Identity Console
管理指南

2022 年 9 月

法律声明

目录

关于本书和库

*管理指南*提供有关 NetIQ Identity Console (Identity Console) 产品的概念性信息。此指南定义术语，并提供各种实施案例。

有关最新版的 *《NetIQ Identity Console 管理指南》*，请参见 NetIQ Identity Console 联机文档站点上该文档的英文版。

目标受众

本指南面向网络管理员。

库中的其他信息

此库提供了以下信息资源：

安装指南

介绍如何安装 Identity Console。该书适用于网络管理员。

关于 NetIQ Corporation

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

我们的观点

适应变化及管理复杂性和风险实乃老生常谈

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

提供更好、更快的关键业务服务

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

我们的理念

销售智能解决方案，而不只是软件

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

推动您走向成功是我们的追求

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

我们的解决方案

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

与销售支持联系

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

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

联系技术支持

有关具体的产品问题，请与我们的技术支持团队联系。

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

联系文档支持

我们的目标是提供满足您的需要的文档。如果您有改进建议，请单击 www.netiq.com/documentation 上发布的 HTML 版文档任何页面底部的**添加注释**。您还可以发送电子邮件至 Documentation-Feedback@netiq.com。我们会重视您的意见，欢迎您提供建议。

联系在线用户社区

Qmunity 是 NetIQ 在线社区的简称，它是让您可与同行和 NetIQ 专家沟通的协作网络。通过提供更多即时信息、指向实用资源的有用链接，以及 NetIQ 专家的支持， Qmunity 有助于确保您可以掌握必要的知识，以充分发挥所依赖的 IT 投资的潜力。有关详细信息，请访问 http://community.netiq.com。

1 Identity Console 是什么？

Identity Console 是一流的基于 Web 的管理控制台，借助 Identity Console，可通过因特网和 Web 浏览器提供对网络管理实用程序的虚拟、安全和自定义的访问权限。 Identity Console 让管理任务权利下放更容易实现。

Identity Console 功能

Identity Console 具有下列功能：

- 管理 eDirectory 对象、用户、纲要、分区、副本、权限等
- 管理 Identity Manager 驱动程序和驱动程序集
- 管理和查看驱动程序的性能统计数字
- 检查对象、查看驱动程序的数据流、管理权利、工作指令等。
- 管理驱动程序的口令同步状态和设置
- 管理口令策略和登录方法
- 管理证书
- 管理各种网络资源
- 提高安全措施，保护您的数据
- 提高可伸缩性，管理更大的 eDirectory 对象
- 通过 One SSO Provider (OSP) 安全登录 Identity Console 门户
- 采用行业最新 UI 技术
- 易于通过 Docker 容器安装和配置

2 如何访问 Identity Console？

可通过任意支持的 Web 浏览器访问 Identity Console 和它提供的所有功能。虽然可以通过未列出的 Web 浏览器访问 Identity Console，但对于非官方支持的任何浏览器，我们不保证提供或者支持全部功能。

重要：有关支持的 Web 浏览器的信息，请参见 *《Identity Console 安装指南》*。

访问 Identity Console

要访问基于服务器的 Identity Console，执行下列步骤：

1. 在受支持的 Web 浏览器的 " 地址 "(URL) 字段中输入下列内容。

   安全登录：https://< *服务器 IP 地址* / 主机名 >:< 端口 >/identityconsole/

   示例中 < *服务器 IP 地址* > 中的 IP 地址应为 IPv4。要使用的默认端口为 9000。
2. 用您的用户 DN 和口令登录。
3. 指定具有或不具有 LDAP 安全端口的 eDirectory 树 IP 或 DNS。

注释：

- 因安全性原因，刷新 Identity Console 中的任意选项卡将使用户注销。
- 因安全性原因，在浏览器中打开重复的 Identity Console 选项卡将使用户注销。
- 应以 cn=admin,ou=sa,o=system 格式指定 DN。
- 如果 eDirectory 配置了非默认端口，则必须指定端口号。

---

3 Identity Console 界面导航

此部分介绍如何在 Identity Console Web 界面中导航。

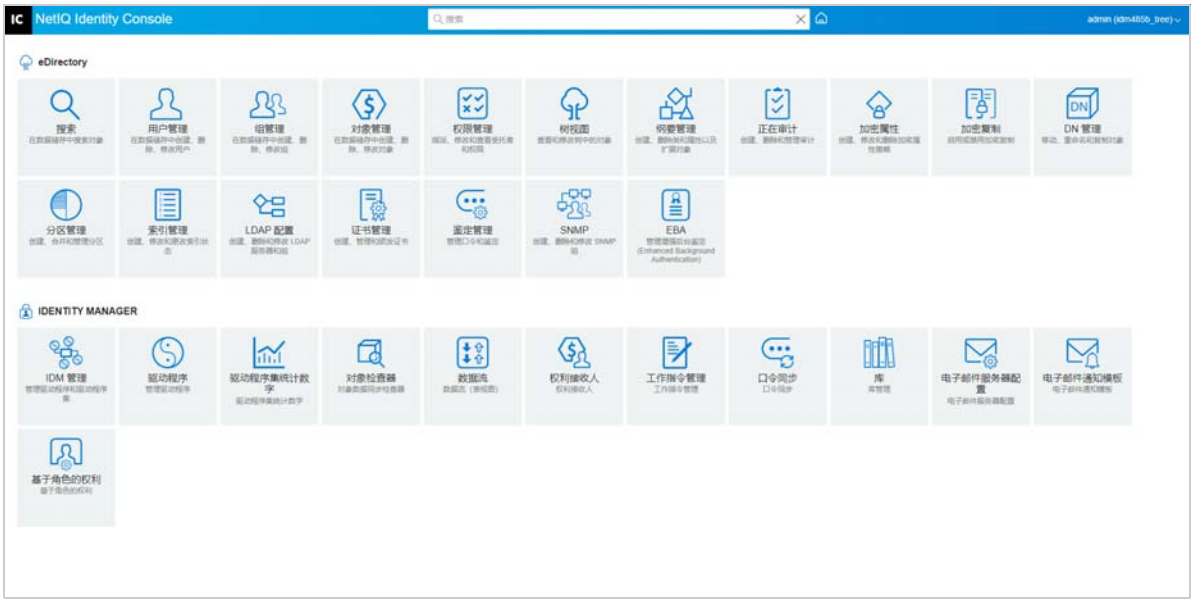
搜索 （技术预览）

搜索 （技术预览）为您提供了搜索功能的介绍性布局。在此预览中，您可以指定关键字，搜索字段确定要搜索和显示匹配结果的信息源。使用此选项，您可以查找资源，并在 Identity Console 应用程序的任何页面上轻松访问它。

Identity Console 界面

Identity Console 界面由 eDirectory 和 Identity Manager 模块组成。

图 3-1 Identity Console 界面



重要：本指南中使用的几个 GIF 动画仅适用于联机文档。如果想要切换为 PDF，将仅显示屏幕截图。

表 3-1 Identity Console Web 门户各模块解释

模块名	说明
搜索	在数据储存中搜索对象。有关更多信息，请参见第 4 章 " 执行搜索 " （第 23 页）。
用户管理	在数据储存中创建、删除和修改用户。有关更多信息，请参见第 5 章 " 管理用户 " （第 25 页）。
组管理	在数据储存中创建、删除和修改组。有关更多信息，请参见第 6 章 " 管理组 " （第 33 页）。
对象管理	在数据储存中创建、删除和修改对象。有关更多信息，请参见第 7 章 " 管理对象 " （第 39 页）。
权限管理	指派、修改和查看受托者和权限。有关更多信息，请参见第 8 章 " 管理权限 " （第 47 页）。
树视图	查看和修改树中的对象。有关更多信息，请参见第 9 章 " 树视图 " （第 51 页）。
纲要管理	创建、删除类、辅助类、属性并扩展对象。有关更多信息，请参见第 10 章 " 管理纲要 " （第 55 页）。
审计	启用、禁用和管理 CEF 审计。有关更多信息，请参见第 11 章 " 管理审计事件 " （第 63 页）。
加密的属性	创建、修改、删除和查看加密属性策略。有关更多信息，请参见第 12 章 " 管理加密属性 " （第 69 页）。
加密复制	启用、禁用和查看加密复制。有关更多信息，请参见第 13 章 " 管理加密复制 " （第 73 页）。
DN 管理	移动、重命名和复制对象。有关更多信息，请参见第 7 章 " 管理对象 " （第 39 页）。
分区管理	创建、合并和移动分区和复本。有关更多信息，请参见第 14 章 " 管理分区和复本 " （第 75 页）。
索引管理	创建、修改和更改索引状态。有关更多信息，请参见第 15 章 " 管理索引 " （第 79 页）。
LDAP 配置	创建、删除和修改 LDAP 对象。有关更多信息，请参见第 16 章 " 配置 LDAP 对象 " （第 83 页）。
证书管理	创建和管理服务器和 CA 证书。有关更多信息，请参见第 17 章 " 管理证书 " （第 87 页）。
鉴定管理	创建和管理 login.post-login 方法和顺序。您还可以使用此模块管理口令策略和询问集。有关更多信息，请参见第 18 章 " 管理鉴定框架 " （第 103 页）。

模块名	说明
SNMP	创建、删除和修改 SNMP 组。有关更多信息，请参见第 19 章 " 管理 SNMP 组对象 "（第 117 页）。
EBA	管理增强的后台鉴定。有关更多信息，请参见第 20 章 " 管理增强的后台鉴定 "（第 121 页）。
IDM 管理	管理 Identity Manager 驱动程序和驱动程序集。有关详细信息，请参见第 21 章 " 管理驱动程序和驱动程序集 "（第 125 页）。您还可以使用此模块管理驱动程序集属性。有关更多信息，请参见第 22 章 " 管理驱动程序集属性 "（第 131 页）。
驱动程序属性	管理各种驱动程序的属性。有关更多信息，请参见第 23 章 " 管理驱动程序属性 "（第 143 页）。
驱动程序集统计数字	管理和查看驱动程序集统计数字。更多信息请参见第 24 章 " 管理驱动程序集统计数字 "（第 169 页）。
对象检查器	管理对象关联和数据同步。有关更多信息，请参见第 25 章 " 检查 Identity Manager 对象 "（第 171 页）。
数据流	管理和查看驱动程序的数据流。有关更多信息，请参见第 26 章 " 管理数据流 "（第 173 页）。
权利接收人	管理权利接收人。有关更多信息，请参见第 27 章 " 管理权利接收人 "（第 175 页）。
工作指令管理	管理工作指令。有关更多信息，请参见第 28 章 " 管理工作指令 "（第 177 页）。
口令同步	管理口令同步和状态。有关更多信息，请参见第 29 章 " 管理口令状态和同步 "（第 181 页）。
库管理	管理库。有关更多信息，请参见第 30 章 " 管理库 "（第 185 页）。
电子邮件服务器配置	管理电子邮件服务器选项。有关更多信息，请参见第 31 章 " 管理电子邮件服务器选项 "（第 187 页）
电子邮件通知模板	管理电子邮件模板。有关更多信息，请参见第 32 章 " 管理电子邮件模板 "（第 189 页）

使用 Identity Console 管理 eDirectory

本部分介绍了您使用 Identity Console 门户管理 eDirectory 服务器可以执行的任务。

4 执行搜索

通过“搜索”部分可以指定要对目录树执行的搜索操作并显示结果。此选项允许您搜索不同对象、用户、组和其他内容。要对数据储存库中的各种对象执行搜索操作，执行下列操作：

1 指定搜索的对象名。使用星号通配符指定部分名称。例如：ldap*、 *cert、 *server* 等。如果此字段仅使用星号， Identity Console 将根据所选类型和环境返回所有搜索结果。

注释：使用环境浏览器，您可以通过在搜索字段中指定星号 (*) 浏览整个 eDirectory 树。您还可以通过使用通配符搜索来过滤环境浏览器中的对象。例如， admin*。 Identity Console 中的多种模块均支持环境浏览器的此行为。

---

2 在类型字段中选择搜索的对象类型。 Identity Console 仅显示指定类型的对象。此字段默认选择用户类型。

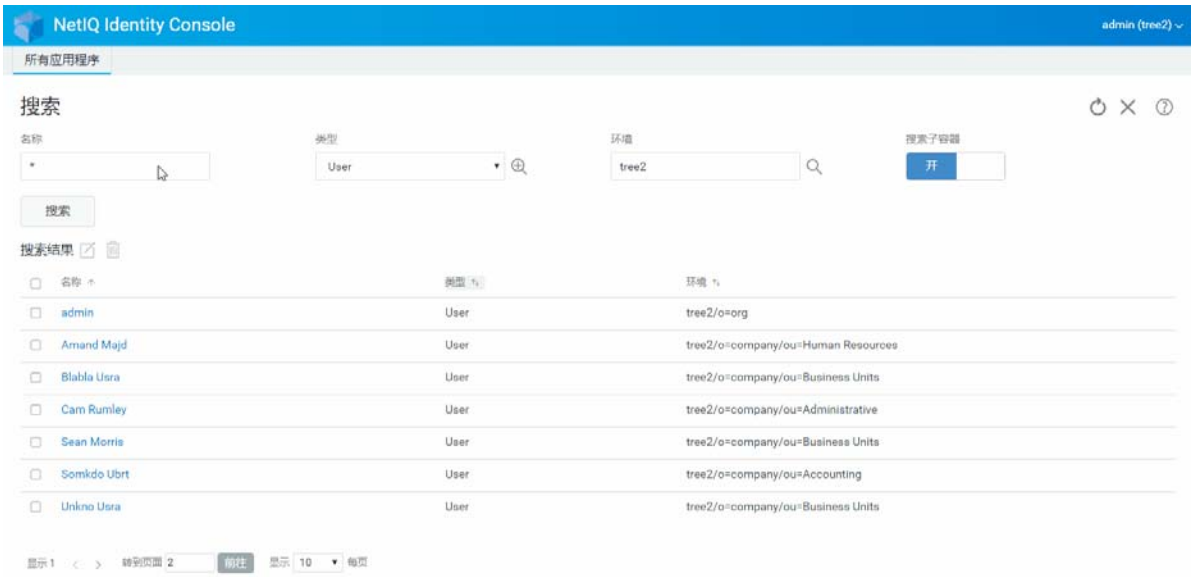
   单击 图标定义其他属性级别的搜索设置。有关详细信息，请参见 配置高级搜索 （第 24 页）。

3 在环境字段中指定搜索操作起始容器。

4 如果希望搜索包含从属容器，为“搜索子容器”选项选择开启。

5 单击 搜索 按钮。

图 4-1 执行搜索操作



配置高级搜索

“ 高级选择 ” 为在目录中搜索所需对象提供更容易配置的环境。

对象类型 : 指定要搜索的对象基类。例如 “ 用户 ”。

辅助类： 单击 ＋ 图标指定要包含在搜索中的辅助类。

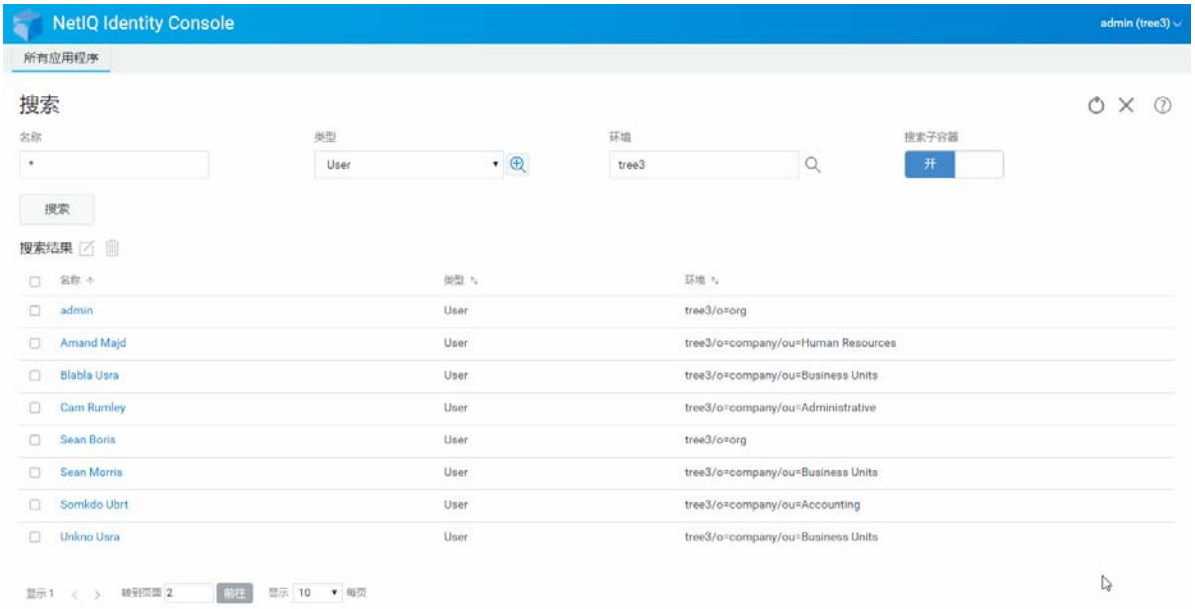
属性 : 指定过滤器要利用的属性 （属性）。

操作员 : 指定要应用于过滤器的逻辑运算符。选项包括。

值 : 指定要作为过滤器使用的属性值。可以使用星号 (*) 作为通配符来指示值的一部分。例如 smi*、 *th 和 *mit*。

此外，使用 ＋ Rule 图标将其他属性添加到列表中，可以将多个属性过滤器链接在一起，组成一个过滤器组。使用多个属性过滤器时，使用逻辑 AND 或逻辑 OR 将这些属性过滤器链接在一起。

图 4-2 配置高级搜索



5 管理用户

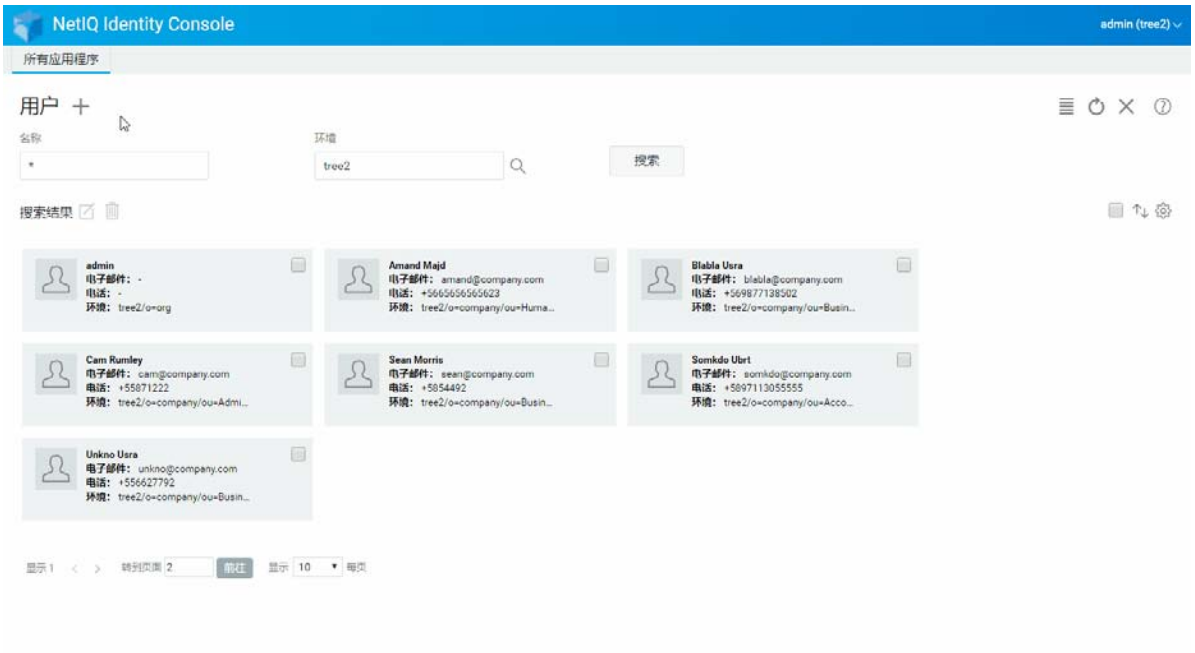
管理用户及其网络访问权限是数据储存的主要目的。使用 Identity Console Web 门户，可以执行下列用户相关任务：

创建用户

创建新的用户对象：

1. 在 Identity Console 登录页中单击用户管理选项。
2. 单击 ＋ 图标。
3. 在 “ 创建用户 ” 页，至少提供所需的用户相关信息，然后单击 创建 按钮。
   - 用户名
   - 环境
   - 姓
   - 口令
4. 此时显示一条确认讯息，指示已创建用户对象。

图 5-1 创建用户



删除用户

删除用户对象：

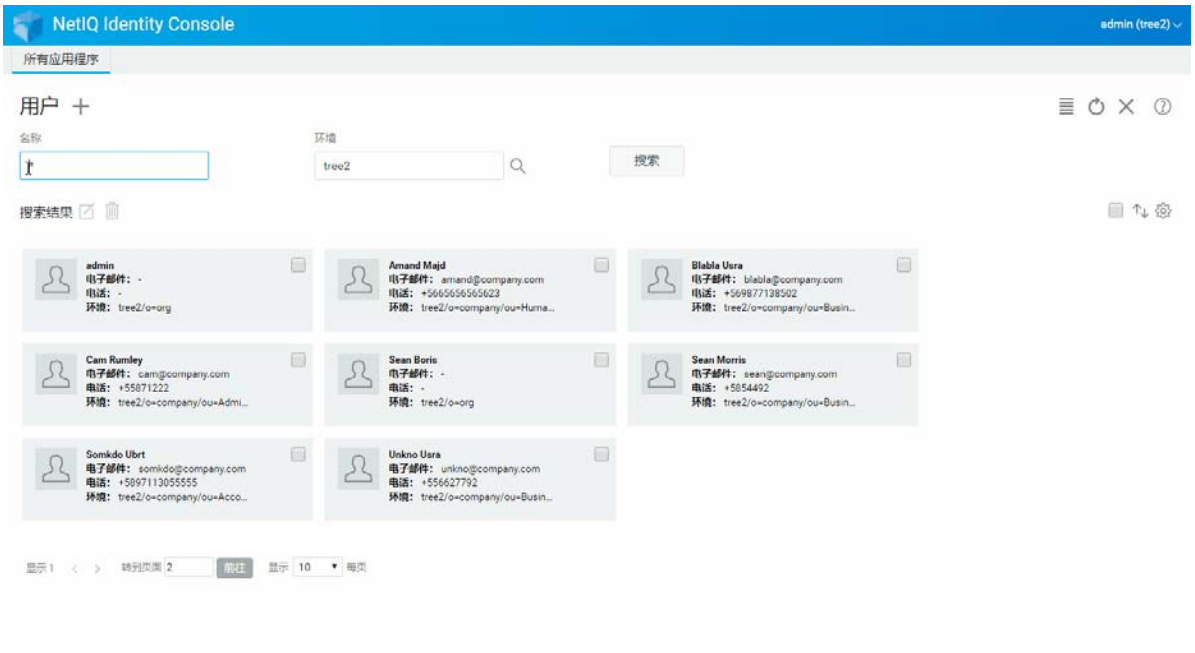
1 在 Identity Console 登录页中单击用户管理选项。

2 键入对象的名称和环境，或使用搜索功能查找对象，然后单击 搜索 按钮。

3 从用户列表中选择用户对象并单击 🗑 图标。

4 此时显示一条确认讯息，指示已删除该用户对象。

图 5-2 删除用户



修改用户

要修改用户对象：

1 在 Identity Console 登录页中单击用户管理选项。

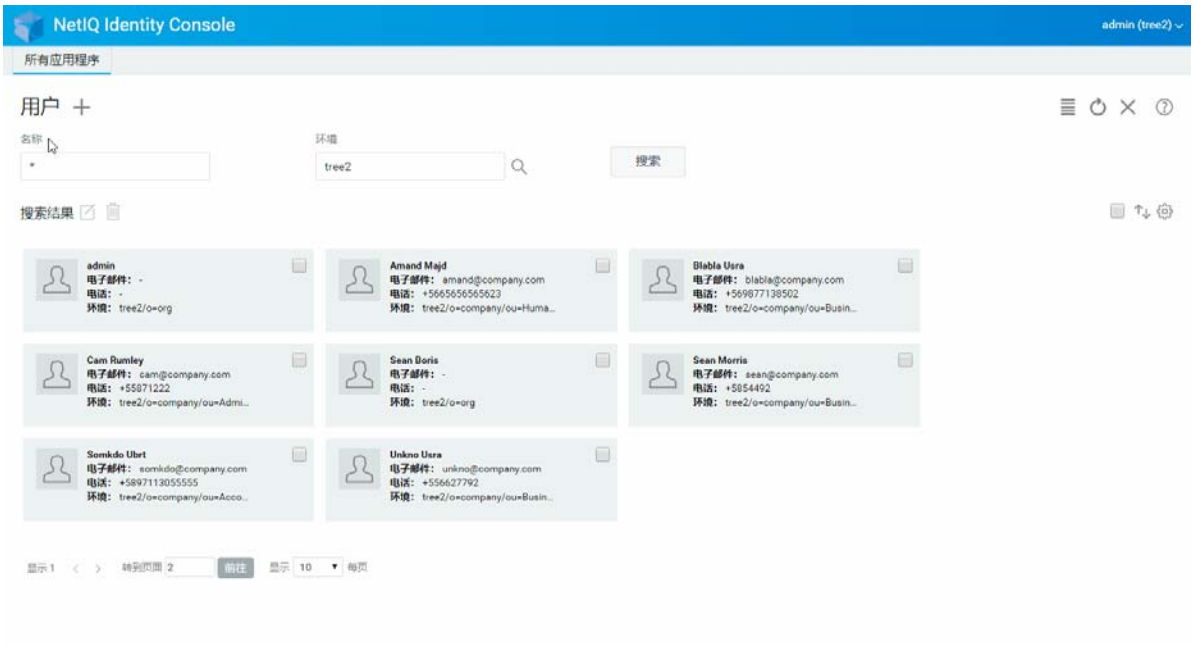
2 键入对象的名称和环境，或使用搜索功能查找对象，然后单击 搜索 按钮。

3 在用户列表中选择用户对象并单击 图标。

4 做更改，然后单击 保存 按钮。

5 此时显示一条确认讯息，指示已修改用户对象。

图5-3 修改用户



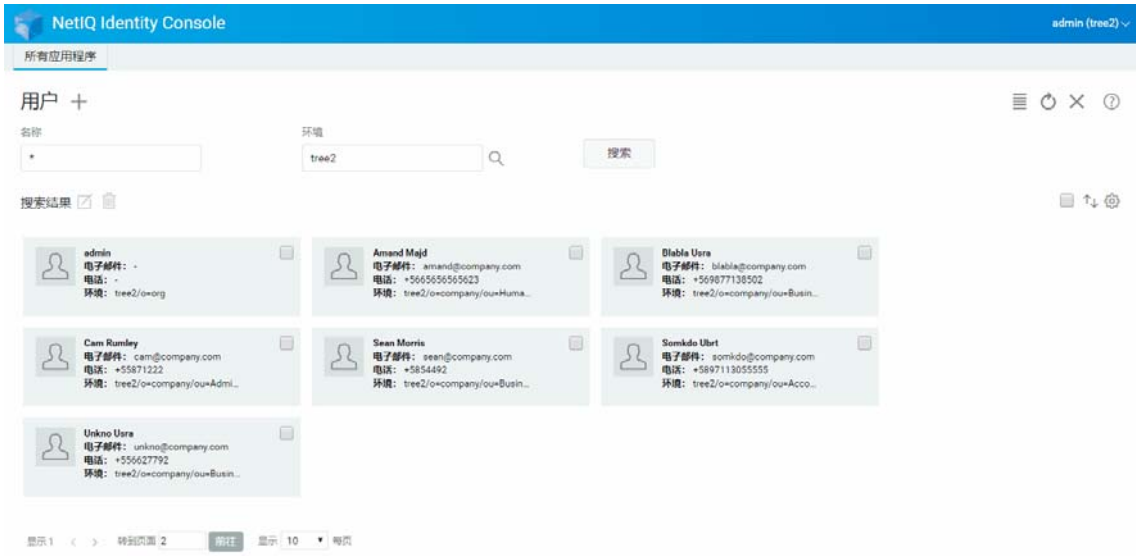
搜索用户

要搜索用户对象：

1 在 Identity Console 登录页中单击用户管理选项。

2 可以按名称或按名称和环境搜索用户。指定必要细节后，单击 搜索 图标。

图5-4 搜索用户

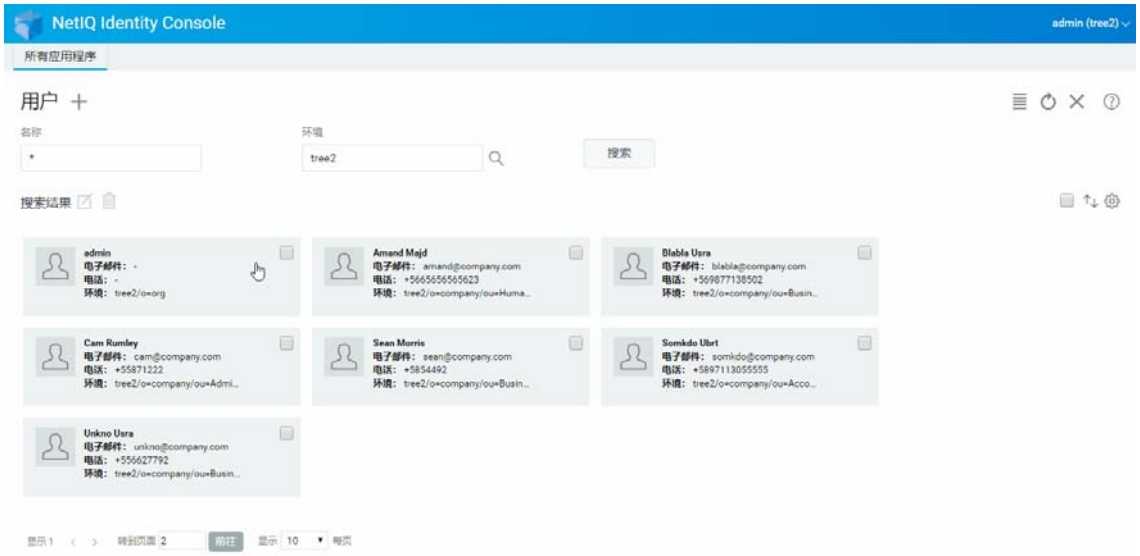


设置口令限制

口令限制允许您执行下列操作：

- 允许用户更改其各自的口令
- 实施口令登录
- 指定口令强度
- 实施周期性口令更改
- 指定口令失效日期
- 实施创建唯一口令
- 口令失效情况下，指定宽限登录期。

图5-5 *口令限制*



启用和禁用用户帐户

要禁用用户帐户，执行下列操作：

1 选择要禁用其帐户的用户并单击 图标。

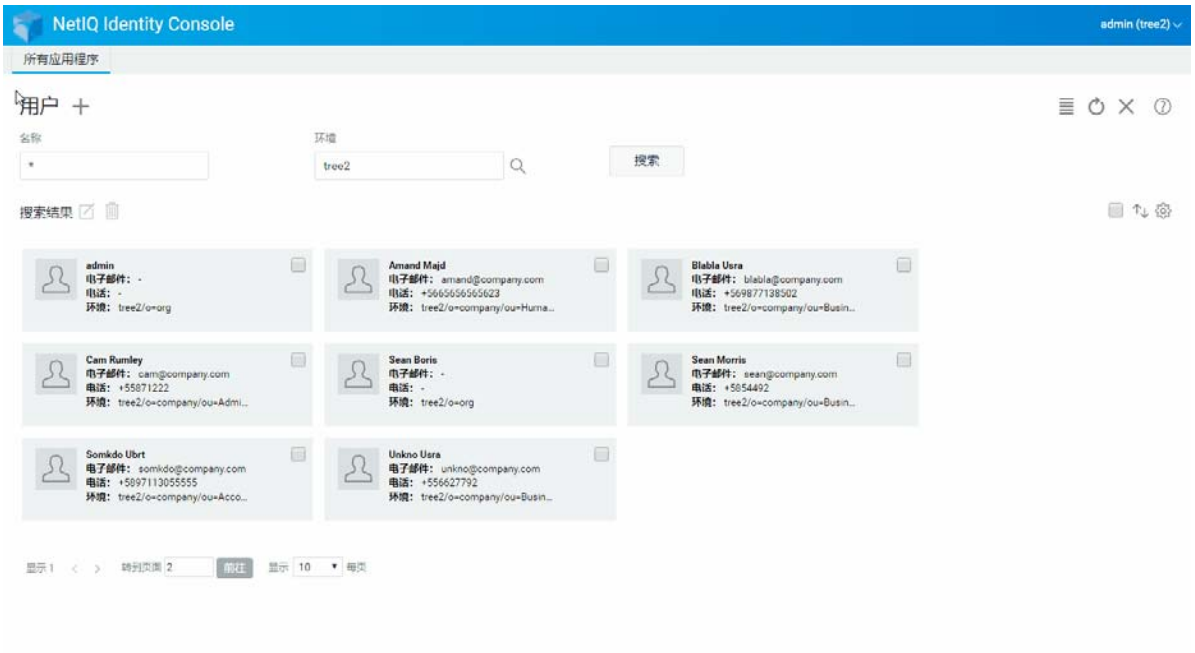
2 单击修改用户页中的限制选项卡。

3 展开登录限制选项卡，勾选帐户已禁用复选框。

4 单击 保存 图标。

5 现已禁用用户帐户。要启用任何已禁用的用户帐户，取消勾选帐户已禁用复选框。

图 5-6 启用和禁用用户帐户



设置帐户失效日期

要为用户设置帐户失效日期，执行下列操作：

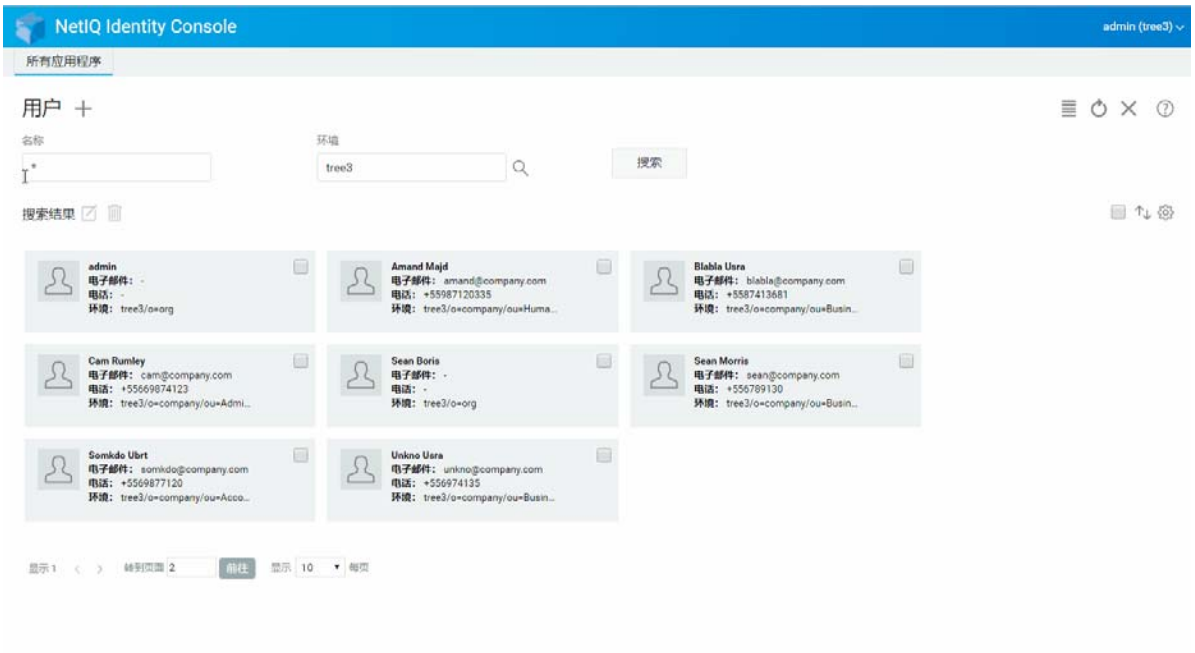
1 选择要设置帐户失效日期的用户，单击 图标。

2 单击修改用户页中的限制选项卡。

3 展开登录限制选项卡，勾选帐户具有失效日期复选框，指定失效日期。

4 单击 保存 图标。

图 5-7 设置帐户失效日期

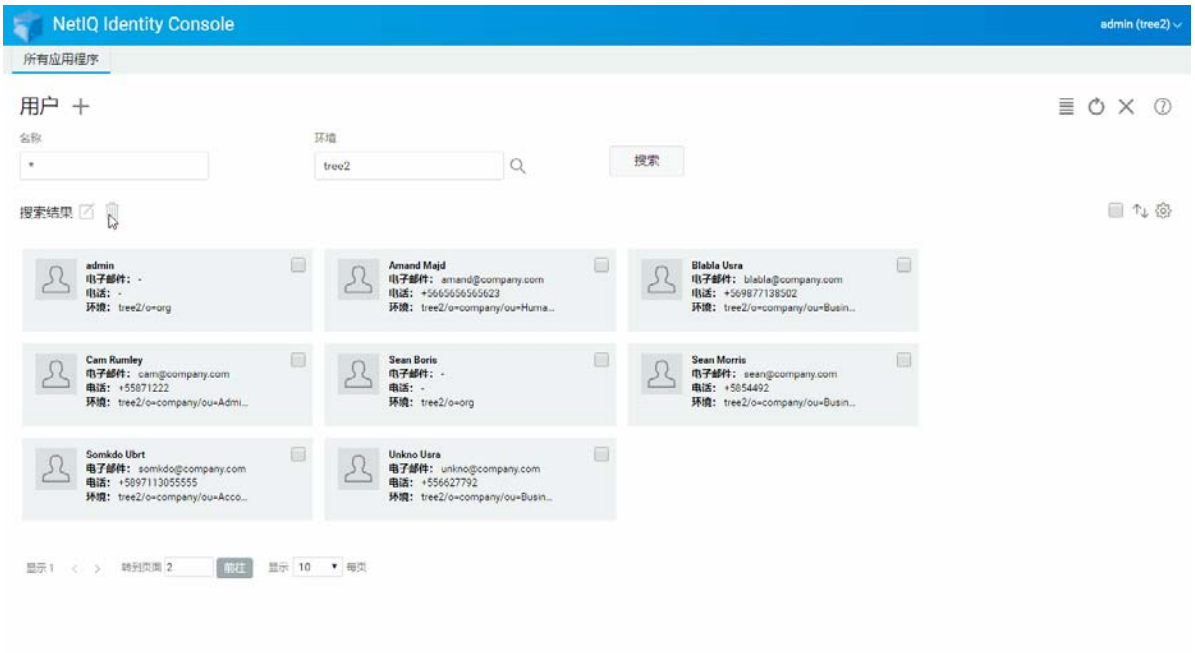


查看和清除入侵者锁定

您可以通过 Identity Console Web 门户查看任意用户帐户的入侵者锁定细节。要查看入侵者锁定细节：

1. 选择要查看其入侵者锁定细节的用户，单击 ☑ 图标。
2. 单击修改用户页中的限制选项卡。
3. 展开入侵者锁定选项卡，查看入侵者锁定细节。
4. 选择清除锁定选项卡，单击 清除锁定 按钮。
5. 单击 保存 按钮。

图5-8 查看和清除入侵者锁定



6 管理组

组通常包含一些成员。任何创建组的用户都会自动成为该组的拥有者。使用 " 组管理 " 功能可以执行下列操作：

有关使用和配置组对象的更多信息，请参见 *《NetIQ eDirectory 9.2 管理指南》*(https://www.netiq.com/documentation/edirectory-92/edir_admin/data/bookinfo.html)。

创建组

要创建组，请执行下列操作：

1 在 Identity Console 登录页中单击**组管理**选项。

2 单击 ＋ 图标。

3 在 " 创建组 " 页中输入下列细节：

- 指定组名
- 指定环境

选择**动态组**，使新组成为 dynamicGroup 类的动态组。否则，组将创建为静态组。

选择**嵌套组**，以将新组设为嵌套组，这样将使用辅助类 nestedGroupAux 创建该组。

注释：您可以使用 修改对象 中提到的过程将静态组转换为动态组或嵌套组。这可以将所选组对象进一步划分为属于 dynamicGroupAux 类或 nestedGroupAux 类。

