CA Identity Manager™

实施指南

12.6.5

ca technologies

CA Technologies 产品引用

本文档引用以下 CA Technologies 产品：

- CA CloudMinder™ 身份管理
- CA Directory
- CA Identity Manager ™
- CA Identity Governance（以前是 CA GovernanceMinder）
- CA SiteMinder®
- CA 用户活动报告
- CA AuthMinder ™

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。

目录

第 1 章： 管理身份和访问权限

此部分包含以下主题：

用户管理和应用程序访问

典型的信息技术 (IT) 部门需要持续维护用户帐户。 IT 管理员必须解决用户的迫切需要，如忘记密码重置、创建新建帐户以及提供补给和办公用品。

同时，IT 管理员必须为用户提供应用程序的各种访问级别。 例如，部门经理生成订购单，需要财务应用程序帐户。

为了解决不断增加的 IT 需求，CA CA Identity Manager 提供管理用户及其对应用程序的访问权限的集成方法，包括：

- 通过角色分配权限。 特别是：
  - 使管理员能够创建和维护用户帐户的角色
  - 为现有用户配给其他帐户的角色（需要配给支持）
- 用户和应用程序访问权限管理指派
- 用户可以用来管理自己帐户的自助服务选项
- 业务应用程序与 CA CA Identity Manager 的集成
- 自定义和扩展 CA CA Identity Manager 的选项

基于角色的权利

您通过分配角色为用户分配权限。 *角色*包含与 CA Identity Manager 中的应用程序功能相对应的任务（如“创建用户”任务）、应用程序中的功能（如“创建订单”功能）或提供用户帐户（如 SAP 帐户）的帐户模板。 在为用户分配角色时，即授予其相应权限。

CA Identity Manager 提供以下类型的角色：

- 用户管理角色，其被称为*管理角色*。

  管理角色还可包括在用户控制台中显示的任何任务。
- 帐户分配角色，其被称为*配给角色*
- 应用程序功能角色，其被称为*访问角色*。

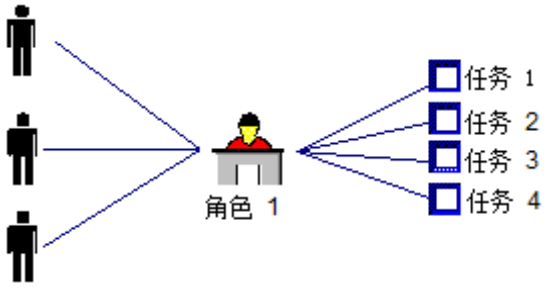
如果您从角色中删除某一任务或帐户模板，用户将再也无法执行该任务、使用端点帐户或使用应用程序功能。

管理角色

管理角色控制用户在 CA Identity Manager 中可以执行的操作。 系统管理员将角色分配给用户；该角色定义用户可以执行的一系列任务。 用户可以对用户帐户执行管理*任务*，例如更改密码或更新职位。

不同的用户对这些任务有不同级别的访问权限。 例如，“员工”角色可能包含让用户能够修改其姓名和地址的任务，而“人力资源经理”角色则包含修改用户职位和工资的任务。

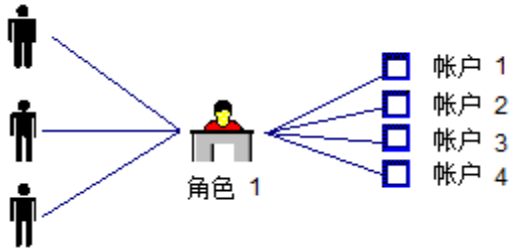
下图显示了四项任务，这些任务组合成一个管理角色并分配给了三名用户：



配给角色

要将用户访问权限授予其他应用程序（如电子邮件系统）的帐户，请分配配给角色。 配给角色包含帐户模板，该模板定义存在于一种类型帐户的属性。 例如，Exchange 帐户的帐户模板定义了邮箱大小等属性。 帐户模板还可定义如何将 CA Identity Manager 用户属性映射到帐户。

下图显示了四个帐户，这些帐户组合成一个配给角色并分配给了三名用户： 将配给角色分配给用户时，每个用户均将获得四个帐户



访问角色

访问角色提供另一种在 CA Identity Manager 或其他应用程序中提供权利的方式。 例如，您可使用访问角色来完成下列任务：

- 提供对用户属性的间接访问
- 创建复杂的表达式
- 在用户配置文件中设置一个属性，另一个应用程序使用该属性来确定权利

访问角色与身份策略类似，也是将一组业务更改应用到用户或用户组。 然而，在使用访问角色来应用业务更改时，您可以通过查看访问角色的成员看到更改应用到哪些用户。

在大多数情况下，访问角色不与任务关联。

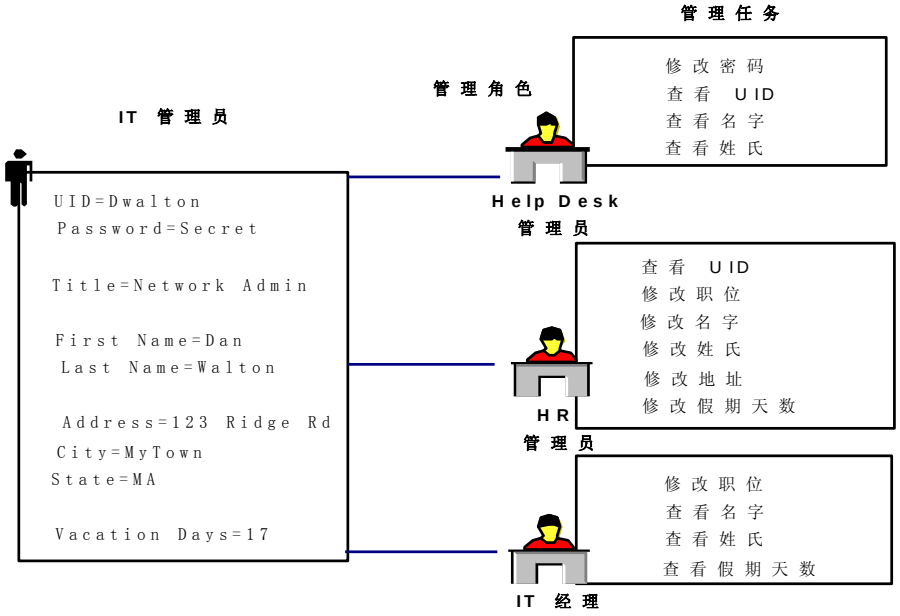
注意：当 CA Identity Manager 与 CA SiteMinder 集成时，访问角色还可提供对受 CA SiteMinder 保护的应用程序的访问。 在这种情况下，访问角色确实包括访问任务。 有关详细信息，请参阅*《Configuration Guide》*中有关 SiteMinder 集成的章节。

用户帐户管理的管理角色

在 CA CA Identity Manager 中，您通过管理角色管理用户存储对象（用户、组和组织）。 您也使用管理角色管理用以管理用户存储对象的角色和任务。 例如，您使用管理角色来修改用户的配置文件属性，为用户提供管理自己帐户的选项，并且批准使用工作流的任务。

属性级别的配置文件管理

您可以为需要读或写不同配置文件属性的不同管理员创建管理角色。 例如，公司可能有几位员工对用户配置文件执行操作，他们各自访问不同属性。 下图显示三个角色和他们的关联的任务。 每个角色对配置文件属性有不同的访问权限。



在此示例中，三个角色可以为同一用户 Dan Walton 管理不同属性：

- 帮助中心管理员可以查看用户名和地址，并可以重置用户密码。
- 人力资源管理员修改用户 ID、用户姓名、地址、头衔以及年假天数。
- IT 经理修改用户职称，查看他们的姓名和假期天数。

当您登录到 CA CA Identity Manager 时无论具备什么角色，都会根据分配给您的 CA CA Identity Manager 帐户的管理角色显示一系列称为类别的选项卡。 单击选项卡以看见您可以在该类别中执行的任务，如下图所示：

用户可以看到的类别以及类别中的任务由用户的管理角色决定。

管理任务的工作流批准

要帮助实现业务流程自动化，您可以设计管理员任务以生成工作流流程。*工作流流程*为公司经常重复的明确定义的流程实现自动化。 CA CA Identity Manager 包括 WorkPoint 工作流引擎。

工作流流程由作为管理任务一部分的 CA CA Identity Manager 事件触发。例如，“创建用户”任务包括称为“CreateUserEvent”和“AddToGroupEvent”的事件。 在事件发生时，工作流引擎可以：

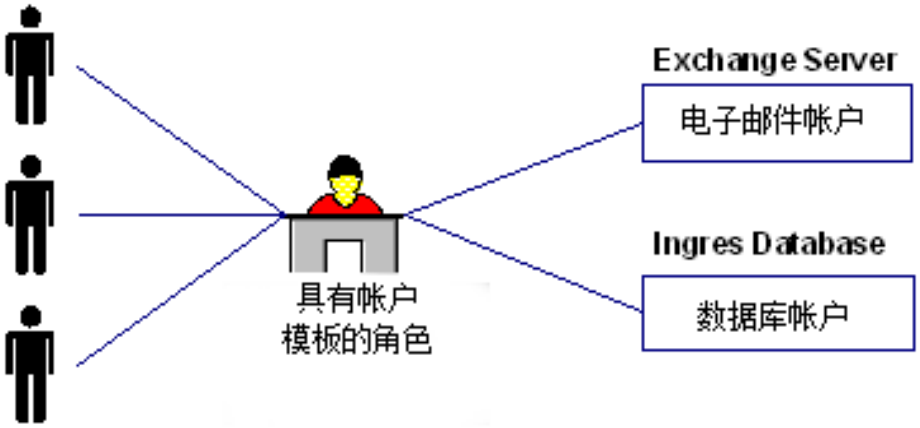
- 要求批准－批准人必须批准某一事件，如修改用户配置文件，然后 CA CA Identity Manager 才能更新用户存储。批准人是有特定任务的批准人角色的管理员。
- 发送通知－工作流引擎在流程的不同阶段可以通知用户事件的状态，如用户启动事件的时间，或批准事件的时间。

- 生成工作列表－工作列表指定特定用户必须执行的任务。 工作流引擎自动更新管理员的工作列表。

对于通用事件，您可以使用随 CA CA Identity Manager 提供的工作流流程。或者，您可以创建自定义工作流流程。

其他帐户的配给角色

在 CA CA Identity Manager 中，您通过使用配给角色向用户提供其他帐户。配给角色包含帐户模板，它们定义存在于管理端点（如电子邮件服务器）的帐户。 如果您在 CA CA Identity Manager 中有用户，您就可以将配给角色分配给其中一些用户。 用户接收由角色中的模板定义的这些帐户。



帐户模板定义帐户的特征。 例如，Exchange 帐户的帐户模板可以定义邮箱大小。 帐户模板还定义了用户属性如何映射到帐户。

要能使用配给角色，您必须使用 Identity Manager 服务器安装配给服务器。 然后，您在用户控制台中创建帐户模板。

密码管理

Identity Manager 包括若干种用于管理用户密码的功能：

- 密码策略－这些策略通过强制执行管理密码到期、组成及使用的规则和限制来管理用户密码。

  注意：对于高级的密码策略，使用 SiteMinder 配置集成。 有关详细信息，请参阅 *《安装指南》*。

- 密码管理者－当用户致电帮助中心时，这些具有密码管理者角色的管理员可以重置密码。

- 自助式服务密码管理－Identity Manager 包括若干个使用户可以管理自己的密码的自助服务任务。 这些任务包括：
  - 自行注册－用户在企业网站注册时，指定密码。
  - 更改我的密码－用户无需 IT 或帮助中心人员的帮助即可修改其密码
  - 忘记密码－在 Identity Manager 验证用户身份后，用户即可重置或找回忘记的密码。
  - 忘记用户 ID－在 Identity Manager 验证用户的身份后，用户即可找回忘记的用户 ID。
- 密码同步（仅用于配给）－密码更改在 Identity Manager 和称为“端点”的目标系统的帐户中是同步的。 根据 Identity Manager 密码策略验证新密码。

用户的自助服务选项

为了进一步减少 IT 工作负荷，CA CA Identity Manager 包括注册新用户和提供忘记的密码的功能。 这些功能不需要管理员参与。 用户通过*公共控制台*获得 CA CA Identity Manager 的访问权限，此控制台不需要登录帐户。 通过此控制台，用户可以在某一站点自行注册或请求关于忘记的密码的提醒。

为了节省 IT 管理员的时间，CA CA Identity Manager 用户可以管理自己的帐户。 因为用户有自主管理角色，他们可以：

- 维护个人信息
- 更改自己的密码
- 加入自行订阅组

Identity Manager 自定义和扩展性

您可以自定义这些 CA CA Identity Manager 功能：

- Identity Manager 目录，此功能向 CA CA Identity Manager 描述用户存储结构。
- 用户界面的外观和功能。
- 用户条目屏幕，此功能确定每个任务屏幕的字段和布局。
- 通过正则表达式、JavaScript 或 Java 实施验证用户数据条目。
- 工作流，此功能定义自动化的工作流流程。 通过将批准人和 WorkPoint 流程设计器的操作链接在一起，来创建或修改流程。

- 电子邮件，此功能向用户通知任务状态。
- 任务提交，第三方应用程序可以将此信息发送到 Identity Manager 任务执行 Web 服务 (TEWS)。 TEWS 处理远程任务请求。 远程任务请求需要符合 WSDL 标准。

您可以使用下列 API 扩展 CA CA Identity Manager 功能：

- 逻辑属性 API－您能够使用与属性实际存储在用户目录中的方式不同的方式显示属性。
- 业务逻辑任务处理程序 API－允许您在数据验证或转换操作期间执行自定义业务逻辑。
- 工作流 API－向工作流流程的自定义脚本提供信息。 脚本评估信息，并且相应确定工作流流程的路径。
- 参与人确定程序 API－使您能够指定有权批准工作流活动的参与人的列表。
- 事件侦听程序 API－使您能够创建侦听特殊的 Identity Manager 事件或事件组的自定义事件侦听程序。 当事件发生时，事件侦听程序可以执行自定义业务逻辑。
- 通知规则 API－允许您确定应当收到电子邮件通知的用户。
- 电子邮件模板 API－在电子邮件通知中加入事件特定信息。

注意：有关 CA CA Identity Manager API 的详细信息，请参阅*《Programming Guide for Java》*。

如果 CA Identity Manager 包含配给，您也可以扩展配给功能，如下所示：

- 自定义连接器－启用配给服务器和端点系统之间的通信。 构成连接器的代码可以包括 GUI 插件、服务器插件和代理插件。

  Connector Xpress 可以生成动态连接器，可以在 Java 或 C++ 中开发自定义静态连接器。
- 程序出口－使您可以引用来自配给服务器流程流的自定义代码。

注意：有关扩展配给功能的详细信息，请参阅 *《Programming Guide for Provisioning》*。

CA Identity Governance 集成

CA Identity Governance 是一个身份生命周期管理产品，使用该产品可以快速准确地开发、维护和分析角色模型。 该产品还提供了集中式的身份遵从策略控制，并对与符合遵从性和安全需求有关的过程进行了自动化。使用 CA Identity Governance，可执行以下操作：

- 验证 CA Identity Manager 用户权限是根据业务遵从策略授予的
- 在创建或修改 CA Identity Manager 用户、角色和帐户时按照建议进行角色和遵从性检查
- 了解您的组织内的角色，建立适合您的组织的角色模型，在 CA Identity Manager 之内重新创建理想的角色模型
- 随着业务的不断发展分析和维护该角色模型

CA Identity Manager 与 CA Identity Governance 以两种方式进行集成：

- CA Identity Manager 的 CA Identity Governance 连接器

  一种特殊类型的连接器，自动同步 CA Identity Manager 和 CA Identity Governance 之间的权限数据。 通过使用该连接器，可以将数据从 CA Identity Manager 导入 CA Identity Governance，或将数据从 CA Identity Governance 导出到 CA Identity Manager。

- Smart Provisioning

  将 CA Identity Manager 与 CA Identity Governance 集成后，还可以配置其他功能，从而使您能够使用角色和遵从性信息（位于角色模型中）来支持身份管理日常操作。在 CA Identity Manager 所作的更改会动态更新 CA Identity Governance 中的角色模型。

