncMessageMapper` 提供给 JMS 侦听器适配器）。**

- `IDMAccountId` - 该属性由 `PasswordSyncMessageMapper` 根据在 JMS 消息中传递的 `resourceAccountId` 和 `resourceAccountGUID` 属性解析。
- `password` - 在 JMS 消息中转发的加密密码。

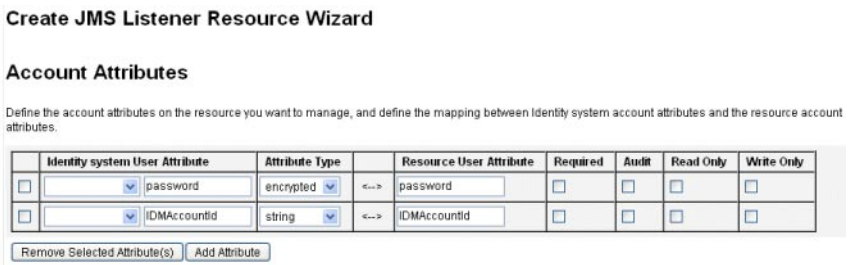


图 11–12 创建 JMS 侦听器资源向导的“帐户属性”页

9 **单击“下一步”。**

将打开“身份模板”向导页，如图 11–13 中所示。请注意，在上一步中添加的属性显示在资源向导的“属性映射”部分中（图 11–13）。

图 11–13 JMS 侦听器资源向导属性映射

10 **单击“下一步”，然后根据需要配置“Identity System 参数”页中的选项。**

有关设置 JMS 侦听器资源适配器的详细信息，请参见《Sun Identity Manager 8.1 Resources Reference》。

实现“同步用户密码”工作流

当 Identity Manager 收到密码更改通知时，它将启动“同步用户密码”工作流。默认“同步用户密码”工作流将签出 ChangeUserPassword 查看器，然后再次将其签入。接下来，工作流将处理所有资源帐户（发送最初密码更改通知的 Windows 资源除外）。最后，Identity Manager 将向用户发送电子邮件，指示所有资源上的密码更改是否成功。

如果要默认实现同步用户密码工作流，则将其作为 JMS 侦听器适配器实例的进程规则进行分配。可以在配置 JMS 侦听器以进行同步时分配进程规则（请参见第 342 页中的“配置活动同步”）。

如果要修改工作流，请复制 `$WSHOME/sample/wfpwsync.xml` 文件并进行修改。然后，将修改的工作流导入到 Identity Manager 中。

可能要对默认工作流执行的修改包括：

- 更改密码后通知哪些实体。
- 无法找到 Identity Manager 帐户时会出现什么情况。
- 如何在工作流中选择资源。
- 是否允许从 Identity Manager 中更改密码。

有关使用工作流的详细信息，请参见《Sun Identity Manager Deployment Reference》中的第 1 章 “Workflow”。

设置通知

Identity Manager 提供了两个电子邮件模板，它们可以通知用户所有资源上的密码更改是否成功。

这两个模板为：

- 密码同步通知
- 密码同步失败通知

两个模板均应该更新，以便在用户需要进一步帮助时，为其提供有关下一步操作的公司特定信息。有关详细信息，请参见第 4 章，配置业务管理对象中的第 92 页中的 “自定义电子邮件模板”。

在 Sun JMS Server 中配置 PasswordSync

Identity Manager 可以使用 Java 消息服务 (Java Message Service, JMS) 从 PasswordSync Servlet 中接收密码更改通知。除了确保传送消息外，JMS 还可以将消息传送到多个系统。

注 – 有关此适配器的详细信息，请参见《Sun Identity Manager 8.1 Resources Reference》 。

本节通过使用示例方案来提供有关使用 Sun JMS 服务器配置 PasswordSync 的说明。

信息通过以下方式进行组织：

示例方案

使用 JMS 服务器配置 PasswordSync 的典型（简单）使用案例是使用户在 Windows 上更改其密码，然后令 Identity Manager 获取新密码，最后在 Sun Directory Server 上使用新密码更新用户帐户。

需要为该方案配置以下环境：

- Windows Server 2003 Enterprise Edition– Active Directory
- Sun Java™ System Identity Manager 6.0 2005Q4M3
- 在 Suse Linux 10.0 上运行的 MySQL
- 在 Suse Linux 10.0 上运行的 Tomcat 5.0.28
- 在 SUSE Linux 10.0 上运行的 Sun Java System Message Queue 3.6 SP3 2005Q4
- 在 SUSE Linux 10.0 上运行的 Sun Java System Directory Server 5.2 SP4
- Java 1.5 (Java 5.0)

以下文件已复制到 Tomcat `common/lib` 目录以启用 JMS 和 JNDI：

- `jms.jar`（来自 Sun Message Queue）
- `fscontext.jar`（来自 Sun Message Queue）
- `imq.jar`（来自 Sun Message Queue）
- `jndi.jar`（来自 Java JDK）

创建和存储管理对象

本节介绍了用于创建和存储以下管理对象的指令，这些指令是示例方案正常工作所必需的：

- 连接工厂对象
- 目的地对象

您可以将管理对象存储到 LDAP 目录或文件中。如果使用的是文件，该文件的所有实例必须相同。

有关说明，请参见

- 第 338 页中的 “将管理对象存储到 LDAP 目录”
- 第 340 页中的 “将管理对象存储到文件”

注 –

- 本节的说明假定您已安装 Sun Java System Message Queue。（所需工具位于安装 Message Queue 的 `bin/` 目录中。）
- 您可以使用该 Message Queue 管理 GUI (`imqadmin`) 或命令行工具 (`imqobjmgr`) 以创建这些管理对象。以下指令使用命令行工具。

将管理对象存储到 LDAP 目录

可以将 PasswordSync 和 JMS 侦听器配置为使用 LDAP 目录中存储的管理对象。图 11–14 展示了该过程。PasswordSync Servlet 和 JMS 侦听器适配器必须从 LDAP 目录中检索连接工厂和目的地设置才能发送和接收消息。

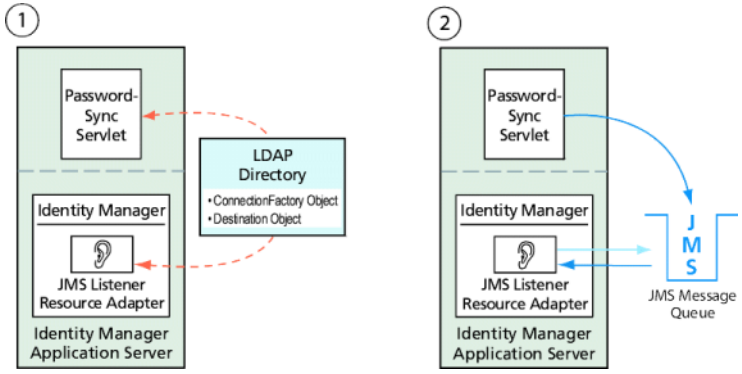


图 11–14　从 LDAP 目录中检索连接工厂和目的地对象

使用 Message Queue 命令行工具

本节介绍了如何使用 Message Queue 命令行工具 (`imqobjmgr`) 将受管理对象存储到 LDAP 目录中。

存储连接工厂对象

打开 Message Queue 命令行工具 (`imqobjmgr`)，然后键入第 339 页中的 “存储连接工厂对象”中的命令以存储连接工厂对象。

示例 11–1　存储连接工厂对象

```
#> ./imqobjmgr add -l "cn=mytestFactory"
-j "java.naming.factory.initial=com.sun.jndi.ldap.LdapCtxFactory"
-j "java.naming.provider.url=ldap://gwenig.coopsrc.com:389/ou=sunmq,dc=coopsrc,dc=com"
-j "java.naming.security.principal=cn=directory manager"
-j "java.naming.security.credentials=password"
-j "java.naming.security.authentication=simple"
-t qf -o "imqAddressList=mq://gwenig.coopsrc.com:7676/jms"
Adding a Queue Connection Factory object with the following attributes:
imqAckOnAcknowledge [Message Service Acknowledgement of Client Acknowledgements] ...
imqSetJMSXUserID [Enable JMSXUserID Message Property] false
Using the following lookup name: cn=mytestFactory The object's read-only state: false
To the object store specified by:
java.naming.factory.initial com.sun.jndi.ldap.LdapCtxFactory
java.naming.provider.url
ldap://gwenig.coopsrc.com:389/ou=sunmq,dc=coopsrc,dc=com
java.naming.security.authentication
simple java.naming.security.credentials netscape
java.naming.security.principal
cn=directory manager Object successfully added.
```

在第 339 页中的 “存储连接工厂对象”中，imqAddressList 定义了 JMS 服务器/代理主机名 (gwenig.coopsrc.com)、端口 (7676) 以及访问方法 (jms)。

存储目的地对象

在 Message Queue 命令行工具 (imqobjmgr) 中，键入第 340 页中的 “存储目的地对象”中的命令以存储目的地对象。

示例 11–2 存储目的地对象

```
#> ./imqobjmgr add -l "cn=mytestDestination"
-j "java.naming.factory.initial=com.sun.jndi.ldap.LdapCtxFactory"
-j "java.naming.provider.url=ldap://gwenig.coopsrc.com:389/ou=sunmq,dc=coopsrc,dc=com"
-j "java.naming.security.principal=cn=directory manager"
-j "java.naming.security.credentials=password"
-j "java.naming.security.authentication=simple"
-t q -o "imqDestinationName=mytestDestination"
Adding a Queue object with the following attributes:
imqDestinationDescription [Destination Description]
A Description for the Destination Object imqDestinationName [Destination Name]
mytestDestination Using the following lookup name: cn=mytestDestination
The object's read-only state: false
To the object store specified by:
java.naming.factory.initial com.sun.jndi.ldap.LdapCtxFactory
java.naming.provider.url ldap://gwenig.coopsrc.com:389/ ou=sunmq,dc=coopsrc,dc=com
java.naming.security.authentication simple
java.naming.security.credentials netscape
java.naming.security.principal cn=directory manager Object successfully added.
```

您可以使用 ldapsearch 或 LDAP 浏览器来查看新创建的对象。

有关在 LDAP 服务器上存储受管理对象的一节到此结束。请跳过下一节（介绍如何在文件中存储管理对象），并转到第 342 页中的 “为该方案配置 JMS 侦听器适配器”上的一节。

将管理对象存储到文件

可以将 PasswordSync 和 JMS 侦听器配置为使用文件中存储的受管理对象。如果未在 LDAP 服务器上存储管理对象（第 338 页中的 “将管理对象存储到 LDAP 目录”），请按照本节中的说明进行操作。

存储连接工厂对象

打开 Message Queue 命令行工具 (imqobjmgr)，然后键入第 340 页中的 “存储连接工厂对象”中的命令以存储连接工厂对象并指定查找名。

示例 11–3 存储连接工厂对象并指定查找名称

```
#> ./imqobjmgr add -l "mytestFactory" -j
"java.naming.factory.initial= com.sun.jndi.fscontext.RefFSContextFactory"
 -j "java.naming.provider.url=file:///home/gael/tmp" -t qf -o
 "imqAddressList=mq://gwenig.coopsrc.com:7676/jms"
Adding a Queue Connection Factory object with the following attributes:
imqAckOnAcknowledge [Message Service Acknowledgement of Client Acknowledgements]
...
imqSetJMSXUserID [Enable JMSXUserID Message Property] false
Using the following lookup name:
mytestFactory
The object's read-only state: false
To the object store specified by:
java.naming.factory.initial com.sun.jndi.fscontext.RefFSContextFactory
java.naming.provider.url file:///home/gael/tmp
Object successfully added.
To specify a destination:
#> ./imqobjmgr add -l "mytestQueue" -j
"java.naming.factory.initial=com.sun.jndi.fscontext.RefFSContextFactory"
-j "java.naming.provider.url=file:///home/gael/tmp" -t q -o
"imqDestinationName=myTestQueue"
Adding a Queue object with the following attributes:
imqDestinationDescription [Destination Description] A Description for the Destination
Object imqDestinationName [Destination Name] myTestQueue
Using the following lookup name:
mytestQueue
The object's read-only state: false
To the object store specified by:
java.naming.factory.initial com.sun.jndi.fscontext.RefFSContextFactory
java.naming.provider.url file:///home/gael/tmp
Object successfully added.
```

在代理上创建目的地

默认情况下，Sun Message Queue 代理允许自动创建队列目的地（请参见 `config.properties`，其中 `imq.autocreate.queue` 的默认值为 `true`）。

如果没有自动创建队列目的地，则必须使用第 341 页中的 “在代理上创建目的地”（其中 *myTestQueue* 为目的地）中所示的命令在代理上创建目的地对象。

示例 11–4 在代理上创建目的地对象

```
name (Queue name):
#> cd /opt/sun/mq/bin
#>./imqcmd create dst -t q -n mytestQueue
Username: <admin>
Password: <admin>
```

示例 11–4 在代理上创建目的地对象 （续）

```
Creating a destination with the following attributes:
Destination Name mytestQueue
Destination Type Queue On the broker specified by:
------------------------
Host Primary Port
------------------------ localhost 7676
Successfully created the destination.
```

您可以将管理对象存储到目录或文件：

- **在目录中**：使用目录是一种集中存储连接工厂和目的地对象的方法。

  使用目录时，这些管理对象将存储为目录条目。

  注 – 如果 Identity Manager PasswordSync Servlet 和 Identity Manager 服务器不在同一台计算机上，则它们都必须能够访问 `.bindings` 文件。您可以在每台计算机上将受管理对象的创建过程重复两次，或者将 `.bindings` 文件复制到每台计算机上的正确位置。

- **在文件中**：如果 Identity Manager PasswordSync Servlet 和 Identity Manager 服务器在同一台服务器上运行（或者没有可用目录），则可以将管理对象存储到文件中。

  使用文件时，这两个管理对象将存储在单个文件（在 Windows 和 UNIX 上，文件名均为 `.bindings`）中，该文件位于为 java.naming.provider.url 指定的目录（例如，在 Windows 上为 `file:///c:/temp`，在 Unix 上为 `file:///tmp` ）下。

为该方案配置 JMS 侦听器适配器

在应用服务器上配置 JMS 侦听器适配器。请按照第 333 页中的 “添加和配置 JMS 侦听器适配器”一节中的说明进行操作。

配置活动同步

然后，配置 JMS 侦听器以进行同步。如果使用的是 JMS，则需要活动同步，但不会将其用于直接连接。

▼ 配置 JMS 侦听器以进行同步

1 在管理员界面中，单击菜单中的“资源”。

2 在资源列表中，选中“JMS 侦听器”复选框。

3 在资源操作列表中，选择“编辑同步策略。”
将打开 JMS 侦听器资源的“编辑同步”页（图 11–15）。

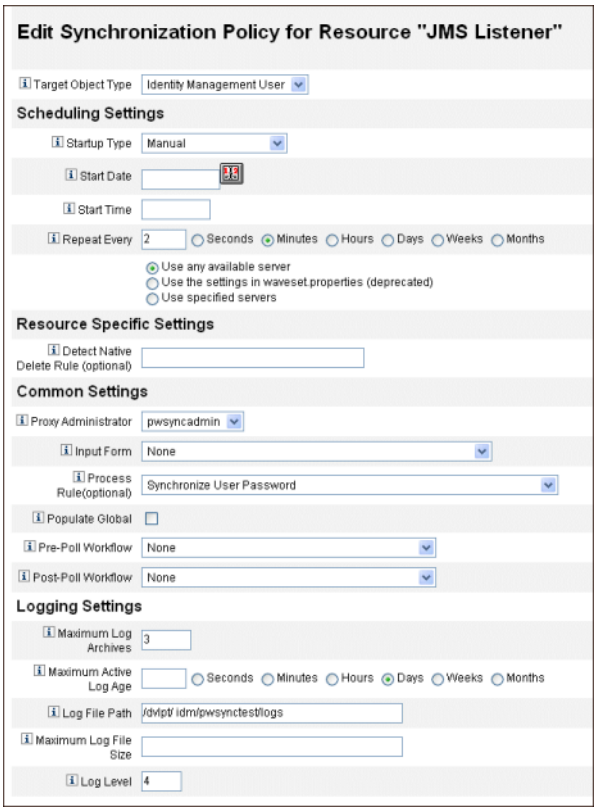


图 11–15 为 JMS 侦听器配置活动同步

4 在“通用设置”下找到“代理管理员”，然后选择 `pwsyncadmin`。（此管理员与空表单相关联。）

5 在“通用设置”下找到“进程规则”，然后从列表中选择“同步用户密码”。默认的同步用户密码工作流接受来自 JMS 侦听器适配器的每个请求并签出 ChangeUserPassword 查看器，然后再签回 ChangeUserPassword 查看器。

6 在“日志文件路径”框中，指定创建活动和归档日志文件时所在的目录路径。

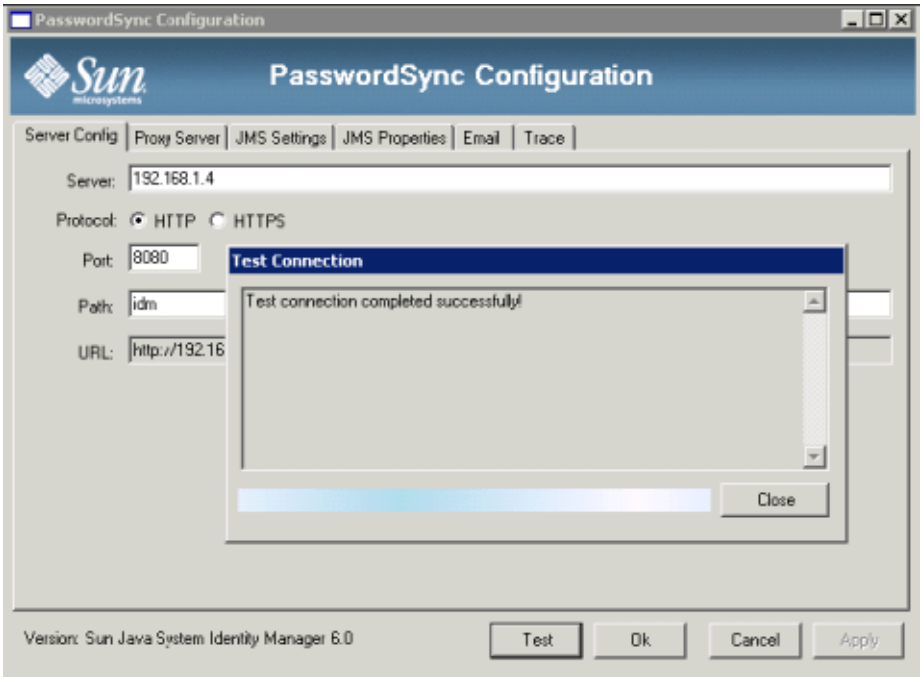
7 出于调试目的，请将日志级别设置为 4 以生成详细日志。

8 单击“保存”。

测试配置

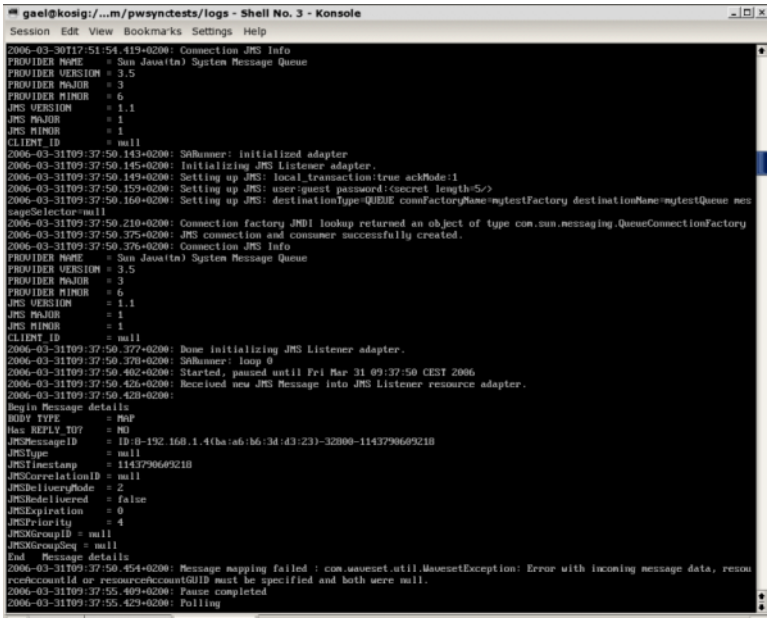
您可以使用 Windows PasswordSync 配置应用程序来调试 Windows 端的配置。

1. **如果尚未运行 PasswordSync 配置应用程序，请启动该应用程序。**
   默认情况下，此配置应用程序安装在 "Program Files" → "Sun Java System Identity Manager PasswordSync" → "Configuration" 中。
2. **在显示“PasswordSync 配置”对话框时，单击“测试”按钮。**
3. **如果使用的是 JMS，将显示“测试连接”对话框，并出现一则消息，指出是否已成功完成测试连接。**



4. 单击“关闭”关闭“测试连接”对话框。
5. 单击“确定”以关闭“PasswordSync 配置”对话框。

之后，JMS 侦听器适配器将在调试模式下运行，并生成包含调试信息的文件（类似于下图中的文件）。



在 Windows 上调试 PasswordSync

PasswordSync 将所有故障写入 Windows 事件查看器。（有关使用事件查看器的帮助，请参见 Windows 帮助。）错误日志条目的源名称是 *PasswordSync*。

有关在 Windows 上排除 PasswordSync 故障的信息，请参见《Sun Identity Manager 8.1 System Administrator's Guide》。

在 Windows 上卸载 PasswordSync

要卸载 PasswordSync 应用程序，请转到 Windows 的"控制面板"并选择"添加或删除程序"。然后选择 "Sun Java System Identity Manager PasswordSync" 并单击"删除"。

注 – 通过加载 Identity Manager 安装介质并单击 `pwsync\IdmPwSync.msi` 图标也可以卸载（或重新安装）PasswordSync。

必须重新启动系统才能完成该过程。

有关 PasswordSync 的常见问题

本节解答了有关 PasswordSync 的一些常见问题。

问题: 在不使用 Java Messaging Service 的情况下能否实现 PasswordSync?

回答: 可以，但这样做会牺牲使用 JMS 跟踪密码更改事件的好处。

要在不使用 JMS 的情况下实现 PasswordSync，请使用以下标志启动配置应用程序：

```
Configure.exe -direct
```

指定 `-direct` 标志后，配置应用程序将显示“用户”选项卡。

如果在不使用 JMS 的情况下实现 PasswordSync，则不必创建 JMS 侦听器适配器。因此，应忽略第 332 页中的 “在应用服务器上部署 PasswordSync”中列出的过程。如果要设置通知，您可能需要改变“更改用户密码”工作流。

注 – 如果您随后运行配置应用程序而不指定 `-direct` 标志，则必须配置 JMS 才能实现 PasswordSync。请使用 `-direct` 标志重新启动应用程序，以便再次绕过 JMS。

问题: PasswordSync 是否可以与用于强制执行自定义密码策略的其他 Windows 密码过滤器一起使用?

回答: 是，可以将 PasswordSync 与其他 `_WINDOWS_` 密码过滤器一起使用。然而，必须是通知软件包注册表值中列出的最后一个密码过滤器。

必须使用以下注册表路径：

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages (value of type REG_MULTI_SZ)
```

默认情况下，安装程序将 Identity Manager 密码拦截设置在列表末尾处。但是，如果您在安装该软件后安装了自定义密码过滤器，则需要将 `lhpwic` 移到通知软件包列表的结尾处。

可以将 PasswordSync 与其他 Identity Manager 密码策略一起使用。如果在 Identity Manager 服务器端选择了策略，必须传递所有资源密码策略以将密码同步推出至其他资源。因此，您应该使 Windows 本机密码策略的严格程度与 Identity Manager 中定义的最严格的密码策略相同。

注 – 密码拦截 DLL 并不强制执行任何密码策略。

问题: 是否可以将 PasswordSync Servlet 安装在 Identity Manager 以外的其他应用服务器上?

回答: 是。除了 JMS 应用程序需要的任何 `jar` 文件以外，PasswordSync Servlet 还需要 `spml.jar` 和 `idmcommon.jar` `jar` 文件。

问题: PasswordSync 服务是否将密码以明文发送到 `lh` 服务器?

回答: 虽然最佳做法是通过 SSL 运行 PasswordSync，但在将所有敏感数据发送到 Identity Manager 服务器之前将对其进行加密。

有关信息，请参见第 321 页中的 “将 PasswordSync 配置为使用 SSL”。

问题: 为什么进行某些密码更改会导致 `com.waveset.exception.ItemNotLocked`?

回答: 如果启用 PasswordSync，密码更改（即使从用户界面启动）将导致资源的密码更改，从而致使资源与 Identity Manager 进行通信。

如果正确配置了 `passwordSyncThreshold` 工作流变量，则 Identity Manager 将检查用户对象并确定该用户对象是否已经处理了密码更改。但是，如果用户或管理员同时对同一个用户进行了其他密码更改，则用户对象将被锁定。

◆ ◆ ◆ 第 12 章

12 安全

本章介绍有关 Identity Manager 安全功能的信息，并详述为进一步减少安全风险可以采取的步骤。

查看以下主题以了解更多有关使用 Identity Manager 管理系统安全的信息。

安全功能

Identity Manager 通过提供以下功能帮助减少安全风险：

- **即时禁用帐户访问**。Identity Manager 使您能够通过单个操作禁用组织或个人的访问权限。
- **登录会话限制**。您可以对并发登录会话设置限制。
- **活动风险分析**。Identity Manager 经常扫描以查看是否存在安全风险，例如非活动帐户和可疑的密码活动。
- **综合的密码管理**。完整灵活的密码管理权能可以确保对访问进行全面控制。
- **对监控访问活动进行审计并报告**。可以运行全面报告，以传送关于访问活动的有针对性的信息。（有关报告功能的详细信息，请参见第 8 章，报告。）
- **细化管理权限控制**。您可以通过向用户分配单个权能或分配一系列通过管理员角色定义的管理职责，在 Identity Manager 中对管理控制进行授权及管理。

- **服务器密钥加密**。Identity Manager 允许通过“任务”区域创建并管理服务器加密密钥。

另外，系统体系结构将尽可能寻求减少安全风险的方法。例如，注销后，就不能通过浏览器的**后退**功能访问先前访问过的页面。

限制并发登录会话

默认情况下，Identity Manager 用户可以使用并发登录会话。不过，可通过打开以修改系统配置对象（第 102 页中的 “编辑 Identity Manager 配置对象”）并编辑 `security.authn.singleLoginSessionPerApp` 配置属性值，将并发会话限制为每个登录应用程序一个会话。此属性是包含每个登录应用程序名称（例如，管理员界面、用户界面或 Identity Manager IDE）的一个属性的对象。将该属性的值更改为 `true` 可为每个用户强制执行单个登录会话。

如果强制执行，则一个用户可以登录到多个会话；但是，只有最后登录的会话保持活动状态且有效。如果用户在无效会话上执行操作，则该用户将被强制退出会话且该会话也将终止。

管理密码

Identity Manager 在多个级别提供密码管理功能：

- **管理更改管理**
  - 从多个位置（“编辑用户”、“查找用户”或“更改密码”页）更改用户的密码
  - 利用细化资源选项更改某个用户在任一资源上的密码
- **管理密码重设**
  - 生成随机密码
  - 向最终用户或管理员显示密码
- **用户更改密码**
  - 向最终用户提供密码更改的自服务，网址为

    http://*localhost*:8080/idm/user
  - 可自定义自服务页面，以符合最终用户的环境（可选）
- **用户更新数据**

  设置要由最终用户管理的任何用户模式属性
- **用户访问恢复**
  - 利用验证回答授予用户更改其密码的访问权限
  - 利用传递验证授权用户使用若干密码中的一个进行访问
- **密码策略**

使用规则定义密码参数

传递验证

利用传递验证向用户和管理员授予通过一个或多个不同密码进行访问的权限。

Identity Manager 通过实现以下方法来管理验证：

- **登录应用程序**（登录模块组的集合）
- **登录模块组**（登录模块的有序集）
- **登录模块**（针对每个已分配的资源设置验证，并指定验证的多个成功登录条件之一）

关于登录应用程序

登录应用程序定义登录模块组的集合，登录模块组进一步定义用户登录 Identity Manager 时使用的登录模块的集合和顺序。每个登录应用程序都由一个或多个登录模块组构成。

登录时，登录应用程序会检查其登录模块组集。如果只设置了一个登录模块组，则会使用这个组，并按组中登录模块的定义顺序处理包含的登录模块。如果登录应用程序中含有多个定义的登录模块组，则 Identity Manager 将检查应用于每个登录模块组的**登录约束规则**以确定要处理的组。

登录约束规则

可以将登录约束规则应用于登录模块组。对于登录应用程序中的每个登录模块组集，如果只有一个组，则不能应用登录约束规则。

当确定要处理一个集合中的哪一个登录模块组时，Identity Manager 评估第一个登录模块组的约束规则。如果成功，则会处理该登录模块组。如果失败，则将依次评估每个登录模块组，直到约束规则成功或评估没有约束规则的登录模块组（随即使用该组）。

注 – 如果登录应用程序包含多个登录模块组，则应将没有登录约束规则的登录模块组放在集合的最后位置。

登录约束规则示例

下例是基于位置的登录约束规则，此规则从 HTTP 标头获取请求者的 IP 地址，然后检查该地址是否位于 192.168 网络。如果 IP 地址中有 192.168.，则此规则将返回值 True 并选择此登录模块组。

示例 12–1 基于位置的登录约束规则

```
<Rule authType='LoginConstraintRule' name='Sample On Local Network'>
<match> <ref>remoteAddr</ref> <s>192.168.</s> </match>
<MemberObjectGroups> <ObjectRef type='ObjectGroup' name='All'/> </MemberObjectGroups>
</Rule>
```

编辑登录应用程序

从菜单栏中选择“安全性”→“登录”以访问“登录”页。

登录应用程序列表显示：

- 定义的每个 Identity Manager 登录应用程序（界面）
- 构成登录应用程序的登录模块组
- 每个登录应用程序的 Identity Manager 会话超时限制设置

在 "Login" 页中，您可以：

- 创建自定义登录应用程序
- 删除自定义登录应用程序
- 管理登录模块组

要编辑登录应用程序，请从列表中选择相应的应用程序。

设置 Identity Manager 会话限制

在“修改登录应用程序”页中，可以为每个 Identity Manager 登录会话设置超时值（限制）。选择小时、分钟和秒数，然后单击“保存”。您建立的限制将显示在登录应用程序列表中。

可以为每个 Identity Manager 登录应用程序设置会话超时。用户登录到 Identity Manager 应用程序之后，将使用当前配置的会话超时值计算用户会话将来因不活动而超时的日期和时间。然后将计算出来的日期与用户的 Identity Manager 会话一起存储，以便在每次提出请求时可以检查此日期。

如果登录管理员更改了登录应用程序会话超时值，则该值会在将来的所有登录中生效。现有会话的超时时间将取决于用户登录时的有效值。

为 HTTP 超时所设置的值将影响所有 Identity Manager 应用程序，并优先于登录应用程序会话超时值。

禁用对应用程序的访问

在“创建登录应用程序”和“修改登录应用程序”页中，可以选择“禁用”选项以禁用登录应用程序，从而禁止用户进行登录。如果用户尝试登录到已禁用的应用程序，则会将该用户重定向到备用页面，并指出当前禁用了该应用程序。可以通过编辑自定义目录来编辑显示在此页面上的消息。

只有取消选择该选项才能解除对登录应用程序的禁用。由于存在安全保护，您不能禁用管理员登录。

编辑登录模块组

登录模块组列表显示：

- 每个登录模块组
- 构成登录模块组的各个登录模块
- 登录模块组是否包含约束规则

在 "Login Module Groups" 页中可以创建、编辑和删除登录模块组。从列表中选择一个登录模块组以进行编辑。

编辑登录模块

针对登录模块的以下各个选项输入详细信息或进行选择。（并非所有选项对每个登录模块均可用。）

- **登录成功要求**。选择应用于此模块的要求。选项包括：
  - **必需**。要求登录模块必须成功。无论验证成功或失败，都将继续验证列表中的下一个登录模块。如果这是唯一的登录模块，则管理员登录成功。
  - **必备**。要求登录模块必须成功。如果验证成功，将继续验证列表中的下一个登录模块。如果验证失败，则验证不再继续进行。
  - **足够**。不要求登录模块必须成功。如果验证成功，将不再继续验证列表中的下一个登录模块，并且管理员成功登录。如果验证失败，将继续验证列表中的下一个登录模块。
  - **可选**。不要求登录模块必须成功。无论验证成功或失败，都将继续验证列表中的下一个登录模块。
- **登录搜索属性**。（仅限 LDAP。）指定尝试绑定（登录）到关联 LDAP 服务器时要使用的 LDAP 用户属性名称的有序列表。按顺序使用每个指定的 LDAP 用户属性以及用户的指定登录名称，搜索匹配的 LDAP 用户。这将允许用户使用 LDAP cn 或电子邮件地址登录到 Identity Manager（将 Identity Manager 配置为传递到 LDAP 时）。

  例如，如果指定以下内容并且用户尝试以 `gwilson` 身份登录，则 LDAP 资源首先尝试查找 `cn=gwilson` 的 LDAP 用户。

  ```
  cn
  mail
  ```

  如果成功，则使用该用户指定的密码尝试绑定。如果不成功，则 LDAP 资源将搜索 `mail=gwilson` 的 LDAP 用户。如果仍失败，则登录失败。

  如果不指定值，则默认 LDAP 搜索属性是：

```
uid

cn
```

- **登录关联规则**。选择用于将用户提供的登录信息映射到 Identity Manager 用户的登录关联规则。此规则用于搜索 Identity Manager 用户（使用规则中指定的逻辑）。此规则必须返回包含一个或多个 `AttributeCondition` 的列表，用于搜索匹配的 Identity Manager 用户。所选规则必须具有 `LoginCorrelationRule` authType。有关 Identity Manager 将验证的用户 ID 映射到 Identity Manager 用户所需的步骤的说明，请参见示例 12–2。
- **新建用户名称规则**。作为登录的一部分，选择自动创建新的 Identity Manager 用户时使用的新用户名称规则。

单击“保存”可以保存登录模块。保存后，可将该模块放在登录模块组中所有其他模块所在的位置。

注意 – 如果将 Identity Manager 登录配置为对多个系统进行验证，则 Identity Manager 要验证的所有目标系统的帐户都应使用相同的用户 ID 和密码。

如果用户 ID 和密码组合不同，则对于用户 ID 和密码不同于在 Identity Manager 的“用户表单”表单中输入的用户 ID 和密码的系统，将不能成功登录。

某些此类系统可能使用锁定策略强制限定锁定帐户前失败登录尝试的次数。对于这些系统，虽然用户可通过 Identity Manager 继续成功登录，但用户帐户最终将被锁定。

示例 12–2 中包含一些伪代码，用于描述 Identity Manager 将验证的用户 ID 映射到 Identity Manager 用户所需的步骤。

示例 12–2 登录模块处理逻辑

```
if an existing IDM user's ID is the same as the specified user ID

   if that IDM user has a linked resource whose resource name matches the
   resource that was authenticated and whose accountId matches the resource
   accountId returned by successful authentication (e.g. dn), then we have
   found the right IDM user

   otherwise if there is a LoginCorrelationRule associated with the
   configured login module

      evaluate it to see if it maps the login credentials to a single IDM
      user

      otherwise login fails

   otherwise login fails
```

示例 12–2 登录模块处理逻辑 （续）

```
if the specified userID does not match an existing IDM user's ID

   try to find an IDM user that has a linked resource whose resource
   name matches the resource accountID returned by successful authentication

     if found, then we have found the right IDM user

     otherwise if there is a LoginCorrelationRule associated with the
     configured login module

         evaluate it to see if it maps the login credentials to a single
         IDM user

         otherwise login fails

     otherwise login fails
```

在示例 12–2 中，系统将尝试使用用户的链接资源（资源信息）查找匹配的 Identity Manager 用户。如果资源信息方法失败，但配置了 loginCorrelationRule，则系统将尝试使用 loginCorrelationRule 查找匹配的用户。

配置公共资源的验证

如果多个资源在逻辑上是相同的（例如，共享某种信任关系的多个 Active Directory 域服务器），或者多个资源均位于同一物理主机上，则可以将这些资源指定为**公共资源**。

您应该声明公共资源，以使 Identity Manager 知道只应尝试并对一组资源验证一次。否则，如果用户键入错误的密码，Identity Manager 将针对每个资源尝试相同的密码。这可能会由于多次登录失败而导致将用户帐户锁定，即便用户仅键入了一次错误密码。

通过使用公共资源，用户可以对一个公共资源进行验证，并且 Identity Manager 将自动尝试并将用户映射到公共资源组中的其余资源。例如，可以将 Identity Manager 用户帐户链接到资源 AD-1 的资源帐户上。不过，登录模块组可能会定义用户必须通过资源 AD-2 的验证。

如果将 AD-1 和 AD-2 定义为公共资源（在这种情况下，位于同一个信任域中），则当用户成功通过 AD-2 的验证时，Identity Manager 也可以通过在资源 AD-1 上查找相同的用户帐户 ID 将用户映射到 AD-1。

注意 – 公共资源组中列出的所有资源也必须包含在登录模块定义中。如果公共资源的完整列表没有同时出现在登录模块定义中，则公共资源功能将无法正常工作。

可以使用以下格式在系统配置对象（第 102 页中的 “编辑 Identity Manager 配置对象”）中定义公共资源。

示例 12–3 配置公共资源的验证

```
<Attribute name='common resources'>
<Attribute name='Common Resource Group Name'>
<List>
<String>Common Resource Name</String>
<String>Common Resource Name</String>
</List
</Attribute> </Attribute>
```

配置 X509 证书验证

可以使用以下信息和过程配置 Identity Manager 的 X509 证书验证。

配置必备条件

要在 Identity Manager 中支持基于 X509 证书的验证，请确保正确配置双向（客户机和服务器）SSL 验证。从客户角度而言，这表明支持 X509 标准的用户证书应已导入到浏览器（或可通过智能卡读卡机获得），用于签署用户证书的信任证书应已导入到信任证书的 Web 应用服务器密钥库中。

还必须为客户机验证启用所用的客户机证书。

▼ 确保选择了客户机证书的“客户机验证”选项

1. **使用 Internet Explorer，选择“工具”，然后选择“Internet 选项”。**
2. **选择“内容”选项卡。**
3. **在“证书”区域中，单击“证书”。**
4. **选择客户机证书，然后单击“高级”。**
5. **在 "Certificate Purposes" 区域中，确保选择 "Client Authentication" 选项。**

在 Identity Manager 中配置 X509 证书验证

▼ 配置 X509 证书验证

1 以 "Configurator"（或同等权限）身份登录 "Administrator Interface"。

2 选择“配置”，然后选择“登录”以显示“登录”页。

3 单击“管理登录模块组”以显示“登录模块组”页。

4 从列表中选择登录模块组。

5 从“分配登录模块”列表中选择“Identity Manager X509 证书登录模块”。Identity Manager 将显示“修改登录模块”页。

6 设置成功登录的要求。

可以接受以下值：

- **必需**。要求登录模块必须成功。无论验证成功或失败，都将继续验证列表中的下一个登录模块。如果这是唯一的登录模块，则管理员登录成功。
- **必备**。要求登录模块必须成功。如果验证成功，将继续验证列表中的下一个登录模块。如果验证失败，则验证不再继续进行。
- **足够**。不要求登录模块必须成功。如果验证成功，将不再继续验证列表中的下一个登录模块，并且管理员成功登录。如果验证失败，将继续验证列表中的下一个登录模块。
- **可选**。不要求登录模块必须成功。无论验证成功或失败，都将继续验证列表中的下一个登录模块。

7 选择登录关联规则。这可以是内置规则或自定义的关联规则。（有关创建自定义关联规则的信息，参见下节。）

8 单击“保存”，返回到“修改登录模块组”页。

9 或者，可以重新排列登录模块顺序（如果为登录模块组分配了多个登录模块），然后单击“保存”。

10 如果尚未为登录应用程序分配登录模块组，请进行分配。在 "Login Module Groups" 页中单击 "Return to Login Applications"，然后选择登录应用程序。为应用程序分配登录模块组后，单击“保存”。

注 – 如果 `waveset.properties` 文件中的 `allowLoginWithNoPreexistingUser` 选项设置为 `true` 值，则配置 Identity Manager X509 证书登录模块时会提示您选择“新建用户名称规则”。在使用相关**登录关联规则**未找到用户时，可使用此规则确定如何命名新创建的用户。新建用户名称规则与登录关联规则的可用输入参数相同。它返回单个字符串，该字符串是**用于创建新 `Identity Manager` 用户帐户的用户名**。`idm/sample/rules` 中包含一个名为 `NewUserNameRules.xml` 的新建用户名称规则示例。

创建和导入登录关联规则

Identity Manager X509 证书登录模块使用登录关联规则确定如何将证书数据映射到相应的 Identity Manager 用户。Identity Manager 中包含一个名为“通过 X509 证书 SubjectDN 相关联”的内置关联规则。

您也可以添加自己的关联规则。请参阅位于 `idm/sample/rules` 目录中作为示例的 `LoginCorrelationRules.xml`。

每个关联规则都必须遵循以下准则：

- 必须将其 `authType` 属性设置为 `LoginCorrelationRule`。
- 它会返回 `AttributeCondition` 列表实例，登录模块利用该实例查找相关的 Identity Manager 用户。例如，登录关联规则可能返回按电子邮件地址搜索相关 Identity Manager 用户的 `AttributeCondition`。

传递到登录关联规则的参数有：

- 标准 X509 证书字段（如 `subjectDN`、`issuerDN` 和有效日期）
- 重要和非重要扩展属性

传递给登录关联规则的证书参数的命名约定为

