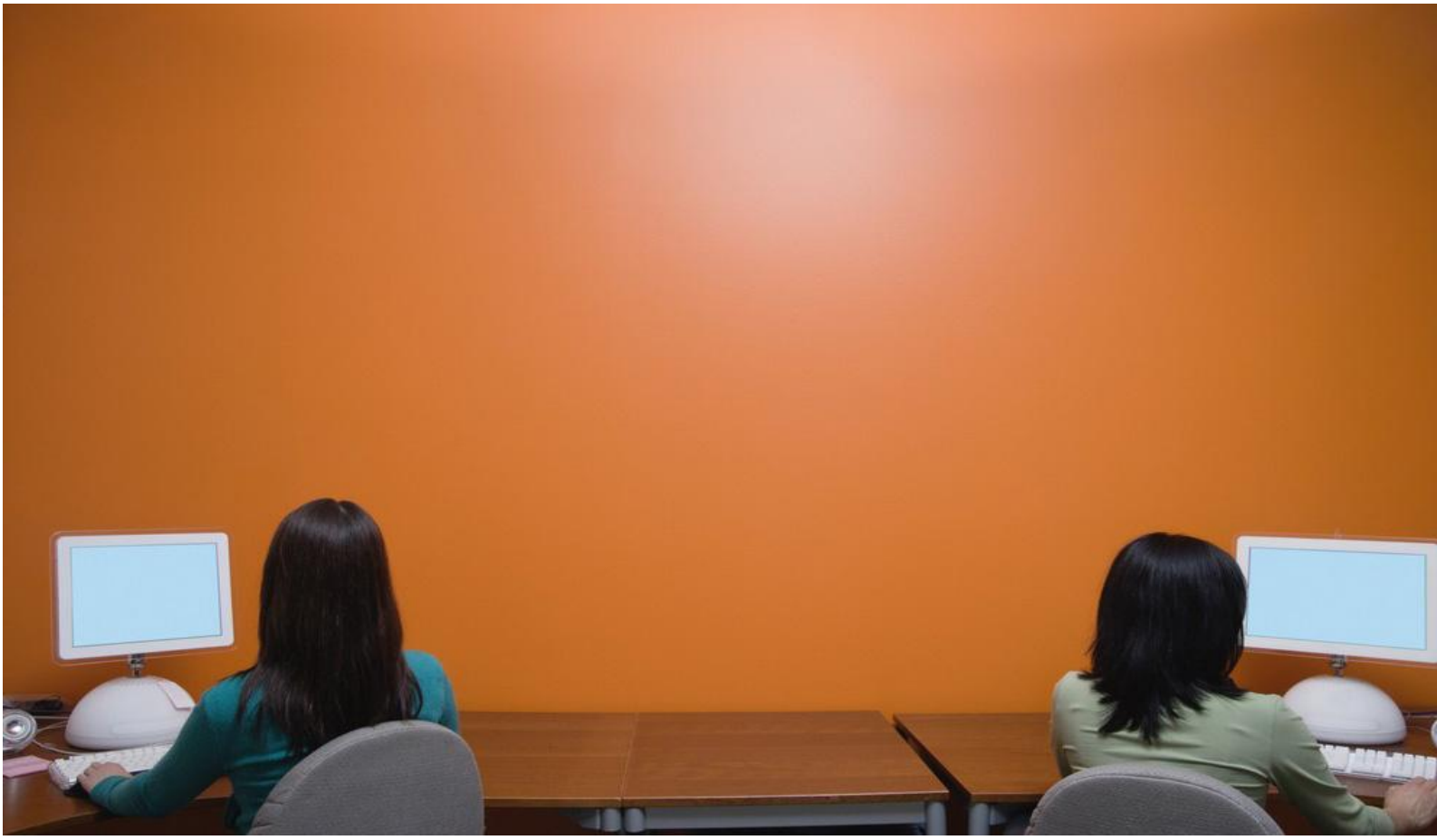
Oracle 系列电子书

Oracle 安全之身份管理器

考虑到简化管理，降低风险和更易于集成这三个驱动因素，OIM 被添加到了 Oracle 身份管理产品套件之中。

- *Oracle 身份管理器概述*
- *理解 Oracle 用户配置流程*
- *Oracle 身份管理器的集成功能*
- *分析 Oracle 身份管理器的部署模型*

TechTarget 中国



Oracle Identity Manager

身份管理器

考虑到简化管理，降低风险和更易于集成这三个驱动因素，OIM 被添加到了 Oracle 身份管理产品套件。——David Knox

当一名新员工刚加入公司时，她需要一间办公室，一台电脑，办公室用品，电子邮件地址，对业务应用软件的访问权限，等等。这个过程重复了很多次，比如员工入职或者雇佣到退休。用户配置是一个由员工入职或者聘用到退休开始的子流程，专门管理用户对资源的访问。

对于大多数希望降低它们账户管理行政负担，同时还试图降低对重要应用程序访问授权集中控制风险的企业来说，用户配置已经变成了一个关键问题。相反，有了用户配置解决方案，新账号创建任务可以以一种一致规范的方式执行，凭借在提供给新用户访问权限之前进行特定审批和核对确认来实现控制。

另一个用户配置的关键困难是技术上的统一系统集成。通常，企业会有基于不同技术和标准构建的范围很广的一大堆应用程序，因此集中账号创建流程通常是一场集成的噩梦。

考虑到简化管理，降低风险和更易于集成这三个驱动因素，OIM 被添加到了 Oracle 身份管理产品套件。该产品是 Oracle 从 Thor Technologies 公司收购来的一款更小的，品种最好的用户配置产品。由于是收购来的产品，Oracle 已经对该产品做了大量开发和改进，但是基本框架和用户配置方法仍然坚持基于以上三个驱动因素考虑。

在本次的 Oracle 技术电子书中，我们将会对 Oracle Identity Manager 进

行一个全面的介绍，其中包括以下内容：

- Oracle 身份管理器概述
- 理解 Oracle 用户配置流程
- 使用 Oracle 身份管理器的集成功能
- Oracle 身份管理器连接器功能简介
- 分析 Oracle 身份管理器的部署模型

Oracle 身份管理器概述

OIM 对于整个身份管理解决方案来说，是一个基本的构建块。访问管理，角色管理，目录服务和授权管理都依赖于有一个用户配置解决方案，这样才能确保正确的身份数据保存在正确的位置供其他解决方案使用。而且，一般配置问题中会涉及那么多不同的策略类型，流程和集成，所以配置技术需要支持高度的灵活性和可定制性。然而，增加灵活性会带来复杂性，因此 OIM 努力在支持配置定制而不使实现流程太困难方面达到一种平衡。

OIM 产品框架设计的架构支持开发人员选择工作需要的复杂程度。通常，需要定制的要求高的话，会使得配置的复杂程度更高。例如，OIM 提供了许多开箱

即用的标准集成解决方案以供连接(以打包的连接器和适配器形式提供)，这为 OIM 提供了连向特殊系统(比如活动目录 Active Directory)的基本解决方案。然而，比如审批工作量或者围绕配置的定制属性，这些额外的需求需要开发人员定制基线连接器来支持那些需求。在本章中，你会学会如何利用 OIM 实现这些需求中的一大部分。

