CA Identity Manager™

配置指南

12.6.4

ca technologies

联系技术支持

要获取在线技术帮助以及办公地址、主要服务时间和电话号码的完整列表，请联系技术支持：http://www.ca.com/worldwide。

CA Technologies 产品引用

本文档参考以下 CA 产品：

- CA Identity Manager
- CA Siteminder®
- CA Directory
- CA User Activity Reporting
- CA Identity Governance

目录

第 1 章： CA Identity Manager 环境简介

此部分包含以下主题：

CA Identity Manager 环境组件

CA Identity Manager *环境*是一个管理命名空间的视图，允许 CA Identity Manager 管理员管理用户、组和组织等对象。 为这些对象分配了关联角色和任务集。 CA Identity Manager 环境可以控制目录的管理和图形表示。

单个用户存储可以关联多个 CA Identity Manager 环境 (p. 14)以定义该目录的不同视图。 然而，一个 CA Identity Manager 环境只能与一个用户存储关联。

CA Identity Manager 环境包含以下元素：

目录

描述一个与 CA Identity Manager 关联的用户存储。 目录元素包括：

- 用户存储的指针，存储了用户、组和组织等管理对象。
- 描述管理对象如何存储在目录中以及其在 CA Identity Manager 中的表示的元数据。

配给目录（可选）

存储与配给服务器相关的数据以管理管理端点中的其他帐户。 一个环境只能与一个配给目录关联。

注意：有关配给服务器或配给目录的更多信息，请参阅 *《安装指南》*。

用户控制台

支持 CA Identity Manager 管理员在 CA Identity Manager 环境中执行任务。

任务和角色定义

确定在 CA Identity Manager 和其他应用程序中的用户权限。这些任务和角色定义最初在 CA Identity Manager 环境中可用，且可以将它们分配给用户。

您可以使用“用户控制台”自定义默认角色和任务。

自助服务

允许用户创建和维护各自访问资源（如客户 Web 站点）的帐户。 自助服务也允许用户在忘记当前密码的情况下索取临时密码。

工作流定义

CA Identity Manager 包含可实现用户管理任务的审批和通知自动化的默认工作流定义，如创建用户配置文件或将用户分配到角色或组。您可以在 CA Identity Manager 中修改默认工作流流程以满足每个企业的需求。

面板

确定 CA Identity Manager 用户界面的外观。

自定义功能

您可以使用 CA Identity Manager API 修改 CA Identity Manager，使之符合您的业务要求。 请参阅 *《Programming Guide for Java》*。

每个 CA Identity Manager 环境都需要一名或多名系统管理员来使用“用户控制台”自定义初始角色和任务。一旦系统管理员创建了初始角色和任务，该管理员就可以向环境中的用户授予管理权限。 这些用户将成为管理用户、组和组织的管理员。 请参阅 *《管理指南》*。

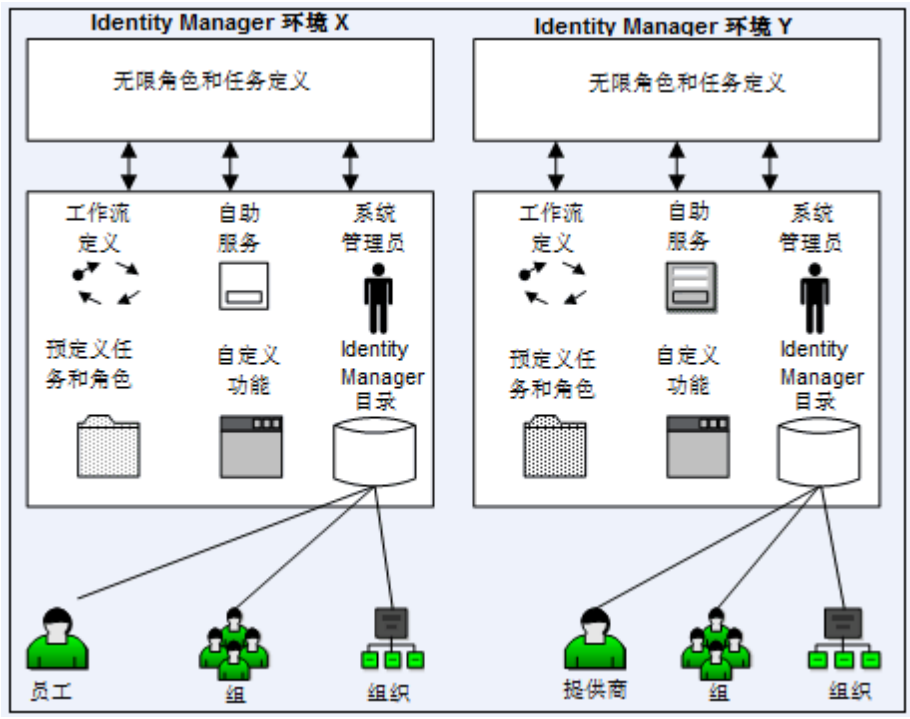
多个 CA Identity Manager 环境

根据需要创建多个 CA Identity Manager 环境：

管理其他用户存储－您可以管理不同类型的用户存储中的用户。 例如，您的公司将其所有用户配置文件存储在 Sun Java 系统 LDAP 目录中。您进入一家合资企业，其合作伙伴使用 Oracle 数据库存储用户信息。 您希望每组用户具有不同的 CA Identity Manager 环境。

- 管理具有不同 LDAP 对象类的对象－考虑 CA Identity Manager 正在管理 LDAP 目录。 在同一目录中，您可以管理具有不同对象类和属性的同一类型的对象。 例如，下图显示了包含两种类型的用户的目录：
  - 具有员工 ID 号的员工。
  - 由供应商编号识别的供应商。

公式 1: 图表显示两个 Identity Manager 环境的示例，其中的目录包含员工和供应商。



CA Identity Manager 管理控制台

作为 CA Identity Manager 系统管理员，您的职责包括：

- 创建 CA Identity Manager 目录
- 配置配给目录
- 配置 CA Identity Manager 环境
- 分配系统管理员
- 启用供初始使用的自定义功能

要配置 CA Identity Manager 环境，请使用基于 Web 的应用程序“管理控制台”。

管理控制台分为以下两部分：

- “Directories”（目录）－使用此部分创建和管理 CA Identity Manager 目录和配给目录，用于描述与 CA Identity Manager 关联的用户存储。
- “Environments”（环境）－使用此部分创建和管理 CA Identity Manager 环境，用于控制目录的管理和图形展示。

如何访问 CA Identity Manager 管理控制台

通过在浏览器中输入以下 URL 访问管理控制台：

http://*hostname:port*/iam/immanage

hostname

定义安装了 CA Identity Manager 的服务器的完全限定域名或 IP 地址。

注意：如果您正在使用 Internet Explorer 7 访问“管理控制台”，且主机名包括 IPv6 地址，则可能会错误显示管理控制台。 若要防止此问题发生，请使用完全限定的主机名或 IPv4 地址。

端口

定义应用程序服务器端口。

注意：如果您正在使用 Web 代理提供面向 CA Identity Manager 的高级身份验证，则不需要指定端口号。

注意：在您用来访问管理控制台的浏览器中，启用 Javascript。

管理控制台的示例路径：

- 对于地质网络日志：

  http://myserver.mycompany.org:7001/iam/immanage

- 对于 JBoss：

  http://myserver.mycompany.org:8080/iam/immanage

- 对于 WebSphere：

  http://myserver.mycompany.org:9080/iam/immanage

如何创建 CA Identity Manager 环境

要创建 CA Identity Manager 环境，请在“管理控制台”中完成以下步骤：

1. 使用目录配置向导 (p. 132)创建 CA Identity Manager 目录。
2. 如果您的环境包括配给，再次使用“目录配置向导”来创建配给目录 (p. 145)。
3. 创建 CA Identity Manager 环境。
4. 访问环境 (p. 164)以确认它正在运行。

第 2 章： 示例 CA Identity Manager 环境

此部分包含以下主题：

示例 CA Identity Manager 环境概述

CA Identity Manager 包括您可以用于了解和测试 CA Identity Manager 的环境示例。

环境示例基于名为 NeteAuto 的汽车贸易公司。NeteAuto 管理员使用 CA Identity Manager 来管理员工、供应商和区域经销商。

使用示例 NeteAuto 环境的用户存储配置是：

- 支持组织的 LDAP 用户存储
- 不支持组织的 LDAP 用户存储。
- 支持组织的关系数据库用户存储
- 不支持组织的关系数据库用户存储。

注意：配给功能不可用，因为此环境无配给目录。

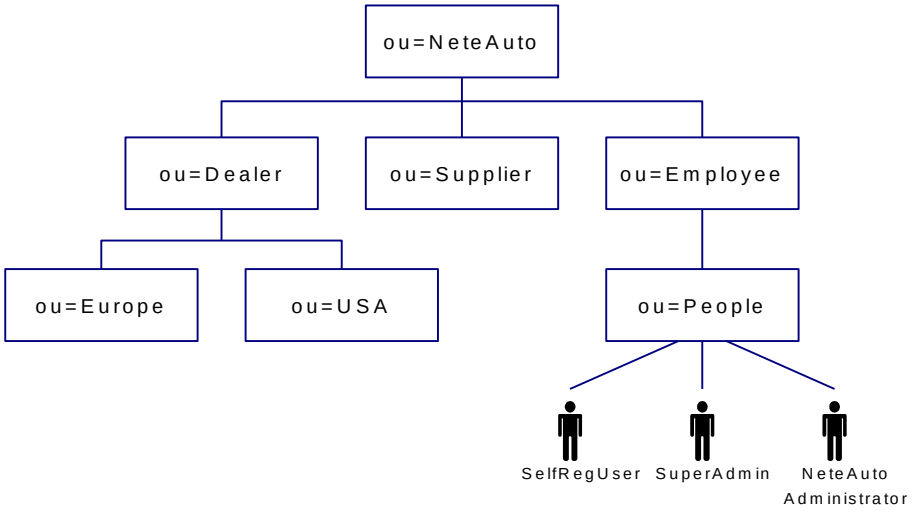
如何配置具有组织支持的 NeteAuto 示例

配置具有组织支持的 NeteAuto 示例需要执行下列步骤：

- 安装必备软件
- 安装示例 CA Identity Manager 环境
- 配置 LDAP 用户目录
- 配置关系数据库
- 创建 CA Identity Manager 目录
- 创建 NeteAuto CA Identity Manager 环境

NeteAuto 的 LDAP 目录结构

下图描述了 LDAP 目录的 NeteAuto 示例：



示例 CA Identity Manager 环境包括以下用户：

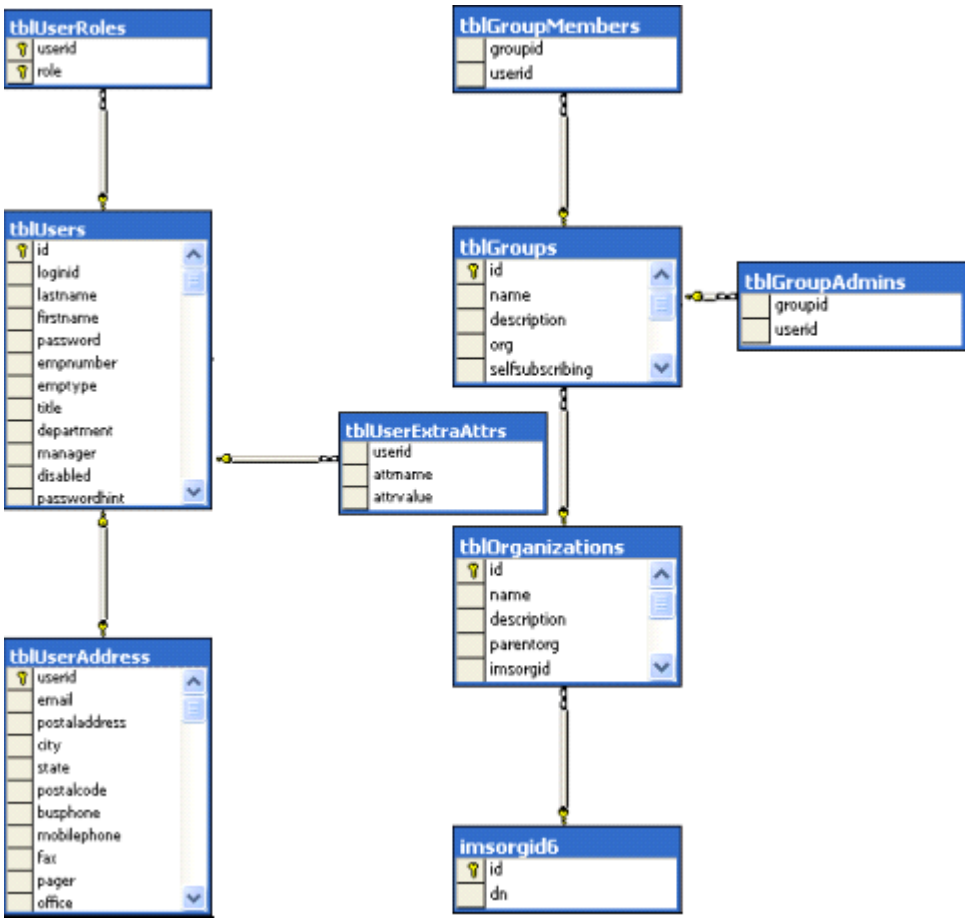
- 超级管理员是具有此 CA Identity Manager 环境的系统管理员角色的管理员帐户。 作为超级管理员，您可以执行所有默认的管理任务。

  注意：有关默认管理任务的说明，请参阅*《管理指南》*。

- SelfRegUser 是 CA Identity Manager 用于启用此 CA Identity Manager 环境的自行注册的管理员帐户。
- 在安装 NeteAuto 环境时，NeteAuto 管理员没有任何权限。 然而，您可以作为用户角色分配“组管理员”，正如“分配组管理员角色”中所描述的。

NeteAuto 的关系数据库

下图描述了 NeteAuto 示例（包括组织表）的关系数据库：



NeteAuto 的必备软件

NeteAuto CA Identity Manager 环境具有以下先决条件：

- 按照*《安装指南》*安装 CA Identity Manager。确保已安装 CA Identity Manager 管理工具。
- 必须可以访问 Sun Java 系统（Sun ONE 或 iPlanet）目录服务器或 Microsoft SQL Server 数据库。

NeteAuto 环境的安装文件

CA Identity Manager 包括一组可用于设置示例 CA Identity Manager 环境的文件。CA Identity Manager 环境是一个管理命名空间的视图，允许 CA Identity Manager 管理员管理用户、组和组织等对象。将这些对象与关联角色和任务集一起管理。CA Identity Manager 环境可控制目录的管理和图形展示。

示例 CA Identity Manager 环境包括：

- 示例对象，如用户和组织
- 角色、任务和屏幕定义

  单击选项卡（如用户或组）时，任务会在“用户控制台”中显示。 用户登录时，关联的任务会根据分配的角色显示。

  注意：有关角色和任务的更多信息，请参阅 *《管理指南》*。
- 自定义 NeteAuto 用户的“用户控制台”的示例面板。
- 用于创建 CA Identity Manager 目录的目录配置文件。

用于创建示例 CA Identity Manager 环境的文件安装在以下位置：

管理工具\samples\NeteAuto

在此路径中，*admin_tools* 指代“管理工具”。 管理工具安装在以下默认位置：

- **Windows：**<安装路径>\tools
- **UNIX：**<安装路径 2>/tools

安装 NeteAuto 环境

执行以下过程以安装 NeteAuto 环境。

遵循这些步骤:

1. 确保已安装必备软件 (p. 21)。
2. 配置用户存储并导入示例数据。
   - 对于 LDAP 用户：配置 LDAP 用户目录 (p. 23)
   - 对于关系数据库用户：配置关系数据库
3. 创建 NeteAuto CA Identity Manager 目录。
4. 创建 NeteAuto CA Identity Manager 环境。
5. 为 NeteAuto 用户配置 CA Identity Manager 用户界面的外观 (p. 36)。

配置 LDAP 用户目录

LDAP 目录的使用取决于安装情况。您可以使用以下步骤来检查目录是否存在或是否应该创建目录。

遵循这些步骤:

1. 在目录服务器控制台中，使用下列 root 创建 LDAP 实例：

   ```
   dc=security,dc=com
   ```

   写下端口号供以后引用。

2. 从管理工具中的 samples\NeteAuto 将 NeteAuto.ldif 文件导入到目录服务器中。

   管理工具安装于以下默认位置：

   - **Windows：** C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools
   - **UNIX：** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

注意： 如果在导入 LDIF 文件或创建 CA Identity Manager 目录时遇到问题，请将以下文本添加到 LDIF 文件的开头：

```
dn: dc=security, dc=com
objectClass: top
objectClass: domain
dc: security
```

保存文件并重复步骤 1 和 2。

配置关系数据库

执行以下步骤以配置关系数据库。

遵循这些步骤:

1. 创建名为 NeteAuto 的数据库实例。
2. 使用密码测试创建名为 neteautoadmin 的用户。 通过编辑用户的属性，向 NeteAuto 授予 neteautoadmin 权限（如公共权限和 db_owner 权限）。

   注意： 要创建 NeteAuto 数据库，neteautoadmin 角色必须至少对于使用 .sql 脚本创建的所有表具有最小（选择、插入、更新和删除）权限。 此外，neteautoadmin 还必须能够执行所有存储的步骤（如果在这些脚本中定义了存储步骤）。

3. 在编辑用户属性时，将 NeteAuto 作为 neteautoadmin 的默认数据库。

4. 以脚本列出的顺序运行以下脚本：

   - *db_type*-rdbuserdirectory.sql－为 NeteAuto 示例配置表，并创建用户条目。
   - ims_*db_type*_rdb.sql－为组织配置支持

     db_type

     根据正在配置的数据库类型，定义 Microsoft SQL 或 Oracle。

   这些脚本文件位于 *admin_tools*\samples\NeteAutoRDB\Organization 文件夹中。 在此示例中，*admin_tools* 指代管理工具，它安装在以下默认位置中：

   - **Windows：** C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools
   - **UNIX：** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

5. 定义名为 neteautoDS 的 JDBC 数据源，它指向 NeteAuto 数据库。

   配置数据源的步骤取决于安装 CA Identity Manager 的应用程序服务器的类型。"如何创建 JDBC 数据源" (p. 90)部分包含创建 JDBC 数据源的应用程序服务器特定说明。

创建 CA Identity Manager 目录

执行以下步骤以创建 CA Identity Manager 目录。

遵循这些步骤:

1. 通过在浏览器中输入以下 URL 打开管理控制台：

   http://*im_server:port*/iam/immanage

   im_server

   定义安装了 CA Identity Manager 的服务器的完全限定域名。

   端口

   定义应用程序服务器端口号。

2. 单击"Directories"（目录）。
3. 单击"Create from Wizard"（通过向导创建）以启动 CA Identity Manager 目录向导。
4. 浏览适当的目录配置 .xml 文件，然后单击"Next"（下一步）。

   目录配置文件位于以下文件夹中：

   - 对于 Sun Java 系统目录服务器用户目录：

     admin_tools\samples\NeteAuto\Organization\directory.xml

- 对于关系数据库：

  admin_tools\samples\NeteAutoRDB\Organization*db_type* directory.xml

  管理工具

  定义管理工具的安装位置。

  管理工具安装于以下默认位置：

  Windows： C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools

  UNIX： /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

  db_type

  指定正在配置的数据库的类型：Microsoft SQL 或 Oracle。

状态信息显示在“Directory Configuration Output”（目录配置输出）屏幕中。

5. 在向导的第二页上，提供以下值：

   - Sun Java 系统目录服务器

     “Name”（名称）

     “NeteAuto Directory”（NeteAuto 目录）

     “Description”（说明）

     “Sample NeteAuto directory”（示例 NeteAuto 目录）

     “Connection Object Name”（连接对象名称）

     “NeteAuto Users”（NeteAuto 用户）

     “Host”（主机）

     安装用户存储的计算机的名称或系统的 IP 地址。

     “Port”（端口）

     用户存储的端口号

     “Search root”（搜索根）

     dc=security, dc=com

     “Username”（用户名）

     可以访问用户存储的帐户的用户名。

     “Password and Confirm Password”（密码和确认密码）

     用户帐户的密码

   - Microsoft SQL Server 和 Oracle 数据库

     “Name”（名称）

     “NeteAutoRDB Directory”（NeteAutoRDB 目录）

     “Description”（说明）

     “Sample NeteAuto directory”（示例 NeteAuto 目录）

“Connection Object Name”（连接对象名称）

NeteAutoRDB

“JDBC Data Source”（JDBC 数据源）

neteautoDS

“Username”（用户名）

Neteautoadmin

“Password”（密码）

测试

6. 单击“Next”（下一步）。
7. 单击“Finish”（完成）退出向导。

创建 NeteAuto CA Identity Manager 环境

执行以下步骤以创建 NeteAuto CA Identity Manager 环境。

遵循这些步骤:

1. 在管理控制台中单击“Environments”（环境）。
2. 在“CA Identity Manager Environments”（CA Identity Manager 环境）屏幕中，单击“New”（新建）。

   此时显示“CA Identity Manager Environment”（CA Identity Manager 环境）向导。
3. 在向导的第一页中，输入以下值：

   “Environment name”（环境名称）

   NeteAuto 环境

   “Description”（说明）

   环境示例

“Alias”（别名）

Neteauto

将别名添加到 URL 以访问“CA Identity Manager Environment”（CA Identity Manager 环境）。 例如，访问 neteauto 环境的 URL 是：

http://*server_name*/iam/im/neteauto

server_name

定义安装了 CA Identity Manager 的服务器的完全限定域名，例如：

http://myserver.mycompany.org/iam/im/neteauto

注意：别名区分大小写。

单击“Next”（下一步）。

4. 选择 CA Identity Manager 目录来关联正在创建的“Environment”（环境）：
   - 对于 Sun Java 系统目录服务器，使用 NeteAuto 目录。
   - 对于 Microsoft SQL Server 或 Oracle 数据库，使用 NeteAutoRDB 目录。

   单击“Next”（下一步）。
5. 为公共任务配置支持，如自行注册和忘记密码任务，如下所示：
   a. 输入公共任务的以下别名：

      Neteautopublic

   b. 输入“SelfRegUser”作为匿名的用户帐户。
   c. 单击“Validate”（验证）查看用户唯一标识符。

   注意：用户不需要登录即可使用公共任务。
6. 选择为“NeteAuto Environment”（NeteAuto 环境）创建的任务和角色：
   a. 选择“Import roles from the file”（从文件导入角色）。
   b. 浏览到以下位置之一：
      - 对于 Sun Java 系统目录服务器用户存储：

        admin_tools\samples\NeteAuto\RoleDefinitions.xml
      - 对于 Microsoft SQL Server 用户存储：

        admin_tools\samples\NeteAutoRDB\Organization\mssqlRoleDefinitions.xml

- 对于 Oracle 用户存储：

  admin_tools\samples\NeteAutoRDB\Organization\oracleRoleDefinitions.xml

  admin_tools 指代管理工具，它们会默认安装在以下位置中：

  Windows： C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools

  UNIX： /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

7. 指定一个用户担任此环境的系统管理员，然后单击“Next”（下一步）：
   a. 在“System Manager”（系统管理员）字段中输入“SuperAdmin”。
   b. 单击“Add”（添加）。

      CA Identity Manager 会将 Superadmin 用户的唯一标识符添加到用户列表中。
   c. 单击“Next”（下一步）。
8. 查看环境的设置，并执行以下任务：
   - （可选）单击“Previous”（上一步）进行修改。
   - 单击“Finish”（完成）创建具有当前设置的 CA Identity Manager 环境。

     “Environment Configuration Output”（环境配置输出）屏幕显示了环境创建的进度。
9. 单击“Continue”（继续）以退出 CA Identity Manager 环境向导。
10. 启动 CA Identity Manager 环境。

创建 NeteAuto 环境后，您可以：

- 为此 CA Identity Manager 环境创建面板。 (p. 36)
- 访问环境 (p. 34)

如何配置没有组织支持的 NeteAuto 示例

配置没有组织支持的 NeteAuto 示例需要执行下列步骤：

- 安装必备软件 (p. 21)
- 安装示例 CA Identity Manager 环境
- 配置数据库
- 创建 JDBC 数据源
- 创建 CA Identity Manager 目录
- 创建 NeteAuto CA Identity Manager 环境

示例 CA Identity Manager 环境描述

对于 Microsoft SQL Server 和 Oracle 数据库，CA Identity Manager 包括不包括组织的 NeteAuto 环境的版本。 此 CA Identity Manager 环境包括以下三名用户：

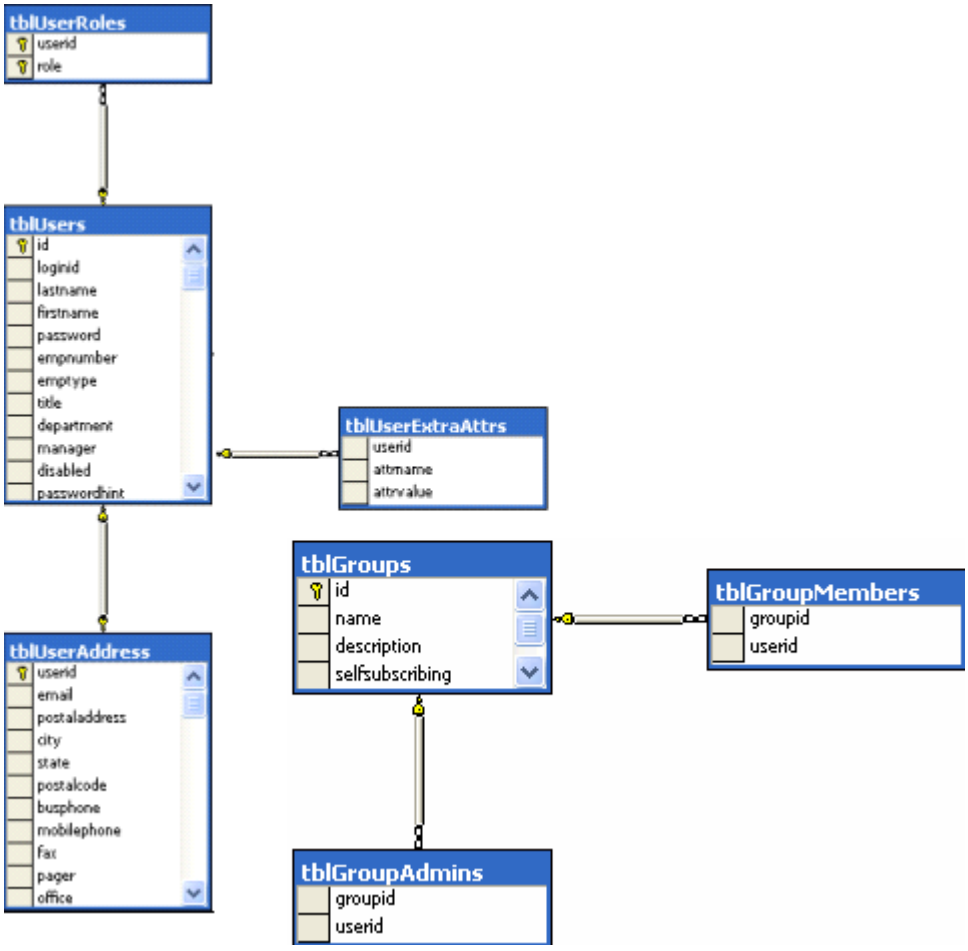
- 超级管理员是具有此 CA Identity Manager 环境的系统管理员角色的管理员帐户。 作为超级管理员，您可以执行所有默认的管理任务。

  注意：有关默认管理任务的说明，请参阅*《管理指南》*。

- SelfRegUser 是 CA Identity Manager 用于启用此 CA Identity Manager 环境的自行注册的管理员帐户。
- 在安装 NeteAuto 环境时，NeteAuto 管理员没有任何权限。

  然而，您可以将组管理员角色分配给 NeteAuto 管理员帐户。

下图描述了无组织的关系数据库的 NeteAuto 示例：



Neteauto 环境的安装文件

CA Identity Manager 包括一组可用于设置示例 CA Identity Manager 环境的文件。 CA Identity Manager 环境是管理命名空间的视图，允许 CA Identity Manager 管理员管理对象。 这些对象与关联角色和任务集在一起。 CA Identity Manager 环境可控制用户存储的管理和图形展示。

示例 CA Identity Manager 环境包括：

- 示例用户
- 角色、任务和屏幕定义

  单击类别（如用户或组）时，任务会在“用户控制台”中显示。 显示的任务取决于分配给用户的角色。

  注意：有关角色和任务的更多信息，请参阅*《管理指南》*。
- 自定义 NeteAuto 用户的“用户控制台”的示例面板。
- 用于创建 CA Identity Manager 目录的目录配置文件。

用于创建示例 CA Identity Manager 环境的文件安装在以下位置：

admin_tools\samples\NeteAutoRDB\NoOrganization

在此路径中，*admin_tools* 指代“管理工具”。

管理工具安装在以下默认位置：

- **Windows：**<安装路径>\tools
- **UNIX：**<安装路径 2>/tools

如何安装 NeteAuto 环境－无组织支持

执行以下过程以安装 NeteAuto 环境。

遵循这些步骤:

1. 确认已安装必备软件 (p. 31)。
2. 配置数据库 (p. 23)。
3. 创建 CA Identity Manager 目录。 (p. 32)
4. 创建 NeteAuto CA Identity Manager 环境 (p. 33)。
5. 为 NeteAuto 用户配置 CA Identity Manager 用户界面 (p. 36)的外观。

必备软件

NeteAuto CA Identity Manager 环境具有以下先决条件：

- 按照*《安装指南》*安装 CA Identity Manager。确认已安装 CA Identity Manager 管理工具。
- 必须具有访问 Microsoft SQL Server 或 Oracle 数据库的权限。

配置关系数据库

执行以下步骤以配置关系数据库。

遵循这些步骤:

1. 创建名为 NeteAuto 的数据库实例。
2. 使用密码测试创建名为 neteautoadmin 的用户。 通过编辑用户的属性，向 NeteAuto 授予 neteautoadmin 权限（如公共权限和 db_owner 权限）。

   注意：要创建 NeteAuto 数据库，neteautoadmin 角色必须至少对于使用 .sql 脚本创建的所有表具有最小（选择、插入、更新和删除）权限。 此外，neteautoadmin 还必须能够执行所有存储的步骤（如果在这些脚本中定义了存储步骤）。
3. 在编辑用户属性时，将 NeteAuto 作为 neteautoadmin 的默认数据库。
4. 以脚本列出的顺序运行以下脚本：
   - *db_type*-rdbuserdirectory.sql－为 NeteAuto 示例配置表，并创建用户条目。
   - ims_*db_type*_rdb.sql－为组织配置支持

     db_type

     根据正在配置的数据库类型，定义 Microsoft SQL 或 Oracle。

   这些脚本文件位于 *admin_tools*\samples\NeteAutoRDB\Organization 文件夹中。 在此示例中，*admin_tools* 指代管理工具，它安装在以下默认位置中：
   - **Windows：**C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools
   - **UNIX：**/opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools
5. 定义名为 neteautoDS 的 JDBC 数据源，它指向 NeteAuto 数据库。

   配置数据源的步骤取决于安装 CA Identity Manager 的应用程序服务器的类型。"如何创建 JDBC 数据源" (p. 90)部分包含创建 JDBC 数据源的应用程序服务器特定说明。

创建 CA Identity Manager 目录

执行以下步骤以创建 CA Identity Manager 目录。

遵循这些步骤:

1. 通过在浏览器中输入以下 URL 打开管理控制台：

   http://*im_server*:*port*/iam/immanage

   im_server

   定义安装了 CA Identity Manager 的服务器的完全限定域名。

   端口

   定义应用程序服务器端口号。

2. 单击“Directories”（目录）。

   此时显示 CA Identity Manager 目录屏幕。

3. 单击“New”（新建）启动 CA Identity Manager 目录向导。

4. 浏览下列目录配置 XML 文件之一，然后单击“Next”（下一步）：

   - Sun Java 系统：

     admin_tools\samples\NeteAuto\NoOrganization\directory.xml

   - SQL Server 数据库：

     admin_tools\samples\NeteAuto\NoOrganization\mssql-directory.xml

   - Oracle 数据库：

     admin_tools\samples\NeteAuto\NoOrganization\oracle-directory.xml

   admin_tools 指代管理工具，它们会默认安装在以下位置中：

   - **Windows：**C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools
   - **UNIX：**/opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

   状态信息显示在“Directory Configuration Output”（目录配置输出）屏幕中。

5. 在向导的第二页中，提供以下值：

   “Name”（名称）

   NeteAutoRDB Directory

   “Description”（说明）

   无组织支持的示例 NeteAuto 目录

   “Connection Object Name”（连接对象名称）

   NeteAutoRDB

“JDBC Data Source”（JDBC 数据源）

neteautoDS

“Username”（用户名）

neteautoadmin

“Password”（密码）

测试

6. 单击“Next”（下一步）。
7. 单击“Finish”（完成）退出向导。

创建 NeteAuto CA Identity Manager 环境

执行以下步骤以创建 NeteAuto CA Identity Manager 环境。

遵循这些步骤:

1. 在管理控制台中单击“Environments”（环境）。
2. 在“CA Identity Manager environments”（CA Identity Manager 环境）屏幕中，单击“New”（新建）。

   此时将打开“CA Identity Manager environment”（CA Identity Manager 环境）向导。
3. 在向导的第一页中，输入以下值：
   - “Environment name”（环境名称）—NeteAuto 环境
   - “Description”（说明）—NeteAuto 是环境示例。
   - “Alias”（别名）—neteautoRDB

     将别名添加到 URL 以访问“CA Identity Manager environment”（CA Identity Manager 环境）。 例如，访问 neteauto 环境的 URL 是：

     `http://domain/iam/im/neteautoRDB`

     在此路径中，*域*定义了安装 CA Identity Manager 的服务器的完全限定域名，如下例所示：

     `http://myserver.mycompany.org/iam/im/neteautoRDB`

     注意：别名区分大小写。

   单击“Next”（下一步）。
4. 选择 NeteAutoRDB 目录 CA Identity Manager 目录以关联正在创建的环境，然后单击“Next”（下一步）。

5. 为公共任务配置支持，如自行注册和忘记密码任务。

   注意：用户不需要登录即可访问公共任务。

   a. 输入公共任务的以下别名：

      neteautoRDBpublic

   b. 输入 SelfRegUser 作为匿名用户帐户。

   c. 单击“Validate”（验证）查看用户唯一标识符（在这种情况下为 2）。

6. 选择为“NeteAuto environment”（NeteAuto 环境）创建的任务和角色：

   - 选择“Import roles from the file”（从文件导入角色）。
   - 浏览至以下位置：

     im_admin_tools_dir\samples\NeteAutoRDB\NoOrganizations\RoleDefinitions.xml

     在此路径中，*im_admin_tools_dir* 定义了 CA Identity Manager 管理工具的安装位置。

7. 指定一个用户担任此环境的系统管理员，然后单击“Next”（下一步）：

   a. 在“System Manager”（系统管理员）字段中输入“SuperAdmin”（超级管理员）。

   b. 单击“Add”（添加）。

   c. 单击“Next”（下一步）。

8. 查看环境设置。

   - 单击“Previous”（上一步）进行修改。
   - 单击“Finish”（完成）创建具有当前设置的 CA Identity Manager 环境。

     “Environment Configuration Output”（环境配置输出）屏幕显示了环境创建的进度。

9. 单击“Finish”（完成）退出 CA Identity Manager 环境向导。
10. 启动 CA Identity Manager 环境。

创建 NeteAuto 环境后，您可以：

- 按“设置 NeteAuto 面板” (p. 36)中所述为此 CA Identity Manager 环境创建面板。
- 按“如何使用 NeteAuto CA Identity Manager 环境”中所述访问该环境

如何使用 NeteAuto CA Identity Manager 环境

您可以使用 NeteAuto CA Identity Manager 环境管理自助服务任务和用户。

自助服务任务管理

自助服务任务包括：

- 作为新用户注册
- 作为自行注册用户登录
- 使用忘记密码功能

作为新用户注册

执行以下步骤注册为新用户。

遵循这些步骤:

1. 在浏览器中输入以下 URL：

   http://*hostname*/iam/im/neteautopublic/index.jsp?task.tag=SelfRegistration

   hostname

   定义运行 CA Identity Manager 的系统的完全限定域名。

   注意：如果您未配置 Neteauto 面板 (p. 36)，您可以从 URL 中省去 imcss，如下所示：

   http://*hostname*/iam/im/neteautopublic/index.jsp?task.tag=SelfRegistration

   此 URL 链接到默认 CA 控制台。

   在“自行注册：最终用户许可协议”页面中，CA Identity Manager 显示了 CA 网站。

   注意：您可以配置默认自行注册任务以显示自定义最终用户许可协议。 有关说明，请参阅 *《管理指南》*。

2. 单击“接受”继续。
3. 在“配置文件”选项卡中，提供以下详细信息：
   a. 输入必需字段的值，使用星号 (*) 表示。
   b. 输入密码提示问题和答案。

      在忘记密码时，CA Identity Manager 会提供密码提示问题并要求您回答。 如果回答正确， CA Identity Manager 会提示用户指定和确认新密码。
4. 将“组”选项卡保留不变。
5. 单击“提交”。

作为自行注册用户登录

执行以下步骤作为自行注册用户登录。

遵循这些步骤:

1. 在浏览器中输入 NeteAuto CA Identity Manager 环境的以下 URL：

   `http://hostname/iam/im/neteauto/imcss/index.jsp`

   hostname

   定义运行 CA Identity Manager 的系统的完全限定域名。

2. 使用注册时指定的用户名和密码登录。

设置 NeteAuto 面板

要设置 NeteAuto 面板，请在 SiteMinder 策略服务器中创建 SiteMinder 响应。

遵循这些步骤:

1. 作为具有域权限的管理员登录到下列界面之一：
   - 对于 CA SiteMinder Web 访问管理器 r12 或更高版本，登录到管理 UI。
   - 对于 CA eTrust SiteMinder 6.0 SP5，登录到策略服务器用户界面。

   注意：有关使用这些界面的信息，请参阅正在使用的 SiteMinder 的版本的文档。

2. 打开 neteautoDomain。
3. 在 neteautoDomain 下，选择“领域”。

   显示下列领域：

   neteauto_ims_realm

   保护 CA Identity Manager 环境。

   neteauto_pub_realm

   启用对公共任务的支持，如自行注册和忘记密码任务。

4. 在每个领域中创建规则。 指定以下详细信息：
   - 资源：*
   - 操作：GET、POST

   要简化管理，请在规则名称中包括 NeteAuto 面板。

5. 为具有以下响应属性的域创建响应：
   - 属性：WebAgent-HTTP-Header-Variable

     此属性可向响应添加新的 HTTP 标头。
   - 属性种类：静态
   - 变量名：面板

     变量值：neteauto
6. 修改 CA Identity Manager 在 neteautoDomain 中创建的策略。 指定以下详细信息：
   - 用户
     - 对于 LDAP：在可用成员中选择“ou=People, ou=Employees, ou=NeteAuto”，并将其添加到“当前成员”中。 单击“确定”。
     - 对于关系数据库：搜索 ID 属性等于 * 的用户。在“可用成员”中选择所有用户并将它们添加到“当前成员”中。 单击“确定”。
   - 规则：
     - 添加在步骤 4 中创建的规则。
     - 对于每个规则，单击“设置响应”。 将每个规则与在步骤 5 中创建的响应关联在一起。

注意：neteauto 面板取决于 imcss 控制台。要查看面板，请将 /imcss/index.jsp 附加到 NeteAuto CA Identity Manager 环境的 URL，如下所示：

http://*hostname*/iam/im/neteauto/imcss/index.jsp

“访问 NeteAuto CA Identity Manager 环境” (p. 38)提供了访问 Neteauto 环境的完整说明。

使用忘记密码功能

执行以下步骤使用忘记密码功能。

遵循这些步骤:

1. 在浏览器中输入以下 URL：

   ```
   http://hostname/iam/im/neteautopublic/index.jsp?task.tag=ForgottenPasswordReset
   ```

   hostname

   定义运行 CA Identity Manager 的系统的完全限定域名。

2. 为您在“作为新用户注册” (p. 35)中创建的自行注册用户输入唯一标识符，然后单击“下一步”。
3. 在每次跳出提示时，回答验证问题。 答案是您在注册期间提供的答案。

   注意：每个问题都需要正确回答。 取消任务或关闭浏览器都将被视作失败的尝试。
4. 单击“提交”。

   CA Identity Manager 提示您提供新密码。

用户管理

用户管理包括以下操作：

- 访问 NeteAuto CA Identity Manager 环境
- 修改用户
- 分配“组管理员”角色
- 创建组
- 管理自行注册用户

访问 NeteAuto CA Identity Manager 环境

执行以下步骤访问 NeteAuto CA Identity Manager 环境。

遵循这些步骤:

1. 在浏览器中输入以下 URL：

   `http://hostname/iam/im/neteauto/imcss/index.jsp`

   hostname

   定义完全限定域名，如下例所示：

   http://myserver.mycompany.com/iam/im/neteauto/imcss/index.jsp .

   注意：如果未配置 Neteauto 面板，您可以使用以下 URL 访问 Neteauto 环境：

   http://*hostname*/iam/im/neteauto
2. 在登录屏幕中，输入以下凭据：

   用户名

   超级管理员

   密码

   测试

修改用户

执行以下步骤修改用户。

遵循这些步骤:

1. 作为使用密码测试的超级管理员登录 NeteAuto 环境。
2. 依次选择“用户”、“管理用户”、“修改用户”。

   将显示“选择用户”屏幕。
3. 单击“搜索”。

   CA Identity Manager 会显示 NeteAuto 环境中的用户列表。
4. 选择 NeteAuto 管理员，如下所示：
   - 对于 LDAP 目录，是 NeteAuto 管理员
   - 对于关系数据库，是 NeteAuto 管理员

   单击“选择”。 CA Identity Manager 会显示 NeteAuto 管理员的配置文件。
5. 在“标题”字段中，输入管理员。 单击“提交”。

   CA Identity Manager 会确认任务提交。
6. 单击“确定”返回主屏幕。

分配组管理员角色

分配组管理员角色是必要的。 执行以下步骤分配组管理员。

遵循这些步骤:

1. 作为超级管理员，选择“角色”和“任务”选项卡，然后选择“管理角色”、“修改管理角色”。
2. 选择“组管理员”角色，然后单击“选择”。

   此时显示“组管理员”角色的配置文件。
3. 单击“成员”选项卡，然后单击“成员策略”下的“添加”。

   此时显示“成员策略”屏幕。
4. 在“成员规则”下，单击“用户”字段的向下箭头。

   从下拉列表中，选择 <user-filter> 所在位置。

   更改“用户”字段，允许您为规则输入筛选。
5. 输入成员资格规则，如下所示：
   a. 在第一个字段中，从下拉列表中选择“标题”。
   b. 在第二个字段中，确保已选择等号 (=)。
   c. 在第三个字段中，输入管理员。

6. 在“作用域规则”部分中，为用户、组和组织（在支持时）定义规则，如下所示：
   a. 在“用户”字段中，单击向下箭头查看选项列表。从列表中选择（所有）：
   b. 在“组和组织”字段（在支持时）中重复执行步骤“a”。
   c. 将“访问任务”字段保留为空。
7. 单击“确定”。

   CA Identity Manager 会显示您创建的成员策略。
8. 单击“提交”。

   CA Identity Manager 会确认任务提交。
9. 单击“确定”返回主屏幕。
10. 关闭 CA Identity Manager。

创建组

执行以下步骤以创建组。

遵循这些步骤:

1. 作为 NeteAuto 管理员登录到 CA Identity Manager，如下所示：
   - 对于 LDAP 目录，输入 NeteAuto 管理员的用户名和密码测试。
   - 对于关系数据库，输入 NeteAuto 管理员的用户名和密码测试。

   此时显示 NeteAuto 管理员可以执行的任务列表。NeteAuto 管理员仅可执行有限的任务，因此 CA Identity Manager 会列出任务，而不是类别。
2. 单击“创建组”。
3. 确认选择了“创建新组”，并单击“确定”。
4. 实施适合您的情况的下列步骤之一：
   - 如果 NeteAuto 环境支持组织：
     a. 在“组织名称”字段中，单击省略符号 (...) 以选择 CA Identity Manager 创建该组的组织。
     b. 在“选择组织”屏幕的底部，展开 NeteAuto。
     c. 选择“经销商”组织。
   - 如果 NeteAuto 环境不支持组织，请转到下一步。
5. 输入该组的以下信息：
   - 组名称：经销商管理员
   - 组说明：NeteAuto 经销商的管理员。
6. 单击“成员资格”选项卡，然后单击“添加一个用户”。

   将显示“选择用户”屏幕。

7. 单击“搜索”。
8. 选择 NeteAuto 管理员，然后单击“选择”。
9. 单击“提交”以创建组。

管理自行注册用户

在您想要管理自行注册用户时，执行以下步骤。

遵循这些步骤:

1. 使用以下凭据作为 NeteAuto 管理员登录到 CA Identity Manager：
   - 对于 LDAP 目录：

     用户名

     NeteAuto 管理员

     密码

     测试
   - 对于关系数据库：

     用户名

     NeteAuto 管理

     密码

     测试

   NeteAuto 管理员可以执行的任务列表会显示在“用户控制台”的左侧。NeteAuto 管理员仅可执行有限的任务，因此 CA Identity Manager 会列出任务，而不是类别。
2. 单击“修改组”。
3. 单击“搜索”。

   CA Identity Manager 会显示组列表。
4. 选择“经销商管理员”，然后单击“选择”。
5. 单击“成员资格”选项卡，然后单击“添加一个用户”。

   将显示“选择用户”屏幕。
6. 单击“搜索”。
7. 在“用户搜索”屏幕中，选择您在“作为新用户注册” (p. 35)中输入的用户。 单击“选择”。
8. 单击“提交”。

   CA Identity Manager 会确认任务提交。
9. 单击“确定”返回主屏幕。

要确认用户是创建的组的成员，请使用“查看组”任务。

如何配置其他功能

在安装 NeteAuto 示例和练习基本 CA Identity Manager 功能后，可以使用 NeteAuto 环境来练习和测试包括电子邮件通知和工作流在内的其他 CA Identity Manager 功能。

注意：有关这些功能的更多信息，请参阅*《管理指南》*。

全局用户名的 SiteMinder 登录名限制

如果某个全局用户需要登录 SiteMinder 策略服务器，则该用户名不能包含下列字符或字符串：

&
*
:
()

变通方法

避免在全局用户名中使用这些字符。

第 3 章： LDAP 用户存储管理

此部分包含以下主题：

CA Identity Manager 目录

*CA Identity Manager 目录*描述了用户、组和组织等对象在用户目录中的存储方式及其在 CA Identity Manager 中的表示方式。CA Identity Manager 目录与一个或多个 CA Identity Manager 环境相关联。

如何创建 CA Identity Manager 目录

为 LDAP 用户存储创建 CA Identity Manager 目录需要执行下列步骤：

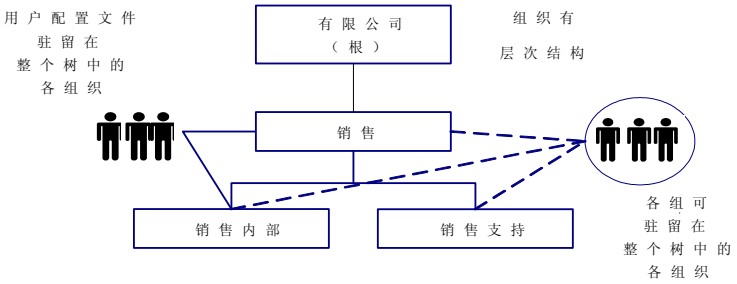
1. 确定目录结构。
2. 通过修改目录配置文件 (directory.xml) (p. 47)，在用户存储中描述对象。
3. 导入目录配置文件并创建目录 (p. 131)。

注意：在使用 SiteMinder 时，请确认在创建 CA Identity Manager 目录前就已应用了策略存储架构。 有关特定策略存储架构的更多信息以及如何应用它们，请参阅*《安装指南》*。

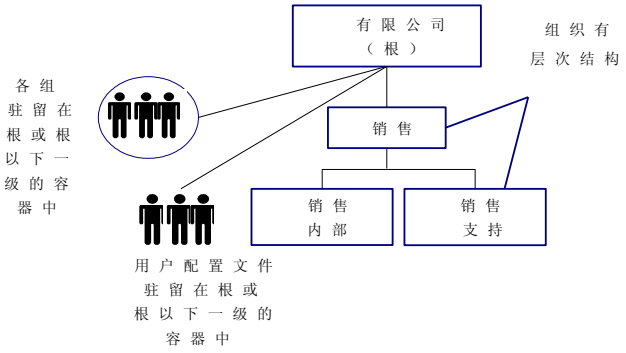
目录结构

CA Identity Manager 支持以下目录结构：

- 层级－包含父组织（根）和子组织。 子组织也可以具有子组织，这样就创建了多级结构，如下图所示：

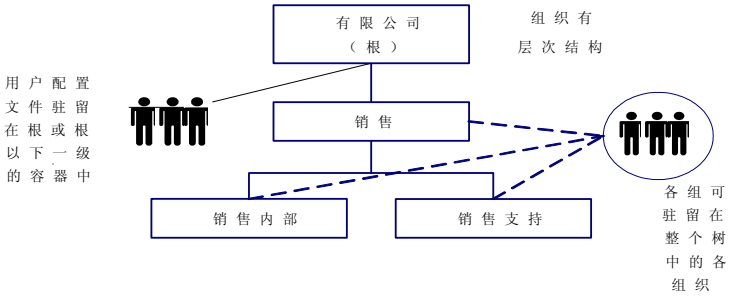


- 平面－用户和组储存在搜索根中或在搜索根下面一级的容器中。 具有层级结构的组织，如以下平面目录结构图所示：



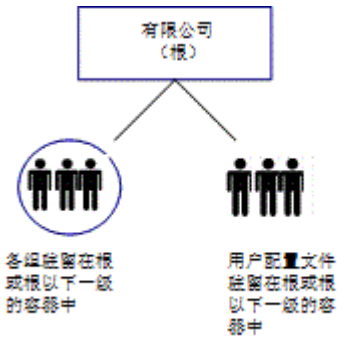
为了在平面目录结构中便于用户管理和指派，用户和组都属于逻辑组织。逻辑组织作为属性存储在用户和组配置文件中。

- 平面用户－分级存储组织和组，但是将用户储存在搜索根中或在搜索根下面一级的容器中。 下图显示了平面用户目录结构的插图：



在平面用户目录结构中，用户属于逻辑组织。 用户的逻辑组织作为属性存储在用户配置文件中。

- 无组织－该目录不包括组织。 用户和组储存在搜索根中或在搜索根下面一级的容器中。 下图显示了无组织目录结构：



注意：一个目录可以包含多个类型的结构。 例如，用户配置文件可以存储在目录的一部分的平面结构中以及在目录的另一部分分级存储。 要支持混合的目录结构，请创建多个 CA Identity Manager 环境。

目录配置文件

要描述与 CA Identity Manager 关联的用户目录的结构，请创建目录配置文件。

目录配置文件包含以下部分中的一个或多个：

CA Identity Manager 目录信息

包含关于 CA Identity Manager 目录方面的信息。

注意：不要在此部分中修改信息。 在管理控制台中创建 CA Identity Manager 目录时，CA Identity Manager 会提示您提供此信息。

属性验证

定义适用于 CA Identity Manager 目录的验证规则。

提供商信息

描述 CA Identity Manager 管理的用户存储。

目录搜索信息

支持您指定 CA Identity Manager 搜索用户存储的方式。

用户对象

描述用户如何存储在用户存储中及其在 CA Identity Manager 中的表示方式。

组对象

描述组如何存储在用户存储中及其在 CA Identity Manager 中的表示方式。

组织对象

描述如何存储组织及其在 CA Identity Manager 中的表示方式。仅在用户存储包括组织时，组织对象才会提供详细信息。

自行订阅对象

为自助服务用户可加入的组配置支持。

目录组行为

指定 CA Identity Manager 目录是否支持动态组和嵌套组。

要创建目录配置文件，请修改配置模板。

如何选择目录配置模板

CA Identity Manager 可提供支持不同目录类型和结构的目录配置模板。 要创建 CA Identity Manager 目录，请修改与您的目录结构最匹配的模板。

下表中描述的模板已随同“管理工具”安装：

admin_tools\directoryTemplates*directory_type*\

管理工具安装在以下默认位置：

- **Windows：**<安装路径>\tools
- **UNIX：**<安装路径 2>/tools

目录的类型和相应的配置模板会显示在下表中：

目录类型	模板
具有层级结构的 Active Directory (ADSI) LDAP 目录	ActiveDirectory\directory.xml
具有层级结构的 Microsoft ADAM 目录	ADAM\directory.xml
具有层级结构的 IBM 目录服务器目录	IBMDirectoryServer\directory.xml
具有层级结构的 Novell eDirectory 用户目录	eDirectory\directory.xml
具有层级结构的 Oracle Internet 目录	OracleInternetDirectory\directory.xml
具有层级结构的 Sun Java 系统（SunOne 或 iPlanet）LDAP 目录	IPlanetHierarchical\directory.xml

目录类型	模板
具有平面结构的 Sun Java 系统（SunOne 或 iPlanet）LDAP 目录	IPlanetFlat\directory.xml
不包含组织的 Sun Java 系统（SunOne 或 iPlanet）LDAP 目录。	IPlanetNoOrganizations\directory.xml
具有层级结构的 CA Directory 用户存储	eTrustDirectory\directory.xml
配给目录 此模板可用于配置 CA Identity Manager 环境的配给目录。 **注意：**安装后即可使用此配置模板。无需修改此模板。	ProvisioningServer\directory.xml
自定义目录	使用与您的目录最相似的模板。

将配置模板复制到新目录，或使用不同名称将其保存，以防覆盖配置模板。

如何描述与 CA Identity Manager 关联的用户目录

为管理目录，CA Identity Manager 必须了解目录的结构和内容。 要描述与 CA Identity Manager 关联的目录，请在相应的模板目录中修改目录配置文件 (directory.xml)。

目录配置文件具有以下重要约定：

- ##－表示必需值。

  要提供所有必需信息，请找到所有双井号 (##)，并将其替换为相应的值。例如，##DISABLED_STATE 表示必须提供属性以存储用户的帐户状态。

- @－表示 CA Identity Manager 填充的值。 请勿修改目录配置文件中的这些值。 导入目录配置文件时，CA Identity Manager 会提示您提供相应的值。

在修改目录配置文件之前，需要以下信息：

- 用户、组和组织对象的 LDAP 对象类
- 用户、组和组织配置文件的属性列表

如何修改目录配置文件

执行以下步骤修改目录配置文件。

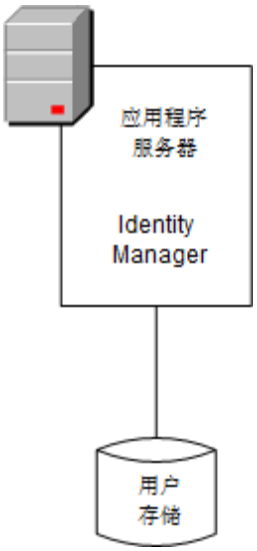
注意：其中相应地注明了必需的步骤。

1. 限制搜索结果 (p. 52)的大小。
2. 修改默认用户、组织或组管理对象。
3. 更改默认属性说明。
4. 修改常用属性 (p. 69)。 （必需）

   在 CA Identity Manager 中，常用属性可标识特殊属性，如密码属性。
5. 为目录结构配置 CA Identity Manager (p. 75)（必需）。
6. 支持用户订阅组 (p. 76)。

连接用户目录

CA Identity Manager 连接到用户目录，以便存储信息（例如，用户、组和组织信息），如下图所示：



无需新的目录或数据库。 然而，现有目录或数据库必须位于具有完全限定域名 (FQDN) 的系统上。

有关支持的目录和数据库类型的列表，请参阅 CA 支持站点上的 CA Identity Manager 支持表。

在管理控制台中创建 CA Identity Manager 目录时，需配置与用户存储的连接。

如果在创建 CA Identity Manager 目录之后导出目录配置，目录配置文件的 Provider 元素中将显示用户目录连接信息。

Provider 元素

配置信息存储在 directory.xml 文件的 Provider 元素及其子元素中。

注意：如果正在创建 CA Identity Manager 目录，则无需在 directory.xml 文件中提供目录连接信息。 而需在管理控制台的 CA Identity Manager 目录向导中提供连接信息。 仅在需要更新时修改 Provider 元素。

Provider 元素包含以下子元素：

LDAP

说明所连接的用户目录。

凭据

提供访问 LDAP 用户存储的用户名和密码。

连接

提供用户存储所在计算机的主机名和端口。

配给域

定义 CA Identity Manager 管理的配给域（仅适用于配给用户）。

已完成的 Provider 元素类似于以下代码：

```
<Provider type="LDAP" userdirectory="@SMDirName">
   <LDAP searchroot="@SMDirSearchRoot" secure="@SMDirSecure" />
   <Credentials user="@SMDirUser"
     cleartext="true">@SMDirPassword</Credentials>
   <Connection host="@SMDirHost" port="@SMDirPort" />
   <eTrustAdmin domain="@SMDirETrustAdminDomain" />
</Provider>
```

Provider 元素包含以下参数：

type

指定数据库的类型。对于所有 LDAP 用户存储，需指定 LDAP（默认）。

userdirectory

指定用户目录连接的名称。

注意：请勿在 directory.xml 文件中指定用户目录连接的名称。 在管理控制台中创建 CA Identity Manager 目录时，CA Identity Manager 会提示您提供名称。

注意：这些参数是可选的。

LDAP 子元素

LDAP 子元素包含以下参数：

searchroot

指定 LDAP 目录中用作目录起点的位置，通常为组织 (o) 或组织单元 (ou)。

安全

强制与 LDAP 用户目录建立安全套接字层 (SSL) 连接，如下所示：

- True－CA Identity Manager 使用安全连接。
- False－CA Identity Manager 在没有 SSL 的情况下连接到用户目录（默认）。

注意：这些参数是可选的。

Credentials 子元素

要连接到 LDAP 目录，CA Identity Manager 必须提供有效凭据。 Credentials 子元素中定义了这些凭据，此 Credentials 子元素类似于以下代码：

```
<Credentials user="@SMDirUser" cleartext="true">
  "MyPassword"
</Credentials>
```

如果未在 Credentials 子元素中指定密码，在管理控制台中创建 CA Identity Manager 目录时，系统将提示您输入密码。

注意：建议在管理控制台中指定密码。

如果在管理控制台中指定密码，CA Identity Manager 将对此密码加密。或者，如果不希望密码以明文显示，请使用与 CA Identity Manager 一起安装的密码工具加密密码。