注意：有关与 CA Identity Manager 的 CA Identity Governance 集成的详细信息，请参阅 CA Identity Governance 总目录中提供的 *《CA Identity Manager Integration Guide》*。

CA 用户活动报告集成

从 CA Identity Manager 12.6 版开始，“CA Enterprise Log Manager”称为 CA 用户活动报告（CA UAR）。

CA UAR 使用 CA Common Event Grammar (CEG) 将源自各种系统的事件映射为一个标准格式，并存储所有事件以便进行复查和分析，即使那些尚未映射的事件也会存储。 而且，CA UAR 向用户提供了大量的解决方案，用于管理和报告收集的数据以及使用可配置数据库查询和/或报告来搜索各种类型的信息和事件。

CA UAR 对于非管理系统以及超出 CA Identity Manager 能力和控制之外的系统提供了更好、更宽和更深入的了解，并且还能让您深入调查身份。

与 CA Identity Manager 集成使您可以使用 CA Identity Manager 用户控制台查看 CA UAR 身份中心报告和/或动态查询到 CA UAR 用户控制台。 在该用户控制台中，您可以配置查看和修改现有 CA Identity Manager/CA UAR 报告和/或查询的方式，同时还能深入调查某个特定的身份。

CA UAR 报告

默认情况下，将随 CA UAR 角色定义提供下列 CA UAR 报告：

任务	调用报告
系统所有事件 (按用户)	CA Identity Manager—按用户 ID 筛选的系统所有事件
帐户管理 (按主机)	帐户管理 (按主机)
帐户创建 (按帐户)	帐户创建 (按帐户)
帐户删除 (按帐户)	帐户删除 (按帐户)
帐户锁定 (按帐户)	帐户锁定 (按帐户)
认证过程活动 (按主机)	CA Identity Manager—流程活动（按主机）
密码策略修改活动	CA Identity Manager—策略修改活动

第 2 章： 满足业务需求

此部分包含以下主题：

处理业务更改

通过使用身份策略，您可以自动处理特定身份管理任务。 身份策略是指在用户符合某一条件或规则时所发生的一组业务更改。 您可以使用身份策略集执行以下操作：

- 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 (p. 23)。 例如，您可以创建一个身份策略集，用于禁止支票签署人角色的成员拥有支票批准人角色，并将公司每个人可签署支票的金额限定在 10000 美元以内。
- 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。

  强制遵从的身份策略称为*遵从策略*。

与身份策略相关联的业务更改包括：

- 分配或撤回角色，包括配给角色（在 CA Identity Manager 包括配给时）
- 分配或吊销组员资格
- 更新用户配置文件中的属性

例如，某家公司可能会创建一个身份策略，规定所有副总裁均属于乡村俱乐部成员组，且均具有工资批准人角色。 当用户的职称变为副总裁，且该用户与该身份策略同步时，CA Identity Manager 会将该用户添加到相应的组和角色。 如果副总裁晋升为 CEO，她将不再满足副总裁身份策略中的条件，因此将吊销该策略所应用的更改，并且将应用基于 CEO 策略的新更改。

基于身份策略的更改操作包含可置于工作流控制下且能进行审核的事件。 在上一示例中，工资批准人角色向其成员授予了重要权限。 为保护工资批准人角色，公司可以创建一个工作流流程，要求在分配此角色之前经过一系列批准，并且可配置 CA Identity Manager 对角色分配进行审核。

为简化身份策略管理，身份策略将组成一个身份策略集。 例如，副总裁策略和 CEO 策略可能属于行政权限身份策略集。

遵守业务策略

遵从是一种企业管理方法，其中包括众多的规程，可以确保公司及其员工遵守企业政策。 这些遵从规程通常涉及对应用程序和系统的权利分配进行记录、自动执行或审核。

CA Identity Manager 包括支持遵从管理的以下功能：

- **Smart Provisioning**

  “智能配给”是一个功能集，它简化了 CA Identity Manager 与 CA Identity Governance 集成后的配给角色分配。 功能包括：

  - 建议配给角色

    CA Identity Manager 可向管理员提供一个适合分配给用户的配给角色列表。配给角色列表是 CA Identity Governance 根据管理员输入的条件确定的。

    建议配给角色有助于确保用户具有正确的权限，同时能够保持公司的角色模型。

  - 遵从和模式消息

    CA Identity Manager 管理员可以在提交更改之前根据 CA Identity Governance 中的角色模型验证提议的更改。提交更改前先进行验证有助于公司维护为其运作所定义的角色模型。

    用户可以验证对配给角色的已建议更改（对其分配或删除）以及用户属性的更改。

CA Identity Manager 执行两种类型的策略验证：

- 遵从

  根据 CA Identity Governance 角色模型来验证提议更改，看这些更改是否违反 CA Identity Governance 中明确的、预先定义的业务策略规则。

- 模式

  将已建议更改和 CA Identity Governance 角色模型作比较，以查看这些更改是否有可能变为“非模式”。CA Identity Manager 也将确保这些更改不会明显改变该角色模型中已建立的模式。

  您可以将 CA Identity Manager 配置为在用户执行特定任务时自动执行这些验证，或者允许用户手动启动验证。

一旦 CA Identity Governance 中已建立角色模型（基于 CA Identity Manager 数据），即可在 CA Identity Manager 环境中实施智能配给。

注意：有关详细信息，请参阅 *《管理指南》*。

- **身份策略**

  您可以创建一个遵从策略，这是一种身份策略 (p. 19)，可以禁止拥有其他权限的用户再拥有某种权限。 例如，您可以禁止拥有批准检查权限的用户发出检查。

  遵从策略增强了您环境中的职责划分。

- **遵从报告**

  CA Identity Manager 包括显示您环境中用户遵从状态的示例报告。通过这些报告，您可以了解哪些用户未遵守您的业务策略。

遵从报告

CA Identity Manager 提供了可供您监控对公司业务策略遵从情况的报告，下表是一些示例。

Report	说明
角色成员	在报表数据库中显示角色，并且列出那些角色的成员

Report	说明
角色	显示报告数据库中的每个角色的以下信息： ■ 与该角色关联的任务 ■ 成员策略和角色成员 ■ 管理员策略和角色管理员 ■ 所有者策略和角色所有者
任务角色	在报告数据库中显示任务以及它们所关联的角色
用户角色	在报告数据库中显示用户并且列出每名用户的角色
非标准帐户趋势	显示孤立帐户、系统帐户和异常帐户的非标准帐户趋势
非标准帐户	显示所有孤立、系统和异常帐户
孤立帐户	显示配给服务器中没有全局用户的所有端点帐户
策略	显示所有身份策略
用户配置文件	显示用户的以下信息： ■ 名称 ■ 用户 ID ■ 用户作为成员或管理员的组 ■ 用户作为成员、管理员或所有者的角色
端点帐户	显示每个端点的帐户（您可以选择要查看哪个端点）
角色管理员	显示角色和他们的管理员
角色所有者	显示角色和他们的所有者
“Snapshots”（快照）	显示所有导出的快照
“User Account”（用户帐户）	显示用户的列表和他们的帐户

Report	说明
“User Entitlements”（用户权利）	显示用户的角色、组和帐户
“User Policy Sync Status”（用户策略同步状态）	显示每个策略的用户状态（哪些策略应当被分配、重新分配或再分配）

注意：有关报告的详细信息，请参阅*《管理指南》*。

强制满足职责隔离要求

职责隔离 (SOD) 要求防止用户收到可能导致利益冲突或欺诈的权限。 CA Identity Manager 提供以下功能来支持 SOD：

- **预防性身份策略**

  通过在提交任务之前执行的这些策略，管理员可以在分配权限或更改配置文件属性之前检查策略违规。 如果违规存在，在提交任务之前，管理员可以清除违规。

  例如，公司可以创建一个预防性身份策略，来阻止具有用户经理角色的用户同时具有用户批准人角色。 如果管理员使用修改用户任务为用户管理者提供用户批准人角色，CA Identity Manager 则会显示一条关于该违规的消息。 管理员可以更改角色分配以便在提交任务之前清除该违规。

- **通过智能配给的策略验证**

  CA Identity Manager 管理员可以在提交更改之前针对 CA Identity Governance 中的业务策略规则 (BPR)，对配给角色和用户属性验证提议的更改。 BPR 表示对权限的各种各样的限制。 例如，BPR 可能会阻止拥有采购部门角色（允许成员从转包商订购库存）的用户同时拥有转包商付款角色。 系统管理员、业务管理者、审核者或角色工程师在 CA Identity Governance 中创建 BPR。

  注意：有关 BPR 的详细信息，请参阅*《CA Identity Governance Sage DNA User Guide》*。

注意：有关预防性身份策略和智能配给的详细信息，请参阅*《CA Identity Manager Administration Guide》*。

用户存储中的转换数据

某些情况下，您可能希望 CA Identity Manager 先转换数据，然后再将其存储到用户存储。例如，您可能希望它以不同于输入时的格式存储信息，或在特定类型的信息出现时应用更改。

CA Identity Manager 包括转换数据的以下功能：

- 身份策略
- 逻辑属性处理程序

注意：您也能使用身份策略和逻辑属性处理程序来实施自定义业务逻辑。

逻辑属性处理程序

逻辑属性处理程序是转换在 CA Identity Manager 任务屏幕上使用的用户属性值的自定义 Java 代码。 使用逻辑属性处理程序，您可以控制物理属性在任务屏幕上的显示方式。 您也能使用逻辑属性处理程序将任务屏幕上的显示值（如成本）转换为存储在用户存储中的一个或多个物理属性（如单位价格和数量）。

注意：有关逻辑属性处理程序的详细信息，请参阅*《Programming Guide for Java》*。

应用自定义业务逻辑

您可以自定义 CA Identity Manager，以便实施您的公司需要的业务逻辑。CA Identity Manager 包括实施自定义业务逻辑的下列选项：

- 身份策略－您可以使用身份策略来定义在用户满足特定的条件或规则时发生的一整套业务更改。 例如，身份策略可以实现特定身份管理任务的自动化，如分配角色，或实施业务规则（如防止用户签署并且批准超过 $20,000 的支票）。

  注意：有关身份策略的详细信息，请参阅*《管理指南》*。
- 逻辑属性处理程序—您可以将这些处理程序与 CA Identity Manager 任务屏幕关联起来，以便控制属性值的显示和修改。

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

- 业务逻辑任务处理程序—使您能够在 CA Identity Manager 任务的数据验证操作期间，执行自定义业务逻辑（如以下内容）：
  - 实施自定义业务规则（例如，管理员所管理的组不能超过五个）。
  - 验证客户特有的任务屏幕字段（例如，“员工 ID”字段的值必须存在于主人力资源数据库中）。

  业务逻辑任务处理程序可以在 Java 或 JavaScript 中实施。

  注意：有关详细信息，请参阅 *《Programming Guide for Java》*。
- 工作流—允许您创建与 CA Identity Manager 事件关联的自定义过程定义。

注意：决定是否在业务逻辑任务处理程序或工作流流程中实施业务逻辑之前，请参阅以下部分：

- 业务逻辑任务处理程序的考虑事项 (p. 25)
- 工作流流程的考虑事项 (p. 25)

业务逻辑任务处理程序的考虑事项

业务逻辑任务处理程序在任务的同步处理阶段执行业务逻辑验证，是发生在事件生成之前。 通过它，您可以：

- 执行任务级验证。 例如，您可以基于用户配置文件屏幕中指定的办公室位置添加或删除组的成员。
- 如果验证失败，防止提交任务。
- 自动转换任务屏幕上的所有信息，以便在任务提交之前符合您的业务策略。

注意：您不应当实施需要花费很长时间才能在业务逻辑任务处理程序中完成的活动。 运行时间长的活动会延迟任务的提交，不太适合会发生用户交互的同步阶段。可改为使用工作流流程，其在任务的异步阶段执行。

工作流流程的考虑事项

工作流流程在任务的异步阶段被调用，并且与各个事件的执行相关联。通过它，您可以：

- 执行基于单个事件数据的批准活动
- 执行运行时间长的自定义业务逻辑活动

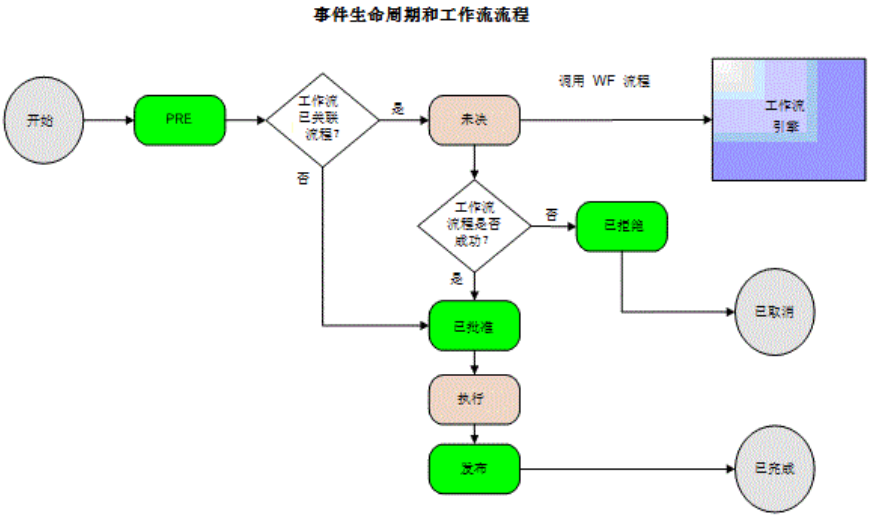
尽管工作流 API 允许您从工作流活动获得任务级数据，但通常您是操作在工作流下的该具体事件的环境中。

批准业务更改

工作流所描述的过程包括必须执行的一个或多个步骤，以便实现一些业务目标，如执行雇用程序，或从外部系统获得用户的信用积分。 通常，工作流流程中会有一个步骤涉及到对业务更改的批准或拒绝。

在 CA Identity Manager 中，工作流流程与事件（发生在任务处理期间的操作）相关联。在事件进入生命周期的“未决”状态时，CA Identity Manager 会调用任何关联的工作流流程并且暂停事件执行，直到过程完成。 然后 CA Identity Manager 基于工作流流程的结果执行或拒绝事件。

此顺序在下图中显示：



CA Identity Manager 包括用于创建和管理工作流流程的 InSession WorkPoint 工作流引擎。

注意：有关详细信息，请参阅 *《管理指南》*。

第 3 章： CA Identity Manager 体系结构

此部分包含以下主题：

CA Identity Manager 组件

CA Identity Manager 实施可能包括以下组件的一部分或全部：

- 服务器
- 用户存储
- 数据库
- 连接器

服务器

取决于您需要的功能，CA Identity Manager 实施包括一个或多个服务器类型。

CA Identity Manager 服务器（必需）

在 CA Identity Manager 之内执行任务。 J2EE CA Identity Manager 应用包括管理控制台和用户控制台。

CA Identity Manager 配给服务器

管理端点系统上的帐户。

如果 CA Identity Manager 安装支持帐户配给，则需要此服务器。

注意：安装配给服务器之前，必须在 CA Directory Server 上远程地安装配给目录（或仅用于本地演示环境）。

SiteMinder 策略服务器

向 CA Identity Manager 提供高级身份验证，并且提供对密码服务和单点登录等 SiteMinder 功能的访问。

该服务器为可选服务器。

用户存储和开通目录

CA Identity Manager 协调以下两个用户存储：

- *CA Identity Manager 用户存储*，即 CA Identity Manager 维护的用户存储。 这通常是包含公司需要管理的用户身份的现有存储。

  用户存储可以是 LDAP 目录或关系数据库。

  在管理控制台中，您可以创建 CA Identity Manager 目录对象，以便连接到用户存储，并且描述 CA Identity Manager 将维护的用户存储对象。

- *开通目录*，即开通服务器维护的用户存储。

  它是 CA Directory 的实例，包含全局用户，它将开通目录中的用户与关于 Microsoft Exchange、Active Directory 和 SAP 等端点的帐户关联在一起。

  只有某些 CA Identity Manager 用户有相应的全局用户。在 CA Identity Manager 用户收到开通角色时，开通服务器将创建全局用户。