总体而言，OIM 仍然是一块复杂的技术，在实施前需要好好理解。学习 OIM 的一个很好的起点是理解 OIM 策略框架中管理用户配置的一些关键概念。

Oracle 身份管理器的各个元素

- **用户**

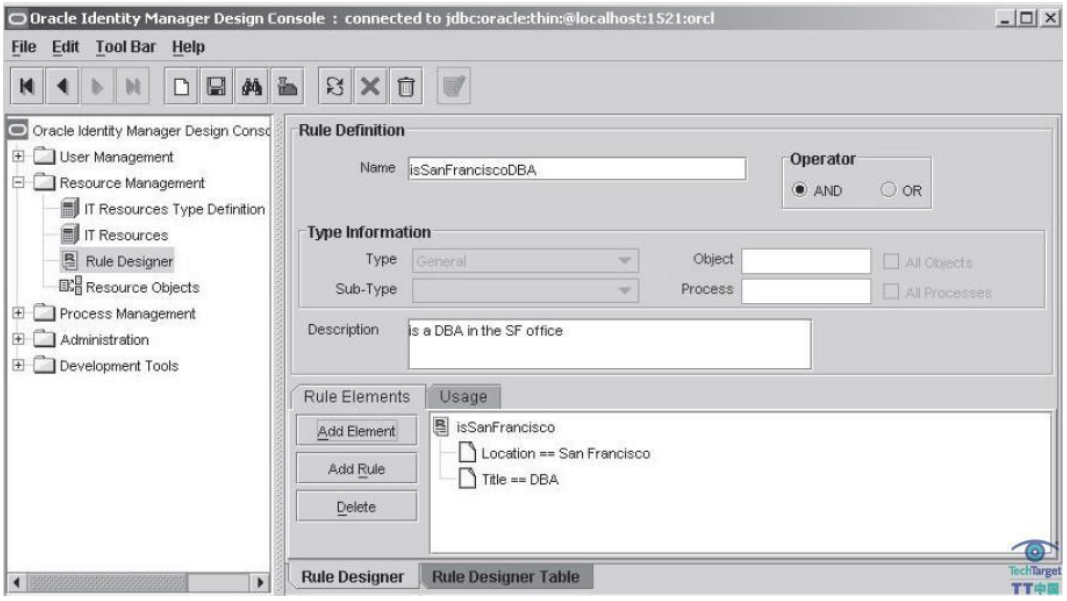
安全要求理解在任何情况下谁可以访问什么。在 OIM 中，用户代表了在企业用户配置范围内的“那个谁”。OIM 用户是应用程序无关的，因此可以利用应用为中心的展现和数据模型支持不同的应用。OIM 用户依据特定的标准身份属性定义了一套具体的默认数据模型，比如，名字，姓氏，员工类型，职称，所属机构，等等。这些属性可以根据需要扩展。数据模型定义了基本的企业级身份数据，它在每种资源中都驱动着用户的账户和权限。

- **用户组**

在许多应用程序中，用户被基于通用功能，组织，工作级别等等进行分组。OIM 提供了用户组对象，它是支持按照特定规则和策略把用户组织成简单几类的一种机制。

有两种方式可以将用户关联到组：通过直接成员分配进行管理，或者由规则驱动成员管理。直接分配机制是大部分人都熟悉的直观的机制。成员管理起来很简单，直接，直观，而且易于理解和验证。直接分配由另一个有相关权限的用户(比如，管理员，主管人员，等等)以一种自由选择的方式执行，而且是以一种静态的方式维护成员(成员被撤销也是以自由选择的方式进行)。因此，对于某些应用和分组情况，直接分配不是一种很受欢迎的方法。

另一种方式与对成员静态分组不同，你可以利用成员规则的概念以一种更自动化的方式管理组成员。成员规则是一些简单的条件陈述，用来评估每个用户是否属于某个组。下图展示了一个成员分组规则："位置==旧金山"。这是一个基于"位置"属性值对成员自动分组的示例。



这条规则定义了它的成员用户的工作职位必须是 DBA，而且必须在旧金山地区工作。用户组利用成员规则实际上非常动态化，为管理谁属于哪些组因而该赋予哪些资源提供了极大的灵活性。这种映射是在访问策略(稍后讨论)内部执行的。

相对于组用户，OIM 还提供了组织的概念。不过，这两种对象都是用来为互补的不同目的组织用户的。通常，用户组基于用户属性跨职能部门划分用户，可能存在把任何组织或者部门的用户跨企业分到了一组的情况。

- **组织**

OIM 中组织的概念代表了一个业务职能或者区域部门，比如销售，产品开发，北美业务部，等等。OIM 组织对象可以被嵌套，从而代表现实世界组织的层次结构。

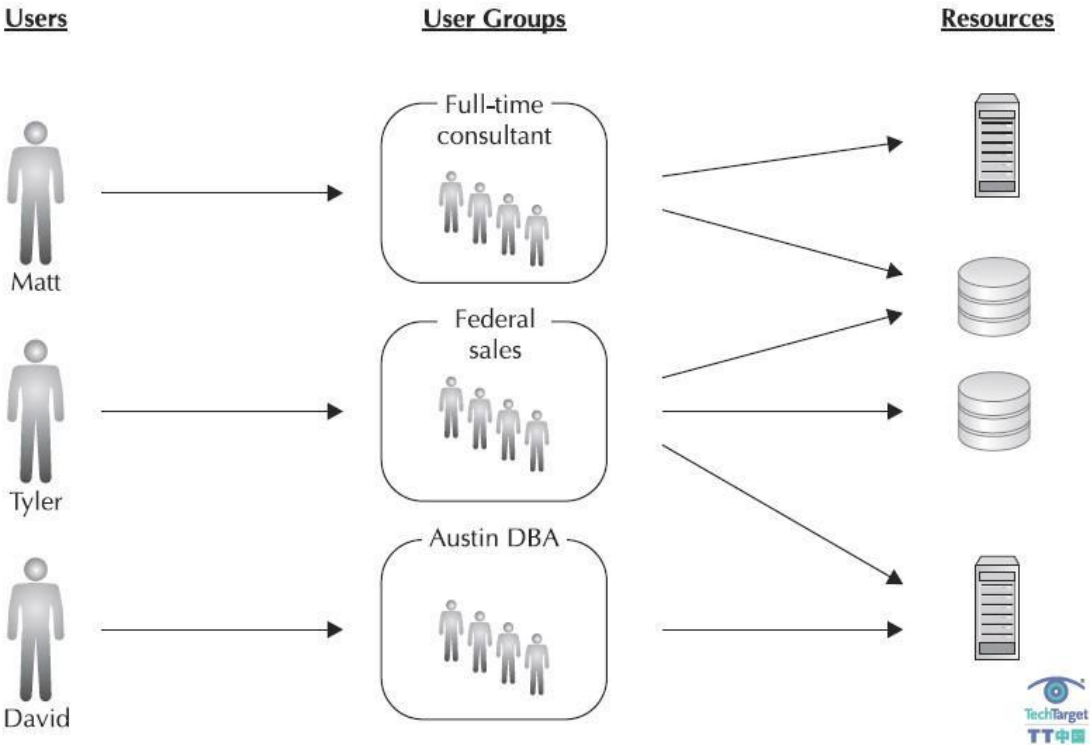
有三种类型的 OIM 组织：公司，部门和分支机构。下面是每种类型如何与普通现实世界组织映射的模型：

