Sun Java™ System

Identity Manager 7.1
管理

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

文件号码：820-2291

版权所有 © 2007 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. 保留所有权利。

对于本文档中介绍的产品，Sun Microsystems, Inc. 对其所涉及的技术拥有相关的知识产权。需特别指出的是（但不局限于此），这些知识产权可能包含在 http://www.sun.com/patents 中列出的一项或多项美国专利，以及在美国和其他国家/地区申请的一项或多项其他专利或待批专利。

本产品包含 SUN MICROSYSTEMS, INC. 的机密信息和商业秘密。未经 SUN MICROSYSTEMS, INC. 的事先明确书面许可，不得使用、泄露或复制。

美国政府权利 - 商业用途。政府用户应遵循 Sun Microsystems, Inc. 的标准许可协议，以及 FAR （Federal Acquisition Regulations，即 “联邦政府采购法规”）的适用条款及其补充条款。

必须依据许可证条款使用。

本发行版可能包含由第三方开发的内容。

Sun、 Sun Microsystems、 Sun 徽标、 Java、 Solaris 和 Java 咖啡杯徽标是 Sun Microsystems, Inc. 在美国和其他国家/地区的商标或注册商标。

UNIX 是 X/Open Company, Ltd. 在美国和其他国家/地区独家许可的注册商标。

所介绍的本产品受美国出口控制法制约，并应遵守其他国家/地区的进出口法律。
严禁将本产品直接或间接地用于核设施、导弹、生化武器或海上核设施，也不能直接或间接地出口给核设施、导弹、生化武器或海上核设施的最终用户。严禁出口或转口到美国禁运的国家/地区以及美国禁止出口清单中所包含的实体，包括但不限于被禁止的个人以及特别指定的国家/地区的公民。

本文档按 “原样” 提供，对于所有明示或默示的条件、陈述和担保，包括对适销性、适用性或非侵权性的默示保证，均不承担任何责任，除非此免责声明的适用范围在法律上无效。

目录

图

表

前言

本指南介绍如何使用 Sun Java™ System Identity Manager 软件让用户安全地访问您的企业信息系统和应用程序。它说明了操作过程和方案以帮助您利用 Identity Manager 系统执行经常性和周期性管理任务。

目标读者

本 *Identity Manager 管理*指南适用于使用 Sun Java System 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 服务提供者使用。

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。

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

本书中使用的约定

本节中的表格介绍本书中使用的约定。

印刷约定

下表介绍本书中使用的印刷约定。

表 1 印刷约定

字样	含义	示例
AaBbCc123	API 和语言元素、HTML 标记、Web 站点 URL、命令名、文件名、目录路径名、计算机屏幕输出和样例代码。	编辑 `.login` 文件。 使用 `ls -a` 列出所有文件。 `% You have mail。`
AaBbCc123	用户键入的内容，与计算机屏幕输出的显示不同。	`% su` `Password:`
AaBbCc123	保留未译的新词或术语以及要强调的词。要使用实名或值替换的命令行变量。	这些被称为 *class* 选项。 该文件位于 *install-dir*`/bin` 目录中。
新词术语强调	新词或术语以及要强调的词。	请**勿**保存文件。
《书名》	书名	阅读 《用户指南》的第 6 章。

符号

下表介绍本书中使用的符号约定。

表 2 符号约定

符号	描述	示例	含义
`[ ]`	包含可选的命令选项。	`ls [-l]`	`-l` 选项不是必需的。
`{ | }`	包含为所需命令选项提供的一组选择。	`-d {y|n}`	`-d` 选项要求您使用 `y` 参数或 `n` 参数。
-	结合同时发生的多个击键。	Ctrl-A	按 A 键的同时按 Ctrl 键。
+	结合相继发生的多个击键。	Ctrl+A+N	按下 Ctrl 键后放开，然后再按后几个键。
>	表示图形用户界面中的菜单项选择。	File > New > Templates	从 "File" 菜单中，选择 "New"。从 "New" 子菜单中，选择 "Templates"。

相关文档

http://docs.sun.com℠ Web 站点使您可联机访问 Sun 技术文档。您可以浏览归档文档库或查找某个特定的书名或主题。

本文档集中的文档

Sun 提供了其他文档和信息以帮助您安装、使用和配置 Identity Manager。

- *Identity Manager 安装* - 帮助您安装和配置 Identity Manager 及相关软件的逐步操作说明和参考信息。
- *Identity Manager 升级* - 帮助您升级和配置 Identity Manager 及相关软件的逐步操作说明和参考信息。
- *Identity Manager 管理* - 提供了相关的步骤、教程和示例，以介绍如何使用 Identity Manager 让用户安全地访问您的企业信息系统并管理用户遵循性。
- *Identity Manager 技术部署概述* - 对 Identity Manager 产品 （包括对象体系结构）的概念性概述并介绍基本产品组件。
- *Identity Manager 工作流、表单和视图* - 介绍如何使用 Identity Manager 工作流、表单和视图的参考信息和过程性信息 （包括自定义这些对象所需的工具的信息）。
- *Identity Manager 部署工具* - 介绍如何使用不同的 Identity Manager 部署工具的参考信息和过程性信息，包括规则和规则库、普通任务和进程、字典支持以及由 Identity Manager 服务器提供的基于 SOAP 的 Web 服务界面。

- *Identity Manager 资源参考资料* - 介绍如何将资源的帐户信息加载并同步到 Identity Manager 的参考信息和过程性信息。
- *Identity Manager 调优、故障排除和错误消息* - 介绍 Identity Manager 错误消息和异常情况的参考信息和过程性信息，并为跟踪和解决工作中可能遇到的问题提供指导。
- *Identity Manager Service Provider Edition Deployment* - 介绍如何计划和执行 Sun Java™ System Identity Manager Service Provider Edition 的参考信息和过程性信息。
- Identity Manager 帮助 - 联机向导和信息，提供有关 Identity Manager 的完整过程性信息、参考信息和术语信息。您可在 Identity Manager 菜单栏单击 "Help" 链接以访问帮助。对关键字段提供了指导 （字段特定信息）。

联机访问 Sun 资源

有关产品下载、专业服务、修补程序及支持和其他开发者信息，请转至以下位置：

- 下载中心
  http://wwws.sun.com/software/download/
- 专业服务
  http://www.sun.com/service/sunps/sunone/index.html
- Sun 企业服务、 Solaris 修补程序和支持
  http://sunsolve.sun.com/
- 开发者信息
  http://developers.sun.com/prodtech/index.html

联系 Sun 技术支持

如果您遇到通过本文档无法解决的技术问题，请访问以下网址
http://www.sun.com/service/contacting

相关的第三方 Web 站点引用

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。

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。

为了共享您的意见，请访问 http://docs.sun.com，并单击 "Send Comments" （发送意见）。在联机表单中，请提供文档标题和文件号码。文件号码是一个七位或九位的数字，可以在书的标题页或文档的顶部找到。

例如，本书的标题为 《Sun Java System Identity Manager 7.1 Identity Manager 管理》，文件号码 820-2291。

提出意见时您还需要在表格中输入文件的英文文件号码和标题。本文件的英文文件号码是 820-0816，文件标题为 《Sun Java System Identity Manager 7.1 Administration》。

第 1 章

Identity Manager 概述

Sun Java™ System Identity Manager 系统使您可以安全高效地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。

本章通过以下主题进行了概述：

简介

当今的企业要求 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。

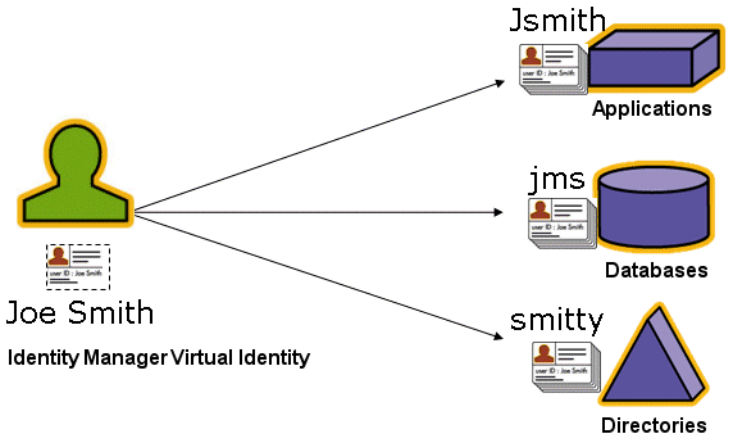
定义用户访问

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。

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 *Identity Manager SPE 部署*。

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 13 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 *Identity Manager 工作流、表单和视图*。

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。其中包括：

- 用户帐户
- 角色
- 资源和资源组
- 组织和虚拟组织
- 目录连接
- 权能
- 管理员角色
- 策略
- 审计策略

用户帐户

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。
- 分配角色，从而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。

您可以授予用户管理权限来管理用户帐户、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。

角色

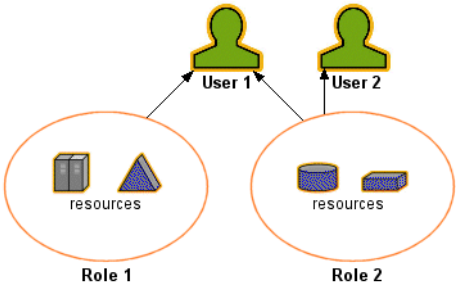
角色是 Identity Manager 对象，代表 Identity Manager 用户类型且允许将资源分组并分配给用户。通常，角色表示用户的工作职责。例如，在一个金融机构中，角色可能对应于各个工作职责，如银行出纳员、信贷员、分行经理、办事员、会计或管理助理。

角色定义用户的一组基本资源和资源属性。也可定义与其他角色之间的关系；例如，包含或排除其他角色的角色。

具有相同角色的用户共享对公共基本资源组的访问权限。可为每个用户分配一个或多个角色，或者不分配角色。

如图 1-2 所示，通过角色 2 的分配，用户 1 和用户 2 可以共享访问相同资源集的权限。但是，通过角色 1 的分配，用户 1 还可访问其他资源。

图 1-2 用户帐户、角色和资源之间的关系



资源和资源组

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 提供对以下资源的访问：

- 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™）

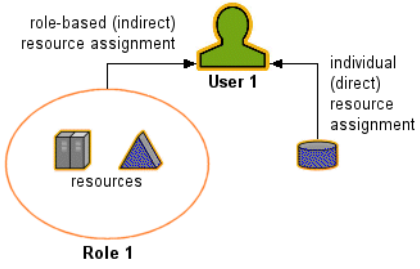
每个 Identity Manager 资源存储的信息被归类为以下若干个主要组：

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

通过以下分配可向 Identity Manager 用户帐户提供访问资源的权限，如图 1-3 中所示：

- 基于角色的分配 - 通过为用户分配角色，可直接将用户分配给一个或多个连接至此角色的资源。
- 单独分配 - 可直接为用户帐户分配各个资源。

图 1-3 资源分配



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。有关资源组的信息，请参见第 105 页上的“资源组”。

组织和虚拟组织

组织是用于启用管理委托的 Identity Manager 容器。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加载到 Identity Manager 系统信息库。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。

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 （已定义资源的基本上下文容器的子容器）中的一个容器。

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。

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 （如密码重置或帐户批准）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。

管理员角色

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。

策略

*策略*通过建立帐户 ID、登录和密码特征的约束，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约束。*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。

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。

对象关系

下表概要说明了各 Identity Manager 对象及它们之间的关系。

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 和一个或多个资源上的帐户。 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给一个或多个角色。 *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	概要描述一类用户并定义帐户在其中受到管理的资源和资源属性的集合。	*资源和资源组* 资源和资源组被分配给角色。 *用户帐户* 具有类似特征的角色组用户帐户。 *角色* 定义与其他角色之间的关系 （包含或排除）。
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* 资源被分配给角色；用户帐户通过其角色分配 “继承”资源的访问权限。 *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。

表 1-1 Identity Manager 对象关系 *（续）*

Identity Manager 对象	它是什么？	适用目标
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。
目录连接		
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 入门

阅读本章内容可以了解 Identity Manager 图形界面以及如何能快速开始使用 Identity Manager。包括下列主题：

Identity Manager 界面

Identity Manager 系统包括三个主要图形界面，用户可通过它们执行任务：

- 管理员界面
- 用户界面
- Identity Manager IDE

Identity Manager 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。

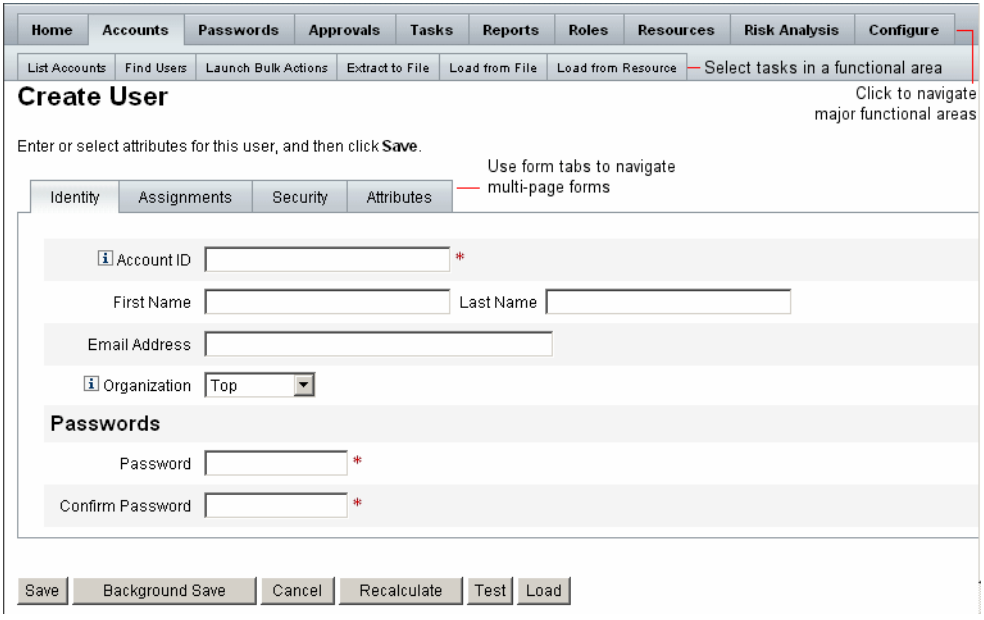
界面通过以下元素进行组织：

- **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** - 可能会在每个导航栏选项卡的下方显示次级选项卡或菜单，这取决于具体实现。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 "Accounts"）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。这在图 2-1 中进行了说明。

图 2-1 Identity Manager 管理员界面



管理员界面登录

登录到管理员界面时，您将保持登录状态（根据为您的实现所建立的会话限制），但有一种例外情况。如果您的 Web 浏览器禁用 Cookie，则执行以下操作时，系统将在会话期间提示您再次登录：

- 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

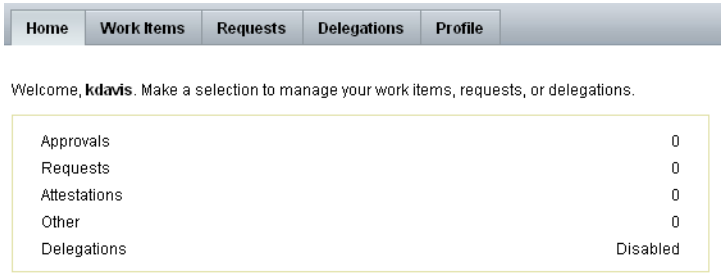
要避免多次登录请求，请启用 Cookie。

Identity Manager 用户界面

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。

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，如下图所示：

图 2-2 用户界面 （"Home" 选项卡）



通过 "Home" 选项卡可快速访问任何暂挂项目。单击列表中的项目可对工作项目请求进行响应或执行其他可用操作。操作完成后，单击 **Return to Main Menu** 以返回到 "Home" 页。

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。

用户界面为用户提供以下选项：

- **工作项目** - 批准或拒绝您拥有的或有权对其执行操作的所有暂挂工作项目。

  工作项目可以包括批准、证明或由 Identity Manager 生成的其他请求的操作项目。

- **请求** - 提交更新用户帐户资源分配和角色分配的请求。

  可以为用户或其雇员执行这些请求。

  使用 "Requests" 选项卡上的 **View** 子选项卡可以查看请求的进程状态详细信息。

- **委托** - 查看当前委托或指定委托。

- **配置文件** - 使用以下子选项卡可更改用户密码或帐户属性，或执行其他自置备任务：

  - **更改密码** - 选择此选项可在选定的资源或所有资源上更改密码。
  - **帐户属性** - 选择此选项可更改用户可编辑的属性，如帐户电子邮件地址。（此电子邮件地址为 Identity Manager 用于发送关于帐户通知的地址）。

- **验证问题** - 选择此选项可更改用户帐户的验证问题的答案。
- **访问权限** - 选择此选项可查看此帐户的资源分配 （直接或间接）。

自定义用户界面

此用户界面通常是自定义的，以提供特定于公司的唯一视图和自定义选项。

自定义导航布局

如果愿意，可以将用户界面中的导航从水平选项卡视图（默认）更改为垂直树视图。要配置垂直导航视图，请设置以下配置对象：

```
ui.web.user.menuLayout = 'vertical'
```

有关自定义用户界面的更多详细信息，请参阅 *Identity Manager 技术部署概述*。

自定义面板显示选项

在管理员界面中，您可以选择要在用户面板上显示的选项。要配置显示选项，请选择**配置**，然后选择**用户界面**。

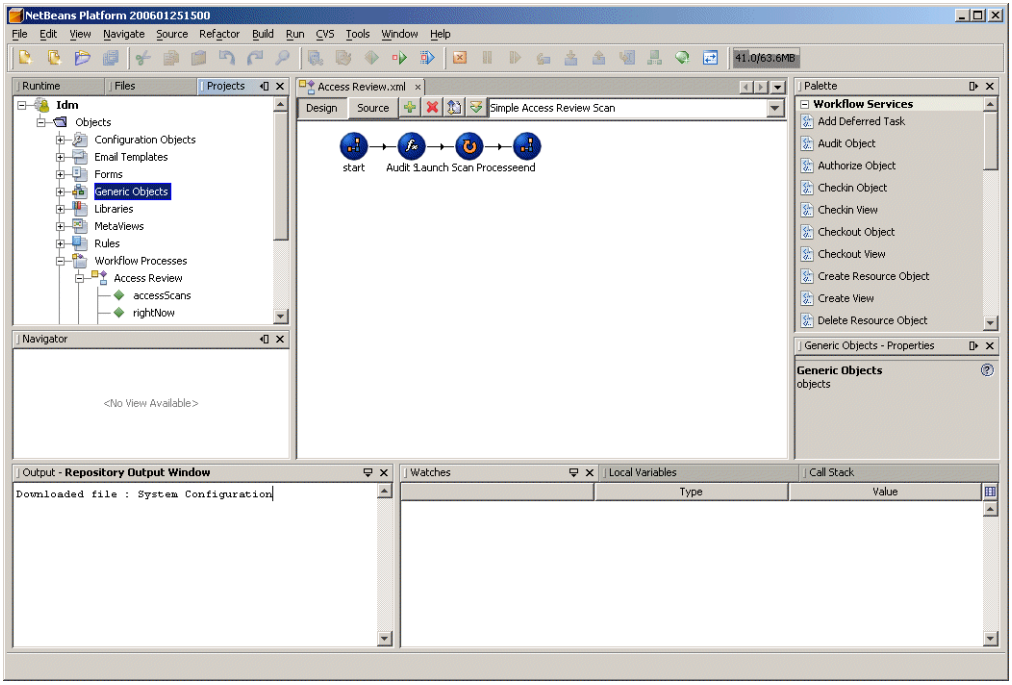
默认情况下，所有可用的可配置信息都显示在用户面板上。可以取消选择一个或多个以下选项，而不显示相应信息：

- **displayPasswordExpirationWarning** - 选择此选项可显示与密码过期相关的消息 （如果对帐户应用密码策略）。
- **displayAttestationReviews** - 选择此选项可显示证明工作项目的数量。
- **displayOtherWorkItems** - 选择此选项可显示其他工作项目的数量。
- **displayRemediations** - 选择此选项可显示修正工作项目的数量。
- **displayApprovals** - 选择此选项可显示批准工作项目的数量。
- **displayLoginFailures** - 选择此选项可显示失败的密码或验证问题登录尝试的次数。仅当为用户帐户策略配置了最大登录尝试值时才会显示此信息。
- **displayDelegations** - 选择此选项可显示一个字符串，用于表示用户已定义了批准委托。
- **displayRequests** - 选择此选项可显示未完成请求的数量，包括帐户的角色、组或资源更新的请求。

Identity Manager IDE

Sun Identity Manager 集成开发环境 (Integrated Development Environment, IDE) 提供 Identity Manager 表单、规则和工作流的图形视图。使用 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。下图显示了 IDE 界面。

图 2-3 Sun Identity Manager IDE 界面



有关 IDE 和使用其处理 Identity Manager 表单和工作流的详细信息，请参见 *Identity Manager 工作流、表单和视图*。

如果您早期版本的 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。

帮助和指导

要成功完成某些任务，可能需要参考 "Help" 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 **Help** 按钮，该按钮位于每个管理员界面和用户界面页的顶部，如图 2-4 中所示。

图 2-4 “帮助”按钮 （位于 Identity Manager 界面）

在每个 "Help" 窗口的底部有一个 "Contents" 链接，通过该链接可转到其他 "Help" 主题和 Identity Manager 术语表。

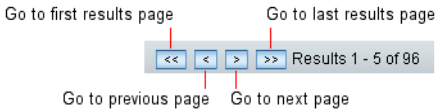
查找信息

使用 "Help" 窗口的搜索功能可以找到包含在 Identity Manager 帮助和文档中的主题和信息。要搜索联机文档资料，请执行以下步骤：

1. 在搜索区域输入一个或多个术语。
2. 选择搜索两种文档类型之一。默认情况下，该功能搜索联机帮助。
   - **联机帮助** - 通常，联机信息会提供一些步骤，以帮助您执行任务或完成表单。
   - **文档** （指导） - Identity Manager 指导主要提供有助于您理解概念和系统对象的信息以及完整的参考信息。
3. 单击 **Search**。

搜索将返回链接的搜索结果。使用 **Previous/Next** 或 **First/Last** 按钮可以遍览列出的结果，如图 2-5 中所示。

图 2-5 搜索结果导航



单击 **Reset** 可以清除 "Help" 窗口中的内容。

搜索行为

如果搜索多个字词，搜索功能将返回包含某一词、所有词和变体的结果。

例如，如果输入以下搜索项：

```
resource adapter
```

那么，返回的结果将包含：

- `resource`（和变体）
- `adapter`（和变体）
- `resource` 和 `adapter`（顺序不限），中间有 0 至 *n* 个词

但是，如果将搜索词用引号引起（例如 "resource adapter"），则搜索功能只返回该短语的完全匹配项。

或者，您可以使用高级查询语法特别指定包括、排除查询元素或指定查询元素的顺序。

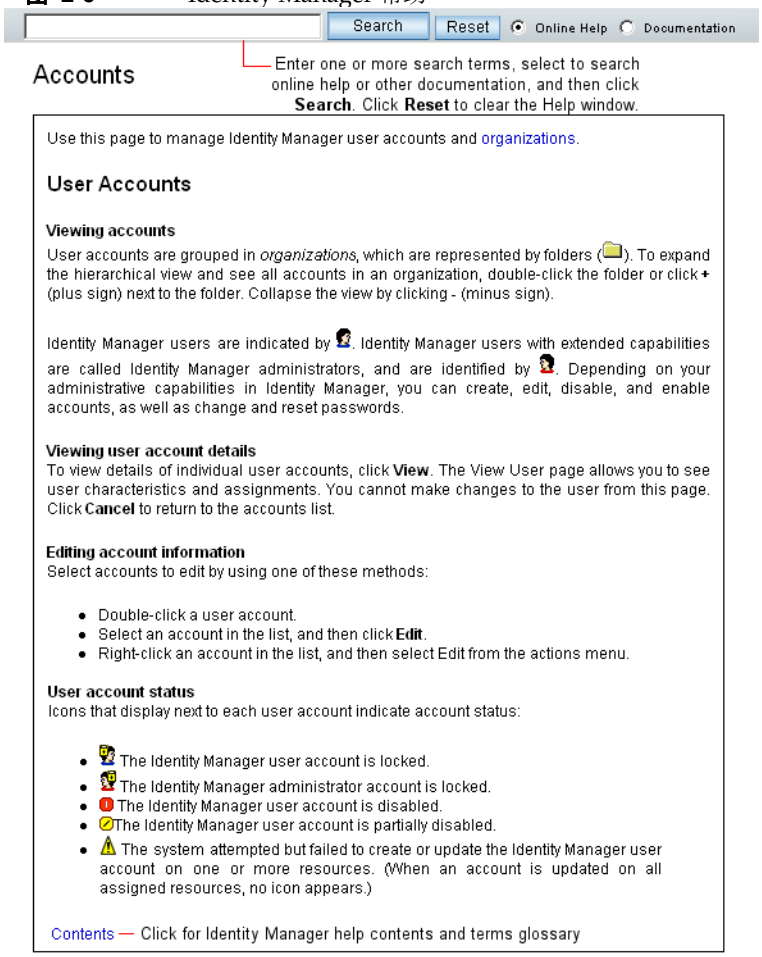
高级查询语法

搜索功能支持的高级查询语法包括：

- **通配字符**（? 和 *），通过它们可以指定拼写模式而不是完整字词或短语
- **查询运算符**（AND 或 OR），通过它们可以确定如何组合查询元素

有关 Identity Manager 高级文档搜索功能的详细信息，请参见本指南中的*附录 B “联机文档资料的高级搜索”*。

图 2-6 Identity Manager 帮助

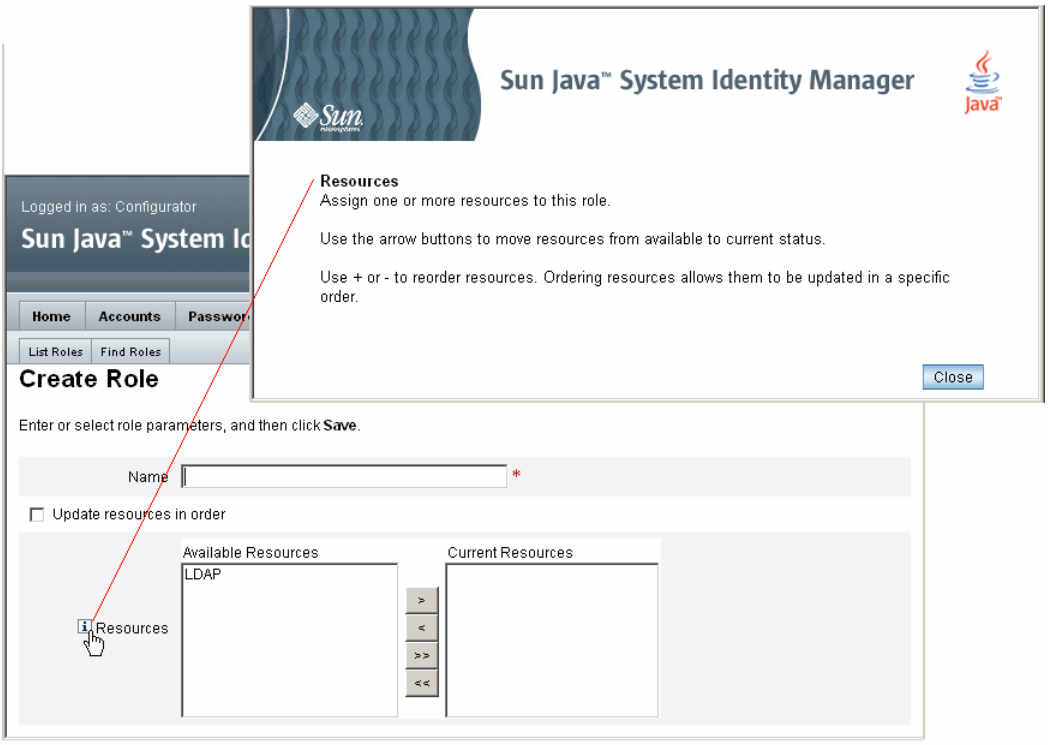


Identity Manager 指导

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 2-7 Identity Manager 指导



登录到 Identity Manager

要登录到 Identity Manager 管理员或用户界面，请输入用户 ID 和密码，然后单击**登录**。

忘记用户 ID

Identity Manager 允许您找回忘记的用户 ID。在登录页面中单击**忘记用户 ID？**时，将显示一个查找页面，并请求与您的帐户关联的身份属性信息（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。但是，可以通过以下任一操作禁用此功能：

- 将 login.jsp 中的 `forgotUserIdMode` 值设置为 false
- 将系统配置属性 `ui.web<admin|user>.disableForgotUserId` 的值设置为 true

所显示的用户属性名称集是通过系统配置属性 `security.authn.<Administrator Interface | User Interface>.lookupUserIdAttributes` 配置的。可以指定的属性为 `UserUIConfig` 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 任务

下列任务矩阵提供对经常执行的 Identity Manager 任务的快速参考。该矩阵显示开始每项任务时应转到的主要 Identity Manager 界面位置，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）。

表 2-1 Identity Manager 界面任务参考

管理 Identity Manager 用户		
要执行的操作：	**转至：**	**或：**
创建和编辑用户	**Accounts** 选项卡， **List Accounts** 选项	**Accounts** 选项卡， **Find Users** 选项 （"User Account Search Results" 页）
批准用户帐户创建	**Work Items** 选项卡， **Approvals** 子选项卡	
设置用户验证 （策略）	**Security** 选项卡， **Policies** 选项	
更改用户密码	**Passwords** 选项卡，**Change User Password** 选项	**Accounts** 选项卡， **List Accounts** 选项 **Accounts** 选项卡， **Find Users** 选项 （"User Account Search Results" 页） Identity Manager 用户界面
重置用户密码	**Passwords** 选项卡， **Reset User Password** 选项	**Accounts** 选项卡， **List Accounts** 选项 **Accounts** 选项卡， **Find Users** 选项 （"User Account Search Results" 页）
查找用户	**Accounts** 选项卡， **Find Users** 选项	**Passwords** 选项卡， **Change User Password** 选项

表 2-1 Identity Manager 界面任务参考 *（续）*

启用或禁用用户	**Accounts** 选项卡， **List Accounts** 选项	**Accounts** 选项卡， **Find Users** 选项 （"User Account Search Results" 页）
解除锁定用户	**Accounts** 选项卡， **List Accounts** 选项	**Accounts** 选项卡， **Find Users** 选项 （"User Account Search Results" 页）
管理 Identity Manager 管理员		
为此，请执行以下操作：	**转至：**	
设置委托管理 （通过组织）	**Accounts** 选项卡， **List Accounts** 选项， "Create User" 页	
分配权能	**Accounts** 选项卡， **List Accounts** 选项， "Create User" 或 "Edit User" 页 **Security** 子选项卡	
分配权能 （通过管理员角色）	**Accounts** 选项卡， **List Accounts** 选项， "Create User" 或 "Edit User" 页 **Security** 子选项卡	
设置批准者 （验证帐户创建）	**Accounts** 选项卡， **List Accounts** 选项， "Create Organization" 页 **Roles** 选项卡， "Create Roles" 页	
配置 Identity Manager		
为此，请执行以下操作：	**转至：**	
创建并管理资源 （资源向导）	**Resources** 选项卡	
管理资源组	**Resource** 选项卡， **List Resource Groups** 选项	
创建和管理角色	**Roles** 选项卡	
查找角色	**Roles** 选项卡， **Find Roles** 选项	
编辑权能	**Security** 选项卡， **Capabilities** 选项	
创建和编辑管理员角色	**Security** 选项卡， **Admin Roles** 选项， "Create Admin Role"/"Edit Admin Role" 页	
设置电子邮件模板	**Configure** 选项卡， **Email Templates** 选项	
设置密码、帐户和命名策略，为组织分配策略	**Security** 选项卡， **Policies** 选项	
配置身份属性	**Meta View** 选项卡， **Identity Attributes** 选项	
配置身份事件	**Meta View** 选项卡， **Identity Events** 选项	
配置 ChangeLog	**Meta View** 选项卡， **ChangeLogs** 选项	
加载和同步帐户与数据		
为此，请执行以下操作：	**转至：**	
导入数据文件 （如 XML 格式的表单）	**Configure** 选项卡， **Import Exchange File** 选项	
加载资源帐户	**Account** 选项卡， **Load from Resource** 选项	

表 2-1 Identity Manager 界面任务参考 *（续）*

从文件加载帐户	**Account** 选项卡， **Load from File** 选项
比较 Identity Manager 用户与资源帐户	**Resources** 选项卡， **Reconcile with Resources** 选项
审计、风险分析和报告	
为此，请执行以下操作：	**转至：**
设置要捕获的审计事件并启用审计	**Configure** 选项卡， **Audit** 选项
运行和管理报告	**Reports** 选项卡， **Run Reports** 选项，以创建、运行和下载报告； **View Reports** 以查看报告结果。
定义和运行风险分析报告	**Reports** 选项卡，**Risk Analysis** 选项
查看图形报告	**Reports** 选项卡， **View Dashboards** 选项
管理遵循性	
为此，请执行以下操作：	**转至：**
定义审计策略	**Compliance** 选项卡， **Manage Policies** 选项
分配审计策略	**Accounts** 选项卡， **Compliance** 选项
管理遵循性违规	**我的工作项目** 选项卡，**修正** 选项
设置周期性访问查看	**Compliance** 选项卡， **Manage Access Scans** 选项
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	**Reports** 选项卡， **Auditor Report** 类型选项

表 2-1 Identity Manager 界面任务参考 *（续）*

管理 Identity Manager 任务	
为此，请执行以下操作：	**转至：**
运行已定义的任务 （或进程）	**Server Tasks** 选项卡， **Run Tasks** 选项
调度任务	**Server Tasks** 选项卡， **Manage Schedule** 选项
查看任务结果	**Server Tasks** 选项卡， **Find Tasks** 或 **All Tasks** 选项
暂停或终止任务	**Server Tasks** 选项卡， **All Tasks** 选项
管理服务提供者用户	
为此，请执行以下操作：	**转至：**
管理服务提供者用户	**Accounts** 选项卡， **Manage Service Provider Users** 选项
管理服务提供者事务	**Server Tasks** 选项卡， **Service Provider Transactions** 选项
配置服务提供者功能	**Service Provider** 选项卡， **Edit Main Configuration** 选项
配置事务默认值	**Service Provider** 选项卡， **Edit Transaction Configuration** 选项
创建或编辑服务提供者策略	**Security** 选项卡， **Policies** 选项

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 "Accounts" 区域并提供用于管理用户帐户的步骤。
第 4 章 “配置”	介绍配置任务以及如何设置 Identity Manager 对象。
第 5 章 “管理”	介绍如何创建和管理 Identity Manager 管理员和组织。
第 6 章 “数据同步与加载”	提供可用于维护 Identity Manager 中当前数据的功能和工具的指南。
第 7 章 “报告”	介绍报告以及如何生成报告。
第 8 章 “任务模板”	介绍可用于配置某些工作流行为的任务模板。

章节主题	描述
第 9 章 “PasswordSync”	介绍如何设置 PasswordSync 实用程序，以将 Windows Active Directory 和 Windows NT 域中的密码更改与 Identity Manager 的更改同步。
第 10 章 “安全”	介绍安全性功能以及如何使用这些功能。
第 11 章 “身份审计”	介绍如何定义审计策略以及管理遵循性。
第 12 章 “审计日志记录”	介绍审计日志以及审计系统如何工作。
第 13 章 “服务提供者管理”	介绍用于管理服务提供者用户的功能。
附录 A “lh 参考消息”	介绍 Identity Manager 命令行中可用的命令。
附录 B “联机文档资料的高级搜索”	有关在联机帮助中使用高级查询搜索 Identity Manager 文档的说明。
附录 C “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 D “活动同步向导”	用于配置 7.0 之前版本的 Identity Manager 的活动同步。

第 3 章

用户和帐户管理

本章介绍通过 Identity Manager 管理员界面管理用户的信息和步骤。您将了解到 Identity Manager 用户和帐户管理任务，包括：

关于用户帐户数据

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。

在管理员界面的 “创建用户” 页 （**帐户**选项卡）中， Identity Manager 将用户数据归在以下区域中：

- Identity
- Assignments
- Security

- 委托
- Attributes
- 遵循性

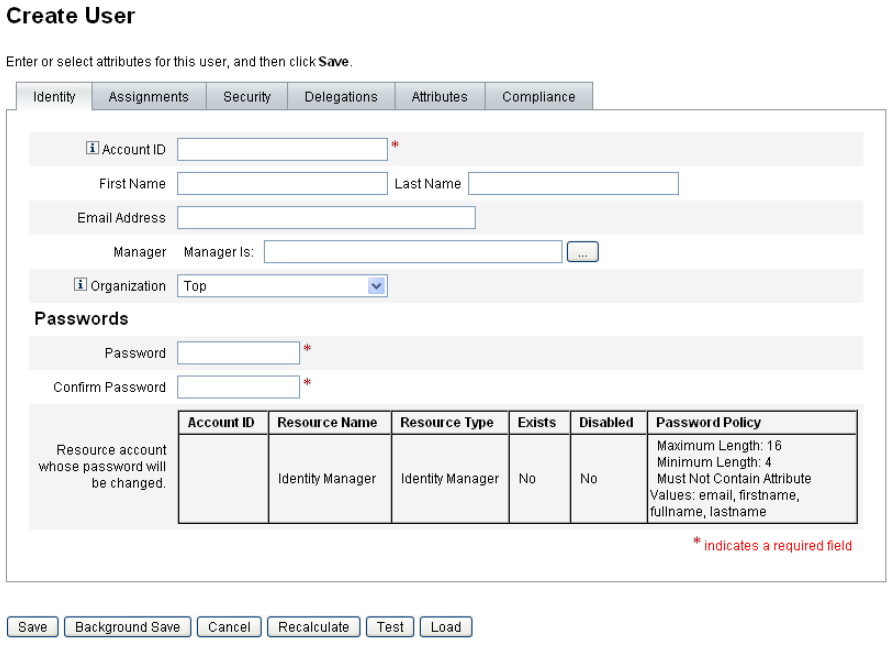
身份

“身份”区域定义用户的帐户 ID、用户名、联系人信息、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，请参阅本章第 80 页上的 “使用用户帐户密码”中的相关节。

下图说明 "Create User" 页的 "Identity" 区域。

图 3-1 创建用户 - 身份



分配

"Assignments" 区域为访问 Identity Manager 对象 （如资源）设置限制。

单击 **Assignments** 表单选项卡以设置以下分配：

- **Identity Manager 帐户策略**分配 - 建立密码和验证限制。
- **角色**分配 - 概要描述一类用户。角色通过间接分配定义用户对资源的访问。
- **资源和资源组**访问 - 显示可以直接分配给用户的可用资源和资源组，以及可以从用户访问中排除的资源。这些资源对通过角色分配间接分配给用户的资源加以补充。

安全

在 Identity Manager 术语中，分配了扩展权能的用户称为 Identity Manager *管理员*。使用 "Security" 选项卡可以通过以下分配为用户建立这些扩展管理权能：

- **管理员角色** - 组合一组特定且唯一的权能和受控组织，有助于将调整的分配用于管理用户。
- **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。
- **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，用户必须被分配至少一个管理员角色，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 136 页上的 “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。

委托

“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，请阅读第 175 页上的 “委托工作项目”。

属性

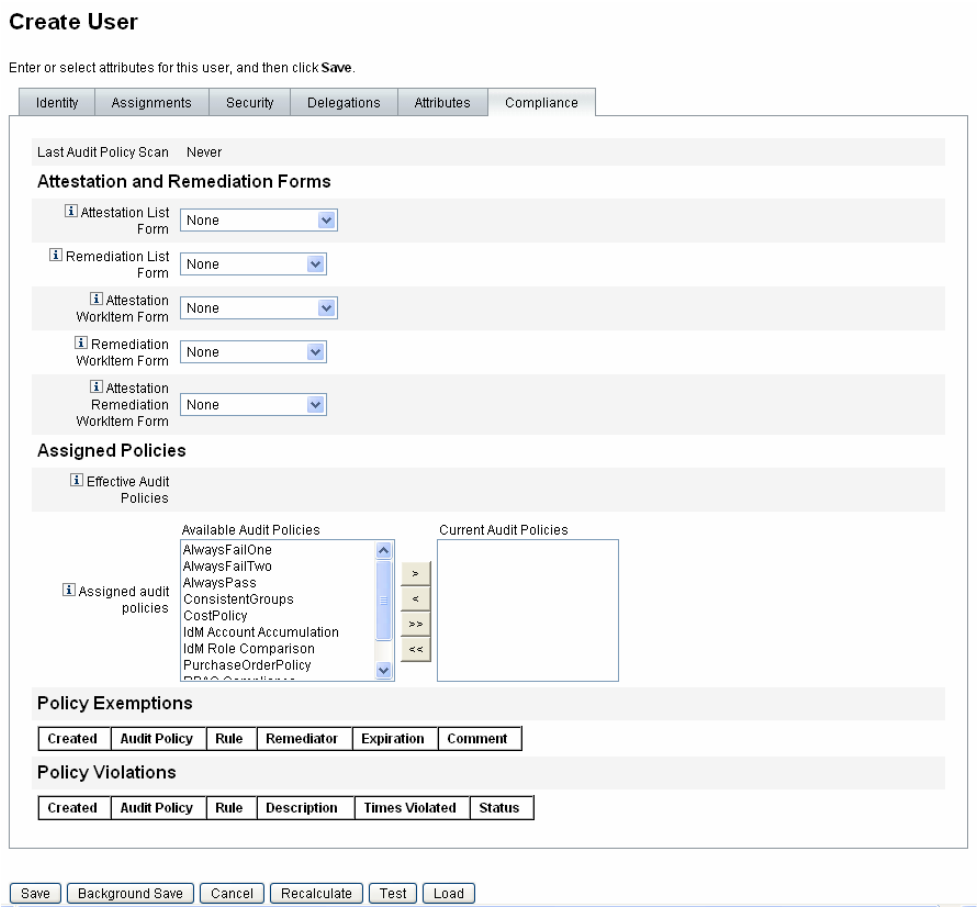
"Create User" 页上的 "Attributes" 选项卡定义与分配的资源关联的帐户属性。列出的属性按分配的资源分类，具体情况根据分配资源的不同而不同。

遵循性

“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。只能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。

图 3-2 "Create User" 页 - "Compliance" 选项卡



要分配审计策略，请将选定策略从 "Available Audit" 列表中移动到 "Current Audit Policies" 列表中。

注 还可以通过选择“用户操作”列表中的**查看遵循性状态**来访问“遵循性”选项卡上的信息。要查看在特定时间段内针对某个用户所记录的遵循性违规，请从“用户操作”列表中选择**查看遵循性违规日志**，然后指定要查看的条目范围。

界面的帐户区域

在 Identity Manager 帐户区域内可管理 Identity Manager 用户。要访问此区域，请从 "Administrator interface" 菜单栏中选择 **Accounts**。

帐户列表显示所有 Identity Manager 用户帐户。帐户按组织和虚拟组织分组，用文件夹分层表示。

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。

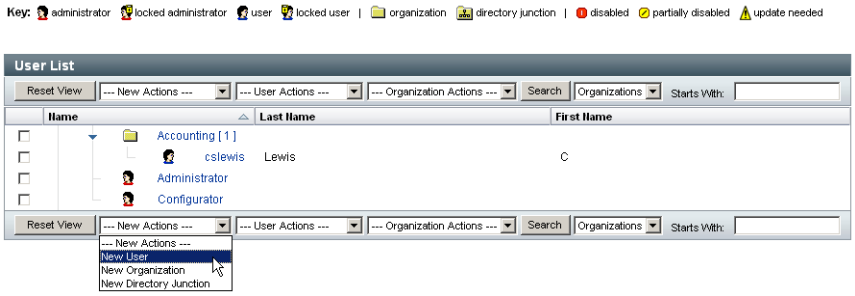
要展开分层结构视图，查看组织中的帐户，请单击文件夹旁的三角指示符。再次单击指示符可折叠视图。

帐户区域中的操作列表

使用操作列表（位于帐户区域的顶部和底部，如图 3-3 所示）可以执行一系列操作。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；更改和重置密码；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。

图 3-3 Accounts List



在 "Accounts List" 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 "Organizations" 或 "Users"，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 **Search**。有关在帐户区域中搜索的详细信息，请参见第 74 页上的 “查找帐户”。

用户帐户状态

每个用户帐户旁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
	Identity Manager 用户帐户已被锁定。这意味着用户因登录尝试失败次数超过为资源建立的登录限制而被锁定在资源帐户之外。
	Identity Manager 管理员帐户已被锁定。
	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。）
	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。）

使用用户帐户

从 "Administrator interface" 的帐户区域中，您可以在以下系统对象上执行一系列操作：

- **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、取消链接以及审计

- **密码** - 更改和重置
- **组织** - 在组织的成员上创建、编辑、刷新和执行用户操作
- **目录连接** - 创建

用户

本节中的主题重点介绍管理用户帐户。有关其他管理级别任务 （如管理组织）的信息，请参见第 5 章 “管理”。

查看

要查看用户帐户的详细信息，请在列表中选择用户，然后从 "User Actions" 列表中选择 **View**。

"View User" 页显示编辑或创建用户时建立的身份、分配、安全和属性信息选项的子集。无法编辑 "View User" 页上的信息。单击 **Cancel** 返回至 "Accounts " 列表。

创建 （"New Actions" 列表， "New User" 选项）

要创建用户帐户，请从 "New Actions" 列表中选择 **New User**。如果要在除顶层以外的组织中创建用户，请选择组织文件夹，然后从 "New Actions" 列表中选择 **New User**。

在一个区域中的可用选项可能取决于您在其他区域中所做的选择。

"Create User" 页 （由*用户表单*定义）使您可以为用户帐户设置以下项目：

- **身份** - 用户名、电子邮件、组织和密码详细信息
- **分配** - 帐户策略、角色和资源
- **安全性** - 组织和权能
- **委托** - 工作项目委托
- **属性** - 已分配的资源的特定属性

要更好地反映业务进程或特定管理员权能，可以专为您的环境配置用户表单。有关自定义用户表单的详细信息，请参见 *Identity Manager 工作流、表单和视图*。

单击 "Create User" 页上的选项卡可浏览创建用户设置。可以按任意顺序在选项卡间移动。完成选择后，可以使用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 "Accounts" 页、 "Find User Results" 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。

表 3-2 后台保存任务状态指示器的说明

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，创建用户时将创建一个可从 “批准” 选项卡查看的工作项目。批准该项目将覆盖生效日期并创建帐户；拒绝该项目将取消帐户创建。有关配置生效的详细信息，请参见第 249 页上的 “配置 "Sunrise and Sunset" 选项卡”。

创建多个用户帐户 （身份）

可以在单个资源上创建多个用户帐户。创建 （或编辑）用户并为用户分配一个或多个资源时，也可在该资源上请求和定义附加帐户。

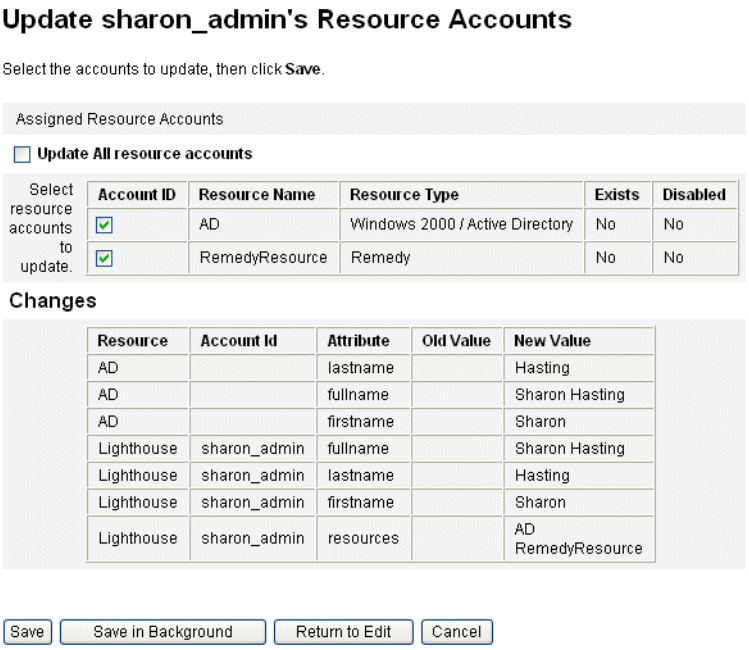
编辑

要编辑帐户信息，请选择以下操作之一：

- 单击帐户列表中的用户帐户。
- 在列表中选择用户帐户，然后从 "User Actions" 列表中选择 **Edit**。

进行更改并保存更改后，Identity Manager 将显示 "Update Resource Accounts" 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。选择 **Update All resource accounts** 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，或者不选择任何资源帐户进行更新。

图 3-4 编辑用户 （更新资源帐户）



再次单击 **Save** 完成编辑，或者单击 **Return to Edit** 进行进一步更改。

移动用户 （用户操作）

“更改用户组织”任务使您可以从当前分配给用户的组织中删除该用户，然后将用户重新分配给或移动到新的组织。

要将用户移动到其他组织，请在列表中选择一个或多个用户帐户，然后从 "User Actions" 列表中选择 **Move**。

重命名 （用户操作）

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，然后从 "User Actions" 列表中选择 **Rename** 选项。

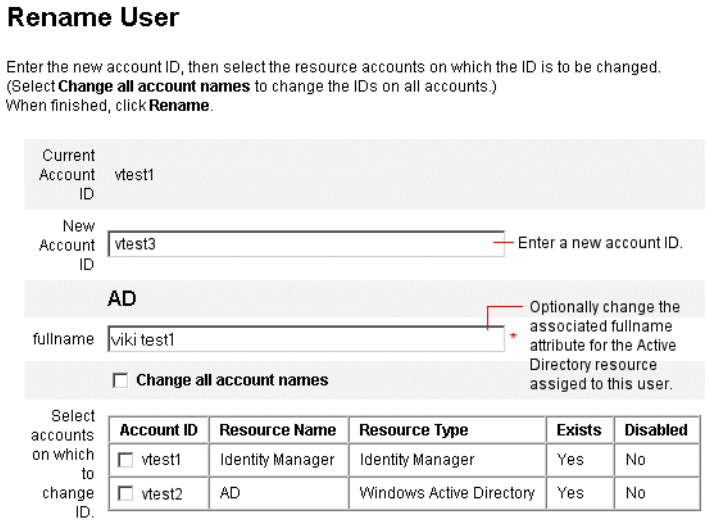
使用 “重命名用户”页可更改用户帐户名、相关资源帐户名和与用户的 Identity Manager 帐户相关的资源帐户属性。

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
- Active Directory 资源帐户名
- Active Directory 资源属性 （全称）

图 3-5 重命名用户



禁用用户 （用户操作、组织操作）

如果禁用用户帐户，即更改了此帐户，使得该用户无法再登录到 Identity Manager 或该用户的已分配资源帐户。

注 对于不支持帐户禁用功能的已分配资源，禁用用户帐户的方式是分配随机生成的新密码。

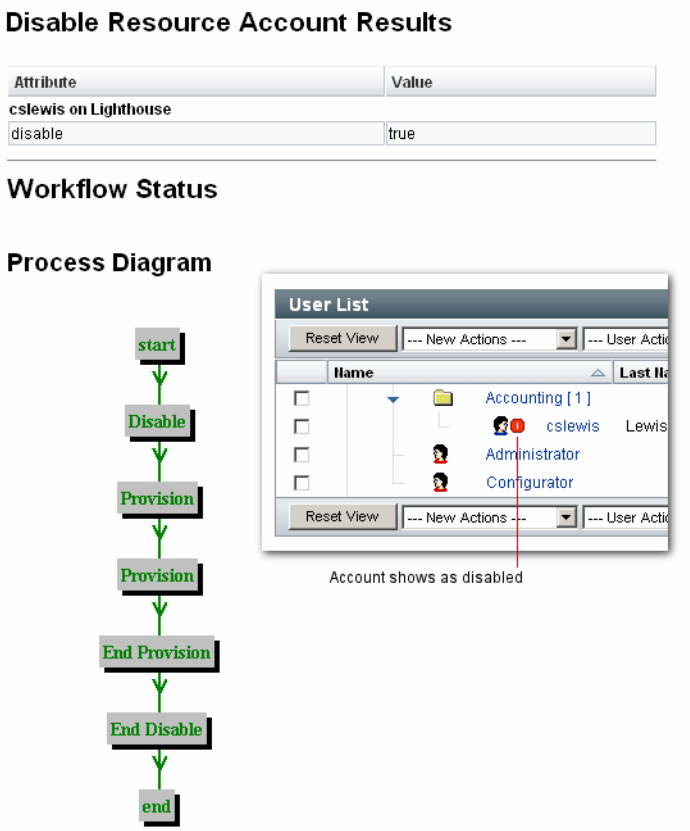
禁用单个用户帐户

要禁用用户帐户，请在列表中选择此帐户，然后从 "User Actions" 列表中选择 **Disable**。

在显示的 "Disable" 页中，选择要禁用的资源帐户，然后单击 **OK**。Identity Manager 将显示禁用 Identity Manager 用户帐户及其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。

图 3-6 说明了 "Disable" 页上的禁用帐户。

图 3-6 禁用帐户



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 "User Actions" 列表中选择 **Disable**。

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。

启用用户 （用户操作、组织操作）

用户帐户的启用过程与禁用过程相反。对于不支持帐户启用功能的资源， Identity Manager 会随机生成一个新密码。根据选定的通知选项，它还会在管理员的结果页中显示该密码。

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

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，然后从 "User Actions" 列表中选择 **Enable**。

在显示的 "Enable" 页中，选择要启用的资源，然后单击 **OK**。Identity Manager 将显示启用 Identity Manager 帐户及其所有相关资源帐户的结果。

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。

更新用户 （用户操作、组织操作）

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

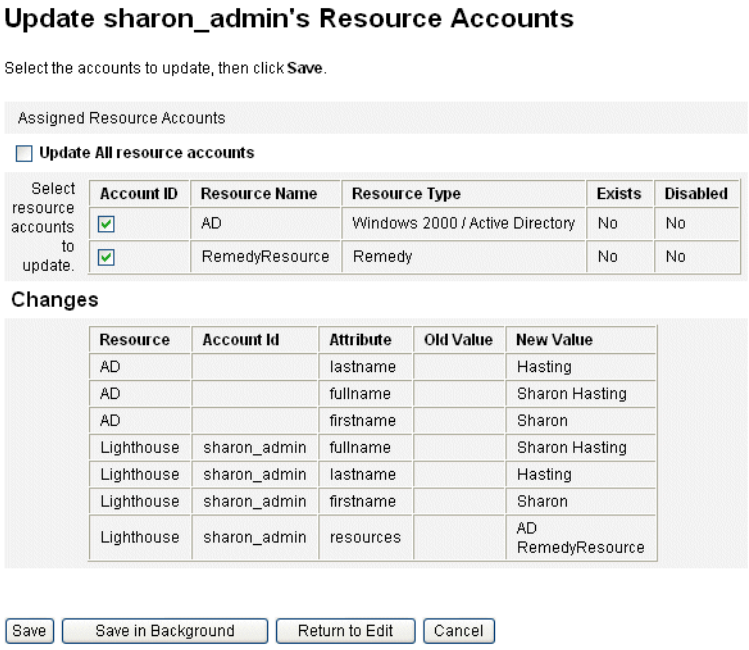
要更新用户帐户，请在列表中选择此帐户，然后从 "User Actions" 列表中选择 **Update**。

在 "Update Resource Accounts" 页中，选择一个或多个要更新的资源，或者选择 **Update All resource accounts** 更新所有分配的资源帐户。完成选择后，单击 **OK** 开始更新过程。或者，单击 **Save in Background** 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 3-7 说明了 "Update Resource Accounts" 页。在图中， Lighthouse 是指 Identity Manager。

图 3-7 更新资源帐户



更新多个帐户

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，然后从 "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。

解除锁定用户 （用户操作、组织操作）

用户因登录重试次数超过为资源建立的登录限制，可能被锁定在一个或多个资源帐户之外。用户的有效 Lighthouse 帐户策略可以建立密码或问题登录尝试失败的最大次数。

用户因超过最大密码登录尝试失败次数而被锁定后，将不允许验证到任何 Identity Manager 应用程序界面（包括 User interface、Administrator interface、Forgot My Password、Identity Manager IDE、SOAP 和控制台）。如果用户因超过最大问题登录尝试失败次数而被锁定，则可以验证到除 "Forgot My Password" 以外的任何 Identity Manager 应用程序界面。

密码登录尝试失败

如果因密码登录尝试失败而锁定，用户帐户将保持锁定状态，直到：

- 管理用户解除锁定。要成功解除锁定帐户，必须为管理员分配 “解除锁定用户”权能，并且必须具有用户成员组织的管理控制权限。
- 如果已设置锁定到期日期和时间，则当前日期和时间要晚于用户的锁定到期日期和时间。（使用 Lighthouse Account Policy 中的 Lock Timeout 值可以设置锁定到期时间。）

问题登录尝试失败

如果因超过问题登录尝试失败最大次数而锁定，用户帐户将保持锁定状态，直到执行以下操作之一：

- 管理用户解除锁定。要成功解除锁定帐户，必须为管理员分配 “解除锁定用户”权能，并且必须具有用户成员组织的管理控制权限。
- 锁定的用户或具有相应权能的用户更改或重置用户密码。

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）
- 更改或重置密码
- 禁用或启用
- 重命名
- 解除锁定

处于锁定状态的用户无法登录到包括 Administrator interface、 User interface 和 Identity Manager IDE 的任何 Identity Manager 应用程序。无论通过向验证问题提供其用户 ID 和答案尝试用 Identity Manager 用户 ID 和密码登录，还是通过一个或多个资源登录，此限制都适用。

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 "User Actions" 或 "Organization Actions" 列表中选择 "Unlock Users"。

删除 （用户操作、组织操作）

删除操作包括从资源删除 Identity Manager 用户帐户访问权限的多个选项：

- **删除** - 对于选定的每个资源，Identity Manager 会删除与其相关的资源帐户。同时会取消选定资源与 Identity Manager 用户的链接。
- **取消分配** - 对于选定的每个资源，Identity Manager 会从用户的已分配资源列表中删除相关的资源。选定资源与用户的链接被取消。而相关资源帐户不会被删除。
- **取消链接** - 对于选定的每个资源， Identity Manager 会从 Identity Manager 用户删除相关的资源帐户信息。

注 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。

要开始删除操作，请选择用户帐户，然后在 "User Actions" 或 "Organization Actions" 列表中选择相应的删除操作。

Identity Manager 将显示 "Delete Resource Accounts" 页。

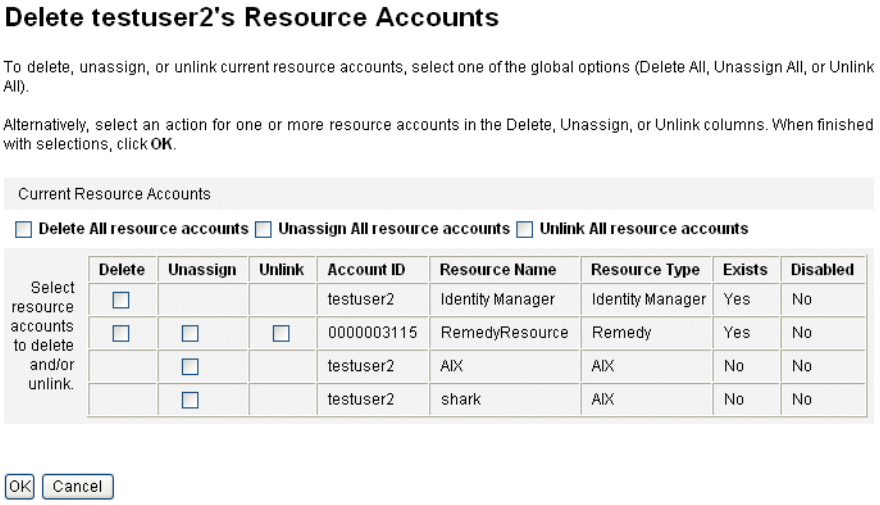
删除用户帐户和资源帐户

要删除 Identity Manager 用户帐户或资源帐户，请在 "Delete" 列中进行选择，然后单击 **OK**。要删除所有资源帐户，请选择 "Delete All resource accounts" 选项，然后单击 **OK**。

取消分配或取消资源帐户的链接

要从 Identity Manager 用户帐户取消分配资源帐户或取消资源帐户的链接，请在 "Unassign" 列或 "Unlink" 列中进行单独选择，然后单击 **OK**。要取消分配所有资源帐户，请选择 "Unassign All resource accounts" 或 "Unlink All resource accounts" 选项，然后单击 **OK**。