独立的用户存储和开通目录

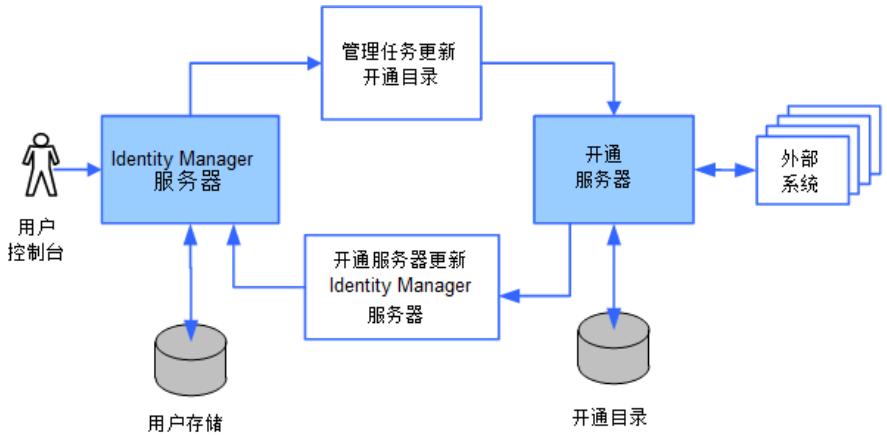
下图显示独立的用户存储和开通目录，这是 CA Identity Manager 全新安装所支持的方案。 在此图中：

- CA Identity Manager 管理员使用在用户存储中编辑用户的管理任务，会影响开通目录。

  此更改也可以更新拥有到开通服务器的连接器的端点（如电子邮件服务器）。

  由开通服务器（或拥有到开通服务器的连接器的端点）进行的更改会更新 CA Identity Manager 用户存储和开通目录。

例如，人力资源应用等端点可能更新用户的电子邮件地址。



数据库

要支持 CA Identity Manager 功能，需要一些信息，而 CA Identity Manager 使用数据源连接到存储这些信息的数据库。 这些数据库可以驻留在数据库的单个物理实例中或单独的实例中。

对象数据库（必需）

包含 CA Identity Manager 配置信息。

任务持久性数据库（必需）

持续维护 CA Identity Manager 活动及其关联事件的相关信息。即使您重新启动 CA Identity Manager 服务器，这也可以使系统准确跟踪 CA Identity Manager 活动。

存档数据库（必需）

来自任务持久性数据库的存档数据。

工作流数据库

存储的工作流流程定义、作业、脚本以及工作流引擎所需的其他数据。

审核数据库

为在 CA Identity Manager 环境中执行的操作提供历史记录。

注意：您可以配置 CA Identity Manager 在审核数据库中存储的信息的数量和类型。 有关详细信息，请参阅*《配置指南》*。

报告数据库

存储快照数据，这些数据反映获取快照时 CA Identity Manager 中对象当时的状态。 您可以通过此信息生成报告，以便查看对象（如用户和角色）之间的关系。

在您使用安装程序时，CA Identity Manager 配置与名为“CA Identity Manager 数据库”的单一数据库的连接，该数据库中包含每个数据库类型的表格。

注意：您可以在单独的数据库中为任务持久性、工作流、审核或报告创建数据存储，并且配置 CA Identity Manager 实现连接。 有关详细信息，请参阅*《安装指南》*。

连接器组件

连接器是端点的软件接口。 配给服务器使用连接器来与端点进行通信。 它将配给服务器操作在端点转换为更改，如“在 Microsoft Exchange 端点上创建新的电子邮件帐户”。

端点的例子包括 UNIX 工作站、Windows PC 或 Microsoft Exchange（针对电子邮件）等应用程序。

连接器服务器

连接器服务器是管理连接器的配给服务器组件。 可以将它安装在配给服务器系统或远程系统上。

一个连接器服务器与多个端点一起使用。 例如，如果有许多 UNIX 工作站端点，您可能有一个连接器服务器来处理管理 UNIX 帐户的所有连接器。 另一个连接器服务器可能处理请求 Windows 帐户的所有连接器。

分布式的连接器服务器可以与多个连接器服务器一起使用。 它在一个连接器服务器繁忙时提供负载平衡，在一个连接器服务器关闭时提供高可用性。

有两种类型的连接器服务器：

- CA IAM 连接器服务器 (CA IAM CS) 管理 Java 编写的连接器
- C++ 连接器服务器 (CCS) 管理 C++ 编写的连接器

C++ 连接器服务器

*C++ 连接器服务器*是管理 C++ 连接器的连接器服务器。 可以将它安装在配给服务器或远程系统上。 C++ 连接器服务器提供面对对象的应用程序框架，该框架可以简化负责 C++ 连接器服务器和端点之间的通信的连接器的开发。

CA IAM CS

CA IAM CS 是处理 Java 连接器的托管、路由和管理的服务器组件。CA IAM CS 向 C++ 连接器服务器提供 Java 替代方案。它在构造上和功能上类似于 C++ 连接器服务器，但是使用 Java API 而不是 C++ API，这使连接器可以在 Java 中实施。 此外，CA IAM CS 是数据驱动的而不是代码驱动的，这样就可以通过容器（或 CA IAM CS）而不是连接器本身实现更多功能。

配给服务器处理用户的配给，然后指派到连接器（使用 C++ 连接器服务器或 CA IAM CS），以管理端点帐户以及组。

连接器和代理

CA Identity Manager 连接器作为更宽的配给服务器体系结构的一部分运行，并且与您的环境中管理的系统进行通信。 连接器作为本地端点类型系统技术的网关。 例如，只有当在配给服务器可以与其通信的连接器服务器上安装了 ADS 连接器时，才能管理运行 Active Directory 服务 (ADS) 的计算机。 连接器管理驻留在这些系统上的对象。 管理对象包括帐户、组以及特定端点类型对象（可选）。

连接器安装在连接器服务器上，一些组件安装在配给服务器（例如服务器插件）或配给管理器上（用户界面插件）。

一些连接器需要在他们管理的系统上具有代理，以便完成通信周期，在这种情况下，可以使用配给安装程序安装这些连接器。 代理可以分成以下类别：

远程代理

安装在管理端点系统上

环境代理

安装在 CA ACF2、CA Top Secret 和 RACF 等系统上

某些组件在 UNIX 和 Windows 上运行，其中包括下列基于 C++ 连接器服务器的选项：

- UNIX（ETC、NIS）
- Access Control (ACC)

  注意：UNIX ACC 连接器只能管理 UNIX ACC 端点。 要管理 Windows ACC 端点则需要 Windows ACC 连接器，此连接器也可以管理 UNIX ACC 端点。
- CA-ACF2
- RACF
- CA-Top Secret

其他基于 C++ 连接器服务器的连接器可以通过 Solaris 配给服务器访问（依靠连接器服务器架构 (CSF)）。 CSF 允许 Solaris 的配给服务器与运行在 Windows 上的连接器通信。

注意：CSF 必须在 Windows 上运行才能使用这些连接器。

Connector Xpress

Connector Xpress 是一种 CA Identity Manager 实用工具，用于管理动态连接器、将动态连接器映射到端点以及建立端点的传递规则。 您可以使用它来配置动态连接器以便配给和管理 SQL 数据库和 LDAP 目录。

通过 Connector Xpress，即使没有创建由配给管理器管理的连接器所需的一般专业技术，您也可以创建和部署自定义连接器。

使用 Connector Xpress，您还可以设置、编辑和删除连接器服务器配置（Java 和 C++）。

对 Connector Xpress 的主输入是端点系统的本机架构。 例如，您可以使用 Connector Xpress 连接到 RDBMS 并检索数据库的 SQL 架构。 然后，可以使用 Connector Xpress 从本机架构中与身份管理和配给相关的部分构建映射。 映射说明了配给层如何表示本机架构的元素。

Connector Xpress 生成描述到动态连接器的到目标系统的运行时间映射的元数据。

Connector Xpress 的输出是完成映射时产生的元数据文档。 元数据是向 CA IAM CS 描述您的连接器结构的 XML 文件。

它描述配给服务器类和属性，以及将它们映射到本机架构的方式。

元数据用于在一个或多个配给服务器上创建动态端点类型。

注意：有关使用 Connector Xpress 的详细信息，请参阅 *CA Identity Manager 总目录*中的 *《Connector Xpress Guide》*。

其他组件

CA Identity Manager 包括一些其他组件，这些组件支持 CA Identity Manager 功能。 其中一些组件与 CA Identity Manager 一起安装，而另一些必须单独安装。

WorkPoint 工作流

在您安装 CA Identity Manager 时，会自动安装 WorkPoint 工作流引擎和 WorkPoint Designer。

通过这些组件，可以将 CA Identity Manager 任务放置在工作流控制下，并可以修改现有的工作流流程定义或创建新定义。

注意：有关工作流的详细信息，请参阅 *《管理指南》*。

配给管理器

CA Identity Manager 配给管理器通过图形界面管理配给服务器。 这用于管理“配给服务器”选项等管理任务。 在某些情况下，您可以使用配给管理器来管理您无法在 CA Identity Manager 用户控制台中管理的某些端点属性。

配给管理器是作为 CA Identity Manager 管理工具的一部分安装的。

注意：此应用程序只能在 Windows 系统上运行。

有关配给管理器的详细信息，请参阅 *《Provisioning Reference Guide》*。

报告服务器

CA Identity Manager 提供可以用来监控 CA Identity Manager 环境的状态的报告。 要使用随 CA Identity Manager 提供的报告，您应安装报告服务器（其包含在 CA Identity Manager 中）。

报告服务器使用 Business Objects Enterprise XI 的技术。 如果您已有 Business Objects 服务器，那么您无需使用报告服务器，也可生成 CA Identity Manager 报告。

注意：有关安装说明，请参阅 *《安装指南》*。

示例 CA Identity Manager 安装

有了 CA Identity Manager，您可以控制用户身份以及对端点系统的应用程序和帐户的访问。基于您需要的功能，选择要安装的 CA Identity Manager 组件。

在所有 CA Identity Manager 安装中，CA Identity Manager 服务器安装在应用程序服务器上。 您使用 CA Identity Manager 安装程序来安装您需要的其他组件。

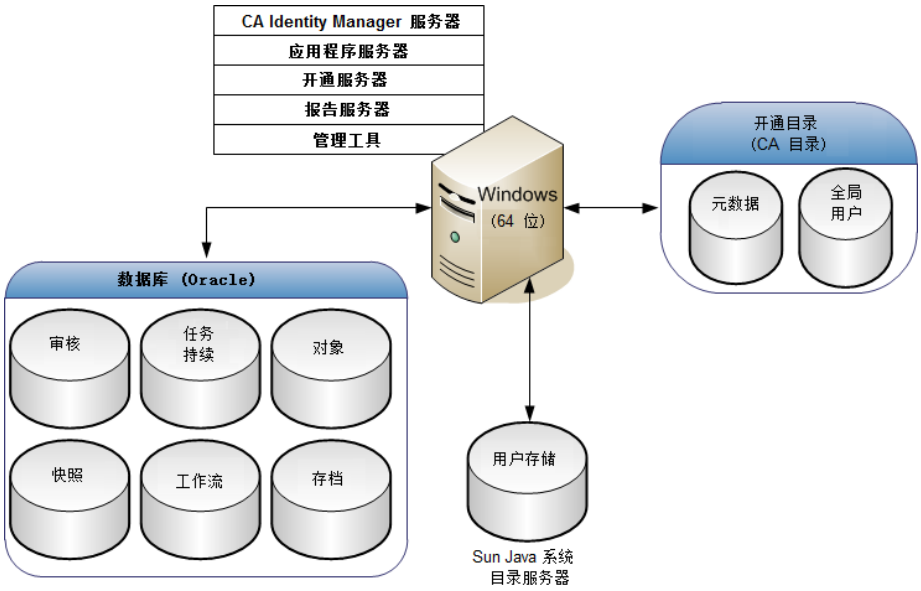
以下部分说明了 CA Identity Manager 高级实施的一些例子。

带有配给组件的安装

通过 CA Identity Manager 配给，您可以创建连接到配给服务器的环境，以便为各种端点系统配给帐户。 您可以将配给角色分配给您通过 CA Identity Manager 创建的用户。配给角色带有帐户模板的角色，这些模板定义用户可以在端点系统上接收的帐户。 帐户为用户提供对其他资源（如电子邮件帐户）的访问权限。

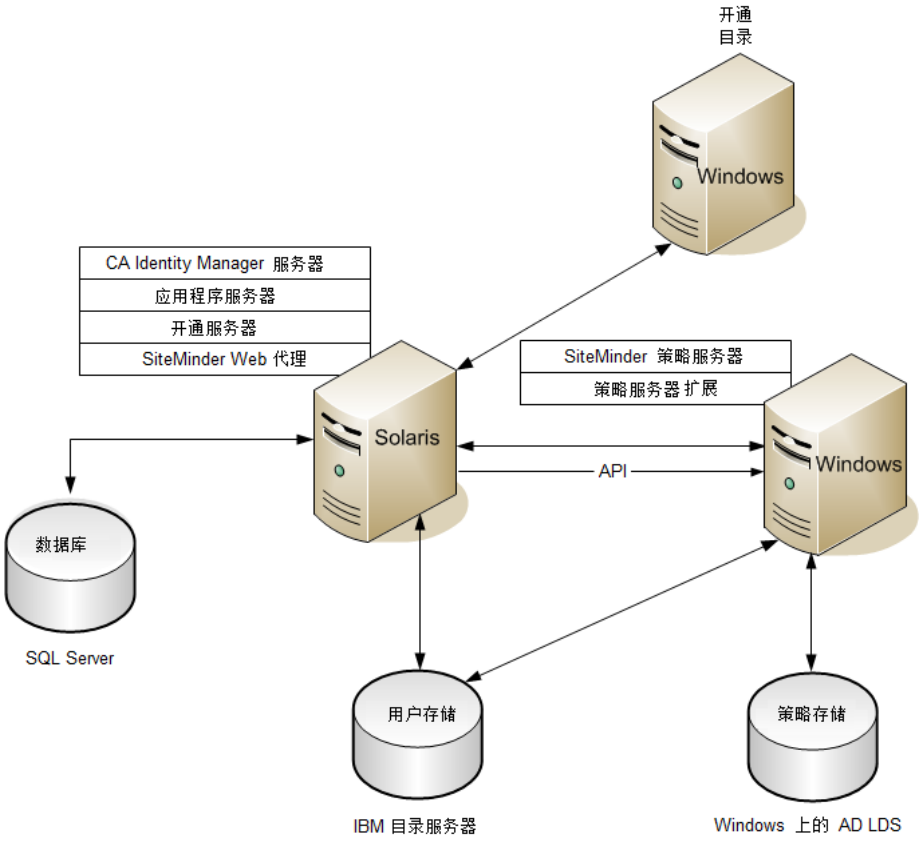
当您将配给角色分配给用户时，该用户就会接收角色中的帐户模板定义的帐户。帐户模板还定义了用户属性如何映射到帐户。在由帐户模板定义的管理端点中创建帐户。

下图是具有配给的 CA Identity Manager 安装的示例：



带有 SiteMinder 策略服务器的安装

SiteMinder 策略服务器为您的 CA Identity Manager 环境提供高级身份验证和保护。 下图是具有 SiteMinder 策略服务器的 CA Identity Manager 安装的示例：



包括 SiteMinder 的 CA Identity Manager 实施包含基本安装或带有配给的安装的所有组件，以及以下其他组件：

SiteMinder Web 代理

与 SiteMinder 策略服务器一起使用以保护用户控制台。 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以及密码服务和单一登录等其他功能。

SiteMinder 策略服务器的扩展名

使 SiteMinder 策略服务器能够支持 CA Identity Manager。 在您的 CA Identity Manager 实施中的每个 SiteMinder 策略服务器系统上安装这些扩展。

SiteMinder 策略存储

存储 SiteMinder 用来管理 Web 资源访问的信息。

在 CA Identity Manager 与 SiteMinder 集成时，策略存储还包括 CA Identity Manager 目录和环境的有关信息，以便 SiteMinder 可以提供高级身份验证。

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。

第 4 章： 规划实施

要策划 CA Identity Manager 实施，您需要确定 CA Identity Manager 管理用户的方式以及实现业务目标所需的功能。 要考虑的一些问题是：