- 公司(Company)对象通常代表任何公司中拥有多种业务职能的经营单位。(比如：销售，市场，财务，IT，等等)。
- 部门(Department)位于公司对象之下，代表业务职能部门(比如：销售，财务，等等)。
- 分支机构位于部门对象之下，提供额外的用户组，通常按地域划分。

实际上，我们并不总是需要真正按照你公司或企业的组织方式来划分和建立组织模型，因为你可能并不总是需要详细管理到那个程度。另外，要记住现实世界的组织模型可以经常变更，因此，如果你的配置和访问策略不依赖于该用户的组织机构，你可能就不会总是想把那些模型与现实完全对应。

访问策略

访问策略是 OIM 映射谁有权限访问什么资源的一种方式。从用户到资源的整体映射可以由从用户到用户组的映射和从用户组到资源的映射组成。下图展示了一个访问策略示例，它可以基于规则和映射(在每个对象上用箭头表示)自动配置给终端用户合适的资源。



除了控制资源，你还可以通过在访问策略中把应用级的权限关联到用户组，来控制每个用户在每种资源内部的权限。例如，假定有两个用户组，“数据分析师”和“数据管理员”，这两个用户组都被配置为可以访问相同的数据库应用，但是它们是不同的数据库角色(比如：分析师和 DBA)。你可以在访问策略里设置用户组到数据库角色的映射。

● 资源对象

资源对象就是 OIM 对象，它代表了用户需要有账号创建的逻辑资源。例如，你可以创建名为“电子邮件服务器”和“客户数据库”的对象。资源对象几乎可以代表所有事物，从应用，数据库和操作系统，到物理资产以及其他任何与配置相关的实体。

资源对象是用来跟踪哪些用户配置了什么逻辑资产。它可以对配置了我们前面例子中提到的电子邮件服务器资源的当前用户列表形成报告。资源对象还用于设计审批工作流程和围绕这些以应用为中心的工作流程的策略。因此，例如，如果一个特定人员被分配来审批所有使用电子邮件服务器系统的新账号，你可以利用资源对象来设置你工作流规则中的条件。

资源对象几乎可以代表所有事物，从应用、数据库、操作系统，到物理资产以及其他任何与配置相关的实体。

OIM 资源对象不代表物理资源自身，因此不包含物理细节(比如：IP 地址，服务器主机名，等等)。对于物理服务器的描述和细节，OIM 提供了叫做 IT 资源的概念。

● IT 资源

IT 资源是一个逻辑资源对象的物理展现。它拥有要配置一个新用户所需要资源的所有物理细节。例如，如果你有一个叫做客户数据库的资源对象，你还需要定义一个或多个相应的 IT 资源对象，代表该资源的物理特征(比如：服务器主机名称，IP 地址，物理位置，等等)。这些信息被 OIM 集成引擎在需要与那些服务器交互完成配置相关任务时使用。

一个 IT 资源的特定属性集高度依赖于在其上创建账号的系统类型(关系数据库 IT 资源要求是对象名称和密码;LDAP 服务器 IT 资源可能是命名空间和目录信息树细节)。OIM 支持你定义 IT 资源类型，以模板的形式为特定 IT 资源定义具体数据模型。

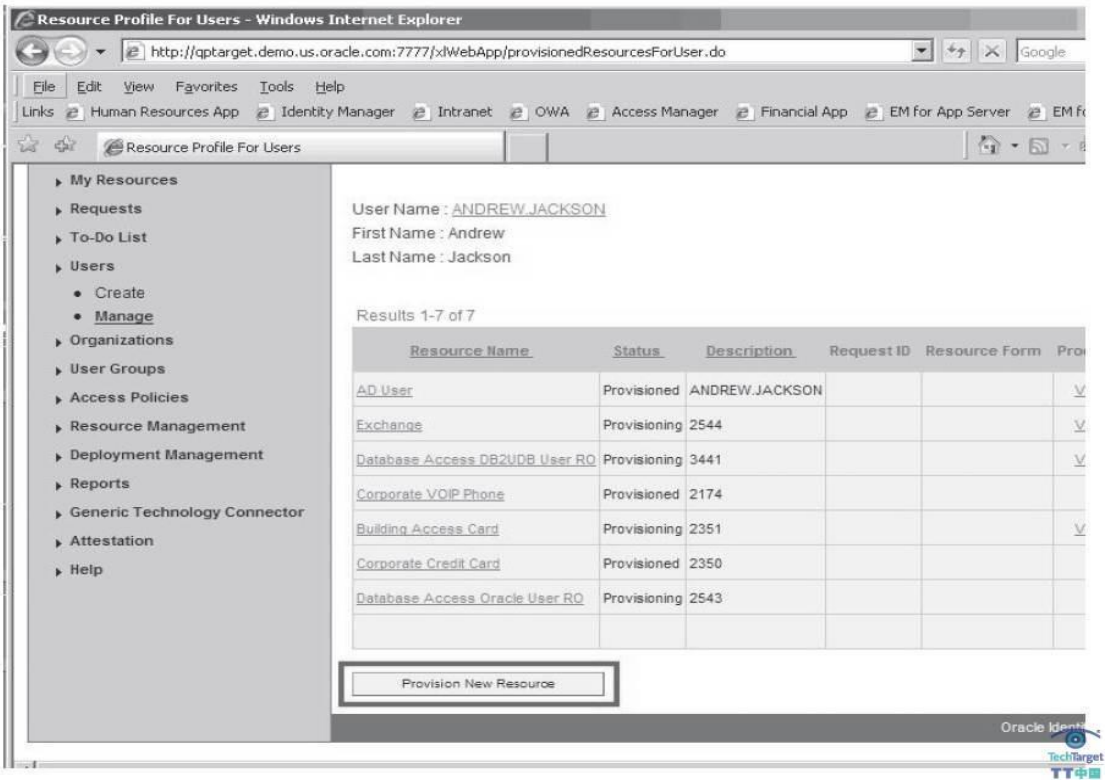
理解 Oracle 用户配置流程

用户配置流程看起来与任何其他业务流程都很相似。它代表一种事件的逻辑流，这种流程用来在企业资源范围内创建账户，创建一个新的用户产品。

每种配置过程都使用一些基本的构建块，下面的内容讲解了用户配置过程中的各种复杂级别。很显然，你对复杂级别的选择取决于特殊资源的必要性和敏感性。配置过程的复杂性级别通常与待配置访问资源的风险级别有关系。对于保存重要敏感数据的系统或者数据库，配置应该强制执行更可靠的验证流程，比如，请求某些用户属性(比如工作代码或资历)和在授予关键系统的账户访问权限之前管理审批。按照传统做法，这些高级配置流程是手工执行的，但是利用 OIM 的流程集成功能，许多这些配置强制任务可以被自动执行。下面的内容为用户配置中流程相关的问题提供了一些配置解决方案。