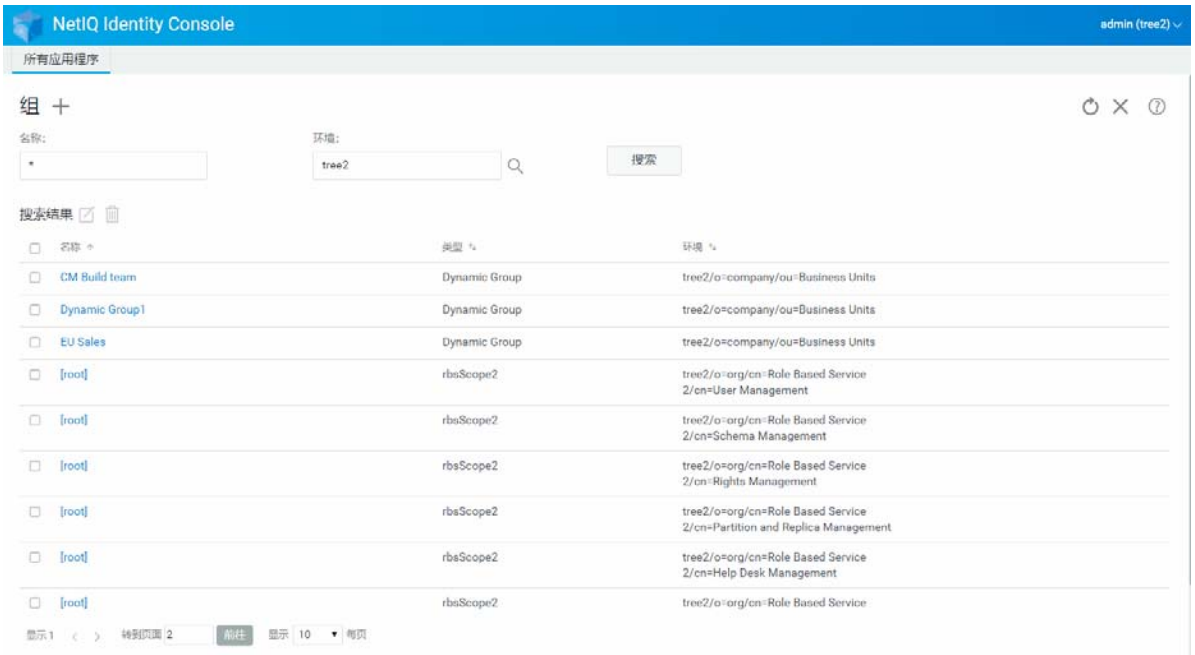
组可以是嵌套组或动态组。无法创建既是嵌套组又是动态组的组。

---

4 指定必要细节后，单击 创建 按钮。

5 此时显示一条确认讯息，指示已创建组。

图 6-1 创建组



删除组

要删除组：

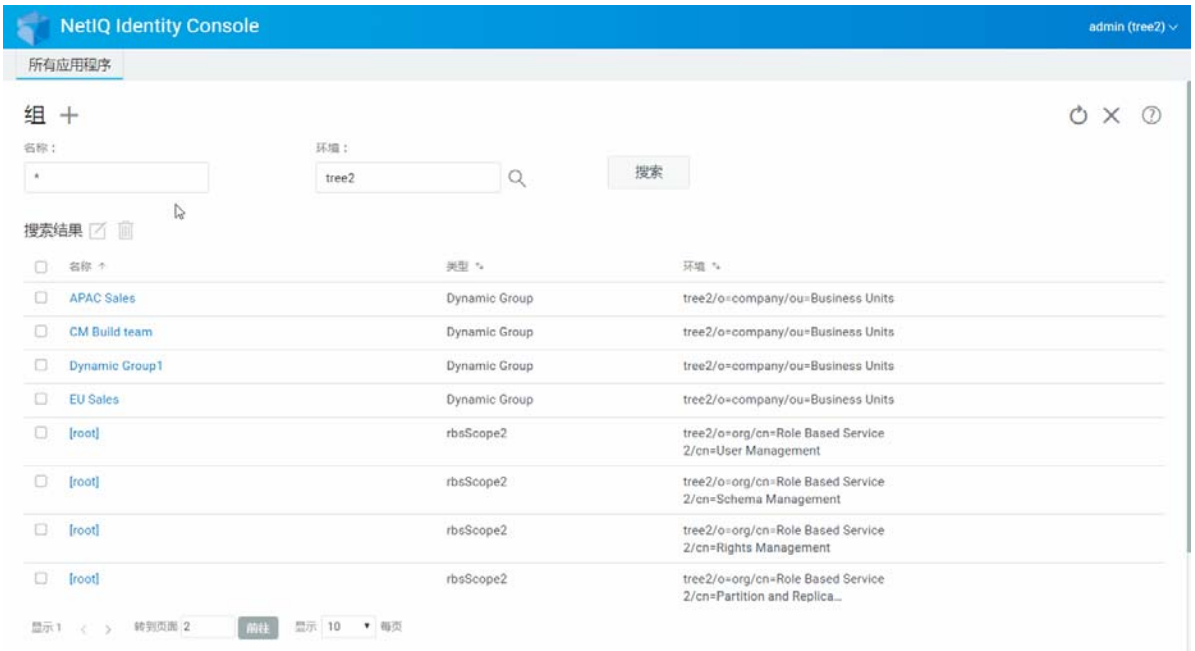
1 在 Identity Console 登录页中单击组管理选项。

2 指定组名称和环境，或使用搜索功能查找属性，然后单击 搜索 按钮。

3 选择要删除的组并单击 🗑 图标。

4 此时显示一条确认讯息，指示已删除组。

图 6-2 删除组



修改组

要修改组：

1 在 Identity Console 登录页中单击组管理选项。

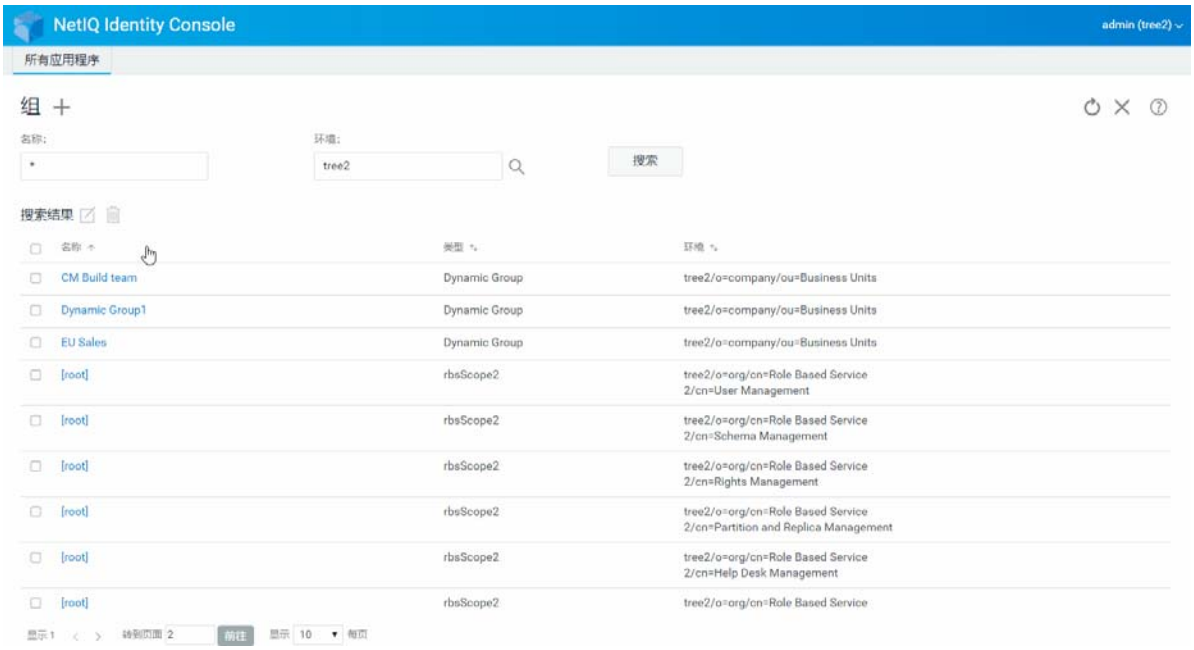
2 键入组名称及环境，然后单击 搜索 按钮。

3 选择要修改的组并单击 图标。

4 做更改，然后单击 保存 按钮。

5 此时显示一条确认讯息，指示已对组进行修改。

图6-3 修改组



添加或修改组成员

要添加或修改组成员：

1 在 Identity Console 登录页中单击组管理选项。

2 键入组名称及环境，然后单击 搜索 按钮。

3 选择组并单击 图标。

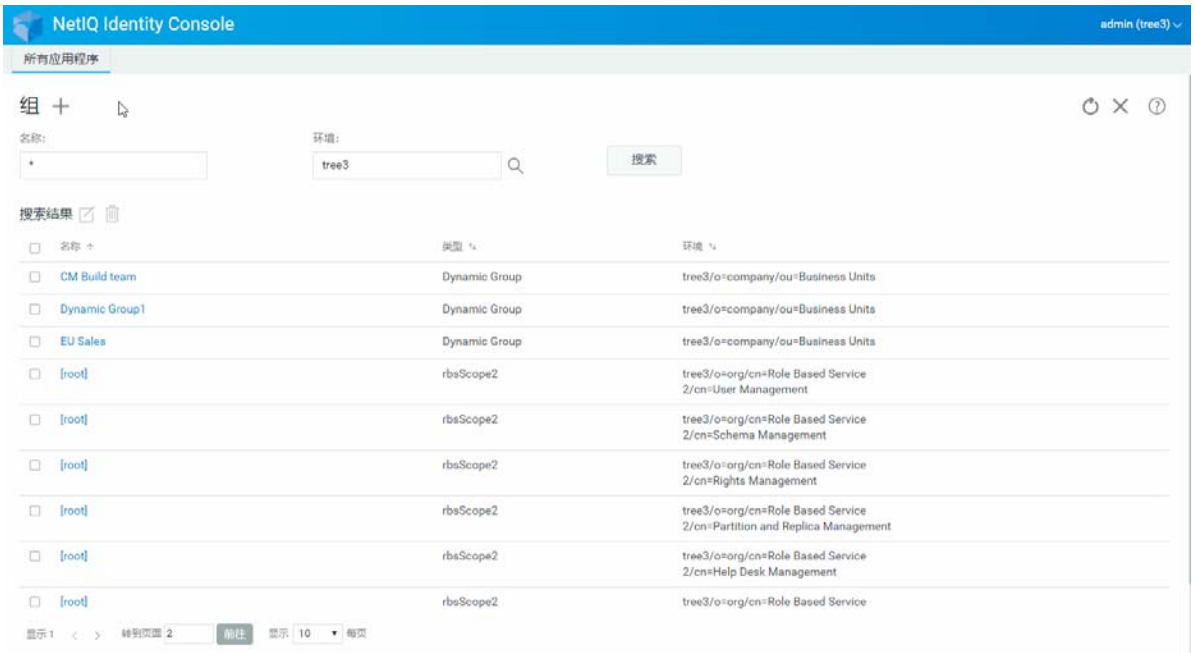
4 单击修改组页中的成员选项卡。

5 使用 图标向组添加新成员。如果想要从组中去除成员，单击 图标。

6 做出更改后，单击 保存 按钮。

7 此时显示一条确认讯息，指示已对组进行修改。

图 6-4 添加或修改组成员



搜索组

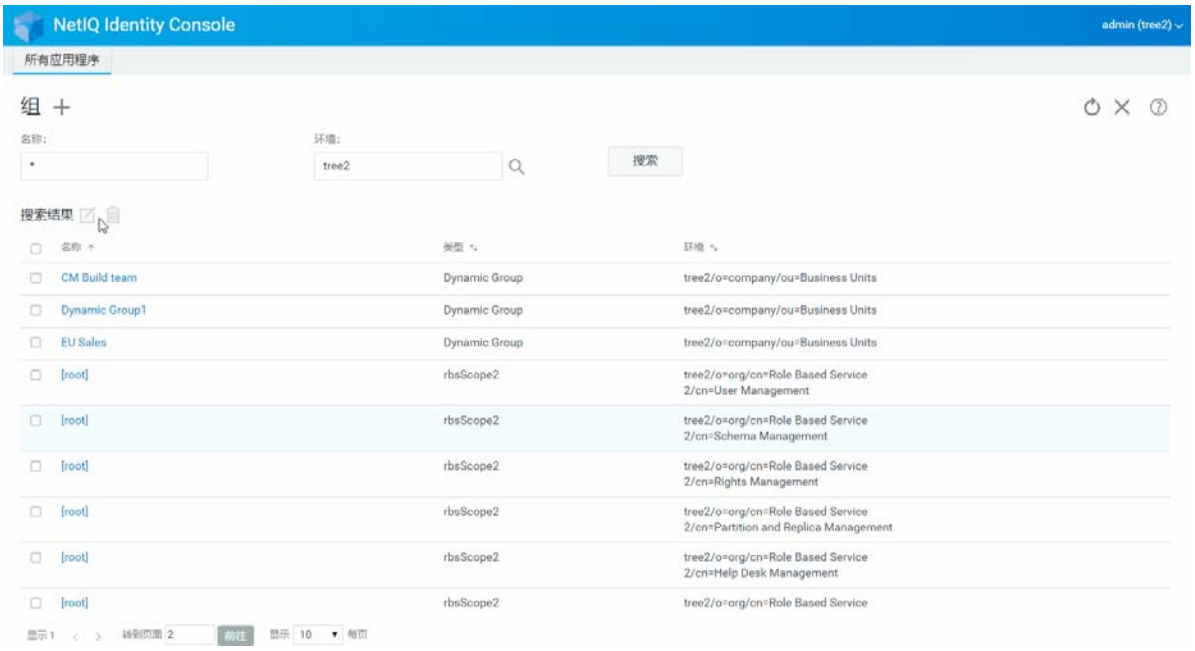
要搜索组：

1 在 Identity Console 登录页中单击组管理选项。

2 按组名称或按名称和环境搜索组。

3 指定必要细节后，单击 搜索 图标。

图6-5 搜索组


NetIQ Identity Console
admin (tree2)
所有应用程序
组
名称:
*
环境:
tree2
搜索
搜索结果
名称
类型
环境
CM Build team
Dynamic Group
tree2/o=company/ou=Business Units
Dynamic Group1
Dynamic Group
tree2/o=company/ou=Business Units
EU Sales
Dynamic Group
tree2/o=company/ou=Business Units
[root]
rbsScope2
tree2/o=org/cn=Role Based Service 2/cn=User Management
[root]
rbsScope2
tree2/o=org/cn=Role Based Service 2/cn=Schema Management
[root]
rbsScope2
tree2/o=org/cn=Role Based Service 2/cn=Rights Management
[root]
rbsScope2
tree2/o=org/cn=Role Based Service 2/cn=Partition and Replica Management
[root]
rbsScope2
tree2/o=org/cn=Role Based Service 2/cn=Help Desk Management
[root]
rbsScope2
tree2/o=org/cn=Role Based Service
显示 1
转到页面 2
前往
显示 10
每页

7 管理对象

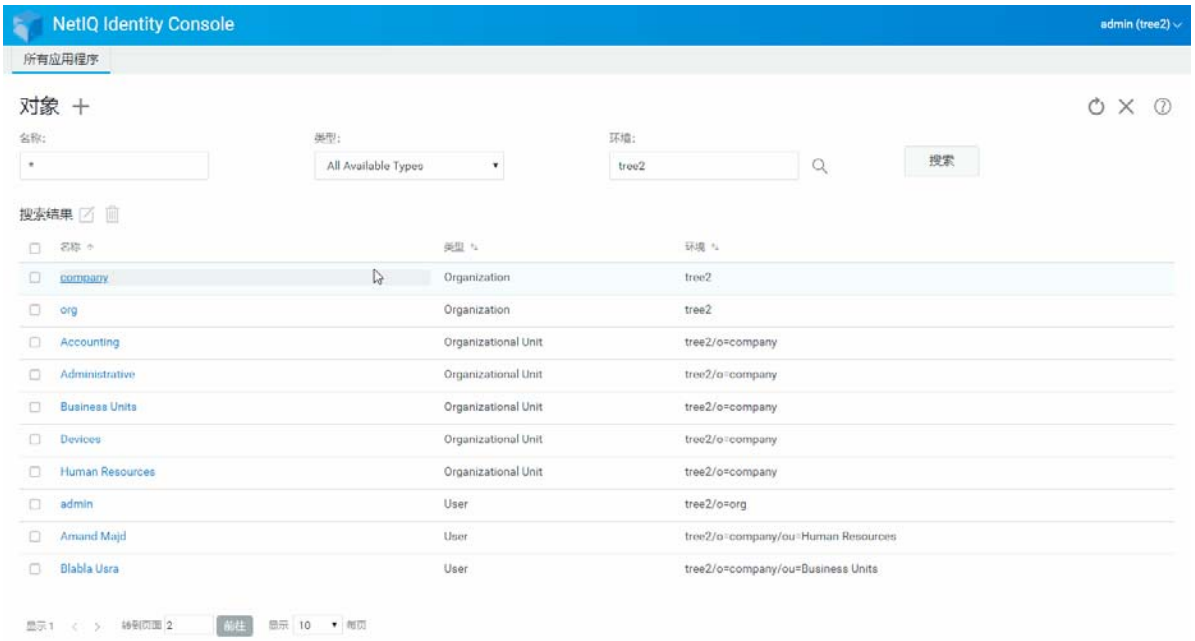
Identity Console 允许您管理数据储存库中的不同对象。使用此模块，您可以创建、修改、删除和搜索对象。

创建对象

要创建新的对象：

1. 在 Identity Console 登录页中单击**对象管理**选项。
2. 单击 + 图标。
3. 在 “ 创建对象 ” 页中输入下列细节：
   - 指定对象名称
   - 指定类型
   - 指定环境
4. 输入所有必要细节后，单击**下一步** > **创建**。
5. 此时显示一条确认讯息，指示已创建对象。

图 7-1 创建对象



删除对象

要删除对象：

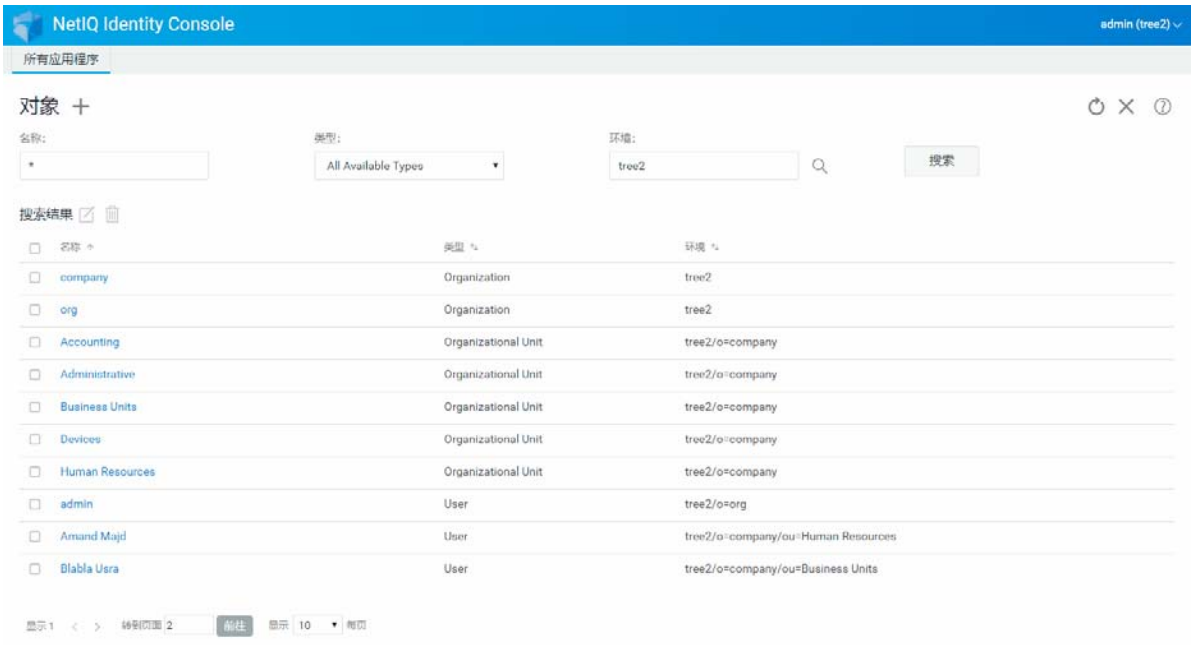
1 在 Identity Console 登录页中单击对象管理选项。

2 指定对象名称、类型和环境，或使用搜索功能查找对象，然后单击 搜索 按钮。

3 从搜索列表中选择对象并单击 图标。

4 此时显示一条确认讯息，指示已删除该对象。

图 7-2 删除对象



修改对象

要修改对象：

1 在 Identity Console 登录页中单击对象管理选项。

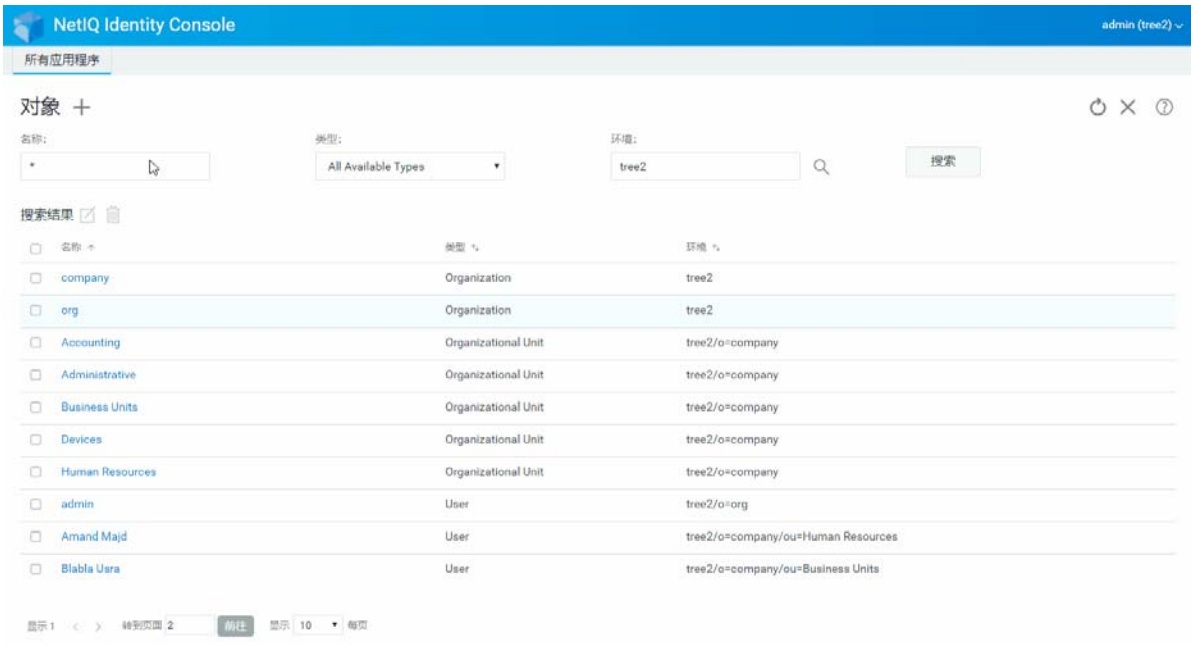
2 键入对象名称、类型和环境，然后单击 搜索 按钮。

3 从搜索列表中选择对象并单击 图标。

4 做更改，然后单击 保存 按钮。

5 此时显示一条确认讯息，指示已修改对象。

图7-3 修改对象



搜索对象

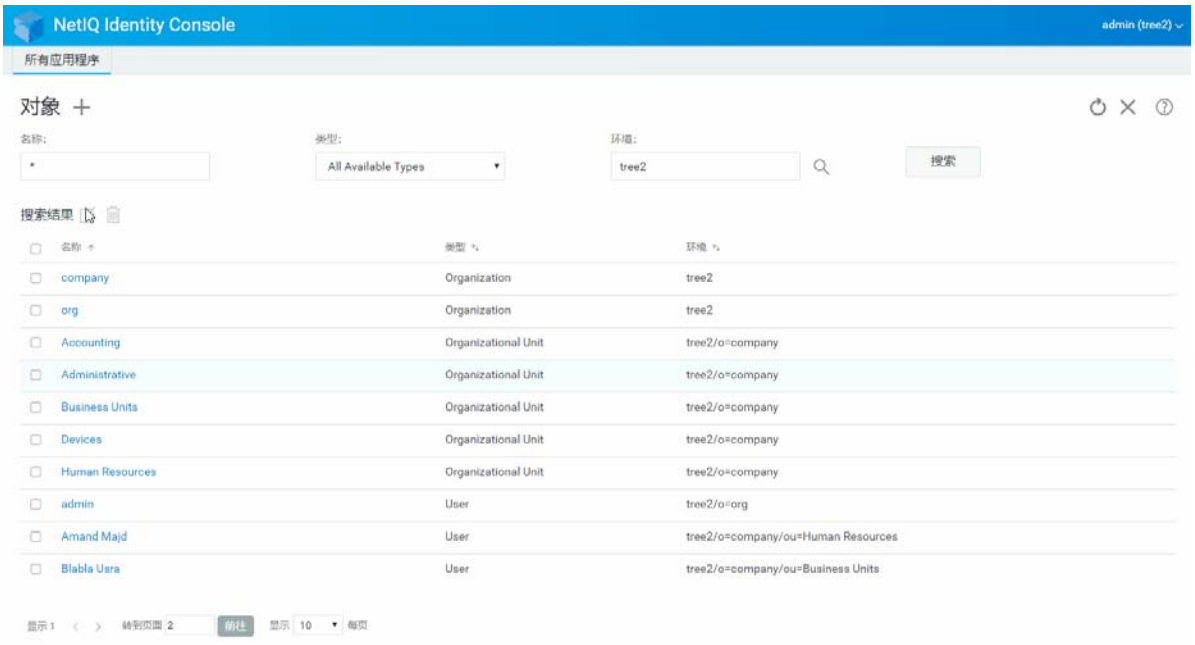
要搜索对象：

1 在 Identity Console 登录页中单击对象管理选项。

2 按对象名称或按名称、类型和环境搜索对象。

3 指定必要细节后，单击 搜索 按钮。

图 7-4 搜索对象



移动对象

要移动对象：

1 在 Identity Console 登录页中单击 **DN 管理**选项。

2 默认已选**移动对象**选项。

3 在**移至**字段中，选择要将对象移至的容器。

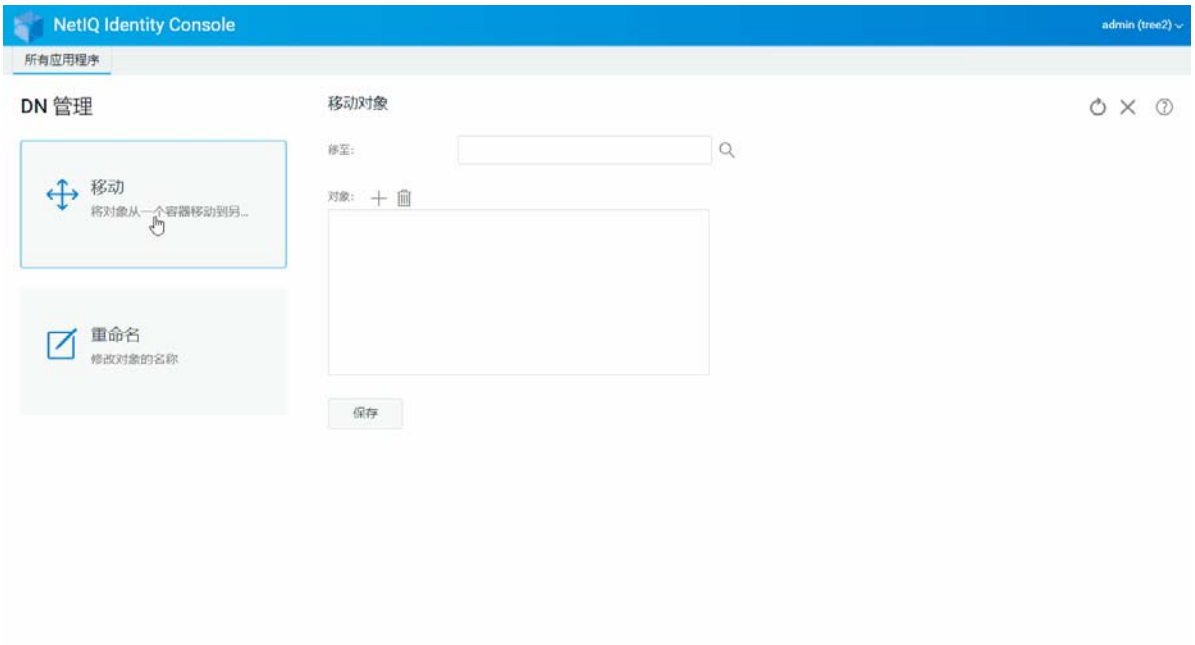
4 单击 ＋ 图标添加要移动到另一个容器中的对象。

   如果要去除所选对象，单击 🗑 图标。

5 单击 保存 按钮。

6 此时出现一条确认讯息，指示移动对象操作已成功。

图 7-5 移动对象

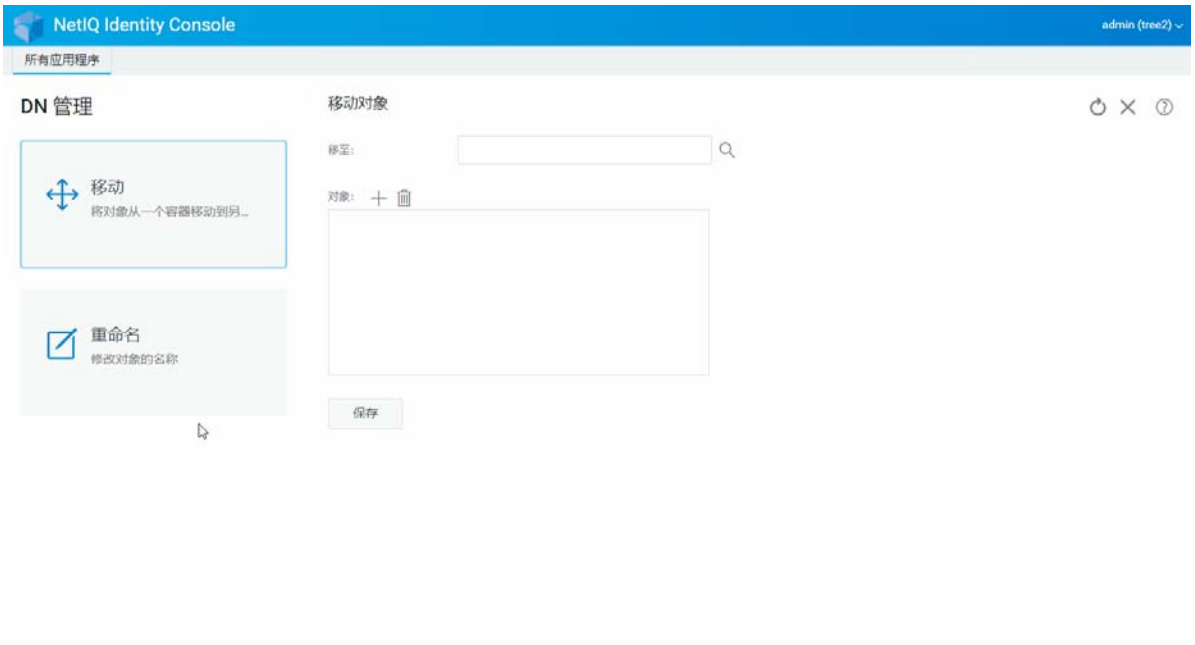


重命名对象

要重命名对象：

1 在 Identity Console 登录页中单击 **DN 管理**选项。
2 选择**重命名对象**选项。
3 使用搜索功能查找要在**对象名称**字段中重命名的对象。
4 仅在**新名称**字段中指定对象的新名称。不要指定环境。
5 如果要保存旧名称，请选择以保存。
6 单击 保存 按钮。
7 此时显示一条确认讯息，指示重命名对象操作已成功。

图 7-6 重命名对象


NetIQ Identity Console
admin (tree2)
所有应用程序
DN 管理
移动对象
移动
将对象从一个容器移动到另...
重命名
修改对象的名称
移至:
对象:
保存

8 管理权限

权限是指 eDirectory 受托者权限和受托者。创建一棵树后，默认的权限指派会为网络提供一般的访问权限和安全性。 Identity Console 允许您执行下列与权限有关的任务：

- 修改继承权限过滤器 （第 47 页）
- 修改受托者权限 （第 48 页）
- 查看有效权限 （第 49 页）

有关 eDirectory 权限的更多信息，请参见 *《NetIQ eDirectory 9.2 管理指南》*(https://www.netiq.com/documentation/edirectory-92/edir_admin/data/bookinfo.html)。

修改继承权限过滤器

eDirectory 提供继承权限过滤器 (IRF) 机制，阻止单个从属项目的权限继承。

有关继承权限过滤器的更多信息，请参见 *《NetIQ eDirectory 9.2 管理指南》*(https://www.netiq.com/documentation/edirectory-92/edir_admin/data/bookinfo.html)。

1 在 Identity Console 登录页中单击**权限管理**选项。

2 选择**继承权限过滤器**。

注释：默认选择继承权限过滤器。

---

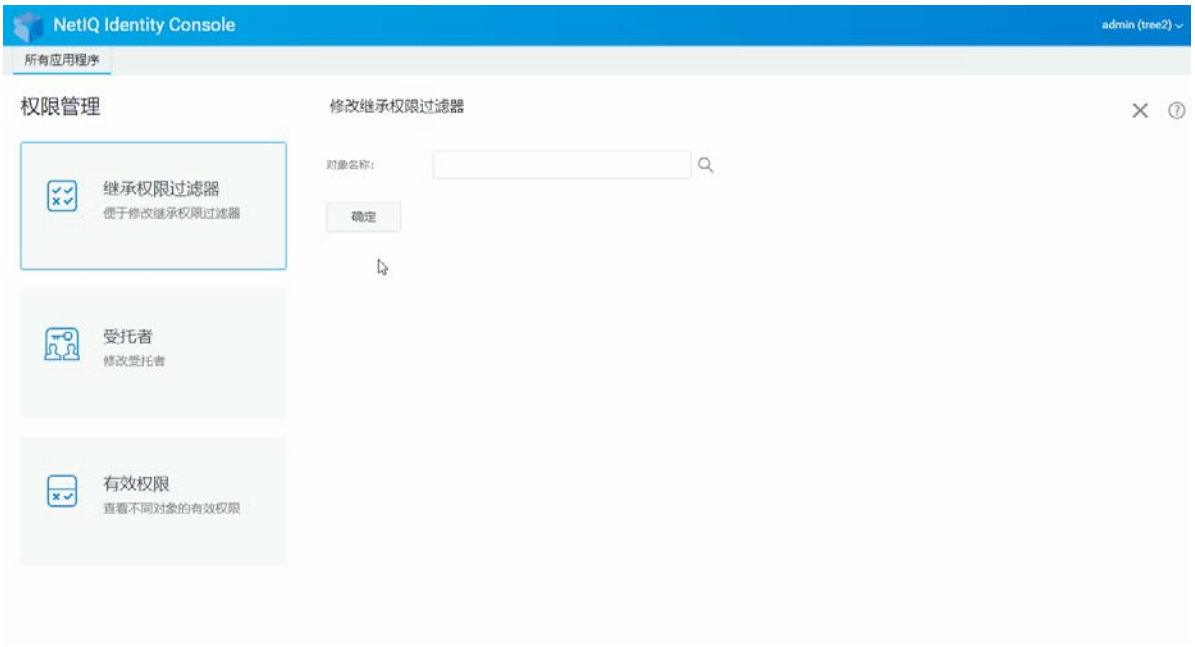
3 指定要修改其继承权限过滤器的对象的全名，或使用 “ 对象选择器 ” 图标查找对象，然后单击**确定**。

   将显示已在此对象上设置的继承权限过滤器列表。

4 在**属性**下，根据需要编辑继承权限过滤器列表，然后单击**应用**。

   要编辑此过滤器列表，必须对该对象的 ACL 属性具有主管或访问控制权限。可以设置过滤器阻止对以下各项的继承权限：对象整体、对象的所有属性以及对象的个别属性。

图 8-1 修改继承权限过滤器



修改受托者权限

受托者是已被授予对目录树中的另一个对象的显式权限的一个对象。修改给定对象的受托者列表：

1 在 Identity Console 登录页中单击权限管理选项。

2 选择受托者。

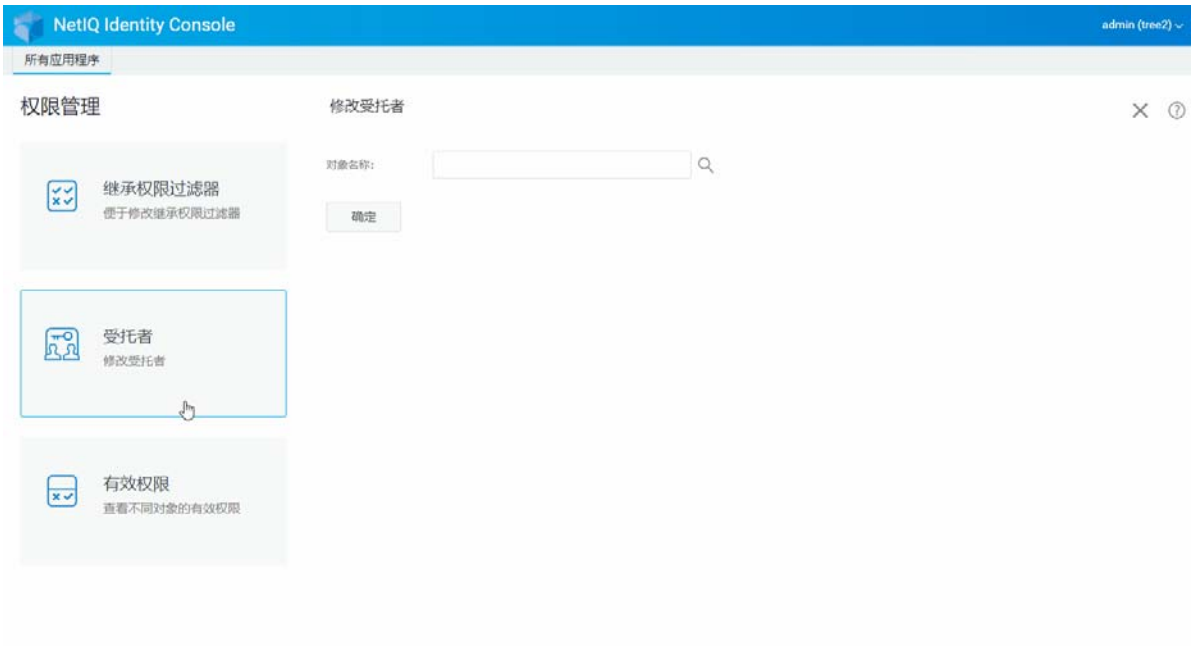
3 指定或使用 " 对象选择器 " 图标查找要查看其受托者列表的对象的名称，然后单击确定。

   此操作将打开对象当前所指派的受托者的列表。

4 根据需要修改受托者列表，然后单击 " 确定 "。

   - 单击 + 图标添加受托者。
   - 通过勾选受托者复选框并单击 图标去除受托者。
   - 通过选择受托者的指派的权限链接来修改该受托者的权限指派。

图 8-2 修改受托者权限



查看有效权限

有效权限是对象在目录树中的任意点拥有的显式权限和继承权限的组合。查看对象对其他对象的有效权限：

1 在 Identity Console 登录页中单击权限管理选项。

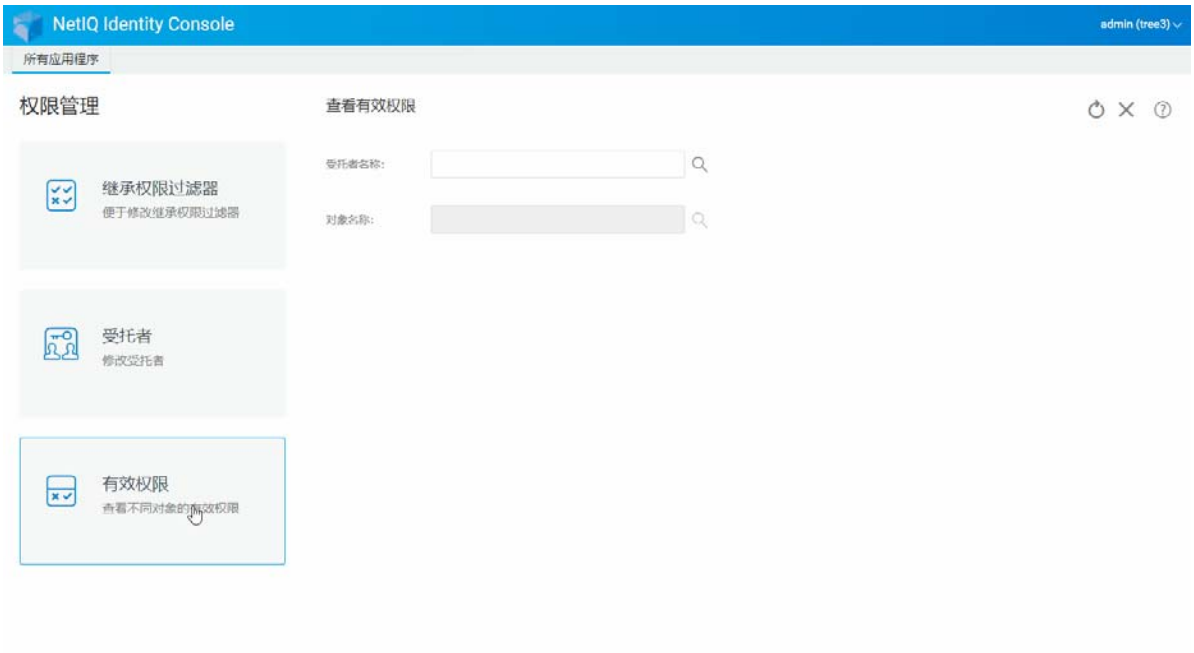
2 选择有效权限。

3 指定或使用 " 对象选择器 " 图标查找要查看其权限的受托者的名称，然后单击确定。

4 在 " 对象名 " 字段中，指定要查看其受托者有效权限的对象的名称。

eDirectory 计算有效权限并在有效权限字段中显示这些权限。

图8-3 查看有效权限


NetIQ Identity Console
admin (tree3)
所有应用程序
权限管理
查看有效权限
受托者名称:
对象名称:
继承权限过滤器
便于修改继承权限过滤器
受托者
修改受托者
有效权限
查看不同对象的有效权限

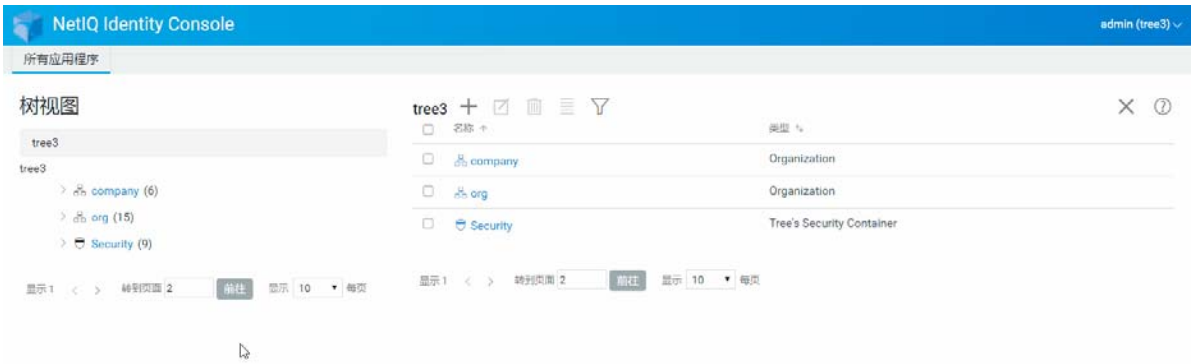
9 树视图

树视图允许您浏览目录树，在该树中创建、删除和修改各种对象。树视图具有导航框架和内容框架。

树视图的导航框架

在树视图中，导航框架显示目录结构。导航框架显示容器，包括卷 （文件系统）、对象等。导航框架下显示的所有选项都可单击，帮您浏览目录结构。默认情况下，每个容器的导航框架最多显示 10 个从属对象，但您可以在树视图的导航框架面板下方更改此设置。

图 9-1 树视图中的导航框架



树视图的内容框架

如果在导航框架中选择一个容器对象，会使内容框架显示该容器中的所有对象。通过内容框架可以实际查看和修改目录对象。内容框架包含一个标题，有几个可用操作：

标题栏：内容框架的标题栏显示当前所选的容器对象的名称。

对象列表标题：通过对象列表标题可以访问下列内容：

- 添加：单击 + 图标可以添加新对象。
- 修改：选择对象并单击 图标进行修改。此操作将打开所选对象的属性簿，方便您修改其属性。不能一次修改多个对象。

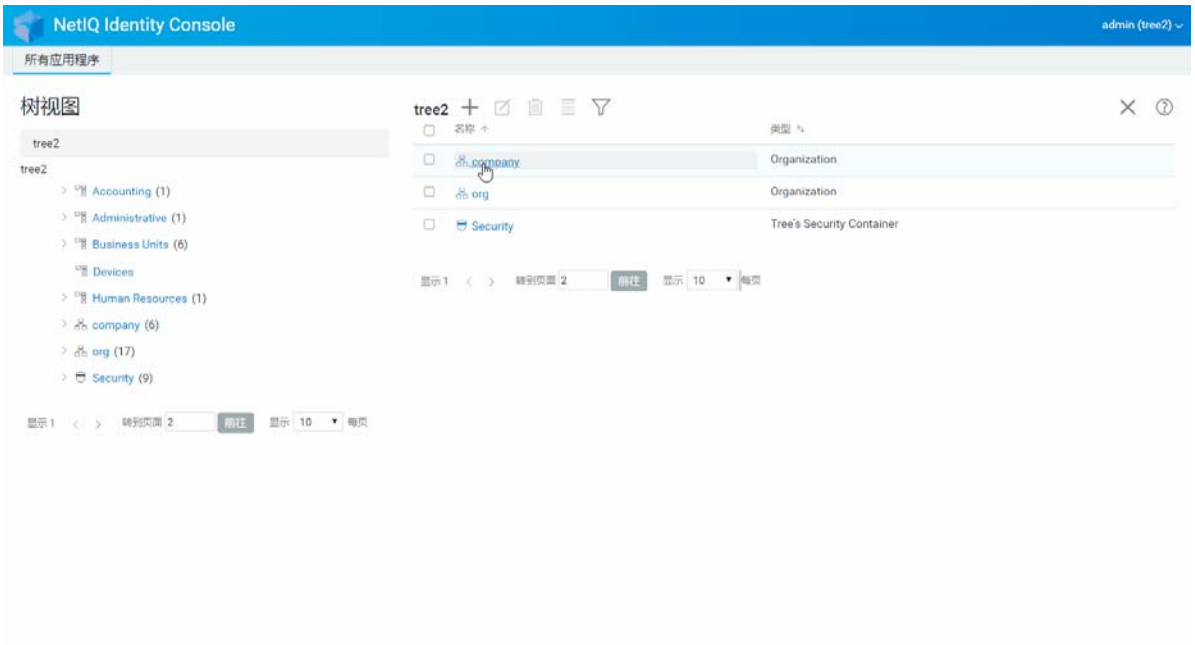
- 删除：选择对象并单击 图标删除所选对象。可以同时删除多个对象。无法删除非叶对象。
- 操作：选择对象并单击 图标，将打开所选对象支持的任务下拉菜单。要执行某项任务，请从下拉菜单中选择该任务，并提供所需的信息。
- 对象计数：树视图在页面底部列出当前页面中的对象数量。默认情况下，针对每个容器，内容框架最多显示 20 个从属对象，但可更改此设置。
- 全选：标题中的复选框用作当前对象页的“全选”复选框。
- 排序：名称和类型列都可排序。单击任意一项可以在字母的升序和降序之间转换对象排序方式。
- 搜索过滤器：单击 。图标起动过滤器弹出窗口。您可以用此选项创建过滤器，限制对象列表中显示的对象。根据需要，您可以按照对象类型和对象名称进行过滤。

  选择 选项打开“高级过滤器”对话框，使用任意对象属性创建过滤器。有关详细信息，请参见 配置高级搜索 （第 24 页）。

要对对象执行操作，勾选其复选框，然后在“对象列表”标题中选择操作图标 。选择（当前级别的）对象可对当前浏览的容器执行操作。使用此操作可以执行下列操作：

- 修改继承权限过滤器 （第 47 页）
- 修改受托者权限 （第 48 页）
- 扩展对象 （第 60 页）
- 重命名对象 （第 44 页）
- 设置口令
- 查看有效权限 （第 49 页）

图 9-2 树视图中的内容框架



10 管理纲要

目录纲要定义了可在树中创建的对象类型 （例如用户、打印机、组等）以及创建对象时的必要和可选信息。 Identity Console 提供下列纲要相关任务：

创建属性

您可以定义属性的自定义类型，并将它们作为可选属性添加到现有对象类中。但是，不能为现有类添加必需的属性。创建属性 :

1. 在 Identity Console 登录页中单击纲要管理选项。
2. 单击 + 图标。
3. 在 “ 创建属性 ” 页中输入下列细节：
   - 属性名称
   - ASN1 ID （可选）
   - 语法
   - 属性标志
4. 输入所有必要细节后，单击 创建 按钮。
5. 此时显示一条确认讯息，指示已创建属性。

图 10-1 创建属性

创建类

使用纲要管理选项可以定义自己的类。然后可使用类中定义的属性来扩展各个对象。要创建类：

1 在 Identity Console 登录页中单击纲要管理选项并选择类。

2 单击 ＋ 图标。

3 在 “ 创建属性 ” 页中输入下列细节：

- 类名
- ASN1 ID （可选）
- 类标志：选择下列任意类标志：
  - **有效类：**如果想创建有效类，设置此标志，有效类可用于创建对象。
  - **无效类：**用作一组属性的占位符。无效类不能用来创建对象，但可以指定作为其它类继承属性的来源类。例如，“ 人员 ” 类是无效类，它包含 “ 用户 ” 类所继承的属性。
  - **辅助类：**只能与单个对象 （而非整个类）关联的属性集合。
  - **容器类：**如果要使其成为容器类，可设置此标志。当使用它创建对象时，这些对象会成为容器对象 （如 OU）。不要为叶对象类设置该标志。