- 我怎样管理用户？
- 我需要帐户配给吗？
- 我的自定义业务需求是什么，我应当使用工作流实施这些需求吗？

基于您作出的决定，您可以确定为环境实施 CA Identity Manager 的最好的方法。

此部分包含以下主题：

确定要管理的对象

确定要管理的内容会帮助您确定所需要安装的组件。 使用 CA Identity Manager，可以管理以下内容：

- 用户身份
- 对端点系统帐户的访问

用户身份

用户身份表示公司需要管理的人员，如员工、承包商、供应商以及其他人员。

要管理用户身份，您只需要安装 CA Identity Manager 服务器和管理工具。

如何配置用户管理支持

在 CA Identity Manager 中，您管理具有管理角色的用户，这可以确定管理员可以执行的 CA Identity Manager 任务。

注意：在 CA Identity Manager 中实施用户管理之前，您应当确定您需要的功能，并且制定分阶段实施该功能的计划 (p. 50)。

要配置用户管理支持，您需要完成以下高级步骤：

1. 安装 CA Identity Manager 服务器和管理工具。

   如果需要为管理用户配给帐户，您也需要安装对配给 (p. 39)的支持。

   注意：有关说明，请参阅 *《安装指南》*。

2. 在 CA Identity Manager 管理控制台中创建以下内容：

   - **CA Identity Manager 目录**

     描述一个与 CA Identity Manager 关联的用户存储。 总目录包括以下内容：

     - 用户存储的指针，存储了用户、组和组织等管理对象。
     - 描述如何在该目录中存储管理对象以及在 CA Identity Manager 中表示这些对象的元数据。

   - **CA Identity Manager 环境**

     提供管理命名空间，这些命名空间允许 CA Identity Manager 管理员通过一组关联的角色和任务管理用户、组和组织等对象。 CA Identity Manager 环境可以控制目录的管理和图形表示。

   有关 CA Identity Manager 目录和环境的详细信息，请参阅 *《配置指南》*。

3. 修改默认管理角色和任务以适合您的业务需求。

   典型角色修改包括在现有的管理角色添加或删除默认任务，或基于默认角色创建新管理角色。

   典型任务修改包括自定义默认用户配置文件选项卡，从而仅在选项卡中包含需要管理的信息。 （默认用户配置文件选项卡包括为用户定义的所有属性。）

   有关修改默认管理角色和任务的信息，请参阅 *《User Console Design Guide》*。

4. 将管理角色分配给将执行用户管理任务的用户。

通过其他应用程序配给帐户

是否实施配给取决于您需要管理的信息的类型。 如果您正在管理重要用户目录，而不想管理其他系统的用户帐户，就不需要配给。 如果想管理各种系统上的用户帐户，那么您应当实施配给支持。

通过与 CA Identity Manager 集成的配给服务器提供配给功能。 配给服务器为帐户配给提供以下功能：

- 端点管理
- 帐户同步
- 帐户模板
- 浏览和关联功能

注意：配给信息存储在配给目录中。 如果 CA Identity Manager 在其他类型的目录中保留用户，您的部署需要包括一个 CA Identity Manager 用户存储和一个配给目录。

端点管理

要配给帐户，需要在 CA Identity Manager 用户控制台中定义和管理端点。*端点*是用户需要访问的系统。端点的示例包括 Oracle 数据库、UNIX NIS 服务器、Windows 服务器以及 Microsoft Exchange 服务器。 使用*帐户模板* (p. 40)来创建帐户，并在管理端点中确定用户权限。

注意：您也能使用配给管理器来定义和管理端点。 虽然我们建议为大多数端点管理任务使用用户控制台，但是仍然有需要配给管理器的一些任务，如管理某些端点属性以及管理除帐户之外的端点对象。 有关配给管理器的详细信息，请参阅*"配给参考"*。

帐户同步

您可以在多个管理端点之间同步用户帐户。 如果启用帐户同步，在配给服务器中对用户配置文件所做的更改将会传播到该用户具有帐户的所有端点。

注意：您在 CA Identity Manager 任务的"配置文件"选项卡上指定帐户同步设置。 有关配置帐户同步的详细信息，请参阅*《管理指南》*。

帐户模板

帐户模板定义如何在管理端点中表示用户。 例如，Exchange 帐户的模板可以定义用户电子邮件地址的格式，如 <first initial><last name>@mycompany.com。

帐户模板还可以确定用户在管理系统中的权限。 例如，除定义电子邮件地址的格式之外，Exchange 帐户的模板也可以限制用户的邮箱大小。

您可以在用户控制台中创建和管理帐户模板。

浏览和关联功能

“浏览”和“关联”功能通过在管理系统中查找更改并进行同步来简化端点管理。

“浏览”功能在端点中查找对象（包括帐户），并且在配给目录中存储对他们的引用。您可以使用“浏览”功能来检测要管理的任何新对象。例如，如果您在 LDAP 目录中配给帐户，而新组织被添加到该目录，您可以使用“浏览”功能来引入这些新组织，以用于帐户模板。

“关联”功能将管理端点的帐户与配给目录的全局用户关联在一起。 在通过端点对帐户进行更改时，“关联”功能可以使这些更改与全局用户帐户同步。

注意：有关浏览和关联功能的详细信息，请参阅 *《管理指南》*。

如何配置对配给的支持

在决定实施配给之后，完成以下高级步骤。

1. 使用 CA Identity Manager 服务器安装程序来安装 CA Identity Manager 服务器、配给服务器、Provisioning Directory Initialization 以及管理工具。

   注意：有关安装 CA Identity Manager 组件的详细信息，请参阅 *《安装指南》*。

2. 配置配给管理器以连接到 CA Identity Manager 服务器。

3. 在 CA Identity Manager 管理控制台中配置配给：

   a. 启用配给。

   b. 完成以下内容，为配给配置环境：

      - 导入自定义角色定义
      - 配置入站管理员
      - 将环境连接到配给服务器。

   注意：有关详细信息，请参阅 *《配置指南》*。

4. 在用户控制台中创建端点。

   这允许 CA Identity Manager 管理端点。

   注意：有关端点管理的详细信息，请参阅 *《管理指南》*。

5. 浏览和关联端点。

   在浏览端点时，CA Identity Manager 查找端点中的对象并将其实例存储在配给目录中。 此操作将在端点中找到的帐户和其他对象填入配给目录。

   在关联某一端点上的帐户时，CA Identity Manager 会将这些帐户与配给目录中的全局用户进行关联。 您可以选择关联功能是否创建不存在的任何全局用户，以及是否将没有匹配的全局用户的帐户与 [default user] 全局用户关联。

6. 通过使用包含用于创建帐户的属性的帐户模板，创建并维护端点帐户。

7. 将帐户模板与配给角色关联在一起。

   在您将配给角色分配给用户时，CA Identity Manager 在关联端点中为这些用户创建帐户。

   注意：有关帐户模板和配给角色的详细信息，请参阅 *《管理指南》*。

确定审核需求

CA Identity Manager 包括允许您监控 CA Identity Manager 环境中的活动的审核功能。

此信息存储在审核数据库中。 存储在审核数据库中的信息的数量和类型是可配置的。

您通过名为“查看提交的任务”的任务查看用户控制台的审核数据。 通过此任务，管理员可以搜索并查看在系统中发生的任务。 管理员可以查看高级任务信息或查看任务和事件详细信息。

CA Identity Manager 审核注意事项

审核数据为在 CA Identity Manager 环境中执行的操作提供了历史记录。要在 CA Identity Manager 中审核数据，您需要以下内容：

- 审核数据库
- 审核设置文件

审核数据库

在您使用 CA Identity Manager 安装程序时，CA Identity Manager 配置与名为“CA Identity Manager 数据库”的单一数据库的连接，并且创建要连接到要审核的数据库表的数据源。

注意：CA Identity Manager 数据库也包括其他 CA Identity Manager 功能使用的数据，这些功能包括任务持久性、工作流和报告。 为了实现可扩展性目的，您可以创建单独的新数据库实例以供审核。

注意：有关审核数据库的详细信息，请参阅 *《安装指南》*。

审核设置

您在审核设置文件中配置审核设置。 审核设置文件确定 CA Identity Manager 审核的信息的数量和类型。 您可以配置审核设置文件，以完成以下操作：

- 为 CA Identity Manager 环境启用审核。
- 为管理任务生成的部分或全部的 CA Identity Manager 事件启用审核。
- 记录特定状态（例如在事件完成或取消时）的事件信息。
- 记录与某一事件有关的属性的信息。 例如，您可以记录在 ModifyUserEvent 事件期间更改的属性。
- 设置属性日志的审核级别。

注意：有关配置审核的详细信息，请参阅 *《配置指南》*。

CA Audit 注意事项

CA Audit 是审核管理系统，它使您能够收集并存储与安全相关的数据，以进行审核、报告、遵从性验证和事件监控。

要与 CA Audit 集成，需要在安装 CA Identity Manager 服务器时安装 iRecorder 组件。 iRecorder 从 CA Identity Manager 检索事件。 基于 CA Audit 策略管理器中的策略，iRecorder 会忽略事件或将它发送到 CA Audit。

确定用户存储需求

CA Identity Manager 实施必须包括包含 CA Identity Manager 维护的用户身份的用户存储。 通常，这是企业用来存储其用户（如员工和客户）相关信息的现有用户存储。

如果您的实施包括配给，CA Identity Manager 也需要包括全局用户的配给目录，这些用户与 Microsoft Exchange、Active Directory 和 Oracle 等端点的帐户关联。

管理多个用户存储

企业可能需要维护多个用户存储。 在每个用户存储中，用户身份允许对不同的公司资源的访问。 您可以使用下列方法之一管理多个用户存储：

- 使用 CA Identity Manager 直接管理配给目录，使用配给服务器间接管理不同的用户存储的用户和帐户。

  此方法允许您：

  - 从一个位置集中管理能够分配到各种企业资源的用户
  - 实施整个企业资源的共同安全和业务规则。 这可能包括以下内容：
    - 基于角色的访问控制
    - 指派管理
    - 基于任务和屏幕管理的企业身份类型，对任务和屏幕进行自定义
    - 基于规则的身份管理的身份策略
    - 自定义和扩展性

  注意：有关这些功能的详细信息，请参阅*《管理指南》*。

- 创建单独的 CA Identity Manager 环境以管理每个用户存储

  如果使用此方式，信息不在环境间共享。

选择要安装的组件

下表列出支持想要实施的功能所需安装的组件。

注意：有关安装这些组件的说明，请参阅*《安装指南》*。

如果需要：	安装这些组件
管理现有的企业用户存储中的用户身份	■ CA Identity Manager 服务器
端点系统的配给帐户	■ 配给服务器 ■ “Provisioning Directory”（配给目录） ■ 配给管理器 ■ 连接器 ■ 连接器服务器 **注意**：有关安装连接器的说明，请参阅*《连接器指南》*来了解要安装的连接器类型。
实施以下功能中的一个或多个： ■ 高级身份验证 ■ 高级密码策略 ■ 不同用户集的不同控制台面板 ■ 为用户配置区域设置首选项	■ SiteMinder 策略服务器 ■ 策略存储 ■ SiteMinder Web 代理 ■ 策略服务器的 CA Identity Manager 扩展 **注意**：有关安装 SiteMinder 策略服务器和策略存储的说明，请参阅*《CA SiteMinder Web Access Manager Policy Server Installation Guide》*。有关安装 Web 代理的说明，请参阅*《CA SiteMinder Web Access Manager Web Agent Installation Guide》*。
生成关于 CA Identity Manager 活动的报告	报告服务器

决定硬件要求

CA Identity Manager 安装的硬件需求取决于想要实施的功能和部署的规模。

以下部分描述典型 CA Identity Manager 实施和所需硬件。

部署类型

在规划 CA Identity Manager 部署所需的硬件时，考虑想要实施的功能和部署的初始规模。 使用以下类别之一来估算部署的规模。

注意：您选择的部署类型决定了配给目录使用的 DxGrid 文件的大小。 在您安装 CA Identity Manager 服务器时指定部署类型。

演示

用于演示或开发环境基本测试的单个服务器部署。 演示部署支持多达 1 万个配给帐户。

注意：此实施类型不支持生产实施。

基本

适合于大多数中小规模实施的高可用性实施。 基本实施支持多达 40 万个配给的帐户。

这种实施需要两个服务器来运行 CA Identity Manager 应用程序及其组件，两个服务器运行 CA Identity Manager 数据库和用户存储。

中等规模

适合于中等规模实施的高可用性实施。 中等规模部署支持多达 60 万个配给的帐户。

大型企业

包括附加服务器群集以处理更多用户和事务的高可用性实施。 大规模部署支持超过 60 万个配给的帐户。

注意：有关高可用性实施的详细信息，请参阅 *《安装指南》*。

配给的其他要求

除基本 CA Identity Manager 实施所需要的组件之外，如果 CA Identity Manager 包括配给，则需要下列其他组件：

- 配给服务器

  可以与 CA Identity Manager 服务器安装在同一台计算机上。

- Provisioning Directory Initialization

  重要说明！ Provisioning Directory Initialization 必须被安装在 CA Directory 上。

- 配给管理器

  可以安装在可以访问配给服务器的任何 Windows 计算机上。

注意：在开发环境中，可以将这些组件安装在同时包括基本安装组件的一台计算机上。

SiteMinder 集成的其他要求

如果 CA Identity Manager 与 SiteMinder 集成，实施必须包括基础 CA Identity Manager 安装的组件以及下列其他组件：

- **策略服务器**

  提供策略管理、身份验证、授权以及帐户服务。

  如果策略服务器专门用于 CA Identity Manager，可以将策略服务器安装在与 CA Identity Manager 服务器相同的计算机上。如果策略服务器需要保护其他应用程序，我们建议将它安装在单独的计算机上，以确保最佳性能。

- **策略存储**

  包含所有策略服务器数据。您可以在支持的 LDAP 或关系数据库中配置策略存储。 在高可用性实施中，我们建议在单独的服务器上安装策略存储。

- **策略服务器的扩展**

  使 SiteMinder 策略服务器能够支持 CA Identity Manager。 在您的 CA Identity Manager 实施中的每个 SiteMinder 策略服务器系统上安装这些扩展。

- **SiteMinder Web 代理**

  与 SiteMinder 策略服务器一起使用以保护用户控制台。 安装在带有 CA Identity Manager 服务器的系统上。

选择导入用户的方式

如果您需要将用户导入现有的用户存储，您选择的方式取决于您的业务需求。

以下部分说明导入用户的选项。

如何将用户导入新用户存储

在决定如何存储用户数据之后，您可能需要将用户从一个存储导入另一个存储。 取决于您的实施，可以使用不同方式来导入用户。

注意：在将用户导入新的用户存储之后，您可以使用身份策略 (p. 48)来将更改应用于导入的用户。

通过 CA Identity Manager 导入用户

CA Identity Manager 提供以下方式，用于将用户添加到它直接管理的用户存储中。

方法	功能	限制
批量加载程序	允许您在用户控制台中使用批量加载程序任务来上传 Feeder 文件，这些文件用于同时管理大量管理对象。 批量加载程序方法的优点是：可以使用信息 (Feeder) 文件，实现大量管理对象处理流程的自动化。 还可将“批加载程序”任务映射至工作流流程。	如果使用批量加载程序，取决于正在导入的用户人数，您可能看到内存不足例外。 要解决此问题，请增加 JVM 内存设置。
通过任务执行 Web 服务 (TEWS) 的远程任务调用	允许执行任何为 Web 服务启用的 CA Identity Manager 任务，包括创建用户任务。 如果为用户同步配置了此任务，CA Identity Manager 将执行任何适用的身份策略。	Web 服务模型的性能特征可能不适合批量导入操作的高传送量需求
IM API	■ 提供基于用户的、能够通过 Java 客户端调用用于创建用户的 API ■ 提供最高传送量能力。	■ 跳过任务服务器提供的审核和安全机制。 ■ 不支持执行身份策略。

注意：有关批量加载程序的详细信息，请参阅*《管理指南》*。有关 TEWS 和 IM API 的详细信息，请参阅*《Programming Guide for Java》*。

对导入的用户执行身份策略

*身份策略*是指在用户符合某一条件或规则时，所发生的一组业务更改。这些更改可以包括分配或吊销角色（包括配给目录中的用户的配给角色）、分配或吊销组成员资格以及更新用户配置文件中的属性。