● 自由选择的账户配置

自由选择账户配置是一种配置类型，在这种类型中现有的 OIM 管理员或者是已授权的用户可以以自由选择的方式给用户分配应用。本质上，自由选择方法的一致性更差一些，它要求管理员必须知道该做什么，而不是利用配置过程中编制好的策略来做。默认情况下，在 OIM 利用打包的连接器设置到应用时，这种配置方式是自动设置的。而且，企业通常利用这种方式作为开始设计和实施他们自动化规则的基线，以使得流程自由选择的程度更弱一些。要在这种方式下把资源分配给用户，你需要利用 OIM 管理控制台的“用户资源属性”选项，如图所示，点击“配置新资源”按钮来启动“配置新资源”向导。

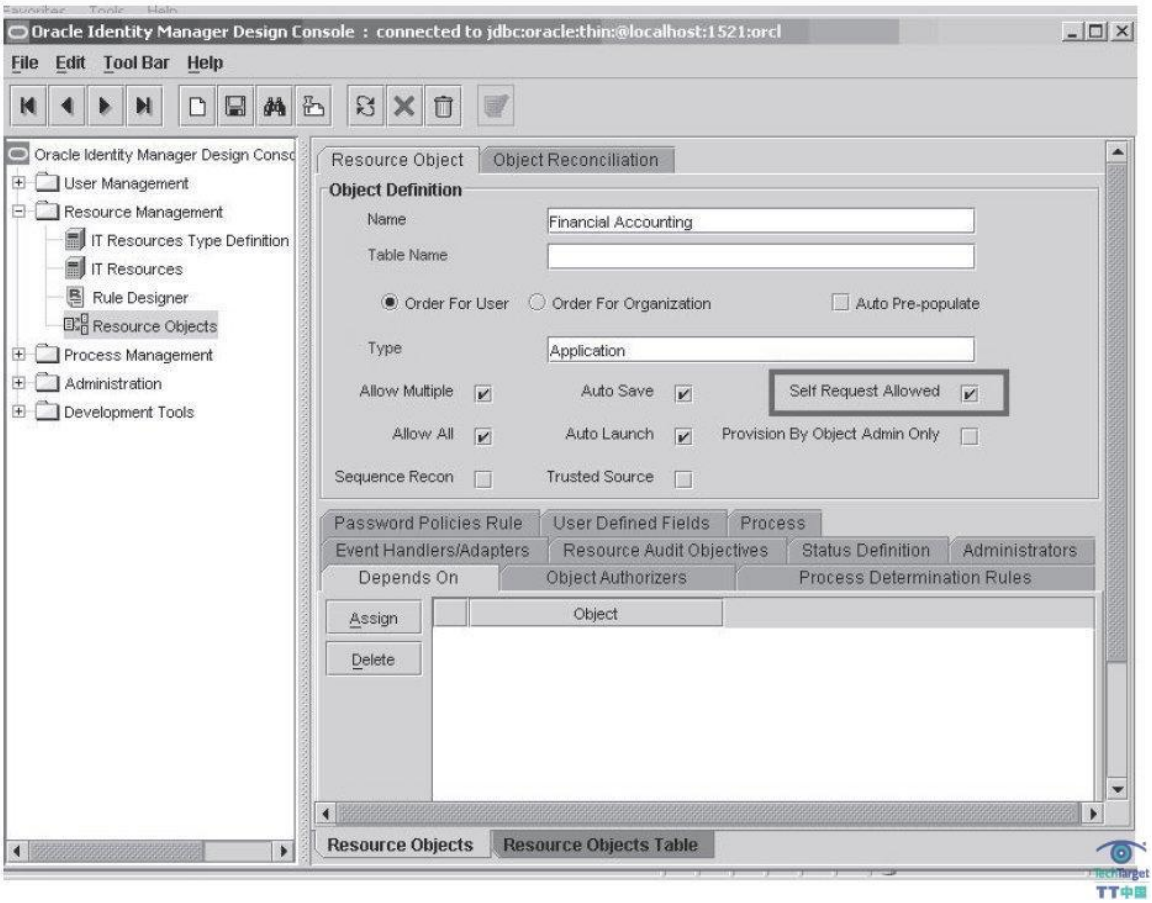


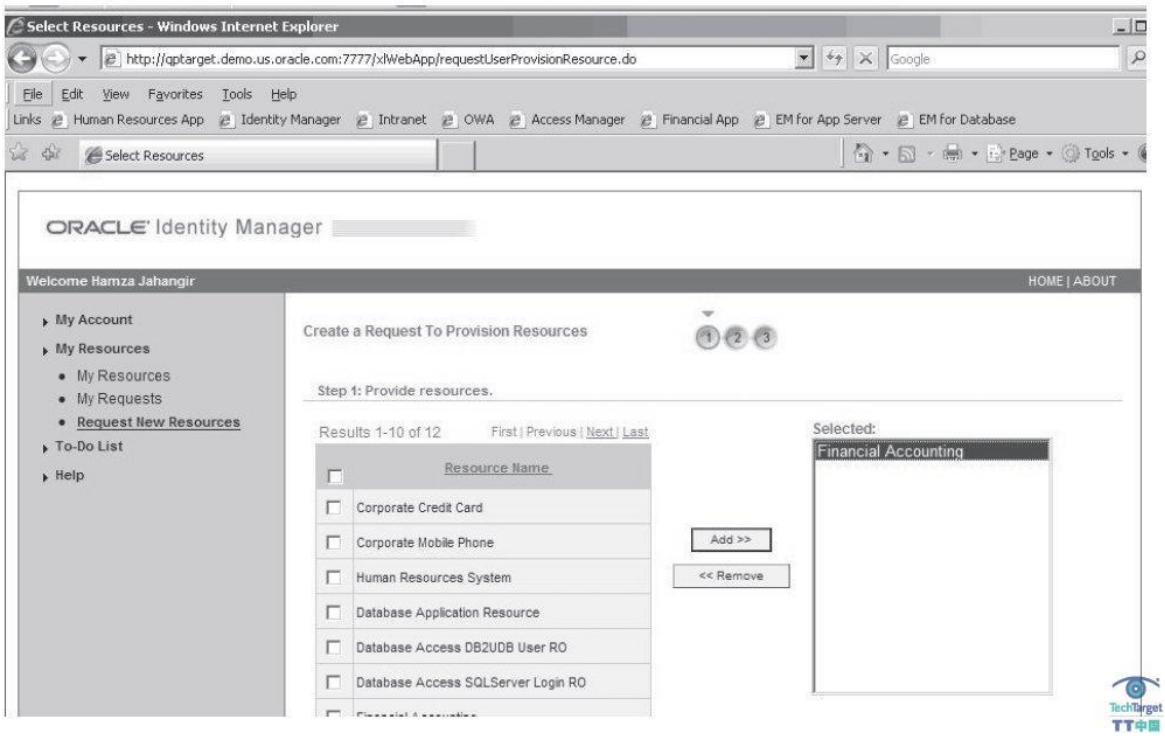
通常，自由选择配置的方式适用于那些期望在从手工配置流程向基本的自动化水平和集中管理方面迈出第一步的企业。此外，如果企业在访问系统和信息方面缺少正规的管理规则和策略，那么基于请求的方式处理配置请求可能是必经的第一步。然而，如果 OIM 已经实施到位了，你可以通过借助一批内建的 OIM 特性加速你改进配置自动化的途径，比如，允许用户通过 OIM 发起请求，执行像密码重置这样的基本的维护任务。