注释：如果您选择有效类和无效类，您还必须为超级类指定值。如果选择 “ 辅助类 ”，“ 超级类 ” 为可选。

---

4 输入所有必要细节后，单击下一步。

5 在接下来显示的屏幕中，选择可选、强制和命名属性并单击确定。

6 此时显示一条确认讯息，指示已创建类。

为类指派属性

如果组织的信息需要更改或您准备合并树，可以为现有类添加可选属性。为现有类添加属性：

注释：强制属性只能在创建类时定义。必备特性是指在创建对象时必须完成的特性。

---

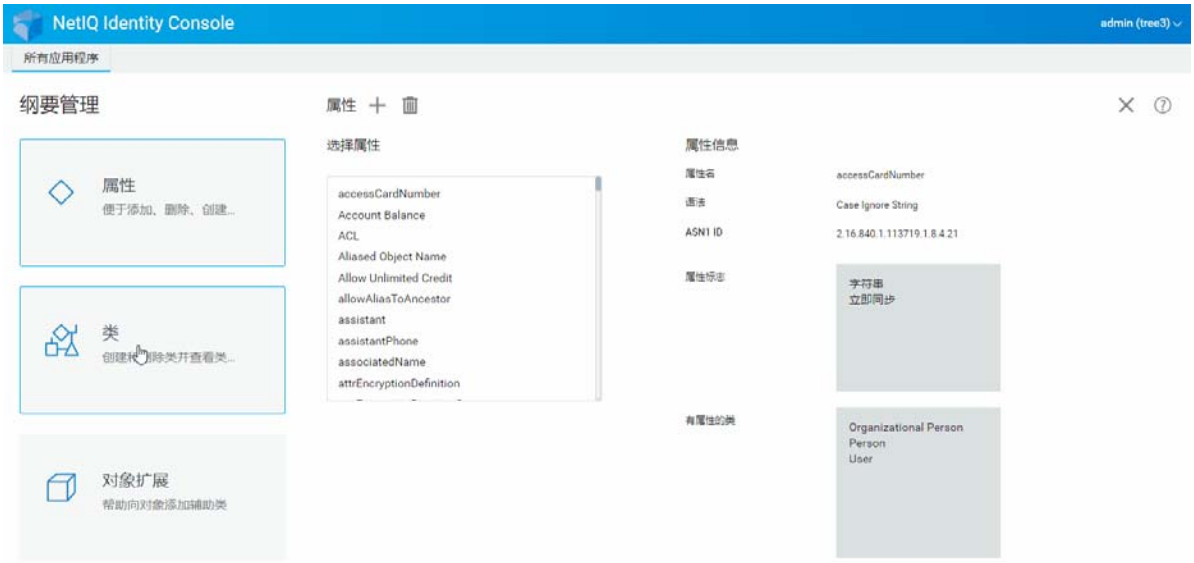
1 在 Identity Console 登录页中单击纲要管理选项并选择类。

2 单击选择类下列出的任意类。

3 屏幕右侧显示相应类信息。

4 单击 + 属性选项旁的 按钮，选择要添加的属性，单击添加 > 保存。

图 10-2 为类指派属性



查看属性信息

可以查看属性的结构细节，例如其语法、标志和使用该属性的类。查看属性的信息：

1 在 Identity Console 登录页中单击纲要管理选项并选择属性。

2 单击选择属性下列出的任意属性。

3 屏幕右侧显示相应属性信息。

图 10-3 查看属性信息

删除属性

如果未使用的特性不属于 eDirectory 树的基本纲要，可将其删除。在合并两个目录树之后，或在属性随着时间推移而过时的情况下，此操作可能会有用。要删除属性：

1 在 Identity Console 登录页中单击纲要管理选项并选择属性。

2 在选择属性列表下选择要删除的属性，单击 图标。

注释：仅当您选择可以删除的属性时，才会启用 图标。

---

3 单击确定以确认删除。

图 10-4 删除属性

删除类

如果未使用的类不属于 eDirectory 树的基本纲要，可将其删除。Identity Console 禁止删除当前在本地复制的分区中正在使用的类。要删除类：

1 在 Identity Console 登录页中单击纲要管理选项并选择类。

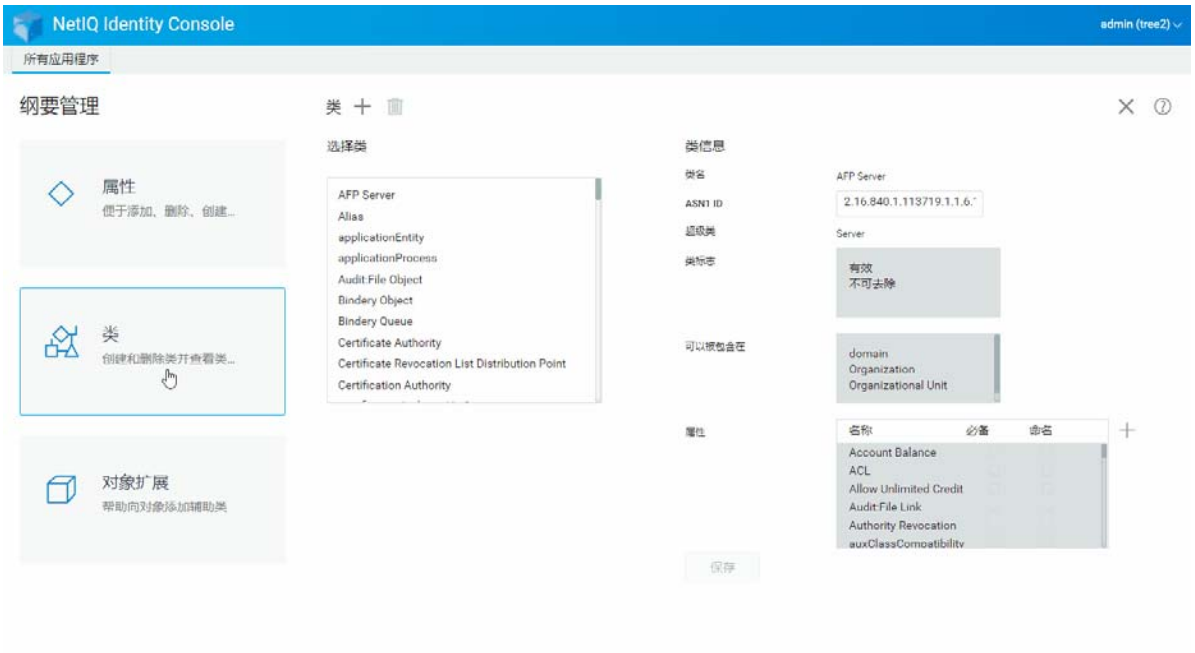
2 在选择类列表下选择要删除的类，单击 图标。

注释：仅当您选择可以删除的类时，才会启用 图标。

---

3 单击确定以确认删除。

图 10-5 删除类



扩展对象

执行下列操作扩展对象：

1 在 Identity Console 登录页中单击纲要管理选项并选择对象扩展。

2 指定对象名称或使用对象选择器选择要扩展的对象，单击 图标。

3 单击 图标，选择附属类，然后单击确定。

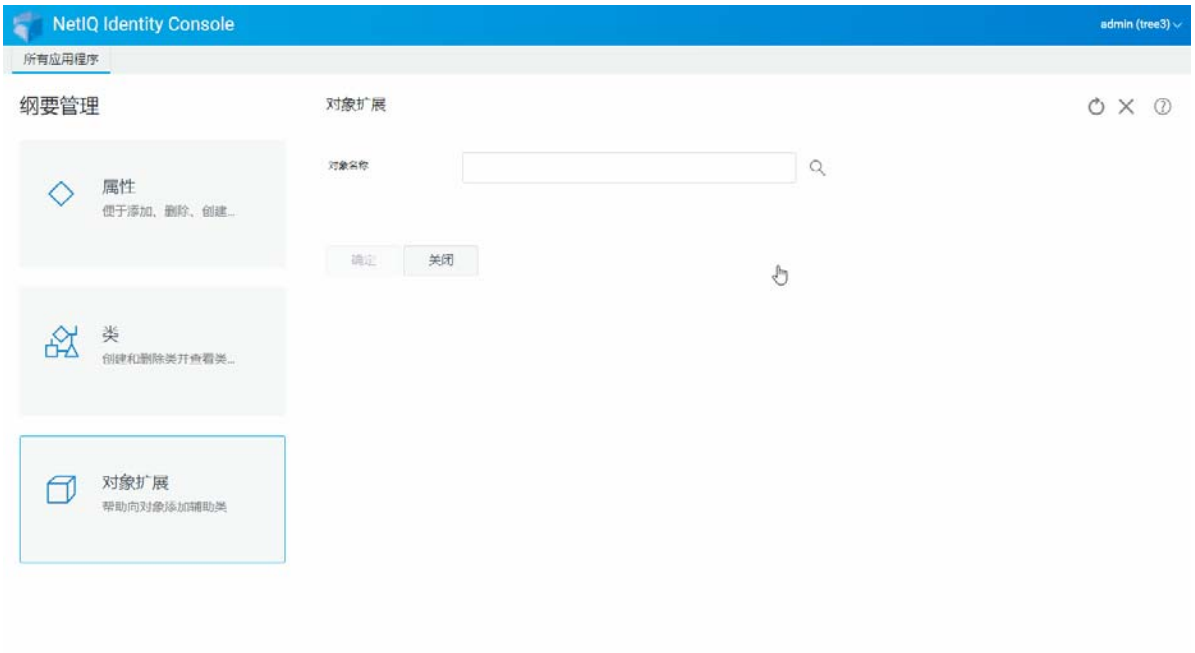
注释：如果所选辅助类附加了强制属性，那么系统将提示您在强制属性弹出窗口中输入所需的值。

---

4 此时显示一条确认讯息，指示已将辅助类添加到对象。

5 要从对象去除现有辅助类，选择类并单击 图标。

图 10-6 扩展对象


NetIQ Identity Console
admin (tree3)
所有应用程序
纲要管理
对象扩展
属性
便于添加、删除、创建...
类
创建和删除类并查看类...
对象扩展
帮助向对象添加辅助类
对象名称
确定
关闭

11 管理审计事件

本章介绍如何用 Identity Console 管理各种审计事件。利用这一功能可以为 NCP 服务器启用或禁用审计事件。

配置 CEF 审计事件

1 用您的用户名和口令登录 Identity Console。

2 选择审计。

3 选择要监视的 NCP 服务器，然后单击确定。

注释：首次为任意 NCP 服务器启用 CEF 事件后，默认会选择少量事件。

---

4 配置 CEF 审计事件：

- **事件配置：**根据环境所需审计启用或禁用下列事件：

注释：默认会折叠事件配置部分下的单个事件类别。可以展开每个类别，选择单个事件。

选项	说明
安全事件	选择要为其记录事件的安全事件。可以记录事件以添加或删除成员、检测入侵者、更改口令或鉴定用户等。
对象事件	选择要为其记录事件的对象事件。可以记录创建、删除、重命名、移动和搜索对象的事件。
属性事件	选择要为其记录事件的属性事件。您可以记录事件以读取和删除属性，添加、删除和比较属性值。
LDAP 事件	选择要为其记录事件的 LDAP 事件。

- **高级设置：**使用高级设置，您可以执行以下操作。
  - **全局：**您可以选择或清除重复项的全局设置。
    - **不发送复制的事件：**选择此选项停止接收从其他服务器复制的重复事件。
  - **日志事件值：**事件记录在文本文件中。大小超过 768 字节的事件值将被视为 “大值 ”。您可以记录任意大小的事件。
    - **记录大值：**选择此选项记录大小超过 768 字节的事件。

- **日志属性值：**选择此选项以显示属性值。这仅适用于添加值和删除值事件。
- **记录加密属性值：**选择此选项以显示已加密的属性值。这仅适用于添加值和删除值事件。

注释：如果事件大小超过 768 字节，事件值会被截断并保存到日志文件中。

了解 CEF 事件类型

您可以配置 CEF 记录下列类别的事件：

- 安全性
- 对象
- 属性
- LDAP

您可以审计下列默认事件类型：

类别	事件类型
安全性	◆ ACL 已更改 ◆ 添加成员 ◆ 删除成员 ◆ 检测到入侵者 ◆ 登录已禁用 ◆ 登录已启用 ◆ 登录 ◆ 更改安全性等于 ◆ 审计配置 ◆ 更改口令 ◆ 帐户解除锁定 ◆ 注销 ◆ 连接 ◆ 模拟 ◆ 鉴定 ◆ 校验口令 ◆ 更改登录配置 ◆ 查询身份凭证

类别	事件类型
对象	◆ 创建对象 ◆ 删除对象 ◆ 重命名对象 ◆ 移动对象 ◆ DSA 读取 ◆ 搜索
属性	◆ 读取属性 ◆ 删除特性 ◆ 添加值 ◆ 删除值 ◆ 比较属性值
LDAP	◆ LDAP 绑定 ◆ LDAP 绑定响应 ◆ LDAP 取消绑定 ◆ LDAP 连接 ◆ LDAP 搜索 ◆ LDAP 搜索响应 ◆ LDAP 搜索项响应 ◆ LDAP 添加 ◆ LDAP 添加响应 ◆ LDAP 比较 ◆ LDAP 比较响应 ◆ LDAP 修改 ◆ LDAP 修改响应 ◆ LDAP 删除 ◆ LDAP 删除响应 ◆ LDAP 修改 DN ◆ LDAP 修改 DN 响应 ◆ LDAP 丢弃 ◆ LDAP 扩展操作 ◆ LDAP 系统扩展操作 ◆ LDAP 扩展操作响应 ◆ 修改 LDAP 服务器配置 ◆ 未知 LDAP 操作 ◆ LDAP 口令修改

配置 CEF 审计过滤

CEF 使用过滤器和事件通知，可以在发生或未发生特定类型事件时进行报告。您还可以根据事件类型，为一个或多个特定对象类或属性过滤事件。CEF 根据 eDirectory 服务器中配置的过滤器评估所有生成的事件，并仅记录与那些过滤器匹配的事件。

本部分介绍配置系统过滤器和通知所需的信息。

用排除项过滤器过滤 eDirectory 事件

单击**排除项过滤器**链接为不希望生成任何事件的那些对象类或属性配置过滤。您可以选择对象类和属性。

要为不想要的 eDirectory 事件配置过滤：

1. 在 Identity Console 中，从主页选择**审计**。
2. 选择要监视的 NCP 服务器，然后单击**确定**。
3. 转到**高级设置**，单击**过滤器**下的**排除项过滤器**。

   随即显示 CEF 排除项过滤窗口。
4. 在**可用对象类**列表中，选择不想收集其事件的对象类，然后单击右箭头，将其移动到**所选对象类**列表中。
5. 在**可用属性**列表中，选择任意数量的属性。选择属性并单击右箭头将属性添加到选定的属性列表中。
6. 单击**确定**。

使用配置的过滤器， CEF 审计模块将停止为所有选择的对象类和属性生成事件。

过滤 CEF 对象事件

您可以为配置对象过滤，以仅查找特定的一个或多个事件。例如，如果希望当有人在 eDirectory 中创建用户帐户时得到通知，可以创建过滤器，选择 “ 用户对象 ” 类为创建新用户对象记录事件。

要配置帐户过滤，单击 “ 对象事件 ” 链接，选择类，然后单击**确定**退出应用程序。

要为 “ 帐户管理 ” 事件配置过滤器：

1. 在 Identity Console 中，从主页选择**审计**。
2. 选择要监视的 NCP 服务器，然后单击**确定**。
3. 转到**高级设置**，单击**过滤器**下的**对象事件**。

随即显示 CEF 对象过滤窗口。

4 在可用对象类列表中，选择任意对象类，然后单击右箭头将对象类移动到所选对象类列表，然后单击确定。

使用配置的过滤器， CEF 审计模块检查为所选对象类生成的所有事件并记录这些事件。

过滤 CEF 属性事件

单击属性事件链接为属性事件配置过滤。例如，如果希望当有人在 eDirectory 中添加新属性值时得到通知，可以创建过滤器为添加新值记录事件。

要为属性事件配置过滤：

1 在 Identity Console 中，从主页选择审计。

2 选择要监视的 NCP 服务器，然后单击确定。

3 转到高级设置，单击过滤器下的属性事件。

显示属性配置过滤窗口

4 在可用对象类列表中，选择想要收集其事件的对象类，然后单击右箭头将其移动到所选对象类列表中。

5 在可用属性列表中，为所选对象类选择任意数量的属性。选择属性并单击右箭头将属性添加到选定的属性列表中。

注释：如果选择一个对象类，将选择该对象类所有属性的所有 “ 属性事件 ”。这种情况下，您将获得所选对象类所有属性的所有 “ 属性事件 ”。

---

6 单击确定。

配置过滤器后， CEF 审计模块检查为所有所选对象类和属性生成的事件并记录这些事件。

12 管理加密属性

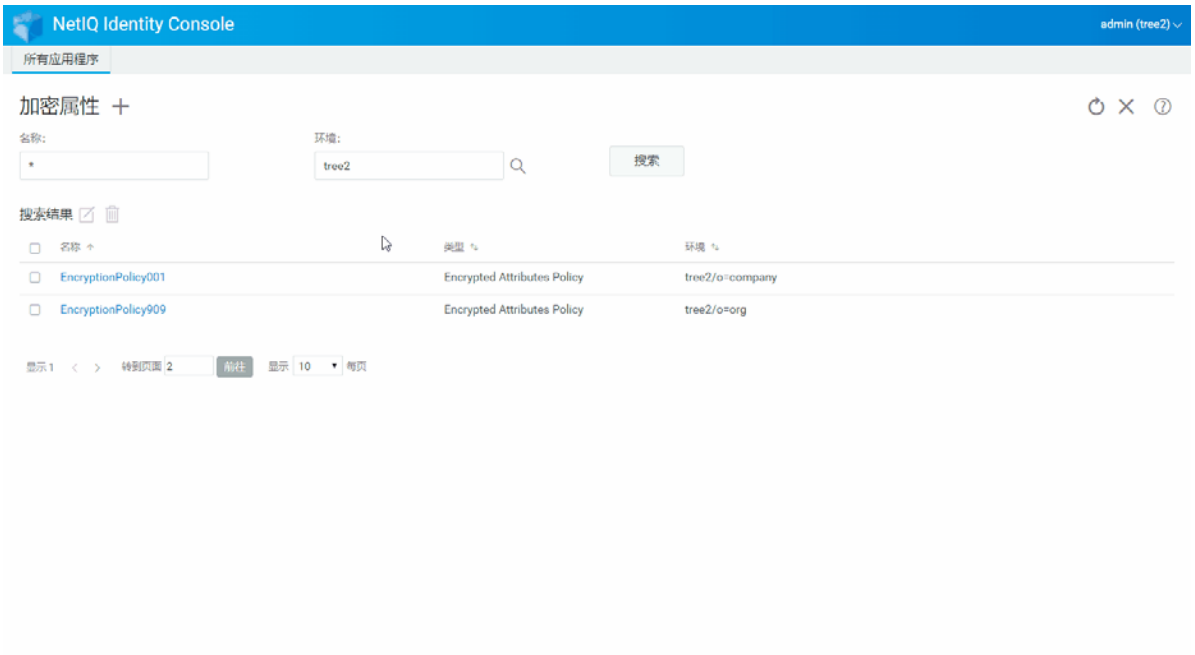
Identity Console 可以从 eDirectory 服务器安全地读取加密属性。您可以使用 Identity Console 为这些加密属性创建、修改或删除若干策略。

为加密属性创建策略

要创建新属性策略：

1. 在 Identity Console 登录页中单击加密属性选项。
2. 单击 ＋ 图标。
3. 在 “ 创建加密属性策略 ” 页中输入下列细节：
   - 指定策略名称
   - 输入或选择环境
   - 选择 NCP 服务器
   - 选择属性
4. 指定所有必需的细节后，单击完成。
5. 此时显示一条确认讯息，指示已创建策略。

图 12-1 创建加密属性策略



删除加密属性策略

要删除加密属性策略：

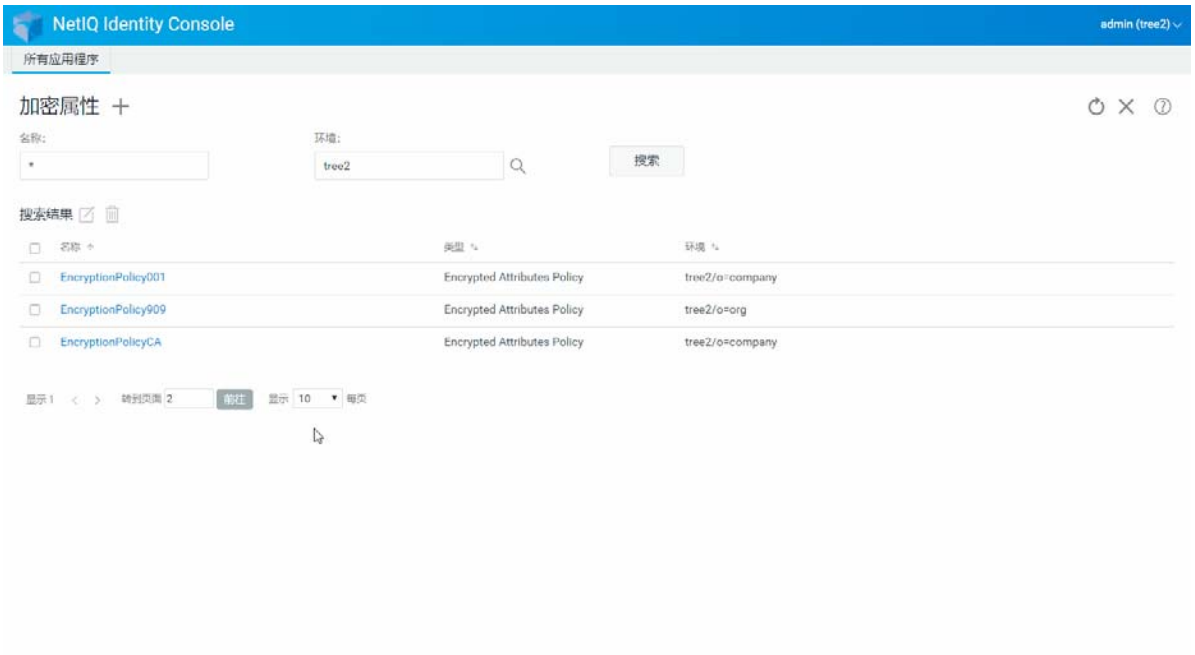
1 在 Identity Console 登录页中单击加密属性选项。

2 指定属性名称和环境，或使用搜索功能查找属性，然后单击 搜索 按钮。

3 从列表中选择属性并单击 🗑 图标。

4 此时显示一条确认讯息，指示已删除策略。

图 12-2 删除加密属性策略



修改加密属性策略

要修改加密属性策略：

1 在 Identity Console 登录页中单击加密属性选项。

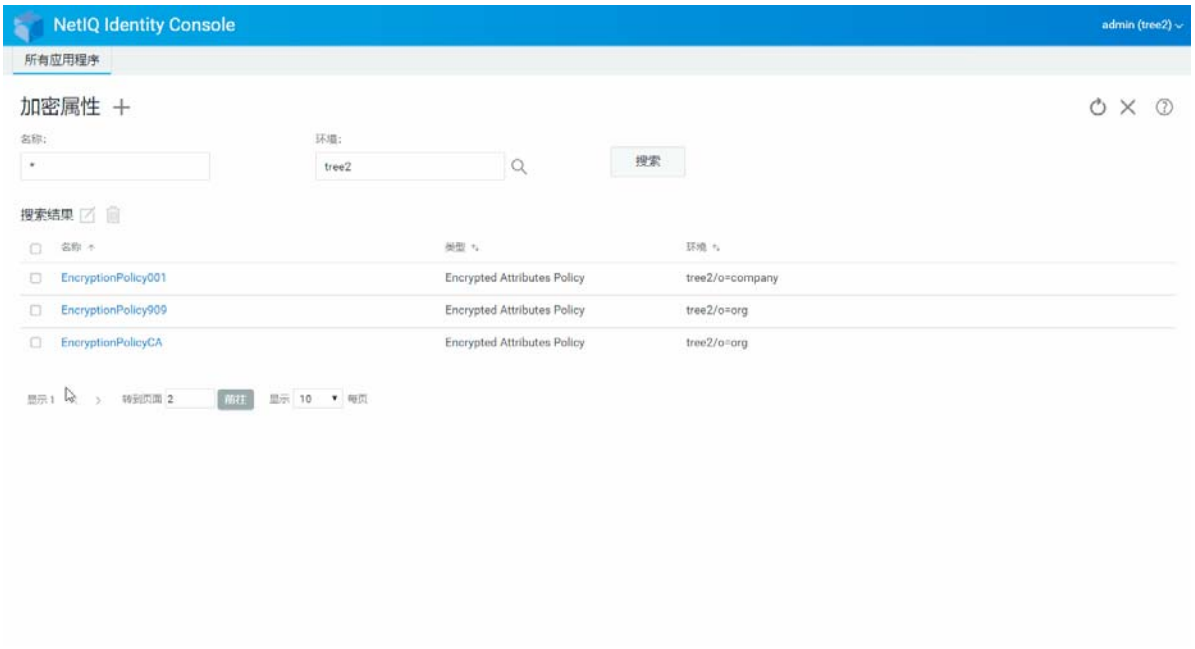
2 键入对象名称和环境，然后单击 搜索 按钮。

3 从对象列表中选择属性并单击 图标。

4 做更改，然后单击 保存 按钮。

5 此时显示一条确认讯息，指示已修改策略。

图 12-3 修改加密属性策略



13 管理加密复制

要启用加密复制，需要为加密复制配置分区。配置设置储存在分区根对象中。您只能选择在分区级别启用加密复制。在分区级别启用加密复制后，托管分区的所有副本间的复制都将加密。例如，假设分区 P1 有副本 R1、 R2、 R3 和 R4。可以对所有副本间的复制进行加密。

- 为分区启用加密复制 （第 73 页）

为分区启用加密复制

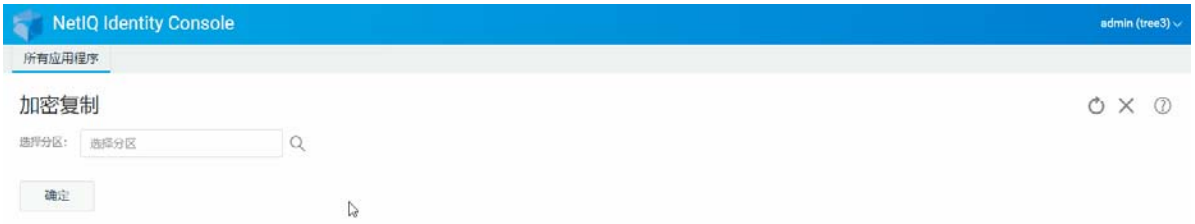
要为分区启用加密复制：

注释：要启用加密复制分区，托管分区的所有服务器必须是 eDirectory 9.2 或更高版本的服务器。

---

1. 在 Identity Console 登录页中单击加密复制选项。
2. 指定或浏览到要启用加密复制的分区。
3. 确保选择启用加密复制选项。禁用分区加密复制时，取消选择此选项。
4. 单击完成。
5. 此时显示一条确认讯息，指示已启用加密复制。

图 13-1 为分区启用加密复制



14 管理分区和复本

通过分区和复本操作可以管理 eDirectory 的物理设计以及目录服务器上的分布。

分区操作创建 eDirectory 树的逻辑分支。例如，如果选择“组织单元”并将其创建为新分区，则“组织单元”及其所有从属对象将从其父分区中分出。所选的“组织单元”成为新分区的根。新分区的复本与父分区的复本位于相同的服务器上，并且新分区中的对象属于新分区的根对象。

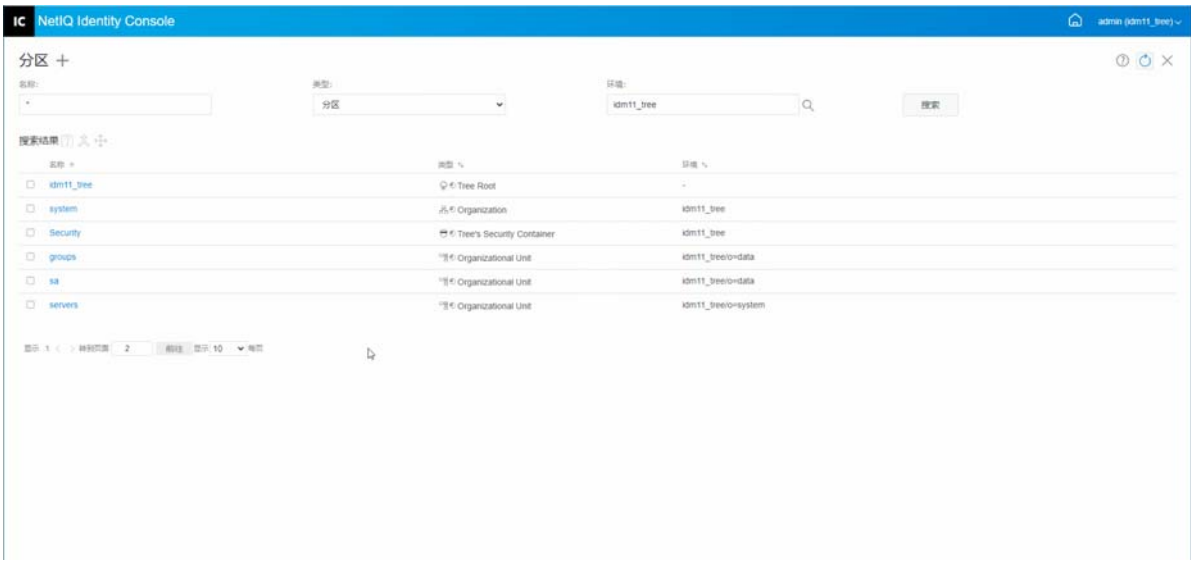
可以使用分区模块执行以下任务：

创建分区

要创建新分区：

1. 在 Identity Console 登录页中单击分区管理选项。
2. 单击 + 图标。
3. 在创建分区页面中，指定要用作新分区的根的容器，或使用对象选择器 图标查找该对象，然后单击创建。
4. 此时显示一条确认讯息，指示已创建分区。

图 14-1 创建新分区



合并分区

要将分区与其父分区合并：

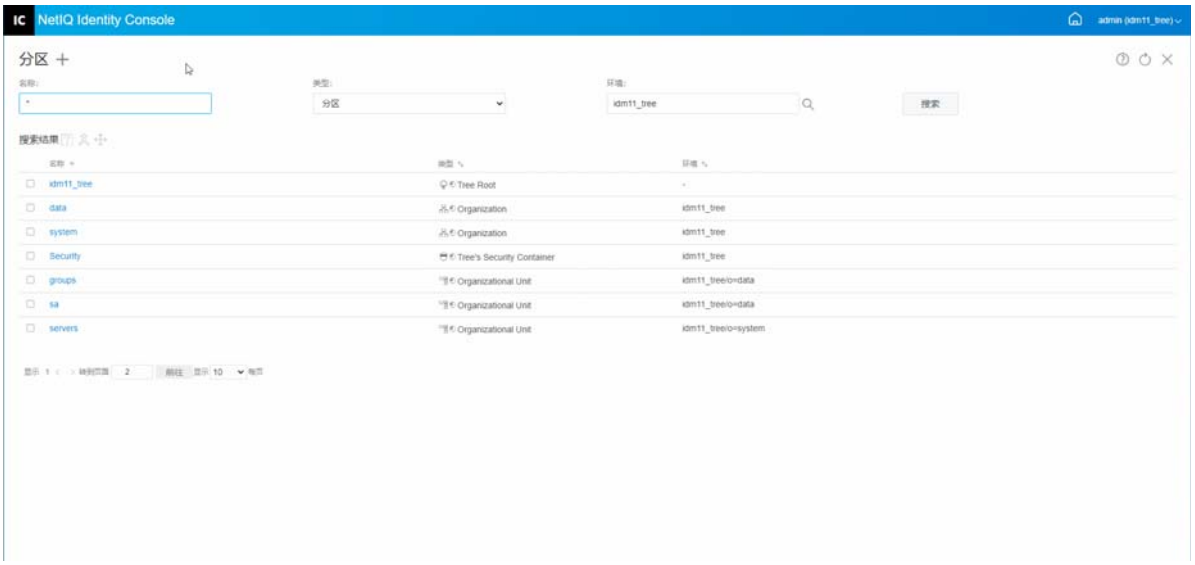
1 在 Identity Console 登录页中单击分区管理选项。

2 指定分区名称、类型和环境，或使用搜索功能查找分区，然后单击 搜索 按钮。

3 从搜索列表中选择分区，然后单击 图标并单击确定。

4 此时显示一条确认讯息，指示已合并分区。

图 14-2 合并分区



修改分区

要修改分区：

1 在 Identity Console 登录页中单击分区管理选项。

2 键入分区名称、类型和环境，然后单击 搜索 按钮。

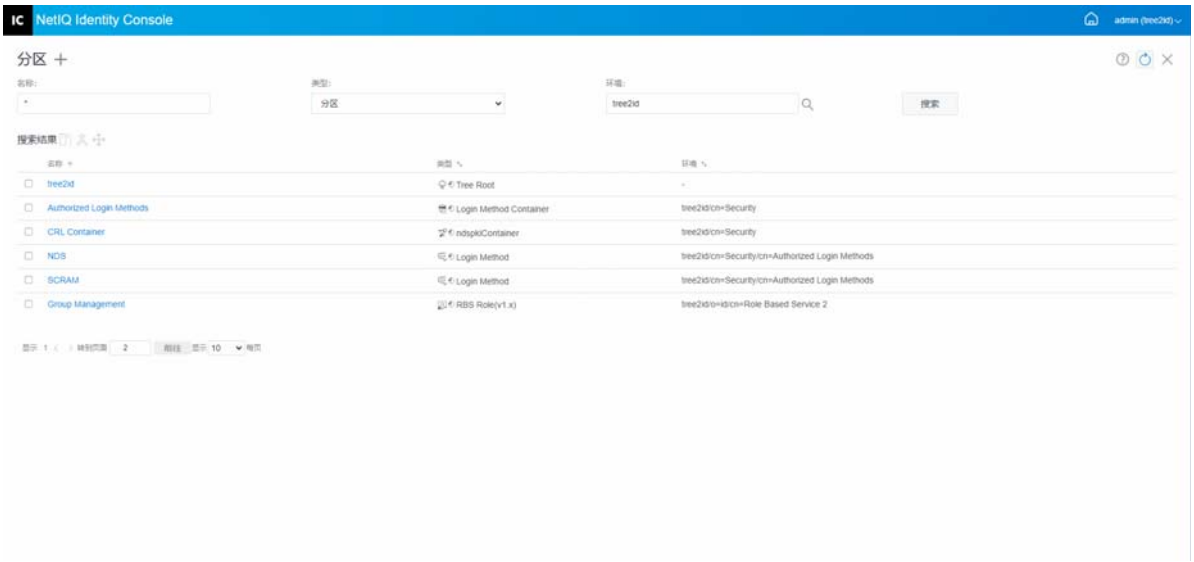
3 从搜索列表中选择分区并单击 图标。

4 单击过滤器下的编辑选项以更改复本过滤器及其相应的类和属性，然后单击确定。

   如果您在类型字段中选择了服务器，您将看到所有服务器的列表。单击每个服务器将显示服务器中所有分区的列表。

5 此时显示一条确认讯息，指示已修改分区。

图 14-3 修改分区



移动分区

移动分区操作可以将子树移动到目录树中。此操作也称为修剪和挂接操作。只能移动没有从属分区的分区。如果存在从属分区，在执行移动操作之前，必须先合并这些分区。

移动分区时， eDirectory 将更改对该分区根对象的所有参照。尽管对象的常用名并未改变，但是树枝 （及其所有的从属）的完整名称将有所改变。

注释：移动分区时，必须遵循 eDirectory 包容规则。例如，不能将 “ 组织单元 ” 直接移至目录树根下，因为根的包容规则只允许包容 “ 位置 ”、 “ 国家 / 地区 ” 或 “ 组织 ” 对象，但不能包容 “ 组织单元 ” 对象。

要移动分区：

1 在 Identity Console 登录页中单击分区管理选项。

2 键入分区名称、类型和环境，然后单击 搜索 按钮。

3 从搜索列表中选择分区并单击 ✣ 图标。

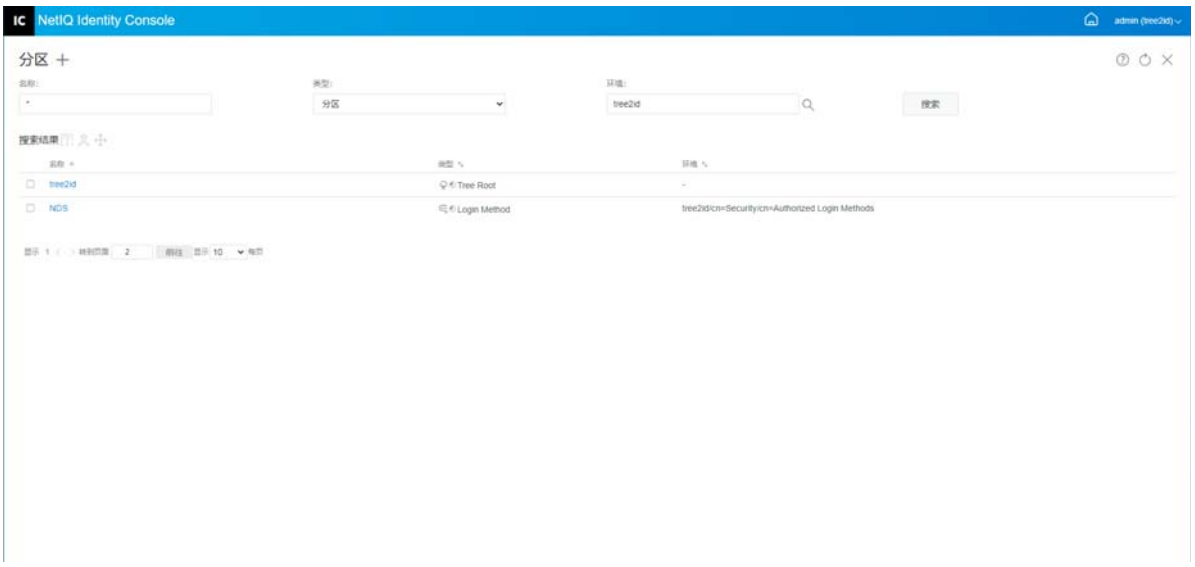
4 选择要将指定分区移动到的目标容器对象，然后单击确定。

注释：创建别名来取代已移动的分区，将创建指向分区新位置的指针。这样可以使任何与原位置相关的操作继续执行而不会中断，直到可以对那些操作进行更新，以反映对象的新位置。用户可以继续登录到网络，并在原始目录位置中找到对象。

---

5 此时出现一条确认讯息，指示移动分区操作已成功。

图 14-4 *移动分区*



15 管理索引

“ 索引管理器 ” 是服务器对象的属性，利用它可以管理数据库索引。 eDirectory 利用这些索引来极大地提高查询性能。

NetIQ eDirectory 自带一组提供基本查询功能的索引。这些默认索引用于以下属性。

可以使用索引模块执行以下任务：

- 创建索引 （第 79 页）
- 删除索引 （第 80 页）
- 复制索引 （第 81 页）
- 更改索引状态 （第 81 页）

创建索引

要创建新索引：

1 在 Identity Console 登录页中单击**索引管理**选项。

2 单击 ＋ 图标。

3 输入索引名称。

4 从可用的 NCP Server 列表中选择服务器。

5 选择所需的属性。

6 选择索引规则：

   6a **子字符串：**这与属性值字符串的子集匹配。例如，如果某个查询需查找带 “der” 的 “LastName”，则会返回 “Derington”、 “Anderson” 和 “Lauder” 作为匹配项。子字符串索引在创建和维护时是最消耗资源的索引。

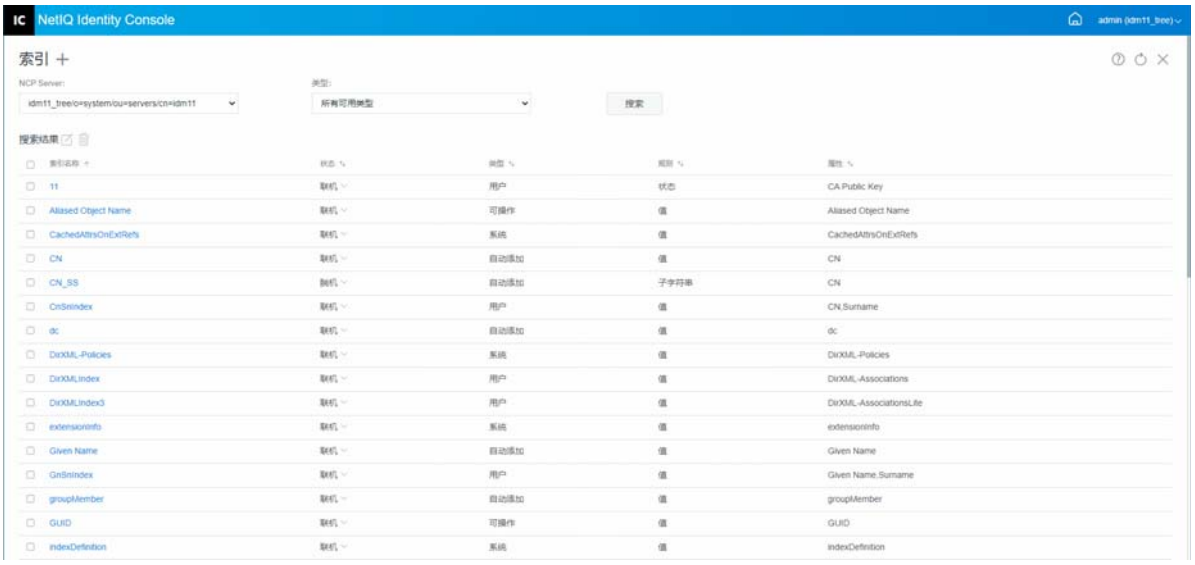
   6b **状态：**这只要求某个属性存在，不要求特定的属性值。如果某个查询需查找具有 “ 登录脚本 ” 属性的所有项，则该查询将使用状态索引。

   6c **值：**这与整个属性值或属性值的第一部分匹配。例如，可以使用值匹配来查找 “LastName” 等于 “Jensen” 的项，以及 “LastName” 以 “Jen” 开头的项。

7 单击 创建 按钮。

8 此时显示一条确认讯息，指示已创建索引。

图 15-1 创建新索引



删除索引

要删除索引：

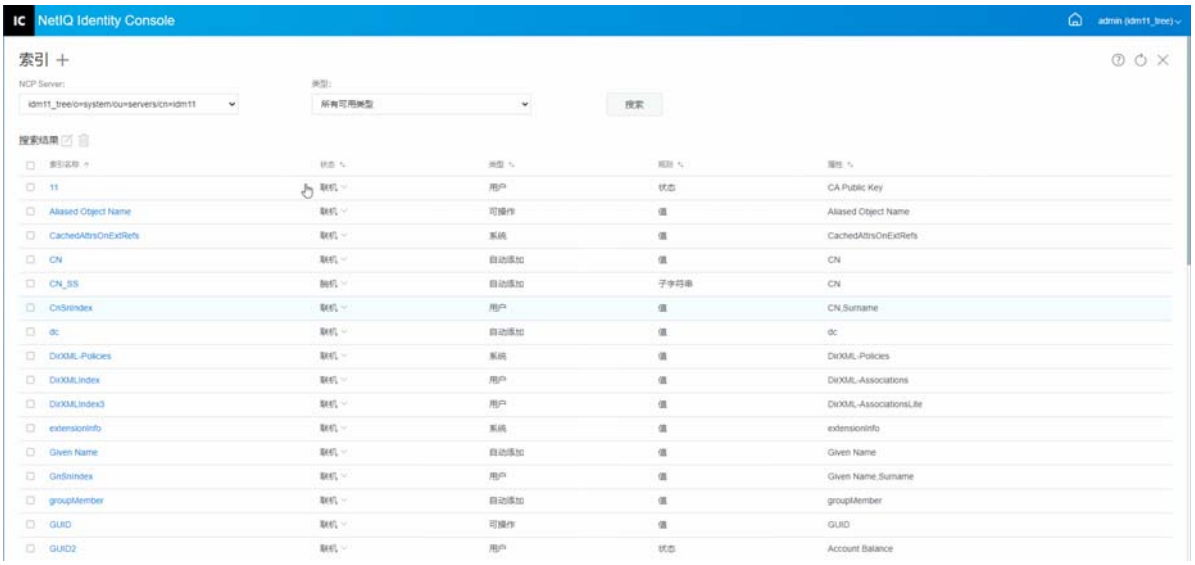
1 在 Identity Console 登录页中单击索引管理选项。

2 选择 NCP Server 和索引的类型，然后单击 搜索 按钮。

3 从搜索列表中选择索引并单击 图标。

4 此时显示一条确认讯息，指示已删除索引。

图 15-2 删除索引



复制索引

如果您发现某个索引在一个服务器上很有用，并且您知道另一个服务器需要此索引，则可以将索引定义从一个服务器复制到另一个服务器。在查看预测数据时，您可能还会发现相反的情况：满足多个服务器需求的索引在其中一个服务器中不再有用。在这种情况下，您可以从不使用索引的那个服务器中删除索引。

要复制索引：

1 在 Identity Console 登录页中单击索引管理选项。

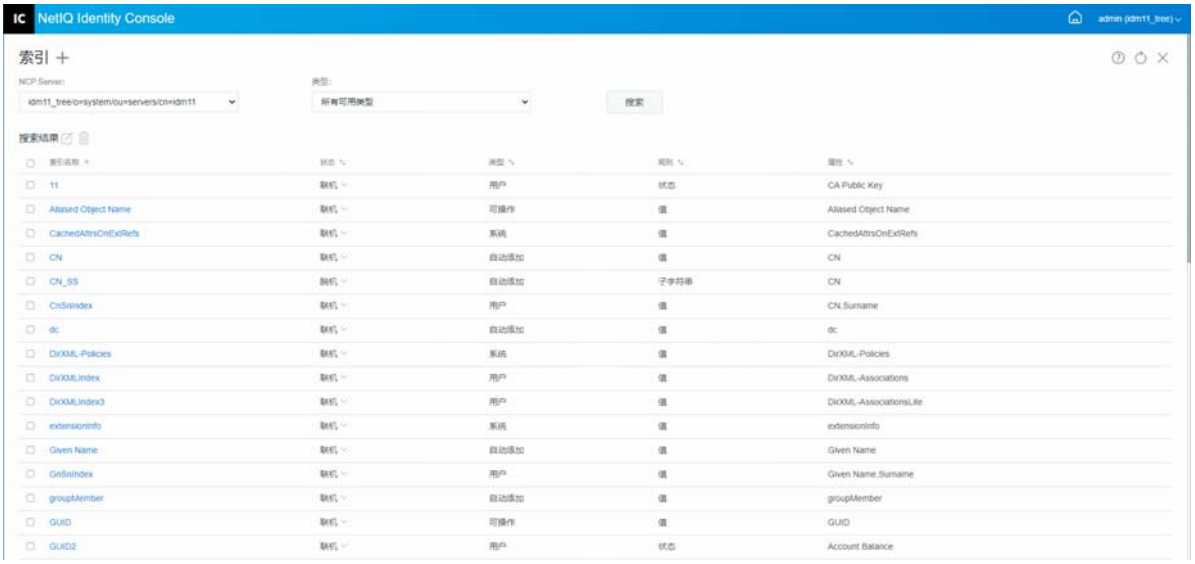
2 选择 NCP Server 和索引的类型，然后单击 搜索 按钮。

3 从搜索列表中选择索引并单击 图标。

4 选择想要复制索引的 NCP Server 并单击 保存 按钮。

5 此时显示一条确认讯息，指示已修改索引。

图 15-3 复制索引



更改索引状态

在高峰时段，您可能想要通过暂时使索引脱机来调整性能。例如，要获得更高的批量装载速度，您可能需要暂停所有用户定义的索引。因为每次添加对象或修改对象都需要更新定义的索引，因此所有索引都处于活动状态可能会减慢数据的批量装载速度。批量装载完成后，可以将索引重新联机。

要使索引脱机：

1 在 Identity Console 登录页中单击索引管理选项。

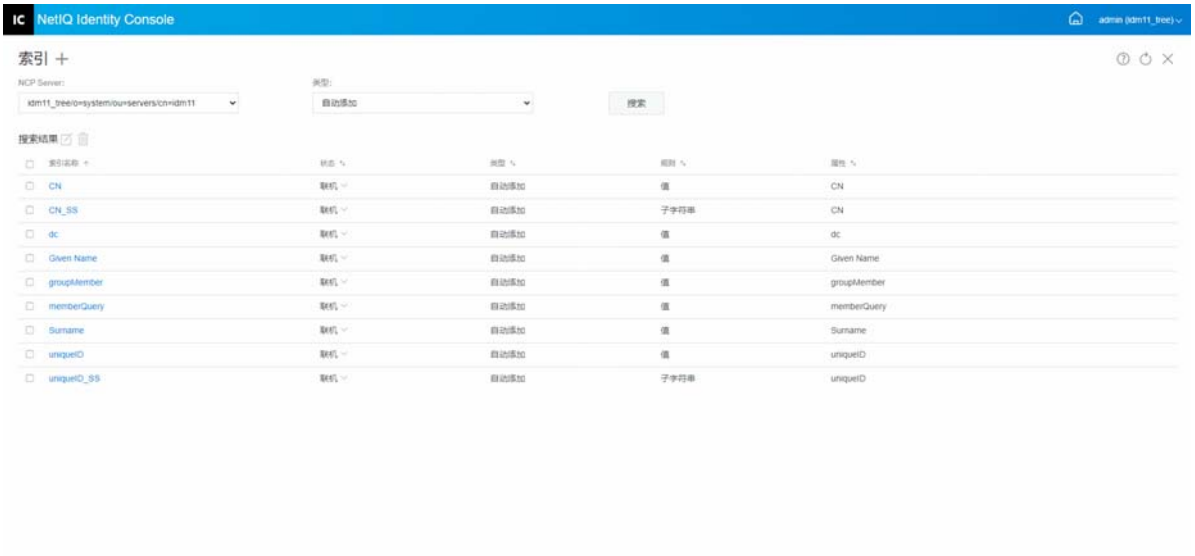
2 选择 NCP Server 和索引的类型，然后单击 搜索 按钮。

3 单击索引列表中的状态下拉列表。索引状态有：

- **联机**：当前正在运行
- **脱机**：已暂停。可以重新启动索引。

注释：无法更改“系统”和“可操作”类型索引的状态。也不能删除此类索引。

图 15-4 使索引脱机



16 配置 LDAP 对象

eDirectory 安装将创建 LDAP 服务器对象和 LDAP 组对象。 LDAP 服务的默认配置位于这两个对象的目录中。您可以使用 Identity Console 中的 LDAP 管理任务来修改默认配置。

LDAP 服务器对象表示特定于服务器的配置数据。但是， LDAP 组对象包含可以在多个 LDAP 服务器之间轻松共享的配置信息。此对象提供通用配置数据，并代表一组 LDAP 服务器。服务器具有通用数据。