图 3-8 删除用户帐户和资源帐户



密码

可以使用 **Change Password** 和 **Reset Password** 用户操作来调用 "Edit User" 页以及更改或重置选定用户的用户密码。另请参见第 80 页上的 “使用用户帐户密码”。

查找帐户

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，请在菜单栏中选择 **Accounts**，然后选择 **Find Users**。可按以下一种或多种搜索类型搜索帐户：

- 帐户详细信息，例如用户名、电子邮件地址、姓或名。这些选项取决于贵机构的具体 Identity Manager 实现。
- 用户的管理员。
- 资源帐户状态，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。

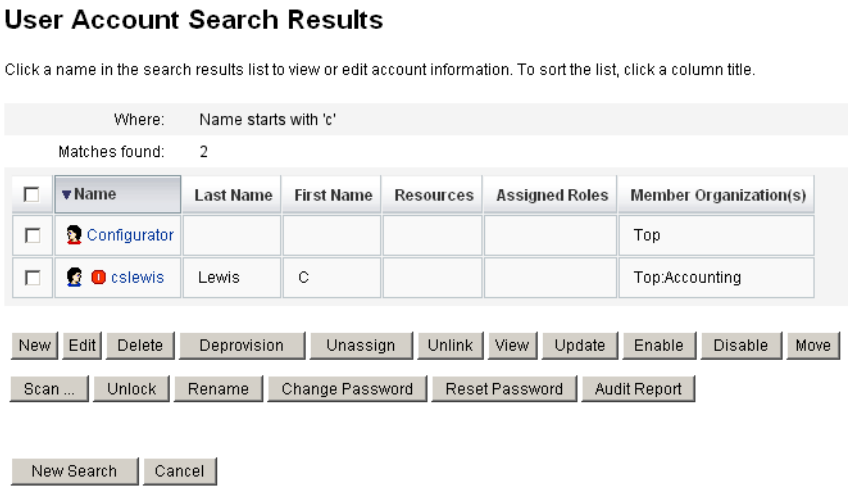
- **已启用** - 用户拥有对所有已分配的资源帐户的访问权限。

- 用户帐户状态，包括：
  - **已锁定** - 因为密码或问题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。
  - **未锁定** - 未限制用户帐户访问。
- 更新状态，包括：
  - **无** - 尚未在任何资源中更新的用户帐户。
  - **部分** - 至少已对一个 （但不是所有）已分配资源进行更新的用户帐户。
  - **所有** - 已对所有已分配资源进行更新的用户帐户。
- 已分配的资源
- Role
- 组织
- 组织控制权限
- 权能
- 管理员角色

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 **Edit**。
- 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/重置密码）。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。

图 3-9 用户帐户搜索结果



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** - 对所有选定的资源帐户执行删除、取消分配和取消链接操作。选择 “以 Identity System 帐户为目标”选项可删除每个用户的 Identity Manager 帐户。
- **删除和取消链接** - 删除所有选定的资源帐户，并取消这些帐户与用户的链接。
- **禁用** - 禁用所有选定的资源帐户。选择 "Target the Identity Manager Account" 选项以禁用每个用户的 Identity Manager 帐户。
- **启用** - 启用所有选定的资源帐户。选择 “以 Identity Manager 帐户为目标”选项可启用每个用户的 Identity Manager 帐户。
- **取消分配，取消链接** - 取消所有选定资源帐户的链接，并删除对这些资源的 Identity Manager 用户帐户分配。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。
- **取消链接** - 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。如果将已经通过角色或资源组间接分配给 Identity Manager 用户的帐户取消链接，可在更新用户时恢复该链接。

如果在文件或应用程序（如电子邮件客户端或电子表格程序）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。在 **Accounts** 选项卡下的 "Find Users" 页上搜索用户。

当任务完成后显示任务结果时，可通过单击 **Download 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

要启动批量帐户操作，请选择或输入值，然后单击 **Launch**。Identity Manager 会启动后台任务，以执行批量操作。

要监视批量操作任务的状态，请转至 **Tasks** 选项卡，然后单击该任务链接。

使用操作列表

可以使用逗号分隔值 (Comma-separated Value, 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。其余行的每一行都对应于要对 Identity Manager 用户、该用户的资源帐户或这两者执行的操作。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：

- **用户** - 包含 Identity Manager 用户的名称。
- **命令** - 包含对 Identity Manager 用户采取的操作。有效命令有：
  - **删除** - 对资源帐户和/或 Identity Manager 帐户执行删除、取消分配和取消链接操作。
  - **删除和取消链接** - 删除资源帐户并取消链接。
  - **禁用** - 禁用资源帐户和/或 Identity Manager 帐户。
  - **启用** - 启用资源帐户和/或 Identity Manager 帐户。
  - **取消分配** - 对资源帐户取消分配并取消链接。
  - **取消链接** - 对资源帐户取消链接。
  - **创建** - 创建 Identity Manager 帐户。或者创建资源帐户。
  - **更新** - 更新 Identity Manager 帐户。或者创建、更新或删除资源帐户。

- **创建或更新** - 如果 Identity Manager 帐户不存在，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。它可具有下列值：

- **all** - 处理所有资源帐户，包括 Identity Manager 帐户。
- **resonly** - 处理 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 "User View" 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 "User View" 中可用属性的信息，请参见 *Identity Manager 工作流、表单和视图*。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** - 放置 Identity Manager 帐户的组织名称。
- **accounts**[*resource_name*].*attribute_name* - 资源帐户的属性。属性的名称在资源的模式中列出。

下面是创建和更新操作的 CSV 格式的示例：

```
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
```

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）在一个字段中分隔多个值。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该字段的值。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

如果字段值带有逗号 (,) 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上 ("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* - 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* - 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** - 将此布尔型属性设置为 true 可中止当前操作。
- **waveset.bulk.abortMessage** - 将此属性设置为消息字符串，当 waveset.bulk.abort 设置为 true 时，可显示该消息字符串。如果未设置此属性，将显示一条普通中止消息。

使用用户帐户密码

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。

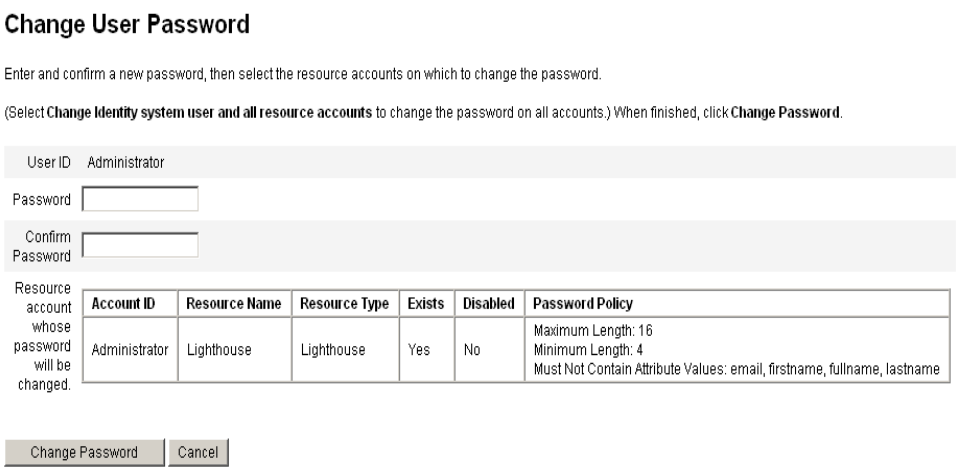
更改用户帐户密码

要更改用户帐户密码：

1. 在菜单栏中选择 **Passwords**。

   默认情况下，将显示 "Change User Password" 页，如下图所示。

图 3-10 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. 在条目字段中键入搜索项目的一个或多个字母，然后单击 **Find**。 Identity Manager 会返回用户 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. 输入并确认新密码信息，然后单击 **Change Password** 以更改所列资源帐户的用户密码。 Identity Manager 将显示一个工作流程图，说明密码更改操作的执行顺序。

重置用户帐户密码

重置 Identity Manager 用户帐户密码的过程与更改过程类似。重置过程与密码更改过程的不同之处为重置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）控制多个重置选项，其中包括：

- 禁用重置前允许的密码重置频率
- 新密码的显示或发送位置。根据为角色选择的 "Reset Notification Option"，Identity Manager 以电子邮件方式将新密码发送给相应用户，或 （在 "Results" 页中）将新密码显示给请求重置密码的 Identity Manager 管理员。

重置时密码到期

默认情况下，重置用户密码时密码立即到期。这表示重置密码后，用户首次登录时，必须选择新密码才能进行访问。可在表单中改写此缺省值，这样，用户密码的到期日期就取决于与用户相关的 “Lighthouse 帐户策略”中的密码到期策略设置。

例如，在 "Reset User Password Form" 中，将 `resourceAccounts.currentResourceAccounts[Lighthouse].expirePassword` 的值设置为 `false`。

有两种利用 "Lighthouse Account Policy" 中的 "Reset Option" 字段使密码到期的方法：

- **永久** - 重置密码时，会使用在 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，则更改或重置的密码将永不到期。
- **临时** - 重置密码时，会使用在 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，则更改或重置的密码将永不到期。如果将 tempPasswordExpiry 的值设置为 0，则密码立即到期。

  `tempPasswordExpiry` 属性只在重置密码 （如随机更改）时适用；它不适用于更改密码的情况。

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。

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，请在菜单栏中选择 **Security**，然后选择 **Policies**。

要编辑密码策略，请在 "Policies" 列表中选择密码策略。要创建密码策略，请从 "New" 选项列表中选择 **String Quality Policy**。

创建策略

密码策略是字符串质量策略的默认类型。命名并提供新策略的可选描述后，您需要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。

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：

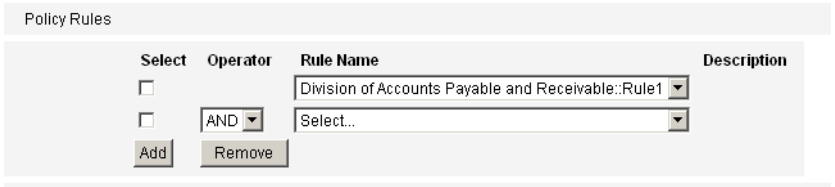
- 字母、数字、大写、小写和特殊字符的最少数量和最多数量
- 嵌入的数字字符的最少数量和最多数量
- 重复字符和顺序字符的最多数量
- 开始字母和数字字符的最少数量

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量。 还可以设置必须通过验证的字符类型规则的最小数量，如图 3-11 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 3-11 密码策略 （字符类型）规则



字典策略选则

可以选择根据字典中的词检查密码。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，请参阅 *Identity Manager 部署工具*中的 “配置字典支持”一章。

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。有关更多信息，请参见第 126 页上的 “字典策略”。

不得包含属性

选择一个或多个密码不能包含的属性。属性包括：

- accountID
- email
- firstname
- fullname

- lastname

可以在 UserUIConfig 配置对象中更改密码允许的 “不得包含” 属性集。UserUIConfig 中的密码属性列于 <PolicyPasswordAttributeNames> 中。

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 "Password Policy" 选项列表中选择它， "Password Policy" 选项列表在 "Create Resource Wizard:Identity Manager Parameters" 或 "Edit Resource Wizard:Identity Manager Parameters" 页的 "Policy Configuration" 区域中。

用户验证

如果用户忘记密码或密码被重置，则该用户可通过回答一个或多个帐户验证问题来获得对 Identity Manager 的访问权限。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 "Create User" 页和 "Edit User" 页中）。

在帐户策略中设置验证：

1. 在菜单栏中选择 **Security** ，然后选择 **Policies**。
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。

重要提示！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。

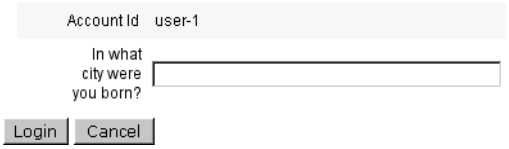
根据验证规则集，可要求用户对以下问题做出回答：

- 所有验证问题
- 任一验证问题
- 从此规则集中随机选择的问题；问题数目由您指定的数值决定
- 从规则集中顺序选择的一个或多个问题

可以检验您的验证选择，方法是：登录到 Identity Manager 的 "User interface"，单击 "Forgot Your Password?"，并回答显示的一个或多个问题。

图 3-12 显示了 "User Account Authentication" 屏幕的示例。

图 3-12 User Account Authentication

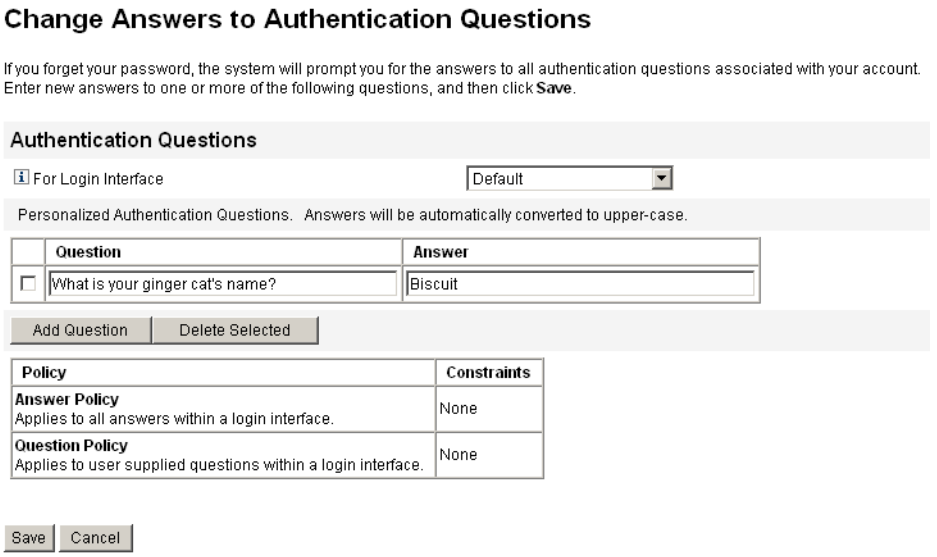


个性化验证问题

在 Lighthouse 帐户策略中，您可以选择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 3-13 显示了此页的示例。

图 3-13 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。

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：

代码示例 3-1 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：

代码示例 3-2 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 4 章中的 “配置 Identity Manager 资源”。
- 权能 - 权能由规则定义。Identity Manager 提供了一系列权能，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 5 章中的 “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 5 章中的了解 Identity Manager 组织。

有关 Identity Manager 管理员和管理任务的详细信息，请参见第 5 章 “管理”。

用户自行搜索

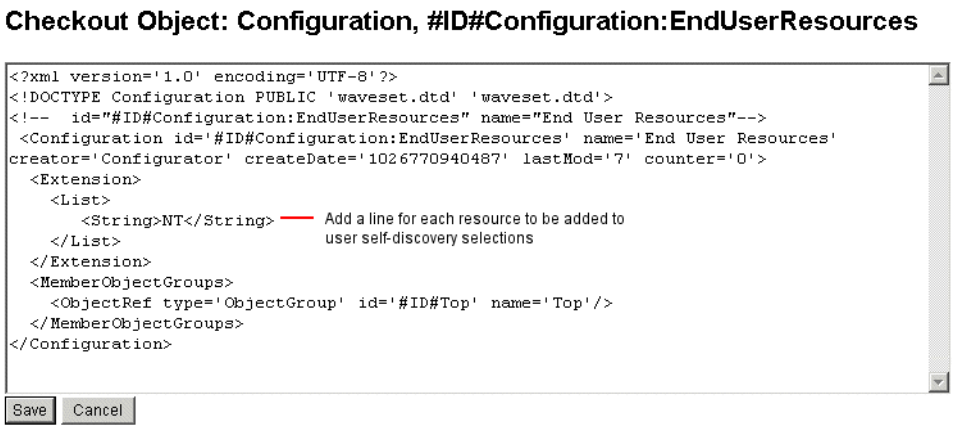
用户可以使用 Identity Manager User interface *搜索*资源帐户。这意味着拥有 Identity Manager 身份的用户可以与现有的但未关联的资源帐户相关联。

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。使用以下步骤执行此操作：

1. 打开 Identity Manager 的 "System Settings" 页 (`idm/debug`)。
2. 从 "Configuration" 类型列表中选择 **Configuration**，然后单击 **List Objects**。
3. 单击 "End User Resources" 旁的 **Edit** 显示配置对象。
4. 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 3-14 所示。

图 3-14 最终用户资源配置对象



5. 单击 **Save**。

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。

关联和确认规则

当操作时没有可用的 Identity Manager 用户名来输入用户字段，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。

关联规则会查找与操作字段匹配的 Identity Manager 用户。确认规则会对照操作字段测试 Identity Manager 用户，以确定用户是否为匹配项。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。

通过分别创建子类型为 `SUBTYPE_ACCOUNT_CORRELATION_RULE` 或 `SUBTYPE_ACCOUNT_CONFIRMATION_RULE` 的规则对象来创建关联或确认规则。

有关关联和确认规则的详细信息，请参见 *Identity Manager 技术部署概述*中的“数据加载和同步”一章。

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。这些可查询属性被配置为 Identity Manager `UserUIConfig` 对象中的 `QueryableAttrNames`。

关联扩展属性需要特殊配置：

- 必须在 `UserUIConfig` 中将扩展属性指定为可查询 （添加到 `QueryableAttrNames` 列表）。
- 要使 `UserUIConfig` 的更改生效， Identity Manager 应用程序 （或应用服务器）可能需要重新启动。

确认规则

任意确认规则的输入如下：

- **`userview`** - Identity Manager 用户的完整视图。
- **`account`** - 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。

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。要启用此功能，请执行以下操作：

1. 登录到管理员界面。
2. 选择**配置**，然后选择**用户界面**。
3. 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，登录页面上现在会显示**请求帐户**按钮。

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。
- **需要隐私策略** - 如果选择此选项，用户必须先接受隐私策略才能请求帐户。默认情况下将启用此选项。
- **启用验证** - 如果选择此选项，用户必须先验证其雇员信息，然后才能请求帐户。默认情况下将启用此选项。
- **过程启动 URL** - 输入 URL，以指定要用于匿名注册过程的工作流。
- **启用通知** - 如果选择此选项，则为用户创建帐户之后，将向该用户发送通知电子邮件。
- **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，可以通过单击登录页面上的**请求帐户**来请求帐户。

Identity Manager 将显示第一个注册页面 （共两页），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

本章介绍使用 "Administrator Interface" 设置 Identity Manager 对象和服务器进程的信息和步骤。有关 Identity Manager 对象的详细信息，请参见 “概述”一章中的第 36 页上的 “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 13 章 “服务提供者管理”。

本章按以下主题进行组织：

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。

什么是角色？

Identity Manager 角色定义在其中管理帐户的资源的集合。使用角色可概要描述一类用户，从而将具有相似特征的 Identity Manager 用户划分为一组。

可将每个用户分配到一个或多个角色，或者不分配到角色。所有分配给某个角色的用户都共享访问相同基本资源组的权限。

所有与某个角色关联的资源都会*间接地*分配给相应用户。间接分配不同于*直接*分配，在直接分配中，资源是专为用户选定的。

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。

您可通过 "Administrator Interface" 的 "Create User" 和 "Edit User" 页将角色分配给用户。

创建角色

可以使用以下方法之一创建角色：

1. 在 Identity Manager 菜单栏中，选择 **Roles**。
2. 在 "Roles" 页中单击 **New**。

   "Create Role" 页允许您：

   - 将资源和资源组分配给角色。
   - 选择角色批准者和通知选项。

提示 要了解有关批准进程的详细信息，请参阅第 177 页上的“帐户批准”。

   - 排除角色。就是说，如果此角色被分配给某个用户，则排除的一个角色或多个角色不会被分配。
   - 选择可以分配此角色的组织。

- 编辑分配给此角色的资源的属性值。

编辑已分配的资源属性值

在 "Create Role" 页上的 "Assigned Resources" 区域中单击 **Set Attribute Values**，以显示分配给该角色的每个资源的属性列表。在此 "Edit" 属性页中，可以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；它还提供用于覆盖或合并现有值的一些选项。

选择以设置每个资源帐户属性的值：

- **值覆盖** - 选择以下选项之一：
  - **无** - 默认选项。不设置任何值。
  - **规则** - 使用规则设置值。如果选择此选项，则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，则必须输入文本。
- **设置方法** - 选择以下选项之一：
  - **默认值** - 将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。设置该值将覆盖任何用户更改。
  - **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。设置该值将覆盖任何用户更改。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。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。

    对于多值属性，必须编辑系统信息库中的角色对象，以指明它占据一个逗号分隔值 (Comma-separated Value, CSV) 字符串；例如：

    ```
    <RoleAttribute name='attrs role:Database Table:attrs' csv='true'>
    ```

  - **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。

单击**确定**可保存所作更改并返回到 “创建或编辑角色”页。

管理角色

可以从 "Roles" 页上的角色列表中对角色执行一系列操作。

- 编辑角色 - 在角色列表中选择角色，并在打开的页中修改角色的属性。
- 查找角色 - 在 “角色”区域中，选择**查找角色**。可按以下一种或多种搜索类型搜索角色：
  - 名称
  - 可用性
  - 批准者
  - 资源
  - 资源组

如果选择多种搜索类型，则搜索必须符合所有指定条件才能成功地返回结果。搜索不区分大小写。

- 克隆或重命名角色 - 选择要编辑的角色，在 “名称”字段中输入新名称，然后单击**保存**。在显示的页中，单击 **Create** 以创建新角色。

重命名角色

要重命名角色，请执行以下步骤：

1. 选择要编辑的角色。
2. 在 "Name" 字段中输入新名称，然后单击 **Save**。

   Identity Manager 将显示 "Create or Rename" 页。
3. 单击 **Rename** 以更改角色名称。

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。这适用于与任务一起创建的角色，同时也适用于现有的、与某个资源角色名匹配的 Identity Manager 角色。

在菜单栏中，选择 **Tasks**，然后选择 **Run Tasks** 选项卡，以访问 "Synchronize Identity System Roles with Resource Roles" 任务页。要启动任务，请指定同步任务的名称、资源、要使用的资源角色属性以及将应用角色的组织，然后单击 "Launch"。

配置 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 资源存储关于如何连接到在其中创建帐户的资源或系统的信息。Identity Manager 资源定义有关某个资源的相关属性，并帮助指定资源信息如何在 Identity Manager 中显示。

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 "Resources" 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 **Resources**。

资源按类型分组，它按照已命名的文件夹显示在列表中。要展开层次视图并查看当前已定义的资源，请单击文件夹旁的指示符。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

从资源列表中可以选择要创建的资源，而该列表可通过管理员界面的 "Resources" 选项卡进行管理。从 "Resource Type Actions" 选项列表中选择 "Configure Managed Resources"，以选择要用于填充资源列表的资源。

在 "Managed Resources" 页上， Identity Manager 将资源分为两类：

- **Identity Manager 资源** - 包含在此表中的资源通常是由 Identity Manager 管理的资源。该表显示了资源类型和版本。通过选择 "Managed?" 列中的选项来选择一个或多个资源，然后单击 **Save** 将其添加到资源列表。
- **自定义资源** - 使用此页面区域可以将自定义资源添加到 “资源”列表中。

要添加自定义资源：

1. 单击 **Add Custom Resource** 向表中添加一行。
2. 输入资源的资源类路径或输入您自定义创建的资源。
3. 单击 **Save** 将资源添加到 "Resources" 列表。

表 4-1 列出了自定义资源类。

表 4-1 自定义资源类

自定义资源	资源类
Access Manager	com.waveset.adapter.AccessManagerResourceAdapter
ACF2	com.waveset.adapter.ACF2ResourceAdapter
ActivCard	com.waveset.adapter.ActivCardResourceAdapter
Active Directory	com.waveset.adapter.ADSIResourceAdapter
Active Directory Active Sync	com.waveset.adapter.ActiveDirectoryActiveSyncAdapter
ClearTrust	com.waveset.adapter.ClearTrustResourceAdapter
DB2	com.waveset.adapter.DB2ResourceAdapter
INISafe Nexess	com.waveset.adapter.INISafeNexessResourceAdapter
Microsoft SQL Server	com.waveset.adapter.MSSQLServerResourceAdapter
MySQL	com.waveset.adapter.MySQLResourceAdapter
Natural	com.waveset.adapter.NaturalResourceAdapter
NDS SecretStore	com.waveset.adapter.NDSSecretStoreResourceAdapter
Oracle	com.waveset.adapter.OracleResourceAdapter
Oracle Financials	com.waveset.adapter.OracleERPResourceAdapter
OS400	com.waveset.adapter.OS400ResourceAdapter
PeopleSoft	com.waveset.adapter.PeopleSoftCompIntfcAdapter com.waveset.adapter.PeopleSoftComponentActiveSyncAdapter
RACF	com.waveset.adapter.RACFResourceAdapter
SAP	com.waveset.adapter.SAPResourceAdapter
SAP HR	com.waveset.adapter.SAPHRResourceAdapter
SAP Portal	com.waveset.adapter.SAPPortalResourceAdapter
Scripted Host	com.waveset.adapter.ScriptedHostResourceAdapter
SecurID	com.waveset.adapter.SecurIdResourceAdapter com.waveset.adapter.SecurIdUnixResourceAdapter
Siebel	com.waveset.adapter.SiebelResourceAdapter
SiteMinder	com.waveset.adapter.SiteminderAdminResourceAdapter com.waveset.adapter.SiteminderLDAPResourceAdapter com.waveset.adapter.SiteminderExampleTableResourceAdapter
Sun ONE Identity Server	com.waveset.adapter.SunISResourceAdapter
Sybase	com.waveset.adapter.SybaseResourceAdapter
Top Secret	com.waveset.adapter.TopSecretResourceAdapter

创建资源

可使用 *Resource Wizard* 创建资源。 "Resource Wizard" 将引导您完成创建 Identity Manager 资源适配器的过程，以管理资源上的对象。

使用 "Resource Wizard" 可以设置：

- **特定于资源的参数** - 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** - 包括用户的帐户名称语法，它对分层名称空间尤其重要。
- **Identity Manager 的资源参数** - 设置策略、建立资源批准者，并设置组织对资源的访问权限。

创建资源：

1. 从 "Resource Type Actions" 选项列表中选择 **New Resource**。

   Identity Manager 将显示 "New Resource" 页。

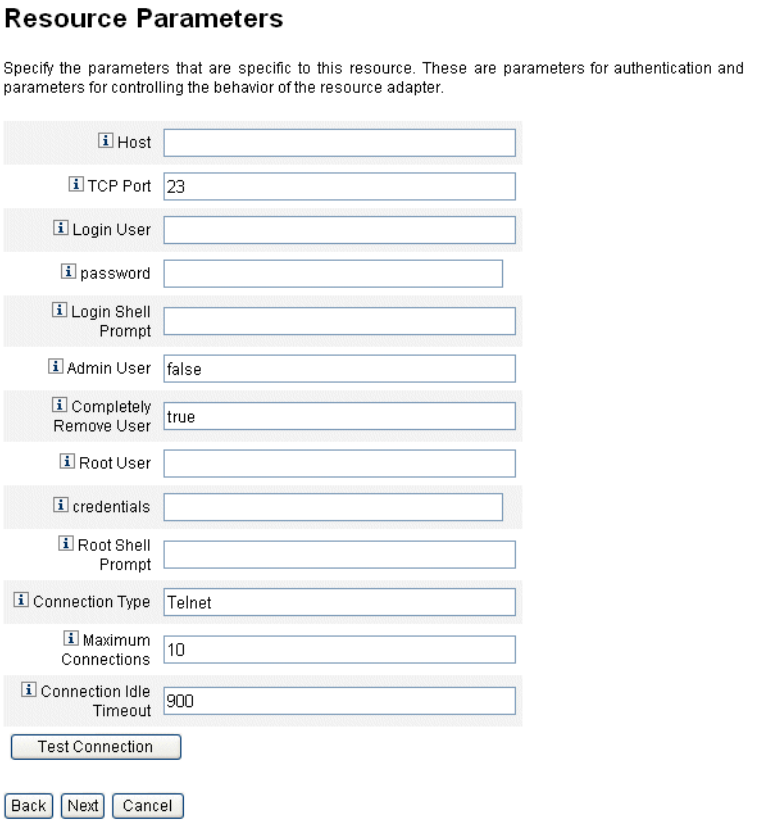
2. 选择资源类型，然后单击 **New**，以显示 "Resource Wizard Welcome" 页。

注 也可先从资源列表中选择资源类型，然后再从 "Resource Type Actions" 列表中选择 "New Resource"。在这种情况下， Identity Manager 不会显示 "New Resource" 页，而是直接启动资源向导。

---

3. 单击 **Next** 开始定义资源。 "Resource Wizard" 步骤和页面按以下顺序显示：
   - **资源参数** - 设置用于控制验证和资源适配器行为的特定于资源的参数。输入参数，然后单击 **Test Connection**，以确保连接有效。在确认连接有效后，单击 **Next** 设置帐户属性。图 4-1 显示了 "Resource Parameters" 页。

图 4-1 Resource Wizard：资源参数

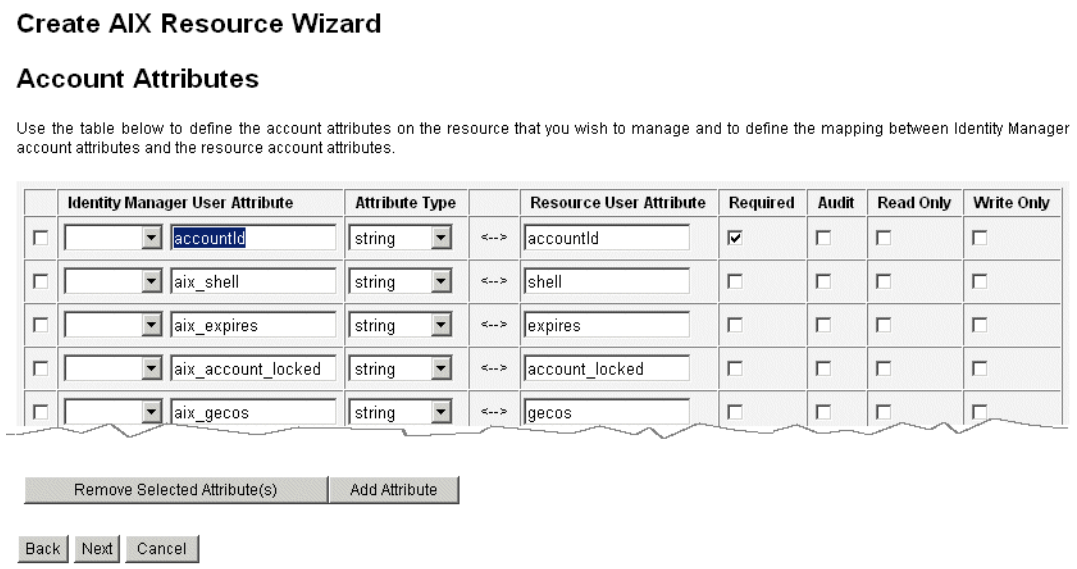


- **帐户属性（模式映射）-** 将 Identity Manager 帐户属性映射到资源帐户属性。

  要添加属性，请单击 **Add Attribute**。选择一个或多个属性，然后单击 **Delete Selected Attributes** 从模式映射中删除属性。完成后，单击 **Next** 设置身份模板。

  图 4-2 显示了 "Resource Wizard" 中的 "Account Attributes" 页。

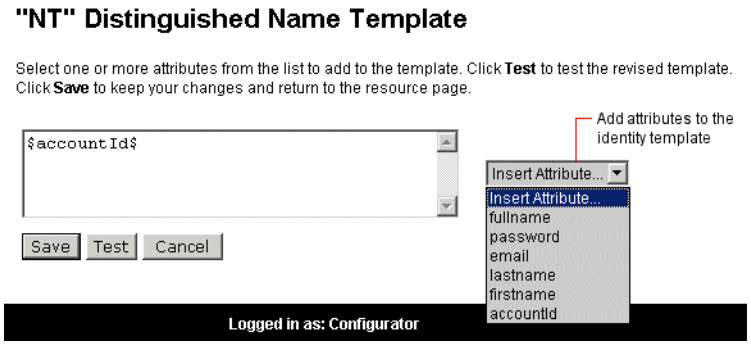
图 4-2 Resource Wizard：Account Attributes （模式映射）



- **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。

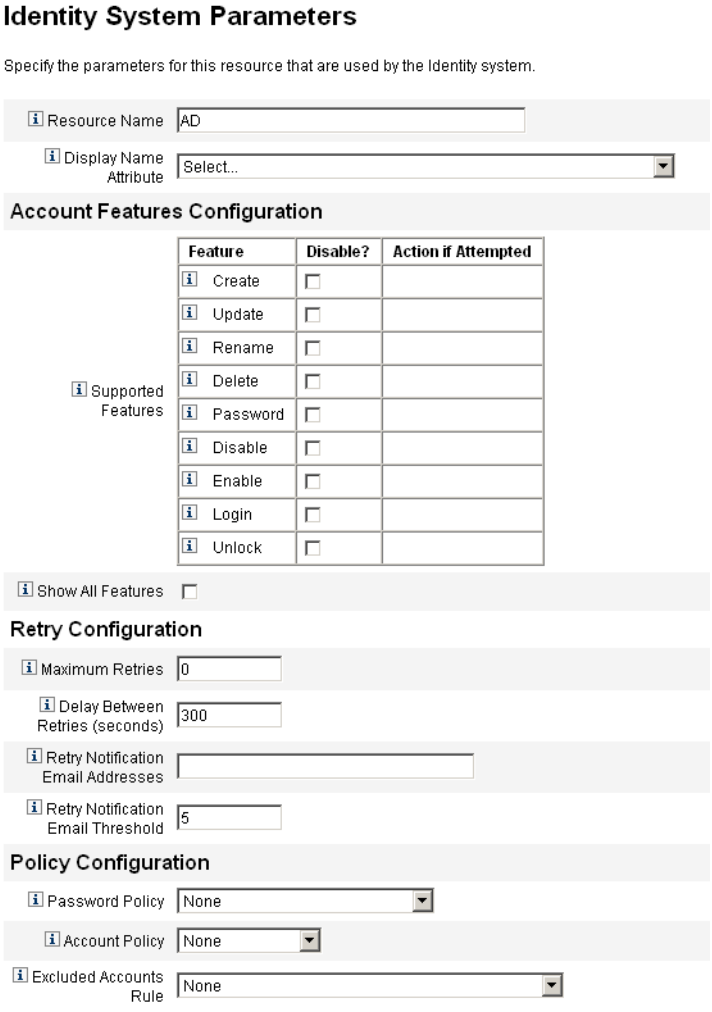
  从 "Insert Attributes" 列表中选择属性。要从模板中删除属性，请在列表中单击，然后从信息串中删除一个或多个项目。删除属性名称以及前导和后续的 $ （美元符号）字符。

图 4-3 资源向导：身份模板



- **Identity System 参数** - 为资源设置 Identity Manager 参数，包括重试和策略配置，如图 4-4 中所示。

图 4-4 资源向导：Identity 系统参数



使用 **Next** 和 **Back** 在页间移动。完成所有选择后，单击 **Save** 以保存该资源，并返回至列表页。

管理资源

可以通过资源列表在资源上执行一系列编辑操作。除了在每个 "Resource Wizard" 页上编辑权能外，还可以：

- **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 **Rename**。
- **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。

使用帐户属性

Identity Manager 资源使用模式映射定义来自外部资源的属性 （*资源帐户属性*）的名称和类型；然后它们将上述属性映射到标准 Identity Manager 帐户属性。通过建立模式映射 （在 "Resource Wizard" 的 "Account Attributes" 页上），可以：

- 仅将资源属性限制在公司需要的范围内。
- 创建与多个资源共用的公共 Identity Manager 属性名称。
- 标识所需用户属性和属性类型。

要访问这些值，请从资源列表中选择资源，然后从 "Resource Actions" 列表中选择 **Edit Resource Schema**。

模式映射的左列（标题为 "Identity system User Attribute"）包含 Identity Manager 帐户属性的名称，这些名称由 Identity Manager 的管理员界面和用户界面中使用的表单所引用。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。

通过定义 Identity System 属性名称，来自不同资源的属性可以用公共名称定义。例如，在 Active Directory 资源上， Identity Manager 中的 `lastname` 属性被映射到 Active Directory 资源属性 `sn`；在 GroupWise 上， `fullname` 属性可以被映射到 GroupWise 属性 `Surname`。这样，管理员仅需要填写一次 `lastname` 的值；当保存用户后，该值将传递给具有不同名称的资源。

资源组

使用资源区域还可以管理资源组，使您可以对资源进行分组，以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 5.5 资源依赖于现有的 Windows NT 或 Windows Active Directory 帐户：在可以成功创建 Exchange 帐户之前，其中之一必须存在。通过使用 Windows NT 资源和 Exchange 5.5 资源 （按顺序）创建资源组，可以确保创建用户时的顺序正确。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 **Resources**，然后选择 **List Resource Groups** 以显示当前定义的资源组列表。在该页单击 **New** 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

可以在资源的全局资源策略中编辑属性。在 "Edit Global Resource Policy Attributes" 页中，可以编辑以下策略属性：

- **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。**None** 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。 **None** 是默认选项。

必须单击 **Save** 才能保存对策略所做的更改。

设置其他超时值

通过编辑 Waveset.properties 文件可以修改 `maxWaitMilliseconds` 属性。`maxWaitMilliseconds` 属性将控制监视操作超时的频率。如果未指定此值，则系统将使用默认值 50。

要设置此值，请将以下行添加到 Waveset.properties 文件：

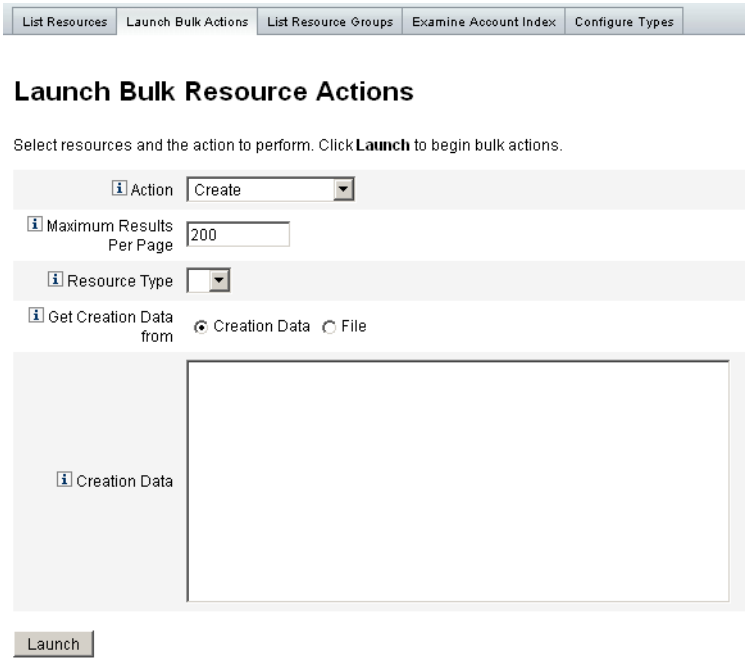
```
com.waveset.adapter.ScriptedConnection.ScriptedConnection.maxwaitMilliseconds。
```

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 4-5 显示了使用创建操作的批量操作的启动页。

图 4-5 "Launch Bulk Resource Actions" 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 **From Action List** 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："Create"、"Clone"、"Update"、"Delete"、"Change Password" 和 "Reset Password"。

  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 "Create" 操作，您需要指定资源类型。

  如果指定 "From Action List"，请使用 **Get action list from** 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 **Launch** 以启动操作，该操作将作为后台任务运行。

Identity Manager ChangeLog

阅读本节中有关 Identity Manager ChangeLog 功能的信息以及有助于配置和使用 ChangeLog 的过程。

什么是 ChangeLog？

通过 *ChangeLog* 可以查看 Identity Manager 资源中包含的身份属性信息。每个 ChangeLog 都定义为捕获对身份属性子集的更改。

随着资源中属性数据的更改，活动同步适配器将捕获信息，然后将更改写入 ChangeLog。然后，专为与企业资源进行交互而开发的自定义脚本将读取 ChangeLog 并更新资源。

使用 ChangeLog 可以间接与来自置备系统的资源进行通信 （通过自定义脚本），因此 ChangeLog 功能与 Identity Manager 的标准资源活动同步和协调功能有所不同。

ChangeLog 与安全

Identity Manager 的 ChangeLog 功能需要本地文件系统中指定目录的写入权限。默认情况下，某些 Web 容器不允许本地文件系统访问其托管的 Web 模块（如 Identity Manager）。

可以通过编辑 Java 策略文件来授予访问权限。如果将 `/tmp/changelogs` 用作目录，策略文件应该包含：

```
grant {
    permission java.io.FilePermission "/tmp/changelogs/*",
"read,write,delete";
};
```

必须为指定的每个 ChangeLog 目录定义文件权限。

默认的 Java 安全策略文件位于：

```
$JAVA_HOME/jre/lib/security/java.policy
```

编辑该文件可能就已足够；但是，如果使用自己的文件（而非默认文件），则服务器运行时将使用诸如以下所示的选项：

```
-Djava.security.manager -Djava.security.policy=/path/to/your/java.policy
```

在这种情况下，编辑由 `java.security.policy` 系统属性标识的文件。

注 可能需要在编辑安全策略文件后重新启动 Web 容器。

ChangeLog 功能要求

ChangeLog 功能要求先配置身份属性再配置 ChangeLog。

注 完成第 118 页上的“配置身份属性和事件”一节中所述的步骤可以满足这些要求。

配置 ChangeLog

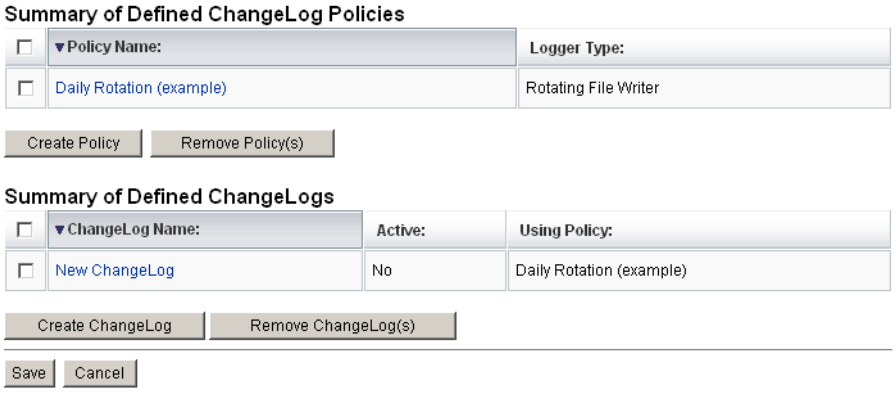
可以通过创建 ChangeLog 策略和 ChangeLog 来配置 ChangeLog。每个 ChangeLog 都必须具有相关的 ChangeLog 策略。ChangeLog 定义更改子集，其中的更改由活动同步检测到并通过身份属性来推送，应写入日志。其相关的 ChangeLog 策略定义应该如何写入 ChangeLog 文件。 ChangeLog 文件将由自定义脚本使用。

要配置 ChangeLog 和 ChangeLog 策略，请选择 **Meta View**，然后选择 **ChangeLogs**。

Identity Manager 将显示 "ChangeLog Configuration" 页，其中有两个摘要区域。

注 如果尚未配置身份属性，则 "ChangeLogs" 选项卡不可见。

图 4-6 ChangeLog 配置



ChangeLog 策略摘要

ChangeLog 策略摘要区域显示当前已定义的 ChangeLog 策略。要编辑现有 ChangeLog 策略，请在列表中单击相应的策略名称。要创建 ChangeLog 策略，请单击 **Create Policy**。

要删除一个或多个 ChangeLog 策略，请在列表中选择相应的策略，然后单击**删除策略**。（此操作不需要确认。）

ChangeLog 摘要

ChangeLog 摘要区域显示当前已定义的 ChangeLog。要编辑现有 ChangeLog，请在列表中单击相应的 ChangeLog 名称。要创建 ChangeLog，请单击**创建 ChangeLog**。

要删除一个或多个 ChangeLog，请在列表中选择相应的 ChangeLog，然后单击 **Remove ChangeLog**。（此操作不需要确认。）

保存对 ChangeLog 配置的更改

必须在 “ChangeLog 配置”页中保存对 ChangeLog 配置（即 ChangeLog 策略或定义的 ChangeLog）进行的所有更改。单击 **Save** 以保存更改并返回至元视图。

创建和编辑 ChangeLog 策略

在 "Edit ChangeLog Policy" 页上输入内容或进行选择，可以创建或编辑 ChangeLog 策略：

- **策略名称** - 输入策略的唯一名称。
- **每日开始时间** - 设置每日时间，用于计算应该开始或变换轮转的时间。使用该策略的 ChangeLog 将从此时间开始，依据从此时间计算的增量进行轮转。例如，如果开始时间设置在午夜 (00:00)，"Rotations Per Day" 为 3，则日志文件的前缀将在 00:00、 08:00 和 16:00 发生变化。

  系统将按以下模式命名文件：`cl_User_yyyyMMddHHmmss.n.suffix`，其中 *HHmmss* 是轮转最近一次开始的时间。（*n* 是序列号，*suffix* 是在 ChangeLog 定义中提供的后缀。）

  在使用 "00:00" 作为开始时间并使用 3 作为轮转次数的情况下，如果在 9:24 a.m. 激活 ChangeLog，那么得到的轮转名称中将包含最近一次轮转开始的时间 （例如 08:00）。在这种情况下，文件名将以 `cl_User_yyyyMMdd080000` 开头。新轮转（文件名的新前缀）将在 16:00 开始。
- **每天轮转次数** - 指定每天要轮转日志的次数。例如，如果要每隔 4 小时轮转一次，请输入值 6。

  此值只能为非负整数。值 0 表示忽略此字段。如果此字段的值不是零，则会忽略 `"Maximum Age of a Rotation"` 设置。

  如果以秒为单位指定轮转的时间，并且 `"Rotations Per Day"` 字段的值为 0，则轮转时间值将用于确定轮转的周期。

  此值只能为非负整数。如果在 `"Rotations Per Day"` 字段中指定了非零值，则会使用该值 （不会使用轮转时间值）。如果这两个字段的值都为 0，则仅应用序列信息。（这种情况下甚至不使用 `"Daily Start Time"` 的值。）
- **保留轮转数** - 指定在 Identity Manager 删除轮转前允许累积的轮转次数。例如，如果每天轮转 3 次，并且要在日志中保存 2 天的更改，请指定值 6。
- **最大文件大小 （字节）** - 如果将更改写入当前文件会导致文件大小超过此限制，则会创建新的日志文件 （具有相同的轮转前缀，但具有新的序列号）。值 0 表示不使用该限制。所有非零限制字段 （大小、行数、使用期限）都将被使用；但是，系统将先检查此限制再检查其他限制。
- **最大文件大小 （行）** - 如果写入更改会使当前文件的行数超出此限制，则会创建新的序列文件，超出的行将写入新文件。值 0 表示*无限制*。系统将在大小限制后和使用期限限制前检查此限制。

- **最长文件使用期限 （秒） -** 当收到更改而现有序列文件存在的时间又超过此处指定的秒数时，将在写入更改之前创建新的序列文件。值 0 表示不使用该限制。在应用该限制之前，将首先应用其他非零限制。

单击**确定**可返回到 “ChangeLog 配置”页。必须在配置页中单击 "OK" 才能保存新 ChangeLog 策略或对现有策略的更改。

创建和编辑 ChangeLog

在 "Edit ChangeLogs" 页中输入内容和进行选择，可以创建或编辑 ChangeLog：

- **ChangeLog 名称** - 输入 ChangeLog 的唯一名称。
- **活动** - 如果选择此选项，则 ChangeLog 将在更改通过活动同步资源并进入身份属性时监视并写入更改 （必须将活动同步作为身份属性应用程序，才能执行此操作）。
- **过滤器** - 输入要使用的 ChangeLog 过滤器的名称。 `Noop` 表示使用默认过滤器，即接受所有更改。对于大多数情况，该过滤器应是足够的。否则，必须指定一个实现 `com.sun.idm.changelog.ChangeLogFilter` 的 Java 类。该类必须位于服务器的类路径中，而且必须具有公共默认构造函数。
- **记录这些操作** - 记录选定类型的事件，包括创建、更新和删除。未选定的事件将被忽略。
- **ChangeLog 视图** - 使用此表定义 ChangeLog 的内容 （列）。该表中的每行都指定 ChangeLog 中的一列。单击 **Add Column** 添加 ChangeLog 列。每列都具有名称、类型和身份属性名称。此表中行的顺序表示 ChangeLog 中列的顺序。定义列之后，可以使用 **Up** 和 **Down** 按钮对列进行排序。

注 在每个 ChangeLog 中名为 `changeType` 的表内，第一列都是隐藏的。该隐式首列表示更改的类型。此列的类型为 "Text"。日志中的数据将是以下值之一：`ADD`、 `MOD` 或 `DEL`。

- **使用已命名的策略** - 从列表中选择用于日志记录的已定义 ChangeLog 策略。
- **输出路径** - 输入文件系统中目录的名称，该目录中将包含日志文件。该路径可以是网络安装位置，但最好使用服务器本地目录。建议仅在每个位置只存储一个 ChangeLog。
- **后缀** - 输入用于 ChangeLog 文件的后缀 （例如， `.csv`）。选定的后缀可以用来将这些文件与其他 ChangeLog 文件区分开。

单击**确定**可返回到 “ChangeLog 配置”页。必须在配置页中单击 "OK" 才能保存新 ChangeLog 或对现有 ChangeLog 的更改。

示例

以下示例详细说明了如何设置身份属性和用于捕获属性数据特定集的 ChangeLog。

示例：定义身份属性

在此示例中，两个 Identity Manager 资源 （资源 1 和资源 2）向第三个资源 （资源 3）提供源数据。资源 3 未与 Identity Manager 系统直接连接。需要建立一个 ChangeLog，以便从资源 1 和资源 2 送往资源 3 的数据中拉取并维护一个数据子集。

```
资源 1: EmployeeInfo
employeeNumber*
givenname
mi
surname
phone

资源 2: OrgInfo
employeeNum*
managerEmpNum
departmentNumber

资源 3: PhoneList
empId*
fullname
phone
department
```

注 * 表示用于关联记录的关键字。

下表定义了身份属性。

表 4-2 用于使用更改日志示例的身份属性

属性	<==	From Resource.Attribute
employee	<==	EmployeeInfo.employeeNumber
dept	<==	OrgInfo.departmentNumber
reportsTo	<==	OrgInfo.managerEmpNum
firstName	<==	EmployeeInfo.givename

表 4-2 用于使用更改日志示例的身份属性 *（续）*

属性	<==	From Resource.Attribute
lastName	<==	EmployeeInfo.surname
middleInitial	<==	EmployeeInfo.mi
fullname	<==	firstName + " " + middleInitial + " " + lastName
phoneNumber	<==	EmployeeInfo.phone

示例：配置 ChangeLog

在定义身份属性之后定义名为 PhoneList ChangeLog 的 ChangeLog。该 ChangeLog 用于将身份属性子集写入 ChangeLog 文件。

PhoneList ChangeLog 中的 ChangeLogView

列名称	类型	身份属性
empId	文本	employee
fullname	文本	fullname
phone	文本	phoneNumber

资源 1 或资源 2 中的记录发生更改时，系统会将 ChangeLog 记录（来自身份属性的所有数据）的整个数据集合 （不只是更改）写入该 ChangeLog。自定义脚本将读取该信息并用其填充资源 3。

ChangeLog 中的 CSV 文件格式

对于 ChangeLog 写入的以逗号分隔值 (Comma-separated Value, CSV) 文件，阅读本节可以了解有关其格式的信息。

请考虑由行和列构成的 ChangeLog 文件，如电子表格或数据库表。每“行”就是文件中的一行。

ChangeLog 格式使用前两行描述其自身。这两行共同定义“模式”，即表中每个“单元”（行中逗号之间的值）的逻辑名称和逻辑类型。

第一行指定文件中属性的名称。第二行描述属性值的类型。其他行显示更改事件的所有数据。

ChangeLog 文件以 Java UTF-8 格式编码。

列

文件中的第一列具有特殊意义。此列用于定义操作类型；例如，更改事件是创建操作、修改操作还是删除操作。该列的名称始终为 changeType，类型始终为 T （表示文本）。其值为以下值之一：ADD、 MOD 或 DEL。

仅有一列中应显示条目的唯一标识符 （主关键字），通常为文件中的第二列。

其他列仅用于命名属性。该名称是取自 ChangeLog 视图表内的列名称值。

行

除定义文件*模式*的前两个标题行外，其余的行都显示属性的值。这些值按第一行中的列顺序显示。 ChangeLog 从身份属性应用，因而包含在删除更改时有关用户的所有已知数据。

此外，其中没有表示 null （或未设置）的特殊标记值。如果检测到更改时没有发现值， ChangeLog 将写入一个空字符串。

值根据文件第二行指定的列类型编码。支持的类型包括：

- T：文本
- B：二进制
- MT：多文本
- MB：多二进制

文本值

文本值以字符串的形式写入，有两种例外：

- 如果值包含 ,（逗号），则 Identity Manager 将通过插入 \ （反斜杠）字符对值中的逗号进行转义。例如，如果 fullname 的值是 Doe, John，则 Identity Manager 写入的值将是
  Doe \,John。
- 如果值包含 \ （反斜杠）字符，则 Identity Manager 将通过添加另一个 \ 对其进行转义。例如，如果 homedir 的值包含 C:\users\home，则 Identity Manager 写入日志的值将是 C:\\users\\home。

文本值不能包含换行符。如果文件需要换行符，请使用二进制值类型。

二进制值

二进制值以 Base64 编码。

多文本值

多文本值的写入方式类似于文本值，但这种值以逗号分隔，两侧有方括号 （使用 [和] ）。

多二进制值

多二进制值的写入方式类似于二进制值（以 Base64 编码），但这种值也以逗号分隔，两侧有方括号 （使用 [和] ）。

格式设置示例

以下示例说明了各种输出格式。每个示例的格式如下：

```
column1,column2,column3,column4
```

每个示例的第 3 列显示示例文本。

- 文本 (T) 数据在文件中显示为字符串：

  ```
  ADD,account0,一些文本数据,column4
  ```

- 二进制 (B) 数据显示为 base64 编码格式。

  ```
  ADD,account0,FGResWE23WDE==,column4
  ```

- 多文本 (MT) 的显示格式如下：

  ```
  ADD,account0,[一,二,三],column4
  ```

- 多二进制 (MB) 的显示格式如下：

  ```
  ADD,account0,[FGResWE23WDE==,FGRCAFEBADE3sseGHSD],column4
  ```

注 Base64 字母表中不包括 , （逗号）、[（左方括号）、] （右方括号）字符或换行符。

ChangeLog 文件名

文件名的格式如下：

```
servername_User_timestamp.sequenceNumber.suffix
```

其中：

- *timestamp* 是开始使用或轮转使用此日志的时间。将具有相同时间戳的文件视为一个*轮转*。

- *sequenceNumber* 是一种单调递增的值，用于将轮转拆分成文件子集，这些文件受字节数上限、行数或秒数的限制。这些文件中的每个文件都称为一个*序列*文件。
- *suffix* 是在 ChangeLog 配置中定义的文件扩展名，通常是 `.csv`。

配置轮转和序列

轮转和序列在 `ChangeLogPolicy` 对象中定义，从 ChangeLog 中引用。

示例

某项策略将如下定义轮转：

- 从上午 7:00 开始。
- 每天轮转 3 次，持续两天

该策略产生的文件名类似于以下名称。（其中每次轮转中都有两个序列文件。）

```
myServer_User_20060101070000.1.csv
myServer_User_20060101070000.2.csv
myServer_User_20060101150000.1.csv
myServer_User_20060101150000.2.csv
myServer_User_20060101230000.1.csv
myServer_User_20060101230000.2.csv

myServer_User_20060102070000.1.csv
myServer_User_20060102070000.2.csv
myServer_User_20060102150000.1.csv
myServer_User_20060102150000.2.csv
myServer_User_20060102230000.1.csv
myServer_User_20060102230000.2.csv
```

可见， 1 月 1 日有 3 次轮转，每次间隔 8 小时，从 07:00:00 开始。 1 月 2 日 与此类似，仅名称中与日 (20060102) 对应的部分不同。

编写 ChangeLog 脚本

阅读本节可以了解有关有助于编写 ChangeLog 脚本的信息。

- 脚本很可能会持续运行，等待新数据、新文件或在无活动时休眠；然后只是读取文件并将每行的更改应用于后端资源。
- ChangeLog 支持删除操作；但 `DEL` 行中将只包括 `accountId` 值。
- 使用轮转和序列可以确定运行脚本的频率。例如，可以指定：
  - 在午夜轮转；在首次轮转后，每晚都对上一次轮转运行脚本。

- 每 4 小时轮转一次，从上午 8:00 开始，然后每 4 小时运行一次脚本 （在 8 点、 12 点、 16 点、 20 点、 24 点、 4 点……）
- 在不轮转的情况下运行脚本，使脚本在序列号突变时读取序列文件。可以控制序列号增大的方式；可以通过大小、数值运算或时间来控制。

- 可以将每个 ChangeLog 都视为表示后端系统中的记录。为便于脚本读取日志，Identity Manager 始终写入给定记录的所有数据 （不论其是否已更改）。脚本可以 “盲目”地在记录中应用数据。

  但它们需要确保后端资源 （或脚本）可以进行以下两种操作之一 （尤其是对于 `ADD` 和 `DEL`）：

  - 以幂等方式应用数据。（*幂等*表示，如果重复应用数据，则不会产生任何效果。）如果脚本从头至尾读取两次 ChangeLog，则资源中数据记录的状态在每次读取后将完全相同。
  - 最多应用一次数据。例如，对于添加和删除操作，如果资源无法实现幂等，则脚本必须通过仅读取一次日志条目或跟踪其进度确保仅应用一次更改。

- 一种可取的方法可能是待序列文件出现后应用先前的文件。例如，在 .2 文件出现后应用 .1 文件。在 .3 文件出现后，应用 .2。应用文件后，请记录您已对磁盘进行此操作。通过这种方法可以避免使用 `fstat` 或 `tail -f` 等调用。

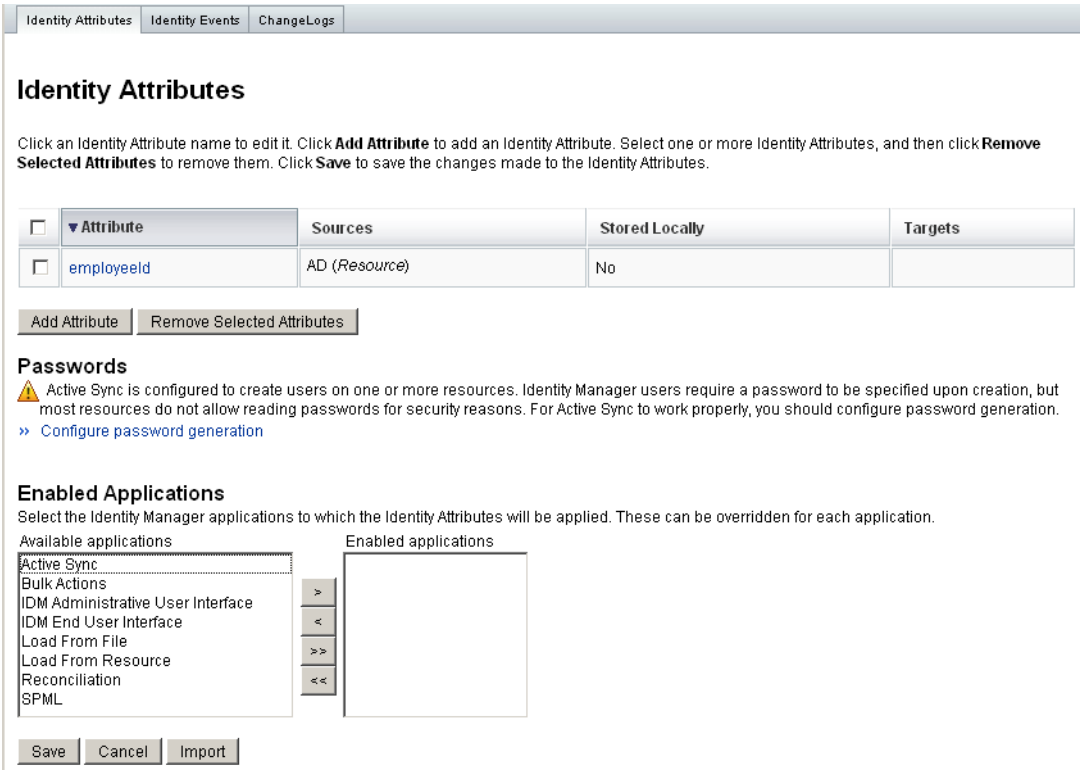
配置身份属性和事件

可以使用管理员界面的 "Meta View" 区域配置身份属性和事件。使用以下各节中的信息和步骤可以配置 Identity Manager 身份属性和身份事件，以及选择要应用属性和事件的 Identity Manager 系统应用程序。