注意：可以仅指定一组凭据。 如果定义多个目录，如“Connection 子元素”中所述，所指定的凭据必须适用于所有目录。

Credentials 子元素包含以下参数：

user

为可以访问此目录的帐户指定登录 ID。

对于配给用户，所指定的用户帐户必须在配给服务器中具有域管理员配置文件或一组等效的权限。

注意：请勿在 directory.xml 文件中指定用户参数的值。 当您在管理控制台中创建 CA Identity Manager 目录时，CA Identity Manager 提示您提供登录 ID。

cleartext

确定密码在 directory.xml 文件中是否以明文显示，如下所示：

- True－密码以明文显示。
- False－密码已加密（默认）。

注意：这些参数是可选的。

Connection 子元素

Connection 子元素描述 CA Identity Manager 管理的用户存储的位置。 此子元素包含以下参数：

host

指定用户目录所在系统的主机名或 IP 地址。

注意：如果连接的系统具有 IPv6 地址，请将 IP 地址用方括号 ([ ]) 括起来，如下所示：

<Connection host="[2::9255:214:22ff:fe72:525a]" port="20389"

failover="[2::9255:214:22ff:fe72:525a]:20389"/>

端口

指定用户目录的端口号。

故障转移

指定冗余用户存储所在系统的主机名和 IP 地址（假使主系统不可用）。 主系统再次可用时，可继续使用故障转移系统。 要返回使用主系统，请重新启动辅助系统。 如果列出多个服务器，CA Identity Manager 将尝试按列出顺序连接到系统。

在*以空格分隔的*列表中，指定故障转移属性的主机名和 IP 地址，如下所示：

failover="IPaddress:port IPaddress:port"

例如：

<Connection host="123.456.789.001" port="20389"

failover="123.456.789.002:20389 123.456.789.003:20389"/>

注意：端口 20389 是配给服务器的默认端口。

注意：这些参数是可选的。

Provisioning 子元素

如果 CA Identity Manager 环境中包含配给，请按如下方式定义配给域：

```
<eTrustadmin domain="@SMDirProvisioningDomain" />
```

Provisioning 子元素包含以下参数：

domain

包含 CA Identity Manager 所管理的配给域的名称。

在管理控制台中创建 CA Identity Manager 目录时，系统将提示您输入域名。 因此，请确认已在目录配置文件 (directory.xml) 中指定域参数的值。

目录搜索参数

可以在 DirectorySearch 元素中设置以下搜索参数：

maxrows

指定搜索用户目录时 CA Identity Manager 可以返回的最大对象数目。 对象数目超出限制时，将显示错误。

通过设置 maxrows 参数的值，可以覆盖 LDAP 目录中限制搜索结果的设置。 在应用冲突的设置时，LDAP 服务器使用最低的设置。

注意：maxrows 参数不限制 CA Identity Manager 任务屏幕上显示的对象数目。 要配置显示设置，请在 CA Identity Manager 用户控制台中修改列表屏幕定义。 有关说明，请参阅 *《User Console Design Guide》*。

maxpagesize

指定在一次搜索中可以返回的对象数目。 如果对象的数目超过页面大小，CA Identity Manager 将执行多个搜索。

指定 maxpagesize 时，需注意以下几点：

- 要使用 maxpagesize 选项，CA Identity Manager 管理的用户存储必须支持分页。 一些用户存储类型需要其他配置才可支持分页。 有关详细信息，请参阅"如何提高大型搜索性能" (p. 83)。
- 如果用户存储不支持分页，并且还指定了 maxrows 的值，则 CA Identity Manager 仅可使用 maxrows 值来控制搜索大小。

timeout

确定 CA Identity Manager 在终止搜索之前搜索目录的最大秒数。

注意：DirectorySearch 元素是可选的。 然而，由于此目录支持分页 (p. 83)，建议指定 DirectorySearch 元素。

更多信息：

如何改善目录搜索性能 (p. 82)
如何改善大规模搜索的性能 (p. 83)

用户、组和组织管理对象说明

在 CA Identity Manager 中，可管理与用户目录中的条目相对应的以下对象类型：

用户

表示企业中的用户。 一名用户属于单个组织。

组

表示具有某种相似之处的用户之间的关联。

组织

表示业务单元。 组织包含用户、组和其他组织等的详细信息。

对象说明包含以下信息：

- 有关对象 (p. 99)的信息，如 LDAP 对象类和对象所存储的容器。
- 存储条目相关信息的属性 (p. 103)。 例如，寻呼机属性存储寻呼机号码。

注意：CA Identity Manager 环境仅支持用户、组和组织对象中的一种类型。例如，所有用户对象都具有相同的对象类。

管理对象说明

通过在目录配置文件的“用户对象”、“组对象”和“组织对象”部分中指定对象信息来对管理对象进行说明。

注意：使用配置模板（directory.xml 文件）时，“组织对象”部分对不支持组织的用户目录不可用。

每个部分均包含 ImsManagedObject 元素，如以下示例所示：

```
<ImsManagedObject name="User" description="My Users"
objectclass="top,person,organizationalperson,inetorgperson" objecttype="USER">
```

如需要，ImsManagedObject 元素可以包括 Container 元素，如以下示例所示：

```
<Container objectclass="top,organizationalUnit" attribute="ou" value="people"
/>
```

指定对象信息

通过提供各种参数的值来指定对象信息。

遵循这些步骤：

1. 在“用户对象”、“组织对象”或“组对象”部分中，找到 ImsManagedObject 元素。

2. 提供以下参数的值：

name

指定管理对象的唯一名称。

注意：此参数是必需的。

description

包含管理对象的说明。

objectclass

指定对象类型（用户、组或组织）LDAP 对象类的名称。 对象类可确定对象可用属性的列表。

如果多个对象类的属性适用于一个对象类型，请在逗号分隔的列表中列出对象类。 例如，如果对象包含 person、organizationalperson 和 inetorgperson 对象类的属性，需添加如下对象类：

objectclass="top,person,organizationalperson,inetorgperson"

每个 LDAP 目录包含一组预定义对象类。 有关预定义对象类的详细信息，请参阅目录服务器文档。

注意：此参数是必需的。

objecttype

指定管理对象的类型。 有效值如下所示：

- 用户
- 组织
- 组

注意：此参数是必需的。

maxrows

指定搜索用户目录时 CA Identity Manager 可以返回的最大对象数目。 对象数目超出限制时，将显示错误。

通过设置 maxrows 参数的值，可以覆盖 LDAP 目录中限制搜索结果的设置。 在应用冲突的设置时，LDAP 服务器使用最低的设置。

注意：maxrows 参数不限制 CA Identity Manager 任务屏幕上显示的对象数目。 要配置显示设置，请在 CA Identity Manager 用户控制台中修改列表屏幕定义。有关说明，请参阅*《User Console Design Guide》*。

maxpagesize

指定在一次搜索中可以返回的对象数目。如果对象的数目超过页面大小，CA Identity Manager 将执行多个搜索。

在指定搜索页大小时，请注意下列几点：

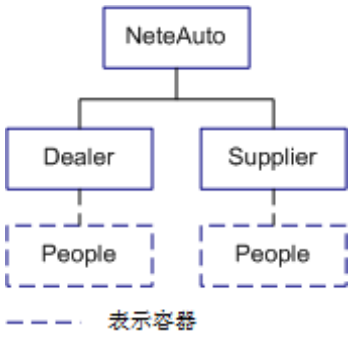
- 要使用“搜索页大小”选项，CA Identity Manager 管理的用户存储必须支持分页。 一些用户存储类型需要其他配置才可支持分页。 有关详细信息，请参阅“如何提高搜索性能” (p. 83)。
- 如果用户存储不支持分页，并且还指定了 maxrows 的值，则 CA Identity Manager 仅可使用 maxrows 值来控制搜索大小。

3. 如需要，可提供容器信息。

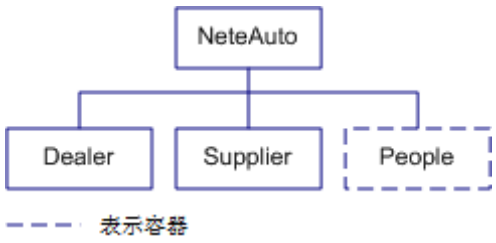
容器

为简化管理，可以对容器中特定类型的对象进行分组。 如果在目录配置文件中指定容器，CA Identity Manager 只可管理容器中的条目。 例如，如果指定名为“People”的用户容器，则 CA Identity Manager 会管理 People 容器中的用户，如下图所示：

- 层级目录



- 平面目录



在这些示例中，所有用户都存在于 People 容器中。

指定容器时，需注意以下几点：

- 如果组织中不存在容器，添加第一个条目后 CA Identity Manager 会立即创建容器。对于层级目录，CA Identity Manager 将在添加条目的组织中创建容器。对于平面目录和不支持组织的目录，CA Identity Manager 将在创建 CA Identity Manager 时指定的搜索根下创建容器。

- CA Identity Manager 将忽略指定容器中不存在的条目。 例如，如果指定 People 容器，将无法管理位于 People 容器之外的用户。

  注意：要管理不属于指定容器的用户，可以创建另一 CA Identity Manager 环境。

容器和常用属性

常用属性是在 CA Identity Manager 中具有特殊含义的属性。 CA Identity Manager 管理用户存储（包括容器）时，以下常用属性可识别有关容器的信息：

%ORG_MEMBERSHIP%

识别存储容器的全名 (DN) 的属性。

例如，全名类似于：

ou=People, ou=Employee, ou=NeteAuto, dc=security, dc=com

%ORG_MEMBERSHIP_NAME%

识别存储属性的用户友好名称的属性。

例如，前一示例中容器的用户友好名称为 People。

这些常用属性显示在 directory.xml 文件“用户对象”和“组对象”部分的属性说明中，如下所示：

```
 <ImsManagedObjectAttr physicalname="someattribute" description="Organization"
displayname="Organization" valuetype="String" required="true"
wellknown="%ORG_MEMBERSHIP%" maxlength="0" permission="WRITEONCE"
searchable="false" />
```

对于层级用户存储结构，physicalname 和 wellknown 参数会映射到常用属性中，如下所示：

```
<ImsManagedObjectAttr physicalname="%ORG_MEMBERSHIP%"
description="Organization" displayname="Organization" valuetype="String"
required="true" wellknown="%ORG_MEMBERSHIP%" maxlength="0"
permission="WRITEONCE" searchable="false" />
```

本示例表示，CA Identity Manager 会自动从 directory.xml 文件的其他信息中派生出容器 DN 和用户友好名称。

对于平面用户存储结构，需提供物理属性名称。

注意：有关说明，请参阅“如何描述平面用户目录结构” (p. 75)。

指定用户或组容器

请按照以下步骤指定用户或组容器。

遵循这些步骤:

1. 在“用户对象”或“组对象”部分中，找到 Container 元素。
2. 提供以下参数的值：

objectclass

确定特定类型的对象所创建的容器的 LDAP 对象类。 例如，用户容器的默认值为“top,organizationalUnit,”，这表示用户在 LDAP 组织单元 (ou) 中创建。

管理动态或嵌套组时，需确保指定支持这些组类型 (p. 77)的对象类。

注意：此参数是必需的。

attribute

指定存储容器名称的属性，例如 ou。

属性与值配对，从而形成容器的相关 DN，如以下示例所示：

ou=People

注意：此参数是必需的。

value

指定容器的名称。

注意：此参数是必需的。

注意：无法对组织指定容器。

属性说明

属性可存储有关条目的信息，如电话号码或地址。条目属性可确定其配置文件。

在目录配置文件的 ImsManagedObjectAttr 元素中，对属性进行了说明。 在目录配置文件的“用户对象”、“组对象”和“组织对象”部分中，可以执行以下操作：

- 修改默认属性说明，以对用户存储中的属性进行说明。
- 通过复制现有说明并根据需要修改值，来创建新的属性说明。

对于用户、组和组织配置文件中的每个属性，只有一个 ImsManagedObjectAttr 元素。 例如，ImsManagedObjectAttr 元素会被描述为用户 ID。

ImsManagedObjectAttr 元素类似于以下代码：

```
<ImsManagedObjectAttr physicalname="uid" displayname="User ID"
description="User ID" valuetype="String" required="true" multivalued="false"
wellknown="%USER_ID%" maxlength="0" />
```

ImsManagedObjectAttr 具有以下参数：

physicalname

此参数必须包含以下项之一：

- 存储配置文件值的 LDAP 属性的名称。例如，用户 ID 存储在用户目录的 uid 属性中。

  注意：为提高性能，需对用于用户控制台中搜索查询的 LDAP 属性进行索引。

- 常用属性 (p. 69)。提供常用属性时，CA Identity Manager 将自动计算值。例如，一旦指定常用属性 %ORG_MEMBERSHIP%，CA Identity Manager 将根据条目的 DN，确定条目所属的组织。

description

包含属性的说明

displayname

指定属性的唯一名称。

在用户控制台中，显示名称会显示在可添加到任务屏幕的属性列表中。 此参数是必需的。

注意：请勿修改目录配置文件 (directory.xml) 中属性的显示名称。 要更改任务屏幕上属性的名称，可以在任务屏幕定义中为属性指定标签。 有关详细信息，请参阅*《管理指南》*。

valuetype

指定属性的数据类型。 有效值如下所示：

字符串

该值可以为任何字符串。

这是默认值。

整数

该值必须为整数。

注意：整数不支持十进制数。

数字

该值必须为整数。 数字选项支持十进制数。

日期

值必须解析为使用以下样式的有效日期：

MM/dd/yyyy

ISODate

该值必须解析为使用 yyyy-MM-dd 模式的有效日期。

UnicenterDate

该值必须解析为使用 YYYYYYYDDD 模式的有效日期，其中：

YYYYYYY 是用于表示年份的七个数字，以三个零开头。 例如：0002008

DDD 是表示日期的三个数字，根据需要以几个零开头。有效值应介于 001 到 366 之间。

结构化

这种属性由结构化数据组成，这些结构化数据使单个属性值能够存储多个相关值。 例如，结构化属性包含以下值，如名字、姓氏和电子邮件地址值。

某些端点类型会使用这些属性，但它们受到 CA Identity Manager 的管理。

注意： CA Identity Manager 可以在用户控制台的表中显示结构化属性。 用户编辑表中的值时，这些值将存储在用户存储中，从而传播回端点。有关显示多值属性的详细信息，请参阅*《管理指南》*。

required

表示属性是否为必需，如下所示：

- True－属性为必需的。
- False－属性为可选的（默认）。

注意：如果属性为 LDAP 目录服务器所必需的，则需将必需参数设置为 true。

multivalued

表示属性是否可以具有多个值。例如，为存储每位组成员的用户 DN，组成员身份属性必须为多值属性。 有效值如下所示：

- True－属性可以具有多个值。
- False－属性只能具有一个值（默认）。

重要说明！ 用户对象定义中的组成员身份和管理角色属性均必须为多值属性。

wellknown

定义常用属性的名称。

常用属性在 CA Identity Manager 中具有特定含义 (p. 69)。这些属性用以下语法进行定义：

%ATTRIBUTENAME%

maxlength

定义属性可以具有的值的最大长度。将 maxlength 参数设置为 0 以指定无限长度。

注意：此参数是必需的。

permission

表示属性的值是否可以在任务屏幕中进行修改。 有效值如下所示：

READONLY

该值可以显示，但无法修改。

WRITEONCE

一旦创建了对象，便无法修改该值。 例如，在创建用户之后，将无法更改用户 ID。

READWRITE

该值可以进行修改（默认）。

hidden

表示属性是否在 CA Identity Manager 任务表单中显示。有效值如下所示：

- True－属性不向用户显示。
- False－属性向用户显示（默认）。

逻辑属性使用隐藏属性。

注意：有关详细信息，请参阅*《Programming Guide for Java》*。

system

仅指定 CA Identity Manager 使用的属性。用户控制台中的用户不可修改这些属性。 有效值如下所示：

- True－用户不可修改此属性。该属性隐藏在 CA Identity Manager 用户界面中。
- False－用户可以修改此属性。此属性可添加到 CA Identity Manager 用户界面的任务屏幕中。 （默认）

validationruleset

将验证规则集与属性相关联。

确认所指定的验证规则集已在“目录配置文件的 ValidationRuleSet 元素”中进行定义。

objectclass

表示当属性不属于 ImsManagedObject 元素中指定的主对象类时，用户、组或组织属性的 LDAP 辅助类。

例如，假定用户的主对象类为 top、person 和 organizationalperson，其中定义了以下用户属性：

- 公用名称 (cn)
- 姓 (sn)
- 用户 ID (uid)
- 密码 (userPassword)

要包含员工辅助类中定义的属性 employeeID，可添加以下属性说明：

```
<ImsManagedObjectAttr physicalname="employeeID" displayname="Employee ID"
description="Employee ID" valuetype="String" required="true"
multivalued="false" maxlength="0" objectclass="Employee"/>
```

指定属性说明

说明属性需执行以下步骤：

1. 阅读以下主题中的相关部分：
   - CA Directory 注意事项 (p. 67)
   - Microsoft Active Directory 注意事项 (p. 67)
   - IBM Directory Server 注意事项 (p. 67)
   - Oracle Internet Directory 注意事项 (p. 68)
2. 在目录配置文件的“用户对象”、“组对象”和“组织对象”部分中，可以执行以下操作：
   - 修改默认属性说明，以对目录属性进行说明。
   - 通过复制现有说明并根据需要修改值，来创建新的属性说明。

   注意：假定已创建新的属性说明，且已指定物理属性。 确保物理属性必须存在于为对象类型指定的对象类（或类）中。
3. （可选）对属性更改显示设置 (p. 63)，以防在用户控制台中显示敏感信息（如密码或工资）。
4. （可选）配置默认排序顺序。
5. 如果管理具有平面或平面用户结构或不包含组织的目录，请转到“说明用户目录结构” (p. 75)。

管理敏感属性

CA Identity Manager 提供了以下方法来管理敏感属性：

- 属性的数据分类

  数据分类允许您在目录配置文件 (directory.xml) 中指定属性的显示和加密属性。

  您可以定义管理敏感属性的数据分类，如下所示：

  - 在 CA Identity Manager 任务屏幕中，将属性的值显示为一串星号。

    例如，您可以将密码显示为星号，而不显示为明文。

  - 在“查看提交的任务”屏幕中，隐藏该属性值。

    此选项使您可以对管理员隐藏属性。例如，向在 CA Identity Manager 中查看任务状态但不需要查看工资详细信息的管理员隐藏工资详细信息（例如工资）。

  - 在创建现有对象的副本时忽略某些属性。

  - 加密属性

- 任务配置文件屏幕中的字段样式

  如果您不想在 directory.xml 文件中修改属性，可在显示敏感属性的屏幕定义中设置属性的显示属性。

  字段样式使您可以将密码等属性显示为一串星号，而不显示为明文。

  注意：有关敏感属性的字段样式的详细信息，请在用户控制台帮助中搜索字段样式。

数据分类属性

数据分类元素提供了一种方法，可以将附加属性与属性说明关联起来。 此元素中的值确定了 CA Identity Manager 处理属性的方式。 此元素支持以下参数：

- sensitive

  使 CA Identity Manager 在“查看提交的任务”屏幕中将该属性显示为一串星号 (*)。 此参数可防止属性的旧值和新值在“查看提交的任务”屏幕中显示为明文。

  另外，如果您在用户控制台中创建了现有用户的副本，此参数可防止属性被复制到新的用户。

- vst_hide

  在“查看提交的任务”选项卡的“事件详细信息”屏幕中隐藏属性。与显示为星号的敏感属性不同，vst_hidden 属性不会显示。

  您可以使用此参数来阻止在“查看提交的任务”中显示对工资等属性所做的更改。

- ignore_on_copy

  使 CA Identity Manager 在管理员于用户控制台中创建对象的副本时忽略某属性。 例如，假设您为用户对象的密码属性指定 ignore_on_copy。 在复制用户配置文件时，CA Identity Manager 不会将当前用户的密码应用于新的用户配置文件。

- AttributeLevelEncrypt

  在将属性值存储在用户存储中时对其加密。 如果 CA Identity Manager 启用了 FIPS 140-2，CA Identity Manager 使用 RC2 加密或 FIPS 140-2 加密。

  有关 CA Identity Manager 中对 FIPS 140-2 的支持的详细信息，请参阅 *《配置指南》*。

  这类属性在运行时显示为明文。

  注意：为了防止属性在屏幕中以明文显示，您还可以为加密的属性添加敏感数据分类元素。 有关详细信息，请参阅"如何添加属性级别的加密" (p. 65)。

- PreviouslyEncrypted

  使 CA Identity Manager 在访问用户存储中的对象时检测和解密属性中任何加密的值。

  您可以使用此数据分类来解密任何先前加密的值。

  在您保存对象时，会将明文值保存在存储中。

用户控制台中的敏感属性

可能有一些属性（例如密码），不应以纯文本形式显示在用户控制台中。 目录配置文件包含了两个属性，您可以使用它们来隐藏敏感属性：

- sensitive

  此参数使 CA Identity Manager 将属性显示为一串星号 (*)。 它可用来防止密码以明文显示。

- vst_hidden

  此参数会在"查看提交的任务"选项卡的"事件详细信息"屏幕中隐藏属性。敏感属性会在"事件"选项卡的 ?? 部分 中显示为星号，与之不同，vst_hidden 属性不会显示。

  您可以使用此参数来防止对工资等属性所做的更改显示在用户控制台中。

在用户控制台中隐藏属性

1. 找到您要在目录配置文件中隐藏的属性。
2. 在属性说明之后，添加以下内容：

   <DataClassification name="*parameter*">

   parameter

   代表以下参数：

   sensitive

   vst_hidden

   例如，sensitive 参数的属性说明如下所示：

   ```
   <ImsManagedObjectAttr physicalname="##PASSWORD_HINT" displayname="Password
   Hint" description="Password Hint" valuetype="String" required="false"
   multivalued="true" wellknown="%PASSWORD_HINT%" maxlength="0">
       <DataClassification name="sensitive"/>
   ```

   vst_hidden 属性的属性说明如下所示：

   ```
   <ImsManagedObjectAttr physicalname="salery" displayname="Salary"
   description="salary" valuetype="String" required="false"
   multivalued="false" maxlength="0">
       <DataClassification name="vst_hidden"/>
   ```

属性级别的加密

您可以通过在目录配置文件 (directory.xml) 中指定属性的 AttributeLevelEncypt 数据分类来加密用户存储中的属性。 在启用了属性级别的加密时，CA Identity Manager 会在将属性的值存储在用户存储中之前将其加密。 该属性在用户控制台中以明文显示。

注意：为了防止属性在屏幕中以明文显示，您还可以为加密的属性添加敏感数据分类元素。 有关详细信息，请参阅“如何添加属性级别的加密” (p. 65)。

如果启用了 FIPS 140-2 支持，则会使用 RC2 加密或 FIPS 140-2 加密来加密该属性。

在实施属性级别的加密之前，请注意下列几点：

- CA Identity Manager 不能在搜索中找到加密的属性。

  假设将加密的属性添加到成员、管理员、所有者策略或身份策略。 由于 CA Identity Manager 无法搜索属性，所以不能正确地解析该策略。

  考虑在 directory.xml 文件中将属性设置为 searchable="false"，例如：

  <ImsManagedObjectAttr physicalname="title" description="Title" displayname="Title" valuetype="String" maxlength="0" searchable="false">

  <DataClassification name="AttributeLevelEncrypt"/>

  </ImsManagedObjectAttr>

- 如果 CA Identity Manager 使用共享用户存储和配给目录，请不要加密配给服务器属性。
- 不要在满足以下条件的环境中为用户密码启用 AttributeLevelEncrypt：
  - 包含了 CA SiteMinder 集成，
  - 并且在关系数据库中存储用户

  如果 CA Identity Manager 与 CA SiteMinder 集成，则在新的用户尝试进行登录并以明文输入密码时，加密的密码会引起问题。
- 如果您为 CA Identity Manager 之外的其他应用程序使用的用户存储启用了属性级别的加密，则其他应用程序将无法使用加密的属性。

如何添加属性级别的加密

假定您为 CA Identity Manager 目录添加了属性级别的加密。 在您保存与该属性关联的对象时，CA Identity Manager 会自动加密现有明文属性值。例如，加密密码属性会在保存用户的配置文件时加密密码。

注意：要加密属性值，您用来保存对象的任务必须包含该属性。 要加密上例中的密码属性，请确保将密码字段添加到了您用来保存对象的任务，例如“修改用户”任务。

在用户存储中，所有新的对象都会使用加密的值进行创建。

遵循这些步骤:

1. 完成以下任务之一：
   - 创建 CA Identity Manager 目录
   - 通过导出目录设置来更新现有目录。
2. 在 directory.xml 文件中将下列数据分类属性添加到您要加密的属性中：

   AttributeLevelEncrypt

   在用户存储中以加密形式保存属性值。

   sensitive（可选）

   在 CA Identity Manager 屏幕中隐藏属性值。 例如，密码显示为星号 (*)。

   例如：

```
<ImsManagedObjectAttr physicalname="salary"
displayname="Salary" description="salary" valuetype="String"
required="false" multivalued="false" maxlength="0"
searchable="false">
<DataClassification name="AttributeLevelEncrypt"/>
<DataClassification name="sensitive"/>
```

3. 如果已创建 CA Identity Manager 目录，请将该目录与环境关联。
4. 要强制 CA Identity Manager 立即加密所有值，请使用批量加载程序修改所有对象。

   注意：有关批量加载程序的详细信息，请参阅*《管理指南》*。

如何删除属性级别的加密

如果您的 CA Identity Manager 目录中具有加密的属性，并且该属性在存储时值为明文，则您可以删除 AttributeLevelEncrypt 数据分类。

在删除该数据分类后，CA Identity Manager 会停止加密新的属性值。在您保存与该属性关联的对象时，现有的值会被解密。

注意：要解密属性值，您用来保存对象的任务必须包含该属性。 例如，要解密现有用户的密码，您应使用包含密码字段的任务保存用户对象，例如“修改用户”任务。

要强制 CA Identity Manager 检测和解密保留在属性的用户存储中的任何加密值，您可以指定另一数据分类：PreviouslyEncrypted。 在您保存对象时，明文值会被保存到用户存储。

注意：添加 PreviouslyEncrypted 数据分类会为每一对象加载增加额外的处理任务。 为防止性能问题，请考虑在添加 PreviouslyEncrypted 数据分类时，加载和保存与该属性关联的每一对象，然后删除该数据分类。 这一方法会将所有存储的加密值自动转换为存储的明文。

遵循这些步骤:

1. 导出适当的 CA Identity Manager 目录的目录设置。
2. 在 directory.xml 文件中，从您想要解密的属性删除数据分类 AttributeLevelEncrypt。
3. 如果您要强制 CA Identity Manager 删除先前加密的值，请添加 PreviouslyEncrypted 数据分类属性。

   例如：

   ```
   <ImsManagedObjectAttr physicalname="salary" displayname="Salary"
   description="salary" valuetype="String" required="false"
   multivalued="false" maxlength="0" searchable="false">
   <DataClassification name="PreviouslyEncrypted"/>
   ```

4. 要强制 CA Identity Manager 立即解密所有值，请使用批量加载程序修改所有对象。

   注意：有关批量加载程序的详细信息，请参阅 *《管理指南》*。

CA Directory 注意事项

对 CA Directory 用户存储的属性进行说明时，需注意以下几点：

- 属性名称需区分大小写。
- 使用 seeAlso 属性来表示在管理员建立组时自行订阅组可能导致错误。

使用照片属性来表示在管理员创建用户时用户帐户（启用或禁用）的状态可能导致错误。

注意：有关 CA Directory 要求的其他信息，请参阅 CA Directory 文档。

Microsoft Active Directory 注意事项

对 Active Directory 的属性进行说明时，需注意以下几点：

- 属性说明中指定属性的大小写形式必须与 Active Directory 中属性的大小写形式一致。 例如，如果选择 unicodePwd 属性来存储用户密码，需在目录配置文件中指定 unicodePwd（包含大写字母 P）。
- 对于用户和组对象，需确保其中包括 sAMAccountName 属性。

IBM Directory Server 注意事项

对 IBM Directory Server 用户目录的属性进行说明时，需参阅以下部分：

- Directory Server 目录中的组 (p. 68)
- 组织对象说明中的对象类“Top” (p. 68)

Directory Server 目录中的组

IBM Directory Server 要求组至少包含一个成员。 为满足此要求，在创建新组时，CA Identity Manager 需添加*冗余用户*作为该组的成员。

配置冗余用户

遵循这些步骤:

1. 在目录配置文件的“组对象”部分中，找到以下元素：

   ```
   <PropertyDict name="DUMMY_USER">
       <Property name="DUMMY_USER_DN">##DUMMY_USER_DN</Property>
   </PropertyDict>
   ```

   注意：如果目录配置文件中不存在这些元素，请按照此处显示的这些元素一一进行添加。

2. 将 ##DUMMY_USER_DN 替换为用户 DN。 CA Identity Manager 可添加此 DN 作为所有新组的成员。

   注意：如果指定现有用户的 DN，则该用户将显示为所有 CA Identity Manager 组的成员。 要防止*冗余用户*显示为组成员，请指定不存在于该目录的 DN。

3. 保存目录配置文件。

组织对象说明中的对象类 Top

重要说明！ 在目录配置文件组织对象的说明中，请勿包含对象类 Top。

例如，当组织对象的对象类为 top、organizationalUnit 时，请按如下方式指定对象类：

```
<ImsManagedObject name="Organization" description="My Organizations"
objectclass="organizationalUnit" objecttype="ORG">
```

包含 top 会导致产生不可预知的搜索结果。

Oracle Internet Directory 注意事项

对 Oracle Internet Directory (OID) 用户存储的属性进行说明时，仅需使用小写字母指定 LDAP 属性。

LDAP 用户存储的常用属性

常用属性在 CA Identity Manager 中具有特殊含义。 这些属性用以下语法进行定义：

%ATTRIBUTENAME%

在此语法中，*ATTRIBUTENAME* 必须为大写。

通过使用属性说明 (p. 103)，将常用属性对应地映射到一个物理属性中。

在以下属性说明中，属性 userpassword 会映射到常用属性 %PASSWORD% 中，以便 CA Identity Manager 将 userpassword 中的值视为密码，如下所示：

```
<ImsManagedObjectAttr
        physicalname="userpassword"
        displayname="Password"
        description="Password"
        valuetype="String"
        required="false"
        multivalued="false"
        wellknown="%PASSWORD%"
        maxlength="0" />
```

一些常用属性是必需的；其他则为可选的。

用户常用属性

用户常用属性的列表及这些属性映射的项如下所示：

%ADMIN_ROLE_CONSTRAINT%

映射到管理员的管理角色列表。

映射到 %ADMIN_ROLE_CONSTRAINT% 的物理属性必须为多值属性，才可容纳多个角色。

建议对映射到 %ADMIN_ROLE_CONSTRAINT% 的 LDAP 属性进行索引。

%CERTIFICATION_STATUS%

映射到用户的认证状态。

此属性需要使用用户认证功能。

注意：有关用户认证的详细信息，请参阅*《管理指南》*。

%DELEGATORS%

映射到对当前用户有已指派工作项的用户的列表。

此属性需要使用指派。 映射到 %DELEGATORS% 的物理属性必须是多值的并且能够保留字符串。

重要说明！ 直接使用 CA Identity Manager 任务或外部的工具编辑此字段可以引起重大安全影响。

%EMAIL%

映射到用户的电子邮件地址。

需要使用电子邮件通知功能。

%ENABLED_STATE%

（必需）

映射到用户的状态。

注意：此属性必须与 SiteMinder 用户目录连接中的禁用标志用户目录属性匹配。

%FIRST_NAME%

映射到用户的名字。

%FULL_NAME%

映射到用户的姓名。

%IDENTITY_POLICY%

指定应用于用户帐户的身份策略的列表，以及已对用户对象执行添加或删除操作的唯一 Policy Xpress 策略 ID 的列表。

CA Identity Manager 使用此属性来确定是否需要将身份策略应用于用户。 假定策略已启用“Apply Once”（应用一次）设置，且策略已在 %IDENTITY_POLICY% 属性中列出。CA Identity Manager 不会将策略中的更改应用于用户。

注意：有关身份策略的详细信息，请参阅*《管理指南》*。

%LAST_CERTIFIED_DATE%

映射到用户认证角色时的日期。

需要使用用户认证功能。

注意：有关用户认证的详细信息，请参阅*《管理指南》*。

%LAST_NAME%

映射到用户的姓氏。

%MEMBER_OF%

映射到用户作为成员所属的组的列表。

映射到 %MEMBER_OF% 的物理属性必须为多值属性，才可容纳多个组。

搜索用户的组时，使用此属性可提高响应速度。

可以将此属性与 Active Directory 或任何目录架构（维护用户对象上用户的组成员身份）结合使用。

%ORG_MEMBERSHIP%

（必需）

映射到用户所属组织的 DN。

CA Identity Manager 使用此常用属性来确定目录的结构 (p. 75)。

用户目录不包含组织时，此属性为非必需的。

%ORG_MEMBERSHIP_NAME%

（必需）

映射到用户配置文件所在组织的用户友好名称。

用户目录不包含组织时，此属性为非必需的。

%PASSWORD%

映射到用户的密码。

此属性必须与 SiteMinder 用户目录连接中的密码属性匹配。

注意：即使属性或字段未设置为隐藏密码，%PASSWORD% 属性的值在 CA Identity Manager 屏幕中始终显示为一系列星号 (*) 字符。

%PASSWORD_DATA%

（密码策略支持所必需的）

指定跟踪密码策略信息的属性。

注意：即使属性或字段未设置为隐藏密码，%PASSWORD_DATA% 属性的值在 CA Identity Manager 屏幕中始终显示为一系列星号 (*) 字符。

%PASSWORD_HINT%

（必需）

映射到用户指定的问答对。 用户忘记密码时，将用到此问答对。

要支持多个问答对，请确保 %PASSWORD_HINT% 属性为多值属性。

如果要使用 SiteMinder 的密码服务功能来管理密码，密码提示属性必须与 SiteMinder 用户目录中的质询/响应属性匹配。

注意：即使属性或字段未设置为隐藏密码，%PASSWORD% 属性的值在 CA Identity Manager 屏幕中始终显示为一系列星号 (*) 字符。

%USER_ID%

（必需）

映射到用户的 ID。

组常用属性

以下项为组常用属性的列表：

%GROUP_ADMIN_GROUP%

表示存储作为组管理员的组的列表的属性。 例如，当第 1 组是 A 组的管理员时，第 1 组将存储在 %GROUP_ADMIN_GROUP% 属性中。

注意：如果未指定 %GROUP_ADMIN_GROUP% 属性，CA Identity Manager 会将管理员组存储在 %GROUP_ADMIN% 属性中。

注意：要将一个组添加为另一个组的管理员，请参阅*《管理指南》*。

%GROUP_ADMIN%

表示包含组管理员 DN 的属性。

映射到 %GROUP_ADMIN% 的物理属性必须为多值属性。

%GROUP_DESC%

表示包含组说明的属性。

%GROUP_MEMBERSHIP%

（必需）

表示包含组成员列表的属性。

映射到 %GROUP_MEMBERSHIP% 的物理属性必须为多值属性。

%GROUP_MEMBERSHIP% 常用属性对于配给用户目录为非必需的。

%GROUP_NAME%

（必需）

表示存储组名称的属性。

%ORG_MEMBERSHIP%

（必需）

表示包含组所属组织 DN 的属性。

CA Identity Manager 使用此常用属性来确定目录的结构 (p. 75)。

用户目录不包含组织时，此属性为非必需的。

%ORG_MEMBERSHIP_NAME%

表示包含组所在组织用户友好名称的属性。

此属性对不包含组织的用户目录无效。

%SELF_SUBSCRIBING%

表示确定用户是否可以订阅组 (p. 74)的属性。

%NESTED_GROUP_MEMBERSHIP%

表示存储作为组成员的组的列表的属性。例如，当第 1 组是 A 组的成员时，第 1 组将存储在 %NESTED_GROUP_MEMBERSHIP% 属性中。

如果未指定 %NESTED_GROUP_MEMBERSHIP% 属性，CA Identity Manager 会将嵌套组存储在 %GROUP_MEMBERSHIP% 属性中。

要包含作为其他组的成员的组，请按照“配置动态组和嵌套组”中所述的相关说明配置嵌套组的支持。

%DYNAMIC_GROUP_MEMBERSHIP%

表示存储生成动态组 (p. 125)的 LDAP 查询的属性。

注意：要扩展组对象的可用属性，使其包含 %NESTED_GROUP_MEMBERSHIP% 和 %DYNAMIC_GROUP_MEMBERSHIP% 属性，可以使用辅助对象类。

组织常用属性

以下常用属性仅适用于以下支持组织的环境：

%ORG_DESCR%

表示包含组织说明的属性。

%ORG_MEMBERSHIP%

（必需）

表示包含组织的父组织 DN 的属性。

%ORG_MEMBERSHIP_NAME%

表示包含组织的父组织用户友好名称的属性。

%ORG_NAME%

（必需）

表示包含组织名称的属性。

%ADMIN_ROLE_CONSTRAINT% 属性

创建管理角色时，需为角色成员身份指定一个或多个规则。 满足成员身份规则的用户将授予角色。 例如，当用户管理器角色的成员身份规则为 title=User Manager 时，拥有“用户管理器”标题的用户将具有用户管理器角色。

注意：有关规则的详细信息，请参阅 *《管理指南》*。

%ADMIN_ROLE_CONSTRAINT% 使您能够指定存储管理员管理角色的配置文件属性。

如何使用 %ADMIN_ROLE_CONSTRAINT% 属性

要将 %ADMIN_ROLE_CONSTRAINT% 用作所有管理角色的约束，请执行以下任务：

- 将 %ADMIN_ROLE_CONSTRAINT% 常用属性与可容纳多个角色的多值配置文件属性配对。
- 在用户控制台中配置管理角色时，请确保以下约束的相关信息：

  “管理角色”等于 *角色名称*

  角色名称

  定义提供约束的角色的名称，如以下示例所示：

  “管理角色”等于“用户管理员”

注意：管理角色是 %ADMIN_ROLE_CONSTRAINT% 属性的默认显示名称。

配置常用属性

请按照以下步骤配置常用属性。

遵循这些步骤:

1. 在目录配置文件中，搜索以下符号：

   ##
2. 将以 ## 开头的值替换为相应的 LDAP 属性。
3. 重复步骤 1 和 2，直到替换所有必需值。
4. 根据需要将可选常用属性映射到物理属性中。
5. 保存目录配置文件。

说明用户目录结构

CA Identity Manager 使用 %ORG_MEMBERSHIP% 常用属性来确定用户目录的结构。

说明用户目录结构的步骤取决于目录结构的类型。

如何说明层级目录结构

已配置层级目录结构的目录配置文件。因此，无需修改 %ORG_MEMBERSHIP% 属性说明。

如何说明平面用户目录结构

遵循这些步骤:

1. 在 directory.xml 文件的“用户对象”部分中找到 %ORG_MEMBERSHIP% 属性说明。
2. 在 physicalname 参数中，将 %ORG_MEMBERSHIP% 替换为存储用户所属组织的属性名称。

如何说明平面目录结构

遵循这些步骤:

1. 在 directory.xml 文件的“用户对象”部分中找到 %ORG_MEMBERSHIP% 属性说明。
2. 在 physicalname 参数中，将 %ORG_MEMBERSHIP% 替换为存储用户所属组织的属性名称。
3. 在“组对象”部分中重复步骤 1。
4. 在 physicalname 参数中，将 %ORG_MEMBERSHIP% 替换为存储组所属组织的属性名称。

如何说明不支持组织的用户目录

确认 directory.xml 中未对组织定义对象说明或常用属性。

如何配置组

对于配置，可将组分成以下类型：

- 自行订阅组
- 动态和嵌套组

配置自行订阅组

通过在目录配置文件中配置对自行订阅组的支持，使自助服务用户能够加入组。

用户自行注册时，CA Identity Manager 将在指定的组织内查找组，然后将自行订阅组显示给用户。

遵循这些步骤:

1. 在“自行订阅组”部分中，按如下方式添加 SelfSubscribingGroups 元素：

   <SelfSubscribingGroups type=*search_type* org=*org_dn*>

2. 添加以下参数的值：

   type

   表示 CA Identity Manager 搜索自行订阅组的位置，如下所示：

   - NONE－CA Identity Manager 不搜索组。指定 NONE 可防止用户自行订阅组。
   - ALL－CA Identity Manager 从根开始搜索组。在用户可以通过层级目录订阅组时指定 ALL。
   - INDICATEDORG－CA Identity Manager 在用户组织及其子组织内搜索自行订阅组。 例如，当用户的配置文件位于营销组织中时，CA Identity Manager 将在营销组织及所有子组织中搜索自行订阅组。
   - SPECIFICORG－CA Identity Manager 在特定组织中搜索。 在 org 参数中提供特定组织的辨别名称 (DN)。

   org

   指定 CA Identity Manager 搜索自行订阅组所在组织的唯一标识符。

   注意：请确保指定 type=SPECIFICORG 时的 org 参数。

在 CA Identity Manager 目录中配置自行订阅组支持之后，CA Identity Manager 管理员即可指定用户控制台中自行订阅的组。

注意：有关管理组的详细信息，请参阅 *《管理指南》*。

配置动态和嵌套组

如果要管理 LDAP 用户存储，可以在目录配置文件中对以下类型的组配置支持：

动态组

使您能够通过在用户控制台中动态地指定 LDAP 筛选查询定义组成员身份。 有了动态组，管理员无需单独搜索和添加组成员。

嵌套组

使您能够将组添加为其他组的成员。

您可以使用目录配置文件启用动态和嵌套组。

遵循这些步骤:

1. 根据需要将以下常用属性 (p. 72)映射到组管理对象的物理属性：
   - %DYNAMIC_GROUP_MEMBERSHIP%
   - %NESTED_GROUP_MEMBERSHIP%

   注意：您选择的物理属性必须支持多个值。
2. 在“目录组行为”部分中，添加下列 GroupTypes 元素：

   `<GroupTypes type=group>`

   注意：GroupTypes 区分大小写。
3. 为下列参数输入值：

   group

   启用对动态和嵌套组的支持。 有效值如下所示：
   - NONE－CA Identity Manager 不支持动态和嵌套组。
   - ALL－CA Identity Manager 支持动态和嵌套组。
   - DYNAMIC－CA Identity Manager 仅支持动态组。
   - NESTED－CA Identity Manager 仅支持嵌套组。

一旦在 CA Identity Manager 目录中配置了对动态和嵌套组的支持，CA Identity Manager 管理员就可以在用户控制台中指定哪些组是动态组和嵌套组。

注意：如果在*没有*设置 %NESTED_GROUP_MEMBERSHIP% 常用参数的情况下，将组类型设为 NESTED 或 ALL。 在这样的情况中，CA Identity Manager 将嵌套组和用户都存储在 %GROUP_MEMBERSHIP% 常用参数中。 处理组成员资格可能更慢一点。

作为组的管理员添加对组的支持

如果正在管理 LDAP 用户存储，您可以启用组，作为其他组的管理员。在您将组分配为管理员时，只有该组的管理员是指定的组的管理员。 您指定的管理员组的成员没有权限管理该组。

遵循这些步骤:

1. 将 %GROUP_ADMIN_GROUP% 常用属性映射到存储担任管理员的组的列表的物理属性。

   注意：您选择的物理属性必须支持多个值。

   组常用属性 (p. 72)提供有关 %GROUP_ADMIN_GROUP% 属性的详细信息。

   注意：如果您在没有设置 %GROUP_ADMIN_GROUP% 常用属性的情况下，将管理员组类型设置为 ALL，CA Identity Manager 会将管理员组存储在 %GROUP_ADMIN% 属性中。

2. 在“目录 AdminGroups 行为”部分中，配置 AdminGroupTypes 元素，如下所示：

   <AdminGroupTypes type="ALL">

   默认 AdminGroupTypes 为 NONE。

   注意：AdminGroupTypes 区分大小写。

一旦在 CA Identity Manager 目录中配置了对作为管理员的组的支持，CA Identity Manager 管理员就可以在用户控制台中指定作为其他组的管理员的组。

验证规则

验证规则会强制性索取用户在任务屏幕字段中输入的数据。 这些要求可以强制限定数据类型或格式。 因此，请确保数据在任务屏幕上的其他数据的上下文中是有效的。

验证规则与配置文件属性关联。CA Identity Manager 在处理任务之前确保为配置文件属性输入的数据满足任何关联的验证规则。

您可以定义验证规则，并可以将他们与目录配置文件中的配置文件属性关联。

其他 CA Identity Manager 目录属性

您可以配置以下其他字段：

- 对搜索结果排序。
- 跨对象类搜索，以确认新用户已经不存在。
- 等待一定时间以在从主 LDAP 目录到从属 LDAP 目录的数据复制完成之前避免 CA Identity Manager 超时。

配置排序顺序

您可以为每个管理对象（如用户、组或组织）指定排序属性。CA Identity Manager 使用此属性来使用通过 CA Identity Manager API 创建的自定义业务逻辑对搜索结果进行排序。

注意：排序属性不影响搜索结果在用户控制台中显示的方式。

例如，在您为用户对象指定 cn 属性时，CA Identity Manager 会根据 cn 属性按字母顺序对搜索用户的结果进行排序。

遵循这些步骤:

1. 在应用排序顺序的管理对象的部分的最后一个 IMSManagedObjectAttr 元素之后，添加以下语句：

```
<PropertyDict name="SORT_ORDER">
    <Property name="ATTR">your_sort_attribute
</Property>
</PropertyDict>
```

2. 将 *your_sort_attribute* 替换成 CA Identity Manager 对搜索结果进行排序的属性。

注意：仅指定一个物理属性。 不要指定常用属性。

例如，假定您必须基于 cn 属性的值对用户搜索结果进行排序。 在目录配置文件的“用户对象”部分的最后一个 IMSManagedObjectAttr 元素之后添加以下元素：

```
<!-- ******************** User Object ******************** -->
   <ImsManagedObject name="User" description="My Users"
      objectclass="top,person,organizationalperson,user"
      objecttype="USER">
   .
   .
   .
        <ImsManagedObjectAttr physicalname="departmentnumber"
                displayname="Department" description="Department"
                valuetype="String" required="true"
                multivalued="false" maxlength="0" />
        <PropertyDict name="SORT_ORDER">
                <Property name="ATTR">cn</Property>
        </PropertyDict>
  </ImsManagedObject>
```

跨对象类搜索

在您创建用户时 CA Identity Manager 搜索用户存储以检查该用户是否存在。 此搜索局限于具有在目录配置文件（directory.xml）的用户对象定义中指定的对象类的用户。如果在那些对象类中没有找到现有用户，CA Identity Manager 将尝试创建用户。

如果存在使用同样的唯一标识符（用户 ID）但是使用不同对象类的用户，LDAP 服务器将无法创建该用户。 在 LDAP 服务器中会报告此错误，但是 CA Identity Manager 不识别此错误。 CA Identity Manager 看起来成功地创建了此用户。

要防止此问题，您可以配置 SEARCH_ACROSS_CLASSES 属性，这样 CA Identity Manager 在检查现有用户时会在所有对象类定义中搜索用户。

注意：此属性仅在执行创建用户等任务时影响对重复用户的搜索。 对于所有其他搜索，可以应用对象类约束。

遵循这些步骤:

1. 在目录配置文件 (directory.xml) 中，找到描述用户对象的 ImsManagedObject 元素。
2. 添加下列 PropertyDict 元素：

```
<PropertyDict name="SEARCH_ACROSS_CLASSES" description="allowing checking
an attribute across classes ">
<Property name="ENABLE">true</Property>
</PropertyDict>
```

注意：PropertyDict 元素必须是 ImsManagedObject 元素的末元素，如下例所示：

```
<ImsManagedObject name="User" description="My Users"
objectclass="top,person,organizationalperson,inetorgperson,customClass"
objecttype="USER">
<ImsManagedObjectAttr physicalname="departmentnumber"
displayname="Department" description="Department" valuetype="String"
required="true" multivalued="false" maxlength="0" />
.
.
.
<PropertyDict name="SEARCH_ACROSS_CLASSES" description="allow checking an
attribute across classes ">
<Property name="ENABLE">true</Property>
</PropertyDict>
```

指定复制等待时间

在包括主从 LDAP 目录之间复制的部署中，您可以配置与从属目录进行通信的 SiteMinder 策略服务器。 在此配置中，策略服务器自动检测在向 LDAP 目录写入数据的操作期间指向该主目录的推荐。数据存储在主 LDAP 目录中，并且根据您的网络资源的复制方案被复制到从属 LDAP 目录。

在此配置中，当您在 CA Identity Manager 中创建对象时，系统将在主目录中创建对象，并将其复制到从属目录。 在复制流程中可能发生延迟，这会导致 CA Identity Manager 中的创建操作失败。

要防止此问题发生，您可以在 REPLICATION_WAIT_TIME 属性中指定 CA Identity Manager 在“超时”之前等待的时间（以秒为单位）。

遵循这些步骤:

1. 在目录配置文件 (directory.xml) 中，找到描述用户对象的 ImsManagedObject 元素。
2. 添加下列 PropertyDict 元素：

```
<PropertyDict name="REPLICATION_WAIT_TIME" description="time delay in
seconds for LDAP provider to allow replication to propagate from master to
slave">
<Property name=REPLICATION_WAIT_TIME"><time in seconds></Property>
</PropertyDict>
```

注意：PropertyDict 元素必须是 ImsManagedObject 元素的末元素，如下例所示：

```
<ImsManagedObject name="User" description="My Users"
objectclass="top,person,organizationalperson,inetorgperson,customClass"
objecttype="USER">
<ImsManagedObjectAttr physicalname="departmentnumber"
displayname="Department" description="Department" valuetype="String"
required="true" multivalued="false" maxlength="0" />
.
.
.
<PropertyDict name="REPLICATION_WAIT_TIME" description="time delay in
seconds for LDAP provider to allow replication to propagate from master to
slave">
<Property name=REPLICATION_WAIT_TIME">800</Property>
</PropertyDict>
```

如果没有定义复制等待时间，使用默认值 0。

指定 LDAP 连接设置

要改善性能，您可以在目录配置文件 (directory.xml) 中指定以下参数：

连接超时

指定 CA Identity Manager 在终止搜索之前搜索目录的最大毫秒数。

如下所示在目录配置文件中指定此属性：

com.sun.jndi.ldap.connect.timeout

连接池最大大小

指定 CA Identity Manager 可以建立对 LDAP 目录的连接的最大数目。

如下所示在目录配置文件中指定此属性：

com.sun.jndi.ldap.connect.pool.maxsize

连接池默认大小

指定 CA Identity Manager 和 LDAP 目录之间的连接的默认数目。

如下所示在目录配置文件中指定此属性：

com.sun.jndi.ldap.connect.pool.prefsize

遵循这些步骤:

1. 在目录配置文件 (directory.xml) 中，找到描述用户对象的 ImsManagedObject 元素。
2. 添加下列 PropertyDict 元素：

```
<PropertyDict name="LDAP_CONNECTION_SETTINGS" description="LDAP Connection Settings">
    <Property name="com.sun.jndi.ldap.connect.timeout">5000</Property>
    <Property name="com.sun.jndi.ldap.connect.pool.maxsize">200</Property>
    <Property name="com.sun.jndi.ldap.connect.pool.prefsize">10</Property>
</PropertyDict>
```

3. 保存 directory.xml 文件。

   在您使用此文件创建 CA Identity Manager 目录时，CA Identity Manager 会配置这些设置。

如何改善目录搜索性能

要改善用户、组织和组目录搜索的性能，请执行以下操作：

- 检索管理员可以在搜索查询中指定的属性。

  注意：对于 Oracle Internet 目录，如果在搜索查询中没有检索到属性，搜索可能失败。

- 配置页面大小和最大行设置 (p. 83)，以确定 CA Identity Manager 处理大规模搜索的方式。
- 调整用户目录。 请参阅您正在使用的用户目录的文档。

如何改善大规模搜索的性能

在 CA Identity Manager 管理大规模用户存储时，返回许多结果的搜索可能导致系统内存不足。 为防止内存问题，您可以定义大规模搜索的限制。

下列二个设置可以确定 CA Identity Manager 处理大规模搜索的方式：

- 最大行数

  指定搜索用户目录时 CA Identity Manager 可以返回的结果的最大数目。 在结果的数目超过限制时，显示错误。

- 页面大小

  指定在一次搜索中可以返回的对象数目。 如果对象的数目超过页面大小，CA Identity Manager 将执行多个搜索。

  在指定页面大小时，注意下列几点：

  - 要使用“搜索页大小”选项，CA Identity Manager 管理的用户存储必须支持分页。 一些用户存储类型需要其他配置才可支持分页。 有关详细信息，请参阅以下主题：

    配置 Sun Java 系统目录服务器分页支持 (p. 84)

    配置 Active Directory 分页支持

  - 如果用户存储不支持分页，并且指定了最大行的值，则 CA Identity Manager 仅使用最大行值来控制搜索大小。

您可以在以下位置配置最大行限制和页面大小：

- 用户存储

  在大多数用户存储和数据库中，您可以配置搜索限制。

  注意：有关详细信息，请参阅您正在使用的用户存储或数据库的文档。

- CA Identity Manager 目录

  您可以在您用来创建 CA Identity Manager 目录的目录配置文件 (directory.xml) 中配置 DirectorySearch 元素 (p. 52)。

  默认情况下，最大行数和页面大小的值对于现有目录是无限的。 对于新目录，最大行数的值是无限的，页面大小的值是 2000。

- 管理对象定义

  要设置适用于一种对象类型而不是整个目录的最大行数限制和页面大小，请在用来创建 CA Identity Manager 目录的 directory.xml 文件中配置*管理对象定义* (p. 53)。

  通过为管理对象类型设置限制，可以基于业务要求进行调整。 例如，大多数公司所具有的用户比组多。 这些公司只能为用户对象搜索设置限制。

- 任务搜索屏幕

  您可以控制用户在用户控制台的搜索和列表屏幕中看到的搜索结果的数目。如果结果的数目超过为任务定义的每页结果数，用户会看到其他结果页面的链接。

  此设置不影响搜索返回的结果的数目。

  注意：有关在搜索和列表屏幕中设置页面大小的信息，请参阅*《管理指南》*。

如果在多个位置定义了最大行限制和页面大小，将应用最适合的设置。 例如，管理对象设置优先于目录级别设置。

配置 Sun Java 系统目录服务器分页支持

Sun Java 系统目录服务器支持虚拟列表视图 (VLV)，此方法以特定顺序或在特定子集中发送搜索结果。 此方法与 CA Identity Manager 原本使用的简单分页结果不同。

要使用 VLV，您要设置权限并且创建索引。 CA Identity Manager 包括您必须配置分页支持的下列文件：

- vlvcntrl.ldif
- vlvindex.ldif
- runvlvindex.cmd、runvlvindex.sh

这些文件是 NeteAuto 示例的一部分（位于管理工具中的 samples\NeteAuto）。

管理工具安装于以下默认位置：

Windows：C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager

UNIX：/opt/CA/IdentityManager/IAM_Suite/Identity_Manager/

遵循这些步骤:

1. 将以下参数添加到 CA Identity Manager 目录的 directory.xml 文件的 DirectorySearch 元素 (p. 52)中，如下所示：

   ```
   minsortrules="1"
   ```

   注意：如果您正在修改现有的 CA Identity Manager 目录，请参阅"如何更新 CA Identity Manager 目录" (p. 155)。

2. 如下所示，设置 vlvcntrl.ldif 文件的权限：
   ```
   ldapmodify -D "cn=Directory Manager" -w password -p port -f
   vlvcntrl.ldif
   ```

3. 如下所示，导入 VLV 搜索和索引定义：
   ```
   ldapmodify -D "cn=Directory Manager" -w password -p port -f
   vlvindex.ldif
   ```

4. 如下所示，阻止该目录：
   ```
   stop-slapd
   ```

5. 使用 runvlvindex 来建立索引。

6. 如下所示，启动该目录：
   ```
   start-slapd
   ```

配置 Active Directory 分页支持

要在 Active Directory 配置分页支持，完成以下高级步骤：

- 为虚拟列表视图配置支持 (p. 85)。
- 为 Active Directory 配置 MaxPageSize (p. 86)。（**仅针对在 CA Identity Manager r12.5 SP7 之前创建的目录**）

配置对虚拟列表视图 (VLV) 的支持

Active Directory 支持虚拟列表视图 (VLV)，此方法将以特定的顺序或在特定子集中提供搜索结果。此方法与 CA Identity Manager 原本使用的简单分页结果不同。

要使用 VLV，您要设置权限并且创建索引。CA Identity Manager 包括您必须配置分页支持的下列文件：

- vlvcntrl.ldif
- vlvindex.ldif
- runvlvindex.cmd、runvlvindex.sh

这些文件是 NeteAuto 示例的一部分（位于管理工具中的 samples\NeteAuto）。

管理工具安装于以下默认位置：

Windows：C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager

UNIX：/opt/CA/IdentityManager/IAM_Suite/Identity_Manager/

遵循这些步骤：

1. 将以下参数添加到 CA Identity Manager 目录的 directory.xml 文件的 DirectorySearch 元素 (p. 52)中，如下所示：

   ```
   minsortrules="1"
   ```

   注意：如果您正在修改现有的 CA Identity Manager 目录，请参阅"如何更新 CA Identity Manager 目录" (p. 155)。

2. 如下所示，设置 vlvcntrl.ldif 文件的权限：
   ```
   ldapmodify -D "cn=Directory Manager" -w password -p port -f
   vlvcntrl.ldif
   ```

3. 如下所示，导入 VLV 搜索和索引定义：
   ```
   ldapmodify -D "cn=Directory Manager" -w password -p port -f
   vlvindex.ldif
   ```

4. 如下所示，阻止该目录：
   ```
   stop-slapd
   ```

5. 使用 runvlvindex 来建立索引。

6. 如下所示，启动该目录：
   ```
   start-slapd
   ```

配置 Active Directory MaxPageSize

Active Directory 使用 1000 作为默认 MaxPageSize。 假定 directory.xml 的 maxpagesize 属性值大于或等于 1000。 在这种情况下，如果搜索结果的数目超过 directory.xml 的 maxrows 值时，CA Identity Manager 将无法显示警告。 这样，执行搜索的管理员就不知道忽略了一些搜索结果。

为防止此问题，请确认目录以及每个管理对象的 maxpagesize 属性值小于 Active Directory MaxPageSize。

假定您使用随 CA Identity Manager 12.5 SP7 或更高版本安装的模板 directory.xml 文件创建 CA Identity Manager 目录。 在这种情况下，您不需要为分页支持执行任何其他步骤。 directory.xml 中的 maxpagesize 属性是默认设置的。

如果您将分页支持添加到现有的 CA Identity Manager 目录中，directory.xml 中的 maxpagesize 属性必须小于 1000。

此外，如果 Active Directory MaxPageSize 是 1000，确保为 CA Identity Manager 目录和所有管理对象适当设置 maxpagesize 属性。