您可以将多个 LDAP 服务器对象与一个 LDAP 组对象关联。然后，所有关联的 LDAP 服务器都会从其 LDAP 服务器对象获取其服务器特定配置，但从 LDAP 组对象获取通用或共享信息。

可以使用 LDAP 模块执行以下任务：

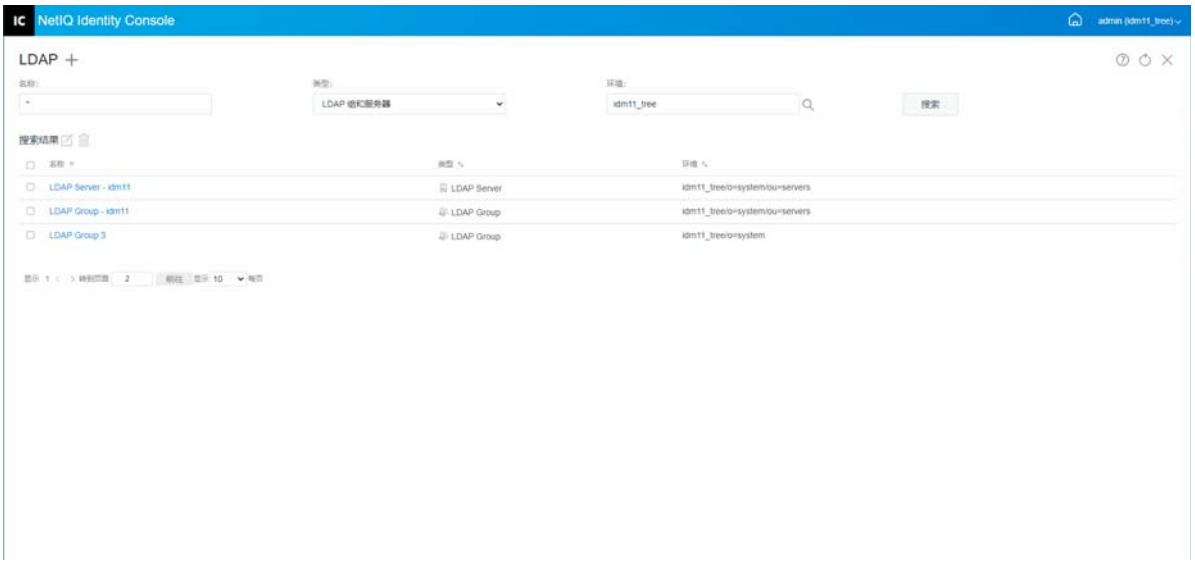
- 创建 LDAP 对象 （第 83 页）
- 删除 LDAP 对象 （第 84 页）
- 修改 LDAP 对象 （第 85 页）

创建 LDAP 对象

要创建新的 LDAP 对象：

1. 在 Identity Console 登录页中单击 **LDAP 配置**选项。
2. 单击 + 图标。
3. 在创建 LDAP 对象页面中，指定名称、类型和环境，或者使用搜索环境 图标来进行查找，然后单击**创建**。
4. 此时显示一条确认讯息，指示已创建 LDAP 对象。

图 16-1　创建新的 LDAP 对象



删除 LDAP 对象

要删除 LDAP 对象：

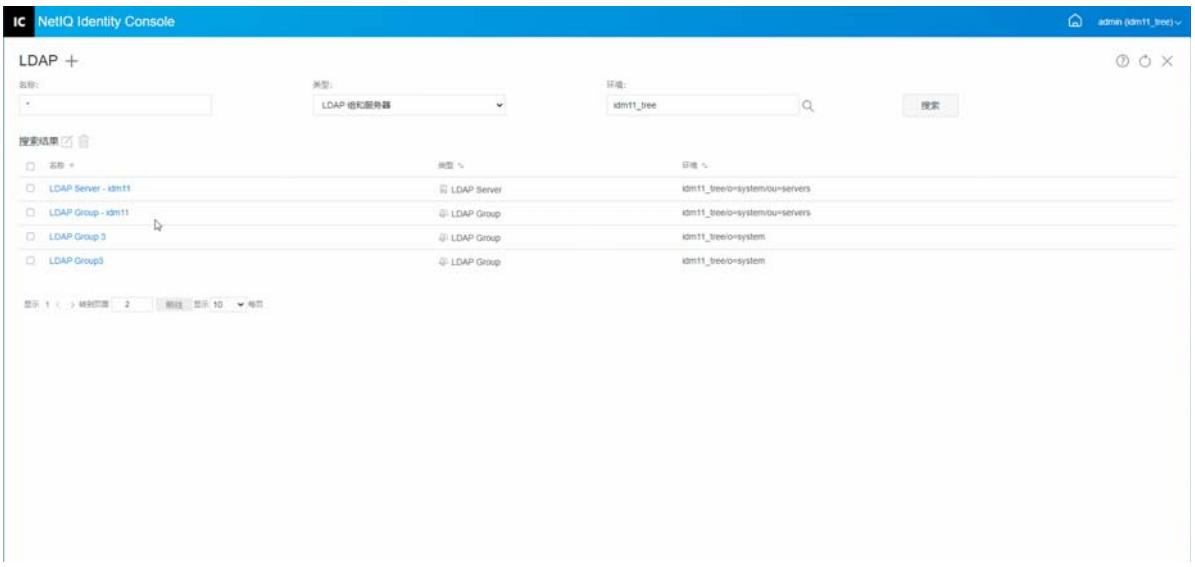
1 在 Identity Console 登录页中单击 **LDAP 配置**选项。

2 指定 LDAP 对象名称、类型和环境，然后单击 搜索 按钮。

3 从搜索列表中选择 LDAP 对象并单击 🗑 图标。

4 此时显示一条确认讯息，指示已删除 LDAP 对象。

图 16-2　删除 LDAP 对象



修改 LDAP 对象

要修改 LDAP 对象：

1 在 Identity Console 登录页中单击 **LDAP 配置**选项。

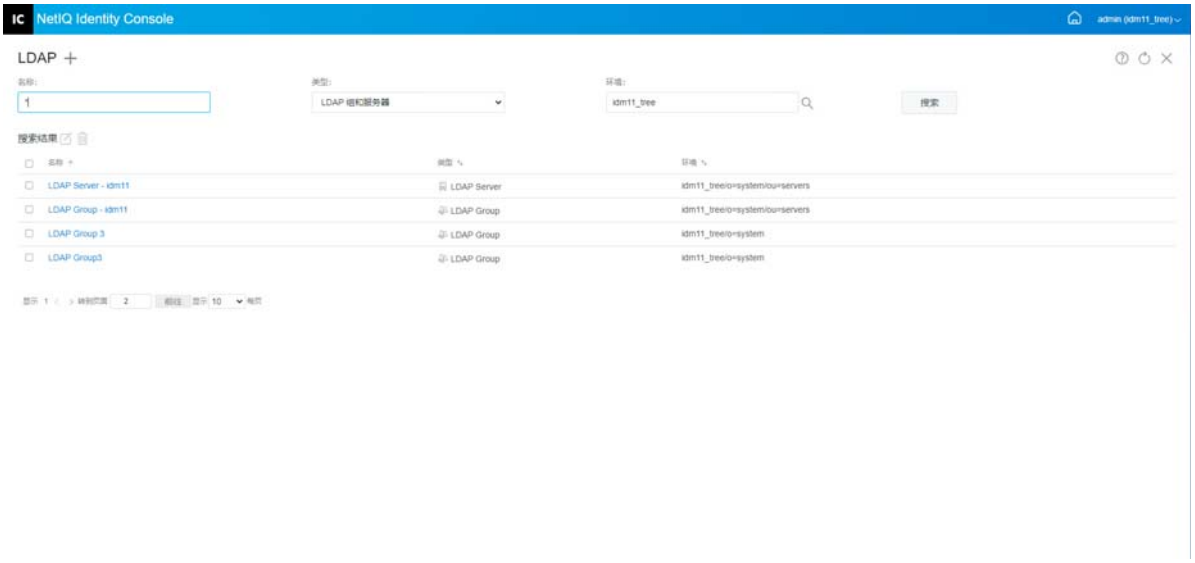
2 键入 LDAP 对象名称、类型和环境，然后单击 搜索 按钮。

3 从搜索列表中选择 LDAP 对象并单击 图标。

4 根据需要修改特定 LDAP 对象的属性和信息，然后单击 保存 按钮。有关 LDAP 对象属性的更多信息，请参阅 *《NetIQ eDirectory Administration Guide》*（NetIQ eDirectory 管理指南）中的 Configuring LDAP Server and LDAP Group Objects on Linux（在 Linux 中配置 LDAP 服务器和 LDAP 组对象）。

5 此时显示一条确认讯息，指示已修改 LDAP 对象。

图 16-3 *修改 LDAP 对象*



17 管理证书

安装 eDirectory 时，会自动安装 NetIQ Certificate Server。 Certificate Server 提供公共密钥加密法服务，这些服务原生集成在 eDirectory 中，可用于创建、发布和管理用户证书和服务器证书。这些服务可保护通过公共通信通道 （如因特网）进行的保密数据传输。

注释：如果您想将证书管理模块与 Identity Console 结合使用，则必须将 eDirectory 服务器升级到 9.2.4 HF2。

Identity Console 提供下列证书管理任务：

管理证书颁发机构

默认情况下， NetIQ Certificate Server 安装过程会为您创建组织证书颁发机构 (CA)。系统会提示您指定组织证书颁发机构名称。单击 " 完成 " 时，将使用默认参数创建组织证书颁发机构并放置在安全性容器中。如果您想要对组织证书颁发机构的创建进行更多控制，可以通过使用 Identity Console 门户手动创建组织证书颁发机构。如果删除组织证书颁发机构，则需要重新创建它。

使用证书颁发机构模块，您可以执行以下任务：

创建组织证书颁发机构对象

要创建组织证书颁发机构对象，执行下列操作：

1 在 Identity Console 登录页中单击证书管理 > 证书颁发机构管理选项。

2 如果没有组织证书颁发机构对象，将打开 " 创建组织证书颁发机构对象 " 对话框和创建对象的相应向导。按照提示创建对象。

注释：确保此处指定的 CRL 文件路径体现 eDirectory 安装路径。

---

3 创建完证书颁发机构后，我们建议您备份证书颁发机构的公共密钥 / 私用密钥对，并将此密钥对存储在安全可靠的地方。有关更多信息，请参见备份组织证书颁发机构证书（第 88 页）。

备份组织证书颁发机构证书

我们建议您备份组织证书颁发机构的私用密钥和证书，以防组织证书颁发机构的主机服务器出现无法恢复的故障。如果出现故障，您可以使用备份文件将组织证书颁发机构恢复到树中的任何服务器。

注释：仅通过 Certificate Server 9.0 及以上版本创建的组织证书颁发机构能够进行备份。对于之前版本的 Certificate Server，组织证书颁发机构私用密钥的创建方式使其无法导出。

备份文件包含证书颁发机构的私用密钥、自我签名证书、公共密钥证书以及操作所需的其他几个证书。此类信息以 PKCS #12 格式 （也称为 PFX）存储。

应在组织证书颁发机构正常工作时对其进行备份。

要备份组织证书颁发机构，执行下列操作：

1 在 Identity Console 登录页中单击证书管理 > 证书颁发机构管理选项。

2 单击证书选项卡。

3 选择 **Self Signed Certificate** （自我签名证书）或 **Public Key Certificate** （公共密钥证书）。在备份操作期间，这两个证书都写入文件。我们建议您单独为 RSA 和 ECDSA 证书选择自我签名证书。

4 单击 图标。

5 选择导出私用密钥，指定具有 6 个或更多字母数字字符的口令用于加密 PFX 文件，并选择导出格式 PKCS12，然后单击确定。

6 加密备份文件写入指定位置。现在可以将此文件储存在安全位置以供紧急使用。

恢复组织证书颁发机构

如果组织证书颁发机构对象被删除或已损坏，或者组织证书颁发机构的主机服务器出现无法恢复的故障，可以使用按备份组织证书颁发机构证书 （第 88 页）中所述创建的备份文件将组织证书颁发机构完全恢复正常。

要恢复组织证书颁发机构，执行下列操作：

1 在 Identity Console 登录页中单击证书管理 > 证书颁发机构管理选项。

2 单击屏幕顶部 （证书颁发机构管理旁边）的 ↑↓，删除现有组织证书颁发机构。

3 系统将提示您配置新的组织证书颁发机构。这将打开 " 创建组织证书颁发机构对象 " 对话框和创建对象的相应向导。

4 在创建对话框中，指定应托管组织证书颁发机构的服务器和组织证书颁发机构对象的名称。

5 选择导入。

6 选择 RSA 和 ECDSA 证书。 Certificate Server 要求两个证书的主体名称相同。但是，Certificate Server 不支持导入外部自我签名证书颁发机构证书。但是，它允许您导入从属证书颁发机构证书。

7 在随后的屏幕中，浏览并选择 RSA 和 ECDSA 的文件名称。

8 输入备份时用于加密文件的口令，然后单击确定。

9 现已恢复组织证书颁发机构的私用密钥和证书，证书颁发机构已完全正常。现在可以再次存储该文件以供将来使用。

验证组织证书颁发机构证书

如果您怀疑证书有问题或认为证书可能不再有效，可以使用 Identity Console 轻松验证证书。eDirectory 树中的任何证书都可以进行验证，包括外部证书颁发机构颁发的证书。

证书验证过程包括对证书中数据以及证书链中数据的多次检查。证书链由根证书颁发机构证书和可选的一个或多个中间证书颁发机构证书组成。

要验证证书：

1 在 Identity Console 登录页中单击证书管理 > 证书颁发机构管理选项。

2 单击证书选项卡。

3 选择 **Self Signed Certificate** （自我签名证书）或 **Public Key Certificate** （公共密钥证书）。

4 单击 ⊙ 验证所选的证书颁发机构证书。

替换组织证书颁发机构证书

如果证书因某种原因而损坏或无效，或者您只是想替换现有证书，执行下列操作：

1 在 Identity Console 登录页中单击证书管理 > 证书颁发机构管理选项。

2 单击证书选项卡。

3 选择 **Self Signed Certificate** （自我签名证书）或 **Public Key Certificate** （公共密钥证书）。

4 单击 ↑↓ 替换所选证书颁发机构证书。

5 导入 .pfx 或 .p12 格式的证书颁发机构证书并指定加密私用密钥的口令。

6 单击确定。

撤消组织证书颁发机构证书

要撤消证书：

1 在 Identity Console 登录页中单击证书管理 > 证书颁发机构管理选项。

2 单击证书选项卡。

3 选择 **Self Signed Certificate** （自我签名证书）或 **Public Key Certificate** （公共密钥证书）。

4 单击 ⊘ 图标。

5 阅读并了解撤消服务器证书所涉及的风险。

6 从下拉列表中选择撤消的有效理由，选择无效日期并指定任何其他注释。

7 单击确定以完成撤消。

图 17-1 管理证书颁发机构

管理服务器证书

使用服务器证书管理模块，管理员可以执行以下任务：

- 创建服务器证书对象 （第 91 页）
- 导出服务器证书对象 （第 91 页）
- 验证服务器证书对象 （第 91 页）
- 替换服务器证书对象 （第 91 页）
- 撤消服务器证书对象 （第 92 页）
- 删除服务器证书对象 （第 92 页）

创建服务器证书对象

要创建服务器证书对象，执行下列操作：

1 在 Identity Console 登录页中单击证书管理 > 服务器证书管理选项。

2 单击 ＋ 图标。

3 在创建服务器证书页面中，指定绰号、服务器并选择以下选项中的一个：
   - **标准 （默认参数）：**允许您创建 RSA 或 ECDSA 类型的默认服务器证书对象。
   - **自定义 （用户指定参数）：**允许您指定服务器证书对象的自定义参数。
   - **导入 （允许导入 PKCS12 文件）：**允许您导入 .pfx 或 .p12 格式的 PKCS12 文件。

4 指定参数后，单击下一步查看证书摘要。

5 在摘要屏幕中，单击确定以创建服务器证书对象。

导出服务器证书对象

要导出服务器证书对象，执行下列操作：

1 在 Identity Console 登录页中单击证书管理 > 服务器证书管理选项。

2 从下拉列表中选择相应的服务器。

3 从列表中选择相应的服务器证书，然后单击 图标。

4 在下一个屏幕上，勾选导出私用密钥复选框，并指定一个口令以保护私用密钥。确认口令并选择导出格式。

注释：服务器证书只能以 PKCS12 格式导出。

---

5 单击确定导出服务器证书对象。

验证服务器证书对象

要验证服务器证书对象，执行下列操作：

1 在 Identity Console 登录页中单击证书管理 > 服务器证书管理选项。

2 从下拉列表中选择相应的服务器。

3 从列表中选择相应的服务器证书，然后单击 图标。

4 此时显示一条确认讯息，指示成功验证服务器证书对象。

替换服务器证书对象

如果服务器证书因某种原因而损坏或无效，或者您只是想替换现有默认证书，执行下列操作：

1 在 Identity Console 登录页中单击证书管理 > 服务器证书管理选项。

2 从下拉列表中选择相应的服务器。

3 从列表中选择相应的服务器证书，然后单击 ↑↓ 图标。
4 阅读并了解替换服务器证书所涉及的风险，然后单击确定。
5 在下一个屏幕中，浏览并选择 .pfx 或 .p12 格式的新服务器证书并指定口令。
6 单击确定以替换服务器证书。

撤消服务器证书对象

要撤消服务器证书对象，执行下列操作：

1 在 Identity Console 登录页中单击证书管理 > 服务器证书管理选项。
2 从下拉列表中选择相应的服务器。
3 从列表中选择相应的服务器证书，然后单击 ⊘ 图标。
4 阅读并了解撤消服务器证书所涉及的风险，然后单击确定。
5 在下一个屏幕中，从下拉列表中选择撤消的有效理由，选择无效日期并指定任何其他注释。
6 单击确定以完成撤消。

删除服务器证书对象

要去除服务器证书对象，执行下列操作：

1 在 Identity Console 登录页中单击证书管理 > 服务器证书管理选项。
2 从下拉列表中选择相应的服务器。
3 从列表中选择相应的服务器证书，然后单击 🗑 图标。
4 在下一个屏幕上，单击确定。
5 此时显示一条确认讯息，指示成功删除服务器证书对象。

图 17-2 管理服务器证书

管理用户证书

使用用户证书管理模块可以执行以下任务：

创建用户证书对象

要创建用户证书对象，执行下列操作：

1 在 Identity Console 登录页中单击证书管理 > 用户证书管理选项。

2 单击 ＋ 图标。

3 在创建用户证书页面中，指定绰号、服务器并选择以下选项中的一个：
   - **标准 （默认参数）：**允许您创建 RSA 或 ECDSA 类型的默认用户证书对象。
   - **自定义 （用户指定参数）：**允许您指定用户证书对象的自定义参数。
   - **导入：**允许您导入 CERT 或 PKCS12 格式的证书文件。

4 指定参数后，单击下一步查看证书摘要。

5 在摘要屏幕中，单击确定以创建用户证书对象。

导出用户证书对象

要导出用户证书对象，执行下列操作：

1 在 Identity Console 登录页中单击证书管理 > 用户证书管理选项。

2 从下拉列表中选择相应的服务器。

3 从列表中选择相应的用户证书，然后单击 图标。

4 在下一个屏幕上，勾选导出私用密钥复选框，并指定一个口令以保护私用密钥。确认口令并选择导出格式。

注释：用户证书只能以 PKCS12 格式导出。

---

5 单击确定导出用户证书对象。

验证用户证书对象

要验证用户证书对象，执行下列操作：

1 在 Identity Console 登录页中单击证书管理 > 用户证书管理选项。

2 从下拉列表中选择相应的服务器。

3 从列表中选择相应的用户证书，然后单击 ⊙ 图标。

4 此时显示一条确认讯息，指示成功验证用户证书对象。

撤消用户证书对象

要撤消用户证书对象，执行下列操作：

1 在 Identity Console 登录页中单击证书管理 > 用户证书管理选项。

2 从下拉列表中选择相应的服务器。

3 从列表中选择相应的用户证书，然后单击 ⊘ 图标。

4 阅读并了解撤消用户证书所涉及的风险。

5 从下拉列表中选择撤消的有效理由，选择无效日期并指定任何其他注释。

6 单击确定以完成撤消。

删除用户证书对象

要去除用户证书对象，执行下列操作：

1 在 Identity Console 登录页中单击证书管理 > 用户证书管理选项。

2 从下拉列表中选择相应的服务器。

3 从列表中选择相应的用户证书，然后单击 🗑 图标。

4 在下一个屏幕上，单击确定。

5 此时显示一条确认讯息，指示成功删除用户证书对象。

图 17-3 管理用户证书

管理可信根和容器

在公共密钥加密法中，可信根提供了信任的基础。可信根用于验证由其他证书颁发机构签名的证书。可信根支持 SSL 安全性、安全的电子邮件和基于证书的鉴定。

使用可信根管理模块可以执行以下任务：

- 创建可信根容器 （第 95 页）
- 创建可信根证书对象 （第 95 页）
- 导出可信根证书对象 （第 96 页）
- 验证可信根证书对象 （第 96 页）
- 删除可信根证书对象 （第 96 页）
- 删除可信根容器 （第 96 页）

创建可信根容器

要创建可信根容器，执行以下任务：

1. 在 Identity Console 登录页中单击证书管理 > 可信根管理选项。默认情况下将勾选可信根容器复选框。
2. 单击 ＋ 图标创建新的可信根容器。
3. 指定可信根容器的名称。
4. 使用对象选择器浏览相应的容器。
5. 单击确定按钮。
6. 此时显示一条确认讯息，指示已成功创建可信根容器。

创建可信根证书对象

要创建可信根对象，执行下列操作：

1. 在 Identity Console 登录页中单击证书管理 > 可信根管理选项。默认情况下将勾选可信根容器复选框。勾选可信根复选框。
2. 单击 ＋ 图标创建新的可信根对象。
3. 指定可信根对象的名称。
4. 从下拉列表中选择相应的可信根容器。
5. 浏览并选择 .der 或 .b64 格式的相应证书文件。

   注释：任何类型的证书都可以存储在可信根对象中 （证书颁发机构证书、中间证书颁发机构证书或用户证书）。

6. 单击确定按钮。
7. 此时显示一条确认讯息，指示已成功创建可信根对象。

导出可信根证书对象

要导出可信根证书对象，执行下列操作：

1 在 Identity Console 登录页中单击证书管理 > 可信根管理选项。默认情况下将勾选可信根容器复选框。勾选可信根复选框。

2 从列表中选择相应的可信根证书，然后单击 图标。

3 在下一个屏幕上，勾选导出私用密钥复选框，并指定一个口令以保护私用密钥。确认口令并选择导出格式。

注释：可信根证书只能以 DER 或 BASE64 格式导出。

---

4 单击确定导出可信根证书对象。

验证可信根证书对象

要验证可信根证书对象，执行下列操作：

1 在 Identity Console 登录页中单击证书管理 > 可信根管理选项。默认情况下将勾选可信根容器复选框。勾选可信根复选框。

2 从列表中选择相应的可信根证书，然后单击 图标。

3 此时显示一条确认讯息，指示成功验证可信根证书对象。

删除可信根证书对象

要去除可信根证书对象，执行下列操作：

1 在 Identity Console 登录页中单击证书管理 > 可信根管理选项。默认情况下将勾选可信根容器复选框。勾选可信根复选框。

2 从列表中选择相应的可信根证书，然后单击 图标。

3 单击警告屏幕上的确定。

4 此时显示一条确认讯息，指示成功删除可信根证书对象。

删除可信根容器

要去除可信根容器，执行下列操作：

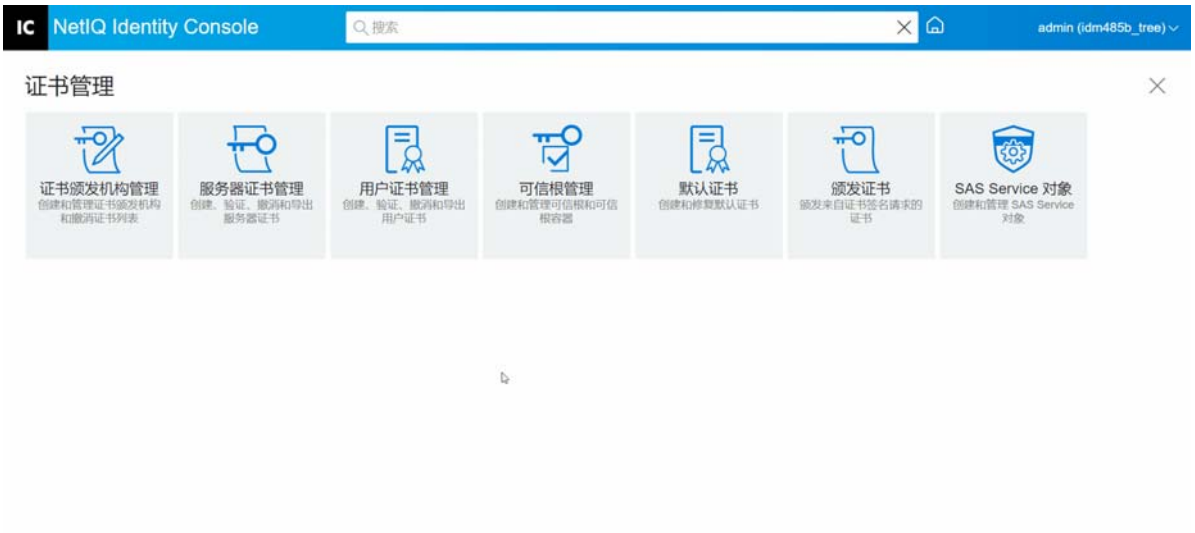
1 在 Identity Console 登录页中单击证书管理 > 可信根管理选项。默认情况下将勾选可信根容器复选框。

2 从列表中选择相应的可信根容器，然后单击 图标。

3 单击警告屏幕上的确定。

4 此时显示一条确认讯息，指示成功删除可信根容器。

图 17-4 管理可信根容器



创建默认服务器证书对象

Certificate Server 安装会创建默认服务器证书对象。

- SSL CertificateDNS - *server_name*
- 服务器上配置的每个 IP 地址的证书 （IPAG *xxx.xxx.xxx.xxx - server_name*）
- 服务器上配置的每个 DNS 名称的证书 （DNSAG *www.example.com - server_name*）

注释：eDirectory 不会自动创建 SSL CertificateIP。 SSL 证书 DNS 包含主题备用名称中列出的所有 IP。当您尝试使用 Identity Console 创建或修复默认证书时，默认情况下不会创建或修复 SSL CertificateIP 证书。但是，插件界面提供了一个复选框，您可以选择该复选框以覆盖默认行为并强制创建 / 修复 SSL CertificateIP 证书。

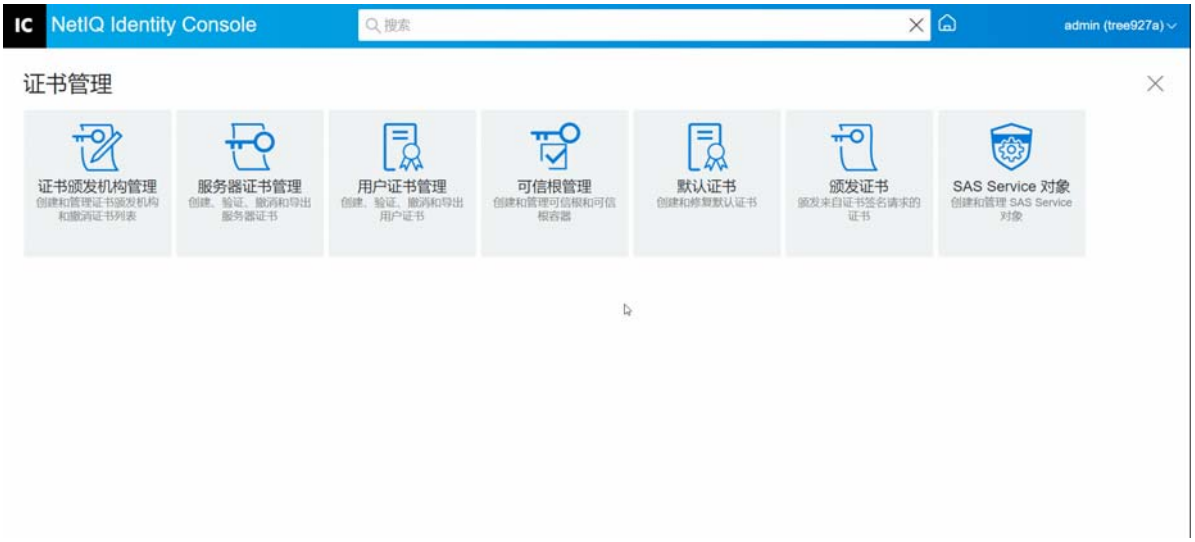
如果组织证书颁发机构有 ECDSA 证书， eDirectory 9.0 及以上版本会自动创建 ECDSA 证书。

如果这些证书因某种原因而损坏或无效，或者如果您只是想替换现有的默认证书，可以使用创建默认服务器证书向导，如下所述：

1. 在 Identity Console 登录页中单击证书管理 > 默认证书选项。
2. 选择要创建默认证书的一个或多个服务器，然后单击下一步。
3. 如果想要重写现有的默认服务器证书，选择 “ 是 ”，如果只想在现有默认服务器证书无效时重写它们，则选择 “ 否 ”。
4. （仅限单个服务器）如果想要使用现有的 DNS 地址，选择该选项。如果想要使用不同的 DNS 地址，选择该选项并指定新的 DNS 地址。
5. （仅限单个服务器）如果想要使用现有的默认 IP 地址，选择该选项。如果想要使用不同的 IP 地址，选择该选项并指定新的 IP 地址。
6. 单击下一步。
7. 审阅摘要页，然后单击完成。

如果您想要对服务器证书对象的创建进行更多控制，可以手动创建服务器证书对象。有关更多信息，请参见创建服务器证书对象 （第 91 页）。

图 17-5 创建默认服务器证书对象



颁发公共密钥证书

您的组织证书颁发机构的工作方式与外部 CA 相同。这意味着，它能够从证书签名请求 (CSR) 颁发证书。当用户将 CSR 发送给您进行签名时，您可以使用您的组织证书颁发机构颁发证书。然后，请求证书的用户可以将颁发的证书直接导入启用加密法的应用程序。

此任务允许您为无法识别服务器证书对象的启用加密法的应用程序生成证书。

要颁发证书，执行下列操作：

1 在 Identity Console 登录页中单击证书管理 > 颁发证书选项。

2 浏览并选择 CSR 文件。

3 在密钥用法规范下选择适当的密钥类型和相应的密钥用法。这些选项允许您选择密钥类型。每种密钥类型均已预先定义了与之相关的密钥用法值：

   3a **未指定：**此选项为默认选择，它不会激活证书中的任何密钥用法。

   3b **证书颁发机构：**此选项激活证书签名和 CRL 签名密钥用法。

   3c **加密：**此选项激活 “ 密钥加密 ” 密钥用法。

   3d **签名：**此选项激活 “ 数字签名 ” 密钥用法。

   3e **SSL 或 TSL：**此选项配置密钥，使其可以在 SSL 或 TLS 事务中使用。

   3f **自定义：**此选项允许您手动选择任意或所有密钥用法选项。

   3g **将密钥用法扩展设置为关键：**除选择未指定的密钥类型外，所有密钥类型都可以将密钥用法扩展标记为关键。无论要将证书用于何种用途，接收软件都必须理解所有关键扩展。因此，将扩展标记为关键确实存在一定的风险，因为并非所有应用程序都能使用该证书。但对于密钥使用这类众所周知的扩展，这种风险很小。通常，如果已指定密钥使用，则应将扩展标记为关键。

4 您可以选择在证书中编码扩展密钥用法扩展。要激活此功能，选择启用扩展密钥用法：

4a **服务器：**此选项激活服务器鉴定扩展密钥用法。

4b **用户：**此选项激活用户鉴定和电子邮件保护扩展密钥用法。

4c **自定义：**此选项允许您选择任意或所有扩展密钥用法。

4d **任何：**使密钥可用于任意扩展密钥用法。

4e **将扩展的密钥用法扩展设置为关键：**无论要将证书用于何种用途，接收软件都必须理解所有关键扩展。因此，将扩展标记为关键确实存在一定的风险，因为并非所有应用程序都能使用该证书。由于许多应用程序都不理解扩展密钥使用扩展，因此，将此扩展标记为关键很可能会导致给定应用程序不接受该证书；所以，应该仅在必要时才将扩展设置为关键。

5 选择适当的基本约束：

5a **证书类型：**

5a1 **未指定：**如果不希望向证书添加基本限制扩展，可选择此选项。

5a2 **证书颁发机构：**选择此选项可向证书中添加证书颁发机构基本限制扩展。如果证书用于证书颁发机构，则必须选择此选项。

5a3 **最终实体：**选择此选项可向证书添加基本限制扩展，指定这是最终实体 （不是证书颁发机构）证书。注意：如果证书类型为 “ 最终实体 ”，则路径长度应设置为 “ 未指定 ”。

5b **路径长度：**

5b1 **未指定：**如果不想指定在此 CA 下可创建多少级从属 CA，可选择此选项。

注释：如果证书类型为 “ 最终实体 ”，则路径长度只能设置为 “ 未指定 ”。

5b2 **特定：**如果要指定在此 CA 下可创建多少级从属 CA，可选择此选项。单击向上箭头和向下箭头指定路径长度。

注释：如果创建的证书是从属证书颁发机构，则路径长度必须与上级证书颁发机构一致。例如，如果上级 CA 的路径长度为 3，则从属 CA 的路径长度必须小于或等于 2。如果上级 CA 的路径长度未指定，则从属 CA 的路径长度也为未指定或任何所需的具体路径长度。

5c **将基本约束扩展设置为关键：**通常，对于 CA 证书，必须将基本限制扩展设置为关键。无论要将证书用于何种用途，接收软件都必须理解所有关键扩展。因此，将扩展标记为关键确实存在一定的风险，因为并非所有应用程序都能使用该证书。但对于基本限制这类众所周知的扩展，这种风险很小。

6 指定以下证书参数：

6a **主题名称：**显示 eDirectory 树的完整类型名。

6b **主题名称：**显示 eDirectory 树的完整类型名。

6c **有效期：**使用该下拉列表可指定证书的有效期。有效期最短为 6 个月，最长到公元 2036 年 （基于 32 位时间值的时间限制）。如果选择 “ 指定日期 ” 选项，则可编辑 “ 生效日期 ” 和 “ 失效日期 ” 字段，以创建自定义的有效期。选定的最大日期必须在 CA 的有效期内。

6c1 **生效日期：**使您可以显示或编辑证书有效的时间和日期。

6c2 **失效日期：**使您可以显示或编辑证书无效的时间和日期。

6d **自定义扩展：**使证书服务器支持要在创建证书时包含的任何标准扩展或自定义扩展。必须已经提前创建扩展并将其存储在文件中 （一个文件中存储一个扩展）。任何扩展都必须采取 ASN.1 编码形式，如 IETF RFC 2459/3280 4.2 节所定义。

如果要在创建的证书中包含一个或多个自定义扩展，请单击 “ 新建 ”，然后浏览包含自定义扩展的文件并将其添加到证书中。重复此过程可添加多个扩展。

要删除自定义扩展文件，先将其选中，然后单击 图标。

7 从以下选项中选择相应的证书格式：

7a **二进制 DER 格式的文件：**此选项可以保存证书或将证书导出到文件名字段中显示的文件。默认情况下，证书文件以 .DER 扩展名导出到基于 Windows 的 Identity Console 工作站和基于 Linux 的 Identity Console 工作站的用户主目录中的驱动器 C: 的根目录。

7b **Base64 格式的文件：**此选项可以将 CSR 保存到或将证书导出到文件名字段中显示的文件。默认情况下，证书和 CSR 文件以 .B64 扩展名导出到基于 Windows 的 Identity Console 工作站和基于 Linux 的 Identity Console 工作站的用户主目录中的驱动器 C: 的根目录。

7c **CER 格式的文件：**此选项可以将 CSR 保存到或将证书导出到文件名字段中显示的文件。默认情况下，证书和 CSR 文件以 .CER 扩展名导出到基于 Windows 的 Identity Console 工作站和基于 Linux 的 Identity Console 工作站的用户主目录中的驱动器 C: 的根目录。

8 在下一个屏幕中查看证书摘要，然后单击确定。

9 此时显示一条确认讯息，指示成功颁发证书。

图 17-6 颁发公共密钥证书

管理 SAS Service 对象

SAS Service 对象可以促进服务器与其服务器证书之间的通信。如果从 eDirectory 树中去除某个服务器，还需要删除与该服务器关联的 SAS Service 对象。如果要将服务器放回树中，必须创建与该服务器关联的 SAS Service 对象。否则，您无法创建新的服务器证书。

作为服务器运行状况检查的一部分，自动创建 SAS Service 对象。您不需要手动创建该对象。

仅当与服务器对象相同的容器中没有正确命名的 SAS Service 对象时，才可以创建新的 SAS Service 对象。例如，对于名为 WAKE 的服务器，将有一个名为 SAS Service - WAKE 的 SAS Service 对象。该实用程序会将 DS 指针从服务器对象添加到 SAS 对象，从 SAS 对象添加到服务器对象，以及对 SAS Service 对象设置正确的 ACL 条目。

如果已存在相应名称的 SAS Service 对象，则无法创建新的 SAS Service 对象。旧 SAS Service 对象的 DS 指针可能错误或丢失，或者 ACL 可能不正确。在这种情况下，可以删除损坏的 SAS Service 对象并使用 Identity Console 门户创建一个新的 SAS Service 对象。

创建或删除 SAS Service 对象

要创建或删除 SAS Service 对象，执行下列操作：

1. 在 Identity Console 登录页中单击证书管理 > **SAS Service 对象**选项。
2. 如果没有为现有服务器创建的 SAS Service 对象，则单击 ＋ 图标以创建新服务对象。
3. 此时显示一条确认讯息，指示已成功创建 SAS Service 对象。
4. 要去除 SAS Service 对象，单击 🗑 图标。
5. 在确认屏幕中单击确定以成功去除 SAS Service 对象。

图 17-7　管理 SAS Service 对象

18 管理鉴定框架

使用鉴定模块可以执行以下任务：

管理登录和登录后方法和顺序

NMAS 包括支持来自 NetIQ 和第三方鉴定开发人员的一些登录和登录后方法。一些登录方法需要其它硬件和软件。确保您拥有所有必要的硬件和软件，以实现您将要使用的方法。

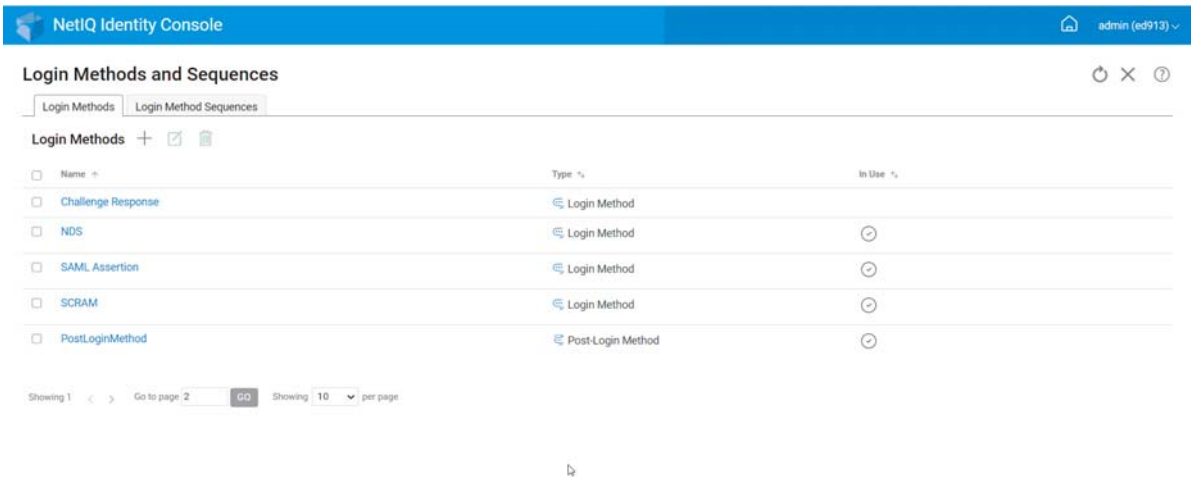
本部分介绍了如何安装、设置和配置 NMAS 的登录和登录后方法和顺序。

安装登录或登录后方法

要安装登录方法，执行以下任务：

1. 单击 Identity Console 登录页中的**鉴定管理** > **登录方法和顺序**选项。
2. 单击 + 图标安装新的登录方法。
3. 浏览并选择要安装的登录方法 (.zip) 文件，然后单击**下一步**。
4. 按照安装向导完成登录方法安装过程。

图 18-1 安装新登录方法



更新现有登录或登录后方法

要更新现有登录方法，执行下列操作：

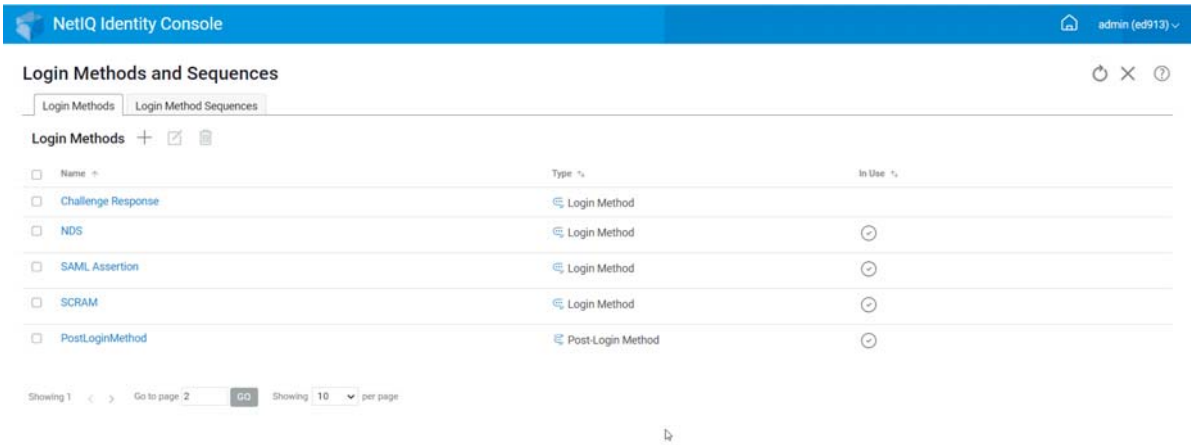
1 单击 Identity Console 登录页中的鉴定管理 > 登录方法和顺序选项。

2 从列表中选择要更新的登录方法，然后单击 ☑ 图标。

3 浏览并选择要更新的登录方法 (.zip) 文件，然后单击下一步。

4 按照更新向导完成登录方法的更新。

图 18-2 更新现有登录方法



卸装登录或登录后方法

要卸装登录或登录后方法，执行下列操作：

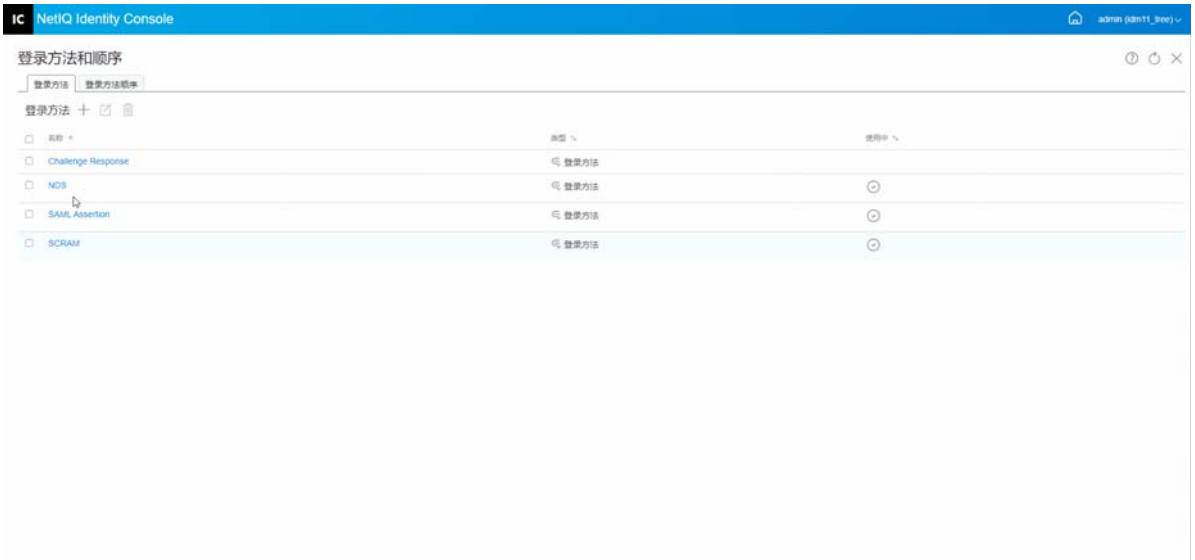
1 单击 Identity Console 登录页中的鉴定管理 > 登录方法和顺序选项。