```
cert.field name.subfield name
```

可用于规则的示例参数名包括：

- `cert.subjectDN`
- `cert.issuerDN`
- `cert.notValidAfter`
- `cert.notValidBefore`
- `cert.serialNumber`

使用传入参数的登录关联规则将返回一个列表，其中包含一个或多个 `AttributeCondition`。Identity Manager X509 证书登录模块使用它们来查找相关的 Identity Manager 用户。

`idm/sample/rules` 中包含一个名为 `LoginCorrelationRules.xml` 的登录关联规则范例。

创建自定义关联规则后，必须将其导入 Identity Manager。在管理员界面中选择“配置”，然后选择“导入交换文件”以使用文件导入工具。

测试 SSL 连接

要测试 SSL 连接，可使用 SSL 转至已配置的应用程序界面的 URL（例如 `https://idm007:7002/idm/user/login.jsp`）。您会被告知正在进入一个安全站点，然后提示您指定要发送 Web 服务器的个人证书。

诊断问题

通过 X509 证书进行验证的问题应以错误消息形式在登录表单中报告。

要获得更全面的诊断，可在 Identity Manager 服务器中启用对以下各个类和级别的跟踪：

- `com.waveset.session.SessionFactory 1`
- `com.waveset.security.authn.WSX509CertLoginModule 1`
- `com.waveset.security.authn.LoginModule 1`

如果在 HTTP 请求中客户机证书属性没有命名为 `javaxservlet.request.X509Certificate`，则会收到一条消息，说明无法在 HTTP 请求中找到此属性。

▼ 更正 HTTP 请求中的客户机证书属性名称

1. **可启用对 `SessionFactory` 的跟踪，以查看完整的 HTTP 属性列表，并确定 X509 证书的名称。**
2. **使用 Identity Manager 调试工具（第 40 页中的“Identity Manager 的“调试”页”）编辑 `LoginConfig` 对象。**
3. **将 Identity Manager X509 证书登录模块的 `<LoginConfigEntry>` 中的 `<AuthnProperty>` 名称更改为正确的名称。**
4. **保存后重试。**

   也可能需要在登录应用程序中先删除，然后再重新添加 Identity Manager X509 证书登录模块。

加密的使用和管理

加密用于确保内存和系统信息库中的服务器数据以及在 Identity Manager 服务器和网关之间传送的所有数据的机密性和完整性。

以下各节提供了有关如何在 Identity Manager 服务器和网关中使用和管理加密的详细信息，并阐述了有关服务器和网关加密密钥的问题。

受加密保护的数据

下表显示了在 Identity Manager 产品中受加密保护的数据类型，包括用于保护每种类型数据的加密器。

表 12–1 受加密保护的数据类型

数据类型	RSAMD5	NIST Triple DES168 位密钥 (DESede/ECB/NoPadding)	PKCS#5 基于密码的加密 56 位密钥 (PBEwithMD5andDES)
服务器加密密钥		默认	配置选项
网关加密密钥		默认	配置选项1
字典策略词	是		
用户密码		是	
用户密码历史记录		是	
用户答案		是	
资源密码		是	
资源密码历史记录	是		
服务器和网关之间的所有有效负载		是	

有关服务器加密密钥的常见问题

请阅读以下各节，以了解有关服务器加密密钥源、位置、维护和使用的常见问题的答案。

问题: 服务器加密密钥来自哪里?

回答: 服务器加密密钥是对称的 triple-DES 168 位密钥。

服务器支持以下两类密钥：

- **默认密钥**。此密钥已编译为服务器代码。
- **随机生成的密钥**。此密钥可以在服务器初始启动或当前密钥的安全性出问题时生成。

问题: 在哪里维护服务器加密密钥?

回答: 在系统信息库中维护服务器加密密钥。在任一给定系统信息库中都会有许多数据加密密钥。

问题: 服务器如何知道使用哪个密钥对已加密的数据进行解密和重新加密?

回答: 存储于系统信息库中的每一加密数据都以服务器加密密钥（用于加密该数据）的 ID 为前缀。将包含加密数据的对象读入内存后，Identity Manager 使用与加密数据的 ID 前缀相关联的服务器加密密钥进行解密，然后使用相同的密钥重新加密（如果数据已更改）。

问题: 如何更新服务器加密密钥?

回答: Identity Manager 提供了名为“管理服务器加密”的任务。

此任务允许授权的安全管理员执行多项密钥管理任务，包括：

- 生成新的“当前”服务器密钥
- 使用“当前”服务器密钥按类型重新加密包含已加密数据的现有对象

有关如何使用此任务的详细信息，请参见本章中的第 364 页中的 “管理服务器加密”。

问题: 如果更改“当前”服务器密钥，则会对现有加密数据造成什么样的影响?

回答: 没有影响。仍将使用现有加密数据 ID 前缀对应的密钥对现有加密数据进行解密或重新加密。如果生成了新的服务器加密密钥并设置为“当前”密钥，则任何要加密的新数据都将使用该新服务器密钥。

为避免出现多密钥问题，以及为了更好地维护数据的完整性，可以使用“管理服务器加密”任务重新加密所有带有“当前”服务器加密密钥的现有加密数据。

问题: 如果导入的加密数据没有可用的加密密钥，此时会出现什么情况?

回答: 如果导入包含加密数据的对象，但加密该数据所使用的密钥不在要导入该数据的系统信息库中，则仍会导入该数据，但不进行加密。

问题: 怎样保护服务器密钥?

回答: 如果未将服务器配置为使用基于密码的加密 (Password-based Encryption, PBE)（PKCS#5 加密，使用 `pbeEncrypt` 属性或“管理服务器加密”任务在系统配置对象中设置），则使用默认密钥对服务器密钥进行加密。对于安装的任何 Identity Manager，设置的默认密钥都是相同的。

如果将服务器配置为使用 PBE 加密，则每次启动服务器时都将生成 PBE 密钥。通过提供一个密码（由特定于服务器的秘密生成）作为 PBEwithMD5andDES 加密器来生成

PBE 密钥。PBE 密钥仅在内存中维护并从不具有持久性。另外，PBE 密钥对于共享一个公共系统信息库的所有服务器都是相同的。

要启用服务器密钥的 PBE 加密，加密器 PBEwithMD5andDES 必须可用。默认情况下，Identity Manager 不包括此加密器，但此加密器采用 PKCS#5 标准，许多 JCE 提供者实现（例如由 Sun 和 IBM 提供的实现）中都提供了该标准。

问题: 我可以导出服务器密钥以安全地存储在外部吗?

回答: 是。如果服务器密钥是 PBE 加密，则在导出之前，将使用默认密钥对这些密钥进行解密和重新加密。这使得它们可以独立于本地服务器 PBE 密钥而稍后被导入同一或其他服务器中。如果使用默认密钥对服务器密钥进行加密，则在导出之前不需要进行任何事先的处理。

将密钥导入服务器后，如果该服务器配置为 PBE 密钥，则将解密这些密钥。然后，如果该服务器配置为 PBE 密钥加密，则使用本地服务器的 PBE 密钥重新加密这些密钥。

问题: 将对服务器和网关之间的哪些数据进行加密?

回答: 在服务器和网关之间传送的所有数据（有效负载）都由针对每个服务器-网关会话随机生成的对称 168 位密钥进行 triple-DES 加密。

有关网关密钥的常见问题

请阅读以下各节，以了解有关网关源、存储、分发和保护的常见问题的答案。

问题: 加密或解密数据的网关密钥来自哪里?

回答: 每次 Identity Manager 服务器连接到网关时，初始握手都将生成一个新的随机 168 位 triple-DES 会话密钥。此密钥将用于加密或解密随后在服务器和网关之间传送的所有数据。对于每个服务器/网关对，生成的会话密钥都是唯一的。

问题: 如何将网关密钥分发到网关?

回答: 会话密钥由服务器随机生成，然后在服务器和网关之间安全地进行交换，方法是使用作为服务器到网关初始握手的一部分的共享机密主密钥对会话密钥进行加密。

在初始握手期间，服务器会查询网关来确定网关支持的模式。网关可以以两种模式操作

- **默认模式**。服务器到网关的初始协议握手使用编译为服务器代码的默认 168 位 triple-DES 密钥加密。
- **安全模式**。生成针对每个共享系统信息库的随机 168 位密钥 triple-DES 网关密钥，并作为初始握手协议的一部分在服务器和网关之间进行通信。此网关密钥与其他加密密钥一样存储于服务器系统信息库中，并存储在网关的本地注册表中。

  当服务器在安全模式下联系网关时，服务器将使用网关密钥加密测试数据并将其发送到网关。然后，网关将尝试解密测试数据，并将一些网关特有数据添加到测试数据中，接着重新加密这些数据并将其发送回服务器。如果服务器可以成功解密测试数据和网关特有数据，则服务器将生成服务器-网关会话唯一密钥，并使用网关密钥

对其进行加密，然后将其发送到网关。收到之后，网关将解密会话密钥并保留该密钥，以供在服务器到网关会话中使用。如果服务器无法成功解密测试数据和网关特有数据，则服务器将使用默认密钥加密网关密钥并将其发送到网关。网关将使用默认密钥中已编译好的网关密钥来解密网关密钥，并将该网关密钥存储于网关的注册表中。然后，服务器将使用网关密钥对服务器-网关会话唯一密钥进行加密，并将其发送到网关以供在服务器到网关会话中使用。

之后，网关将仅接受已使用网关密钥加密了会话密钥的服务器请求。启动时，网关将检查注册表中的密钥。如果密钥存在，网关将使用该密钥。如果密钥不存在，则网关将使用默认密钥。一旦网关在注册表中设置了密钥，网关将不再允许使用默认密钥建立会话，这将阻止某些人设置流氓服务器并建立到网关的连接。

问题: 我可以更新网关密钥（用于加密或解密服务器到网关有效负载）吗?

回答: Identity Manager 提供了名为“管理服务器加密”的任务，它允许授权的安全管理员执行多项密钥管理任务，包括生成新的“当前”网关密钥并使用该“当前”网关密钥更新所有网关。这是用于加密每个会话密钥（用于保护在服务器和网关之间传送的所有有效负载）的密钥。将使用默认密钥或 PBE 密钥对新生成的网关密钥进行加密，具体取决于系统配置（第 102 页中的 “编辑 Identity Manager 配置对象”）中 `pbeEncrypt` 属性的值。

问题: 在服务器、网关的什么地方存储网关密钥?

回答: 在服务器上，网关密钥就像服务器密钥一样存储在系统信息库中。在网关上，网关密钥存储于本地注册表主键中。

问题: 怎样保护网关密钥?

回答: 保护网关密钥的方式与保护服务器密钥相同。如果将服务器配置为使用 PBE 加密，则网关密钥将使用 PBE 生成的密钥进行加密。如果该选项为 False，则将使用默认密钥加密。有关详细信息，请参见第 360 页中的 “有关服务器加密密钥的常见问题”。

问题: 我可以导出网关密钥以安全地存储在外部吗?

回答: 可以通过“管理服务器加密”任务导出网关密钥，就像导出服务器密钥一样。有关详细信息，请参见第 360 页中的 “有关服务器加密密钥的常见问题”。

问题: 如何销毁服务器和网关密钥?

回答: 通过从服务器系统信息库中删除服务器和网关密钥就可以销毁它们。请注意，只要仍在使用该密钥加密服务器数据或仍有网关依赖该密钥，就不应该删除该密钥。通过执行 "Manage Server Encryption" 任务，可以使用当前服务器密钥重新加密所有服务器数据，并将当前网关密钥与所有网关同步以确保在删除任何旧密钥之前不再使用旧密钥。

管理服务器加密

通过使用 Identity Manager 服务器加密功能，您可以创建新的 3DES 服务器加密密钥，然后使用 3DES、PKCS#5 或 AES（高级加密标准）加密对这些密钥进行加密。只有具备“安全管理员”权能的用户才可以运行“管理服务器加密”任务（该任务是从“管理服务器加密”页中配置的）。

▼ 访问“管理服务器加密”页

要打开“管理服务器加密”页，请

1. **从菜单栏中选择“服务器任务”>“运行任务”。**
2. **在显示“可用任务”页时，单击“管理服务器加密”以打开“管理服务器加密”页。**

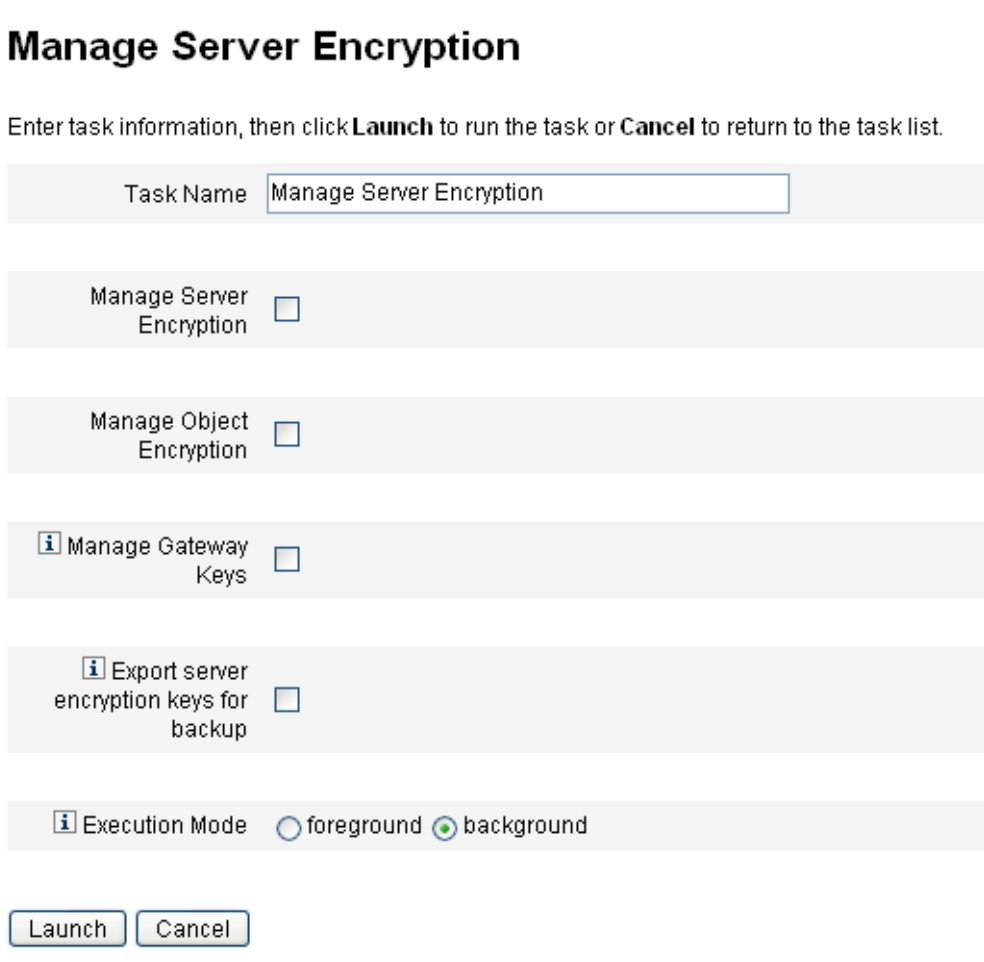


图 12–1 “管理服务器加密”页

▼ 配置服务器加密

可以使用该页配置服务器和对象加密、网关密钥、备份选项以及执行模式。

1 **输入一个任务名称。**

此字段默认为**管理服务器加密**。如果不想使用默认设置，您可以输入不同的任务名称。

2 **选择下面的一个或多个选项。**

- **管理服务器加密**。选择该选项可配置服务器加密。

将显示下面的附加选项：

- **服务器加密密钥的加密**。您必须指定一种加密服务器加密密钥的方法。加密类型可以包括 Triple DES、PKCS#5 (DES) 或 PKCS#5 (AES)。

注 –

- 该页上仅显示可在您的系统上实例化的加密类型。例如，如果您的系统不支持 PKCS#5 (AES)，则仅显示 Triple DES 和 PKCS#5 (DES)。
- PKCS#5 (AES) 要求您为运行 Identity Manager 的 JVM 下载并配置 "Unlimited Strength Jurisdiction Policy File"。有关详细信息，请参阅 Java 供应商文档。

  另外，PKCS#5 (AES) 还要求您为运行 Identity Manager 的 JVM 安装 `Bouncy Castle JCE provider jar` 文件并将其配置为 JCE 提供者。此 `jar` 文件封装在 Identity Manager 安装映像中，它位于 *wshome*`/WEB-INF/lib` 目录中。提供了两个 `jar` 文件：`bcprov-jdk15-137.jar` 和 `bcprov-jdk16-137.jar`，它们分别用于相应的 Java 版本。有关详细信息，请参阅 Java 供应商文档和 Bouncy Castle 文档。

  - **生成新的服务器加密密钥，并设置为当前的服务器加密密钥**。选择此选项可生成新的服务器加密密钥。选择此选项之后生成的每一份加密数据都是使用此密钥进行加密。生成新的服务器加密密钥不会影响应用于已存在的加密数据的密钥。
  - **生成新的安全随机 PBE 密码**。选择此选项可在每次启动服务器时基于服务器特定的秘密生成新密码。如果未选择此选项，或者未将服务器配置为使用基于密码的加密，Identity Manager 将使用默认密钥加密服务器密钥。
- **管理对象加密**。选择此选项可指定应重新加密的对象类型以及要使用的加密方法。
  - **对象类型的加密**。选择显示的加密类型之一，其中可能包括 Triple DES（默认）、AES 256 位密钥、AES 192 位密钥或 AES 128 位密钥。

注 – 使用 192 或 256 位密钥的 AES 要求您为运行 Identity Manager 的 JVM 下载并配置 "Unlimited Strength Jurisdiction Policy File"。有关详细信息，请参阅 Java 供应商文档。

该页上仅显示可在您的系统上实例化的加密类型。例如，如果您的系统不支持使用 "Unlimited Strength Jurisdiction Policy File" 的 AES 192 或 256 位密钥，则仅显示 Triple DES 和 AES 128 位密钥选项。

  - **选择要使用当前服务器加密密钥重新加密的对象类型**。选择表中列出的一种或多种 Identity Manager 对象类型。
- **管理网关密钥**。选择此选项可指定网关加密。

将显示以下选项：

- **选择网关密钥选项**。请选择以下任一选项：
  - **生成新密钥并同步所有网关**。最初启用安全网关环境时选择此选项。此选项生成一个新的网关密钥并将其传送至所有网关。
  - **使用当前网关密钥同步所有网关**。选择此选项可同步任何新网关，或者同步尚未与新网关密钥通信的网关。若在使用当前网关密钥将所有网关同步时有一个网关关闭，或要为新网关强制执行密钥更新，请选择此选项。
- **网关密钥类型**。选择显示的密钥类型之一，其中可能包括 Triple DES、AES 256 位密钥、AES 192 位密钥或 AES 128 位密钥。

注 – 使用 192 或 256 位密钥的 AES 要求您为运行 Identity Manager 的 JVM 下载并配置 "Unlimited Strength Jurisdiction Policy File"。有关详细信息，请参阅 Java 供应商文档。

该页上仅显示可在您的系统上实例化的加密类型。例如，如果您的系统不支持使用 "Unlimited Strength Jurisdiction Policy File" 的 AES 192 或 256 位密钥，则仅显示 Triple DES 和 AES 128 位密钥选项。

- **导出服务器加密密钥进行备份**。选择此选项可将现有服务器加密密钥导出为 XML 格式的文件。选择此选项后，Identity Manager 会另显示一个字段以便您指定导出该密钥的路径和文件名。

注 – 如果使用的是 PKCS#5 加密并选择生成和设置新的服务器加密密钥，则选择此选项。而且，您还应将导出的密钥存储在可移动介质上，并存放在安全的位置（请勿放在网络上）。

---

3 选择执行模式。

您可以在前台或后台（默认设置）运行此任务。

注 – 如果您选择使用新生成的密钥重新加密一个或多个对象类型，执行该任务会需要一些时间，且最好在后台运行此任务。

---

4 在此页上配置完选项后，单击“启动”。

使用验证类型保护对象

通常，可以使用在 AdminGroup 权能中指定的权限授予访问 Identity Manager objectType（例如，Configuration、Rule 或 TaskDefinition）的权限。但是，授予访问一个或多个受控组织内的所有 Identity Manager objectType 对象的权限有时仍显得过于宽泛。

通过使用授权类型 (AuthType)，您可以进一步缩小范围，或者将此访问限制为某个给定 Identity Manager objectType 的部分对象。例如，在填充规则以从用户表单中进行选择时，您可能不希望授权用户访问其控制范围内的所有规则。

要定义新的授权类型，请在 Identity Manager 系统信息库中编辑 AuthorizationTypes 配置对象，然后添加一个新的 <AuthType> 元素。

此元素需要两个属性：

- 新授权类型的名称
- 现有授权类型或者新元素扩展或限定的 objectType

例如，如果要添加一个新 Rule 授权类型 Marketing Rule 以扩展 Rule，您应该定义以下内容：

```
<AuthType name='Marketing Rule' extends='Rule'/>
```

然后，要启用将使用的授权类型，您必须在两个位置中引用该授权类型。

- 在为新授权类型授予一个或多个权限的自定义 AdminGroup 权能中
- 在应属于该类型的对象中

下面是这两种引用的示例。第一个示例说明了授予访问 Marketing Rules 的权限的 AdminGroup 权能定义。

示例 12–4 AdminGroup 权能定义

```
<AdminGroup name='Marketing Admin'>
  <Permissions>
    <Permission type='Marketing Rule' rights='View,List,Connect,Disconnect/>
  </Permissions>
  <AdminGroups>
    <ObjectRef type='AdminGroup' id='#ID#Account Administrator'/>
  </AdminGroups>
</AdminGroup>
```

第二个示例说明了允许用户访问对象的 Rule 定义，因为已为这些用户授予了访问 Rule 或 Marketing Rule 的权限。

示例 12–5 Rule 定义

```
<Rule name='Competitive Analysis Info' authType='Marketing Rule'>
 ...
</Rule>
```

注 – 任何用户只要被授予父授权类型或某种授权类型扩展的静态类型的权限，则对于所有子授权类型就将具有相同的权限。因此，使用上面的示例，被授予 `Rule` 的权限的任何用户对于 `Marketing Rule` 也将具有相同的权限。但是，反过来并不成立。

安全实践

作为 Identity Manager 管理员，可以通过在安装时和安装后遵照以下建议进一步减少受保护帐户和数据的安全风险。

安装时

在安装期间减少安全风险：

- 通过使用 HTTPS 的安全 Web 服务器访问 Identity Manager。
- 重设默认 Identity Manager 管理员帐户（管理员和配置器）的密码。要进一步保护这些帐户的安全，可将其重命名。
- 限制对 "Configurator" 帐户的访问。
- 将管理员的权能集限制为仅是他们的工作职责所需的那些操作，并且通过设置组织分层结构限制管理员权能。
- 更改 Identity Manager 索引信息库的默认密码。
- 启用审计功能，以跟踪 Identity Manager 应用程序中的活动。
- 编辑 Identity Manager 目录中的文件的权限。
- 自定义工作流以插入批准或其他检查点。
- 开发恢复过程，以描述如何在出现紧急情况时恢复 Identity Manager 环境。

使用时

在使用期间减少安全风险：

- 定期更改默认 Identity Manager 管理员帐户（管理员和配置器）的密码。
- 如果当前没有使用 Identity Manager，请注销该系统。

- 设置或了解 Identity Manager 会话的默认超时时间段。会话超时值可能不同，因为可以为每个登录应用程序单独设置这些值。

如果您的应用服务器是 Servlet 2.2 兼容的服务器，则 Identity Manager 安装进程会将 HTTP 会话超时设置为默认值 30 分钟。通过编辑属性可以更改此值；但是，应将此值设置得更小，以提高安全性。不要将此值设置为高于 30 分钟。

▼ 要更改会话超时值

1. **编辑 `web.xml` 文件，该文件位于应用服务器目录树中的 `idm/WEB-INF` 目录中。**
2. **更改下列各行中的数字值：**

```
<session-config>  <session-timeout>30</session-timeout></session-config>
```

◆ ◆ ◆ 第 13 章

13 身份审计：基本概念

本章介绍了身份审计和审计控制背后的概念。审计控制可用于监控和管理企业信息系统和应用程序中的审计和遵循性。

在本章中，您可以了解以下概念和任务：

关于身份审计

Identity Manager 将**审计**定义为对企业范围内身份数据的系统捕获、分析和响应，以确保遵循内部和外部的策略与法规。

遵循会计和数据隐私法案并不是一项简单的任务。Identity Manager 的审计功能提供了一种灵活的方法，可让您实现适用于企业的遵循性解决方案。

在大多数环境下，会有不同的组涉及到遵循性：内部和外部审计小组（视审计为主要任务）；非审计人员（可能将审计视为非正式任务）。IT 通常也与遵循性有关，这有助于将内部审计小组的要求付诸于选定解决方案的实现。成功实现审计解决方案的关键在于准确地捕获非审计人员的知识、控制和过程，然后自动应用这些信息。

身份审计的目标

身份审计提高了审计性能，如下所示：

- **身份审计自动检测遵循性违规，便于通过即时通知进行快速修正**

  利用 Identity Manager 审计策略功能，可以定义违规的**规则**（即，条件）。定义完成后，系统会扫描是否存在违反既定策略的情况（例如，未授权的访问更改或错误的访问权限）。检测时，系统会根据已定义的提升链通知相应的人员。然后，用户调用的任务或者由策略违规自动调用的工作流可以修正（更正）违规。

- **按需提供有关内部审计控制有效性的关键信息**

  Auditor 报告提供有关违规和异常的摘要状态信息，以便快速分析风险状态。“报告”选项卡还提供违规的图形报告。您可以按资源、组织或策略查看违规，并根据您定义的报告特征自定义每个图表。

- **身份证书查看的自动化控制可降低操作风险**

  利用工作流权能可将策略和访问违规自动通知给选定的查看者。

- **准备详述用户活动和符合调整要求的综合报告**

  使用“报告”区域可定义详细的报告和图表，其中提供有关访问历史和权限以及其他策略违规的信息。系统会通过报告权能保留可在其中进行搜索的安全和综合的身份审计跟踪，以访问数据，更新用户概要文件。

- **简化周期性查看的过程以维护安全性和对法规的遵循性**

  执行周期性访问查看可收集用户权利记录，并确定哪些权利需要查看。然后，该进程会向指定的证明者通知要查看的暂挂请求，并在证明者完成对这些请求所执行的操作后更新状态或暂挂请求。

- **标识用户帐户的潜在利益冲突权能**

  Identity Manager 提供了任务划分报告，可标识具有特定权能或权限（可能导致利益冲突）的用户。

了解身份审计

Identity Manager 提供了一项用于审计用户帐户权限和访问权限的功能，还提供了另一项用于维护和证明遵循性的功能。这些功能是基于策略的遵循性和周期性访问查看。

基于策略的遵循性

对于公司针对所有用户帐户建立的要求，Identity Manager 通过审计策略系统使管理员能够维护对这些要求的遵循性。

可以使用审计策略通过两种不同却互补的方法来确保遵循性：连续遵循性和周期性遵循性。

对于置备操作可能在 Identity Manager 外部执行的环境，这两种技术更具互补性。如果帐户可能被不执行或不遵循现有审计策略的进程所更改，则需要周期性遵循性。

连续遵循性

连续遵循性表示审计策略将应用于所有置备操作，因此不能使用不符合当前策略的方法修改帐户。

可以通过将审计策略分配给组织和/或用户来启用连续遵循性。对用户执行的任何置备操作都将导致对分配给用户的策略进行评估。如果评估产生了任何策略失败，都会中断置备操作。

基于组织的策略集是分层定义的。任何用户都只有一个有效的组织策略集。所应用的策略集是分配给最低级别组织的策略集。例如：

组织	直接分配的策略集	有效的策略
Austin	策略 A1、A2	策略 A1、A2
销售		策略 A1、A2
开发	策略 B、C2	策略 B、C2
支持		策略 B、C2
测试	策略 D、E5	策略 D、E5
财务		策略 A1、A2
Houston		<无>

周期性遵循性

周期性遵循性表示 Identity Manager 将根据需要评估策略。任何不符合的情况均会被捕获为遵循性违规。

执行周期性遵循性扫描时，您可以选择要在扫描中使用的策略。扫描过程混合了直接分配的策略（分配给用户的策略和分配给组织的策略）和任意一组选定的策略。

具有“审计者管理员”权能的 Identity Manager 用户可以创建审计策略，并通过定期执行策略扫描和查看策略违规来监视对这些策略的遵循性。可以通过修正和缓解过程管理违规。

有关审计者管理员权能的详细信息，请参见第 6 章，管理中的第 184 页中的“了解和管理权能”。

Identity Manager 审计允许常规的用户扫描。这些扫描执行审计策略以检测是否与既定的帐户限制有偏差。一旦检测到违规，便会启动修正活动。这些规则可以是 Identity Manager 提供的标准审计策略规则，也可以是自定义的用户定义规则。

基于策略的遵循性的逻辑任务流

图 13–1 显示了一个用于建立基于策略的审计控制的逻辑任务流。

周期性访问查看

Identity Manager 提供了周期性访问查看功能，使管理员与其他责任方可以临时或定期查看并验证用户访问权限。有关该功能的详细信息，请参见第 412 页中的 “周期性访问查看和证明”。

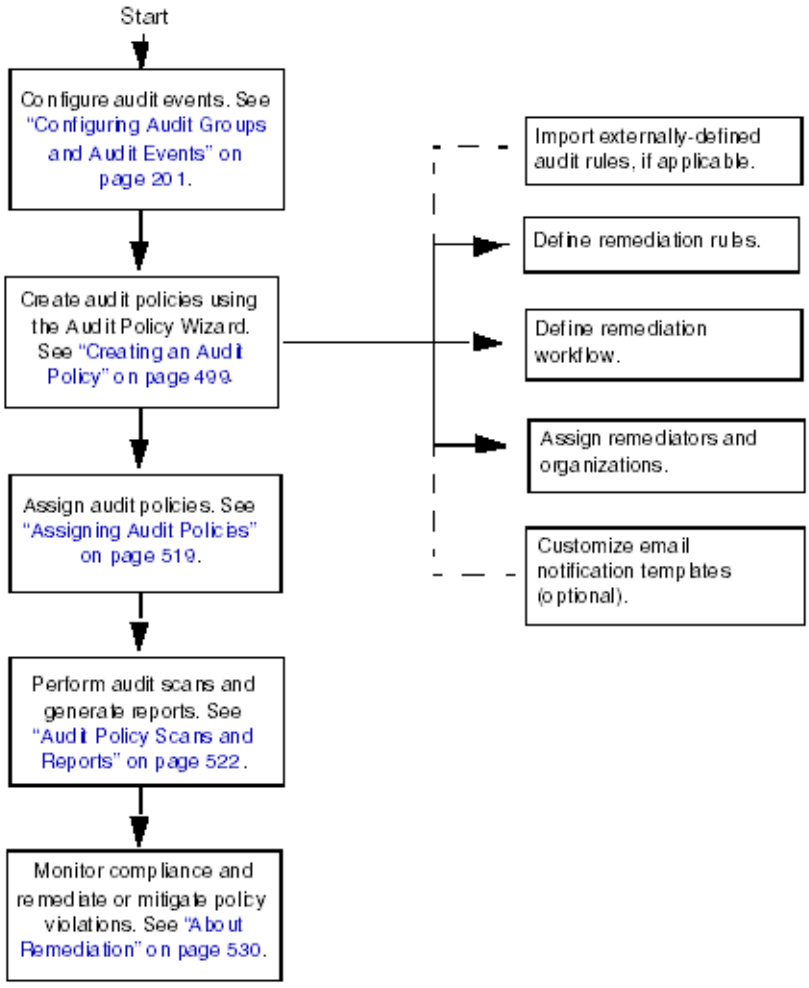


图 13–1 用于建立基于策略的遵循性的逻辑任务流

使用管理员界面中的身份审计

本节介绍了如何使用管理员界面访问身份审计功能。还介绍了身份审计中使用的电子邮件通知模板。

使用界面的“遵循性”部分

要创建和管理审计策略，请使用 Identity Manager 管理员界面的遵循性部分。

▼ 使用“遵循性”部分创建和管理审计策略

1 **登录到管理员界面（第 38 页中的“登录到 Identity Manager 最终用户界面”）。**

2 **在菜单栏中单击“遵循性”。**

“遵循性”部分中包含以下子选项卡（或菜单项）：

- 管理策略
- 管理访问扫描
- 访问查看

管理策略

“管理策略”页列出了您有权查看和编辑的策略。您还可以在该区域中管理访问扫描。

在“管理策略”页中，您可以使用审计策略完成以下任务：

- 创建审计策略
- 选择要查看或编辑的策略
- 删除策略

可以在第 378 页中的 “审计策略方案示例”一节中找到有关这些任务的详细信息。

管理访问扫描

可以使用“管理访问扫描”选项卡来创建、修改和删除访问扫描。可在此处定义要运行或要调度为周期性访问查看的扫描。有关该功能的详细信息，请参见第 412 页中的 “周期性访问查看和证明”。

访问查看

通过使用“访问查看”选项卡，您可以启动、终止、删除和监视访问查看的过程。它将显示扫描结果的摘要报告，并提供一些信息链接，通过这些链接可以访问有关查看状态和暂挂活动的更多详细信息。

有关该功能的更多信息，请参见第 420 页中的 “管理访问查看”。

身份审计任务界面参考

要了解如何使用管理员界面执行其他身份审计任务，请参见表 B–8。此快速参考介绍了应该从哪里启动各种审计任务。

电子邮件模板

身份审计在许多操作中使用电子邮件通知。其中每个通知都会使用一个电子邮件模板对象。电子邮件模板允许对电子邮件消息的标题和正文进行自定义。

表 13–1 身份审计电子邮件模板

模板名称	用途
访问查看修正通知	最初在修正状态下创建用户权利时通过访问查看发送给修正者。
批量证明通知	证明者具有暂挂证明时通过访问查看发送给证明者。
策略违规通知	发生违规时通过审计策略扫描发送给修正者。
访问扫描开始通知	访问查看启动扫描时发送给访问扫描的拥有者。
访问扫描结束通知	访问扫描完成时发送给访问扫描的拥有者。

启用审计日志记录

必须先启用 Identity Manager 审计日志记录系统并将其配置为收集审计事件，您才能开始管理遵循性和访问查看。默认情况下将启用审计系统。具有配置审计权能的 Identity Manager 管理员可以配置审计。

Identity Manager 可提供遵循性管理审计配置组。

可以使用以下步骤查看或修改遵循性管理组存储的事件：

1. **登录到管理员界面**（第 38 页中的“登录到 Identity Manager 最终用户界面”）。
2. **在菜单栏中选择“配置”，然后单击“审计”。**
3. **在“审计配置”页上，选择遵循性管理审计组名称。**

注 –

- 有关设置审计配置组的详细信息，请参见第 96 页中的“配置审计组和审计事件”。
- 有关审计系统如何记录事件的信息，请参见第 10 章，审计日志记录。

关于审计策略

审计策略针对一个或多个资源的一组用户定义了帐户限制。它由定义策略限制的**规则**和发生违规后用于处理违规的**工作流**组成。审计扫描使用审计策略中定义的条件来判断组织中是否发生了违规。

以下组件构成审计策略：

- **策略规则**定义了特定违规。策略规则可以包含使用 XPRESS 语言、XML 对象语言或 JavaScript 语言编写的函数。
- **修正工作流**（可选）在审计扫描发现违反策略规则时启动。
- **修正者**是经授权可对策略违规进行响应的指定用户。修正者可以是单个用户或用户组。

使用审计策略规则创建策略

在审计策略中，规则会根据属性定义可能的冲突。审计策略中可包含引用大范围资源的上百条规则。在规则评估过程中，规则可以访问一个或多个资源中的用户帐户数据。审计策略可以限制哪些资源可供规则使用。

规则可以仅检查单个资源的单个属性，也可以检查多个资源的多个属性。

使用修正工作流解决策略违规问题

创建用于定义策略违规的规则后，可以选择将在审计扫描检测到违规时启动的工作流。Identity Manager 提供默认的“标准修正”工作流，它为审计策略扫描提供默认的修正处理。在其他操作中，此默认修正工作流为给每个指定的级别 1 修正者（如有必要，还可以是后续级别的修正者）生成通知邮件。

注 – 与 Identity Manager 工作流进程不同，必须为修正工作流分配 `AuthType=AuditorAdminTask` 和 `SUBTYPE_REMEDIATION_WORKFLOW` 子类型。如果要导入用于审计扫描的工作流，则必须手动添加此属性。有关详细信息，请参见第 383 页中的“（可选）将任务划分规则导入到 Identity Manager 中”。

指定修正者

如果分配修正工作流，则必须至少指定一个修正者。最多可以为审计策略指定三个级别的修正者。有关修正的详细信息，请参见第 404 页中的“遵循性违规修正和缓解”。

您必须先分配修正工作流，才能分配修正者。

审计策略方案示例

假定您负责处理应付账款和应收帐款，而且必须执行一些手续，以防止责任集中于会计部门雇员的潜在危险。此策略必须确保负责处理应付帐款的人员无需负责处理应收帐款。

该审计策略将包含以下内容：

- 一组规则。每条规则指定一个构成策略违规的条件。
- 一个启动修正任务的工作流。
- 一组指定的管理员或修正者，他们有权查看并响应由上述规则创建的策略违规。

规则识别出策略违规后（在此方案中，用户授权过多），相关工作流可启动与修正相关的特定任务，包括自动通知选择修正者。

级别 1 修正者是审计扫描识别出策略违规时要联系的第一个修正者。当超出该区域中标识的提升时间段时，Identity Manager 会通知下一级别的修正者（如果为审计策略指定了多个级别）。

下一节“使用审计策略”介绍了如何使用审计策略向导创建审计策略。

◆ ◆ ◆ 第 14 章

14 审计：审计策略

本章介绍了如何使用审计策略向导创建、编辑、删除和分配审计策略。

在本章中，您可以了解以下概念和任务：

使用审计策略

要创建审计策略，请使用 Identity Manager 审计策略向导。在定义审计策略后，可随后对策略执行各种操作，例如修改或删除策略。

审计策略规则

审计策略规则定义了特定违规。策略规则可以包含使用 XPRESS 语言、XML 对象语言或 JavaScript 语言编写的函数。

可以使用审计策略向导来创建简单规则，也可以使用 Identity Manager IDE 或 XML 编辑器创建功能更强大的规则。

- 规则必须为 `SUBTYPE_AUDIT_POLICY_RULE` 子类型。由审计策略向导生成的规则将自动分配此子类型。
- 规则必须属于 authType `AuditPolicyRule`。由审计策略向导生成的规则将自动分配此 authType。

使用审计策略向导创建的规则将返回值 `true` 或 `false`。返回值 `true` 的策略规则将导致策略违规。不过，可以使用 Identity Manager IDE 创建一个规则，以便在审计扫描或访问查看期间跳过某个用户。返回值 `ignore` 的审计策略规则将停止该用户的规则处理，并跳到下一个目标用户。

有关创建审计策略规则的信息，请参见《Sun Identity Manager Deployment Reference》中的第 4 章 “Working with Rules”。

创建审计策略

要创建审计策略，请使用审计策略向导。

▼ 打开审计策略向导

“审计策略向导”可指导您完成创建审计策略的过程。可以使用以下步骤访问该向导：

1. **登录到管理员界面（第 38 页中的“登录到 Identity Manager 最终用户界面”）。**
2. **单击“遵循性”选项卡。**
   将打开“管理策略”子选项卡或菜单。
3. **要创建新的审计策略，请单击“新建”。**

创建审计策略：概述

您可使用此向导执行以下任务，以创建审计策略：

- 选择或创建用于定义策略限制的规则
- 分配批准者并建立提升限制
- 分配修正工作流

完成每个向导屏幕中显示的任务后，单击“下一步”移至下一步骤。

准备工作

在创建审计策略之前，一定要仔细进行规划！在开始之前，请确保完成以下任务：

- 确定要在“审计策略向导”中创建策略所使用的规则。您所选择的规则由要创建的策略类型和要定义的特定限制确定。有关详细信息，请参见下一节中的第 383 页中的“确定所需规则”。
- 导入要包含在新策略中的任何修正工作流或规则。有关详细信息，请参见第 383 页中的“（可选）将任务划分规则导入到 Identity Manager 中”。
- 请确保您具有创建审计策略所需的权能。有关所需的权能，请参见第 6 章，管理中的第 184 页中的“了解和管理权能”。

▼ 确定所需规则

您在策略中指定的限制会在您创建或导入的规则集中实现。在使用审计策略向导创建规则时，请执行以下步骤：

1. **确定要使用的特定资源。**
2. **从资源的有效属性列表中选择帐户属性。**
3. **选择要对属性施加的条件。**
4. **输入用于比较的值。**

   有关在审计策略向导之外创建审计策略规则的信息，请参见《Sun Identity Manager Deployment Reference》中的第 4 章 “Working with Rules”。

（可选）将任务划分规则导入到 Identity Manager 中

“审计策略向导”无法创建任务划分规则。必须在 Identity Manager 的外部构建这些规则，并使用“配置”选项卡上的“导入交换文件”选项导入这些规则。

（可选）将工作流导入到 Identity Manager 中

▼ 导入外部工作流

要使用 Identity Manager 中当前不可用的修正工作流，请导入外部工作流。您可以使用 XML 编辑器或 Identity Manager IDE 来创建自定义工作流。

1. **设置 `authType='AuditorAdminTask'` 并添加 `subtype='SUBTYPE_REMEDIATION_WORKFLOW'`。您可以选择使用 Identity Manager IDE 或 XML 编辑器设置这些配置对象。**

2 使用“导入交换文件”选项导入工作流。

a. 登录到管理员界面（第 38 页中的“登录到 Identity Manager 最终用户界面”）。

b. 单击“配置”选项卡，然后单击“导入交换文件”子选项卡或菜单。
将打开“导入交换文件”页。

c. 浏览到要上载的工作流文件，然后单击“导入”。
在成功导入工作流后，它将显示在审计策略向导（第 382 页中的“创建审计策略”）的“修正工作流”选项列表中。

命名和描述审计策略

在审计策略向导（如图 14–1 中所示）中输入新策略的名称及其简要描述。

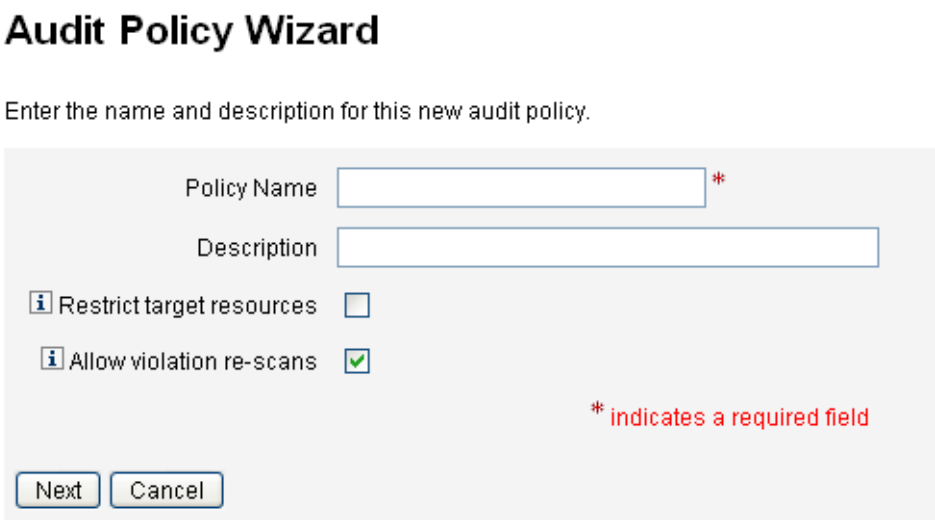


图 14–1 审计策略向导：输入名称和描述屏幕

注 – 审计策略名称不能包含以下字符：'（撇号）、.（句点）、|（管道符号）、[（左括号）、]（右括号）、,（逗号）、:（冒号）、$（美元符号）、"（双引号）、\（反斜杠）或 =（等号）。

还应避免使用以下字符：_（下划线）、%（百分号）、^（插入符号）和 *（星号）。

如果只希望在执行扫描时访问选定的资源，请选择“限制目标资源”选项。

如果希望在违规修正后立即重新扫描用户，请选择“允许违规重新扫描”选项。

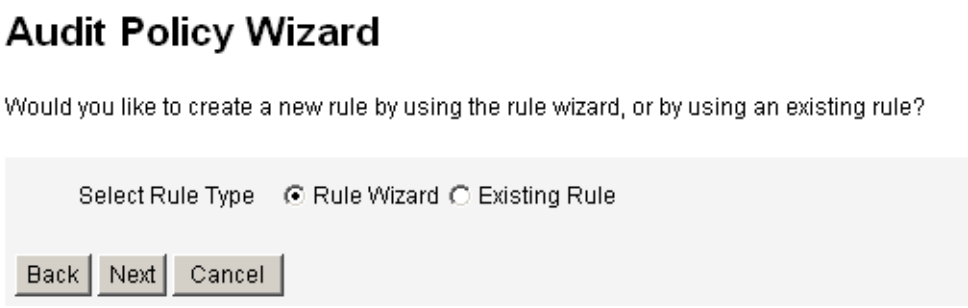
注 – 如果审计策略不限制资源，则在扫描期间将访问用户具有帐户的所有资源。如果这些规则仅使用少数资源，则将策略限定为这些资源会更有效。

单击“下一步”进入下一页。

▼ 选择规则类型

使用此页面可以开始定义规则或将规则包含在策略中。（创建策略时您的大部分工作是定义和创建规则。）

正如下图中所示，可以选择使用 Identity Manager 规则向导创建自己的规则，也可以并入现有的规则。规则向导仅允许在每项规则中使用一个资源。导入的规则可根据需要引用多个资源。



1. **确定是要创建新规则还是使用现有规则。**

   请选择以下任一选项：

   - 要创建新规则，请选择“规则向导”选项（默认设置）。
   - 要并入使用 Identity Manager IDE 创建的现有规则，请选择“现有规则”选项。

2. **单击“下一步”。**

3. **根据步骤 1 中选择的内容，继续执行以下某个小节中的操作：**

   - 如果选择了“规则向导”，请转至第 386 页中的 “使用规则向导创建新规则”一节，然后按照提供的说明进行操作。
   - 如果选择了“现有规则”，请转至第 386 页中的 “选择现有规则”一节，然后按照提供的说明进行操作。

选择现有规则

要在新策略中包含现有规则，请在“选择规则类型”屏幕上选择“现有规则”，然后单击“下一步”。接下来，从“选择现有规则”下拉菜单中选择一个现有审计策略规则。

注 – 如果看不到先前已导入到 Identity Manager 中的规则的名称，请确认您已在规则中添加了第 378 页中的 “使用审计策略规则创建策略”中描述的附加属性。

单击“下一步”。

跳到第 389 页中的 “添加规则”一节。

使用规则向导创建新规则

如果选择通过审计策略向导中的“规则向导”选项创建规则，请在以下各节所述的页面上输入信息。

命名和描述新规则

可以选择命名并描述新规则。使用此页面可输入描述性文本，每当 Identity Manager 显示规则时，这些描述性文本就会显示在该规则名称旁边。请输入简洁易懂且能够描述规则的描述。此描述显示在 Identity Manager 的“查看策略违规”页中。

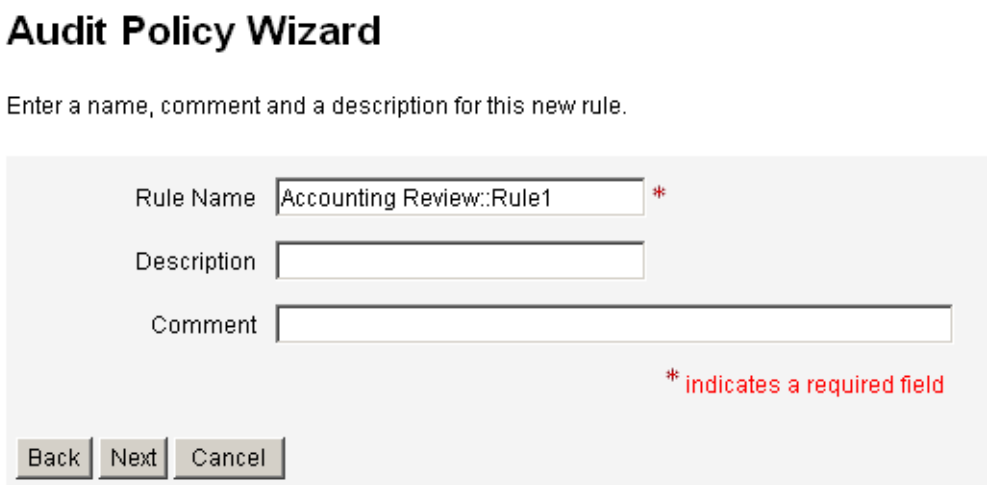


图 14–2 审计策略向导：输入规则描述屏幕

例如，如果要创建一条规则，用以确定 Oracle ERP responsibilityKey 属性值同时为 `Payable User` 和 `Receivable User` 的用户，则可在“描述”字段中输入以下文本：**确定同时具有应付款用户和应收款用户职责的用户**。

使用“注释”字段提供有关规则的任何其他信息。

选择规则引用的资源

使用此页面可以选择规则要引用的资源。每个规则变量必须对应于此资源的一个属性。您有权查看的所有资源将显示在此选项列表中。在此例中，选择 Oracle ERP。

图 14–3 审计策略向导：选择资源屏幕

注 – 支持每个可用资源适配器的大多数（不是全部）属性。有关可用的特定属性的信息，请参见《Sun Identity Manager 8.1 Resources Reference》。

单击“下一步”移至下一页。

创建规则表达式

使用此屏幕输入新规则的规则表达式。此示例创建一条规则，在该规则中，用户的 Oracle ERP `responsibilityKey` 属性值不能同时为 `Payable User` 和 `Receivable User` 属性值。

▼ 创建规则表达式

1. **从可用属性列表中选择用户属性。此属性将直接对应于规则变量。**
2. **从列表中选择逻辑条件。有效条件包括 =（等于）、!=（不等于）、<（小于）、<=（小于等于）、>（大于）、>=（大于等于）、is true、is null、is not null、is empty 和 contains。针对此示例的用途，您可以在可能的属性条件列表中选择 `contains`。**
3. **输入表达式的值。例如，如果输入 `Payable user`，则指定了 `responsibilityKeys` 属性值为 `Payable user` 的 Oracle ERP 用户。**

4 （可选）单击 AND 或 OR 运算符添加另一行并创建另一个表达式。

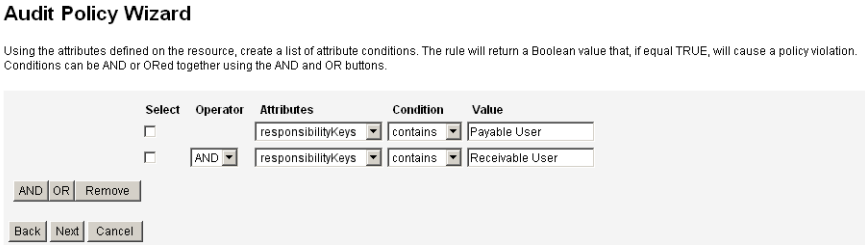


图 14–4 审计策略向导：选择规则表达式屏幕

此规则返回一个布尔值。如果两个语句都为真，则策略规则返回 TRUE 值，这样便导致策略违规。

注 – Identity Manager 不支持规则嵌套控制。此外，如果使用审计策略向导创建在规则之间使用不同布尔运算符的策略，可能会产生无法预测的结果，原因是未指定评估顺序。

对于复杂的规则表达式，请使用 XML 编辑器创建规则（而不是使用审计策略向导）。通过使用 XML 编辑器，您可以在必要时否定创建的内容，从而仅在规则之间使用单个布尔运算符。

以下代码示例显示了您已在此屏幕中创建的规则的 XML：