在将用户帐户导入新的用户存储之后，您可以使用身份策略将更改应用于用户帐户。

本部分描述通过一步或两步为导入的用户执行身份策略的方式。

一步方式

您可以使用下列导入方法一步为导入到新的用户存储里的用户执行身份策略：

- 用户控制台的批量加载程序
- 通过 TEWS 创建用户任务执行
- 入站同步

两步方式

如果使用两步方式，您首先导入用户，然后为这些用户执行身份策略。在 CA Identity Manager 管理配给服务器中的用户时，您可以使用此方法。根据您的导入要求，此方法可以提供更多的灵活性。

1. 使用导入工具之一将用户添加到配给目录。
2. 通过 TEWS 为每个导入的用户调用 CA Identity Manager 同步用户任务。

通过配给服务器导入用户

配给服务器包括在配给目录中增加和管理用户的批量导入选项。 下表说明将用户导入配给目录的方式。

方法	功能	限制
批处理实用工具 (etautil)	一个命令行界面工具，允许您在配给目录中管理对象	■ 目前仅支持 Windows 系统

方法	功能	限制
浏览和关联	■ 在已知的端点（包括用户）中查找配给服务器可以管理的新对象 ■ 为存在于端点和配给服务器的对象实例提供关联功能。 浏览和关联功能中存在附加信息。	■ 默认情况下，当前支持的连接器可以使用浏览和关联功能。可以使用自定义连接器进行扩展 ■ 当处理大规模用户群体时，“关联”选项可能会影响可扩展性。 如果您选择此导入选项，确保评估性能和扩展性影响。

使全局用户与 CA Identity Manager 用户存储同步

在将用户导入配给服务器之后，您可以使用以下方法将这些用户添加到 CA Identity Manager 用户存储：

- **入站同步**

  入站同步使 CA Identity Manager 用户与在配给目录中发生的更改一起更新。 配给目录中的更改包括使用配给管理器或带有连接到配给服务器的连接器的系统生成的更改。

  在使用入站同步导入用户时注意以下内容：

  - 在 CA Identity Manager 管理控制台中，您可以自定义如何将来自入站请求的属性映射到 CA Identity Manager 任务的属性。

    注意：有关详细信息，请参阅 *《管理指南》*。

  - 考虑哪些配给服务器更改需要与公司用户存储同步。同步大量更改可能影响性能和可扩展性。

- **配给角色和帐户模板**

  配给服务器可以使用配给角色和**帐户模板**管理 CA Identity Manager 用户存储中的帐户。这要求已经获取指向 CA Identity Manager 用户存储的管理端点，且存在适用的帐户模板和角色。 在这种情况下，对于通过通过配给服务器导入用户中说明的选项之一创建的全局用户，可以为他们分配在 CA Identity Manager 用户存储中初建该用户帐户的配给角色。

制定部署计划

在规划大规模实施时，您应当分阶段部署 CA Identity Manager 功能。 使用下列部署顺序，您可以快速通过 CA Identity Manager 受益，可以随着时间的推移评估改变实施的需要，并且可以谨慎构建环境，以获得最佳性能和可扩展性：

- 自助服务和密码管理
- 身份策略
- 工作流批准
- 用户、组和组织对象的指派管理
- 角色管理的指派管理

在每个部署阶段之后，确保评估性能并且进行调整，然后再进入下一个阶段。 优化 CA Identity Manager (p. 57) 提供有关性能、调整和可扩展性的信息。

部署自助服务和密码管理

在部署其他 CA Identity Manager 功能之前先部署自助服务任务和密码管理，原因如下：

- 自助服务任务和密码管理容易部署，可以使您迅速大幅度受益。
- 这些特点不依赖指派管理模型，并且可以根据需要重新配置以解决变化的业务需求。
- 这些功能通常生成由 CA Identity Manager 定期处理的大量任务。 因此，在您部署其他功能之前，它们可以测试实施的可扩展性。

要部署自助服务任务，您需要完成下列步骤：

1. 配置自行注册任务

   这是公共任务，在安装期间默认启用此任务。 要配置此任务，根据需要从默认自行注册任务添加或删除字段。

2. 部署自行管理者角色。

   应当将此角色的成员规则配置为适用于所有用户，或应当包括自动将该角色分配给新用户的成员规则。 例如，您可以创建将自行管理者角色分配给所有全职员工的成员规则。 在用户自行注册时，CA Identity Manager 可以将员工类型设置为全职（使用逻辑属性处理程序或业务任务处理程序）。 如果用户满足成员规则中的条件，会自动接收自行管理者角色。

注意：当您为自行管理者角色配置成员规则时，不允许管理员添加或删除角色成员。 自动分配角色之后，就不需要管理员明确分配角色。

要部署密码管理功能，请完成下列步骤：

1. 配置公共密码管理任务，如忘记密码任务。
2. 创建确定密码创建方式及到期时间的密码策略。
3. 部署密码管理者角色，该角色可以使角色成员重置用户密码。

注意：有关角色、任务和密码管理的信息，请参阅*《管理指南》*。

部署身份策略

身份策略是指在用户符合某一条件或规则时所发生的一组业务更改。 在部署完整授权模型之前，您可以使用身份策略来提供业务驱动的权利。 例如，您可以创建分配销售经理配给角色的身份策略，该角色将销售应用程序的访问权限授予职称是销售经理的所有用户。 如果销售代表升职成为销售经理，他自动获得对工作所需的所有系统的访问权限，而无需等待管理员参与。

要部署身份策略，请完成下列步骤：

1. 配置身份策略，这些身份策略由对用户配置文件属性所做的更改触发。
2. 配置用户管理者角色，以便允许少量管理员使用用户任务（如创建用户和修改用户）来更改触发身份策略的属性。

   确保配置用户管理者成员策略的作用域规则，以确定角色成员可以管理的用户集。

在部署身份策略时注意以下内容：

- 考虑最初创建授予*不需要*工作流批准的权限的身份策略。 这样，您就可以部署身份策略，而无需定义工作流流程、批准表单和批准人模型。
- 在创建身份策略之前，您应当熟悉在 CA Identity Manager 中实施业务规则的其他方法（如数据验证规则、逻辑属性、业务逻辑任务处理程序以及工作流流程），以确定哪种方法可以提供最佳解决方案。

  注意：有关这些方法的详细信息，请参阅*《管理指南》*和*《Programming Guide for Java》*。
- 身份策略是在 CA Identity Manager 中分配权利的有效方法，但是这些策略可能显著影响性能 (p. 72)。
- 如果初始部署用户任务，考虑删除或隐藏管理与身份策略相同的权利的关系选项卡（如“角色”选项卡）。 这防止出现未被授权的权利的风险，并且防止不适当构建的角色对性能的可能影响。

注意：有关身份策略的详细信息，请参阅*《管理指南》*。

部署工作流批准

工作流批准可以将其他级别的安全和自动化添加到您的 CA Identity Manager 实施中。

部署工作流批准需要以下任务：

1. 决定哪些事件或任务需要批准。
2. 为每个工作流流程定义批准人集，称为参与人。

   注意：所有参与人由参与人确定程序动态确定。 要维持良好性能，请将参与人限制为三十名用户。
3. 配置批准表单。
4. 在需要时，定义自定义工作流流程。

环境和任务级别工作流批准

CA Identity Manager 支持两种类型的批准：环境级别批准和任务级别批准。 环境级别批准是针对全部事件的实例定义的，与它们所关联的任务无关。 任务级别批准是针对与特定任务关联的特定事件定义的。 任务级别批准优先于环境级别批准。

大多数批准是在环境级别定义的，以确保同一事件出现相同的工作流活动，而与它所关联的任务无关。 不过，在下列情况中，考虑实施任务级别工作流：

- 您有专门的任务，来执行生成事件（无需批准）的特定业务更改。
- 您有由身份策略触发的更改操作，来生成无需工作流批准的事件。
- 您需要相应灵活性，将特定工作流流程与针对任务的更改关联在一起。

随着事务量增加，环境级别批准可能需要大量处理和系统资源。 这最后可能导致性能和可扩展性问题。 在适当的时候，使用任务级别批准可以减少或消除这些问题。

部署用户、组和组织的指派管理

指派管理是通过使不同 CA Identity Manager 用户执行修改、分配和使用角色的功能来对用户和他们的权利进行管理。

注意：必须精心构造授权模型，以确保您的 CA Identity Manager 实施具有良好性能和可扩展性。

作用域规则强制实施授权，这些规则是在管理角色的成员和管理策略中定义的。 作用域规则确定角色成员可以使用角色的对象。 例如，作用域规则可以使用户管理者能够管理它的部门的用户，但是不能管理其他部门的用户。

通常，作用域规则应当反映用户存储的逻辑结构。例如，在分等级的 LDAP 用户存储中，作用域可能是由组织定义的。 在关系数据库中，作用域可能是使用部门 ID 等属性定义的。

在对用户、组和组织部署指派管理时，注意以下内容：

- 限制与用户相关的任务的关系选项卡（如“管理角色”和“配给角色”选项卡）的访问。 这些关系选项卡包含在默认用户任务（如创建用户和修改用户）中。 考虑从默认任务中删除它们，仅在与少量管理角色关联的特定任务中使用它们。
- CA Identity Manager 动态评估每个作用域规则；不将作用域信息存入缓存。 考虑创建包含简单目录查询的作用域规则，以确保良好性能。
- 通过确定 CA Identity Manager 需要多长时间才能返回管理员可以管理的对象，从而评估作用域规则的性能。

部署角色的指派管理

角色的指派管理在 CA Identity Manager 中进行最重要的授权，并对性能产生最大影响 (p. 58)。 因为这些原因，您应当考虑在已经部署所有其他功能之后部署角色指派管理。

在为角色部署指派管理时，注意以下几点：

- 限制管理角色、管理角色成员和管理角色管理员的数目，以保护环境并确保良好性能。
- 一旦您为角色部署指派管理，实施性能和可扩展性测试。 根据需要优化环境。

第 5 章： 与 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：

带有 SiteMinder 策略服务器的安装 (p. 35)

SiteMinder 身份验证

CA Identity Manager 包括以下应当被保护的控制台：

用户控制台

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

管理控制台

使 CA Identity Manager 管理员能够创建和配置 CA Identity Manager 目录、配给目录和 CA Identity Manager 环境。

CA Identity Manager 包括本地身份验证，此验证在默认情况下保护用户控制台。 在默认情况下不会保护管理控制台，但是您可以通过配置 CA Identity Manager 保护它。 CA SiteMinder 也能用于保护管理控制台。

要为用户控制台配置其他类型的身份验证（如证书或密钥身份验证），CA Identity Manager 必须与 SiteMinder 集成。

注意：有关详细信息，请参阅 *《配置指南》*。

第 6 章： 优化 CA Identity Manager

此部分包含以下主题：

CA Identity Manager 性能

CA Identity Manager 性能取决于不同功能和组件的单个性能。

您可以在 CA Identity Manager 环境中优化以下功能：

- 角色
- 任务
- 组成员资格和管理
- 身份策略

要获得更高性能，您还可以调整以下组件：

- 用户存储
- 配给组件
- 运行时间组件，包括数据库（如任务持久性数据库），以及应用程序服务器设置

要确保最佳性能，请使用以下部分中的准则配置 CA Identity Manager 功能。 然后，根据需要衡量性能并调整组件。 因为组件一起工作，可能需要多次重复，才能为环境找到最佳调整设置。

角色优化

CA Identity Manager 包括三种类型的角色：

- 管理角色

  确定用户在用户控制台中拥有的权限。

  在用户登录 CA Identity Manager 环境时，用户帐户有一个或多个管理角色。每个管理角色包含用户可以在该 CA Identity Manager 环境中完成的任务（如创建用户）。 用户具有的管理角色决定用户控制台的显示，因此用户只能看见与他们的角色关联的任务。

- 配给角色

  在管理端点（如电子邮件系统）中提供用户帐户。

- 访问角色

  提供在 CA Identity Manager 中提供权利的其他方式。

角色包括确定以下内容的策略：

- 谁可以使用角色（仅针对管理员和访问角色）以及他们可以使用角色的位置
- 谁可以管理角色成员和管理员
- 谁可以修改角色定义

评估角色以及他们的关联权限可能对 CA Identity Manager 的性能造成很大影响。

角色评估影响登录性能的方式

在 CA Identity Manager 用户尝试登录用户控制台时，将发生下列操作：

1. CA Identity Manager 提示用户提供凭据，如用户名和密码。
2. 使用下列方式之一验证用户凭据：
   - CA Identity Manager 本地身份验证
   - SiteMinder 身份验证，前提条件是 CA Identity Manager 实施包括 SiteMinder

3. CA Identity Manager 评价环境中的每个管理角色的每个成员策略，以确定哪些管理角色适用于该用户。

   注意：此评估对于给定的用户只发生一次。 在初始评估之后，CA Identity Manager 缓存结果。 CA Identity Manager 会一直使用缓存的信息，直到用户或成员策略集发生更改，这样会导致 CA Identity Manager 刷新缓存中的信息。

4. CA Identity Manager 用户控制台显示用户基于他的角色可以查看的类别。

对于登录用户控制台的每个用户都会发生此过程。 如果 CA Identity Manager 环境包含大量角色或无效成员策略，角色成员资格评估可以显著影响性能。 在这种情况下，用户登录用户控制台时看到的初始屏幕显示会很缓慢。

注意：在用户访问公共任务进行自行注册或请求忘记的密码时，CA Identity Manager 不需要评估成员策略。 在这些情况中，因为 CA Identity Manager 不显示完全的用户控制台，所以不需要用户的角色列表。

角色对象和性能

为了支持每个角色，CA Identity Manager 根据角色配置在 CA Identity Manager 对象存储 (p. 29)中创建大量对象。

CA Identity Manager 为每个角色创建一个基础对象。 除基础对象之外，CA Identity Manager 针对每个策略创建一个对象。

大量角色对象可能影响对象存储进行搜索和策略评估的性能。

对象存储性能

CA Identity Manager 在对象存储中存储管理用户和授权所需的信息。 在对象存储中有大量角色对象可能导致以下问题：

- 搜索 CA Identity Manager 任务屏幕上的管理对象可能花费更长时间。

  要减少对搜索的影响，为用于搜索的属性编制索引 (p. 76)。
- 角色管理任务可能执行缓慢。

  受到大型对象存储影响的角色管理任务的一些例子如下所示：

  - 因为 CA Identity Manager 必须确认角色名称在对象存储中是唯一的，因此创建管理角色任务非常缓慢。
  - 删除管理角色任务必须删除为支持此角色创建的所有对象，必须更新对象缓存。
- CA Identity Manager 花费很长时间来评估角色策略。

为改善性能，CA Identity Manager 将对象存储的信息存入缓存。

优化角色策略评估

对于每个管理角色，您可以创建三种类型的策略：

- 成员策略

  定义用于确定接收角色的用户的成员规则，以及用于确定角色成员可以管理的对象的作用域规则。
- 管理策略

  为角色定义管理规则、作用域规则和管理员权限。
- 所有者策略

  定义可以修改角色的人

要优化 CA Identity Manager 评价角色策略时的性能，请考虑以下内容：

- 限制 CA Identity Manager 环境中管理角色的数目。
- 遵循创建策略规则的准则 (p. 61)。
- 调整用户存储。
- 如果 CA Identity Manager 包括 SiteMinder，调整策略存储。

策略规则创建准则

确定角色策略评估的整体性能的关键因素之一是评估任何一个策略规则所需的时间。 要改善策略规则评估时间，请在您创建策略时，注意以下方面：

- 如果可能，通过使用复杂表达式创建策略规则，限制 CA Identity Manager 创建的策略对象的数目以及它执行的用户存储搜索的数目。

  使用复杂表达式的单个规则与使用简单表达式的多个规则相比更为有效。

- 如果可能，选择最有效率和可缩放的策略规则类型。
- 启用策略规则的内存中评估选项。

  内存中的评估选项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，从而大大减少策略评估的时间。 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。