2 从列表中选择要卸装的登录方法，然后单击 图标。

3 在下一个屏幕上，单击确定。

4 此时出现一条确认讯息，指示已卸装登录方法。

图 18-3 卸装登录方法



创建新的登录方法顺序

为您的环境创建了不同的登录方法后，您可以决定使用这些方法的顺序。要创建新的登录方法顺序，执行下列操作：

1 单击 Identity Console 登录页中的鉴定管理 > 登录方法和顺序选项。

2 选择登录方法顺序选项卡。

3 单击 ＋ 图标创建新的登录方法顺序。

4 指定名称并选择顺序类型。

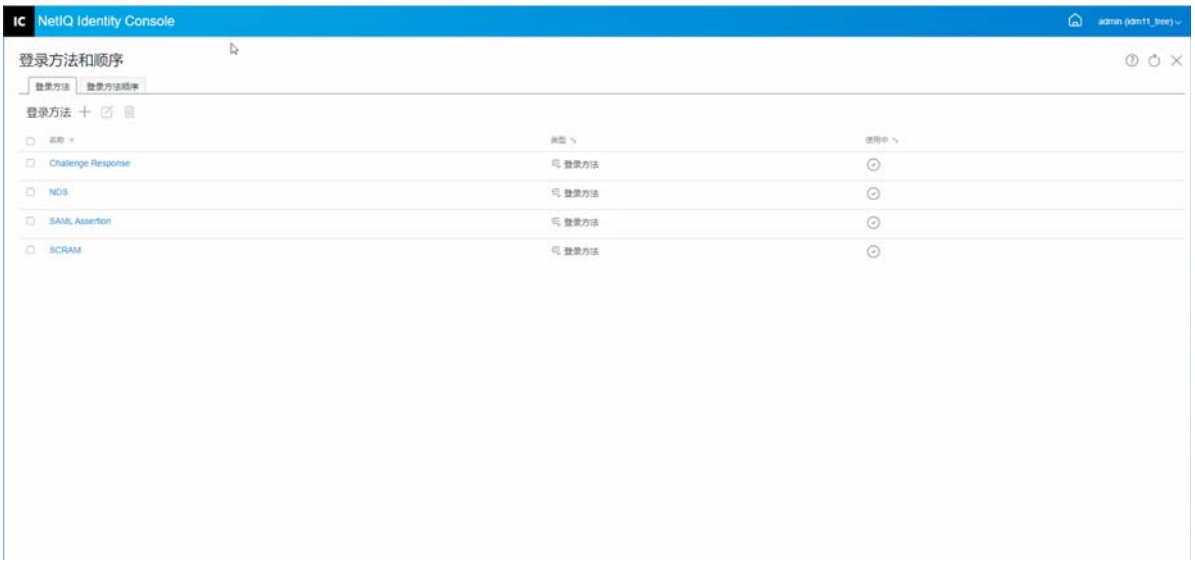
5 从可用的登录和登录后方法列表中选择所需的登录和登录后方法。

注释：您可以通过单击登录方法对象上显示的上下箭头来决定登录方法的顺序。

6 单击创建按钮。

7 此时出现一条确认讯息，指示已成功创建新的登录方法顺序。

图 18-4 创建登录方法顺序



修改登录方法顺序

要修改现有的登录方法顺序，执行下列操作：

1 单击 Identity Console 登录页中的鉴定管理 > 登录方法和顺序选项。

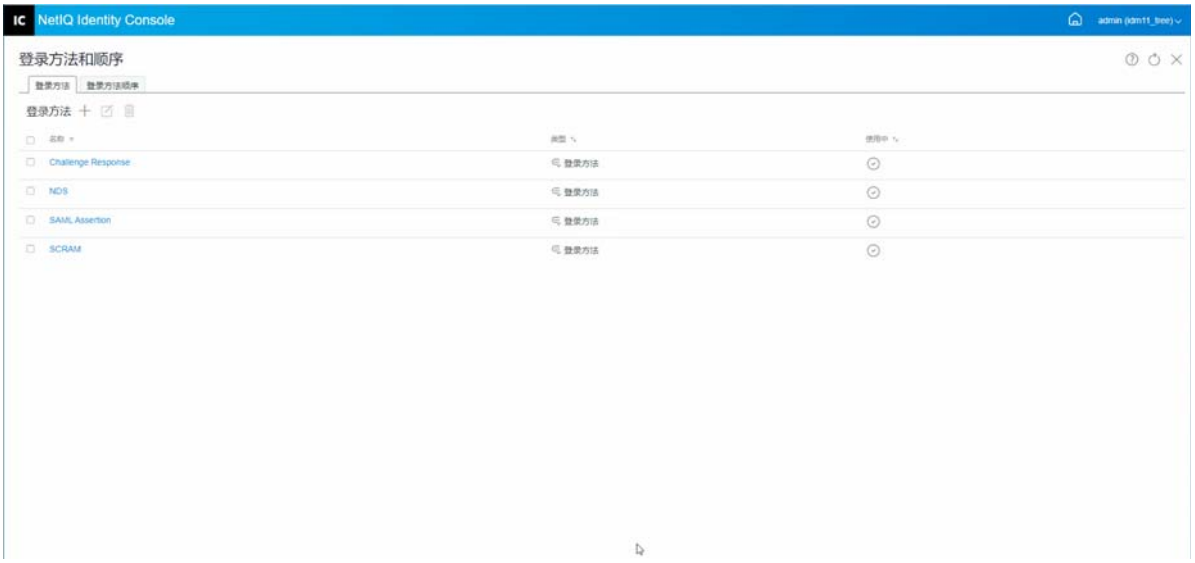
2 选择登录方法顺序选项卡。

3 单击 ☑ 图标修改现有登录方法顺序。

4 在修改登录方法顺序页面中进行必要的更改，然后单击保存。

5 此时出现一条确认讯息，指示已成功修改登录方法顺序。

图 18-5 修改登录方法顺序



授权或取消授权登录方法顺序

应授权登录方法顺序并将其设置为默认值，以便将其与用户、容器和分区关联起来。要授权登录方法顺序，执行下列操作：

1 单击 Identity Console 登录页中的鉴定管理 > 登录方法和顺序选项。

2 选择登录方法顺序选项卡。

3 从列表中选择相应的登录方法顺序，然后单击 ⊙ 图标。

4 要取消登录方法顺序的授权，选择登录方法顺序并单击 ⊗ 图标。

5 或者，您还可以授权或取消授权登录方法顺序列表中授权列下的下拉菜单中的登录方法顺序。

图 18-6 授权或取消授权登录方法顺序

设置默认登录方法顺序

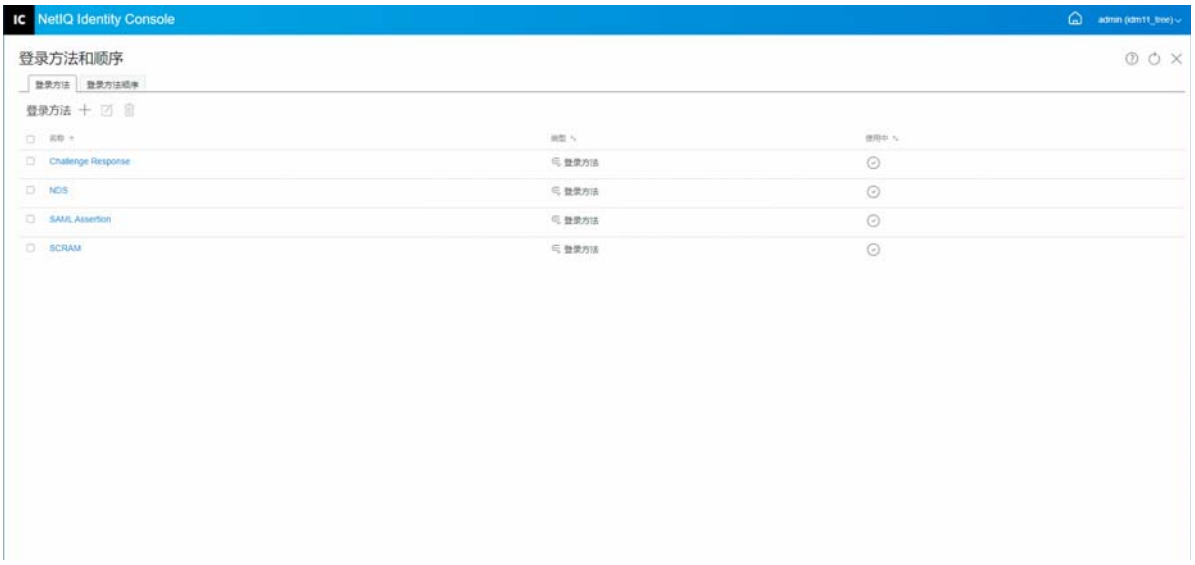
要设置默认登录顺序，以便用户在登录时不需要指定登录顺序：

1 单击 Identity Console 登录页中的鉴定管理 > 登录方法和顺序选项。

2 选择登录方法顺序选项卡。

3 启用 ⊗ 图标将授权登录方法顺序设置为默认。

图 18-7 设置默认登录方法顺序



删除登录方法顺序

要删除登录方法顺序：

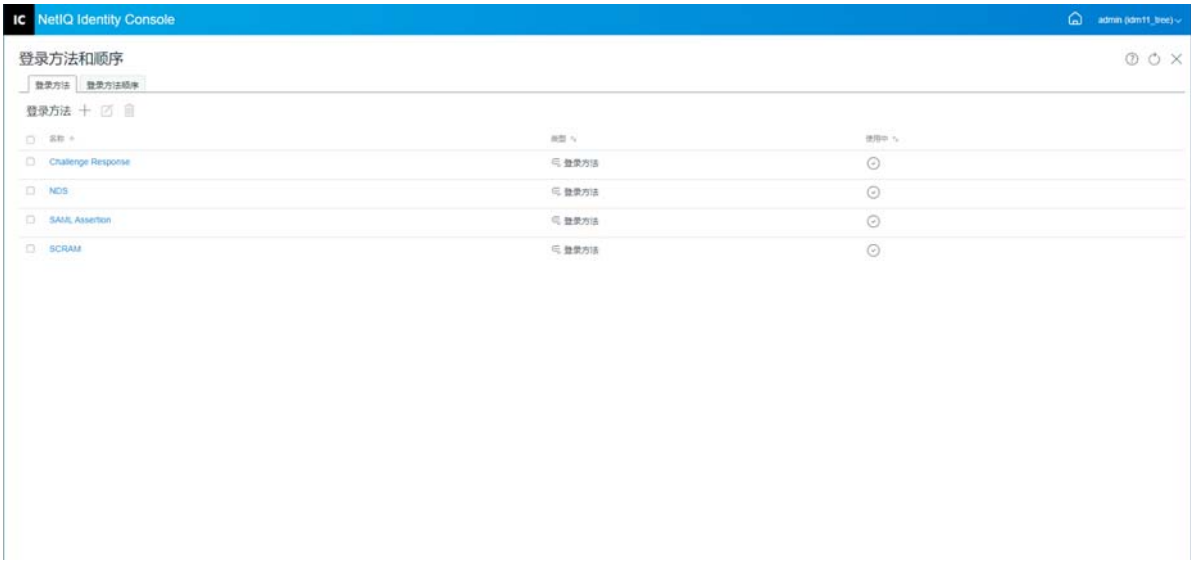
1 单击 Identity Console 登录页中的鉴定管理 > 登录方法和顺序选项。

2 选择登录方法顺序选项卡。

3 从列表中选择相应的登录方法顺序，然后单击 图标。

4 在下一个确认屏幕中单击确定。

图 18-8 删除登录方法顺序



管理口令策略

口令策略是管理员定义的规则集合，用于指定创建和替换最终用户口令的准则。 NMAS 使您能够实施您在 eDirectory 中指派给用户的口令策略。口令策略还可以包括忘记口令自助服务功能，以减少呼叫 Help Desk 解决忘记口令的问题。另一个自助功能是重设置口令自助服务，该功能允许用户在查看管理员在口令策略中指定的规则时更改其口令。用户通过 Identity Manager User Application 或 Identity Console 访问这些功能。

使用口令策略模块可以执行以下任务：

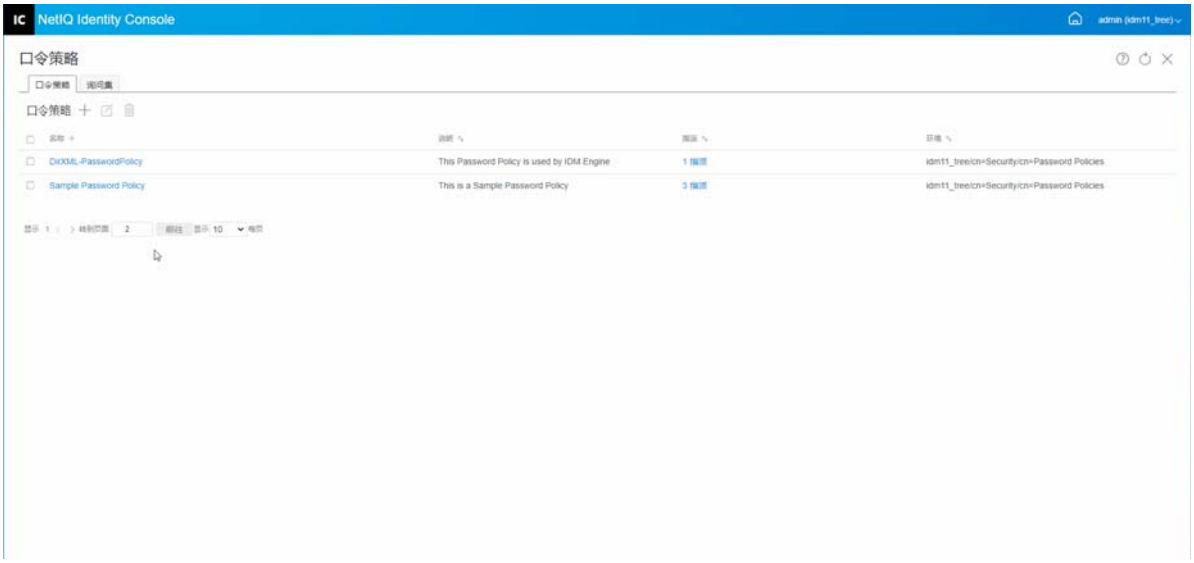
- 使用默认设置创建口令策略 （第 109 页）
- 使用自定义设置创建口令策略 （第 110 页）
- 修改口令策略 （第 112 页）
- 删除口令策略 （第 113 页）

使用默认设置创建口令策略

要创建新口令策略，执行下列操作：

1. 单击 Identity Console 登录页中的鉴定管理 > 口令策略选项。
2. 单击 ＋ 图标创建新的口令策略。
3. 在下一个屏幕中指定名称、环境、说明和口令更改讯息。
4. 如果想要通过默认设置创建口令策略，勾选基于默认设置创建新的口令策略框，然后单击下一步查看摘要页面。
5. 校验摘要页面中的细节，然后单击创建。
6. 此时显示一条确认讯息，指示已成功创建口令策略。

图 18-9 使用默认设置创建口令策略



使用自定义设置创建口令策略

要通过自定义设置创建口令策略，执行下列操作：

1 单击 Identity Console 登录页中的鉴定管理 > 口令策略选项。

2 单击 + 图标创建新的口令策略。

3 在下一个屏幕中指定名称、环境、说明和口令更改讯息。

4 如果想要通过自定义设置创建口令策略，单击下一步。

5 在配置页面中执行下列操作：

5a **启用通用口令：**启用策略的通用口令，使您可以使用口令策略功能中的选项。但是，在为策略启用通用口令之前，您的环境必须满足通用口令的先决条件。

5b **启用高级口令规则：**此选项启用在高级口令规则中找到的口令规则。这些规则通过允许您控制某些准则，如口令有效期和口令内容 （如字母、数字、大写或小写字母、特殊字符的组合）来帮助您保护环境。可以排除您认为不安全的口令，例如，您的公司名称。

5c **口令同步：**这些选项决定通用口令在 eDirectory 内如何与其他类型的身份库口令同步。口令同步包含以下选项：

5c1 **设置口令时去除 NDS 口令：**如果选择此选项，设置通用口令时将禁用 NDS 口令。用户将无法使用通过 NDS 口令直接登录 （而不是与 NMAS 通信）的旧方法或实用程序。如果设置此选项，默认情况下，将禁用下一个选项设置口令时同步 NDS 口令。

5c2 **设置口令时同步 NDS 口令：**如果选择此选项，则在类似 Identity Console 的应用程序中设置通用口令时，将同时更改 NDS 口令。

5c3 **设置口令时同步简单口令：**此选项提供与使用简单口令和用户供应的 NetIQ 和第三方客户端的兼容性。

5c4 **设置口令时同步分发口令：**此选项可以确定元目录引擎是否可以在 eDirectory 中检索或设置用户通用口令。

5d **通用口令检索：**下列选项可用：

5d1 **允许用户检索口令：**允许用户代理检索口令。此选项决定 “ 忘记口令自助服务 ” 功能是否可以为用户取回口令，以便可以使用电子邮件将此口令发送给用户。如果不选择此选项，则 “ 忘记口令 ” 选项卡上口令策略中的相应功能将灰显。

5d2 **允许管理员检索口令：**如果有需要此选项的特定服务，勾选此框。 Identity Manager 不需要管理员检索口令。但是，某些第三方服务可能会利用此选项。

5d3 **允许以下人员检索口令：**通过单击 + 图标选择可以检索口令的相应用户。

5e **鉴定：**

5e1 **校验现有口令是否符合口令策略 （登录时校验）：**如果您正在部署新口令策略或更改现有策略的高级口令规则，并且您要确保现有口令符合新策略或更改过的规则时，则此选项十分有用。

如果选择此选项，当用户登录时，将检查口令以确保口令符合新建或修改过的口令策略中的高级口令规则。如果一个现有的口令不符合，则要求用户进行更改。

完成后，单击下一步。

6 高级口令规则通过允许您控制口令细节，如口令有效期、更改口令的频率和口令包含的内容等，来帮助您确保环境安全。

特殊字符是那些除了数字 （0-9）或字母字符的字符。

在高级口令规则页面中执行下列操作：

6a 您可以使用 Microsoft 复杂性策略（Microsoft Windows Server 2008 之前）、Microsoft Server 2008 口令策略或 Novell 语法管理口令语法设置。

6b 在向导中指定更改口令、口令有效期、口令长度和组成以及口令排除项所需的选项，然后单击下一步。

7 可以通过为忘记口令的用户启用忘记口令自助服务以降低 Help Desk 成本。用户可以通过 Identity Console 门户使用这些自助服务功能。在忘记口令页面中执行下列操作：

注释：如果启用 " 忘记口令 "，则还必须指定是否需要 " 询问集 " 来帮助用户登录。

7a **询问集：**如果使用询问集，用户在回答询问集问题之前无法使用忘记口令自助服务。为确保用户经提示通过 Identity Console 门户输入此信息，选择需要询问集选项。

7b **操作：**此选项卡下的可用选项使用户能够使用询问集和通用口令重设置口令，使当前口令或口令提示能够通过电子邮件发送，以及显示口令提示选项。

7c **鉴定：**勾选强制用户在鉴定时配置询问问题和 / 或提示框，以确保提示用户指定询问集或口令提示。

完成后，单击下一步。

8 只有将策略指派给一个或多个对象后，策略才会生效。为简化管理，我们建议在树中尽可能高的位置指派策略。口令策略可指派给以下对象：

8a **登录策略对象：**我们建议您为树中的所有用户创建默认口令策略，并指派给位于安全性容器中的登录策略对象。

8b **是分区根的容器：**如果将策略指派给是分区根的容器，则该分区中的所有用户，包括子容器的用户在内，都将继承策略指派。

8c **不是分区根的容器：**如果将策略指派给不是分区根的容器，则仅在该特定容器中保存的用户会继承策略指派。子容器中保留的用户不继承策略。

要将策略应用于不是分区根的容器下的所有用户，将策略分别指派给每个子容器。

8d **用户：**可以将策略指派给一个或多个用户。

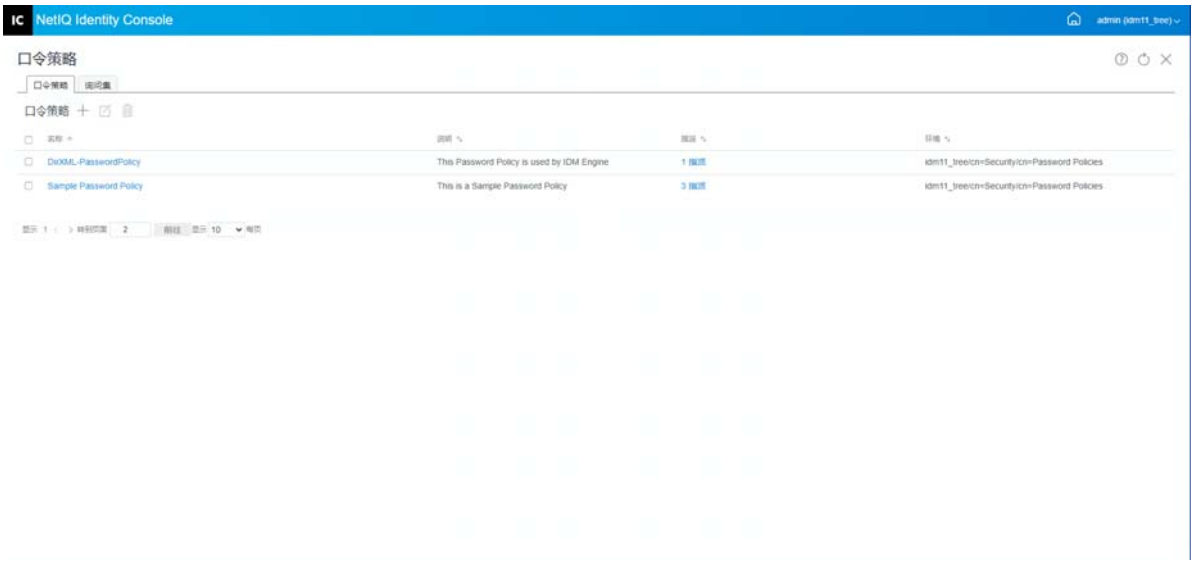
要指派策略，单击 + 图标。浏览并选择相应的对象以指派口令策略。

如果想要去除策略关联，从列表中选择策略并单击 🗑 图标。

9 校验摘要页面中的细节，然后单击创建。

10 此时显示一条确认讯息，指示已成功创建口令策略。

图 18-10 使用自定义设置创建口令策略



修改口令策略

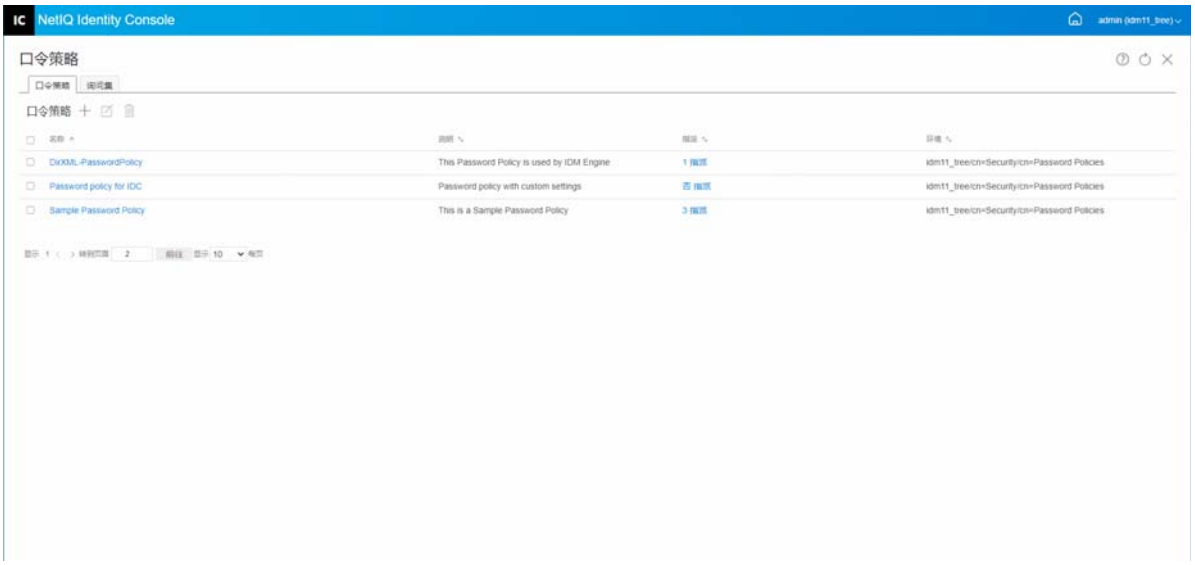
要修改现有口令策略，执行下列操作：

1 单击 Identity Console 登录页中的鉴定管理 > 口令策略选项。

2 从列表中选择相应口令策略并单击 ☑ 图标。

3 在修改口令策略页面中进行必要的更改，然后单击保存。

图 18-11 修改口令策略



删除口令策略

要删除口令策略，执行下列操作：

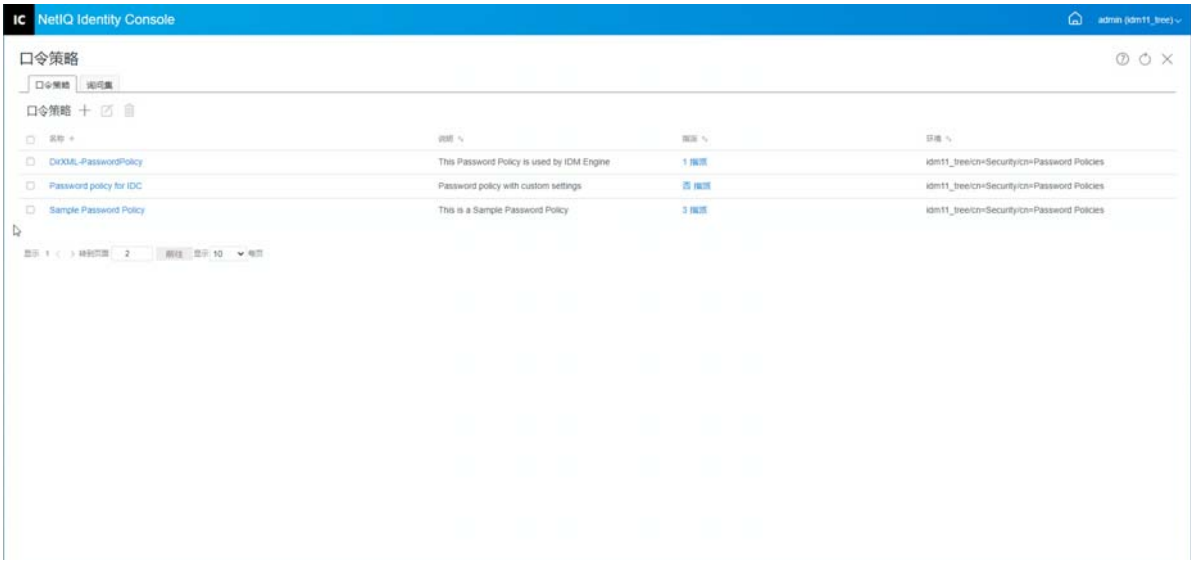
1 单击 Identity Console 登录页中的鉴定管理 > 口令策略选项。

2 从列表中选择相应口令策略并单击 图标。

3 在下一个警告屏幕中，单击确定。

4 此时显示一条确认讯息，指示已删除口令策略。

图 18-12 删除口令策略



管理询问集

询问集是用户为了验证身份而要回答的一个或多个问题。询问集是口令自助服务的一部分。

当用户忘记了口令或在使用口令方面遇到问题时，可以使用口令自助服务，而不用呼叫 Help Desk。询问集使用户能够验证身份，然后通过电子邮件接收提示或口令，或使用 Web 浏览器重设置口令。

您可以允许用户创建并回答他们自己的问题，或要求用户回答由您创建的问题。

询问集页面允许您搜索现有询问集；创建新的询问集；以及编辑现有询问集。

- 创建新的询问集 （第 114 页）
- 修改询问集 （第 114 页）
- 删除询问集 （第 115 页）

创建新的询问集

要创建新询问集，执行下列操作：

1 单击 Identity Console 登录页中的鉴定管理 > 口令策略 > 询问集。

2 单击 ＋ 图标以创建新的询问集。

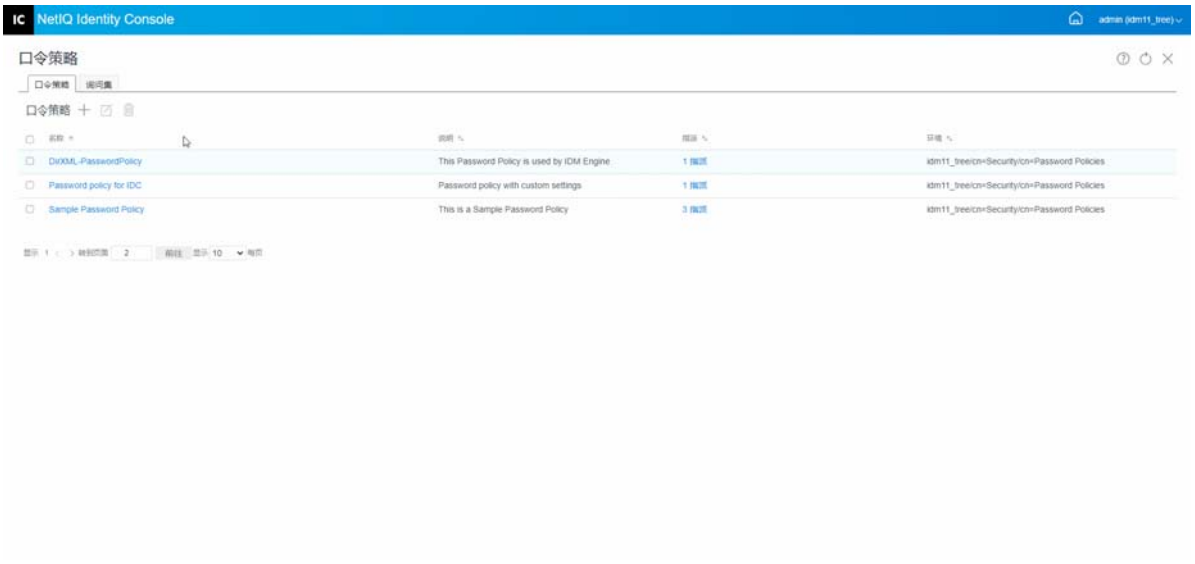
3 指定询问集对象的名称，并选择应创建询问集的容器或子容器。

4 创建一组为检索用户口令而要询问的一组问题。您也可以从现有的随机问题集中进行选择。

5 设置要提出的问题数量，然后单击创建。

6 此时显示一条确认讯息，指示已成功创建询问集。

图 18-13　创建询问集



修改询问集

要修改现有询问集，执行下列操作：

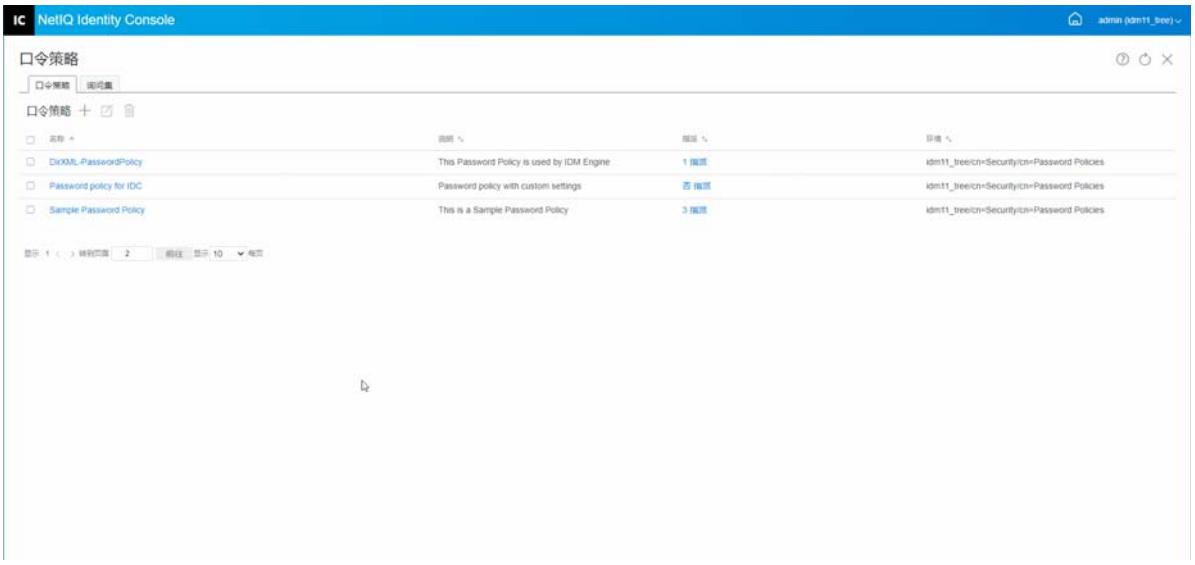
1 单击 Identity Console 登录页中的鉴定管理 > 口令策略 > 询问集。

2 从列表中选择相应的询问集并单击 ☑ 图标。

3 在修改询问集页面中进行必要的更改，然后单击保存。

4 此时显示一条确认讯息，指示已成功修改询问集。

图 18-14 修改询问集



删除询问集

要删除询问集，执行下列操作：

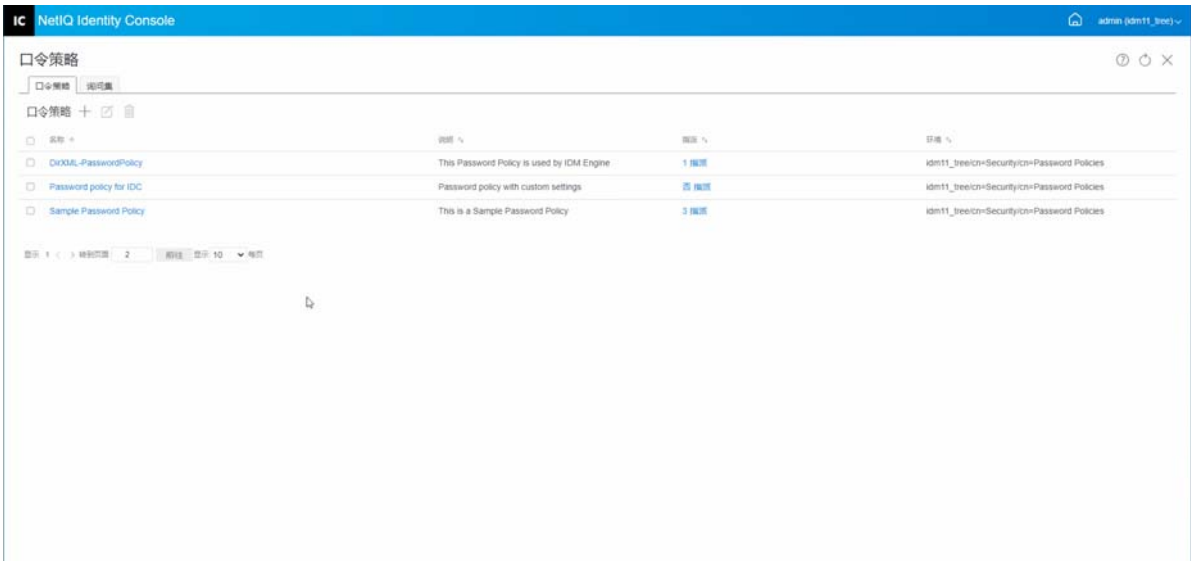
1 单击 Identity Console 登录页中的鉴定管理 > 口令策略 > 询问集。

2 从列表中选择所需的询问集并单击 图标。

3 在确认屏幕中单击确定。

4 此时显示一条确认讯息，指示已成功删除询问集。

图 18-15 删除询问集



19 管理 SNMP 组对象

简单网络管理协议 (SNMP) 是因特网的标准操作和维护协议，用于在管理控制台应用程序和托管设备之间交换管理信息。

使用 SNMP 模块可以执行以下任务：

- 创建 SNMP 组对象 （第 117 页）
- 修改 SNMP 组对象 （第 118 页）
- 删除 SNMP 组对象 （第 118 页）

创建 SNMP 组对象

要创建 SNMP 组对象，执行下列操作：

1. 在 Identity Console 登录页中单击 **SNMP** 模块。
2. 单击 ＋ 图标创建新的 SNMP 组对象。
3. 指定名称并选择环境以创建新的 SNMP 组对象。
4. 单击**创建**按钮。
5. 屏幕中会显示一条讯息，确认已成功创建 SNMP 组对象。

图 19-1 创建 SNMP 组对象

修改 SNMP 组对象

要修改 SNMP 组对象，执行下列操作：

1 在 Identity Console 登录页中单击 **SNMP** 模块。

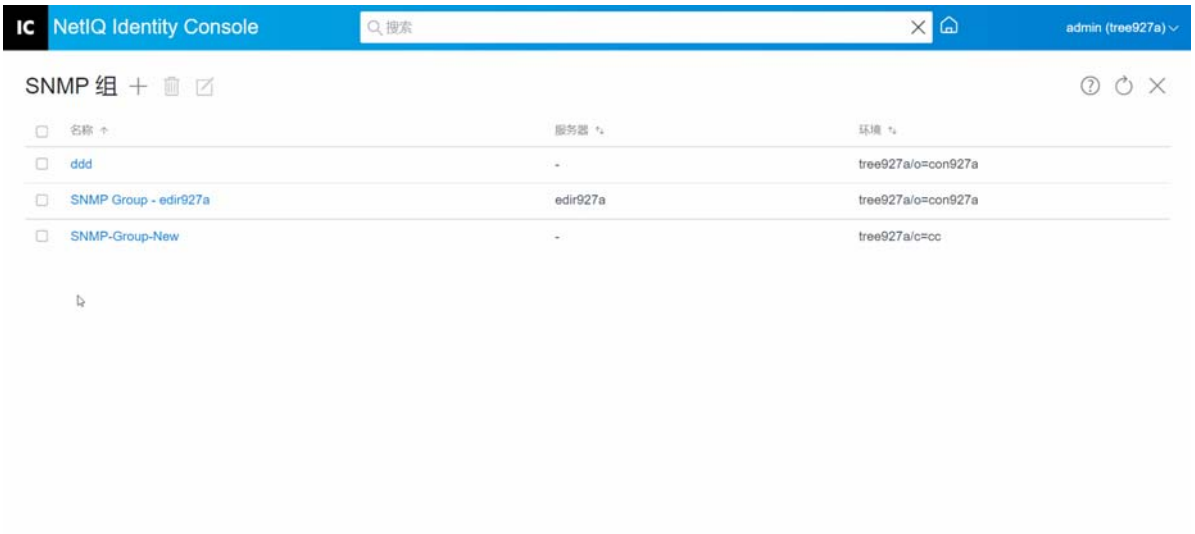
2 选择要修改的 SNMP 组对象并单击 图标。

3 在一般 / 陷阱页面中修改可配置参数。

4 完成后，单击保存按钮。

5 屏幕中会显示一条讯息，确认已成功修改 SNMP 组对象。

图 19-2 修改 SNMP 组对象



删除 SNMP 组对象

要删除 SNMP 组对象，执行下列操作：

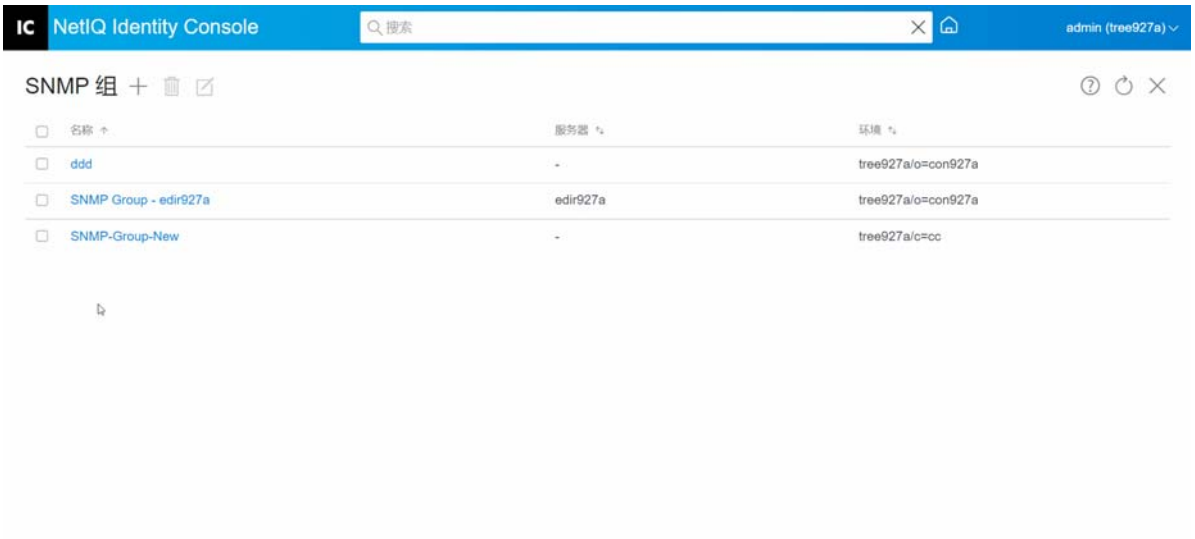
1 在 Identity Console 登录页中单击 **SNMP** 模块。

2 选择要修改的 SNMP 组对象并单击 图标。

3 在下一个屏幕中单击确定。

4 屏幕中会显示一条讯息，确认已成功删除 SNMP 组对象。

图 19-3 删除 SNMP 组对象



20 管理增强的后台鉴定

要从 Identity Console 的 EBA 插件访问 eDirectory，您的树中必须有一个启用了 EBA 的服务器，并且带有效的 eba.p12 文件。有关如何在 eDirectory 树中启用 EBA 的更多信息，请参见 *《NetIQ eDirectory Administration Guide》*（NetIQ eDirectory 管理指南）中的 Enabling EBA on an eDirectory Tree （在 eDirectory 树中启用 EBA）。

注释：如果您想将 EBA 模块与 Identity Console 结合使用，则必须将 eDirectory 服务器升级到 9.2.4 HF2。

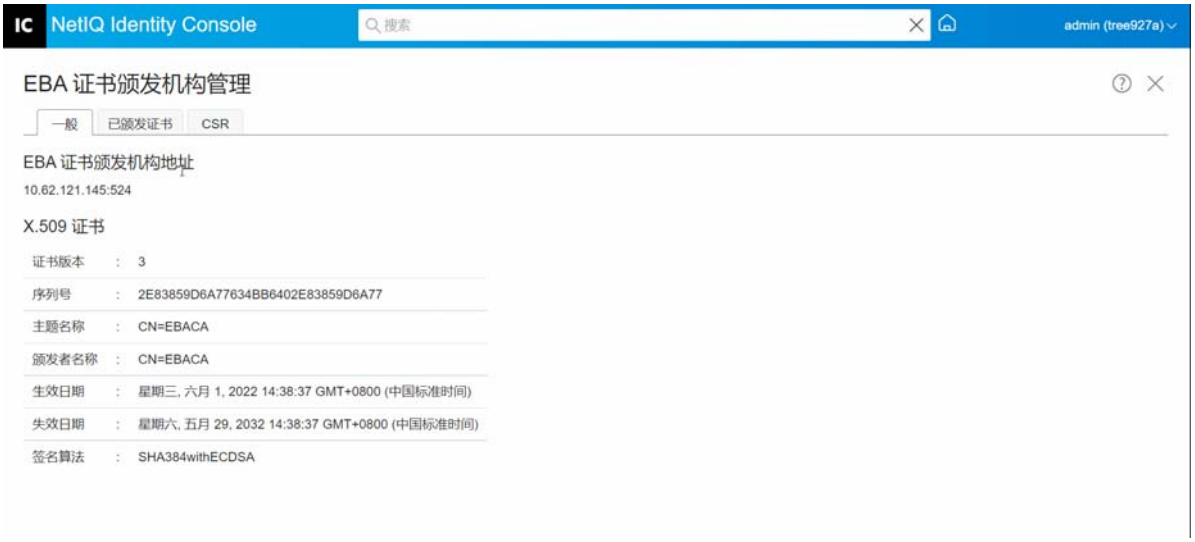
要打开 EBA 证书颁发机构管理页面，登录到 Identity Console 门户并单击 **EBA** 模块。

EBA 证书颁发机构管理页面包括以下选项卡，以管理 EBA 证书颁发机构的不同方面：

- **常规：**显示 EBA CA 及其证书的 IP 地址。
- **已颁发证书：**显示 NCP CA 证书及其 IP 地址和端口。

  若要撤消证书，选择证书，然后单击 ⊘。仅在极端情况下使用此选项，因为拥有 NCP 证书颁发机构证书的服务器在被撤消证书时将变得不起作用。通常，当服务器遭到破坏时，才有必要撤消证书。
- **CSR：**列出等待管理员批准的证书签名请求。要批准证书签名请求，从列表中选择证书并单击**批准**。

图 20-1 *管理增强的后台鉴定*



II 使用 Identity Console 管理 Identity Manager

本部分介绍了您使用 Identity Console 门户管理 Identity Manager 服务器可以执行的任务。

21 管理驱动程序和驱动程序集

驱动程序集是一个可容纳多个 Identity Manager 驱动程序的容器。在任何时候，一台服务器上只能有一个驱动程序集处于活动状态。因此，所有活动的驱动程序都必须分在同一驱动程序集中。可以使用 Designer 工具创建驱动程序集。有关详细信息，请参见 《*NetIQ Designer for Identity Manager Administration Guide*》（NetIQ Designer for Identity Manager 管理指南）中的 Configuring Driver Sets （配置驱动程序集）。

添加或删除服务器

一个驱动程序集每次可以与一个或多个服务器关联。但是，根据您的需求，您可以将不同的驱动程序集对象关联到可用的服务器。

要添加新服务器，单击特定驱动程序集对象的 ⋮ 图标 > 选择**添加服务器**，然后从环境浏览器中选择相应的服务器。

要删除现有服务器，选择**去除服务器**选项。

图 21-1 将服务器添加到驱动程序集

使用产品激活密钥激活驱动程序集

在使用任何驱动程序集以及驱动程序集中驻留的驱动程序之前，必须使用电子邮件 ID 中收到的激活代码将其激活。购买许可证后，您将收到来自 NetIQ 的激活密钥。使用激活密钥执行下列操作以激活驱动程序集：

1 单击 Identity Console 主屏幕中的 **IDM 管理**选项卡。

2 单击要激活的特定驱动程序集框上的操作图标 ⋮ 并单击**激活安装**。

   应用 " 激活 " 时， "IDM 管理 " 磁贴中的每个驱动程序集选项卡都显示与该驱动程序集关联的所有服务器的激活信息。此信息有助于确定激活何时失效。

3 如果已将激活文件下载到计算机中，勾选复选框**选择一个包含身份凭证的文件**。

4 浏览并选择激活文件，然后单击**提交**。

5 或者，您可以使用激活文件的内容激活驱动程序集。勾选复选框**输入身份凭证**。

   5a 打开产品激活身份凭证文件，然后将其内容复制到剪贴板。

   5b 如果选择复制内容，不要包含任何多余的行或空格。应从身份凭证的第一个破折号 (-) 开始复制 (----BEGIN PRODUCT ACTIVATION CREDENTIAL)，一直复制到其最后一个破折号 (-) (END PRODUCT ACTIVATION CREDENTIAL-----) 并单击**完成**。

6 此时显示一条确认讯息，指示已成功激活驱动程序集。

图 21-2 激活驱动程序集

查看驱动程序集的激活信息

激活驱动程序集后，您必须校验已成功激活驱动程序集。要进行校验，执行下列操作：

1 单击 Identity Console 主屏幕中的 **IDM 管理**选项卡。

2 单击要校验激活信息的特定驱动程序集对象上的操作图标 ⋮，然后单击**激活信息**。

3 计算机中弹出与激活相关的信息窗口。您可以校验此页面中特定驱动程序集的激活细节。

图 21-3 查看驱动程序集的激活信息

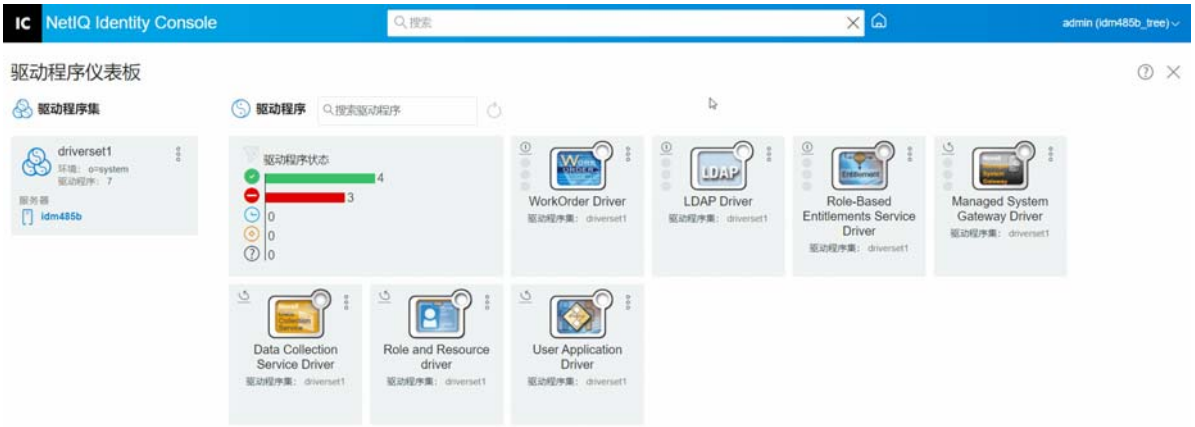
启动和停止驱动程序

创建驱动程序时，默认停止驱动程序。要使驱动程序运行，必须启动驱动程序。 Identity Manager 是事件驱动型系统，因此启动驱动程序后，事件发生前，它一直处于空闲状态。执行下列操作以启动 / 停止驱动程序。