```
<Description>Payable User/Receivable User</Description>
  <RuleArgument name='resource' value='Oracle ERP'>
    <Comments>Resource specified when  audit policy was created.</Comments>
    <String>Oracle ERP</String>
  </RuleArgument>
    <and>
      <contains>
        <ref>accounts[Oracle ERP].responsibilityKeys</ref>
        <s>Receivable User</s>
      </contains>
      <contains>
        <ref>accounts[Oracle ERP].responsibilityKeys</ref>
        <s>Payables User</s>
      </contains>
    </and>
    <MemberObjectGroups>
      <ObjectRef type='ObjectGroup' id='#ID#Top' name='Top'/>
```

```
    </MemberObjectGroups>
</Rule>
```

要从规则中删除表达式，请选中属性条件，然后单击“删除”。

单击“下一步”继续使用审计策略向导。可通过添加现有规则或再次使用向导来添加更多规则。

添加规则

可通过导入现有规则或使用向导来创建其他规则。（有关详细信息，请参见第 385 页中的 “选择规则类型”。）

根据需要，单击 AND 或 OR 运算符继续添加规则。要删除规则，请选择规则，然后单击“删除”。

仅在**所有**规则的布尔表达式均评估为 true 时，才发生策略违规。使用 AND/OR 运算符将规则分组后，即使所有的规则均未评估为 true，策略也可能评估为 true。Identity Manager 仅在规则评估为 true，且策略表达式也评估为 true 时，才创建违规。

注 – Identity Manager 不支持规则嵌套控制。此外，如果使用审计策略向导创建在规则之间使用不同布尔运算符的策略，可能会产生无法预测的结果，原因是未指定评估顺序。

对于复杂的规则表达式，请使用 XML 编辑器创建规则（而不是使用审计策略向导）。通过使用 XML 编辑器，您可以在必要时否定创建的内容，从而仅在规则之间使用单个布尔运算符。

选择修正工作流

使用此屏幕选择要与此策略关联的“修正”工作流。此处分配的工作流确定检测到审计策略违规时在 Identity Manager 中执行的操作。

注 – 将为每个失败的审计策略启动一个工作流。对于由特定策略的策略扫描所创建的每个遵循性违规，每个工作流都将包含一个或多个工作项目。

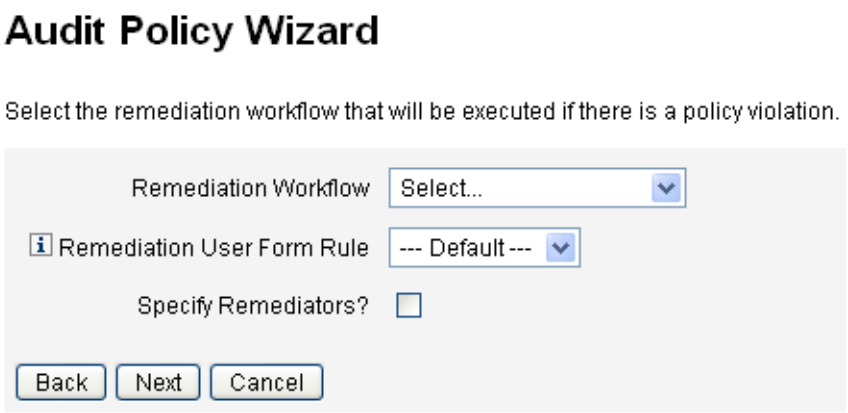


图 14–5 审计策略向导：选择修正工作流屏幕

注 – 有关导入通过 XML 编辑器或 Identity Manager IDE 创建的工作流的信息，请参见第 383 页中的“（可选）将任务划分规则导入到 Identity Manager 中”。

可以使用“修正用户表单规则”下拉菜单选择一个规则，以计算在通过修正编辑用户时要应用的用户表单。默认情况下，编辑用户以响应修正工作项目的修正者将使用为其分配的用户表单。如果审计策略指定了修正用户表单，则会使用此表单。这样在审计策略指出特定的问题时，可以使用与之对应的特定表单。

要指定将与此修正工作流关联的修正者，请选中“是否指定修正者？”复选框。如果选择此选项，然后单击“下一步”，则会显示“分配修正者”页。如果不选择此选项，向导接下来会显示“审计策略向导分配组织”屏幕。

为修正选择修正者和超时时间

如果指定修正者，在检测到此策略违规时，将会通知分配给此审计策略的修正者。此外，默认工作流还会向修正者分配修正工作项目。任何 Identity Manager 用户都可以成为修正者。

您可以选择至少分配一个级别 1 修正者，或指定的用户。检测到策略违规时，会首先通过电子邮件（由修正工作流启动）与级别 1 修正者联系。如果在级别 1 修正者响应前已达到指定的提升超时时间段，则 Identity Manager 会接着联系此处指定的级别 2 修正者。Identity Manager 仅在提升时间段结束之前级别 1 和级别 2 修正者都没有响应时，才联系级别 3 修正者。

注 – 如果为选定的最高级别修正者指定了提升超时值，则提升超时时将从列表中删除工作项目。默认情况下，提升超时值设置为 0。在这种情况下，工作项目不会过期，并保留在修正者的列表中。

"Assigning Remediators" 是可选选项。如果选择此选项，请在指定设置后单击“下一步”以进入下一个屏幕。

要将用户添加到可用的修正者列表中，请输入用户 ID，然后单击“添加”。或者，单击 ...（更多）以搜索用户 ID。在“开头为”字段中输入一个或多个字符，然后单击“查找”。从搜索列表中选择用户后，单击“添加”可将该用户添加到修正者列表中。单击“解除”可关闭搜索区域。

要从修正者列表中删除用户 ID，请在列表中选择该 ID，然后单击“删除”。

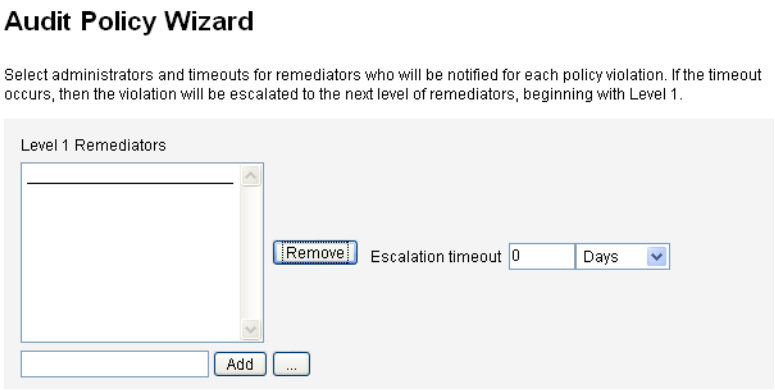


图 14–6 审计策略向导：选择级别 1 修正者区域

选择可访问此策略的组织

可以使用该屏幕（如图 14–7 中所示）选择可查看和编辑此策略的组织。

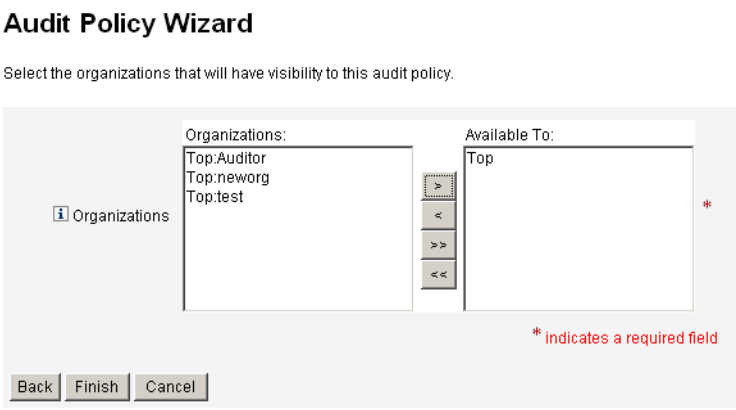


图 14–7 审计策略向导：分配组织可视性屏幕

选择组织后，单击“完成”可创建审计策略并返回到“管理策略”页。现在此列表中将显示新创建的策略。

编辑审计策略

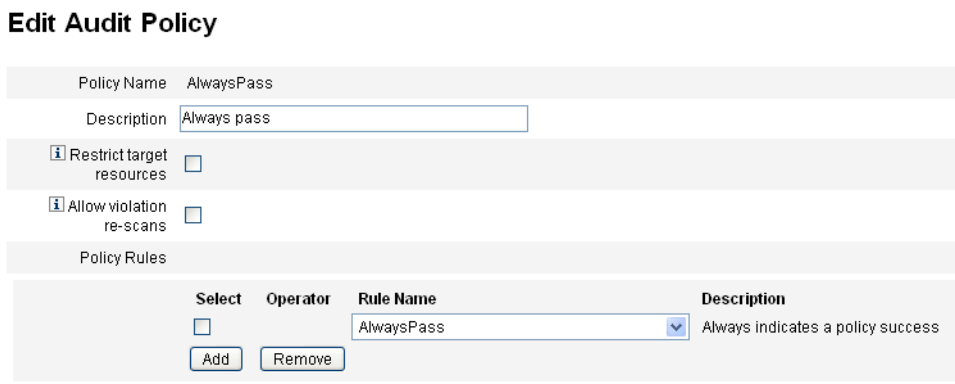
审计策略的普通编辑任务包括：

- 添加或删除规则
- 更改目标资源
- 调整有权访问策略的组织列表
- 更改与每个修正级别关联的提升超时时间
- 更改与策略关联的修正工作流

编辑策略页

单击“审计策略”名称列中的策略名称，以打开“编辑审计策略”页。此页将审计策略信息归类到以下区域：

- 标识和规则区域
- 修正者和提升超时时间区域
- 工作流和组织区域



使用页面的此区域可以：

- 编辑策略描述
- 添加或删除规则

注 – 不能使用此产品直接编辑现有规则。可以使用 Identity Manager IDE 或 XML 编辑器编辑规则，然后将其导入到 Identity Manager 中。然后即可删除上一版本，并添加新修订的版本。

编辑审计策略描述

通过选择“描述”字段中的文本然后输入新文本，可以编辑审计策略描述。

编辑选项

可随意选择或取消选择“限制目标资源”或“允许违规重新扫描”选项。

从策略中删除规则

要从策略中删除规则，可单击规则名称前面的“选择”按钮，然后单击“删除”。

向策略中添加规则

单击“添加”追加一个新字段，可使用该字段选择要添加的规则。

更改策略使用的规则

在 "Rule Name" 列中，从选项列表中选择其他规则。

修正者区域

图 14–8 显示了“修正者”区域的一部分，可在其中为策略分配级别 1、级别 2 和级别 3 修正者。

图 14–8 “编辑审计策略”页：分配修正者

使用页面的此区域可以：

- 为策略删除或分配修正者
- 调整升级超时时间

删除或分配修正者

通过输入用户 ID 然后单击“添加”，可以选择一个或多个修正级别的修正者。要搜索用户 ID，请单击 ...（更多）。必须至少选择一个修正者。

要删除修正者，请在列表中选择用户 ID，然后单击“删除”。

调整提升超时时间

选择超时值，然后输入新值。默认情况下未设置任何超时值。

注 – 如果为选定的最高级别修正者指定了提升超时值，则提升超时时将从列表中删除工作项目。

修正工作流和组织区域

图 14–9 显示了用于为审计策略指定修正工作流和组织的区域。

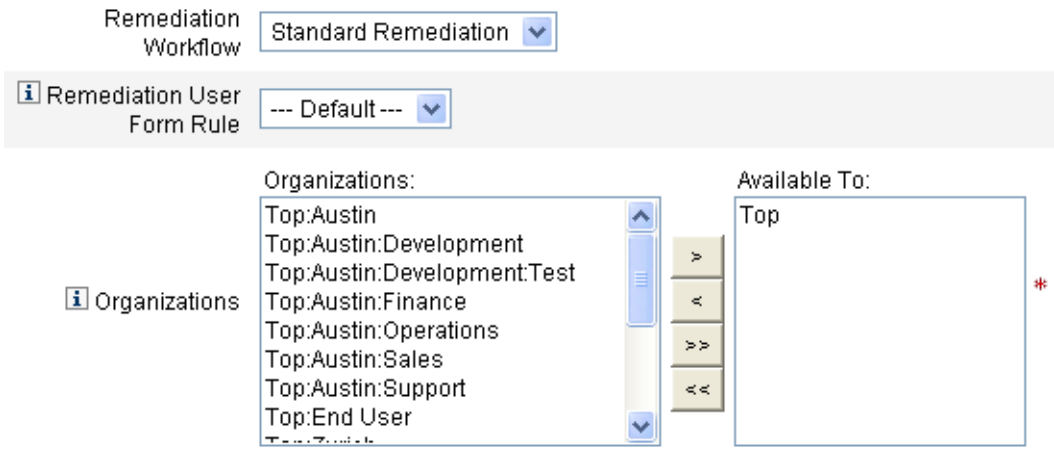


图 14–9 “编辑审计策略”页：修正工作流和组织

使用页面的此区域可以：

- 更改在发生策略违规时启动的修正工作流
- 选择修正用户表单规则
- 调整有权访问此策略的组织

更改修正工作流

要更改分配给策略的工作流，可在选项列表中选择备用工作流。默认情况下，不向审计策略分配工作流。

注 – 如果未向审计策略分配工作流，则将不会向任何修正者分配违规。

在列表中选择修正工作流，然后单击“保存”。

选择修正用户表单规则

可以选择一条规则，以计算通过修正编辑用户时所应用的用户表单。

分配或删除组织可视性

调整可使用此审计策略的组织，然后单击“保存”。

示例策略

Identity Manager 提供了以下示例策略（可从“审计策略”列表中访问这些策略）：

- IDM 角色比较策略
- IDM 帐户累积策略

IDM 角色比较策略

此示例策略允许您将用户的当前访问权限与 Identity Manager 角色所指定的访问权限进行比较。该策略可确保为用户设置由角色指定的所有资源属性。

此策略在以下情况下将会失败：

- 用户缺少由角色指定的任何资源属性
- 用户的资源属性与角色所指定的资源属性不同

IDM 帐户累积策略

此示例策略可验证用户拥有的所有帐户是否至少由该用户所拥有的一个角色引用。

如果分配给用户的角色未明确引用某些资源，而该用户在任一此类资源上拥有帐户，则此策略将会失败。

删除审计策略

从 Identity Manager 中删除审计策略时，还会删除所有引用此策略的违规。

当您单击 "Manage Policies" 查看策略时，可从界面的 "Compliance" 区域删除策略。要删除审计策略，请在策略视图中选择策略名称，然后单击“删除”。

审计策略疑难解答

通常，对策略规则进行调试是解决审计策略问题的最好方法。

要调试规则，可在规则代码中添加以下跟踪元素。

```
<block trace='true'>
<and>
    <contains>
        <ref>accounts[AD].firstname</ref>
        <s>Sam</s>
    </contains>
    <contains>
        <ref>accounts[AD].lastname</ref>
```

```
        <s>Smith</s>
    </contains>
</and>
</block>
```

- 如果在 Identity Manager 界面中看不到工作流，请确认：
  - 您已经在工作流中添加了 `subtype='SUBTYPE_REMEDIATION_WORKFLOW'` 属性。Identity Manager 管理员界面中不显示没有该子类型的工作流。
  - 您具有 authType `AuditorAdminTask` 的权能。
  - 您可以控制包含工作流的组织。
- 如果已导入规则，但在审计策略向导中看不到这些规则，请确认：
  - 每个规则都属于 `subtype="SUBTYPE_AUDIT_POLICY_RULE'` 或 `subtype="SUBTYPE_AUDIT_POLICY_SOD_RULE'`。
  - 您具有 authType `AuditPolicyRule` 的权能。
  - 您可以控制包含工作流的组织。

分配审计策略

要将审计策略分配给组织，用户必须（至少）具有“分配组织审计策略”权能。要将审计策略分配给用户，该用户必须具有“分配用户审计策略”权能。具有分配审计策略权能的用户同时具有这两种权能。

要分配组织级别的策略，请在“帐户”选项卡上选择“组织”，然后在“分配的审计策略”列表中选择策略。

▼ 分配用户级别的策略

1. **单击“帐户”区域中的用户。**
2. **在用户表单中选择“遵循性”。**
3. **在“分配的审计策略”列表中选择策略。**

注 – 在修正用户违规时，将始终对直接分配给该用户的审计策略（通过用户帐户或组织分配进行分配）进行重新评估。

解除审计者权能限制

默认情况下，执行审计任务所需的权能包含在“顶层”组织（对象组）中。因此，只有控制“顶层”组织的管理员才能向其他管理员分配这些权能。

可以通过为其他组织添加权能来解除此限制。Identity Manager 提供了两个帮助执行此任务的实用程序，它们位于 `sample/scripts` 目录中。

▼ 添加权能

要为“顶层”组织以外的组织添加执行审计任务所需的权能，请执行以下步骤：

1. **运行以下命令以列出所有权能（管理组）及其关联组织（对象组）：**

   ```
   beanshell objectGroupUpdate.bsh -type AdminGroup -action list -csv
   ```

   此命令可捕获使用逗号分隔值 (Comma-Separated Value, CSV) 格式的文件的输出。

2. **编辑 CSV 文件，根据需要调整权能在组织分层结构中的位置。**

3. **运行以下命令以更新 Identity Manager。**

   ```
   beanshell objectGroupUpdate.bsh -data CSVFileName -action add -groups NewObjectGroup
   ```

◆ ◆ ◆ 第 15 章

15 审计：监视遵循性

本章介绍如何执行审计查看和实现实践，以帮助您管理对联邦委托法规的遵循性。

在本章中，您可以了解以下概念和任务：

审计策略扫描和报告

本节介绍了有关审计策略扫描的信息，以及运行和管理审计扫描的步骤。

扫描用户和组织

扫描可以在单个的用户或组织上运行选定的审计策略。您可能要扫描用户或组织以查看是否发生了特定违规，或执行未分配给用户或组织的策略。可以从界面的“帐户”区域启动扫描。

注 – 您还可以从“服务器任务”选项卡中启动或调度审计策略扫描。

▼ 扫描用户帐户或组织

1. **在管理员界面中，从主菜单中选择“帐户”。**
2. **在“帐户”列表中，执行以下任一操作：**

   a. **选择一个或多个用户，然后从“用户操作”选项列表中选择“扫描”。**

b. **选择一个或多个组织，然后从“组织操作”选项列表中选择“扫描”。**

将显示“启动任务”对话框。图 15–1 是审计策略用户扫描的“启动任务”页示例。

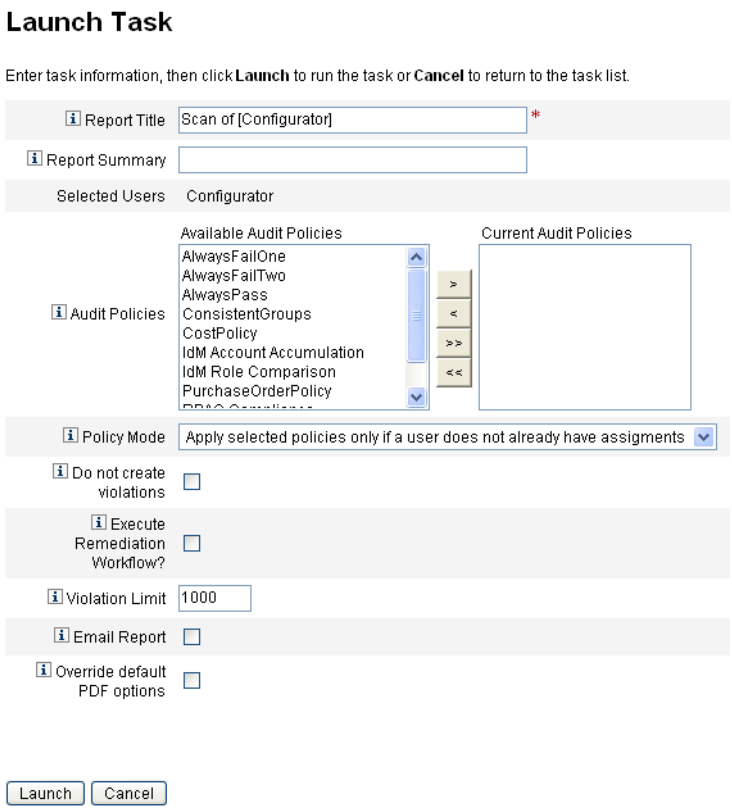


图 15–1 “启动任务”对话框

3 **在“报告标题”字段中输入扫描的标题。（必需）**

4 **指定其余选项。**

这些选项包括：

- **报告摘要**：输入扫描的描述。
- **添加策略**：选择一个或多个要运行的审计策略。必须至少指定一个策略。
- **策略模式**：选择策略模式，以确定选定策略与已分配策略的用户之间的交互方式。分配可直接来自用户或来自分配了用户的组织。

- **不创建违规**：如果要对审计策略进行评估并报告违规，但不希望创建或更新遵循性违规，也不希望执行修正工作流，则启用此框。不然，扫描操作的任务结果会显示创建的违规。在测试审计策略时，此选项非常有用。
- **是否执行修正工作流？**：启用此框可运行在审计策略中分配的修正工作流。如果审计策略未定义修正工作流，将不运行任何修正工作流。
- **违规限制**：编辑此框可设置扫描中止前可发出的最大遵循性违规数。此值提供一种安全保护措施，可限制运行审计策略（这些审计策略在检查时可能过于危险）所带来的风险。空值表示未设置任何限制。
- **电子邮件报告**：启用此框可指定报告收件人。也可以让 Identity Manager 附加一个包含 CSV（Comma-separated Values，逗号分隔值）格式报告的文件。
- **覆盖默认 PDF 选项**：启用此框可覆盖默认 PDF 选项。

5 **单击"启动"开始扫描。**

要查看审计扫描的报告结果，请查看"审计者报"。

使用审计者报告

Identity Manager 提供了许多审计者报告。下表介绍了这些报告。

表 15–1 Auditor 报告描述

Auditor 报告类型	描述
访问查看范围	显示选定访问查看所指的用户之间的重叠部分或差异部分。由于大多数访问查看的用户范围都由查询或某项成员资格操作所指定，因此实际的用户集会随时间而变化。此报告可显示由两个不同的访问查看所指定的用户之间的重叠部分和/或差异部分（以确定查看在操作中是否有效）；由两个不同的访问查看所生成的权利之间的重叠部分和/或差异部分（以确定范围是否随时间而变化）；用户和权利之间的重叠部分和/或差异部分（以确定是否为查看范围内的所有用户生成了权利）。
访问查看详细信息	显示所有用户权利记录的当前状态。该报告可以按用户的组织、访问查看和访问查看实例、权利记录的状态和证明者进行过滤。
访问查看摘要	提供有关所有访问查看的摘要信息。它概述了列出的每个访问查看扫描的扫描的用户、扫描的策略以及证明活动的状态。
访问扫描用户范围	比较选定的扫描以确定扫描范围中包含哪些用户。它可显示重叠部分（包含在所有扫描中的用户）或差异部分（包含在多个扫描但未包含在全部扫描中的用户）。尝试组织多个访问扫描以包含相同用户或不同用户（视扫描需求而定）时，此报告非常有用。
审计策略摘要	该报告概述了所有审计策略的关键元素，包括每个策略的规则、修正者和工作流。

表 15–1 Auditor 报告描述 （续）

Auditor 报告类型	描述
审计的属性	该报告显示所有指示指定的资源帐户属性变更的审计记录。 该报告可搜索每个已存储的可审计属性的审计数据。它将基于任何扩展的属性搜索数据，而这些扩展的属性可从 WorkflowServices 或标记为可审计的资源属性指定。有关配置此报告的信息，请参见第 404 页中的 “配置审计属性报告”。
审计策略违规历史	在指定时间段内创建的每个策略的所有遵循性违规的图形视图。可以按策略过滤该报告，并可以按天、周、月或季对其进行分组。
用户访问	显示特定用户的审计记录和用户属性。
组织违规历史	在特定时间段内创建的每个资源的所有遵循性违规的图形视图。可以按组织过滤该报告，并可以按天、周、月或季对其进行分组。
资源违规历史	在指定时间范围内创建的每个资源的所有遵循性违规的图形视图。
任务划分	显示冲突表中安排的任务划分违规。使用基于 Web 的界面时，您可以通过单击链接来访问其他信息。 可以按组织过滤该报告，并可以按天、周、月或季对其进行分组。
违规摘要	显示当前所有的遵循性违规。可以按修正者、资源、规则、用户或策略过滤该报告。

可通过 Identity Manager 界面中的“报告”选项卡查看这些报告。

注 – RULE_EVAL_COUNT 值等于在策略扫描期间计算的规则数。该值有时包含在报告中。

Identity Manager 按如下方式计算 RULE_EVAL_COUNT 值：

扫描的用户数 x（策略中的规则数 + 1）

计算中包含 +1 是因为，Identity Manager 还将**策略规则**计算在内，这是实际确定是否违反策略的规则。策略规则检查审计规则结果，并执行布尔逻辑以得出策略结果。

例如，如果策略 A 包含三个规则，策略 B 包含两个规则，并且您已扫描 10 个用户，则 RULE_EVAL_COUNT 值等于 70，原因如下：

10 个用户 x（3 + 1 + 2 + 1 个规则）

创建 Auditor 报告

要运行报告，必须先创建报告模板。您可以为报告指定各种条件，包括指定接收报告结果的电子邮件收件人。创建并保存报告模板后，可在“运行报告”页中查看该报告模板。

下图显示了具有已定义审计者报告列表的“运行报告”页示例。

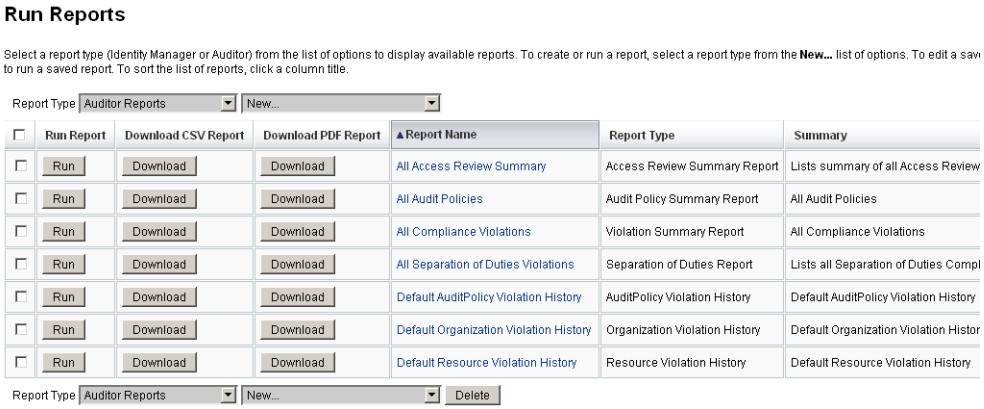


图 15–2 “运行报告”页选项

▼ 创建审计者报告

1 **在管理员界面中，单击主菜单中的“报告”。**

将打开“运行报告”页。

2 **选择“审计者报告”作为报告类型。**

3 **在报告的“新建”列表中选择一个报告。**

将显示“定义报告”页。报告对话框的字段和布局因每个报告类型而异。有关指定报告条件的信息，请参阅 Identity Manager 帮助。

输入并选择了报告条件后，您可以执行以下操作：

- 运行报告而不保存。

  单击“运行”开始运行报告。Identity Manager 不保存报告（如果定义新报告）或更改的报告条件（如果编辑现有报告）。

- 保存报告。

  单击“保存”以保存报告。保存报告后，您可从“运行报告”页（报告列表）运行报告。从“运行报告”页运行报告后，您可以通过“查看报告”选项卡立即查看或稍后查看输出。

有关调度报告的信息，请参见第 237 页中的 “调度报告”。

配置审计属性报告

审计属性报告（请参见表 15–1）可以报告对 Identity Manager 用户和帐户所做的属性级别的更改。但是，标准的审计日志记录不会生成足够的审计日志数据来支持完整的查询表达式。

标准的审计日志记录**会**将更改的属性写入审计日志的 `acctAttrChanges` 字段中，但是更改属性的写入方式使报告查询只能基于更改属性的名称来与记录匹配。报告查询不能准确地与属性值进行匹配。

可以通过指定以下参数对报告进行配置，使其与包含对属性 `lastname` 所做的更改的记录进行匹配：