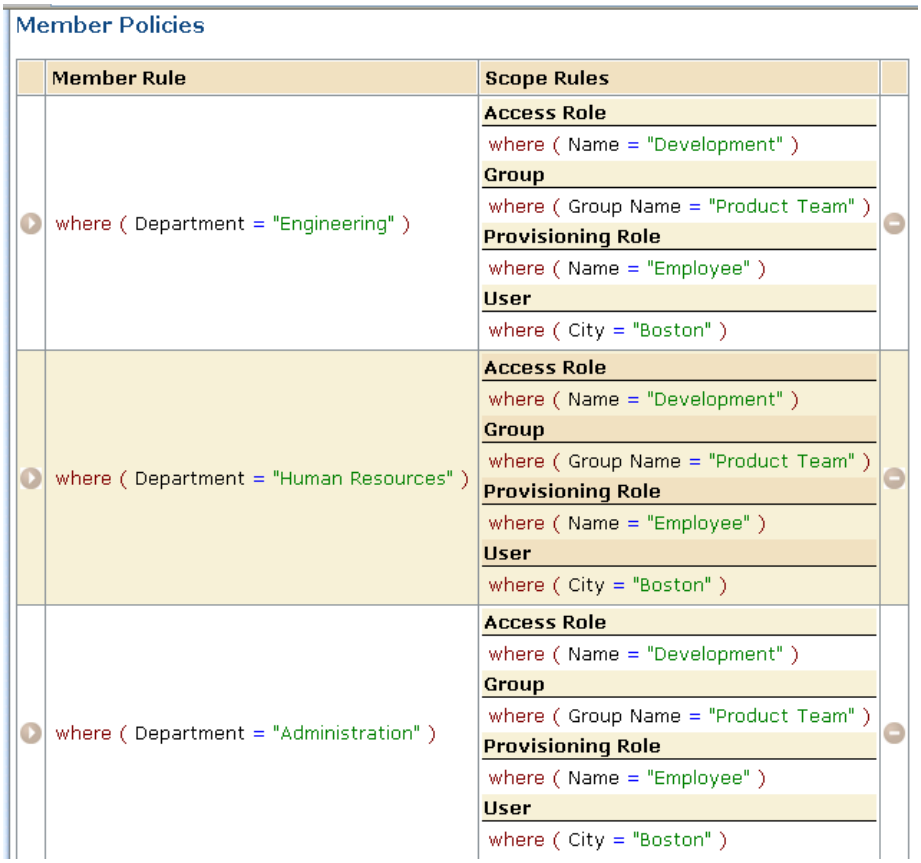
  注意：有关内存中评估选项的详细信息，请参阅*《配置指南》*。

- 调整用户存储。
- 如果您的 CA Identity Manager 实施包括 SiteMinder，请调整策略存储。

限制策略对象和用户存储搜索

角色策略的每个规则都需要对象存储中的对象集。 在 CA Identity Manager 评估规则时，它加载这些对象并且执行任何必要的用户存储搜索。

以下示例显示了包括三个成员规则的成员策略。 每个规则各包括四个作用域规则。


Member Policies

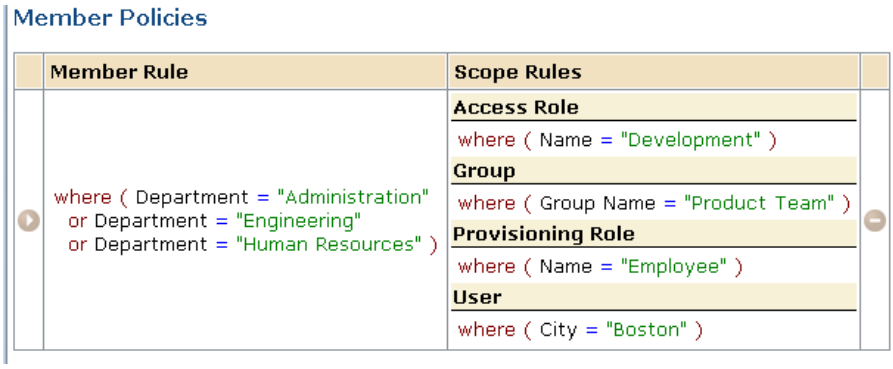
Member Rule	Scope Rules
where (Department = "Engineering")	**Access Role** where (Name = "Development") **Group** where (Group Name = "Product Team") **Provisioning Role** where (Name = "Employee") **User** where (City = "Boston")
where (Department = "Human Resources")	**Access Role** where (Name = "Development") **Group** where (Group Name = "Product Team") **Provisioning Role** where (Name = "Employee") **User** where (City = "Boston")
where (Department = "Administration")	**Access Role** where (Name = "Development") **Group** where (Group Name = "Product Team") **Provisioning Role** where (Name = "Employee") **User** where (City = "Boston")

在此示例中，在评估和应用成员策略时，CA Identity Manager 创建对象并执行下表中所述的用户存储搜索。

规则	策略对象	可能用户存储搜索
■ 成员规则：where (Department = "Administration") ■ 用户作用域：City = "Boston" ■ 组作用域：Group Name = "Product Team" ■ 配给角色作用域：Name = "Employee" ■ 访问任务作用域：Name = "Development"	5	5（每个规则定义对象一个）
■ 成员规则：where (Department = "Engineering") ■ 用户作用域：City = "Boston" ■ 组作用域：Group Name = "Product Team" ■ 配给角色作用域：Name = "Employee" ■ 访问任务作用域：Name = "Development"	5	5
■ 成员规则：where (Department = "Human Resources") ■ 用户作用域：City = "Boston" ■ 组作用域：Group Name = "Product Team" ■ 配给角色作用域：Name = "Employee" ■ 访问任务作用域：Name = "Development"	5	5

在此示例中，CA Identity Manager 创建 15 个对象，并执行 15 个目录搜索来确定成员资格和作用域。

要限制策略对象的数目和 CA Identity Manager 执行的用户存储搜索数，将规则组合到复杂表达式。 下列示例以一个成员规则指定第一个示例中同样的权利。



在此示例中，CA Identity Manager 只创建十个策略对象，只执行五次用户存储搜索。

规则	策略对象	可能用户存储搜索
■ 成员规则： where (Department = "Administration") OR where (Department = "Engineering") OR where (Department = "Human Resources") ■ 用户作用域：City = "Boston" ■ 组作用域：Group Name = "Product Team" ■ 配给角色作用域：Name = "Employee" ■ 访问任务作用域：Name = "Development"	5	5

选择可缩放策略规则类型

除策略规则的数目之外，策略规则的类型也可以影响性能。 通常，以构建用户存储的方式和确定授权的方式为基础构造策略规则。 例如，您可以基于组成员资格、组织或用户属性创建策略规则。 然而，如果有多种方式可以构造策略规则，在决定构造哪种类型的规则之前，考虑下表中的性能准则。

注意：下表的策略规则类型是以性能顺序列出的，以最有效率的规则类型开始。

策略规则类型	性能备注
组织	■ 最佳整体性能 ■ 不需要 LDAP 目录中的搜索。 CA Identity Manager 使用评估的用户的 DN，以及策略规则中的组织的 DN

策略规则类型	性能备注
角色	■ CA Identity Manager 在对象存储缓存中存储角色对象信息和以前评估的结果 ■ 在大多数情况下，性能将与组织策略规则一样出色
用户属性	■ 提供最好的用户存储搜索性能，并且是受大量用户的影响最小 ■ 能够使用内存内评估以获得显著性能提升
组成员身份	■ 性能取决于组大小和用户存储类型

任务优化

在 CA Identity Manager 中，用户在用户控制台中看到的任务取决于该用户的具体权限。 为了显示和执行任务，CA Identity Manager 必须执行多个安全评估，如果应用于 CA Identity Manager 环境中的所有用户，可能对性能造成很大影响。

在下列操作发生时，CA Identity Manager 执行安全评估：

- 用户登录用户控制台

  在这种情况下，CA Identity Manager 必须评估用户的角色，以便确定用户可以在用户控制台中访问哪些任务。

- 用户调用任务

  在调用任务时，CA Identity Manager 必须确定用户能使用该任务管理哪些对象。

- 用户访问关系选项卡

  关系选项卡是用户从中可以查看或管理任务主题和授权集之间的一对多关系的任何选项卡。 关系选项卡的一个示例是“管理角色”选项卡，该选项卡显示用户具有的角色。

- 用户在关系选项卡上添加对象

  例如，在用户在“管理角色”选项卡上将其他角色添加到其他用户时，CA Identity Manager 执行其他安全检查。

任务性能受到以下内容的影响：

- 任务作用域，它确定管理员可以使用任务的位置
- “关系”选项卡，它显示对象与其他对象的关系

任务作用域评估和性能

在管理员使用涉及搜索管理对象（如用户、组、组织、任务或角色）的管理任务时，CA Identity Manager 评估和应用任务作用域规则。 这些规则可以显著影响 CA Identity Manager 显示要为任务选择的对象的列表花费的时间。

注意：与成员、管理员和所有者策略评估不同，有关作用域规则评估的信息不存储在缓存中。

任务作用域由以下内容决定：

- 任务管理的对象的类型。
- 适用于包括该任务的管理角色的作用域规则。 在成员、所有者和管理策略中定义作用域规则。
- 任何用户定义的搜索条件。

例如，考虑修改用户任务，此任务包含在用户管理者角色中。 用户管理者角色具有一个成员策略，该策略带有允许用户管理者管理员工组织中的用户的作用域规则。 管理员打开修改用户任务并且输入搜索条件：姓氏以 A 开头。 在这种情况下，修改用户任务的作用域是在员工组织的所有姓氏以 A 开头的用户。

CA Identity Manager 如何呈现关系选项卡

关系选项卡允许用户使用权利集查看和管理任务主题具有的关系。 例如，“配给角色”选项卡显示用户拥有的配给角色。

为了确定关系选项卡上显示的对象，CA Identity Manager 执行大量安全评估，这可能会显著影响性能。

下列示例显示了 CA Identity Manager 呈现“配给角色”选项卡所采用的步骤：

1. 管理员单击修改用户任务的“配给角色”选项卡。
2. CA Identity Manager 检索包含选定用户的配给角色。
3. 如果选项卡配置为允许角色管理员进行管理，CA Identity Manager 执行第二次调用，以检索选定的用户是管理员的配给角色的列表。
4. CA Identity Manager 评估在启动任务的管理员可以管理该角色的成员资格时，用户必须看到的每个配给角色。

   如果管理员可以管理角色成员，CA Identity Manager 在该选项卡的角色列表中的角色的“成员资格”列中显示一个活动复选框。

5. CA Identity Manager 评估在启动任务的管理员可以管理该角色的管理权限时，用户必须看到的每个配给角色。

   如果管理员可以管理管理权限，CA Identity Manager 在该选项卡的角色列表中的角色的“管理员”列中显示一个活动复选框。

   CA Identity Manager 必须完成步骤 2-5，以便显示用户当前具有的配给角色。 如果管理员需要分配新的配给角色，需要下列其他步骤。
6. 管理员单击“添加”按钮以找到要分配的新配给角色。
7. CA Identity Manager 显示管理员可以用来搜索要添加的角色的搜索屏幕。
8. 管理员输入搜索筛选器以找到要添加的角色。
9. CA Identity Manager 返回符合以下条件的配给角色列表：
   - 角色匹配管理员输入的搜索筛选器。
   - 管理员可以管理角色的成员资格。
   - 用户在角色管理员的管理作用域中。
   - 用户尚未具备配给角色。
10. CA Identity Manager 重复第 9 步以确定管理员可以管理管理权限的角色。

关系选项卡和性能

因为 CA Identity Manager 执行的安全评估的数量，呈现关系选项卡可能显著影响性能。 决定性能的因素随选项卡的类型变化。

对于角色关系选项卡，下列因素可以影响性能：

- 任务的主题是成员的角色数
- 任务的主题是管理员的角色数
- CA Identity Manager 需要用来计算主题角色的系统的总对象数
- 每个角色成员/管理策略数
- 成员/管理策略作用域规则的复杂性
- 保存缓存的任务调用程序授权，以限制安全实施的效果的能力

要在组成员资格选项卡上确定组成员资格和管理权限，CA Identity Manager 必须在用户存储中搜索所有的组。 这些搜索的性能取决于以下因素：

- 用户存储的组对象数
- 任何组中的成员数
- 用户存储所在的数据库或目录的性能

任务处理和性能

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。

在 CA Identity Manager 处理任务时，它处理与该任务关联的每个事件。在事件处理期间，CA Identity Manager 保存每个事件四次。 一旦出现意外的系统关闭，这允许 CA Identity Manager 保留进程中操作。

在 CA Identity Manager 同时处理多个事件时，将事件添加到队列。 在第一个事件完成生命周期的第一个阶段时，会将它保存，并移到队列后面以等待第二个阶段处理开始。 CA Identity Manager 然后为队列的下一事件完成第一个处理阶段，将该事件移到队列的末端。 过程继续，直到队列的所有事件已经完成第一个处理阶段。 然后，队列的第一个事件开始第二个处理阶段。 操作继续，直到队列的所有的事件完成全部四个处理阶段。

在正常负载条件下，此行为不影响性能。 然而，如果系统正在处理大量的任务和事件，例如处于用户数量庞大的批量加载阶段，那么每个事件和任务必须在队列中等待更长时间，因此，完成时间也就更长。

要防止加载条件下的性能问题，考虑以下操作：

- 使用某一任务的“配置文件”选项卡上的“任务优先级”设置。

  通过“任务优先级”设置，您可以将任务的优先级设置为“高”、“中”或“低”。

  应该将需要立即处理的任务设置为“高”。应该将处于批量加载中的任务设置为“低”。

  如果设置了任务优先级，则将与具有相同优先级的任务一起处理与该任务关联的事件。 例如，如果将“修改用户”任务设置为“高”优先级，而一位管理员修改用户配置文件，CA Identity Manager 就会在具有“中”或“低”优先级的任务之前处理该任务。 如果有其他“高”优先级任务，CA Identity Manager 为第一个“高”优先级事件完成第一个处理阶段，然后将该事件移至其他“高”优先级事件的列表的末端。
- 安装单独的专用 CA Identity Manager 服务器，以处理批量加载操作

优化任务的准则

当您创建 CA Identity Manager 环境时，CA Identity Manager 部署的默认任务已配置为支持各种管理使用情况。 大多数 CA Identity Manager 实施不需要在默认任务中提供的所有功能。 在创建 CA Identity Manager 环境之后，修改这些任务来适合特定管理需求。

下列步骤是修改任务的准则：

- **创建专用的用户管理任务**

  默认创建用户、修改用户和查看用户任务提供全部管理功能。 在多数实施中，只有少量管理员需要所有的可用能力。

  创建仅包括必要功能的新任务。 例如，如果大多数用户管理任务仅涉及配置文件和组管理，那么可以创建只包括“配置文件”和“组”选项卡的新的修改用户任务。 删除默认修改用户任务中提供的“管理角色”、“访问角色”和“配给角色”选项卡。

  如果将未使用的选项卡留在经常使用的任务中会导致巨大性能开销。当使用任务执行 Web 服务 (TEWS) 客户端时这一情况尤为突出，因为在这一客户端中这些选项卡可能通过随 CA Identity Manager 提供的选项卡 java 类意外激活。

  您创建的专用任务应当符合您为环境定义的指派管理模型 (p. 54)。

- **禁用关系选项卡的“管理管理员”**

  默认情况下，所有关系选项卡为选项卡管理的对象（如角色和组）提供管理管理权限的能力。 多数实施不需要向管理员提供此功能。

  要消除在 CA Identity Manager 评估管理权限时产生的其他开销，如果不需要管理管理员功能，请在下列选项卡上清除“管理管理员”选项：

  - 管理角色
  - 配给角色
  - 访问角色
  - 组

  要使用户可以管理特定选项卡上的管理权限，创建默认选项卡的副本，启用“管理管理员”选项，并禁用“管理成员”选项。 将新的选项卡添加到专用任务中，这些任务只供需要它们的管理员使用。

- **在角色关系选项卡中启用作用域化搜索**

  您可以配置每个角色选项卡，以包括允许管理员为分配给用户的新角色指定条件的搜索。对于 CA Identity Manager 必须评估以确定管理员可以分配给用户哪些角色的成员和管理策略规则，角色搜索会限制规则的数量。