1 单击 Identity Console 主屏幕中的 **IDM 管理**选项卡。
2 单击计算机屏幕右侧的特定驱动程序集对象以显示与之关联的所有驱动程序。
3 单击特定驱动程序上的操作图标 ⋮，然后选择**启动驱动程序**。
4 要停止驱动程序对象，单击特定驱动程序上的操作图标 ⋮，然后选择**停止驱动程序**。
5 （可选）或者，您可以同时启动或停止驻留在同一驱动程序集对象中的所有驱动程序。

   单击驱动程序集对象上的操作图标 ⋮，然后选择**启动所有驱动程序**或**停止所有驱动程序**。

图 21-4 启动和停止驱动程序



搜索驱动程序

Identity Console 提供在服务器中搜索特定驱动程序的选项。要搜索驱动程序，执行下列操作：

1 单击 Identity Console 主屏幕中的 **IDM 管理**选项卡。
2 在**搜索框**中指定驱动程序的名称。计算机屏幕中将显示特定驱动程序对象。您还可以通过单击 ↻ 图标来刷新驱动程序列表。

图 21-5 搜索驱动程序

过滤驱动程序和驱动程序集

可以从 **IDM 管理**页面根据驱动程序状态过滤驱动程序。要过滤驱动程序：

1 单击 Identity Console 主屏幕中的 **IDM 管理**选项卡。

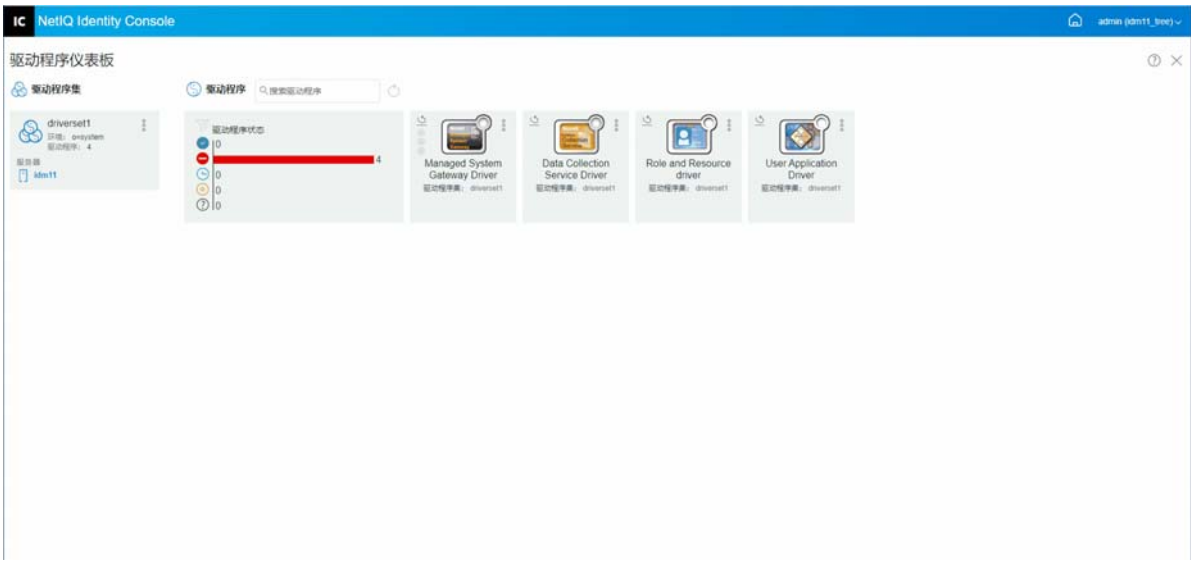
2 单击 **Drivers' Status** （驱动程序状态）磁贴上的以下图标，根据驱动程序的状态过滤出驱动程序：

- 单击 图标可以过滤出服务器中所有正在运行的驱动程序。
- 单击 图标可以过滤出服务器中所有停止的驱动程序。
- 单击 图标可以过滤出所有正在启动的驱动程序。
- 单击 图标可以过滤出所有正在停止的驱动程序。
- 单击 图标可以过滤出没有关联状态的所有驱动程序。当驱动程序集没有关联服务器时，驻留在该驱动程序集中的驱动程序将显示**未知**状态。

要清除已应用于驱动程序的任何过滤器，单击 **Drivers' Status** （驱动程序状态）磁贴上显示的 图标。

3 也可以使用 Identity Console 门户过滤驱动程序集。默认情况下， Identity Console 门户将显示与服务器中所有驱动程序集关联的所有驱动程序。如果您想查看特定驱动程序集下的驱动程序，则必须从 Identity Console 门户左侧的驱动程序集列表中选择相应的驱动程序集。要清除选择的驱动程序集，再次单击选定的驱动程序集。

图 21-6 过滤驱动程序和驱动程序集



删除驱动程序集

要删除驱动程序集，执行下列操作：

1 单击 Identity Console 主屏幕中的 **IDM 管理**选项卡。

2 单击要删除的相应驱动程序集上的操作按钮 ⋮。

3 选择 **“ 删除 ”**。

驱动程序操作

单击单个驱动程序磁贴上的操作图标 ⋮ 支持下列操作：

- **启动驱动程序**：可以启动驱动程序
- **停止驱动程序**：可以停止驱动程序
- **重启动驱动程序**：可以重启动已停止的驱动程序
- **删除驱动程序**：可以删除驱动程序
- **统计数字**：可以查看驱动程序的性能统计数字
- **复制数据**：可以将驱动程序的数据从一台服务器复制到另一台服务器。此选项仅适用于多服务器环境。

22 管理驱动程序集属性

本部分提供所有驱动程序集通用属性信息。这包括所有属性 （命名口令、日志级别、驱动程序集检查器等）。

本部分包括以下类别：

配置驱动程序集

要修改驱动程序集的配置，执行下列操作：

1. 单击 **IDM 管理** > **单击相应驱动程序集的环境菜单 （三个点）** > **驱动程序集属性**。
2. 默认情况下，将显示**驱动程序集配置**页面。驱动程序集配置选项分为以下类别：

命名口令

Identity Manager 允许您为驱动程序集安全存储多个口令。此功能称为 “ 命名口令 ”。通过密钥或名称访问每个不同的口令。

您可以向驱动程序集或单个驱动程序添加命名口令。驱动程序集中的所有驱动程序都可以使用该驱动程序集的命名口令。

若要在驱动程序策略中使用命名口令，应使用其名称来引用该口令，而不要使用实际口令，Identity Manager 引擎会将此口令发送至驱动程序。本部分描述的储存和检索命名口令的方法可用于任何驱动程序，无需对驱动程序 Shim 进行更改。

可以通过选择**驱动程序集配置**下的 **IDM 管理** > **单击相应驱动程序集的环境菜单 （三个点）** > **驱动程序集属性** > **命名口令**来访问命名口令。

要添加新的命名口令，单击 ＋ 图标。要去除现有命名口令，选择相应口令并单击 🗑 图标。

全局配置值

显示全局配置对象的有序列表。对象包含 Identity Manager 启动时加载的驱动程序的扩展 GCV 定义。您可以添加或去除 " 全局配置 " 对象，也可以更改执行对象的顺序。单击 图标以保存 GCV。要刷新 GCV 列表，单击 图标。

配置 Java 环境参数

要配置 Java 环境参数，执行下列操作：

1 在 Identity Console 中，选择 **IDM 管理** > **单击相应驱动程序集的环境菜单 （三个点）** > **驱动程序集属性**。

2 单击**驱动程序集配置**下的 **Java 环境参数**以显示包含 Java 环境参数的属性页面。

3 根据需要修改下列设置：

类路径附加部分：指定使 JVM 搜索包 (.jar) 和类 (.class) 文件的其他路径。使用此参数与使用 java -classpath 命令相同。输入多个类路径时，对于 Windows JVM，使用分号 (;) 分隔它们，对于 UNIX 或 Linux JVM，使用冒号 (:) 分隔它们。

JVM 选项：指定要用于 JVM 的其他选项。参阅您的 JVM 文档以了解有效的选项。

DHOST_JVM_OPTIONS 是相应环境变量。它指定了 JVM 1.2 的参数。例如：

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

每个选项字符串都由空格隔开。如果选项字符串包含空格，则必须用双引号引起来。

驱动程序集属性选项优先于 DHOST_JVM_OPTIONS 环境变量。此环境变量附加在驱动程序集属性选项的末尾。

初始堆大小：指定 JVM 可用的初始 （最小）堆大小。增加初始堆大小可以减少启动时间并提高吞吐量性能。使用数字值，后跟 G、 M 或 K。如果没有指定字母大小，大小将默认为字节。使用此参数与使用 Java -Xms 命令相同。

DHOST_JVM_INITIAL_HEAP 是相应环境变量。它以十进制字节数指定初始 JVM 堆大小。此参数优先于驱动程序集属性选项。

参阅 JVM 文档以获取有关 JVM 默认初始堆大小的信息。

最大堆大小：指定 JVM 可用的最大堆大小。使用数字值，后跟 G、 M 或 K。如果没有指定字母大小，大小将默认为字节。使用此参数与使用 java -Xmx 命令相同。

DHOST_JVM_MAX_HEAP 是相应的环境变量。它以十进制字节数指定最大 JVM 堆大小。此参数优先于驱动程序集属性选项。

参阅 JVM 文档以获取有关 JVM 默认最大堆大小的信息。

4 单击 以保存您的更改。

5 重启动身份库以应用更改。

管理已赋值属性列表

要将属性添加到特定驱动程序集的已赋值属性列表中，执行下列操作：

1 在 Identity Console 中，选择对象管理模块。

2 从下拉列表中选择 **DirXML-DriverSet** 类型，然后单击 “ 搜索 ” 按钮。

3 单击搜索列表中的相应驱动程序集。

4 要将未赋值属性添加到已赋值属性列表中，单击已赋值属性旁边的 ＋ 图标，并从列表中选择相应的未赋值属性。

5 完成后，单击确定。

图 22-1 管理驱动程序集配置参数

管理驱动程序集作业

Identity Console 允许您使用 “ 作业 ” 选项为驻留在相关驱动程序集中的所有驱动程序排定事件。

作业日程安排器页面包括作业名称，作业是启用的还是禁用的，计划运行的时间，以及作业说明。单击作业名称打开 “ 作业 ” 页。在 “ 已启用 ” 列下单击启用 / 禁用图标以启用或禁用作业。单击作业说明以查看作业的完整说明。

通过选择 Identity Console 主页面中的 **IDM 管理** > 单击相应驱动程序集的环境菜单 （三个点）> 驱动程序集属性 > 高级选项卡来访问作业页面。作业选项卡包含一个表，显示选定驱动程序的现有作业对象，列出的选定驱动程序使用驱动程序项中的完整判别名。

作业日程安排器页面允许您执行以下任务：

- **创建作业**：单击 ＋ 图标以创建新作业。

  在**新建作业**弹出窗口中，要创建新作业，请执行以下步骤：

  1. 指定作业名。

2. 选择作业类型。
3. 单击 图标，然后从可用的服务器列表中选择要运行作业的服务器。否则，请指定服务器名称，然后选择服务器。
4. 单击创建按钮。

- **启动作业**：单击作业左侧的框选择作业，然后单击 图标。
- **停止作业**：单击作业左侧的框选择作业，然后单击 图标。
- **启用作业**：单击作业左侧的框选择作业，然后单击 图标。
- **禁用作业**：单击作业左侧的框选择作业，然后单击 图标。
- **获取状态**：单击作业左侧的框选择作业，然后单击 图标。
- **删除作业**：单击作业左侧的框选择作业，然后单击 图标。

单击作业打开 **Job Property** （作业属性）页。在此可以设置作业的运行方式。

一般：显示作业的 Java 类名。使用此页启用或禁用作业，在运行作业后删除作业，选择应该运行此作业的一个或多个服务器，指定电子邮件服务器和为作业指定不同的显示名称与说明。

日程表：允许您设置何时运行作业。指定 " 启动作业时间 " 以设置时间，以及是否每天、每周、每月、每年运行作业。还可以自定义要运行作业的时间，也可以选择启用切换开关以手动运行作业。

范围：允许您定义此作业适用的对象。对象可以是容器、动态组、组或叶对象。单击 " 添加 " 选择要应用此作业的对象。可以使用 " 浏览 " 按钮选择对象，然后单击 " 确定 "。要从范围列表中去除对象，请单击 DN 对象左侧的框选择范围对象，然后单击 " 去除 "。

当添加对象时，选择它将显示更多选项。如果选择组对象，则该选项只能将该作业应用到组成员或组。如果选择容器对象，则您可以选择只将该作业应用到此容器的所有后代或此容器的所有子代，或者仅应用到此容器。

参数：允许您向作业添加其他参数，并在参数设置后即可查看。这些参数因选定作业的类型而异。

结果：允许您定义如何处理作业结果。" 结果 " 页分成两部分：中间结果和最终结果 （允许有以下结果：" 成功 "、" 警告 "、" 错误 " 和 " 已中止 "）。" 结果 " 列的右侧是 " 操作 " 列。可以单击 " 操作 " 列来设置每个结果的通知方式。操作包含发送审计结果或在结果完成时发送电子邮件。如果没有选择选项，则对结果将不采取任何操作。

在**跟踪**选项卡中，可以为特定驱动程序配置跟踪。有关更多信息，请参见配置跟踪级别 （第 159 页）

管理特定驱动程序集库

库对象存储由一个或多个驱动程序共享的多个策略和其他资源。可以在驱动程序集对象或任何 eDirectory 容器中创建库对象。一个 eDirectory 树中可以有多个库。只要运行驱动程序的服务器持有库对象的读 / 写或主复本，驱动程序就可以引用树中的任何库。

样式表、策略、规则和其他资源对象可以存储在库中，并由一个或多个驱动程序参照。

使用库管理模块可以执行以下任务：

- 查看和删除现有库 （第 135 页）
- 查看和删除库中的对象 （第 135 页）

查看和删除现有库

要查看和删除现有库，执行下列操作：

1. 在 Identity Console 中，选择 **IDM 管理** > **单击相应驱动程序集的环境菜单 （三个点）** > **驱动程序集属性** > **高级** > **库**。
2. 在列表中选择相应的库。
3. 单击 图标。单击**确定**确认该操作。

查看和删除库中的对象

您可以查看和删除库对象中的策略以及映射表。要删除对象，执行下列操作：

1. 在 Identity Console 中，选择 **IDM 管理** > **单击相应驱动程序集的环境菜单 （三个点）** > **驱动程序集属性** > **高级** > **库**。
2. 单击列表中的相应库。
3. 要删除策略，选择**策略**选项卡。
4. 从列表中选择相应策略并单击 图标。
5. 要删除映射表，选择**映射表**选项卡。
6. 从列表中选择相应的映射表并单击 图标。
7. 单击**确定**确认该操作。

图 22-2 管理驱动程序集的作业和库

配置驱动程序集的日志和跟踪级别

要为您的驱动程序集配置日志和跟踪，从 Identity Console 主页中选择 **IDM 管理** > **单击相应驱动程序集的环境菜单 （三个点）** > **驱动程序集属性** > **日志和跟踪配置**选项卡。本部分包括以下类别：

- 配置日志级别 （第 136 页）
- 配置跟踪级别 （第 137 页）
- DirXML 脚本跟踪 （第 138 页）

配置日志级别

每个驱动程序集都有一个日志级别字段，您可以在此字段中定义应跟踪的错误级别。此处指定的级别将决定哪些讯息会记录到日志中。默认情况下，日志级别设置为跟踪错误讯息 （也包括严重讯息）。要跟踪其他讯息类型，更改日志级别。要配置日志级别，在 Identity Console 中选择 **IDM 管理** > **单击相应驱动程序集的环境菜单 （三个点）** > **驱动程序集属性** > **日志和跟踪配置** > **日志级别**。下表介绍了日志级别设置：

选项	描述
关闭对驱动程序集、订购者和发布者日志的日志记录	关闭驱动程序集对象、订购者通道和发布者通道上所有驱动程序的日志记录。
日志中的最大项数 (50-500)	日志中的项数。默认值是 50。

选项	描述

日志级别	可选择以下日志级别：
	◆ 记录错误：只记录错误
	◆ 记录错误和警告：记录错误和警告
	◆ 记录特定事件：记录已选事件。选择此选项可提供以下事件列表：
	  ◆ 元目录引擎事件
	  ◆ 状态事件
	  ◆ 操作事件
	  ◆ 转换事件
	  ◆ 身份凭证供应事件
	◆ 仅更新上次日志时间：更新上次日志时间。
	◆ 日志记录关闭：为驱动程序关闭日志记录。

配置跟踪级别

您可以为特定驱动程序集配置跟踪。根据为驱动程序集指定的跟踪级别，引擎在处理事件时，跟踪显示与驱动程序相关的事件。驱动程序跟踪级别仅影响设置跟踪的驱动程序或驱动程序集。如果您正在使用 Remote Loader， Remote Loader 跟踪文件将直接设置在 Remote Loader 上，并且仅包含驱动程序 Shim 跟踪。

要为驱动程序集配置跟踪，选择 **IDM 管理** > 单击相应驱动程序集的环境菜单 （三个点） > 驱动程序集属性 > 日志和跟踪配置 > 跟踪选项卡。下表介绍了跟踪设置：

参数	驱动程序
跟踪级别	随着驱动程序跟踪级别的提高，“ 跟踪 ” 中显示的信息量也会增加。 跟踪级别 1 只显示错误，但不显示导致错误的原因。如果希望查看口令同步信息，将跟踪级别设置为 5。 如果选择使用驱动程序集的设置，将采用驱动程序集的值。
XSL 跟踪级别	跟踪显示 XSL 事件。仅在对 XSL 样式页查错时才设置此跟踪级别。如果不希望看到 XSL 信息，将级别设置为 0。
Java 调试端口	允许开发者挂接 Java 调试程序。附加 Java 调试程序后重启动身份库。
跟踪文件	指定文件名和为所选驱动程序写入 Identity Manager 信息的位置。 如果选择使用驱动程序集的设置，将采用驱动程序集的值。

参数	驱动程序
跟踪文件编码	跟踪文件使用系统的默认编码。如果需要，您可以指定其他编码。 如果选择使用驱动程序集的设置，将采用驱动程序集的值。
跟踪文件大小限制	允许设置 Java 跟踪文件大小限制。如果将文件大小设置为无限制，则此文件可以大到占据所有磁盘剩余空间。 **注释：**如果指定了文件大小限制，则在多个文件中创建跟踪文件。 Identity Manager 会自动将最大文件大小除以 10，创建 10 个单独的文件。这些文件的合并大小等于最大跟踪文件大小。 如果选择使用驱动程序集的设置，将采用驱动程序集的值。

DirXML 脚本跟踪

“DirXML 脚本跟踪 ” 选项允许您选择驱动程序集的跟踪级别。该选择应用于驱动程序集中的所有策略。可选择以下 DirXML 脚本跟踪选项：

- 所有 DirXML 脚本跟踪开启
- 所有 DirXML 脚本跟踪关闭
- DirXML 脚本规则跟踪开启
- DirXML 脚本规则跟踪关闭

单击 以保存您的更改。

图 22-3 管理驱动程序集的日志和跟踪级别

管理驱动程序集检查器和统计数字

您可以使用驱动程序集检查器查看驱动程序集关联对象的详细信息。本部分包括以下类别：

- 查看驱动程序集统计数字 （第 139 页）
- 查看版本信息 （第 139 页）
- 查看关联统计数字 （第 140 页）

查看驱动程序集统计数字

您可以通过 Identity Console 门户查看单个驱动程序或整个驱动程序集的各种统计数字。这包括按类别 （添加、去除、修改等）的超速缓存文件大小、超速缓存文件中未处理的事务大小、最旧和最新的事务以及未处理事务的总数等统计数字。要查看驱动程序集统计数据：

1. 在 Identity Console 中，选择 **IDM 管理** > **单击相应驱动程序集的环境菜单 （三个点）** > **驱动程序集属性** > **检查器和统计数字** > **统计数字**。
2. 从下拉列表中选择相应的服务器。

   显示一个页面，允许您查看驱动程序集中包含的所有驱动程序的统计数字。

   - 要刷新统计数据，单击 ⟳ 图标。
   - 要关闭驱动程序的统计数字，单击驱动程序统计数字窗口右上角的 ✕ 按钮。
   - 要打开所有驱动程序的统计数字，单击**操作** > **全部显示**。
   - 要折叠驱动程序的未处理事务列表，单击列表上方的 ⌃ 按钮。要折叠所有驱动程序的未处理事务列表，单击**操作** > **折叠所有事务**。
   - 要展开事务列表，单击 ⌄ 按钮。要展开所有驱动程序的未处理事务列表，单击**操作** > **展开所有事务**。
   - 要关闭禁用驱动程序的统计数字仪表板，单击**操作**，然后选择**关闭禁用的驱动程序**。

查看版本信息

Identity Manager 引擎、驱动程序 Shim 和驱动程序配置文件都包含一个单独的版本编号。Identity Console 中的版本发现选项可帮助您找到 Identity Manager 引擎版本和驱动程序 Shim 版本。驱动程序配置文件包含自己的命名约定。要查看版本信息：

1. 在 Identity Console 中，选择 **IDM 管理** > **单击相应驱动程序集的环境菜单 （三个点）** > **驱动程序集属性** > **检查器和统计数字** > **版本发现**。
2. 查看版本信息的顶级显示：
   - 鉴定的目标 eDirectory 树

     注释：在 Identity Manager 环境中使用时， eDirectory 称作身份库。
   - 选定的驱动程序集
   - 与驱动程序集关联的服务器

如果驱动程序集与两台或更多的服务器相关联，则可以在每台服务器上查看 Identity Manager 信息。

- 驱动程序

3 单击视图图标 可以显示顶层视图中包含的相同信息的文本表示。

4 单击 " 导出 " 按钮 将文本导出并保存到本地或网络驱动器中的文件。

查看关联统计数字

通过使用 Identity Manager 关联统计数字功能，您可以找到由 Identity Manager 管理的身份关联细节。 Identity Manager 使用关联统计数字来获取 Identity Manager 驱动程序的关联计数。

要获得驱动程序的活动、非活动和系统托管的对象，运行关联统计作业。您可以按日、按周、按月或按年排定关联统计作业。默认情况下，该作业排定为每周运行一次。

关联统计信息仪表板显示关联细节。或者，您可以通过将关联导出到文件来查看细节。

注释：

- 驱动程序关联计数按服务器划分。如果对象与多个驱动程序关联，则为每个驱动程序单独计算关联计数。
- 如果关联超过 200,000 个，我们建议您将驱动程序集的最大堆大小设置为 2 GB 或更多。有关设置堆大小的信息，请参阅配置 Java 环境参数 （第 132 页）。

要查看关联统计数字：

1 在 Identity Console 中，选择 **IDM 管理** > **单击相应驱动程序集的环境菜单 （三个点）** > **驱动程序集属性** > **检查器和统计数字** > **关联统计数字**。

2 选择要运行关联统计的服务器。

3 关联计数显示之前计算的结果。

   Identity Console 显示与驱动程序集关联的所有驱动程序的活动、非活动和系统托管对象的关联计数。

   Identity Console 将组和组织单元视作系统托管的对象。如果对象中的登录已禁用属性设置为 true，并且过去 120 天内未修改对象，则 Identity Console 会认为对象不活动。所有剩余的对象都被视为活动托管对象。

4 单击 图标获取更新的结果。

   当在服务器上禁用某个驱动程序时， Identity Console 不会在仪表板中显示该驱动程序。

5 单击 图标导出与服务器关联的驱动程序的系统细节和关联计数细节。

6 要导出与特定驱动程序关联的对象，单击所需对象旁边的 并保存文件。

   注释：如果是扇出驱动程序，则仅导出唯一的对象。如果对象与扇出驱动程序的多个实例关联，则 Identity Console 在仪表板中显示所有关联计数。但是，如果您选择将对象导出到一个文件中， Identity Console 将仅导出唯一的对象。

   ---

7 单击操作并选择组织关联计数仪表板所需的选项。

图 22-4 管理驱动程序集统计数字

23 管理驱动程序属性

本部分提供所有驱动程序通用属性信息。这包括所有属性 （命名口令、引擎控制值、日志级别等）。

将显示驱动程序的激活信息，提醒您激活失效驱动程序的操作。

要修改驱动程序的配置，执行下列操作：

1 单击 Identity Console 主屏幕中的驱动程序选项卡。

2 单击相应驱动程序磁贴以查看驱动程序的配置页面。

默认情况下，显示连接参数页面。驱动程序配置选项分为以下类别：

连接参数

连接参数控制驱动程序应本地运行还是远程运行。

- **Java**：使用此选项来指定为驱动程序的 shim 组件实例化的 Java 类名称。此类可以作为类文件放在类目录中，或作为 .jar 文件放在 lib 目录中。选择此选项在本地运行驱动程序。您还必须指定驱动程序对象口令和驱动程序超速缓存限制。您可以通过单击设置口令链接来设置新口令。

  例如， com.microfocus.nds.dirxml.driver.scim.SCIMDriverShim

- **本机**：此选项用于指定以本机语言 （如 C++）为驱动程序开发的 .dll 的名称。您还必须指定驱动程序对象口令和驱动程序超速缓存限制。您可以通过单击设置口令链接来设置新口令。

  例如， addriver.dll

- **连接到 Remote Loader**：当驱动程序远程连接到连接系统时使用此选项。如果选择了此选项，则必须指定以下子选项：

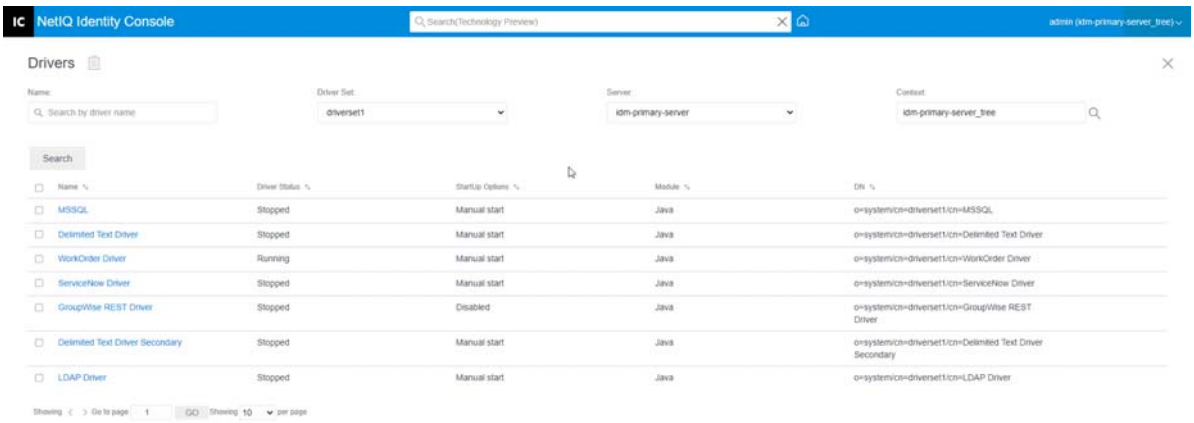
  - Remote Loader 连接参数：包括 Remote Loader 环境细节信息，如主机名称、连接端口等。

- **Remote Loader 口令**：Remote Loader 的口令。
- **驱动程序对象口令**：指定驱动程序对象的口令。如果您正在使用 Remote Loader，则必须在此页面上输入口令。Remote Loader 使用此口令将其自身鉴定到远程驱动程序 Shim。

- **鉴定**：鉴定参数用于鉴定 Identity Manager 引擎和 Remote Loader 服务器。指定以下参数：
  - **鉴定 ID**：指定用户应用程序 ID。此 ID 用于将身份库订购信息传递给应用程序。
  - **鉴定环境**：指定应用程序 Shim 应与之通信的服务器的 IP 地址或名称。
  - **应用程序口令**：设置应用程序鉴定口令的选项。

完成后，单击 图标以保存配置。

图 23-1 管理连接参数



驱动程序配置

驱动程序配置部分允许您配置驱动程序特定参数、引擎控制值、全局配置值等。更改驱动程序参数时，可以调整驱动程序行为，使其符合您的网络环境。本部分包括以下类别：

驱动程序参数

驱动程序参数分为驱动程序设置、订购者设置和发布者设置。这些设置将根据您的驱动程序配置进行填充。有关驱动程序参数的更多信息，请参阅 Identity Manager Drivers Documentation （Identity Manager 驱动程序文档）中的特定驱动程序指南。

完成后，您可以通过单击 保存参数。如果您想将参数设置为其默认值，单击 图标。要使用 xml 文件修改驱动程序配置，单击 图标。

全局配置值

显示全局配置对象的有序列表。对象包含 Identity Manager 启动时加载的驱动程序的扩展 GCV 定义。您可以在全局配置值选项卡下使用 XML 编辑器查看或修改对象。单击 图标以保存 GCV。要刷新 GCV 列表，单击 图标。要删除 GCV，选择相应的 GCV 对象并单击 图标。

引擎控制值

引擎控制值是更改 Identity Manager 引擎某些默认行为的一种方式。只有当服务器与驱动程序集对象关联时，才能访问这些值。

选项	描述
Subscriber channel retry interval in seconds （以秒为单位的订购者通道重试间隔）	订购者通道重试间隔控制 Identity Manager 引擎在应用程序 shim 的订购者对象返回重试状态后重新处理超速缓存事务的频率。
Qualified form for DN-syntax attribute values （DN 语法属性值的合格形式）	DN 语法属性值的合格规范控制 DN 语法属性值的值是以不合格的斜杠形式还是有效的斜杠形式呈现。 “True” 设置表示以合格形式显示值。
Qualified form from rename events （重命名事件的合格形式）	重命名事件的合格形式控制来自身份库的重命名事件的新名称部分是否通过类型限定符呈现给订购者通道。例如：CN=。 “True” 设置表示以合格形式显示名称。
Maximum eDirectory replication wait time in seconds （以秒为单位的 eDirectory 复制最长等待时间）	此设置控制 Identity Manager 引擎等待特定更改在本地复本和远程复本之间进行复制的最长等待时间。这仅影响 Identity Manager 引擎需要联系同一树中的远程 eDirectory 服务器执行操作的操作，并且可能需要等到某些更改复制到远程服务器或从远程服务器进行复制后才能完成操作（例如，当 Identity Manager 服务器不持有移动对象的主复本时的对象移动；从模板创建的用户文件系统权限操作。）

选项	描述
Use non-compliant backwards-compatible mode for XSLT （为 XSLT 使用不合规的向后兼容模式）	此控件会将 Identity Manager 引擎使用的 XSLT 处理器设置为向后兼容模式。向后兼容模式将导致 XSLT 处理器使用一种或多种不符合 XPath 1.0 和 XSLT 1.0 标准的行为。这样做是为了向后兼容依赖非标准行为的现有 DirXML 样式表。 例如，在 Identity Manager 2.0 以及之前版本的 DirXML 版本中，当一个操作数是节点集，而另一个操作数不是节点集时， XPath “!=” 运算符的行为不正确。此行为已更正；但是，通过此控件默认禁用了已更正的行为，以向后与现有 DirXML 样式表兼容。
Maximum application objects to migrate at once （一次迁移的最多应用程序对象）	此控件用于限制 Identity Manager 引擎在作为从应用程序迁移对象操作的一部分而执行的单个查询期间从应用程序请求的应用程序对象数量。 如果在从应用程序进行迁移操作过程中遇到 java.lang.OutOfMemoryError 错误，则此数字应设置为低于默认值。默认端口为 50。 **注释：**此控件不会限制迁移的应用程序对象的数量；只限制批的大小。
Set creatorsName on objects created in Identity Vault （在身份库中创建的对象上设置 creatorsName）	Identity Manager 引擎使用此控件来确定，对于在身份库中由此驱动程序创建的所有对象，是否应将 creatorsName 属性设置为此驱动程序的 DN。 设置 creatorsName 属性使得易于识别该驱动程序创建的对象，而且可以实行绩效惩罚。如果不设置， creatorsName 属性默认为托管驱动程序的 NCP Server 对象的 DN。
Write pending associations （写入待发关联）	此控件确定 Identity Manager 引擎是否在订购者通道处理期间写入有关对象的待发关联。 写入待发关联提供很少好处或根本没有好处，但确实会影响性能。但是，此选项用于向后兼容。
Use password event values （使用口令事件值）	此控件确定报告订购者通道添加和修改事件的 nspmDistributionPassword 属性的值来源。 将该控件设置为 False 表示获取 nspmDistributionPassword 的当前值并报告为属性事件的值。这意味着只有当前口令值可用。这是默认行为。 将该控件设置为 True 表示随 eDirectory 事件记录的值被解密并报告为该属性事件的值。这意味着在发生事件时旧口令值 （如果存在）和替换口令值可用。对于需要旧口令才能设置新口令的某些应用程序，该控件可用于同步口令。
Retry Out of Band events （重试带外事件）	此控件确定如果收到带外同步事件的**重试**状态，是否重试带外同步事件。 如果控件设置为 False，则不会重试带外同步。如果设置为 True，则会重试带外同步，直至成功。
Use Rhino ECMAScript engine （使用 Rhino ECMAScript 引擎）	确定 Identity Manager 引擎是否使用 Rhino ECMAScript 引擎。引擎将 Rhino 用作默认 ECMAScript 引擎。 默认情况下，此控件为 **true**，如果您将此控件设置为 **false**，引擎将使用 Nashorm 脚本。

选项	描述
Enable Subscriber Service Channel （启用订购者服务通道）	确定 Identity Manager 引擎是否处理驱动程序订购者服务通道上的带外查询。这些查询的一些常见示例有代码映射刷新、数据收集和从 dxcmd 触发的查询。 当此控件设置为 true 时，通道会分开处理这些查询，而不会中断事件的正常处理。 目前，此控件仅能与 JDBC 扇出驱动程序 （默认启用）搭配使用。
Enable password synchronization status reporting （启用口令同步状态报告）	此控件确定 Identity Manager 引擎是否报告订购者通道口令更改事件的状态。 报告订购者通道口令更改事件的状态允许应用程序 （如 Identity Manager User Application）监视应同步到连接应用程序的口令更改的同步进度。
Combine values from template object with those from add operation （将模板对象的值与添加操作的值组合在一起）	此值确定 Identity Manager 引擎在执行添加操作时是否将创建模板和添加操作中的类似值组合在一起。将此值设置为 True，则会同时使用模板的多值属性值与在添加操作中指定的相同属性的值。将此值设置为 False，则如果在添加操作中指定了相同属性的值，将会忽略模板的值。
Allow event loopback from publisher to subscriber channel （允许事件从发布者回写到订购者通道）	此值确定 Identity Manager 引擎是否允许事件从驱动程序的发布者通道循环到订购者通道。如果将此值设置为 False， Identity Manager 引擎将不允许事件回写。将此值设置为 True， Identity Manager 引擎将允许事件从发布者通道回写到订购者通道。
Revert to calculated membership value behavior （还原为计算出的成员资格值行为）	此值确定 Identity Manager 引擎在执行与组成员资格相关的读取和搜索操作时使用的方法。 如果将此值设置为 False （默认设置），则 Identity Manager 引擎在读取或搜索身份库对象的成员和组成员属性时，将仅返回 “ 静态 ” 值。静态值是指通过直接指派给组 （而非通过嵌套组继承指派）收到组成员资格的对象。 将此值设置为 True 将导致 Identity Manager 引擎还原为使用 Identity Manager 3.6 之前版本所用的方法。在低于 3.6 的版本中， Identity Manager 引擎在搜索成员和组成员属性时会检索所有 “ 计算的 ” 值。已计算值包括的对象有 1) 静态指派的成员资格或 2) 通过 eDirectory 使用的嵌套组层次结构计算动态指派的成员资格。对组成员属性的搜索会返回直接指派给组或通过嵌套组指派成员资格的任何对象。
Maximum time to wait for driver shutdown in seconds （以秒为单位的等待驱动程序关闭的最长时间）	此设置控制 Identity Manager 引擎等待驱动程序发布者通道关闭的最长时间。如果驱动程序未在指定时间间隔内关闭， Identity Manager 引擎将终止驱动程序。

选项	描述
Regular Expression escape meta-characters （正则表达式转义元字符）	此控件确定扩展正则表达式环境中本地变量时将转义的元字符。必须为此控件值添加以逗号分隔的所有要转义字符的列表。 如果某个元字符不在控件值中，则在正则表达式的本地变量扩展时将不会转义该元字符。 使用此控件时，请确保以下几点： ◆ 值不为空。默认情况下，它填充了 **$**。本地变量扩展需要此字符。 ◆ 该值应是有效的逗号 (,) 分隔的列表，否则将在策略评估中遇到错误。 ◆ 要转义所有元字符，将 "\,$,^,.,?,*,+,[,],(,),|" 指定为一个值。 ◆ 如果不需要转义某个元字符，从值中去除该字符。 ◆ 要转义任何元字符，指定元字符后跟反斜杠 (\)。
Ignore Entitlement Changes of other drivers （忽略其他驱动程序的权利更改）	此控件确定 Identity Manager 引擎忽略还是处理其他驱动程序的权利更改。默认值为 True。这意味着驱动程序会自动忽略其他驱动程序的权利更改。如果此控件设置为 False，则将超速缓存其他驱动程序的权利更改，此驱动程序将处理更改。
Allow Entitlement event loopback from cprs to subscriber channel （允许权利事件从 cprs 回写到订购者通道）	此控件确定 Identity Manager 引擎是否允许由 CPRS 指派生成的权利事件回写到驱动程序的订购者通道。默认值为 “False”。这意味着事件不会回写到订购者通道。如果此控件设置为 True，则事件将流向驱动程序的订购者通道。

启动选项

启动选项允许您在 Identity Manager 服务器启动时设置驱动程序状态。

- **自动开始**：每次启动 Identity Manager 服务器时，驱动程序都会启动。
- **手动**：Identity Manager 服务器启动时，驱动程序不启动。必须使用 Identity Console 门户启动驱动程序。
- **禁用**：驱动程序有一个超速缓存文件，存储所有事件。驱动程序设置为禁用时，将删除此文件，在将驱动程序状态更改为手动或自动开始之前，不会在文件中存储任何新事件。

设置首选启动选项后，单击 图标以保存。要重设置启动选项，单击 图标。

命名口令

通过 Identity Manager 可以安全地储存驱动程序的多个口令。此功能称为 “ 命名口令 ”。通过密钥或名称访问每个不同的口令。

您可以向驱动程序集或单个驱动程序添加命名口令。驱动程序集中的所有驱动程序都可以使用该驱动程序集的命名口令。单个驱动程序的命名口令仅对该驱动程序可用。

若要在驱动程序策略中使用命名口令，应使用其名称来引用该口令，而不要使用实际口令，Identity Manager 引擎会将此口令发送至驱动程序。本部分描述的储存和检索命名口令的方法可用于任何驱动程序，无需对驱动程序 Shim 进行更改。

要添加新的命名口令，单击 ＋ 图标。要去除现有命名口令，单击 图标。要保存列表，单击 图标。

安全性等于

使用 " 安全性等于 " 页面查看或更改驱动程序明确地安全性上等价于的对象列表。该对象有效具有所列对象的全部权限。

您可以通过单击 ＋ 图标在安全性等于列表中添加新对象。如果您添加或删除此列表中的对象，则系统会自动将此对象添加至该对象的 " 安全性与我等效 " 属性中或将其从中删除。您无需将 [public] 受托者或此对象的父容器添加到列表中，因为此对象已隐式实现安全性上等价于它们。

要从此列表中去除现有对象，单击 图标。要保存列表，单击 图标。

排除对象

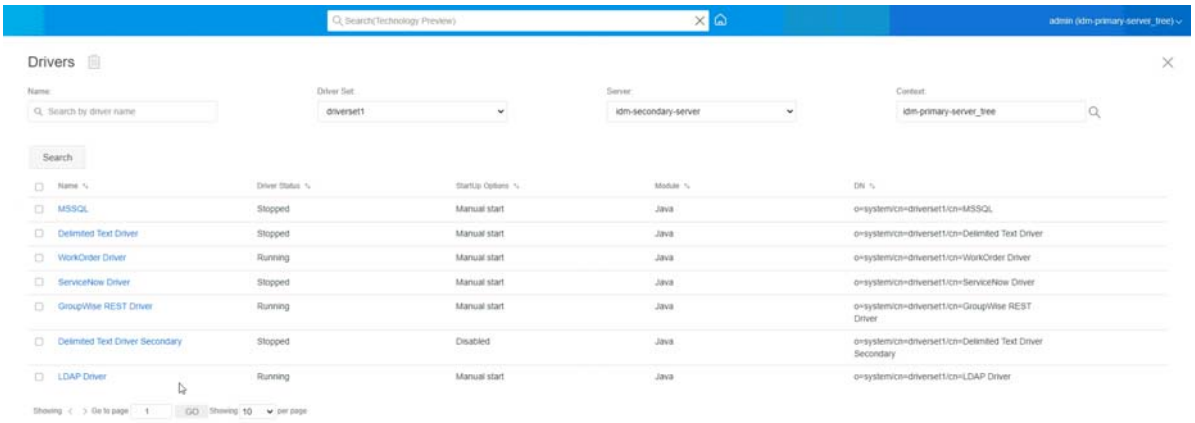
使用此选项可以创建将不复制到应用程序中的对象的列表。建议您将所有代表管理角色的对象 （例如，管理员对象）添加至此列表中。您可以通过单击 ＋ 图标在列表中添加新对象。要从此列表中去除现有对象，单击 图标。要保存列表，单击 图标。

管理已赋值属性列表

要将属性添加到特定驱动程序的已赋值属性列表中，执行下列操作：

1. 在 Identity Console 中，选择对象管理模块。
2. 从下拉列表中选择 **Dir-XML-Driver** 类型，然后单击 " 搜索 " 按钮。
3. 单击搜索列表中的相应驱动程序。
4. 要将未赋值属性添加到已赋值属性列表中，单击已赋值属性旁边的 ＋ 图标，并从列表中选择相应的未赋值属性。
5. 完成后，单击确定。

图 23-2 管理驱动程序配置



数据转换和同步

本部分包括以下类别：

数据同步视图

驱动程序概述页面分为以下类别：

过滤器

过滤器存在于驱动程序中，使您能够指定应用程序可以从身份库发送和接收的类和属性。如果要特定的类通过元目录引擎处理，则应该将类添加到相应通道上的过滤器中。还可以按定义的特定属性值过滤对象。

要添加要包含在同步中的类和属性并修改驱动程序过滤器，单击“发布者”或“订购者”通道上的过滤器。

注释：“概述”的图形说明显示了两个独立的对象，用于发布者通道和订购者通道上的驱动程序过滤器。尽管显示了两个对象，但两个通道使用的是同一个过滤器。

所有策略

默认情况下，将显示所有策略页面。您可以通过单击 图标在容器中导入现有策略。您还可以去除不需要的任何策略。要为驱动程序选择跟踪级别，单击 图标。您可以使用 和 图标上下移动列表中的策略。

注释：Identity Console 不支持为驱动程序添加和部署新策略。我们建议您使用 iManager 和 Identity Designer 来添加和部署新策略。

将数据迁移到身份库中

使用此任务定义 Identity Manager 用于将对象从应用程序迁移到身份库的准则。迁移对象时，元目录引擎会将所有“匹配”、“布局”、“创建”策略以及发布者过滤器应用于该对象。使用在“类”列表中指定的顺序将对象迁移到身份库中。您可以使用此选项执行以下任务：

1. **添加类和属性：**要添加或去除要迁移的类和属性，单击 图标，然后选择要添加的类及其各自的属性。选择类和属性后，单击添加以保存更改。
2. **编辑属性值：**要更改编辑列表时指定的迁移属性值，单击编辑属性 图标。
3. **Re-order the Class List** （重新排序类列表）：使用 和 按钮对列表中的类进行排序。使用在“类”列表中指定的顺序将对象迁移到身份库中。
4. **刷新：**单击 图标刷新列表。

从身份库中迁移数据

使用导出选项卡可以选择希望从身份库迁移至应用程序的容器或对象。迁移对象时，元目录引擎会将所有匹配、创建、布局策略和订购者过滤器应用于对象。

要将对象或容器从身份库迁移到其他应用程序，单击 图标。浏览并选择要迁移的对象，然后单击确定以将对象添加到迁移列表。要从迁移列表中去除对象，单击 图标。

选择完要迁移的对象后，单击 以开始迁移。屏幕上将显示迁移进度。如果要停止迁移，单击 按钮。

同步对象

同步操作查找已修改的对象并使它们同步。您可以选择检查所有对象以立即开始同步。或者，您也可以设置开始同步的日期 / 时间。

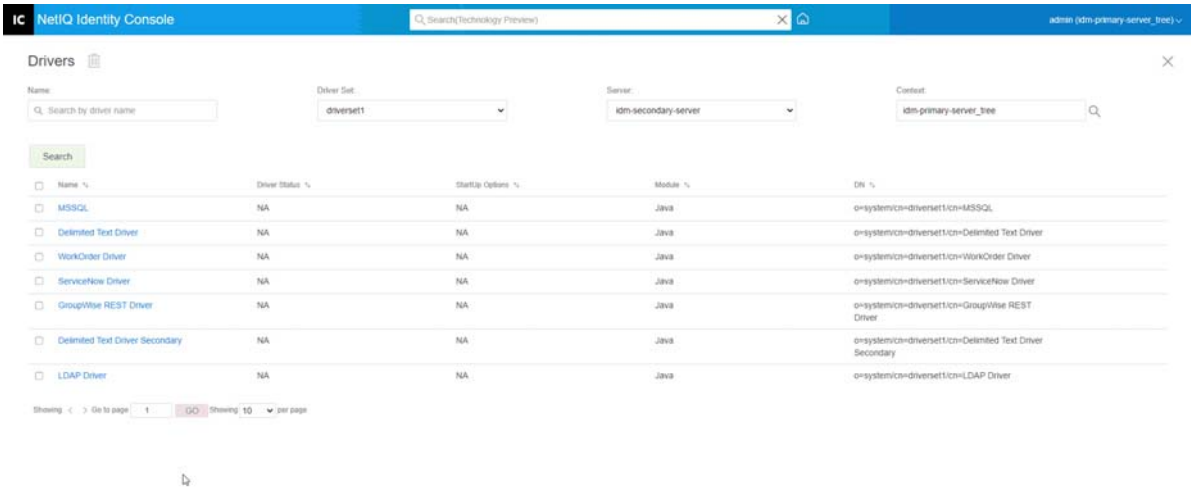
DirXML 脚本跟踪

“ 跟踪 DirXML 脚本 ” 选项允许您选择驱动程序的跟踪级别。它还会将跟踪设置应用于所有发布者和订购者通道。可选择以下 DirXML 脚本跟踪选项：

- 所有 DirXML 脚本跟踪开启
- 所有 DirXML 脚本跟踪关闭
- DirXML 脚本规则跟踪开启
- DirXML 脚本规则跟踪关闭

单击 以保存您的更改。

图 23-3 管理驱动程序的数据同步



类属性过滤器

您可以使用类属性过滤器指定在应用程序和身份库之间可以发送和接收的类和属性。如果要特定的类通过元目录引擎处理，则应该将类添加到相应通道上的过滤器中。您还可以按您定义的特定属性值来过滤对象。您可以使用此选项来执行以下操作：