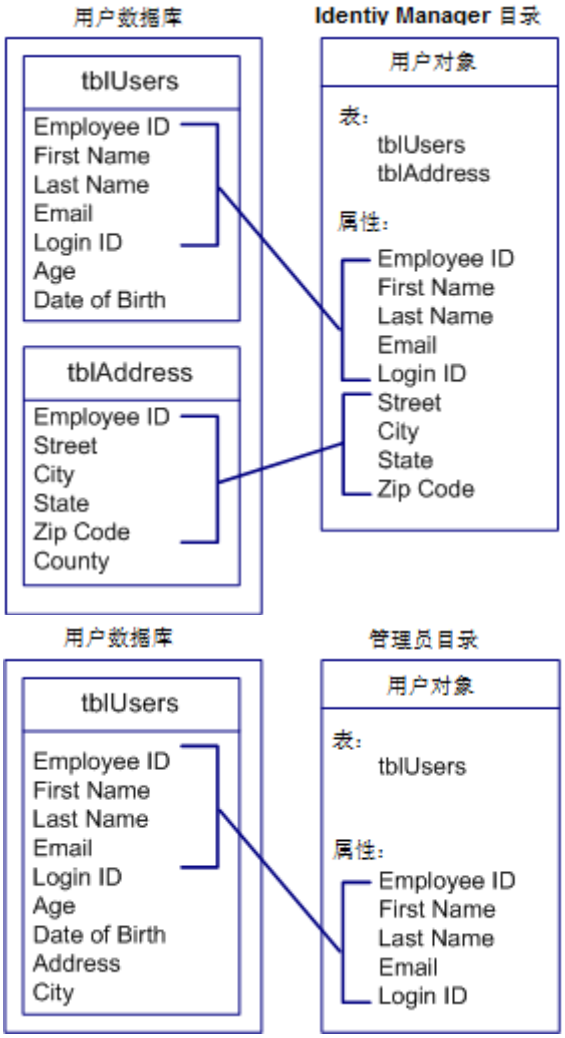
第 4 章： 关系数据库管理

此部分包含以下主题：

CA Identity Manager 目录

*CA Identity Manager 目录*描述怎样将用户、组等对象及组织（可选）存储在用户存储中，并描述在 CA Identity Manager 中表示它们的方式。 CA Identity Manager 目录与一个或多个 CA Identity Manager 环境相关联。

下图显示了 CA Identity Manager 目录与用户存储关联的方式：



注意：数据库的一些用户属性不是 CA Identity Manager 目录的一部分。 因此，CA Identity Manager 不管理它们。

为关系数据库配置 CA Identity Manager 时的重要提示

在配置 CA Identity Manager 以管理关系数据库之前，确保数据库符合以下要求：

- 必须可以通过 JDBC 驱动程序或开放式数据库连接 (ODBC) 驱动程序访问数据库（在 CA Identity Manager 与 SiteMinder 集成时）。 驱动程序必须支持外联结。 如果使用超过两张表表示管理对象，驱动程序也必须支持嵌套的外联结。

  注意：如果驱动程序不支持外联结，查询数据库时 CA Identity Manager 使用内联结。 这可能导致意外查询结果。

- 唯一标识 CA Identity Manager 管理的每个对象，如用户、组或组织（如果支持）。 例如，用户的唯一标识符可能是登录 ID。

  注意：确保唯一标识符存储在一列中。

- CA Identity Manager 需要一些多值属性，这些属性能够作为分隔列表存储在单独的表的单个单元或多行中。 例如，下列 tblGroupMembers 表存储组的成员：

ID	成员
研究	dmason
研究	rsavory
营销	dmason
营销	awelch

  ID 列包含组的唯一标识符，成员列包含该组的成员的唯一标识符。 例如，dmason 和 rsavory 是研究组的成员。 向该组添加新成员时，会将其他行添加到 tblGroupMembers。

- 当您的环境包括组织时，请执行下列任务：
  - 针对数据库编辑并且运行 CA Identity Manager 随附的 SQL 脚本，以配置组织支持 (p. 126)。
  - CA Identity Manager 需要名为“根”的顶级组织。 所有其他组织与根组织相关。

    有关组织要求的详细信息，请参阅“组织管理” (p. 126)。

创建 WebSphere 的 Oracle 数据源

遵循这些步骤:

1. 在 WebSphere 管理控制台中，导航到您配置 JDBC 驱动程序时创建的 JDBC 提供程序。
2. 使用下列属性创建数据源，然后单击“应用”：

   名称：用户存储数据源

   JNDI 名称：userstore

   URL：jdbc:oracle:thin:@*db_systemname*:1521:*oracle_sid*

3. 为用户存储数据源配置新的 J2C 身份验证数据条目：
   a. 输入以下属性：

      别名：用户存储

      用户 ID：*username*

      密码：*password*

      其中，*username* 和 *password* 是创建数据库时为帐户指定的用户名和密码。

   b. 单击“确定”，然后使用屏幕顶端的导航链接返回您正在创建的数据源。
4. 选择您通过以下字段的列表框创建的用户存储 J2C 身份验证数据条目：
   - 组件管理身份验证别名
   - “Container-managed Authentication Alias”（容器管理身份验证别名）
5. 单击“确定”，然后保存配置。

   注意：要确认正确配置了数据源，在数据源的配置屏幕中单击“测试连接”。如果测试连接失败，重新启动 WebSphere 并且再次测试连接。

如何创建 CA Identity Manager 目录

遵循这些步骤:

1. 如果您使用 SiteMinder，在创建 CA Identity Manager 目录之前应用策略存储架构。

   注意：有关特定策略存储架构及其应用方式的详细信息，请参阅*《安装指南》*。
2. 如果您正在使用 SiteMinder，创建用于 SiteMinder 的 ODBC 数据源 (p. 96)。
3. 为 CA Identity Manager 管理的用户数据库创建数据源。
4. 通过修改目录配置文件 (directory.xml)，将数据库描述到 CA Identity Manager。 有关详细信息，请参阅“如何在目录配置文件中描述数据库”。
5. 在管理控制台中，导入目录配置文件并且创建该目录。

如何创建 JDBC 数据源

CA Identity Manager 需要在安装 CA Identity Manager 的应用程序服务器中包含 JDBC 数据源，以连接到用户存储。 对于每个应用程序服务器，创建数据源的说明不同。

为 JBoss 应用程序服务器创建 JDBC 数据源

遵循这些步骤:

1. 创建以下文件的副本：

   jboss_home\server\default\deploy\objectstore-ds.xml

   jboss home

   安装 CA Identity Manager 的 Jboss 应用程序服务器的安装位置。

   新文件必须位于同样位置。

2. 将文件重命名为 userstore-ds.xml。

3. 编辑 userstore-ds.xml，如下所示：

   a. 找到 <jndi-name> 元素。

   b. 将 <jndi-name> 元素的值从 jdbc/objectstore 更改为 userstore，如下所示：

      <jndi-name>userstore</jndi-name>

   c. 在 <connection-url> 元素中，将 DatabaseName 参数更改为作为用户存储的数据库的名称，如下所示：

      <connection-url>

      jdbc:sqlserver://*ipaddress:port*;selectMethod=cursor;DatabaseName=*userstore_name*

      </connection-url>

      ipaddress

      指定安装用户存储的计算机的 IP 地址。

      port

      指定数据库的端口号。

      userstore_name

      指定作为用户存储的数据库的名称。

4. 如果您计划创建支持 FIPS 所必需的 JBoss 安全领域，执行下列步骤：
   a. 将安全域重命名为 <security-domain>imuserstoredb</security-domain>。
   b. 保存文件。
   c. 忽略剩余的步骤。而是完成"创建 JDBC 数据源的 JBoss 安全领域" (p. 93)中的步骤。
5. 如下所示对 userstore-ds.xml 进行其他更改：
   a. 将 <user-name> 元素的值更改为对用户存储具有读和写访问权限的帐户的用户名。
   b. 将 <password> 元素的值更改为在 <user-name> 元素中指定的帐户的密码。

   注意：用户名和密码在此文件的明文显示。因此，您可能希望创建 JBoss 安全领域，而不是编辑 userstore-ds.xml。
6. 保存文件。

使用 JDBC 数据源的 JBoss 安全领域

确保您在 JBoss 应用程序服务器中创建 JDBC 数据源。 您可以配置数据源，以使用用户名和密码，或者可以配置它以使用安全领域。

重要说明！ 如果使用 FIPS，确保使用“JBoss 安全领域”选项。

遵循这些步骤:

1. 完成“创建 JBoss 应用程序服务器的 JDBC 数据源” (p. 91)中的步骤。

   不要如第 4 步中所述在 userstore-ds.xml 中指定用户名和密码。

2. 在 *jboss_home*\server\default\conf 中打开 login-cfg.xml。

3. 在文件中找到以下条目：

```
<application-policy name="imobjectstoredb">
  <authentication>
    <login-module
code="com.netegrity.jboss.datasource.PasswordEncryptedLogin"
flag="required">
      <module-option name="userName">fwadmin</module-option>
      <module-option
name="password">{PBES}:gSex2/BhDGzEKWvFmzca4w==</module-option>
      <module-option
name="managedConnectionFactoryName">jboss.jca:name=jdbc/objectstore,servi
ce=NoTxCM</module-option>
    </login-module>
  </authentication>
</application-policy>
```

4. 复制完整条目，并将它粘贴在 login-cfg.xml 文件中的 <policy> 和 </policy> 标记之间。

5. 在粘贴到文件中的条目中，进行以下更改：

   a. 将名称属性值从 imobjectstoredb 更改为 imuserstoredb，如下所示：

   ```
   <application-policy name="imuserstoredb">
   ```

   b. 指定用来针对用户存储进行身份验证的用户名称，如下所示：

   ```
   <module-option name="userName">user_store_user</module-option>
   ```

   c. 为前一步骤中的用户指定密码，如下所示：

   ```
   <module-option
   name="password">user_store_user_password</module-option>
   ```

   注意：要加密用户存储密码，请使用随 CA Identity Manager 安装的密码工具 (pwdtools)。

   d. 在 <module-option name="managedConnectionFactoryName"> 元素中，提供正确的 jdbc.jca:name，如下所示：

   ```
   <module-option name="managedConnectionFactoryName">
      jboss.jca:name=userstore,service=NoTxCM
   </module-option>
   ```

6. 保存文件。
7. 重新启动应用程序服务器。

为 WebLogic 创建 JDBC 数据源

在 WebLogic 管理控制台中创建数据源。

注意：有关 WebLogic 连接池的完整信息，请参阅《Oracle WebLogic 11 Documentation》。

遵循这些步骤:

1. 在 WebLogic 管理控制台中使用下列参数创建 JDBC 数据源：

   名称：用户存储数据源

   JNDI 名称：userstore

2. 使用下列信息为数据源创建连接池：

   - 对于 SQL Server 2005 数据库，使用以下值：

     URL：jdbc:sqlserver://*db_systemName*:1433

     驱动程序类名称：com.microsoft.sqlserver.jdbc.SQLServerDriver

     属性：user=*username*

     databaseName=*user store name*

     selectMethod=cursor

     密码：*password*

   - 对于 Oracle 数据库，使用以下值：

     URL：jdbc:oracle:thin:@*tp_db_systemname*:1521:*oracle_SID*

     驱动程序类名称：oracle.jdbc.driver.OracleDriver

     属性：user=*username*

     密码：*password*

3. 在配置之后，将池的目标设置为服务器实例 *wl_server_name*。

   在部署池之后，检查控制台，查看是否有任何错误发生。

   注意：您可能看到指明无法使用不存在的池创建数据源的错误。 要解决此错误，请重新启动 WebLogic。

WebSphere 数据源

以下部分描述如何为 WebSphere 应用程序服务器创建 SQL 或 Oracle 数据源。

为 WebSphere 创建 SQL Server 数据源

遵循这些步骤:

1. 在 WebSphere 管理控制台中，导航到您配置 JDBC 驱动程序时创建的 JDBC 提供程序。
2. 在“Additional Properties”（其他属性）部分选择“Data Sources”（数据源）。
3. 使用下列属性创建数据源，然后单击“Apply”（应用）：

   名称：用户存储数据源

   JNDI 名称：userstore

   databaseName：*userstore_name*

   serverName：*db_systemname*
4. 如下所示配置 selectMethod 属性：
   a. 在“Additional Properties”（其他属性）部分中选择“Custom Properties”（自定义属性）。
   b. 单击 selectMethod 自定义属性。
   c. 在“Value”（值）字段中输入以下文本：

      cursor
   d. 单击“OK”（确定），然后使用屏幕顶端的导航链接返回您正在创建的数据源。
5. 为用户存储数据源配置新的 J2C 身份验证数据条目：
   a. 从“相关项”部分中选择 J2EE 连接器体系结构 (J2C) 身份验证数据条目。
   b. 单击“新建”。
   c. 输入以下属性：

      别名：用户存储

      用户 ID：*username*

      密码：*password*

      其中，*username* 和 *password* 是创建数据库时为帐户指定的用户名和密码。
   d. 单击“确定”，然后使用屏幕顶端的导航链接返回您正在创建的数据源。
6. 选择您在“Component-managed Authentication Alias”（组件管理身份验证别名）字段的列表框中创建的用户存储 J2C 身份验证数据条目。
7. 单击“OK”（确定），然后保存配置。

   注意：要确认正确配置了数据源，在数据源的配置屏幕中单击“Test Connection”（测试连接）。 如果测试连接失败，重新启动 WebSphere 并且再次测试连接。

创建 WebSphere 的 Oracle 数据源

遵循这些步骤:

1. 在 WebSphere 管理控制台中，导航到您配置 JDBC 驱动程序时创建的 JDBC 提供程序。
2. 使用下列属性创建数据源，然后单击“应用”：

   名称：用户存储数据源

   JNDI 名称：userstore

   URL：jdbc:oracle:thin:@*db_systemname*:1521:*oracle_sid*
3. 为用户存储数据源配置新的 J2C 身份验证数据条目：
   a. 输入以下属性：

      别名：用户存储

      用户 ID：*username*

      密码：*password*

      其中，*username* 和 *password* 是创建数据库时为帐户指定的用户名和密码。

   b. 单击“确定”，然后使用屏幕顶端的导航链接返回您正在创建的数据源。
4. 选择您通过以下字段的列表框创建的用户存储 J2C 身份验证数据条目：
   - 组件管理身份验证别名
   - “Container-managed Authentication Alias”（容器管理身份验证别名）
5. 单击“确定”，然后保存配置。

   注意：要确认正确配置了数据源，在数据源的配置屏幕中单击“测试连接”。如果测试连接失败，重新启动 WebSphere 并且再次测试连接。

如何创建用于 SiteMinder 的 ODBC 数据源

如果 CA Identity Manager 与 SiteMinder 集成，在 SiteMinder 计算机上定义指向该数据库的 ODBC 数据源。 记下数据源的名称以备之后使用。 处理方式如下：

- **Windows：**将 ODBC 数据源配置成系统 DN。 有关说明，请参阅 Windows 操作系统文档。
- **UNIX：**在 *policy_server_installation*/db 的 system_odbc.ini 文件中添加条目，指定 ODBC 数据源的参数。

如何在目录配置文件中描述数据库

为了管理数据库，CA Identity Manager 必须理解数据库结构和内容。 要向 CA Identity Manager 描述数据库，请创建目录配置文件 (directory.xml)。

目录配置文件包含以下部分中的一个或多个：

CA Identity Manager 目录信息

包含 CA Identity Manager 使用的 CA Identity Manager 目录的有关信息。

属性验证

定义适用于 CA Identity Manager 目录的验证规则。

提供商信息

描述 CA Identity Manager 管理的用户存储。

目录搜索信息

支持您指定 CA Identity Manager 搜索用户存储的方式。

用户对象 (p. 99)

说明用户在用户存储中的存储方式及其在 CA Identity Manager 中的表示方式。

组对象 (p. 99)

说明组在用户存储中的存储方式及其在 CA Identity Manager 中的表示方式。

组织对象 (p. 99)

描述存储组织的方式，以及在 CA Identity Manager 中表示组织的方式。

自行订阅组

为自助服务用户可加入的组配置支持。

您安装 CA Identity Manager 管理工具的目录包括关系数据库的以下目录配置文件模板：

admin_tools\directoryTemplates\RelationalDatabase\directory.xml

管理工具

定义 CA Identity Manager 管理工具的安装位置，如下例中所示：

- **Windows**：C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools
- **UNIX**：/opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

注意：在 directoryTemplates\RelationalDatabase 中为支持组织的环境配置了目录配置文件模板。 要查看针对不包括组织的环境的目录配置文件，您可以参阅 NeteAuto 示例的 directory.xml 文件，该文件位于 *admin_tools*\samples\NeteAutoRDB\NoOrganization。

将配置模板复制到新目录，或使用不同名称将其保存，以防覆盖配置模板。 您然后可以修改模板来反映数据库结构。

目录配置文件有两个重要的约定：

- ##－表示必需值。

  要提供所有必要的信息，请找到所有的磅字符 (##) 并且将它们替换成适当值。 例如，##PASSWORD_HINT 表示，您必须提供属性以存储用户回答的问题，以便用户在忘记密码的情况下收到临时的密码。

- @－表示 CA Identity Manager 填充的值。 请勿修改目录配置文件中的这些值。 导入目录配置文件时，CA Identity Manager 会提示您提供相应的值。

在修改目录配置文件之前，需要以下信息：

- 用户、组和组织对象的表名（如果您的结构包括组织）。
- 用户、组和组织配置文件的属性列表（如果您的结构包括组织）。

修改目录配置文件

执行以下程序，以便修改目录配置文件。

遵循这些步骤:

1. 配置与数据库的连接。
2. 指定 CA Identity Manager 在终止搜索之前搜索目录的时间长度。
3. 定义 CA Identity Manager 管理的用户和组管理对象 (p. 99)。
4. 修改常用属性。

   在 CA Identity Manager 中，常用属性可标识特殊属性，如密码属性。
5. 为自行订阅组配置支持。
6. 如果您的环境包括组织，则配置组织支持。

更多信息：

管理对象说明 (p. 99)
组织管理 (p. 126)
如何配置自行订阅组 (p. 125)
关系数据库的常用属性 (p. 120)

管理对象说明

在 CA Identity Manager 中，您管理与用户存储的条目对应的以下各种类型的对象：

- 用户－表示企业中的用户。
- 组－表示有共同特征的用户的集合。
- （可选）组织－表示业务单元。 组织可以包含用户、组和其他组织。

  注意："组织管理" (p. 126)提供有关配置组织的信息。

对象说明包含以下信息：

- 对象相关信息 (p. 99)，如存储对象的表。
- 存储条目相关信息的属性 (p. 103)。 例如，寻呼机属性存储寻呼机号码。

重要说明！ CA Identity Manager 环境仅支持一种用户、组和组织对象。

如何描述管理对象

通过在目录配置文件的"用户对象"、"组对象"和"组织对象"（如果数据库包括组织）部分中指定对象信息可以描述管理对象。

每一个部分包含 ImsManagedObject 元素，如下列代码：

```
<ImsManagedObject name="User" description="My Users">
```

ImsManagedObject 元素可能包括以下元素：

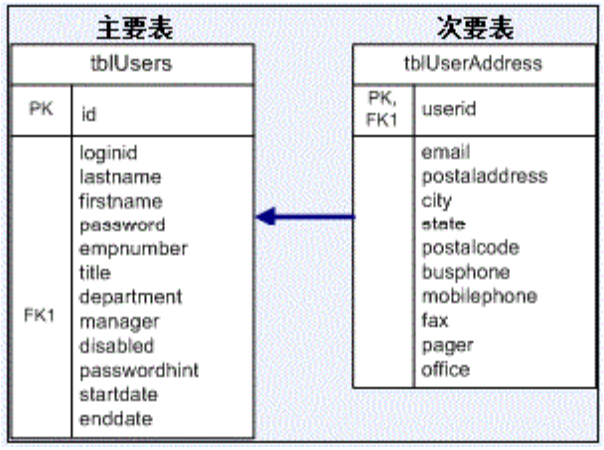
- Table（必需）
- UniqueIdentifier（必需）
- ImsManagedObjectAttr（必需）
- RootOrg（仅针对组织对象）

数据库表

在目录配置文件中使用表元素，来定义存储管理对象相关信息的表。

每个管理对象必须有一个包含对象唯一标识符的主表。 附加信息可能存储在次表中。

下图显示将用户信息存储在主表和次表中的数据库：



如果对象的信息存储在多个表中，为每张表创建表元素。 在次表的表元素中使用参考元素来定义它与主表的关系。

例如，如果用户相关基本数据存储在 tblUsers 中，地址信息存储在 tblUserAddress 中，用户管理对象的表定义将与以下条目类似：

```
<Table name="tblUsers" primary="true" />
<Table name="tblUserAddress">
  <Reference childcol="userid" primarycol="id" />
</Table name>
```

表元素

表元素的参数如下所示：

name

（必需）

指定存储对象的管理配置文件的部分或全部属性的表的名称。

primary

表明表是否是管理对象的主表。 主表包含对象的唯一标识符，如下所示：

- True－表是主表。
- False－表是次表（默认）。

如果您不指定主参数，CA Identity Manager 将此表作为次表。

注意：只能有一个表是主表。

filter

标识适用于管理对象的表项目的子集。

可选的筛选器参数如下例所示：

```
filter="ORG=2"
```

注意：筛选器仅适用于 CA Identity Manager 生成的查询。 如果您使用自定义查询覆盖生成的查询，在“自定义查询”中指定筛选器。

fullouterjoin

指出外联结是否是完全外联结。

- True－外联结是完全外联结。在这种情况下，在已返回行的联结的两个表中可以找到返回有效行所需的条件。
- False－外联结是相对于主表的左侧外联结。 在这种情况下，只有查询中的一个表的行必须满足此条件（默认）。

注意：参数是可选的，除非另外指定。

表参数可以包含一个或多个参考元素以使主表和次表链接。

参考元素

参考元素中的参数如下所示：

childcol

表示映射到主表列的次表的列（在相应的表元素中指定）。

primarycol

表示映射到次表的列的主表的列。

注意：参数是可选的，除非另外指定。

指定对象信息

通过提供各种参数的值来指定对象信息。

遵循这些步骤:

1. 在“用户对象”、“组对象”或“组织对象”部分中找到 ImsManagedObject 元素。
2. 提供以下参数的值：

   name

   （必需）

   提供管理对象的唯一名称。

   description

   提供管理对象的说明。

objecttype

（必需）

指定管理对象的类型。 有效值如下所示：

- USER
- GROUP
- ORGANIZATION

ImsManagedObject 元素必须类似以下代码：

```
<ImsManagedObject name="User" description="My  Users" objecttype="USER">
```

3. 提供表信息，如“数据库表” (p. 99)中所述。
4. 指定包含对象唯一标识符 (p. 102)的列。
5. 描述构成对象的配置文件的属性 (p. 103)。
6. 如果您要配置组织对象，转到组织管理 (p. 126)。

如何为管理对象指定唯一标识符

CA Identity Manager 管理的每个对象必须有唯一标识符。确保唯一标识符存储在管理对象的主表的一列中。 在数据库表 (p. 99)中描述主表。

使用 UniqueIdentifier 和 UniqueIdentifierAttr 元素定义唯一标识符，如下所示：

```
<UniqueIdentifier>
  <UniqueIdentifierAttr name="tablename.columnname" />
</UniqueIdentifier>
```

UniqueIdentifierAttr 元素需要名称参数。 名称参数的值是存储唯一标识符的属性。 值可以是物理属性或常用属性 (p. 69)。

如果指定物理属性，注意下列几点：

- 确保指定的属性位于数据库中，且已经在目录配置文件中定义，如“如何修改属性说明” (p. 103)所述。 在属性说明中，确保指定只读或写一次权限，以防止在会话期间更改唯一标识符。
- 使用以下语法来指定物理属性：

  tablename.columnname

  tablename

  定义属性所在的表的名称。 您指定的表必须是主表。

  columnname

  定义存储属性的列的名称。
- 如果数据库生成唯一标识符，为属性指定自定义操作 (p. 112)。 例如，您可能必须指定从数据库提取最后生成的标识符的操作。

如何修改属性说明

属性存储用户、组或组织实体相关信息，如电话号码或地址。 实体的属性确定其配置文件。

在目录配置文件的 ImsManagedObjectAttr 元素中，对属性进行了说明。 在目录配置文件的“用户对象”、“组对象”或“组织对象”部分中，您可以执行以下操作：

- 修改默认属性说明来描述您的数据库属性。
- 通过复制现有说明并根据需要修改值，来创建新的属性说明。

在用户、组和组织配置文件中每个属性有一个 ImsManagedObjectAttr 元素。 例如，ImsManagedObjectAttr 元素可能描述用户 ID。

ImsManagedObjectAttr 元素类似以下内容：

```
<ImsManagedObjectAttr
 physicalname="tblUsers.id"
 displayname="User Internal ID"
 description="User Internal ID"
 valuetype="Number"
 required="false"
 multivalued="false"
 maxlength="0"
 hidden="false"
 permission="READONLY">
```

注意：如果您在使用 Oracle 数据库，在配置管理对象属性时，注意以下内容：

- Oracle 数据库在默认情况下是区分大小写的。 目录配置文件的属性和表名的大小写必须与 Oracle 中的属性大小写匹配。

  确保为字符串 datatypes 指定最大长度，防止截断。 要限制字符串的长度，您可以创建验证规则，以在用户输入的字符串超过最大长度的时候，显示错误。

ImsManagedObjectAttr 参数如下所示：

注意：参数是可选的，除非另外指定。

physicalname

（必需）

指定属性的物理名，它必须包含以下内容之一：

- 名称以及存储该值的位置。

  格式：*tablename.columnname*

  例如，如果属性存储在 tblUsers 表的 id 列中，该属性的物理名如下所示：

  tblUsers.id

  您必须在“表元素” (p. 99)中定义包含属性的每个表。

- 常用属性。

  常用属性可以表示计算的值。例如，您可以使用常用属性来引用自定义操作 (p. 112)计算的属性。

displayname

（必需）

指定属性的唯一名称。

在用户控制台中，显示名称会显示在可添加到任务屏幕的属性列表中。

注意：不要在目录配置文件 (directory.xml) 中修改属性的显示名称。 要更改任务屏幕上属性的名称，可以在任务屏幕定义中为属性指定标签。 有关详细信息，请参阅*《管理指南》*。

description

提供属性的说明。

valuetype

指定属性的数据类型。 有效值如下所示：

字符串

该值可以为任何字符串。

这是默认值。

整数

该值必须为整数。

注意：整数不支持十进制数。

数字

该值必须为整数。 数字选项支持十进制数。

日期

值必须解析为使用以下样式的有效日期：

MM/dd/yyyy

ISODate

值必须使用模式 yyyy - MM - dd 解析为有效日期

UnicenterDate

该值必须解析为使用 YYYYYYYDDD 样式的有效日期，其中：

YYYYYYY 是年的七位数表示，以三个 0 开始。 例如：0002008

DDD 是天的三位数表示，必要时以 0 开始。 有效值包括 001 到 366。

如果属性的值类型不正确，CA Identity Manager 查询可能失败。

要确保属性正确存储在数据库中，您可以使它与验证规则关联。

required

表示是否必须为属性指定值，如下所示：

- True－需要
- False－可选（默认）

multi-valued

表示属性是否可以有多个值，如下所示：

- True－属性可以有多个值。
- False－属性只能有一个值（默认）。

例如，用户配置文件的组成员资格属性是多值的，以存储用户所属的组。

要将多值属性存储在分隔列表中而不是存储在多行表中，您必须在分隔符参数中定义分隔符。

确保可能值的数目和列允许的每个值的长度是足够的。

重要说明！用户对象定义中的组成员资格属性必须是多值的。

wellknown

提供常用属性的名称。

常用属性在 CA Identity Manager 中具有特定含义。

格式：*%ATTRIBUTENAME%*

注意：在自定义操作与属性关联时，您必须指定一个常用属性 (p. 69)。

maxlength

确定列的最大大小。

permission

表示是否可以在任务屏幕中修改属性值，如下所示：

READONLY

值可以显示但无法修改

WRITEONCE

一旦创建了对象，便无法修改该值。例如，在创建用户之后，无法更改用户 ID

READWRITE

值可以修改（默认）

hidden

表示是否在 CA Identity Manager 任务屏幕中显示属性，如下所示：

- True－属性不向用户显示。
- False－属性向用户显示（默认）。

逻辑属性使用隐藏属性。

注意：有关逻辑属性的详细信息，请参阅《*Programming Guide for Java*》。

system

表示仅由 CA Identity Manager 使用的属性，并且用户不能在用户控制台中修改这些属性，如下所示：

- True－用户不可修改此属性。 在用户控制台中不会显示属性。
- False－用户可以修改此属性。可以添加到用户控制台中的任务屏幕（默认）。

validationruleset

将验证规则集与属性相关联。

必须在目录配置文件的 ValidationRuleSet 元素中定义您指定的验证规则集。

delimiter

定义在一列中存储多个值时分隔值的字符。

重要说明！ 要应用分隔符，必须将多值参数设置为“true”。

注意：要防止在用户控制台中显示敏感信息（如密码或工资），您可以指定 DataClassification (p. 63) 参数。

管理敏感属性

CA Identity Manager 提供了以下方法来管理敏感属性：

- 属性的数据分类

  数据分类允许您在目录配置文件 (directory.xml) 中指定属性的显示和加密属性。

  您可以定义管理敏感属性的数据分类，如下所示：

  - 在 CA Identity Manager 任务屏幕中，将属性的值显示为一串星号。

    例如，您可以将密码显示为星号，而不显示为明文。

  - 在“查看提交的任务”屏幕中，隐藏该属性值。

    此选项使您可以对管理员隐藏属性。例如，向在 CA Identity Manager 中查看任务状态但不需要查看工资详细信息的管理员隐藏工资详细信息（例如工资）。

- 在创建现有对象的副本时忽略某些属性。
- 加密属性

- 任务配置文件屏幕中的字段样式

  如果您不想在 directory.xml 文件中修改属性，可在显示敏感属性的屏幕定义中设置属性的显示属性。

  字段样式使您可以将密码等属性显示为一串星号，而不显示为明文。

  注意：有关敏感属性的字段样式的详细信息，请在用户控制台帮助中搜索字段样式。

数据分类属性

数据分类元素提供了一种方法，可以将附加属性与属性说明关联起来。 此元素中的值确定了 CA Identity Manager 处理属性的方式。 此元素支持以下参数：

- sensitive

  使 CA Identity Manager 在“查看提交的任务”屏幕中将该属性显示为一串星号 (*)。 此参数可防止属性的旧值和新值在“查看提交的任务”屏幕中显示为明文。

  另外，如果您在用户控制台中创建了现有用户的副本，此参数可防止属性被复制到新的用户。

- vst_hide

  在“查看提交的任务”选项卡的“事件详细信息”屏幕中隐藏属性。与显示为星号的敏感属性不同，vst_hidden 属性不会显示。

  您可以使用此参数来阻止在“查看提交的任务”中显示对工资等属性所做的更改。

- ignore_on_copy

  使 CA Identity Manager 在管理员于用户控制台中创建对象的副本时忽略某属性。 例如，假设您为用户对象的密码属性指定 ignore_on_copy。 在复制用户配置文件时，CA Identity Manager 不会将当前用户的密码应用于新的用户配置文件。

- AttributeLevelEncrypt

  在将属性值存储在用户存储中时对其加密。 如果 CA Identity Manager 启用了 FIPS 140-2，CA Identity Manager 使用 RC2 加密或 FIPS 140-2 加密。

  有关 CA Identity Manager 中对 FIPS 140-2 的支持的详细信息，请参阅*《配置指南》*。

  这类属性在运行时显示为明文。

  注意：为了防止属性在屏幕中以明文显示，您还可以为加密的属性添加敏感数据分类元素。 有关详细信息，请参阅"如何添加属性级别的加密" (p. 65)。

- PreviouslyEncrypted

  使 CA Identity Manager 在访问用户存储中的对象时检测和解密属性中任何加密的值。

  您可以使用此数据分类来解密任何先前加密的值。

  在您保存对象时，会将明文值保存在存储中。

用户控制台中的敏感属性

可能有一些属性（例如密码），不应以纯文本形式显示在用户控制台中。 目录配置文件包含了两个属性，您可以使用它们来隐藏敏感属性：

- sensitive

  此参数使 CA Identity Manager 将属性显示为一串星号 (*)。 它可用来防止密码以明文显示。

- vst_hidden

  此参数会在"查看提交的任务"选项卡的"事件详细信息"屏幕中隐藏属性。敏感属性会在"事件"选项卡的 ?? 部分 中显示为星号，与之不同，vst_hidden 属性不会显示。

  您可以使用此参数来防止对工资等属性所做的更改显示在用户控制台中。

在用户控制台中隐藏属性

1. 找到您要在目录配置文件中隐藏的属性。
2. 在属性说明之后，添加以下内容：

   <DataClassification name="*parameter*">

   parameter

   代表以下参数：

   sensitive

   vst_hidden

   例如，sensitive 参数的属性说明如下所示：

```
<ImsManagedObjectAttr physicalname="##PASSWORD_HINT" displayname="Password
Hint" description="Password Hint" valuetype="String" required="false"
multivalued="true" wellknown="%PASSWORD_HINT%" maxlength="0">
    <DataClassification name="sensitive"/>
```

   vst_hidden 属性的属性说明如下所示：

```
<ImsManagedObjectAttr physicalname="salery" displayname="Salary"
description="salary" valuetype="String" required="false"
multivalued="false" maxlength="0">
    <DataClassification name="vst_hidden"/>
```

属性级别的加密

您可以通过在目录配置文件 (directory.xml) 中指定属性的 AttributeLevelEncypt 数据分类来加密用户存储中的属性。 在启用了属性级别的加密时，CA Identity Manager 会在将属性的值存储在用户存储中之前将其加密。 该属性在用户控制台中以明文显示。

注意：为了防止属性在屏幕中以明文显示，您还可以为加密的属性添加敏感数据分类元素。 有关详细信息，请参阅“如何添加属性级别的加密” (p. 65)。

如果启用了 FIPS 140-2 支持，则会使用 RC2 加密或 FIPS 140-2 加密来加密该属性。

在实施属性级别的加密之前，请注意下列几点：

- CA Identity Manager 不能在搜索中找到加密的属性。

  假设将加密的属性添加到成员、管理员、所有者策略或身份策略。 由于 CA Identity Manager 无法搜索属性，所以不能正确地解析该策略。

  考虑在 directory.xml 文件中将属性设置为 searchable="false"，例如：

  <ImsManagedObjectAttr physicalname="title" description="Title" displayname="Title" valuetype="String" maxlength="0" searchable="false">

  <DataClassification name="AttributeLevelEncrypt"/>

  </ImsManagedObjectAttr>

- 如果 CA Identity Manager 使用共享用户存储和配给目录，请不要加密配给服务器属性。
- 不要在满足以下条件的环境中为用户密码启用 AttributeLevelEncrypt：
  - 包含了 CA SiteMinder 集成，
  - 并且在关系数据库中存储用户

  如果 CA Identity Manager 与 CA SiteMinder 集成，则在新的用户尝试进行登录并以明文输入密码时，加密的密码会引起问题。
- 如果您为 CA Identity Manager 之外的其他应用程序使用的用户存储启用了属性级别的加密，则其他应用程序将无法使用加密的属性。

如何添加属性级别的加密

假定您为 CA Identity Manager 目录添加了属性级别的加密。 在您保存与该属性关联的对象时，CA Identity Manager 会自动加密现有明文属性值。例如，加密密码属性会在保存用户的配置文件时加密密码。

注意：要加密属性值，您用来保存对象的任务必须包含该属性。 要加密上例中的密码属性，请确保将密码字段添加到了您用来保存对象的任务，例如“修改用户”任务。

在用户存储中，所有新的对象都会使用加密的值进行创建。

遵循这些步骤:

1. 完成以下任务之一：
   - 创建 CA Identity Manager 目录
   - 通过导出目录设置来更新现有目录。
2. 在 directory.xml 文件中将下列数据分类属性添加到您要加密的属性中：

   AttributeLevelEncrypt

   在用户存储中以加密形式保存属性值。

   sensitive（可选）

   在 CA Identity Manager 屏幕中隐藏属性值。 例如，密码显示为星号 (*)。

   例如：

```
<ImsManagedObjectAttr physicalname="salary"
displayname="Salary" description="salary" valuetype="String"
required="false" multivalued="false" maxlength="0"
searchable="false">
<DataClassification name="AttributeLevelEncrypt"/>
<DataClassification name="sensitive"/>
```

3. 如果已创建 CA Identity Manager 目录，请将该目录与环境关联。
4. 要强制 CA Identity Manager 立即加密所有值，请使用批量加载程序修改所有对象。

   注意：有关批量加载程序的详细信息，请参阅*《管理指南》*。

如何删除属性级别的加密

如果您的 CA Identity Manager 目录中具有加密的属性，并且该属性在存储时值为明文，则您可以删除 AttributeLevelEncrypt 数据分类。

在删除该数据分类后，CA Identity Manager 会停止加密新的属性值。在您保存与该属性关联的对象时，现有的值会被解密。

注意：要解密属性值，您用来保存对象的任务必须包含该属性。 例如，要解密现有用户的密码，您应使用包含密码字段的任务保存用户对象，例如“修改用户”任务。

要强制 CA Identity Manager 检测和解密保留在属性的用户存储中的任何加密值，您可以指定另一数据分类：PreviouslyEncrypted。 在您保存对象时，明文值会被保存到用户存储。

注意：添加 PreviouslyEncrypted 数据分类会为每一对象加载增加额外的处理任务。 为防止性能问题，请考虑在添加 PreviouslyEncrypted 数据分类时，加载和保存与该属性关联的每一对象，然后删除该数据分类。 这一方法会将所有存储的加密值自动转换为存储的明文。

遵循这些步骤:

1. 导出适当的 CA Identity Manager 目录的目录设置。
2. 在 directory.xml 文件中，从您想要解密的属性删除数据分类 AttributeLevelEncrypt。
3. 如果您要强制 CA Identity Manager 删除先前加密的值，请添加 PreviouslyEncrypted 数据分类属性。

   例如：

   ```
   <ImsManagedObjectAttr physicalname="salary" displayname="Salary"
   description="salary" valuetype="String" required="false"
   multivalued="false" maxlength="0" searchable="false">
   <DataClassification name="PreviouslyEncrypted"/>
   ```

4. 要强制 CA Identity Manager 立即解密所有值，请使用批量加载程序修改所有对象。

   注意：有关批量加载程序的详细信息，请参阅 *《管理指南》*。

自定义操作

您可以为特定管理对象定义自定义操作，以完成以下内容：

- 使用存储过程
- 优化数据库结构查询
- 检索数据库生成的唯一标识符

自定义操作仅适用于属性。

指定自定义操作时，请记住以下几点：

- 指定自定义操作的用户必须熟悉 SQL。
- CA Identity Manager 不验证自定义操作。直到运行时间才会报告语法错误和无效查询。
- 如果您为属性指定自定义操作，您无法在 CA Identity Manager 任务的搜索筛选中使用该属性。
- 自定义操作必须符合 XML 标准。使用 XML 语法表示特殊字符。例如，指定单引号 (') 作为 '

要指定自定义操作，请使用操作元素。

操作元素

操作元素定义 SQL 语句，该语句可以执行自定义查询，或调用存储过程，以创建、检索、修改或删除属性。操作元素是 IMSManagedObjectAttr 元素的子元素，如下例所示：

```
<ImsManagedObjectAttr physicalname="tblUsers.id" displayname="User Internal ID"
description="User Internal ID" valuetype="Number" required="false"
multivalued="false" maxlength="0" hidden="false" permission="READONLY">
  <Operation name="GetDb" value="select @@identity" />
```

操作元素参数如下所示：

name

指定操作的预定义名。 有效操作如下所示：

- 创建
- Get
- 设置
- 删除
- GetDB

  在通过数据库或从存储过程生成唯一标识符时，GetDB 操作在创建任务期间从数据库检索唯一标识符。

value

定义要执行的 SQL 语句或存储过程。 有效值如下所示：

- INSERT
- SELECT
- UPDATE
- DELETE
- CALL（针对存储过程）

注意：参数是可选的，除非另外指定。

操作元素可以包含一个或多个参数元素。

参数元素

参数元素指定发送到查询的值。 在定义多个参数元素时，会将值按照给定列出顺序发送到该查询。

参数元素需要名称参数。 名称参数的值可以是物理属性或常用属性 (p. 69)。

注意：CA Identity Manager 必须理解发送到参数元素的查询的值。例如，值可能是在 ImsManagedObjectAttr 属性中定义的物理名或常用属性。

如果指定物理属性，注意下列几点：

- 使用以下语法来指定物理属性：

  tablename.columnname

  - *tablename*

    提供属性所在的表的名称。 您指定的表必须是主表。

  - *columnname*

    提供存储属性的列的名称。

- 指定的属性必须位于数据库中，且已经在目录配置文件中定义，如"如何修改属性说明" (p. 103)中所述。

示例：业务编号属性的自定义操作

在下列示例中，通过调用存储过程生成业务编号属性；该属性不是数据库中的物理属性。

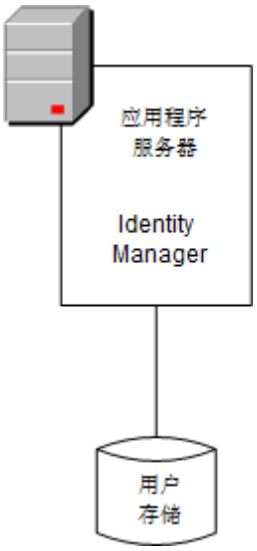
```
<ImsManagedObjectAttr wellknown="%BUSINESS_NUMBER%"     displayname="Business
Number" description="Business Number"     valuetype="String" required="false"
multivalued="false"     maxlength="0">
<Operation name="Get" value="call sp_getbusinessnumber(?)">
    <Parameter name="%USER_ID%"/>
</Operation>
<Operation name="Set" value="call sp_setbusinessnumber(?,?)">
    <Parameter name="%USER_ID%"/>
    <Parameter name="%BUSINESS_NUMBER%"/>
</Operation>
<Operation name="Delete" value="call sp_deletebusinessnumber(?)">
    <Parameter name="%USER_ID%"/>
</Operation>
```

请注意下列事项：

- sp_getbusinessnumber、sp_setbusinessnumber 和 sp_deletebusinessnumber 是用户定义的存储过程。
- 从 Get 操作返回的值映射到 %BUSINESS_NUMBER% 属性。
- 问号 (?) 表示查询执行之前在运行时间进行的替换。 例如，在 Get 操作中，将 %USER_ID% 常用属性发送到 sp_getbusinessnumber 存储过程。

连接用户目录

CA Identity Manager 连接到用户目录，以便存储信息（例如，用户、组和组织信息），如下图所示：



无需新的目录或数据库。 然而，现有目录或数据库必须位于具有完全限定域名 (FQDN) 的系统上。

有关支持的目录和数据库类型的列表，请参阅 CA 支持站点上的 CA Identity Manager 支持表。

在管理控制台中创建 CA Identity Manager 目录时，需配置与用户存储的连接。

如果在创建 CA Identity Manager 目录之后导出目录配置，目录配置文件的 Provider 元素中将显示用户目录连接信息。

数据库连接说明

要描述数据库连接，请使用 directory.xml 文件中的 Provider 元素及其子元素。

注意：如果正在创建 CA Identity Manager 目录，则无需在 directory.xml 文件中提供目录连接信息。 而需在管理控制台的 CA Identity Manager 目录向导中提供连接信息。

仅在需要更新时修改 Provider 元素。

Provider 元素

Provider 元素包含以下子元素：

JDBC（必需）

标识在连接到用户存储时使用的 JDBC 数据源。 指定在创建 JDBC 数据源 (p. 90)时您已经提供的 JNDI 名称。

Credentials（必需）

提供用于访问数据库的用户名和密码。

DSN

标识在连接到用户存储时使用的 ODBC 数据源。

注意：只有当 CA Identity Manager 与 SiteMinder 集成时，此子元素才适用。在不包括 SiteMinder 的 CA Identity Manager 环境中，将忽略此子元素。

SiteMinderQuery

指定在关系数据库中查找用户信息的自定义查询方案。

注意：只有当 CA Identity Manager 与 SiteMinder 集成时，此子元素才适用。在不包括 SiteMinder 的 CA Identity Manager 环境中，将忽略此子元素。

完成的数据库连接如下例所示：

```
<Provider type="RDB" userdirectory="@SMDirName">
        <JDBC datasource="@SMDirJDBCDataSource"/>
        <Credentials user="@SMDirUser"
                cleartext="true">@SMDirPassword</Credentials>
        <DSN name="@SMDirDSN" />
        <SiteMinderQuery name="AuthenticateUser" query="SELECT TBLUSERS.LOGINID
FROM    TBLUSERS WHERE TBLUSERS.LOGINID='%s' AND TBLUSERS.PASSWORD='%s'" />
</provider>
```

Provider 元素的属性如下所示：

type

指定数据库类型。对于 Microsoft SQL Server 和 Oracle 数据库，指定 RDB（默认）。

userdirectory

指定用户目录连接的名称。 此参数对应您在目录创建期间提供的连接对象名称。

如果 CA Identity Manager 与 SiteMinder 集成以进行身份验证，它使用您在安装期间为连接对象指定的名称在 SiteMinder 中创建用户目录连接。 如果您想连接到现有的 SiteMinder 用户目录，请在提示时为连接对象输入该用户目录的名称。 CA Identity Manager 使用您指定的名称填充 userdirectory 参数。

如果 CA Identity Manager 不与 SiteMinder 集成，userdirectory 参数的值是您提供给连接到用户存储的 JDBC 的任何名称。

注意：请勿在 directory.xml 文件中指定用户目录连接的名称。 CA Identity Manager 提示您在目录创建期间提供名称。

数据库凭据

为了连接到数据库，CA Identity Manager 必须为数据源提供有效凭据。在凭据元素中定义凭据，如下例所示：

```
<Credentials user="@SMDirUser" cleartext="true">
  "MyPassword"
</Credentials>
```

如果您不在凭据元素中指定密码，并且尝试在管理控制台中创建 CA Identity Manager 目录，它会提示密码凭据。

注意：建议在管理控制台中指定密码。

如果在管理控制台中指定密码，CA Identity Manager 将对此密码加密。或者，如果不希望密码以明文显示，请使用与 CA Identity Manager 一起安装的密码工具加密密码。 SiteMinder Passwords 提供了有关使用密码工具的说明。

注意：可以仅指定一组凭据。 如果您定义多个数据源，您指定的凭据必须适用于所有数据源。

凭据参数如下所示：

user

为可以访问数据源的帐户定义登录 ID。

不要为 directory.xml 文件中的用户参数指定值。 当您在管理控制台中创建 CA Identity Manager 目录时，CA Identity Manager 提示您提供登录 ID。

cleartext

确定密码是否在 directory.xml 文件中明文显示：

- True－密码以明文显示。
- False－密码已加密（默认）。

注意：这些参数是可选的。

数据源名 (DSN)

directory.xml 文件的 DSN 元素有一个参数－CA Identity Manager 用来连接到数据库的 ODBC 数据源的名称。 名称参数的值必须匹配现有的数据源名称。

注意：只有 CA Identity Manager 与 SiteMinder 集成时，此元素才适用。 如果 CA Identity Manager 不与 SiteMinder 集成，忽略此元素。

如果名称参数的值是 @SmDirDSN，您不必在 directory.xml 文件中指定 DSN 名称。导入 directory.xml 文件时，CA Identity Manager 会提示提供 DSN 名称。

要配置故障切换，请定义多个 DSN 元素。 如果主数据源无法响应请求，定义的下一个数据源响应请求。

例如，假定您已经以下列方式配置故障切换：

```
<DSN name="DSN1">
<DSN name="DSN2">
```

CA Identity Manager 使用数据源 DSN1 连接数据库。 如果 DSN1 存在问题，CA Identity Manager 尝试使用 DSN2 连接数据库。

注意：您在凭据元素 (p. 117)中指定的凭据必须适用您定义的所有 DSN。

SQL 查询方案

CA Identity Manager 使用查询方案来在关系数据库中查找用户和组信息。

注意：只有 CA Identity Manager 与 SiteMinder 集成时，此元素才适用。 在不包括 SiteMinder 的环境中，将忽略此参数。

当您在管理控制台中创建 CA Identity Manager 目录时，CA Identity Manager 生成一组查询方案，这些方案基于 SiteMinder 中必需的查询方案。（有关 SiteMinder 查询方案的完整信息，请参阅 *《CA SiteMinder Web Access Manager Policy Server Configuration Guide》*。）将 SiteMinder 查询方案的表和列名替换成您在目录配置文件中指定的数据。

如何定义自定义查询方案

在目录配置文件的 SiteMinder 查询元素中定义查询方案。 SiteMinder 查询元素类似以下内容：

```
<SiteMinderQuery name="SetUserProperty" query="update tblUsers set %s =
&apos;%s&apos; where loginid = &apos;%s&apos;" />
```

注意：在示例查询中，' 是单引号 (') 的 XML 语法。

当 CA Identity Manager 与 SiteMinder 集成时，SiteMinder 查询元素才适用。

查询方案参数如下所示：

name

指定 SiteMinder 查询方案的重定义名称。

不要修改此值。

query

指定要执行的 SQL 语句或存储过程。 有效值如下所示：

- INSERT
- SELECT
- UPDATE
- DELETE
- CALL（针对存储过程）

注意：这些参数是 SiteMinder 查询元素所必需的。

在您自定义查询方案之前，请执行以下操作：

- 熟悉默认查询方案。

  注意：有关 SQL 查询方案的详细信息，请参阅 *《CA SiteMinder Web Access Manager Policy Server Configuration Guide》*。
- 获得开发 SQL 查询的广泛经验。

修改默认查询方案

执行以下程序，以修改默认查询方案。

遵循这些步骤:

1. 导出目录配置文件。

   CA Identity Manager 生成包含 CA Identity Manager 目录的所有当前设置的目录配置文件，包括生成的查询方案。

2. 保存目录配置文件。

   注意：如果您想创建原始目录配置文件的备份，请在保存导出的文件之前使用不同的名称或在不同的位置保存文件。

3. 找到想要修改的 CA Identity Manager 生成的查询方案。

4. 输入要在询问参数中执行的查询方案或存储过程。

   注意：不要修改查询名称。

5. 在完成必要更改之后，保存目录配置文件。

   导入文件以更新 CA Identity Manager 目录 (p. 156)。

关系数据库的常用属性

常用属性在 CA Identity Manager 中具有特殊含义。 这些属性用以下语法进行定义：

%ATTRIBUTENAME%

在此语法中，*ATTRIBUTENAME* 必须为大写。

使用属性说明 (p. 103)将常用属性映射到一个物理属性。

在下列属性说明中，属性 tblUsers.password 映射到常用属性 %PASSWORD%，因此 CA Identity Manager 将 tblUsers.password 的值看成是密码：

```
<ImsManagedObjectAttr
        physicalname="tblUsers.password"
        displayname="Password"
        description="Password"
        valuetype="String"
        required="false"
        multivalued="false"
        wellknown="%PASSWORD%"
        maxlength="0" />
```

一些常用属性是必需的；其他则为可选的。

用户常用属性

用户常用属性的列表如下：

%ADMIN_ROLE_CONSTRAINT%

包含分配给管理员 (p. 124)的管理角色 (p. 124)的列表。

映射到 %ADMIN_ROLE_CONSTRAINT% 的物理属性必须是多值的，以适应多个角色。

我们建议检索映射到 %ADMIN_ROLE_CONSTRAINT% 的属性。

%CERTIFICATION_STATUS%

（使用用户认证功能需要此属性）

包含用户的认证状态。

注意：有关用户认证的详细信息，请参阅*《管理指南》*。

%DELEGATORS%

映射到对当前用户有已指派工作项的用户的列表。

此属性需要使用指派。 映射到 %DELEGATORS% 的物理属性必须是多值的并且能够保留字符串。

重要说明！ 直接使用 CA Identity Manager 任务或外部的工具编辑此字段可以引起重大安全影响。

%EMAIL%

（启用电子邮件通知功能需要此属性）

存储用户的电子邮件地址。

%ENABLED_STATE%

（必需）

跟踪用户的状态。

注意：映射到 %ENABLED_STATE% 的物理属性的数据类型必须是字符串。

%FIRST_NAME%

包含用户的名字。

%FULL_NAME%

（必需）

包含用户的姓氏和名字。

%IDENTITY_POLICY%

包含已经应用于用户帐户的身份策略列表。

CA Identity Manager 使用此属性来确定身份策略是否必须应用于用户。 如果策略启用了“Apply Once”（应用一次）设置，并且策略位于 %IDENTITY_POLICY% 属性中，CA Identity Manager 不将策略的更改应用于该用户。

注意：有关身份策略的详细信息，请参阅 *《管理指南》*。

%LAST_CERTIFIED_DATE%

（使用用户认证功能需要此属性）

包含用户角色的认证日期。

注意：有关用户认证的详细信息，请参阅 *《管理指南》*。

%LAST_NAME%

包含用户的姓氏。

%ORG_MEMBERSHIP%

（支持组织时需要此属性）

包含用户所属组织的唯一标识符。

%ORG_MEMBERSHIP_NAME%

（支持组织时需要此属性）

包含用户所属组织的用户友好名称。

%PASSWORD%

包含用户密码。

注意：即使属性或字段未设置为隐藏密码，%PASSWORD% 属性的值在 CA Identity Manager 屏幕中始终显示为一系列星号 (*) 字符。

%PASSWORD_DATA%

（密码策略支持所必需的）

指定跟踪密码策略信息的属性。

注意：即使属性或字段未设置为隐藏密码，%PASSWORD_DATA% 属性的值在 CA Identity Manager 屏幕中始终显示为一系列星号 (*) 字符。

%PASSWORD_HINT%

（必需）

包含用户指定的问答对。 问答对用于忘记密码的情况。

注意：即使没有将属性或字段设置成隐藏密码，在 CA Identity Manager 屏幕中 %PASSWORD_HINT% 属性的值总是显示为一系列星号 (*) 字符。

%USER_ID%

（必需）

存储用户登录 ID。

组常用属性

组常用属性的列表如下：

%GROUP_ADMIN%

包含组管理员。

注意：%GROUP_ADMIN% 属性必须是多值的。

%GROUP_DESC%

包含组的说明。

%GROUP_ID%

包含组的唯一标识符。

%GROUP_MEMBERSHIP%

（必需）

包括组的成员列表。

注意：%GROUP_MEMBERSHIP% 属性必须是多值的。

%GROUP_NAME%

（必需）

存储组的名称。

%ORG_MEMBERSHIP%

（支持组织时需要此属性）。

包含该组所属组织的唯一标识符。

%ORG_MEMBERSHIP_NAME%

（支持组织时需要此属性）。

包含该组所属组织的用户友好名称。

%SELF_SUBSCRIBING%

确定用户是否可以订阅到组。

%Admin_Role_Constraint% 属性

创建管理角色时，需为角色成员身份指定一个或多个规则。 满足成员资格规则的用户具备此角色。 例如，如果用户管理者角色的成员资格规则是 title=User Manager，则具有职称 User Manager 的用户具有用户管理者角色。

注意：有关规则的详细信息，请参阅 *《管理指南》*。

通过 %ADMIN_ROLE_CONSTRAINT% 您可以指定一个配置文件属性，以存储管理员的所有管理角色。

如何使用 %ADMIN_ROLE_CONSTRAINT% 属性

要使用 %ADMIN_ROLE_CONSTRAINT% 作为所有管理角色的约束，请执行下列任务：

- 将 %ADMIN_ROLE_CONSTRAINT% 常用属性与可容纳多个角色的多值配置文件属性配对。
- 在 CA Identity Manager 用户界面中配置管理角色时，下列方案可以作为约束：

  “管理角色”等于 *角色名称*

  角色名称

  定义您正在提供约束的角色的名称。

  例如，管理角色等于用户管理者

注意：管理角色是 %ADMIN_ROLE_CONSTRAINT% 属性的默认显示名称。

配置常用属性

请按照以下步骤配置常用属性。

遵循这些步骤:

1. 在目录配置文件中，搜索以下符号：

   ##

   必要值由磅字符 (##) 标识。

2. 将以 ## 开始的值替换成所需的属性物理名（如果位于数据库中）。 提供使用下列格式的属性名称：

   tablename.columnname

   例如，如果密码属性存储在 tblUsers 表的密码列中，以下列方式指定该属性：

   tblUsers.password

3. 重复步骤 1 和 2，直到您已经替换所有必要值并且已经加入您所需的可选值。

4. 根据需要将可选常用属性映射到物理属性中。
5. 保存目录配置文件。

如何配置自行订阅组

通过在目录配置文件中配置对自行订阅组的支持，使自助服务用户能够加入组。

遵循这些步骤:

1. 在“自行订阅组”部分中，按如下方式添加 SelfSubscribingGroups 元素：

   ```
   <SelfSubscribingGroups type=search_type org=org_dn>
   ```

2. 为下列参数输入值：

   type

   表明 CA Identity Manager 搜索自行订阅组的位置。有效值如下所示：

   - NONE－CA Identity Manager 不搜索组。指定 NONE 以防止用户订阅组。
   - ALL－CA Identity Manager 在用户存储中搜索所有组。如果用户可以订阅所有组，指定 ALL。
   - INDICATEDORG（*仅针对支持组织的环境*）－CA Identity Manager 在用户的组织及其子组织中搜索自行订阅组。例如，当用户的配置文件位于营销组织中时，CA Identity Manager 将在营销组织及所有子组织中搜索自行订阅组。
   - SPECIFICORG（*仅针对支持组织的环境*）－CA Identity Manager 在指定组织中搜索。 在 org 参数中提供指定组织的唯一标识符。

   org

   定义 CA Identity Manager 搜索自行订阅组的组织的唯一标识符。

   注意：如果 type=SPECIFICORG，确保您指定了组织参数。

3. 如果您更改任何以下项，重新启动 SiteMinder 策略服务器：
   - 发送到 SPECIFICORG 的类型参数或来自 SPECIFICORG 的类型参数
   - 组织参数的值

在 CA Identity Manager 目录中配置自行订阅组支持之后，CA Identity Manager 管理员即可指定用户控制台中自行订阅的组。

在用户自行注册时，CA Identity Manager 在指定的组织中查找组，并向用户显示自行订阅组。

验证规则

验证规则会强制性索取用户在任务屏幕字段中输入的数据。 这些要求可以实施数据类型或格式，或者可以确保数据在任务屏幕上的其他数据的环境中是有效的。

验证规则与配置文件属性关联。在处理任务之前，CA Identity Manager 确保为配置文件属性输入的数据满足任何关联的验证规则。

您可以定义验证规则，并可以将他们与目录配置文件中的配置文件属性关联。

组织管理

对于关系数据库，CA Identity Manager 可以选择管理组织。如果您的数据库支持组织，则以下内容为“true”：

- 组织具有层级结构。
- 用户、组和其他组织等所有管理对象属于一个组织。
- 如果删除组织，也会删除属于该组织的对象。

配置组织对象的方式与配置用户和组对象相同，只是需要几个其他步骤。

如何设置组织支持

实施下列步骤，设置组织支持：

1. 在数据库中配置组织支持 (p. 126)。
2. 在 ImsManagedObject (p. 99) 中说明组织对象。

   确保配置 Table 和 UniqueIdentifier 子元素。
3. 配置顶级组织 (p. 126)。
4. 描述构成组织的属性 (p. 103)。
5. 为组织对象 (p. 128)定义常用属性。