```
Attribute Name = 'acctAttrChanges'
Condition = 'contains'
Value = 'lastname'
```

注 – 由于数据在 `acctAttrChanges` 字段中的存储方式，必须使用 `Condition='contains'`。此字段不具有多值属性。实际上，它是一个包含所有更改属性的**之前/之后**值的数据结构，其表示形式为 `attrname=value`。因此，上述设置允许报告查询与 `lastname=` *xxx* 的任何实例相匹配。

也可以只捕获那些特定属性为特定值的审计记录。为此，请按照第 280 页中的 “配置“审计”选项卡”一节中的步骤进行操作。选中“审计整个工作流”复选框，单击“添加属性”按钮以选择为生成报告而要记录的属性，然后单击“保存”。

接下来，启用任务模板配置（如果尚未启用）。为此，请按照第 257 页中的 “启用任务模板”一节中的步骤进行操作。不要更改“选定的进程类型”列表中的默认值，只需单击“保存”。

现在，工作流可以提供能够同时匹配属性名称和属性值的审计记录了。虽然，启用此级别的审计可以提供更多的信息，但是要注意，这会显著增加性能开销，使工作流的运行速度变慢。

遵循性违规修正和缓解

本节介绍如何使用 Identity Manager 修正来保护您的重要资产。

以下主题详述了 Identity Manager 修正进程的元素：

关于修正

Identity Manager 在检测到未解决的（未缓解的）审计策略遵循性违规时，将创建一个修正请求，该请求必须由**修正者**进行处理。修正者是一个指定的用户，允许其评估并响应审计策略违规。

修正者提升

Identity Manager 允许您定义三个修正者升级的级别。修正请求最先发送到级别 1 修正者。如果在超时之前级别 1 修正者没有对修正请求进行操作，则 Identity Manager 会将违规提升至级别 2 修正者，并开始新的超时时间段。如果级别 2 修正者在超时之前未响应，则该请求再次被升级至级别 3 修正者。

要执行修正，必须至少为您的企业指定一个修正者。为每个级别指定一个以上的修正者是可选的，但它是建议做法。多个修正者可帮助确保工作流不被延迟或停止。

修正安全性访问

这些验证选项用于 authType `RemediationWorkItem` 的工作项目。

- 修正工作项目拥有者
- 修正工作项目拥有者的直接或间接管理员
- 控制修正工作项目拥有者所属组织的管理员

默认情况下，验证检查的行为是以下行为之一：

- 所有者为尝试执行该操作的用户
- 所有者位于由尝试执行该操作的用户控制的组织中
- 拥有者为尝试执行该操作的用户的下属

第二个和第三个检查可通过修改以下选项单独配置：

- **controlOrg**。有效值为 true 或 false。
- **subordinate**。有效值为 true 或 false。
- **lastLevel**。包括在结果中的最后一个下属级别；-1 表示所有级别。lastLevel 的整数值默认为 -1，表示直接或间接下属。

可通过以下方式添加或修改这些选项：

用户表单：修正列表

修正工作流进程

Identity Manager 提供了标准修正工作流，从而为审计策略扫描提供修正处理。

标准修正工作流生成一个包含有关遵循性违规信息的修正请求（查看类型的工作项目），并向审计策略中指定的每个级别 1 修正者发送一个电子邮件通知。修正者缓解违规时，工作流会更改现有遵循性违规对象的状态并向其分配一个到期日期。

可以通过将用户、策略名称和规则名称进行组合来唯一标识遵循性违规。如果审计策略评估为 true，则将为每个用户/策略/规则组合创建新的遵循性违规（如果该组合当前尚不具有违规）。如果该组合具有违规，并且违规处于已缓解状态，则工作流进程将不执行任何操作。如果未缓解现有违规，则其反复出现次数将增加一次。

有关修正工作流的详细信息，请参见第 377 页中的 “关于审计策略”。

修正响应

默认情况下，为每个修正者提供三个响应选项：

- **修正**。修正者指示已经为修复有关资源的问题而进行了工作。

  修改遵循性违规时，Identity Manager 会创建一个审计事件来记录修正。此外，Identity Manager 还存储修正者名称及提供的所有注释。

  注 – 修正后，在进行下次审计扫描前将不会删除违规。如果将审计策略配置为允许重新扫描，则违规修正后将立即对用户进行重新扫描。

- **缓解**。修正者允许违规，并在一定的时间内对用户违规进行免除。

  如果是经过权衡后的违规（例如，一个属于两个组的业务案例），则可长期缓解此违规。您也可以短期缓解违规（例如，因资源的系统管理员休假，您不知道如何修复问题的情况）。

  Identity Manager 中存储了缓解违规的修正者的名称、免除的到期日期及提供的所有注释。

  注 – Identity Manager 检测到到期的免除时，它会将违规从已缓解状态返回至暂挂状态。

- **转发**。修正者将解决违规的职责重新分配给另外一个人。

修正示例

您的企业建立了一条规则，规定用户无法同时负责“应付帐款”和“应收帐款”，并且您收到了用户违反此规则的通知。

- 如果该用户是一个主管，并且在公司雇佣其他人负责其中的一个职位之前，他同时负责这两个职位，则可以缓解此违规，并签发一个最长六个月的免除期。
- 如果用户违反此规则，可请求 Oracle ERP 管理员更正此冲突，然后，在资源的相关问题解决修复后修正此违规。或者，您还可以将修正请求转发给 Oracle ERP 管理员。

修正电子邮件模板

Identity Manager 提供了一个“策略违规通知”电子邮件模板（可通过选择“配置”选项卡，然后再选择“电子邮件模板”子选项卡获得）。可对此模板进行配置，以通知修正者暂挂违规。有关详细信息，请参见第 4 章，配置业务管理对象中的第 92 页中的 “自定义电子邮件模板”。

使用“修正”页

选择“工作项目”→“修正”以访问“修正”页。

您可使用此页执行以下操作：

- 查看暂挂违规
- 排列策略违规的优先级
- 缓解一个或多个策略违规
- 修正一个或多个策略违规
- 转发一个或多个策略违规
- 从修正工作项目中编辑用户

查看策略违规

进行操作之前，可通过“修正”页查看有关违规的详细信息。

根据您所具有的权能或您在 Identity Manager 权能分层结构中的位置，您可能可以查看其他修正者的违规并对这些违规执行操作。

以下是与查看违规相关的主题：

- 第 408 页中的 “查看暂挂请求”
- 第 408 页中的 “查看已完成的请求”
- 第 409 页中的 “更新表”

查看暂挂请求

默认情况下，分配给您的暂挂请求将显示在“修正”表中。

您可使用“列出修正”选项来查看不同修正者的暂挂修正请求：

- 选择“我的直接报告”可查看组织中直接向您报告的用户的暂挂请求。
- 选择“搜索用户”可输入或查找您要查看其暂挂请求的一个或多个用户。输入用户 ID，然后单击“应用”以查看该用户的暂挂请求。或者，单击 **...**（更多）以搜索用户。找到并选择用户之后，单击“解除”可关闭搜索区域。

生成的表中提供关于每个请求的以下信息：

- **修正者**。分配的修正者的名称。仅当查看其他修正者的修正请求时才会显示此列。
- **用户**。发送请求的用户。
- **审计策略/请求**。修正者请求的操作。
- **审计规则/描述**。请求的修正注释。
- **违规状态**。违规的当前状态。
- **严重程度**。分配给请求的严重程度（“无”、“低”、“中”、“高”或“严重”）。
- **优先级**。分配给请求的优先级（“无”、“低”、“中”、“高”或“紧急”）。
- **请求日期**：发出修正请求的日期和时间。

注 – 每个用户都可以选择一个自定义表单，以显示与特定修正者相关的修正数据。要分配自定义表单，请选择用户表单上的“遵循性”选项卡。

查看已完成的请求

要查看已完成的修正请求，请单击“我的工作项目”选项卡，然后单击“历史”选项卡。将显示先前已修正的工作项目的列表。

结果表（由 `AuditLog` 报告生成）提供关于每个修正请求的以下信息：

- **时间戳**。修正请求的日期和时间
- **主体**。处理请求的修正者的名称
- **操作**。修正者是缓解还是修正了请求
- **类型**。**遵循性违规**或**用户权利**
- **对象名称**。被违反的审计策略的名称
- **资源**。提供修正者的帐户 ID（或可能显示 N/A）
- **ID**。与策略违规相关的帐户 ID
- **结果**。始终指示 `Success`

单击表格中的时间戳将打开“审计事件详细信息”页。

“审计事件详细信息”页提供有关已完成请求的信息，包括有关修正或缓解、事件参数（如果适用）和可审计属性的信息。

更新表

要更新“修正”表中提供的信息，请单击“刷新”。“修正”页将通过任何新的修正请求更新该表。

排列策略违规的优先级

可以通过向策略违规分配优先级和/或严重程度来排列策略违规的优先级。可以在“修正”页中排列违规的优先级。

▼ 编辑违规的优先级或严重程度

1. **在列表中选择一个或多个违规。**
2. **单击“确定优先级”。**
   将显示“排列策略违规优先级”页。
3. **（可选）设置违规的严重程度。选项包括“无”、“低”、“中”、“高”或“严重”。**
4. **（可选）设置违规的优先级。选项包括“无”、“低”、“中”、“高”或“紧急”。**
5. **完成选择后单击“确定”。Identity Manager 将返回到修正列表。**

注 – 只能对类型为 CV（Compliance Violation，遵循性违规）的修正设置严重程度和优先级值。

缓解策略违规

可以在“修正”和“查看策略违规”页中缓解策略违规。

在“修正”页

▼ 在“修正”页中缓解暂挂策略违规

1. **在表中选择行以指定要缓解的请求。**
   - 选中一个或多个选项，以指定要缓解的请求。
   - 选中表标题中的选项，以缓解表中列出的所有请求。

   Identity Manager 只允许输入一组描述缓解操作的注释。除非各个违规是相关的，只需一个单独的注释即可，否则，您可能不想执行批量缓解。

只能缓解包含遵循性违规的请求，而不能缓解其他修正请求。

2 **单击“缓解”。**

将显示“缓解策略违规”页（或“缓解多项策略违规”页）。

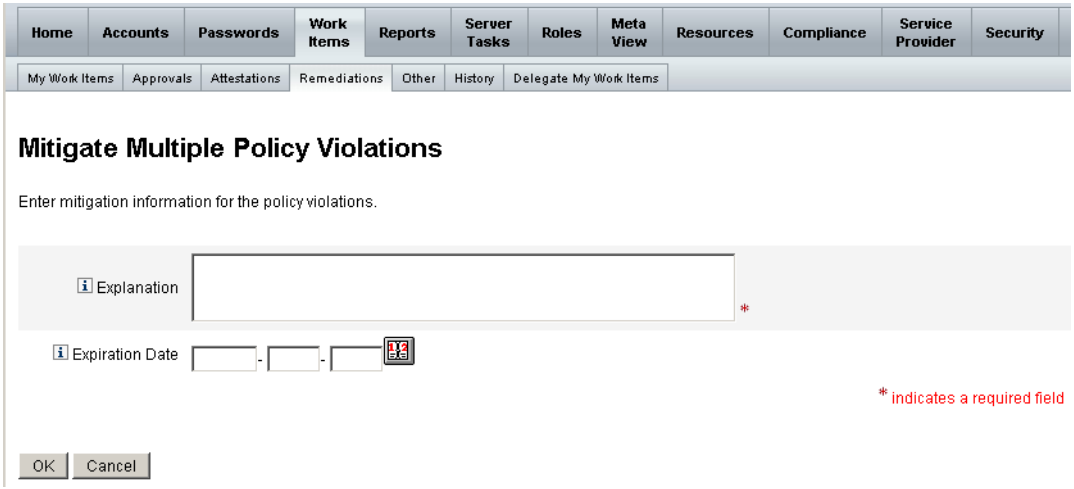


图 15–3 “缓解策略违规”页

3 **在“说明”字段中输入有关缓解的注释。（必需）**

您的注释可提供针对此操作的审计跟踪，因此，请确保输入完整、有意义的信息。例如，解释缓解策略违规的原因、日期、选择免除期的原因。

4 **直接在“到期日期”字段中键入日期（格式为 YYYY-MM-DD）可提供免除的到期日期，也可单击日期按钮后在日历中选择日期。**

注 – 如果不提供日期，则免除会无限期有效。

---

5 **单击“确定”以保存更改并返回到“修正”页。**

修正策略违规

▼ 修正一个或多个策略违规

1 **使用表中的复选框指定要修正的请求。**

- 选中表中的一个或多个复选框，以指定要修正的请求。

- 选中表标题中的复选框，以修正表中列出的所有请求。

  如果选择了多个请求，请记住 Identity Manager 仅允许输入一组注释来说明修正操作。除非各个违规是相关的，只需一个单独的注释即可，否则，您可能不想执行批量修正。

2 **单击“修正”。**

3 **屏幕将显示“修正策略违规”页（或“修正多项策略违规”页）。**

4 **在“注释”字段中输入关于修正的注释。**

5 **单击“确定”以保存更改并返回到“修正”页。**

注 – 在修正用户违规时，将始终对直接分配给该用户的审计策略（即，通过用户帐户或组织分配所分配的策略）进行重新评估。

转发修正请求

可将一个或多个修正请求转发给另一个修正者。

▼ 转发修正请求

1 **使用表中的复选框指定要转发的请求。**

- 选中表标题中的复选框，以转发表中列出的所有请求。
- 选中表中的各个复选框，以转发一个或多个请求。

2 **单击“转发”。**

将显示“选择并确认转发”页。

图 15–4 “选择并确认转发”页

3 **在“转发至”字段中输入修正者名称，然后单击“确定”。或者，也可以单击 . . .（更多）以搜索修正者名称。从搜索列表中选择一个名称，然后单击“设置”在“转发至”字段中输入该名称。单击“解除”可关闭搜索区域。**

重新显示“修正”页时，新的修正者名称将显示在表的“修正者”列中。

从修正工作项目中编辑用户

从修正工作项目中，您可以（具有适当的用户编辑权能）编辑用户以修正问题（如相关的权利历史中所述）。

要编辑用户，请单击“查看修正请求”页中的“编辑用户”。随后出现的“编辑用户”页中将显示以下内容：

- 此工作项目的与用户相关的权利历史
- 用户的属性

  此处显示的选项与“帐户”区域中所提供的“编辑用户”表单上的选项相同。

修改用户之后，请单击“保存”。

注 – 保存用户编辑后，将会运行“更新用户”工作流。由于此工作流可能需要进行批准，因此对用户帐户所做的更改在保存后的一段时间内可能无效。如果审计策略允许重新扫描，并且“更新用户”工作流尚未完成，则后续的策略扫描可能会检测到相同的违规。

周期性访问查看和证明

Identity Manager 提供了用于处理访问查看的进程，通过访问查看，管理员或其他责任方可以查看并验证用户访问权限。该进程有助于识别和管理随时间累积的用户权限，还有助于维护沙宾法案 (Sarbanes-Oxley)、GLBA 以及其他联邦管制委托授权的遵循性。

可以根据需要执行访问查看，也可以调度为定期执行（例如每个日历季度执行一次），这使您可以执行周期性访问查看，以维护正确级别的用户权限。访问查看可以包括审计策略扫描（可选）。

关于周期性访问查看

周期性访问查看是用于证明在某个特定的时间点，一组雇员对相应的资源具有适当权限的周期性进程。

周期性访问查看包括以下活动：

- **访问查看扫描**。执行基于规则的**用户权利**评估以确定是否需要证明的扫描。
- **证明**。通过批准或拒绝用户权利来响应证明请求的进程。

用户权利是在一组特定资源上的用户帐户的详细信息记录。

访问查看扫描

要启动周期性访问查看，必须首先至少定义一个访问扫描。

访问扫描定义了将进行扫描的对象、扫描的资源、扫描过程中要评估的所有可选审计策略，以及用于确定要手动证明的权利记录以及执行者的规则。

访问查看工作流进程

通常，Identity Manager 访问查看工作流可以：

- 构建用户列表、获取每个用户的帐户信息，以及评估可选审计策略
- 创建用户权利记录
- 确定每个用户权利记录是否需要证明
- 向每个证明者分配工作项目
- 等待所有证明者批准或等待首次拒绝
- 如果在指定的超时时间段内未收到对请求的任何响应，则提升到下一个证明者
- 使用解决方案更新用户权利记录

有关修正权能的描述，请参见第 428 页中的 “访问查看修正”。

所需的管理员权能

要执行周期性访问查看并管理查看进程，用户必须具有“审计者周期性访问查看管理员”权能。具有 Auditor 访问扫描管理员权能的用户可创建并管理访问扫描。

要分配这些权能，请编辑用户帐户并修改安全属性。有关这些权能及其他权能的详细信息，请参见第 6 章，管理中的第 184 页中的 “了解和管理权能”。

证明进程

证明是由一个或多个指定的证明者执行的认证进程，以确认在特定日期用户权利的适当性。在访问查看过程中，证明者会通过电子邮件通知接收访问查看证明请求的通知。证明者必须是 Identity Manager 用户，但无需是 Identity Manager 管理员。

证明工作流

Identity Manager 使用证明工作流，该工作流在访问扫描标识需要查看的权利记录后启动。访问扫描将根据其中定义的规则进行确定。

由访问扫描评估的规则将确定是否需要手动证明用户权利记录，或是否可自动批准或拒绝该记录。如果需要手动证明用户权利记录，访问扫描将使用第二条规则来确定适当的证明者。

要手动证明的每个用户权利记录均将分配给工作流，每个证明者负责一个工作项目。给这些工作项目证明者的通知可使用 ScanNotification 工作流发送，对于每个证明者，该工作流可在每次扫描时将这些项目捆绑到一个通知中。除非已选定 ScanNotification 工作流，否则向每个用户权利发送通知。这表示每次扫描时证明者可接收多个通知，并且通知数目可能较大（取决于扫描的用户数）。

证明安全访问

这些验证选项用于 authType `AttestationWorkItem` 的工作项目：

- 工作项目拥有者
- 工作项目拥有者的直接或间接管理员
- 控制工作项目拥有者所属组织的管理员
- 已通过验证检查验证的用户

默认情况下，验证检查的行为是以下行为**之一**：

- 所有者为尝试执行该操作的用户
- 所有者位于由尝试执行该操作的用户控制的组织中
- 所有者为尝试执行该操作的用户的下属

第二个和第三个检查可通过修改以下表单属性单独配置：

- `controlOrg` — 有效值为 true 或 false
- `subordinate` — 有效值为 true 或 false
- `lastLevel` — 包括在结果中的最后一个下属级别；`-1` 表示所有级别

`lastLevel` 的整数值默认为 `-1`，表示直接或间接下属。

可以在以下位置添加或修改这些选项：

用户表单：访问批准列表。

注 – 如果将证明安全设置为受组织控制，则还需要“审计者证明者”权能以修改其他用户的证明。

委托证明

默认情况下，访问扫描工作流会优先处理用户为证明工作项目和通知所创建的“访问查看证明”和“访问查看修正”类型的委托。访问扫描管理员可取消选择“按照委托”选项以忽略委托设置。如果证明者已将所有工作项目委托给另一用户，但尚未为访问查看扫描设置“按照委托”选项，则该证明者（**而非**已向其分配委托的用户）将收到证明请求通知和工作项目。

计划进行周期性访问查看

对于任何企业，访问查看都是一个费时费力的过程。Identity Manager 周期性访问查看通过自动执行进程的诸多步骤，有助于将成本和时间降至最低。但是，某些进程仍然十分耗时。例如，从数以千计的用户的多个位置获取用户帐户数据的进程就十分耗时。手动证明记录的操作同样十分耗时。合理的计划可提高进程的效率，并极大地降低投入。

计划进行周期性访问查看需要注意以下事项：

- 根据所涉及的用户数和资源数，扫描时间将有很大的差别。

  对大型组织进行一次周期性访问查看时，扫描会耗费一天或多天的时间，而完成手动证明则需一周或多周的时间。

  例如，对于具有 50,000 个用户和十个资源的组织，根据以下计算，完成访问扫描可能需要约一天的时间：

  1 秒/资源 * 50K 用户 * 10 资源 / 5 并发线程 = 28 小时

  如果资源分布于各地，则网络时延会增加进程时间。

- 使用多个 Identity Manager 服务器进行并行处理将提高访问查看进程的速度。

  当扫描的并非公共资源时，运行并行扫描最为有效。定义访问查看时，通过对每个扫描使用不同资源来创建多个扫描并将资源限制为特定的一组资源。然后，启动任务时，选择多个扫描并将它们调度为立即运行。

- 自定义证明工作流以及规则增强了您的控制能力，并带来了更高的效率：

  例如，自定义 "Attestor" 规则可将证明任务扩展到多个证明者。证明进程将相应地分配工作项目并发送通知。

- 使用 "Attestor Escalation Rules" 有助于缩短证明请求的响应时间。

  设置 "Default Escalation Attestor" 规则或使用自定义规则来设置证明者的提升链。另外，指定提升超时值。

- 了解如何使用 "Review Determination Rules" 通过自动确定要手动查看的权利文件记录来节省时间。
- 通过指定扫描级别通知工作流来捆绑扫描的证明请求通知。

调节扫描任务

在扫描过程中，有多个线程会访问用户的视图，还可能访问用户具有帐户的资源。访问视图之后，会对多个审计策略和规则进行评估，这可能会导致创建遵循性违规。

为了防止两个线程同时更新相同的用户视图，该过程将针对此用户名建立一个内存中的锁定。如果无法在 5 秒（默认值）之内建立此锁定，则会向扫描任务中写入一个错误并跳过该用户，从而防止对同一组用户进行并发扫描。

可以编辑多个“可调节参数”的值，这些参数是作为任务参数提供给扫描任务的：

- `clearUserLocks`（布尔值）。如果为 true，将在扫描开始前解除所有当前用户锁定。
- `userLock`（整数）。尝试锁定用户时等待的时间（以毫秒为单位）。默认值为 5 秒。负值将禁用对该扫描的锁定。
- `scanDelay`（整数）。分发扫描线程之间的休眠时间（以毫秒为单位）。默认值为 0（无延迟）。如果为此参数提供值，则扫描速度会变慢，但系统对其他操作的响应能力将变强。
- `maxThreads`（整数）。用于处理扫描的并发线程数。默认值为 5。如果资源的响应速度很慢，则增大此数值可能会提高扫描吞吐量。

要更改这些参数的值，请编辑相应的“任务定义”表单。有关详细信息，请参见《Sun Identity Manager Deployment Reference》中的第 2 章 “Identity Manager Forms”。

创建访问扫描

▼ 定义访问查看扫描

1. **选择“遵循性”→“管理访问扫描”。**
2. **单击“新建”以显示“创建新的访问扫描”页。**
3. **为访问扫描指定名称。**

注 – 访问扫描名称不能包含以下字符：

'（撇号）、.（句点）、|（管道符号）、[（左括号）、]（右括号）、,（逗号）、:（冒号）、$（美元符号）、"（双引号）、\（反斜杠）或 =（等号）

另外，还要避免使用以下字符：_（下划线）、%（百分号）、^（插入符号）和 *（星号）

---

4. **添加有助于识别扫描的描述（可选）。**
5. **启用“动态权利”选项为证明者提供附加选项。**

   这些选项包括：

   - 可以立即重新扫描暂挂证明，以刷新权利数据并重新评估证明需求。
   - 可以将暂挂证明路由到其他用户以进行修正。进行修正后，权利数据会被刷新并重新评估，以确定证明的必要性。
6. **指定“用户范围类型”（必需）。**

从以下选项中进行选择：

- **根据属性条件规则**。根据选定的用户范围规则扫描用户。

  Identity Manager 提供了以下默认规则：

  - 所有管理员

    注 – 可通过使用 Identity Manager IDE 来添加用户范围规则。有关 Identity Manager IDE 的信息，请访问 `https://identitymanageride.dev.java.net/`。

  - 我的所有下属
  - All Non-Administrators
  - 我的直接下属
  - Users without a Manager
- **分配给资源**。扫描在一个或多个选定资源上具有帐户的所有用户。选择此选项后，页面将显示“用户范围资源”，可以用其指定资源。
- **根据特定角色**。扫描至少包含指定的一个角色或包含指定的所有角色的所有成员。
- **组织成员**。选择该选项可扫描一个或多个选定组织的所有成员。
- **报告给管理员**。扫描已报告给选定管理员的所有用户。管理员层次结构取决于用户的 Lighthouse 帐户的 Identity Manager 属性。

  如果用户范围为**组织**或**管理员**，则可使用“递归范围”选项。此选项允许按受控成员链进行递归式用户选择。

7 如果您选择同时扫描审计策略以便在访问查看扫描期间检测违规，请通过将您的选项从“可用审计策略”移动到“当前审计策略”列表，来选择要应用到此扫描的审计策略。

向访问扫描结果中添加审计策略的行为与在同一用户组中执行审计扫描的行为相同。但是，除此之外，由审计策略检测到的任何违规都将存储在用户权利记录中。此信息可简化自动批准或拒绝，因为该规则可将用户权利记录中是否存在违规作为其逻辑的一部分。

8 如果在上述步骤中扫描了审计策略，则可以使用“策略模式”选项指定访问扫描如何确定要为给定用户执行的审计策略。用户可同时具有按用户级别和/或组织级别分配的策略。默认的访问扫描行为将在用户仍不具有任何指定策略时才应用指定给访问扫描的策略。

a. 应用选定策略并忽略其他分配

b. 仅在用户尚不具有任何分配时才应用选定策略

c. 除了分配给用户的策略外，还应用选定策略

9 **（可选）指定查看进程所有者。使用此选项可指定已定义的访问查看任务的拥有者。如果已指定一个查看进程拥有者，则对于在响应证明请求时遇到潜在冲突的证明者，他可以选择放弃而无需批准或拒绝用户权利，并且证明请求将会转发给该查看进程拥有者。单击选择框（省略号）可搜索用户帐户并进行选择。**

10 **按照委托。选择此选项可以对访问扫描启用委托。如果已选中此选项，访问扫描将仅应用委托设置。默认情况下将启用"按照委托"。**

11 **限制目标资源。选择此选项可限制扫描目标资源。**

此设置会对访问扫描的效率产生直接的负面影响。如果未限制目标资源，每个用户权利记录均将包括用户链接到的每个资源的帐户信息。这表示在扫描期间将为每个用户查询所有分配的资源。通过使用该选项指定资源的子集，您可以大大缩短 Identity Manager 创建用户权利记录所需的处理时间。

12 **执行违规修正。选择该选项可在检测到违规时启用审计策略的修正工作流。**

如果选择此选项，则针对任何分配的审计策略所检测到的违规将导致执行相应审计策略的修正工作流。

通常不应该选择此选项，除非情况比较复杂。

13 **访问批准工作流。选择默认的标准证明工作流或选择自定义的工作流（如果有）。**

此工作流用于将要查看的用户权利记录显示给适当的证明者（如同由证明者规则确定）。默认的标准证明工作流为每个证明者创建一个工作项目。如果访问扫描指定了升级，此工作流将负责升级暂停过久的工作项目。如果未指定任何工作流，则用户证明将无限期地处于暂挂状态。

.

注 – 有关在此步骤和以下步骤中提到的 Identity Auditor 规则的详细信息，请参见《Sun Identity Manager Deployment Reference》中的第 4 章 "Working with Rules"。

---

14 **证明者规则。选择默认的证明者规则，或选择自定义的证明者规则（如果有）。**

证明者规则将作为输入值提供给用户权利记录，并且返回证明者名称列表。如果选择了"按照委托"，则访问扫描将按照原始名称列表中每个用户所配置的委托信息，把名称列表转换成相应用户。如果 Identity Manager 用户的委托导致路由循环，则将放弃委托信息，并且工作项目将提交给原始证明者。**默认证明者**规则指示证明者应该是权利记录所代表的用户的管理员 (idmManager)，或者是配置器帐户（如果该用户的 `idmManager` 为 null）。如果证明需包括资源拥有者以及管理员，则必须使用自定义规则。

15 证明者提升规则。使用此选项可指定"默认提升证明者"规则，或选择自定义规则（如果可用）。您也可以为规则指定升级超时值。默认的提升超时值为 0 天。

该规则将为已经过升级超时时间段的工作项目指定升级链。"默认提升证明者"规则将提升到所分配的证明者的管理员 (`idmManager`)，或提升到配置器（如果证明者的 `idmManager` 值为 null）。

您可以以分钟、小时或天数为单位指定升级超时值。

手册包含有关证明者提升规则的其他信息。

16 查看确定规则。（必需）

选择以下规则之一以指定扫描进程将如何确定部署权利记录：

- **拒绝更改的用户**。自动拒绝用户权利记录，如果该用户权利与上一个具有相同访问扫描定义的用户权利不同，且已批准上一个用户权利。否则，强制执行手动证明并批准所有与先前已批准的用户权利相同的用户权利。默认情况下，此规则只比较用户视图的"帐户"部分。
- **查看更改的用户**。强制执行手动证明任一用户权利记录，如果该用户权利与上一个具有相同访问扫描定义的用户权利不同，且已批准上一个用户权利。批准所有与先前已批准的用户权利相同的用户权利。默认情况下，此规则只比较用户视图的"帐户"部分。
- **查看所有人**。强制执行手动证明所有用户权利记录。

"Reject Changed Users" 和 "Review Changed Users" 规则将比较用户权利和相同访问扫描（其中已批准权利记录）的上一个实例。

您可以通过复制并修改规则来更改此行为，以便将比较操作限制在用户视图的任何选定部分。

此规则可以返回以下值：

- **-1**. 不需要证明
- **0**. 自动拒绝证明
- **1**. 需要手动证明
- **2**. 自动批准证明
- **3**. 自动修正证明（自动修正）

手册包含有关查看确定规则的其他信息。

17 修正者规则。选择要使用的规则，以确定在自动修正的情况下，应由谁修正特定用户的权利。该规则可以检查用户的当前用户权利和违规，并且必须返回应该负责修正的用户的列表。如果未指定任何规则，则不会执行任何修正。权利具有遵循性违规时通常会使用此规则。

18 **修正用户表单规则。选择规则，用于在编辑用户时为证明修正者选择相应的表单。修正者可以设置自己的表单（将覆盖此表单）。如果扫描搜集与自定义表单匹配的特定数据，则应设置此表单规则。**

19 **通知工作流。**

选择以下选项之一可为每个工作项目指定通知行为。

- **无**。此选项为默认选项。此选项可导致证明者会因他必须证明的每个用户权利而收到一封电子邮件通知。
- **ScanNotification**。此选项可将证明请求捆绑到单个通知中。通知可指示分配给收件人的证明请求数目。

  如果访问扫描中指定了查看进程拥有者，则 ScanNotification 工作流还将在扫描开始和结束时向查看进程拥有者发送通知。请参见第 416 页中的 “创建访问扫描”。

  ScanNotification 工作流使用以下电子邮件模板：

  - 访问扫描开始通知
  - 访问扫描结束通知
  - 批量证明通知

    您可以自定义 ScanNotification 工作流。

20 **违规限制。使用该选项可指定扫描在异常中止之前可发出的最大遵循性违规数。默认限制为 1000。值字段为空表示无限制。**

虽然通常情况下在审计扫描或访问扫描期间，策略违规数目与用户数目相比相对较小，但是设置此值可提供保护，以免受可大量增加违规数目的有缺陷策略的影响。例如，请考虑以下情况：

如果访问扫描涉及 50,000 个用户并为每个用户生成两到三个违规，则对每个遵循性违规的修正成本可能会对 Identity Manager 系统产生不利影响。

21 **组织。选择可使用此访问扫描对象的组织。此字段为必填字段。**

单击“保存”可保存扫描定义。

删除访问扫描

您可以删除一个或多个访问扫描。要删除访问扫描，请从“遵循性”选项卡中选择“管理访问扫描”，选择扫描名称，然后单击“删除”。

管理访问查看

定义访问扫描之后，即可将其作为访问查看的一部分使用或调度。启动访问查看之后，可使用多个选项管理查看进程。

请阅读以下各节以了解详细信息：

- 第 421 页中的“启动访问查看”
- 第 421 页中的“调度访问查看任务”
- 第 422 页中的“管理访问查看进度”
- 第 423 页中的“修改扫描属性”
- 第 423 页中的“取消访问查看”
- 第 424 页中的“删除访问查看”

启动访问查看

要从管理员界面启动访问查看，请使用以下方法之一：

- 单击“遵循性”→“访问查看”页中的“启动查看”。
- 在“服务器任务”→“运行任务”页中选择“访问查看”任务。

在所显示的“启动任务”页中，指定访问查看的名称。从 "Available Access Scans" 列表中选择扫描并将其移动至 "Selected" 列表。

如果选择了多个扫描，则可以选择以下启动选项之一：

- **立即**。选择此选项后，单击“启动”按钮时将立即开始运行扫描。如果在启动任务中为多个扫描选择了此选项，则扫描将并行运行。
- **等待**。此选项可使您指定在启动扫描之前等待的时间，该时间与访问查看任务的启动相关。

注 – 您可以在访问查看会话期间启动多个扫描。但是，考虑到每个扫描可能涉及大量的用户，因此要完成扫描进程可能要耗费数小时的时间。最佳实践证明您可以分别管理扫描。例如，您可以启动某个扫描以立即运行，并调度其他扫描在错开的时间进行。

单击“启动”可启动访问查看进程。

注 – 分配给访问查看的名称很重要。某些报告可能会对具有相同名称的周期性运行的访问查看进行比较。

启动访问查看时，将显示工作流程图以指明该进程中执行的步骤。

调度访问查看任务

可从 "Server Tasks" 区域中调度访问查看任务。例如，要设置周期性访问查看，请选择“管理进度表”，然后定义进度表。您可以将任务调度为每月或每季度发生一次。

要定义进度表，请在“调度任务”页中选择“访问查看”任务，然后填写“创建任务进度表”页上的信息。

单击“保存”以保存已调度的任务。

注 – 默认情况下，Identity Manager 可将访问查看任务的结果保留一周。如果选择在不到一周的时间内即调度一次查看，请将“结果选项”设置为删除。如果 "Results Options" 未设置为删除，则不会运行新的查看，因为先前任务的结果仍然存在。

管理访问查看进度

使用 "Access Reviews" 选项卡可监视访问查看的进度。可通过“遵循性”选项卡访问该功能。

在“访问查看”选项卡中，您可以查看所有活动的和以前处理的访问查看的摘要。以下信息会提供给所列出的每个访问查看：

- **状态**。查看进程的当前状态：正在启动、正在终止、已终止、正在执行的扫描数、已调度的扫描数、等待证明或已完成。
- **启动日期**。启动访问查看任务的日期（时间戳）。
- **用户总数**。要扫描的用户总数。
- **权利详细信息**。表中的附加列，按状态提供权利总数。其中包括暂挂、已批准、已拒绝、已终止和已修正的权利的详细信息，以及权利总数。

  “已修正”列指出当前处于 REMEDIATING 状态的权利数。权利在修正后将变为 PENDING 状态，因此在访问查看结束后，此列的值为零。

要查看关于查看的更多详细信息，请选择该查看以打开摘要报告。

图 15–5 显示了示例访问查看摘要报告。

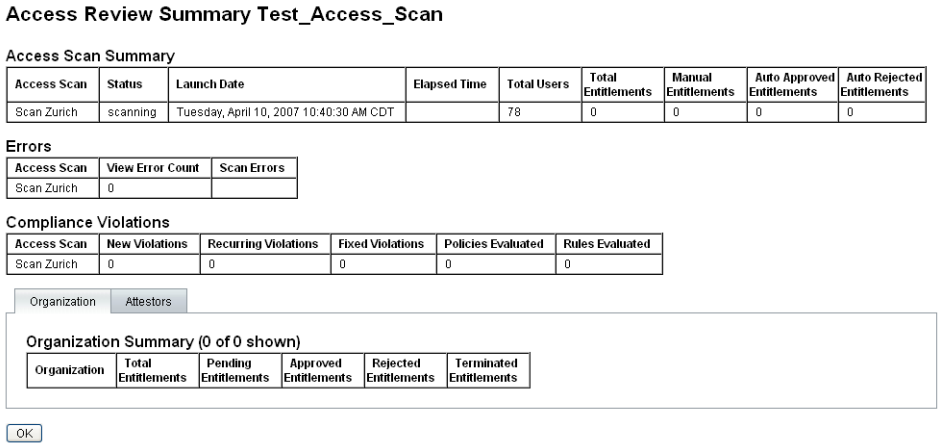


图 15–5 “访问查看摘要报告”页

单击“组织”或“证明者”表单选项卡可查看按这些对象进行分类的扫描信息。

您还可以通过运行 "Access Review Summary Report" 在报告中查看和下载这些信息。

修改扫描属性

设置访问扫描之后，您可以编辑扫描以指定新选项，例如指定要扫描的目标资源或指定运行访问扫描时要为违规扫描的审计策略。

要编辑扫描定义，请从“访问扫描”列表中将其选中，然后在“编辑访问查看扫描”页中修改属性。

必须单击“保存”才能保存对扫描定义所做的所有更改。

注 – 更改访问扫描的范围可能会更改新获得的用户权利记录中的信息，因为如果“查看确定规则”对用户权利和以前的用户权利记录进行比较，则更改可能会对此规则产生影响。

取消访问查看

在“访问查看”页中，单击“终止”可停止进行中的选定查看。

终止查看将导致以下操作：

- 取消调度所有已调度的扫描
- 停止所有活动的扫描
- 删除所有暂挂工作流和工作项目
- 所有暂挂证明都被标记为已取消
- 用户已完成的所有证明将保留不变

删除访问查看

在“访问查看”页中，单击“删除”可删除选定的查看。

如果访问查看任务的状态为**已终止**或**已完成**，则可以删除该访问查看。无法删除正在进行中的访问查看任务，除非先将其终止。

删除访问查看将删除由该查看生成的所有用户权利记录。删除操作将记录在审计日志中。

要删除访问查看，请单击“访问查看”页中的“删除”。

注 – 取消和删除访问查看可能导致对大量 Identity Manager 对象和任务进行更新，完成该过程可能需要几分钟的时间。可以通过在“服务器任务”→“所有任务”中查看任务结果来检查操作的进度。

管理证明责任

您可以从 Identity Manager 管理员界面或用户界面中管理证明请求。本节提供了有关响应证明请求以及证明中包含的责任的信息。

访问查看通知

在扫描期间，当证明请求需要证明者的批准时，Identity Manager 会向证明者发送通知。如果已委托证明者职责，则将请求发送给委托者。如果定义了多个证明者，则每个证明者都将收到一封电子邮件通知。

请求将显示为 Identity Manager 界面中的证明工作项目。当已分配的证明者登录到 Identity Manager 时，屏幕将显示暂挂的证明工作项目。

查看暂挂证明请求

从界面的“工作项目”区域查看证明工作项目。选择“工作项目”区域中的“证明”选项卡，即可列出所有需要批准的权利记录。在“证明”页中，您还可以列出所有直接报告和指定用户（您可对其进行直接或间接控制）的权利记录。

对权利记录执行操作

证明工作项目包含需要查看的用户权利记录。权利记录提供了有关用户访问权限、已分配资源以及策略违规的信息。

对证明请求可能会做出以下响应：

- **批准**。证明从权利记录中所记录的日期开始，权利是适当的。
- **拒绝**。权利记录指出当前无法验证或修正的可能差异。

- **重新扫描**。请求重新扫描以重新评估用户权利。
- **转发**。可使您为查看指定其他收件人。
- **放弃**。对此记录的证明不合适，并且尚未发现更合适的证明者。证明工作项目将转发至查看进程拥有者。仅在访问查看任务中已定义查看进程拥有者时，才可使用此选项。

如果在指定的升级超时时间段之前，证明者未采取以上任何一种操作对请求进行响应，则通知将发送至升级链中的下一个证明者。在记录响应之前，通知进程将继续。

可以从“遵循性”→“访问查看”选项卡中监视证明状态。

闭环修正

您可以避免拒绝用户权利，方法如下：

- 将权利标记为需要请求其他用户进行修复（请求修正）。在这种情况下，将创建一个新的修正工作项目，并将其分配给一个或多个指定的修正者。

  接着，新的修正者可以选择编辑用户（使用 Identity Manager 或独立编辑），然后在工作项目达到要求后将其标记为已修正。此时，将对用户权利进行重新扫描和再次评估。
- 请求对权利进行重新评估（重新扫描）。在这种情况下，将对用户权利进行重新扫描和再次评估。原始的证明工作项目将会结束。根据访问扫描中定义的规则，如果权利仍需要证明，将创建一个新的证明工作项目。

请求修正

您可以将暂挂证明路由到其他用户以进行修正（如果访问扫描已定义此操作）。

注 – 可以通过“创建访问扫描”或“编辑访问扫描”页上的“动态权利”选项启用此功能。

▼ 从其他用户请求修正

1. **从证明列表中选择一个或多个权利，然后单击“请求修正”。**

   将显示“选择并确认请求修正”页。

2. **输入用户名，然后单击“添加”将该用户添加到“转发至”字段。或者，单击 ...（更多）以搜索用户。在搜索列表中选择用户，然后单击“添加”将该用户添加到“转发至”列表。单击“解除”可关闭搜索区域。**

3. **在“注释”字段输入注释，然后单击“继续”。**

   Identity Manager 将返回到证明列表。

注 – 修正请求的详细信息将显示在各用户权利的“历史”区域中。

重新扫描证明

您可以对暂挂证明进行重新扫描和重新评估（如果访问扫描已定义此操作）。

注 – 可以通过“创建访问扫描”或“编辑访问扫描”页上的“动态权利”选项启用此功能。

▼ 重新扫描暂挂证明

1. **从证明列表中选择一个或多个权利，然后单击“重新扫描”。**
   将显示“重新扫描用户权利”页。
2. **在“注释”区域输入有关重新扫描操作的注释，然后单击“继续”。**

转发证明工作项目

可以将一个或多个证明工作项目转发至其他用户。

▼ 转发证明

1. **在证明列表中选择一个或多个工作项目，然后单击“转发”。**
   将显示“选择并确认转发”页。
2. **在“转发至”字段中输入用户名。或者，单击 "..."（更多）以搜索用户名。**
3. **在“注释”字段中输入有关转发操作的注释。**
4. **单击“继续”。**
   Identity Manager 将返回到证明列表。

注 – 转发操作的详细信息将显示在各用户权利的“历史”区域中。

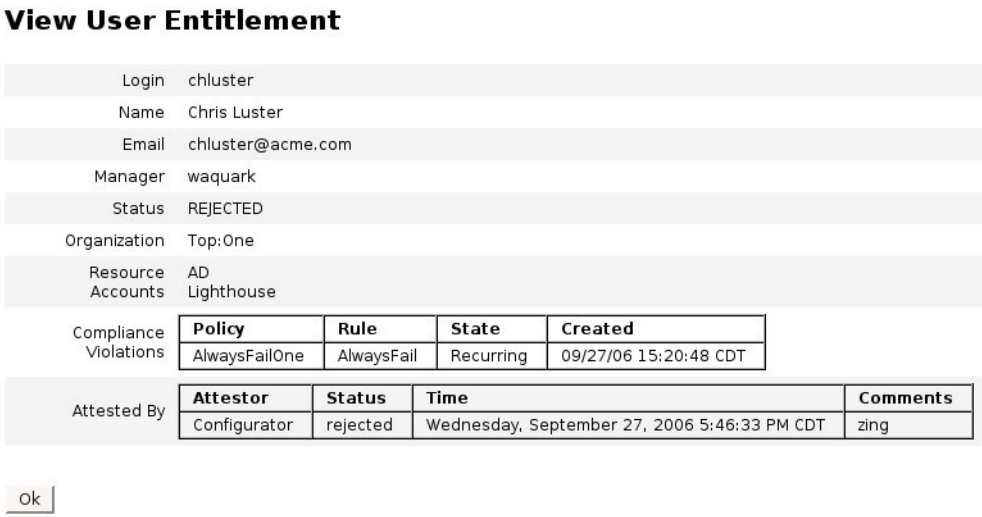
对访问查看操作进行数字签名

您可以设置数字签名以处理访问查看操作。有关配置数字签名的信息，请参见第 203 页中的 “对批准签名”。此处讨论的主题说明了将证书和 CRL 添加到 Identity Manager 以获得签名批准时所需的服务器端和客户端配置。

访问查看报告

Identity Manager 提供了以下报告，您可以使用这些报告评估访问查看的结果：

- **访问查看覆盖报告**。以表格形式提供包含用户权利重叠和/或差异的用户列表，具体取决于定义报告的方式。此报告还可能包含其他列，用于显示包含重叠和/或差异的访问查看。
- **访问查看详细信息报告**。该报告以表格形式提供了以下信息：
  - **名称**。用户权利记录的名称
  - **状态**。查看进程的当前状态：正在启动、正在终止、已终止、正在执行的扫描数、已调度的扫描数、等待证明或已完成
  - **证明者**。分配为记录证明者的 Identity Manager 用户
  - **扫描日期**。记录扫描何时发生的时间戳
  - **处理日期**。证明权利记录的日期（时间戳）
  - **组织**。权利记录中的用户组织
  - **管理器**。已扫描用户的管理员
  - **资源**。用户拥有其帐户且已捕获至该用户权利的资源
  - **违规**。查看期间检测到的违规数目
  - 单击报告中的名称可打开用户权利记录。第 427 页中的 “访问查看报告”显示了用户权利记录视图中提供的信息示例。



View User Entitlement

Login	chluster
Name	Chris Luster
Email	chluster@acme.com
Manager	waquark
Status	REJECTED
Organization	Top:One
Resource Accounts	AD Lighthouse

Compliance Violations

Policy	Rule	State	Created
AlwaysFailOne	AlwaysFail	Recurring	09/27/06 15:20:48 CDT

Attested By

Attestor	Status	Time	Comments
Configurator	rejected	Wednesday, September 27, 2006 5:46:33 PM CDT	zing

Ok

- **访问查看摘要报告**。

此报告（已在第 422 页中的 “管理访问查看进度”中讨论，并在图 15–5 中展示）显示有关为报告选择的访问扫描的以下摘要信息：

- **查看名称**。访问扫描的名称
- **日期**。启动查看的时间戳
- **用户计数**。为查看扫描的用户数目
- **权利计数**。生成的权利记录数目
- **已批准**。已批准的权利记录数目
- **已拒绝**。已拒绝的权利记录数目
- **暂挂**。仍处于暂挂状态的权利记录数目
- **已取消**。已取消的权利记录数目

这些报告均可从“运行报告”页以可移植文档格式 (PDF) 或逗号分隔值 (CSV) 格式下载。

访问查看修正

可以在“工作项目”选项卡的“修正”区域中管理遵循性违规修正和缓解以及访问查看修正。但是，这两种修正类型之间存在着差异。本节介绍了访问查看修正的特有行为，以及它与第 404 页中的 “遵循性违规修正和缓解”中所述的修正任务和信息之间的差异。

关于访问查看修正

证明者请求修正用户权利时，“标准证明”工作流将创建一个修正请求，该请求必须由修正者（可以评估和响应修正请求的指定用户）进行处理。

只能修正问题，而无法缓解问题。必须在问题解决之后，证明才能继续。

访问查看产生修正后，“访问查看”面板将跟踪与该查看有关的所有证明者和修正者。

访问查看修正请求提升

访问查看修正请求最高只能提升至初始修正者。

修正工作流进程

访问查看修正的逻辑是在“标准证明”工作流中定义的。

证明者请求修正用户权利时，“标准证明”工作流将执行以下操作：

- 生成修正请求（类型为 `accessReviewRemediation`），其中包含需要修正的用户权利的有关信息。
- 向请求的修正者发送电子邮件。

接着，新的修正者可以选择编辑用户（使用 Identity Manager 或独立编辑），然后在工作项目达到要求后将其标记为已修正。此时，将对用户权利进行重新扫描和再次评估。

访问查看修正响应

默认情况下，为访问查看修正者提供了三个响应选项：

- **修正**。修正者指示已经为修复问题执行了某些操作。

  接着将对用户权利进行重新扫描和再次评估。如果用户权利再次被标记为需要证明，则原始证明者将在“证明”工作项目列表中再次看到该用户权利。

  修正请求操作的详细信息将显示在各用户权利的“历史”区域中。
- **转发**。修正者将解决修正请求的职责重新分配给另外一个人。

  转发操作的详细信息将显示在各用户权利的“历史”区域中。
- **编辑用户**。修正者选择直接编辑用户以修正问题。

  仅当修正者具有修改用户的权限时才会显示此按钮。更改用户并单击“保存”后，修正者将进入“修正确认”页，以提供用于描述对用户所做更改的注释。

  接着将对用户权利进行重新扫描和再次评估。如果用户权利再次被标记为需要证明，则原始证明者将在“证明”工作项目列表中再次看到该用户权利。

  编辑的详细信息将在各用户权利的“历史”区域中显示为修正请求操作。

“修正”页

对于所有访问查看修正工作项目，“类型”列将显示为 UE（user entitlement，用户权利）。

不支持的访问查看修正操作

访问查看修正不支持排列优先级和缓解功能。

◆ ◆ ◆ 第 16 章

数据导出器

通过使用数据导出器功能，您可以将有关用户、角色和其他对象类型的信息写入到外部数据仓库中。

本章提供的信息和过程可以帮助您设置和维护数据导出器。有关规划和实现数据导出器的完整详细信息，请参见《Sun Identity Manager Deployment Guide》中的第 5 章 “Data Exporter”。

本章采用以下组织形式：

什么是数据导出器？

Identity Manager 包含与在分布式系统和应用程序中管理身份有关的数据并对这些数据进行处理。为提高整体性能，Identity Manager 并不完全保留在正常置备和其他日常活动期间生成的所有数据。例如，默认情况下，Identity Manager 不会保留中间状态工作流活动和任务实例。如果需要捕获 Identity Manager 通常丢弃的全部或部分数据，您可以启用数据导出器功能。

如果启用了数据导出器，则 Identity Manager 会将检测到的每个对指定对象（数据类型）的更改作为记录存储到系统信息库表中。这些事件将排入队列，直到任务将其写入外部数据仓库中为止。（您可以配置每种数据类型的导出频率。）可以对导出的数据执行进一步处理，或者将其作为使用商业转换、报告和分析工具进行的查询和转换的基础。

将数据导出到数据仓库会对 Identity Manager 服务器性能产生不利影响，除非业务上需要导出数据，否则不应启用该功能。

Identity Manager 还允许创建和执行取证查询。取证查询将搜索数据仓库，以找出符合指定条件的用户或角色对象。有关详细信息，请参见第 442 页中的 “配置取证查询”。

计划实现数据导出器

由于默认情况下禁用了数据导出器，因此，必须对其进行配置才能恢复运行。要配置数据导出器，您需要在开始配置之前做出以下决定：

- 将导出哪些数据类型?
- 将使用哪些技术来捕获每种类型的数据?
- 每种数据类型的导出频率是多少?
- 每种类型的导出模式中包含哪些内容?
- 是否需要自定义仓库接口代码 (Warehouse Interface Code, WIC) 工厂类?

在启用数据导出器后，默认配置将导出所有数据类型的所有属性。这可能会消耗从不使用的仓库存储，从而给 Identity Manager 和仓库造成不必要的处理负担。数据仓储具有审慎保守的特点，仅在以后可能会用到数据时才捕获该数据。您不必导出所有可导出的数据。您可以配置要导出的数据类型，并限制导出某些事件。

在做出这些决定后，请使用以下步骤实现数据导出器：

▼ 实现数据导出器

1. （可选）为选定类型自定义导出模式并重新生成仓库 DDL。有关详细信息，请参阅《Sun Identity Manager Deployment Guide》中的“Customizing Data Exporter”。
2. 在仓库 RDBMS 上创建一个用户帐户，并在该系统上加载仓库 DDL。有关详细信息，请参阅《Sun Identity Manager Deployment Guide》中的“Customizing Data Exporter”。
3. 按第 433 页中的“配置数据导出器”中所述配置数据导出器。
4. 测试数据导出器，确保已正确对其进行了配置。有关详细信息，请参见第 441 页中的“测试数据导出器”。
5. （可选）创建可以搜索已写入数据仓库中的数据的取证查询。有关详细信息，请参见第 442 页中的“配置取证查询”。
6. 使用 JMX 并监视日志文件以维护数据导出器。有关详细信息，请参见第 446 页中的“维护数据导出器”。

配置数据导出器

在“数据导出器配置”页中，可以定义要保留的数据类型、指定要导出的属性以及计划数据的导出时间。可以单独配置每种数据类型。

▼ 配置数据导出器

1 **在管理员界面中，单击主菜单中的“配置”。然后单击“仓库”次级选项卡。将打开“数据导出器配置”页。**

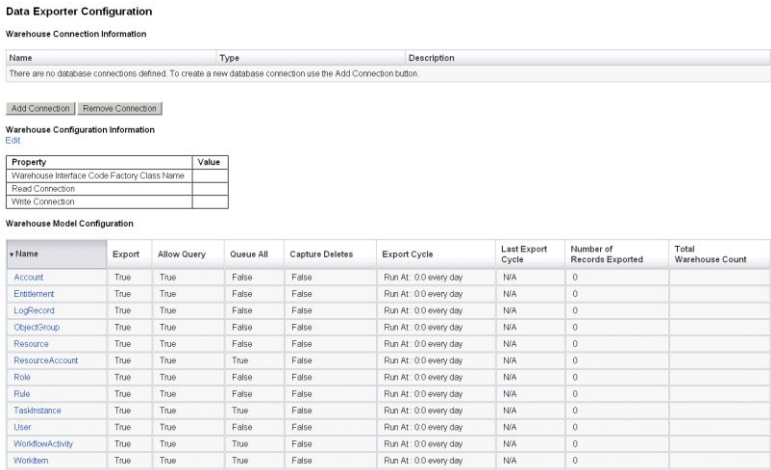


图 16–1 数据导出器配置

2 **要定义读取连接和写入连接，请单击“添加连接”按钮。将打开“编辑数据库连接”页。**

填写该页上的字段，然后单击“保存”以返回到“数据导出器配置”页。有关详细信息，请参见第 434 页中的 “定义读取连接和写入连接”。

3 **要指定 WIC 类和数据库连接，请单击“仓库配置信息”部分中的“编辑”链接。将打开“数据导出器仓库配置”页。**

填写该页上的字段，然后单击“保存”以返回到“数据导出器配置”页。有关详细信息，请参见第 435 页中的 “定义仓库配置信息”。

4 **在“仓库模型配置”表中，单击一个数据类型链接。将打开“数据导出器类型配置”页。**

填写该页上的“导出”、“属性”和“进度表”选项卡，然后单击“保存”以返回到“数据导出器配置”页。有关详细信息，请参见第 436 页中的 “配置仓库模型”。

对于每种数据类型，请重复此步骤。

5 **要配置在导出每种数据类型前后运行的工作流，请单击“导出器自动化”部分中的“编辑”链接。将打开“数据导出器自动化配置”。**

填写该页上的字段，然后单击“保存”以返回到“数据导出器配置”页。有关详细信息，请参见“配置导出器自动化”一节。

6 **要配置导出任务守护进程，请单击“仓库任务配置”部分中的“编辑”链接。将打开“数据导出器仓库配置”页。**

填写该页上的字段，然后单击“保存”以返回到“数据导出器配置”页。有关详细信息，请参见第 439 页中的 “配置仓库任务”。

注 – 在完成这些步骤后，即可完全正常运行导出。在启用导出后，数据记录将开始排队以进行导出。如果未启用导出任务，队列表将填满，然后排队将暂停。通常，小批导出（更频繁）比大批导出效率更高，但导出受制于仓库本身的写入可用性，这种可用性可能会由于其他原因而受到限制。

---

7 **（可选）设置队列的最大大小。有关详细信息，请参见第 441 页中的“修改配置对象”。**

定义读取连接和写入连接

Identity Manager 在导出周期内使用写入连接。Identity Manager 使用读取连接指示仓库中当前（在仓库配置期间）有多少条记录以及为取证查询界面提供服务。

可以将仓库连接定义为应用服务器数据源、JDBC 连接或对数据库资源的引用。如果定义了 JDBC 连接或数据库资源，数据导出将在写入操作期间大量使用少数几个连接，然后关闭所有连接。在仓库配置和取证查询执行期间，数据导出器仅使用读取连接，并在操作完成后立即关闭这些连接。

导出器对写入连接和读取连接使用相同的模式，并且您可以对两者使用相同的连接信息。不过，如果使用单独的连接，部署可以向一组仓库临时表中写入内容，将这些表转换为实际仓库，然后将仓库表转换为 Identity Manager 从中读取数据的数据市场。

可以编辑“数据导出配置”表单以禁止 Identity Manager 从仓库中读取数据。此表单包含 `includeWarehouseCount` 属性，它可导致 Identity Manager 查询仓库并显示每种数据类型的记录数。要禁用此功能，请复制“数据导出配置”表单，将 `includeWarehouseCount` 属性值更改为 `true`，然后导入自定义表单。

▼ 定义读取连接和写入连接

1 **在“数据导出器配置”页中，单击“添加连接”按钮。**

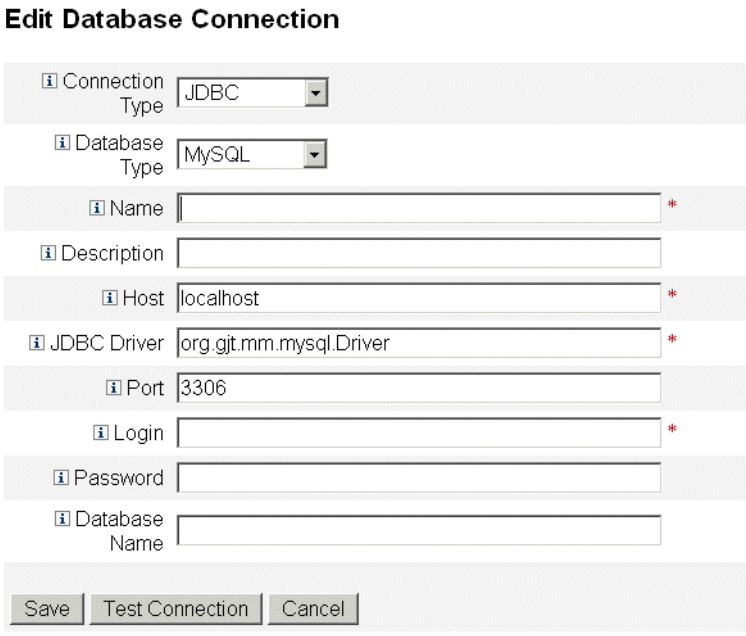


图 16–2 数据导出器配置

2 **可通过从“连接类型”下拉菜单中选择一个选项，指定 Identity Manager 如何建立到数据仓库的读取连接或写入连接。**

- **JDBC**。使用 Java 数据库连接 (Java Database Connectivity, JDBC) 应用程序编程接口连接到数据库。连接池是由仓库接口代码提供的。
- **资源**。使用在资源中定义的连接信息。连接池是由仓库接口代码提供的。
- **数据源**。将基础应用服务器用于连接管理和连接池。这种类型的连接从应用服务器中请求连接。

  根据从**连接类型**下拉菜单中选择的选项，页面上显示的字段可能会有所不同。有关配置数据库连接的详细信息，请参阅联机帮助。

3 **单击“保存”以保存配置更改，并返回到“数据导出器配置”页。**

如果使用单独的读取连接和写入连接，请重复此过程。

定义仓库配置信息

要配置仓库，您必须选择读取连接和写入连接，并指定仓库接口代码工厂类。WIC 工厂类提供了 Identity Manager 和仓库之间的接口。Identity Manager 提供了一个默认代码

实现，但您也可以生成自己的代码。有关创建自定义工厂类的信息，请参见《Sun Identity Manager Deployment Guide》中的第 5 章 “Data Exporter”。

在执行导出任务的 Identity Manager 服务器以及任何配置了数据导出器的服务器上，`$WSHOME/exporter` 目录中必须存在包含工厂类的 `jar` 文件以及任何提供支持的 `jar` 文件。在任何给定时间，只有一个 Identity Manager 服务器可以导出数据。

▼ 定义仓库配置信息

1 **在“数据导出器配置”页中，单击“仓库配置信息”部分中的“编辑”链接。**

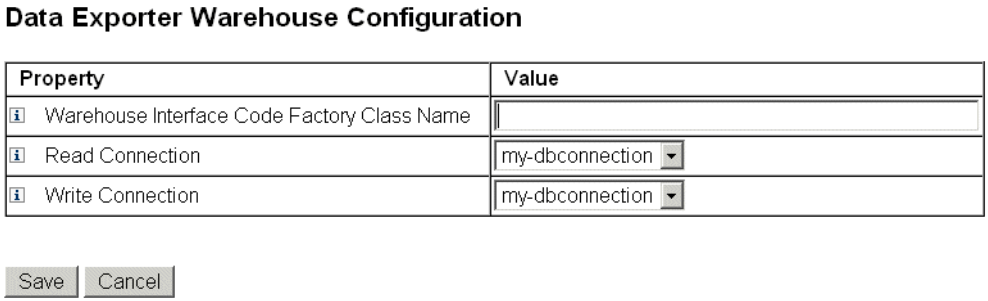


图 16–3 数据导出器配置

2 **在“仓库接口代码工厂类名称”字段中指定一个值。如果集成人员未创建自定义类，请输入值 `com.sun.idm.warehouse.base.Factory`。**

3 **从“读取连接”和“写入连接”下拉菜单中选择选项以指定连接。**

4 **单击“保存”以保存配置更改，并返回到“数据导出器配置”页。**

配置仓库模型

每个可导出的数据类型都具有一组选项，用于控制是否导出该类型、如何导出该类型以及何时导出该类型。导出数据会增加 Identity Manager 服务器上的负载，因此应该仅为业务需要的数据类型启用导出操作。

下表描述了可以导出的每种数据类型。

表 16–1 支持的数据类型

数据类型	描述
帐户	包含用户和资源帐户之间的关联的记录
管理员组	一组适用于所有对象组的 Identity Manager 权限
管理员角色	分配给一个或多个对象组的权限
审计策略	针对 Identity Manager 对象评估的规则集合，用于确定是否遵循业务策略。
遵循性违规	包含用户违反审计策略的情况的记录
权利	包含特定用户的证明列表的记录
日志记录	包含单个审计记录的记录
对象组	作为组织模拟的安全容器
资源	置备帐户的系统/应用程序
资源帐户	组成特定资源上的帐户的一组属性
角色	用于访问的逻辑容器
规则	可以由 Identity Manager 执行的逻辑块
任务实例	指示正在执行或已完成的进程的记录
用户	包含零个或多个帐户的逻辑用户。
工作流活动	Identity Manager 工作流的单个活动
工作项目	Identity Manager 工作流中的手动操作

▼ 配置仓库模型

1 **在“数据导出器配置”页中，单击一个数据类型链接。**

2 **在“导出”选项卡中，指定是否导出该数据类型。如果不希望导出该数据类型，请取消选中“导出”复选框，然后单击“保存”。否则，根据需要选择此“导出”选项卡上的其余选项。**

- **允许查询**。控制是否可以查询模型。
- **全部排入队列**。捕获对该类型的对象进行的所有更改。选中此选项可能会显著增加导出器的处理开销。应谨慎使用此选项。
- **捕获删除**。记录删除的所有该类型的对象。选中此选项可能会显著增加导出器的处理开销。应谨慎使用此选项。

3 **在“属性”选项卡中，可以选择将哪些属性指定为取证查询的一部分，以及在查询结果中显示哪些属性。无法从管理员界面中删除默认属性。有关更改默认属性的信息，请参见《 Sun Identity Manager Deployment Guide 》中的第 1 章“Working with Attributes”。**

新属性名称具有以下特征：

- `attrName` — 该属性是一个顶层标量属性。
- `attrName[]` — 该属性是一个具有列表值的顶层属性，列表中的元素为标量。
- `attrName['`*key*`']` — 该属性包含映射值，需要提供具有指定关键字的映射值。
- `attrName[].`*name2* — 该属性是具有列表值的顶层属性，列表中的元素都为结构。*name2* 是被访问结构中的属性。

注 – 如果要将属性导出到 `EXT_RESOURCEACCOUNT_ACCTATTR` 表中，必须选中要导出的每个属性的“审计”框。

---

4 **指定与“进度表”选项卡上的数据类型关联的信息的导出频率。周期相对于服务器上的午夜零点。周期为 20 分钟的导出操作将发生在午夜零点，以及零点过后的第 20 分钟和第 40 分钟。如果尝试导出所需的时间比计划的周期长，则会跳过下一个周期。例如，如果将周期定义为 20 分钟、从午夜零点开始，并且需要 25 分钟才能完成导出，则下次导出将在 0:40 开始。不会执行最初预定在 0:20 进行的导出。**

配置导出器自动化

Identity Manager 允许指定在导出数据前后执行的工作流。

如果发生的事件为取消导出提供了充分的理由，则可以使用周期开始工作流禁止导出。例如，在预定的导出时间，如果在临时表中读取或写入数据的应用程序需要独占访问这些表，则应该取消导出。该工作流应返回值 1 以取消导出。Identity Manager 将创建一条审计记录以指示跳过了导出，并提供错误结果。如果该工作流返回 0，并且未发生错误，则会导出该数据类型。

在导出所有记录后，将运行周期完成工作流。该工作流通常会触发另一个应用程序来处理导出的数据。在该工作流完成后，导出器将检查另一种要导出的数据类型。

`$WSHOME/sample/web/exporter.xml` 文件中提供了示例工作流。导出器工作流的 `subtype` 为 `DATA_EXPORT_AUTOMATION`，`authType` 为 `WarehouseConfig`。

▼ 配置导出器自动化

1 **在“数据导出器配置”页中，单击“导出器自动化”部分中的“编辑”链接。**

2 **（可选）在“周期开始工作流”下拉菜单中，选择一个要在导出前运行的工作流。**

3 **（可选）在“周期开始工作流”下拉菜单中，选择一个要在导出后运行的工作流。**

配置仓库任务

并不要求在专用服务器上运行导出任务；但如果希望导出大量的数据，则应该考虑使用专用服务器。在将数据从 Identity Manager 传输到仓库时，导出任务的效率较高，并且在导出操作期间会占用尽可能多的 CPU。如果没有使用专用服务器，应限制服务器处理交互通信，因为在导出大量数据期间会显著增加响应时间。

▼ 配置仓库配置信息

1 **在“数据导出器配置”页中，单击“仓库任务配置”部分中的“编辑”链接。**

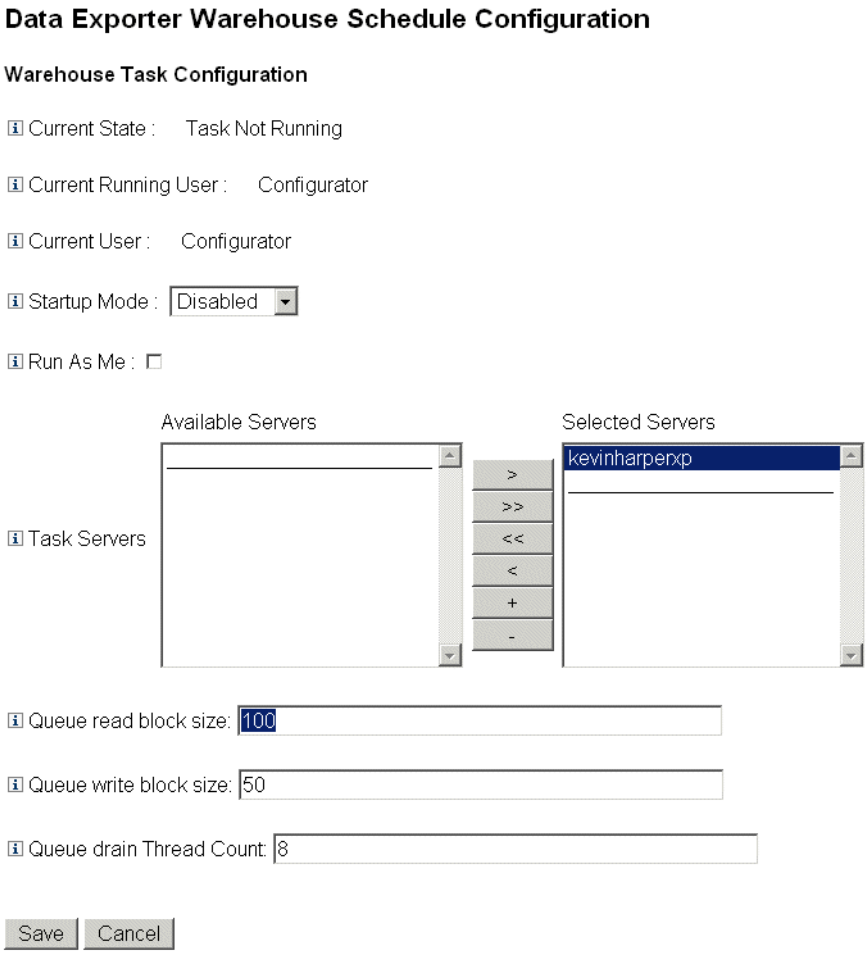


图 16–4 数据仓库进度表配置

2 从“启动模式”下拉菜单中选择一个选项，以确定在启动 Identity Manager 时是否自动启动仓库任务。选择“已禁用”表示必须手动启动任务。

3 选中“以本人身份运行”复选框，以便使用管理帐户运行导出器任务。

4 选择可运行该任务的服务器。您可以指定多个服务器，但在任何给定时间只能运行一个仓库任务。如果执行任务的服务器停止，调度程序将自动在列表中的另一个服务器（如果可用）上重新启动任务。

5 在“队列读取块大小”字段中，指定在写入之前从队列读取到内存缓冲区的记录数。此字段的默认值适用于大多数导出。如果 Identity Manager 系统信息库服务器比仓库服务器慢，则增加该值。

6 在“队列写入块大小”字段中，指定在单个事务中写入仓库的记录数。

7 在“队列清空线程计数”字段中，指定用于读取队列记录的 Identity Manager 线程数。如果队列表中包含大量不同类型的记录，则增大该数字。如果队列表中包含的数据类型较少，则减小该数字。

8 单击“保存”以保存配置更改，并返回到“数据导出器配置”页。

修改配置对象

在数据导出器已配置并且正常运行后，将在内部队列表中捕获配置为排入队列的任何数据类型。默认情况下，该表没有上限，但可通过编辑**数据仓库配置**配置对象来配置上限。此对象具有一个名为 `warehouseConfig` 的嵌套对象。请将以下行添加到 `warehouseConfig` 对象中：