使用身份属性

要配置身份属性，请选择 **MetaView**，然后选择 **Identity Attributes**。将显示 "Identity Attributes" 页。下图显示了此页的示例。

图 4-7 在 "Meta View" 中配置 "Identity Attributes"



要添加身份属性，请单击 **Add Attribute**。添加到列表后，可以通过在列表中单击身份属性名称来对其进行编辑。要删除一个或多个身份属性，请选择相应的身份属性，然后单击**删除选定属性**。

可以选择一个或多个要添加到属性或从属性中删除的响应。

在单击 **Save** 后，操作才会生效。

如果自上次修改身份属性之后，资源已更改，则 "Identity Attributes" 页将显示以下警告消息（图 4-8）。单击警告消息中的 **Configure the Identity Attributes from resource changes** 以同化更改。

图 4-8 "Resources Have Changed" 警告消息

密码

配置活动同步，以在一个或多个资源上创建用户。Identity Manager 用户需要在创建时指定密码，但出于安全原因，多数资源不允许读取密码。如果尚未设置密码生成，请单击 **Configure password generation**。

选择如何设置身份用户以及通过活动同步创建的其他资源帐户的密码：

- **使用默认密码** - 选择此选项，然后输入密码。 password.password 身份属性将通过此值设置用户密码。
- **Use rule to generate password** - 选择此选项以选择密码生成使用的规则。`password.password` 身份属性将使用选定的规则生成密码。
- **Use Identity System Account Policy password generation** - 选择此选项以选择密码生成使用的策略。选择此选项会将 `waveset.assignedLhPolicy` 身份属性设置为选定的策略。如果未配置选定的策略以生成密码，并且您具有创建和修改策略所需的权限，则页面将重新显示其他选项，通过这些选项您可以创建策略的副本或修改现有策略。

  此选项将基于为 Identity System 帐户策略配置的密码策略生成随机密码。由于该选项可随机生成密码，因此是最安全的密码生成选项。

选择应用程序

使用 "Enabled Applications" 区域选择要应用身份属性的 Identity System 应用程序。从 “可用应用程序” 区域选择一个或多个应用程序，然后将其移至 “已启用的应用程序” 区域。在单击 **Save** 后，操作才会生效。

注 要使用 ChangeLog 功能，必须启用活动同步应用程序。有关更多信息，请参见第 196 页上的 “活动同步适配器”。

添加和编辑身份属性

在 "Add Identity Attributes" 页或 "Edit Identity Attributes" 页中，进行以下选择以添加或编辑身份属性：

- **属性名称** - 选择或输入属性名称。从所提供的默认值中进行选择 （从资源模式映射条目、可操作的身份属性和用户扩展的属性中选择）；或在文本框中输入值。
- **源** - 选择一个或多个源，用于填充此身份属性的值。将按顺序对源进行评估，然后将身份属性设置为第一个非 null 值。
  - **资源** - 该值来自所选资源的选定属性。
  - **规则** - 该值是根据对选定规则的评估而得到的。
  - **常量** - 将该值设置为提供的常量值。

  单击 +（加号）可以添加新行，以选择另一个源。单击源旁边的 -（减号）可以将其删除。要对源重新排序，请单击箭头以在列表中上移或下移它们。
- **属性特性** - 使用此区域可指定身份属性的属性设置。
  - **身份属性的设置方法** - 选择以下选项之一可指定 Identity Manager 将如何在资源上设置属性值：
    - **设置成值** - 在所有目标上强制设置身份属性的值。如果选择此选项，由源确定的值将覆盖用户在表单中输入的任何值，以及在表单、工作流、规则或角色中所设置的值。对于典型实现，此选项是适当的设置。

      有关身份属性的其他信息，请参见 *Identity Manager 技术部署概述*。
    - **默认值** - 仅在目标上未设置属性值时才设置值。
    - **与值合并** - 将值添加到现有值。重复的值将被过滤掉。
  - **将属性存储在 IDM 系统信息库中** - 选择此选项可以在本地将身份属性存储在 Identity System 系统信息库中。如果要对身份属性强制存储 Identity System 用户，或者需要该属性能够处理查询，请选择此选项。
  - **在所有分配的资源上设置值** - 如果要以全局方式对所有支持此属性的已分配资源设置身份属性，请选择此选项。
- **目标** - 选择将设置此身份属性的目标资源。如果未指定目标，则单击 **Add Target**。要从列表中删除目标，请选择相应目标，然后单击 **Remove Selected Targets**。

  单击 **OK** 添加身份属性并返回至 "Identity Attributes" 页。必须单击 "Identity Attributes" 页中的 **Save** 才能保存添加的身份属性。

添加目标资源

如果仅将身份属性用于 ChangeLog，则不必为身份属性设置目标。例如，如果要使用 ChangeLog，但还要使用标准的 “输入表单”来通过活动同步推送数据，则可以为身份属性设置目标。如果没有任何目标，则 MetaView 将仅计算身份属性的值，而不会对任何其他资源设置这些值。

进行选择以添加要设置身份属性的目标资源：

- **目标资源** - 选择将设置选定身份属性的目标资源。
- **目标属性** - 选择将接收该值的目标资源属性的名称。
- **条件** - 选择要运行的规则，此规则用于确定是否要对此目标资源设置选定的身份属性。该规则应返回值 True 或 False。如果未设置条件，则始终会对选定的事件类型设置目标属性。
- **应用到:** - 选择事件类型，将针对这些类型对此目标资源设置选定的身份属性。将结合这些选择与 “条件”来确定是否应设置目标属性。

  单击 **OK** 以添加目标资源并返回至 "Add Identity Attribute" 页或 "Edit Identity Attribute" 页。

删除目标资源

要删除一个或多个目标资源，请在列表中选择相应目标资源，然后单击 **Remove Selected Targets**。

导入身份属性

使用 “导入身份属性”功能，您可以选择一个或多个表单来导入和填充身份属性值。Identity Manager 将分析导入的表单值并对身份属性做出最佳猜测；但是，导入后，可能需要编辑身份属性。

请选择以下导入项目：

- **与现有身份属性合并** - 如果选择此选项，Identity Manager 会将导入的值与现有身份属性合并。如果未选择此选项，则会先清除身份属性再进行导入。
- **要导入的表单** - 从 “可用表单”区域中选择一个或多个表单以填充身份属性。

  单击 **Import** 以导入表单。“身份属性”页将显示新的或合并后的身份属性。

  单击 **Save** 以保存对身份属性的更改。

注 如果需要更正身份属性条件， Identity Manager 将显示一个警告页，列出一条或多条警告。单击 **OK** 可以返回至 "Configure" 区域。

配置身份事件

还可以为由 Identity Manager 管理的资源配置身份事件，以定义在这些资源上发生的事件的行为。在身份事件中定义的行为将在活动同步期间使用，以确定事件发生的时间，并执行相应操作以对该事件做出响应。

例如，您可以配置身份事件，以检测用于触发要删除的身份用户和所有其他资源帐户的授权人力资源 (Human Resources, HR) 系统上的删除，并对其做出响应。

要配置身份事件，请选择 **MetaView**，然后选择 **Identity Events** 选项卡。在 "Identity Events" 页上，单击 **Add Event** 并指定事件类型。还可以通过选择 "Identity Event" 页上的事件并指定以下选项来编辑身份事件。

- **事件类型** - 选择 “删除”、“启用”或 “禁用”以指定要配置的身份事件类型。
- **源** - 选择要应用身份事件的资源 （例如，对于 Active Directory 为 AD）。如果资源需要事件检测规则来检测和响应事件 （因为其不具有本机支持），请在 **determined by** 字段中选择规则。可以添加和删除资源。
- **响应** - 从 “响应”列表中选择响应，或单击**添加响应**以添加响应 （如果未定义任何响应）。要从选择列表中删除响应，请选择相应响应，然后单击 **Remove Selected Responses**。

完成选择后，单击 **OK**。

配置 Identity Manager 策略

阅读本节可以了解配置用户策略的信息和步骤。

什么是策略？

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

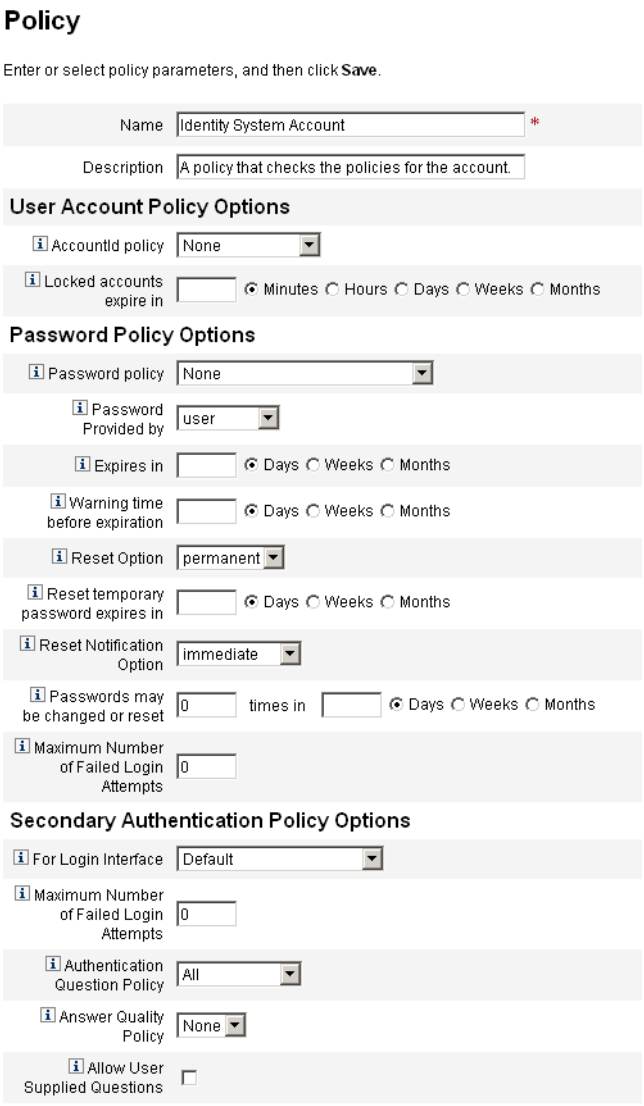
注 Identity Manager 还提供专用于审计用户遵循性的审计策略。第 11 章 “身份审计”中对审计策略进行了论述。

可在 "Policies" 页中创建和编辑 Identity Manager 用户策略。在菜单栏中选择 **Security**，然后选择 **Policies**。在显示的列表页中，可以编辑现有策略和创建新的策略。

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限制。通过 "Create Organization" 和 "Edit Organization" 页以及 "Create User" 和 "Edit User" 页，可以将 Identity System 帐户策略 （在图 4-9 中显示）分配给组织或用户。

图 4-9 Identity Manager 策略

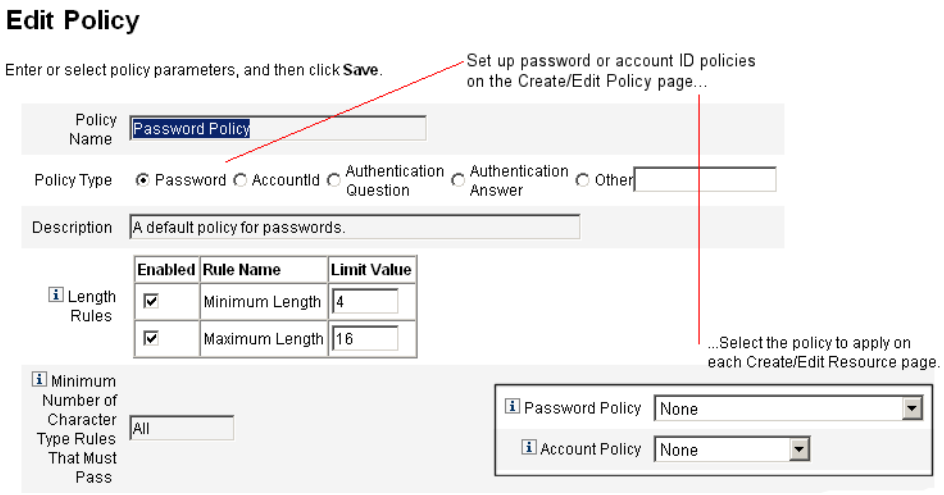


可以设置或选择的选项包括：

- **用户策略选项** - 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置选项。
- **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。

- **SPE 系统帐户策略** - 此策略类型在服务提供者实现中使用，为服务提供者用户建立用户、密码和验证策略选项及限制。通过 "Create Organization" 和 "Edit Organization" 页以及 "Create SPE User" 和 "Edit SPE User" 页，可将策略分配给组织或用户。
- **字符串质量策略** - 字符串质量策略包括密码、帐户 ID、验证等策略类型，可以设置长度规则、字符类型规则，还可以设置允许的字词和属性值。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。图 4-10 提供了一个示例。

图 4-10 创建/编辑密码策略



可以为密码和帐户 ID 设置的选项和规则包括：

- **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。

策略中不得包含属性

可在 UserUIConfig 配置对象中更改允许的 “不得包含”属性集。UserUIConfig 中列出的属性如下：

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

字典策略

字典策略使 Identity Manager 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。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" 页上的 "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

请按照以下步骤操作：

1. 在菜单栏中选择 **Configure**，然后选择 **Policies**。

2. 单击 **Configure Dictionary** 显示 "Dictionary Configuration" 页。
3. 选择并输入数据库信息：
    - **数据库类型** - 选择用于存储字典的数据库类型 （Oracle、 DB2、 SQLServer 或 MySQL）。
    - **主机** - 输入数据库正在其中运行的主机的名称。
    - **用户** - 输入连接到数据库时使用的用户名。
    - **密码** - 输入连接到数据库时使用的密码。
    - **端口** - 输入数据库正在侦听的端口。
    - **连接 URL** - 输入连接时使用的 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** - 输入与数据库交互时使用的 JDBC 驱动程序类。
- **数据库名称** - 输入将要加载字典的数据库的名称。
- **字典文件名** - 输入加载字典时使用的文件名。

4. 单击 **Test** 以测试数据库连接。
5. 如果连接测试成功，请单击 **Load Words** 以加载字典。加载任务可能需要几分钟才能完成。
6. 单击 **Test** 以确保正确加载字典。

实现字典策略

从 Identity Manager 策略区域实现字典策略。在“策略”页中单击以编辑密码策略。在 “编辑策略”页中，选择 “根据字典的词检查密码”选项。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 "Create Role" 或 "Edit Role" 页的 "Notification recipients" 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 "Create Role" 或 "Edit Role" 页的 "Notification recipients" 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。
- **密码重置** - 发送 Identity Manager 密码重置通知。根据为相关 Identity Manager 策略选择的 "Reset Notification Option" 值，系统会立即 （在 Web 浏览器中）为重置密码的管理员显示通知，或者向密码将被重置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。这种通知将列出已成功更新的资源，还将指明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。这种通知将列出错误，还将指明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** - 分别由 “通知协调响应”、“通知协调启动”和 “通知协调完成”默认工作流调用。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 "Resources" 区请求资源时，系统会发送此通知。
- **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。
- **临时密码重置** - 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 "Password Reset Notification Option" 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

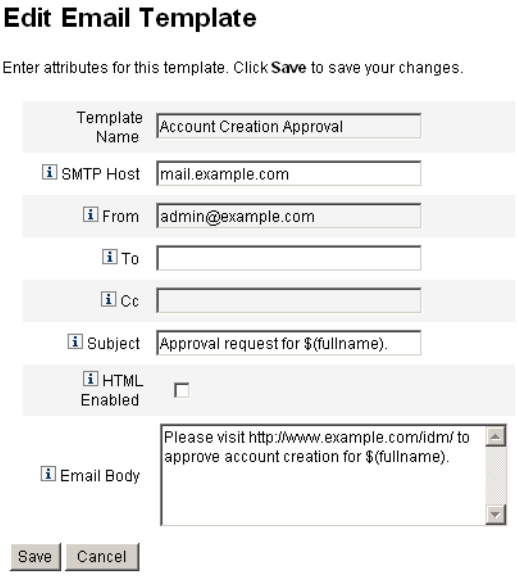
可以通过自定义电子邮件模板为收件人提供具体指导，告诉他如何完成一项任务或如何查看结果。例如，您可能想要通过添加以下消息自定义 "Account Creation Approval" 模板以将批准者引导到帐户批准页：

请转至 `http://host.example.com:8080/idm/approval/approval.jsp` 以批准为 `$(fullname)` 创建帐户。

要自定义电子邮件模板，请执行以下步骤（该步骤使用 "Account Creation Approval" 模板作为示例）：

1. 在菜单栏中选择 **Configure**。
2. 在 "Configure" 页中选择 **Email Templates**。
3. 单击以选择 "Account Creation Approval" 模板。

图 4-11 编辑电子邮件模板



4. 输入模板的详细信息：
   - 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 "To" 和 "Cc" 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 "Email Body" 字段中，自定义内容以提供指向 Identity Manager 位置的指针。

5. 单击 **Save**。

也可以通过使用 Identity Manager IDE 修改电子邮件模板。有关 IDE 的详细信息，请参见 *Identity Manager 部署工具*。

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

也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 4-3 电子邮件模板变量

模板	允许的变量
密码重置	$(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 4-3 电子邮件模板变量

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

配置审计组和审计事件

设置审计配置组使您可以记录和报告您选择的系统事件。配置审计组和事件需要配置审计管理权能。

要配置审计配置组，请在菜单栏中选择 **Configure**，然后选择 **Audit**。

"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。

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。

检查是否已选中 "Enable Audit" 复选框。清除复选框以禁用审计系统。

编辑审计配置组中的事件

要编辑组中的事件，您可为对象类型添加或删除操作。要执行此操作，请将 "Actions" 列中的项目从该对象类型的 **Available** 区域移动到 **Selected** 区域，然后单击 **OK**。

为审计配置组添加事件

要在组中添加事件，请单击 **New**。 Identity Manager 将事件添加到页的底部。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。单击 **OK** 将事件添加到该组。

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 Server 设置** - 通过在 “资源”区域创建 Remedy 资源来设置 Remedy 配置。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。要执行此操作，请选择 **Configure**，然后选择 **Remedy Integration**。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 *Identity Manager 工作流、表单和视图*。

配置 Identity Manager 服务器设置

可编辑特定于服务器的设置，以使 Identity Manager 服务器仅运行特定任务。为此，请选择 **Configure**，然后选择 **Servers**。

要编辑单个服务器的设置，可在 "Configure Servers" 页的列表中选择一个服务器。Identity Manager 将显示 "Edit Server Settings" 页，可在其中编辑协调程序、调度程序、 JMX 和其他设置。

协调程序设置

默认情况下，协调程序设置显示在 "Edit Server Settings" 页上。您可接受默认值或取消选定 **Use default** 选项以指定一个值：

- **并行资源限制** - 指定协调程序可并行处理的最大资源数。
- **最少工作线程数** - 指定协调程序将始终保持活动状态的处理线程数。
- **最多工作线程数** - 指定协调程序可使用的最大处理线程数。协调程序将仅启动工作量所需的线程数；这就限制了线程的数量。

调度程序设置

在 "Edit Server Settings" 页上单击 **Scheduler** 以显示调度程序选项。您可接受默认值或取消选择 “使用默认值”选项以指定一个值：

- **调度程序启动** - 选择调度程序的启动模式：
  - **自动** - 启动服务器时启动。此为默认启动模式。
  - **手动** - 启动服务器时启动，但保持暂停直到手动启动。
  - **已禁用** - 启动服务器时不启动。
- **启用跟踪** - 选择此选项可激活调度程序对标准输出的调试跟踪。
- **最大并发任务数** - 选择此选项可指定调度程序在任意时刻运行的任务的最大数量（默认情况除外）。对超过此限制的其他任务的请求将被延迟，或在其他服务器上运行。
- **任务限制** - 指定可在服务器上执行的任务集。为此，请从可用任务列表中选择一个或多个任务。所选任务的列表可以是包含列表或排除列表，这取决于您选择的选项。您可选择允许除列表中选定任务以外的所有任务 （默认行为），或仅允许选定的任务。

单击 **Save** 以保存对服务器设置的更改。

电子邮件模板服务器设置

单击 "Servers" 菜单上的 **Email Templates** 可指定默认 SMTP 服务器设置。

使用此选项时，通过清除 **Use Default** 选项并输入要使用的邮件服务器可指定默认电子邮件服务器 （默认情况除外）。输入的文本将用于替换电子邮件模板中的 *smtpHost* 变量。

JMX

使用此设置可启用 JMX 群集轮询并配置轮询线程的间隔。通过转到 Identity Manager 调试页并单击 **Show MBean Info** 按钮可查看收集的 JMX 数据。

要启用 JMX 轮询，请单击 "Servers" 选项卡中的 **JMX**，并选择以下选项：

- **启用 JMX** - 使用此选项可启用或禁用 JMX 群集 MBean 的轮询线程。要启用 JMX，请清除默认选项 （使用默认值 [false]）。

注 由于将系统资源用于轮询循环，因此请仅在要使用 JMX 时启用此选项。

- **轮询间隔 (ms)** - 启用 JMX 后，使用此选项可更改服务器轮询系统信息库更改的默认间隔。指定间隔 （以毫秒为单位）。

  默认的轮询间隔设置为 60000 毫秒。要更改该值，请清除此选项的复选框并在提供的输入字段中输入新值。

单击 **Save** 以保存对服务器设置的更改。

编辑默认服务器设置

默认服务器设置功能使您可以设置所有 Identity Manager 服务器的默认设置。除非您在各个服务器设置页上进行了不同的选择，否则服务器将继承这些设置。要编辑默认设置，请单击 **Edit Default Server Settings**。“编辑默认服务器设置”页显示与各个服务器设置页相同的选项。

除非您已取消选择该设置的 “使用默认值”选项，否则对每个默认服务器设置的更改会传播到对应的服务器设置。

单击 **Save** 以保存对服务器设置的更改。

第 5 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，还介绍在 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。您可以建立 Identity Manager 管理员来管理：

- 用户帐户
- 系统对象，例如角色和资源
- 组织

Identity Manager 以直接或间接分配下列项目的方式区分管理员和用户：

- **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和其他多种职责。在很多情况下，管理员需要执行对其他用户或管理员*透明*或者有限定范围的帐户管理任务。

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 仅允许管理员查看和管理特定的、定义范围内的那些对象，以此来支持职责的划分和此委托管理模型。

Identity Manager 通过下列措施实现将单独系统活动委托给管理员的功能：

- 提供对特定组织以及这些组织内的对象的有限控制
- 过滤 Identity Manager 用户创建和编辑页的管理员视图
- 以权能形式为管理员提供特定作业任务

设置新用户帐户或编辑用户帐户时，您可以在 "Create User" 页中为用户指定委托。

您也可以从 "Work Items" 选项卡委托工作项目，例如批准请求。有关详细信息，请参见第 175 页上的 “委托工作项目”。

创建管理员

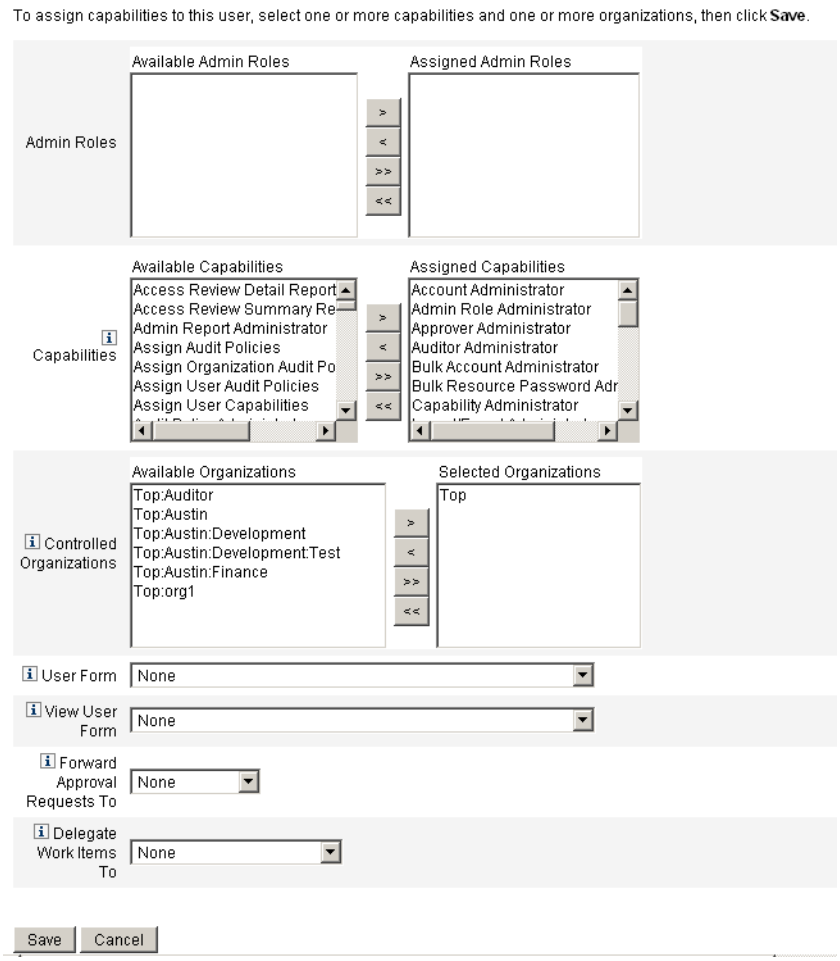
可通过扩展 Identity Manager 用户的权能创建 Identity Manager 管理员。创建或编辑用户时，可以通过下列方法为该用户提供管理控制：

- 指定该用户可以管理的组织
- 在该用户管理的组织内分配权能
- 选择该用户在创建并编辑 Identity Manager 用户时将使用的表单 （如果分配的权能允许他执行这些操作）
- 选择接收暂挂批准请求的批准者 （如果分配的权能允许批准者批准请求）

要授予用户管理权限，请在菜单栏中选择 **Accounts** 以转至 Identity Manager "Accounts" 区域。对于新用户，请在 "Create User" 页中选择 **Security** 选项卡以分配管理员属性。

要将管理员属性分配给现有用户，请在 “帐户” 列表中选择用户，然后通过从 “用户操作” 列表中选择 “编辑用户权能” 以编辑用户的权能。下图对打开的 "Security" 表单进行了说明：

图 5-1 "User Account Security" 页：指定管理员权限



选择一个或多个选项，以建立管理控制：

- **受控组织** - 选择一个或多个组织。该管理员可以控制选定组织中的对象以及在分层结构中处于该组织之下的任何组织中的对象。管理员控制的范围由分配给他的权能进一步定义。必须在此区域进行选择。
- **权能** - 选择此管理员在其所控制的组织内将具有的一项或多项权能。有关 Identity Manager 权能的详细信息和描述，请阅读第 4 章 “配置”。

- **用户表单** - 选择此管理员在创建和编辑 Identity Manager 用户时将使用的用户表单 （如果分配了此权能）。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该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，以将所有当前暂挂的批准请求转发至该用户。还可以从 "Approvals" 页进行此管理员设置。
- **将工作项目委托给** - 使用此选项指定用户帐户的委托（如果可用）。您可以指定 IDMManager、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 4 章 “配置”介绍您可以分配的内置 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。

管理员可以在下列位置更改其他管理员的密码：

- **“帐户”区域 -** 在列表中选择管理员，然后在 “用户操作”列表中选择 “更改密码”。
- **“编辑用户”页 -** 选择**身份**表单选项卡，然后输入新密码并确认。
- **“密码”区域 -** 输入管理员名称，然后单击**更改密码**。

提示 输入一个或多个字符，然后单击 **Find** 以列出所有匹配项。

管理员可从 "Passwords" 区域更改自己的密码。选择 **Passwords**，然后选择 **Change My Password** 以访问自助服务密码字段。

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、重置选项和通知选择。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进行设置。

验明管理员操作

您可以设定一个选项，以要求管理员在处理特定帐户变更前输入其 Identity Manager 登录密码。如果密码无效，则该帐户操作不能继续。

支持此选项的 Identity Manager 页为：

- 编辑用户 (`account/modify.jsp`)
- 更改用户密码 (`admin/changeUserPassword.jsp`)
- 重置用户密码 (`admin/resetUserPassword.jsp`)

请按以下各节中所述设置这些选项：

编辑用户验明选项

按如下所示在 `account/modify.jsp` 页中设置此选项：

```
requestState.setOption(UserViewConstants.OP_REQUIRES_CHALLENGE, "email,
fullname, password");
```

其中，该选项的值是包含以下一个或多个用户视图属性名称的列表（以逗号分隔）：

- 应用程序
- adminRoles
- assignedLhPolicy
- 权能
- controlledOrganizations
- email
- firstname
- fullname
- lastname

- 组织
- password
- 资源
- 角色

"Change User Password and Reset User Password Challenge" 选项

按如下所示在 admin/changeUserPassword.jsp 和 admin/resetUserPassword 页中设置此选项：

```
requestState.setOption(UserViewConstants.OP_REQUIRES_CHALLENGE, "true");
```

其中，选项值可以是 true 或 false。

更改验证问题回答

使用 "Passwords" 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 **Passwords**，然后选择 **Change My Answers**。

有关验证的详细信息，请参见第 85 页上的 “用户验证”。

自定义管理员界面中的管理员名称显示

可以在某些 Identity Manager 管理员界面页和区域 （例如以下区域）中按属性 （例如电子邮件或全称）而不是按 accountId 来显示 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）被*静态分配*给一个组织。用户还可以被*动态地分配*给其他组织。

Identity Manager 管理员被额外分配给*控制*组织。

创建组织

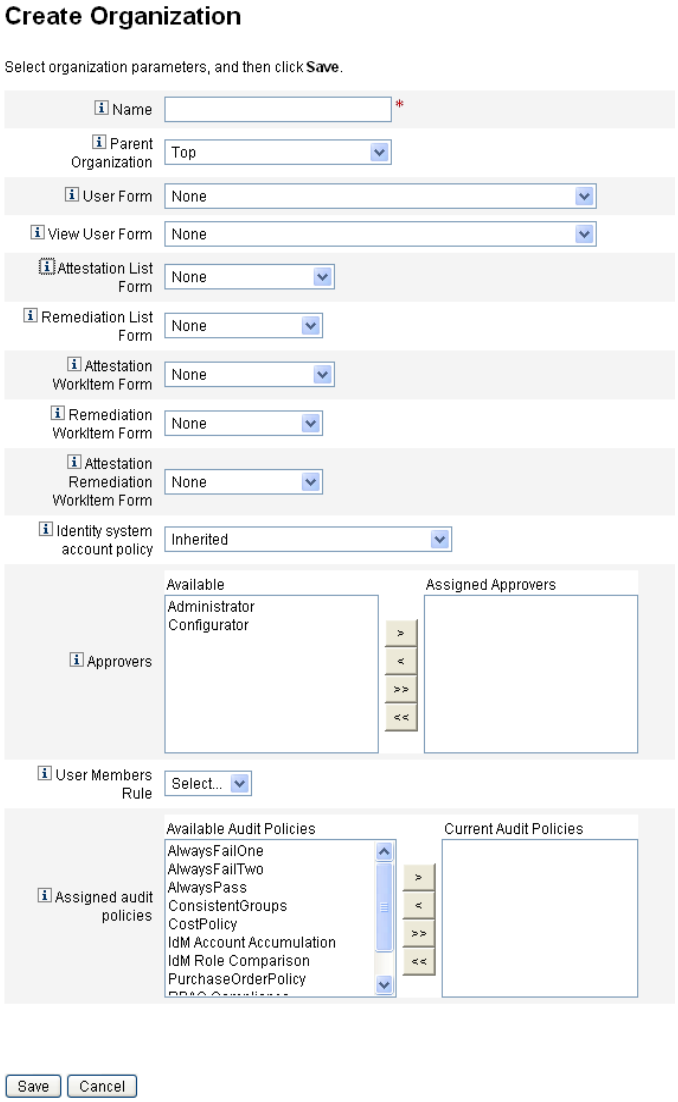
在 Identity Manager "Accounts" 区域创建组织。要创建组织，请执行以下步骤：

1. 在菜单栏中选择 **Accounts**。
2. 在 "Accounts" 页上的 "New Actions" 列表中选择 **New Organization**。

提示 要在组织分层结构中的特定位置上创建组织，请在列表中选择组织，然后从 "New Actions" 列表选择 **New Organization**。

图 5-2 说明了 “创建组织”页。

图 5-2 “创建组织”页


Create Organization
Select organization parameters, and then click Save.
Name
Parent Organization
Top
User Form
None
View User Form
None
Attestation List Form
None
Remediation List Form
None
Attestation WorkItem Form
None
Remediation WorkItem Form
None
Attestation Remediation WorkItem Form
None
Identity system account policy
Inherited
Approvers
Available
Administrator
Configurator
Assigned Approvers
User Members Rule
Select...
Assigned audit policies
Available Audit Policies
AlwaysFailOne
AlwaysFailTwo
AlwaysPass
ConsistentGroups
CostPolicy
IdM Account Accumulation
IdM Role Comparison
PurchaseOrderPolicy
Current Audit Policies
Save
Cancel

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。组织成员资格由以下内容确定：

- **直接 （静态）分配** - 在 “创建用户” 或 “编辑用户” 页中将用户直接分配给组织。（选择 **Identity** 表单选项卡以显示 "Organizations" 字段。）用户必须被直接分配给一个组织。
- **规则驱动 （动态）分配** - 通过将评估时可返回一组成员用户的规则分配给组织，将用户动态分配给组织。 Identity Manager 将在下列情况下评估用户成员规则：
  - 列出组织中的用户
  - 查找用户 （使用 "Find Users" 页），包括搜索具有用户成员规则的组织中的用户
  - 请求访问用户，并且当前管理员控制具有成员规则的组织

从 "Create Organization" 页的 "User Members Rule" 字段中选择用户成员规则。图 5-3 显示了用户成员规则的示例。

图 5-3 创建组织：用户成员规则选择

以下示例显示如何设置可以动态控制组织用户成员资格的用户成员规则。

注 有关在 Identity Manager 中创建和使用规则的信息，请参见 *Identity Manager 部署工具*。

关键定义和包含项

- 对于 “用户成员规则”选项框中显示的规则，必须将其 `authType` 设置为 `authType=謪serMembersRule'`。
- 该环境是目前已验证的 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`。

以下为用户成员规则示例的语法示例。

代码示例 5-1 用户成员规则示例

```
<Rule name='Get Team Players'
     authType='UserMembersRule'>
   <defvar name='Team players'>
      <block>
         <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>
            <列表>
               <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>
```

分配组织控制

从 "Create User" 或 "Edit User" 页分配一个或多个组织的管理控制。选择 **Security** 表单选项卡以显示 "Controlled Organizations" 字段。

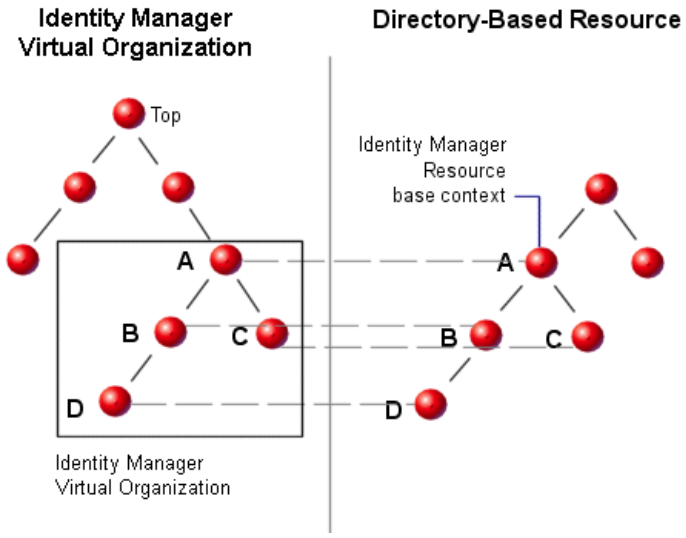
您还可以从 "Admin Roles" 字段分配一个或多个管理员角色，从而分配组织的管理控制。

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（已定义资源的基本上下文容器的子容器）中的一个容器。图 5-4 说明了此结构。

图 5-4 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环境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

从 Identity Manager "Accounts" 区域设置目录连接：

1. 在 Identity Manager 菜单栏中，选择 **Accounts**。
2. 在 "Accounts" 列表中选择 Identity Manager 组织，然后在 "New Actions" 列表中选择 "New Directory Junction"。

   您选择的组织将是所设置的虚拟组织的父组织。

   Identity Manager 将显示 "Create Directory Junction" 页。
3. 进行选择即可设置虚拟组织：
   - **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目录结构的现有目录。
   - **用户表单** - 选择要应用于此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 "Organization Actions" 列表中选择 "Refresh Organization"。

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 **Delete**。

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 （如重置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 用户都需要分配有权能；而只有那些要通过 Identity Manager 执行一项或多项管理操作的用户才需要。例如，允许用户在无需分配权能的情况下更改自己的密码，但要更改其他用户的密码则需要分配权能。

分配的权能决定了您可以访问 Identity Manager 的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 的一定区域，包括：

- **Home** 和 **Help** 选项卡
- **Passwords** 选项卡（仅 **Change My Password** 和 **Change My Answers** 子选项卡）
- **Reports** （仅限于与管理员的特定职责相关的类型）

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

1. 在菜单栏中选择 **Security**。
2. 选择 **Capabilities** 选项卡以显示 Identity Manager 权能列表。

创建权能

要创建权能，请单击 **New**。命名新的权能，然后选择可使用此权能的权能、分配者和组织。必须至少选择一个组织。

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

要编辑未受保护的权能，请在列表中右键单击该权能，然后选择 **Edit**。

不能编辑内置权能；但是，可以用其他名称保存，以创建您自己的权能或在您创建的权能中使用它们。

保存和重命名权能

要*克隆*权能（用其他名称保存权能以创建新的权能）：

- 右键单击列表中的一个权能，然后选择 **Save As**。
- 输入一个新名称，然后单击 **OK**。

您可以对这个新权能进行编辑，即使复制的权能是受保护的。

分配权能

从 "Create User" 和 "Edit User" 页为用户分配权能。还可以通过分配管理员角色（通过界面中的 "Security" 区域设置），将权能分配给用户。有关详细信息，请参见第 167 页上的 “了解和管理管理员角色”。

权能分层结构

基于任务的权能包含在以下功能性权能分层结构中：

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
  - 重置密码管理员
- 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

- 连接权能
- 连接权能规则
- 连接受控组织规则
- 连接组织

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

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

批量资源密码管理员

- 批量更改资源密码管理员
- 批量重置资源密码管理员

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
    - 重置密码管理员
  - 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

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）
- 重置密码管理员 （需要进行验证）

策略管理员

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
  -
- 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 Active Sync 资源管理员
- 控制 Active Sync 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
- 重置资源密码管理员

角色管理员

安全管理员

服务提供者管理员

- 服务提供者用户管理员
  - 服务提供者创建用户
  - 服务提供者删除用户
  - 服务提供者更新用户
  - 服务提供者查看用户

服务提供者管理员角色管理员

用户帐户管理员

- 删除用户
- 密码管理员
- 创建用户
- 禁用用户
- 启用用户
- 导入用户
- 重命名用户
- 解除锁定用户
- 更新用户

查看组织

- 列出组织

查看资源

- 列出资源

Waveset 管理员

权能定义

表 5-1 说明了每个基于任务的权能并着重说明每个权能可访问的选项卡和子选项卡。按名称的字母顺序列出权能。

所有权能都授予用户或管理员访问 **Passwords > Change My Password** 和 **Change My Answers** 选项卡的权限。

表 5-1 Identity Manager 权能描述

权能	管理员/用户可执行的操作：	访问这些选项卡和子选项卡：
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	**Reports > Run Reports** 选项卡、 **View Reports** 选项卡 - 仅 "Access Review Detail Report" **Reports > View Dashboards**
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	**Reports** - 仅 "Access Review Summary Report" **Reports > View Dashboards**
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。	**Accounts** - **List Accounts**、 **Find Users**、**Extract to File**、**Load from File** 和 **Load from Resource** 选项卡 **Passwords** - 所有子选项卡 **Work Items - Approvals** 子选项卡 **Tasks** - 所有子选项卡
管理员报告管理员	创建、编辑、删除和运行管理员报告。	**Reports** - **Manage Reports** 和 **Run Reports** 子选项卡 （仅管理员报告）
管理员角色管理员	创建、编辑和删除管理员角色。	**Security - Admin Roles** 子选项卡
批准者管理员	批准或拒绝其他用户发出的请求。	**仅 "Default"**
分配审计策略	将审计策略分配给用户帐户和组织。	**Accounts** - "User Actions" 列表中的 **Edit User Audit Policy**。 **Accounts - "Organization Actions" 列表中的 Edit Organization Audit Policy**。
分配组织审计策略	仅向组织分配审计策略。	**Accounts** - "Organization Actions" 列表中的 **Edit Organization Audit Policy**；**List Accounts** 选项卡

表 5-1 Identity Manager 权能描述 *（续）*

权能	管理员/用户可执行的操作：	访问这些选项卡和子选项卡：
分配用户审计策略	仅向用户分配审计策略。	**Accounts** - "User Actions" 列表中的 **Edit User Audit Policy**；**List Accounts** 选项卡；**Find Users** 选项卡
分配用户权能	更改用户权能分配 （分配和取消分配）。	**Accounts** - **List Accounts** （仅 "Edit"）和 **Find Users** 子选项卡。 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”）。
审计策略管理员	创建、修改和删除审计策略。	**Compliance - Manage Policies**
审计策略扫描报告管理员	创建、修改、删除和执行审计策略扫描报告。	**Reports** - 仅 "Audit Policy Scan Report"
审计报告管理员	创建、修改、删除和执行审计报告。	**Reports** - 仅 "Audit Report"
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。	**Reports** - 仅 "Audited Attribute Report"
审计日志报告管理员	创建、修改、删除和执行审计日志报告。	**Reports** - 仅 "AuditLog Report"
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	**Compliance - Manage Access Scans**
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。	**Compliance -** 所有子选项卡 **Reports** - "Run Reports"、"View Reports" 和 "Manage Auditor Reports" **Accounts** - "Edit User Audit Policies" 和 "Edit Organization Audit Policies" 操作。
审计者证明者	当启用了组织安全性后，需要证明其他用户的证明。	**仅 "Default"**
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。	**Compliance - Manage Access Scans**、**Access Review** 子选项卡
Auditor 修正者	修正、缓解和转发审计策略违规。	**Remediations** - 所有子选项卡
Auditor 报告管理员	创建、修改、删除和执行任何 Auditor 报告。	**Reports** - 对 Auditor 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。	**Accounts** - **List Accounts**、**Find Users** 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。	**Reports** - 仅 "Organization Violation History" 报告
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。	**Accounts** - 所有子选项卡 **Passwords** - 所有子选项卡 **Approvals** - 所有子选项卡 **Tasks** - 所有子选项卡

表 5-1 Identity Manager 权能描述 *（续）*

权能	管理员/用户可执行的操作：	访问这些选项卡和子选项卡：
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。	**Accounts** - **List Accounts**、**Find Users** 和 **Launch Bulk Actions** 子选项卡。无法创建或删除用户。 **Passwords** - 所有子选项卡 **Approvals** - 所有子选项卡 **Tasks** - 所有子选项卡
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。	**Accounts** - **List Accounts**、**Find Users** 和 **Launch Bulk Actions** 子选项卡。无法创建、删除用户或向用户分配权能。 **Passwords** - 所有子选项卡 **Tasks** - 所有子选项卡
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）。	**Accounts** - **List Accounts** （仅 "Create"）、**Find Users** 和 **Launch Bulk Actions** 子选项卡 **Tasks** - 所有子选项卡
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 （针对各个用户并使用批量操作）。	**Accounts** - **List Accounts** （仅 "Create"）、**Find Users** 和 **Launch Bulk Actions** 子选项卡 Tasks - 所有子选项卡
批量删除 IDM 用户	删除现有 Identity Manager 用户帐户 （针对各个用户并使用批量操作）。	**Accounts** - **List Accounts** （仅 "Delete"）、**Find Users** 和 **Launch Bulk Actions** 子选项卡 **Tasks** - 所有子选项卡
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）。	**Accounts** - **List Accounts** （仅 "Deprovision"）、**Find Users** 和 **Launch Bulk Actions** 子选项卡 **Tasks** - 所有子选项卡
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）。	**Accounts** - **List Accounts** （仅 "Disable"）、**Find Users** 和 **Launch Bulk Actions** 子选项卡 **Tasks** - 所有子选项卡
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）。	**Accounts** - **List Accounts** （仅 "Enable"）、**Find Users** 和 **Launch Bulk Actions** 子选项卡 **Tasks** - 所有子选项卡
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）。	**Accounts** - **List Accounts** （仅 "Unassign"）、**Find Users** 和 **Launch Bulk Actions** 子选项卡 **Tasks** - 所有子选项卡

表 5-1 Identity Manager 权能描述 *（续）*

权能	管理员/用户可执行的操作：	访问这些选项卡和子选项卡：
批量解除用户的链接	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）。	**Accounts** - **List Accounts** （仅 "Unlink"）、 **Find Users** 和 **Launch Bulk Actions** 子选项卡 **Tasks** - 所有子选项卡
批量更新用户	更新现有用户和资源帐户 （针对各个用户并使用批量操作）。	**Accounts** - **List Accounts** （仅 "Update"）、**Find Users** 和 **Launch Bulk Actions** 子选项卡 **Tasks** - 所有子选项卡
批量用户帐户管理员	对用户执行所有常规和批量操作。	**Accounts** - 所有子选项卡 **Passwords** - 所有子选项卡 **Tasks** - 所有子选项卡
权能管理员	创建、修改和删除权能。	**Configure** - **Capabilities** 子选项卡
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	**Accounts** - 所有子选项卡。无法删除用户。 **Passwords** - 所有子选项卡 **Approvals** - 所有子选项卡 **Tasks** - 所有子选项卡 **Reports** - 创建管理员和用户报告，运行和编辑管理员报告，运行组织范围内的审计日志报告。无法运行组织范围以外的管理员和用户报告。
更改活动同步资源管理员	更改活动同步资源参数	**Tasks** - **Find Tasks**、 **All Tasks** 和 **Run Tasks** 子选项卡 **Resources** - 对于活动同步资源："Edit" 操作菜单和 "Edit Active Sync Parameters"
更改密码管理员	更改用户和资源帐户密码。	**Accounts - List Accounts 和 Find Users** 子选项卡 （仅 "Change Password"） **Passwords** - 所有子选项卡 **Tasks** - 所有子选项卡。仅 "Export Password Scan" 任务 （从 **Run Tasks** 子选项卡）
更改密码管理员 （需要进行验证）	成功确认用户的验证问题回答后更改用户和资源帐户密码。	**Accounts - List Accounts 和 Find Users** 子选项卡 （仅 "Change Password"；操作前需要进行验证） **Passwords** - 所有子选项卡 **Tasks** - 所有子选项卡。仅 "Export Password Scan" 任务 （从 **Run Tasks** 子选项卡）

表 5-1 Identity Manager 权能描述 *（续）*

权能	管理员/用户可执行的操作：	访问这些选项卡和子选项卡：
更改资源密码管理员	更改资源管理员帐户密码。	**Tasks** - 所有子选项卡 **Resources - List Resources** 子选项卡。仅更改资源密码 （在操作菜单的 **Manage Connection-->Change Password** 中）
更改用户帐户管理员	执行除删除现有用户之外的所有操作。不包括批量操作	**Accounts** - **List Accounts** 和 **Find Users** 子选项卡。无法创建、删除用户或向用户分配权能。 **Passwords** - 所有子选项卡 **Tasks** - 所有子选项卡
配置审计	配置系统中审计的事件和配置组。	**Configure** - **Audit Events** 子选项卡
配置证书	配置信任证书和 CRL。	**Security - Certificates**子选项卡
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）。	**Tasks** - **Find Tasks**、 **All Tasks** 和 **Run Tasks** **Resources** - 对于活动同步资源：活动同步操作菜单 （所有选项）
创建用户	分配资源和启动用户创建请求。不包括批量操作	**Accounts** - **List Accounts** （仅 "Create"）和 **Find Users** 子选项卡 **Tasks** - 所有子选项卡
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。	**Accounts** - **List Accounts** （仅 "Delete"）和 **Find Users** 子选项卡 **Tasks** - 所有子选项卡
删除 IDM 用户	删除 Identity Manager 用户帐户。不包括批量操作。	**Accounts** - **List Accounts** （仅 "Delete"）和 **Find Users** 子选项卡 **Tasks** - 所有子选项卡
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。	**Accounts** - **List Accounts** （仅 "Deprovision"）和 **Find Users** 子选项卡 **Tasks** - 所有子选项卡
禁用用户	禁用现有用户和资源帐户。不包括批量操作	**Accounts** - **List Accounts** （仅 "Disable"）和 **Find Users** 子选项卡 **Tasks** - 所有子选项卡
启用用户	启用现有用户和资源帐户。不包括批量操作	**Accounts** - **List Accounts** （仅 "Enable"）和 **Find Users** 子选项卡 **Tasks** - 所有子选项卡
导入用户	从定义的资源导入用户。	**Accounts** - **Extract to File**、 **Load from File** 和 **Load from Resource** 子选项卡
导入/导出管理员	导入和导出所有类型的对象。	**Configure** - **Import Exchange File** 子选项卡

表 5-1 Identity Manager 权能描述 *（续）*

权能	管理员/用户可执行的操作：	访问这些选项卡和子选项卡：
许可证管理员	设置 Identity System 产品许可证	通过此权能可以使用 `lh license` 命令。（但无法使用管理员界面。）
登录管理员	编辑给定登录界面的登录模块集。	**Configure** - **Login** 子选项卡
元视图管理员	修改身份属性配置	**Meta View - Identity Attributes** 选项卡
组织管理员	创建、编辑和删除组织。	**Accounts** - **List Accounts** 子选项卡（仅 "Edit Organizations"、 "Create Organizations"、 "Edit Directory Junctions"、 "Create Directory Junctions" 和 "Delete Organizations"）
组织批准者	批准新组织的请求。	**Work Items - Approvals** 子选项卡
组织违规历史管理员	创建、修改、删除和执行组织违规历史报告。	**Reports** - 仅 "Organization Violation History" 报告
密码管理员	更改和重置用户和资源帐户密码。	**Accounts** - **List Accounts** （仅列出、更改和重置密码）和 **Find Users** 子选项卡 **Passwords** - 所有子选项卡 **Tasks** - 所有子选项卡
密码管理员 （需要进行验证）	成功确认用户的验证问题回答后更改和重置用户和资源帐户密码。	**Accounts** - **List Accounts** （仅列出、更改和重置密码；操作成功前需要进行验证）和 **Find Users** 子选项卡 **Passwords** - 所有子选项卡 **Tasks** - 所有子选项卡
策略管理员	创建、编辑和删除 “策略”。	**Configure** - **Policy** 子选项卡
策略摘要报告管理员	创建、修改、删除和执行策略摘要报告。	**Reports** - 仅 "Policy Summary Report"
协调管理员	编辑协调策略和控制协调任务。	**Server Tasks** - 所有子选项卡 （查看协调任务）。 **Resources** - **List Resources** 子选项卡
协调报告管理员	创建、编辑、删除和运行协调报告。	**Reports** - **Run Reports** （仅 "Account Index Report"）和 **Manage Reports** 子选项卡
协调请求管理员	管理协调请求。	**Tasks** - 所有子选项卡 **Resources** - **List Resources** 子选项卡（仅列出和协调功能）
Remedy 集成管理员	修改 Remedy 集成配置。	**Tasks** - 所有子选项卡 （查看任务，运行角色同步） **Configure** - **Remedy Integration** 子选项卡

表 5-1 Identity Manager 权能描述 *（续）*

权能	管理员/用户可执行的操作：	访问这些选项卡和子选项卡：
重命名用户	重命名现有用户和资源帐户。	**Accounts** - "List Accounts" 子选项卡 （列出范围内的所有帐户，重命名用户）
报告管理员	配置审计设置和运行所有报告类型。	**Tasks** - 所有子选项卡 （查看任务，运行角色同步） **Reports** - 所有子选项卡
重置密码管理员	重置用户和资源帐户密码。	**Accounts - List Accounts 和 Find Users** 子选项卡 （仅 "Reset Password"） **Passwords** - 所有子选项卡 **Tasks** - 所有子选项卡。仅 "Export Password Scan" 任务 （从 **Run Tasks** 子选项卡）
重置密码管理员 （需要进行验证）	成功确认用户的验证问题回答后重置用户和资源帐户密码。	**Accounts - List Accounts 和 Find Users** 子选项卡 （仅 "Reset Password"；操作成功前需要进行验证） **Passwords** - 所有子选项卡 **Tasks** - 所有子选项卡。仅 "Export Password Scan" 任务 （从 **Run Tasks** 子选项卡）
重置资源密码管理员	重置资源管理员帐户密码。	**Tasks** - **Find Tasks**、 **All Tasks** 和 **Run Tasks** 子选项卡 **Resources - List Resources** 子选项卡。仅重置资源密码 （在操作菜单的 **Manage Connection -->重置密码**中）
资源管理员	创建、修改和删除资源。	**Reports** - 资源用户报告、资源组报告返回范围以外资源上的错误。 **Resources** - **List Resources** 子选项卡 （编辑全局策略，编辑参数和资源组。无法管理连接或资源对象。）
资源组管理员	创建、编辑和删除资源组。	**Resources** - **List Resource Groups** 子选项卡
资源对象管理员	创建、修改和删除资源对象。	**Tasks** - **Find Tasks**、 **All Tasks** 和 **Run Tasks** 子选项卡 （查看涉及资源对象的任务）。 **Resources** - **List Resources** 子选项卡 （仅列出和管理资源对象）

表 5-1 Identity Manager 权能描述 *（续）*

权能	管理员/用户可执行的操作：	访问这些选项卡和子选项卡：
资源密码管理员	更改和重置资源代理帐户密码。	**Tasks** - **Find Tasks**、 **All Tasks** 和 **Run Tasks** 子选项卡 **Resources - List Resources** 子选项卡。仅更改资源密码 （在操作菜单的 **Manage Connection-->Change Password** 中）
资源报告管理员	创建、编辑、删除和运行资源报告。	**Reports** - 所有子选项卡 （仅资源报告）
资源违规历史管理员	创建、修改、删除和执行资源违规历史报告。	**Reports** - 仅 "Resource Violation History" 报告
风险分析管理员	创建、编辑、删除和运行风险分析。	**Risk Analysis** - 所有子选项卡
角色管理员	创建、修改和删除角色。	**Tasks** - **Find Tasks**、 **All Tasks** 和 **Run Tasks** 子选项卡 （同步角色） **Roles** - 所有子选项卡
角色报告管理员	创建、编辑、删除和运行资源报告。	**Reports** - 仅 "Role Report"
运行访问查看详细信息报告	运行访问查看详细信息报告	**Reports** - 仅 "Access Review Detail Report"
运行访问查看摘要报告	运行访问查看摘要报告	**Reports** - 仅 "Access Review Summary Report"
运行管理员报告	运行管理员报告。	**Reports** - 仅 "Admin Report"
运行审计策略扫描管理员	运行和管理审计策略扫描报告	"Reports" - 仅 "Audit Policy Scan Report"
运行审计策略扫描报告	运行审计策略扫描报告。	**Reports** - 仅 "Audit Policy Scan Report"
运行审计报告	运行审计报告。	**Reports** - 仅 "AuditLog Report" 和 "Usage Report"
运行审计属性报告	执行已审计的属性报告。	**Reports** - 仅 "Audited Attribute Report" **Reports > View Dashboards**
运行审计者报告	运行任何 Auditor 报告。	**Reports** - 任何 Auditor 报告 **Reports > View Dashboards**
运行审计日志报告	执行 "AuditLog Report"。	**Reports** - 仅 "AuditLog Report"
运行审计策略违规历史	执行组织违规历史报告。	**Reports** - 仅 "Organization Violation History" 报告 **Reports > View Dashboards**
运行策略摘要报告	执行策略摘要报告。	**Reports** - 仅 "Policy Summary Report"

表 5-1 Identity Manager 权能描述 *（续）*

权能	管理员/用户可执行的操作：	访问这些选项卡和子选项卡：
运行组织违规历史	执行组织违规历史报告。	**Reports** - 仅 "Organization Violation History" 报告 **Reports > View Dashboards**
运行协调报告	运行协调报告。	**Reports** - 仅 "AuditLog Report" 和 "Usage Report"
运行资源报告	运行资源报告。	**Reports** - 仅 "AuditLog Report" 和 "Usage Report"
运行资源违规历史	执行资源违规历史报告。	**Reports** - 仅 "Resource Violation History" 报告
运行风险分析	运行风险分析。	**Reports** - "Run Risk Analysis" 和 "View Risk Analysis" 子选项卡
运行角色报告	运行角色报告。	**Reports** - 仅 "Role Report"
运行任务报告	运行任务报告。	**Reports** - 仅 "Task Report"
运行用户访问报告	执行详细用户报告。	**Reports** - 仅 "User Access Report" **Reports > View Dashboards**
运行用户报告	运行用户报告。	**Reports** - 仅 "User Report"
运行违规摘要报告	执行违规摘要报告。	**Reports** - 仅 "Violation Summary Report" **Reports > View Dashboards**
安全管理员	创建具有权能的用户；管理加密密钥、登录配置和策略。	**Accounts** - **List Accounts** （删除、创建、更新、编辑、更改并编辑密码）和 **Find Users** 子选项卡 （审计报告） **Passwords** - 所有子选项卡 **Tasks** - **Find Tasks**、 **All Tasks** 和 **Run Tasks** 子选项卡 **Reports** - 所有子选项卡 **Resources** - **List Resources** （列出和控制资源对象） **Security** - **Policies** 和 **Login** 子选项卡
任务划分报告管理员	创建、编辑、运行和删除任务划分报告。	**Report** - 仅 "Separation of Duties Report" 的所有操作
运行任务划分报告	运行任务划分报告	**Report** - 仅 "Separation of Duties Report" **Reports > View Dashboards**
服务提供者管理员角色	管理服务提供者管理员角色以及相关的规则。	**Security - Admin Roles** 选项卡

表 5-1 Identity Manager 权能描述 *（续）*

权能	管理员/用户可执行的操作：	访问这些选项卡和子选项卡：
服务提供者管理员	创建、编辑和管理服务提供者用户和事务；配置事务数据库和跟踪的事件。	**Accounts - Manage Service Provider Users** 子选项卡 **Server Tasks > Service Provider Transactions** 选项卡 **Reports > View Dashboards** 选项卡 **Reports > Dashboard Configuration** 选项卡 **Service Provider** - 所有子选项卡
服务提供者创建用户	为服务提供者 （外联网）用户创建用户帐户。	**Accounts - Manage Service Provider Users** 子选项卡
服务提供者删除用户	删除服务提供者用户帐户。	**Accounts - Manage Service Provider Users** 子选项卡
服务提供者更新用户	更新服务提供者用户帐户。	**Accounts - Manage Service Provider Users** 子选项卡
服务提供者用户管理员	管理服务提供者 （外联网）用户。	**Accounts > Manage Service Provider Users** - 所有子选项卡
服务提供者查看用户	查看服务提供者 （外联网）用户帐户信息。	**Accounts - Manage Service Provider Users** 子选项卡
SPML 访问	允许访问 Identity Manager 中的服务置备标记语言 (Service Provisioning Markup Language, SPML) 功能。	**Security - Capabilities** 子选项卡
任务报告管理员	创建、编辑、删除和运行任务报告。	**Reports** - 仅 "Task Report"。
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。	**Accounts** - **List Accounts** （仅 "Unassign"）和 **Find Users** 子选项卡 **Tasks** - 所有子选项卡
解除用户的链接	取消现有资源帐户的链接。不包括批量操作。	**Accounts** - **List Accounts** （仅 "Unlink"）和 **Find Users** 子选项卡 **Tasks** - 所有子选项卡
解除锁定用户	对支持解除锁定的现有用户的资源帐户解除锁定。不包括批量操作。	**Accounts** - **List Accounts** （仅 "Unlock"）和 **Find Users** 子选项卡 **Tasks** - **Find Tasks**、 **All Tasks** 和 **Run Tasks** 子选项卡
更新用户	编辑现有用户和启动用户更新请求。	**Accounts** - 编辑和更新用户 **Tasks** - 管理现有任务 （通过 **All Tasks** 子选项卡）
用户访问报告管理员	创建、运行、编辑和删除用户访问报告	**Reports** - 仅 "User Access Report" **Reports > View Dashboards**