- **设置模板**：使用此选项设置添加到过滤器的所有属性的默认选项。单击类属性过滤器标签旁边的 图标。
- **添加新类**：通过单击 图标添加新类。
- **添加新属性**：通过单击 图标添加新属性。
- **从以下位置复制过滤器**：此选项允许您从其他驱动程序复制过滤器。单击 图标复制过滤器。
- **编辑 XML**：使用编辑 XML 文件 图标编辑类和属性过滤器设置。
- **删除类或属性**：通过单击相关类或属性旁边的 图标删除任意类或属性。

您可以在发布者和订购者频道中为类和属性值设置以下选项：

- 同步
- 忽略
- 通知
- 重设置

合并权限

如果属性在任一通道中都不同步，则不会发生合并。

如果属性在一个通道中同步而在另一通道中不同步，则该通道的目标上的所有现有值会被去除并替换为该通道的源中的值。如果源有多个值并且目标只能提供单个值，则只有其中一个值能用于目标端。

如果属性在两个通道中都同步且两端都只提供单个值，则连接应用程序会获得存储在身份库中的值 （除非身份库中没有值）。在这种情况下，身份库从连接的应用程序获取值。

如果属性在两个通道中都同步并且只有一端提供多个值，且多值通道中没有值，则单值通道的值将添加到多值通道中。如果在单值端上没有值，则可以选择值以添加到单值端。您可以为合并管理机构设置以下选项：

- 默认值
- 身份库
- 应用程序
- 无

单击 以保存您的更改。

ECMA 脚本

显示 ECMAScript 资源文件的有序列表。这些文件包含 Identity Manager 在驱动程序启动时加载的驱动程序的扩展功能。您可以通过单击 导入其他文件，通过单击 去除现有文件，或更改执行文件的顺序。您还可以在列表中上下移动脚本。您可以通过单击 图标来保存 ECMA 脚本列表。

互逆属性映射

互补属性映射使您可以创建和管理对象间的回指链接或参照。例如，组对象包括一种成员属性，它参照属于该组的所有用户对象。类似地，每个用户对象包括一种组成员资格属性，它参照用户是其成员的组对象。要使元目录引擎在身份库中保留 Group object （组对象） > Members attribute synchronized with the User object （与用户对象同步的成员属性） > Group Membership attribute for all Group objects and User objects （针对所有组对象和用户对象的组成员资格属性），必须链接这些属性。对象属性间的这种链接称为互补属性映射。

您可以使用此模块来执行以下操作：

- 创建自定义互逆属性映射 （第 154 页）
- 添加新的互逆属性映射 （第 154 页）
- 去除互逆属性映射 （第 155 页）
- 从互逆映射列表中去除属性 （第 155 页）
- 对映射的属性重新排序 （第 155 页）
- 去除自定义互逆属性映射 （第 155 页）
- 编辑互逆属性 XML （第 155 页）

创建自定义互逆属性映射

仅当互逆属性映射页面显示该驱动程序不包含自定义互逆属性映射。单击上方的 “+” 图标以创建基本的互逆属性映射提示时此部分才适用。

1 单击 图标创建新的自定义互逆属性映射列表。
2 将显示驱动程序的默认属性映射。现在，您即可添加映射、修改现有映射或删除映射。

添加新的互逆属性映射

创建互逆属性映射时，必须先将其中一个属性添加到互逆映射列表中。

1 单击操作下拉菜单旁边的 图标。
2 在新的属性条目中，从下拉列表中选择所需的属性。

3 指定互逆映射的细节：

3a **来源类**：指定映射列表中的属性关联的类名称。例如，如果您将组成员资格属性放在互逆映射列表中，则关联的来源类为用户。

3b **目标类**：指定要与之创建互逆映射的属性关联的类名称。例如，如果您将组成员资格属性放在互逆映射列表中，则关联的目标类为组。

3c **互逆属性**：指定要创建互逆映射的属性名称。

4 如果要将属性映射到其他互逆属性，单击属性名称右侧的 + 图标。

将在属性列表的结尾添加用于该属性的新部分。选择源类、目标类和互补属性。

去除互逆属性映射

要去除互逆属性映射：

1 勾选来源类前面要删除的互逆属性映射的复选框。

2 单击属性下拉列表旁边的 图标。

从互逆映射列表中去除属性

要从互逆映射列表中去除属性：

1 通过勾选属性前面的复选框来选择要去除的属性。

2 单击操作下拉列表旁边的 图标。

对映射的属性重新排序

将按照所列的顺序从上到下对属性映射进行解析。您可在列表中上下移动映射的属性，以确保能够按照正确顺序对其进行解析。通常，您应首先列出特定映射，然后列出更多的一般映射。例如，应首先列出组对象上“成员”属性的映射，然后再列出任何对象（< 任意类 > 选项）上“成员”属性的映射。

选择要移动的所映射属性前面的复选框，然后单击 ↑ 将属性上移或单击 ↓ 将属性下移。

去除自定义互逆属性映射

您可删除已创建的自定义属性映射。这将导致元目录引擎对驱动程序使用默认属性映射。

要去除自定义互逆属性映射，单击屏幕顶部的 图标。

编辑互逆属性 XML

如果需要，您可以直接编辑互逆属性的 XML。为此，单击自定义互逆属性映射页面上的编辑 XML 图标 。这将打开一个基本的 XML 编辑器，允许您修改 XML。完成后，单击“确定”或“取消”以关闭 XML 编辑器。

高级设置

高级设置分为以下类别：

- 管理权利 （第 156 页）
- 管理对象映射表 （第 156 页）
- 管理驱动程序的作业 （第 157 页）

管理权利

权利页包含显示选定驱动程序 （以其完整判别名列出）中当前定义的所有权利的表。可以在此页面执行下列操作：

- **在 XML 中编辑**：要在 XML 文件中编辑权利，从列表中选择权利并单击 图标。然后勾选 **Enable XML Editing** （启用 XML 编辑）框。
- **删除**：要删除权利，单击权利名称左侧的框，然后单击 图标。可以看见叙述操作无法复原的讯息并询问是否确实要删除选定的权利。单击**确定**删除权利，或单击**取消**停止操作。可以单击多个框删除多个权利，或单击左上方的框以删除所有的权利。

管理对象映射表

Identity Manager 策略使用映射表将一组值映射到另一组相应的值。安装权利包时，此包的策略将添加到驱动程序启动策略集中。驱动程序仅在驱动程序启动时执行一次这些策略。有关详细信息，请参见 《*NetIQ Identity Manager Driver Administration Guide*》（NetIQ Identity Manager Driver 管理指南）中的 Mapping Table Objects （映射表对象）。

使用对象映射表，您可以执行下列操作：

- **修改现有映射**：要修改现有对象映射表，单击列表中的映射并在下一个屏幕中执行下列操作：
  - 添加新列。

    指定列的值，然后选择值是区分大小写、不区分大小写还是数值。
  - 添加新行并指定行的值。
  - 单击 图标。
- **删除映射**：要从列表中去除映射，从列表中选择相应映射并单击 图标。
- **在 XML 中编辑**：要在 XML 文件中编辑映射，单击列表中的映射并选择 图标。然后，勾选 **Enable XML Editing** （启用 XML 编辑）框。

管理驱动程序的作业

Identity Console 允许您使用作业选项为所有单个驱动程序排定事件。

作业日程安排器页面包括作业名称，作业是启用的还是禁用的，排定运行的时间，以及作业说明。单击作业名称打开作业页。在 " 已启用 " 列下单击启用 / 禁用图标以启用或禁用作业。单击作业说明以查看作业的完整说明。

作业选项卡包含一个表，显示选定驱动程序的现有作业对象，列出的选定驱动程序使用驱动程序项中的完整判别名。

作业日程安排器页面允许您执行以下任务：

- **创建作业**：单击 + 图标以创建新作业。

  在**新建作业**弹出窗口中，要创建新作业，请执行以下步骤：

  1. 指定作业名。
  2. 选择作业类型。
  3. 单击 ∨ 图标，然后从可用的服务器列表中选择要运行作业的服务器。否则，请指定服务器名称，然后选择服务器。
  4. 单击创建按钮。
- **启动作业**：单击作业左侧的框选择作业，然后单击 ⊳ 图标。
- **停止作业**：单击作业左侧的框选择作业，然后单击 ⊡ 图标。
- **启用作业**：单击作业左侧的框选择作业，然后单击 ⊙ 图标。
- **禁用作业**：单击作业左侧的框选择作业，然后单击 ⊗ 图标。
- **获取状态**：单击作业左侧的框选择作业，然后单击 ⓘ 图标。
- **删除作业**：单击作业左侧的框选择作业，然后单击 🗑 图标。

单击作业打开 **Job Property** （作业属性）页。在此可以设置作业的运行方式。

一般：显示作业的 Java 类名。使用此页启用或禁用作业，在运行作业后删除作业，选择应该运行此作业的一个或多个服务器，指定电子邮件服务器和为作业指定不同的显示名称与说明。

日程表：允许您设置何时运行作业。指定 " 启动作业时间 " 以设置时间，以及是否每天、每周、每月、每年运行作业。还可以自定义要运行作业的时间，也可以选择启用切换开关以手动运行作业。

范围：允许您定义此作业适用的对象。对象可以是容器、动态组、组或叶对象。单击 " 添加 " 选择要应用此作业的对象。可以使用 " 浏览 " 按钮选择对象，然后单击 " 确定 "。要从范围列表中去除对象，请单击 DN 对象左侧的框选择范围对象，然后单击 " 去除 "。

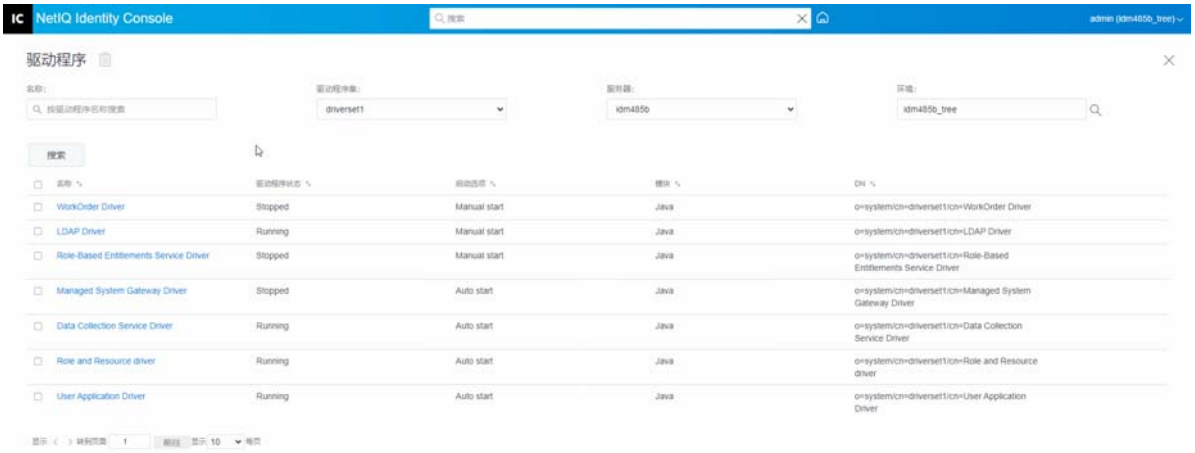
当添加对象时，选择它将显示更多选项。如果选择组对象，则该选项只能将该作业应用到组成员或组。如果选择容器对象，则您可以选择只将该作业应用到此容器的所有后代或此容器的所有子代，或者仅应用到此容器。

参数：允许您向作业添加其他参数，并在参数设置后即可查看。这些参数因选定作业的类型而异。

结果：允许您定义如何处理作业结果。“结果”页分成两部分：中间结果和最终结果（允许有以下结果：“成功”、“警告”、“错误”和“已中止”）。“结果”列的右侧是“操作”列。可以单击“操作”列来设置每个结果的通知方式。操作包含发送审计结果或在结果完成时发送电子邮件。如果没有选择选项，则对结果将不采取任何操作。

在**跟踪**选项卡中，可以为特定驱动程序配置跟踪。有关更多信息，请参见配置跟踪级别（第 159 页）

图 23-4 管理高级设置



配置驱动程序的日志和跟踪级别

要为您的驱动程序配置日志和跟踪，从 Identity Console 主页中选择驱动程序 > 日志和跟踪配置选项卡。本部分包括以下类别：

- 配置日志级别（第 158 页）
- 配置跟踪级别（第 159 页）

配置日志级别

每个驱动程序都有一个日志级别字段，您可以定义应跟踪的错误级别。此处指定的级别将决定哪些讯息会记录到日志中。默认情况下，日志级别设置为跟踪错误讯息（也包括严重讯息）。要跟踪其他讯息类型，更改日志级别。要配置日志级别，选择日志和跟踪配置 > 日志级别选项卡。下表介绍了日志级别设置：

选项	描述
Use log settings from the Driver Set （使用驱动程序集的日志设置）	如果选择此选项，则驱动程序会根据 “ 驱动程序集 ” 对象的日志设置记录事件。
关闭对驱动程序集、订购者和发布者日志的日志记录	为此驱动程序关闭对驱动程序集对象、订购者通道和发布者通道上的所有日志记录。
日志中的最大项数 (50-500)	日志中的项数。默认值是 50。
日志级别	可选择以下日志级别： ◆ 记录错误：只记录错误 ◆ 记录错误和警告：记录错误和警告 ◆ 记录特定事件：记录已选事件。选择此选项可提供以下事件列表： ◆ 元目录引擎事件 ◆ 状态事件 ◆ 操作事件 ◆ 转换事件 ◆ 身份凭证供应事件 ◆ 仅更新上次日志时间：更新上次日志时间。 ◆ 日志记录关闭：为驱动程序关闭日志记录。

配置跟踪级别

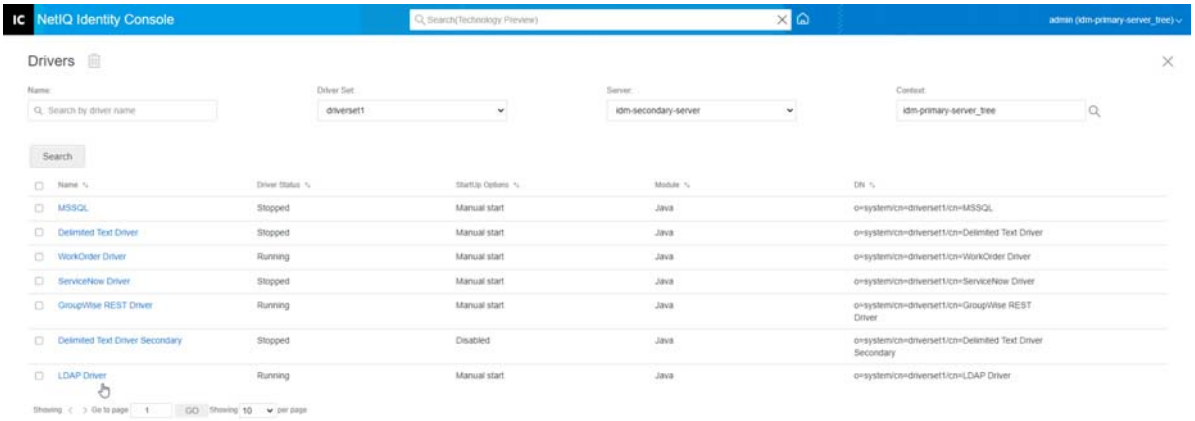
您可以为特定驱动程序配置跟踪。根据为驱动程序指定的跟踪级别，引擎在处理事件时，跟踪显示与驱动程序相关的事件。驱动程序跟踪级别仅影响设置跟踪的驱动程序或驱动程序集。如果您正在使用 Remote Loader， Remote Loader 跟踪文件将直接设置在 Remote Loader 上，并且仅包含驱动程序 Shim 跟踪。

要为驱动程序配置跟踪，选择日志和跟踪配置 > 跟踪选项卡。下表介绍了跟踪设置：

参数	驱动程序
跟踪级别	随着驱动程序跟踪级别的提高，“ 跟踪 ” 中显示的信息量也会增加。 跟踪级别 1 只显示错误，但不显示导致错误的原因。如果希望查看口令同步信息，将跟踪级别设置为 5。 如果选择使用驱动程序集的设置，将采用驱动程序集的值。
跟踪文件	指定文件名和为所选驱动程序写入 Identity Manager 信息的位置。 如果选择使用驱动程序集的设置，将采用驱动程序集的值。

参数	驱动程序
跟踪名称	追加在驱动程序跟踪讯息前的为所输入的值，而不是驱动程序名称。用于驱动程序名称过长的情况。
跟踪文件编码	跟踪文件使用系统的默认编码。如果需要，您可以指定其他编码。
跟踪文件大小限制	允许设置 Java 跟踪文件大小限制。如果将文件大小设置为无限制，则此文件可以大到占据所有磁盘剩余空间。 **注释：**如果指定了文件大小限制，则在多个文件中创建跟踪文件。 Identity Manager 会自动将最大文件大小除以 10，创建 10 个单独的文件。这些文件的合并大小等于最大跟踪文件大小。 如果选择使用驱动程序集的设置，将采用驱动程序集的值。

图 23-5 *管理驱动程序的日志和跟踪级别*



检查驱动程序

您可以使用驱动程序检查器查看驱动程序关联对象的详细信息。本部分包括以下类别：

- 驱动程序检查器 （第 161 页）
- 驱动程序超速缓存检查器 （第 161 页）
- 带外同步超速缓存检查器 （第 162 页）
- 驱动程序清单 （第 163 页）
- 监控驱动程序运行状况 （第 163 页）

驱动程序检查器

要查看与驱动程序关联的对象：

1 在 Identity Console 中，选择驱动程序 > 检查器 > 驱动程序检查器选项卡。

2 在驱动程序字段中，指定要检查的驱动程序的完全判别名，或单击浏览图标以浏览和选择所需的驱动程序。

3 选择要检查的驱动程序后，单击确定以显示驱动程序检查器页面。

   此页显示与所选驱动程序关联对象的相关信息。您可以执行下列操作：

   - **删除**：去除驱动程序与对象之间的关联。勾选您不再希望与驱动程序关联的对象前面的复选框，单击 图标，然后单击确定以确认删除。
   - **刷新**：选择刷新 图标可重读与驱动程序关联的所有对象，并刷新信息。
   - **显示**：选择每页显示的关联数量。您可选择预定义数量 （25、 50 或 100），也可根据需要指定其他数量。默认值为每页 10 个关联。如果关联比显示的数量多，则可使用箭头按钮显示下一页和上一页的关联。
   - **操作**：对与驱动程序关联的对象执行操作。单击操作，然后选择下列某一选项：
     - **显示所有关联**：显示与驱动程序关联的所有对象。
     - **过滤禁用的关联**：显示与具有禁用状态的驱动程序关联的所有对象。
     - **过滤手动关联**：显示与具有手动状态的驱动程序关联的所有对象。
     - **过滤迁移关联**：显示与具有迁移状态的驱动程序关联的所有对象。
     - **过滤待发关联**：显示与具有待发状态的驱动程序关联的所有对象。
     - **过滤已处理关联**：显示与具有已处理状态的驱动程序关联的所有对象。
     - **过滤未定义关联**：显示与具有未定义状态的驱动程序关联的所有对象。
     - **关联摘要**：显示与驱动程序关联的所有对象的状态。
   - **对象 DN**：显示关联对象的 DN。
   - **状态**：显示对象的关联状态。
   - **对象 ID**：显示关联的值。

驱动程序超速缓存检查器

您可以使用 Identity Console 查看驱动程序超速缓存文件中的事务。驱动程序超速缓存检查器显示有关超速缓存文件的信息，包括将由驱动程序处理的事件列表。

1 在 Identity Console 中，选择驱动程序 > 检查器 > 驱动程序超速缓存检查器选项卡。

2 在驱动程序字段中，指定要检查其超速缓存的驱动程序的完全判别名，或单击浏览图标以浏览和选择所需的驱动程序，然后单击确定以显示驱动程序超速缓存检查器页面。

只有当驱动程序未运行时，才能读取驱动程序超速缓存文件。如果驱动程序停止，驱动程序超速缓存检查器页面将显示超速缓存。如果驱动程序正在运行，则页面显示 Driver not stopped, cache cannot be read （驱动程序未停止，无法读取超速缓存）注释，而不显示超速缓存项。要停止驱动程序，单击 按钮；然后读取并显示超速缓存。

- **服务器上的驱动程序超速缓存：**列出包含超速缓存文件此实例的服务器。如果驱动程序在多个服务器上运行，则可以选择列表中的另一台服务器来查看该服务器的驱动程序超速缓存文件。
- **启动 / 停止驱动程序图标：**显示驱动程序的当前状态，并允许您启动或停止驱动程序。只能在驱动程序停止时读取超速缓存。
- **删除：**选择超速缓存中的项，然后单击 图标将其从超速缓存文件中去除。
- **操作：**允许您对超速缓存文件中的项执行操作。单击操作以展开菜单，然后选择以下某个选项：
  - **清除所有超速缓存的事件：**使您能够清除所有超速缓存的事件。
  - **超速缓存摘要：**汇总超速缓存文件中存储的所有事件。

查看驱动程序的连接系统细节

要查看特定驱动程序的连接系统细节，执行下列操作：

1. 在 Identity Console 中，单击对象检查器模块。
2. 浏览并选择要显示连接系统的特定驱动程序对象。
3. 所选驱动程序对象的所有连接系统细节都将显示在您的计算机上。

带外同步超速缓存检查器

要查看带外同步超速缓存中的事件：

1. 在 Identity Console 中，选择驱动程序 > 检查器 > 带外同步超速缓存检查器选项卡。
2. 在驱动程序字段中，指定要检查其超速缓存的驱动程序的完全判别名，或单击浏览图标以浏览和选择所需的驱动程序，然后单击确定。

   只有当驱动程序未运行时，才能读取驱动程序超速缓存文件。如果驱动程序停止，驱动程序超速缓存检查器页面将显示超速缓存。如果驱动程序正在运行，则页面显示 Driver not stopped, cache cannot be read （驱动程序未停止，无法读取超速缓存）注释，而不显示超速缓存项。要停止驱动程序，单击 按钮；然后读取并显示超速缓存。

   - **超速缓存文件名：**显示超速缓存的文件名。
   - **服务器上的驱动程序超速缓存：**列出包含超速缓存文件此实例的服务器。如果驱动程序在多个服务器上运行，则可以选择列表中的另一台服务器来查看该服务器的驱动程序超速缓存文件。
   - **启动 / 停止驱动程序图标：**显示驱动程序的当前状态，并允许您启动或停止驱动程序。只能在驱动程序停止时读取超速缓存。
   - **删除：**选择超速缓存中的项，然后单击 图标将其从超速缓存文件中去除。

- **操作：**允许您对超速缓存文件中的项执行操作。单击操作以展开菜单，然后选择以下某个选项：
  - **超速缓存摘要：**汇总超速缓存文件中存储的所有事件。
  - **清除所有超速缓存的事件：**使您能够清除所有超速缓存的事件。

驱动程序清单

驱动程序清单类似于驱动程序的 " 履历 "。它声明了该驱动程序支持的对象，并包括了一些配置设置。驱动程序清单应该由驱动程序开发商提供。通常情况下，网络管理员无需编辑驱动程序清单。如果管理员想要编辑驱动程序清单，可以通过选择驱动程序 > 检查器 > 驱动程序清单 > **Enable XML Editing** （启用 XML 编辑）选项来做到这一点。

监控驱动程序运行状况

通过驱动程序状态监视，您可以查看驱动程序的当前状态为绿色、黄色还是红色，并可以定义用于响应各种状态要执行的操作。

您可以创建确定各种状态的条件 （准则），您还可以定义驱动程序的状态更改时希望执行的操作。例如，如果驱动程序状态从绿色变为黄色，则您可执行如重启动驱动程序、关闭驱动程序以及向指定解决驱动程序问题的人员发送电子邮件等操作。

您可以使用此模块来执行以下任务：

- 修改驱动程序运行状况条件 （第 163 页）
- 修改驱动程序运行状况操作 （第 165 页）
- 创建自定义状态 （第 167 页）
- 修改自定义状态 （第 167 页）

修改驱动程序运行状况条件

您可以控制确定各个状态的条件。绿色状态用于表示状态良好的驱动程序，而红色状态用于表示状态不佳的驱动程序。

将首先计算绿色状态的条件。如果驱动程序未能满足绿色条件，则将计算黄色条件。如果驱动程序未能满足黄色条件，则自动为驱动程序指派红色状态。

修改状态的条件：

1. 在 Identity Console 中，如需修改特定驱动程序的条件，打开驱动程序的 " 驱动程序运行状况配置 " 页面：

   1a 打开 Identity Console 主页。

   1b 选择驱动程序 > 在列表中单击相应的驱动程序 > 检查器 > 驱动程序运行状况配置。

2. 单击要修改的状态 （" 绿色 " 或 " 黄色 "）的选项卡。

   该选项卡显示状态的当前条件。条件分为若干组，并且使用逻辑运算符 （AND 或 OR）合并各个条件和组。对于绿色状态，请考虑以下示例：

```
GROUP1
Condition1 and
Condition2
Or
GROUP2
Condition1 and
Condition2 and
Condition3
```

在该示例中，如果 GROUP1 条件或 GROUP2 条件计算为 true，则将为驱动程序指派绿色状态。如果两个条件组都不为 true，则将计算黄色状态的条件。

可以进行计算的条件包括：

- **驱动程序状态：**正在运行、已停止、正在启动、未在运行或正在关闭。例如，绿色状态的默认条件之一是驱动程序正在运行。
- **驱动程序处于超速缓存溢出：**用于保留驱动程序事务的超速缓存状态。如果驱动程序处于超速缓存溢出状态，则已使用所有可用超速缓存。例如，绿色状态的默认条件是 " 驱动程序处于超速缓存溢出 " 条件为 false ；而黄色状态的默认值为 " 驱动程序处于超速缓存溢出 " 条件为 true。
- **最新：**超速缓存中最新事务的期限。
- **最早：**超速缓存中最早事务的期限。
- **总大小：**超速缓存的大小。
- **未处理的大小：**超速缓存中所有未处理事务的大小。
- **未处理的事务：**超速缓存中未处理事务的数量。您可指定所有事务类型或特定事务类型 （如添加、去除或重命名）。
- **事务历史记录：**在给定时间段内，在订购者或发布者通道中不同点所处理的事务数量。此条件使用多个元素，格式如下：

  < *事务类型* > < *事务位置和时间段* > < *关系运算符* > < *事务数量* >。

  - < *事务类型* >：指定正在计算的事务类型。这可以是所有事务、添加、去除和重命名等等。
  - < *事务位置和时间段* >：指定订购者或发布者通道中的位置以及要进行评估的时间段。例如，您可以评估过去 48 小时内，作为由发布者报告的事件进行处理的事务总量。默认情况下，事务历史记录数据保留两周，这表示您无法指定大于两周的时间段，除非您更改 " 事务数据持续时间 " 的默认设置。
  - < *关系运算符* >：指定标识的事务与 < 事务数量 > 之间必须存在的比较关系，包括：等于、不等于、小于、小于或等于、大于、大于或等于。
  - < *事务数量* >：指定评估中使用的事务数量。

  以下提供了一个 " 事务历史记录 " 条件的示例：

  <number of adds> <as publisher commands> <over the last 10 minutes> <is less than> <1000>

- **可用的历史记录：**可供评估用的事务历史记录数据量。此条件的主要用途是确保 " 事务历史记录 " 条件不会使当前状态由于没有为要评估的时间段收集足够的事务历史记录数据而失败。

例如，假定您希望使用“事务历史记录”条件对过去 48 小时内作为发布者命令添加的数量进行评估（上述“事务历史记录”部分中显示的示例）。但是，您不希望条件在数据不足 48 小时的情况下失败，在最初设置驱动程序的状态配置后，或当驱动程序的服务器重启动时，可能出现这种情况（因为事务历史数据保存在内存中）。因此，您要创建一个如下的条件组：

Group1 Available History <is less than> <48 hours> or Group2 Available History <is greater than or equal to> <48 hours> and Transactions History <number of adds> <as publisher commands> <over the last 48 hours> <is less than> <1000>

如果任一条件组为 true，即：a) 数据不足 48 小时；或 b) 至少有 48 小时的数据且过去 48 小时内作为发布者命令的添加数量小于 1000，则状态评估为 true。

如果两个条件均计算为 false，即：a) 至少有 48 小时的数据；且 b) 过去 48 小时内作为发布者命令的添加数量大于 1000，则状态计算为 false。

3 根据需要修改准则。

- 要添加新组，单击 + 条件组旁边的 图标。
- 要添加条件，单击逻辑运算符 (AND/OR) 旁边的 + 图标。或者，您也可以单击添加新条件链接。
- 要对条件组或个别条件重新排序，勾选要移动的组或条件前面的复选框，然后单击箭头按钮以将其上下移动。您还可以使用箭头按钮在组之间移动条件。

4 完成后，通过单击保存按钮保存更改。

5 如果想要更改与您设置的条件相关的操作，请参阅修改驱动程序运行状况操作（第 165 页）。

修改驱动程序运行状况操作

您可确定当驱动程序状态更改时要执行的操作。例如，如果状态从绿色更改为黄色，您可关闭或重启动驱动程序、生成某个事件或启动某个工作流程。或者，如果状态从黄色更改为绿色，将会执行与绿色状态相关联的所有操作。

每当满足条件时，仅执行一次运行状况状态的操作，只要状态保持为 true，则不会重复操作。如果状态由于其条件不再满足而发生更改，则下次满足条件时，将再次执行操作。

1 在 Identity Console 中，如需修改特定驱动程序的操作，打开驱动程序的“驱动程序运行状况配置”页面：

   1a 打开 Identity Console 主页。

   1b 选择驱动程序 > 在列表中单击相应的驱动程序 > 检查器 > 驱动程序运行状况配置。

2 如需修改特定状态的操作，单击状态的绿色、黄色或红色选项卡。

3 单击操作文本标题旁边的加号 (+) 图标添加操作，然后选择需要的操作类型：

- **启动驱动程序：**启动驱动程序。
- **停止驱动程序：**停止驱动程序。
- **重启动驱动程序：**停止，然后启动驱动程序。
- **清除驱动程序超速缓存：**从超速缓存中去除所有事务（包括未处理的事务）。

- **发送电子邮件：**向一个或多个收件人发送电子邮件。您希望在电子邮件讯息正文中使用的模板必须已经存在。要在电子邮件中包括驱动程序名称、服务器名称和当前状态信息，将 $Driver$、$Server$ 和 $HealthState$ 标记添加到电子邮件模板中，然后在讯息文本中包括这些标记。例如：

  ```
  The current health state of the $Driver$ driver running on $Server$
  is $HealthState$.
  ```

  重要：要向多个用户发送电子邮件，务必使用逗号 (,) 将每个电子邮件地址分开。不要使用分号代替逗号。

- **写入跟踪讯息：**如果未在驱动程序运行状况作业中配置跟踪文件，向驱动程序运行状况作业的日志文件或驱动程序集的日志文件写入讯息。
- **生成事件：**生成可由 Audit 和 Sentinel 使用的事件。
- **执行 ECMAScript：**执行现有 ECMAScript。

  有关如何构建 ECMA 脚本的信息，请参阅《*NetIQ Identity Manager - Using Designer to Create Policies*》（NetIQ Identity Manager - 使用 Designer 创建策略）中的 Using ECMAScript in Policies （在策略中使用 ECMAScript）。

- **Start Workflow （启动工作流程）：**启动供应工作流程。
- **发生错误时：**如果操作失败，指示如何处理剩余操作、当前状态和驱动程序状态作业。
  - **通过以下方式影响操作：**您可以继续执行剩余操作、停止执行剩余操作或默认为当前设置。仅当有多个出错时操作且在之前某个出错时操作中设置了影响操作的方式选项时，才应用当前设置。
  - **通过以下方式影响状态：**您可以保存当前状态、拒绝当前状态或默认应用当前设置。保存状态将使状态的条件继续评估为 true。拒绝状态将使状态的条件评估为 false。仅当有多个出错时操作且在之前某个出错时操作中设置了影响状态的方式选项时，才应用当前设置。
  - **通过以下方式影响驱动程序运行状况作业：**您可以继续运行作业、中止和禁用作业或默认应用当前设置。继续运行作业将使作业完成对条件的评估，以确定驱动程序状态并执行与该状态相关联的所有操作。中止或禁用作业将停止作业的当前活动并关闭作业；除非您启用作业，否则作业将不再运行。仅当有多个出错时操作且在之前某个出错时操作中设定了影响驱动程序状态作业的方式设置时，才应用当前设置。

4 完成后，通过单击保存按钮保存更改。

创建自定义状态

您可以创建一个或多个自定义状态以执行与驱动程序的当前状态 （绿色、黄色和红色）无关的操作。如果满足自定义状态的条件，无论当前状态如何，都将执行自定义状态的操作。

与绿色、黄色和红色状态一样，当条件满足时，自定义状态的操作仅执行一次；只要状态保持为 True，就不会重复操作。如果状态由于其条件不再满足而发生更改，则下次满足条件时，将再次执行操作。

1 在 Identity Console 中，打开要创建自定义状态的驱动程序的 " 驱动程序运行状况配置 " 页面：

   1a 打开 Identity Console 主页。

   1b 选择驱动程序 > 在列表中单击相应的驱动程序 > 检查器 > 驱动程序运行状况配置。

2 单击驱动程序运行状态图标 （绿色、黄色和红色）旁边的 + 图标

3 按照修改驱动程序运行状况条件 （第 163 页）和修改驱动程序运行状况操作 （第 165 页）中的说明定义自定义状态的条件和操作。

修改自定义状态

要修改自定义状态，执行下列操作：

1 在 Identity Console 中，打开要创建自定义状态的驱动程序的 " 驱动程序运行状况配置 " 页面：

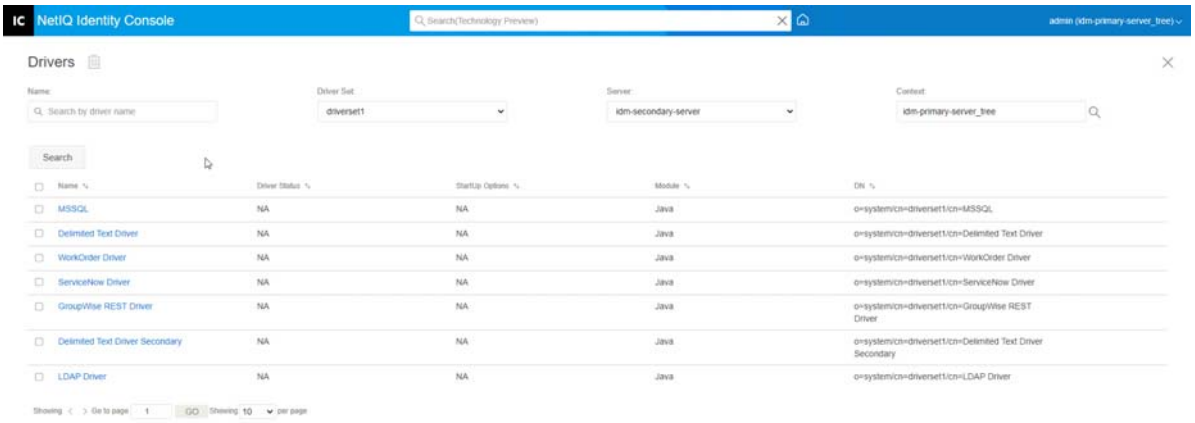
   1a 打开 Identity Console 主页。

   1b 选择驱动程序 > 在列表中单击相应的驱动程序 > 检查器 > 驱动程序运行状况配置。

2 单击驱动程序运行状态图标 （绿色、黄色和红色）旁边的 图标

3 按照修改驱动程序运行状况条件 （第 163 页）和修改驱动程序运行状况操作 （第 165 页）中的说明定义自定义状态的条件和操作。

图 23-6 管理驱动程序检查器



24 管理驱动程序集统计数字

您可以通过 Identity Console 门户查看单个驱动程序或整个驱动程序集的各种统计数字。这包括按类别 （添加、去除、修改等）的超速缓存文件大小、超速缓存文件中未处理的事务大小、最旧和最新的事务以及未处理事务的总数等统计数字。要查看驱动程序集统计数据：

1 在 Identity Console 中，打开驱动程序集统计数字页面。

2 从下拉列表中选择相应的服务器。

显示一个页面，允许您查看驱动程序集中包含的所有驱动程序的统计数字。

- 要刷新统计数据，单击 ⟳ 图标。
- 要关闭驱动程序的统计数字，单击驱动程序统计数字窗口右上角的 ✕ 按钮。
- 要打开所有驱动程序的统计数字，单击操作 > 全部显示。
- 要折叠驱动程序的未处理事务列表，单击列表上方的 ︿ 按钮。要折叠所有驱动程序的未处理事务列表，单击操作 > 折叠所有事务。
- 要展开事务列表，单击 ﹀ 按钮。要展开所有驱动程序的未处理事务列表，单击操作 > 展开所有事务。
- 要关闭禁用驱动程序的统计数字仪表板，单击操作，然后选择关闭禁用的驱动程序。

图 24-1 管理驱动程序集统计数字

25 检查 Identity Manager 对象

您可以使用对象检查器查看对象如何参与 Identity Manager 关系的详细信息。这些关系包括与对象关联的连接系统，数据是如何在身份库和连接系统之间流动，当前存储在身份库和连接系统中的属性值，以及连接系统驱动程序配置等。

要检查 Identity Manager 对象，单击 Identity Console 主页中的对象检查器选项。指定要检查的对象的完整判别名，或单击浏览图标以浏览和选择所需的对象。

连接系统部分列出了与对象关联的每个连接系统。使用对象检查器页面，您可以执行以下操作：

- **添加关联**：要添加与连接系统的新关联，单击 + 图标。浏览并选择集成驱动程序对象并指定关联对象 ID。
- **删除关联**：要删除与连接系统的关联，勾选关联左边的复选框，然后单击 图标。要删除全部关联，勾选 “ 删除 ” 列下方的复选框，然后单击 图标。

图 25-1 检查 Identity Manager 对象

26 管理数据流

数据流在单个视图中显示多个驱动程序的发布者和订购者通道。您可以使用此选项查看和更新所有驱动程序的数据所有权。

要访问数据流的表视图，单击 Identity Console 主页中的数据流 （表视图）模块。然后，浏览并选择相应容器以显示驱动程序列表。

要管理单个驱动程序的数据所有权，执行下列操作：

1 每个驱动程序都有两个按钮来管理发布者和订购者通道的数据流。左侧的按钮管理发布者通道的数据流，右侧的按钮管理订购者通道的数据流。

   1a **同步**：选择此选项以同步特定属性。选择此选项后，发布者通道中图标将改为 ↑，订购者通道中图标将改为 ↓。

   1b **忽略**：选择此选项以停止同步特定属性。选择此选项后图标将更改为 ⊘。

   1c **通知**：选择此选项，以获得对特定属性的任何更改的通知。但更改不会自动同步。选择此选项后图标将更改为 🔔。

   1d **重设置**：选择此选项，将属性值重设置为其他通道指定的值。选择此选项后图标将更改为 ↻。

   注释：可以在发布者或订购者通道上设置此值，但不能同时在两个通道上设置此值。

图 26-1 管理数据流

27 管理权利接收人

权利参考和结果保留在已授予权利或已撤消权利的对象上。权利参考和结果包含该权利当前是否已授予该对象或从该对象撤消的信息。权利接收方是包含权利参照的任何对象。

权利参考

要查看权利参考和结果，单击 Identity Console 主页中的权利接收人选项并选择 “ 权利参考 ”。填写对象的完整判别名 DirXML-EntitlementRecipient。单击 “ 对象选择器 ” 按钮选择对象。

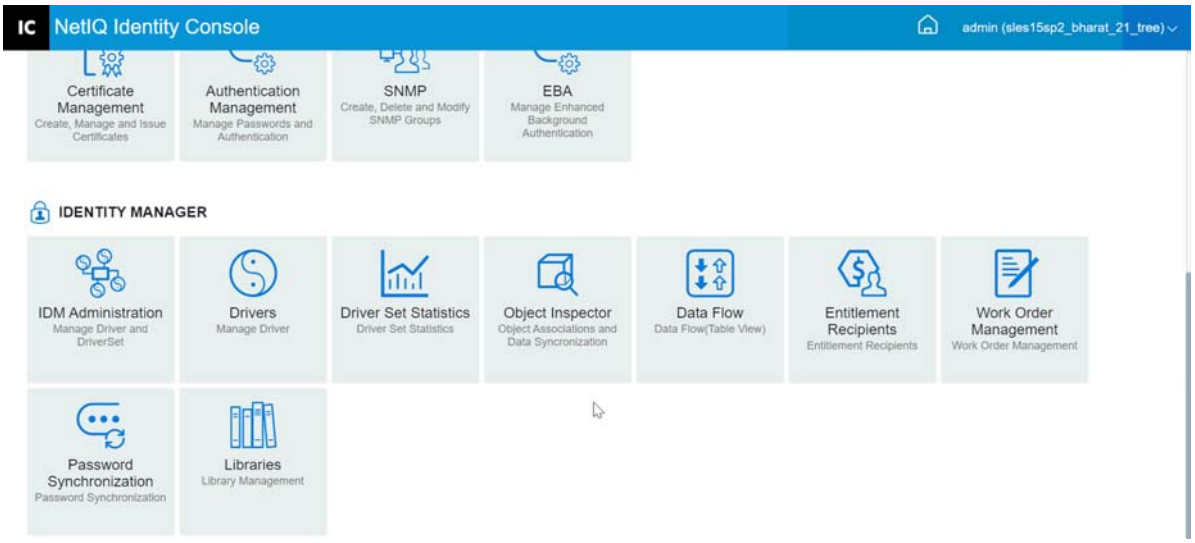
权利结果

Identity Console 权利结果表列出了与选定的对象关联的权利结果。要查看关联的权利，请选择权利 DN。要以 XML 格式查看权利结果，请选择相应的结果 ID。

- **权利结果列标题：**列标题包括权利的完整判别名、它目前的授予或撤销状态 （结果的来源）、结果的状态、任何与结果一同产生的讯息、结果的时戳和结果的标识。
  - **权利 DN：**单击对象权利的完整判别名可以打开 “ 修改对象 ” 页。此页允许您查看将 eDirectory 属性指派给对象的方式。您还可以使用此页修改对象的属性。显示在 “ 修改对象 ” 页上的类别数量取决于选定的对象。
  - **状态：**显示权利已被授予还是撤消。如果插件在 XML 流中找到任何其他值，则它将直接显示此值。
  - **讯息：**DirXML shim 与结果状态关联的任何讯息。存储在 XML 结果文件 <msg></msg> 部分的信息。单击 “ 结果 ID” 项，可在一个 “XML 查看器 ” 页中查看结果的完整细节。
  - **时戳：**权利引擎处理并写入结果的时间。单击 “ 结果 ID” 项，可在一个 “XML 查看器 ” 页中查看结果的完整细节。
  - **结果 ID：**单击 “ 结果 ID” 项，可在一个 “XML 查看器 ” 页中查看结果的完整细节。查看完此结果时，单击 “ 关闭 ”。

要删除一个权利结果项，单击权利结果项左边的复选框，然后选择删除。

图 27-1 管理权利接收人



28 管理工作指令

Identity Manager 驱动程序可以根据驱动程序处理的事件创建工作指令。例如，如果您使用人力资源驱动程序 （SAP HR、 PeopleSoft 等），则可以在添加新用户时让驱动程序生成工作指令。

您可以使用 Identity Console 创建和管理为支持此特定功能的各种驱动程序创建的工作指令。

创建新的工作指令

要创建新工作指令，执行下列步骤：

1. 在 Identity Console 登录页中单击工作指令选项。
2. 单击 + 图标以创建新的工作指令。
3. 指定工作指令的名称，然后单击确定。

   该名称用于身份库中的 WorkOrder 对象的名称。
4. 填写以下字段：

   状态：新工作指令的状态可以是待发或是暂挂。通常，工作指令状态为待发。可以通过选择暂挂停止工作指令。处理工作指令后，此字段显示生成的工作指令状态。

   到期日期：您可以选择使驱动程序立即执行该工作指令或排定该工作指令的日程。要排定 “ 到期日期 ”，单击日历图标。使用日历来选择日期。使用箭头选择月、年和时间。

   重复工作指令：选择此选项，以便多次处理工作指令。通过选择周、日、小时或分钟的数字指定重复工作指令之前的时间间隔。除非手动删除、编辑或驱动程序发送回错误讯息，否则工作指令会在删除日停止重复。

   删除日期：使用日历控制选择日期以删除已配置的工作指令。除非选择即使工作指令有错误，也删除工作指令，否则将不会删除有错误状态的工作指令。

   相关工作指令：当创建新的工作指令时，可以使其附属于一个或多个工作指令。单击 🔍 以浏览并选择相关工作指令。要从列表中去除工作指令，选择工作指令，然后单击 🗑。

   类型：使用此字段指定工作指令类型。驱动程序不更改此属性。当处理该工作指令时，该属性将传递给 WorkToDo 对象。

   工作指令编号：唯一的工作指令编号。此值由公司工作指令系统 （例如，工作指令数据库）指派而不是由 NetIQ eDirectory 指派。

   联系信息：负责工作指令的人的联系信息。

工作指令处理日志：处理工作指令后，驱动程序会在此字段中记录工作指令结果和状态。您可以检查工作指令的当前状态，并确定在尝试配置工作指令时驱动程序遇到的任何问题。

在处理工作指令之前，工作指令的状态属性将保持为待发。到期日期失效时处理工作指令。驱动程序通过将状态属性设置为“已配置”、“警告”或“错误”报告处理结果。如果工作指令是“暂挂”，则它将会忽略该工作指令。

- **待发：**驱动程序正在等待到期日期以完成工作指令。
- **已配置：**已成功处理工作指令。
- **错误：**驱动程序无法执行工作指令。
- **警告：**有一条有关工作指令的警告。例如，如果工作指令有一个到期日期更晚的附属工作指令，则驱动程序会发送一个警告。

说明：工作指令说明。

工作指令内容：驱动程序规则将此字段中的数据用于处理工作指令。例如，它可能是“命令转换”用以处理工作指令的 XML。

删除现有工作指令

要删除现有工作指令，执行下列操作：

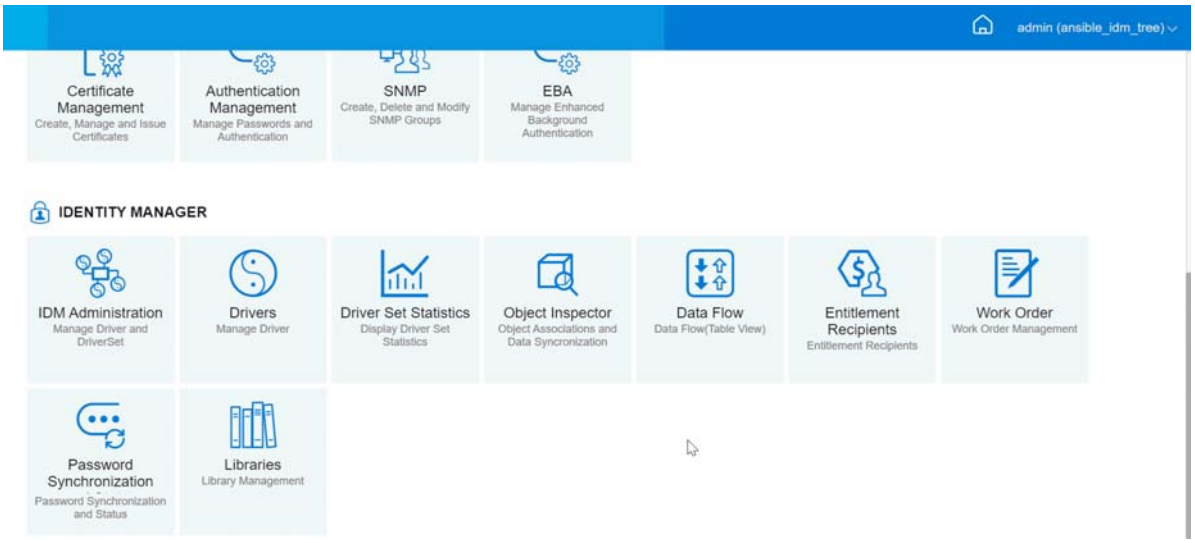
1. 在 Identity Console 登录页中单击工作指令选项。
2. 选择要删除的工作指令。
3. 单击 图标。