- **自助服务配置**

自由选择账户配置要求管理员或者有权限的用户来启动配置过程。换句话说，用户仍然需要打个电话或者发一封电子邮件给管理员，申请一个针对某个应用的账户。然而，OIM 很容易就可以配置为自助形式，这样用户在请求对新资源的访问权限时完全可以通过 OIM 框架进行交流。要实现这一点，你需要在你想设置的资源对象上把“允许自助服务”标记设置为启用。下图展示了配置界面中的该选项。

一旦对某个资源设置了这项配置，在 OIM 管理控制台的“请求新资源”选项中，该资源就会出现在选项列表中，如下图所示：



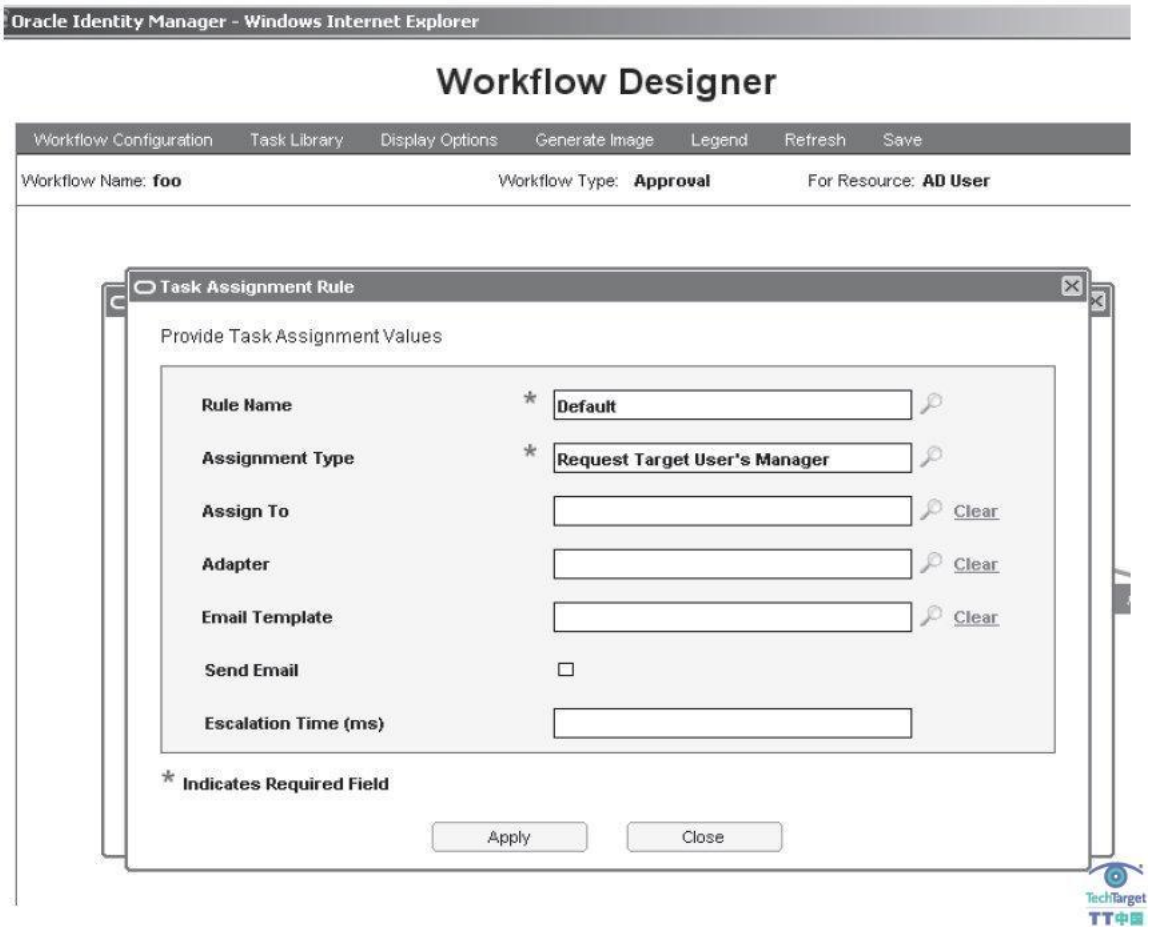


在过去几年里，自助服务用户配置已经成为了一种很流行的解决方案，特别是在提供像重设密码和在新系统和应用中申请账户这类简单功能时用的更多。它能极大地降低管理员的负担，避免根据终端用户提交的纸质请求以手工输入数据的方式执行重复性很高的任务。然而，在资源中启用自助服务功能通常会导致一些人为疏忽，比较有代表性的是强制通过审批工作流程，允许管理员核对和签收终端用户的请求。没有了这些审批，资源可能又成了完全公开的资源。

- **基于工作流的配置**

基于工作流的配置流程在给用户授权访问应用程序或者其他资源之前，会从指定的审批人收集需要的申请。例如，财务应用程序可能要求每一个新申请的账户都必须有 CFO 审批，来维持对可以访问敏感财务信息的人员做到严密控制。

要设置审批工作流，你可以利用 OIM 管理控制台的图形化工作流设计器，你可以按如下标签页顺序找到它：资源管理|管理|资源名称|资源工作流|创建新工作流。



要继续上图中的例子，我们将在“财务会计”资源对象上创建一个审批工作流，要求有两次审批：一次是用户的经理审批，另一次是应用程序管理员的审批。下面是创建该工作流的步骤：

1、指定描述性的名称，创建审批工作流。

2、右击“工作流设计器”，创建一个新任务。

3、双击新创建的任务，跳转到“分配”标签页。

4、编辑默认规则，选择“分配类型”，如图 9-6 所示。

5、选择“请求目标用户”的“经理”类型，它被配置为通过请求终端用户的经理来请求批准。

6、一旦两个任务都设置好了，也适当地配置好了，就可以通过右击“开始”图标，然后选择“添加非条件任务”来建立流程序列了。然后把箭头拖拽到你的第一个任务(经理审批)上去。