表 5-1 Identity Manager 权能描述 *（续）*

权能	管理员/用户可执行的操作：	访问这些选项卡和子选项卡：
用户帐户管理员	对用户执行所有操作。	**Accounts** - **List Accounts**、 **Find Users**、 **Extract to File**、 **Load from File** 和 **Load from Resource** 子选项卡。无法分配用户权能（**List Accounts** 子选项卡上的 **Security** 表单选项卡）。 **Tasks** - **Find Tasks**、 **All Tasks** 和 **Run Tasks** 子选项卡
用户报告管理员	创建、编辑、删除和运行用户报告。	**Reports** - "Run user Report"。
查看用户	查看单个用户详细信息。	**Accounts** - 从列表中选择用户以查看单个用户帐户信息。不允许执行任何更改操作。
违规摘要报告管理员	创建、修改、删除和执行违规摘要报告。	**Reports** - 仅 "Violation Summary Report" **Reports > View Dashboards**
Waveset 管理员	执行系统范围内的任务，如修改系统配置对象。	**Server Tasks** - 所有子选项卡。同步角色，编辑源适配器模板和调度报告 **Reports** - 所有子选项卡 **Resources** - 列出资源 （仅列出，不允许进行更改操作） **Configure** - **Audit**、 **Email Templates**、 **Form and Process Mappings** 和 **Servers** 子选项卡

了解和管理管理员角色

通过*管理员角色*可将一组唯一的权能和控制范围或受管理的组织分配给一个或多个管理员。可将多个管理员角色分配给一个管理员。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创建和编辑用户 （这些用户是在该管理员角色中指定的受控组织的成员）的权限。而另一个分配给同一管理员的管理员角色可能仅授予在由该管理员角色指定的受控组织中更改用户密码的权限。

建议将管理员角色用于授予管理员权限，而不用于直接将权能和受控组织分配给用户。通过管理员角色可以重复使用权能和范围或控制对，并可简化大量用户的管理员权限的管理工作。

可以直接或间接 （动态）将权能或组织 （或两者）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，您可将用户报告管理员权能与 Top 受控组织分配给某管理员角色。

- **动态** （间接） - 此方法使用权能和受控组织*规则*的分配。每次分配了该管理员角色的管理员登录时都将评估这些规则，以基于验证管理员动态确定一组明确的权能和/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。

可以直接或间接 （动态）将管理员角色分配给管理员：

- **直接** - 将管理员角色明确分配给管理员 （用户帐户）。
- **间接 （动态） -** 使用管理员角色规则分配管理员角色。每次管理员登录时，Identity Manager 都将评估该规则，以确定是否要将该管理员角色分配给验证管理员。

  例如，当用户登录并且其 Active Directory (Active Directory, AD) 用户所在城市为 `Austin`、州为 `Texas` 时，规则可能返回 `true`。因此，将分配管理员角色。

注 通过将系统配置属性 `security.authz.checkDynamicallyAssignedAdminRolesAtLoginTo.`*`logininterface`* 设置为 `true` 或 `false`，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。对于所有界面，默认值均为 false。

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样例规则。这些规则位于 Identity Manager 安装目录的 `sample/adminRoleRules.xml` 中。表 5-2 提供了规则名称以及必须为规则指定的 `authType`。

表 5-2 管理员角色样例规则

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样例规则的信息，请参见“服务提供者管理”一章中的第 415 页上的 “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 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“服务提供者管理”一章中的第 415 页上的 “委托管理”。

可以通过管理员界面编辑用户管理员角色 （选择 **Security**，然后再选择 **Admin Roles**）。

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。

但是，如果用户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，通过用户管理员角色进行的权能和受控组织动态分配将能够实现对这些对象进行动态细化授权。

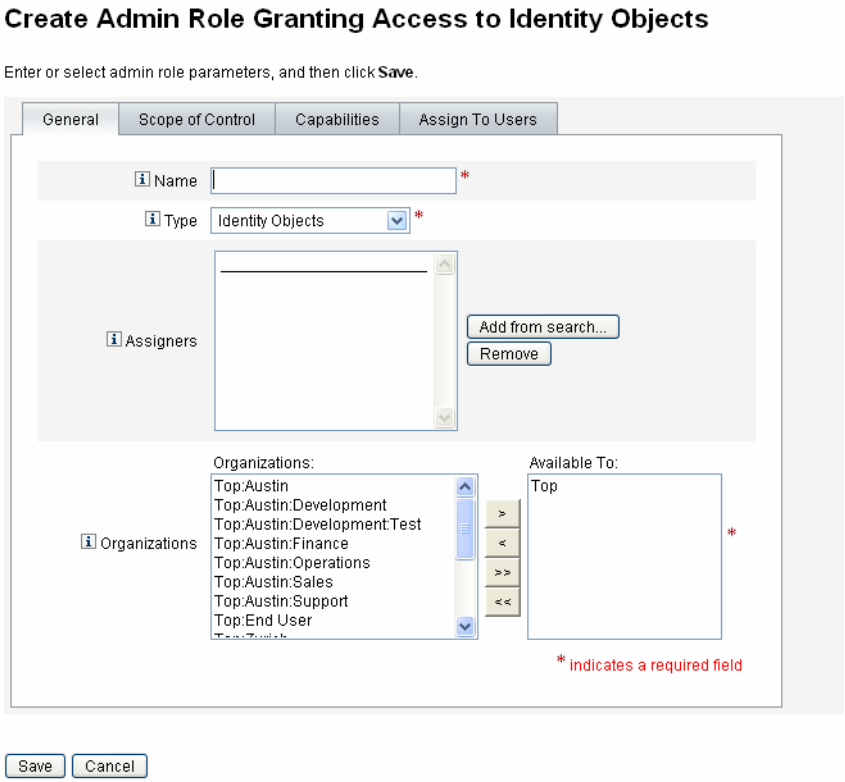
创建和编辑管理员角色

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 **Security**，然后单击 **Admin Roles** 选项卡。"Admin Roles" 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 **New** 可创建管理员角色。Identity Manager 将显示 “创建管理员角色” 选项 （在图 5-5 中进行了说明）。"Create Admin Role" 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 5-5 "Admin Role Create" 页："General" 选项卡



"General" 选项卡

使用创建管理员角色或编辑管理员角色视图中的 "General" 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** - 为类型选择**身份对象**或**服务提供者用户**。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 "Identity Objects"。如果创建管理员角色以向服务提供者用户授予访问权限，请选择 "Service Provider Users"。

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 “服务提供者管理”一章中的第 415 页上的 “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。

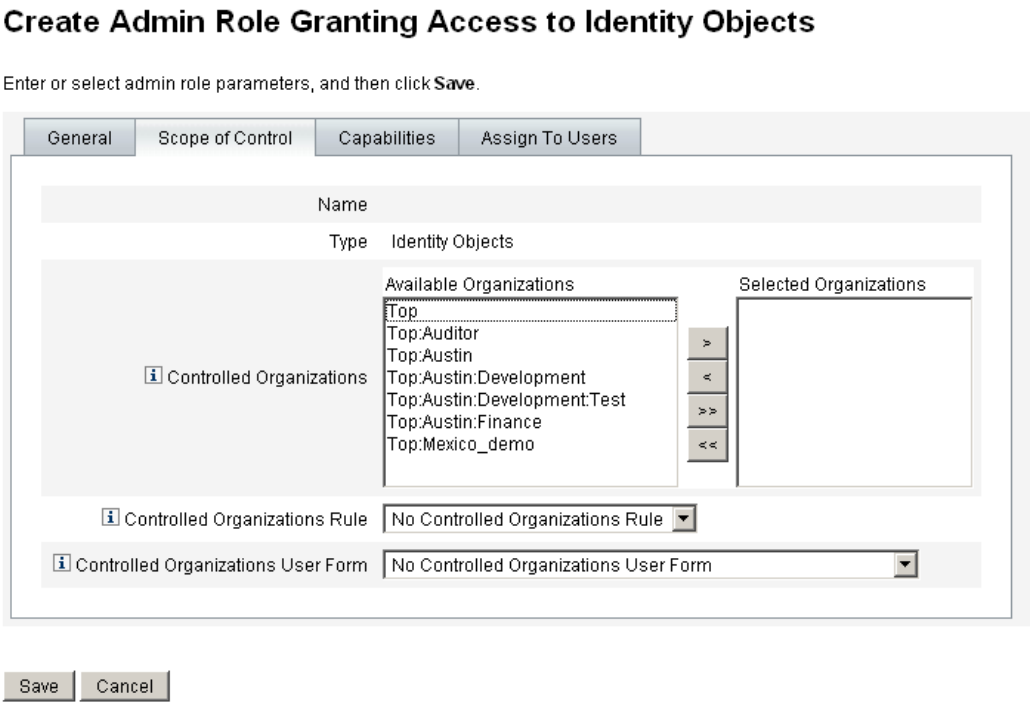
- **组织** - 选择可使用此管理员角色的一个或多个组织。此字段为必填字段。

  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。

Scope of Control

使用此选项卡（如图 5-6 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的用户管理组织的规则，以及选择管理员角色的用户表单。

图 5-6 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"。
- **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所使用的用户表单。默认情况下，将选择 "No Controlled Organizations User Form"。

  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。

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 "Capabilities" 选项卡中，请选择以下选项：

- **权能** - 这些权能是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 "Assigned Capabilities" 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零个或多个权能的列表。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。

当在该管理员所控制的组织中创建或编辑用户时，被分配管理员角色的管理员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。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要使用的用户表单：

- 如果用户表单是直接分配给该管理员的，则使用该表单。
- 如果没有直接分配给该管理员的用户表单，但该管理员具有分配的管理员角色：
  - 控制被创建或编辑的用户为其成员的组织，并且
  - 指定一个用户表单

  那么使用该用户表单。
- 如果没有直接分配给该管理员或通过管理员角色间接分配的表单，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）。
- 如果管理员的所有成员组织都没有分配用户表单，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。

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 "Work Items" 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** - 对新帐户或帐户更改的批准请求。
- **证明** - 查看和批准用户权利文件的请求。
- **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，请在菜单栏中单击**工作项目**选项卡。可以访问工作项目以从此选项卡中管理请求，也可以选择一种工作项目类型以列出此类型的请求。

注 如果您是暂挂工作项目 （或委托工作项目）的工作项目拥有者，则在您登录 Identity Manager 用户界面时将显示 "Work Items" 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 "Work Items" 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。

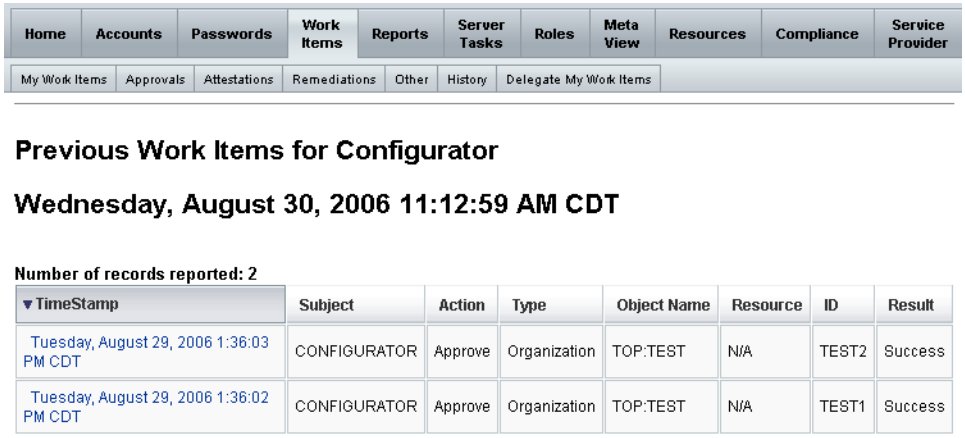
有关对请求做出响应的详细信息，请参见以下主题：

- 第 177 页上的 “帐户批准”
- 第 364 页上的 “管理证明责任”
- 第 344 页上的 “遵循性违规修正和缓解”

查看工作项目历史

使用 "Work Items" 区域中的 "History" 选项卡可以查看先前工作项目操作的结果。图 5-7 显示了工作项目历史的视图示例。

图 5-7 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。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）。

您也可以从 “创建用户” 和 “编辑用户” 页的 “委托” 表单选项卡，以及用户界面主菜单来委托工作项目。

在有效委托期内，受托者可以代表您批准工作项目。委托的工作项目包括受托者的姓名。

任何用户都可以为其未来的工作项目配置委托。可以编辑用户的管理员也可以为用户配置委托。

审计日志条目

如果已委托请求，则已批准和已拒绝的工作项目的审计日志条目将包括您（委托者）的姓名。当创建或修改用户时，对用户委托的批准者信息的更改将记录在审计日志条目的详细更改区域中。

查看当前委托

从**工作项目**选项卡中选择**委托我的工作项目**。Identity Manager 将显示“当前委托”页，可以在该页中查看和编辑当前有效的委托。

查看以前的委托

从“工作项目”选项卡中选择“委托我的工作项目”，然后选择“前一个”。Identity Manager 将显示以前委托的可用于设置新委托的工作项目。

创建委托

要创建委托，请选择 “委托我的工作项目”，然后选择 “新建”。选择以下项目：

- **选择要委托的工作项目类型** - 从选择列表中选择工作项目类型。

  默认的工作项目类型包括：

  - 批准
  - 组织批准
  - 资源批准
  - 角色批准
  - 证明
  - 查看
  - 访问查看修正

注 您必须至少是一个角色的批准者，才能委托 “角色批准”类型的工作项目。同样，您必须至少是一个资源的批准者，才能委托“资源批准”工作项目；您必须至少是一个组织的批准者，才能委托 “组织批准”工作项目。

如果您选择 “组织批准”、“资源批准”或 “角色批准”，页面将以相关对象类型的选择区域重新显示。选择列表中所列出的角色、资源和组织仅包括您可以批准的部分。

这样，您可以仅对一个您可以批准的资源委托资源批准。

- **将工作项目委托给** - 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）。
  - **DelegateWorkItemRule** - 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。
- **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。
- **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。

单击**确定**可保存所作的选择，并返回到等待批准的工作项目列表。

结束委托

结束一个或多个委托：

1. 选择 “委托”，然后选择 “当前”。
2. 选择一个或多个要结束的委托，然后单击**结束**。

   Identity Manager 将删除选定的委托配置，并将选定类型的所有已委托工作项目返回到您的暂挂工作项目列表中。

帐户批准

将用户添加到 Identity Manager 系统后，作为*批准者*分配给新帐户的管理员必须对帐户创建进行验证。 Identity Manager 支持适用于这些 Identity Manager 对象的三类批准：

- **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。

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 180 页上的“配置数字签名的批准和操作”。

设置批准者

为上述每一类批准设置批准者都是可选的，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。

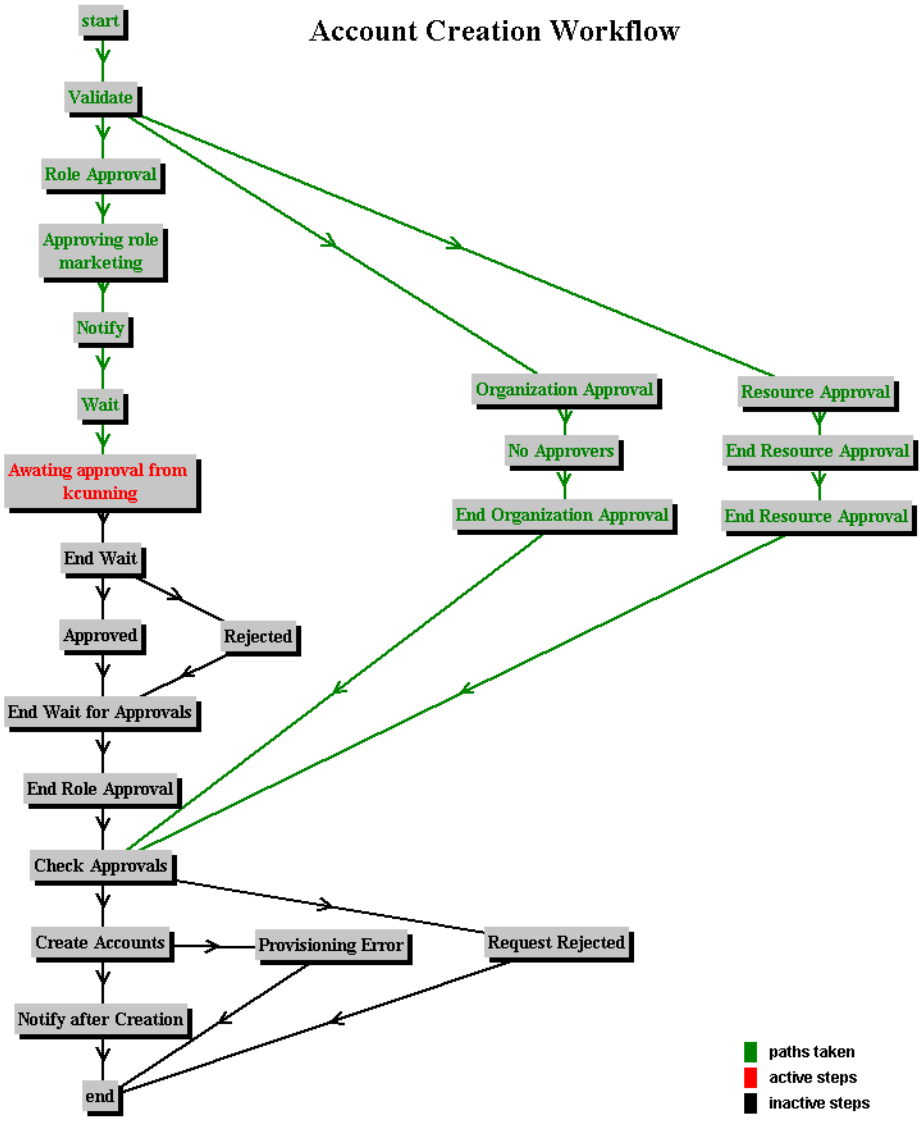
可以将多个批准者分配给各个类别。因为一个类别内只需要一个批准，所以可设置多个批准者，以帮助确保不会延迟或停止工作流。如果一个批准者不可用，则其他批准者可用于处理请求。批准仅适用于帐户创建。默认情况下，帐户更新和删除不需要批准；但是，可以自定义此过程以要求批准。

Identity Manager 以工作流程图的方式说明了帐户创建请求的批准过程和状态。可以通过使用 Identity Manager IDE 自定义工作流，以更改批准流程、捕获帐户删除并捕获更新。

有关 IDE、工作流和更改批准工作流的说明示例的详细信息，请参见 *Identity Manager 工作流、表单和视图*。

图 5-8 说明了帐户创建工作流和批准适合工作流进程的位置。

图 5-8 帐户创建工作流



Identity Manager 批准者可以批准或拒绝批准请求。要使用数字签名批准帐户，必须先按第 180 页上的 “配置数字签名的批准和操作”中所述设置数字签名。

可以在 Identity Manager 界面的 "Work Items" 区域中查看暂挂批准和管理批准。在 "Work Items" 页中，单击 **My Work Items** 以查看暂挂批准。单击 **Approvals** 选项卡以管理批准。

对批准签名

可以按以下步骤对批准签名。

1. 在 Identity Manager 管理员界面中，选择 **Work Items**。
2. 单击 **Approvals** 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 提示是否要信任 applet。
5. 单击 **Always**。

   Identity Manager 将显示带日期的批准摘要。
6. 输入或单击 **Browse** 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 182 页上的 “为获得签名批准的客户端配置”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 182 页上的 “为获得签名批准的客户端配置”过程中的步骤 10l 所述）。
8. 单击 **Sign** 批准请求。

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。可对以下项目进行数字签名：

- 用户批准
- 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。

为获得签名批准的服务器端配置

要启用服务器端配置，请执行以下步骤：

1. 在系统配置中，设置 `security.nonrepudiation.signedApprovals=true`
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：

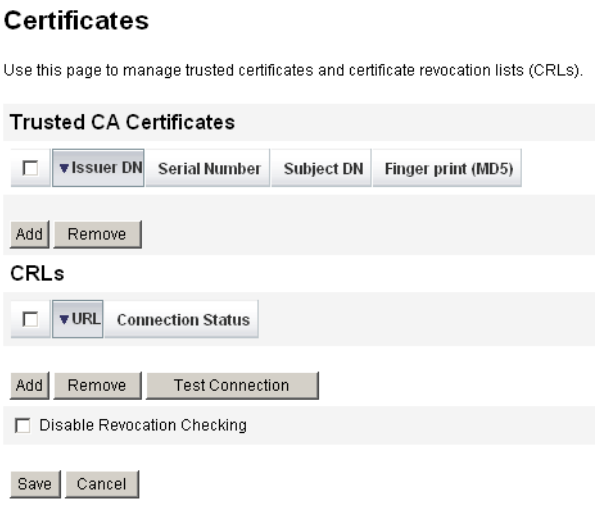
   a. 转到 http://*IPAddress*/certsrv，然后通过管理权限登录。

   b. 选择检索 CA 证书或证书撤销列表，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. 在管理员界面中选择 **Configure**，然后选择 **Certificates**。 Identity Manager 将显示 "Certificates" 页。

图 5-9 证书



   b. 在 "Trusted CA Certificates" 区域中，单击 **Add**。Identity Manager 将显示 "Import Certificate" 页。

c. 浏览到信任证书后将其选中，然后单击 **Import**。

该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 CRL 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 **Test Connection** 验证 URL。

6. 单击 **Save**。

7. 可以使用 jarsigner 对 applets/ts1.jar 签名。

注 有关详细信息，请参阅 http://java.sun.com/j2se/1.4.2/docs/tooldocs/windows/jarsigner.html。Identity Manager 附带的 `ts1.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。

为获得签名批准的客户端配置

要启用客户端配置，请执行以下步骤：

必备条件

客户机系统必须运行安装了 JRE 1.4 或更高版本的 Web 浏览器。

过程

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：

1. 使用 Internet Explorer 浏览到 http://*IPAddress*/certsrv，然后通过管理权限登录。

2. 选择 "Request a certificate"，然后单击 **Next**。
3. 选择 "Advanced request"，然后单击 **Next**。
4. 单击 **Next**。
5. 选择 "User for Certificate Template"。
6. 选择以下选项：
   a. Mark keys as exportable
   b. Enable strong key protection
   c. Use local machine store
7. 单击 **Submit**，然后单击 **OK**。
8. 单击 **Install this certificate**。
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 **Add...**
    c. 选择计算机帐户。
    d. 单击 **Next**，然后单击 **Finish**。
    e. 单击 **Close**。
    f. 单击 **OK**。
    g. 转到**证书 -> 个人 -> 证书**。
    h. 右键单击**管理员所有任务 -> 导出**。
    i. 单击 **Next**。
    j. 单击 **Next** 确认导出专用密钥。
    k. 单击 **Next**。
    l. 输入密码，然后单击 **Next**。
    m. 文件 *CertificateLocation*。
    n. 单击 **Next**，然后单击 **Finish**。单击 **OK** 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。

查看事务签名

按以下步骤查看 Identity Manager 审计日志报告中的事务签名。

1. 在 Identity Manager 管理员界面中选择 **Reports**。
2. 从 "Run Reports" 页的 "New..." 选项列表中选择 "AuditLog Report"。
3. 在 “报告标题”字段中输入标题 （如 “批准”）。
4. 在 "Organizations" 选择区域中，选择所有组织。
5. 选择 "Actions" 选项，然后选择 "Approve"。
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，其中包括：
   - 颁发机构
   - 主题
   - 证书序列号
   - 已签名的消息
   - 签名
   - 签名算法

第 6 章

数据同步与加载

本章介绍有关使用 Identity Manager 数据同步和加载功能的信息和过程。您将了解有关数据同步工具（搜索、协调和同步）以及如何使用这些工具保持数据最新的信息。

数据同步工具：使用哪一个？

按照以下准则选择 Identity Manager 数据同步工具以执行任务。

表 6-1 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
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 *推送到*或 *引入* Identity Manager	使用活动同步适配器进行同步（多个资源实现）

搜索

Identity Manager 帐户搜索功能帮助简化快速部署和加速帐户创建任务。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。

提取到文件

可以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 之前对其进行查看和更改。

要提取帐户：

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

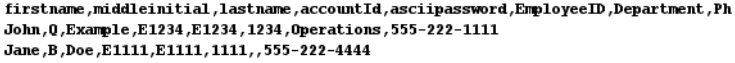
通常，要加载的帐户在一个电子表格中列出并以逗号分隔值 (Comma-separated Value, CSV) 格式保存，以便加载到 Identity Manager 中。 CSV 文件内容必须遵循以下格式准则：

- **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，一个文件的前三行可能类似于下图中的文件条目：

```
firstname,middleinitial,lastname,accountId,asciipassword,EmployeeID,Depart
ment,Phone
John,Q,Example,E1234,E1234,1234,Operations,555-222-1111
Jane,B,Doe,E1111,E1111,1111,,555-222-4444
```

图 6-1 用于加载数据的格式正确的 CSV 文件的示例



在本例中，第二个用户 (Jane Doe) 没有部门。缺少的值用相邻的逗号 (,,) 表示。

注 要在执行加载操作期间启用应用身份属性的功能，请使用元视图将 “从文件加载”添加到身份属性的已启用应用程序列表中。

启用后，加载操作不会显示以下选项：

- 用户表单
- 更新属性
- 合并属性

如果选择**更新帐户**选项，则完全处理所有身份属性，并重新置备帐户。否则只会处理那些来自要加载的文件，且流向身份用户的属性。

要加载帐户：

1. 在菜单栏中选择**帐户**，然后选择**从文件加载**。

   Identity Manager 会显示 “从文件加载”页，可使用该页指定加载选项，然后继续：

   - **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的资源帐户的 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** - 选择此选项只将与现有 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** - 仅在加载帐户过程中生成错误消息时才记录单独的结果。
     - **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。

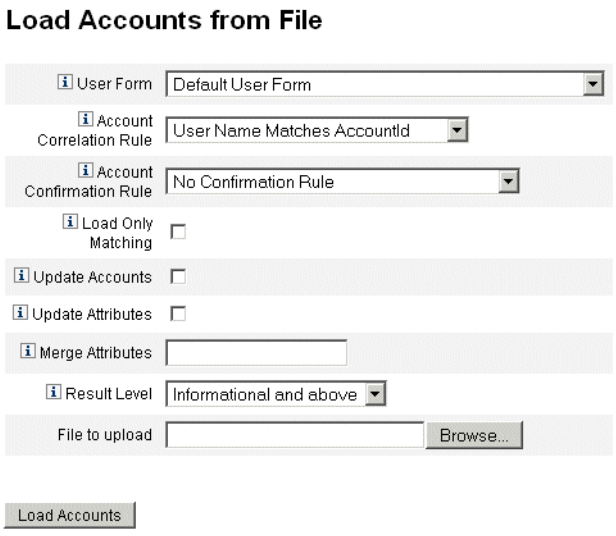
2. 在 "File to Upload" 字段中，指定要加载的文件，然后单击 **Load Accounts**。

注

- 如果输入文件不包含用户列，则为使加载能够正确继续进行，必须选择确认规则。
- 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。

图 6-2 说明了 "Load from File" 屏幕中的可用字段和选项。

图 6-2 从文件加载



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选项直接提取帐户并将其导入 Identity Manager。

要导入帐户，请在菜单栏中选择 **Accounts**，然后选择 **Load from Resource**。

Identity Manager 允许指定加载选项，然后继续。"Load from Resource" 页面与 "Load from File" 页面中的可用加载选项及这些选项的操作结果相同。

注 要在执行加载操作期间启用应用身份属性的功能，请将 “从资源加载”添加到身份属性的已启用应用程序列表中。

启用后，加载操作不会显示以下选项：

- 用户表单
- 更新属性
- 合并属性

如果选择**更新帐户**选项，则完全处理所有身份属性，并重新置备帐户。否则只会处理那些来自要加载的资源，且流向身份用户的属性。

协调

使用协调功能可突出显示 Identity Manager 上的资源帐户与某个资源上实际存在的帐户之间的不一致性，并定期关联帐户数据。

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。 "Resources" 列表显示每个资源上次协调的时间及其当前协调状态。

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。可以将协调配置为检测对帐户属性进行的本机更改（不是通过 Identity Manager 进行的更改）。

编辑协调策略

要编辑协调策略：

1. 在菜单栏中选择 **Resources**。
2. 在 "Resources" 列表分层结构中选择资源。
3. 在 "Resource Actions" 选项列表中选择 **Edit Reconciliation Policy**。

Identity Manager 将显示 "Edit Reconciliation Policy" 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，每台服务器都可以运行协调。请在策略中指定哪台 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 **Do not reconcile** 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 "Inherit" 选项从更高级别策略继承指定的进度表。取消选择 “继承”选项可指定进度表或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。如果选择**继承默认策略**选项，则从较高级别的策略继承进度表。要在策略中指定针对资源运行增量式协调的频率，或者要选择任务进度表重复规则，请取消选择**继承**选项。

  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 **Reconciled Account Attributes** 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的资源帐户的 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 **No Confirmation Rule**， 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。协调只能执行指定的代理管理员可以执行的那些操作。响应将使用与此管理员相关的用户表单 （如需要）。

  还可以选择 “无代理管理员” 选项。如果选择了此选项，则可以查看协调结果，但不运行任何响应操作或工作流。
- **情况选项** （和 “响应”） - 协调会识别多种类型的情况。在 "Response" 列中指定协调应执行的任何操作：
  - **已确认** - 所需帐户存在。
  - **已删除** - 所需帐户不存在。
  - **找到** - 协调进程在分配的资源上找到匹配帐户。
  - **缺少** - 分配给用户的资源上不存在匹配的帐户。
  - **冲突** - 两个或多个 Identity Manager 用户被分配给资源上的同一帐户。
  - **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。

- **不匹配** - 帐户与任何用户都不匹配。
- **有争议** - 帐户与多个用户匹配。

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。

- **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**。

单击 **Save** 以保存策略更改。

启动协调

有两个选项可用于启动协调任务：

- **协调进度表** - 可以在“编辑协调策略”页中设置协调进度表，以定期运行协调。
- **立即协调** - 立即运行协调。要执行此操作，请在资源列表中选择资源，然后在 "Resource Actions" 列表中选择以下选项之一：
  - 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

要取消协调，请选择资源，然后在 "Resource Actions" 列表中选择 **Cancel Reconciliation**。

查看协调状态

"Resources" 列表中的 "Status" 列可报告若干种协调状态。其中包括：

- **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）。

资源上每个帐户的详细状态信息都可用。在列表中选择资源，然后在 "Resource Actions" 列表中选择 **View Reconciliation Status**。

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

要搜索帐户索引，请在 "Resource Actions" 列表中选择 **Search Account Index**。

选择一种搜索类型，然后输入或选择搜索属性。单击 **Search** 以查找与所有搜索条件均匹配的帐户。

- **资源帐户名** - 选择此选项，再选择任一修饰符 （starts with、 contains 或 is），然后输入部分或完整的帐户名称。
- **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，再选择任一修饰符（starts with、 contains 或 is），然后输入部分或完整的拥有者名称。要搜索无拥有者帐户，搜索处于 "UNMATCHED" 或 "DISPUTED" 情况下的帐户。
- **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。

单击 **Search** 以根据搜索参数来搜索帐户。要限制搜索结果，也可在 **Limit results to** 字段中指定数量。默认限制为找到的前 1000 个帐户。

单击 **Reset Query** 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。要执行此操作，请选择 **Resources**，然后选择 **Examine Account Index**。

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 **Group by resource** 索引视图。Identity Manager 会为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 + 或 ñ 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。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 **Group by user** 索引视图。在此视图中，Identity Manager 用户和组织显示为类似 "Accounts List" 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的指示符。在用户名的下方将显示该用户的帐户以及 Identity Manager 已知的帐户的当前状态。

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。

活动同步适配器

Identity Manager 活动功能允许存储在*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。

您可以通过使用元视图，或通过在资源同步策略中指定输入表单 （适用于适当的目标对象类型），来配置资源属性更改流向 Identity Manager 的方式。

使用元视图可指定数据更新的方式，以及指定要为活动同步应用程序启用的身份属性。有关配置身份属性的详细信息，请参见第 118 页上的“配置身份属性和事件”。

继续下一节以配置同步。

配置同步

Identity Manager 使用同步策略启用资源的同步。要配置同步，请在 "Resources" 选项卡上选择您要为其配置同步的资源，然后从 "Resource Actions" 列表中选择 **Edit Synchronization Policy**。

编辑同步策略

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“Service Provider Edition 用户”。

注	在服务提供者实现中，必须配置同步策略 （指定 “Service Provider Edition 用户”为对象类型）以启用这些用户的数据同步。有关服务提供者用户的详细信息，请参见第 13 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。

  "Startup Type" 可以是 "Manual"、 "Automatic"、 "Automatic with Failover" 或 "Disabled"：

  - **“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。

使用 **Start Date** 和 **Start Time** 选项可指定何时开始轮询。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。

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，则 Identity Manager 将根据此信息和轮询间隔来确定轮询的开始时间。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，每台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。
- **普通设置** - 可为数据同步活动指定以下常规设置：
  - **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。此可选配置项目允许在将属性保存到帐户之前对其进行转换。
  - **规则** - 使用该选项可指定数据同步过程中要使用的规则：
    - **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** - 为以下日志记录选项指定值：
  - **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，活动日志将被归档。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 "Maximum Log File Size" 指定的条件进行评估。

    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 "Maximum Active Log Age" 指定的使用期限条件进行评估。
  - **日志级别** - 输入日志记录级别：
    - 0 - 无日志记录
    - 1 - 错误
    - 2 - 信息
    - 3 - 详细
    - 4 - 调试

单击 **Save** 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。在 "Edit Synchronization Policy" 页中，选择 **Disabled** 作为 Identity Manager 用户的 **Startup Type**；对于服务提供者用户，请取消选择 **Enable Synchronization** 选项。将显示警告消息，指示已禁用活动同步。

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 ActiveSync 适配器配置可能影响服务器性能。调谐 ActiveSync 适配器性能涉及以下任务：

- 更改轮询时间间隔
- 指定运行适配器的主机
- 启动和停止
- 适配器日志记录

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 "Resource Actions" 列表的 *Synchronization* 段选择开始、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，请编辑文件 `waveset.properties`。将 `sources.hosts` 属性编辑为以下选项之一：

- 设置 `sources.hosts=`*hostname1,hostname2,hostname3*。这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* 必须与服务器的 Identity Manager 列表中的条目匹配。可以通过 "Configure" 选项卡查看服务器列表。

或者

- 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。服务提供者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 149 页上的 “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 "Synchronization Policy" 的 "Logging" 段为相应的用户类型 （"Identity Manager Users" 或 "Service Provider Users"）指定这些值。

删除适配器日志

只能在适配器已经停止时删除适配器日志。多数情况下会在删除日志之前对其进行复制，以便归档。

第 7 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。

本章分为以下几节：

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** - 可以在此区域定义、运行、删除和下载报告。还可以管理调度的报告。
- **任务** - 定义报告后，可以转至 “任务”区域调度和操作报告任务。

报告

可以从 "Run Reports" 页执行大多数与报告相关的活动，使用该页您可以完成以下报告活动：

- 创建、修改和删除报告
- 运行报告
- 下载报告信息以在其他应用程序（如 StarOffice）中使用。

要查看该页，请在菜单栏中选择 **Reports**。将出现 **Run Reports** 页，其中显示可用报告的列表。

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

图 7-1 显示 "Run Reports" 页的示例。

图 7-1 "Run Reports" 选项

使用以下方法之一开始定义报告：

- 创建报告。
- 选择要修改的报告，然后使用新名称保存 （也称为报告克隆）。

创建报告

要创建报告，请执行以下步骤：

1. 在菜单栏中选择 **Reports**。
2. 选择报告类别："**Identity Manager Reports**" 或 "**Auditor Reports**"，然后从 **New** 选项列表中选择报告类型。

Identity Manager 将显示 "Define a Report" 页，在此页中可选择和保存用来创建报告的选项。

克隆报告

要克隆报告，请从列表中选择一个报告。输入新报告名称，并调整报告参数（可选），然后单击 **Save** 用新名称保存报告。

用电子邮件发送报告

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。

还可以选择要附加到电子邮件的报告格式：

- **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。

运行报告

输入并选择了报告条件后，您可以执行以下操作：

- 运行报告但不保存 - 单击**运行**可运行报告。 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**可保存报告。保存后，您可从 "Run Reports" 页 （报告的列表）运行报告。

调度报告

根据您希望立即运行报告，还是希望进行调度以使之按固定时间间隔运行，可以做出不同的选择：

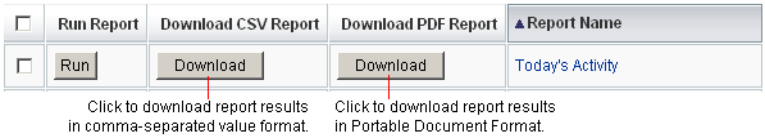
- **报告 > 运行报告** - 允许立即运行保存的报告。在报告列表中，单击 **Run**。Identity Manager 将运行报告，然后以摘要和明细格式显示结果。
- **任务 > 调度任务** - 调度要运行的报告任务。选择报告任务后，可以设置报告的频率和选项。还可以调整报告的具体细节 （就如同在 "Define a Report" 页的 "Reports" 区域中一样）。

下载报告数据

从 "Run Reports" 页，在以下任一列中单击 **Download**：

- **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。

图 7-2 下载报告



为报告输出配置字体

对于以可移植文档格式 (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。

要配置报告字体选项，请单击 **Reports**，然后选择 **Configure**。可使用以下选项：

- **PDF 报告选项**
  - **PDF 字体名称** - 选择在生成 PDF 报告时要使用的字体。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 "Embed Font in PDF Documents" 选项。
  - **PDF 文档中的嵌入字体** - 选择此选项可以在生成的 PDF 报告中嵌入字体定义。这将保证在任意 PDF 查看器中可以查看该报告。

注 嵌入字体会极大地增加文档的大小。

- **CSV 报告选项** - 选择生成报告时要使用的字符集。

单击**保存**可以保存报告配置选项。

报告类型

Identity Manager 提供多种报告类型：

- 审计者
- 审计日志
- 实时
- 摘要
- 系统日志
- 使用情况

可通过以下其中一种报告类别或这两种报告类别访问这些报告：

- Identity Manager 报告
- Auditor 报告

审计者

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。有关审计策略和 Auditor 报告的详细信息，请参见第 11 章 “身份审计”。

Identity Manager 提供以下 Auditor 报告：

- 访问查看报告
- 审计策略扫描
- 审计策略摘要报告
- 已审计的属性报告
- 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
- 违规摘要报告
- 任务划分报告

要定义 Auditor 报告，请选择 "Run Reports" 页上的 **Auditor Reports** 选项，然后从 "Auditor Reports" 列表中选择报告。有关审计者报告的详细信息，请参见第 11 章 “身份审计”。

审计日志

审计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、密码更改和重置、自置备活动、策略违规、服务提供者（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 **Configure**，然后选择 **Audit**。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 131 页上的 “配置审计组和审计事件”。

您可以通过从 "Run Reports" 页上的报告选项列表中选择 "AuditLog Report" 来运行该报告。从 Identity Manager 报告和 Auditor 报告类别中均可找到该报告。

设置并保存报告参数后，便可以从 "Run Reports" 列表页运行该报告。单击 **Run** 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。

实时

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** - 概述组属性，包括用户成员资格。
- **资源状态** - 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** - 列出用户资源帐户和帐户属性。

要定义实时报告，请从 "Run Reports" 页上的 **Identity Manager Reports** 列表中选择一个报告选项。

设置并保存报告参数后，便可以从 "Run Reports" 列表页运行该报告。单击 **Run** 生成一个包含所有符合保存条件的结果的报告。

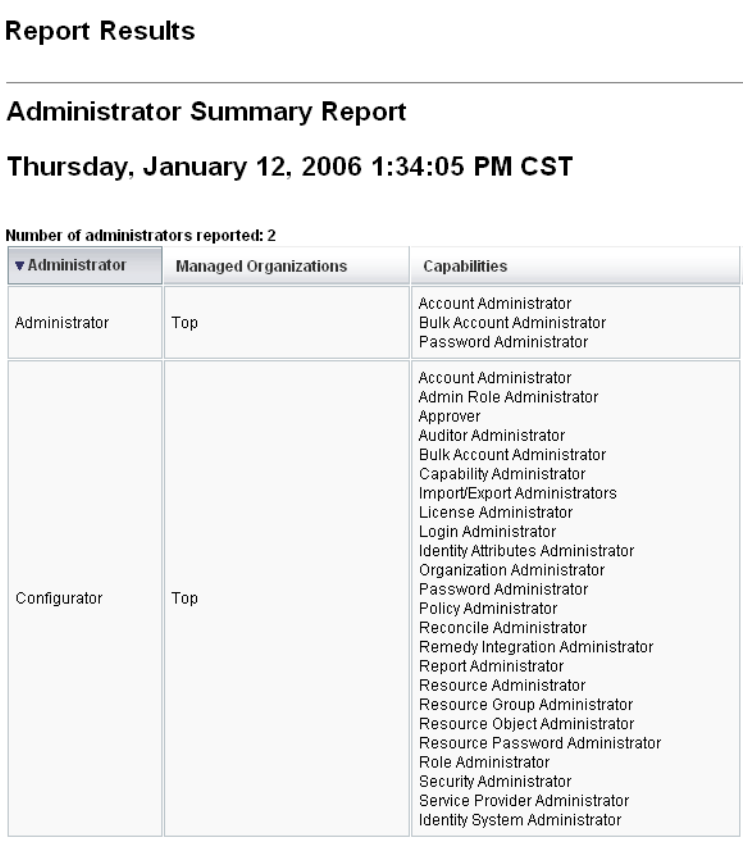
摘要报告

摘要报告类型包括 **Identity Manager 报告**列表中的以下报告：

- **帐户索引** - 根据协调情况报告选定的资源帐户。
- **管理员** - 查看 Identity Manager 管理员、管理员所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** - 列出分配了管理员角色的用户。
- **角色** - 概述 Identity Manager 角色及关联的资源。定义角色报告时，可以按相关组织选择要包含的角色。
- **任务** - 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** - 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** - 允许管理员查找未回答最小数量的验证问题的用户，此数量由帐户策略要求指定。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。

如下图所示，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。

图 7-3 管理员摘要报告



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

系统日志

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内容：

- 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，要在 "Recent Systems Messages" 报告中查看特定条目，请编辑该报告并选择 **Event** 字段，然后输入请求的 syslog ID 并单击 **Run**。

注 也可运行 `lh syslog` 命令从系统日志中提取记录。有关命令选项的详细信息，请参阅附录 A “lh 参考消息”中的 “syslog 命令”。

要定义系统日志报告，请从 "Run Reports" 页上的报告选项列表中选择 **SystemLog Report**。

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或表格摘要。可以采用饼图、条形图或表格形式显示输出。

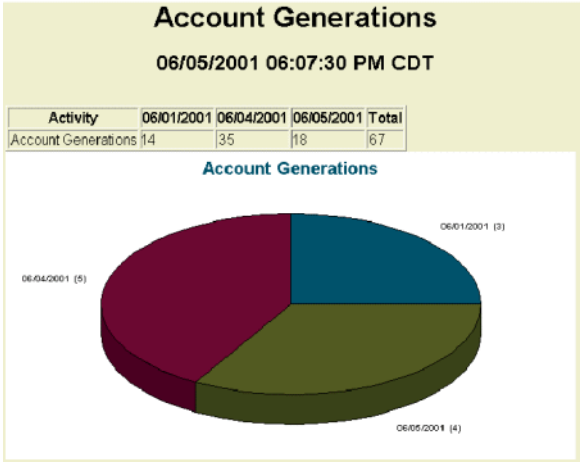
要定义使用情况报告，请从 "Run Reports" 列表页上的报告选项列表中选择 **Usage Report**。

设置并保存报告参数后，便可以从 "Run Reports" 列表页运行该报告。

使用情况报告图表

在下图中，上方的表格显示报告包含的事件。下方的图表以图形形式显示相同的信息。将鼠标指针移至饼图任一部分之上时，即会显示该部分的值。

图 7-4 使用情况报告 （生成的用户帐户）



可以对饼图的各部分进行操作以突出显示它们。右键单击并按住某个数据片，然后将其拖离饼图中心，以与其他数据片分开显示。您可以对饼图的一个或多个部分执行此操作。对于大多数控制，请单击中心附近的数据片，以便允许您将其拖到与其余数据片相距更远的位置。

也可以旋转饼图以获得所需的视图。单击并按住饼图边缘附近，然后将鼠标移向右侧或左侧来旋转视图。

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、Windows NT 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` 页的 RiskReportTask 对象下找到一个表单列表，然后可以使用业务进程编辑器对它们进行修改。有关配置 Identity Manager 表单的详细信息，请参见 *Identity Manager 工作流、表单和视图*。

要创建风险分析报告，请在菜单栏中单击 **Risk Analysis**，然后从 "New" 选项列表中选择一个报告。

可以将报告限制为仅扫描选定的资源；根据资源的类型，可以扫描以下帐户：

- 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。

定义完成后，可以将风险分析报告调度为按指定间隔运行。

1. 单击 **Schedule Tasks**，然后选择要运行的报告。
2. 在 "Create Task Schedule" 页，输入名称和进度表信息，然后调整其他风险分析选项 （可选）。
3. 单击 **Save** 以保存该进度表。

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 提供了样例 *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 217 页上的 “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 "Configure Reports" 页的 "Tracked Event Configuration" 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 **Enable event collection** 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事件的时区。这主要确定日期边界开始的时间。

  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。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。

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
- 创建图形
- 编辑图形
- 删除图形

查看定义的图形

Identity Manager 提供一些样例图形。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。

1. 在菜单栏中单击 **Reports**。
2. 单击 **Dashboard Graphs**。
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 **Pause refresh** 以暂停面板刷新。单击 **Resume** 以更新视图。

注 对于包含多个图形的面板，有时在初始加载所有图形前暂停刷新很有用。

6. 如果需要，单击 **Refresh now** 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 如果任何一个图形显示了错误消息，请使用调试页设置 "System Configuration" 配置对象中的 `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。

创建图形

可以使用以下步骤创建面板图形：

1. 从菜单栏中选择 **Reports**。
2. 选择**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**新建**以显示 “创建面板图形” 页。
5. 输入 **Graph Name**。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。

6. 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。

7. 从列表中选择所需类型的 **Tracked Event**。

   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** - 跟踪资源操作数。
   - **资源操作持续时间** - 跟踪资源操作的持续时间。
   - **工作流持续时间** - 跟踪执行工作流所花费的时间。
   - **工作流执行计数** - 跟踪执行每个工作流的次数。

8. 从列表中选择 **Time Scale**。

   它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。

9. 从列表中选择 **Metric**。根据选定的跟踪事件，将选择一个默认值（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。可能的度量有：

   - Count - 时间间隔内事件发生的总次数
   - Average - 时间间隔内事件值的算术平均值
   - Maximum - 时间间隔内的最大事件值
   - Minimum - 时间间隔内的最小事件值
   - Histogram - 分别计数时间间隔内各个离散区域的事件值

10. 从列表中选择 **Show count as**。

    图形计数显示为原始总数或按不同的时间范围进行划分。

11. 从列表中选择 **Graph Type**。

    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。

基本尺寸

12. 如果需要，从列表中选择以下选项：

    - **Resource Name**。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。
    - **Server Instance**。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。
    - **Operation Type**。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。

图形选项

13. 如果需要，输入 **Graph Subtitle**

    这会在图形的主标题下面产生一个副标题。

高级图形选项

14. 如果需要，请选择 **Advanced Graph Options**。如果您要设置以下选项，请选择该选项：

    - **Grid Lines**
    - **Font**
    - **Color Palette**

15. 单击 **Save** 以创建图形。

编辑图形

可通过以下方法编辑图形：选择**报告**选项卡，从 “选择面板图形类型”选项列表中选择一类面板图形，然后从列表中选择图形名称。

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：

- **Graph Name** - 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、 SPE（服务提供者）和 IDM。
- **Tracked Event** - 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。
- **Time Scale** - - 控制数据聚集的频率及其保留的频率。
- **Metric** - 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。
- **Graph type** - 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。
- **Graph Subtitle** - 如果需要，请在图形主标题下输入副标题。
- **Advanced Graph Options** - 如果您要设置以下选项，请选择该选项：
  - **Grid Lines**
  - **Font**
  - **Color Palette**

16. 单击 **Save**。

删除图形

通过从列表中选择图形并单击**删除**，可以删除图形。

注	删除某个图形会自动将其从所有包含该图形的面板中删除，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 提供了一组样例面板，建议管理员使用这些样例面板自定义他们自己的部署。有关说明，请参见第 218 页上的 “创建面板”。

"Reports" 菜单中的以下区域允许您使用面板。

您可以在 Identity Manager 界面的 **Reports** 区域中查看现有的面板。单击 "View Dashboards"、**Dashboard Graphs** 以列出当前定义的面板，然后单击要查看的面板旁的 **Display**。

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 **Pause** 以暂停面板刷新或单击 **Refresh** 以更新视图。

以下各节提供了使用面板的步骤：

- 创建面板
- 编辑面板
- 删除面板

创建面板

要创建面板，请执行以下步骤：

1. 在菜单栏中单击 **Reports**。
2. 单击 **View Dashboards**。
3. 单击 **New**。
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 **Save**。

编辑面板

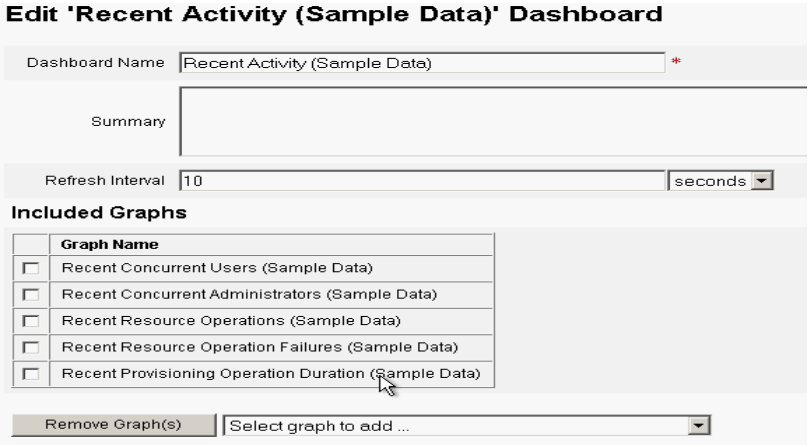
使用创建面板中描述的步骤编辑面板 （除选择 "New" 外），选择要修改的面板并编辑以下属性：

- 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 7-5 说明了样例面板编辑页。

图 7-5 编辑面板



删除面板

要删除服务提供者面板，请在 "Service Provider" 区域中单击 **Manage Dashboards**，然后选择所需的面板并单击 **delete**。

注 使用上述步骤不会删除包含在面板中的图形。请使用 "Manage Dashboard Graphs" 页删除图形 （请参见 “删除图形”）。

搜索事务

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。

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 "Search Transactions" 页您可以搜索 "Transaction Persistent Store" 中的事务。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。

要搜索事务：

1. 登录到 Identity Manager。
2. 在菜单栏中单击 **Service Provider**。
3. 单击 **Search Transations**。

   将显示 **Search Conditions** 页。

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 Identity Manager 中的 **"Accounts"-> "Find Users"** 页。

4. 如果需要，请选择 **User Name**。

   这允许您仅搜索与具有您输入的 **accountId** 的用户相对应的事务。

注 如果您在 Service Provider Edition 事务配置页中配置了所有自定义的可查询用户属性，则这些属性将在此处显示。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。

5. 如果需要，请选择针对 **Type** 搜索。

   这允许您搜索选定类型的事务。

6. 如果需要，请选择针对 **State** 搜索。

   这允许您搜索处于以下选定状态的事务：

   - **Unattempted** 表示尚未尝试的事务。
   - **Pending retry** 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。
   - **Success** 表示已经成功完成的事务。
   - **Failure** 表示已经完成但具有一个或多个故障的事务。

7. 如果需要，请选择针对 **Attempts** 搜索。

   这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。

8. 如果需要，请选择针对 **Submitted** 搜索。

   这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。

9. 如果需要，请选择针对 **Completed** 搜索。

   这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。

10. 如果需要，请选择针对 **Cancelled Status** 搜索。

    这允许您根据事务是否已取消搜索这些事务。

11. 如果需要，请选择针对 **Transaction ID** 搜索。

    这允许您根据事务唯一的 ID 搜索这些事务。使用该选项可以根据您输入的出现在所有审计日志记录中的 ID 值查找事务。

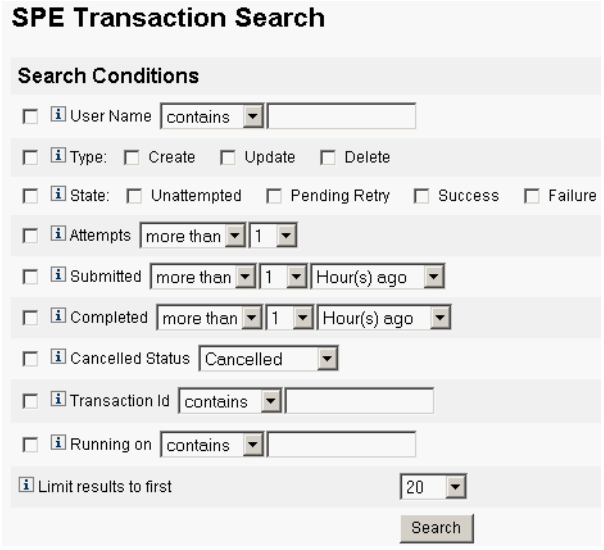
12. 如果需要，请选择针对 **Running On**（哪一台服务器）搜索。

    这允许您根据运行事务的 Service Provider Edition 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。

13. 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 7-6 搜索事务



14. 单击 **Search**。

    将显示搜索结果。

15. 如果需要，请单击结果页面底部的 **Download All Matched Transactions**。这将把结果保存为 XML 格式的文件。

注 您可以取消搜索结果中返回的事务。选择结果表中的事务，然后单击 **Cancel Selected**。您无法取消已完成或已被取消的事务。

第 8 章

任务模板

Identity Manager 的*任务模板*使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。

本章中的以下主题介绍了如何将任务模板用于您的系统以及如何使用任务模板来配置工组流行为：

启用任务模板

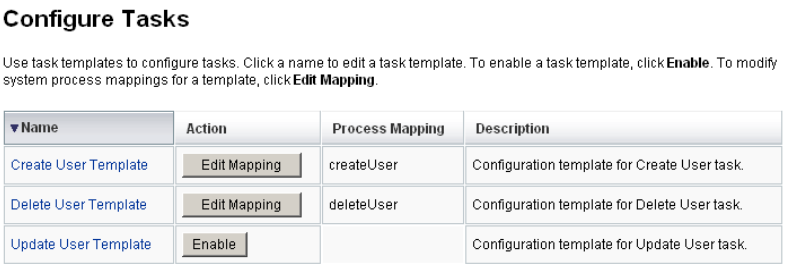
Identity Manager 提供了以下可以配置的任务模板：

- **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，必须映射任务模板进程。要映射进程类型，请执行以下步骤：

1. 从 Identity Manager 管理员界面中，选择 **Tasks**，然后选择 **Configure Tasks**。图 8-1 说明了 "Configure Tasks" 页。

图 8-1 Configure Tasks



"Configure Tasks" 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。

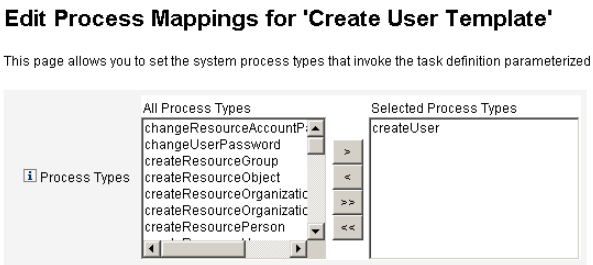
启用和编辑进程映射的过程是相同的。

- **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 **Enable** 打开模板的 "Edit Process Mappings" 页。

   例如，针对创建用户模板将显示以下页面 （图 8-2）：

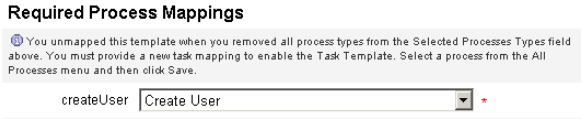
图 8-2 "Edit Process Mappings" 页



注 默认进程类型 （在本例中，为 `createUser`）自动显示在 "Selected Process Types" 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 "Selected Process Types" 列表中删除进程类型而不选择替换的进程类型，则将显示 "Required Process Mappings" 部分，指示您选择新任务映射。

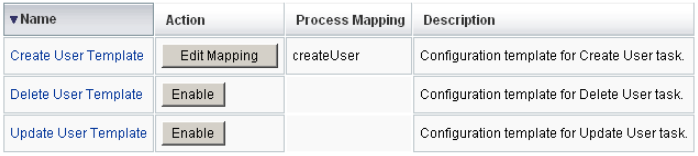
图 8-3 "Required Process Mappings" 部分



3. 单击 **Save** 以映射选定的进程类型，并返回 "Configure Tasks" 页。

注 重新显示 "Configure Tasks" 页后， **Edit Mapping** 按钮将替换 **Enable** 按钮，而进程名称将列在 "Process Mapping" 列中。

图 8-4 更新后的 "Configure Tasks" 表



4. 为其余每个模板重复映射进程。

注

- 可以通过选择 **Configure > Form and Process Mappings** 来验证映射。显示 "Configure Form and Process Mappings" 页后，向下滚动到 "Process Mappings" 表，验证以下进程类型已映射至表中显示的 "Process Name Mapped To" 条目。

进程类型	Process Name Mapped To
createUser	创建用户模板
deleteUser	Delete User Template
updateUser	Update User Template

  如果成功启用模板，则 "Process Name Mapped To" 条目应该全部包含词 *Template*。

- 如果按上表所示在 **Process Name Mapped To** 列中键入 **`Template`**，则还可以直接通过此页映射这些进程类型。

成功映射模板进程类型后，可以配置任务模板。

配置任务模板

要配置各种任务模板，请按照以下步骤操作：

1. 在 "Task Template" 表中选择 "Name" 链接。将显示以下页面之一：
   - **编辑任务模板创建用户模板** - 打开此页可以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** - 打开此页可以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** - 打开此页可以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。

表 8-1 任务模板选项卡

选项卡名称	用途	模板
General （*默认选项卡*）	使您可以定义在 "Home" 和 "Account" 页上的任务栏中以及 "Tasks" 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
	使您可以指定如何删除/取消置备用户帐户	仅适用于删除用户模板
Notification	使您可以配置 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	使您可以按类型启用或禁用批准、指定其他批准者以及在 Identity Manager 执行某些任务之前指定帐户数据的属性。	所有模板
Audit	使您可以启用和配置工作流的审计。	所有模板
Provisioning	使您可以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	使您可以在指定日期/时间执行创建任务 （*生效*），或在指定日期/时间执行删除任务 （*失效*）。	仅适用于创建用户任务模板
Data Transformations	使您可以配置在置备期间如何转换用户数据。	仅适用于创建用户和更新用户任务模板

2. 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 228 页上的 “配置 "General" 选项卡”
   - 第 230 页上的 “配置 "Notification" 选项卡”
   - 第 235 页上的 “配置 "Approvals" 选项卡”
   - 第 247 页上的 “配置 "Audit" 选项卡”
   - 第 248 页上的 “配置 "Provisioning" 选项卡”
   - 第 249 页上的 “配置 "Sunrise and Sunset" 选项卡”
   - 第 254 页上的 “配置 "Data Transformations" 选项卡”

3. 配置完模板后，单击 **Save** 按钮以保存所做的更改。

配置 "General" 选项卡

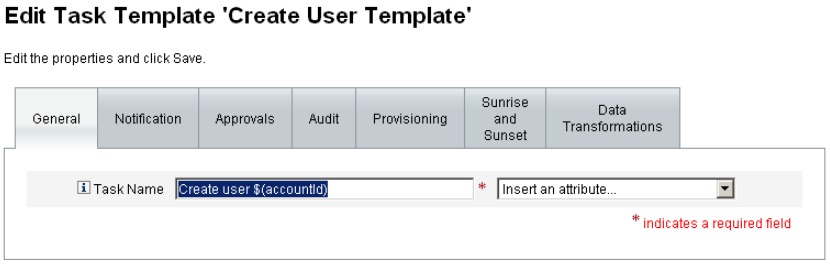
本节提供配置 "General" 选项卡的说明。

注 由于"Create User Template" 和 "Update User Template" 的 "Edit Task Template" 页是相同的，因此在同一小节中说明这两张选项卡的配置。

对于创建用户模板或更新用户模板

默认情况下，打开 "Edit Task Template Create User Template" 或 "Edit Task Template Update User Template" 后，将显示 "General" 选项卡页。此页如下图所示，由 "Task Name" 文本字段和菜单构成。

图 8-5 "General" 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。

要更改默认任务名称，请执行以下步骤：

1. 在 **Task Name** 字段中键入名称。

   可以编辑或完全替换默认的任务名称。

2. **Task Name** 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 "Task Name" 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 **Save** 以保存更改并返回到 "Configure Tasks" 页。
- 在 "Home" 和 "Accounts" 选项卡底部的 Identity Manager 任务栏中，将显示新的任务名称。
- 单击 **Cancel** 以放弃更改并返回到 "Configure Tasks" 页。