在数据库中配置组织支持

遵循这些步骤:

1. 在编辑器中打开下列 SQL 脚本之一：
   - Microsoft SQL Server 数据库：

     ims_mssql_rdb.sql

- Oracle 数据库：

  ims_oracle_rdb.sql

  这些文件位于以下位置：

  admin_tools\directoryTemplates\RelationalDatabase

  admin_tools 指向“管理工具”的安装位置，默认情况下将其安装在下列位置之一：

  Windows： C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools

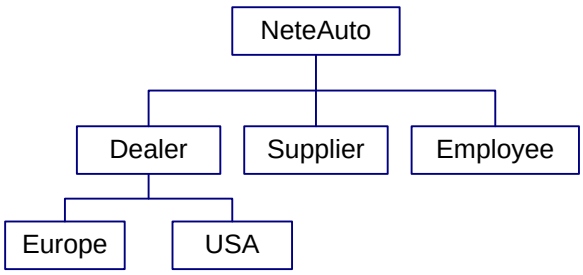
  UNIX： /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

2. 在 SQL 脚本中，搜索 <@primary organization table@> 并将其替换成组织对象的主表的名称。 保存 SQL 脚本。
3. 针对数据库运行 SQL 脚本。

根组织规范

根组织作为该目录中的顶级组织或父组织。 所有组织都与根组织相关。

在下图中，NeteAuto 是根组织。 其他组织是 NeteAuto 的子组织：



完整的根组织定义类似以下示例：

```
<ImsManagedObject name="Organization" description="My  Organizations"
objecttype="ORG">
   <RootOrg value="select orgid from tblOrganizations where parentorg is null">
      <Result name="%ORG_ID%" />
   </RootOrg>
```

在您定义组织对象的基本信息（包括构成组织配置文件的表和组织对象的唯一标识符）之后，在 directory.xml 文件中指定根组织：

- 在 RootOrg 元素的值参数中，定义 CA Identity Manager 用来检索根组织的查询，如下例所示：

  ```
  <RootOrg value="select orgid from tblOrganizations where parentorg  is null">
  ```

- 在结果元素的名称参数中，输入该组织的唯一标识符，如下例所示：

  ```
  <Result name="%ORG_ID%" />
  ```

  注意：名称参数的值必须是组织对象的唯一标识符。

组织的常用属性

为组织配置文件的配置文件的属性定义常用属性，如"常用属性" (p. 69)中所述。

必要和可选组织常用属性如下所示：

%ORG_DESCR%

包含组织的说明。

%ORG_MEMBERSHIP%

（必需）

包含组织的父组织。

注意：有关 %ORG_MEMBERSHIP% 属性的详细信息，请参阅"如何定义组织的层次结构"。

%ORG_MEMBERSHIP_NAME%

（必需）

包含组织的父组织 (p. 128)的用户友好名称。

%ORG_NAME%

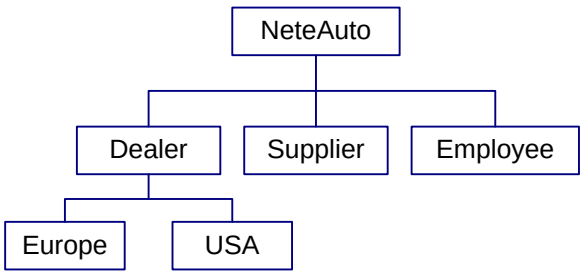
（必需）

包含该组织的名称。

如何定义组织的层次结构

在 CA Identity Manager 中，组织具有包括根组织和子组织的层次结构。 子组织也可以有子组织。

除根组织之外，每个组织都有父组织。例如，在下图中，Dealer 是 USA 和 Europe 组织的父组织：



父组织的唯一标识符存储在组织的配置文件的属性中。CA Identity Manager 可以使用此属性的信息构建组织层次结构。

要指定存储父组织的属性，请使用 %ORG_MEMBERSHIP% 和 %ORG_MEMBERSHIP_NAME% 常用属性以及在属性描述中存储父组织的名称的物理属性，如下所示：

```
<ImsManagedObjectAttr physicalname="tblOrganizations.parentorg"
displayname="Organization" description="Parent Organization" valuetype="Number"
required="false" multivalued="false" wellknown="%ORG_MEMBERSHIP%" maxlength="0"
/>
```

如何改善目录搜索性能

改善用户、组织和组目录搜索的性能，请执行下列任务：

- 检索管理员可以在搜索查询中指定的属性。
- 通过为目录配置文件 (directory.xml) 中的超时搜索参数指定值，覆盖默认目录超时设置。
- 调整用户目录。 请参阅您正在使用的数据库的文档。

在 ODBC 数据源中配置数据库专用选项。 有关详细信息，请参阅数据源的文档。

如何改善大规模搜索的性能

在 CA Identity Manager 管理大规模用户存储时，返回许多结果的搜索可能导致系统内存不足。

下列二个设置可以确定 CA Identity Manager 处理大规模搜索的方式：

- 最大行数

  指定搜索用户目录时 CA Identity Manager 可以返回的结果的最大数目。 在结果的数目超过限制时，显示错误。

- 页面大小

  指定在一次搜索中可以返回的对象数目。 如果对象的数目超过页面大小，CA Identity Manager 将执行多个搜索。

  注意：如果用户存储不支持分页，并且指定了最大行的值，则 CA Identity Manager 仅使用最大行值来控制搜索大小。

您可以在以下位置配置最大行限制和页面大小：

- 用户存储

  在大多数用户存储和数据库中，您可以配置搜索限制。

  注意：有关详细信息，请参阅您正在使用的用户存储或数据库的文档。

- CA Identity Manager 目录

  您可以在您用来创建 CA Identity Manager 目录的目录配置文件 (directory.xml) 中配置 DirectorySearch 元素 (p. 52)。

  默认情况下，最大行数和页面大小的值对于现有目录是无限的。 对于新目录，最大行数的值是无限的，页面大小的值是 2000。

- 管理对象定义

  要设置适用于一种对象类型而不是整个目录的最大行数限制和页面大小，请在用来创建 CA Identity Manager 目录的 directory.xml 文件中配置*管理对象定义* (p. 53)。

  通过为管理对象类型设置限制，可以基于业务要求进行调整。 例如，大多数公司所具有的用户比组多。 这些公司可以只为用户对象搜索设置限制。

- 任务搜索屏幕

  您可以控制用户在用户控制台的搜索和列表屏幕中看到的搜索结果的数目。 如果结果的数目超过为任务定义的每页结果数，用户会看到其他结果页面的链接。

  此设置不影响搜索返回的结果的数目。

  注意：有关在搜索和列表屏幕中设置页面大小的信息，请参阅*《管理指南》*。

如果在多个位置定义了最大行限制和页面大小，将应用最适合的设置。 例如，管理对象设置优先于目录级别设置。

第 5 章： CA Identity Manager 目录

CA Identity Manager 目录提供有关 CA Identity Manager 管理的用户目录的信息。此信息描述怎样将用户、组等对象及组织存储在用户存储中，并描述在 CA Identity Manager 中显示它们的方式。

在管理控制台的 CA Identity Manager 目录部分中创建、查看、导出、更新和删除 CA Identity Manager 目录。

注意：如果 CA Identity Manager 使用 SiteMinder 策略服务器群集，在创建或更新 CA Identity Manager 目录之前阻止除一个以外所有其余策略服务器。

此部分包含以下主题：

创建 CA Identity Manager 目录的先决条件

在创建 CA Identity Manager 目录之前，您必须进行以下操作：

- 在您创建或修改 CA Identity Manager 目录之前，阻止除了一个以外的所有其余的 CA Identity Manager 节点。

  注意：如果有一个 CA Identity Manager 节点群集，当在管理控制台中进行更改时，只能启用一个 CA Identity Manager 节点。

- 在创建或更新 CA Identity Manager 目录之前阻止除了一个以外的所有其余的策略服务器。

  注意：如果有一个 SiteMinder 策略服务器群集，当在管理控制台中进行更改时，只能启用一个 SiteMinder 策略服务器群集。

如何创建目录

在管理控制台中创建 CA Identity Manager 目录（描述用户存储的结构和内容）以及配给目录（存储配给服务器的必要信息）。这些目录与 CA Identity Manager 环境关联。

使用以下方式之一创建目录：

- 使用目录配置向导

  引导管理员完成为用户存储创建目录的流程。 此方式有助于减少可能的配置错误。

  注意：使用目录配置向导只能为 LDAP 用户存储创建新目录。要为关系数据库创建目录，或更新现有的目录，请直接导入 directory.xml 文件。

- 使用 XML 配置文件

  允许管理员选择完全配置的 XML 文件来创建或修改用户存储或配给服务器。

  如果您要为关系数据库创建目录或更新现有的目录，选择此方式。

更多信息：

使用 XML 配置文件创建目录 (p. 143)
使用目录配置向导创建目录 (p. 132)

使用目录配置向导创建目录

目录配置向导可引导管理员完成为用户存储创建目录的过程，并可帮助减少配置错误。 在启动向导之前，您必须首先上载 CA Identity Manager LDAP 目录配置模板。 这些模板预先配置了一些常用属性和必需属性。 为您的 LDAP 用户存储或配给目录输入连接详细信息之后，可以选择 LDAP 属性，映射常用属性，以及为这些属性输入元数据。 完成属性映射时，单击“完成”即可创建该目录。

启动目录配置向导

目录配置向导允许管理员选择 CA Identity Manager 模板，并修改该模板以供您的环境使用。

遵循这些步骤:

1. 在管理控制台中，单击“Directories”（目录），选择“Create from Wizard”（从向导创建）。

   系统会提示您选择目录配置文件来配置用户存储。

2. 单击“Browse”（浏览）以选择配置文件来配置下列默认位置的用户存储或配给服务器，然后单击“Next”（下一步）。

   ```
   admin_tools\directoryTemplates\directory\
   ```

   注意：admin_tools 指定了安装管理工具的目录，而该目录指定了 LDAP 供应商的名称。

   管理工具安装在以下默认位置：

   - Windows：C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools
   - UNIX：/opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

3. 在“Connection Details”（连接详细信息）屏幕上，指定 LDAP 目录或配给服务器的连接信息、目录搜索参数以及故障切换连接信息，然后单击“Next”（下一步）。

4. 在“Configure Managed Object”（配置管理对象）屏幕上，指定要配置的对象，然后单击“Next”（下一步）。 可以从下列对象中进行选择：

   - “Configure User Managed Object”（配置用户管理对象）
   - “Configure Group Managed Object”（配置组管理对象）
   - “Configure Organization Object”（配置组织对象）
   - “Show summary and deploy directory”（显示摘要并部署目录）

     注意：仅当您已经完成目录的配置后再选择“Show summary and deploy directory”（显示摘要并部署目录）。

   a. 在“Select Attribute”（选择属性）屏幕上，根据需要查看和修改所需的结构和辅助类，然后单击“Next”（下一步）。

   b. 在“Select Attributes: Mapping Well-Knowns”（选择属性: 常用映射）屏幕上，将 CA Identity Manager 常用别名映射到所选 LDAP 属性，然后单击“Next”（下一步）。

   c. （可选）在“Describe User Attributes”（说明用户属性）屏幕上，查看和修改属性定义，然后单击“Next”（下一步）。 您可以修改显示名称和说明。

   d. （可选）在“User Attribute Details”（用户属性详细信息）屏幕上，为每一要管理的所选属性定义元数据，然后单击“Next”（下一步）。

      此时会显示“Managed Object Selection”（管理对象选择）屏幕。

      要配置组或组织，请选择管理对象并单击“Next”（下一步），以完成这些对象的“Attributes”（属性）屏幕的操作。

5. 从列表中选择“Show summary and deploy directory”（显示摘要并部署目录），然后单击“Next”（下一步）。

   此时显示“Confirmation”（确认）屏幕。

6. 查看目录详细信息。

   如果存在错误，请单击“Back”（返回）按钮，以在适当的屏幕上进行修改。单击“Finish”（完成）以应用更改。

   CA Identity Manager 验证配置并且创建目录。 然后，您会退回到“Directories listing”（目录列表）屏幕，您可以在此查看新的目录。

“Select Directory Template”（选择目录模板）屏幕

使用此屏幕为 LDAP 选择目录 XML 文件，以配置用户存储或配给服务器。

单击“Browse”（浏览）按钮选择配置文件，以配置下列默认位置的用户存储或供给服务器：

admin_tools\directoryTemplates\directory\

注意：admin_tools 指定了安装管理工具的目录，而该目录指定了 LDAP 供应商的名称。

管理工具安装在以下默认位置：

- Windows：C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools
- UNIX：/opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

在您选择目录 XML 文件之后，单击“下一步”继续“连接详细信息”屏幕中的操作。

“连接详细信息”屏幕

使用此屏幕来输入您的用户存储的配置凭据。 您也可以输入目录搜索参数，并添加故障切换连接。 在您输入连接信息后，单击“下一步”来选择要管理的对象。

注意：出现在此屏幕上的字段取决于用户存储的类型，以及您是使用目录配置向导创建连接还是直接导入 XML 文件。

此屏幕包含以下字段：

“Name”（名称）

指定您正在连接的用户目录的名称。

“Description”（说明）

指定用户目录的说明。

“Host”（主机）

指定用户存储所在的计算机的主机名。

“Port”（端口）

指定用户存储所在的计算机的端口。

“User DN”（用户 DN）

指定访问 LDAP 用户存储的用户域名。

“JDBC Data Source JNDI Name”（JDBC 数据源 JNDI 名称）

指定 CA Identity Manager 用来连接到数据库的现有 JDBC 数据源的名称。

“Username”（用户名）

指定访问配给服务器的用户名。

注意：仅针对配给服务器。

“Domain”（域）

指定访问配给服务器的域名。

注意：仅针对配给服务器。

“Password”（密码）

指定访问 LDAP 用户存储/配给服务器的密码。

“Confirm Password”（确认密码）

确认访问 LDAP 用户存储/配给服务器的密码。

“Secure Connection”（安全连接）

在选定时，强制与 LDAP 用户目录进行安全套接字层 (SSL) 连接。

“Search Root”（搜索根）

指定 LDAP 目录中用作目录起点的位置，通常为组织 (o) 或组织单元 (ou)。

注意：仅针对 LDAP 用户。

“Search Maximum Rows”（搜索最大行）

指定搜索用户目录时 CA Identity Manager 可以返回的结果的最大数目。 在结果的数目超过限制时，显示错误。

设置最大行可以覆盖限制搜索结果的 LDAP 目录的设置。在应用冲突的设置时，LDAP 服务器使用最低的设置。

“Search Page Size”（搜索页大小）

指定在一次搜索中可以返回的对象数目。 如果对象的数目超过页面大小，CA Identity Manager 将执行多个搜索。

在指定搜索页大小时，请注意下列几点：

- 要使用“Search Page Size”（搜索页大小）选项，CA Identity Manager 管理的用户存储必须支持分页。一些用户存储类型可能需要其他配置来支持分页。 有关详细信息，请参阅*《配置指南》*。
- 如果用户存储不支持分页，并且指定了“Search Maximum Rows”（搜索最大行）的值，则 CA Identity Manager 仅使用“Search Maximum Rows”（搜索最大行）值来控制搜索大小。

“Search Timeout”（搜索超时）

指定 CA Identity Manager 在终止搜索之前搜索目录的最大秒数。

“Failover Host”（故障切换主机）

指定主系统不可用时冗余用户存储或备用配给服务器所在的系统的主机名。如果列出了多个服务器，CA Identity Manager 尝试按同样的列表顺序连接各个系统。

“Failover Port”（故障切换端口）

指定主系统不可用时冗余用户存储或备用配给服务器所在的系统的端口。如果列出了多个服务器，CA Identity Manager 尝试按同样的列表顺序连接各个系统。

“Add”（添加）按钮

单击此按钮来添加其他故障切换主机名和端口号。

“Configure Managed Objects”（配置管理对象）屏幕

使用此屏幕来选择要配置的对象。

此屏幕包含以下字段：

“Configure User Managed Object”（配置用户管理对象）

说明用户在用户存储中的存储方式及其在 CA Identity Manager 中的表示方式。

“Configure Group Managed Object”（配置组管理对象）

说明组在用户存储中的存储方式及其在 CA Identity Manager 中的表示方式。

“Configure Organization Managed Object”（配置组织管理对象）

如果用户存储包括组织，说明组织在 CA Identity Manager 中的存储方式和表示方式。

“Show summary and deploy directory”（显示摘要并部署目录）

指定您要部署目录的所有已被定义的管理对象。 在您选择“Show summary and deploy directory”（显示摘要并部署目录）之后，单击“Next”（下一步），您就会被带到摘要页面。

“Save”（保存）按钮

单击此按钮保存您的 xml 文件。

“Back”（返回）按钮

单击此按钮返回“连接详细信息”屏幕进行修改。

“Next”（下一步）按钮

单击此按钮打开“Select Attributes”（选择属性）屏幕，以选择要配置的用户、组或组织属性。

“Select Attributes”（选择属性）屏幕

使用此屏幕来为您的用户、组或组织对象更改或添加结构和辅助类。 此屏幕根据您使用的目录类型的常用目录架构和最佳实践预配置了一些值。 通过从下拉式菜单中选择新类，管理员可以更改结构类。 选择类会使用属于新的结构类的属性更新表。

从下拉式菜单中选择一个类后，可以添加辅助类。 选择辅助类会使用属于新的辅助类的属性更新表。

以下列表是显示在此屏幕中的字段：

“Structural Class Name”（结构类名称）

指定要配置的属性的结构类。

“Change”（更改）按钮

单击此按钮更改结构类。

“Auxiliary Class Name”（辅助类名称）

指定要配置的属性的辅助类。

“Add”（添加）按钮

单击此按钮添加要配置的辅助类。

“Object Class”（对象类）

指定容器对象类。

ID

指定容器 ID。

“Name”（名称）

指定容器名称。

“Attributes Table”（属性表）

指定物理名称、对象类、属性是否多值以及所选属性的数据类型。此表中的属性可以按“Selected”（已选）、“Object Class”（对象类）、“Multi-Valued”（多值）和“Data Type”（数据类型）进行排序。

“返回”按钮

单击此按钮返回“Configured Managed Objects”（配置管理对象）屏幕。

“Next”（下一步）

单击此按钮打开“Well-Known Mapping”（常用映射）屏幕，以映射必需和可选的常用别名。

“Well-Known Mapping”（常用映射）屏幕

使用此屏幕将 CA Identity Manager 常用属性映射到所选 LDAP 属性。通过将新的常用属性输入文本字段，然后单击“添加”按钮，管理员可以将其添加到常用属性的列表（如果其是自定义代码所必需的）。 屏幕会刷新，这样您就可以继续根据需要添加任意数量的常用属性。

以下列表是显示在此屏幕中的字段：

“Required Well-Knowns”（必需的常用属性）

为需要映射到 LDAP 属性的用户、组或组织（如果适用）指定常用属性。

“Optional Well-Knowns”（可选的常用属性）

为可以选择映射的用户、组或组织（如果适用）指定常用属性。

“New Well-Known”（新的常用属性）

指定自定义代码引用的常用属性。

“Add”（添加）按钮

单击此按钮向可选常用属性表添加新的常用属性。

“Back”（返回）按钮

单击此按钮返回“Select User Attributes”（选择用户属性）屏幕以选择更多属性。 在您返回此屏幕时，会保存您已进行的映射，并使其可用。

“Next”（下一步）按钮

单击此按钮打开“Basic Object Attribute Definition”（基本对象属性定义）屏幕，以指定基本属性定义。

更多信息

LDAP 用户存储的常用属性 (p. 69)
组常用属性 (p. 72)
用户常用属性 (p. 69)
组织常用属性 (p. 73)

“Basic Object Attribute Definition”（基本对象属性定义）屏幕

使用此屏幕来查看和修改常用的定义：显示名称和说明。

以下列表是显示在此屏幕中的字段：

“Managed Object Table”（管理对象表）

指定管理对象的显示名称、物理名称、常用名称以及说明。 如果需要，使用下拉式菜单来更改说明。在您进行更改后，单击“Next”（下一步）以继续。

“Back”（返回）按钮

单击此按钮返回“Well-Known Mapping”（常用映射）屏幕，以便修改映射的详细信息。

“Next”（下一步）按钮

单击此按钮前往“Detailed Object Attribute Definition”（详细对象属性定义）屏幕，以指定其他属性定义。

“Detailed Object Attribute Definition”（详细对象属性定义）屏幕

使用此屏幕可指定其他属性定义。 管理员可以通过修改显示名称、管理用户控制台屏幕中的属性、值的数据类型、最大长度以及验证规则集，为每个选定的属性定义元数据。 指定属性定义后，单击“Next”（下一步）继续。

该屏幕上的字段如下所列：

“Display Name”（显示名称）

指定管理对象属性的唯一名称。 这是在“用户控制台”中显示的名称。

“Tags”（标记）

为管理对象属性值指定数据分类标记。 可搜索标记外的所有标记都是可选标记，且均已默认为“false”。 可以选择下列标记：

“Required”（必需）

表示在创建对象时该属性是必需的。

“Multiple Values”（多值）

表示该属性显示为多值。

“Hidden”（隐藏）

表示该属性处于隐藏状态。

“System”（系统）

表示该属性是系统属性且不会添加到任务屏幕中。

“Searchable”（可搜索）

表示已将该属性添加到搜索筛选中。 默认为“true”。

“Sensitive Encrypt”（敏感加密）

表示该属性敏感且显示为一串星号 (*)。

“Hide in VST”（隐藏在 VST 中）

表示该属性隐藏在“查看提交的任务”的“事件详细信息”屏幕中。

“Do not copy”（请勿复制）

表示在管理员创建对象的副本时，必须忽略该属性。

“Previously encrypted”（先前已加密）

表示在用户存储中访问的属性先前已加密且需要解密。在保存对象时，将明文值保存到用户存储中。

“Untagged encrypted”（未加标记的已加密）

表示该属性先前已在用户存储中加密，且未在加密文本的开头包含加密算法标记名称。

“Data Type”（数据类型）

指定用户控制台中的管理对象属性的值的数据类型。 可以从以下列表中进行选择：

- READONLY
- WRITEONCE
- READWRITE

“Maximum Length”（最大长度）

指定管理对象属性的值的最大长度

默认值：0

“Validation Rule Set”（验证规则集）

指定用于验证管理对象属性的值的验证规则集。 可以从以下列表中进行选择：

- “User Validation”（用户验证）
- “Phone Format”（电话格式）
- “International Phone Format”（国际电话格式）

“Back”（返回）按钮

单击此按钮返回“Basic Object Attribute Definition”（基本对象属性定义）屏幕，以便进行修改。

“Next”（下一步）按钮

单击此按钮前往“Configure Managed Objects”（配置管理对象）屏幕。在此屏幕中，您可以选择要配置的下一个管理对象。 配置管理对象后，选择“Show summary and the deploy directory”（显示摘要并部署目录）以查看目录信息和部署该目录。

更多信息

管理敏感属性 (p. 62)

“Confirmation”（确认）屏幕

此屏幕会显示目录详细信息的摘要。

此屏幕中出现的字段已在下表中列出：

“Connection Details”（连接详细信息）

为用户目录指定连接详细信息。

“User/Group/Organization Details”（用户/组/组织详细信息）

指定对 directory.xml 所做的更改。

“Back”（返回）按钮

单击此按钮修改向导中的任何详细信息。

“Save”（保存）按钮

单击此按钮保存您的选择。

“完成”按钮

如果所有的目录详细信息正确，请单击退出向导。

已验证配置，且已创建目录。然后返回到新建目录所在的“Directories”（目录）列表页面。 要编辑或导出新建目录，请从目录列表中选择它。

使用 XML 配置文件创建目录

您可以通过在管理控制台中导入已完成的 directory.xml 文件，来创建或更新 CA Identity Manager 目录。

注意：如果您正在使用 directory.xml 文件而不是使用目录配置向导创建目录，确保您已经修改默认配置模板。 有关详细信息，请参阅 *《配置指南》*。

遵循这些步骤:

1. 通过在浏览器中输入以下 URL 打开管理控制台：

   http://*hostname*:*port*/iam/immanage

   hostname

   定义安装了 CA Identity Manager 的服务器的完全限定域名。

   端口

   定义应用程序服务器端口号。

2. 单击“Directories”（目录）。

   此时显示 CA Identity Manager 目录窗口。

3. 单击“Create or Update from XML”（通过 XML 创建或更新）。

4. 输入用于创建 CA Identity Manager 目录的目录配置 XML 文件的路径和文件名，或浏览文件。 单击“Next”（下一步）。

5. 向此窗口的字段提供值，如下所示：

   注意：在此窗口中显示的字段取决于您在第 4 步中在目录配置文件中提供的用户存储类型和信息。 如果您已经向目录配置文件中的这些字段中任一个提供值，CA Identity Manager 不提示您再次提供这些值。

   “Name”（名称）

   确定您正在创建的 CA Identity Manager 目录的名称。

   “Description”（说明）

   （可选）说明 CA Identity Manager 目录。

   “Connection Object Name”（连接对象名称）

   指定 CA Identity Manager 目录说明的用户目录的名称。输入下列详细信息之一：

   - 如果 CA Identity Manager 没有与 SiteMinder 集成，为 CA Identity Manager 用来连接到用户存储的对象指定任何有意义的名称。
   - 如果 CA Identity Manager 与 SiteMinder 整合，并且您想在 SiteMinder 中创建用户目录连接对象，指定任何有意义的名称。 CA Identity Manager 使用您指定的名称在 SiteMinder 中创建用户目录连接对象。
   - 如果 CA Identity Manager 与 SiteMinder 集成，您想连接到现有的 SiteMinder 用户目录，准确指定 SiteMinder 用户目录连接对象的名称，与显示在策略服务器用户界面中的名称相同。

   “JDBC Data Source JNDI Name”（JDBC 数据源 JNDI 名称）（仅针对关系目录）

   指定 CA Identity Manager 用来连接到数据库的现有 JDBC 数据源的名称。

   “Host”（主机）（仅针对 LDAP 目录）

   指定安装用户目录系统的主机名或 IP 地址。

   对于 CA Directory 用户存储，使用主机系统的完整域名。 不要使用本地主机。

   对于 Active Directory 用户存储，指定域名，而不是 IP 地址。

   “Port”（端口）（仅针对 LDAP 目录）

   指定用户目录的端口号。

   “Provisioning Domain”（配给域）

   CA Identity Manager 管理的配给域。

   注意：“Provisioning Domain”（配给域）名区分大小写。

“Username/User DN”（用户名/用户 DN）

指定可以访问用户存储的帐户的用户名。

对于配给用户存储，您指定的用户帐户必须具有域管理员的配置文件，或者对于配给域相等的权限集。

“Password”（密码）

指定您在用户名（对于关系数据库）或用户 DN 字段（对于 LDAP 目录）指定的用户帐户的密码。

“Confirm Password”（确认密码）

再次输入您在“Password”（密码）字段输入的密码以确认。

“Secure Connection”（安全连接）（仅针对 LDAP 目录）

表示 CA Identity Manager 是否使用安全连接。

确保为 Active Directory 用户存储选择此选项。

单击“Next”（下一步）。

6. 查看 CA Identity Manager 目录的设置。 单击“Finish”（完成）以使用当前设置创建 CA Identity Manager 目录，或单击“Previous”（上一步）进行修改。

   状态信息显示在“Directory Configuration Output”（目录配置输出）窗口中。

7. 单击“Continue”（继续）退出。

   CA Identity Manager 创建该目录。

启用配给服务器访问

通过使用管理控制台中的“Directories”（目录）链接，启用对配给服务器的访问。

注意：此步骤的先决条件是在 CA Directory 上安装配给目录。有关详细信息，请参阅*《安装指南》*。

遵循这些步骤:

1. 通过在浏览器中输入以下 URL 打开管理控制台：

   `http://hostname:port/iam/immanage`

   hostname

   定义安装了 CA Identity Manager 服务器的系统的完全限定主机名。

   port

   定义应用程序服务器端口号。

2. 单击“Directories”（目录）。

   此时显示 CA Identity Manager 目录窗口。

3. 单击“Create from Wizard”（通过向导创建）。

4. 为配置配给目录输入目录 XML 文件的路径和文件名。 它存储在“Administrative Tools”文件夹的 directoryTemplates\ProvisioningServer 中。该文件夹的默认位置是：

   - Windows：<安装路径>\tools
   - UNIX：<安装路径 2>/tools

   注意：您可以不做修改，直接使用安装时的这一目录配置文件。

5. 单击“Next”（下一步）。

6. 在此窗口为这些字段提供值，如下所示：

   “Name”（名称）

   是与您正在配置的配给服务器关联的配给目录的名称。

   - 如果 CA Identity Manager 没有与 SiteMinder 集成，为 CA Identity Manager 用来连接到用户目录的对象指定一个有意义的名称。
   - 如果 CA Identity Manager 与 SiteMinder 集成，您有两种选择：

     如果您想在 SiteMinder 中创建用户目录连接对象，指定任何有意义的名称。 CA Identity Manager 使用您指定的名称在 SiteMinder 中创建此对象。

     如果您想连接到现有的 SiteMinder 用户目录，准确指定 SiteMinder 用户目录连接对象的名称，与显示在策略服务器用户界面中的名称相同。

   “Description”（说明）

   （可选）说明 CA Identity Manager 目录。

   “Host”（主机）

   指定安装用户目录系统的主机名或 IP 地址。

   “Port”（端口）

   指定用户目录的端口号。

   “Domain”（域）

   指定 CA Identity Manager 所管理的配给域的名称。

   重要说明！ 在通过管理控制台创建配给目录时，如果使用英语以外的语言字符作为域名，配给目录创建会失败。

   名称必须匹配您在安装期间指定的配给域的名称。

   注意：域名区分大小写。

   “Username”（用户名）

   指定可以登录到配给管理器的用户。

   该用户帐户必须具有域管理员的配置文件，或者对于配给域相等的权限集。

“Password”（密码）

指定您在“用户名”字段指定的全局用户的密码。

“Confirm Password”（确认密码）

再次输入您在“Password”（密码）字段输入的密码以确认。

“Secure Connection”（安全连接）

表示 CA Identity Manager 是否使用安全连接。

确保为 Active Directory 用户存储选择此选项。

“Directory Search Parameters”（目录搜索参数）

maxrows 定义搜索用户目录时 CA Identity Manager 可以返回的结果的最大数目。 此值覆盖在 LDAP 目录中设置的任何限制。 在应用冲突的设置时，LDAP 服务器使用最低的设置。

注意：maxrows 参数不限制在 CA Identity Manager 任务屏幕上显示的结果数。 要配置显示设置，请在 CA Identity Manager 用户控制台中修改列表屏幕定义。 有关说明，请参阅 *《User Console Design Guide》*。

timeout 确定 CA Identity Manager 在终止搜索之前搜索目录的最大秒数。

“Failover Connections”（故障切换连接）

作为备用配给服务器的一个或多个可选系统的主机名和端口号。如果列出了多个服务器，CA Identity Manager 尝试按列出的顺序连接各个系统。

如果主配给服务器发生故障，使用备用的配给服务器。在主配给服务器再次可用时，仍然继续使用备用配给服务器。如果您转回使用该配给服务器，请重新启动备用配给服务器。

7. 单击“Next”（下一步）。
8. 选择要管理的对象，如“Users”（用户）或“Groups”（组）。
9. 在您根据需要配置对象之后，单击“Show summary deploy directory”（显示摘要并部署目录），查看配给目录的设置。
10. 单击这些操作之一：
    a. 单击“Back”（返回）进行修改。
    b. 如果您想之后返回进行部署，单击“Save”（保存）以保存目录信息。
    c. 单击“Finish”（完成）以完成此步骤并开始使用配给配置环境 (p. 165)。

查看 CA Identity Manager 目录

执行以下步骤，以查看 CA Identity Manager 目录。

遵循这些步骤:

1. 在 CA Identity Manager 管理控制台中，单击“Directories”（目录）。
2. 单击 CA Identity Manager 目录的名称以进行查看。“Directory Properties”（目录属性）窗口出现，显示 CA Identity Manager 目录属性。

CA Identity Manager 目录属性

CA Identity Manager 目录属性如下所示：

注意：显示的属性取决于与 CA Identity Manager 目录关联的数据库或目录的类型。

“Name”（名称）

定义 CA Identity Manager 目录的唯一名称。

“Description”（说明）

提供 CA Identity Manager 目录的说明。

“Type”（类型）

定义目录提供程序的类型。

“Connection Object Name”（连接对象名称）

显示 CA Identity Manager 目录说明的用户目录的名称。

如果 CA Identity Manager 与 SiteMinder 集成，连接对象名称与 SiteMinder 用户目录连接的名称匹配。

“Root Organization”（根组织）（针对包括组织的用户存储）

指定用户存储的入口点。

对于 LDAP 目录，将根组织指定为 DN。 对于关系数据库，显示根组织的唯一标识符。

“JDBC Data Source”（JDBC 数据源）

指定 CA Identity Manager 用来连接到数据库的 JDBC 数据源的名称。

URL

提供用户存储的 URL 或 IP 地址。

“Username”（用户名）

指定可以访问用户存储的帐户的用户名。

“Search Maximum Rows”（搜索最大行）

表示作为搜索结果的返回行的最大数目。

“Search Page Size”（搜索页大小）

指定在一次搜索中可以返回的对象数目。 如果对象的数目超过页面大小，CA Identity Manager 将执行多个搜索。

注意：CA Identity Manager 管理的用户存储必须支持分页。一些用户存储类型可能需要其他配置来支持分页。 有关详细信息，请参阅*《配置指南》*。

“Supports Paging”（支持分页）

表示该目录支持分页。

“Search Timeout”（搜索超时）（仅针对 LDAP 目录）

指定 CA Identity Manager 在终止搜索之前搜索用户存储的最大秒数。

“Provisioning Domain”（配给域）（仅针对配给服务器目录）

CA Identity Manager 管理的配给域。

CA Identity Manager“Directory Properties”（目录属性）窗口

CA Identity Manager 目录的一般信息位于您选择的目录的属性窗口。“Directory Properties”（目录属性）窗口分为以下几部分：

“Directory Properties”（目录属性）

显示 CA Identity Manager 目录（如果该环境启用配给，包括关联的配给域）的基本属性。

“Managed Objects”（管理对象） (p. 150)

提供 CA Identity Manager 管理的用户存储对象的类型的说明。

“Validation Rule Sets”（验证规则集） (p. 154)

列出适用于 CA Identity Manager 目录的验证规则集。

“Environments”（环境）

列出与 CA Identity Manager 目录关联的环境。 一个目录可以与多个 CA Identity Manager 环境关联。

要查看有关 CA Identity Manager 环境的详细信息，请单击该环境的名称。

要修改 CA Identity Manager 目录中的属性，按照更新 CA Identity Manager 目录 (p. 156)中的描述导入目录配置文件。

除查看属性之外，您也能执行以下操作：

“Update Authentication”（更新身份验证）

允许管理员更改 CA Identity Manager 用来验证管理控制台管理员的目录。 管理员也能在现有身份验证目录中添加其他管理控制台管理员。

注意：只有本地 CA Identity Manager 安全保护管理控制台时“Update Authentication”选项才能应用。有关启用本地安全性或使用其他安全方式的信息，请参阅*《配置指南》*。

“Export”（输出） (p. 156)

将目录定义导出为 XML 文件。在导出目录设置之后，您可以修改 XML 文件，然后将它重新导入以更新该目录。 您也能将该 XML 文件导入到其他目录，以便为该目录配置相同设置。

“Update”（更新） (p. 156)

允许管理员添加或更改对象属性等管理对象定义、设置搜索参数并更改目录属性。

如何查看管理对象特性和属性

管理对象描述用户存储中某一类型的条目（如用户、组或组织）。 适用于管理对象的特性和属性也适用于该类型的所有条目。 例如，用户配置文件包括用户管理对象的所有特性和属性。

要查看管理对象的详细信息，请单击对象的名称以打开“Managed Object Properties”（管理对象特性）窗口。

“Managed Object Properties”（管理对象特性）

“Managed Object Properties”（管理对象特性）窗口说明一种管理对象的特性和属性。

“Managed Object Properties”（管理对象特性）窗口相关信息取决于您正在管理的用户存储的类型。 对象的管理特性如下所示：

“Description”（说明）

提供管理对象说明。

“Type”（类型）

表明管理对象表示的条目类型。 对象类型可以是下列类型之一：

- 用户
- 组
- 组织

“Object Class”（对象类）（仅针对 LDAP 目录）

为管理对象指定对象类。 一个管理对象可能有多个对象类。

“Sort Order”（排序顺序）（仅针对 LDAP 目录）

指定 CA Identity Manager 用来在自定义业务逻辑中对搜索结果进行排序的属性。 “Sort Order”（排序顺序）不影响用户控制台中搜索结果的顺序。

例如，在您为用户对象指定 cn 属性时，CA Identity Manager 会根据 cn 属性按字母顺序对搜索用户的结果进行排序。

“Primary Table”（主表）（仅针对关系数据库）

指定包含管理对象的唯一标识符的表。

“Maximum Rows”（最大行数）

指定搜索此类型的对象时 CA Identity Manager 可以返回的结果的最大数目。 在结果的数目超过限制时，显示错误。

设置最大行可以覆盖限制搜索结果的 LDAP 目录的设置。在应用冲突的设置时，LDAP 服务器使用最低的设置。

“Page Size”（页面大小）

指定在一次搜索中可以返回的对象数目。 如果对象的数目超过页面大小，CA Identity Manager 将执行多个搜索。

注意：CA Identity Manager 管理的用户存储必须支持分页。一些用户存储类型可能需要其他配置来支持分页。 有关详细信息，请参阅*《配置指南》*。

容器属性（仅针对 LDAP 目录）

在 LDAP 目录中，*容器*组包含特定类型的对象。 在指定容器时，CA Identity Manager 仅处理容器中的条目。例如，如果您指定容器 ou=People 时，CA Identity Manager 仅处理“People”容器中的用户。

注意：位于 LDAP 目录中但不在定义的容器中的用户和组，可能会显示在用户控制台中。 在管理那些用户和组时，可能会遇到问题。

容器仅对用户和组分组。 不能为组织指定容器。

容器的属性如下所示：

objectclass

指定创建特定类型对象的容器的 LDAP 对象类。例如，用户容器的默认值为“top,organizationalUnit,”，这表示用户在 LDAP 组织单元 (ou) 中创建。

ID

指定存储容器名称的属性，例如 ou。 属性与“名称”值配对以形成容器的相关的 DN，如下列所示：

ou=People

名称

指定容器名称。

次表属性（仅针对关系数据库）

次表包含管理对象的其他属性。 例如，名为“tblUserAddress”的次表可以包含用户管理对象的街道、城市、省/自治区/直辖市以及邮政编码属性。

显示次表的下列属性：

表

指定表的名称。

参考

描述主表和次表之间的映射。

使用下列格式显示参考：

primarytable.attribute=secondarytable.attribute

例如，tblUsers.id = tblUserAddress.userid 表示主表 tblUsers 的 id 属性映射到 tblUserAddress 表的 userid 属性。

“Managed Object Properties”（管理对象特性）窗口的“Attribute Properties”（属性特性）

为“Managed Object Properties”（管理对象特性）窗口中的属性显示下列特性：

显示名称

属性用户友好名称。 在用户控制台中为特定任务设计任务窗口时，此名称显示在可用属性列表中。

物理名

用户存储中的属性的名称。

Well-Known 名称

常用名称表示在 CA Identity Manager 中有特别意义的属性，如用于存储用户密码的属性。

“Attribute Properties”（属性特性）窗口中的“Attribute Properties”（属性特性）

您可以通过单击特性名称以打开“Attribute Properties”（属性特性）窗口，来查看关于属性的附加信息。

“Attribute Properties”（属性特性）窗口中显示下列属性特性：

说明

提供属性说明。

物理名

指定用户存储中属性的名称。

对象类（仅针对 LDAP 目录中的用户、组和组织属性）

在属性不是为用户对象指定的主要对象类的一部分时，是用户属性的 LDAP 附属类。

您只能为用户和组对象指定辅助对象类。

Well-Known 名称

表示在 CA Identity Manager 中有特别意义的属性，如用于存储用户密码的属性。

必需

表示是否为属性必要值，如下所示：

- true 表示属性必须有值。
- false 表示值是可选的。

只读

表示属性的权限级别，如下所示：

- true 表示属性无法修改。
- false 表示属性能够被修改。

隐藏

表示某一属性是否可以显示在特定任务的任务窗口中。

隐含属性常常用于逻辑属性方案。

注意：有关详细信息，请参阅 *《Programming Guide for Java》*。

支持多个值

指出属性是否可以有多个值，如下所示（例如，用于存储组成员的属性是多值的）：

- true 表示属性可以支持多个值。
- false 表示属性只能有一个值。

“Multiple Value Delimiter”（多值分隔符）（仅针对关系数据库）

在一列中存储多个值时分隔值的字符。

“System Attribute”（系统属性）

表示属性是否只能由 CA Identity Manager 使用，如下所示：

- true 表示属性是系统属性。 不能将该属性添加到任务窗口。
- false 表示用户可以使用此属性。 属性可以显示在任务窗口上。

数据类型

指定该属性的数据类型。 默认值为 String。

“Maximum Length”（最大长度）

指定属性值可以允许的最大长度。 如果设置为 0，则值的长度没有限制。

“Validation Rule Set”（验证规则集）

在属性与验证规则集关联时，指定验证规则集的名称。

“Validation Rule Sets”（验证规则集）

验证规则会强制性要求用户在任务窗口字段中输入的数据。 此要求可以强制限制数据类型或格式，也可以确保该数据在任务窗口的其他数据上下文中是有效的。

一个或多个验证规则划分到一个验证规则集。 验证规则集然后与配置文件属性关联。 例如，您可以创建包含“格式日期”有效性规则的验证规则集，它会强制使用 mm-dd-yyyy 的日期格式。您然后可以将验证规则集与存储员工的开始日期的属性关联在一起。

注意：您在目录的配置文件或用户控制台中创建验证规则和规则集。

“Managed Object Properties”（管理对象特性）窗口显示适用于 CA Identity Manager 目录的验证规则集的列表。 要查看验证规则集的详细信息，请单击该规则集的名称以打开“Validation Rule Set Properties”（验证规则集特性）窗口。

“Validation Rule Properties”（验证规则特性）

下列信息显示在“Validation Rule Properties”（验证规则特性）窗口中：

名称

提供验证规则的名称。

说明

提供规则说明。

类

提供实施验证规则的 Java 类名称。

除非验证规则是在 Java 类中定义的，否则不会显示此字段。

文件名

提供包含验证规则的 JavaScript 实施文件的名称。

除非验证规则是在文件中定义的，否则不会显示此字段。

正则表达式

提供实施验证规则的正则表达式。

除非验证规则是作为正则表达式定义的，否则不会显示此字段。

“Validation Rule Set Properties”（验证规则集特性）

下列信息显示在“Validation Rule Set Properties”（验证规则集特性）窗口中：

名称

指定验证规则集的名称。

说明

提供验证规则集的说明。

“Validation Rule Set Properties”（验证规则集特性）页面也包含集中的验证规则的列表。您可以单击验证规则的名称以打开“Validation Rule Properties”（验证规则特性）窗口。

如何更新 CA Identity Manager 目录的设置

要查看 CA Identity Manager 目录的当前设置，请导出目录设置并将其另存为 XML 文件。

在导出目录设置之后，您可以修改并重新导入该 XML 文件以更新该目录。您也能将该 XML 文件导入到其他目录，以便为该目录配置相同设置。

导出 CA Identity Manager 目录

执行以下步骤，以导出 CA Identity Manager 目录。

遵循这些步骤:

1. 单击“目录”。

   此时显示 CA Identity Manager 目录列表。

2. 单击要导出的目录的名称。

   显示“CA Identity Manager 目录属性”窗口。

3. 在属性窗口的底部，单击“导出”。
4. 出现提示时，保存 XML 文件。

更新 CA Identity Manager 目录

更新 CA Identity Manager 目录的目的是：

- 添加或更改管理对象定义，包括对象的属性。
- 设置搜索参数
- 更改目录属性

注意：CA Identity Manager 不删除对象或属性定义。

目录配置文件可以只包含需要进行的更改。不需要包括已经定义的特性或属性。

注意：如果有一个 CA Identity Manager 节点群集，当在管理控制台中进行更改时，只能启用一个 CA Identity Manager 节点。 在您创建或修改 CA Identity Manager 目录之前，阻止除了一个以外的所有其余的 CA Identity Manager 节点。

遵循这些步骤:

1. 将当前 CA Identity Manager 目录设置导出到 XML 文件。
2. 修改 XML 文件以反映您的更改。
3. 单击“Directories”（目录）。

   此时显示 CA Identity Manager 目录列表。

4. 单击要更新的目录的名称。

   显示“Properties for the CA Identity Manager directory”（CA Identity Manager 目录属性）。

5. 在属性窗口的底部，单击“Update”（更新）。

6. 输入用来更新 CA Identity Manager 目录的 XML 文件的路径和文件名，或者浏览到该文件。 单击“Finish”（完成）。

   状态信息显示在“Directory Configuration Output”（目录配置输出）字段中。

7. 单击“Continue”（继续）。

删除 CA Identity Manager 目录

在您删除 CA Identity Manager 目录之前，删除与它关联的任何一个 CA Identity Manager 环境。

遵循这些步骤:

1. 在管理控制台中单击“Directories”（目录）。

   此时显示 CA Identity Manager 目录列表。

2. 选中要删除的目录左侧的复选框。
3. 单击“Delete”（删除）。

   此时显示确认消息。

4. 单击“OK”（确定）确认删除。

第 6 章： CA Identity Manager 环境

此部分包含以下主题：

CA Identity Manager 环境

CA Identity Manager 环境是用户存储的视图。 在 CA Identity Manager 环境中，可以管理用户、组、组织、任务和角色。 您也能在管理端点（如电子邮件帐户或其他应用程序）提供用户帐户。

使用管理控制台，您可以完成以下任务：

- 创建、修改或删除 CA Identity Manager 环境。
- 导出和导入 CA Identity Manager 环境。
- 配置高级设置
- 导入角色和任务
- 重置系统管理员帐户

创建 CA Identity Manager 环境的先决条件

在您开始之前，使用下表中的工作表收集您需要的信息：

CA Identity Manager 环境配置工作表	
所需信息	**值**
选择的有意义的 CA Identity Manager 环境名称。 例如：MyEnvironment	

CA Identity Manager 环境配置工作表	
所需信息	**值**
CA Identity Manager 用来为环境的默认密码策略形成重定向 URL 的基本 URL。 例如： http://server.yourcompany.org	
添加到 URL 以访问环境中受保护任务的别名。 例如： http://server.yourcompany.org/iam/im/alias	
添加到 URL 以访问公共任务（如自行注册和忘记密码任务）的别名。 例如： http://server.yourcompany.org/iam/im/public_alias/index.jsp?task.tag=SelfRegistration **注意：**当您的环境不包括公共任务时，您不需要指定公共别名。	
如果您提供公共别名，则为作为公共用户的现有的用户名。CA Identity Manager 在访问公共任务时使用公共用户的凭据，而不是用户提供的凭据。	
CA Identity Manager (p. 87) 的名称	
如果 CA Identity Manager 环境支持配给，则为配给目录的名称。	
管理 CA Identity Manager 环境的现有的用户的唯一标识符。 例如：myadmin	
CA Identity Manager 与 SiteMinder 进行整合时保护 CA Identity Manager 环境的 SiteMinder 代理或代理组的名称。	

创建 CA Identity Manager 环境

通过 CA Identity Manager 环境，您可以管理具有一组角色和任务的目录中的对象。 使用 CA Identity Manager 环境向导来指导您完成创建 CA Identity Manager 环境的步骤。

在创建 CA Identity Manager 环境之前注意下列几点：

- 假定您正在使用 LDAP 用户存储，并且您已经配置用户容器（如您的 CA Identity Manager 目录的目录配置文件 (directory.xml) 中的 ou=People）。 确认在您创建 CA Identity Manager 环境时，您选择的用户存在于该容器。 选择用户容器中不存在的用户帐户可能导致失败。
- 在您配置 CA Identity Manager 环境，以便管理具有扁平型或用户扁平型结构的 LDAP 用户目录时，选定的用户的配置文件必须包括用户的组织。 为帮助确保正确配置了用户的配置文件，请将用户组织名添加到与 directory.xml file (p. 75) 文件中的 %ORG_MEMBERSHIP% 常用属性一致的物理属性中。 例如，如果物理属性说明映射到 directory.xml 文件的 %ORG_MEMBERSHIP% 常用属性，并且用户属于该员工组织时，用户的配置文件必须包含属性/值对 description=Employees。

遵循这些步骤:

1. 如果 CA Identity Manager 使用策略服务器群集，请阻止除了一个策略服务器以外的所有其余策略服务器。
2. 如果您有一串 CA Identity Manager 节点，请阻止除了一个以外的所有其余 CA Identity Manager 节点。
3. 在管理控制台中单击“Environments”（环境）。
4. 单击“New”（新建）。

   此时将打开“CA Identity Manager environment”（CA Identity Manager 环境）向导。
5. 提供以下信息：
   - **“Environment name”（环境名称）**

     为环境指定唯一名称
   - **“Description”（说明）**

     描述环境
   - **“Protected alias”（受保护别名）**

     指定唯一名称，如员工。此别名被添加到 URL，以在 CA Identity Manager 环境中访问受保护的任务。例如，如果别名是员工，访问员工环境的 URL 是 http://my*server.mycompany.com*/iam/im/employees

     注意：别名是区分大小写的并且不能包含空格。我们建议在您指定别名的时候，使用小写字母，不加标点或空格。

- **“Base URL”（基本 URL）**

  为 CA Identity Manager 指定 URL。URL 需要主机名；不能包括本地主机。此外，不要包括别名，例如 http://*myserver.mycompany.com*/iam/im。

  如果您正在使用 Web 代理，请确保更改基本 URL 以反映 Web 代理的 URL。

  注意：如果您正在使用 Web 代理来保护 CA Identity Manager 资源，不要在“Base URL”（基本 URL）字段指定端口号。 如果您使用 Web 代理，且基本 URL 包含端口号，则与 CA Identity Manager 任务的链接将无法正常工作。

  有关保护 CA Identity Manager 资源的详细信息，请参阅您的应用程序服务器的*《安装指南》*。

  单击“Next”（下一步）。

6. 选择 CA Identity Manager 目录来与您正在创建的环境关联，然后单击“Next”（下一步）。

7. 如果 CA Identity Manager 环境支持配给，选择要使用的适当配给服务器。

   注意：如果已经选择配给目录作为 CA Identity Manager 目录，不建议选择配给服务器。

8. 为公共任务配置支持。 通常，这些任务是自助服务任务，例如自行注册或忘记密码任务。 用户不需要登录即可访问公共任务。

   注意：要使用户能够使用自助服务任务，需要配置公共任务支持。

   a. 指定添加到 URL 的唯一名称，用于访问公共任务。

      示例：您将使用以下 URL 来访问默认自行注册任务：

      http://*myserver.mycompany.com*/iam/im/*alias*/index.jsp?task.tag=SelfRegistration

      在此 URL 中，*别名*是您提供的唯一名称。

   b. 指定下列现有的用户帐户之一，作为公共用户帐户。CA Identity Manager 使用此帐户来允许未知用户无需提供凭据即可访问公共任务。

      - LDAP 用户输入唯一标识符或公共用户帐户的相关 DN。确保此值映射到 %USER_ID% 常用属性 (p. 69)。 例如，如果用户 DN 的 DN 是 uid=Admin1、ou=People、ou=Employees、ou=NeteAuto，输入“Admin1”。

      - 关系数据库用户可输入映射到目录配置文件的 %USER_ID% 常见属性的值，或用户的唯一标识符。

   单击“Validate”（验证）以查看用户的完全标识符。

9. 选择要为此环境创建的任务和角色。 您可以完成以下任务：

   - **“Create default roles”（创建默认角色）**

     创建环境中最初提供的一组默认任务和角色。管理员可以使用这些任务和角色作为模板，在用户控制台中创建新的任务和角色。

- **“Create only the system manager role”（仅创建系统管理员角色）**

  仅仅创建系统管理员角色和相关联的任务。

  需要系统管理员角色来访问环境。

  系统管理员可以在用户控制台中创建新的任务和角色。

- **“Import roles from the file”（从该文件导入角色）**

  导入您从其他的 CA Identity Manager 环境导出的角色定义文件。

  注意：为了使用 CA Identity Manager 环境，角色定义文件必须至少包括系统管理员角色或包含类似任务的角色。

  选择“Import roles from the file”（从该文件导入角色）选项按钮，并且输入角色定义文件的路径和文件名，或浏览到要导入的文件。

10. 选择角色定义文件来创建您的环境的默认任务组，然后单击“Next”（下一步）。

    角色定义文件是 XML 文件，这些文件定义支持特定功能所需的一组任务和角色。 例如，如果您想管理 Active Directory 和 UNIX NIS 端点，请选择那些角色定义文件。

    注意：此步骤是可选的。 如果您不想创建其他默认任务以支持新功能，忽略此屏幕。

11. 如下所示，定义作为此环境系统管理员的用户：

    a. 在“System Manager”字段中，输入映射到目录配置文件的 %USER_ID% 常用属性的值，或指定以下用户帐户之一：

       - LDAP 用户输入用户的唯一标识符或相关 DN。例如，如果用户 DN 的 DN 是 uid=Admin1、ou=People、ou=Employees、ou=NeteAuto，输入“Admin1”。
       - 关系数据库用户输入用户的唯一标识符。

    b. 单击“Add”（添加）。

       CA Identity Manager 将用户的完整标识符添加到用户的列表中。

    c. 单击“Next”（下一步）。

    在指定系统管理员时，注意下列几点：

    - 系统管理员*不能*是与用户存储的管理员同样的用户。
    - 您可以为环境指定多个系统管理员。但是，您只能在管理控制台中指定初始的系统管理员。要指定其他系统管理员，请将系统管理员角色分配给用户控制台中适当的用户。

12. 在“Inbound Administrator”（入站管理员）字段中，指定可以执行映射到入站映射的管理任务的 CA Identity Manager 管理员帐户。

    用户必须能在任何用户上执行所有那些任务。 配给同步管理者角色包含默认入站映射中的配给任务。

13. 输入密钥库的密码，这是加密和解密数据的密钥的数据库。

    定义此密码是定义动态密钥的先决条件。您在使用“系统”、“密钥”任务创建环境之后可以修改密码。

    此时显示概述环境设置的页面。

14. 查看环境设置。单击“Previous”（上一步）进行修改，或者单击“Finish”（完成）以使用当前设置创建 CA Identity Manager 环境。

    “Environment Configuration Output”屏幕显示环境创建的进度。

15. 单击“Continue”（继续）以退出 CA Identity Manager 环境向导。

16. 启动环境。

    单击环境名称，然后单击“Start”（启动）。

17. 如果您在第 1 步中阻止了任何策略服务器，现在请重新启动它们。

如何访问 CA Identity Manager 环境

在创建 CA Identity Manager 环境之后，您可以通过在浏览器中输入 URL 来访问它。

注意：在您用来访问管理控制台的浏览器中，启用 Javascript。

URL 的格式取决于您如何配置环境以及想要访问的任务的类型。

- 要通过用户控制台访问受保护的任务，请使用以下 URL：

  `http://hostname/iam/im/alias`

  hostname

  定义安装 CA Identity Manager 的服务器的完全限定域名－例如，myserver.mycompany.com

  别名

  定义环境别名的别名，例如员工。

  使用授权管理员帐户登录 CA Identity Manager 环境，例如使用您为 CA Identity Manager 环境创建的系统管理员帐户。

  注意：除非您配置公共任务，否则全部 CA Identity Manager 任务都将受到保护。

- 要访问公共任务（不要求用户来提供凭据），请使用下列格式的 URL：

  `http://hostname/iam/im/alias/index.jsp?task.tag=tasktag`

  hostname

  定义安装 CA Identity Manager 的服务器的完全限定域名，例如，myserver.mycompany.com。

别名

定义公共任务的别名，例如，self-service。

task_tag

定义任务的标记，以进行调用。

在用户控制台中配置任务时，可以指定任务标记。

默认自行注册以及忘记密码重置任务的任务标记分别是 SelfRegistration 和 ForgottenPasswordReset。

注意：有关详细信息，请参阅*《管理指南》*。

如何为配给配置环境

在启用对配给服务器的访问 (p. 145)之后，您可以为配给配置环境。

然后，创建称为“入站管理员”的特殊 CA Identity Manager 用户，创建与配给服务器的连接，并且在配给管理器中配置入站同步。

注意：无论何时您修改环境的配给属性，请务必重新启动应用程序服务器，以使更改生效。

配置入站管理员

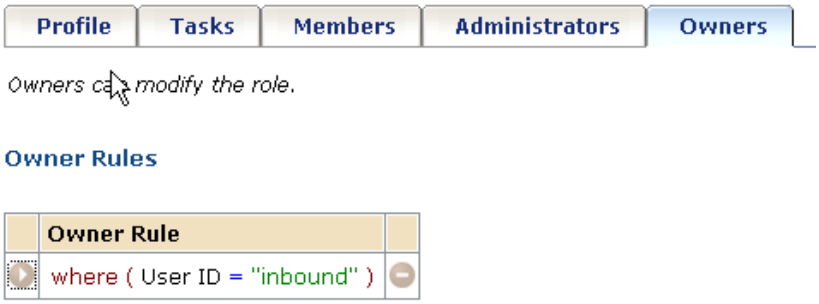
要使入站同步生效，创建称为*入站管理员*的特殊 CA Identity Manager 用户。 在 CA Identity Manager 之前的版本中，入站管理员叫做*企业用户*。没有用户登录到此用户帐户，而是 CA Identity Manager 在内部使用此帐户。 但是，应创建此用户帐户并分配给它适当的任务。

遵循这些步骤:

1. 以具有系统管理员角色的用户身份登录到 CA Identity Manager 环境。
2. 创建用户。 您可以将该用户命名为 **inbound**，以记住其目的。
3. 选择“管理角色”、“修改管理角色”，并选择包含您用于同步的任务的角色。
   - 配给创建用户
   - “Provisioning Enable/Disable User”（配给启用/禁用用户）
   - 配给修改用户

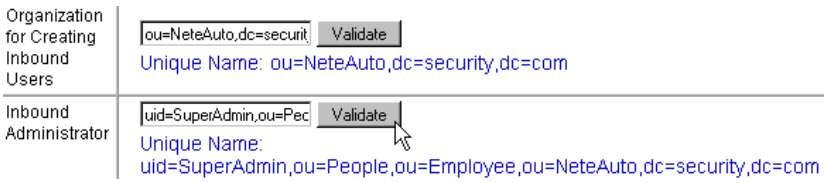
   注意：如果您没修改默认同步任务，使用配给同步管理者角色。

4. 在“成员”选项卡上，添加包含以下内容的成员策略：
   - 新用户符合的成员规则。
   - 提供对触发入站同步的配给目录更改影响的所有用户的访问权的作用域规则。



5. 在管理控制台中：
   a. 选择“Environment”（环境）。
   b. 选择“Advanced Settings”（高级设置）、“Provisioning”（配给）。
   c. 如果 CA Identity Manager 目录包括组织，完成“Organization for Creating Inbound Users”（创建入站用户的组织）字段。