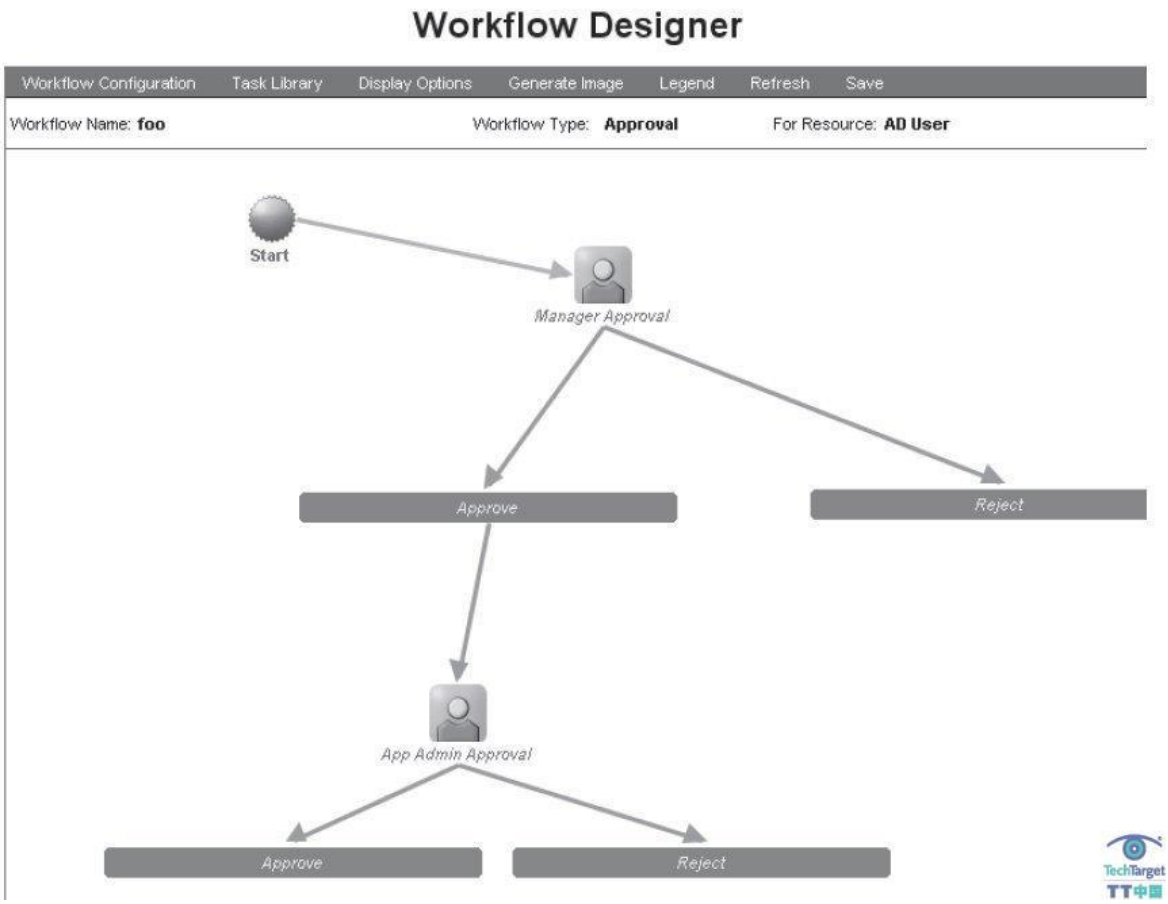
7、右击你的第一项任务中的“审批”框，选择“添加反应生成的任务”，然后把箭头拖拽到第二个任务(应用管理员审批)上来完成工作流。下图展示了该工作流的完整视图。

● IT 资源

让我们回想一下驱动用户配置工作的两个关键问题：

1、谁对什么资源有访问权限?

2、谁应该获得什么资源?



需求驱动的配置确实帮助我们回答了第一个问题，因为所有用户配置都通过集中的流程产生，因此可以跟踪谁被配置到了哪里。然而，对于第二个问题，请求驱动的方式不能负责确保用户是否应该访问某个资源，因为配置是以自由选择的方式产生的。

要解决这个问题，企业安全机构必须帮忙提供给我们一套访问策略，在其中定义关于“谁应该访问什么资源”的规则。一旦那些策略被定义好了，你可以非常容易地在 OIM 中通过 Web 管理控制台的“访问策略选项”配置它们。

在设置访问策略时，需要按下面的高级别步骤配置：

1、在 OIM 中找到“创建访问策略”选项。

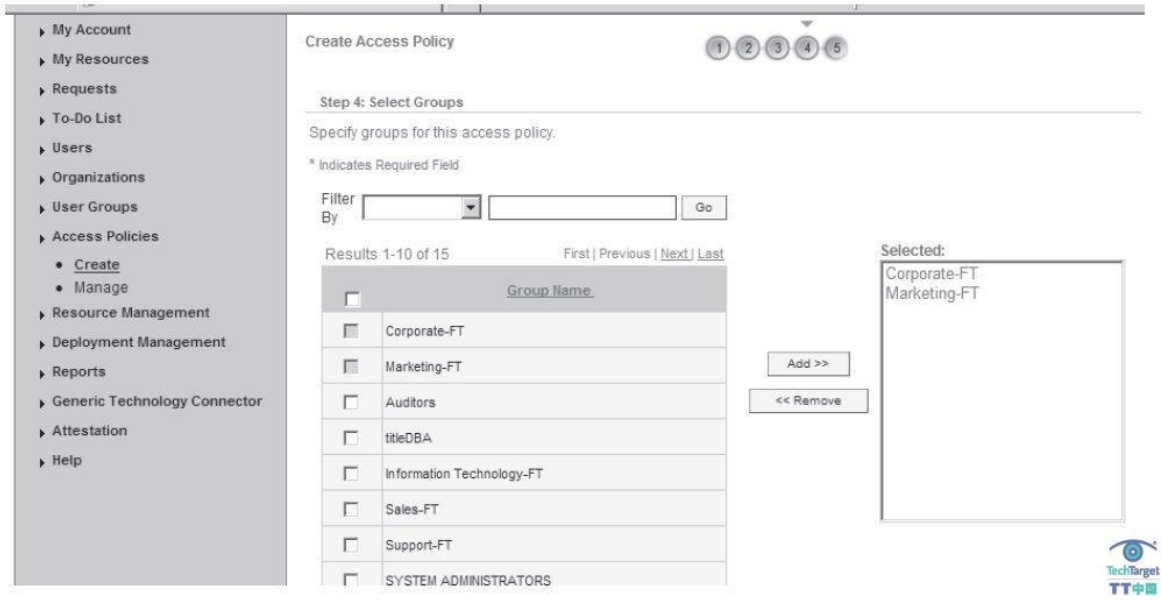
2、在选中的访问策略下选择待分配的资源，如下图所示。

3、设置应该让访问生效的日期。

4、通过该访问策略，选择应该拒绝用户访问的资源。

选择应用该访问策略的用户组，如图所示。

一旦你定义好了访问策略的这四个方面(分配什么，什么时间生效，不分配什么，给谁分配)，你就准备好让你企业的大部分用户通过收集这些访问策略实现配置自动化了。如果你已经定义了审批工作流，访问策略会自动触发那些流程通过适当的权限流转。



使用 Oracle 身份管理器的集成功能

OIM 的关键优势之一就是它那灵活的集成平台。然而，高度灵活的框架通常会变得更复杂，不易于使用。因此，自 9.1 版本起，OIM 提供了几种集成模式，支持用户在对外部系统开发集成应用时选择灵活性和复杂性的级别。我发现这种方式或多或少也符合二八原则：大约 80%的用例是由 20%的集成类型满足的。那 20%的集成类型被简化成了标准的连接器和模板。

OIM 支持两种类型的系统集成：配置和协调。配置利用从 OIM 资产库中获取的数据，自动从 OIM 服务器创建账号，分配应用程序或者资源。协调基于外部身份源(即，真实的源)自动化进行 OIM 身份记录的创建。多数情况下，OIM 把外部

人力资源应用作为权威的员工数据来源进行协调，然后配置到业务生产应用，比如电子邮件，内部门户网站，以及其它 ERP 系统。

协调集成方式通常由业务事件驱动，比如新员工入职，增加新客户，组织机构变更，员工调动，等等。既然这些业务事件是在 ERP 系统中启动的(大多数情况下也可能是人力资源系统)，那么配置 OIM 把协调集成的方式设置到那些系统就很有意义了，那样它可以监听到相关的身份变化事件。OIM 采用两种协调方式：信任源协调和目标资源协调。