对于删除用户模板

默认情况下，打开 "Edit Task Template Delete User Template" 后，将显示 "General" 选项卡页。

要指定如何删除/取消置备用户帐户，请执行以下步骤：

1. 使用**"Delete Identity Manager Account"** 按钮可以指定是否可以在删除操作期间删除 Identity Manager 帐户，选项如下：
   - **永不** - 启用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** - 如果启用此按钮，则仅当用户帐户在取消置备后没有链接的资源帐户时才可以删除用户帐户。
   - **始终** - 启用此按钮可以始终允许删除用户帐户，即使仍分配有资源帐户。
2. 使用 **"Resource Accounts Deprovisioning"** 框可以控制*所有*资源帐户的取消置备操作，选项如下：
   - **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 系统与资源帐户的全部链接。如果尚未链接分配给用户的帐户，则用户将以带有徽章的形式显示，以表明需要更新。

注 这些控制选项将覆盖在 "Individual Resource Accounts Deprovisioning" 表中的选择。

---

3. 使用 **Individual Resource Accounts Deprovisioning** 框以允许对用户取消置备操作（与资源帐户取消置备操作进行比较）进行如下细化选择：
   - **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。

- **取消链接** - 启用此框可以断开 Identity Manager 系统与资源帐户的链接。如果尚未链接分配给用户的帐户，则用户将以带有徽章的形式显示，以表明需要更新。

注 如果要为不同的资源分别指定取消置备策略，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。

4. 完成后，可以
   - 选择其他选项卡以继续编辑模板。
   - 单击 **Save** 以保存更改并返回到 "Configure Tasks" 页。
   - 单击 **Cancel** 以放弃更改并返回到 "Configure Tasks" 页。

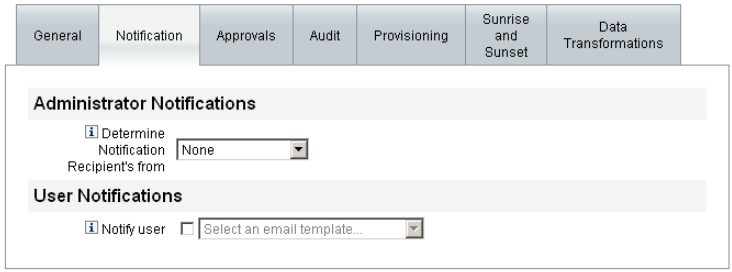
配置 "Notification" 选项卡

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 "Notification" 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 电子邮件模板的更多信息，请参见本指南中标题为 “了解电子邮件模板”的一节。

下图显示了创建用户模板的 "Notification" 页。

图 8-6 "Notification" 选项卡：创建用户模板



要指定 Identity Manager 确定通知收件人的方式，请完成以下进程：

1. 完成 "Administrator Notifications" 部分。
2. 完成 "User Notifications" 部分。
3. 完成后，可以
   - 选择其他选项卡以继续编辑模板。
   - 单击 **Save** 以保存更改并返回到 "Configure Tasks" 页。
   - 单击 **Cancel** 以放弃更改并返回到 "Configure Tasks" 页。

配置管理员通知

从 **Determine Notification Recipients from** 菜单选择选项以决定通知管理员收件人的方法。

- **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。继续第 231 页上的 “通过属性指定收件人”。
- **规则** - 选择此选项可以按照指定规则进行评估，以获取通知收件人的帐户 ID。继续第 232 页上的 “通过规则指定收件人”。
- **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。继续第 233 页上的 “通过查询指定收件人”。
- **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。继续第 234 页上的 “通过管理员列表指定收件人”。

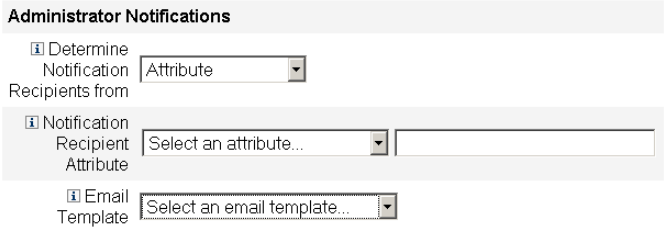
通过属性指定收件人

要通过特定属性获取通知收件人的帐户 ID，请执行以下步骤：

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。

1. 从 **Determine Notification Recipients from** 菜单中选择 **Attribute**，将显示以下新选项：

图 8-7 Administrator Notifications：属性



   - **通知收件人属性** - 提供用于确定收件人帐户 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 **Notification Recipient Attribute** 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。

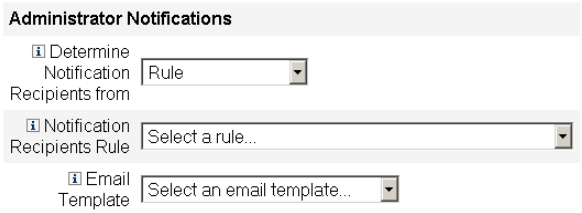
通过规则指定收件人

要通过特定规则获取通知收件人的帐户 ID，请执行以下步骤：

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。

1. 从 **Determine Notification Recipients from** 菜单中选择 **Rule**， "Notification" 表单中将显示以下新选项：

图 8-8 Administrator Notifications：Rule



- **通知收件人规则** - 提供评估后返回收件人帐户 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 **Notification Recipient Rule** 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。

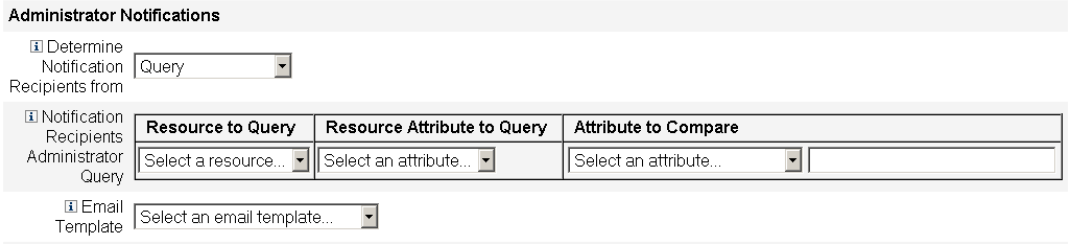
通过查询指定收件人

注 目前只支持 LDAP 和 Active Directory 资源查询。

要通过查询特定资源获取通知收件人的帐户 ID，请执行以下步骤：

1. 从 **Determine Notification Recipients from** 菜单中选择 **Query**，"Notification" 表单中将显示以下新选项，如图 8-9 中说明：

图 8-9 管理员通知：查询



- **通知收件人管理员查询** - 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。

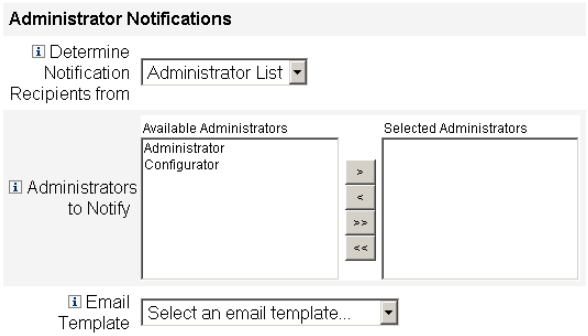
- **要查询的资源属性** - 提供当前为系统定义的资源属性列表。
- **要比较的属性** - 提供当前为系统定义的属性列表。
- **电子邮件模板** - 提供电子邮件模板的列表。

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收件人

从 **Determine Notification Recipients from** 菜单中选择 **Administrators List**，"Notification" 表单中将显示以下新选项：

图 8-10 Administrator Notifications：Administrators List



- **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。

4. 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。
5. 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。

要创建、更新或删除用户通知用户，请启用 **Notify user** 复选框，如图 8-11 中所示，然后从该列表中选择电子邮件模板。

图 8-11 指定电子邮件模板

配置 "Approvals" 选项卡

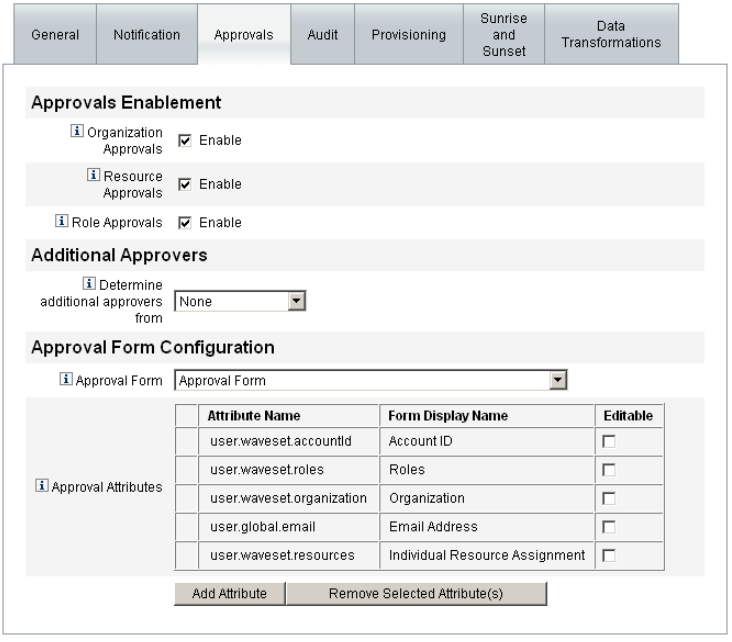
可以使用 "Approvals" 选项卡指定附加批准者，并在 Identity Manager 执行创建、删除或更新用户任务之前指定任务批准表单的属性。

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*其他批准者* - 需要批准任务的其他管理员。

注 如果在工作流中配置了附加批准者，则需要原有批准者*和*在模板中指定的所有附加批准者的共同批准。

下图说明初始 "Approvals" 页的管理用户界面。

图 8-12 "Approvals" 选项卡：创建用户模板



要配置批准，请执行以下步骤：

1. 完成 "Approvals Enablement" 部分 （请参见第 236 页上的 “启用批准”）。
2. 完成 "Additional Approvers" 部分（请参见第 236 页上的“指定附加批准者”）。
3. 完成 "Approval Form Configuration" 部分 （仅适用于创建用户模板和更新用户模板）（请参见第 244 页上的 “配置批准表单”）。
4. 配置完 "Approvals" 选项卡后，可以
   - 选择其他选项卡以继续编辑模板。
   - 单击 **Save** 以保存更改并返回到 "Configure Tasks" 页。
   - 单击 **Cancel** 以放弃更改并返回到 "Configure Tasks" 页。

启用批准

如果使用以下 **Approvals Enablement** 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，已针对创建用户模板和更新用户模板启用这些复选框，但对于删除用户模板却是*禁用的*。

- **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

使用 **Determine additional approvers from** 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。此菜单上的选项包括：

表 8-2 "Determine additional approvers from" 菜单选项

选项	描述
None （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。
Rule	批准者的帐户 ID 是按照特定 规则进行评估而获取的。
Query	批准者的帐户 ID 是通过查询特定资源而获取的。

表 8-2 "Determine additional approvers from" 菜单选项

选项	描述
Administrator List	直接从列表中选择批准者。

选择这些选项中的任何一个（除 **None** 以外），管理用户界面中都将显示附加选项。将从第 236 页开始说明如何配置这些选项。

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 （第 237 页）
- 通过规则 （第 238 页）
- 通过查询 （第 239 页）
- 通过管理员列表 （第 240 页）

通过属性

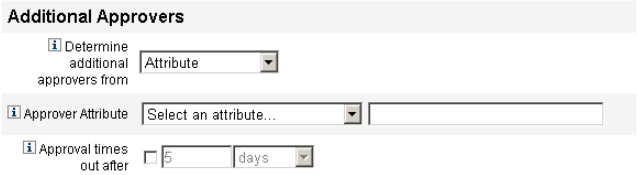
要通过属性决定附加批准者，请执行以下步骤：

1. 从 **Determine additional approvers from** 菜单中选择 **Attribute**。

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。

将显示以下新选项：

图 8-13 Additional Approvers：属性



- **批准者属性** - 提供用于确定批准者帐户 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** - 提供方法以指定批准超时。

注 **Approval times out after** 设置对原始批准和提升批准都起作用。

2. 通过 **Approver Attribute** 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 241 页上的“配置批准超时”以获取有关说明。
   - 如果不打算指定超时时间段，则可以继续第 244 页上的 “配置批准表单”，或保存更改然后配置其他选项卡。

通过规则

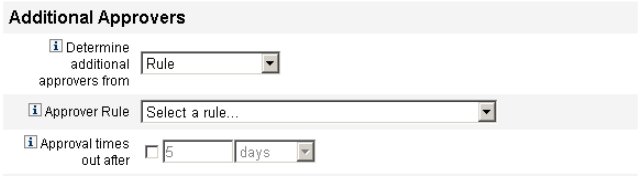
要通过特定规则获取批准者的帐户 ID，请执行以下步骤：

1. 从 **Determine additional approvers from** 菜单中选择 **Rule**。

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。

将显示以下新选项。

图 8-14 Additional Approvers：Rule



- **批准者规则** - 提供评估后返回收件人帐户 ID 的规则（当前为系统定义）列表。
- **批准超时期限** - 提供方法以指定批准超时。

注 **Approval times out after** 设置对原始批准和提升批准都起作用。

2. 从 **Approver Rule** 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 241 页上的“配置批准超时”以获取有关说明。
   - 如果不打算指定超时时间段，则可以继续第 244 页上的 “配置批准表单”，或保存更改然后配置其他选项卡。

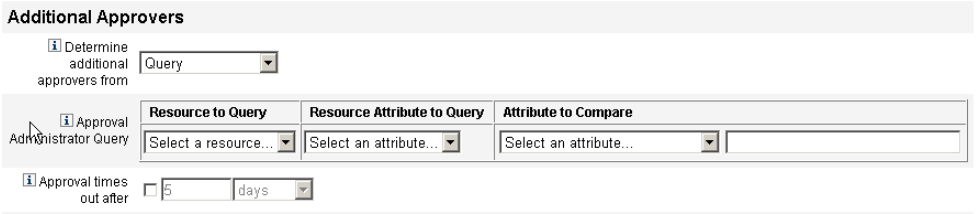
通过查询

注 目前只支持 LDAP 和 Active Directory 资源查询。

要通过查询特定资源获取批准者帐户 ID，请执行以下步骤：

1. 从 **Determine additional approvers from** 菜单中选择 **Query**，将显示以下新选项：

图 8-15 Additional Approvers：Query



- **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** - 提供方法以指定批准超时。

注 **Approval times out after** 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 **Resource to Query** 菜单中选择资源。
   b. 从 **Resource Attribute to Query** 和 **Attribute to Compare** 菜单中选择属性。

3. 决定是否要为批准请求指定超时值。

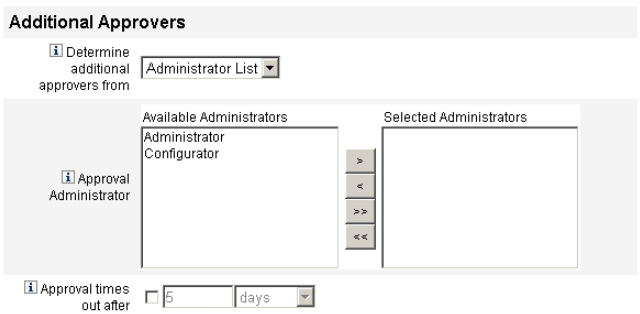
   - 如果要指定超时时间段，请继续阅读第 241 页上的“配置批准超时”以获取有关说明。
   - 如果不打算指定超时时间段，则可以继续第 244 页上的 “配置批准表单”，或保存更改然后配置其他选项卡。

通过管理员列表

要直接从管理员列表中选择附加批准者，请执行以下步骤：

1. 从 **Determine additional approvers from** 菜单中选择 **Administrators List**，将显示以下新选项：

图 8-16 Additional Approvers：Administrators List



   - **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** - 提供方法以指定批准超时。

注 **Approval times out after** 设置对原始批准和提升批准都起作用。

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 241 页上的“配置批准超时”以获取有关说明。

- 如果不打算指定超时时间段，则可以继续第 244 页上的 “配置批准表单”，或保存更改然后配置其他选项卡。

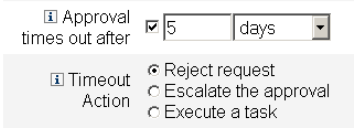
配置批准超时

要配置批准超时，请执行以下步骤：

1. 启用批准超时复选框。

   旁边的文本字段和菜单将变为活动状态，并显示 **Timeout Action** 按钮，如下图中所示。

图 8-17 批准超时选项



2. 使用 **Approval times out after** 文本字段和菜单可以指定超时时间段，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 **Approval times out after** 设置对原始批准和提升批准都起作用。

3. 启用以下**超时操作**按钮之一，以指定批准请求超时后将采取的操作：

   - **拒绝请求** - 如果在指定的超时值之前没有批准， Identity Manager 将自动拒绝请求。
   - **提升批准** - 如果在指定的超时值之前没有批准， 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 242 页上的 “提升批准”以获取有关说明。
   - **执行任务** - 如果在指定的超时值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 **Approval Timeout Task** 菜单，可以通过该菜单指定批准请求超时后要执行的任务。请继续阅读第 243 页上的 “执行任务”以获取有关说明。

提升批准

启用 "Timeout Action" 旁的 **Escalate the approval** 按钮后，将显示以下 **Determine escalation approvers from** 菜单：

图 8-18 "Determine Escalation Approvers From" 菜单

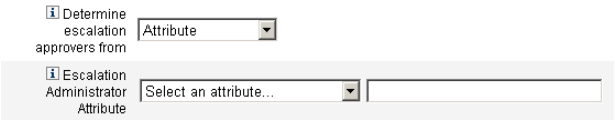
从该菜单中选择以下选项之一来指定如何确定提升批准的批准者。

- **属性** - 根据新用户视图中指定的属性确定批准者帐户 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。

  显示 **Escalation Administrator Attribute** 菜单时，从列表中选择属性。所选属性将显示在旁边的文本字段中。

  图 8-19 "Escalation Administrator Attribute" 菜单

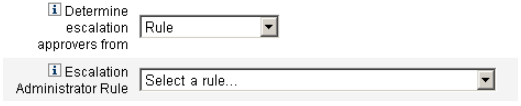
  

- **规则** - 按照特定规则进行评估，以确定批准者帐户 ID。

  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。

  显示 **Escalation Administrator Rule** 菜单时，从列表中选择规则。

  图 8-20 "Escalation Administrator Rule" 菜单

- **查询** - 通过查询特定资源确定批准者帐户 ID。

  显示 **Escalation Administrator Query** 菜单时，按以下步骤构建查询：

  a. 从 **Resource to Query** 菜单中选择资源。

  b. 从 **Resource Attribute to Query** 菜单中选择属性。

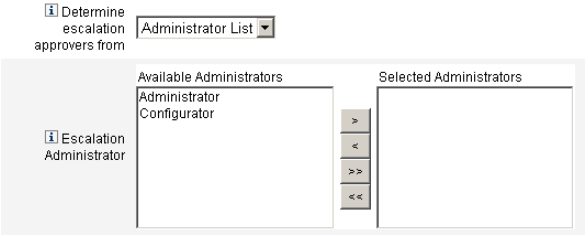
  c. 从 **Attribute to Compare** 菜单中选择属性。

图 8-21 "Escalation Administrator Query" 菜单

- **管理员列表**（默认） - 直接从列表中选择 批准者。

  显示**提升管理员**选择工具后，按以下步骤选择批准者：

图 8-22 "Escalation Administrator" 选择工具



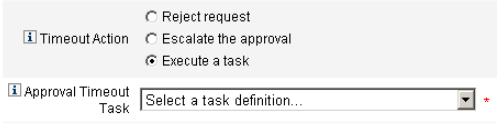
  a. 从**可用管理员**列表中选择一个或多个管理员名称。

  b. 将选定名称移至**选定的管理员**列表中。

执行任务

启用 "Timeout Action" 旁的 **Execute a task** 按钮后，将显示以下 **Approval Timeout Task** 菜单：

图 8-23 "Approval Timeout Task" 菜单



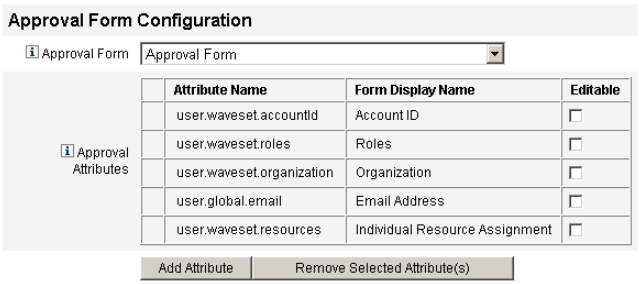
指定批准请求超时后要执行的任务。例如，可以允许请求者提交帮助台请求或发送报告给管理员。

配置批准表单

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 "Approval Form Configuration" 部分的功能选择批准表单，然后将属性添加到批准表单 （或从中删除属性）。

图 8-24 Approval Form Configuration



默认情况下， "Approval Attributes" 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 "Approval Attributes" 表中指定的批准属性。

要为其他批准者配置批准表单，请执行以下步骤：

1. 从 **Approval Form** 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 **Approval Attributes** 表的 **Editable** 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，请参见第 245 页上的 “添加属性”。
   - 要从表单删除属性，请参见第 246 页上的 “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。

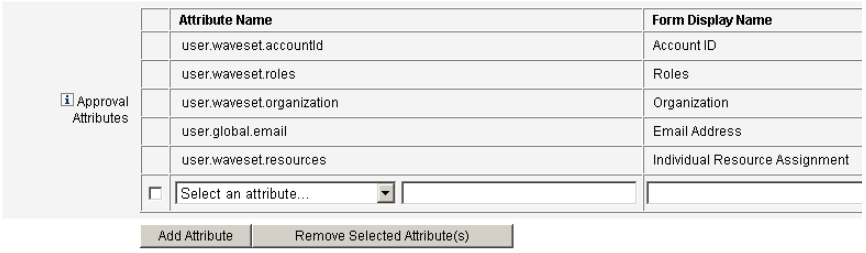
添加属性

要将属性添加到批准表单

1. 单击 "Approval Attributes" 表下的 **Add Attribute** 按钮。

   "Approval Attributes" 表中的 **Attribute name** 菜单将变为活动状态，如下图所示：

图 8-25 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，则表中将包含以下信息：

   - 如果需要，可以更改默认属性名称或默认表单显示名称，方法是将新名称键入相应的文本字段。
   - 若要允许批准者更改属性值，可启用**可编辑**复选框。

     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

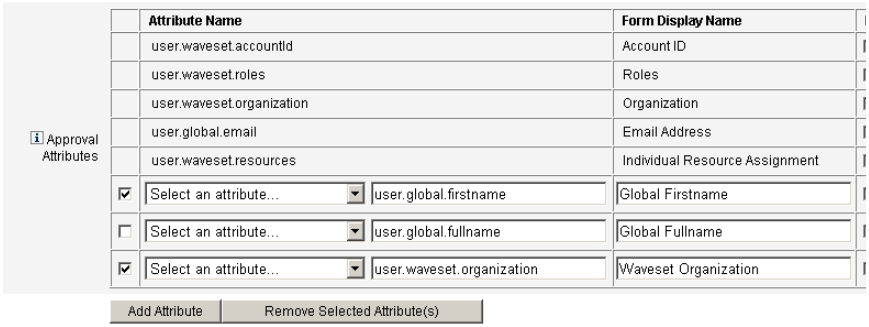
注 除非修改 XML 文件，否则不能从批准表单中删除默认属性。

要从批准表单中删除属性，请执行以下步骤：

1. 启用 "Approval Attributes" 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。

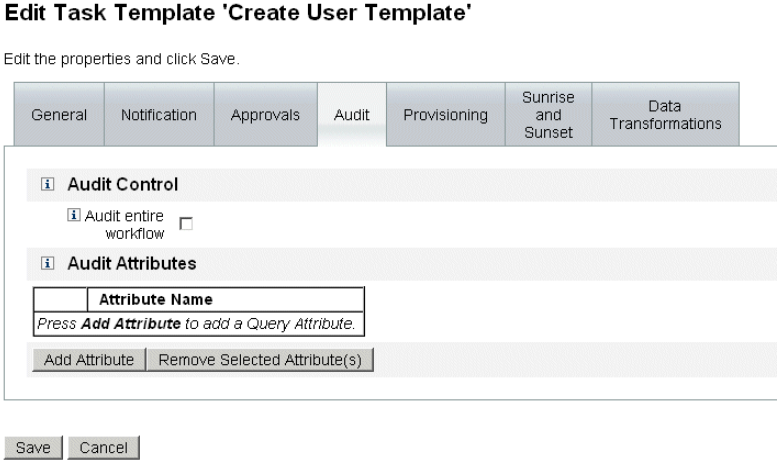
图 8-26 删除批准属性



配置 "Audit" 选项卡

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。特别地，可以配置 "Audit" 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 8-27 审计创建用户模板

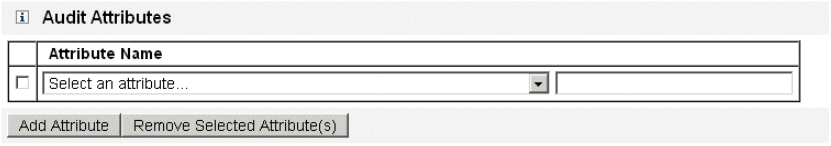


要通过用户模板的 “审计” 选项卡配置审计，请执行以下步骤：

1. 启用 **Audit entire workflow** 复选框以激活工作流审计功能。
2. 单击 **Add Attribute** 按钮 （在 "Audit Attributes" 部分），以选择要记录的属性以供报告。

3. 当 "Audit Attributes" 表中显示 **Select an attribute** 菜单后，从列表中选择属性。属性名称将显示在旁边的文本字段中。

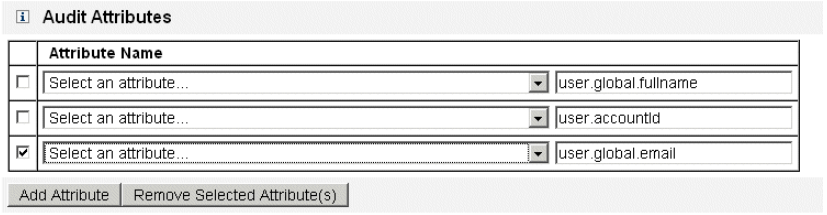
图 8-28 添加属性



要从 "Audit Attributes" 表中删除属性，请执行以下步骤：

1. 启用要删除的属性旁边的复选框。

图 8-29 删除 user.global.email 属性



2. 单击**删除选定属性**按钮。

配置完此选项卡后，可以

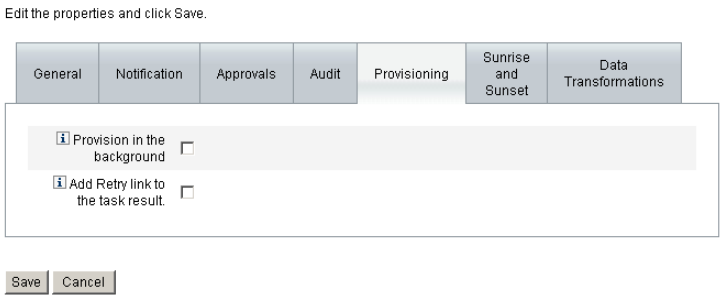
- 选择其他选项卡以继续编辑模板。
- 单击 **Save** 以保存更改并返回到 "Configure Tasks" 页。
- 单击 **Cancel** 以放弃更改并返回到 "Configure Task" 页。

配置 "Provisioning" 选项卡

注 此选项卡仅适用于创建用户模板和更新用户模板。

可以使用 "Provisioning" 选项卡配置以下与置备有关的选项：

图 8-30 "Provisioning" 选项卡：创建用户模板



- **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。**Retry** 链接可让用户在第一次尝试失败后再次尝试执行该任务。

配置完 "Provisioning" 选项卡后，可以

- 选择其他选项卡以继续编辑模板。
- 单击 **Save** 以保存更改并返回到 "Configure Tasks" 页。
- 单击 **Cancel** 以放弃更改并返回到 "Configure Tasks" 页。

配置 "Sunrise and Sunset" 选项卡

注 此选项卡仅适用于创建用户模板。

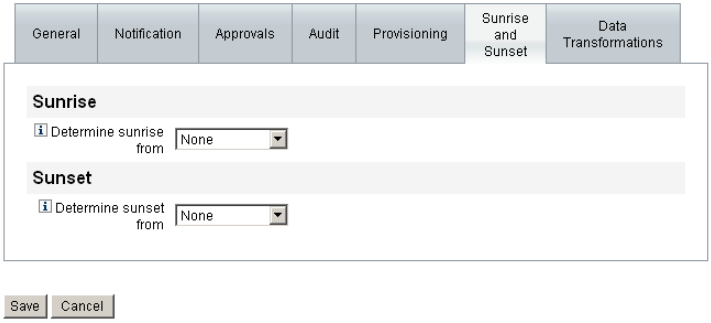
使用 "Sunrise and Sunset" 选项卡，可以选择一种方法来确定以下操作发生的时间和日期。

- 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 8-31 说明 "Sunrise and Sunset" 选项卡的设置。

图 8-31 "Sunrise and Sunset" 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。

要配置生效，请执行以下步骤：

1. 从 **Determine sunrise from** 菜单中选择以下选项之一，以指定 Identity Manager 确定置备的时间和日期的方法。
   - **指定时间** - 将置备延迟到指定的未来时间。请继续阅读第 251 页以获取有关说明。
   - **指定日期** - 将置备延迟到指定的未来日历日期。请继续阅读第 251 页以获取有关说明。
   - **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 252 页以获取有关说明。
   - **指定规则** - 根据规则 （评估后将生成日期/时间字符串）来延迟置备。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 252 页以获取有关说明。

注 **Determine sunrise from** 菜单的默认选项为 **None**，即允许立即进行置备。

2. 从 **Work Item Owner** 菜单中选择用户，该用户将拥有生效工作项目。

注 可在 "Approvals" 选项卡中找到生效工作项目。

3. 配置完生效后，可以
   - 选择其他选项卡以继续编辑创建用户模板。
   - 单击 **Save** 以保存更改并返回到 "Configure Tasks" 页。
   - 单击 **Cancel** 以放弃更改并返回到 "Configure Tasks" 页。

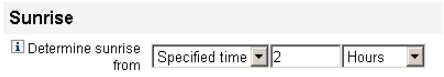
指定时间

要在指定时间进行置备，请执行以下步骤：

1. 从 **Determine sunrise from** 菜单中选择 **Specified time**。
2. 当新的文本字段和菜单显示在 **Determine sunrise from** 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，如果要在两小时后置备新用户，则进行如下指定：

图 8-32 在两个小时后置备新用户



指定日期

要在指定的日历日期进行置备，请执行以下步骤：

1. 从 **Determine sunrise from** 菜单中选择 **Specified day**。
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，如果要在九月的第二个星期一置备新用户，则进行如下指定：

图 8-33 按照日期置备新用户

指定属性

要根据用户帐户数据中的属性值来确定置备日期和时间，请执行以下步骤：

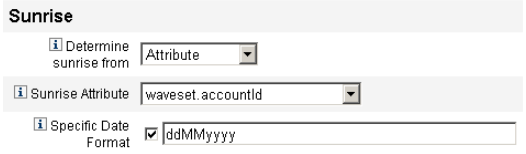
1. 从 **Determine sunrise from** 菜单中选择 **Attribute**，以下选项将变为活动状态：
   - **生效属性**菜单 - 提供当前为视图 （与此模板配置的任务相关）定义的属性列表。
   - **特定日期格式**复选框和菜单 - 允许您指定属性值的日期格式字符串 （如果需要）。

注 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 **Sunrise Attribute** 菜单中选择属性。
3. 如果需要，启用 **Specific Date Format** 复选框，并在 **Specific Date Format** 字段变为活动状态后输入日期格式字符串。

   例如，如果要根据使用了日、月和年格式的 `waveset.accountId` 属性值来置备新用户，则进行如下指定：

图 8-34 通过属性置备新用户



指定规则

要通过评估指定的规则来决定置备日期和时间，请执行以下步骤：

1. 从 **Determine sunrise from** 菜单中选择 **Rule**，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。

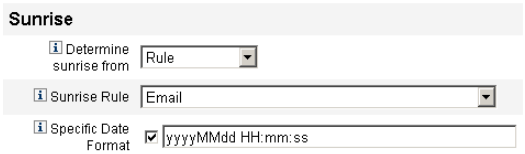
- **特定日期格式**复选框和菜单 - 允许您针对规则的返回值指定日期格式字符串（如果需要）。

注 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 **Sunrise Rule** 菜单中选择规则。
3. 如果需要，启用 **Specific Date Format** 复选框，并在 **Specific Date Format** 字段变为活动状态后输入日期格式字符串。

例如，如果要根据使用了年、月、日、小时、分钟和秒格式的电子邮件规则来置备新用户，请进行如下指定：

图 8-35 通过规则置备新用户



配置失效

配置失效部分 （取消置备）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。

唯一的不同之处是生效部分还提供了 **Sunset Task** 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。

要配置失效，请执行以下步骤：

1. 使用 **Determine sunset from** 菜单指定方法来确定取消置备的时间：

注 **Determine sunset from** 菜单的默认选项为 **None**，即允许立即取消置备。

- **指定时间** - 将取消置备延迟到指定的未来时间。请查看第 251 页上的“指定时间”以获取有关说明。

- **指定日期** - 将取消置备延迟到指定的未来日历日期。请查看第 251 页上的“指定日期”以获取有关说明。
- **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。

  请查看第 252 页上的 “指定属性”以获取有关说明。
- **规则** - 根据规则 （评估后将生成日期/时间字符串）来延迟取消置备。与指定属性一样，可以指定数据必须符合的日期格式。

  请查看第 252 页上的 “指定规则”以获取有关说明。

2. 使用 **Sunset Task** 菜单指定任务以在指定的日期和时间取消对用户的置备。
3. 配置完此选项卡后，可以
   - 选择其他选项卡以继续编辑模板。
   - 单击 **Save** 以保存更改并返回到 "Configure Tasks" 页。
   - 单击 **Cancel** 以放弃更改并返回到 "Configure Tasks" 页。

配置 "Data Transformations" 选项卡

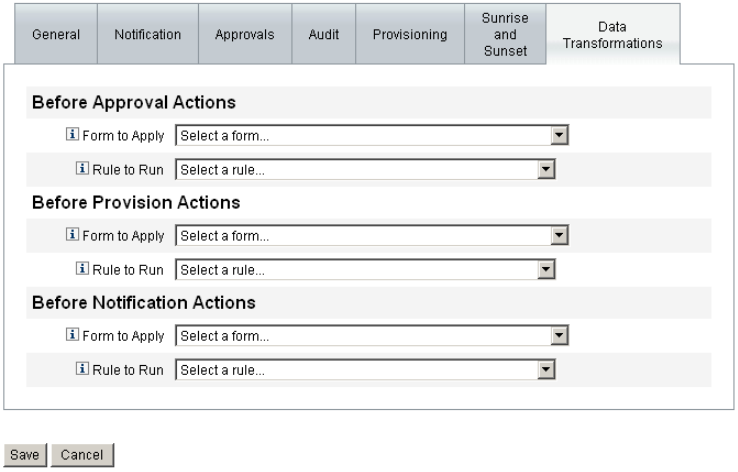
注 此选项卡仅适用于创建用户模板和更新用户模板。

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 "Data Transformations" 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 "Data Transformations" 选项卡后，将显示以下页面：

图 8-36 "Data Transformations" 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 - 提供当前为您的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 - 提供当前为您的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。

配置完此选项卡后，可以

- 选择其他选项卡以继续编辑模板。
- 单击 **Save** 以保存更改并返回到 "Configure Tasks" 页。
- 单击 **Cancel** 以放弃更改并返回到 "Configure Tasks" 页。

第 9 章

PasswordSync

本章介绍 Sun Java™ System Identity Manager PasswordSync 的功能，该功能使 Windows 客户端能够更改 Windows Active Directory 和 Windows NT 域中的密码，从而使更改与 Identity Manager 同步。

信息通过以下方式进行组织：

什么是 PasswordSync？

PasswordSync 功能可以使在 Windows Active Directory 和 Windows NT 域上的用户密码更改与 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。

在域控制器上安装 PasswordSync 之后，该控制器将与作为 Java 通讯服务 (Java Messaging Service, JMS) 客户端代理的 Servlet 进行通信。该 Servlet 接着与启用 JMS 的信息队列通信。 JMS 侦听器资源适配器从队列中删除消息并使用工作流任务处理密码更改。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向用户通知密码更改的状态。

注 密码更改必须将要转发的更改请求的本机密码策略传递至 Identity Manager 服务器以实现同步。如果提议的密码更改不遵循本机密码策略， ADSI 将显示错误信息对话框，并且不向 Identity Manager 发送任何同步数据。

安装之前

只能在 Windows 2000、 Windows 2003 和 Windows NT 域控制器上设置 PasswordSync 功能。必须在与 Identity Manager 同步的域中的每个域控制器上安装 PasswordSync。

PasswordSync 需要具有与 JMS 服务器的连通性。有关 JMS 系统要求的详细信息，请参见 *Sun Java™ System Identity Manager 资源参考资料*中的 JMS 侦听器资源适配器部分。

此外， PasswordSync 还要求您

- 在每个域控制器上安装 Microsoft .NET 1.1 或更高版本
- 删除 PasswordSync 的所有先前版本

以下各节将详细讨论这些要求。

安装 Microsoft .NET 1.1

要使用 PasswordSync，必须安装 Microsoft .NET 1.1 或更高版本的 Framework。如果您使用 Windows 2003 域控制器，则默认安装此 Framework。如果您使用 Windows 2000 或 Windows NT 域控制器，则可以从 Microsoft 下载中心下载此工具包：

http://www.microsoft.com/downloads

注

- Microsoft .NET 1.1 Framework 需要 Internet Explorer 5.01 或更高版本。Internet Explorer 5.0 （与 Windows 2000 SP4 捆绑）版本太低。
- 在 "Keywords" 搜索字段中输入 `NET Framework 1.1 Redistributable` 可快速找到框架工具包。
- 该工具包将安装 .NET 1.1 framework。

卸载 PasswordSync 的先前版本

安装更高版本之前，*必须*先删除先前安装的任何 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。

安装 PasswordSync

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。

1. 从 Identity Manager 安装介质中，单击 `pwsync\IdmPwSync.msi` 图标。将显示 "Welcome" 窗口。

   安装向导提供了以下导航按钮：

   - **Cancel**：随时可以单击以退出向导，而不保存任何更改。
   - **Back**：单击以返回上一个对话框。
   - **Next**：单击以前进到下一个对话框。

2. 阅读 "Welcome" 屏幕上提供的信息，然后单击 "Next" 显示“Choose Setup Type PasswordSync Configuration”窗口。
   PasswordSync 安装

3. 单击 "Typical" 或 "Complete" 安装完整的 PasswordSync 软件包，或者单击 "Custom" 控制安装哪些软件包组件。

4. 单击 "Install" 安装该产品。

   将显示一则消息，以通知您是否已成功安装 PasswordSync。

5. 单击 "Finish" 完成安装过程。

   请确保选择了 "Launch Configuration Application"，以便可以开始配置 PasswordSync。有关该过程的详细信息，请参见第 260 页上的 “配置 PasswordSync”。

注 屏幕将显示对话框，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。

表 9-1 介绍了在每个域控制器上安装的文件。

表 9-1 域控制器文件

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
%$INSTALL_DIR$%\DotNetWrapper.dll	处理 .NET SOAP 通信的 DLL。
%$INSTALL_DIR$%\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。

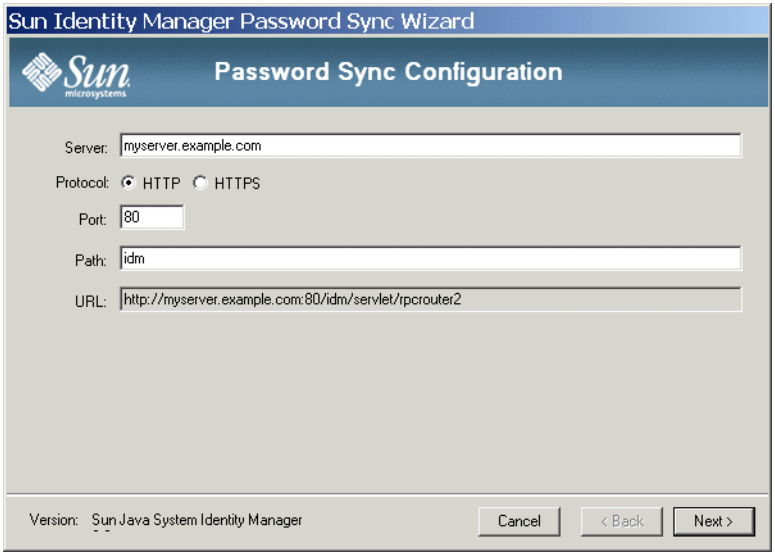
使用以下步骤配置 PasswordSync。

1. 如果还没有运行 PasswordSync 配置应用程序，请开始运行。

   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。

   将显示 "PasswordSync Configuration" 对话框 （请参见图 9-1）。

图 9-1 PasswordSync 配置对话框

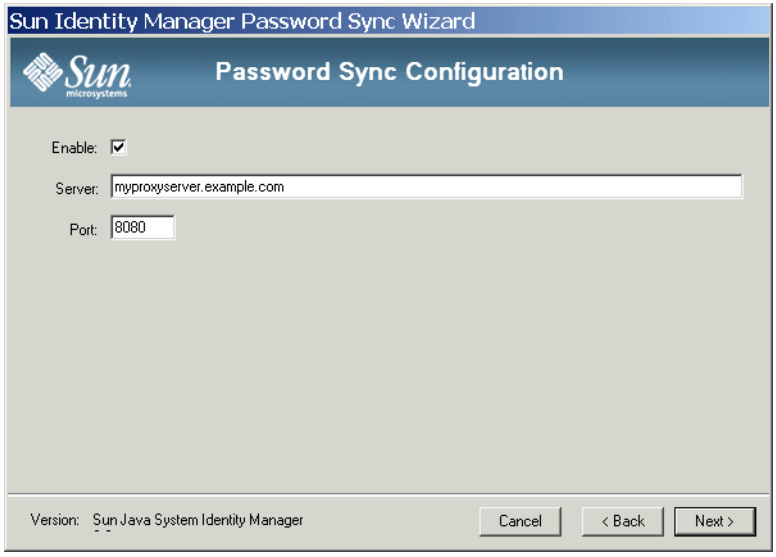


根据需要编辑字段。

- **Server** 必须用安装 Identity Manager 的全限定主机名或 IP 地址替换。
- **Protocol** 指示是否与 Identity Manager 进行安全连接。如果选择了 HTTP，则默认端口为 80；如果选择了 HTTPS，则默认端口为 443。
- **Path** 指定到应用程序服务器上 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。

2. 单击 "Next" 显示 "Proxy Server Configuration" 页 （图 9-2）。

图 9-2 代理服务器对话框

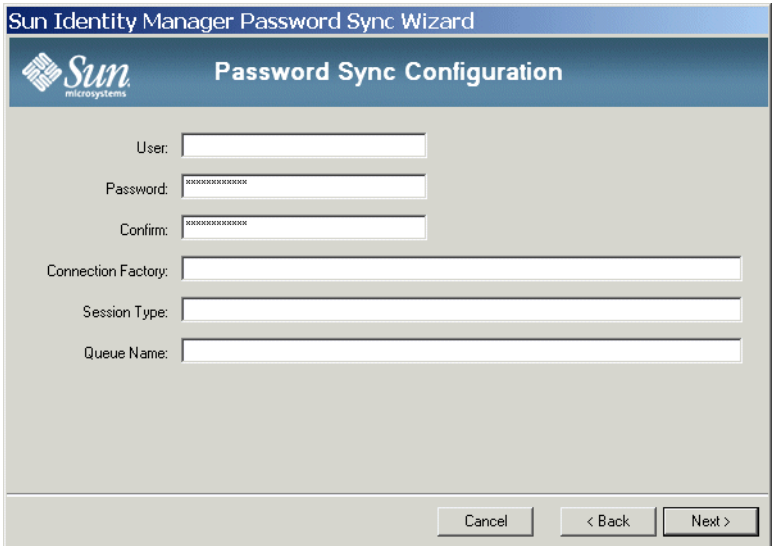


根据需要编辑字段。

- 如果必须使用代理服务器，则单击 "Enable"。
- **Server** 必须用代理服务器的全限定主机名或 IP 地址替换。
- **Port**：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。）

3. 单击 "Next" 显示 JMS 设置对话框 （图 9-3）。

图 9-3 JMS 设置对话框

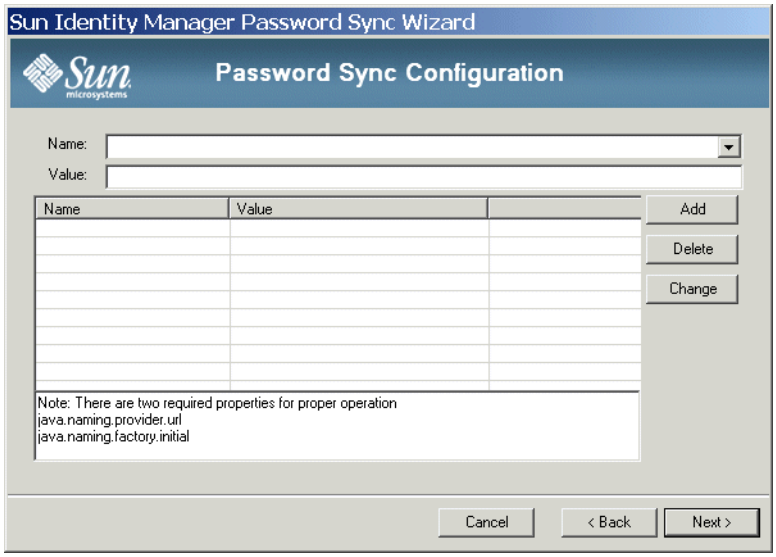


根据需要编辑字段。

- **User** 指定在队列中加入新消息的 JMS 用户名。
- **Password** 和 **Confirm** 指定 JMS 用户的密码。
- **Connection Factory** 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 **Session Type** 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`。
- **Queue Name** 指定密码同步事件的目标查找名称。

4. 单击 "Next" 显示 JMS 属性对话框 （图 9-4）。

图 9-4 JMS 属性对话框



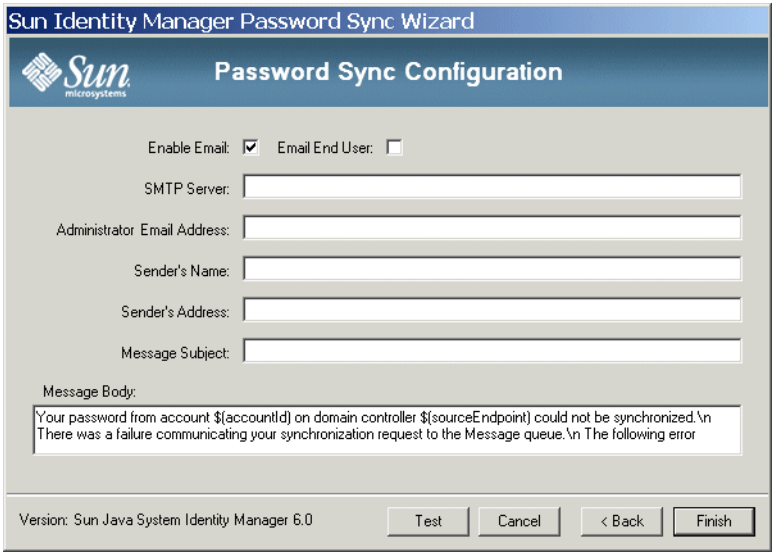
JMS 属性对话框允许您定义用于构建初始 JNDI 上下文的属性集。必须定义以下名称/值对：

- `java.naming.provider.url` - 必须将该值设置为运行 JNDI 服务的计算机的 URL。
- `java.naming.factory.initial` - 必须将该值设置为 JNDI 服务提供者的初始上下文工厂的类名 （包括软件包）。

"Name" 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 "Value" 字段中输入其相应的值。

5. 单击 "Next" 显示电子邮件对话框 （图 9-5）。

图 9-5 电子邮件对话框



通过电子邮件对话框，您可以配置是否在用户的密码更改没有成功同步 （由于通信错误或 Identity Manager 之外的其他错误所致）时发送电子邮件通知。

根据需要编辑字段。

- 选择 **Enable Email** 启用该功能。如果用户要接收通知，请选择 **Email End User**。否则，将仅通知管理员。
- **SMTP Server** 是发送故障通知时使用的 SMTP 服务器的全限定名或 IP 地址。
- **Administrator Email Address** 是用于发送通知的电子邮件地址。
- **发件人名称**是发件人的 “友好名”。
- **发件人地址**是发件人的电子邮件地址。
- **Message Subject** 指定所有通知的主题行。
- **Message Body** 指定通知的文本。

  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。

6. 单击 "Finish" 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，请从命令行输入以下命令：

```
C:\InstallDir\Configure.exe -wizard
```

调试 PasswordSync

本节提供了有关如何查找进行 PasswordSync 故障诊断时需要的信息以及如何使用配置工具启用跟踪的详细信息。本节还列出了调试 PasswordSync 或启用配置工具无法实现的功能时可能需要的注册表主键。

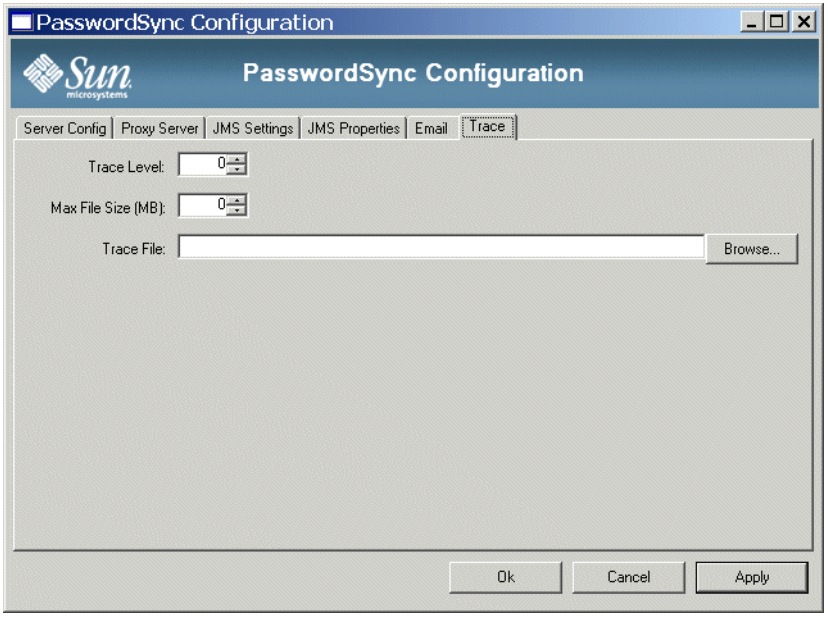
错误日志

PasswordSync 将所有故障写入 Windows 事件查看器。错误日志条目的源名称是 *PasswordSync*。

跟踪日志

首次运行配置工具时，向导并不包括用于配置跟踪的面板。但是，每次启动该工具后都会显示 "Trace" 选项卡 （图 9-6）。

图 9-6 "Trace" 选项卡



"Trace Level" 字段指定写入跟踪日志时 PasswordSync 将提供的详细级别。值 0 表示已关闭跟踪；值 4 为提供最多详情。

当跟踪文件超过 "Max File Size (MB)" 字段中指定的大小时，PasswordSync 会将文件移到附加了 .bk 的基本名。例如，如果将跟踪文件设置为 `C:\logs\pwicsvc.log`，并且将跟踪级别设置为 100 MB，则当跟踪文件超过 100 MB 时，PasswordSync 将该文件重命名为 `C:\logs\pwicsvc.log.bk` 并将新数据写入新的 `C:\logs\pwicsvc.log` 文件。

注册表主键

您可使用 Windows 注册表编辑器编辑表 9-2 中列出的注册表主键。这些主键位于：

`HKEY_LOCAL_MACHINE\SOFTWARE\Waveset\Lighthouse\PasswordSync`

此位置也存在其他主键，但可以使用配置工具来编辑它们。

表 9-2 注册表主键

主键名称	类型	描述
allowInvalidCerts	REG_DWORD	如果设置为 1，则该主键将在 .NET 客户端上设置以下标志： • SECURITY_FLAG_IGNORE_UNKNOWN_CA • INTERNET_FLAG_IGNORE_CERT_CN_INVALID • INTERNET_FLAG_IGNORE_CERT_DATE_INVALID 结果，客户端将容许证书到期或具有无效的 CN 或主机名。这仅适用于使用 SSL 的情况。 在测试环境中 （大多数证书从无效的证书授权机构 [CA] 产生）进行调试时，该设置非常有用。 默认值为 0。
clientConnectionFlags	REG_DWORD	将会传递给 .NET SOAP 客户端的可选连接标志。 默认值为 0。
clientSecurityFlags	REG_DWORD	可以传递到 .NET SOAP 客户端的可选安全标志。 默认值为 0。
installdir	REG_SZ	安装 PasswordSync 应用程序的目录。
soapClientTimeout	REG_DWORD	出现故障之前 SOAP 客户端与 Identity Manager 服务器的通信超时 （以毫秒为单位）。

卸载 PasswordSync

要卸载 PasswordSync 应用程序，请转至 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。

部署 PasswordSync

要部署 PasswordSync，必须在 Identity Manager 中执行以下操作：

- 配置 JMS 侦听器适配器
- 实现同步用户密码工作流
- 设置通知

配置 JMS 侦听器适配器

一旦域控制器间接将消息置于队列中，就必须将资源适配器配置为接受这些消息。必须创建 JMS 侦听器资源适配器并将其配置为与队列通信。有关设置该适配器的详细信息，请参见 *Sun Java™ System Identity Manager 资源参考资料*。

必须配置以下资源参数：

- **目标类型** - 通常将该值设置为 “队列”。因为有一个订阅服务器而可能有多个发布服务器，所以各主题通常不相关。
- **初始上下文 JNDI 属性** - 该文本框定义用于构建初始 JNDI 上下文的属性集。必须定义以下名称/值对：
  - `java.naming.provider.url` - 必须将该值设置为运行 JNDI 服务的计算机的 URI。
  - `java.naming.factory.initial` - 必须将该值设置为 JNDI 服务提供者的初始上下文工厂的类名 （包括软件包）。

  可能需要定义其他属性。属性和值的列表应该与配置应用程序的 JMS 设置页上指定的属性和值相匹配。
- **连接工厂的 JNDI 名称** - 在 JMS 服务器中定义的连接工厂的名称。
- **用户**和**密码** - 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。

实现同步用户密码工作流

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，然后再签回 ChangeUserPassword 查看器。完成签入后，工作流迭代所有资源帐户并选择除源资源以外的所有资源。 Identity Manager 使用电子邮件通知用户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。可以在适配器的活动同步向导中分配进程规则。

如果要修改默认的同步用户密码工作流，请复制 `$WSHOME/sample/wfpwsync.xml` 文件并进行修改。然后将修改后的工作流导入 Identity Manager。

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 进行密码更改。

有关使用工作流的详细信息，请参见 *Sun Java™ System Identity Manager 工作流、表单和视图*。

设置通知

Identity Manager 提供密码同步通知和密码同步故障通知的电子邮件模板。这些模板可通知用户在多个资源间更改密码的尝试是否成功。

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。请参见第 127 页上的 “自定义电子邮件模板”。

使用 Sun JMS Server 配置 PasswordSync

Identity Manager 提供了 JMS 侦听器适配器，该适配器使密码更改事件可以在 JMS 消息服务器上进行排队，以增强可靠性并确保传送。

注 有关该适配器的详细信息，请参见 *Sun Java™ System Identity Manager 资源参考资料*。

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：

概述

本节介绍了示例方案、 Windows PasswordSync 解决方案以及 JMS 解决方案。

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 ñ Active Directory
- Sun Java™ System Identity Manager 6.0 2005Q4M3
- 在 Suse Linux 10.0 上运行的 MySQL 4.1.13
- 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 1.4.2

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）

解决方案概述

分析在 Windows PasswordSync 解决方案中起作用的所有组件时，会发生以下情况：

1. 用户在工作站上更改其密码后， PasswordSync 将向当前 Active Directory 域控制器发送密码修改，并且 Identity Manager 密码捕获 `dll`（位于域控制器上）将捕获明文密码。
2. 密码捕获 `dll` 将向 Identity Manager SOAP 请求处理程序发出 SOAP 请求。

   用户 ID、加密的密码以及必需的 JMS 配置信息全部封装在此 SOAP 请求中。例如，

代码示例 9-1 SOAP 请求示例

```
POST /idm/servlet/rpcrouter2 HTTP/1.0
Accept:text/*
SOAPAction:"urn:lighthouse"
Content-Type:text/xml; charset=utf-8
User-Agent:VCSoapClient
Host: 192.168.1.4:8080
Content-Length: 1154
Connection:Keep-Alive
Pragma:no-cache
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xmlns:xsd="http://www.w3.org/2001/XMLSchema"
   xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">
<soap:Body soap:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
<snp:queuePasswordUpdate xmlns:snp="urn:lighthouse">
<userEmailAddress xsi:nil="1"/>
<resourceAccountId>CN=John Smith,OU=people,DC=org,DC=local</resourceAccountId>
<resourceAccountGUID>b4e1c14b79d3a949a618a607dde7784d</resourceAccountGUID>
<password>zkpS8qcIJkVBWa/Frp+JqA==</password>
<accounts xsi:nil="1"/>
<resourcename xsi:nil="1"/>
<resourcetype>Windows Active Directory</resourcetype>
<clientEndpoint>W2003EE</clientEndpoint>
<jmsUser>guest</jmsUser>
<jmsPassword>guest</jmsPassword>
<queueName>cn=pwsyncDestination</queueName>
<connectionFactory>cn=pwsyncFactory</connectionFactory>
<sessionType>LOCAL</sessionType>
<JNDIProperties>java.naming.factory.initial=com.sun.jndi.ldap.LdapCtxFactory;java.naming.
   provider.url=ldap://gwenig.coopsrccom:389/ou=sunmq,dc=coopsrc,dc=com</JNDIProperties>
<singleResult>true</singleResult>
</snp:queuePasswordUpdate>
</soap:Body>
</soap:Envelope>
```

3. SOAP 处理程序接收请求并使用请求中所包含的 JMS 参数来启动到 JMS Message Queue 代理的连接。然后，SOAP 处理程序将发送包含用户 ID 和加密密码 （以及某些稍后将讨论的其他参数）的消息。

   例如， Message Queue 代理上的 SOAP 处理程序将发送类似于以下消息的消息（类型为 *MapMessage*）：

代码示例 9-2 SOAP 处理程序消息

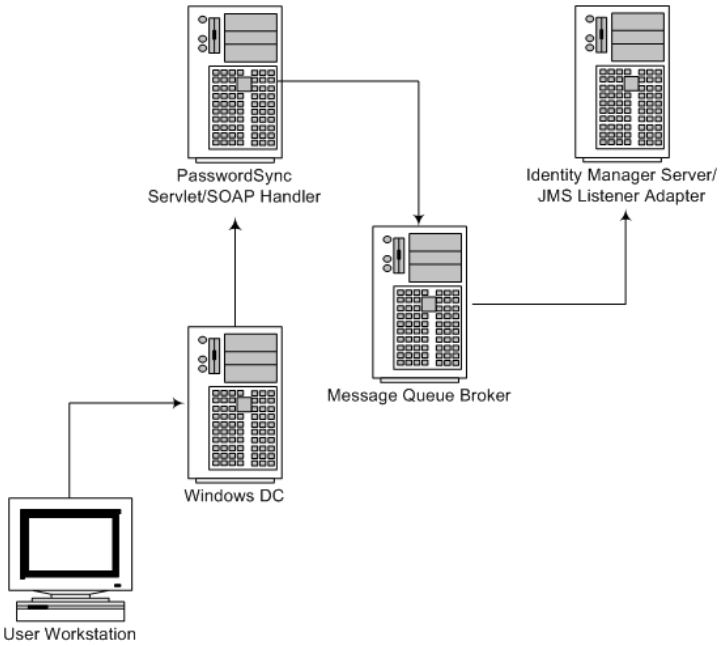
```
password:zkpS8qcIJkVBWa/Frp+JqA==
accounts:null
resourceAccountGUID:8f245d1490de7a4192a8821c569c9ac4
requestTimestamp: 1143639284325
queueName:cn=pwsyncDestination
jmsUser:guest
resourcetype:Windows Active Directory
resourcename:null
JNDIProperties:
java.naming.factory.initial=com.sun.jndi.ldap.LdapCtxFactory;
java.naming.provider.url=ldap://gwenig.coopsrc.com:389/
ou=sunmq,dc=coopsrc,dc=com
connectionFactory:cn=pwsyncFactory
clientEndpoint:W2003EE
userEmailAddress:null
sessionType:LOCAL
jmsPassword:guest
resourceAccountId:CN=John Smith,OU=people,DC=org,DC=local
```