```
<Attribute name='maxQueueSize' value='YourValue'/>
```

`maxQueueSize` 的值可以为小于 2^{31} 的任意正整数。在达到该限制时，数据导出器将禁止进行排队。直到清空队列后，才能导出生成的数据。

Identity Manager 在正常运行时每小时可能会生成数千条更改的记录，因此，队列表可能会迅速变大。由于队列表位于 Identity Manager 系统信息库中，这种增长会消耗 RDBMS 中的表空间，并且可能会耗尽表空间。如果表空间数量有限，则可能需要在队列上设置上限。

可以使用数据队列 JMX Mbean 来监视队列表的大小。有关详细信息，请参见第 446 页中的 “监视数据导出器”。

测试数据导出器

在正确配置数据导出器后，它将作为后台进程运行，以便按配置的间隔将数据发送到仓库。要按需运行导出器，请使用“数据仓库导出器启动程序”任务。

▼ 启动数据仓库导出器启动程序

1 禁用仓库任务。有关详细信息，请参见第 439 页中的“配置仓库任务”。

2 在主菜单中单击“服务器任务”。然后单击“运行任务”次级选项卡。将打开“可用任务”页。

3. 单击“数据仓库导出器启动程序”链接。将打开“启动任务”页。
4. 选中“调试选项”复选框以显示其他选项。
5. 选中“忽略初始 LastMod”复选框，以使导出器忽略它用于确定 Identity Manager 系统信息库中已导出记录的“上次轮询”时间戳。如果选择该选项，则会导出 Identity Manager 系统信息库中所有具有选定类型的记录。
6. 从“导出一次”列表中选择要导出的数据类型。如果未在“导出一次”列表中选择任何类型，导出任务将作为守护进程运行，并按照以前定义的进度表导出数据。如果选择一种或多种数据类型，Identity Manager 将立即导出这些类型，然后退出导出任务。
7. 根据需要，为该页上的其他字段设置值。
8. 单击“启动”开始执行任务。

配置取证查询

通过使用取证查询，Identity Manager 可以读取已存储在数据仓库中的数据。这些查询可以根据用户、角色或相关数据类型的当前或历史值来找出用户或角色。取证查询类似于“查找用户”或“查找角色”报告，但也有所不同，原因是它可以根据历史数据评估匹配条件，并且允许搜索与正在查询的用户或角色具有不同数据类型的属性。

取证查询的用途是使用 Identity Manager 对结果执行操作。取证查询并不是一种通用报告工具。

取证查询可能会提出类似于以下内容的问题：

- 在时间 A 和 B 之间，谁具有系统 X 的访问权限以及该访问权限是由谁批准的?
- 在过去的 48 小时内处理了多少个置备请求，每个请求花费了多长时间?

无法保存取证查询的结果。应该使用商业报告工具完成仓库数据的常规报告。

创建查询

取证查询可以搜索用户对象或角色对象。取证查询可能非常复杂，允许创建者针对相关数据类型选择一个或多个属性条件。用户取证查询可以搜索数据类型为 User、Account、ResourceAccount、Role、Entitlement 和 WorkItem 的属性。角色取证查询可以搜索数据类型为 Role、User 和 Work Item 的属性。

在单个数据类型中，所有属性条件之间具有逻辑“与”关系，因此，必须符合所有条件才能匹配。默认情况下，各个数据类型之间的匹配项具有逻辑“与”关系；但如果选中了“使用 OR”复选框，则各个数据类型之间的匹配项具有逻辑“或”关系。

仓库可能包含单个用户对象或角色对象的多条记录，而单个查询可能会返回同一个用户或角色的多个匹配项。为便于区分这些匹配项，可以使用日期范围限制每种数据类型，以便仅将指定日期范围内的记录视为匹配项。可以使用日期范围限制每种相关数据类型，因此，可以发出以下形式的查询：

```
find all Users with Resource Account on ERP1 between May and July 2005
who were attested by Fred Jones between June and August 2005
```

日期范围是从午夜开始到午夜结束。例如，范围从 2007 年 5 月 3 日到 2007 年 5 月 5 日，时间长度为 48 小时。它不包含从 2007 年 5 月 5 日开始的任何记录。

每个属性条件的操作数（要进行比较的值）都必须指定为查询定义的一部分。该模式将某些属性限制为具有一组有限的可能值；而对其他属性则没有任何限制。例如，必须以 `YYYY-MM-DD HH:mm:ss` 格式输入大多数日期字段。

注 – 由于仓库中可能有大量数据，并且查询具有一定的复杂性，因此可能需要很长时间才能生成查询结果。如果在运行取证查询时离开查询页，则无法看到查询结果。

▼ 创建取证查询

1 **在管理员界面中，单击主菜单中的“遵循性”。**
将打开“审计策略”页（“管理策略”选项卡）。

2 **单击“取证查询”次级选项卡。**
将打开“搜索数据仓库”页。

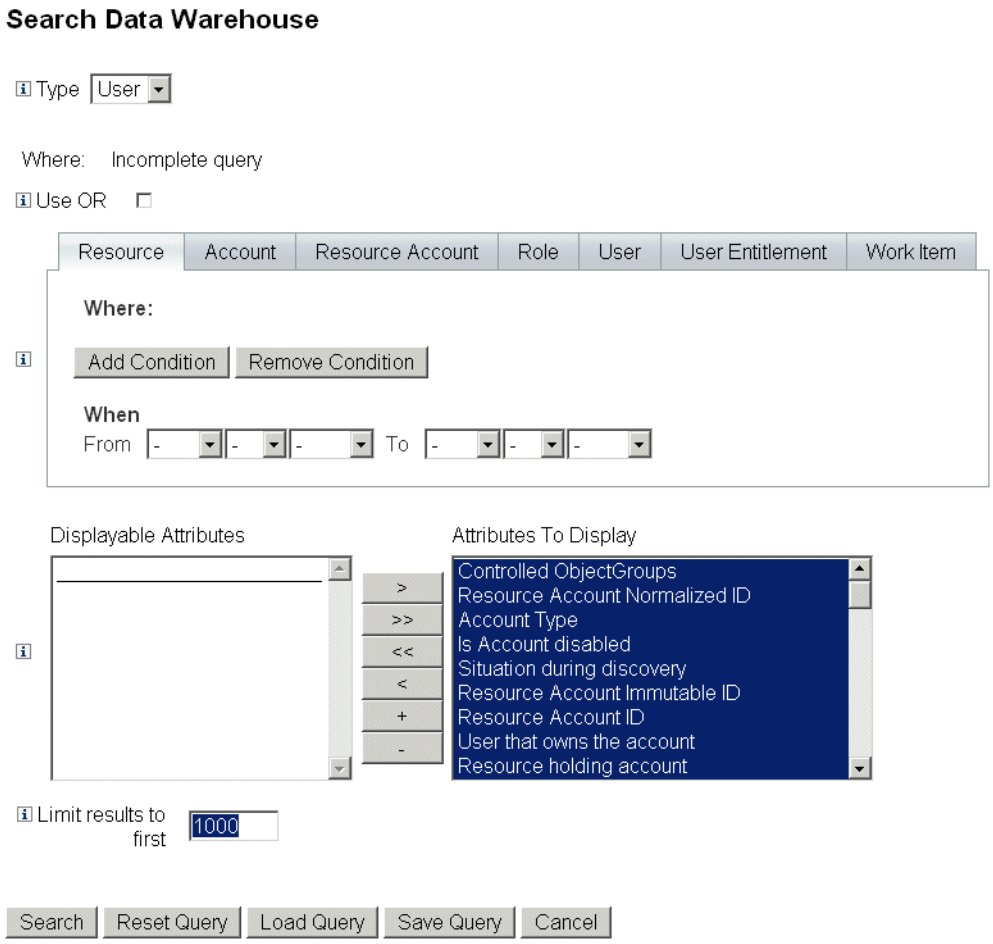


图 16–5 搜索数据仓库

3 从“类型”下拉菜单中，选择是搜索用户记录还是搜索角色记录。

4 选中“使用 OR”复选框，以使 Identity Manager 对查询的每种数据类型的结果执行逻辑“或”运算。默认情况下，系统对结果执行逻辑“与”运算。

5 选择一个表示将出现在取证查询中的数据类型的选项卡。

a. 单击“添加条件”。将显示一组下拉菜单。

b. 从左侧的下拉菜单中选择一个操作数（要检查的条件），从右侧的下拉菜单中选择比较类型，然后输入要搜索的字符串或整数。可能的操作数列表是按外部模式定义的。有关每个操作数的说明，请参阅联机帮助。

c. （可选）选择一个日期范围以缩小查询范围。

根据需要，在当前选定的数据类型中添加更多条件。对于将包含在取证查询定义中的所有数据类型，请重复此步骤。

6 在可用属性中，选择要在取证查询结果中显示的属性。

7 在“只返回前”字段中，指定一个值。在使用多种数据类型中的条件时，限制将应用于每种类型的子查询，并且最终结果是所有子查询的交集。因此，最终结果可能会由于子查询限制而排除某些记录。

8 单击“搜索”以立即运行取证查询，或者单击“保存查询”以重复使用该查询。有关重复使用取证查询的信息，请参见第 445 页中的“保存取证查询”。

保存取证查询

在配置了一个查询并（可选）执行该查询以确保它生成所需的结果后，可以保存该查询以供以后执行。

▼ 保存取证查询

1 在“搜索数据仓库”页中，单击“保存查询”。将打开“保存取证查询 (Forensic Query)”页。

2 指定查询的名称和描述。

3 选中“保存条件值”复选框，以保存在“搜索数据仓库”页中输入的条件值（字符串和整数）。如果未选中此复选框，则保存的取证查询将用作模板，您必须在每次运行查询时输入值。

4 任何人都可以执行任何已保存的查询，但默认情况下，只有查询创建者可以修改查询。要允许其他用户修改您的查询，请选中“允许他人更改此查询”复选框。

5 由于查询将返回用户对象或角色对象，因此，您可以选择要在结果中显示的对象属性。如果要显示“要显示的属性”列表中未包含的属性，您可以转到“数据导出器配置”页，然后在用户或角色类型中添加新的可显示属性。

加载查询

您可以加载任何用户保存的任何查询，但是只能修改自己创建的查询，或由其他人标记为可被任何人修改的查询。

▼ 加载取证查询

1. **在“搜索数据仓库”页中，单击“加载查询”。将打开“加载取证查询 (Forensic Query)”页。如果已将查询保存为模板，“查询摘要”列将显示不完整的查询。**
2. **选中查询左侧的复选框，然后单击“加载查询”。**

维护数据导出器

本节介绍了如何跟踪数据导出器的状态。该信息分为以下几个主题：

- 第 446 页中的 “监视数据导出器”
- 第 447 页中的 “监视日志记录”

监视数据导出器

在导出器已配置并且正常运行后，您可以选择对其进行监视以确保其继续正常运行。导出器包含几个 JMX Bean，可用于确定导出器的运行状况。JMX Bean 包含以下统计信息：导出器的平均读取/写入速率、内部内存队列的当前/最大大小以及永久性队列的大小。导出器还会在导出期间生成审计记录，每种数据类型的每个周期各生成一条记录。审计记录包含导出的该类型记录数以及导出操作占用的时间。

数据导出器提供了以下用于监视导出器的 JMX 管理 Bean。

表 16–2 JMX 管理 Bean

Bean 名称	描述
DataExporter	包含当前排队的导出数以及队列上限。
DataQueue	包含当前缓存的排队导出数以及到达高速缓存的速率。
ExporterTask	包含导出读取（从 Identity Manager 中）数、写入（到仓库）数、读取和写入速率（记录数/秒）以及错误数。

可以对数据导出器进行配置，以使其在 Identity Manager 正常运行期间将导出记录排入队列表中。由于该队列可能需要扩大以存放大量记录，并且在服务器重新启动后仍需保留该队列，因此，该队列将由 Identity Manager 系统信息库中的表进行备份。由于写

入系统信息库通常会减慢 Identity Manager 的正常运行速度，因此，该队列使用较小的内存高速缓存将记录缓存到内存中，直到可以在系统信息库中永久保留这些记录为止。

可以绘制 DataQueue MBean 属性图表，以显示在内存中排队的最大记录数（在单个 Identity Manager 服务器上）。在平衡型系统上，内存高速缓存中的记录数应该很小并很快变为零。如果发现此数字很大（数千条）或者在几秒内未恢复为零，则应该检查系统信息库的写入性能。

ExportTask MBean 包含两个错误计数：一个是读取错误计数，一个是写入错误计数。这些计数应该为零，但可能会由于多种原因而出现错误，尤其是在写入期间。最常见的写入错误是由于仓库表列容纳不下导出的数据造成的 - 该错误通常为字符串溢出。某些导出的字符串数据非常大，导出表列必须对此设置一个上限。

监视日志记录

Identity Manager 包含两组无限制增长的对象：审计日志和系统日志。数据导出器解决了一些与日志表有关的维护问题。

审计日志

Identity Manager 将固定的审计记录写入到审计日志中，以作为所执行的操作的历史审计跟踪。Identity Manager 在某些报告中使用这些记录，记录中的数据可以显示在管理员界面中。不过，由于审计日志会无限制增长，并按一定的速率增长，部署者必须确定何时截断审计日志。在启用数据导出器之前，如果要在截断以前保留记录，您必须转储系统信息库中的表。如果启用了数据导出器并将其配置为导出日志记录，则旧记录会保留在仓库中，并且 Identity Manager 可以根据需要截断审计表。

系统日志

系统日志具有与审计日志相同的固定属性，但系统日志的生成频率通常较低。数据导出器不导出系统日志。要截断系统日志并保留旧记录，您必须转储系统信息库中的表。

◆ ◆ ◆ 第 17 章

17 服务提供者管理

本章提供了在 Sun Identity Manager 中管理服务提供者功能而需要了解的信息。要使用此信息，了解轻量目录访问协议 (Lightweight Directory Access Protocol, LDAP) 目录和联合管理会很有帮助。有关 Sun Identity Manager Service Provider (服务提供者) 实现的更深入介绍，请参见《Sun Identity Manager Service Provider 8.1 Deployment》。

本章包含以下主题：

服务提供者功能概述

在服务提供者环境中，您需要能够管理所有最终用户（包括外联网用户以及内联网用户）的用户置备。通过使用服务提供者功能，公司管理员可以将身份帐户分为两种不同的类型：Identity Manager 用户和服务提供者用户。Identity Manager 中的服务提供者用户是已配置为服务提供者用户类型的用户帐户。

通过提供以下功能，将 Identity Manager 用户置备和审计权能扩展到服务提供者实现：

增强的最终用户页面

提供了可以为服务提供者实现自定义的增强的最终用户页面。

密码和帐户 ID 策略

如同其他 Identity Manager 用户一样，您可以定义服务提供者用户和资源帐户的帐户 ID 和密码策略。

可使用服务提供者系统帐户策略（已添加到主“策略”表中）为服务提供者用户激活策略检查代码。

Identity Manager 和服务提供者同步

可以将 Identity Manager 与服务提供者帐户的同步配置为在任何 Identity Manager 服务器上运行，或限制为在选定服务器上运行。

如同 Identity Manager 同步一样，通过“资源”页中的“资源操作”选项可以轻松地停止和启动服务提供者同步。请参见第 483 页中的 “启动和停止同步”。

Identity Manager 用户同步的输入表单与服务提供者用户同步的输入表单不同。请参见第 479 页中的 “最终用户界面”。

Access Manager 集成

您可以使用 Sun Access Manager 7 2005Q4 在服务提供者最终用户页面上进行验证。如果配置了与 Access Manager 集成，则 Access Manager 可确保只有经过验证的用户才可以访问最终用户页面。

服务提供者需要使用用户名以进行审计。更新 `AMAgent.properties` 文件以将用户的 ID 添加到 HTTP 标头，例如：