- **设置任务同步选项**

  对于每一个 CA Identity Manager 任务，您可以指定用户同步选项（使用户与身份策略同步）和配给帐户同步选项（使用户与配给的帐户同步）。 在任务完成时，或在事件完成时，这些选项使您能够使用户同步。

  要消除评估和处理时间，设置在任务完成时而不是事件完成时出现的同步。

组成员/管理员优化准则

要改善搜索组成员和管理员的性能，请考虑以下内容：

- 在目录配置文件 (directory.xml) 中定义常用属性，此文件向 CA Identity Manager 说明用户存储结构和内容。

  常用属性是在 CA Identity Manager 中有特别意义的属性。

  要改善组成员/管理员搜索，请为用户对象定义以下常用属性：

  %MEMBER_OF%

  在存储用户是其成员的组的列表的用户对象上标识属性。

  如果定义，此属性可以防止 CA Identity Manager 在用户存储中的所有组中搜索所有成员。在超大组中执行组搜索可以显著影响性能。

  %ADMINISTRATOR_OF%

  在存储用户是管理员的组的列表的用户对象上标识属性。

  与 %MEMBER_OF% 属性类似，此常用属性可以消除冗长组搜索。

- 在目录配置文件中指定组类型

  CA Identity Manager 支持三种类型的组：标准组、嵌套组和动态组。

  在定义目录配置文件的组对象时，您可以指定用户存储支持的组的类型。 如果您的实施不支持嵌套或动态组，如下所示设置组类型属性：

  GroupType = NONE

  “NONE”这一设置指定对标准组的支持。

  默认组类型设置是“ALL”，这可能影响性能。

  注意：有关目录配置文件的常用属性和组类型的详细信息，请参阅*《配置指南》*。

- 设置配给目录缓存索引来改善 GlobalGroup 性能

  对于包括合并的用户存储和配给目录的 CA Identity Manager 实施，GlobalGroup 成员资格可以为角色和身份策略的策略规则评估进行优化。

  要启用此优化，请在配给目录缓存中检索以下属性，配给服务器使用这些属性解析组成员资格：

  eTID

  唯一的对象 ID 属性。 对于组成员资格查找，值是查找涉及的特定用户或组。

  eTPID

  在搜索成员资格时使用的对象的父 ID。

  eTCID

  在搜索成员资格时使用的对象的子 ID。

  另外，添加下列散列条目：

  eTSuperiorClass

  成员资格查找中的父对象的类型

  eTSubordinateClass

  成员资格查找中的子对象的类型

  注意：有关配给目录缓存的详细信息，请参阅*《安装指南》*。

身份策略优化

*身份策略*是指在用户符合某一条件或规则时所发生的一组业务更改。 这些更改可以包括分配或吊销角色、分配或吊销组成员资格以及更新用户配置文件中的属性。

在发生用户同步时，CA Identity Manager 评估身份策略。

身份策略性能受到以下内容的影响：

- 配置身份策略的方式
- 用户同步发生的频率

用户和身份策略如何同步

使用身份策略时，了解 CA CA Identity Manager 如何评估策略及将策略应用到用户很重要。 如果对用户同步过程了解得不够透彻，则在配置身份策略集时可能会出现意外结果。

以下步骤说明了 CA CA Identity Manager 如何评估和应用身份策略：

1. 用户同步过程开始：
   - **自动** - 可以将 CA CA Identity Manager 任务配置为自动触发用户同步。
   - **手工** - 使用用户控制台中的“同步用户”任务来同步用户。
2. CA CA Identity Manager 确定应用到用户的身份策略集。
3. CA CA Identity Manager 将要应用到用户的身份策略集和已应用到该用户的策略列表进行比较。

   注意：已应用到用户的策略列表存储在用户配置文件中的已知属性 %IDENTITY_POLICY% 中。 有关配置此属性的信息，请参阅《*Configuration Guide*》。
   - 如果某一身份策略位于适用策略列表中，*且*该策略先前*未*应用到用户，则 CA CA Identity Manager 会将该策略添加到分配列表中。
   - 如果某一身份策略位于适用策略列表中，该策略先前已应用到用户，且该策略的“应用一次”设置处于禁用状态，则 CA CA Identity Manager 会将该策略添加到重新分配列表中。
   - 如果某一身份策略未在适用策略列表中，且该策略已应用到用户，则此用户将不再匹配策略条件。 CA CA Identity Manager 会将这些策略添加到取消分配列表中。
4. CA CA Identity Manager 为用户评估所有策略后，将按以下顺序应用策略：
   a. 取消分配列表中的身份策略
   b. 分配列表中的身份策略
   c. 重新分配列表中的身份策略

5. 应用身份策略后，CA CA Identity Manager 将重新评估这些策略，以确定是否需要根据在第一次同步过程（步骤 2 至 4）中发生的更改进行任何其他更改。

   这有助于确保应用身份策略时所做的更改不会触发其他身份策略。

6. CA CA Identity Manager 会继续重新评估和应用身份策略，直到用户与所有适用策略同步，或者直到 CA CA Identity Manager 达到在管理控制台中定义的最大递归级别。

   例如，为用户分配角色时，某个身份策略可能会更改用户所在的部门。新部门会触发另一个身份策略。不过，如果递归级别设置为 1，则只有再次同步用户时，才会进行随后的更改。

   有关设置递归级别的详细信息，请参阅管理控制台在线帮助。

设计有效身份策略

创建身份策略时请使用以下准则：

- **限制策略对象的数目**

  CA Identity Manager 在支持身份策略的对象存储中创建对象。要减少对象存储的对象的数目，请使用复杂表达式创建身份策略。
  为角色策略 (p. 62)推荐类似方法。

- **限制身份策略集迭代次数**

  您可以为身份策略配置递归级别，它确定在同步用户时，CA Identity Manager 评估和应用身份策略的次数。例如，为用户分配角色时，某个身份策略可能会更改用户所在的部门。新部门会触发另一个身份策略。不过，如果递归级别设置为 1，则只有再次同步用户时，才会进行随后的更改。

  设置递归级别会限制 CA Identity Manager 必须评估身份策略的次数。

- **限制身份策略规则之间的依存关系**

  您可以创建一个身份策略，其中一个策略的更改操作（应用策略操作或删除策略操作）用于另一个策略的身份策略条件，如下表所示。

身份策略条件	应用策略时的操作	针对删除策略的操作
(Job Code = "100") 位置	成为 (provisioning role "Account Manager") 的成员	删除 (provisioning role "Account Manager") 的成员
(provisioning role "Account Manager") 的成员	成为 (group "Account Managers") 的成员	删除 (group "Account Managers") 的成员

在 CA Identity Manager 评估这种策略时，它必须至少两次评估和应用更改，以确保两个条件都可以满足。为整个 CA Identity Manager 环境设置的递归级别必须大于 1，这会使每个身份策略集产生其他评估。

限制触发用户同步的任务

在用户同步过程中评估和应用身份策略。 您可以通过为任务指定下列用户同步选项之一来配置自动同步：

任务完成时

CA Identity Manager 在任务中的所有事件完成后启动用户同步流程。

每个事件时

CA Identity Manager 在任务中的每个事件完成时启动用户同步流程。

要获得最佳性能，限制触发自动用户同步的任务的数目。

在配置用户同步时考虑以下内容：

- **为密码任务禁用用户同步**

  在大多数情况下，密码不用于身份策略条件。

- **为同步用户任务禁用用户同步**

  自同步用户任务触发身份策略评估以来，如果为此任务启用了用户同步选项，CA Identity Manager 再次执行评估。

- **创建专用任务**

  如果可能，创建执行触发身份策略条件的修改的任务，并仅针对这些任务启用用户同步。

优化身份策略规则评估

要缩短包括用户属性的身份策略条件的评估时间，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比较属性值与策略条件。这限制了 CA Identity Manager 直接访问用户存储的次数。

注意：有关内存中评估选项的详细信息，请参阅*《配置指南》*。

用户存储调整

用户存储调整涉及大量步骤，包括以下步骤：

- 优化用户存储的结构
- 调整基础存储
- 实施负载平衡和复制

这些步骤取决于您正在使用的用户存储的类型。 为调整这些区域的信息，请参阅包含用户存储的数据库或目录的文档。

除一般调整的注意事项之外，还应考虑以下专门针对 CA Identity Manager 的注意事项：

- **衡量用户存储搜索性能**

  要获得最佳性能，CA Identity Manager 策略评估搜索应当在 10-20 毫秒之内完成。

  为确保 CA Identity Manager 可以持续在建议的时间完成这些搜索，需要考虑在多个负载条件下测试搜索性能。

  您也能使用此测量方法来确定用户存储到达其物理限制从而需要增加服务器来平衡负载的时间。

- **编制属性索引**

  为用于角色策略或身份策略的每个属性编制索引。 为属性编制索引可以显著提高性能。

  注意：有关检索属性的信息，请参阅包含用户存储的 LDAP 目录或关系数据库的文档。

- **将 LDAP 绑定存入缓存**

  在 CA Identity Manager 中，在 CA Identity Manager 目录对象上定义的代理用户执行所有的目录 LDAP 绑定。 对于每个连接，针对同一用户重复出现同样的 LDAP 绑定。

  如果您正在使用 LDAP 目录作为用户存储，配置该目录以将 LDAP 绑定（或会话）存入缓存（如果该目录支持）。

- **启用用户存储缓存**

  在 CA Identity Manager 评估用户的策略决策时，将该信息存储在授权缓存中。 在存入缓存的信息到期时，CA Identity Manager 再次评估该用户的所有策略。

  要在随后的策略规则评估中改善用户存储搜索的性能，如果用户存储支持，使用户存储将搜索的数据存入缓存。

CA Directory 包括名为“dxCache”的缓存，它是可以在缓存数据中进行搜索的内存中的数据库实施。

注意：有关 CA Directory 的详细信息，请参阅 *《CA Directory Administrator Guide》*。

调整配给组件

如果 CA Identity Manager 实施包含配给，使用以下优化措施来确保最佳性能：

- 优化 CA Identity Manager 服务器和配给服务器之间的连接

  CA Identity Manager 使用 Java IAM (JIAM) API 与配给服务器进行通信。 要改善通信性能，请配置以下内容：

  - 针对配给服务器的多个连接的 JIAM 会话池

    注意：CA 建议将初始会话数值设置为 8，最大的会话数设置为 128。

  - 从配给服务器检索的对象的 JIAM 缓存

  注意：有关 JIAM 配置设置的详细信息，请参阅 *《管理指南》*。

- 将帐户同步设置为在任务结束时发生 (p. 70)，而不是在每个事件结束时发生
- 调整配给服务器

  注意：有关详细信息，请参阅 *《管理指南》*和 *《安装指南》*。

运行时间组件调整

CA Identity Manager 的业务更改是通过任务完成的。 任务包括一个或多个事件，事件表示 CA Identity Manager 为完成任务而执行的活动。 例如，创建用户任务可能包括 CreateUserEvent 和 AddToGroupEvent。

CA Identity Manager 包括以下组件，它们在运行时处理任务和事件：

- CA Identity Manager 数据库，它支持 CA Identity Manager 功能
- JMS 消息，它负责处理事件

调整 CA Identity Manager 数据库

执行任务时 CA Identity Manager 使用以下数据库：

- 任务持久性

  持续维护 CA Identity Manager 任务和事件的相关信息。 这允许 CA Identity Manager 在系统发生故障的情况下还原事件和任务的最后已知状态。

  注意：因为任务及其事件在状态转换期间会保存到数据库或从数据库检索，因此这一数据库对 CA Identity Manager 性能具有最重要的影响。

- 审核

  为在 CA Identity Manager 环境中执行的操作提供历史记录。

- 工作流

  存储的工作流流程定义、作业、脚本以及工作流引擎所需的其他数据。

- 报告

  存储快照数据，这些数据反映获取快照时 CA Identity Manager 中对象当时的状态。

CA Identity Manager 通过 JDBC 连接池与每个数据库通讯。 在托管 CA Identity Manager 的应用程序服务器中创建和配置 JDBC 连接池。 当您配置 JDBC 连接池时，注意以下事项：

- 考虑将在任何一个时刻执行的并发任务的数量。
- 在您配置 JDBC 连接池大小的时候，考虑另一个运行时间组件。 每个运行时间组件与另一个运行时间组件系统工作。

  注意：CA 建议将初始连接池值设置为 128。

- 对于任务持久性数据库，池中的数据库连接的数量必须允许每个执行任务在整个任务的有效时间内都可以检索和更新任务和事件数据。
- 任务持久性数据库使用已准备的语句。 确保为您要用来存储任务持久性数据的数据库配置已准备的语句缓存。

  注意：有关配置已准备的语句缓存的详细信息，请参阅用于任务持久性的数据库的文档。

JMS 设置

CA Identity Manager 任务包括 CA Identity Manager 为完成任务所执行的事件和操作。

在事件的生命周期内，它通过下列状态实现转换：

- BEGIN
- APPROVED
- EXECUTING
- COMPLETED
- INVALID

工作流控制的事件也具有下列类似状态：

- PENDING
- REJECTED

CA Identity Manager 使用 JMS 消息来控制这些状态转换。

JMS 消息如何推动事件转换

CA Identity Manager 使用 JMS 消息来推动事件的状态转换。 下列步骤说明了所涉及的步骤：

1. 用户提交任务。
2. 任务生成一个或多个事件。
3. 当事件可以进行处理时，CA Identity Manager 将事件的状态设为 BEGIN，并在任务持久性数据库保留该事件。
4. CA Identity Manager 创建包含事件 ID 的 JMS 消息，并且将该消息发布到事件消息队列中。
5. 在收到消息时，JMS 将调用作为事件控制器的实施的事件消息驱动 Bean 的实例。
6. 事件控制器使用消息中的事件 ID 来从任务持久性数据库中检索事件，并且执行事件的当前状态的操作。
7. 当该状态结束时，会将事件设置为下一状态，保留在任务持久性数据库中，并发布新的 JMS 消息以处理下一状态。

   此循环会持续到事件完成其状态机。

JMS 消息和性能

对于任何事件，都有三到五个需要通过 JMS 消息进行状态变换的状态：

- BEGIN
- PENDING （仅在工作流控制下）
- APPROVED 或 REJECTED
- EXECUTING
- COMPLETED 或 INVALID

处理单个事件时，会出现下列操作：

- 三到五次发布到事件消息队列
- 三到五次调用消息驱动 Bean
- 六到十次连接任务持久性数据库（每种状态下都有一个读取操作及一个写入操作）

这些操作可能影响 CA Identity Manager 处理任务所需的时间量。

为确保状态变换期间的最佳表现，调整托管 CA Identity Manager 的应用程序服务器中的 JMS 资源，以便可以使用适合的 JMS 资源。

调整 JMS 设置

下列应用程序服务器 JMS 调整参数定义队列连接和消息驱动 Bean 实例池。

- **WebSphere JMS 调整**

  WebSphere 向队列连接工厂提供了两个参数，您可以配置它们以改善性能。 使用 WebSphere 管理控制台设置以下属性：

  - 在“资源”下面，找到以下队列连接工厂：iam-im-neteQCF 和 iam-im-wpConnectionFactory。
  - 为每一项编辑连接池属性，将最大的连接数设置为 128。

- **WebLogic 调整**

  在 WebLogic 应用程序服务器中，队列连接工厂根据 JMS 线程池的大小，从服务器的 JMS 线程池或者默认执行池中获取连接处理线程。如果 JMS 线程池大小是 0，则 WebLogic 使用执行池中的线程。

  我们建议将 JMS 线程池线程的数目设置为和 CA Identity Manager 事件消息驱动 Bean 中的 Bean 池大小的最大值相同，后者在默认情况下设置为 128。

您使用 WebLogic 服务器控制台来为安装了 CA Identity Manager 的域和服务器设置 JMS 服务属性中的 JMS 线程池的大小。

通过修改下列位置的描述符文件中的 max-beans-in-free-pool 的设置，来设置 CA Identity Manager 事件消息驱动 Bean 池大小：

WebLogic_home\domain\applications\iam_im.ear\identityminder_ejb.jar\META-INF\weblogic-ejb-jar.xml

```
<weblogic-enterprise-bean>
        <ejb-name>SubscriberMessageEJB</ejb-name>
        <message-driven-descriptor>
            <pool>
                <max-beans-in-free-pool>128</max-beans-in-free-pool>

<initial-beans-in-free-pool>16</initial-beans-in-free-pool>
            </pool>

<destination-jndi-name>com.netegrity.ims.msg.queue</destination-jndi-name
>
        </message-driven-descriptor>
    </weblogic-enterprise-bean>
```