4. Message Queue 代理将消息排入队列中，并且 JMS 侦听器适配器将检索消息。现在， Identity Manager 可以启动工作流。

   图 9-7 说明了该示例方案中使用的配置：

注	尽管图中所示 SOAP 处理程序和 Identity Manager 分别位于不同服务器，但您可以在同一服务器上运行它们。

图 9-7 方案配置



JMS 概述

Java 消息服务 (Java Message Service, JMS) API 是一种消息传送标准，该标准允许应用程序组件（基于 Java 2 Platform, Enterprise Edition [J2EE]）创建、发送、接收以及读取消息。通过该 API 可实现松散耦合的可靠异步分布式通信。

要发送或接收消息， JMS 客户端必须先连接到 JMS 提供程序，此提供程序通常作为消息代理来实现。该连接将在客户端和代理之间打开一个通信通道。接下来，客户端必须设置一个用于创建、生成和使用消息的会话。

JMS 并未完全定义以下消息传送元素：

- **连接工厂** - 连接工厂管理对象可以生成到代理的客户端连接。这些对象将封装特定于提供程序的信息，可以控制消息传送行为的某些方面，例如连接处理、客户端标识、消息头覆盖、可靠性和流量控制等。从给定的连接工厂获取的每个连接均显示为该工厂配置的行为。
- **目标** - 目标管理对象引用代理上的物理目标。这些对象将封装特定于提供程序的命名 （地址-语法）约定，并指定在其中使用目标的消息传送域 - 队列或主题。

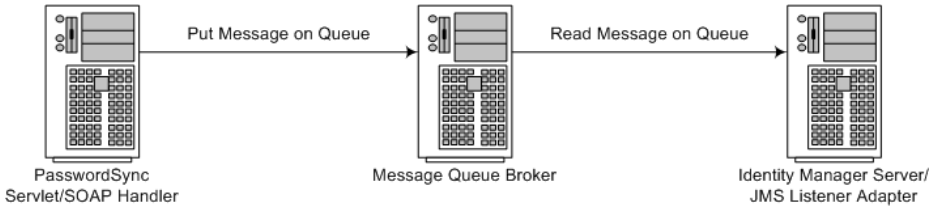
这两个对象不是通过编程方式创建的，通常是使用管理工具创建和配置的。之后，它们将存储在对象存储库中， JMS 客户端可以通过标准的 JNDI 查找来访问它们。

注 有关连接工厂和目标的详细信息，请参阅位于以下位置的 《Sun Java™ System Message Queue 技术概述》：

http://docs.sun.com/source/819-3565/intro.html

图 9-8 说明了该示例方案中的通信流：

图 9-8 通信流方案



SOAP 处理程序收到来自于 Windows 密码捕获 `dll` 的请求后，SOAP 处理程序将用作代理，以将 SOAP 请求转换为 JMS 消息。之后， JMS 侦听器适配器将接收消息并触发相关工作流。

要使用 JMS 代理， Identity Manager SOAP 处理程序和 Identity Manager JMS 侦听器适配器必须都具有连接工厂和目标 （可使用 JNDI 查找）。

Identity Manager SOAP 处理程序将在 SOAP 消息中获取所需的详细信息 （如先前所示）：

代码示例 9-3 SOAP 消息

```
<jmsUser>guest</jmsUser>
<jmsPassword>guest</jmsPassword>
<queueName>cn=pwsyncDestination</queueName>
<connectionFactory>cn=pwsyncFactory</connectionFactory>
<sessionType>LOCAL</sessionType>
<JNDIProperties>java.naming.factory.initial=com.sun.jndi.ldap.LdapCtxFactory;java.naming.
  provider.url=ldap://gwenig.coopsrc.com:389/ou=sunmq,dc=coopsrc,dc=com</JNDIProperties>
```

在 Windows 上安装和配置 PasswordSync 时将提供以下所有参数（图 9-9 和图 9-10 中所示）：

图 9-9 “JMS 设置”选项卡

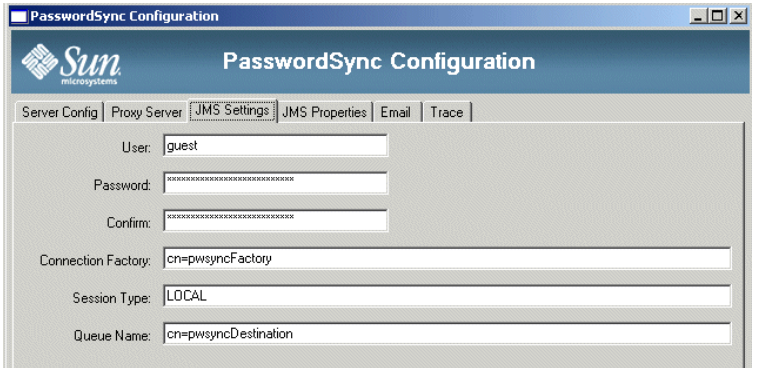
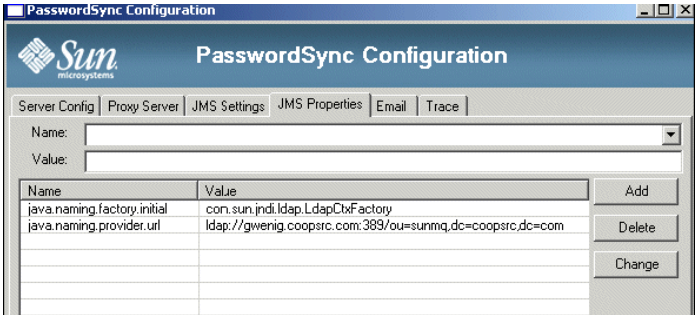


图 9-10 "JMS Properties" 选项卡



以下各节介绍了这些参数：

- JMS 设置参数
- JMS 属性参数

JMS 设置参数

"JMS Settings" 选项卡包含以下参数：

- **User** 和 **Password** 字段：定义连接到 JMS 代理时所使用的证书。
- **Connection Factory** 字段：指定连接工厂对象的 JNDI 查找名称。
- **Session Type** 字段：指定
- **Queue Name** 字段：指定目标对象的 JNDI 查找名称。

在代码示例 9-4 中，连接工厂和队列名称为 LDAP RDN，这实现了一个完整的 DN（在与 java.naming.provider.url 结合时）。一个简单的 ldapsearch 即可显示管理对象条目：

代码示例 9-4 连接工厂和队列名称示例

```
Connection Factory:
#> ldapsearch -h gwenig.coopsrc.com -b 'dc=coopsrc,dc=com' 'cn=pwsyncfactory'
dn:cn=pwsyncFactory,ou=sunmq,dc=coopsrc,dc=com
objectClass:top
objectClass:javaContainer
objectClass:javaObject
objectClass:javaNamingReference
javaClassName:com.sun.messaging.QueueConnectionFactory
javaFactory:com.sun.messaging.naming.AdministeredObjectFactory
javaReferenceAddress:#0#version#3.0
javaReferenceAddress:#1#readOnly#false
javaReferenceAddress:#2#imqOverrideJMSPriority#false
javaReferenceAddress:#3#imqConsumerFlowLimit#1000
javaReferenceAddress:#4#imqAddressListIterations#1
javaReferenceAddress:#5#imqOverrideJMSExpiration#false
javaReferenceAddress:#6#imqConnectionType#TCP
javaReferenceAddress:#7#imqLoadMaxToServerSession#true
javaReferenceAddress:#8#imqPingInterval#30
javaReferenceAddress:#9#imqSetJMSXUserID#false
javaReferenceAddress:#10#imqConfiguredClientID#
javaReferenceAddress:#11#imqSSLProviderClassname#com.sun.net.ssl.internal.ssl.Provider
javaReferenceAddress:#12#imqJMSDeliveryMode#PERSISTENT
javaReferenceAddress:#13#imqConnectionFlowLimit#1000
javaReferenceAddress:#14#imqConnectionURL#http://localhost/imq/tunnel
javaReferenceAddress:#15#imqBrokerServiceName#
javaReferenceAddress:#16#imqJMSPriority#4
javaReferenceAddress:#17#imqBrokerHostName#localhost
javaReferenceAddress:#18#imqJMSExpiration#0
javaReferenceAddress:#19#imqAckOnProduce#
javaReferenceAddress:#20#imqEnableSharedClientID#false
javaReferenceAddress:#21#imqAckTimeout#0
javaReferenceAddress:#22#imqAckOnAcknowledge#
javaReferenceAddress:#23#imqConsumerFlowThreshold#50
javaReferenceAddress:#24#imqDefaultPassword#guest
javaReferenceAddress:#25#imqQueueBrowserMaxMessagesPerRetrieve#1000
javaReferenceAddress:#26#imqDefaultUsername#guest
javaReferenceAddress:#27#imqReconnectEnabled#false
javaReferenceAddress:#28#imqConnectionFlowCount#100
javaReferenceAddress:#29#imqAddressListBehavior#PRIORITY
javaReferenceAddress:#30#imqReconnectAttempts#0
javaReferenceAddress:#31#imqSetJMSXAppID#false javaReferenceAddress:
#32#imqConnectionHandler#com.sun.messaging.jmq.jmsclient.protocol.
tcp.TCPStreamHandler
javaReferenceAddress:#33#imqSetJMSXRcvTimestamp#false
javaReferenceAddress:#34#imqBrokerServicePort#0
javaReferenceAddress:#35#imqDisableSetClientID#false
javaReferenceAddress:#36#imqSetJMSXConsumerTXID#false
javaReferenceAddress:#37#imqOverrideJMSDeliveryMode#false
```

代码示例 9-4 连接工厂和队列名称示例 *（续）*

```
javaReferenceAddress:#38#imqBrokerHostPort#7676
javaReferenceAddress:#39#imqQueueBrowserRetrieveTimeout#60000
javaReferenceAddress:#40#imqSSLIsHostTrusted#true
javaReferenceAddress:#41#imqSetJMSXProducerTXID#false
javaReferenceAddress:#42#imqConnectionFlowLimitEnabled#false
javaReferenceAddress:#43#imqReconnectInterval#3000
javaReferenceAddress:#44#imqAddressList#mq://gwenig:7676/jms
javaReferenceAddress:#45#imqOverrideJMSHeadersToTemporaryDestinations#false
cn:pwsyncFactory
```

目标如下：

代码示例 9-5 目标示例

```
#> ldapsearch -h gwenig.coopsrc.com -b 'dc=coopsrc,dc=com' 'cn=pwsyncdestination'
dn:cn=pwsyncDestination,ou=sunmq,dc=coopsrc,dc=com
objectClass:top
objectClass:javaContainer
objectClass:javaObject
objectClass:javaNamingReference
javaClassName:com.sun.messaging.Queue
javaFactory:com.sun.messaging.naming.AdministeredObjectFactory
javaReferenceAddress:#0#version#3.0
javaReferenceAddress:#1#readOnly#false
javaReferenceAddress:#2#imqDestinationName#pwsyncQueue
javaReferenceAddress:#3#imqDestinationDescription#A Description for the Destination Object
cn:pwsyncDestination
```

JMS 属性参数

在示例方案中，连接工厂和目标对象位于 LDAP 目录中。

`java.naming.factory.initial` 是用于创建初始 JNDI 上下文的工厂类的值。

`java.naming.provider.url` 包含环境属性的名称，该属性用于为正在使用的服务提供者指定配置信息。如果不提供详细信息， PasswordSync 将使用匿名 LDAP 会话来检索连接工厂和目标对象。

要提供证书和绑定方法，请指定以下属性：

- `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

注 必须为 JMS 侦听器适配器定义这些相同的设置。

图 9-11 JMS 侦听器资源参数页

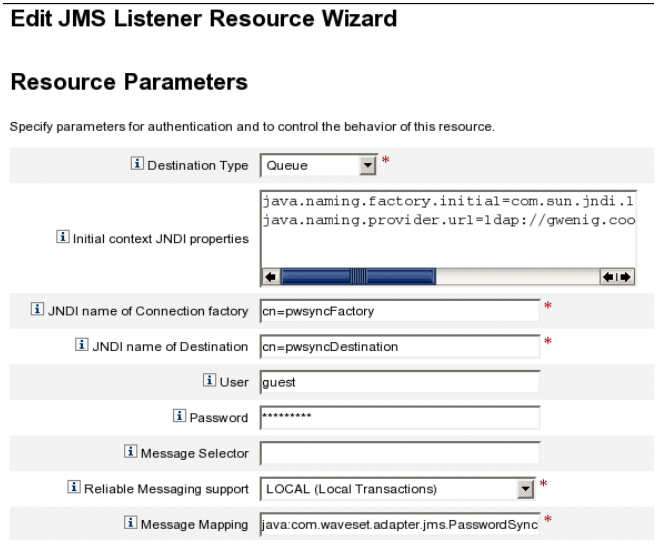
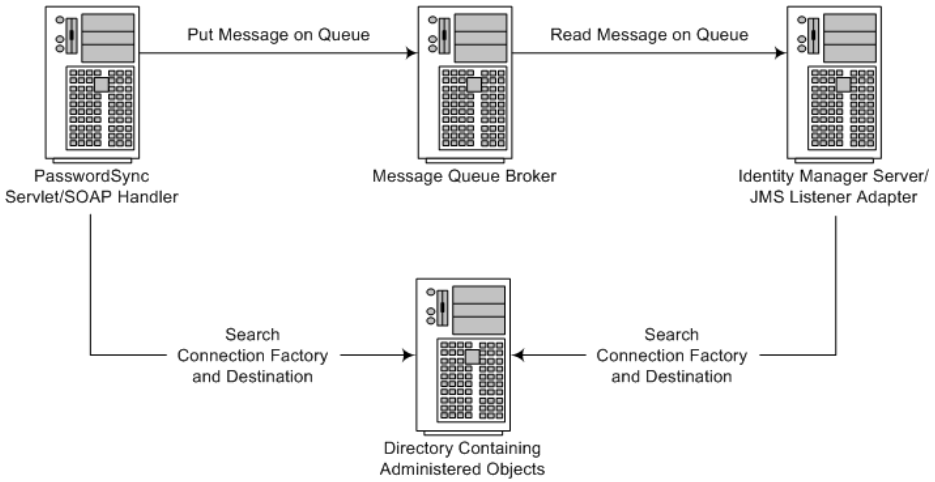


图 9-12 详细说明了该过程：

图 9-12 检索连接工厂和目标对象



SOAP 处理程序和 JMS 侦听器适配器必须都搜索连接工厂和目标才能发送/接收消息。

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
- 目标对象

注

- 本节的指令假设您已安装 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 Message Queue 管理 GUI (`imqadmin`) 或命令行工具 (`imqobjmgr`) 来创建这些管理对象。以下指令使用命令行工具。

将管理对象存储到 LDAP 目录

本节介绍了将连接工厂对象存储到 LDAP 目录时所需的命令。

存储连接工厂对象

使用代码示例 9-6 中的命令来存储连接工厂对象：

代码示例 9-6 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.
```

其中 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)。

存储目标对象

使用代码示例 9-7 中的命令来存储目标对象：

代码示例 9-7 存储目标对象

```
#> ./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
```

代码示例 9-7 存储目标对象

```
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.
```

注 您可以使用 ldapsearch 或 LDAP 浏览器来查看新创建的对象。

将管理对象存储到文件

本节介绍了如何使用命令行工具将管理对象存储到文件。

存储连接工厂对象

代码示例 9-8 介绍了存储连接工厂对象以及指定查找名称时所需的命令：

代码示例 9-8 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
```

代码示例 9-8 存储连接工厂对象并指定查找名称

```
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.
```

在代理上创建目标

默认情况下，Sun Java System Message Queue 代理允许自动创建队列目标（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标，则必须使用代码示例 9-9（其中 *myTestQueue* 为目标）中所示的命令在代理上创建目标对象：

代码示例 9-9 在代理上创建目标对象

```
name (Queue name):
#> cd /opt/sun/mq/bin
#>./imqcmd create dst -t q -n mytestQueue
Username:<admin>
Password:<admin>
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：

- **存储到目录**：如果在您的 Identity Manager 部署中， Identity Manager SOAP 处理程序和 Identity Manager 服务器未在同一台服务器上运行，则使用目录是一种集中存储连接工厂和目标对象的方法。

  使用目录时，这些管理对象将存储为目录条目。

注	如果 Identity Manager SOAP 处理程序和 Identity Manager 服务器不在同一台计算机上，那么它们必须都可以访问 .bindings 文件。您可以在每台计算机上将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。

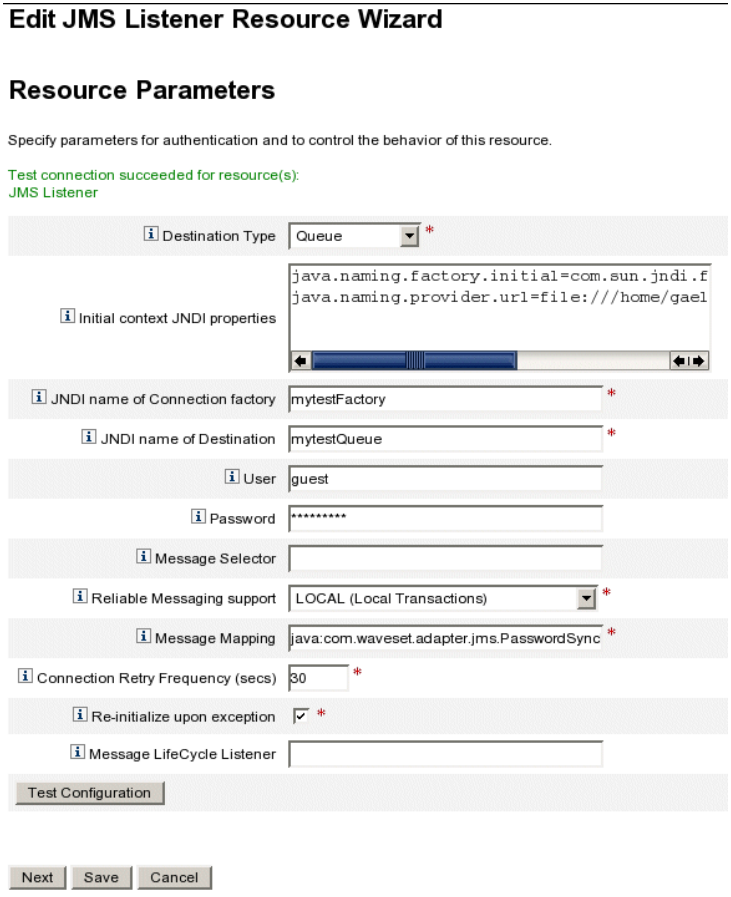
- **存储到文件**：如果 Identity Manager SOAP 处理程序和 Identity Manager 服务器在同一台服务器上运行（或者您没有可用目录），则可以将管理对象存储到文件。

  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

JMS 侦听器适配器配置的第一个页面类似于图 9-13 中的页面：

图 9-13 JMS 侦听器适配器资源参数页

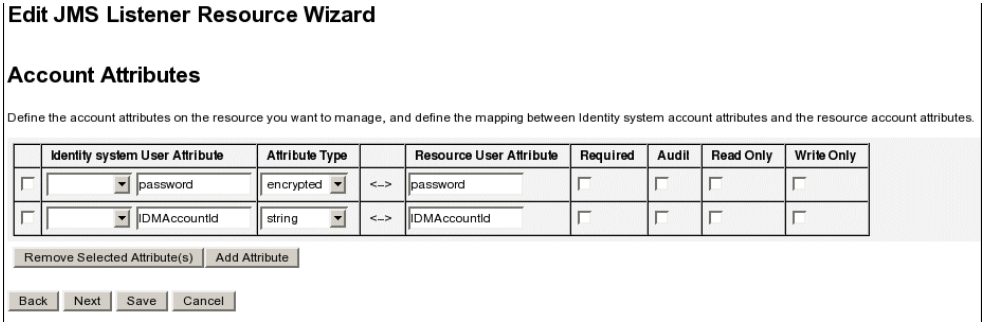


要配置 JMS 侦听器适配器：

1. 在 "Message Mapping" 字段中指定 **`java:com.waveset.adapter.jms.PasswordSyncMessageMapper`** 以将传入的 JMS 消息转换为同步用户密码工作流可以使用的格式。
2. 在此方案中，映射以下属性 （通过 `PasswordSyncMessageMapper` 使 JMS 侦听器适配器可使用这些属性）：
   - **IDMAccountId**：该属性由 PasswordSyncMessageMapper 根据在 JMS 消息中传递的 `resourceAccountId` 和 `resourceAccountGUID` 属性解析。

- **password**：可以在 SOAP 请求中收到加密的密码并在 JMS 消息中转发该密码。

图 9-14 映射 IDMAccountID 和 password 帐户属性



在模式映射中配置这些属性字段后，活动同步向导 （图 9-15）的 "Attribute Mappings" 部分中的资源即可使用这些属性。

注 此处不提供任何身份模板。

图 9-15 活动同步属性映射

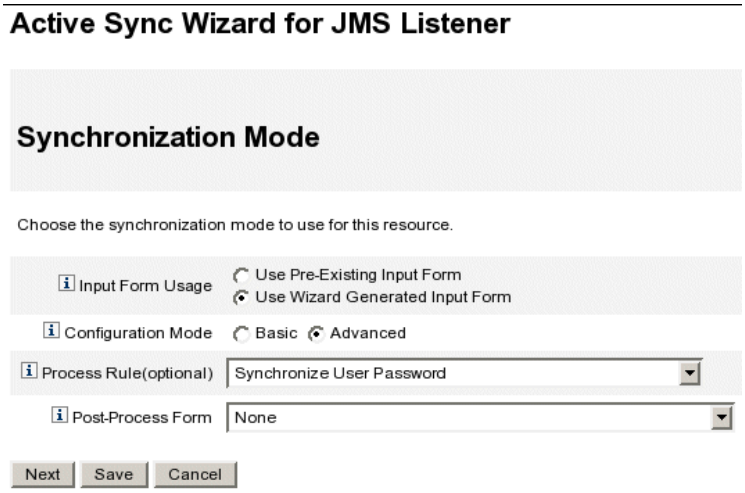
配置活动同步

使用 JMS 侦听器的活动同步向导在高级配置模式下为该方案配置活动同步。

1. 显示 "Synchronization Mode" 屏幕（图 9-16）时，您可以保留这些参数的默认值，并单击 "Next" 继续。

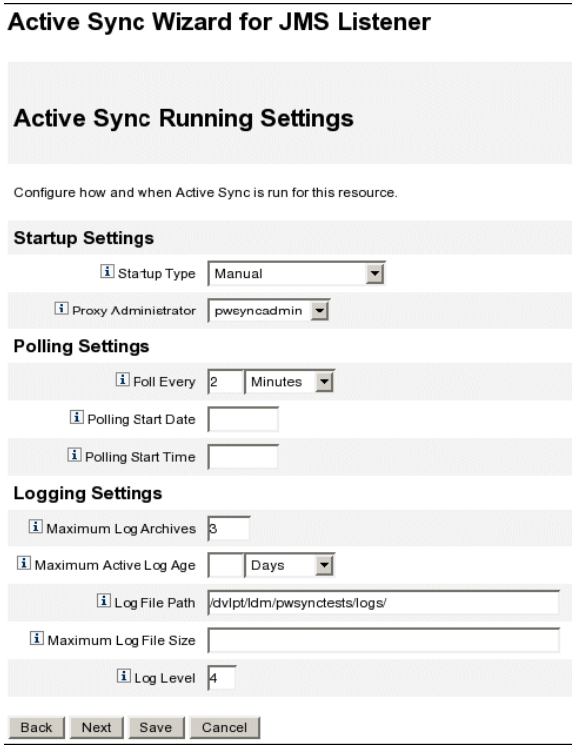
   默认的同步用户密码工作流接受来自 JMS 侦听器适配器的每个请求并签出 ChangeUserPassword 查看器，然后再签回 ChangeUserPassword 查看器。

图 9-16 "Synchronization Mode" 屏幕



2. 显示 "Active Sync Running Settings" 面板时，必须定义与空表单关联的代理管理员 (`pwsyncadmin`)。

图 9-17 "Active Sync Running Settings" 面板



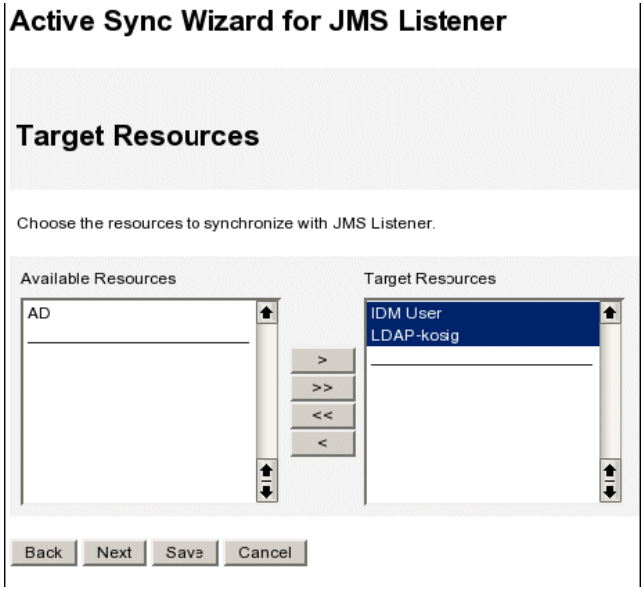
3. 出于调试目的，请将 "Log Level" 设置为 **4** 并指定日志文件路径，以在特定目录中生成详细日志文件。

   例如，图 9-17 中显示的日志文件将保存到 `/dvlpt/Idm/pwsynctests/logs/` 目录。

4. 完成后，单击 "Next" 继续。

5. 请勿更改接下来的两个活动同步向导面板中的默认值。只需单击 "Next"，直到显示 "Target Resources" 屏幕 （图 9-18）。

图 9-18 "Target Resources" 屏幕



6. 使用目标资源选择工具指定目标资源。从 "Available Resources" 列表中选择资源，然后单击 > 按钮将资源移入 "Target Resources" 列表。

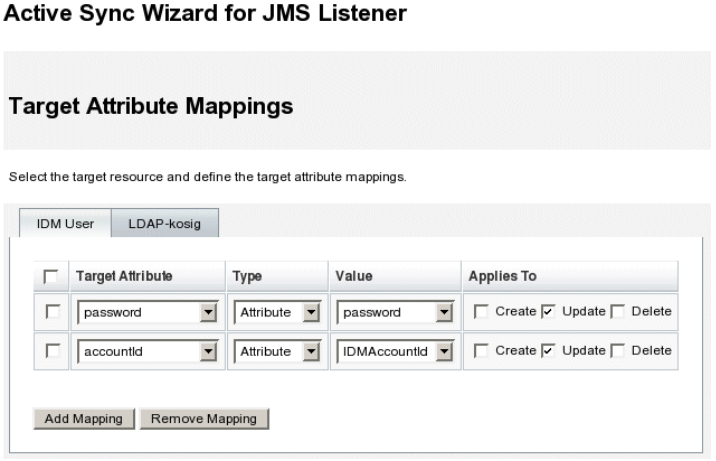
   例如，在该方案中，你要将 Windows 密码与 Sun Directory Server 同步，并且还要同步 Identity Manager 密码。

7. 单击 "Next"，显示 "Target Attribute Mappings" 面板后，选择 "IDM User" 选项卡（如果未选择）。

8. 在 "IDM User" 选项卡上，使用表指定 Identity Manager 用户的目标属性映射。

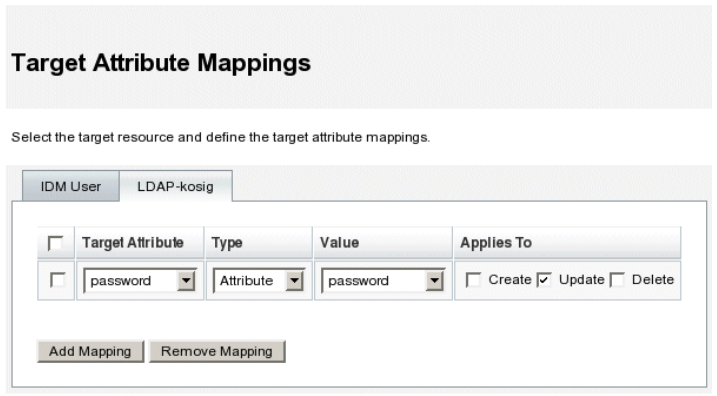
   例如，在图 9-19 中定义 `password` 和 `accountID`：

图 9-19 定义 password 和 accountID



9. 完成后，单击 "Add Mapping"。
10. 选择 "LDAP-kosig" 选项卡为 Sun Directory 定义目标属性映射 （图 9-20）：

图 9-20 为 Sun Directory 定义目标属性映射



11. 完成后，单击 "Add Mapping"，然后保存更改。

调试配置

您可以使用 Windows PasswordSync 配置应用程序来调试 Windows 端的配置。

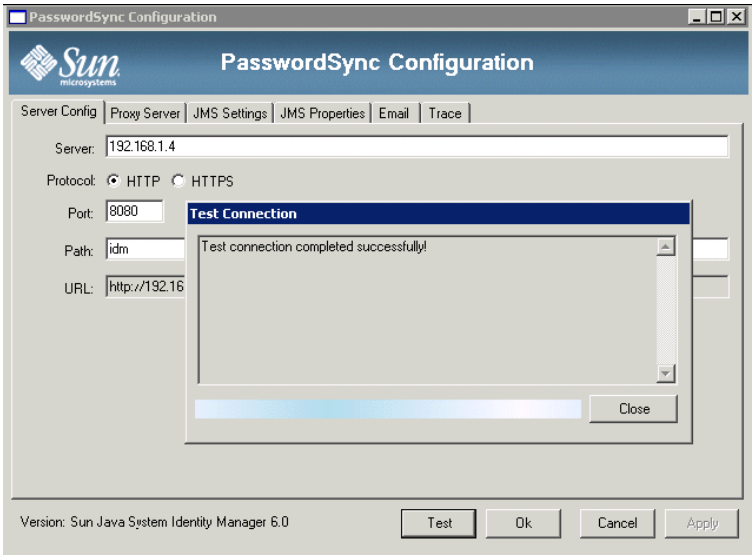
1. 如果还没有运行 PasswordSync 配置应用程序，请开始运行。

   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. 显示 "PasswordSync Configuration" 对话框后，单击 "Test" 按钮。

3. 将显示 "Test Connection" 对话框 （图 9-21），并出现一则消息，报告是否已成功完成测试连接。

图 9-21 "Test Connection" 对话框

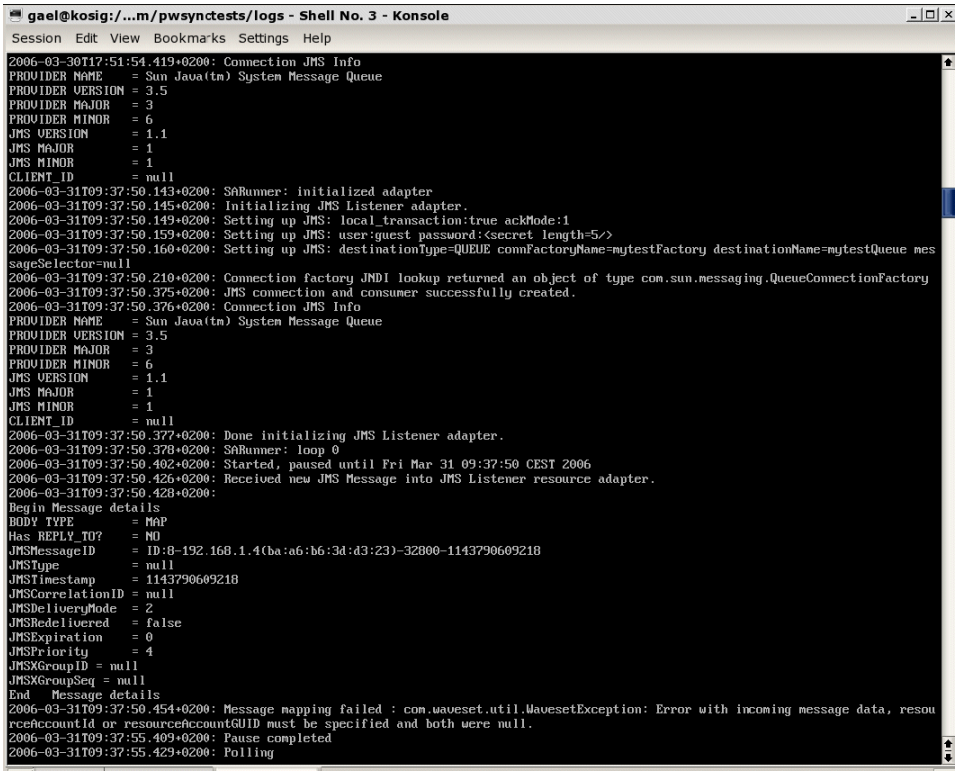


4. 单击 "Next" 关闭 "Test Connection" 对话框。

5. 单击 "OK" 关闭 "PasswordSync Configuration" 对话框。

   之后， JMS 侦听器适配器将运行调试模式，并生成包含调试信息的文件，类似于图 9-22 中的文件：

图 9-22 调试信息文件

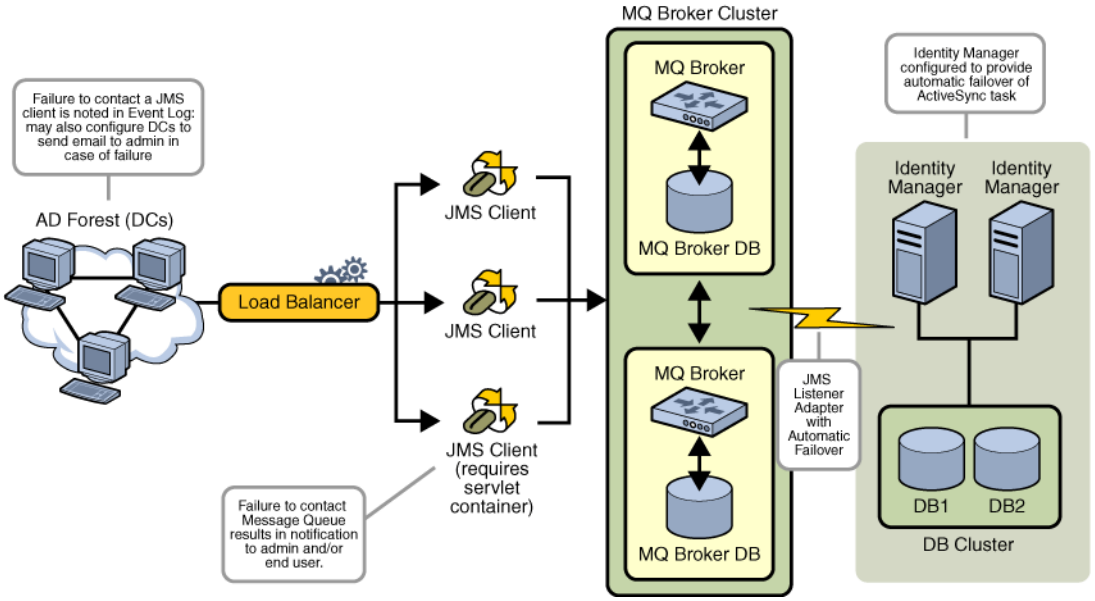


PasswordSync 的故障转移部署

PasswordSync 的体系结构有助于消除 Identity Manager 的 Windows 密码同步部署中的任何单点故障。

如果配置每个 Active Directory 域控制器 (Active Directory Domain Controller, ADC) 以通过负载平衡器连接到一系列 JMS 客户端中的一个客户端 （请参见图 9-23），则 JMS 客户端可向 Message Queue 代理群集发送消息，这确保了在任何 Message Queue 出现故障时也不会丢失任何消息。

图 9-23 PasswordSync 的故障转移部署



注 Message Queue 群集可能需要数据库以实现消息的持久保存。（供应商的产品文档中提供了有关配置 Message Queue 代理群集的说明。）

如果 Identity Manager 服务器上运行了配置为可用于自动故障转移的 JMS 侦听器适配器，该服务器将与 Message Queue 代理群集进行通讯。虽然适配器一次仅在一个 Identity Manager 上执行，但如果主 ActiveSync 服务器出现故障，则该适配器将开始在辅助 Identity Manager 服务器上轮询与密码相关的消息，并将密码更改传播到下游资源。

有关 PasswordSync 的常见问题

在不使用 Java Messaging Service 的情况下能否实现 PasswordSync？

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。可使用第 260 页上的“配置 PasswordSync”中所描述的过程配置 PasswordSync，但要注意以下不同之处：

- 不要配置 “JMS 设置”和 “JMS 属性”选项卡。
- 在 “用户”选项卡中，指定用于连接 Identity Manager 的帐户 ID 和密码。

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，您应该忽略第 268 页上的“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。

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？

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`（类型 `REG_MULTI_SZ` 的值）

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。

是否可以将 PasswordSync Servlet 安装在 Identity Manager 以外的其他应用服务器上？

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。

PasswordSync 服务是否将密码以明文发送到 lh 服务器？

虽然我们建议通过 SSL 运行 PasswordSync，但是在将敏感数据发送到 Identity Manager 服务器之前，所有数据都是加密的。

密码更改有时是否会导致 com.waveset.exception.ItemNotLocked？

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 10 章

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 允许利用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。（有关报告功能的更多信息，请参见第 7 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 中授予管理控制并进行管理。
- *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 用户可进行并发登录会话。但是，您可以通过更改系统配置对象中 `security.authn.singleLoginSessionPerApp` 配置属性的值将并发会话限制为每个登录应用程序一个会话。该属性是一个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。

密码管理

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

- **管理密码重置**
  - 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至 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

登录约束规则是应用于在登录应用程序中定义的登录模块组的。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。

Identity Manager 评估第一个登录模块组的约束规则，来确定要处理一个集合中的哪一个登录模块组。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。

代码示例 10-1 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

在菜单栏中，选择 **Configure**，然后选择 **Login** 以访问 "Login" 页。

登录应用程序列表显示：

- 已定义的每个 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 "Modify Login Application" 页中，可以为每个 Identity Manager 登录会话设置超时值 （限制）。选择小时数、分钟数和秒数，然后单击 **Save**。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 "Create Login Application" 和 "Modify Login Application" 页中，可以选择 "Disable" 选项来禁用登录应用程序，从而阻止用户登录。如果用户尝试登录已禁用的应用程序，则该界面将重定向到备用页面，指示当前已禁用该应用程序。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：

- 已定义的每个 Identity Manager 登录模块组
- 每个登录模块组包含的登录模块
- 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。从此列表中选择任一登录模块组对其进行编辑。

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，并且管理员登录成功。如果验证失败，则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。当配置为传递到 LDAP 时，这将允许用户通过 LDAP cn 或电子邮件地址登录到 Identity Manager。

  例如，如果指定：

  ```
  cn
  mail
  ```

并且如果用户尝试以 gwilson 身份登录，则 LDAP 资源首先尝试查找 cn=gwilson 的 LDAP 用户。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** - 选择登录关联规则，用于将用户提供的登录信息映射到 Identity Manager 用户。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。
- **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 "User Login" 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。

配置公共资源的验证

如果您有多个物理上或逻辑上相同的资源 （例如，两个为同一个物理主机定义的资源，或者几个表示 NT 或 AD 域环境中信任域服务器的资源），那么您可将系统配置对象中的一组资源指定为*公共资源*。

通过建立公共资源，您可以允许一个用户验证到这些公共资源之一，但通过使用另一个公共资源将用户映射到其相关的 Identity Manager 用户。例如，一个用户可能有一个链接到资源 AD-1 的 Identity Manager 用户的资源帐户。该登录模块组可能定义用户必须验证到资源 AD-2。如果 AD-1 和 AD-2 被定义为公共资源 （此种情况下为在同一个信任域中），那么如果该用户成功验证到 AD-2，则 Identity Manager 可通过查找资源 AD-1 中具有相同帐户 ID 的用户来映射到相关 Identity Manager 用户。

以下示例中显示了指定此系统配置对象属性的格式：

代码示例 10-2 配置公共资源的验证

```
<Attribute name=扮ommon resourcesí>
    <Attribute name=íCommon Resource Group Nameí>
        <List>
            <String>Common Resource Name</String>
            <String>Common Resource Name</String>
        </List
    </Attribute>
</Attribute>
```

配置 X509 证书验证

使用以下信息和过程配置 Identity Manager 的 X509 证书验证。

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 （客户端和服务器） 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。

还要为客户端验证选择所用的客户端证书。要进行验证：

1. 使用 Internet Explorer，选择 **Tools**，然后选择 **Internet Options**。
2. 选择 **Content** 选项卡。
3. 在 "Certificates" 区域中，单击 **Certificates**。
4. 选择客户端证书，然后单击 **Advanced**。

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

要配置 Identity Manager X509 证书验证：

1. 以 "Configurator" （或同等权限）身份登录 "Administrator Interface"。
2. 选择 **Configure**，然后选择 **Login**，以显示 "Login" 页。
3. 单击 **Manage Login Module Groups**，以显示 "Login Module Groups" 页。
4. 从列表中选择登录模块组。
5. 在 "Assign Login Module..." 列表中，选择 "Identity Manager X509 Certificate Login Module"。 Identity Manager 显示 "Modify Login Module" 页。
6. 设置成功登录的要求。可接受的值有：
   - **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，并且管理员登录成功。如果验证失败，则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 **Save**，返回到 "Modify Login Module Group" 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 **Save**。
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 **Save**。

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 "New User Name Rule"。在使用相关 `"Login Correlation Rule"` 未找到用户时，可使用此规则确定如何命名新创建的用户。

"New User Name Rule" 与 "Login Correlation Rule" 的可用输入参数相同。它返回单个字符串，该字符串用于创建新 Identity Manager 用户帐户的用户名。

idm/sample/rules 中包含一个新建用户名称规则样例，名为 NewUserNameRules.xml。

创建和导入登录配置规则

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 中包含一个内置关联规则，名为 Correlate via X509 Certificate subjectDN。

您也可以添加自己的关联规则。每个关联规则都必须遵循以下准则：

- 其 `authType` 属性必须设置为 `LoginCorrelationRule`。（在 `<LoginCorrelationRule>` 元素中设置 `authType=抛oginCorrelationRuleí`。）
- 它会返回 `AttributeConditions` 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`。

传递到登录配置规则的参数有：

- 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有：

```
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配置规则返回包含一个或多个 AttributeConditions 的列表。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 的登录关联规则样例。

创建自定义关联规则后，必须将其导入 Identity Manager。在 "Administrator Interface" 中选择 **Configure**，然后选择 **Import Exchange File**，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 请求中客户端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。要更正这一点：

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 调试设备编辑 LoginConfig 对象。
3. 将 Identity Manager X509 证书登录模块的 <LoginConfigEntry> 中的 <AuthnProperty> 名称改为正确的名称。

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更多信息，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 10-1 受加密保护的数据类型

数据类型	RSA MD5	NIST Triple DES 168 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[1]
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	

1. 通过系统配置对象使用 `pbeEncrypt` 属性或 "Manage Server Encryption" 任务进行配置。

服务器加密密钥的问题及答案

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。

服务器加密密钥来自哪里？

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** - 此密钥将编译为服务器代码。
- **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。

在哪里维护服务器加密密钥？

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。

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？

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）。

如何更新服务器加密密钥？

Identity Manager 提供了名为 "Manage Server Encryption" 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更多信息，请参见本章中的 “管理服务器加密”。

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？

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。

为了避免出现多密钥问题，以及更好地维护数据完整性，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。

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？

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。

怎样保护服务器密钥？

如果未将服务器配置为使用基于密码的加密 (PBE) - PKCS#5 加密（通过 `pbeEncrypt` 属性或 "Manage Server Encryption" 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 PBEwithMD5 和 DES 必须可用。默认情况下，Identity Manager 不包括此加密法，但此加密法采用 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。

我可以导出服务器密钥以安全地存储在外部吗？

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。

将对服务器和网关之间的哪些数据进行加密？

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。

有关网关密钥的问题及答案

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。

加密或解密数据的网关密钥来自哪里？

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。

如何将网关密钥分发到网关？

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 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。网关将使用在默认密钥中编译的网关密钥解密网关密钥，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。如果有，则使用。如果没有，则使用默认密钥。一旦网关在注册表中设置了密钥，则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和建立到网关的连接。

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？

Identity Manager 提供了名为 "Manage Server Encryption" 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中 `pbeEncrypt` 属性的值。

在服务器、网关的什么地方存储网关密钥？

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。

怎样保护网关密钥？

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。有关更多信息，请参见前面标题为 “怎样保护服务器密钥？”的一节。

我可以导出网关密钥以安全地存储在外部吗？

可以通过 "Manage Server Encryption" 任务导出网关密钥，就像导出服务器密钥一样。有关更多信息，请参见前面标题为 “我可以导出服务器密钥以安全地存储在外部吗？”的一节。

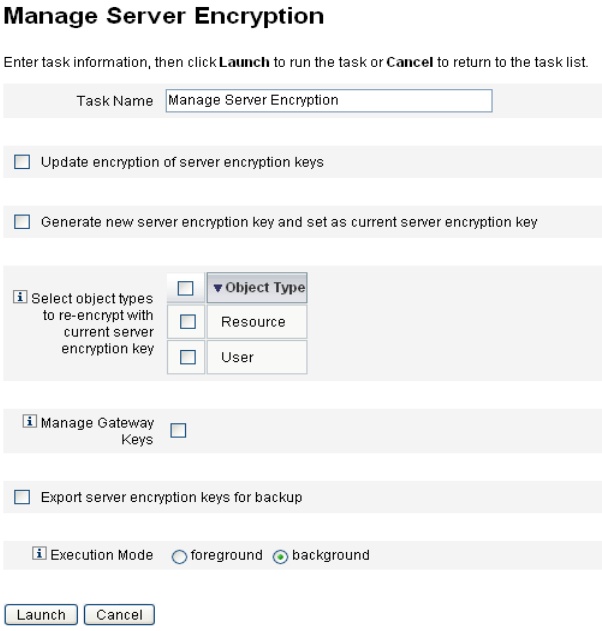
如何销毁服务器和网关密钥？

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

Identity Manager 服务器加密功能允许您创建新的 3DES 服务器加密密钥，然后使用 3DES 或 PKCS#5 加密对这些密钥进行加密，如下图中所示。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 （该任务可从**服务器任务**选项卡访问）。

图 10-1 管理服务器加密任务



选择 **Run Tasks**，然后从列表中选择 "Manage Server Encryption"，为此任务配置以下信息：

- **更新服务器加密密钥的加密** - 选择此选项可以指定是使用默认 (3DES) 加密还是使用 PKCS#5 加密来对服务器加密密钥进行加密。选择此选项时，将显示两种加密选择 （"Default" 和 "PKCS#5"），请选择其中一个。
- **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** - 选择此选项可以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。
- **选择要使用当前服务器加密密钥重新加密的对象类型** - 选择一个或多个要使用当前加密密钥重新加密的 Identity Manager 对象类型 （如资源或用户）。
- **管理网关密钥** - 如果选择该选项，则该页将显示以下网关密钥选项：
  - **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**
  选择此选项可同步所有新网关，或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。

- **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 会显示一个附加的字段，用于指定导出该密钥的路径和文件名。

注 如果您要使用 PKCS#5 加密方法并且选择生成和设置新的服务器加密密钥，则您还应选择此选项。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）。

- **执行模式** - 选择在后台 （默认选项）还是在前台运行此任务。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，执行此任务会需要一些时间，且最好在后台运行此任务。

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

您应：

- 通过使用 https 的安全 Web 服务器访问 Identity Manager。
- 重置默认 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

您应：

- 定期更改默认 Identity Manager 管理员帐户 （管理员和配置器）的密码。
- 如果当前没有使用系统，请注销 Identity Manager。
- 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。
2. 更改下列各行中的数字值：

```
<session-config>
  <session-timeout>30</session-timeout>
</session-config>
```

第 11 章

身份审计

本章介绍了 Identity Manager 中的功能，这些功能使您可以设置审计控制以监视和管理企业信息系统和应用程序中的审计和遵循性。

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。

本章所述功能的重点在于如何执行审计查看和实现实践，以帮助您维护安全性控制，并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：

身份审计的目标

身份审计解决方案可通过以下方式提高审计性能：

- *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 审计策略功能可定义违规的*规则*（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。

- *请求时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”选项卡还提供了违规的图形报告。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法规遵循性*

  执行周期性访问查看可收集用户权利文件记录，并确定哪些权利文件需要查看。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 提供两种不同的功能，用于审计用户帐户权限和访问权限，以及维护和证明遵循性。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*表示策略将应用于所有置备操作，因此无法使用不符合当前策略的方法修改帐户。

通过将审计策略分配给组织和/或用户，可以启用连续遵循性。对用户执行的任何置备操作都将导致对分配给用户和组织的策略进行评估。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。

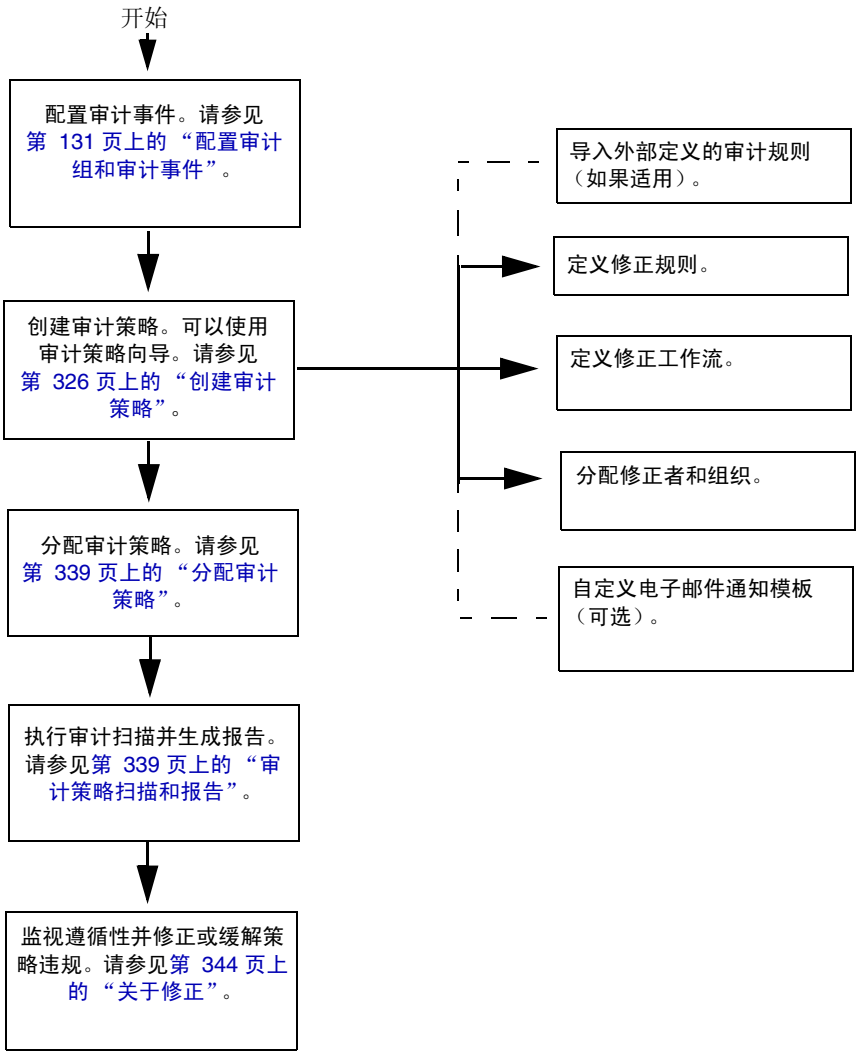
具有 “审计者管理员”权能的 Identity Manager 用户可以创建审计策略，并通过定期执行策略扫描和查看策略违规来监视对这些策略的遵循性。可以通过修正和缓解过程管理违规。

有关 Auditor 管理员权能的详细信息，请参见第 149 页上的 “了解和管理权能”。

Identity Manager 审计允许常规的用户扫描，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

下图显示了完成本节中所述审计任务的逻辑任务流：


开始
配置审计事件。请参见第 131 页上的 “配置审计组和审计事件”。
创建审计策略。可以使用审计策略向导。请参见第 326 页上的 “创建审计策略”。
分配审计策略。请参见第 339 页上的 “分配审计策略”。
执行审计扫描并生成报告。请参见第 339 页上的 “审计策略扫描和报告”。
监视遵循性并修正或缓解策略违规。请参见第 344 页上的 “关于修正”。
导入外部定义的审计规则（如果适用）。
定义修正规则。
定义修正工作流。
分配修正者和组织。
自定义电子邮件通知模板（可选）。

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 352 页上的 “周期性访问查看和证明”。

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。要查看或修改遵循性管理组存储的事件，请从菜单栏中选择**配置**，然后单击**审计**。在 "Audit Configuration" 页上，选择 **Compliance Management** 审计组名称。

有关设置审计配置组的详细信息，请参见 “配置”一章中的第 131 页上的 “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 12 章 “审计日志记录”。

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 11-1 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文件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。

管理员界面的遵循性区域

可在 Identity Manager 管理员界面的 “遵循性” 区域中创建和管理审计策略。在菜单栏中选择**遵循性**可访问 “管理策略” 页，该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。

管理策略

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 “使用审计策略” 一节中找到有关这些任务的详细信息。

管理访问扫描

使用 “遵循性” 区域中的**管理访问扫描**选项卡可创建、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 352 页上的 “周期性访问查看和证明”。

访问查看

使用 “遵循性” 区域中的该选项卡，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。

有关该功能的详细信息，请参见第 361 页上的 “管理访问查看”。

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：

- **Policy rules**，其中可包含以 XPRESS、XML Object 或 JavaScript 语言编写的定义特定违规的函数。
- **Remediation workflow**，可在审计扫描识别出策略规则的违规时启动（可选）。
- **修正者**，或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。

审计策略规则

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。

规则必须为 `SUBTYPE_AUDIT_POLICY_RULE` 或 `SUBTYPE_AUDIT_POLICY_SOD_RULE` 子类型。由审计策略向导生成或引用的规则会自动分配此子类型。

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。

有关规则逻辑的讨论，请参见 “*Identity Manager 部署工具*”中的 “*使用规则*”。

修正工作流

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 326 页上的 “（可选）将工作流导入 Identity Manager”*。

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，请参见本章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

您负责处理应付账款和应收帐款，而且必须执行一些过程，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：

- 由四条规则组成的集合。每条规则指定一个构成策略违规的条件。
- 启动修正任务的工作流。
- 指定的管理员或修正者组，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）。

使用审计策略

Identity Manager 提供了审计策略向导功能，以帮助您设置审计策略。定义审计策略后，您可以对策略执行各种操作，如修改或删除该策略。本节中的主题介绍了如何创建和管理审计策略和审计策略规则。

审计策略向导还可以创建规则，但仅限于它可以创建的规则类型。使用 Identity Manager IDE 可创建功能更强大的规则供向导使用。

默认情况下，使用向导创建的所有规则都属于 authType `AuditPolicyRule`。您所创建的任何审计策略规则 （使用向导或 Identity Manager IDE）都应该指定此 authType。

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。

创建审计策略

"Audit Policy Wizard" 可指导您完成创建审计策略的过程。要访问"Audit Policy Wizard"，请在界面的 **Compliance** 区域中单击 **Manage Policies**，然后创建新的审计策略。

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 **Next**移至下一步骤。

准备工作

在创建审计策略之前需制定大量的计划，包括以下任务：

- 确定要在 "Audit Policy Wizard" 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。
- 导入要包含在新策略中的任何修正工作流或规则。
- 请确保您具有创建审计策略所需的权能。请参见第 149 页上的 “了解和管理权能”中的所需权能。

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。使用审计策略向导创建规则时，应执行以下操作：

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。

（可选）将任务划分规则导入 Identity Manager 中

"Audit Policy Wizard" 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 Identity Manager

要使用 Identity Manager 当前未提供的修正工作流，请完成以下任务以导入外部工作流：

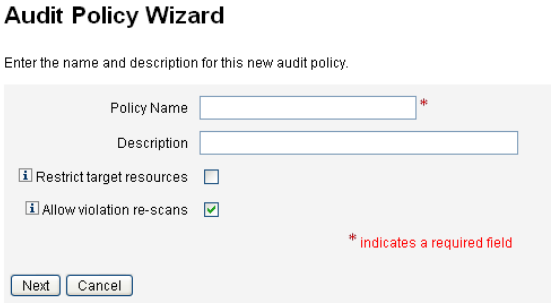
1. 设置 `authType='AuditorAdminTask'` 并添加 `subtype='SUBTYPE_REMEDIATION_WORKFLOW'`。您可以选择使用 Identity Manager IDE 或 XML编辑器设置这些配置对象。
2. 使用 “导入交换文件”选项导入工作流。（可从**配置**选项卡访问此功能）。

成功导入工作流后，它会显示在 "Audit Policy Wizard" 的 "Remediation Workflow" 选项列表中。

命名和描述审计策略

在审计策略向导 （如图 11-1 所示）中输入新策略的名称及其简要描述。

图 11-1 Auto Policy Wizard：输入名称与描述屏幕



注 审计策略名称不能包含以下字符：'（撇号）、.（句点）、|（管道字符）、[（左括号）、]（右括号）、,（逗号）、:（冒号）、$（美元符号）、"（双引号）或 =（等号）。

如果您只希望在执行扫描时访问选定的资源，请启用 **Restrict target resources** 选项。

如果您希望在违规修正后立即重新扫描用户，请启用**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。

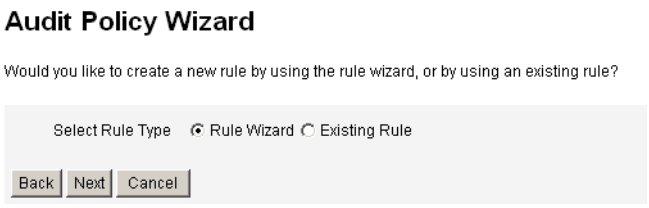
单击 **Next** 进入下一页。

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。）

如图 11-2 所示，您可以选择使用 Identity Manager 规则向导创建您自己的规则，也可以结合使用现有规则。默认情况下将选择 "Rule Wizard" 选项。有关创建规则的说明，请单击**下一步**启动 “规则向导” 并转至第 331 页上的 “使用规则向导创建新规则”。

图 11-2 Audit Policy Wizard：选择规则类型屏幕



选择现有规则

选择规则选项后，请单击 **Existing Rule** 将现有规则包含在新策略中。然后，单击 **Next** 查看并选择您有权访问的现有审计策略规则。

在 "Rules" 选项列表中选择其他规则，然后单击 **Next**。

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 324 页上的 “审计策略规则”中描述的附加属性。

添加规则

可以使用向导创建其他规则，也可以导入规则。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。

根据需要，单击 **AND** 或 **OR** 继续添加规则。要删除规则，请选择规则然后单击 **Remove**。

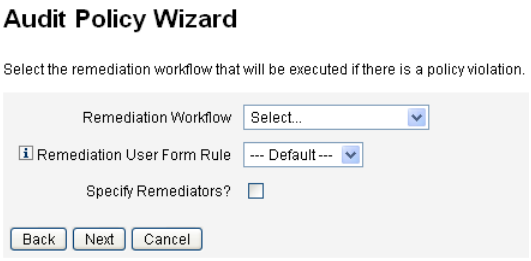
仅在*所有*规则的布尔表达式均评估为 true 时，才发生策略违规。使用 AND/OR 运算符对规则分组后，即使所有的规则均未评估为 true，策略也可能评估为 true。Identity Manager 仅在规则评估为 true，且策略表达式也评估为 true 时，才创建违规。审计策略向导无法明确控制布尔表达式嵌套，因此最好不要构建深层表达式。

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 11-3 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 集成开发环境 (IDE) 创建的工作流的信息，请参见第 326 页上的 “（可选）将工作流导入 Identity Manager”。

选择**修正用户表单规则**可以选择一条规则，用于计算通过修正编辑用户时所应用的用户表单。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，请选择**是否指定修正者？**。如果启用此选项，然后单击**下一步**，则会显示 “指定修正者”页。如果不启用此选项，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

如果选择指定修正者，则检测到此策略违规时，会通知分配了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。

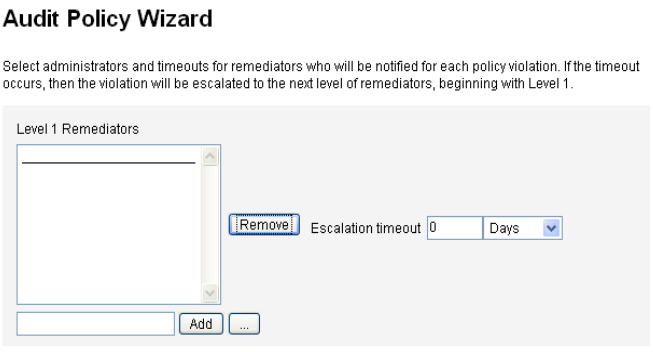
注 如果为选定的最高级别修正者指定了提升超时值，则提升超时时将从列表中删除工作项目。默认情况下，提升超时值设置为 0。在这种情况下，工作项目不会过期，并保留在修正者的列表中。