      此组织是在发生入站同步时创建用户的地方。例如，在用户被添加到配给目录时，CA Identity Manager 将用户添加到此组织中。
   d. 使用您在第 2 步中创建的用户的用户 ID，完成“Inbound Administrator”（入站管理员）字段。
   e. 单击“Validate”（验证）以确认接受此用户 ID，如下例中所示，其中完整的用户 ID 显示在输入的用户 ID 下面。



   f. 修改此屏幕上的其他字段。 不需要修改。

      修改时，确认您理解字段交互的方式。有关每个字段的详细信息，请单击屏幕中的“Help”（帮助）链接。

将环境连接到配给服务器

遵循这些步骤:

1. 在管理控制台中单击“Environments”（环境）。

   此时显示现有环境列表。
2. 单击想要与配给服务器关联的环境的名称。

3. 在“Provisioning Server”（配给服务器）字段单击右箭头图标。

   将打开“Provisioning Properties”（配给属性）屏幕。

4. 选择“Provisioning Server”（配给服务器）。
5. 单击屏幕底部的“Save”（保存）。
6. 在配给管理器中配置同步 (p. 167)。

在配给管理器中配置同步

入站同步使 CA Identity Manager 与在配给目录中发生的更改一起更新。 更改包括使用配给管理器进行的更改，以及配给服务器有连接器的端点中的更改。 每个配给服务器各支持单个环境。 然而，如果当前环境不可用，您可以在群集的不同系统上配置备份环境。

遵循这些步骤:

1. 选择“Start”（开始）、“CA Identity Manager”、“Provisioning Manager”（配给管理器）。
2. 单击“System”（系统）、“CA Identity Manager Setup”（CA Identity Manager 安装）。
3. 将安装 CA Identity Manager 服务器的系统名称填入“Host Name”（主机名）字段。
4. 将应用程序服务器端口号填入“Port”（端口）字段。
5. 将环境的别名填入“Environment name”（环境名称）字段。
6. 如果您希望使用 HTTPS 协议与 CA Identity Manager 服务器进行通信，而不是使用 HTTP 并且加密各个通知，选择“安全连接”（Secured Connection）。
7. 单击“Add”（添加）。
8. 对每一个环境的备份版本重复步骤 3-6。

   如果当前环境的应用程序服务器不可用，CA Identity Manager 会故障转移到备份环境。 您可以为当前环境和备份环境重新排序，以设置故障转移顺序。

9. 如果这是第一个环境，在“Shared Secret”（共享密钥）字段中填入在该用户 CA Identity Manager 安装期间为嵌入式组件输入的密码。

   注意：如果在此安装中启用了 FIPS，则不应用这些字段。

10. 如下所示设置日志级别：
    - “No Log”（没有日志）－没有信息写入日志文件。
    - “Error”（错误）－只记录错误消息。
    - “Info”（信息）－记录错误和信息消息（默认）。
    - “Warning”（警告）－记录错误、警告和信息消息。
    - “Debug”（调试）－记录所有信息。
11. 在登录到环境之前重新启动应用程序服务器。

注意：有关入站同步操作和在同步期间遇到的任何问题的日志，请参阅以下文件：

PSHOME\logs\etanotify<date>.log

导入自定义配给角色

在创建环境时，可以选择使用您创建的默认角色或自定义角色定义文件。 如果您导入自定义角色定义，也会导入“仅针对配给”的角色定义。 在您创建环境之后，从 ProvisioningOnly-RoleDefinitions.xml 文件导入角色定义，该文件位于以下文件夹之一：

admin_tools/ProvisioningOnlyRoleDefinitions/Organization
admin_tools/ProvisioningOnlyRoleDefinitions/NoOrganization

admin_tools 的默认位置为：

- **Windows**：C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools
- **UNIX**：/opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

“重置用户密码”任务的帐户同步

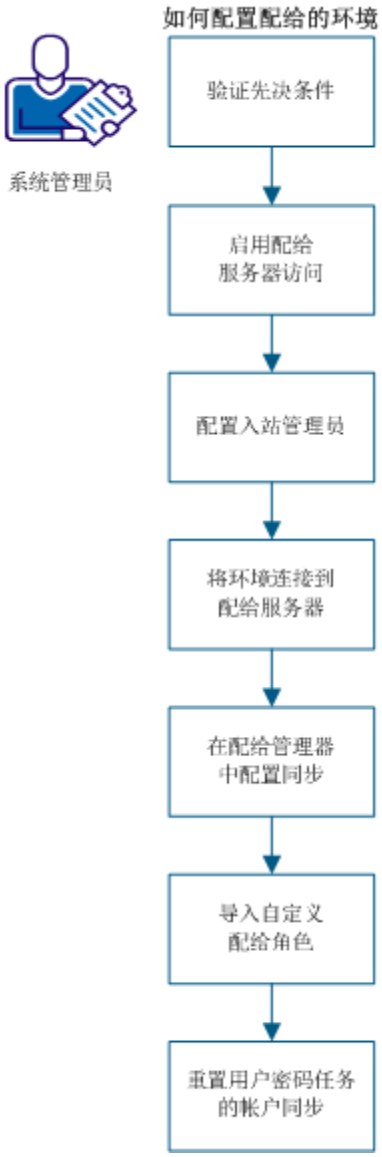
要在 CA Identity Manager 环境中启用配给，应导入一个称为 ProvisioningOnly-RoleDefinitions.xml 的配置文件，该文件将创建用于用户配给的角色和任务。

在该文件中，“重置用户密码”任务的默认帐户同步设置为“关”。（在启用配给之前，同步设置为“任务完成时”。）

要使用“重置用户密码”任务触发帐户同步，请在为启用配给而导入 rovisioningOnly-RoleDefinitions.xml 文件后，设置帐户同步选项。

如何使用 Connector Xpress 创建和部署连接器

您可以为环境配置配给以便向由 CA Identity Manager 管理的用户提供其他系统中的帐户。 帐户为用户提供对其他资源（如电子邮件帐户）的访问权限。 您通过分配您通过 CA Identity Manager 创建的配给角色，提供这些其他帐户。



作为管理员，请完全以下步骤：

1. 验证先决条件 (p. 170)
2. 启用配给服务器访问 (p. 145)
3. 配置入站管理员 (p. 165)
4. 将环境连接到配给服务器 (p. 166)
5. 在配给管理器中配置同步 (p. 167)

6. 导入自定义配给角色 (p. 168)
7. 重置用户密码任务的帐户同步 (p. 168)

验证先决条件

在您为配给配置环境之前，请确保配给目录安装在 CA Directory 上。有关详细信息，请参阅*《安装指南》*。

启用配给服务器访问

通过使用管理控制台中的“Directories”（目录）链接，启用对配给服务器的访问。

注意：此步骤的先决条件是在 CA Directory 上安装配给目录。有关详细信息，请参阅*《安装指南》*。

遵循这些步骤：

1. 通过在浏览器中输入以下 URL 打开管理控制台：

   `http://hostname:port/iam/immanage`

   hostname

   定义安装了 CA Identity Manager 服务器的系统的完全限定主机名。

   port

   定义应用程序服务器端口号。

2. 单击“Directories”（目录）。

   此时显示 CA Identity Manager 目录窗口。

3. 单击“Create from Wizard”（通过向导创建）。
4. 为配置配给目录输入目录 XML 文件的路径和文件名。 它存储在“Administrative Tools”文件夹的 directoryTemplates\ProvisioningServer 中。该文件夹的默认位置是：

   - Windows：<安装路径>\tools
   - UNIX：<安装路径 2>/tools

   注意：您可以不做修改，直接使用安装时的这一目录配置文件。

5. 单击“Next”（下一步）。

6. 在此窗口为这些字段提供值，如下所示：

“Name”（名称）

是与您正在配置的配给服务器关联的配给目录的名称。

- 如果 CA Identity Manager 没有与 SiteMinder 集成，为 CA Identity Manager 用来连接到用户目录的对象指定一个有意义的名称。
- 如果 CA Identity Manager 与 SiteMinder 集成，您有两种选择：

  如果您想在 SiteMinder 中创建用户目录连接对象，指定任何有意义的名称。 CA Identity Manager 使用您指定的名称在 SiteMinder 中创建此对象。

  如果您想连接到现有的 SiteMinder 用户目录，准确指定 SiteMinder 用户目录连接对象的名称，与显示在策略服务器用户界面中的名称相同。

“Description”（说明）

（可选）说明 CA Identity Manager 目录。

“Host”（主机）

指定安装用户目录系统的主机名或 IP 地址。

“Port”（端口）

指定用户目录的端口号。

“Domain”（域）

指定 CA Identity Manager 所管理的配给域的名称。

重要说明！ 在通过管理控制台创建配给目录时，如果使用英语以外的语言字符作为域名，配给目录创建会失败。

名称必须匹配您在安装期间指定的配给域的名称。

注意：域名区分大小写。

“Username”（用户名）

指定可以登录到配给管理器的用户。

该用户帐户必须具有域管理员的配置文件，或者对于配给域相等的权限集。

“Password”（密码）

指定您在“用户名”字段指定的全局用户的密码。

“Confirm Password”（确认密码）

再次输入您在“Password”（密码）字段输入的密码以确认。

“Secure Connection”（安全连接）

表示 CA Identity Manager 是否使用安全连接。

确保为 Active Directory 用户存储选择此选项。

“Directory Search Parameters”（目录搜索参数）

maxrows 定义搜索用户目录时 CA Identity Manager 可以返回的结果的最大数目。 此值覆盖在 LDAP 目录中设置的任何限制。 在应用冲突的设置时，LDAP 服务器使用最低的设置。

注意：maxrows 参数不限制在 CA Identity Manager 任务屏幕上显示的结果数。要配置显示设置，请在 CA Identity Manager 用户控制台中修改列表屏幕定义。 有关说明，请参阅*《User Console Design Guide》*。

timeout 确定 CA Identity Manager 在终止搜索之前搜索目录的最大秒数。

“Failover Connections”（故障切换连接）

作为备用配给服务器的一个或多个可选系统的主机名和端口号。如果列出了多个服务器，CA Identity Manager 尝试按列出的顺序连接各个系统。

如果主配给服务器发生故障，使用备用的配给服务器。在主配给服务器再次可用时，仍然继续使用备用配给服务器。如果您转回使用该配给服务器，请重新启动备用配给服务器。

7. 单击“Next”（下一步）。
8. 选择要管理的对象，如“Users”（用户）或“Groups”（组）。
9. 在您根据需要配置对象之后，单击“Show summary deploy directory”（显示摘要并部署目录），查看配给目录的设置。
10. 单击这些操作之一：
    a. 单击“Back”（返回）进行修改。
    b. 如果您想之后返回进行部署，单击“Save”（保存）以保存目录信息。
    c. 单击“Finish”（完成）以完成此步骤并开始使用配给配置环境 (p. 165)。

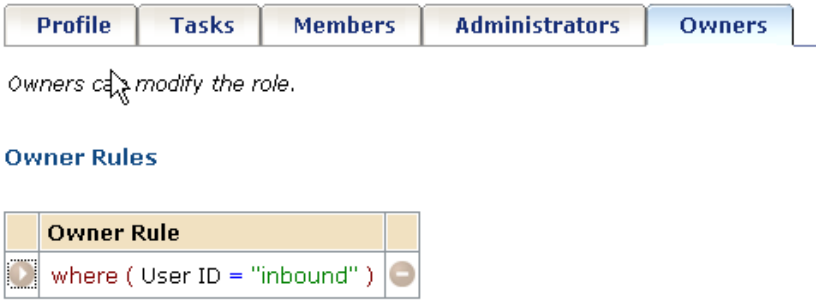
配置入站管理员

要使入站同步生效，创建称为*入站管理员*的特殊 CA Identity Manager 用户。 在 CA Identity Manager 之前的版本中，入站管理员叫做*企业用户*。没有用户登录到此用户帐户，而是 CA Identity Manager 在内部使用此帐户。 但是，应创建此用户帐户并分配给它适当的任务。

遵循这些步骤:

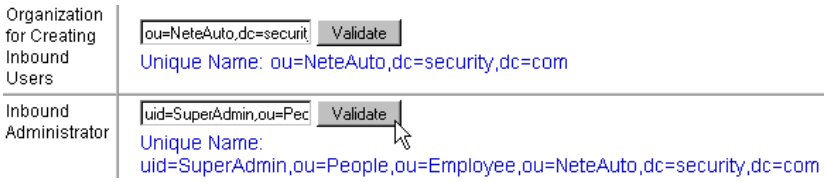
1. 以具有系统管理员角色的用户身份登录到 CA Identity Manager 环境。
2. 创建用户。 您可以将该用户命名为 **inbound**，以记住其目的。
3. 选择“管理角色”、“修改管理角色”，并选择包含您用于同步的任务的角色。
   - 配给创建用户
   - “Provisioning Enable/Disable User”（配给启用/禁用用户）
   - 配给修改用户

   注意：如果您没修改默认同步任务，使用配给同步管理者角色。
4. 在“成员”选项卡上，添加包含以下内容的成员策略：
   - 新用户符合的成员规则。
   - 提供对触发入站同步的配给目录更改影响的所有用户的访问权的作用域规则。



5. 在管理控制台中：
   a. 选择“Environment”（环境）。
   b. 选择“Advanced Settings”（高级设置）、“Provisioning”（配给）。
   c. 如果 CA Identity Manager 目录包括组织，完成“Organization for Creating Inbound Users”（创建入站用户的组织）字段。

      此组织是在发生入站同步时创建用户的地方。例如，在用户被添加到配给目录时，CA Identity Manager 将用户添加到此组织中。
   d. 使用您在第 2 步中创建的用户的用户 ID，完成“Inbound Administrator”（入站管理员）字段。
   e. 单击“Validate”（验证）以确认接受此用户 ID，如下例中所示，其中完整的用户 ID 显示在输入的用户 ID 下面。



f. 修改此屏幕上的其他字段。 不需要修改。

修改时，确认您理解字段交互的方式。有关每个字段的详细信息，请单击屏幕中的“Help”（帮助）链接。

将环境连接到配给服务器

遵循这些步骤:

1. 在管理控制台中单击“Environments”（环境）。

   此时显示现有环境列表。
2. 单击想要与配给服务器关联的环境的名称。
3. 在“Provisioning Server”（配给服务器）字段单击右箭头图标。

   将打开“Provisioning Properties”（配给属性）屏幕。
4. 选择“Provisioning Server”（配给服务器）。
5. 单击屏幕底部的“Save”（保存）。
6. 在配给管理器中配置同步 (p. 167)。

在配给管理器中配置同步

入站同步使 CA Identity Manager 与在配给目录中发生的更改一起更新。 更改包括使用配给管理器进行的更改，以及配给服务器有连接器的端点中的更改。 每个配给服务器各支持单个环境。 然而，如果当前环境不可用，您可以在群集的不同系统上配置备份环境。

遵循这些步骤:

1. 选择“Start”（开始）、“CA Identity Manager”、“Provisioning Manager”（配给管理器）。
2. 单击“System”（系统）、“CA Identity Manager Setup”（CA Identity Manager 安装）。
3. 将安装 CA Identity Manager 服务器的系统名称填入“Host Name”（主机名）字段。

4. 将应用程序服务器端口号填入“Port”（端口）字段。
5. 将环境的别名填入“Environment name”（环境名称）字段。
6. 如果您希望使用 HTTPS 协议与 CA Identity Manager 服务器进行通信，而不是使用 HTTP 并且加密各个通知，选择“安全连接”（Secured Connection）。
7. 单击“Add”（添加）。
8. 对每一个环境的备份版本重复步骤 3-6。

   如果当前环境的应用程序服务器不可用，CA Identity Manager 会故障转移到备份环境。 您可以为当前环境和备份环境重新排序，以设置故障转移顺序。
9. 如果这是第一个环境，在“Shared Secret”（共享密钥）字段中填入在该用户 CA Identity Manager 安装期间为嵌入式组件输入的密码。

   注意：如果在此安装中启用了 FIPS，则不应用这些字段。
10. 如下所示设置日志级别：
    - “No Log”（没有日志）－没有信息写入日志文件。
    - “Error”（错误）－只记录错误消息。
    - “Info”（信息）－记录错误和信息消息（默认）。
    - “Warning”（警告）－记录错误、警告和信息消息。
    - “Debug”（调试）－记录所有信息。
11. 在登录到环境之前重新启动应用程序服务器。

注意：有关入站同步操作和在同步期间遇到的任何问题的日志，请参阅以下文件：

PSHOME\logs\etanotify<date>.log

导入自定义配给角色

在创建环境时，可以选择使用您创建的默认角色或自定义角色定义文件。 如果您导入自定义角色定义，也会导入“仅针对配给”的角色定义。 在您创建环境之后，从 ProvisioningOnly-RoleDefinitions.xml 文件导入角色定义，该文件位于以下文件夹之一：

admin_tools/ProvisioningOnlyRoleDefinitions/Organization
admin_tools/ProvisioningOnlyRoleDefinitions/NoOrganization

admin_tools 的默认位置为：

- **Windows**：C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools
- **UNIX**：/opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

“重置用户密码”任务的帐户同步

要在 CA Identity Manager 环境中启用配给，应导入一个称为 ProvisioningOnly-RoleDefinitions.xml 的配置文件，该文件将创建用于用户配给的角色和任务。

在该文件中，“重置用户密码”任务的默认帐户同步设置为“关”。（在启用配给之前，同步设置为“任务完成时”。）

要使用“重置用户密码”任务触发帐户同步，请在为启用配给而导入 rovisioningOnly-RoleDefinitions.xml 文件后，设置帐户同步选项。

管理环境

本部分说明如何管理环境。

修改 CA Identity Manager 环境属性

通过管理控制台的 CA Identity Manager 环境属性屏幕，您可以完成以下任务：

- 查看环境的当前设置。
- 修改说明、基本 URL 以及受保护别名和公共别名。
- 在升级之后导入现有的 CA Identity Manager 环境。

  注意：有关导入现有 CA Identity Manager 环境的详细信息，请参阅*《安装指南》*的升级部分。
- 启动和停止环境
- 访问用于配置以下任务的页面：
  - **“Advanced Settings”（高级设置）**

    配置高级功能，包括使用 CA Identity Manager API 生成的功能。
  - **“Role and Task Settings”（角色和任务设置）**

    导入您从其他的 CA Identity Manager 环境导出的角色定义文件。
  - **“System Manager”（系统管理员）**

    分配系统管理员角色。

遵循这些步骤:

1. 如果 CA Identity Manager 使用 SiteMinder 策略服务器群集，请阻止除一个以外的所有其他策略服务器。
2. 如果您有一串 CA Identity Manager 节点，请阻止除了一个以外的所有其余 CA Identity Manager 节点。

3. 单击“Environments”（环境）。

   显示 CA Identity Manager 环境屏幕，其中包含 CA Identity Manager 环境列表。

4. 单击 CA Identity Manager 环境的名称以进行修改。

   “CA Identity Manager Properties”（CA Identity Manager 属性）屏幕出现并显示以下属性：

   OID

   定义环境的唯一标识符。 在您创建 CA Identity Manager 环境时，CA Identity Manager 会生成此标识符。

   通过任务持久性数据库配置任务删除时，请使用此 OID。 请参阅*《安装指南》*。

   “Name”（名称）

   指定 CA Identity Manager 环境的唯一名称。

   “Description”（说明）

   提供 CA Identity Manager 环境的说明。

   “CA Identity Manager Directory”（CA Identity Manager 目录）

   指定环境关联的 CA Identity Manager 目录。

   “Enable Verbose Log Output”（启用详细日志输出）

   控制在您导入环境时，CA Identity Manager 在环境日志中记录和显示的信息量。在您从文件导入环境或其他对象定义时，环境日志显示在管理控制台的状态窗口中。

   注意：选中此复选框会显著影响性能。

   详细日志包括环境中的每个对象（任务、屏幕、角色和策略）和其属性的验证和部署消息。

   要查看详细日志，请选中此复选框并且保存“环境”属性。 当您通过文件导入角色或其他设置时，日志中会显示附加信息。

   “Provisioning Server”（配给服务器）

   指定用作配给用户存储的配给目录。

   单击右箭头按钮以在“Provisioning Properties”（配给属性）页面中配置配给目录。

   “Version”（版本）

   定义 CA Identity Manager 的版本号。

“Base URL”（基本 URL）

指定不包括环境的受保护别名或公共别名的 CA Identity Manager URL 部分。

CA Identity Manager 使用基本 URL 来形成重定向 URL，来在环境默认密码策略中指向密码服务任务。

“Protected Alias”（受保护别名）

在 CA Identity Manager 环境用户控制台中，定义访问受保护任务的基本 URL 名称。

“Public Alias”（公共别名）

定义访问公共任务（如自行注册和忘记密码任务）的基本 URL 名称。

“Public User”（公共用户）

定义 CA Identity Manager 用来代替用户提供的凭据访问公共任务的用户帐户。

“Job Timeout”（作业超时）

确定在任务被提交之后，在显示状态消息之前 CA Identity Manager 等待的时间。

此值在“高级设置”的“用户控制台”页面中设置。

“Status”（状态）

停止或重新启动 CA Identity Manager 环境。

“Migrate Task Persistence Data from CA Identity Manager 8.1”（从 CA Identity Manager 8.1 迁移任务持久性数据）

将数据从 CA Identity Manager 8.1 任务持久性数据库迁移到 CA Identity Manager 12.6.4 任务持久性数据库。

有关详细信息，请参阅 *《安装指南》*。

注意：只有在 CA Identity Manager 的先前版本创建并迁移到 CA Identity Manager 12.6.4 的环境中才会显示“Migrate Task Persistence Data from CA Identity Manager 8.1”（从 CA Identity Manager 8.1 迁移任务持久性数据）按钮。

5. 根据需要修改说明、基本 URL 或受保护域名或公共别名。
6. 如果您修改了任何环境属性，请重新启动 CA Identity Manager 环境。
7. 如果您在第 1 步中阻止了任何策略服务器，现在请重新启动它们。

环境设置

环境专用信息存储在三个环境设置文件中：

- *alias*_environment_roles.xml
- *alias*_environment_settings.xml
- *alias*_environment.xml

注意：*alias* 是指环境的别名。 在创建环境时指定别名。

在导出环境设置时，生成包含这些文件的 ZIP 文件，这些文件反映当前配置。

在您导出环境设置之后，导入这些设置以完成下列任务之一：

- 使用类似设置管理多个环境。 在这种情况下，可以使用所需设置创建一个环境，然后将这些设置导入到其他环境中，再根据需要自定义每个环境的设置。
- 将环境从开发系统迁移到生产系统。
- 在升级到新版本 CA Identity Manager 之后更新现有的环境。

导出 CA Identity Manager 环境

要在生产系统上部署 CA Identity Manager 环境，通过开发或预运行系统导出环境，再将该环境导入到生产系统。

注意：在您导入先前导出的环境时，CA Identity Manager 会在管理控制台的状态窗口中显示日志。 要查看此日志中每个管理对象及其属性的验证和部署信息，请在您导出环境*之前*，在“Environment Properties”（环境属性）页面上选择“Enable Verbose Log Output”（启用详细日志输出）字段。请注意选择“Enable Verbose Log Output”（启用详细日志输出）字段在导入期间可能引起重大性能问题。

遵循这些步骤:

1. 在管理控制台中单击“Environments”（环境）。

   显示 CA Identity Manager 环境屏幕，其中包含 CA Identity Manager 环境列表。
2. 选择要导出的环境。
3. 单击“Export”（导出）按钮。

   此时显示“File Download”（文件下载）屏幕。
4. 将 ZIP 文件保存到生产系统可以访问的位置。
5. 单击“Finish”（完成）。

将环境信息导出为 ZIP 文件，您可以将此文件导入到其他环境。

导入 CA Identity Manager 环境

您可以导入 CA Identity Manager 环境设置以完成下列任务之一：

- 使用类似设置管理多个环境。 在这种情况下，可以使用所需设置创建一个环境，然后将这些设置导入到其他环境中，再根据需要自定义每个环境的设置。
- 将环境从开发系统迁移到生产系统。
- 在升级到新版本 CA Identity Manager 之后更新现有的环境。

遵循这些步骤:

1. 在管理控制台中单击“Environments”（环境）。

   显示 CA Identity Manager 环境屏幕，其中包含 CA Identity Manager 环境列表。

2. 单击“Import”（导入）按钮。

   此时将显示“Import Environment”（导入环境）屏幕。

3. 浏览找到导入环境所需的 ZIP 文件。
4. 单击“Finish”（完成）。

将环境导入 CA Identity Manager。

重新启动 CA Identity Manager 环境

遵循这些步骤:

1. 在管理控制台中单击“Environments”（环境）。

   显示 CA Identity Manager 环境屏幕，其中包含 CA Identity Manager 环境列表。

2. 单击 CA Identity Manager 环境的名称以便启动。

   此时显示“CA Identity Manager Environment Properties”（CA Identity Manager 环境属性）屏幕。

3. 选择下列选项之一：

   “Restart Environment”（重新启动环境）

   停止和启动环境。

   “Stop”（停止）

   阻止当前运行的环境。

   “Start”（启动）

   启动当前没有运行的环境。

删除 CA Identity Manager 环境

使用此步骤删除 CA Identity Manager 环境。

注意：如果 CA Identity Manager 与 SiteMinder 进行整合以进行高级身份验证，CA Identity Manager 也会删除保护此环境以及为此环境创建的默认身份验证方案的 SiteMinder 策略域。

遵循这些步骤:

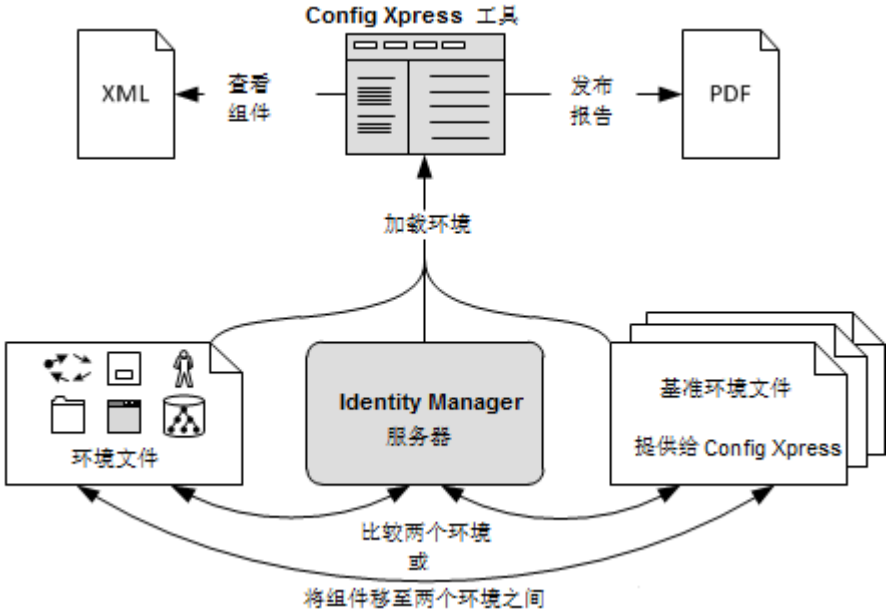
1. 在“Environments”（环境）屏幕中，选中要删除的“CA Identity Manager Environments”（CA Identity Manager 环境）的复选框。
2. 单击“Delete”（删除）。

   CA Identity Manager 显示一条确认消息。
3. 单击“OK”（确定）确认删除。

管理配置

Config Xpress 是 CA Identity Manager 中包含的工具。您可以使用此工具来分析和处理 CA Identity Manager 环境的配置。

最重要的是，本工具使您可以在环境之间移动组件。 Config Xpress 自动检测任何其他必要组件，并且提示您也移动它们。 此协助功能可以帮您减少工作量并减少出现问题的风险。



遵循这些步骤:

1. 设置 Config Xpress (p. 182)。
2. 使用工具之前，请将 CA Identity Manager 环境加载到 (p. 183) Config Xpress 以进行分析。
3. 使用 Config Xpress 在加载的环境中完成以下任务：
   - 在环境之间移动组件 (p. 185)。
   - 发布系统组件的 PDF 报告 (p. 186)。
   - 显示特定组件的 XML 配置 (p. 187)。

设置 Config Xpress

安装驱动器中包含 Config Xpress 的安装文件，但是未安装此工具。

Config Xpress 对软件的要求如下：

- CA Identity Manager r12.0 和更高版本
- Windows 操作系统
- Adobe Air Runtime
- 查看报告的 PDF Reader

遵循这些步骤:

1. 从 http://get.adobe.com/air 下载 Adobe Air Runtime，然后进行安装。
2. 确保安装了管理工具。
3. 在以下位置查找 Config Xpress 的安装文件：

   ```
   C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\ConfigXpress
   ```

4. 运行 Config Xpress.air 以安装 Config Xpress。
5. 在安装完成后，开始 Config Xpress。

将一个环境加载到 Config Xpress

在您可以使用 Config Xpress 之前，将一个或多个环境加载到此工具。 此任务使您可以在 Config Xpress 中处理环境。

您可以通过 live CA Identity Manager 服务器直接将环境加载到 Config Xpress，也可以通过环境文件加载。 如果使用了通过 Config Xpress 安装的基准环境文件之一，您可以将环境与即用型配置进行比较。

加载环境的过程可能要花费几分钟。

遵循这些步骤:

1. 打开 Config Xpress。
2. 要直接从 CA Identity Manager 服务器加载**实时环境**，请按以下步骤操作：
   a. 单击“Server (Network)”（服务器 (网络)）选项卡。
   b. 输入 CA Identity Manager 服务器的名称和端口。 例如：

      ```
      servername.ca.com:8080
      ```

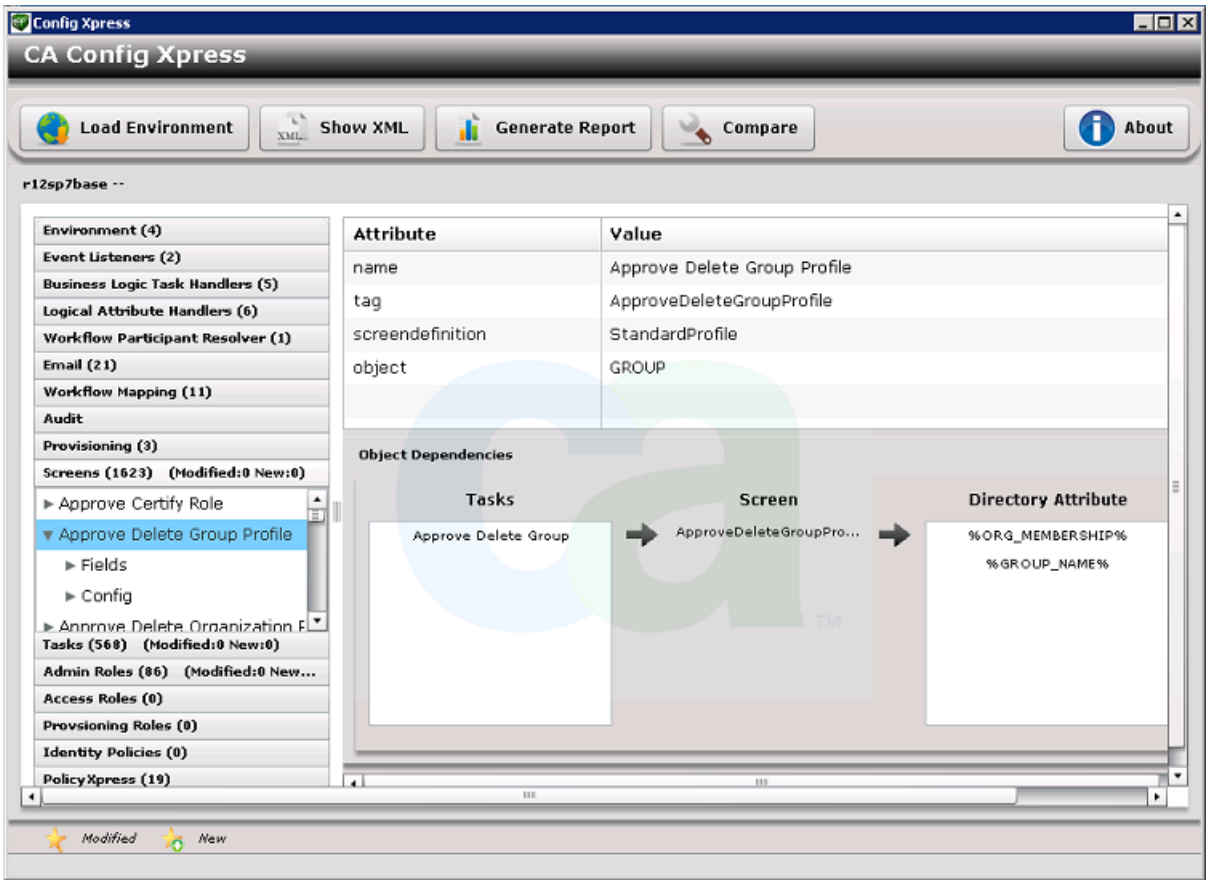
   c. 如果您的服务器设置为仅允许 HTTPS，选择“使用 HTTPS”。
   d. 如果服务器的版本比 r12.5 SP6 更新，选择 12.5 SP7。
   e. 单击“Connect”（连接）。
   f. 从*“Choose Environment to load”*（选择要加载的环境）表中选择环境，然后单击“Load”（加载）。
3. 要加载从 CA Identity Manager 环境导出的**环境文件**，请按以下步骤操作：
   a. 导出 CA Identity Manager 环境。
   b. 在 Config Xpress 中，单击“File System”（文件系统）选项卡。
   c. 选择版本，然后浏览到环境文件，然后单击“Load”（加载）。
4. 要加载使用 Config Xpress 安装的**基准环境文件**，请按以下步骤操作：
   a. 单击“Base Versions”（基础版本）选项卡。
   b. 选择您需要的版本，然后单击“Select”（选择）。

Config Xpress 可分析环境，然后显示环境的详细信息。

您现在可以用 PDF (p. 186) 或 XML (p. 187) 发布部分或全部环境。 如果加载第二个环境，您可以比较这些环境并且在她们之间移动组件 (p. 185)。

示例：加载基准配置文件之后的 Config Xpress

此快照显示了 Config Xpress 显示依存对象的方式：



将组件从一个环境移动到其他环境

如果没有 Config Xpress，在预运行区域之间移动组件的任务非常复杂、极易失败。

如果使用 Config Xpress 来移动组件，这一工具会同时移动所有必要对象。例如，如果您移动需要屏幕的任务，Config Xpress 会询问是否想同时选择必要组件。Config Xpress 知道此任务使用此屏幕，此屏幕也应当被移到目标环境。

如果您想将组件移至实时环境，Config Xpress 可以立即上传该组件。 如果想将组件移至环境文件，请将组件另存为 XML 文件然后将该文件导入环境中。

遵循这些步骤:

1. 加载包含想要移动的组件的环境。
2. 将此环境与第二个进行比较：
   a. 单击“Compare”（比较）。
   b. 加载目标环境。

      Config Xpress 会显示两个环境之间的差异列表。
3. 在差异列表中，找到想要移动的组件。 您可以单击“Name”（名称）列对此列表进行排序。
4. 对于每个组件，执行下列步骤：
   a. 在“Action”（操作）列中选择项目。

      Config Xpress 会分析组件，这可能需要一些时间。
   b. 如果组件具有从属组件，则会出现“Add Modified Dependant Screens”（添加已修改从属屏幕）框。 单击“Yes”（是）或“No”（否）继续。

   在选择了所有想要移动的组件后，就可以移动更新的组件了。
5. 如果您要将组件移至实时服务器，请单击“Upload To”（上载至）。

   组件会立即移动。
6. 如果您要将组件移至环境文件：
   a. 单击“Save”（保存）。
   b. 输入文件名，然后再次单击“Save”（保存）。

      Config Xpress 会将您选择的所有组件保存在 XML 文件中。您现在可以将此 XML 文件导入实际的目标环境中。

发布 PDF 报告

Config Xpress 可以生成记载 CA Identity Manager 环境的当前状态的报告。您可以使用此报告来获得生产环境的快照。 在生成此报告时，您可以选择包括完整配置还是只包括安装之后所做的更改。

此报告可用于以后的参考，也可用作系统恢复计划的一部分。

遵循这些步骤:

1. 将环境加载到 Config Xpress。
2. 单击“Generate Report”（生成报告）。

   在“Generate PDF Report”（生成 PDF 报告）对话框中，您可以更改字体大小，还可以输入标题或封面文字。 此外，您可以选择包括所有配置项或仅包括新增的或修改的项。

   重要说明！ 如果您没有单击*“Only include details of new or modified tasks, screens, roles”*（仅包括新增或修改的任务、屏幕、角色的详细信息）框，报告将包含整个环境。 PDF 文件将有约 2000 页长，40 多 MB。
3. 单击“确定”。
4. 输入文件名，然后保存报告。 保存过程可能需要几分钟，如果您选择发布整个环境，需要的时间可能更长。

   报告会在 PDF 阅读器中打开。

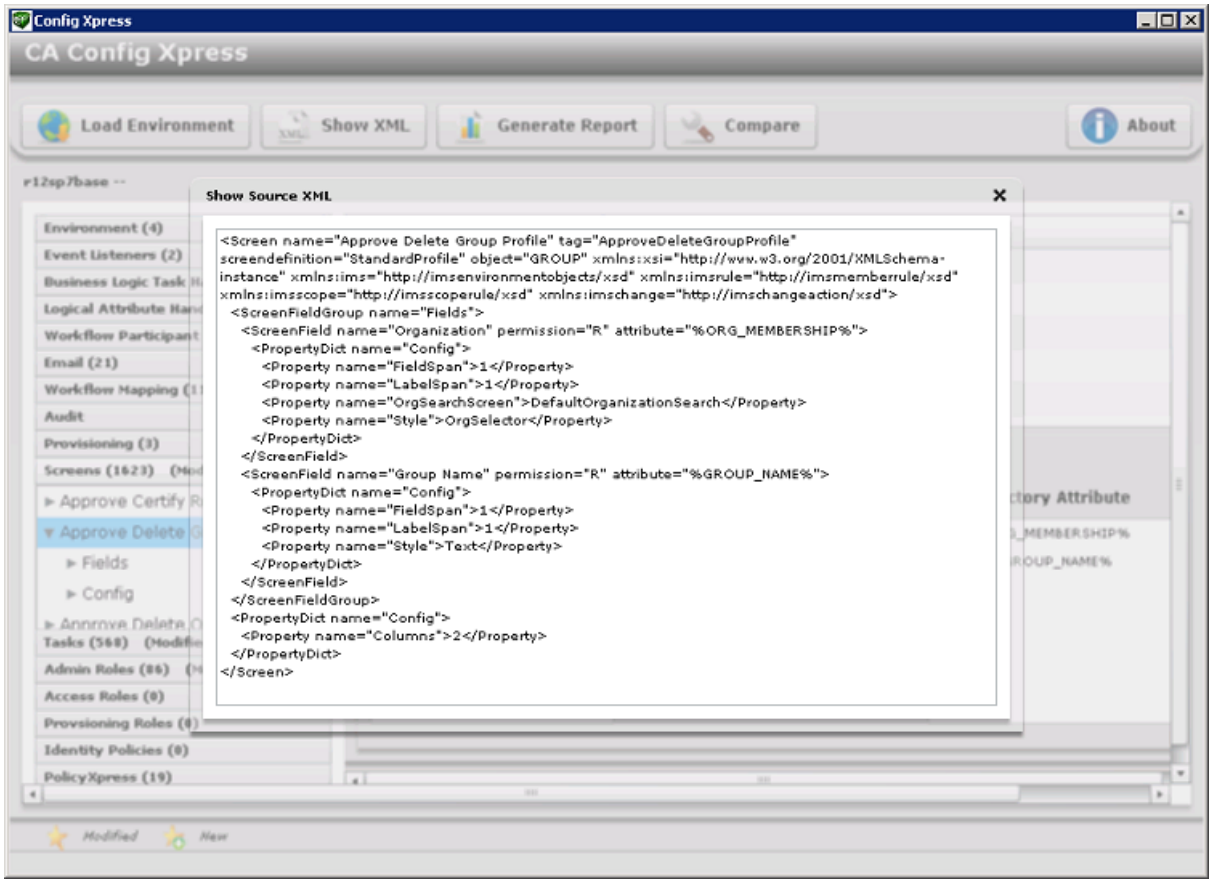
显示 XML 配置

Config Xpress 可以显示特定组件的 XML 配置。研究此 XML 文件可以帮助您了解系统。

遵循这些步骤:

1. 将环境加载到 Config Xpress。
2. 单击 Config Xpress 屏幕中的某个组件。
3. 单击“显示 XML”。

   XML 配置即会显示：



优化策略规则评估

可动态地识别一组用户的策略规则，用于评估角色成员、管理员、所有者策略以及身份策略。 在大规模的 CA Identity Manager 实施中，对这些规则的评估可能会花费较长时间。

注意：有关成员、管理员、所有者及身份策略的详细信息，请参阅*《管理指南》*。

要缩短包括用户属性的规则的评估时间，您可以启用内存中的评估选项。 在启用内存中的评估选项后，CA Identity Manager 会从用户存储中检索要评估的用户的信息，并且在内存中存储该用户的表示。CA Identity Manager 使用内存中的表示来将属性值与策略规则进行比较。 这限制了 CA Identity Manager 直接访问用户存储的次数。

您可以在管理控制台中为环境启用内存中的评估选项。

遵循这些步骤:

1. 打开管理控制台。
2. 选择“Environments”（环境）、*“Environment Name”（环境名称）*、“Advanced Settings”（高级设置）、“Miscellaneous”（杂项）。

   此时会打开“User Defined Properties”（用户定义的属性）页面。
3. 在“Property”（属性）字段中输入以下文本：

   UseInMemoryEvaluation
4. 在“Value”（值）字段中输入以下数值之一：

   0

   禁用内存中的评估。

   1

   启用内存中的评估。 在指定了此选项时，属性比较区分大小写。

   3

   启用内存中的评估。在指定了此选项时，属性比较不区分大小写。
5. 单击“Add”（添加）。

   CA Identity Manager 会将新的属性添加到环境的现有属性列表中。
6. 单击“Save”（保存）。

“Role and Task Settings”（角色和任务设置）

在管理控制台的“Role and Task Settings”（角色和任务设置）屏幕中，您可以使用称为角色定义文件的 XML 文件导入或导出屏幕、选项卡、角色以及任务设置。CA Identity Manager 提供了预定义的角色定义文件，这些文件创建了一整套功能的屏幕、选项卡、角色以及任务。 例如，存在支持智能配给的角色定义文件，还存在支持端点管理屏幕的其他文件。

另外，您还可以使用角色定义文件将一个环境的设置应用到多个环境。 请执行下列任务：

- 在一个环境中配置屏幕、选项卡、任务和角色设置。
- 将这些设置导出到 XML 文件。
- 将该 XML 文件导入到所需环境。

导出角色和任务设置

执行以下步骤，以导出角色和任务设置。

遵循这些步骤:

1. 在管理控制台中单击“Environments”（环境）。

   此时显示 CA Identity Manager 环境的列表。
2. 单击适当的 CA Identity Manager 环境的名称。

   此时显示此环境的“Properties”（属性）屏幕。
3. 单击“Role and Task Settings”（角色和任务设置），然后单击“Export”（导出）。
4. 单击“Open”（打开）以在浏览器窗口中查看文件，或者单击“Save”（保存）以将设置保存为 XML 文件。

导入角色和任务设置

角色和任务设置由名为角色定义文件的 XML 文件定义。您可以导入预定义的角色定义文件，以便支持特定的 CA Identity Manager 功能集（例如智能配给），也可以将角色定义文件从一个环境导入到另一个环境。

注意：您也可以为使用 Connector Xpress 创建的自定义连接器导入角色定义。使用角色定义生成器创建这些角色定义文件。 有关详细信息，请参阅*《Connector Xpress 指南》*。

执行以下步骤，以导入角色和任务设置。

遵循这些步骤:

1. 在管理控制台中单击“Environments”（环境）。

   此时显示 CA Identity Manager 环境的列表。

2. 单击您要导入角色和任务设置的 CA Identity Manager 环境的名称。

   此时显示此环境的“Properties”（属性）屏幕。

3. 单击“Role and Task Settings”（角色和任务设置），然后单击“Import”（导入）。

4. 完成下列操作之一：

   - 选择一个或多个角色定义文件来创建环境的默认角色和任务。

     要选择所有可用角色定义文件，请单击“Select/Deselect All”（全选/取消全选）。

   - 输入角色定义文件的路径和文件名，以导入或浏览文件。 然后单击“Finish”（完成）。

5. 单击“Finish”（完成）。

   状态显示在“Role Configuration Output”（角色配置输出）窗口中。

6. 单击“Continue”（继续）退出。

如何创建动态端点的角色和任务

使用 Connector Xpress，您可以配置动态连接器，以支持 SQL 数据库和 LDAP 目录的配给和管理。 对于每个动态连接器，您可以使用角色定义生成器为在用户控制台中显示的帐户管理屏幕创建任务和屏幕定义。

在运行角色定义生成器之后，您可以在管理控制台中导入所生成的角色定义文件 (p. 189)。

注意：有关角色定义生成器的详细信息，请参阅 *《Connector Xpress 指南》*。

修改系统管理员帐户

系统管理员负责设置并维护 CA Identity Manager 环境。 通常，系统管理员的任务包括：

- 创建与管理初始环境
- 创建与修改管理角色
- 创建与修改其他管理员帐户

在创建 CA Identity Manager 环境时，即会创建系统管理员帐户。 如果此帐户被“锁定”（例如系统管理员忘记了密码），您可以使用系统管理员向导重新创建帐户。

系统管理员向导会引导您完成相关步骤，将系统管理角色分配给用户。

在修改系统管理员帐户之前请注意下列几点：

- 确保您使用的是 LDAP 用户存储，并且已经在您的 CA Identity Manager 目录的目录配置文件 (directory.xml) 配置了用户容器（例如 ou=People）。 所选用户必须在您配置系统管理员的同一容器中。 选择用户容器中不存在的用户帐户可能导致失败。
- 在 CA Identity Manager 环境管理具有扁平型或用户扁平型结构的用户目录时，所选用户的配置文件也必须包括此组织。 要确保用户的配置文件被正确地配置，请将用户组织的名称添加到与 directory.xml 文件 (p. 75)中的 %ORG_MEMBERSHIP% 常用属性相对应的物理属性中。 例如，如果物理属性说明映射到 directory.xml 文件的 %ORG_MEMBERSHIP% 常用属性，并且用户属于该员工组织时，用户的配置文件必须包含属性/值对 description=Employees。

遵循这些步骤:

1. 在 CA Identity Manager 环境屏幕，单击适当的 CA Identity Manager 环境的名称。

   此时显示特定环境屏幕的属性。

2. 单击“System Manager”（系统管理员）。

   此时显示系统管理员向导。

3. 输入具有系统管理员角色的用户的唯一名称，如下所示：
   - 对于关系数据库用户，输入用户的唯一标识符或映射到目录配置文件中的 %USER_ID% 常用属性的值。
   - 对于 LDAP 用户，输入用户的相关 DN。 例如，如果用户的 DN 是 uid=Admin1、ou=People、ou=Employees、ou=NeteAuto，输入 Admin1。

   注意：请确保系统管理员和用户存储的管理员 *不是*同一用户。

4. 单击“验证”以显示用户的完整标识符。
5. 单击“下一步”。
6. 在向导的第二页中，选择角色来分配给用户，如下所示：
   - 如果要分配系统管理员角色，请执行下列任务：
     a. 选择系统管理员角色旁边的单选按钮。
     b. 单击“完成”。

- 如果要分配系统管理员角色之外的角色，请执行下列任务：
  a. 在第一个列表中选择条件。
  b. 在第二个列表框中输入部分或完整的角色名称或者星号 (*)。 单击“搜索”。
  c. 从搜索结果列表中选择要分配的角色。
  d. 单击“完成”。

“System Manager Configuration Output”（系统管理员配置输出）屏幕会显示状态信息。

7. 单击“继续”以关闭系统管理员向导。

访问 CA Identity Manager 环境的状态

CA Identity Manager 包括了一个状态页面，您可以用来验证以下状态：

- CA Identity Manager 目录加载正确。
- CA Identity Manager 可以连接到用户存储。
- CA Identity Manager 环境加载正确。

要访问状态页面，请在浏览器中输入以下 URL：

`http://hostname/iam/im/status.jsp`

hostname

确定安装 CA Identity Manager 的服务器的完全限定域名，例如 myserver.mycompany.com。

如果 CA Identity Manager 环境正确启动，并且所有的连接成功运行，则状态页面会如下图所示：

状态页面还会指出环境是否兼容 FIPS 140-2。

CA Identity Manager 环境故障排除

下表对可能的错误消息和故障排除过程进行了说明：

消息	说明	疑难解答
未加载	在 CA Identity Manager 启动时，与环境关联的 CA Identity Manager 目录未加载。	1. 验证用户存储正在运行。 如果 CA Identity Manager 集成了 SiteMinder，请验证 SiteMinder 可以连接到用户存储。
“Not OK”（未就绪）	CA Identity Manager 无法连接到 CA Identity Manager 目录。	在策略服务器用户界面中，您可以打开与用户存储关联的 SiteMinder 用户目录连接的属性页，然后单击“View Contents”（查看内容）按钮，验证连接。 如果您可以看到用户存储的内容，SiteMinder 就可以成功连接。 有关策略服务器的详细信息，请参阅 CA *《SiteMinder Web Access Manager Policy Server Configuration Guide》*。 2. 重新启动 CA Identity Manager 和策略服务器。
“SM connection is not OK”（SM 连接故障）	CA Identity Manager 无法连接到 SiteMinder 策略服务器（针对包含 SiteMinder 的实施）	1. 验证以下条件： ■ 策略服务器正在运行。 ■ Web 代理正在保护资源。 您可以通过访问策略服务器用户界面来验证 Web 代理运行正确。如果提示您提供凭据，则 Web 代理运行正确。 2. 重新启动 CA Identity Manager 和策略服务器。
“IMS is not available now”（IMS 现在不可用）	CA Identity Manager 中发生了错误。	检查应用程序服务器日志，获取错误详细信息。
Windows 500 错误消息	在删除了 LDAP 用户目录的连接后访问状态页时，该页不显示。	将 Internet 浏览器选项“Show friendly error message”（显示友好错误消息）设置为关闭来查看状态页。

第 7 章：“Advanced Settings”（高级设置）

通过管理控制台的“Advanced Settings”（高级设置）窗口，您可以进行以下设置：

- 访问配置高级设置的屏幕
- 按照“导入/导出自定义设置” (p. 206)中所述导入和导出高级设置。

此部分包含以下主题：

审核

审核日志保留在 CA Identity Manager 环境中执行的操作的记录。 您可以使用审核日志的数据监控系统活动。

CA Identity Manager 审核 *事件*。 事件是由 CA Identity Manager 任务生成的操作。一个任务可以生成多个事件。 例如，CreateUser 任务可以生成 CreateUserEvent 和 AddToGroupEvent 事件。

默认情况下，CA Identity Manager 将所有事件信息导出到审核数据库。要控制 CA Identity Manager 记录的事件信息的类型和数量，您可以执行以下操作：

- 为 CA Identity Manager 管理任务启用审核。
- 为管理任务生成的部分或全部的 CA Identity Manager 事件启用审核。
- 在出现特殊状态时（例如在事件完成或取消时）记录事件信息。

- 记录与某一事件有关的属性的信息。 例如，您可以记录在 ModifyUserEvent 期间更改的属性。
- 设置事件和属性的审核级别。

业务逻辑任务处理程序

在提交 CA Identity Manager 任务以进行处理之前，业务逻辑任务处理程序执行自定义业务逻辑。通常，自定义业务逻辑会验证数据。例如，在 CA Identity Manager 将成员添加到组之前，业务逻辑任务处理程序可以检查该组的成员资格限制。如果达到了组成员资格限制，业务逻辑任务处理程序显示消息，通知组管理员无法添加新成员。

您可以使用预定义的业务逻辑任务处理程序，也可以使用业务逻辑任务处理程序 API 创建自定义处理程序。

注意：有关创建自定义业务逻辑的信息，请参阅*《Programming Guide for Java》*。

业务逻辑任务处理程序屏幕包括现有的全局业务逻辑任务处理程序的列表。 此列表包括 CA Identity Manager 附带的预定义处理程序和您站点上定义的任何自定义处理程序。CA Identity Manager 按照在该列表中显示的顺序执行这些处理程序。

只能在 Java 中实施全局业务逻辑任务处理程序。

自动清除重置用户密码任务的密码字段

如果先前输入的值违反密码策略，或者“密码”和“确认密码”字段的值不匹配，您可以配置 CA Identity Manager 自动清除密码字段。

遵循这些步骤:

1. 启动管理控制台。
2. 选择要管理的环境，然后单击“Advanced Settings”（高级设置）。

   此时将显示“Advanced Settings”（高级设置）页面。
3. 单击“Business Logic Task Handlers”（业务逻辑任务处理程序）、“BlthPasswordServices”。

   此时显示“Business Logic Handler Properties”（业务逻辑处理程序属性）页面。

4. 创建以下属性：

   ClearPwdIfInvalid=true

   PwdConfirmAttrName=|passwordConfirm|

5. 验证 ConfirmPasswordHandler 设置是否如下所示：

   - 对象类型－用户
   - 类－ConfirmPasswordHandler
   - ConfirmationAttributeName = |passwordConfirm|
   - OldPasswordAttributeName = |oldPassword|
   - passwordAttributeName = %PASSWORD%

   用户现在可以清除重置用户密码任务中的密码字段。

事件列表

管理任务包括 CA Identity Manager 要完成任务所执行的*事件*和操作。 一项任务可能包括多个事件。 例如，“创建用户”任务可能包括创建用户的配置文件、将用户添加到组以及分配角色等事件。

CA Identity Manager 审核事件、强制执行与事件相关联的客户特定的业务规则，以及当事件映射到工作流流程时要求批准事件。

使用本页来查看 CA Identity Manager 中可用的事件列表。

电子邮件通知

在任务或事件完成时，或在工作流控制下的事件达到指定状态时，CA Identity Manager 可以发送电子邮件通知。 例如，电子邮件可以通知批准人，事件需要批准。

要指定电子邮件通知的内容，您可以使用预定义的电子邮件模板，也可以自定义模板以满足需求。

使用管理控制台，您可以完成以下任务：

- 为 CA Identity Manager 环境启用电子邮件通知。
- 指定创建电子邮件的模板集。
- 表明需要发送电子邮件通知的事件和任务。

事件侦听程序

一个 CA Identity Manager 任务由一个或多个操作组成，称为事件，CA Identity Manager 在任务的执行期间会执行这些事件。 例如，“创建用户”任务可能包括以下事件：

- CreateUserEvent－在组织中创建用户配置文件
- AddToGroupEvent－（可选）将用户添加为组成员
- AssignAccessRole－（可选）将访问角色分配给用户

事件侦听程序“侦听”特定事件，然后在事件的生命周期的指定点执行自定义业务逻辑。 例如，在 CA Identity Manager 中创建新用户之后，事件侦听程序可以将用户的信息添加到其他应用程序的数据库中。

注意：有关配置事件侦听程序的详细信息，请参阅*《Programming Guide for Java》*。

身份策略

身份策略将一组业务更改应用于满足特定的规则或条件的用户。 可以使用身份策略执行以下任务：

- 自动执行某些身份管理任务，例如分配角色和组员资格、分配资源或修改用户配置文件属性。
- 强制执行职责划分。例如，您可以创建一种身份策略，来禁止“支票签名人”角色的成员具备“支票批准人”角色。
- 强制遵从。例如，您可以审核担任某一职务且酬劳超过 100000 美元的用户。

在用户控制台中创建和管理身份策略集。有关身份策略的详细信息，请参阅*《管理指南》*。

在您使用身份策略之前，使用管理控制台完成以下任务：

- 为 CA Identity Manager 环境启用身份策略。
- 设置递归级别（可选）。

逻辑属性处理程序

通过 CA Identity Manager 逻辑属性，您可以采用易于理解的格式在任务屏幕上显示用户存储属性（称为*物理属性*）。 CA Identity Manager 管理员使用任务屏幕在 CA Identity Manager 中执行功能。

用户存储中不存在逻辑属性。 通常，逻辑属性表示一个或多个物理属性来简化演示。 例如逻辑属性*日期*可以表示物理属性*月*、*日*和*年*。

逻辑属性由逻辑属性处理程序处理，该程序是使用逻辑属性 API 编写的 Java 对象。 例如，在显示任务屏幕时，逻辑属性处理程序可以将用户存储的物理属性数据转换为逻辑属性数据。

您可以使用 CA Identity Manager 包含的预定义逻辑属性和逻辑属性处理程序，也可以使用逻辑属性 API 创建新的逻辑属性和逻辑属性处理程序。

注意：有关详细信息，请参阅 *《Programming Guide for Java》*。

“Miscellaneous”（杂项）

在此屏幕上定义的用户定义属性适用于整个 CA Identity Manager 环境。 将它们作为名称/值对发送到使用 CA Identity Manager API 创建的每个自定义 Java 对象的 init() 方法。 自定义对象可以按照对象业务逻辑需要的任何方式使用此数据。

也为特定自定义对象定义用户定义的属性。 例如，假定用户定义的属性在名为“MyListener”的事件侦听程序的属性屏幕中进行定义。 通过一次调用将在“Miscellaneous”（杂项）屏幕中定义的特定对象的用户定义属性和全环境属性发送给 MyListener.init()。

要添加用户定义的属性，请指定属性名和值，并单击“添加”。

要删除一个或多个用户定义的属性，请选中每个要删除的名称/值对旁边的复选框，并单击“删除”。

完成更改后，单击“保存”。 重新启动应用程序服务器，使更改生效。

注意：所有杂项属性是区分大小写的。 因此，如果您定义名为“SelfRegistrationLogoutUrl”的属性和另一个名为“selfregistrationlogouturl”的属性，则会添加两个属性。

通知规则

通知规则确定接收电子邮件通知的用户。 在任务完成或任务的事件达到某些状态（如待批准、批准或拒绝）时，用户根据通知规则收到电子邮件通知。

注意：有关电子邮件通知功能的详细信息，请参阅 *《管理指南》*。

CA Identity Manager 包含以下预定义通知规则：

ADMIN_ADAPTER

将电子邮件消息发送给启动任务的管理员

USER_ADAPTER

将电子邮件消息发送给受任务影响的用户

USER_MANAGER

将电子邮件发送到当前上下文的用户的管理员

要创建自定义通知规则，请使用通知规则 API。

注意：有关通知规则的详细信息，请参阅*《Programming Guide for Java》*。

组织选择器

组织选择器是自定义逻辑属性处理程序，该处理程序确定 CA Identity Manager 创建自行注册用户的配置文件的位置，这由用户在注册期间提供的信息决定。 例如，可以将在注册时提供促销代码的用户的配置文件添加到“促销用户”组织。