● 信任源协调

信任源协调(TSR)用于协调从外部可靠来源(比如，人力资源系统，CRM，等等。)获取到的信息，通常会涉及到对 OIM 本地信息库的创建，修改或者删除用户等操作。如果配置了合适的用户组合访问策略，外部协调时间可以触发配置流程在配置了用户的应用和资源中创建或修改账户数据。例如，一条新员工记录进入人力资源系统会触发在 OIM 中(通过协调)创建一条相应的记录，然后会接着触发配置事件(通过配置策略)在 MS Exchange 电子邮件服务器中创建电子邮件账号。

信任源协调 TSR 有两种实现形式：

基于属性的方式。每种信任源都负责协调用户的一个或多个属性。例如，人力资源系统可以被认为是拥有姓和名属性的权威来源，而企业 LDAP 服务器可以认为是电子邮件地址属性的可靠来源。

基于用户类型的方式。每种信任源负责协调 OIM 中一种特定类型的用户。例如，HR 系统可以是员工数据的信任源，而 CRM 系统可以是客户类用户类型的信任源。

- **目标资源协调**

目标资源协调(TRR)主要被用来协调已配置用户的数据变化。例如，如果有人在活动目录中修改了用户的电话号码，而没有在 OIM 管理控制台中相应修改，那么 OIM 可以利用 TRR 配置来协调这种变更。

TRR 是 OIM 中非常强大的一个功能，因为它不仅可以从外部源选择简单的属性变更，而且它还能用来迅速识别外部系统中的流氓账户。

TRR 是 OIM 中非常强大的一个功能，因为它不仅可以从外部源选择简单的属性变更，而且它还能用来迅速识别外部系统中的流氓账户。如果有人试图在外部资源(比如，活动

目录)中创建一个授权的账户，TRR 可以检测到潜在的问题账户，然后根据你的配置采取一些步骤。例如，TRR 可以配置自动禁用流氓账户，直到管理员明确地对该访问重新授权才生效的策略，

TRR 对于协调目标系统(比如，LDAP 组，角色，等等)中的值列表也是很有用的，这样你可以映射访问策略到实际的目标系统角色和组。

Oracle 身份管理器连接器功能简介

OIM 与外部目标系统之间的每种集成选择都会归结到下面的分类中：

- 预建连接器。它是为专门的系统或者应用程序实现的专用连接器。比如：活动目录，仁科应用，SAP 应用，DB2，Oracle 数据库，等等。
- 通用技术连接器。它是为通用格式和业界标准建立的连接器。比如：展平文件，Web 服务，以及服务配置标记语言。

- **预建连接器**

OIM 提供了一个连接器包，其中为绝大部分各种类型的第三方系统批量预建和打包了连接器。这些系统包括数据库，企业资源计划(ERP)应用，操作系统，轻量级目录访问协议(LDAP)服务器，等等。在 OIM 中设置这些连接器是非常简单的过程：

1、把连接器文件复制到 OIM 服务器。

2、使用 OIM Web 控制台中的“部署管理”选项，导入连接器描述文件(基于 XML 的文件)到 OIM 资产库。

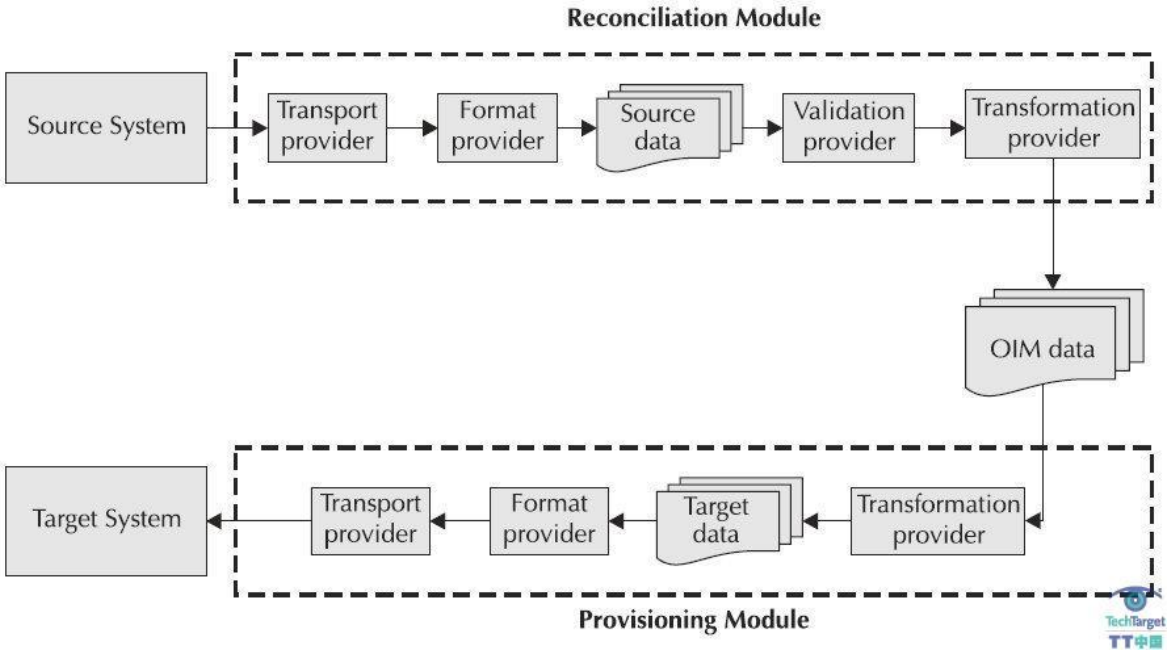
3、定义关联到此连接器的 IT 资源。通过这个连接器安装流程，OIM 会自动创建新资源的基本元素，创建必要的资源，(各种)IT 资源，以及关联到该连接器的 IT 资源类型对象。到这个程度，环境已经具备了基本的请求驱动配置的条件。

● 通用技术连接器

在 Oracle 收购 OIM 产品之后，向其中添加的第一批功能之一就是通用技术连接器(GTC)的开发。Oracle 意识到 OIM 在支持高端系统集成问题方面表现的非常出色。比如，利用预建连接器连接到 ERP 系统和 LDAP 服务器，或者在 OIM 开发框架上层开发定制的连接器。但是，对于规模更小一点的应用，可能是部门级的应用来说，这些应用可能是基于更简单的数据库技术(比如，Application Express 或者微软的 Access 数据库)构建的，没有更简单的方式来实现 OIM 向这些应用快速简单的集成。当企业期待使所有类型的应用(不管是企业级应用，还是部门级应用)实

现自动化配置时，Oracle 需要一套面向那些应用和系统的解决方案，实现以更简单的方法配置。这就是 GTC 的起源，在 OIM 9.1 中有介绍。

GTC 支持对定制构建的应用或者基于更简单的数据交换格式(比如，逗号分隔的字段)的其它系统进行简单的集成。它还支持许多业界标准协议，比如，服务配置标记语言(SPML)。GTC 是利用通用应用程序集打包集成的另一个例子，可以以一种标准的格式读取和交换信息。虽然 GTC 不必解决所有复杂的集成情况，但它确实为中低复杂程度的应用提供了一种快速集成的途径。图 9-10 描绘了基于 GTC 集成的配置过程。