过滤工作指令列表

要过滤出工作指令列表，执行下列操作：

1. 在 Identity Console 登录页中单击工作指令选项。
2. 单击“工作指令管理”下的操作。
3. 从下拉菜单中选择过滤类型：
   - **全部显示：**列出与驱动程序关联的所有工作指令。
   - **已配置：**仅列出与驱动程序关联的已配置工作指令。
   - **错误：**仅列出具有错误状态的工作指令。
   - **暂挂：**列出手动暂挂的工作指令。
   - **待发：**列出尚未到期的工作指令。

图 28-1 管理工作指令


admin (ansible_idm_tree)
Certificate Management
Create, Manage and Issue Certificates
Authentication Management
Manage Passwords and Authentication
SNMP
Create, Delete and Modify SNMP Groups
EBA
Manage Enhanced Background Authentication
IDENTITY MANAGER
IDM Administration
Manage Driver and DriverSet
Drivers
Manage Driver
Driver Set Statistics
Display Driver Set Statistics
Object Inspector
Object Associations and Data Syncronization
Data Flow
Data Flow(Table View)
Entitlement Recipients
Entitlement Recipients
Work Order
Work Order Management
Password Synchronization
Password Synchronization and Status
Libraries
Library Management

29 管理口令状态和同步

您可以使用 Identity Console 门户校验单个驱动程序的口令同步和口令状态。若要校验，在 Identity Console 主页中选择口令同步模块。

您可以使用此模块执行以下操作：

- 检查口令同步状态 （第 181 页）
- 校验口令同步设置 （第 182 页）

检查口令同步状态

您可以确定特定用户的分发口令是否与连接系统中的口令相同。执行下列操作以检查口令同步状态：

1. 在 Identity Console 中，选择口令同步 > 口令状态。
2. 浏览并选择要检查口令状态的用户。
3. 可以看到以下口令状态：
   - 口令已同步。
   - 口令未同步。
   - 口令状态未知，因为不能联系已连接系统以请求口令检查。
   - 出现错误。

   注释：要查看有关上述每个状态的更多细节，您必须将鼠标悬停在口令状态列下的状态上。

口令状态任务可使驱动程序执行检查对象口令的操作。并非所有驱动程序都支持口令检查。支持检查的驱动程序的驱动程序清单中必须包含口令检查功能。 Identity Console 不允许将口令检查操作发送给清单中不包含此功能的驱动程序。

检查对象口令操作将检查分发口令。如果分发口令未更新，检查对象口令可能会报告口令未同步。

如果发生以下情况之一，则不会更新分发口令：

- 您正在使用 NDS 口令进行同步或使用通用口令进行同步的同步方法。有关更多信息，请参见使用自定义设置创建口令策略 （第 110 页）。

注释：口令状态操作检查 NDS 口令，而不是身份库的通用口令。因此，如果用户口令策略中未指定将 NDS 口令与通用口令同步，则始终报告未同步口令。而实际上，分发口令和连接系统中的口令可能是同步的，但如果 NDS 口令和分发口令与通用口令不同步，则 “ 检查口令状态 ” 将不会报告准确的结果。

校验口令同步设置

口令同步允许您使用 Identity Manager 同步连接系统的口令。要查看连接系统的口令同步设置，从下拉列表中选择相应的驱动程序集。

使用 " 口令同步 "，可以设置已连接系统以执行以下操作：

- 将口令发布到 Identity Manager。
- 订阅 Identity Manager 或其他连接系统的口令。
- 在已连接系统中实施 " 口令策略 "。
- 发送通知电子邮件。

执行下列操作检查口令同步设置：

1. 在 Identity Console 中，在主页中选择口令同步 > 口令同步。
2. 选择要检查其设置的驱动程序所属的驱动程序集。
3. 单击列表中驱动程序的名称。

注释：启用和禁用的设置因驱动程序而异。只有驱动程序支持的功能设置可用。

---

4. 校验是否正确配置设置。

   Identity Manager 接受口令 （发布者通道）：如果启用此选项， Identity Manager 会允许口令从连接系统流入身份库。禁用此选项意味着不允许 <password> 元素流向 Identity Manager。发布者通道上的口令同步策略会将它们从 XML 中去除。

   此设置应用于连接系统自己提供的用户口令以及发布者通道上的策略创建的口令值。

   如果启用此选项，但禁用下面的分发口令选项，则来自连接系统的 <password> 值将直接写入身份库中的通用口令。如果用户的口令策略不启用 " 通用口令 "，则会将该口令写入到 "NDS 口令 "。

   使用分发口令进行口令同步：只有启用 Identity Manager 接受口令 （发布者通道）设置的情况下，此设置才可用。

   如果启用此选项，则会将来自于连接系统的口令值写入 " 分发口令 "。" 分发口令 " 是可逆的，这意味着可以从口令同步的身份库数据储存中检索到它。它被 Identity Manager 用于与已连接系统进行双向口令同步。对于 Identity Manager，要将口令从此系统分发到其他系统，必须启用此选项。

   只接受符合用户口令策略的口令：仅在启用使用分发口令进行口令同步设置的情况下，此设置才可用。

   如果选择了此选项， Identity Manager 不会将口令从此连接系统写入身份库中的 " 分发口令 " 或将其发布到连接系统，除非口令符合用户的口令策略。

   如果口令不符合，启用 Reset the user's password to the Distribution Password （将用户口令重设置为分发口令）设置，以重设置连接系统中的用户口令。这允许您在连接系统以及身份库中实施口令策略。如果您没有选择此选项，则用户口令可能会在连接系统中失去同步。但是，在决定是否使用此选项时，您需要考虑连接系统的口令策略。一些已连接系统可能不允许重设置，因为它们不允许重复口令。

通过使用通过电子邮件设置通知用户口令同步失败，您可以在无法设置或重设置口令时通知用户。“通知”对于此选项非常有帮助。如果用户更改为已连接系统允许的、但 Identity Manager 因为口令策略拒绝的口令，则用户在收到通知或尝试用旧口令登录到已连接系统之前不会知道该口令已经被重设置。

始终接受口令；忽略口令策略：仅在启用使用分发口令进行口令同步设置的情况下，此设置才可用。

如果选择此选项，则 Identity Manager 不会实施此连接系统的用户口令策略。无论口令策略是否合规， Identity Manager 将此连接系统的口令写入到身份库中的分发口令，并将其分发到其他连接系统。

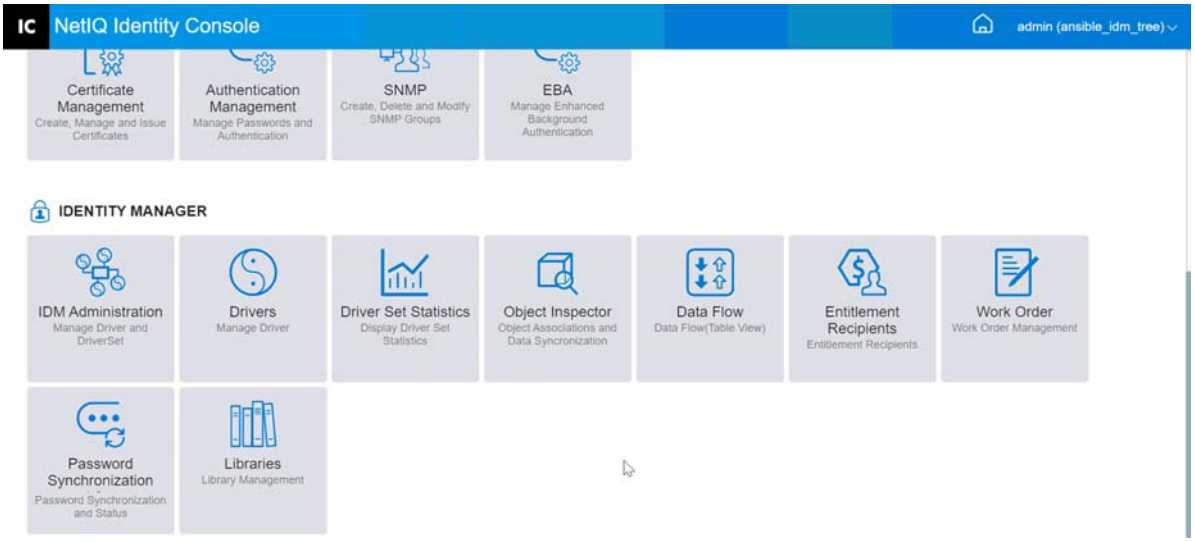
应用程序接受口令（订购者通道）：如果启用此选项，则驱动程序会将口令从身份库发送到此连接系统。这还意味着如果用户在将口令发布到身份库的“分发口令”的另一连接系统中更改口令，则此连接系统中的口令也会更改。

默认情况下，“分发口令”与身份库中的“通用口令”相同，因此在身份库中对“通用口令”所做的更改也会发送到连接系统。

通过电子邮件通知用户口令同步失败：启用此选项的情况下，如果没有同步、设置或重设置口令，则会向用户发送电子邮件。根据电子邮件模板向用户发送的电子邮件。此模板由“口令同步”应用程序提供。但是，要使模板工作，必须自定义它并指定要发送通知讯息的电子邮件服务器。有关说明，请参阅 *《NetIQ Identity Manager Password Management Guide》*（NetIQ Identity Manager 口令管理指南）中的 Configuring E-Mail Notification （配置电子邮件通知）。

5 完成后，单击保存以保存您的更改。这些设置将保存为“全局配置值”。

图 29-1 管理口令同步



30 管理库

库对象存储由一个或多个驱动程序共享的多个策略和其他资源。可以在驱动程序集对象或任何 eDirectory 容器中创建库对象。一个 eDirectory 树中可以有多个库。只要运行驱动程序的服务器持有库对象的读 / 写或主复本，驱动程序就可以引用树中的任何库。

样式表、策略、规则和其他资源对象可以存储在库中，并由一个或多个驱动程序参照。

使用库管理模块可以执行以下任务：

- 查看和删除现有库 （第 185 页）
- 查看和删除库中的对象 （第 185 页）

查看和删除现有库

要查看和删除现有库，执行下列操作：

1. 在 Identity Console 中，从主页选择库模块。
2. 在列表中选择相应的库。
3. 单击 图标。单击确定确认该操作。

查看和删除库中的对象

您可以查看和删除库对象中的策略以及映射表。要删除对象，执行下列操作：

1. 在 Identity Console 中，从主页选择库模块。
2. 单击列表中的相应库。
3. 要删除策略，选择策略选项卡。
4. 从列表中选择相应策略并单击 图标。
5. 要删除映射表，选择映射表选项卡。
6. 从列表中选择相应的映射表并单击 图标。
7. 单击确定确认该操作。

图 30-1 管理库


IC
NetIQ Identity Console
搜索
admin (idm485b_tree)
证书管理
创建、管理和颁发证书
鉴定管理
管理口令和鉴定
SNMP
创建、删除和修改 SNMP 组
EBA
管理增强后台鉴定 (Enhanced Background Authentication)
IDENTITY MANAGER
IDM 管理
管理驱动程序和驱动程序集
驱动程序
管理驱动程序
驱动程序集统计数字
驱动程序集统计数字
对象检查器
对象数据同步检查器
数据流
数据流（表视图）
权利接收人
权利接收人
工作指令管理
工作指令管理
口令同步
口令同步
库
库管理
电子邮件服务器配置
电子邮件服务器配置
电子邮件通知模板
电子邮件通知模板
基于角色的权利
基于角色的权利

31 管理电子邮件服务器选项

可以使用 “ 电子邮件服务器选项 ” 指定 SMTP 电子邮件服务器的设置。

主机名

您的 SMTP 电子邮件服务器的主机名。也可以是 IP 地址。您还可以指定一个自定义端口，后接主机名或 IP 地址。

重要：使用冒号 (:) 来分隔主机名或 IP 地址与端口。

寄件人

您可以指定一个有效的电子邮件地址，该地址将显示为电子邮件标头的 “ 发件人 ” 字段。

超时值

超时选项允许您设置发送通知电子邮件的时间限制 （以秒为单位）。

启用 SSL

如果需要，您可以选择启用 SSL 选项。

使用身份凭证鉴定到服务器

用于安全的 SMTP 服务器。如果服务器需要在发送电子邮件之前鉴定，则请在此处指定用户名和口令。

尽管在这里指定了鉴定信息，但是可能还需要为发送通知电子邮件的应用程序单独指定。

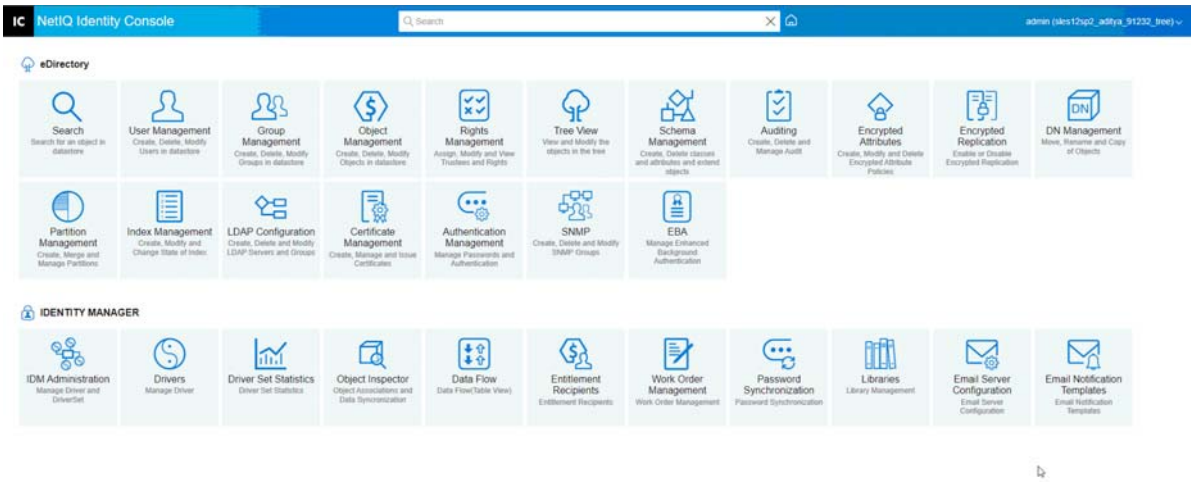
例如，可以使用在这里指定的鉴定信息发送 “ 忘记口令 ” 电子邮件通知。但是， “Identity Manager 口令同步 ” 使用驱动程序策略发送通知电子邮件。可能也需要提供该驱动程序策略中的鉴定信息。

要对服务器进行鉴定，执行以下步骤：

1. 选择**通过使用身份凭证对服务器进行鉴定**选项。
2. 指定**用户名**和**口令**。
3. 单击**测试服务器连接**以验证连接性。
4. 单击**保存**。

注释：保存身份凭证细节后，**测试服务器连接**将被禁用。

图 31-1 电子邮件服务器配置



32 管理电子邮件模板

此列表显示了可用的通知模板。使用这些模板可以向此树中的用户发送电子邮件讯息。可以使用您自己的文本自定义这些模板。

有些应用程序提供他们自己的模板。这些模板对象在安全性容器内，通常可以在树的根部找到。

可以按名称、日期或主题对列表进行排序。

主题

用户在电子邮件 “ 主题 ” 标题中看到的文本。要编辑一个模板，单击该模板的 “ 主题 ” 标题。通过使用 “ 编辑电子邮件通知模板 ” 界面，您可以修改模板及其细节。

模板名称

每个模板有一个唯一名称。发送电子邮件的应用程序参照此名称。

上次修改时间

上次修改模板的日期和时间。

新建

让您可以创建一个新的电子邮件模板。

1. 单击 + 图标。
2. 指定新模板的名称 （例如， Approval），然后单击确定。

如果您禁用了弹出菜单，则返回到 “ 编辑电子邮件通知模板 ” 弹出菜单。新模板名称显示在 “ 名称 ” 列中，但是 “[No Subject] （无主题） ” 显示在 “ 主题 ” 标题列中。在此情况下，单击 “[无主题]” 可以提供该新模板的详细信息。

编辑电子邮件通知模板

使用 “ 编辑电子邮件通知模板 ” 页可以修改电子邮件模板。可以使用自己的文本自定义模板。

模板名称

显示模板的名称。

主题

用户在电子邮件 “ 主题 ” 标题中看到的文本。可以更改主题行的文本。模板的实际名称保持相同。

发送方式

SMTP 服务器用于发送电子邮件的格式：文本或 HTML。

令牌或替换标记

这些替换标记可帮助您为用户个性化讯息。可以从可用标记列表中复制替换标记，并将它们粘贴到讯息中。

每个模板包括默认令牌或替换标记，是用户个性化电子邮件所需要的变量。例如，将口令发送给用户的 " 忘记口令 " 电子邮件模板包括名为 "CurrentPassword" 的默认令牌或替换标记。

添加：您可以定义要在讯息的正文部分使用的其它令牌或替换标记。

要添加令牌或替换标记，执行以下步骤：

1. 单击  图标。
2. 在添加替换标记窗口中指定名称和说明。
3. 单击确定。
4. 新令牌或替换标记列在 " 替换标记 " 列中。

复制标记：单击  将所选标记复制到系统缓冲区，然后您可以单击鼠标粘贴并在邮件的主题行或邮件正文中使用。

删除：在列表中选择令牌或替换标记，然后单击  从列表中删除该标记。请确保不会去除讯息正文所需的标记。

讯息正文

电子邮件讯息文本。

指定所有电子邮件通知模板修改后，单击更新。

删除

（从身份库中）去除已经创建的模板。您无法删除 Identity Manager 等应用程序附带的默认模板。

1. 选择要删除的模板。

   如果单击模板的 " 主题 " 标题，则 Identity Console 将显示 Edit Email Templates （编辑电子邮件模板）对话框。
2. 单击 " 删除 " 图标。
3. 单击确定。

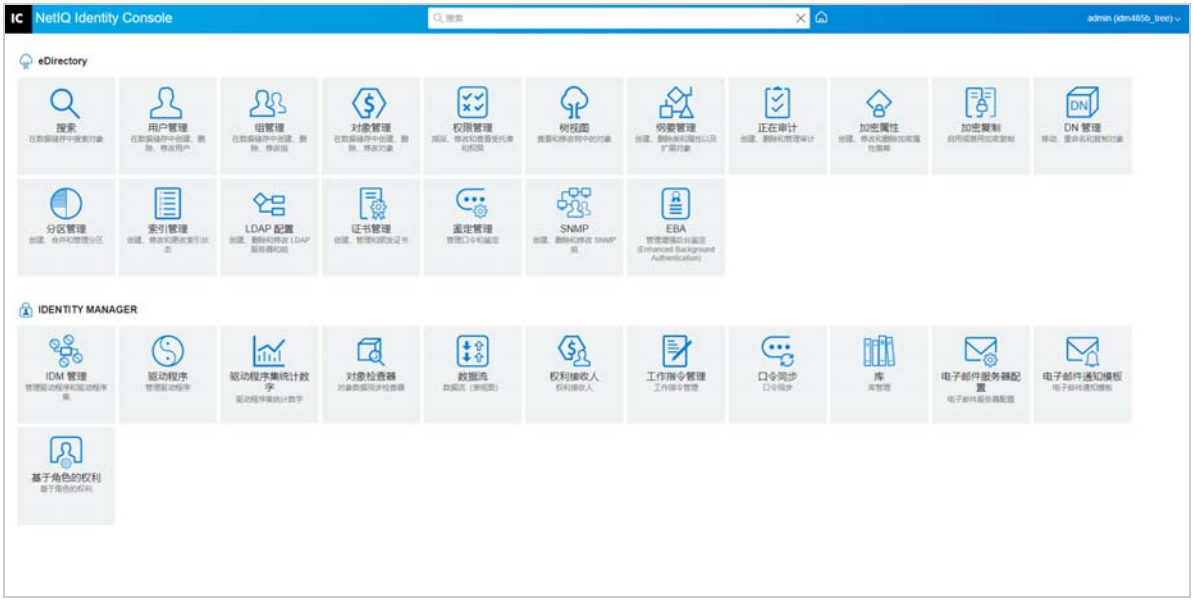
过滤器模板

使您能够过滤要显示的电子邮件模板。仅显示选定的模板。 Filter by all （过滤条件：所有）选项显示所有模板。

刷新模板

单击该 图标刷新并去除任何应用的过滤器模板。

图 32-1 *电子邮件通知模板*



33 管理基于角色的权利

“ 基于角色的权利 ” 允许您将已连接系统上的权利授予一组 NetIQ® Identity Console 用户。通过 “ 基于角色的权利 ” 策略，可以简化业务策略管理，减少配置 Identity Manager 驱动程序的需要。

“ 基于角色的权利 ” 模块包括：

基于角色的权利

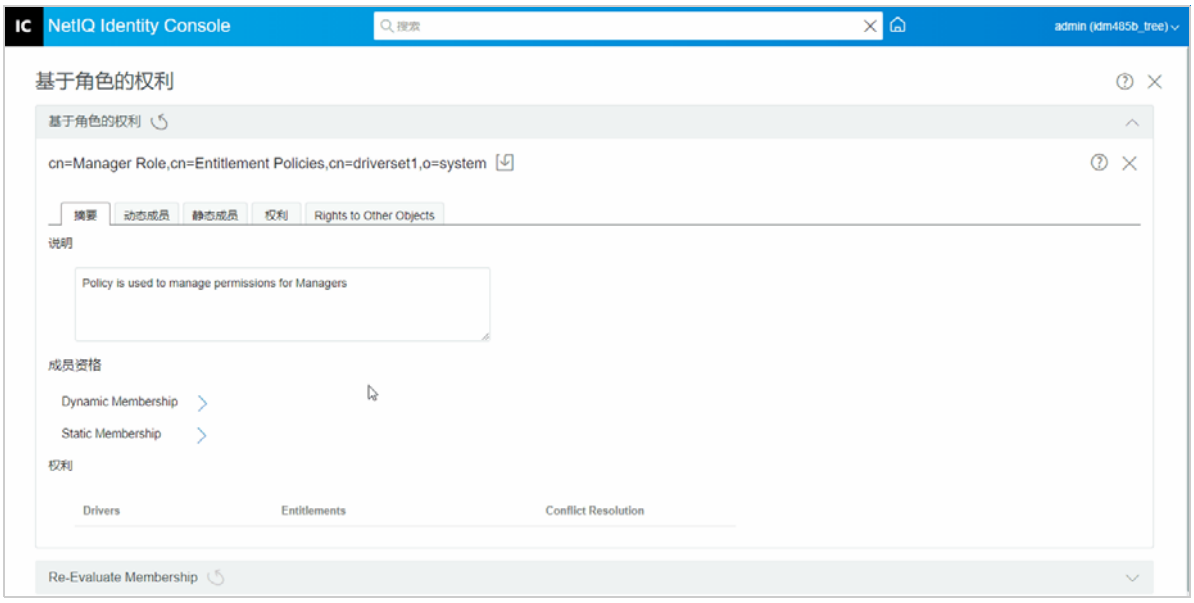
“ 基于角色的权利 ” 策略是 Identity Console 动态组对象，并具有附加功能以允许您授予已连接系统上的 “ 基于角色的权利 ”。创建一项 “ 基于角色的权利 ” 策略时，可以为策略定义成员资格和应授予 “ 基于角色的权利 ” 策略成员的权利。每个 “ 基于角色的权利 ” 策略都和被指派给某个特定服务器的单个驱动程序集对象关联。和 Identity Manager 驱动程序一样，每个权利策略仅能管理该策略所指派到的服务器的主复本或读 / 写复本中的对象。

以下各节详细介绍了基于角色的授权：

摘要

此页汇总了权利策略的成员资格准则和权利的高级别视图。

图 33-1 摘要页



成员资格：

为动态成员资格指定的准则以 LDAP 过滤器的语法显示。“ 搜索身份 ” 表示当查询动态成员资格时，使用哪个对象的权限，“ 基本 DN” 和 “ 范围 ” 表示在查询中包含树的哪些部分。

通过选择该复选框，可以查看静态成员资格包含项和排除项。

在 “ 摘要 ” 页上不显示所有成员的组合列表，因为该列表可能很长。要查看权利策略所有成员 （包括动态和静态）的组合列表，使用 “ 成员资格 ”>“ 查看成员资格 ” 选项卡。

权利：

授予给权利策略成员的已连接系统上的权利。请谨记，基于角色的权利与已连接系统是松散一致的。这表示已连接系统的权利状态没有显示在权利策略界面上。如果要将权利授予权利策略，则以后该权利不再在已连接系统中可用，但仍会列在权利策略中直到被手动去除。

冲突解决方法：

对于具有值的 “ 基于角色的权利 ”，如果两个或更多 “ 基于角色的权利 ” 策略向一个用户授予了不同的值，这些方法用于确定授予用户的值。具有值的权利的一个示例是，在电子邮件分发列表中的成员资格，其中值是分发列表的名称。

冲突解决方法为在每个驱动程序对象上为每个权利分别设置。如果一个权利用于多个 “ 基于角色的权利 ” 策略，该冲突解决方法在所有 “ 基于角色的权利 ” 策略中都是相同的。要为权利更改冲突解决方法，在驱动程序的驱动程序清单中更改该权利的设置。

- **无法识别：**“ 基于角色的权利 ” 策略尚未在向导中完成，或者在驱动程序清单中输入的设置不正确。
- **合并：**默认设置是 “ 合并 ”（驱动程序清单中的 union）。这表明用户被授予了其所属的所有 “ 基于角色的权利 ” 策略中的所有值。

  当使用默认设置 “ 合并 ” 时，策略列表的优先级顺序对于此特定的权利是不重要的。

例如，用户被两个不同的“基于角色的权利”策略 （“管理员”策略和“小组成员”策略）授予了 GroupWise® Driver A 的电子邮件分发列表的成员资格。在策略 1 中，该用户被授予在“管理员”电子邮件分发列表中的成员资格，在策略 2 中，该用户被授予“小组成员”电子邮件分发列表中的成员资格。使用“合并”设置，用户同时被授予两个电子邮件列表中的成员资格。

- **优先级：**此设置表示如果多个“基于角色的权利”策略向一个用户授予同一驱动程序对象中同一权利的不同值，则用户仅被授予列表中最上面的“基于角色的权利”策略指定的值。

  当使用“优先级”设置时，策略列表的优先级顺序对于此特定的权利是重要的。

  例如，用户被两个不同的“基于角色的权利”策略 （“管理员”策略和“小组成员”策略）授予了 Identity Manager Driver for GroupWise A 的电子邮件分发列表的成员资格。在“管理员”策略中，该用户被授予在“管理员”电子邮件分发列表中的成员资格，在“小组成员”策略中，该用户被授予“小组成员”电子邮件分发列表中的成员资格。在策略列表中，“管理员”策略比“小组成员”策略位置高。使用“优先级”设置，用户仅被授予“管理员”电子邮件分发列表中的成员资格。

  对冲突解决方法使用优先级可能是有用的，例如，在已连接系统上的属性仅允许单个值。如果对于同一用户，两个不同的“基于角色的权利”策略为该属性授予值，则用户仅接收列表中最高级别的“基于角色的权利”策略授予的值。

注释：对没有值的权利 （例如，帐户），不提供冲突解决方法设置。没有值的权利始终授予给“基于角色的权利”策略中的成员，而不考虑列表中的策略优先级。

动态成员

为动态成员资格指定的准则以 LDAP 过滤器的语法显示。“搜索身份”表示当查询动态成员资格时，使用哪个对象的权限，“基本 DN”和“范围”表示在查询中包含树的哪些部分。

成员资格过滤器

您可以定义成员资格的准则，如在树中的位置和对象的属性。例如，成员资格可以取决于用户是否在活动容器中，或职位是否包括“管理员”字样。满足此准则的用户将自动成为“基于角色的权利”策略的成员，而不需要将每个用户专门添加到该策略中。动态成员资格和动态组对象相同。

如果某个对象因更改而不再满足动态成员资格的准则，则下次重评估该用户时，权利将自动撤销。

设置搜索参数

指定要“权利策略”管理的用户的位置。选择保存用户的容器（基本 DN），以及要从该容器继续向下搜索的距离（搜索的范围）。对于要在指定的容器中管理用户的“权利策略”，用户必须在服务器上的读 / 写复本或主复本中。

为“搜索范围”提供的以下选项：

- 此容器及其子容器：如果树中此容器以下的用户符合为动态成员资格指定的准则，则他们是“权利策略”的成员。如果子容器中的用户符合准则，则它们也是成员。
- 仅此容器：仅当此容器中的用户符合为动态成员资格指定的准则时，它们才是“权利策略”的成员。即使此容器下子容器中的用户符合准则，它们也不是成员。

定义过滤器准则

指定确定用户是“权利策略”成员的特征。

在“权利策略”的“摘要”页中，指定的动态成员资格准则会以 LDAP 过滤器的语法显示。

默认情况下，动态成员资格被设置为将所有用户类对象（和从用户类派生出的类对象）作为“权利策略”的成员包含在搜索范围内。

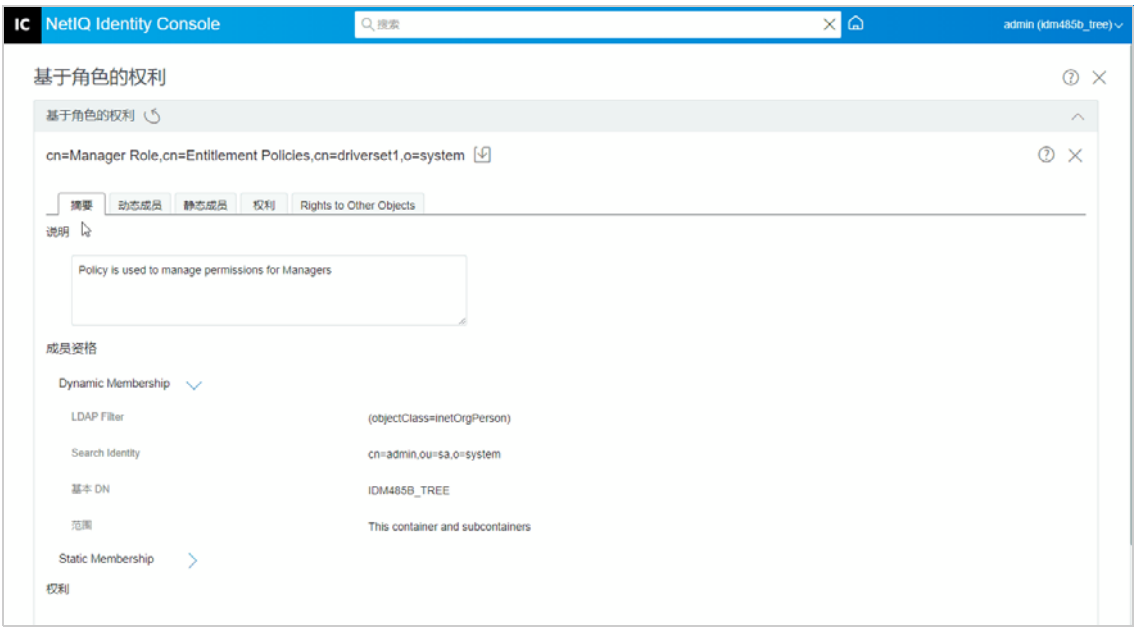
注释：如果创建从用户派生出来的新的对象类，则在您对权利策略作出修改之前，现有的“权利策略”不会意识到该类。这样可以避免新类的用户无意识地授予权利。在对“权利策略”作出任何修改后，会更新该策略的派生用户类列表。

创建动态成员资格

在“动态成员”选项卡上，执行以下操作：

1. 单击动态成员选项卡。
2. 根据需要使用搜索身份、搜索开始于和搜索范围过滤器。
3. 单击特定的创建组创建新条件或行，然后提供所需的搜索准则或条件。

图 33-2 动态成员



搜索范围：“搜索范围”指示位于搜索基本 DN 或其以下的条目集，这些条目可能被视为搜索操作的潜在匹配项。

搜索准则：您可以限制搜索，以帮助您从大量记录中查找特定记录或记录组。

基本 DN：基本 DN 是服务器搜索用户的起点。

LDAP 组：用户、组和组织单元（用户和组的容器）的分层组织。

注释：用户可以创建具有条件的单个或多个组。条件由属性、运算符和值组成。默认情况下，填充对象类 > 等于 > 用户。

静态成员

静态成员是使用静态关键字声明的成员类。静态成员具有某些有限的访问权限。

在“静态成员”选项卡上，可以执行以下操作：

包括成员：

静态添加动态成员资格筛选器未包含的成员。

排除成员：

排除满足过滤器准则但不应包含在权利策略中的成员。

权利

基于角色的权利允许您在连接的系统上授予权利，在 Identity Manager 中授予权限。权利可为以下一种：

- 已连接系统的帐户。

- 已连接系统电子邮件分发列表中的成员资格。
- 已连接系统的组成员资格。
- 已连接系统的相应对象的属性 （由指定值填充）。

注释：因为权利功能是 Identity Manager 的一部分，所以在可以授予已连接系统上的权利之前，您必须已经安装 Identity Manager 驱动程序，并且将其配置为支持权利。

创建权利

在 " 权利 " 选项卡上，执行以下操作：

1. 单击权利选项卡。
2. 单击 ＋ 以添加驱动程序并提供连接的系统中的权利。

   显示添加驱动程序屏幕。
3. 从下拉菜单中选择驱动程序。
4. 单击添加。

   显示添加权利屏幕。
5. 从下拉菜单中选择要添加的权利组。
6. 选择查询类型：
   - **超速缓存：**以前运行查询时。
   - **外部查询：**当查询是新的时。

   显示添加组权利屏幕。
7. 从下拉菜单中选择组权利，然后单击选择。

对其他对象的权利

使用此页可以向权利策略提供 eDirectory 对象的受托者权限。权利策略的每个成员都成为该对象的一个受托者。

除了指派所有属性的权限，还可以单击 " 添加属性 " 以指派特定属性的权限。

" 继承 " 复选框确定权限是否在树中向下流动。例如，如果您要向容器对象指派权限，并且希望权利策略对此对象以及该容器下子容器具有相同的权限，请选择 " 继承 " 复选框。

当您在此页上完成更改后， eDirectory 中的对象的权限将被授予权利策略成员。相反，下次为该用户修改用于动态成员资格的属性时，或移动或重命名该用户时，已连接系统中的权利将被授予给权利策略的每个成员。（当撤销权限或权利时，情况相同。）使用 " 再评估成员资格 " 任务以强制更新。

创建对其他对象的权限

要创建权限：

1. 单击 **Rights to other Objects** （对其他对象的权限）选项卡。

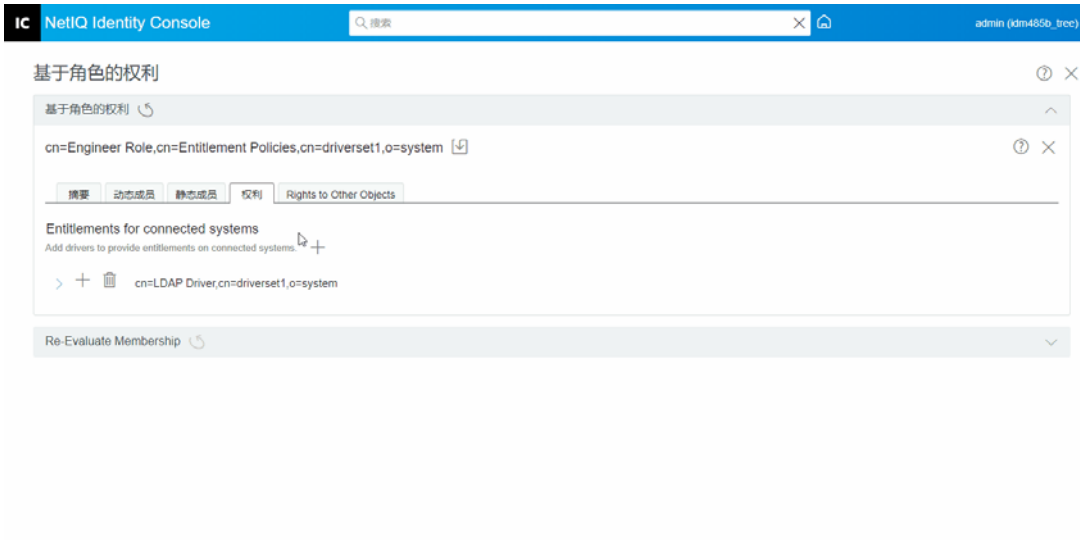
在这里，您可以添加一个新对象，并浏览希望此权利策略成为其受托者的对象。

1a 要添加对象，单击 + 按钮。

显示环境浏览器页面。该页面由对象组成。

1b 展开对象，然后根据您的要求选择组或单个用户，并为其指派权限。

图 33-3 对其他对象的权利

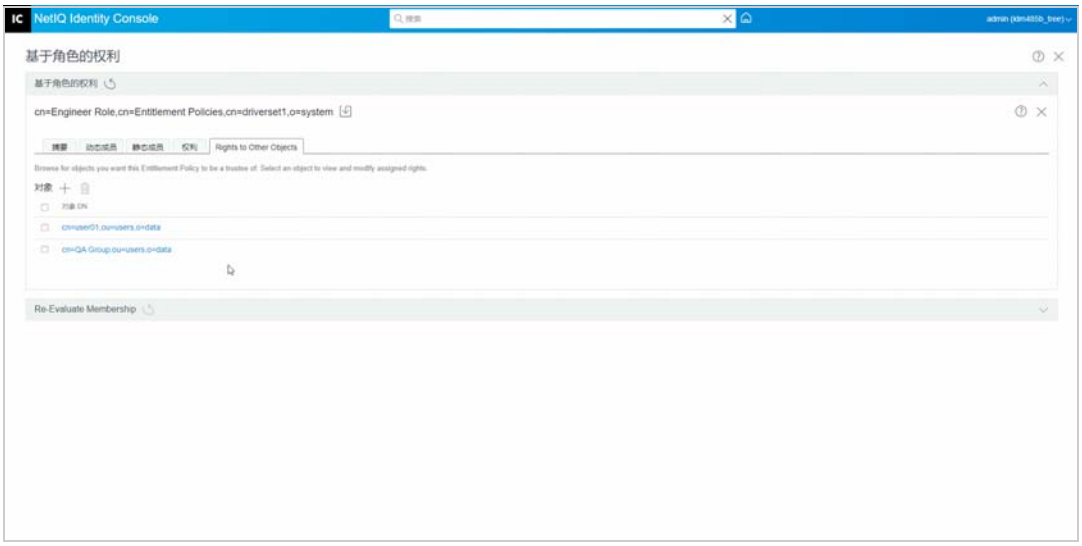


1c 要添加更多属性，请单击 +。

显示选择属性页。此页包含对象可以具有的属性列表。

1d 单击完成。

图 33-4 选择属性



2 （可选）用上和下 箭头对“基于角色的权利”策略进行优先级排序。

确定策略的优先级是为了解决多个策略之间的权利冲突。最顶层的策略具有最高优先级。有关详细信息，请参见：确定“基于角色的权利”策略的优先级 （第 200 页）

确定“基于角色的权利”策略的优先级

创建“基于角色的权利”策略时，影响特定用户的策略可能有冲突。

列表中的“基于角色的权利”策略顺序代表优先级。可以使用向上箭头和向下箭头按钮更改列表中的顺序。

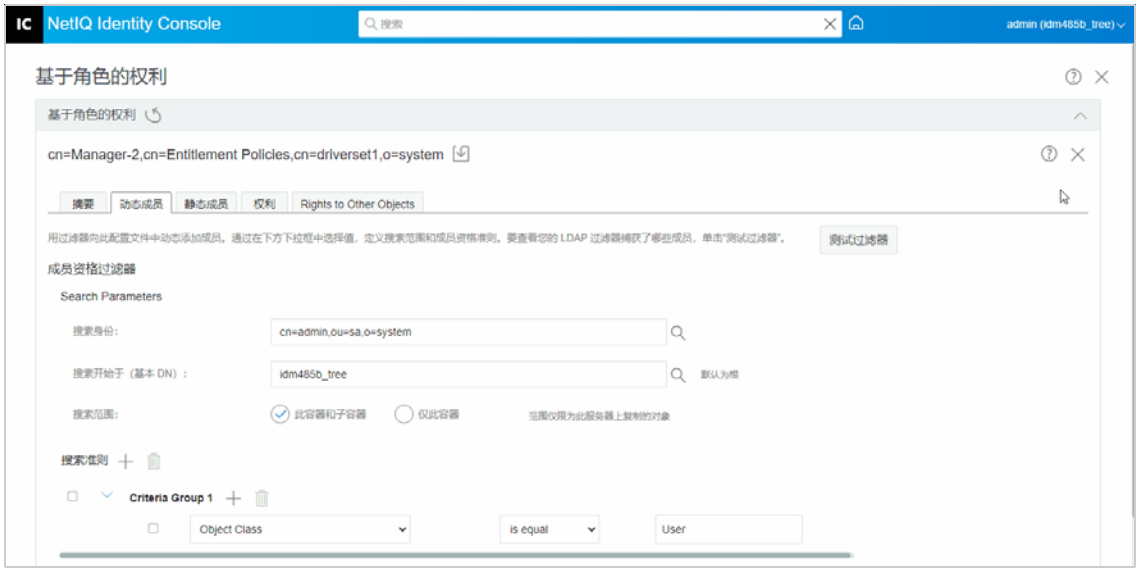
- 如果已连接系统的某个属性仅允许单值，该设置可能有用。如果对于同一用户，两个不同的“基于角色的权利”策略为该属性授予值，则用户接收列表中最高级别的“基于角色的权利”策略授予的值。再比如，您可能将环境配置为用权利将用户放置到另一系统的分级结构中。您希望将用户放置在某个位置上，而不是同时置于两个位置。
- 请牢记该设置与每个驱动程序提供的每个权利无关。
- 通常，在列表中应该将管理员 (administrator) 或管理员 (manager) 策略置于高于终端用户或个别贡献者策略的位置。应将较窄成员资格的组放在高于较宽成员资格的组之上。

要确定“基于角色的权利”策略的优先级，请执行以下操作：

1 选择要升级或降级的权利策略。

2 用上或下 箭头对“基于角色的权利”策略进行优先级排序。

图 33-5 确定策略的优先级

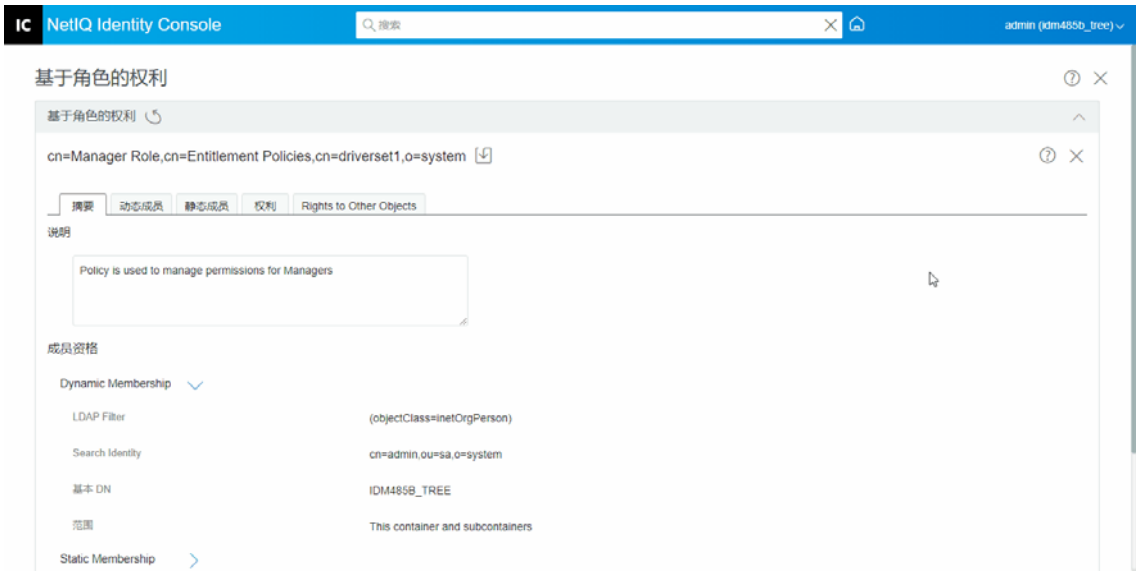


3 单击保存 按钮。

策略成员资格细节的摘要显示在摘要选项卡中。

4 重启动驱动程序。

图 33-6 关闭并重启动



注释：注意：必须重启动驱动程序才能使更改生效。

重新评估成员资格

基于角色的权利功能可让您将针对连接系统的权利授予一组用户。

当创建或编辑 " 基于角色的权利 " 策略后，必须重新评估每个用户的成员资格，以确定是否需要授予、更改或撤销已连接系统的权利。默认情况下，下一次为每个用户更改影响成员资格的属性时，或移动和重命名用户时，每次对一个用户进行重新评估。此默认行为最大程度地减少了对系统资源的使用，但是也意味着更改 " 基于角色的权利 " 策略的时间和为特定用户授予、更改或撤消权利的时间之间有严重的延迟。

可以使用 重新评估 " 基于角色的权利 " 策略 （第 202 页）任务指定要立即重新评估的用户，以确保一次性更新所有的用户权利。我们建议每次创建或编辑 " 基于角色的权利 " 策略都执行此操作。

Identity Manager 3.6 之前是针对驱动程序集中的所有 （而非单个权利策略） " 基于角色的权利 " 策略重新评估成员资格。但是， Identity Manager 3.6 允许您评估 " 基于角色的权利 " 策略并将其成员添加到所选的对象列表中。如果定义了一个权利策略并创建了成员资格列表，将在所选对象项旁看到 " 评估权利策略以将其成员添加到列表中 " 标题。选择该策略，然后单击 ＋ 图标将策略的成员添加到所选对象列表中。您可以向所选对象列表添加成员或对象或从列表中去除成员和对象。

要最大限度的使用系统资源，在使用 重新评估 " 基于角色的权利 " 策略 （第 202 页）前，应对特定驱动程序集中的 " 基于角色的权利 " 策略作出所有更改。

注释：重新评估权利只对已连接系统上的权利是必需的。当为一个 " 基于角色的权利 " 策略更改 Identity Console 权限时，这些更改对每个用户会立即生效。要执行成员资格重新评估，权利服务驱动程序必须在运行。

重新评估“基于角色的权利”策略

要重新评估成员资格：

1 单击重新评估成员资格 > 选择驱动程序集。

将显示已创建策略的列表。

2 选择需要评估的策略，然后单击评估 Evaluate。

对象选项卡上显示属于该组的用户。

3 （可选）要添加特定用户，请单击 +。

仅当列表中缺少用户，并且您想要添加特定用户时，才能使用此添加 + 功能。

4 （可选）要去除特定用户，请单击 🗑。

仅当需要从列表中去除特定用户时，才能使用删除 🗑 功能。

5 单击重新评估成员资格按钮 ▷。

图 33-7 重新评估成员资格