Provisioning（配给）

在您使用带有配给的 CA Identity Manager 时，请使用此屏幕。

注意：为 CA Identity Manager 环境设置配给 (p. 165)是更详细的步骤，可以提供逐步说明。

“Provisioning Properties”（配给属性）选项如下所示：

“Enabled”（已启用）

指定使用两个用户存储，一个针对 CA Identity Manager，另一个单独的用户存储（称为配给目录）针对配给帐户。 如果禁用此选项，仅使用 CA Identity Manager 用户存储。

“Use Session Pool”（使用会话池）

启用对会话池的使用。

“Session Pool Initial Sessions”（会话池初始会话）

定义会话池在启动时可用的最小会话数。

默认值：8

“Session Pool Maximum Sessions”（会话池最大会话数）

定义池中会话的最大数目。

默认值：32

“Enable Password Changes from Endpoint Accounts”（从端点帐户启用密码更改）

在配给服务器中为每位用户定义“Enable Password Synchronization Agent”（启用密码同步代理）设置。此选项允许在 CA Identity Manager 用户和关联的端点帐户之间实现密码同步。

“Enable Accumulation of Provisioning Role Membership Events”（启用配给角色成员资格累计事件）

如果启用，此复选框确保 CA Identity Manager 以指定顺序执行与配给角色成员资格有关的事件。 所有的“Add”（添加）操作都会被合并到单个操作中，然后发送到配给服务器进行处理。 “Add”（添加）操作处理完成后，CA Identity Manager 即会将“Remove”（删除）操作合并到单个操作中，然后将该操作发送到配给服务器。 生成名为“AccumulatedProvisioningRoleEvent”的单个事件，从而按此顺序执行事件。

注意：有关 AccumulatedProvisioningRoleEvent 的详细信息，请参阅*《管理指南》*。

“Organization for Creating Inbound Users”（创建入站用户的组织）

定义 CA Identity Manager 使用的用户存储的完全限定路径。只有用户存储包括组织时，才会显示此字段。

“Inbound Administrator”（入站管理员）

定义可以执行映射到入站映射的任务的 CA Identity Manager 管理员帐户。 这些任务包含在配给同步管理者角色中。 管理员必须能在任何一个 CA Identity Manager 用户上执行每项任务。

“Provisioning Directory”（配给目录）

配给目录是配给信息的存储库，包括域、全局用户、端点类型、端点、帐户以及帐户模板。 当选择它时，会显示将 CA Identity Manager 用户存储映射到配给目录的其他选项。

“Enable Session Pooling”（启用会话池）

为了改善性能，在与配给服务器进行通信时，CA Identity Manager 可以将大量会话预分配到池。

如果禁用“Session Pools”（会话池）选项，CA Identity Manager 根据需要创建和销毁会话。

对于新环境，默认情况下会启用会话池。 对于现有环境，您可以启用“Session Pools”（会话池）。

遵循这些步骤:

1. 在管理控制台中，依次选择“Advanced Settings”（高级设置）、“Provisioning”（配给）。
2. 选择“Use Session Pool”（使用会话池）。
3. 定义会话池在启动时的最小会话数。
4. 定义池中会话的最大数目。
5. 单击“Save”（保存）。
6. 重新启动应用程序服务器。

   根据定义设置启用会话池。

启用密码同步

配给服务器允许在 CA Identity Manager 用户和关联的端点用户帐户之间实现密码同步。 换句话说，如果在 CA Identity Manager 中创建或修改具有配给角色的用户，会将此配给用户设置为允许通过端点帐户更改密码。

注意：在您在管理控制台中启用此功能时，会将此环境中的*所有*用户设置为允许通过端点帐户更改密码。

启用密码同步

1. 在管理控制台中，依次选择“Advanced Settings”（高级设置）、“Provisioning”（配给）。
2. 选中“Enable Password Changes from Endpoint Accounts”（从端点帐户启用密码更改）。
3. 单击“Save”（保存）。
4. 重新启动应用程序服务器。

属性映射

属性映射将配给相关的管理任务中的用户属性（如配给创建用户）与配给服务器中的相应属性关联。 可以将单个配给属性映射到 CA Identity Manager 用户存储中的多个属性。

默认任务中的属性存在默认映射，在“入站映射”部分列出了这些映射。 如果您通过某种方式修改这些管理任务之一，以使用不同属性，则根据需要更新属性映射。

入站映射

入站映射将配给服务器生成的事件映射到管理任务。 这些映射是预设的，无法修改。

出站映射

出站映射将管理任务生成的事件与应用到配给目录的事件关联。 默认映射是为影响用户属性的事件提供的。

用户控制台

使用用户控制台访问 CA Identity Manager 环境，此环境是允许用户执行管理任务的一种 Web 应用程序。为用户控制台定义特定属性，管理员可以使用这些属性在管理控制台中访问用户控制台的环境。

“用户控制台”页面包含下列字段：

“General Properties”（常规属性）

定义应用于环境的属性。

“Show Recently Completed Tasks”（显示最近完成的任务）

确定在任务完成时 CA Identity Manager 是否显示状态消息。

如果选择此选项，用户必须单击“OK”（确定）以清除 CA Identity Manager 显示的状态消息。

要禁用消息，以防止用户必须在每个状态消息出现时单击“OK”（确定），请清除该选项。

“Show About Link”（显示“关于”链接）

确定是否在用户控制台的右下角显示“About”（关于）链接。 如果选择此选项，CA Identity Manager 用户可以单击“About”（关于）链接以查看 CA Identity Manager 组件的版本信息。

“Enable Language Switching”（启用语言切换）

确定 CA Identity Manager 是否在登录屏幕和用户控制台中包括“Choose Language”（选择语言）下拉列表。 选择此字段时，CA Identity Manager 用户可以通过从列表中选择新的语言，来更改用户控制台中的语言。

注意：要显示“Choose Language”（选择语言）字段，请确认您选择了“Enable Language Switching”（启用语言切换）字段，*并*配置 CA Identity Manager 以支持多种语言。

有关详细信息，请参阅 *《User Console Design Guide》*。

“Job Timeout”（作业超时）

确定在任务被提交之后，在显示状态消息之前 CA Identity Manager 等待的时间。

如果任务在指定时间之内完成，CA Identity Manager 显示以下消息：

“任务已完成”

如果任务需要更长时间才能完成或在工作流控制下，CA Identity Manager 显示以下消息：

“Task has been submitted for processing on the *current date*”（已在当前日期提交任务以进行处理）

注意：更改可能不会立即生效。

“Theme Properties”（主题属性）

让您自定义环境中的用户控制台的图标和标题。 例如，您可以将公司徽标和公司名添加到用户控制台屏幕中。

“Theme Properties”（主题属性）包括以下设置：

“Icon (URI)”（图标 (URI)）

使用应用程序服务器可以访问的映像的 URI 定义图标。

示例：http://myserver.mycompany.com/images/front/logo.gif

“Icon Link (URI)”（图标链接 (URI)）

使用 URI 定义映像的导航链接。

“Icon Title”（图标标题）

定义显示为图标上的鼠标悬停文本的工具提示。

标题

指定自定义文本，此文本显示在用户控制台顶部的图标旁边。

注意：如果您定义了自定义面板，可以通过引用该面板的属性文件来指定图标或标题。 例如，如果某自定义面板的属性文件中的图标图像对应的条目是 image/logo.gif，可以在“Icon”（图标）字段中输入同样的字符串。

“Login Properties”（登录属性）

指定在用户访问环境时被引导至的登录页的身份验证方法和位置。

“Authentication Provider module class name”（身份验证提供程序模块类名称）

指定身份验证提供程序模块的类名称。

登录页面

指定在访问环境时用户被引导至的页面。

Web 服务

CA Identity Manager 任务 执行 Web 服务 (TEWS) 使第三方客户端应用程序可以将 CA Identity Manager 任务提交至 CA Identity Manager 进行远程执行。

您可以使用“Web 服务属性”屏幕为环境配置 TEWS。在此屏幕上，您可以完成以下任务：

- 为 CA Identity Manager 环境启用 TEWS。
- 生成特定于任务的 Web 服务定义语言 (WSDL) 文档。
- 允许模仿。
- 指定管理员密码是身份验证所必需的。
- 配置 SiteMinder 身份验证。
- 如果 CA Identity Manager 与 SiteMinder 集成，配置 SiteMinder 以保护 Web 服务 URL
- 指定 Web 安全服务用户名令牌身份验证。
- 在三种可能的身份验证类型中至少指定一种。

有关通过任务 执行 Web 服务向 CA Identity Manager 发送远程请求的详细信息，请参阅 *《Programming Guide for Java》*。

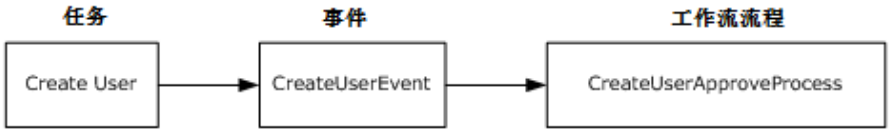
工作流属性

如果启用，工作流功能会控制与工作流流程有关的 CA Identity Manager 任务的执行。

工作流流程是为实现业务目标（如创建用户帐户）而执行的一系列步骤。通常，其中某一步骤会涉及批准或拒绝任务。

管理员任务与一个或多个事件有关，事件可能触发一个或多个工作流流程。 在工作流流程完成之后，CA Identity Manager 会执行或拒绝基于工作流流程结果的任务。

下图显示了 CA Identity Manager 任务、关联事件及工作流流程之间的关系：



“Workflow Properties”（工作流属性）

使用此复选框可以为 CA Identity Manager 环境启用或禁用工作流。

“Work Item Delegation”（工作项指派）

如果启用，工作项指派将允许参与人（指派人）指定其他用户（被指派人）获得批准指派人工作列表中的任务的权限。 在指派人“离岗”时，参与人可以将工作项分配给其他批准人。指派人在指派期间保留对其工作项的完全访问权限。

指派使用以下常用属性：

%DELEGATORS%

此常用属性存储向具有该属性的用户进行指派的用户的用户名以及指派创建时间。

注意：有关工作项指派的详细信息，请参阅*《管理指南》*。

工作流参与人确定程序

工作流流程中的活动（例如批准或拒绝任务）由*参与人*执行。

您可以使用“Workflow Participant Resolvers”（工作流参与人确定程序）屏幕将自定义参与人确定程序映射到完全限定的参与人确定程序 Java 类。

自定义*参与人确定程序*是一个 Java 对象，可以确定工作流活动的参与人，并向 CA Identity Manager 返回列表。 然后，CA Identity Manager 将列表传递给工作流引擎。

通常，仅当标准参与人确定程序均无法提供活动所需的参与人列表时，您才可以编写自定义参与人确定程序。

注意：有关开发自定义参与人确定程序的信息，请参阅*《Programming Guide for Java》*。 有关标准参与人确定程序的信息，请参阅*《管理指南》*。

导入/导出自定义设置

在管理控制台的“Advanced Settings”（高级设置）屏幕，您可以将高级设置应用于多个环境，如下所示：

- 在一个环境中配置高级设置。
- 将高级设置导出到 XML 文件。
- 将 XML 文件导入到所需的环境。

Java 虚拟机内存不足错误

症状：

我在压力较大或负载较高时收到了 JVM 内存不足错误，影响了 CA Identity Manager 服务器的功能。

解决方案：

我们建议您设置 JVM 调试选项，以便在内存不足时收到报警。

注意：有关设置 JVM 调试选项的详细信息，请访问 http://www.oracle.com，参阅其中的“Java HotSpot VM 选项中的调试选项”。

第 8 章： 审核

此部分包含以下主题：

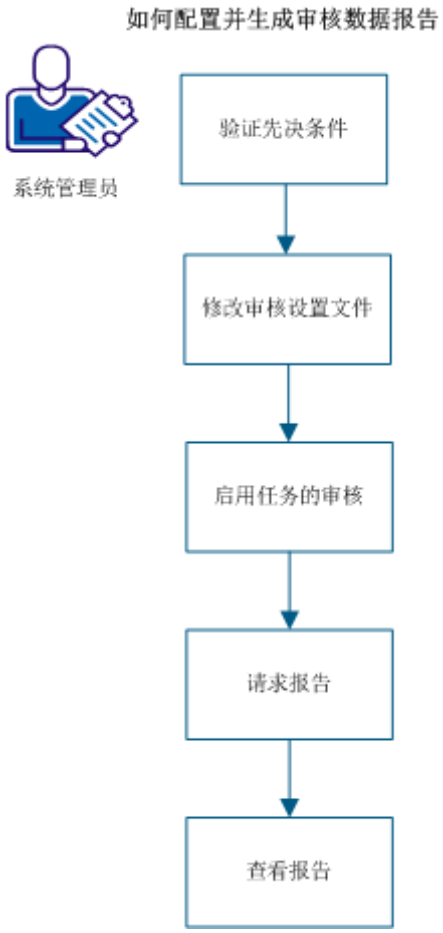
如何配置和生成审核数据报告

审核数据为在环境中执行的操作提供了历史记录。 在您配置和启用审核时，系统记录有关审核数据库中任务的信息。 审核信息可用于生成报告。 一些审核数据示例包括以下几点：

- 指定时间段的系统活动。
- 访问特定环境时的用户登录和注销事件。
- 特定用户执行的任务
- 在特定时间段内修改的对象的列表。
- 用户分配的角色
- 为特定用户帐户执行的操作。

审核数据是针对 CA Identity Manager *事件*生成的。事件是由 CA Identity Manager 任务生成的操作。 例如：“创建用户”任务可以包括 AssignAccessRoleEvent 事件。

下图描述系统管理员如何配置审核并生成审核数据的报告：



作为管理员，请完全以下步骤：

1. 验证先决条件 (p. 211)
2. 修改审核设置文件 (p. 211)
3. 启用任务的审核 (p. 215)
4. 请求报告 (p. 216)
5. 查看报告 (p. 218)

验证先决条件

验证在配置审核设置之前是否满足以下先决条件：

- 创建单独的数据库实例用于存储与审核相关的数据。 默认情况下，CA Identity Manager 数据库架构文件位于以下位置：
  - **Windows**：C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\Identity Manager\tools\db
- 配置报告服务器连接以请求和查看审核报告。
- 添加审核报告的连接对象。 执行以下步骤：
  a. 登录到具有管理权限的用户控制台。
  b. 转到“角色和任务”、“管理任务”并搜索要修改的审核报告。
  c. 在“报告的连接对象”字段中输入以下连接名称：
  `rptParamConn`

修改审核设置文件

在审核设置文件中配置审核设置，以便定义 CA Identity Manager 必须审核的信息类型。 您可以配置审核设置文件，以执行以下任务：

- 审核部分或全部生成事件的管理任务。
- 记录特定状态的事件信息，如在事件完成或被取消时。
- 记录与某一事件有关的属性的信息。 例如，您可以记录在 ModifyUserEvent 事件期间更改的属性。

- 设置属性日志的审核级别。

审核设置文件是您通过导出审核设置创建的 XML 文件。 文件具有以下架构：

```
<Audit enabled="" auditlevel="" datasource="">
  <AuditEvent name="" enabled="" auditlevel="">
    <AuditProfile objecttype="" auditlevel="">
      <AuditProfileAttribute name="" auditlevel="" />
    </AuditProfile>
    <EventState name="" severity=""/>
  </AuditEvent>
</Audit>
```

有关审核元素和架构的更多信息，请参阅在审核设置文件中的注释。

AuditProfileAttribute 元素表示 CA Identity Manager 审核的属性。 该属性适用于在 AuditProfile 元素中指定的对象。

注意：如果没有指定任何审核配置文件属性，则在 AuditProfile 元素中指定的对象的所有属性都会被记录。

下表显示了 CA Identity Manager 对象类型的有效属性：

CA Identity Manager 对象类型的有效属性

对象类型	有效属性
ACCESS ROLE	■ name－角色的用户可见名称 ■ description－关于角色目的的可选注释。 ■ members－可以使用该角色的用户。 ■ administrators－可以分配角色成员或管理员的用户。 ■ owners－可以修改角色的用户。 ■ enabled－表示角色是否被启用。 ■ assignable－表示角色是否可由管理员分配。 ■ tasks－与角色有关的访问任务。
ACCESS TASK	■ name－任务的用户可见名称 ■ description－关于任务目的的可选注释 ■ application－与任务有关的应用程序。 ■ tag－任务的唯一标识符 ■ reserved1, reserved2, reserved3, reserved4－任务的保留字段的值

CA Identity Manager 对象类型的有效属性	
对象类型	**有效属性**
ADMINISTRATIVE ROLE	■ name－角色的用户可见名称 ■ description－关于角色目的的可选注释 ■ members－可以使用该角色的用户。 ■ administrators－可以分配角色成员或管理员的用户。 ■ owners－可以修改角色的用户。 ■ enabled－表示角色是否被启用。 ■ assignable－表示角色是否可由管理员分配。 ■ tasks－与角色有关的任务。
ADMINISTRATIVE TASK	■ name－任务的用户可见名称 ■ description－关于任务目的的可选注释 ■ tag－任务的唯一标识符 ■ category－显示任务的 CA Identity Manager 用户界面中的类别 ■ primary_object－任务操作的对象 ■ action－针对对象执行的操作。 ■ hidden－表示是否*不*让任务显示在菜单中。 ■ public－表示尚未登录到 CA Identity Manager 的用户是否可以获得该任务。 ■ auditing－表示任务是否启用审核信息的记录。 ■ external－表示任务是否是外部任务。 ■ url－在执行外部任务时，CA Identity Manager 将用户重定向到的 URL。 ■ workflow－表示 CA Identity Manager 事件是否与任务触发器工作流关联 ■ webservice－表示该任务是否为可以为其从 CA Identity Manager 管理控制台生成 Web 服务描述语言 (WSDL) 输出的一个任务。
GROUP	在目录配置文件 (directory.xml) 中为 GROUP 对象定义的任何有效属性。
ORGANIZATION	在目录配置文件 (directory.xml) 中为 Organization

CA Identity Manager 对象类型的有效属性	
对象类型	**有效属性**
PARENTORG	对象定义的任何有效属性。
RELATIONSHIP	■ %CONTAINER%－父对象的唯一标识符。 例如，如果 RELATIONSHIP 对象描述角色成员资格，则容器将是角色。 ■ %CONTAINER_NAME%－父组的用户可见名称 ■ %ITEM%－包含在父对象内的对象的唯一标识符。 例如，如果 RELATIONSHIP 对象描述角色成员资格，该项将是角色成员。 ■ %ITEM_NAME%－嵌套组的用户可见名称
USER	在目录配置文件 (directory.xml) 中为 USER 对象定义的任何有效属性。
NONE	无属性

注意：以下几点适用于之前的表：

- Enabled、assignable、auditable、workflow、hidden、webservice 和 public 记录为 true 或 false。
- 在审核角色的任务时，记录用户可见名称。
- 数据库以编译 XML 格式存储成员、管理员和所有者策略。 此格式不同于将每一策略显示为表达式的用户界面。

遵循这些步骤:

1. 登录到管理控制台，选择“环境”、“高级设置”，然后单击“审核”。
2. 单击“Export”（导出）。

   系统将当前审核设置导出到审核设置 XML 文件。

3. 修改上一步中导出的 XML 文件中的审核设置。 请执行下列任务：
   a. 设置 Audit enabled ="true" 的值，并向元素数据源提供“iam_im_<auditdb>.xml”的 JNDI 名称值。
   b. 指定下列 JNDI 名称：
      `java:/auditDbDataSource`
      注意：此数据源位于以下位置：
      `iam/im/jdbc/auditDbDataSource`
   c. 在文件中添加、修改或删除元素。
   d. 修改为每个事件记录的信息级别。
4. 重复步骤 1 和 2。 单击“导入”并上传修改过的审核设置 XML 文件。
5. 重新启动环境。

审核设置文件现在已被更新。

启用任务的审核

针对您已在审核设置文件中配置审核的任务启用审核。

遵循这些步骤:

1. 登录到具有系统管理员权限的用户控制台。
2. 创建或修改要启用审核的任务。
3. 在“配置文件”选项卡上，请确保选择了“启用审核”复选框。
4. 单击“提交”。

现在该任务启用了审核。

请求报告

要查看该报告，为用户请求具有报告管理权限的报告。 选择跟踪审核数据的适当报告。 如果您的报告请求需要批准，系统会向您发送电子邮件报警。

在排定报告之前，请执行以下步骤：

1. 登录到具有管理权限的用户控制台。
2. 转到“角色和任务”、“修改管理任务”并选择要修改的审核报告。
3. 选择“选项卡”选项卡，然后单击“IAM ReportServerScheduler”进行编辑。
4. 选择“启用重现选项”复选框。
5. 单击“确定”和“提交”。

遵循这些步骤:

1. 登录到具有报告任务用户权限的用户控制台。
2. 依次选择“报告”、“报告任务”、“请求报告”。

   随即将显示报告列表。
3. 选择基于审核的报告。

   此时将显示参数屏幕。
4. 单击“排定报告”，并为您的报告选择日程。

   立即

   指定立即运行报告。

   一次

   指定报告在特定时间段内运行一次。选择想要生成报告的开始日期、结束日期、开始时间和结束时间。

   （仅审核报告）按小时

   指定在开始时间生成报告，之后每“n”小时生成一次；“n”表示连续报告之间的时间间隔。 选择开始日期、结束日期、开始时间、结束时间和连续报告之间的时间间隔。

   （仅审核报告）按天

   指定在开始时间生成报告，之后每“n”天生成一次；“n”表示连续报告之间的时间间隔。 选择开始日期、结束日期、开始时间、结束时间和连续报告之间的时间间隔。

   （仅审核报告）按周

   指定从开始日期开始，每周在选定的日期生成报告。 选择想要生成报告的开始日期、结束日期、开始时间和结束时间。

（仅审核报告）按月

指定从开始日期开始每月生成报告，之后每“n”个月生成一次。“n”表示连续报告之间的时间间隔。 选择开始日期、结束日期、开始时间、结束时间和连续报告之间的时间间隔。

（仅审核报告）在该月份的第 N 天运行报告

指定在所选月份特定一天生成报告。选择想要生成报告的开始日期、结束日期、开始时间和结束时间。

（仅审核报告）第一个星期一

指定在该月份的第一个星期一生成报告。选择想要生成报告的开始日期、结束日期、开始时间和结束时间。

（仅审核报告）该月份的最后一天

指定在该月份最后一天生成报告。 选择想要生成报告的开始日期、结束日期、开始时间和结束时间。

（仅审核报告）每个月的第 N 个星期的第 X 天

指定在每月特定周的特定一天生成报告。选择想要生成报告的开始日期、结束日期、开始时间和结束时间。 例如，您可以在每月第三周的星期五生成报告。

5. 单击“提交”。

报告请求即会提交。 根据您的环境配置，请求会立即运行，或在管理员批准后运行。

通常，报告请求必须先由系统管理员或具有报告管理权限的其他用户批准，然后系统才能完成该请求。 需要批准的原因是，一些报告的运行可能需要很长时间或重要的系统资源。 如果您的报告请求需要批准，系统会向您发送电子邮件报警。

注意：如果需要批准，请启用环境的工作流。

查看报告

根据您的环境配置，在管理员批准报告请求后，报告将可用于查看。 如果您的报告请求正在等待批准，系统会向您发送电子邮件报警。 在获得批准前，您要查看的报告不会显示在搜索列表中。

注意：要使用“查看我的报告”任务查看 CA Identity Manager 中的报告，请在您的浏览器中启用第三方会话 cookie。

遵循这些步骤:

1. 在用户控制台中，依次选择“报告”、“报告任务”，然后单击“查看我的报告”。
2. 搜索要查看的生成报告。

   重现生成报告和即时报告实例都会显示出来。

   注意：如果该报告的状态为未决/周期，则不会生成报告，且可能需要花费时间完成。
3. 选择您想要查看的报告。
4. （可选）单击“导出此报告”（左上角）将该报告导出为以下格式：
   - Crystal Reports
   - PDF
   - Microsoft Excel (97-2003)
   - Microsoft Excel (97-2003) 仅数据
   - Microsoft Excel (97-2003) - 可编辑
   - RTF 文本格式
   - 分隔值 (CSV)
   - XML

清除审核数据库

审核数据库最终可能会累计不再需要的记录。 要删除这些记录，请执行 db\auditing 目录中的以下数据库程序：

`garbageCollectAuditing12 environment-ID MM/DD/YYYY`

environment-ID

定义 CA Identity Manager 环境的 ID

MM/DD/YYYY

定义日期，此日期前的审核记录必须删除。

第 9 章： 生产环境

本部分提供了迁移功能特定部分的分步操作说明。 请确保仅在开发环境中进行了有限更改且对这些更改非常了解时才使用它。

此部分包含以下主题：

迁移管理角色和任务定义

您可以自定义 CA Identity Manager 角色和任务，以便满足公司的特定需要。 自定义包括创建或修改管理角色和任务，也包括为管理角色和任务使用“创建”或“修改”任务。

另一方法是在 roledefinition.xml 文件中修改角色和任务，但*不建议*这样。 因为存在编辑错误风险，所以在所做更改非常有限时才能使用这一方法。

此流程仅迁移管理角色和任务定义。 如果角色与组织绑定，则请考虑迁移整个 CA Identity Manager 环境。

重要说明！ 如果您在生产环境中更改角色或任务定义，则在您从开发环境导入角色或任务定义时，更改会丢失。 导入角色和任务定义会覆盖同样名称的现有角色和任务定义。

导出管理角色和任务定义

如果直接对 roledefinition.xml 文件进行更改，则可以将此文件直接导入生产环境。 否则，要导出角色和任务定义：

1. 如果您有策略服务器群集，请检查只有一个策略服务器正在运行。
2. 停止一个以外的所有其余 CA Identity Manager 节点。
3. 登录到管理控制台。
4. 单击“CA Identity Manager environments”（CA Identity Manager 环境）。
5. 选择要导出角色和任务定义的 CA Identity Manager 环境。

6. 单击“Roles”（角色），然后单击“Export”（导出），并为文件提供一个名称。
7. 按照下一步骤中的说明导入此文件。

导入管理角色和任务定义

遵循这些步骤:

1. 将上一步骤中创建的文件复制到生产环境。
2. 登录到生产环境中的管理控制台。
3. 单击“CA Identity Manager environments”（CA Identity Manager 环境）。
4. 选择适当的 CA Identity Manager 环境。
5. 单击“Roles”（角色）。
6. 单击“Import”（导入）并指定导出生成的 XML 文件的名称。
7. 如果这些步骤成功，启动您停止的任何其他策略服务器和 CA Identity Manager 节点。

   注意：如果仍要在 CA Identity Manager 环境中进行任何更改，请重复第 6 步。

验证角色和任务导入

要验证成功导入了角色和任务，请以能够使用以下任务的管理员帐户登录 CA Identity Manager：

- 修改管理角色
- 修改管理任务

执行这些任务，并验证角色和任务反映了最新导入的角色定义。

迁移 CA Identity Manager 面板

CA Identity Manager 面板可以自定义，以使应用程序具有特定外观。如果您已经为一组用户修改或创建了新的面板，请使用下列步骤将面板从开发迁移到生产环境。

如果您修改了面板，请复制修改的文件。

遵循这些步骤:

1. 将新的和修改的文件从开发服务器复制到生产服务器，如映像文件、样式表、属性文件以及控制台页面 (index.jsp)。
2. 如果使用了多个面板，请配置 SiteMinder 响应。

   注意：有关使用多个面板的详细信息，请参阅*《配置指南》*。

要验证面板的迁移，请登录用户控制台，然后检查面板是否正确显示。

在生产环境中更新 CA Identity Manager

在将 CA Identity Manager 从开发迁移到生产之后，您可能需要执行增量更新。要将新的 CA Identity Manager 功能从开发环境迁移到生产环境，请执行下列步骤：

1. 迁移 CA Identity Manager 环境。
2. 复制 iam_im.ear。
3. 迁移工作流流程定义。

迁移 CA Identity Manager 环境

CA Identity Manager 环境是在管理控制台中创建的。 CA Identity Manager 环境包含一系列角色和任务定义、工作流定义以及使用 CA Identity Manager API 创建的自定义功能，还包含一个 CA Identity Manager 目录。

遵循这些步骤:

1. 如果 CA Identity Manager 与 SiteMinder 集成，并且您有策略服务器群集，请检查只有一个策略服务器正在运行。
2. 停止一个以外的所有其余 CA Identity Manager 节点。
3. 从开发环境的管理控制台导出 CA Identity Manager 环境。
4. 在生产环境的管理控制台中导入导出的环境。
5. 如果 CA Identity Manager 与 SiteMinder 集成，请在策略服务器用户界面中重新保护 CA Identity Manager 领域。

   在您导出 CA Identity Manager 环境时，不会从策略存储中导出策略域。
6. 重新启动您停止的策略服务器和 CA Identity Manager 节点。

在迁移 CA Identity Manager 环境时，会发生以下活动：

- 如果同一对象存在于两个位置，开发服务器上的更改会覆盖生产服务器上的更改。
- 如果新对象是在开发环境中创建的，则会被添加到生产服务器。
- 如果新对象是在生产服务器上创建的，则会保持。

导出 CA Identity Manager 环境

要在生产系统上部署 CA Identity Manager 环境，通过开发或预运行系统导出环境，再将该环境导入到生产系统。

注意：在您导入先前导出的环境时，CA Identity Manager 会在管理控制台的状态窗口中显示日志。 要查看此日志中每个管理对象及其属性的验证和部署信息，请在您导出环境*之前*，在“Environment Properties”（环境属性）页面上选择“Enable Verbose Log Output”（启用详细日志输出）字段。请注意选择“Enable Verbose Log Output”（启用详细日志输出）字段在导入期间可能引起重大性能问题。

遵循这些步骤:

1. 在管理控制台中单击“Environments”（环境）。

   显示 CA Identity Manager 环境屏幕，其中包含 CA Identity Manager 环境列表。

2. 选择要导出的环境。
3. 单击“Export”（导出）按钮。

   此时显示“File Download”（文件下载）屏幕。

4. 将 ZIP 文件保存到生产系统可以访问的位置。
5. 单击“Finish”（完成）。

   将环境信息导出为 ZIP 文件，您可以将此文件导入到其他环境。

导入 CA Identity Manager 环境

在从开发系统导出 CA Identity Manager 环境之后，您可以将它导入生产系统。

遵循这些步骤:

1. 在管理控制台中单击“Environments”（环境）。

   显示 CA Identity Manager 环境屏幕，其中包含 CA Identity Manager 环境列表。

2. 单击“Import”（导入）按钮。

   此时将显示“Import Environment”（导入环境）屏幕。

3. 浏览找到导入环境所需的 ZIP 文件。
4. 单击“Finish”（完成）。

将环境导入 CA Identity Manager。

验证 CA Identity Manager 环境迁移

要验证 CA Identity Manager 环境迁移正确，请确认生产环境的策略服务器的策略服务器用户界面中显示了该 CA Identity Manager 环境。

在策略服务器用户界面中，验证下列几点：

- CA Identity Manager 用户目录设置准确。
- 新的 CA Identity Manager 域存在
- 正确的身份验证架构保护 CA Identity Manager 领域。

此外，在登录管理控制台后，验证在您选择“Environments”（环境）后 CA Identity Manager 环境会显示。

迁移针对 JBoss 的 iam_im.ear

每次将功能从开发环境迁移到生产环境时，都要重新部署 iam_im.ear。 通过迁移整个 EAR，可以确保您的生产环境与开发环境相同。

遵循这些步骤:

1. 将 iam_im.ear 从您的开发环境复制到您的生产环境可以访问的位置。
2. 在 iam_im.ear 的副本中，编辑策略服务器连接信息，以使其反映生产环境。

   要完成此更改，请将 *jboss_home*/server/default/iam_im.ear/policyserver_rar/META-INF/ra.xml 从生产环境复制到 iam_im.ear。
3. 按照步骤 2 将安装的 iam_im.ear 替换为您的开发环境的 iam_im.ear 的副本：
   a. 在生产服务器上，删除 iam_im.ear：

      cluster_node_jboss_home\server\default\deploy\iam_im.ear

   b. 将已删除文件替换为开发环境的 iam_im.ear 的经过编辑的副本。
4. 针对群集中的每个节点重复这些步骤。

迁移针对 WebLogic 的 iam_im.ear

每次将功能从开发环境迁移到生产环境时，都要重新部署 iam_im.ear。 通过迁移整个 EAR，可以确保您的生产环境与开发环境相同。

遵循这些步骤:

1. 保存策略服务器连接信息。

   策略服务器连接信息存储在 policyserver_rar/WEB-INF 目录的 ra.xml 文件中。将此文件复制到其他位置，以便重新部署之前可以在 iam_im.ear 中替换它。

2. 将 iam_im.ear 复制到 WebLogic 管理服务器可以访问的位置。

3. 替换策略服务器连接信息。

   在 iam_im.ear 中，将 policyserver_rar/WEB-INF/ra.xml 文件替换为步骤 1 中保存的文件。

4. 重新部署 iam_im.ear

   a. 登录到 WebLogic 控制台。

   b. 转到“Deployments”（部署）、“Application”（应用程序）、“Identity Manager”。

在“Deploy”（部署）选项卡上，选择“Deploy (Re-Deploy) Application”（部署（重新部署）应用程序）。

迁移针对 WebSphere 的 iam_im.ear

遵循这些步骤:

1. 将 *imsInstall.jacl* 脚本从 *was_im_tools_dir**WebSphere-tools* 复制到 *deployment_manager_dir* *bin* 目录，其中：

   - *was_im_tools_dir* 是安装了针对 WebSphere 的 CA Identity Manager 工具的开发系统目录。
   - *deployment_manager_dir* 是部署管理器的安装位置。

2. 在您配置 CA Identity Manager 应用程序的开发系统中，将 *was_im_tools_dir* *WebSphere-tools**imsExport.bat* 或 *imsExport.sh* 复制到 *was_home**bin*。

3. 在命令行上，导航到 *was_home**bin*。

4. 确保 WebSphere 应用程序服务器正在运行。

5. 按如下所示导出部署的 CA Identity Manager：

   对于 Windows，输入此命令：

   ```
   imsExport.bat "path-to-exported-ear"
   ```

   其中，*path-to-exported-ear* 是 imsExport 实用工具创建的完整路径和文件名。

   对于 Windows 系统，在指定 was_im.ear 的路径时请使用正斜杠 (/) 而不要使用反斜杠 (\)。 例如：

   ```
   imsExport.bat "c:/program files/CA/CA Identity Manager/
   exported_ear/iam_im.ear"
   ```

   对于 UNIX，输入此命令：

   ```
   ./wsadmin -f imsExport.jacl -conntype RMI -port 2809 path to exported ear
   ```

   其中，*path-to-exported-ear* 是包含导出的 EAR 文件的文件名的完整路径。

6. 将导出的 EAR 文件从您导出该文件的开发系统中的位置复制到安装了部署管理器的系统中的位置。

7. 将 *was_im_tools_dir*/WebSphere-ear/iam_im.ear/policyserver_rar/META-INF/ra.xml 替换为来自生产环境的文件。

   ra.xml 文件包含了策略服务器连接信息。

8. 在安装了部署管理器的系统中，部署 Identity Manager EAR：

   a. 从命令行导航到：

      deployment_manager_dir \bin。

   b. 请确保 WebSphere 应用程序正在运行。

   c. 运行 imsInstall.jacl 脚本，如下所示：

   注意：执行 imsInstall.jacl 脚本可能会花费几分钟时间。

   Windows：

   wsadmin -f imsInstall.jacl *"path-to-copied-ear" cluster_name*

   其中，*path-to-copied-ear* 是包含您复制到部署管理器系统的 Identity Manager EAR 的文件名的完整路径。

   例如：

   wsadmin -f imsInstall.jacl "c:\Program Files\CA\Identity Manager\WebSphere-tools\was_im.ear" im_cluster

UNIX：

./wsadmin -f imsInstall.jacl *path-to-copied-ear cluster_name*

其中，*path-to-copied-ear* 是包含您复制到部署管理器系统的 Identity Manager EAR 的文件名的完整路径。

例如：

./wsadmin -f imsInstall.jacl /opt/CA/Identity Manager/WebSphere-tools/was_im.ear im_cluster

9. 如果 CA Identity Manager 与 SiteMinder 集成，请验证下列几点：
   - SiteMinder 代理可以连接到您的策略存储。
   - 策略服务器可以连接到用户存储。
   - CA Identity Manager 域已创建。

迁移工作流流程定义

如果您在开发环境中使用了工作流，请导出工作流定义并将其导入到生产环境中。 然后，在每个服务器节点配置工作流。

导出流程定义

在开发环境系统中，导出工作流流程定义。

遵循这些步骤:

1. 确保应用程序服务器正在运行。
2. 转到 *admin_tools*\Workpoint\bin\ and run Archive.bat（对于 Windows）或 Archive.sh（对于 UNIX），如下所示：
   a. 在“导入”对话框中，选择根对象。
   b. 单击“添加”。
   c. 指定要生成的文件的名称。
   d. 单击“导出”。
   e. 单击“执行”。

   admin_tools 引用管理工具，该工具默认安装在以下位置之一：
   - **Windows：** C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools
   - **UNIX：** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools
3. 按照下一部分“导入流程定义” (p. 227)中的说明进行操作。

导入流程定义

在生产环境系统中，导入工作流流程定义。

遵循这些步骤:

1. 重新启动应用程序服务器。
2. 如需要，请按照以前的步骤导出定义，创建当前定义的备份副本。
3. 转到 *admin_tools*\Workpoint\bin\ 并按如下所示运行 Archive 脚本：
   a. 在“导入”对话框中，选择要导入的所有项。
   b. 当系统提示您使用新格式还是旧格式时，请保留旧格式。

      新格式不支持 CA Identity Manager。
   c. 提供导出时生成的文件的名称。
   d. 单击“执行”。

   admin_tools 引用管理工具，该工具默认安装在以下位置之一：

   - **Windows：** C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools
   - **UNIX：** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

第 10 章： CA Identity Manager 日志

此部分包含以下主题：

如何跟踪 CA Identity Manager 中的问题

CA Identity Manager 提供了以下方法来记录状态和跟踪问题：

“查看提交的任务”任务

显示 CA Identity Manager 环境中所有事件和任务的状态。管理员在用户控制台中使用此任务。

“查看提交的任务”提供以下类型的信息：

- 该环境中发生的事件和任务的列表。
- 与事件有关的属性的列表。
- 成功和失败事件
- 处于未决或停滞状态的事件。
- 拒绝的事件，包括拒绝理由
- 帐户同步状态
- 身份策略同步状态
- 配给信息（在启用配给时）。

应用程序服务器日志

显示 CA Identity Manager 安装中的所有组件的信息，并提供 CA Identity Manager 中的所有操作的详细信息。

日志文件的位置和类型取决于您使用的是下列应用程序服务器类型中的哪一种：

- WebLogic－CA Identity Manager 信息被写入标准输出。 默认情况下，标准输出是运行服务器实例的控制台窗口。
- JBoss－CA Identity Manager 信息被写入运行服务器实例的控制台窗口，并写入 *jboss_home*\server\log\server.log
- WebSphere－CA Identity Manager 信息被写入运行服务器实例的控制台窗口，并写入 *was_home*\AppServer\logs*server_name*\SystemOut

有关详细信息，请参阅您的应用程序服务器的文档。

目录服务器日志文件

包含了用户目录中发生的活动方面的信息。

记录的信息类型和日志文件的位置取决于您使用的目录服务器的类型。 有关详细信息，请参阅目录的服务器文档。

策略服务器日志文件

在 CA Identity Manager 与 SiteMinder 集成时，显示下列信息：

- SiteMinder 连接问题
- SiteMinder 身份验证问题
- SiteMinder 策略存储中 CA Identity Manager 管理的对象的信息。
- 密码策略评估

有关配置 SiteMinder logs 日志的信息，请参阅 *《CA SiteMinder Web Access Manager Policy Server Administration Guide》*。

策略服务器探查器

如果 CA Identity Manager 与 SiteMinder 集成，允许您跟踪内部策略服务器诊断信息和处理功能，包括与 CA Identity Manager 有关的功能。

有关详细信息，请参阅"如何跟踪组件和数据字段" (p. 230)。

Web 代理日志文件

如果 CA Identity Manager 与 SiteMinder 集成，Web 代理将信息写入下列两个日志：

- 错误日志文件－包含程序和运行级别的错误，例如未能与策略服务器通讯的 Web 代理。
- 跟踪日志文件－包含警告和通知消息，例如跟踪消息和流状态消息。还包括头详细信息和 Cookie 变量等数据。

注意：有关 Web 代理日志文件的详细信息，请参阅 *《CA SiteMinder Web Access Manager Web Agent Configuration Guide》*。

如何跟踪组件和数据字段

在 CA Identity Manager 与 SiteMinder 集成时，您可以使用 SiteMinder 策略服务器探查器跟踪策略服务器的 CA Identity Manager 扩展中的组件和数据字段。 该探查器让您可以配置跟踪输出筛选器，以便仅捕获组件或数据字段的特定值。

注意：有关使用策略服务器探查器的说明，请参阅 *《CA SiteMinder Web Access Manager Policy Server Administration Guide》*。

您可以为下列组件启用跟踪：

Function_Begin_End

在执行策略服务器的 CA Identity Manager 扩展中的特定方法时，提供低级跟踪语句。

IM_Error

跟踪 SiteMinder 策略服务器的 CA Identity Manager 扩展中的运行时错误。

IM_Info

提供 CA Identity Manager 扩展的常规跟踪信息。

IM_Internal

跟踪有关内部 CA Identity Manager 操作的常规信息。

IM_MetaData

在 CA Identity Manager 处理目录元数据时，提供跟踪信息。

IM_RDB_Sql

提供关系数据库的跟踪信息。

IM_LDAP_Provider

提供 LDAP 目录的跟踪信息。

IM_RuleParser

跟踪解析和评估成员、所有者和管理策略的过程，这些策略在运行时进行解释的一个 XML 文件中定义。

IM_RuleEvaluation

跟踪对成员、管理员、所有者以及作用域规则的评估。

IM_MemberPolicy

跟踪对成员策略的评估，包括成员资格和作用域。

IM_AdminPolicy

跟踪对管理策略的评估。

IM_OwnerPolicy

跟踪对所有者策略的评估。

IM_RoleMembership

跟踪有关角色成员资格的信息，例如用户具有的角色列表和某一特定角色的成员列表。

IM_RoleAdmins

跟踪有关角色管理的信息，例如用户可以管理的角色列表和某一特定角色的管理员列表。

IM_RoleOwners

跟踪有关角色所有权的信息，例如用户拥有的角色列表和某一特定角色的所有者列表。

IM_PolicyServerRules

跟踪对成员规则的评估（例如策略服务器已解析的 RoleMember、RoleAdmin、RoleOwner）和作用域规则（例如 AccessTasks 的“所有”规则和“AccessTaskFilter”规则）

IM_LLSDK_Command

跟踪内部 CA Identity Manager SDK 和策略服务器之间的通信。技术支持使用此跟踪组件。

IM_LLSDK_Message

跟踪消息通过 Java 代码从内部 CA Identity Manager SDK 显式发送到策略服务器。 技术支持使用此跟踪组件。

IM_IdentityPolicy

跟踪身份策略的评估和应用。

IM_PasswordPolicy

跟踪对密码策略的评估。

IM_Version

提供有关 CA Identity Manager 版本的信息。

IM_CertificationPolicy

跟踪对认证策略的评估。

IM_InMemoryEval

跟踪 CA Identity Manager 策略的处理，包括成员、管理员、所有者和身份策略。 技术支持使用此跟踪组件。

IM_InMemoryEvalDetail

提供关于 CA Identity Manager 策略（包括成员、管理员、所有者和身份策略）的处理的其他信息。 技术支持使用此跟踪组件。

在 *《CA SiteMinder Web Access Manager Policy Server Administration Guide》* 中列出了您可以配置跟踪的数据字段。

第 11 章： CA Identity Manager 保护

此部分包含以下主题：

用户控制台安全性

用户控制台是管理员可以用来在 CA Identity Manager 环境中管理用户、组和组织等对象的用户界面。 为这些对象分配了关联角色和任务集。 在管理员登录到用户控制台时，与管理员有关的任务显示在该环境中。

默认情况下，CA Identity Manager 使用本地身份验证保护对用户控制台的访问。CA Identity Manager 管理员输入有效的用户名和密码，才能登录到 CA Identity Manager 环境。CA Identity Manager 根据 CA Identity Manager 管理的用户存储对用户名和密码进行身份验证。

如果 CA Identity Manager 与 SiteMinder 集成，CA Identity Manager *自动*使用 SiteMinder 基本身份验证来保护该环境。使用基本身份验证不需要其他配置。您可以使用 SiteMinder 管理用户界面配置高级身份验证方法。

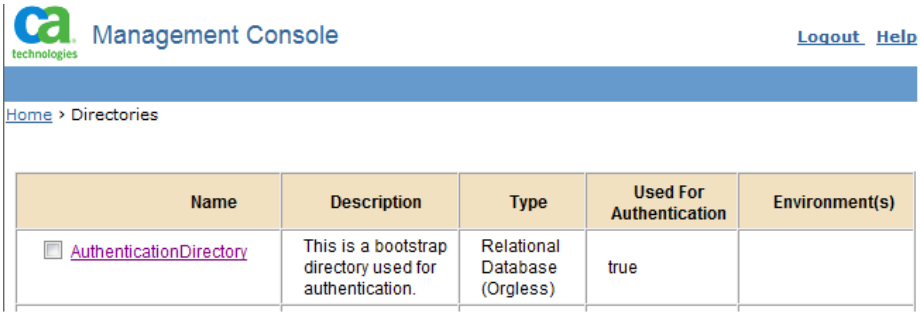
注意：有关详细信息，请参阅 *《CA SiteMinder Web Access Manager Policy Server Configuration Guide》*。

管理控制台安全

管理控制台使管理员能够创建和管理 CA Identity Manager 目录和环境。 管理员也可以使用管理控制台为环境配置自定义功能。

CA Identity Manager 安装包括了保护管理控制台安全的选项。 默认为选中此选项。 在安装期间，您要指定 CA Identity Manager 用来对可以访问管理控制台的管理员进行身份验证的凭据。 CA Identity Manager 使用您在名为“AuthenticationDirectory”的 bootstrap 目录中提供的凭据创建用户。 您可以在管理控制台中查看此目录。

注意：在 CA Identity Manager 与 CA SiteMinder 集成时，您不得使用本地安全性来保护管理控制台。



添加其他管理控制台管理员

默认情况下，受本地 CA Identity Manager 安全性保护的管理控制台有一个管理员帐户，该帐户是安装期间在新的 CA Identity Manager 目录中创建的。

要添加其他管理员，请指定包含需要访问管理控制台的用户的 CA Identity Manager 目录。 使用现有目录时，您可以向组织内的用户授予管理控制台访问权限，而不必创建新帐户。

您只能为身份验证指定一个目录。 您不得删除为身份验证配置的目录。

遵循这些步骤:

1. 使用安装期间您提供的用户凭据登录到管理控制台。
2. 打开目录，然后单击包含请求管理控制台访问权限的用户的目录。
3. 单击“Update Authentication”（更新身份验证）。
4. 选择“Used for Authentication”（用于身份验证）选项。
5. 输入第一个用户的登录名，然后单击“Add”（添加）。
6. 继续添加请求管理控制台访问权限的用户，直到添加完所有用户。 然后，单击“Save”（保存）。

   您指定的用户现在可以使用其用户名和密码访问管理控制台。

禁用管理控制台的本地安全性

如果您启用了管理控制台的本地安全性，但现在想要使用其他应用程序来为其提供保护，请禁用本地安全性，然后再实施其他安全方法。

遵循这些步骤:

1. 在 web.xml 文件中禁用管理控制台的本地安全性，如下所示：
   a. 在文本编辑器中打开 *CA Identity Manager_installation*\iam_im.ear\management_console.war\WEB-INF\web.xml。
   b. 将 ManagementConsoleAuthFilter 的 Enable 参数的值设为 false，如下所示：

```
<filter>
<filter-name>ManagementConsoleAuthFilter</filter-name>
<filter-class>com.netegrity.ims.manage.filter.Management
ConsoleAuthFilter</filter-class>
<init-param>
<param-name>Enable</param-name>
<param-value>false</param-value>
</init-param>
</filter>
```

   c. 保存 web.xml 文件。
2. 重新启动 CA Identity Manager 服务器。

   管理控制台不再由本地安全性保护。

使用 SiteMinder 保护管理控制台安全

要对管理控制台进行最初的保护，您可以创建 SiteMinder 策略。

SiteMinder 策略会识别您希望保护的资源（如管理控制台），并授予一组用户对该资源的访问权限。

遵循这些步骤:

1. 针对管理控制台禁用本地安全性 (p. 235)。
2. 作为具有域权限的管理员登录到下列界面之一：
   - 对于 CA SiteMinder r12 或更高版本，登录到管理 UI。
   - 对于 CA SiteMinder 6.0 SP*x*，登录到策略服务器用户界面。

   注意：有关使用这些界面的信息，请参阅正在使用的 SiteMinder 的版本的文档。
3. 为适当的 CA Identity Manager 环境找到策略域。

   在 CA Identity Manager 与 SiteMinder 集成时，此域是自动创建的。域名具有以下格式：

   *Identity Manager-environment*Domain

   在此格式中，*Identity Manager-environment* 指定了您要修改的环境的名称。例如，在名称为 *employees* 时，域名为 *employees*Domain。
4. 使用下列资源筛选器创建领域：

   /iam/immanage/
5. 创建领域规则。 指定星号 (*) 作为筛选器可以保护管理控制台中的所有页面。
6. 创建新的策略，并将其与您在前一步骤中创建的规则关联起来。

   确保将可以访问管理控制台的用户与策略关联。
7. 重新启动应用程序服务器。

在升级之后保护现有环境

在升级到 CA Identity Manager 12.6 或更高版本后，您可以使用本地安全性保护管理控制台。

注意：在 CA Identity Manager 与 CA SiteMinder 集成时，您不能使用本地 CA Identity Manager 安全性保护管理控制台。

遵循这些步骤：

1. 在 web.xml 文件中启用管理控制台的本地安全性，如下所示：
   a. 在文本编辑器中打开 *CA Identity Manager_installation*\iam_im.ear\management_console.war\WEB-INF\web.xml。
   b. 将 ManagementConsoleAuthFilter 的 Enable 参数的值设为 true，如下所示：

```
<filter>
<filter-name>ManagementConsoleAuthFilter</filter-name>
<filter-class>com.netegrity.ims.manage.filter.Management
ConsoleAuthFilter</filter-class>
<init-param>
<param-name>Enable</param-name>
<param-value>true</param-value>
</init-param>
</filter>
```

   c. 保存 web.xml 文件。
2. 在 CA Identity Manager 对象存储中创建 IM_AUTH_USER 表。

   IM_AUTH_USER 表存储关于管理控制台管理员的信息。
   a. 导航到 CA\Identity Manager\IAM Suite\Identity Manager\tools\db\objectstore
   b. 针对对象存储运行下列脚本之一：
      - sql_objectstore.sql
      - oracle_objectstore.sql

   注意：有关针对现有数据库运行脚本的信息，请访问该数据库的供应商文档。

3. 使用密码工具来加密用户密码。

   密码工具随 CA Identity Manager 工具安装在以下位置：

Windows: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\PasswordTool

UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools/PasswordTool

   PasswordTool

   使用以下命令运行密码工具：
   `pwdtools -JSAFE -p anypassword`

   “JSAFE”选项使用 PBE 算法加密纯文本值。

1. 将 bootstrap 用户信息插入 IM_AUTH_USER 表。在 IM_AUTH_USER 表中指定所有列的值。

   例如：

   USER_NAME: admin1

   PASSWORD: *anypassword*

   DISABLED: 0

   ID:1

2. 重新启动 CA Identity Manager 服务器。

   管理控制台由本地安全性保护。

CSRF 攻击保护

CA Identity Manager 经过了增强，以改善对跨站请求伪造 (CSRF) 攻击的抵御。默认情况下，CA Identity Manager 中禁用了这一增强功能。

要启用该增强功能：

1. 打开位于以下位置的 web.xml 文件：

   application-server/iam_im.ear/user_console.war/WEB-INF

2. 找到带有 <param-name> csrf-prevention-on 的 <context-param> 元素。
3. 将 <param-value> 设为 true。
4. 重新启动应用程序服务器。

第 12 章： CA SiteMinder 集成

此部分包含以下主题：

SiteMinder 和 CA Identity Manager

在 CA Identity Manager 与 CA SiteMinder 集成时，CA SiteMinder 可以将以下功能添加到 CA Identity Manager 环境中：

高级身份验证

CA Identity Manager 默认包括 CA Identity Manager 环境的本地身份验证。 CA Identity Manager 管理员输入有效的用户名和密码，才能登录到 CA Identity Manager 环境。 CA Identity Manager 根据 CA Identity Manager 管理的用户存储对用户名和密码进行身份验证。

在 CA Identity Manager 与 CA SiteMinder 集成时，CA Identity Manager 使用 CA SiteMinder 基本身份验证来保护环境。 在您创建 CA Identity Manager 环境时，会在 CA SiteMinder 中创建策略域和身份验证方案，以保护该环境。

在 CA Identity Manager 与 CA SiteMinder 集成时，您也可以使用 SiteMinder 身份验证保护管理控制台。

访问角色和任务。

访问角色使 CA Identity Manager 管理员能够在 CA SiteMinder 保护的应用程序中分配权限。 访问角色表示用户可以在业务应用程序中执行的单个操作，如在财务应用程序中生成订购单。

目录映射

管理员可能需要管理某些用户，这些用户的配置文件所在的用户存储和对该管理员进行身份验证时使用的用户存储不同。 在管理员登录到 CA Identity Manager 环境时，身份验证使用的是一个目录，获得管理用户的授权使用的是另一个不同的目录。

在 CA Identity Manager 与 CA SiteMinder 集成时，您可以配置 CA Identity Manager 环境，以针对身份验证和授权使用不同目录。

不同用户集的面板

面板用来更改用户控制台的外观。 在 CA Identity Manager 与 CA SiteMinder 集成时，您可以让不同组的用户看到不同的面板。要完成此更改，请使用 SiteMinder 响应将面板与一组用户关联起来。 响应会与策略中同一组用户关联的规则配对。 在规则生效时，会触发该响应，将有关面板的信息传递给 CA Identity Manager，来构建用户控制台。

注意：有关详细信息，请参阅*《User Console Design Guide》*。

本地化环境的区域设置首选项

在 CA Identity Manager 与 CA SiteMinder 集成时，您可以使用 imlanguage HTTP 头定义用户的区域设置首选项。 在 SiteMinder 策略服务器中，您在 SiteMinder 响应内设置此头，并且指定某一用户属性作为头的值。 此 imlanguage 头作为最高优先级区域设置首选项发挥作用。

注意：有关详细信息，请参阅 *《User Console Design Guide》*。

更多信息：

使用自定义身份验证方案来收集用户凭证 (p. 284)

资源保护方式

高级身份验证要求您在实施中使用 SiteMinder 策略服务器。 托管 CA Identity Manager 服务器的应用程序服务器所在的操作环境与 Web 服务器不同。 要提供转发服务，Web 服务器需要：

- 应用程序服务器供应商提供的插件。
- 保护“用户控制台”、“自行注册”和“忘记密码”功能等 CA Identity Manager 资源的 SiteMinder 代理。

Web 代理控制 请求 CA Identity Manager 资源的用户的访问权限。 在用户通过身份验证并获得授权后，Web 代理将允许 Web 服务器处理请求。

Web 服务器收到请求时，应用程序服务器插件会将其转发给托管 CA Identity Manager 服务器的应用程序服务器。

Web 代理保护用户和管理员可见的 CA Identity Manager 资源。

SiteMinder 与 CA Identity Manager 集成概述

在策略管理员和身份管理员协力将 SiteMinder 集成到现有 CA Identity Manager 安装时，CA Identity Manager 体系结构扩展为包括以下组件：