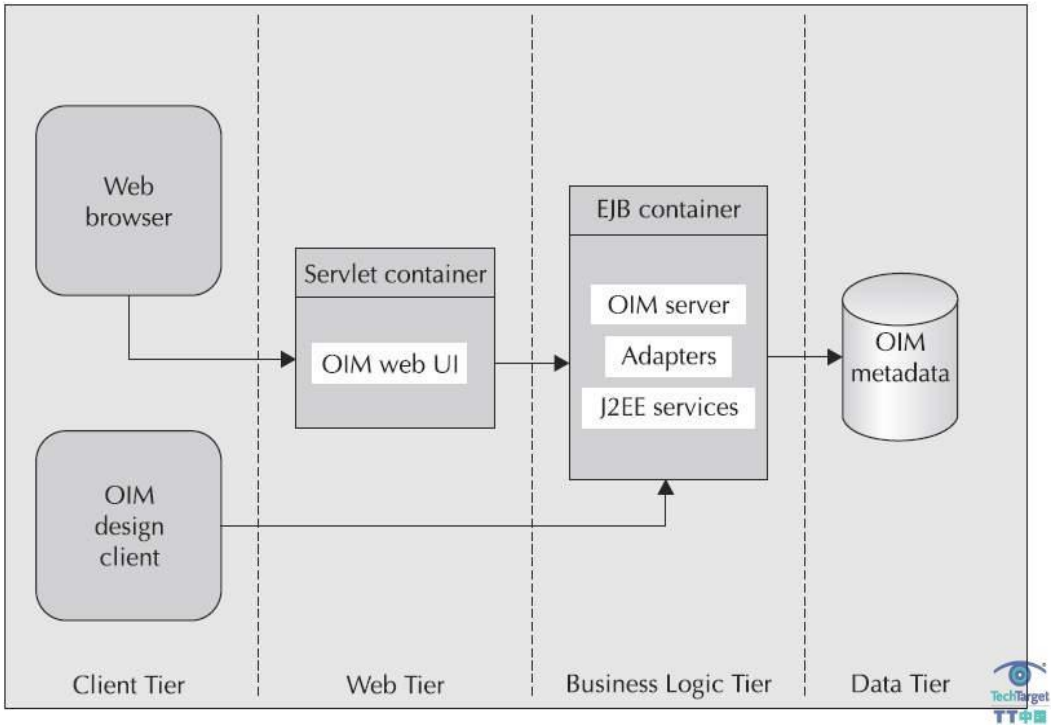


基于 GTC 的集成提供了一组打包功能，我们称之为“供应器”，它们执行端对端用户配置流程中需要执行的不同类型动作。这个过程由从原系统身份数据协调开始，到向配置目标应用完成。

在任何时候，你需要处理支持更简单的或者标准数据交换格式(比如，逗号分隔的文件或者 SPML 格式)时，GTC 都是一种有用的选择。通常情况下，设置和维护基于 GTC 集成的成本比其它类型的 OIM 集成成本要低很多。与预建连接器不同，GTC 代码包含在 OIM 服务器，这样就不需要安装额外的软件。

分析 Oracle 身份管理器的部署模型

每一种 OIM 组件(设计客户端，web 应用和核心服务器引擎)都是用 Java 编写，而且是以多层部署模型实现的，如下图所示：



客户层。在使用 OIM 时，有两种类型的客户端可用：一种是基于 web 的管理控制台，另一种是设计时客户端。Web 管理控制台主要用于管理用户，资源和支撑它们的所有构件。设计时客户端是身份管理流程的开发人员为设计和配置核心组件(比如：资源对象，IT 资源，配置流程，与被配置或者协调的物理应用交互的集成配置)而使用的。两种类型的客户端都遵守分布式交互模型，这样你可以用任意多客户端，从任意多计算机上与 OIM 业务逻辑层定义的相同的策略集和对象交互。

Web 层。该层以 OIM 管理用户界面 Web 应用容器的形式存在。它是基于纯 Java 的 Web 应用环境，使用了像 JSP，servlet，Struts 和 JavaBean 这类技术。由于使用了这些标准技术，OIM web 层可以被部署到许多应用服务器和容器中。

业务逻辑层。该层是 OIM 产品的核心。在这一层中，OIM 解决了谁(用户)来配置，配置到哪里(目标资源)和如何访问(流程)的问题。这一层也是完全用 Java 编写的，而且应用了 J2EE 设计模式，因此继承了组合-平台-中立和分布式组件架构的核心优点。基于 Java 的 OIM 业务层为新增集成连接器和适配器留出了标准开发平台。J2EE 的分布特性使得业务逻辑层可以跨多个应用服务器部署分布，而访问数据层的同一份公共元数据。

数据层。数据层是基于 SQL 的关系数据库，为用户配置平台存储所有身份信息，访问信息和配置信息的元数据。唯一可以允许存留在数据库之外的数据是 JAR 文件(Java 档案文件)，其中包含连接第三方资源和目标系统的代码。数据层是被业务层

排他访问的，不应该为了直接操纵数据的目的与任何外部客户端和工具直接集成。实际上，我们推荐你考虑使用 Oracle 数据库保护技术(比如 Oracle 数据库 Vault 和透明数据加密)，来加固和保护存储在 OIM 信息库中身份相关的敏感元数据。

总结

本次 Oracle 迷你电子书讨论了 Oracle 身份管理器的相关内容，这是一个易于理解，但是难以实现的用户配置领域。配置是每个企业都必须遵守的一个过程，不管手工执行还是以自动方式处理都要持续地进行。因此，优化这一配置流程对于达到运营的高效性，以及为避免流程被违背或忽略提供保证非常关键。安全问题还包括没有解除配置的孤立账户。开放的，未使用的账户是心怀不轨的员工和攻击者的立足点，也是法规审计人员寻求处理的问题列表中排在最前面的问题。企业要构建更好的流程和策略，降低管理负担;还要建立身份管理的一致性，在对信息的访问授权和监控方面建立一致性，对企业的所有资产实现更高级别的安全和保护。因此，真正成功的用户配置解决方案会在这两者之间做到平衡。

我们的编辑团队

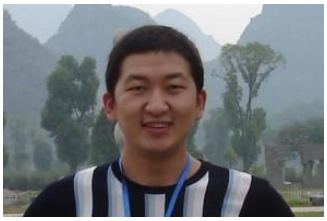
您若有何意见与建议，欢迎与我们的编辑联系。

诚挚感谢以下人员热情参与 TechTarget 中国《Oracle 系列电子书》的内容编辑工作！

诚邀更多的数据库专业人士加入我们的内容建设团队！

David Knox

David Knox 作为 Oracle 安全领域的专家，拥有超过十年以上的数据库安全工作经验，先就职于甲骨文公司，担任解决方案高级工程师，编写并出版过多本 Oracle 安全系列书籍。



冯昀晖

TechTarget 中国特邀技术编辑。资深软件工程师，有超过七年的政府和企业信息化软件解决方案经验，熟悉 SQL Server、Oracle 等数据库技术，爱好阅读、健身和中国象棋。