"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，也可以单击 **...**（更多）以搜索用户 ID。在“前缀”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**。

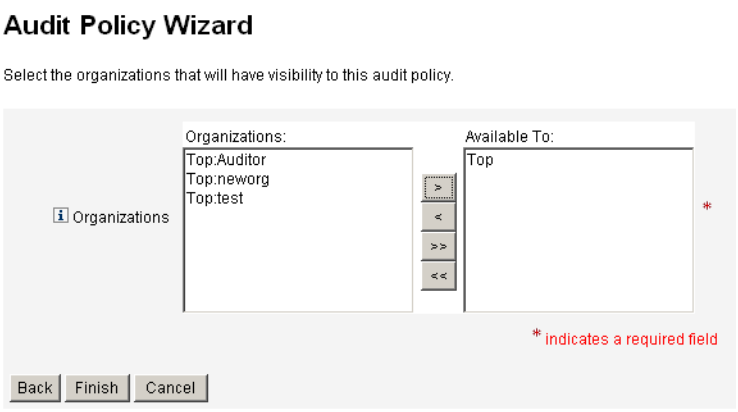
图 11-4 审计策略向导：选择级别 1 修正者区域



选择可访问此策略的组织

使用该屏幕 （如图 11-5 所示）可选择可以查看和编辑此策略的组织。

图 11-5 Audit Policy Wizard：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。

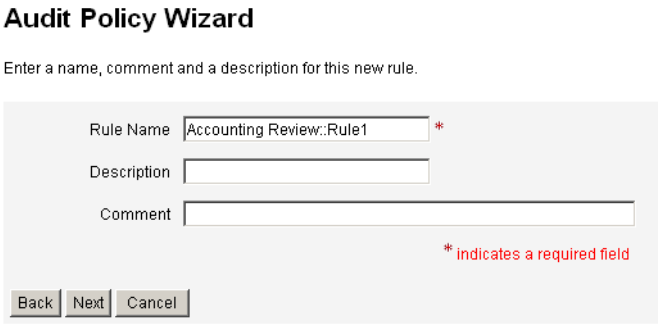
使用规则向导创建新规则

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。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 "Review Policy Violations" 页中。

图 11-6 Audit Policy Wizard：输入规则描述屏幕



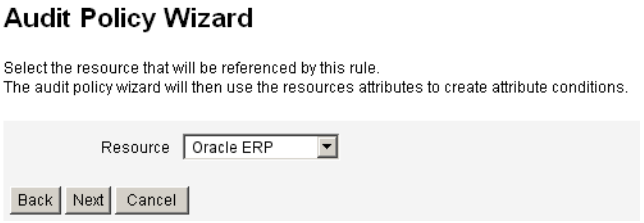
例如，如果要创建一条规则，用以确定 Oracle ERP responsibilityKey 属性值同时为 `Payable User` 和 `Receivable User` 的用户，则可在 "Description" 字段中输入以下文本：**确定同时具有应付款用户和应收款用户职责的用户**。

使用 "Comments" 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 11-7 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 “*Identity Manager 资源参考资料*”。

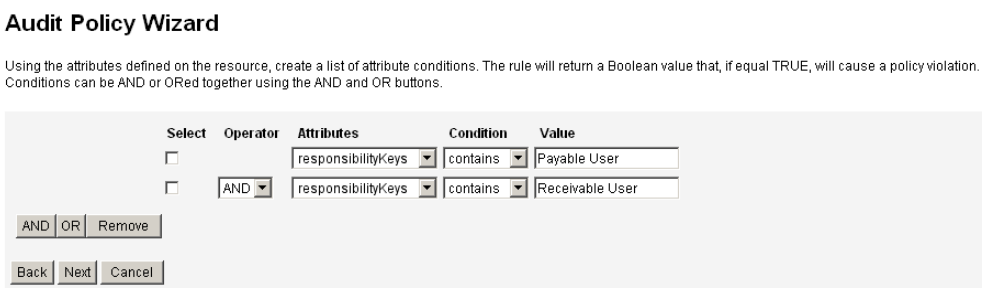
单击 **Next** 移至下一页。

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。

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 responsibilityKey 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 11-8 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。如果指定了多条规则，则策略评估者将始终先执行 AND 操作，再执行 OR 操作。例如 R1 AND R2 AND R3 或 R4 AND R5 (R1 + R2 + R3) | (R4 + R5)。

以下代码示例显示了您已在此屏幕中创建的规则的 XML：

代码示例 11-1 新创建规则的 XML 语法示例

```
<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 **Remove**。

单击 **Next** 继续使用 "Audit Policy Wizard"。然后即可使用向导创建新规则或添加现有规则，以添加更多规则。

编辑审计策略

审计策略的普通编辑任务包括：

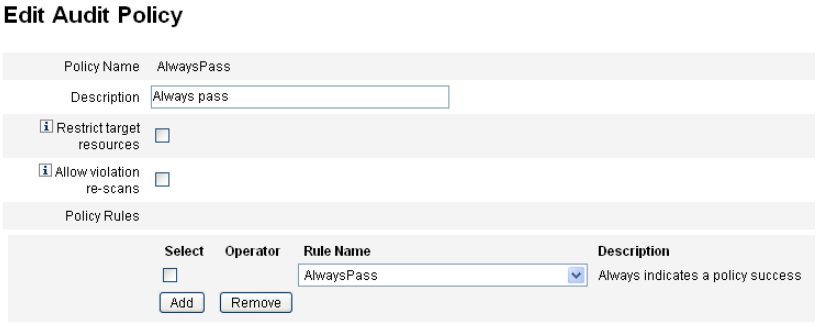
- 添加或删除规则
- 更改目标资源
- 调整有权访问策略的组织列表
- 更改与每个修正级别关联的提升超时时间
- 更改与策略关联的修正工作流

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

图 11-9 "Edit Audit Policy" 页：标识和规则区域



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 **Add** 追加一个新字段，可使用该字段选择要添加的规则。

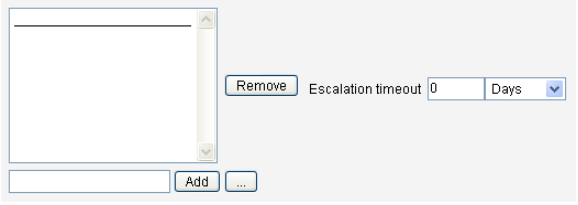
更改策略使用的规则

在 "Rule Name" 列中，从选项列表中选择其他规则。

修正者区域

图 11-10 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 11-10 "Edit Audit Policy" 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

- 调整提升超时时间

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

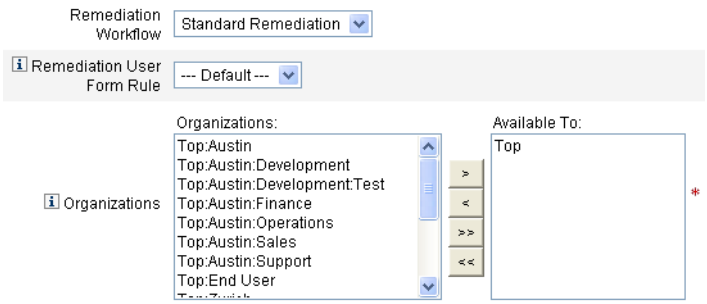
选择超时值，然后输入新值。默认情况下未设置任何超时值。

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 11-11 显示了用于为审计策略指定修正工作流和组织的区域。

图 11-11 "Edit Audit Policy" 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 **Save**。

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 **Save**。

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，同时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。

调试规则

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>
```

问题

我无法在 Identity Manager 界面中看到我的工作流。

解决方案

请确认以下事项：

- 您已经在工作流中添加了 `subtype='SUBTYPE_REMEDIATION_WORKFLOW'` 属性。在 Identity Manager 管理员界面中看不到没有此子类型的工作流。
- 您具有 authType `AuditorAdminTask` 的权能。
- 您可以控制工作流所在的组织。

问题

我已导入规则，但在审计策略向导中看不到这些规则。

解决方案

请确认以下事项：

- 每条规则都属于 `subtype='SUBTYPE_AUDIT_POLICY_RULE'` 或 `subtype='SUBTYPE_AUDIT_POLICY_SOD_RULE'` 子类型。
- 您具有 authType `AuditPolicyRule` 的权能。

- 您可以控制工作流所在的组织。

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 （即，通过用户帐户或组织分配所分配的策略）进行重新评估。

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。

要从 "Accounts" 区域对用户帐户或组织启动扫描，请：

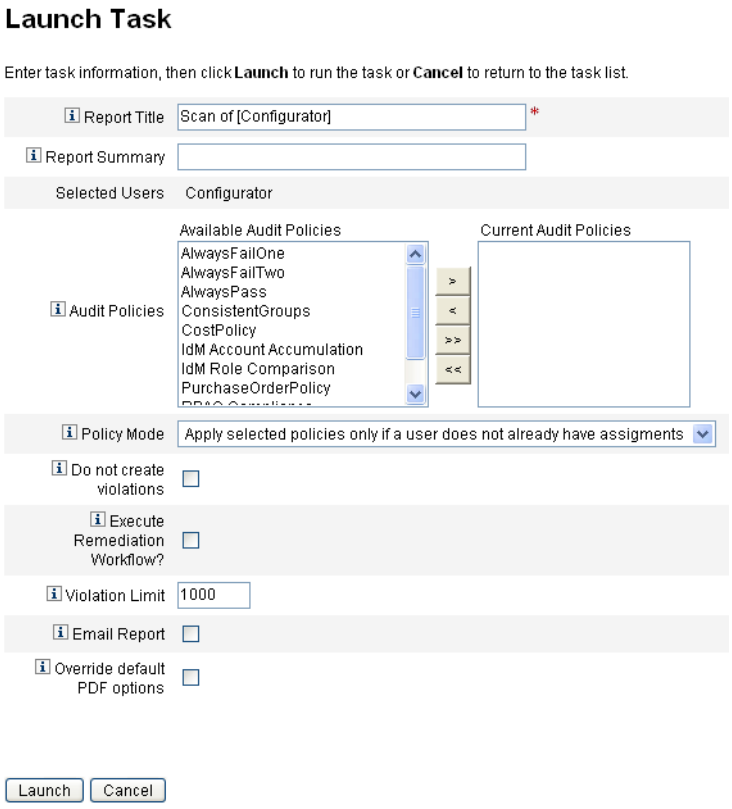
1. 选择**帐户**。
2. 在 “帐户”列表中，执行以下任一操作：

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 "Organization Actions" 选项列表中选择 **Scan**。

将显示 "Launch Task" 对话框。表 11-3 是审计策略用户扫描的 "Launch Task" 页的示例。

图 11-12 启动任务对话框



3. 在 "Report Title" 字段中为扫描指定标题。此字段为必填字段。您也可以在 "Report Summary" 字段中为扫描指定描述。

4. 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。

5. 选择 **Policy Mode**。这决定了选定的策略与已分配策略的用户的交互方式。分配可直接来自用户或来自分配了用户的组织。

6. （可选）选择**不创建违规**选项。启用此选项后，将对审计策略进行评估并报告违规，但不会创建或更新遵循性违规，也不会执行修正工作流。但是，由扫描产生的任务将显示应该创建的违规，这样在测试审计策略时，此选项非常有用。
7. 选中 **Execute Remediation Workflow?** 以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。
8. 编辑**违规限制**值，以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。
9. 选中 **Email Report** 以指定报告的收件人。您也可使 Identity Manager 附加一个包含 CSV （逗号分隔值）格式报告的文件。
10. 如果要覆盖默认 PDF 选项，则启用**覆盖默认 PDF 选项**选项。
11. 单击 **Launch** 开始扫描。

    要查看审计扫描的报告结果，请查看 "Auditor Reports"。

使用 Auditor 报告

Identity Manager 提供了许多 Auditor 报告。下表介绍了这些报告。

表 11-2 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文件之间的重叠部分和/或差异部分 （以确定范围是否随时间而变化）；用户和权利文件之间的重叠部分和/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文件）。
访问查看详细信息	显示所有用户权利文件记录的当前状态。该报告可以按用户的组织、访问查看和访问查看实例、权利文件记录的状态以及证明者进行过滤。
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 11-2 Auditor 报告描述

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。
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。

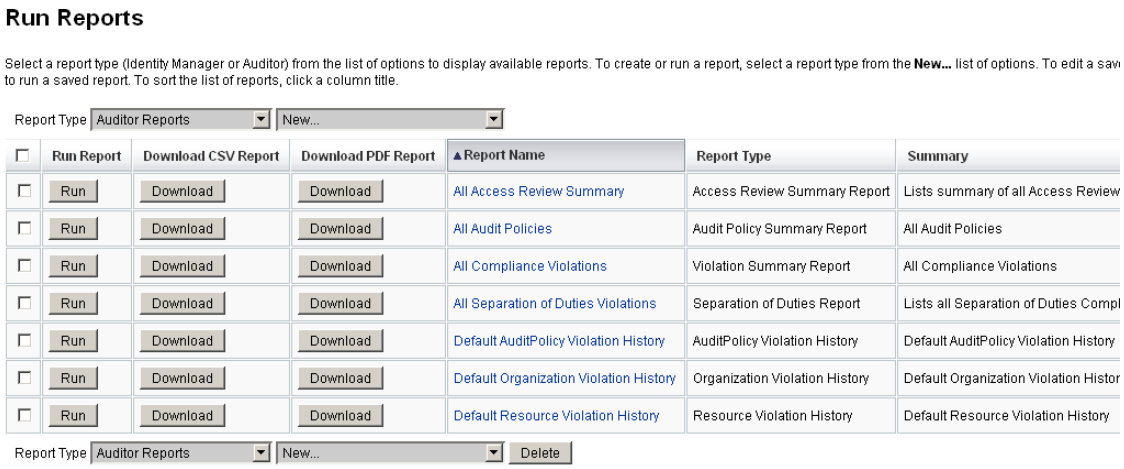
可通过 Identity Manager 界面中的 "Report" 选项卡查看这些报告。

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。

图 11-13 显示了具有已定义 Auditor 报告列表的 "Run Reports" 页示例。

图 11-13 "Run Reports" 页选项



要创建 Auditor 报告，请执行以下步骤：

1. 从菜单栏中选择 **Reports**。
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（如果定义了新报告）或已更改的报告条件 （如果编辑了现有报告）。
- 保存报告 - 单击**保存**保存报告。保存报告后，您可从 "Run Reports" 页 （报告列表）运行报告。

从 "Run Reports" 页运行报告后，您可以通过 "View Reports" 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 204 页上的 “调度报告”。

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（指定的用户，允许评估并响应审计策略违规）进行处理。

修正者提升

Identity Manager 允许您定义三个修正者提升的级别。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，则该请求再次被提升至级别 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，验证检查的行为如下：

- 拥有者为尝试执行该操作的用户，或
- 拥有者位于由尝试执行该操作的用户所控制的组织中，或
- 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：

```
UserForm: Remediation List
```

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 323 页上的 “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** - 修正者指出已经为修复资源问题执行了某些操作。

  修改遵从性违规时， 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 "Policy Violation Notice" 电子邮件模板（可通过选择 **Configuration** 选项卡，然后再选择 **Email Templates** 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 127 页上的 “自定义电子邮件模板”。

使用修正页

选择**工作项目**，然后选择**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 347 页上的 “查看暂挂请求”
- 第 348 页上的 “查看已完成的请求”
- 第 348 页上的 “更新表格”

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 **List Remediations for** 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，也可以单击 **...**（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** - 所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** - 请求修正者执行的操作。
- **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”）

- **Date of Request**：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 **My Work Items** 选项卡，然后单击 **History** 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文件
- **对象名称** - 所违反的审计策略的名称
- **资源** - 提供修正者的帐户 ID （也可能显示 N/A）
- **ID** - 始终显示 N/A
- **结果** - 始终显示成功

单击表格中的时间戳将打开 "Audit Events Details" 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。

更新表格

要更新 "Remediations" 表中提供的信息，请单击 **Refresh**。“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 "Remediations" 页

在 "Remediations" 页缓解暂挂策略违规：

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。

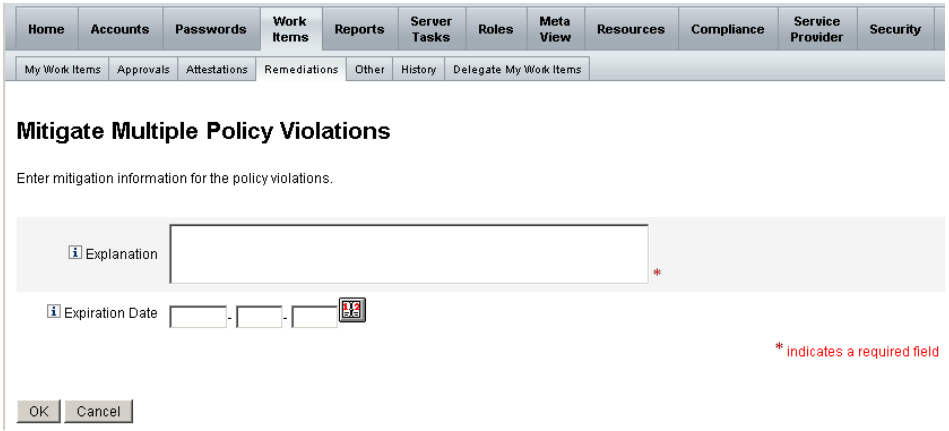
注 Identity Manager 只允许输入一组描述缓解操作的注释。除非各个违规是相关的，只需一个单独的注释即可，否则，您可能不想执行批量缓解。

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 **Mitigate**。

   将显示 “缓解策略违规” 页 （或 “缓解多项策略违规” 页）：

图 11-14 "Mitigate Policy Violation" 页



3. 在 “说明” 字段中输入有关缓解的注释。（此字段为必填字段）。

   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 "Remediate Policy Violation" 页 （或 "Remediate Multiple Policy Violations" 页）。
4. 在 "Comments" 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，方法如下：

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 **Forward**。

   将显示 “选择并确认转发”页。

图 11-15 "Select and Confirm Forwarding" 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 （如相关的权利文件历史中所述）。

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文件历史
- 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 - 定义并运行 （或调度运行）的扫描，可以评估指定的一组用户的*用户权利文件*，并执行基于规则的评估以确定是否需要进行证明。
- 证明 - 通过批准或拒绝用户权利文件来响应证明请求的进程。

*用户权利文件*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文件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
- 创建用户权利文件记录
- 确定每个用户权利文件记录是否需要证明
- 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
- 如果在指定的超时期间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文件记录

有关修正权能的描述，请参见第 369 页上的 “访问查看修正”。

所需的管理员权能

要进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 149 页上的 “了解和管理权能”。

证明

*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文件的适当性。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识别出需要查看的权利文件记录后启动。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文件记录，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文件记录，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文件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文件发送通知。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，验证检查的行为如下：

- 拥有者为尝试执行该操作的用户，或
- 拥有者位于由尝试执行该操作的用户所控制的组织中，或
- 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` - 包含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：

`UserForm: AccessApprovalList`

.

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 "Follow Delegation" 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。有关此任务的详细信息，请参见 “*Identity Manager 工作流、表单和视图*”。

创建访问扫描

要定义访问查看扫描，请执行以下步骤：

1. 选择**遵循性**，然后选择**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）、|（管道字符）、[（左括号）、]（右括号）、,（逗号）、:（冒号）、$（美元符号）、"（双引号）或 =（等号）。

---

4. （可选）添加有助于识别扫描的描述。

5. （可选）启用**动态权利文件**选项。如果启用该选项，则会为证明者提供以下附加选项：

   - 可以立即重新扫描暂挂证明，以刷新权利文件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。经过修正后，权利文件数据将被刷新并重新进行评估，以确定是否需要证明。

6. 从以下选项中选择 **User Scope Type**：（此字段为必填字段）。

   - **根据属性条件规则** - 选择此选项可以根据选定的用户范围规则扫描用户。Identity Manager 提供了以下规则：
     - 所有管理员
     - All Non-Administrators
     - Users without a Manager

注 可通过使用 Identity Manager 集成开发环境 (IDE) 来添加用户范围规则。有关详细信息，请参见*Identity Manager 部署工具*。

   - **分配给资源** - 选择此选项可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”区域，可在该区域中指定资源。
   - **组织成员** - 选择此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** - 选择此选项可扫描已报告给选定管理员的所有用户。管理员分层结构取决于用户 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文件记录中。此信息可简化自动批准或拒绝，因为该规则可将用户权利文件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 **Review Process Owner**。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文件，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 "Follow Delegation"。

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，每个用户权利文件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 创建用户权利文件记录所需的处理时间。

12. **执行违规修正** - 选择此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 （如果可用）。

    此工作流用于将要查看的用户权利文件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提升，此工作流将负责提升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。

14. **证明者规则** - 选择 “默认证明者”规则，或选择自定义的证明者规则 （如果可用）。

    证明者规则将作为输入值提供给用户权利文件记录，并且返回证明者名称列表。如果选择了 "Follow Delegation"，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文件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。有关自定义规则的信息，请参见 *Identity Manager 部署工具*指南。

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提升超时值。默认的提升超时值为 0 天。

    该规则将为已经过提升超时阶段的工作项目指定提升链。“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提升超时值。

16. **查看确定规则** - 选择以下规则之一可指定扫描进程将如何确定权利文件记录的处理方式：（此字段为必填字段）。

    - **拒绝更改的用户** - 自动拒绝用户权利文件记录，如果该用户权利文件与上一个具有相同访问扫描定义的用户权利文件不同，且已批准上一个用户权利文件。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文件相同的用户权利文件。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文件记录，如果该用户权利文件与上一个具有相同访问扫描定义的用户权利文件不同，且已批准上一个用户权利文件。批准所有与先前已批准的用户权利文件相同的用户权利文件。默认情况下，此规则只比较用户视图的 “帐户”部分。
    - **查看所有用户** - 强制执行手动证明所有用户权利文件记录。

注 "Reject Changed Users" 和 "Review Changed Users" 规则将比较用户权利文件和相同访问扫描 （其中已批准权利文件记录）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。有关自定义规则的信息，请参见 *Identity Manager 部署工具*。

此规则可以返回以下值：

- -1 - 不需要任何证明
- 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）

17. **修正者规则** - 选择规则，用于确定在执行自动修正时，应该由谁修正特定用户的权利文件。该规则可以检查用户的当前用户权利文件和违规，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。权利文件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文件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。请参见步骤 9。

      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** - 使用此选项可指定扫描在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 **Save** 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：

- 启动访问查看
- 调度访问查看任务
- 管理访问查看进度
- 修改扫描属性
- 取消访问查看

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 **Launch** 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 **Save** 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

可以使用**访问查看**选项卡监视访问查看的进度。可通过 **Compliance** 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：

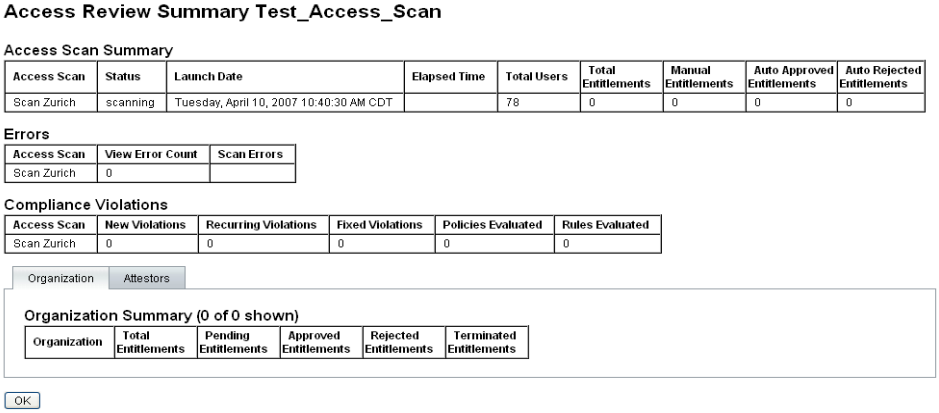
- **状态** - 查看进程的当前状态：正在启动、正在终止、已终止、正在执行的扫描数、已调度的扫描数、等待证明或已完成。
- **启动日期** - 启动访问查看任务的日期 （时间戳）。
- **用户总数** - 要扫描的用户总数。
- **权利文件详细信息** - 表中的附加列，按状态提供权利文件总数。其中包括暂挂、已批准、已拒绝、已终止和已修正的权利文件的详细信息，以及权利文件总数。

  “已修正”列指出当前处于 REMEDIATING 状态的权利文件数。权利文件在修正后将变为 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 11-16 显示了 "Access Review Summary" 报告的示例。

图 11-16 "Access Review Summary Report" 页



Access Review Summary Test_Access_Scan

Access Scan Summary

Access Scan	Status	Launch Date	Elapsed Time	Total Users	Total Entitlements	Manual Entitlements	Auto Approved Entitlements	Auto Rejected Entitlements
Scan Zurich	scanning	Tuesday, April 10, 2007 10:40:30 AM CDT		78	0	0	0	0

Errors

Access Scan	View Error Count	Scan Errors
Scan Zurich	0	

Compliance Violations

Access Scan	New Violations	Recurring Violations	Fixed Violations	Policies Evaluated	Rules Evaluated
Scan Zurich	0	0	0	0	0

Organization | Attestors

Organization Summary (0 of 0 shown)

Organization	Total Entitlements	Pending Entitlements	Approved Entitlements	Rejected Entitlements	Terminated Entitlements

OK

单击**组织**或**证明者**表单选项卡可查看按这些对象分类的扫描信息。

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 **Save** 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文件记录中的信息，因为如果 “查看确定规则”对用户权利文件和以前的用户权利文件记录进行比较，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文件记录。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 将向证明者发送通知。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 **Attestation** 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。

查看暂挂请求

从界面的 "Work Items" 区域查看证明工作项目。选择 "Work Items" 区域中的 **Attestation** 选项卡，即可列出所有需要批准的权利文件记录。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）的权利文件记录。

对权利文件记录执行操作

证明工作项目包含需要查看的用户权利文件记录。权利文件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** - 证明从权利文件记录中所记录的日期开始，权利文件是适当的。
- **拒绝** - 权利文件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文件。
- **转发** - 允许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。

如果在指定的提升超时阶段之前，证明者未采取以上任何一种操作对请求进行响应，则通知将发送至提升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 **Compliance > Access Reviews** 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文件，方法如下：

- 将权利文件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，将对用户权利文件进行重新扫描和再次评估。

- 请求对权利文件进行重新评估 （重新扫描）。在这种情况下，将对用户权利文件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，如果权利文件仍需要证明，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 “动态权利文件”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文件，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，也可以单击 **...**（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文件的 “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 “动态权利文件” 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文件，然后单击**重新扫描**。

   将显示 “重新扫描用户权利文件” 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，也可以单击 **...**（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文件的 “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 180 页上的 “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，以使您可以评估访问查看的结果：

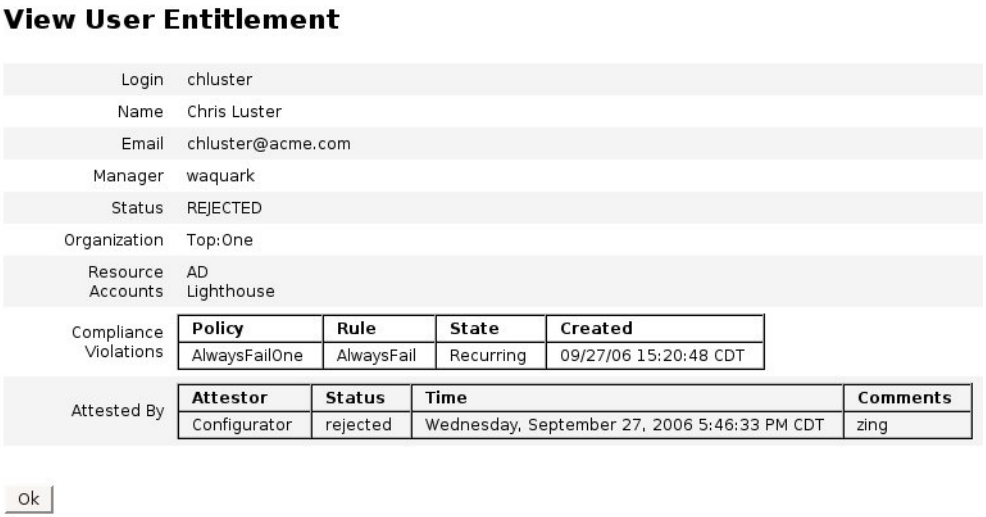
- **访问查看范围报告** - 此报告指出选定访问查看所指的用户之间的重叠部分或差异部分。由于大多数访问查看的用户范围都由查询或某项成员资格操作所指定，因此实际的用户集会随时间而变化。

  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文件之间的重叠部分和/或差异部分 （以确定范围是否随时间而变化）；用户和权利文件之间的重叠部分和/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文件）。

- **访问查看详细信息报告** - 此报告以表的形式提供了以下信息：
  - **名称** - 用户权利文件记录的名称
  - **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** - 证明权利文件记录的日期 （时间戳）
  - **组织** - 权利文件记录中的用户组织
  - **管理员** - 已扫描的用户的管理员
  - **资源** - 用户拥有其帐户且已捕获至该用户权利文件的资源
  - **违规** - 查看期间检测到的违规数

单击报告中的名称可打开用户权利文件记录。图 11-17 显示了用户权利文件记录视图中提供的信息示例。

图 11-17 用户权利文件记录



- **访问查看摘要报告** - 此报告 （已在第 362 页上的 “管理访问查看进度”中讨论，并在图 11-16 中说明）将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
  - **状态** - 启动查看的时间戳
  - **用户计数** - 查看中已扫描的用户数
  - **权利文件计数** - 所生成的权利文件记录数
  - **已批准** - 已批准的权利文件记录数
  - **已拒绝** - 已拒绝的权利文件记录数
  - **暂挂** - 仍处于暂挂状态的权利文件记录数
  - **已取消** - 已取消的权利文件记录数

这些报告均可从 "Run Reports" 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 344 页上的 “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文件时，“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。

修正者提升

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文件时，“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文件的有关信息。
- 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，将对用户权利文件进行重新扫描和再次评估。

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** - 修正者指出已经为修复问题执行了某些操作。

接着将对用户权利文件进行重新扫描和再次评估。如果用户权利文件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文件。

修正请求操作的详细信息将显示在各用户权利文件的 “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文件的 “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。

  接着将对用户权利文件进行重新扫描和再次评估。如果用户权利文件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文件。

  编辑的详细信息将在各用户权利文件的 “历史” 区域中显示为修正请求操作。

使用 “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，用户权利文件）。

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。

身份审计任务参考

表 11-3 提供了通常执行的身份审计任务的快速参考。该表显示了开始每项任务时应转到的主要 Identity Manager 界面位置，并显示执行任务时可以使用的替代位置或方法 （如果可用）。

表 11-3 身份审计任务参考

要执行的操作：	**转至：**
创建、编辑或删除审计策略	**Compliance** 选项卡， **Manage Policies** 子选项卡
为审计策略定义修正者并分配修正工作流	**Compliance** 选项卡， **Manage Policies** 子选项卡
对一个或多个用户或组织执行审计扫描	**Accounts** 选项卡，从 "User Actions" 或 "Organization Actions" 列表中选择 **Scan**
对策略违规修正请求进行响应	**Work Items** 选项卡， **Remediations** 子选项卡
缓解策略违规	**Work Items** 选项卡， **Remediations** 子选项卡
查看已修正的策略违规	**Work Items** 选项卡， **Remediations** 子选项卡
生成审计策略报告	**Reports** 选项卡， **Run Report** 子选项卡
禁用或启用审计	**Configure** 选项卡， **Audit** 子选项卡
设置要捕获的审计事件	**Configure** 选项卡， **Audit** 子选项卡
编辑管理员审计权能	**Security** 选项卡， **Capabilities** 子选项卡
设置审计通知使用的电子邮件模板	**Configure** 选项卡， **Email Templates** 子选项卡
导入数据文件/规则 （如 XML 格式的表单）	**Configure** 选项卡， **Import Exchange File** 子选项卡
定义访问查看扫描	**Compliance** 选项卡， **Manage Scans** 子选项卡
运行访问查看	**Compliance** 选项卡， **Access Reviews** 子选项卡
终止访问查看	**Compliance** 选项卡， **Access Reviews** 子选项卡
调度访问查看	**Server Tasks** 选项卡， **Manage Schedule** 子选项卡
设置周期性访问查看	**Compliance** 选项卡， **Manage Access Scans** 子选项卡
监视访问查看状态	**Compliance** 选项卡， **Access Reviews** 子选项卡
配置证明者	**Compliance** 选项卡， **Manage Access Scans** 子选项卡
执行证明者责任 （查看和证明用户权利文件）	**Work Items** 选项卡， **My Work Items** 选项卡， **Attestation** 子选项卡
查看任务划分报告	**Reports** 选项卡， **Run Report** 子选项卡

第 12 章

审计日志记录

本章介绍 Sun Java™ System Identity Manager 审计系统如何记录事件。信息通过以下方式进行组织：

概述

Identity Manager 审计的目的是记录操作人员、操作内容、操作时间以及操作的 Identity Manager 对象。

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 11 章 “身份审计”。

Identity Manager 对哪些项目进行审计？

大多数默认审计是通过内部 Identity Manager 组件执行的。但是，有些接口允许从工作流或 Java 代码中生成事件。

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，视图处理程序需要生成审计记录。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 （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。审计记录程序通过 com.waveset.session.WorkflowServices 应用程序连接工作流功能。

创建事件

虽然 Identity Manager 处理内部审计，但在某些情况下，您可能要从自定义工作流中记录审计事件。

从工作流中审计

使用 com.waveset.session.WorkflowServices 应用程序可以从任何工作流进程中生成审计事件。表 12-1 介绍可用于此应用程序的参数。

表 12-1 com.waveset.session.WorkflowServices 的参数

参数	类型	描述
op	字符串	对 WorkflowServices 执行的操作。必须设置为审计。
type	字符串	正在进行审计的对象类型名称。
action	字符串	已执行操作的名称。
状态	字符串	指定操作的状态名称。
name	字符串	受指定操作影响的对象的名称。
资源	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。
属性	映射	（*可选*）已添加或已修改的属性名称和值的映射。
参数	映射	（*可选*）最多映射五个与事件相关的附加名称或值。
组织	List	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。值将是您要在审计日志中保存的任何先前的值。

有关默认对象、操作和状态名称的列表，请参阅表 12-18。

示例

代码示例 12-1 说明了简单的工作流活动。它显示了事件的生成，该事件将记录由 ResourceAdministrator 执行的名为 ADSIResource1 的资源删除活动：

代码示例 12-1 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>
```

代码示例 12-2 显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。

代码示例 12-2 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>
```

代码示例 12-2 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'>
          <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'>
       <或者>
          <ref>ACTUAL_APPROVER</ref>
          <ref>APPROVER</ref>
      </or>
    </Argument>
    <Argument name='approver' value='$(APPROVER)'/>
</Action>
```

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标。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。

在 `sample/auditconfig.xml` 文件中定义了审计配置 (`#ID#Configuration:AuditConfiguration`) 对象。此配置对象具有一个扩展，该扩展是一个通用对象。在顶级它具有以下属性：

- filterConfiguration
- extendedTypes
- extendedActions
- extendedResults
- 发布器

filterConfiguration

`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 12-2 中列出的属性。

表 12-2 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`	List	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） - 对 objectType 命名。 • `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。

代码示例 12-3 说明了默认资源管理组。

代码示例 12-3 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 提供以下默认事件组：

- 帐户管理
- 遵从性管理
- 配置管理
- Identity Manager 登录/注销
- 密码管理
- 资源管理
- 角色管理
- 安全管理
- 任务管理
- Identity Manager 之外的更改
- Service Provider Edition

可以在 Identity Manager 管理界面 (configure/auditeventconfig.jsp) 的 "Audit Events" 页中配置每个组。此页允许您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组的 enabledEvents，但可以通过使用 Identity Manager 调试页来执行此操作。

以下各节介绍它们启用的默认事件组和事件。

帐户管理

默认情况下将启用此组。

表 12-3 默认帐户管理事件组

类型	操作
资源帐户	创建、更新、删除、启用、禁用、拒绝、批准、重命名
Identity Manager Account	创建、更新、删除、启用、禁用、重命名

遵从性管理

默认情况下将启用此组。

表 12-4 默认遵循性管理组事件

类型	操作
审计策略	所有操作
遵循性违规	所有操作
修正工作流	所有操作

配置管理

默认情况下将启用此组。

表 12-5 默认配置管理事件组

类型	操作
配置	所有操作
UserForm	所有操作
Rule	所有操作
EmailTemplate	所有操作

表 12-5 默认配置管理事件组

类型	操作
LoginConfig	所有操作
策略	所有操作
XMLDATA	导入
日志	所有操作

Identity Manager 登录/注销

默认情况下将启用此组。

表 12-6 默认 Identity Manager 登录/注销事件组

类型	操作
用户	登录、注销、证书到期
管理员	登录、注销、证书到期

密码管理

默认情况下将启用此组。

表 12-7 默认密码管理事件组和事件

类型	操作
资源帐户	更改/重置密码

资源管理

默认情况下将启用此组。

表 12-8 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
ResourceAction	所有操作

表 12-8 默认资源管理事件组和事件

类型	操作
属性解析	所有操作

角色管理

默认情况下将禁用此组。

表 12-9 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

默认情况下将启用此组。

表 12-10 默认安全管理事件组和事件

类型	操作
对象组	所有操作
AdminGroup	所有操作
管理员	所有操作
加密密钥	所有操作

任务管理

默认情况下将禁用此组。

表 12-11 任务管理事件组和事件

类型	操作
任务实例	所有操作
TaskDefinition	所有操作
TaskSchedule	所有操作
TaskResult	所有操作
置备任务	所有操作

Identity Manager 之外的更改

默认情况下将禁用此组。

表 12-12 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

Service Provider Edition

默认情况下将启用此组。

表 12-13 Service Provider Edition 事件组和事件

类型	操作
IDMXUser	创建、修改、删除、用户名恢复、质询响应、更新验证答案、操作前标注和操作后标注

extendedTypes

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 12-14 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。

表 12-14 扩展对象属性

参数	类型	描述
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 “日志数据库键”。
supportedActions	List	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	List	（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。

代码示例 12-4 说明了扩展类型的 Identity Manager 帐户。

代码示例 12-4 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

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 12-15 中列出的属性。

表 12-15 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 “日志数据库键”。

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。

代码示例 12-5 说明了如何添加退出操作。

代码示例 12-5 添加退出操作

```
<Object name='Logout'>
  <Attribute name='displayName' value='LG_LOGOUT'/>
  <Attribute name='logDbKey' value='LO'/>
</Object>
```

extendedResults

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 12-16 中描述的属性。

表 12-16 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。

所有特定于客户的键都应使用 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。

发布器

发布器列表中的每个项目均为通用对象。每个发布器都具有以下属性：

表 12-17 发布器属性

属性	类型	描述
类	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。
描述	字符串	发布器的描述。
filters	List	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	List	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

在 Identity Manager 数据库中有两个表用于存储审计数据：

- **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。

waveset.log

本节列出了 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 C “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 “日志数据库键”的部分。

- **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）。
- **actionDateTime VARCHAR(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)** - 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。
- **interface VARCHAR(50)** - 从中执行操作的 Identity Manager 界面 （如管理员、用户、 IVR 或 SOAP 界面）。
- **acctAttrChanges VARCHAR(4000)** - 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。通过对名称或值执行 "contains" SQL 语句可以查询此字段。

  代码示例 12-6 说明了 acctAttrChanges 列中的值：

代码示例 12-6 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"
```

- **acctAttr01label-acctAttr05label VARCHAR(50)** - 这五个附加 NAME 槽是最多可以提升五个属性的列，这些属性将存储在各自的列中，而不存储在大的二进制大对象中。可以使用 "audit?" 设置从 "Resource Schema Configuration" 页中提升属性，此属性可用于数据挖掘。
- **acctAttr01value-acctAttr05value VARCHAR(128)** - 五个附加 VALUE 槽，最多可以提升五个属性，这些属性将存储在单独的列中，而不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五个槽。这些是客户端 IP 和会话 ID 的示例。
- **parm01value-parm05value VARCHAR(128)** - 用于存储与事件相关的参数的五个槽。这些是客户端 IP 和会话 ID 的示例。
- **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)** - 所生成的分配给每个记录的名称。

waveset.logattr

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。

日志数据库键

对象类型、操作、操作状态和原因列都以键的形式存储在数据库中以节省空间。

对象类型、操作和结果

表 12-18 介绍以键的形式存储在数据库中的对象类型、操作和结果：

表 12-18 以键的形式存储的对象类型、操作和结果

对象类型名称	DbKey	操作名称	DbKey	结果名称	DbKey
Account	AN	批准	AP	成功	S
管理员	AD	绕过检验	BV	失败	F
AdminGroup	AG	取消协调	CR		
Attribute Definition	AF	质询响应	CD		
Application	AP	更改密码	CP		
权能	US	创建	CT		
配置	CN	连接	CO		
搜索	DS	删除	DL		
EmailTemplate	ET	取消置备	DP		
Extract	ER	禁用	DS		
ExtractTask	EX	断开	DC		
Identity Manager Account	LA	启用	EN		
IDMXUser	UX	执行	LN		
LoadConfig	LD	导出	EP		
LoadTask	LT	导入	IM		
LoginConfig	LC	List	LI		
策略	PO	加载	LD		
Provisioning Task	PT	登录	LG		
资源	RS	更新	MO		
资源帐户	RA	退出	LO		
Resource Form	RF	本机更改	NC		
资源对象	RE	操作后	PT		
RiskReportTask	RR	操作前	PE		
Role	RL	置备	PV		
Rule	RU	重置密码	RP		
用户	US	重新置备	RV		

表 12-18 以键的形式存储的对象类型、操作和结果

对象类型名称	DbKey	操作名称	DbKey	结果名称	DbKey
TaskDefinition	TD	拒绝	RJ		
TaskInstance	TI	终止	TR		
TaskSchedule	TS	用户名恢复	UR		
TaskTemplate	TT				
TaskResult	TR				
UserForm	UF				
WorkItem	WI				
XMLDATA	XD				

原因

表 12-19 介绍以键的形式存储在数据库中的原因：

表 12-19 以键的形式存储的原因

原因名称	英语文本	DbKey
策略违规	策略 {0} 违规: {1}	PV
证书无效	证书无效	CR
权限不足	权限不足	IP
数据库访问失败	数据库访问失败	DA
帐户已禁用	帐户已禁用	DI

防止审计日志篡改

可以配置 Identity Manager 以防止以下形式的审计日志被篡改：

- 添加或插入审计日志记录
- 修改现有审计日志记录
- 删除审计日志记录或整个审计日志
- 截断审计日志

所有 Identity Manager 审计日志记录都具有唯一的、基于服务器的序列号以及记录和序列号的加密散列。创建篡改检测报告时，其将扫描每个服务器的审计日志以查看是否：

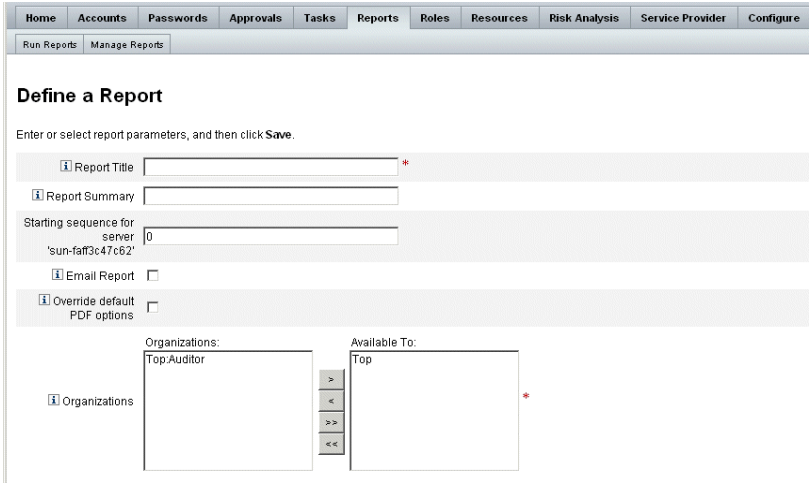
- 序列号中存在间隔 （表示已删除的记录）
- 散列不匹配 （表示已修改的记录）
- 存在重复的序列号 （表示已复制的记录）
- 上一个序列号小于预期的序列号 （表示已截断的日志）

配置防篡改日志记录

要配置防篡改日志记录，请执行以下步骤：

1. 通过选择 **Reports > New > Audit Log Tampering Report** 创建篡改报告。
2. "Define a Tampering Report" 页显示时（请参见图 12-1），请为报告输入一个标题，然后 **Save** 它。

图 12-1 配置审计日志篡改报告



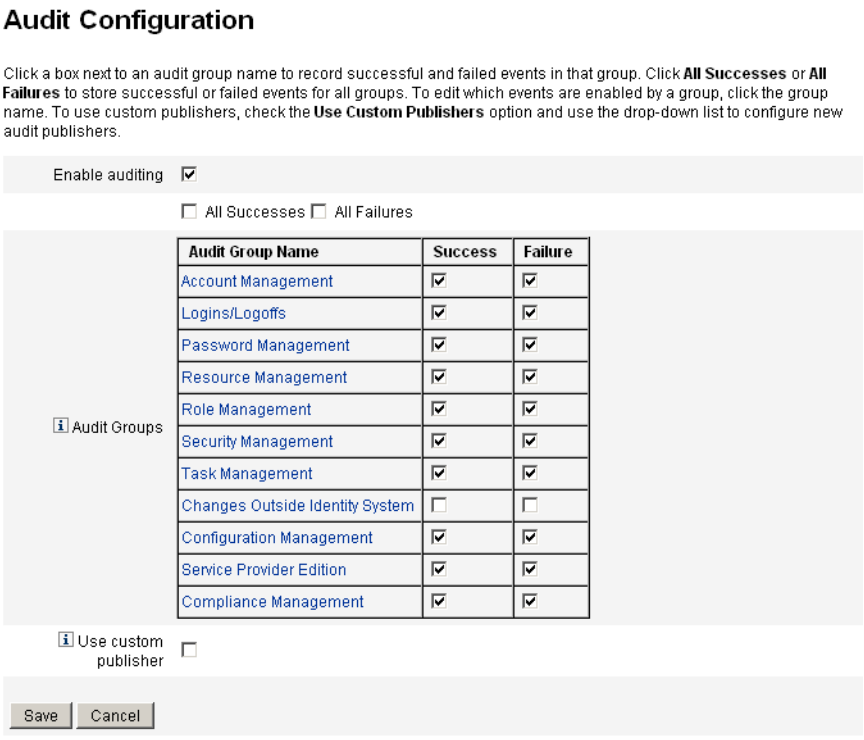
还可以指定以下可选参数：

- **报告摘要** - 输入报告的描述性摘要。
- **服务器 '<*server_name*>' 的起始序列** - 输入服务器的启动序列号。

- 此选项使您可以无需将旧日志条目标记为篡改即可将其删除，并且可以出于性能原因限制报告的范围。
- **电子邮件报告** - 启用此选项可以通过电子邮件将报告结果发送到指定的电子邮件地址。
- 选择此选项时，页面将刷新并提示输入电子邮件地址。但是，请谨记，通过电子邮件传送文本内容是不安全的，敏感信息（如帐户 ID 或帐户历史记录）可能会泄漏。
- **覆盖默认 PDF 选项** - 选择此选项可以覆盖此报告的默认 PDF 选项。
- **组织** - 选择对此报告应具有访问权限的组织。

3. 然后，选择 **Configure > Audit** 打开 "Audit Configuration" 页 （如图 12-2 所示）。

图 12-2 防篡改审计日志记录配置



4. 选择 **Use Custom Publisher**，然后单击 "Repository publisher" 链接。
5. 选择 **Enable tamper-resistant audit logs**，然后单击 **OK**。
6. 单击 **Save** 以保存设置。

   可以再次关闭此选项，但未签名的条目将在审计日志篡改报告中进行标记，您必须重新配置报告才能忽略这些条目。

使用自定义发布器

Identity Manager 可以将审计事件提交给自定义审计发布器。可使用以下自定义发布器：

- 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。
- 脚本 - 允许使用自定义脚本存储审计事件。

可以在参考工具包中找到这些发布器的源代码。也可以在参考工具包中找到 Javadoc 格式的接口文档。

开发发布器

所有发布器都可以实现 AuditLogPublisher 接口。（有关接口的详细信息，请参阅 Javadoc）。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。（请参见参考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。

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 `configure(`*Map*`)` 仅调用一次。（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。

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

参考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 Java System Application Server 使用此格式。

格式化程序必须实现 AuditRecordFormatter 接口。此外，发布器必须具有一个无参数的构造函数。有关详细信息，请参阅引用工具包中的 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 13 章

服务提供者管理

本章介绍了在 Sun Java™ System Identity Manager 中管理服务提供者 (SPE) 功能所需要了解的信息。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。有关服务提供者实现的更深入介绍，请参见 “*Identity Manager SPE 部署*”。

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，您需要可以管理所有最终用户 （外联网用户和内联网用户）的用户置备。使用 Identity Manager Service Provider Edition 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 "Service Provider User" 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 **SPE System Account Policy** （已添加到主 "Policies" 表）为服务提供者用户激活策略检查代码。

Identity Manager 与服务提供者同步

可以将 Identity Manager 与服务提供者帐户同步配置为在任何 Identity Manager 服务器上运行或限制在选定的服务器上运行。

如同 Identity Manager 同步一样，通过 "Resources" 页上的 "Resource Actions" 选项可以轻松地停止和启动服务提供者同步。请参见第 431 页上的“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 427 页上的 “最终用户界面”。

Access Manager 集成

您可以使用 Sun Java System 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。

服务提供者需要用户名以进行审计。更新 `AMAgent.properties` 文件可以将用户的 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。默认情况下已导入名为 SPE 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。
  - 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。
- 如果需要，可配置服务提供者帐户策略。

编辑主配置

要编辑服务提供者实现的配置对象，请执行以下步骤：

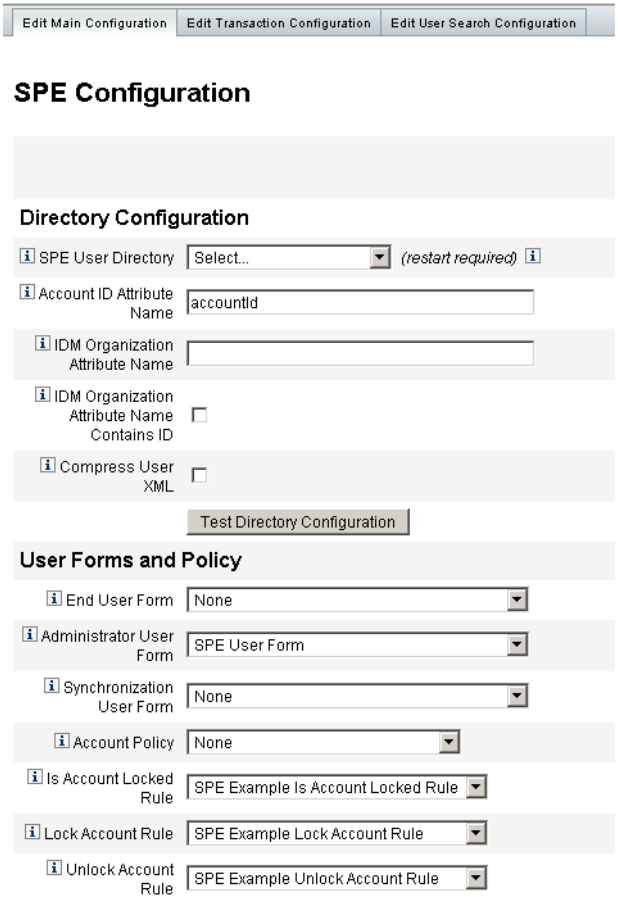
1. 以配置者权限登录到 Identity Manager。
2. 在菜单栏中单击 **Service Provider**。
3. 单击 **Edit Main Configuration**。屏幕上将显示 **SPE Configuration** 页。在 "SPE Configuration" 页中的以下段中，根据需要输入信息或进行选择：
   - 目录配置
   - 用户表单和策略
   - 事务数据库
   - 跟踪的事件配置
   - 同步帐户索引
   - 标注配置

目录配置

在 “目录配置” 小节中，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 13-1 显示了 "SPE Configuration" 页的这一区域，以及下一节中介绍的 "User Forms and Policy" 区域。

图 13-1 服务提供者 (SPE) 配置 （目录、用户表单和策略）



1. 从列表中选择 **SPE End-User Directory**。

   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 **Account ID Attribute Name**。

   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 Organization Attribute Name**。

   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，则应指定 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 Organization Attribute Name Contains 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 **Compress User 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 **Test Directory Configuration** 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 13-1 所示）中，请指定要用于服务提供者用户管理的表单和策略。

1. 从列表中选择 **End User Form**。

   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 **None**，则不使用默认用户表单。

2. 从列表中选择 **Administrator User Form**。

   这是用于管理员上下文中的默认用户表单。该表单包括服务提供者帐户编辑页。如果选择 **None**，则不使用默认用户表单。

注 如果不选择 "Administrator User Form"，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 **Synchronization User Form**。

   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 **Account Policy**。

   这些选项包括通过 "Configure" > "Policies" 定义的任何身份帐户策略。

5. 从列表中选择 **Is Account Locked Rule**。

   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 **Lock Account Rule**。

   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。

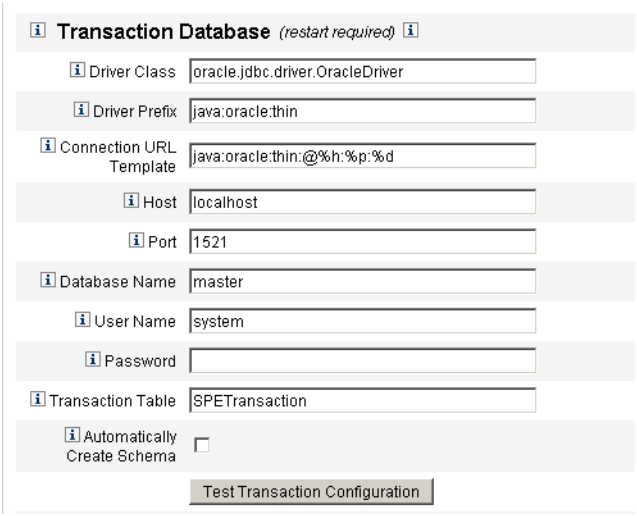
7. 选择 **Unlock Account Rule**。

   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 “SPE 配置” 页的此部分（如图 13-2 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。

图 13-2 服务提供者配置 （事务数据库）



1. 输入以下数据库信息：
   - **Driver Class** - 指定 JDBC 驱动程序类名。
   - **Driver Prefix** - 此字段是可选的。如果已指定，将在注册新驱动程序前查询 JDBC DriverManager。
   - **Connection URL Template** - 此字段是可选的。如果已指定，将在注册新驱动程序前查询 JDBC DriverManager。
   - **Host** - 输入正在运行该数据库的主机的名称。
   - **Port** - 输入数据库服务器侦听的端口号。
   - **Database Name** - 输入要使用的数据库的名称。
   - **User Name** - 输入有权读取、更新和删除选定数据库中事务和审计表中各行的数据库用户的 ID。
   - **Password** - 输入数据库用户密码。
   - **Transaction Table** - 输入选定数据库中用于存储暂挂事务的表名称。
2. 启用 **Automatically Create Schema** 选项，可以使 Identity Manager 自动创建表的模式。

   生产系统应禁用该选项。对于生产系统，请自定义 `web/samples` 中的样例数据库初始化脚本。

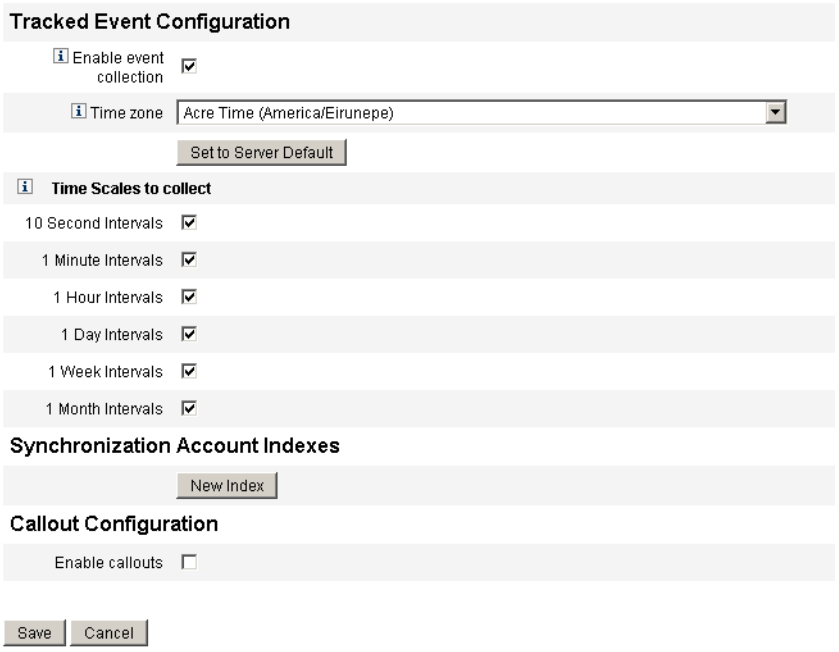
3. 如果适用，单击 **Test Transaction Configuration** 以验证您的条目。

继续到 "Service Provider Configuration" 页的下一段以配置跟踪的事件。

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 13-3 所示。清除 **Enable event collection** 复选框将禁用收集。

图 13-3 服务提供者配置 （跟踪的事件、帐户索引和标注配置）



要设置时区并指定服务提供者跟踪事件的收集间隔，请执行以下步骤：

1. 从列表中选择 **Time zone**。

   选择记录跟踪事件时要使用的时区，或选择 **Set to Server Default** 以使用服务器上设置的时区。

2. 选择 **Time Scales to collect** 选项。

   按以下时间间隔聚集的收集：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使用 ActiveSync 资源时，可能需要定义 **Account Indexes** 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，从 ActiveDirectory 中删除事件仅包含 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唯一标识符。
- **身份** - 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 ActiveSync 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。

定义了服务提供者资源中的所有索引属性后：

1. 在配置页的 "Synchronization Account Indexes" 区域中，单击 **New Index** 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 **Resource**。

   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 Attribute** 或 **Full Identity Attribute** 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 **New Index** 以定义其他资源的索引属性。

5. 要删除索引，请单击 **Resource** 选项字段右侧的 **Delete** 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"。

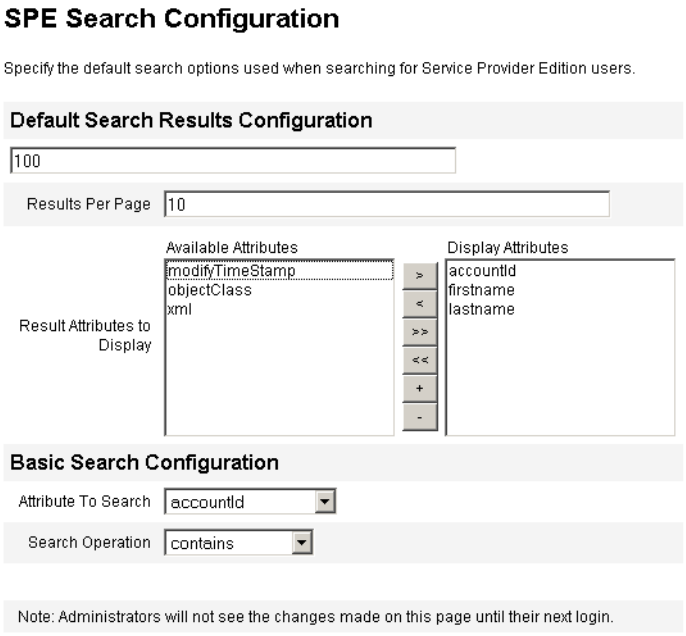
如果指定操作后标注，请使用 **Wait for post-operation callout** 选项指定事务必须等待操作后标注处理完成后才能完成。这可确保任何相关事务都只能在操作后标注成功完成后执行。

注 在 "SPE Configuration" 页上所有段的选择完成后，单击 **Save** 完成配置。

编辑用户搜索配置

使用此页（如图 13-4 所示）可以为委托管理员在“管理服务提供者用户”页上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 13-4 搜索配置