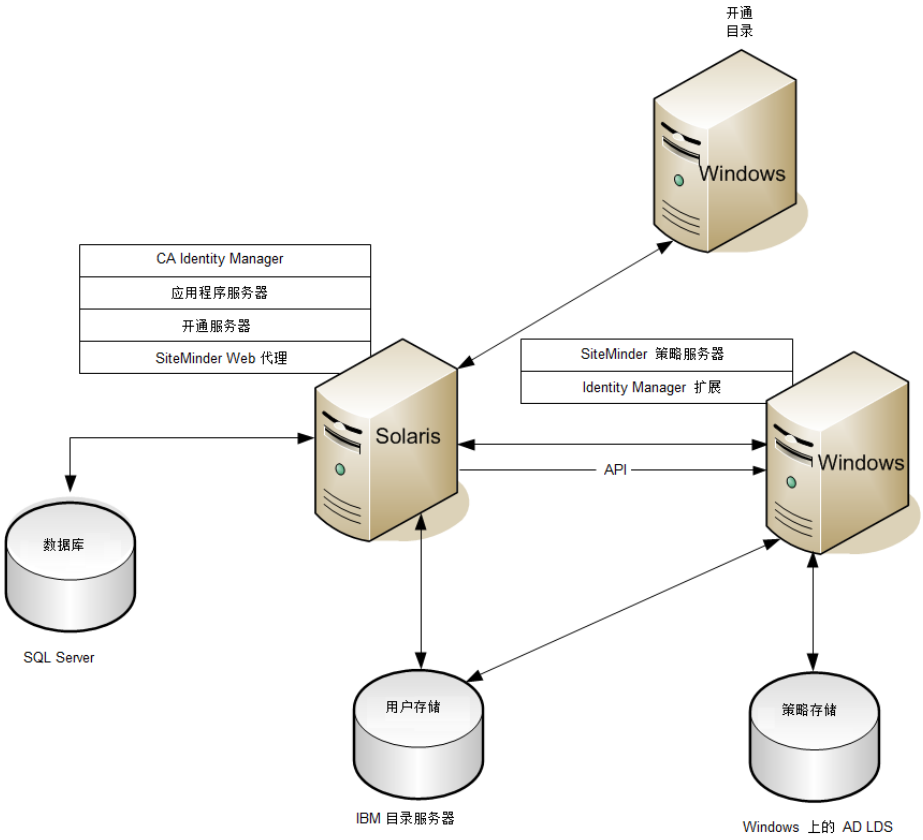
SiteMinder Web 代理

保护 CA Identity Manager 服务器。 Web 代理安装在 CA Identity Manager 服务器所在的系统中。

SiteMinder 策略服务器

向 CA Identity Manager 提供高级身份验证和授权。

下图是包含 SiteMinder 策略服务器和 Web 代理的 CA Identity Manager 安装示例：

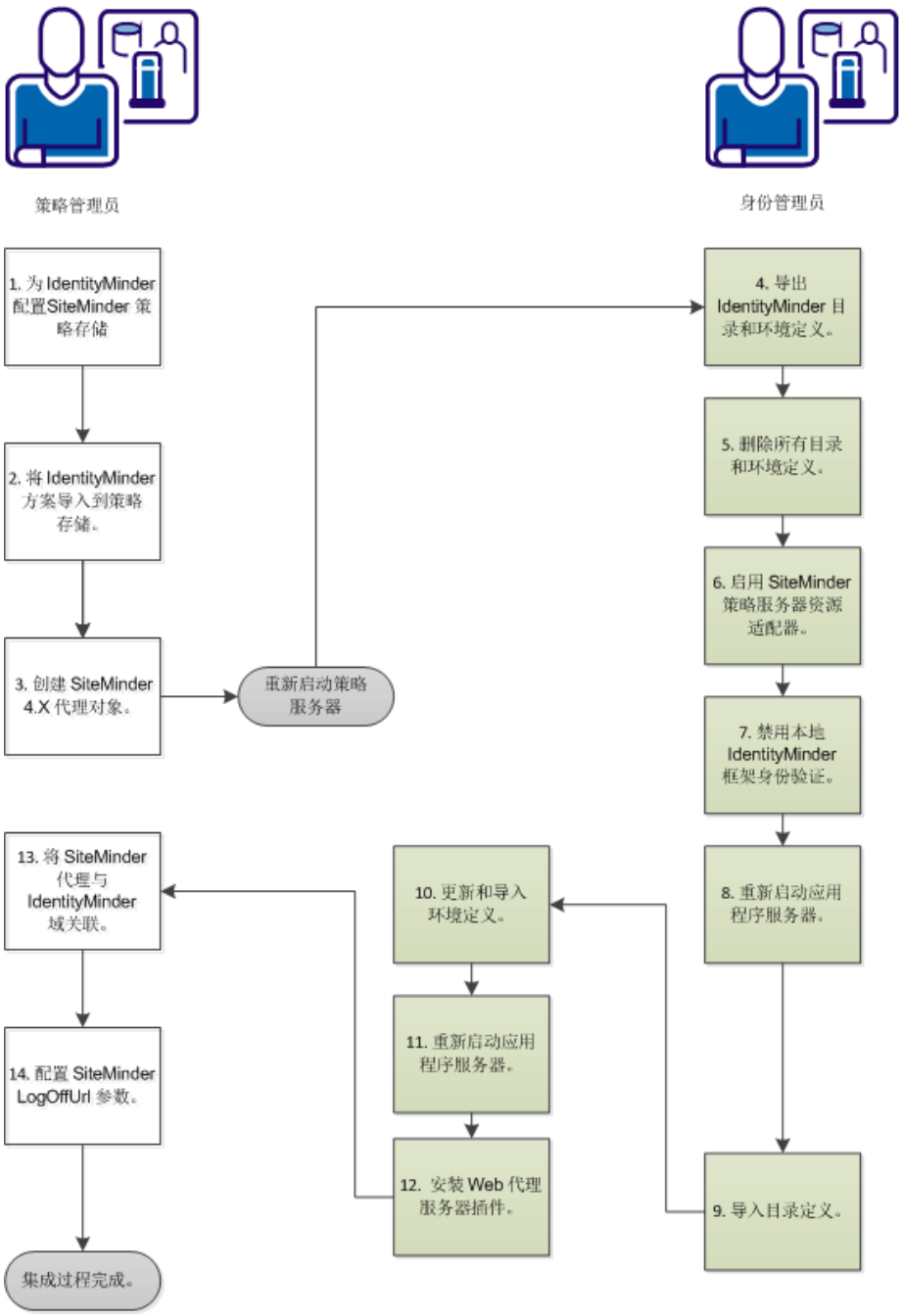


注意：作为示例，组件被安装在了不同平台上。但是，您可以选择其他平台。CA Identity Manager 数据库安装在 Microsoft SQL Server 中，用户存储安装在 IBM 目录服务器中。 SiteMinder 策略存储安装在 Windows 的 AD LDS 中。

完成此过程需要两个角色：CA Identity Manager 身份管理员和 SiteMinder 策略管理员。 在一些组织中，这两个角色由一个人充任。 在两个人参与时，完成此方案中的步骤需要紧密的合作。 策略管理员开始并结束此过程；身份管理员完成中间的所有步骤。

重要说明！ 对于以 Release12.5 SP7 开始的 CA Identity Manager 安装，需要 Java Cryptography Extension Unlimited Strength Jurisdiction Policy Files（JCE 库）。 从 Oracle 网站下载这些库。 将其加载到以下文件夹：
<Java_path>\<jdk_version>\jre\lib\security\。

下图说明了将 SiteMinder 集成到 CA Identity Manager 的完整过程：



遵循这些步骤:

1. 为 CA Identity Manager 配置 SiteMinder 策略存储。 (p. 244)
2. 将 CA Identity Manager 架构导入策略存储。 (p. 249)
3. 创建 SiteMinder 4.X 代理对象。 (p. 250)
4. 导出 CA Identity Manager 目录和环境。 (p. 251)
5. 删除所有目录和环境定义。 (p. 251)
6. 启用 SiteMinder 策略服务器资源适配器。 (p. 252)
7. 禁用本地 CA Identity Manager 框架身份验证筛选器。 (p. 253)
8. 重新启动应用程序服务器。 (p. 253)
9. 为 SiteMinder 配置数据源。 (p. 254)
10. 导入目录定义。 (p. 254)
11. 更新并导入环境定义。 (p. 255)
12. 重新启动应用程序服务器。 (p. 253)
13. 安装 Web 代理服务器插件。 (p. 255)
14. 将 SiteMinder 代理与 CA Identity Manager 域关联。 (p. 271)
15. 配置 SiteMinder LogOffUrl 参数。 (p. 272)

为 CA Identity Manager 配置 SiteMinder 策略存储

作为策略管理员，您可以使用 CA Identity Manager 管理工具来访问 SQL 脚本或 LDAP 架构文本，以将 IMS 架构添加到策略存储中。 身份管理员应已将这些工具安装在了“Admin Tools”文件夹中。 按照以下步骤之一配置策略存储：

配置关系数据库 (p. 245)

配置 Sun Java 系统目录服务器或 IBM 目录服务器 (p. 245)

配置 Microsoft Active Directory (p. 246)

配置 Microsoft ADAM (p. 246)

配置 CA 目录服务器 (p. 247)

配置 Novell eDirectory 服务器 (p. 248)

配置 Oracle Internet 目录 (OID) (p. 249)

配置关系数据库

完成配置之后，您可以使用关系数据库作为 SiteMinder 策略存储。

遵循这些步骤:

1. 将数据库配置为支持的 SiteMinder 策略存储。

   注意：有关配置说明，请参阅*《SiteMinder Policy Server Installation Guide》*。

2. 针对数据库运行适当脚本：

   - **SQL：** C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\policystore-schemas\MicrosoftSQLServer\ims8_mssql_ps.sql
   - **Oracle：** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools/policystore-schemas/OracleRDBMS/ims8_oracle_ps.sql

   前面的路径是默认安装位置。 您的安装位置可能不同。

配置 Sun Java 系统目录服务器或 IBM 目录服务器

要配置 Java 或 IBM 目录服务器，请应用适当的架构文件。

遵循这些步骤:

1. 将此目录配置成受支持的 SiteMinder 策略存储。

   注意：有关配置说明，请参阅*《CA SiteMinder Policy Server Installation Guide》*。

2. 将适当的 LDIF 架构文件添加到目录中。 LDIF 文件的默认 Windows 位置是 C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\policystore-schemas。

   为您的目录添加以下架构文件：

   - **IBM 目录服务器：**

     IBMDirectoryServer\V3.identityminder8

   - **Sun Java 系统目录服务器 (iPlanet)：**

     SunJavaSystemDirectoryServer\sundirectory_ims8.ldif

配置 Microsoft Active Directory

要配置 Microsoft Active Directory 策略存储，请应用 activedirectory_ims8.ldif 脚本。

遵循这些步骤:

1. 将此目录配置成受支持的 SiteMinder 策略存储。

   注意：有关配置说明，请参阅*《CA SiteMinder Policy Server Installation Guide》*。

2. 按如下所示修改 activedirectory_ims8.ldif 架构文件：

   a. 在文本编辑器中，打开 activedirectory_ims8.ldif 文件。 默认 Windows 位置为：

      C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\policystore-schemas\MicrosoftActiveDirectory

   b. 将 {root} 的所有实例替换为目录的根组织。

      该根组织必须与您在策略服务器管理控制台中配置策略存储时指定的根组织匹配。

      例如，如果根为 dc=myorg,dc=com，请将 dn: CN=imdomainid6,CN=Schema,CN=Configuration,{root} 替换为 dn: CN=imdomainid6,CN=Schema,CN=Configuration,dc=myorg,dc=com

   c. 保存文件。

3. 按照文档中的说明为您的目录添加架构文件。

配置 Microsoft ADAM

要配置 Microsoft ADAM 策略存储，请应用 adam_ims8.ldif 脚本。

遵循这些步骤:

1. 将此目录配置成受支持的 SiteMinder 策略存储。

   注意：有关配置说明，请参阅*《CA SiteMinder Policy Server Installation Guide》*。

   记下 CN 值（guid 字符串）。

2. 按如下所示修改 adam_ims8.ldif 架构文件：

   a. 在文本编辑器中打开 adam_ims8.ldif\.ldif 文件。 默认 Windows 位置为：

      C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\policystore-schemas\MicrosoftActiveDirectory

   b. 将每个 cn={guid} 参考替换为您在此程序第 1 步中配置 SiteMinder 策略存储时发现的字符串。

例如，如果 guid 字符串是 CN={39BC711D-7F27-4311-B6C0-68FDEE2917B8}，那么将每个 cn={guid} 参考替换为 CN={39BC711D-7F27-4311-B6C0-68FDEE2917B8}。

c. 保存文件。

3. 按照文档中的说明为您的目录添加架构文件。

配置 CA 目录服务器

要配置 CA 目录服务器，请创建自定义架构文件。在以下步骤中，*dxserver_home* 是 CA 目录的安装目录。 此文件在 Windows 中的默认源位置是 C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\policystore-schemas\eTrustDirectory。

遵循这些步骤:

1. 将此目录配置成受支持的 SiteMinder 策略存储。

   注意：有关配置说明，请参阅《*CA SiteMinder Policy Server Installation Guide*》。

2. 将 etrust_ims8.dxc 复制到 *dxserver_home*\config\schema。

3. 按如下所示创建自定义架构配置文件：

   a. 将 *dxserver_home*\config\schema\default.dxg 复制到 *dxserver_home*\config\schema*company_name*-schema.dxg。

   b. 编辑 *dxserver_home*\config\schema*company_name*-schema.dxg 文件，在文件底部添加以下行：

   ```
   # Identity Manager Schema
   source "etrust_ims8.dxc";
   ```

4. 编辑 *dxserver_home*\bin\schema.txt 文件，在文件结尾添加 etrust_ims_schema.txt 的内容。 此文件在 Windows 中的默认源位置是 C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\policystore-schemas\eTrustDirectory。

5. 按如下所示创建自定义限制配置文件：

   a. 将 *dxserver_home*\config\limits\default.dxc 复制到 *dxserver_home*\config\limits*company_name*-limits.dxc。

   b. 按如下所示在 *dxserver_home*\config\limits*company_name*-limits.dxc 文件中将默认大小限制增加为 5000：

   ```
   set max-op-size=5000
   ```

   注意：升级 CA 目录会覆盖 limits.dxc 文件。 因此，在升级完成后务必将 max-op-size 重置为 5000。

6. 按如下所示编辑 *dxserver_home*\config\servers*dsa_name*.dxi：

```
# 架构
source "company_name-schema.dxg";

#service limits
source "company_name-limits.dxc";
```

其中，*dsa_name* 是使用自定义配置文件的 DSA 的名称。

7. 运行 dxsyntax 实用工具。
8. 作为 dsa 用户停止并重新启动 DSA，以便使架构更改生效，如下所示：

```
dxserver stop dsa_name
dxserver start dsa_name
```

配置 Novell eDirectory 服务器

要配置 Novell eDirectory 服务器策略存储，请应用 novell_ims8.ldif 脚本。

遵循这些步骤:

1. 将此目录配置成受支持的 SiteMinder 策略存储。

注意：有关配置说明，请参阅《*CA SiteMinder Policy Server Installation Guide*》。

2. 在安装策略服务器的系统的命令窗口中输入以下信息，查找您的 Novell eDirectory 服务器的 NCPServer 的识别名称 (DN)：

```
ldapsearch -h hostname -p port -b container -s sub
-D admin_login -w password objectClass=ncpServer dn
```

例如：

```
ldapsearch -h 192.168.1.47 -p 389 -b "o=nwqa47container" -s sub -D
"cn=admin,o=nwqa47container" -w password objectclass=ncpServer dn
```

3. 打开 novell_ims8.ldif 文件。
4. 将每个 NCPServer 变量替换为您在第 2 步中找到的值。

novell_ims8.ldif 在 Windows 中的默认位置是：

C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\policystore-schemas\NovelleDirectory

例如，如果 DN 值是“cn=servername,o=servercontainer”，则您应将 *NCPServer* 的每个实例替换为“cn=servername,o=servercontainer”。

5. 使用 novell_ims8.ldif 文件更新 eDirectory 服务器。

有关说明，请参阅 Novell eDirectory 文档。

配置 Oracle Internet 目录 (OID)

要配置 Oracle Internet 目录，请更新 oracleoid ldif 文件。

遵循这些步骤:

1. 将此目录配置成受支持的 SiteMinder 策略存储。

   注意：有关配置说明，请参阅*《CA SiteMinder Policy Server Installation Guide》*。

2. 使用 oracleoid_ims8.ldif 文件更新 Oracle Internet 目录服务器。 此文件在 Window 中的默认安装位置是：

   install_path\policystore-schemas\OracleOID\

   有关说明，请参阅 Oracle Internet 目录文档。

验证策略存储

要验证策略存储，请确认下列几点：

- 您的策略服务器日志不包含以下列代码开始的警告部分：
  `*** IMS NO SCHEMA BEGIN`

  只有在您已经为 SiteMinder 策略服务器安装扩展，但却没有扩展策略存储架构时，此警告才会出现。

- 策略存储数据库或目录中存在 CA Identity Manager 对象。 CA Identity Manager 对象以 ims 前缀开始。

将 CA Identity Manager 架构导入策略存储

策略管理员将 CA Identity Manager 架构导入策略存储。 此任务允许 CA Identity Manager 创建、更新和删除策略对象。 示例包括目录对象、域、领域、规则、策略以及启用访问角色和任务的策略对象。

遵循这些步骤:

1. 在 SiteMinder 策略服务器上，关闭策略服务器服务。
2. 针对您正在使用的版本运行 CA Identity Manager 安装程序。
3. 当问及哪些组件要安装时，为 SiteMinder 选择扩展（如果 SiteMinder 在本地安装）。
4. 验证策略服务器服务重新启动，然后继续。

创建 SiteMinder 4.x 代理对象

策略管理员创建 SiteMinder 4.x Web 代理。 此任务使 SiteMinder 和 CA Identity Manager 之间能够通信。 身份管理员在 CA Identity Manager 配置期间会引用此代理。

遵循这些步骤:

1. 登录到 SiteMinder 管理 UI。

   您的管理员权限的相关选项卡出现。

2. 依次单击“基础架构”、“代理”、“代理”和“创建代理”。

   此时显示“创建代理”对话框。

3. 选择“创建类型为代理的新对象”，然后单击“确定”。

   此时显示“创建代理”对话框。

4. 输入名称和可选说明。

   注意：请使用易于和相应的 SharePoint 连接向导关联的名称。

5. 选择“SiteMinder”。

6. 从下拉列表中选择“Web 代理”。

7. 按照下列步骤启用 4.x 功能：

   a. 选中“支持 4.x 代理”复选框。

      此时显示信任设置字段。

   b. 完成以下字段以添加信任设置：

      IP 地址

      指定策略服务器的 IP 地址。

      共享密钥

      指定与 4.x 代理对象关联的密码。SharePoint 连接向导也需要此密码。

      确认密钥

      确认与 4.x 代理对象关联的密码。SharePoint 连接向导也需要确认此密码。

8. 单击“提交”。

   此时提交“创建代理对象”任务以进行处理，并显示确认信息。

导出 CA Identity Manager 目录和环境

集成流程将会删除当前所有的环境和目录定义。 为了确保能保留此信息，身份管理员应使用 CA Identity Manager 管理控制台导出环境。 在完成集成之后，这些定义会还原目录和环境。

遵循这些步骤:

1. 打开 CA Identity Manager 管理控制台。
2. 单击“Directories”（目录）。
3. 单击列表中的第一个目录，然后单击“Export”（导出）。
4. 保存目录 xml 文件并将其存档。
5. 对剩余的目录重复执行此流程。
6. 单击“Home”（主页），然后单击“Environments”（环境）。
7. 选择第一个环境。
8. 单击“Export”（导出）。
9. 对剩余的环境重复执行此流程。

   注意：对每个环境执行此流程都会花费几分钟的时间。

删除所有目录和环境定义

身份管理员需要使用 CA Identity Manager 管理控制台来删除目录和环境定义，以便为 SiteMinder 保护 CA Identity Manager 做好准备。

遵循这些步骤:

1. 打开 CA Identity Manager 管理控制台。
2. 单击“环境”。
3. 选择第一个环境。
4. 单击“删除”。
5. 对剩余的每个环境重复执行此流程。

   注意：由于环境引用目录，请在删除这些目录之前删除您的环境。
6. 导航回到“Directories”（目录）部分。
7. 选择列出的所有目录。
8. 单击“删除”。

启用 SiteMinder 策略服务器资源适配器

身份管理员启用 SiteMinder 策略服务器资源适配器。 适配器用于验证 SMSESSION cookie。 在完成验证之后，SiteMinder 创建用户上下文。

遵循这些步骤:

1. 在正在运行 CA Identity Manager 的应用程序服务器上，导航到位于 iam_im.ear 之内的 \policysever.rar\META-INF 文件夹。
2. 在编辑器中打开 ra.xml 文件。
3. 搜索已启用的配置属性，然后将“配置属性值”更改为“true”，如下例所示：

```
        <config-property-name>validateSmHeadersWithPS</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>true</config-property-value>
    </config-property>
    <config-property>
        <config-property-name>Enabled</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>true</config-property-value>
    </config-property>
    <!-- Set FIPS Mode to true if SiteMinder is in FIPS Only Mode -->
    <config-property>
        <config-property-name>FIPSMode</config-property-name>
```

4. 找到属性 ConnectionURL，然后提供 SiteMinder 策略服务器的主机名。 请使用完全限定域名 (FQDN)。
5. 找到属性 UserName，并指定用于与 SiteMinder 通讯的帐户。 此帐户的默认值为 SiteMinder。
6. 找到属性 AdminSecret。 提供加密的密码。 从导出的文件 directory.xml 中复制密码，然后将其粘贴到 ra.xml。 如果您不能确定是否拥有一个普通密码，请使用 CA Identity Manager 密码工具来加密密码。
7. 将加密密码粘贴到 ra.xml 文件。
8. 指定策略管理员在 SiteMinder 配置期间创建的 4.x 代理名称。
9. 指定加密密码。 在必要时使用密码工具来加密密码。
10. 保存对 ra.xml 文件所做的更改。

此时已启用 SiteMinder 策略服务器资源适配器。

更多信息：

修改 SiteMinder 密码或共享密钥 (p. 299)

禁用本地 CA Identity Manager 框架身份验证筛选器

使用 SiteMinder 适配器后，不再需要框架身份验证筛选器。 身份管理员可以禁用此筛选器。

遵循这些步骤:

1. 在 iam_im.ear 下的 \user_console.war\WEB-INF 文件夹中查找并编辑 web.xml 文件。
2. 找到 FrameworkAuthFilter，然后将“启用 init-param”的值切换为 false。

   如果您正在使用 CA Identity Manager r12.5 SP7 或更高版本，请确认 Java Cryptographic Extension Unlimited Strength Jurisdiction Policy Files (JCE) 已下载到 CA Identity Manager 环境中的 \<Java_path>\<jdk_version>\jre\lib\security。这些文件使 CA Identity Manager 能够连接到 SiteMinder。

   如果已安装 JCE 库，您能够在 CA Identity Manager 应用程序的启动期间看到以下消息：

   ```
   2012-07-06 11:23:56,079 WARN  [ims.default] (main) * 启动步骤 2：正在尝试启动 PolicyServerService
   2012-07-06 11:23:56,081 WARN  [ims.default] (main) Unlimited Strength Java Crypto Extensions 已启用：TRUE
   ```

   否则，“Unlimited Strength Java Crypto Extensions 已启用”条目的值为 false。CA Identity Manager 无法连接到策略服务器。

重新启动应用程序服务器

重新启动会使用所做更改刷新应用程序服务器。 身份管理员会验证切换是否成功，以及是否存在连接到 SiteMinder 策略服务器的正确连接。

遵循这些步骤:

1. 当应用程序服务器作为服务运行时，请使用服务面板来重新启动 CA Identity Manager。
2. 参阅 server.log 以验证连接

为 SiteMinder 配置数据源

如果您的 CA Identity Manager 环境使用关系数据库作为其身份存储，则需要身份管理员在 SiteMinder 策略服务器上完成一个额外步骤。 SiteMinder 需要本地的数据源来与数据库进行通信。

遵循这些步骤:

1. 对于 Windows 服务器，打开“管理工具”下的“ODBC 数据源管理员”控制台。
2. 单击“系统 DSN”选项卡。
3. 单击“添加”，然后选择与您的数据库对应的 SiteMinder 驱动程序。
4. 提供所需的信息以引用关系数据库用户存储。
5. 在继续后面操作之前测试连接。

导入目录定义

为了能够导入环境，身份管理员需要先导入环境所引用的目录。 在 CA Identity Manager 中导入目录定义时，也会将目录信息添加到 SiteMinder 策略存储中。

遵循这些步骤:

1. 确保 CA Identity Manager 正在运行并且已连接到 SiteMinder，
2. 导航到 CA Identity Manager 管理控制台
3. 单击“Directories”（目录），然后单击“Create or Update from XML”（通过 XML 创建或更新）。
4. 选择您的目录配置文件 (directory.xml)。 这是您在“导出 CA Identity Manager 目录和环境” (p. 251)中导出的文件。
5. 单击“下一步”。
6. 单击“Finish”（完成）并且查看加载输出。 确认该目录存在于 CA Identity Manager 和 SiteMinder。
7. 对“配给存储”和剩余的任何目录重复这些步骤。
8. 登录到 SiteMinder 管理用户界面，以验证创建用户目录的结果。

更新并导入环境定义

身份管理员将更新后的环境重新导入到 CA Identity Manager。

遵循这些步骤:

1. 有别于目录导出，环境以 zip 文件的形式导出。 从 zip 文件中拖动出一个 *name*.xml 文件的副本。
2. 复制 *name*.xml 文件。 在元素 ImsEnvironment 的末尾、封闭的 /> 括号之前插入对保护代理（非 SM 4.x 代理）的引用：*agent="idmadmin"*。
3. 保存文件并将其粘贴回 zip 文件。
4. 打开 CA Identity Manager 管理控制台，然后依次单击“Environments”（环境）、“Import”（导入）。
5. 输入更新后的环境 zip 文件的名称。
6. 单击“Finish”（完成）并查看导入输出结果。
7. 对剩余的所有环境重复此流程。
8. 重新启动应用程序服务器。

安装 Web 代理服务器插件

取决于已安装的应用程序，身份管理员需要安装以下插件中的一个，这些插件是 Web 服务器将请求转发至应用程序服务器所使用的插件：

- WebSphere (p. 256)
- JBoss (p. 261)
- WebLogic (p. 265)

在 WebSphere 上安装代理插件

安装了 Web 代理的 Web 服务器将请求转发到托管 CA Identity Manager 服务器的应用程序服务器。 供应商提供的 Web 服务器代理插件提供此服务。

执行以下适用于您的部署的步骤：

1. 配置 IBM HTTP 服务器 (p. 256)（所有的 Web 服务器）
2. 配置代理插件 (p. 256)（所有的 Web 服务器）
3. 以下之一：
   - 完成 IIS 上的配置 (p. 259)
   - 完成 iPlanet 或 Apache 上的配置 (p. 261)

配置 IBM HTTP 服务器

对于所有 Web 服务器，您安装代理插件并且使用 configurewebserver 命令。

遵循这些步骤:

1. 从 WebSphere Launch Pad 安装代理插件。
2. 通过运行 configurewebserver1.bat 命令，将 Web 服务器添加到 WebSphere 单元中，如下所示：
   a. 在文本编辑器中编辑 *websphere_home*\Plugins\bin\configurewebserver1.bat/.sh。
   b. 在 wsadmin.bat/.sh 后面添加用户名和密码，如下所示：
   `wsadmin.bat -user wsadmin -password password -f configureWebserverDefinition.jacl`
   c. 运行 configurewebserver1.bat/.sh。

   注意：有关 configurewebserver 命令的详细信息，请参阅 IBM WebSphere 文档。
3. 继续执行配置代理插件 (p. 256)这一步骤。

配置代理插件

对于所有 Web 服务器，您可以使用 WebSphere 的 GenPluginCfg 命令来更新插件：

遵循这些步骤:

1. 登录到安装了 WebSphere 的系统。
2. 从命令行中导航到 *websphere_home*\bin（*websphere_home* 为 WebSphere 的安装位置）。

   例如：

   - **Windows：**

     C:\Program Files\WebSphere\AppServer\profile\AppSrv01\bin
   - **UNIX：**

     /*home_dir*/WebSphere/AppServer/profile/AppSrv01/bin
3. 运行 GenPluginCfg.bat 或 GenPluginCfg.sh 命令。

   运行此命令后将在以下位置生成 plugin-cfg.xml 文件：

   websphere_home\AppServer\profiles\AppSrv01\config\cells
4. 继续执行以下步骤之一：
   - 完成 IIS 上的配置 (p. 259)
   - 完成 iPlanet 或 Apache 上的配置 (p. 261)

完成 IIS (7.x) 上的配置

开始执行此步骤之前，请确认您正在使用的是 6.1.0.9 或更新版本的 Web 服务器插件。 插件的早期版本不支持 Windows Server 2008 操作系统。

遵循这些步骤:

1. 安装带有 IIS 版本 6.0 管理兼容性组件的 IIS 版本 7.x。 默认情况下不安装 IIS 版本 6.0 管理兼容性组件。
2. 完成下列步骤以打开 Windows Server 2008 的“服务器管理器”窗口：
    1. 依次单击“开始”、“管理工具”、“服务器管理器”。
    2. 依次单击“操作”、“添加角色”，然后单击“下一步”。
    3. 在“选择服务器角色”页面上选择“Web 服务器 (IIS)”角色，然后单击“下一步”。
    4. 单击“添加功能”，在显示 Windows 进程激活服务功能的提示之后，单击“下一步”。
    5. 在 IIS 简介页面上单击“下一步”。
3. 当显示“角色服务”窗口时，请确保除已选择的默认选项外，以下选项也被选中。
    - Internet 信息服务：管理工具
    - IIS 版本 6.0 管理兼容性：IIS 版本 6.0 管理控制台、IIS 版本 6.0 脚本工具、IIS 版本 6.0 WMI 兼容性以及 IIS 元数据库兼容性
    - 应用程序开发：ISAPI 扩展、ISAPI 筛选器
4. 单击“下一步”以启用所选择的选项，然后在下一窗口上单击“安装”以执行安装。
5. 安装完成后，单击“安装结果”窗口上的“关闭”。
6. 打开命令提示符，并转到：\Program Files\IBM\WebSphere\AppServer\profiles\Dmgr01\bin。
7. 运行此命令：GenPluginCfg.bat。

    将在以下位置生成 plugin-cfg.xml 文件：C:\Program Files\IBM\WebSphere\AppServer\profiles\Dmgr01\config\cells。
8. 在 c:\ 下创建目录，例如：c:\plugin。
9. 将 plugin-cfg.xml 文件复制到 c:\plugin 目录。
10. 将 iisWASPlugin_http.dll 文件复制到 c:\plugin 目录。
11. 在 Windows Server 2008 操作系统上，依次选择“开始”、“所有程序”、“管理工具”、“Internet 信息服务 (IIS) 管理器”。 此操作将启动 IIS 应用程序，并为 Web 站点实例创建新的虚拟目录。这些说明假定您正在使用的是默认网站。
12. 展开左侧的树，直到您能看到“默认网站”。
13. 右键单击“默认网站”，单击“添加虚拟目录”以使用默认安装来创建目录。

14. 在虚拟目录创建向导的“虚拟目录别名”窗口中的“别名”字段上输入“setPlugins”。
15. 浏览到向导的“网站内容目录”窗口“物理路径”字段中的 c:\plugin 目录，然后单击“确定”。
16. 单击“测试设置”按钮。如果设置测试失败，您可以更改物理目录的权限。或者，选择“连接为”，以便让 IIS 作为具有物理路径中的文件权限的 Windows 用户帐户进行连接。
17. 单击“确定”以将虚拟目录 setPlugins 添加到您的网站。
18. 在导航树中选择您刚才创建的 setPlugins 虚拟目录。
19. 双击“处理程序映射”，然后在“操作”面板上单击“编辑功能权限”。
20. 如果尚未选择“脚本”和“执行”，请将其选中。
21. 单击“确定”。
22. 返回到“IIS 管理器”窗口，然后在该窗口左侧的导航树中展开“网站”文件夹。
23. 在导航树中选择“默认网站”。
24. 在“默认网站属性”面板上完成下列步骤，以便添加 ISAPI 筛选器：
    1. 双击“ISAPI 筛选器”选项卡。
    2. 单击以打开“添加/编辑筛选器属性”对话框。
    3. 在“筛选器名称”字段输入 iisWASPlugin。
    4. 单击“浏览”以选择位于 c:\plugin\iisWASPlugin_http.dll 目录中的插件文件。
    5. 单击“确定”以关闭“添加/编辑筛选器属性”对话框。
25. 选择导航树中的顶层服务器节点。
26. 双击“功能”面板上“ISAPI 和 CGI 限制”。

    要确定指定给“ISAPI 或 CGI 路径”属性的值，请浏览并选择您在前一步骤中所选的相同插件文件。 例如：c:\plugin\iisWASPlugin_http.dll。
27. 单击“操作”面板上的“添加”。
28. 在“说明”字段中输入 WASPlugin，选择“允许执行扩展路径”，然后单击“确定”以关闭“ISAPI 和 CGI 限制”对话框窗口。

29. 在位置 c:\plugin 中创建新文件 plugin-cfg.loc。将 plugin-cfg.loc 文件中的值设置为配置文件的位置。 默认位置是 C:\plugin\plugin-cfg.xml。

更新 Web 代理

在配置 IIS 7.x 之后，对 Web 代理做出以下更改：

1. 单击“应用程序池”，并将“默认应用程序池”更改为“经典”模式。
2. 单击“提交”。
3. 确保该代理在 ISAPI 筛选优先级列表中要高于由 CA Identity Manager 使用的应用程序服务器的插件。
4. 重新启动 IIS 版本 7.x 和 WebSphere 应用程序服务器配置文件。

完成 IIS 上的配置

当您完成对 IBM HTTP 服务器和代理插件的配置后，请确保代理 plugin-cfg.xml 位于正确的位置，并且执行步骤来配置其他插件文件。

遵循这些步骤:

1. 按照如下方法复制 plugin-cfg.xml：
   a. 登录到安装了 Web 代理的系统。
   b. 在 C: 驱动器下创建不包含空格的文件夹。 例如：C:\plugin。
   c. 将 plugin-cfg.xml 文件复制到 C:\plugin 文件夹。
2. 在 C:\plugin 文件夹中创建命名为 plugin-cfg.loc 的文件，并将下列行添加到文件：

   C:\plugin\plugin-cfg.xml
3. 从 www.ibm.com 下载 Websphere 插件安装程序，并保存到安装了 WebSphere 的系统中。
4. 转到 WebSphere Plugin 安装程序所在的位置。
5. 使用以下命令来生成 iisWASPlugin_http.dll 文件：

   ```
   install is:javahome "c:\IBM\WebSphere\AppServer\Java
   ```

   根据您的配置回答所显示的问题。

   结束向导后，iisWASPlugin_http.dll 文件将保存在 C:\IBM\WebSphere\Plugs\bin 文件夹中。 查找 32 位或 64 位子文件夹。

6. 将 iisWASPlugin_http.dll 文件复制到具有 Web 代理的系统的 C:\plugin 文件夹。
7. 按照如下方法创建虚拟目录：
   a. 打开“IIS 管理器”。
   b. 右键单击“默认网站”。
   c. 单击“新建虚拟目录”并且提供以下值：

      别名：sePlugins（区分大小写。）

      路径：c:\plugin

      权限：读取 + 执行（ISAPI 或 CGI）
8. 按照如下方法添加 ISAPI 筛选器：
   a. 右键单击“默认网站”。
   b. 单击“属性”。
   c. 在“ISAPI 筛选器”选项卡上单击“添加”。
   d. 提供以下值：

      筛选器名称：sePlugins

      可执行文件：c:\plugin\iisWASPlugin_http.dll
9. 按照以下所述创建 Web 服务扩展：
   a. 在 IIS6 管理器中，展开计算机名。
   b. 创建一个 Web 服务扩展并将其设置为允许。

      扩展名称：WASPlugin

      路径：C:\plugin\iisWASPlugin_http.dll
   c. 右键单击每个 Web 服务扩展以将其更改为允许状态。
10. 重新启动 IIS Web 服务器。

    在主 WWW 服务中，确保 WebSphere 插件 (sePlugin) 显示在 SiteMinder Web 代理插件之后，并且已成功启动 WebSphere 插件。

完成 iPlanet 或 Apache 上的配置

完成对 IBM HTTP 服务器和代理插件的配置之后，请确保代理 plugin-cfg.xml 位于正确的位置并重新启动 Web 服务器。

遵循这些步骤:

1. 将 plugin-cfg.xml 从安装代理插件的系统中复制到以下位置：

   websphere_home\AppServer\profiles*server_name*\config\cells*websphere_cel*\nodes\webserver1_node\servers\webserver1\

2. 确保在所有 iPlanet Web 服务器上，在 SiteMinder Web 代理插件 (NSAPIWebAgent.so) 之后加载 WebSphere 插件 (libns41_http.so)。

3. 检查 IPlanet 6.0 Web 服务器的 *iplanet_home*/https-*instance*/config/magnus.conf 中的插件顺序。

4. 将下列行从 *iplanet_home*/https-*instance*/config/magnus.conf 复制到 *iplanet_home*/https-*instance*/config/obj.conf（IPlanet 5.x Web 服务器）：

   ```
   Init fn="load-modules" funcs="as_init,as_handler,as_term"
   shlib="/export/WebSphere/AppServer/bin/libns41_http.so"

   Init fn="as_init"
   bootstrap.properties="/export/WebSphere/AppServer/config/cells/plugin-cfg.xml"
   ```

   在 obj.conf 文件中 AuthTrans fn="SiteMinderAgent" 之后添加以下代码：

   ```
   Service fn="as_handler"
   ```

5. 确保在 Apache Web 服务器上，先于 WebSphere 插件 (mod_ibm_app_server_http.so) 加载 SiteMinder Web 代理插件 (mod2_sm.so)。 此命令位于 *apache_home*/config/httpd.conf 中的“Dynamic Shared Object (DSO) Support（动态共享对象 (DSO) 支持）”部分，

6. 重新启动 Web 服务器。

安装 JBoss 代理插件

在 SiteMinder Web 代理对 CA Identity Manager 资源请求进行验证和授权之后，Web 服务器将请求转发至托管 CA Identity Manager 服务器的应用程序服务器。要转发这些请求，需要在安装 SiteMinder Web 代理的系统上安装和配置 JK Connector。 有关 JK Connector 的详细信息，请参阅下列 Jakarta Project 网站：

http://community.jboss.org/wiki/usingmodjk12withjboss

CA Identity Manager 管理工具包含可供您用于配置 JK Connector 的示例配置文件。 有关说明，请参阅下表所述的目录中的 readme.txt 文件：

平台	位置
Windows 系统上的 IIS Web 服务器	C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\samples\ConnectorConfiguration\windows\IIS_JBoss*
Solaris 系统上的 Sun Java System Web 服务器	/opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools/samples/ConnectorConfiguration/solaris/Iplanet_JBoss*
Solaris 系统上的 Apache Web 服务器	/opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools/samples/ConnectorConfiguration/solaris/apache_JBoss*

安装和配置 JBoss 应用程序插件 (IIS 7.x)

此步骤说明如何配置随 IIS 7.0 启动的 JBoss Apache 插件

遵循这些步骤:

1. 在文件系统中部署和更新 ISAPI 筛选器。

   将 ISAPI 文件夹部署在 C 驱动器的根目录。

2. 编辑解压的文件夹中的 jakarta.reg 文件。

   如果 ISAPI 文件夹位于 C:\ 根目录，请勿更改此文件。 如果该文件夹位于其他文件夹，请在第 9、11 和 12 行中指定该文件夹。

3. 保存更改，然后双击以更新注册表。

4. 通过指定 JBoss 应用程序服务器的位置，来编辑 workers.properties 文件。端口和类型无需更改。

5. 在 Windows 2008 上安装 IIS7 或 IIS7.5。

6. 打开系统管理器，并确认已安装了 IIS ISAPI 筛选器和 ISAPI 扩展。

7. 在“运行”窗口中启动 inetmgr。

8. 选择 m/c 名称，然后双击“ISAPI 和 CGI 限制”。

9. 单击右边面板上的“添加”按钮。

10. 此时显示“添加 ISAPI 或 CGI 限制”窗口。

11. 选择 isapi_redirect.dll，然后输入 ISAPI 作为说明。

12. 选择“允许执行扩展路径”。

13. 单击“ISAPI 或 CGI 限制”窗口中的“确定”。

14. 在“连接”部分中展开“站点”，选择“默认网站”，然后右键单击“添加虚拟目录”。
15. 输入“jakarta”作为别名，然后在物理路径中输入文件 isap_redirect.dll(c:\ajp) 的位置。
16. 单击“测试设置”按钮：
    - 如果已通过身份验证和授权，单击“确定”。
    - 如果授权失败，单击“连接为”按钮。
17. 选择特定用户并提供管理用户名和密码。
18. 再次单击“测试设置”按钮。 这次授权通过。
19. 单击左侧的“默认网站”，然后双击“ISAPI 筛选器”。
20. 单击右边面板上的“添加”按钮。
21. 输入名称并且提供 isapi_redirect.dll 文件的位置。
22. 单击“确定”。
23. 展开“默认网站”，然后单击 jakarta 虚拟目录。
24. 双击“处理程序映射”。
25. 选择“ISAPI-dll”，然后单击“编辑功能权限”。
26. 确认已选择所有的权限（读取、脚本、执行）。
27. 单击“确定”。

更新 Web 代理

在配置 IIS 7.x 之后，对 Web 代理做出以下更改：

1. 单击“应用程序池”，并将“默认应用程序池”更改为“经典”模式。
2. 单击“提交”。
3. 确保该代理在 ISAPI 筛选优先级列表中要高于由 CA Identity Manager 使用的应用程序服务器的插件。

JBoss 插件配置完毕。

安装和配置 JBoss 应用程序插件 (IIS 6.0)

此集成流程假定，SiteMinder 在到达 CA Identity Manager 之前进行用户验证和授权。 用户需要在到达 CA Identity Manager 之前拥有 SMSESSION cookie。 请使用受 SiteMinder Web 代理保护的应用程序插件（代理重定向）。 通过此配置，SiteMinder 对用户进行身份验证，然后在创建 SMSESSION cookie 之后，将其重定向到 CA Identity Manager。

下列步骤适用于部署和配置 IIS 6.0 的 JBoss Apache 插件：

遵循这些步骤:

1. 在文件系统上部署和更新 ISAPI 筛选器。

   确保将 ISAPI 文件夹部署到 C 驱动器的根目录。

2. 编辑解压的文件夹中的 jakarta.reg 文件。

   如果 ISAPI 文件夹位于 C:\ 根目录，请勿更改此文件。 如果该文件夹位于其他文件夹，请在第 9、11 和 12 行中指定该文件夹。

3. 保存更改，然后双击以更新注册表。

4. 通过指定 JBoss 应用程序服务器的位置，来编辑 workers.properties 文件。端口和类型无需更改。

5. 在 IIS 上部署 ISAPI 筛选器。

6. 通过管理工具打开 Internet 信息服务管理器。

7. 展开层级，直至显示“默认网站”。右键单击，然后选择“新建”、“虚拟目录”。

8. 输入 *jakarta* 作为别名。

9. 引用您安装了 ISAPI 插件的路径。

10. 选择“读取”、“运行脚本”（如 ASP）以及“执行”（如 ISAPI 应用程序或 CGI）。

11. 单击“下一步”以继续并完成向导。

12. 右键单击“默认网站”，选择“属性”，然后选择“ISAPI 筛选器”选项卡，最后单击“添加”。

13. 输入 *jakarta* 作为筛选器名称，然后单击“浏览”以选择 isapi_redirect.dll。 单击“确定”两次。

14. 对于 IIS 6.0，在“Web 服务扩展”下启用此筛选器。

15. 选择“Web 服务扩展”文件夹。 单击左侧的蓝色链接以添加新的 Web 服务扩展。

16. 提供 Jakarta-Tomcat 作为名称。 单击“添加”，然后浏览查找上面的 dll。 单击“确定”，然后单击“设置扩展状态为允许”，再单击“确定”。

17. 重新启动 IIS 服务器。

启用了代理后，您现在可以通过 IIS 访问 CA Identity Manager。 例如，以下是在配置代理前后用于访问 CA Identity Manager 的链接：

之前

http://identitymgr.forwardinc.ca:8080/idmmange
http://identitymgr.forwardinc.ca:8080/idmmange

之后

http://smserver.forwardinc/idmmanage
http://smserver.forwardinc/idmmanage

注意：为了能使代理工作，您需要在 URL 的结尾添加斜杠“/”。 如果未能转到管理控制台，请查阅代理日志。

在 WebLogic 上安装代理插件

当 Web 代理对 CA Identity Manager 资源请求进行身份验证和授权时，Web 服务器将请求转发到托管 CA Identity Manager 服务器的应用程序服务器。

1. 按照 WebLogic 文档所述，为您的 Web 服务器安装 WebLogic 代理插件。

   注意：对于 IIS 用户，在安装代理插件时，一定要根据文件扩展名和路径来配置代理。 当您根据文件扩展名配置代理时，请在“应用程序映射”选项卡中，使用以下属性来添加应用程序映射：
   可执行文件：IISProxy.dll
   扩展名：.wlforward

2. 按照以下部分之一所述，为 CA Identity Manager 配置代理插件：
   - IIS 代理插件 (p. 267)
   - iPlanet 代理插件 (p. 269)
   - Apache 代理插件 (p. 271)

为 IIS (7.x) 配置代理插件

下列步骤阐述了如何为 IIS 7.x 部署和配置 WebLogic 代理插件。

注意：这些说明针对 32 位操作环境。同样也适用于 64 位操作环境。但是 .dll 文件的安装位置有所区别：

- %WL_HOME%server\plugin\win\32\
- %WL_HOME%server\plugin\win\64\

遵循这些步骤:

1. 在 IIS7 上安装并配置 Web 代理。
2. 在“C”驱动器中创建名为“plugin”的文件夹。

3. 将下列文件复制到该插件文件夹：
   - lisforward.dll
   - lisproxy.dll
   - iisproxy.ini

   您可以在 \\lodimmaple.ca.com\RegressionHarness\thirdparty\weblogic\Weblogic_Proxy_Files_IIS7 中找到这些文件。
4. 在 IIS7 上安装应用程序开发和管理工具角色服务。
5. 打开 Inet 管理器，然后选择“默认网站”。
6. 单击“处理程序映射”。
7. 双击“静态文件”并将“请求路径”修改为 *.*。
8. 单击“请求限制”按钮。
9. 在“映射”选项卡上，选择“仅当请求映射至以下内容时才调用处理程序”、“文件或文件夹”。
10. 在“处理程序映射”对话框中，单击右侧菜单选项上的“添加脚本映射...”。 输入以下值：
    - 请求路径： *
    - 可执行文件：iisProxy.dll
    - 名称：proxy
11. 单击“请求限制”按钮。
12. 清除“仅当请求映射至以下内容时才调用处理程序”。
13. 提示您确认是否允许此 ISAPI 扩展时，单击“是”。
14. 单击 IIS 管理器树的根节点（计算机名），然后单击“ISAPI 和 CGI 限制”。
15. 单击“操作”窗格中的“添加”，并输入下列值：
    - ISAPI 或 CGI 路径：C:\plugin\ iisproxy.dll。
    - 说明：Weblogic
    - 选择“允许执行扩展路径”。
16. 单击 IIS 管理器树的根节点（计算机名），然后单击“ISAPI 和 CGI 限制”。 选择“Weblogic”选项，然后单击右侧窗格上的“编辑功能设置”。
17. 选择“允许未指定的 ISAPI 模块”和“允许未指定的 CGI 模块”。
18. 对 Web 代理进行相同的操作。
19. 在“功能”视图中的“默认网站”上，双击“处理程序映射”。

20. 在“处理程序映射”页面的“操作”窗格上，单击“添加脚本映射”，然后输入下列值：
    - 请求路径：.jsp
    - 可执行文件：iisproxy.dll
    - 名称：JSP
21. 单击“请求限制”。
22. 在“映射”选项卡上，选择“仅当请求映射至文件时才调用处理程序”、“文件”。
23. 单击“确定”。
24. 单击“添加脚本映射”并输入下列值：
    - 请求路径：.do
    - 可执行文件：C:\plugin\iisproxy.dll
25. 单击“请求限制”。 该设置与 .jsp 的相同。
26. 单击“确定”。
27. 单击“添加脚本映射”并输入下列值：
    - 请求路径：.wlforward
    - 可执行文件：C:\plugin\iisproxy.dll
28. 单击“请求限制”。 该设置与 .jsp 的相同。
29. 单击“默认网站”，然后双击“ISAPI 筛选器”。
30. 单击右侧窗格上的“查看排序列表”。
31. 将 SiteMinder 代理可执行文件置于列表的第二位。 在列表中，此条目之后仅有 Weblogic 可执行文件。

    注意：如果 SiteMinder 代理可执行文件显示在 Weblogic 可执行文件之后，请使用“向上移动”操作来移动 SiteMinder 代理。
32. 单击“应用程序池”，并将“默认应用程序池”更改为“经典”模式。

WebLogic 插件配置完毕。

(WL) 配置 IIS 6.0 代理插件

以下步骤适用于对 IIS 6.0.x 进行 WebLogic 代理插件配置：

遵循这些步骤:

1. 在安装了 web 代理的系统上创建文件夹。 例如：c:\weblogic_proxy。
2. 登录到正在运行 CA Identity Manager 服务器的系统。
3. 转到此文件夹：*Weblogic_Home*\wlserver_11\server\plugin

4. 将下列文件复制到在第 1 步中创建的 weblogic 代理文件夹。
   - iisforward.dll
   - iisproxy.dll
5. 在同一文件夹中创建命名为 iisproxy.ini 的文件，并且添加以下内容：

   ```
   # This file contains initialization name/value pairs
   # for the IIS/WebLogic plug-in.
   WebLogicHost=host-name
   WebLogicPort=7001
   ConnectTimeoutSecs=20
   ConnectRetrySecs=2
   WlForwardPath=/castylesr5.1.1,/iam,/im , /ca/Odata/
   WLLogFile= c:\weblogic_proxy \proxy.log
   DebugConfigInfo=ON
   ```

   将 *host-name* 替换为实际的主机名。
6. 启动 IIS 管理器。
7. 展开“网站”。
8. 右键单击“默认网站”。
9. 选择“属性”。
10. 添加筛选器，方法如下：
    a. 单击“ISAPI 筛选器”。
    b. 单击“添加”，在对话框中输入以下值：

       筛选器名称：WebLogic

       可执行文件：iisforward.dll 的路径
11. 提供 iisproxy.dll 文件的位置，方法如下：
    a. 单击“主目录”。
    b. 单击“配置”。
    c. 单击“添加”。
    d. 输入 iisproxy.dll 文件的路径。
    e. 在“扩展名”字段中输入 .jsp。
    f. 清除“确认文件存在”选项。
12. 对 .do 和 .wlforward 扩展名重复第 11 步。
13. 添加指向 iisforward.dll 的位置的 wlforward（均为小写）Web 服务扩展。

    将扩展状态设置为“允许”。
14. 右键单击每个 Web 服务扩展以将其更改为允许状态。
15. 重新启动 IIS Web 服务器。

配置 iPlanet 代理插件

要配置此插件，请修改下列 iPlanet 配置文件：

- magnus.conf
- obj.conf

iPlanet 配置文件对文本位置有严格规则。 要避免这些问题，请注意以下几点：

- 消除额外的前导和尾空格。 额外的空格会导致 iPlanet 服务器启动失败。
- 如果您需要输入超过一行所能显示的字符，请在该行末尾添加反斜线 (\)，然后在下一行中继续输入。反斜线直接将第一行末尾附加到下一行开头。如果处于第一行末尾和第二行开头的单词之间需要有空格，请务必将空格置于第一行末尾（斜杠前）或第二行开头。
- 切勿将属性拆分为多行。

可在下列位置找到 iPlanet 实例的 iPlanet 配置文件：

iplanet_home/https-*instance_name*/config/

其中，*iplanet_home* 是 iPlanet 安装的根目录，而 *instance_name* 则是特定服务器的配置。

遵循这些步骤:

1. 从 *weblogic_home*/server/lib 目录中，将与您的 iPlanet Web 服务器版本对应的 libproxy.so 文件复制到安装了 iPlanet 的文件系统。
2. 在文本编辑器中，修改 iPlanet magnus.conf 文件。

   若要让 iPlanet 将 libproxy.so 文件作为 iPlanet 模块加载，请将下列行添加到 magnus.conf 文件的开头：

   ```
   Init fn="load-modules" funcs="wl_proxy,wl_init"\
   shlib=path in file system from step 1/libproxy.so
   Init fn="wl_init"
   ```

   例如：

   ```
   Init fn="load-modules" funcs="wl_proxy,wl_init"\
   shlib=/usr/local/netscape/plugins/libproxy.so
   Init fn="wl_init"
   ```

   函数 load-modules 将共享库标记为在 iPlanet 启动时加载。 值 wl_proxy 和 wl_init 指定插件所要执行的函数。

3. 在文本编辑器中，按照如下方法修改 iPlanet obj.conf 文件：

   a. 在以下列文本开始的最后一行后：

      NameTrans fn=....

      将下列 Service 指令添加到“Object name="default"”部分：

      ```
      Service method="(GET|HEAD|POST|PUT)" type=text/jsp fn="wl-proxy"
      ```

      注意：您可以在现有的 Service 指令的下一行中添加此指令。

   b. 将以下代码添加到文件末端：

      ```
      <Object name="idm" ppath="*/iam/*">">
      Service fn="wl-proxy" WebLogicHost="hostname" WebLogicPort="portnumber"
      PathTrim="/weblogic"
      </Object>
      <Object name="weblogic1" ppath="*/console*">
      Service fn="wl-proxy" WebLogicHost="hostname" WebLogicPort="portnumber"
      PathTrim="/weblogic"
      </Object>
      ```

      其中，*hostname* 是安装了 WebLogic 的系统的服务器名和域，*portnumber* 则是 WebLogic 端口（默认为 7001）。

      您可能拥有多个对象条目。

      例如：

      ```
      <Object name="idm" ppath="*/iam/*">">
      Service fn="wl-proxy" WebLogicHost="MyServer.MyCompany.com"
      WebLogicPort="7001" PathTrim="/weblogic"
      <Object name="weblogic1" ppath="*/console*">
      Service fn="wl-proxy" WebLogicHost="MyServer.MyCompany.com"
      WebLogicPort="7001" PathTrim="/weblogic"
      </Object>
      ```

4. 保存 iPlanet 配置文件。

5. 重新启动 Web 服务器实例。

IM_12.8--配置 Apache 代理插件

配置 Apache 代理插件需要编辑 http.conf 文件。

遵循这些步骤:

1. 在 Solaris 上安装了 Web 代理之后，停止 Apache Web 服务器，然后将 mod_wl_20.so 文件从以下位置：

   weblogic_home/server/lib/solaris

   复制到

   apache_home/modules

2. 编辑 http.conf 文件（位于 *apache_home*/conf）并且进行以下更改：

   a. 在“加载模块”部分下，添加以下代码：

   ```
   LoadModule weblogic_module     modules/mod_wl_20.so
   ```

   b. 用 Apache 服务器系统的名称来编辑服务器名称。

   c. 在文件结尾添加一个 If 块，如下所示：

   ```
   <IfModule mod_weblogic.c>
     WebLogicHost weblogic_server.com
     WebLogicPort 7001
     MatchExpression /iam
     MatchExpression /castylesr5.1.1
     MatchExpression /ca/Odata
   </IfModule>
   ```

3. 保存 http.conf 文件。
4. 重新启动 Apache Web 服务器。

将 SiteMinder 代理与 CA Identity Manager 域关联

策略管理员在完成 CA Identity Manager 任务之后执行此任务。 当您将环境加载到 CA Identity Manager 时，请引用 4.X 代理。 当在 SiteMinder 策略服务器上创建域/领域时，SiteMinder 使用该代理。 此代理验证 SMSESSION cookie。 更新域/领域，然后引用用于访问 CA Identity Manager 的 Web 服务器上的全功能代理。 此 Web 服务器充当 CA Identity Manager 的访问点，并创建 SMSESSION cookie。

遵循这些步骤:

1. 登录到 SiteMinder 管理 UI。
2. 导航到“策略”、“域”。
3. 修改环境的域。
4. 在“领域”选项卡上，编辑第一个列出的域：XXX_ims_realm。
5. 搜索并选择代理服务器上的代理。

   注意：如果您没有代理服务器代理（Web 服务器代理），请创建一个。 确认您拥有一个针对 CA Identity Manager 的 Web 服务器和代理服务器。

6. 两次单击“确定”，然后对公共的领域 XXX_pub_realm 重复此流程。
7. 在更新这两个域之后，单击“提交”。
8. 等待代理刷新，或重新启动代理服务器代理所在的 Web 服务器。

配置 SiteMinder LogOffUrI 参数

将 SiteMinder 添加到环境后，在 CA Identity Manager 中注销不会进行任何操作。要重新启用此功能，请在代理服务器上更新代理的代理配置对象 (ACO)。

遵循这些步骤:

1. 登录到 SiteMinder 管理 UI。 依次单击“基础架构”选项卡、“代理”、“扩展代理配置”，然后单击“修改代理配置”。
2. 找到您的 ACO。查找参数 #LogoffUri。单击该参数左边的播放按钮（指向右边的箭头）。
3. 从“值”字段的名称中删除磅字符 (#)，然后输入 /idm/logout.jsp。
4. 单击“确定”，然后单击“提交”以更新代理配置对象。

   在下次代理从策略服务器获取其配置时，传播新的设置。

疑难解答

下列主题说明您可能会遇到的常见错误。 在所有可能的地方都会提供错误以及相应的解决方案，以便为您在集成过程中提供帮助。

丢失 Windows DLL

症状：

丢失 Windows DLL (MSVCP71.dll)

据我们所观察，在启用 SiteMinder 连接之后，JBoss 会抛出丢失 DLL (MSVCP71.dll) 的 Java 错误。

注意：如果 JBoss 作为服务运行时，可能不出现此错误。 如果可以的话，在不将 JBoss 作为服务运行的情况下测试您的配置。

解决方案：

遵循这些步骤:

1. 如果 SiteMinder 策略服务器运行在 Windows 上，在该策略服务器上找到 MSVCP71.dll。
2. 将此 DLL (MSVCP71.dll) 复制到 \Windows\system32 文件夹。
3. 在您将此文件放置在正确的位置后，通过操作系统来注册该文件。
4. 从命令窗口中运行 regsvr32 命令。 只要加载了此文件，就应该能够排除此故障。
5. 重新启动应用程序服务器。

不正确的 SiteMinder 策略服务器位置

症状：

不正确的 SiteMinder 策略服务器位置。

解决方案：

ra.xml 中引用不正确的位置时，会出现“Cannot connect to policy server: xxx”错误。

遵循这些步骤:

1. 检查 ra.xml 中所提供的主机名。

```
</config-property>
<config-property>
    <config-property-name>ConnectionURL</config-property-name>
    <config-property-type>java.lang.String</config-property-type>
    <config-property-value>smserver.forwardinc.ca,44441,44442,44443</config-property-value>
</config-property>
<config-property>
    <config-property-name>UserName</config-property-name>
```

2. 在 ConnectionURL 属性中指定 SiteMinder 策略服务器的主机名。 使用 FQN（完全限定的名称）。

不正确的管理员名称

症状：

不正确的管理员名称

解决方案：

ra.xml 中引用不正确的管理员时，此时显示错误“未知管理员”。

遵循这些步骤:

1. 检查 ra.xml 中的 UserName 属性。

```
    <config-property-value>smserver.forwardinc.ca,44441,44442,44443</co
</config-property>
<config-property>
    <config-property-name>UserName</config-property-name>
    <config-property-type>java.lang.String</config-property-type>
    <config-property-value>SiteMinder</config-property-value>
</config-property>
<!--The property 'password' has been removed.  'AdminSecret' is used in
This is due to the fact that we have added algorithm name padding in th
the algorithm name (for ex, PBES) with its own handlers.  This crashes
```

2. 在 UserName 属性中，指定用于与 CA SiteMinder 通讯的帐户。 例如，使用 SiteMinder 帐户（默认值）。

不正确的管理密钥

症状：

不正确的管理密钥

解决方案：

ra.xml 中使用了不正确的管理密钥时，会出现“Cannot connect to the policy server: Invalid credentials”错误。

遵循这些步骤:

1. 检查 ra.xml 中的 AdminSecret 属性。

```
-->
<config-property>
    <config-property-name>AdminSecret</config-property-name>
    <config-property-type>java.lang.String</config-property-type>
    <config-property-value>{PBES}:xfx8/9xxmHD0B3Raw9VZJA==</config-property-value>
</config-property>
<config-property>
    <config-property-name>AgentName</config-property-name>
```

2. 在 AdminSecret 属性中，为 UserName 属性中引用的用户名指定加密密码。

更多信息：

修改 SiteMinder 密码或共享密钥 (p. 299)

不正确的代理名称

症状：

不正确的代理名称

解决方案：

ra.xml 中使用了不正确的代理名称时，会出现“Cannot connect to the policy server: Failed to init Agent API: -1”错误。

遵循这些步骤：

1. 检查 ra.xml 中的 AgentName 属性。

```
</config-property>
<config-property>
    <config-property-name>AgentName</config-property-name>
    <config-property-type>java.lang.String</config-property-type>
    <config-property-value>idmagent</config-property-value>
</config-property>
<config-property>
```

2. 指定您在 SiteMinder 配置期间的第 3 步中所创建的 4.X 代理名称。

不正确的代理密钥

症状：

不正确的代理密钥

解决方案：

ra.xml 中使用了不正确的代理密钥时，会出现“Cannot connect to the policy server: Failed to init Agent API: -1”错误，同时在前面出现加密处理程序错误。

遵循这些步骤：

1. 检查 ra.xml 中的 AgentSecret 属性。

```
<config-property>
    <config-property-name>AgentSecret</config-property-name>
    <config-property-type>java.lang.String</config-property-type>
    <config-property-value>{PBES}:xfx8/9xxmHD0B3Raw9VZJA==</config-property-value>
</config-property>
<config-property>
```