- **JBoss 调整**

  在 JBoss 应用程序服务器中，队列连接工厂从服务器的标准 JMS 池会话工厂获得连接处理线程。 默认情况下，最大线程数目设置为 15。

  我们建议设置此值以与标准消息 Bean 容器大小的最大值相匹配。

  在下列文件中的 JMSContainerInvoker 的 MaximumSize 元素中设置 JMS 会话池部分工厂：

  jboss_home\server\default\conf\standardjboss.xml

```
<invoker-proxy-binding>
         <name>message-driven-bean</name>
         ….
         <proxy-factory-config>

<JMSProviderAdapterJNDI>DefaultJMSProvider</JMSProviderAdapterJNDI>

<ServerSessionPoolFactoryJNDI>StdJMSPool</ServerSessionPoolFactoryJNDI>
            <MaximumSize>128</MaximumSize>
            <MaxMessages>1</MaxMessages>
            ….
         </proxy-factory-config>
     </invoker-proxy-binding>
```

通过修改下列描述符文件中最大大小值，设置 CA Identity Manager 事件消息驱动 Bean 池大小：

jboss_home\server\default\conf\standardjboss.xml

```
<container-configuration>
         <container-name>Standard Message Driven Bean</container-name>
         <call-logging>false</call-logging>

<invoker-proxy-binding-name>message-driven-bean</invoker-proxy-binding-name>
        ......
         <container-pool-conf>
            <MaximumSize>128</MaximumSize>
         </container-pool-conf>
   </container-configuration>
```

调整 JBoss 5 的性能

在 JBoss 5 的默认安装中，JBoss 热部署扫描程序每 5 秒运行一次，这会影响 JBoss 性能。 如果不需要，则可以禁用该功能，或者更改其运行频率。

禁用或修改热部署

1. 编辑下列位置中的 hdscanner-jboss-beans.xml：

   单个节点：*jboss_home*/server/default/deploy

   群集：*jboss_home*/server/all/deploy

2. 要禁用此功能，请在 HDScanner bean 中添加下列行：
   ```
   <attribute name="ScanEnabled">False</attribute>
   ```
3. 要修改扫描频率，请将 scanPeriod 属性值增加至 5000（毫秒）以上。

注意：详细信息请参阅链接：
http://community.jboss.org/wiki/JBossASTuningSlimming。

查找内存不足错误

如果 Java Heap 太小，您可能看到“内存不足”的异常。我们建议初始大小设置为 1024。

第 7 章： 创建灾难恢复计划

此部分包含以下主题：

灾难引起的服务丢失

一旦出现灾难，用户可能无法访问对他们的业务极其重要的服务。因此，这些用户无法向其他用户提供服务。

恢复服务访问的紧急程度取决于实际使用 CA Identity Manager 的情况。在一些组织中，用户需要不间断使用 CA Identity Manager 提供的服务，而其他用户需要在一天之内恢复系统。 无论发生哪种情况，我们建议您进行一些准备工作，以保护您的 CA Identity Manager 实施免受可能造成系统部分或完全损失的事件的伤害。

通过为 CA Identity Manager 配置冗余体系结构，您可以确保服务对用户的高可用性。 在主要组件发生故障时，备选组件继续提供相同服务。此外，您可以经常备份关键系统和软件，以便您可以还原完全丢失的任何系统或数据。

本文提供这些方案的总体规划准则。 我们建议您使用这些准则来开发符合您的组织需求的专用灾难恢复流程。

如何计划灾难恢复

要制定有效的灾难恢复计划，请阅读本章中详细描述的以下阶段。

✓	阶段
	1. 确定灾难恢复需求 (p. 85) 基于组织需求，确定可能发生什么类型的灾难，以及需要还原服务的速度。
	2. 设计冗余体系结构 (p. 85) 根据您的需求，设计带有位于远程位置的冗余组件的体系结构。
	3. 制定备份计划 (p. 87) 要保护您的安装，请开发备份组件的计划。
	4. 制定还原流程 (p. 88) 制定还原丢失组件的流程。
	5. 将恢复计划存档 (p. 91) 将从灾难恢复 CA Identity Manager 的计划存档。
	6. 测试恢复计划 (p. 92) 基于您的灾难恢复流程，验证您是否可以将您的 CA Identity Manager 实施恢复为事件发生之前的状态。
	7. 提供灾难恢复培训 (p. 93) 通过确认负责从灾难中恢复系统的人员经过了相关培训，来满足要求。

确定灾难恢复需求

以下是确定灾难恢复计划的需求需要考虑的一些通用准则：

1. 使用以下知识组建团队：
   - 支持 CA Identity Manager 的体系结构和系统的知识
   - 如何备份 CA Identity Manager 使用的关系数据库和 LDAP 用户存储的知识
2. 确认要建立的可能灾难方案，包括系统在一个或多个站点部分或完全损失的情况。
3. 列出对支持您的安装非常关键的系统。
4. 定义每个系统可接受的最长停机时间。

   例如，支持备用服务器的系统恢复优先级可能较低。

设计冗余体系结构

要应对关键组件的故障，请考虑以下预防性操作，需要使用远程位置的备用组件（服务器和目录）和冗余数据库。

使用 *《安装指南》* 为 CA Identity Manager 配置冗余。包括以下组件：

- 作为群集的一部分的冗余 CA Identity Manager 应用程序服务器节点
- 策略服务器群集提供故障转移功能（如果您正在使用 CA SiteMinder 保护 CA Identity Manager）
- 备用配给服务器、配给目录和连接器服务器。 如果主要组件丢失，系统切换到备用组件。

为以下数据库配置冗余：

- 作为 CA Identity Manager 的一部分的任何运行时间数据库（如工作流或审核数据库）。

  请参阅随 ORACLE 或 Microsoft SQL Server 提供的文档。
- Business Objects 数据库（如果您使用报告服务器）。

  请参阅 SAP 文档网站上的 Business Objects Enterprise 版本 2 以及版本 2 SP 4 文档。

备用 CA Identity Manager 服务器

如果为 CA Identity Manager 提供冗余应用程序服务器节点，则可以提供可扩展性、提高性能且在单个服务器故障时可以进行灾难恢复。 为应用程序服务器提供故障转移功能的最常见方式是创建群集。 创建群集的步骤请参阅 *《安装指南》* 的群集部分。

注意：对于 CA Identity Manager r12.0 和更高版本，应用程序服务器群集是实施多节点部署的唯一有效的方式。CA Identity Manager 环境要求使用行业标准 J2EE 群集体系结构，它使用 JMS 队列作为基础结构。因此，在 CA Identity Manager 配置中使用多个节点的唯一有效的方式是使用应用程序服务器群集。

有关此更改的详细信息，请参阅 TechDoc 545594。

备用配给组件

几个配给组件可以选择一个备用组件以提供高可用性。 备用组件应当位于远程站点，以实现最高水平的保护。

有关备用服务器和目录的具体配置的详细信息，请参阅 *《安装指南》* 的“高可用性配给”一章。

多站点配给目录

您可以创建主配给目录和备用配给目录，备用目录位于远程站点。 CA Directory 建议您安装三个配给目录，一个主目录和两个备用目录。

多站点配给服务器

要应对主配给服务器的故障，您可以配置备用配给服务器。 主配给服务器和备用配给服务器之间的差异是，主服务器安装填充了“配给目录”容器项。 同样，卸载主服务器会删除这些项。 除了安装和卸载之外，主服务器和备用服务器运转方式相同。

多站点连接器服务器

对于 Java 或者 C++ 连接器服务器，您可以配置多个连接器服务器来为同一端点或同样的端点类型服务。

对于您配置的每个连接器服务器，都应当配置位于远程位置的一个备用连接器服务器，来处理同样的端点。 如果连接器服务器出现故障，备用服务器立即管理与端点的通信。

冗余数据库

支持的数据库软件 Microsoft SQL Server 和 Oracle 可以提供提供冗余数据库功能。 如果主数据库出现故障，则可以立即使用冗余数据库。 针对影响整个站点的情况，冗余数据库应当位于远程站点。

制定备份计划

要防止丢失任何系统或全部系统，为您备份的所有数据使用非现场存储，并使用符合最大停机时间要求的备份排定。 备份和还原流程使用不同应用程序，因此应当进行协调，以作为整体恢复 CA Identity Manager 系统。

备份计划中包括以下组件：

组件	说明	备份方法
CA Identity Manager 用户存储	包含 CA Identity Manager 用户记录的 LDAP 用户目录或关系数据库	请参阅与数据库或 LDAP 软件一起提供的文档。
CA Identity Manager 数据库	任务持久性、工作流、审核、对象存储、报告以及任务持久性存档的数据库 工作流、任务持久性和审核更改频率最高，应当相应排定备份。	请参阅与数据库软件一起提供的文档。
SiteMinder 策略存储	如果您正在使用 SiteMinder，这是具有 SiteMinder 策略服务器的对象的 LDAP 用户目录或关系数据库	请参阅与数据库或 LDAP 软件一起提供的文档。
配给目录	包含配给用户和配给对象的记录的 LDAP 用户目录	请参阅 CA 目录文档。
应用程序服务器 JMS 持久性存储	用于保存 CA Identity Manager 任务事件处理消息的存储	请参阅应用程序服务器文档。

组件	说明	备份方法
报告数据库	快照数据库 Business Objects 数据库	请参阅与数据库软件一起提供的文档。
自定义报告	自定义报告和相关 XML 文件	请参阅 SAP 文档网站上的 Business Objects Enterprise 版本 2 以及版本 2 SP4 文档。

在使用文件系统备份程序的备份计划中加入以下组件：

组件	说明
Web 服务器组件	部署的 Web 服务器组件（如应用程序服务器插件和 SiteMinder Web 代理）的配置。 如果您正在使用负载平衡或者正在使用 SiteMinder 来保护对用户控制台的访问，则需要 Web 服务器前端。
XML 数据文件	用于创建、维护和存档 CA Identity Manager 对象存储对象的全部 CA Identity Manager 目录和环境文件。
CA Identity Manager 自定义组件	在下列部署的 iam_im.ear 文件夹中找到的文件： ■ Config ■ User_console.war WEB-INF\web.xml
脚本和程序	TEWS 脚本、程序、程序出口
Connector Xpress 组件	自定义连接器 Connector Xpress 项目文件
灾难恢复文档	如果您创建自己的灾难恢复文档，发生说明更改时，定期备份该文档。

制定还原流程

还原流程取决于备份方法。故障系统的恢复流程取决于具体情况。然而，在许多情况下，还原方式是重新安装软件。 有关详细信息，请参阅 *《安装指南》* 的“高可用性配给”一章。

还原 CA Identity Manager 用户存储

要还原 CA Identity Manager 用户存储，请参阅与数据库或 LDAP 软件一起提供的文档。 确认来自备份的数据存储是原封不动的，包括对所有用户存储的访问。

还原 CA Identity Manager 数据库

要还原 CA Identity Manager 数据库，请参阅与数据库一起提供的文档。确认来自备份的数据存储是原封不动的，包括对所有数据库的访问。

还原 SiteMinder 策略存储

要还原 SiteMinder 策略存储，请参阅与数据库或 LDAP 软件一起提供的文档。 确认来自备份的数据存储是原封不动的，包括对所有用户存储的访问。

还原 CA Identity Manager 服务器

如果丢失了 CA Identity Manager 服务器的一个群集节点，请执行下列操作：

1. 使用标准记录步骤来添加节点。

   请参阅*安装指南*有关群集安装的章节。

2. 更新与配给服务器的连接。

   有关详细信息，请参阅*《安装指南》*的“高可用性配给”一章中的“配给故障切换”部分。

还原配给服务器和目录

您可以通过安装备用服务器来还原丢失的配给服务器。 如果所有系统都发生故障，还原在灾难期间丢失的数据。

使用以下步骤：

1. 将任何自定义架构文件复制到 CA Directory config\schema 目录。
2. 安装新的配给目录。

   数据存储是空的。
3. 从备份位置还原数据。
4. 使用配给服务器安装程序，为新还原的配给目录提供详细信息。

   域信息应该已经在该位置存在。
5. 通过备份恢复任何自定义连接器和配置文件。

注意：有关详细信息，请参阅 CA Directory 文档。

还原连接器服务器

如果您丢失了连接器服务器，请执行下列操作：

1. 使用连接器服务器安装程序安装新的连接器服务器

   在安装期间使用配给服务器注册它。
2. 使用 csfconfig 或 Connector Xpress 删除丢失的连接器服务器的注册。

还原报告服务器

如果您丢失了报告服务器，请参阅适用步骤的 Business Objects 文档。 在 SAP 文档网站上，查看 Business Objects Enterprise 版本 2 以及版本 2 SP 4 文档。

还原管理任务

如果在发生灾难时管理任务正在执行，在下列条件下可以恢复该任务。

- 如果用户保存未决状态信息的存储已经保存，任何处于未决状态等待批准的管理任务仍然可用。 这些存储包括任务持久性数据库、保存任务和事件 JMS 消息的 JMS 存储以及工作流数据库。
- 处于“进行中”状态（除“未决”之外的任何其他状态）的任务受其他条件的影响。

  此状态的任务需要将新的 JMS 消息发送到 CA Identity Manager 事件消息队列，然后才能继续被处理。 在恢复时，在将该事件发送到队列之前出现的中断会防止任务继续执行。

  在这种情况下，有两个选项可以恢复任务：

  - 如果任务是以失败的状态显示在“查看提交的任务”任务中，请转到任务详细信息页面，并且使用“Resubmit Task”选项来重新提交此任务。
  - 进行同样的更改，提交新的任务。

将恢复计划存档

基于此章的方针，我们建议您编写适用于自己组织的特殊灾难恢复文档。

请考虑以下方式：

1. 为每个系统确定您的体系结构和备选组件的系统名称和位置。

   对于每个系统，都请列出安装的软件，如安装的具体 JDK，应用程序服务器的修补程序版本和安装的内存数量。 对于您认为需要完全重建的任何系统，此详细信息都是必不可少的。
2. 如有必要，请编写恢复每个组件或重建整个系统的过程。
3. 如果系统和 CA Identity Manager 用户界面的用户名和密码仅仅为一或两个人所知，请确定一种定位或重置方法。
4. 创建灾难恢复文档的备份副本，并将其存储在众所周知的非现场位置，对其加以保护，以防丢失。

测试恢复计划

为有助于成功实现灾难恢复，您可以安排一次模拟灾难，使特定系统不可用。 考虑以下部分中描述的以下测试。

1. 测试故障切换流程。
2. 测试系统恢复。

测试故障切换流程

所有服务器或目录都应当在远程站点有备用服务器或目录，包括这些组件：

- CA Identity Manager 服务器
- 配给服务器
- 配给目录
- C++ 和 Java 连接器服务器
- 报告服务器
- 策略服务器

手动停止每个组件，并确认所有操作能使用备选组件继续运行。 例如，您可以对配给服务器执行以下测试：

1. 在具有主配给服务器的系统上，从“Windows 服务”对话框停止“配给服务”服务。

   主配给服务器停止。

2. 在用户控制台中，执行下列操作：

   a. 将配给角色分配给用户。

   b. 确认为该用户创建了端点帐户。

      创建的帐户取决于处理与 CA Identity Manager 服务器通信的备选配给服务器。

此过程是一次测试的示例。 对于您停止的每个组件，请开发相似测试以确认系统在使用备选组件。

测试还原过程

根据您的灾难恢复文档，对每个关键组件执行测试，以便确认您可以还原失效的系统。

提供灾难恢复培训

如果认为恢复过程可靠，请帮忙确保必须实施恢复的用户都能这样做。尽管您的组织可能需要其他步骤，以下内容是一些一般准则：

1. 将恢复文档的位置广而告之。
2. 执行培训预演。
3. 加入来自培训的反馈，以有助于确保最终的灾难恢复过程是足够的。

注意：您也可以选择将这次培训作为分配恢复协调者的机会，包括作为恢复协调者的一个人以及作为备选协调者的第二个人。 应当指导这些人在明文规定的位置会面，以开始灾难恢复。