要配置默认搜索设置以搜索服务提供者用户，请执行以下步骤：

1. 在菜单栏中单击 **Service Provider**。
2. 单击 **Edit User Search Configuration**。
3. 输入 **Maximum Results Returned** 的数值 （默认值为 100）。
4. 输入 **Results Per Page** 的数值 （默认值为 10）。
5. 使用箭头键选择 **Result Attributes to Display** 旁的 **Available Attributes**。
6. 从列表中选择 **Attribute to search**。
7. 从列表中选择 **Search Operation**。
8. 单击 **Save**。

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 SPE 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者事务的步骤：

- 设置默认事务执行选项
- 设置事务持久性存储
- 设置高级事务处理设置
- 监视事务

设置默认事务执行选项

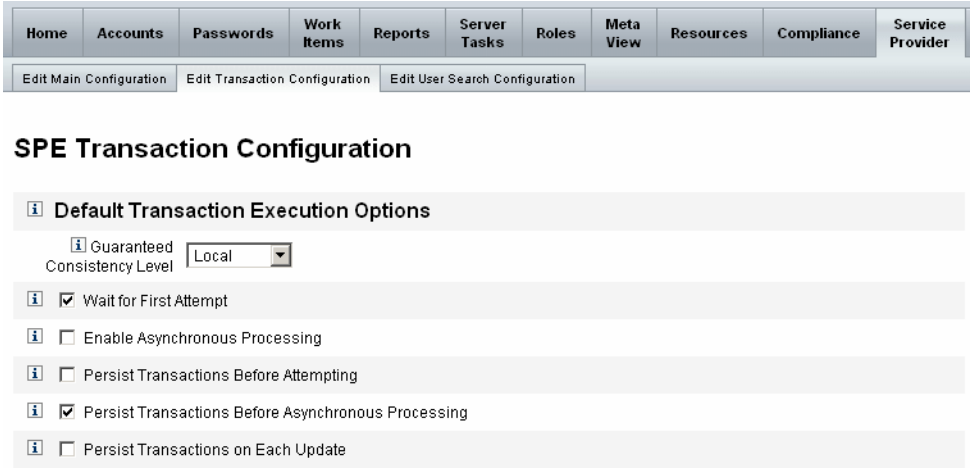
这些选项控制事务的执行方式，包括同步/异步处理及何时在事务持久性存储中对其进行持久性处理。可以在 IDMXUser 视图中或通过用于对其进行处理的表单覆盖这些选项。有关更多信息，请参见 “*Identity Manager SPE 部署*”。

要配置服务提供者事务，请执行以下步骤：

1. 单击 **Service Provider > Edit Transaction Configuration**。屏幕上将显示 **SPE Transaction Configuration** 页。

   图 13-5 显示了 "Default Transaction Execution Options" 区域。

图 13-5 事务配置



2. 从以下选项中选择 **Guaranteed Consistency Level**，以指定用户更新的事务一致性级别：

   - **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。
   - **完成** - 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. 选择以下您选择启用的默认事务执行选项：

   - **等待第一次尝试** - 规定当 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。

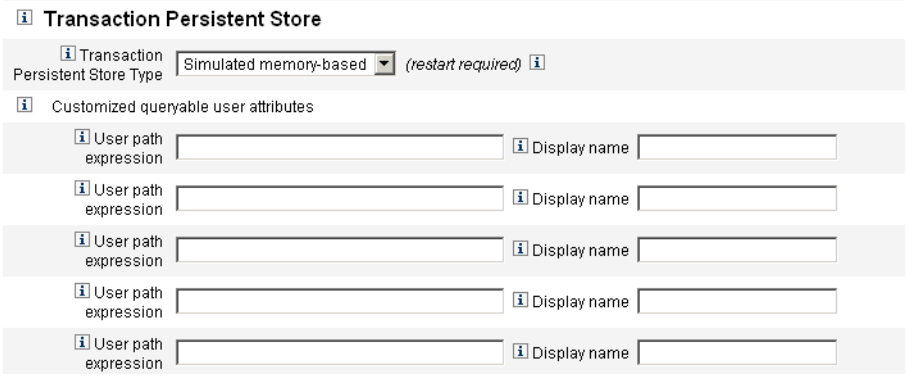
     启用异步处理将允许系统重试事务。也可以允许设置高级事务处理设置中配置的工作线程异步运行，以提高吞吐量。如果选择此选项，则应该为要通过同步输入表单置备到或更新的资源配置重试时间间隔和尝试次数。

     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，包括服务提供者用户 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导致不必要的系统开销。考虑禁用该选项，除非 **Wait for First Attempt** 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 **Search Transaction** 页进行搜索并且总是最新的，因此该操作可以帮助隔离问题。

设置事务持久性存储

"SPE Transaction Configuration" 页上的这些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，如下图所示。

图 13-6 配置 SPE 事务持久性存储



要设置这些选项，请执行以下步骤：

1. 从列表中选择所需的**事务持久性存储类型**。

   如果选择了 **Database** 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**基于模拟的内存**选项，则需要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 **Database** 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 **Transaction Persistent Store Type** 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 **Customized queryable user attributes**。

   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。它们包括：

   - **用户路径表达式** - 将路径表达式输入到 IDMXUser 对象中。

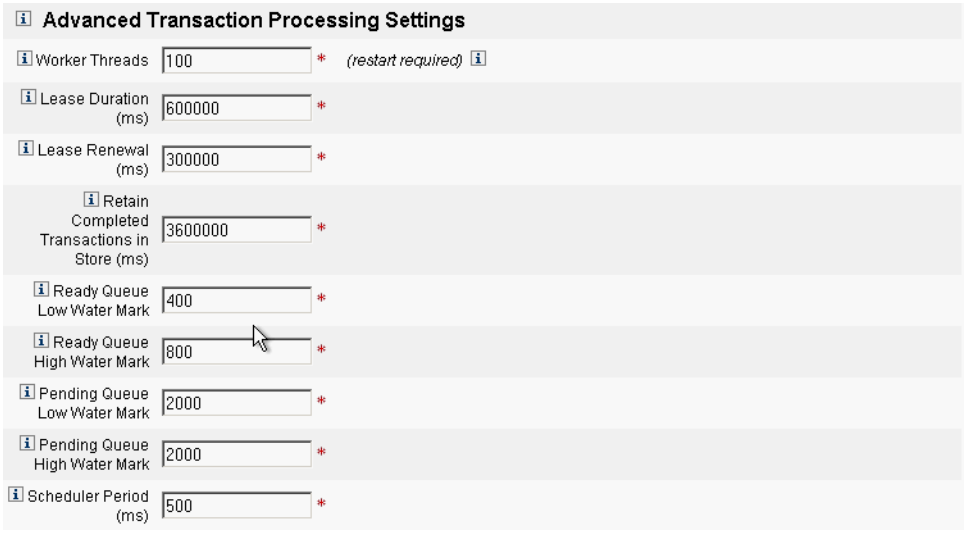
- **显示名称** - 选择与路径表达式对应的显示名称。该显示名称显示在事务搜索页中。

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 13-5 说明了 "Edit Transaction Configuration" 页上的 "Advanced Transaction Processing Settings" 区域。

图 13-7 高级事务处理设置



1. 请输入所需的 **Worker Threads （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 **Worker Threads** 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 **Lease Duration (ms)** （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. 输入所需的 **Lease Renewal (ms)** 时间 （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. 输入所需的 **Retain Completed Transactions in Store (ms)**（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. 输入所需的 **Ready Queue Low Water Mark** （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. 输入所需的 **Ready Queue High Water Mark** （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. 输入所需的 **Pending Queue Low Water Mark** （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. 输入所需的 **Pending Queue High Water Mark** （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. 输入所需的**调度程序周期 (ms)**（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 **Save** 接受设置。

监视事务

服务提供者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。

要搜索事务：

1. 登录到 Identity Manager。
2. 在菜单栏中单击 **Server Tasks**。
3. 单击 **Service Provider Transactions**。

   屏幕上将显示 **SPE Transaction Search 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 **Accounts > Find Users** 页。

4. 如果需要，请选择 **User Name**。

   这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 Transaction Configuration" 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。

5. 如果需要，请选择针对 **Type** 搜索。

   这允许您搜索选定类型的事务。

6. 如果需要，请选择针对 **State** 搜索。

   这允许您搜索处于以下选定状态的事务：

   - **Unattempted** 表示尚未尝试的事务。
   - **Pending retry** 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。
   - **Success** 表示已经成功完成的事务。
   - **Failure** 表示已经完成但具有一个或多个故障的事务。

7. 如果需要，请选择针对 **Attempts** 搜索。

   这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。

8. 如果需要，请选择针对 **Submitted** 搜索。

   这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。

9. 如果需要，请选择针对 **Completed** 搜索。

   这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。

10. 如果需要，请选择针对 **Cancelled Status** 搜索。

    这允许您根据事务是否已取消搜索这些事务。

11. 如果需要，请选择针对 **Transaction ID** 搜索。

    这允许您根据事务唯一的 ID 搜索这些事务。使用该选项可以根据您输入的出现在所有审计日志记录中的 ID 值查找事务。

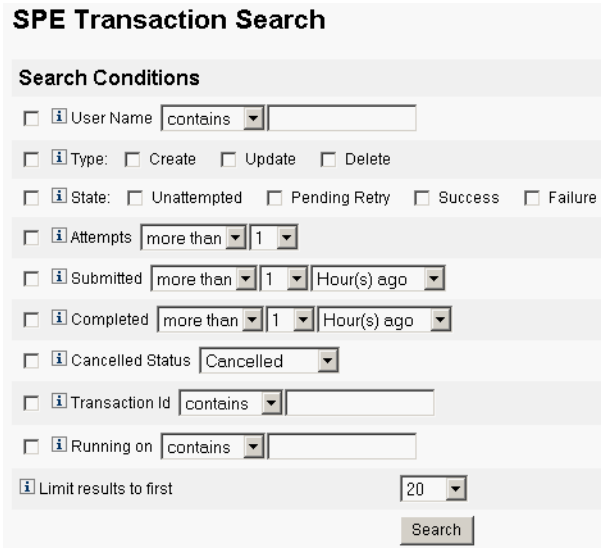
12. 如果需要，请选择针对 **Running On** （哪一台服务器）搜索。

    这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。

13. 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 13-8 搜索事务



14. 单击 **Search**。

    将显示搜索结果。

15. 如果需要，请单击结果页面底部的 **Download All Matched Transactions**。这将把结果保存为 XML 格式的文件。

注 您可以取消搜索结果中返回的事务。选择结果表中的事务，然后单击 **Cancel Selected**。您无法取消已完成或已被取消的事务。

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 Organization Attribute Name Contains 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。
- 服务提供者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。这需要 Service Provider Edition 管理员在 `Top` 中具有服务提供者用户权能来管理这些用户。
- 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。具有特定于 Service Provider Edition 任务的权能，可以将其分配给用户 （在 **Edit User** 页的 **Security** 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 委托管理的更多信息，请参见第 5 章“管理”中的“委托管理”。

通过管理员角色分配委托

要授予对服务提供者用户的细化权能和控制范围，请使用服务提供者用户管理员角色。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 系统配置中将其启用。

如果启用通过管理员角色分配进行委托，则 "SPE Configuration" 中的 "IDM Organization Attribute Name" 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 （SPE 委托管理），请使用 Identity Manager 调试页将系统配置对象中的以下属性设置为 `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 SPE 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 （设置为 false）了 SPE 委托管理，则会使用基于组织的授权模型。

启用 SPE 委托管理后，跟踪的事件会捕获有关执行的授权规则数和持续时间的信息。这些统计信息可以在面板中找到

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，请执行以下步骤创建管理员角色并指定控制范围、权能和应将其分配给的用户：

注 在创建服务提供者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。您必须指定规则的 `authType` 才能使用这些规则，即 SPEUsersSearchContextRule、 SPEUsersSearchFilterRule、SPEUsersAfterSearchFilterRule、 CapabilitiesOnSPEUserRule、UserIsAssignedAdminRoleRule、SPEUserIsAssignedAdminRoleRule。

Identity Manager 提供了样例规则，您可以使用这些样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更多信息，请参见 *“Identity Manager SPE 部署”*。

1. 在 "Security" 选项卡上，选择 "Admin Roles"，然后单击 **New** 打开 "Create Admin Role" 页。
2. 指定管理员角色的名称，并选择 **Service Provider Users** 类型。
3. 请按以下各节所述指定 "Scope of Control"、"Capabilities" 和 "Assign To Service Provider Users" 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可以查看的服务提供者用户。如果请求在目录中列出服务提供者用户，则会强制指定控制范围。

您可以为服务提供者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 "None"，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，并可评估结果以确定允许请求用户可访问的识别名 (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

服务提供者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者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者用户，则会强制指定权能。

在 "Capabilities" 选项卡上，选择要为该管理员角色应用的 "Capabilities Per User Rule"。

将管理员角色分配给服务提供者用户

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，可以将服务提供者用户管理员角色动态地分配给服务提供者用户。

单击 "Assign To Service Provider Users" 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，方法是将以下系统配置对象设置为 `true`：

`security.authz.checkDynamicallyAssignedAdminRolesAtLoginTo.`*`logininterface`*

所有界面的默认值为 `false`。

委托服务提供者用户管理员角色

默认情况下，服务提供者用户可以将分配给他们的服务提供者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者用户。

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。

服务提供者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。

管理服务提供者用户

本节包含通过 Identity Manager 管理服务提供商用户的步骤和信息。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。这是由服务提供者主配置（请参见初始配置）中的 Identity Manager **Organization Attribute Name** 字段指定的。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 **Organization Attribute Name**，则 "Create User" 或 "Edit User" 页上将显示可用组织的多选项列表。默认情况下显示组织的简称。您可以修改 SPE 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。

可从主 "Policies" 表中获取 **SPE System Account Policy**。

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账户。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样例。自定义该表单以满足您在服务提供者环境中管理用户的需求。有关更多信息，请参见 “*Identity Manager 工作流、表单和视图*”。

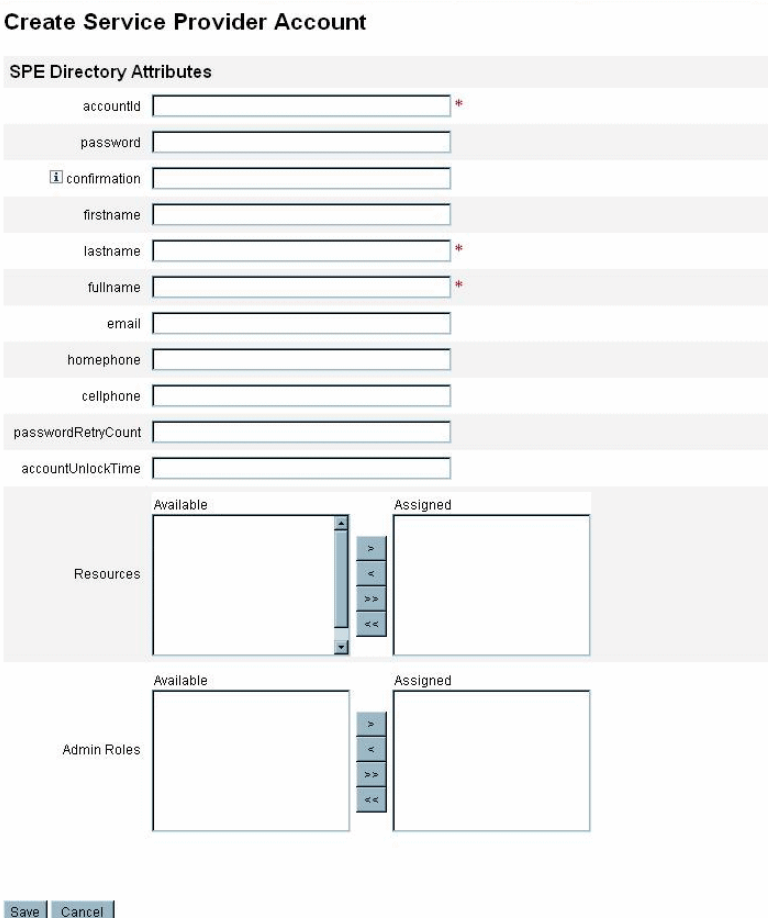
要创建服务提供者帐户：

1. 在菜单栏中单击 **Accounts**。
2. 单击 **Manage Service Provider Users** 选项卡。
3. 单击 **Create Account**。

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 "Account Attributes" 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. 根据需要输入以下值：
   - **accountid** （此字段为必填字段）
   - **password**
   - **confirmation** （这是密码确认）
   - **firstname** （此字段为必填字段）
   - **lastname** （此字段为必填字段）
   - **fullname**
   - **email**
   - **home phone**
   - **cell phone**
   - **password retry count**
   - **account unlock time**
5. 使用箭头键从 "Available" 列表中分配所有所需的 "Resources"。
6. **Account Status** 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 13-9 创建服务提供者用户和帐户



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，可自定义提供的服务提供者用户表单样例。

7. 单击 **Save** 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 **Accounts** 区域中，单击 **Manage Service Provider Users**，然后输入搜索值并单击 **Search**。

以下主题介绍了服务提供者搜索功能：

- 高级搜索
- 搜索结果
- 删除、取消分配帐户或解除帐户的链接
- 设置搜索选项

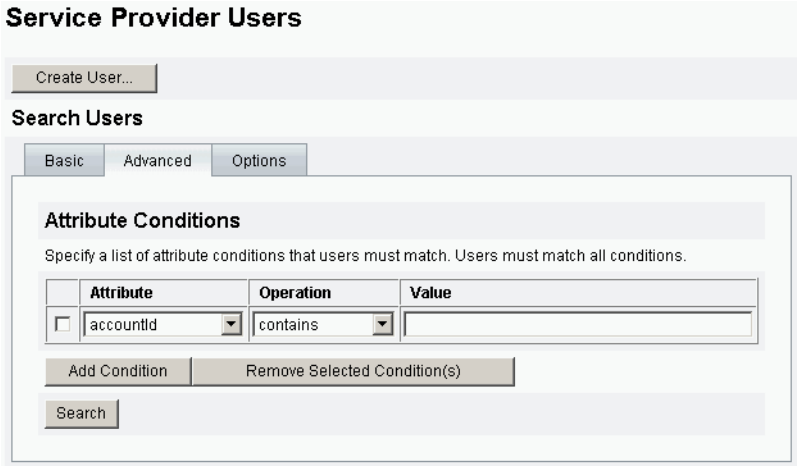
高级搜索

要执行服务提供者用户的高级搜索，请从 "Service Provider Users Search" 页中单击 **Advanced**，然后完成以下操作：

1. 从列表中选择所需的 **Attribute**。
2. 从列表中选择所需的 **Operation**。

   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。
3. 输入所需的搜索值，然后单击 **Search**。

图 13-10 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**。

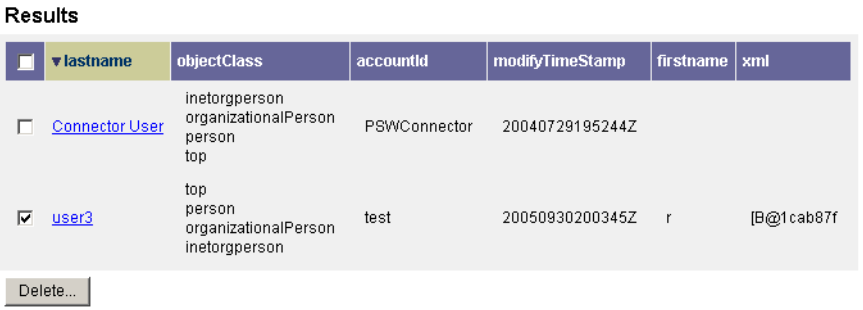
搜索结果

服务提供者搜索结果将显示在表中，如图 13-11 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 13-11 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 **Delete** 按钮。该操作将打开删除用户页，并显示其他选项（请参见“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。服务提供者的帐户链接功能允许您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、链接确定规则和链接验证选项。

要链接用户帐户，请使用以下过程：

1. 在菜单栏中单击**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**需要进行链接验证**，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

要删除、取消分配用户帐户或解除用户帐户的链接，请执行以下步骤：

1. 在菜单栏中单击 **Accounts**。
2. 单击 **Manage Service Provider Users**。
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 **Delete** 按钮。
6. 如果需要，请选择其中一个全局选项：

- **Delete All resource accounts**

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链接。

- **Unassign All resource accounts**

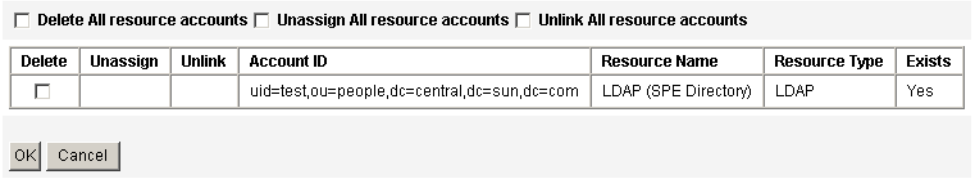
注 取消分配资源将删除该资源分配。取消分配会将资源帐户取消链接。取消分配资源时，将不删除该资源帐户。

- **解除所有资源帐户的链接**

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**取消链接**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 **OK**。

图 13-12 删除、取消分配帐户或解除帐户的链接



设置搜索选项

执行以下步骤来设置服务提供者用户的搜索选项：

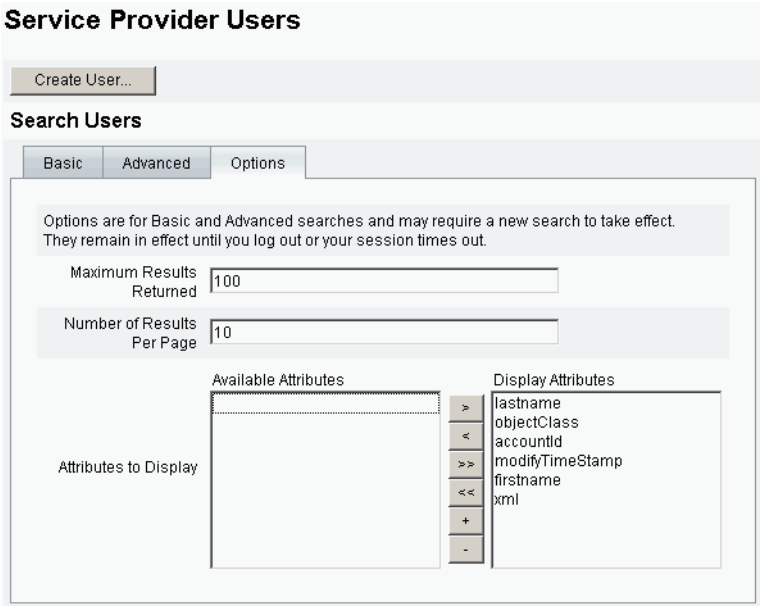
1. 在菜单栏中单击 **Accounts**。
2. 单击 **Service Provider**。

3. 单击 **Options**。

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 **Maximum Results Returned**。
5. 输入 **Number of Results Per Page**。
6. 使用箭头键从 **Available Attributes** 中选择所需的 **Display Attribute**。

图 13-13 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 “*Identity Manager SPE 部署*”。

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。这将允许与访问管理系统（如 Sun Java System Access Manager）集成。

样例

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），包括通过质询问题进行验证
- 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地自定义这些页面。可以自定义以下内容：

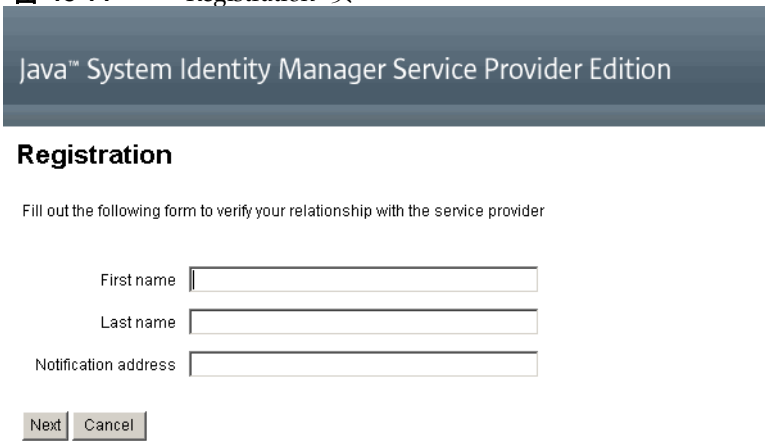
- 品牌化
- 配置选项 （例如失败的登录尝试次数）
- 添加/删除页面

有关自定义页面的更多信息，请参见 “*Identity Manager SPE 部署*”。

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。

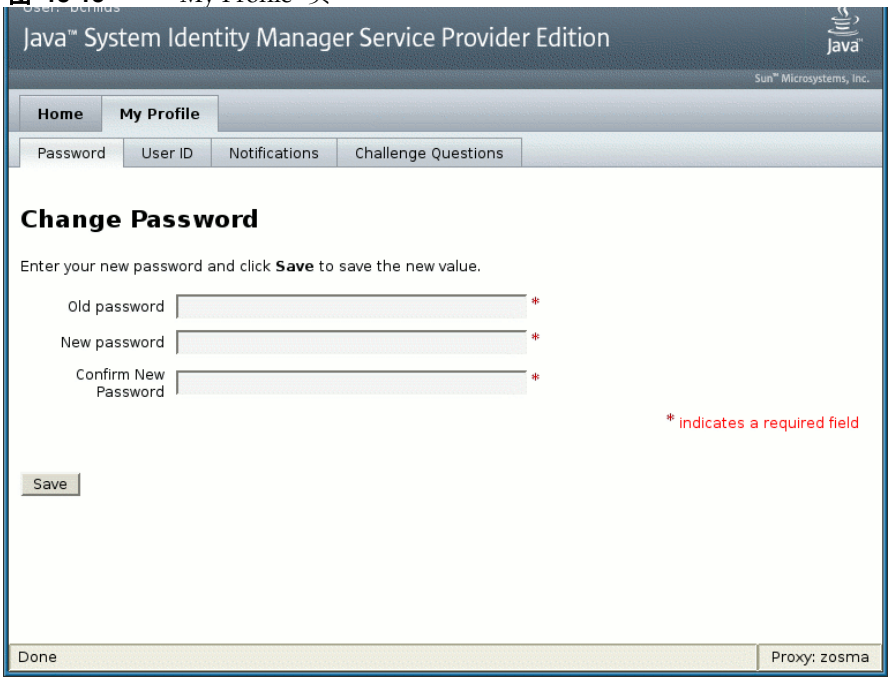
图 13-14 "Registration" 页



"Home" 屏幕和配置文件屏幕

图 13-15 显示了最终用户 "Home" 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 13-15 "My Profile" 页



同步

通过同步策略可启用服务提供者用户的同步。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者实现中启用同步：

- 配置同步
- 监视同步
- 启动和停止同步
- 迁移用户

注 从 Identity Manager 的 **Resources** 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 196 页上的 “配置同步”中的说明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者用户的同步进程。

- 选择 **Service Provider Edition User** 作为目标对象类型。
- 在 "Scheduling Settings" 段中，选择 **Enable Synchronization**。

按照第 196 页上的 “配置同步”中的说明，指定适合您的环境的其他选项。

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（有关更多信息，请参见 “*Identity Manager SPE 部署*”）。

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 **Save** 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 "Synchronization Resource Action" 下选择 **Start for Service Provider**时，将启动同步。

监视同步

Identity Manager 提供以下监视服务提供者同步的方法。

- 在 "Resource" 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，为服务提供者实现配置 Identity Manager 时，启用服务提供者同步。要禁用服务提供者活动同步，请执行以下步骤：

1. 在 **Resources** 区域中，选择资源然后单击 **Edit Synchronization Policy** 以编辑策略。
2. 清除 **Enable Synchronization** 复选框。

3. 单击 **Save**。

   保存策略后，同步将停止。

要停止同步而不将其禁用，请从 "Synchronization Resource Action" 中选择 **Stop for Service Provider**。

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。该任务可将现有的 Identity Manager 用户迁移到服务提供者用户目录。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。

要迁移现有 Identity Manager 用户：

1. 请在菜单栏中单击 **Tasks**。
2. 单击 **Run Tasks**
3. 单击 **SPE Migration**。
4. 输入唯一的 **Task Name**。
5. 从列表中选择 **Resource**。

   这是 Identity Manager 中表示服务提供者目录服务器的资源。不会迁移在 Identity Manager 用户中找到的该资源的链接。
6. 输入 **Identity Attribute**。

   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 **Identity Rule**。

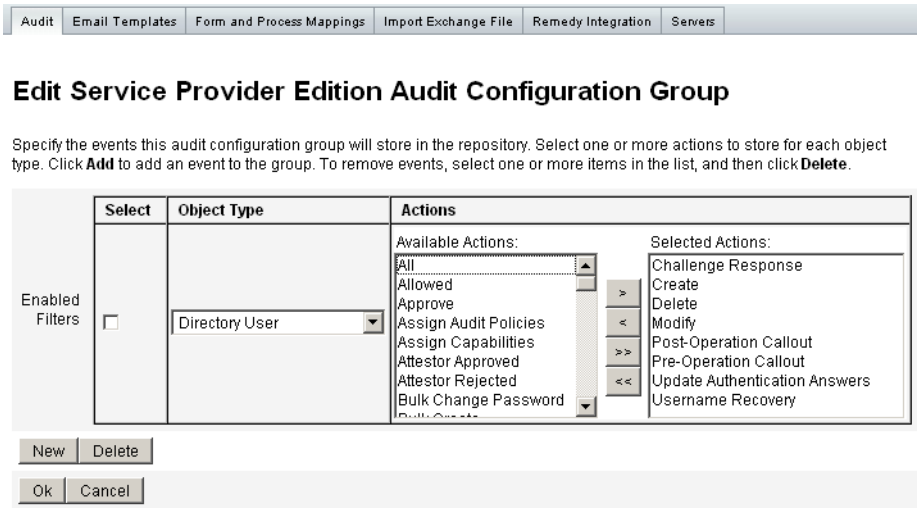
   这是可以通过 Identity Manager 用户的属性计算目录用户名称的可选规则。身份规则可以计算简单名称 （通常为 uid），然后会通过资源的身份模板处理该简短名称，以形成目录服务器的识别名 (DN)。该规则还可以返回不使用 ID 模板的完全指定的 DN。
8. 单击 **Launch** 可启动后台迁移任务。

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 Service Provider Edition 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 13-16。

有关审计日志记录和修改 Service Provider Edition 审计配置组中事件的更多信息，请参见第 12 章 “审计日志记录”

图 13-16 编辑 Service Provider Edition Audit Configuration Group 页



lh 参考消息

用法

使用以下语法可以调用 Identity Manager 命令行界面并执行 Identity Manager 命令：

```
lh { $class | $command } [ $arg [$arg... ] ]
```

用法说明

要显示命令用法帮助，请键入 lh （不要提供任何参数）。

设置路径环境变量：

- 使用 lh 命令时，应将 JAVA_HOME 设置为 JRE 目录，该目录包含带 Java 可执行文件的 bin 目录。此位置因安装而异。

  如果您有 Sun 的标准 JRE （不含 JDK），通常的目录位置为 C:\Program Files\Java\j2re1.4.1_01。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\j2re1.4.1_01。

  完整的 JDK 安装含有多个 Java 可执行文件。此时，将 JAVA_HOME 设置为包含正确 bin/java.exe 文件的嵌入式 jre 目录。对于典型安装，将 JAVA_HOME 设置为 D:\java\jdk1.3.1_02.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，将变量设置为默认安装目录：

  set WSHOME=C:\Program Files\tomcat\webapps\idm

注 请确保 WSHOME 变量的值不包含以下内容：

- 引号 (" ")
- 路径末尾处的反斜杠 (\)

不要使用引号，即使应用程序部署目录的路径中包含空格。

在 UNIX 系统上，您也必须导出路径变量，如下所示：

```
export WSHOME
export JAVA_HOME
```

类

必须是全限定类名，如 `com.waveset.session.WavesetConsole`。

命令

必须是以下命令之一：

- `config` - 启动业务进程编辑器。
- `console` - 启动 Identity Manager 控制台。
- `export` - 导出交换文件。
- `js` - 调用 JavaScript 程序。
- `javascript` - 与 js 相同。
- `import` - 导入 Identity Manager 对象。
- `license [options] {status | set {parameters }}` - 设置 Identity Manager 许可证密钥。
- `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。
- `syslog [options]` - 从系统日志中提取记录。

- `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）。

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`

导出命令

使用情况

`export [-v] Outfile [ typeSet | typeName... ]`

选项

- `-v` - 启用详细模式。
- `typeName` 选项：`all`、`default` 或 `users`。`all` 选项可以导出所有对象类型，以下类型除外：
  - 日志
  - Syslog
  - TestItem
  - 服务器
  - 管理员

一般来说，将日志文件从一个环境导出到另一个环境并非常见做法。

license 命令

使用情况

```
license [选项] { status | set {参数} }
```

选项

- `-U` *username*（如果配置器帐户已重命名）
- `-P` *PathtoPassword*`.txt`（如果配置器密码已更改）

`set` 选项的参数必须以 `-f` *File* 形式表示。

示例

- `lh license status`
- `lh license set -f` *File*

syslog 命令

使用情况

```
syslog [选项]
```

选项

- `-d` *Number* - 显示前 *Number* 天的记录（默认值=1）
- `-F` - 仅显示致命严重级别的记录

- -E - 仅显示错误严重级别或更高级别的记录
- -W - 仅显示警告严重级别或更高级别的记录 （默认）
- -X - 包括报告的错误原因 （如果可用）

联机文档资料的高级搜索

在搜索 Identity Manager 联机文档资料时，可以使用高级语法创建复杂的查询。其中包括：

- 通配字符 - 允许指定拼写模式而不是完整字词。
- 查询运算符 - 指定要组合或修改查询元素的方式。

注 在同一搜索中，可以同时使用通配字符和查询运算符。

通配字符

*通配符*是在搜索中代表其他字符或成组字符的特殊字符。

Identity Manager 联机文档资料搜索功能支持以下通配字符

表 B-1 支持的通配字符

通配字符	用途
问号 (?)	匹配任意一个字符。 例如，搜索 t?p 将匹配诸如 tap、tip 和 top 等字词。搜索 ball???? 将匹配诸如 ballpark、 ballroom 和 ballyhoo 等字词，但不会查找 ballet 或 balloon，因为这些词在 "ball" 之后不是正好包含四个字母。
星号 (*)	匹配任意一组字符。 例如，搜索 comp* 会查找以字母 comp 开头的任意匹配项，如 computer、company 或 comptroller。

查询运算符

*查询运算符*允许您组合、修改或排除搜索元素。可以以大写、小写或大小写混合的方式键入查询运算符。通常，查询运算符以尖括号开头和结尾，例如 <CONTAINS>。

注 基本布尔运算符（AND、OR 和 NOT）和特殊字符运算符（例如 <、= 和 !=）不要求使用尖括号。

优先级规则

当在查询中使用一种以上运算符时，优先级规则和括号将决定运算符范围。AND 运算符的优先级高于 OR 运算符。例如，以下查询：

```
resource AND adapter OR attribute
```

等同于：

```
(resource AND adapter) OR attribute
```

如果希望搜索功能解释为要与 "resource" 一起查找 "adapter" 和 "attribute" 中的任意一个词，则必须使用括号，如下所示：

```
resource AND (adapter OR attribute)
```

默认运算符

如果键入一连串查询字词或元素而没有指定运算符，则会使用标准的默认运算符 <AND> 来组合查询元素。

如果查询由单个词组成而没有明确的一元字词运算符（例如 <EXACT>、<MORPH> 或 <EXPAND>），则认为这些词受默认字词运算符 <MORPH> 控制。

下表列出了联机文档资料搜索功能的常用查询运算符。

表 B-2 用于联机文档资料搜索的常用查询运算符

运算符	描述	示例
<AND> 或 AND	为搜索添加强制性条件。	搜索 "apples AND oranges" 将返回包含 "apples" 和 "oranges"（顺序不限）的匹配项。将会忽略仅含一个词的文档。

表 B-2 用于联机文档资料搜索的常用查询运算符

运算符	描述	示例
<CASE>	与其后所跟词大小写匹配。 注：Identity Manager 自动采用大写查询词在匹配时区分大小写，因此无需 <CASE>。小写词不区分大小写，因此在匹配时必须将小写词与 <CASE> 结合使用。	搜索 "<CASE> bill" 会查找 "bill" 而非 "Bill" 的匹配项。
<EXACT>	查找准确包含指定字词的文档。	搜索 "<EXACT> soft" 会查找包含 "soft" 一词的文档，而不会查找包含 "softest" 或 "softer" 的文档。
<MORPH>	查找包含指定字词结构变体的文档，其中包括复数、过去式和涉及前缀、后缀和复合词等的复杂形式。也会使用词典中的规范来正确处理不规则形式。	搜索 "<MORPH> surf" 会查找包含由 "surf" 演变出的变体 （如 "surfs"、"surfed" 和 "surfing"）的文档，以及包含带前缀 ("resurf") 的词和复合词 ("surfboard") 的文档。
<NEAR>	查找指定字词之间间隔不超过 1000 个词的文档。两个词的距离越近，该文档在搜索结果中的位置越靠前。	搜索 "resource <NEAR> configuration" 将会查找包含这两个词而且间隔不超过 1000 个词的文档。
<NEAR/n>	查找两词之间间隔不超过 n 个字词的文档。 注：*n* 的值必须在 1 和 1024 之间。	搜索 "buy <NEAR/3> sell" 会查找包含 "buy low and sell high" 的文档，因为 "buy" 和 "sell" 之间不超过三个词。
<NOT> 或 NOT	查找不包含指定字词或短语的文档。	搜索 "surf <AND> <NOT> channel" 会查找包含 "surf" 但不包含 "channel" 的文档。

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

表 C-1 列出了 Oracle 数据库类型的数据模式值：

表 C-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
resourceName	VARCHAR(128)
accountName	VARCHAR(50)
objectType	CHAR(2)
objectName	VARCHAR(128)
action	CHAR(2)
actionDate	CHAR(8)

表 C-1 Oracle 数据库类型的数据模式值

数据库列	值
actionTime	CHAR(12)
acctAttrChanges	VARCHAR(4000)
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)
parm02label	VARCHAR(50)
parm02value	VARCHAR(128)
parm03label	VARCHAR(50)
parm03value	VARCHAR(128)
parm04label	VARCHAR(50)
parm04value	VARCHAR(128)
parm05label	VARCHAR(50)
parm05value	VARCHAR(128)

DB2

表 C-2 列出了 DB2 数据库类型的数据模式值：

表 C-2 DB2 数据库类型的数据模式值

数据库列	值
ID	VARCHAR(50) NOT NULL

表 C-2 DB2 数据库类型的数据模式值

数据库列	值
name	VARCHAR(128) NOT NULL
resourceName	VARCHAR(128)
accountName	VARCHAR(50)
objectType	CHAR(2)
objectName	VARCHAR(128)
action	CHAR(2)
actionDate	CHAR(8)
actionTime	CHAR(12)
actionStatus	CHAR(1)
interface	VARCHAR(50)
server	VARCHAR(128)
subject	VARCHAR(128)
reason	CHAR(2)
message	VARCHAR(255)
acctAttrChanges	CLOB(16M)
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)
parm02label	VARCHAR(50)
parm02value	VARCHAR(128)
parm03label	VARCHAR(50)

表 C-2 DB2 数据库类型的数据模式值

数据库列	值
parm03value	VARCHAR(128)
parm04label	VARCHAR(50)
parm04value	VARCHAR(128)
parm05label	VARCHAR(50)
parm05value	VARCHAR(128)

MySQL

表 C-3 列出了 MySQL 数据库类型的数据模式值：

表 C-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
resourceName	VARCHAR(128)
accountName	VARCHAR(50)
objectType	CHAR(2)
objectName	VARCHAR(128)
action	CHAR(2)
actionDate	CHAR(8)
actionTime	CHAR(12)
actionStatus	CHAR(1)
interface	VARCHAR(50)
server	VARCHAR(128)
subject	VARCHAR(128)
reason	CHAR(2)
message	VARCHAR(255)
acctAttrChanges	BLOB
acctAttr01label	VARCHAR(50)
acctAttr01value	VARCHAR(128)

表 C-3 MySQL 数据库类型的数据模式值

数据库列	值
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)
parm02label	VARCHAR(50)
parm02value	VARCHAR(128)
parm03label	VARCHAR(50)
parm03value	VARCHAR(128)
parm04label	VARCHAR(50)
parm04value	VARCHAR(128)
parm05label	VARCHAR(50)
parm05value	VARCHAR(128)

Sybase

表 C-4 列出了 Sybase 数据库类型的数据模式值：

表 C-4 Sybase 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
resourceName	VARCHAR(128)
accountName	VARCHAR(50)
objectType	CHAR(2)

表 C-4 Sybase 数据库类型的数据模式值

数据库列	值
objectName	VARCHAR(128)
action	CHAR(2)
actionDate	CHAR(8)
actionTime	CHAR(12)
actionStatus	CHAR(1)
interface	VARCHAR(50)
server	VARCHAR(128)
subject	VARCHAR(128)
reason	CHAR(2)
message	VARCHAR(255)
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)
acctAttr05label	VARCHAR(50)
acctAttr05value	VARCHAR(128)
parm01label	VARCHAR(50)
parm01value	VARCHAR(128)
parm02label	VARCHAR(50)
parm02value	VARCHAR(128)
parm03label	VARCHAR(50)
parm03value	VARCHAR(128)
parm04label	VARCHAR(50)
parm04value	VARCHAR(128)
parm05label	VARCHAR(50)

表 C-4 Sybase 数据库类型的数据模式值

数据库列	值
parm05value	VARCHAR(128)

审计日志数据库映射

表 C-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 C-5 对象键类型、操作和操作状态数据库键

审计对象类型	数据库键	操作	数据库键	操作状态	数据库键
管理员	AD	批准	AP	失败	F
管理员组	AG	更改密码	CP	成功	S
Application	AP	更改资源密码	CR		
审计配置	AC	配置	CG		
审计日志	AL	连接	CN		
电子邮件模板	ET	创建	CT		
Lighthouse 帐户	LA	证书到期	CE		
登录配置	LC	删除	DL		
通知	NT	删除帐户	DA		
对象组	OG	取消置备	DP		
策略	PO	禁用	DS		
Remedy 配置	RC	断开	DC		
资源帐户	RA	启用	EN		
资源	RS	启动	LN		
资源对象	RE	加载	LD		
Role	RL	登录	LG		
角色属性	RT	退出	LO		
任务定义	TD	本机更改	NC		
任务实例	TI	保护资源密码	PT		
任务进度表	TS	置备	PV		

表 C-5 对象键类型、操作和操作状态数据库键

审计对象类型	数据库键	操作	数据库键	操作状态	数据库键
用户	US	拒绝	RJ		
工作流案例	WC	重新置备	RV		
工作流进程	WP	重置密码	RP		
工作流任务	WT	终止	TR		
		更新	MO		
		视图	VW		

活动同步向导

概述

在 7.0 之前版本的 Identity Manager 中，活动同步向导可用于创建和管理活动同步。此附录所包含的信息说明如何使用活动同步向导在支持的 Identity Manager 版本中设置和管理活动同步。对于 7.0 和更高版本，同步策略可用于配置同步。

设置同步

使用 Identity Manager 资源区域中的 "Active Synce Wizard" 设置活动同步。此向导通过一组操作步骤（具体步骤视选项的不同而定）指导您完成对资源活动同步的设置。

要启动活动同步向导，请在资源列表中选择资源，然后在 "Resource Actions" 选项列表中选择 **Active Sync Wizard**。

同步模式

使用 "Synchronization Mode" 页可以确定在活动同步设置过程中可选择的配置选项范围。

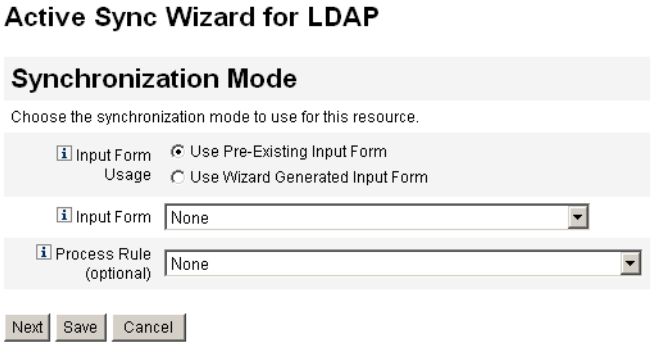
从这些选项中选择：

输入表单用法 - 选择设置活动同步时使用的模式。可以选择使用之前已存在的表单，但这会限制该资源的配置选项的使用。也可以使用由活动同步向导生成的表单，该表单可以提供一组完整的配置选项。

- 如果选择 "Pre-Existing Input Form" （默认），则可选择下列选项：
    - **输入表单** - 选择将处理数据更新的输入表单。此可选配置项目允许在将属性保存到帐户之前对其进行转换。

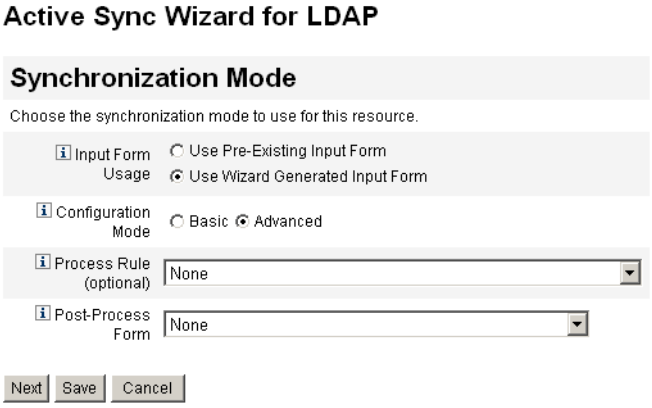
- **进程规则** - （可选）选择要为每个传入帐户运行的进程规则。此选择将覆盖所有其他选项。如果指定了进程规则，则会为每一行运行该进程，而不管资源上的其他设置如何。既可以是进程名称，也可以是进程名称的评估规则。

图 D-1 活动同步向导：同步模式，已存在表单选项



- 如果选择 **Use Wizard Generated Input Form**，请继续针对以下选项进行选择：
  - **配置模式** - 选择在活动同步向导内使用基本模式还是高级模式。基本模式为默认选项。如果选择高级模式，您可定义事件类型和设置进程规则。
  - **进程规则** -（仅在高级配置模式下显示。）（可选）为每个传入帐户选择要运行的进程规则。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。
  - **后处理表单** -（仅在高级配置模式下显示。）（可选）选择要运行的除活动同步向导生成的表单之外的表单。此表单将覆盖活动同步向导的全部设置。

图 D-2 活动同步向导：同步模式，向导生成的表单选项



单击 **Next** 继续使用向导。显示 "Active Sync Running Settings" 页面。

运行设置

该页面允许您为活动同步建立以下设置：

- 启动
- 轮询
- 日志

启动设置

在以下选项中选择活动同步启动的选项：

- **启动类型** - 选择以下选项之一：
  - **“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。
- **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。

轮询设置

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，则 Identity Manager 将根据此信息和轮询间隔来确定轮询的开始时间。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。

选择轮询设置的选项：

- **轮询频率** - 指定轮询的频率。输入数字，然后选择时间单位 （天、小时、分钟、月、秒或周）。默认单位是分钟。
- **轮询开始日期** - 输入第一个调度间隔开始的日期 （格式为 yyyyMMdd）。
- **轮询开始时间** - 输入一天中第一个调度间隔开始的时间 （格式为 `HH:mm:ss`）。

日志记录设置

在以下选项中选择设置日志记录信息和日志记录级别的选项：

- **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，活动日志将被归档。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 "Maximum Log File Size" 指定的条件进行评估。

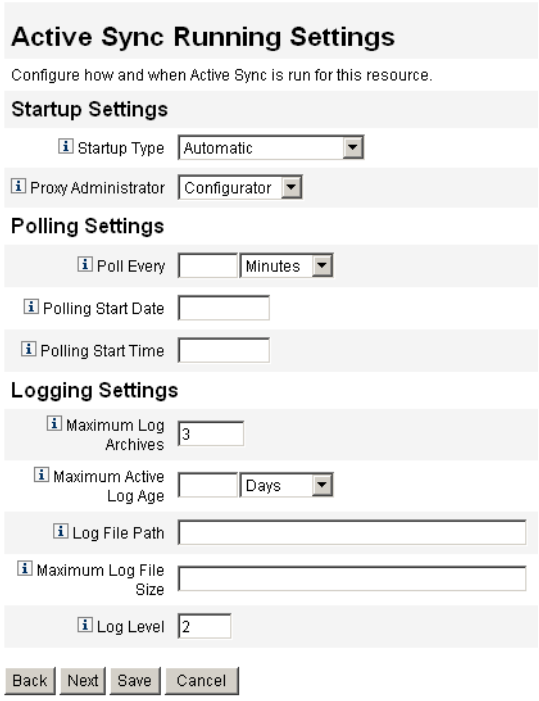
输入数字，然后选择时间单位 （天、小时、分钟、月、秒或周）。默认单位是天。

- **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 "Maximum Active Log Age" 指定的使用期限条件进行评估。
- **日志级别** - 输入日志记录的级别：
  - 0 - 无日志记录

- 1 - 错误
- 2 - 信息
- 3 - 详细
- 4 - 调试

图 D-3 是运行设置页的示例视图。

图 D-3 活动同步向导：运行设置



单击 **Next** 继续使用向导。显示 "General Active Sync Settings" 页面。

常规活动同步设置

使用此页指定常规活动同步配置参数。

特定于资源的设置

特定于资源的可用设置因资源类型而异。例如，对于 LDAP 资源，以下设置可能适用。

- **要同步的对象类** - 输入要同步的对象类。更改日志针对所有对象，而此项功能会过滤那些仅对已列出对象类的更新。
- **要同步的帐户的 LDAP 过滤器** - 输入要同步的对象的可选 LDAP 过滤器。更改日志是针对所有对象的；此过滤器将只更新与指定过滤器匹配的对象。如果指定了过滤器，则只有在对象符合过滤器条件并且包含已同步的对象类时，才会对其进行同步。
- **要同步的属性** - 输入要同步的属性名称。此功能将忽略更改日志中的未更新任何指定属性的更新。例如，如果仅列出了 department，则将只处理影响 department 的更改。所有其他更新都将忽略。如果此项为空白 （默认值），则会处理所有更改。
- **更改日志块大小** - 输入每次查询取得的更改日志条目数。默认数量为 100。
- **更改编号属性名称** - 输入更改日志条目中的更改编号属性名称。
- **过滤更改方式** - 输入目录管理员的名称 (RDN) 以过滤更改。将过滤与此列表中条目匹配的具有属性 `modifiersname` 的更改。

标准值是此适配器使用的管理员名称，可以避免循环。条目格式应为 `cn=Directory Manager`。

公共设置

- **关联规则** - （可选）指定一个关联规则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** - （可选）指定一个确认规则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** - （可选）指定在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** - （可选）指定一个规则，它可以针对每个传入的用户更新进行评估并返回 true 或 false，以确定是否应进行删除操作。
- **创建不匹配帐户** - 如果为 true，则适配器将尝试创建在 Identity System 中未找到的帐户。如果为 false，适配器将通过由解析进程规则返回的进程来运行帐户。
- **针对创建事件分配 Active Sync 操作资源** - 如果选择此选项，则将活动同步源资源分配给检测到创建事件时创建的用户。
- **全局填充** - 传入帐户中的所有属性将始终可用于 ActiveSync 名称空间下的表单。如果选择此选项，则所有属性 （accountId 除外）也可用于全局名称空间。

- **重置时，忽略以往的更改** - 初次启动或重置适配器时，选择忽略以往的更改。要重置适配器，请编辑 XmlData 对象 SYNC_resourceName 以为所需的同步进程（例如 ActiveSync）删除 MapEntry。此选项仅对部分适配器可用。
- **轮询前工作流** - 选择要在每次轮询之前立即执行的可选工作流。
- **轮询后工作流** - 选择要在每次轮询之后立即执行的可选工作流。

单击 **Save** 或 **Next** 将更改保存至资源的常规设置中：

- 如果正在使用已存在的输入表单，则单击 **Save** 以完成向导选项并返回 "Resources" 列表。
- 如果正在使用向导生成的输入表单，则单击 **Next** 继续。
  - 如果正在使用 *basic* 配置模式，则显示 "Target Resources" 页。（在本章中快进至第 461 页上的 “目标资源”。）
  - 如果正在使用 *advanced* 配置模式，则显示 "Event Types" 页。

事件类型

此页用于配置一种机制，以确定活动同步资源上是否发生了某一类型的更改事件。

关于事件

活动同步事件定义为在活动同步资源上的更改。针对每种资源列出的事件类型取决于资源的类型以及受更改事件影响的对象的类型。其中一些事件类型为创建、删除、更新、禁用、启用和重命名。

忽略事件

您可选择一种用于确定是否忽略活动同步事件的机制。选项包括：

- **无** - 不忽略活动同步事件。
- **规则** - 使用规则确定是否忽略活动同步事件。如果选择此选项，则必须额外在选项列表中选择一个规则。
- **条件** - 使用条件确定是否忽略活动同步事件。选择此选项后，单击 "Edit Condition" 以使用 "Condition Panel" 来定义条件。

用来确定事件类型的选项包括：

- **无** - 没有用于确定事件类型的方法。
- **规则** - 使用规则确定事件类型。如果选择此选项，则必须额外在选项列表中选择一个规则。
- **条件** - 使用条件确定事件类型。选择此选项后，单击 "Edit Condition" 以使用 "Condition Panel" 来定义条件。

单击 **Next** 继续使用向导。显示 "Process Selection" 页。

进程选择

检入特定活动同步事件实例或活动同步事件类型的用户视图时，使用此页面设置要运行的工作流或进程。

进程模式

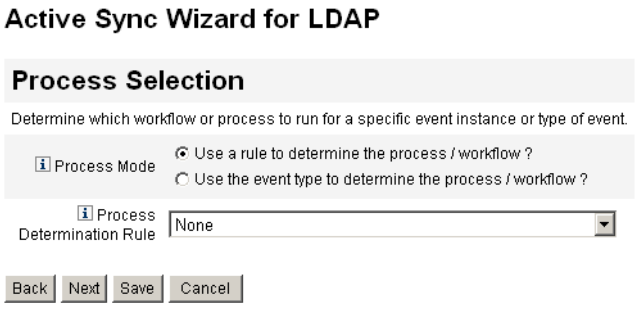
提供了两种进程模式，这两种模式可确定活动同步事件发生时将运行哪个工作流或进程：

- **规则** - 可以使用特定的规则来确定要为每个活动同步事件实例运行的工作流或进程。这表示每次事件发生时就会执行此规则。

  选择此选项后，请从列表中选择一种规则 （进程确定规则）。

  图 D-4 说明了您指定规则时所用的 "Process Selection" 页。

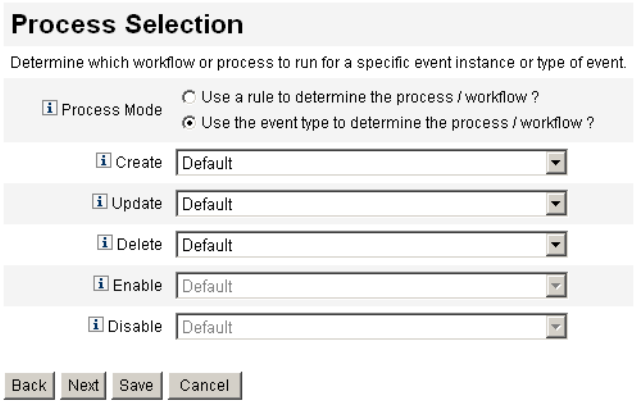
  图 D-4 活动同步向导：进程选择 （规则）

- **事件类型** - 可以根据每个事件实例的事件类型运行工作流或进程。此选项为默认选项。

  选择此选项后，为每个列出的事件类型选择要运行的工作流或进程，如图 D-5 中所示。

图 D-5 活动同步向导：进程选择 （事件类型）

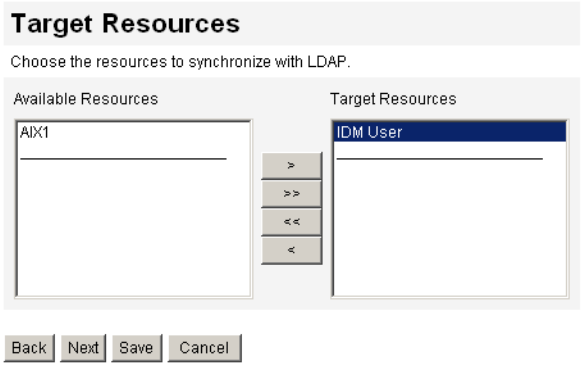


单击 **Next** 继续使用向导。显示 "Target Resources" 页。

目标资源

此页用于指定要与该资源同步的目标资源。

图 D-6 活动同步向导：目标资源

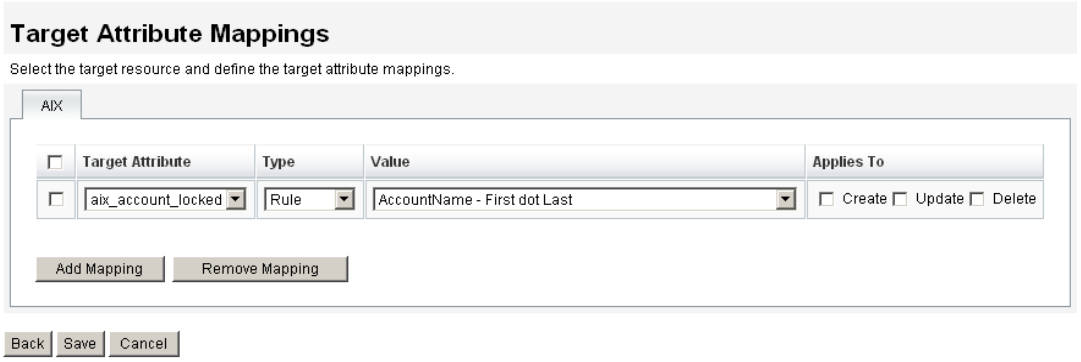


1. 从 “可用资源” 区域选择一个或多个资源，然后将其移至 “目标资源” 区域。
2. 单击 **Next** 继续。显示 "Target Attribute Mapping" 页。

目标属性映射

此页用于为每个目标资源定义目标属性映射。

图 D-7 活动同步向导：目标属性映射



1. 从选项列表中选择目标资源。要向列表中添加目标属性，请单击 **Add Mapping**。
2. 为每一个目标属性选择属性、类型和属性值。
3. 在 "Applies To" 列中，选择要应用映射的一个或多个操作 （"Create"、"Update" 或 "Delete"）。
4. 针对每个目标资源继续进行选择。

要从列表中删除属性行，请选择该行，然后单击 **Remove Mapping**。

单击 **Save** 以保存属性映射并返回资源列表。

词汇表

access review （访问查看） 证明一组雇员在特定日期具有适当的用户权利的管理和审计过程。

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。

dministrator （管理员） 安装 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。

administrator interface （管理员界面） Identity Manager 的主要管理视图。

approver （批准者） 具备管理权能的用户，负责批准或拒绝访问请求。

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。

attestation task （证明任务） 需要证明的用户权利查看的逻辑集合。如果将用户权利分配给同一证明者并从相同的访问查看实例中生成，则用户权利将分组到单一的证明任务。

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。

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 以前的版本提供） 。在当前版本的 Identity Manager 中， BPE 已由 Identity Manager IDE 代替。请参见*Identity Manager IDE*。

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。

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**。

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。

ide *请参见* Identity Manager IDE。

Identity Manager IDE Identity Manager 集成开发环境 (Integrated Development Environment, IDE) 是一个 Java 应用程序，允许您在部署中查看、自定义和调试 Identity Manager 对象。

identity template （身份模板） 定义用户的资源帐户名称。

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 Identity Manager 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。

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 （资源） Identity Manager 对象，用于存储有关如何连接到已创建帐户的资源或系统的信息。

Identity Manager 可访问的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。

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 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 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。

role （角色） 在 Identity Manager 中，指一类用户的模板或配置文件。每个用户都能被分配一个或多个角色，这些角色定义帐户资源访问权限和默认资源属性。

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 （模式） 资源的用户帐户属性列表。

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。

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 （用户） 拥有 Identity Manager 系统帐户的人。用户可拥有 Identity Manager 中一定范围的权能；而具有扩展权能的用户为 Identity Manager 管理员。

user account （用户帐户） 使用 Identity Manager 创建的帐户。

指 Identity Manager 帐户或 Identity Manager 资源上的帐户。用户帐户的设置过程是动态过程；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） 显示某个特定日期向某个用户分配的资源及其资源重要属性的用户视图。

user interface （用户界面） Identity Manager 系统的受限视图。

专为不具备管理权能的用户而设计，该视图允许这些用户执行一定范围的自服务任务，如更改密码、设置验证问题的答案和管理委托分配。

virtual organization （虚拟组织） 在目录连接中定义的组织。*请参见*目录连接。

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。

work items （工作项目） Identity Manager 中的工作流、表单或过程生成的操作请求，此操作请求将分配给已指定为批准者、证明者或修正者的用户。

索引

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

W

X

Y

Z

Z