2. 指定在创建此代理时所使用的加密密码。

更多信息：

修改 SiteMinder 密码或共享密钥 (p. 299)

CA Identity Manager 中无用户上下文

症状：

CA Identity Manager 中无用户上下文。

用户尝试在不使用 SMSESSION cookie 的情况下访问 CA Identity Manager 时，CA Identity Manager 无法验证此用户。在此情况下，您可能会看到空白的 CA Identity Manager 用户界面。

如果您已为环境启用了工作流，则可能会看到如下所示的故障。

```
Exception during page display:

java.lang.IllegalArgumentException
        at com.netegrity.webapp.bean.WorkList.(WorkList.java:84)
        at com.netegrity.webapp.bean.WorkList.(WorkList.java:70)
        at com.netegrity.webapp.bean.WorkList.getConsoleWorkListFromRequest(WorkList.java:109)
        at com.netegrity.taglib.skin.TagUtilLocal.getWorkItems(TagUtilLocal.java:660)
        at com.netegrity.taglib.skin.TagUtilLocal.hasWorkItems(TagUtilLocal.java:846)
        at com.netegrity.taglib.skin.IfWorkItemsTag.doStartTag(IfWorkItemsTag.java:73)
        at idm_jsp.app.ca12.home_jsp._jspService(Unknown Source)
        at org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:70)
        at javax.servlet.http.HttpServlet.service(HttpServlet.java:803)
        at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:290)
        at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:206)
        at org.apache.catalina.core.ApplicationDispatcher.invoke(ApplicationDispatcher.java:654)
        at org.apache.catalina.core.ApplicationDispatcher.doInclude(ApplicationDispatcher.java:557)
        at org.apache.catalina.core.ApplicationDispatcher.include(ApplicationDispatcher.java:481)
        at org.apache.jasper.runtime.JspRuntimeLibrary.include(JspRuntimeLibrary.java:968)
        at idm_jsp.app.ca12.index_jsp._jspx_meth_skin_ifhomepage_0(Unknown Source)
        at idm_jsp.app.ca12.index_jsp._jspService(Unknown Source)
        at org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:70)
        at javax.servlet.http.HttpServlet.service(HttpServlet.java:803)
        at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:290)
        at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:206)
        at org.apache.catalina.core.ApplicationDispatcher.invoke(ApplicationDispatcher.java:654)
        at org.apache.catalina.core.ApplicationDispatcher.processRequest(ApplicationDispatcher.java:445)
        at org.apache.catalina.core.ApplicationDispatcher.doForward(ApplicationDispatcher.java:379)
        at org.apache.catalina.core.ApplicationDispatcher.forward(ApplicationDispatcher.java:292)
        at com.netegrity.webapp.filter.ConsolePageFilter.doFilter(ConsolePageFilter.java:521)
        at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:235)
        at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:206)
        at com.netegrity.webapp.page.jsf.FacesFilter.doFilter2(FacesFilter.java:180)
```

解决方案：

若干因素会导致此问题，但通常会是以下之一：

- 您直接访问 CA Identity Manager。
- 代理服务器的 SiteMinder 代理被禁用（也就是说，没有保护任何内容－没有在创建 SMSESSION Cookie）。
- CA Identity Manager 环境的 SiteMinder 域配置错误。

前两种原因是显而易见的。确保您在已启用完全功能的 Web 代理的情况下路由到 Web 服务器。 但是，如果直接访问 Web 服务器并且已启用了代理，那么您就需要修改域。

遵循这些步骤:

1. 登录到 SiteMinder 管理 UI。
2. 找到 CA Identity Manager 域，然后单击逐个层以进行修改。单击“领域”选项卡，然后单击列表中的第一个领域。
3. 正斜杠的默认位置为该领域的下方。 将其删除。
4. 单击此领域下方的“规则”。

   此规则的默认有效资源是星号“*”。
5. 在星号的前面添加正斜杠“/”。

   您已将正斜杠从领域移到此规则。 保护是相同的，但是 SiteMinder 以不同的方式进行处理。

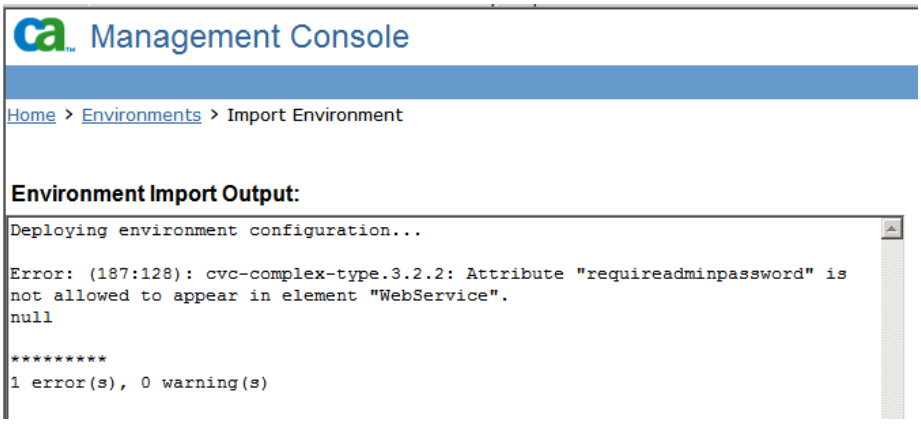
   您可以通过 SiteMinder 成功登录到 CA Identity Manager。 要验证适当的保护，请查阅 SiteMinder 代理日志。

加载环境时的错误

症状：

完成与 SiteMinder 的集成后，当将环境导回到 CA Identity Manager 时，可能会出现有关“requireadminpassword”属性和“WebService”元素的错误。

注意：当 SiteMinder 不属于部署的一部分时，也可能产生此问题。



解决方案：

此错误允许部分部署环境。 部分部署会在 CA Identity Manager 对象存储中创建空元素。 更正环境 XML 之一并重新导入。

遵循这些步骤:

1. 找到并浏览存档的 ZIP 文件。
2. 创建一个 XXX_environment_settings.xml 的副本。
3. 编辑该文件，然后找到“WebService”元素。
4. 删除标记“requireadminpassword=false”。

   注意：请同时删除标记*和*值。 而不是仅删除值。
5. 保存所作的更改，然后将文件放回到 ZIP 文件。
6. 重新导入此已归档的环境 zip 文件。

   您不必删除在失败的尝试时创建的环境。 重新导入校正后的文件可以修复上次失败尝试中出现的错误。

无法创建 CA Identity Manager 目录或环境

症状：

启用 SiteMinder 集成后，无法创建 CA Identity Manager 目录或环境。

解决方案：

此问题可能是由于注册表中丢失条目造成的。

确认 SiteMinder 策略服务器计算机上存在以下注册表设置：

- Solaris 或 Linux：

  确认 sm.registry 中存在以下条目：
  ImsInstalled=8.0; REG_SZ

- Windows：

  确认以下位置存在设置“ImsInstalled=8.0 REG_SZ”：
  HKLM\SOFTWARE\Netegrity\SiteMinder\CurrentVersion

  注意：如果不存在注册表路径 \Netegrity\SiteMinder\CurrentVersion，请手动创建此路径。

如果您更改了注册表，请务必重新启动策略服务器，以使所作的更改生效。

重要说明！ 在修改注册表之前，请创建一份完整的系统备份。

用户无法登录

症状：

新用户无法使用明文密码登录到环境。

解决方案：

确保目录配置文件 (directory.xml) 中的密码属性定义不包含以下数据分类：

<DataClassification name="AttributeLevelEncrypt"/>

在包括以下组件的环境中，启用属性级别加密可阻止用户登录：

- CA SiteMinder 以及
- 关系数据库

如何配置 CA Identity Manager 代理设置

当 CA Identity Manager 与 SiteMinder 集成时，CA Identity Manager 使用内置的 CA Identity Manager 代理来与 SiteMinder 策略服务器进行通信。 要调整性能，请为 CA Identity Manager 代理配置下列连接设置。

1. 完成以下步骤之一：
   - 如果 CA Identity Manager 正运行在 WebLogic 或 WebSphere 应用程序服务器上，在应用程序服务器的控制台中，编辑连接器描述符 policyserver_rar 中的资源适配器。
   - 如果 CA Identity Manager 正运行在 JBoss 应用程序服务器上，打开 <JBoss_home>\server\default\deploy\iam_im.ear\policyserver_rar\META-INF 中的 olicyserver-service.xml。
2. 将设置配置为：

   ConnectionMax

   设置连接到策略服务器的最大连接数，例如：20。

   ConnectionMin

   设置连接到策略服务器的最小连接数，例如：2。

   ConnectionStep

   设置当所有的代理连接都已使用时允许打开的额外连接数。

   ConnectionTimeout

   指定代理在超时前，需要等待以连接到 SiteMinder 的时间总量（单位为秒）。
3. 重新启动应用程序服务器。

配置 SiteMinder 高可用性

如果已经创建了 SiteMinder 策略服务器群集，您可以配置应用程序服务器群集，以将其用于负载平衡和故障切换。

遵循这些步骤:

1. 编辑下列位置中的 ra.xml 文件：
   WebSphere：
   WAS_PROFILE/config/cells/*CELL_NAME*/applications/iam_im.ear/deployments/IdentityMinder/policyserver_rar/META-INF
   Jboss：*jboss_home*/server/all/deploy/iam_im.ear/policyserver_rar/META-INF
   WebLogic：*wl_domain*/applications/iam_im.ear/policyserver_rar/META-INF
2. 修改以下项（具体说明见下一节）：
   - 策略服务器的连接设置
   - 策略服务器的数目
   - 群集的负载平衡或故障切换的选择。
3. 对群集中的每个 CA Identity Manager 服务器重复这些步骤。
4. 重新启动应用程序服务器，使更改生效。

注意：当您正在创建 CA Identity Manager 目录或环境，或者修改目录或环境设置时，请将 SiteMinder 故障切换和 FailoverServers 设为 false。 否则，目录对象可以被创建但是不能及时复制以供使用。 例如，在服务器 1 中创建一个目录。 然后，在服务器 2 上，使用该目录的对象 ID 创建属性，但此时尚不存在第二个目录。 您会接收到一个“未找到对象”的错误。

修改策略服务器连接设置

策略服务器连接信息必须反映生产环境中的主服务器。 此信息包括 ConnectionURL、SiteMinder 管理员帐户的用户名和密码、代理的名称和共享密钥。

下例中，可编辑的值将以大写字母显示。

```
<config-property>
        <config-property-name>ConnectionURL</config-property-name>
   <config-property-type>java.lang.String</config-property-type>
        <config-property-value>DEVELOPMENT.SEVERCOMPANY.COM,VALUE,VALUE,VALUE
</config-
                property-value>
</config-property>

<config-property>
        <config-property-name>UserName</config-property-name>
   <config-property-type>java.lang.String</config-property-type>
        <config-property-value>SITEMINDER-ADMIN-NAME</config-property-
value>
</config-property>
```

```
<config-property>
        <config-property-name>AdminSecret</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>ENCRYPTED-PASSWORD</config-
                property-value>
</config-property>
<config-property>
        <config-property-name>AgentName</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>DEVELOPMENT-AGENT-NAME</config-property-
                value>
</config-property>

<config-property>
        <config-property-name>AgentSecret</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>ENCRYPTED-AGENT-SECRET</config-
                property-value>
</config-property>
```

注意：请使用 CA Identity Manager 密码工具来加密要求加密文本的值。 有关详细信息，请参阅*《配置指南》*。

添加其他策略服务器

要将其他策略服务器添加到 CA Identity Manager 安装实例中，请编辑 ra.xml 文件中的 **FailoverServers** 条目。

注意：请在 FailoverServers 条目中加入主策略服务器和所有的故障切换服务器。

为各个策略服务器输入 IP 地址以及身份验证、授权和核算服务的端口号。 使用分号来分隔各个条目，如下所示：

```
<config-property>
        <config-property-name>FailoverServers</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>
                172.123.123.123,44441,44442,44443;172.123.123.124,33331,
                33332,33333
        </config-property-value>
</config-property>
```

选择负载平衡或故障切换

CA Identity Manager 默认使用轮循负载平衡（使用 ConnectionURL 和 FailoverServers 标识的服务器）。 如果将 FailOver 设置保持为 false 会启用负载平衡。

要选择故障切换，请将 FailOver 设为 true：

```
<config-property>
        <config-property-name>FailOver</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>true</config-property-value>
</config-property>
```

从现有的 CA Identity Manager 部署中删除 SiteMinder

本部分详细说明了如何从现有的 CA Identity Manager 环境中删除 CA SiteMinder。

遵循这些步骤:

重要说明！ 密码历史信息在迁移之后将不可访问。

1. 停止应用程序服务器。
2. 将“已启用的配置属性”的值设为 false，在 ra.xml 文件（位于 \iam_im.ear\policyserver.rar\META-INF）中禁用策略服务器。
3. 编辑 \iam_im.ear\User_console.war\WEB-INF 中的 web.xml 文件，并将 FrameworkAuthFilter 属性设为“Enabled = true”。

   注意：WebSphere 的 web.xml 文件位于 *WebSphere_home*/AppServer/profiles/*Profile_name*/config/cells/*Cell_name*/applications/iam_im.ear/deployments/IdentityMinder/user_console.war/WEB-INF。
4. 启动应用程序服务器。
5. （仅针对 WebSphere）在管理控制台中，使用与 ra.xml 文件中相同的值来更新 policyServer 对象。

SiteMinder 操作

以下部分将讨论如何修改 SiteMinder 功能（包括策略域和身份验证方案）以支持 CA Identity Manager：

使用自定义身份验证方案来收集用户凭证

SiteMinder 使用身份验证方案来收集用户凭证，并在用户登录时确认其身份。验证用户身份后，CA Identity Manager 将根据用户权限生成个性化的用户控制台。

您可以实施任何 SiteMinder 身份验证方案以保护 CA Identity Manager 环境。

例如，您可以实施 HTML 表单身份验证方案，以便在 HTML 表单中收集凭据。通过使用 HTML 表单，您可以创建可以包括品牌宣传元素（如公司徽标）以及到“自行注册”和“忘记密码”页面链接的登录页面。

注意：有关身份验证方案的信息，请参阅《*CA SiteMinder Policy Server Configuration Guide*》。

遵循这些步骤:

1. 登录到下列界面之一：
   - 对于 CA SiteMinder Web 访问管理器 r12 或更高版本，登录到管理 UI。
   - 对于 CA eTrust SiteMinder 6.0 SP5，登录到策略服务器用户界面。

   注意：有关使用这些界面的信息，请参阅与您当前使用的 SiteMinder 版本对应的文档。
2. 按照《*CA SiteMinder Policy Server Configuration Guide*》中所述，创建一个身份验证方案。
3. 修改保护相应 CA Identity Manager 环境的领域，以使用您在步骤 1 中创建的身份验证方案。

   领域名称具有以下格式：

   *Identity Manager-environment*_ims_realm

   注意：如果您为公开的任务配置了支持，您可以看见一个额外的领域 *Identity Manager-environment*_pub_realm。 此领域使用匿名身份验证方案，以允许未知的用户在没有提供凭据的情况下，使用自行注册和忘记密码功能。 请不要修改这些领域的身份验证方案。

将数据定义导入到策略存储

您可以使用 SiteMinder 策略来控制用户对应用程序功能的访问。 策略服务器安装包含必要的数据定义以允许此控制。 您可以从以下位置导入 IdmSmObjects.xdd 文件：

siteminder_home\xps\dd

siteminder_home 是策略服务器的安装路径。

计划访问角色

要控制对应用程序的访问，您需要创建访问角色和任务。 访问任务提供对应用程序功能的访问。 访问角色包含一个或多个应用程序的一个或多个访问任务。为用户分配访问角色后，用户便可以使用该角色包含的功能。

“应用程序访问的访问角色”包含有关访问角色用途的详细信息。

访问角色需要在 Identity Manager 和 SiteMinder 中配置。 涉及到两种管理员：

- Identity Manager 管理员：必须能在 Identity Manager 中创建访问角色和任务。 默认的系统管理员和访问角色管理器角色包括这些任务。
- SiteMinder 管理员：必须拥有系统作用域权限，并且能管理系统和域对象。 有关详细信息，请参阅*“CA eTrust SiteMinder 策略设计”*。

注意：策略设计用户界面中的术语*“Identity Manager 环境”*即当前所述的 *Identity Manager 环境*。 此外，随此产品提供的 SiteMinder 文档使用*“Identity Manager”*表示它。 自 r8.1 起，新的产品命名为*“Identity Manager”*。

下列流程描述了创建访问角色的步骤：

1. 具有“访问角色管理员”角色的 Identity Manager 管理员：
   a. 创建访问任务。
   b. 创建访问角色。
   c. 将角色和任务信息传递给 SiteMinder 管理员。
2. SiteMinder 管理员通过以下步骤创建基于角色的访问控制策略：
   a. 将与一个或多个 Identity Manager 环境关联的用户目录分配给策略域。
   b. 将一个或多个 Identity Manager 环境与步骤 1 中的策略域关联。
   c. 在策略域中创建领域和规则（如果它们尚未存在）。 领域和规则应对应于访问角色将为其授予访问权限的资源。
   d. 创建策略并将其绑定到 Identity Manager 环境中的角色。
   e. （可选）指定将授权信息发送给受保护资源的响应。

   有关之前步骤的说明，请参阅*“CA eTrust SiteMinder 策略设计”*。

启用用于 SiteMinder 的访问角色

为了将访问角色用于 CA SiteMinder，CA CA Identity Manager 为 CA Identity Manager 对象存储中所有与 SiteMinder 策略存储中的访问角色相关的对象制作镜像。 要启用此功能，您需要在 CA Identity Manager 管理控制台中配置属性。

启用用于 SiteMinder 的访问角色

1. 打开管理控制台。
2. 依次选择“Environment”（环境）、*“您的环境”*、“Advanced Settings”（高级设置）和“Miscellaneous”（杂项）。
3. 通过提供以下信息来添加新的属性：
   - 在“Property”（属性）字段中，输入以下内容：

     EnableSMRBAC
   - 在“Value”（值）字段中，输入以下内容：

     true

4. 单击“Add”（添加）。 然后，单击“Save”（保存）。

   此时显示表示环境需要重新启动的消息。

5. 单击“Restart Environment”（重新启动环境）。

   CA CA Identity Manager 现在支持与 CA SiteMinder 结合使用的访问角色和任务。

一旦您启用了与 CA SiteMinder 结合使用的访问角色后，请注意：

- 如果在 CA Identity Manager r8x 中使用访问角色，您需要执行额外的迁移步骤，以便能管理 CA CA Identity Manager 当前版本中的访问角色。 有关详细信息，请参阅 *《升级指南》*。
- 要在 SiteMinder 中禁用对访问角色的支持，请从 SiteMinder 策略存储中删除 CA Identity Manager 访问角色和任务对象。 然后，从“Miscellaneous Properties”（杂项属性）列表中删除“EnableSMRBAC”属性并重新启动环境。

将访问任务添加到管理角色

默认情况下，“角色和任务”选项卡中不会显示访问任务，您需要将访问任务添加到已登录的用户的管理角色中。

遵循这些步骤:

1. 使用包含创建访问角色任务的角色登录到 CA Identity Manager 帐户。
2. 依次单击“角色和任务”、“修改管理角色”。
3. 选择已登录的用户的管理角色。
4. 单击“任务”选项卡、“按类别筛选”字段，从下拉列表中选择“角色和任务”。
5. 从“添加任务”下拉列表中选择“创建访问任务”。
6. 单击“提交”。

创建访问任务

访问任务是用户能够在业务应用程序中执行的单项操作，如在财务应用程序中生成采购订单。 为用户分配了包含访问任务的访问角色后，用户便可以执行该操作。

重要说明！ 要创建访问任务，您需要为已登录的用户的管理角色添加访问任务 (p. 287)。

遵循这些步骤:

1. 依次选择“角色和任务”、“访问任务”、“创建访问任务”。
2. 选择下列选项之一：
   - 创建访问任务
   - 创建访问任务副本。

3. 完成以下字段：

   名称

   您可以分配给任务的唯一名称，如 Generate Purchase Order。

   标记

   任务的唯一标记。该标记必须以字母或下划线开头，并且仅包含字母、数字或下划线。

   说明

   关于任务用途的可选说明。

   应用程序 ID

   与任务关联的应用程序的标识符（如应用程序名称）。应用程序 ID 不能包含任何空格或非字母数字字符。

   记下此 ID，在 SiteMinder 中启用该角色时需要此 ID。

4. 要完成此访问任务，请单击“提交”。

如何创建访问角色

访问角色包含对应用程序中的功能提供访问的访问任务。例如，角色可能包含以下任务：允许角色成员在采购应用程序中添加订单，以及在库存控制应用程序中更新数量。

您需要完成以下步骤以创建访问角色：

1. 开始创建访问角色。 (p. 288)
2. 在“配置文件”选项卡中定义访问角色的基本属性。 (p. 289)
3. 选择角色的访问任务。 (p. 289)
4. 定义角色的成员策略。 (p. 290)
5. 定义角色的管理策略。 (p. 290)
6. 定义角色的所有者规则。 (p. 291)

开始创建访问角色

1. 以承担创建访问角色任务的角色，登录到 Identity Manager 帐户。
2. 依次单击“访问角色”->“创建访问角色”。

   选择可创建新角色或角色副本的选项。如果选择“复制”，将搜索角色。
3. 继续执行下一部分“定义访问角色的配置文件”。

定义访问角色的配置文件

定义访问角色的配置文件

1. 输入名称、说明并完成为角色定义的所有自定义属性。

   注意：可以在“配置文件”选项卡指定自定义属性，以便用于指定访问角色的有关附加信息。 可以使用这些附加信息帮助在含有很多角色的环境中进行角色搜索。

2. 如果想要在创建角色之后即使其可用，请选择“已启用”。
3. 继续执行下一部分“为访问角色定义成员策略”。

选择角色的访问任务

在“任务”选项卡上完成以下步骤：

1. 选择包含在此角色中的任务。 依次选择应用程序、任务。 您可以加入其他应用程序中的任务。

   注意：如果其他角色存在您需要的任务，请单击“从其他角色复制任务”。 您可以编辑此时显示的列表。

   在创建角色或任务的过程中，您可以看到添加、编辑和删除项的图标，如下：

   前进或选择当前项目进行查看或编辑。

   如果禁用了 JavaScript，请单击前进按钮以从下拉列表中选择。

   后退或撤消之前的选择。

   插入一个元素，例如任务或规则。

   删除当前任务，或规则中的表达式。

   在列表中将当前项目向上移动。

   在列表中将当前项目向下移动。

2. 继续完成下一小节，“为访问角色定义管理策略”。

为访问角色定义成员策略

成员策略定义了角色的成员规则和作用域规则。 您可以为一个角色定义多个成员策略。 对于每个策略，符合成员规则中的条件的用户拥有使用策略中定义的角色的作用域。

遵循这些步骤:

1. 选择“成员”选项卡。
2. 单击“添加”以定义成员策略。
3. （可选）在“成员策略”页面上，根据需要为必须能使用此角色的用户定义成员规则。

   定义成员规则自动地将角色分配给在成员策略中满足条件的用户。

   注意：定义仅使用目录属性的成员策略，例如：title=Manager。 如果您定义的成员策略引用了没有存储在用户目录中的对象（如管理角色），SiteMinder 无法解析此引用。
4. 验证“成员”选项卡上显示的成员策略。

   要编辑策略，请单击左侧的箭头符号。 要删除策略，请单击减号图标。
5. 在“成员”选项卡上，启用“管理员可以添加和删除该角色的成员”复选框。

   启用此功能后，定义“添加操作”和“删除操作”。 这些操作将定义添加或删除角色成员用户时会出现的情况。

为访问角色定义管理策略

管理策略为角色定义管理规则、作用域规则和管理员权限。 您可以为角色定义几个管理策略。 每个策略表示如果管理员满足该管理规则的条件，就具备为策略定义的作用域和管理员权限。

遵循这些步骤:

1. 选择访问角色的“管理员”选项卡。
2. 如果您想使“管理管理员”选项可用，启用“管理员可以添加和删除该角色的管理员”复选框。

   启用此功能后，定义添加或删除角色管理员用户时所执行的操作。
3. 在“管理员”选项卡上添加管理策略，这些策略包含管理员规则、作用域规则和管理员权限。 每个策略需要至少一个权限（管理成员或管理管理员）。

   您可以为满足此规则的管理员添加多个具有不同规则和不同权限的管理策略。

   注意：定义仅使用目录属性的管理策略，例如：title=Manager。 如果您定义的成员策略引用没有存储在用户目录中的对象（如管理角色），SiteMinder 无法解析此引用。
4. 要编辑策略，请单击左侧的箭头符号。 要删除策略，请单击减号图标。
5. 继续执行下一部分，“为访问角色定义所有者规则”。

为访问角色定义所有者规则

所有者规则定义可以修改角色的用户。您可以为一个角色定义几个所有者规则。

遵循这些步骤:

1. 选择访问角色的“所有者”选项卡。
2. 定义所有者规则，此规则确定哪些用户可以修改此角色。

   注意：定义仅仅使用目录属性的所有者规则，例如：title=Manager。如果您定义的所有者规则引用没有存储在用户目录中的对象（如管理角色），SiteMinder 无法解析此引用。
3. 单击“提交”。

   将显示一条消息，表示该任务已提交。 在用户可以使用角色之前，可能会出现短暂的延迟。

在 SiteMinder 中启用访问角色

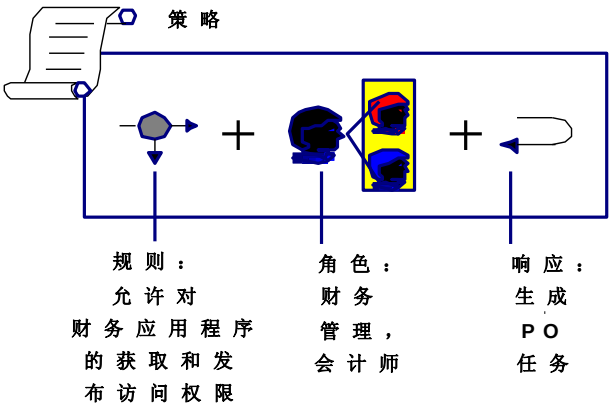
SiteMinder 管理员将角色绑定到定义用户如何与资源交互的安全策略。 策略可能与以下对象链接：

- 用户和用户组－标识受策略影响的一组用户。
- 角色－标识已经在 Identity Manager 中为其分配一组权限的用户。
- 规则－标识资源以及允许使用或拒绝使用该资源的操作。 资源通常是 URL、应用程序或脚本。
- 响应－确定对规则的反应。 在规则触发后，会将响应返回 SiteMinder 代理。

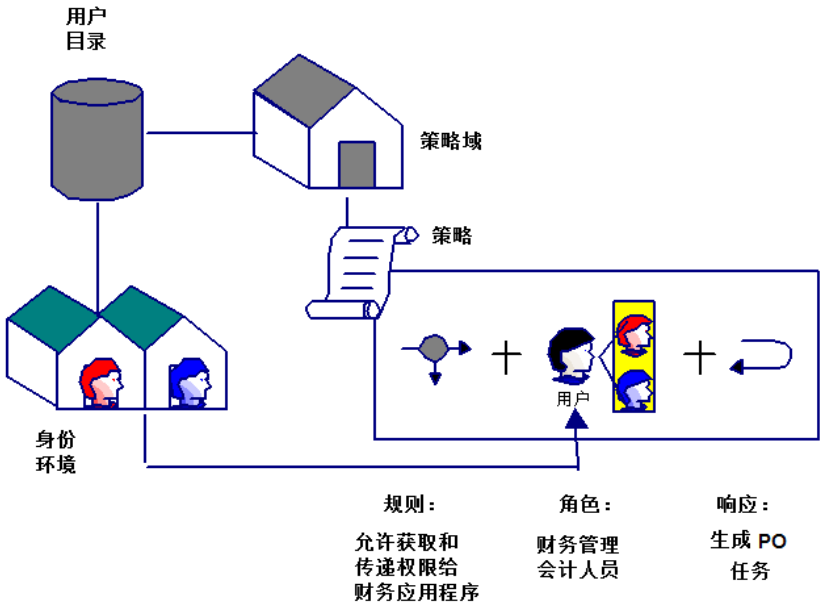
  Identity Manager 使用 SiteMinder 响应来将特定任务和角色信息发送给受保护资源。

您可以将 SiteMinder 策略绑定到用户，或绑定到角色，或绑定到用户 *和*角色。在用户或角色成员尝试访问受保护资源时，SiteMinder 使用策略中的信息来确定是否授予访问权，以及是否触发响应。

下图说明基于角色的策略中的策略对象的关系。



在策略域中创建 SiteMinder 策略，这在逻辑上将用户目录和受保护的资源联系在一起。 下图说明基于角色的策略中的策略对象的关系。



为向受保护的应用程序提供用户授权，SiteMinder 管理员使该应用程序的策略以及响应配对。 响应包含由 SiteMinder 生成的响应属性，该属性通过 Identity Manager 检索授权信息。

在 SiteMinder 为受保护资源进行角色成员授权时，会发生下列事件：

1. 策略的规则在 SiteMinder 执行，触发成对响应。
2. 策略服务器从 Identity Manager 获得要在响应中包含的授权信息。
3. 策略服务器将响应属性传给 Web 代理。
4. Web 代理将授权信息作为 HTTP 头变量或 cookie 提供给应用程序。

SiteMinder 生成的响应属性

Identity Manager 通过 SiteMinder Web 代理响应将授权信息发送给应用程序。这些响应在响应属性中包含 HTTP 头变量，应用程序可以使用这些变量确定用户的访问权限。 响应包含在 SiteMinder 策略中，它们确定用户与受保护资源交互的方式。

SiteMinder 管理员可以配置包括两种类型的响应属性的响应，以向应用程序传递信息：

- SM_USER_APPLICATION_ROLES[:*application id*]--返回分配给用户的角色列表
- SM_USER_APPLICATION_TASKS[:*application id*]--返回基于分配给用户的角色该用户可以执行的任务的列表

应用程序 ID 将所请求的角色和任务集限制为特定应用程序。 例如，如果您创建下列响应属性：

SM_USER_APPLICATION_ROLES:Finance_application

SiteMinder 将在 Finance 应用程序中具有任务的角色返回 Web 代理，代理然后将信息传递给 Finance 应用程序。

注意： 您提供的*应用程序 id* 应当与您使用“在 Identity Manager 中创建访问任务”时提供的*应用程序 id* 匹配。 如果您还没有创建该任务，应用程序 ID 可以是您选择的任何名称，但是它不能包含任何空格或非字母数字字符。

您可以在逗号分隔的列表中指定多个应用程序 ID，以便在一个响应属性中从多个应用程序返回一组角色和任务。例如，要返回用户在 Finance 和 Purchasing 应用程序具有的角色的列表，请指定以下内容：

SM_USER_APPLICATION_ROLES:Finance, Purchasing

在 SiteMinder 中启用访问角色的清单

注意：下列步骤假定，要应用您正在创建的访问角色的应用程序已经受到 SiteMinder 的保护。 如果您正在为不受 SiteMinder 的保护的应用程序创建访问角色，请参阅《*CA eTrust SiteMinder Policy Design Guide*》，了解在 SiteMinder 中配置应用程序的说明。

✓	步骤	参考.....
	1. 在策略服务器用户界面中，将与 Identity Manager 环境关联的用户目录分配给策略域。	*CA eTrust SiteMinder 策略设计*
	2. 将 Identity Manager 环境添加到保护应用访问角色的应用程序的 SiteMinder 域。	*CA eTrust SiteMinder 策略设计*
	3. 在策略域中，创建与访问角色将授予访问权的资源对应的领域和规则（如果他们还不存在）。	*CA eTrust SiteMinder 策略设计*
	4. 创建响应以将授权信息传递给资源。	创建 SiteMinder 响应 (p. 295)

✓	步骤	参考.....
	5. 创建策略并将它与以下内容关联： ■ 您在 Identity Manager 中创建的角色 ■ 您在第 2 步中创建的领域和规则。 ■ 您在第 4 步中创建的响应。	*CA eTrust SiteMinder 策略设计*

将 Identity Manager 环境添加到策略域中

要使 SiteMinder 能够支持访问角色，将 CA Identity Manager 环境与 SiteMinder 中的用户目录和策略域相关联。

注意：将与 CA Identity Manager 环境关联的用户存储添加到策略域，*然后才*能将 CA Identity Manager 环境添加到策略域。

要将 CA Identity Manager 环境添加到策略域

1. 在策略服务器用户界面的“策略域”对话框中，添加与带有如下策略域的 CA Identity Manager 环境关联的用户存储：
   a. 选择“用户目录”选项卡。
   b. 通过选项卡的底部的下拉列表框，选择要加入策略域中的用户目录。
   c. 单击“添加”按钮。
      策略服务器用户界面将该目录添加到显示在“用户目录”选项卡的列表中。
   d. 单击“应用”。
2. 如下所示将 CA Identity Manager 环境添加到策略域中：
   a. 选择“CA Identity Manager 环境”选项卡。
   b. 通过选项卡的底部的下拉列表选择要与策略域关联的 CA Identity Manager 环境。
   c. 单击“添加”。
      策略服务器用户界面将您的选择添加到选项卡顶部的 CA Identity Manager 环境列表中。
3. 单击“确定”保存选择，然后关闭该对话框。
   在创建策略时，就可以使用所选择的 CA Identity Manager 环境。

创建 SiteMinder 响应

1. 登录策略服务器用户界面。
2. 根据您的管理权限，执行下列操作之一：
   - 如果您有管理系统和域对象权限：
     a. 在“对象”窗格中，单击“域”选项卡。
     b. 选择要向其添加响应的策略域。
   - 如果有管理域对象权限，请在“对象”窗格中选择要为其添加响应的策略域。
3. 从菜单栏中选择“编辑”、“<domain name>”、“创建响应”。

   将打开“SiteMinder 响应”对话框（见“响应”对话框）。
4. 为新响应输入名称和说明。
5. 在“代理类型”分组框中，选择 SiteMinder 单选按钮。
6. 从“代理类型”分组框的下拉列表中选择“Web 代理”选项，然后单击“应用”以保存更改。
7. 单击“创建”。

   将打开“SiteMinder 响应属性编辑器”对话框。
8. 从“属性”下拉列表选择“WebAgent-HTTP-Header-Variable”响应属性。
9. 在“属性设置”选项卡中，选择“用户属性”单选按钮。
10. 在“变量”字段中，输入将发送到应用程序的变量的名称。

    例如，如果您指定变量 TASKS，会将下列头返回该应用程序：

    HTTP_TASKS
11. 在“属性名称”字段中，指定响应属性，如下所示：
    - SM_USER_APPLICATION_ROLES[:*application id1, application_id2, ...application_idn*]--返回分配给用户的角色列表
    - SM_USER_APPLICATION_TASKS[:*application id1, application_id2, ...application_idn*]

    SiteMinder 生成的响应属性 (p. 292)提供详细信息。
12. 单击“确定”以保存更改，并返回“SiteMinder 管理”窗口。

将角色添加到 SiteMinder 策略

当已被分配适当的访问角色的用户尝试访问受保护资源时，SiteMinder 策略服务器确认已为该用户分配访问角色，然后触发策略中包含的规则，以查看是否允许用户访问该资源。

将访问角色添加到 SiteMinder 策略

1. 在“SiteMinder 策略”对话框中，单击“用户”选项卡。

   对于策略域中包含的每个用户目录和 CA Identity Manager 环境，“用户”选项卡都包含相应的选项卡。

2. 选择包含您想要添加到策略的角色的 CA Identity Manager 环境。
3. 单击“添加/删除”按钮。

   将打开“SiteMinder 策略 Identity Manager 角色”对话框。

4. 要将角色添加到策略，请从“可用成员”列表中选择条目，并且将它移至“当前成员”列表。
5. 单击“确定”，保存更改并返回“SiteMinder 策略”对话框。

排除策略中的角色

除使用访问角色来给应用程序授权之外，您也能使用访问角色来防止访问角色的成员访问某个应用程序。 要防止访问角色成员访问某个应用程序，需要从 SiteMinder 策略排除这些角色。如果被分配了 CA Identity Manager 的排除访问角色的用户尝试访问受保护资源，策略服务器验证分配用户的 CA Identity Manager 角色排除。 验证后，它会阻止对该资源的访问。

遵循这些步骤:

1. 在“SiteMinder 策略”对话框中，单击“用户”选项卡。

   对于策略域中包含的每个用户目录和 CA Identity Manager 环境，“用户”选项卡都包含相应的选项卡。

2. 单击包含希望从策略中排除的角色的 CA Identity Manager 环境。
3. 单击“添加/删除”按钮。

   将打开“SiteMinder 策略 CA Identity Manager 角色”对话框。

4. 要将角色添加到策略，请从“可用成员”列表中选择条目，然后单击指向“当前成员”列表的“左箭头”按钮。

   相反步骤将从“当前成员”列表中删除角色。

5. 在“当前成员”列表中，选择要排除的角色，然后单击位于列表下方的“排除”按钮。

   带有斜线的红圈显示在已排除角色的左侧。

6. 单击“确定”，保存更改并返回“SiteMinder 策略”对话框。

配置 LogOff URI

要保护 CA Identity Manager 环境，配置保护环境的 SiteMinder Web 代理，以在用户注销 CA Identity Manager 之后终止用户会话。

通过删除 Web 浏览器中的 SiteMinder 会话和身份验证 cookie，并且指示策略服务器删除任何会话信息，Web 代理可以终止用户会话。

要终止 SiteMinder 会话，请针对保护 CA Identity Manager 环境的 SiteMinder 代理在代理配置对象的 LogOffURI 字段中配置注销功能。

注意：

- SiteMinder 代理有一个 LogOff URI。 该代理保护的所有应用程序使用同一个注销页面。
- 当您按照“配置注销页面”所述在管理控制台中配置自定义注销页面时，CA Identity Manager 将注销请求发送到自定义注销页面*和* LogOff URI。 然而，CA Identity Manager 仅向用户显示自定义注销页面。

遵循这些步骤:

1. 登录到下列界面之一：
   - 对于 CA SiteMinder r12 或更高版本，登录到管理 UI。
   - 对于 CA eTrust SiteMinder 6.0 SP5，登录到策略服务器用户界面。

   注意：有关使用这些界面的信息，请参阅正在使用的 SiteMinder 的版本的文档。
2. 如下所示，修改保护 CA Identity Manager 环境的代理的代理配置对象中的 #LogOffUri 属性：
   - 删除井号 (#)
   - 在“值”字段中，指定以下 URI：

     /iam/im/logout.jsp

   注意：在安装 Web 代理时选择代理配置对象。 有关详细信息，请参阅《*CA SiteMinder Web Access Manager Policy Server Installation Guide*》。
3. 保存更改。
4. 重新启动 Web 服务器。

SiteMinder 领域的别名

*别名*是用于访问 CA Identity Manager 环境的添加到 URL 的唯一的字符串。例如，如果环境的别名是 *employees*，则访问该环境的 URL 如下所示：

`http://myserver.mycompany.org/iam/im/employees`

myserver.mycompany.org

定义安装了 CA Identity Manager 的服务器的完全限定域名。

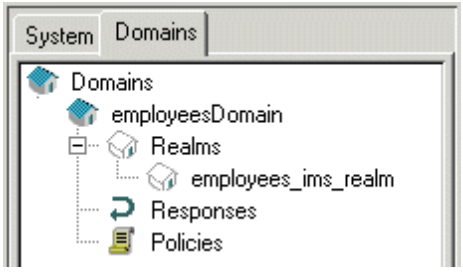
在管理控制台中创建 CA Identity Manager 环境时，至少指定一个别名。（您也可以指定公共别名。）

SiteMinder 使用环境名称来命名保护环境的对象。例如，如果指定名称 *employees*，SiteMinder 创建名为 *employeesobject_type* 的对象。

object_type

定义 SiteMinder 对象，如 employees_ims_realm。

下图显示了 SiteMinder 创建的两个对象：



更新 SiteMinder 领域中的别名

如果您在管理控制台中修改受保护别名或公共别名，CA Identity Manager 尝试在策略服务器中更新该别名。如果 CA Identity Manager 无法更新该名称，您可以在下列界面之一手动更新它们：

- 对于 CA SiteMinder Web Access Manager r12 或更高版本，使用管理 UI。
- 对于 CA eTrust SiteMinder 6.0 SP5，使用策略服务器用户界面。

遵循这些步骤:

1. 为 CA Identity Manager 环境定位领域。

   这些领域是在 CA Identity Manager 与 SiteMinder 整合时自动创建的（与其他必要的 SiteMinder 对象一起）。

   领域使用以下命名约定：

   - *Identity Manager-environment*_ims_realm—保护用户控制台。
   - *Identity Manager-environment*_pub_realm—启用对公共任务（如自行注册和忘记密码任务）的支持。只有当已经配置公共别名时，才会显示此领域。

     注意: 如果您使用策略服务器用户界面来修改该领域，首先为 CA Identity Manager 环境找到该策略域（*Identity Manager-environment* 域）。 这些领域位于域下。

2. 修改领域的资源，如下所示：

   /iam/im/*new_alias*

   不要在资源筛选器中删除别名前的 /iam/im/。

3. 保存更改。

注意： 修改 CA Identity Manager 属性提供了在管理控制台中更改别名的说明。

修改 SiteMinder 密码或共享密钥

当您向策略服务器安装 CA Identity Manager 扩展时，为 CA Identity Manager 用来与策略服务器进行通信的 SiteMinder 管理员帐户提供密码。

您可以更改此密码；但是密码必须加密。 要加密密码，请使用和 CA Identity Manager 一起提供的密码工具。

注意： 在您更改 SiteMinder 密码之前，确保为环境定义了 JAVA_HOME 变量。

遵循这些步骤:

1. 如下所示加密密码：

   a. 从命令行导航到 *admin_tools*\PasswordTool，其中 *admin_tools* 是管理工具的安装位置，如下列所示：

      - **Windows：** C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\PasswordTool
      - **UNIX：** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools/PasswordTool

b. 输入以下命令：

pwdtools *new_password*

在此命令中，*new_password* 是要加密的密码。

注意：有关 pwdtools 实用工具的选项的信息，请输入以下命令：

pwdtools help

c. 复制加密的密码。

2. 完成如下相关步骤：

- 如果 CA Identity Manager 正在 WebLogic 应用程序服务器上运行，执行以下任务：

  a. 在 WebLogic 控制台中，编辑 policyserver_rar 连接器描述符中的 WebLogic 资源适配器。

  b. 将加密密码添加为“密码”属性的值。

- 如果 CA Identity Manager 正在 JBoss 应用程序服务器上运行，执行以下任务：

  a。 通过 *JBoss_home*\server\default\deploy\iam_im.ear\policyserver_rar\META-INF 打开 ra.xml。

  b. 将加密密码添加为“密码”配置属性的值。

- 如果 CA Identity Manager 在 WebSphere 应用程序服务器上运行，完成下列任务：

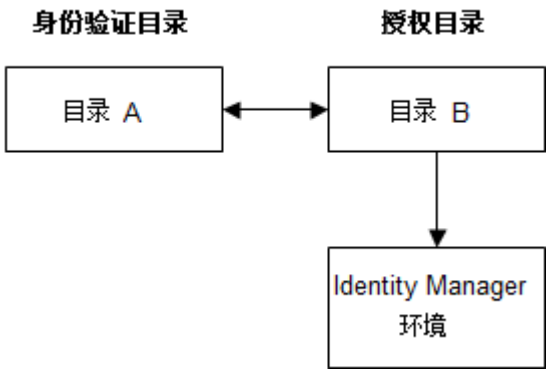
  a。 在 WebSphere 控制台中，打开 ra.xml。

  b. 将加密密码添加为“密码”配置属性的值。

3. 重新启动应用程序服务器。

配置 CA Identity Manager 环境以使用不同目录进行身份验证和授权

管理员可能需要管理这种类型的用户：用户配置文件位于用于验证管理员的用户存储之外的其他用户存储。 换句话说，在登录到 CA Identity Manager 环境时，管理员必须使用一个目录获得验证，并获得授权管理第二个目录的用户，如下图所示：



遵循这些步骤:

1. 登录到下列界面之一：
   - 对于 CA SiteMinder Web 访问管理器 r12 或更高版本，登录到管理 UI。
   - 对于 CA eTrust SiteMinder 6.0 SP5，登录到策略服务器用户界面。

   注意：有关使用这些界面的信息，请参阅您正在使用的 SiteMinder 的版本的文档。
2. 创建两个用户目录。

   一个目录引用身份验证数据（管理员配置文件），另一个目录引用授权数据（用户配置文件）。
3. 在管理控制台中创建 CA Identity Manager 环境。

   选择授权目录作为 CA Identity Manager 目录。
4. 在使用的 SiteMinder 版本的界面中，将身份验证目录添加到您在前一步骤中创建的 CA Identity Manager 环境的域中。

   在您创建环境以及 SiteMinder 与 CA Identity Manager 集成时，会自动创建域和 SiteMinder 所需的其他对象。

   域使用以下命名约定：

   *Identity Manager-environment*Domain
5. 确保此目录显示在与域关联的目录的列表中的第一位。
6. 找到 *Identity Manager-environment*_ims_realm。
7. 将授权目录映射到领域定义的“高级”部分的身份验证目录。
8. 找到下列 *Identity Manager-environment*response_ims 响应。

9. 将响应属性添加到响应中，如下所示：

字段	值
属性	Web-Agent-HTTP-Header-Variable
属性种类	用户属性
变量名称	sm_userdn
属性名称	SM_USERNAME

10. 保存更改。

CA Identity Manager 现在使用不同目录进行身份验证和授权。

如何改善 LDAP 目录操作的性能

因为对 LDAP 用户目录的全部 CA Identity Manager 请求的路由安排都通过固定的一组连接，目录操作可能要花更长时间处理。

要增加 CA Identity Manager 对用户目录的请求的吞吐量，请配置 SiteMinder 以打开到同一目录的多个连接。要完成此步骤，请在策略服务器用户界面的“LDAP 目录故障切换和负载平衡设置”对话框中，多次添加 LDAP 服务器。

输入 LDAP 服务器的次数（创建连接的数量）取决于 CA Identity Manager 的负荷。

附录 A： FIPS 140-2 遵从性

此部分包含以下主题：

FIPS 概述

美国联邦信息处理标准 (FIPS) 140-2 版本是产品进行加密时所应使用的密码库和算法的安全标准。FIPS 140-2 加密会作用于 CA 产品的组件之间以及 CA 产品和第三方产品之间的所有敏感数据的通信。FIPS 140-2 明确说明了在保护敏感的公开数据的安全系统内使用加密算法的要求。

CA Identity Manager 使用了被美国政府采用的高级加密标准 (AES)。 CA Identity Manager 包含了 RSA Crypto-J v3.5 和 Crypto-C ME v2.0 密码库，这两个密码库已经过验证，满足 FIPS 140-2 对密码模块的安全要求。

通讯

FIPS 加密覆盖 CA Identity Manager 和下列组件之间的所有数据通信：

- CA Identity Manager 服务器
- 配给服务器
- 供给管理器和客户端
- C++ 连接器服务器
- C++ 连接器服务器端点（如果端点支持）
- CA IAM 连接器服务器 (CA IAM CS)
- CA IAM CS 端点（如果端点支持）
- Connector Xpress（如果端点支持）
- Windows 密码同步代理
- Java Identity and Access Management (JIAM)

安装

Identity Manager 安装程序允许您配置 CA CA Identity Manager，以遵守 FIPS 140-2。

Identity Manager 环境中的所有组件均需要启用 FIPS 140-2，才能使 Identity Manager 支持 FIPS 140-2。 您需要 FIPS 加密密钥来在安装期间启用 FIPS 140-2。以下位置提供了生成 FIPS 密钥的密码工具 (pwdtools.bat/pwdtools.sh)：

```
C:\Program Files\CA\Identity Manager\IAM Suite\Identity
Manager\PasswordTool\pwdtools.bat
```

重要说明！ 在所有安装过程中使用同样的 FIPS 140-2 加密密钥，并且一定要保存好密码工具生成的密钥文件。

连接到 SiteMinder

在 Identity Manager 安装期间连接到 CA SiteMinder 时请注意，只有下表所列各项支持 FIPS 模式和产品版本配置：

Identity Manager r12	SiteMinder	SiteMinder 版本
FIPS-only 模式	FIPS-only 模式	r12
FIPS-only 模式	FIPS-compatible 模式	r12
非 FIPS 模式	FIPS-compatible 模式	r12
非 FIPS 模式	非 FIPS 模式	r6

密钥文件存储

CA CA Identity Manager 将文件系统用于了 FIPS 加密密钥存储。 CA Identity Manager 管理员负责为特定组或用户类型（例如有权运行 CA CA Identity Manager 的用户）设置目录访问许可，从而保护文件免受未经授权的访问。

下表列出了每个 CA Identity Manager 组件的 FIPS 密钥文件的位置。

组件	安装的位置
CA Identity Manager 服务器	*IdentityMinder.ear*\config\com\netegrity\config\keys\FIPSkey.dat *IdentityMinder.ear* 是 CA CA Identity Manager 在应用程序服务器上的安装位置。

组件	安装的位置
配给服务器	*Provisioning Server install*\data\tls\keymgmt\imps_datakey
C++ 连接器服务器	*Provisioning Server install*\data\tls\keymgmt\imps_datakey

密码工具

FIPS 兼容的密码工具实用工具 pwdtools.bat（或 pwdtools.sh）可以通过命令行在 CA Identity Manager 安装期间生成加密密钥。

在使用密码工具之前编辑 pwdtools.bat/pwdtools.sh 文件，并且根据需要设置变量 JAVA_HOME。

重要说明！ CA Identity Manager 不支持数据迁移或再加密。 因此，确保加密密钥在安装之后没有更改。

此命令使用以下语法：

```
pwdtools -{FIPSKEY|JSAFE|FIPS|RC2} -p plain text [-k <key file location>] [-f <encrypting parameters file>]
```

JSAFE

使用 PBE 算法加密纯文本值。

示例：

```
pwdtools -JSAFE -p mypassword
```

注意：在早期版本中，bootstrap 管理员的密码以明文存储。 如果您正在升级或迁移到 CA Identity Manager Service Pack 12.6.01 或以上版本，您需要手动加密明文密码。 确保在使用工具时指定“JSAFE”选项并执行这些步骤：

1. 在升级或迁移到 CA Identity Manager Service Pack 12.6.01 及以上版本后，转到 CA Identity Manager 对象存储数据库并搜索下表：
   IM_AUTH_USER
2. 使用 JSAFE 的密码工具加密明文密码。
3. 在表中将明文替换为加密的密码。

FIPSKEY

对于安装程序，创建 FIPS 密钥文件。您在安装 CA Identity Manager 之前生成密钥。

示例：

```
pwdtools -FIPSKEY -k C:\keypath\FIPSkey.dat
```

其中，*keypath* 是您想存储 FIPS 密钥的位置的完整路径。

密码工具在指定位置创建 FIPS 密钥。 在安装过程中，向安装程序提供 FIPS 密钥文件的位置。

注意：通过为特定组或用户类型（如获得授权可以运行 CA Identity Manager 的用户）设置目录访问权限，从而确保保护该密码。

FIPS

使用 FIPS 密钥文件加密纯文本值。 FIPS 使用现有的 FIPS 密钥文件。

示例：

```
pwdtools -FIPS -p firewall -k C:\keypath\FIPSkey.dat
```

其中，*keypath* 是 FIPS 关键目录的完整路径。

注意：使用您在安装过程中指定的 FIPS 密钥文件。

RC2

使用 RC2 算法加密纯文本值。

重要说明！ CA Identity Manager 使用 FIPS 密钥文件来检查以 FIPS 模式还是非 FIPS 模式启动应用程序。 因此，确保密钥文件命名为 FIPSKey.dat，带有下列应用程序服务器部署路径：

```
iam_im.ear\config\com\netegrity\config\keys\FIPSkey.dat
```

其中 iam_im.ear 位于应用程序服务器部署目录中，例如：

```
jboss_home\server\default\deploy
```

FIPS 模式检测

要确定 CA Identity Manager 是以 FIPS 模式还是非 FIPS 模式运行，请使用 CA Identity Manager 环境状态页面。

要查看该状态页面，请在浏览器中输入以下 URL：

`http://server_name/idm/status.jsp`

server_name

确定安装 CA Identity Manager 的服务器的完全限定域名，例如 myserver.mycompany.com。 在此例中，完整 URL 是：

http://myserver.mycompany.com/idm/status.jsp

FIPS 状态显示在页面的底部。

注意：您也可以通过查找以下密钥文件来检查 CA Identity Manager 是否以 FIPS 模式运行：

`/config/com/netegrity/config/keys/FIPSkey.dat`

如果此文件存在，则 CA Identity Manager 正在以 FIPS 模式运行。

FIPSkey.dat 密钥文件由密码工具 pwdtools.bat（或 pwdtools.sh）在 CA Identity Manager 安装期间创建。

加密文本格式

将算法名称作为前缀添加到加密文本，此名称会告知 CA Identity Manager 所使用的加密方法。

在 FIPS 模式下，前缀是 {AES}。 例如，如果您加密文本“密码”，加密文本类似于以下示例：

{AES}:eolQCTq1CGPyg6qe++0asg==

在非 FIPS 模式（或 JSAFE 模式）下，根据算法，前缀（算法标记）是 {PBES} 或 {RC2}。 例如，如果您加密文本“密码”，加密的文本类似于：

{PBES}:gSex2/BhDGzEKWvFmzca4w==

您可以使用系统下的密钥任务创建动态密钥。如果您定义动态密钥，密钥 ID 插入算法标记和标记分隔符 (‘:’) 之间。 如果加密数据没有密钥 ID 则表示加密使用硬编码密钥。 这可以用于向后兼容，或者用于没有为给定的算法定义动态密钥的情况。

加密信息

下列 CA Identity Manager 信息会被加密：

- Jboss 的数据源配置中的密码
- 忘记密码恢复信息
- 配给服务器回叫密钥
- 工作流会话信息
- 策略服务器连接信息

FIPS 模式日志

下列 CA Identity Manager 组件在日志文件中指出是否启用了 FIPS 模式：

- Identity Manager 服务器
- 配给服务器
- C++ 连接器服务器
- Java 连接器服务器
- 配给管理器
- 密码同步代理

在任何情况下，表明启用了 FIPS 模式的日志条目均以以下字符串结尾：

FIPS 140-2 MODE: ON

附录 B： 将 CA Identity Manager 证书替换成 SHA-2 签署的 SSL 证书

SHA-2 SSL 证书散列法是一种加密算法，是由国家标准与技术局 (NIST) 和国家安全局 (NSA) 开发的。 SHA2 证书与所有以前的算法相比更安全。 在 CA Identity Manager 中，您可以配置 SHA-2 签署的 SSL 证书，代替 SHA-1 散列函数签署的证书。

注意：有关配置 SSL 证书的详细信息，请参阅 *《安装指南》*。

下表显示了在 CA Identity Manager 服务器上的可以放置 SHA-2 签署的证书的路径位置：

证书	安装位置	说明
配给服务器证书	[配给服务器安装目录]/data/tls/server/eta2_servercert.pem [配给服务器安装目录]/data/tls/server/eta2_serverkey.pem *cs_install*/ccs/data/tls/server/eta2_servercert.pem *cs_install*/ccs/data/tls/server/eta2_serverkey.pem *cs_install*/jcs/conf/eta2_server.p12	以 .pem 格式由配给服务器使用、以 .p12 格式由 CA IAM CS 使用（包括签署的证书、私钥和根 CA 证书）。 **注意：**将 eta2_server.p12 导入别名 eta2_server 之下的 *cs_install*/jcs/conf/ssl.keystore 并删除现有条目。ssl.keystore 密码是在安装过程中提供的连接器服务器的密码。

证书	安装位置	说明
配给客户端证书	[配给服务器安装目录]/data/tls/client/eta2_clientcert.pem [配给服务器安装目录]/data/tls/client/eta2_clientkey.pem [配给管理器安装目录]/data/tls/client/eta2_clientcert.pem [配给管理器安装目录]/data/tls/client/eta2_clientkey.pem *cs_install*/ccs/data/tls/client/eta2_clientcert.pem *cs_install*/ccs/data/tls/client/eta2_clientkey.pem *cs_install*/jcs/conf/eta2_client.p12	以 .pem 格式由配给服务器使用、以 .p12 格式由 CA IAM CS 使用（包括签署的证书、私钥和根 CA 证书）。
配给目录受信任证书	*cadir_install*/config/ssld/impd_trusted.pem	以 .pem 格式由 CA Directory 使用。 它必须包含下列结构的证书内容： -----BEGIN CERTIFICATE----- 证书内容 -----END CERTIFICATE-----
配给目录个性证书	*cadir_install*/config/ssld/personalities/impd-co.pem *cadir_install*/config/ssld/personalities/impd-inc.pem *cadir_install*/config/ssld/personalities/impd-main.pem *cadir_install*/config/ssld/personalities/impd-notify.pem *cadir_install*/config/ssld/personalities/impd-router.pem	以 .pem 格式由 CA Directory 使用。

证书	安装位置	说明
根 CA 证书	[配给服务器安装目录]/data/tls/et2_cacert.pem [配给管理器安装目录]/data/tls/et2_cacert.pem *cs_install*/ccs/data/tls/et2_cacert.pem *conxp_install*/lib/jiam.jar [应用程序服务器安装目录]/iam_im.ear/library/jiam.jar	将证书导入位于[Connector Xpress 安装目录]/conf/ssl.keystore 的 Connector Xpress 密钥库。 还需要将证书导入 jiam.jar 密钥库。要导入，请解压缩 jar 文件，将证书导入 admincacerts.jks，然后将 jar 内容重新打包。 admincacerts.jks 的密钥库密码是“changeit”。 确认替换了 jiam.jar 的所有副本。

有用命令

OpenSSL 程序是使用 OpenSSL 的库的各种加密功能的命令行工具。 此工具是与 IMPS 一起提供的，位于[配给服务器安装目录]/bin。

下表显示 OpenSSL 程序的几个有用的命令，可以执行与管理证书有关的各种命令：

命令	说明
openssl x509 –in cert.pem –text –noout	打印 .pem 证书的内容。
openssl.exe pkcs12 -in my.pkcs12 –info	打印 .p12 文件的内容。
openssl.exe pkcs12 -export -chain –inkey key.pem –in cert.pem -CAfile cacert.pem -out my.p12	将 .pem 证书/密钥对转换为 .p12。
keytool –list –v -keystore my.keystore	打印 java 密钥库的内容。
keytool –list –v –alias myalias –keystore my.keystore	打印 java 密钥库中特定别名的内容

命令	说明
keytool –delete –alias myalias –keystore my.keystore	从 java 密钥库中删除别名
keytool –importkeystore –destkeystore my.keystore –srckeystore src.p12 –srcstoretype PKCS12 –srcalias 1 –destalias myalias	将 .p12 导入 java 密钥库。
keytool -import -trustcacerts -alias myrootca -file rootcacert.pem -keystore my.keystore	将 .pem 根 CA 证书导入 java 密钥库。