```
com.sun.identity.agents.config.response.attribute.mapping[uid] = HEADER_speuid
```

最终用户页面验证过滤器会将 HTTP 标头值置入 HTTP 会话（其他代码希望该标头值置入其中）。

初始配置

要配置服务提供者功能，请执行以下步骤编辑目录服务器的 Identity Manager 配置对象：

- 编辑主配置
- 编辑用户搜索配置

注 –

在继续之前，请确保您已经：

- 定义了 LDAP 资源。默认情况下，将导入一个名为“服务提供者最终用户目录”的样例资源。如果要将用户信息和配置信息存储在不同的目录中，您可以配置多个资源。
- 此模式必须包括 XML 对象的映射。

  如果需要，请配置服务提供者帐户策略。
- 为目录资源配置的基本上下文仅适用于存储在该目录中的用户。

编辑主配置

▼ 编辑服务提供者实现的配置对象

1 **在管理员界面中，单击菜单中的“服务提供者”。**

2 **单击“编辑主配置”。**

将打开“服务提供者配置”页。

3 **填写“服务提供者配置”表单。**

按照以下各节提供的说明进行操作：

- 第 451 页中的 “目录配置”
- 第 453 页中的 “用户表单和策略”
- 第 454 页中的 “事务数据库”
- 第 456 页中的 “配置“跟踪的事件配置””
- 第 457 页中的 “同步帐户索引”
- 第 458 页中的 “标注配置”

目录配置

在“目录配置”一节中，将介绍为服务提供者用户配置 LDAP 目录和指定 Identity Manager 属性的信息。

图 17–1 显示了“服务提供者配置”页的这一区域以及下一节中介绍的“用户表单和策略”区域。

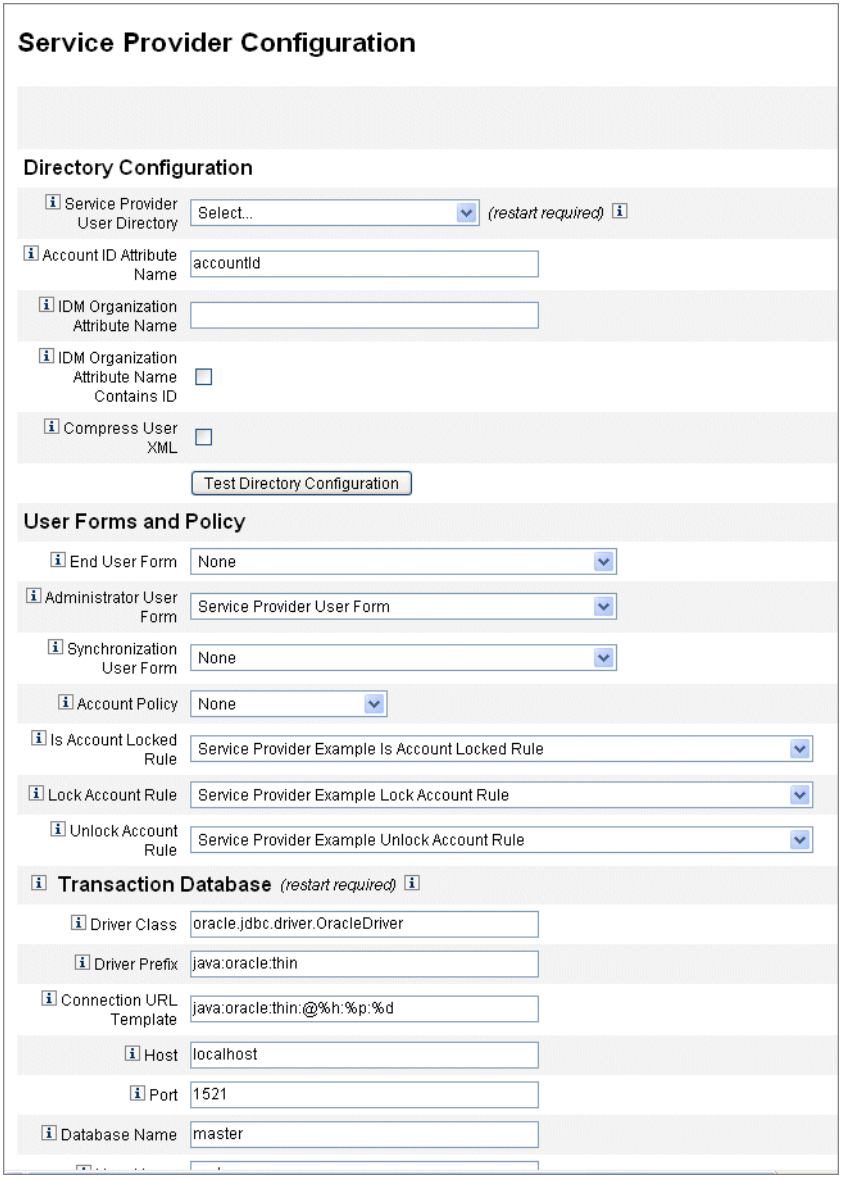


图 17–1 服务提供者配置（目录、用户表单和策略）

▼ 填写“目录配置”表单

1 从列表中选择“服务提供者最终用户目录”。

选择在其中存储所有服务提供者用户数据的 LDAP 目录资源。

2 **输入帐户 ID 属性名称。**

这是包括帐户的唯一简短标识符的 LDAP 帐户属性名称。它被视为用户通过 API 进行验证及帐户访问时使用的名称。该属性名称必须在模式映射中定义。

3 **指定 IDM 组织属性名称。**

该选项指定包含组织（该组织是 LDAP 帐户在 Identity Manager 中所属的组织）名称或 ID 的 LDAP 帐户属性名称。它用于 LDAP 帐户的委托管理。属性名称必须存在于 LDAP 资源模式映射中，并且是 Identity Manager 系统属性名称（模式映射左边的名称）。

注 – 如果要通过组织授权启用委托管理，应指定 Identity Manager 组织属性名称（如果需要，还应指定“IDM 组织属性名称包括 ID”）。

---

4 **如果您选择“IDM 组织属性名称包括 ID”，请启用该选项。**

如果 LDAP 资源属性（是指 LDAP 帐户所属的 Identity Manager 组织）包含 Identity Manager 组织的 ID 而非名称，请选择该选项。

5 **如果您选择“压缩用户 XML”，请启用该选项。**

如果您选择压缩存储在目录中的用户 XML，请选择该选项。

6 **单击“测试目录配置”以验证配置的条目。**

注 – 您可以根据需要测试目录、事务和审计配置。要对以上三方面进行全面测试，请单击三个测试配置按钮。

用户表单和策略

在“用户表单和策略”区域（如上面的图 17–1 中所示）中，可以指定用于服务提供者用户管理的表单和策略。

▼ 为服务提供者用户管理指定表单和策略

1 **从列表中选择“最终用户表单”。**

除了委托管理员页面和同步期间，该表单可用于所有其他环境。如果选择“无”，则不使用默认用户表单。

2 **从列表中选择“管理员用户表单”。**

这是用于管理员上下文中的默认用户表单。其中包括“服务提供者帐户”编辑页。如果选择“无”，则不使用默认用户表单。

注 – 如果不选择“管理员用户表单”，则管理员将无法通过 Identity Manager 创建或编辑服务提供者用户。

3 **从列表中选择“同步用户表单”。**

如果没有为运行服务提供者同步的资源指定任何表单，则会使用默认的“同步用户表单”。如果在资源的同步策略上指定了输入表单，将使用该表单。资源通常需要不同的同步输入表单。在这种情况下，应该对每个资源设置同步用户表单，而不是从列表中选择表单。

4 **从列表中选择“帐户策略”。**

这些选项包括通过“配置”>“策略”定义的任何身份帐户策略。

5 **从列表中选择“帐户是否锁定规则”。**

选择要针对服务提供者用户视图运行的规则，该规则可以确定帐户是否锁定。

6 **选择“锁定帐户规则”。**

选择要针对服务提供者用户视图运行的规则，该规则可以在视图中设置能锁定帐户的属性。

7 **选择“解除锁定帐户规则”。**

选择要针对服务提供者用户视图运行的规则，该规则可以在视图中设置能解除锁定帐户的属性。

事务数据库

可以使用“服务提供者配置”页中的此部分（如图 17–2 中所示）来配置事务数据库。仅当使用 JDBC 事务持久性存储时，才需要使用这些选项。更改其中的任何值均需要重新启动服务器以将其应用。

必须根据 `create_spe_tables` DDL 脚本（位于 Identity Manager 安装的 `sample` 目录中）中所示的模式设置事务的数据库表。可能需要为目标环境自定义相应的脚本。

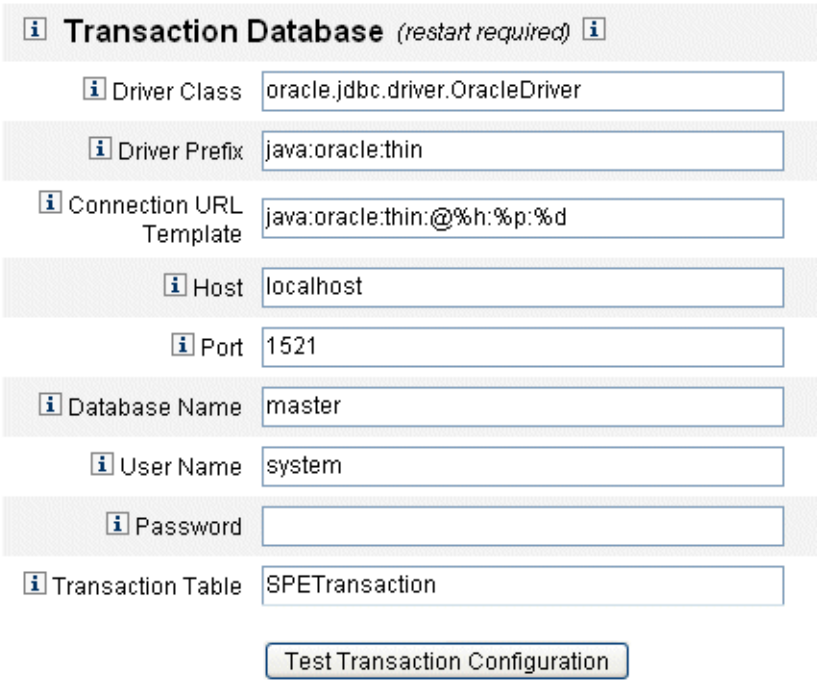


图 17–2 服务提供者配置（事务数据库）

▼ 配置事务数据库

1 **输入以下数据库信息：**

- **驱动程序类**。指定 JDBC 驱动程序类名。
- **驱动程序前缀**。该字段是可选的。如果已指定，将在注册新驱动程序前查询 JDBC DriverManager。
- **连接 URI 模板**。该字段是可选的。如果已指定，将在注册新驱动程序前查询 JDBC DriverManager。
- **主机**。输入正在运行数据库的主机的名称。
- **端口**。输入数据库服务器要侦听的端口号。
- **数据库名称**。输入要使用的数据库的名称。
- **用户名**。输入有权从选定数据库的事务和审计表中读取、更新和删除行的数据库用户 ID。
- **密码**。输入数据库用户密码。
- **事务表**。输入选定数据库中用于存储暂挂事务的表的名称。

2 **如果适用，单击“测试事务配置”以验证您的条目。**

继续到 "Service Provider Configuration" 页的下一段以配置跟踪的事件。

配置“跟踪的事件配置”

启用事件收集后，您便可以实时跟踪统计信息，从而有助于维护预期级别和商定级别的服务。默认情况下启用事件收集，如图 17–3 中所示。清除“启用事件收集”复选框将禁用收集。

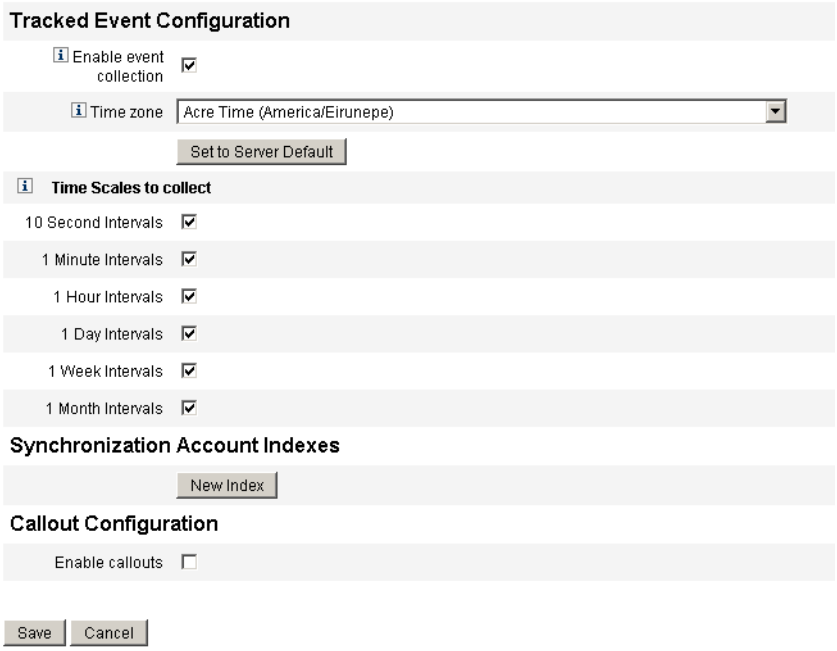


图 17–3 服务提供者配置（跟踪的事件、帐户索引和标注配置）

▼ 为服务提供者跟踪事件指定时区和收集间隔

1 **从列表中选择“时区”。**

选择记录跟踪事件时要使用的时区，或选择“设置为服务器默认值”以使用服务器上设置的时区。

2 **选择“用于收集的时间范围”选项。**

将按以下时间间隔聚集收集：每 10 秒钟、每分钟、每小时、每日、每周和每月。禁用您不希望按其进行收集的任何间隔。

同步帐户索引

在服务提供者实现中同步资源时，可能需要定义帐户索引以正确地将此资源发送的事件与服务提供者目录中的用户相关联。

默认情况下，资源事件需要包含与目录中 accountId 属性相匹配的属性 accountId 值。在某些资源中，不会始终发送 accountId。例如，ActiveDirectory 中的删除事件仅包含 ActiveDirectory 生成的帐户 GUID。

不包含 accountId 属性的资源必须包含以下任一属性的值。

- **guid**。该属性通常包含系统生成的唯一标识符。
- **identity**。该属性通常与除 LDAP 资源之外的所有资源的 accountId 相同，在 LDAP 资源中，identity 包含对象的完整 DN。

如果需要使用 guid 或 identity 进行关联，则必须定义这些属性的帐户索引。索引仅是一个或多个可用于存储特定于资源的身份的目录用户属性的选项。身份存储在目录中后，便可将其用于搜索过滤器以关联同步事件。

要定义帐户索引，请先确定哪些资源将用于同步以及其中的哪些资源需要索引。然后编辑服务提供者目录的资源定义，并在模式映射中为每个活动同步资源的 GUID 或 identity 属性添加属性。例如，如果从 ActiveDirectory 同步，则可以定义映射到未使用的目录属性（例如管理员）的名为 AD-GUID 的属性。

▼ 定义资源的索引属性

在定义了服务提供者资源中的所有索引属性后，请执行以下步骤：

1. **在配置页的“同步帐户索引”区域中，单击“新建索引”按钮。**
   表单可扩展为包含资源选项字段，之后是两个属性选项字段。在选择资源之前，属性选项字段保持为空

2. **从列表中选择“资源”。**
   现在，属性字段包含在模式映射中为选定资源定义的值。

3. **为“GUID 属性”或“完整身份属性”选择适当的索引属性。**
   通常不必同时设置二者。如果同时设置二者，则软件首先尝试使用 GUID 进行关联，然后使用完整身份进行关联。

4. **您可以再次单击“新建索引”以定义其他资源的索引属性。**

5. **要删除索引，请单击“资源”选项字段右侧的“删除”按钮。**
   删除索引仅会从配置中删除索引，而不会修改当前可能在索引属性中存储值的所有现有目录用户。

注 – 删除索引仅会从配置中删除索引，而不会修改当前可能在索引属性中存储值的所有现有目录用户。

标注配置

选择 "Callout Configuration" 段中的该选项可以启用标注。启用标注后，将显示标注映射，使您可以为每个列出的事务类型选择操作前和操作后选项。

默认情况下，将操作前和操作后选项设置为 "None"。

如果指定操作后标注，请使用“等待操作后的标注”选项指定事务必须等待操作后标注处理完成后才能完成。这可确保任何相关事务都只能在操作后标注成功完成后执行。

注 – 在“服务提供者配置”页中的所有部分中选择完设置后，单击“保存”以完成配置。

编辑用户搜索配置

通过使用此页（如图 17–4 中所示），可以为“管理服务提供者用户”页上委托的管理员进行的搜索配置默认搜索设置。这些默认值适用于 "Manage Service Provider Users" 页上的所有用户，但是可以根据每个会话将其覆盖。

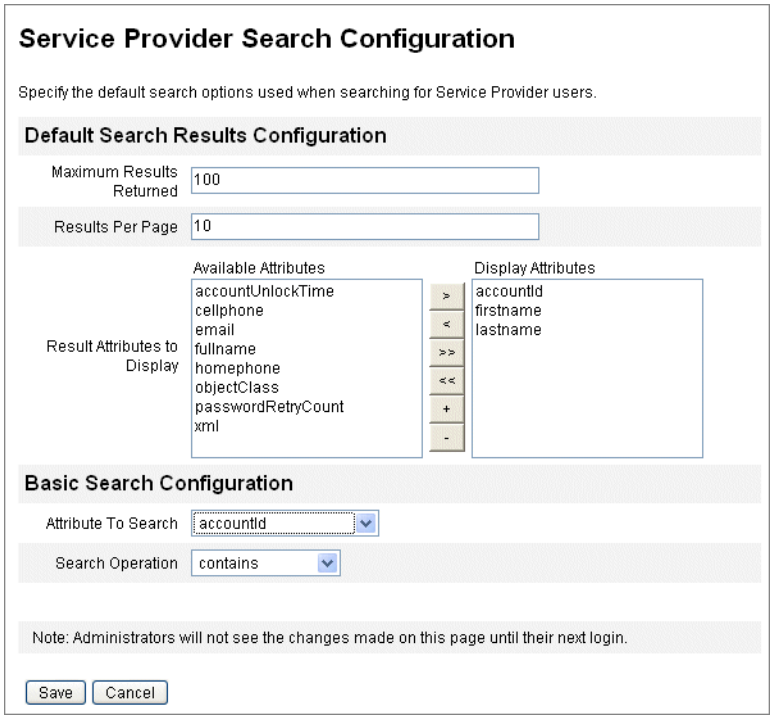


图 17–4 搜索配置

▼ 配置默认搜索设置以搜索服务提供者用户

1. 在菜单栏中单击“服务提供者”。
2. 单击“编辑用户搜索配置”。
3. 输入“返回的最大结果数”的数值（默认值为 100）。
4. 输入“每页的结果数”的数值（默认值为 10）。
5. 使用方向键选择“要显示的结果属性”旁边的“可用的属性”。
6. 从列表中选择“要搜索的属性”。
7. 从列表中选择“搜索操作”。
8. 单击“保存”。

注 – 只有在注销并重新登录后，对搜索配置所做的更改才会生效。

如果尚未配置服务提供者目录，则无法使用这些配置对象。

事务管理

某个事务可以封装单个置备操作，例如创建新用户或分配新资源。为确保这些事务在资源不可用时也能完成，需要将其写入事务持久性存储。

本节中的以下主题包含用于管理服务提供商事务的步骤：

- 第 460 页中的 “设置默认事务执行选项”
- 第 462 页中的 “设置事务持久性存储”
- 第 463 页中的 “设置高级事务处理设置”
- 第 465 页中的 “监视事务”

设置默认事务执行选项

这些选项控制事务的执行方式，包括同步/异步处理及何时在事务持久性存储中对其进行持久性处理。可以在 IDMXUser 视图中或通过用于对其进行处理的表单覆盖这些选项。有关详细信息，请参见《Sun Identity Manager Service Provider 8.1 Deployment》 。

▼ 配置服务提供者事务

1 **单击“服务提供者”→“编辑事务配置”。**

将显示“服务提供者事务配置”页。

图 17–5 显示了“默认事务执行选项”区域。

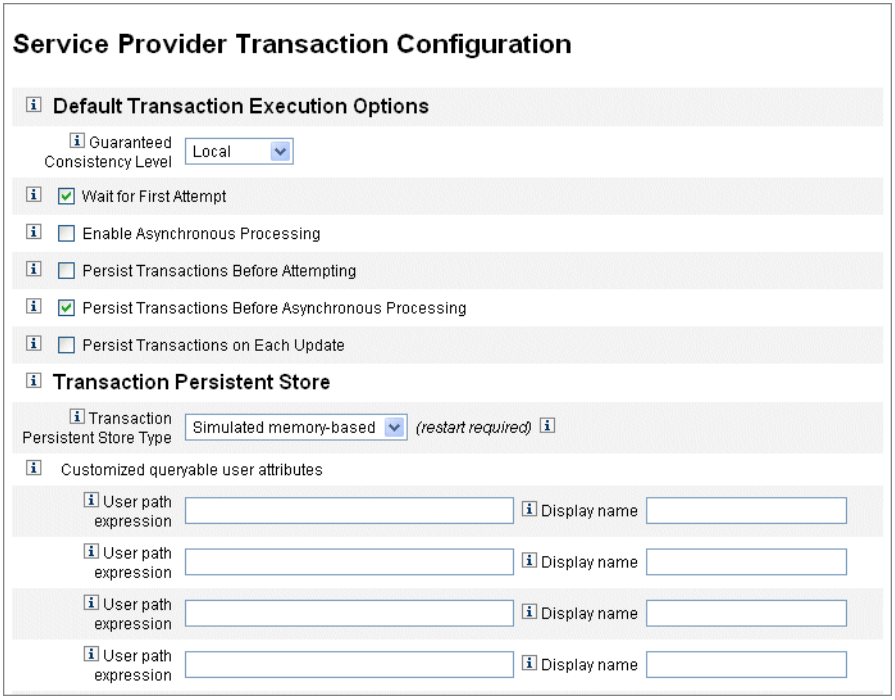


图 17–5 事务配置

2 **选择相应的"一致性级别保证"选项，以指定用户更新的事务一致性级别。**

这些选项包括：

- **无**。不保证用户的资源更新按顺序进行。
- **本地**。保证由同一服务器处理的用户资源更新按顺序进行。
- **完全**。保证用户在所有服务器上的所有资源更新都按顺序进行。此选项要求在进行尝试或异步处理之前保留所有事务。

3 **根据需要，启用默认事务执行选项。**

这些选项包括：

- **等待第一次尝试**。指定了当 IDMXUser 视图对象登入时控制权如何返回给调用方。如果启用该选项，则在置备事务完成一次尝试之前，登入操作将被阻塞。如果禁用异步处理，则当控制权返回时，事务要么成功，要么失败。如果启用异步处理，则事务将在后台继续重试。如果禁用该选项，则登入操作将在尝试置备事务之前将控制权返回给调用方。请考虑启用该选项。
- **启用异步处理**。该选项控制在登入调用返回后是否继续处理置备事务。

  启用异步处理将允许系统重试事务。这样做还可以让工作者线程（在第 463 页中的“设置高级事务处理设置”中配置）异步运行，从而提高吞吐量。如果选择此选项，请配置重试时间间隔，并尝试使用同步输入表单置备或更新资源。

  在选择“启用异步处理”后，请输入“重试超时”值。该值是服务器重试失败的置备事务的时间上限（毫秒）。该设置补充单个资源的重试设置，包括服务提供商用户 LDAP 目录。例如，如果在达到资源重试限制之前达到了该限制，则事务将异常中止。如果该值为负，则重试次数仅受单个资源的设置的限制。
- **在尝试前使事务具有持久性**。如果启用，置备事务将在尝试前被写入到事务持久性存储中。由于大多数置备事务在第一次尝试时就会成功，因此启用该选项可能会产生不必要的系统开销。考虑禁用该选项，除非“等待第一次尝试”选项已禁用。如果选择 "Complete" 一致性级别，则无法使用该选项。
- **在异步处理前使事务具有持久性（默认选项）**。如果启用，置备事务将在异步处理前被写入到事务持久性存储中。如果“等待第一次尝试”选项已启用，则需要重试的事务将在控制权返回到调用方前具有持久性。如果“等待第一次尝试”选项已禁用，则事务会在尝试前一直具有持久性。建议启用该选项。如果选择 "Complete" 一致性级别，则无法使用该选项。
- **每次更新时使事务具有持久性**。如果启用，置备事务将在每次重试尝试后具有持久性。由于事务持久性存储（可以从“搜索事务”页中进行搜索）始终是最新的，因此该操作可以帮助隔离问题。

设置事务持久性存储

“服务提供者事务配置”页上的选项适用于事务持久性存储。可以配置要在存储中显示的存储类型以及其他可查询属性，如下图中所示。

图 17–6 配置服务提供者事务持久性存储

▼ 在“服务提供者事务配置”页中设置选项

1 **从列表中选择所需的“事务持久性存储类型”。**

如果选择了“数据库”选项，则在服务提供者配置主页中配置的 RDBMS 将用于使置备事务具有持久性。这保证了必须重试的事务不会在服务器重新启动时丢失。选择该选项要求在服务提供者配置主页中配置 RDBMS。如果选择了“模仿的基于内存”选项，则要求重试的事务将仅存储到内存中并且将在服务器重新启动时丢失。在生产环境中，请启用“数据库”选项。

注 – 基于内存的事务持久性存储不适合在群集环境中使用。

更改“事务持久性存储类型”后，必须重新启动所有正在运行的 Identity Manager 实例才能使更改生效。

---

2 **如果需要，请输入“自定义的可查询用户属性”。**

选择要在事务摘要中显示的 IDMXUser 对象的附加属性。这些属性可以从搜索事务页中查询并显示在搜索结果中。

这些属性包括：

- **用户路径表达式**。将路径表达式输入到 IDMXUser 对象中。
- **显示名称**。选择与路径表达式对应的显示名称。该显示名称显示在事务搜索页中。

设置高级事务处理设置

这些高级选项控制事务管理器的内部工作。除非性能分析说明提供的默认值不是最佳的，否则不要对其进行更改。所有条目都是必需的。

图 17–5 展示了“编辑事务配置”页中的“高级事务处理设置”区域。

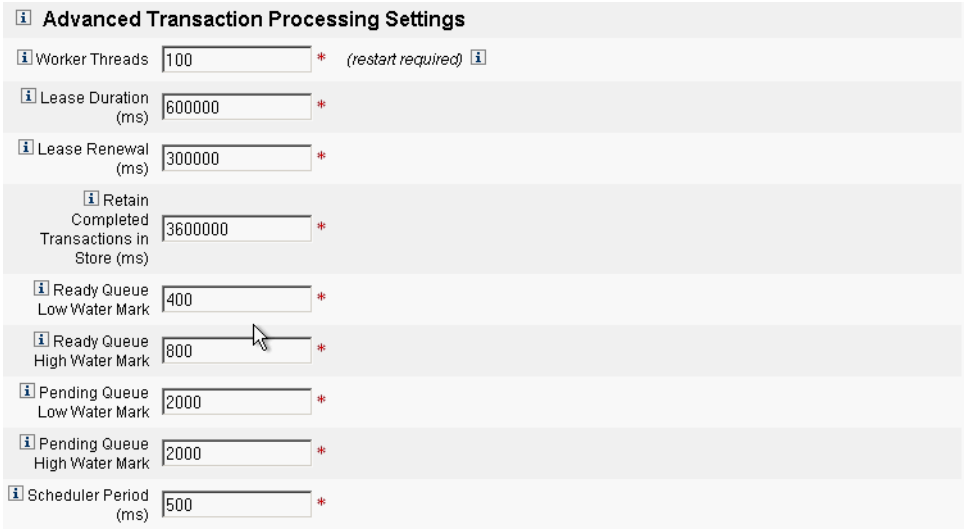


图 17–7 高级事务处理设置

▼ 指定高级事务处理设置

1 **输入所需的"工作者线程"数（默认值为 100）。**

这是用来处理事务的线程数。该值限定了可以并发处理的事务数。这些线程在启动时静态分配。

注 – 更改"工作者线程"设置后，必须重新启动所有正在运行的 Identity Manager 实例才能使更改生效。

---

2 **输入所需的"租用持续时间"（毫秒）（默认值为 600000）。**

它控制服务器将锁定要重试的事务的时间。需要时将更新租用。但是，如果服务器没有完全关闭，则在原始服务器租用到期前其他服务器不能锁定事务。该值至少应为一分钟。将该值设置得较小可能会影响事务持久性存储的负荷。

3 **输入"租用更新时间"（毫秒）（默认值为 300000）。**

此选项可控制更新锁定事务的租用的时间。当租用时间还剩余该毫秒值时，租用会更新。

4 **输入"完成的事务保留在存储中的时间"（毫秒）（默认值为 360000）。**

从事务持久性存储中删除完成的事务前要等待的时间（毫秒）。除非事务被配置为立即具有持久性，否则事务持久性存储不会包含所有完成的事务。

5 **输入“就绪队列低水位标记”（默认值为 400）。**

当事务调度程序的准备运行事务队列降到该限制以下时，将使用可用的准备运行事务重新填充队列，最高可到高水位限制。

6 **输入“就绪队列高水位标记”（默认值为 800）。**

当事务调度程序的准备运行事务队列降到低水位限制以下时，将使用可用的准备运行事务重新填充队列，最高可到该限制。

7 **输入“暂挂队列低水位标记”（默认值为 2000）。**

事务调度程序的暂挂队列容纳有等待重试的失败事务。如果队列大小超过高水位标记，则所有超过低水位标记的事务将被刷新到事务持久性存储中。

8 **输入“暂挂队列高水位标记”（默认值为 2000）。**

事务调度程序的暂挂队列容纳有等待重试的失败事务。如果队列大小超过高水位标记，则所有超过低水位标记的事务将被刷新到事务持久性存储中。

9 **输入“调度程序周期”（毫秒）（默认值为 500）。**

这是事务调度程序应运行的频率。当运行时，事务调度程序会将准备运行事务从暂挂队列移动到就绪队列，并执行其他周期性任务，例如，使事务具有持久性以进入事务持久性存储中。

10 **单击“保存”接受设置。**

监视事务

服务提供商事务将写入事务持久性存储中。您可以在事务持久性存储中搜索事务以查看事务状态。

注 – 使用 "Edit Transaction Configuration" 页（请参见“事务管理”），管理员可以控制使事务具有持久性的时间。例如，即使事务尚未进行首次尝试，也可以使其立即具有持久性。

使用 "Transactions Search" 页可以指定搜索条件，从而使您可以根据与事务事件相关的特定条件（例如用户、类型、状态、事务 ID、当前状态和事务的成功或失败）来过滤要查看的事务。这包括仍在进行重试的事务以及已完成的事务。可以取消尚未完成的事务，以阻止其进一步的尝试。

▼ 搜索事务

1 **在管理员界面中，单击“服务器任务”→“服务提供者事务”。**

将打开“服务提供者事务搜索”页，您可以在该页中指定搜索条件。

注 – 搜索仅返回与以下选定的**所有**条件匹配的事务。这类似于“帐户”→“查找用户”页。

2 配置搜索。

选择下面的一个或多个选项：

- **用户名**。允许您仅搜索与具有您输入的 accountId 的用户相对应的事务。

  注 – 如果已在“服务提供者事务配置”页上配置任何自定义的可查询用户属性，则它们会在此显示。例如，如果将它们配置为自定义的可查询用户属性，则您可以选择根据 "Last Name" 或 "Full Name" 进行搜索。

- **类型**。允许您搜索选定类型的事务。
- **状态**。允许您搜索处于以下选定状态的事务：
  - **尚未尝试**表示尚未尝试的事务。
  - **暂挂重试**表示这样的事务：已经尝试一次或多次，具有一个或多个错误，并计划重试，重试次数不超过为单个资源配置的重试限制。
  - **成功**表示已经成功完成的事务。
  - **失败**表示已经完成但具有一个或多个故障的事务。
- **尝试次数**。允许您根据事务已尝试的次数搜索这些事务。将会重试失败的事务，重试次数不超过为单个资源配置的重试限制。
- **已提交**。允许您根据事务初次提交的时间搜索这些事务，以小时、分钟或天为增量。
- **已完成**。允许您根据事务完成的时间搜索这些事务，以小时、分钟或天为增量。
- **取消状态**。允许您根据事务是否已取消搜索这些事务。
- **事务 ID**。允许您根据事务的唯一 ID 搜索这些事务。通过使用该选项，您可以根据输入的 ID 值（出现在所有审计日志记录中）查找事务。
- **运行环境**。允许您根据运行事务的服务提供者服务器搜索这些事务。服务器的标识符基于它的计算机名称，除非它已在 `Waveset.properties` 文件中被覆盖。
- **将搜索结果数限制为从列表中选择的首个条目数**。返回的结果数不会超过指定的限制值。即使有更多的结果可用，也不会做任何指示。

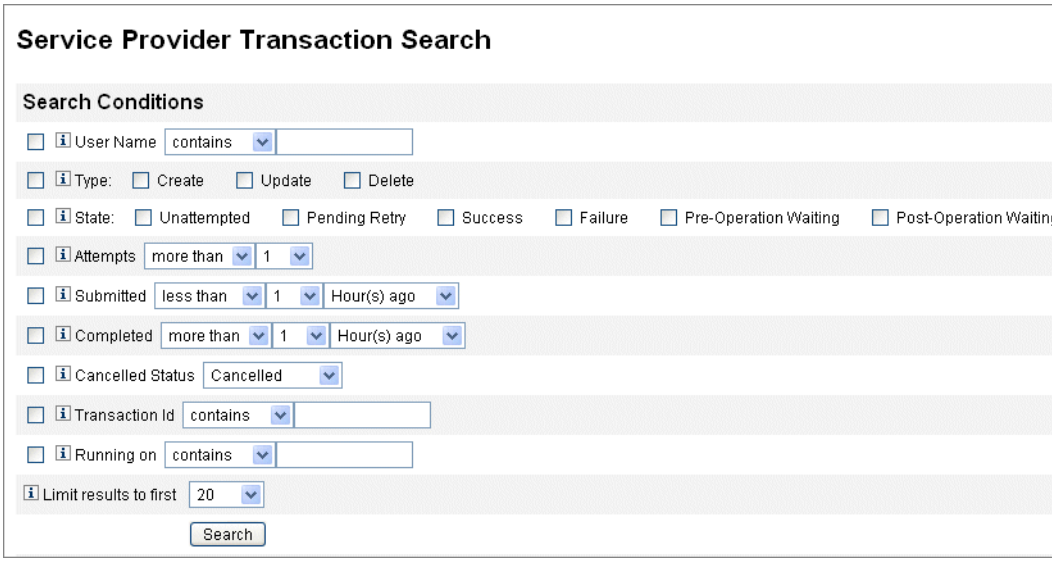


图 17–8 搜索事务

3 **单击“搜索”。**

将显示搜索结果。

4 **可以单击结果页面底部的“下载所有匹配的事务”，将结果保存为 XML 格式的文件。**

注 – 要取消搜索结果中返回的事务，请在结果表中选择该事务，然后单击“已选择取消”。您无法取消已完成或已被取消的事务。

服务提供者用户的委托管理

通过使用 Identity Manager **管理员角色**或通过基于组织的授权模型可启用服务提供者用户的委托管理。

通过组织授权委托

默认情况下，Identity Manager 通过基于组织的授权模型提供管理职责的委托。

在基于组织的授权模型中创建委托管理员时，请谨记以下几点：

- 服务提供者管理员是具有特定权能和受控组织的 Identity Manager 用户。
- 用户的组织属性值可以是 Identity Manager 组织的名称，也可以是对象 ID。这取决于 Identity Manager 主配置屏幕中的“Identity Manager 组织属性名称包括 ID”字段的设置。
- 您可以创建 Identity Manager 分层结构，并以您要委托这些组织管理的方式将组织置于该分层结构中。请使用组织的特定标识，而不是组织的简单名称。
- 服务提供商用户通过目录服务器中的用户属性获取其组织。
  - 您必须在目录服务器资源的模式映射中设置这些属性。
  - 属性比较是通过对管理员受控组织列表进行**完全匹配**来完成的。目录中存储的值必须与组织名称相匹配，而不是整个分层结构。如果管理员控制 `Top:orgA:sub1`，则 `sub1` 必须为存储在服务提供者用户的组织属性中的值。
  - 如果未设置属性或属性与 Identity Manager 组织不对应，则会将服务提供者用户视为 Top 组织的成员。这要求服务提供者管理员在 `Top` 中具有服务提供者用户权能才能管理这些用户。

  属性设置可确定按服务提供者管理员进行搜索的范围。
- 要创建委托管理员帐户，应先创建 Identity Manager 管理员，然后添加服务提供者管理员权能。可以将特定于服务提供者任务的权能分配给用户（在“编辑用户”页的“安全性”选项卡中）。受控组织可指定管理员可以修改的服务提供者用户。适用于服务提供者用户的所有资源均适用于所有 Identity Manager 管理员。

注 – 有关 Identity Manager 委托管理的详细信息，请参见第 6 章，管理中的第 172 页中的“委托管理”

通过管理员角色分配委托

要授予对服务提供商用户的细化权能和控制范围，请使用服务提供商用户管理员角色。可以将管理员角色配置为在登录时动态分配给一个或多个 Identity Manager 用户或服务提供者用户。

可以定义规则并将其分配给管理员角色，管理员角色可指定授予分配了管理员角色的用户的权能（例如 `Service Provider Create User`）。

要将管理员角色委托用于服务提供者用户，您必须在 Identity Manager 系统配置对象（第 102 页中的“编辑 Identity Manager 配置对象”）中将其启用。

如果启用通过管理员角色分配进行的委托，则“服务提供者配置”中的“IDM 组织属性名称”不是必填项。

启用服务提供者管理员角色委托

要启用服务提供者管理员角色委托（服务提供者委托管理），请打开要修改的系统配置对象（第 102 页中的 “编辑 Identity Manager 配置对象”）并将以下属性设置为 `true`：

`security.authz.external.`*app name*`.`*object type*

其中 *app name* 为 Identity Manager 应用程序（例如管理员界面），*object type* 为 `Service Provider Users`

可以为每个 Identity Manager 应用程序（例如管理员界面或用户界面）和每个对象类型启用该属性。当前，唯一受支持的对象类型为 `Service Provider Users`。默认值为 `false`。

例如，要为 Identity Manager 管理员启用服务提供者委托管理，请将“系统配置”配置对象中的以下属性设置为 "true"：

```
security.authz.external.Administrator Interface.Service Provider Users
```

如果为给定的 Identity Manager 或服务提供者应用程序禁用了服务提供者委托管理（设置为 false），则会使用基于组织的授权模型。

在启用服务提供者委托管理后，跟踪的事件将捕获有关执行的授权规则数和持续时间的信息。可以在面板中找到这些统计信息。

配置服务提供者用户管理员角色

要配置服务提供者用户管理员角色，请创建一个管理员角色，然后指定控制范围、权能以及应将其分配给的用户。

注 – 在创建服务提供商用户管理员角色之前，应为管理员角色定义搜索上下文、搜索过滤器、搜索过滤器后、权能和用户分配规则。

要使用以下规则，您必须指定该规则的 `authType`：

- SPEUsersSearchContextRule
- SPEUsersSearchFilterRule
- SPEUsersAfterSearchFilterRule
- CapabilitiesOnSPEUserRule
- UserIsAssignedAdminRoleRule
- SPEUserIsAssignedAdminRoleRule

Identity Manager 提供了示例规则，您可以使用这些示例规则为服务提供者用户管理员角色创建这些规则。您可以在 Identity Manager 安装目录的 `sample/adminRoleRules.xml` 中找到这些规则。

有关为您的环境创建这些规则的详细信息，请参见《Sun Identity Manager Service Provider 8.1 Deployment》。

▼ 配置服务提供者用户管理员角色

1 **在管理员界面中，单击菜单中的“安全性”，然后单击“管理员角色”。**
将打开“管理员角色”页。

2 **单击“新建”。**
将打开“创建管理员角色”页。

3 **指定管理员角色的名称，并选择“服务提供者用户”类型。**

4 **按照以下各节所述，指定“控制范围”、“权能”和“分配给用户”选项。**

指定控制范围

服务提供者用户管理员角色的控制范围可指定允许给定的 Identity Manager 管理员、Identity Manager 最终用户或 Identity Manager 服务提供者最终用户查看的服务提供者用户。如果请求在目录中列出服务提供商用户，则会强制指定控制范围。

您可以为服务提供商用户管理员角色控制范围指定以下一个或多个设置：

- **用户搜索上下文**。指定是使用规则还是文本字符串来开始搜索。
  如果指定为“无”，则默认搜索上下文将是配置为服务提供者用户目录的 Identity Mananger 资源中指定的基本上下文。
- **用户搜索过滤器**。指定搜索过滤器是应用规则还是文本字符串。
  所选规则指定或返回的文本字符串应为表示用户集的 LDAP 兼容的搜索过滤器字符串，在搜索上下文中，这些用户将由分配了此管理员角色的用户控制。指定的过滤器将与用户指定的搜索过滤器结合，以确保搜索返回的用户不包括分配了此 AdminRole 的用户无权列出的任何用户。
- **用户搜索过滤器后规则**。选择在应用用户搜索过滤器后将应用的规则。
  该规则在对服务提供者用户目录执行初始 LDAP 搜索后运行，并评估结果以确定允许请求用户访问的识别名 (DN)。
  当需要使用非 LDAP 用户属性（例如组成员资格）确定用户是否应在请求用户的控制范围中时，或需要使用信息库而不是服务提供者用户目录（例如 Oracle 数据库或 RACF）做出过滤决策时，可以使用该类型的规则。

指定权能

服务提供商用户管理员角色的权能用于指定请求用户对所请求访问的服务提供商用户具有的权能和权限。如果请求查看、创建、修改或删除服务提供商用户，则会强制指定权能。

在“权能”选项卡上，选择要为该管理员角色应用的“权能规则”。

为用户分配管理员角色

通过指定将在登录时进行评估以确定是否向验证用户分配管理员角色的规则，可以将服务提供商用户管理员角色动态地分配给服务提供商用户。

单击“分配给用户”选项卡，然后选择要为分配应用的规则。

注 – 必须为每个登录界面（例如用户界面和管理员界面）启用将管理员角色动态分配给用户的操作，方法是：将以下系统配置对象（第 102 页中的 “编辑 Identity Manager 配置对象”）设置为 `true`：

`security.authz.checkDynamicallyAssignedAdminRolesAtLoginTo.` *logininterface*

所有界面的默认值为 `false`。

委托服务提供商用户管理员角色

默认情况下，服务提供商用户可以将分配给他们的服务提供商用户管理员角色分配（或**委托**）给其控制范围内的其他服务提供商用户。

事实上，任何具有编辑服务提供者用户权能的 Identity Manager 用户均可将分配给他们的服务提供者用户管理员角色分配给其控制范围内的服务提供者用户。

服务提供商用户管理员角色还可以包括**分配者**列表，无论是何控制范围，这些分配者均可分配管理员角色。这些直接分配可以确保至少一个已知用户帐户可以分配管理员角色。

管理服务提供商用户

本节介绍了通过 Identity Manager 管理服务提供者用户的步骤和信息。

本节包含以下主题：

用户组织

通过服务提供者，用户的属性值可以确定将该用户分配给哪个组织。这是在服务提供者主配置的 Identity Manager 组织属性名称字段中指定的（请参见第 450 页中的 “初始配置”）。但是，这些组织的名称必须与目录服务器中分配的用户属性值相匹配。

如果定义了 Identity Manager 组织属性名称，则“创建用户”和“编辑用户”页上将显示可用组织的多重选择列表。默认情况下显示组织的简称。您可以修改服务提供者用户表单以显示完整的组织路径。

您可以选择哪个属性将成为组织名称属性。然后便可在服务提供者用户管理页面中使用该组织名称属性限制可以搜索并管理该用户的管理员。

注 – 现在具有服务提供者和资源帐户的帐户 ID 和密码策略。

可以从主“策略”表中找到“服务提供者系统帐户策略”。

创建用户和帐户

所有服务提供者用户均必须在服务提供者目录中具有帐户。如果用户具有其他资源的帐户，则这些帐户的链接将存储在用户的目录条目中，因此查看用户时可使用有关这些帐户的信息。

注 – 提供了用于创建和编辑用户的服务提供者用户表单示例。自定义该表单以满足您在服务提供商环境中管理用户的需求。有关详细信息，请参见《Sun Identity Manager Deployment Reference》中的第 2 章 “Identity Manager Forms”。

▼ 创建服务提供者帐户

1. **在管理员界面中，单击菜单栏中的“帐户”。**
2. **单击“管理服务提供者用户”选项卡。**
3. **单击“创建用户”。**

注 – 使用默认的服务提供者用户表单时，实际显示的字段取决于在服务提供者目录资源的“帐户属性”表（模式映射）中配置的属性。而且，当您向用户（例如委托管理员）分配资源时，将看到新添加到显示部分中的段，您可以在其中指定这些资源的属性值。您也可以自定义字段。

---

4. **根据需要，为这些资源指定属性值。**

   这些属性值包括：

   - **帐户 ID**（必需）
   - **密码**
   - **确认**（密码确认）
   - **名字**（必需）

- 姓氏（必需）
- 全名
- 电子邮件
- 住宅电话
- 移动电话
- 密码重试计数
- 解除锁定帐户时间

5 使用方向键从“可用”列表中分配所有所需的“资源”。

6 “帐户状态”用于显示帐户处于锁定还是解除锁定状态。单击该选项可以锁定或解除锁定帐户。

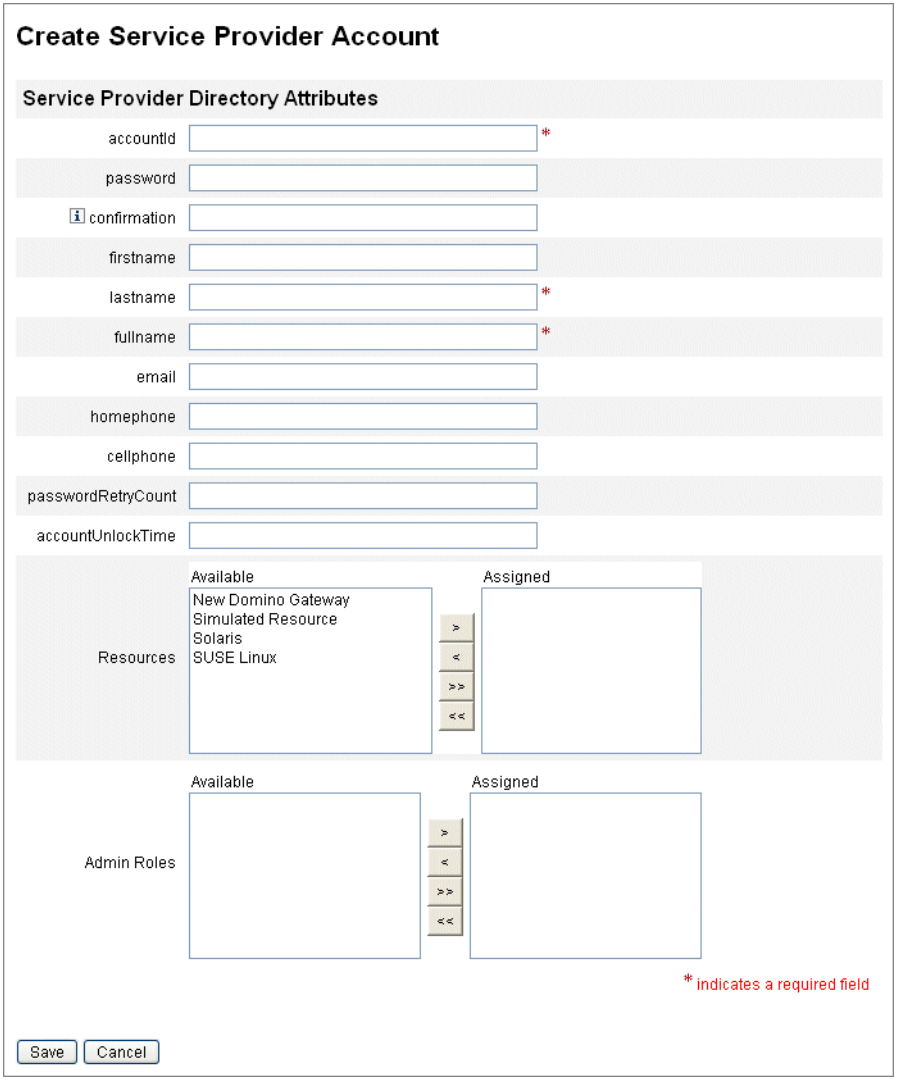


图 17–9 创建服务提供商用户和帐户

注 – 该表单可根据为目录帐户（在顶部）定义的属性自动填充资源帐户属性的值。例如，如果资源定义 `firstName`，则产品将使用目录帐户中的 `firstName` 值对其进行填充。但是在此初始填充后，对这些属性的修改不会推送到资源帐户。如果需要，请自定义提供的示例服务提供者用户表单。

---

7 单击“保存”以创建用户帐户。

搜索服务提供者用户

服务提供者包括可配置的搜索权能，可帮助管理用户帐户。搜索仅返回在您的范围（如组织所定义的，或可能由其他因子所定义的）内的用户。

要执行服务提供者用户的基本搜索，请在 Identity Manager 界面中的“帐户”区域中，单击“管理服务提供者用户”，然后输入搜索值并单击“搜索”。

以下主题介绍了服务提供者搜索功能：

高级搜索

可以使用以下说明执行服务提供者用户的高级搜索。

▼ 执行服务提供者用户的高级搜索

1. **在“服务提供者用户搜索”页中，单击“高级”。**
2. **从列表中选择所需的“属性”。**
3. **从列表中选择所需的“操作”。**
   通过指定一组条件以过滤搜索返回的用户，且返回的用户必须满足所有指定的条件。
4. **输入所需的搜索值，然后单击“搜索”。**

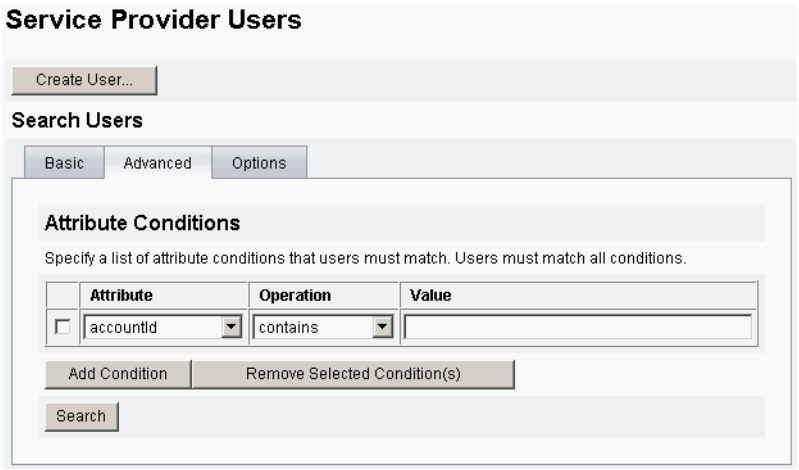


图 17–10 搜索用户

您可以使用以下选项添加或删除属性条件。

- 单击“添加条件”并指定新的属性。
- 选择项目并单击“删除选定条件”。

搜索结果

服务提供者搜索结果将显示在表中，如图 17–11 中所示。单击属性的列标题，可以按任意属性对结果进行排序。显示的结果取决于您选择的属性。

使用箭头按钮可转至结果的首页、上一页、下一页和尾页。在文本框中输入数字并按 Enter 键，可跳转至特定页。

要编辑用户，请单击表中的用户名。

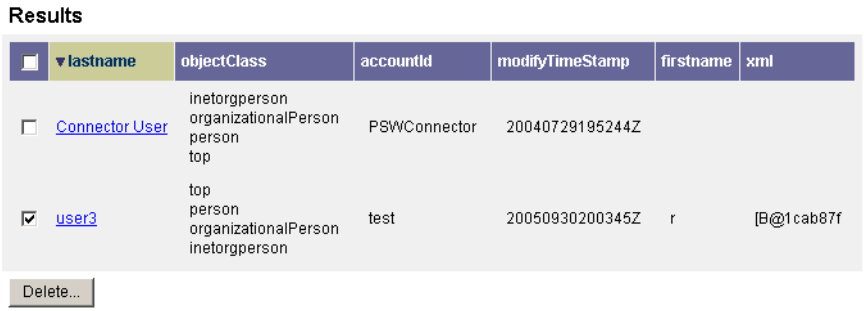


图 17–11 搜索结果示例

通过搜索结果页，可以删除用户或解除资源帐户的链接，方法是通过选择一个或多个用户然后单击“删除”按钮。该操作将打开删除用户页，并显示其他选项（请参见第 477 页中的 “删除、取消分配帐户或解除帐户的链接”）

链接帐户

服务提供者可安装于用户在多个资源上具有帐户的环境中。通过使用服务提供者的帐户链接功能，您可以以增量方式将现有资源帐户分配给服务提供者用户。帐户链接过程由服务提供者链接策略控制，此策略可定义链接关联规则、链接确认规则和链接验证选项。

▼ 链接用户帐户

1. **在管理员界面中，单击菜单栏中的“资源”。**
2. **选择所需的资源。**
3. **在“资源操作”菜单中选择“编辑服务提供者链接策略”。**
4. **选择链接关联规则。此规则可搜索用户可能拥有的资源上的帐户。**
5. **选择链接确认规则。此规则可从链接关联规则所选的潜在帐户列表中清除所有资源帐户。**

注 – 如果链接关联规则仅选择一个帐户，则不需要链接确认规则。

---

6. **选择“要求链接验证”，将目标资源帐户链接到服务提供者用户。**

删除、取消分配帐户或解除帐户的链接

▼ 删除、取消分配用户帐户或解除用户帐户的链接

1. **在菜单栏中单击“帐户”。**
2. **单击“管理服务提供者用户”。**
3. **执行基本搜索或高级搜索。**
4. **选择所需的一个或多个用户。**
5. **单击“删除”按钮。**
6. **选择可选全局选项之一。**

这些选项包括：

- **删除所有资源帐户**

  注 – 删除资源将删除该资源帐户，但资源分配依然存在。对用户进行后续更新将重新创建帐户。但删除资源始终会将该资源帐户取消链接。

- **取消分配所有资源帐户**

  注 – 取消分配资源将删除该资源分配。取消分配会将资源帐户取消链接。取消分配资源时，将不删除该资源帐户。

- **取消链接所有资源帐户**

  注 – 取消链接将删除用户和资源帐户之间的链接，但并不删除帐户。也不会删除资源分配，因此对用户进行后续更新将重新链接帐户或在资源上新建帐户。

7. **也可以在“删除”、“取消分配”或“解除链接”列中为一个或多个资源帐户选择一个操作。**
8. **选择所需用户帐户后，单击“确定”。**

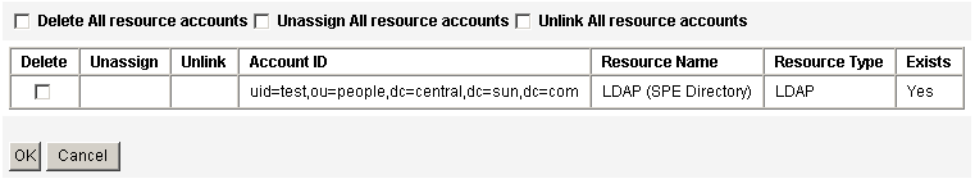


图 17–12 删除、取消分配帐户或解除帐户的链接

设置搜索选项

▼ 设置服务提供者用户的搜索选项

1. **在管理员界面中，单击菜单栏中的“帐户”。**
2. **单击“服务提供者”。**
3. **单击“选项”。**

注 – 这些选项仅对当前登录会话有效。这些选项会影响搜索结果的显示方式，它们会影响基本搜索结果和高级搜索结果，并且某些设置仅对新搜索有效。

4 **输入“返回的最大结果数”。**

5 **输入“每页的结果数”。**

6 **使用方向键从“可用的属性”中选择所需的“显示属性”。**

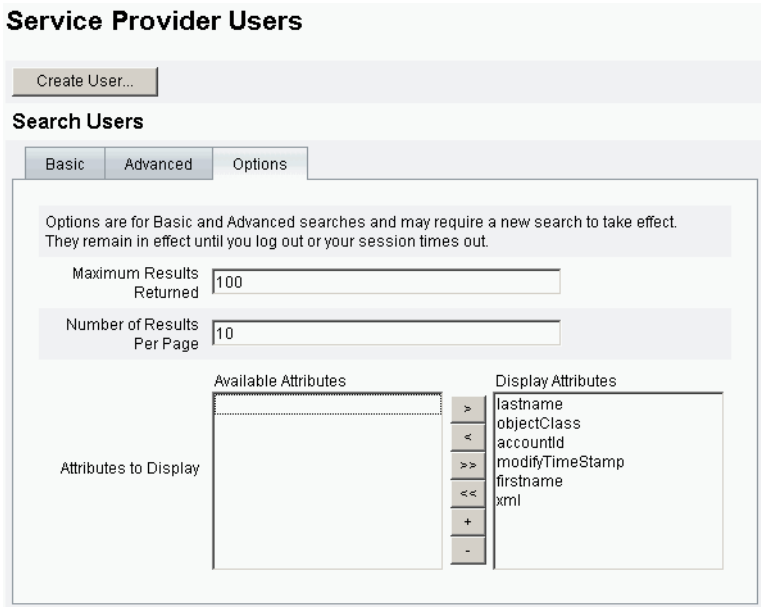


图 17–13 设置服务提供者用户的搜索选项

最终用户界面

随附的最终用户页面样例提供了 xSP 环境中典型的注册和自助服务示例。这些样例是可扩展的并且可以对其进行自定义。您可以更改外观、修改页面之间的导航规则或显示用于部署的特定于语言环境的消息。有关自定义最终用户页面的详细信息，请参见《Sun Identity Manager Service Provider 8.1 Deployment》。

除了审计自助服务和注册事件以外，还可以使用电子邮件模板将通知发送给受影响的用户。还提供了使用帐户 ID 和密码策略以及帐户锁定的示例。应用程序开发者还可以使用 Identity Manager 表单。如果需要，可以扩展或替换作为 Servlet 过滤器实现的模块验证服务。这样，便可与访问管理系统（如 Sun Access Manager）集成在一起。

最终用户页面示例

使用随附的样例最终用户页面，用户可以通过一系列易于导航的屏幕注册和维护基本用户信息，并接收其操作的电子邮件通知。

示例页面包括以下功能：

- 登录（和退出），包括使用质询问题进行验证
- 注册
- 密码更改
- 用户名更改
- 质询问题更改
- 通知地址更改
- 处理忘记用户名的情况
- 处理忘记密码的情况
- 电子邮件通知
- 审计

注 – Identity Manager 使用验证表进行注册。仅允许该表中的用户进行注册。例如，当用户 Betty Childs 注册时，如果在验证表中找到 Betty Childs 的条目（包含电子邮件地址 bchilds@example.com），则接受注册。

可以为您的部署轻松自定义这些页面。

可以方便地为您的部署自定义这些页面，如下所示：

- 更改品牌信息
- 修改配置选项（例如失败的登录尝试次数）
- 添加或删除页面

有关自定义这些页面的详细信息，请参见《Sun Identity Manager Service Provider 8.1 Deployment》。

新用户注册

要求新用户注册。在注册期间用户可以设置其登录、质询问题和通知信息。

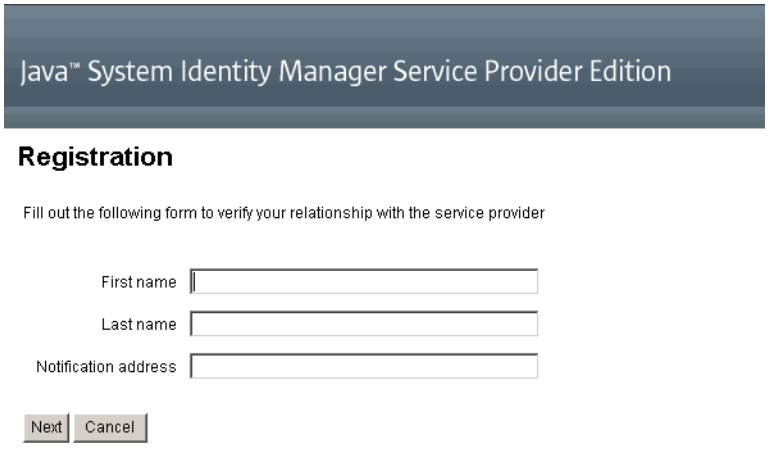


图 17–14 “注册”页

“主页”屏幕和配置文件屏幕

图 17–15 显示了最终用户“主页”选项卡和配置文件页面。用户可以更改其登录 ID 和密码、管理通知及创建质询问题。

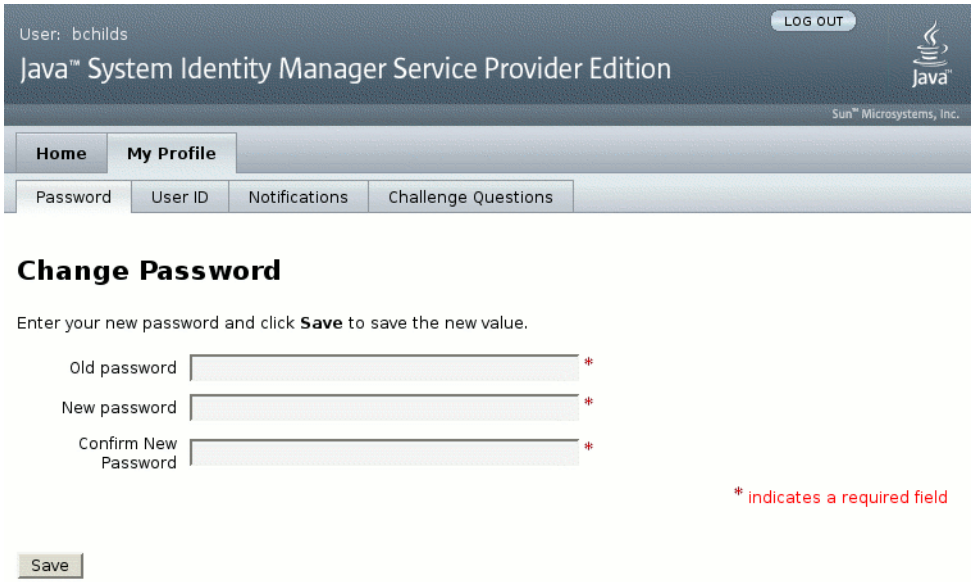


图 17–15 “我的配置文件”页

服务提供者用户同步

可通过同步策略启用服务提供者用户同步。要使用 Identity Manager 为服务提供者用户同步资源上属性的更改，您必须配置服务提供者同步。

以下主题介绍了如何在服务提供商实现中启用同步：

注 – 从 Identity Manager 的“资源”区域的资源列表中配置服务提供者同步。

配置同步

要配置服务提供者同步，请按第 227 页中的“编辑或配置同步”中所述编辑资源的同步策略。

编辑同步策略时，必须指定以下选项以启用服务提供商用户的同步进程。

- 选择“服务提供者用户”作为“目标对象类型”。
- 在“调度设置”段中，选择“启用同步”。

按照第 227 页中的“编辑或配置同步”中的说明，指定适合您的环境的其他选项。服务提供者同步任务的默认同步间隔为 1 分钟。

注 – 确认规则和表单必须使用 IDMXUser 视图，而非 Identity Manager 输入用户视图（有关详细信息，请参见《Sun Identity Manager Service Provider 8.1 Deployment》）。

这是必需的，因为确认规则会访问关联规则中标识的每个用户的用户视图，从而影响同步性能。

单击“保存”可以保存策略定义。如果在策略中未禁用同步，则按指定对其进行调度。如果指定禁用同步，则将停止同步服务（如果当前正在运行）。如果启用，则重新启动 Identity Manager 服务器时，或在“同步资源操作”下选择“启动服务提供者”时，将启动同步。

监视同步

Identity Manager 提供了以下方法来监视服务提供者同步。

- 在“资源”列表上的描述字段中查看同步状态。
- 使用 JMX 界面监视同步度量。

启动和停止同步

默认情况下，在为服务提供者实现配置 Identity Manager 时，将启用服务提供者同步。

▼ 禁用服务提供者活动同步

1. **在管理员界面中，单击菜单中的“资源”。**
   将打开“列出资源”页。
2. **在“服务提供者”区域中，选择资源，然后单击“编辑同步策略”以编辑策略。**
3. **清除“启用同步”复选框。**
4. **单击“保存”。**
   保存策略后，同步将停止。

   要停止同步而不将其禁用，请从“同步资源操作”中选择“停止服务提供者”。

注 – 如果通过使用资源操作停止同步，而不是禁用同步，则启动任何 Identity Manager 服务器后将再次启动同步。

迁移用户

服务提供者功能包含示例用户迁移任务及关联的脚本。该任务将现有 Identity Manager 用户迁移到服务提供者用户目录中。本节介绍如何使用示例迁移任务。建议您修改该示例以用于您的环境。

▼ 迁移现有 Identity Manager 用户

1. **在管理员界面中，单击菜单中的“服务器任务”。**
   将打开“查找任务”页。
2. **单击次级菜单中的“运行任务”。**
3. **单击“SPE 迁移”。**
4. **输入唯一的“任务名称”。**
5. **从列表中选择“资源”。**
   这是 Identity Manager 中的一个资源，它表示服务提供者目录服务器。不会迁移在 Identity Manager 用户中找到的该资源的链接。

6 **输入“身份属性”。**

这是包含目录用户的唯一简短身份的 Identity Manager 用户属性。

7 **从列表中选择“身份规则”。**

这是可以通过 Identity Manager 用户的属性计算目录用户名称的可选规则。身份规则可以计算简单名称（通常为 UID），然后会通过资源的身份模板处理该简短名称，以形成目录服务器的标识名 (Distinguished Name, DN)。该规则还可以返回不使用 ID 模板的完全指定的 DN。

8 **单击“启动”可启动后台迁移任务。**

配置服务提供者审计事件

在服务提供者实现中，Identity Manager 的审计日志记录系统可以审计与外联网用户活动相关的事件。Identity Manager 提供了服务提供者审计配置组（默认情况下已启用），该配置组可指定为服务提供者用户记录的审计事件。请参见图 17–16。

有关审计日志记录和修改服务提供者审计配置组中的事件的详细信息，请参见第 10 章，审计日志记录。

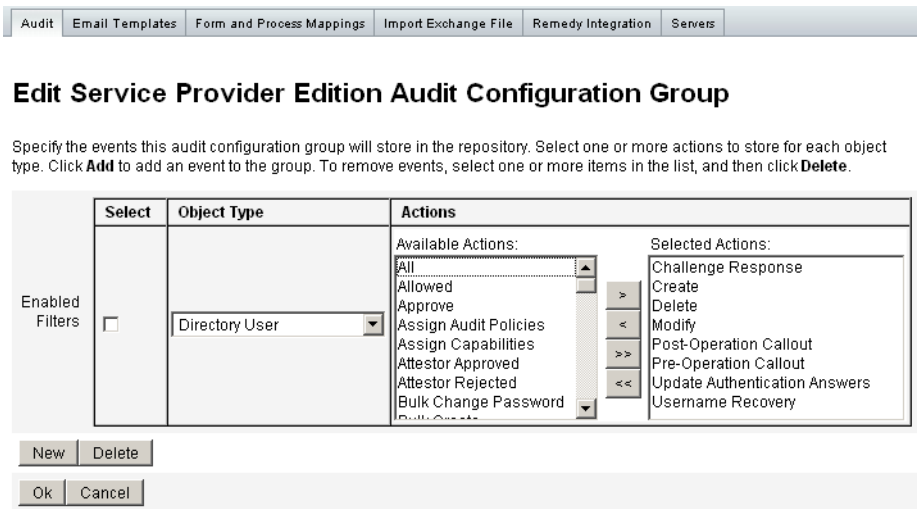


图 17–16 “编辑服务提供者审计配置组”页

◆ ◆ ◆ 附 录 A

lh 参考消息

本附录提供了一些有助于您使用 Identity Manager 命令行界面和执行 Identity Manager 命令的信息。

该信息包括以下主题：

lh 命令语法

可以使用以下语法调用 Identity Manager 命令行界面和执行 Identity Manager 命令：

```
lh { $class | $command } [ $arg [$arg... ] ]
```

其中：

- class 必须是全限定类名，如 com.waveset.session.WavesetConsole。
- command 必须是以下命令之一：
  - assessment 可以在升级期间使用。支持用于报告所有修改的对象和报告所有安装的 Identity Manager 版本的子命令。有关详细信息，请参见《Sun Identity Manager 8.1 Upgrade》指南。
  - config 启动业务进程编辑器。
  - console 启动 Identity Manager 控制台。
  - genReports 生成一组随机数据，可以使用这些数据来说明 Identity Manager 报告功能。
  - import 导入 Identity Manager 对象。为严格模式指定 -s 选项。在启用严格模式后，导入期间的引用检查将会比较严格。
  - js 调用 JavaScript 程序。

- javascript 还调用 JavaScript 程序。
- msgtool 基于 WPMessages.properties 生成自定义消息目录。可以处理此目录以对文本或语言进行自定义更改。
- script 执行 JavaScript 或 BeanShell。
- setRepo 设置 Identity Manager 索引系统信息库。
- setup 启动 Identity Manager 设置进程，使您可以设置许可证密钥、定义 Identity Manager 索引系统信息库和导入配置文件。
- spml 启动 SPML 浏览器。
- syslog [options] 从系统日志中提取记录。有关详细信息，请参见第 487 页中的 “syslog 命令”。
- waveset console 命令的别名。请参见上面的 console。
- xmlparse 验证 Identity Manager 对象的 XML。
- xpress [options] *Filename* 对表达式求值。有效选项为 -trace（启用跟踪输出）。

用法说明

在使用 lh 命令时，必须注意以下说明：

- 要查看命令用法帮助，请键入 lh（不带任何参数）。
- 在为 lh 命令设置路径环境变量时，
  - 请将 JAVA_HOME 位置设置为 JRE 目录，其中包含 bin 目录及 Java 可执行文件。此位置因安装而异。

    如果具有 Sun 的标准 JRE（不含 JDK），通常的目录位置为 C:\Program Files\Java\jre1.5.0_14（或类似位置）。此目录包含带 Java 可执行文件的 bin 目录。此时，将 JAVA_HOME 设置为 C:\Program Files\Java\jre1.5.0_14。

    完整的 JDK 安装含有多个 Java 可执行文件。此时，将 JAVA_HOME 设置为含有正确 bin/java.exe 文件的嵌入式 jre 目录。对于典型安装，将 JAVA_HOME 设置为 C:\java\jdk1.5.0_14\jre。
  - 将 WSHOME 变量设置为 Identity Manager 安装目录，如下所示：

    ```
    set WSHOME=<path_to_identity_manager_directory>
    ```

    例如，要将变量设置为默认安装目录，请键入：

    ```
    set WSHOME=C:\Program Files\tomcat\webapps\idm
    ```

注 – WSHOME 变量值**不得**包含以下字符：

- 引号 (" ")
  不要使用引号，即使应用程序部署目录的路径中包含空格。
- 路径末尾处的反斜杠 (\)

在 UNIX 系统上，还必须键入以下命令以导出路径变量：

```
export WSHOME
export JAVA_HOME
```

- 要在 64 位模式下运行命令，请取消注释 lh 脚本中的 FLAGS="$FLAGS -d64" 行。
- 启动 Identity Manager 命令行界面
  - 在 Windows 的命令行中键入以下命令：

    ```
    %WSHOME%\bin\lh
    ```
  - 在 UNIX 的命令行中键入以下命令：

    ```
    $WSHOME/bin/lh
    ```

lh 命令示例

- lh com.waveset.session.WavesetConsole
- lh console
- lh console– u $user– p *PathtoPassword*.txt
- lh setup -U *Administrator* -P *PathtoPassword*.txt
- lh setRepo– c -A *Administrator* -C *PathtoPassword* .txt
- lh setRepo– t *LocalFiles* – f $WSHOME

syslog 命令

本节提供了有关 syslog 命令的信息，其中包括：

- 第 487 页中的 “syslog 命令用法”
- 第 488 页中的 “syslog 命令选项”

syslog 命令用法

可以使用以下语法调用 syslog 命令：

```
syslog [options]
```

syslog 命令选项

可以使用以下选项包含或排除信息。

表 A–1 syslog 命令选项

选项	描述
-d *Number*	显示前 *Number* 天（默认值=1）的记录。
-E	仅显示严重级别为“错误”或以上级别的记录。
-F	仅显示严重级别为“致命”的记录。
-i *LogID*	仅显示具有指定系统日志 ID 的记录。 系统日志 ID 显示在某些错误消息上，并引用特定系统日志条目。
-W	仅显示严重级别为“警告”或以上级别的记录（默认）。
-X	包括报告的错误原因（如果可用）。

◆ ◆ ◆ 附 录 B

审计日志数据库模式

此附录提供了有关支持的数据库类型的审计数据模式值和审计日志数据库映射的信息。

Oracle 数据库类型

表 B–4 列出了 Oracle 数据库类型的数据模式值。

表 B–1 Oracle 数据库类型的数据模式值

数据库列	值
id	VARCHAR(50) NOT NULL
name	VARCHAR(128)NOT NULL
repomod	TIMESTAMP
resourceName	VARCHAR(128)
accountName	VARCHAR(50)
objectType	CHAR(2)
objectName	VARCHAR(128)
action	CHAR(2)
actionDateTime	CHAR(21)

表 B–1 Oracle 数据库类型的数据模式值 （续）

数据库列	值
actionStatus	CHAR(1)
interface	VARCHAR(50)
server	VARCHAR(128)
subject	VARCHAR(128)
reason	CHAR(2)
message	VARCHAR(255) 或 CLOB（请参见表结尾处的注释[1]。）
acctAttrChanges	VARCHAR(4000) 或 CLOB
acctAttr01label	VARCHAR(50)
acctAttr01value	VARCHAR(128)
acctAttr02label	VARCHAR(50)
acctAttr02value	VARCHAR(128)
acctAttr03label	VARCHAR(50)
acctAttr03value	VARCHAR(128)
acctAttr04label	VARCHAR(50)
acctAttr04value	VARCHAR(128)
acctAttr05label	VARCHAR(50)
acctAttr05value	VARCHAR(128)
parm01label	VARCHAR(50)
parm01value	VARCHAR(128) 或 CLOB（请参见表结尾处的注释[1]。）
parm02label	VARCHAR(50)
parm02value	VARCHAR(128) 或 CLOB（请参见表结尾处的注释[1]。）
parm03label	VARCHAR(50)
parm03value	VARCHAR(128) 或 CLOB（请参见表结尾处的注释[1]。）
parm04label	VARCHAR(50)
parm04value	VARCHAR(128) 或 CLOB（请参见表结尾处的注释[1]。）
parm05label	VARCHAR(50)
parm05value	VARCHAR(128) 或 CLOB（请参见表结尾处的注释[1]。）
sequence	CHAR(19)

表 B–1 Oracle 数据库类型的数据模式值 （续）

数据库列	值
xmlSize	NUMBER(19,0)
xml	BLOB

注 – 可以配置这些列的列长度限制。默认数据类型为 VARCHAR，并在括号内注明了默认大小限制。有关如何调整大小限制的信息，请参见第 306 页中的 “审计日志配置”。

DB2 数据库类型

表 B–2 列出了 DB2 数据库类型的数据模式值。

表 B–2 DB2 数据库类型的数据模式值

数据库列	值
id	VARCHAR(50) NOT NULL
name	VARCHAR(128)NOT NULL
repomod	TIMESTAMP
resourceName	VARCHAR(128)
accountName	VARCHAR(50)
objectType	CHAR(2)
objectName	VARCHAR(128)
action	CHAR(2)
actionDateTime	CHAR(21)
actionStatus	CHAR(1)
interface	VARCHAR(50)
server	VARCHAR(128)
subject	VARCHAR(128)
reason	CHAR(2)
message	VARCHAR(255) 或 CLOB（请参见表结尾处的注释[1]。）
acctAttrChanges	CLOB(16M)

表 B–2 DB2 数据库类型的数据模式值 （续）

数据库列	值
acctAttr01label	VARCHAR(50)
acctAttr01value	VARCHAR(128)
acctAttr02label	VARCHAR(50)
acctAttr02value	VARCHAR(128)
acctAttr03label	VARCHAR(50)
acctAttr03value	VARCHAR(128)
acctAttr04label	VARCHAR(50)
acctAttr04value	VARCHAR(128)
acctAttr05label	VARCHAR(50)
acctAttr05value	VARCHAR(128)
parm01label	VARCHAR(50)
parm01value	VARCHAR(128) 或 CLOB（请参见表结尾处的注释[1]。）
parm02label	VARCHAR(50)
parm02value	VARCHAR(128) 或 CLOB（请参见表结尾处的注释[1]。）
parm03label	VARCHAR(50)
parm03value	VARCHAR(128) 或 CLOB（请参见表结尾处的注释[1]。）
parm04label	VARCHAR(50)
parm04value	VARCHAR(128) 或 CLOB（请参见表结尾处的注释[1]。）
parm05label	VARCHAR(50)
parm05value	VARCHAR(128) 或 CLOB（请参见表结尾处的注释[1]。）
sequence	CHAR(19)
xmlSize	DECIMAL(19,0)
xml	CLOB(16M)

注 – 可以配置这些列的列长度限制。默认数据类型为 VARCHAR，并在括号内注明了默认大小限制。有关如何调整大小限制的信息，请参见第 306 页中的 “审计日志配置”。

MySQL 数据库类型

表 B–3 列出了 MySQL 数据库类型的数据模式值。

表 B–3 MySQL 数据库类型的数据模式值

数据库列	值
id	VARCHAR(50) BINARY NOT NULL
name	VARCHAR(128) BINARY NOT NULL
repomod	TIMESTAMP
resourceName	VARCHAR(128)
accountName	VARCHAR(255)
objectType	CHAR(2)
objectName	VARCHAR(128)
action	CHAR(2)
actionDateTime	CHAR(21)
actionStatus	CHAR(1)
interface	VARCHAR(50)
server	VARCHAR(128)
subject	VARCHAR(128)
reason	CHAR(2)
message	VARCHAR(255) 或 CLOB（请参见表结尾处的注释[1]。）
acctAttrChanges	TEXT
acctAttr01label	VARCHAR(50)
acctAttr01value	VARCHAR(128)
acctAttr02label	VARCHAR(50)
acctAttr02value	VARCHAR(128)
acctAttr03label	VARCHAR(50)
acctAttr03value	VARCHAR(128)
acctAttr04label	VARCHAR(50)
acctAttr04value	VARCHAR(128)

表 B–3 MySQL 数据库类型的数据模式值 （续）

数据库列	值
acctAttr05label	VARCHAR(50)
acctAttr05value	VARCHAR(128)
parm01label	VARCHAR(50)
parm01value	VARCHAR(128) 或 CLOB（请参见表结尾处的注释[1]。）
parm02label	VARCHAR(50)
parm02value	VARCHAR(128) 或 CLOB（请参见表结尾处的注释[1]。）
parm03label	VARCHAR(50)
parm03value	VARCHAR(128) 或 CLOB（请参见表结尾处的注释[1]。）
parm04label	VARCHAR(50)
parm04value	VARCHAR(128) 或 CLOB（请参见表结尾处的注释[1]。）
parm05label	VARCHAR(50)
parm05value	VARCHAR(128) 或 CLOB（请参见表结尾处的注释[1]。）
sequence	CHAR(19)
xmlSize	BIGINT
xml	MEDIUMTEXT

注 – 可以配置这些列的列长度限制。默认数据类型为 VARCHAR，并在括号内注明了默认大小限制。有关如何调整大小限制的信息，请参见第 306 页中的 “审计日志配置”。

SQL Server 数据库类型

表 B–4 列出了 SQL Server 数据库类型的数据模式值。

表 B–4 SQL Server 数据库类型的数据模式值

数据库列	值
id	NVARCHAR(50) NOT NULL
name	NVARCHAR(128) NOT NULL
repomod	DATETIME NOT NULL CURRENT_TIMESTAMP

表 B–4 SQL Server 数据库类型的数据模式值 （续）

数据库列	值
resourceName	NVARCHAR(128)
accountName	NVARCHAR(255)
objectType	NCHAR(2)
objectName	NVARCHAR(128)
action	NCHAR(2)
actionDateTime	NCHAR(21)
actionStatus	NCHAR(1)
interface	NVARCHAR(50)
server	NVARCHAR(128)
subject	NVARCHAR(128)
reason	NCHAR(2)
message	NVARCHAR(255) 或 CLOB（请参见表结尾处的注释[1]。）
acctAttrChanges	NTEXT
acctAttr01label	NVARCHAR(50)
acctAttr01value	NVARCHAR(128)
acctAttr02label	NVARCHAR(50)
acctAttr02value	NVARCHAR(128)
acctAttr03label	NVARCHAR(50)
acctAttr03value	NVARCHAR(128)
acctAttr04label	NVARCHAR(50)
acctAttr04value	NVARCHAR(128)
acctAttr05label	NVARCHAR(50)
acctAttr05value	NVARCHAR(128)
parm01label	NVARCHAR(50)
parm01value	NVARCHAR(128) 或 CLOB（请参见表结尾处的注释[1]。）
parm02label	NVARCHAR(50)
parm02value	NVARCHAR(128) 或 CLOB（请参见表结尾处的注释[1]。）
parm03label	NVARCHAR(50)

表 B–4 SQL Server 数据库类型的数据模式值 （续）

数据库列	值
parm03value	NVARCHAR(128) 或 CLOB（请参见表结尾处的注释[1]。）
parm04label	NVARCHAR(50)
parm04value	NVARCHAR(128) 或 CLOB（请参见表结尾处的注释[1]。）
parm05label	NVARCHAR(50)
parm05value	NVARCHAR(128) 或 CLOB（请参见表结尾处的注释[1]。）
sequence	NTEXT
xmlSize	NUMERIC(19,0)
xml	NTEXT

注 – 可以配置这些列的列长度限制。默认数据类型为 VARCHAR，并在括号内注明了默认大小限制。有关如何调整大小限制的信息，请参见第 306 页中的 “审计日志配置”。

审计日志数据库映射

表 B–5 包含存储的审计日志数据库键和显示字符串之间的映射，这些字符串即键在审计报告输出中的映射结果。Identity Manager 将作为常量使用的项目存储为简短的数据库键，以节省系统信息库中的空间。产品界面不显示这些映射。相反，只有在检查审计报告结果的转储输出时可以看到它们。

表 B–6 包含可审计的操作数据库键，表 B–7 包含操作状态键，表 B–8 包含以键的形式存储在数据库中的原因代码。

表 B–5 对象键类型数据库键

类型名称	英文文本	DbKey
AccessReview	AccessReview	AV
AccessReviewWorkflow*	Access Review Workflow	AW
AccessScan	AccessScan	AS
Account	Account	AN
AdminGroup	Capability	AG
Administrator	Administrator	AD

表 B–5 对象键类型数据库键 （续）

类型名称	英文文本	DbKey
AdminRole	Admin Role	AR
Application	Resource Group	AP
AttributeDefinition	AttributeDefinition	AF
AttrParse	AttrParse	AT
AuditConfig	AuditConfig	AC
AuditPolicy	AuditPolicy	CP
BeanPod	Bean Pod	BP
ComplianceViolation	ComplianceViolation	CV
Configuration	Configuration	CN
DataExporter	Data Exporter	DE
Discovery	Discovery	DS
Email*	Email	EM
EmailTemplate	EmailTemplate	ET
EncryptionKey	EncryptionKey	KY
Event	Event	EV
Extract	Extract	ER
ExtractTask	ExtractTask	EX
IDMXUser*	Directory User	UX
LighthouseAccount*	Identity System Account	LA
LoadConfig	LoadConfig	LD
LoadTask	LoadTask	LT
Log	Log	LG
LoginApp	LoginApp	LP
LoginConfig	LoginConfig	LC
LoginModGroup	LoginModGroup	LF
MetaView	Meta View	MV
ObjectGroup	Organization	OG
Policy	Policy	PO

表 B–5 对象键类型数据库键 （续）

类型名称	英文文本	DbKey
ProvisioningTask	ProvisioningTask	PT
RemediationWorkflow*	Remediation Workflow	RW
RemedyConfig	RemedyConfig	RC
Resource	Resource	RS
ResourceAccount*	Resource Account	RA
ResourceAction	ResourceAction	RN
ResourceForm	ResourceForm	RF
ResourceObject	ResourceObject	RE
RiskReportTask	RiskReportTask	RR
Role	Role	RL
Rule	Rule	RU
SnapShot	SnapShot	SS
ServerObject	ServerObject	SV
SysLog	SysLog	SL
System	System	SY
TaskDefinition	TaskDefinition	TD
TaskInstance	TaskInstance	TI
TaskResult	TaskResult	TR
TaskResultPage	ResultPage	TP
TaskSchedule	TaskSchedule	TS
TaskTemplate	TaskTemplate	TT
TestNotification*	Test Notification	TN
User	User	US
UserEntitlement	UserEntitlement	UE
UserForm	UserForm	UF
WorkflowCase*	Workflow Case	WC
WorkItem	WorkItem	WI
XmlData	XmlData	XD

[1]

表 B–6 操作数据库键

操作名称	英文文本	DbKey
Allowed*	Allowed	AL
Approve	Approve	AP
Assign Audit Policies	Assign Audit Policies	AA
Assign Capabilities	Assign Capabilities	AC
AttestorApproved*	Attestor Approved	TA
AttestorRejected*	Attestor Rejected	AR
AttestorRemediate*	Remediation Requested	AF
AttestorRescan*	Rescan Requested	AN
Bulk Change Password	Bulk Change Password	BW
Bulk Create	Bulk Create	BC
Bulk Delete	Bulk Delete	BD
Bulk Deprovision	Bulk Deprovision	BP
Bulk Disable	Bulk Disable	BF
Bulk Enable	Bulk Enable	BE
Bulk Modify	Bulk Modify	BM
Bulk Reset Password	Bulk Reset Password	BR
Bulk Unassign	Bulk Unassign	BU
Bulk Unlink	Bulk Unlink	BL
Bypass Verify	Bypass Verify	BV
CancelReconcile*	Cancel Reconcile	CR
challengeResponse*	Challenge Response	CD
Change Password	Change Password	CP
Connect	Connect	CN
Control Active Sync	Control Active Sync	CA

[1] * 扩展类型

表 B–6 操作数据库键 （续）

操作名称	英文文本	DbKey
Create	Create	CT
CredentialsExpired*	Credentials Expired	CE
Debug	Debug	DB
Delegate	Delegate	DG
Delete	Delete	DL
Deprovision	Deprovision	DP
Disable	Disable	DS
Disconnect	Disconnect	DC
Enable	Enable	EN
End Activity	End Activity	EA
End Process	End Process	PE
End Workflow	End Workflow	EW
Execute	Execute	LN
Expired*	Expired	EX
Export	Export	EP
Fixed*	Fixed	FX
Import	Import	IM
List	List	LI
Lock	Lock	LK
Login	Login	LG
Logout*	Logout	LO
Mitigated*	Mitigated	VM
Modify	Modify	MO
Modify Active Sync	Modify Active Sync	MA
NativeChange*	Native Change	NC
Notify*	Notify	NO
PostOperation*	Post-Operation Callout	PT
PreOperation*	Pre-Operation Callout	PP

表 B–6 操作数据库键 （续）

操作名称	英文文本	DbKey
Prioritize*	Prioritize	PR
Provision	Provision	PV
Recurring*	Recurring	RC
Reject	Reject	RJ
Remediated*	Remediated	VR
Rename	Rename	RE
RequestReconcile*	Request Reconcile	RR
ResetPassword	ResetPassword	RP
Run Debugger	Run Debugger	RD
ScanBegin*	Scan Begin	SB
ScanEnd*	Scan End	SE
StartActivity*	Start Activity	SA
StartProcess*	Start Process	SP
StartWorkflow*	Start Workflow	SW
Terminate*	Terminate	TR
Unassign	Unassign	UA
Unlink	Unlink	UN
Unlock	Unlock	UL
updateAuthenticationAnswers*	Update Authentication Answers	AQ
usernameRecovery*	Username Recovery	UR
View	View	VW
View Only	View Only	VO

[2]

[2] * 扩展操作

表 B–7 操作状态数据库键

结果	DbKey
Success	S
Failure	F

表 B–8 以键的形式存储的原因

原因名称	英文文本	DbKey
PolicyViolation	Violation of policy {0}: {1}	PV
InvalidCredentials	Invalid Credentials	CR
InsufficientPrivileges	Insufficient Privileges	IP
DatabaseAccessFailed	Database Access Failed	DA
AccountDisabled	Account Disabled	DI

◆ ◆ ◆ 附 录 C

用户界面快速参考

表 C–1 是经常执行的 Identity Manager 任务的快速参考。该表显示了开始执行每项任务时应转到的主要 Identity Manager 界面位置，并显示了执行同一任务可以使用的替代位置或方法（如果可用）。

Identity Manager 界面任务参考

表 C–1 任务参考

要执行的任务	转至	或转至
管理 Identity Manager 用户：		
创建和编辑用户	“帐户”选项卡，“列出帐户”选项	“帐户”选项卡，“查找用户”选项（“用户帐户搜索结果”页）
批准用户帐户创建	“工作项目”选项卡，“批准”选项卡	
设置用户验证（策略）	“安全性”选项卡，“策略”选项	
更改用户密码	“密码”选项卡，“更改用户密码”选项	“帐户”选项卡，“列出帐户”选项 “帐户”选项卡，“查找用户”选项（“用户帐户搜索结果”页） Identity Manager 用户界面
重设用户密码	“密码”选项卡，“重设用户密码”选项	“帐户”选项卡，“列出帐户”选项 “帐户”选项卡，“查找用户”选项（“用户帐户搜索结果”页）

表 C–1 任务参考 （续）

要执行的任务	转至	或转至
查找用户	“帐户”选项卡，“查找用户”选项	“密码”选项卡，“更改用户密码”选项
启用或禁用用户	“帐户”选项卡，“列出帐户”选项	“帐户”选项卡，“查找用户”选项（“用户帐户搜索结果”页）
解除锁定用户	“帐户”选项卡，“列出帐户”选项	“帐户”选项卡，“查找用户”选项（“用户帐户搜索结果”页）
管理 Identity Manager 管理员：		
设置委托管理（通过组织）	“帐户”选项卡，“列出帐户”选项，“创建用户”页	
分配权能	“帐户”选项卡，“列出帐户”选项，“创建用户”或“编辑用户”页，“安全性”选项卡	
分配权能（通过管理员角色）	“帐户”选项卡，“列出帐户”选项，“创建用户”或“编辑用户”页，“安全性”选项卡	
设置批准者（验证帐户创建）	“帐户”选项卡，“列出帐户”选项，“创建组织”页 “角色”选项卡，“创建角色”页	
配置 Identity Manager：		
创建并管理资源（资源向导）	“资源”选项卡	
管理资源组	“资源”选项卡，“列出资源组”选项	
创建和管理角色	“角色”选项卡	
查找角色	“角色”选项卡，“查找角色”选项	
编辑权能	“安全性”选项卡，“权能”选项	
创建和编辑管理员角色	“安全性”选项卡，“管理员角色”选项，“创建/编辑管理员角色”页	
设置电子邮件模板	“配置”选项卡，“电子邮件模板”选项	

表 C–1 任务参考 （续）

要执行的任务	转至	或转至
设置密码、帐户和命名策略，为组织分配策略	“安全性”选项卡，“策略”选项	
加载和同步帐户和数据：		
导入数据文件（如 XML 格式的表单）	“配置”选项卡，“导入交换文件”选项	
加载资源帐户	“帐户”选项卡，“从资源加载”选项	
从文件加载帐户	“帐户”选项卡，“从文件加载”选项	
将 Identity Manager 用户与资源帐户进行比较	“资源”选项卡，“协调资源”选项	
审计和管理遵循性：		
禁用或启用审计	“配置”选项卡，“审计”选项	
设置要捕获的审计事件	“配置”选项卡，“审计”选项	
定义审计策略（创建、编辑、删除）	“遵循性”选项卡，“管理策略”选项	
分配审计策略	“帐户”选项卡，“遵循性”选项	
为审计策略定义修正者并分配修正工作流	“遵循性”选项卡，“管理策略”选项卡	
对策略违规修正请求进行响应	“我的工作项目”选项卡，“修正”选项	
缓解策略违规	“工作项目”选项卡，“修正”选项卡	
查看已修正的策略违规	“工作项目”选项卡，“修正”选项卡	
生成审计策略报告	“报告”选项卡，“运行报告”选项卡	
对一个或多个用户或组织执行审计扫描	“帐户”选项卡，从“用户操作”或“组织操作”列表中选择“扫描”	
设置周期性访问查看	“遵循性”选项卡，“管理访问扫描”选项	

表 C–1 任务参考 （续）

要执行的任务	转至	或转至
监视周期性访问查看	“遵循性”选项卡，“访问查看”选项	
查看审计报告	“报告”选项卡，“审计者报告”类型选项	
编辑管理员审计权能	“安全性”选项卡，“权能”选项卡	
设置审计通知使用的电子邮件模板	“配置”选项卡，“电子邮件模板”选项卡	
导入数据文件/规则（如 XML 格式的表单）	“配置”选项卡，“导入交换文件”选项卡	
定义访问查看扫描	“遵循性”选项卡，“管理扫描”选项卡	
运行访问查看	“遵循性”选项卡，“访问查看”选项卡	
终止访问查看	“遵循性”选项卡，“访问查看”选项卡	
调度访问查看	“服务器任务”选项卡，“管理进度表”选项卡	
设置周期性访问查看	“遵循性”选项卡，“管理访问扫描”选项卡	
监视访问查看状态	“遵循性”选项卡，“访问查看”选项卡	
配置证明者	“遵循性”选项卡，“管理访问扫描”选项卡	
执行证明者责任（查看和证明用户权利）	“工作项目”选项卡，“我的工作项目”选项卡，“证明”选项卡	
风险分析和报告：		
运行和管理报告	“报告”选项卡，“运行报告”选项（以创建、运行和下载报告）；“查看报告”选项（以查看报告结果）。	
定义和运行风险分析报告	“报告”选项卡，“风险分析”选项	

表 C–1 任务参考 （续）

要执行的任务	转至	或转至
查看图形报告	“报告”选项卡，“查看面板”选项	
查看任务划分报告	“报告”选项卡，“运行报告”选项卡	
管理 Identity Manager 任务：		
运行已定义的任务（或进程）	“服务器任务”选项卡，“运行任务”选项	
调度任务	“服务器任务”选项卡，“管理进度表”选项	
查看任务结果	“服务器任务”选项卡，“查找任务”或“所有任务”选项	
暂停或终止任务	“服务器任务”选项卡，“所有任务”选项	
管理服务提供者用户：		
管理服务提供商用户	“帐户”选项卡，“管理服务提供者用户”选项	
管理服务提供商事务	“服务器任务”选项卡，“服务提供者事务”选项	
配置服务提供商功能	“服务提供者”选项卡，“编辑主配置”选项	
配置事务默认值	“服务提供者”选项卡，“编辑事务配置”选项	
创建或编辑服务提供商策略	“安全性”选项卡，“策略”选项	

◆ ◆ ◆ 附 录 D

权能定义

本附录为 Identity Manager 中使用的各种权能提供了定义。

该信息分为以下几节：

- 第 509 页中的“基于任务的权能定义”
- 第 526 页中的“功能性权能定义”

有关权能的一般信息，请参见第 184 页中的“了解和管理权能”。

注 – 所有权能都授予用户或管理员访问“密码”→“更改我的密码”和“更改我的回答”选项卡的权限。

基于任务的权能定义

本节介绍了可以分配给用户的每种基于任务的权能。它还列出了可使用每种权能访问的选项卡和子选项卡。这些权能是按名称的字母顺序列出的。

注 – 该表不包含可供所有用户使用的默认选项卡和子选项卡（如“更改我的密码”选项卡）的相关信息。

表 D–1 Identity Manager 基于任务的权能定义

权能	管理员/用户可执行的操作	可以访问以下选项卡和子选项卡
访问查看详细信息报告管理员	创建、编辑、删除和执行访问查看详细信息报告、访问查看覆盖报告和访问扫描用户范围覆盖报告	“报告”→“运行报告”和“查看报告”选项卡

表 D–1 Identity Manager 基于任务的权能定义 （续）

权能	管理员/用户可执行的操作	可以访问以下选项卡和子选项卡
访问查看摘要报告管理员	创建、编辑、删除和执行访问查看摘要报告	“报告”→“运行报告”和“查看报告”选项卡
帐户管理员	对用户执行所有操作，包括分配权能。不包括批量操作。	“帐户”→“列出帐户”、“查找用户”、“提取到文件”、“从文件加载”和“从资源加载”选项卡 “密码”→“更改用户密码”和“重设用户密码”选项卡 “服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡 “角色”→“列出角色”和“查找角色”选项卡
管理员报告管理员	创建、编辑、删除和运行管理员报告和管理员角色报告。	“报告”→“运行报告”和“查看报告”选项卡（仅限管理员报告和管理员角色报告）
管理员角色管理员	创建、编辑和删除管理员角色。	“安全性”→“管理员角色”选项卡
应用程序管理员	创建、编辑和删除应用程序角色。	“服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡（同步角色） “角色”→“列出角色”和“查找角色”选项卡
资产管理员	创建、编辑和删除资产角色。	“服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡（同步角色） “角色”→“列出角色”和“查找角色”选项卡
分配审计策略管理员	将审计策略分配给用户帐户和组织。 在“用户操作”列表中编辑用户审计策略以及在“组织操作”列表中编辑组织审计策略。	“帐户”→“列出帐户”和“查找用户”选项卡。
分配组织审计策略管理员	仅向组织分配审计策略。 在“组织操作”列表中编辑组织审计策略。	“帐户”→“列出帐户”选项卡
分配用户审计策略管理员	仅向用户分配审计策略。 在“用户操作”列表中编辑用户审计策略	“帐户”→“列出帐户”和“查找用户”选项卡

表 D–1 Identity Manager 基于任务的权能定义 （续）

权能	管理员/用户可执行的操作	可以访问以下选项卡和子选项卡
分配用户权能	更改用户权能分配（分配和取消分配）。 必须与另一个用户管理员权能一起分配（例如，“创建用户”或“启用用户”）。	“帐户”→“列出帐户”（仅限编辑）和“查找用户”选项卡。
审计策略管理员	创建、修改和删除审计策略。	“遵循性”→“管理策略”选项卡
审计策略扫描报告管理员	运行或调度审计策略扫描任务。	“服务器任务”→“查找任务”、“所有任务”、“运行任务”和“管理进度表”选项卡
审计报告管理员	创建、修改、删除和执行审计报告。 仅限访问审计日志报告、历史用户更改报告、单个用户审计日志报告以及使用情况报告。	“报告”→“运行报告”和“查看报告”选项卡。
审计日志报告管理员	创建、修改、删除和执行审计日志报告。	“报告”→“运行报告”选项卡
已审计的属性报告管理员	创建、修改、删除和执行已审计的属性报告。	“报告”→“运行报告”和“查看报告”选项卡
审计者访问扫描管理员	创建、编辑和删除周期性访问查看扫描	“遵循性”→“管理访问扫描”选项卡
审计者管理员	设置、管理和监视审计策略、审计扫描和用户遵循性。	“帐户”→“列出帐户”和“查找用户”选项卡 “服务器任务”→“查找任务”、“所有任务”、“运行任务”和“管理进度表”选项卡 “报告”→“运行报告”和“查看报告”选项卡 “遵循性”→“管理策略”、“管理访问扫描”和“访问查看”选项卡
审计者证明者	当启用了组织安全性时，需要证明其他用户的证明。	仅限“默认密码”和“工作项目”选项卡
审计者周期性访问查看管理员	管理周期性访问查看 (Periodic Access Review, PAR)、管理访问扫描、管理证明和管理 PAR 报告。	“服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡 “遵循性”→“管理访问扫描”和“访问查看”选项卡
审计者修正者	修正、缓解和转发审计策略违规。	仅限“默认密码”和“工作项目”选项卡

表 D–1 Identity Manager 基于任务的权能定义 （续）

权能	管理员/用户可执行的操作	可以访问以下选项卡和子选项卡
审计者报告管理员	创建、修改、删除和执行任何 Auditor 报告。	“服务器任务”→“查找任务”、“所有任务”、“运行任务”和“管理进度表”选项卡
		“报告”→对审计者报告的所有操作
审计者查看用户	查看与用户关联的遵循性信息。	“帐户”→“列出帐户”和“查找用户”选项卡
审计策略违规历史管理员	创建、修改、删除和执行审计策略违规历史报告。	“报告”→“运行报告”选项卡
批量帐户管理员	对用户执行常规和批量操作，包括分配权能。	“帐户”→“列出帐户”、“查找用户”、“启动批量操作”、“提取到文件”、“从文件加载”和“从资源加载”选项卡
		“密码”→“更改用户密码”和“重设用户密码”选项卡
		“服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡
		“角色”→“列出角色”和“查找角色”选项卡
批量更改帐户管理员	对现有用户执行除删除之外的常规和批量操作，包括分配权能。	“帐户”→“列出帐户”、“查找用户”和“启动批量操作”选项卡。
	无法创建或删除用户 。	“密码”→“更改用户密码”和“重设用户密码”选项卡
		“服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡
		“角色”→“列出角色”和“查找角色”选项卡
批量更改资源密码管理员	更改指定资源上的指定资源连接帐户的密码。	“服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡
		“资源”→“列出资源”和“启动批量操作”选项卡

表 D–1 Identity Manager 基于任务的权能定义 （续）

权能	管理员/用户可执行的操作	可以访问以下选项卡和子选项卡
批量更改用户帐户管理员	执行除删除现有用户之外的常规和批量操作。 无法创建、删除用户或向用户分配权能。	“帐户”→“列出帐户”、“查找用户”和“启动批量操作”选项卡。 “密码”→“更改用户密码”和“重设用户密码”选项卡 “服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡 “角色”→“列出角色”和“查找角色”选项卡
批量创建用户	分配资源和启动用户创建请求（通过使用批量操作对单个用户执行操作）。	“帐户”→“列出帐户”（仅限创建）、“查找用户”和“启动批量操作”选项卡 “服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡 “角色”→“列出角色”和“查找角色”选项卡
批量删除用户	删除 Identity Manager 用户帐户；取消置备、取消分配资源帐户和解除其链接（通过使用批量操作对单个用户执行操作）。	“帐户”→“列出帐户”、“查找用户”和“启动批量操作”选项卡 “服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡 “角色”→“列出角色”和“查找角色”选项卡
批量删除 IDM 用户	删除现有 Identity Manager 用户帐户（通过使用批量操作对单个用户执行操作）。	“帐户”→“列出帐户”（仅限删除）、“查找用户”和“启动批量操作”选项卡 “服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡 “角色”→“列出角色”和“查找角色”选项卡
批量取消置备用户	删除现有资源帐户和取消现有资源帐户的链接（通过使用批量操作对单个用户执行操作）。	“帐户”→“列出帐户”（仅限取消置备）、“查找用户”和“启动批量操作”选项卡 “服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡 “角色”→“列出角色”和“查找角色”选项卡

表 D–1 Identity Manager 基于任务的权能定义 （续）

权能	管理员/用户可执行的操作	可以访问以下选项卡和子选项卡
批量禁用用户	禁用现有用户和资源帐户（通过使用批量操作对单个用户执行操作）。	“帐户”→“列出帐户”（仅限禁用）、“查找用户”和“启动批量操作”选项卡 “服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡 “角色”→“列出角色”和“查找角色”选项卡
批量启用用户	启用现有用户和资源帐户（通过使用批量操作对单个用户执行操作）。	“帐户”→“列出帐户”（仅限启用）、“查找用户”和“启动批量操作”选项卡 “服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡 “角色”→“列出角色”和“查找角色”选项卡
批量重设资源密码管理员	重设指定资源上的指定资源连接帐户的密码。	“服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡 “资源”→“列出资源”和“启动批量操作”选项卡
批量取消分配用户	取消分配现有资源帐户和取消现有资源帐户的链接（通过使用批量操作对单个用户执行操作）。	“帐户”→“列出帐户”（仅限取消分配）、“查找用户”和“启动批量操作”选项卡 “服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡 “角色”→“列出角色”和“查找角色”选项卡
批量取消用户的链接	取消现有资源帐户的链接（通过使用批量操作对单个用户执行操作）。	“帐户”→“列出帐户”（仅限解除链接）、“查找用户”和“启动批量操作”选项卡 “服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡 “角色”→“列出角色”和“查找角色”选项卡

表 D–1 Identity Manager 基于任务的权能定义 （续）

权能	管理员/用户可执行的操作	可以访问以下选项卡和子选项卡
批量更新用户	编辑、移动和更新现有用户和资源帐户（通过使用批量操作对单个用户执行操作）。	“帐户”→“列出帐户”（仅限编辑、移动和更新操作）、“查找用户”和“启动批量操作”选项卡
		“服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡
		“角色”→“列出角色”和“查找角色”选项卡
批量用户帐户管理员	对用户执行所有常规和批量操作。	“帐户”→“列出帐户”、“查找用户”、“启动批量操作”、“提取到文件”、“从文件加载”和“从资源加载”选项卡
		“密码”→“更改用户密码”和“重设用户密码”选项卡
		“服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡
		“角色”→“列出角色”和“查找角色”选项卡
业务角色管理员	创建、编辑和删除业务角色。	“服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡（同步角色）
		“角色”→“列出角色”和“查找角色”选项卡
权能管理员	创建、修改和删除权能。	“安全性”→“权能”选项卡
更改帐户管理员	对现有用户执行除删除外的所有操作，包括分配权能。不包括批量操作	“帐户”→“列出帐户”和“查找用户”选项卡
	创建管理员报告和用户报告，运行和编辑管理员报告，运行组织范围内的审计日志报告。	“密码”→“更改用户密码”和“重设用户密码”选项卡
	无法运行组织范围以外的管理员报告或用户报告。无法删除用户。	“服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡
		“角色”→“列出角色”和“查找角色”选项卡
更改资源活动同步管理员	更改活动同步资源参数。	“服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡
		“资源”→“列出资源”选项卡

表 D–1 Identity Manager 基于任务的权能定义 （续）

权能	管理员/用户可执行的操作	可以访问以下选项卡和子选项卡
更改密码管理员	更改用户和资源帐户密码。 仅限访问“导出密码扫描”任务（从“运行任务”选项卡）	“帐户”→“列出帐户”和“查找用户”选项卡 “密码”→“更改用户密码” “服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡。 “角色”→“列出角色”和“查找角色”选项卡
更改密码管理员（需要进行验证）	成功验证用户的验证问题回答后更改用户和资源帐户密码。 仅限访问“导出密码扫描”任务（从“运行任务”选项卡）	“帐户”→“列出帐户”和“查找用户”选项卡 “密码”→“更改用户密码”选项卡（执行操作前需要进行验证） “服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡 “角色”→“列出角色”和“查找角色”选项卡
更改资源密码管理员	更改资源管理员帐户密码。仅限更改资源密码（在操作菜单的“管理连接”→“更改密码”中）	“服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡 “资源”→“列出资源”选项卡。
更改用户帐户管理员	对现有用户执行除删除和批量操作以外的所有操作。也无法创建、删除用户或向用户分配权能。	“帐户”→“列出帐户”和“查找用户”选项卡 “密码”→“更改用户密码”和“重设用户密码”选项卡 “服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡 “角色”→“列出角色”和“查找角色”选项卡
配置审计	配置系统中审计的事件和配置组。	“配置”→“审计”选项卡
配置证书	配置信任证书和 CRL。	“安全性”→“证书”选项卡
控制活动同步资源管理员	控制活动同步资源状态（如启动、停止和刷新）。	“资源”→“列出资源”选项卡 对于活动同步资源：活动同步操作菜单

表 D–1 Identity Manager 基于任务的权能定义 （续）

权能	管理员/用户可执行的操作	可以访问以下选项卡和子选项卡
创建用户	分配资源和启动用户创建请求。不包括批量操作	“帐户”→“列出帐户”（仅限创建）和“查找用户”选项卡 “服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡 “角色”→“列出角色”和“查找角色”选项卡
数据仓库管理员	配置数据导出器并运行数据仓库导出器启动程序任务。	“报告”→“面板图形”和“查看面板”选项卡 “资源”→“列出资源”选项卡 “配置”→“仓库”选项卡
数据仓库查询	配置和运行取证查询	“报告”→“面板图形”和“查看面板”选项卡 “资源”→“列出资源”选项卡 “遵循性”→“取证查询 (Forensic Query)”
删除用户	删除 Identity Manager 用户帐户；取消置备、取消分配资源帐户和解除其链接。不包括批量操作。	“帐户”→“列出帐户”（仅限删除）和“查找用户”选项卡 “服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡 “角色”→“列出角色”和“查找角色”选项卡
删除 IDM 用户	删除 Identity Manager 用户帐户。不包括批量操作。	“帐户”→“列出帐户”（仅限删除）和“查找用户”选项卡 “服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡 “角色”→“列出角色”和“查找角色”选项卡
取消置备用户	删除现有资源帐户和取消现有资源帐户的链接。不包括批量操作。	“帐户”→“列出帐户”（仅限取消置备）和“查找用户”选项卡 “服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡 “角色”→“列出角色”和“查找角色”选项卡

表 D–1 Identity Manager 基于任务的权能定义 （续）

权能	管理员/用户可执行的操作	可以访问以下选项卡和子选项卡
禁用用户	禁用现有用户和资源帐户。不包括批量操作	“帐户”→“列出帐户”（仅限禁用）和“查找用户”选项卡 “服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡 “角色”→“列出角色”和“查找角色”选项卡
启用用户	启用现有用户和资源帐户。不包括批量操作	“帐户”→“列出帐户”（仅限启用）和“查找用户”选项卡 “服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡 “角色”→“列出角色”和“查找角色”选项卡
最终用户管理员	查看和修改最终用户权能中指定的对象类型和最终用户受控组织规则的权限。	所有默认选项卡
外部资源管理员	仅限查看和配置外部资源。无法创建新资源。	“配置”→“外部资源”选项卡
配置 Identity Manager 模式	使用 Identity Manager 配置对象 `IDM` **模式配置**查看和配置用户或角色的有效模式。	所有默认选项卡
导入用户	从定义的资源导入用户。	“帐户”→“列出帐户”、“查找用户”、“提取到文件”、“从文件加载”和“从资源加载”选项卡 “角色”→“列出角色”和“查找角色”选项卡
导入/导出管理员	导入和导出所有类型的对象。	“配置”→“导入交换文件”选项卡
IT 角色管理员	创建、编辑和删除 IT 角色。	“服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡（同步角色） “角色”→“列出角色”和“查找角色”选项卡
登录管理员	编辑给定登录界面的登录模块集合。	“安全性”→“登录”选项卡
组织管理员	创建和编辑组织和目录连接。仅限删除组织。	“帐户”→“列出帐户”选项卡
组织批准者	批准新组织的请求。	仅限“默认密码”和“工作项目”选项卡

表 D–1 Identity Manager 基于任务的权能定义 （续）

权能	管理员/用户可执行的操作	可以访问以下选项卡和子选项卡
组织违规历史管理员	仅限创建、编辑、删除和执行组织违规历史报告。	“报告”→“运行报告”选项卡
密码管理员	列出、更改和重设用户和资源帐户密码。	“帐户”→“列出帐户”和“查找用户”选项卡 “密码”→“更改用户密码”和“重设用户密码”选项卡 “服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡 “角色”→“列出角色”和“查找角色”选项卡
密码管理员（需要进行验证）	仅限列出、更改和重设用户和资源帐户密码。操作成功前需要成功验证用户的验证问题回答。	“帐户”→“列出帐户”和“查找用户”选项卡 “密码”→“更改用户密码”和“重设用户密码”选项卡 “服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡 “角色”→“列出角色”和“查找角色”选项卡
执行调试	从 Identity Manager 调试页中访问和执行操作。 **注 –** 无法从菜单中访问 Identity Manager 调试页。要访问这些调试页，请在浏览器中键入以下 URL： `http://<AppServerHost>:<Port>/idm/debug`	所有默认选项卡
策略管理员	创建、编辑和删除“策略”。	“安全性”→“策略”选项卡
策略摘要报告管理员	创建、编辑、删除和执行策略摘要报告。	“报告”→“运行报告”和“查看报告”选项卡
注册 Identity Manager 产品组件	在 Sun Microsystems 中注册 Identity Manager 安装或创建本地服务标记。	“配置”→“产品注册”选项卡
协调管理员	编辑协调策略和控制协调任务。	“服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡（查看协调任务）。 “资源”→“列出资源”和“检查帐户索引”选项卡

表 D–1 Identity Manager 基于任务的权能定义 （续）

权能	管理员/用户可执行的操作	可以访问以下选项卡和子选项卡
协调报告管理员	创建、编辑、删除和运行协调报告。	“报告”→“运行报告”（仅限帐户索引报告）和“查看报告”选项卡
协调请求管理员	管理协调请求。	“服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡
		“资源”→“列出资源”（仅列出和协调功能）和“查看报告”选项卡
Remedy 集成管理员	编辑 Remedy 集成配置（查看任务、运行角色同步）。	“服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡
		“配置”→“Remedy 集成”选项卡
重命名用户	重命名现有用户和资源帐户（列出范围内的所有帐户、重命名用户）。	“帐户”→“列出帐户”和“查找用户”选项卡
		“服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡
		“角色”→“列出角色”和“查找角色”选项卡
报告管理员	配置审计设置和运行所有报告类型（查看任务、运行角色同步）。	“服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡
		“报告”→“运行报告”、“查看报告”、“运行风险分析”和“查看风险分析”选项卡
		“角色”→“列出角色”和“查找角色”选项卡
		“配置”→“审计”选项卡
重设密码管理员	重设用户和资源帐户密码。	“帐户”→“列出帐户”和“查找用户”选项卡（仅限重设密码）
		“密码”→“重设用户密码”
		“服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡（具有此权能的用户无法执行任何任务）
		“角色”→“列出角色”和“查找角色”选项卡

表 D–1 Identity Manager 基于任务的权能定义 （续）

权能	管理员/用户可执行的操作	可以访问以下选项卡和子选项卡
重设密码管理员（需要进行验证）	重设用户和资源帐户密码。操作成功前需要成功验证用户的验证问题回答。	“帐户”→“列出帐户”和“查找用户”选项卡
		“密码”→“重设用户密码”
		“服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡（具有此权能的用户无法执行任何任务）
		“角色”→“列出角色”和“查找角色”选项卡
重设资源密码管理员	重设资源管理员帐户密码（在操作菜单的“管理连接”→“重设密码”中）。	“服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡
		“资源”→“列出资源”选项卡
资源管理员	创建、编辑和删除资源。至于范围之外的资源，资源用户报告和资源组报告将返回错误。编辑全局策略、参数和资源组。无法管理连接或资源对象	“服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡
		“资源”→“列出资源”、“列出资源组”和“检查帐户索引”选项卡
		“配置”→“连接器服务器”
资源批准者	批准资源分配	所有默认密码和工作项目选项卡
资源组管理员	创建、编辑和删除资源组。	“资源”→“列出资源组”选项卡
资源对象管理员	查看、创建、修改和删除资源对象。	“服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡
		“资源”→“列出资源”选项卡
资源密码管理员	更改和重设资源代理帐户密码。	“服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡
		“资源”→“列出资源”选项卡（仅限在操作菜单的“管理连接”→“更改密码”中更改资源密码）
资源报告管理员	创建、编辑、删除和运行资源报告。	“报告”→“运行报告”和“查看报告”选项卡
资源违规历史管理员	创建、编辑、删除和执行资源违规历史报告。	“报告”→“运行报告”
风险分析管理员	创建、编辑、删除和运行风险分析。	“报告”→“风险分析”和“查看风险分析”选项卡

表 D–1 Identity Manager 基于任务的权能定义 （续）

权能	管理员/用户可执行的操作	可以访问以下选项卡和子选项卡
角色管理员	创建、编辑、同步和删除角色。	“服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡 “角色”→“列出角色”和“查找角色”选项卡
角色批准者	批准角色分配	所有默认密码和工作项目选项卡
角色报告管理员	创建、编辑、删除和运行资源报告。	“报告”→“运行报告”和“查看报告”选项卡 “角色”→“列出角色”选项卡
运行访问查看详细信息报告	运行访问查看详细信息报告	“报告”→“运行报告”和“查看报告”选项卡
运行访问查看摘要报告	运行访问查看摘要报告	“报告”→“运行报告”和“查看报告”选项卡
运行管理员报告	运行管理员报告。	“报告”→“运行报告”和“查看报告”选项卡
运行审计策略扫描报告	运行审计策略扫描报告。	“服务器任务”→仅限“所有任务”、“查找任务”和“运行任务”
运行审计报告	仅限运行审计报告、审计日志报告、历史用户更改报告、单个用户审计日志报告以及使用情况报告。	“报告”→“运行报告”和“查看报告”选项卡
运行审计属性报告	执行和查看审计属性报告。	“报告”→“运行报告”和“查看报告”选项卡
运行审计者报告	运行所有审计日志报告类型的报告。	“服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡 “报告”→“运行报告”和“查看报告”选项卡
运行审计日志报告	执行和查看审计日志报告、当日活动报告和每周活动报告。	“报告”→“运行报告”
运行审计策略违规历史	执行和查看组织违规历史报告、当日活动报告和每周活动报告。	“报告”→“运行报告”
运行策略摘要报告	执行和查看策略摘要报告。	“报告”→“运行报告”和“查看报告”选项卡
运行组织违规历史	执行组织违规历史报告。	“报告”→“运行报告”选项卡
运行协调报告	执行和查看帐户索引报告。	“报告”→“运行报告”和“查看报告”选项卡

表 D–1 Identity Manager 基于任务的权能定义 （续）

权能	管理员/用户可执行的操作	可以访问以下选项卡和子选项卡
运行资源报告	执行和查看资源用户报告和资源组报告。	“报告”→“运行报告”和“查看报告”选项卡
运行资源违规历史	执行资源违规历史报告。	“报告”→“运行报告”选项卡
运行风险分析	执行和查看风险分析。	“报告”→“运行风险分析”和“查看风险分析”选项卡
运行角色报告	执行和查看角色报告。	“报告”→“运行报告”和“查看报告”选项卡 “角色”→“列出角色”选项卡
运行任务划分报告	执行和查看任务划分报告。	“报告”→“运行报告”和“查看报告”选项卡
运行任务报告	执行和查看任务报告。	“报告”→“运行报告”和“查看报告”选项卡
运行用户访问报告	执行和查看详细用户报告和用户访问报告。	“报告”→“运行报告”和“查看报告”选项卡
运行用户报告	执行和查看用户报告。	“报告”→“运行报告”和“查看报告”选项卡
运行违规摘要报告	执行违规摘要报告。	“报告”→“运行报告”选项卡
安全管理员	创建具有权能的用户；启用和禁用用户、列出和控制资源对象、管理加密密钥、管理登录和审计配置以及管理策略。	“帐户”→“列出帐户”（某些操作）和“查找用户”选项卡（审计报告） “密码”→“更改用户密码”和“重设用户密码”选项卡 “服务器任务”→“查找任务”、“所有任务”、“运行任务”和“配置任务”选项卡 “报告”→“运行报告”、“查看报告”、“面板图形”、“查看面板”和“配置报告” “资源”→“列出资源” “配置”→“审计”和“仓库”选项卡 “安全性”→“证书”、“登录”和“策略”选项卡 “服务提供者”→“编辑用户搜索配置”
任务划分报告管理员	创建、编辑、执行、查看和删除任务划分报告。	“报告”→“运行报告”和“查看报告”选项卡

表 D–1 Identity Manager 基于任务的权能定义 （续）

权能	管理员/用户可执行的操作	可以访问以下选项卡和子选项卡
服务提供商管理员角色管理员	管理服务提供商管理员角色以及相关的规则。	“安全性”→“管理员角色”选项卡
服务提供商管理员	创建、编辑和管理服务提供商用户和事务；配置事务数据库和跟踪的事件。	“帐户”→“管理服务提供者用户”选项卡
		“服务器任务”→“服务提供者事务”选项卡
		“报告”→“面板图形”选项卡
		“报告”→“查看面板”选项卡
		“服务提供者”→“编辑主配置”、“编辑事务配置”和“编辑用户搜索配置”选项卡
服务提供商创建用户	为服务提供商（外联网）用户创建用户帐户。	“帐户”→“管理服务提供者用户”选项卡
服务提供商删除用户	删除服务提供商用户帐户。	“帐户”→“管理服务提供者用户”选项卡
服务提供商更新用户	更新服务提供商用户帐户。	“帐户”→“管理服务提供者用户”选项卡
服务提供商用户管理员	管理服务提供商（外联网）用户。	“帐户”→“管理服务提供者用户”
服务提供商查看用户	查看服务提供商（外联网）用户帐户信息。	“帐户”→“管理服务提供者用户”选项卡
任务报告管理员	创建、编辑、删除、执行和查看任务报告。	“报告”→“运行报告”和“查看报告”选项卡
取消分配用户	取消分配现有资源帐户和取消现有资源帐户的链接。不包括批量操作。	“帐户”→“列出帐户”（仅限取消分配）和“查找用户”选项卡
		“服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡
		“角色”→“列出角色”和“查找角色”选项卡

表 D–1 Identity Manager 基于任务的权能定义 （续）

权能	管理员/用户可执行的操作	可以访问以下选项卡和子选项卡
取消用户的链接	取消现有资源帐户的链接。不包括批量操作。	“帐户”→“列出帐户”（仅限解除链接）和“查找用户”选项卡
		“服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡
		“角色”→“列出角色”和“查找角色”选项卡
解除锁定用户	对于支持解除锁定的现有用户资源帐户，解除其锁定。不包括批量操作。	“帐户”→“列出帐户”（仅限解除锁定）和“查找用户”选项卡
		“服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡
		“角色”→“列出角色”和“查找角色”选项卡
更新用户	编辑现有用户和启动用户更新请求。管理现有的服务器任务。	“帐户”→“列出帐户”和“查找用户”选项卡
		“服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡
		“角色”→“列出角色”和“查找角色”选项卡
用户访问报告管理员	创建、编辑、删除、执行和查看用户访问报告。	“报告”→“运行报告”和“查看报告”选项卡
用户帐户管理员	除了无法分配用户权能之外，可对用户执行所有操作。	“帐户”→“列出帐户”、“查找用户”、“提取到文件”、“从文件加载”和“从资源加载”选项卡。
		“密码”→“更改用户密码”和“重设用户密码”选项卡
		“服务器任务”→“查找任务”、“所有任务”和“运行任务”选项卡
		“角色”→“列出角色”和“查找角色”选项卡
用户报告管理员	创建、编辑、删除、执行和查看用户报告。	“报告”→“运行报告”和“查看报告”选项卡
查看应用程序	列出应用程序类型角色和查看应用程序类型角色信息。不允许执行任何更改操作。	“角色”→“列出角色”和“查找角色”选项卡
查看资产	列出资产类型角色和查看资产类型角色信息。不允许执行任何更改操作。	“角色”→“列出角色”和“查找角色”选项卡

表 D–1 Identity Manager 基于任务的权能定义 （续）

权能	管理员/用户可执行的操作	可以访问以下选项卡和子选项卡
查看业务角色	列出业务角色和查看业务角色信息。不允许执行任何更改操作。	“角色”→“列出角色”和“查找角色”选项卡
查看 IT 角色	列出 IT 角色和查看 IT 角色信息。不允许执行任何更改操作。	“角色”→“列出角色”和“查找角色”选项卡
查看角色	列出所有角色类型和查看所有角色信息。不允许执行任何更改操作。	“角色”→“列出角色”和“查找角色”选项卡
查看用户	查看单个用户详细信息。不允许执行任何更改操作。	“帐户”→“列出帐户”和“查找用户”选项卡
违规摘要报告管理员	创建、编辑、删除和执行违规摘要报告。	“报告”→“运行报告”选项卡
Identity System 管理员	执行系统范围内的任务，如编辑系统配置对象、同步角色、编辑源适配器模板以及运行报告。	“服务器任务”→“查找任务”、“所有任务”、“运行任务”、“管理进度表”和“配置任务”选项卡 “报告”→“运行报告”、“查看报告”、“面板图形”、“查看面板”和“配置报告”选项卡 “资源”→“列出资源” “配置”→“审计”、“仓库”、“电子邮件模板”、“表单和进程映射”、“服务器”、“用户界面”和“产品注册”选项卡 “遵循性”→“访问查看” “安全性”→“证书”

功能性权能定义

功能性权能包含基于任务的权能以及其他功能性权能。

- **帐户管理员**
  - 批准者管理员
    - 组织批准者
    - 资源批准者
    - 角色批准者
  - 分配用户权能
  - SPML 访问
  - 用户帐户管理员

- 创建用户
- 删除用户
  - 删除 IDM 用户
  - 取消置备用户
  - 取消分配用户
  - 取消用户的链接
- 禁用用户
- 启用用户
- 密码管理员
  - 更改密码管理员
  - 重设密码管理员
- 重命名用户
- 解除锁定用户
- 更新用户
- 查看用户
- 导入用户

- **管理员角色管理员**
- **审计者管理员**
  - 分配审计策略
    - 分配组织审计策略
    - 分配用户审计策略
  - 审计策略管理员

    审计者查看用户
  - 审计者周期性访问查看管理员

    审计者访问扫描管理员
  - 审计者报告管理员
  - 密码管理员
  - 用户帐户管理员
  - 分配用户权能
- **审计者报告管理员**
  - 访问查看详细信息报告管理员

    运行访问查看详细信息报告
  - 访问查看摘要报告管理员

    运行访问查看摘要报告
  - 审计策略扫描报告管理员

运行审计策略扫描报告

- 已审计的属性报告管理员
  运行审计属性报告
- 审计策略违规历史管理员
  运行审计策略违规历史报告
- 组织违规历史管理员
  运行组织违规历史报告
- 策略摘要报告管理员
- 资源违规历史管理员
  运行资源违规历史报告
- 运行审计者报告
- 任务划分报告管理员
  运行任务划分报告
- 用户访问报告管理员
  运行用户访问报告
- 违规摘要报告管理员

- **审计者查看用户**
  查看用户
- **批量帐户管理员**
  - 批准者管理员
  - 分配用户权能
  - 批量用户帐户管理员
    - 批量创建用户
    - 批量删除用户
      - 批量删除 IDM 用户
      - 批量取消置备用户
      - 批量取消分配用户
      - 批量取消用户的链接
    - 批量禁用用户
    - 批量启用用户
    - 密码管理员
    - 重命名用户
    - 解除锁定用户
    - 查看用户

        - 导入用户
- **批量更改帐户管理员**
    - 批准者管理员
    - 分配用户权能
    - 批量更改用户帐户管理员
        - 批量禁用用户
        - 批量启用用户
        - 批量更新用户
        - 密码管理员
        - 重命名用户
        - 解除锁定用户
        - 查看用户
- **批量资源管理员**
    - 更改活动同步资源管理员
    - 控制活动同步资源管理员
    - 资源组管理员
- **批量资源密码管理员**
    - 批量更改资源密码管理员
    - 批量重设资源密码管理员
- **权能管理员**
- **更改帐户管理员**
    - 批准者管理员
    - 分配用户权能
    - 更改用户帐户管理员
        - 密码管理员
            - 更改密码管理员
            - 重设密码管理员
        - 禁用用户
        - 启用用户
        - 重命名用户
        - 解除锁定用户
        - 更新用户
        - 查看用户
- **配置证书**
- **数据仓库管理员**
- **数据仓库查询**

- **调试**
- **最终用户管理员**
- **IDM 模式配置**
- **导入/导出管理员**
- **许可证管理员**
- **登录管理员**
- **元视图管理员**
- **组织管理员**
- **密码管理员（需要进行验证）**
  - 更改密码管理员（需要进行验证）
  - 重设密码管理员（需要进行验证）
- **策略管理员**
- **产品管理员**
- **协调管理员**

  协调请求管理员
- **Remedy 集成管理员**
- **报告管理员**
  - 管理员报告管理员

    运行管理员报告
  - 审计报告管理员

    运行审计报告
  - 审计者报告管理员
    - 访问查看详细信息报告管理员

      运行访问查看详细信息报告
    - 访问查看摘要报告管理员

      运行访问查看摘要报告
    - 审计策略扫描报告管理员

      运行审计策略扫描报告
    - 已审计的属性报告管理员

      运行审计属性报告
    - 审计日志报告管理员

      运行审计日志报告
    - 审计策略违规历史管理员

      运行审计策略违规历史

- 组织违规历史管理员
  运行组织违规历史
- 策略摘要报告管理员
  运行策略摘要报告
- 协调报告管理员
  运行协调报告
- 资源违规历史管理员
  运行资源违规历史
- 运行审计者报告
  - 运行访问查看详细信息报告
  - 运行访问查看摘要报告
  - 运行审计策略扫描报告
  - 运行审计属性报告
  - 运行审计日志报告
  - 运行审计策略违规历史
  - 运行组织违规历史
  - 运行策略摘要报告
  - 运行资源违规历史
  - 运行任务划分报告
  - 运行用户访问报告
  - 运行违规摘要报告
- 任务划分报告管理员
  运行任务划分报告
- 用户访问报告管理员
  运行用户访问报告
- 违规摘要报告管理员
  运行违规摘要报告

- 协调报告管理员
  运行协调报告
- 资源报告管理员
  运行资源报告
- 风险分析管理员
  运行风险分析
- 角色报告管理员
  运行角色报告
- 任务报告管理员

运行任务报告

- 用户报告管理员

运行用户报告

- 配置审计

- **资源管理员**
  - 更改活动同步资源管理员
  - 控制活动同步资源管理员
  - 资源组管理员
- **资源对象管理员**
- **资源密码管理员**
  - 更改资源密码管理员
  - 重设资源密码管理员
- **角色管理员**
  - 应用程序管理员
  - 资产管理员
  - 业务角色管理员
  - IT 角色管理员
- **安全管理员**
- **服务提供者管理员**
  - 服务提供商用户管理员
  - 服务提供商创建用户
  - 服务提供商删除用户
  - 服务提供商更新用户
  - 服务提供商查看用户
- **服务提供者管理员角色管理员**
- **Waveset 管理员**

词汇表

access review（访问查看） 使管理员或其他责任方能够查看并验证用户访问权限的审计过程。可以自动批准或拒绝用户权利记录，也可以手动证明这些记录。另请参见 *attestation*（**证明**）。

account attribute（帐户属性） 帐户属性为 Identity Manager 管理员提供了一种方法，可以创建映射到受管资源上的属性的一组标准名称。例如，名为 *fullname* 的 Identity Manager 属性可能映射到 Active Directory 资源上的 *displayName* 属性以及 LDAP 资源上的 *cn* 属性。对 Identity Manager 中用户的 *fullname* 属性所做的任何更改随后都将传递给用户远程资源帐户上用户的 *displayName* 和 *cn* 属性。

admin role（管理员角色） 唯一的一组权能，用于分配给管理用户的每一组组织。

administrator interface（管理员界面） 管理员用来配置和管理 Identity Manager 的用户界面。

administrator（管理员） 配置 Identity Manager 或负责操作任务（如创建用户和管理对资源的访问）的人。

Application (Role)（应用程序（角色）） “应用程序”角色类型是 Identity Manager 中的四种角色类型之一，是用户工作时需要使用的资源和/或资源组和/或资源上的特定应用程序的集合。无法将应用程序角色直接分配给用户，但可以将其分配给 IT 角色和业务角色。

approval（批准） 授予或拒绝用户访问角色、资源或组织的请求的过程。具有对批准工作项目查看和响应权限的 Identity Manager 管理员称为**批准者**。

approver（批准者） 具备管理权能的用户，负责批准或拒绝访问请求。

Asset (Role)（资产（角色）） “资产”角色类型是 Identity Manager 中的四种角色类型之一，（通常）是为需要手动置备的非连接资源和/或非数字资源（例如，移动电话和便携式计算机）保留的。无法将资产角色直接分配给用户，但可以将其分配给 IT 角色和业务角色。

attestation task（证明任务） 需要证明的用户权利查看的逻辑集合。如果用户权利被分配给同一个证明者且由同一个访问查看实例产生，则会将这些用户权利分组为单个证明任务。

attestation（证明） 验证特定用户在特定时间点是否具有相应资源的适当权限的过程。对证明工作项目具有查看和响应权限的 Identity Manager 用户称为**证明者**。Identity Manager 规则决定了需要手动证明用户权利记录还是自动批准或拒绝该记录。

attestor（证明者） 负责验证（**证明**）用户权利是否适当的用户。证明者在 Identity Manager 中具有扩展权限，这些扩展权限是管理需要证明的用户权利所必需的。

attest（证明） 访问查看期间由证明者执行的操作，用于确认用户权利是否适当。

Business Process Editor, BPE（业务进程编辑器） Identity Manager 表单、规则和工作流的图形视图（随 Identity Manager 7.0 以前的版本一起提供）。在当前版本的 Identity Manager 中，BPE 已由 Identity Manager IDE 代替。请参见词汇表。

Business Role（业务角色） “业务角色”是 Identity Manager 中的四种角色类型之一，用于将组织中执行类似任务的人员所需的访问权限划分到各个组中。“业务角色”角色类型由一个或多个资产角色、应用程序角色和/或 IT 角色组成。业务角色用于直接分配给用户。

capability（权能） 控制在 Identity Manager 中执行的操作的用户帐户的访问权限组；Identity Manager 中的低级别访问控制。

delegation（委托） 在指定时间段内将未来的工作项目临时分配给一个或多个其他用户的过程。

directory junction（目录连接） 分层相关的一组组织，这些组织镜像目录资源的实际层级容器集合。目录连接中的每个组织都是**虚拟组织**。

entitlement（权利） 请参见 *user entitlement*（**用户权利**）。

escalation timeout（升级超时） 为工作项目请求指定的时间范围，在这个时间范围内分配的工作项目拥有者在 Identity Manager 进程将此工作项目发送给下一个分配的响应者之前必须做出响应。

form（表单） 与 Web 页相关的对象，包含浏览器如何在该页上显示用户视图属性的规则。表单可合并业务逻辑，并经常用于在视图数据显示给用户之前对其进行操作。

Identity Manager IDE Identity Manager 集成开发环境 (Identity Manager IDE) 是一个应用程序，允许您在部署中查看、自定义和调试 Identity Manager 对象。Identity Manager IDE 将作为 NetBeans 插件提供。

identity template（身份模板） 定义用户的资源帐户名称。

IT Role（IT 角色） “IT 角色”角色类型是 Identity Manager 中的四种角色类型之一，它是角色（资产、应用程序和/或其他嵌套 IT 角色）以及资源和/或资源组的集合。在某些配置中，可以将 IT 角色直接分配给用户，但通常是将 IT 角色分配给业务角色，然后再将业务角色分配给用户。

organization（组织） 用于启用管理委托的 Identity Manager 容器。

组织定义由管理员控制或管理的实体（如用户帐户、资源和管理员帐户）的范围。组织提供“其中”上下文，主要用于实现 Identity Manager 的管理目的。

periodic access review（周期性访问查看） 按照周期性间隔（例如每季度）执行的访问查看。

policy（策略） 建立 Identity Manager 帐户的限定条件。

Identity Manager 策略建立用户、密码和验证选项，并绑定到组织或用户。资源密码和帐户 ID 策略设置规则、允许的字词和属性值，并绑定到各个资源。

reconciliation（协调） 这是一项 Identity Manager 功能，用于定期比较 Identity Manager 中的资源帐户和位于资源本身的帐户。协调将关联帐户数据并突出显示存在的差异。

remediation（修正） 更正 Identity Manager 审计功能发现的遵循性违规的过程。Identity Manager 审计企业中的数据，以确保符合内部和外部策略及规定。有权查看和响应策略违规的管理员称为**修正者**。

remediator（修正者） 指定作为为审计策略分配的修正者的 Identity Manager 用户。

Identity Manager 检测到需要修正的遵循性违规时，会创建修正工作项目并将该工作项目发送到修正者的工作项目列表中。

resource adapter account（资源适配器帐户） 由 Identity Manager 资源适配器使用的证书，用以访问受管理的资源。

resource adapter（资源适配器） Identity Manager 组件，提供 Identity Manager 引擎和资源间的链接。

Identity Manager 可使用此组件管理给定资源上的用户帐户（包括创建、更新、删除、验证和扫描功能），并利用该资源进行传递验证。

resource group（资源组） 用于指示创建、删除和更新用户资源帐户的资源的集合。

resource wizard（资源向导） 指导完成资源创建和修改过程（包括资源参数、帐户属性、身份模板和 Identity Manager 参数的设置和配置）的 Identity Manager 工具。

resource（资源） 在 Identity Manager 中，资源可存储有关如何连接到创建帐户的远程资源或系统的信息。Identity Manager 可访问的远程资源包括主机安全管理器、数据库、目录服务、应用程序、操作系统、ERP 系统及消息平台等。

role（角色） 角色是一个 Identity Manager 对象，通过该对象，可以将资源访问权限分组并有效地分配给用户。角色可分为以下四种角色类型：业务角色、IT 角色、应用程序角色和资产。IT 角色、应用程序和资产将资源权利划分到各个组中。随后可将这三个组分配给业务角色，以使用户在工作时能够访问所需的资源。

rule（规则） Identity Manager 信息库中的对象，包含以 XPRESS、XML Object 或 JavaScript 语言编写的函数。规则提供一种存储常用的逻辑或静态变量的机制，以便在表单、工作流和角色中重新使用这些变量。

schema map（模式映射） 将资源帐户属性映射到资源的 Identity Manager 帐户属性。

Identity Manager 帐户属性可创建转至多个资源的常用链接，且由表单进行引用。

schema（模式） 资源的用户帐户属性列表。

service provider users（服务提供者用户） 服务提供者的外联网用户或客户，不同于服务提供者公司的员工或内联网用户。

user account（用户帐户） 使用 Identity Manager 创建的帐户。

可以指 Identity Manager 帐户或 Identity Manager 所管理的远程资源上的帐户。用户帐户设置过程是动态的过程。要填写的信息或字段取决于通过角色分配直接或间接提供给用户的资源。

user entitlement（用户权利） 在 Identity Manager 中，是指为实施访问限制的资源或系统上的用户授予的可审计访问权限。

user interface（用户界面） 在 Identity Manager 中，不具备管理权能的用户可通过用户界面执行一定范围的自助服务任务，如更改密码、设置验证问题的答案和管理委托分配。也称为**最终用户界面**。

user（用户） 拥有 Identity Manager 系统帐户的人。用户可以在 Identity Manager 中拥有一系列 capability（权能）。拥有扩展权能的人是 Identity Manager *administrator*（**管理员**）。

virtual organization（虚拟组织） 在目录连接中定义的组织。**请参见**目录连接。

work items（工作项目） Identity Manager 工作流、表单或过程生成的操作请求。批准、更改批准、证明和修正是工作项目的四种类型。

workflow（工作流） 符合逻辑的可重复过程，在此过程中，文档、信息或任务从一个参与者传递至另一个参与者。Identity Manager 工作流包括多个过程，它们可对用户帐户的创建、更新、启用、禁用和删除进行控制。

索引

结

解

禁

进

控

类

联

列

密

日

删

身

审

生